

System Release 5.2.2 Intelligent Middleware



Feature Manual

JULY 2020

MN003206A01-G

Copyrights

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

© 2020 Motorola Solutions, Inc. All Rights Reserved

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

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

Disclaimer

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

Trademarks

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

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



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

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

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

Contact Us

Motorola Solutions Support Center

The Solutions Support Center (SSC) is the primary contact for technical support included in your organization's service agreement with Motorola Solutions.

Service agreement customers should be sure to call the SSC in all situations listed under Customer Responsibilities in their agreement, such as:

- Before reloading software.
- To confirm troubleshooting results and analysis before taking action.

Your organization received support phone numbers and other contact information appropriate for your geographic region and service agreement. Use that contact information for the most efficient response. However, if needed, you can also find general support contact information on the Motorola Solutions website, by following these steps:

- Enter motorolasolutions.com in your browser
- Ensure that your organization's country or region is displayed on the page. Clicking or tapping the name of the region provides a way to change it.
- Select "Support" on the motorolasolutions.com page.

Comments

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

Provide the following information when reporting a documentation error:

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

Document History

Edition	Description	Date
MN003206A01-A	Original release of the <i>Feature Manual</i> for IMW 5.2.	September 2016
MN003206A01-B	Minor structural changes. Updates related to supported IMW installation suites.	November 2016
MN003206A01-C	Updates related to the IMW features descriptions.	May 2018
MN003206A01-D	Minor updates.	December 2018
MN003206A01-E	Updates related to Location Service and Security Functionality descriptions.	February 2019
MN003206A01-F	Minor updates.	April 2019
MN003206A01-G	Updated the following section: <ul style="list-style-type: none">• Device Provisioning on page 52	July 2020

Contents

Copyrights.....	2
Contact Us.....	3
Document History.....	4
List of Figures.....	8
List of Tables.....	9
About IMW Feature Manual.....	10
What Is Covered In This Manual.....	10
Helpful Background Information.....	10
Navigation Through .pdf Files.....	10
Chapter 1: IMW Description.....	11
1.1 IMW Overview.....	11
1.2 IMW Supported Systems.....	13
1.3 IMW Supported Releases and Services.....	13
1.4 Networks and Supported Devices.....	14
1.5 Third-Party Software Components.....	15
1.6 IMW Software Components Overview.....	15
1.7 ESU Launchpad Overview.....	17
1.8 IMW Network Setup Overview.....	19
1.9 Hardware Component Configuration.....	20
1.10 IMW 5.2 Installation Configurations	21
1.11 IMW Features and Services.....	23
1.11.1 Services Overview.....	23
1.11.2 Location Service Overview.....	24
1.11.2.1 Location on Push to Talk.....	25
1.11.2.2 Location-Based Modules Overview.....	25
1.11.2.3 IMW Telemetry.....	26
1.11.2.4 REST-based Location Reporting Triggers.....	26
1.11.3 Messaging Service.....	27
1.11.4 Multi-Group Management Service.....	28
1.11.5 Context Service Overview.....	29
1.11.6 Identity Service Overview.....	30
1.12 IMW Functions.....	30
1.12.1 Configuration Functionality.....	31
1.12.1.1 IMW Configuration Manager.....	31
1.12.1.2 UNS Administrative Client.....	31

1.12.1.3 UNS Web Location Administrative Client.....	32
1.12.2 Fault Management Functionality.....	32
1.12.3 Security Functionality.....	32
1.12.3.1 Administrator and User Authorization.....	32
1.12.3.2 Agency Data Segregation and Access Control.....	33
1.12.3.3 Fine Grained Authorization.....	34
1.12.3.4 Zero Touch Provisioning.....	34
1.12.3.5 IMW Security.....	35
1.12.3.6 IMW Server Licensing.....	35
1.12.3.7 Information Assurance.....	36
1.12.3.8 IMW and Network Security.....	36
1.13 IMW Redundancy Overview.....	36
1.13.1 Automatic Control of IMW Redundancy.....	37
1.13.2 Network Connectivity Between IMW Servers.....	38
1.13.3 Client Applications Interaction with IMW Redundancy.....	38
1.13.4 Switchover Triggers.....	38
1.13.5 Fault Management Reporting.....	39
1.13.6 Configuration of IMW Parameters When Servers Are Synchronized.....	39
1.13.7 Automated Virtual Machine Standby with DAS.....	40
1.14 Client Applications and Solutions Supported by IMW.....	41
1.14.1 MotoMapping.....	41
1.14.2 Advanced Messaging Solution.....	41
1.14.3 Converged Services Client.....	42
Chapter 2: ASTRO 25 System Deployments.....	43
2.1 How IMW Functions Within an ASTRO 25 System.....	43
2.2 ASTRO 25 Supported Devices.....	43
2.3 ASTRO 25 System Presence Service.....	43
2.3.1 Device Presence.....	43
2.3.2 User Presence.....	44
2.3.3 IMW Presence Deployment in an ASTRO 25 Advanced Messaging Solution.....	44
2.3.4 Subscriber Radio Inactivity Time.....	45
2.3.5 User Session Timer.....	45
2.3.6 User Authentication For Pre-A7.12 Radios Only.....	45
2.4 Talkgroup and Radio Site Affiliation.....	46
2.5 ASTRO 25 Outdoor Location Solution and IMW Location Service.....	46
2.6 CADI and IMW.....	48
2.7 Device Provisioning.....	48
2.8 User Provisioning.....	48
2.9 IMW Migration in the ASTRO 25 System.....	49

Chapter 3: Dimetra IP System Deployments.....	50
3.1 How IMW Functions Within a Dimetra IP System.....	50
3.2 Dimetra IP Presence Service.....	50
3.2.1 Basic Device Presence.....	50
3.2.2 Talkgroup and Radio Site Affiliation.....	50
3.2.3 Status Messaging.....	51
3.3 Dimetra IP Location Service.....	51
3.3.1 Dimetra IP Cell-Based Location.....	51
3.3.2 Dimetra IP Short Data-Based Location.....	51
3.4 MCADI and IMW.....	52
3.5 ATIA and IMW.....	52
3.6 Device Provisioning.....	52
3.7 Dimetra IP Roaming Service.....	53
Chapter 4: Application Interfaces.....	54
4.1 3GPP Parlay X.....	54
4.1.1 Heartbeats on the Extended Parlay X Interface.....	54
4.1.2 Presence Filtering.....	55
4.1.3 IMW Network Time Synchronization.....	55
4.1.4 Parlay X Interface Capacities.....	55
4.1.5 Parlay X API Licensing.....	56
4.2 IMW REST and WebSocket Interfaces Overview.....	57
4.2.1 IMW REST and WebSocket APIs.....	59
4.2.2 IMW REST and WebSocket Interface Capacity.....	59
4.2.3 Developer Access to IMW REST and WebSocket API.....	62
4.2.3.1 Adding Application to the System.....	63
4.2.3.2 Application Types.....	64
4.2.3.3 Application Data Summary.....	65
4.3 Other Legacy Interfaces.....	67
4.3.1 Legacy PN-Watcher Interface (Presence).....	67
4.3.2 Legacy MotoLocator Web Services API.....	67
4.3.3 ASTRO 25 System LRRP API.....	67
Chapter 5: Network Configuration.....	69
5.1 ASTRO 25 System Network Configuration.....	69
5.2 Dimetra IP System Network Configuration.....	69
5.3 IMW Connectivity Within a Network Environment.....	69
Appendix A: IMW Location Archive Writer Database Disk Space Requirements.....	71

List of Figures

Figure 1: IMW System Context Overview.....	12
Figure 2: IMW with 3 API Endpoints Architecture.....	17
Figure 3: ESU Launchpad Overview.....	18
Figure 4: Access Control Settings in Configuration Manager.....	33
Figure 5: Talkgroup Range Settings.....	34
Figure 6: Services Access Control Flags.....	34
Figure 7: Auto-Provisioning based on Device Network ID Configuration.....	35
Figure 8: IMW Redundancy Architecture.....	37
Figure 9: Virtual Machine Architecture.....	41
Figure 10: ASTRO® 25 Outdoor Location Solution – High-Level View.....	47
Figure 11: Dimetra IP Short Data Reporting.....	52
Figure 12: Dimetra Inter-System Interface.....	53

List of Tables

Table 1: IMW Supported Releases and Services.....	13
Table 2: Networks and Supported Devices.....	14
Table 3: HP DL360 Gen9 Low Capacity Configuration.....	20
Table 4: HP DL380 Gen9 High Capacity Configuration.....	20
Table 5: HP DL360 Gen9 Low Tier UNS Configurations.....	21
Table 6: HP DL380 Gen9 High Tier UNS Configurations.....	21
Table 7: HP DL360/380 Gen8 Low Tier UNS Configurations.....	21
Table 8: HP DL380 Gen8 High Tier UNS Configurations.....	22
Table 9: Groups Supported by MGM.....	28
Table 10: Service Operator Roles.....	32
Table 11: Data Encryption: Radio Networks – IMW – Client Applications.....	36
Table 12: Maximum Values for IMW REST Presence Subscriptions in a Total Box Steady State.....	60
Table 13: Maximum Values for IMW REST Location Subscriptions in a Total Box Steady State.....	60
Table 14: Maximum Values for IMW REST Presence Subscriptions in a Total Box Busy Hour.....	61
Table 15: Maximum Values for IMW REST Location Subscriptions in a Total Box Busy Hour State....	62
Table 16: Application Types.....	64
Table 17: Application Data Summary.....	65

About IMW Feature Manual

This manual describes the Intelligent Middleware (IMW) platform, including an overview of the functions and capabilities, technical details of the implementation, and design considerations.

This manual provides a high-level overview of the features and functions of the IMW platform. The user of this document will find guidance on variations of IMW configurations, the platforms that support IMW, and the ability to provide redundant IMW deployments.

What Is Covered In This Manual

This manual contains the following chapters:

- [IMW Description on page 11](#) presents a general overview of IMW services, features, and supported devices.
- [ASTRO 25 System Deployments on page 43](#) describes how IMW functions in an ASTRO 25 system and presents IMW services available in an ASTRO 25 system.
- [Dimetra IP System Deployments on page 50](#) describes how IMW functions in a Dimetra IP system and presents IMW services available in a Dimetra IP system.
- [Application Interfaces on page 54](#) describes the Application Programming Interfaces (APIs) that applications may use to subscribe to receive presence updates for selected entities.
- [Network Configuration on page 69](#) gives details on how to configure the network with IMW to enable communication in different systems.

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.

Navigation Through .pdf Files

Navigating through .pdf files is much easier if you use **Previous View** and **Next View** buttons. They allow you to move directly from one place to another with one click.

You can make the **Previous View** button available in your **Page Navigation** toolbar by selecting **View** → **Show/Hide** → **Toolbar Items** → **Page Navigation** → **Previous View** from the Adobe Reader main menu. The same sequence applies to the **Next View** button.

When the buttons are available in your toolbar, you can click them to see the previous or next view in the .pdf file. For example, after jumping to another chapter using the **Bookmarks** pane, you can come back to the previous view by clicking the **Previous View** button. Similarly, after using a link to another section, you can easily move back and forth between the two pages using the **Previous View** and **Next View** buttons.

The keyboard shortcuts for the **Previous View** and **Next View** buttons are ALT + LEFT ARROW and ALT + RIGHT ARROW, respectively.



NOTICE: If the **Previous View** and **Next View** buttons are not available in your version of Adobe Reader, install the latest version of the application.

Chapter 1

IMW Description

This chapter provides a high-level description of the Intelligent Middleware (IMW) and the function it serves on your system.

1.1

IMW Overview

The Intelligent Middleware (IMW) solution is a suite of network services across different types of radio networks with a **common Application Programming Interface (API)**. Third-party applications that use this API can transparently track and communicate with wireless devices regardless of access network protocols and device types.

The IMW API is a restricted and licensed interface. Only third-party applications developed by licensed application developers may gain access to the interface. The IMW framework enables interoperability between third-party applications, such as mapping applications, and Radio Access Networks (RANs), including ASTRO® 25 systems, and Dimetra IP.

IMW APIs provide uniform access to network-level information across multiple RANs, using the following API standards in order to help maintain a set of uniform interfaces for applications to use across IMW provided services.

- The industry standard 3GPP Parlay X Web Services specifications. The 3GPP Parlay X standard uses generally accepted Simple Object Access Protocol (SOAP)-based web services technologies. The IMW interfaces are based on these standards, but also provide proprietary extensions to these interfaces. IMW Parlay X APIs provide query and subscription access to presence data and location data over HTTP or HTTPS. Requests and responses are encoded using the eXtensible Markup Language (XML) format.
- The industry standard Open Mobile Alliance (OMA) REST specifications. The OMA REST standard provides APIs similar to those defined by the 3GPP Parlay X standard, but uses generally accepted RESTful API specifications. The IMW interfaces are based on these standards, but also provide proprietary extensions to these interfaces. IMW REST and WebSocket APIs provide query access to presence and location data, group management, and messaging over HTTP or HTTPS; subscription access to presence data, location data, group data, and context data is provided over WebSockets or Secure WebSockets. Requests and responses are encoded using the JavaScript Object Notation (JSON) format.

Additional legacy interfaces are supported.

IMW Services

IMW provides a number of services to track and manage data sent by devices. The major functionalities include:

- Location Service that allows users and applications to receive device location information.
- Presence Service that allows users and applications to receive a device or user presence status.
- Multi-Group Management (MGM) Service that allows users and applications to create and manage groups and track affiliation of ASTRO® 25 devices to ASTRO® 25 talkgroups and sites, and track affiliation of Dimetra devices to Dimetra talkgroups and sites.
- Messaging Service that enables sending short messages, statuses, and attachments.
- Context Service that enables gathering, sharing, and utilizing context and personnel-related information that may be provided to IMW by additional sensors located in the system.

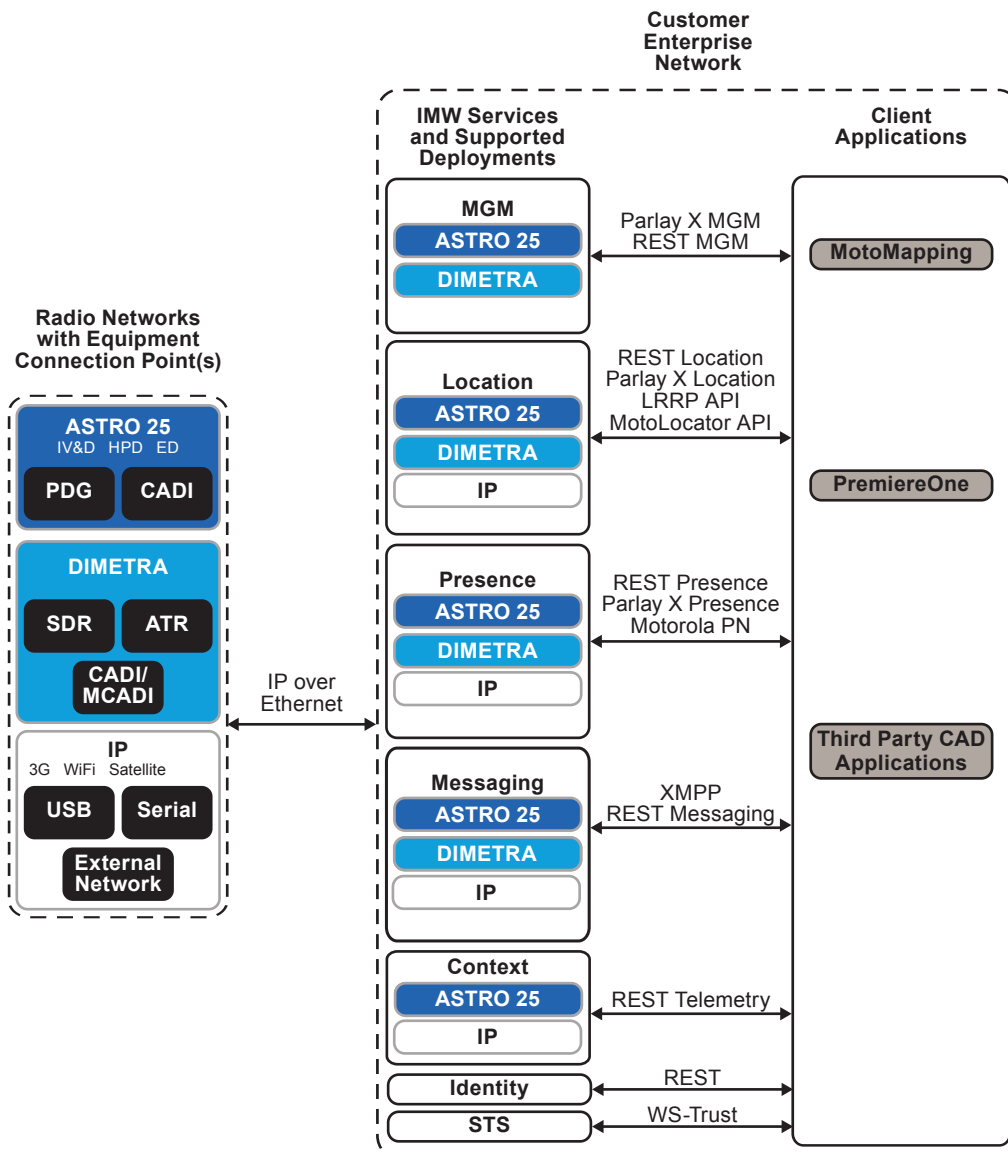
Additionally, IMW supports Identity Service that enables a secure Single Sign-On (SSO) feature for the IMW users to all the purchased services. The Identity Service provides authentication and authorization of both users and applications.

