SYSTEM RELEASE 7.15
ASTRO® 25
INTEGRATED VOICE AND DATA

MCC 7100 IP Dispatch Console Setup and User Guide

JULY 2016

MN000672A01-E

Copyrights

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

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)
	For help identifying an item or part number, select choice 3 from the menu.
	302-444-9842 (International Orders)
	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
MN000672A01-A	Original release of the *MCC 7100 IP Dispatch Console Setup and User Guide*.	October 2014
MN000672A01-B	Terminology update changing CRYPTRmicroManagement to CRYPTRManagement and CRYPTR 2 to CRYPTR, along with another minor updates of the *MCC 7100 IP Dispatch Console Setup and User Guide* manual.	October 2015
MN000672A01-C	Updated section with two restrictions while managing peripheral configuration profiles. See Peripheral Configuration Profile.	December 2015
MN000672A01-D	Added note to Configuring Windows SNMP Components for a Console Inside the ASTRO RNI on page 48.	April 2016
MN000672A01-E	MOTOPATCH installation is now indicated as optional in the following sections: • Installing the MCC 7100 IP Dispatch Console Inside the ASTRO RNI on page 42 • Upgrading an Existing MCC 7100 IP Dispatch Console on page 44 • Recovering an MCC 7100 IP Dispatch Console Installation on page 84 • Setting Up the PRX 7000 Console Proxy on page 89 • Recovering a PRX 7000 Console Proxy Installation on page 99	July 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

Send Feedback

This page intentionally left blank.

About MCC 7100 IP Dispatch Console Setup and User Guide

This manual provides setup and user guide descriptions for the MCC 7100 IP Dispatch Console (software only) feature. It also describes the requirements and considerations necessary for implementing this feature in an ASTRO® 25 system.

What is Covered In This Manual?

This manual contains the following chapters:

- MCC 7100 IP Dispatch Console Description on page 29, describes the MCC 7100 IP Dispatch Console, its components and operational features.

- MCC 7100 IP Dispatch Console Setup and Installation on page 39, provides setup and installation procedures for all components related to the MCC 7100 IP Dispatch Console.

- PRX 7000 Console Proxy Setup and Installation on page 89, provides information and activities associated with the setup and installation of the PRX 7000 Console Proxy.

- USB Audio Interface Module on page 101, provides information and activities associated with the setup and installation of the USB Audio Interface Module.

- Console Dispatch Status and Peripheral Configuration Tool on page 119, provides descriptions and procedures for using the Peripheral Configuration Tool and Console Dispatch Status that are installed as part of the MCC 7100 IP Dispatch Console and PRX 7000 Console Proxy installations.

- Instant Recall Recorder on page 141 provides descriptions and procedures for using the Instant Recall Recorder that is installed as part of the MCC 7100 IP Dispatch Console.

- MCC 7100 IP Dispatch Console Additional Procedures and Information on page 151, provides additional helpful procedures and information that are not part of the typical MCC 7100 IP Dispatch Console installation.

- Enhanced Alert Tones on page 159, provides information about creating customized alert tones and using them on the MCC 7100 IP Dispatch Console.

- MCC 7100 IP Dispatch Console System Release Compatibility on page 165, support using the MCC 7100 IP Dispatch Console in ASTRO® 25 System Release 7.11 and ASTRO® 25 System Release 7.13.

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

For associated information about the radio system, see the following documents.

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides standards and guidelines that should be followed when setting up a Motorola communications site.

Table continued…

Related Information	Purpose
	Also known as 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 Documentation Overview	For an overview of the ASTRO® 25 system documentation, open the graphical user interface for the ASTRO® 25 system documentation set and select the **System Documentation Overview** link. This link opens a file that includes: • ASTRO® 25 system release documentation descriptions • ASTRO® 25 system diagrams For an additional overview of the system, review the architecture and descriptive information in the manuals that apply to your system configuration.
Dynamic System Resilience	Provides information necessary to understand, operate, maintain, and troubleshoot the Dynamic System Resilience (DSR) feature which may be implemented on your ASTRO® 25 system. This feature adds a geographically separate backup zone core to an existing zone core to protect against catastrophic zone core failures.
Conventional Operations	Provides information regarding conventional channel resource operating characteristics in standalone systems or ASTRO® 25 radio communication systems with K Series, L Series, or M Series.
MCC 7500 Dispatch Console with Voice Processor Module	Describes site-level characteristics of VPM-based Console Dispatch sites including theory of operation, installation, and configuration for hardware and software, operation, maintenance, and troubleshooting information.
MCC 7500/7100 Elite Admin User's Guide	Provides administrators with information required to configure and administer the Elite Dispatch software application to enable communication paths between dispatch console operators and radio system resources for the MCC 7500 and MCC 7100 dispatch consoles.
MCC 7500/7100 Elite Dispatch User's Guide	Provides user guide information intended for dispatch console operators. This manual describes how to use the Elite Dispatch software application supporting the MCC 7500 and MCC 7100 dispatch consoles.
Dispatch Console Backward Compatibility Guide	The Dispatch Console Backward Compatibility Guide is a reference guide that provides a list of console features supported by various ASTRO® 25 system releases. While the backward compatibility feature makes it possible to use an MCC 7500 Dispatch Console or MCC 7100 IP Dispatch Console in a system release previous to the system release in which the console was introduced, the features available for a backward compatible console can be limited to those identified in this manual.

Chapter 1

MCC 7100 IP Dispatch Console Description

The MCC 7100 IP Dispatch Console is a software-based dispatch console that requires no external hardware connections to perform dispatch operations. The MCC 7100 IP Dispatch Console can be located inside the ASTRO® 25 Radio Network Infrastructure (RNI) at a console site or conventional subsystem. It can also be deployed outside the ASTRO® 25 RNI and connected over the Internet through a firewall to a console proxy located inside the ASTRO® 25 RNI.

Figure 1: MCC 7100 IP Dispatch Console System Diagram
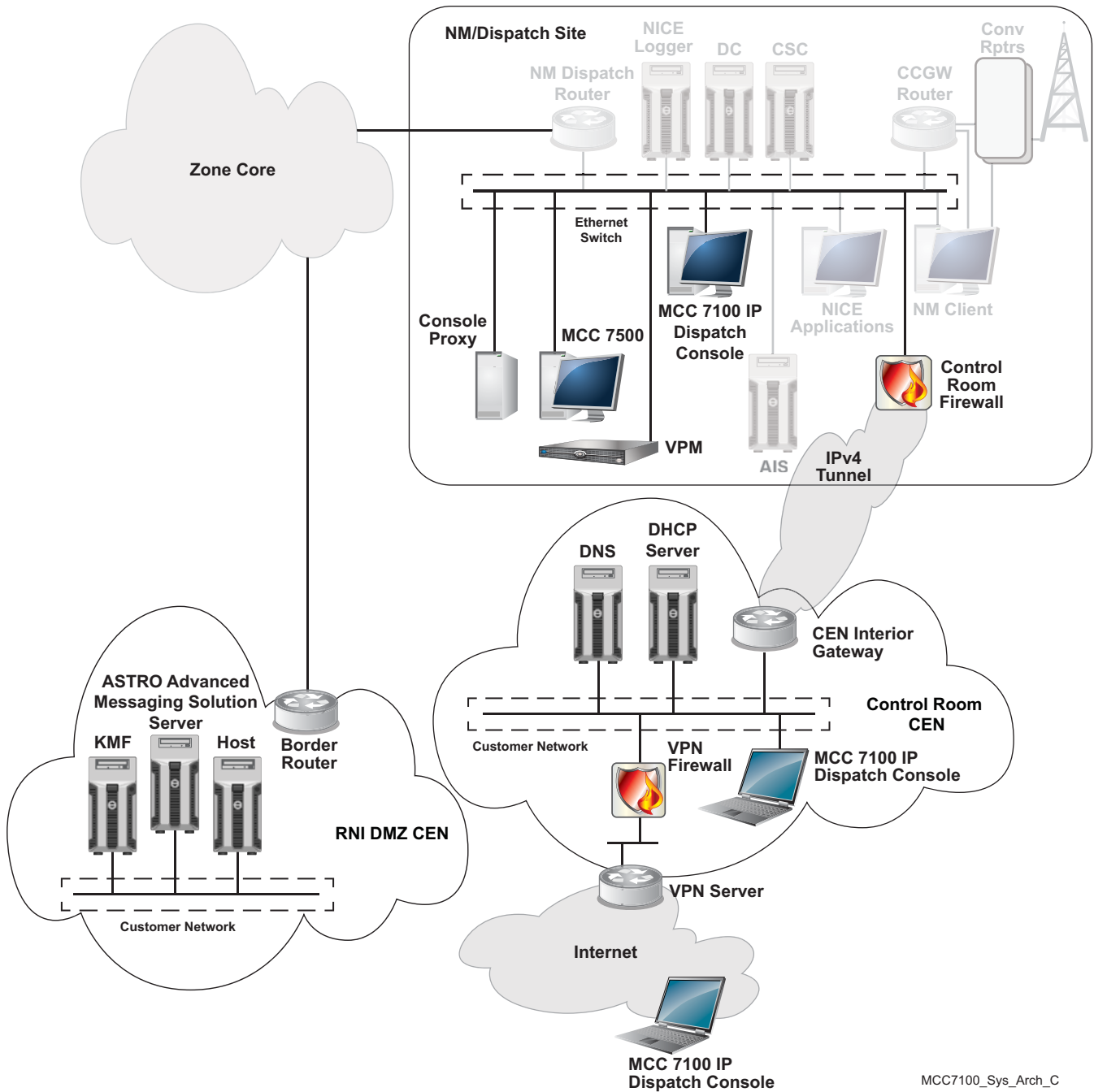
The MCC 7100 IP Dispatch Console system components include :

- MCC 7100 IP Dispatch Console Software
- PRX 7000 Console Proxy
- Console Site Control Room Firewall
- Customer Supported Components:
  - DNS Server
  - DHCP Server
  - Customer Enterprise Network (CEN) Firewall

- Virtual Private Network (VPN)

MCC 7100 IP Dispatch Console in Console Site Architectures

Dispatch console sites can have one or more console operator positions. The location of the dispatch console, the system architectures it supports, and your organizational requirements determine the equipment required at a console site.

An MCC 7100 IP Dispatch Console is supported in K, L, and M core system architectures. An MCC 7100 IP Dispatch Console is not supported in ASTRO® 25 Express systems.

The MCC 7100 IP Dispatch Console can be located in the following console sites:

• Console Site - inside the ASTRO® 25 Radio Network Infrastructure (RNI)

• Remote Console Site - outside the ASTRO® 25 RNI

• Remote Console Site at a Distributed Conventional Hub Site in a Conventional Subsystem

MCC 7100 IP Dispatch Console Features

This section provides a list of features supported by the MCC 7100 IP Dispatch Console as compared to the MCC 7500 Dispatch Console within the following areas:

• System Level

• ASTRO® 25 Trunking

• ASTRO® 25 Conventional

• MDC 1200 Conventional

• Analog Conventional

• General Security

• Integrated Tone Paging Encoder

• Peripheral Configuration Tool

• Console Dispatch Status

• Integrated Instant Recall Recorder

System Level Features

This section provides a list of the system level features supported by the MCC 7100 IP Dispatch Console.

Table 1: System Level Feature for the MCC 7100 IP Dispatch Console

System Level Feature	
Co-hab with ASTRO® 25 Advanced Messaging Solution Smart Client	Full Participation in Radio System Agency Partitioning
Configured via Radio System Configuration Manager	Participation in Radio System Fault Management when in ASTRO® 25 Radio Network Infrastructure (RNI)
Deployment inside or outside the ASTRO® 25 RNI	Supports Enhanced Local Alias Management (ELAM)

ASTRO 25 Trunking Features

This section provides a listing of the ASTRO® 25 Trunking features supported by the MCC 7100 IP Dispatch Console.

Table 2: ASTRO 25 Trunking Feature for the MCC 7100 IP Dispatch Console

ASTRO® 25 Trunking Feature	
Advanced Multi Band Excitation (AMBE) Half Rate Vocoder for Phase II Time Division Multiple Access (TDMA) Resources	Trunked Private Calls
Improved Multi-Band Encoder (IMBE)/AMBE Vocoder for ASTRO® 25 Resources	Trunked Push-to-Talk (PTT) ID and Alias
Trunked Announcement Group Calls	Trunked Tactical/Normal
Trunked Call Alerts	Trunked Talkgroup Calls
Trunked Emergency Alarms	Trunked Remote Monitor
Trunked Emergency Calls	Trunked Repeater On/Off

ASTRO 25 Conventional Features

This section provides a list of the ASTRO® 25 Conventional features supported by the MCC 7100 IP Dispatch Console.

Table 3: ASTRO 25 Conventional Feature for the MCC 7100 IP Dispatch Console

ASTRO® 25 Conventional Feature	
Autokey Key Display	Secure Keyset Select
Call Alert	Radio Check
Emergency Alarm and Call	Radio Enable/Disable
Ignore Mobile to Mobile Calls	Radio Message Display
Mixed Mode (Analog/Digital) Operation	Radio Status Display
Momentary Key Override	Radio Status Request
Push-to-Talk (PTT) ID and Alias	Received Key Display
Secure Call	Remote Monitor
Secure Key Select	Voice Selective Call

MDC 1200 Analog Conventional Features

This section provides a list of the MDC 1200 analog conventional features supported by the MCC 7100 IP Dispatch Console.

Table 4: MDC 1200 Analog Conventional Feature for the MCC 7100 IP Dispatch Console

MDC 1200 Conventional Feature	
Call Alert	Radio Check
Emergency Alarm	Radio Message Display

Table continued…

MDC 1200 Conventional Feature	
Emergency Call	Radio Status Display
Ignore Mobile-to-Mobile Calls	Radio Status Request
Push-to-Talk (PTT) ID and Alias	Remote Monitor
Radio Enable/Disable	Voice Selective Call

Analog Conventional Features

This section provides a list of the analog conventional features supported by the MCC 7100 IP Dispatch Console.

Table 5: Analog Conventional Feature for the MCC 7100 IP Dispatch Console

Analog Conventional Feature	
Analog Talk & Listen	Private Line (PL) Selection
E & M Control	Repeater On/Off
Frequency Selection	RF Cross Busy
Line Operated Busy Light (LOBL)	RF Cross Mute
Main/Alternate Conventional Interfaces	Tone Remote Control
Monitor	Supervisor Takeover (via Relay)
Mute Second Receiver	WildCard I & II

NOTICE: A conventional talkgroup has cross busy indications that show activity by other talkgroups on the same conventional talkgroup channel or a RF cross busy conventional talkgroup channel. However, when the MCC 7100 IP Dispatch Console is deployed outside the ASTRO® 25 Radio Network Infrastructure (RNI), these indications may be delayed, which reduces their usefulness.

Encryption Features

This section provides a list of the encryption features supported by the MCC 7100 IP Dispatch Console.

Table 6: Encryption Feature for the MCC 7100 IP Dispatch Console

Encryption Feature	
Advanced Encryption Standard (AES) Algorithm	Multi-Select Cross-Mode Alert
Advanced Digital Privacy (ADP) Algorithm	Patch Cross-Mode Alert
Clear Audio Alert	Receive Cross-Mode Indication
Digital Encryption Standard – Output FeedBack (DES-OFB) Algorithm	Software or Hardware based encryption
Key Management via Key Variable Loader (KVL) for Micro SD card only	Supports Multiple Algorithms Simultaneously
Key Management using Over The Ethernet Keying (OTEK)	Supports up to 5, 10, 15, 20 Encrypted Calls Simultaneously

Table continued…

Encryption Feature	
Key Management via Store and Forward for Micro SD card only	

Integrated Tone Paging Encoder Features

This section provides a list of the integrated tone paging encoder features supported by the MCC 7100 IP Dispatch Console.

Table 7: Integrated Tone Paging Encoder Feature for the MCC 7100 IP Dispatch Console

Integrated Tone Paging Encoder Feature	
ASTRO® 25 Conventional Call Alert	Simultaneous Paging Operation
Digital Dial 1 (1500 Hz)	Quick Call I
Digital Dial 2 (2805 Hz)	Quick Call II B - Tone & Voice
Digital Dial 3 (1500/2805)	Quick Call II C - Tone Only
Knox	Quick Call II D - Battery Saver
Manual Group Pages	Quick Call II E - Competitive
Manual Individual Pages	Quick Page Buttons
MDC 1200 Call Alert	Selected Channel" Paging
Motorola 5/6 Tone	Single Tone 0.5
Pre-Defined Group Pages	Single Tone 1.5
Pre-Defined Individual Pages	Talk Extend
Private Line Stripping	Touch Code
Sequential Paging Operation	Trunked Call Alert

MCC 7100 IP Dispatch Console System Components

This section describes the main system components used with the MCC 7100 IP Dispatch Console.

MCC 7100 IP Dispatch Console

The MCC 7100 IP Dispatch Console is a software-based dispatch console that requires no external hardware connections to perform dispatch operations. Audio Vocoding is performed within the Microsoft Windows 7 operating system. If equipped, the MCC 7100 IP Dispatch Console can work with the computer built-in speakers and microphone.

External peripherals such as a microphone, headset, and footswitch are also supported. Use a minimum audio quality of DAQ 3.4 when using certified commercially available peripherals. The MCC 7100 IP Dispatch Console can be configured to dispatch trunking and/or conventional resources. The MCC 7100 IP Dispatch Console supports secure, Advanced Encryption Standard (AES), Advanced Digital Privacy (ADP), and Digital Encryption Standard - Output FeedBack (DES-OFB), end-to-end audio encryption. You can perform key storage through hardware CRYPTR micro or software. See Load Secure Keys and Algorithms on page 55 for details.

The MCC 7100 IP Dispatch Console can be located inside the ASTRO® 25 Radio Network Infrastructure (RNI) at a console site or conventional subsystem. The MCC 7100 IP Dispatch Console can also be deployed outside the ASTRO® 25 RNI and connect through a firewall to a PRX 7000 Console Proxy located inside the ASTRO® 25 RNI.

PRX 7000 Console Proxy

Use the PRX 7000 Console Proxy when MCC 7100 IP Dispatch Consoles are deployed outside the ASTRO® 25 Radio Network Infrastructure (RNI). Due to routing issues, multicast audio packets are unable to be sent outside of the ASTRO® 25 RNI into the customer network and ultimately over the Internet. The PRX 7000 Console Proxy is located at a traditional console site or in a conventional subsystem. The PRX 7000 Console Proxy is an application that converts multicast audio packets (delivered inside the ASTRO® 25 RNI) to unicast audio packets, and sends them outside of the ASTRO® 25 RNI to an MCC 7100 IP Dispatch Console. The PRX 7000 Console Proxy is also used to perform link maintenance inside the ASTRO® 25 RNI on behalf of the MCC 7100 IP Dispatch Consoles when deployed outside of the ASTRO® 25 RNI.

Console Site Control Room Firewall

The SSG 140 control room firewall used at a console site allows secured communications with outside networks. It is configured for Network Address Translation (NAT) functionality to help eliminate conflicts between an IP address in a Customer Enterprise Network (CEN) and an IP address in the ASTRO® 25 Radio Network Infrastructure (RNI). The control room firewall is configured to allow only dispatch console-related traffic to and from the CEN. The control room firewall communicates with the CEN interior gateway using Internet Protocol version 4 (IPv4).

The PRX 7000 Console Proxy communicates to the remote MCC 7100 IP Dispatch Console through a firewall. The firewall the console site allows traffic to/from the PRX 7000 Console Proxy and CEN. The user must provide any VPN functionality in the CEN.

The interior gateway in the CEN and the console site control room firewall share the link from the console site to the zone core.

A control room firewall can be installed at any console site in the system. Multiple control room firewalls can be in a system; one at each console site. The control room firewall is the demarcation point for the ASTRO® 25 network. The user provides the networking equipment used to establish a path to a remote MCC 7100 IP Dispatch Console.

NOTICE: An Intrusion Detection System (IDS) is not required at each console site, but is an option for security conscious users.

License Server

The license server is a web server used to generate a license file for activating an MCC 7100 IP Dispatch Console during installation. This file contains the required licensing information as well as the number of connections that the PRX 7000 Console Proxy supports. The license server is not part of the ASTRO® 25 Radio Network Infrastructure (RNI) or the Customer Enterprise Network (CEN). Motorola hosts the license server.

NOTICE: The Motorola Licensing group generates license files, and provides instructions on how to allocate and download license files.

Key Management Facility for MCC 7100 IP Dispatch Console

The Key Management Facility (KMF) is the centralized key manager in the ASTRO® 25 system. The KMF delivers keys securely, using the Over-the-Ethernet-Keying (OTEK) feature, to the MCC 7100 IP Dispatch Consoles configured with hardware-based encryption. For MCC 7100 IP Dispatch Consoles configured with software-based encryption, the KMF exports a file used to import keys into the console.

NOTICE: The KMF does not support Advanced Digital Privacy (ADP) keys.

Customer Enterprise Network Components

The network components that are provided by the customer are defined in this section. The following components reside within the Customer Enterprise Network (CEN):

- Domain Name Services (DNS) Server
- Dynamic Host Configuration Protocol (DHCP) Server
- Virtual Private Network (VPN) Server

DNS Server

The Domain Name Services (DNS) server contains a database of network hostnames and their associated IP addresses for Intranet resources connected to the Intranet. The DNS server contains entries for the ASTRO Radio Network Infrastructure (RNI) devices (PRX 7000 Console Proxy, ELAM Server, KMF, etc…).

DHCP Server

The Dynamic Host Configuration Protocol (DHCP) server assigns an IP address to a computer from a defined range of numbers configured for a given network. Each MCC 7100 IP Dispatch Console that is remote from the ASTRO RNI will be assigned a static IP address in the DHCP Server.

VPN Server

The VPN server allows for virtual private network (VPN) connections by an MCC 7100 IP Dispatch Console deployed outside the CEN. The MCC 7100 IP Dispatch Console connects to the CEN over the Internet. This provides individual dispatch operators with secure access to the CEN and ultimately to the ASTRO RNI.

MCC 7100 IP Dispatch Console Theory of Operations

This section describes the functional relationships between components that support the MCC 7100 IP Dispatch Console.

Zone Database Server and LDAP

The MCC 7100 IP Dispatch Console uses Lightweight Directory Access Protocol (LDAP). The Dynamic Host Configuration Protocol (DHCP) server assigns an IP address to a computer from a defined range of IP address numbers configured for a given network. Each MCC 7100 IP Dispatch Console outside the ASTRO® 25 Radio Network Infrastructure (RNI) is assigned a static address in the DHCP Server.

MCC 7100 IP Dispatch Console Encryption

The MCC 7100 IP Dispatch Console supports secure encryption. See Load Secure Keys and Algorithms on page 55 for a complete description on encryption.

MCC 7100 IP Dispatch Console Link Op

The first dispatch console at a console site that registers with the system and assigns a resource is known as the Link Op. The Link Op refers to the console that is in control of the active link between the site and the zone controller or site controller.

A Link Op is required at a site that contains a PRX 7000 Console Proxy so that an MCC 7100 IP Dispatch Console outside the ASTRO® 25 Radio Network Infrastructure (RNI) can operate. Every site, including remote console sites, require a Link Op inside the ASTRO® 25 RNI to operate. An MCC 7100 IP Dispatch Console outside the ASTRO® 25 RNI cannot become a Link Op.

> **NOTICE:** For more information, see the "MCC 7500/7100 Dispatch Console - Control Paths and Affiliation" section in the *Conventional Operations* manual.

MCC 7100 IP Dispatch Console and ISSI 8000/CSSI 8000

The MCC 7100 IP Dispatch Console operator position supports the ISSI 8000 feature. The MCC 7100 IP Dispatch Consoles receive foreign talkgroup and other foreign system configuration data downloaded from the PRX 7000 Console Proxy (Lightweight Directory Access Protocol (LDAP) server). See the *ISSI 8000/CSSI 8000 – InterSystem Gateway* manual for details.

Centralized Event Logging for the MCC 7100 IP Dispatch Console

The MCC 7100 IP Dispatch Console inside the ASTRO® 25 Radio Network Infrastructure (RNI) sends event logs to the Centralized Event Logging server in the same way as supported by the MCC 7500 Dispatch Console inside the ASTRO® 25 RNI, except for connection information. The MCC 7100 IP Dispatch Console deployed outside the ASTRO® 25 RNI does not send event logs to the Centralized Event Logging server. The PRX 7000 Console Proxy logs the following events with Centralized Event Logging server:

- Remote clients connected
- Remote clients disconnected
- Remote clients refused

See the *Centralized Event Logging* manual.

Audio Logging and the MCC 7100 IP Dispatch Console

The Archiving Interface Server (AIS) / Logger supports the logging of audio from an MCC 7100 IP Dispatch Console (inside and outside the Radio Network Infrastructure (RNI), as follows:

- Recording of console audio by the AIS/Logging recorder is supported.
- Local (Voice Processor Module (VPM)-based) audio logging is not supported.

> **NOTICE:** See the *MCC 7500 Dispatch Console with Voice Processor Module* manual for details.

MCC 7100 IP Dispatch Console Aux I/O Comparator Display

The Aux I/O comparator display function in the MCC 7100 IP Dispatch Console uses modified MOSCAD Remote Terminal Units (RTUs). The Aux I/O architecture is a client-server model where the MOSCAD RTU and the MCC 7100 IP Dispatch Console provide the server and client functionality, respectively.

The Aux I/O data for the comparator display function, that is, comparator controls, report status changes, and so on, between the RTU-server and the MCC 7100 IP Dispatch Console client is communicated through a TCP/IP connection established between the RTU and the MCC 7100 IP Dispatch Console.

The MCC 7100 IP Dispatch Console can connect to one or more RTUs by establishing a TCP/IP connection with each RTU. Similarly, an RTU can support multiple MCC 7100 IP Dispatch Console connections.

If the link between the remote MCC 7100 IP Dispatch Console and the Aux I/O server is lost, the affected MCC 7100 IP Dispatch Consoles no longer receives any of the comparator display functionality until it reestablishes a connection.

The MCC 7100 IP Dispatch Console supports up to 200 Aux I/Os on the SDM3000 units ("global" Aux I/O) functionality.

> **NOTICE:** The MCC 7100 IP Dispatch Console supports four local Aux Outputs with specific functions tied to them:
>
> - Indicating Emergency;
> - Indicating presence of an inbound call on the currently selected channel
> - Indicating a console PTT
> - Providing an external output to report activity of one or more general Aux I/Os of the console.

If you employ the Aux I/O Server device in a Conventional Subsystem, configure it properly to support the Unified Network Configurator (UNC) discovery. Perform the configuration using the SDM3000 Builder application. If the Aux I/O Server device used in a Conventional Subsystem is not configured properly, UNC discovery lists the device in the UNC Lost and Found folder. If this situation occurs, configure the device properly and rediscover it. For detailed information about the SDM3000 Builder, see the *MOSCAD Network Fault Management* manual. After the UNC recognizes the Aux I/O Server device in a Conventional Subsystem, you can use UNC to configure the device. For more information, see the *Unified Network Configurator* manual.

Chapter 2

MCC 7100 IP Dispatch Console Setup and Installation

This chapter provides setup and installation procedures for all components related to the MCC 7100 IP Dispatch Console.

MCC 7100 IP Dispatch Console Software Requirements

The MCC 7100 IP Dispatch Console requires a Windows-based computer or workstation running at least Windows 7 Professional 64-bit operating system with an approved service pack .

Windows XP and Windows Vista operating systems are not supported.

Windows 8 64-bit operating system or Windows 8.1 64-bit operating system are supported only outside the ASTRO® 25 Radio Network Interface (RNI). However, if you use hardware encryption, the CRYPTR micro requires the Windows 7 Professional 64-bit operating system with an approved service pack.

> **NOTICE:** Windows 7 Ultimate is supported but not required.

MCC 7100 IP Dispatch Console Hardware Requirements

The Motorola-certified HP Z420 desktop computer supports MCC 7100 IP Dispatch Console software. The software is also supported by a provided laptop or desktop computer provided by your organization, meeting the minimum hardware requirements in Table 9: Laptop Hardware Specifications on page 40.

Motorola-Certified HP Z420 Hardware Specifications

The following hardware specifications are for the Motorola certified HP Z420 workstation:

> **NOTICE:** The HP Z400 workstation does not support the MCC 7100 IP Dispatch Console software.

Table 8: Hardware Specifications for HP Z420 Workstation

Hardware	Specification
Processor	Intel® Xeon E5-1603, 2.8 GHz,1066Mhz memory, Quad Core
Hard Drive	250 GB 7200 rpm SATA 3.0 Gb/s NCQ
Hard Disk Controller	Integrated SATA controller
System Memory	4 GB total memory (2 x 2 GB DDR3 1600 MHz ECC)
LAN	Integrated Intel 82579LM PCIe GbE Controller
Optical Storage	16X SuperMulti DVDRW SATA
Keyboard	HP USB Standard Keyboard
Mouse	Microsoft Wheel Optical 3-button USB Mouse

Table continued…

Hardware	Specification
Graphics	NVIDIA Quadro NVS 310 512 MB Dual Head
Expansion Slots	2 PCI Express Gen3 x16 mechanical/electrical
	1 PCI Express Gen3 x8 mechanical/electrical
	1 PCI Express Gen2 x8 mechanical/x4 electrical
	1 PCI Express Gen2 x4 mechanical/x1 electrical
	1 Legacy PCI
Built-in I/O Ports	6 USB 2.0, 3 Serial,1 Parallel
Power Supply	600 W (90% efficient power supply)
Power Consumption	max 600 W

Laptop Minimum Hardware Requirements

The following hardware specifications are the minimum requirements for a laptop provided by your organization.

Table 9: Laptop Hardware Specifications

Hardware	Specifications
Processor	Intel® Core™ i5-3230M Processor (2.6 GHz, 3 MB cache, 2 cores)
System Memory	4 GB 1600 MHz DDR3 SDRAM (1 x 4 GB)
Hard Drive	250 GB 7200 rpm SATA 3.0 Gb/s NCQ
Optical Storage	Minimum of 1 DVD drive to install software
Network Interface	10/100/1000
Wireless (optional)	802.11a/b/g/n
Expansion slots	1 USB 2.0 port per peripheral. Expansion hub is also acceptable.
	If you use hardware key storage, a Native SD Host controller bus Interface is required.
	NOTICE: Ensure that the SD Host Controller manufacturer is compliant. See the MCC 7100 product planner for details on how to test if a computer has a compliant SD Host Controller.

MCC 7100 IP Dispatch Console Cohab Configurations

You can install the MCC 7100 IP Dispatch Console as a standalone product or cohabited with other applications.

IMPORTANT:
Before you install the MCC 7100 IP Dispatch Console software, uninstall any prior installations of dispatch console software, for example, MCC 7500 Dispatch Console software. See the *MCC 7500 Dispatch Console with Voice Processor Module* manual for removing the MCC 7500 Dispatch Console software.

Only one third-party or cohabitation application can be installed on an MCC 7100 IP Dispatch Console.

The MKM 7000 Console Alias Manager (CAM) Client and the third-party MACH Alert client are available from a dispatch console operator position through the Internet Explorer browser.

Inside the ASTRO® 25 Radio Network Infrastructure (RNI), the following cohabitation applications are supported:

- K core Configuration Manager
- ASTRO® 25 Advanced Messaging Solution Smart Client if required by your organization policies
- Radio Control Manager (RCM) if required by your organizations policies
- MKM 7000 CAM Server
- Client software for MCN Server 8000™ Remote Comparator Display Software from CTI Products

Outside the ASTRO® 25 RNI, the following cohabitation applications are supported:

- ASTRO® 25 Advanced Messaging Solution Smart Client

MCC 7100 IP Dispatch Console Call Capacities

The MCC 7100 IP Dispatch Console supports four capacities that are enforced by licensing. The capacities can also depend on the location of the dispatch console.

Table 10: MCC 7100 IP Dispatch Console Call Capacities

Maximum Number of Simultaneous Streams	Maximum Number of Resources Configured	Location	Voice Encryption
5	15	Inside ASTRO® 25 Radio Network Infrastructure (RNI) and outside ASTRO® 25 RNI	Advanced Encryption Standard (AES), Digital Encryption Standard – Output Feed-Back (DES-OFB), and Advanced Digital Privacy (ADP)
10	30	Inside ASTRO® 25 RNI and outside ASTRO® 25 RNI	AES, DES-OFB, and ADP
15	45	Inside ASTRO® 25 RNI only*	AES, DES-OFB, and ADP
20	60	Inside ASTRO® 25 RNI only*	AES, DES-OFB, and ADP

* If you deploy a higher tier dispatch console outside the ASTRO® 25 RNI, the number of the simultaneous streams it supports is automatically downgraded to ten streams.

Dynamic System Resilience Considerations

Dynamic System Resilience (DSR) strengthens ASTRO®25 voice and data communications networks for greater redundancy to ensure operational continuity in the event of disaster. Two cores support each zone in a system with DSR: a primary core and a geographically separate backup core. For more information, see the *Dynamic System Resilience* manual.

⚠️ **CAUTION:** An ASTRO® 25 Conventional System (K core) system does not support DSR.

When you install or upgrade a dispatch console in a system with DSR, the dispatch console must apply the DSR configuration to operate in the DRS mode. To enable the DSR mode, meet the following requirements during the installation:

- Allow the dispatch console to apply the DSR configuration: Start the Elite application to receive the following critical change notification that appears in the status bar of the application: `Critical configuration parameters have changed. Please reboot the PC to utilize the updates.` Reboot the computer or the dispatch console cannot apply the DSR configuration and operate in DSR mode. For example, it cannot operate when switching between the primary and backup Master Switching Office (MSO).

- Configure the primary and secondary DNS server addresses for both master sites. For the correct network settings, see Setting Up the Domain for an MCC 7100 IP Dispatch Console Inside the ASTRO Radio Network Infrastructure on page 66 and the system configuration documentation, or contact Motorola Solution Support Center (SSC) for further assistance.

> **NOTICE:** The console site can operate seamlessly on the primary master site with some dispatch consoles in a DSR mode, and others in non-DSR mode until the reboot of all dispatch consoles.

Setting Up the MCC 7100 IP Dispatch Console

Perform the following process to install the MCC 7100 IP Dispatch Console, and the necessary system components on which it depends, in your system.

Prerequisites: If you use a system with Dynamic System Resilience (DSR), see Dynamic System Resilience Considerations on page 41.

Process:

> Depending on the type of installation you need, follow one of these processes:
>
> - For a new installation inside the ASTRO® 25 Radio Network Infrastructure (RNI), see Installing the MCC 7100 IP Dispatch Console Inside the ASTRO RNI on page 42.
>
> - For a new installation outside the ASTRO® 25 RNI, see Installing the MCC 7100 IP Dispatch Console Outside the ASTRO RNI on page 43.
>
> - For an existing installation, see Upgrading an Existing MCC 7100 IP Dispatch Console on page 44.

Installing the MCC 7100 IP Dispatch Console Inside the ASTRO RNI

Follow this procedure for a new installation of the MCC IP Dispatch Console in the ASTRO® 25 Radio Network Infrastructure (RNI).

Process:

1 Optional: Install MCC 7500 Aux I/O Server. See "Aux I/O Server Installation" in the *MCC 7500 Dispatch Console with VPM* manual.

2 Configure Windows OS:

   a Install the operating system. See Windows Installation and Motorola Operating System Installer for MCC 7100 IP Dispatch Console on page 45.

   b Configure Windows Components. See Configuring Windows Components on page 46.

3 Generate License Certificates for the MCC 7100 IP Dispatch Console. See Generating License Certificates for the MCC 7100 IP Dispatch Console on page 50.

4 Configure Network Interface Card (NIC) on a computer or server inside the ASTRO® 25 RNI. See Configuring the Network Interface Card for an MCC 7100 IP Dispatch Console Inside the ASTRO RNI on page 51.

5 Optional: Install third-party or cohab software. See Third-Party or Cohab Software Installation on page 61.

6 Optional: Install MOTOPATCH for Windows. See MOTOPATCH Installation on page 61.

7 Install the MCC 7100 IP Dispatch Console software. See Installing the MCC 7100 IP Dispatch Console Software on page 52.

8 If you use SNMPv3, configure it. See "Configuring Console Site Elements for SNMPv3" procedure in the *SNMPv3* manual.

9 Apply Windows Supplemental Configuration. See Applying the Windows Supplemental Configuration on page 61.

10 Add the MCC 7100 IP Dispatch console to the domain for the console site. See Setting Up the Domain for an MCC 7100 IP Dispatch Console Inside the ASTRO Radio Network Infrastructure on page 66.

11 Configure Provisioning Manager, or Configuration Manager for ASTRO® 25 Conventional System (K core), for Consoles. See "Console Configuration in Provisioning Manager" in the *MCC 7500 Dispatch Console with VPM* manual.

> 📝 **NOTICE:** Perform this step after Zone and Console Site objects have been configured.

12 Setup the peripherals. See Peripheral Configuration on page 63.

13 Setup the network. See Setting Up the Network on page 65.

14 Discover the MCC 7100 IP Dispatch Console in the Unified Event Manager. See "Discovering Single Device" in the *Unified Event Manager* manual.

15 Optional: Load secure keys and Algorithms. See Load Secure Keys and Algorithms on page 55.

16 Start Elite Admin. See "Starting Elite Admin" in the *MCC 7500/7100 Elite Admin User's Guide* manual.

17 Create a desired `*.elt` file. See "Creating a New Configuration" in the *MCC 7500/7100 Elite Admin User's Guide* manual.

18 Start Dispatch. See "Starting Elite Dispatch" in the *MCC 7500/7100 Elite Dispatch User's Guide* manual.

19 Verify Call Functionality. See "Communicating with Radios" in the *MCC 7500/7100 Elite Dispatch User's Guide* manual.

Installing the MCC 7100 IP Dispatch Console Outside the ASTRO RNI

Follow this procedure for a new installation of the MCC IP Dispatch Console outside the ASTRO® 25 Radio Network Infrastructure (RNI).

Process:

1 Optional: Install MCC 7500 Aux I/O Server. See "Aux I/O Server Installation" in the *MCC 7500 Dispatch Console with VPM* manual.

2 Configure Windows OS:

    a Install the operating system. See Windows Installation and Motorola Operating System Installer for MCC 7100 IP Dispatch Console on page 45.

    b Configure Windows Components. See Configuring Windows Components on page 46.

    c Install .NET Framework 3.5. See Installing the .NET Framework 3.5 Outside the ASTRO RNI on page 44

3 Generate License Certificates for the MCC 7100 IP Dispatch Console. See Generating License Certificates for the MCC 7100 IP Dispatch Console on page 50.

