SmartPTT PLUS 9.14.100

Installation and Configuration Guide

January 2025

Elcomplus, Inc.

Revision History

Revision	Description	Date
7.1	Eleventh release of the document. The document is compliant with SmartPTT PLUS 9.14.100 Modified: Adding and Editing Groups in Capacity Max, Capacity Max, Installing on New Computer, Profiles, Managing Profiles, Restoring Event Log Database, Restoring Monitoring Database, Restoring User Database, Event Log Database, Monitoring Database, Configuring Desktop Clients Connection, Available Actions.	January 2024
7.0	Tenth release of the document. The document is compliant with SmartPTT PLUS 9.14.	December 2024
6.0	Ninth release of the document. The document is compliant with SmartPTT PLUS 9.13.	April 2023
5.0	Eighth release of the document. The document is compliant with SmartPTT PLUS 9.12.	November 2022
4.0	Seventh release of the document. The document is compliant with SmartPTT PLUS 9.11.	July 2022
3.0	Sixth release of the document. The document is compliant with SmartPTT PLUS 9.10.	October 2021
2.1.1	Fifth release of the document. The document is compliant with SmartPTT PLUS 9.8.1.	August 2021
2.1	Fourth release of the document. The document is compliant with SmartPTT PLUS 9.8.1.	November 2020
2.0	Third release of the document. The document is compliant with SmartPTT PLUS 9.8.	October 2020
1.1	Second release of the document. The document is compliant with SmartPTT PLUS 9.7.2.	July 2020
1.0	Initial release of the document. The document is compliant with SmartPTT PLUS 9.7.1. The document substitutes the following ***outdated*** manuals: SmartPTT PLUS Installation and Configuration Guide, SmartPTT PLUS Radioserver Configurator User Guide, SmartPTT PLUS System Requirements	May 2020

Contents

About This Document

This document describes installation, configuration, and the following maintenance of the SmartPTT dispatch software. The document is intended for engineers who have an experience of the client—server software configuration for Windows operating systems.

Additional Information

The document does ***not*** contain information about dispatch console configuration and use. All the corresponding information is available in *SmartPTT Dispatcher Guide*.

The document does ***not*** contain information related to the Windows computer administration as well as the radio device configuration. The only exceptions is being made for parameters that are required for SmartPTT configuration. All the corresponding information can be obtained from the following sources:

Source	***Description***
Microsoft Docs	Microsoft documentation storage for end users, developers, and IT professionals.
MOTOTRBO™ Systems	Information on MOTOTRBO family of products by Motorola Solutions.

If you need assistance in radio devices configuration or computer administration, submit a request to SmartPTT Technical Support Center.

1 Preliminary Configuration

Before the SmartPTT installation, various preliminary actions must be performed. The following information describes the required configuration without providing details and instructions for its implementation.

1.1 Addressing

SmartPTT operates in IP networks that use Internet Protocol version 4 (IPv4). Only dot-decimal notation for IP addresses representation is supported. SmartPTT does not support IPv6.

SmartPTT software can be installed on computers with multiple active IP addresses. At the same time it may require to select specific IP addresses to connect to various services or devices.

SmartPTT partly supports domain names. For example, the SmartPTT Radioserver address can be set as a domain name in the SmartPTT Dispatcher settings. However, in many other situations it is necessary to use exactly IP addresses.

Important
The use of domain names may require the support of the DNS server in the customer network or making changes to the Windows system files (for example, the ***hosts*** file).

Because some SmartPTT Radioserver settings require IP address selecting, IP addresses have to be fixed for each computer where the SmartPTT software is installed. For this, static IP addressing can be used or IP addresses should be assigned to MAC addresses over Dynamic Host Configuration Protocol (DHCP).

1.2 Authentication Types

SmartPTT supports the following authentication types:

- In the *Legacy* mode, you can use an account stored in the SmartPTT database to log in to SmartPTT.
- In the *Local* mode, you can use a local Windows account to log in to SmartPTT. The account must belong to the user group that exists on the SmartPTT computer.
- In the *Domain* mode, you can use a domain account to log in to SmartPTT. The account must belong to a user group that exists in the domain of the SmartPTT computer.

If the legacy authentication is used, the account name is case sensitive. If the local or domain authentication is used, then the account name is not case sensitive.

Required User Account Settings

SmartPTT has the following requirements to Windows user accounts:

- User accounts must be enabled.
- User password must not be expired at the moment of use.
- Users must not be required to change their passwords at the next logon.

SmartPTT provides the following user groups:

- *System Administrators* have access to the system configuration in SmartPTT Radioserver Configurator.
- *Database Administrators* can create, update, and restore databases.

- *Console Administrators* have an access to authorization in SmartPTT Dispatcher with the administrator rights, including the operator profiles creation and configuration. These users can select one of the existing databases to use in the system, but cannot create or update them.
- *Console Operators* can log in to SmartPTT Dispatcher and use its functions, but cannot configure it.

If you plan to use *Local* or *Domain* authentication in SmartPTT, before you install SmartPTT, in the Windows OS or on the domain server, it is recommended to create groups for System Administrators, Database Administrators, Console Administrators, Console Operators, and then place the required users to the created groups.

For information on creating Windows users see Creating Windows User and Creating Local User Group.

Automatic Authorization

You can configure automatic authorization under the current Windows account in SmartPTT Dispatcher. For this, a user with administrator permissions must add the name of the Windows user to the SmartPTT Dispatcher operators list. Both local and domain accounts can be used for automatic login.

1.2.1 Creating Windows User

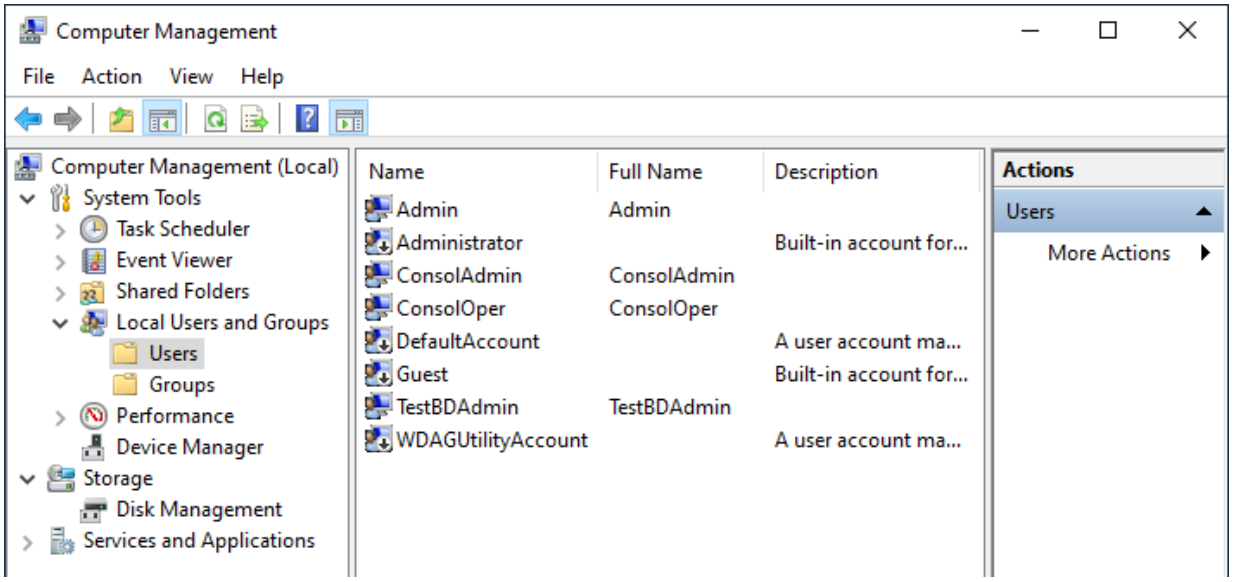
Follow the procedure to create Windows user accounts for SmartPTT.

Prerequisites:

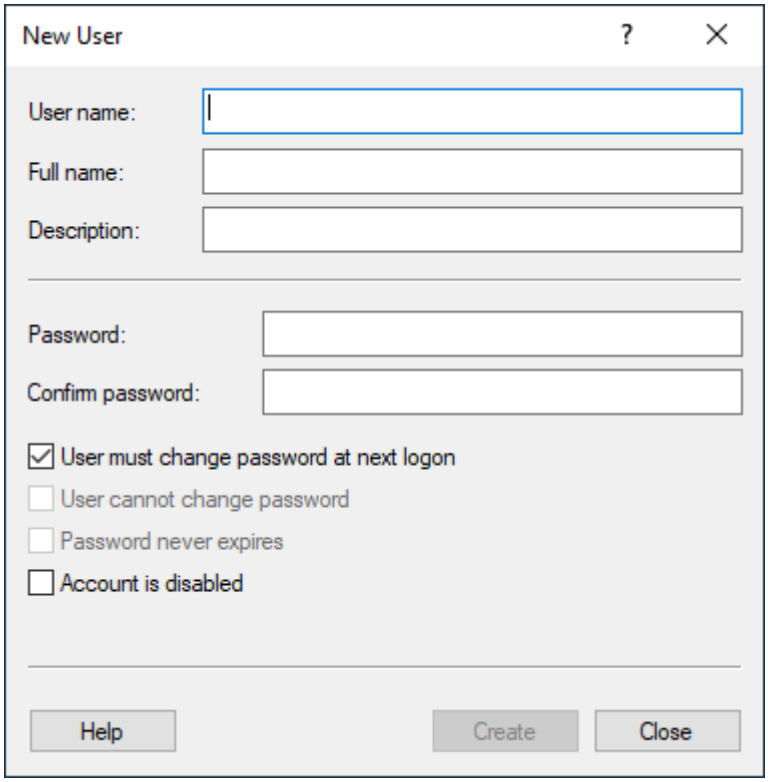
Log in to SmartPTT computer as a Windows administrator.

Procedure:

1. Right-click the ***Start*** button.
   The shortcut menu appears.
2. From the shortcut menu, select ***Computer Management***.



3. In the ***Computer Management*** window, on the left pane, expand ***System Tools → Local Users and Groups*** and click ***Users***.
4. On the right pane, click ***More Actions*** and select ***New User***.
   The ***New User*** window appears.



5. Configure the new user account:
   a. In the ***User name*** field, type the user name (login).
   b. In the ***Password*** field, type the user password.
   c. In the ***Confirm password*** field, type the password again.
   d. Clear the ***User must change password at next logon*** check box.
   e. Clear the ***Account is disabled*** check box.
   f. *(Optional)* To prevent the user from changing their password, select the ***User cannot change password*** check box.
   g. *(Optional)* To prevent the password from expiring, select the ***Password never expires*** check box.
   h. At the bottom of the window, click ***Create***.
6. Repeat the previous step to create another user account.
7. At the bottom of the window, click ***Close*** to close it.

1.2.2 Creating Local User Group

Follow the procedure to create Windows user groups for SmartPTT.

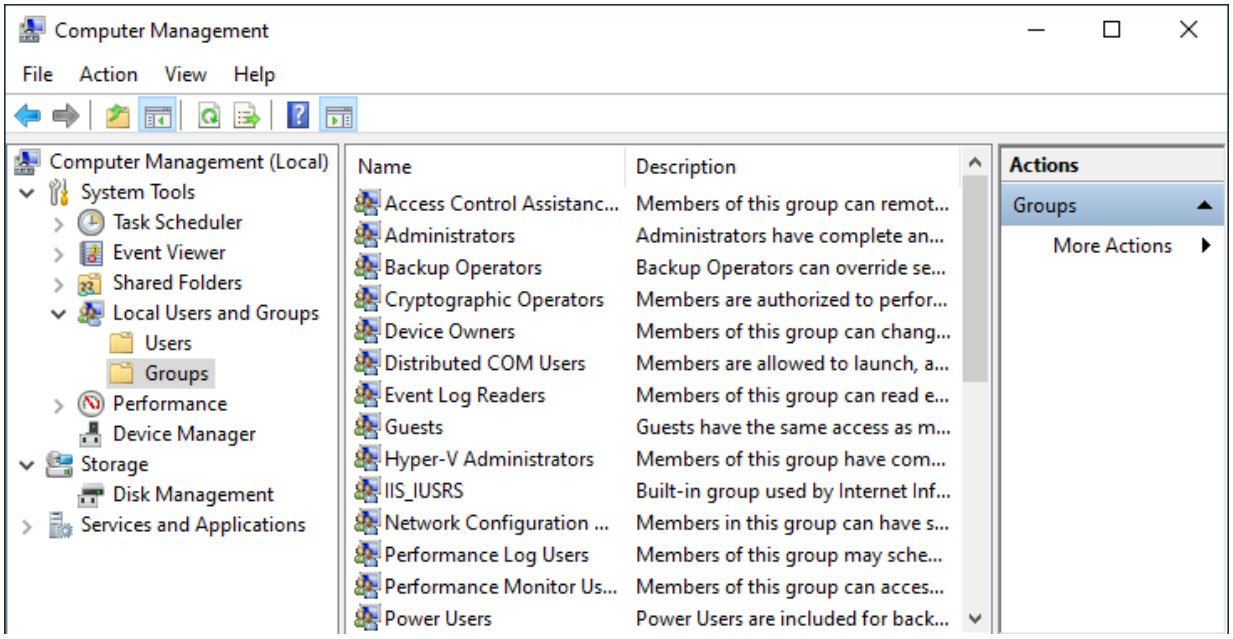
Prerequisites:

- Log in to SmartPTT computer as a Windows administrator.
- Create all desired Windows user accounts. For details, see Creating Windows User.

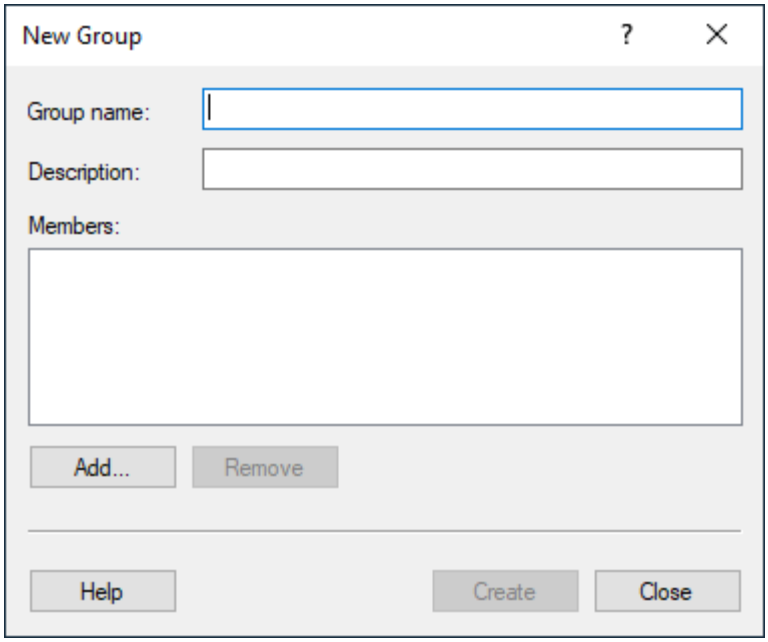
Procedure:

1. Right-click the ***Start*** button.
   The shortcut menu appears.

2. From the shortcut menu, select ***Computer Management***.
3. In the ***Computer Management*** window, on the left pane, expand ***System Tools*** → ***Local Users and Groups***, and then click ***Groups***.



4. On the right pane, click ***More Actions*** and select ***New Group***.
   The ***New Group*** window appears.



5. In the ***Group name*** field, enter a name of the group.
6. Add users to the group:
   a. In the ***New Group*** window, click ***Add***.
   b. In the window that appears, click ***Locations***.
   c. In the window that appears, select the local computer and click ***OK***.

d. In the ***Enter the object names to select*** field, type the desired Windows user name and click ***Check Names***.
In the field, the user name appears in the *<hostname>/<username>* format and is underlined.

e. *(Optional)* To add another user, type their name in the ***Enter the object names to select*** field without a preceding space or punctuation mark.

f. In the ***Select Users*** window, click ***OK***.

7. In the ***New Group*** window, click ***Create***.

Postrequisites:

Repeat the procedure to create more groups.

1.3 Disk Space Estimation

SmartPTT software uses disk space on the computer as follows:

- The installed SmartPTT Radioserver (primary or redundant) uses 350–400 MB.
- The installed SmartPTT Dispatcher application occupies 350–400 MB.
- A database management system (DBMS) manages several databases. The maximum database size is determined by the SQL server.
- SmartPTT stores downloaded maps and plans in the file system or database. For details, see “Positioning” in *SmartPTT Dispatcher Guide*.
- If necessary, each SmartPTT component can be configured to create and manage backup copies of databases.
- If necessary, each SmartPTT component can provide records of voice transmissions independent of each other and save them as audio files on local or network storage.

To estimate the required space and select the appropriate drive, it is necessary to consider all the aspects mentioned above.

If you require an assistance in free disk space calculations, contact the Elcomplus, Inc. representative in your region.

Voice Transmission Records

Records of voice transmissions are saved to a hard disk as unencrypted audio files in MP3, OGG or WAV format. They can be stored both on local and network file storage. To access the folder, only the file protocol must be used; other protocols are not supported. Either it is possible to access the folder without authorization.

The one minute voice transmission takes approximately 300 KB (B). To estimate the required space, consider the following:

- The average number of recorded voice transmissions during the working day or shift (N).
- The average duration of voice transmissions during the working day or shift (D).
- Storage duration of voice transmissions (P).
- The safety factor assuming the excess of real values over the average (R).

To estimate the required disk space, the specified parameters have to be multiplied with each other. If necessary, the result must be converted to the required units of measure.

$$C = B \cdot N \cdot D \cdot P \cdot R$$

EXAMPLE

In a system with 200 active radios every 5 minutes (N = 200 / 5 = 40 calls/min) the 12 seconds call is registered (D = 0.2 min). If records are stored for 100 days (P = 100 · 24 · 60 = 144,000 min), and the safety factor R = 1.5, then a storage with volume (C) is needed = 518,400,000 KB = 519 GB.

1.4 Positioning Services

SmartPTT supports outdoor and indoor positioning services.

- For information on outdoor positioning services, see Outdoor Positioning Services.
- For information on indoor positioning services, see Indoor Positioning Services.

1.4.1 Outdoor Positioning Services

SmartPTT supports various types of maps. They are as follows:

- Maps that are available over HTTP.
- Maps that are available in the file storage.
- Maps that are available in the database.

NOTE
The size of the map in the database is limited by the database size. For example, the maximum database size in the SQL Server Express is 10 GB.

For information on different types of maps, see “Maps” in *SmartPTT Dispatcher Guide*.

If necessary, SmartPTT supports authorization in the HTTP map server. Authorization settings must be as follows:

- The server must accept credentials in the URL as text (for example, *http://maps.company?password=passwordtext*).
- The server must provide free access to maps (without authorization).

Google Maps and Baidu Maps require a valid API key. To obtain the key, contact the Elcomplus, Inc. representative in your region.

SmartPTT supports operation with address services. These services display information about the object address by its geographical coordinates on a map. For this, Google and OpenStreetMap address services are used.

1.4.2 Indoor Positioning Services

SmartPTT supports indoor positioning service for continuous control over customer's employees movement inside buildings.

SmartPTT supports the following technologies and equipment of indoor positioning services:

- Motorola Solutions (iBeacon technology).
- BluFi Wireless.
- Kilchherr Elektronik AG.

To display location of customer's employees, files with floor/building plans should be uploaded to SmartPTT Dispatcher. Both raster (bitmap) and vector images are supported. For details, see “Indoor Tracking” in *SmartPTT Dispatcher Guide*.

For information on third party products that are required for Indoor Tracking, see Third Party Products.

1.4.3 Online Map Keys

Some map providers require SmartPTT to use specific keys. This affects the following maps:

- Google Maps. For details, see Google Map Keys.
- Baidu Maps. For details, see Baidu Map Keys.

Other maps are not affected.

1.4.3.1 Google Map Keys

To use Google Maps in third-party applications, Google forces developers and customers to use API keys. Keys unlock the following features:

- Tracking service.
- Address service.

These features are determined by the following Google API modules:

- Maps JavaScript API.
- Places API.

All of those APIs must be activated in the customer API key.

> ***NOTE***
> For SmartPTT Mobile users, individual generation of an API key is not required, since the key is already embedded in the application.

API Key Generation

To generate API key, the following actions must be performed:

- Project must be created (or exist) in the Google Cloud Platform. For details, see Creating and Managing Projects in the Google Cloud website.
- In the project settings, the ***Application Restrictions*** parameter must be set to *None* or *HTTP referrers*.
- In the same project settings, the ***API Restrictions*** parameter must be set to *Select API*.
- Required API modules must be included in the key:
  - For information on the Maps JavaScript API inclusion to the key, see Get an API Key (Maps JavaScript API) on the Google Maps Platform website.
  - For information on the Places API inclusion to the key, see Get an API Key (Places API) on the Google Maps Platform website.
- Billing ***must be*** activated for API modules:
  - For information on the Maps JavaScript API billing, see Maps JavaScript API Usage and Billing on the Google Maps Platform website.
  - For information on the Places API billing, see Places API Usage and Billing on the Google Maps Platform website.

Important
If you will not use billing, you may lose Google Maps features for reasons beyond the SmartPTT operation. For details, submit a request to the Google Maps Support Team.

If you need an assistance in the key generation, submit a request to the SmartPTT Technical Support Center.

1.4.3.2 Baidu Map Keys

Using Baidu Maps in SmartPTT requires developers and customers to enter API keys. These keys provide the ability to use Baidu maps to track the object location.

NOTE
For SmartPTT Mobile users, individual generation of an API key is not required, since the key is already embedded in the application.

API Key Generation

To generate API key, the following actions must be performed:

- An account must be created at http://passport.baidu.com. You will need a valid email address and password.
- A developer account must be created at http://developer.baidu.com/user/reg. You will need to confirm your mobile phone number by entering the code sent via SMS.
- API key generation must be completed at http://lbsyun.baidu.com/apiconsole/key.

1.5 NTP Services

Some MOTOTRBO network elements support Network Time Protocol (NTP) to adjust dates and times. The elements are as follows:

- SRL series repeaters
- XRC controllers
- XRT voice gateway
- Capacity Max System Server (CMSS)
- MOTOTRBO Network Interface Service (MNIS) host
- Device Discovery and Mobility Service (DDMS) host

It is recommended to connect all computers of the SmartPTT dispatch subsystem to the same NTP server that is used by repeaters or other system infrastructure components. If the NTP server will be one of these computers (for example, the SmartPTT Radioserver host), then either the corresponding service must be configured in its operating system (W32Time) or third-party solutions should be used.

1.6 Power Saving Mode

To optimize power consumption, the function of switching to power saving mode (sleep mode, hibernation mode, or automatic turning off) may be activated in the Windows operating system.

Important
The power saving mode must be disabled on the radioserver computer. If dispatch consoles must continuously record voice transmissions or information about events, power saving mode must be disabled on them too.

This requirement does not concern the automatic screen lock mode that does not affect the performance of the SmartPTT software components.

1.7 Date and Time Format

SmartPTT Radioserver and SmartPTT Dispatcher record to the database date and time of events in Coordinated Universal Time (UTC) format. These date and time formats are not easy to read. Therefore, in SmartPTT Dispatcher they are converted to the following formats:

- The time is displayed in the long time format specified in the operating system.
- The date is displayed in the short date format specified in the operating system.

Date and time formats are specified in the regional settings of the operating system. The settings are applied each time SmartPTT Dispatcher is started and remain unchanged during the session.

1.8 Generating HID with a Standalone Utility

Follow the procedure to obtain the hardware identifier (HID) required to order the SmartPTT license before installing the software.

Prerequisites:

- For each computer with at least one installed SmartPTT component, finalize SmartPTT hosts specifications and operating system language settings.
- Determine the desired license.
  For information on SmartPTT licenses, contact the Elcomplus, Inc. representative in your region.
- From the SmartPTT Technical Support Center, obtain the utility for HID generation.

Procedure:

1. Start the utility (HID.EXE file) on the SmartPTT Radioserver host.
2. Ensure that HID appears in the ***Hardware ID*** field.
3. Perform one of the following actions:

To copy HID to the clipboard,	click ***Save to clipboard***.
To save HID to a file,	click ***Save to file***.
To send an email,	perform the following actions: 1. In the ***Company*** field, type the company name acquiring the license.

2. Click ***Send E-mail***.

Postrequisites:

- Send the information to the Elcomplus, Inc. representative to purchase a license file.
- Install the received license file after installing the software. For details, see Installing License.

1.9 Firewall Configuration

Firewall configuration is required for uninterruptible connection between SmartPTT components and communication systems. All port numbers below are default ones. They can be changed if required. However, some port ranges are limited. For details, see the corresponding documentation and/or embedded help files.

1.9.1 Firewall Conventions

List of ports that must be unlocked for uninterruptible communication is available in the table view. Corresponding tables consist of the following columns:

Local Port

Number of the port that is used by the host described. In the column, the following options are available:

- *any* — port number is selected automatically.
- *<port number>* — default port number.
- *<port number>** — port number can be used for simultaneous use by multiple connections.

Protocol

Type of the transport protocol that is used for data provision. In the column, the following options are available:

- *TCP* — transmission control protocol.
- *UDP* — user datagram protocol.

Role

Role of the host described in establishing a connection. In the column, the following options are available:

- *Server* — host that can receive incoming connections from remote device/service.
- *Client* — host that can initiate the connection to remote device/service.
- *Peer* — host that can receive and initiate connections to remote device/service.

Remote Device/Service

Description of devices or services which interact with the host described.

Remote port

Port number that is used by the corresponding remote device or service.

Description

Explains what the port is used for.

Brief description of each connection is provided in the table before the connection parameters (port numbers, quantities, etc.).

1.9.2 Radioserver Host

Table below provides information about network ports that must be unlocked on the radioserver computer. For information on table conventions, see Firewall Conventions.

- DBMS Connection
- MOTOTRBO Radio Systems
  - IP Site Connect / Capacity Plus / Linked Capacity Plus / ERDM (network application interface)
  - Capacity Plus (direct interface)
  - Capacity Plus Multi-Site (Linked Capacity Plus)
  - Capacity Max
  - Connect Plus
- Control Stations
  - Local MOTOTRBO Control Station
  - Remote RG-1000e/RG-2000
- Clients
  - Desktop Client
  - Web Client
  - SmartPTT Mobile
  - Third-Party Apps
- Services
  - Email
- Add-on Modules
  - Option Board Features
  - Indoor Tracking using Kilchherr
  - NexLog Recording System
  - Avigilon Connection
  - Phone Line Connection over SIP trunk
  - Network Monitoring

DBMS CONNECTION

Local Port	*Protocol*	*Role*	*Remote Device/Service*	*Remote Port*	*Description*
any	TCP	Client	Microsoft SQL	1433	Database Engine connection

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
any	UDP	Client	Microsoft SQL	1434	Browser Service connection

IP SITE CONNECT / CAPACITY PLUS / LINKED CAPACITY PLUS / ERDM

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
50000	UDP	Peer	Repeater MOTOTRBO	50000	Control commands, data and voice traffic exchange
any	TCP	Client	Motorola DDMS	3000	Radio registration data receiving
any	TCP	Client	Motorola DDMS	5055	Radio users data receiving
any	TCP	Client	MNIS Data Gateway	55000	Control commands and data exchange in TCP connection mode
4001	UDP	Peer	MNIS Data Gateway	4001	Radio location data receiving and sending over LRRP protocol and MNIS
5017	UDP	Peer	MNIS Data Gateway	5017	Radio location update over LIP protocol and MNIS
4007	UDP	Peer	MNIS Data Gateway	4007	Text message sending and receiving over MOTOTRBO Advanced protocol and MNIS
4008	UDP	Peer	MNIS Data Gateway	4008	Telemetry data and remote control commands receiving over MNIS

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description

MOTOTRBO™ CAPACITY PLUS MULTI-SITE (LINKED CAPACITY PLUS)

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
50000	UDP	Peer	MOTOTRBO repeater	50000	Control commands, data and voice traffic exchange
any	TCP	Client	Motorola DDMS	3000	Radio registration data receiving

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
any	TCP	Client	Motorola DDMS	5055	Radio users data receiving
any	TCP	Client	MNIS Data Gateway	55000	Control commands and data exchange in TCP connection mode
5017	UDP	Peer	MNIS Data Gateway	5017	Radio location update over LIP protocol and MNIS
4001	UDP	Peer	MNIS Data Gateway	4001	Radio location update over LRRP protocol and MNIS
4007	UDP	Peer	MNIS Data Gateway	4007	Text message sending and receiving over MOTOTRBO Advanced protocol and MNIS
4008	UDP	Peer	MNIS Data Gateway	4008	Telemetry data and remote control commands receiving over MNIS

MOTOTRBO™ CAPACITY MAX

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
any*	TCP	Client	Server CMSS, TC	60015	Connection to the separate CMSS presence notification service (up to 5 connections available)
any*	TCP	Client	Server CMSS, VRC GW	56000	Connection to VRC MNIS (voice gateway; up to 15 connections available)
40000*	UDP	Peer	Server CMSS, VRC GW	56000	Voice data transmission between radioserver and voice gateway
51112	UDP	Server	Server CMSS, SysAdvisor	any	Monitoring data receiving
4001	UDP	Peer	MNIS Data Gateway	5017	Radio location update over LRRP protocol and MNIS
4007	UDP	Peer	MNIS Data Gateway	4007	Text message sending and receiving over MOTOTRBO Advanced protocol and MNIS
4008	UDP	Peer	MNIS Data Gateway	4008	Telemetry data and remote control commands receiving over MNIS
any.	TCP	Client	MNIS Data Gateway	55000	Control commands and data exchange in TCP connection mode

MOTOTRBO™ CONNECT PLUS

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
38000	TCP and UDP	Client	XRC controller	38000	Access to site repeater monitoring service that is hosted in XRC controllers
50005	TCP and UDP	Client	XRC controller	50005	Connection to the XRC controller radio registration service
50001	TCP and UDP	Client	XRC controller	50001	Connection to the radio location service that is hosted in XRC controllers
50007	TCP and UDP	Client	XRC controller	50007	Connection to the text message service that is hosted in XRC controllers
any	TCP and UDP	Client	XRT controller	10001	Control commands, data transmission
19000	UDP	Peer	XRT controller	any	Voice call reception and initiation

LOCAL MOTOTRBO CONTROL STATION

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
any	TCP	Client	MotoTRBO control station	8002	Control commands
5017	UDP	Peer	MotoTRBO control station	5017	Radio location updates over LIP
4001	UDP	Peer	MotoTRBO control station	4001	Radio location updates over LRRP
4005	UDP	Peer	MotoTRBO control station	4005	Information on the presence of a radio on the network
4007	UDP	Peer	MotoTRBO control station	4007	Incoming and outgoing text messages
4008	UDP	Peer	MotoTRBO control station	4008	Telemetry data and remote control commands receiving over MNIS

REMOTE RG-1000e/RG-2000

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
30010	TCP	Client	RG-1000e	30010	Control commands
any	UDP	Peer	RG-1000e	30010	Voice call reception and initiation
any	UDP	Peer	RG-1000e	30010	Radio location updates
any	UDP	Peer	RG-1000e	30010	Incoming and outgoing text messages

DESKTOP CLIENT

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
8888	TCP	Server	AWS	any	Control commands and data transmission commands
18500*	UDP	Peer	AWS	18501	Voice traffic transmission

WEB CLIENT

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
8443*	TCP	Server	Web-client	any	Control commands and data transmission commands
18500	UDP	Server	Web-client	3478	STUN service
18500*	UDP	Peer	Web-client	18501	Voice traffic transmission

SMARTPTT MOBILE

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
8443*	TCP	Server	SmartPTT Mobile	any	Control commands and data transmission commands
18500*	UDP	Peer	SmartPTT Mobile	18501	Voice traffic transmission

THIRD-PARTY APPS

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
8191*	TCP	Server	Third-party API	any	Application connection
18500*	UDP	Peer	Third-party API	any	Voice call reception and initiation

EMAIL SERVERS

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
any	TCP	Client	POP3	110 or 995	Email Message Reception
any	TCP	Client	IMAP	143 or 993	Email Message Reception
any	TCP	Client	SMTP	25, 587, 465	Email Message Transmission

OPTION BOARD FEATURES

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
4010	UDP	Client	MOTOTRBO control station	4010	Movement reports

INDOOR TRACKING USING KILCHHERR

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
3100	UDP	Client	MOTOTRBO control station	3100	Location reports reception

NEXLOG RECORDING SYSTEM

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
any	UDP	Client	NEXLOG server	13000-13200	Voice traffic transmission

AVIGILON CONNECTION

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
any	TCP and UDP		Avigilon service	any	

PHONE LINE CONNECTION OVER SIP TRUNK

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
5060	TCP or UDP	Peer	PBX IP	TCP or UDP	SIP protocol signaling

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
18650-18950	UDP	Peer	PBX IP	UDP	Media sending and receiving

NETWORK MONITORING

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
any	UDP	Client	SNMP device	161	Sending SNMP requests and commands from server to device
162	UDP	Server	SNMP device	any	Sending SNMP notifications from device to server

1.9.2.1 Connect Plus Ports

In Connect Plus, UDP ports that are related to the voice call reception and initiation are used according to the following rules:

- Each voice call requires UDP connection.
- Port numbers are ***not*** fixed to talkpaths.
- Port numbers are allocated starting the one that is configured in SmartPTT Radioserver Configurator (default value is *19000*). For details, see Configuring Connection to Connect Plus.
- Maximum number of ports is determined by the number of voice call IDs configured in all XRT gateways. For details, see Adding and Editing XRT Gateways.

If SmartPTT is connected to multiple Connect Plus radio systems, each system must have its own range of UDP ports for voice calls. Port ranges must be different.

EXAMPLE

SmartPTT is planned to be connected to the second Connect Plus radio system. In the first system, it is able to monitor up to 40 simultaneous voice calls. In it, the first UDP port for voice calls (UDP Start Port) is 19000.

In this case, firewall must be configured in the following way:

- For the first system, 40 UDP ports must be unlocked. They are ranged from 19000 to 19039.
- For the second system, the UDP Start Port must be 19040 or more. Number of ports is determined by the number of simultaneous calls that SmartPTT will monitor in that system.

1.9.3 Dispatch Console Host

Table below provides information about network ports that must be unlocked on dispatch console computers. For information on table conventions, see Firewall Conventions.

Local Port	Protocol	Role	Remote Device/Service	Remote Port	Description
any	TCP	Client	Server SmartPTT	8888	Control commands and data transmission commands
18501	UDP	Peer	Server SmartPTT	18500	Voice traffic exchange over RTP
18501	TCP	Peer	AWS	18501	Connection to another dispatch console and data transmission
5060	TCP or UDP	Client	PBX IP	5060	Connection to PBX over the SIP protocol (transport protocol depends on PBX settings)
18700-18750	UDP	Peer	PBX IP	any	Voice reception and transmission between dispatch console and PBX

2 System Requirements

Certain requirements need to be satisfied in order to successfully install and use SmartPTT. These include hardware, software and infrastructure requirements and are described in the following section.

2.1 Minimum System Requirements for SmartPTT Dispatcher

Software Requirements

SmartPTT Dispatcher can be installed and used on Windows computers only.

OS Family	*Version*
Windows 11	Pro (64 bit)
Windows 10	Pro version 1909 or later (64 bit)
	Enterprise 2016 LTSB (64 bit)
Windows 8.1	Windows 8.1 (64 bit)
	NOTE Windows 8.1 must have the latest updates or the KB 2919355 update. For details, see Microsoft Support information.

NOTE
To ensure operating system security and SmartPTT stable operation, it is recommended to install the latest Windows updates.

Hardware Requirements

Processor:	Intel® Core™ i5 (7th generation or higher) for systems with less than 3,000 subscribers.
	Intel® Core™ i7 for systems with more than 3,000 subscribers or activated GPS/Monitoring/Indoor services.
Memory (RAM):	4 GB for systems with less than 3,000 subscribers.
	8 GB for systems with more than 3,000 subscribers or activated GPS/Monitoring/Indoor services.
Storage:	7200 rpm SATA drive.
	20 GB space for software and database.
Graphics adapter:	1 GB RAM PCI-E or similar CPU-integrated for systems with voice transmission only.
	2 GB RAM PCI-E or similar CPU-integrated for systems with activated GPS/Monitoring/Indoor services.
Monitor:	display size: 23”

	screen resolution: 1366 × 768 px
	color depth: 16 bit
Input/output ports:	1 input port per input device or Human Interface Device (HID).
	1 analog audio output per playback device (speaker or headset).
	1 audio input per microphone.
Sound adapter:	Multichannel sound adapter.
Audio recording device:	A microphone or a headset.
Playback device:	Headphones or a headset.
LAN:	10/100/1000 Mbps Ethernet adapter.
Pointer:	A mouse or a trackball.
Keyboard:	A standard keyboard.

NOTE
These are standard system requirements for SmartPTT Dispatcher. They can change depending on the configuration, complexity and/or workload of the system.

NOTE
We have experienced issues with USB ports on Dell PCs that cause audio peripherals to disconnect. For this reason we recommend installing SmartPTT on HP or other brands of PCs.

2.2 Minimum System Requirements for SmartPTT Radioserver

Software Requirements

SmartPTT Radioserver can be installed on Windows computers only.

OS Family	***Version***
Windows 11	Pro (64-bit)
Windows Server	Windows Server 2019
	Windows Server 2016
	Windows Server 2012 R2
Windows 10	Pro version 1909 or later (64-bit)
	Enterprise 2016 LTSB (64-bit)
Windows 8.1	Windows 8.1 (64-bit)

OS Family	Version
	NOTE Windows 8.1 must have the latest updates or the KB 2919355 update. For details, see Microsoft Support information.

NOTE
To ensure operating system security and SmartPTT stable operation, it is recommended to install the latest Windows updates.

Hardware Requirements

Processor:	Intel® Core™ i5 (7th generation or higher) for systems with less than 3,000 subscribers.
	Intel® Core™ i7 for systems with more than 3,000 subscribers or activated GPS/Monitoring/Indoor services.
Memory (RAM):	4 GB for systems with less than 3,000 subscribers.
	8 GB for systems with more than 3,000 subscribers or activated GPS/Monitoring/Indoor services.
Storage:	7200 rpm SATA drive.
	40 GB space (software and database only).
	190 GB space (software, database, and voice records).
Input/output ports:	1 USB port per connected USB device (mouse, speaker, etc.)
	(Optional) 1 analog audio output per speaker
	(Optional) 1 analog audio input per microphone
LAN:	10/100/1000 Mbps Ethernet adapter.

NOTE
These are standard system requirements for SmartPTT Radioserver. They can change depending on the configuration, complexity and/or workload of the system.

NOTE
We have experienced issues with USB ports on Dell PCs that cause audio peripherals to disconnect. For this reason we recommend installing SmartPTT on HP or other brands of PCs.

2.3 Networking Requirements

2.3.1 Network Quality

Computer networks where SmartPTT is installed and used, must comply with the following requirements:

Parameter	Value
Packet Loss	Slightly distorted voice: 0.0–2.5 %
	Distorted voice: 2.5–15.0 %
Two-Way Delay	Radio network connection: 0–90 ms
	PBX connection: 0–60 ms
Jitter	Radio network connection: 0–90 ms
	PBX connection: 0–60 ms

IP access to the radio network means the connection to hardware/software solution that provides access to the radio network:

- Connection to the RG-1000e or RG-2000 device.
- Connection to repeaters:
  - Master repeater (for voice calls and monitoring).
  - Other repeaters (for monitoring).
- Connection to a computer with a MNIS Data Gateway Relay application.
- Connection to a computer with Device Discovery and Mobility Service (DDMS).
- Connection to the XRC controller (Connect Plus).
- Connection to the XRT gateway (Connect Plus).
- Capacity Max System Server (CMSS) connection.

NOTE
Motorola radio hardware may have more specific requirements for the above parameters. For this information, refer to the respective hardware documentation.

2.3.2 Bandwidth Requirements

Computer networks where SmartPTT is installed and used must provide specific bandwidth between the computer with SmartPTT Radioserver and the other IP devices of the dispatch system. All following requirements are applicable to one-way transmissions.

Voice transmission

All following requirements are applicable to a single voice stream.

Source/Target	Minimum	Comments
SmartPTT Dispatcher application	13 kbps	For DMR vocoder
	100 kbps	For G.711 vocoder
RG-1000e/RG-2000 radio gateway	from 65 kbps	Exact value depends on vocoder parameters
Master repeater	20 kbps	
XRT Gateway	20 kbps	Applicable to Connect Plus only
Capacity Max System Server	20 kbps	
PBX	65 kbps	For G.729 or Speex vocoders
	100 kbps	For G.711 vocoder
Applications that use SmartPTT WebSocket	from 65 kbps	For each of the following applications: • SmartPTT Web Client • SmartPTT Mobile • Third Party app over SmartPTT Server API Exact value depends on vocoder parameters.

Required bandwidth should be increased if you use the bridging, cross patches, conference calls, or voice communication between dispatchers. For details on increased bandwidth, contact Elcomplus, Inc. representative in your region.

If you have an alternate/redundant SmartPTT Radioserver, the bandwidth to that computer must comply with the synchronization settings between the main and redundant servers.

Voice traffic between SmartPTT Dispatcher applications (the Dispatchers feature) is not sent to SmartPTT Radioserver. To provide this feature, the bandwidth between dispatcher computers must be 65 kbps or more per each configured contact.

Data transmisison

In SmartPTT, data transmisison includes text messages, indoor and outdoor location, telemetry information and control commands.

Source/Target	Minimum	Comments
SmartPTT Dispatcher application	3.5 kbps	For Enhanced CSBK location data from 10 subscribers and location update period 7.5 s
Master repeater	20.0 kbps	For each repeater without a revert channel
	45.0 kbps	For each repeater with a revert channel
Remote MNIS host	20.0 kbps	For each repeater without a revert channel
	45.0 kbps	For each repeater with a revert channel

Source/Target	Minimum	Comments
XRC controller	20.0 kbps	For each repeater without a revert channel
	45.0 kbps	For each repeater with a revert channel
Avigilon server	3150 kbps	For each camera. This value is obtained based on the following conditions: • Resolution is 1920 x 1080. • FPS is 25. • Service packets in stream no more than 5% of the video stream. • *H.264 Base codec - medium quality*. • Average dynamics of the image change.

Bandwidth must be increased if you activate and use the Bridging feature in SmartPTT Radioserver, create a cross patch, or organize a conference call.

If you have a redundant SmartPTT Radioserver, the bandwidth to that computer must comply with the synchronization settings between the main and redundant servers.

Monitoring service

Source/Target	Minimum	Comments
SmartPTT Dispatcher application	42 kbps	For each configured repeater if the ***Monitoring*** panel is closed
	45 kbps	For each configured repeater if the ***Monitoring*** panel is opened
Repeater	42 kbps	For each configured repeater

2.4 Support and Compatibility

2.4.1 MOTOTRBO Infrastructure

SmartPTT 9.14.100 has been tested and found compatible with the MOTOTRBO firmware and software listed in the table below.

WARNING
Different MOTOTRBO fimware and software versions may not be mutually compatible. For information on MOTOTRBO products compatibility, contact Motorola Solutions representatives in your region.

Firmware/Software	Version	Comments
Subscriber radio	M2024.01	

Firmware/Software	Version	Comments
Firmware	M2024.02 M2023.01 M2022.02 M2022.01 M2021.04	
Repeater Firmware	M2024.01 M2024.02 M2023.01 M2022.02 M2022.01 M2021.04	
Control Station Firmware	M2024.01 M2024.02 M2023.01 M2022.02 M2022.01 M2021.04	
MOTOTRBO Network Interface Services Software (MNIS)	M2024.01 M2024.02 M2023.01 M2022.02 M2022.01 M2021.04	Provides data transmission in IP Site Connect, Capacity Plus, and Linked Capacity Plus
Device Discovery and Mobility Service Software (DDMS)	03.100.5001	Provides radio registration information in IP Site Connect, Capacity Plus, and Linked Capacity Plus
XRC and XRT Firmware	R02.80.XX	Connect Plus only
Capacity Max System Server (CMSS) Firmware	M2024.01 M2024.02 M2023.01 M2022.02	

Firmware/Software	Version	Comments
	M2022.01	
	M2021.04	

Additional information on infrastructure:

- Within the radio system, all repeaters, subscriber radios and control stations should use the same or compatible firmware versions.
- If you activate the Bridging feature, you should bridge only the radio fleet objects which are associated with the same or compatible firmware versions.
- Access and operation in radio systems for SmartPTT require separate licensing.

2.4.2 Elcomplus Products

SmartPTT is compatible with the following Elcomplus, Inc. products:

Product	Version	Comments
Radio gateway RG-1000e	R3.X	Current version of firmware used on the device for control station remote connection and operation.
	R2.2	Previous version of firmware used on the device.
Radio gateway RG-2000	Any version	Version of firmware used on the device for control station remote connection and operation.

2.4.3 Third Party Products

SmartPTT is compatible with a range of third-party products. Below you will find a list of hardware and software products that proved to be compatible with the SmartPTT applications.

Database Management Systems

SmartPTT uses Microsoft SQL Server as a database. The following versions are supported:

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019 Express
- Microsoft SQL Server 2019 Enterprise

For information on use of other Microsoft SQL Server versions and editions, submit a request to SmartPTT Technical Support Center.

Option Boards

- Connect-RTLS RF800 (BluFi Wireless).
- K-TERM 44 (Kilchherr Elektronik AG).

Beacons

- Connect-RTLS RF800 (BluFi Wireless).
- K-TERM 70IC Beacon Transmitter (Kilchherr Elektronik AG).
- iBeacons.

Option Boards Software

SmartPTT supports MOTOTRBO™ option boards programmed using Tallysman Sprite Configurator. Use the version 0.3.16 for the Movement Reports Restoration feature.

Sound cards

- Internal PCI-E Sound Blaster Audigy RX.
- External Sound Blaster X-Fi Go.
- ESI MAYA44XTe.
- ICON Digital Cube Pro USB.

Accessories

SmartPTT supports HID-compliant devices. The devices listed below have been tested in SmartPTT and are fully compatible with it.

- Desktop USB microphone D-9 by Holmco
- Desktop USB microphone PS12/PS20 by pei tel
- Desktop microphone DM-160 by CXD
- Desktop USB microphone VM-1S™
- Desktop USB microphone TM-2 USB V2
- Desktop USB microphone VCC-3 USB Command Console
- Desktop USB microphone VCC-2 USB mini-Command Console
- Push-to-talk button PTT-13 by Imtradex
- USB corded headsets Blackwire C310-M and C320-M by Plantronics
- Yellow foot switch X-keys XK-3 USB Switch Interface by P.I. Engineering
- Modular console Tipro TM-HHA-6AW with analog interface without touchcomputer.

Hardware

- SmartPTT Dispatcher can be installed and used on BeFREE 10 computers.

- SmartPTT supports the IP Gear Claro 30 SIP-gateway (by ESTel) for access to analog telephone networks.
- SmartPTT can connect to NexLog recorders running under NexLog Recorder Software 2.8.2.
- SmartPTT can connect to Avigilon system cameras using the Avigilon Control Center Server 7 software.

NOTE
We have experienced issues with USB ports on Dell PCs that cause audio peripherals to disconnect. For this reason we recommend installing SmartPTT on HP or other brands of PCs.

2.5 Audio File Requirements

Audio files that will be used in SmartPTT must comply with specific requirements. This implies the following features:

- Voice notifications.
- Sounds used in SmartPTT Radioserver rules.
- Radioserver autoreply to phone users.

Parameter	***Value***
File format	MP3, OGG, or WAV ***Important*** File format and its extension must be the same.
Encoding algorithm	16-bit PCM
Sample rate	MP3: 8 kHz
	OGG: 8 kHz
	WAV: 8 kHz
Number of audio channels	single (mono audio)
Maximum volume level	−22 dBFS (−10 dBm)
Audio frequency parameters	range: 300–3400 Hz
	spectrum: continuous (not isolated tones) ***Important*** SmartPTT does not deliver single tone audio as well as isolated tones within audio.
Audio length	must not exceed transmission duration in radio network (~60 seconds)

3 Software Installation

3.1 Installing on New Computer

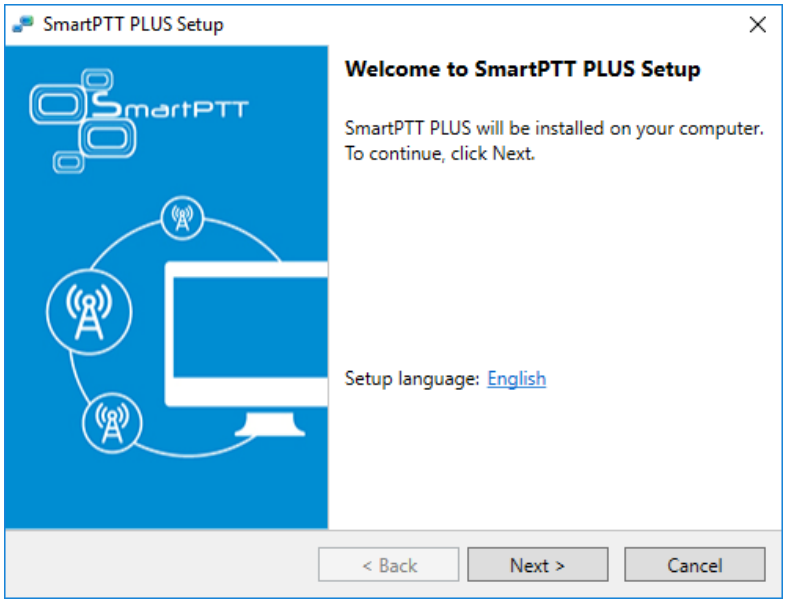
Follow the procedure to perform installation of SmartPTT for the first time.

Prerequisites:

- Log on to Windows as an administrator.
- Install Microsoft SQL Express.
- If you plan to use *Local* or *Domain* authentication in SmartPTT, before you install SmartPTT, in the Windows OS or on the domain server, it is recommended to create groups for System Administrators, Database Administrators, Console Administrators, Console Operators, and then place the required users to the created groups. For details, see Authentication Types.

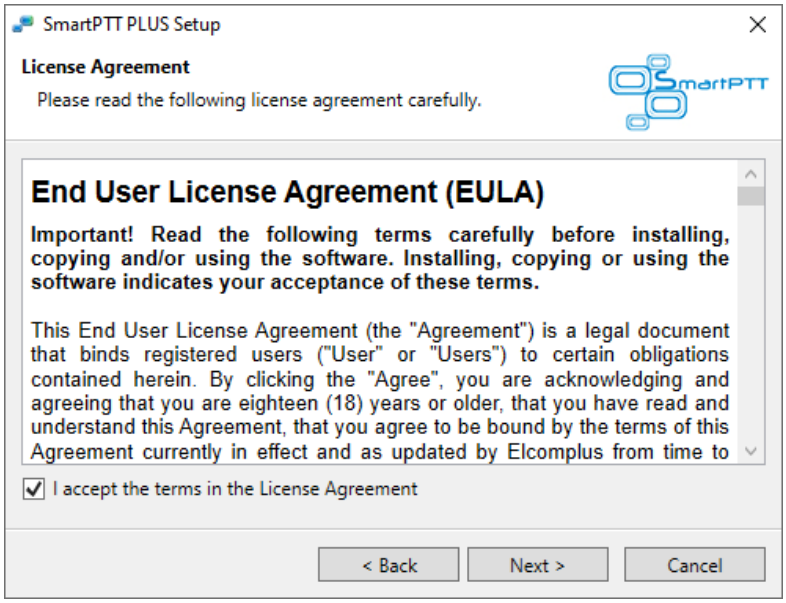
Procedure:

1. Start the installation file.

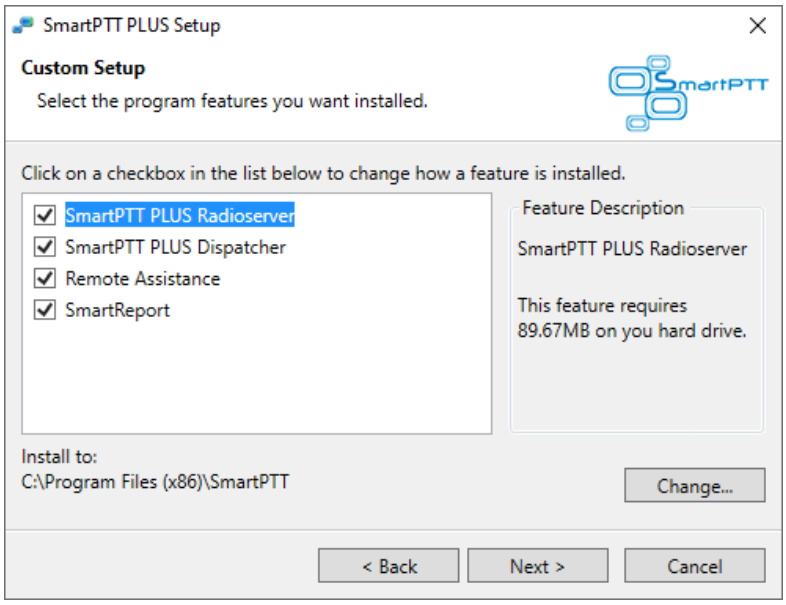


2. *(Optional)* In the welcoming window, change the installation language:
   a. Next to the ***Setup language*** heading, click the selected language.
   b. From the dialog box, select the required language, and then click ***Apply***.
   c. In the welcoming window, click ***Next***.
3. If .NET Framework is required to be installed, agree to install it.
   The ***License Agreement*** window appears.

