

KODIAK

Carrier-based Deployment

Broadband PTT Product Specification

Release 12.3



DECEMBER 2023

© 2023 Motorola Solutions, Inc. All Rights Reserved.

MN009625A01-005

Intellectual Property and Regulatory Notices

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.

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.

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.

License Rights

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 nonexclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Open Source Content

This product may contain Open Source software used under license. Refer to the product installation media for full Open Source Legal Notices and Attribution content.

European Union (EU) and United Kingdom (UK) Waste of Electrical and Electronic Equipment (WEEE) Directive



The European Union's WEEE directive and the UK's WEEE regulation require that products sold into EU countries and the UK must have the crossed-out wheeled bin label on the product (or the package in some cases). As defined by the WEEE directive, this crossed-out wheeled bin label means that customers and end users in EU and UK countries should not dispose of electronic and electrical equipment or accessories in household waste.

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

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 mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

© 2023 Motorola Solutions, Inc. All Rights Reserved

Contact Us

The Centralized Managed Support Operations (CMSO) is the primary contact for technical support included in your organization's service agreement with Motorola Solutions. To enable faster response time to customer issues, Motorola Solutions provides support from multiple countries around the world.

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

- To confirm troubleshooting results and analysis before taking action

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

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

Comments

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

Provide the following information when reporting a documentation error:

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

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to <https://learning.motorolasolutions.com> to view the current course offerings and technology paths.

Document History

Version	Description	Date
MN009625A01-005	<p>Updated Large talkgroups information in the following sections:</p> <ul style="list-style-type: none">• Introduction on page 16• Talkgroup Member Details on page 38• Location Reporting on page 64• Location Tracking/Geofencing on page 65• Video Services on page 74 <p>Updated Cross-Carrier on page 96 with the Cross-carrier subscribers provisioning information.</p> <p>Updated SIM Change on page 133 with the note: "If your device contains a "Data Only SIM Card", it will need to be reactivated through the WAVE Portal"</p> <p>Updated Security on page 140 chapter and the following sections:</p> <ul style="list-style-type: none">• System Access Control on page 140• Encryption of Data in Transit on page 140• PTT Application Security on page 140• Server Encryption of Data at Rest on page 141	December 2023
MN009625A01-004	<p>Updated Integrated Secure Messaging on page 69 with the 3GPP MCDATA compliant messaging solution.</p>	September 2023
MN009625A01-003	<p>Updated the Supported Devices in Introduction on page 16.</p> <p>Updated browser support. User can use Google Chrome, Microsoft Edge, or Mozilla Firefox.</p> <p>Updated Access Control on page 99. Added the</p>	July 2023

Version	Description	Date
MN009625A01-002	Multifactor Authentication (MFA), Password Management, and updated Password Requirements sections. Updated PTT Services on page 25 section - Tones section with Emergency Cancel Tone.	June 2023
MN009625A01-001	Updated Fault Management on page 144 with SNMP V3. Removed Windows 8 software support. Removed Microsoft Internet Explorer support. Added the support of ESRI map service. See Location Message on page 72 .	November 2022

Contents

Intellectual Property and Regulatory Notices.....	2
Contact Us.....	3
Document History.....	4
List of Figures.....	13
List of Tables.....	14
Chapter 1: Introduction.....	16
1.1 Scope.....	21
1.2 References.....	21
1.3 What's New in this Release?.....	22
Chapter 2: PTT Services.....	25
2.1 Call Origination.....	25
2.2 Tones.....	25
2.3 Call Teardown.....	28
2.4 Call Reception.....	28
2.5 Call Interaction.....	28
2.6 PTT Roaming Support.....	30
2.7 Call Rejoin.....	31
2.8 Alerts.....	32
2.8.1 Instant Personal Alerts.....	32
2.8.2 Missed Call Alerts.....	32
2.8.3 Geofence Alerts.....	33
2.9 Affiliation.....	33
2.9.1 Service Affiliation.....	35
2.9.2 Notifications.....	35
2.10 Affiliation Monitoring.....	35
2.10.1 Affiliation Monitoring User Experience.....	36
2.10.2 Supported Talkgroups.....	36
2.10.3 Affiliated Talkgroup Member.....	36
2.10.4 Configuration.....	37
2.11 Remote Talkgroup Select.....	37
2.11.1 Supported User Types.....	37
2.12 MCX Talkgroups.....	37
2.12.1 Configuration.....	38
2.12.2 Talkgroup Member Details.....	38
2.13 Background Call Mode.....	38

2.13.1 PTT Accessory Support.....	39
2.13.2 Dedicated PTT Button.....	39
2.14 Broadcast Calling and Messaging	39
2.15 Device ID Management.....	40
2.15.1 Provisioning.....	41
2.15.2 PTT User Type "User".....	41
2.15.3 User ID.....	41
2.15.4 User Registration.....	41
2.15.5 Password Management.....	42
2.15.6 Password Security.....	42
2.15.7 Administrator Functionality.....	42
2.15.8 First Time Login.....	43
2.15.9 Caveats.....	44
2.16 First-to-Answer Private Calls.....	44
2.17 One Touch Calling.....	44
2.17.1 Server-Based DRX Optimization.....	44
2.18 Operational Status Messaging (OSM).....	45
2.18.1 CAT Administration.....	46
2.18.2 Caveats.....	46
2.18.3 Dispatch.....	47
2.18.4 Third-Party Dispatch.....	47
2.18.5 Motorola Solutions LEX L11.....	47
2.19 Dynamic Area-Based Talkgroups.....	48
2.20 2-Way Calls to External Telephony Users.....	49
2.20.1 2-Way Calls to External Telephony Users Experience.....	49
2.21 PTT Call History.....	49
2.22 PTT Voice Message Fallback.....	50
2.23 Silent Mode Behavior (Privacy Mode).....	50
2.24 Simultaneous PTT Audio Sessions.....	51
2.25 Simultaneous PTT Video Sessions.....	52
2.26 Supervisory Override (Talker Priority).....	52
2.27 Talkgroup Scanning	52
2.28 Authorized User.....	55
2.29 Remote Supervision.....	55
2.29.1 User Check.....	55
2.29.2 Enable or Disable PTT Service.....	56
2.29.3 Remote Emergency	56
2.30 Ambient Listening.....	56
2.31 Discreet Listening.....	58

2.32 Wi-Fi Support.....	58
2.33 Audio Codec Support.....	59
2.34 Corporate Address-Book Search.....	59
2.35 Userless Device Mode.....	60
Chapter 3: Presence Service.....	61
3.1 Self-Presence.....	61
3.2 Contact Presence.....	62
3.3 Presence Notification Options.....	62
3.4 Decoupled Presence for Calling and Alert Origination.....	63
3.5 Temporarily Unreachable SMS Configuration.....	63
3.6 Presence Throttling.....	63
Chapter 4: Location Services.....	64
4.1 Location Reporting.....	64
4.1.1 On-demand Location Update.....	64
4.1.1.1 One Time On-Demand Location Update.....	65
4.1.1.2 Periodic On-Demand Location Update.....	65
4.2 Location Tracking/Geofencing	65
Chapter 5: Messaging Services.....	69
5.1 Integrated Secure Messaging.....	69
5.1.1 Media Types.....	69
5.1.2 Secure Text Messaging.....	70
5.1.3 Multimedia Content.....	71
5.1.4 Location Message.....	72
5.1.5 Store-and-Forward.....	72
5.1.6 Broadcast Secure Text Messaging.....	73
5.1.7 Origination Permissions.....	73
Chapter 6: Video Services	74
6.1 Video Session Types.....	74
6.2 Supported Video Resolutions.....	75
6.3 Push Video User Experience.....	75
6.4 Pull Video User Experience.....	75
6.5 Video Interaction.....	75
6.6 Telephony Interaction.....	77
6.7 Configuration and Provisioning.....	77
6.8 Caveats.....	78
6.9 Supported User Types.....	79
Chapter 7: Emergency Services.....	80
7.1 Emergency Calling and Alert.....	80

7.1.1 Emergency Life Cycle.....	80
7.1.2 CAT Administration Control.....	81
7.1.3 Emergency Originator.....	81
7.1.4 Emergency Recipient - Talkgroup Steering.....	82
7.1.5 Emergency Cancellation.....	82
7.1.6 Authorized User Recipient of Emergency Call.....	83
7.1.7 Authorized User or Dispatcher Remote Emergency.....	83
7.1.8 More Frequent Location Updates During User Emergency.....	83
7.1.9 Caveats.....	83
7.1.10 Supported User Types.....	84
Chapter 8: Broadband Regroup Service.....	85
8.1 Authorized user.....	85
8.2 Preconfigured Template Groups.....	85
8.3 User Experience.....	85
8.4 Emergency Call and Alert	86
8.5 Talkgroup Scanning.....	86
8.6 Interop Groups.....	86
Chapter 9: PTT Applications.....	87
9.1 PTT Standard Application Mode.....	91
9.2 PTT Radio Application Mode.....	91
9.2.1 Talkgroup Scanning.....	93
9.2.2 Missed Call Alerts.....	93
9.2.3 Scan List Administration.....	93
9.2.4 Configuration.....	93
9.2.5 Hook Signaling.....	93
9.2.6 Background Call Mode.....	94
9.2.7 User Type.....	94
9.2.8 User Provisioning.....	94
9.2.9 Zones.....	95
9.3 PTT Application Upgrade Notification.....	95
9.4 Cross-Carrier.....	96
9.5 Dispatch.....	96
9.6 PTT Accessory Support.....	97
9.7 Cellular Network Transitions.....	97
9.8 IPv4 and IPv6 Fallback Support.....	98
9.9 Backward Compatibility.....	98
Chapter 10: Administration.....	99
10.1 Central Admin Tool.....	99

10.1.1	Access Control.....	99
10.1.2	PTT Users.....	100
10.1.3	Talkgroups.....	101
10.1.4	External Users.....	102
10.1.5	Integrated Users.....	102
10.1.6	Interop Connections.....	102
10.1.7	User Sets.....	103
10.2	Permissions.....	103
10.3	Contact and Talkgroup Management.....	103
10.3.1	Addressing.....	103
10.3.2	Dial Plans.....	103
10.3.3	Contact and Talkgroup Sizes.....	104
10.3.4	Contact and Talkgroup Name Length.....	104
10.4	User Profiles.....	104
10.4.1	Talkgroup.....	105
10.4.2	Talkgroup Profile.....	105
10.4.3	Talkgroup and User Profile Sharing.....	106
10.4.4	User Role-Based Login.....	106
10.5	Corporate-Level Configuration.....	107
10.6	Restore Contacts and Talkgroups.....	107
10.7	Display Name and Customization of Contact Names.....	107
10.8	Auto-Pairing.....	108
Chapter 11:	APIs.....	109
11.1	Converged Data APIs	109
11.2	3GPP Mission Critical (MC) Standard APIs.....	109
11.3	PTT Mobile APIs.....	113
11.3.1	Integrated Mobile APIs.....	113
11.3.2	PTT App-to-App and Accessory API.....	114
11.4	PTT Web Application APIs.....	114
11.4.1	Integrated Web APIs.....	114
11.4.2	Integrated Tracking APIs.....	115
11.4.3	Security and Encryption.....	116
11.5	PTT-Integrated Authentication API.....	116
11.6	Life-Cycle Management for APIs.....	117
11.6.1	Backward Compatibility.....	117
11.6.2	End of Support (EOS).....	117
Chapter 12:	Interoperability with Land Mobile Radio (LMR) Systems.....	118
12.1	Project 25 (P25) Inter-RF Subsystem Interface (ISSI).....	118
12.2	Radio over IP (RoIP).....	118

12.3 Critical Connect Interoperability (Optional).....	118
12.3.1 LMR Interoperability based on Feature Set.....	119
Chapter 13: Subscriber Life-Cycle Management.....	120
13.1 Subscriber Types.....	120
13.1.1 Personal User.....	120
13.1.2 Administrator-Managed.....	120
13.1.3 Administrator-Managed and Personal User-Managed.....	121
13.2 Subscriber States.....	121
13.3 Subscriber Provisioning.....	121
13.3.1 Feature Sets and Add-On Features.....	122
13.3.2 Welcome SMS (Optional).....	125
13.3.3 User Types Provisioning and Restrictions.....	125
13.3.4 Activation of PTT Applications over Cellular Network.....	126
13.3.5 Activation of Wi-Fi Only and Dispatch PTT Applications.....	127
13.3.6 Summary of Provisioning Methods.....	127
13.3.7 Provisioning with License Packs and License Management Tool.....	128
13.3.8 Auto-Pairing.....	130
13.4 PTT Activation / Authentication.....	130
13.4.1 Cellular Network Activation / Authentication.....	130
13.4.2 Multiple PoC Servers Support.....	131
13.4.3 Wi-Fi Network Activation / Authentication.....	131
13.4.4 Wi-Fi Only Device Activation.....	132
13.4.5 Device Activation Control.....	132
13.5 MSISDN Change.....	132
13.6 SIM Change.....	133
13.7 Device Change.....	133
Chapter 14: Branding and Language Support.....	134
Chapter 15: Quality of Service (QoS), Priority and Preemption (QPP).....	136
15.1 QPP Packages.....	136
15.2 Additional Settings.....	138
15.3 Rx Interface.....	138
Chapter 16: Security.....	140
16.1 System Access Control.....	140
16.2 Encryption of Data in Transit.....	140
16.3 PTT Application Security.....	140
16.4 Server Encryption of Data at Rest.....	141
Chapter 17: Platform High Availability.....	142
17.1 PTT Application Server Notification Channel on Standby Site.....	142

Chapter 18: Operations, Administration, Maintenance, and Provisioning (OAMP)... 143

18.1 License Management Tool (LMT)..... 143

18.2 Customer Service Support Web Portal (WCSR)..... 143

 18.2.1 WCSR ID Management..... 144

18.3 Network Management..... 144

 18.3.1 Fault Management..... 144

 18.3.2 Configuration Management..... 145

 18.3.3 Performance Management..... 145

 18.3.4 Revenue Assurance Reconciliation (RAR)..... 146

 18.3.5 Usage Detail Records (UDR)..... 146

 18.3.6 Log Server – Server and PTT Application Logging..... 148

 18.3.7 Backup / Restore..... 150

Chapter 19: Regulatory Compliance..... 151

19.1 Lawful Intercept..... 151

 19.1.1 PTT Calling, Presence, IPA..... 151

 19.1.2 Integrated Secure Messaging..... 151

19.2 Retrieval of Stored Communications (PSC)..... 152

List of Figures

Figure 1: Call Rejoin Example.....	32
Figure 2: Device Authentication Process.....	126
Figure 3: SIM Swap and IMSI Detection Flow.....	133

List of Tables

Table 1: Tones.....	25
Table 2: In-Call Tones.....	27
Table 3: User Call Origination Permissions.....	27
Table 4: Incoming Call Interaction.....	29
Table 5: Outgoing Call Interaction.....	30
Table 6: Services on a Talkgroup for Collaboration/Command User with PTT Radio Mode.....	33
Table 7: Services on Affiliated Talkgroup for MCPTT Users.....	34
Table 8: Others Services for MCPTT Users.....	34
Table 9: PTT Privacy Mode Behavior.....	50
Table 10: PTT Privacy Mode Alerts Behavior.....	51
Table 11: Call Behavior Summary with Scan Mode ON.....	53
Table 12: Cellular and Wi-Fi User Experience.....	58
Table 13: Supported Presence States.....	61
Table 14: Area-Based Warning Tones.....	67
Table 15: Supported Media Types - Captured or Recorded.....	69
Table 16: Supported Media Types - Gallery or Device.....	70
Table 17: Origination Permissions.....	73
Table 18: PTT User Incoming Video Session Behavior.....	76
Table 19: PTT User Outgoing Video Session Behavior.....	76
Table 20: Dispatcher Incoming Video Session Behavior.....	76
Table 21: PTT Standard and PTT Radio Feature Capabilities.....	88
Table 22: Call Permissions Types and Definitions.....	101
Table 23: User-Level Contact Sizes.....	104
Table 24: Corporate-Level Contact and Talkgroup Sizes.....	104
Table 25: Display Scenario.....	108
Table 26: LMR Interoperability by Feature Set.....	119
Table 27: PTT User Feature Availability by Feature Set.....	122
Table 28: Dispatcher Feature Availability by Feature Set.....	123
Table 29: User Type Provisioning Options.....	125
Table 30: User Type Provisioning Restrictions.....	126
Table 31: Summary of Provisioning Methods.....	127
Table 32: QPP Feature Set Mapping.....	136
Table 33: QCI Characteristics.....	137
Table 34: CSR Role Privileges.....	143
Table 35: Usage Detail Records.....	146
Table 36: ISM UDRs.....	147

Table 37: PTT Application Statistics and Logs..... 149
Table 38: PTT Application Usage Statistics..... 149

Chapter 1

Introduction

Broadband Push-to-Talk (PTT) is a key part of the Motorola Solutions suite of integrated communications applications, delivering voice, video, and data communications at the push of a button to get the right information to the right people at the right time in the moments that matter.

Broadband PTT provides a feature-rich PTT over Cellular (PoC) service built on Motorola Solutions' extensive push-to-talk experience.

A 3GPP standards-compliant solution, can be easily integrated with commercial wireless networks to increase profits, improve customer retention, and attract new customers.

Broadband PTT is built on a proven, highly scalable, and reliable all Internet Protocol (IP) Platform, that is designed to simplify network planning and growth. Multiple servers can be distributed across LTE, 5G, 4G-LTE, or Wi-Fi networks for broad geographic coverage and scalability to serve a large and expanding user base.

Broadband PTT is the ideal solution for mobile workforce communications, useful as a standalone PTT service, for 2-way radio augmentation (including P25, TETRA, DMR, and analog), and for PTT enablement of third-party productivity applications. The broad selection of compatible devices and accessories also makes a perfect fit for industries with mobile workforces.

Our device ecosystem leads the industry, providing our customers with the largest number of devices commercially available in the market across a diverse group of OEMs.

PTT functionalities are available as feature sets. You may add the Command feature set, which provides a set of features for enhancing safety, and the MCPTT feature set, which provides an advanced set of MCPTT features and capabilities. Subscribers can have either Collaboration, Command, or MCPTT features, based on their provisioned level of service.

Collaboration

The features included in each feature set are as follows:

- PTT Calling, Presence, IPA
- Broadcast Calling
- Messaging - Text, Image, Video file, PDF, Microsoft Office files, Location Sharing
- Voice Messaging
- Standard Talkgroups (up to 250 members)
- Priority Talkgroup Scanning
- Location Services
- Geo-fence for Supervisor and Dispatcher
- Quick Groups from Maps
- SRTP/SRTCP support
- AMR-WB or Opus Codec
- Single User Profile (PTT Radio only)

Command

Includes Collaboration Feature Set

- Emergency Calling and Alerting
- Ambient Listening
- Discreet Listening
- Large Talkgroups (up to 3,000 members, available upon request)
- Dynamic Area-Based Talkgroups
- Enable or Disable PTT Service
- User Check and Monitoring

MCPTT

Includes Collaboration and Command Feature Set

- Talkgroup Affiliation
- Talkgroup Profile
- MCX Talkgroups (up to 100,000 members; up to 3000 affiliated members at any given time)
- Remote Talkgroup Select
- Calls with External Telephony Users
- Manual Answer (Hook signaling) for 1:1 PTT
- Operational Status Messaging (OSM)
- Simultaneous PTT Audio Sessions for Dispatch
- Simultaneous PTT Video Sessions for Dispatch
- End-to-end encryption
- Userless Device Mode
- User Profiles
- Regroup Services

Broadband PTT solution supports the following:

- PTT Services – delivers instant voice communication to a group or an individual and supports the following:
 - Alerts – provides the convenience of a quick alert for requesting a callback or displaying a missed call.
 - Background Call Mode – allows the user to hear incoming PTT calls while the PTT application remains in the background.
 - Broadcast Calling – initiates a preemptive one-way call to a large group of users at the same time.
 - One Touch Calling (*selected devices only) – allows a PTT user to call a particular contact or talkgroup or most recent history entry when the PTT button is pressed or allows the PTT button to be assigned to open the application to the preferred landing page (History, Contacts, Groups, Favorite Contacts, Favorite Groups).
 - PTT History – provides the PTT call and message history.
 - PTT Voice Message Fallback – allows a PTT call to be converted into a voice message if the called party is unavailable.
 - Silent Mode Behavior (Privacy Mode) – provides alerting and barge behavior while the device is in silent mode, which can be controlled through the PTT Privacy Mode setting.
 - Supervisory Override (Talker Priority) – allows selected talkgroup members to take the floor and speak at any time during a call, even if someone else has the floor.

- Talkgroup Scanning with priority – allows a PTT user to select up to 16 talkgroups for monitoring, with three that can be set as prioritized groups.
- Wi-Fi Support – allows the PTT application to use Wi-Fi access points connected to the Internet.
- Audio Codec Support – PTT application supports various audio codecs such as AMR-BE, AMR-NB, AMR-WB, and OPUS. The system-level configuration allows default codec selection for PTT calls.
- Presence Services – provides real-time presence status for individual users.
- Location Services – provides location information and geo-fencing for dispatchers and PTT supervisors.
- Messaging Services – provides multimedia messaging to a group or an individual including Voice Message Fallback when the user is not available. Operational status messaging allows the fixed status code messaging to a group to indicate the current operational status of the user to dispatch or authorized supervisor.
- Emergency Services – provides emergency calling functionality as follows:
 - Emergency alert and cancellation
 - Receive Emergency calls - Private and Group
 - Emergency talker priority
 - Multiple users in a talkgroup can initiate an emergency call
 - Authorized users can obtain user information or control for a remote user as follows:
 - Remote emergency call start or cancel
 - Current Emergency status
 - User Location
 - User device Battery strength
 - User device Wi-Fi signal strength (when user is on Wi-Fi coverage; device dependent)
 - User device LTE signal strength when user is on cellular coverage; device dependent)
- Affiliation service - allows the MCPTT user to affiliate to a talkgroup to indicate the interest in receiving PTT, Messaging, and Video call communication on the talkgroup. It also allows the dispatch user to remotely monitor the current affiliation of the user as well as change the current affiliation of the user remotely.
- Regroup Service - allows the dispatch user to enable Push-to-talk, messaging and video across 2 or more predefined groups by regrouping them together into a temporary group.
- PTT Applications – support the following user types:
 - Standard PTT Application Mode – provides all the features and capabilities for those with little to no LMR experience and greater need for 1:1 PTT calling.
 - PTT Radio Application Mode – emulates the look and feel of an LMR radio, including support for up to 96 talkgroups across 12 available zones.
 - PTT Application Upgrade Notification – provides a facility to indicate that application upgrades are available and provides the ability to indicate that device support is ending so that older devices can be removed from the system.
 - Cross-Carrier – provides PTT service to a user on another carrier through the data plan and Internet data connection available on the device.
 - Dispatch – allows organizations to manage the day-to-day dispatch operations and rapidly respond to incidents, urgent situations, customer requests, facility events, and other situations that require quick actions.
- Centralized Contact and Group Management – provides the Central Admin Tool (CAT) which allows administrators to manage user profiles and the following:

- PTT Users – allows you to manage the PTT user profile such as name, email ID and permission type.
- Talkgroups – allows you to manage talkgroups including, assigning avatar, talkgroup scanning, supervisory override, talkgroup sharing, permission to the talkgroup members for call initiation, and receive and in call accessibility. There are three types of talkgroups that you can manage: standard, dispatch, and broadcast groups.
- User profiles – allows you to manage the PTT users with PTT Radio mode using the user profiles that consist of Talkgroups, User Sets and feature permissions.
- External Users – allows you to manage users external to the corporation.
- Integrated Users – allows you to manage the users of types, such as Integrated Mobile, Integrated Tracking, and Integrated Web.
- Interop Connections – allows you to manage the users between the Interop and PTT.
- User Sets – allows you to manage the user sets to PTT Users, Talkgroups, or Integrated Users.
- APIs – provides PTT enablement of partner applications:
 - Workforce management
 - Transportation and logistics
 - Healthcare
 - Manufacturing
 - Constructions
 - Public safety and public service
 - IoT/Smart city applications
- Land Mobile Radio (LMR) Voice Interop – provides interoperability with the following:
 - Legacy
 - P25 FDMA through ISSI – supports a secure and robust direct IP connection to LMR systems using the P25 standards-based interface.
 - Console Subsystem Interface (CSSI) – supports a secure and robust direct Internet Protocol (IP) connection to P25-compatible consoles.
 - Radio over IP (RoIP) with VPN and TLS – supports interoperability between the Broadband PTT and LMR radio.
 - Critical Connect
 - P25 FDMA and TDMA through ISSI (ASTRO® 25 and other vendor P25)
 - Site Link Interface for ASTRO® 25 and DIMETRA™
 - RoIP with TLS only
- Subscriber Life Cycle Management – provides access to the following:
 - Subscriber Types – supports Personal User, Administrator User, and Administrator and Personal User types of subscribers.
 - Subscriber States – supports the subscriber states (provisioned, activated, or suspended).
 - Subscriber Provisioning – supports a programmatic SOAP or REST interface for the provisioning system to provision users in the PoC system.
 - PTT Activation or Authentication – supports Cellular Network Activation or Authentication and Wi-Fi Network Activation or Authentication.
- Quality of Service (QoS) – provides access to Dynamic QoS, Priority, and Preemption using the Rx interface, which provides select users with prioritized access to LTE network resources when making a PTT call over an LTE network.

- Operations, Administration, Maintenance, and Provisioning (OAMP) – provides access to the following:
 - SOAP or REST – allows subscribers to be provisioned using a SOAP or REST interface. SOAP is supported for existing customers only. New customers are required to use REST.
 - Logging – provides device debug logs and application log retrieval. The remote log server can be configured to push stored usage and statistical data to a third-party mediation or analytical tool for processing.
 - Customer Service Support Web Portal (WCSR) – allows Customer Service Representatives (CSRs) to manage and view subscribers provisioned to solve customer issues.
 - Network Management – allows system administrators to perform configuration, network monitoring, and network performance data collection.
 - Billing – generates Usage Detail Records (UDRs) that the customer may use to charge their subscribers.
 - Reporting – provides Revenue Assurance Reconciliation (RAR) report information about each subscriber stored within the Motorola Solutions PTT platform.
- Regulatory Compliance – Lawful Intercept (LI)

Add-On Features (Added to Each Selected Feature Set)

- LMR Voice interoperability
- QoS, Priority, and Preemption
- Video Services

For more details on the tiered-feature sets, refer to [Subscriber Life-Cycle Management on page 120](#).

Supported Devices

The PTT application supports the following devices:

- Android OS current release to N-2 OS versions, including smartphones and tablets, and PTT-centric ruggedized devices
- iOS current release to N-2 OS versions, including smartphones and iPads
- Feature Phones, including PTT-centric ruggedized devices as per porting agreement



NOTE: The Broadband PTT applications are supported for the current release and previous two releases (N to N-2).

Supported Accessories

Supported accessories are as follows:

- Remote Speaker Microphone (RSM) including wired and Bluetooth
- Surveillance Kit with PTT Button
- Bluetooth Low Energy (BTLE) PTT Button
- Discreet Headset Microphone
- Bluetooth Microphone
- Bluetooth PTT button
- Intrinsically Safe Devices
- Car Kits
- Dispatch Accessories

1.1

Scope

This document provides a list of features and functionality available to users as part of the Broadband PTT solution. The document also provides details on how the customer can provision the service. Finally, it lists the capabilities and requirements to integrate the Broadband PTT in the customer network.

1.2

References

1. 3PP TS 24.379 Mission Critical Push To Talk (MCPTT) call control; Protocol specification.
2. OMA-TS-Presence_SIMPLE_RLS-V1 OMA Presence Simple Specification
3. RFC3261 SIP: Session Initiation Protocol
4. RFC3263 Session Initiation Protocol (SIP): Locating SIP Servers
5. RFC4566 SDP: Session Description Protocol
6. RFC7865 Session Initiation Protocol (SIP) Recording Metadata
7. TR 26.179 Mission Critical Push To Talk (MCPTT); Codecs and Media Handling
8. TR 24.980 Minimum Requirements for Support of Mission Critical Push To Talk (MCPTT) Service Over the GM Reference Point
9. TS 22.179 Mission Critical Push to Talk (MCPTT) over LTE; Stage 1
10. TS 22.280 Mission Critical Services Common Requirements
11. TS 22.281 Mission Critical Video over LTE
12. TS 22.282 Mission Critical Data over LTE
13. TS 23.280 Common Functional Architecture to Support Mission-Critical Services; Stage 2
14. TS 23.379 Functional Architecture and Information Flows to Support Mission Critical Push To Talk (MCPTT); Stage 2
15. TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP)
16. TS 24.281 Mission Critical Video (MCVideo) Signaling Control; Protocol Specification
17. TS 24.282 Mission Critical Data (MCData) Signaling Control; Protocol Specification
18. TS 24.379 Mission Critical Push To Talk (MCPTT) Call Control; Protocol Specification
19. TS 24.380 Mission Critical Push To Talk (MCPTT) Media Plane Control; Protocol Specification
20. TS 24.481 Mission Critical Services (MCS) Group Management; Protocol specification
21. TS 24.482 Mission Critical Services (MCS) Identity Management; Protocol Specification
22. TS 24.483 Mission Critical Services (MCS) Management Object (MO)
23. TS 24.484 Mission Critical Services (MCS) configuration management; Protocol specification
24. TS 24.581 Mission Critical Video (MCVideo) media plane control; Protocol specification
25. TS 24.582 Mission Critical Data (MCData) media plane control; Protocol specification
26. TS 29.214 Policy and Charging Control over Rx Reference Point
27. TS 33.179 Security of Mission Critical Push To Talk (MCPTT) over LTE
28. TS 33.180 Security of Mission Critical (MC) service over LTE

1.3

What's New in this Release?

Release 12.3 contains the following new content or features:

- Removed Windows 8 software support.
- Updated browser support. User can use Google Chrome, Microsoft Edge, or Mozilla Firefox.
- Added the support of ESRI map service.
- Updated the [PTT Services on page 25](#) section - Call Origination section to include updated tones and in-call tones.
- Updated the [PTT Services on page 25](#) section - PTT Call History section to include device regional date and time format support.
- Updated the [PTT Services on page 25](#) section - Call Tear down section to include support for Hang timer for Private and group PTT calls.
- Added the [PTT Services on page 25](#) section - First-to-Answer Private Calls section to include where first-to-answer private calls are originated from Dispatcher (authorized user) to two or more target users where the first target user accepts the call joins the call with the authorized user and other target users disconnect automatically.
- Updated the [PTT Services on page 25](#) section - Discreet Listening section to allow Authorized user to utilize discreet listening to listen to First to answer calls
- Updated the [PTT Services on page 25](#) section - Affiliation section - Service Affiliation section to include when a user deaffiliates.
- Updated the [PTT Services on page 25](#) section - Dynamic Area-Based Talkgroups - Talkgroup member experience - to include users do not automatically join to the call in progress when they enter the area. Users with affiliation feature, the ongoing call is dropped when they leave the area, however, users without affiliation feature do not leave the call, when they leave the area.
- Updated the [Location Services on page 64](#) section - Location Tracking/Geofencing (Optional) section to include Area-Based Warning Tones (Optional).
- Updated the [Messaging Services on page 69](#) section - Store-and-forward section to include that Store-and-forward is not applicable with Talkgroup Affiliation Services.
- Updated the [Video Services on page 74](#) section to include the Caveats section.
- Updated the [Video Services on page 74](#) section - Telephony Interaction section to update content.
- Updated the [Emergency Services on page 80](#) section - Emergency Cancellation section to include downgrading of an emergency call.
- Updated the [Emergency Services on page 80](#) section - More Frequent Location Updates During User Emergency section to include that iOS devices are not supported.
- Updated the [Broadband Regroup Service on page 85](#) section to include Regroup Service section
- Updated the [PTT Applications on page 87](#) section - Hook Signaling section to include that PTT Standard mode does not support hook signaling.
- Updated the [PTT Applications on page 87](#) section - Hook Signaling section to include Web Dispatch is now a supported PTT user type.
- Updated [Access Control on page 99](#). Added the **Multifactor Authentication (MFA), Password Management**, and updated **Password Requirements** sections.
- Updated the [Administration](#) section - Central Admin Tool (CAT) section - Talkgroups section - to include The administrator can create pre-configured groups to which no users are assigned using CAT, but users can dynamically add users to create groups thereby supporting the group-regroup functionality.