4 Optional: Install third-party or cohab software. See Third-Party or Cohab Software Installation on page 61.

5 Install the MCC 7100 IP Dispatch Console software. See Installing the MCC 7100 IP Dispatch Console Software on page 52.

6 Apply Windows Supplemental Configuration. See Applying the Windows Supplemental Configuration on page 61.

7 Configure Provisioning Manager for Consoles. See "Console Configuration in Provisioning Manager" in the *MCC 7500 Dispatch Console with VPM* manual.

> **NOTICE:** Perform this step after Zone and Console Site objects have been configured.

8 Setup the peripherals. See Peripheral Configuration on page 63.

9 Setup the network. See Setting Up the Network on page 65.

10 Optional: Load secure keys and Algorithms. See Load Secure Keys and Algorithms on page 55.

11 Start Elite Admin. See "Starting Elite Admin" in the *MCC 7500/7100 Elite Admin User's Guide* manual.

12 Create a desired `*.elt` file. See "Creating a New Configuration" in the *MCC 7500/7100 Elite Admin User's Guide* manual.

13 Start Dispatch. See "Starting Elite Dispatch" in the *MCC 7500/7100 Elite Dispatch User's Guide* manual.

14 Verify Call Functionality. See "Communicating with Radios" in the *MCC 7500/7100 Elite Dispatch User's Guide* manual.

Installing the .NET Framework 3.5 Outside the ASTRO RNI

Perform this procedure only if you use Windows 8 operating system. Windows 8 operating system comes with the .NET Framework, version 4.5. The MCC 7100 IP Dispatch Console software requires the .NET Framework, version 3.5.

Prerequisites: Locate the installation media form which you installed Windows 8 operating system. The installation media can be a DVD-ROM or an ISO Image.

Procedure:

1 Open the command prompt window as an administrator.

For more information, see the *Windows Help and Support* online help.

2 To install the .NET Framework 3.5 from the `\sources\sxs` folder on the installation media, run the following command: `DISM /Online /Enable-Feature /FeatureName:NetFx3 / All /LimitAccess /`

`Source: `**`<.Net Framework 3.5 files location>`**
where **`<.Net Framework 3.5 files location>`** is the full path to the .NET files necessary to restore the feature, for example, `d:\sources\sxs`

Upgrading an Existing MCC 7100 IP Dispatch Console

Follow this procedure for a new installation of the MCC IP Dispatch Console in the ASTRO® 25 Radio Network Infrastructure (RNI).

Process:

1 Optional: Generate License Certificates for the MCC 7100 IP Dispatch Console. See Generating License Certificates for the MCC 7100 IP Dispatch Console on page 50.

2 Optional: Install third-party or cohab software. See Third-Party or Cohab Software Installation on page 61.

3 Optional: Install MOTOPATCH for Windows. See MOTOPATCH Installation on page 61.

4 Install the MCC 7100 IP Dispatch Console software. See Installing the MCC 7100 IP Dispatch Console Software on page 52.

5 If you use SNMPv3, configure it. See "Configuring Console Site Elements and Transcoders for SNMPv3" procedure in the *SNMPv3* manual.

6 Apply Windows Supplemental Configuration. See Applying the Windows Supplemental Configuration on page 61.

7 Optional: Load secure keys and Algorithms. See Load Secure Keys and Algorithms on page 55.

8 Start Elite Admin. See "Starting Elite Admin" in the *MCC 7500/7100 Elite Admin User's Guide* manual.

9 Create a desired `*.elt` file. See "Creating a New Configuration" in the *MCC 7500/7100 Elite Admin User's Guide* manual.

10 Start Dispatch. See "Starting Elite Dispatch" in the *MCC 7500/7100 Elite Dispatch User's Guide* manual.

11 Verify Call Functionality. See "Communicating with Radios" in the *MCC 7500/7100 Elite Dispatch User's Guide* manual.

Windows Installation and Motorola Operating System Installer for MCC 7100 IP Dispatch Console

To install the MCC 7100 IP Dispatch Console software, obtain a computer with Windows 7 operating system with an approved service pack.

Computers Provided by Motorola

Workstations purchased from Motorola are imaged with the correct Windows 7 operating system and approved service pack. All required drivers are configured and installed.

To install a fresh Windows Operating System (OS) with an approved service pack on a workstation or on a laptop, use the DVDs provided by Motorola:

- Motorola Operating System Installer (MOSI) 64-bit installation media

- Windows 7 Professional 64-bit OEM media

The MOSI media supports both local and over-the-network Windows OS installation and configuration that minimizes the amount of wait time that you normally experience when you perform the installation.

The MOSI media is updated periodically to provide continual support for installations on computers supported by MOSI. To install the Windows OS, use the MOSI media that came with your system or, if necessary, use an updated version of this installation media. Information on using MOSI is available on the Motorola Online (MOL) web portal. See the MOSI media label or readme.txt for information regarding the access to MOL.

Laptops Provided by your Organization

To install the Windows OS with an approved service pack on your own laptop, use the Windows 7 Professional 64-bit OEM media.

When you name a laptop during the installation of the Windows 7 operating system, adhere to the following restrictions:

- Minimum length: 2 characters
- Maximum length: 49 characters
- Allowed numbers: [0–9]
- Allowed English letters: [a-z A-Z]
- Allowed special characters: period or decimal point (.) and hyphen or minus sign (–)
- No leading and trailing spaces

If you use your laptop for the installation, you are responsible for installing all required drivers.

Configuring Windows Components

The general configuration of Windows 7 components is applicable for all MCC 7100 IP Dispatch Console installations, inside or outside the ASTRO® 25 Radio Network Infrastructure (RNI).

Prerequisites:
Before you install the MCC 7100 IP Dispatch Console software, configure the general Windows 7 Professional operating system components.

Install the required Windows 7 operating system with an approved service pack . See Windows Installation and Motorola Operating System Installer for MCC 7100 IP Dispatch Console on page 45 or contact the Motorola Solution Support Center (SSC).

Process:

1 Set display properties. See Setting Display Properties on page 46.

2 Set power save properties. See Setting Windows Power Options on page 47.

3 Set up SNMP services. See Setting Up SNMP Services Inside the ASTRO RNI on page 48.

4 Configure SNMP Components for a console inside the ASTRO® 25 RNI. See Configuring Windows SNMP Components for a Console Inside the ASTRO RNI on page 48.

5 Configure primary DNS suffix. See Configuring Primary DNS Suffix on page 49.

Setting Display Properties

The settings for screen resolution and color is dependent on the video adapter install on the computer. See the Windows 7 documentation or the computer manufacturer documentation for assistance with changing display settings.

Procedure:

1 In the **Control Panel** of the Windows operating system, navigate to the **Screen Resolution** pane.

2 In the **Resolution** drop-down menu, set the resolution to **1024x768** or greater.

   The available options depend on the installed video adapter.

3 Click **Advanced settings**.

4 In the **Monitor** tab, from the **Colors** drop-down list, select **True Color (32 bit)**.

5 Click **OK** on all subsequent windows.

Setting Windows Power Options

Set the power options for the Windows operating system correctly to ensure uninterrupted operation. See the Windows documentation or the computer manufacturer documentation for information regarding the steps for setting power options. The steps in this procedure may not reflect recent updates to the operating system. For installations on HP laptop/workstation, disable the "HP Power Assistant Service". See the relevant HP documentation for details.

Procedure:

1 In the **Control Panel** of the Windows operating system, navigate to the **Power Options** pane.

2 For the **Balanced (recommended)** plan, click **Change plan settings**.

3 Click **Change advanced power settings**.

   The **Power Options** window appears.

4 Expand **Hard disk** → **Turn off hard disk after** and perform one of the following actions:

   • If you use a laptop, from the **On battery** and **Plugged in** lists, select **Never**.

   • If you use a desktop computer, from the **Setting** list, select **Never**.

5 Expand **Sleep** → **Sleep after** and perform one of the following actions:

   • If you use a laptop, from the **On battery** and **Plugged in** lists, select **Never**.

   • If you use a desktop computer, from the **Setting** list, select **Never**.

6 Expand **Sleep** → **Allow hybrid sleep** and perform one of the following actions:

   • If you use a laptop, from the **On battery** and **Plugged in** lists, select **Off**.

   • If you use a desktop computer, from the **Setting** list, select **Off**.

7 Expand **Sleep** → **Hibernate after** and perform one of the following actions:

   • If you use a laptop, from the **On battery** and **Plugged in** lists, select **Never**.

   • If you use a desktop computer, from the **Setting** list, select **Never**.

8 Expand **Sleep** → **Allow wake timer** and perform one of the following actions:

   • If you use a laptop, from the **On battery** and **Plugged in** lists, select **Disable**.

   • If you use a desktop computer, from the **Setting** list, select **Disable**.

9 Expand **USB settings** → **USB selective suspend setting** and perform one of the following actions:

   • If you use a laptop, from the **On battery** and **Plugged in** lists, select **Disabled**.

   • If you use a desktop computer, from the **Setting** list, select **Disabled**.

10 Expand **Display** → **Turn off display after** and perform one of the following actions:

   • If you use a laptop, from the **On battery** and **Plugged in** lists, select **Never**.

   • If you use a desktop computer, from the **Setting** list, select **Never**.

11 Click **OK**.

12 Close the **Control Panel** window.

Setting Up SNMP Services Inside the ASTRO RNI

The services for Windows Simple Network Management Protocol (SNMP) are initially configured in Windows.

Procedure:

1   In the **Control Panel** of the Windows operating system, navigate to the **Programs and Features** pane.

2   From the left-hand menu, select **Turn Windows features on or off**.

3   In the **Windows Features** window, expand the **Simple Network Management Protocol (SNMP)** node.

4   Select the **WMI SNMP Provider** check box.

5   Click **OK**.

Configuring Windows SNMP Components for a Console Inside the ASTRO RNI

The configuration of Simple Network Management Protocol (SNMP) allows the computer to receive SNMP trap messages. These messages are then forwarded to SNMP management programs running on the computer.

> **NOTICE:** The following procedure is required for all consoles (regardless of which SNMP version is in use). Secure SNMP version 3 (SNMPv3) configuration should be performed later when applicable. See "Configuring Console Site Elements for SNMPv3" in the *SNMPv3* manual.

> **NOTICE:** The SNMP services are not available for a console deployed outside the ASTRO® 25 Radio Network Infrastructure (RNI).

Procedure:

1   In the **Control Panel** of the Windows operating system, navigate to the **Administrative Tools** pane.

2   Double-click **Services**.

> **NOTICE:** If a **User Account Control** dialog box displays, click **Continue**.

3   In the **Services** window, double-click **SNMP Trap**.

4   In the **General** tab of **SNMP Trap Properties** window, from the **Startup type** drop-down list, select **Disabled**. Click **OK**.

5   In the **Services** window, double-click **SNMP Service**.

6   In the **Security** tab of the **SNMP Service Properties** window, select the **Send authentication trap** check box.

7   In the **Accepted community names** section, click **Add**.

8   In the **SNMP Service Configuration** window, add a community:

   a   From the **Community rights** drop-down list, select **READ WRITE**.

   b   In the **Community Name** field, enter `M`.

   c   Click **Add**.

9   In the **SNMP Service Configuration** window, add another community:

   a   From the **Community rights** drop-down list, select **READ ONLY**.

    b In the **Community Name** field, enter `D`.

    c Click **Add**.

10 In the **SNMP Service Configuration** window, add another community:

    a From the **Community rights** drop-down list, select **READ ONLY**.

    b In the **Community Name** field, enter `public`.

    c Click **Add**.

11 Select **Accept SNMP packets from these hosts**.

12 If **localhost** in not listed in the list of accepted hosts, perform the following actions:

    a Under the list, click **Add**.

    b In the **Host name, IP or IPX address** field, enter `localhost`. Click **Add**.

13 In the **Security** tab, click **Apply**.

14 In the **Traps** tab, in the **Community name** drop-down list, enter `M`. Click **Add to list**.

15 Under the **Trap destinations** list, click **Add**.

16 In the **Host name, IP or IPX address** field of the **SNMP Service Configuration – Traps** window, enter `127.0.0.1` and click **Add**.

17 In the **Traps** tab, click **Apply**.

18 Click **OK**.

Configuring Primary DNS Suffix

Configure the primary Domain Name Service (DNS) suffix for an MCC 7100 IP Dispatch Console inside the ASTRO® 25 Radio Network Infrastructure (RNI).

> **NOTICE:** Do not follow this procedure for MCC 7100 IP Dispatch Consoles outside the ASTRO® 25 RNI. If you have an MCC 7100 IP Dispatch Console outside the ASTRO® 25 RNI that is on the Customer Enterprise Network (CEN) domain, verify that it meets one of the following conditions:
>
> • They are installed in an ASTRO® 25 System Release 7.11.
>
> • They are installed in an ASTRO® 25 System Release 7.13 or later, and the suffix was input as part of the hostname in the Provisioning Manager.
>
> If it meets one of the following conditions, enter the DNS suffix for the ASTRO® 25 domain in the Console Status application of this console. See ASTRO Domain Configuration on page 121.

Procedure:

1 In the **Run** window of the Windows operating system, enter `sysdm.cpl`. Press ENTER.

2 In the **Computer Name** tab, click **Change**.

3 In the **Computer Name/ Domain Changes** window, click **More**.

4 In the **DNS Suffix and NetBIOS Computer Name** window, perform the following actions:

    a In the **Primary DNS suffix for this computer** field, enter the DNS suffix in the form of `nmd<S>.zone<Z>`

    where `<S>` is the console site ID and `<Z>` is the zone ID.

> **IMPORTANT:** This DNS suffix naming convention is valid only for consoles inside the ASTRO® 25 RNI.

     b   Clear the **Change primary DNS suffix domain membership changes** check box.

     c   Click **OK**.

5   Close the **Control Panel** windows.

6   When prompt to restart the computer, click **Restart Later**.

Installing the .NET Framework 3.5 on the Windows 8 Operating System Outside the ASTRO RNI

Perform this additional procedure only if you use the Windows 8 operating system. The Windows 8 operating system comes with the .NET Framework, version 4.5. The MCC 7100 IP Dispatch Console software requires the .NET Framework, version 3.5.

Prerequisites: Locate the installation media form which you installed the Windows 8 operating system. The installation media can be a DVD-ROM or an ISO Image.

Procedure:

1   Open the command prompt window as an administrator.

    For more information, see the *Windows Help and Support* online help.

2   Install the .NET Framework 3.5 from the `\sources\sxs` folder on the installation media by running the following command:
```
DISM /Online /Enable-Feature /FeatureName:NetFx3 /All /LimitAccess /
Source:<.Net Framework 3.5 files location>
```

    where `<.NET Framework 3.5 files location>` is the full path to the .NET files necessary to restore the feature, for example, `d:\sources\sxs`

Generating License Certificates for the MCC 7100 IP Dispatch Console

Perform this procedure to obtain a capacity license for the MCC 7100 IP Dispatch Console software and any other licenses for additional licensed features used with the consoles from the FlexNet Operations Portal.

Process:

1   Place the software order that includes the number of the MCC 7100 IP Dispatch Console licenses and the number of licenses for additional features to be used with the consoles.

2   Wait for an order fulfillment E-mail sent by Motorola.

    The E-mail contains an Entitlement ID and instructions on how to acquire license files. If you do not have the Entitlement ID, you cannot access the server and obtain the license certification.

3   Log on to `http://licensing.motorolasolutions.com`.

> **NOTICE:** If you do not have a user account, use the Entitlement ID to create it. After you create the account, you receive an automated E-mail that contains a default password. The E-mail is sent to the registered E-mail address.

4   After you log on, manage, select, and activate all relevant entitlements.

    The FlexNet Operations Portal guides you through the fulfillment process.

5   Configure the server host by either selecting an existing host or adding a host.

    When asked to configure a server host, enter the Ethernet MAC address for the target computer without dashes. The list of MAC addresses along with their associated network adapters can be

                                                        Send Feedback

found by running a Windows command prompt and entering `ipconfig /all` from the target computer.

> **IMPORTANT:** The MAC address selected in this step must be the address associated with a permanent network adapter on the server. The licensing services could be adversely affected by choosing a network adapter that is frequently enabled or disabled.

6 Enter the fulfillment count.

> **NOTICE:** The fulfillment count is the number of licensed audio streams for the MCC 7100 IP Dispatch Console. The number of allowable audio streams is associated with the license and available in 5, 10, 15, or 20 streams.

7 After you review the license information, generate the license files and complete the process.

8 Manage the licenses and either save the license files to the computer or send them in an E-mail.

You use the license files when prompted during the installation of the MCC 7100 IP Dispatch Console software.

Network Interface Card Configuration

Modify the configuration of the Network Interface Card (NIC) on the computer to support the console proxy.

> **NOTICE:** The IP address of the console computer affects SNMPv3 functionality. Modifying the IP address of the console computer for any reason after its initial setting may require SNMPv3 user credentials on the computer be reset. See the *SNMPv3* manual for details.

Configuring the Network Interface Card for an MCC 7100 IP Dispatch Console Inside the ASTRO RNI

Configure the Network Interface Card (NIC) on the computer or server running the MCC 7100 IP Dispatch Console software inside the ASTRO® 25 Radio Network Infrastructure (RNI).

The NIC enables communication of an MCC 7100 IP Dispatch Console inside the ASTRO® 25 RNI. The configuration of the NIC is required only for new installations and as part of the disaster recovery process.

> **NOTICE:** This procedure is intended as a guide and may not reflect recent updates to the Windows 7 operating system. See the relevant Microsoft operating system documentation or the computer manufacturer documentation for specific help on how to configure the NIC.

Prerequisites: Acquire the following Domain Name Service (DNS) network settings:

- List of DNS server IP addresses
- List of DNS suffixes
- An Ethernet network cable

> **NOTICE:** See the system configuration documentation (provided by Motorola) for the correct network settings and relevant lists of DNS server IP addresses and DNS suffixes, otherwise contact Motorola Solution Support Center (SSC) for assistance.

> **NOTICE:** In Windows 7, the *Local Area Connection* icon in Managed Network Connections may indicate that the network connection is partially available (yellow triangle with an exclamation mark) even though there is network connectivity to the ASTRO® 25 RNI. This icon may indicate partial availability when there is no connection from the ASTRO® 25 RNI to the external internet, which is a typical system configuration.

Procedure:

1 Log on to the Windows 7operating system as an administrator.

2   Connect the Ethernet network cable between the dispatch console computer and the ASTRO®
25 RNI network.

3   In the **Control Panel**, navigate to the **Network and Sharing Center** pane.

4   From the left-hand menu, select **Change adapter settings**.

5   If the **Local Area Connection** is disabled, right-click it. Select **Enable**.

6   Right-click **Local Area Connection**. Select **Properties**.

7   In the **Local Area Connection Properties** window, under the **Connect using** field, click
Configure.

8   In the **Network Connection Properties** window, select the **Advanced** tab.

9   From the **Property** list, select **Link Speed & Duplex**.

10 From the **Value** drop-down list, select **100 Mbps Full Duplex**. Click **OK**.

11 Right-click **Local Area Connection**. Select **Properties**.

12 Double-click **Internet Protocol (TCP/IPv4)** and perform the following actions:

> ⊘ **IMPORTANT:** Do not use (TCP/IPv6) to configure Internet protocols.

   a   In the **General** tab, select the **Use the Following IP address** option.

   b   In the **IP address**, **Subnet mask** and **Default gateway** fields, enter values provided for this
   network interface card.

   c   Select the **Use the following DNS server addresses:** option.

   d   Click **Advanced**.

   e   In the **Advanced TCP/IP Settings** window, select the **DNS** tab.

   f   Under the **DNS server addresses in order of use** list, click **Add**.

   g   In the **TCP/IP DNS Server** window, enter the DNS server address. Click **Add**.

   h   Repeat step 12 f and step 12 g for each DNS server in the order of use.

   i   Select the **Append these DNS suffixes (in order):** option.

   j   Under the list of DNS suffixes, click **Add**.

   k   In the **TCP/IP Domain Suffix** window, enter the domain suffix. Click **Add**.

   l   Verify that **Register this connection's addresses in DNS** check box is checked.

   m   In the **WINS** tab, verify that the **Enable LMHOSTS lookup** check box is **not** checked.

   n   On all subsequent windows, click **OK**.

   o   When prompted to reboot, click **No**.

13 Connect a network interface cable to the NIC.

Installing the MCC 7100 IP Dispatch Console Software

Perform this procedure to manually install a new instance of the MCC 7100 IP Dispatch Console
software or upgrade from the previous version of the software.

Prerequisites:
Ensure that you meet the following requirements:

• The Windows computer or workstation on which you want to install the software is running Windows
7 Professional with an approved service pack.

- You have valid license files for the console. If you must create or update the license files, see Generating License Certificates for the MCC 7100 IP Dispatch Console on page 50.

During the installation, the CRYPTR micro install package installs an SD host controller driver. Learn more about the process and ensure that you meet all the requirements. See CRYPTR micro Installation Considerations on page 54.

Procedure:

1 Log on to the Windows operating system as an administrator.

2 If you upgrade from a previous version of the MCC 7100 IP Dispatch Console software, close the Elite Admin and Elite Dispatch applications and stop all third-party software.

3 Insert the MCC 7100 installation media into the CD/DVD drive.

4 Double-click the `Setup.exe` file.

5 In the **User Account Control** window, click **Yes**.

   Numerous command windows can open and close as prerequisite programs are installed.

6 From the welcome page of the Motorola MCC 7100 setup wizard, click **Next**.

7 In the next page, perform one of the following actions:

   - If you upgrade from a previous version without changes and additions to the licensed applications, click **Update**.

   - If you perform a fresh installation or upgrade and new or modified license files are available, browse to the folder that contains the license files that you obtained. Click **Next** or **Update**. The option available depends on whether you upgrade or install the software.

   - If you perform a fresh installation or upgrade but new or modified license files are not available:

     1 Click **Next** or **Update**.
       The option available depends on whether you upgrade or install the software.

       The installation or upgrade continues. However, because of the missing license files, the Elite applications or other licensed applications such as Instant Recall Recorder (IRR) may not start or operate as expected until you import the necessary license files.

     2 Plan to import the license files as a post-requisite to this procedure.

8 Select the intended location to install the console software by performing one of the following actions:

   - If you want to use the console software inside the Motorola Solutions Radio Network Infrastructure (RNI), click **MCC 7100 IRNI**.

   - If you want to use the console software outside the RNI:

     1 Click **MCC 7100 ORNI**.

     2 Perform one of the following actions:

        - If you install the software on a K core system or the console is already configured with a primary Domain Name Service (DNS) suffix that matches the `nmd<S>.zone<Z>` format, click **Install**.

        - If you install the software on an M core or L core system and the DNS suffix is not configured, enter the required compatible ASTRO[®] 25 Radio Network Infrastructure (RNI) domain for the configured console.

> 📝 **NOTICE:** The ASTRO® 25 RNI domain must be appropriate for the platform configured in Network Manager and take the form of `nmd<S>.zone<Z>`, where `<S>` is the configured console site ID and `<Z>` is the configured zone ID.

9 Confirm that you agree to install the software and reboot the computer by clicking **Yes** in the confirmation window.

During the installation, the computer may restart up to two times.

Postrequisites: If you did not have the new or modified license files at the moment of the installation, import them before you use the licensed applications. See Updating License Files for MCC 7100 IP Dispatch Console on page 72.

CRYPTR micro Installation Considerations

During the installation of the MCC 7100 IP Dispatch Console software, observe the CRYPTR micro installation considerations.

> 📝 **NOTICE:** Windows 8 64-bit operating system that you can install on dispatch consoles outside ASTRO® 25 Radio Network Infrastructure (RNI), does not support hardware-based encryption which is the CRYPTR micro device.

> ⚠️ **WARNING:** As a result of the Microsoft security advisory issued in March 2015, the Windows 7 SHA-2 Security Patch (Security Update for Windows KB3033929) is required as part of the MCC 7100 IP Dispatch Console software if hardware-based encryption is required. Failure to do so will result in driver signing error and the MCC7100 IP Dispatch Console will not recognize the CRYPTR micro. Verify the SHA-2 Windows Security Update is installed successfully before installing the MCC 7100 IP Dispatch Console software. If the MCC 7100 IP Dispatch Console software was installed before the SHA-2 Security Patch, the Windows Security Update can still be installed followed by a reboot of the laptop.

Install the CRYPTR micro correctly:

- Place the CRYPTR micro in the SD slot before or after the installation of the MCC 7100 software. If you insert the CRYPTR micro in the SD slot after the MCC 7100 software installation completes, the CRYPTR micro driver installation completes at the time of insertion.

- A dialog box prompting to allow or cancel an installation from an unknown publisher appears during the installation. Select **Allow**.

- During the CRYPTR micro driver installation, messages appear to notify the user about the configuration and the resetting of the CRYPTR micro. No user interaction is required in response to these messages.

- On rare occasions, the CRYPTR micro driver installation cannot proceed without rebooting the computer immediately. If you reboot the computer, the MCC 7100 software installation fails and rolls back. Reboot the computer and restart the installation of the MCC 7100 software.

Verify CRYPTR micro was programmed successfully:

- Use the CRYPTRManagement application to verify the CRYPTR micro version numbers are present in the About CRYPTRManagement window.

- On rare occasions, the following error message will be displayed when using CRYPTRManagement application after installing the MCC 7100 software: "Previous Crypto Module Programming Failed. Crypto Module has only boot block installed. Please Press Upgrade to load the image." If this error message is observed, the CRYPTR micro can be programmed separately using the CRYPTRManagement application. To program the CRYPTR micro, follow the instructions in Upgrading the CRYPTR micro Software Upgrade on page 70. During the procedure, the same message will appear again. Click OK and continue on with the instructions.

Resolve any issues you encounter:

- During the CRYPTR micro driver installation, the Microsoft Standard Compliant SD Host Controller is possible to overwrite the EOM SD Host Controller Driver of the computer. As the result, the CRYPTR micro may stop working after a Windows operating system update. If the problem occurs, reinstall the CRYPTR micro driver by using the instructions in Resolving SD Host Controller Driver Considerations (CRYPTR Micro Failures) on page 79.

- If the CRYPTR micro software upgrade fails during installation, the following message appears: `CRYPTRmicro software upgrade failed. Use the CRYPTRManagement application at a later time to upgrade the device.`. Use the CRYPTRManagement application at a later time to ensure that the CRYPTR micro image is upgraded to the current version. For more information, see Upgrading the CRYPTR micro Software Upgrade on page 70.

Associated Windows Components Software Installation

This section describes the installation of associated Windows components software.

Load Secure Keys and Algorithms

> **NOTICE:** This section is applicable only for secure-capable MCC 7100 IP Dispatch Console software installations.

To encrypt outgoing audio from an MCC 7100 IP Dispatch Console and decrypt incoming audio from other consoles and subscriber radios, the MCC 7100 IP Dispatch Console must have its talkgroups associated with encryption keys.

The association of talkgroups, patches, and Multiselect (MSEL) with a secure key is configured in the ASTRO® 25 system Network Manager. Each key is assigned a Common Key Reference (CKR) that helps identify the key. The Network Manager associates a talkgroup or a special call type with a CKR. This information is downloaded from the Network Manager to the MCC 7100 IP Dispatch Console.

The key material for performing actual encryption and decryption is stored locally on the MCC 7100 IP Dispatch Console, either in the CRYPTR micro device or in the software key file. This key material is also associated with a CKR, so that the appropriate key can be selected for a given talkgroup or a special call type.

> **NOTICE:** Windows 8 64-bit operating system that you can install on dispatch consoles outside ASTRO® 25 Radio Network Infrastructure (RNI), does not support hardware-based encryption which is the CRYPTR micro device.

A CKR, keyset, Key ID, Algorithm ID, and key material are stored for each key. The crypto-administrator for your organization defines these values. These values are defined as common for all devices on an ASTRO® 25 system that must communicate securely to one another. The crypto-administrator initiates updates to the keys as needed using Over the Ethernet Keying (OTEK), key loading the CRYPTR micro using a KVL, or distributing software key files.

> **NOTICE:** CKR and keyset pairs must be unique. Duplicate CKR to keyset pairs is not allowed by the tools and device, since the combination of CKR and keyset uniquely identifies how audio is encrypted on a talkgroup.

On MCC 7100 IP Dispatch Console, the secure keys are stored in one or more software key files on the console or on the CRYPTR micro card. The two configurations are mutually exclusive. During startup, MCC 7100 IP Dispatch Console first checks for the presence of the CRYPTR micro hardware storage device. If absent, the MCC 7100 IP Dispatch Console checks for the presence of one or more software key files. If neither one is present, the MCC 7100 IP Dispatch Console cannot support secure communication. In this case, the Console Dispatch Status application reports that it is configured for hardware encryption mode, but the CRYPTR micro device is not present. To check the secure status of an MCC 7100 IP Dispatch Console, see Console Dispatch Status (MCC 7100 IP Dispatch Console) on page 119 for details.

Hardware Key Storage (CRYPTR micro)-Based Encryption

In this mode of operation, the encryption keys are stored on a SDIO-based secure device CRYPTR micro. The CRYPTR micro is inserted into the SD slot of an MCC 7100 IP Dispatch Console, and can be left there throughout laptop reboots and MCC 7100 IP Dispatch Console software installations.

> **NOTICE:**
> Windows 8 64-bit operating system that you can install on dispatch consoles outside the ASTRO® 25 Radio Network Infrastructure (RNI) does not support hardware-based encryption which is the CRYPTR micro device.
>
> On certain laptops, the CRYPTR micro must be removed after a reboot and then reinserted. This behavior is dependent on specific peripheral hardware installed in the laptop. See Detection of CRYPTR micro Device Troubleshooting on page 80 for details.

The device has a form factor of a microSD card and uses a microSD to SD adapter to fit into the SD slot of a computer.

Figure 2: microSD to SD Adapter

CRYPTR micro

SD Adapter
microSD to SD

SD_Adapter_Micro_A
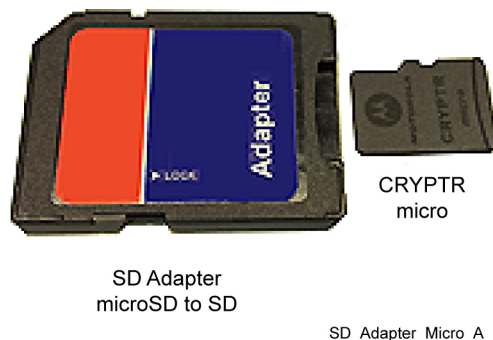
Encryption keys stored on the CRYPTR micro have the following information:

- Common Key Reference (CKR)
- Keyset
- Key ID
- Algorithm ID
- Key Material

Keyset information is also stored on the CRYPTR micro. The MCC 7100 IP Dispatch Console reads this information from the CRYPTR micro when the dispatch application starts up. It then associates each key with a talkgroup or a call type (MSEL, Patch) by matching the CKRs. If a match is found for a talkgroup or a call type, the MCC 7100 IP Dispatch Console is able to make secure calls on that talkgroup and able to decrypt incoming audio. If a match is not found, the Dispatch Console reports key failure during an attempt to use that talkgroup in secure mode.

> **NOTICE:** Before ejecting the CRYPTR micro, close all applications that use the CRYPTR micro. Eject it using the Windows Safely Remove Hardware feature in the desktop tray. The name for the CRYPTR micro device is `generic SDIO device`.

A CRYPTR micro does not have any keys following an initial installation or an upgrade. The two methods of loading keys onto the CRYPTR micro are:

1. For keyloading using a Key Variable Loader (KVL 4000), eject the CRYPTR micro from the MCC 7100 IP Dispatch Console and insert it into the KVL 4000 using a keyloading cable for CRYPTR micro.

2. Use the KVL 4000 user interface to program the needed keys into the CRYPTR micro. Then, reinsert the CRYPTR micro into the MCC 7100 IP Dispatch Console and restart the MCC 7100 IP Dispatch Console Dispatch.

IMPORTANT:
CRYPTR micro is a device introduced in late 2012. The programming and hardware key management of the CRYPTR micro can only be performed using the KVL 4000 Version B. KVL 4000 Version B (T7537B) is required and consists of two components which are PDA MC55A0 and the Security Adapter NTN2564B. To determine the correct KVL 4000 version, ensure that it meets the following requirements:

- Personal Digital Assistant (PDA): The label must read: MC55A0. The information is on the back of the PDA. To read the information, remove the battery.

- Security Adapter: The label must read: T7537B. The information is on the back of the Security Adapter.

Previous versions of the KVL 4000, Version A (T5737A), are not compatible with this feature and no upgrade options are available. Owners of the KVL 4000 Version A must purchase KVL4000 Version B (T5737B - PDA MC55A0 and the Security Adapter NTN2564B) to support this feature. See the KVL product documentation for the most recent information.

In addition, TKN1039A cable is required to interface the KVL 4000 to the CRYPTR micro.

NOTICE: See the *KVL 4000 ASTRO 25 User Guide* to perform key loading.

Figure 3: KVL 4000 Model T7537B with CRYPTR micro Keyloading Cable

Encryption keys on the CRYPTR micro can be automatically updated when centrally managed by a Key Management Facility (KMF). A KMF can be present in the ASTRO® 25 network and configured to manage a particular CRYPTR micro.

> 📝 **NOTICE:** A KMF may be inside or outside the ASTRO® 25 RNI. If outside the ASTRO® 25 RNI, see Configuring the Local Hosts File for Consoles in Conventional K Core Systems or Outside the ASTRO RNI on page 67 for details.

A CRYPTR micro must also be pre-configured to accept updates from a particular KMF. A crypto-administrator configures the CRYPTR micro, using a KVL: Individual RSI is the ID of the CRYPTR micro itself, KMF Radio Set Identifier (RSI) is the ID of the KMF that manages keys on the CRYPTR micro. See the *Key Management Facility* manual.

A crypto-administrator can perform initial key provisioning using the Store and Forward procedure on the CRYPTR micro as follows:

1 Connect a KVL 4000 to the KMF and download encryption keys for a CRYPTR micro to the KVL 4000.

2 Insert a CRYPTR micro into the KVL 4000 with the CRYPTR micro keyloading cable.

3 Initiate a Store and Forward procedure from the KVL 4000. See the *KVL 4000 ASTRO 25 User Guide*.

4 Reconnect the KVL 4000 back to the KMF and upload responses from the CRYPTR micro back to the KMF.

After this provisioning is configured and the CRYPTR micro is inserted in the MCC 7100 IP Dispatch Console, the CRYPTR micro can accept Over the Ethernet Keying (OTEK). OTEK can take place when the MCC 7100 IP Dispatch Console is operational, no Elite restart necessary.

For security reasons, the MCC 7100 IP Dispatch Console software logs in to the CRYPTR micro every time the dispatch application is started. During normal operation, the login process takes place without user intervention.

Manual password reset is required when the CRYPTR micro is newly programmed and its password is defaulted. The default password for the User account is `CryptrAdmin12345`. The default password for the Admin account is also `CryptrAdmin12345`.

To change the passwords, use the **CRYPTRManagement** application. After you use **CRYPTRManagement** to update the password on the CRYPTR micro, it also securely writes in the new password, so that from that point on, automatic log ons in to the CRYPTR micro can take place.

For status of the CRYPTR micro, see the **Encryption/Licensing** tab of the **Console Dispatch Status** application. Specifically, mismatched and default passwords errors are reported in the **Console Dispatch Status** application. For more information, see Console Dispatch Status (MCC 7100 IP Dispatch Console) on page 119.

Software Keyfiles-Based Encryption

In this mode of operation, the encryption keys are stored in one or more files on the MCC 7100 IP Dispatch Console. The key files format is XML. The Key Management Facility (KMF) can generate key files and transfer them manually to the MCC 7100 IP Dispatch Console. Or, you can generate them by the Keyfile Generation tool right on the MCC 7100 IP Dispatch Console or another computer, and manually transfer them to the MCC 7100 IP Dispatch Console.

Encryption keys stored on software keyfiles have the following information:

• Common Key Reference (CKR)

• Keyset

• Key ID

• Algorithm ID

• Key Material

> 📝 **NOTICE:** The Key Management Facility does not support ADP keys.

Keyset information is also stored on software keyfiles. The MCC 7100 IP Dispatch Console reads this information from the software keyfiles when the dispatch application starts up. It then associates each key with a talkgroup or a call type (Multiselect (MSEL), Patch) by matching the CKRs. If a match is successfully found for a talkgroup or a call type, the MCC 7100 IP Dispatch Console can make secure calls on that talkgroup and able to decrypt incoming audio. If a match is not found, the Dispatch Console reports key failure during an attempt to use that talkgroup in secure mode.

NOTICE: If Secure/Crypto keys must be loaded after an installation or upgrade of an MCC 7100 IP Dispatch Console software, they can be reloaded at any time after the MCC 7100 IP Dispatch Console software is installed. A restart of the dispatch application is required to use any updated loaded keys.

Key Store in the Console Dispatch Status application launches the key storage directory in Windows Explorer, where the key files are placed. Up to 10 files are read in, from the newest to the oldest. If the key files format and contents do not pass strict validation rules, errors are reported in the Event Viewer. Since key files are not created manually, but with the use of the KMF or the Keyfile Generation application, both key entry tools enforce most of the validation rules. Additional errors that can happen but cannot be enforced by the key entry tools include:

- Exceeding total supported number of keys across all key files (500)

- Exceeding total supported number of ADP keys across all key files (8)

- Inability to decrypt contents of encrypted keys (no Key Encryption Key (KEK)/invalid KEK in the MCC 7100 IP Dispatch Console)

- Conflicting entries across multiple key files: entries with the same CKR and keyset values. The key from the newer keyfile is kept and the duplicate entry from an older keyfile is ignored.

- Conflicting entries across multiple key files: conflicting keyset names and which one is active. In this case, data from the newer keyfile is kept and a conflicting entry from an older keyfile is ignored.

- No keyfiles exist and thus no keys following an initial installation or an upgrade.

A KMF can manage the MCC 7100 IP Dispatch Console in software encryption mode by generating keyfiles, which are then copied to the MCC 7100 IP Dispatch Console. Over-the-Ethernet-Keying (OTEK) is not supported when using software-based key storage. To generate a keyfile on the KMF, the crypto-administrator creates a group of keys on the KMF and exports it to an XML key file. For details on this procedure, see *Key Management Facility* manual. In this case, each key entry in the file is encrypted with a Common Key Encryption Key (CKEK). The crypto-administrator distributes the CKEK to the MCC 7100 IP Dispatch Console, for the MCC 7100 IP Dispatch Console to be able to decrypt the keys. The MCC 7100 IP Dispatch Console can store up to 20 CKEKs.