Detailed information on IMW services is provided in the following sections.

IMW may be used as a standalone, or as a sub-component of many Motorola Solutions-supported solutions, including:

- ASTRO® 25 Advanced Messaging Solution
- ASTRO® 25 Outdoor Location Solution
- POP 25
- MotoMapping
- PremierOne

Figure 1: IMW System Context Overview



1.2

IMW Supported Systems

Intelligent Middleware (IMW) provides flexible deployment options through software licensing. Customers must purchase and install the appropriate software license to enable the desired IMW functionality. All IMW services and prerequisite software is available on a DVD for installation and configuration by customers and field personnel.

Individual RANs:

- ASTRO 25
- Dimetra IP

Dual RAN systems:

- ASTRO 25
- Dimetra IP

The following features of IMW are licensed, requiring a license file be generated by back-end systems and the license file be loaded onto the IMW during installation.

- Presence Service
- Location Service
- Multi-Group Management (MGM) Service
- Context Service
- Max allowed number of devices for Presence Service
- Max Allowed Number of entities to be tracked by the Location Service

1.3

IMW Supported Releases and Services

The following table lists what ASTRO® 25 and Dimetra IP releases are supported by Intelligent Middleware (IMW). It also provides information on what OS is supported for particular deployments.

Table 1: IMW Supported Releases and Services

System Type	Releases Supported	Services Supported	OS Supported	Comments
ASTRO (North America)	ASTRO 7.4 and higher	Location Presence Identity Messaging MGM Context	Windows Server 2012 R2 Standard Edition (64-bit) Red Hat Enterprise Linux 6.6 (Messaging and Identity Servers)	Information Assurance required.
ASTRO (outside North America)	ASTRO 7.4 and higher	Location Presence Identity Messaging MGM Context	Windows Server 2012 R2 Standard Edition (64-bit) Red Hat Enterprise Linux 6.6 (Messaging and Identity Servers)	Information Assurance required when certified hardware is purchased.

System Type	Releases Supported	Services Supported	OS Supported	Comments
TETRA	Dimetra 8.0 (DIPS) and higher	Location Presence Identity MGM	Windows Server 2012 R2 Standard Edition (64-bit)	Full Information Assurance or Transparent IA available.

1.4

Networks and Supported Devices

The following table lists examples of devices that report location. The networks from which the Location Service receives location reports are established by configuring the service for each device.

Table 2: Networks and Supported Devices

Network	Supported Devices
ASTRO® 25	<ul style="list-style-type: none"> APX Portable/Mobile devices (including APX 1000, APX 2000, APX 4000, APX 6000, APX 6000 XE, APX 6000 Li, APX 6500, APX 6500Li, APX 7000, APX 7000L, APX 7000XE and multi-band) with internal GPS module. XTS 5000/XTS 2500 ASTRO® 25 system portable radios with the GPS Remote Speaker Microphone (GPS RSM 1.0 and GPS RSM 2.0). HPD 1000 Data Modem with integrated GPS. Placer 450, Placer TrimFleet APU and MW800, Trimble Placer™ Gold APU and Trimble Placer™ Gold DRU Plus connected directly to an ASTRO® 25 Mobile Radio, including the XTL 5000, XTL 2500, XTL 1500 and ASTRO® Spectra Plus™. Placer Gold APU and Placer Gold DRU Plus connected to a Mobile Data Terminal that is connected to an ASTRO® 25 mobile radio. Cellocator Olympic for ASTRO connected to a Mobile Data Terminal (MDT) that is connected to an ASTRO® 25 Mobile Radio, including the XTL 5000, XTL 2500, XTL 1500, and ASTRO® Spectra Plus™. Cellocator Olympic for ASTRO connected to an ASTRO® 25 APC Mobile Radio. Cellocator Olympic for ASTRO connected to a Mobile Data Terminal that is connected to an HPD 1000 Data Modem with integrated GPS.
WiFi & 3G	MW800(XP), MW810(XP), ML910(XP), MC35, MC55, MC75
Dimetra IP	<ul style="list-style-type: none"> MTP810, MTP830, MTP850, MTP3100, MTP3150, MTP3200, MTP3250, MTP3500, MTP3550, MTP5200, MTM5400, MTM5500, MTP6450, MTP6550, MTP6750, MTP8500EX, MTP8550EX, MTH800, MTM800, TCR1000 OEM Modem TOM100 Barrett 2050 Transceiver CM5000, CM9000 Codan NGT Darim PVE

Network	Supported Devices
	<ul style="list-style-type: none"> • MCNF RFID, Axis MDVR, Milestone, ML910, MW810, MW800 • TrakM8 SOLO, TrakM8 T8 • SRH3500W, SRH3900 • SRP2000 • THR880i • Thuraya XT Satellite phone
MOTOTRBO™	MOTOTRBO™ DP and DM: XPR 6350, 6380, 6550, 6580, 7350, 7550

1.5

Third-Party Software Components

Intelligent Middleware (IMW) is dependent on a number of third-party software components for proper operation.

Virtualization Support

IMW server and other supporting servers, such as Identity and Messaging are implemented as virtual machines on the hardware platform using the VMware ESXi 5.5 technology. Virtual machine environments benefit the IMW owner because they are isolated from other applications running on their own virtual machines in the same server. This way, IMW, and other applications do not interfere with each other in the event of failure. The goal of deploying virtual machines is to reduce the number of physical servers required while maintaining the separation between applications.

Operating System

IMW platform is virtualized with some components running on Microsoft Windows Server 2012 R2 64-bit (IMW core, SQL server, and API Endpoints) and others on Red Hat Enterprise Linux 6.6 (Messaging and Identity Server). Only the English language version is supported.

Microsoft SQL Server

IMW uses Microsoft SQL Server to store provisioned information (for example, Device IDs). IMW can operate with two different versions of SQL Server: Express and Standard. Both versions are Microsoft SQL Server 2014 with Service Pack 1 (64-bit).

Larger and more complex IMW deployments may require SQL Server Standard edition. SQL Server Standard edition is **required** if one of the following conditions is met:

- IMW is deployed in the redundant configuration.
- IMW Location Archive Writer is used.
- IMW is used with MotoMapping and more than 100 devices.

SQL Server Standard edition is installed on a separate Windows Server 2012 virtual machine dedicated only for the SQL database.

1.6

IMW Software Components Overview

Intelligent Middleware (IMW) platform is virtualized and consists of such network components as IMW Core, IMW API Endpoints (AEs), Database Server, Identity Server, and Messaging Server. The actual set of the virtualized components varies depending on the deployment.

IMW Core

The IMW Core virtual machine controls the services of IMW system. The IMW Core virtual machine resides on the IMW server and provides legacy interfaces (Parlay X, LRRP API, MotoLocator), LMR radio interfaces (to or from ASTRO and Dimetra), group management, context data, backup, and restore functionality, as well as IMW Configuration UI. The following are the components that may reside on the IMW core virtual machine:

- Location Service
- Presence Service
- GeoFence Service
- Multi-Group Management (MGM) Service
- Context Service
- Messaging Gateway
- Domain Name Server

Each IMW Core virtual machine hosts Domain Name Server that makes a use of Microsoft Domain Name System. By default, the IMW DNS is disabled and activates while configuring the IMW clusters, or in the case of ASTRO® 25 redundant configurations, when setting up the IMW redundancy. All the configuration data for IMW DNS is derived from IMW Configuration Manager. The IMW platform is assigned a fixed DNS name through which it may be reached from the Customer network.

The IMW Core hosts the following applications that are used to manage and configure the IMW system:

- IMW Configuration Manager
- IMW Administrative Client
- IMW Web Location Administrative Client

IMW API Endpoints

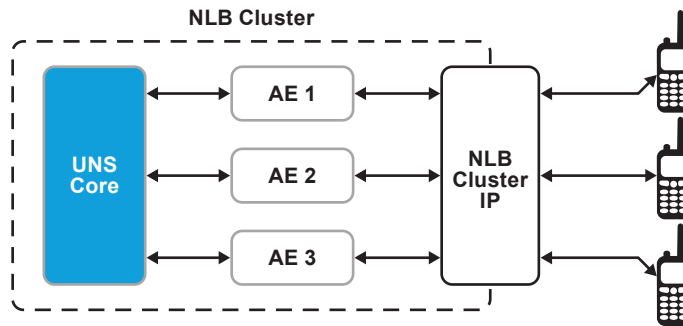
IMW API Endpoints are special purpose virtual machines designed to meet the need for handling a large number of subscriptions, for example. Having multiple AE virtual machines enables IMW to upscale the overall load of distributing notifications and handling queries (for presence, location, groups, and context) from several thousands of watchers. AE virtual machines are where the REST and WebSocket APIs are handled by the IMW.

IMW with AEs can be installed in the following configurations:

- IMW core virtual machine and up to three AE virtual machines
- AE services are installed on the IMW virtual machine with the other services

All AE virtual machines are clustered using Microsoft Network Load Balancing (NLB). Each virtual machine has its own dedicated IP address for internal communication and a shared cluster IP for external communications. All applications communicate with IMW using the cluster IP and the subscriptions are distributed among AEs by NLB.

Figure 2: IMW with 3 API Endpoints Architecture



In the ASTRO® 25 redundant deployments, NLB cluster is assigned IMW Customer IP, which is shared between the two IMW servers (active and standby).

AE interface is expected to consume a lot of bandwidth as it is reporting the Presence, Location, Group, and Context data of many devices.

IMW Database, Identity, Messaging, and Additional Components

The IMW Core virtual machine communicates with such virtualized components as: Database Server, Identity Server, Messaging Server.

Database Server

SQL Database server gathers information about the devices and users. In configurations with IMW Redundancy and Location Data Archiving, SQL Standard edition is required.

Identity Server

Identity Server is a separate Linux virtual machine that collects user credentials, validates authenticity of the user, and provides a token for authenticated users.

Messaging Server

Messaging server is a separate XMPP Linux virtual machine.

The IMW platform can be installed with such additional components as Advanced Messaging Solution (AMS) and Priority Management Solution (PMS). The AMS virtual machine is installed only for deployments within ASTRO® 25 network system. For more information on available network configurations, see [IMW 5.2 Installation Configurations on page 21](#).

Advanced Messaging Solution

AMS is a PremierOne based solution that delivers messaging to ASTRO® 25 subscriber units.

Priority Management Solution

The Priority Manager Application, residing within the Linux virtual machine, is designed as an agency-level application to prioritize data based on the user roles, applications, and incident priority (provisioned in the IMW Configuration Manager).

1.7

ESU Launchpad Overview

ESU Launchpad is a web-based framework that facilitates IMW installation by providing a central point for configuring and managing IMW installation scenarios, and monitoring installation progress of the IMW components.

ESU Launchpad platform consists of:

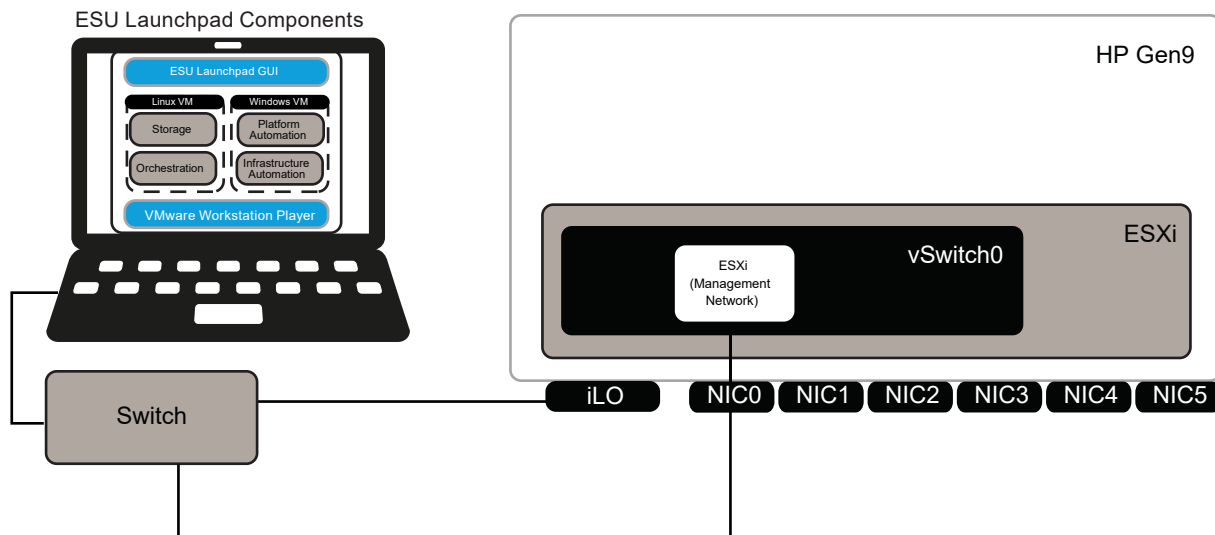
- ESU Launchpad web-based interface
- VMware Workstation Player

- Red Hat Enterprise Linux 64-bit virtual machine that is used for storing installation files and installation orchestration
- Windows 7 64-bit virtual machine that is responsible for platform and infrastructure automation

ESU Launchpad does not include the IMW software. The software needs to be obtained and uploaded to ESU Launchpad storage before installation.

ESU Launchpad is installed on a Windows service laptop, which is connected to an ESXi server through a switch. ESU requires a Layer 2 connectivity to the ESXi NIC and iLO NIC. ESU Launchpad allows for configuring connectivity with the server when ESXi, iLO, and IMW virtual machines are on different subnets.

Figure 3: ESU Launchpad Overview



ESU allows for the automation of the following configuration and installation operations:

- ESXi configuration
- iLO and BIOS configuration for HP Gen9 servers
- datastore creation
- virtual machine deployment and basic configuration
- IMW software installation, including Windows Supplemental Configuration and MotoMapping server installation

ESU Launchpad Software and Hardware Requirements

System requirements:

- Operating system: 64-bit Windows 7, 8, 8.1, 10
- 64-bit x86 Intel Core 2 Duo Processor or equivalent/AMD Athlon™ 64 FX Dual Core Processor or equivalent (1.3 GHz or faster core speed)
- 6 GB RAM or more
- 80.5 GB of free disk space
- 1000 Mbps Ethernet adapter
- Firefox v. 29 or later

Firefox is recommended for the best performance during software uploading. It has 10 times better performance than other browsers.

- Enabled Virtualization Technology (VT) in BIOS.

Running ESU Launchpad without VT enabled is not possible as you cannot power on a 64-bit virtual machine. For more information, see <https://kb.vmware.com/kb/1003944>.

For instructions on how to enable VT, see the vendor documentation for your laptop model.

1.8

IMW Network Setup Overview

The following is summary of the network addresses employed by the Intelligent Middleware (IMW) platform.

Each of the virtual machine requires two IP addresses, one for each network interface. UNS_APP and MGMT addresses are configured while the IMW installation:

UNS_APP

Interface that is used to communicate with the applications and clients, other virtual machines on the server, or the redundant inter-IMW traffic.

MGMT

Interface that is used to communicate non-application functionality with the IMW core such as communication with ESXi, remote logon, sending traps, and error log reporting.

Addresses and DNS names

Applications and radio devices communicate with the IMW using the following addresses that are configured in the IMW Configuration Manager:

IMW Customer IP

One of the base addresses used by ASTRO® 25 devices and third-party applications to access the IMW.

IMW Customer Fully qualified Domain Name

One of the base names used by applications, ASTRO® 25 devices to access IMW.

IMW DNS IP Address

DNS IP address is used by external applications and clients to resolve the IP addresses of the IMW platform components (such as API Endpoints, Database Server, Identity Server, Messaging Server, Advanced Messaging Solution, Priority Management Solution). The IMW DNS IP address points to IMW Core virtual machine and cannot be configured. To access the IMW externally through the FQDN address, the external DNS requires configuration.



NOTICE: The IMW and Dimetra redundant configurations require additional Customer IP, FQDN, and DNS addresses. In the case of ASTRO® 25 redundant deployment, only one Customer IP and FQDN are used.

1.9

Hardware Component Configuration

This section specifies hardware configurations for Intelligent Middleware (IMW), including HP ProLiant DL360 and HP ProLiant DL380 servers.