- Updated the [Administration](#) section - User Sets section - to include User Set also allows creation of a common contact list which is common to all profiles, each user can be assigned to a single common contact list.
- Updated the [Administration](#) section - User Profiles section to include Talkgroup and User Profile Sharing to include Prebuilt Trust Relationship Matrix.
- Updated the [Administration](#) section - User Profiles section to include Talkgroup and User Profile Sharing to include User Profile Sharing.
- Deleted [APIs on page 109](#) section - Affiliation Monitoring APIs section.
- Added [APIs on page 109](#) section - Converged Data APIs section.
- Changed [APIs on page 109](#) section - 3GPP Mission Critical (MC) Standard APIs.
- Updated [APIs on page 109](#) section - PTT Mobile APIs to remove Mobile Application Deep Linking APIs section.
- Updated [APIs on page 109](#) section - PTT Mobile APIs to remove Integrated Mobile APIs section.
- Updated [APIs on page 109](#) section - PTT Web APIs - Integrated Web APIs section to remove Calling APIs section.
- Updated [APIs on page 109](#) section - PTT Web APIs - Integrated Web APIs section to remove Call Recording APIs section.
- Updated [APIs on page 109](#) section - PTT Web APIs - Integrated Web APIs section to remove PTT Accessory Support APIs section.
- Updated [APIs on page 109](#) section - PTT Web APIs - Integrated Tracking APIs section to remove PTT Accessory Support APIs section.
- Updated [APIs on page 109](#) section - PTT Mobile APIs to include provisioning for Integrated Mobile APIs.
- Updated [APIs on page 109](#) section - PTT Mobile APIs to include PTT App-to-App and Accessory API.
- Updated [APIs on page 109](#) section - PTT Web Application APIs section - Integrated Web APIs section - Integrated Tracking APIs section - Life-Cycle Management for APIs section - to include Backward Compatibility for 3GPP APIs.
- Added the [Interoperability with Land Mobile Radio \(LMR\) Systems on page 118](#) section - Critical Connect Interoperability section - which provides interoperable communication between users on different ASTRO 25 networks, and between users on an ASTRO 25 network and those on Motorola Solutions' broadband PTT.
- Updated [Subscriber Life-Cycle Management on page 120](#) section - Subscriber Provisioning - Feature Sets and Add-On Features to include Regroup Service.
- Updated the [Branding and Language Support on page 134](#) section - Dispatch Application Branding section.
- Updated the [Branding and Language Support on page 134](#) section - Dispatch Application Branding to include multi-language support including Right-to-Left language.
- Updated the [Quality of Service \(QoS\), Priority and Preemption \(QPP\) on page 136](#) section - Rx Interface section content.
- Updated [Security on page 140](#) section - to include Database Encryption section.

MCPTT

Release 12.3 contains the following new content or features:

- Updated the [Introduction on page 16](#) section to include TS 33.180 Security of Mission Critical (MC) service over LTE reference.

- Updated the [PTT Services on page 25](#) section - 2-Way Calls to External Telephony Users section to include a note that full-duplex calls do not support Discreet Listening.
- Added the [PTT Services on page 25](#) section - to include MCX Talkgroups section.
- Updated the [Administration](#) section - Profiles section to include minimum and maximum supported profiles.
- Updated the [Administration](#) section to include Talkgroup Profile and Talkgroup Sharing sections.
- Updated the [Quality of Service \(QoS\), Priority and Preemption \(QPP\) on page 136](#) section - Network Requirements for Mission Critical PTT Deployments in the Quality of Service (QoS), Priority and Preemption (QPP) section.
- Added the [Broadband Regroup Service on page 85](#) Service section.
- Added [Simultaneous PTT Video Sessions on page 52](#) section to include the Dispatch section.
- Updated the [Discreet Listening on page 58](#) section to include support for first-to-answer private calls by a dispatcher.
- Updated user profile description. See the [User Profiles on page 104](#) section.
- Updated [Location Services on page 64](#) section - Location Tracking/Geofencing section.

Chapter 2

PTT Services

2.1

Call Origination

Our patented fast call setup provides a near-instantaneous communication to make the following types of calls:

- 1:1 call by selecting a contact from the contact list or manually entering the terminating MSISDN. Auto answer (Default).
- A prearranged group call by selecting a group from the group list
- A user-managed group call can be originated from a member's history list
- A Quick Group call by selecting up to 10 members from the contact list
- A Quick Group call by selecting up to 10 members on the map for supervisors with location capability enabled
- An area-based talkgroup call by adding or deleting members when they enter and leave a defined geographic area

To initiate the call, the originator presses the PTT button, waits for the floor acquired tone and starts talking.



NOTE:

On iOS, a call can be initiated only while the application is open (visible). You can initiate a call using a PTT accessory button and opening the application first. On Android, initiating a call with PTT key accessory does not bring the application to the foreground, unless the display is off.

The terminating PTT device(s) auto-answers the call with no user interaction required after which the talk hint tone is played, followed by the originator talking and a floor available tone when the originator has released the floor. After hearing the floor available tone, the terminating contact must press and hold the PTT button to talk. Five seconds before the maximum floor hold duration is reached, a floor revoke tone is played as a warning, and again when the floor is revoked. The maximum floor hold duration default is 180 seconds.

2.2

Tones

To initiate the call, the originator presses the PTT button, waits for the floor acquired tone and starts talking. The following table lists the name and describes each tone.

Table 1: Tones

Name	Description
Activation Tone	Played upon successful activation.
Alert (IPA/MCA) Tone	Played by the handset when an incoming Instant Personal Alert is received or a Missed Call has occurred. Four tones are required as this tone is user-selectable.
Attention Tone	Played to indicate a pop-up dialog message.
Area Warning Tone - Blast Tone	Played to indicate when you are within a blast area.

Name	Description
Area Warning Tone - Emergency Tone	For iOS, the app is suspended when put into the background and cannot play the periodic tone. Played to indicate to when the user to follow emergency procedures. This tone is played to escalate the priority from the blast notification to a mining emergency notification. For iOS, the app is suspended when put into the background and cannot play the periodic tone.
Area Warning Tone - Evacuation Tone	Played to indicate when you are notified to immediately evacuate the mining site for an impending blast. For iOS, the app is suspended when put into the background and cannot play the periodic tone.
Emergency Alert Tone	Played when emergency alert is received.
Emergency Alert - Originator Tone	Played when an emergency alert is initiated or declared.
Emergency Call Tone	Played upon receiving emergency call.
Emergency Cancel Tone	Played when an emergency is canceled.
Emergency Fail Tone	Played if emergency cannot be declared or if emergency call cannot originate.
Error (Floor Busy) Tone	Played to indicate the user cannot take the floor.
Floor Acquired (Grant) Tone	Played after the user presses the PTT button to indicate it is ready for talking.
Floor Free Tone	Played to listeners on a PTT call to indicate the talker has released the floor.
Floor Released Tone	Played to the user after releasing the PTT button to indicate the floor is released. (Default is OFF)
Floor Revoke Tone	Played five seconds before the floor is revoked. The same tone is also played when the actual floor is revoked.
Floor Unavailable (Bong) Tone	Played when a user tries to get a floor that is already acquired or the called party is unavailable. An appropriate visual indication is displayed for both scenarios.
Incoming Call (Talk Hint) Tone	Played to listeners to announce the start of a PTT call (first volley only).
Incoming Phone Call Tone	Played when there is an incoming 2-way phone call. Tone is repeated every 3 seconds.
Incoming Private PTT Call (Manual Answer) Tone	Played when there is an incoming PTT private call. Tone is repeated every 3 seconds.
Incoming Video Tone	Played when there is an incoming video alert waiting for user to accept. Alert is repeated every 5 seconds while alert is waiting for user action.
Network Loss Tone Repeat	The Network Loss Tone Repeat setting determines whether the phone plays the network loss tone continuously at a periodic interval or play once the user's PTT application detects network loss. When selected, a tone plays when the application transitions from one network to another.

Name	Description
Network Up/Network Down Tone	Network Up tone is played when server connection is restored. Network Down tone is played when server connection is lost (optional tone repeat). Previously known as Call Suspend tone.
One-Touch Action Selection Change Tone	Played when switching one-touch action from accessory with multi-function key button and multiple actions are supported.
Phone Call Progress Tone	Played to caller while waiting for telephony call to answer. Tone is repeated every 3 seconds.
Remote Ambient Start Tone	Played on target user's device when ambient listening is initiated remotely (optional tone).
Status Message Sent Tone	Played upon successfully sending status message.
Status Message Failure Tone	Played if status message is not sent successfully.
Success Tone	Played upon successful activation: valid key press.
Voice Message Recording Tone	Played when recording voice message (voice message fallback).

All participants get a visual indicator unique to the tone played on their PTT device.

The PTT application displays the following during an active call:

1. Caller name and number or Group name. In the case of a quick group call, the call is indicated as 'Quick Group' call on the PTT application display.
2. Talker name in real time
3. Call timer

The following table indicates the behavior and control of when in-call tones are played:

Table 2: In-Call Tones

Action	User A	User B
User A initiates call	Floor Grant*	Incoming*
User A releases floor	Floor Release* **	Floor Free*
User A takes floor	Floor Grant*	No Tone

*User-controlled via application setting.

** Default setting is OFF.

The following table shows the user call origination permissions.

Table 3: User Call Origination Permissions

Originating	Terminating		
	Personal	Administrator	Administrator and Personal
Personal User	✓	✗	✓
Administrator User	✗	✓*	✓*
Administrator and Personal User	✓	✓*	✓

* Within corporation or external subscribers

An administrator-managed user can receive calls from anybody within the corporation including external users.

A Private call is set up if the contact is in Available state. Likewise, a Group or Quick Group call is set up if at least one group member is in Available state.

A Broadcast call is set up if at least one group member is in Available state or DND state if the administrator configures DND override for the broadcast group.

An Emergency call is set up if the contact or at least one group member is in Available or DND state.

2.3

Call Teardown

The server tears down the call when all participants press the END key or if there is only one participant left on the call.

Alternatively, the call is torn down if the hang timer expires. The hang timer starts when the floor is available, and it is configurable system-wide for private and group PTT calls – default value is 30 seconds. Range: 5 seconds minimum and 60 seconds maximum. Call hang timer does not apply to first volley that originating user initiates. It only applies from the subsequent volley on the call.

2.4

Call Reception

When a call is received, the user hears a floor taken tone followed by the caller audio unless disabled by the application settings.

When Privacy Mode is set to Silent and phone's ringer is set to silent or vibrate-only, the audio is heard through the earpiece.

2.5

Call Interaction

A three-way call between an originated PoC call and a cellular voice call or another PoC call is not allowed.



NOTE: iOS devices do not support Call Priority.

Call Priority (Android Only)

With Call Priority, you can allow or reject another incoming call based on the Call Priority setting (Ongoing or Cellular). The default is .



NOTE: Call Priority is supported on Android 9 (Pie) and later using 9.0.3 PTT applications and later.

The following table describes the incoming call interaction for the downloadable and embedded PTT application.

Table 4: Incoming Call Interaction

Existing Call or Session	Incoming Call or Session		
	PTT Call	Cellular Call	Data Session
PTT Call	<p>Reject the call to the originator with reason “busy.” Show “missed call” notification to the user after PTT call ends. Ongoing PTT call may be preempted based on Priority Scan feature.</p>	<p>The user is presented with a dialog to either accept or reject the call as per built-in device behavior (not controlled by PTT application). If the user answers the cellular call, the PTT call is put in the background. PTT voice is lost during ringing, that is, normal device behavior for a cellular call while on a data session. When the cellular call ends, if the PTT call is still on, it comes to the foreground. The PTT call can also end silently in the background.</p> <p>For Android devices that support Call Priority</p> <p>When Call Priority setting is set to Ongoing, an ongoing PTT call continues, and an incoming cellular call is rejected without indication to the user (that is, no ringing).</p> <p>When Call Priority setting is set to Cellular, an incoming cellular call ends the PTT call.</p>	<p>Transparent to call. The user can do simultaneous PTT voice and data. Media applications may cause interactions, which are device-dependent</p>
Cellular Call	<p>Send disconnect with reason “busy” Show “missed call” notification to the user after the cellular call ends.</p> <p>For Android devices that support Call Priority</p> <p>When Call Priority setting is set to Ongoing or Cellular, an ongoing cellular call continues, and an incoming PTT call is rejected with user busy indication. A PTT missed call alert is provided to the user when the PTT call is rejected when accepted.</p>	<p>Outside the scope of this document</p>	<p>Outside the scope of this document</p>

Existing Call or Session	Incoming Call or Session		
	PTT Call	Cellular Call	Data Session
Data Session	Accept call and user can do simultaneous PTT voice and data. Media applications may cause interactions, which are device-dependent	Outside the scope of this document	Outside the scope of this document

The following table describes the outgoing call interaction.

Table 5: Outgoing Call Interaction

Existing Call or Session	Outgoing Call or Session		
	PTT Call	Cellular Call	Data Session
PTT Call	Not allowed	Puts PTT call in the background per normal device behavior. When the cellular call ends, if the PTT call is still on, it comes to the foreground. The PTT call can also end silently in the background.	Transparent to call. The user can do simultaneous PTT voice and data. Media applications may cause interactions, which are device-dependent .
Cellular Call	Not allowed	Outside the scope of this document.	Outside the scope of this document.
Data Session	Allow call and user can do simultaneous PTT voice and data. Media applications may cause interactions, which are device-dependent .	Outside the scope of this document.	Outside the scope of this document.

2.6

PTT Roaming Support

The PTT Roaming feature allows or disallows use of the PTT service based on the current network information reported by the application. For PTT roaming detection, MCC (Mobile Country Code) and MNC (Mobile Network Code) values are used.

During user provisioning, a user can be optionally assigned one or more roaming profile identifiers. Each roaming profile identifier specifies a list of MCC/MNC pairs that PTT service is allowed within. For a user to have PTT service, the user’s current MCC/MNC must match an entry in the user’s roaming profile. “Wildcard” values for MCC and or MNC are allowed within the roaming profile.

Each profile contains three separate lists corresponding to “Home,” “National Roaming” and “International Roaming” to aid in maintaining the roaming profiles.



NOTE: PTT Roaming is not supported in deployments with CDMA networks. Roaming profiles do not allow SID/NID values to be configured.

Roaming Detection

The PTT application reports changes in MCC or MNC to the server whenever they occur. Reporting of changes are subject to a configurable debounce timer to ensure that updates do not flood the network whenever rapid changes occur. The server checks the location information sent by the PTT application against a set of “allowed” networks, based on the user’s roaming profile. If the reported MCC/MNC is not allowed for that user, the registration request is denied, and a message is displayed to the user that PTT service is not available in their area.

A different method of roaming detection exists for Apple devices running iOS. These devices do not allow applications to access the current MCC/MNC of the connected network. Consequently, roaming detection is supported by determining the country in which the user is currently located using Location Services/GPS fixes at periodic intervals (configurable, default = 30 minutes). If the device determines that the current country is the same as the home country, the home MCC/MNC provided by the device is sent to the server. If the current country does not match the home country, the PTT application uses a built-in lookup table to determine the MCC associated with the current country and uses MNC value of 000 (since the actual MCC/MNC is not available). Note that the MCC reported by the PTT application may not reflect the actual MCC for the connected network when roaming into a country that has more than one MCC (for example, in the United States or India).

International Roaming

International roaming support offers per-user provisioning to control whether or not devices connected to other cellular networks are allowed to use PTT service. Android PTT applications report MCC/MNC changes to the server for validation of roaming. iOS PTT applications use GPS to determine the current country. If the current country is within the user’s home country, the home MCC/MNC is reported. If the current country is outside of the user’s home country, MCC is reported to the server based on a built-in lookup table and MNC=000. A single MCC is reported if a country has multiple MCC assignments (for example USA, India).



NOTE: The iOS client requires the user to give "Always Allow" location permission to support roaming detection and international roaming. Location permission and location services must be turned on before logging into the application.

2.7

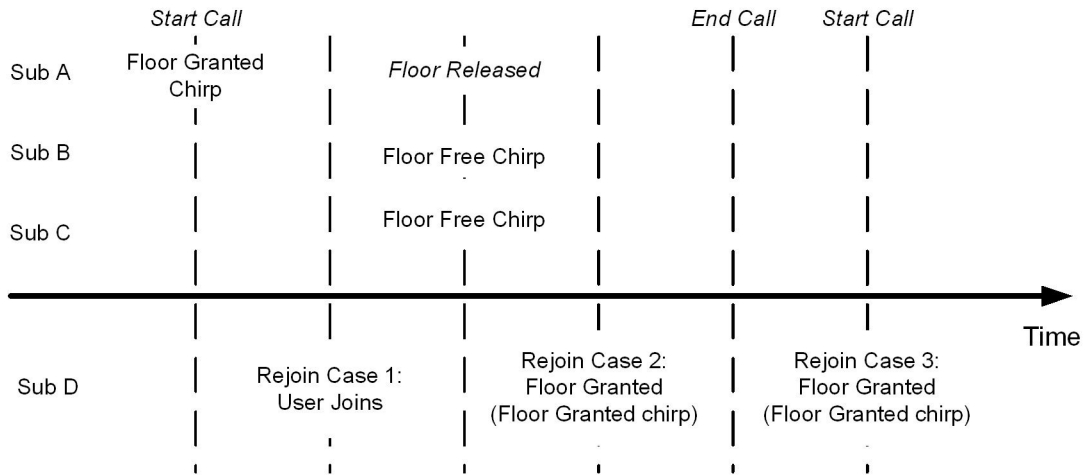
Call Rejoin

The Call Rejoin feature allows a user to rejoin an active prearranged group call. The originator rejoins an active call from history or the group’s list when they attempt to initiate a new call to the active group. If a call is not active, a new call is initiated to the group.

Since quick group calls show only the originator in history, making a call from history calls the originator.

Example- A, B, and C are on a prearranged group call where A originated the call. Shown are the three (3) possible points where D can join the call, and the chirp/tones played to D and others.

Figure 1: Call Rejoin Example



2.8

Alerts

Alerts provide a visual and or audio indication to notify the user of change in status or an attempt to contact the user.

2.8.1

Instant Personal Alerts

The Instant Personal Alert (IPA) feature allows a user to send an alert to an individual contact. This feature is useful to request another user to Push to Talk (PTT) you back. To send an IPA, the originating user must be in the Available state, and the receiving user's presence status must be "Available" or "Busy (DND)" (see note below). An IPA can only be sent to a single contact, that is, it cannot be sent to a group. When an IPA is received, it is displayed immediately. If the user is on a call, the IPA presentation may happen immediately, if supported by the device and OS.



NOTE: An IPA alert is visual and optionally audible and behaves in the same way as Missed Call Alerts (see the description in [Missed Call Alerts on page 32](#)).

The recipient of the IPA sees a notification on their PTT application and can call back using the IP notification.

2.8.2

Missed Call Alerts

Missed Call Alerts are seen in the following scenarios:

Missed Call Alerts (MCAs) are supported for PTT Radio user types for any missed private calls. MCAs on the selected group and the scanned group are not supported.

- 1:1 call on the recipient's device when the recipient never takes the floor during the call
- Scenarios with missed calls are shown in [Call Interaction on page 28](#).

Unless the user is on a cellular or PTT call, Missed Call Alerts appear immediately on the screen (visual alert) and can be set to provide an audible alert. Audible alerts can be once, repeated for a certain time, or until cleared by the user. The user can select the audible alert from a set of built-in tones. Note that both the MCA and IPA audible alert setting can be turned on/off independently, but the user-selected tone is used for both MCAs and IPAs. Visual alerts (pop-ups) from multiple callers are queued up on the screen as new alerts

occur before the previous ones are dismissed, but only one pop-up alert is displayed per caller. Even though only a single pop-up is displayed per caller, all missed calls can be found in the PTT history.

2.8.3

Geofence Alerts

The Geofence Alerts provide a dispatcher or PTT supervisor an indication (tone and visual) that talkgroup members have entered or left the defined Geofence boundary (when active).

The talkgroup member may also receive a notification when they cross the fence boundary from outside to inside. Notifications can be enabled/disabled by a dispatcher or supervisor.

Area-based Warning Tones

This feature allows an authorized web dispatcher to initiate a warning tone from a console which is broadcast to all field workers within a particular area. A use case for this feature is a mining company that needs to inform workers of a situation in which a blast will be happening, an emergency exists, or evacuation is necessary. For any given geofence, the dispatcher can select from three priorities of tones (high, medium, or low). The tones are system-wide configurable.

2.9

Affiliation

Affiliation is defined as a user or device registering interest for communication events (voice, video, data, location, etc.) on a given talkgroup and report its affiliation details. The Affiliation feature is included in the MCPTT feature set and is only applicable to PTT Radio mode users with MCPTT feature set. Affiliation does not apply to PTT Standard mode users. The following table shows feature interaction for MCPTT users with Affiliation feature.


 **NOTE:** Video call automatic late join is not supported for newly affiliating group members. Late join for talkgroups is supported by third-party dispatchers.

Table 6: Services on a Talkgroup for Collaboration/Command User with PTT Radio Mode

Event	PTT Call	Emergency Alert	Emergency Call	Messaging & OSM	Video Call
Selected Talkgroup	Calls received. MCA received if user is busy.	Emergency alert received.	Emergency call received.	All messages received.	Calls received. ¹ MCA received if user is busy.
Non Selected Scanning Talkgroup	Calls received on all scanned talkgroups based on priority. No MCA received if user is busy.	Emergency alert received.	Emergency call not received. ²	All messages received.	Calls received. ¹ MCA received if user is busy.
Other Talkgroups	Calls not received. No MCA received.	Emergency alert received.	Emergency call not received. ²	All messages received.	Calls received. ¹ MCA received if user is busy.

¹ Max affiliation limit of for video calls apply.

Event	PTT Call	Emergency Alert	Emergency Call	Messaging & OSM	Video Call
-------	----------	-----------------	----------------	-----------------	------------

² If Talkgroup steering is ON - the emergency call is received from any talkgroup.

Table 7: Services on Affiliated Talkgroup for MCPTT Users

Event	PTT Call	Emergency Alert	Emergency Call	Messaging & OSM	Video Call
Selected Talkgroup	Calls received. MCA received if user is busy.	Emergency alert received.	Emergency call received.	All messages received.	Calls received. ¹ MCA received if user is busy.
Non Selected Scanning Talkgroup	Calls received on all scanned talkgroups based on priority. ² No MCA received if user is busy.	Emergency alert received.	Emergency call received.	All messages received.	Calls received. MCA received if user is busy.
Other Talkgroups	Calls not received. No MCA received.	No Emergency alert received.	Emergency call not received.	No messages received.	No calls received. No MCA received.

¹ Max affiliation limit of for video calls apply

² With affiliation when talkgroup scanning is ON, scanning only applies to any new calls that are received on the scanned talkgroup. User does not auto late join to ongoing calls to scanned groups.

Table 8: Others Services for MCPTT Users


Event	User Behavior
Private/Quick Group PTT/Video Call/ Messages	Affiliation is not applicable to private or quick group calls/messages. All calls are received when user is idle. All private messages received.
Geofences and Area-based Warning Tones	Geofence configuration for talkgroups is only received when a user is affiliated on the talkgroup for which a geofence is configured. If a new user affiliates to a talkgroup that already has a geofence configured, the geofence configuration is automatically sent to the device.
Private Call Emergency	Affiliation is not applicable to private or quick group call. Emergency call preempts any other call except another emergency call.
Area-Based Dynamic Talkgroup	Calls or messages received when the user is inside a Geofence. MCA received when the user is busy. ABDG talkgroup acts as normal-priority scanned talkgroup; that is, calls are received depending upon the user is not busy in any other calls. ABDG talkgroup can be a selected talkgroup.


Event	User Behavior
Location	Location on a talkgroup is available to an authorized user based on supervisory privilege permission assigned by CAT. Location is reported to authorized users only from affiliated users to talkgroups.
Presence	Affiliation is not applicable to presence.

2.9.1

Service Affiliation

When the user or device affiliates to a talkgroup, all services are automatically affiliated (PTT Voice calling, Data services, and Video). When user deaffiliates to the talkgroup, all services are automatically deaffiliated and ongoing calls drops (including ongoing emergency calls). User talkgroup affiliation change is not allowed when user is in emergency state.

 **NOTE:** Broadcast talkgroups do not support affiliation queries.

 **NOTE:** Users without Affiliation feature continue to have existing feature interaction. There is no change in the interaction behavior for users when the Affiliation feature is disabled.

2.9.2

Notifications

Notifications (Integrated Secure Messaging, Emergency, OSM, MCA, Geofence alerts, etc.) are shown only for affiliated talkgroups and scanned talkgroups. Notifications are not shown for non-affiliated talkgroups.

Emergency call is received for the selected talkgroup while Emergency alert is received for the scanned talkgroup (scanning is enabled) and selected talkgroup. No emergency alerts and calls for non-affiliated talkgroups.

2.10

Affiliation Monitoring

Affiliated users are those MCPTT users who are logged in and registered interest for Communication Events on a given talkgroup (Corporate talkgroups and area-based talkgroups).

The Affiliation Monitoring feature allows a dispatcher to know which members are available (affiliated) on a talkgroup. The feature also allows the dispatcher to know which talkgroups a particular subscriber is affiliated to.

Affiliation monitoring is available for dispatch and third-party dispatchers with the MCPTT tiered-feature set. The third-party dispatch application uses the 3GPP MCPTT UNI interface to subscribe and receive affiliation monitoring reports. Dispatchers and third-party dispatchers can subscribe to a talkgroup and monitor membership affiliation.

Dispatchers receive a notification on any change in the affiliation of members to a monitored talkgroup. Additionally, dispatch user and the third-party dispatch interface also allows to monitor the MCPTT user's affiliated group and any changes to that by subscribing to MCPTT user's affiliation monitoring.

2.10.1

Affiliation Monitoring User Experience

The following apply when dispatchers successfully subscribe for real-time affiliation monitoring for a talkgroup:

- Receives an initial list of affiliated members.
- Receives notifications whenever there is a change in user affiliation for the talkgroup until the authorized user unsubscribes (by removing the group from monitored window) for affiliation monitoring on the talkgroup.
- Displays the affiliated member list dynamically.
- Remains subscribed for affiliation monitoring on the talkgroup until it unsubscribes. The subscription is persisted across the login cycle.

An authorized user can get a list of all affiliated talkgroups for a contact or user. When an authorized user requests affiliation monitor on a contact or user, the following information is available:

- Currently affiliated user talkgroup.
- For each of the contact, whether it is a selected.
- For each of the contacts whether it is in an emergency call.

2.10.2

Supported Talkgroups

The talkgroups available for subscription to affiliation monitoring are as follows:

- Corporate talkgroup
- Area-based talkgroup



NOTE: Broadcast talkgroups do not support affiliation queries.

2.10.3

Affiliated Talkgroup Member

An affiliated talkgroup member is defined as the following:

- A PTT Radio user or dispatcher who is provisioned with the MCPTT tiered-feature set.
- PTT Radio user who has selected a talkgroup when talkgroup scanning is disabled.
- PTT Radio user who has selected a talkgroup.
- Dispatcher who has monitored a talkgroup when simultaneous session is enabled.
- Priority assigned to talkgroups includes normal priority/no priority and priority with any number assigned to it.
- Any user who is part of the emergency destination is not an affiliated user until it falls into one of the above categories.
- Inactive area-based talkgroup members (dynamic members who are outside the area) are not affiliated members.

2.10.4

Configuration

The maximum number of talkgroups that can be monitored for affiliation is configurable: (0 to 100; default is 25).



NOTE: The number of monitored talkgroups for dispatch user is less than or equal to the configured number of affiliation monitoring talkgroups.

2.11

Remote Talkgroup Select

The Remote Talkgroup Select allows a dispatcher to change the selected talkgroup of any of its contacts (PTT Radio users who are provisioned with the MCPTT tiered-feature set). This functionality is also available for third-party dispatchers using an MCPTT UNI interface.



NOTE: When a dispatcher changes the user's currently selected talkgroup to any other talkgroup, this is not associated with the user's currently selected profile. The OSM capability is temporarily not available to the user in that talkgroup.

PTT Radio users are notified by a pop-up message when affiliation to talkgroups are changed.

When a user is temporarily unreachable, offline, or in an emergency state, a failure notification is sent to the dispatcher.

Upon changing the selected talkgroup of a PTT Radio user, the PTT Radio user starts receiving audio from the selected talkgroup if there is active communication on the talkgroup. If the PTT Radio user is in an active PTT call on any selected talkgroup, the PTT call ends for the user, and the user is forced to go to dispatch selected talkgroup.

The Remote Talkgroup Select feature is available in the MCPTT tiered-feature set.

For more information, see the "Dispatch Product Specification."

2.11.1

Supported User Types

Remote Talkgroup Affiliation as a authorized user supports the following user types:

- Third-Party Dispatch
- Web Dispatch



NOTE: Radio users without Affiliation feature are not supported for Remote Talkgroup Select by dispatch users.

2.12

MCX Talkgroups

MCX Talkgroups feature allows the CAT administrator to add up to members (configurable; default 100,000) to a talkgroup with Affiliation feature enabled.

A maximum of 3,000 members are allowed to be affiliated an MCX group at one time. Group video calls are restricted to first 15 affiliated members. Once the limit of affiliated users is reached, an error message is shown to the user attempting to affiliate. A dispatcher cannot use Remote Group Select to affiliate a new member to an MCX talkgroup that has reached its affiliation limit.

MCX Talkgroups is provided with the MCPTT tiered-feature set.

2.12.1

Configuration

The number of members with Affiliation feature enabled within an MCX talkgroup is configurable (default 100,000 with maximum up to 300,000).

CAT administrators and third-party dispatchers can create talkgroups of up to members. CAT does not allow any non-MCPTT users to be part of the MCX Talkgroups.

The system restricts a maximum 3,000 members affiliated to a talkgroup.

A user cannot affiliate if the affiliated member count for the talkgroup has exceeded the maximum limit. Otherwise, an error is received.

An authorized user cannot add a new member or affiliate a new member to the talkgroup if the affiliated member count for the talkgroup has exceeded the maximum limit.

An authorized user (dispatcher) can view the affiliated member count and the affiliated members in a talkgroup.

2.12.2

Talkgroup Member Details

Display of member, affiliated member, and count on users is as follows:

- A PTT application in Standard mode or PTT Radio mode and Dispatch user with a talkgroup size of fewer than 250 members shows the member list.
- A PTT application in Standard mode or PTT Radio mode and Dispatch user with a talkgroup size of more than 250 members shows the total number of members in the group however it does not show the complete member list.
- Dispatch with Affiliation feature shows affiliated member count and affiliated members for all monitored talkgroups for all group types.

Area-based talkgroup supports up to 250 members. Only active members with Affiliation feature are reported as affiliated if the area-based talkgroup is the selected talkgroup (monitored talkgroup with the simultaneous session when talkgroup scanning is disabled on dispatch).

Geofence on affiliated talkgroup tracks and shows notifications only for affiliated members.

2.13

Background Call Mode

Background Call Mode allows the user to hear incoming PTT calls while the PTT application remains in the background. If the backlight is off when the call is received, it remains OFF.

This feature is useful when the user wants to hear PTT calls but not be interrupted while using other applications. The user enables the Background Call Mode through the application settings, and the setting is OFF by default. Outgoing PTT call behavior does not change: calls can be initiated while the PTT application is in the foreground.

For iPhone, when Background Call Mode is OFF, received PTT calls turn on the display if it was off and show an incoming call notification. Tapping the call notification brings the application to the foreground. When Background Call Mode is ON, received calls are heard, and there is no incoming call notification. While the application is not shown on the screen (that is, in the background) and a PTT call is in progress, the phone displays a red call in progress banner. Touching the red banner opens the application to the call screen.

2.13.1

PTT Accessory Support

- Bluetooth PTT accessories (Bluetooth RSMs, Bluetooth Low Energy (BTLE) PTT buttons) allow the user to take the floor while the application is in the background.
- USB-C PTT accessories allow the user to take the floor while the application is in the background.

2.13.2

Dedicated PTT Button

Support for taking the floor while in the background varies by device vendor.

- Samsung “Active” devices allow the user to take the floor only while the application is in the foreground.
- Kyocera, Motorola Solutions LEX L11, and Sonim smartphones allow the user to take the floor while the application is in the foreground or background.
- iPhone allows the user to take the floor with a BTLE accessory button while the application is in the foreground or background. The initial floor request for an incoming call must be while the application is in the foreground. Beginning with iOS 12.4, a call can be originated only while the application is in the foreground.

2.14

Broadcast Calling and Messaging



NOTE: Broadcast Calling provides the ability for a dispatcher or designated PTT user (called the broadcaster) to send a one-way secure text message or make a one-way, high-priority call to a group of up to 500 members. Since broadcast messages are one-way, broadcast group members cannot reply or send secure text messages to the group. Multimedia or location messages are not allowed to broadcast groups.

Broadcast Calling and messaging consists of two modes of call delivery as follows:

- Batch delivery of Broadcast calls
- Instant delivery of Broadcast calls


Batch Delivery

Calls are delivered in a manner called "call batching" that increases the likelihood that a large number of collocated users can receive the call. Incoming broadcast calls have a tone preamble and preempt ongoing calls, including priority scan list calls. Other broadcast calls do not preempt broadcast calls.

Call batching increases the likelihood of broadcast call delivery. Each batch is delivered in the same manner as a group call; if a user joins late (for example, due to the extra time required for preemption of another PTT call), they hear the broadcast call in progress. At the beginning of the broadcast call, all the group members are segregated into call batches based on a subset of members (up to 250), if the system is so configured. Users attempted in the first batch receive the call near real time, just as any other group call. The call audio is stored locally on the server long enough for delivery to the remaining call batches.

The batch size is configured system-wide. A failed attempt to reach a broadcast talkgroup member due to the user being busy (active talker on a call, or cellular call, or incoming emergency call) or having a temporarily unreachable condition causes the call to be retried once after all other batches are attempted. When a user is in an emergency state, the user is excluded from broadcast call delivery. There is a configuration to limit the total length of time for overall broadcast call delivery (Time to live) from the beginning of the first batch it has started. The value configured by default is 300 seconds. There is only one broadcast call and delivery supported on the same group at a time. Any broadcast call initiation to a broadcast group fails while an active call delivery is ongoing on that group.

Broadcast groups are created and administered by the Administrator through the CAT. Each group can be configured to override the Do Not Disturb (DND) availability state set by the user for important calls.