Important
For Window 8.1, restart your computer after the .NET Framework installation. For other Windows versions, restart may not be required.



4. In the window that appeared, select ***I accept the terms in the License Agreement***, and then click ***Next***.
   The ***Custom Setup*** window appears.



5. In the window that appeared, select components that will be installed:

   a. Select the software component that must be installed on the computer.

NOTE
If the component is already installed, it will be selected and unavailable. It will not be re-installed.

   b. *(Optional)* For each of the required component, change the installation path:

      i. Click ***Change***.

      ii. In the dialog box, select the required path.

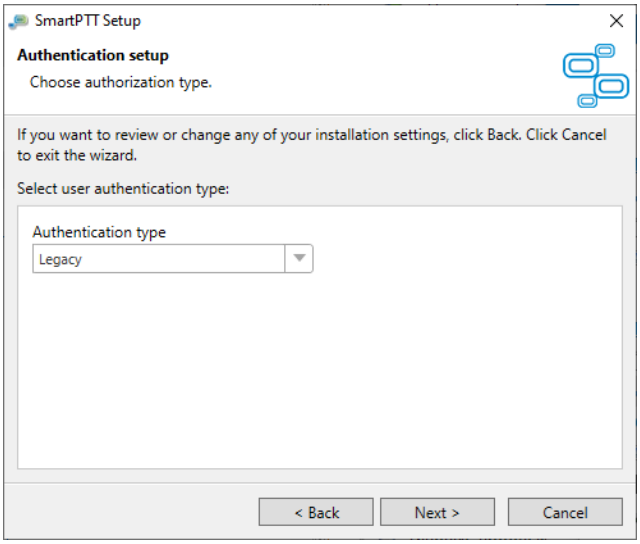
      iii. Click ***OK***.

Important
It is recommended to keep default installation paths unchanged.

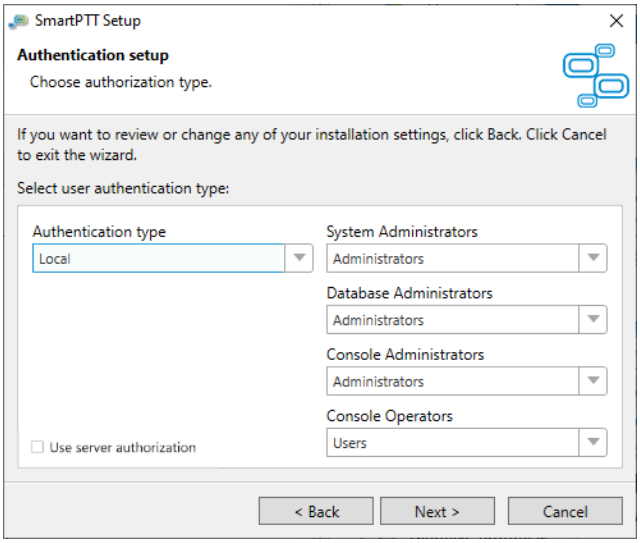
c. In the ***Custom Setup*** window, click ***Next***.
The ***Authentication setup*** window appears.

6. In the window that appears, select the desired user authentication type that will be used to login to SmartPTT:

To store authentication user data in SmartPTT,	from the ***Authentication type*** list, select *Legacy*.
To use local Windows accounts for authentication,	perform the following actions:



1. From the ***Authentication type*** list, select *Local*.



2. Select ***Use server authorization*** checkbox, to allow users to authorize in SmartPTT Dispatcher only when connection to the radioserver is available.

Important
The checkbox must be used only if you install SmartPTT Dispatcher. Otherwise, login issues occur.

3. From the ***System Administrators*** list, select one of the user groups who will be able to log in SmartPTT Radioserver Configurator and configure it.

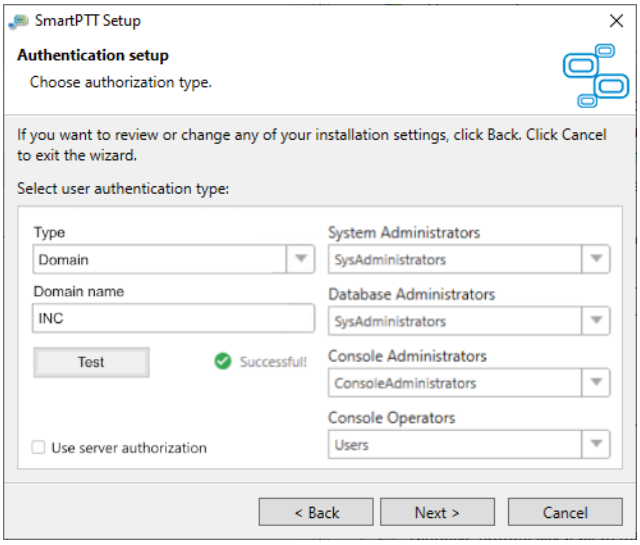
4. From the ***Database Administrators*** list, select one of the user groups who will be able to create, update, and restore databases.
5. From the ***Console Administrators*** list, select one of the user groups who will have an access to authorization in SmartPTT Dispatcher with the administrator rights, including the operator profiles creation and configuration. These users can select one of the existing databases, but cannot create or update them.
6. From the ***Console Operators*** list, select one of the user groups who will be able to log in SmartPTT Dispatcher and use its functions.

NOTE
Each list displays the groups that currently exist in Windows.

To use domain Windows accounts for authentication,

perform the following actions:

1. From the ***Authentication type*** list, select *Domain*.



2. Select ***Use server authorization*** checkbox, to allow users to authorize in SmartPTT Dispatcher only when connection to the radioserver is available.

Important
The checkbox must be used only if you install SmartPTT Dispatcher. Otherwise, login issues occur.

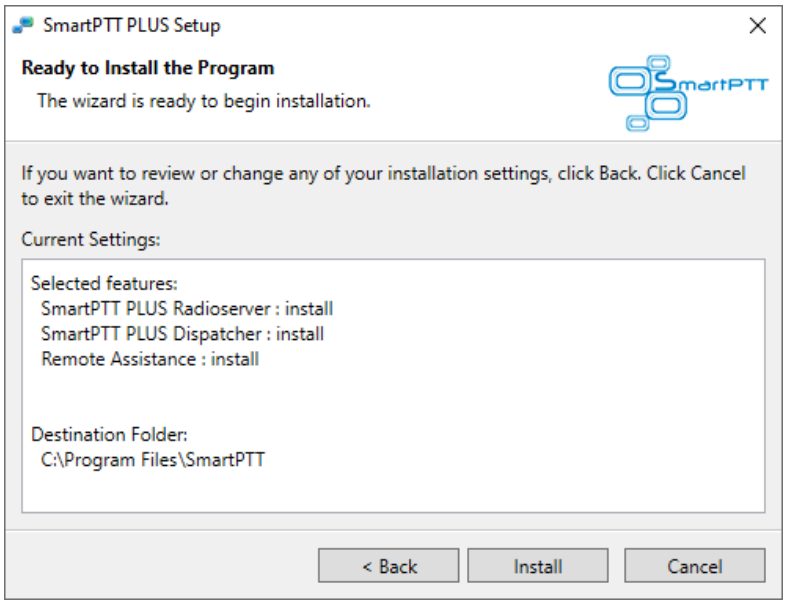
3. In the ***Domain*** field, specify the desired domain name.
4. To connect the domain specified, click ***Test***. It may take some time to check if the domain server is available.
   The message about the result of the check will appear.
5. From the ***System Administrators*** list, select one of the user groups who will be able to authorize in SmartPTT Radioserver Configurator and configure it.

6. From the ***Database Administrators*** list, select one of the user groups who will be able to create, update, and restore databases.
7. From the ***Console Administrators*** list, select one of the user groups who will have an access to authorization in SmartPTT Dispatcher with the administrator rights, including the operator profiles creation and configuration. These users can select one of the existing databases, but cannot create or update them.
8. From the ***Console Operators*** list, select one of the user groups who will be able to log in SmartPTT Dispatcher and use its functions.

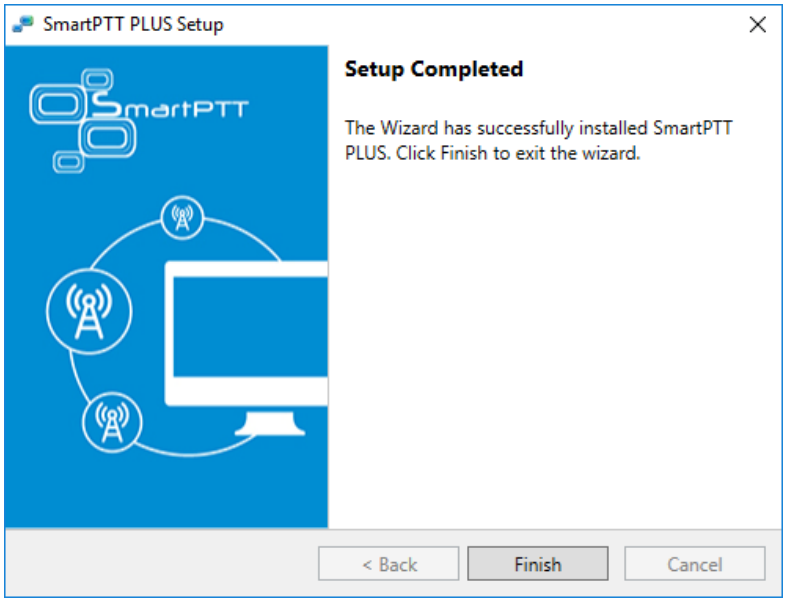
NOTE
Each list displays the groups which are available in the domain specified.

NOTE
If the *Local* or *Domain* type is specified, the ***Login*** window appears each time SmartPTT Radioserver Configurator is started.

7. In the ***Authentication setup*** window, click ***Next***.
   The ***Ready to Install the Program*** window appears.



8. In the window that appeared, look through the installation summary to check the data correctness. Then click ***Install***. When the installation completes, the ***Setup Completed*** window appears.



9. In the window that appeared, click ***Finish*** to exit the installation program.

Postrequisites:

Restart the computer to guarantee that all Windows configuration changes are applied.

3.2 Modifying Installed Software

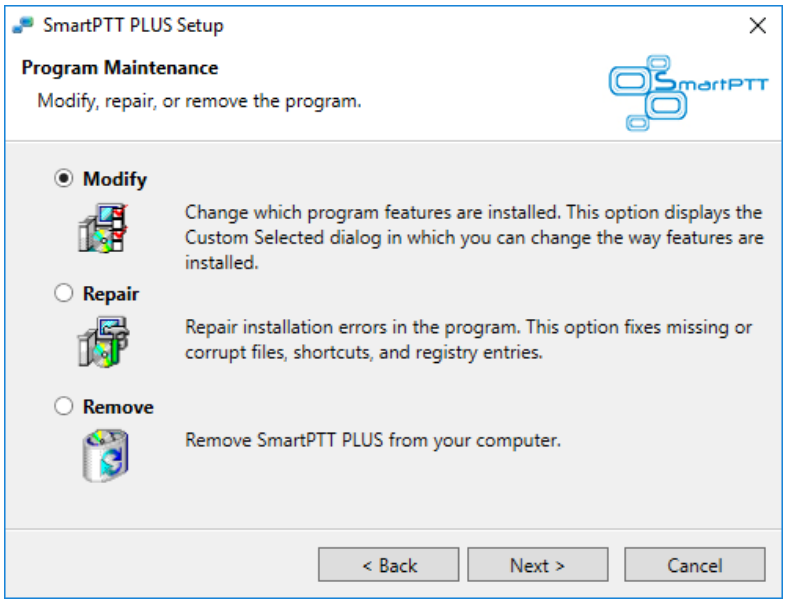
Follow the procedure to modify the SmartPTT components installed on the computer.

Prerequisites:

- Log on to Windows as an administrator.
- Copy the installation file (SmartPTTSetup.exe) to the computer.

Procedure:

1. Start the installation file.
2. In the welcoming window, click ***Next***.
   The ***Program Maintenance*** window appears.



3. In the window that appeared, perform one of the following actions:
   - To install additional components, click ***Modify***.
   - To repair the incorrectly installed software, click ***Repair***.
   - To remove one or several software components, click ***Remove***.
4. Click ***Next***, and then follow the instructions provided by the installation program.

3.3 Dispatch Software Upgrade

If you start ***SmartPTTSetup.exe*** on the computer, that already has an older version of SmartPTT (except Web Client), the information window appears that offers you to upgrade your SmartPTT software. Before you start an upgrade, it is recommended to perform the following actions:

- Export SmartPTT Radioserver settings to the configuration file.
- For SmartPTT Dispatcher, save settings to the configuration file.

WARNING
The decision to include databases in the configuration files must be made by the maintenance engineer. Including databases into the file may increase it size up to many gigabytes.

After this, you should start ***SmartPTTSetup.exe*** to upgrade the software. Installation program should detect the older software versions automatically. If it does not, your SmartPTT version is too old. In this case, you should uninstall SmartPTT Radioserver and SmartPTT Dispatcher manually.

After an upgrade completes, restart the computer and perform the following actions:

- Import SmartPTT Radioserver settings from the configuration file.
- For SmartPTT Dispatcher, restore settings from the configuration file.

If you use intermediate versions to update the old database, then in order for the database to be updated correctly, you must run SmartPTT Dispatcher and SmartPTT Radioserver on these intermediate versions at least once, and only then install the next intermediate or target SmartPTT version.

3.4 Configuring Antivirus Software

If antivirus software (anti-malware) is installed and used on the radioserver and/or dispatch console host, it can prevent SmartPTT executable (.exe) files from starting. To avoid this, you should configure antivirus software to start the following executable files without checking:

Component	*File Path*
SmartPTT Radioserver	\<installation folder>\Server\DebugInfoCollector.exe
	\<installation folder>\Server\GrantSqlAccess.exe
	\<installation folder>\Server\HID.exe
	\<installation folder>\Server\RadioService.exe
	\<installation folder>\Server\RSConfigurator.exe
SmartPTT Dispatcher	\<installation folder>\Client\CefSharp.BrowserSubprocess.exe
	\<installation folder>\Client\Client.exe
	\<installation folder>\Client\DebugInfoCollector.exe
	\<installation folder>\Client\GrantSqlAccess.exe

To determine the DBMS files that should be allowed to start without checking, contact Microsoft Support.

4 Basic Configuration

Basic SmartPTT configuration includes actions that can be performed despite of the radio or other communication system connection. Note that those actions may provide additional requirements to the dispatch and radio system infrastructure, IP address management, network ports management, radios identifications, etc.

Important
If local or domain authentication is used, only users included in the *System Administrators* group have access to SmartPTT Radioserver Configurator. For details, see SmartPTT Installation.

4.1 Loging in to Radioserver Configurator

If you selected a local or domain authentication during SmartPTT installation, you must enter user credentials to start using SmartPTT Radioserver Configurator. For details, see Installing on New Computer.

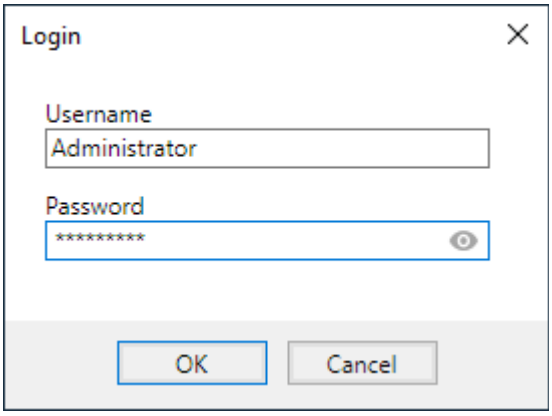
Follow the procedure to log in to SmartPTT Radioserver Configurator.

Prerequisites:

Depending on the configuration you want to perform in SmartPTT Radioserver Configurator, obtain user credentials. The user account must belong to the *System Administrators* or *Database Administrators* group. For details, see Authentication Types.

Procedure:

1. Start SmartPTT Radioserver Configurator.
   The ***Login*** window appears.



2. In the window that appears, perform the following actions:

To obtain full access to all SmartPTT Radioserver Configurator settings,	in the ***Username*** field, enter the name of the user who belongs to the *System Administrators* group.
To obtain access only to database settings in SmartPTT Radioserver Configurator,	in the ***Username*** field, enter the name of the user who belongs to the *Database Administrators* group.

3. In the ***Login*** window, in the ***Password*** field, enter the user password. To view the entered password, click the icon ( ).
4. Click ***OK***.
   The main SmartPTT Radioserver Configurator window appears.

Postrequisites:

In SmartPTT Radioserver Configurator, go to the desired settings.

4.2 DBMS Configuration

The document provides information on the database management system (DBMS) configuration using the official applications provided by the DBMS developer. Those applications provide graphical user interface for DBMS configuration. The applications are as follows:

- Microsoft SQL Server Configuration Manager.
- Microsoft SQL Server Management Studio.

The Microsoft SQL Server does ***not*** included in the installation package.

All the related screenshots are presented for Microsoft SQL Server Express. Customer's DBMS may be different.

Configuration Overview

To configure DBMS, the following actions must be performed:

- DBMS autostart must be configured. For details, see Configuring DBMS Autostart.
- Remote access must be allowed. For details, see Configuring Remote DBMS Access.
- *(Optional)* User accounts must be created to provide Windows-independent authentication. For details, see Adding SQL Server Users.
- DBMS memory consumption must be limited. For details, see Limiting DBMS Memory Use.
- Network traffic must be unlocked for DBMS. For details, see Radioserver Host.
- *(Optional)* Size of database files must be limited. For details, see Limiting Database Files Size.

4.2.1 Configuring DBMS Autostart

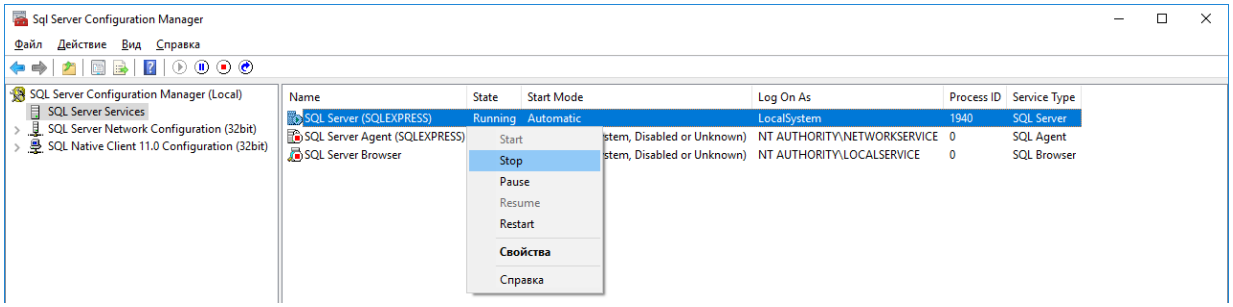
Follow the procedure to configure automatic start of the DBMS service after computer restart. This will reduce the time of system startup after DBMS host restart.

Prerequisites:

Start SQL Server Configuration Client (SSCC) on the DBMS host. For details, see SQL Server Configuration Manager in the *Microsoft Docs* portal.

Procedure:

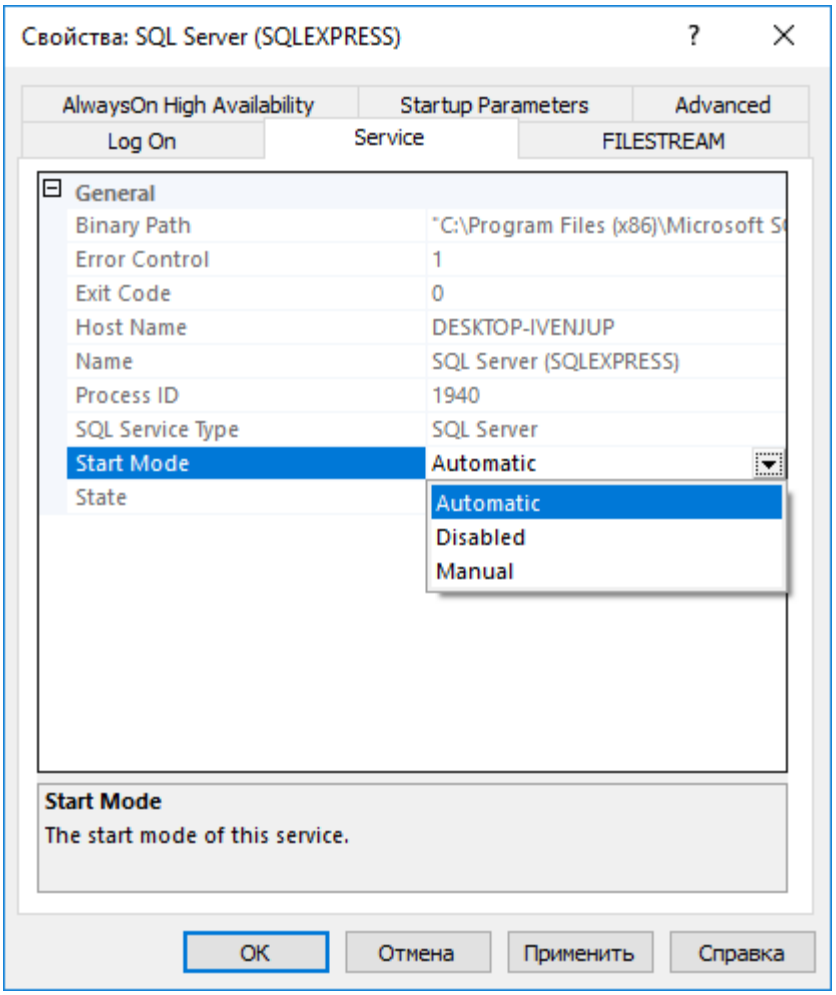
1. In SSCC, in the left pane, expand ***SQL Server Configuration Manager (Local)***, and then click ***SQL Server Services***.
2. Stop DBMS services:
   a. In the right pane, right-click ***SQL Server***, and then select ***Stop*** from the action menu.



b. Repeat step 2a for ***SQL Server Browser***.

3. Configure DBMS autostart:

   a. Right-click ***SQL Server***, and then select ***Properties*** from the action menu.
   The ***Properties: SQL Server*** window appears.



   b. In the window that appears, open the ***Service*** tab.

   c. On the tab, in the ***Start Mode*** list, click the current value, and then select *Automatic*.

   d. In the ***Properties: SQL Server*** window, click ***OK*** to apply changes and close the window.

4. Repeat step 3 for the ***SQL Server Browser*** service.

5. Start DBMS services:

   a. In the right pane, right-click ***SQL Server***, and then select ***Start*** from the action menu.

   b. Repeat step 5a for ***SQL Server Browser***.

4.2.2 Configuring Remote DBMS Access

Follow the procedure to allow remote access to the DBMS.

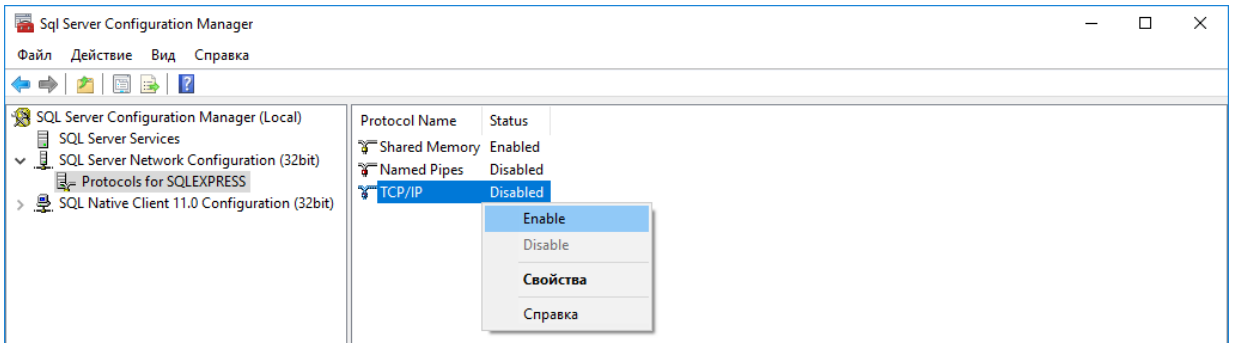
Prerequisites:

Start SQL Server Configuration Client (SSCC) on the DBMS host. For details, see SQL Server Configuration Manager in the *Microsoft Docs* portal.

Procedure:

1. Allow the TCP/IP protocol for communication with DBMS:

   a. In SSCC, in the left pane, expand ***SQL Server Configuration Manager (Local)*** → ***SQL Server Network Configuration***, and then select ***Protocols for <DBMS Name>***.



   b. In the right pane, right-click ***TCP/IP***, and then select ***Enable*** from the actions menu.

   c. In the warning dialog box, click ***OK***.

   d. Restart DBMS:

      i. In the left pane, click ***SQL Server Services***.

      ii. In the right pane, right-click ***SQL Server***, and then select ***Restart*** from the actions menu.

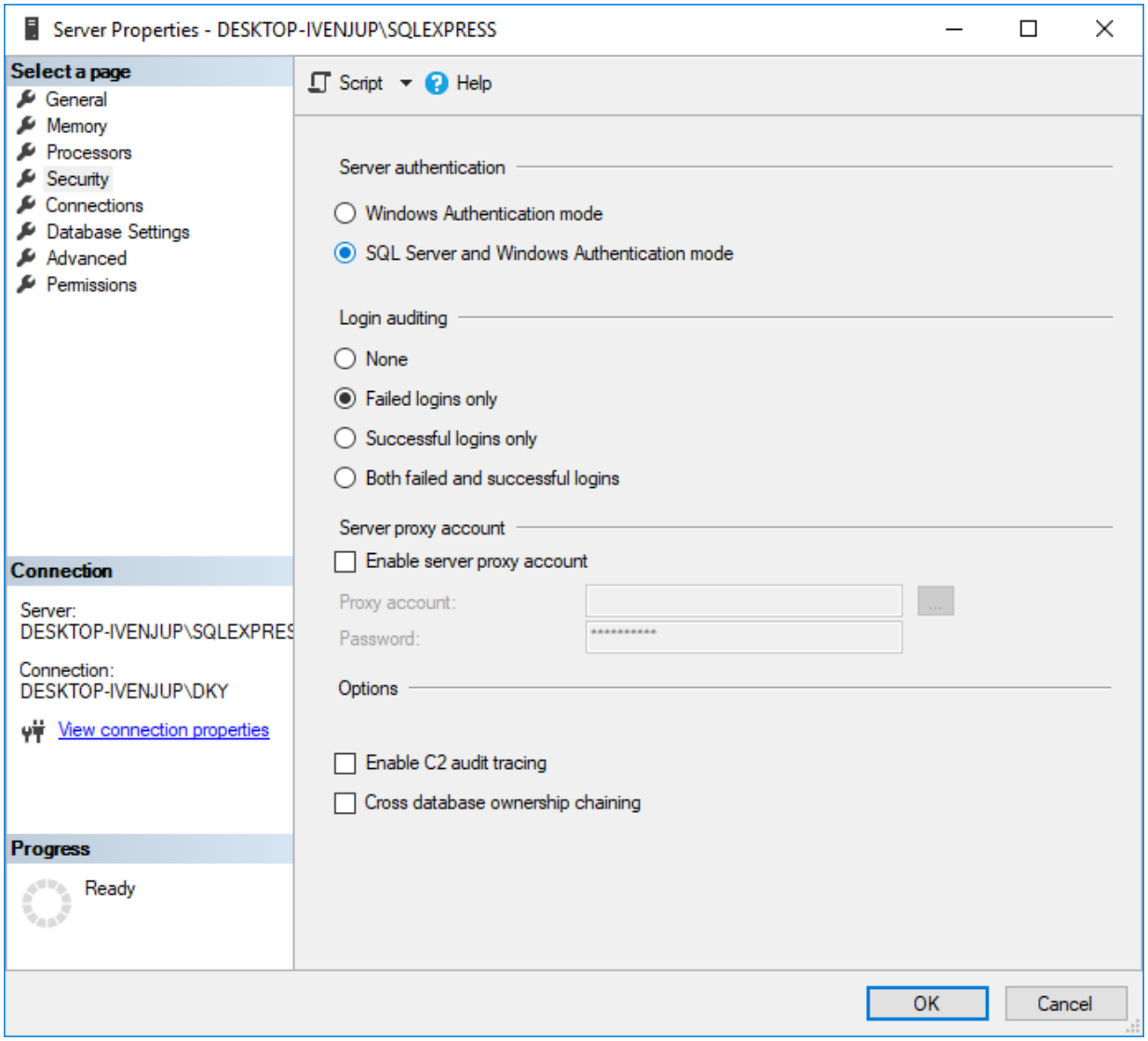
2. Start SQL Server Management Studio (SSMS), and then connect to the required DBMS.

3. Open the ***Object Explorer*** panel.

4. On the panel, right-click ***<Computer Name>\<DBMS Name>***, and then select ***Properties*** from the action menu.
   The ***Server Properties*** window appears.

5. In the window that appears, modify authentication settings:

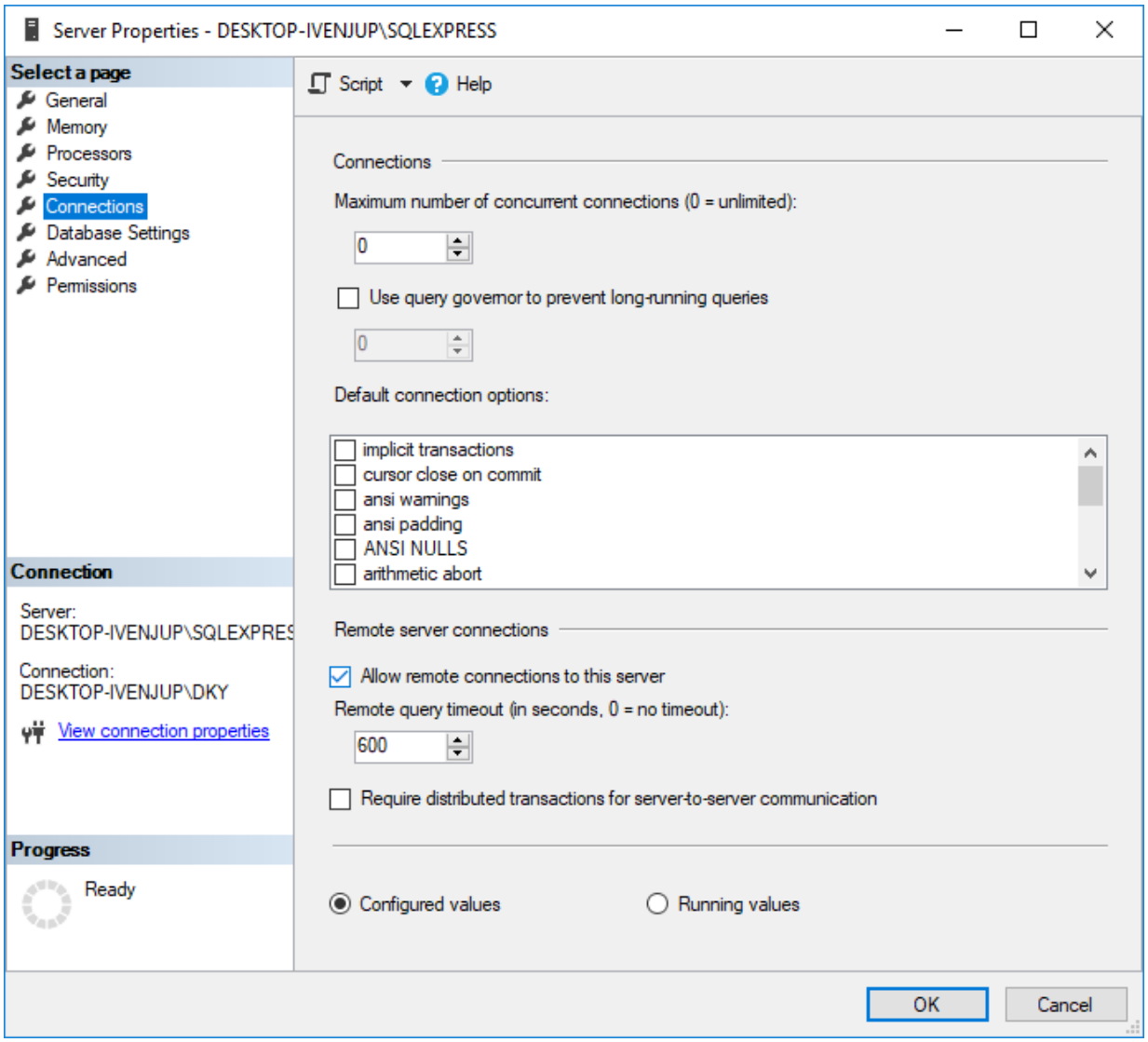
   a. In the left pane of the window, click ***Security***.
   Security settings appear in the right pane.



   b. In the right pane, click ***SQL Server and Windows Authentication mode***.

6. Configure the remote access parameter for the DBMS:

   a. In the left pane, click ***Connections***.



   b. In the right pane, in the ***Maximum number of concurrent connections*** field, enter one of the following values:

To allow unlimited number of connections,	enter *0*.
To limit the maximum number of simultaneous connections,	enter the required number of connections.

   c. In the right pane, in the ***Remote server connections*** area, select ***Allow remote connections to this server***.

   d. *(Optional)* In the ***Remote query timeout*** field, enter the request timeout.

   e. Click ***OK*** to apply changes and close the window.

7. On the ***Object Explorer*** panel, right-click ***<Computer Name>\<DBMS Name>***, and then select ***Restart*** from the actions menu.

4.2.3 Adding SQL Server Users

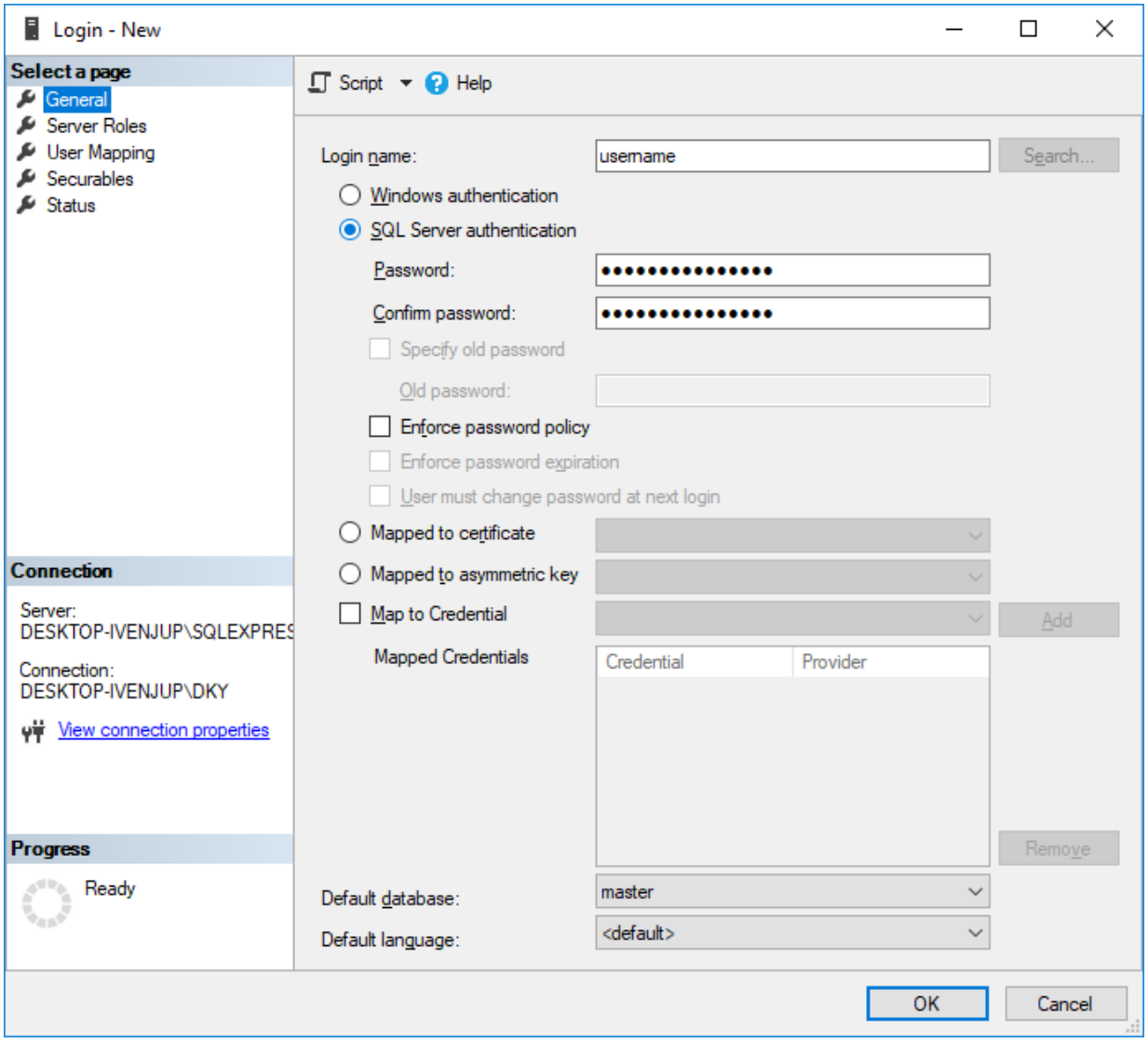
Follow the procedure to add a user account to the SQL service and use its credentials for DBMS authentication.

Prerequisites:

- Determine user login and password.
- Connect to the DBMS using SQL Server Management Studio (SSMS).

Procedure:

1. In SSMS, open the ***Object Explorer*** panel.
2. On the ***Object Explorer*** panel, expand ***<Computer Name>\<DBMS Name>*** → ***Security***.
3. Right-click ***Logins***, and then select ***New Login*** from the actions menu.
   The ***Login - New*** window appears.
4. In the window that appears, set user credentials:
   a. In the left pane, click ***General***.



   b. In the right pane, in the ***Login name*** field, enter user login.

c. Click ***SQL Server authentication***.

d. In the ***Password*** field, enter user password.

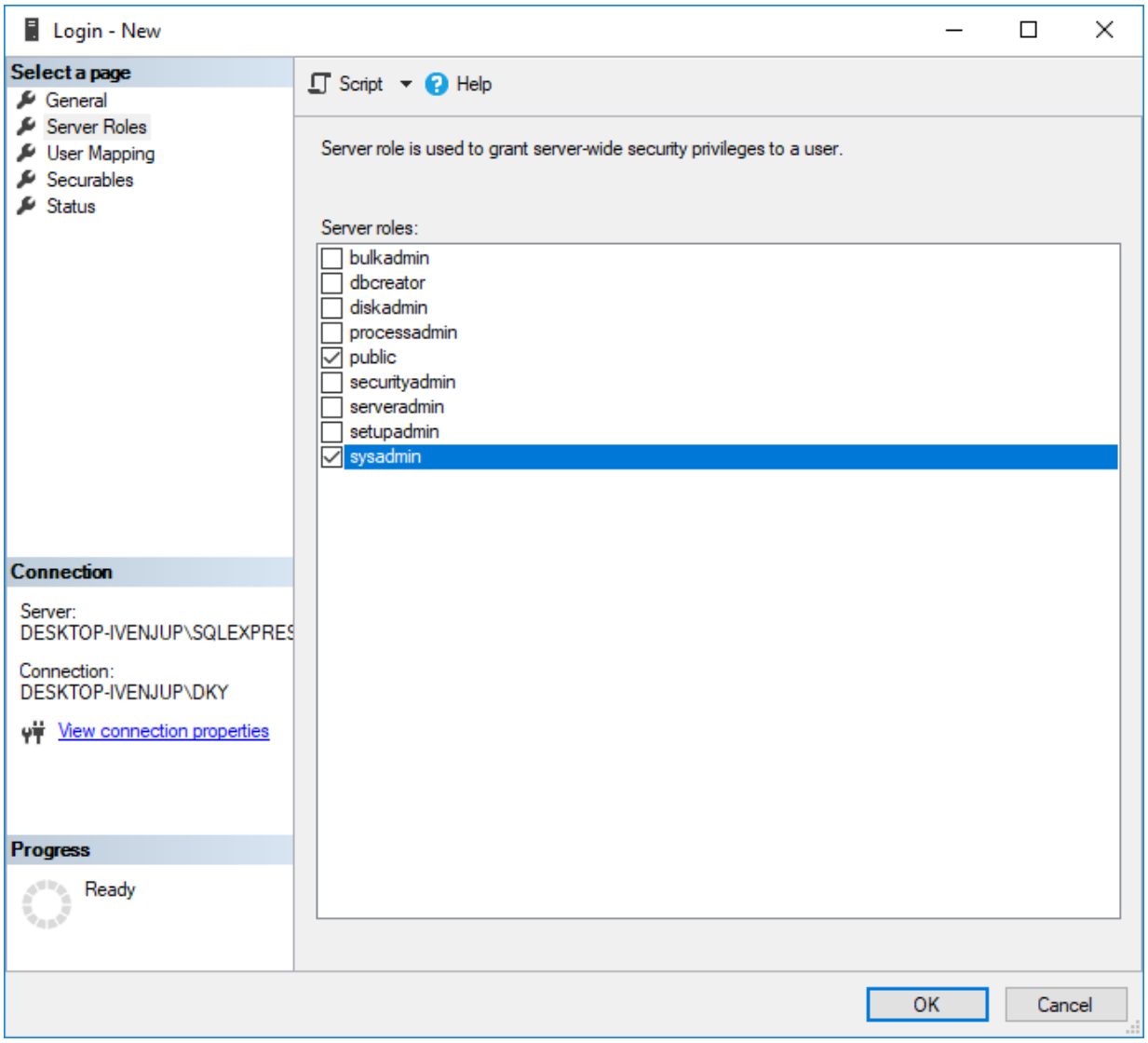
e. In the ***Confirm password*** field, enter user password again.

f. Modify password policy settings:

To make password policy settings compliant with the operating system settings,	perform the following actions: 1. Select ***Enforce password policy***. 2. Clear ***Enforce password expiration***. 3. Clear ***User must change password at next login***.
To turn off password policy for the user,	clear ***Enforce password policy***.

5. Configure user rights:

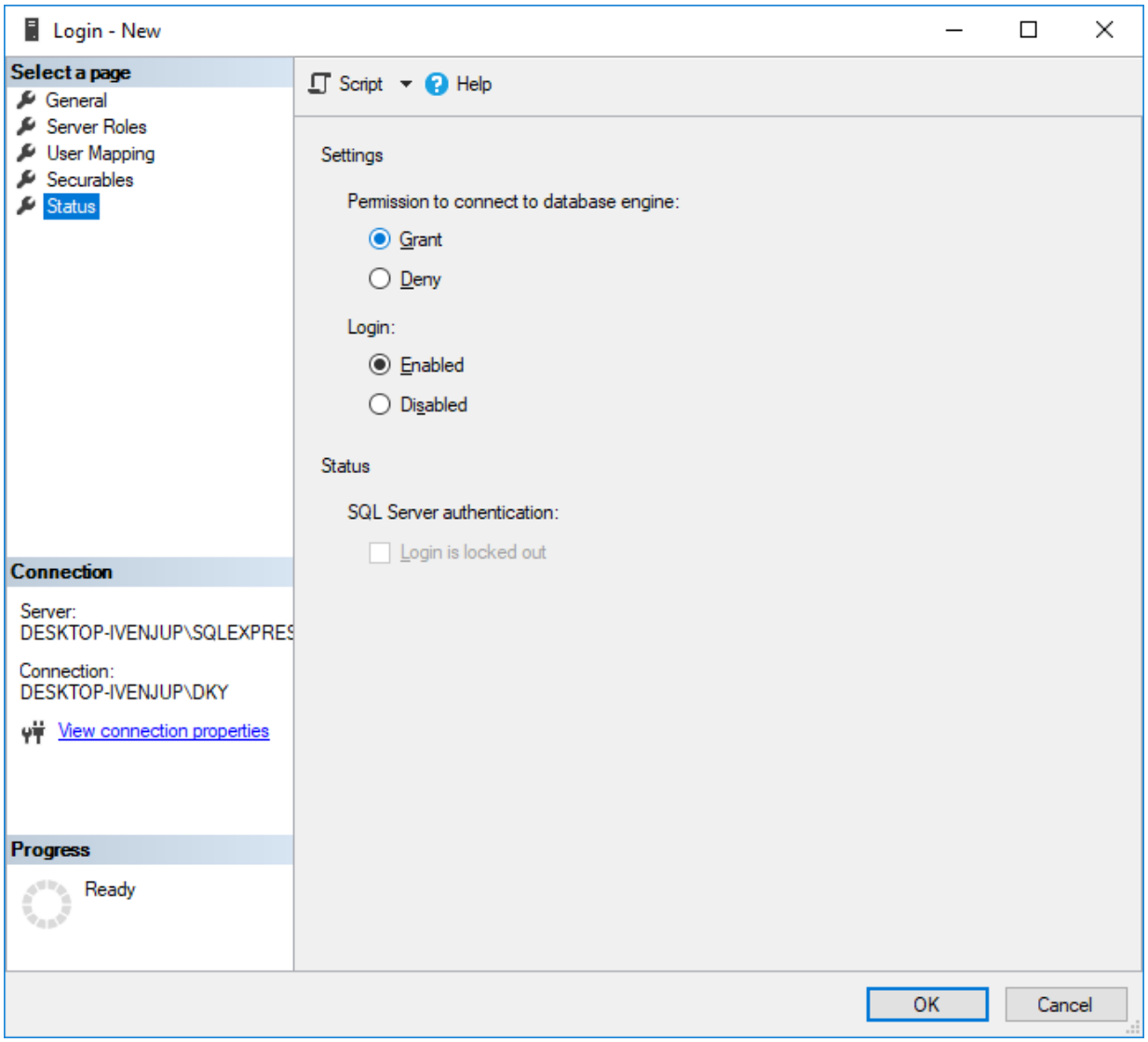
a. In the left pane, click ***Server Roles***.



b. In the right pane, in the ***Server Roles*** area, select ***sysadmin***.

6. Configure user status:

   a. In the left pane, click ***Status***.



   b. In the right pane, in the ***Permission to connect to database engine*** area, click ***Grant***.

   c. In the ***Login*** area, click ***Enabled***.

7. In the ***Login - New*** window, click ***OK*** to create the user account and close the window.

8. On the ***Object Explorer*** panel, right-click ***<Computer Name>\<DBMS Name>***, and then select ***Restart*** from the actions menu.

4.2.4 Limiting DBMS Memory Use

Follow the procedure to limit the size of Random-Access Memory (RAM) used by DBMS. By default, DBMS is able to consume all the available RAM. This may result in a serious decrease in computer performance, especially if DBMS is installed on the same computer as another server application.

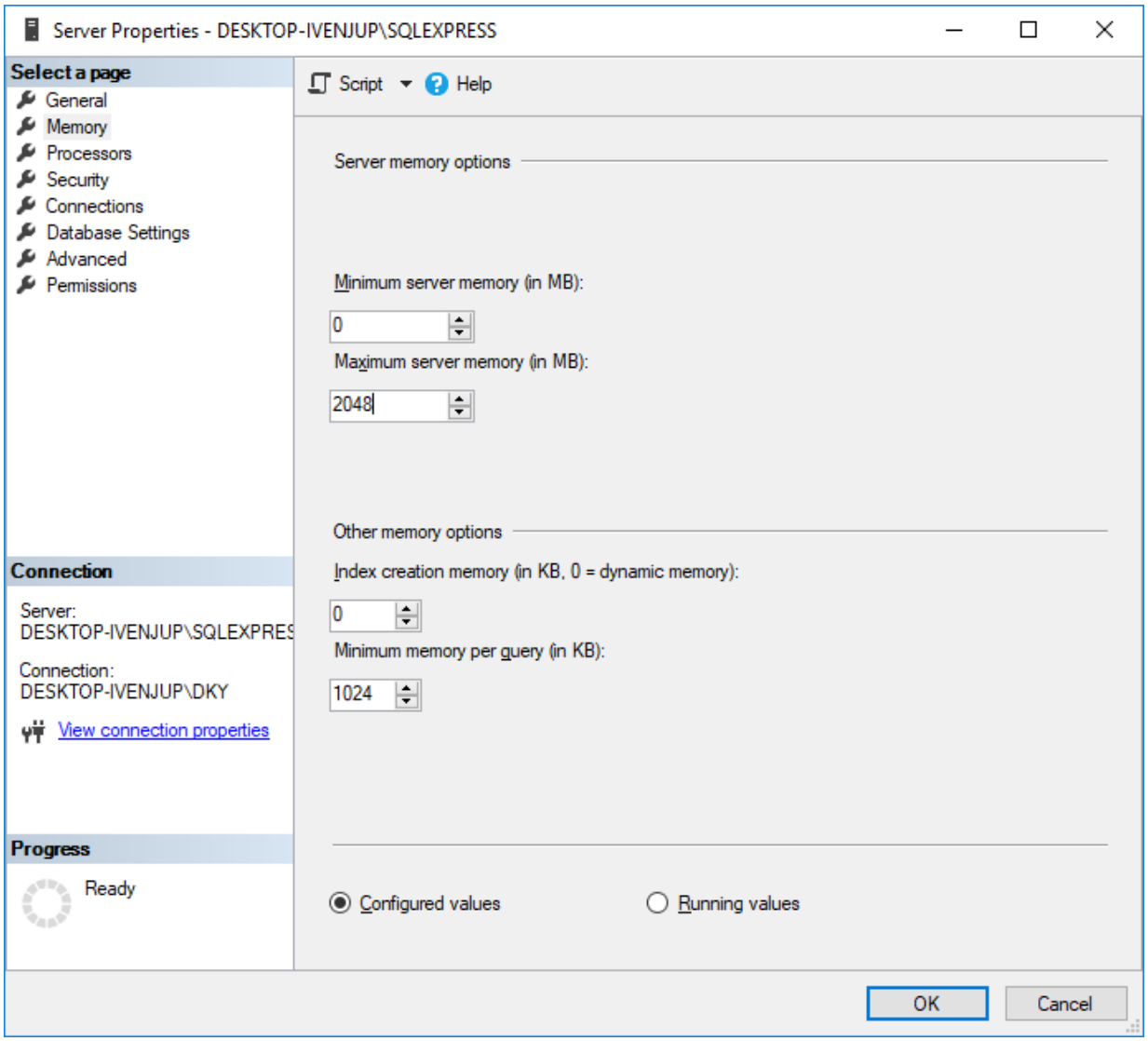
WARNING
Modify the settings only after consultation with your system administrator.