Hardware Component Configuration for New IMW Deployments

Table 3: HP DL360 Gen9 Low Capacity Configuration

Hardware Specification	Description
Server Model	HP ProLiant DL360 Gen9
Processor	Intel® Xeon® processor E5-2620v3 (2.4 GHz/6-core/15 MB/85 W)
Expansion Card	HP Smart Array P440ar/2 GB FBWC 12 Gb 2-ports Int FIO SAS Controller
System Memory	32 GB total memory (4 x 8 GB Single Rank x 4 DDR4-2133)
Hard Disks	2400 GB Total Raw Disk Space (4 x 600 GB SAS 10K rpm SFF (2.5-inch))
Optical Disks	HP DL360 Gen9 SFF DVD-RW/USB Kit
Removable Storage	8 GB microSD EM Flash Media Kit
Networking	4 NICs (Embedded 4x1 GbE Network Adapter)

Table 4: HP DL380 Gen9 High Capacity Configuration

Hardware Specification	Description
Server Model	HP ProLiant DL380 Gen9
Processor	2 x Intel® Xeon® processor E5-2680v3 (2.5 GHz/12-core/30 MB/120 W)
Expansion Card	HP Smart Array P440ar/2 GB FBWC 12 Gb 2-ports Int FIO SAS Controller
System Memory	128 GB total memory (16 x 8 GB Single Rank x 4 DDR4-2133)
Hard Disks	9600 GB Total Raw Disk Space (supports up to eight 1.2 TB 6G SAS 10K rpm SFF (2.5-inch) SC)
Optical Disks	HP 9.5 mm SATA DVD-RW JackBlack G9
Removable Storage	8 GB microSD EM Flash Media Kit
Networking	16 NICs (1 x embedded HP Ethernet 1 Gb 4-port 331i Adapter, 1 x HP Ethernet 1 Gb 4-port 331FLR Adapter, 2 x HP Ethernet 1 Gb 4-port 331T Adapter)

1.10

IMW 5.2 Installation Configurations

Depending on the hardware used, Intelligent Middleware (IMW) 5.2 can be installed in one of the following configurations:

Table 5: HP DL360 Gen9 Low Tier UNS Configurations

UNS Configuration	Virtual Machines	SQL Database Edition	Supported Radio Networks
UNS 5.1 Low Tier G9, Standard	UNS Core Database Server Identity Server (low) Messaging Server*	Express	ASTRO® 25 Dimetra IP
UNS 5.1 Low Tier G9, Standard + Data Archiving Includes the UNS Location Archive Writer and supports redundant installations.	UNS Core Database Server Identity Server (low) Messaging Server*	Standard	ASTRO® 25 Dimetra IP
* Messaging Server virtual machine is deployed, but not supported in Dimetra IP system.			

Table 6: HP DL380 Gen9 High Tier UNS Configurations

Configuration	Virtual Machines	SQL Database Edition	Supported Radio Networks
UNS 5.1 Hi Tier G9, Standard	UNS Core UNS API Endpoint (x 3) Database Server Identity Server Messaging Server*	Express	ASTRO® 25 Dimetra IP
UNS 5.1 Hi Tier G9, Standard + Data Archiving Includes the UNS Location Archive Writer and supports redundant installations.	UNS Core UNS API Endpoint (x 3) Database Server Identity Server Messaging Server*	Standard	ASTRO® 25 Dimetra IP
* Messaging Server virtual machine is deployed, but not supported in Dimetra IP system.			

Table 7: HP DL360/380 Gen8 Low Tier UNS Configurations

UNS Configuration	Virtual Machines	SQL Database Edition	Supported Radio Networks
UNS 5.1 Low Tier Dimetra G8, Standard	UNS Core	Express	Dimetra IP

UNS Configuration	Virtual Machines	SQL Database Edition	Supported Radio Networks
	Database Server Identity Server (low) Messaging Server* (low)		
UNS 5.1 Low Tier Dimetra G8, Standard + Data Archiving Includes the UNS Location Archive Writer and supports redundant installations.	UNS Core Database Server Identity Server (low) Messaging Server* (low)	Standard	Dimetra IP
UNS 5.1 Low Tier Astro G8, Standard	UNS Core Database Server Identity Server (low) Messaging Server* (low)	Express	ASTRO® 25
UNS 5.1 Low Tier Astro G8, Standard + Data Archiving Includes the UNS Location Archive Writer and supports redundant installations.	UNS Core Database Server Identity Server (low) Messaging Server* (low)	Standard	ASTRO® 25
* Messaging Server virtual machine is deployed, but not supported in Dimetra IP system.			

Table 8: HP DL380 Gen8 High Tier UNS Configurations

Configuration	Virtual Machines	SQL Database Edition	Supported Radio Networks
UNS 5.1 Hi Tier G8, Standard	UNS Core Database Server Identity Server Messaging Server	Express	ASTRO® 25
UNS 5.1 Hi Tier G8, Standard + Data Archiving	UNS Core Database Server Identity Server Messaging Server	Standard	ASTRO® 25

1.11

IMW Features and Services

The following chapter presents an overview of the available services and provides an introduction to the features and functions provided by Intelligent Middleware (IMW).

1.11.1

Services Overview

Intelligent Middleware (IMW) offers a variety of data services such as Location, Presence, Group Management, and Authentication that can be leveraged by client applications using the IMW interfaces.

Main IMW Services

Location Service

Location Service is a resource tracking solution that obtains geographic coordinates from User Equipment to enable operators to locate and track outdoor personnel and vehicles. Location Service provides the ability for third-party applications to monitor and archive the current location of GPS-based location reporting devices that are deployed in different types of Radio Access Networks (RANs).

IMW offers additional functionalities connected to the Location Service. For more information, see [Location-Based Modules Overview on page 25](#).

Presence Service

Presence Service provides the ability for an application to receive device and user presence data. The Presence Service also supports tracking the presence of devices and users across ASTRO® 25, and Dimetra IP networks, and permits applications to support any of these networks by providing a single API to application developers for presence information.

Messaging Service

The Messaging Service is a solution for LMR systems that enables exchanging short messages and attachments between Land Mobile Radio (LMR) devices as well as sending messages to a group of devices when used with the Multi-Group Management (MGM) service.



NOTICE: Attachments cannot be sent to LMR radios.

Context Service

The Context Service enables gathering, sharing, and utilizing information that may be provided to Intelligent Middleware (IMW) by sensors located in the system. Dispatchers benefit from the solution by receiving context and personnel-related information such as discharge of a weapon and battery level of a device. The Context Service is available for ASTRO® 25 system.

GeoFence Service

The Intelligent Middleware (IMW) Geofence API provides a set of operations to manage geofences on the IMW. An operator can define the area (shape) of a geofence, the set of devices targeted by that geofence, and the actions to be performed when devices enter or exit the selected area.

Group Management

Multi-Group Management Service

The MGM Service provides a single entry point for group management across all radio systems (Dimetra IP, and ASTRO® 25). The MGM Service supports statically provisioned groups, application and user created groups, LMR talkgroups, and LMR sitegroups. Client applications can subscribe to groups, manage them, and receive notifications about added/removed users or devices in a group. The groups (other than LMR talkgroups and LMR sitegroups) can contain a mix of users,

devices from different RANs and other groups. When combined with the Messaging Service, the MGM allows an application or user to send a message or an attachment to a group of users.

Authentication Services

Identity Service

The IMW supports client authentication and authorization using OAuth Access Tokens issued by the OAuth Provider residing on Identity Server. Identity Server is a separate virtual machine dedicated to providing authorization and authentication services to IMW API client applications. The Identity Service is responsible for validating that client applications can be granted access to resources on the IMW server.

Roaming Services

Dimetra IP Roaming

The Dimetra Inter-System roaming feature allows foreign devices to roam between TETRA systems and obtain Group Calls, Private Calls, and Short Data Service in a system which is not their Home System. The following IMW services are available for foreign devices:

- Presence Service
- MGM Service

1.11.2

Location Service Overview

Location Service is a resource tracking solution that uses Global Positioning System (GPS) satellites to enable operators to locate and track outdoor personnel and vehicles.

The Location Service provides the ability for third-party applications to monitor and archive the current location of GPS-based location reporting devices that are deployed in different types of RANs. The service acts as a gateway, translating location data received from mobile device messages and forwarding the data to interested applications.

The Location Service retains compatibility with existing ASTRO® 25 and Dimetra IP application interfaces.

Implementation of the IMW 3GPP Parlay X interface requires upgrading applications that use prior implementations. This adds a new mechanism to report the result of multiple device requests when one or more device updates fail.

The Location Service also has the following functions:

- Receives and decompresses location data from GPS devices using disparate protocols, then translates and rebroadcasts the data using a unified protocol.
- Simplifies application development by providing a single integration point for location and telemetry information for all Motorola devices that are supported on the networks.
- Provides intelligent routing of messages by managing requests to the devices. For devices supported by the Presence Service, Location Service ensures that no messages are sent to absent devices and that multiple requests of the same type are not sent to the same device. By managing requests, the Location Service reduces traffic on the network.
- Ensures idle reporting for devices that do not use the Presence Service so that devices are kept in contact with the location application.
- Enables auto-request location reporting of new devices so that the developer does not have to manually enter that request at the mapping application.



NOTICE: If two applications attempt to change the location reporting rate for the same device, the device reports at the rate requested by the last application

1.11.2.1

Location on Push to Talk

The Location on Push to Talk (PTT) is a unique feature for APX trunking radios. It utilizes an embedded signaling mechanism to allow the currently transmitting subscriber to send location data during a voice call.

Other location reports, such as Periodic Location Updates or Location on events, can occur only when the subscriber is not participating in a voice call. These reports, if configured, are queued and sent after the call ends, provided they do not stay in the queue longer than their Queue Dwell Time. If a Periodic Location Update stays queued longer than its Queue Dwell Time, it is discarded and not sent after the voice call ends.

A single press of the PTT button generates one location report. The Location on PTT feature does not keep updating subscriber location during the group voice call. However, every new voice transmission sends a new location report. Thanks to this, the feature provides a more timely representation of the real-time position of the transmitting subscriber in situations that require a lot of quick voice calls, for example during a high-speed car chase scenario.

The Location on PTT requires A7.17 or later ASTRO@ 25 infrastructure and subscribers.

Per Agency, Location on PTT is configurable in the following options:

- Disable
- Enable for all group calls including emergency calls
- Enable only for emergency calls

Once a subscriber starts to transmit in a voice group call, the location information is received after 2 to 7 seconds, depending on the mapping application loading.

Altitude is not available for Location on PTT.



NOTICE:

The location updates in this solution are not encrypted - Motorola Solutions cannot guarantee the privacy of location information.

1.11.2.2

Location-Based Modules Overview

The additional Intelligent Middleware (IMW) Location modules usability for a specific system varies. This section provides a brief overview of these modules and lists the applicable installation and configuration procedures. See the Intelligent Middleware *Software Installation and Administration Guide* for specific details on configuration.

Event Service

Receives all significant events occurring in the Location Service system and manages what happens when these events occur. This functionality is unavailable on the 3GPP Parlay X web services API. The services provided by the Event Service are available only with the legacy MotoLocator API.

Boundary Service

Receives a feed of location updates from the Location Service and checks whether certain boundary conditions have been violated. Boundary Service can raise events based on geofence violations, speed violations, excessive idle time, and changes in trigger and device state. Using the MotoLocator web services API, third-party applications can set up geofences and subscribe to location-based events. The services provided by the Boundary Service are available only with the legacy MotoLocator API. Type of events that can be triggered when a boundary condition is detected include, but are not limited to:

- Callouts to MotoMapping
- Callouts to third-party applications

- Transmissions of an over-the-air message
- Transmissions of a Simple Network Management Protocol (SNMP) alarm
- Change of the talkgroup a device is a member of (ASTRO only)

The service is installed as part of the IMW suite installation.



NOTICE: To use the **Spatial** and **Geo Select** boundary conditions, and the **GeoFencing** feature, you must have MotoMapping software. For more information about MotoMapping and for MotoMapping installation procedures, see *MotoMapping User Guide*. The **Geo Select** feature is available only in ASTRO systems.

Text Service

Text Service is a one-way text messaging service that integrates to AMS. It allows the configuration of the Event Service to send text messages as an action within the Event Service.

Archive Writer

Stores location history. It allows archiving history data and also creates a backup of the location history data. Archived location reports may be useful in forensic investigations. You may configure archiving for a specified time period (days of data in each archive file online). Reports are purged after a configurable time period. Customers are responsible for backing up data onto an appropriate medium and storing it safely offsite.

1.11.2.3

IMW Telemetry

As well as tracking the location of a device, Intelligent Middleware (IMW) provides telemetry support for Cellocator Olympic for ASTRO and for TrakM8 SOLO and T8 devices over ASTRO® 25 or Dimetra IP networks to track the status of GPIO pins on target devices using an appropriate API.

The following APIs are used:

- Parlay X for any device type
- LRRP for (ASTRO® 25 system) Cellocator Olympic for ASTRO
- ML Web services for (Dimetra IP) TrakM8

For the Cellocator Olympic for ASTRO device the following telemetry capabilities are available:

- Five digital inputs can be used to interface with sensors (like ignition or door) in a vehicle.
- Two digital outputs can be used to interface with actuators (like control sirens, lights or blinkers) in a vehicle.
- One analog input can be used for battery measurement.

1.11.2.4

REST-based Location Reporting Triggers

End user Land Mobile Radio (LMR) devices are able to trigger location reports depending on specific conditions. By sending REST requests to devices, external applications can change the way a target device reports its location to receive reliable and accurate location information on incidents or emergencies.

This feature is available for Dimetra IP system. Control Room Operator can control the location reporting behavior of an individual target device with REST PUT requests. A separate request can be sent to delete all triggers. The location updates contain information about the reason of report.

The following location report configurations are supported:

Trigger Location on PTT

A configuration that allows sending location reports with Push-to-Talk (PTT) button.

Trigger Location on Emergency

A configuration that allows sending location reports with Emergency button.

Location Triggers

Location report interval can be specified in seconds or meters. For example, a device can be set to send reports every 10 seconds or 100 meters.

Time Threshold Limitation

A configuration that allows to set a maximum frequency of location reports. Regardless of other settings, the device will not report location more frequently than the value specified for time threshold limitation.

If a trigger is sent to a radio that is currently unavailable in the system, the request is stored and delivered once the radio is back in the network. The Control Room Operator is notified that the request has been sent.

1.11.3

Messaging Service

The Messaging Service enables sending short messages, statuses, and information. It is supported for the following geographically redundant and non-redundant radio system configurations:

- ASTRO® 25 Systems
- Land Mobile Radio (LMR) devices

The new communicator allows participating in IMW communication groups based on MGM (Multi-Group Management). IMW supports messaging using a REST API or an XMPP library.

The Messaging Service enables sending information to a group of devices and users based on MGM. For example, a dispatcher can send a message to all the users in a given group, instead of sending it individually. When some users or devices belong to one group, they are also members of the IMW communication group. Changing the group membership entails changing the IMW communication group membership. All devices and users in an ASTRO® 25 system may also send a message to all devices or users in a given talkgroup or ASTRO® 25 sites but it is not enabled by Messaging Service. It is enabled by AMS Standalone.



NOTICE:

- AMS does not support geo-redundancy or high availability (HA).
- AMS does not use MGM for group messaging, it uses the PremierOne group management messaging.

The Messaging Service is available for multiple agencies.

A Linux server based on Extensible Messaging and Presence Protocol (XMPP) as well as API Endpoints are provided as part of the IMW system to service all REST APIs for Messaging (REST only), Presence, Location, and MGM.

If messaging is integrated with the AMS, then additional configuration of the Simple Mail Transfer Protocol (SMTP) server parameters on the IMW core is required.

If messaging is integrated with a Dimetra system, then additional configuration of the Short Data Router (SDR) connection parameters on the IMW core is required.

Dimetra Messaging users are logically bound to devices in the Configuration Manager. Static mapping of a user to a device allows reaching the user by sending messages to the device or devices the user is logged on to.

For Dimetra devices to use the Messaging Service, the device messaging application must be programmed with the SDR Connection ISSI of the Messaging Host as the Store and Forward Server and the SDS to Phone option selected in the Customer Programming Software (CPS).

The number of users enabled for messaging is defined by server licenses.

For more information on the Messaging Service in IMW, see the IMW *Installation and Configuration* webhelp.

1.11.4

Multi-Group Management Service

Multi-Group Management (MGM) is a group definition service that supports all of the systems (DIMETRA IP, and ASTRO® 25). MGM provides a comprehensive view of users, groups, and devices across multiple networks. The MGM service supports statically provisioned groups, application and user created groups, and Land Mobile Radio (LMR) groups. The groups (other than LMR talkgroups and LMR sitegroups) can contain a mix of users, devices from different Radio Access Networks (RANs) and other groups. Client applications can subscribe to groups, manage them, and receive notifications about added/removed users or devices in a group. Such services as Messaging, Location, Presence, and also third-party applications can use the group definitions provided by the MGM service.

The MGM service uses REST-based API, which distinguishes two types of clients:

Users

Affiliated with a person. Multiple devices can be assigned to one user.

Applications

For example, CAD console.

In the case of Dimetra IP system deployments, third-party applications may also query membership of a particular PTT talkgroup or RF site using the MGM Parlay X API.

Group Lists

Users and Applications can query and subscribe to their group lists.

For Users

Group List is the list of Static Groups and Application Groups in which the User is a group member, the Static Groups that the User is authorized to use, and the Application Groups the User is authorized to use and manage.

For Applications

Group List is the list of Static Groups that the Application is authorized to use and the Application Groups that the Application is authorized to use and manage.

Groups Supported by MGM

Table 9: Groups Supported by MGM



NOTICE: The access to some operations may be restricted based on the authorization scopes that have been imposed on the client.