 **NOTE:** Receiving broadcast calls with DND override is supported by release 7.10 and later PTT applications only. PTT Applications before release 7.10 do not receive broadcast calls while in DND state.

Instant Delivery

Broadcast calls with Instant delivery mode are delivered in near-real time as opposed to batched delivery. User experience for instant delivery is similar to batched delivery except that broadcast message is delivered to all the member of the broadcast group as and when the broadcast call occurs. There is no further retry to deliver the broadcast call to users to which the broadcast call delivery failed at first attempt.

Feature Configuration

The default configuration for the feature is set at the system level, and some settings can be further adjusted on a per-corporation basis. Corporate-level configuration is done on an exception basis.

System-Wide

- Feature enable
- Default time-to-live period for call delivery (default = 5 minutes)
- Maximum call length (default = 3 minutes)
- Maximum number of members per group (default = 500)
- Delay (guard) time between batches (default = 15 seconds)
- Batch size (default is 250) 500 maximum

Corporate-Wide

- Time-to-live
- Maximum call length
- Maximum number of members per groups


Feature Applicability

All PTT applications can receive broadcast calls.

2.15

Device ID Management

Device ID management allows multiple PTT users to share a device certified for PTT with other PTT users, for example, between shift workers.

 **NOTE:** The Device ID Management supports 9.1 PTT applications and later. It is required for cross-carrier users and tablet users.

Other than shift users, Device ID management can also be used to log into multiple devices a user may possess. For example, a tablet and phone owned by the same user. However, the PTT user can have only one active session at any point in time. Once logged in to one device, a session from another previously logged in device is deactivated.

The PTT user can have either System-Generated ID or Email ID as User ID. However, if the PTT user has a dedicated phone number and the PTT user wants to use the phone number as a PTT identity, the user's phone number can replace the System-Generated ID.

2.15.1

Provisioning

There is a new type of provisioning method called "User."

"User" types of devices can be provisioned using License Packs or one at a time.

All existing provisioned "Wi-Fi" and "Cross Carrier" user types automatically convert to "User" type.

There is no change to the following:

- End users provisioned as "Handset" user type
- Web Dispatch console provisioning, user ID creation, and activation
- Integrated and Interop types of user provisioning and activation

2.15.2

PTT User Type "User"

For subscribers with PTT type of "User," there are two options for the assignment of the User ID, depending on whether the device is a shared device or assigned to a particular user.

- Any Device- the user can log in from any device using a system-generated ID or email ID.
- Own Device with Phone Number- a user's phone number can be used as their User ID instead of System-Generated ID. Note that this option does not restrict the user from logging into other devices using the User ID. In other words, the user can log in to any device with or without a SIM (except the ones activated as handset client).

2.15.3

User ID

The administrator assigns the User ID, which can be any of the following:

- System-Generated ID - up to 15 digits (For backward compatibility it may be set to less than 14 digits). System generates this ID when user is provisioned.
- Phone Number (CAT assigned)
- Email ID (CAT assigned) is optional

The administrator can search CAT by System-Generated ID (or Phone Number) and Email ID.

2.15.4

User Registration

The PTT user is registered as follows:

- System-Generated ID is assigned to each user as the User ID. Additionally, the administrator enters the Phone Number and or Email ID as a User ID.
- The system generates a temporary password and is visible to the administrator. The password length is configurable system-wide—6-15 digits numeric or special characters.
- Temporary password can be communicated to the end user by one of the following methods:
 - By email with instructions, if email is provided
 - By SMS sent to the phone number, if phone number is provided

- If the user does not have an email ID or phone number, where the instructions and temporary password can be sent, the administrator can verbally communicate the User ID and temporary password to the user.
- The PTT user is prompted to change the password upon the first login when using the temporary password.
- PTT system hosting Handset users and User license users - Password for User type does not expire.
- PTT system hosting only User license users - Password expires at 90 days (default; configurable to 365 days maximum)

2.15.5

Password Management

Password management allows you to change or reset the password of your application account.



NOTE: These system-wide settings may change based on your service provider configuration.

The system default configuration is set as follows:

1. Password expires every 90 days.
2. Password history cannot be the same as any of the last five passwords used.
3. Password cannot be same as your username.

2.15.6

Password Security

The password is secured and encrypted at rest and in transit by default. Multifactor authentication is available for Dispatch and CAT base on service provider configuration



NOTE: Multifactor authentication (MFA) is available for CAT and Dispatch based on system-level configuration.



NOTE: Password strength settings depend on the type of access account (handset, WDS, CAT). The handset complexity may differ from other access account types. The handset is six characters minimum

- The following password rules apply when a new password is created:
 - Password can have:
 - At least six characters (Password length is configurable system-wide)
 - Lowercase letter (a-z)
 - Uppercase letter (A-Z)
 - Number (0-9)
 - Special characters @#\$\$%^&+=

2.15.7

Administrator Functionality

The administrator performs the following tasks:

- Views and manages the “User” licenses
- Changes the type of application mode: Standard or PTT Radio.
- ID management
 - Sends or resends the instructions.

- Changes the User ID.
 - Changes phone number to CAT-generated ID and vice versa.
 - Add or changes the Email ID.
 - Changes User ID which updates all the contacts and talkgroups that the User ID is assigned.



NOTE: Email ID entered by the administrator is different than the provisioned email ID. The provisioned email address is not used in CAT.

2.15.8

First Time Login

The administrator assigns the PTT user a User ID (email ID or a phone number) and password (temporary).

Handset Users

The first-time login process for handset users is as follows:

- When the user starts the PTT application, the PTT application attempts to send SMS/HTTPS for device identification. If SMS verification fails, the PTT application attempts again up to three times. If the SMS verification fails, the PTT application allows the user to log in using User ID/Password prompt.



NOTE: Tablet devices do not send SMS.

User License Users

The PTT users can be use user license type with either for private use (fixed device for a user) or device sharing use (across multiple users, for example, common devices used across multiple shift users).

Private Mode

The first-time login process for private mode users is as follows:

- When the user starts the PTT application, the PTT application attempts to send SMS/HTTPS for device identification. If SMS verification fails, the PTT application attempts again up to three times. If the SMS verification fails, the PTT application shows the User ID/Password prompt.
- The user enters a User ID and a temporary password.
- The user enters a new password and selects "Remember Password."
- Choose Yes to member your username and password. The PTT user is prompted to re-enter their User ID and Password so it can be stored in the device. The User ID and Password are encrypted. The user is logged into the PTT service.
- All subsequent application starts automatically login with the stored User ID and Password. The PTT user can exit private mode by using the "Switch User" option. In this case, the saved User ID and Password are cleared from the device.

Shared Mode

The first-time login process for shared mode users is as follows:

- When the user starts the PTT application, the PTT application attempts to send SMS/HTTPS for device identification. If SMS verification fails, the PTT application attempts again up to three times. If the SMS verification fails, the PTT application shows the User ID/Password prompt.
- The user enters a User ID and a temporary password.
- The user enters a new password and the user is logged into the PTT service.

2.15.9

Caveats

Device ID management caves are as follows:

- PTT application displays the phone number or system ID in contact details and not Email ID.
- User can search or add contacts using system ID or phone number only within the PTT application.

2.16

First-to-Answer Private Calls

First-to-answer private calls are originated from Dispatcher (authorized user) to two or more target users where the first target user to accept the call joins the call with the authorized user and other target users disconnect automatically.

Only manual PTT call answer mode is supported for first-to-answer calls.

A first-to-answer private call can be originated to up to 10 (default 5) users.



NOTE: First-to-answer private calls require 10.0 and higher applications with PTT radio mode.



NOTE: Calls to 9.1.1 and lower PTT applications and standard mode users disconnect automatically.

User experience

The first-to-answer private calls user experience is as follows:

- All target user devices ring simultaneously.
- The first user who accepts the incoming private call joins the call with the dispatcher.
- Other target users are disconnected automatically and no missed call alerts are indicated; the PTT call history is updated.
- The target user is not aware of incoming call type, that is, 1-1 private or first-to-answer private call.

2.17

One Touch Calling

When One Touch Calling is enabled, PTT users can call a predetermined contact or talkgroup or most recent history entry when the PTT button is pressed once, or assign the PTT button to open the application to the preferred landing page (History, Contacts, Groups, Favorite Contacts, and Favorite Groups). One Touch Calling provides a simplified calling experience for PTT users who primarily communicate with a single contact or talkgroup.

When using the PTT Radio Mode, One Touch Calling applies to the selected talkgroup and the landing page options are not applicable.

One Touch Calling applies to devices that support Motorola Solutions Broadband PTT applications capable of DRX.

2.17.1

Server-Based DRX Optimization

Overview

- User Experience

- One Touch feature delivers a similar user experience with fast call setup using DRX settings
- Discontinuous reception (DRX) has been adopted in the Long Term Evolution (LTE) system as a core technology to prolong the battery life of the user equipment (UE).
- Patented PTT application-specific adaptive DRX algorithm is used to determine a predictive time slot for UE to apply a configurable DRX value when the probability of receiving calls for a specific subscriber is high.
- Advantages:
 - DRX helps with faster call setup for One-touch calling
 - Adaptive DRX algorithm assists in battery life improvement over statically applied short DRX for a longer duration
- Algorithm is applied on a per subscriber basis.

Algorithm Details

- Device applies the default DRX if no configuration is received from the server.
- Calls received outside of the faster DRX slot; the client will be able to set the short DRX for the current running time slot so that subsequent calls within the time slot can achieve a faster call setup.
- Device applies the default DRX algorithm under following conditions:
 - Outside of indicated time slots
 - Connects to Wi-Fi network
 - Out of coverage of LTE network (No networks)
 - Subscriber logs out
 - Subscriber sets DND
 - If the battery runs into low battery event

2.18

Operational Status Messaging (OSM)

PTT Radio users can use predefined Operational Status Messages (OSMs) to communicate to authorized dispatchers or authorized PTT Radio supervisors in a selected talkgroup. OSMs are displayed in the PTT call history.

OSM consist of short and long message descriptions. The OSM setting in the PTT application determines if short, long, or both message formats are displayed.

OSM supports UTF-8 encoding for all supported languages.

OSM can be sent as follows:

- From programmable hard key on the device (if supported and configured) during the following:
 - During a PTT call
 - While composing an integrated secure message
 - While the application is in the background
- Sent to a selected talkgroup

Received OSMs display the following information:

- Sender name and talkgroup name
- Time message was originated (UTC)
- Short description

- Long description
- Additional notes (if any; form message)

Incoming messages are logged in to talkgroup history

No reply or user acknowledgment is allowed

OSM supports Android PTT Radio and iOS PTT Radio including Motorola Solutions LEX L11 device. OSM is configured at the system-level. OSM is included in the MCPTT tiered-feature set.



NOTE:

Authorized dispatch PTT users cannot send OSMs. Authorized PTT Radio supervisors can send and receive OSMs.

OSM does not support broadcast talkgroups, location-based dynamic talkgroups, or quick group talkgroups.

PTT Standard Mode does not support use of OSMs.

2.18.1

CAT Administration

The corporate configuration in CAT is used to configure the OSMs.

The CAT administrator creates a default OSM list for the corporation which applies to new talkgroups when enabled.

Multiple lists per corporations are supported and each talkgroup can have a unique list.

A search function is available to search for a list.

Changes to the list are pushed to users in near real time.

Bulk file (CSV) import supported for a list (one list at a time).

CAT corporate configuration supports:

- 100 OSMs per list. Default is 25 system-wide
- Up to 100 lists per organization
- A unique list name in the corporation -100 characters maximum
- A code up to 5 digits (Max 65535)



NOTE: OSM codes are unique within a list, can exist across multiple lists, and multiple codes can be within a list.

- A short message- 1-15 alphanumeric characters (10 default) including special characters
- A long message 1-300 alphanumeric characters (100 default)
- Allow to append message- Yes/No (No default)
Append messages can contain up to 15 characters (10 default) and is configured system-wide.

2.18.2

Caveats

The OSM caveats are as follows:

- No special characters such as (=, ', ", /, -, +, @) are allowed in the Excel file used for importing. Commas (,) and pipe (|) characters must not be used at the beginning of any name.
- Authorized dispatchers can only receive OSMs.
- Broadcast talkgroups, location-based dynamic talkgroups, or quick group talkgroups are not supported.

- PTT Standard Mode is not supported.
- Status codes are not visible to the end user; only the description is shown.
- Messages are delivered in real-time (uses default bearer- not a guaranteed delivery)
- No delivery or read receipt.
- If message recipients are not online, logged in, or available, an error tone is provided to the user.
- There is no default list of status codes available for a corporation.
- OSM messages can only be sent by PTT Radio users on a selected talkgroup. While user is using any other PTT functionality, OSM message can not be send from within the PTT application.

2.18.3

Dispatch

The dispatchers receive the following:

- A list of status codes and description at user login
- Any updates to OSMs configuration by CAT administrator (codes and description) is available to dispatch application in real time
- Dispatch authorized users receive the status code if the dispatcher is part of the user selected talkgroup
- Timestamp when the message was originated (UTC)
- User location when the message was originated (User's last known location)



NOTE: No reply or user acknowledgment is allowed for dispatchers.

2.18.4

Third-Party Dispatch

The third-party dispatch application uses the 3GPP MCPTT UNI interface to receive status codes. The third-party dispatchers OSM recipients receive the following:

- A list of status codes and description at user login using configuration management interface (subject to standards definition)
- Updates to CAT configuration may not be available to third-party dispatch application in real time
- Status codes via MCPTT UNI interface
- Timestamps (UTC) when the message was originated
- User location when the message was originated



NOTE: A no reply or user acknowledgment is allowed.

2.18.5

Motorola Solutions LEX L11

Motorola Solutions LEX L11 supports programmable keys to which status messages can be assigned:

Up to four programmable keys as follows:

- Short press- Key1
- Long press- Key1
- Short press- Key2

- Long press- Key2

By default, keys are mapped to the first four messages in the operational status message list for a talkgroup.

Status can be sent while the application is in foreground or background or while the device is locked.

An error tone is played when the key is not mapped, and the user presses the key.

2.19

Dynamic Area-Based Talkgroups

Dynamic area-based talkgroups are groups whose members are automatically assigned or removed as they enter or leave a defined geographic area. This type of group is useful when there is a set of users who need to communicate while at a certain location, such as an incident. The talkgroups are created and maintained by a dispatcher. The dispatcher assigns candidate members to the group. In addition to the candidate members who are active while in the area, the dispatcher can add members who are always active, regardless of their location. As members enter a geographic area, the talkgroup is shared. When leaving the area, the user is removed from the talkgroup. Members receive notifications upon entering and exiting the talkgroup. While the talkgroup is active, members are allowed PTT call origination and messaging within the talkgroup.

Dynamic area-based talkgroups can be assigned as monitored groups on the dispatch console. A maximum of 250 members is allowed for each talkgroup. The maximum number of area-based dynamic talkgroups allowed per group owner (dispatcher) is 50 (default=10) the maximum number of talkgroups allowed per group member is 100 (default = 100).



NOTE: The talkgroup count assigned to the user excludes the dynamic area-based talkgroups.

This feature is enabled at the system-level. The maximum number of area-based talkgroups are in addition to the maximum number of provisioned talkgroups for the device. See area-based talkgroups in [Table 21: PTT Standard and PTT Radio Feature Capabilities on page 88](#).



NOTE:

Area-based talkgroup feature is applicable only for release 9.0 clients (dispatcher and PTT application).

At least one member must be a dynamic member to create an Area-based talkgroup.

Talkgroup members without the Command feature set are not allowed in the talkgroups.

Talkgroup Member Experience

- As members enter the area, the talkgroup is shared and shown at the top of the channel list of the PTT Radio client and the top of the talkgroup list for the Standard client.
- Members receive notifications upon entry and exit of the defined geographic area.
- Users do not automatically join to the call in progress when they enter the area.
- For users with the affiliation feature, the ongoing call is dropped when they leave the area. However, users without the affiliation feature do not leave the call when they leave the area.
- Area-based talkgroup members do not see a member list.
- Area-based talkgroups allow PTT call origination and messaging to active and static members.

Dispatcher Experience

- Dispatcher (Owner) creates and manages the area-based talkgroups.
- Dispatcher (Owner) can view who has an active membership for dynamic members.

For more information, see the "[Dispatch Product Specification](#)."

2.20

2-Way Calls to External Telephony Users

The 2-way Calls to External Telephony Users features are as follows:

- PTT system supports private (1-1) 2-way calls between broadband PTT users and external telephony users. Private call is full-duplex call with manual call answer (confirmed call). Additionally, Private (1-1) full duplex 2-way calls are also supported across broadband users when this feature is enabled.



NOTE: Full-duplex calls do not support Discreet Listening.

- Integration with external SIP gateway is required to enable the telephony calls.
- System can prepend a pre-configured routing code (2-4 digits) for external telephony calls to (routing digits configurable per corporate) external SIP gateway. This pre-configured code can be programmed into external SIP gateway to route the calls appropriately into private PBX connected to the external SIP gateway.
- In-band DTMF is supported for IVR menu selection.
- The call interaction for full duplex 2-way calls with other PTT calls, Emergency calls and Broadcast calls is similar to LTE call interaction. Incoming emergency calls and broadcast calls do not preempt ongoing full duplex 2-way calls.
- PTT Voice message fallback is not supported for 2-way calls.

2.20.1

2-Way Calls to External Telephony Users Experience

The user experience for 2-Way Calls to External Telephony Users or other broadband users is similar to LTE calls and is as follows:

- The user initiates a private call using manual dial - SIP DID.
- The user can save the external telephony contact locally in PTT address book.
- The user can also initiates a private call using private contact.
- Ongoing 2-way full duplex calls are not allowed to be mute from the PTT application.
- Incoming 2-way calls are not allowed to be answered via external PTT button. However, incoming call can be answered while user device is in locked state or PTT application is in background or PTT application is in foreground.



NOTE: Other telephony features such as call hold, call wait are not supported.

2.21

PTT Call History

The PTT Call History lists the following events:

- Incoming PTT calls (both individual and group)
- Outgoing PTT calls (both individual and group)
- Missed PTT calls – based on PTT call and cellular call interaction as described in [Call Interaction on page 28](#)
- Incoming emergency call
- Outgoing emergency call

- Emergency alert and cancel events sent and received
- Incoming Instant Personal Alerts
- Outgoing Instant Personal Alerts
- Incoming Multimedia Messages (Text, Video, Audio, Files)
- Outgoing Multimedia Messages (Text, Video, Audio, Files)
- Incoming Video calls
- Outgoing Video calls
- Operational status message sent
- Operational status message received (applicable to OSM supervisors only)

The history is a rolling history with the maximum size based on device memory availability. The history maintains the date and time of the event. The date and time format follow the device setting to provide the user with a familiar format for their region. The history is maintained by the Broadband PTT application and is affected if the device is changed or reactivated. Multimedia messages stored on the server at the time of reactivation are restored, and all other history such as alerts and call entries are lost. All history content can be cleared in the PTT application from the top-level, and PTT calls can be originated from the history.

2.22

PTT Voice Message Fallback

PTT Voice Message Fallback allows a PTT call to be converted into a voice message if the called party is not available (for example, DND, offline, busy, TU).

The minimum length of a valid Voice Message Fallback recording is configurable system-wide (1–15 seconds, default = 3 seconds). Therefore, when a Voice Message Fallback occurs, and the user recording is less than the default (3 seconds), the voice message is discarded.

The PTT Voice Message Fallback is configured system-wide by Operations.

2.23

Silent Mode Behavior (Privacy Mode)

The Broadband PTT application alerting and barge behavior while the device ringer is in silent mode can be controlled through the PTT Privacy Mode setting. The PTT application activates Privacy Mode when the user sets the phone ringer to silent or vibrate only. The following table describes the behavior of the alerts and PTT calls when Privacy Mode is active.



NOTE: Privacy Mode setting is applied only when built-in device ringer mode is set to Vibrate or Silent.

Table 9: PTT Privacy Mode Behavior

PTT Privacy Mode Setting	Built-in Ringer Setting		
	Normal (not silent or vibrate only)	Vibrate Only	Silent Only
OFF	PTT call volume: Normal PTT call audio route: Incoming call alert: Normal	PTT call volume: Normal PTT call audio route: Speakerphone/Earpiece (based on user setting)	PTT call volume: Normal PTT call audio route: Speakerphone/Earpiece (based on user setting)

PTT Privacy Mode Setting	Built-in Ringer Setting		
	Normal (not silent or vibrate only)	Vibrate Only	Silent Only
		Incoming call alert: Normal	Incoming call alert: Normal
Use Earpiece	PTT call volume: Normal PTT call audio route: Speakerphone/Earpiece (depending on user setting) Incoming call alert: Normal	PTT call volume: Normal PTT call audio route: Earpiece Incoming call alert: Vibrate	PTT call volume: Normal PTT call audio route: Earpiece Incoming call alert: Silent

In call tones, for example, Floor available, Floor granted, and others, follow the PTT call volume as specified in the table above. The PTT call behavior, as described above is affected by each incoming PTT call even if the user changes the call volume or audio routing (earpiece/speakerphone) during a PTT call.

The behavior of alerts (Instant Personal Alerts and Missed Call Alerts), while Privacy Mode is active, are based on the following table.

Table 10: PTT Privacy Mode Alerts Behavior

PTT Notifications Setting	Built-in Ringer Setting		
	Normal (not silent nor vibrate only)	Vibrate Only	Silent Only
Audible Alert ON, Vibrate Alert ON	Audible, Vibrate	Silent, Vibrate	Silent, No Vibrate
Audible Alert ON, Vibrate Alert OFF	Audible, No Vibrate	Silent, Vibrate	Silent, No Vibrate
Audible Alert OFF, Vibrate Alert ON	Silent, Vibrate	Silent, Vibrate	Silent, No Vibrate
Audible Alert OFF, Vibrate Alert OFF	Silent, No Vibrate	Silent, Vibrate	Silent, No Vibrate

2.24

Simultaneous PTT Audio Sessions

The Simultaneous PTT Audio Sessions feature allows a dispatcher to simultaneously monitor up to 20 talkgroups. It is available on the Dispatch application and available using a Mission Critical UNI interface (up to 25 for third-party interface). A separate audio stream is provided for each monitored talkgroup with independent transmit and receive permissions. The Dispatch user can independently select each monitored group to be mute/unmute to route the audio from the monitored group to the speaker. Dispatch can also select multiple groups to transmit on multiple groups simultaneously. Multiple group selection supports

transmit audio only, the incoming audio from multiple selected groups is not re-transmitted to the other groups.

Additionally, up to five additional dynamic sessions are available to allow for incoming and outgoing private, quick group calls. Broadcast calls are not assigned to be monitored. Dynamic sessions are not applicable to dispatcher using third-party MC UNI interface.

Dynamic sessions can not be monitored, and missed calls are sent if all dynamic sessions are busy. Call in progress indication, along with talker identification, is provided for each simultaneous session.



NOTE: Simultaneous PTT audio session is not applicable to handset PTT users (Standard and PTT Radio mode).

The Simultaneous PTT Audio Sessions feature is included in the MCPTT tiered-feature set.

For more information, see the "Dispatch Product Specification."

2.25

Simultaneous PTT Video Sessions

The Simultaneous PTT Video Sessions feature allows a dispatcher using the Dispatch application to view up to 5 live stream videos simultaneously. Each live stream video session is shown in the video pane. One live stream at a time can be enlarged while the other videos are shown as smaller thumbnails. Audio from each live stream can be assigned to a speaker and muted/un-muted independently.

The Simultaneous PTT Video Sessions feature is available in the MCPTT tiered-feature set. The video add-on is required on the dispatch subscriber to enable the live stream video feature.

The maximum number of simultaneous video sessions allowed is system-wide configurable 1-5, default 5.

The Simultaneous PTT Video Sessions feature is also available using a Mission Critical UNI interface. For more information, see the Control Room Interface Reference Document (ITRD).

For more information about this feature, see the "Dispatch Product Specification."

2.26

Supervisory Override (Talker Priority)

The Supervisory Override (Talker Priority) feature allows one or more members of a group to act as a supervisor and preempt any talker during a group call including other supervisors.

Multiple supervisors in the same group can preempt each other during a prearranged group call. Some of the types of users such as external, Interop users cannot be selected as a supervisor. A supervisor sees an icon next to the group name in their group list for which they have talker priority. Supervisors are identified by an icon next to their name in the group member list. Further, each supervisor is identified during a call by an icon while speaking. PTT users in emergency have higher talker priority than Supervisors. The dispatcher user highest priority over other supervisors and users in emergency

2.27

Talkgroup Scanning

The Talkgroup Scanning feature allows a user to monitor and communicate with a subset of the administrator-managed talkgroups to which they belong. Whenever a call is active on a talkgroup within the scan list, the application automatically joins that call and allows the user to take the floor, if desired. When the current call ends, the user joins the next active call from the scan list. While Talkgroup Scanning is turned on, calls from talkgroups (public or corporate) that are not on the scan list are not delivered. Incoming one-to-one calls and Quick Group calls are not affected by Talkgroup Scanning. Likewise, the Talkgroup

Scanning feature does not prohibit a user from originating a call to any contact, a list of contacts (Quick Group), or talkgroup (regardless of whether it is part of the scan list or not).

Priority Scanning

A configurable number of the talkgroups within the scan list can be designated as Priority talkgroups. These talkgroups are assigned with Priority 1 (highest) through Priority n (lowest), with the default set at 3. Each priority level can have only a single talkgroup assigned to it. Talkgroups on the scan list not assigned as priority talkgroups are considered to have no priority.

For PTT Radio mode, the priority of incoming calls on the selected channel is elevated to a higher Priority than Priority 1 talkgroup but lower than Emergency and Broadcast (Collaboration and Command feature sets).

The following is call type priority – higher priority call types preempt lower priority call types. Call types with the same priority do not preempt.

1. Emergency
2. Broadcast
3. Priority scan 1
4. Priority scan 2
5. Priority scan 3
6. Non-priority scan / Private call / Quick Group call / Area-Based call

Missed Call Alerts

Missed Call Alerts are received for Private (1:1) and Quick Group calls when a priority call is in progress. Missed Call Alerts are received for priority scan list calls if the user has the presence status of Do Not Disturb. Non-priority scan list calls do not provide Missed Call Indication.

Missed Call Alerts are provided to the Dispatcher and shown in the call logs.

Call Behavior Summary


The following table summarizes call behavior while scan mode is ON:


Table 11: Call Behavior Summary with Scan Mode ON

Current Call Type	Incoming Call Type	Behavior
Emergency call	Any call type: <ul style="list-style-type: none"> • Emergency Call* • Broadcast Call** • Priority Scan List Call • Non-Priority Scan List Call • Private Call (1:1) • Quick Group Call 	The current call continues. Missed call alert received only for incoming Private Call or Quick Group call.
Broadcast call**	Any call type: <ul style="list-style-type: none"> • Broadcast Call** • Priority Scan List Call • Non-Priority Scan List Call 	The current call continues. Missed call alert received only for incoming Private Call or Quick Group call.

Current Call Type	Incoming Call Type	Behavior
	<ul style="list-style-type: none"> Private Call (1:1) Quick Group Call 	
Priority 1-n scan list call	<ul style="list-style-type: none"> Broadcast Call** Higher priority scan list call Currently selected channel (PTT Radio) 	The current call is preempted.
	<ul style="list-style-type: none"> Lower priority scan list call 	The current call continues, and no missed call indicated.
	<ul style="list-style-type: none"> Private (1:1) call Quick Group call 	The current call continues and Missed Call Alert shown for an incoming call.
Non-Priority scan list call	<ul style="list-style-type: none"> Broadcast Call** Priority scan list call Currently selected channel (PTT Radio) 	The current call is preempted.
	<ul style="list-style-type: none"> Other non-priority scan list call 	The current call continues, and no missed call indicated.
	<ul style="list-style-type: none"> Private (1:1) call Quick Group call 	The current call continues and Missed Call Alert shown for an incoming call.
Private (1:1) call or Quick Group call	<ul style="list-style-type: none"> Broadcast Call** Priority scan list call 	The current call is preempted.
	<ul style="list-style-type: none"> Non-priority scan list call 	The current call continues, and no missed call indicated.
	<ul style="list-style-type: none"> Other Private (1:1) call Quick Group call 	The current call continues and Missed Call Alert indicated for an incoming call.
Area-Based call	<ul style="list-style-type: none"> Emergency Call Broadcast Call Priority 1 Scan List Call Priority 2 Scan List Call Currently selected channel (PTT Radio) 	The current call is preempted.
	<ul style="list-style-type: none"> Non-Priority Scan List Call 	The current call continues, and no missed call indicated.
	<ul style="list-style-type: none"> Other Private (1:1) Call Area-Based Call 	The current call continues.

Current Call Type	Incoming Call Type	Behavior
	<ul style="list-style-type: none">Quick Group Call	

 **NOTE:** * Emergency calls preempt all call types except other emergency calls.

 **NOTE:** ** Broadcast calls preempt all call types except other broadcast calls and emergency calls. Talkgroup scanning does not affect emergency and broadcast calls. Please see [Affiliation on page 33](#) for Talkgroup scanning behavior with Affiliation feature.

Configuration

The Talkgroup Scanning feature is an optional feature controlled by system-wide configuration (enable or disable) with the default set to enable. The maximum scan list size is configurable system-wide from 1-16 (default = 8) for the standard PTT application and Dispatch. The maximum number of priority groups is configurable from 1-3 (default = 3).

2.28

Authorized User

An authorized user is a PTT user who has permission (configurable) to perform additional capabilities for their contacts. The administrator can enable any CommandCommand or higher feature set user as an authorized user at the subscriber-level.

An authorized user may have permissions the do the following:

- Activate ambient listening for the remote user
- Activate discreet listening for the remote user

2.29

Remote Supervision

Remote Supervision provides additional permissions (configurable) that allow an authorized user to perform remote actions on specific users (target users).

Third-party dispatchers can perform remote supervision without a user being in their contact list. Remote Supervision is provisioned using Command or higher feature set and is configured by the administrator in CAT.

Remote Supervision is comprised of the following bundled permissions:


- [User Check on page 55](#)
- [Enable or Disable PTT Service on page 56](#)
- [Remote Emergency on page 56](#)

2.29.1

User Check

The User Check feature is designed to provide tools that allow an authorized user to add a layer of supervision and remote help to a user (target user).

An authorized user is specific users who may have a supervisory role or and dispatchers. This feature is available from the dispatch and PTT Radio Mode for the mobile application. When invoked, the following information is available to the authorized user.

- Current location
- Signal strength (LTE and Wi-Fi)
 -  **NOTE:** Signal strength is only available on Android application.
- Battery level

2.29.2

Enable or Disable PTT Service

An authorized user can disable PTT service for a targeted user. Once disabled, the user no longer has access to PTT service. Authorized users can be dispatchers or mobile users while in PTT Radio mode.

PTT service can be re-enabled for the target user by an authorized user.

2.29.3

Remote Emergency

A remote emergency allows authorized user to invoke emergency on behalf of any other user.

In this case, if the target user is unable to start an emergency on their own or if an authorized user believes that this target user is in danger, the authorized user can initiate a remote emergency on behalf of the target user. The destination of the emergency alert and call is the same as this user had been configured in CAT. Remote emergency start on behalf of the target user is not confirmed end to end if emergency start has failed for target user for any reason (such as target user not reachable, no users available on the group where emergency is started etc) the authorized user is not notified for the emergency start failure.

Authorized user must perform the user-check to confirm if the remote emergency start has been successful for target user or not. Like remote emergency start, remote emergency cancel is also supported where authorized user can cancel the ongoing emergency of the user. In case of user is not reachable, emergency is still canceled for the user and other participants in that emergency are notified with clear status.

2.30

Ambient Listening

There are two types of Ambient Listening features, which are provisioned using the Command or higher feature set and is configured by the administrator in Central Admin Tool (CAT).



NOTE: iOS 12.4 and above does not support Remote Started Ambient Listening. The device initiates an ambient listening session to the authorized user, but no audio is heard.

Remote Started Ambient Listening – where an Authorized User (AU) can remotely open the microphone of a specific user. This device user that is being listened by AU is called a target user. The Target User (TU) does not get an indication that they are being listened to (OS restrictions apply) when ambient listening starts or during an ambient listening session or while terminating the ambient listening session. Also, TU can do any function normally (make calls, text, etc.) as if no session is active. This feature is reserved for the PTT Radio mode only, which is set up in CAT. The ongoing remote started ambient listening session is interrupted for any incoming calls as well as when TU initiates an outgoing call to any contact or group. Remote started ambient listening is not supported when user is in emergency state.

The following Ambient Listening features are provisioned system-wide:

Self-Started Ambient Listening – is when a specific Target User (TU) decides to open their microphone and send the audio to a specific Authorized User (AU). There is no indication on the TU device that they have self-started an ambient listening session (OS restrictions apply) when ambient listening starts, during an ambient listening session, or while terminating the ambient listening session. The ongoing self-started ambient listening session is interrupted for incoming calls when the target user initiates an outgoing call to

any contact or group. The incoming calls to the user do not interrupt the ambient listening session except for incoming emergency calls and broadcast calls.

An authorized user can be a PTT app user with Radio mode, a Dispatch user, or a third-party dispatch user. An AU is required to be enabled by CAT to allow ambient listening to the authorized user's contact. By default, it is disabled. Third-party dispatch users using the MC UNI interface can perform ambient listening on all users in the PTT system.