Prerequisites:

Connect to the required DBMS using SQL Server Management Studio (SSMS).

Procedure:

1. In SSMS, open the ***Object Explorer*** panel.
2. On the panel, right-click ***<Computer Name>\<DBMS Name>***, and then select ***Properties*** from the actions menu.
   The ***Server Properties*** window appears.



3. In the window that appears, in the left pane, click ***Memory***.
4. In the right pane, in the ***Maximum server memory*** field, enter the maximum RAM size that will be available to DBMS.
5. In the ***Server Properties*** area, click ***OK***.
6. On the ***Object Explorer*** panel, right-click ***<Computer Name>\<DBMS Name>***, and then select ***Restart*** from the actions menu.

4.2.5 Limiting Database Files Size

Follow the procedure to limit the size of database files. When the maximum data file size is reached, DBMS starts to add the corresponding entries to the database log file. This behavior decreases free disk space.

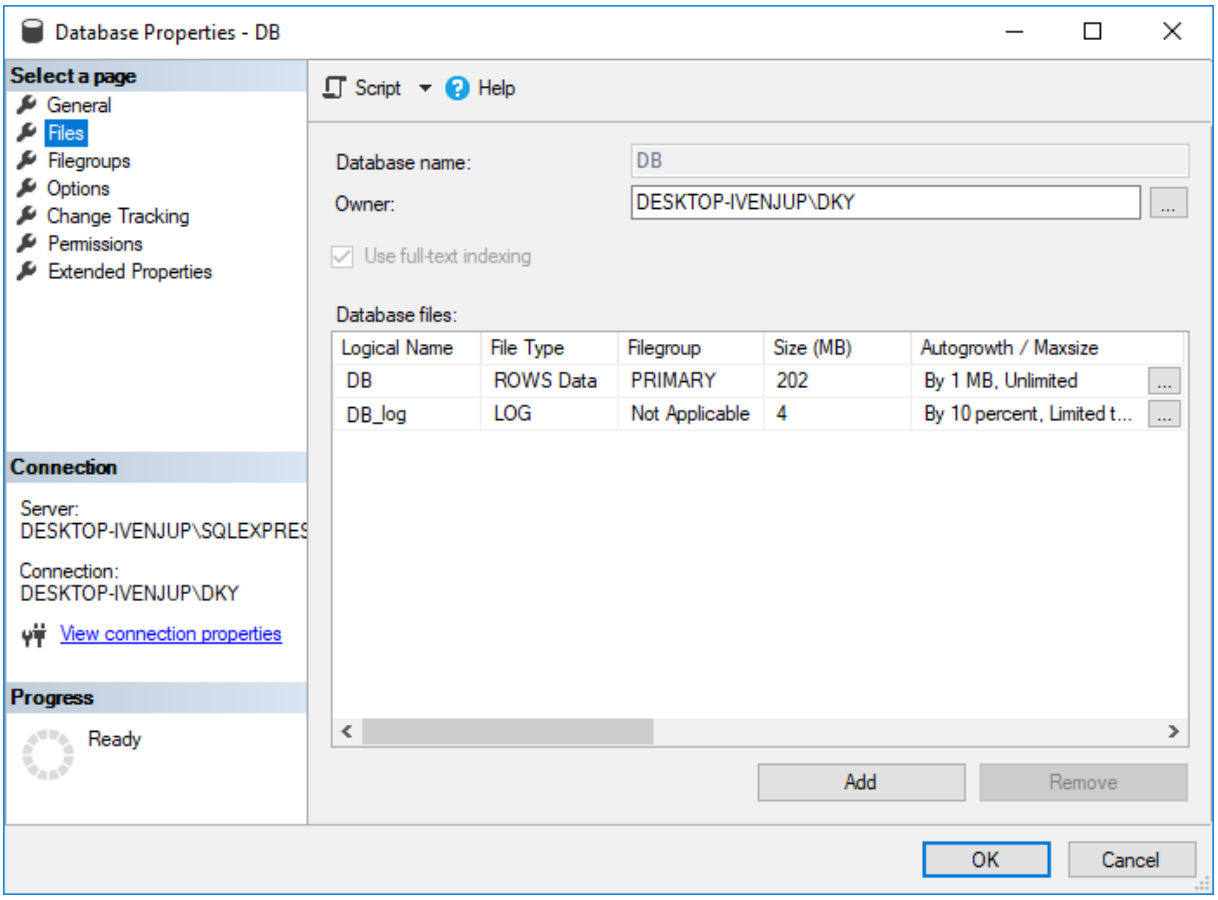
WARNING
Modify the settings only after consultation with your system administrator.

Prerequisites:

Connect to the required DBMS using SQL Server Management Studio (SSMS).

Procedure:

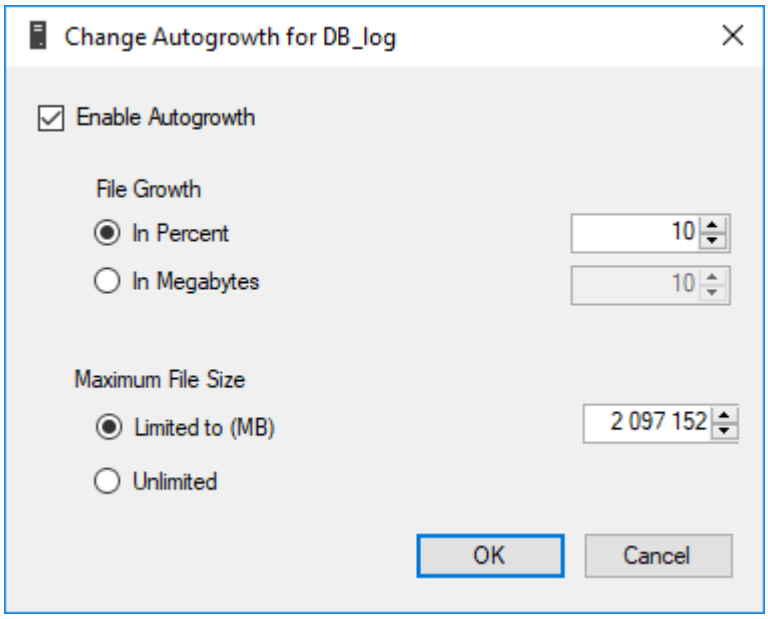
1. In SSMS, open the ***Object Explorer*** panel.
2. On the panel, expand the ***Databases*** node, right-click the desired database name, and then select ***Properties*** from the actions menu.
   The ***Database Properties*** window appears.
3. In the opened window, in the left pane, click ***Files***.



4. In the ***Database files*** table, perform one of the following actions:

To configure the data file autogrowth,	for the ***ROWS Data*** entry, in the ***Autogrowth / Maxsize*** column, click the Browse (...) button.
To configure the log file autogrowth,	for the ***LOG*** entry, in the ***Autogrowth / Maxsize*** column, click the Browse (...) button.

The ***Change Autogrowth*** window appears.



5. Select the ***Enable Autogrowth*** check box to enable automatic growth of the file when its maximum file size is reached.
6. In the ***File Growth*** area, configure the file growth parameters:

To configure file growth in percent,	perform the following actions: 1. Select ***In Percent***. 2. In the field on the right, enter the value in percent to increase the file size. ***NOTE*** The value must be large enough to stay ahead of the needs of the workload transactions and avoid frequent expansion.
To configure file growth in megabytes,	perform the following actions: 1. Select ***In Megabytes***. 2. In the field on the right, enter the value in megabytes to increase the file size. ***NOTE*** The value must be large enough to stay ahead of the needs of the workload transactions and avoid frequent expansion.

7. In the ***Maximum File Size*** area, configure the maximum file size:

To limit the file size,	perform the following actions: 1. Select ***Limited to (MB)***. 2. In the field on the right, specify the maximum file size in megabytes.

To enable unlimited growth for the file in memory-optimized filegroup,	select ***Unlimited***.

8. Click ***OK*** to confirm changes and close the window.
9. In the ***Database Properties*** window, click ***OK***.

4.3 Licensing

To unlock SmartPTT Radioserver Configurator tools, SmartPTT features must be licensed. If SmartPTT Radioserver and the dispatch console are installed on the same computer, you can install licenses either in SmartPTT Radioserver Configurator or in SmartPTT Dispatcher. If SmartPTT Radioserver and the dispatch console are installed on different computers, you must install licenses for both applications. If the radioserver and the dispatch console are installed on different computers, the license installation requirements depend on the client profile settings in the radioserver. If the client profile allows radioserver to apply its license to the desktop client, it is sufficient to install the license only on the radioserver. Otherwise, the license must be installed in both applications. For information on profile configuration, see Profiles.

Licensing includes the following actions:

- Hardware ID generation. Hardware ID is required to order SmartPTT licenses. The ID can be obtained in one of the following ways:
  - Using SmartPTT Radioserver Configurator (after the software installation). For details, see Generating HID in Radioserver Configurator.
  - Using standalone utility. For details, see Generating HID with a Standalone Utility.

Important
Hardware ID is derived from the SmartPTT host hardware configuration. If that configuration changes, it will render the license invalid. Therefore, SmartPTT host hardware configuration changes must be completed before ordering a license.

- License file installation. For details, see Installing License.

4.3.1 Generating Hardware ID

Follow the procedure to generate the hardware ID (HID) required to order a SmartPTT license file.

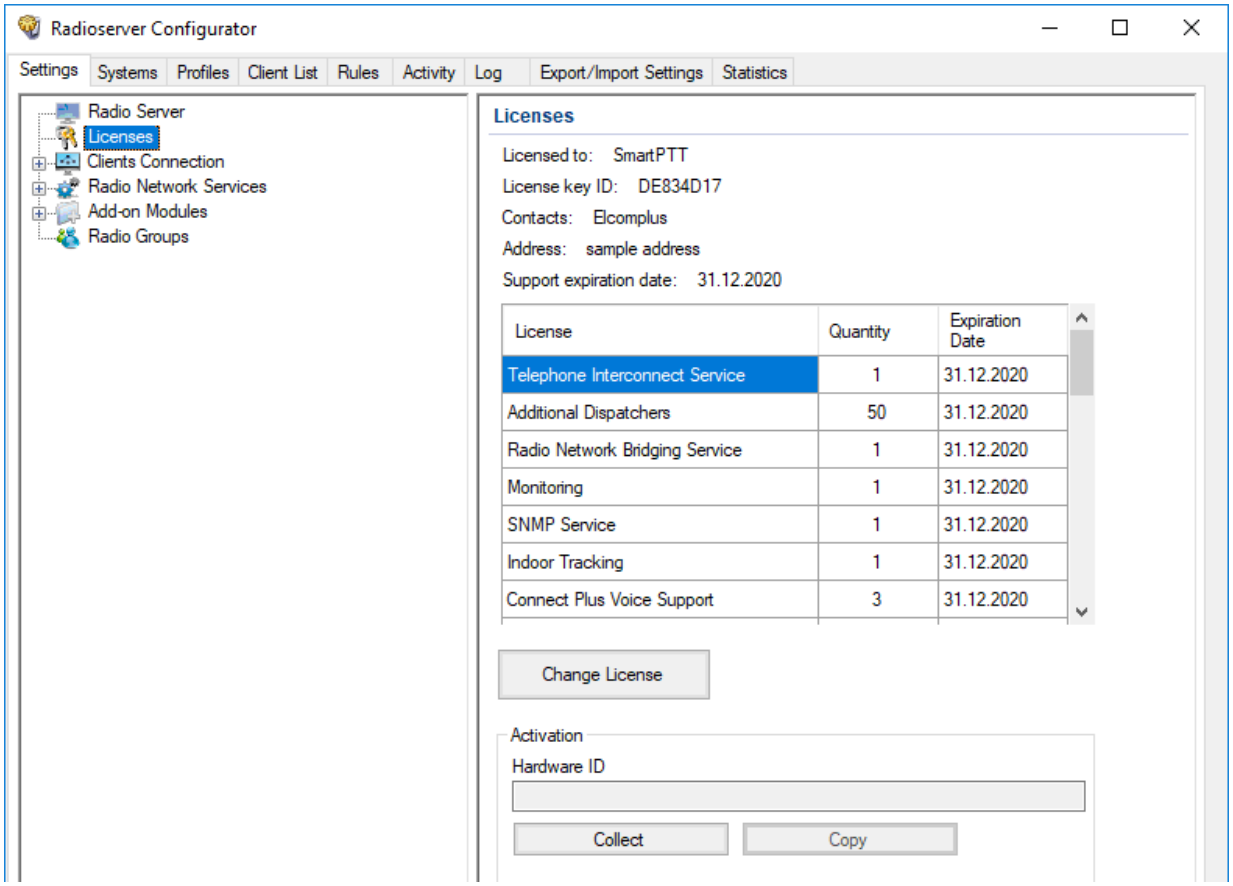
NOTE
HID can also be obtained before SmartPTT installation using a standalone utility. For details, see the “Generating HID with a Standalone Utility” section of *SmartPTT Installation and Configuration Guide*.

Prerequisites:

- Configure the computer hardware and operating system language settings.
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
1. In the left pane, select ***Licenses***.



3. In the right pane, in the ***Activation*** area, click ***Collect***.
   A string of characters appears in the ***Hardware ID*** field.
4. Click ***Copy*** to copy the hardware ID to the clipboard.

Postrequisites:

Send the hardware ID to Elcomplus, Inc. to receive the license file.

4.3.2 Installing License

To use all desired SmartPTT features, a license must be installed.

Follow the procedure to install SmartPTT license.

Prerequisites:

Generate HID, send it to the Elcomplus, Inc. representative, and obtain the SmartPTT license file (.spttlx).

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, select ***Licenses***.
3. Click ***Change License***.
   The file selection window appears.
4. In the window that appears, select the license file and click ***Open***.
   The ***License Installation*** window appears.

5. Ensure that the licensed services and their expiration dates are correct, and click ***Apply***. Otherwise, click ***Cancel*** and select another license file or submit a request to the SmartPTT Technical Support Center.
   The new license parameters appear in the right pane.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

4.3.3 Viewing License Items

Follow the procedure to view items of the installed license file. The procedure may be required to determine if specific features are available or unavailable in SmartPTT.

Important
This document does not contain exact license item names. If you need assistance in matching license item names and SmartPTT features, submit a request to SmartPTT Technical Support Center.

Prerequisites:

Install the SmartPTT license file. For details, see Installing License.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, click ***Licenses***.
   The license information appears in the right pane.
3. In the upper part of the right pane, perform the following actions:

To view the licensee name,	see the ***Licensed to*** entry.
To view the license ID,	see the ***License key ID*** entry.
To view the contact information of the user,	see the ***Contacts*** entry.
To view the licensee address,	see the ***Address*** entry.
To view the last date of the SmartPTT upgrade installation,	see the ***Support expiration date*** entry.

4. In the table below, view the available license items. Use scrollbar if required.
   a. In the ***License*** column, view the license item name.
   b. Next to the desired license item, in the ***Quantity*** column, view the quantity of the purchased license items.
   c. Next to the desired license item, in the ***Expiration Date*** column, view the last date of the feature provision.

4.4 Configuring Radioserver

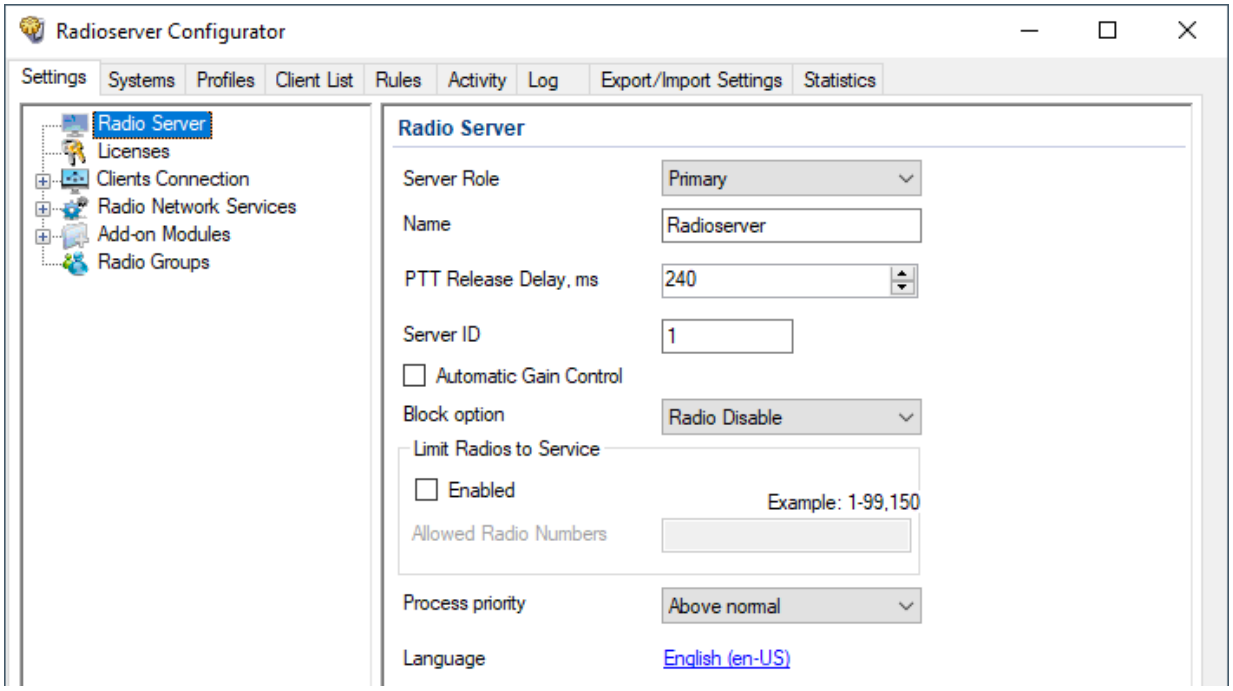
Follow the procedure to configure the primary SmartPTT Radioserver.

Prerequisites:

- From radio codeplugs, obtain information on the following commands support:
  - Radio Disable.
  - Radio Inhibit.
- Obtain Radio IDs that must be accessible to a radioserver.
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, click ***Radio Server***.
   The SmartPTT Radioserver settings appear in the right pane.



3. From the ***Server Role*** list, select *Primary*.
4. *(Optional)* In the ***Name*** field, type the desired radioserver name.
5. *(Optional)* If you are experiencing clipped voice transmissions from subscribers, increase the value in the ***PTT Release Delay, ms*** field. The range of possible values is *0–2160*. You may need to experiment to determine the value that suits your system.

Important
If you are performing initial configuration of SmartPTT Radioserver, or if you are not experiencing clipped voice transmissions, leave the default value of *240*. Generally, you should not reduce this delay.

6. If your system includes more than one radioserver, in the ***Server ID*** field, type a unique number. The range of possible values is *1–255*.

7. *(Optional)* Select the ***Automatic Gain Control*** check box to automatically adjust the incoming calls volume.
8. In the ***Block option*** field, select the appropriate radio command that blocks radios:

If radios support the Radio Enable command,	select *Radio Disable*.
If radios support the Radio Inhibit command,	select *Deny Channel*.

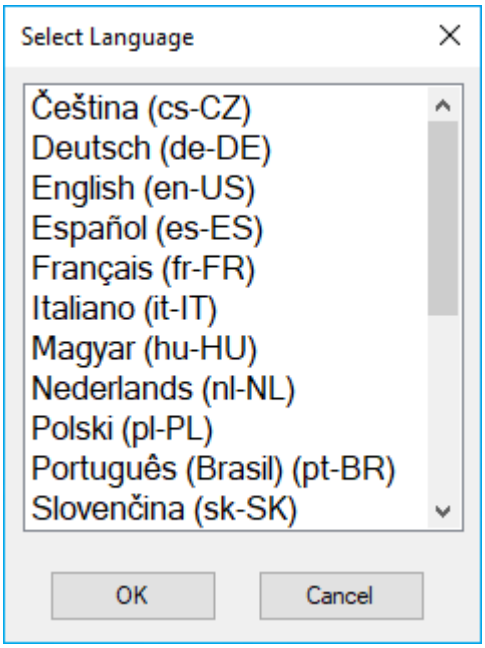
9. *(Optional)* In the ***Limit Radios to Service*** area, configure the list of radios that will be available to dispatchers:
   a. Select the ***Enabled*** check box.
   b. In the ***Allowed Radio Numbers*** field, type the desired Radio IDs.

Important
If the dispatcher manually adds a radio that is not on the allowed list when limit radios to service is enabled, the radio will be inactive and inaccessible.

10. From the ***Process priority*** list, select the radioserver process priority relative to other processes on the computer.

Important
If *Real time* is selected from the list, all computer resources will be given to SmartPTT Radioserver, which may make the computer operating system unstable.

11. *(Optional)* To change the interface language of SmartPTT Radioserver Configurator, perform the following actions:
    a. Click the current ***Language*** value.
    The ***Select Language*** window appears.



    b. In the window that appears, select the desired language from the list.
    c. Click ***OK***.

12. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

4.4.1 Managing Radio Groups

Follow the procedure to add, edit, or delete a group of radios that may be needed for various radioserver subservices configuration.

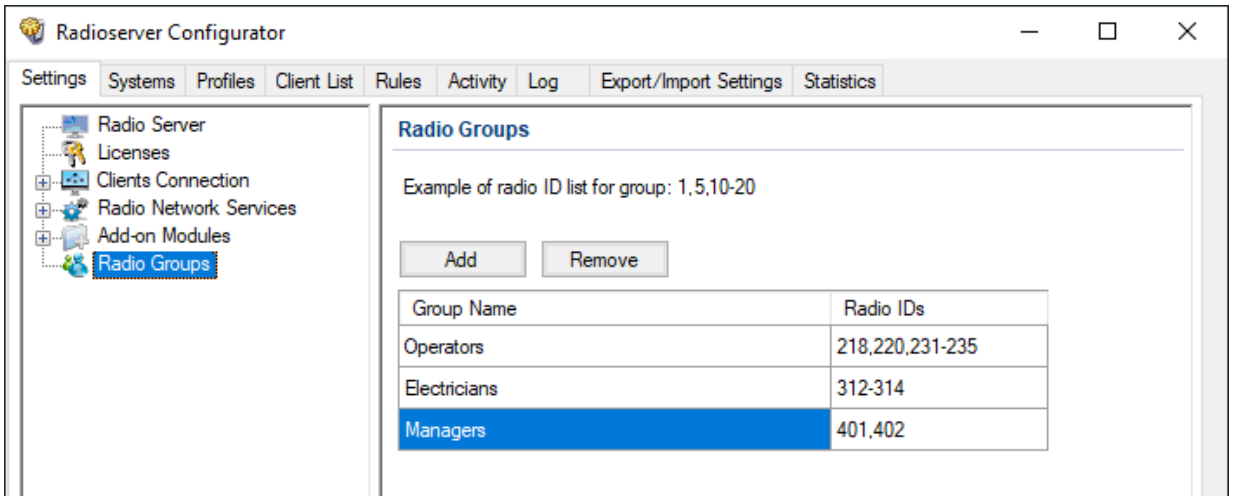
Important
Do not confuse radio groups and talkgroups.

Prerequisites:

- Obtain Radio IDs that must be configured for various purposes.
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, click ***Radio Groups***.
   The radio group settings appear in the right pane.



3. Perform one of the following actions:

To add a new group,	click ***Add***.
To modify a group,	proceed to the next step of the procedure.
To delete a group,	perform the following actions: 1. Click the desired group. 2. Click ***Remove***. 3. Proceed to the last step of the procedure.

4. In the desired table row, in the ***Radio IDs*** column, type the desired IDs. Use hyphens to enter radio ID ranges; use commas to list radio IDs and ID ranges.
5. *(Optional)* In the desired table row, in the ***Group Name*** column, double-click the current group name, and then type the desired name.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (******)*** or ***Restart (******)***.

4.5 Radios and Radio Users

The section describes information reception on radios presence and availability. Information includes the following aspects:

- Registration information provision over the DMR/MOTOTRBO protocol. For details, see Registration of Radios.
- Information on the current radio user. For details, see Radio Users.

4.5.1 Registration of Radios

Radio registration is a process in which dispatchers are informed about the radio availability for voice and text transmissions, location requests, and other activities.

SmartPTT supports radio registration using the following mechanisms:

- Registration determined by the dedicated DMR/MOTOTRBO protocol. For details, see Configuring ARS.
- On-activity radios registration (for example, when they initiate a call).

NOTE
On-activity registration is configured for each radio system connection and does ***not*** depend on the registration service activity in SmartPTT.

- Using the Radio Check command.

NOTE
Registration of radios in analog systems has the limited support. For details, submit a request to the SmartPTT Technical Support Center.

Registration information access can be limited over the profile mechanism. If the service is turned off in the profile, all radios will appear “offline”.

4.5.1.1 MOTOTRBO Registration

This section contains information about delivering registration information over the MOTOTRBO protocol.

Data Provider

Registration information is provided from radios to the dispatch subsystem by different providers.

Radio System Access Type	***Provider***
Control stations (except analog interfaces)	Control station
Network Application Interface (except Capacity Max)	Device Discovery and Mobility Service (DDMS)
Capacity Max	Presence Service in Capacity Max System Server
Connect Plus	Presence Notifier in XRC controllers

Recipient

Registration information is sent by a radio to another radio ID.

Radio System Access Type	Radio ID Assignee
Control stations (except analog interfaces)	Control station
Network Application Interface (incl. Capacity Max)	MOTOTRBO Network Interface Service (MNIS)
Connect Plus	Radioserver

Registration Information Update

Registation information is updated in the following way:

- Radioserver sends up to 5 registration update requests to the radio network.
- Radio response timeout is equal to 30 seconds.
- For different radios, registration request interval is equal to 1 second.

4.5.1.2 Configuring ARS

Follow the procedure to activate and configure the radio registration service.

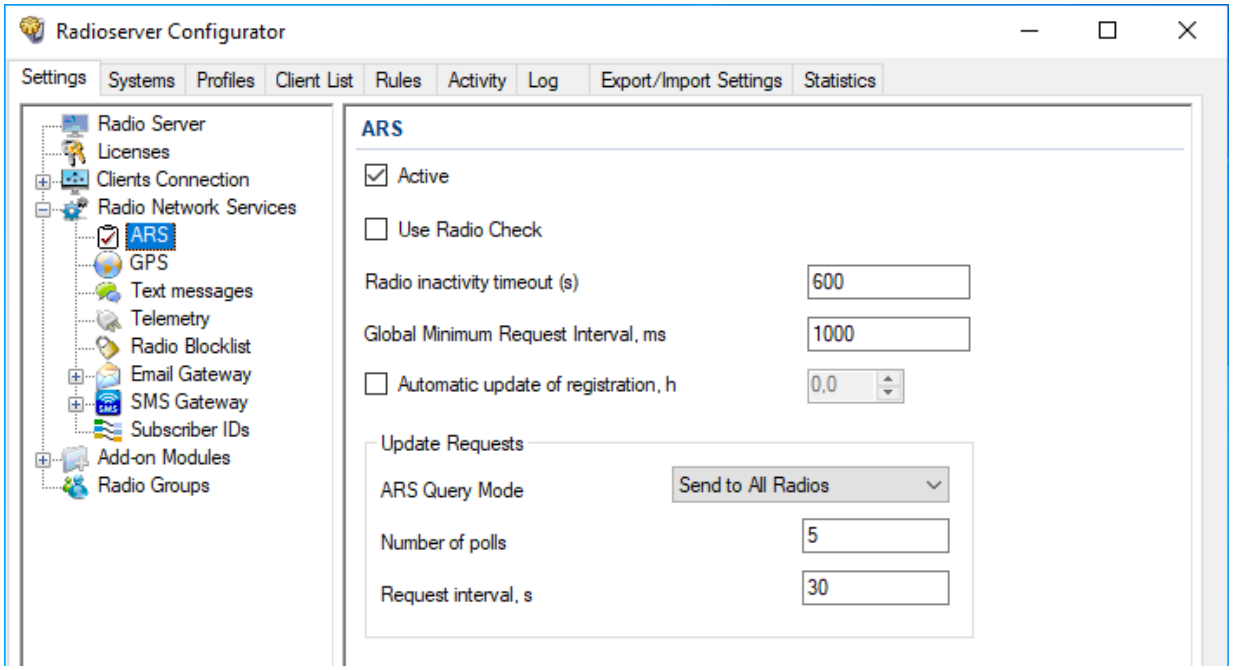
Prerequisites:

When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.

2. In the left pane, expand ***Radio Network Services***, and then click ***ARS***.
   The registration service settings appear in the right pane.



3. Select the ***Active*** check box.
4. If SmartPTT is used in analog systems, select the ***Use Radio Check*** check box.
5. In the ***Radio inactivity timeout (s)*** field, type the radio inactivity timeout in seconds.

NOTE
If a radio does not transmit/respond to anything until the timeout expires, SmartPTT Radioserver will request its presence status update.

6. In the ***Global Minimum Request Interval, ms*** field, type the minimum time interval (in milliseconds) between sequential presence status requests from the radioserver.
7. *(Optional)* Configure the periodic presence status requests:
   a. Select the ***Automatic update of registration, h*** check box.
   b. In the unlocked field, enter the request sending period (in hours) that exceeds the radio inactivity timeout.
8. From the ***ARS Query Mode*** list, select the mode in which SmartPTT Radioserver will send requests to radios to check their presence in the radio network:

For SmartPTT Radioserver to send requests to all radios in the database,	select *Send to All Radios*.
For SmartPTT Radioserver to send requests only to online radios,	select *Send to Active Radios*.

9. In the ***Number of polls*** field, enter a maximum number of requests that SmartPTT Radioserver will send to check radio presence in the network.
10. In the ***Request interval, s*** field, enter time interval after which SmartPTT Radioserver will send requests to radios to check their presence in the radio network.
11. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

4.5.2 Radio Users

Radio users have the unique ID that is sent from the radio to inform SmartPTT about the current user of the radio. The feature is available only for MOTOTRBO systems that use Device Discovery and Mobility Service (DDMS), or MOTOTRBO Capacity Max.

User Database Configuration

To configure the connection to the user database, perform the following actions:

- Configure DBMS. For details, see DBMS Configuration.
- Connect SmartPTT Radioserver to DBMS. For details, see Configuring User Database Connection.
- Configure a list of users. For details, see Managing Radio Users.
- Configure database autobackup. For details, see Configuring User Database Autobackup.

In addition, perform the following actions in the MOTOTRBO infrastructure:

- Enable the *Sign In / Sign Out* feature in radio codplugs.
- If you use the Capacity Max network, perform the following actions:
  - Configure the authentication server for user authorization.
  - Assign the server to subscribers for their authorization.
- If you use the NAI networks, in DDMS, configure the authentication server for user authorization.
- If you use the NAI networks, where MNIS and DDMS interfaces are installed separately from the SmartPTT Radioserver host, additionally in MNIS, in the DDMS settings, specify the radioserver IP address.

NOTE
When using local or domain authentication, database configuration is available only to users in the *Database Administrators* group.

4.5.2.1 Configuring User Database Connection

Follow the procedure to configure the user authorization service.

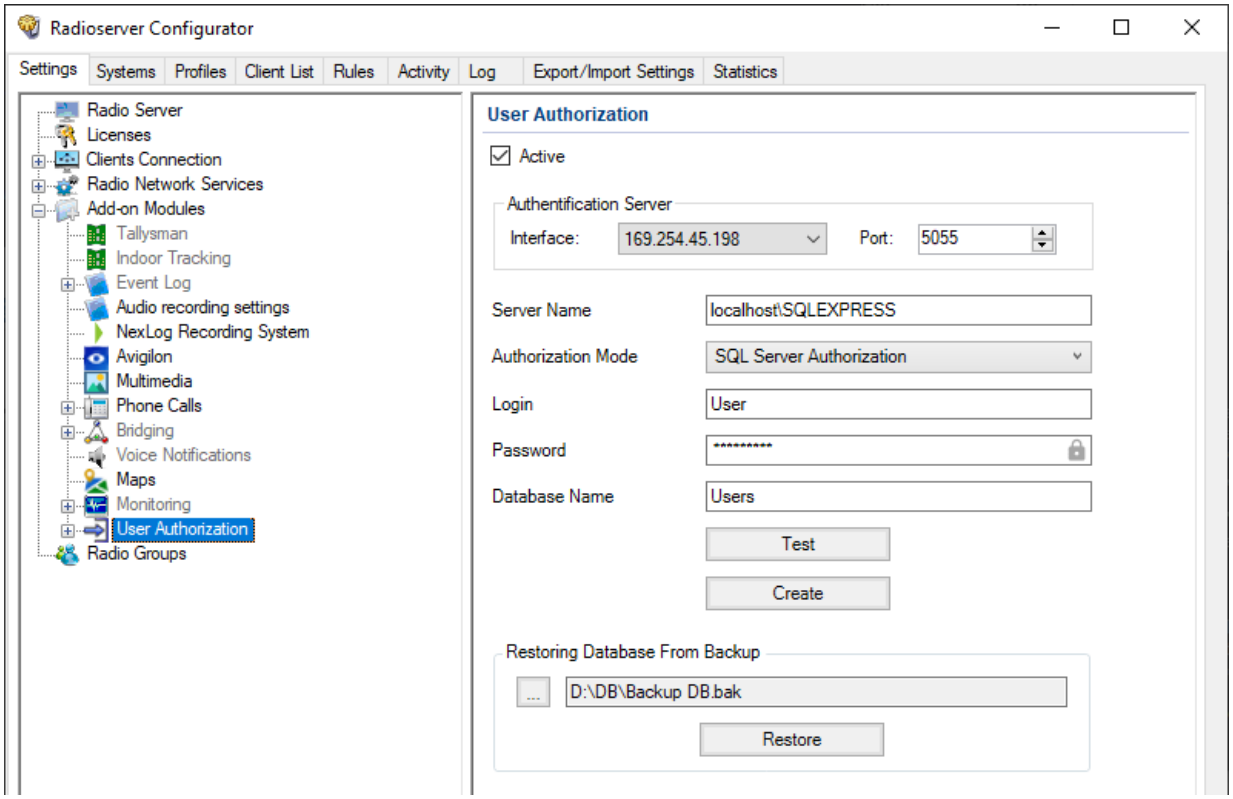
Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *Database Administrators* group. For details, see Loging in to Radioserver Configurator.
- Configure DBMS. For details, see DBMS Configuration.
- Obtain the DBMS network address and process name.
- To use DBMS authorization, obtain the desired credentials. For details, see Adding SQL Server Users.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.

2. In the left pane, expand the ***Add-on Modules*** node, and then click ***User Authorization***.
   The user authorization settings appear in the right pane.



3. Select the ***Active*** check box.
4. From the ***Interface*** list, select the proper element:

To use any radioserver address for connection,	select *Any*.
To use fixed radioserver IP address,	select the desired address.

Important
If a radioserver and the MNIS service are installed on the same computer, use fixed address that is different from the MNIS IP address (default is *192.168.56.1*).

Important
If a a radio or control station is connected to the radioserver host, use fixed address that is different from the radio or control station address (default is *192.168.10.1*).

5. In the ***Port*** field, enter the port number for authorization requests.
6. In the ***Server Name*** field, type the DBMS address in the following format:
   <host name or IP address>\<DBMS service name>
7. Configure authorization in the DBMS:

To use Windows authorization,	from the ***Authorization Mode*** list, select *Windows NT Authorization*.

To use DBMS authorization,	perform the following actions: 1. From the ***Authorization Mode*** list, select *SQL Server Authorization*. 2. In the ***Login*** field, type the login of the desired SQL Server account. 3. In the ***Password*** field, type the password of the desired SQL Server account. To view the entered password, click the eye icon ( ). For security reasons, the password will not be available for viewing in subsequent sessions.

8. In the ***Database Name*** field, type the DBMS process name.

Important
If SQL Server was installed after SmartPTT, or if it is located on a remote computer, the database will not be available for configuration or use. Additionally, the database will be inaccessible if the user has created an account for database authorization instead of using Windows authentication.

9. *(Optional)* Click ***Test*** to check the connection with SQL Server and access to the database.
A message appears if the connection was successful or not.
10. Click ***Create*** to create a database with the specified parameters.
A message appears if the connection was successful or not.
11. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Add radio users. For details, see Managing Radio Users.
- Configure database auto backup. For details, see Configuring User Database Autobackup.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

4.5.2.2 Managing Radio Users

Follow the procedure to add, edit, or delete the radio user entry.

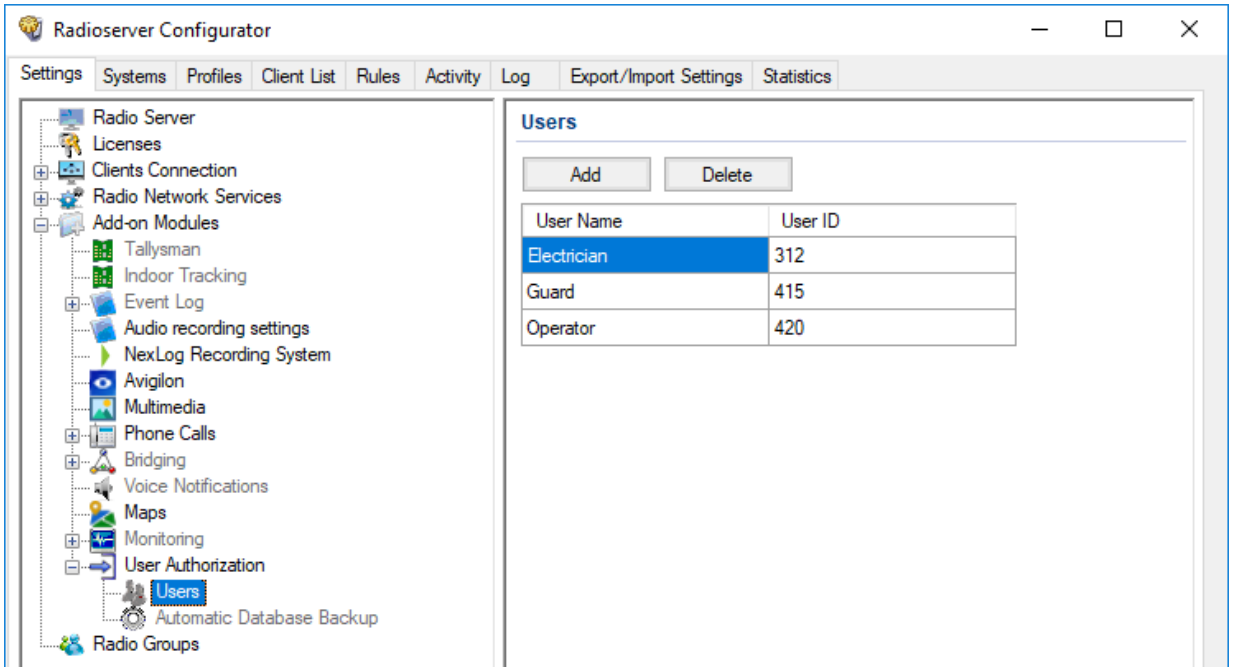
Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *Database Administrators* group. For details, see Loging in to Radioserver Configurator.
- Determine user IDs.
- Configure the user database connection. For details, see Configuring User Database Connection.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.

2. In the left pane, expand ***Add-on Modules*** → ***User Authorization***, and then click ***Users***.
   List of users appears in the right pane.



3. Perform one of the following actions:

To add a new user,	click ***Add***.
To modify a user's name and/or ID,	proceed to the next step of the procedure.
To delete a user,	perform the following actions: 1. Click the desired user entry. 2. Click ***Delete***. 3. Proceed to the last step of the procedure.

4. In the desired table row, in the ***User ID*** column, double-click the current ID, and then type the desired ID.

Important
Do not confuse User ID and Radio ID.

5. *(Optional)* In the same row, in the ***User Name*** column, double-click the current user name, and then type the desired name.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

4.5.2.3 Configuring User Database Autobackup

Follow the procedure to configure the automatic database backup.

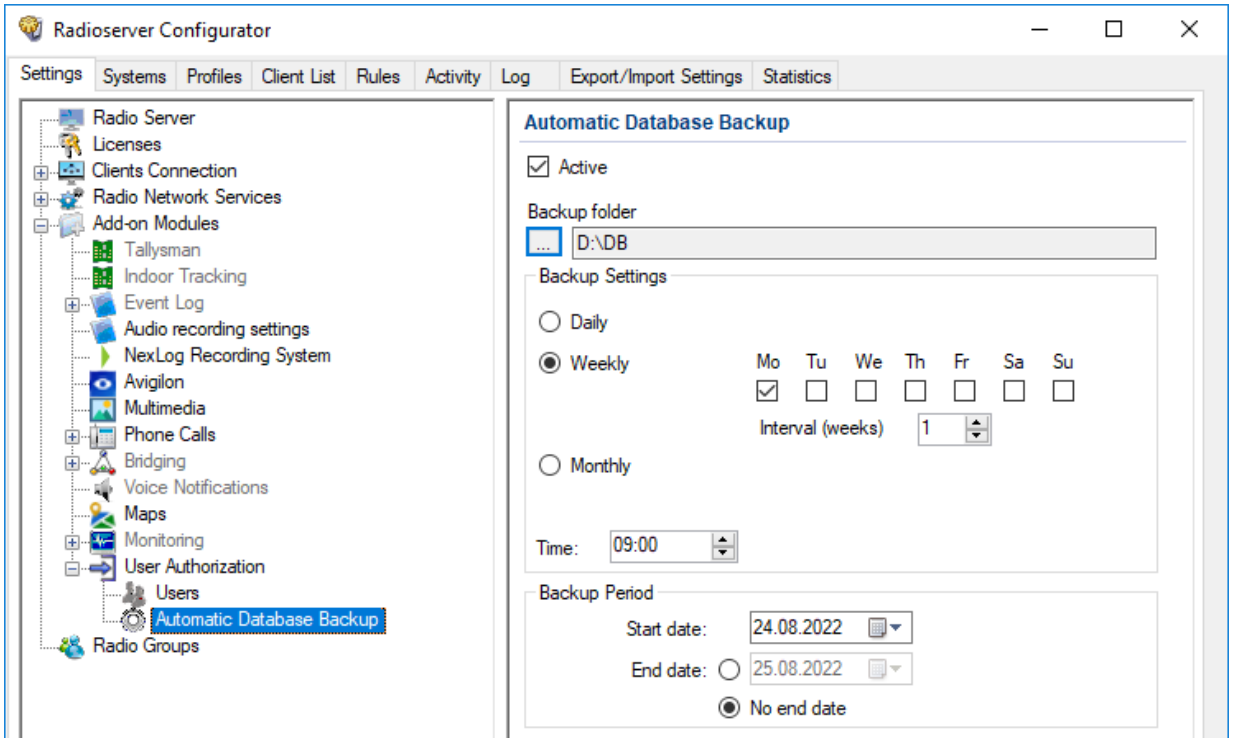
Important
If SQL Server was installed after SmartPTT, or if it is located on a remote computer, the database will not be available for configuration or use. Additionally, the database will be inaccessible if the user has created an account for database authorization instead of using Windows authentication.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *Database Administrators* group. For details, see Loging in to Radioserver Configurator.
- Add radio users. For details, see Configuring User Database Connection.
- Determine the backup storage.
- Make a schedule for backups.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Add-on Modules*** → ***User Authorization***, and then click ***Automatic Database Backup***.
   The backup settings appear in the right pane.



3. Select the ***Active*** check box.
4. Specify the folder for backups:
   a. Click the Browse (...) button to the left of the ***Backup folder*** field.
      The dialog box appears.
   b. In the dialog box, select the desired directory and click ***OK***.
5. In the ***Backup Settings*** area, configure the period of the backup:

To create backups once in a few days,	perform the following actions: 1. Click ***Daily***. 2. In the ***Interval (days)*** field, enter the number of days between backups (*1* means daily backups).
To create backups on specific days of week with the specific time period,	perform the following actions: 1. Click ***Weekly***. 2. Using check boxes to the right, select week days when the backup must be created. 3. In the ***Interval (weeks)*** field, enter the number of weeks between backups (*1* means weekly backups).
To create backups on specific days of month,	perform the following actions: 1. Click ***Monthly***. 2. In the ***Day of month*** field, enter the day of the month when the backup must be created. 3. In the ***Interval (month)*** field, enter the number of months between backups (*1* means monthly backups).

6. In the ***Time*** field, enter the time when the backup process starts.
7. *(Optional)* In the ***Backup Period*** area, configure start and end dates of the time interval when the backups must be created:
   a. In the ***Start date*** field, enter the start date of the backup creation.
   b. Configure the date when the backup creation will be stopped:

To create backups at a specified interval as long as the SmartPTT Radioserver is running,	click ***No end date***.
To stop creating backups after the specified end date,	perform the following actions: 1. Click ***End date***. 2. In the unlocked field, enter the end date.

8. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

4.6 Location

SmartPTT supports radios that are able to report their location in the various location systems. Those systems are as follows:

- Satellite systems that are widespead for global geographical location determination (radio latitude and longitude).
- Beacon systems that are widespread for indoor and/or local location determination. For details, see Location with Option Boards.

Interaction with satellite systems can be organized in the following ways:

- Data exchange over the MOTOTRBO protocol. For details, see Location in Radio Systems.
- Data exchange using the dedicated protocol provided by option boards. For details, see Location with Option Boards.

Important
Location using satellites is supported only for MOTOTRBO radios.

MOTOTRBO radios support location setup and reporting using MOTOTRBO proprietary protocols as well as Location Information Protocols (LIP). For instance, LIP is used for location requests sent over the control channel in Capacity Max. Beware that LIP support does not guarantee interoperability with other LMR manufacturers. For more information on that, please contact Motorola Solutions.

Location Report Recipient

Each MOTOTRBO radio (with and without an option board) provides its location report to the specific ID. The ID is selected from the pool of Radio IDs.

As radio systems work together with SmartPTT, ID selection is affected with the following limitations:

- If radioserver receives location reports over a control station, all radios must report their location to the Radio ID of the control station.
- If radioserver receives location reports over the Network Application Interface (NAI) or it is connected to Capacity Max, radios must report their location to the Radio ID assigned to the MNIS service.

Important
Dispatcher IDs must never be used as recipient IDs of the location reports.

4.6.1 Location in Radio Systems

SmartPTT supports location requests and provides location reports/responses to SmartPTT Dispatcher applications. SmartPTT Dispatcher uses location reports for the following purposes:

- Shows the current radio location on maps.
- Tracks radios using routes, geofences, and points of interest.

Also, location reports could be used for rules configuration. For details, see “Positioning Rules” in *SmartPTT Dispatcher Guide*.

Location Update Rate

In MOTOTRBO, the location update rate is determined with the following factors:

- Radio system interface (control station, direct IP connection, or NAI).
- CSBK data support.
- Window size.

As a result, the following results could be achieved:

Minimum Update Interval	*Maximum Update Rate*	*Window Size*
7.5 s	8 times per minute	1 or 2

Minimum Update Interval	Maximum Update Rate	Window Size
15 s	4 times per minute	5
30 s	2 times per minute	6
60 s	1 time per minute	7
120 s	30 times per hour	8
240 s	15 times per hour	9
480 s	7–8 times per hour	10

Radio Channel Capacity

Maximum number of location reports that could be provided over the radio channel is determined by the following factors:

- Radio system interface (control station, direct IP connection, NAI).
- CSBK data support.
- Window size.
- Voice/data ratio configured on the repeater slot.

Depending on them, the following results could be achieved:

Window Size	Number of location reports per minute			
	90%	75%	60%	45%
1	904	752	600	456
2	448	376	304	224
5	180	150	120	90
6	150	125	100	75
7	128	107	86	64
8	112	93	75	56
9	100	83	66	50
10	90	75	60	45

In the table, percentage is related to the repeater slot allocation for data retransmission.

Important
All the numbers in the table are the maximum values. Real slot capacity is lower because of the radio signal attenuation, radio frequency interference, on-site surface complexity, etc.

4.6.1.1 Configuring GPS

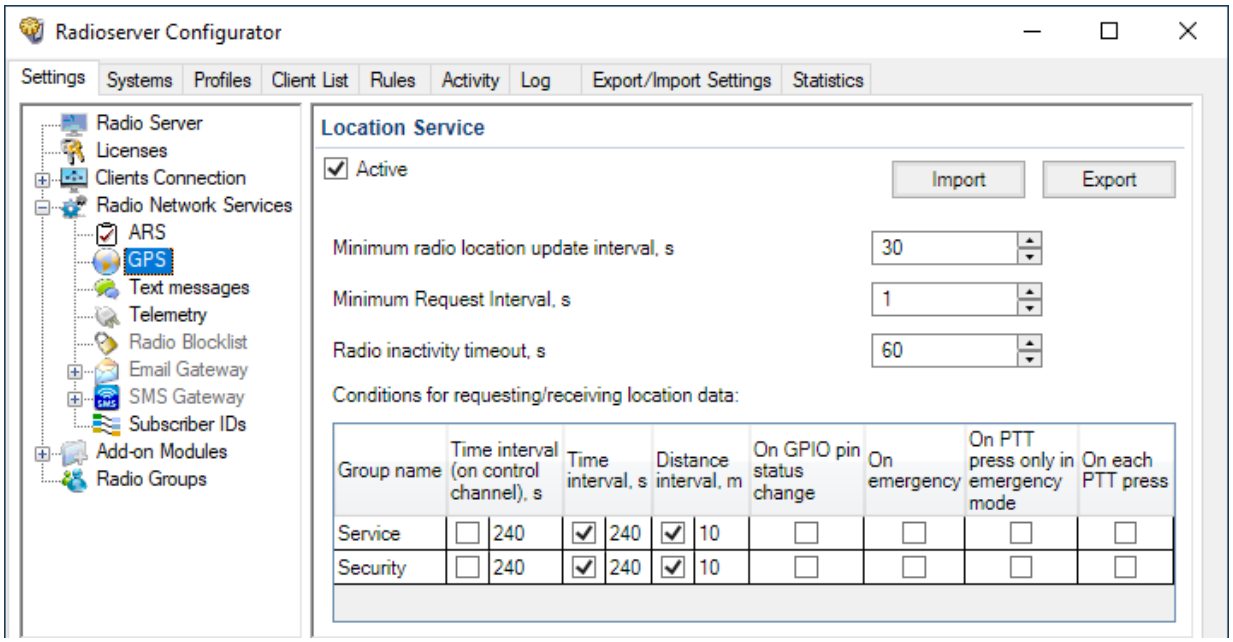
Follow the procedure to activate and configure GPS location service.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Add radio groups. For details, see Managing Radio Groups.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Radio Network Services***, and then click ***GPS***.
   The satellite location settings appear in the right pane.



3. Select the ***Active*** check box.
4. *(Optional)* If you want to import a previously saved list of location trigger settings, in the top right corner of the pane, click ***Import***, and then select the desired file.

Important
The contents of the file will overwrite any triggers you have configured in the table.