Group Type	Created by	Allowed Members	Allowed Client Operations
Static Groups	Agency and Group Operators through the IMW Configuration Manager	Users, LMR Devices	<ul style="list-style-type: none">Querying for the current members of those groupsSubscribing for notification reporting changes in the current members of those groups
Application Groups	Users and Applications using API	Users, LMR Devices, and/or other groups	<ul style="list-style-type: none">Querying for the current members of those groups

Group Type	Created by	Allowed Members	Allowed Client Operations
			<ul style="list-style-type: none"> Managing (creating and deleting) groups Adding and removing members and referenced groups from Application Groups Nesting Applications Groups (maximum 2 level) Subscribing for notification reporting changes in the current members of those groups Changing group display name and subject
LMR Talk-groups and Sitegroups	Dynamically updated from LMR TG and location affiliation	LMR devices	<ul style="list-style-type: none"> Querying for the current members of those groups Subscribing for notification reporting changes in the current members of those groups

1.11.5

Context Service Overview

Context Service enables gathering, sharing, and utilizing information that may be provided to Intelligent Middleware (IMW) by sensors located in the system. Sensors are data capturing devices that report on a specific measurement such as discharge of a weapon and battery level of a device. Dispatchers benefit from the solution by receiving context and personnel-related information.

The IMW Context Service is available for ASTRO® 25 system. LEX L10 (Cascade) devices may be paired with sensors providing context-related data. APX radios are limited to such solutions as measurements on the battery charge level.

The following are available sensor types:

Firearm Sensor

Delivers telemetry for real-time event-awareness:

- Holster/Unholster - Dispatcher is immediately notified when an officer unholsters their weapon.



NOTICE: In non-emergency situations, for example, when an officer removes weapon before entering court, **Disarm** button is used to prevent the IMW from sending alerts to applications.

- Discharge - Alerts are immediately sent to dispatch when an officer discharges their weapon.

Battery Charge Sensor

Provides data on the battery level of a device.

Devices linked with sensors transmit the sensor related data over-the-air (OTA) to the IMW system with the use of Sensor Request Response Protocol (SRRP), which is a Motorola proprietary protocol.

The sensor related information can be associated with Sensor Profiles in the IMW Configuration Manager. Sensor Profiles allow the operator to specify sensor triggers such as discharge of a weapon and low battery level of a device. One trigger is configurable for each sensor.

Applications such as, Computer Aided Dispatch (CAD), other Motorola and third-party applications, can access and use the sensor related data via an API.

For more information, see the following sections in the Intelligent Middleware *Configuration Manager User Guide*:

- "Adding and Editing Sensor Profiles"
- "Configuring SRRP"

1.11.6

Identity Service Overview

Identity Service is a solution that manages user authentication, authorization, and controls access to IMW services.

Identity Service enables a secure Single Sign-On (SSO) feature for the IMW users to all the purchased services. Instead of logging to each service separately, a user provides their credentials only once, in return, the Identity Server assigns an OAuth Access Token which is used by the Application Server throughout the authentication session. As long as the user stays logged in, the provided token is the source of authentication.

Identity Service Components

Identity Client

Allows the device to communicate with the Identity Server. After a Single Sign-On, the Identity Client requests tokens which later enable the user to access multiple services without further logons.. For safety reasons, Identity Client accepts requests only from applications signed with the MSI key and does not save any user credentials. Identity Client manages and caches tokens received from the Identity Server and broadcasts tokens, logon, and logoff notifications.

Identity Server

Is a separate virtual machine that provides authorization and authentication services to IMW API client applications. Identity Server issues OAuth 2.0 Access Tokens to the API client after successfully authenticating the resource owner and obtaining authorization. The provided Access Token has to be included in each API message as it communicates the authorization scopes of the user to IMW services.

Identity Service Features

Single Sign-On (SSO)

SSO enables secure access to IMW services with only one logon.

Security Token Service

Assigns OAuth 2.0 tokens to the authentication sessions.

Federation

Enables access to IMW services across multiple agencies. Once the system administrator from Agency A grants access to a user from Agency B, the user can log on using Agency B credentials and use Agency A resources.

Certificate Authentication

Replaces standard logon with user certificate authentication

1.12

IMW Functions

This section provides an introduction to the functions provided by Intelligent Middleware (IMW).

In addition to providing , Presence, and Location services, IMW provides the following platform level services:

- Configuration
- Fault Management

- Security

1.12.1

Configuration Functionality

This section describes the tools provided by IMW to administer the system.

1.12.1.1

IMW Configuration Manager

The Intelligent Middleware (IMW) Configuration Manager is a web-based application that can be used to manage (create, update, delete, and view) the following ASTRO® 25, and Dimetra IP services configuration:

- Location
- Presence
- GeoFence
- Multi-Group Management (MGM) Service
- Context
- Registrar
- Security Token Service (STS)
- Messaging

The IMW Configuration Manager functions also include:

- Configuration and management of objects essential for providing proper support to the application users (that includes licenses, radio systems, agencies, devices, service operator accounts, and Applications accounts.)
- Distribution of configuration settings to IMW components.
- Adding and deleting sensor profiles, modification of triggering values.

Once the configuration is created or modified, it should be full or delta downloaded to IMW for the configuration to take effect. Certain configuration changes require IMW services restart via the UNS Administrative Client interface.

1.12.1.2

UNS Administrative Client

The Unified Network Services (UNS) Administrative Client controls essential aspects of the IMW operations.

A Box Admin Service operator account can login into **UNS Administrative Client** interface to perform the following IMW Box-specific functions:

- View and control the status of IMW services, such as Presence, Location, and MGM
- View and manage certificates
- Configure, view, and export log files

1.12.1.3

UNS Web Location Administrative Client

Unified Network Services (UNS) **Location Administrative Client** is a web-based application that enables access to the system by users who represent tenant agencies of the IMW, such as police and fire departments that share the IP infrastructure.

IMW retains provisioned UNS Location Administrative Client user credentials, RAN device identity information and the configured behavioral information in a Microsoft SQL database. The IMW system administrator controls the database and performs backup and restoration through the **UNS Administrative Client**. The UNS Location Administrative Client provides authorized users commands to:

- Provision telemetry message content meanings (location must be deployed), for example Speed Threshold Exceeded or System Alarm for Low Battery
- Configure Boundary and Event services

IMW retains provisioned UNS Web Location Administrative Client user credentials, RAN device identity information, and the configured behavioral information in a Microsoft SQL database. The IMW system administrator controls the database and performs backup and restoration through the UNS Administrative Client commands.

1.12.2

Fault Management Functionality

This section describes the Intelligent Middleware (IMW) features that let agencies monitor the continuous operation of the IMW system.

- Centralized Fault Reporting – IMW reports faults on an SNMP v1 and SNMP v3 interfaces. You can define IP addresses for up to two fault managers and configure IMW to report faults to existing fault management systems.
- Logging/Auditing – IMW records log files to recognize and localize faults in the IMW system. For procedures related to logs, see the “UNS Administrative Client Description” section of the *Intelligent Middleware Software Installation and Administration Guide*.
- Monitoring the status of each service – the UNS Administrative Client allows the IMW administrator to view and control the current operational status of all of IMW services.

1.12.3

Security Functionality

The following sections describe the control of access to Intelligent Middleware (IMW) by administrators, applications or users of the IMW as well as using supplemental configuration of the IMW system at installation time.


1.12.3.1

Administrator and User Authorization

Each organization administers the Intelligent Middleware (IMW) by assigning different roles to service operators. The following are available types of service operator accounts in IMW Configurations Manager:

Table 10: Service Operator Roles

Role Name	Description
Super User	The operator assigned to this role can execute any operation allowed in the IMW Configuration Manager, including man-

Role Name	Description
	<p>agement of other accounts. A Super User account operator is also enabled to access the UNS Administrative Client.</p> <p> NOTICE: An account with Super User role is created automatically after system installation so that the system administrator can start working immediately.</p>
Agency Operator	The operator assigned to this role administrates an agency and has rights to update any data related to that agency. This type of operator is able to access MotoMapping and any third-party application that uses the legacy MotoLocator interface to communicate with the IMW.
Group Operator	The operator assigned to this role is the administrator of a Group and the Agency data assigned to that Group. This type of operator is able to access MotoMapping and any third-party application that uses the legacy MotoLocator interface to communicate with the IMW.
Box Admin	The operator assigned to this role is the administrator of the IMW and PSM box-specific data.

1.12.3.2

Agency Data Segregation and Access Control

Agency Data Segregation and Access Control enables control over the security groups that are assigned to new application groups created by external applications.

Service Operators can configure access limitations for groups created by external application users. Instead of assigning new groups to particular Agencies, data access can be narrowed down to particular security group that is set to default in Configuration Manager.

Figure 4: Access Control Settings in Configuration Manager

Associated Application			
<div> <input type="button" value="New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Search.."/> </div>			
<input type="checkbox"/>	Application	Security Group	Default Security Group for Application created Groups
<input type="checkbox"/>	700	agency1	No
<input type="checkbox"/>	700	sg2	No
<input type="checkbox"/>	700	sg3	No
<input type="checkbox"/>	700	sg4	No
<input checked="" type="checkbox"/>	700	sg1	Yes

New application groups inherit the security group allocation from the operator that creates them. Only selected data from other security groups within one Agency are made available. Application users are authorized to access data about entities assigned to the same security group or hierarchically lower-level groups.

1.12.3.3

Fine Grained Authorization

IMW allows to customize authorization settings for application users. Access control can be defined for data generated by services, individual users and devices, groups of users and devices or other groups, including devices affiliated with particular talkgroups and base stations.

With Fine Grained Authorization feature, Service Operators can configure access polices for:

- Talkgroup ranges
- Operator defined groups of devices or users
- Services like Presence, Location, Group Management

Configuration Manager contains special parameters for defining talkgroup ranges and access control to services.

Figure 5: Talkgroup Range Settings

Group Network ID Range (Application Access Control)			
<div>New Edit Delete</div> <div>Search.. 🔍</div>			
<input type="checkbox"/>	Group Network Id Start	Group Network Id Stop	Agency
<input type="checkbox"/>	100	199	foreign_agency
<input type="checkbox"/>	200	249	foreign_agency
			Security Group
			sg1
			sg2

Figure 6: Services Access Control Flags

Site Access	Yes	▼
Presence Access	Yes	▼
Location Access	No	▼
Messaging Access	Yes	▼
Depository Access	Yes	▼
Group Management Access	Yes	▼
Sensor Access	No	▼

1.12.3.4

Zero Touch Provisioning

With Zero Touch Provisioning, IMW server automatically discovers devices from infrastructure and allocates them to particular agencies and data partitions according to the operator policy.

Dedicated provisioning parameters in Configuration Manager allow Service Operators to set agency, security group and static group allocation rules for a range of devices based on their ID numbers.

Figure 7: Auto-Provisioning based on Device Network ID Configuration

Dimetra and Astro Auto-Provisioning

Home Device Network ID Range					
<input type="button" value="New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			<input type="text" value="Search.."/> <input type="button" value="Q"/> <input type="button" value="v"/>		
<input type="checkbox"/>	Home Device Network Id Start	Home Device Network Id Stop	Agency	Security Group	Static Group
<input type="checkbox"/>	1	100	Agency-1	security-group-1a	static-group-1
<input type="checkbox"/>	5000	6000	Agency-1	security-group-2	static-group-1
<input type="checkbox"/>	9001	9010	Agency-1	Agency-1	static-group-1

Zero Touch Provisioning differentiates between Home and Foreign devices. If a device from a foreign network is discovered in the infrastructure, for example a Police radio from a foreign unit, the system issues a temporary ID number for recognition and group allocation purposes.

1.12.3.5

IMW Security

Motorola Solutions certificates are installed on Intelligent Middleware (IMW) system by default to ensure communications security. The IMW certificates are unique for each deployment and are provided with the installation suite.

To encrypt information, the IMW supports AES-128, AES-192, AES-256, and 3Key-3DES algorithms. These algorithms apply to all TLS and HTTPS (including secure Parlay X, IMW REST, WebSocket) connections. To provide digital signature, the IMW supports such secure hashing algorithms as SHA-256 and HMAC.

The IMW complies with the NIST SP 800–131A recommendation. For more information, see *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths* <http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>.

1.12.3.6

IMW Server Licensing

Each copy of the Intelligent Middleware (IMW) software has a license file that defines the functions and capabilities of the software. Server licenses determine which of the IMW services are available for implementation and the allowed number of devices and users. IMW server licensing provides a method of assuring any exchange of information with the software.

Server licenses are distributed in the form of .bin extension files. Every server license file has a MAC address matching one of the virtual machines it has been generated for.

For more information, see the following sections in the *Intelligent Middleware Configuration Manager User Guide*:

- “Obtaining the IMW Server License”
- “Importing Server Licenses”
- “IMW Server Licensing”

1.12.3.7

Information Assurance

Information Assurance reduces the available mechanisms that an attacker may use to penetrate a system by turning off services, closing interface ports, and removing default logins from the system as it is installed. This process results in leaving only the minimal OS functionality required of the system applications.

1.12.3.8

IMW and Network Security

Depending on the radio network and the API used for exchanging data between Intelligent Middleware (IMW) and client applications connected to it, data may be transmitted encrypted or unencrypted. The following table shows a summary of encryption and transfer methods on different stages of data transmission from radio networks to IMW in the CEN and between IMW and client applications.

Table 11: Data Encryption: Radio Networks – IMW – Client Applications

Radio Net- work	Device/Radio to RNI Core	RNI Core to CEN	Inside CEN	IMW to Applications
ASTRO® 25	Data optionally encrypted with ASTRO® 25 PDEG Encryption Unit	Data optionally encrypted with ASTRO® 25 PDEG Encryption Unit	Unencrypted	<ul style="list-style-type: none">• Parlay X – HTTPS (default), HTTP (optional)• REST – HTTPS (default), HTTP (optional)• LRRP – HTTP only
Dimetra IP	Air interface encrypted	Unencrypted	Unencrypted	<ul style="list-style-type: none">• Parlay X – HTTPS (default), HTTP (optional)• REST – HTTPS (default), HTTP (optional)• MotoLocator – HTTP (default), HTTPS (optional)

1.13

IMW Redundancy Overview

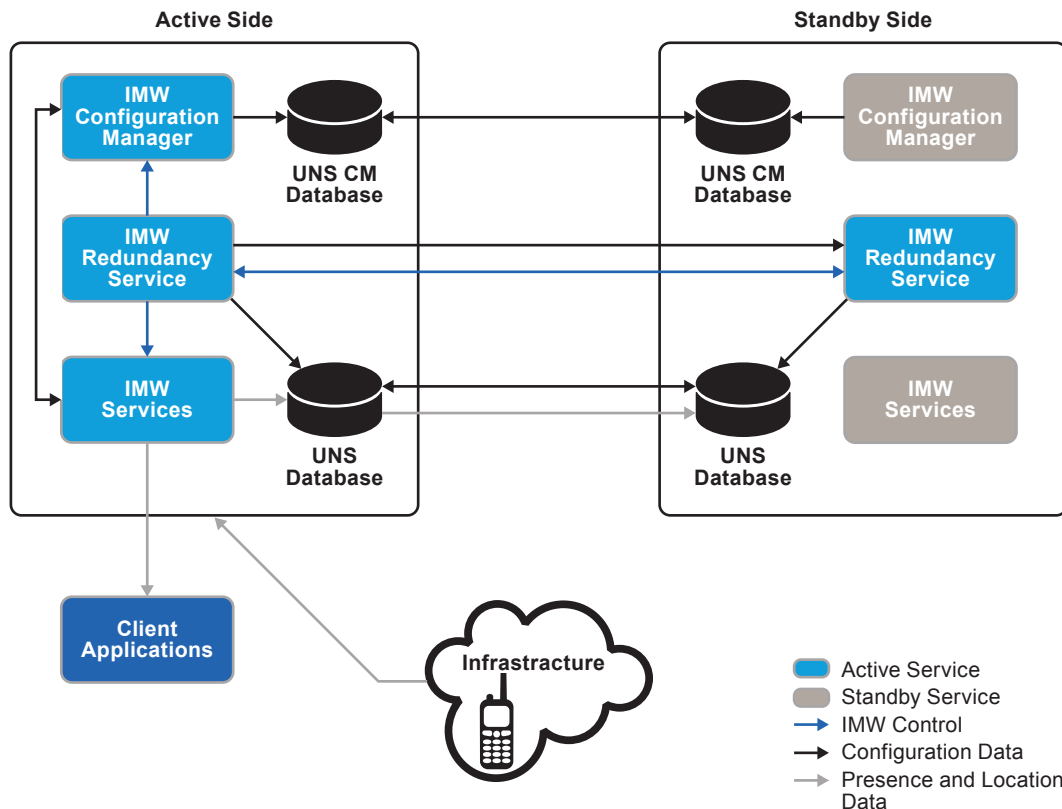
Intelligent Middleware (IMW) supports an automatic redundancy model. In this solution, the system achieves higher availability of service by deploying two IMW servers: primary and secondary. One of the servers plays an **active role** in the model, and the other plays a **standby role**. The two IMW servers may be deployed in the same office (locally redundant configuration) or remotely (geographically redundant configuration).



NOTICE: IMW redundancy is not supported with converged ASTRO® 25 deployments.

The following section provides an overview of the IMW redundancy architecture.

Figure 8: IMW Redundancy Architecture



The active role is claimed by the server on which the administrator selects **Start Redundancy** option. All the configuration data is automatically transferred to the standby side. When the roles are assigned, the IMW redundancy application monitors the health of both servers. If the redundancy application detects an internal fault in any of the servers, it takes appropriate actions to resolve the fault and then the operation continues. If the fault in the active server cannot be resolved, the standby IMW becomes active, and the formerly active IMW server that failed is taken off-line for diagnostics. If the diagnostics succeed, the server is returned to service as the standby server and the incident is logged. If the diagnostics fail, the server is left off-line and the remaining IMW server operates without a standby server until the failed server is repaired.