The following is an example of the command to execute on the MCC 7100 IP Dispatch Console in order to store a CKEK:

1 Log on as an administrator.

2 Open a command prompt and execute the following command:
```
pwvadmin changeproperty -app APP_GROUP_CRYPTO -property keyfile_KEK1 -
value
"Algid=AES256,KeyID=0xF5A1,Key=0x010101010101010101010101010101010101010101
010101010101010101010101"
```

The format of this command includes password property name "keyfile_KEK1", "keyfile_KEK2", …, "keyfile_KEK20". The command also includes the name of the algorithm, keyed, and the key material. Adhere to the order of parameters and spacing between them for the key to be properly stored.

Backing up and restoring the KEKs in the MCC 7100 IP Dispatch Console is essential for restoring secure communications after an upgrade. However, if you only use clear key files or the CRYPTRmicro, you need not store KEKs in the MCC 7100 IP Dispatch Console.

If a KMF does not manage secure communications in the MCC 7100 IP Dispatch Console, encryption keys are entered manually in a spreadsheet and then exported as an XML file. The MCC 7100 IP

Dispatch Console comes with a macros-enabled spreadsheet `KeyfileGen.xlsm`. The spreadsheet is in `C:\Program Files (x86)\Motorola MCC 7100\bin\KeyfileGen.xlsm`.

Create Software Keyfiles using Microsoft Excel

KeyfileGen.xlsm can be opened using Microsoft Excel or OpenOffice. Macros must be enabled. If KeyfileGen.xml may be used on a computer other than the MCC 7100 IP Dispatch Console where it was installed, it may be copied to another computer. In this case, the schema file `ikmf-app-file.xsd` must be copied with it and placed in the same folder.

The spreadsheet has a sheet for entering up to 500 keys and a sheet for entering two keysets. Enter the Common Key Reference (Common Key Reference (CKR), Keyset ID, KeyID, Algorithm, and key data in clear (unencrypted). The spreadsheet enforces ranges of data as follows:

* CRK from 1 to 4095

* Keysets 1 and 2

* Key ID from 0000 to FFFF (hex values, leading 0s required)

* Encryption Algorithms limited to AES256, DES, ADP

* Key Material length as appropriate for the algorithm

* Odd parity per byte for DES keys

* Total number of keys (500)

> **NOTICE:** Keys generated by the KeyfileGen tool are not encrypted. Use the "Keysets" sheet to enter keyset names and select which keyset is active.

> **IMPORTANT:** All the features of Microsoft Excel to copy data across keys and keysets are supported. However, do not delete rows as the number of keys is restricted to 500 and the number of keysets is exactly two. You can also save the spreadsheet for later use.

If a row on the "Keys" sheet has a blank CKR field, this row is ignored and is not exported to the XML file.

If ADP keys are used, set their keyset to "1". ADP keys have no concept of keysets. You may keep default values in the "Keyset" sheet, unless there are DES and/or AES256 keys, which truly use keysets.

Export the key file by pressing the **Validate and Save** button on top of the "Keys" sheet. If the button cannot be pressed, you may need to enable macros in Excel.

> **NOTICE:** If any of the keys or keysets cannot be validated, the key file is not generated and an error message is displayed. You can correct the problem and attempt to export the key file again.

Some of the errors detected during validation are:

* Invalid parity for DES keys

* Length of key material not matching what the algorithm requires

* Duplicate CKR/Keyset pairs

* Maximum number of ADP keys exceeded

> **NOTICE:** From the Console Dispatch Status application, click **KeyStore** under the **Encryption/Licensing** tab to open the keystorage directory where the keyfiles are stored.

XML files containing keys can also be imported into `KeyfileGen.xlsm`. To import, open `KeyfileGen.xlsm`, right-click on a cell and select **XML → Import**, then browse to the file. Changes can be made and export the updated file using **Validate and Save**.

Third-Party or Cohab Software Installation

After you install the MCC 7100 IP Dispatch Console software and load secure keys and algorithms, you can install the certified third-party or cohab software, for example, McAfee antivirus, Motorola Syslog, and Motorola MOSCAD FSA application.

Because each system is different, the certified applications for the specific system may be unique and not all software is compatible. See the system planner for the specific applications and configuration of the third-party and cohab software for the system.

Some third-party or cohab software may require a network connection to complete or configure its application. Then, revisit these actions after you establish the network connection, for example, when you recover or set up a new MCC 7100 IP Dispatch Console.

In all cases, see the appropriate third-party installation manuals.

> **NOTICE:**
> For an outside the ASTRO® 25 Radio Network Infrastructure (RNI) MCC 7100 IP Dispatch Console installation, at the same time as the MCC 7100 IP Dispatch Console application, consider the following issues when installing other software, and when running other software.
>
> - High CPU usage
> - High network utilization
> - High disk usage
> - High priority anti-virus scans
> - System restore
> - Audio processing
> - Multimedia applications
>
> Running these types of programs at the same time as the MCC 7100 IP Dispatch Console may disrupt the audio performance of the MCC 7100 IP Dispatch Console application, so minimize it or, if possible, avoid it.

MOTOPATCH Installation

Before inserting and opening the *MOTOPATCH for Windows* DVD, install the correct Windows 7 Professional operating system service pack. See the instruction in the README.txt file included in the *MOTOPATCH for Windows* DVD.

Applying the Windows Supplemental Configuration

Use the ASTRO® 25 Windows Supplemental CD to install specific Windows supplemental files by using a Windows Install Framework script.

Apply the Windows supplemental configuration for only consoles inside the ASTRO® Radio Network Infrastructure (RNI) in a K core system, or consoles outside the ASTRO® 25 RNI. Install or reinstall the Windows supplemental files in the following circumstances:

- When you install or upgrade the MCC 7100 IP Dispatch Console software
- When the Windows Supplemental CD changes
- When you reinstall the operating system.

NOTICE:
By performing the following procedure, you disable the Windows operating system restore feature. System restore has the potential to disrupt the audio of an active call when a system restore point is initiated.

For best performance of the MCC 7100 IP Dispatch Console application, leave system restore disabled. However, if the system restore is required, schedule it while the MCC 7100 IP Dispatch Console application is shut down or during off hours so that it causes the least amount of disruption to dispatch operations.

Prerequisites: Ensure that you installed any cohab applications.

Procedure:

1 Depending on the location of the console, perform one of the following actions:

- For a console inside the ASTRO® 25 RNI in a K core system, perform the "Applying Device-Specific Settings Using the Windows Supplemental CD" procedure from the *Windows Supplemental Configuration* manual.
During this procedure, in the **Device Specific Settings** pane of the **Windows Supplemental CD** window, select one of the following devices:

  - For dispatch IP consoles, select **Windows7 MCC7100 IP Consoles**

  - For patch IP consoles, select **Windows7 MCC7100 Patch IP Consoles**

- For a console outside the ASTRO® 25 RNI that has no domain access, perform the "Applying Device-Specific Settings Using the Windows Supplemental CD" procedure from the *Windows Supplemental Configuration* manual.
During this procedure, in the **Device Specific Settings** pane of the **Windows Supplemental CD** window, select **Windows7 MCC7100 Console Operator Position Outside the RNI**.

- For a console outside the ASTRO® 25 RNI that is joined to a Customer Enterprise Network (CEN) domain, perform the following actions:

  1 Import the **MCC7100 IP Consoles Outside RNI** Group Policy Object (GPO). See Importing Group Policy Objects into a Customer Enterprise Network Domain on page 62.

  2 Link the **MCC7100 IP Consoles Outside RNI** GPO to the appropriate Organizational Unit (OU) on the CEN domain controller.
For detailed instructions, see the appropriate documentation and contact the CEN network administrator.

2 Optional: From Windows Supplemental CD, install the optional Event Logging Client (Syslog) component: `logging.xml`.

Importing Group Policy Objects into a Customer Enterprise Network Domain

To import MCC 7100 IP Dispatch Console Group Policy Objects (GPOs) into a Customer Enterprise Network (CEN) domain running on the Windows Server 2008 R2 operating system, use the PowerShell framework.

Prerequisites: Obtain the ASTRO® 25 Windows Supplemental CD.

Procedure:

1 Insert the Windows Supplemental CD to the domain controller.

2 From the **Start** menu, select **All Programs → Accessories → Windows PowerShell → Windows PowerShell**.

3 In the **PowerShell** command line, navigate to the `Supplemental_Utils` directory on the Windows Supplemental CD.

4 Run the following command: `.\ImportGroupPolicy.ps1` "***<GPO name>***"

where ***<GPO name>*** is the name of the GPO that you want to import from the Windows Supplemental CD to the domain controller.

If you enter an incorrect GPO name, the command line provides you with the list of the correct GPOs and you can renter the command.

> **NOTICE:**
> In case of incorrect Powershell policy that prevents the script from running, an error appears saying that the `.\ImportGroupPolicy.ps1` file cannot be loaded because the execution of scripts is disabled on this system. To resolve the issue, set the execution policy by running the following command:
>
> `Set-ExecutionPolicy RemoteSigned`

Step example: In this example, the administrator entered an incorrect GPO name, they were provided with the list of the correct GPOs, and reran the command successfully.

```
PS E:\Supplemental_Utils> .\ImportGroupPolicy.ps1 "MCC7100 IP Consoles Outside RNd"
The name of GPO is incorrect. The list of available GPOs you can import from current GPO

- MCC 7100 FIPS Disable Outside RNI Console
- MCC7100 IP Consoles Outside RNI

Please run script again with valid GPO name!

PS E:\Supplemental_Utils> .\ImportGroupPolicy.ps1 "MCC7100 IP Consoles Outside RNI"
Copying MCC7100 IP Consoles Outside RNI GPO... Please wait patiently...

DisplayName       : MCC7100 IP Consoles Outside RNI
DomainName        : ucs.astro
Owner             : UCS\Domain Admins
Id                : 8cc542c9-1d2e-433c-9393-bb89efbdbe58
GpoStatus         : AllSettingsEnabled
Description       : WHK Version:R04.01.00
                    Version:A7.9_v1

                    Revision History:
                    Date ModifiedComment
                    12/02/2010      Added Comments to the GPO
CreationTime : 12/4/2013 10:30:05 AM
ModificationTime : 3/19/2014 9:50:41 AM
UserVersion       : AD Version: 7, SysVol Version: 7
ComputerVersion   : AD Version: 7, SysVol Version: 7
WmiFilter         :

Information:3/19/2014 9:50:42 AM:ImportGroupPolicy.ps1:Exit with 0.
```

Peripheral Configuration

During the installation, the MCC 7100 IP Dispatch Console, software automatically configures the input (internal microphone) and output (external speakers) of the console computer as the source for voice and audio. These settings are saved as the default profile in the Peripheral Configuration Tool.

To modify the following settings, perform the procedures provided in this section in the Control Panel of the Windows operating system:

• If you want to modify the default profile in the Peripheral Configuration Tool.

> **NOTICE:** You can modify the Peripheral Configuration Tool default profile only from the Windows operating system-level. If you modify the profile in the Peripheral Configuration Tool, you can only save it as a new profile. You cannot save changes to the default profile.

• If you want to disable a specific peripheral connected to the computer. In this way, you prevent it from appearing in the Peripheral Configuration Tool and being available to Windows operating system as a selectable default audio device.

- If you want to enable a specific peripheral connected to the computer. In this way, you get it available in the Peripheral Configuration Tool and to Windows operating system as a selectable default audio device.

- If you want to disable feedback for headset devices. Feedback in a headset device appears when audio spoken into the headset microphone is played back into the headset speaker.

To create configurations in the Peripheral Configuration Tool or perform more advanced configuration, see the *Peripheral Configuration Tool* instructions.

Modifying the Default Audio Peripherals

You can modify the audio peripherals settings initially configured during the installation of the MCC 7100 IP Dispatch Console software only within the Windows operating system. This modification changes the default profile created by the Peripheral Configuration Tool. You cannot delete the profile or modify it within the Peripheral Configuration Tool.

Procedure:

1 In the **Control Panel** of the Windows operating system, navigate to the **Sound** window.

2 In the **Playback** tab, from the list of connected audio devices, select the device that you want to be the default device. Click **Set Default**.

> **NOTICE:** If the Peripheral Configuration Tool is in the default mode, the default speakers automatically switch to the new devices.

3 In the **Recording** tab, from the list of connected audio devices, select the device that you want to be the default device. Click **Set Default**.

4 Close all subsequent windows.

Disabling/Enabling Audio Devices in Windows

A dispatcher can permanently disable audio services configured in the Windows operating system. Depending on the MCC 7100 IP Dispatch Console installation, it may be necessary to disable unused devices such as a line-in audio jack. This process prevents the device from being listed and mapped in the Peripheral Configuration Tool or available to the Windows operating system as a selectable default audio device.

> **NOTICE:** If the Elite application is started when you perform this procedure and the device that you disable is mapped to a peripheral, the audio is lost.

Procedure:

1 In the **Control Panel** of the Windows operating system, navigate to the **Sound** window.

2 To disable or enable a speaker, select the **Playback** tab and perform the following actions:

   a Select the device from the list of connected audio devices.

   b Right-click the device and select **Disable** or **Enable**.

3 To disable or enable a microphone, select the **Recording** tab and perform the following actions:

   a Select the device from the list of connected audio devices.

   b Right-click the device and select **Disable** or **Enable**.

4 Close all subsequent windows.

Disabling Feedback Audio for Headset Devices

In the Windows operating system, a connected USB headset by default plays audio spoken into the headset microphone back into the headset speaker. Turn off this option if the Peripheral Configuration Tool includes headset peripherals.

The headset device may be labeled as **Speakers**. See the description of the device for details.

Procedure:

1 In the **Control Panel** of the Windows operating system, navigate to the **Sound** window.

2 In the **Playback** tab, select the connected audio headset device.

3 Click **Properties**.

4 In the **Levels** tab, click the speaker icon.

5 Click all subsequent windows.

Setting Up the Network

Perform this process to set up network for the dispatch console.

Process:

To setup network for the dispatch console that you installed, perform the following actions:

- For a console inside the ASTRO® 25 Radio Network Infrastructure (RNI) in an M core or L core system:

  1 Set up the domain for the console. See Setting Up the Domain for an MCC 7100 IP Dispatch Console Inside the ASTRO Radio Network Infrastructure on page 66.

  2 Optional: Configure credentials for Secure SNMPv3 Common Agent. See Credentials for Secure SNMPv3 Common Agent (Optional) on page 69.

- For a console inside the ASTRO® 25 RNI in a Conventional K core system:

  1 Configure the local `hosts` file for the console. See Configuring the Local Hosts File for Consoles in Conventional K Core Systems or Outside the ASTRO RNI on page 67.

  2 Configure the External Network Time Protocol (NTP) Time Source for the console. See Configuring the External NTP Time Source on Consoles in ASTRO 25 Conventional K Core System on page 69.

  3 Optional: Configure credentials for Secure SNMPv3 Common Agent. See Credentials for Secure SNMPv3 Common Agent (Optional) on page 69.

- For a console outside the ASTRO® 25 RNI:

  1 Set up a proxy server connection. See Setting Up a Proxy Server Connection Outside the ASTRO RNI on page 65.

  2 Configure the local `hosts` file for the console. See Configuring the Local Hosts File for Consoles in Conventional K Core Systems or Outside the ASTRO RNI on page 67.

  3 Add the console to the ASTRO® 25 Domain Name Service (DNS) server. See Adding a Remote Console to the ASTRO DNS Server on page 69.

Setting Up a Proxy Server Connection Outside the ASTRO RNI

Configure remote MCC 7100 IP Dispatch Consoles to connect to the PRX 7000 Console Proxy located inside the ASTRO® 25 Radio Network Infrastructure (RNI). The IP address (or hostname) for the PRX

7000 Console Proxy is referring to the IP address of the server assigned in the Customer Enterprise Network (CEN) and not the ASTRO® 25 RNI configured IP address.

Procedure:

1 From the Windows **Start** menu, select **All Programs** → **Motorola** → **MCC 7100 Dispatch** → **Console Status**.

2 Select the **Proxy Server List** tab.

3 Click **Add** to create a proxy server entry.

4 In the **Host IP** field, enter the `<hostname>` or `<IP address>` for the PRX 7000 server.

> **NOTICE:** When using an IP address, use the NAT'd IP address of the CEN for the PRX 7000 Console Proxy. The proxy server is only included if a proxy is configured by hostname in the Console Dispatch Status application.

5 Enter a text string to uniquely identify each proxy server entry.

Step example: `Site 55 Server`

6 Click **Save**.

Setting Up the Domain for an MCC 7100 IP Dispatch Console Inside the ASTRO Radio Network Infrastructure

After you configure the IP and Domain Name Service (DNS) information of the dispatch console, add the MCC 7100 IP Dispatch Console to the console site Active Directory domain.

> **NOTICE:** This procedure is not applicable for ASTRO® 25 Conventional System (K core).

Prerequisites: Configure the DNS server IP addresses and DNS suffixes. See Configuring the Network Interface Card for an MCC 7100 IP Dispatch Console Inside the ASTRO RNI on page 51.

> **IMPORTANT:** Apply a secure password to the Administrator account at this time. Failure to do so may result in a security breach. Follow standard Microsoft procedures to change the password on this account.

> **NOTICE:** A domain administrator account and password associated with this domain account are required to join the Active Directory domain. For additional domain authentication information, see the *Authentication Services* manual.

Procedure:

1 In the Windows operating system, navigate to `<systemdrive>`**\Program Files (x86)\Motorola \AAA\bin**

2 Double-click **JoinADomain.exe**.

> **NOTICE:** If the Active Domain (AD) cannot be found, manually enter the domain name.

3 If the **User Account Control** window appears, click **Yes**.

4 In the **Join Active Directory Domain** window, enter the `<user name>` and `<password>` for the domain account used to join the Windows-based device to the active directory domain.

The Organization Unit (OU) selection gets updated.

5 From the **Organization Unit (OU)** drop-down list, select the relevant organization unit.

The basic OUs are:

• Windows 7 MCC 7100 IP Consoles

- Windows 7 MCC 7100 IP Consoles with Ext Voice Encryption
- Windows 7 MCC 7100 Patch IP Consoles
- Windows 7 MCC 7100 Patch IP Consoles with Ext Voice Encryption
- Windows 7 MCC 7100 Patch OP Testing

6 Click **Join**.

> **NOTICE:** After your computer has joined the domain, the local administrator account (not the domain account) is renamed to `MotoSec`.

7 When prompted to reboot, click **Yes**

8 Log on to the Windows operating system with a domain account and perform a group policy update:

    a In the **Start** menu search box, enter `cmd`.

    b From the list of results, right-click **cmd** and select **Run as administrator**.

    c When prompted in the **User Account Control** window, select **Yes**.

    d In the command prompt window, enter `gpupdate /force` and wait for the operation to complete.

    e Close the command prompt window.

    f Reboot the computer.

Configuring the Local Hosts File for Consoles in Conventional K Core Systems or Outside the ASTRO RNI

A conventional K core system is a conventional system that contains no core so no Zone Controller (ZC) , Unified Event Manager (UEM), and Domain Controller (DC) are available in this system.

Perform all configurations using the Configuration Manager application. Call processing is handled through conventional site controllers. No Domain Name Service (DNS) exists in the system.

Similarly, for an MCC 7100 IP Dispatch Console located outside the ASTRO® 25 Radio Network Infrastructure (RNI), the DNS configuration in the Customer Enterprise Network (CEN) may or may not contain the proper DNS entries for the key ASTRO® 25 RNI devices.

To make it possible for the installed MCC 7100 IP Dispatch Console software to continue using DNS APIs, edit the local `hosts` file.

Prerequisites:
In the Windows operating system of the computer on which you installed the dispatch console, navigate to `C:\Windows\System32\drivers\etc` and create a backup copy of the `hosts` file.

For the list of host names, see Appendix D in the *K Core Quick Start Guide* manual and a template for a 10-site K-System.

Procedure:

1 In the Windows operating system of the computer on which you installed the dispatch console, navigate to the Notepad editor.

Instead of the Notepad editor, you can use a different editor, for example, Notepad ++.

2 Right-click the editor and select **Run as administrator**.

3 From the editor, navigate to `C:\Windows\System32\drivers\etc\hosts`

4 In the `hosts` file, map the IP addresses to the host name for the listed devices.

Perform this step by following the instructions in the `hosts` file and the tips in this step.

Zone Controller (Site Control Path)

Include the hostname and the actual IP address. Do not use fully qualified host names.

Example for a Dynamic System Resilience (DSR) system (does not apply to K Core systems):

```
10.5.231.255 scp1
10.5.232.255 scp2
10.5.239.255 scp3
10.5.240.255 scp4
```

> **NOTICE:** The Outside the RNI MCC 7100 requires two Site Control Path hostnames to communicate with the DSR Backup Core in case it loses connection to the primary core Site Control Paths.

Example for a non-DSR system:

```
10.5.231.255 scp1
10.5.232.255 scp2
```

Conventional Site Controller

Include the hostname and the actual IP address. Use fully qualified host names.

Example:

```
10.5.55.95 csc01.nmd55.zone5
```

MOSCAD RTU

Include the hostname and the NAT'd IP address. Use fully qualified host names.

Example:

```
172.76.9.243 rtu1.nmd13.zone5
```

KMF Server

Include the hostname and the NAT'd IP address. Use fully qualified host names.

Example:

```
172.76.9.1kmf01.cen1
```

CAM Server (ELAM feature)

Include the hostname and the NAT'd IP address. Do not use fully qualified host names.

Example:

```
172.76.9.140 z1nmd55cam1
```

LDAP Server

Include the hostname and the NAT'd IP address. Do not use fully qualified host names.

Example:

```
172.76.9.101 zds01
```

Proxy Server

Include the hostname and the NAT'd IP address. The hostname must exactly match the hostname configured in the Console Status application.

Example:

```
172.76.9.3 Proxy1
```

> **NOTICE:** Include the IP address and hostname for the proxy server in the CEN. The proxy server is only included if a proxy is configured by hostname with the use of the Console Dispatch Status application. See .

5 Save changes to the `hosts` file.

Configuring the External NTP Time Source on Consoles in ASTRO 25 Conventional K Core System

Use a `net time` command to configure the external time source for an MCC 7100 IP Dispatch Console in K-core systems.

Procedure:

1 In the **Run** window of the Windows operating system, enter `cmd`. Press ENTER.

2 In the **DOS** command window, enter `net time /setsntp:`**`<IPAddress>`**.

> NOTICE: Because no domain controller exists in a K core system, use an IP Address instead of a hostname.

3 Press ENTER.

Credentials for Secure SNMPv3 Common Agent (Optional)

Set up or restore the secure SNMPv3 credentials only for an MCC 7100 IP Dispatch Console inside the ASTRO® 25 Radio Network Infrastructure (RNI). This section provides the rules to follow when you use SNMPv3 credentials.

The IP address of the dispatch console directly affects SNMPv3 functionality. If you modify the IP address after its initial setting, it can require that you reset the SNMPv3 user credentials on the dispatch console computer. For more information, see the "Configuring Console Site Elements for SNMPv3" procedure in the *SNMPv3* manual.

The Unified Event Manager (UEM) is a fault management application designed to handle the critical fault management functions. To configure secure settings for fault management, see the "Configuring the UEM for SNMPv3" section in the *SNMPv3* manual.

> IMPORTANT:
> When you launch the SNMPv3 Common Agent GUI, the account must be a member of the Network Security Administrators group. A local administrator or domain administrator that are not part of the Network Security Administrators group, must launch the GUI from an elevated command prompt.
>
> If you must re-image the dispatch console or re-install the operating system, create a backup copy of the `snmpd.conf` file. When you restore the credentials, copy the backed-up file to `C:\ProgramData\Motorola\Motorola Common Agent\persist\snmpd.conf`.
>
> Modifications to secure SNMPv3 credentials do not take effect until the computer is restarted.

Adding a Remote Console to the ASTRO DNS Server

Add an MCC 7100 IP Dispatch Consoles outside the ASTRO® 25 Radio Network Infrastructure (RNI) to the Domain Name Server (DNS). This action involves adding the hostname and IP address of the remote console to the DNS inside the ASTRO® 25 RNI.

> NOTICE: The IP address on the connecting remote console must be the IP address of the ASTRO® 25 RNI and not the IP address of the Customer Enterprise Network (CEN).

Procedure:

1 In the **Control Panel** of the Windows operating system, navigate to the **Administrative Tools** pane.

2 Double-click **DNS**.

3 In the **DNS Manager** window, on the left pane, expand **`<DNS hostname>`** → **Forward Lookup Zones**.

4 Right-click the location of the Proxy Server, for example `nmd1.zone1` and select **New Host**.

5 In the **Name** field, enter the remote console ASTRO® 25 RNI **hostname**.

6 In the **IP address** field, enter the remote console ASTRO® 25 RNI **IP address**.

> **NOTICE:** For example, `z001s001op01.nmd1.zone1`, and `10.1.1.1`. This address should correspond to the hostname of the remote console combined with the ASTRO® 25 RNI suffix configured during the installation or in the Console Dispatch Status, for example `myOP.CENsuffix.nmd1.zone1`.

7 Select the **Create Associated Pointer (PTR) Record** check box.

8 Click **OK**.

9 Click **Done**.

Hardware Crypto Configuration

Configuring the crypto hardware includes:

- Changing the Default CRYPTR micro Password
- CRYPTR micro Software Upgrade

Changing the Default CRYPTR micro Password

To change the CRYPTR micro officer (administrative) and user passwords, use the CRYPTR micro Management application.

When and where to use: After an installation or upgrade, reset the passwords to the default values and change them before running Elite Dispatch and processing secure calls.

Procedure:

1 Navigate to `C:\Program Files (x86)\Motorola\Motorola CRYPTR micro Support Applications\`.

2 Right-click `CRYPTRManagement` and select **Run As Administrator**.

> **NOTICE:** Running as Administrator is required only when changing the officer/user passwords and is not required to use other functionality provided by the Management application.

3 In the **Application Configuration** screen, from the pull down menu, select **SDIO**. Click **OK**.

4 From the main screen, choose **Login Admin** to change the **Office** password, or **Login User** to change the user password.

5 Where prompted, enter the **default** password. Click **OK**.

6 Where prompted, enter the **default** password again along with the new password.

7 Click **OK**.

Upgrading the CRYPTR micro Software Upgrade

The CRYPTR micro software can be upgraded during MCC 7100 IP Dispatch Console software installation or upgrade.

In this case, the CRYPTR micro upgrade is silent and does not require user intervention. If the CRYPTR micro device is inserted during the MCC 7100 IP Dispatch Console upgrade, it is upgraded automatically. If it is inserted post-upgrade, it is upgraded immediately.

If the CRYPTR micro software must be upgraded on its own, not as part of the MCC 7100 IP Dispatch Console upgrade, use the **CRYPTRManagement** application:

1 Open the **CRYPTRManagement** application.

2 In the **Application Configuration** screen, from the pull down menu, select **SDIO**. Click **OK**.

3 Login as **admin**.

4 Click **CRYPTR Upgrade**. The **CRYPTR Upgrade** window pops up.

5 Browse to C:\Program Files (x86)\Motorola MCC 7100\bin\red_cryptr_upgrade.prod.binC:\Program Files (x86)\Motorola\Motorola CRYPTR micro Support Applications\Driver. Select red_cryptr_upgrade.prod.bin.

6 To initiate programming, click **Start Upgrade**. If ejection of the CRYPTR micro is required, the utility prompts you to do so.

The version of CRYPTR micro software can be verified post-upgrade by using **CRYPTRManagement**application:

1 Insert the CRYPTR micro into the SD slot.

2 Open the **CRYPTR micro Management** application.

3 To see the CRYPTR micro version numbers, view the contents of `About...` box.

Disabling FIPS

To support Digital Encryption Standard – Output FeedBack (DES-OFB) and ADP encryption algorithms, first disable Federal Information Processing Standards (FIPS) in the Windows operating system.

Procedure:

1 Disable FIPS by performing one of the following actions:

If…	Then…
If you disable FIPS in systems where the console is joined to an ASTRO® 25 domain,	perform one of the following actions: • If you configure a dispatch IP console, join it to the **Windows7 MCC7100 IP Consoles with Ext Voice Encryption** Organizational Unit (OU). • If you configure a patch IP console, join it to the **Windows7 MCC7100 Patch IP Consoles with Ext Voice Encryption** OU. See "Joining and Rejoining a Windows-Based Device to an Active Directory Domain with a Script" in the *Windows Supplemental Configuration* manual.
If you disable FIPS in systems where the console is outside the Radio Network Infrastructure (RNI) and is joined to a Customer Enterprise Network (CEN) domain,	a Import the **MCC 7100 FIPS Disable Outside RNI Console** Group Policy Object (GPO). See Importing Group Policy Objects into a Customer Enterprise Network Domain on page 62. b Link the **MCC 7100 FIPS Disable Outside RNI Console** GPO to the appropriate OU for the console on the CEN domain controller. The correct order of linking the GPO is of crucial importance. The **MCC 7100 FIPS Disable Outside RNI Console** GPO must be at the top of the link order. For detailed instructions, see the appropriate documentation and contact the CEN network administrator.
If you disable FIPS in K core systems or on an MCC 7100 IP	perform the "Applying Device-Specific Settings Using the Windows Supplemental CD" procedure from the *Windows Supplemental Configuration* manual.

If…	Then…
Dispatch Console outside RNI where the operating position is not joined to any domain,	During this procedure, in the **Device Specific Settings** pane of the **Windows Supplemental CD** window, select **Windows7 MCC7100 IP Consoles Operator Position Outside the RNI with Ext Voice Encryption**.

2 If you disabled FIPS while the Elite software was running, restart the software.

MCC 7100 IP Dispatch Console Maintenance and Troubleshooting

This section provides information and procedures that help maintain the MCC 7100 IP Dispatch Console and resolve any issues that can occur.

Dispatch Console Computer Firewall Exceptions

When you run a firewall application on the dispatch console computer, the firewall application may prompt you to allow traffic from certain components of the dispatch console.

Depending on the configuration of the firewall application, you can be prompted for any of the following dispatch console processes:

- `AuxioManager.exe`
- `FileAudioDSP.exe`
- `IRR.exe`
- `ProxyClient.exe`
- `RCSync.exe`
- `RCSyncUser.exe`
- `WinQUICC.exe`

If the firewall application prompts you for any of the processes, allow the traffic so that it does not disrupt the dispatch console operation.

Updating License Files for MCC 7100 IP Dispatch Console

Perform this procedure to import and activate the MCC 7100 IP Dispatch Console license files in the following situations.

- You did not have the license files available at the moment of the console installation
- You accidentally removed the license files from the predefined location
- Your license expired and you must replace it with a new one that you generated

Prerequisites: Ensure that you have valid license files. To generate new license files, see Generating License Certificates for the MCC 7100 IP Dispatch Console on page 50.

Procedure:

1 Copy the license files to the following location: `C:\ProgramData\Motorola MCC 7100\Licenses` on the MCC 7100 IP Dispatch Console computer.

2 Reboot the computer.

Upgrading the MCC 7100 IP Dispatch Console Software

Use this process to upgrade an existing installation of the MCC 7100 IP Dispatch Console software.

Prerequisites: A previous version of the MCC 7100 IP Dispatch Console software is installed on a Motorola-certified computer. The MCC 7100 Elite and Admin applications are closed, and all third-party software is closed or stopped.

⚠️ **CAUTION:** For MCC 7100 IP Dispatch Console using a CRYPTR micro for encryption, Secure/ Crypto keys and algorithms may be erased during the upgrade. This erasing is dependent upon the type of change to the secure software from version to version. Reload this information into the secure card if necessary.

Process:

1 Log on to the Windows operating system as an administrator.

2 Install the MCC 7100 IP Dispatch Console software. See Installing the MCC 7100 IP Dispatch Console Software on page 52.

    📝 **NOTICE:** If any issues occur during the upgrade process, manually remove the existing version of the MCC 7100 IP Dispatch Console software. See Removing All MCC 7100 IP Dispatch Console Applications on page 151 for details. Afterwards, repeat the upgrade process.

3 Install software of associated Windows components. See Associated Windows Components Software Installation on page 55.

Failure to Upgrade or Uninstall the MCC 7100 IP Dispatch Console Software

Symptom:

While upgrading or uninstalling the MCC 7100 IP Dispatch Console software, an error message is displayed similar to `Another app has exclusive access to the file C:\...\Debug.mdb`

Solution:

Click **Retry**.

📝 **NOTICE:** If unsuccessful, restart the computer and perform and repeat the upgrade or uninstall procedure.

Elite Console Application Stuck in Application Initializing State

Symptom:

After starting the Elite dispatch console and choosing the Elite configuration file, the **Internal system error occurred** window opens and reads, `See Event Viewer application log for details.` After authenticating with the console user credentials, the Elite dispatch console application fails to assign resources and the **Application Initialization** window opens and reads `The application is initializing, please stand by` …. The Elite dispatch console application never finishes initializing and remains stuck in the application initializing state.

The Windows Application Event log error message states to check this troubleshooting procedure in the installation manual.

The **Application Initialization** windows opens after choosing the Elite configuration file, specifying the console user credentials, and completing database synchronization. It is normal for this window to be displayed briefly in a working scenario. However, in this case, the application never initializes. This error condition may occur after upgrading the MCC 7100 IP Dispatch Console software, applying the Windows Supplemental CD, or restarting Windows.

Solution:

Delete and recreate the Windows user account profile. See Restoring the Windows User Account Profile on page 74 for the required steps.

> **NOTICE:** Elite dispatch console application files are not stored in the user profile folder. However, other program files stored in the user profile folder must be backed up and copied to a different folder, otherwise they are deleted. When the process is completed, the copied data can be moved back to the user profile folder.

Restoring the Windows User Account Profile

Perform this procedure to restore the Windows user account profile as a troubleshooting measure when Elite console application is stuck in the initialization state.

Procedure:

1 Close the Elite application.

2 Log out of Windows.

3 Log on Windows as an administrator (either domain or local admin).

> **NOTICE:** The account must be different than the account used for the Elite dispatch.

4 Delete the profile as follows:

    a From the **Control Panel**, select **System**.

    b Click **Change settings**.

    c In the **System Properties** window, click the **Advanced tab**.

    d Under **User Profiles**, click **Settings**.

      The **User Profiles** window opens.

    e Select the relevant profile and click **Delete**.

    f Click **OK**.

5 Log out of Windows.

6 Log on Windows with the original account.

    The account profile is recreated and is used by the Elite console.

Elite Console Denied Access Due to an Embedded Password Mismatch

> **NOTICE:** Running Elite as a local Admin or domain Admin on a system with Full (not transparent) Information Assurance (IA) also results in this error. Elite must be ran from an elevated Command prompt when using local Admin or domain Admin accounts on fully IA secured system.

Symptom:

The Elite application shows the error, `The console was denied access to data due to an embedded password mismatch or internal error. Contact System Administrator.` and does not launch (has cached NM data) or launches based on cached data but still displays the error message.

Solution:

Uninstall and reinstall the MCC 7100 IP Dispatch Console software, as follows:

                            Send Feedback

1 Manually uninstall the MCC 7100 IP Dispatch Console software. See Removing All MCC 7100 IP Dispatch Console Applications on page 151.

2 Install the MCC 7100 IP Dispatch Console software. See Installing the MCC 7100 IP Dispatch Console Software on page 52.

Elite Console Denied Access Due to an Embedded Password Mismatch after Reinstalling All Software

Symptom:

The Elite application shows the error, `The console was denied access to data due to an embedded password mismatch or internal error. Contact System Administrator.` after the MCC 7100 IP Dispatch Console software is reinstalled.

Solution:

Add a new domain console user to the local **pwvault** group. See Adding a New Domain Console User on page 75.

Adding a New Domain Console User

Procedure:

1 In the **Control Panel** of the Windows operating system, navigate to the **Administrative Tools** pane.

2 Double-click **Computer Management**.

3 In the left-hand navigation tree, expand **Local Users and Groups** → **Groups**.

4 Double-click **Power Users**.

5 In the **Power Users Properties** window, click **Add**.

6 In the **Select Users, Computers, Service Account, or Groups** window, click **Advanced**.

7 Click **Find Now**.

8 Select the domain console user. Click **OK**.

9 Click **OK** on all remaining widows.

10 Reboot the computer.

Elite Crash Error When Logging off the Dispatch Operator Position

When you shut down or restart the operator position workstation, or switch between the Windows operating system accounts on the operator position, an error message appears stating that the Elite application crashed.

The message appears when you shut down or restart the operator position workstation or switch between the Windows operating system accounts on the operator position without existing the Elite Admin or Elite Dispatch application before.

If you encounter this message, ignore it. Next time you turn on the workstation or log on to the operating system, start the Elite application as usual.

To avoid this issue in the future, exit the Elite application any time you log off the operating system.

Audio Troubleshooting on MCC 7100 IP Dispatch Console

The MCC 7100 IP Dispatch Console uses on-board peripherals and interfaces to those devices through the Windows audio layer. If the system is experiencing an absence of audio through the

peripheral devices, the first step is to verify that the devices are present and enabled in the Windows Sound control panel application.

Audio Quality Issues

Symptom:

A connection to the console proxy is being established, but send-and-receive audio quality issues exist (choppy or non-existent voice, dropped calls). The MCC 7100 IP Dispatch Console provides a utility to check the current health of the link to the console proxy.

Solution:

Check the link to the console proxy as follows:

1 From the Windows **Start** menu, select **Start → Motorola → MCC 7100 Dispatch → Console Status**.

2 The active proxy connection is displayed along with a three-bar indicator of the link health. If this indicator is fluctuating or consistently display one or zero bars, contact a system administrator to help diagnose any potential network issues.

Volume Levels Are Too Low

The MCC 7100 IP Dispatch Console contains controls (configurable in Elite Admin) to adjust the speaker volume for the individual speakers mapped through the Peripheral Configuration Tool. Set the speaker volume to an appropriate level for the given speakers. See the *MCC 7500 Elite Dispatch User Guide* for details.

Resolving No Audio Sent or Received from the Peripherals

The Peripheral Configuration Tool and the Windows Sound applet can be used to diagnose any potential peripheral issues. For example, a connection is established between a remote console and the console proxy but no audio is heard at the peripherals.

Process:

1 From the Windows **Start** menu, select **All Programs → Motorola → MCC 7100 Dispatch → Peripheral Configuration Tool**.