5. In the ***Minimum radio location update interval (s)*** field, type the minimum radio location update time interval (in seconds) that can be set by the dispatcher.
6. In the ***Minimum Request Interval, s*** field, type the minimum time interval (in seconds) between location requests to any radio.
7. In the ***Radio inactivity timeout (s)*** field, type the time interval (in seconds) after which a radio that did not send GPS location is considered as potentially inactive to send location update request.
8. In the ***Conditions for requesting/receiving location data*** table, configure automatic GPS update for radios included in the desired group:

To update the position of radios over the control channel with a specific time interval, ***NOTE*** This is available only in Capacity Max systems. The number and frequency of location updates over the control channel is limited. Also, keep in mind that these updates cannot be used for building the coverage map.	perform the following actions: 1. In the corresponding entry, in the ***Time interval (on control channel), s*** column, select the check box. 2. Next to the check box, type the desired update interval (in seconds). ***NOTE*** If radio coordinates are not received on the control channel within the specified interval, they are requested again after the time specified in the ***Radio inactivity timeout*** field.
To update the position of radios with a specific time interval,	perform the following actions: 1. In the corresponding entry, in the ***Time interval, s*** column, select the check box. 2. Next to the check box, type the desired update interval (in seconds).
To update the position when radios pass a certain distance,	perform the following actions: 1. In the corresponding entry, in the ***Distance interval, m*** column, select the check box. 2. Next to the check box, type the desired distance (in meters).
To update the position when radios send the telemetry signal,	in the corresponding entry, in the ***On GPIO pin status change*** column, select the check box. ***Important*** To ensure correct operation of the feature, the ***GNSS Report*** check box must be selected for the desired GPIO physical pins in the radio codeplugs.
To update the position when radios send the emergency alarm,	in the corresponding entry, in the ***On emergency*** column, select the check box.
To update the position when the radio PTT button is pressed to make the emergency call,	in the corresponding entry, in the ***On PTT press only in emergency mode*** column, select the check box.
To update the position each time the radio PTT button is pressed,	in the corresponding entry, in the ***On each PTT press*** column, select the check box. ***Important*** The feature is available only in NAI radio systems.

NOTE
In SmartPTT Dispatcher, you can also configure conditions of radio location updates.
For information on the algorithm for choosing between settings, see Location.

9. *(Optional)* To export the configured triggers as a CSV file, at the top right corner of the pane, click ***Export***, and then select the destination file.
10. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

4.6.2 Location with Option Boards

SmartPTT supports radios that use option boards for satellite navigation. In particular, it supports option boards programmed with the Tallysman Sprite Configurator.

Capabilities and Limitations

Boards programmed with Tallysman Sprite Configurator provide the following features to SmartPTT:

- High rate of location updates (up to 6 times per minute).
- Location reports storing when the radio is out of the RF coverage zone (up to 12 times per minute).
- Great reports storage interval (up to 30 days).

When the radio returns to the RF coverage zone, it starts sending stored reports to SmartPTT. With this, SmartPTT provides the following features:

- Provides reports to active dispatch consoles in real time.
- Dispatch consoles update radio tracks and log location reports in its database.

Using option boards for satellite location results in the following limitations:

- ATEX-compliant radios do not support option board installation and use.
- Radios cannot be used in the Connect Plus radio systems due to the dedicated option boards utilization.
- Location reports cannot be provided over the revert channel of the radio system.
- Location reports cannot be provided over control stations that are accessible over RG-1000e.
- Radios cannot operate in the Enhanced GNSS mode.

Location Configuration

To configure radio location using option boards, the following actions must be performed:

- Option board must be programmed with the Tallysman Sprite Configurator. For details, see Configuring Location Storage in GOB.
- *(Optional)* Revert mode needs to be configured. For details, see Configuring GOB Reverting.
- Option board reports must be supported in SmartPTT. For details, see Configuring GOB Reports Reception.

4.6.2.1 Configuring Location Storage in GOB

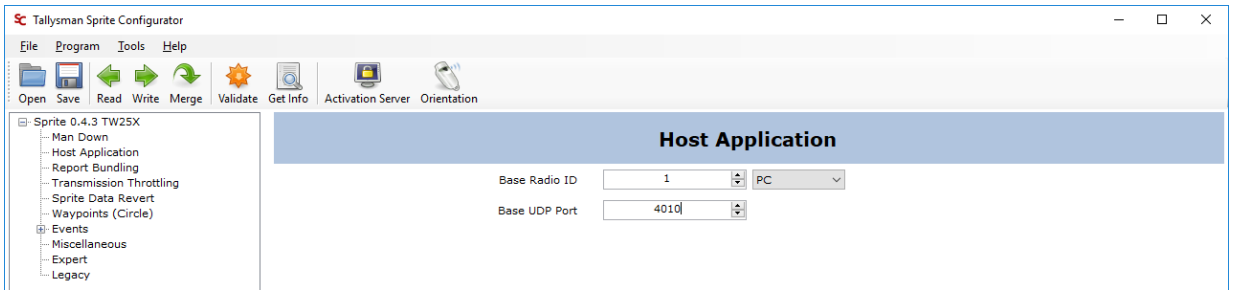
Follow the procedure to view and/or modify option board settings required to support location reports storage and their provision to SmartPTT.

Prerequisites:

- Determine the proper target ID for location reports:
  - If control stations are used, from the station codeplug, obtain its Radio ID.
  - If NAI is used to access a radio system, or radioserver connects to Capacity Max, use the MNIS Application ID. For details, see “MNIS Application ID” in the MNIS Configuration Utility embedded help.
- Determine if a control station or IP Site Connect slot is used as a data channel:
  - For information on control station parameters, see Configuring MOTOTRBO Control Station Connection.
  - For information on the IP Site Connect slot parameters, see Configuring SmartPTT Identification.
- Start the Tallysman Sprite Configurator, and then ensure that its version is 0.3.16.

Procedure:

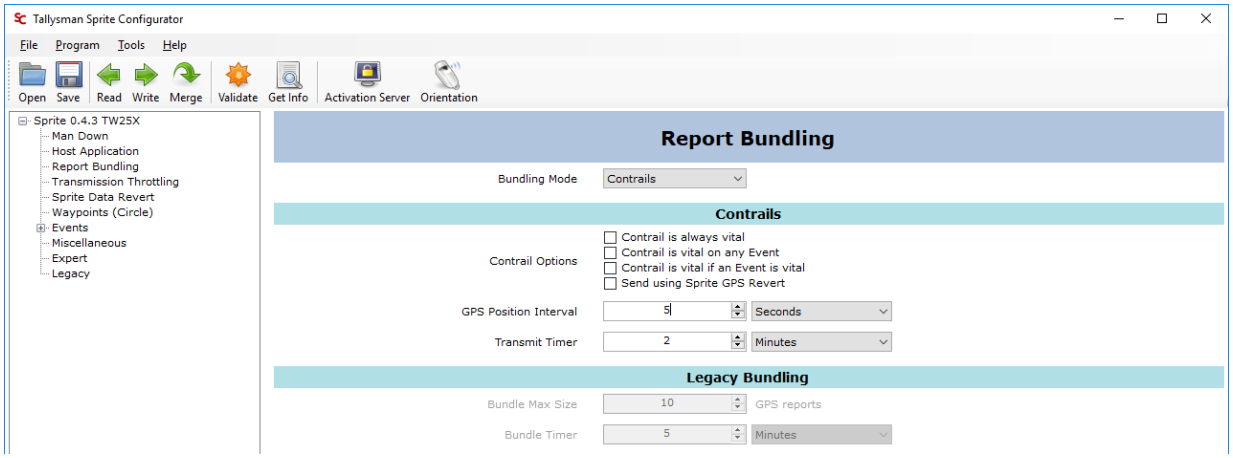
1. Open the option board codeplug.
2. In the left pane, expand the ***<Codeplug Internal Name>***, and then click ***Host Application***.
   Host settings appear in the right pane.



3. In the right pane, enter the SmartPTT Radioserver identification information:
   a. In the ***Base Radio ID*** field, enter radioserver ID in the relevant radio system.
   b. From the list that appears next to field, select *PC*.
   c. In the ***Base UDP Port*** field, set the radioserver UDP port used to receive location reports.

NOTE
If default value is applicable, leave the parameter unchanged.

4. In the left pane, click ***Report Bundling***.
   Report settings appear.



5. In the right pane, from the ***Bundling Mode*** list, select *Contrails*.
6. Clear the following check boxes:
   - Contrail is always vital
   - Contrail is vital on any Event
   - Contrail is vital if an Event is vital
7. Configure the location report delivery mode:

To send reports over the fixed slot,	configure reverting. For details, see Configuring GOB Reverting.
To send reports over the slot that provided the location request,	clear the ***Send using Sprite GPS Revert*** check box.

8. Configure the location request interval:
   a. From the list next to the ***GPS Position Interval*** field, select the desired measurement units.
   b. In the ***GPS Position Interval*** field, set the desired period of time. The recommended value is *10 s*.
9. Configure the location transmission attempt interval:
   a. From the list next to the ***Transmit Timer*** field, select the desired measurement units.
   b. In the ***Transmit Timer*** field, set the desired period of time. The recommended value is *2 s*.
10. In the left pane, expand ***Events***.
11. For each subnode of the ***Events*** node, perform the following actions:
    a. Click the subnode.
    b. In the right pane, clear the ***Event Enabled*** check box.
12. Save changes to the codeplug and write them to the option board.

4.6.2.2 Configuring GOB Reverting

Follow the procedure to configure the location data sending over the fixed channel configured in the radio. This option is available only in IP Site Connect radio systems.

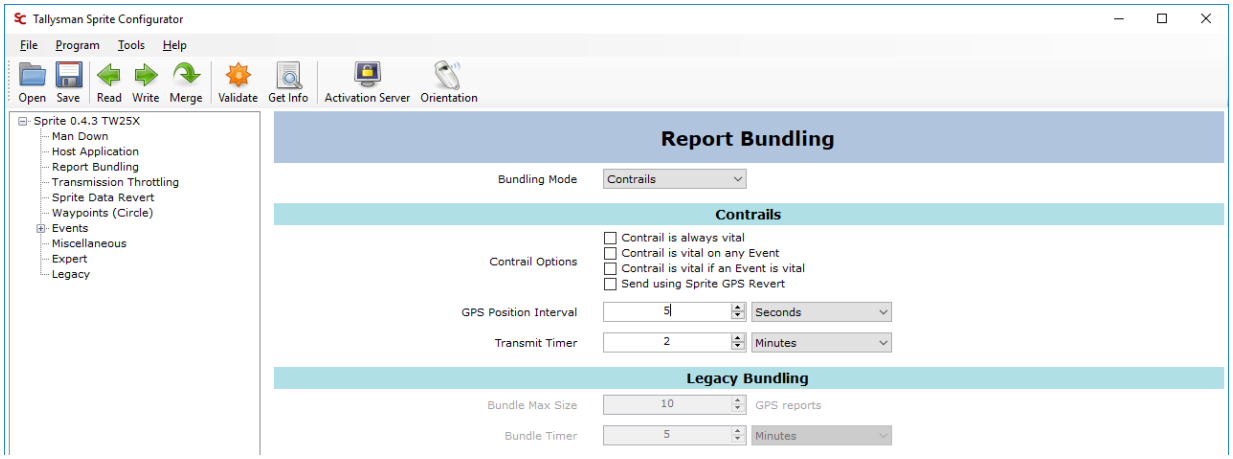
Important
In radio system, the required channel must ***not*** be used as data revert channel. Sending location reports over the revert channels is not supported.

Prerequisites:

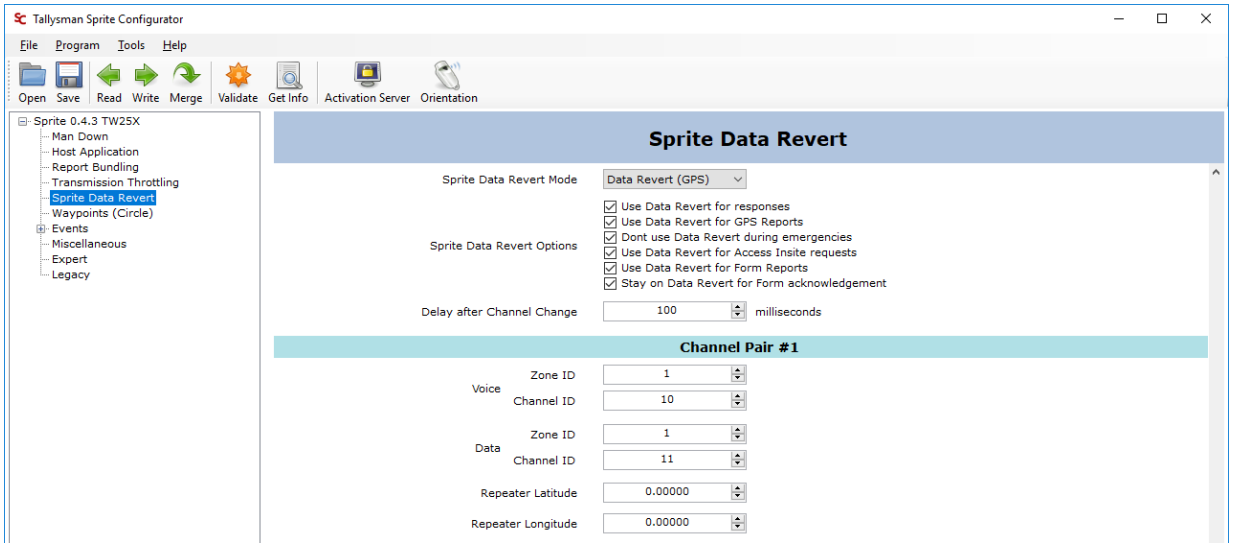
- Turn off the Enhanced GNSS mode for time slot of the repeater that is placed in the same site as the radio. If the slot is system-wide, turn off Enhanced GNSS in all repeaters of the system.
- From the radio codeplug, obtain the Zone ID and Channel ID for the corresponding slot.
- In radio codeplugs, turn off the Data Revert mode.
- Start the Tallysman Sprite Configurator, and then ensure that its version is 0.3.16.

Procedure:

1. Open the option board codeplug.
2. In the left pane, expand the ***<Codeplug Internal Name>***, and then click ***Report Bundling***.
   Revert settings appear in the right pane.



3. In the right pane, in the Contrails area, select the ***Send using Sprite GPS Revert*** check box or ensure that it is selected.
4. In the left pane, click ***Sprite Data Revert***.
   Revert mode settings appear in the right pane.



5. In the right pane, from the ***Sprite Data Revert Mode*** list, select *Data Revert (GPS)*.
6. To the right of the ***Sprite Data Revert Options*** heading, select all check boxes.
7. *(Optional)* In the ***Delay after Channel Change*** field, set the delay (in milliseconds) between the data channel selection and location data sending.
8. In the ***Channel Pair #1*** area, perform the following actions:
   a. To the right of the ***Data*** heading, in the ***Zone ID*** field, enter the zone ID where the target channel belongs.
   b. To the right of the ***Data*** heading, in the ***Channel ID*** field, enter the ID of the channel that will be used for location reports sending.
9. In the same area, in all other fields, enter *0*.
10. Enter *0* in all fields of all of the following areas (from ***Channel Pair #2*** to ***Channel Pair #8***).
11. Save changes to the codeplug and then write them to the option board.

Postrequisites:

- Configure other option boards in the same way.
- In the corresponding slot settings, activate the Data Channel mode. For details, see Configuring SmartPTT Identification.

4.6.2.3 Configuring GOB Reports Reception

Follow the procedure to configure movement reports restoration in SmartPTT.

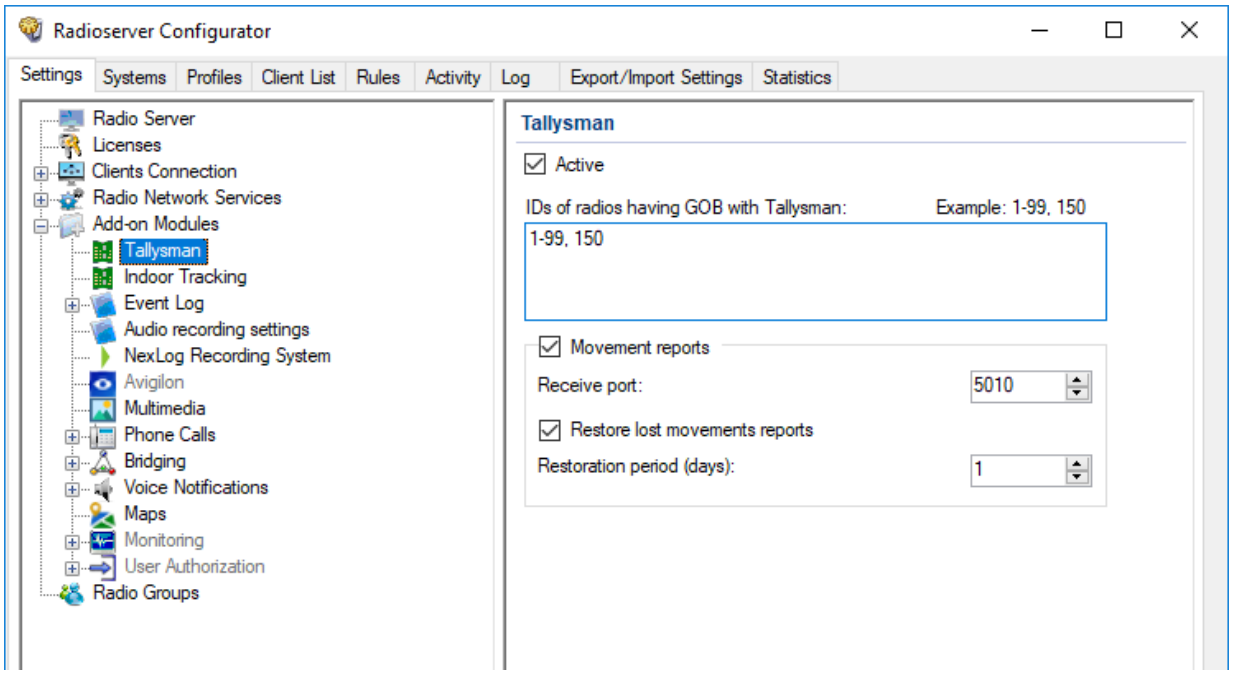
Prerequisites:

- Obtain Radio IDs of radios that have option boards configured for the feature.
- Using Tallysman Sprite Configurator, obtain the target UDP port (related to the ***Base UDP Port*** parameter). For details, see Configuring Location Storage in GOB.
- Determine the necessity of the restoration period limitation and determine the limiting value.

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Add-on Modules***, and then click ***Tallysman***.



3. In the right pane, select the ***Active*** check box.
4. In the ***IDs of radios having GOB with Tallysman*** field, type radio IDs of subscriber units with properly configured option boards. Use hyphens to enter radio ID ranges; use commas to list radio IDs and ID ranges.
5. Select the ***Movement reports*** check box.
6. In the ***Receive port*** field, set the value of the ***Base UDP Port*** parameter from the Tallysman Sprite Configurator.
7. To limit the restoration period, perform the following actions:
   a. Select the ***Restore lost movements reports*** check box.
   b. In the ***Restoration period (days)*** field, set the restoration period in days.

NOTE
The day unit here is equal to 24 hours. If you type *3*, SmartPTT Radioserver requests coordinates collected on the GOB within the last 72 hours.

8. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

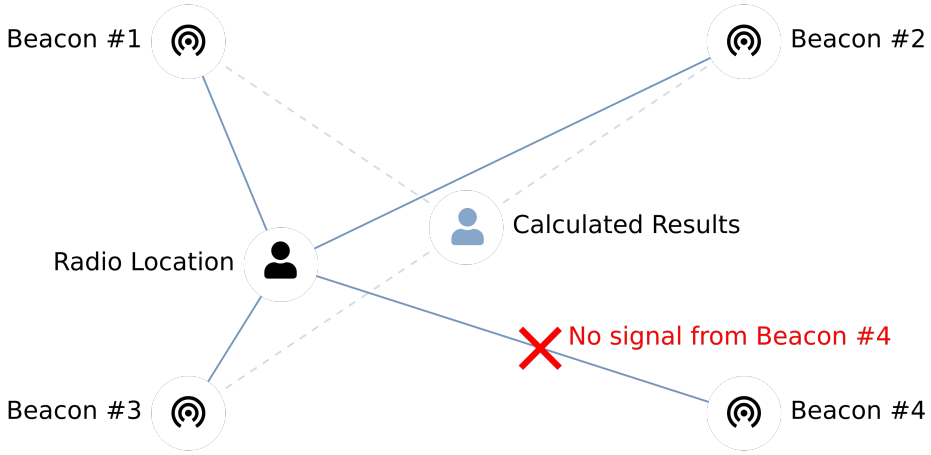
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- In the firewall software on the computer, unlock the specified UDP port. For details, see Radioserver Host.

4.6.3 Beacon-Based (Indoor) Location

SmartPTT supports radios that report their location using radio beacon signals. Such systems operate in the following way:

- Radio receives signals from one or multiple nearby radio beacons which location is known.
- Radio sends IDs of beacons that were recognized to SmartPTT.
- SmartPTT receives beacon IDs and determines the radio location in the point that is equidistant from the beacons.

Important
SmartPTT does ***not*** support the radio location determination based on the signal strength or other methods due to their unreliability.



NOTE
Beacon-based location systems may also be referred to as “Indoor Location Services”.

SmartPTT supports the following beacon-based technologies:

- iBeacon. For details, see iBeacons Technology.
- BluFi Wireless. For details, see BluFi and Kilchherr.
- Kilchherr Elektronic AG. For details, see BluFi and Kilchherr.

Location reports are sent to the radioserver ID that is determined in one of the following ways:

- If radioserver uses control stations to receive reports, on-site radios must send reports to the Radio ID of the control station.
- If radioserver uses NAI for the radio system connection or connects to Capacity Max, radios must send reports to the MNIS Application ID.

4.6.3.1 iBeacons Technology

iBeacon technology is based on the Bluetooth capabilities. It requires radios to have the built-in Bluetooth module. With it, radio accesses the following features:

- Beacon-based location in Connect Plus.
- Using option boards for various purposes:
  - Radios registration.

- Location using satellite systems. For details, see Location with Option Boards.

Important
In Connect Plus, radios must send location reports to the radioserver ID.

iBeacon Configuration

To configure the iBeacon location technology, the following actions must be performed:

- Ensure that the radio has the built-in Bluetooth module.
- In the radio, install the license that unlocks indoor services.
- In the radio codeplug, turn on the following services:
  - Location services
  - Indoor location services
  - Bluetooth
- Add a list of beacons to the radio codeplug.

Important
All of the information above provides the minimum required modification of the radio codeplug. It is ***not*** related to the complete radio configuration. If you need assistance in the MOTOTRBO devices configuration, contact Motorola Solutions representatives in your region.

4.6.3.2 BluFi and Kilchherr

Reports provision using BluFi technology and Kilchherr technology differs from the iBeacon technology. They are based on the dedicated option boards. Using boards results in the following limitations:

- They are ***not*** applicable in Connect Plus.
- They are incompatible with the location reports storage. For details, see Location with Option Boards.

BluFi

To configure radios to use the BluFi technology, the following actions must be performed:

- Option board must be configured as instructed by BluFi. For information on compatible option boards, see Third Party Products.
- Text messages must be turned on in radioserver. For details, see Configuring Beacons in SmartPTT.

Kilchherr

To configure radios to use the Kilchherr technology, compatible option boards must be configured as instructed by vendors. For information on compatible option boards, see Third Party Products.

4.6.3.3 Configuring Beacons in SmartPTT

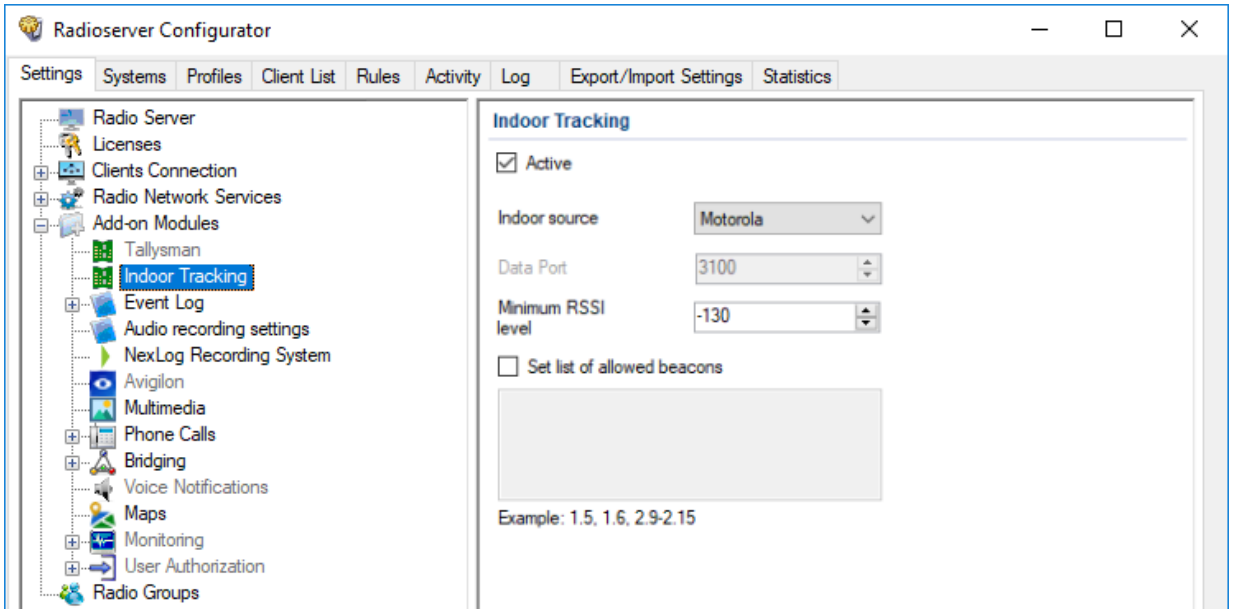
Follow the procedure to activate beacon-based location in SmartPTT.

Prerequisites:

- Configure radio devices to support the desired beacon-based location.
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- If BluFi is used, activate text message service in SmartPTT. For details, see Activating Text Message Sending and Receiving.
- Ensure that the SmartPTT license allows Indoor services. For details, see Viewing License Items.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Add-on Modules***, and then click ***Indoor Tracking***.
   The beacon-based location settings appear in the right pane.



3. In the right pane, select the ***Active*** check box.
4. Configure the desired technology:

To use iBeacon,	perform the following actions: 1. From the ***Indoor source*** list, select *Motorola*. 2. In the ***Minimum RSSI level*** field, enter the minimal reliable signal strength level.
To use BluFi Wireless,	from the ***Indoor source*** list, select *BluFi*.
To use Kilchherr,	perform the following actions: 1. From the ***Indoor source*** list, select *Kilchherr*. 2. In the ***Data Port*** field, enter the radioserver port number.

5. *(Optional)* Configure beacons:

To receive signals from any beacon,	clear the ***Set list of allowed beacons*** check box.
To receive signals from the limited set of iBeacons,	perform the following actions: 1. Select the ***Set list of allowed beacons*** check box. 2. In the unlocked field, type beacon IDs in the following format: *<group number>.<beacon number in the group>*. Use hyphens to enter ranges; use commas to list IDs and ID ranges.
To receive signals from the limited set of BluFi/Kilchherr beacons,	perform the following actions: 1. Select the ***Set list of allowed beacons*** check box. 2. In the unlocked field, type beacon IDs. Use hyphens to enter ranges; use commas to list IDs and ID ranges.

NOTE
List of configured iBeacons must correlate with the list of beacons configured in radio codeplugs.

6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (*** ***)***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (*** ***)*** or ***Restart (*** ***)***.
- If Kilchherr is used, in the firewall software on the computer, unlock the specified UDP port. For details, see Radioserver Host.

4.6.4 Complex Location Reports

If the radio location is simultaneously tracked with satellite and beacon location systems, radio channel bandwidth can be insufficient for data transmission. As a result, several reports and/or beacon signals could be lost. This results in the invalid radio location.

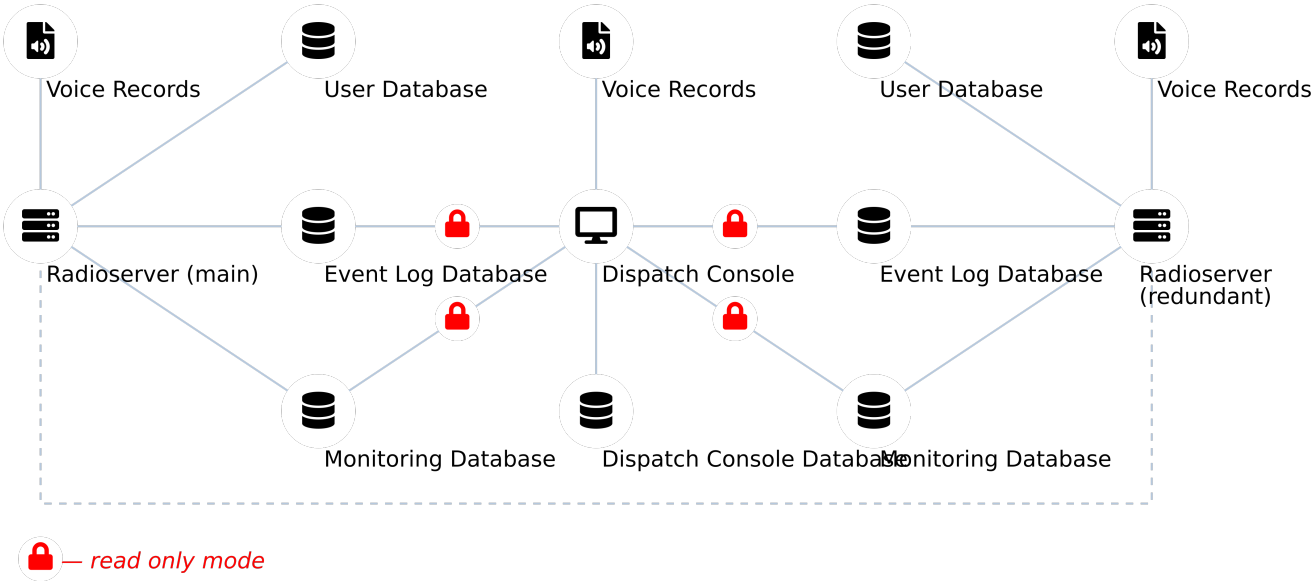
To optimize the location update, the following actions are recommended to be performed:

- Radio codeplugs must be modified in the following way:
  - Enhanced GNSS must be turned off for the used slots.
  - Configure Windows Size to be equal to *10*.
  - Turn on the compressed UDP headings.
  - Select the compression format to be equal to *MSI*.
- In repeater codeplugs, Enhanced GNSS must be turned on for repeater slots.
- In SmartPTT Dispatcher, indoor location update interval must be configured to be equal to 30 seconds.

4.7 Logging

SmartPTT logs information about events that occur during its operation. The following software components are able to log information:

- Radioserver.
- Each individual dispatch console.



The following information is related to the radioserver logging. For information on the dispatch console logging, see the following sections:

- For events information, see “Event Log and Notification Panels” in *SmartPTT Dispatcher Guide*.
- For voice records information, see “Call Records” in *SmartPTT Dispatcher Guide*.

DBMS Utilization

SmartPTT uses database management system to store event records. Voice records are stored outside DBMS. For details, see Voice Recording.

SmartPTT supports Microsoft SQL Server only. For information on the supported DBMS versions, see Third Party Products.

DBMS access and authorization are managed by various services. They can be implemented in one of the following ways:

Authorization Type	Applicability
Windows local authorization	Radioserver and DBMS are installed on the same computer.
Windows active directory (domain) authorization	Radioserver and DBMS are installed on the same computer. • Radioserver and DBMS are installed on different computers that belong to the same active directory. • Radioserver and DBMS are running on behalf of the same active directory user.
DBMS-controlled authorization	DBMS is configured to authenticate users.

4.7.1 Event Log Database

Event log database in radioserver stores the following event information:

- Voice calls (group and private calls).
- Emergency alarms and calls.
- Voice-equivalent transmissions (voice notifications, audio files data).
- Radio registration reports.
- Radio location reports.
- Radio commands and their responses.
- Telemetry and remote control commands.

Activate and configure the database to provide the following SmartPTT features:

- Radioserver rules. For details, see Rules.
- Viewing radioserver-logged events and listening to radioserver-logged voice records in SmartPTT Dispatcher. For details, see “Database” in *SmartPTT Dispatcher Guide*.
- Creating reports in SmartPTT Dispatcher. For details, see “Reports” in *SmartPTT Dispatcher Guide*.

Important
Radioserver database (not DBMS) must ***not*** be used by SmartPTT Dispatcher to log events information.

Event Log Database Configuration

To configure the event log database, perform the following actions:

- Configure the database management system. For details, see DBMS Configuration.
- Connect SmartPTT Radioserver to the database. For details, see Configuring Event Log Database Connection.
- Configure the database retention policy. For details, see Configuring Event Log Database Retention Policy.
- Configure the database automatic backup. For details, see Configuring Event Log Automatic Backup.

NOTE
When using local or domain authentication, database configuration is available only to users in the *Database Administrators* group.

4.7.1.1 Configuring Event Log Database Connection

Follow the procedure to configure the event log database connection and enable event logging.

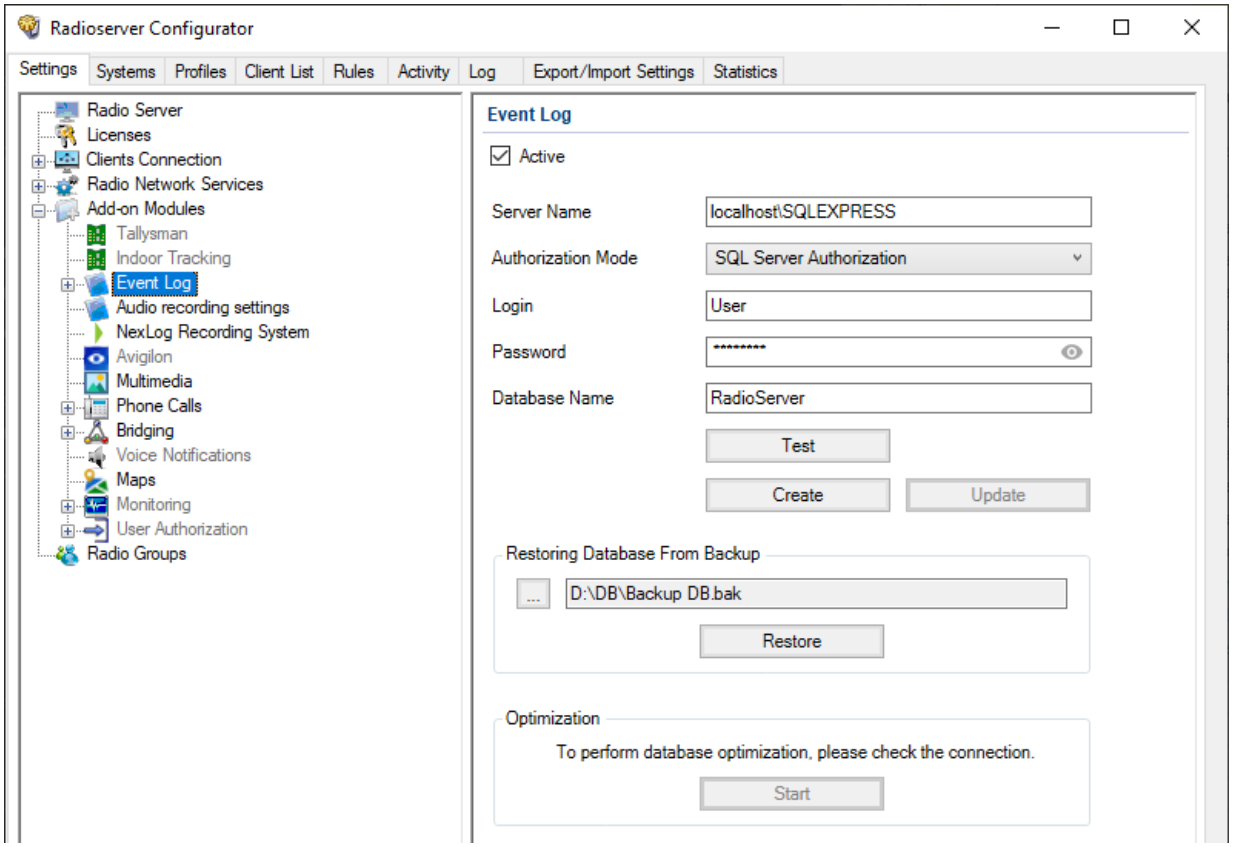
Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *Database Administrators* group. For details, see Loging in to Radioserver Configurator.
- Obtain IP address/domain name of the DBMS host.
- Obtain DBMS process name.
- If DBMS authorization is used, obtain the corresponding credentials. For details, see Adding SQL Server Users.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.

2. In the left pane, expand the ***Add-on Modules*** node, and then click ***Event Log***.
   The event log settings appear in the right pane.



3. Select the ***Active*** check box.
4. In the ***Server Name*** field, type the DBMS address in the following format:
   <IP Address or Host Name>\<Process Name>
5. Configure authorization:

To use Windows authorization,	from the ***Authorization Mode*** list, select *Windows NT Authorization*.
To use DBMS authorization,	perform the following actions: 1. From the ***Authorization Mode*** list, select *SQL Server Authorization*. 2. In the ***Login*** field, type the user login. 3. In the ***Password*** field, type the user password.

6. In the ***Database Name*** field, type the database name.

Important
If SQL Server was installed after SmartPTT, or if it is located on a remote computer, the database will not be available for configuration or use. Additionally, the database will be inaccessible if the user has created an account for database authorization instead of using Windows authentication.

7. *(Optional)* Click ***Test*** to check the connection with SQL Server and access to the database.
   A message appears if the connection was successful or not.

8. Click ***Create*** to create a database with the specified parameters.
   A message appears if the connection was successful or not.
9. Click ***Update*** to update a database that was used in the previous versions of SmartPTT.
10. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Configure database retention policy. For details, see Configuring Event Log Database Retention Policy.
- Configure database automatic backup. For details, see Configuring Event Log Automatic Backup.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

4.7.1.2 Configuring Event Log Database Retention Policy

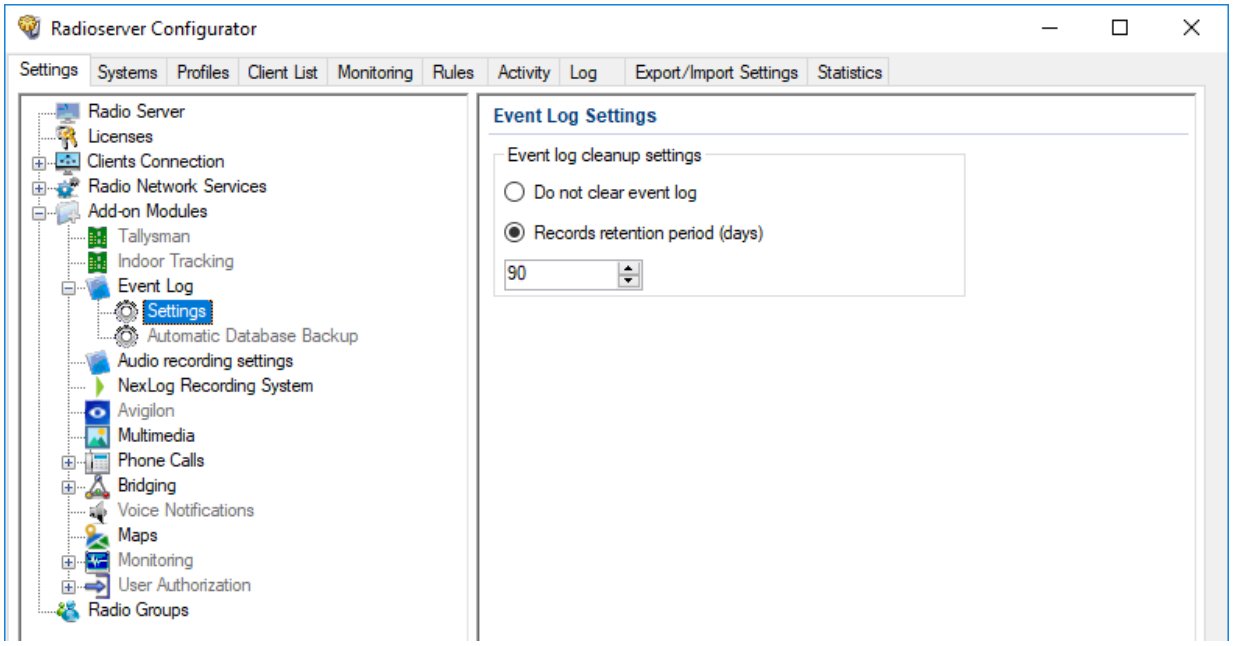
Follow the procedure to configure automatic cleanup of the event log. This helps to avoid database overflow and save the disk space.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *Database Administrators* group. For details, see Loging in to Radioserver Configurator.
- Configure the event log database connection. For details, see Configuring Event Log Database Connection.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Add-on Modules → Event Log***, and then click ***Settings***.
   The event retention settings appear in the right pane.



3. In the right pane, perform one of the following actions:

To prevent log entries deletion from the database,	click ***Do not clear event log***.

To delete outdated event entries,	perform the following actions: 1. Click ***Records retention period (days)***. 2. In the unlocked field, enter the retention period duration (in days).

4. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

4.7.1.3 Configuring Event Log Database Autobackup

Follow the procedure to configure the event log database automatic backup.

Important
If SQL Server was installed after SmartPTT, or if it is located on a remote computer, the database will not be available for configuration or use. Additionally, the database will be inaccessible if the user has created an account for database authorization instead of using Windows authentication.

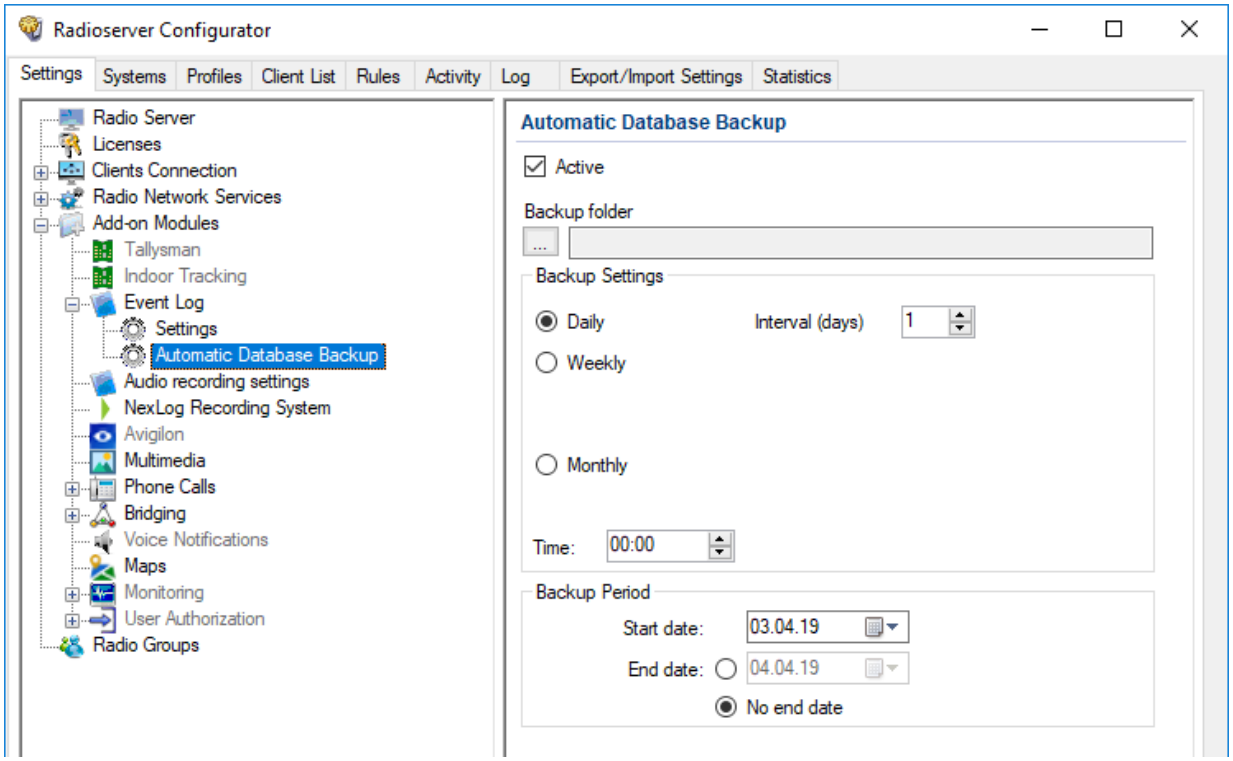
Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *Database Administrators* group. For details, see Loging in to Radioserver Configurator.
- Configure the event log database connection. For details, see Configuring Event Log Database Connection.
- Determine the backup storage.
- Make a schedule for backups.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.

2. In the left pane, expand ***Add-on Modules → Event Log***, and then click ***Automatic Database Backup***.
   The database backup settings appear in the right pane.



3. Select the ***Active*** check box.
4. Determine the backup storage directory:
   a. Click the Browse (...) button to the left of the ***Backup folder*** field.
      The browse window appears.
   b. In the window that appears, specify the directory, and then click ***OK***.
5. In the ***Backup Settings*** area, configure the backup period:

To create backups once in several days,	perform the following actions: 1. Click ***Daily***. 2. In the ***Interval (days)*** field, enter the number of days between backups (*1* means daily backups).
To create backups on the specific days of week with the specific time period,	perform the following actions: 1. Click ***Weekly***. 2. Using check boxes to the right, select week days when the backup must be created. 3. In the ***Interval (weeks)*** field, enter the number of weeks between backups (*1* means weekly backups).
To create backups once in several months,	perform the following actions: 1. Click ***Monthly***.

	2. In the ***Day of month*** field, enter the day of the month when the database backup starts. 3. In the ***Interval (month)*** field, enter the number of months between backups (*1* means monthly backups).

6. In the ***Time*** field, enter the time when the database backup creation starts.
7. *(Optional)* In the ***Backup Period*** area, configure start and end dates of the time interval when the backups must be created:
   a. In the ***Start date*** field, enter the start date of the backup creation.
   b. Configure the date when the backup creation will be stopped:

To create backups at a specified interval as long as the SmartPTT Radioserver is running,	click ***No end date***.
To stop creating backups after the specified end date,	perform the following actions: 1. Click ***End date***. 2. In the unlocked field, enter the end date.

8. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (*** ***)***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (*** ***)*** or ***Restart (*** ***)***.

4.7.2 Voice Recording

SmartPTT supports recording voice transmissions between radios and dispatchers. The following components can perform voice logging:

- SmartPTT radioserver. For details, see Radioserver Voice Logging.
- Each SmartPTT Dispatcher.
  For information on voice recording in dispatch consoles, see “Call Records” in *SmartPTT Dispatcher Guide*.

In addition to SmartPTT, the following products are also able to record voice calls:

- NexLog Recording Systems that receive voice streams from the radioserver in real time. For details, see NexLog Voice Logging.
- RG-1000e/RG-2000 radio gateways that provide 2-wire interface for analog voice loggers. For details, see “Recorder” in *RG-1000e Installation and Configuration Guide* or *RG-2000 Installation and Configuration Guide*.

Also, SmartPTT API provides users with the ability to create their own voice loggers.

4.7.2.1 Radioserver Voice Logging

SmartPTT provides the ability to record incoming and outgoing calls made in the radio system. The records are saved as audio files in local or remote file storage.

Recorded Call Types

SmartPTT radioserver records the following call types:

- Group calls.
- Private calls.
- All Calls.

It also logs the following voice-equivalent transmissions:

- Voice notifications.
- Audio files (configured using rules and deferred actions).

Radioserver does ***not*** record the following call types:

- Voice calls initiated by phone subscribers or addressed to phone subscribers (including private and group calls).
- Voice calls between dispatchers (Console Intercom).

Also, radioserver does ***not*** include service tones in audio files (grant tone, override tone, etc.).

Call Recording Conditions

To record voice calls, one of the following conditions must be fulfilled:

- Call initiator and/or recipient is included in the allowed radio ID list on the radioserver.
- Call initiator and/or recipient is a dispatcher or radioserver.

SmartPTT does ***not*** require configuring talkgroups and All Calls to record group calls.

Records Storage

SmartPTT records calls into audio files in the predefined local/network directory.
This recording mode can be used simultaneously with sending voice streams to the NexLog digital recorder in real time. For details, see NexLog Voice Logging.

Important
Radioserver record storage must be different from the dispatch console record storage due to the different retention periods.

Audio files content complies with the following requirements:

Call Type	*Audio File Content*
Group call	One or several voice transmissions to the same talkgroup with or without a hangtime between them. Voice recording continues until the hangtime expires and the channel/slot is free.
Private call	One or several voice transmissions between radios.

Call Type	Audio File Content
	One or serveral voice transmissions between a radio and a uniquely identified dispatcher.
	One or several voice transmissions between radio and dispatchers that do not have their own IDs (if a call is initiated to the radioserver ID).
All Call	Single voice transmission from the initiator.

4.7.2.1.1 Configuring Centralized Voice Logging

Follow the procedure to configure centralized (radioserver-controlled) call recording.

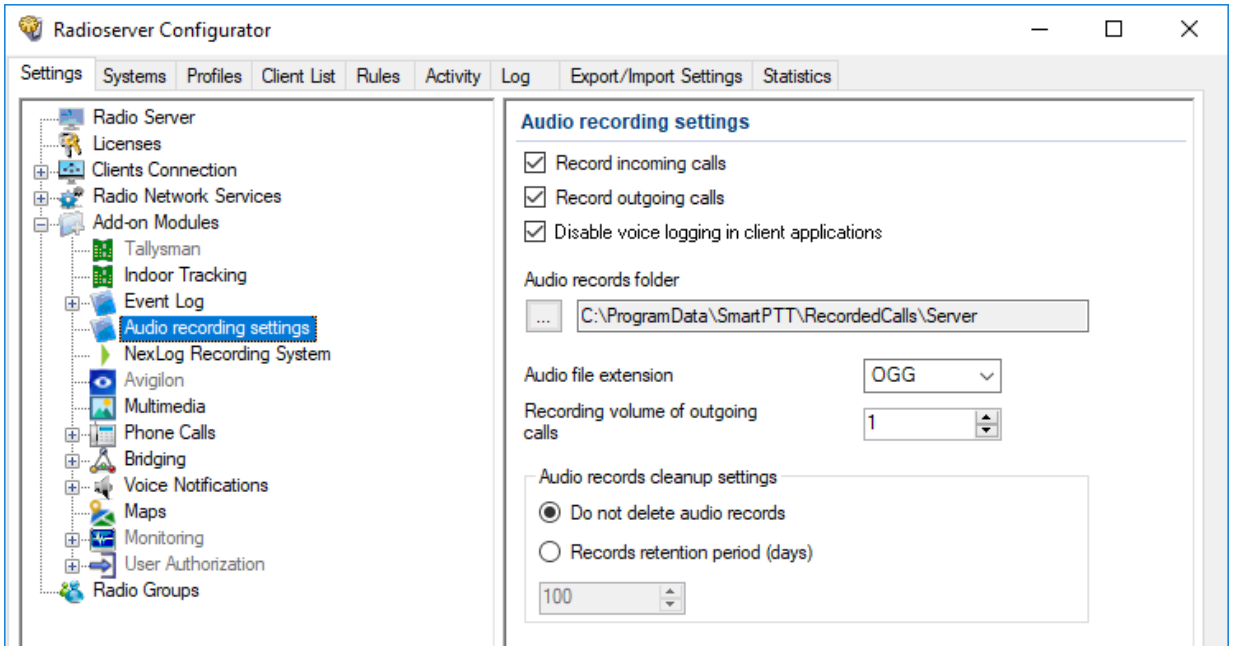
NOTE
SmartPTT records all voice transmissions received from the radio network, regardless of configured talkgroups and profile restrictions.

Prerequisites:

- Prepare call recording directory.
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure that the SmartPTT license allows voice call recording. For details, see Viewing License Items.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand the ***Add-on Modules*** node, and then click ***Audio recording settings***.
   The audio recording settings appear in the right pane.



3. Configure the recorded call types:

To record voice calls from radio networks,	select the ***Record incoming calls*** check box.

To record voice calls from dispatchers,	select the ***Record outgoing calls*** check box.
To record and store voice calls only on radioserver,	select the ***Record calls on radioserver only*** box.

4. Specify the directory where radioserver records will be stored:
   a. Click the Browse ( ) button to the left of the ***Audio records folder*** field.
   b. In the window that appears, select the desired directory, and then click ***OK***.
   The specified path is displayed in the ***Audio records folder*** field.
5. From the ***Audio file extension*** list, select the desired audio format:

To save records in the MP3 format,	select *MP3*.
To save records in the OGG format,	select *OGG*.
To save records in the WAV (uncompressed) format,	select *WAV*.