NOTICE: In the case of Dimetra system deployments, Presence service might be running on the active and standby servers to ensure that no presence status changes are missed during IMW switchover.

1.13.1

Automatic Control of IMW Redundancy

Intelligent Middleware (IMW) Redundancy control is automatic and includes the following activities:

- Arbitration of the active and standby roles for each IMW server.
- Detection of the active server failure and a switchover to the standby server.
- Synchronization of the configuration data from the active server to the standby server.
- An upgraded user interface reporting the status of the servers, the status of services running on each server, and the synchronization of information between servers.
- Visibility of the data replication status of the IMW services on the active or standby IMW servers.
- Notification sent to the external application about which IMW server is currently active.

The following actions might be performed manually by the administrator:

- Invoking a switchover between the servers.
- Freezing the automatic switchover.
- Forcing data replication.

1.13.2

Network Connectivity Between IMW Servers

The Intelligent Middleware (IMW) synchronized standby redundancy feature uses network connectivity between the two paired servers. The network connectivity allows for the following functions:

- 1 Arbitrate which server is to provide the active role of the pair at the start-up or switchover.
- 2 Verify the status of the active server during operation.
- 3 Synchronize SQL database tables between servers.

The required bandwidth between servers is 25 Mbps as there are only infrequent updates of the synchronized data triggered by administrator changes to the configuration data.



NOTICE: Changing the system time to the past may cause a IMW data replication failure.

1.13.3

Client Applications Interaction with IMW Redundancy

In the case of Dimetra deployments, a third-party application interacting with Intelligent Middleware (IMW) must be aware that the IMW Redundancy model is in place and must know the IP network addresses for each IMW server. When the IMW is deployed in Astro® 25 network, a third-party application must be aware either of customer IP address or IP network addresses for each IMW servers.

During initial connection to the IMW, the client application should attempt to open a connection with both paired IMW servers. The active IMW server responds to the connection and an interaction between the application and IMW continues normally. The standby IMW does not respond to the application, therefore the application does not establish a connection with the standby IMW.

The client application using the ParlayX APIs is recommended to subscribe to the event heartbeat notification. When a switchover from the active to the standby IMW takes place, IMW notifies the application about the switchover by either failing to send a heartbeat message at the configured interval, or send the application API a message that the connection has been closed. The assumption for the second type of notification is that the IMW server which was active fails in a way that it is still possible for it to close the connection. When the client application is notified about the switchover, it should attempt to reconnect to IMW on both IP network addresses until it establishes a connection. Establishing a connection may take more than one attempt.

1.13.4

Switchover Triggers

An automatic switchover to the standby Intelligent Middleware (IMW) server is triggered by the following events:

- 1 The standby IMW server does not receive heartbeats from the active IMW server. A lack of heartbeat may be caused by the following situations:
 - The active IMW shutdown
 - The active IMW switch to the malfunction state
 - A network failure.

- 2 The SQL server is not working on the active IMW server.
- 3 One of the key IMW services is not working correctly on the active IMW server.



IMPORTANT: A client application connecting to IMW using the Parlay X APIs needs to subscribe to the heartbeat event to be able to detect switchover from the active to the standby IMW. When a switchover occurs, all the existing subscriptions are removed without any notification, which means that the client application needs to subscribe to the heartbeat event again.

1.13.5

Fault Management Reporting

A fault management application is not obligatory for Intelligent Middleware (IMW), but it is highly recommended to define at least one to enable the detection, isolation, and correction of malfunctions in your network. The IMW notifies a registered fault manager about its operational status and about the redundancy mode. The Simple Network Message Protocol (SNMP) Agent is a IMW process that notifies the fault manager about traps.



NOTICE: After a reboot, during the machine power-up, all IMW processes start simultaneously, and the SNMP Agent may not send all the traps to the fault manager if some processes started before the SNMP Agent itself was fully operational.

The following objects are related to the IMW synchronized standby redundancy:

- **Redundancy** – reports the redundancy status of IMW server. The status depends on the current redundancy configuration and on the server role. The redundancy status is reported by both the active and standby IMW servers.
- **IMW Redundancy Service** – manages data replication and monitors the redundant server. The IMW Redundancy Service status is reported by both the active and standby IMW servers.
- **Inter IMW Link** – this link is a logic representation of any communication path between an active and standby IMW servers. This link is used for data synchronization and monitoring the health of the servers. If the link is down, a switchover to the standby IMW server is triggered. The Inter IMW Link status is reported by both the active and standby IMW servers.
- **Database Replication** – reports the status of database replication between the active and standby IMW servers. The database status is reported by both the active and standby IMW servers.



NOTICE: Traps about data replication not working correctly are sent only from the IMW server on which redundancy was started.

1.13.6

Configuration of IMW Parameters When Servers Are Synchronized

When the primary and secondary Intelligent Middleware (IMW) servers are **not** synchronized, configuration of IMW parameters may be performed on either server as long as they have the **Standalone** role shown on the **Redundancy** tab. It is enough to configure one of the servers as all the parameters will be copied to the **Active** IMW server when redundancy is started.

When the primary and secondary IMW servers are synchronized, the replication status is **Running**, and the servers take the active and standby roles, any configuration of IMW parameters may be performed only on the **Active** IMW server.



NOTICE: Changing connection parameters related to Geographical Redundancy (for example, IP addresses, host names) will not take effect until redundancy is stopped and started again.

An exceptional situation to the rule that IMW parameters may only be edited on the active IMW server is when you are editing parameters on the active IMW server and a switchover to the standby IMW server takes place. In such a scenario, IMW lets you finish editing your parameters that you started editing before the switchover took place.



NOTICE: No configuration may be performed on any server which is in the **Malfunction** role.

If network connectivity is lost between a synchronized pair of IMW servers, it is not recommended to perform any configuration on either IMW server until you restore connectivity between them. Any configuration changes you introduce when the IMW servers are not communicating with each other will not be synchronized automatically. If you choose to change configuration parameters when the servers are not communicating with each other anyway, after the connectivity is restored you need to press **Force Synch** on the **Redundancy** tab to ensure data consistency between the servers.



CAUTION: When you press **Force Synch**, the configuration data from the active IMW server overwrites the configuration data of the standby IMW server.

1.13.7

Automated Virtual Machine Standby with DAS



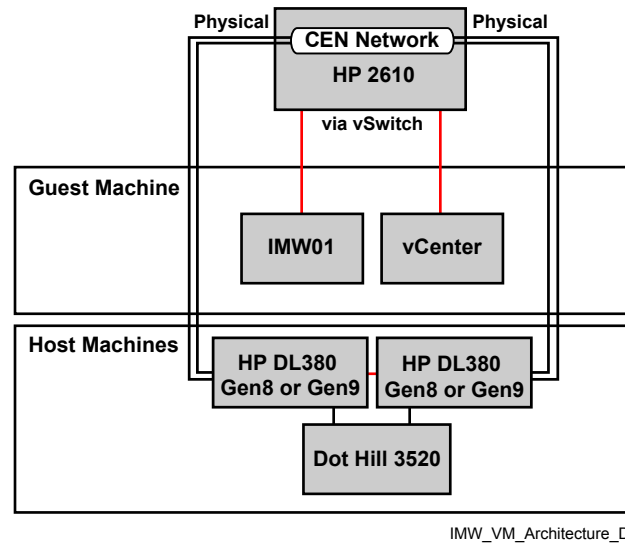
NOTICE: The following section is relevant for the upgrading customers only.

With the DotHill 3520 External Direct Attached storage (DAS) for ASTRO® 25 RANs, IMW uses virtual machine technology to provide redundant platform recovery of the IMW service from hardware or network connectivity failure. A single instance of IMW is bundled into a virtual machine image labeled **Guest Machine** and is deployed to common storage shared between two physical hardware platforms. Both IMW servers are in the same room and they are connected to the DotHill 3520 External Direct Attached Storage (DAS). One IMW server is running and the other is idle.

A management application, **VCenter**, monitors the guest machine. The application supervises both management and failure recovery. If the virtual machine monitor detects hardware platform failure it loads and executes the same virtual machine image onto the redundant hardware platform.

Shared storage means that the new instance of IMW can access all the data stored by the prior instance. The server IP address is migrated during switchover so that reporting devices and applications are unaware of the physical hardware switchover. Registrations remain in effect and the application subscriptions to updates of presence or location data continue unchanged. If the virtual machine or its Windows OS crashes, the virtual machine management software restarts the failed virtual machine on the same hardware. The IMW application software automatically restarts because it is hosted in the guest machine OS. Shared storage is configured as RAID 10 to enhance reliability and is accessible from either the primary or backup machine. However, the two hardware platforms must be physically close enough to the common storage to meet the distance limitations of the cables that connect them to the common storage.

Figure 9: Virtual Machine Architecture



1.14

Client Applications and Solutions Supported by IMW

Intelligent Middleware (IMW) supports a number of Motorola Solutions products, including mapping applications, CAD applications, messaging solutions, and also third-party applications.

1.14.1

MotoMapping

MotoMapping is a mapping application that is used with the Location Service, through which vehicle tracking and personnel location services are delivered in a graphical display.

MotoMapping consists of a mapping application, which is installed on client computers and a MotoMapping server that is installed on the Intelligent Middleware (IMW) server. MotoMapping is not part of the IMW installer, it is available on a separate MotoMapping installation media. To learn more about MotoMapping installation and configuration, see the *MotoMapping User Guide*.

1.14.2

Advanced Messaging Solution

ASTRO® 25 Advanced Messaging Solution (AMS) is a PremierOne-based solution that delivers messaging to ASTRO® 25 subscriber units. A messaging client called the Smart Client provides messaging, address book, and query functionality. In some configurations, the messaging service is integrated with PremierOne dispatch services. The AMS requires the Presence Service to access subscriber radio status information. The AMS in addition to the IMW consists of the following components:

- PremierOne server – a server that provides the message processing and hosts a provisioning application for configuration of text messaging.
- Smart Client – a messaging client running on a PC or an MCC 7500 console that provides messaging services.
- (Optional) PremierOne server CAD and/or Mobile – applications for dispatching and managing resources (CAD) and responding to incidents in the field (Mobile).

AMS can be installed on a dedicated virtual machine on the physical IMW server or on a separate physical server.

For more information, see the following documents:

- *ASTRO® 25 Advanced Messaging Solution Server Installation Guide for A1 and A2 (non-HA)*
- *ASTRO® 25 Advanced Messaging Solution Provisioning Guide for Configurations A1 and A2*

1.14.3

Converged Services Client

Converged Services (CS) Client enables communication between a device and Intelligent Middleware (IMW)/Priority Management (PM).

CS Client supports the following IMW services:

- Presence Service
- Location Service
- Identity Management
- Multi-Group Management (MGM)

For more information on the CS Client, see the *Connecting Clients to IMW* manual.

Chapter 2

ASTRO 25 System Deployments

2.1

How IMW Functions Within an ASTRO 25 System

The figure shows ASTRO® 25 architecture.

2.2

ASTRO 25 Supported Devices

The Intelligent Middleware (IMW) server can support simultaneous tracking of up to 48,000 active ASTRO® 25 devices. You may configure up to 128,000 devices.

2.3

ASTRO 25 System Presence Service

The Presence Service is deployable with an ASTRO® 25 system or an ASTRO® 25 Conventional with Integrated Voice and Data (IV&D) system, Release 7.4 or newer. Other documentation may call the presence client an Automatic Registration Service (ARS) application or, more simply, a Registration Application.

ASTRO® 25 subscriber radios are pre-configured with the IP address of the Presence Service so that they can initiate reporting their presence to the service automatically. They do this by sending messages to the Presence Service after certain events, like when a user initiates a subscriber radio function by logging on or off with a user name. These messages consist of ARS registration and deregistration messages. The Presence Service, in turn, notifies applications that subscribe to it using its API.

An application that subscribes to receive notifications from the Presence Service, is called a **watcher**. Watchers can subscribe to groups of users and devices as well as to receive notifications for device IDs and user names, which are the two types of “presentities.” Device IDs and user names are entities for which a watcher may want to receive presence status and attribute information.

Third-party applications use the Parlay X or the IMW REST interface.

The Presence Service also enforces the following business rules for ASTRO® subscriber radios:

- A user may only be logged into one radio at a time.
- A user may only be logged into the IMW system for a period of time.
- Devices must re-register with IMW periodically or become inactive.

The Presence Service is backward compatible with legacy ASTRO® 25 data applications, such as the Text Messaging Service (TMS) and POP25.

2.3.1

Device Presence

Data applications integrated with ASTRO® 25 IV&D data services may use the Presence Service to learn IP addresses and presence status of subscriber units.

Every radio has an associated Device ID that is derived from its Layer 2 ID. The Presence Service also provides a dynamic association between a subscriber radio and a user-provided User Name. In this way, a User Name may be associated with different subscriber radios at different times, but the Device

ID is always associated with the same radio. Subscriber radio/User Name association is an optional feature of the Presence Service. The service provides interested applications with the association between a Device ID and User Name as well as the subscriber radio IP address and presence status information.

Applications may then track the association of Device IDs and User Names with the IP address that can be used to communicate with the subscriber radio. Applications can also track the presence status of the Device ID/User Name combination as **present**, **absent**, or **unknown** so that the application can take appropriate action while in a given presence status or while transitioning from one state to another.

- PremierOne
- POP25
- Legacy Text Messaging Service.

Mode Changes on the ASTRO 25 IV&D System

For the ASTRO® 25 IV&D system, when a subscriber radio changes away from a data service-capable mode, no notification is sent until the unit mode returns to a data-capable mode with ARS enabled. In this case, although the presence status of the Device ID may not have changed, a Device ID notification is sent anyway so that the watcher initializes the subscriber radio client application. This ensures the subscriber radio has a Device ID in case initialization information was lost while it was in the non-data service-capable mode.

The Device ID notification is also sent when a subscriber radio powers on after the Presence Service fails to detect that it had previously powered off.

2.3.2

User Presence

Subscriber radios provide a User Name notification when:

- A user logs on to the unit with a User Name.
- A radio is powered on or off.
- The user logs off the unit.

When the user logs on to a different subscriber radio without logging off a previous one, the association with the previous subscriber radio is removed and the watchers are notified of the new association. Watchers are notified of the removal of the association with the Device ID of the previous radio. The removal of the User Name association with the previous radio Device ID also sends a User Deregistration message from the Presence Service to the previous radio to remove the user name from the radio.

2.3.3

IMW Presence Deployment in an ASTRO 25 Advanced Messaging Solution

In an ASTRO 25 Advanced Messaging Solution, radio users with post-ASTRO® 25 System Release 7.12 subscriber radios authenticate directly with the Premier One messaging server. The presence status of these users is published to Intelligent Middleware (IMW) so that it can provide a consistent view of user presence on pre- and post-A7.12 subscriber radios to requesting watcher applications. The IMW allows sending messages to and receiving messages from ASTRO® 25 subscribers.

2.3.4

Subscriber Radio Inactivity Time

Presence status in the Presence Service is only valid for a period of time called the **Subscriber Radio Inactivity Time**. The default value is four hours plus two minutes (242 minutes), but the period is configurable.

If the Presence Service does not receive a refresh notification or other device registration from a subscriber radio within the Subscriber Radio Inactivity Time:

- 1 It changes the state of the User Name and Device ID associated with the unit to **Absent**.
- 2 It notifies the watchers.

This situation may occur if a subscriber radio changes to a non-data-capable mode on the ASTRO® 25 IV&D system or moves out of system coverage for longer than the Subscriber Radio Inactivity Time. After Subscriber Radio Inactivity Time expiration, the presence status of the User Name and Device ID recover automatically when the subscriber radio returns to the coverage area or to a data-capable mode with ARS enabled on the ASTRO® 25 IV&D.

Intelligent Middleware (IMW) provides no immediate notification when a subscriber radio leaves the coverage area or it changes to a non-data-capable mode on the ASTRO® 25 IV&D system. Notification is only provided when the unit changes to a data-capable mode with ARS enabled on the ASTRO® 25 IV&D system or returns to coverage following Subscriber Radio Inactivity Time expiration. If a subscriber radio returns to coverage prior to the Subscriber Radio Inactivity Time expiration, its status does not change and no notification is provided. As a result, a User Name/Device ID can be in a Present state but the watcher cannot communicate with a subscriber radio application that is out of coverage or in a non-data-capable mode on the ASTRO® 25 IV&D system.

2.3.5

User Session Timer

When operating with the AMS, the Presence Service maintains a user session timer. Regardless of user activity, when this timer expires, the user is logged off and must manually log on again.

At this point the timer is reset (just as it is each time a user logs on). The default value of the user session timer is eight hours and is typically configured to automatically log users off upon completion of their shifts.

2.3.6

User Authentication For Pre-A7.12 Radios Only

The Presence Service can authenticate users of pre-A7.12 radios with a four-digit Personal Identification Number (PIN). Administrators may enable or disable this functionality.

When enabled, the Presence Service validates a User Name and PIN when a radio user with a pre-A7.12 subscriber registers with the service. The radio user may enter the User Name and PIN, or a subscriber radio using Customer Programming Services (CPS) may provision them. In either case, when the subscriber radio sends a registration message containing a User Name to the Presence Service, Intelligent Middleware (IMW) uses Microsoft® Windows OS authentication services to request validation of the User Name/PIN combination. Systems that support Information Assurance may impose a minimum password length restriction for this validation. The IMW uses an AuthPrefix configuration to transform the four-digit numeric PIN to a longer Windows OS-style password. Administrators can enable or disable this PIN-based authentication of pre-A7.12 radios. When enabled, the Presence Service can also be configured to use internal or external customer network-based authentication services. The customer must provide valid User Name/AuthPrefix + PIN pairs in the authentication service being used.