2 Examine the **Audio Input** and **Audio Output** tabs.

> **NOTICE:** Verify the name and description of the currently mapped peripherals. The mapped peripherals drop-down list displays the current peripheral type (Speaker 1-8, Headset Microphone, and so on).

3 Verify that mappings are present.

> **NOTICE:** The minimum set of peripherals required for dispatch is at least one desktop speaker and one desktop microphone. Verify that one speaker is mapped in the **Output** tab and one desktop microphone is mapped in the **Input** tab.

> **NOTICE:** If any of the mapped peripherals display an icon that is grayed out, that peripheral is disconnected or disabled. Reconnect the device if necessary, or re-enable the device in the **Windows Sound** panel. See Disabling/Enabling Audio Devices in Windows on page 64 for details. After correcting the problem, the grayed out icon of the device in the **Peripheral Configuration Tool** should change to a solid icon.

> **NOTICE:** If the mapped speaker devices appear enabled, connected, and mapped, the Peripheral Configuration Tool allows the user to send a test tone to a selected output device.

4 Select the relevant audio device.

5 Right-click on the row and select the **Test** option.

A test tone plays through the selected device.

6 If audio is still not heard, verify the audio levels are not muted, as follows:

   a Make sure that system audio is unmuted.

   b If the system audio is unmuted and sound is still not heard, verify and fix the audio levels for each audio device.

   c From the **Control Panel → Sound**, right-click the relevant audio device and select **Properties**.

   d In the **Levels** tab, verify that the slider is set to the appropriate volume.

7 Perform additional troubleshooting steps for audio, if necessary:

   a Verify that no console features are enabled that would prevent audio from being played on the speaker (for example, acoustic cross mute).

   b Verify that Elite Dispatch is correctly configured to route select/unselect audio to that peripheral. The speaker must be mapped in the Peripheral Configuration Tool, connected, and configured in the Elite Dispatch Audio menu.

   c Verify that the MCC 7100 mixer is not muted. All audio devices may appear to be configured correctly but the slider on the MCC 7100 mixer is set to 0.

Secure Audio Troubleshooting on MCC 7100 IP Dispatch Console with CRYPTR micro-Based Encryption

This section describes the procedures required to troubleshoot secure audio on the MCC 7100 IP Dispatch Console with CRYPTR micro-based encryption.

CRYPTR micro Password Issues

Symptom:

Console Dispatch Status application indicates a problem with CRYPTR micro password. Secure Audio does not work.

Solution:

Perform the following actions:

1 If the password in the CRYPTR micro is known, but it does not match, update the password in the MCC 7100 IP Dispatch Console. This solution applies to both User and Admin passwords for the CRYPTR micro.

2 If the password in the CRYPTR micro is the default password, use the **CRYPTRManagement** application to change the password. The password in the MCC 7100 IP Dispatch Console is updated automatically at the same time.

3 If the passwords in the CRYPTR micro are not known, use **CRYPTRManagement** to reset the password. Enter an invalid password 10 times in a row, at which point the contents of the CRYPTR micro is erased and the password is defaulted.

> **NOTICE:** Any keys previously stored in the CRYPTR micro is lost.

Testing an Unresponsive CRYPTR micro Card

Test an unresponsive CRYPTR micro card to determined whether it should be replaced, or if the SD Host Controller driver was not installed correctly in the MCC 7100 IP Dispatch Console.

Symptom:

The CRYPTR micro card in the MCC 7100 IP Dispatch Console has become unresponsive. The CRYPTRManagement application does not display the version numbers for the CRYPTR micro software in the **About CRYPTRManagement** window.

> **NOTICE:** The CRYPTR micro card has no visual or audible user interface that can determine its state. Therefore, an additional working CRYPTR micro card is used as part of the troubleshooting process to determine the state of the unresponsive card.

Solution:

To determine if the card is functioning properly, the CRYPTR micro card is visually inspected and tested using the MCC 7100 IP Dispatch Console and/or the KVL 4000.

> **NOTICE:** If a KVL 4000 is used and cannot detect the unresponsive CRYPTR micro card when attempting to perform any action on the CRYPTR micro, the CRYPTR micro card is damaged and must be replaced. See Recovering a Damaged or Missing CRYPTR micro Card on page 87 for details.

Procedure:

1 Eject the unresponsive CRYPTR micro card from the MCC 7100 IP Dispatch Console.

2 Insert the working CRYPTR micro card into the MCC 7100 IP Dispatch Console.

> **NOTICE:** Use a working CRYPTR micro card to determine if the card is defective or if the MCC 7100 IP Dispatch Console was configured properly.

3 Open an explorer window and browse to `C:\Program Files (x86)\Motorola\Motorola CRYPTR micro Support Applications`

4 Double-click the **CRYPTRManagement** application.

5 In the **Application Configuration** screen, from the pull down menu, select **SDIO**. Click **OK**.

6 Click the **Motorola symbol** in the upper left-hand corner of the **CRYPTRManagement** window and select **About CRYPTRManagement**.

7 From the **About CRYPTRManagement** window, view the version numbers for the CRYPTR micro software.

   • If the window returns meaningful version numbers, the unresponsive CRYPTR micro card is damaged and must be replaced with a new one. See Recovering a Damaged or Missing CRYPTR micro Card on page 87 for details.

   • If the window becomes unresponsive and then displays "None" for version numbers, the MCC 7100 IP Dispatch Console may be improperly configured (for example, does not contain a driver for the CRYPTR micro card). See Resolving SD Host Controller Driver Considerations (CRYPTR Micro Failures) on page 79 to troubleshoot the configuration issue.

Secure Call Failures

This section defines the most common secure call failures and provides a possible solution.

Symptom:

CRYPTR micro is in place but secure audio does not work.

Solution:

Verify that CRYPTR micro is keyloaded with the appropriate keys. Use the CRYPRmicroManagement utility to display the list of keys in the CRYPTR Micro.

Symptom:

CRYPTR micro is in place, some keys are loaded, but secure audio does not work.

Solution:

Verify that CRYPTR micro is keyloaded with the appropriate keys. Use the CRYPRmicroManagement utility to display the list of keys in the CRYPTR Micro.

Symptom:

CRYPTR micro is in place, but Over-the-Ethernet-Keying (OTEK) does not work.

Solution:

Verify that the OTEK settings for the MCC 7100 IP Dispatch Console are correct. While the MCC 7100 IP Dispatch Console software is running, open the Console Dispatch Status application to the **Encryption/Licensing** tab and check the **OTEK Status**. If it reports OTEK Not Configured, enable OTEK in Network Manager. If the Console Dispatch Status application reports OTEK Not Connected, check with your administrator whether the configured Key Management Facility (KMF) is in service. If the Console Dispatch Status application reports OTEK Connected, and OTEK is not functional, safely remove the CRYPTR micro and verify with a KVL 4000 that the individual Radio Set Identifier (RSI) and KMF RSI are programmed as intended.

Symptom:

Software key files are in place, but secure audio does not work.

Solution:

Check Windows Event Log for errors and warnings regarding reading of the software key files during dispatch application startup.

Resolving SD Host Controller Driver Considerations (CRYPTR Micro Failures)

Symptom:

Previously working CRYPTR micro card not recognized by the MCC 7100 IP Dispatch Console software and secure calls are not working. The Console Dispatch Status application shows None even though the CRYPTR micro is inserted into the SD slot.

The MCC 7100 IP Dispatch Console package installs and overwrites the SD Host Controller driver currently installed in Windows.

> **NOTICE:** System updates, service packs, and other installation packages may all subsequently overwrite the driver needed by the console. If this overwrite occurs, re-install the console SD card driver.

Procedure:

1 In the **Control Panel** , select **Device Manager**.

2 Verify that **CRYPTR micro SDIO Device** is found under **Memory Technology Devices**.

> **NOTICE:** If not found, eject the **CRYPTR micro** and re-insert it. Then verify that the **CRYPTR micro SDIO Device** is now found. If not found, check the Windows Event Log for any errors from the CRYPTR micro driver. Report any errors to Motorola Solution Support Center (SSC).

3 If no errors, re-install the CRYPTR micro driver as follows:

a Log on as an administrator and open a command **DOS** window.

b Enter
```
"C:\Program Files (x86)\Motorola\Motorola CRYPTR micro Support
Applications\Driver\CRYPTRmicro_install_app.exe" /i "C:\Program
Files (x86)\Motorola\Motorola CRYPTR micro Support Applications
```

```
\Driver\CRYPTRmicroDriver.inf" somerandomstring "Soft Console" "Soft
Console Product" "Motorola Solutions"
```

   c Reboot the computer.

   d Eject and re-insert the CRYPTR micro.

   e Look for the **CRYPTR micro SDIO Device** in the Device Manager.

Detection of CRYPTR micro Device Troubleshooting

Use Windows Device Manager to check whether the computer detects the CRYPTR micro. The CRYPTR micro is represented by a node called **CRYPTR micro SDIO device** in the **Memory Technology Driver Folder** in Device Manager.

> **NOTICE:** See Windows help to locate and open your Device Manager with administrator privileges.

When the CRYPTR micro is present in the SD slot, the node is present in Device Manager. When the CRYPTR micro is absent from the slot, the node is absent. In some cases, the entire **Memory Technology Driver Folder** in Device Manager is also absent. Device Manager adds and removes the node upon insertion and removal of the CRYPTR micro. Some examples of abnormal behavior are as follows:

- The CRYPTR micro SDIO Device node remains present in the Memory Technology Folder after the CRYPTR micro is ejected.
- The CRYPTR micro SDIO Device node remains absent from the Memory Technology Folder even though the device is in place.

The following are symptoms and solutions for detecting the CRYPTR micro:

Symptom:

The CRYPTR micro is in place but secure audio does not work following a computer reboot. All non-secure functionality of the MCC 7100 IP Dispatch Console is operational. The Console Dispatch Status application reports `Not Present`. The CRYPTRManagement application returns `None` for the version information. For all other operations, it returns `Link Down Error. Crypto module is not present.`

> **NOTICE:** A specific laptop either always exhibits this behavior or always works properly following a reboot. During testing by Motorola, this issue was observed on HP Elitebook 8440p laptops with Ricoh SD Host Controller. A laptop equipped with a Ricoh SD Host Adapter is more likely to exhibit this issue than other laptops. Technicians can use Device Manager to display the properties of the SD Host Adapter/SD Host Controller. In the **Details** tab, display the Hardware IDs property. If some of the properties contain the string `VEN_1180`, the computer has a Ricoh SD Host Controller. Laptops equipped with a JMicron or an O2Micro SD Host controller are not likely to exhibit this issue.

Solution:

Eject and reinsert the CRYPTR micro. Use Device Manager to verify that the CRYPTR micro node was not present before ejection and reinsertion, but is now present. Restart the MCC 7100 IP Dispatch Console application. The Console Dispatch Status and CRYPTRManagement applications should detect the CRYPTR micro.

Symptom:

The CRYPTR micro is in place but secure audio does not work following an ejection and reinsertion of the CRYPTR micro while MCC 7100 applications are running. All non-secure functionality of the MCC 7100 IP Dispatch Console is operational. The Console Dispatch Status application reports `Not Present`. The CRYPTRManagement application returns "`None` for the version information. For all other operations, it returns `Link Down Error. Crypto module is not present.`

Solution:

Use Device Manager to view the CRYPTR micro node. If present, eject the CRYPTR micro. If the CRYPTR micro node is present, reboot the computer, insert the CRYPTR micro, and restart the MCC 7100 IP Dispatch Console application. The Console Dispatch Status and CRYPTRManagement applications should detect the CRYPTR micro.

Symptom:

The CRYPTR micro is in place but secure audio does not work. All non-secure functionality of the MCC 7100 IP Dispatch Console is operational. The Console Dispatch Status application reports `Not Present`. The CRYPTRManagement application returns `None`for the version information. For all other operations, it returns `Link Down Error. Crypto module is not present.`

Solution:

Use Device Manager to view the CRYPTR micro node. If it does not appear despite rebooting the computer or ejecting and reinserting the CRYPTR micro multiple times, reinstall the CRYPTR micro driver as described in Resolving SD Host Controller Driver Considerations (CRYPTR Micro Failures) on page 79. If the CRYPTR micro node is not present when it is ejected and reinserted, use Device Manager to display the properties of the SD Host Adapter/SD Host Controller. In the **Details** tab, display the Hardware IDs property. Contact Motorola Solution Support Center (SSC) for further troubleshooting and provide all hardware IDs.

Troubleshooting Connection Issues (Outside the ASTRO Radio Network Infrastructure)

The state of the connection between the remote MCC 7100 IP Dispatch Console and the PRX 7000 Console Proxy can be checked using the Console Dispatch Status application, as follows:

1 Open the PRX 7000 Console Dispatch Status, see Console Dispatch Status (PRX 7000 Console Proxy) on page 123.

2 After connected, right-click on the IP address of a remote connection in the Remote OP Connection List and select **Link Details**.

> **NOTICE:** If the link state shows zero bars, the connection is not established.

Check the following items if a remote MCC 7100 IP Dispatch Console cannot connect to the PRX 7000 Console Proxy server:

- Verify that a network path exists from the connecting remote MCC 7100 IP Dispatch Console to the control room firewall.

- Verify (if using a Virtual Private Network (VPN) connection) that a network path exists from the VPN server to the control room firewall.

- Verify that a proxy connection is configured on the connecting remote MCC 7100 IP Dispatch Console. This verification can be done from the Status application.

- Verify that the system clocks for the PRX 7000 Console proxy and remote MCC 7100 IP Dispatch Console are time synchronized. Due to security restrictions on the remote link, the clocks must be within 24 hours of each other.

- Check for an affiliated console on the console site.

- Open the Console Dispatch Status application on the PRX 7000 Console Proxy and verify that the connecting remote MCC 7100 IP Dispatch Console is not included on the black list.

- Open the Console Dispatch Status application on the PRX 7000 Console Proxy and check the remote MCC 7100 IP Dispatch Console capacity.

- Verify that the number of connecting remote MCC 7100 IP Dispatch Consoles does not exceed the licensed capacity, and that the licensed capacity is not zero. If the licensed capacity is zero, see Troubleshooting the MCC 7100 IP Dispatch Console License Issues on page 82 for details.

• Check the power mode settings on the PRX 7000 Console Proxy and remote MCC 7100 IP Dispatch Console.

- Verify the power mode setting, as described in Setting Windows Power Options on page 47, and, if necessary, restart the FLEXlm licensing service.

• Using the Console Dispatch Status application on the remote MCC 7100 IP Dispatch Console, verify that the proxy server hostname or IP address is the address configured in the Customer Enterprise Network (CEN).

• Network elements between the MCC 7100 IP Dispatch Console and the PRX 7000 Console Proxy may not support standard Maximum Transmission Unit (MTU) or MTU Path Discovery. See Changing the Maximum Transmission Unit on page 83 for details.

Troubleshooting the MCC 7100 IP Dispatch Console License Issues

If you cannot start the Elite Dispatch or Elite Admin application, perform the following procedure to determine the issue. The typical symptoms of issues with the MCC 7100 IP Dispatch Console licenses are:

• The following error that appears when you log on to the Elite Dispatch or Elite Admin application:
`Operating License could not be found. Please install a valid license before invoking the application`

• The call capacity information in the **Licensing Status** pane in the **Licensing/Encryption** tab of the Console Status application is `0 Calls`.

Procedure:

• Verify that the new or modified license files are available in the following directory: `C:\ProgramData\Motorola MCC 7100\Licenses`. If not, see Updating License Files for MCC 7100 IP Dispatch Console on page 72

• Verify that the MAC address obtained during the license generation phase corresponds to an enabled network device.

  If this network device is disabled, the licensing services do not run.

• Verify that the Windows power settings are correct. See Setting Windows Power Options on page 47

• If you use a temporary license, open the license file in a text editor and verify that the license did not expire by looking for a similar line:

  `+ INCREMENT soft_console_capacity motsol 1.0 07-feb-2012 20 \`

  The expiration date in non-temporary cases is set to `permanent`.

  If the license has expired, perform the following actions:

  a. Generate a new license. See Generating License Certificates for the MCC 7100 IP Dispatch Console on page 50

  b. Import the new license file into the predefined location. See Updating License Files for MCC 7100 IP Dispatch Console on page 72.

• Verify that the FLEXlm License Manager service is up and running:

  - If the service is not running, start the service.

- If the service is running but the `motsol.exe` executable is not running in the Task Manager, restart the service.

Troubleshooting the Instant Recall Recorder License Issues

If you cannot start the Instant Recall Recording (IRR) application, use the following procedure to determine the issue. The typical symptom of the IRR licensing issue is the following error that appears when you want to start the Instant Recall Recorder application: `Operating License could not be found. Please install a valid license before invoking.`

Procedure:

- Verify that the new or modified license files are available in the following directory: `C: \ProgramData\Motorola MCC 7100\Licenses`. If not, see Updating License Files for MCC 7100 IP Dispatch Console on page 72

- Verify that the MAC address obtained during the license generation phase corresponds to an enabled network device.

  If this network device is disabled, the licensing services do not run.

- Verify that the Windows power settings are correct. See Setting Windows Power Options on page 47

- If you use a temporary license, open the license file in a text editor and verify that the license did not expire by looking for a similar line:

  `? INCREMENT software_irr motsol 1.0 07-feb-2012 1 \`

  The expiration date in non-temporary cases is set to `permanent`.

  If the license has expired, perform the following actions:

  a. Generate a new license. See Generating License Certificates for the MCC 7100 IP Dispatch Console on page 50

  b. Import the new license file into the predefined location. See Updating License Files for MCC 7100 IP Dispatch Console on page 72.

- Verify that the FLEXlm License Manager service is up and running:

  - If the service is not running, start the service.

  - If the service is running but the `motsol.exe` executable is not running in the Task Manager, restart the service.

Changing the Maximum Transmission Unit

If intermediate network elements (routers, switches) drop packets greater than 1500 bytes, it may be necessary to change the value of the Maximum Transmission Unit (MTU) on the PRX 7000 Console Proxy or the MCC 7100 IP Dispatch Console to a lower value.

⚠️ **CAUTION:** Modify the MTU only as a last resort, after the all network settings have been check and verified.

Procedure:

1 Select **Start** and enter `regedit` in the search field.

2 In the registry editor, navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet \Services\Tcpip\Parameters\Interfaces\interface-name`.

3 Right-click **MTU** of type **REG_DWORD** and select **Modify**.

4 Enter the desired MTU size in hexadecimal.

> **NOTICE:** The range of the MTU is 0x44 to the dynamically determined MTU (in bytes). Set this value to `0xFFFFFFFF`, to change the MTU back to the default value of the network interface dynamically determined MTU.

5 Click **OK**.

6 Close the **Registry Editor**.

7 Restart the computer.

MCC 7100 IP Dispatch Console Disaster Recovery

This section provides details and references required to recover the MCC 7100 IP Dispatch Console in the event of a failure.

Recovering an MCC 7100 IP Dispatch Console Installation

Disaster recovery is used if the current installation of the MCC 7100 IP Dispatch Console has become unstable or inoperable. Follow this process to reinstall all necessary components.

Recovery of an MCC 7100 IP Dispatch Console installation during a disaster recovery event requires a full installation.

Process:

1 Backup critical files used by the MCC 7100 IP Dispatch Console. See Critical Backup Files for the MCC 7100 IP Dispatch Console on page 85 for a list of files.

2 Install the recommended Windows operating system, if not previously installed and configured.

    a Install the operating system by using the correct installation media. See Windows Installation and Motorola Operating System Installer for MCC 7100 IP Dispatch Console on page 45 for all required installation and configuration procedures.

    b Configure Windows Components. See Configuring Windows Components on page 46.

3 Optional: If performing disaster recovery on replacement hardware, generate new License Certificates for the MCC 7100 IP Dispatch Console. See Generating License Certificates for the MCC 7100 IP Dispatch Console on page 50.

4 Configure Network Interface Card (NIC) on the computer or server inside the ASTRO® 25 Radio Network Infrastructure (RNI). See Configuring the Network Interface Card for an MCC 7100 IP Dispatch Console Inside the ASTRO RNI on page 51.

5 Install the MCC 7100 IP Dispatch Console software. See Installing the MCC 7100 IP Dispatch Console Software on page 52.

6 If using SNMPv3, configure it. See the "Configuring Console Site Elements and Transcoders for SNMPv3" procedure in the *SNMPv3* manual.

7 Load secure keys and algorithms. See Load Secure Keys and Algorithms on page 55.

8 Install third-party or cohab software. See Third-Party or Cohab Software Installation on page 61.

9 Optional: Install MOTOPATCH. See MOTOPATCH Installation on page 61.

10 Perform Windows Supplemental Configuration. See Applying the Windows Supplemental Configuration on page 61.

11 Setup the peripherals. See Peripheral Configuration on page 63.

12 Setup the network. See Setting Up the Network on page 65.

13 Perform the CRYPTO configuration. See Hardware Crypto Configuration on page 70.

14 Restore critical files backed up in step 1.

After completing the full installation, recover all the critical backup files to the previously installed location. If required, create the necessary directory structure when you recover these files. If a file exists, accept any confirmation dialog boxes from the Windows operating system asking to replace the file.

If you use the USB AIM, restore the AIM Local Relays setting by performing .

15 **Only for dispatch consoles inside the ASTRO® 25 Radio Network Infrastructure (RNI):** Rediscover the MCC 7100 IP Dispatch Console in the Unified Event Manager (UEM):

a Delete the MCC 7100 IP Dispatch Console from the UEM. See the "Deleting Devices" procedure in the *Unified Event Manager* manual.

b Discover the MCC 7100 IP Dispatch Console in the UEM. See the "Discovering Devices" procedure in the *Unified Event Manager* manual.

> **NOTICE:**
> If recovering from a backup installation, the previously saved password vault files must be recovered and imported again. To recover and import, log on as an administrator, open a command prompt and execute the following command:
> `C:\Program Files (x86)\Motorola\PWVault\pwvadmin.exe import -app APP_GROUP_CRYPTO -fpath <PATH>`
>
> where `PATH` is the directory and filename where the files were backed up.

Critical Backup Files for the MCC 7100 IP Dispatch Console

Archiving of critical files is essential to the operation of the MCC 7100 IP Dispatch Console. Perform it periodically. Archive the files to an external device, for example, external storage or network storage.

Table 11: MCC 7100 IP Dispatch Console Files to Backup

File Type	Location	Note
License files	`C:\ProgramData\Motorola MCC 7100\Licenses`	Back up the license files to speed up the recovery process.
Proxy Connection List	`C:\ProgramData\Motorola MCC 7100\ProxyClient \clientOptions.txt`	The Proxy Connection List is a single file. **NOTICE:** The Proxy Connection List file is available for dispatch consoles outside the ASTRO® 25 Radio Network Infrastructure (RNI).
Peripheral Configuration files	`C:\ProgramData\Motorola MCC 7100\PeripheralConfig`	Back up all the `.xml` files.
Network hosts file	`C:\Windows\System32\drivers \etc\hosts`	These files are used only for configurations outside the ASTRO® 25 RNI or in K core systems.

Table continued…

File Type	Location	Note
SNMPv3 file	`C:\ProgramData\Motorola\Motorola Common Agent\persist\snmpd.conf`	The SNMPv3 file is a single file.
Elite configuration files	`C:\Users\Public\Public Documents\Motorola MCC 7100\config`	Back up all the `elt` files.
Secure Configuration files	`C:\ProgramData\Motorola\PWVault\Data`	Back up the `CRYPTO.context` file and the `CRYPTO.data` file. To backup the secure configuration data, log on as an administrator, open a command prompt and execute the following command: `C:\Program Files (x86)\Motorola\PWVault\pwvadmin.exe export –app APP_GROUP_CRYPTO –quiet –fpath` *<PATH>* where *<PATH>* is the directory and filename where the backed up data are placed.
Secure Software Key files	If you use software key storage mode, locate and back up your key files.	To open the keystore directory in which the key-files are stored, in the Console Dispatch Status application, select the **Encryption/Licensing** tab, and click **Key Store**. NOTICE: Perform these actions only when you uninstall the dispatch console. Key-files are preserved during an upgrade.
Enhanced Alert Tones	`C:\Users\Public\Public Documents\Motorola MCC 7100\alert tones`	If using Enhanced Alert Tones, back up the folders with the audio files.

Table continued…

File Type	Location	Note
Audio Interface Module Local Relay settings	`C:\Program Files (x86)\Motorola MCC 7100\bin \LocalRelayValues.txt`	If using the USB Audio Interface Module device, back up the Local Relays settings.

Configuring the Audio Interface Module Local Relays

Configure local relays for the USB Audio Interface Module (USB AIM) device locally on the dispatch console. By disabling the local relays, you can silence the operation of the USB AIM.

Procedure:

1 Open a command prompt with administrative privileges.

2 Navigate to the following directory: `C:\Program Files (x86)\Motorola MCC 7100\bin\`

3 Change the settings by using the following script:

    `cscript.exe ConfigureLocalRelays.vbs [/help] [/enableall | /disableall | /reset ] [/enable <PORT_TYPE> | /disable <PORT_TYPE> ]`
    where:

    `<PORT_TYPE>` is `INBOUND`, `PTT`, `EMERGENCY`, or `ALARM`;

    `/enable` enables the port type that follows;

    `/disable` disables the port type that follows;

    `/enableall` enables all relay ports;

    `/disableall` disables all relay ports;

    `/reset` resets the settings to the fresh installation default settings when `INBOUND` is disabled and all other ports are enabled;

    `/help` prints usage for this script.

Recovering a Damaged or Missing CRYPTR micro Card

Troubleshooting procedures have indicated that the CRYPTR micro card must be replaced and reconfigured.

Prerequisites: See Testing an Unresponsive CRYPTR micro Card on page 77 to ensure that the CRYPTR micro card was tested and determined to be defective.

Process:

1 Insert the replacement CRYPTR micro card into the MCC 7100 IP Dispatch Console and launch the CRYPTRManagement application. Using the **About CRYPTRManagement** window, view the version numbers for the CRYPTR micro software, see Testing an Unresponsive CRYPTR micro Card on page 77. Verify that these version numbers are up-to-date.

2 If the version numbers are not up-to-date, upgrade the CRYPTR micro card.

    📝 **NOTICE:** The up-to-date versions of the CRYPTR micro software image are at `C: \Program Files (x86)\Motorola\Motorola CRYPTR micro Support Applications\Driver\red_cryptr_upgrade.prod.bin`

   a Open an explorer window and browse to `C:\Program Files (x86)\Motorola \Motorola CRYPTR micro Support Applications`

   b Double-click the **CRYPTRManagement** application.

   c In the **Application Configuration** screen, from the pull down menu, select **SDIO**. Click **OK**.

   d Login as **admin**.

e Click **CRYPTR Upgrade**. The CRYPTR Upgrade Application window pops up.

f Browse to `C:\Program Files (x86)\Motorola\Motorola CRYPTR micro Support Applications\Driver\red_cryptr_upgrade.prod.bin`

> **NOTICE:** The **CRYPTRManagement** application guides you through the upgrading process for the CRYPTR micro card, including ejecting and reinserting the CRYPTR micro card. See Upgrading the CRYPTR micro Software Upgrade on page 70.

3 Use the CRYPTRManagement application to change Admin and User passwords on the CRYPTR micro card. See Changing the Default CRYPTR micro Password on page 70 for details.

4 Reload key management parameters and encryption keys. If using manual key management, use a Key Variable Loader (KVL) 4000 to program encryption keys into the CRYPTR micro card. If using centralized key management, use a KVL 4000 to load the Individual RSI, Key Management Facility (KMF) Radio Set Identifier (RSI), and MNP, if not using defaults. Then perform a Store-and-Forward procedure. See Load Secure Keys and Algorithms on page 55.

PRX 7000 Console Proxy Setup and Installation

This chapter provides information and activities associated with the setup and installation of the PRX 7000 Console Proxy. This chapter also includes setup verification information and activities, maintenance and troubleshooting, and field replacement unit information, and disaster recovery information to support the PRX 7000 Console Proxy.

PRX 7000 Console Proxy Software and Hardware Requirements

The PRX 7000 Console Proxy requires a Windows-based computer or workstation running a 64-bit version of Windows 7 Professional operating system with an approved service pack. The server must also conform to the minimum supported hardware specifications of an MCC 7500 Dispatch Console when running in a cohab environment. See the *MCC 7500 Dispatch Console with Voice Processor Module* manual for details.

> 🖉 **NOTICE:** The HP Z420 is the recommended workstation to use for the PRX 7000 Console Proxy. See Table 8: Hardware Specifications for HP Z420 Workstation on page 39 for details.

PRX 7000 Console Proxy Cohab with MCC 7500 Installations

The PRX 7000 Console Proxy can be installed as a standalone product or cohabited with an MCC 7500 Dispatch Console (Voice Processor Module (VPM)-based) installation inside the ASTRO® 25 Radio Network Infrastructure (RNI). Either or both can be installed with no impact to performance. See the *MCC 7500 Dispatch Console with Voice Processor Module* manual for MCC 7500 Dispatch Console installation procedures.

> ⚠ **WARNING:** The PRX 7000 Console Proxy installation does not allow the console proxy to be installed cohabited with an MCC 7100 IP Dispatch Console installation (or the other way around).

Setting Up the PRX 7000 Console Proxy

This process provides the order in which the components associated with the PRX 7000 Console Proxy must be installed and/or configured.

Process:

1 Install the recommended Windows 7 operating system, as follows:

   a Run the Motorola OS Installer (MOSI). See Windows Installation and Motorola Operating System Installer for PRX 7000 Console Proxy on page 90.

   b Configure the computer power settings. See Setting Windows Power Options on page 47.

2 Generate License Certificates for the PRX 7000 Console Proxy. See Generating License Certificates for the PRX 7000 Console Proxy on page 91.

3 Install PRX 7000 Console Proxy software. See Installing the PRX 7000 Console Proxy Software on page 92.

4 Configure black list of remote MCC 7100 IP Dispatch Console. See Adding a Remote MCC 7100 IP Dispatch Console to the Black List on page 126.

5 Optional: Install MOTOPATCH. See MOTOPATCH Installation on page 61.

6 Install Supplemental CD. See Windows Supplemental Configuration (K Core) on page 93.

7 Configure Network Interface Card (NIC) on computer or server inside the ASTRO® 25 Radio Network Infrastructure (RNI). See Configuring the Computer Network Interface Card for the PRX 7000 Console Proxy on page 94.

8 Setup the Active Directory Domain for the console site. See Setting Up the Domain for the PRX 7000 Console Proxy on L and M Core on page 95.

Operating System Installation for the PRX 7000 Console Proxy

Before installing the PRX 7000 Console Proxy software, update the current Windows operating system with Windows 7 Professional with an approved service pack.

Windows Installation and Motorola Operating System Installer for PRX 7000 Console Proxy

Workstations purchased from Motorola are imaged with the correct Windows 7 operating system and approved service pack. All required drivers are configured and installed.

To install a fresh Windows Operating System (OS) with an approved service pack on a workstation, use the following DVDs provided by Motorola:

• Motorola Operating System Installer (MOSI) 64-bit installation media

• Windows 7 Professional 64-bit OEM media with the appropriate service pack

The MOSI media supports both local and over-the-network Windows OS installation and configuration that minimizes the wait time that you normally experience when performing the installation.

The MOSI media is updated periodically to provide continual support for installations on computers supported by MOSI. To install the Windows OS, use the MOSI media that came with your system or, if necessary, use an updated version of this installation media. Information on using MOSI is available on the Motorola Online (MOL) web portal. See the MOSI media label or `readme.txt` for information regarding the access to MOL.

Setting Windows Power Options

Set the power options for the Windows operating system correctly to ensure uninterrupted operation. See the Windows documentation or the computer manufacturer documentation for information regarding the steps for setting power options. The steps in this procedure may not reflect recent updates to the operating system. For installations on HP laptop/workstation, disable the "HP Power Assistant Service". See the relevant HP documentation for details.

Procedure:

1 In the **Control Panel** of the Windows operating system, navigate to the **Power Options** pane.

2 For the **Balanced (recommended)** plan, click **Change plan settings**.

3 Click **Change advanced power settings**.

The **Power Options** window appears.

4 Expand **Hard disk → Turn off hard disk after** and perform one of the following actions:

• If you use a laptop, from the **On battery** and **Plugged in** lists, select **Never**.

• If you use a desktop computer, from the **Setting** list, select **Never**.

5 Expand **Sleep → Sleep after** and perform one of the following actions:

- If you use a laptop, from the **On battery** and **Plugged in** lists, select **Never**.
- If you use a desktop computer, from the **Setting** list, select **Never**.

6 Expand **Sleep** → **Allow hybrid sleep** and perform one of the following actions:

- If you use a laptop, from the **On battery** and **Plugged in** lists, select **Off**.
- If you use a desktop computer, from the **Setting** list, select **Off**.

7 Expand **Sleep** → **Hibernate after** and perform one of the following actions:

- If you use a laptop, from the **On battery** and **Plugged in** lists, select **Never**.
- If you use a desktop computer, from the **Setting** list, select **Never**.

8 Expand **Sleep** → **Allow wake timer** and perform one of the following actions:

- If you use a laptop, from the **On battery** and **Plugged in** lists, select **Disable**.
- If you use a desktop computer, from the **Setting** list, select **Disable**.

9 Expand **USB settings** → **USB selective suspend setting** and perform one of the following actions:

- If you use a laptop, from the **On battery** and **Plugged in** lists, select **Disabled**.
- If you use a desktop computer, from the **Setting** list, select **Disabled**.

10 Expand **Display** → **Turn off display after** and perform one of the following actions:

- If you use a laptop, from the **On battery** and **Plugged in** lists, select **Never**.
- If you use a desktop computer, from the **Setting** list, select **Never**.

11 Click **OK**.

12 Close the **Control Panel** window.

Generating License Certificates for the PRX 7000 Console Proxy

Perform this procedure to obtain a license certificate from the FlexNet Operations Portal before installing the PRX 7000 Console Proxy software.

> **NOTICE:** Before obtaining a license certification, an Entitlement ID is required to access the server. Motorola e-mails the entitlement ID to the user. It contains instructions on how to acquire license files.

Process:

1 Places the software order, including the number of licenses required.

2 An order fulfillment e-mail, containing an Entitlement ID and instructions, is sent to the user.

3 Log on `http://licensing.motorolasolutions.com`.

> **NOTICE:** If a user account does not exist, use the Entitlement ID to initially create one. An automated e-mail, containing a default password, is sent to the registered e-mail address.

4 After logging on, the user manages, selects, and activates all relevant entitlements.

> **NOTICE:** The **FlexNet Operations Portal** guides the user through the fulfillment process.

5 Configure the server host by either selecting an existing host or adding a host.

> **NOTICE:** When asked to configure a server host, enter the Ethernet MAC address for the target computer without dashes. You can find the list of MAC addresses with their associated network adapters by running a Windows command prompt and entering `ipconfig /all` from the target computer.

> **IMPORTANT:** Address associate the MAC address selected in this step with a permanent network adapter on the server. The licensing services could be adversely affected by choosing a network adapter that is frequently enabled or disabled.

6 Enter 1 for the fulfillment count.

> **NOTICE:** The license for the PRX 7000 Console Proxy can have a maximum of 10 remote connections.

7 After reviewing the license information, generate the license file and complete the process.

8 Next, manage the license and either save the license file to the computer or e-mail the license.

> **NOTICE:** This license file is used when prompted during the installation of the PRX 7000 Console Proxy software installation.

Installing the PRX 7000 Console Proxy Software

Perform this procedure to install the PRX 7000 Console Proxy software and the following setup programs on a Motorola-approved computer:

OpenSSL
A toolkit implementing the Secure Sockets Layer, Transport Layer Security, and general-purpose cryptography library.

Certificate Generation and Deployment (CGD)
A tool that creates and distributes Motorola default certificates for target windows devices to authenticate with the installed Trusted Root Certificate.

DirectX
Collection of Application Programming Interfaces (APIs).

.NET Framework
Runtime and associated files required to run applications developed to target the .NET Framework.

7-Zip
File archiving utility with a high compression ratio.

Password Vault
Secured password manager for storing passwords.

Prerequisites:
Meet the following requirements:

- The computer or workstation on which you want to install the PRX 7000 Console Proxy is running Windows 7 Professional.

- You have a valid license file for the proxy. If you must create or update the license file, see Generating License Certificates for the PRX 7000 Console Proxy on page 91.

Procedure:

1 Insert the PRX 7000 installation media into the CD/DVD drive.

2 Open the PRX 7000 installation media and double-click `Setup.exe`.

3 From the welcome page of the Motorola PRX 7000 setup wizard, click **Next**.

4 On the next page, perform one of the following actions:

- To upgrade from a previous version without changes and additions to the PRX 7000 license file, click **Install**.

- To perform a fresh installation or upgrade when a new or modified license file is available, browse to the folder that contains the license file that you obtained. Click **Install**.

- To perform a fresh installation or upgrade when a new or modified license file is not available:

    1 Click **Install**.
    The installation or upgrade continues. However, because of the missing license file, the application may not start or operate as expected until you import the necessary license file.

    2 Plan to import the license file as a post-requisite to this procedure.

5 Confirm that you agree to install the software and reboot the computer by clicking **Yes** in the confirmation window.

6 Verify the installation of the PRX 7000 services, as follows:

  a From the Windows **Start** menu, select **All Programs** → **Motorola** → **PRXY 7000** → **Console Status**.

  b Verify the value for the licensed capacity in the **Remote OP Connection List** window.

Postrequisites: If you did not have the new or modified license files at installation, import them before you use PRX 7000 application. See Updating License Files for PRX 7000 Console Proxy on page 96.

Black List Configuration for Remote MCC 7100 IP Dispatch Consoles (Optional)

The black list blocks specific remote MCC 7100 IP Dispatch Consoles from connecting to the PRX 7000 Console Proxy inside the ASTRO® 25 Radio Network Infrastructure (RNI). Any remote dispatch console that is inadvertently added to the black list is prevented from establishing a connection. See Adding a Remote MCC 7100 IP Dispatch Console to the Black List on page 126 for details.

MOTOPATCH Installation

Before inserting and opening the *MOTOPATCH for Windows* DVD, install the correct Windows 7 Professional operating system service pack. See the instruction in the `README.txt` file included in the *MOTOPATCH for Windows* DVD.

Windows Supplemental Configuration (K Core)

Use the ASTRO® 25 Windows Supplemental CD to install specific Windows Supplemental CD files using a Windows Install Framework script.