6. In the ***Recording volume of outgoing calls*** field, enter the desired volume gain index for outgoing calls (initiated by dispatchers). To not change the recording volume, enter *1*.
7. In the ***Audio records cleanup settings*** area, configure audio records retention policy:

To prevent audio files from deletion by the radioserver,	click ***Do not delete audio records***.
To delete outdated audio files,	perform the following actions: 1. Click ***Records retention period (days)***. 2. In the unlocked filed, enter the retention period (in days).

8. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

4.7.2.2 NexLog Voice Logging

SmartPTT provides compatibility with the NexLog recorders from Eventide and can be configured to upload audio records of incoming and outgoing calls to the NexLog server.

The NexLog Recording System feature provides the ability to record and upload audio/voice to NexLog recorders. The Eventide's MediaWorks software helps to manage NexLog recordings by providing features such as a graphical timeline, adding text notes to the voice recordings, copying incident-related calls to a separate tab with the possibility of further export, etc. For details, visit the NexLog Recording Systems webpage.

NOTE
Voice logging using the NexLog recorder does not require radioserver-controlled call recording configuration. Both recording modes can be used simultaneously.

SmartPTT Radioserver routes the following radio network call types and voice-equivalent transmissions to the NexLog recorder:

- Private calls
- Group calls
- All Calls
- Phone calls
- Calls made using bridging or cross patches
- Voice notifications

SmartPTT can also provide the NexLog recorder with additional information such as call initiator IDs and radio location data.

SmartPTT integration with NexLog requires the following:

- NexLog server configuration. For details, see “NexLog Configuration” below.
- SmartPTT configuration. For details, see Configuring NexLog Connection.

NexLog Configuration

To configure NexLog to operate with SmartPTT, on the NexLog server, the following actions must be performed:

- Channels for SmartPTT Radioserver data transmission must be configured and the desired RTP ports must be assigned to them.
- Codec for processing the call recordings audio must be configured.

If you need assistance in NexLog configuration, contact Eventide representatives in your region.

4.7.2.2.1 Configuring NexLog Connection

Follow the procedure to configure SmartPTT connection to the NexLog recorder.

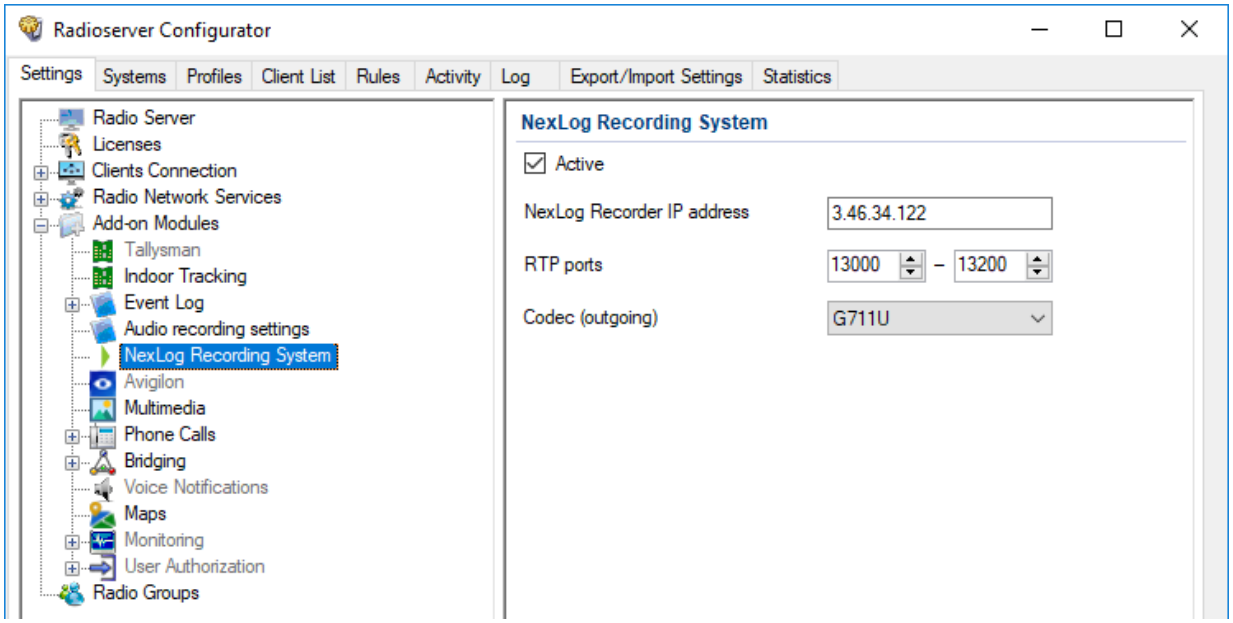
Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure that the SmartPTT license allows NexLog connection. For details, see Viewing License Items.
- From the NexLog recorder settings, obtain the following information:
  - Recorder IP address.
  - Range of RTP/UDP ports allocated for SmartPTT.
  - Vocoder type.
- If the NexLog recorder and radioserver are in different networks controlled by different routers over the router that supports Network Address Translation (NAT), obtain the IP address and UDP port range that will be translated to the recorder IP address and RTP/UDP port range.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.

2. In the left pane, expand ***Add-on Modules***, and then click ***NexLog Recording System***.
   The recorder connection settings appear in the right pane.



3. Select the ***Active*** check box.
4. In the ***NexLog Recorder IP address*** field, type the IP address or domain name of the NexLog recorder (accounting for the potential NAT use).
5. In the ***RTP ports*** fields, enter the lower and upper boundaries of the RTP/UDP port range allocated in the NexLog recorder to receive SmartPTT data (accounting for the potential NAT use).

Important
The number of ports is determined by the number of simultaneously recorded audio streams.

6. From the ***Codec (outgoing)*** list, select the desired option:

If the NexLog recorder uses the A-law algorithm,	select *G711A*.
If the NexLog recorder uses the μ-law algorithm,	select *G711U*.

7. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (*** ***)***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (*** ***)*** or ***Restart (*** ***)***.
- In the firewall software on the computer, unlock the configured UDP ports. For details, see Radioserver Host.

4.7.3 Monitoring Database

SmartPTT network monitoring database stores the following events information:

- Relative radio signal strength (RSSI).
- Radio network equipment status.
- Alarms information.

Important
Monitoring database is available only if the SmartPTT license allows network monitoring. For details, see Viewing License Items.

Monitoring database must be connected and configured to provide the following SmartPTT features:

- MOTOTRBO radio systems and control stations monitoring. For details, see MOTOTRBO Radio Systems.
- Third-party SNMP services integration. For details, see External SNMP Services.
- Automatic alarm notifications that can be addressed to radio network, phone numbers (SMS), email addresses, or external SNMP services. For details, see Configuring Alarm Notifications.
- RF coverage map calculation. For details, see “Configuring Coverage Map” in *SmartPTT Dispatcher Guide*.
- Radio channels monitoring. For details, see “Configuring Air Monitoring” in *SmartPTT Dispatcher Guide*.
- Generating monitoring reports. For details, see “Monitoring Reports” in *SmartPTT Dispatcher Guide*.

Monitoring Database Configuration

To configure the event log database, perform the following actions:

- Install SmartPTT license with network monitoring permission. For details, see Installing License.
- Configure the database management system. For details, see DBMS Configuration.
- Connect SmartPTT Radioserver to the database. For details, see Configuring Monitoring Database Connection.
- Configure the database retention policy. For details, see Configuring Monitoring Database Retention Policy.
- Configure the database automatic backup. For details, see Configuring Monitoring Database Autobackup.

NOTE
When using local or domain authentication, database configuration is available only to users in the *Database Administrators* group.

4.7.3.1 Configuring Monitoring Database Connection

Follow the procedure to configure the monitoring database connection.

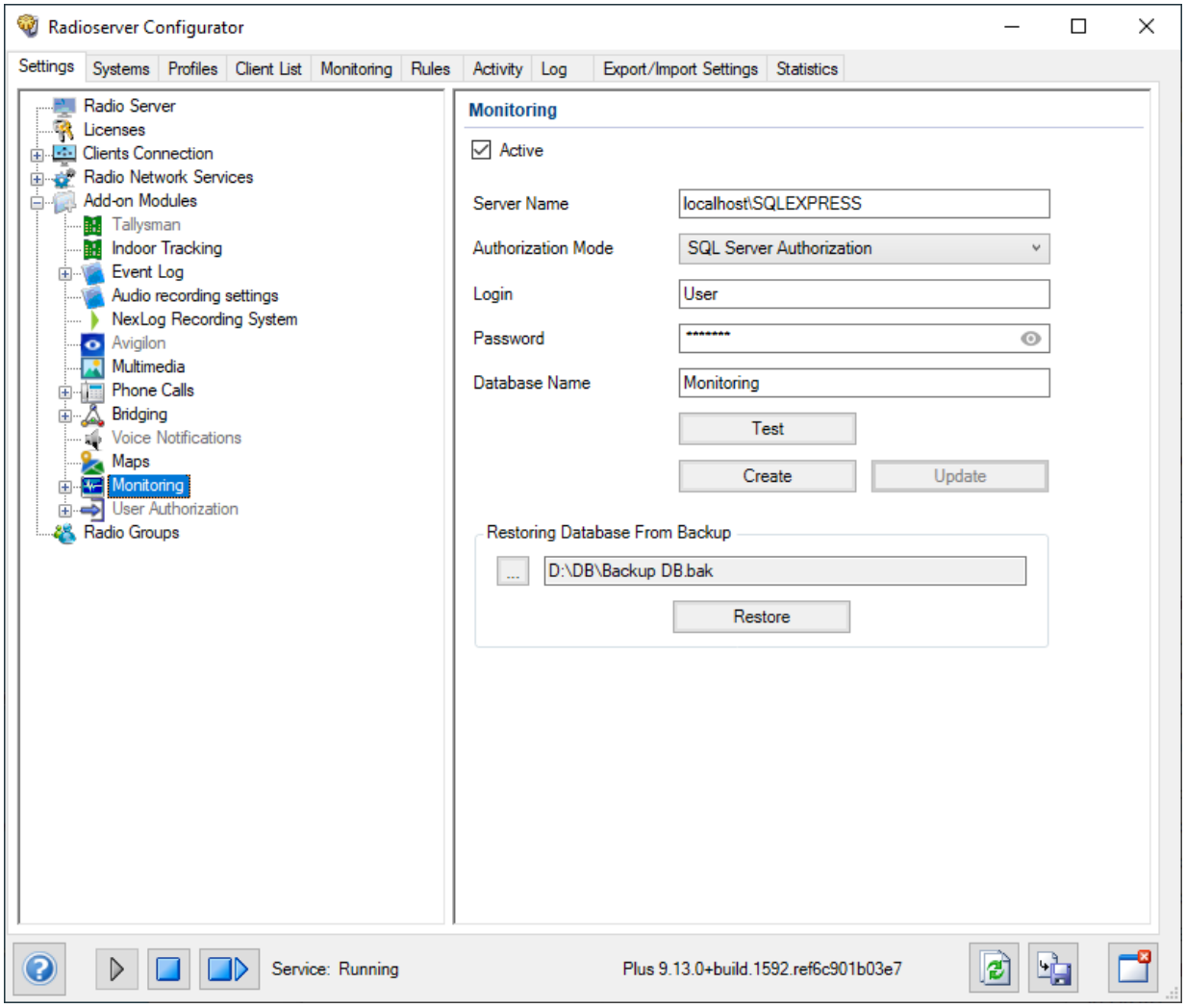
Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *Database Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure that the SmartPTT license allows network monitoring. For details, see Viewing License Items.
- Obtain IP address/domain name of the DBMS host.
- Obtain DBMS process name.
- If DBMS authorization is used, obtain the corresponding credentials. For details, see Adding SQL Server Users.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.

2. In the left pane, expand the ***Add-on Modules*** node, and then click ***Monitoring***.
   The monitoring settings appear in the right pane.



3. Select the ***Active*** check box.
4. In the ***Server Name*** field, type the DBMS address in the following format:
   <IP Address or Host Name>\<Process Name>
5. Configure authorization:

To use Windows authorization,	from the ***Authorization Mode*** list, select *Windows NT Authorization*.
To use DBMS-controlled authorization,	perform the following actions: 1. From the ***Authorization Mode*** list, select *SQL Server Authorization*. 2. In the ***Login*** field, type the user login. 3. In the ***Password*** field, type the user password. To view the entered password, click the eye icon ( ).

6. In the ***Database Name*** field, type the database name.

Important
If SQL Server was installed after SmartPTT, or if it is located on a remote computer, the database will not be available for configuration or use. Additionally, the database will be inaccessible if the user has created an account for database authorization instead of using Windows authentication.

7. *(Optional)* Click ***Test*** to check the connection with SQL Server and access to the database.
   A message appears if the connection was successful or not.
8. Click ***Create*** to create a database with the specified parameters.
   A message appears if the connection was successful or not.
9. Click ***Update*** to update a database that was used in the previous versions of SmartPTT.
10. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (*** ***)***.

Postrequisites:

- Configure the database retention policy. For details, see Configuring Monitoring Database Retention Policy.
- Configure the database automatic backup. For details, see Configuring Monitoring Database Autobackup.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (*** ***)*** or ***Restart (*** ***)***.

4.7.3.2 Configuring Monitoring Database Retention Policy

Follow the procedure to configure automatic cleanup of the monitoring database. This helps to avoid database overflow and save the disk space.

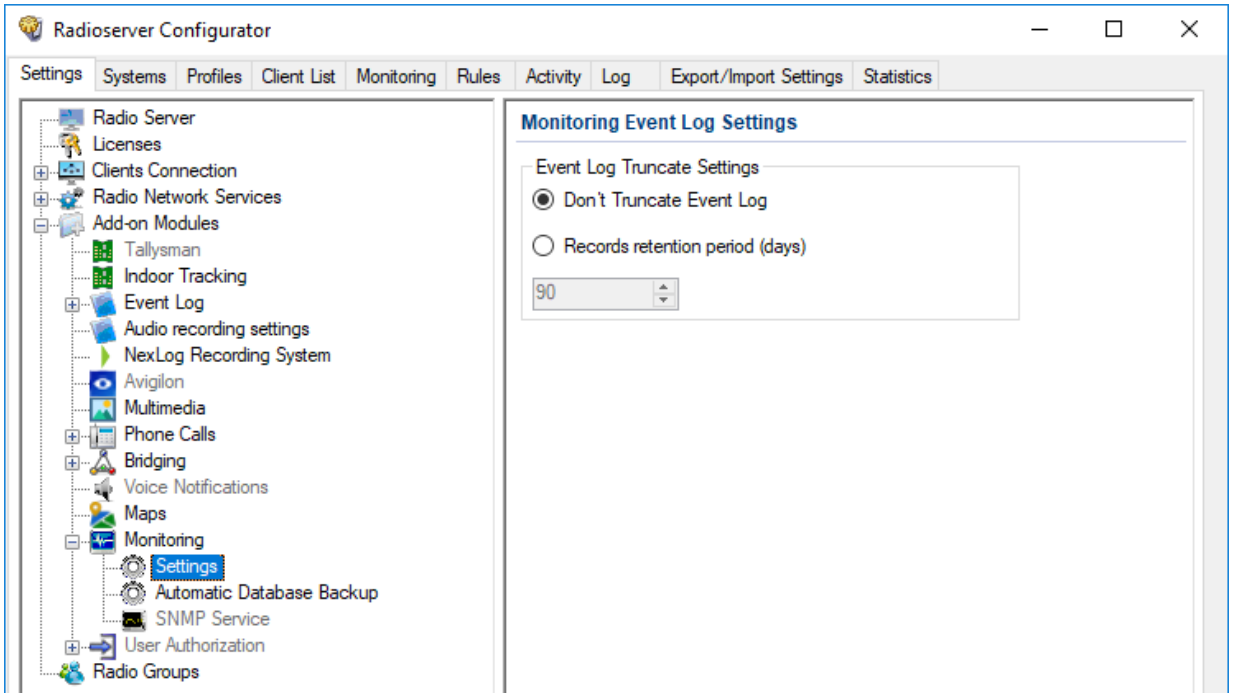
Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *Database Administrators* group. For details, see Loging in to Radioserver Configurator.
- Configure the monitoring database connection. For details, see Configuring Monitoring Database Connection.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.

2. In the left pane, expand ***Add-on Modules → Monitoring***, and then click ***Settings***.
   The monitoring database cleanup settings appear in the right pane.



3. In the right pane, perform one of the following actions:

To prevent log entries deletion from the database,	click ***Don't Truncate Event Log***.
To delete outdated event entries,	perform the following actions: 1. Click ***Records retention period (days)***. 2. In the unlocked field, enter the retention period duration (in days).

4. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

4.7.3.3 Configuring Monitoring Database Autobackup

Follow the procedure to configure the monitoring database automatic backup.

Important
If SQL Server was installed after SmartPTT, or if it is located on a remote computer, the database will not be available for configuration or use. Additionally, the database will be inaccessible if the user has created an account for database authorization instead of using Windows authentication.

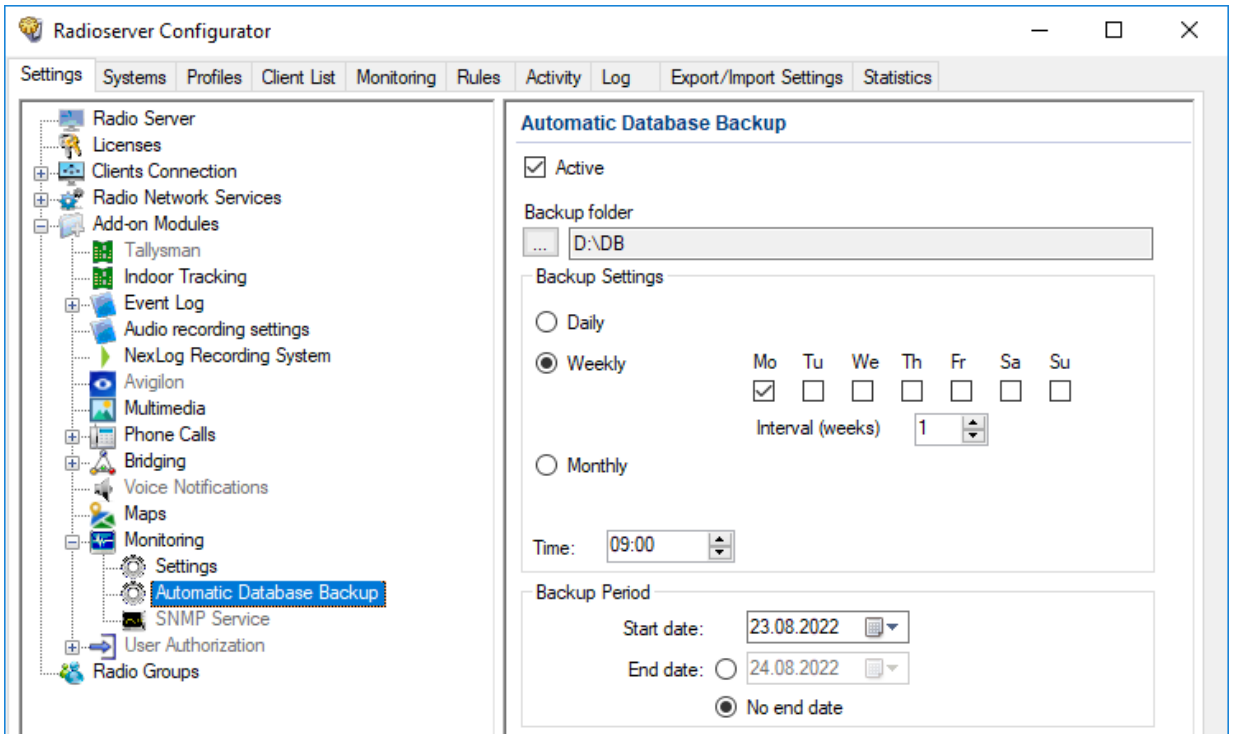
Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *Database Administrators* group. For details, see Loging in to Radioserver Configurator.
- Configure the monitoring database connection. For details, see Configuring Monitoring Database Connection.

- Determine the backup storage.
- Make a schedule for backups.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Add-on Modules → Monitoring***, and then click ***Automatic Database Backup***.
   The backup settings appear in the right pane.



3. Select the ***Active*** check box.
4. Determine the backup storage directory:
   a. Click the Browse (...) button to the left of the ***Backup folder*** field.
      Browse dialog box appears.
   b. In the dialog box, specify the directory, and then click ***OK***.
5. In the ***Backup Settings*** area, configure the backup period:

To create backups once in several days,	perform the following actions: 1. Click ***Daily***. 2. In the ***Interval (days)*** field, enter the number of days between backups (*1* means daily backups).
To create backups on specific days of week with the specific time period,	perform the following actions: 1. Click ***Weekly***. 2. Using check boxes to the right, select week days when the backup must be created.

	3. In the ***Interval (weeks)*** field, enter the number of weeks between backups (*1* means weekly backups).
To create backups once in several months,	perform the following actions: 1. Click ***Monthly***. 2. In the ***Day of month*** field, enter the day of month when the database backup starts. 3. In the ***Interval (month)*** field, enter the number of months between backups (*1* means monthly backups).

6. In the ***Time*** field, enter the time of the day when the database backup creation starts.
7. *(Optional)* In the ***Backup Period*** area, configure start and end dates of the time interval when the backups must be created:
   a. In the ***Start date*** field, enter the start date of the backup creation.
   b. Configure the date when the backup creation will be stopped:

To create backups at a specified interval as long as the SmartPTT Radioserver is running,	click ***No end date***.
To stop creating backups after the specified end date,	perform the following actions: 1. Click ***End date***. 2. In the unlocked field, enter the end date.

8. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

4.7.4 Event Viewer

Radioserver saves system events into the operating system event log. For example, it adds the following types of events into the log:

- Dispatch console connection to the radioserver.
- Radioserver service stop.

Events are available to view using the Windows Event Viewer. Radioserver log in that app is named ***SmartPTT***. It is available alongside other applications and services logs.

For information on Event Viewer and the log, see the Event Viewer page on the Microsoft Docs website.

4.8 Radio Blocklist

For security reasons, SmartPTT provides the ability to create and manage a blocklist or allowlist of radios (formerly called blacklist/whitelist). When the allowlist is activated, all radios ***not*** in the list are blocked. When the blocklist is activated, all radios in the list are blocked. The radio is blocked automatically after radio registration in the network. For details, see Configuring Radio Blocklist.

Important
The radioserver does not send commands to unblock the radios.

The specific block radio command is determined by the ***Block option*** parameter of the SmartPTT Radioserver settings. For details, see Configuring Radioserver.

4.8.1 Configuring Radio Blocklist

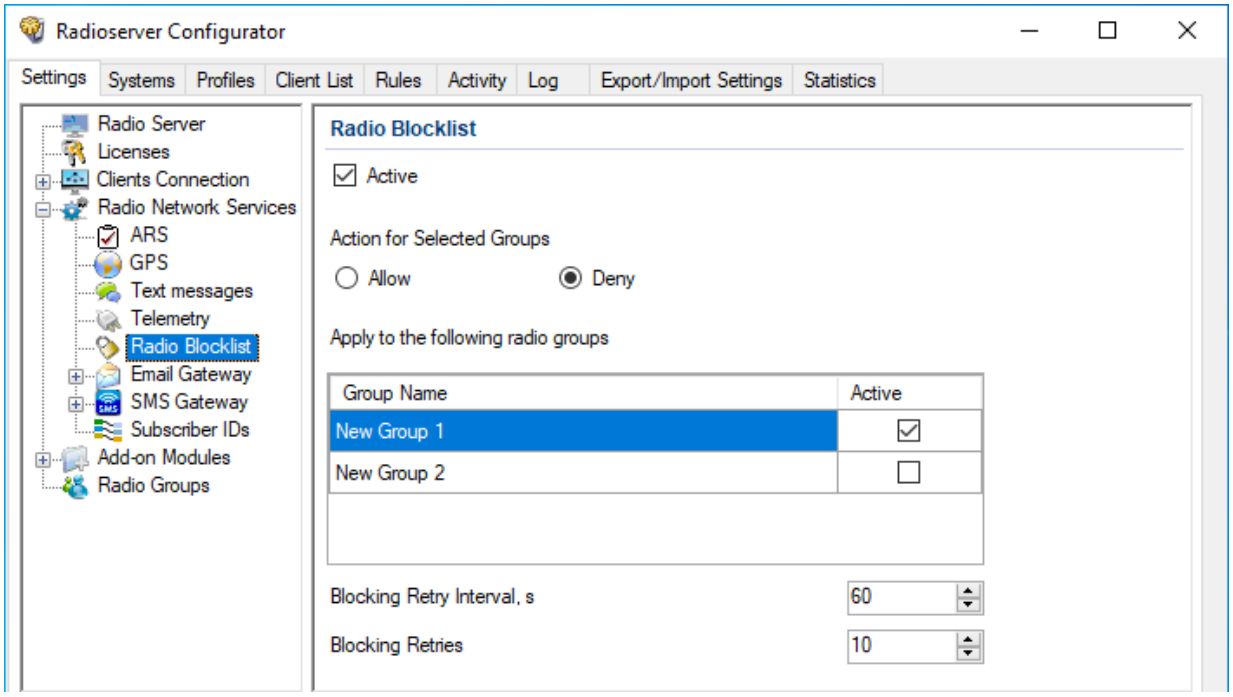
Follow the procedure to configure a blocklist or allowlist of radios.

Prerequisites:

- Configure *Radio Disable* reception in radio codeplugs.
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- In the ***Radio Groups*** node of Radioserver Configurator, create the desired radio groups. For details, see Managing Radio Groups.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Radio Network Services***, and then click ***Radio Blocklist***.
   The radio blocklist settings appear in the right pane.



3. Select the ***Active*** check box.

4. In the ***Action for Selected Groups*** area, select one of the following actions:

To deny access to the radio network for all radios except included in the selected groups,	select the ***Allow*** option.
To deny access to the radio network for all radios included in the selected groups,	select the ***Deny*** option.

5. In the table, in the ***Active*** column, select the check box for groups that must be included in blocklist/allowlist.
6. In the ***Blocking Retry Interval s*** field, enter the minimum interval (in seconds) between attempts to block the same radio.
7. In the ***Blocking Retries*** field, enter the maximum quantity of attempts to block the same radio.
8. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

4.9 Activating Text Message Sending and Receiving

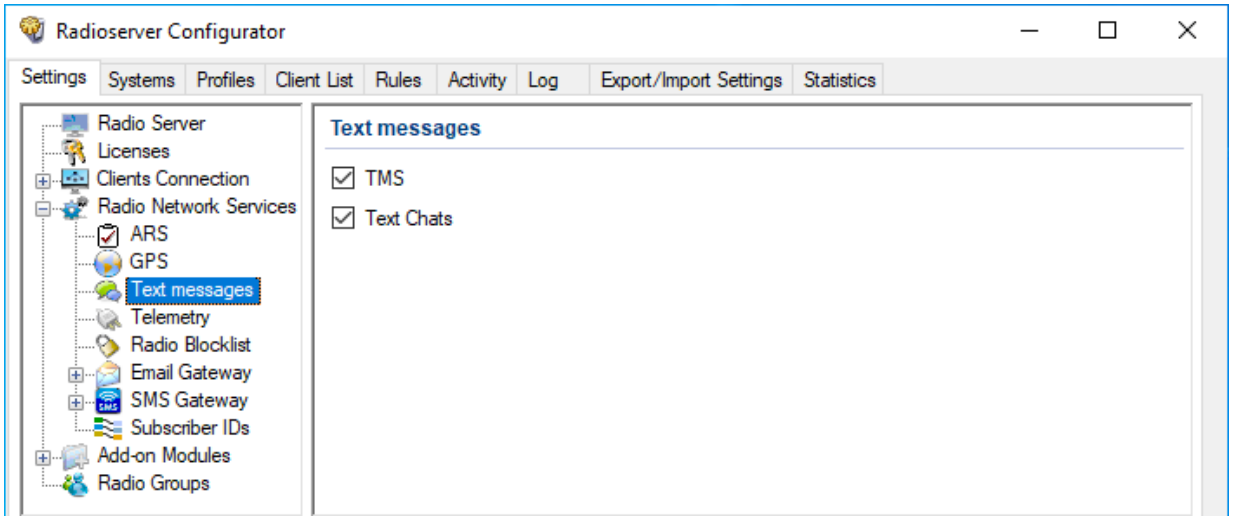
Follow the procedure to activate the receiving and sending of text messages (TMS) and text chats.

Prerequisites:

When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Radio Network Services***, and then click ***Text messages***.
   The text message and text chat settings appear in the right pane.



3. In the right pane, perform one of the following actions:

To enable exchanging text messages (TMS) between radios and dispatchers,	select the ***TMS*** check box.

To enable exchanging text messages between mobile clients in the SmartPTT Mobile application,	select the ***Text Chats*** check box.

4. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

4.10 Activating Telemetry

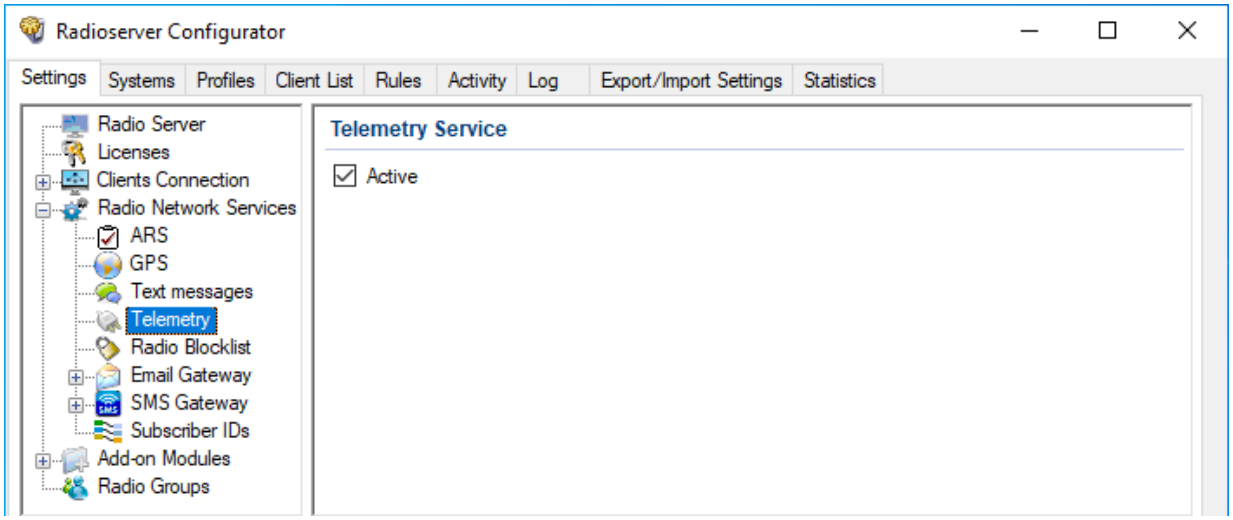
Follow the procedure to activate the telemetry service.

Prerequisites:

When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Radio Network Services***, and then click ***Telemetry***.
   The telemetry settings appear in the right pane.



3. Select the ***Active*** check box.
4. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- Configure radio GPIO pins to process incoming and outgoing signals for desired electronic devices.

4.11 Rules

Rules are the automatic SmartPTT reaction on events occurred in the radio system. For example, SmartPTT may react on the following events:

- Emergency alarm or call.
- Text message with a specific content.
- Dispatch console (desktop client) disconnection from radioserver.

For information on the full list of events, see Rule Conditions.

When event is detected, radioserver is able to perform one or several actions:

- Send an audio file to the radio network.
- Send a group or a private text message.
- Send a voice notification. For details, see Voice Notifications.

Radioserver actions may trigger other rules.

NOTE
SmartPTT Dispatcher provides additional rules to its users. For details, see “Rules and Lone Worker Mode” in *SmartPTT Dispatcher Guide*.

4.11.1 Rule Conditions

Rule conditions are set of logical expressions that consist of the following elements:

- Attribute (for example, “Event Type”).
- Operator (for example, “Equal to”).
- Value (for example, “Call”).

Each rule may have several expressions. For example, in may consist of the “Incoming Call” and “Incoming Message” expressions. To trigger a rule, all attributes must match the event.

SmartPTT does ***not*** prevent users from invalid conditions configuration. For example, it does ***not*** prevent users from configuring the “Outgoing ARS” condition.

4.11.1.1 Condition Attributes

Condition attributes are as follows:

Attribute	***Description***
Direction	Shows if dispatch subsystem receives (incoming event) or transmits (outgoing event) to the radio network.
Event Type	One or multiple event types. For details, see Event Types below.
Date	Calendar date or date range when an event must occur.

Attribute	Description
Additional Information	Miscellaneous information that is related to the transmission (for example, text message fragment or target ID).
Control Station	Name of the control station, IP Site Connect slot, or trunked system.
Talkgroup	Name of the talkgroup that receives voice call or text message.
Radio	ID of a radio that receives or initiates a transmission.
User	Radio user name. Applicable to radio systems accessible over NAI and for Capacity Max. For details, see Radio Users.
Status	Result of various transmissions. For details, see Statuses below.
Duration	Voice call duration.
SCADA object	Name of the SCADA point which alarm must trigger a rule.
SCADA Alarm	Name of the SCADA point parameter which alarm must trigger a rule.

Event Types

In the ***Event Type*** list, the following options are available:

- ARS — radio registration/de-registration. For details, see Registration of Radios.
- Call — group or private voice call (including emergency call) or voice notification or the Remote Monitor voice.
- Message — text message and/or job ticket.
- Telemetry — telemetry information and/or remote control command.
- Alarm — incoming emergency alarm.
- Block — Block Radio or Unblock Radio command. For details, see Configuring Radioserver.
- User Authorization — radio user signs in or signs out from the radio.

Statuses

In the ***Status*** list, the following options are available:

- Monitoring — the Remote Monitor command is sent.
- Phone Call — voice call to/from the phone network.
- Radio is available — one of the Radio Check command result.
- Sign In — radio user signs in to the radio (authorizes in it).
- Sign out — radio user signs out from the radio.

Meaning of other attribute values is the same as their names.

4.11.1.2 Condition Operations

For each attribute, the following operations are available:

Attribute	Equal to	Not equal to	Between	Contains
Direction	YES			
Event Type	YES	YES		
Date			YES	
Additional Information	YES			YES
Control Station	YES			YES
Talkgroup	YES			YES
Radio	YES	YES		
User	YES	YES		
Status	YES	YES		
Duration	YES	YES	YES	
SCADA object	YES	YES		
SCADA Alarm	YES	YES		

The following operations are available for the Duration attribute only:

- Greater than
- Greater than or equal to
- Less than
- Less than or equal to

4.11.2 Adding or Modifying Rules for Radios

Follow the procedure to add a new rule for events on radios or modify an existing one.

Prerequisites:

- Create a list of events that must be affected by rules. Include the initiator and target information in the list of events.
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Connect to radio networks:
  - To access the MOTOTRBO radio systems, see MOTOTRBO Radio Systems.

- To access the P25 radio systems, see P25 Radio Systems.

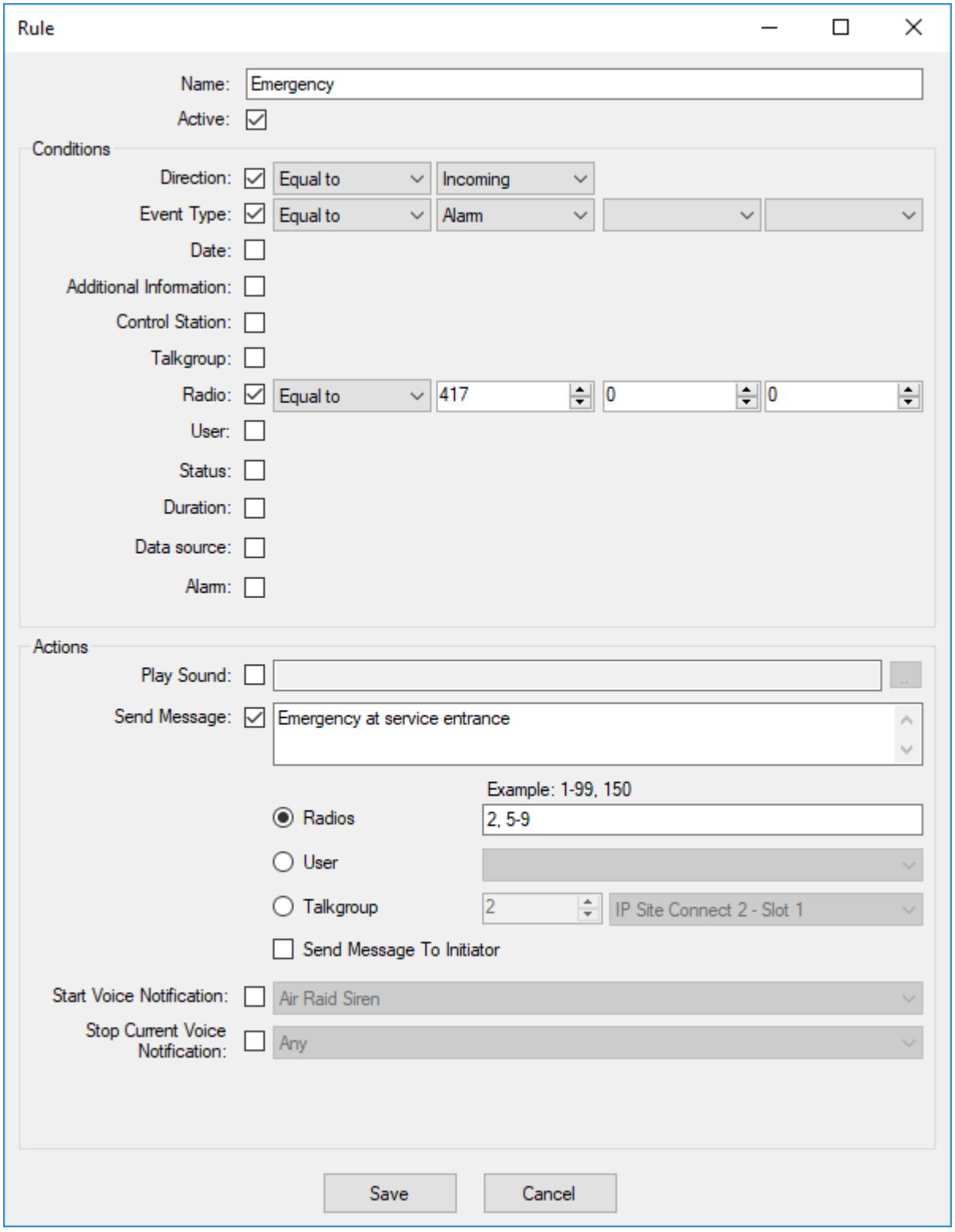
- *(Optional)* Ensure that audio files comply with their requirements. For details, see Audio File Requirements.
- *(Optional)* Create and configure voice notifications. For details, see Managing Voice Notifications.

Procedure:

1. In SmartPTT Radioserver Configurator, select the ***Rules*** tab.
2. On the ***Rules*** tab, select the ***Events on radios*** option.
3. Perform one of the following actions:

To add a new rule,	click ***Add (***  ***)*** at the top of the window.
To modify an existing rule,	select the desired rule in the rule table, and then click ***Modify (***  ***)***.

The ***Rule*** window appears.



4. In the ***Name*** field, type the rule name.
5. *(Optional)* Select the ***Active*** check box to create an active rule.
6. In the ***Conditions*** area, perform the following actions:
   a. Select the check box that is related to the desired condition attribute. For details, see Rule Conditions.
   b. From the list next to the check box, select the desired dispatcher.
   c. In the fields and/or from the lists placed next to the dispatcher, select the desired condition values.

7. Repeat step 6 for all the desired conditions.
8. In the ***Actions*** area, configure the actions that will be taken when the rule is triggered. For details, see Configuring Actions.
9. Click ***Save*** at the bottom of the ***Rule*** window to apply changes and close the window.
   The configured rule appears in the rules table.
10. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

4.11.2.1 Configuring Actions

Follow the procedure to configure the actions that will be taken when the rule is triggered.

Prerequisites:

- Start the rule configuration.
- Ensure that the desired voice notification is created and configured. For details, see Managing Voice Notifications.
- If an audio must be sent to the initiator, create an audio file that complies with the general audio file requirements.For details, see Audio File Requirements

4.11.3 Adding or Modifying Rules for Dispatcher

Follow the procedure to add a new or edit an existing rule that is related to the SmartPTT Dispatcher connection status. The rule is not applicable to other types of clients.

Important
Created rule will be applied to all SmartPTT Dispatcher applications.

Prerequisites:

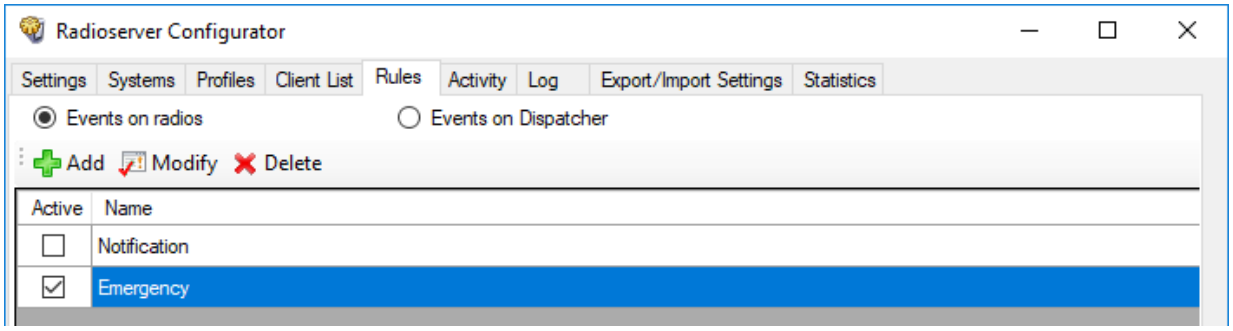
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- *(Optional)* Ensure that audio files comply with their requirements. For details, see Audio File Requirements

4.11.4 Managing Rules

Follow the procedure to activate/deactivate or delete an existing rule.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Rules*** tab.



2. Show the desired rules:

To show rules related to events in the radio network,	click ***Event on radios***.
To show rules related to the dispatch console disconnection and/or connection,	click ***Events on Dispatcher***.

3. Click the desired rule.
4. Perform one of the following actions:

To activate the desired rule,	perform the following actions: 1. Click ***Modify*** ( ) at the top of the window. The ***Rule*** window opens. 2. Select the ***Active*** check box. 3. At the bottom of the window, click ***Save***.
To deactivate the desired rule,	perform the following actions: 1. Click ***Modify*** ( ) at the top of the window. The ***Rule*** window opens. 2. Select the ***Active*** check box. 3. At the bottom of the window, click ***Save***.
To delete a rule,	in the top part of the ***Rules*** tab, click ***Delete*** ( ), and then confirm the deletion.

5. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration*** ( ).

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start*** ( ) or ***Restart*** ( ).

4.12 Voice Notifications

A voice notification is a preconfigured audio file that can be sent to a talkgroup or during All Call as a voice transmission.

Before you can configure and use voice notifications, you must record or obtain notification files in the MP3, OGG, or WAV format. For information on the audio file requirements, see Audio File Requirements.

All desired audio files can be uploaded in SmartPTT Radioserver Configurator, and then assigned to talkgroups and All Calls. Only one talkgroup or All Call can be selected for each control station or a conventional radio system channel.

Important
Custom voice notifications must be played on the user radio equipment before you use them in the radio network. That way, you can ensure that they will be played correctly on the subscribers' end.

Voice notifications can be played in one of the following ways:

- From the ***Voice Notifications*** window in SmartPTT Dispatcher. For details, see “Playing Voice Notifications” in *SmartPTT Dispatcher Guide*.

- Using the Voice Notification element in custom consoles. For details, see “Custom Console Elements” in *SmartPTT Dispatcher Guide*.
- Automatically, when triggered by a rule configured in SmartPTT Radioserver Configurator. For details, see Rules.

Voice notifications are sent to radio networks as voice transmissions. They cannot be sent in radio networks where voice calls are ***not*** licensed or configured. Also, they cannot be sent to other VoIP system like phone systems.

If transmission of notifications has already started, the system continues transmitting voice notifications after the radioserver is stopped.

A voice notification can interrupt an ongoing transmission. The voice notification priority depends on the system settings.

Voice notifications can be configured to ignore an interruption request from radios.

If all channels are busy and the system settings do not allow to interrupt transmissions, the notification will be queued, and the operator will see an indication. If the voice notification was in the queue when the radioserver was stopped or connection failed, the notification will not be sent, the queue will be cleared, and the operator will receive an according indication.

To create a voice notification, SmartPTT Radioserver reads the audio file that is available in the local or network file storage. SmartPTT does not copy audio files to its internal storage. If the audio file is unavailable, or access to it requires authorization, the voice notification transmission will fail.

A redundant radioserver automatically copies voice notification files from the primary radioserver if server synchronization is enabled.

When you use a redundant radioserver, it monitors iteration number of all currently playing voice notifications. If the primary radioserver is disconnected during a voice notification playback, the redundant radioserver will play all remaining iterations of the voice notification, including the one during which the disconnection occurred.

4.12.1 Managing Voice Notifications

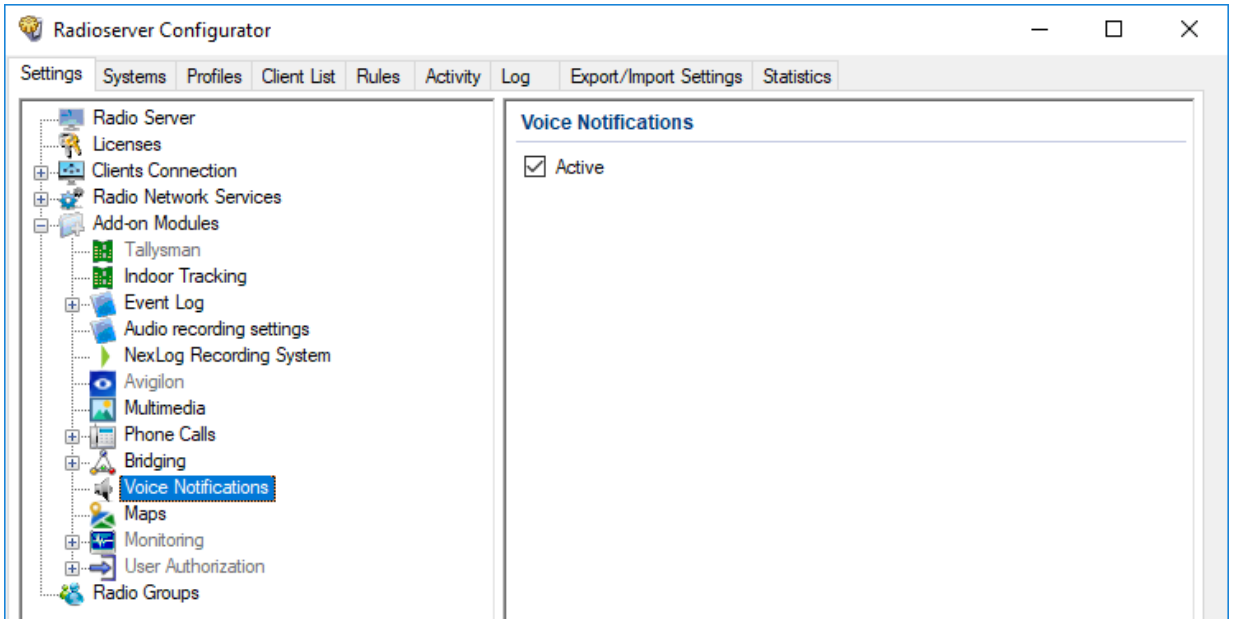
Follow the procedure to add a voice notification and configure its recipients.

Prerequisites:

- Configure talkgroups in the desired radio networks.:
  - To access the MOTOTRBO radio systems, see MOTOTRBO Radio Systems.
  - To access the P25 radio systems, see P25 Radio Systems.
- Create an audio file that complies with SmartPTT requirements. For details, see Audio File Requirements.

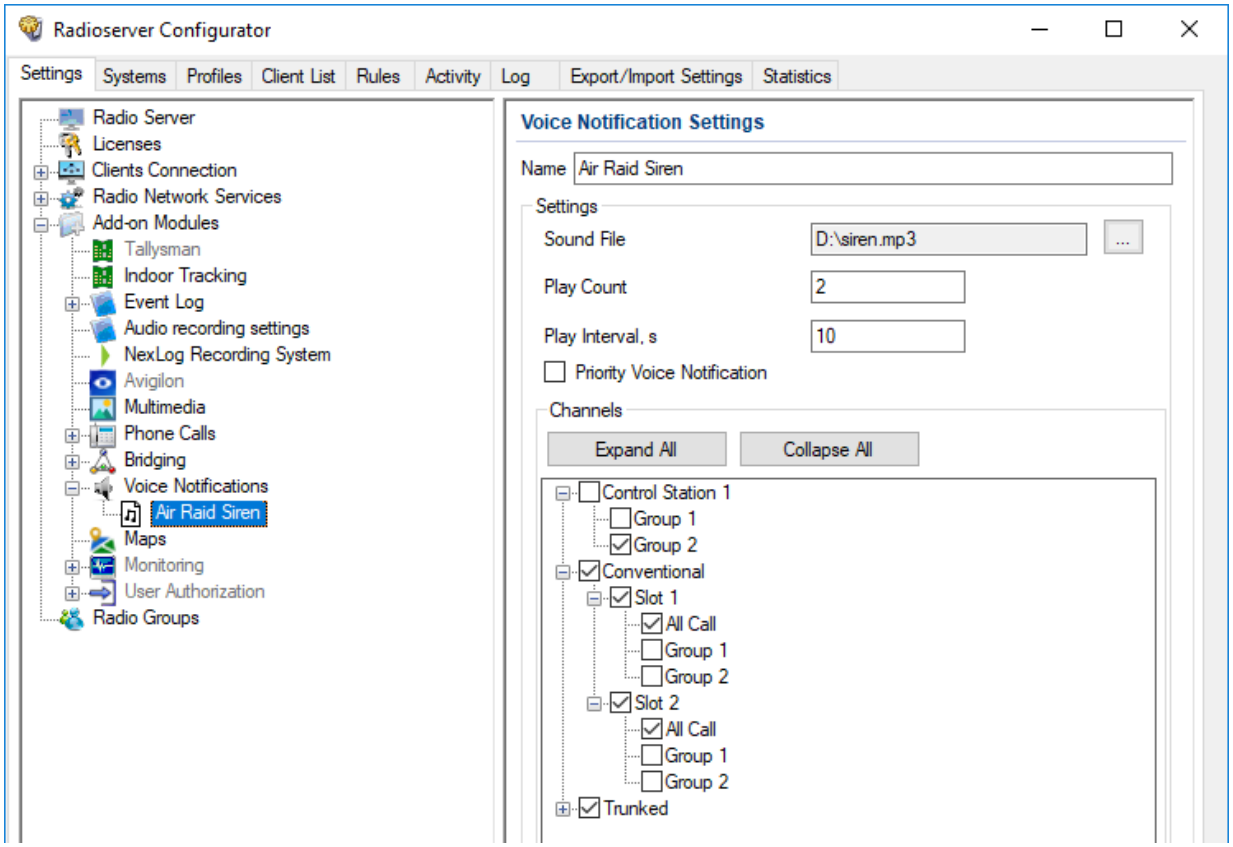
Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Add-on Modules***, and then click ***Voice Notifications***.
   In the right pane, the ***Active*** check box appears.