Maximum Session Duration for Ambient Listening

Maximum duration supported for Ambient Listening session is as follows:

- Minimum – 1 minute (60 seconds)
- Maximum – 24 hours (1440 minutes; 32,400 seconds)
- The default setting is 1 hour (60 minutes; 3600 seconds).

When the maximum duration for an Ambient Listening session expires, it is terminated by the system without any indication to the target user. The listening user (AU) sees an indication that the Ambient Listening session has timed out and can reinitiate the Ambient Listening session if desired.

Ambient Listening Session Reconnect


When an Ambient Listening session is in progress, the listening user (AU) does not receive any incoming PTT calls (except emergency calls).

The Ambient Listening session is interrupted if the target user makes or receives any call. Once the target user is back to idle, the Ambient Listening session reconnects between target user and authorized user. If the Ambient Listening session reconnect attempt fails (due to authorized user not being available or network not reachable), the session is ended. The authorized user must initiate a new session manually in this case. The automatic reconnect of the Ambient Listening session is supported until the maximum duration (1-hour default, 24 hours maximum) is expired or the authorized user ends the session at will. Ambient listening session reconnect is only supported for remotely initiated ambient listening calls and does not apply to self-initiated ambient listening calls.

The PTT system supports QoS, Priority, and Preemption (Rx session setup) for Ambient Listening sessions. For more details, see [QPP Packages on page 136](#).

Device Pseudo Power OFF and ON During Ambient Listening

When pseudo power OFF is enabled, the PTT application continues with the Ambient Listening session until AU exits the call, or the maximum Ambient Listening session duration expires. During this state, there are no PTT calls (including emergency calls) or user notifications for incoming messaging, IPA or MCA, etc. There is no indication to the user that the device is ON and PTT application is sending or receiving traffic. When pseudo power OFF is disabled (the user powers on the device), the PTT application assumes the existing PTT application behavior. It allows user activities on the PTT application (to initiate PTT calls or receive PTT calls, to message, etc.). At the same time, an Ambient Listening session is ongoing in the application background.

 **NOTE:** This feature is device-dependent.

2.31

Discreet Listening

An authorized user can remotely activate the Discreet Listening feature to listen to any target user's PTT calls. In addition, an authorized user can monitor all PTT calls (including emergency calls) the target user makes or receives.

If any dispatch user initiates the first-to-answer private call to the target user, those calls can also be monitored by an authorized user. Discreet Listening is undetectable by the selected target user. The user does not receive any indication on the PTT application that the user is being listened to remotely. Authorized users can be dispatchers or mobile users while in PTT Radio Mode. The target user can be mobile users in either PTT Standard Mode or PTT Radio Mode. Discreet Listening is provisioned as part of the Command or higher feature set and is enabled and configured by the administrator in CAT.

When the authorized user activates Discreet Listening for the target user, any new PTT call to or from the target user is monitored. When a target user makes or receives a new call, the authorized user receives the regular 1:1 (private) listen-only call. While a Discreet Listening call is in progress, the authorized user can listen to any emergency calls initiated or received by the target user.

Discreet listening calls to an authorized user are preempted by any incoming broadcast and emergency call to the authorized user. Discreet listening calls are not preempted for any other call types. Discreet Listening to broadcast calls and full-duplex calls is not supported.

2.32

Wi-Fi Support

A unique feature of the Broadband PTT is support for PTT application access through Wi-Fi access points connected to the Internet. Wi-Fi support extends PTT coverage into areas that are not fully covered by cellular data networks such as hotels, factories, warehouses, and underground work areas.


To use PTT over a Wi-Fi network, customers need to have 802.11g/n/r/ac access points with Internet access, and a PTT supported device with Wi-Fi. The PTT application uses standard HTTPS and TLS connections over TCP when connected to Wi-Fi, easing Wi-Fi network, and firewall configuration required to enable PTT service.


The PTT application automatically performs a hand off from the cellular network to a Wi-Fi network whenever the phone connects to Wi-Fi. The PTT application switches back to cellular data as soon as the Wi-Fi connection is lost.

The following table describes the user experience for hand off between cellular/Wi-Fi when the device is idle (that is, not in a PTT call).

Table 12: Cellular and Wi-Fi User Experience

Transition Type	User Experience
Cellular to Wi-Fi	<ul style="list-style-type: none">• Automatic transition within 6-12 seconds• No Indication if the PTT application is in background• “Reconnecting” message is displayed to the user during transition if the PTT application is in the foreground
Wi-Fi to Cellular	Same behavior as cellular to Wi-Fi transition

 **NOTE:** The transition could take longer as some devices require complete Wi-Fi signal loss before disconnecting from Wi-Fi.

Transition Type	User Experience
Wi-Fi to Wi-Fi (AP to AP with Same SSID) (Access Point to Access Point Roaming)	Seamless Assuming: <ul style="list-style-type: none"> The Wi-Fi network is designed according to Motorola Solutions guidelines No signal “dead zone” exists between access points (AP) wireless controllers are used for AP to AP roaming
Wi-Fi to Wi-Fi (AP to AP with different SSID)	Same behavior as cellular to Wi-Fi transition  NOTE: The transition could take longer as some devices require complete Wi-Fi signal loss (with previous AP/SSID) before transitioning to another Wi-Fi AP

In rare cases that the user does not want to use available Wi-Fi networks for PTT, the Android PTT application provides a setting to ignore the Wi-Fi connection and remain on the cellular network.

Automatic PTT application activation occurs over the cellular network if available with Wi-Fi activation using an activation code as a fallback. See [Wi-Fi Network Activation / Authentication on page 131](#) for more details.

2.33

Audio Codec Support

PTT application supports various audio codecs such as AMR-NB, AMR-WB, and OPUS.

The system-level configuration allows default Codec selection for PTT calls.


- AMR-WB - Adaptive Multi-Rate Wideband (AMR-WB) 23.85-kbps bit rate constant with 16-KHz sampling rate provides improved speech quality compared to narrowband speech codecs. Selectable rates of 6.60, 8.85, 12.65, 14.25, 15.85, 18.25, 19.85, 23.05 and 23.85 kbps. AMR-WB supports modes 0-8. AMR-WB Codec is available on Android and iOS-based PTT application version 9.0.1 and above. Rate selection and modes are configured system-wide per deployment. AMR-WB is included in the Collaboration tiered feature set. AMR-WB can be configured as Octet mode or Bandwidth Efficient mode of operation using system-wide settings. The default mode is 8 (octet-aligned).
- AMR-NB - Adaptive Multi-Rate Narrow band (AMR-NB) 12.2-kbps bit rate constant with 8-KHz sampling rate.
- OPUS-High-Definition (HD) voice with 32-kbps variable bit rate and 48-KHz sampling rate. OPUS Codec is available on PTT application version 8.3 and above. All Android and iOS-based PTT application support OPUS Codec along with Mobile integrated APIs.

2.34

Corporate Address-Book Search

The corporate address book search feature allows PTT users to search for a contact through all corporate users (PTT users only) by name and is supported on handset devices only and not supported on dispatch.

In the PTT application, a user can search for any contact by name in their organization's PTT directory and initiate a PTT call, IPA, or message. This is optional feature can be enabled system-wide (default disabled).

 **NOTE:** PTT directory is all the users in the corporation (up to 40K), including 1000 pushed by the administrator and any personal contacts the user has stored.

A user is allowed to store the found corporate contact as a user-managed personal contact (if user-managed contacts are allowed for that user).

If the found contact is already on the 1000 corporate contact list or as a personal contact, there is not any option to save.



NOTE:

The application does not support dynamic search. Instead, the user can start the search operation by entering the name and pressing **Search** button.

2.35

Userless Device Mode

Userless Device Mode is included in the MCPTT feature set and it requires the device subscription for PTT service.



NOTE: Support for Userless Device Mode requires the device MDN to be provisioned in the PTT system.

Userless Device Mode can be used when there is no dedicated user assigned to a device, such as those mounted in vehicles or trains. Userless device mode allows a shared device to be used even when there is no user logged in to the device, for example, devices shared between by users on different shifts. Any user can pick any device to make instant PTT or emergency call without logging in with specific user credentials.

In Userless device mode, the device is required to be provisioned in the PTT system. Once PTT service is activated on the device, the device is always logged in to PTT service. PTT application does not allow the user of the device to logout of the application. Users can perform normal PTT operations as allowed from the administrator such as make/receive PTT calls, initiate emergency, send/receive messages while device is in userless device mode. Userless device mode is enabled for provisioned devices by the CAT administrator. When the device is operating in the userless device mode, any user can login to PTT applicable using their user credential. When user logs out, device fallback to userless device mode and another user of the device can login to PTT app using it's own credentials. Allowing the same device to be used by multiple users with their own credential and when device is not used can still logging to PTT service for default operations. When a device is in userless device mode, it can be remotely tracked by device location in case the device is stolen or lost.

Userless device mode is included in the MCPTT tiered-feature set.

Chapter 3

Presence Service

The Presence Service allows users to change their presence status as well as see the presence of all contacts. Individual service, for example, calls and Instant Personal Alerts are dependent on Presence status. Users can only change their status from Available to Do Not Disturb (DND) and vice versa.

Presence updates are done using a push mechanism from the device as opposed to a polling-pull mechanism from the server to reduce network impact.

Each PoC server has an integrated presence server that handles the associated users.

3.1

Self-Presence

The following presence states are supported:

- Available
- Unavailable/Offline
- DND – Do Not Disturb

The following table describes the features available in the different presence states:

Table 13: Supported Presence States

Presence State	Call Origination	Call Termination	IPA Origination	IPA Termination
Available	✓	✓	✓	✓
DND	✓	✗	✗	✓
Unavailable /Off-line	✗	✗	✗	✗

The previous presence status is remembered and restored after log out or device power cycle. When the user logs out of the application, the user’s presence status is marked as Offline using the Best Effort.



NOTE: The PTT Radio mode of the client does not allow the user to change their presence status to DND.

3.2

Contact Presence

The presence state of contacts is displayed within the contacts list in the PTT application. The Presence state is not shown for groups or group members. Changes in presence states are communicated and displayed on the PTT application in real-time.

3.3

Presence Notification Options

Each user may have a large number of other administrator-managed users in their contact lists. It can lead to a situation in which presence changes for one user are sent to a large number of other users.

As long as the users are located in different geographic locations, this does not present a problem. However, if a large number of users are colocated (for example, on a single campus) for the cell site serving those users can experience depletion of bandwidth during peak periods of presence updates, such as a shift change. This depletion of bandwidth may cause interference with call completion. Broadband PTT provides the following options to control presence notifications:

- Normal Presence Notifications
- Relevant Presence Notifications
- Disable Presence Notifications

These options can be configured on a per-corporation basis, and all users within the corporation are affected. A change in the configuration for the presence notifications option takes effect the next time the user logs into the service (manual login or power cycle of the phone).

This feature does not prevent users from updating their presence; the server tracks the presence state of users and service behavior associated with the user's current presence state applies. For example, when the user has selected the **Do Not Disturb** state, PTT calls are not received, although the user shows up as `Online` to others. When a user attempts to place a PTT call to a user that is `Offline` or `Do Not Disturb`, an error message is returned to the originator indicating that the user cannot receive calls.

The following sections describe each of these options in more detail.

Normal Presence Notifications

This option provides a full real-time presence for all contacts for all the corporation's users. As users change their presence status, the update is reflected in the contact lists of all the "watchers."

Relevant Presence Notifications

This option provides real-time presence updates for contacts that are relevant to the user. Other contacts are shown as `Available`. The relevant contact list is comprised of two parts with the split between them configurable: history-based relevant contacts and recently used relevant contacts. The history-based relevant contacts are chosen based on the calling and Instant Personal Alert (IPA) history over the past 30 days. At least once per day, the list of called or alerted contacts is compiled for each user of the corporation. Real-time presence is provided for the most called contacts.

For infrequently called contacts, a recently used relevant list is used. Real-time history is provided if a call or IPA fails due to a presence mismatch. It provides the user with immediate feedback on recently used contacts. The recently used contacts continue to show real-time presence until replaced by other recently used contacts or the contact is called frequently enough to be moved into the history-based presence list.

Disable Presence Notifications

This option disables presence updates from being notified to “watchers.” When presence notifications are disabled, all contacts are shown with an `Online` presence.

3.4

Decoupled Presence for Calling and Alert Origination

PTT calls are delivered to users with presence status of `Available`. Likewise, Instant Personal Alerts (IPAs) are delivered to users with presence status of `Available` or `Do Not Disturb (DND)`.

Normally, the PTT application sends a call or IPA origination requests to the server, which validates the presence status of the intended recipients. If the intended users are not available, an error code is returned to the originator, and an appropriate error message is displayed to the user.

The PTT service can be configured such that the PTT application uses the latest presence indication locally available for contacts to block the user from originating calls and alerts when the called user is unavailable. When enabled, the PTT application provides user feedback of this condition before sending the call setup or IPA request to the server. This configuration is not recommended by Motorola Solutions as calls and IPAs could be blocked if the PTT application does not receive timely presence updates for PTT contacts.

3.5

Temporarily Unreachable SMS Configuration

The Temporarily Unreachable SMS configuration provides the ability to disable Temporarily Unavailable SMS messages sent by the PTT application. Configuration is system-wide enable/disable.

3.6

Presence Throttling

Presence throttling is an optional feature that allows throttling of presence notifications based on some watchers in a particular cell.

The throttling mechanism delays the presence notifications if necessary to maintain the number of presence updates sent to users in a particular cell under a maximum threshold. User cell location is based on the `CellID` reported during periodic registration requests. As such, throttling is based on an approximate number of watchers in a cell.

The watchers are tracked per PoC server, not system-wide.

Chapter 4

Location Services

Location Services include Location Reporting and Location Tracking/Geofencing.

4.1

Location Reporting

Location Reporting is a service that uses PTT application location information to report the location periodically or on-demand at variable intervals to the PoC Server.

A dispatcher can request more frequent location reporting of a user or a group using the on-demand Location request capability. This capability can request periodic reporting based on time intervals or distance traversed. On-demand location trigger settings can be activated for a configured time or made active "forever." For example, a dispatcher can request location reporting every 60 seconds or every 100 meters of movement and make this trigger active for 8 hours. After 8 hours, the location reporting of the user or the group reverts to the system default configuration (15 mins or 500 meters). If the On-demand trigger is activated "forever," the user or users within the group reports the location every 60 seconds or 100 meters until the dispatcher disables the "forever" configuration. The administrator configures the min-max range of on-demand time or distance trigger parameters and is specific to each deployment based on system capacity and resource requirements. Location reporting change is not available on broadcast group and large groups up to 3000 members.

Android and Android Open Source Project (AOSP)

Location Reporting on an Android device uses the Global Positioning System (GPS) method, which provides more accurate notification of location change updates based on minimal distance change of the device with decreased battery life.

iOS

Location Reporting on an iOS device uses two methods as follows:

- The standard Significant Location Change (SLC) method is the default option. It provides less accurate notifications of location change updates based on significant distance change of the device with good battery life. The device determines significant distance change.
- Global Positioning System (GPS) method - provides more accurate notification of location change updates based on distance change of the device with decreased battery life.



NOTE: Distance-based location updates from iOS devices require iOS users to turn on GPS. Suppose that iOS users are using SLC-based mechanism. In that case, time and distance-based updates are not guaranteed and published as per the iOS algorithm.


4.1.1

On-demand Location Update

The location information of all the fleet members is updated with a system-wide frequency.

This system-wide frequency is decided by considering the battery life of the handsets. If battery life is not a concern and the dispatcher has to locate the fleet members more frequently, the On-demand location feature can be utilized.

There are two ways the dispatcher can request a location of the fleet member on demand which are explained here.

 **NOTE:** Reducing the location reporting interval to a lower value impacts the data consumption and battery usage on the device.

4.1.1.1

One Time On-Demand Location Update

The One Time On-demand location update enables the dispatcher to select a fleet member and get the current location information.

4.1.1.2

Periodic On-Demand Location Update

For example, dispatcher can set an on-demand location request for contacts and talkgroups to update every 5 minutes for 2 hours or when the members move a distance more than 100 meters. The throttle time setting is used when the fleet member is moving fast and the location publish is frequent, which can discharge the handset battery of the fleet member. For example, if dispatcher sets the throttle time to 60 seconds, the fleet member waits for 60 seconds to publish the latest location due to change in distance after the last published location (depend on the location update interval setting) irrespective of the fleet member is moving fast or slow. If you select the **Forever** check box, the on-demand location update for the selected contacts and talkgroups do not end until dispatcher ends the request or sends a new request.

4.2

Location Tracking/Geofencing

Location Tracking allows a PTT supervisor or dispatcher of any talkgroup to check the current location of all talkgroup members on the map, to create a boundary (Geofence) for a talkgroup, and receive notifications when members enter or leave the boundary. Multiple supervisors in a talkgroup are allowed to have location permissions. Only one supervisor with location capabilities can create a fence at any point in time. A maximum of 250 supervisors is allowed for each talkgroup. Location tracking and Geofencing is not available on broadcast talkgroups and Large talkgroups up to 3000 members.

Geolocation

PTT application provides supervisors and dispatchers with the ability to check the geographic location of all talkgroup members on maps. Supervisors can be assigned to a prearranged talkgroup and can optionally be enabled for location service using the CAT. Multiple supervisors per prearranged talkgroup can have location service.

CAT allows administrators to enable multiple supervisors for Geolocation Service.

Once the supervisor is assigned to a prearranged talkgroup and enabled for location service, the supervisor identifies the talkgroup with a distinct icon. Upon selecting the location-enabled talkgroup, all the talkgroup members' current location is requested and automatically updated on the supervisor's map. The supervisor also receives automatic location updates.

All the talkgroup members are displayed on the map with the relevant presence of each member. The supervisor or dispatcher can initiate PTT calls from within the map window by selecting a talkgroup member's location marker.

Restrict Automatic Location Publish (Default Yes)

Once a user is assigned as a contact to a dispatch console or location-capable supervisor, the client starts publishing the location. In some cases, the user's location is supposed to be discreet and should not

be published under normal circumstances. Restrict Location Publish feature provides that control to the administrator. A PTT user (assigned as a contact to a dispatcher, authorized user or supervisor) publishes location only when Automatic Location Publish is enabled.

Automatic Location Publish is not applicable during emergency calling and when the user explicitly sends location during a secure message.

Geofence

In addition to geographic location reporting to a supervisor, the supervisor or dispatcher is also allowed to define the virtual boundary, popularly known as Geofence, to monitor location activity for all talkgroup members. Geofences for a talkgroup can be created by a single PTT supervisor and multiple dispatchers (up to 25). However, only one supervisor is allowed to create and manage a Geofence at any given time. The Geofence is circular, and it is set using a distance from the fence center. Geofence can be a static fence or follow me fence. The static type of a fence is one with a static location as fence center. The dispatcher uses a static type of a fence. The follow me type of a fence has the supervisor's location as the center, and the fence follows the supervisor as they move. Geofences can be preconfigured and the dispatcher can make the fence active or inactive.

Geofences have an action associated with them that can be either "Fence Cross Notification" or "Play a Tone". The action for fence cross notification allows time-based fixed interval location reporting and, optionally, distance-based location reporting. Distance-based interval reporting sends a location update when the user has moved a configurable distance (100 to 500 meters) and also allows a throttle time to be configured so that fast-moving users do not report too often.

A Geofence with the action of "Play a Tone" allows a continuous warning tone to be played while the user is within the fence. See [Area-Based Warning Tones \(Optional\) on page 67](#) below for more details.


Once configured, active Geofences are evaluated locally on the user's device.

When using Geofence consider the following:

- **Network Coverage** - for reliable Geofence operations, reliable data connection, network coverage, and GPS coverage is necessary. On most devices, enabling WiFi can significantly improve location accuracy.
- **GPS/Location Feature Enable** - GPS/Location is mandatory for Geofences with Tone Alert operations. If a user disables GPS/Location on the device while a tone alert Geofence is active, the application shows a persistent message in a banner to make sure that user is aware of active fences. The Geofence feature uses Android or iOS platform capabilities for fence computation. While a Geofence is active on the device, battery usage increases compared to regular PTT usage without active Geofences.
- **Device-specific Considerations** - (1) Android and iOS devices have a built-in algorithm to ensure that the user has crossed a defined Geofence. This may result in a delayed identification that the user has crossed the Geofence, if the user is near the fence boundary. Google and Apple do not specify the delay or distance. (2) Geofence crossing detection is not available while an iOS device is in Airplane Mode, even if WiFi is enabled. Android devices may detect fence crossings while in Airplane Mode if WiFi is enabled, but the accuracy is affected.
- **Interaction with the MCPTT affiliation feature** - Geofence configuration is only received by a user's device while affiliated to the talkgroup for which the Geofence is configured by the dispatcher. If the user changes the affiliated talkgroup, Geofence configuration is missed, resulting in the user not participating in a Geofence or continuing to participate in a Geofence if it was deactivated while the user's device was not affiliated to the talkgroup associated with the Geofence. See [Affiliation on page 33](#) for additional details.
- **Fence Radius** - a Geofence radius is recommended to be at least 100-150 meters to ensure accuracy of Geofence events.

Fence Notifications

Once the fence is defined and enabled, the supervisor or dispatcher can see the fence overlaid on the map with all the talkgroup members' locations. When any talkgroup member enters or leaves the area defined by the Geofence, a fence cross notification is sent to that talkgroup member and supervisor or dispatcher, notifying each of the location activities.

 **NOTE:** The dispatcher or supervisor needs to be affiliated with the talkgroup to create a fence for a talkgroup on Dispatch or Supervisor. Also, only the affiliated members can get the Geofence notification.

Initial Fence Notifications

Additional configuration of member notification allows a supervisor or dispatcher to notify talkgroup members about fence creations and their relative status relative to the fence when it is initially defined and enabled. When set to In-Fence notification, all the talkgroup members inside the fence receive status notification that they are inside the fence. When set to the Out-Fence notification, all the talkgroup members outside the fence receive an initial status notification that they are outside the fence.

Notify Me and Notify Member.

The supervisor or dispatcher can enable or disable fence notification message for members. Fence notification message for supervisor can also be controlled via Notify me settings using Notify member settings available inside PTT application.

Active Boundary Time

Active Boundary Time allows a supervisor or dispatcher to set the duration to monitor talkgroup members' location activity anywhere starting from 1 hour to 7 days.

Update Interval

The supervisor or dispatcher is also allowed to tune the location reporting from talkgroup members to more frequent updates. The range is from 1 minute to an hour. By default, talkgroup member location is reported to a supervisor every 5 minutes.

Area-Based Warning Tones (Optional)

This feature allows an authorized web dispatcher to configure the action to play a continuous warning tone on a user device to all field workers within a particular area (Geofence). A use case for this feature is a mining company that needs to inform workers of a situation in which a blast will be happening, an emergency exists, or evacuation is necessary. For any given Geofence, the dispatcher can select from three types of tones with priorities of high, medium, or low. The tones are system wide configurable.

The Area-Based Warning Tones are as follows:

Table 14: Area-Based Warning Tones

Name	Description
Area Warning Tone - Blast Tone	Played to indicate when you are within a blast area. For iOS, when the app is suspended, the periodic blast tone is not played periodically while in the blast geofence. The app is suspended when put into the background and cannot play the periodic tone.
Area Warning Tone - Emergency Tone	Played to indicate to when the user to follow emergency procedures. This tone is played to escalate the priority from the blast notification to a mining emergency notification. For iOS, when the app is suspended, the periodic blast tone is not played periodically while in the blast geofence.

Name	Description
Area Warning Tone - Evacuation Tone	The app is suspended when put into the background and cannot play the periodic tone. Played to indicate when you are notified to immediately evacuate the mining site for an impending blast. For iOS, when the app is suspended, the periodic blast tone is not played periodically while in the blast geofence. The app is suspended when put into the background and cannot play the periodic tone.

Chapter 5

Messaging Services

5.1

Integrated Secure Messaging

3GPP MCDATA compliant Integrated Secure Messaging allows a PTT user to exchange secure text messages, multimedia content, and location information with other PTT users.

Text messages are free-form or user-defined and include store-and-forward (with time-to-live) to ensure that the recipient has the best chance to receive the communication. On the originating device, a user can compose a message while offline, and it is sent when the connection is restored. One-to-one messages provide the sender with a delivery-receipt confirming the delivery of the content. Multimedia content can include images, videos, and recorded audio, and other files. Location messages allow a PTT user to send a specific address or GPS coordinates of their current location.

All user types are supported except an Interop user type.

Android, Android Open Source Project (AOSP), iOS, Web dispatch PTT applications are supported.

5.1.1

Media Types

The table below describes the media types for both Android and iOS devices.

Table 15: Supported Media Types - Captured or Recorded

Attachment Type	Source Format	Sent Format	Rate or Resolution
Capturing images from the camera	JPEG	JPEG	Android 1280 x 720 for landscape images 720 x 1280 for portrait images JPEG with 0.5% compression ratio
	PNG	JPEG	iOS 807 x 605 for landscape images 605 x 807 for portrait images JPEG with 0.5% compression ratio
Recording audio	AAC	AAC	Android 64 kbps encoding
	AAC	AAC	iOS AAC with no compression
Recording video	MP4	MP4	Android 640 x 360 for landscape images 360 x 640 for portrait images
	MOV	MP4	iOS Medium Quality 640 x 480 for landscape images 480 x 640 for portrait images

Table 16: Supported Media Types - Gallery or Device

Attachment Type	Source Format	Sent Format	Rate or Resolution
Image	BMP, GIF, JPEG, PNG	JPEG	Android 1280 x 720 for landscape images 720 x 1280 for portrait images JPEG with 0.5% compression ratio
	JPEG, PNG	JPEG	iOS JPEG with 0.5% compression ratio
Video	MP4, 3GP, MKV, MOV	MP4	Android 640 x 360 for landscape video 360 x 640 for portrait video iOS Medium Quality iPhone 6+
			980 x 735 for landscape video 735 x 980 for portrait video Phone 6s 568 x 320 for landscape video 320 x 568 for portrait video
Document	DOC, DOCX, PDF, PPT, PPTX, XLS, XLSX	DOC, DOCX, PDF, PPT, PPTX, XLS, XLSX	Android and iOS PDF uncompressed

5.1.2

Secure Text Messaging

Secure text messages are sent by selecting a contact or a group.

When a user receives a secure text message, you also receive a system notification. The receiver can reply to the sender and reply all (for group messages). Messages can be forwarded to other PTT users and delivery receipts for 1:1 messages ensures delivery.

Secure text messages are shown in threaded history along with other call history.

Secure text messaging supports the following:

- UTF-8 encoded
- Up to 2000 characters (ranges from 500–2000 (single-byte) depending on language) default = 300 (0 = disabled)
- Text messages are free-form or selected from a list of preconfigured messages
- Up to 10 configurable user messages
- International language

5.1.3

Multimedia Content

Multimedia content includes images, video, and recorded audio, and files as a message attachment.

All multimedia content is automatically compressed before sending.

Multimedia messages are also shown in threaded history along with call history.

The maximum multimedia attachment size that can be transferred (originated or received) and is configurable system-wide from 0–20MB, default = 5MB (0=disabled). If file size is exceeded, you receive an error message.



NOTE: The multimedia attachment size configuration includes the messaging overhead. For example, with 20 MB of size configuration, actual multimedia that can be sent is approximately 17-18 MB in size.

Secure Image Messaging

An image is sent from the picture gallery or a picture taken by the camera on the device.

When a user receives an image message, you also receive a system notification. Thumbnails are shown for photos. Automatic download of attachments is based on the user settings. The recipient can reply to the sender and reply all (for group messages). Messages can be forwarded to other PTT users and delivery receipts for 1:1 messages ensures delivery.

Secure text messaging supports the following:

- Animated GIF 89a
- GIF 87a
- GIF 89a
- JPEG
- PNG

Images are converted to JPEG 0.5% compression.

Secure Video Messaging

A video is sent from the video gallery or video recorded by the camera on the device.

When a user receives a video message, they also receive a system notification. Thumbnails are shown for videos. Automatic download of attachments is based on the user settings. The recipient can reply to the sender and reply all (for group messages). Messages can be forwarded to other PTT users and delivery receipts for 1:1 messages ensures delivery.

Secure video messaging supports the following:

- H.263
- H.264
- MPEG-4

The video is converted to MP4 medium resolution.

Secure Voice Messaging

A voice message is a recorded audio message that can be sent to recipients. While sending a voice message, you can record, preview, rerecord, erase, and send the message.

When a user receives a voice message, they also receive a system notification. Automatic download of attachments is based on the user settings. You can reply to the sender and reply all (for group messages). Messages can be forwarded to other PTT users and delivery receipts for 1:1 messages to ensure delivery.

Secure voice messaging supports the following formats:

- AAC
- MP4

Document Messaging

A document message is sent or received from within the PTT application to other PTT users.

Document messaging supports the following formats:

- DOC
- DOCX
- PDF
- PPT
- PPTX
- XLS
- XLSX

5.1.4

Location Message

Select location pin icon to share location on Google or ESRI map and share within PTT application.

When a user receives a location message, you also receive a system notification. The recipient can reply to the sender and reply all (for group messages). Messages can be forwarded to other PTT users and delivery receipts for 1:1 messages ensures delivery.

Location messages are also shown in threaded history along with call history.

The device OS provides the location.



NOTE: Location services must be enabled on the device and the PTT application must be granted permission to use Location Services. Google asset tracking fees apply.

5.1.5

Store-and-Forward

The Store-and-forward feature is used to keep and send messages to unavailable users who are offline or Temporarily Unreachable.

Store-and-forward service parameters are configured system-wide.

Time-to-live (TTL) for notifications is configurable system-wide 30–10,080 minutes (7 days) default = 2,880 minutes (2 days). This parameter allows the messages to be stored on the server when messages are not being able to deliver to the user due to a user being offline or the user not reachable.



NOTE: Store-and-Forward not applicable with Talkgroup Affiliation Services.

Messages are discarded after TTL expiry and not delivered to the user when the user becomes available.

PTT user application allows the attachments to be downloaded automatically as and when received or download the message is viewed. Attachment downloads are allowed for up to 30 days from the time they are sent (configurable on a system-wide basis, maximum 30 days).

A device change restores messages based on the above configuration (default 30 days).

All messages sent to Handset type user or User license type user with Private use remain on the device until the user removes the PTT application or the PTT application to reactivate the PTT subscription. A User license type user with shared use mode can download the messages for up last 7 Days (default).

5.1.6

Broadcast Secure Text Messaging

Broadcasters can send a one-way secure text message to other broadcast group members.

Broadcast group members cannot reply or send secure text messages to the group. See [Broadcast Calling and Messaging on page 39](#) for more details.

5.1.7

Origination Permissions

The following table shows the user message origination permissions for different PTT user subscription types.

Table 17: Origination Permissions

Originating	Terminating		
	Personal	Administrator	Administrator and User
Personal	✓	✗	✓
Administrator	✗	✓*	✓*
Administrator and User	✓	✓*	✓

* Within corporation or external subscribers

Chapter 6

Video Services

Video Services allows a user to send or push a one-way, live H.264 streaming video with audio to another user, dispatcher, or talkgroup. Dispatchers can request video from users (confirmed video pull) by invitation. The Video Services feature is provisioned as an add-on feature to any tiered feature set.

Recipients can be any PTT contact or corporate talkgroup assigned to a user that is capable of receiving video calls.

The user can stream the video from a device-integrated camera (front or rear). By default, the video session opens with the back camera of the device. When the camera is changed from rear to front, the next streaming video resets to the default rear camera. The user has the capability to flip the camera on live streaming.

Each video session allows a single streamer, and each participant can have a single active video call at a time.

When sending video to a talkgroup, the video stream is available to any member of the talkgroup that is configured to receive group video and begins streaming as soon as the first recipient accepts the invitation.

Talkgroup members may leave and rejoin a video call at any time.

A private (1:1) streaming video call ends if the recipient leaves the session.

Video is sent and received securely using TLS over Wi-Fi and DTLS over cellular data connections.

A video session continues until either the streamer ends the call or all receiving participants leave the call. Each video session in group can have up to maximum 15 video recipients.

6.1

Video Session Types

The video session types supported are as follows:

- Mobile-initiated video streaming
 - Private 1:1 video
 - Quick Group video
 - Talkgroup video (corporate talkgroups)
- Dispatch pull requested video stream (confirmed, unconfirmed)
 - Confirmed video: user accepts a request to stream
 - Unconfirmed video: video stream starts automatically; initiation by authorized users
- Simultaneous streaming video and audio PTT calls

6.2

Supported Video Resolutions

The Streaming Video feature provides high video quality but also adapts to different network conditions to provide a continuous video stream. Supported video resolutions are 360p to 720p, depending on the camera capabilities. The maximum resolution supported is application build-time configurable, default is 720p.

6.3

Push Video User Experience

A user sends a video to contact, quick group, or corporate talkgroup. While streaming, a preview of the video is shown in the app. The streamer can mute the microphone, stop sending the video, or end the video session.

When the streamer stops sending video, another call member can stream the video if the video feature is enabled. The receiver device receives an incoming video stream alert that repeats until the session answer time expires or the user accepts the incoming stream. The application settings can be configured to accept incoming videos automatically. Once accepted, the video is displayed. Incoming video sessions are shown in the conversation history. PTT call audio, and video audio are mixed, or PTT call audio has priority using the app setting. Past video streams show in history (no playback).