> **IMPORTANT:** Re-install the Windows supplemental installations when upgrading/installing console proxy software, when the supplemental CD changes, or when reinstalling the operating system.

The following software and operational installations are performed using the Windows Supplemental CD:

- PuTTY

- Group Policy Objects - scripts related to Active Directory and DNS, including script for Windows devices to join the domain.

> **NOTICE:** See the *Windows Supplemental Configuration* manual for installation procedures. The installation of programs such as OpenSSL and CGD are performed as part of the PRX 7000 Console Proxy installation. See Installing the PRX 7000 Console Proxy Software on page 92 for details.

Network Interface Card Configuration

Modify the configuration of the Network Interface Card (NIC) on the computer to support the console proxy.

NOTICE: The IP address of the console computer affects SNMPv3 functionality. Modifying the IP address of the console computer for any reason after its initial setting may require SNMPv3 user credentials on the computer be reset. See the *SNMPv3* manual for details.

Configuring the Computer Network Interface Card for the PRX 7000 Console Proxy

Configure the Network Interface Card (NIC) on the computer or server running the console proxy software inside the ASTRO® 25 Radio Network Infrastructure (RNI).

NOTICE: In Windows OS, the Local Area Connection icon in Managed Network Connections may indicate that the network connection is partially available (yellow triangle with an exclamation mark) even though there is network connectivity to the ASTRO® 25 RNI. This icon may indicate partial availability when there is no connection from the ASTRO® 25 RNI to the external internet, which is a typical system configuration.

The NIC enables communication from the console proxy to an MCC 7100 IP Dispatch Console inside the ASTRO® 25 RNI or to remote MCC 7100 IP Dispatch Console outside the ASTRO® 25 RNI through a control room firewall. Configuration of the NIC is required only for new installations and as part of the disaster recovery process.

NOTICE: This procedure is intended as a guide and may not reflect recent updates to the Windows operating system. See the relevant Microsoft operating system documentation or the computer manufacturer documentation for specific help on how to configure the network interface card.

Prerequisites: Acquire the following DNS network settings:

* List of DNS server IP addresses
* List of DNS suffixes

NOTICE: See the system configuration documentation (provided by Motorola) for the correct network settings and relevant lists of DNS server IP addresses and DNS suffixes, otherwise contact Motorola Solution Support Center (SSC) for assistance.

Procedure:

1 Log on to Windows as an administrator.

2 In the **Control Panel**, navigate to the **Network and Sharing Center** pane.

3 From the left-hand menu, select **Change adapter settings**.

4 If the Local Area Connection is disabled, right-click the **Local Area Connection**. Select **Enable**.

5 Right-click **Local Area Connection** and select **Properties**.

6 In the **Local Area Connection Properties** window, click **Configure** under **Connect using**.

   The **Network Connection Properties** window for the specific card opens.

7 Click the **Advanced** tab.

8 From **Property**, select **Link Speed & Duplex**.

9 From the **Value** drop-down list, select **100Mbps/Full Duplex** and click **OK**.

   NOTICE: For Motorola-purchased computers (HP Z420), select **100 Mb Full**.

10 Right-click **Local Area Connection** and select **Properties**.

11 Double-click **Internet Protocol (TCP/IPv4)** and set the following values:

    a Select **Use the Following IP address:** in the **General** tab.

    b Enter the **IP address**, **Subnet mask**, and **Default gateway** provided for this network interface card.

    c Select **Use the following DNS server addresses:**.

    d To open the **Advanced TCP/IP Settings**, click **Advanced** window.

    e Select the **DNS** tab.

    f Click **Add...**, enter the **DNS server address** in the **TCP/IP DNS Server** window, and click **Add** to save the address.

        NOTICE: Repeat this step for each DNS server in the order of use.

    g Select **Append these DNS suffixes (in order):**.

    h Under the list of DNS suffixes, click **Add...**. In the **TCP/IP Domain Suffix** window, enter the **Domain suffix**, and click **Add** to save the suffix.

    i Check **Register this connection's addresses in DNS**.

    j Select the **WINS** tab and verify that the **Enable LMHOSTS lookup** check box is NOT selected.

    k Click **OK** on all subsequent windows to save all IP settings.

    l Click **No** when prompt to reboot.

Setting Up the Domain for the PRX 7000 Console Proxy on L and M Core

Perform this procedure on the server running the console proxy software inside the ASTRO® 25 Radio network Infrastructure (RNI).

Prerequisites:
Configure the DNS server IP addresses and DNS suffixes. See Configuring the Computer Network Interface Card for the PRX 7000 Console Proxy on page 94.

A domain administrator account and password associated with this domain account are required to join the Active Directory domain. For additional domain authentication information, see the *Authentication Services* manual.

Apply a secure password to the Administrator account at this time. Failure to do so may result in a security breach. Follow standard Microsoft procedures to change the password on this account.

Procedure:

1 In the Windows Operating System (OS), navigate to the PRX 7000 bin directory:

    • On a 32-bit OS: **`<systemdrive>`**`\Program Files (x86)\Motorola\AAA\bin`

    • On a 64-bit OS: **`<systemdrive>`**`\Program Files\Motorola\AAA\bin`

2 Double-click **JoinADomain.exe**.

        NOTICE: If the Active Domain (AD) cannot be found, manually enter the domain name.

3 If the **User Account Control** window appears, click **Yes**.

4 In the **Join Active Directory Domain** window, enter the **_<user name>_** and **_<password>_** for the domain account used to join the Windows-based device to the active directory domain.

The Organization Unit (OU) selection gets updated.

5 From the **Organization Unit (OU)** drop-down list, select the correct organization unit.

6 Click **Join**.

> 📝 **NOTICE:** After the computer has joined the domain, the local administrator account (not the domain account) is renamed to `MotoSec`.

7 Log on to the Windows operating system with a domain account and perform a group policy update:

   a In the **Start** menu search box, enter `cmd`.

   b From the list of results, right-click **cmd** and select **Run as administrator**.

   c When prompted in the **User Account Control** window, select **Yes**.

   d In the command prompt window, enter `gpupdate /force` and wait for the operation to complete.

   e Close the command prompt window.

   f Reboot the computer.

PRX 7000 Console Proxy Maintenance and Troubleshooting

This section provides the procedures required to maintain and troubleshoot the PRX 7000 Console Proxy.

Updating License Files for PRX 7000 Console Proxy

Perform this procedure to import and activate the PRX 7000 Console Proxy license files in the following situations:

- You did not have the license files available at the moment of the console installation
- You accidentally removed the license files from the predefined location
- Your license expired and you must replace it with a new one that you generated

Prerequisites: Ensure that you have valid license files. To generate new license files, see Generating License Certificates for the PRX 7000 Console Proxy on page 91.

Procedure:

1 Copy the license files to the following location: `C:\ProgramData\Motorola Dispatch \Licenses` on the PRX 700 Console Proxy computer.

2 Reboot the computer.

Upgrading the PRX 7000 Console Proxy Software

Perform this process to upgrade an existing installation of the PRX 7000 Console Proxy software.

Process:

1 Log on to the Windows as an administrator.

2 Install the PRX 7000 Console Proxy software. See Installing the PRX 7000 Console Proxy Software on page 92.

> **NOTICE:** If any issues occur during the upgrade process, manually remove the existing version of the PRX 7000 Console Proxy software. See Uninstalling the PRX 7000 Console Proxy Software on page 97 for details. Afterwards, repeat the upgrade process.

Uninstalling the PRX 7000 Console Proxy Software

Perform this procedure to uninstall a previous installation of the PRX 7000 Console Proxy software that was not installed incorrectly.

Prerequisites: The proxy server software must be removed from the computer using the built-in functionality of the operating system, for example, using **Programs and Features** under **Control Panel** and selecting **Motorola Solutions PRX 7000 Server**.

> **NOTICE:** Executing the PRX 7000 Uninstall removes ONLY the PRX 7000 application package. Other third-party packages installed by the master installer such as the Password Vault, 7zip, OpenSSL, .NET runtimes, and CGD are not automatically removed and must be uninstalled manually to remove them from the system.

Procedure:

1. Log on to the Windows as an administrator.

2. In the **Control Panel** of the Windows operating system, navigate to the **Programs and Features** pane.

3. Select **Motorola Solutions PRX 7000 Server**.

4. Click **Uninstall**.

   > **NOTICE:** During the uninstall process, the following error can appear: `ERROR 1306: Another app has exclusive access to the file C:\...\Debug.mdb. Please shutdown all other apps and retry.` If the error appears, wait one minute, then click **Retry**.

5. Reboot the computer.

Remote Console Cannot Connect to the Proxy Server

Use the Console Dispatch Status application to check the state of the connection between the remote MCC 7100 IP Dispatch Console and the PRX 7000 Console Proxy:

1. Open the PRX 7000 Console Dispatch Status, see Console Dispatch Status (PRX 7000 Console Proxy) on page 123.

2. After connected, right-click on the IP address of a remote connection in the Remote OP Connection List and select **Link Details**.

   > **NOTICE:** If the link state shows zero bars, the connection is not established.

Check the following items if a remote MCC 7100 IP Dispatch Console cannot connect to the PRX 7000 Console Proxy server:

- Verify that a network path exists from the connecting remote MCC 7100 IP Dispatch Console to the control room firewall.

- Verify (if using a VPN connection) that a network path exists from the VPN server to the control room firewall.

- Verify that a proxy connection is configured on the connecting remote MCC 7100 IP Dispatch Console. This verification can be done from the Status application.

- Verify that the system clocks for the PRX 7000 Console proxy and remote MCC 7100 IP Dispatch Console are time synchronized. Due to security restrictions on the remote link, the clocks must be within 24 hours of each other.

- Check for an affiliated console on the console site.

- Open the Console Dispatch Status application on the PRX 7000 Console Proxy and verify that the connecting remote MCC 7100 IP Dispatch Console is not included on the black list.

- Open the Console Dispatch Status application on the PRX 7000 Console Proxy and check the remote MCC 7100 IP Dispatch Console capacity.

  - Verify that the number of connecting remote MCC 7100 IP Dispatch Consoles does not exceed the licensed capacity, and that the licensed capacity is not zero. If the licensed capacity is zero, see Troubleshooting the MCC 7100 IP Dispatch Console License Issues on page 82 for details.

- Check the power mode settings on the PRX 7000 Console Proxy and remote MCC 7100 IP Dispatch Console.

  - Verify the power mode setting, as described in Setting Windows Power Options on page 47, and restart the FLEXlm licensing service, if necessary.

- Using the Console Dispatch Status application on the remote MCC 7100 IP Dispatch Console, verify that the proxy server hostname or IP address is the address configured in the Customer Enterprise Network (CEN).

- Network elements between the MCC 7100 IP Dispatch Console and the PRX 7000 Console Proxy may not support standard Maximum Transmission Unit (MTU) or MTU Path Discovery. SeeChanging the Maximum Transmission Unit on page 83 for details.

Troubleshooting the PRX 7000 Console Proxy License Issues

If issues with the PRX 7000 Console Proxy licenses occur, perform the following procedure to determine the reason for the issues. The typical symptom of issues with the PRX 7000 Console Proxy licenses is the incorrect licensed remote OP connection capacity. Verify the capacity in the **Remote OP Connection List** tab of the PRX 7000 Console Status application. If the capacity is `0`, determine the issue.

Procedure:

- Verify that the new or modified license files are available in the following directory: `C: \ProgramData\Motorola Dispatch\Licenses`. If not, see Updating License Files for PRX 7000 Console Proxy on page 96.

- Verify that the MAC address obtained during the license generation phase corresponds to an enabled network device.

  If this network device is disabled, the licensing services do not run.

- Verify that the Windows power settings are correct. See Setting Windows Power Options on page 47

- If you use a temporary license, open the license file in a text editor and verify that the license did not expire by looking for a similar line:

  `+ INCREMENT console_proxy_conn motsol 1.0 07-feb-2012 10 \`

  The expiration date in non-temporary cases is set to `permanent`.

  If the license expired, perform the following actions:

  a. Generate a new license. See Generating License Certificates for the PRX 7000 Console Proxy on page 91

  b. Import the new license file into the predefined location. See Updating License Files for PRX 7000 Console Proxy on page 96.

- Verify that the FLEXlm License Manager service is up and running:
  - If the service is not running, start the service.
  - If the service is running but the `motsol.exe` executable is not running in the Task Manager, restart the service.

Changing the Maximum Transmission Unit

If intermediate network elements (routers, switches) drop packets greater than 1500 bytes, it may be necessary to change the value of the Maximum Transmission Unit (MTU) on the PRX 7000 Console Proxy or the MCC 7100 IP Dispatch Console to a lower value.

> **CAUTION:** Modify the MTU only as a last resort, after the all network settings have been check and verified.

Procedure:

1 Select **Start** and enter `regedit` in the search field.

2 In the registry editor, navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\interface-name`.

3 Right-click **MTU** of type **REG_DWORD** and select **Modify**.

4 Enter the desired MTU size in hexadecimal.

> **NOTICE:** The range of the MTU is 0x44 to the dynamically determined MTU (in bytes). Set this value to `0xFFFFFFFF`, to change the MTU back to the default value of the network interface dynamically determined MTU.

5 Click **OK**.

6 Close the **Registry Editor**.

7 Restart the computer.

PRX 7000 Console Proxy Disaster Recovery

This section provides details and references to help recover the PRX 7000 Console Proxy in the event of a failure.

Recovering a PRX 7000 Console Proxy Installation

Use disaster recovery if the current installation of the PRX 7000 Console Proxy has become unstable or inoperable. Follow this process to reinstall all necessary components.

Recovery of a PRX 7000 Console Proxy during a disaster recovery event requires a full installation.

Process:

1 Backup critical files used by the PRX 7000 Console Proxy. See Critical Backup Files for the PRX 7000 Console Proxy on page 100 for a list of files.

2 If necessary, install the Windows operating system. See Operating System Installation for the PRX 7000 Console Proxy on page 90.

3 Optional: If performing disaster recovery on replacement hardware, generate new License Certificates for the PRX 7000 Console Proxy. See Generating License Certificates for the PRX 7000 Console Proxy on page 91.

4 Install the PRX 7000 Console Proxy software. See Installing the PRX 7000 Console Proxy Software on page 92.

5 Optional: Install MOTOPATCH. See MOTOPATCH Installation on page 61.

MN000672A01-E
Chapter 3: PRX 7000 Console Proxy Setup and Installation

6   Install Supplemental CD. See Windows Supplemental Configuration (K Core) on page 93.

7   If necessary, configure the Network Interface Card (NIC). See Configuring the Computer Network Interface Card for the PRX 7000 Console Proxy on page 94.

8   If necessary, set up the Active Directory Domain. See Setting Up the Domain for the PRX 7000 Console Proxy on L and M Core on page 95.

9   Restore critical files backed up in step 1.

Critical Backup Files for the PRX 7000 Console Proxy

Archiving critical files is essential to the operation of the PRX 7000 Console Proxy. Perform archiving periodically. Archive the files to an external device, for example, external storage or network storage.

Table 12: PRX 7000 Console Proxy Files to Backup

File Type	Location	Note
License files	`C:\ProgramData\Motorola Dispatch\Licenses`	Back up the license files to speed up the recovery process.
Proxy Black List	`C:\ProgramData\Motorola PRX 7000\ProxyServer \blacklist.txt`	The Proxy Black List is a single file.

USB Audio Interface Module

USB Audio Interface Module

The USB Audio Interface Module (USB AIM) is an external device that you connect to the MCC 7100 IP Dispatch Console. It functions as an interface between analog devices and the console position and as a general-purpose input/output module.

The USB AIM supports audio routing between the dispatch operator and peripherals. The dispatch operator uses Motorola-standard peripherals that connect to the USB AIM device. The USB AIM connects to the MCC 7100 IP Dispatch Console with a USB cable.

The Instant Recall Recorder (IRR) software installed at the console position computer supports short-term audio logging so there is no requirement to support an external IRR port on the USB AIM device. The dispatch operator can replay the recorded audio directly from the hard drive of the console position computer.

Figure 4: USB Audio Interface Module – Audio Routing

Foot Switch   Desktop Mic   Headset Jackbox   Headset Jackbox   Computer

AIMMCC7100_IP_Connection_A
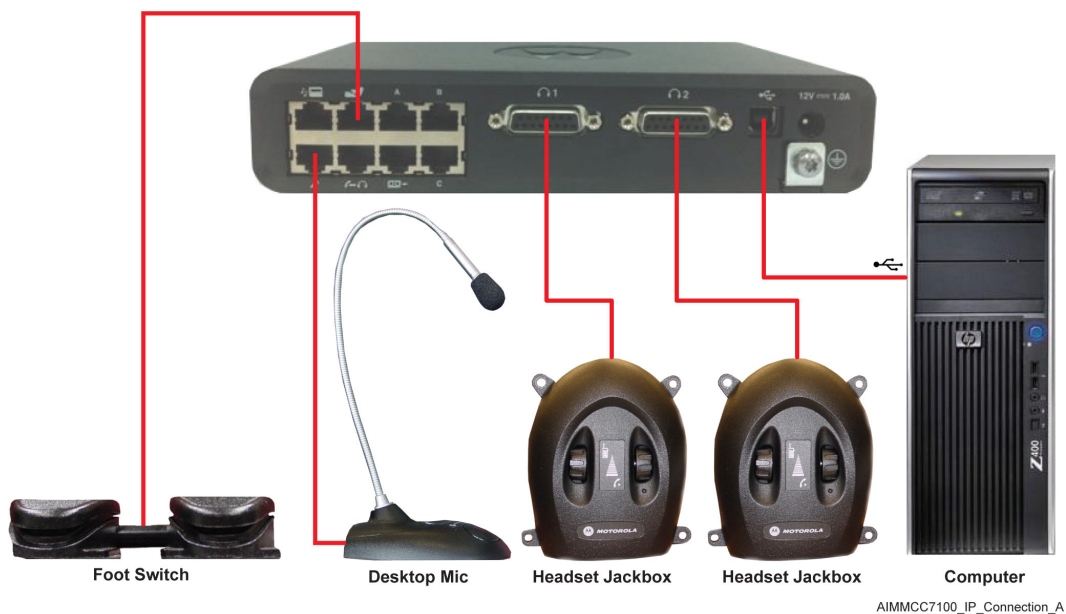
USB Audio Interface Module Connections

The USB Audio Interface Module (USB AIM) supports all the Motorola-standard peripherals except for the desktop speakers.Instead of the Motorola-standard speakers, use off-the-shelf USB speakers connected directly to the console operator position computer. In addition to the ports for standard peripherals and external devices, the USB AIM supports four generic local auxiliary outputs. These

ports activate warning lights to provide information about the operations performed by the dispatch operator.

Figure 5: USB Audio Interface Module Port Connections

AIM_USB_rear1_A
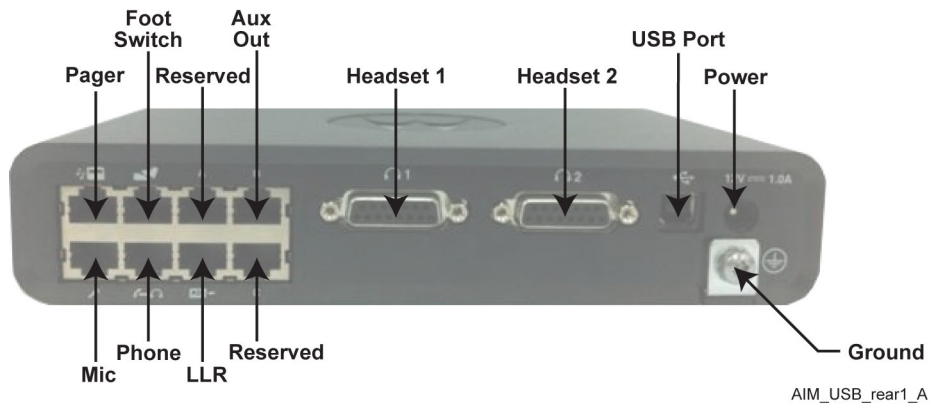
The USB port is used to connect the USB AIM device to the MCC 7100 IP Dispatch Console. Other ports are used to connect peripherals.

NOTICE: Do not connect the USB AIM to the telephone network directly.

Table 13: USB Audio Interface Module Peripherals

Port Type	Peripheral Type
Two DB-15 connectors	Two headset jacks
Eight RJ-45 connectors	One desk microphone
	One footswitch
	One external paging encoder
	One telephone/headset port
	One local logging recorder
	One auxiliary output port for four generic auxiliary output channels

Peripherals Supported with USB Audio Interface Module

The USB Audio Interface Module (USB AIM) supports most of the Motorola-standard peripherals. The following sections provide information on the Motorola-standard peripherals that you can connect to the USB AIM device and about the USB AIM ports.

Desk Microphone

The USB Audio Interface Module (USB AIM) can support a desktop microphone. The desktop microphone contains a transmit button and a monitor button in the base for use with the selected radio channel or channels. For each dispatch console, you can use one desktop microphone.

Figure 6: Gooseneck Microphone

MCC7500_microphone

The desk microphone can be attached to a horizontal surface or left freestanding so that the dispatcher can pick it up. The 18-inch long, flexible shaft allows the dispatcher to position the microphone head within a few inches of their mouth even when the base is placed behind a keyboard or writing area.

If a desk microphone is connected to a dispatch console while no headsets are connected, the desk microphone is active whenever any transmit function is active.

Each MCC 7100 Dispatch Console can support one desktop microphone.

If a desk microphone is connected to a dispatch console while one or two headsets are connected, the desk microphone is active only during a transmit function when the dispatcher presses the transmit button on it. This solution prevents the desk microphone from picking up unwanted background sound when the dispatcher uses a headset to transmit.

Footswitch

Each MCC 7100 IP Dispatch Console can support one footswitch.

The footswitch provides two foot pedals in a rugged, metal housing with a 10-ft cable. One pedal is for the general transmit feature and the other pedal is for the monitor feature.

The footswitch allows a dispatch operator to operate these features with their feet so their hands are freed for other tasks.

If necessary, the footswitch can be permanently fastened to the floor.

Figure 7: Footswitch

MCC7500_footswitch

Table 14: Footswitch Pinout

This table presents footswitch connector pinout. The pinout is the same as for Voice Processor Module (VPM) footswitch port.

Pin Number	Description (+) and (−) symbols indicate pin polarity
3	PTT In (+)
4	PTT In (−)
5	Monitor In (−)
6	Monitor In (+)

Headset Jacks

The USB Audio Interface Module (USB AIM) can support up to two headset jacks. A headset jack allows a dispatch console user to use a headset while operating the dispatch console. The headset jack supports headsets that use either PJ7 (6-wire) or PJ327 (4-wire) long frame connectors. The 6-wire headsets have a Push-to-Talk (PTT) button while the 4-wire headsets do not have a PTT button.

The headset jacks shipped from the factory are configured for the 6-wire headsets. For the 4-wire operation, open the housing and make changes, depending on the version of the headset box. For more information, see Configuring the Headset Jack Box for 4-Wire Operation on page 105.

Figure 8: Headset Jack

MCC7500_headset

The headset jack has two volume controls:

- For adjusting the level of the received radio audio
- For adjusting the level of the received telephone audio

A small dimple is molded into the headset jack housing near the telephone volume control so that a dispatcher can tell them apart without having to look at them. The headset jack allows the dispatch console users to use headsets, which decreases the ambient noise in a control room and reduces the effect of any ambient noise on dispatch console transmissions. This solution improves the quality of the audio being transmitted from the control room and allows the dispatch console users to hear received audio more clearly.

When a headset is plugged into a headset jack, the selected receive audio is typically removed from the speakers and routed to the headset earpiece.

> **NOTICE:** A radio resource may be configured so its selected receive audio remains in a speaker even when a headset is in use. If two headsets are connected to a dispatch console, the same audio is heard in the earpieces of both headsets.

If a telephone set connected to a dispatch console telephone/headset port is taken off hook while a headset is connected to a dispatch console, the selected radio audio is removed from the headset earpiece and routed to the appropriate speakers. The received telephone audio is routed to the headset earpiece. The headset microphone becomes live and its audio is routed to the external telephone set. In this way, a dispatch console user can talk and listen on the telephone set in a hands-free full-duplex mode.

The headset jack is mounted either underneath a writing surface or on top of a writing surface. The headset jack is designed with a low profile and rounded edges to minimize "knee banging" when mounted underneath a writing surface.

Configuring the Headset Jack Box for 4-Wire Operation

Prerequisites: The headset jack box is configured for use with a 6-wire headset as shipped. If a 4-wire headset is used, either cut a wire jumper or reposition DIP switches inside the headset jack box. With headset jack box disconnected from equipment, remove the four screws holding the top and bottom housing together; the access for the T10 Torx screws is on the bottom of the headset jack box.
For proper operation of the headset microphone audio to be presented to the external telephone caller, both the headset jack box and the headset base must be 4-wire or both must be configured for 6-wire, and the parameters in the Zone Configuration Manager (ZCM) must match. If you change the ZCM, ensure that you perform the **Commit** operation.

Procedure:

1. **Headset Jack Box with NO DIP switches on the underside of the headset jack box:**
   Perform the following actions:

   a Separate the top and bottom housing exposing circuit board and the tip and ring contacts.

   b Identify the brown wire connected between J3 on the circuit board and the switch contacts.

   c Cut the brown wire.

   d Reassemble the jack box.

2. **Headset Jack Box with the two DIP switches on the underside of the box:** Configure Switch 2:

   - For 6-wire operation: S2-1 = ON, S2-2 = ON.
   - For 4-wire operation: S2-1 = OFF, S2-2 = OFF.

     > **CAUTION:** Do not reposition other switches in the headset jack box, because doing so adversely affects operation of the headsets.

Figure 9: Locations of S1 and S2

This figure shows the locations of S1 and S2.
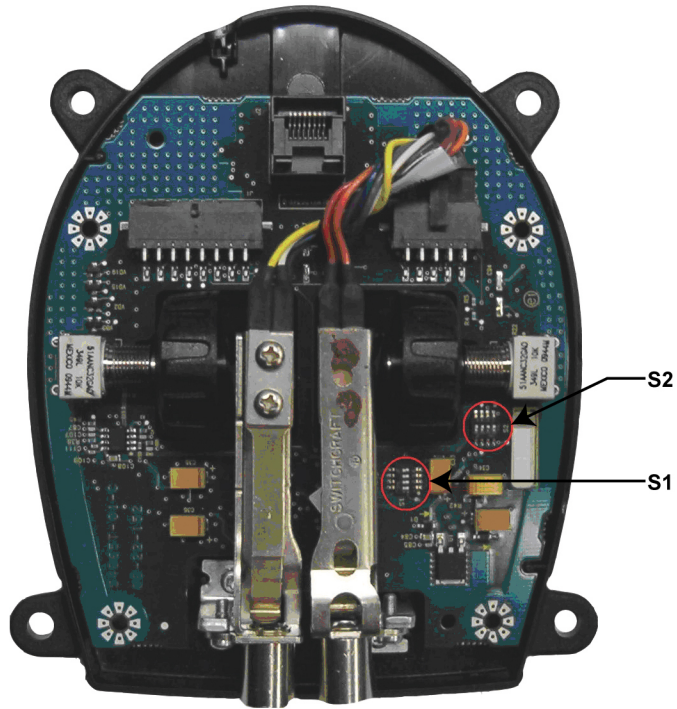
Headset_jack_S1_S2_locations

Figure 10: Locations of S1 and S2

This figure shows the location of the brown wire.
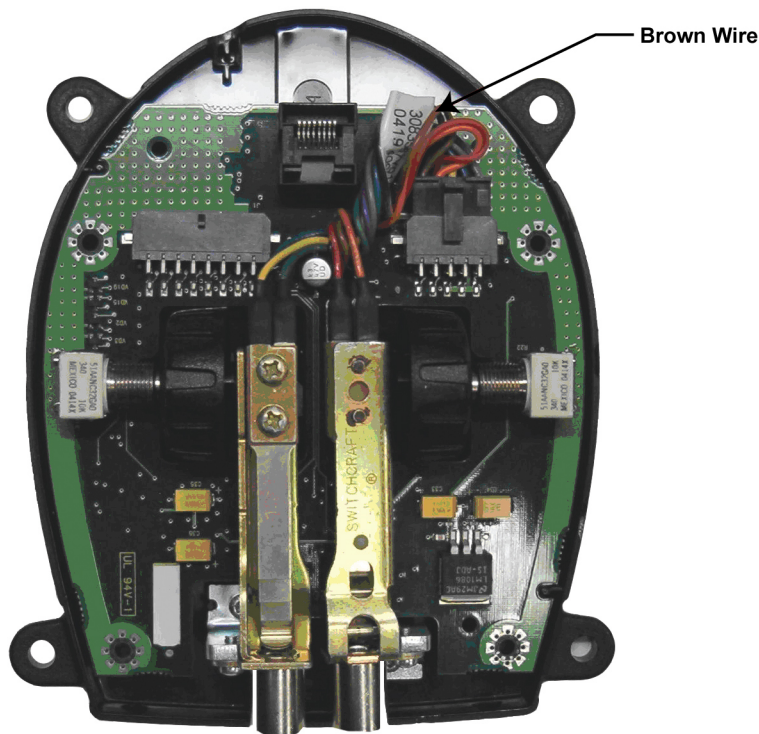
Headset_jack_brown_wire

External Paging Encoder Port

The external paging encoder port allows use of an external tone paging encoder with a dispatch console to provide tone paging services. The dispatch console transmits the paging tones generated by the encoder on the selected conventional radio resource or resources. If a dispatcher wants to send paging tones on an ASTRO® 25 Conventional channel, an external paging encoder is required.

This feature has an RJ-45 connector with an analog 600-Ohm audio input to which the paging tones are applied. A paging Push-to-Talk (PTT) input enables a dry contact closure to be applied that indicates when the dispatch console should transmit the tones on the radio channel or channels.

When the dispatch console sees the paging PTT input go active, it transmits the audio appearing at the audio input on the selected conventional channels. If Private Line (PL) Stripping is enabled on a conventional channel, the PL is stripped when the paging tones are transmitted.

No de-emphasis filtering is performed and no talk extend is provided with externally generated tones. The external paging encoder provides these functions.

Table 15: External Paging Encoder Port Pinout

Pin Number	Description (+) and (–) symbols indicate pin polarity
1	Paging PTT In (–)
2	Paging PTT In (+)
3	Paging Audio In (–)
6	Paging Audio In (+)

Local Logging Recorder Port

The local logging recorder port allows an external logging recorder to be connected to a dispatch console. The port provides an RJ-45 connector with a 600-Ohm analog output. The audio that appears on this output is configured and is typically the audio transmitted and/or received at that dispatch console.

The configuration of audio presented at this port is tied to the physical dispatch console, so that no matter what user is logged on the dispatch console, the same type of audio is logged. This configuration is done as part of configuring the dispatch console at the Provisioning Manager. The local logging recorder port is configured to log any combination of the following audio sources:

- Audio received from the currently selected radio resources. Either the individual volume setting of the radio resource or the master volume control on the speaker or headset jack adjusts the level of this volume.

- Microphone audio being transmitted to the radio resources currently selected by the operator.

- Microphone audio being transmitted to the radio resources not selected by the operator.

- Any tones generated by the dispatch console that appear in its speakers, for example, trunking tones and emergency tones.

- Tones generated by an external paging encoder.

Long-term, console-specific audio recording is used to record a portion of the inbound and outbound audio present on a specific dispatch console. This recording is done by providing a logging port at the dispatch console and wiring that port to a track of an audio recording device. These recordings are typically archived for long-term storage, and provide a historical record of the radio communications made at a given dispatch console.

In the local logging recorder port, audio out to logger pins are pins 4 and 5. This pinout is the same as for the Voice Processor Module (VPM) local logging recorder port.

Telephone/Headset Port

The telephone/headset port allows an external telephone set to be connected to the dispatch console. The dispatch operators can then use their headset to communicate on both the radio system and the telephone set. The port provides the following inputs and outputs:

- A 600-Ohm analog audio output for the microphone audio from the headset
- A 600-Ohm analog audio input for the audio received from an external telephone
- An input buffer for the Off-Hook signal from the external telephone
- An input buffer for an Auxiliary Jack Sense signal from the external telephone

When a dispatch console senses a dry closure on the Off-Hook input buffer, it removes the selected radio audio from the headset earpiece and routes it into the appropriate speakers. Then it routes any audio appearing at the telephone/headset port audio input to the headset earpiece. The dispatch console also routes the headset microphone audio to the telephone/headset port audio output, which allows the dispatch console user to communicate hands-free on the telephone set.

When the dispatch console senses a dry closure on the Auxiliary Jack Sense input buffer, it ignores any closures on the Off-Hook input buffer. This system causes the headset to work with the radio system instead of the external telephone system, and allows the dispatch console headset to be used for radio operations when another person is staffing the telephone set.

If the dispatch console user transmits on any radio resources while the Off-Hook signal is active, the headset microphone is rerouted to the radio system for the duration of the transmission. When the transmission ends, the headset microphone is routed back to the telephone/headset port audio output. The headset earpiece audio routing is not changed during the transmission, so the dispatch console user can hear the audio received on the telephone.

The telephone/headset port allows a dispatcher to use a single headset to communicate on both the radio system and a telephone system, such as a 911 system.

NOTICE: Do not connect the USB Audio Interface Module (USB AIM) to the telephone network directly.

The ability to communicate with a 911 system is available even when the USB AIM cannot communicate with the MCC 7100 IP Dispatch Console computer.

Table 16: External Phone Interface Connector Pinout

This table presents external phone interface connector pinout. The pinout is the same as for Voice Processor Module (VPM) phone port.

Pin Number	Description (+) and (−) symbols indicate pin polarity
1	Jack Sense In (−)
2	Jack Sense In (+)
3	Audio In from Phone System (−)
4	Audio Out to Phone System (−)
5	Audio Out to Phone System (+)
6	Audio In from Phone System (+)
7	Off Hook In (+)

Table continued…

Pin Number	Description (+) and (–) symbols indicate pin polarity
8	Off Hook In (–)

Local Console Relay Outputs – MCC 7100 Configurable Functions

The Local Console Relay feature uses the existing Aux output ports on the USB Audio Interface Module (USB AIM) to provide relay closures whenever:

- The dispatcher is transmitting audio on a radio resource
- An inbound call is occurring on a selected channel
- There is an emergency activity (acknowledged or unacknowledged) on the console
- A pre-designated alarm Aux I/O is activated

The relay closures activate warning lights that serve as an indication that the dispatcher is busy and should not be disturbed. The alarm Aux I/O acts as a notification that a critical situation has arisen that requires attention.

The Elite Admin user interface is used to set Aux I/O that triggers the Aux I/O alarm relay. The **Alarm off** button on the console GUI is used to turn off the Aux I/O alarm relay. No relay defaults to indicating an inbound call is occurring on the selected channel to reduce excess relay chatter during dispatch operations. To enable the relays when a System release console is connected to an A7.15 or previous release core, see Enabling the Relays in the Windows Registry. Multiple public Aux I/Os can be mapped to a single Alarm Aux I/O port on the console. The activation of any of these Aux/IO triggers the alarm.

Table 17: Generic Auxiliary Outputs Pinout

To configure the MCC 7100 local console Aux I/Os, see the *Provisioning Manager* manual or the *Configuration Manager – Conventional* manual.

Pin Number	Description (+) and (–) symbols indicate pin polarity
1	Local AuxIO 1 (-)
2	Local AuxIO 2 (+)
3	Local AuxIO 3 (-)
4	Local AuxIO 4 (+)
5	Local AuxIO 4 (-)
6	Local AuxIO 3 (+)
7	Local AuxIO 2 (-)
8	Local AuxIO 1 (+)

USB Audio Interface Module Specifications

Before you mount and install the USB Audio Interface Module (USB AIM), verify that you meet the environmental requirements necessary for the device to operate.

Table 18: USB Audio Interface Module Specifications

USB Audio Interface Module Feature	Specifications
Physical dimensions	Height (excluding the rubber foot): 1.65 inches (42 mm)
	Width: 8.39 inches (213 mm)
	Depth: 5.23 inches (133 mm)
Weight	1.43 lb (0.65 kg)
AC Operating Voltage for the USB AIM Power Supply	90 VAC - 264 VAC
	Minimum input voltage 90 VAC with 57 Hz~63 Hz
	Maximum input voltage 264 VAC with 47 Hz~53 Hz
	Typical input voltages are 115 VAC and 230 VAC
DC Operating Voltage for the USB AIM Device	12 VDC (nominal)
Maximum Power Consumption	0.5 A at 12 VDC (6 W)
Operating Temperature	5 °C (41 °F) — 40 °C (104 °F)
Storage Temperature	-25 °C (-13 °F) — 70 °C (158 °F)
Relative Humidity Operating	0% — 90% relative humidity at 40 °C non-condensing

USB Audio Interface Module FRU/FRE Information

If you cannot resolve your issues with the USB Audio Interface Module (USB AIM) (B1941) by performing basic diagnostics and troubleshooting, replace the item.

The following table provides information about the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) for the USB AIM.

Table 19: USB AIM FRU/FRE Information

Part Number	Description
PMPN4052A	USB Audio Interface Module Interchangeable Power Supply without Adaptor (1 piece)
RLN6349A	North American Power Adaptor (1 piece)
RLN6234A	European Power Adaptor (1 piece)
1564027V01	UK Power Adaptor (1 piece)
58012005001	Australia Power Adaptor (1 piece)
RLN6448A	Brazil Power Adaptor (1 piece)
PMHN4249A	Mounting Bracket Kit

Table continued…

Send Feedback

Part Number	Description
30009477001	USB 2.0 Cable for USB Audio Interface Module (1 piece)

USB Audio Interface Module Bonding and Grounding Requirements

General Bonding and Grounding Requirements

Mount the USB Audio Interface Module (USB AIM) device under the writing surface or on the top of the writing surface using the mounting brackets shipped with the device.

For the information about grounding and bonding equipment in dispatch centers, see the following sections in the *Standards and Guidelines for Communication Sites* manual:

- "Bonding to Equipment and Ancillary Support Apparatus"

- "Grounding (Earthing) for Dispatch Centers and Network Operator Positions and Work Areas"

Grounding Cabling Standards

When you attach the equipment grounding (earthing) conductors to your equipment and the ancillary support apparatus, meet the following bonding standards:

- Each electronic equipment chassis must have a separate and independent equipment grounding conductor.

- Paint, enamel, lacquer, and other electrically non-conductive coatings must be removed from threads and bonding surface areas to ensure good electrical continuity (NFPA 70-2005, Article 250.12).