3. Select the ***Active*** check box.
4. Perform one of the following actions:

To add a new voice notification,	right-click the ***Voice Notifications*** node, and then from the actions menu, select ***Add***.
To modify an existing voice notification,	expand the ***Voice Notifications*** node, and then select the desired voice notification.
To delete an existing voice notification,	perform the following actions: 1. Expand the ***Voice Notifications*** node. 2. Right-click the desired voice notification, and then from the actions menu, select ***Delete***. 3. Proceed to the last step of this procedure.



5. In the right pane, in the ***Name*** field, type the voice notification name.
6. Select the desired audio file:
   a. To the right of the ***Sound File*** field, click the Browse (...) button.
   b. In the window that appears, select the desired file.
7. In the ***Play Count*** field, type the number of times the voice notification will be repeated.
8. In the ***Play Interval, s*** field, type the time interval between repetitions of the voice notification.
9. *(Optional)* To increase the priority of the notification, select the ***Priority Voice Notification*** check box. Notifications with higher priority can interrupt other notifications and calls from clients to radio network.
10. Configure voice notification recipients:
    a. In the ***Channels*** area, click ***Expand All*** to expand all nodes of the radio network object tree. If necessary, click Expand (⊞) or Collapse (⊟) to expand or collapse an individual node.
    b. Select the check boxes next to the desired recipients.

NOTE
Only one recipient (talkgroup or All Call) can be selected for each control station or a conventional radio system.

    c. Clear the check boxes next to the undesired recipients.
11. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

5 Client Applications and Profiles

SmartPTT supports different types of clients, two types of roles, and such functionality as profiles that are assigned to clients. They are required to successfully differentiate user access to the SmartPTT features. Label assignment is also available to clients. This functionality provides the ability to set the rules for mutual visibility of clients.The interaction of client accounts, client labels, user roles and profiles is described in the sections below.

Client Connections

SmartPTT supports the following types of clients:

- SmartPTT Dispatcher applications (also known as “desktop clients”). For details, see Desktop Clients.
- SmartPTT Web Clients. For details, see Web Clients.
- SmartPTT Mobile applications. For details, see SmartPTT Mobile.
- Third-party applications that use Server API. For details, see Third-Party Apps.

Profiles

Profiles are tools for client permissions and restrictions management.
For information on profiles, see Profiles.

For a profile, you can do the following:

- Restrict access to networks and features within these networks. For details, see Available Networks.
- Restrict actions within these networks. For details, see Available Actions.
- Configure call parameters in SmartPTT Mobile application. For details, see Configuring Personalities.

User Roles

The role determines permissions granted to the application user.
For information on user roles in SmartPTT Dispatcher, see “Operators” in *SmartPTT Dispatcher Guide*.

SmartPTT provides two types of roles for its users:

- Administrator. This role has unlimited access rights to all functionality of the system, including the possibility to add new operator accounts.
- Operator. An operator account is limited by functionality that the Administrator determined. The number of operator accounts in SmartPTT Dispatcher is unlimited.

Interaction

If authorization on SmartPTT Radioserver is enabled for desktop clients, then SmartPTT Dispatcher must log in under the client account to connect to SmartPTT Radioserver. In SmartPTT Dispatcher, the administrator specifies the client credentials that will be used when SmartPTT Dispatcher connects to SmartPTT Radioserver.

SmartPTT Mobile, Web Client, and API users also require a client account. Users log in with this account.

Client accounts are configured on the ***Clients*** tab of SmartPTT Radioserver Configurator.

SmartPTT Radioserver functionality available to clients can be limited by profiles. You can configure profiles on the ***Profiles*** tab of SmartPTT Radioserver Configurator and then assign profiles to clients on the ***Clients*** tab.

In SmartPTT Dispatcher, you can also create operator accounts with limited access to SmartPTT Dispatcher functionality. To log in to SmartPTT Dispatcher, an operator needs to type credentials. The list of operator credentials is created by the Administrator in SmartPTT Dispatcher. For details, see “Managing Operator Accounts” in *SmartPTT Dispatcher Guide*.

NOTE
Operators do not need to type or know their client credentials.

Below are the steps that must be performed to configure desktop client authentication:

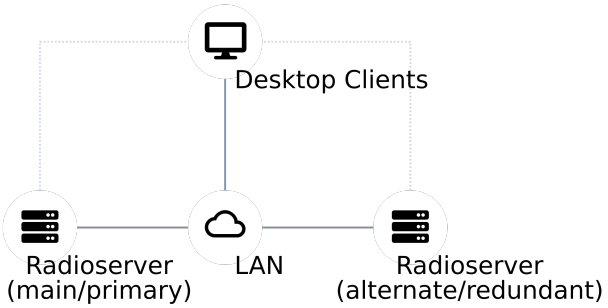
- SmartPTT Radioserver interface must be configured. For details, see Configuring Desktop Clients Connection.
- The configured TCP and UDP ports must be unlocked in the firewall software. For details, see Radioserver Host.
- Profiles must be created. SmartPTT provides the ability to create several profiles for one client account. For details, see Managing Profiles.
- Client accounts must be created and available profiles for specific client accounts must be selected. For details, see Managing Client Account Parameters.
- In SmartPTT Dispatcher, operator accounts must be associated with client accounts. For details, see “Operators” and “Radioservers” in *SmartPTT Dispatcher Guide*.

Client Visibility Limitation

In systems with several different groups of clients on the same radioserver, it may be necessary to isolate some clients from others. SmartPTT provides functionality for adding client labels. This feature provides the ability to see selected clients (with common labels) or not to see them (if there are no common labels). For details, see Client Labels.

5.1 Desktop Clients

In SmartPTT, desktop client means SmartPTT Dispatcher, a primary client application in SmartPTT.



Examples of the SmartPTT Dispatcher capabilities are as follows:

- Voice and data communication in radio networks, phone networks, and with other dispatchers.
- Radio networks integration using bridging, cross patches, and conference calls.
- Tracking radios on maps, creating geofences, and points of interest.
- Network device monitoring tools.
- Reports generation on the radio network events and network devices performance.

For information on the application capabilities, see *SmartPTT Dispatcher Guide*.

Radioserver Configuration

Configuration can be performed in two ways:

- With client authorization on SmartPTT Radioserver.
  For information on desktop client authentication, see Client Applications and Profiles.
- Without client authorization.
  To allow desktop client connection without authorization, only radioserver network ports must be configured and unlocked.
  For details, see Configuring Desktop Clients Connection and Radioserver Host.

5.1.1 Configuring Desktop Clients Connection

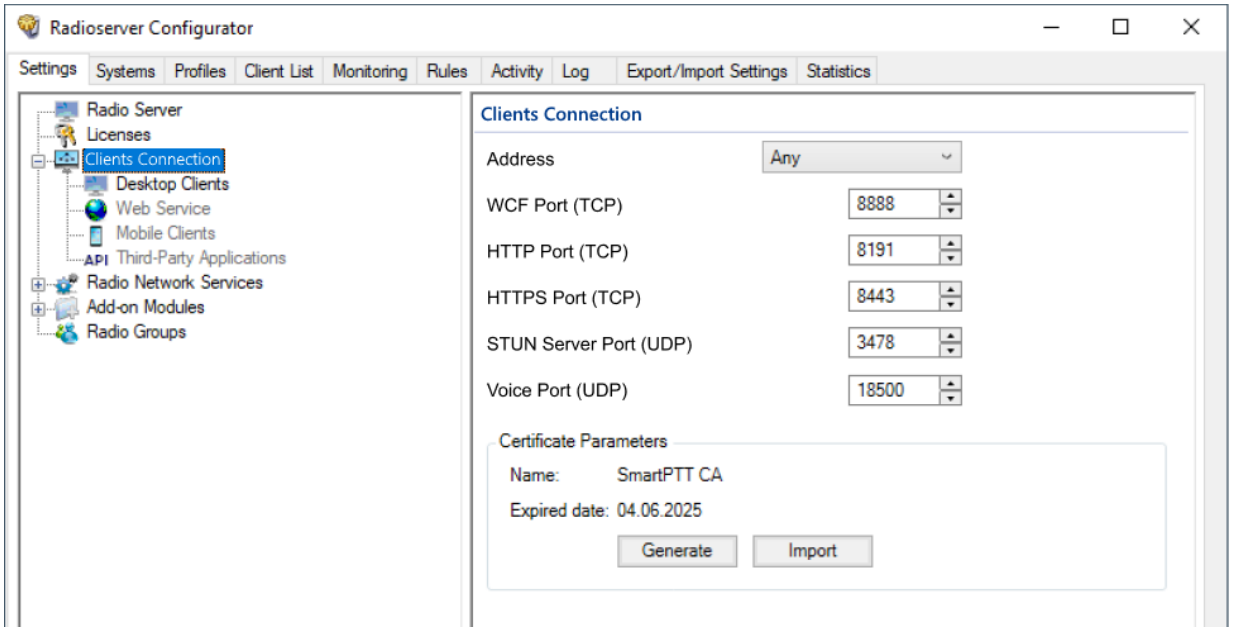
Follow the procedure to configure the ability to connect the SmartPTT Dispatcher applications to SmartPTT Radioserver.

Prerequisites:

- Determine the SmartPTT Radioserver host IP address.
- Determine the WCF port and Voice port numbers for connecting to the application.
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, click ***Clients Connection***.



3. In the right pane, from the ***Address*** list, select the desired option:

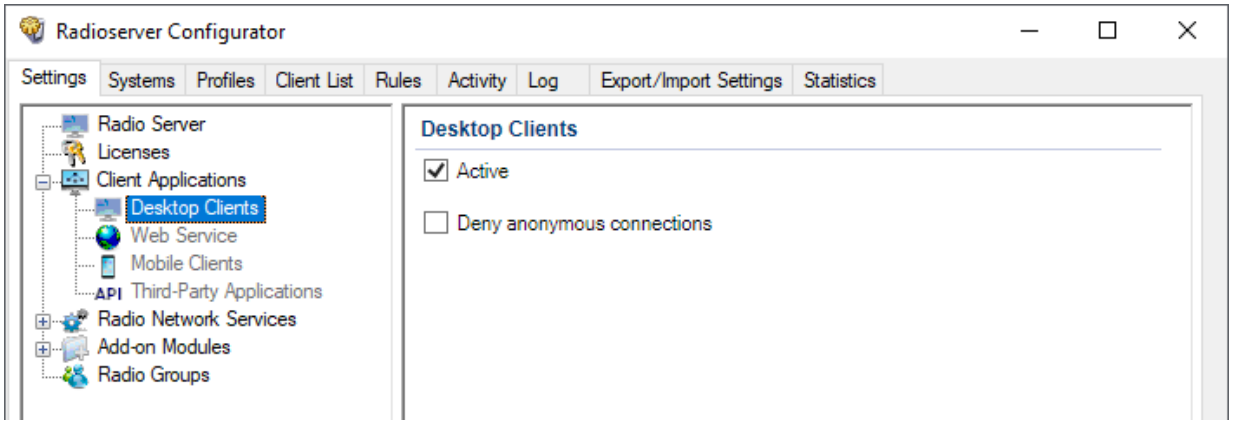
To allow SmartPTT Radioserver to accept connection requests to any address of its own,	select *Any*.

To allow client applications to connect to SmartPTT Radioserver only through a specific address,	select the desired IP address from the list.

4. *(Optional)* In the ***WCF Port (TCP)*** field, you can change the port number for connection with SmartPTT Dispatcher. The default value is *8888*.
5. In the ***Certificate Parameters*** area, configure the certificate that will be used for encrypted connection to SmartPTT Dispatcher:

To use the self-signed certificate SmartPTT,	click ***Generate***.
To import a custom certificate,	perform the following actions: 1. Click ***Import***. 2. In the window that appears, select the certificate file in the PFX or P12 format. 3. In the next window that appears, enter the password to upload the selected certificate.

6. *(Optional)* In the **Voice Port (UDP)** field, you can change the UDP port number that will be used to exchange voice traffic between SmartPTT Radioserver and SmartPTT Dispatcher applications.
7. In the left pane, expand the ***Client Connections*** node.
8. Click the ***Desktop Clients*** node.



9. In the right pane, select the ***Active*** check box.
10. On the tab, perform one of the following actions:

To enable/disable authentication on SmartPTT Radioserver for desktop clients,	select the ***Deny anonymous connections*** check box.

	Important If desktop client authorization on the radioserver is enabled, in SmartPTT Radioserver Configurator, create and configure one or multiple profiles, then create a client account, and assign one or multiple profiles to the client. In SmartPTT Dispatcher, the operator will be able to switch between the profiles that have been assigned to their client account. For details, see Managing Profiles and Managing Client Account Parameters.
To allow desktop clients to connect to SmartPTT Radioserver without authentication,	clear the ***Deny anonymous connections*** check box. ***Important*** If authorization of desktop clients on the radioserver is disabled, in SmartPTT Radioserver Configurator, create and configure one or multiple profiles for anonymous connections. In SmartPTT Dispatcher, any operator will be able to switch between these profiles. For details, see Managing Profiles.

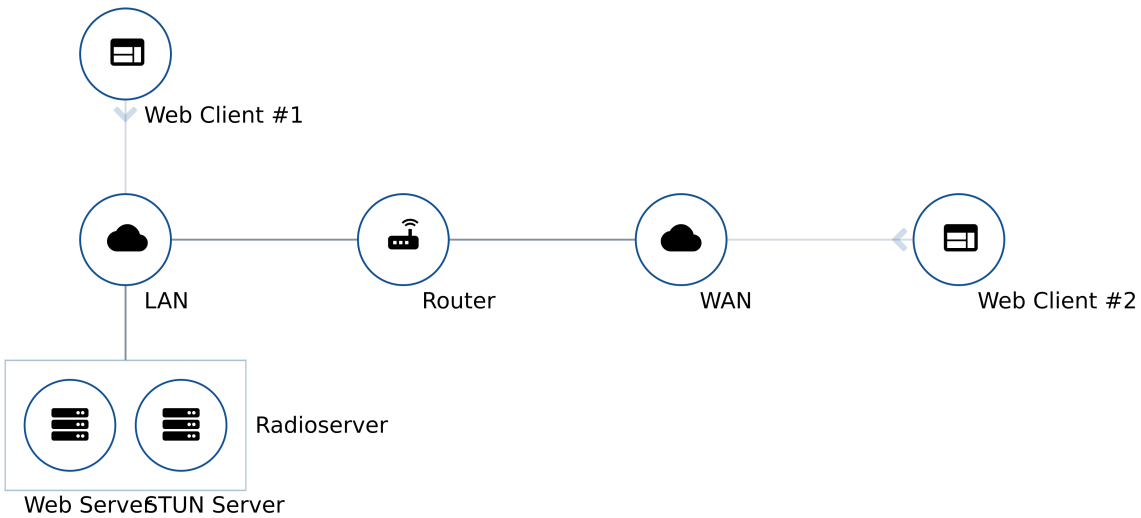
11. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

5.2 Web Clients

SmartPTT provides basic dispatch functions from the web browser. Corresponding application is named SmartPTT Web Client. It is installed together with SmartPTT Radioserver.



Web Client provides the following features:

- Work on the Internet.
- Text messages reception and initiation.

- Showing radios on Google Maps.
- Radioserver access over LAN and WAN.

For detailed information on the Web Client, see *SmartPTT Web Console Setup and User Guide*.

Radioserver Configuration

To configure Web Clients support on SmartPTT Radioserver, the following actions must be performed:

- Google API key with active billing must be generated. For details, see Google Map Keys.
- SmartPTT license must allow voice and/or data communication for Web Clients. For details, see Viewing License Items.
- *(Optional)* Profiles must be created and configured. For details, see Managing Profiles.
- Client accounts must be created. For details, see Managing Client Account Parameters.
- Dedicated SmartPTT Radioserver interface must be configured. For details, see Configuring Web Client Connection.
- Set TCP and UDP ports must be unlocked in the firewall software. For details, see Radioserver Host.

5.2.1 Configuring Web Client Connection

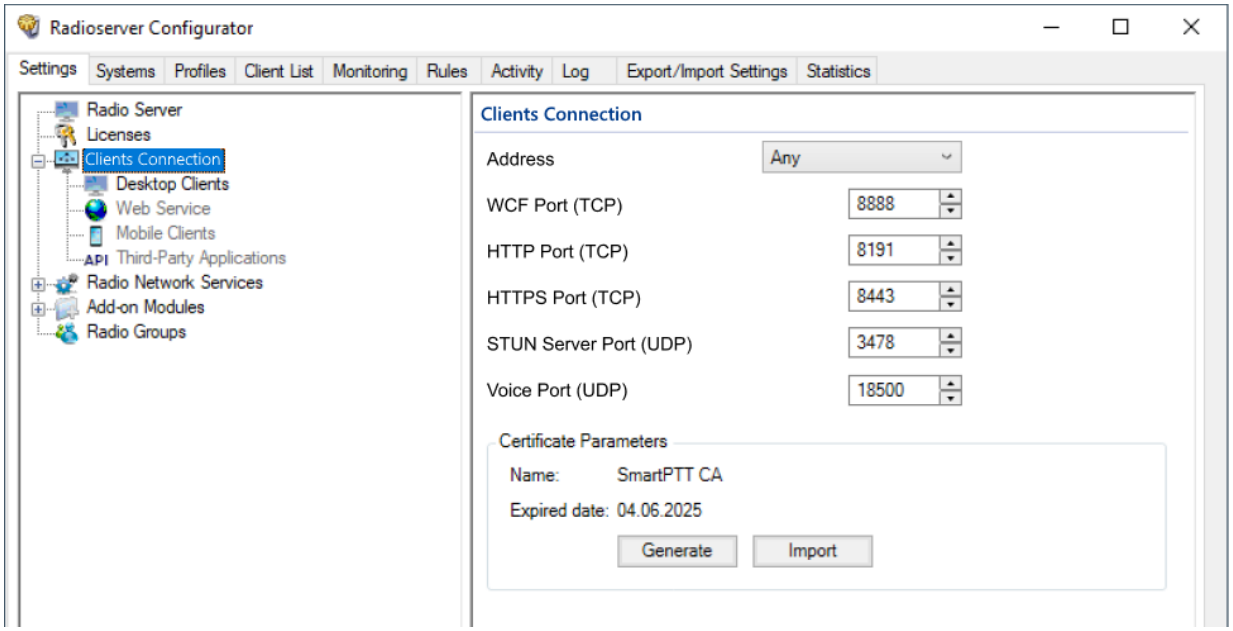
Follow the procedure to configure client connections to support SmartPTT Web Client.

Prerequisites:

- Determine the SmartPTT Radioserver host IP address.
- Determine the HTTPS port and Voice UDP port numbers for SmartPTT Web Client connection.
- *(Optional)* Determine the STUN Server TCP port number to support SmartPTT Web Client users who are not in the SmartPTT Radioserver Local Area Network.
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure you have the required license. For details, see Installing License.
- Obtain a Google API key to unlock Google Maps.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, click ***Clients Connection***.



3. If required, in the right pane, from the ***Address*** list, select the desired option:

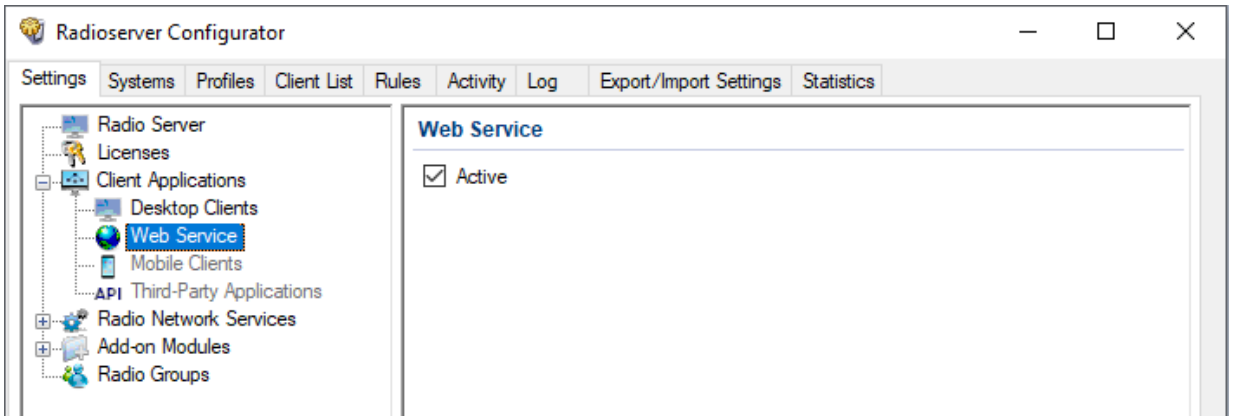
To allow SmartPTT Radioserver to accept connection requests to any address of its own,	select *Any*.
To allow client applications to connect to SmartPTT Radioserver only through a specific address,	select the desired IP address from the list.

4. Specify the ports for SmartPTT Web Client connection:
   a. In the ***HTTPS Port (TCP)*** field, enter the desired port number for receiving connections from web applications.
   b. In the **Voice Port (UDP)** field, enter the desired port number that will be used to exchange voice traffic between SmartPTT Radioserver and SmartPTT Web Client.
   c. *(Optional)* In the ***STUN Server Port (UDP)*** field, enter the desired port number for identification of SmartPTT Web Clients outside the SmartPTT Radioserver local network.
5. In the ***Certificate Parameters*** area, configure the certificate that will be used for encrypted connection to Web Client:

To use the self-signed certificate SmartPTT,	click ***Generate***.
To import a custom certificate,	perform the following actions: 1. Click ***Import***. 2. In the window that appears, select the certificate file in the PFX or P12 format. 3. In the next window that appears, enter the password to upload the selected certificate.

6. In the left pane, expand the ***Clients Connection*** node.

7. Click the ***Web Service*** node.



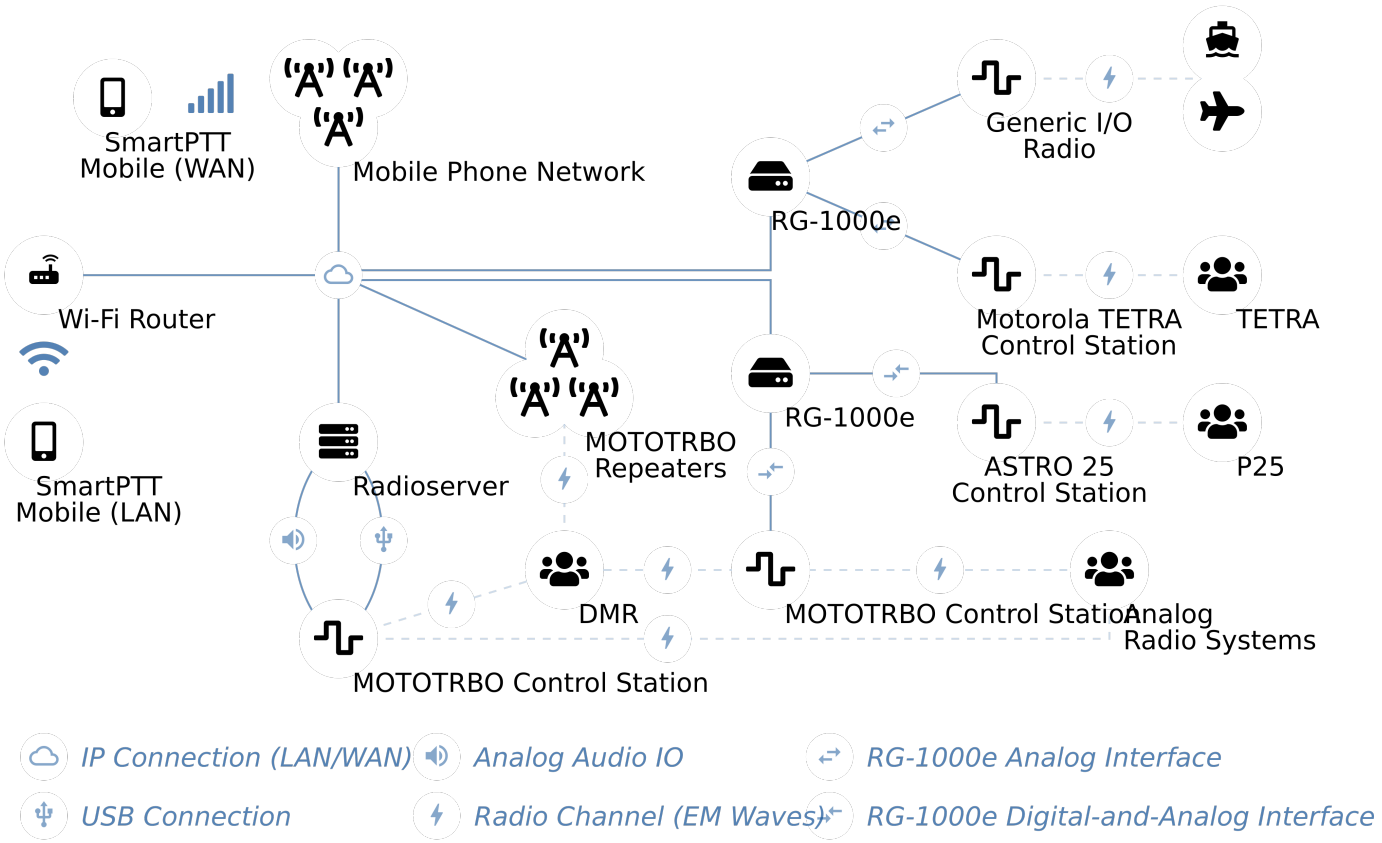
8. In the right pane, select the ***Active*** check box.
9. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***..

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

5.3 SmartPTT Mobile

SmartPTT provides basic dispatch functions to SmartPTT Mobile users. SmartPTT Mobile is a lightweight application for both Android and iOS operating systems with voice and data communication capabilities. SmartPTT Mobile is distributed via Google Play and App Store.



SmartPTT Mobile provides the following features:

- Voice communication with radios and talkgroups (group and private calls).
- Voice communication with other SmartPTT Mobile users (group and private calls).
- Tracking SmartPTT Mobile users and radios online/offline status in real time.
- Ability to create virtual groups for simultaneous voice communication with other SmartPTT Mobile users and DMR talkgroups.

NOTE
These groups can be managed both by SmartPTT Mobile users and by SmartPTT Dispatcher. Virtual groups that consist only of SmartPTT Mobile users are presented as dynamic groups in SmartPTT Dispatcher, and virtual groups that include both DMR talkgroups and dynamic groups are presented as cross patches between talkgroups and dynamic groups in SmartPTT Dispatcher and as multigroups in SmartPTT Mobile.

- Ability to display call history of the contact.
- Ability to work in two modes: in high priority mode and in normal mode.
- Displaying SmartPTT Mobile users and radios on maps.

For detailed information on SmartPTT Mobile, see *SmartPTT Mobile User Guide for Android* or *SmartPTT Mobile User Guide for iOS*.

Radioserver Configuration

To configure SmartPTT Mobile support on SmartPTT Radioserver, the following actions must be performed:

- *(Optional)* For SmartPTT Mobile version 5.1.1 or later for Android, obtain the OpenStreetMap address.
- SmartPTT license must allow voice and/or data communication for SmartPTT Mobile. For details, see Viewing License Items.
- *(Optional)* Install license that allows to send multimedia data in chats.
- Create and configure profiles with personalities or without them. For details, see Managing Profiles.
- Create and configure client accounts. For details, see Managing Client Account Parameters.
- Configure dedicated SmartPTT Radioserver interface, generate a certificate, and activate mobile client connection. For details, see Configuring SmartPTT Mobile Connection.
- Unlock the set TCP and UDP ports in the firewall software. For details, see Radioserver Host.

5.3.1 Configuring SmartPTT Mobile Connection

Follow the procedure to configure client connections to support SmartPTT Mobile. For details, see SmartPTT Mobile.

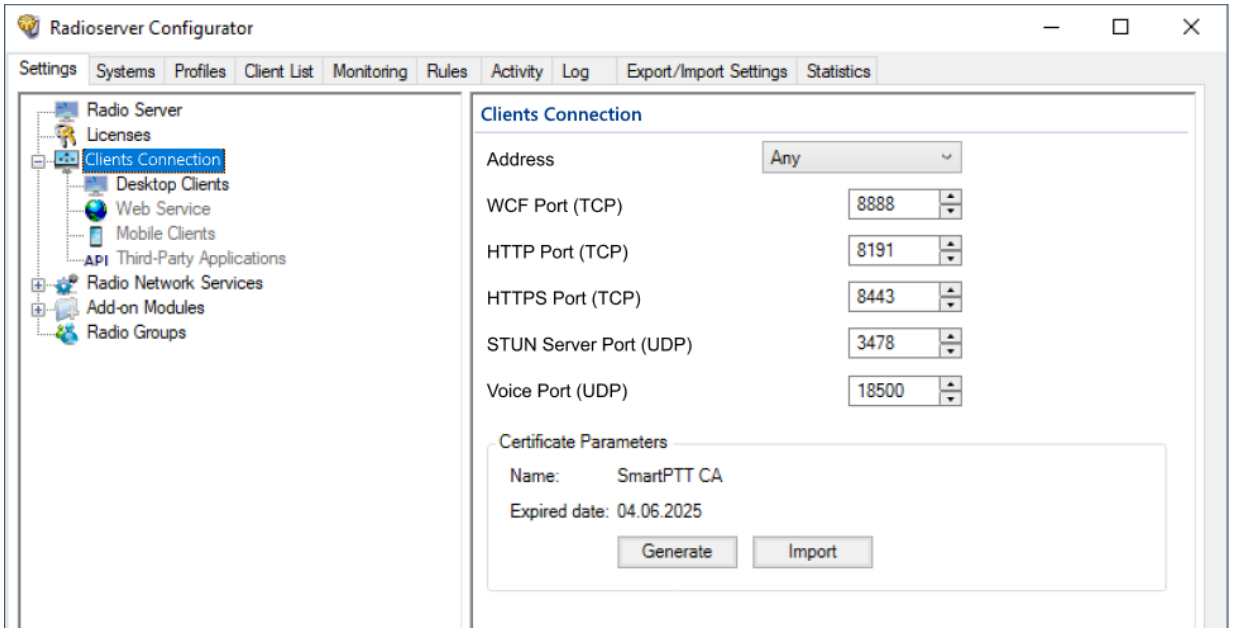
Prerequisites:

- Determine the SmartPTT Radioserver host IP address.
- Determine the HTTPS port and Voice UDP port numbers for the mobile application connection.
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure you have the required license. For details, see Installing License.

- *(Optional)* Obtain an OpenStreetMap address to unlock offline OpenStreetMap maps.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, click ***Clients Connection***.



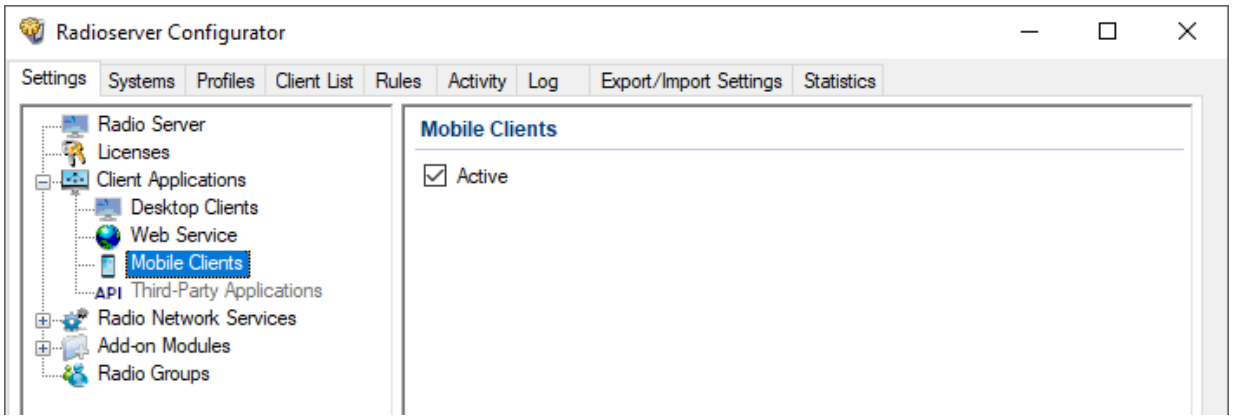
3. If required, in the right pane, from the ***Address*** list, select the desired option:

To allow SmartPTT Radioserver to accept connection requests to any available address,	select *Any*.
To allow client applications to connect to SmartPTT Radioserver using only a specific address,	select the desired IP address from the list.

4. In the ***HTTPS Port (TCP)*** field, enter the desired port number to receive connections from SmartPTT Mobile.
5. In the **Voce Port (UDP)** field, enter the UDP port number that will be used to exchange voice traffic between SmartPTT Radioserver and SmartPTT Mobile.
6. In the ***Certificate Parameters*** area, configure the certificate that will be used for encrypted connection to SmartPTT Mobile:

To use the self-signed certificate SmartPTT,	click ***Generate***.
To import a custom certificate,	perform the following actions: 1. Click ***Import***. 2. In the window that appears, select the certificate file in the PFX or P12 format. 3. In the next window that appears, enter the password to upload the selected certificate.

7. In the left pane, expand the ***Clients Connection*** node.
8. Click the ***Mobile Clients*** node.



9. In the right pane, select the ***Active*** check box.
10. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

5.3.2 Configuring Multimedia

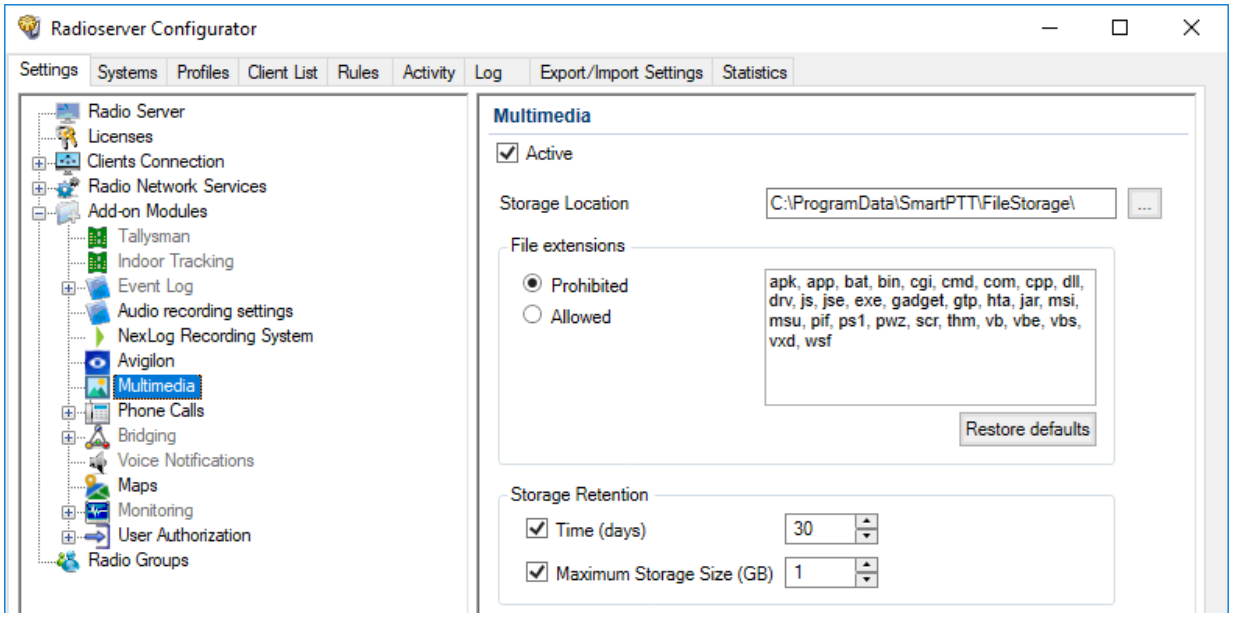
Follow the procedure to configure multimedia transmission in the SmartPTT Mobile chats.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure the SmartPTT license allows multimedia transmissions. For details, see Viewing License Items.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane of the tab, expand the ***Add-on Modules*** node, and then click ***Multimedia***.
   The multimedia transmission settings appear in the right pane of the tab.



3. In the right pane of the tab, select the ***Active*** check box.
4. Specify the directory where multimedia sent by SmartPTT Mobile users will be stored:
   a. To the right of the ***Storage Location*** field, click the Browse (...) button.
   b. In the window that appears, select the desired directory, and then click ***OK***.
5. In the ***File extensions*** area, allow/prohibit extensions for files that can be sent in text chats:

To prohibit sending files with specified extensions,	perform the following actions: 1. Select ***Prohibited***. 2. In the field to the right, type the desired file extensions.
To allow sending files with only specified extensions,	perform the following actions: 1. Select ***Allowed***. 2. In the field to the right, type the desired file extensions.
To restore default extension list,	click ***Restore defaults***.

6. In the ***Storage Retention*** area, configure multimedia storage parameters:

To configure the period after which data will be deleted,	perform the following actions: 1. Select the ***Time (days)*** check box. 2. In the field to the right, type the desired period in days.
To specify the maximum storage size,	perform the following actions: 1. Select the ***Maximum Storage Size (GB)*** check box. 2. In the field to the right, type the maximum size. When the maximum size is achieved, the system will delete old files to free space for new files. The size of

deleted files is equal to the size of new files that must be saved.

7. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

5.4 Third-Party Apps

SmartPTT provides the platform-independent language-agnostic application programming interface (API). The API allows third-party applications development which includes end-user apps and middleware.

API provides the following capabilities to developers:

- SmartPTT Radioserver connection over the WebSocket protocol.
- Asynchronous data exchange with SmartPTT Radioserver using JSON-like messages.
- Voice and data exchange.
- Software Development Kit (SDK) access that includes traffic analyzer and embedded documentation.

For information on SDK and API, submit a request to SmartPTT Technical Support Center.

Radioserver Configuration

To configure third-party applications on SmartPTT Radioserver, the following actions must be performed:

- SmartPTT license must allow API usage. For details, see Installing License.
- *(Optional)* Profiles must be created and configured. For details, see Managing Profiles.
- Client accounts must be created. For details, see Managing Client Account Parameters.
- Dedicated SmartPTT Radioserver interface must be configured. For details, see Configuring Third-Party Applications.
- Set TCP and UDP ports must be unlocked in the firewall software. For details, see Radioserver Host.

5.4.1 Configuring Third-Party Applications

Follow the procedure to configure client connections to support third-party applications that use Server API.

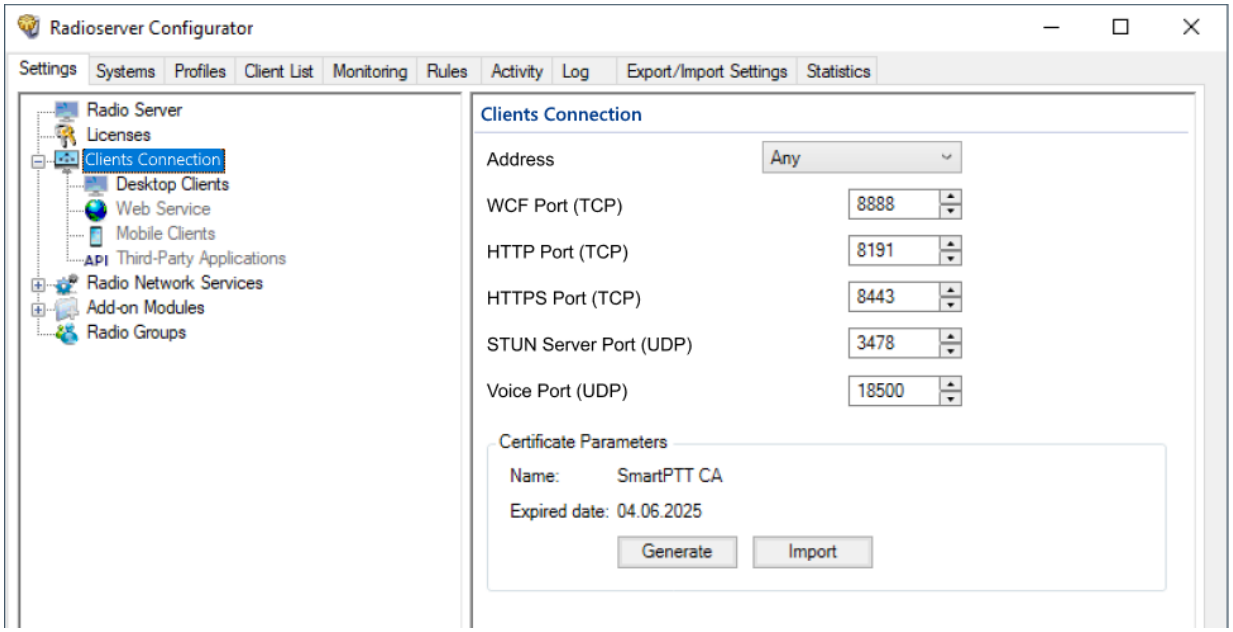
Prerequisites:

- Determine the SmartPTT Radioserver host IP address.
- Determine the HTTP port number for receiving connections from the desired application.
- If third-party applications support voice transmission, determine the Voice UDP port number.
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.

- Ensure you have the required API license. For details, see Installing License.

Procedure:

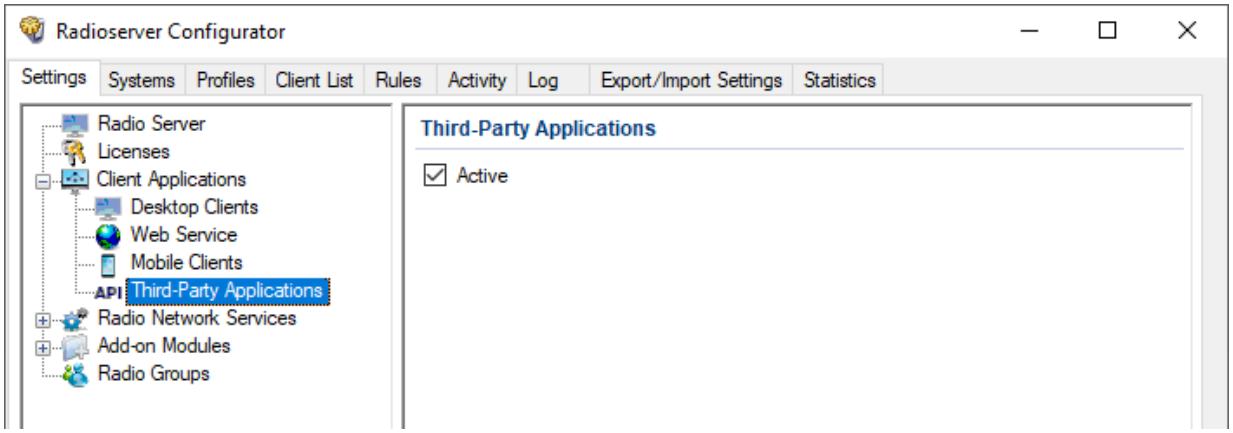
1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, click ***Clients Connection***.



3. If required, in the right pane, from the ***Address*** list, select the desired option:

To allow SmartPTT Radioserver to accept connection requests to any available address,	select *Any*.
To allow third-party applications to connect to SmartPTT Radioserver using only a specific address,	select the desired IP address from the list.

4. In the ***HTTP Port (TCP)*** field, enter the desired port number for receiving connections from third-party applications.
5. If third-party applications support voice transmission, in the **Voice Port (UDP)** field, enter the UDP port number that will be used to exchange voice traffic between SmartPTT Radioserver and third-party applications.
6. In the left pane, expand the ***Clients Connection*** node.
7. Click the ***Third Party Applications*** node.



8. In the right pane, select the ***Active*** check box.
9. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

5.5 Profiles

In SmartPTT, profile is a tool for client permissions and restrictions management. Profiles control the following features:

- Access to radio systems, including per-slot and per-control station. For details, see Available Networks.
- Access to the radioserver license from SmartPTT Dispatcher.
- Access to a limited set of radios and talkgroups.
- Access to groups consisting of SmartPTT Mobile users.
- Access to a limited networks and features within them. For details, see Available Networks.
- Access to a limited dispatcher actions. For details, see Available Actions.
- Personality settings of the SmartPTT Mobile profile. For details, see Configuring Personalities

In addition to profiles, client permissions and restrictions in SmartPTT Dispatcher can be adjusted on per-console basis using operator rights. For details, see “Operators” in *SmartPTT Dispatcher Guide*.

Profiles can be assigned only to client accounts. Before the assignment, consider the following details:

- For Web Client, the SmartPTT Mobile mobile client or API application to be able to connect to SmartPTT Radioserver, you must create and assign a profile to the client.
- For SmartPTT Dispatcher to be able to connect to SmartPTT Radioserver when desktop client authorization is enabled, you must create and assign a profile to the client.
- For SmartPTT Dispatcher to be able to connect to SmartPTT Radioserver when desktop client authorization is disabled, you must create a profile for anonymous connections.

Important
If no profiles are assigned to the client account in SmartPTT Radioserver Configurator, or there is no profile for anonymous connections when desktop client authorization is disabled, SmartPTT Dispatcher cannot connect to SmartPTT Radioserver, and the connection error is displayed.
After you assign a profile to this client account in SmartPTT Radioserver Configurator, or after you create a profile for anonymous connections when desktop client authorization is disabled, SmartPTT Dispatcher does not connect automatically. You must restart SmartPTT Dispatcher or reconnect it to SmartPTT Radioserver.

- If you want SmartPTT Dispatcher to connect to SmartPTT Radioserver without authorization, then perform the following actions:
  - Disable desktop client authorization on SmartPTT Radioserver. For details, see Configuring Desktop Clients Connection.
  - Create one or more profiles for anonymous connections. In the settings of such profiles, you must select the ***Use for anonymous connections*** check box. For details, see Managing Profiles.
    As a result, in the SmartPTT Dispatcher, any operator will be able to switch between these profiles.
- If you want SmartPTT Dispatcher to connect to SmartPTT Radioserver with authorization, then perform the following actions:
  - Enable desktop client authorization on SmartPTT Radioserver. For details, see Configuring Desktop Clients Connection.
  - Create and configure one or more profiles. In the settings of such profiles, clear the ***Use for anonymous connections*** check box. For details, see Managing Profiles.
  - Create a client account and assign one or more profiles to that customer. For details, see Managing Client Account Parameters.
    In SmartPTT Dispatcher, the operator will be able to switch between the profiles that have been assigned to their client account.
  - In SmartPTT Dispatcher, in SmartPTT Radioserver connection settings, specify the client credentials. For details, see “Radioserver Management“ of the *SmartPTT Dispatcher Guide*.
- You can assign the same profile to multiple accounts.
- You can assign multiple profiles to one client account. The feature provides an operator with the ability to change profiles in SmartPTT Dispatcher. For details, see Managing Client Account Parameters. This may help when, for example, several users work under one operator account and they have different restrictions to the SmartPTT Radioserver data.

The *default* profile is the profile that provides full access to all SmartPTT Dispatcher features. The *default* profile is available only if you selected *Legacy* authentication type during SmartPTT installation. For details, see Installing on New Computer.

The *default* profile is automatically assigned to all new clients added on the ***Clients*** tab. For details, see Managing Client Account Parameters. If you delete the *default* profile, you will have to assign profiles to all new clients manually.

If local or domain authentication is used, assign any profile to all clients manually, or to a linked user group. Otherwise, clients without a profile will not be able to connect to SmartPTT Radioserver.

Important
A user with the *Administrator* role is prohibited from changing their rights and rights of other *Administrators* in SmartPTT Dispatcher. You can configure rights for the administrator profile only in SmartPTT Radioserver Configurator. For details, see Managing Profiles.

5.5.1 Available Networks

Available networks and available features within them are as follows:

Available functionality	Description
Network	Allows/denies operation with the functionality of the radio network or control station.

<Radioserver alias>	Allows/denies operation with virtual control station functionality. For details, see SmartPTT Mobile.
	You can change the radioserver alias in ***Settings*** → ***Radioserver*** → ***Name***. The subnodes of this node refer to the SmartPTT Mobile users:
	• ***Dynamic Groups*** allows/denies interaction with dynamic groups.
	• ***Network Services*** allows/denies interaction with the SmartPTT Mobile users. This node has the following subnodes:
	  • ***Text Messages*** allows/denies SmartPTT Mobile users to exchange text messages.
	  • ***Other Network Services*** allows/denies access to voice calls services and location services.
	NOTE
	If you use mobile clients in your system, in the profile of each mobile client, select the ***<Radioserver alias>*** check box.

All Call/All Call on sites	Allows/denies receiving and initiating All Calls including All Calls on sites (available for Linked Capacity Plus and Capacity Max networks).
<Talkgroup name>	Allows/denies interaction with the talkgroup.

The following features are available for repeater-based systems only. They are unavailable for control stations.

Temporary Talkgroups	Allows/denies interaction with temporary talkgroups created in SmartPTT. This does not provide the permissions to manage such groups or add/remove their members (available only for Capacity Max networks).
Radio Network Services	The subnodes of this node refer to the radio network services: • ***Voice calls*** For details, see Voice calls below. • ***ARS*** allows/denies access to ARS service. This requires configuring ARS on SmartPTT Radioserver. For details, see Configuring ARS.

	• ***GPS*** allows/denies access to GPS service. This requires configuring GPS on SmartPTT Radioserver. For details, see Configuring GPS. ***NOTE*** This parameter does not prohibit operation with Indoor beacon systems. For details, see Beacon-Based Location (Indoor). • ***TMS*** allows/denies access to TMS service. This requires activating TMS on SmartPTT Radioserver. For details, see Activating Text Message Sending and Receiving. • ***Telemetry*** allows/denies access to Telemetry service. This requires activating Telemetry service on SmartPTT Radioserver. For details, see Activating Telemetry.
Voice calls	The subnodes of this node refer to the voice calls: • ***Group calls*** allows/denies voice calls to the talkgroup. • ***Private calls*** allows/denies initiating and receiving private calls to radios. • ***Private calls monitoring*** allows/denies remote monitor of private calls within the network including calls from one radio to another, calls from a radio to another dispatcher, calls from a radio to a telephone subscriber.

Available Networks and their Features Applicability to Different Client Types

The following network-level features are applicable to desktop clients only:

- Temporary talkgroups (Capacity Max).
- Job tickets.
- Telemetry.
- Private calls monitoring.

Other features are also applicable to other client types.

The functionality of the SmartPTT Mobile virtual control station is used to restrict the dispatcher actions applied to SmartPTT Mobile users.

5.5.2 Available Actions

For SmartPTT clients the following dispatcher actions are available:

Action	*Description*
Call Prioritization (Capacity Max)	Contains the following subnodes:

Action	Description
	• ***Increase permanently*** If the check box is selected, all calls initiated by the dispatcher will have high priority and will interrupt calls with normal priority (only for Capacity Max networks). This setting blocks the ***Increase outgoing call priority (Capacity Max)*** check box. • ***Allow increase*** If the check box is selected, the call priority can be increased from normal to high before initiating the call (only for Capacity Max networks). High priority calls interrupt those with normal priority. For details, see “Increasing Call Priority” in SmartPTT Dispatcher Guide. ***NOTE*** Emergency calls and All Calls always have high priority and cannot be interrupted.
Access real-time monitoring info	Allows/denies the system monitoring in real time in SmartPTT Dispatcher.
Cross patches management	Allows/denies editing those cross patches which include only talkgroups allowed to the dispatcher by the profile. The ***Immediate patch disable*** allows the operator to disable a cross patch without waiting until current calls will be finished.
Temporary talkgroups management (Capacity Max)	Allows/denies managing temporary talkgroups. The setting is applicable only when the ***Temporary Talkgroups*** check box is selected under the Capacity Max network node on the ***Available Networks*** tab.
Access to audio recordings	Contains the following subnodes: • ***Listen to audio recordings*** allows/denies the operator to listen to radioserver recordings directly in SmartPTT Dispatcher. • ***Download audio recordings*** allows/denies the operator to download from SmartPTT Dispatcher audio recordings stored on the radioserver.
Access to Audit Log	Allows you to obtain the following authentication information via API request: attempts to log in to SmartPTT Radioserver Configurator and connect the client, log out of SmartPTT Radioserver Configurator and disconnect the client, as well as changing SmartPTT Radioserver Configurator settings.