Video call late join is not supported. Instead, any new user affiliating to the group does not receive the ongoing video stream on the group. If a user ends the continuing video call, it does not automatically rejoin the ongoing video streaming call. Users can manually join the ongoing video streaming call when initiating the call to a talkgroup. The user does not get any indication for any ongoing video streaming call on a talkgroup.

A dispatcher receives an alert pop-up for an incoming video stream. The dispatcher can view the video stream by accepting the alert. The video session is displayed in a separate video player window. Ongoing group video sessions are additionally indicated for monitored groups. The dispatcher can view a single video stream at a time, but can switch between ongoing group video streams on monitored groups.

6.4

Pull Video User Experience

The dispatcher can request a stream from a user. The request is sent to the device for a confirmed request, and the user accepts and starts the video. An unconfirmed request is sent to the mobile device, and the mobile device starts sending video automatically if the user setting does not prohibit (user privacy setting). Monitored talkgroups show active video streams.



NOTE: Release 9.1 is limited to pulled 1:1 video to the dispatcher.

iOS 12.4 and above, does not support unconfirmed video transmission because video and audio cannot be initiated while the app is in the foreground.

On Android devices, the user must bring the app to the foreground to send a video and see the video preview. An unconfirmed pull request while the display off brings the app to the foreground for a video preview.

6.5

Video Interaction

The following table lists the incoming call video session behavior for mobile users:



NOTE: While there is a video session ongoing, if a user enters into an emergency, the ongoing video session continues.

Table 18: PTT User Incoming Video Session Behavior

Ongoing		Incoming Video Session Behavior
PTT Call	Video Session	
✗	✗	Tone indicates an incoming video session Video barge is based on app setting: “Auto Answer” or “Manual”
✓	✗	
✗	✓	Missed video session Missed Call Alert (MCA) indication
✓	✓	When in DND, incoming video session is not delivered When in DND, incoming video pull requests are allowed If ongoing PTT call and video session are on same talkgroup: incoming video session from another talkgroup is MCA. When in DND, incoming video session is not delivered. When in DND, incoming video pull requests are allowed. If an ongoing PTT call and video session are on different talkgroups and incoming video session is on the same talkgroup as PTT call: the existing video session is ended, and incoming video session is received.

The following table lists the originating (push) call video session behavior for mobile users:

Table 19: PTT User Outgoing Video Session Behavior

Ongoing		Outgoing Video Session Behavior
PTT Call	Video Session	
✗	✗	User can originate video session (group, 1:1, quick group)
✓	✗	User can originate video session to participants in the PTT call context
✗	✓	Video session origination is not allowed; only single video session at a time is supported
✓	✓	

The following table lists the incoming (pull) call video session behavior for dispatchers:

Table 20: Dispatcher Incoming Video Session Behavior

Ongoing			Incoming Video Session Behavior
PTT Call	Video Session	Monitored Group Video	
✗	✗	✗	Toast notification displayed Video barge is based on app setting: “Auto Answer” or “Manual”
✗	✗	✓	Toast notification displayed

Ongoing			Incoming Video Session Behavior
PTT Call	Video Ses- sion	Monitored Group Video	
			Video barge is based on app setting: "Auto Answer" or "Manual"
			Monitored groups show video in progress indication
			Dispatcher can view a monitored group video session at any time
✗	✓	✗	Toast notification displayed
✗	✓	✓	Monitored groups show video in progress indication
			Dispatcher can view a monitored group video session at any time - dispatcher ongoing video session leg is dropped
			Incoming 1:1 calls are not received, but indicated with an MCA.

6.6

Telephony Interaction

The Telephony interaction is as follows:

Android Devices

- Ongoing Call Priority (Default)
 - An ongoing cellular call continues and an incoming PTT video session is rejected with user busy indication. No Missed Call Alert (MCA) is displayed.
 - An ongoing PTT video session continues and an incoming cellular call is rejected.
- Telephony Call Priority
 - An incoming PTT video session is rejected during a cellular telephony call.
 - An ongoing PTT video session will end if a cellular call is answered.

iOS devices

No configuration parameter exists. Behavior is the same as Telephony Call Priority previously described except for an ongoing cellular call continues, and an incoming PTT video session is rejected.

6.7

Configuration and Provisioning

The video services configuration and provisioning is as follows:

System-Wide Configuration

System-wide configuration is as follows:

- Video services allowed enable or disable
- Corporate-Level allowed enable or disabled (default = disabled)

- Unconfirmed pull video allowed enable/disable (default = enabled)
- Video idle time before video session ends: 2-120 seconds (default = 10 seconds)
- Video transmit hold time: 30 seconds to 2 hours (default = 1 hour)
- Video answer timeout: 10 sec to 32 seconds (default = 32 seconds)
- Maximum number of users allowed to receive video in a group; 2-250 members (default = 15), including the originator. Values above 15 require system engineering validation and may be supported.

CAT Configuration

CAT configuration is as follows:

- Video allowed enable or disable, subscriber-level
- Group video receive allowed enable or disable, subscriber-level
When enabled, the user is able to receive group video sessions, subject to the max number of allowed receivers in a group. When disabled, the user is NOT able to receive group video but is able to send video and receive 1:1 video and quick group video. Default is enabled.



NOTE: CAT control is allowed only for subscribers provisioned with the video streaming feature.

- Unconfirmed video pull allowed enable or disable, assigned to authorized users for specific target users

Subscriber Provisioning

Video services is provisioned using an add-on feature, additional charge per subscriber.

Device Setting

- Allow unconfirmed pull enable allow/disallow (default = disallowed). When set to allow, an unconfirmed pull request automatically initiates video. When set to disallow, an unconfirmed pull request is rejected.

6.8

Caveats

The video services caveats are as follows:

- Simultaneous video sessions are supported for MCPTT tier. Only one active video session allowed at a time for mobile users and dispatchers.
- Unconfirmed video pull is not supported with iOS 12.4 and later.
- A video session may drop during the user network transition from LTE and Wi-Fi and vice versa.
- The user must bring the application to the foreground to send video and see the preview.
- The supported browsers Google Chrome, Microsoft Edge, or Mozilla Firefox must be used for dispatchers.
- Landscape mode video is not supported.
- 1:1 video session is active only while the console is participating; if console user switches to a talkgroup video session, the 1:1 video session ends for dispatchers
- Dispatchers cannot stream video.
- A maximum of 15 viewers are allowed for group video. Video session origination for a group with more than 15 viewers gives an error message.
- Talkgroup video is allowed to corporate talkgroups only
- Incoming video calls are not delivered to users in DND

- Streaming video on a broadcast talkgroup is not supported
- Lawful Intercept or CALEA for video is not supported
- In-call permissions (initiate, receive, listen only) do not apply to video calls

6.9

Supported User Types

Video services apply to the following user types:

- Handset Standard
- Handset PTT Radio
- User Standard
- User PTT Radio
- Cross-carrier Standard
- Cross-carrier PTT Radio
- Wi-Fi Only Standard
- Wi-Fi Only PTT Radio
- Dispatch (Authorized User only)



NOTE: Specified caveats are based on user types.

Chapter 7

Emergency Services

7.1

Emergency Calling and Alert

The 3GPP MCPTT Standard specifications define emergency service.

Emergency Calling and Alert feature was developed in compliance with the 3GPP MCPTT technical specification for emergency services. Emergency Calling and Alert is available for Command or higher tiered-feature sets.

Multiple users in a group can declare an emergency. When a second user declares an emergency, they preempt the first user if that user has the PTT floor. Participating users in an emergency talkgroup call receive an alert from all users in an emergency and can view all members at any time except for late joiners. Furthermore, a dispatcher can preempt any user in an emergency. When a user is in an emergency, the user can use a PTT hard key to cancel the emergency or request the PTT floor again (System-wide configurable).

The following emergency services are provided:

- Broadband PTT LMR emergency origination and termination.
- Both Private and Group Emergency calls are supported.



NOTE: A dispatcher cannot initiate an emergency alert or call except when initiating a remote emergency call on behalf of a regular user.

- Administration control

7.1.1

Emergency Life Cycle

The Emergency Life Cycle is as follows:

A user can activate the emergency button in the application or use a supported hardware button (even when a device is in the locked state). This action sends an Emergency Alert containing emergency PTT user's location, battery status, and signal strength. The display of this information varies depending if the recipient is a regular user or an authorized user for this user. The repeated emergency alert from the user already in emergency is not sent to any other participants in the group. The destination of the emergency alert can be members of a specific group or a specific user, depending on CAT configuration. This action also puts the user into Emergency State.

Once a user is in Emergency State, any call made while in this state is considered an Emergency Call. The destination of this call is the same destination as the Emergency Alert. While in Emergency State, a user may not be able to change groups or users, until the Emergency State condition is canceled.

Emergency cancellation can be performed by the originator of the emergency alert or by any of their authorized users including Dispatchers. Emergency cancellation permissions are configured in CAT by the Administrator to allow users to turn on or off their emergency. Only an authorized user or dispatcher can cancel the emergency if this is turned off.




NOTE: All the new emergency calls as well as normal calls upgraded to emergency are captured in Call Detailed Records.


7.1.2


CAT Administration Control

The CAT controls the following emergency services features:

- Emergency Destination
 - Selected Talkgroup – applies to PTT Radio mode only.
 - Specific Talkgroup – a primary and secondary destination can be configured.
 - Specific User (Private call) – a primary and secondary destination can be configured.

 **NOTE:** Selection of a contact as the emergency destination for both Primary and Secondary is not recommended. A contact may be unavailable for various reasons and therefore, the emergency call may not be initiated. Please exercise caution when using this configuration.


 **NOTE:** Primary and Secondary destinations can only be one talkgroup and one user. Setting up both destinations are Talkgroups or Users is not supported.
- Emergency Call Type
 - Manual – Once a user is in the Emergency State, the user needs to press the PTT button to trigger an emergency call
 - Automatic – A user can automatically trigger a call (hold the PTT floor) for 10 seconds (configurable). Without user interaction, the floor is automatically released unless a dispatcher takes the floor. While user initiates an emergency call and if dispatch user is currently holding the PTT floor, after dispatcher releases the floor, the PTT system automatically enables the microphone of the MCPTT user that declared a last emergency. Any PTT key press, while automatic microphone releases the PTT floor from emergency user (system-wide configuration; default disabled, when enabled, any PTT key press from user in emergency is ignored when automatic microphone is active). For subsequent transmissions in the same emergency call, the user must press the **PTT** button.

 **NOTE:**
iOS 12.4 or above, when a remote emergency is initiated, the user is put into the emergency state. If the user attempts to initiate an emergency call using a PTT accessory button, the call cannot start until the user brings the app to the foreground.

iOS 12.4 or above, when an emergency call originated with automatic call initiation enabled, either remotely or locally with the PTT accessory button, the handset initiates an emergency call, gives the talk permit chirp, and holds the floor for 10 seconds without sending audio. Subsequent attempts for the user in an emergency to take the floor.
- Emergency Recipient Behavior
 - Talkgroup Steering **ON/OFF**
- User Permissions
 - Authorized Users – Receive GPS location, cancel emergency, remote emergency start
 - Regular Users – Send GPS location, allow remote actions

7.1.3

Emergency Originator

 **NOTE:** For specialized devices and accessories that support the hard emergency button, it can be programmed to use as an emergency start only or emergency start and cancel (toggle).

The Emergency Originator user experience is as follows:

- Use soft, hard button or Accessory Emergency button to enter the emergency state and clear an emergency

- Audio (tones) and visual (lights) indications are based on device support
- Call destination is CAT programmable
- Emergency call type is CAT programmable
- Cancellation – the user or the authorized user can cancel emergency anytime

7.1.4

Emergency Recipient - Talkgroup Steering

The Emergency Recipient user experience with Talkgroup Steering ON receives the emergency alert and emergency call, the following happens:

1. If the emergency is on the selected channel, the user has normal participation until the emergency call starts. If there is an ongoing, the emergency originator preempts any ongoing PTT call in that group (destination of the emergency call). Talkgroup priority is elevated based on Quality of Service, Priority, and Preemption (QPP) configuration, if enabled. If scanning is ON, it is paused and resumes when an emergency is canceled.
2. If an emergency is not on the selected channel, the user is moved to the emergency talkgroup that the emergency call is on and the emergency originator preempts any ongoing PTT call in that group (destination of the emergency call). Talkgroup priority is elevated based on QPP configuration, if enabled. If scanning is ON, it is paused and resumes when an emergency is canceled.

The emergency recipient user experience with Talkgroup Steering OFF is as follows:

1. Receive an emergency alert, and emergency call, if the emergency is on the selected channel, the emergency originator preempts any ongoing PTT call in this group. Talkgroup priority is elevated based on QPP configuration, if enabled. If an emergency is not on the selected channel, the emergency alert is received; however, the emergency call is not received. The user may change the selected group to a group in an emergency by manually selecting the group. With user affiliation feature enabled, user does not receive any emergency call or alerts on the nonselected groups.
2. If scanning is on, the emergency talkgroup takes the highest priority. If the user does not want to listen to the emergency talkgroup, they can disable scanning and select a different talkgroup (see scanning OFF behavior). If an emergency call is in one of the scanning groups, the user participates in the emergency. With the user affiliation feature enabled, the user does not receive an emergency call on any nonselected group; however emergency alerts are only received on the selected group and all scanned groups.



NOTE: Talkgroup steering does not apply to MCPTT users enabled with affiliation feature.

7.1.5

Emergency Cancellation

Emergency Cancellation can be configured by administrator to enable or disable a user from initiating an emergency cancellation. Emergency cancellation is available for the following:

- User initiating the emergency state or call
- Authorized user

When an emergency is canceled for the user, the user's emergency status is cleared and the call is downgraded to normal call. Ongoing PTT call on a group does not get downgraded to normal until last user on the group is cleared from emergency. Emergency Cancellation has a predefined status to log valid versus not valid emergency calls as follows:

- Verified Emergency

- False Emergency



NOTE: Emergency cancellation options are configurable and can be turned off system-wide.

Emergency cancellation status is provided in the participating dispatcher logs.

7.1.6

Authorized User Recipient of Emergency Call

An authorized user (Supervisor or Dispatcher) displays map and action buttons if the initiator is a Broadband PTT client

Broadband PTT users have the following additional features:

- User location (if GPS enabled)*
- Refresh for location*
- Show battery strength*
- Show Wi-Fi signal strength*
- Show LTE signal strength*



NOTE: Show Wi-Fi and LTE signal strength is only available on Android devices.



NOTE: When the User Check feature is not enabled in the system, this information is static and provided when the emergency alert is originated and at the time an emergency call is initiated.

7.1.7

Authorized User or Dispatcher Remote Emergency

An authorized user is defined in CAT and is someone (a particular user or a dispatcher) who has “extra privileges or permissions” from a regular user, like a supervisor. One of these permissions is the ability to remotely start emergency on behalf of a regular user, which when initiating remote emergency start, is called a “Target User.”

7.1.8

More Frequent Location Updates During User Emergency

When a PTT user enters into an emergency state, the user's last known location is shared with authorized user followed by more frequent location reporting every 30 seconds (configurable) while the emergency state remains active.



NOTE: This feature not supported on iOS devices.

7.1.9

Caveats

Emergency calling caveats are as follows:

- Not able to enter emergency state or start an emergency call in the same talkgroup until the emergency state is cleared. Emergency initiation fails if there are no users available in the destination group to receive emergency.
- Originator cannot switch talkgroups until emergency state is cleared.

- Rehoming cannot be done to a member who is currently in the emergency state.
- For remote emergencies, the target user should be configured in CAT as someone who can start an emergency call, and an emergency destination should be set for the standard type of user.

7.1.10

Supported User Types

Emergency calling applies to the following user types:

- Handset Standard
- Handset PTT Radio
- User Standard
- User PTT Radio
- Cross-carrier Standard
- Cross-carrier PTT Radio
- Wi-Fi Only Standard
- Wi-Fi Only PTT Radio
- Dispatch (Authorized User only)



NOTE: Specified caveats are based on user types.

Chapter 8

Broadband Regroup Service

Broadband Regroup service is a 3GPP standards-based feature that enables Push-to-talk, messaging, and video across two or more predefined groups by regrouping them into a super group. Up to 20 groups are allowed to be regrouped in a single regroup request. Any constituent group can be part of only one super group at any time. Broadband Regroup service is only applicable to MCPTT tier users, and only MCX groups are allowed to be regrouped for Third Party Dispatchers ONLY.

8.1

Authorized user

A dispatch user is an authorized user allowed to bridge multiple groups on-demand and perform regroup requests. A dispatch user wanting to regroup must be a member of each group to perform regroup operations on any group, but it is not necessary to be currently affiliated. The dispatch user performing the regroup is the only one who can ungroup. A regroup request is persistent until the ungroup operation has been performed. The ungroup operation removes all constituent groups from the super group. If a dispatch user logs out without ungrouping, then the system automatically ungroups the ongoing regroups requested by that dispatch user. Dispatch users must use preconfigured template groups to send a regroup request with a list of constituent groups.



NOTE: An ongoing regroup can not be modified, and therefore adding or removing a group from regrouping is not supported.

8.2

Preconfigured Template Groups

To use the regroup service, an administrator must configure template groups using the CAT portal before using this service. The template groups are downloaded to all users in the corporation, including shared members. Preconfigured template groups are used to configure the newly formed super group after regrouping is performed. An example of configuration includes the group encryption key.

Up to 3000 maximum users can affiliate with a super group formed after regrouping operation. If the regroup request would result in a super group that would have more than 3000 currently affiliated users in total, then the regroup request is rejected. After a super group is formed from a regroup request, any users attempting to affiliate to the super group beyond 3000 users will be rejected.

8.3

User Experience

Regroup service can be performed by a dispatch user for one or more services such as PTT or messaging, or video. It is recommended that regroup operation is performed on all services together for a seamless communication experience. When regroup is performed on constituent groups, all ongoing PTT calls on constituent groups are ended immediately. The PTT application notifies the user to initiate a new call using a pop-up display. Users may press the hard PTT button, if available, or use a pop-up notification to bring the PTT application to the foreground and press the soft-PTT button to initiate a PTT call on the newly formed super group.

Group regroups information (that is, list of groups) is shared with other dispatchers and all the affiliated members of the constituent groups. PTT users affiliated with a constituent group can visually identify that the current affiliated group is regrouped. The PTT app also plays a tone when the affiliated group is re-grouped

or ungrouped. A PTT user can also display the list of constituent groups upon tapping on the regroup icon on the call screen. A PTT user can identify the regroup name when optionally provided by the dispatch user.

The conversation history on the super group is placed under a new history thread. The conversation history for the super group thread is also accessible from the call screen while regroup is active for that selected group for messaging service. History thread for a constituent group also provides an entry when the constituent-affiliated group is regrouped and ungrouped.

Similar to regroup, when the ungroup request is performed, all the ongoing calls on super groups end immediately, and the super group is removed from the system. While the regroup is active on any constituent groups, service on constituent groups is blocked.

Regroup service is only applicable to PTT, Messaging, and Video services. The following list of services remains on constituent groups during regroup operation and is not associated with the super group:

- Location monitoring of constituent group
- Affiliation monitoring of constituent group
- Send OSM on constituent group
- Remote Group Select (user affiliates to the super group if the remotely selected group is currently regrouped)

8.4

Emergency Call and Alert

Emergency calls and alerts are supported seamlessly on the super group formed by regrouping operation. Any user affiliated with a super group is allowed to initiate an emergency. Suppose that the user is configured to initiate an emergency on the selected group. In that case, an emergency alert is sent to all affiliated users of the super group, followed, optionally, by the initiation of an emergency call if a hot mic is configured.



NOTE: If a user has a dedicated emergency destination set using the admin portal, then regroup operation on the dedicated emergency destination group is not allowed.

A regroup request is rejected if any of the constituent groups currently have an active emergency. In this case, dispatch users must clear ongoing emergencies on constituent groups before performing the regroup operation on that group. Likewise, any upgroup operation on the super group is rejected if the super group has an ongoing emergency. Dispatch users must clear ongoing emergencies on a super group before requesting an ungroup operation.

If an authorized user logs out during an ongoing emergency on a super group, then the super group is upgrouped, and all ongoing emergencies are canceled automatically.

8.5

Talkgroup Scanning

PTT users with talkgroup scanning enabled may have up to 16 talkgroup affiliated. The regroup operation may be performed on any of those scanned groups that the user is affiliated with. Scanning priority is not maintained for the newly created super group when one of the scanned groups is part of the regroup request. PTT calls are delivered on all super groups with P1 priority, that is, irrespective of the priorities on one or more constituent groups that the user is affiliated to.

8.6

Interop Groups

LMR Interop groups cannot be part of a super regroup. Regroup operations that involve LMR groups may be regrouped using LMR dispatch consoles.

Chapter 9

PTT Applications

The PTT Applications can be provisioned as one of the following user types:

- Cross Carrier PTT Radio
- Cross Carrier Standard
- Dispatch
- Handset PTT Radio
- Handset Standard
- Integrated Mobile
- Integrated Tracking
- Integrated Web
- Wi-Fi PTT Radio
- Wi-Fi Standard



NOTE: On iOS 13.1, when the PTT app is in the background, and the Volume Boost setting is set to anything other than the default, no audio is heard during an incoming PTT call.

PTT Standard and PTT Radio User Types

The PTT Application supports two modes as follows:

- PTT Standard Mode
- PTT Radio Mode

The Administrator assigns the mode (user type) to the user. The user sees a notification when the mode is changed.

The PTT Standard Application mode provides a user experience tailored to users with little to no Land Mobile Radio (LMR) experience and a greater need for 1:1 calling. Standard mode support all the broadband PTT features and capabilities except the PTT App UI Lock, Zones/Channels, User Check, Ambient Listening, Discreet Listening, Enable or Disable PTT Service, Operational Status Messaging, Manual Answer (Hook signaling) for 1:1 PTT, calls with External Telephony Users, User Profiles, User Role-Based Login, and Affiliation.

The PTT Radio Application mode provides a simplified user interface that mirrors the experience of an LMR user.

Landscape Screen Orientation

The tablet PTT application supports landscape orientation. The smartphone PTT application does not support landscape screen orientation. Landscape orientation is supported for certain specialty, purpose-built devices such as an in-vehicle device used only in PTT Radio mode. For these devices, an error message is displayed and the application is not usable if the Administrator changes the device type to the PTT Standard Application mode. Customers that require landscape support should contact their account manager for evaluation of the need on a case-by-case basis.

The following table lists the PTT Standard and PTT Radio capabilities by Feature, PTT Standard, PTT Radio, Feature Phone PTT Standard, and Feature Phone PTT Radio.

Table 21: PTT Standard and PTT Radio Feature Capabilities

Feature	PTT Standard	PTT Radio	Feature Phone PTT Standard	Feature Phone PTT Radio
System				
Affiliation	✗	✓	✗	✓
Background Call Mode	✓	✓	✓	✓
Broadcast Call Origination	✓	✓	✓	✓
Large Talkgroup	3000	3000	3000	3000
PTT Calling	Talkgroup + Private Call + Quick Groups	Talkgroup + Private Call + Quick Groups	Talkgroup + Private Call + Quick Groups	Talkgroup + Private Call + Quick Groups
SIP Recording	✓	✓	✓	✓
Supervisory Override (Talker Priority)	✓	✓	✓	✓
Wi-Fi Support	✓	✓	✓	✓
Alerts				
Geofence Alerts	✓	✓	✓	✓
Instant Personal Alert	Receive/Send	Receive/Send	Receive/Send	Receive/Send
Missed Call Alerts	✓	✓	✓	✓
CAT				
Administrator-managed contacts	1000	1000	1000	1000
Administrator-managed talkgroups	100	96	100	96
Administrator-managed zones	✗	CAT-assigned	✗	CAT-assigned
Administrator-managed features	CAT-assigned	CAT-assigned	CAT-assigned	CAT-assigned
Restrict Automatic Location Publish	CAT-assigned	CAT-assigned	CAT-assigned	CAT-assigned
User-managed contacts	300	300	300	300
User-managed talkgroups	30	None	30	None
User-managed members per talkgroup	30	None	30	None
Talkgroup scanning	User-controlled scan list (16)	CAT-assigned (16)	User-controlled scan list (16)	CAT-assigned (16)
Priority scanning	User-assigned priorities (3)	CAT-assigned priorities (3)	User-assigned priorities (3)	CAT-assigned priorities (3)

Feature	PTT Standard	PTT Radio	Feature Phone PTT Standard	Feature Phone PTT Radio
Group avatars	User-assigned	CAT-assigned	User-assigned	CAT-assigned
Emergency¹				
Emergency Call and Alert	✓	✓	✓	✓
Initiate Remote Emergency Call as Authorized User	CAT-assigned	CAT-assigned	✗	✗
Remote Supervision as Authorized User	CAT-assigned	CAT-assigned	✗	✗
Emergency Call Initiation from Remote User	✓	✓	✓	✓
User Check¹				
Initiate Remote User Check as Authorized User	✗	CAT-assigned	✗	✗
Report User Check as Target User	✗	✓	✗	✓
Ambient Listening¹				
Remote Initiate Ambient Listening as Authorized User	✗	CAT-assigned	✗	✗
Self-Initiate Ambient Listening	✗	CAT-assigned	✗	CAT-assigned
Ambient Listening as Target User	✗	✓	✗	✓
Discreet Listening¹				
Remote Initiate Discreet Listening as Authorized User	✗	CAT-assigned	✗	✗
Discreet Listening as Target User	✓	✓	✓	✓
Enable or Disable PTT Service¹				
Remote Enable/Disable PTT Service as Authorized User	✗	CAT-assigned	✗	✗
Enable/Disable PTT Service as Target User	✓	✓	✓	✓
Messaging				
Integrated Secure Messaging	✓	✓	✓	✓
Text Messaging	✓	✓	✓	✓

Feature	PTT Standard	PTT Radio	Feature Phone PTT Standard	Feature Phone PTT Radio
Image Messaging	✓	✓	✓	✓
Video Messaging	✓	✓	✓	✓
Voice Messaging	✓	✓	✓	✓
PTT Voice Message Fallback	✓	✓	✓	✓
Document Messaging	✓	✓	Yes, device-dependent for rendering	Yes, device-dependent for rendering
Location Messaging	✓	✓	✓	✓
Broadcast Text Messaging	✓	✓	✓	✓
Operational Status Messaging ²	✗	✓	✗	✓
Presence				
Contact	✓	✓	✓	✓
Self-availability	Available/DND/Offline/No Connection	Online/Offline/No Connection	Available/DND/Offline/No Connection	Online/Offline/No Connection
Location				
Area-based Talk-groups ¹	100	100	100	100
Location Reporting	✓	✓	✓	✓
Location Tracking as Supervisor	✓	✓	✗	✗
PTT App				
Call from Lock Screen (One-Touch Calling)	✓	✓	✓	✓
Client upgrade notification (LCMS)	✓	✓	✓	✓
Incoming call priority	✓	✓	✓	✓
Manual dialing	✓	✗	✓	✓
One Touch Calling	(device-dependent)	(device-dependent)	(device-dependent)	(device-dependent)
Online or Integrated Tutorial	Online	Online	✓	✓
PTT accessory support	✓	✓	✓	✓
PTT History	✓	✓	✓	✓

Feature	PTT Standard	PTT Radio	Feature Phone PTT Standard	Feature Phone PTT Radio
Silent Mode Behavior (Privacy Mode)	✓	✓	✓	✓
Speed Dial	✗	✗	(device-dependent)	(device-dependent)

¹ Command tiered-feature set.

² MCPTT tiered-feature set.

9.1

PTT Standard Application Mode

The types of PTT applications supported are as follows:

- Feature phone - Motorola Solutions provides the application that is incorporated into an Android Open Source Program (AOSP) based feature phone device. These devices use the Android OS, but is not Google Mobile Services certified. The physical form factor is either a candy bar or flip phone with small touch or nontouch display, numeric keypad, soft keys, and navigation key. The application is upgraded using firmware updates.
- Downloadable PTT application on open OS platforms including Android and iOS - Motorola Solutions provides these PTT applications. Android PTT applications can be fully certified on a particular model or released as a "best effort" PTT application. Noncertified Android PTT applications provide advanced user settings to support application compatibility related to audio and wired PTT accessories.

The PTT application user interface must support a minimum of English with other translations provided by the customer. The PTT application uses the default language as set elsewhere in the device including right-to-left language support. The PTT application displays the user interface in English if the PTT application is not compatible with the user-selected language.

Motorola Solutions provides a document to customers and OEMs describing the required functionality to be supported in a device.

9.2

PTT Radio Application Mode

The PTT Radio Application Mode provides a simplified user interface that mirrors the experience of a Land Mobile Radio (LMR) user. The PTT Radio mode supports the Android smartphone, iPhone, Android tablet, and iPad tablet. Supported user types include Handset PTT Radio, Cross-carrier PTT Radio, and Wi-Fi PTT Radio. Main features include:

- Support for up to 96 administrator-managed talkgroups
- Support for administrator-managed contacts
- Support for 1:1 private contact creation
- CAT configuration for talkgroups, contacts, scan list, zones
- Supervisory override
- Location reporting
- PTT accessory support
- Wi-Fi support
- 1:1 private calling

- Talkgroup calling
- Quick Group calling
- Quick Group calling from a map for supervisors with location capability enabled
- Instant Personal Alerts
- Secure messaging
- Call history
- Mapping
- Emergency alerts and calling
- User check and monitor
- Ambient and Discreet listening
- Area-based talkgroups
- Manual Answer (Hook signaling) for 1:1 PTT
- Calls with External Telephony Users
- User Profiles
- User Role-Based Login

The PTT Radio supports two modes of operation:

- Talkgroup select
The user chooses one talkgroup to monitor. Calls from the selected administrator-managed talkgroup are received. Calls from user-managed talkgroups are not received. Talkgroup members automatically join a talkgroup that is in progress. Private, Quick Group, Broadcast, and Emergency calls are also received.
- Priority talkgroup scanning
All talkgroups assigned to the scan list is monitored for activity, and calls are heard based on talkgroup priority. The administrator assigns Talkgroup priorities. If your phone has a PTT side key or PTT accessory, while scanning, a PTT side key, or PTT accessory key allows you to talk on the currently active call or the selected talkgroup, depending on application setting. Talkgroups in the scan list can be assigned from any groups assigned to channels in any zone.

The CAT controls which users have priority scanning.

9.2.1

Talkgroup Scanning

The CAT assigns talkgroups in the scan list.

9.2.2

Missed Call Alerts

Missed Call Alerts are supported in Release 9.1.1 and above for any incoming private calls that are missed by user.

9.2.3

Scan List Administration

An administrator administers scan lists through the Central Admin Tool (CAT). The administrator enables or disables the feature for a user, and assigns talkgroups to the scan list and priorities to the talkgroups. Talkgroups in the scan list can be assigned from any of the groups assigned to channels in any zone.

9.2.4

Configuration

System-wide configuration controls the Talkgroup Scanning feature and a maximum number of priority groups. For more information, see [Talkgroup Scanning on page 52](#). The PTT Radio scan list size is configurable system-wide from 1-16 (default = 8).

The PTT Radio scan mode is CAT controlled.

The number of channels allowed per zone is configurable system-wide from 6-96 (default is 16). The number of Zones is determined based on the number of channels configured per zone. If there are sixteen default channels configuration, the number of zones is six.

9.2.5

Hook Signaling

PTT Radio supports private 1:1 PTT call answer modes as follows:

- Automatic call answer - existing functionality
- Manual call answer
 - User device rings when an incoming private call
 - User “accept” or “reject” a call
 - Call answer using soft UI button or PTT key on the phone
 - Half-duplex call or full-duplex call
 - Call timeout - 15 sec default (5-60 sec configurable system-wide)



NOTE: Emergency private call follows the automatic call answer.

Hook Signaling - User Experience

The following is the hook signaling user experience:

- An originating user initiates the call using a PTT button or UI.
- Originating user does not take the PTT floor and starts ringing.

- Terminator user device rings.
- Terminating accepts incoming call while ringing.
- The originator takes the PTT floor if the floor is idle.
- Call times out based on manual commencement mode (15 sec default).
- Originating or terminating user may end the call.

Backward compatibility

Hook signaling backward compatibility is as follows:

- R9.0/R9.1 PTT application supports automatic call answer
- R10.0 PTT application supports automatic and manual call answer



NOTE: PTT Standard mode does not support hook signaling.

Supported PTT user types

The supported PTT user types are as follows:

- PTT Radio mode of application
- Web Dispatch
- Third-party dispatcher using MCPTT UNI interface

9.2.6

Background Call Mode

For more information on Background Call Mode, see the [PTT Services on page 25](#).

9.2.7

User Type

The Administrator can switch the user type between PTT Radio and Standard modes.

9.2.8

User Provisioning

The Broadband PTT user provisioning interface supports the following types of PTT Radio applications:

- Handset PTT Radio
- Cross-Carrier PTT Radio
- Tablet/Wi-Fi-only PTT Radio

The Motorola Solutions License Packs interface supports provisioning the following PTT applications:

- PTT Radio Tablet/Wi-Fi-only
- PTT Radio Cross Carrier Handset

For the complete talkgroup scanning description, see [Talkgroup Scanning on page 52](#).

9.2.9

Zones

The Administrator assigns talkgroups to zones for a PTT Radio user type.

A zone is used to categorize channels into logical groupings. Each talkgroup can be assigned to a single channel within a zone. Each talkgroup can be assigned to multiple channels as long as the talkgroup is assigned to only one channel within each zone. Each channel a talkgroup is assigned uses one of the 96 total channels allowed. If a talkgroup is assigned to a channel in three zones, three of the 96 channels are considered "in-use." The number of channels allowed per zone is configurable. See [Configuration on page 93](#) for more information.