  ⚠️ **CAUTION:** Using a star washer does not alleviate the requirement to remove non-conductive coatings from attachment surfaces because the star washer does not provide enough contact surface area.

- Connections to steel and galvanized steel pipes, conduit, or other round member items must be made by using a UL 486A listed, bolted clamp with stainless steel securing hardware or other suitable listed means. In high-humidity areas, the clamps must be stainless steel or tin-plated UL 486A listed to prevent galvanic corrosion.

- Connections to vibrating or moveable items must be made by using an exothermic weld or a compression-type two-hole lug.

- Connections to structural building steel must be made by using an exothermic weld, listed irreversible high compression-type connection, or listed tin-plated flange-type bonding connector equipped with two securing bolts.

- Connections to the raised flooring support system must be made by using a tin-plated listed compression lug, listed pedestal clamp, or exothermic welding. Where practical, the lug should be effectively bonded to the upper support plate of the pedestal or to cross connecting stringer.

Integrate equipotential bonding at a network operator position into the position equipment to the greatest extent possible. This solution reduces the need to place equipment grounding conductors. Bond all telecommunication cable shields, data cable shields, and the equipment or furniture AC Equipment Ground (ACEG) together at the Sub-System Ground Bus Bar (SSGB) position or within the equipment. Bond outer shields of telecommunication cables serving the network operator position or cluster of positions (to or from a different location) directly to the SSGB or by using conductors:

- 16 mm2 csa (#6 AWG) insulated copper conductor for lengths not exceeding 3.9 m (13 ft)

- 6 mm2 csa (#10 AWG) insulated copper conductor for lengths not exceeding 1.8 m (6 ft)

The outer shield ground is provided automatically when the cable connector contains a shield-to-chassis connection.

Installing and Configuring USB Audio Interface Module

The USB Audio Interface Module (USB AIM) is an external device that you connect to the MCC 7100 IP Dispatch Console. Perform the following process to cable, ground, and configure the USB AIM device.

Prerequisites:
Verify that you have the USB AIM power supply and the USB cable necessary to connect the device to the MCC 7100 IP Dispatch Console computer. The cables necessary to connect peripherals to the USB AIM device are provided with the peripherals.

Verify that you have the brackets necessary to mount the USB AIM device.

Plan mounting and grounding the USB AIM device. See USB Audio Interface Module Bonding and Grounding Requirements on page 111 andUSB Audio Interface Module Specifications on page 110.

Process:

1   Connect the USB AIM.

    See Connecting USB Audio Interface Module on page 112.

2   Configure the USB AIM by using the Peripheral Configuration Tool application.

    See Configuring USB Audio Interface Module on page 112.

Connecting USB Audio Interface Module

To prepare the USB Audio Interface Module (USB AIM) device for operating in your system, connect it to the MCC 7100 IP Dispatch Console, plug in all the necessary peripherals, and power it on.

Procedure:

1   Connect the USB AIM device to the MCC 7100 IP Dispatch Console computer using the provided USB cable.

2   Connect the peripherals to the appropriate USB AIM ports.

    See USB Audio Interface Module Connections on page 101.

3   Connect the USB AIM device to a 12 V power socket using the provided power supply.

    The green and red LEDs on the front of the device are on for a time. Then the red LED goes off and the green LED stays on.

The USB AIM is operational but not configured.

Configuring USB Audio Interface Module

After connecting the USB Audio Interface Module (USB AIM) to the MCC 7100 IP Dispatch Console, it is operational but not configured. To use the peripherals connected to the USB AIM, create a configuration in the Peripheral Configuration Tool application installed on the MCC 7100 IP Dispatch Console computer.

To use the peripherals connected to the USB AIM, create a configuration in the Peripheral Configuration Tool.

Prerequisites:
Verify the state of the LEDs on the front of the device. If only the green LED is on, the device is fully operational and you can continue. If the state of the LEDs is different, resolve the issue. See USB Audio Interface Module Indicators on page 114

Ensure that the MCC 7100 IP Dispatch Console computer has the Windows 7 Service Pack 1 installed.

Procedure:

1 From the Windows **Start** menu, select **All Programs → Motorola → MCC 7100 Dispatch →
Peripheral Configuration Tool**.

The application automatically detects the USB AIM connected to the dispatch console. In the
Summary pane, the USB AIM status is `Connected`. A default configuration or a configuration
created by a user is displayed. If a default configuration is displayed, the mapped devices are
non-Motorola peripherals connected to the dispatch console or Motorola-standard peripherals
connected to the USB AIM. If the mapped peripherals are Motorola-standard, the Motorola logo
appears for them.

2 Click **Configure AIM**.

> **NOTICE:** The External Phone Interface operates only with the Motorola-standard
> headset connected to the USB AIM. If using the External Phone Interface, keep the
> Motorola-standard headset mapped the Peripheral Configuration Tool and connected to
> the USB AIM.

In the **Summary** pane, the appropriate graphical icons are highlighted and the Motorola logo
appears for the Motorola-standard peripherals connected to the USB AIM.

3 If the speakers are not configured, perform the following actions:

a Navigate to the **Audio Outputs** tab.

b Map the MCC 7100 IP Dispatch Console speakers to physical speakers connected to the
dispatch console computer by selecting them from the drop-down lists available for each
physical speaker.

4 In the **Profile** pane, click **Save As**.

5 In the **Save As** window, enter the name of the new configuration. Click **Save**.

The application automatically selects the new configuration as the currently used configuration.

Upgrading the USB Audio Interface Module Software

If you experience problems with the USB Audio Interface Module (USB AIM), the USB-AIM may
contain an older or unsupported software version. Perform this procedure to upgrade the software.

Prerequisites: Ensure that you do not have any active calls. During the upgrade of the USB AIM
software, the audio peripherals connected to the device are not usable. Additionally, the USB AIM
device restarts during the upgrade process and all the operations performed by the USB AIM are
terminated.

Procedure:

1 From the Windows **Start** menu, select **All Programs → Motorola → MCC 7100 Dispatch →
Peripheral Configuration Tool**.

2 From the **File** menu, select **USB AIM Software Update**.

3 In the firmware information window, select **Update**.

4 In the warning window, click **Yes**.

The upgrade process takes a few minutes. After the upgrade process finishes, the USB AIM
restarts. In the firmware information window, you receive a message about a successful
software upgrade.

5 Click **OK**.

USB AIM Device Information

Retrieve details about your USB Audio Interface Module (USB AIM) device using the **USB AIM Device Information** window in the Peripheral Configuration Tool application.

The window contains the following information:

- Firmware version

- Kit number

- Tanapa number

Accessing the USB-AIM Device Information

In the main menu of the Peripheral Configuration Tool application, click **File → USB AIM Device Information**.

> **NOTICE:** If the Peripheral Configuration Tool cannot access the information about the USB AIM, an error appears in the **USB AIM Device Information** window. If you encounter this issue, close the window and unplug the USB cable from the USB AIM and from the MCC 7100 IP Dispatch Console computer. Wait a while, plug the cable in, and reopen the **USB AIM Device Information** window.

Copying the USB AIM Device Information

In the **USB AIM Device Information** window, click **Copy to clipboard**.

USB Audio Interface Module Troubleshooting

To diagnose problems with the USB Audio Interface Module (USB AIM), use the LED indicators on the front of the device. They provide helpful information about the possible causes of the problem.

If you cannot diagnose the problem using the LED indicators, review the troubleshooting scenarios for a procedure that can work for the symptoms you observe.

If you cannot find a scenario for your issue, or the provided scenario does not work, contact Motorola Solution Support Center (SSC).

USB Audio Interface Module Indicators

USB Audio Interface Module (USB AIM) has one green LED and one red LED on the front panel. Use these LEDs to verify the status of the device and resolve any issues.

When the USB AIM is fully operational, the green LED on the front of the device is on and the red LED is off, and the device is in the online state. Any other configuration indicates possible issues.

Figure 11: USB AIM State Indicators

Green LED — Red LED

AIM_USB_front1_A

Table 20: USB AIM States

Green LED State	Red LED State	USB AIM Device State	USB AIM Device State Description
On	Off	Online	The USB AIM is operational. The USB interface is up and working.
Flashing	Off	Link Down	The USB AIM is operational but the USB interface is not active. External Phone Interface is active. **Possible Issues:** The USB cable is unplugged. The host computer is down. **See:** Troubleshooting USB Audio Interface Module USB Communication Issues on page 117
On	Flashing	Impaired	The USB AIM can be operational but requires servicing. The state of the USB interface is unknown. Codecs initialized. **Possible Issues:** An alternate Field-Programmable Gate Array (FPGA) image is present but it is corrupt and failed to boot. The EE Non-Volatile Memory (NVM) checksum failure occurred. There is a mismatch between the FPGA version and the NVM version. **See:** Upgrading the USB Audio Interface Module Software on page 113
Off	On	Failure	Hardware or firmware failure. **Possible Issues:** The host computer is in the sleeping mode. Power-On Self-Test (POST) failed. Codecs failed to initialize. I2C failed. **See:** Troubleshooting USB Audio Interface Module USB Communication Issues on page 117 Upgrading the USB Audio Interface Module Software on page 113

Table continued…

Green LED State	Red LED State	USB AIM Device State	USB AIM Device State Description
On	On	Booting	The device hung in the booting state that takes place just after you power on the device. **Possible Issues:** The USB AIM FPGA did not configure.

USB AIM Status Icon

From the **Summary** pane of the Peripheral Configuration Tool, use the USB Audio Interface Module (USB AIM) status icon to verify the state of the device. The icon shows one of the three possible states of the device.

USB AIM ✓	The USB AIM is connected and fully operational.
USB AIM	The USB AIM is not connected.
USB AIM ✗	The USB AIM is connected but not operational. Hover over the icon to learn additional details about the problem.

Diagnosing Audio Malfunction in USB Audio Interface Module

If you experience problems with the USB Audio Interface Module (USB AIM) audio, the possible issues are problems with the USB connection between the USB AIM and the dispatch console, problems with the USB AIM, or problems with the MCC 7100 IP Dispatch Console computer.

Procedure:

1 In the **Control Panel** of the Windows operating system, navigate to the **Sound** window.

2 In the **Recording** tab, for each device on the list, perform the following actions:

   a Right-click the device and select **Properties**.

   b In the **Properties** window, select the **Listen** tab.

   c Ensure that the **Listen to this device** check box is **not** selected.

   d Click **OK**.

3 In the **Sound** window, click **OK** to save changes to all the devices.

4 Disconnect the USB AIM from the MCC 7100 IP Dispatch Console computer.

5 Ensure that the External Phone Interface (EPI) is connected to the USB AIM.

6 Restart the USB AIM by unplugging the power supply, waiting a while, and plugging it in again.

   The USB AIM goes into the EPI fallback mode.

7 Verify that the USB AIM audio works in the EPI fallback mode by performing a phone call.

8 Connect the USB device to the MCC 7100 IP Dispatch Console.

9 Perform one of the following actions:

  - If the audio in the EPI fallback mode worked properly, verify the USB communication between the USB AIM and the dispatch console.
    See Troubleshooting USB Audio Interface Module USB Communication Issues on page 117

  - If the audio in the EPI fallback mode did not work properly, try to upgrade the USB AIM software.
    See Upgrading the USB Audio Interface Module Software on page 113.

Troubleshooting USB Audio Interface Module USB Communication Issues

If you experience problems with the USB communication between the USB Audio Interface Module (USB AIM) and MCC 7100 IP Dispatch Console, the issue can be the connection itself or a problem with the MCC 7100 IP Dispatch Console computer. The symptoms can be the USB AIM indicating the Link Down or Failure state and the audio malfunction.

Procedure:

Verify the state of the LED indicators on the front of the USB AIM:

If…	Then…
If the green LED flashes and the red LED is off,	perform the following actions: a Verify that the USB cable is properly connected to the USB AIM and the dispatch console computer. b Verify that the dispatch console computer is turned on.
If the green LED is off and the red LED is on,	verify that the dispatch console is not in the sleep mode.

If you solved the problem by using these verification actions, the green LED is on and the red LED is off which means that the USB AIM is again online and fully operational. If the USB AIM state did not change, the problem can be the USB AIM failure.

Postrequisites: If you did not manage to solve the issue, upgrade the USB AIM software.

Troubleshooting USB Audio Interface Module Upgrade Issues

If you were unable to upgrade the USB Audio Interface Module (USB AIM), the reason can be a lost USB connection. If you encountered any upgrade issues, use the following scenario to retry to upgrade the USB AIM software.

Procedure:

1 Unplug the USB cable from the USB AIM and from the MCC 7100 IP Dispatch Console computer, wait a while, and plug the cable in again.

2 Retry to upgrade the USB AIM software in a typical way.

3 Restart the USB AIM device by unplugging the power supply, waiting a while, and plugging it in again.

The green and red LEDs on the front of the device are on for a while. Then the red LED goes off and the green LED stays on.

4 Retry to upgrade the USB AIM software in a typical way.

Troubleshooting Peripherals

If any of the peripherals connected to the USB Audio Interface (USB AIM) do not work properly, verify that they can communicate with the USB AIM and that there are no connection issues.

Procedure:

1 Ensure that the peripherals are connected to the appropriate ports.

See USB Audio Interface Module Connections on page 101.

2 Verify that the cables and connections for the peripheral devices are in an operating condition and not worn or broken and replace the defective cables.

3 Verify that the peripherals are mapped correctly in the Peripheral Configuration Tool application.

See Configuring USB Audio Interface Module on page 112.

Chapter 5

Console Dispatch Status and Peripheral Configuration Tool

This chapter provides descriptions and procedures for using the Console Dispatch Status and Peripheral Configuration Tool.

> **NOTICE:** The Console Dispatch Status application is installed as part of the MCC 7100 IP Dispatch Console and PRX 7000 Console Proxy software installations.

Console Dispatch Status (MCC 7100 IP Dispatch Console)

In an MCC 7100 IP Dispatch Console installation, use the Console Dispatch Status application to setup and point to proxy server connections for MCC 7100 IP Dispatch Consoles deployed outside the ASTRO® 25 Radio Network Infrastructure (RNI). For inside the ASTRO® 25 RNI configurations, the Console Dispatch Status is used only for licensing and encryption.

Up to five proxy server connections can be configured in the Console Dispatch Status. After configured, the Console Dispatch Status application can access any of the proxy server connections to establish a secure link to the ASTRO® 25 RNI. Only one proxy server connection can be accessed at any time. Additional proxy server connections configured are used as a backup in case the current connection is not available. The Console Dispatch Status application displays the status of the active proxy connection. The status of inactive proxy server connections is unknown.

Launch the Console Dispatch Status application from the **Start** menu of the Windows operating system by selecting **All Programs → Motorola → MCC 7100 Dispatch → Console Status**.

To exit the application, click **File → Exit**. Clicking **X** closes the window and places an icon in the Windows taskbar. The **Help** menu launches the online help or opens the **About** window.

Console Dispatch Status Taskbar Icon

Use the **Console Dispatch Status** taskbar icon to monitor the Link Statistics, open the **Console Dispatch Status** window, or close (**Exit**) the application. By default, the taskbar icon does not appear in the Windows taskbar until the Console Dispatch Status application is opened and minimized. See Customizing the Console Dispatch Status Taskbar Icon on page 119 for details.

Figure 12: Console Dispatch Status Taskbar Icon
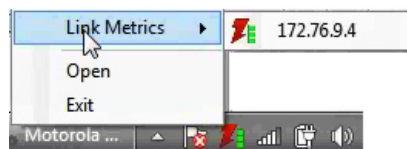
Customizing the Console Dispatch Status Taskbar Icon

Customize the **Console Dispatch Status** taskbar icon so it can appear in the taskbar notification area.

Procedure:

1   Open the Console Dispatch Status application.

2 Click **X** in the upper right-hand corner to close the application.

This selection shows the list of application icons that can be customized to appear in the taskbar notification area.

3 In the Windows taskbar notification area, click the **Show hidden icons** arrow.

Figure 13: Windows 7 Taskbar Notification Area
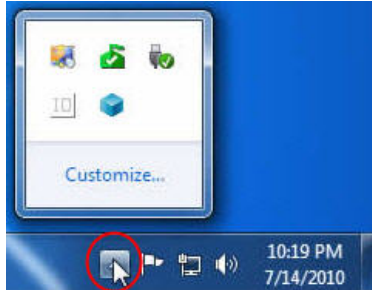
4 Select **Customize**.

5 Locate **ConsoleStatusApp** and set the behaviors to **Show icons and notifications**.

6 Click **OK**.

> **NOTICE:** Selecting **File → Exit** closes the application and removes the icon from the taskbar notification area. Clicking **X** to close the application minimizes the application as an icon in the taskbar notification area.

Proxy Server List

> **NOTICE:** The Proxy Server List tab appears only when the Console Dispatch Status application is launched from an MCC 7100 IP Dispatch Console deployed outside the ASTRO® 25 Radio Network Infrastructure (RNI).

The status of configured proxy server connections are monitored and displayed under the **Proxy Server List** tab. The **Proxy Server List** tab is visible only for MCC 7100 IP Dispatch Consoles deployed outside the ASTRO® 25 RNI. For consoles inside the ASTRO® 25 RNI, only the **Encryption / Licensing** tab is shown.

Proxy Server List Status Indicator

The state of the connection is displayed under the Link column. The three-bar link indicator moves up and down, indicating the strength of the connection to the proxy server. The status can change from three green bars (excellent) to all grayed out (no connection).

Figure 14: Proxy Server List Status Indicator

Proxy Server List Buttons

Use the buttons on the Proxy Server List to manage the proxy server connections configured for the MCC 7100 IP Dispatch Console:

Table 21: Proxy Server List Buttons

Button	Description
Link Metrics	Opens the **Link Statistic** window used to diagnostic network issues.
Add	Used to setup and configure proxy server connections.
Edit	Used to modify the currently selected proxy server connection
Remove	Used to remove the currently selected proxy server connection
Up and Down Arrows	Used to change the ordering of the selected proxy server connection

ASTRO Domain Configuration

During installation, the DNS suffix assigned to the domain controller is configured and automatically assigned as the Configured ASTRO® 25 Domain. For consoles outside the ASTRO® 25 Radio Network Infrastructure (RNI) that are on the Customer Enterprise Network (CEN) domain, enter the DNS suffix for the ASTRO® 25 domain. To change the domain, click **Edit Domain**. However, any change to the ASTRO Domain Configuration requires a restart of the Elite Dispatch.

Adding a Proxy Server Connection

The Console Dispatch Status application manages proxy server connections by adding a proxy server host name or IP address.

NOTICE: The proxy server connections added to the Console Dispatch Status application can be from any proxy server within the same site or from a different site.

Procedure:

1 From the Windows **Start** menu, select **All Programs → Motorola → MCC 7100 Dispatch → Console Status**.

2 From the **Proxy Server List** tab, click **Add**.

3 For the proxy connection in the site, enter a **Host Name** or **IP address**.

NOTICE: The IP address used in the Console Dispatch Status is the IP address mapped in the Control Room Firewall for the PRX 7000 Proxy Server.

4 If necessary, enter a description in the **Notes** field when only using an IP address for the proxy connection.

5 Click **Save**.

Editing a Proxy Server Connection

Procedure:

1 From the Windows **Start** menu, select **All Programs → Motorola → MCC 7100 Dispatch → Console Status**.

2 Select an existing proxy server connection in the **Proxy Server List**.

3 Click **Edit**.

4 Modify the **Host Name/IP** or **Notes** field.

5 Click **Save**.

Removing a Proxy Server Connection

Procedure:

1 From the Windows **Start** menu, select **All Programs** → **Motorola** → **MCC 7100 Dispatch** → **Console Status**.

2 Select an existing proxy server connection in the **Proxy Server List**.

3 Click **Remove**.

4 Click **Save**.

Encryption/Licensing

✏️ **NOTICE:** The **Encryption/Licensing** tab appears only when the Console Dispatch Status application is launched from the MCC 7100 IP Dispatch Console.

The **Encryption/Licensing** tab provides status information regarding the Crypto Status, Over-the-Ethernet-Keying (OTEK) Status, and Licensing Status for the MCC 7100 IP Dispatch Console.

The **Crypto Status** section displays the method used to store encryption keys. These keys can be either software key files on the MCC 7100 IP Dispatch Console or keys loaded onto a CRYPTR micro device. **Key Store** opens an explorer window and displays the directory defined in the Key Storage Path, and is used to manage key files stored in the console. The **OTEK Status** section displays the status of the OTEK connection and the server. The **Licensing Status** section displays the current call capacity for the configured license.

MCC 7100 IP Dispatch Console Call Capacities

The MCC 7100 IP Dispatch Console supports four capacities that are enforced by licensing. The capacities can also depend on the location of the dispatch console.

Table 22: MCC 7100 IP Dispatch Console Call Capacities

Maximum Number of Simultaneous Streams	Maximum Number of Resources Configured	Location	Voice Encryption
5	15	Inside ASTRO® 25 Radio Network Infrastructure (RNI) and outside ASTRO® 25 RNI	Advanced Encryption Standard (AES), Digital Encryption Standard – Output Feed-Back (DES-OFB), and Advanced Digital Privacy (ADP)
10	30	Inside ASTRO® 25 RNI and outside AS-TRO® 25 RNI	AES, DES-OFB, and ADP
15	45	Inside ASTRO® 25 RNI only*	AES, DES-OFB, and ADP

Table continued…

Maximum Number of Simultaneous Streams	Maximum Number of Resources Configured	Location	Voice Encryption
20	60	Inside ASTRO® 25 RNI only*	AES, DES-OFB, and ADP

* If you deploy a higher tier dispatch console outside the ASTRO® 25 RNI, the number of the simultaneous streams it supports is automatically downgraded to ten streams.

Console Dispatch Status (PRX 7000 Console Proxy)

In a PRX 7000 Console Proxy installation, the Console Dispatch Status application displays a list of MCC 7100 IP Dispatch Consoles connected to the PRX 7000 Console Proxy, along with the quality of their connection (link health). In addition, specific MCC 7100 IP Dispatch Consoles deployed outside the ASTRO® 25 Radio Network Infrastructure (RNI) can be denied access to the console proxy by adding their respective IP addresses to the Remote OP Connection Black List.

Launch the Console Dispatch Status application from the **Start** menu of the Windows operating system by selecting **Motorola** → **PRXY 7000** → **Console Status**.

To exit the application, click **File** → **Exit**. Click **X** to close the window and place an icon in the Windows taskbar. Use the **Help** menu to launch the online help or open the **About** window.

> **NOTICE:** The taskbar icon for the Console Dispatch Status running on a PRX 7000 Console Proxy is similar to the taskbar icon when running on the MCC 7100 IP Dispatch Console. See Console Dispatch Status Taskbar Icon on page 119 for customization details.

Console Dispatch Status Taskbar Icon

Use the **Console Dispatch Status** taskbar icon to monitor the Link Statistics, open the **Console Dispatch Status** window, or close (**Exit**) the application. By default, the taskbar icon does not appear in the Windows taskbar until the Console Dispatch Status application is opened and minimized. See Customizing the Console Dispatch Status Taskbar Icon on page 119 for details.

Figure 15: Console Dispatch Status Taskbar Icon
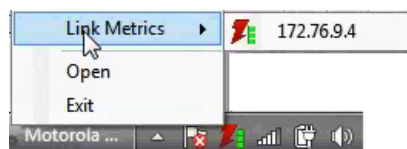
Customizing the Console Dispatch Status Taskbar Icon

Customize the **Console Dispatch Status** taskbar icon so it can appear in the taskbar notification area.

Procedure:

1 Open the Console Dispatch Status application.

2 Click **X** in the upper right-hand corner to close the application.

   This selection shows the list of application icons that can be customized to appear in the taskbar notification area.

3 In the Windows taskbar notification area, click the **Show hidden icons** arrow.

Figure 16: Windows 7 Taskbar Notification Area
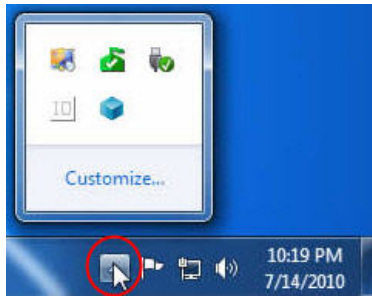
4 Select **Customize**.

5 Locate **ConsoleStatusApp** and set the behaviors to **Show icons and notifications**.

6 Click **OK**.

> **NOTICE:** Selecting **File → Exit** closes the application and removes the icon from the taskbar notification area. Clicking **X** to close the application minimizes the application as an icon in the taskbar notification area.

Remote OP Connection List

> **NOTICE:** The **Remote OP Connection List** tab appears only when the Console Dispatch Status application is launched from the PRX 7000 Console Proxy.

After connected, the Remote OP Connection List displays the IP addresses of all connected MCC 7100 IP Dispatch Consoles. In addition, the number of allowed remote connections and remaining connections is displayed in text just below the Remote OP Connection List tab.

Figure 17: Remote OP Connection List
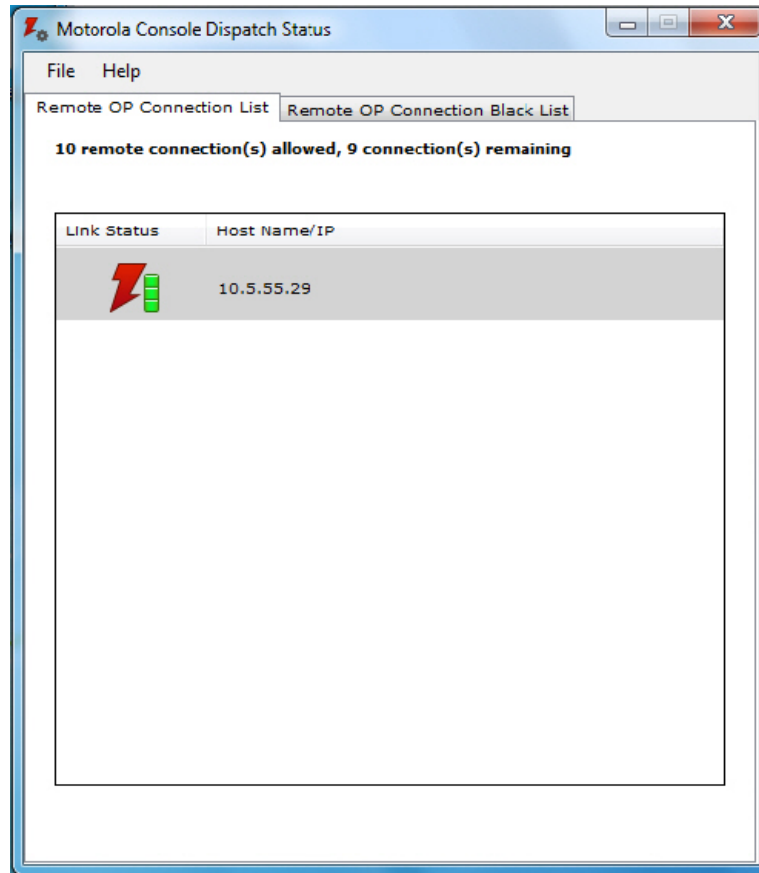
Remote OP Connection Black List

> **NOTICE:** The **Remote OP Connection Black List** tab appears only when the Console Dispatch Status application is launched from the PRX 7000 Console Proxy.

The **Remote OP Connection Black List** displays the Host Names and/or IP addresses of all MCC 7100 IP Dispatch Consoles that are not allowed access to the ASTRO® 25 Radio Network Infrastructure (RNI). From this tab, the user can Add, Edit, or Remove MCC 7100 IP Dispatch Consoles from the black list.

Figure 18: Remote OP Connection Black List
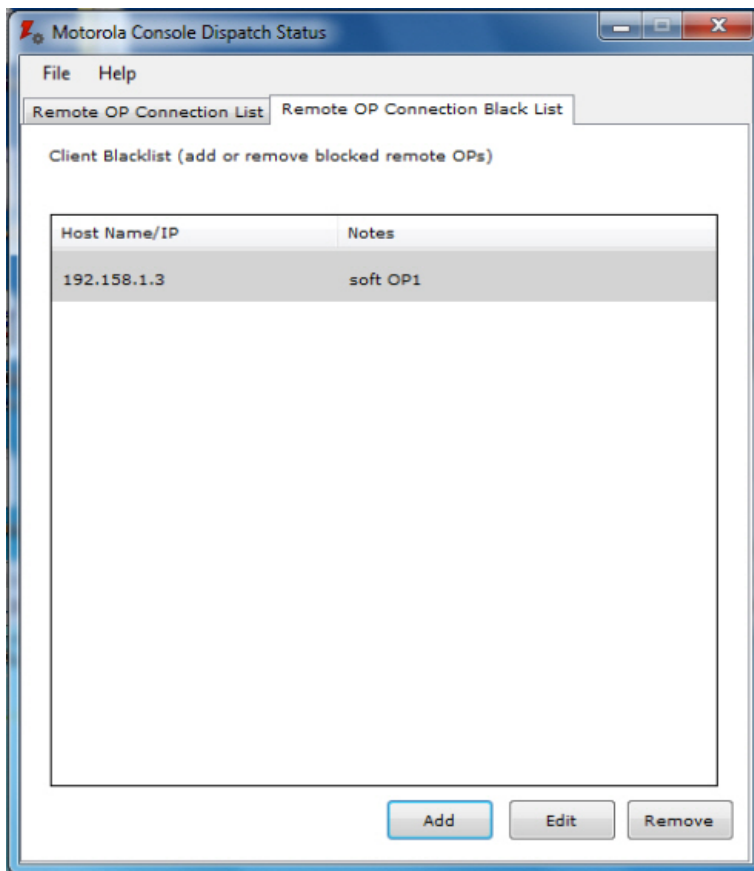
Adding a Remote MCC 7100 IP Dispatch Console to the Black List

Procedure:

1 From the Windows **Start** menu, select **All Programs** → **Motorola** → **PRXY 7000** → **Console Status**.

2 Click the **Remote OP Connection Black List** tab and click **Add**.

3 Enter the **Host Name** or **IP Address** of the remote MCC 7100 IP Dispatch Console to add to the console proxy black list.

> **IMPORTANT:** This IP address must be the ASTRO® 25 Radio Network Infrastructure (RNI) IP address for the connecting remote dispatch console and not the Customer Enterprise Network (CEN) IP address.

4 Click **Save**.

5 Restart **Elite Dispatch**.

Editing a Remote MCC 7100 IP Dispatch Console on the Black List

Procedure:

1 From the Windows **Start** menu, select **All Programs** → **Motorola** → **PRXY 7000** → **Console Status**.

2 Click the **Remote OP Connection Black List** tab.

3 Select the remote MCC 7100 IP Dispatch Console and click **Edit**.

4   Modify the **Host Name** or **IP Address** of the remote MCC 7100 IP Dispatch Console.

> **IMPORTANT:** This IP address must be the ASTRO® 25 Radio Network Infrastructure (RNI) IP address for the connecting remote dispatch console and not the Customer Enterprise Network (CEN) IP address.

5   Click **Save**.

Removing a Remote MCC 7100 IP Dispatch Console from the Black List

Procedure:

1   From the Windows **Start** menu, select **All Programs → Motorola → PRXY 7000 → Console Status**.

2   Click the **Remote OP Connection Black List** tab.

3   Select the remote MCC 7100 IP Dispatch Console and click **Remove**.

4   Click **Save**.

MCC 7100 Peripheral Configuration Tool

Use the Peripheral Configuration Tool to configure the audio input and audio output devices used by the MCC 7100 IP Dispatch Console. When launched, the tool reads all audio devices connected to the dispatch console.

Launch the Peripheral Configuration Tool from the **Start** menu of the Windows operating system by selecting **All Programs → Motorola → MCC 7100 Dispatch → Peripheral Configuration Tool**.

Figure 19: Motorola Peripheral Configuration Tool
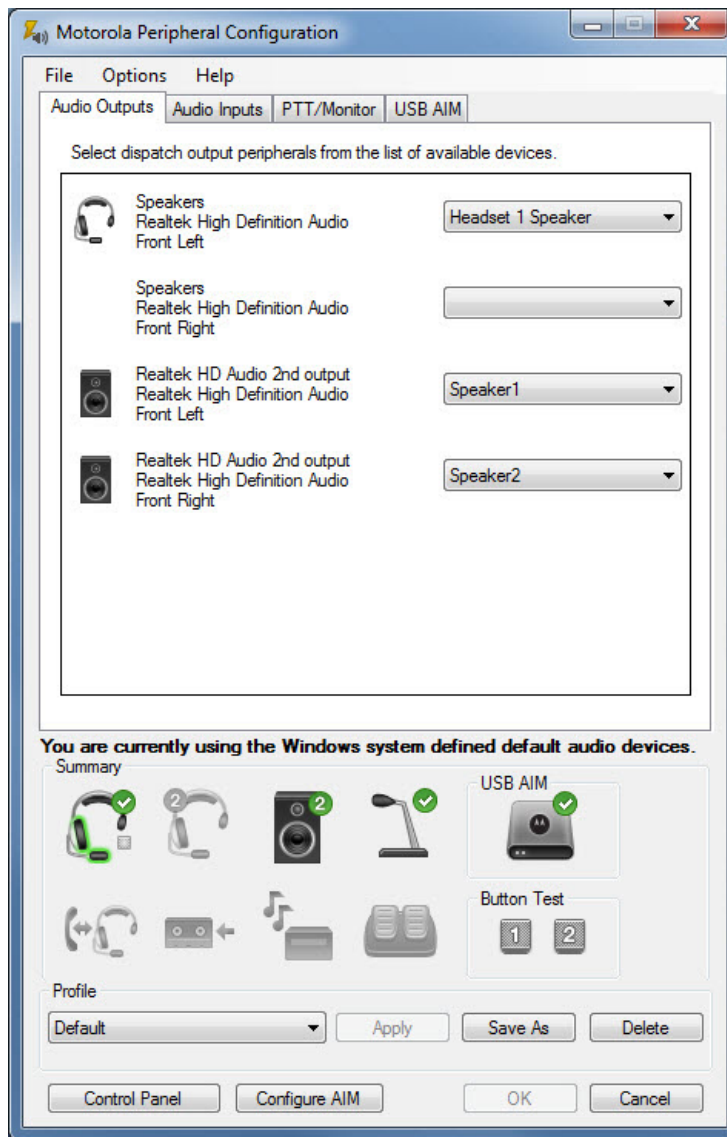
Audio Outputs Tab

The **Audio Outputs** tab displays all the audio speaker devices configured in the Windows operating system. All audio devices in this tab are speakers. They can be the internal computer speakers, external desktop speakers, or the headset speakers. The Peripheral Configuration Tool separates all available channels of an audio output device. Using the Peripheral Configuration Tool, you can selectively map or unmap the channels to audio speaker devices and make the devices available for use by the Elite Dispatch. For computers containing a special sound card that supports more than two speakers, all the speakers are available in the tool, except for any subwoofer output. The tool supports up to eight desktop speakers.

To remove a device from the list of available devices, disable the output device in the **Sound** panel of the Windows operating system. To open the **Sound** panel, click **Control Panel** in the Peripheral Configuration Tool.

Mapping and Unmapping a Speaker

To map or unmap speaker devices, change the current settings in the **Audio Outputs** tab of the Peripheral Configuration Tool. You can configure the Elite Dispatch to selectively choose which speakers to enable or disable.

Procedure:

1 From the Windows **Start** menu, select **All Programs** → **Motorola** → **MCC 7100 Dispatch** → **Peripheral Configuration Tool**.

2 Select the **Audio Outputs** tab.

   The list of speaker devices configured in the Windows operating system appears.

3 Map or unmap a speaker device by performing one of the following actions:

   • To map a speaker device, go to the drop-down list next to the device and select the speaker (channel) that you want to hear on this device.

   • To unmap a speaker device, go to the drop-down list next to the device and select the blank selection.

Figure 20: Mapping and Unmapping Speakers
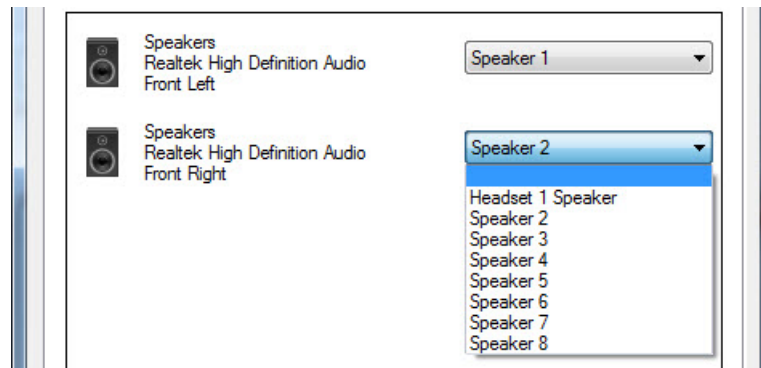
   The number in the speaker icon in the **Summary** section changes to indicate the number of mapped speakers. If you unmap a speaker from the configuration, the number in the speaker icon changes from green to yellow to indicate that all available speakers are not configured.

4 Close the Peripheral Configuration Tool by clicking **OK**.

Testing a Speaker

After you configure speaker devices in the Peripheral Configuration Tool, identify each of them by sending an audible tone to them.

Procedure:

1 From the Windows **Start** menu, select **All Programs** → **Motorola** → **MCC 7100 Dispatch** → **Peripheral Configuration Tool**.

2 In the **Audio Outputs** tab, right-click the speaker device that you want to test. Click **Test**.

Figure 21: Speaker Test
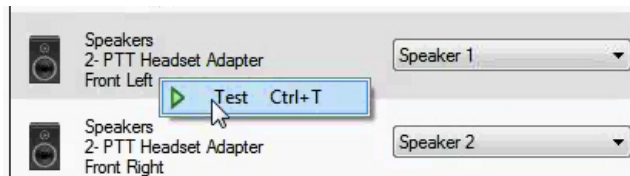
An audible tone is sent to the speaker.

3 Close the Peripheral Configuration Tool by clicking **OK**.

Configuring a non-Motorola Headset

To configure a non-Motorola headset, associate the headset speaker and the headset microphone. If the headset has a Push-to-Talk (PTT) button, you can also configure the headset PTT. You can configure the non-Motorola headset only as **Headset 1**.

Procedure:

1 From the Windows **Start** menu, select **All Programs** → **Motorola** → **MCC 7100 Dispatch** → **Peripheral Configuration Tool**.

2 Select the **Audio Outputs** tab.

3 From the drop-down list next to the device that you want to configure as your headset speaker, select **Headset 1 Speaker**.