Operator permissions	Allows managing permissions of SmartPTT Dispatcher operators. Contains the following subnodes:
	• ***Create reports*** allows/denies building reports.
	  • ***Use radioserver data for location reports*** allows/denies building reports using coordinates from SmartPTT Radioserver.
	  • ***Use radioserver data for monitoring reports*** allows/denies building monitoring reports using monitoring data from SmartPTT Radioserver.

Action	Description

	• ***Access coverage map*** allows/denies operations with a coverage map.
	  • ***Use server data*** allows/denies using SmartPTT Radioserver data for generating a coverage map.
	• ***Outgoing Calls*** allows/denies the outgoing calls that are available within networks according to the settings on the ***Available Networks*** tab.
	  • ***Limit concurrent calls*** limits the number of simultaneous outgoing calls that the dispatcher can initiate.
	If selected, a specific value is set. If not selected, the number of simultaneous outgoing calls is limited by the bandwidth of the radio system. It ranges from 1 to 45. The default value is *45*.
	NOTE
	This parameter does not refer to the following calls: routing calls configured by a dispatcher, telephone calls, voice calls between dispatchers.
	• ***Request location*** allows/denies performing the following actions related to the radio location:
	  • Set Location
	  • Find on Map
	  • Show Address
	  • Remove from Map
	  • Find on Indoor Map
	• ***Allow remote monitor*** allows/denies using the Remote Monitor function.
	NOTE
	The Remote Monitor function requires permission to operate with private calls.
	• ***Block and unblock radios*** allows/denies blocking/unblocking radios.
	• ***Allow radio kill*** allows/denies using the Radio Kill command (available only for Capacity Max networks).
	• ***Bridging management*** allows/denies configuring the calls routing on SmartPTT Radioserver.
	• ***Edit radio lists*** allows/denies adding, editing, or deleting radios on the ***Radio Fleet*** panel and in the ***Radios*** window of SmartPTT Dispatcher.
	• ***Manage unregistered radios*** shows/hides radios which were not added to SmartPTT Dispatcher.
	• ***Connect with external dispatchers*** allows/denies communicating with other SmartPTT dispatchers.
	• ***Make telephone calls*** allows/denies communicating with telephone subscribers.

Action	*Description*
	• ***Change channel on control station*** allows/denies selecting control station channels. • ***Reboot control station*** allows/denies rebooting (restarting) control stations. • ***Manage radio location settings*** allow/denies configuring settings of radio location update. • ***Send text messages*** allows/denies sending text messages to radios, talkgroups, and radio categories. • ***Send telemetry commands*** allows/denies sending telemetry commands. ***NOTE*** The right does not affect the data acquisition module. • ***Manage routes*** allows/denies managing routes on a map and building plan. • ***Manage geofences*** allows/denies managing geofences on a map and building plan. • ***Manage points of interest*** allows/denies managing points of interest on a map. • ***Manage cameras*** allows/denies managing camera markers on a map. • ***Manage tracks*** allows/denies displaying tracks and the radio movement along the track on a map. • ***Edit custom radio properties*** allows/denies managing parameters on the ***Others*** tab of the ***Radio Properties*** window. • ***Make conference calls*** allows/denies initiating conference calls. • ***Create deferred actions*** allows/denies creating deferred actions for radios. • ***Manage statuses*** allows/denies managing radio statuses. • ***Manage custom rules*** allows/denies managing custom rules. • ***Manage positioning rules*** allows/denies managing positioning rules. • ***Manage lone worker rules*** allows/denies managing Lone Worker profiles.
Override operator local permissions	Enables/disables priority of the profile settings in SmartPTT Radioserver Configurator over operator permissions settings in SmartPTT Dispatcher. If this check box is selected, then when connecting to SmartPTT Radioserver, SmartPTT Dispatcher uses permissions set in SmartPTT Radioserver Configurator in the active user profile. For details, see “Operators” in *SmartPTT Dispatcher Guide*.

Overriding Permissions when Working with Multiple Radioservers

SmartPTT Dispatcher can be connected to multiple radioservers on which ***Override operator local permissions*** is enabled in active profiles, and these profiles have operator permissions that differ from each other. In this case, if an action is allowed on at least

one of the radioservers, this action is considered allowed to the SmartPTT Dispatcher operator even if it is prohibited on other radioservers.

The feature concerns the following permissions:

- Edit radio lists
- Connect with external dispatchers
- Make telephone calls
- Request Location
- Manage routes
- Manage geofences
- Manage points of interest
- Manage tracks
- Access Coverage Map
- Create Reports
- Edit custom radio properties
- Make conference calls
- Create deferred actions
- Manage statuses
- Manage custom rules
- Manage positioning rules
- Manage lone worker rules

For example, if the ***Create reports*** permission is enabled on *Radioserver A*, and this permission is disabled on *Radioserver B*, the operator will be able to create reports in SmartPTT Dispatcher, since he has the permission from *Radioserver A*.

If the following actions are allowed on one of the radioservers, the actions concern only resources and data of the radioserver on which these actions are allowed:

- Manage unregistered radios
- Allow Outgoing Calls
- Limit Concurrent Calls
- Change channel on control station
- Block and Unblock Radios
- Allow Radio Kill
- Allow Remote Monitor
- Reboot control station
- Manage radio location settings

- Send text messages
- Send telemetry commands
- Set up Bridging
- Manage cameras
- Use Server Data for Location Reports
- Use Server Data for Monitoring Reports
- Use Server Data
- Access Server Event Log

For example, if the ***Use radioserver data for location reports*** permission is enabled on *Radioserver A*, and this permission is disabled on *Radioserver B*, the operator will be able to create reports based only on data from *Radioserver A*, but will not be able to create reports based on data from *Radioserver B*.

If SmartPTT Dispatcher loses connection to one of the radioservers, the permissions of this radioserver are deactivated.

Available Dispatcher Actions Applicability to Different Client Types

The actions available within the network apply to different types of SmartPTT clients according to the following table:

Actions	***Desktop***	***Web Clients***	***SmartPTT Mobile***	***Third-Party Apps***
Call prioritization (Capacity Max)	YES	NO	NO	NO
Cross patches management	YES	YES	YES	NO
Immediate patch enable/disable	YES	NO	NO	NO
Temporary talkgroups management (Capacity Max)	YES	NO	NO	NO
Dynamic groups visibility	YES	NO	YES	NO
Editing dynamic groups	YES	NO	YES	NO
Access to audio recordings				
Listen to audio recordings	YES	NO	NO	NO
Download audio recordings	YES	NO	NO	NO
Access to audit log	YES	NO	NO	NO
Operator permissions				
Create reports	YES	NO	NO	NO
Use radioserver data for location reports	YES	NO	YES	NO

Actions	Desktop	Web Clients	SmartPTT Mobile	Third-Party Apps
Use radioserver data for monitoring reports	YES	NO	NO	NO
Access coverage map	YES	NO	NO	NO
Use server data	YES	NO	NO	NO
Allow outgoing calls	YES	YES	YES	YES
Limit concurrent calls	YES	YES	YES	YES
Request location	YES	YES	YES	YES
Allow remote monitor	YES	NO	NO	NO
Block and unblock radios	YES	YES	NO	YES
Allow radio kill	YES	NO	NO	NO
Edit radio lists	YES	NO	NO	NO
Manage unregistered radios	YES	NO	NO	NO
Connect with external dispatchers	YES	NO	NO	NO
Make telephone calls	YES	YES	NO	NO
Change channel on control station	YES	NO	NO	NO
Reboot control station	YES	NO	NO	NO
Manage radio location setting	YES	NO	NO	NO
Send text messages	YES	YES	YES	NO
Send telemetry commands	YES	NO	NO	NO
Manage routes	YES	NO	NO	NO
Manage geofences	YES	NO	NO	NO
Manage points of interest	YES	NO	NO	NO
Manage cameras	YES	NO	NO	NO
Manage tracks	YES	NO	NO	NO
Edit customs radio properties	YES	NO	NO	NO

Actions	Desktop	Web Clients	SmartPTT Mobile	Third-Party Apps
Make conference call	YES	NO	NO	NO
Create deferred actions	YES	NO	NO	NO
Manage statuses	YES	NO	NO	NO
Manage custom rules	YES	NO	NO	NO
Manage positioning rules	YES	NO	NO	NO
Manage lone workers rules	YES	NO	NO	NO
Override operator local permissions	YES	NO	NO	NO

Visibility of dynamic groups and cross-patches

Below is a table of the visibility of dynamic groups (called virtual groups in SmartPTT Mobile) and cross patches (called multi-groups in SmartPTT Mobile) involving dynamic groups for different clients under the following conditions:

- Client 1 is the member of the dynamic group 2
- Client 2 is the member of the dynamic group 1
- Client 3 is the member of the dynamic groups 1 and 3
- Clients 4 and 5 are the members of the dynamic group 3
- Cross patch combines the dynamic groups 1 and 2
- Clients 2 and 5 have a common label and can see each other, other clients do not see each other directly

Client Name	Group 1	Group 2	Group 3	Cross Patch
Client 1	Does not see, can hear through the cross patch	Can see, can hear	Does not see, cannot hear	Can see, can hear
Client 2	Can see, can hear	Does not see, can hear through the cross patch	Can see and hear if the *Adjacent groups* option is enabled	Can see, can hear
Client 3	Can see, can hear	Does not see, can hear through the cross patch	Can see, can hear	Can see, can hear
Client 4	Does not see, cannot hear	Does not see, cannot hear	Can see, can hear	Does not see, cannot hear
Client 5	Can see and hear if the *Adjacent groups* option is enabled	Does not see, can hear through the cross patch if the *Adjacent groups* option is enabled	Can see, can hear	Can see and hear if the *Adjacent groups* option is enabled

5.5.3 Managing Profiles

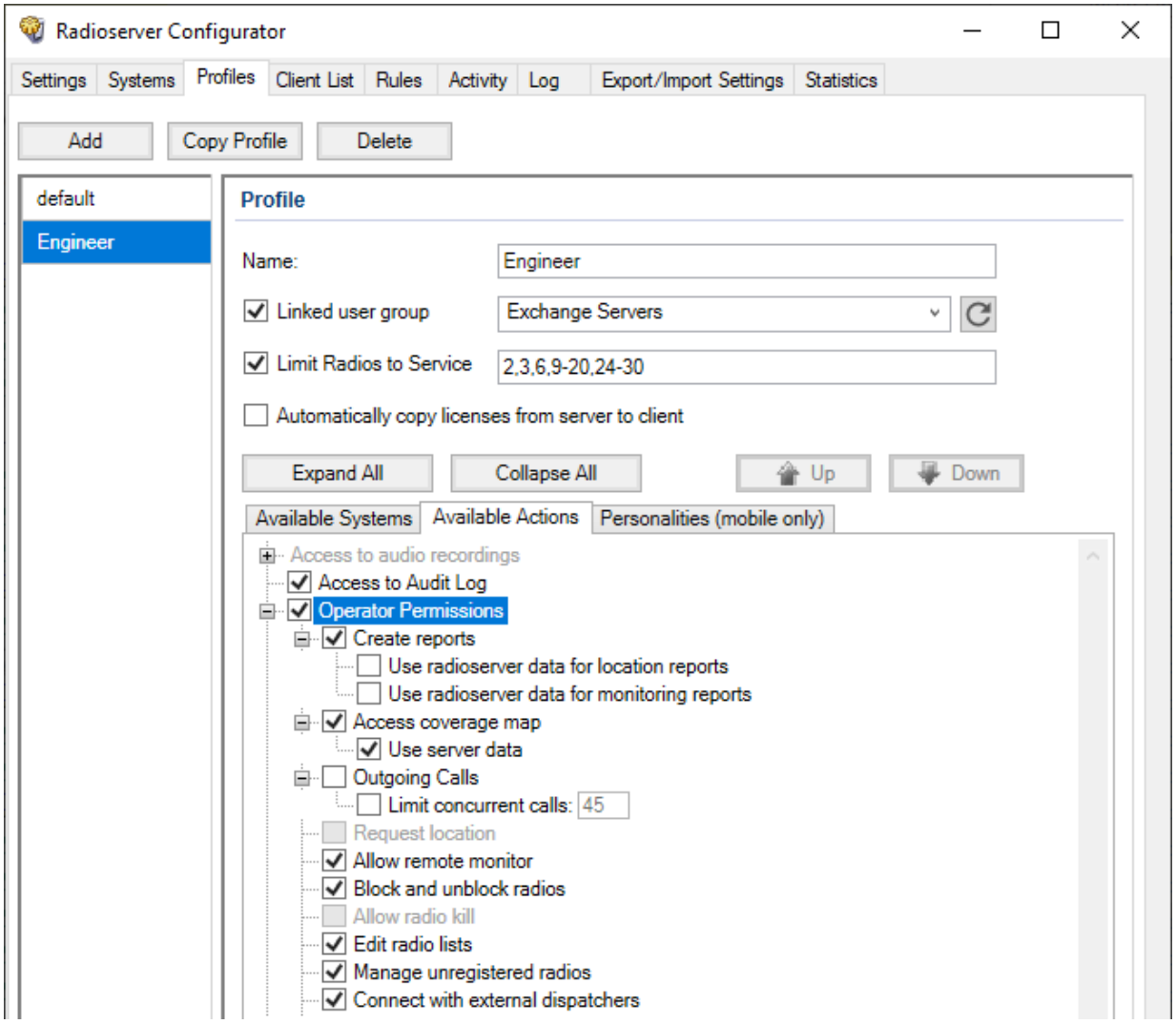
Follow the procedure to add, make a copy, delete, or edit a profile.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- In the ***Clients Connection*** node of the ***Settings*** tab, activate the desired type of the client.
- On the ***Systems*** tab, add and configure the desired radio networks.
- On the ***Settings*** tab, activate and configure necessary features.
- Determine the profile name.
- *(Optional)* Determine radio IDs that will be available to the profile.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Profiles*** tab.



2. In the left pane, perform one of the following actions:

To add a new profile,	click ***Add***.
To copy the existing profile,	perform the following actions: 1. In the list, select the desired profile. 2. Click ***Copy Profile***.
To modify an existing profile,	in the list, click the desired profile.
To delete a profile,	perform the following actions: 1. In the list, select the desired profile. 2. Click ***Delete***. 3. Proceed to the last step of this procedure.

3. In the ***Name*** field, type the desired profile name.
4. *(Optional)* To assign the current profile to the desired user group, select the ***Linked user group*** check box. The check box is available if local or domain authentication is selected during SmartPTT installation. For details, see Installing on New Computer.
   From the drop-down list, select the desired user group. The list displays local or domain groups depending on the authentication type selected when SmartPTT was installed. The current profile will be assigned to all users in the selected group.
5. *(Optional)* To make the profile available to all SmartPTT Dispatcher operators when the anonymous connections to the radioserver are allowed, select the ***Use for anonymous connections*** check box. For details, see Desktop Clients.
6. *(Optional)* If you need to limit profile access to radios, configure the radio filter:
   a. Select the ***Limit Radios to Service*** check box.
   b. In the ***Limit Radios to Service*** field, enter IDs of radios with which the profile is allowed to interact. To specify a range of radios, use a hyphen. To enumerate identifiers, use a comma without a space. Example: *10,20,30-40,50-60*.

NOTE
The radio filter is not applicable to the SmartPTT Mobile users.

7. *(Optional)* If you want SmartPTT Dispatcher to use radioserver licenses, select the ***Automatically copy licenses from server to client*** check box. After connecting to the radioserver, SmartPTT Dispatcher applies the radioserver license file and allows you to configure its licensed features.
8. On the ***Available Systems*** tab, select networks, their services and features which will be available to a client with the profile. For details, see Configuring Access to Networks.
9. On the ***Available Actions*** tab, select actions which will be available to a client with the profile in the radio network. For details, see Configuring Access to Actions.
10. *(Optional)* For mobile clients that are used in the radio mode, on the ***Personalities (mobile only)*** tab, configure a personality. For details, see Configuring Personalities.
11. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***. Changes will be applied without restarting SmartPTT Radioserver.

Postrequisites:

(Optional) If you want to deny anonymous desktop client connections to the radioserver, select the ***Deny anonymous connections***

check box. Then create a new client account and assign desired profiles to it. For details, see Client Applications and Managing Client Account Parameters.

5.5.3.1 Configuring Available Networks

Follow the procedure to configure profile access to radio networks, their services, and features.

Prerequisites:

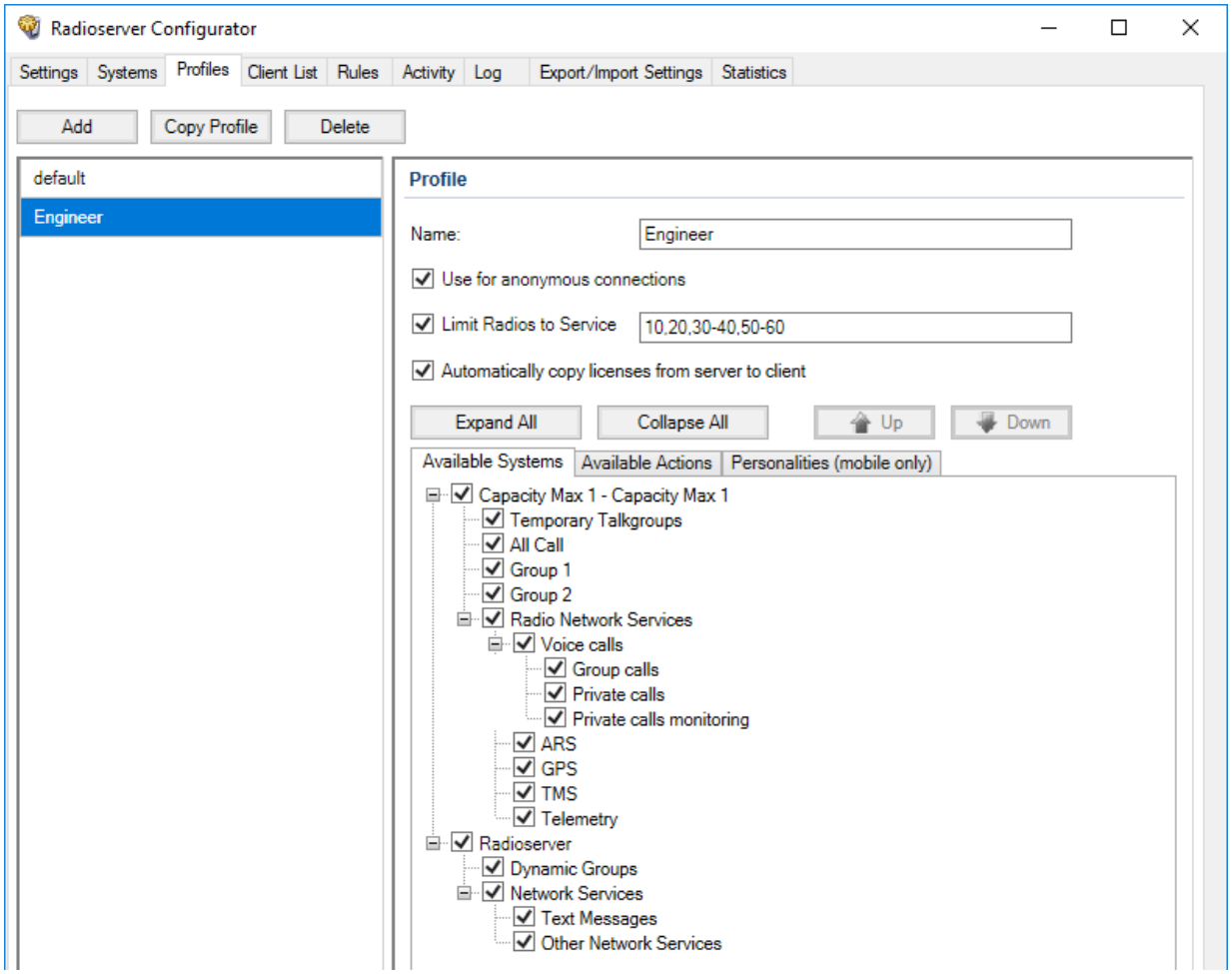
- Connect to radio networks.:
  - To access the MOTOTRBO radio systems, see MOTOTRBO Radio Systems.
  - To access the P25 radio systems, see P25 Radio Systems.
- *(Optional)* Configure base radioserver services. For details, see Basic Configuration.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Profiles*** tab.
2. In the left pane, click the desired profile.
3. In the right pane, open the ***Available Systems*** tab.
4. On the tab, perform one of the following actions:

To expand a subnode in the tree,	click the Expand (⊞) button next to the desired node name.
To expand all nodes of the tree,	click ***Expand All***.

5. Select the check box next to the network name so that a profile can access it.
   To give a profile access to the SmartPTT Mobile virtual control station features, select the check box near the node name that matches the radioserver name.



6. To configure profile access to features referred to groups, perform the following actions:

To allow interaction with talkgroups,	select the ***<Group name>*** check box.
To allow receiving and initiating All Calls,	select the ***All Call*** check box.
To allow interaction with temporary talkgroups created in SmartPTT,	under the desired Capacity Max network node, select the ***Temporary Talkgroups*** check box.

7. To configure profile access to features referred to radio network services, perform the following actions:

To allow receiving information about radio state (*Online*/*Offline*) from the ARS service,	select the ***ARS*** check box.
To allow receiving information about radio location,	select the ***GPS*** check box.
To allow exchanging text messages and sending tasks,	select the ***TMS*** check box.
To allow transmitting telemetry signals to radios,	select the ***Telemetry*** check box.
To allow access to all radio network services,	select the ***Radio Network Services*** check box.
To allow access to all services for SmartPTT Mobile users,	under the node name that matches the radioserver name, select the ***Network Services*** check box.

To allow SmartPTT Mobile users to exchange text messages,	perform the following actions: 1. Expand the node name that matches the radioserver name → ***Network Services***. 2. Select the ***Text Messages*** check box.
To allow SmartPTT Mobile users to use voice calls services and location services,	perform the following actions: 1. Expand the node name that matches the radioserver name → ***Network Services***. 2. Select the ***Other Network Services*** check box.

8. To configure profile access to features referred to voice calls, perform the following actions:

To allow voice calls to talkgroups,	select the ***Group calls*** check box.
To allow initiating and receiving radio private calls,	select the ***Private calls*** check box.
To allow remote monitor of private calls within the network including calls from one radio to another, calls from a radio to another dispatcher, calls from a radio to a telephone subscriber,	select the ***Private calls monitoring*** check box.
To allow access to any voice calls,	select the ***Voice calls*** check box.

9. *(Optional)* Use the ***Up*** or ***Down*** buttons to move the selected network node up/down the tree located on the ***Available Systems*** tab. The order of the network nodes affects the order in which objects are displayed on the ***Radio Fleet*** panel in SmartPTT Dispatcher.
10. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (***  ***)***. Changes will be applied without restarting SmartPTT Radioserver.

Postrequisites:

- Configure available actions within the selected network for a profile. For details, see Configuring Access to Actions.
- Create the client account and assign the desired profile to it. For details, see Managing Client Account Parameters.

5.5.3.2 Configuring Available Actions

Follow the procedure to configure profile access to actions in the radio network.

Prerequisites:

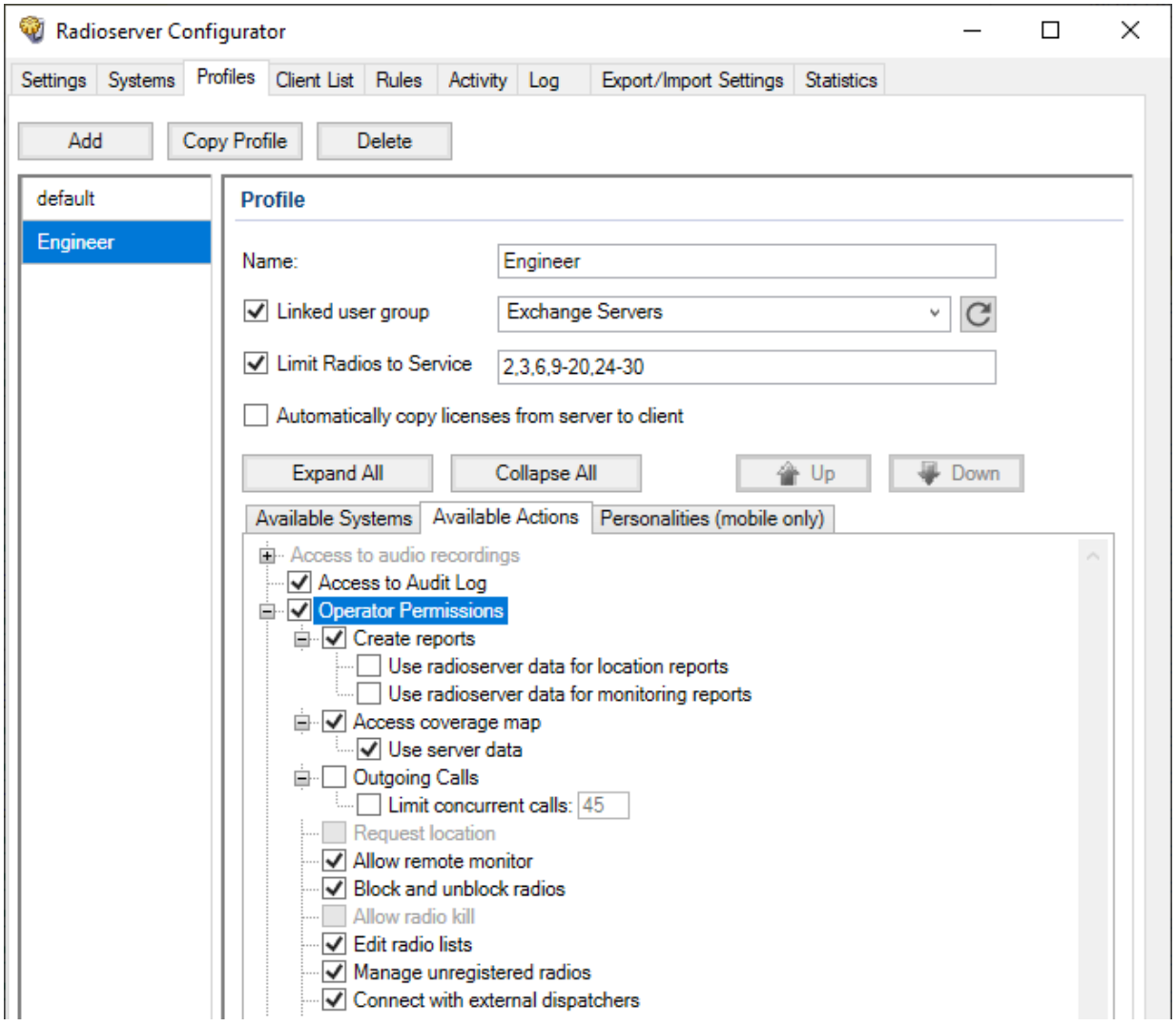
- Connect to radio networks.:
  - To access the MOTOTRBO radio systems, see MOTOTRBO Radio Systems.
  - To access the P25 radio systems, see P25 Radio Systems.
- Enable the following features:
  - Radio Network Services.
  - Bridging. For details, see Managing Bridging.

- Event Log database. For details, see Configuring Event Log Database Connection.
- Monitoring. For details, see Configuring Monitoring Database Connection.
- Configure the available networks. For details, see Configuring Access to Networks.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Profiles*** tab.
2. In the left pane, click the desired profile.
3. In the right pane, open the ***Available Actions*** tab.
4. On the tab, perform one of the following actions:

To expand a subnode in the tree,	click the Expand button (⊞) button next to the desired node name.
To expand all nodes of the tree,	click ***Expand All***.



5. To configure profile access to actions referred to outgoing calls, perform the following actions:

To allow initiating outgoing calls,	select the ***Outgoing Calls*** check box.

To limit the maximum number of simultaneous outgoing calls that the dispatcher can initiate at the same time,	perform the following actions: 1. Select the ***Maximum number of simultaneous calls*** check box. 2. In the field to the right, specify the desired value. The range of possible values is *1–45* calls. The default value is *45*. ***NOTE*** If you clear the check box, the number of simultaneous outgoing calls is limited by the bandwidth of the radio system
For all calls initiated by the dispatcher to have high priority and interrupt calls with normal priority (available only for Capacity Max networks),	select the ***High priority calls (Capacity Max)*** check box.
To access the dispatcher to the option that increases the call priority from normal to high before initiating their call (available only for Capacity Max networks),	select the ***Increase outgoing call priority (Capacity Max)*** check box.

6. To configure profile access to actions referred to requesting data from SmartPTT Radioserver, perform the following actions:

To allow viewing the SmartPTT Radioserver Event Log and requesting the history of events and data on the radio movement,	select the ***Request data from radioserver*** check box.
To allow viewing the SmartPTT Radioserver Event Log,	select the ***Event Log*** check box.
To allow requesting the history of events and data on the radio movement,	select the ***Reports and Movement reports*** check box.

7. To configure profile access to actions referred to monitoring, perform the following actions:

To allow monitoring in real time and building monitoring reports and coverage maps according to monitoring data,	select the ***Monitoring*** check box.
To allow air and equipment monitoring in real time,	select the ***Air monitoring*** check box.
To allow building monitoring reports and coverage maps according to monitoring data from SmartPTT Radioserver,	select the ***Monitoring reports and coverage map*** check box.

To configure profile access to specific actions in the radio network, perform the following actions:

To allow requesting radio location data once or multiple times,	select the ***Radio location request*** check box.
To allow remote radio monitoring,	select the ***Remote Monitor*** check box.

To allow blocking/unblocking radios from the dispatch console,	select the ***Block/Unblock radios*** check box.
To allow sending the Radio Kill command to radios (available only for Capacity Max networks),	select the ***Radio Kill (Capacity Max)*** check box.
To allow editing those cross patches which include talkgroups allowed to the client by the profile,	select the ***Cross patches management*** check box.
To allow the profile to edit cross patches, stop cross patches without waiting until current calls will be finished,	perform the following actions: 1. Expand the ***Cross patches management*** node. 2. Select the ***Immediate patch enable/disable*** check box.
To allow editing, activating, and deactivating temporary talkgroups (available only for Capacity Max networks),	select the ***Temporary talkgroups management (Capacity Max)*** check box.
To allow configuring the calls routing on SmartPTT Radioserver,	select the ***Bridging management*** check box.

9. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***. Changes will be applied immediately, without SmartPTT Radioserver restart.

Postrequisites:

- Create the client account and assign the desired profile to it. For details, see Managing Client Account Parameters.
- Add labels that determine mutual visibility of clients. For details, see Managing Client Labels.

5.5.3.3 Configuring Personalities

Follow the procedure to add, copy, delete, and configure a personality for the SmartPTT Mobile client profile. Personality allows you to assign a default contact for the SmartPTT Mobile PTT button and configure a list of groups to listen to.

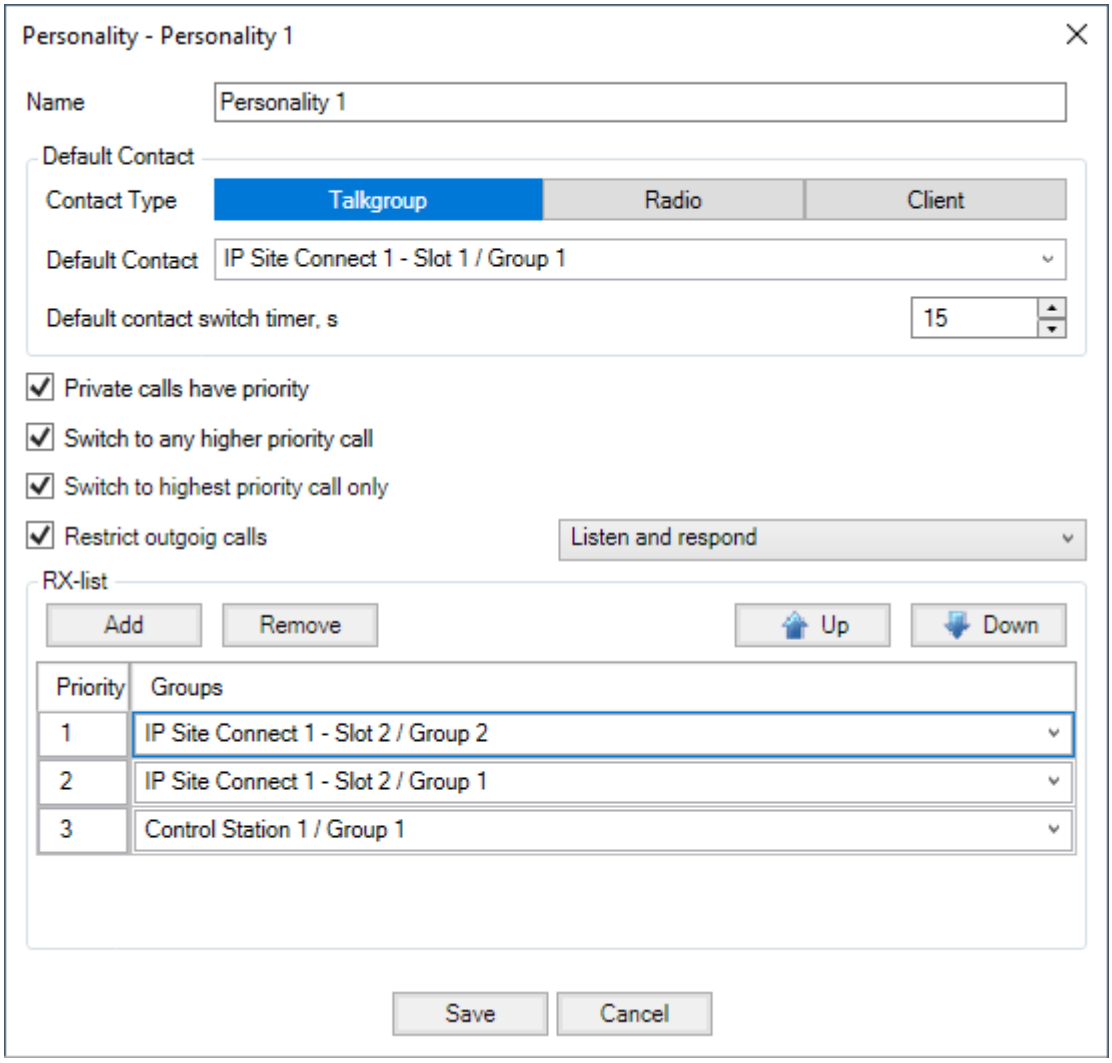
Prerequisites:

- Configure mobile client connection. For details, see Configuring SmartPTT Mobile Connection.
- Configure a profile to use with SmartPTT Mobile client accounts. For details, see Managing Client Account Parameters.
- Select networks and provide access to the virtual control station as well as talkgroups of the required networks on the ***Available Actions*** tab. For details, see Configuring Access to Networks.
- Configure client accounts that must be available for the personality to listen to. For details, see Client List.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Profiles*** tab.
2. In the left pane, click the desired profile.
3. In the right pane, open the ***Personalities (mobile only)*** tab.
4. On the tab, perform one of the following actions:

To add a new personality,	perform the following actions: 1. Click ***Add***. The ***Personality*** window appears. 2. Go to the next step.
To copy a personality,	perform the following actions: 1. Click a desired personality in the tree to select it. 2. Click ***Copy Personality***. 3. Go to the last step.
To delete a personality,	perform the following actions: 1. Click a desired personality in the tree to select it. 2. Click ***Delete***. 3. Go to the last step.
To edit personality settings,	perform the following actions: 1. Click the Edit button next to the desired personality name. The ***Personality*** window appears. 2. Go to the next step.



5. In the ***Name*** field, specify a unique personality name.
6. *(Optional)* In the ***Default Contact*** area, configure the contact that must be assigned to the PTT button in SmartPTT Mobile by default:

To select a talkgroup as contact type,	perform the following actions: 1. Next to ***Contact Type***, select ***Talkgroup***. 2. From the ***Default Contact*** menu, select one of the available talkgroups. 3. In the ***Default contact switch timer*** field, specify the amount of time after which PTT button must switch to the default contact after assigning another contact on it. The range of available values is from 1 to 60 seconds. The default value is *15*.
To select a radio as contact type,	perform the following actions: 1. Next to ***Contact Type***, select ***Radio***. 2. From the ***Default Contact*** menu, select the radio ID type.

	3. In the field next to the ***Default Contact*** menu, specify the radio ID. 4. In the ***Default contact switch timer*** field, specify the amount of time after which PTT button must switch to the default contact after assigning another contact on it.
To select a client as contact type,	perform the following actions: 1. Next to ***Contact Type***, select ***Client***. 2. From the ***Default Contact*** menu, select one of the available clients. 3. In the ***Default contact switch timer*** field, specify the amount of time after which PTT button must switch to the default contact after assigning another contact on it.

7. Configure priority of calls:

To increase the priority of private calls over group calls,	select the ***Private calls have priority*** check box.
To enable automatic switching to any higher-priority call from a call in which the user is participating,	select the ***Switch to any higher priority call*** check box.
To enable automatic switching to the highest priority call,	select the ***Switch to highest priority call only*** check box.

8. *(Optional)* Limit the ability to make outgoing calls:

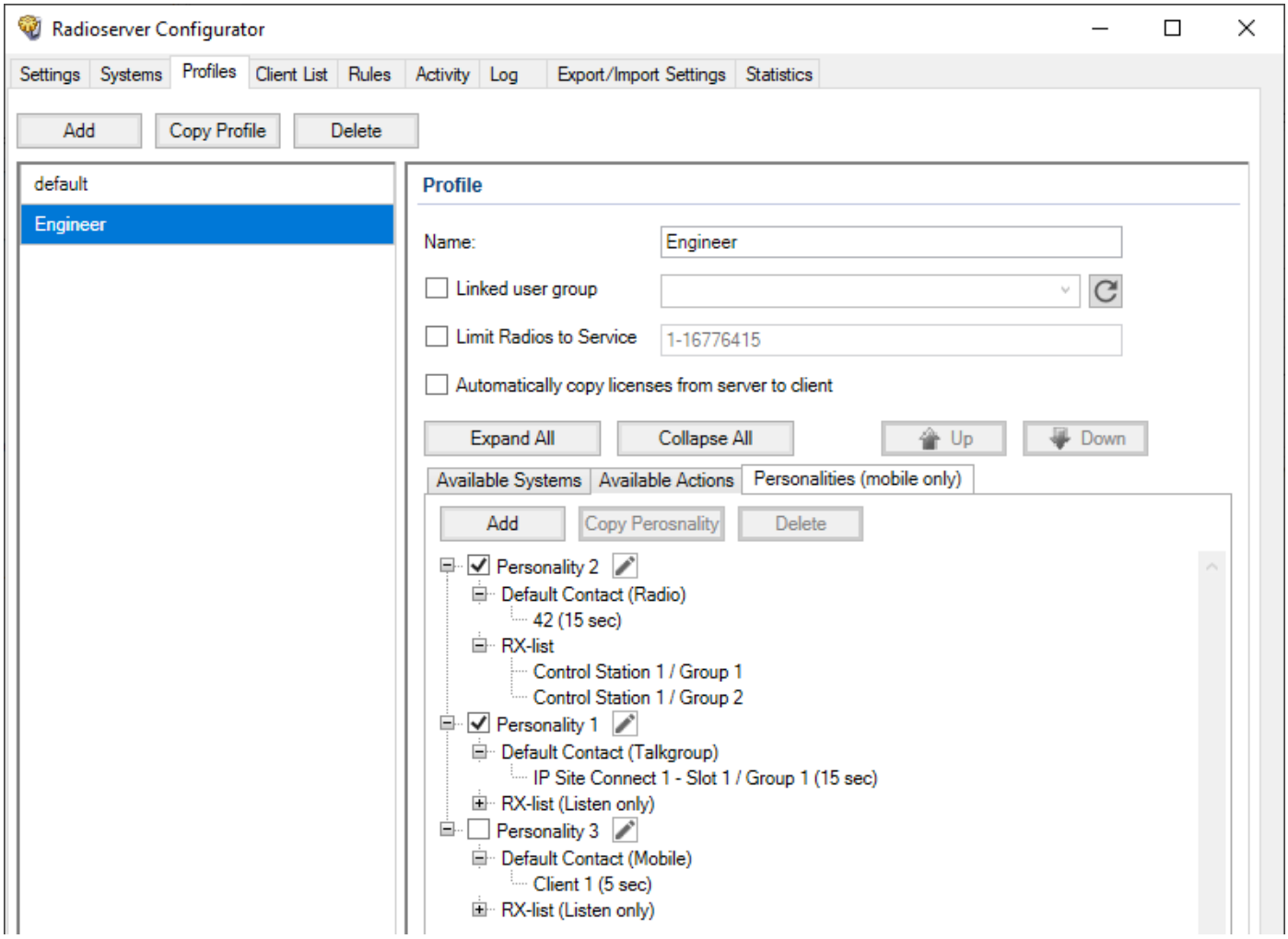
To allow the user to only receive incoming calls from groups and contacts,	perform the following actions: 1. Select the ***Restrict outgoing calls*** check box. 2. In the list on the right, select *Listen only*. The user is prohibited from making outgoing calls and responds during hangtime, except for calls and responds to the default contact.
To allow the user to receive incoming calls from groups and contacts and respond them during hangtime,	perform the following actions: 1. Select the ***Restrict outgoing calls*** check box. 2. In the list on the right, select *Listen and respond*. The user is prohibited from making outgoing calls, except for calls the default contact.

9. Configure the RX-list:

To add a group to the list,	perform the following actions: 1. Click ***Add***. The new entry appears.

	2. In the ***Groups*** column, from the list select the desired group.
To remove a group from the list,	click ***Remove***.
To configure the priority of the groups,	use ***Up*** and ***Down*** arrows, or specify the desired value manually in the ***Priority*** column.

9. Click ***Save***.



10. On the ***Personalities (mobile only)*** tab, select the check boxes of all desired personalities to make them available to the profile.
11. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***. Changes are applied immediately, without SmartPTT Radioserver restart.

Postrequisites:

Create the client account and assign the desired profile to it. For details, see Managing Client Account Parameters.

5.6 Managing Client Account Parameters

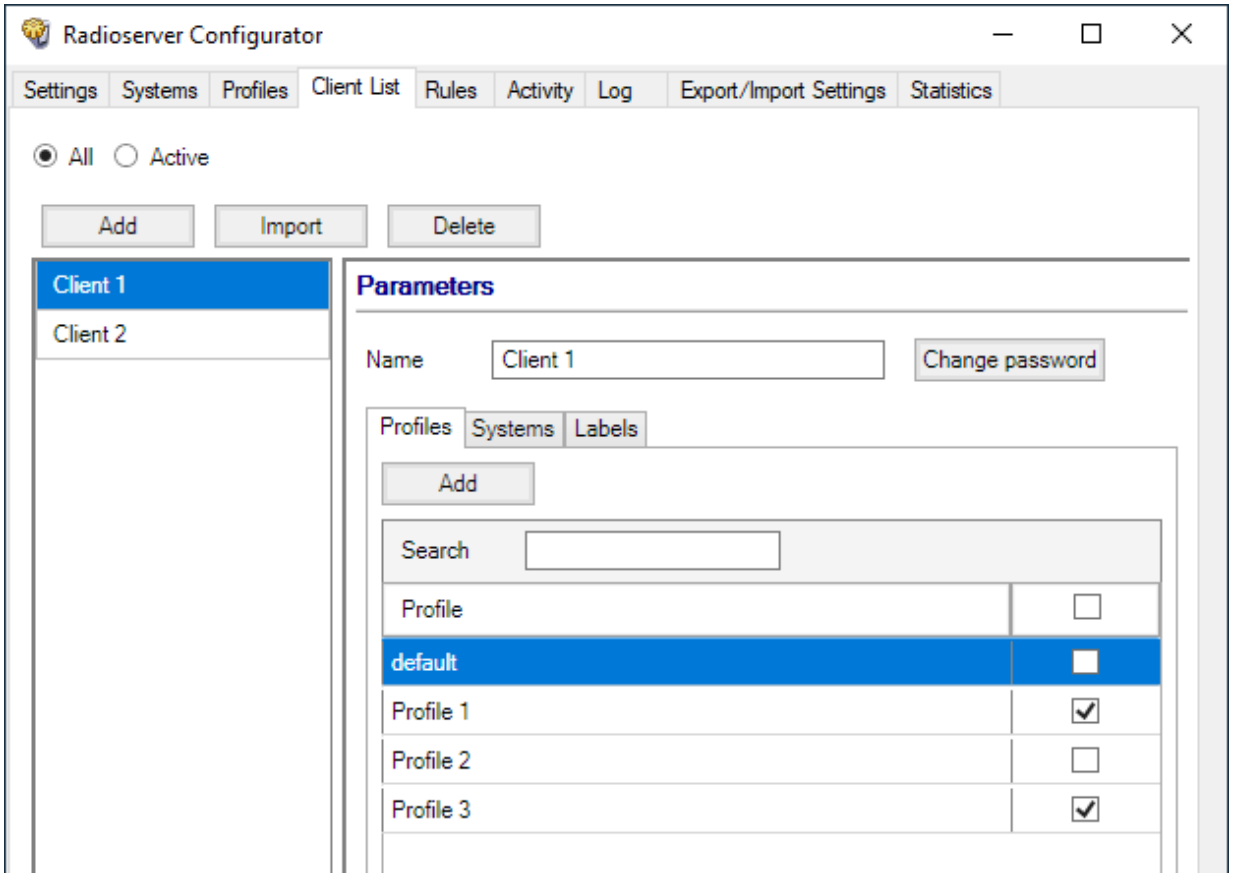
Follow the procedure to create a new or modify an existing client account used in SmartPTT Dispatcher, Web Client, SmartPTT Mobile, or third-party application.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- *(Optional)* Create and configure a profile for assigning to the client account. For details, see Managing Profiles.
- Determine radio ID to the client.
- Determine the unique dispatcher identifier.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Client List*** tab.
2. At the top of the ***Client List*** tab, click ***All***.

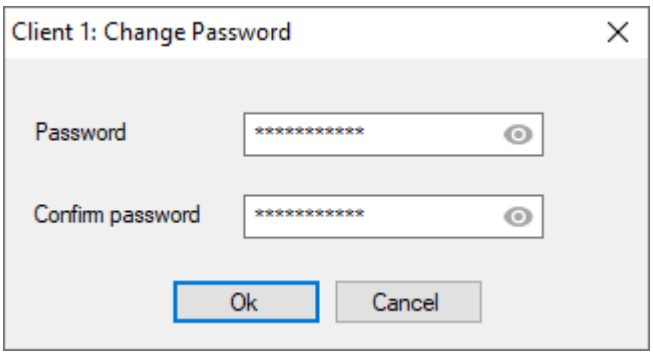


3. Perform one of the following actions:

To create a new client account,	click the ***Add*** button.
To edit an existing client account properties,	in the left pane, click the name of the desired client account.
To import a list of clients from a file,	perform the following actions: 1. Click the ***Import*** button.

	2. In the window that appears, select a file with CSV or XLSX extension.
To delete a client account,	perform the following actions: 1. In the left pane, click the name of the client account you want to delete. 2. Click the ***Delete*** button. 3. Proceed to the last step of the procedure.

4. In the ***Parameters*** pane, in the ***Name*** field, type the user name.
5. Set the user password:
   a. Next to the ***Name*** field, click ***Change password***.
   The dialog box for entering password appears.



   b. In the window that appears, in the ***Password*** field, type the password using 8 or more characters from at least three categories: uppercase and lowercase letters (A–Z, a–z), numbers (0–9), and special characters (!, $, #, %, etc.). To view the entered password, click the eye icon ( ).
   c. In the ***Confirm password*** field, type the password one more time.
   d. Click ***Ok*** to set the password and close the dialog box.
6. On the ***Profiles*** tab, in the last column, select check boxes for the profiles that must be available to the configured client. If you want to select all profiles in the list, then select the top check box in the last column.
   Default is a default profile that has no restrictions. All other profiles in the table must be configured first on the ***Profiles*** tab. For details, see Managing Profiles.

Important
You must assign at least one profile for each client otherwise client applications (SmartPTT Dispatcher, SmartPTT Web Client, SmartPTT Mobile) will not be able to connect to SmartPTT Radioserver and will display a connection error.

NOTE
If you assign multiple profiles to one client account, the operator can change their profiles in SmartPTT Dispatcher.

7. Open the ***Systems*** tab.
8. *(Optional)* In the table below, in the ***Unique ID*** column, set Radio ID to the client:
    a. If the client must connect to the network under a Radio ID different from the SmartPTT Radioserver identifier, select the check box into the ***Unique ID*** column next to the network name.
    b. In the ***ID*** column, type the identifier assigned to the client within the specified network. It must be unique within the specified network.
9. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***. Changes will be applied immediately, without restarting SmartPTT Radioserver.

Postrequisites:

Add labels that determine mutual visibility of clients. For details, see Managing Client Labels.

5.7 Client Labels

SmartPTT provides the ability to hide clients that use the same radioserver from each other.

When several groups of clients are working in the system, it may be necessary to isolate these groups from each other. It is convenient, if a large radio system is rented and users from different organizations are on the same radioserver. In such case, each group of tenants needs to create its own isolated space.

Labels are a tool used to determine which clients are visible to each other. Labels are assigned to clients on the ***Clients*** tab of SmartPTT Radioserver Configurator.
If a client has a common label with another client, then they will see each other in the system interface. If the client does not have common labels with other clients, then they will not receive any information about each other from SmartPTT Radioserver.

NOTE
An unlimited number of labels can be assigned to one client account.

Actions

To configure the rules for mutual visibility of clients on SmartPTT Radioserver, you must perform the following actions:

- Create client accounts on the ***Clients*** tab in SmartPTT Radioserver Configurator. For details, see Managing Client Account Parameters.
- Select client accounts for which you want to add labels.
- Create labels for clients on the ***Clients*** tab in SmartPTT Radioserver Configurator. For details, see Managing Client Labels.
- Assign labels to the desired client accounts.
- Connect to SmartPTT Radioserver using an account with labels assigned.

5.7.1 Managing Client Labels

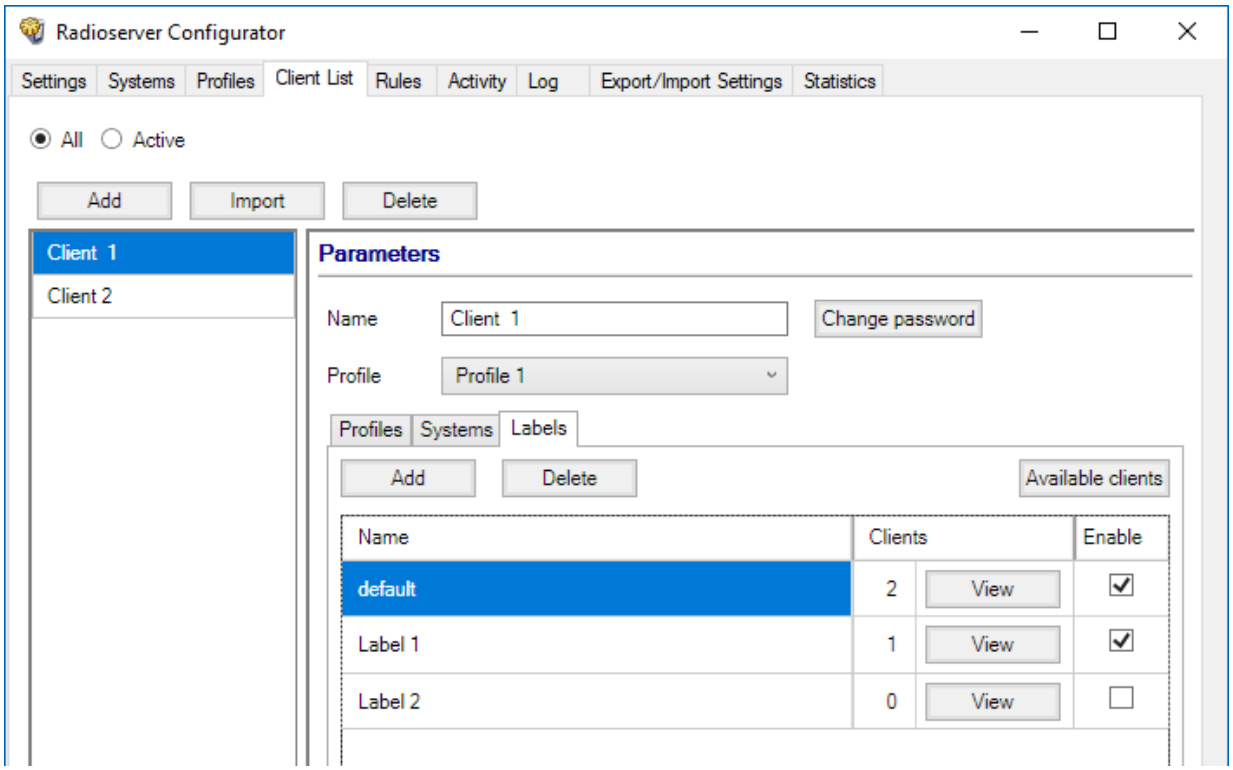
Follow the procedure to add labels that determine mutual visibility of clients, as well as delete the label or change its name.