9.3

PTT Application Upgrade Notification

The PTT Application Upgrade Notification solution provides a facility to indicate that application upgrades are available. It also provides the ability to indicate that device support is ending so that older devices can be removed from the system. These notifications can be blocking (causing the PTT application to go offline) or nonblocking (user can dismiss the notification and continue using the PTT application).

The PTT Application Upgrade Notification solution provides the following:

- PTT Application version upgrade – notify that update is available or mandatory
- Device support – notify the user that support for a mobile device is ending or has ended
- OS support – notify the user that support for a dispatch OS is ending or has ended

Two types of notifications are supported:

- Informational – can be dismissed and continue using the PTT application; the user can opt out of further notifications unless prohibited by configuration
- Deny – the user is logged out of the service and cannot continue to use PTT

The following user types support PTT application upgrade notification:

- Handset
- Tablet/Wi-Fi-only
- Dispatch (Desktop dispatch only)
- Cross-Carrier
- Interop

The following user types do not support the PTT application upgrade notification:

- Integrated Mobile APIs
- Integrated Tracking APIs
- Integrated Web APIs using a browser plug-in

A Life-Cycle Management Server facilitates life-cycle management (LCMS), managed by the Operations Teams. The LCMS can be deployed on a stand-alone server or use dedicated or shared hardware with other servers.

A facility for PTT applications to notify users with the server configured message:

- Notification is shown at each login or every 24 hours (configurable 1 hour to 30 days) and is available within the application settings
- Message up to 250 bytes with multilanguage support

- Notifications can be targeted to specific device models and PTT application versions using the User Agent information
- Notification actions:
- Upgrade option allows the user to upgrade from Play Store/App Store for mobile clients or another server for Desktop dispatch.
- More Info option opens a browser to configured URL.

Supported by 8.0.3 PTT applications and later:

- Legacy PTT applications can use the Client Access Control List to deny service
- Legacy PTT application version upgrade must be managed manually by the customer – Motorola Solutions can provide reports on request

9.4

Cross-Carrier

Cross-Carrier is a feature available to corporations with access to the Central Admin Tool (CAT). The feature provides Push-to-Talk (PTT) service to a user on another carrier through the data plan and Internet data connection available on the device. Cross-Carrier PTT enables selling PTT to enterprises with multiple carriers providing wireless service. Cross-carrier users download and install the same application as on-carrier users. The data used by PTT is charged against the user's data plan by the agreement with their carrier.

Cross-carrier subscribers are provisioned in the system and assigned a Pseudo Number as their PTT ID. The corporate or agency administrator assigns a user ID in the form of an email address and generates a temporary password used to login along with the user ID.

The application recognizes that it is running on an off-network device by reading the Home MCC/MNC from the device and comparing it to a built-in list. If the home MCC/MNC is not found in the list, the device is considered off-network. If the home MCC/MNC is not found in the PTT application's built-in list, the PTT application queries the server with MCC/MNC to determine on/off network status. The Operations team configures the MCC/MNC list on the server.

iOS applications are not allowed to read the Home MCC/MNC so the application will prompt the user during activation to choose if the device is on-carrier or off-carrier. The application first attempts to send an SMS activation and then prompts the user if the activation attempt is unsuccessful.

Service is "best effort" using the data plan and data connection available to the user. The application uses TCP/IP to maintain a connection to the PTT server. The application learns and adapts to the serving network NAT timer. The application also uses UDP/DTLS as needed, for example, during PTT calls.

Feature Applicability

Cross-carrier applies to Android PTT applications. With release 9.1 and above, the cross-carrier license type is not applicable with device sharing enabled and are converted to User license type.

9.5

Dispatch

Dispatch is a feature-rich browser-based application that enables organizations to manage daily dispatch operations effectively. It allows dispatchers to manage the activities for a set of mobile PTT users (also called fleet members) working in the field.

Dispatch enables an organization to manage the day-to-day dispatch operations and rapidly respond to incidents, urgent situations, customer requests, facility events, and other situations that require quick actions. Dispatch provides PTT calling, location, emergency calling, alerts, and indicates presence through an intuitive

user interface. Multiple dispatchers on the same talkgroup call allow dispatchers to work in shifts, train a trainee, and other situations, which need collaboration between dispatchers on a talkgroup call. Dispatch allows the creation of web dispatch accounts, migration of web dispatch, resetting the password and resend of the activation link.

For more information, see the "Dispatch Product Specification."

9.6

PTT Accessory Support

PTT applications support the following types of accessories:

- **Remote Speaker Microphone (RSM)**
A remote speaker microphone (RSM) is an accessory with a loudspeaker and a built-in PTT button that lets the user remotely control the phone's PTT application. Two types of RSM connections are supported: those that connect by wire to the phone's USB-C connector and those that use Bluetooth.

While a remote speaker microphone is connected to the phone, cellular calls can be heard, but the PTT button cannot be used for call control.

- **Surveillance Kit with PTT Button**
A surveillance kit is an accessory that provides an in-ear earpiece, a microphone, and a PTT button. The surveillance kit provides the user the ability for discreet PTT communication. Two types of surveillance kit connections are supported: those that connect by wire to the phone's USB-C connector and those that use Bluetooth.

While a surveillance kit is connected to the phone, cellular calls can be heard, but the PTT button cannot be used for cellular call control.

- **Bluetooth Low Energy PTT Button**
Bluetooth Low Energy (BTLE), also known as Bluetooth Smart, is part of the Bluetooth 4.0 specification and enables ultra-low power consumption data-only accessories. The PTT application provides support for BTLE PTT buttons.

The accessories available vary by phone model and operating system. See your account manager for a detailed list of accessories supported for each phone model.

In addition to PTT accessories, the PTT application supports regular wired headsets and Bluetooth headsets that support the Hands-free Profile (HFP). There is also limited support for car audio systems supporting the Hands-free Profile.

9.7

Cellular Network Transitions

The PTT application uses the standard cellular network and data session management procedures of the device. The PTT application registers with the PoC server when the network transition causes any of the following:

- MCC/MNC change
- Data session re-establishment

The registration request to the PoC Server includes the MCC/MNC. The server makes the roaming determination based on location info (MCC/MNC) for the user and communicates the roaming privileges to the PTT application.

Existing calls are dropped on reregistration.



NOTE: iOS devices do not support detection of MCC/MNC change.

Restriction of PTT Service Operation to 4G

This feature prevents the utilization of 2G and 3G capability so that users have a guarantee of critical service availability (system-wide configuration). When the feature is turned on, and the PTT application detects 2G/3G, the application displays, "No Connection" message. When 4G is detected, the PTT service is restored. If Wi-Fi setting is turned on and you are connected to a network, the application resumes PTT service (system-wide configuration).

9.8

IPv4 and IPv6 Fallback Support

Typically, cellular networks are configured to support either IPv4 or IPv6 or both. Fallback between IPv6 and IPv4 transports is supported on cellular and Wi-Fi networks based on IP address availability. IPv6 or IPv4 can be configured as preferred (IPv4 default). Preference applies when a device receives both an IPv4 and IPv6 address. IPv4 Fallback provides a seamless transition between LTE and 3G networks by switching between IPv6 on LTE and IPv4 on 3G when 3G does not support IPv6.

IPv4 Fallback is provided on all supported Android and iOS devices, including tablets.

9.9

Backward Compatibility

PTT applications older than Release 12.1 do not support regroup service. The use of regrouping service on constituent groups with affiliated members using older PTT applications will cause a service outage for those PTT users with the older PTT application version.

Chapter 10

Administration

The following sections describe the administrative functionality available for the Broadband PTT:

- [Central Admin Tool on page 99](#)
- [Permissions on page 103](#)
- [Contact and Talkgroup Management on page 103](#)
- [User Profiles on page 104](#)
- [Corporate-Level Configuration on page 107](#)
- [Restore Contacts and Talkgroups on page 107](#)
- [Display Name and Customization of Contact Names on page 107](#)
- [Auto-Pairing on page 108](#)

10.1

Central Admin Tool

The Central Admin Tool (CAT) allows administrators to manage the user's profile, contacts, talkgroups, and features. When the administrator makes any changes, they are automatically pushed to the device near real time.

The navigation menu segregates the PTT Users, Talkgroups, User Profiles, External Users, Integrated Users, Interop Connections, and User Sets for easy management.

10.1.1

Access Control

Log In

To access CAT, there are two options available as follows:

- **Single Sign-On (SSO)** – The customer's SSO system provides access to the CAT portal. Creation and authentication of Administrators is done as part of the customer's SSO system and not done by CAT. When the Administrator makes any changes, they are automatically pushed to the device near real time.
- **Login ID (email address) and password** provided by Motorola Solutions Unified Communications Operations.

Multifactor Authentication (MFA)



NOTE: First-time log in requires account activation. The CAT provides multifactor authentication (MFA).

User must install the MFA mobile application. Motorola Solutions has certified the use of the Google Authenticator. The application can be downloaded from the application store on a mobile device.

If the administrator enables the MFA, each log-in requires two-factor authentication. To access the application, after entering credentials user must enter the one-time password from the mobile app.

The dispatcher can reset or change the password from the sign-in page or the **Settings** in the Dispatch respectively.

Password Management

Password management allows you to change or reset the password of your application account.



NOTE: These system-wide settings may change based on your service provider configuration.

The system default configuration is set as follows:

1. Password expires every 90 days.
2. Password history cannot be the same as any of the last five passwords used.
3. Password cannot be same as your username.

Resetting Password

User can reset password from the login screen or call Motorola Solutions Unified Communications Operations to reset the password. The password must meet the minimum requirements of the password policy of the application as follows:

- At least 16 characters
- One lower case letter [a to z]
- One upper case letter [A to Z]
- One number between [0 to 9]
- One of these special characters: @#%&+=



NOTE: These system-wide settings may change based on your service provider configuration.

An error message displays if the entered password does not match the minimum requirements of the password policy.

10.1.2

PTT Users

The PTT Users are the Handset, Wi-Fi, Cross-Carrier and Dispatch types of subscribers. This menu allows an Administrator to manage subscriber profile information such as name, permissions, activation code, and others along with contacts and talkgroups. Additional features that can be configured are emergency setting, authorization during an emergency, integrated secure messaging capabilities, and call permissions.

Administrator-Managed Contacts

Administrator assigns and manages contacts for each user. Administrator-managed contacts can contain a combination of individual contacts and user sets.

Administrator-Managed Talkgroups

Administrator assigns and manages talkgroups for each user. These talkgroups are assigned using the Talkgroups menu. For a PTT Radio mode, the zone, channel, and scan list assignment can be performed.

Administrator-Managed Features

The Administrator can view and control some of the features assigned to a PTT User such as Feature Sets, Device Information, Messaging, Automatic Location Publish Control, and Emergency.

10.1.3

Talkgroups

The Administrator assigns and manages talkgroups for each user. A talkgroup can contain a combination of individual contacts (Talkgroup members) and user sets. The talkgroup, along with the talkgroup members are pushed to the PTT application for all talkgroup members except external users. Three types of talkgroups can be created: Standard, Dispatch, and Broadcast. The administrator can create pre-configured groups to which no users are assigned using CAT, but users can dynamically add users to create groups thereby supporting the group-regroup functionality.

Changes to a talkgroup can be made by adding, deleting, or updating the associated user set or individual contact. Any changes to the talkgroup are propagated to all administrator-managed users that have the talkgroup. The deletion of an administrator-managed user deletes the user from all the talkgroups in which they are a member. The Talkgroups menu contains details, such as Talkgroup Name, Talkgroup Type, Avatar (applicable for PTT Radio Users Type only), Members, Supervisors, Broadcasters, and Dispatchers. Talkgroup name is unique within the corporation.

Administrator-Managed Talkgroup Members

The Administrator can assign one or more members to a talkgroup. The members of the talkgroups can be given specific calling permissions such as In Call Floor Control, Call Initiation, Call Receiving). See [Call Permissions on page 101](#) for more information.

Administrator-Managed Talkgroup Supervisors

The Administrator can assign one or more supervisors to a talkgroup. Supervisors obtain talker priority in the group and can preempt other users or supervisors. Supervisors do not preempt dispatchers and broadcasters. Additionally, supervisors can have location capabilities which allow them to track members of the group on a map and put Geofence around them.

Call Permissions

Three types of call permissions can be assigned to each user at the talkgroup member level. These call permissions are as follows:

- In Call — In call permission allows the user to take the floor during the call. When set to Listen Only, the user can hear the call but cannot participate in the call.
- Call Initiation — Call initiation permission allows the user to initiate the call to the group.
- Call Receiving — Call receiving permission allows the user to receive the group call whenever it starts.

The following table lists the Call Permissions types and definitions.

Table 22: Call Permissions Types and Definitions

Function	Permission	Description
In Call	Listen and Talk	While In call permission is set to Listen and Talk, PTT user is allowed to listen to the PTT call as well as allowed to transmit/talk to the active PTT call. Listen and Talk is default permission for all the talkgroup members.
	Listen Only	While In call permission is set to Listen only, PTT user is allowed to listen to the PTT call but NOT allowed to transmit/talk on the active PTT call.
Call Initiation	Allow	When set to Allow, PTT user is allowed to initiate new PTT call to the talkgroup. PTT user is also allowed to rejoin for the session that is missed due to network issues, busy on another call, and others, reasons. Allow is default permission for all talkgroup members.

Function	Permission	Description
	Do not Allow	When set to Do not Allow, PTT user is NOT allowed to initiate new PTT call or rejoin existing active PTT call.
Call Receiving	Allow	When set to Allow, PTT user is configured to receive all the calls on the predefined talkgroup that user is a member. PTT user is paged for all the calls that are initiated on the talkgroup by other members. There would be no retry for paging if the user missed the call for any reason. Allow is default permission to all the talkgroup members.
	Do not Allow	When set to Do not Allow, PTT user is NOT allowed to receive any incoming PTT call. PTT user is not paged for any calls that are initiated on that talkgroup by other members.

Other than the standard groups, the Central Admin Tool allows you to manage two other types of talkgroups, Dispatch Groups and Broadcast Groups. For more information on Dispatch Groups refer to [Dispatch on page 96](#) and for Broadcast Groups, refer to [Broadcast Calling and Messaging on page 39](#) within this document.

10.1.4

External Users

External users are vendors or partners of the corporation which also use the same PTT service but are provisioned as personal users or users from a different corporation.

The administrator needs to know the PTT Phone Number of the user to add as an external user. A user with permissions set as “Administrator” in their corporation is not allowed to be added as an external user in another corporation. The administrator can assign an external user as a contact to the users of their corporation, but cannot push contacts and talkgroups to the external user. In other words, the external user’s device cannot be managed by an administrator from a corporation other than their own. The location of the external users is also not published for use by other corporations. The External Users menu contains the details, such as Name and Phone Number. External users can be imported in bulk to the system using a CSV file.



NOTE: Do not import any file name with special characters such as (=, ', ", /, -, +, @) in the Excel file. Commas (,) and pipe (|) characters must not be used at the beginning of any name.

10.1.5

Integrated Users

Integrated Users are the third-party applications such as workforce management which are developed using PTT communication platform. The Administrators can manage individual Integrated user profile information such as name, permissions activation code, as well as assign contacts and talkgroups.

10.1.6

Interop Connections

Interop Connections are used for communication between PTT and LMR systems.

The **Interop Connections** menu includes the Interop Talkgroup and Interop User details. For more details on each type of users, refer to *Interoperation Gateway Product Specification*.

10.1.7

User Sets

A user set is a logical set of users where the list of members is optionally assigned as contacts with the others.

User sets are a fast way to program multiple devices easily. The CAT supports management (create, assign, edit, delete, and view) of user sets. Additionally, a User Set can be assigned to a subscriber or added as a member of a group. User Set also allows creation of a common contact list which is common to all profiles, each user can be assigned to a single common contact list.

A user can be a member of multiple sets. Any changes to a user set, that is, additions, deletions, or updates are propagated to all users or groups that have the user set.

Deletion of a member from a user set deletes that member from the user sets, contact lists, and groups of all associated users.

The Administrator can see all the user sets and individual contacts per user. The Administrator can also see all user sets, talkgroups, and contacts a user is a member.

10.2

Permissions

Broadband PTT supports the following user permissions:

- Administrator: Contacts and talkgroups of users with these permissions are managed only by the administrator. The user does not have any control over the contacts and talkgroups.
- Administrator and User: Additional to the administrator assigned contacts and talkgroups, users with these permissions can add their contacts and talkgroups which are not managed by the administrator.

Permission Management

The CAT allows the Administrator to change permissions between "Administrator" and "Administrator and User" and vice versa at the individual user level. If a user is changed from "Administrator and User" to the "Administrator" permission, all personal talkgroups and contacts for that user are deleted from the platform.

10.3

Contact and Talkgroup Management

10.3.1

Addressing

A PoC Mobile user is identified by a TEL URI, for example, <tel:+19726653400>. A PoC talkgroup is identified by a SIP URI, for example, <tel:+19726653400; org.openmobilealliance.groups =Maintenance>. Subscriber addressing is not visible to users and is used internally within the solution.

10.3.2

Dial Plans

National Dial Plan Format

National Dial Plan format (in US: NPA-NXX-XXXX, for example, 416-665-0200)

National Dial Prefix + National Dial Plan Format (in US: National Dial Prefix + NPA-NXX-XXXX, for example, 1-416-665-0200)

International Dial Plan Format

“+” + Country Code + International number, for example, +914166650200

10.3.3

Contact and Talkgroup Sizes

The following table shows the maximum configurable limits for the CAT. These parameters are system-wide and configurable.

Table 23: User-Level Contact Sizes

Contacts	Min	Max
Administrator-Managed User	0	1000
Personal User	0	300

The following table lists the corporate-level contact and talkgroup sizes:

Table 24: Corporate-Level Contact and Talkgroup Sizes

	Max Users	Max Talkgroups	Max External Users	Max User Sets
Corporate Level	40,000	10000 ¹ (non-dispatch) /10000 (dispatch)	1000	1000

¹ Corporate level talkgroups support up to 10000 (Standard + Broadcast) Groups and 10000 Dispatch Groups.



NOTE:

Large talkgroups up to 3000 members are available upon customer request.

For more information on the Central Admin Tool, refer to the *Central Admin Tool User Guide*.

10.3.4

Contact and Talkgroup Name Length

The maximum length of contact and talkgroup names is 30 alphanumeric characters. Display of the name on the device is dependent type of device and resolution of the screen, etc.


10.4

User Profiles

A user profile is a template for configuring or updating users in large batches. The number of user profiles allowed to be assigned to the user is 20 (configurable; 80 maximum) supported by the system-wide configuration with average of 20 user profiles per user.

For users without user role-based login, the user is assigned a single default profile used for the user during the login. Users with a role based login feature (see [User Role-Based Login on page 106](#)) can select the profile during the login to PTT application.

A user profile is a template for configuring or updating users in large batches (the same as a talkgroup profile).

 **NOTE:** User Profile Management only supports PTT Radio Mode.

A user profile consists of the following attributes:

- **User Profile or Role Name**—Name can be up to 100 alpha-numeric characters. A user can be assigned more than one role, but only a single role is active at a time.
- **Features Configuration**—Same as current Features tab in CAT.
- **User Sets (No Auto-pairing)**—New functionality to have User Sets without auto-pairing.
- **Groups**—List of talkgroups.
- **Group Permissions**—each talkgroup in the user profile can have following permissions:
 - Transmit/Receive/In-Call permissions
 - Scanning priority
 - Zone/Position
 - Location capabilities permissions
 - Geofence permissions
 - Dispatcher - The user of this profile is assigned to is a dispatcher in this talkgroup
 - Broadcaster - The user of this profile is assigned is a broadcaster on this talkgroup

10.4.1

Talkgroup

A talkgroup consists of the following attributes:


- **Talkgroup Type**—Broadcast, Dispatch, or Standard.
- **Avatar**—Selection from a list of Avatars.
- **OSM List**—List Name.
- **Talkgroup Members**—There are no actual talkgroup members added to the talkgroup directly. This information is derived from the relationship of Talkgroups to User Profiles to User
- **Dispatchers**—There are no actual dispatchers added to the talkgroup directly. This information is derived from the relationship of Talkgroups to User Profiles to User.
- **Broadcasters**—There are no actual broadcasters added to the talkgroup directly. This information is derived from the relationship of Talkgroups to User Profiles to User.

10.4.2

Talkgroup Profile

A talkgroup profile is essentially a template to create multiple talkgroups in bulk with the same attributes.

It has the same attributes as a talkgroup except that modification of the talkgroup profile propagates to all the talkgroups created using the Talkgroup Profile. Talkgroup profile can be use to create standard, broadcast, and dispatch talkgroups.

 **NOTE:** Talkgroup profile does not support dispatch talkgroups.

10.4.3

Talkgroup and User Profile Sharing

Public safety agencies are provisioned as an individual entity corporation.

Each agency is autonomous where there can be one or more local administrators who manage the users, user profiles, talkgroup profiles, and talkgroups locally for the day to day activities.

Higher-level agencies may manage specific user-profiles and talkgroups to maintain control and lower-level agencies only manage users that higher-level agencies created and shared to lower-level agencies. Lower-level agencies assign their shared talkgroups to locally managed user profiles or assign shared user profiles to their local users.

Command line tool at the operator level supports Trust Relationship Matrix to build hierarchy across higher and lower level agencies. Talkgroups are shared only based on prebuilt trust relationships (one way).

Prebuilt Trust Relationship Matrix

The matrix is preloaded in the system as a part of the CLI tool. A new entry can be added to the matrix, or existing entry can be removed from the matrix. When an existing entry is removed, existing talkgroups sharing is not removed - new talkgroup or user profile sharing is restricted. Each trust relation is one way to build two-way sharing - two independent entries to the matrix required.

Talkgroup Sharing

Based on the Trust relationship Matrix a talkgroup can be shared with other agencies.

New Talkgroup profile attribute allows talkgroups to be shared across a list of agencies (based on the trust relationship matrix) when enabled. When sharing is enabled for a talkgroup, it shows the drop-down list of agencies. CAT administrator selects one or more or all agencies that talkgroup is shared with. Once a talkgroup is shared with other agencies, a talkgroup is shown other agency CAT portal. Shared talkgroup ownership remains within the scope of the agency who has shared the talkgroup agency that is receiving shared talkgroup can not modify the shared talkgroup. All Services are shared across agencies, such as PTT calling, streaming video, OSM, Messaging Location, etc.

User Profile Sharing

Based on the Trust relationship Matrix a user profile can also be shared with other agencies.

New user profile attribute allows user profile to be shared across a list of agencies (based on the trust relationship matrix) when enabled. When sharing is enabled for a user profile, it shows the drop-down list of agencies. CAT administrator selects one or more or all agencies that the user profile is shared with. Once a user profile is shared with other agencies, a user profile is shown in other agency's CAT portal. Shared user profile ownership remains within the scope of the agency who has shared the user profile the agency that is receiving the shared profile can not modify the shared profile. All Services are shared across agencies, such as PTT calling, streaming video, OSM, Messaging Location, etc.

10.4.4

User Role-Based Login

When the user logs into the PTT application, they select a profile from the list authorized by the agency administrator for that user. An administrator assigns a default user profile, which shows up as selected on top of the list. All contacts or talkgroups are downloaded to the app based on the user profile. Only one profile is active at a time. All services are allowed to a user based on the user profile. Default selected talkgroup is the last selected talkgroup for that user profile.

When the user logs into the PTT application, they select a profile from the list authorized by the agency administrator for that user. An administrator assigns a default user profile, which shows up as selected on top of the list. All contacts or talkgroups are downloaded to the app based on the user profile. Only one profile is active at a time. All services are allowed to a user based on the user profile. Default selected talkgroup is the last selected talkgroup for that user profile.

Upon device power on/off the user automatically logs in to previously selected profile (when “Remember me” is selected) without asking the user to select a profile

User Profile Change

User profile change is always user-initiated and is available in the application settings menu. While the user is in an emergency, the change of user profile or role is restricted. MCPTT users are allowed to have more than one user profile assigned by the CAT administrator and can switch user profiles from the PTT application. Collaboration and Command users are restricted to only one user profile.

10.5

Corporate-Level Configuration

Broadband PTT provides the ability to configure certain options (for example, Presence Notification) on a per-corporation basis.

As users are provisioned within a corporation, the corporate features are applied to the user automatically. Changes to the corporate-level feature set are applied to newly-provisioned users and when a user is deleted and re-added. Corporate-level configuration is performed on an exception basis.

The corporate-level feature set is controlled by a command line interface (CLI) and is set by the Operations team.

10.6

Restore Contacts and Talkgroups

The capability to restore contacts and talkgroups to a device is useful if a user suddenly loses all contacts and talkgroups due to a device failure, a change in device, or a re-installation of the PTT application.

There are two methods for initiating restoration of contacts and groups. If the PoC server receives an activation message from a device PTT application as a result of SIM or device change, the PoC server initiates a synchronization process of all contacts and groups stored on the server. Secondly, a Customer Service Representative or Administrator can initiate a forced synchronization, usually as a result of a call for support from a user. In all cases, the PTT application pulls the data from the PoC server.

10.7

Display Name and Customization of Contact Names

Each user has a Network/Display Name that is set in the following decreasing order of priority:

1. Name provided when the user is provisioned.
2. Name as set by the administrator.
3. User's MSISDN

Based on the system-configuration, PTT users can be allowed or restricted to change their name on the application.

The following table shows what name is displayed for various scenarios. Two options are provided, option 2 is displayed if option 1 is not available.

Table 25: Display Scenario

Display scenario	Personal User	Administrator User	Administrator and User User	
			Personal Con- tacts	Corporate Con- tacts
Contacts	Local name	Network name	Local name	Network name
Group Member	Local name	Network name	Local name	Network name
Incoming call/ Talker ID	Local name	Network name	Local name	Network name
	Network Name		Network Name	
IPA notification	Local name	Network name	Local name	Network name
	Network Name		Network Name	

10.8

Auto-Pairing

This feature allows small corporations that do not have access to the CAT to have their administrator-managed contacts automatically distributed to all their users. Also, an all-member group is created that has all the administrator-managed contacts as members. As users are added to or removed from the corporation, the contacts and corporate all-member group are automatically maintained. The contacts and groups are maintained as corporate-type contacts and groups. For additional information on auto-pairing, see [Auto-Pairing on page 130](#).

Chapter 11

APIs

11.1

Converged Data APIs

- **UC Converged Data API** - Converged data API package supports 1:1 or group text messaging with multimedia attachments and provides situational awareness information with location, presence, and status events. Converged APIs are based on REST and WebSocket technologies. This API can be used to support the following PTT features:
 - Presence Query and Reporting
 - Location Query and Reporting
 - Location Triggers
 - Dynamic Data Group Management
 - Talkgroup-based Presence, Location
 - Operational Status Query & Reporting (Broadband only)
 - Affiliation State Query and Reporting
 - User, Device, Group Inventory
 - 1:1 and Group Text Message w/Attachments
 - 1:1 and Group Text Notifications
- **UC Messaging API** - Data API for third-party applications that only requires Messaging capabilities (1-1 or group messaging with multimedia attachments). The API also provides presence status for users. These APIs can be used to support the following PTT features:
 - 1:1 and Group Text Message w/Attachments
 - Presence Query and Reporting
- **UC Location API** -Data API for third-party applications that only requires location and presence information for situational awareness.
 - Presence Query and Reporting
 - Location Query and Reporting
 - Location Triggers

11.2

3GPP Mission Critical (MC) Standard APIs

3GPP Mission Critical (MC) APIs, also referred to as 3GPP Control Room Interface (CRI), which provides a unique opportunity for partners to develop applications such as Large Control Rooms, Dispatchers, or Gateways that can connect and interwork with a wide range of features and functionalities provided by Motorola's MCX Platform. Motorola's original 3GP MC APIs are based on 3GPP Release 15 specifications and after got updated for various features and capabilities from later 3GPP Standards 16 Specifications. The 3GPP Release-16 is the latest fully ratified Mission Critical Standards specifications.

First Responders in the Public Safety domain, such as police officers, firefighters, etc., handle incidents of mission-critical nature for which they need to communicate in dynamic groups spread across multiple

agencies. Such communications are coordinated and controlled by fixed users working in a control center called Control Room Interface or CRI (also known as "dispatchers" as per 3GPP standards). 3GPP MC APIs enable integration of large-scale 3rd Party Control Room Applications with the Motorola MCX Platform. Such an application can invoke privileged mode operations typically only available to Super Users such as Dispatchers/Control Rooms. CRI is powered with particular admin and call management privileges that normal UE devices used by the first responders do not have; for example, CRI can remotely cancel the Emergency Group Calls or change the UEs' location reporting interval criteria.

The 3GPP Standard interface can also be utilized by partners to develop interworking solutions with specific technologies such as TETRA/LMR technologies.

From the 3GPP point of view, CRI is just an extension of the User Equipment (UE) with additional permissions and authority. It must connect to the MCX server using the usual standard interface as used by any normal UE. CRI uses a wide range of systems and software infrastructure enabled with MCPTT, MCDATA, and MCVIDEO capabilities, resulting in many configurations used by public safety agencies. As an authorized user, a CRI can simultaneously communicate with multiple groups, create cross-agency groups, override a UE device if required, do ambient listening to users in danger, initiate emergency, broadcast, etc.

While control rooms could use all features and functionalities specified in the 3GPP specifications, some features or procedures may be more important and relevant from a control room perspective. All features require implementing specific 3GPP-defined procedures to support required features or functionalities. This section provides an overview list of such procedures.

Foundation Features or Procedures

All control rooms are required to implement all Foundation Features to connect and interwork with the MCX System:

- MCX & SIP Account Provisioning
- OIDC Authentication
- SIP Registration
- MCX Service Authorization
- User Profile/Group info retrieval
- Affiliation to Groups

Control Rooms implementing End-to-End Encryption are required to implement the following:


- Bootstrap Transport Key (Trk) Provisioning
- KMS Init and Provisioning procedures
- CSK Key upload/download procedures

Control Rooms can optionally Subscribe to User Profile changes to receive notification on the contact list or Group membership changes.

MCPTT Features or Procedures

The following is a list of common MCPTT procedures that may be implemented using 3GPP MC APIs:

- MCPTT Private Calling
 - 1-1 half-duplex call
 - Manual Commencement Mode (also know as Hook Signaling)
 - Automatic Commencement Mode
 - Talker identity
- MCPTT Group Calling
 - Automatic commencement

- Talker identity
- Normal and Emergency
- Floor priority or override
- Group call leave or rejoin
- Group Call late join
- Emergency Alerts or Call
 - Receive Emergency 1-1 Alert
 - Receive 1-1 Emergency Call in Automatic Commencement mode
 - Receive Group Emergency Alerts
 - Remote cancel 1-1 Emergency Alert and Emergency Call
 - Receive Group Emergency Calls in Automatic Commencement Mode
 - Remote Cancel Emergency Alert of a group Member or user
 - Remote downgrade Emergency Group Call
 - Multiple PTT user emergencies
 - Control room user overrides user in an emergency
 - Control Room users are allowed to do ambient listening to a user in an emergency state
 -  **NOTE:** CRI self-emergency mode set and CRI remote emergency mode set are not in scope.
 - Broadcast Group Call
 - Ambient Listening(AL)
 - MPTT user-initiated (Local AL)
 - Remotely initiated by control room (Remote AL)
 - Auto-reconnect for AL
 - Simultaneous Sessions
 - Call back alerts
 - Regroup user or group
 - First-to-Answer call
 - End-to-End encryption of User Plane

MCDATA Features or Procedures

The following is a list of common MCDATA procedures that may be implemented using 3GPP MC APIs:

- SDS over Control Plane
- SDS over User Plane
- Private and Group messaging
- Send or receive multimedia messages from the control room to PTT users
 - Text
 - Audio clip
 - Video clip
 - File document
 - Location coordinates

- Conversation/Threading
- Enhanced Status (Operational Status)
- ○ Receive Op status code message from PTT users
 - Download Op status codes from MC Server
- Delivery receipt for private messages
- Broadcast messaging - One-way text messaging
- MC Data Store support

MCVIDEO Features or Procedures

The following is a list of common MCVideo procedures that may be implemented using 3GPP MC APIs:

- One-to-one on-Demand MCV Call
- Group on-Demand MCV call
- One to one Video Pull
- Video-Codecs: H.264
- Leave and Rejoin the MCV call

Location Features or Procedures

The following is a list of common Location Monitoring procedures that may be implemented using 3GPP MC APIs:

- Location tracking (Aligned to 3GPP Stage-2 procedures)
- SUBSCRIBE/NOTIFY based
- Change of location reporting frequency for MCPTT user/group
- Time and Distance-based location updates

User Monitoring or Supervisory Features

The following is a list of common Location Monitoring procedures that may be implemented using 3GPP MC APIs:

- User monitoring/Supervisory Features
- Simultaneous audio sessions
- User Group affiliation (Large talk group membership – up to a maximum of 3000)
- Group affiliation or Real-time group attachment monitoring
- Remote Group Affiliation (ReGA)
 - Confirmed Remote Group Affiliation - Acknowledgment from Target Device client
 - Allow Remote Group Select to a group that does not belong to the target user's currently selected profile. The Group should be part of at least one of the Target User's Device profiles.