Before authenticating a User Name/PIN, the Presence Service appends the AuthPrefix to the beginning of each PIN value it receives from a subscriber radio. If the authentication service is external

to the Presence Service OS, the AuthPrefix may be set to any text string value that satisfies the system administrator password policy. Customers must append the AuthPrefix string to each PIN value when providing User Name/PIN pairs in the authentication service. If the User Name is not authenticated, customers may leave AuthPrefix blank (the default setting).

A User Name/PIN pair is not validated against a particular Device ID. If a User Name fails authentication, it is not associated with the subscriber radio. If the Presence Service is configured not to use authentication services, it considers all User Names valid and does not require PINs. Subscriber radios retain a User Name and PIN (if applicable) until the radio user logs off or the User Name and PIN fail authentication, in which case they are deleted.

2.4

Talkgroup and Radio Site Affiliation

When deployed in ASTRO® 25 systems, Intelligent Middleware (IMW) tracks talkgroup and radio site affiliation of radio subscribers using Multi-Group Management (MGM) Service.

For that purpose, MGM uses information provided by the CADI Server in CADI Affiliation Events. MGM communicates with watcher applications using the IMW REST interface. Applications can monitor which radios are in which talkgroups or sites. Also, MGM allows applications to subscribe to getting updates automatically when the group status changes.

2.5

ASTRO 25 Outdoor Location Solution and IMW Location Service

The Location Service replaces the legacy MUPS in an ASTRO® 25 Outdoor Location Solution. The solution uses the networks to transport location and telemetry data over the air to the Location Service.

The ASTRO® 25 Outdoor Location Solution is available for any combination of these systems:

- ASTRO® 25 Conventional with Integrated Voice and Data (IV&D) system, Release 7.9 or newer

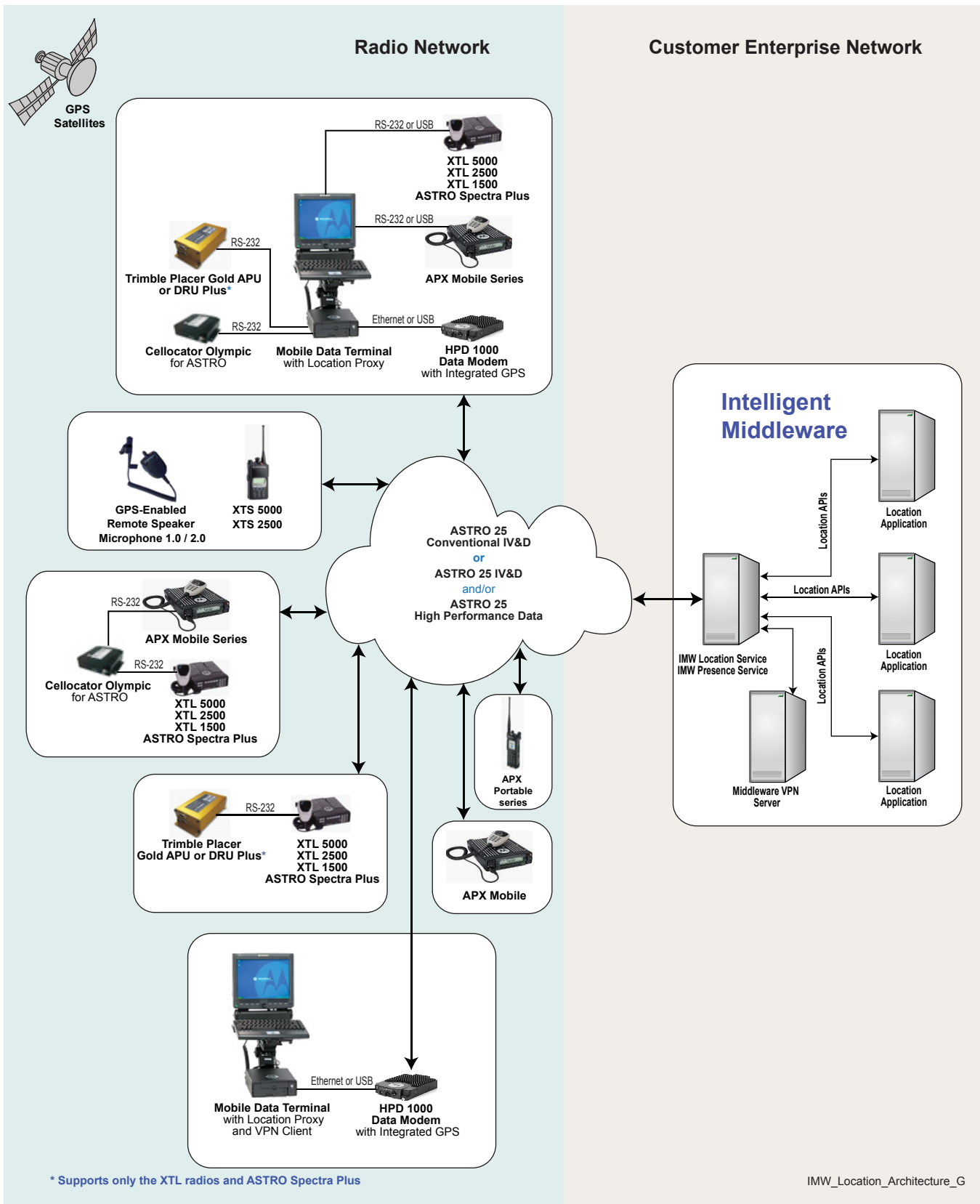


NOTICE: For location reporting, the use of the Integrated Voice and Data (IV&D) Enhanced Data is preferred when possible, due to the higher capacity it provides. Enhanced Data is only supported on ASTRO® 25 Trunked IV&D systems with GTR series site equipment and APX subscriber units.

- ASTRO® 25 System
- ASTRO® 25 High Performance Data (HPD) system

The Location Service is a key component of the ASTRO® 25 Outdoor Location Solution and routes location data of GPS-enabled ASTRO® 25 devices to the customer's mapping applications. Mapping applications subscribe to receive location updates of desired devices using an API.

Figure 10: ASTRO® 25 Outdoor Location Solution – High-Level View



2.6

CADI and IMW

Intelligent Middleware (IMW) deployed in ASTRO® 25 systems uses Computer Aided Dispatch Interface (CADI) as part of the optional Geo Select feature. Information provided by CADI is also used by the Multi-Group Management (MGM) Service to track radio group affiliation.

CADI is a component of the ASTRO® 25 radio systems that provides an interface to applications in the CEN (such as IMW). It provides information on the presence of the subscriber radio in the system, the cell, the talkgroup, and the RF site through which the radio is accessing the system at that moment. It also allows some real-time control over the radios. CADI is limited to be used by one CADI client at a time, which for ASTRO® 25 deployments with Geo Select and/or MGM feature is IMW. Geo Select feature allows the operator to configure geofences and automatically force radios to a specific talkgroup when they enter that geofence. The IMW tracks which talkgroup a radio is on using the CADI Affiliation Event and instructs the radio to change talkgroups using the CADI Regroup Command.

As part of the MGM, the IMW tracks the talkgroups and sites ASTRO® 25 radios are using based on the CADI Affiliation Events.

2.7

Device Provisioning

Devices tracked by the Presence Service must be pre-provisioned in the Intelligent Middleware (IMW) Configuration Manager. Alternatively, administrators may configure the IMW to dynamically auto-provision devices that have not been recorded in the provisioning database.

With Auto-Provisioning **Enabled**, as devices become available, they are added to the provisioning database and are also announced to the Presence Service. Their availability is then announced to interested watcher applications. Auto-Provisioning should be used after initial deployment to quickly get devices provisioned therefore it should be disabled after most of the devices have been provisioned.

For more information on provisioning, see [Zero Touch Provisioning on page 34](#).

2.8

User Provisioning

Pre-provisioning of users in Intelligent Middleware (IMW) Configuration Manager is required for all ASTRO® 25 System customers. Alternatively, administrators may configure the IMW to dynamically auto-provision users that have not been recorded in the provisioning database.

With Auto-Provisioning **Enabled**, as users register, they are added to the provisioning database and are also announced to the Presence Service. Their availability is then announced to interested watcher applications.

Additionally, for customers who use the **User Authentication** feature, every User Name and corresponding AuthPrefix + PIN must be provisioned in the target authentication directory. The IMW can work with a local Windows SAM database or a remote Windows Active Directory as the authentication directory. Customers who want to use the existing IT username space (that is, use the same Active Directory as for authentication on IT applications like OS logon, email) for radio user authentication as well, must update passwords for the subset of user accounts that are expected to log on to the ASTRO® 25 radios to follow the “AuthPrefix + PIN” pattern.



NOTICE: The **Auto Provisioning** feature cannot be used in parallel with the **User Authentication** feature.

2.9

IMW Migration in the ASTRO 25 System

The Presence Service replaces the existing ASTRO® 25 Presence Notifier application. Intelligent Middleware (IMW) is not supported on the legacy Presence Notifier hardware platform.

Customers choosing to upgrade from existing ASTRO® 25 systems that use Presence Notifier to IMW must uninstall the Presence Notifier application. If the Presence Notifier uses dedicated hardware, decommission it and replace it with the new IMW-compliant hardware. Legacy watcher applications can continue to run on the legacy hardware but must be reconfigured to use the IMW host IP address as the Presence Notifier IP address.

Chapter 3

Dimetra IP System Deployments

3.1

How IMW Functions Within a Dimetra IP System

The figure shows Dimetra IP architecture.

3.2

Dimetra IP Presence Service

The Presence Service provides presence status of subscriber radios based on CADI events forwarded to Intelligent Middleware (IMW) by an MCADI.

The Service can interface with multiple MCADIs that are present in a Dimetra IP cluster. The IMW host is located in the screened network domain when Perimeter Protection is deployed and in the DMZ when Perimeter Protection is not deployed.

The Presence Service records the last reported presence status for a device. For asynchronous notification, a watcher can query the last known presence status for a device instead of subscribing. The presence information of a device includes attributes like:

- Basic on/off device presence
- Talkgroup and radio site affiliation
- Status Messaging about last reported status code

3.2.1

Basic Device Presence

The Presence Service provides basic on/off presence of Dimetra IP subscribers based on Multi-Computer Aided Dispatch Interface (MCADI) affiliation and de-affiliation events.

Watcher applications can use this information to track availability of the device for PTT communications. The Dimetra IP Presence Service provides device presence, but does not provide user presence.

3.2.2

Talkgroup and Radio Site Affiliation

The Presence Service tracks the affiliation of a device to a particular PTT talkgroup identifier and Dimetra radio site (Dimetra IP network Site ID and Zone ID).

When a device changes its talkgroup affiliation or site/zone, an MCADI event is forwarded to the Presence Service and a presence notification is generated for the interested watchers over the Parlay X presence interface. The notification consists of the affiliated talkgroup ID, Site ID, Zone ID, and a timestamp noting when affiliation was announced as a presence attribute.

The watcher application can query the list of devices affiliated with a particular talkgroup ID. This additional functionality is available through a forward-looking server interface based on 3GPP Parlay X Address List Management specification (TS 29199.13), only for Dimetra IP systems.

3.2.3

Status Messaging

When CADI/MCADI forwards a status event to the Presence Service, it generates a presence notification containing the reported status code as a presence attribute. This numeric code is reported over the control channel.

The receiving application defines the meaning of the code. Also, the presence attribute is tagged with a timestamp corresponding to when the event was received. This indicates how recent the status is. A second type of status indicator, a “Predefined Status Message,” is also available. The Presence Service only stores information about the last status message sent, indicating the device ID and the timestamp. This information identifies the last time the server heard from a particular radio, in the event contact is lost.

If a third-party application has a strong interest in a particular status message, for example, an alarm message, the Presence Service may predefine it and configure it to be tracked and reported separately. If the device generates another status message, the customer may query when the device last sent a predefined status message to help identify a chain of events.

3.3

Dimetra IP Location Service

Intelligent Middleware (IMW) support of location tracking of Dimetra IP subscriber radios is provided in two forms:

- Cell-based location (derived from the entry into or exit from specific cells)
- Short data location reporting (if it is the subscriber radio GPS location)

3.3.1

Dimetra IP Cell-Based Location

Dimetra IP deployment supports cell-based location for subscribers when MotoMapping gives visibility to the Dimetra IP cell to which the device is assigned.

The Location Service takes information about device affiliation with cells from the ATR by processing an ATIA stream and formatting it into CADI messages. Cell-based location is not available to ASTRO® 25, ASTRO® 25 High Performance Data (HPD) system or MOTOTRBO™ networks. Using the CADI events, the Presence Service can track device affiliation to a Dimetra IP zone and site. When a device affiliates to a different zone or site, Intelligent Middleware (IMW) sends a presence notification to interested watchers. The notification contains three pieces of information:

- The affiliated zone ID as a presence attribute
- The affiliated site ID as a presence attribute
- A timestamp of when the Presence Service recorded the affiliation

3.3.2

Dimetra IP Short Data-Based Location

Intelligent Middleware (IMW) uses the Dimetra IP short data messaging service to support Dimetra IP radios.

The radios report their GPS-derived locations over the air. The IMW forwards reporting interval commands to the radios and receives location updates from the radios through the short data messaging system.

Figure 11: Dimetra IP Short Data Reporting



3.4

MCADI and IMW

When deployed in a Dimetra IP system, Intelligent Middleware (IMW) connects to the Dimetra IP-provided MCADI interface to receive subscriber radio status changes.

It allows IMW to provide applications with information on the presence of the subscriber radio in the system, the cell, and the talkgroup through which the radio is accessing the system at that moment. Planning for a IMW deployment into a Dimetra IP system requires the deployment of MCADI.

3.5

ATIA and IMW

Intelligent Middleware (IMW) Location uses the Dimetra IP RAN-provided ATIA interface to monitor the individual cell loading to detect cell data channel overloading due to too many radios reporting location in the cell.

When IMW detects this condition it reduces the reporting frequency (longer time between location reports) for radios within the overloaded cell. Deployment of an ATIA interface on a Dimetra IP system is required to support this feature. Factor this cost into the system planning for IMW deployment.

3.6

Device Provisioning

Administrators must pre-provision devices that are tracked by the Presence Service in the Intelligent Middleware (IMW) Configuration Manager. Alternatively administrators can configure IMW to dynamically auto-provision devices that have not been recorded in the provisioning database.

Auto-Provisioning should be **Enabled** only when staging IMW with a new Dimetra IP Network system. It is not recommended to use this setting when adding IMW to an existing Dimetra IP network system. With Auto-Provisioning **Enabled**, as devices become available, they are added to the provisioning database and are also announced to the Presence Service. Their availability is then announced to interested watcher applications.



NOTICE: Even if Auto-Provisioning is disabled, IMW may update the radio Friendly Name with the value received in a CADI Affiliation message. The update happens when IMW receives a CADI Deaffiliation message followed by a CADI Affiliation message.

Customers do not need to provision devices that are tracked by the Presence Service. As devices become available and are announced to the Presence Service, their availability is also announced to interested watcher applications. As a result, watcher subscriptions are never rejected as an “unknown device.”

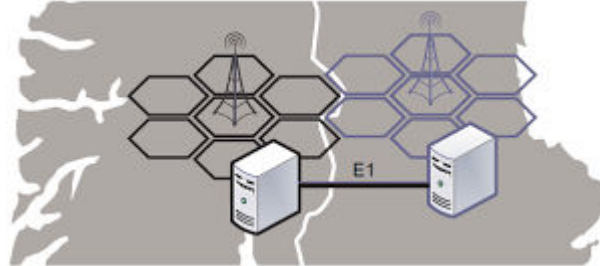
For more information on provisioning, see [Zero Touch Provisioning on page 34](#).

3.7

Dimetra IP Roaming Service

The Inter-System Interface (ISI) allows radios to migrate from/to other TETRA systems and communicate to radios located in both home and visiting systems.

Figure 12: Dimetra Inter-System Interface



The ISI feature allows foreign devices to roam between TETRA systems and obtain Group Calls, Private Calls, and Short Data Service in a system which is not their Home System.

The ISI allows foreign radios, identified by their Individual TETRA Subscriber Identity (ITSI), to use Dimetra SwMI resources. Dimetra radios are identified by an Individual Short Subscriber Identity (ISSI) and alias. Foreign radios are identified by a temporary Visiting Associated Short Subscriber Identification [(V)ASSI] which is interpreted as an Individual Short Subscriber Identity (ITSI) and assigned to the device by the Dimetra SwMI as long as it is registered in that Dimetra system. Both the IMW and the SwMI must be configured with the same Foreign Device Network ID [(V)ASSI] Ranges. Each Agency is provisioned with one or more configurable [(V)ASSI] ranges known as Foreign Device Network ID.

The IMW dynamically learns about foreign devices in real time and auto-provisions those foreign radios into the IMW Configuration Manager.

The IMW supports the following services for the foreign devices:

- Presence Service
- Multi-Group Management (MGM) Service

Chapter 4

Application Interfaces

This chapter describes the Application Programming Interfaces (APIs) that applications may use to subscribe to receive presence updates for selected entities.