The ear piece speaker on the headset icon in the **Summary** pane is highlighted.

4 Select the **Audio Inputs** tab.

5 From the drop-down list next to the device that you want to configure as your headset microphone, select **Headset 1 Microphone**.

The microphone on the headset icon in the **Summary** pane is highlighted.

6 If the headset contains a PTT button, select the **PTT/Monitor** tab.

7 From the drop-down list next to the device that you want to configure as your headset PTT, select **Headset 1 PTT**.

8 Save the profile:

- To save the changes to the existing profile, select **Apply**.
- To save the changes as a new profile, select **Save As**.

9 Close the Peripheral Configuration Tool by clicking **OK**.

Audio Inputs Tab

The **Audio Inputs** tab displays all the audio microphone devices configured in the Windows operating system.

To remove a device from the list of available devices, disable the input device in the **Sound** panel of the Windows operating system. To open the **Sound** panel, click the **Control Panel** button in the Peripheral Configuration Tool.

Mapping and Unmapping a non-Motorola Desktop Microphone

Map or unmap microphone devices by changing the current settings in the **Audio Inputs** tab.

Procedure:

1 From the Windows **Start** menu, select **All Programs** → **Motorola** → **MCC 7100 Dispatch** → **Peripheral Configuration Tool**.

2 Select the **Audio Inputs** tab.

3 Map or unmap a microphone device by performing one of the following actions:

- To map a microphone device, from the drop-down list next to the device, select **Desktop Microphone**.

- To unmap a microphone device, from the drop-down list next to the device, select the blank selection.

> **NOTICE:**
> Only one desktop microphone can be configured for the MCC 7100 IP Dispatch Console.
>
> If you use a non-Motorola desktop microphone and either a non-Motorola headset or the Motorola-standard headset is mapped in the Peripheral Configuration Tool and connected to the dispatch console, you cannot transmit by using the desktop microphone. Use the headset microphone.

4 Close the Peripheral Configuration Tool by clicking **OK**.

PTT/Monitor Tab

The **PTT/Monitor** tab displays a list of dispatch Push To Talk (PTT) devices connected to the computer. The tab supports USB foot switches, USB headsets with PTT functionality, and joysticks.

Configuring a non-Motorola USB Footswitch

Configure a USB footswitch as a Push-to-Talk (PTT) in the Peripheral Configuration Tool.

Prerequisites: Connect the USB footswitch to the computer and install all the necessary USB footswitch drivers.

Procedure:

1 From the Windows **Start** menu, select **All Programs** → **Motorola** → **MCC 7100 Dispatch** → **Peripheral Configuration Tool**.

2 Select the **PTT/Monitor** tab.

3 From the drop-down list next to the device that you want to use as the PTT device, select **Footswitch**.

The footswitch icon in the **Summary** pane is highlighted.

4 Optional: Test the PTT device by using the test buttons in the **Button Test** pane.

You can use the test buttons only to test non-Motorola PTT devices. The buttons are not available for the Motorola PTT devices connected to the USB Audio Interface Module.

5 Save the profile:

- To save the changes to the existing profile, select **Apply**.

- To save the changes as a new profile, select **Save As**.

6 Close the Peripheral Configuration Tool by clicking **OK**.

USB AIM Tab

The **USB AIM** tab contains a list of Motorola peripherals that can be connected to the USB Audio Interface Module (USB AIM) device. The list is visible only when the USB AIM device is connected to the MCC 7100 IP Dispatch Console. When the device is connected to the console computer, all the Motorola peripherals are listed, whether they are connected to the USB AIM or not. By using the **USB AIM** tab, you can map or unmap the peripherals.

Mapping and Unmapping Motorola Peripherals

Perform this procedure to map or unmap the peripherals connected to the USB Audio Interface Module device (USB AIM).

Prerequisites: Connect the USB AIM to the MCC 7100 IP Dispatch Console computer.

Procedure:

1   From the Windows **Start** menu, select **All Programs** → **Motorola** → **MCC 7100 Dispatch** → **Peripheral Configuration Tool**.

2   Map the peripherals by performing one of the following actions:

If…	Then…
If you want to map all the Motorola peripheral devices,	click **Configure AIM**.
If you want to map or unmap a single Motorola peripheral device,	perform the following actions: a Select the **USB AIM** tab. b For the peripheral that you want to map or unmap, perform one of the following actions: • To map a peripheral device, go to the drop-down list next to the device and select it from the list. • To unmap a peripheral device, go to the drop-down list next to the device and select the blank selection.

Figure 22: Mapping and Unmapping the Motorola Peripherals
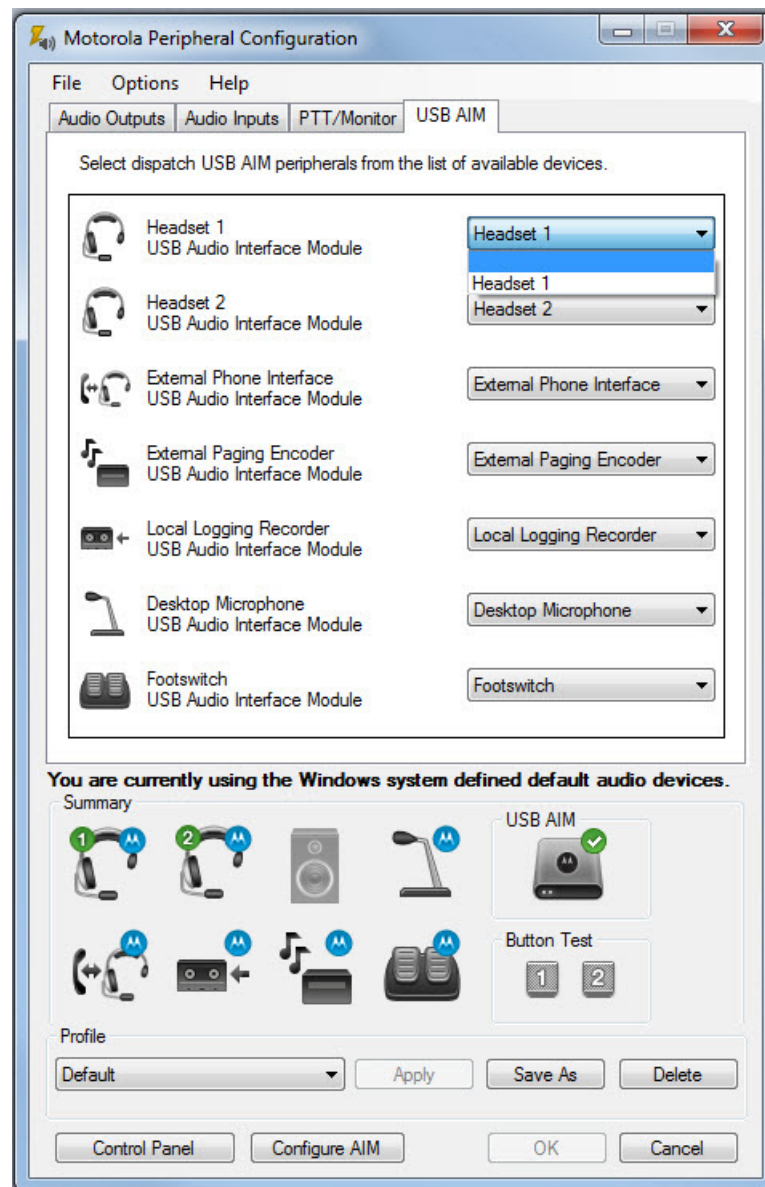
NOTICE:
The External Phone Interface operates only with the Motorola headset connected to the USB AIM. Before you use the External Phone Interface, ensure that the Motorola headset is mapped in the Peripheral Configuration Tool and connected to the USB AIM device.

You can use up to two Motorola headsets. If you want to use a Motorola headset together with a non-Motorola headset, map the Motorola headset as **Headset 2**. You can map the non-Motorola headset only as **Headset 1**.

3   Close the Peripheral Configuration Tool by clicking **OK**.

Peripheral Configuration Summary

The **Summary** pane consists of icons that represent the peripheral device types that you can map to the MCC 7100 IP Dispatch Console, the USB Audio Interface Module (USB AIM) icon that represents the state of the USB AIM, and the **Button Test** pane that contains two buttons to test the Push-to-Talk

(PTT) function of non-Motorola PTT devices. The peripheral device icons indicate that the devices are mapped but not necessarily connected.

Figure 23: Peripheral Configuration Summary
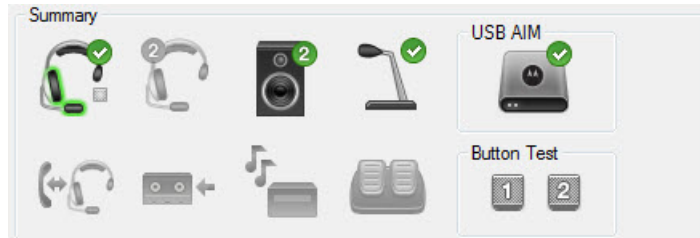
The peripheral devices that you map to the MCC 7100 IP Dispatch Console can be Motorola and non-Motorola peripherals. To map the Motorola peripherals, you need the USB AIM. You connect the peripherals to the USB AIM device. After you connect the USB AIM device to the dispatch console computer and configure it, all the mapped Motorola peripherals are displayed in the **Summary** pane, whether they are connected or not. All the mapped Motorola peripherals are indicated with the Motorola logo.

Figure 24: Peripheral Configuration Summary – Motorola peripherals
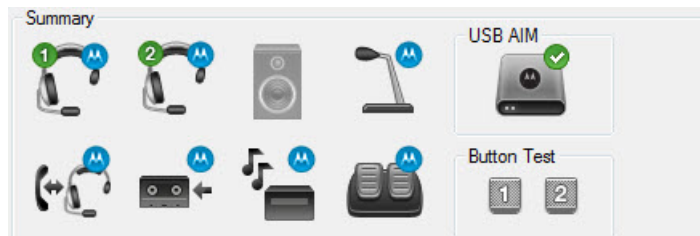
The included graphical icons are for two headsets, speakers, a microphone, an external phone interface, a local logging recorder, an external paging encoder, and USB foot pedal switches. The graphical icons are dynamically updated as each audio device is mapped. The graphical icons for headset 2, the external phone interface, local logging recorder, and external paging encoder always represent Motorola devices that can connect only to the USB AIM device. The bookshelf speaker icon indicates the number of non-Motorola speakers currently mapped. The icons for headset 1, desktop microphone, and USB foot pedal switches can represent either Motorola or non-Motorola peripherals depending on what is mapped. Motorola headsets are either mapped or unmapped as single devices. For a non-Motorola headset that can be mapped as headset 1, you can configure the speaker, microphone, and PTT switch independently. When only a speaker or microphone is mapped for the non-Motorola headset, a red X appears instead of a green check mark on the headset graphical icon.

Peripheral Configuration Profile

Use the **Profile** pane for managing audio profiles. The user can select from the list of existing profiles, apply changes to existing profiles, create and save a new profile, or delete existing profiles.

> **NOTICE:**
> When trying to save a profile in which no device is mapped, an error appears.
>
> When trying to save a profile in which a headset is configured incorrectly, for example, a headset speaker is mapped and no headset microphone is mapped, an error appears.
>
> Do not use a single peripheral configuration profile for more than one operator position.
>
> If using multiple Windows user accounts on a dispatch console operator position, do not use a single peripheral configuration profile for more than one of these user accounts. Instead, create separate profiles for each user account. Each time you change to a different Windows user account, run the Peripheral Configuration Tool and select a profile dedicated to the Windows account that you selected.

The default profile uses the current audio output and input devices from the Windows operating system. If no USB audio devices are connected, the internal speakers and microphones are used. If a USB device, such as a headset, is connected, the speaker and microphone of this device are used.

Any changes to the default devices in the Windows operating system cause an immediate change in the Peripheral Configuration Tool and in the Elite Dispatch, if running. For example, a change to the default microphone immediately causes the Elite Dispatch to switch to the new default device.

Creating a Profile with non-Motorola Peripherals

Create and use custom profiles to allow users to selectively choose which audio input and output devices to use.

Procedure:

1 From the Windows **Start** menu, select **All Programs** → **Motorola** → **MCC 7100 Dispatch** → **Peripheral Configuration Tool**.

2 In **Audio Outputs**, map the speaker devices.

3 In **Audio Inputs**, map the microphone devices.

4 In the **PTT/Monitor** tab, map the push-to-talk devices.

5 Save the profile by performing the following actions:

    a In the **Profile** pane, click **Save As**.

    b In the **Save As** window, enter the name for the profile. Click **Save**.

6 Close the Peripheral Configuration Tool by clicking **OK**.

> **NOTICE:** If default devices switch in the Windows operating system, no notification is made. Only the configured devices in the custom profile are used. If the devices are disconnected, audio is lost from those devices. Default mode automatically switches to devices configured in the Windows operating system.

Customizing a Profile with Motorola Peripherals

Perform this procedure to customize a profile that uses the Motorola peripherals by unmapping the Motorola peripherals or replacing them with non-Motorola peripherals. The Motorola peripherals that you can replace with non-Motorola peripherals are headset 1, desktop microphone, and footswitch.

Prerequisites: Connect and configure the USB Audio Interface Module (USB AIM). See Configuring USB Audio Interface Module on page 112.

Procedure:

1 Perform one of the following actions:

If…	Then…
If you want to unmap a Motorola peripheral,	**a** Select the **USB AIM** tab. **b** From the drop-down list next to the device that you want unmap, select the blank selection.
If you want to replace the Motorola headset 1 with a non-Motorola peripheral,	**a** Select the **Audio Outputs** tab. **b** From the drop-down list next to the device that you want to configure as your headset speaker, select **Headset 1 Speaker**. **c** Select the **Audio Inputs** tab. **d** From the drop-down list next to the device that you want to configure as your headset microphone, select **Headset 1 Microphone**. **e** Select the **PTT/Monitor** tab. **f** From the drop-down list next to the device that you want to configure as your headset Push-to-Talk (PTT), select **Headset 1 PTT**.
If you want to replace the Motorola desktop microphone with a non-Motorola peripheral,	**a** Select the **Audio Inputs** tab. **b** From the drop-down list next to the device that you want map as your desktop microphone, select **Desktop Microphone**.
If you want to replace the Motorola footswitch with a non-Motorola peripheral,	**a** Select the **PTT/Monitor** tab. **b** From the drop-down list next to the device that you want map as your footswitch, select **Footswitch**.

2 Save the profile:

- To save the changes to the existing profile, select **Apply**.
- To save the changes as a new profile, select **Save As**.

3 Close the Peripheral Configuration Tool by clicking **OK**.

Deleting a Profile

Perform this procedure to selectively choose which profiles to remove from the tool, or delete all profiles except for the currently active profile that does not appear in the list of profiles to delete.

Procedure:

1 From the Windows **Start** menu, select **All Programs → Motorola → MCC 7100 Dispatch → Peripheral Configuration Tool**.

2 In the **Profile** pane, click **Delete**.

3 In the **Select Profile(s) to Delete** window, perform one of the following actions:

- To remove all the profiles except for the currently active profile, select the **Select All** check box.
- To remove a single profile, select the check box next to it.

4 Click **Delete**.

5 Confirm the deletion by clicking **OK**.

Control Panel Button

When the **Audio Outputs** tab, the **Audio Inputs** tab, or the **USB AIM** tab is selected, selecting **Control Panel** opens the Window **Sound** panel. When the **PTT/Monitor** tab is selected, selecting **Control Panel** opens the **Game Controller** window. The default audio devices currently configured in the Windows operating system are shown both in the **Sound** panel and in the Peripheral Configuration Tool.

Figure 25: Sound and Game Controller in the Windows operating system
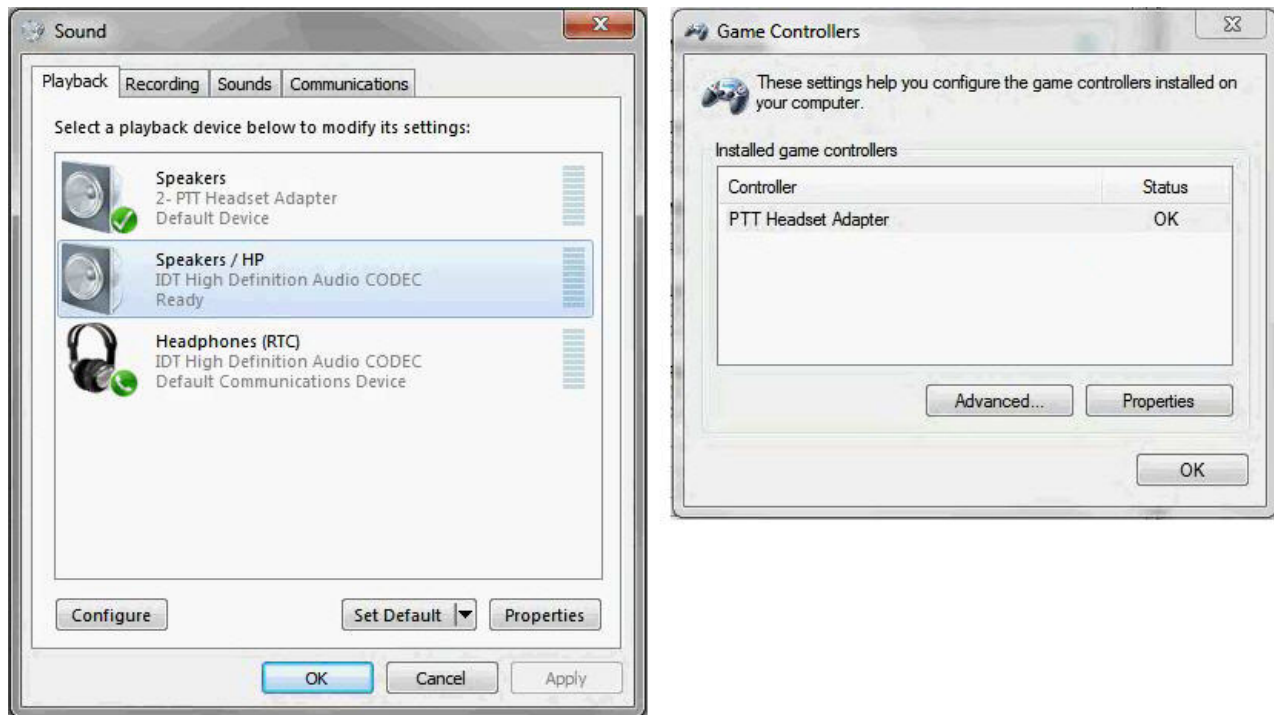
The **Playback** and **Recording** tabs in the **Sound** panel are similar to the **Audio Outputs** and **Audio Inputs** tabs in the Peripheral Configuration Tool, respectively. The only difference is that only one speaker is shown in the **Sound** panel whereas two speakers are shown and configurable in the Peripheral Configuration Tool. This separation of speakers allows each speaker to be treated as a separate channel for use by the Elite Dispatch.

> **NOTICE:** To prevent speakers or microphones configured in the Windows operating system from appearing in the **Audio Outputs** and **Audio Inputs** tabs of the Peripheral Configuration Tool, disable them from the **Sound** panel.

Motorola Peripherals – Audio Gain

It is important to adjust the audio gain for the peripherals so that the communication can be effective.

Adjust the audio gain for all the Motorola peripherals:

- External Telephone Interface
- Local Logging Recorder
- External Paging Encoder
- Two pairs of the Motorola headsets
- Motorola desktop microphone

The Motorola peripherals are connected to the USB Audio Interface Module (USB AIM) device.

To change the audio gain for each Motorola peripheral, adjust the audio gain parameters in the Provisioning Manager or Configuration Manager application. See the *Provisioning Manager* manual or the *Configuration Manager* manual.

> **NOTICE:** If you change the audio gain for the Motorola peripherals locally in the Windows operating system, the changes are temporary. When you edit the profile in the Peripheral Configuration Tool, restart the Elite application, or disconnect and connect the USB AIM device, the previous settings are restored.

Configuring USB Audio Interface Module

After connecting the USB Audio Interface Module (USB AIM) to the MCC 7100 IP Dispatch Console, it is operational but not configured. To use the peripherals connected to the USB AIM, create a configuration in the Peripheral Configuration Tool application installed on the MCC 7100 IP Dispatch Console computer.

To use the peripherals connected to the USB AIM, create a configuration in the Peripheral Configuration Tool.

Prerequisites:
Verify the state of the LEDs on the front of the device. If only the green LED is on, the device is fully operational and you can continue. If the state of the LEDs is different, resolve the issue. See USB Audio Interface Module Indicators on page 114

Ensure that the MCC 7100 IP Dispatch Console computer has the Windows 7 Service Pack 1 installed.

Procedure:

1 From the Windows **Start** menu, select **All Programs** → **Motorola** → **MCC 7100 Dispatch** → **Peripheral Configuration Tool**.

   The application automatically detects the USB AIM connected to the dispatch console. In the **Summary** pane, the USB AIM status is `Connected`. A default configuration or a configuration created by a user is displayed. If a default configuration is displayed, the mapped devices are non-Motorola peripherals connected to the dispatch console or Motorola-standard peripherals connected to the USB AIM. If the mapped peripherals are Motorola-standard, the Motorola logo appears for them.

2 Click **Configure AIM**.

   > **NOTICE:** The External Phone Interface operates only with the Motorola-standard headset connected to the USB AIM. If using the External Phone Interface, keep the Motorola-standard headset mapped the Peripheral Configuration Tool and connected to the USB AIM.

   In the **Summary** pane, the appropriate graphical icons are highlighted and the Motorola logo appears for the Motorola-standard peripherals connected to the USB AIM.

3 If the speakers are not configured, perform the following actions:

   a Navigate to the **Audio Outputs** tab.

   b Map the MCC 7100 IP Dispatch Console speakers to physical speakers connected to the dispatch console computer by selecting them from the drop-down lists available for each physical speaker.

4 In the **Profile** pane, click **Save As**.

5 In the **Save As** window, enter the name of the new configuration. Click **Save**.

   The application automatically selects the new configuration as the currently used configuration.

Upgrading the USB Audio Interface Module Software

If you experience problems with the USB Audio Interface Module (USB AIM), the USB-AIM may contain an older or unsupported software version. Perform this procedure to upgrade the software.

Prerequisites: Ensure that you do not have any active calls. During the upgrade of the USB AIM software, the audio peripherals connected to the device are not usable. Additionally, the USB AIM device restarts during the upgrade process and all the operations performed by the USB AIM are terminated.

Procedure:

1 From the Windows **Start** menu, select **All Programs → Motorola → MCC 7100 Dispatch → Peripheral Configuration Tool**.

2 From the **File** menu, select **USB AIM Software Update**.

3 In the firmware information window, select **Update**.

4 In the warning window, click **Yes**.

   The upgrade process takes a few minutes. After the upgrade process finishes, the USB AIM restarts. In the firmware information window, you receive a message about a successful software upgrade.

5 Click **OK**.

Troubleshooting USB Audio Interface Module Upgrade Issues

If you were unable to upgrade the USB Audio Interface Module (USB AIM), the reason can be a lost USB connection. If you encountered any upgrade issues, use the following scenario to retry to upgrade the USB AIM software.

Procedure:

1 Unplug the USB cable from the USB AIM and from the MCC 7100 IP Dispatch Console computer, wait a while, and plug the cable in again.

2 Retry to upgrade the USB AIM software in a typical way.

3 Restart the USB AIM device by unplugging the power supply, waiting a while, and plugging it in again.

   The green and red LEDs on the front of the device are on for a while. Then the red LED goes off and the green LED stays on.

4 Retry to upgrade the USB AIM software in a typical way.

USB AIM Status Icon

From the **Summary** pane of the Peripheral Configuration Tool, use the USB Audio Interface Module (USB AIM) status icon to verify the state of the device. The icon shows one of the three possible states of the device.

     The USB AIM is connected and fully operational.

Table continued…
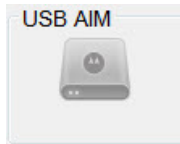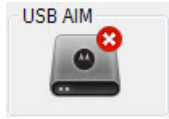
	The USB AIM is not connected.
	The USB AIM is connected but not operational. Hover over the icon to learn additional details about the problem.

USB AIM Device Information

Retrieve details about your USB Audio Interface Module (USB AIM) device using the **USB AIM Device Information** window in the Peripheral Configuration Tool application.

The window contains the following information:

- Firmware version
- Kit number
- Tanapa number

Accessing the USB-AIM Device Information
In the main menu of the Peripheral Configuration Tool application, click **File → USB AIM Device Information**.

> **NOTICE:** If the Peripheral Configuration Tool cannot access the information about the USB AIM, an error appears in the **USB AIM Device Information** window. If you encounter this issue, close the window and unplug the USB cable from the USB AIM and from the MCC 7100 IP Dispatch Console computer. Wait a while, plug the cable in, and reopen the **USB AIM Device Information** window.

Copying the USB AIM Device Information
In the **USB AIM Device Information** window, click **Copy to clipboard**.

Chapter 6

Instant Recall Recorder

Welcome to the Instant Recall Recorder

To access items from the contents pane, click **Contents**. In the contents pane, open topics by expanding the title nodes.

To find a specific word or phrase, click **Search**. In the search box, type a word or phrase that you want to find. Press **ENTER**.

Instant Recall Recorder

The Instant Recall Recorder (IRR) is a licensed application installed as part of the MCC 7100 IP Dispatch Console software. The IRR software makes it possible to record audio traffic on the dispatch console on which it is installed. Using the IRR application, the dispatch operator can replay the recorded audio traffic to, for example, verify a specific piece of information.

The IRR application requires no additional installation tasks. To make your dispatch operators able to replay the calls that took place on their dispatch consoles, order the number of IRR licenses you need. When you follow the standard procedure for installing the MCC 7100 IP Dispatch Console software, the IRR software is installed automatically. After you place the IRR license files in the right folder on the dispatch console position, the dispatch operator can start using the software.

After you install the MCC 7100 IP Dispatch Console software, you can start the application directly from the Windows operating system or from the Elite Dispatch application.

Before you start using the IRR, use the default settings or perform a short and easy configuration in the application to adjust it your specific needs. For example, you can specify the audio types that you want to record, the time after which the IRR application deletes the stored audio, and the peripheral in which you want to play back the recorded audio. The configuration is the only action that you perform to be able to easily manage and play back the calls recorded on your MCC 7100 IP Dispatch Consoles.

Audio Types Recorded by the Instant Recall Recorder Application

The Instant Recall Recorder (IRR) application can record four audio types that appear on the dispatch console position on which it is installed. Depending on the configuration, the IRR application records one or more types of audio.

Recorded Audio Types

The IRR application can record the following audio types:

- Inbound audio from the currently selected channels
- Outbound audio from the microphone to the selected channels
- Outbound audio from the microphone to the unselected channels
- Tones generated by the dispatch console that appear in the speakers of the dispatch console

The IRR application can record the outbound audio from the dispatch console microphone, the audio that appears on selected resources, and any locally generated tones. Depending on the configuration, the IRR application records only inbound audio on the selected resources or more audio types. To select one of the two available configurations, use the **Configuration** dialog.

Receive Audio

The IRR application records only the inbound audio on the selected resources which is the audio that appears in the headset or selected speakers of the dispatch console.

Receive and Transmit Audio

The IRR application can record all the audio types within the scope of the IRR functionality.

> **NOTICE:** The types of audio that the IRR application records when you specify receive and transmit audio as the recording source depends on the platform configuration in the Provisioning Manager or Configuration Manager.

Audio Types That Are Not Recorded

The IRR application can record defined types of audio. The IRR application does not record the following types of audio:

- Inbound audio on the unselected resources which is the audio that appears in the unselected speakers of the dispatch console.

- Outbound audio other than the audio from the dispatch console microphone. For example, it does not record outbound audio the dispatch console retransmits from other consoles or subscriber radios.

- Outbound patch audio.

  > **NOTICE:** If the dispatch console is configured in the Provisioning Manager or Configuration Manager to record inbound audio from the selected channels, it can record the inbound patch audio that comes from a patch resource selected.

- Audio from patch resources that are not selected. Although entries for these resources can appear in the call list, the IRR application does not record audio for them as it is outbound audio the dispatch console retransmits to other resources in the patch.

Audio Only Records

The IRR application can record private calls between the console position and subscribers or other dispatch consoles.

However, in the case of inbound private calls, the dispatch console opens all audio paths before the dispatch console or the other party key up. As the result, for inbound private call entries, the IRR application cannot display all the details that it normally displays for other calls.

As the result, the IRR application displays the call information in the following way:

- No specific Unit Alias appears. Instead, you see an Audio Only entry.

- No unit ID and Channel Alias appears.

- Start Time, End Time, and Duration data appear as for other calls.

After either private call party keys up, a new entry appears in the call list. The new entry displays all the details in the standard way.

Configuring the Instant Recall Recorder Application

Before you start using the Instant Recall Recorder (IRR), adjust the application to your needs. For example, specify the audio types that you want to record, the retention period, and the peripheral in which you want to play back the recorded audio.

Procedure:

1 Start the IRR application.

   See .

2   From the main menu, select **Settings → Configuration**.

3   From the **Configuration** dialog, in the **Recording Source** section, specify the audio type that you want to record.

> 📝 **NOTICE:** Before you decide about the recorded audio type, learn more about the audio types the IRR application records and about the audio types that are *not* within the scope of the IRR functionality. See Audio Types Recorded by the Instant Recall Recorder Application on page 141.

  • To record the inbound calls on the selected resources only, select **Receive Audio**.

  • To record more audio types, select **Receive and Transmit Audio**.

4   In the **Storage Options** section, specify where you want to store the recorded audio:

  a   Click **Browse**.

  b   In the **Browse For Folder** window, navigate to the folder in which you want to store the audio.

  The default location for storing the IRR audio is `C:\Users\`*`username`*`\AppData\Roaming\Motorola MCC 7100\IRRSession`.

5   Decide whether you want to make it possible to save calls in a separate `.wav` file:

  • To make the **Save to File** active, select the **Save to File Enabled** check box.

  • To make the **Save to File** inactive, clear the **Save to File Enabled** check box.

6   Decide whether you want the location in which you store the recorded audio purged each time you exit the IRR application:

  • If you want the IRR audio purged each time you exit the IRR application, select the **Purge on Exit** check box.

  • If you want to keep the IRR audio after you exit the IRR application, clear the **Purge on Exit** check box.

7   Decide the time after which the IRR application deletes the stored audio by using the **Retention Period** slider.

  By moving the thumb of the **Retention Period** slider, you change the values in the **Record Retention** and **Disk Space Used** fields. If it is more convenient, you can use the fields instead of the slider.

8   From the **Output Devices** drop-down list, select the peripheral in which you want to hear the played back IRR audio.

9   Save changes by clicking **OK**.

Instant Recall Recorder Basic Operations

Before you start using the Instant Recall Recorder (IRR) application, learn how to perform basic operations and about the options it offers, especially about the customization options.

Starting the Instant Recall Recorder Application

You can start the Instant Recall Recorder (IRR) application directly from the Windows operating system or from the Elite Dispatch application.

Procedure:

  Start the IRR application by performing one of the following actions:

  • To start the application from the Windows operating system, from the **Start** menu, select **All Programs → Motorola → MCC 7100 Dispatch → Instant Recall Recorder**.

- To start the application from the Elite Dispatch, in the toolbar, click the **Open IRR** button

  .

Closing the Instant Recall Recorder Application

If the **Start Instant Recall Recorder with Elite** option is enabled in the Elite Dispatch configuration, the Instant Recall Recorder (IRR) closes automatically always when you exit the Elite Dispatch application. If you use a configuration in which this option is not enabled, or want to exit the IRR without closing the Elite Dispatch application, use the following procedure.

Procedure:

From the IRR main menu, select **File → Exit**.

Fixing the Instant Recall Recorder Window on the Top of the Desktop

If you pin the Instant Recall Recorder (IRR) window and then use other applications, the IRR windows does not hide under the windows of these applications, but stays on the top of your desktop.

Procedure:

In the IRR title bar, click the **Pin the window** button .

Instead, from the IRR main menu, you can select **View → Stay on Top**.

The IRR window gets fixed on the desktop and the **Pin the window** button changes into the **Unpin the window** button .

Switching the Instant Recall Recorder Window to the Compact Mode

The compact mode is a window view in which only playback buttons, the volume control, and optionally, the progress bar are displayed.

Procedure:

1 In the menu bar, click **Compact Mode** .

   Instead, from the IRR main menu, you can select **View → Compact Mode**.

2 Optional: Expand the Call List section by clicking the **Call List** icon .

3 To deactivate the compact mode, click **Expanded Mode** .

Expanding and Collapsing Sections in the Instant Recall Recorder Window

You can adjust the appearance of the Instant Recall Recorder (IRR) window to your needs by collapsing the sections that you do not use or use rarely. By default, all the sections in the IRR window are expanded.

Procedure:

Expand or collapse sections in the IRR window by performing one of the following actions:

- To collapse a section, in the upper-right corner of the section, click the **Hide** icon .

- To expand a collapsed section, on the right side of the IRR window, click the appropriate **Expand** icon .

Instead, you can collapse and expand sections by selecting or clearing the section check boxes in the **View** menu.

Managing Detail Columns in the Instant Recall Recorder Call List

The call list section consists of six columns that contain details about the recorded calls, for example, the information about the duration of the calls and the aliases and IDs of the units that took part in the calls. You can adjust the call list by changing the sequence of the columns and hiding the columns that you do not need.

Procedure:

Adjust the call list to your needs by performing the following actions:

If…	Then…
If you want to change the sequence of the columns in the call list,	click the header of column that you want to move and drag it to a new position.
If you want to hide a column that you do not use,	perform the following actions: a Right-click any column header in the call list. b In the **sensitive** menu, clear the check box next to the name of the column that you want to hide.

Playing Back Calls in the Instant Recall Recorder Application

Use the Instant Recall Recorder (IRR) application to play back the recorded calls. During a single playback session, you can play back single calls, multiple calls, or portions of calls.

Procedure:

1 Start the IRR application.

See .

2 Play back the desired audio portion by performing one of the following actions:

If…	Then…
If you want to play back a single call,	perform the following actions: a In the call list, highlight the call that you want to play back. b Click **Play**.
If you want to play back multiple calls,	perform the following actions: a In the call list, select the check boxes for the calls that you want to play back. b Click **Play**.
If you want to play back a call from somewhere in the middle,	perform the following actions: a In the call list, highlight the call that you want to play back. b In the sound visualization section, double-click the waveform in the place from which you want to start playing back the call. Instead, you can move the thumb in the progress bar. c Click **Play**.

If…	Then…
If you want to play back a portion of a call,	perform the following actions: a In the call list, highlight the call that you want to play back. b In the sound visualization section, highlight the audio portion that you want to play back. You cannot highlight an audio portion that is shorter than 50 ms. c Click **Play**.

3 If you want the audio portion continuously repeated, click **Turn Repeat On** .

4 If you want to play back a previous or the next call from the call list, perform one of the following actions:

- If you want to play back a call that is one position higher than the call or calls that you selected, click **Rewind**.

- If you want to play back a call that is one position lower than the call or calls that you selected, click **Fast Forward**.

Filtering Calls in the Instant Recall Recorder Application

If you want to reduce the number of calls on the Instant Recall Recorder (IRR) call list, you can filter for specific information.

Procedure:

1 In the IRR call list, click the **Filter** icon next to the value according to which you want to filter.

Instead, you can access the filters by using the **View** menu.

2 In the **filter** window, enter the required information.

See .

3 Activate the filter by clicking **Filter**.

A box with the filter details appears above the call list.

4 Deactivate the filter by clicking the exit icon in the box with the filter details.

Call Filters in the Instant Recall Recorder Application

If you want to reduce the number of calls on the Instant Recall Recorder (IRR) call list, you can filter for specific information by using one of the six filters available in the IRR application.

The filters available in the IRR correspond with the detail columns in the call list.

Unit Alias

Use to limit the number of entries on the call list to calls with a unit that has a specific unit alias. To use this filter, enter the whole unit alias that you look for, a string of characters from this unit alias, or a specific character from this unit alias.

Unit ID

Use to limit the number of entries on the call list to calls with a unit that has a specific unit ID or calls with unit IDs that suit the range that you specify. To use this filter, enter the whole unit ID that you look for or specify the minimum and maximum unit ID in the range.

Channel Alias

Use to limit the number of entries on the call list to calls that took place on a channel with a specific alias. To use this filter, enter the whole channel alias that you look for, a string of characters from this unit alias, or a specific character from this unit alias.

Start Time

Use to limit the number of entries on the call list to calls that took place within a specific range of time. To use this filter, specify the range of time by setting the start time and the end time of the call.

End Time

Use to limit the number of entries on the call list to calls that took place a specific time ago. Specify the time that elapsed from the call or calls that you look for in hours, minutes, or seconds or by using all the values. You can also enter the specific time when the call or calls ended.

Duration

Use to limit the number of entries on the call list to calls of a specific duration. To use the filter, specify the minimum and maximum duration of the call or calls that you look for.

Sorting Calls in the Instant Recall Recorder

To sort calls in the call list of the Instant Recall Recorder (IRR) application, click the header of column according to which you want to sort the calls.

Procedure:

Sort the calls in the call list by performing one of the following actions:

- To sort the calls in the ascending order, click the header of the column according to which you want to sort.

- To sort the calls in the descending order, double-click the header of the column according to which you want to sort.

Rewinding and Fast Forwarding Calls in the Instant Recall Recorder Application

If you play back a call and want to omit a specific portion or hear it once again, use the Instant Recall Recorder (IRR) fast-forward and rewind options.

Procedure:

Rewind or fast forward the played back audio by performing one of the following actions:

- To rewind a played back call, click and hold the **Rewind** button.

- To fast forward a played back call, click and hold the **Fast Forward** button.

Instead of the **Rewind** and **Fast Forward** buttons, you can drag the thumb of the progress bar to the left or to the right.

Changing the Playback Speed in the Instant Recall Recorder Application

If listening to a call at lower or higher speed can help you retrieve the information you need, adjust the playback speed to your.

Procedure:

1 Change the playback speed by performing one of the following actions:

- To decrease the playback speed to 50 percent of the original call speed, under the speed slider, click **1/2**.

- To increase the playback speed to 200 percent of the original call speed, under the speed slider, click **2**.
  - To gradually change the playback speed, in the speed slider, click to the left or to the right of the thumb.