Group-Regroup Feature

- CRI Authorized user to initiate Group-regroup operation
- PTT, Messaging, and video services supported

Security & Encryption

3GPP MC APIs use the IMS User-to-network interface (also known as Gm interface), and Motorola supports all SIP signaling over TLS (V1.2) transport with Digest authentication. For all HTTP/XCAP-based interfaces, TLS V1.2 is used as well. All MCPTT User plane traffic is end-to-end Encrypted based on the 3GPP MIKEY-SAKKE standard as specified in 3GPP TS 33.180 3GPP R15.

For large-scale control Room systems, it is preferred to use VPN to transport all types of control plane and user plane traffic between the Control Room and Motorola MCX Server.

Media Codec

3GPP TS 26.179 defines codecs and media handling and has specified the use of AMR-WB with Bandwidth-Efficient mode as mandatory. Some MCPTT Clients may use the Voice Activity Detection (VAD) feature to optimize data usage on the RAN Network.

3GPP MC APIs

3GPP MC APIs are based on the following 3GPP Standard Specifications. See [References on page 21](#) for more details.

11.3

PTT Mobile APIs

11.3.1

Integrated Mobile APIs

The PTT-Integrated Mobile APIs allow mobile application partners to augment their services by adding core PTT functionality.

Mobile APIs are JavaScript-based. Voice communication is supported over WebRTC protocols. Signaling communication with PoC servers uses SIP and RTCP for session management and floor management, respectively.

Provisioning for the Integrated Mobile API user uses License Packs with a user type of Integrated Mobile.

Mobile APIs are supported for Android 5.0+ devices. The supported APIs are as follows:

Base API

The Base API is mandatory for integration to use core PTT functionalities:

- Login (includes authentication and login)
- Logout
- Subscription Change Notification
- Get Configuration
- Debug Logging (optional)
- Send IPA

Calling API

The Calling APIs are mandatory for integration to use core PTT functionalities:

- Originate/Receive 1:1 Call
- Originate/Receive Group Call

- Originate/Receive Quick Group Call
- Floor Control- Acquire, Release, Status Notification
- End Call
- Talker Identification
- Instant Personal Alert (IPA) Notification
- Missed Call Alert (MCA) Notification

11.3.2

PTT App-to-App and Accessory API

PTT App-to-App API allows third-party mobile applications to invoke Broadband PTT application contextually. PTT application is deployed on the mobile device, but the context is passed and invoked from a different application using these APIs. API supports PTT Voice and Messaging (Text only).

PTT Accessory API allows third-party PTT Accessory integration using Bluetooth and USB-C interfaces.

11.4

PTT Web Application APIs

11.4.1

Integrated Web APIs

The Integrated Web APIs allow web application partners to augment their service by adding various PTT services such as PTT calling, presence and location. Web APIs are available using a browser plug-in. The plug-in allows only one user session across different browsers or within the same browser across different windows. The following APIs are available:

Base APIs

The Base APIs are mandatory for integration to use core PTT functionalities.

- Login (includes authentication and login)
- Setup and Install plug-in
- Check and Get plug-in version
- Get self-username
- Set user-agent and client type
- Subscription Change Notification and Presence change notification
- Set Logging
- Logout

Calling APIs

The Calling APIs are mandatory for integration to use core PTT functionalities.

- Originate/Receive 1:1 Call
- Originate/Receive Group Call
- Originate/Receive Quick Group Call
- Call Status

- Floor Control – Acquire, Release, Status Notification
- End Call
- Talker Identification
- Instant Personal Alert (IPA) Notification
- Missed Call Alert (MCA) Notification

Alert API

The Alert API is optional for integration.

- Send Instant Personal Alert (IPA)

Presence APIs

The Presence APIs are optional for integration.

- Set self-presence to ON, OFF, or Do Not Disturb
- Receive self-presence status

Contacts Retrieval APIs

The contacts retrieval APIs are optional for integration.

- Request contact list
- Receive contacts and presence status

Group Retrieval APIs

The Group retrieval APIs are optional for integration.

- Request groups list
- Request group members
- Receive group list and members

11.4.2

Integrated Tracking APIs

The Integrated Tracking APIs enhances Motorola Solutions Web APIs to some of the features that are available on the Dispatch application. Partners can enhance their application for dispatch and LMR like call functions using Integrated Tracking APIs. Provisioning for the Integrated Tracking API user uses License Packs with an Integrated Tracking user type.

All API feature sets available for Integrated Web user are available for Integrated Tracking user as well. Also, the following feature sets are also available and are optional for integration:

Broadcast Calling APIs

- Initiate Broadcast call to Group
- Receive delivery receipt

If an application provider implements a set of any APIs, support for all the APIs within that feature set are mandatory. Notifications for optional feature sets must be handled gracefully by the APIs. For example, if the PTT server sends a location request notification and the partner application does not support location APIs, the API implementation must ensure proper response to the server.

11.4.3

Security and Encryption

Broadband PTT encrypts all communication between the PTT plug-in and PTT server. It ensures the privacy of all voice traffic and signaling information traveling between the plug-in and server. The encryption method used is the Advanced Encryption Standard (AES-256). The SHA-2 hashing algorithm signs all server certificates.

11.5

PTT-Integrated Authentication API

The PTT-Integrated Authentication APIs allow application partners to automatically assign user licenses, create activation codes, delete licenses, and update licenses.

The user logs into the PTT-integrated application using the partner application login mechanism. Using the PTT-Integrated Authentication APIs, the partner application can request the pseudo-number and activation code from the PTT server, which is used for logging in to the PTT server seamlessly.

Single Sign-On for PTT Service

The Single Sign-on for PTT Service is as follows:

1. Provisioning system enables a user service for the partner application server and PTT server.
2. Partner application server requests the license (username) and activation code (password) from the PTT server for single sign-on.
3. The PTT server provides license details (pseudo-number generated for license) and activation code for partner application.
4. The user downloads and installs the partner application.
5. The user logs into the partner application by following the partner application login procedures.
6. The user logs in seamlessly to the PTT server using PTT credentials (Pseudo-number and activation code).



NOTE: Partner application may implement login procedures depending upon the application requirement. Onboarding procedure provided above can be used as a reference.

Supported User Types

The PTT-Integrated Authentication API supports authentication for the following types of APIs:

- Integrated Mobile APIs
- Integrated Tracking APIs
- Integrated Web APIs

Supported APIs

The PTT-Integrated Authentication API supports the following features:

- Create – Assign a license to the user and generates an activation code
- Generate activation code – Generate activation code for the license
- Delete – Unassigns the license for the user
- Update user – Update user license – used for migration

Activation Code generated using APIs is unique system-wide and is 32 alphanumeric digits long. Each activation code generated has a validity period that can be retrieved using available APIs. Upon activation

code expiry, the partner application server can request a new activation code. Motorola Solutions recommends third-party application owners to store the activation codes locally on their application server once received using authentication APIs.

For information on the PTT-Integrated Authentication API, see the "ICD_REST_APIS-3rd_Party_Authentication."

11.6

Life-Cycle Management for APIs

11.6.1

Backward Compatibility

APIs are backward compatible with up to N-2 release, where N is current production release of PTT web plug-in.

Our Sandbox environment is available on N/N+1 release for partner integration depending upon schedule. Deprecation of any existing API is published using our API portal and release notes. It is the responsibility of the third-party application to integrate with new APIs promptly. We recommend upgrading to a newer version of the plug-in upon general availability.

3GPP APIs compatibility is based on 3GPP Release versions, and typically N-1 3GPP Release is supported, where N is the latest version of 3GPP Release incorporated into Kodiak Product.

11.6.2

End of Support (EOS)

End of Support plug-in version can be communicated to third-party application owner using email or our API portal.

For EOS Plug-In Version

- PTT service continues to be allowed by the server
- No new development or bug fixes can be planned on EOS plug-in version
- New server code base is tested for backward compatibility
- Third-party application is required to upgrade web plug-in or OS for support
- Web plug-in is not available for download or sideload

For End of Life (EOL)

- End of Life plug-in version is communicated to third-party application owner using email or our API portal.

For EOL Plug-In Version

- Server denies PTT service
- Web plug-in is not available for download or sideload

Chapter 12

Interoperability with Land Mobile Radio (LMR) Systems

12.1

Project 25 (P25) Inter-RF Subsystem Interface (ISSI)

Broadband PTT supports a secure and robust direct IP interface to Land Mobile Radio (LMR) systems using the Project 25 (P25) standards ISSI-based protocol. This interface enables direct communication between Broadband PTT users and P25 Interop Users. Features include:

- Talkgroup Call
- Talker ID
- Call Alert
- Broadband to LMR Interop Patch

For detailed information about Motorola Solutions' ISSI, see the "Interoperation Gateway Product Specification."

12.2

Radio over IP (RoIP)

Broadband PTT supports the use of Radio over Internet Protocol (RoIP) gateways to send and receive digital voice streams to and from the donor radio. This interface provides connectivity between the Broadband PTT users and LMR talkgroups using RoIP gateway.

Supported features include:

- Talkgroup Call
- Broadband to LMR Interop Patch

For detailed information about the RoIP feature, see the "Interoperation Gateway Product Specification."

12.3

Critical Connect Interoperability (Optional)

As optional capability, Critical Connect provides interoperable communication between users on LMR networks and those on Motorola Solutions' Broadband PTT.

Critical Connect is a subscription-based interoperability-as-a-service solution that delivers simple, flexible, scalable interoperable PTT communications between multiple LMR networks as well as LMR and LTE networks to create one unified system. With one link to Critical Connect, agencies can connect with other agencies' LMR systems, as well as personnel outside of LMR coverage, expanding their radio talkgroups to incorporate LTE devices while maintaining aliases and emergency protocol of the LMR system.

12.3.1

LMR Interoperability based on Feature Set

The following table lists the LMR Interoperability for each subscribed feature set.



NOTE: PTT users are required to have an LMR Interop subscription to be able to Interop with any LMR technology.

Table 26: LMR Interoperability by Feature Set

PTT User Type Subscription	Collaboration	Business Con- nect	Command
BB to RoIP	✓	✓	✓
BB to P25 (ISSI/CSSI)	✓	✓	✓
Wireline BB to MOTOTRBO	✗	✓	✓
Wireline BB to ASTRO 25	✗	✗	✓
Wireline BB to DIMETRA	✗	✗	✓

PTT Pkg configuration for a list of LMR technologies accessible for the PTT user that is, PTT user can Interop.

Chapter 13

Subscriber Life-Cycle Management

Each 'Administrator' or 'Administrator and Personal User' subscriber is associated with a Corporate ID. The Administrator profile is automatically created when the first user is provisioned with that Corporate ID.

Each Personal user is associated with an Account ID. The account profile is automatically created when the first user is provisioned with that Account ID.

13.1

Subscriber Types

Broadband PTT supports the following types of subscribers:

- Personal User: These subscribers manage their own PTT contacts and groups.
- Administrator User: These subscribers only receive contacts and groups from an Administrator.
- Administrator and Personal User: These subscribers receive contacts and groups from an administrator and can define and manage their contacts and groups when configured.

13.1.1

Personal User

Contact and talkgroup management is performed from the PTT application, which includes the create, update, delete, and view functions.

User-Managed Contacts

A Personal User can add to their PoC contact list any phone number as defined by the dial plans. No validation is done to check to see if the phone number is a valid PoC phone number. Calls fail if the number is not a valid PoC subscriber to the user or if it is a Corporate PoC subscriber to the user.

The user can add contacts to the PoC contact list from the built-in phone book, or the user can manually enter a phone number into the PoC contact list.

Deletion of a user removes them from the platform. Deletion does not remove them from other subscribers to the user that may have them as a contact or talkgroup member.

User-Managed Talkgroups

Groups are created on the PTT application by selecting members from PoC contacts. The talkgroup along with talkgroup members is accessible on the PTT application. The recipient of the call can initiate the call to the group from the history.

13.1.2

Administrator-Managed

The user provisioned with Administrator permissions has their contacts and talkgroups managed by the Administrator. The user cannot add a contact, talkgroup, or talkgroup member on their device or through the

Central Admin Tool (CAT). Administrator users can only call other corporate users within the same Corporate ID.

13.1.3

Administrator-Managed and Personal User-Managed

An Administrator-Managed and Personal User-Managed user can be subscribed with corporate features and personal features at the same time. The Administrator manages contacts and groups. When configured, the user can manage personal contacts and groups. When configured, an Administrator-Managed and Personal User-Managed subscriber can create a personal group with personal and corporate contacts from their contact list.

An Administrator-Managed and Personal User-Managed subscriber is provisioned with a flag indicating if the provisioned subscriber automatically gets all existing subscribers with the same Corporate ID as contacts in their PTT application. If there are ten subscribers with the same Corporate ID, the subscriber automatically has nine contacts. This capability supports SMB customers with automatic contact list management even though they are not a corporation. If the flag is not set, all contacts within a Corporate ID are part of the list, and the Administrator needs to assign contacts to the appropriate user set.

This flag applies to Administrator User and Administrator and Personal User-Managed subscribers only.

13.2

Subscriber States

A PoC user can be in one of the following states:


- Provisioned – the user is provisioned as a PoC user
- Activated – PTT application has activated the service and has the necessary configuration for the user to start using the service
- Suspended – the user can maintain their configuration, contacts, and groups but cannot use the service.

13.3

Subscriber Provisioning

The provisioning system uses a programmatic SOAP or REST interface to provision users in the Broadband PTT. The key functions provided by the interface for provisioning are:

- Create Subscriber
- Update Subscriber
- Delete Subscriber

 **NOTE:** When a user is deleted using provisioning, they are removed automatically from all user sets and talkgroups of other corporations where they may be an external user.

- Change Service Auth Status (Suspend, Unsuspend Subscriber)
- Get Subscriber Details using MDN
- Change MDN

The provisioning system supports suspending a user irrespective of their state on the PTT platform.

The provisioning interface allows a corporate name to be associated with a corporate ID.

All users with the same corporate ID are provisioned in the same PoC server with the Corporate Anchoring. Users with the same corporate ID are anchored to the PoC server. Users in a corporation can be rehomed from one PoC server to another during capacity planning. The server triggers the rehome notification; once

the PTT application receives the notification, the PTT application automatically logs into the new designated PoC server. The rehomeing process takes approximately 15 seconds to complete. Ongoing calls and other services may fail during this process and may not be automatically re-established. Instead, users may have to reinitiate the disconnected service manually. Typically the failure duration may last up to 15 seconds; therefore, it is not recommended to perform the rehome operation while the user is on active duty.

The rehomeing process is a planned exercise performed during the maintenance window by the Operations team in collaboration with impacted customers. Typically, the rehomeing operation is performed for the users during their off-duty hours, when users are offline. This procedure is repeated multiple times to minimize the end-user impact until the capacity planning exercise is completed.

When the user's provisioning is changed, the user is affected as follows:

Subscriber Type Change to 'Corporate Only'

A subscriber's personal contacts and talkgroups are deleted. Administrator-managed contacts and talkgroups are preserved.

Subscriber Account ID Change

Subscriber's corporate contacts and talkgroups are deleted. Personal contacts and talkgroups are preserved.

Subscriber MDN Change

In the case of a changeMDN operation, the subscriber's state is reset to 'provisioned.' In this case, the activation process is expected to be the same as a newly provisioned subscriber. See [Restore Contacts and Talkgroups on page 107](#) for more details.

13.3.1

Feature Sets and Add-On Features

Feature Sets allows the availability of the features to the user depending upon the level of service that is purchased. The supported feature sets are Collaboration, Command, and MCPTT.

Collaboration is the base feature set that a PTT subscriber can have. The subscriber gets additional features with an upgrade to MCPTT tiered-feature set.

Even if the tiered-feature set is provisioned, a feature is only available to a subscriber if it is supported by its client type, role, and application version, for example, Geofence feature is available for supervisors and dispatchers only and is available for 8.3 onwards clients.

The following table lists the PTT features available.

Table 27: PTT User Feature Availability by Feature Set

Features - PTT users	Collaboration	Command	MCPTT
PTT Calling, Presence, IPA	✓	✓	✓
Messaging - Text, Image, Video, Location, File	✓	✓	✓
Voice messaging	✓	✓	✓
Priority talkgroup scanning	✓	✓	✓
Broadcast calling	✓	✓	✓
Geolocation	✓	✓	✓

Features - PTT users	Collaboration	Command	MCPTT
Geofence	✓	✓	✓
Quick group from map	✓	✓	✓
Emergency calling and alert	✗	✓	✓
Area-based talkgroups (as member)	✗	✓	✓
User check	✗	✓	✓
Ambient listening	✗	✓	✓
Discreet listening	✗	✓	✓
Enable or disable PTT service	✗	✓	✓
Device ID Management	✓	✓	✓
CAT & WCSR ID Management	✓	✓	✓
AMR-WB	✓	✓	✓
Opus	✓	✓	✓
Userless Mode	✗	✗	✓
End to End Encryption	✗	✗	✓
Talkgroup Affiliation	✗	✗	✓
User Profiles	✗	✗	✓
User Role-Based Login	✗	✗	✓
Manual Answer (Hook signaling)	✗	✗	✓
Regroup Service	✗	✗	✓

The following table lists the Dispatch features available.

Table 28: Dispatcher Feature Availability by Feature Set

Features - Dispatch Console	Collaboration	Command	MCPTT
PTT Calling, Presence, IPA	✓	✓	✓
Messaging - Text, Image, Video, Location, File	✓	✓	✓
Voice messaging	✓	✓	✓
Talkgroup monitoring	✓	✓	✓
Priority talkgroup scanning	✓	✓	✓
Broadcast calling	✓	✓	✓
Geolocation	✓	✓	✓

Features - Dispatch Console	Collaboration	Command	MCPTT
Geofence	✓	✓	✓
Breadcrumb	✓	✓	✓
Messaging storage	30 days	30 days	30 days
Call recording storage	30 days	30 days	30 days
Location history storage	30 days	30 days	30 days
Area-based talkgroups	✗	✓	✓
Emergency calling and alert	✗	✓	✓
User check	✗	✓	✓
Ambient listening	✗	✓	✓
Discreet listening	✗	✓	✓
Enable or disable PTT service	✗	✓	✓
Remote Talkgroup Affiliation	✗	✗	✓
Simultaneous PTT Audio Sessions	✗	✗	✓
Talkgroup Affiliation	✗	✗	✓
Affiliation Monitoring	✗	✗	✓
Manual Answer (Hook signaling)	✗	✗	✓
Regroup Service	✗	✗	✓ ¹

 **NOTE:** ¹3GPP MC APIs only

Add-On Features (Feature Sets)

Additional to the above feature sets, the subscriber can purchase additional features on top of any feature set. Following add-on features are supported.

- Per-user charging for Interop calls: User must have this feature to make and receive Interop calls.
- QoS, Priority, and Preemption: User is assigned a QoS profile using this add-on feature. See the [Quality of Service \(QoS\), Priority and Preemption \(QPP\) on page 136](#) for more information.
- Video Services: User must have this feature to push and pull streaming video. See the [Video Services on page 74](#) for more information.

13.3.2

Welcome SMS (Optional)

The “Welcome SMS” is a text message sent immediately upon successful provisioning of a new PTT user. The text message delivery is enabled on a system-wide basis and can contain up to a 160-character message. The message is delivered over an SMPP v3.4 interface.

13.3.3

User Types Provisioning and Restrictions

Each user must be provisioned with a user type, and each PTT application must also be provisioned with a PTT number that identifies the “contact number” of the PTT user. The following table shows the options for each user type:

Table 29: User Type Provisioning Options

User Type	PTT Number
Cross-Carrier PTT Radio	Pseudo Number assigned by License Packs or MDN assigned by the provisioning interface.
Cross-Carrier Standard	Pseudo Number assigned by License Packs or MDN assigned by the provisioning interface.
Dispatch	Pseudo Number assigned by License Packs or MDN assigned by the provisioning interface.
Handset PTT Radio	MDN assigned by the provisioning interface.
Handset Standard	MDN assigned by the provisioning interface.
Integrated Mobile	Pseudo Number assigned by License Packs or MDN assigned by the provisioning interface.
Integrated Tracking	Pseudo Number assigned by License Packs or MDN assigned by the provisioning interface.
Integrated Web	Pseudo Number assigned by License Packs or MDN assigned by the provisioning interface.
Interop Talkgroup	Pseudo Number assigned by License Packs or MDN assigned by the provisioning interface or MDN assigned by the system administrator.
Interop User	Pseudo Number assigned by License Packs or MDN assigned by the provisioning interface.
Wi-Fi PTT Radio	Pseudo Number assigned by License Packs or MDN assigned by the provisioning interface.
Wi-Fi Standard	Pseudo Number assigned by License Packs or MDN assigned by the provisioning interface.

The PTT number for users is typically the same as the Mobile Directory Number (MDN) assigned to a user. When provisioned using the license packs, PTT numbers are assigned automatically by the platform. The automatically assigned number is up to 15-digits long and is treated as international number format. See [Contact and Talkgroup Management on page 103](#) for more details on PTT user addressing.

Some user types have restrictions on the user types allowed to be provisioned. The following table outlines these restrictions:

Table 30: User Type Provisioning Restrictions

User Type	Allowed User Types		
	Administrator	Administrator and User	Personal
Cross-Carrier PTT Radio	✓	✗	✗
Cross-Carrier Standard	✓	✓	✗
Dispatch	✓	✓	✗
Handset PTT Radio	✓	✗	✗
Handset Standard	✓	✓	✓
Integrated Mobile	✓	✓	✗
Integrated Tracking	✓	✓	✗
Integrated Web	✓	✓	✗
Interop Talkgroup	✓	✓	✗
Interop User	✓	✓	✗
Wi-Fi PTT Radio	✓	✗	✗
Wi-Fi Standard	✓	✓	✗

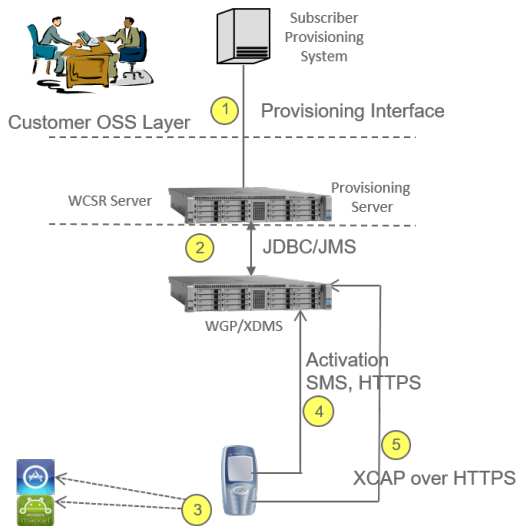
13.3.4

Activation of PTT Applications over Cellular Network

Broadband PTT provides a unique, automated activation mechanism to minimize user input and errors. For device PTT application provisioning, the solution uses intrinsic network capabilities to authenticate the user and eliminates the need for password distribution and manual entry by the user.

A combination of Mobile Originated SMS and HTTPS transactions are used to support device authentication. The following diagram shows the device authentication process:

Figure 2: Device Authentication Process



- Customer's subscriber provisioning system sends CreateSubscriber to the PTT system.
- The subscriber is provisioned and is in "Provisioned" state.
- Subscriber downloads the PoC client application from appropriate marketplace / app store.
- When the subscriber access the PoC Client, the PoC client sends Activation message to server by originating a SMS via SMPP and HTTPS request
- If the subscriber is provisioned, PoC configuration is downloaded to the client. Subscriber is now in 'activated' state and PTT application is ready for use. Corporate subscribers' clients will also download any corporate contacts and groups.

If the user tries to activate the service before being provisioned in the system, the activation is rejected with an appropriate message.

For activation with device ID management, see [Device ID Management on page 40](#).

13.3.5

Activation of Wi-Fi Only and Dispatch PTT Applications

If a user is provisioned as a Wi-Fi or Dispatch PTT Application, the activation occurs differently than device PTT applications and donor PTT applications. Activations of these PTT applications occur over an Internet connection and are managed by the Central Admin Tool (CAT).

These user types are indicated within CAT with an icon corresponding to their type. To activate one of these PTT applications, the Administrator, using CAT, must generate an activation code. This activation code is sent to the activating user's email address. The user must enter the activation code into the PTT application when prompted during activation.

The PTT servers integrate with the customer's email servers over SMTP or use PTT-provided email servers.

For activation with device ID management, see [Device ID Management on page 40](#).

See [Activation Code Format on page 132](#) for details regarding the activation code format.

13.3.6

Summary of Provisioning Methods

The following table lists a summary of provisioning methods for each user type:

Table 31: Summary of Provisioning Methods

User Type	Provisioning Method
Embedded PTT applications & Downloadable PTT applications	Activation using SMS and HTTP(S) PTT application/server communication over cellular network or Wi-Fi with an activation code (see Presence Notification Options on page 62 for more details)
Wi-Fi	CAT generation of an activation code sent using email
Dispatch	CAT generation of an activation code sent using email
Cross-carrier	CAT generation of an activation code sent using email
Integrated Mobile	CAT generation of an activation code
Integrated Tracking	CAT generation of an activation code
Integrated Web	CAT generation of an activation code

13.3.7

Provisioning with License Packs and License Management Tool

Broadband PTT provides a License Packs feature which supports bulk provisioning of PTT applications that do not have individual Mobile Directory Numbers (MDNs):



NOTE: Provisioning is performed using REST or SOAP APIs. New customers are required to use REST APIs.

- Wi-Fi PTT Application
- Dispatch
- Integrated Web APIs, Integrated Tracking APIs, and Integrated Mobile APIs (refer to [PTT Applications on page 87](#) for additional information)
- Cross-Carrier PTT Application
- Interop User

Pseudo Numbers

For each requested license for Billing Phone Number, a “Pseudo Number” is assigned.

The system generates Pseudo Numbers.

The user number associated with the Billing Number is dedicated as the billing number for the pool of PTT applications and cannot itself be used to activate the PTT application.

The Billing Phone Number associated with the Pseudo Number can be viewed by retrieving the user information for the Pseudo Number using the WCSR and LMT. Similarly, the Pseudo Numbers associated with a Billing Phone Number can be retrieved using the WCSR and LMT.

Life Cycle Management

Creation

When Broadband PTT users are provisioned, the attributes contained within the user profile are inherited from the Billing Phone Number.

Update

The following fields may be updated:

- Billing phone number (CTN/MDN)
- Corporate name

Upgrade/Downgrade License Pack

Upgrading a license pack allows increasing the number of lines (Pseudo Numbers) associated with a Billing Number. The downgrade of a license pack reduces the number of lines (Pseudo Numbers). The following sections provide details on the upgrade and downgrade experience.

Upgrade license pack experience

An Upgrade License Pack Provisioning Request is made with the total number of lines desired to add additional Pseudo Numbers associated with a Billing Phone Number.

For example:

- A Billing Phone Number 214-222-4333 has 20 dispatch PTT application licenses associated with it.

- An upgrade license pack request is made for 214-222-4333 with a total count of 25 dispatch PTT application licenses (a net increase of 5 licenses).

The LMT server adds five additional Dispatch Pseudo Numbers to the account associated with the Billing Phone Number 214-222-4333.

Downgrade license pack experience

When the number of licenses for a Billing Number is downgraded (or reduced), the Pseudo Numbers without any administrator-managed contacts and groups are deleted as per the following logic:

- Pseudo Numbers which are provisioned but are not activated yet.
- Pseudo Numbers that are activated but don't have any administrator-managed contacts or groups.
- The lines with the last sequential number. For example: If the following five numbers are associated with a license pack, the last two are deleted.
 - 612-111-1111
 - 612-111-1112
 - 612-111-1113
 - 612-111-1114
 - 612-112-1111

A Downgrade License Pack provisioning request is made with the total number of lines desired for that Billing Number to remove Pseudo Numbers associated with a Billing Phone Number.


For example:

A Billing Phone Number 214-222-4333 has 20 dispatch PTT application licenses associated with it, and the desired number of dispatch PTT application licenses is 15.

The Administrator must make sure that at least five Pseudo Numbers associated with 214-222-4333 have no contacts and groups.

A downgrade license pack request is made for 214-222-4333 with a total count of 15 dispatch PTT application licenses (a net decrease of five licenses).

The five Pseudo Numbers that do not have contacts or groups are deleted.

-  **NOTE:** When a Pseudo Number is deleted, all the personal contacts and groups are lost.

Changing the type of licenses

Changes to user types are not allowed, and a provisioning request to change the user type errors out. If this type of change is required, it is recommended to use a sequence of delete and add provisioning requests.

Deletion

When the Billing Phone Number is deleted, all the Pseudo Numbers associated with it are also deleted. All the contacts and groups for the Pseudo Numbers are lost.

Suspension and Resume

When the Billing Phone Number is suspended, all the Pseudo Numbers associated with it are also suspended. The same is the case with resume.

For more information on the License Management Tool (LMT), refer to the *License Management Tool User Guide*.

13.3.8

Auto-Pairing

This feature allows corporations that do not have access to the Central Admin Tool (CAT) to have all the users in the corporation as contacts. Also, an all-member group is created that has all the users in the corporation as members. As users are added to or removed from the corporation, the contacts and groups are automatically maintained.

The server maintains Auto-Pairing as an administrator-managed user set and administrator-managed group. The user set is named as “all_subscribers_sub-list.” Note that the user does not see the user set name on their device; this name is visible only if the corporation later gains access to the CAT. The all-member administrator-managed group is similarly named as “all_subscribers_group,” which is shown in the group list for the members on their device and can be used to call all the members of the corporation.

Configuration

This feature is configured system-wide through a provisioning parameter. Once the number of users provisioned in a corporation exceeds the configured size (1-250, default=50), the auto-pairing is disabled for that corporation. Existing distributed contacts remain as-is, and the all-member group also remains unchanged. If the corporation reduces the number of users below the configured size, auto-pairing of the provisioned user does not automatically restart. Auto-Pairing is also automatically disabled for a corporation the first time an administrator accesses the CAT. Once the feature is disabled, reducing the number of users in the corporation does not enable the auto-pairing again.

This feature is not applicable to personal types of subscribers.

13.4

PTT Activation / Authentication

See the following sections on Push-to-Talk activation and authentication:

- [Cellular Network Activation / Authentication on page 130](#)
- [Multiple PoC Servers Support on page 131](#)
- [Wi-Fi Network Activation / Authentication on page 131](#)
- [Wi-Fi Only Device Activation on page 132](#)
- [Device Activation Control on page 132](#)

13.4.1

Cellular Network Activation / Authentication

An inactivated PTT application sends an activation MO SMS and HTTPS request to the PoC system when the user starts the application. The PoC system uses a source MSISDN in the activation SMS to ensure that the correct user is considered for activation. A token is generated and sent in the activation SMS and HTTP request. This token is used to bind the HTTPS request to the respective SMS and an MSISDN. This token is an MD5 hash of a random number and current time in milliseconds, and it is unique. The PTT application also generates and sends an authcode over activation HTTPS request and server returns a user ID in the response.

This user ID and authcode are used for authentication for subsequent SIP registrations and HTTP transactions.

13.4.2

Multiple PoC Servers Support

A single PTT application can support multiple server deployments when the device can fetch activation configuration information from the PoC server

- Device state is preactivation - MSISDN is not securely known

Feature supports on-premise and global or regional deployments

Activation configuration supports multiple activation options: SMS/HTTPS, activation code, free trial

A deployment ID is added and is used to fetch the deployment configuration

- Can be preconfigured through a Mobile Device Management (MDM) file
- If not preconfigured, the user is prompted for a deployment ID, provided by the Welcome SMS, email, or other means

Activation Options

The following activation options are to be deployed:

- SMS/HTTPS (with activation code fallback allowed)
- Activation code only
- Free trial (for ample, WAVE PTX)

The solution needs a way for an inactivated device to determine, or let the user decide, which PoC server to connect.

The device should have a method of loading a configuration file with the deployment information so that preceding options, along with server address, preloaded or pushed using Mobile Device Management (MDM).

Deployment ID

Each deployment has a Deployment ID code assigned to it. The code has the following information:

- Customer ID (4-alphanumeric characters)
 - Ensures uniqueness of deployment ID
 - Motorola Solutions reserves 'WAVE' for our deployments
 - On-premise customers can assign their customer ID if they want it to remain nonpersonal
- Valid Transport Methods for configuration file retrieval
 - Cellular-only, Wi-Fi only, or Any
- Deployment Designation (one or more alphanumeric characters)

The Deployment ID should be unique to resolve correctly for a particular system.

The Deployment ID maps to a unique deployment configuration file to be requested by the device from the PoC server.

13.4.3

Wi-Fi Network Activation / Authentication

If the device supports cellular and Wi-Fi, the activation occurs automatically over the cellular network. If the cellular network is not available at the activation time, the user can exit the application and wait for the cellular network to become available or activate over an open Wi-Fi connection using their activation code.

Activation occurs over the Wi-Fi connection for devices that support only a Wi-Fi data connection (devices that do not have a cellular radio).

To activate over Wi-Fi, the user must enter an activation code provided by the Administrator. The activation code is generated by the CAT and can be sent using email directly from the CAT.

Activation Code Format

- The activation code is unique, system-wide, and not per corporation.
- The activation code is seven numeric digits long (provides 10,000,000 unique codes).
- The activation code expires after one activation or 7 days of nonuse.

13.4.4

Wi-Fi Only Device Activation

If a device, such as a tablet, cannot send SMS and supports Wi-Fi, service activation/authentication occurs using an activation code over Wi-Fi, as described in the previous section.