4.1

3GPP Parlay X

Intelligent Middleware (IMW) provides four elements of the 3GPP Parlay X interface that give external applications access to IMW functionality:

- 1 **Common** – provides application authentication and continuously monitors communications availability on the link from the application to IMW. See the Intelligent Middleware system *Common Interface Control Document* to learn more about this interface.
- 2 **Presence** provides subscriptions to users or device presence updates and delivers those updates when they occur and filter criteria are met. See the Intelligent Middleware system *Presence Interface Control Document* to learn more about this interface.
- 3 **Location** provides subscriptions to device location updates, allows applications to set the location-update reporting rates and delivers those updates when they occur and filter criteria are met. Location reports may also include telemetry data reported from radio devices, which indicate in-vehicle events like siren or light activation, door opens. when location services support radio networks that report telemetry data (ASTRO® 25 systems and Dimetra IP). See the Intelligent Middleware system *Location Interface Control Document* to learn more about this interface.

Application developers must register with the Motorola Solutions Application Partner Program to receive the API document and runtime credentials to access a deployed IMW system.

Web Services Interoperability

All IMW Web service interfaces are available through a Microsoft® WCF WS 2007 Federation HTTP Binding. This binding is compliant with industry-standard Web services interoperability profiles and protocols.

4.1.1

Heartbeats on the Extended Parlay X Interface

The Extended Parlay X interface provides a mechanism for a watcher to subscribe for periodic heartbeat messages from the Intelligent Middleware (IMW).

The heartbeat messages work in the following manner:

- 1 The watcher sends a Heartbeat Subscription request to IMW stating the configured reporting frequency and the allowed inactivity duration.
- 2 IMW periodically sends heartbeat messages to the watcher at the configured frequency.
- 3 The watcher acknowledges receipt of the heartbeat messages from IMW.
- 4 If IMW fails to receive a heartbeat message acknowledgement for the allowed inactivity duration, IMW considers the watcher to be offline and begins cleaning up subscriptions for the watcher.
- 5 If the watcher fails to receive a heartbeat message from IMW for the specified inactivity duration, it performs a recovery procedure.

4.1.2

Presence Filtering

When using the extended Parlay X API, watcher applications may specify content filters for notifications from the Presence Service. Content filtering helps watcher applications reduce the size of each notification by letting watchers specify which presence attributes to include in or exclude from notifications.

4.1.3

IMW Network Time Synchronization

The Intelligent Middleware (IMW) server and the application servers that interface with it must be synchronized with an external network time server so that they can exchange time-based WS-trust certificates. If the IMW is installed in a CEN with a domain server then the domain server becomes the definitive time source. Otherwise, the field team or the customer must install a network time server in the CEN.

4.1.4

Parlay X Interface Capacities

The following section presents capacity for a maximum number of queries, requests, and subscriptions on the Parlay X Interface for Presence and Location.

Based on the target loading, customers who expect the notifications load to exceed the ability of a watcher to handle it should consider one of the following:

- Design the application to specify the appropriate notification rate in subscription messages to Intelligent Middleware (IMW). The application must handle the rate without buffer overruns. The Intelligent Middleware *Presence Interface Control Document* describes how to achieve it. If specified, IMW paces the notifications based on the requested rate.
- Enable notification pacing on the Presence Service. This universal setting enables pacing for all applications connected to the IMW.

Parlay X Presence Interface Capacity

The Presence Service can support up to 100 watchers with a total of 3,000 subscriptions on the Parlay X interface. Each subscription can handle up to 100 identifiers. Special Group Identifiers are set up for subscribing to all devices or all users.

Across all subscriptions, the service can support an average load of 350 notifications per second and a peak load of 500 notifications per second. Depending on the total number of devices and users, system design should restrict the number of watcher applications that subscribe to presence updates for all entities in the system.

Parlay X Location Interface Capacity

The Location Service can support up to 200 simultaneous subscriptions on the Parlay X interface. Each subscription can handle up to 500 devices. Applications that need to track more than 500 devices must create enough aggregate subscriptions to support them all.

Across all subscriptions, the Location Service can support a notification rate of 1,500 reports per second for ASTRO 25 and Dimetra. Although the inbound location report rate from ASTRO® 25 system devices is only 167 reports per second, the total notification rate on the Parlay X is much higher, which lets it support multiple mapping applications.

Based on the target loading, customers who expect the location reporting load for a subscription to exceed the ability of a mapping application to handle it might consider one of the following solutions:

- Instead of subscribing for location updates, mapping applications can query for device location. The Location Service supports up to 100 of these requests per second. IMW normally responds to application requests by retrieving the most recently received location report from each device from its database. Only if the database has no recently stored report does IMW query the device.
- When a device is queried, it may take several minutes for the application to receive a response, due to over-the-air data channel loading experienced in either direction. It means that IMW may make several attempts to deliver the message.

IMW supports, by default, up to 20 concurrent requests, but the configurable maximum is 100. System designers should consider that increasing the allowed number of concurrent requests increases the load on the air interface. For ASTRO™ 25 system air interface capacity and performance, see the *ASTRO® 25 Outdoor Location Solution System Planner*.

From a loading perspective, the Location Service can handle up to 100 non-subscribed, immediate location queries per second. System designers should ensure that total query load on the Location Service does not exceed the maximum, which may increase resource consumption (like CPU and memory) and impact performance of the Location Service as well as any other IMW services running on the host. In general, limit the use of location queries, because they use air bandwidth inefficiently.

4.1.5

Parlay X API Licensing

This section describes how to enable Parlay X API access for a developer on a Intelligent Middleware (IMW) system.

Motorola Solutions restricts access to the IMW and the IMW web service with WS-Trust and WS-Security protocols. Only developers that have a Motorola Solutions license can develop a compatible API. These developers receive a run-time developer ID and license key, which must be packaged with the developed application so that it can authenticate and receive access to a deployed IMW system over this interface. IMW uses interoperable Web services protocols, such as WS-Security and WS-Trust, for implementing admission control of licensed third-party applications. The following procedure must be performed before deployment, ideally during the development phase:

- 1 An end-user or vendor becomes a Motorola Solutions application development partner.
- 2 An application developer ID and License key is generated for that end-user/vendor.
- 3 A third-party developer signs up for IMW API access and receives a unique developer ID and a license key that correspond to the licensing agreement. The ID and key are built with the application software to allow the composition of IMW token requests. Developers that sign up to receive IMW SDK/API documentation are issued a unique developer ID and license key, which can be used for all IMW deployments. The client application must provide the ID and key when requesting services (authentication with IMW Security Token Service [STS]) from IMW services. Optionally, IMW may be provisioned to require a valid user name and password from external client applications. IMW can prohibit client application user IDs from logging in to the IMW system administrative console.
- 4 The system administrator configures the API license file on the IMW server. To enable API access on a particular IMW deployment, customers must obtain a license file that grants access to a particular third-party application to the IMW deployment. Customers can retrieve the IMW client license file through the World Wide Radio Solutions Application Partner Portal. The license file contains the list of allowed developer IDs with a list of allowed API features that the application can invoke when interfacing with IMW. The license key of the third-party developer is also in the license file so that the IMW can perform the necessary validation when issuing tokens to the WS clients. The license key is encrypted in the file to prevent disclosure to field personnel.
- 5 The system administrator creates accounts for third-party applications on the IMW host and the account provisions credentials for the application on the IMW server. Optionally, credentials required by IMW to connect to third-party application are configured in IMW. After installing the appropriate API licenses, create and provision security credentials at either end. The IMW system administrator must:

- Create an account in the IMW Microsoft® Windows Active Directory for the third-party application.
 - Set an appropriate password.
 - Set a password expiration policy.
 - Configure the username and password in the third-party application.
 - If the customer chose not to replace the default bootstrap certificates in IMW, export the IMW CA certificate and import it to the third-party application certificate store (so the third-party application can perform appropriate certificate validations during HTTPS handshakes with IMW).
 - If the customer chose to enable “reverse authentication” of IMW with the third-party application, create an account for IMW in the third-party application and configure the same credentials into IMW. Credentials can be a username/password pair or X.509 certificates.
- 6** Comparison of the Developer ID, IMW licensing, and application licenses key validates the application for use.

For more information, see the following sections:

- “Exporting the Root Certificate” in the *Intelligent Middleware Software Installation and Administration Guide*.
- “Importing the Root Client Certificate” in the *Intelligent Middleware Software Installation and Administration Guide*.
- “Importing Client Licenses” in the *Intelligent Middleware Configuration Manager User Guide*.

4.2

IMW REST and WebSocket Interfaces Overview

Representational State Transfer (REST) and WebSocket APIs provide means of obtaining or managing data over HTTP or HTTPS and allow for the following operations:

- manage groups and group members and obtain information about them
- send messages to users and groups on LMR systems
- modify location reporting cadence and location triggers for LMR devices
- query LMR devices location

Applications can access Intelligent Middleware (IMW) data through queries or subscriptions. Applications, in the case of MGM REST API, can query to receive information about groups and make an update to the group, for example, create, add or delete members of a group. Applications can also subscribe to receive notifications using the WebSocket standard, for example to receive notification about changes in the location status of devices, or when members of a group change.

Requests and responses are encoded using the JavaScript Object Notation (JSON) format. JSON is a lightweight, text-based, language-independent data interchange format and provides a lighter, simpler alternative to XML-based messages.

Queries and Subscriptions

IMW REST API queries are made using HTTP operation GET and return information about the last known status of groups. Other HTTP operations include: POST (creation), PUT (update), and DELETE.

Subscriptions allow client applications that use the REST and WebSocket API to receive updates on group data. Applications can subscribe to services using WebSocket (WS) or WebSocket Secure (WSS). Applications must create a separate subscription for each service and each resource. When a WS subscription is created, the application can receive notifications when the information has changed. First, the application receives the full snapshot of data, then only the changes since the last

update. Subscriptions cannot be modified once they are created. To modify the subscription, it needs to be terminated and created again.

Subscriptions and queries on the IMW REST and WebSocket APIs have the following general features:

- Both subscriptions and queries are based on the URL format
- Both queries and subscriptions require authentication and authorization with OAuth tokens
- Queries and subscriptions support the use of Entity Tags (MGM supports Entity Tags only for subscriptions to groups)
- Subscriptions support notification throttling

Entity Tags

Entity Tags are identifiers that provide a mechanism for client applications to query for information containing only the changes since the last update. Entity Tags are assigned by IMW to data sent to a client application that allow applications to query for a specific version of information at a URL. This solution allows for saving the bandwidth as the IMW server does not need to send full information for every query, but only when a change in content occurs. Applications can then use the Entity Tag received with the information coming from IMW in queries and subscriptions requests.

If an application sends a query without an Entity Tag, it receives the full requested data. If a query contains an Entity Tag, the application receives only the partial update of the data based on what has changed in relation to the Entity Tag included in the request. In some cases, the IMW server may not be able to provide a partial update when the information about the requested resource cannot be resolved based on the value of the Entity Tag, for example, when the Entity Tag is old and IMW no longer holds information about it, or the Entity Tag value does not match the resource identifier included in the request. In this scenario, IMW sends the full information to the application, as if the request was without an Entity Tag.

Notification Throttling

In the case when subscriptions are made by a client application on a wireless device, frequent incoming notifications may significantly reduce the battery life on the device. To minimize battery usage, IMW sends notifications at a default frequency (30 seconds). If an application has more than one subscription, IMW does not send the data for each subscription separately but instead sends the notifications for all subscriptions at the same moment. Throttling can be disabled when the subscription is created.

Authentication and Authorization

IMW provides IMW administrators (for example owners of agencies) with mechanisms to authenticate and authorize client applications that try to access IMW resources. The IMW authorization framework is based on the OAuth 2.0 standard and all client applications using the REST and WebSocket API must support authentication and authorization with OAuth Access Tokens. Client applications requesting OAuth Access Tokens must request permissions for each API they want to access, and, in some cases, specify what operations they wish to perform using the API.

OAuth Access Tokens are issued by the Identity Service server and allow the client application to authenticate with the IMW server. Tokens have an expiration time and need to be regenerated periodically.

Authorization provides another security layer by determining what resources can be accessed by the client application and what operations on these resources the application can perform. Authorization can be configured on the Identity Service server and in the IMW Configuration Manager on the IMW server.

4.2.1

IMW REST and WebSocket APIs

The Intelligent Middleware (IMW) REST and WebSocket APIs are based on the APIs defined in Open Mobile Alliance (OMA) ParlayREST specifications. IMW offers the following APIs:

MGM API

Multi Group Management (MGM) REST API supports operations on LMR talkgroups and LMR sitegroups, Static Groups, and Application Groups. The operations include:

- Creating, updating, and deleting Application Groups
- Adding and removing members of Application Groups
- Adding and removing groups to/from Application Group
- Querying the list of Static Groups and Application Groups
- Querying the content of groups
- Subscribing to changes in the content of groups and group lists

The access to some of the operations may be restricted based on the authorization scopes that have been granted to the requester.

MGM API supports Entity Tags with subscriptions to groups.

Messaging API

Messaging REST API provides an alternative to messaging using the XMPP protocol. The API allows sending messages to the following recipients:

- ASTRO® 25 users or devices
- ASTRO® talkgroups or sitegroups
- Application Groups
- Static Groups

Presence API (supported only for Converged Services Client)

The Presence REST API provides an interface for applications to view status information on the availability of a wireless device, or its user, on the network. Client applications can obtain presence data by means of HTTP queries or WebSocket-based subscriptions. The API supports Entity Tags and notification throttling.

Location API (supported only for Converged Services Client)

The Location REST API provides an interface to obtain location data. Client applications can obtain location data by means of HTTP queries or WebSocket-based subscriptions. The API supports the following operations:

- Querying device location
- Subscribing to device location updates

The Location REST API supports Entity Tags and notification throttling.

Telemetry API

The IMW Telemetry API is based on the IEEE 1451 Standard for a Smart Transducer Interface for Sensors and Actuators. It allows users to manage Transducer Interface Modules (TIMs) and its associated transducer channels (sensors/actuators) and subscribe or query sensor information connected to devices in the system.

4.2.2

IMW REST and WebSocket Interface Capacity

Intelligent Middleware (IMW) Representational State Transfer (REST) Interface and WebSocket capacities differ depending on the hardware configuration, network system, and traffic. The following

tables present the IMW REST and WebSocket capacities for Presence and Location subscriptions in low and high tier hardware configurations, and for steady and busy hour traffic for various network systems.

Table 12: Maximum Values for IMW REST Presence Subscriptions in a Total Box Steady State

For more information on the available hardware configurations, see: [Hardware Component Configuration on page 20](#)

System	Presence Subscriptions	
	Capabilities	Traffic of
		ASTRO or Dimetra devices
ASTRO + Advanced Messaging Solution (AMS)	<ul style="list-style-type: none"> Total number of opened subscriptions: 9.9 Average number of tracked devices/users for single subscription: 100 	<ul style="list-style-type: none"> Total number of updates for the whole system per second: 96
Low Tier DIMETRA + BB DEMO	<ul style="list-style-type: none"> Total number of opened subscriptions: 9.9 Average number of tracked devices/users for single subscription: 500 	<ul style="list-style-type: none"> Total number updates for the whole system per second: 133.14
DIMETRA + BB DEMO	<ul style="list-style-type: none"> Total number of opened subscriptions: 9.9 Average number of tracked devices/users for single subscription: 500 	<ul style="list-style-type: none"> Total number updates for the whole system per second: 466
BB	<ul style="list-style-type: none"> Total number of opened subscriptions: 1666.5 Average number of tracked devices/users for single subscription: 500 	

Table 13: Maximum Values for IMW REST Location Subscriptions in a Total Box Steady State

System	Location Subscriptions	
	Capabilities	Traffic of
		ASTRO or Dimetra devices
ASTRO + BB DEMO + AMS	<ul style="list-style-type: none"> Total number of opened subscriptions: 9.9 Average number of tracked devices/users for single subscription: 50 	<ul style="list-style-type: none"> Total number of updates for the whole system per second: 1200
Low Tier DIMETRA + BB DEMO	<ul style="list-style-type: none"> Total number of opened subscriptions: 9.9 	<ul style="list-style-type: none"> Total number updates for the whole system per second: 300

System	Location Subscriptions	
	Capabilities	Traffic of
		ASTRO or Dimetra devices
	<ul style="list-style-type: none"> Average number of tracked devices/users for single subscription: 50 	
DIMETRA + BB DEMO	<ul style="list-style-type: none"> Total number of opened subscriptions: 9.9 Average number of tracked devices/users for single subscription: 50 	<ul style="list-style-type: none"> Total number updates for the whole system per second: 1050
BB	<ul style="list-style-type: none"> Total number of opened subscriptions: 1666.5 Average number of tracked devices/users for single subscription: 50 	

Table 14: Maximum Values for IMW REST Presence Subscriptions in a Total Box Busy Hour

System	Presence Subscriptions	
	Capabilities	Traffic of
		ASTRO or Dimetra devices
ASTRO + BB DEMO + AMS	<ul style="list-style-type: none"> Total number of opened subscriptions: 19.8 Average number of tracked devices/users for single subscription: 100 	<ul style="list-style-type: none"> Total number of updates for the whole system per second: 96
Low Tier DIMETRA + BB DEMO	<ul style="list-style-type: none"> Total number of opened subscriptions: 9.9 Average number of tracked devices/users for single subscription: 500 	<ul style="list-style-type: none"> Total number updates for the whole system per second: 133.14
DIMETRA + BB DEMO	<ul style="list-style-type: none"> Total number of opened subscriptions: 9.9 Average number of tracked devices/users for single subscription: 500 	<ul style="list-style-type: none"> Total number updates for the whole system per second: 466
BB	<ul style="list-style-type: none"> Total number of opened subscriptions: 3333 Average number of tracked devices/users for single subscription: 500 	

Table 15: Maximum Values for IMW REST Location Subscriptions in a Total Box Busy Hour State

System	Location Subscriptions	
	Capabilities	Traffic of
		ASTRO or Dimetra devices
ASTRO + BB DEMO + AMS	<ul style="list-style-type: none">• Total number of opened sub- scriptions: 19.8• Average number of tracked devi- ces/users for single subscription: 50	<ul style="list-style-type: none">• Total number of updates for the whole system per second: 1600
Low Tier DIMETRA + BB DEMO	<ul style="list-style-type: none">• Total number of opened sub- scriptions: 19.9• Average number of tracked devi- ces/users for single subscription: 50	<ul style="list-style-type: none">• Total number updates for the whole system per second: 450
DIMETRA + BB DEMO	<ul style="list-style-type: none">• Total number of opened sub- scriptions: 19.9• Average number of tracked devi- ces/users for single subscription: 50	<ul style="list-style-type: none">• Total number updates for the whole system per second: 1575
BB	<ul style="list-style-type: none">• Total number of opened sub- scriptions: 3333• Average number of tracked devi- ces/users for single subscription: 50	

4.2.3

Developer Access to IMW REST and WebSocket API

Intelligent Middleware (IMW) offers a variety of data services such as Location, Presence, Messaging, and Multi-Group Management (MGM) that can be leveraged by third-party applications. Developers can create applications using IMW interfaces. The following section describes obtaining the access to IMW REST and WebSocket API, lifecycle of API use, and parties involved in the process.