2 To set the playback speed to the original call speed, click **1** under the speed slider.

Modifying the Playback Volume and Playback Quality in the Instant Recall Recorder Application

Use the mechanisms available in the Instant Recall Recorder (IRR) application to adjust the volume and improve the quality of the played back calls. To adjust the volume, use a standard volume slider or enable the Automatic Gain Control (AGC). To improve the playback quality, use the noise reduction option.

Procedure:

- To change the volume of the played back call, perform one of the following actions:
  - To gradually decrease or increase the volume, in the **Volume** slider, click to the left or to the right of the thumb.
  - To set the volume to a specific volume, click and drag the thumb of the **Volume** slider.

- To mute the call, click the **Mute** icon .

- To level out the volume of a call for which the signal strength changes, set **Automatic Gain Control** to **On**.

- To reduce the irrelevant noise, set **Noise Reduction** to **On**.

Zooming In and Zooming Out Waveform in the Instant Recall Recorder Application

To see more details for the call that you play back, zoom in on the waveform.

When and where to use: By default, the whole call audio is visible in the waveform in the **Sound Visualization** section of the Instant Recall Recorder (IRR). You can zoom in and zoom out on a call when you play it back or just before you start playing it back. In the described scenario, you set the zoom options before you start playing the call.

Procedure:

1 In the call list, highlight the call that you want to play back.

2 In the **Sound Visualization** window, set the zoom options by using the **Zoom In** and **Zoom Out** icons.

3 Click **Play**.

4 To restore the default waveform view, click the **Zoom Out** icon until it becomes inactive.

Saving Calls to a File in the Instant Recall Recorder Application

In the Instant Recall Recorder (IRR) application, you can save a specific call or multiple calls from the call list to a `.wav` file in any localization that you specify.

Prerequisites: Enable the **Save to File** option in your IRR application:

1 From the main menu, select **Settings** → **Configuration**.

2 In the **Configuration** dialog, select the **Save to File Enabled** check box.

Procedure:

    1 Select the calls that you want to save:

If…	Then…
If you want to save a single call,	perform the following actions: **a** In the call list, highlight the call. **b** From the main menu, select **File** → **Save to File**.
If you want to save multiple calls,	perform the following actions: **a** In the call list, select the check boxes for the calls. **b** From the main menu, select **File** → **Save to File**.
If you want to save a portion of a call,	perform the following actions: **a** In the call list, highlight the call. **b** In the sound visualization section, highlight the audio portion that you want to save. You cannot highlight an audio portion shorter than 50 ms. **c** Right-click the highlighted audio portion. Click **Save Selection to File**.

    2 In the **Save As** dialog, navigate to the location in which you want to save the `.wav` file.

    3 Specify the name for the `.wav` file.

    4 Click **Save**.

This page intentionally left blank.

Appendix A

MCC 7100 IP Dispatch Console Additional Procedures and Information

This appendix provides helpful procedures and information that are not part of the typical MCC 7100 IP Dispatch Console installation.

Removing All MCC 7100 IP Dispatch Console Applications

Perform this procedure to remove a previous version of the MCC 7100 IP Dispatch Console software. The assumption is that the version that you want to remove is software that was successfully installed and is in an operational state.

When and where to use: By uninstalling the Motorola MCC 7100 Series software, you remove only the MCC 7100 application package. Other dependency packages that are both Motorola packages, for example, Motorola Password Vault and Motorola OpenSSL, and non-Motorola packages, for example, 7-zip and DirectX runtimes, are not automatically removed. To remove them from the system, uninstall them manually.

Procedure:

1 Log on to the Windows operating system as an administrator.

2 In the **Control Panel**, navigate to the **Programs and Features** pane.

3 Select **Motorola MCC 7100 Console Operator Position Series**.

4 Click **Uninstall**.

   📝 **NOTICE:** An error message can appear stating: `ERROR 1306: Another app has exclusive access to the file C:\...\Debug.mdb. Please shutdown all other apps and retry`. If the message appears, wait one minute and click **Retry**.

5 Close the **Programs and Features** window.

6 Reboot the computer.

Removing the Elite Admin and Elite Dispatch Applications Only

By default, both Elite Admin and Elite Dispatch applications are installed on the MCC 7100 IP Dispatch Consoles. You can remove the Elite Admin or Dispatch application individually. To re-add the removed components, reinstall the application software.

Procedure:

1 Log on to the Windows operating system as an administrator.

2 In the **Control Panel**, navigate to the **Programs and Features** pane.

3 From the list, select **Motorola MCC 7100 Console Operator Position Series**. Click **Change**.

4 On the welcome page of the **InstallShield Wizard** window, click **Next**.

5 On the **Program Maintenance** page, select **Modify**. Click **Next**.

6 On the **Custom Setup** page, click the drop-down menu for the feature that you want to remove and select **This Feature will not be available**. Click **Next**.

7 On the **Ready to Modify the Program** page, click **Install**.

8 On the **InstallShield Wizard Completed** page, click **Finish**.

9 When prompted to reboot, click **Yes**.

Configuring a Preconfigured Patch Console (Inside the ASTRO RNI)

A preconfigured patch console must be a member of the preconfigured patch organization unit at the domain controller to prevent the security banner from being displayed during login.

An MCC 7100 IP Dispatch Console can be configured as a preconfigured patch console. This configuration allows the console to automatically log on to Windows, start Elite, and activate preconfigured Patch Groups.

> **NOTICE:** If converting a regular dispatch console to a preconfigured patch console, the console must be rejoined to the domain as follows:
>
> • Add the dispatch console to the domain for the console site. See Setting Up the Domain for an MCC 7100 IP Dispatch Console Inside the ASTRO Radio Network Infrastructure on page 66.
>
> • Rejoin the console to the domain. See the "Joining and Rejoining a Windows-Based Device to an Active Directory Domain Using a Script" section in the *Authentication Services* manual.

Prerequisites: This process applies only to an MCC 7100 IP Dispatch Console configured as a preconfigured patch console deployed inside an ASTRO® 25 Radio Network Infrastructure (RNI). This process assumes that an ELT file exists for the preconfigured patch console. See the *MCC 7500/7100 Elite Admin User's Guide* for creating Elite configuration files.

Process:

1 Configure automatic Windows login. See Configuring an Automatic Windows Login on page 152 for details.

2 Add Elite authentication to Windows registry. See Adding Elite Authentication Username and Password to the Windows Registry on page 154 for details.

3 Create batch file for automatic network authentication. See Creating Batch File for Automatic Network Authentication on page 155 for details.

4 Reboot the computer.

> **NOTICE:** After a reboot, Windows automatically logs in and starts Elite.

Configuring an Automatic Windows Login

An automatic Windows log on is supported only for MCC 7100 IP Dispatch Consoles configured as permanent patch consoles.

> **CAUTION:** A security risk exists when configuring automatic Windows Login.

> **NOTICE:** A console previously configured for automatic Windows login may no longer login as anticipated after the computer is joined to the domain.

> **NOTICE:** The user may be required to create the registry keys mentioned in this section.

Process:

1 Add Windows domain username and password to Windows registry.

2 Configure the domain controller for the preconfigured patch OP.

Adding Windows Domain Username and Password to Windows Registry

Procedure:

1 In Windows, select **Start** and enter `regedit32` in the search field.

> **NOTICE:** When prompted for permission, click **Continue**.

2 In the registry editor, navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`.

3 Double-click **AutoAdminLogon** value.

4 In the **Edit String**, enter `1` window.

5 Click **OK**.

6 Ensure that the **AutoLogonCount** entry does not exist.

> **NOTICE:** If **AutoLogonCount** exists, delete it from the registry.

7 Double-click the **DefaultUserName** value.

> **NOTICE:** If **DefaultUserName** does not exist, a new String Value must be created.

8 In the **Edit String** box, enter a valid Windows Local username for the computer.

9 Click **OK**.

10 Double-click the **DefaultPassword** value.

> **NOTICE:** If **DefaultPassword** does not exist, a new String Value must be created.

11 Enter a valid Windows Domain Password for the Username used in step 8.

12 Click **OK**.

13 Double-click the **DefaultDomainName** value.

> **NOTICE:** If **DefaultDomainName** does not exist, a new String Value must be created.

14 In the **Edit String** dialog box, enter a valid Windows Domain for the computer.

15 Click **OK**.

16 Exit the Registry Editor.

Configuring the Domain Controller for the Preconfigured Patch OP

✏️ **NOTICE:** This procedure is not applicable for ASTRO® 25 Conventional System (K core).

Procedure:

1 Log on to the Zone Level Domain Controller.

   ✏️ **NOTICE:** When prompted for permission, click **Continue**.

2 Open **Administrative Tools**, and select **Group Policy Management**.

3 In the list of Group Policy Objects, locate the **Preconfigured Patch Dispatch Console GPO**.

4 Right-click the **Preconfigured Patch Dispatch Console GPO** and select **Edit**.

5 In the Group Policy Object Editor, select **Polices** from the **Computer Configuration** section.

6 From the **Policies** section, select **Administrative Templates**.

7 From the **Administrative Templates** section, select **Classic Administrative Templates (ADM)**.

8 Double-click the **Custom Settings** folder, and then double-click the **Logon** folder.

9 Double-click the **Specify password for AutoLogon policy** option.

10 Set the policy to **Enabled**, and in the **Password** field, specify the password that the preconfigured patch OP uses to log on to the windows domain, and click **OK**.

11 Close the Group Policy Object Editor.

12 Open **Administrative Tools**, select **Active Directory Users and Computers**.

13 Locate the Preconfigured Patch Dispatch Consoles OU. Verify that the computer object for the Preconfigured Patch OP is a member of this OU.

14 Log on to the Preconfigured Patch OP.

15 From the **Start** menu, select **Run** and enter `gpupdate /force`.

   This action forces the Preconfigured Patch OP to download the password specified on the Zone Level Domain Controller.

Adding Elite Authentication Username and Password to the Windows Registry

Procedure:

1 Select **Start** and enter `regedt32` in the search field.

   ✏️ **NOTICE:** When prompted for permission, click **Continue**.

2 In the registry editor, navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432 Node\Motorola\Console\Elite`.

3 Double-click the **U** value

4 In the **Value Data** field, enter a valid **Username** for the Network Authentication.

   ✏️ **NOTICE:** This username corresponds to the console user created in Provisioning Manager.

5 Click **OK**.

6 Double-click the **P** value.

7 In the **Edit String** dialog box, enter the password for the username used in step 4

8 Click **OK**.

9 Close the Registry Editor.

Creating Batch File for Automatic Network Authentication

Procedure:

1 In the Windows operating system, open **Notepad**.

2 Enter the following: `ping 127.0.0.1 -n 6 >NUL`.

> 📝 **NOTICE:** This line in the `bat` file pauses the computer for 5 seconds before continuing. This delay is required for Elite Dispatch software to properly initialize after Windows has been restarted. The delay required varies based on the configuration of the device depending on what cohab applications are installed (including antivirus software), CPU speed, and hardware configuration. If the Elite software does not initialize with the 5 second delay, it may be necessary to increase the delay time.
> To adjust the delay time, change the number after the "-n" argument. The delay time is 1 second less than the number after "-n". For example, "`ping 127.0.0.1 –n 11 >NUL`" creates a 10 second delay.

3 Press ENTER.

4 On the second line, enter
"*<Path to Elite.exe>*" "*<path to ELT file to be used for preconfigured patch>*" –authenticate

Step example:
If the `elite.exe` is installed in the default location and an ELT file called `preconfiguredpatch.elt` exists, then the line is (including quotation marks):

"`C:\Program Files (x86)\Motorola MCC 7100\bin\elite.exe`" "`C:\Users \Public\Motorola MCC 7100\config\precofiguredpatch.elt`" -authenticate

5 Save the file as **PreconfiguredPatch.bat** and save it to the following location:

`C:\Users\`*<Windows AUTHENTICATION USERNAME>*`\AppData\Roaming\Microsoft \Windows\Start Menu\Programs\Startup`.

> 📝 **NOTICE:** The **AUTHENTICATION USERNAME** should match the one used in the Registry for Automatic Login. The exceptions is if zone suffixes or enumerated instances exist, for example, "C:\Users\motosec.zone1.004". In these cases, use the most recent directory that matches your currently logged in Windows User account.

6 Reboot the computer.

> 📝 **NOTICE:** After the computer reboots, Windows automatically logs in and starts Elite.

Fault Management

This section includes fault management for the MCC 7100 IP Dispatch Console including:

- Fault Management for Devices Inside the ASTRO® 25 Radio Network Infrastructure (RNI)
  - MCC 7100 IP Dispatch Console Fault Management
  - PRX 7000 Console Proxy Fault Management
  - Control Room Firewall Fault Management

- Fault Management for Devices Outside the ASTRO® 25 RNI

Fault Management for Devices Inside the ASTRO Radio Network Infrastructure

When auto-discovering the MCC 7100 IP Dispatch Console from the Unified Event Manager (UEM), ensure that the console application is up and running, otherwise auto-discovery fails and the device must to be rediscovered.

MCC 7100 IP Dispatch Console Fault Management

The MCC 7100 IP Dispatch Console supports the same fault interface as the MCC 7500 Dispatch Console. The MCC 7100 IP Dispatch Console has the same sysOid as the MCC 7500 Dispatch Consoles. Faults from the MCC 7100 IP Dispatch Console are displayed as "Motorola Dispatch Console – MCC 7500".

PRX 7000 Console Proxy Fault Management

The PRX 7000 Console Proxy is managed as an IP managed device by the Unified Event Manager (UEM). The computer is discovered as a generic node and is supervised using Internet Control Message Protocol (ICMP) requests. The UEM manages and reports the network path status from the UEM to console proxy computer.

Control Room Firewall Fault Management

Firewalls in an ASTRO® 25 Core are IP managed devices. The Control Room Firewall is discovered as a generic node, and supervised using Internet Control Message Protocol (ICMP) requests. The Unified Event Manager (UEM) manages and reports communication link status for the Control Room Firewall.

See "Discovering Devices" in the *Unified Event Manager* manual.

Fault Management for Devices Outside the ASTRO RNI

The MCC 7100 IP Dispatch Console fault management is not supported outside the ASTRO® 25 Radio Network Infrastructure (RNI). Due to the nature of the deployment, MCC 7100 IP Dispatch Consoles outside the ASTRO® 25 RNI may be active for a brief period of time. The dispatch consoles are not expected to run in a 24 hours a day, 7 days a week environment. MCC 7100 IP Dispatch Consoles outside the RNI are not discovered in Unified Event Manager (UEM).

Embedded Password Management

The MCC 7100 IP Dispatch Console supports password management for embedded passwords. For procedures on using password management, see "Appendix C - Embedded Password Management" in the *Authentication Services* manual.

> **NOTICE:** When changing an embedded password for the MCC 7100 IP Dispatch Console, shut down the Elite Dispatch application. Restart Elite after the password is changed.

Enabling Receive AGC Through Registry Setting

Perform this procedure to enabling receive Automatic Gain Control (AGC) through the registry setting.

Enabling Receive AGC enables the feature for all AGC-capable resources on the Dispatch Console. The feature is not configurable on a per-resource basis.

Procedure:

1 From the Windows menu, select **Run**. Enter `Regedt32.exe`.

2 In the **Registry Editor** dialog box, navigate to `\\HKEY_LOCAL_MACHINE\SOFTWARE \Wow6432Node\Motorola\Console\AM\`

3 If the value for AGCRx exists, proceed to step 4. If the value does not exist, perform the following actions to create it.

   a Right-click in the main Window of the registry editor. Select **New → String Value**.

   b Name the parameter `AGCRx`

4 Double-click the AGCRx value.

5 In the **Edit String** dialog box, enter a value of `1`.

6 Close the registry editor.

This page intentionally left blank.

Appendix B

Enhanced Alert Tones

Use the information in this appendix to create and configure alert tones that meet the requirements of your organization.

Enhanced Alert Tones Overview

The Enhanced Alert Tones feature increases the number of the alert tones that you can use with the dispatch console. It also provides increased flexibility in using the alert tones as it makes it possible to replace the predefined and unconfigurable alert tones provided by Motorola with alert tones that you can customize according to your needs.

Before the introduction of Enhanced Alert Tones, the dispatch console supported three distinct, predefined, and unconfigurable alert tones. They were available based on the console configuration parameters in Provisioning Manager or Configuration Manager application, and based on the dispatch console position setup in the Elite Admin application.

With Enhanced Alert Tones, you can use up to 15 console alert tones. With the initial installation of the dispatch console software that supports Enhanced Alert Tones, 15 predefined enhanced alert tones are installed in a predetermined location on the console client.

You can override the default enhanced alert tones by creating customized enhanced alert tones with an audio file processing software application. The custom files must meet the required audio file specifications and the file location and naming conventions.

Enhanced Alert Tones Audio File Specifications

Enhanced Alert Tones make it possible to create custom alert tones. You can create new audio files or customize the predefined alert tones provided by Motorola. However, all the files must meet some requirements.

General Specifications

If an enhanced alert tone file does not meet the required criteria, the dispatcher fails to play the tone and instead an error notification appears in the status line of the Elite application. Your customized enhanced alert tone files must meet the following requirements:

- The file has `.wav` extension
- The audio is sampled at 8 ksps
- The audio is mono (single channel)
- The audio samples are 16-bit Pulse Code Modulation (PCM)
- The audio is longer than 20 milliseconds but shorter than five minutes

The `.wav` file should have an average level of -28 dBov to achieve the desired system output level of -22 dBm0.

> 📝 **NOTICE:**
> Use commercially available sound editing software to modify or create customized `.wav` files for the enhanced alert tone feature.
>
> If you formatted an enhanced alert tone according to the listed specifications and the dispatch console cannot use it, your sound editing software may have saved the alert tone in a non-standard `.wav` format which the dispatch console cannot process. If you encounter this issue, re-record the audio by using an application which saves the `.wav` files in the standard format that the dispatch console can process.
>
> Cohabitation of sound editor software on the MCC 7500 operator position computer is not supported. Use of sound editor software on the MCC 7500 operator position may have unintended effects on the MCC 7500 software.

AMBE+2 Specifications

If you use a digital trunking system that uses the AMBE+2 vocoder, meet the following requirements:

- The frequencies of the generated tone must be between 120 Hz and 3840 Hz

- The duration of a continuous tone at one frequency must be greater than or equal to 50 milliseconds

Any tones outside of those boundaries exhibit severe distortions that can be intolerable for listeners. The decoded frequencies of the generated tones may be outside the tolerance of most analog equipment.

If using an analog conventional system that uses the G.728 vocoder, there are no restrictions on the content of the `.wav` files.

Enhanced Alert Tones Audio Files Configuration

This section describes how to override the predefined enhanced alert tones or remove access to an enhanced alert tone.

Audio File Location

Alert tones are stored in two separate directories. One directory is for the predefined alert tones and the other is for custom alert tones. The predefined alert tones are stored in the following directory:

    C:\Users\Public\Documents\Motorola MCC 7100\alert tones\default

The custom alert tones are stored in the following directory:

    C:\Users\Public\Documents\Motorola MCC 7100\alert tones\customized

The Elite application supports up to 15 alert tones. Custom alert tones override their corresponding predefined alert tones. After the initial installation, the **default** directory contains 15 predefined alert tone `.wav` files, and the **customized** directory is empty.

Custom Alert Tones Installation

To override a predefined alert tone with a custom alert tone, meet the following requirements:

- The custom audio file meets the required specifications. See Enhanced Alert Tones Audio File Specifications on page 159

- The name of the custom audio file is `AlertTone<number>.wav`

    where `<number>` is the number of the predefined alert tone that you want to override.

- The custom audio file is in the following directory for the custom alert tones:

    C:\Users\Public\Documents\Motorola MCC 7100\alert tones\customized

For example, to override the predefined alert tone 15 with a custom file, save the custom file in the **customized** folder with the name `AlertTone15.wav`. To restore access to the predefined alert tone, remove the custom alert tone file from the **customized** directory. Separate directories for the predefined alert tones and the custom alert tones make it easy to replace and restore the predefined alert tones.

If the corresponding **Alert Tone** button or the **Alert Tone Selector** button is added to the toolbar in the `.elt` configuration file used by the Elite Dispatch application, you can send the custom alert tone immediately after you install it. If none of the buttons is configured in the `.elt` file, add the button by using the Elite Admin application and restart the Elite Dispatch application. See the *MCC 7500/7100 Elite Admin User Guide* and the *MCC 7500/7100 Elite Dispatch User Guide* manuals.

Permanent Removal of an Alert Tone

The common way of making specific alert available or unavailable for dispatchers is by modifying the `.elt` configuration files in the Elite Admin application. Make an alert tone available by adding the corresponding **Alert Tone** button or the **Alert Tone Selector** button to the toolbar of the Elite Dispatch application. However, if you want to be sure that a specific dispatch position does not have access to a specific alert tone, you can remove the alert tone from both the **customized** and **default** directories. Keep a backup of the removed predefined alert tone files in the event you want to quickly restore them.

To remove the corresponding **Alert Tone** button from the toolbar of the Elite Dispatch application or to remove the corresponding selection from the list of the **Alert Tone Selector** button, restart the Elite Dispatch application.

Restoration of a Removed Alert Tone

To restore an alert tone, it means that you removed the alert tone and want to place it back in the **default** or **customized** directory. The name of the restored default alert tone must be `DefaultAlertTone`***<number>***`.wav` and the name of the restored customized alert must be `AlertTone`***<number>***`.wav`

where ***<number>*** is the number of the alert tone that you want to restore, for example, `DefaultAlertTone15.wav`.

If the corresponding **Alert Tone** button or the **Alert Tone Selector** button is configured in the `.elt` file, the alert tone is available as soon as you load the `.elt` file into the Elite Dispatch application. If the corresponding **Alert Tone** button and the **Alert Tone Selector** button are not added to the toolbar in the `.elt` configuration file, add any of the buttons to the toolbar by using the Elite Admin application.

NOTICE: The customized alert tones always have higher priority than the default alert tones. To restore a default alert tone, place it back in the **default** folder. To use it in the Elite Dispatch application, remove the corresponding alert tone from the **customized** folder.

The changes are not always visible in the `.elt` configuration file that is opened in the Elite Dispatch application at the moment of restoration. See the following scenarios for the actions to perform to use the restored alert tones in a configuration loaded at the moment of restoration.

When you restore a customized alert tone, one of the following scenarios takes place:

- The loaded `.elt` file is configured for a specific alert tone, but the alert tone is removed both from the **default** and **customized** folder. Restore the alert tone in the **customized** folder. To see it in the `.elt` configuration loaded in the Elite Dispatch application, reload the `.elt` file.

- The loaded `.elt` file is configured for a specific alert tone which is removed only from the customized folder. Restore the alert tone in the **customized** folder to use it instead of the default alert tone. No reload is necessary for the changes to be visible in the `.elt` configuration loaded in the Elite Dispatch application.

- The loaded `.elt` is not configured for a specific alert tone. Restore the alert tone in the **customized** folder and you want to use it in the loaded `.elt` configuration. After you restore the alert tone, perform appropriate configuration in the Elite Admin application and reload the `.elt` file.

When you restore a default alert tone, one of the following scenarios takes place:

- The loaded `.elt` file is configured for a specific alert tone, but the alert tone is removed both from the **default** and **customized** folder. Restore the alert tone in the **default** folder. To see it in the `.elt` configuration loaded in the Elite Dispatch application, reload the `.elt` file.

- The loaded `.elt` file is configured for a specific alert tone which is removed only from the **default** folder. Restore the default alert tone and want to use it in the loaded `.elt` configuration. After you restore the alert tone, remove the customized alert tone. No reload is necessary for the changes to be visible in the `.elt` configuration loaded in the Elite Dispatch application.

- The loaded `.elt` file is not configured for a specific alert tone. The alert tone is removed both from the **default** and **customized** folder. Restore the default alert and want to use it in the loaded `.elt` configuration. After you restore the default alert tone, perform appropriate configuration in the Elite Admin application and reload the `.elt` file.

- The loaded `.elt` file is not configured for a specific alert tone. It is removed from the **default** but not from the **customized** folder. Restore the default alert and want to use it in the loaded `.elt` configuration. After you restore the default alert tone, remove the customized alert tone, perform appropriate configuration in the Elite Admin application, and reload the `.elt` file.

Provisioning Manager Configuration

Before you launch the console application, establish the following parameters in Provisioning Manager.

Tone Pre-time Delay
The Tone Pre-time Delay parameter is particular to conventional channels. It defines the amount of time the console waits to send an alert tone to a voice channel after it indicates the call request to the system for the first time. This pre-time gives the transmitting station and the receiving radios time to detect that a transmission begins on the selected voice channel. It prevents any front-end truncation of the audio that can occur on conventional channels.

For example, if the MDC signaling Pre-time Delay parameter of a channel is configured to truncate alert tones, the Tone Pre-time Delay must be equal to, or greater than the MDC signaling Pre-time Delay. The default value is 0 with the range between 0 to 3,300 milliseconds, in increments of 100.

Alert Tone Talk Extend Time
The Alert Tone Talk Extend Time (sec) makes it possible to set the amount of time all the resources remain keyed after the alert tone is generated which allows the dispatcher to transmit a voice message on the selected channels. By setting the Alert Tone Talk Extend Time parameter, you determine the amount of time the console keeps the voice channel or talkgroup keyed before it automatically dekeys. During this time, the dispatcher can press the transmit button on the console and begin speaking without having to re-initiate the transmission. The Alert Tone Talk Extend Time keeps the resources keyed for the dispatcher after they send the alert tones out. The default time is 1.2 seconds, the range is 0-7.

For more information about setting the parameters, see the *Provisioning Manager* manual.

Elite Admin Configuration

After you create the audio files and save them in the appropriate folder on the console dispatch client, make them available for dispatchers by using the Elite Admin application.

When you launched the Elite Admin application, the alert tones are mapped to the application in the following way:

- If there are no custom files, only the available Motorola alert tones are mapped.

- If for any of the Motorola alert tones, there is a counterpart in the folder with custom alert tones, the custom alert tone is mapped instead of the Motorola alert tone.

As the result, the number of alert tones that can be available for dispatchers is 15 or less. The available alert tones can be either Motorola alert tones or custom alert tones, or both types. In the Elite Admin application, make them available for dispatchers by adding them to one of the toolbars in the `.elt` configurations.

Another configuration that you perform by using the Elite Admin application is setting the transmission methods for the available alert tones. Perform it by assigning the available alert tones to one of the following categories:

Momentary
Alert tones that are sent only while the dispatcher presses the **Alert Tone** button on the toolbar in the Elite Dispatch application.

Latched
Alert tones sent for a predefined time after the dispatcher presses the **Alert Tone** button on the toolbar in the Elite Dispatch application. They can stop sending the latched alert tone before the predefined time ends by pressing the **Alert Tone** button again.

See the *MCC 7500/7100 Elite Admin User Guide* manual.

Elite Dispatch Configuration and Operation

After you launch the Elite Dispatch application, the software automatically takes the following actions:

- Obtains the Tone Pre-time Delay and the Alert Tone Talk Extend timers that you set up for the system

- Uses the `.elt` file that you established in the Elite Admin application to determine which audio files must be available for transmission

- Checks whether the available audio files conform to the format and specifications

- Enables properly configured audio files for use in the application

The Elite Dispatch software also compares the number of audio files available in the defined location on the console client to the number of alert tones defined in the `.elt` configuration. If any of the audio files specified in the `.elt` configuration are present in the defined localization, the corresponding **Alert Tone** button is not available to the dispatcher.

To transmit an alert tone, the dispatcher clicks the **Alert Tone Selector** button or the corresponding **Alert Tone** button in the Elite Dispatch application. The **Alert Tone** buttons are numbered accordingly. If you configured the micro help text for the **Alert Tone** buttons, additional information about the alert tone appears when you hover over the button.

For information about using alert tones in the Elite Dispatch application, see the *MCC 7500/7100 Elite Dispatch User Guide* manual.

This page intentionally left blank.

Appendix C

MCC 7100 IP Dispatch Console System Release Compatibility

The backward compatibility feature makes it possible to use an MCC 7100 IP Dispatch Console together with the features available on this console in releases previous to the release in which the console was introduced.

- MCC 7100 IP Dispatch Consoles released in ASTRO® 25 7.14 are backward compatible with ASTRO® 25 7.11 and ASTRO® 25 7.13 systems.

- MCC 7100 IP Dispatch Consoles released in ASTRO® 25 7.15 are backward compatible with ASTRO® 25 7.13 and ASTRO® 25 7.14 systems.

Before you decide between installing and not installing a newer dispatch console in a previous system, see the *Dispatch Console Compatibility Guide* manual. The manual contains details about the features available for dispatch consoles used in system releases previous to the release in which the consoles were introduced.

If you want to use a new dispatch console in a system release previous to the release in which the console was introduced, ensure to obtain and configure all the required components.

Before you install any application or operating system software, audit each dispatch console to determine which version of the system release is installed.

ASTRO 7.15 Components in an ASTRO 7.13 System

Table 23: ASTRO 7.15 MCC 7100 IP Dispatch Console System Components in an ASTRO 7.13 System

MCC 7100 IP Dispatch Console System Components	ASTRO® 25 System Release 7.13 Requirements
System Architectures	The System Architectures that support MCC 7100 IP Dispatch Consoles are K, L core, M1/M2 and M3 cores.
Client Operating System	You must install the MCC 7100 IP Dispatch Console software on a client running the Windows 7 Professional operating system or Windows 8 operating system when installed outside ASTRO Radio Network Infrastructure (RNI).
PRX 7000 Console Proxy Cohabitation	You can install the PRX 7000 Console Proxy on a standalone client dedicated to this software application or cohabited with an ASTRO 7.15 MCC 7500 Dispatch Console.
Installation Media	To install the MCC 7100 IP Dispatch Console in the ASTRO 7.13 system, you use the ASTRO 7.15 installation media.
Firewall	You must update the ASTRO 7.13 ZCP firewall configuration.
Console Site LAN Switch	You must update the ASTRO 7.13 console site LAN switch configuration.

Table continued…

MCC 7100 IP Dispatch Console System Components	ASTRO® 25 System Release 7.13 Requirements
Console Site Router	You must update the ASTRO 7.13 console site router configuration.

Setting Up the MCC 7100 IP Dispatch Console in a System From a Previous ASTRO 25 Release

Prerequisites: Before you install any application or operating system software, audit each dispatch console to determine which version of the system release is installed.

- MCC 7100 IP Dispatch Consoles released in ASTRO® 25 7.14 are backward compatible with ASTRO® 25 7.11 and ASTRO® 25 7.13 systems.

- MCC 7100 IP Dispatch Consoles released in ASTRO® 25 7.15 are backward compatible with ASTRO® 25 7.13 and ASTRO® 25 7.14 systems.

When and where to use: Use this procedure to prepare your ASTRO® 25 system for installation of the MCC 7100 IP Dispatch Console.

Procedure:

1. Obtain updated configuration files for all the following devices:
    - Console site LAN switch – see the *System LAN Switch* manual.
    - Site routers - see the *System Gateways – GGM 8000* manual or the *System Routers – S6000/S2500* manual.
    - Zone Core Protection (ZCP) firewall - see the *Fortinet Firewall* manual.
    - Control room firewall if present in your system - see the *Fortinet Firewall* manual.

2. Update the Group Policies Objects (GPO) on the domain controllers for the MCC 7100 IP Dispatch Consoles. See the *Authentication Services* manual.

3. Set up the MCC 7100 IP Dispatch Console in Provisioning Manager to ensure the console authentication with the Lightweight Directory Access Protocol (LDAP) database.

4. Install the PRX 7000 Console Proxy. See Setting Up the PRX 7000 Console Proxy on page 89.
    - In an ASTRO® 25 7.15 system, you can install the PRX 7000 Console Proxy on a dedicated standalone client running Windows 7 or cohabited with the one of the following applications:
        - ASTRO® 25 7.17 MCC 7500 Dispatch Console
        - ASTRO® 25 7.15 or ASTRO® 25 7.17 Console Alias Manager (CAM) client

    -

    - When you install the ASTRO® 25 7.15 PRX 7000 Console Proxy application on an ASTRO® 25 7.13 system, it must use the ASTRO® 25 7.13 version of the windows supplemental configuration (secure) kit.
    - When you install the ASTRO® 25 7.15 PRX 7000 Console Proxy application on an ASTRO® 25 7.13 system, it can use the ASTRO® 25 System Release 7.13 version of the antivirus software.

5. Install the MCC 7100 IP Dispatch Console (and anti-virus software). See Setting Up the MCC 7100 IP Dispatch Console on page 42.

6. Update the Customer Enterprise Network (CEN) to support the MCC 7100 IP Dispatch Consoles outside the ASTRO® 25 Radio Network Infrastructure (RNI).

> **NOTICE:** The VPN network in the CEN must be configured to allow the MCC 7100 IP Dispatch Console deployed outside the ASTRO® 25 RNI to access the VPN.

7 Transfer security keys to the MCC 7100 IP Dispatch Console. See Load Secure Keys and Algorithms on page 55.

8 Set up the MCC 7100 IP Dispatch Console peripherals:

  • If you use the Motorola peripherals, see USB Audio Interface Module on page 101 and MCC 7100 Peripheral Configuration Tool on page 127.

  • If you use non-Motorola peripherals only, see MCC 7100 Peripheral Configuration Tool on page 127.

9 Optional: If you use the Instant Recall Recorder (IRR) software, see Instant Recall Recorder on page 141.

ASTRO 7.15 Components in an ASTRO 7.14 System

Table 24: ASTRO 7.15 MCC 7100 IP Dispatch Console System Components in an ASTRO 7.14 System

MCC 7100 IP Dispatch Console System Components	ASTRO® 25 System Release 7.14 Requirements
System Architectures	The System Architectures that support MCC 7100 IP Dispatch Consoles are K core, L core, M1/M2 and M3 cores.
Client Operating System	Install the MCC 7100 IP Dispatch Console software on a client running the Windows 7 Professional operating system or Windows 8 operating system when installed outside ASTRO® 25 Radio Network Infrastructure (RNI).
PRX 7000 Console Proxy Cohabitation	You can install the PRX 7000 Console Proxy on a stand-alone client dedicated to this software application or co-habited with an ASTRO® 25 7.15 MCC 7500 Dispatch Console.
Installation Media	To install the MCC 7100 IP Dispatch Console in the ASTRO® 25 7.14 system, use the ASTRO® 25 7.15 installation media.
Firewall	Update the ASTRO® 25 7.14 ZCP firewall configuration.
Console Site LAN Switch	Update the ASTRO® 25 7.14 console site LAN switch configuration.
Console Site Router	Update the ASTRO® 25 7.14 console site router configuration.

Setting Up the ASTRO 7.15 MCC 7100 IP Dispatch Console in an ASTRO 7.14 System

Prepare your ASTRO® 25 7.14 system for installing the ASTRO® 25 7.15 MCC 7100 IP Dispatch Consoles and using the features available for this console.

Prerequisites: Before you install any application or operating system software, audit each dispatch console to determine which version of the system release is installed.

Procedure:

1 Obtain updated configuration files for all the following devices:

   - Console site LAN switch. See the *System LAN Switch* manual.

   - Site routers. See the *System Gateways – GGM 8000* manual or the *System Routers – S6000/S2500* manual.

   - Zone Core Protection (ZCP) firewall. See the *Fortinet Firewall* manual.

   - Control room firewall if equipped. See the *Fortinet Firewall* manual.

2 Update the Group Policies Objects (GPO) on the domain controllers for the MCC 7100 IP Dispatch Consoles. See the *Authentication Services* manual.

3 Set up the MCC 7100 IP Dispatch Console in Provisioning Manager to ensure the console authentication with the Lightweight Directory Access Protocol (LDAP) database.

4 Install the PRX 7000 Console Proxy. See Setting Up the PRX 7000 Console Proxy on page 89.

   In an ASTRO® 25 7.14 system, you can install the PRX 7000 Console Proxy on a dedicated standalone client running Windows 7 or cohabited with one of the following applications:

   - ASTRO® 25 7.15 MCC 7500 Dispatch Console

   - ASTRO® 25 7.14 or ASTRO® 25 7.15 MKM 7000 Console Alias Manager (CAM) client

   > **NOTICE:** When you install the ASTRO® 25 7.15 PRX 7000 Console Proxy on an ASTRO® 25 7.14 system, it must use the ASTRO® 25 7.14 version of the Windows supplemental configuration (secure) kit. The ASTRO® 25 7.15 application installed on an ASTRO® 25 7.14 system can utilize the ASTRO® 25 7.14 version of the antivirus software.

5 Install the MCC 7100 IP Dispatch Console (and anti-virus software). See Setting Up the MCC 7100 IP Dispatch Console on page 42.

6 Update the Customer Enterprise Network (CEN) to support the MCC 7100 IP Dispatch Consoles outside the ASTRO® 25 Radio Network Infrastructure (RNI).

   > **NOTICE:** The VPN network in the CEN must be configured to allow the MCC 7100 IP Dispatch Console deployed outside the ASTRO® 25 RNI to access the VPN.

7 Transfer security keys to the MCC 7100 IP Dispatch Console. See Load Secure Keys and Algorithms on page 55.

8 Set up the MCC 7100 IP Dispatch Console peripherals:

   - If you use the Motorola peripherals, see USB Audio Interface Module on page 101 and MCC 7100 Peripheral Configuration Tool on page 127.

   - If you use non-Motorola peripherals only, see MCC 7100 Peripheral Configuration Tool on page 127.

9 If you use the Instant Recall Recorder (IRR) software, see Instant Recall Recorder on page 141.

Other System Updates and Considerations

When you install the MCC 7100 IP Dispatch Console in a release earlier than ASTRO ® System Release 7.15 , review the relevant features for any updates and considerations related to the backward compatibility feature.

Audio Logging

See the ASTRO® 25 7.15 *MCC 7500 Dispatch Console with Voice Processor Module* manual for details.

Bandwidth Management

See the ASTRO® 25 7.15 *Bandwidth Management* manual for details.

Centralized Event Logging

See the ASTRO® 25 7.15 *Centralized Event Logging* manual for details.

KVL 4000

See the ASTRO® 25 7.15 *KVL 4000 ASTRO 25 User Guide* for details.

MCC 7500 Elite Software

The MCC 7100 Elite Admin and Elite Dispatch software support the MCC 7100 IP Dispatch Console. See the following manuals for details:

* ASTRO® 25 7.15 *MCC 7500/7100 Elite Admin User's Guide*
* ASTRO® 25 7.15 *MCC 7500/7100 Elite Dispatch User's Guide*

User Configuration Manager and Provisioning Manager

See the ASTRO® 25 7.14 *Provisioning Manager* manual.

This page intentionally left blank.