13.4.5

Device Activation Control

The desired mechanism to prevent an unsupported downloadable application device model is using controls provided by the application store. Sometimes the application store does not offer the ability to block specific models. The server offers a system-wide configurable list of device models, which can be activated for PTT. A PTT application is not activated if downloaded on a device model, not on this list. This list is configurable at the discretion of the customer. Note that only committed devices are tested and supported for PTT functionality.

13.5

MSISDN Change

When a user changes their phone number, the provisioning system sends a ChangeMDN request to the PoC system.

For a Personal user, all the contacts and groups for the user is transferred to the new MDN.

The personal user has to notify all their contacts that their number has changed so that they can make the necessary change in their PTT contact list.

The above applies to the personal contacts of an 'Administrator and User' subscriber.

For an Administrator/Administrator and User user, the ChangeMDN changes the MSISDN for all administrator-managed user sets, contacts, and groups that the MDN is part of. All administrator-managed users with a contact that changes the MSISDN get the contact updated in their contact and group lists.

The PTT application has to power cycle the phone once the change MDN provisioning is successfully performed on the PoC system.

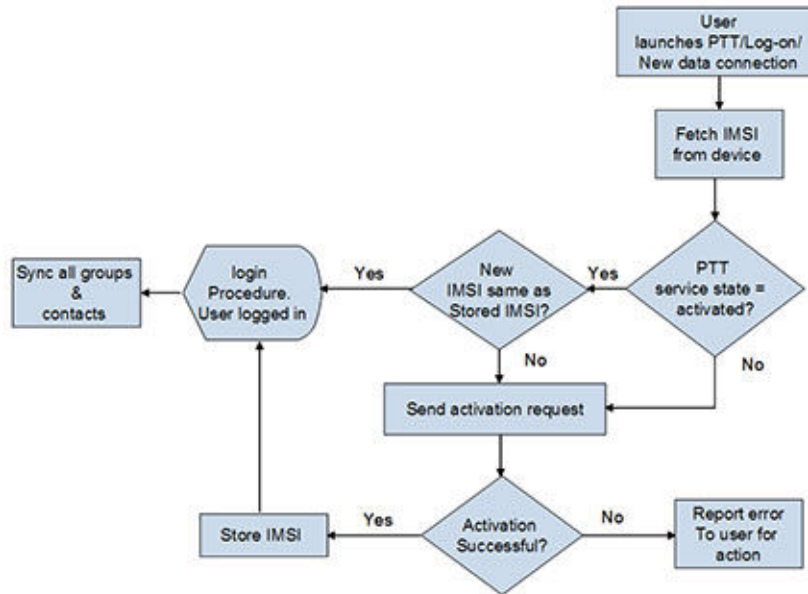
13.6


SIM Change

When a user replaces their SIM with a new SIM but the same MSISDN, the PTT application recognizes that the IMSI has changed and reactivates with the server after confirming with the user. It pushes all the user configuration information and the user's contacts and groups to the PTT application. Call history is reset.

If the MSISDN is different, the server provides the configuration and related information for that MSISDN. The SIM swap and IMSI detection flow are as follows:

Figure 3: SIM Swap and IMSI Detection Flow



 **NOTE:** If your device contains a Data Only SIM Card, it needs to be reactivated through the WAVE Portal.

13.7

Device Change

Users may upgrade or change their mobile device from time to time. The PTT application on the device is reactivated since the application on the new phone does not have any configuration information. This downloads all the user configuration information and the user's contacts and groups to the PTT application. Call history and favorites are reset.

Chapter 14

Branding and Language Support

The CAT portal is in English and provides multi-language support including Right-to-Left language. The default language is English, and an alternate language preference is passed to the PoC system by the customer's SSO system. The customer provides the translations.

Also, the following branding options are provided:

- Images (logo, header)
- Page title, labels, and links textual modifications
- Button modifications
- Help, error, confirmation, and success messages modifications
- Font and color modifications for title, labels, and links

The customer shall provide the necessary assets required to perform the modifications based on the guidelines provided by Motorola Solutions (restrictions the size, resolution of the images, length of the strings, etc.)

PTT Applications

PTT applications are in English and provide multi-language support including Right-to-Left language. Motorola Solutions allows the following standard branding and configuration that can be branded by the customer:

- Application name
- Application icon
- Application splash screen

The following customer-specific configuration is supported:

- End-User License Agreement (EULA)
- URL to help pages
- Activation SMS short code and URL
- Application package name (Android applications)

Dispatch Application Branding

Dispatch Applications are in English and provide multi-language support including Right-to-Left language. The following can be branded by the customer for the Dispatch Application:

- Dispatch name
- Dispatch strings and Email Templates
- Dispatch icons
- Dispatch sign in screen background image
- Tones

The following customer-specific configuration is supported:

- End-User License Agreement (EULA)
- Links/URLs to help pages

- Activation URL
- Dispatch plug-in

Language translation for client strings

- Customer to provide translations for client string list

User Guide

- Non-branded English source document is provided to the customer in PDF format.

Branding validation

- Customer performs final client branding validation to ensure meaningful translations; text fits within allotted space, etc.

Chapter 15

Quality of Service (QoS), Priority and Preemption (QPP)

Broadband PTT supports policy-based QoS, Priority and Preemption (QPP) that provides PTT users with prioritized access to the LTE network and its resources during times of congestion. Policies such as the type of the user, type of call the user made, etc.

15.1

QPP Packages

Policies are defined on the Broadband PTT using QPP packages. QPP packages are provisioned for a broadband user using the user provisioning interface such as provisioning APIs, WCSR. The Broadband PTT user can be provisioned with one and only one QPP feature set. Multiple add-on packages can be configured in the system, with each feature set to map to unique QPP profiles to serve a wide variety of customer bases and markets. The configuration for default user treatment is supported. If the Broadband PTT user is not configured with an add-on feature set, the PTT system can provide a default QPP treatment for the user defined by the system administrator.

The system administrator controls system-wide configuration for multitiered QPP packages. The following are examples for illustrative purposes only:

- Default
- Silver- feature set 1
- Gold-feature set 2
- Platinum-feature set 3

Each feature set is a mapping of PTT call types to QPP profile. QPP profiles are also defined and maintained at system level, which determines the QPP attributes to be applied to a user during run-time such as QCI, ARP, bearer preemption ability, MBR (uplink or downlink), and others.

Following call types can be configured as a part of the feature set.

- 1:1 private call
- Regular talkgroup call
- Broadcast call
- Emergency call
- Ambient Listening call

The following table illustrates the mapping of QPP feature set, feature, and profile levels.

Table 32: QPP Feature Set Mapping

Call Type	Default	Silver	Gold	Platinum
Private call- PTT User	Default	Default	Default	Level 1
Talkgroup call	Default	Default	Level 1	Level 2
Broadcast talkgroup call	Default	Level 1	Level 2	Level 3

Call Type	Default	Silver	Gold	Platinum
Emergency call	Level 1	Level 2	Level 3	Level 4
Ambient Listening call	Level 1	Level 2	Level 3	Level 4

Network Requirements for Mission Critical PTT Deployments

Mobile data networks must comply with the cellular network requirements outlined in the "Mission Critical PTT Network Requirements" document for Mission Critical application and to meet MCPTT KPIs as defined in 3GPP TS 22.179. Over the top PTT services typically use QCI 9 or QCI 8 for all internet packet data, including PTT signaling and PTT voice/video. However, PTT service integrated with cellular networks may use QCI 5 or 69 for PTT SIP signaling and QCI 7 or 65 for PTT voice. The following table explains QCI characteristics values:

Table 33: QCI Characteristics

QCI	Resource Type	Priority	Packet Delay Budget	Packet Error Loss Rate	Example Services
1	GBR	2	100ms	10 ⁻²	Conversational Voice
2	GBR	4	150ms	10 ⁻³	Conversational Video (Live Streaming)
3	GBR	3	50ms	10 ⁻³	Real-Time Gaming, V2X messages
4	GBR	5	300ms	10 ⁻⁶	Non-Conversational Video (Buffered Streaming)
65	GBR	0.7	75ms	10 ⁻²	Mission Critical User Plane Push To Talk voice (for example, MCPTT)
66	GBR	2	100ms	10 ⁻²	Non-Mission-Critical User Plane Push To Talk voice
75	GBR	2.5	50ms	10 ⁻²	V2X messages
5	non-GBR	1	100ms	10 ⁻⁶	IMS Signaling
6	non-GBR	6	300ms	10 ⁻⁶	Video (Buffered Streaming) TCP-Based (for example, WWW, email, chat, FTP, P2P and the like)
7	non-GBR	7	100ms	10 ⁻³	Voice, Video (Live Streaming), Interactive Gaming
8	non-GBR	8	300ms	10 ⁻⁶	Video (Buffered Streaming) TCP-Based (for example, WWW, email, chat, FTP, P2P and the like)
9	non-GBR	9	300ms	10 ⁻⁶	Video (Buffered Streaming) TCP-Based (for ex-

QCI	Resource Type	Priority	Packet Delay Budget	Packet Error Loss Rate	Example Services
					ample, WWW, email, chat, FTP, P2P and the like). Typically used as default carrier
69	non-GBR	0.5	60ms	10^{-6}	Mission Critical delay sensitive signaling (for example, MC-PTT signaling)
70	non-GBR	0.5	200ms	10^{-6}	Mission Critical Data (for example, services are the same as QCI 6/8/9)

15.2

Additional Settings

In addition to Quality of Service (QoS), Priority and Preemption (QPP) packages, below are system level configurations, which are applicable during QPP treatment of user.

QPP Treatment for Call Participants

System-wide configured flag is used to determine the QPP treatment of the participating users when there is an emergency call. A similar configuration for the private call and normal group calls, broadcast group calls exists. Following are the options:

- User receives provisioned QPP: all the active participants in the group call receive the QPP treatment as per their provisioning feature set or default (if configured).
- User receives the same QPP attributes as call originator: all the active participants in the group call receive: the QPP treatment same as of the originator (irrespective of user provisioned feature set).

Call Continue of the Bearer Is Not Established (True/False)

In scenarios where guaranteed QoS is required when the user places a PTT call, this flag must be set to **false**. If the flag is set to **true**, then the ongoing call continues even in case of Rx session setup failure. If set to **false**, then the ongoing call is dropped for the user if the Rx session setup is failed for a user.

15.3

Rx Interface

Access to the Rx interface is required to provide dynamic QPP for premium Broadband PTT customers on wireless networks. The Rx reference point is used to exchange application-level session information between the Policy and Charging Rules Function (PCRF) and the PoC server. Dedicated bearers are dynamically created when a PTT call is placed compared to the subscription-based static bearer solution that is established when PTT applications are powered on and stays on until devices are turned off. PoC server is aware of radio access (RAT-Type) of user devices and initiates Rx session to set up dedicated bearers only when a call is set up.

Using the Rx interface, dedicated bearers are set up when the device is in LTE coverage or moves to LTE coverage while a Broadband PTT call is active. If the user is in eHRPD or WLAN, PoC server will not set up an Rx session.

Broadband PTT connects to PCRF through Diameter Routing Agents (DRA) to establish the Rx session. PoC server also subscribes to certain events, for example, Release of Bearer, so that the event is triggered by PCRF when the device moves from LTE to eHRPD network and aid PoC server to release the dedicated bearer.

Triggers for Rx Establishment

- User device is in LTE coverage. The user logs into the PTT Application. At a later point in time, when PTT call or video call is set up, PoC server establishes communication with the PCRF via the Rx interface.
- User device moves from eHRPD/WLAN to LTE and has an active PTT call or video call. The device informs the PoC server about new RAT. PoC server initiates Rx session establishment.

Trigger for Rx Tear Down

- The PTT call or video call has ended on an existing Rx session.
- User device moves from LTE to eHRPD/WLAN and has an existing Rx session.
- Inactivity timer on PoC server expires.
- Network initiates release of Rx.

Dynamic assignment of QoS, Priority and Preemption for PTT signaling bearer is not supported by the PTT system. PTT signaling bearer is required to be statically configured on the LTE network to ensure guaranteed QoS for emergency service since emergency alerts are sent over PTT signaling bearer. Similarly, QPP for secure messaging is not dynamically assigned by the PTT system.

Chapter 16

Security

Motorola Solutions security practices are based on National Institute of Standards and Technology (NIST) cybersecurity framework functions: Govern, Identify, Protect, Detect, Respond and Recover. The following sections describe some key security features supported in the product:

- [System Access Control on page 140](#)
- [Encryption of Data in Transit on page 140](#)
- [PTT Application Security on page 140](#)
- [Server Encryption of Data at Rest on page 141](#)

16.1

System Access Control

The Broadband PTT solution has a role-based hierarchy with well managed security privileges, secure authentication, and authorization for all users accessing the system. The solution includes 2FA (2nd Factor Authentication) support for Central AdminTool (CAT), Web Dispatch (WDS), and Critical Connect (Universal Gateway Portal (UGW) Patch users using an Authenticator App.

16.2

Encryption of Data in Transit

Broadband Push-to-talk (PTT) system encrypts all communication between the PTT application and server.

Data in transit is protected using secure protocols (TLS v1.2, DTLS, HTTPS) and encryption of application payload. The encryption method used is AES-256, the Advanced Encryption Standard, formalized by the National Institute of Standards and Technology (NIST). Broadband PTT system uses FIPS 140-2 level 1 compliant encryption for TLS & DTLS.

The PTT solution includes an integrated Key Management System (KMS). The KMS is 3GPP 33.180 TS compliant and supports signaling encryption and MIKEY-SAKKE Identity Based Encryption (IBE) for key distribution. It auto-generates, auto-rotates & auto-distributes keys to all PTT devices. PTT audio for broadband-only calls is end to end encrypted using Secure RTP (SRTP) in compliance with 3GPP 33.180 TS.



NOTE: End-to-end encryption does not apply when interworking between PTT applications with and without SRTP support as well as for use cases including Land Mobile Radio (LMR) Interop, call recording, and lawful intercept.

End-to-end encryption may not be available on all devices.

16.3

PTT Application Security

The PTT application encrypts locally stored sensitive data using AES-256 and the native device's key store best practices. The data includes PTT application authentication credentials, contacts, groups, configuration, and settings. The database can be decrypted by the PTT application only on the specific device on which it was encrypted.

All external server FQDNs are provided with certificates issued by a Certificate Authority (CA). The limited CA bundle to be trusted by client applications (Android, iOS, and Windows) for verifying the server certificate

is pinned into our application clients. This prevents an attacker from injecting untrusted servers in the path between the PTT application and the server to eavesdrop communication.

The PTT application does not log sensitive data such as username, password, configuration values received from the server, or PTT application configuration values.

16.4

Server Encryption of Data at Rest

All user-generated content (messages, attachments, call recordings, location, etc.) is encrypted when stored at rest in server databases. Encryption material is secured using a system vault. The cipher algorithm used for encryption-key generation is AES-256.

Chapter 17

Platform High Availability

Broadband PTT provides high availability by supporting in-chassis redundancy with geographical redundancy for all servers in the solution. In-chassis redundancy is achieved in an active-standby or load-shared configuration. Broadband PTT provides automatic switchover to the redundant servers and customer-controlled manual switchback after rectifying fault. Appropriate alarms are generated and sent to the NOC. Once the fault is detected, the switchover is instantaneous since all users and service data is replicated in real time between the primary server, secondary server, and the GeoServer.

Active calls are not maintained across switchovers.

17.1

PTT Application Server Notification Channel on Standby Site

This feature allows the server to notify a PTT application that it needs to switch network connections to the active site, reducing the time required when a switchover occurs between the primary site and a geo-redundant site or vice versa.

Chapter 18

Operations, Administration, Maintenance, and Provisioning (OAMP)

18.1

License Management Tool (LMT)

The License Management Tool (LMT) provides the ability to downgrade the license packs. It applies to the following user types: Cross Carrier PTT Radio, Cross Carrier PTT Standard, Dispatch, Integrated Mobile, Integrated Tracking, Integrated Web, Interop Talkgroup, Interop User, Wi-Fi PTT Radio, and Wi-Fi Standard.

18.2

Customer Service Support Web Portal (WCSR)

Broadband PTT includes a Customer Service Representative (CSR) portal that allows CSRs to manage or view users and help to solve customer issues. The following hierarchical CSR roles are supported to manage different types of customer issues supporting different CSR privileges

Table 34: CSR Role Privileges

CSR Role	CSR1	CSR2	CSR3	CSR4
Create Subscriber	✓	✓	✗	✗
Update Subscriber	✓	✓	✗	✗
Delete Subscriber	✓	✓	✗	✗
Get Subscriber Details	✓	✓	✓	✓
Migrate Subscriber	✓	✓	✗	✗
Resync Subscriber	✓	✓	✗	✗
Status Subscriber	✓	✓	✗	✗
CAT UI / View Billing Number Information (LMT)	✓	✓	✗	✗
PAM License View	✓	✗	✗	✓
Create/Modify/Delete/Get Operations of Admin Users	✓	✗	✗	✓

The CSR1 can link into the CAT to manage administrator-manage contacts and groups by manually entering the Corporate ID. There is no additional authentication for the CSR to access any CAT data. CAT audit logs are not differentiated as coming from the CSR.

CSR users are created by Unified Communications Operations.

The WCSR portal is in English, and additional languages can be supported. The customer provides the translations.

18.2.1

WCSR ID Management

WCSR ID Management allows administrators to access WCSR with a login ID (email address) and password.

Unified Communications Operations creates the User ID. SSO method is available upon customer request.

New users are assigned access to a combination of the following elements based on the role assigned:

1. Create Subscriber
2. Update Subscriber
3. Delete Subscriber
4. Get Subscriber Details
5. Migrate Subscriber
6. Resync Subscriber
7. Status Subscriber
8. CAT UI and View Billing Number Information (LMT)
9. PAM License View
10. Create/Modify/Delete/Get Operations of Admin Users

WCSR access is controlled through a user id/password login mechanism. The user id and passwords are created when the CSR is created.

All transactions performed by a CSR that change data are logged for auditing purposes.

For more information on the Customer Service Support Web Portal, refer to the *WCSR User Guide*.

18.3

Network Management

The Element Management System (EMS) is the operations, administration, and maintenance platform for the PoC system. The EMS enables system administrators to perform configuration, network monitoring, and network performance data collection.

All functions of the EMS are accessible through a web-based interface in English.

The EMS provides the following two types of users:

- Administrators: Have the privilege for fault, configuration, performance, and security functionality of the system. They have the privilege to add users to the EMS.
- Users: Have the privilege of fault and performance management functionality of the PoC Server.

Successful and unsuccessful user logins and logouts are logged with a timestamp.

18.3.1

Fault Management

The EMS provides sophisticated centralized fault management capabilities for management of the Broadband PTT. The various PoC servers that comprise the Broadband PTT report alarms or failures to the Central EMS.

The key features of EMS Fault Management include:

- Event/Alarm processing and propagation
- Event/Alarm drill-down categorized by severity, resource type, and time of day on the EMS GUI

- Alarms severity categorized as critical, major, minor, and warning
- Alarm severity reassignment and synchronization operations using the EMS GUI

The EMS provides alarms to the following:

- The customer's NOC using SNMP
- EMS GUI interface

The customer's NOC servers capable of receiving SNMP V2c or V3 traps are configured on the EMS to receive traps as and when they are generated. SNMP v3 offers enhanced security features, such as encryption and authentication. These features help protect against unauthorized access and ensure the data's integrity. The northbound SNMP interface provides the following key features:

- The EMS Server can be configured to forward faults or traps from a specific list of network elements to a particular customer's NOC server.
- The EMS Fault Manager has a trap definition for each alarm type generated in the platform and a generic trap definition used to send different types of alarms using the same trap definition. Motorola Solutions can support either of the options based on the customer's preference and provide appropriate MIB files.



NOTE: It is preferred to use a generic trap definition and process the data that is coming in so that as more alarms are added there is less integration effort on the customer side.

Each alarm includes the following information:

- Object id
- Alarm severity
- Alarm category
- Description
- Failed component
- Time of the failure
- Recommended Action (listed in the Alarms handbook)

18.3.2

Configuration Management

The EMS GUI provides a centralized function to configure all the servers as well as other network-wide parameters. The key configurations required are as follows:

- PoC server configuration
- Presence server configuration
- XDM server configuration
- Card backup configuration using a Cron job

18.3.3

Performance Management

Performance Management helps analyze the performance of various subsystems of the PoC server. It allows statistical reporting to gauge how the service is being used for capacity planning. Performance measurements are available for call processing, presence, XDM server, and platform subsystems with collection generated periodically (default 30 minutes with a minimum of 5 minutes).

These measurements are made visible through the EMS GUI in graphs and reports to help the customer visualize the performance of the subsystems. The performance data is also made available in a flat-file format. The customer may pull this data to store within their data warehouse and generate customized

reports standard for their company. The performance collection capabilities comply with ITU-T, Telcordia, 3GPP, and TMF standards.

The system can generate threshold-based alarms with the provision to send these selected alarms as SNMP traps to an external NMS platform. For example, an alarm is generated if the CPU usage exceeds 90%.

18.3.4

Revenue Assurance Reconciliation (RAR)

The Revenue Assurance Reconciliation (RAR) report provides information about each user stored within the Broadband PTT. This information is available to allow reconciliation of users within the PTT system against customer billable users. Only one RAR report is generated for the entire system. The user records generated in each file are nonoverlapping. Dates and timestamps reported in the RAR report are based on UTC.

Examples of information included in the RAR report are (not an exhaustive list):

- Mobile Directory Number (MDN)
- Subscriber Status (Provisioned, Active, Suspended)
- Corporate ID
- Subscriber Name
- User Type
- Date and time provisioned (first time provisioned using provisioning interface and not when MDN is changed)
- Billing number (license packs)
- Feature set
- Add on feature

18.3.5

Usage Detail Records (UDR)

Call Usage

Broadband PTT generates Usage Detail Records (UDRs) in ASCII format that the customer may use to charge their users. UDRs are generated for both postpaid and prepaid users and include various diagnostic codes for operations monitoring. A UDR includes roaming and MCC/MNC at the start of the call. The following table lists the UDRs that are generated for the different types of sessions:

Table 35: Usage Detail Records

	Subscriber A Originates	Mobile Originating	Mobile Terminating
Broadband PTT Calls	1:1	A - B	A - B
	Prearranged Group. Group consists of A,B,C,D	A - B	A - B
		A - C	A - C
		A - D	A - D
	Quick group with members Subscriber B and C	A - B	A - B
A - C		A - C	

UDRs are stored in files with one of the following filename formats:

<PTTServerID>.YYYY-MM-DD.SSSSS, where:

- <PTTServerID> is the ID that is provided by the customer.
- Timestamp in YYYY-MM-DD format
- Five-digits SEQNUM of system generated incremental number starting with 00001 and incrementing by one until it reaches the maximum number, wrapping around to the beginning.

<PTTServerID>.YYYYMMDD.HHMMSS.SSSSS, where:

- <PTTServerID> is the ID that is provided by the customer.
- Timestamp in YYYYMMDD format
- Timestamp in HHMMSS format
- Six-digits SEQNUM of system generated incremental number starting with 000001 and incrementing by one until it reaches the maximum number, wrapping around to the beginning.

A UDR file contains a header followed by UDR records. The UDR header contains the UDR filename and number of records contained in the file. Each UDR record is either a Mobile Originated (MO) or Mobile Terminated (MT) type. The records contain various details about the calls. Included in these records are detailed release diagnostic information that can be used to support PTT call connection analysis. A comprehensive list of the supported fields is available.

The UDR file generation is configurable as follows:

- File size – Ranges from 1000 to 10,000 UDR records (default is 1000)
- Open Period – 5 minutes to 24 hours (default is 60 minutes)
- Directory location

UDR files must be pulled by the customer Data Mediation Center using FTP or SFTP. The Data Mediation Center can delete the UDR files and remove automatically after a configurable number of days (default is 30 days).

Message Usage

Broadband PTT generates Integrated Secure Messaging (ISM) Usage Detail Records (UDRs) in ASCII format that the customer may use to charge their users. UDRs are generated for both postpaid and prepaid users and include various diagnostic codes for operations monitoring. An ISM UDR includes roaming and MCC/MNC at the start of the call. The following table lists the ISM UDRs that are generated for the different types of sessions:

Table 36: ISM UDRs

	Subscriber A Originates	Mobile Originating	Mobile Terminating
Broadband	1:1	A - B	A - B
PTT Calls	Prearranged Group. Group consists of A,B,C,D	A - B	A - B
		A - C	A - C
		A - D	A - D
Quick group with members Subscriber B and C	A - B	A - B	A - B
		A - C	A - C

ISM UDRs are stored in files with one of the following filename formats:

<PTTServerID>.YYYY-MM-DD.SSSSS, where:

- <PTTServerID> is the ID that is provided by the customer.

- Timestamp in YYYY-MM-DD format
- Five-digits SEQNUM of system generated incremental number starting with 00001 and incrementing by one until it reaches the maximum number, wrapping around to the beginning.

PTTServerID.YYYYMMDD.HHMMSS.SSSSS, where:

- **<PTTServerID>** is the ID that is provided by the customer.
- Timestamp in YYYYMMDD format
- Timestamp in HHMMSS format
- Six-digits SEQNUM of system generated incremental number starting with 000001 and incrementing by one until it reaches the maximum number, wrapping around to the beginning.

An ISM UDR file contains a header followed by ISM UDR records. The ISM UDR header contains the ISM UDR filename and number of records contained in the file. Each ISM UDR record is either a Mobile Originated (MO) or Mobile Terminated (MT) type. The records contain various details about the calls. Included in these records are detailed release diagnostic information that can be used to support PTT call connection analysis. A comprehensive list of the supported fields is available.

The ISM UDR file generation is configurable as follows:

- File size – Ranges from 1000 to 10,000 ISM UDR records (default is 1000)
- Open Period – 5 minutes to 24 hours (default is 60 minutes)
- Directory location

ISM UDR files must be pulled by the customer Data Mediation Center using FTP or SFTP. The ISM UDR files can be deleted by the Data Mediation Center and are removed automatically after a configurable number of days (default is 30 days).

18.3.6

Log Server – Server and PTT Application Logging

The log server provides storage for other PTT servers and PTT application logs and provides high availability by employing a redundant server architecture. Each network element is configured with a primary and secondary server address.

The log server is accessible by Operations for debugging purposes. All logs are sent to the primary server, and upon failure, the network elements are connected to the secondary server. The primary and secondary servers are connected to RAID 5 storage providing data storage reliability. The server provides storage for the network elements within a single site. Therefore, in geo-redundant system deployments, a log server deployed within the primary site handles logging for the primary site, and the log server at the geo site handles logging for the geo site. PTT Application logs are stored at the primary site with failover to the geo site if the primary site log server is unavailable.

Access to the logs is provided through a Secure File Transfer Protocol (SFTP). Alternatively, the remote log server can be configured to push stored usage and statistical data to a mediation or analytical tool for processing. PTT log files are all common delimiter formatted and stamped with universal time (UTC).

Server Logs

The server logs include user event logs for presence changes, registration status changes, etc. The logs are retained for a configurable period.

PTT Application Statistics and Logs

Compatible PTT applications can send statistics and logs to the log server for later retrieval. PTT applications report their capability for collecting and reporting statistics and logging information to the server. The server, in turn, informs the PTT applications which data to log. These include the following:

Table 37: PTT Application Statistics and Logs

Type	Description	Reporting Interval
Jitter statistics	Statistics related to voice packet jitter (packet loss, out-of-order packets, arrival jitter, etc.) collected per volley	Enabled per user. When enabled, statistics are collected and reported until disabled. Data is reported after a configured number of volleys for each call and at the end of each call.
Application logs	PTT application logs used for diagnosing field issues	On demand through command line interface (CLI) available to the network operations team.
General statistics	Network, call, and health statistics.	Enabled per user. Collected and reported at random intervals around a configurable reporting interval. Collected data is purged when it reaches a configurable age.

PTT Application Usage Statistics

The PTT application Usage Statistics feature helps track feature usage of the PTT application to aid in improving the user experience. The PTT application can be enabled to report the following statistics related to user behavior:

- Originating call screen Instant Personal Alert screen
- Foreground/Background state of the PTT application for incoming calls
- Maximum number of favorite contacts
- Maximum number of favorite groups
- Collection/reporting period is configurable 1-90 days. Reporting occurs at random intervals around the configured reporting period.
- Data collection enable is controlled by the Operations team per corporation, per user, or as a percentage of the user population
- UI Statistics can be enabled per category
- Call Originations
- IPA Originations
- Incoming Call Application State
- Tab Selection
- Tab Utilization
- Presence
- Settings Snapshot
- Favorites
- Collection period (1-900 days, default 7)
- Stats enabled by Operations based on MDN list, Corporate ID, or User Agent list

Table 38: PTT Application Usage Statistics

Category	Description	Standard	PTT Radio
Call Originations	Count of calls originated from each application screen	✓	✓

Category	Description	Standard	PTT Radio
IPA Originations	Count of IPAs originated from each application screen	✓	✗
Incoming Call Application State	Count of incoming calls when the app is in foreground and background	✓	✓
Tab Selection	Count of number of times the user accesses each top-level tab	✓	✗
Tab Utilization	Time spent on each top-level tab reported in seconds.	✓	✗
Presence Utilization	Time spent in Available and DND presence states, reported in seconds.	✓	✗
Settings Snapshot	Snapshot of current user settings	✓	✓
Favorites	The maximum number of favorite contacts and favorite groups	✓	✗
Integrated Secure Messages	Count of message originations from each application screen	✓	✗

18.3.7

Backup / Restore

To be able to change a hardware card quickly, the Broadband PTT supports backup and restore functionality for all server cards. The media card software load is bundled with the PoC server and does not need to be backed up separately. It includes the software load, database as well as other configuration information. The frequency and time of backup are configurable.

All backup files are transferred to the customer provided backup servers using FTP or SFTP.

Logs are also backed up to the Customer backup server for diagnostic purposes.

Chapter 19

Regulatory Compliance

19.1

Lawful Intercept

The PTT system introduces support for standards-based X1 interface, which is fully compliant to ETSI TS 103 221-1.

The PTT system replaces the previous proprietary interface that used CLI commands over SSH. The ETSI interface is HTTPS based and allows for dynamic management of DF destinations and more granular management of LI targets.

The PTT system also introduces support for X2 and X3 interfaces compliant to ETSI TS 103 221-2 with the IRI and CC payloads compliant to 3GPP TS 33.108 and ATIS 0700005 standards.

19.1.1

PTT Calling, Presence, IPA

The PTT system supports the X2 interface, which is fully compliant to the ETSI TS 103 221-2 format.

The IRI payloads are encapsulated within a binary wrapper structure as defined by the ETSI standard. Most of the IRI payloads are encoded in the ASN.1 formats as defined by the 3GPP TS 33.108. In contrast, the rest are encoded in the ASN.1 formats as defined by ATIS 0700005 + ATIS 1000678 standards as required by the United States lawful interception annexure within the 33.108 specification.

Similarly, the PTT system supports the X3 interface fully compliant to the binary wrapper structure as by the ETSI TS 103 221-2 standard. The communication content payload for PTT voice calling and MCVideo calling features are encoded in the ASN.1 format as defined by the ATIS 0700005 + ATIS 1000678 standards as required by the United States lawful interception annexure within the 33.108 specification.

19.1.2

Integrated Secure Messaging

LEA uses the same X1 interface to identify the LI target for the interception of the Integrated Secure Messaging (ISM) feature.

The PTT system also introduces support for the 3GPP and ETSI standards-based lawful interception interfaces for ISM. This replaces the previous proprietary interface where the ISM messages were periodically pushed from the PTT system towards the DFs over SFTP as compressed ZIP files. As described for lawful interception for PTT calling and other features, ISM lawful interception also uses the binary wrapper structures defined by the ETSI standards for both X2 and X3. Similarly, the IRI and CC payloads are encoded in the ASN.1 formats defined by 3GPP TS 33.108. Due to the nature of the ISM feature where large multimedia files or other documents may be attached, the events' actual reporting may not be real-time if there are other ongoing ISM interceptions. For formats allowed as attachments to ISM, see [Media Types on page 69](#) for more details.

19.2

Retrieval of Stored Communications (PSC)

Preservation of Stored Communications (PSC) consists of all communication between users that is stored by the platform including all historic information. These features are configured system-wide by Unified Communications Operations.

The PTT solution provides access to PTT-related stored communications on the server for a PTT subscriber. Any communication that is not transient between users when a request is made for Stored Communication is stored by the platform. All historic information that is stored by the platform is provided.

PTT platform provides a mechanism to retrieve and report all Previously Stored Communications for specific PTT subscribers. The request to retrieve such communication is based on a valid warrant against these PTT subscribers (LI subjects). This is expected to be a one-time operation. When the LI subject is added to the PTT system, PTT platform does not prohibit LI users from issuing the retrieval command for PSC multiple times. Each time the retrieval is performed, the PTT platform reports all stored PTMsg communication available in the PTT platform at the time the retrieval command is issued.

PSC is retrieved and reported as a zip file containing separate JSON files containing IRI data for each PTMsg, JSON metadata file for each PTMsg and separate files in their respective formats for each attachment. These files are first created/collected in the file system, combined into one or more zip files and transferred to a specified DF server over SFTP. Each zip file has a maximum size of 1GB. If the total size of all PTX messages exceeds this limit, multiple zip files created since the operation to retrieve PSC for specified LI subject take some time to complete. The PTT platform also provides an additional command to check the status of the retrieval operation.