There are three phases in the lifecycle of API use:

1 Development

In the development phase, the Developer first accesses the Motorola Solutions Intelligent Middleware Developer portal at the following URL: http://www.motorolasolutions.com/en_us/products/intelligent-middleware.html

The website allows the Developer to request a developer license and access to the Developer Portal.

Motorola Solutions Developer Support team processes the Developer request, and provides access to the Developer Portal along with credentials the Developer can use to access Developer Support resources, including the development Sandbox. One of these credentials is a unique API Key of the Developer. The API Key identifies the Developer as a licensed IMW API Developer, and must be built in to any applications that the Developer creates for use on Customer IMW deployments.

Motorola Solutions also provides a License Key File to the Developer, that the Developer can provide to a Customer to install in the IMW of the Customer. This provisions the Customer IMW

with the API Key of the Developer, giving the Developer's applications access to the Customer IMW APIs.

Each application that attempts to use a IMW API must also provide deployment-specific credentials that are in the form of a Client ID and optionally a password. These credentials vary on each deployment, so the Developer should build their application in such a way as to allow these credentials to be provisioned on the application.

Once the application is built, the Developer provides it to the Customer for Deployment.

2 Deployment

In the Deployment phase, the Customer and the Developer deploy an application on the system of the Customer. The application is provisioned to access the Customer IMW APIs.

In order to accomplish this, the Developer first provides the Customer with the License Key file, and the Customer provisions it in the Customer IMW, thus supplying the IMW with the API Key of the Developer. Then the Developer registers the application with the Customer, providing information about what application type is being registered, what services (scopes) the application uses, and the Redirect URL (if any, depending on the application type) that the application utilizes. The Customer provisions their Identity Server with this information for the Developer, and provides the Developer with a Client ID and, optionally, a Secret. The Developer provisions the Client ID and Secret in the application, and makes the application available for distribution to the Application End Users via the Customer's chosen application distribution mechanism.

Once the application is available for distribution, it is ready for Utilization.

3 Utilization

In the Utilization phase, Application End Users acquire the application from the Customer's distribution mechanism, and install and run the application on the application client device. Depending on the application type, this application client device may be a computer or a mobile device like a smartphone or tablet, and the Application End User may have to log in to the application with user credentials issued by the Customer. Depending on the application type, the Customer may have to provision these user credentials in the IMW and the Identity Server in order for the IMW to authenticate the identity of the Application End User, and to authorize the Application End User to use the services that the IMW provides on the APIs.

Once the Application End User has successfully logged into the application, the Application End User can utilize the services provided by the application using the IMW APIs.

In each of these three phases, several roles are involved in the use of the APIs:

Motorola Solutions Developer Support

provides documentation for the APIs, issues licensing credentials for API developers, deploys a development Sandbox for developers to use, and provides support to answer developer questions.

Developer

creates applications using IMW REST and WebSocket APIs.

Customer

deploys a IMW on a system to provide services to the end users of the system.

Application End User

uses applications to access IMW services.



NOTICE: Application End User may be a mobile device user that is already provisioned in the IMW of the Customer.

4.2.3.1

Adding Application to the System

Prerequisites:

The application developer must provide the deployment administrator with the following information:

- Redirect URLs
- Client License File
- Client Certificate

The deployment administrator must provide the application developer with the following information:

- IMW, Identity Server, and Messaging Server IP addresses or FQDNs
- IMW root and intermediate certificates (see "Exporting the Root Certificate" in the *Software Installation and Administration User Guide*)

Procedure:

- 1 Provision Client ID/Secret with Redirect URL in the Identity Server. See "Adding IMW Application Account" in the *Software Installation and Administration User Guide*.
- 2 Provision IMW with client License key file. See "Configuring Applications" in the *Configuration Manager User Guide*.
- 3 Provision IMW with the Client ID and Secret as Application Username and Password. See "Adding Applications" in the *Configuration Manager User Guide*.

The data you enter when adding an application has to match with the corresponding setup entries in the Identity Server.

- 4 If necessary, provision IMW with client certificate. See "Configuring Applications" in *Configuration Manager User Guide*.

Postrequisites: Provide Client ID and Secret (Application Username and Password in the preceding process) to the application developer or user.

4.2.3.2

Application Types

The following table explains the types of applications that developers can create, and the application data provisioning required by the Intelligent Middleware (IMW) and Identity Server.

Table 16: Application Types

Application Type	Description	Information needed
Client Application	A client application uses APIs based on its own identity, not that of its users. If users are required to log in, the application authenticates these users itself, and does not present their identities on the APIs.	API Key, License Key File, Client ID/Secret Scopes, Server Addresses, Server TLS Certificates
Web Application	A web application runs on a web server. Application End Users access the application via an HTML user interface rendered in a user-agent (web browser, for example) on the device used by the Application End User.	API Key, License Key File, Client ID/Secret, Scopes, Redirect URL, User ID/Password, Server Addresses, Server TLS Certificates
User-agent-based Application	A user-agent-based application is an application in which the application code (java-	API Key, License Key File, Client ID/Secret, Scopes, Redirect URL, User ID/Password,

Application Type	Description	Information needed
	script, for example) is downloaded from a web server and executes within a user-agent (web browser, for example) on the device used by the Application End User.	Server Addresses, Server TLS Certificates
Native Application	A native application is an application installed and executed on the device used by the Application End User.	API Key, License Key File, Client ID/Secret, Scopes, Redirect URL, User ID/Password, Server Addresses, Server TLS Certificates

4.2.3.3

Application Data Summary

The following table summarizes information needed to use the Intelligent Middleware (IMW) REST and WebSocket APIs, including the purpose, source, and use of the information.

Table 17: Application Data Summary

Credential	Purpose	Source	Use	Application Type
API Key	For all IMW deployments, identifies the Developer as one that is licensed by Motorola Solutions.	Motorola Solutions Developer Support provides the API Key to the Developer.	Developer builds the API Key into their application.	All application types
License Key File	Provides the Developer's API Key for provisioning in the IMW.	Motorola Solutions Developer Support provides the License Key File to the Developer.	Developer provides License Key File containing the API Key to the Customer for provisioning on Customer IMW.	All application types
Client ID/ Secret	Identifies the Developer's application as a legitimate application on a given Customer IMW deployment.	Customer provides the Client ID/Secret to the Developer when the application is registered on the Customer system.	Developer provisions Client ID/ Secret in the application. Customer provisions Client ID/Secret in the Identity Server and the Client ID in the IMW.	All application types
Scopes	Identifies the API services that the application uses.	Motorola Solutions Developer Support identifies the available	Developer builds defined and used Scopes into the Applica-	All application types

Credential	Purpose	Source	Use	Application Type
		Scopes for the Developer in the API documentation.	tion, and informs the Customer of the Scopes used. Customer provisions the used Scopes into the Identity Server for the Developer's Client ID.	
Redirect URL	Identifies the Application End User on the Customer IMW deployment.	Customer provides the credentials to the Application End User.	Customer provisions User ID/ Password in Identity Server and the User ID in the IMW. Application End User enters User ID/Password to login to application.	Web Applications, User-agent-based Applications, Native Applications
User ID/ Password	Identifies the Application End User on the Customer IMW deployment.	Customer provides the credentials to the Application End User.	Customer provisions User ID/ Password in Identity Server and the User ID in the IMW. Application End User enters User ID/Password to login to application.	Web Applications, User-agent-based Applications, Native Applications
Server Addresses	Allows application to communicate with the deployed Intelligent Middleware servers.	Customer provides Server Addresses to the Developer and the Application End User.	Developer and Application End-User provision Server Addresses in application.	All application types
Server Certificates	Allows Intelligent Middleware servers to verify TLS sessions with the application.	Customer provides Server Certificates to the Developer and the Application End User.	Developer and Application End-User provision Server Certificates in the device that the application runs on.	All application types

4.3

Other Legacy Interfaces

The Location Service is backward compatible with legacy ASTRO® 25 Outdoor Location Solution mapping applications that use the legacy ASTRO® 25 Location API.

The service is backward compatible with the MotoMapping application, as well as other legacy MotoLocator mapping applications that use an existing MotoLocator mapping API in Dimetra IP networks.

Intelligent Middleware (IMW) legacy interfaces include:

- PN-Watcher Protocol Interface
- MotoLocator Web services API



NOTICE: The MLS API is installed only with the Location with Additional Modules suite.

- ASTRO® 25 systems Location Request Response Protocol (LRRP) API

4.3.1

Legacy PN-Watcher Interface (Presence)

Intelligent Middleware (IMW) supports the legacy PN-Watcher interface to provide presence information to legacy Motorola Solutions watcher applications, including:

- Text Messaging Services
- POP25

The PN-Watcher interface is not an open interface. Third-party applications must use the most recent Parlay X interface.

Keep-Alives on the PN-Watcher Interface

The PN-Watcher interface employs a Keep-Alive message from a watcher and a Keep-Alive acknowledgement message from the Presence Service in the following manner:

- 1 A watcher sends a UDP Keep-Alive message to the same UDP destination port number from which subscription messages are sent.
- 2 The Presence Service returns a UDP Keep-Alive acknowledgement message to the source UDP port number of the Keep-Alive message.
- 3 Watchers may take appropriate action if no acknowledgement is received for any Keep-Alive messages.

4.3.2

Legacy MotoLocator Web Services API

Dimetra IP systems that deploy legacy Motorola Solutions mapping applications (such as MotoMapping) use the legacy Web services-based MotoLocator API. The Legacy MotoLocator Web Services API is made available for MotoLocator applications.

4.3.3

ASTRO 25 System LRRP API

Legacy Mapping Applications written for ASTRO® 25 Outdoor Location Solution can interface with the Intelligent Middleware (IMW) server using the legacy ASTRO® 25 systems Location API.

The Legacy API is the Project 25 (P25) standards-based (LRRP) in Extensible Markup Language (XML) form for exchanging location-related requests and responses over TCP/IP v4. For third-party

applications, this legacy API provides additional features (compared to the 3GPP Parlay X interface), such as:

- Triggering telemetry outputs on a subscriber.
- Reporting device types, along with location reports.
- Querying a device type.

Chapter 5

Network Configuration

5.1

ASTRO 25 System Network Configuration

Configure the DMZ-RNI firewall and CEN border router to enable communications between the customer network and subscriber radios through UDP port numbers that are reserved for location reporting.

Configure CADIs for ASTRO® 25 if tracking ASTRO® 25 devices in ASTRO® 25 Talkgroups or Sites, or using the GEO Select features.

See the “Installation” and “Configuration” sections of the *ASTRO® 25 Integrated Voice and Data System Gateways - GGM8000* or *ASTRO® 25 Integrated Voice and Data System Routers - S6000/S2500* manuals for more information.

5.2

Dimetra IP System Network Configuration

Configure the RNI-screened-subnet firewall to enable communications between the Location Service and the following:

- MCADIs
- ATIA
- Short Data Router (SDR)
- Air Traffic Router (ATR)

5.3

IMW Connectivity Within a Network Environment

Intelligent Middleware (IMW) connectivity within the network environment of an agency works according to a set of rules.

- 1 Each IMW must be connected to at least one RAN (ASTRO, or Dimetra).
- 2 Maximum 100 applications may connect to each IMW.
- 3 An agency may deploy more than one IMW, with the following rules applying:
 - A radio can report presence and location to one IMW, so multiple IMWs each support a unique set of radios.
 - All applications may connect to all IMWs, or applications may be “local” to one or more IMW, for example fire and police radios may report to different IMWs and fire or police applications may connect to the respective IMWs.
- 4 IMW may be deployed on a pair of servers in a High Availability (HA) configuration.
 - Only one IMW server may be connected to the application and RAN at a given time.
 - In HA deployments, applications using ParlayX API must implement the heart beat interface to detect loss of the IMW service.
 - When the IMW is deployed with an ASTRO RAN, applications are configured with one IMW application address, regardless of which IMW is the active one.

- When the IMW is deployed with a Dimetra RAN, applications are configured with two IMW addresses. The applications may attempt to open both IMW addresses but only the active IMW responds.

Appendix A

IMW Location Archive Writer Database Disk Space Requirements

Intelligent Middleware (IMW) Location Archive Writer requires a considerable amount of disk space to store historical location data so it is recommended to estimate the required disk space in advance before setting up the system. Taking this precaution allows you to assess if additional storage is required and if the customer needs to obtain an extra hard drive. The following information also helps estimate approximate disk space required for archiving location data, if the customer wants to use this option.

IMW Location Archive Writer Database

During IMW installation, the installer creates a database for storing historical location data. The predicted size of the database is calculated on the basis of the number of devices reporting location, frequency of location updates, and the number of days for which the data is stored. For each day, IMW creates a table in which the data is stored. At the moment of installation, IMW creates two tables: one for the current day and one for the next day. Then, for each new day, a new table is created. To make the predicted size of the table more precise, IMW calculates the space separately for devices sending only location updates and devices sending location and telemetry data, as telemetry data takes up considerably more disk space than location data.

The customer must decide for how many days the tables will be kept in the database. The parameter that defines it is called the **Number of Historical Location Storage Days** and it is 7 by default. The total disk space required for the database includes the number of historical location days plus two days (the current day and the next day).

Since it is not possible to predict exactly the amount of data to be stored, the size of the tables is not fixed. If, on a given day, the incoming data exceeds the limits set up during installation, the table will expand. If, however, the amount of data exceeds the total limit for the database size, Archive Writer starts deleting the location history tables starting from the oldest to make space for the new updates.

If the table for a given day reaches the maximum number of historical location days, the table for that day is removed from the database to make space for the new day. If the customer decides to enable archiving, that day is backed up and moved to the backup location set up as **Backup Files Directory** during installation. The customer is able to retrieve location history days from the folder if needed.

Calculating Database Disk Space Requirements

You can calculate approximate required disk space using the formulas in the following steps:

- 1 Calculate the predicted table size for devices **without telemetry** for one day:

$$\text{table 1 [MB]} = 0.5 * n * f$$

where:

n is the number of devices without telemetry (0–100,000)

f is the predicted frequency of location updates from devices without telemetry per minute (0–60)



NOTICE: The update rate is calculated by dividing 60 by the frequency of location updates in seconds. For example, if a device is configured to report location every 30 seconds, the frequency of location updates is estimated as follows: $60 / 30 \text{ (seconds)} = 2$. If a device is configured to report location once every 120 seconds, the frequency of location updates is 0.5.

Example: For 2000 devices without telemetry that are expected to send location updates once every 60 seconds, the predicted disk space is:

$$0.5 * 2000 * 1 = 1000 \text{ MB}$$

2 Calculate the predicted table size for devices **with telemetry** for one day:

$$\text{table 2 [MB]} = 23 * n * f$$

where:

n is the number of devices with telemetry (0–100,000)

f is the predicted frequency of location updates from devices with telemetry per minute (0–60)

Example: For 1000 devices with telemetry that are expected to send location updates once every 120 seconds, the predicted disk space is:

$$23 * 1000 * 0.5 = 11500 \text{ MB}$$

3 Calculate the total required disk space for the database:

$$\text{Total disk space [MB]} = (\text{table 1} + \text{table 2}) * (\text{number of historical location storage days} + 2)$$

where number of historical location storage days is the number of days for which you want to store the location history (2–366). Two additional days are added to include the tables for the current day and next day.

Example: $(1000 + 11500) * (14 + 2) = 200000 \text{ MB}$

The predicted required disk space for storing 14 days of historical data with the above parameters is approximately 195 GB.



NOTICE: IMW requires at least additional 2 GB free hard drive that serve as buffer preventing from running out of disk space.