Prerequisites:

- Create a new client account. For details, see Managing Client Account Parameters.
- *(Optional)* Create and configure a profile for assigning it to the client account. For details, see Managing Profiles.
- Determine clients to add common labels.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Client List*** tab.
2. At the top of the ***Client List*** tab, click ***All***.
3. In the ***Parameters*** pane, in the left part of SmartPTT Radioserver Configurator, open the ***Labels*** tab for the selected client.

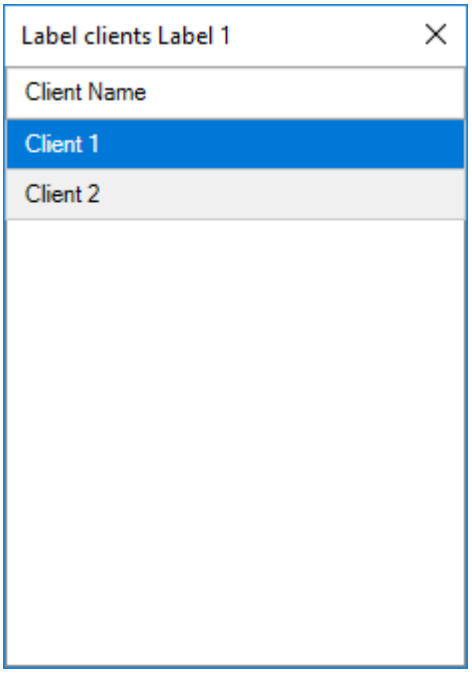


4. Perform one of the following actions:

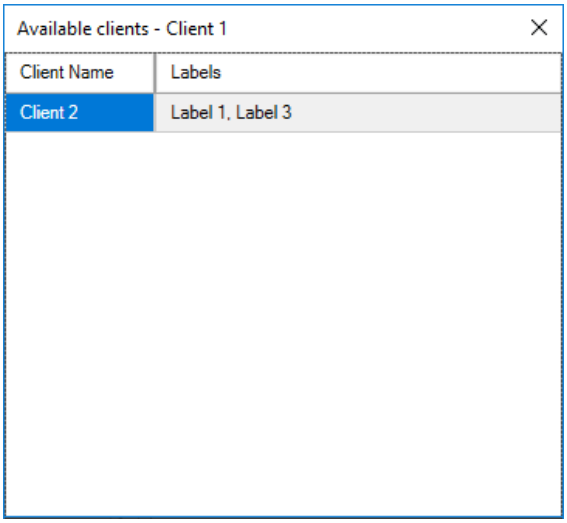
To add a new label,	click ***Add***.
To change the label name,	in the table below, double-click the entry with the name of the desired label.
To delete the label,	perform the following actions: 1. In the table, click the name of the label you want to delete. 2. Click ***Delete***. A confirmation window appears. Deleting a label is available even if the label is assigned to a client. 3. Proceed to the last step of the procedure.

5. To assign the label to the selected client, select the check box in the ***Enable*** column.
6. If required, perform the desired actions with the added labels:

To see clients to whom this label is added,	click the ***View*** button in the ***Clients*** column. The ***Label clients <Label Name>*** window appears.



To see with whom the client has common labels and whom the client can see,	click the ***Available clients*** button. The ***Available clients — <Client Name>*** window appears.



7. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (***  ***)***. Changes will be applied without restarting SmartPTT Radioserver.

6 MOTOTRBO Radio Systems

SmartPTT supports direct (wireline) connection to the following MOTOTRBO™ repeater systems:

- Single-site conventional systems. For details, see Single-Site MOTOTRBO Systems.
- IP Site Connect. For details, see IP Site Connect.
- Capacity Plus (Capacity Plus Single Site). For details, see Capacity Plus.
- Linked Capacity Plus (Capacity Plus Multi-Site). For details, see Linked Capacity Plus.
- Capacity Max. For details, see Capacity Max.
- Connect Plus. For details, see Connect Plus.

SmartPTT also supports control stations. For details, see MOTOTRBO Control Stations.

6.1 Single-Site MOTOTRBO Systems

Single-site systems are radio systems with single repeater. Such systems may operate in one of two modes:

Regular Mode

In this mode, radio channel is a duplex channel (receive and transmit radio frequencies are different). SmartPTT accesses such systems in the same way as it accesses IP Site Connect. For details, see IP Site Connect Configuration (NAI).

Extended Range Direct Mode (ERDM)

In this mode, radio channel is a simplex channel (receive and transmit frequencies are equal) with time-slots utilized as receive and transmit channels. SmartPTT accesses such systems over NAI. For details, see ERDM Systems.

To allow SmartPTT connection, repeater must have the IP Site Connect license installed. For details, contact Motorola Solutions representative in your region.

6.1.1 ERDM Systems

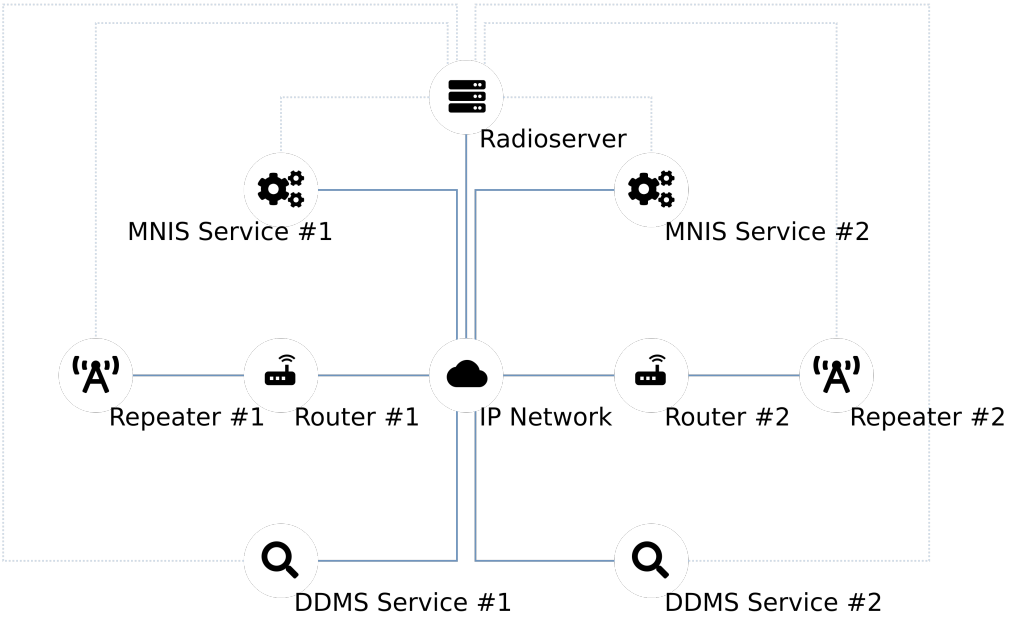
Extended Range Direct Mode (ERDM) is a special operation mode of a single-site digital (MOTOTRBO) radio system. Such systems are also known as Single Frequency Repeaters (SFR).

In ERDM, radio channel is configured as a simplex channel (receive and transmit frequencies are equal). At the same time, receive and transmit channels are assigned to DMR time slots. As a result, systems operate in the following way:

- Single radio frequency is used.
- First time slot is used to transmit information.
- Second time slot is used to receive information.

This mode provides the ability to save your expenses on radio frequency licensing. For other details, contact Motorola Solutions representative in your region.

SmartPTT is able to connect to multiple repeaters that operate in ERDM. As a result, it increases RF coverage area.



To access the repeater, SmartPTT uses Network Application Interface (NAI). The interface is provided by Motorola Solutions and its usage requires the following additional software:

- MOTOTRBO Network Interface Service (MNIS) provides data communication between the single-site system and SmartPTT.
- Device Discovery and Mobility Service (DDMS) provides ARS and (if configured) radio user information to SmartPTT.

Each repeater connection requires its own MNIS and DDMS.

Radioserver requires simultaneous connection to repeater, MNIS, and DDMS (see dotted lines on the diagram).

6.1.2 SmartPTT Features in ERDM

Repeater that operates in ERDM is able to provide the following features to SmartPTT:

- Radio registration information (ARS).
- Radio user identification.
- Voice call reception and initiation (includes group calls and private calls).
- Emergency alarms and calls.
- Radio location updates.
- Text messaging and job ticketing.
- Radio commands.
- Telemetry and remote control over radios.

Based on provided features, SmartPTT implements the following features:

- Simultaneous connection to multiple ERDM-operating repeaters.
- Integration with other radio systems using cross patches, bridging, and conference calls.

- Event logging and voice recording.
- Rules configuration.

For network monitoring, the following features are provided:

- IP devices monitoring over SNMP.
- Over-the-air traffic monitoring.
- Network topology visualization.

NOTE
SmartPTT does ***not*** show on-site/fielded radios on topology diagrams.

- Statistical information gathering (system performance, alarm statistics), reports generation.
- Open Voice Channel Mode (OVCM) calls.

6.1.3 ERDM Systems Configuration

SmartPTT connection to ERDM-operating repeater requires the following:

- Radio system compliance with the planning requirements.
- MNIS and DDMS configuration.
- Additional radio devices configuration.
- Dispatch software configuration.

Important
All of the following information (except SmarPTT configuration) is dedicated to the minimum configuration required to include dispatch software to the radio system. It is ***not*** sufficient for the whole system operation in ERDM. For more information and/or configuration assistance, contact Motorola Solutions representatives in your region.

Planning Requirements

To support SmartPTT connection, the radio system must comply with the following requirements:

- Repeater features must include the following items:
  - IP Site Connect.
  - Extended Range Direct Mode.
  - Voice over NAI.
  - Data over NAI.
- Repeater and all radios must have the same CAI IDs and CAI Group IDs.
- If radioserver, repeater, MNIS, and/or DDMS are in different networks controlled by different routers, corresponding routers must support Network Address Translation (NAT).
- Security key IDs and values must be known to people who will configure radios, MNIS, and radioserver.

Important
MOTOTRBO software and firmware do ***not*** provide tools to view the configured security/privacy key.

MNIS and DDMS Configuration

To configure MNIS and DDMS, the following actions must be performed:

- MNIS must have the following IDs:
  - Free Radio ID
  - Free Repeater Radio ID
- MNIS must be connected to the ERDM-operating repeater over IP.
- Security keys that are configured in radio codeplugs must be configured in MNIS.
- MNIS must be connected to DDMS.

Additional Radio Devices Configuration

To configure radio devices to operate together with SmartPTT in ERDM-operating systems, the following actions must be performed:

- For all radios, MNIS Radio IDs must be used as ARS ID.
- To update the location when the radio sends telemetry data, ensure that the ***GNSS Report*** check box is selected for the desired GPIO physical pins in the radio codeplugs.
- All routers must be configured to translate the following addresses:
  - Repeater
  - Radioserver
  - MNIS service
  - DDMS service

SmartPTT Configuration

To configure SmartPTT, the following actions must be performed:

- SmartPTT license with data exchange and/or voice calls in conventional (IPSC) systems permission must be installed. For details, see Installing License.
- Repeater connection must be configured. For details, see Adding and Editing ERDM System Configuration.
- Radioserver identification must be performed. For details, see Configuring SmartPTT Identification in ERDM.
- Talkgroups and All Calls must be configured. For details, see Adding and Editing Groups in ERDM.
- Security keys must be configured in SmartPTT. For details, see Configuring Encryption in ERDM.
- SmartPTT must be connected to DDMS. For details, see Configuring DDMS Connection.
- SmartPTT must be connected to MNIS. For details, see Configuring MNIS Connection.

If you need assistance in the SmartPTT configuration, submit a request to SmartPTT Technical Support Center.

6.1.3.1 Adding and Editing ERDM System Configuration

Follow the procedure to add a new or edit an existing connection to the radio system.

Prerequisites:

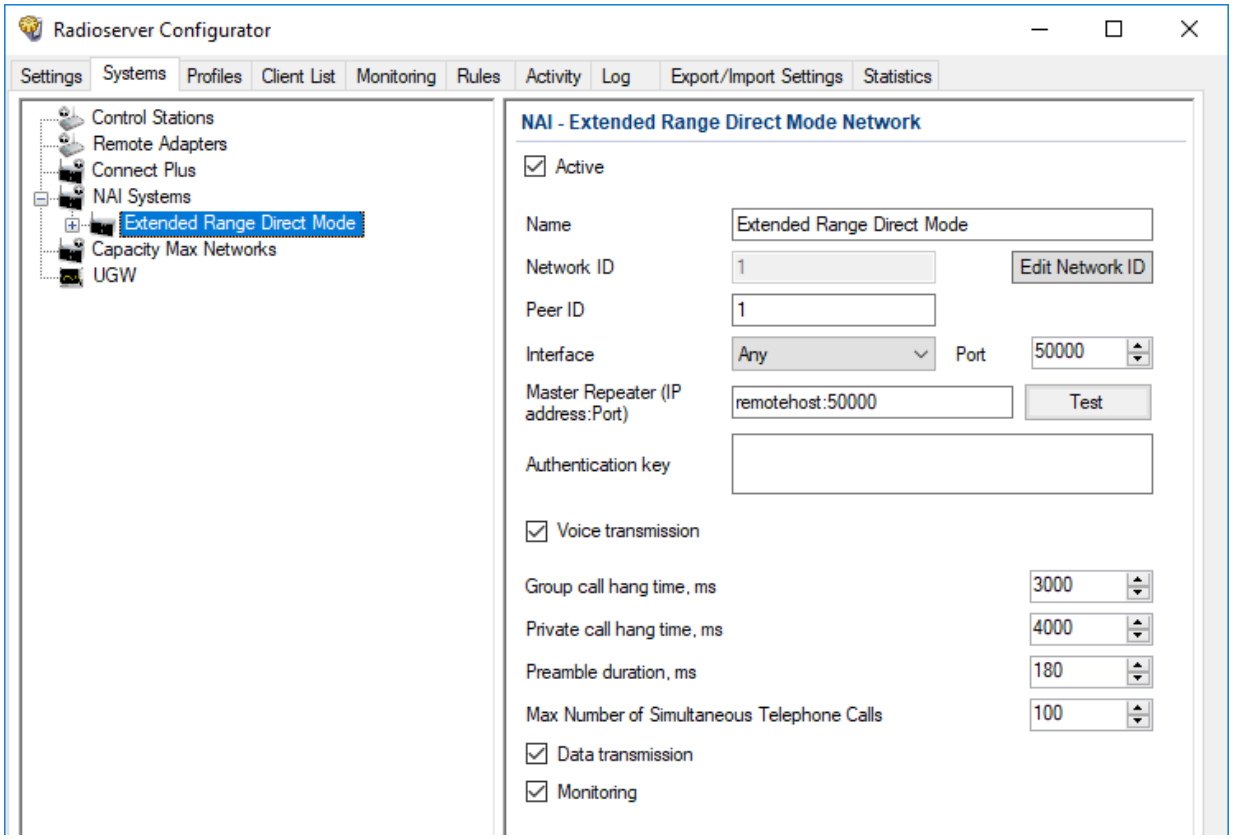
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure that SmartPTT license allows data exchange and/or voice calls in conventional (IPSC) systems.
- From the repeater codeplug, obtain the following data:
  - Repeater IP address and UDP port number.
  - Repeater private authentication key.
- From radio codeplugs, obtain the following data:
  - Hangtime duration for group and private calls.
  - Duration of the voice transmission delay (preamble).
- If the repeater and radioserver are in different networks controlled by different routers over the router that supports Network Address Translation (NAT), obtain the IP address and UDP port that will be translated to the master repeater IP address and UDP port number.
- *(Optional)* Turn on SmartPTT monitoring. For details, see Configuring Monitoring Database Connection..

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, perform one of the following actions:

To add a new network,	right-click the ***NAI Systems*** node, point to ***Add***, and then select ***NAI - Extended Range Direct Mode***.
To modify an existing network,	expand the ***NAI Systems*** node, and then click ***<network name>***.

The connection settings appear in the right pane of the tab.



3. In the right pane, configure the general connection settings:
   a. Select the ***Active*** check box.
   b. In the ***Name*** field, type the radio system name.
   c. Leave the value in the ***Network ID*** field unchanged.
4. Configure the repeater connection:
   a. In the ***Peer ID*** field, type the ID of the virtual repeater reserved for a radioserver.
   b. From the ***Interface*** list, select one of the following options:

To use any of the radioserver host IP addresses (except 127.0.0.1),	select *Any*.
To fix the IP address,	select the desired IP address.

Important
If a radioserver and MNIS are installed on the same computer, use fixed IP address that is different from the MNIS Tunnel IP address (by default, *192.168.56.1*).

Important
If a radio or control station is connected to the computer, use fixed IP address that is different from the radio or control station IP address (by default, *192.168.10.1*).

c. In the ***Port*** field, enter the radioserver host port that will be used to connect to the repeater.

d. In the ***Master Repeater (IP address:Port)*** field, type the IP address and UDP port that a radioserver will use to connect to the repeater (includes the potential NAT use). Input format is <IP address in dot-decimal notation>:<UDP port>.

e. In the ***Authentication key*** field, type the repeater private authentication key. To view the entered key, click the eye icon ( ). For security reasons, the key will not be available for viewing in subsequent sessions.

f. *(Optional)* Click ***Test*** to check the connection.

5. Configure voice call parameters in the radio system:

   a. Select the ***Voice transmission*** check box to allow voice reception and transmission for SmartPTT.

   b. In the ***Group call hang time, ms*** field, enter the hangtime duration (in milliseconds) for group calls.

   c. In the ***Private call hang time, ms*** field, enter the hangtime duration (in milliseconds) for private calls.

6. In the ***Preamble duration, ms*** field, enter the transmission start delay (in milliseconds).
7. Leave the value in the ***Max Number of Simultaneous Telephone Calls*** field unchanged.
8. Select the ***Data transmission*** check box to turn on data exchange between a radioserver, MNIS, and DDMS.
9. *(Optional)* Select the ***Monitoring*** check box to turn on the radio system devices diagnostics.
10. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Identify a radioserver in the system. For details, see Configuring SmartPTT Identification in ERDM.
- Configure talkgroups and All Call in the network. For details, see Adding and Editing Groups in ERDM.
- Configure security keys. For details, see Configuring Encryption in ERDM.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- In the firewall software on the computer, unlock the specified UDP port. For details, see Radioserver Host.
- *(Optional)* Configure network device monitoring. For details, see Network Monitoring..

6.1.3.2 Configuring SmartPTT Identification in ERDM

Follow the procedure to configure SmartPTT identification in the radio network.

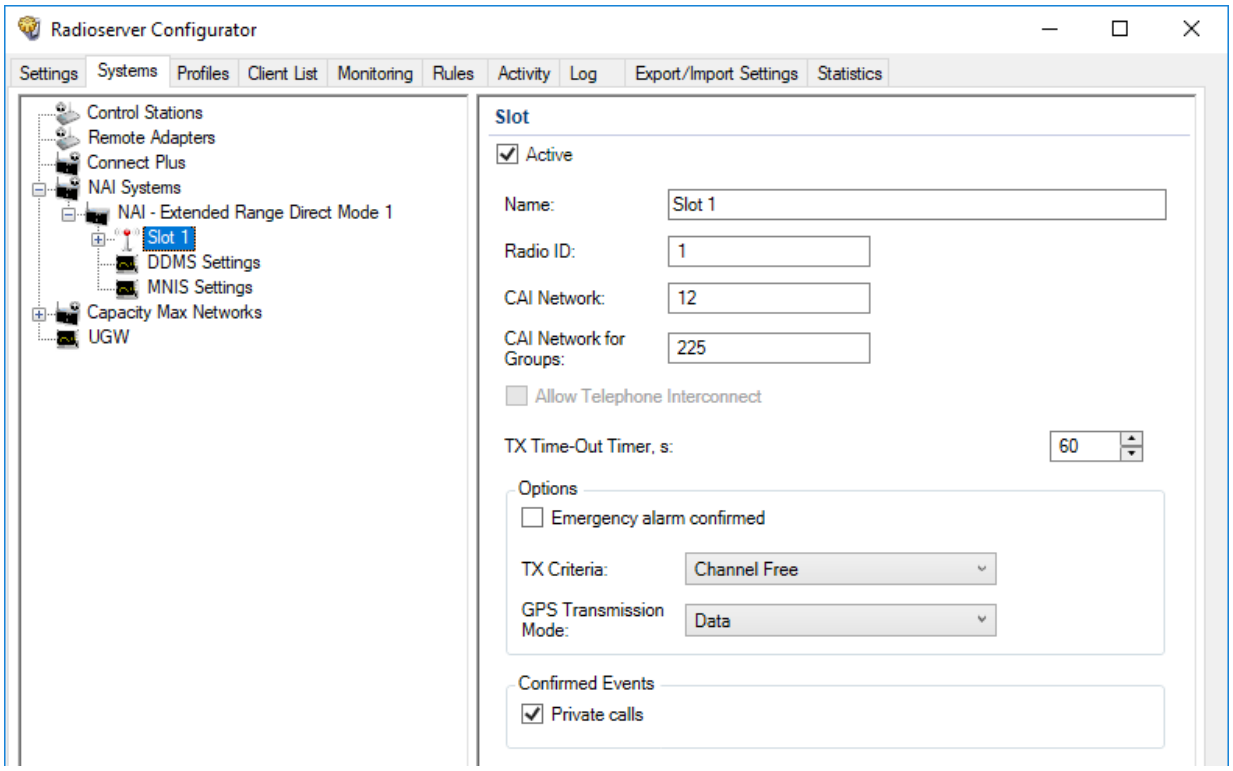
Prerequisites:

- Add and configure SmartPTT connection to the ERDM repeater. For details, see Adding and Editing ERDM System Configuration.
- Determine the radioserver ID as a virtual radio.

- From radio codeplugs, obtain the following data:
  - CAI and CAI group values.
  - Voice transmission duration.
  - CSBK data settings (active or inactive).
- From the MNIS configuration file, obtain information on the repeater location (configured or not).
- Determine the necessity for the following radioserver functions:
  - Radio system integration with phone systems.
  - Emergency alarms and calls acknowledgment.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***NAI Systems*** → ***<system name>***, and then click ***<slot name>***.
   The identification parameters appear in the right pane of the tab.



3. In the right pane, select the ***Active*** check box.
4. In the ***Name*** field, type the title that will represent the radio network in SmartPTT Dispatcher.
5. Type the radioserver identification parameters:
   a. In the ***Radio ID*** field, type the identifier of the radioserver as a virtual radio.

Important
Do not assign this ID to a client or radio in any radio network.

   b. In the ***CAI Network*** field, type the CAI ID.
   c. In the ***CAI Network for Groups*** field, type the CAI Group ID.

6. In the ***TX Time-Out Timer, s*** field, enter the maximum duration (in seconds) of voice transmissions in the radio network.
7. In the ***Options*** area, select the ***Emergency alarm confirmed*** check box to enable emergency confirmation by SmartPTT Radioserver.
8. From the ***TX Criteria*** list, select one of the following options:

If the call initiator must transmit only when no other transmissions is detected over the radio channel,	select *Channel Free*.
If the call initiator must interrupt another participant of the radio network according to the selected MSI or DMR protocol,	select *Tx Interrupt*.
If the call initiator must completely ignore other transmissions over the radio channel,	select *Always*.

9. From the ***GPS Transmission Mode*** list, select one of the following options:

If CSBK data is used in the radio system but site coordinates are ***not*** configured in MNIS,	select *CSBK*.
In CSBK data is ***not*** used in the radio system or outdoor location service is used together with indoor positioning service,	select *Data*.

10. In the ***Confirmed Events*** area, select the ***Private calls*** check box to support private call request confirmation.
11. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

6.1.3.3 Adding and Editing Groups in ERDM

Follow the procedure to add or edit talkgroups or All Call in the radio system.

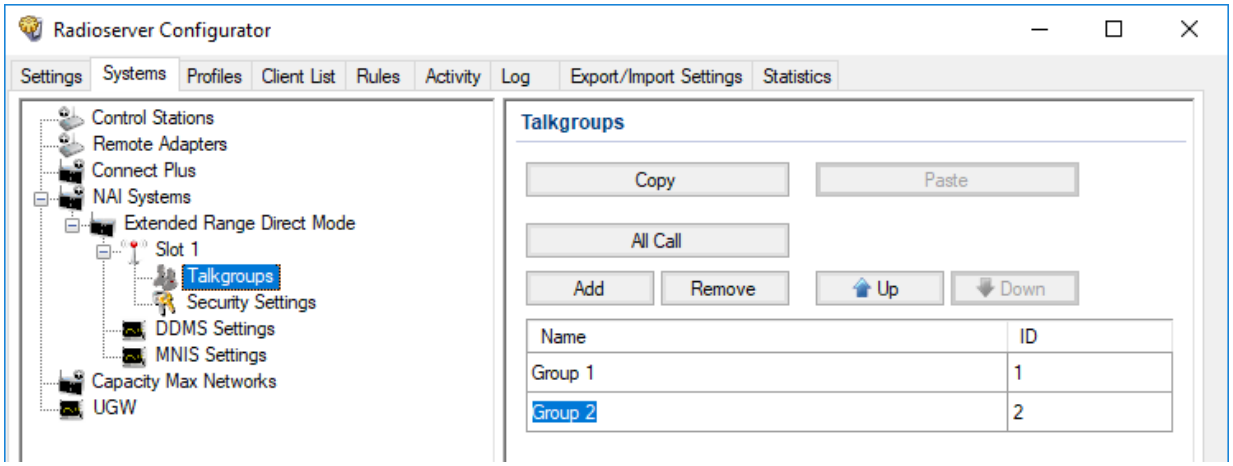
Prerequisites:

- Add and configure SmartPTT connection to the ERDM repeater. For details, see Adding and Editing ERDM System Configuration.
- From radio codeplugs, obtain the list of talkgroup IDs.
- If SmartPTT license allows voice calls in conventional (IPSC) systems, determine the All Call necessity. For details, see Viewing License Items.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.

2. In the left pane, expand ***NAI Systems*** → ***<system name>*** → ***<slot name>***, and then click ***Talkgroups***.
   The list of talkgroups appear in the right pane.



3. In the right pane, perform one of the following actions:

To add a new talkgroup,	click ***Add***.
To add All Call,	click ***All Call***.
To edit an existing talkgroup or All Call,	proceed to the next step of the procedure.

4. In the desired table entry, perform the following actions:
   a. In the ***ID*** column (if appears), double-click the current ID, and then type the desired talkgroup ID.
   b. In the same entry, in the ***Name*** column, double-click the current name, and then type the desired name.

Important
The group ID must be unique across all slots of NAI systems.

NOTE
SmartPTT Radioserver Configurator does not show the All Call ID.

5. *(Optional)* Using ***Up*** and ***Down*** buttons, reorder rows in the table.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (*** ***)***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (*** ***)*** or ***Restart (*** ***)***.

6.1.3.4 Configuring Encryption in ERDM

Follow the procedure to support voice transmissions decryption and encryption in SmartPTT.

Prerequisites:

- Ensure that SmartPTT license allows the following features:
  - Voice calls in conventional (IPSC) systems.
  - *(Optional)* AES-compliant security keys.

  For details, see Viewing License Items.

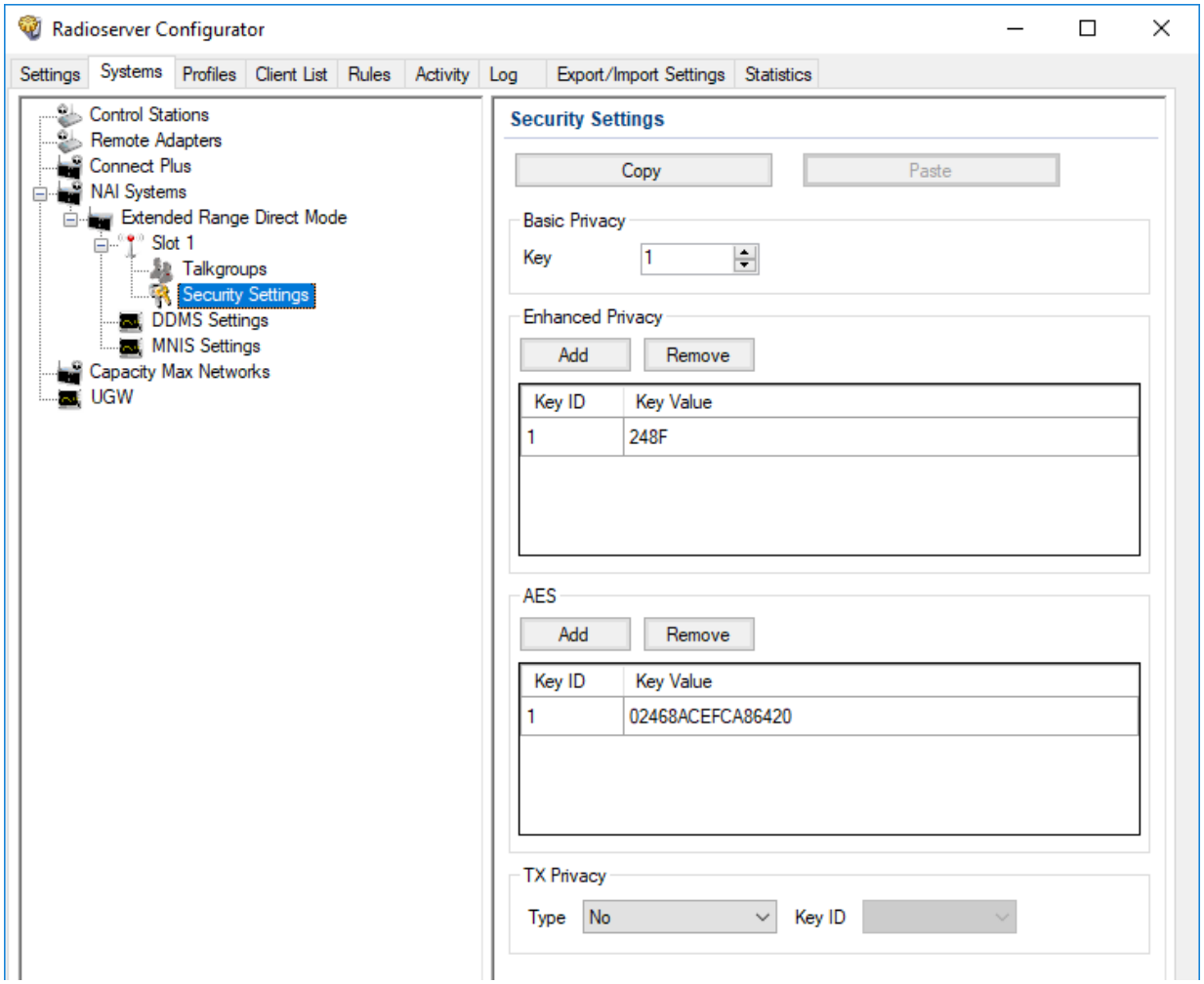
- Obtain security key IDs and values for all encryption types used in the radio system.

Important
MOTOTRBO configuration tools do not show the configured security/privacy keys for security reasons.

- Determine the key that will be used to encode dispatcher transmissions.
- Add and configure SmartPTT connection to the ERDM repeater. For details, see Adding and Editing ERDM System Configuration.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***NAI Systems*** → ***<system name>*** → ***<slot name>***, and then select ***Security Settings***.
   The security key settings appear in the right pane.



3. In the right pane, in the ***Basic Privacy*** area, perform the following actions:

If basic encryption is used in the radio system,	in the ***Key*** field, enter the value of the basic security key.
If basic encryption is ***not*** used in the radio system,	leave the value in the ***Key*** field unchanged.

4. Add a new security key to the dispatch subsystem:

To add a new enhanced key,	perform the following actions: 1. In the ***Enhanced Privacy*** area, click ***Add***. 2. In a new row of the table, in the ***Key ID*** column, double-click the current ID, and then type the desired ID. 3. In the same row, in the ***Key Value*** column, double-click the current value, and then type the desired value.
To add a new symmetric (AES-compliant) key,	perform the following actions: 1. In the ***AES*** area, click ***Add***. 2. In a new row of the table, in the ***Key ID*** column, double-click the current ID, and then type the desired ID. 3. In the same row, in the ***Key Value*** column, double-click the current value, and then type the desired value.

5. *(Optional)* Modify an existing security key:

To edit a basic security key,	in the ***Basic Privacy*** area, in the ***Key*** field, enter the desired basic security key.
To modify an existing enhanced security key,	perform the following actions: 1. In the ***Enhanced Privacy*** area, in a desired row of the table, in the ***Key ID*** column, double-click the current ID, and then type the desired ID. 2. In the same row, in the ***Key Value*** column, double-click the current value, and then type the desired value.
To modify an existing symmetric (AES-compliant) key,	perform the following actions: 1. In the ***AES*** area, in a desired row of the table, in the ***Key ID*** column, double-click the current ID, and then type the desired ID. 2. In the same row, in the ***Key Value*** column, double-click the current value, and then type the desired value.

6. Configure outgoing transmission encryption (from dispatchers to the radio network):

To use a basic security key,	from the ***Type*** list, select *Basic*.
To use one of enhanced security keys,	perform the following actions: 1. From the ***Type*** list, select *Enhanced*. 2. From the ***Key ID*** list, select the ID of the desired key.

To use one of symmetric (AES-compliant) security keys,	perform the following actions: 1. From the ***Type*** list, select *AES (Symmetric Key)*. 2. From the ***Key ID*** list, select the ID of the desired key.
To perform unencrypted (clear) transmissions,	from the ***Type*** list, select *No*.

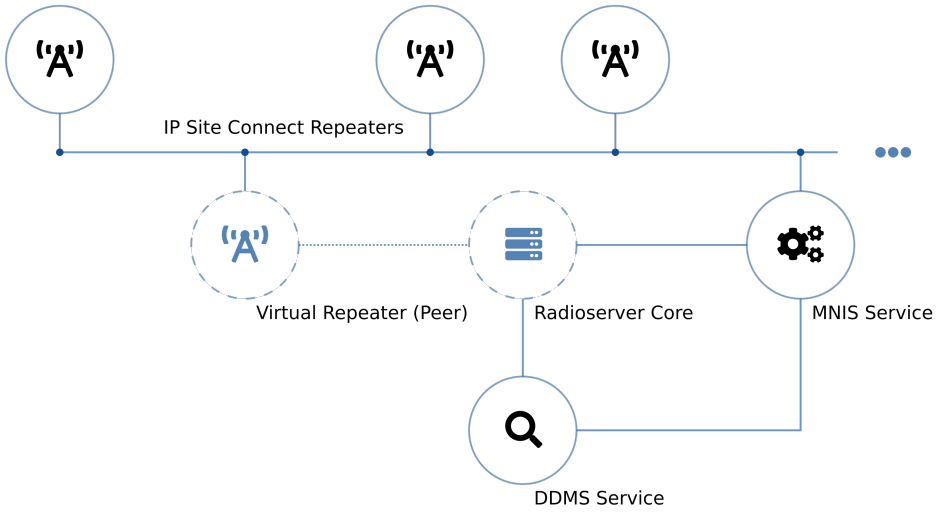
7. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- Duplicate security keys for other slots of the system. For details, see Settings Duplication.

6.2 IP Site Connect

MOTOTRBO™ IP Site Connect is a digital conventional radio system that is compliant with DMR Tier II standards. The system provides two logical channels over the single duplex channel (using the TDMA technology) and a great RF coverage zone (up to 15 sites per system). For details, see MOTOTRBO™ IP Site Connect on the Motorola Solutions website.



SmartPTT is able to connect to multiple IP Site Connect radio systems at once. This (alongside other features) allows to increase the system RF coverage by configuring SmartPTT bridging.

SmartPTT connects to IP Site Connect using Netowrk Application Interface (NAI). It is a dedicated interface provided by Motorola Solutions that includes the following additional software:

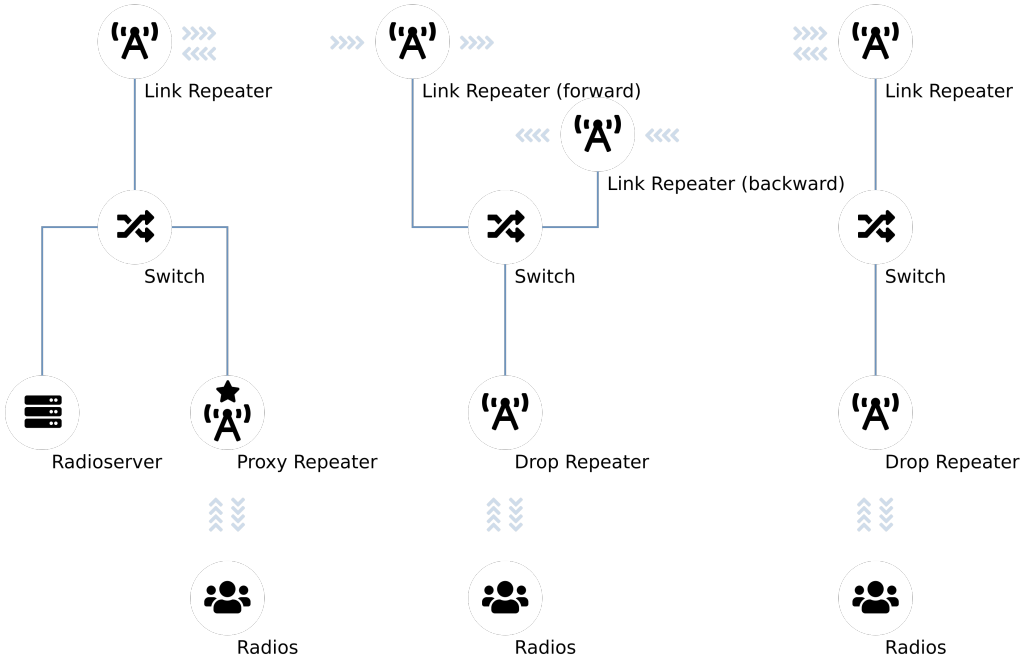
- MOTOTRBO Network Interface Service (MNIS) provides data communication between the radio system and SmartPTT.
- Device Discovery and Mobility Service (DDMS) provides ARS information to SmartPTT.

To connect to IP Site Connect, SmartPTT must allow at least one of the following features:

- Voice and radio commands (includes emergency alarms and calls).
- Data exchange.

6.2.1 Link Mode in IP Site Connect

A MOTOTRBO Link system is an IP Site Connect modification where at least two sites have a wireless IP connection. The connection is provided by additional repeaters installed to those sites.



MOTOTRBO Link systems are necessary if no wireline network equipment can be mounted on the site. For more information, contact Motorola Solutions representative in your region.

In the systems, the following terms are used:

- Origin site is the first site of the MOTOTRBO Link repeater chain.
- Terminating site is the last site of the MOTOTRBO Link repeater chain.
- Drop repeater provides voice and data communication for on-site radios.
- Link repeater provides the inter-site communication.
- Proxy repeater is a drop repeater that provides SmartPTT connection to IP Site Connect.

To use SmartPTT in MOTOTRBO Link systems, the following requirements must be followed:

- Radio system must have the single MOTOTRBO Link repeater chain.
- Proxy repeater must be in the origin or terminating site of that chain.
- Proxy repeater must be the master repeater of the system.

6.2.2 SmartPTT Features in IP Site Connect

IP Site Connect provides the following features to SmartPTT:

- Information on radio presence in the network (ARS).
- Voice call reception and initiation (includes group calls and private calls).
- Emergency alarms and calls.

- Radio location updates (includes revert channel support).
- Text messages and job tickets.
- Radio commands.
- Telemetry and remote control over radios.

SmartPTT provides the following features for IP Site Connect users:

- Simultaneous access to multiple systems.
- Connecting multiple IP Site Connect networks to one MNIS service.
- Wide and Local Area Channel support.
- Integration with other radio systems using cross patches, bridging, and conference calls.
- Telephone interconnect over SIP trunk.
- Event logging and voice recording.
- Per-console and system-wide rules.
- Availability for Web Client users, SmartPTT Mobile users, and API-applications.

For network monitoring purposes, the following features are available:

- Network device monitoring over SNMP.
- Logical and physical channel monitoring (also referred to as “air monitoring”).
- Radio network topology visualization.

NOTE
SmartPTT does ***not*** show on-site/fielded radios on topology diagrams.

- Statistical information gathering (system performance, alarm statistics), reports generation.
- Open Voice Channel Mode (OVCM) calls.

6.2.3 IP Site Connect Configuration

Connection to IP Site Connect requires additional radio devices configuration, MNIS configuration, DDMS configuration, and dispatch software configuration.

Radio Devices Configuration

To support SmartPTT connection, the following actions must be performed:

- Radio IDs must be reserved for the following needs:
  - Dispatch subsystem (SmartPTT) identification.
  - MNIS identification.
  - *(Optional)* Individual dispatcher (operator) identification.
- To update the location when the radio sends telemetry data, the ***GNSS Report*** check box must be selected for the desired GPIO physical pins in the radio codeplugs.

- Peer IDs (Repeater Radio ID) must be reserved for the following needs:
  - SmartPTT identification as a software peer.
  - MNIS identification.
- MNIS Radio ID must be configured as the ARS ID in all radio codeplugs.
- MNIS Radio ID must be configured as the TMS ID in all radio codeplugs.
- All radios and repeaters must have the same CAI IDs and CAI Group IDs.
- IP address and UDP port of the master repeater must be obtained.
- *(Optional)* Repeater Peer IDs must be obtained to create local slots in SmartPTT.
- Security keys must be obtained from radio codeplugs.

If you need assistance in the MOTOTRBO devices configuration, contact Motorola Solutions representatives in your region.

MNIS and DDMS Configuration

To configure MNIS and DDMS, the following actions must be performed:

- Dedicated IDs (Radio ID and Peer ID) must be assigned to MNIS.
- MNIS must be connected to the IP Site Connect master repeater.
- *(Optional)* Repeater/RF site coordinates (latitude and longitude) must be configured in MNIS to increase the rate of radio location updates.
- Security keys must be configured in MNIS.
- DDMS address must be configured in MNIS.
- ARS ports must be synchronized in MNIS and DDMS.

If you need assistance in the MOTOTRBO software configuration, contact Motorola Solutions representatives in your region.

SmartPTT Configuration

To configure SmartPTT to work in IP Site Connect, the following actions must be performed:

- Connection to the master repeater must be configured. For details, see Adding and Editing IP Site Connect.
- *(Optional)* If necessary, local slots must be added. For details, see Adding and Editing Local Slots.
- SmartPTT Radioserver must be identified on both logical channels (time slots) of the system and local slots (if added). For details, see Configuring SmartPTT Identification.
- Talkgroups and All Calls must be configured for all logical channels (time slots) and local slots. For details, see Adding and Editing Talkgroups in IPSC.
- Security keys must be configured in SmartPTT. For details, see Configuring Encryption in IPSC.
- SmartPTT must be connected to the DDMS service. For details, see Configuring DDMS Connection.
- SmartPTT must be connected to the MNIS service. For details, see Configuring MNIS Connection.

If you need assistance in the SmartPTT configuration, submit a request to SmartPTT Technical Support Center.

Network Monitoring

For network monitoring configuration in SmartPTT, the following actions must be performed:

- IP addresses of all repeaters in the system must be obtained.
- IP addresses of all other network devices must be obtained. This includes uninterruptible power supplies (UPS), switches, routers, etc.

For information on network monitoring configuration, see Network Monitoring.

6.2.3.1 Configuring Connection to IP Site Connect

Follow the procedure to add or edit connection to IP Site Connect..

Prerequisites:

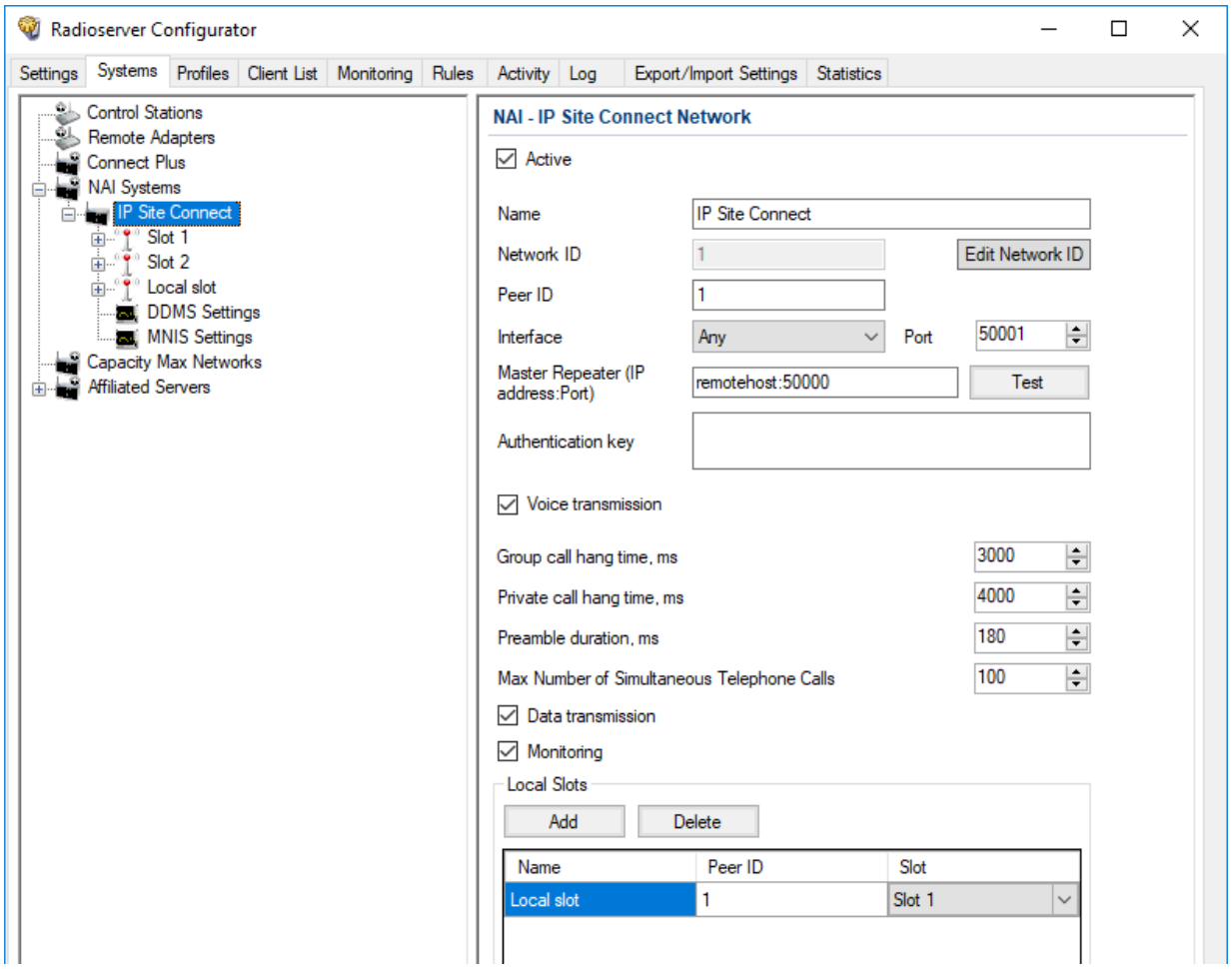
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure that SmartPTT has the license for voice and data exchange in the network. For details, see Viewing License Items.
- From codeplugs of repeaters, obtain the following data:
  - IP address and UDP port of a master repeater.
  - Repeater private authentication key.
- If the repeater and radioserver are in different networks controlled by different routers over the router that supports Network Address Translation (NAT), obtain the IP address and UDP port that will be translated to the master repeater IP address and UDP port number.
- From radio codeplugs, obtain the following data:
  - Duration of the voice transmission delay (preamble duration).
  - Duration of the group and private call hangtime.
- Determine the maximum number of voice calls between the radio system and the phone system.
- *(Optional)* Turn on SmartPTT monitoring. For details, see Configuring Monitoring Database Connection.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, perform one of the following actions:

To add a new network,	right-click the ***NAI Systems*** node, point to ***Add***, and then select ***NAI - IP Site Connect***.
To edit an existing network,	expand the ***NAI Systems***, and then click the desired network.

In the right pane, the connection settings appear.



3. Select the ***Active*** check box to unlock the settings.
4. In the ***Name*** field, type the network name.
5. Leave the value in the ***Network ID*** field unchanged.
6. In the ***Peer ID*** field, type a unique SmartPTT Radioserver identifier as a virtual repeater (Repeater Radio ID).
7. From the ***Interface*** list, select the SmartPTT Radioserver IP address to connect to the master repeater:

To provide SmartPTT Radioserver ability to select IP address,	select *Any*.
To use specific IP address,	select the desired IP address from the list.

Important
If SmartPTT Radioserver and MNIS are installed on the same computer, use a fixed IP address that is different from the MNIS Tunnel IP address (by default, *192.168.56.1*).

Important
If a radio or control station is connected to the computer, use a fixed IP address that is different from the radio or control station IP address (by default, *192.168.10.1*).

8. In the ***Port*** field, enter the radioserver port number that is used for repeater connection.
9. In the ***Master Repeater (IP address:Port)*** field, type master repeater IP address and port.

10. In the ***Authentication Key*** field, type the repeater private authentication key. To view the entered key, click the eye icon ( ). For security reasons, the key will not be available for viewing in subsequent sessions.
11. *(Optional)* Click ***Test*** to check the connection between the radioserver and master repeater.
12. Configure voice call parameters in the radio system:
    a. Select the ***Voice transmission*** check box to allow voice reception and transmission for SmartPTT.
    b. In the ***Group call hang time, ms*** field, enter the hangtime duration (in milliseconds) for group calls.
    c. In the ***Private call hang time, ms*** field, enter the hangtime duration (in milliseconds) for private calls.
    d. In the ***Preamble duration, ms*** field, enter the transmission start delay (in milliseconds).
    e. In the ***Max Number of Simultaneous Telephone Calls*** field, enter the maximum number of voice calls between radio system and phone system.
13. Select the ***Data transmission*** check box to allow SmartPTT data exchange with MNIS and DDMS services.
14. *(Optional)* Select the ***Monitoring*** check box to turn on the radio system device diagnostics.
15. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Identify radioserver in the system. For details, see Configuring SmartPTT Identification.
- *(Optional)* Configure local slots. For details, see Adding and Editing Local Slots.
- Configure talkgroups and All Call in the network. For details, see Adding and Editing Talkgroups in IPSC.
- Configure security keys. For details, see Configuring Encryption in IPSC.
- If data transmission is allowed, configure DDMS service. For details, see Configuring DDMS Connection.
- If data transmission is allowed, configure MNIS service. For details, see Configuring MNIS Connection.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- In the firewall software on the computer, unlock the specified UDP port. For details, see Radioserver Host.

6.2.3.2 Adding and Editing Local Slots

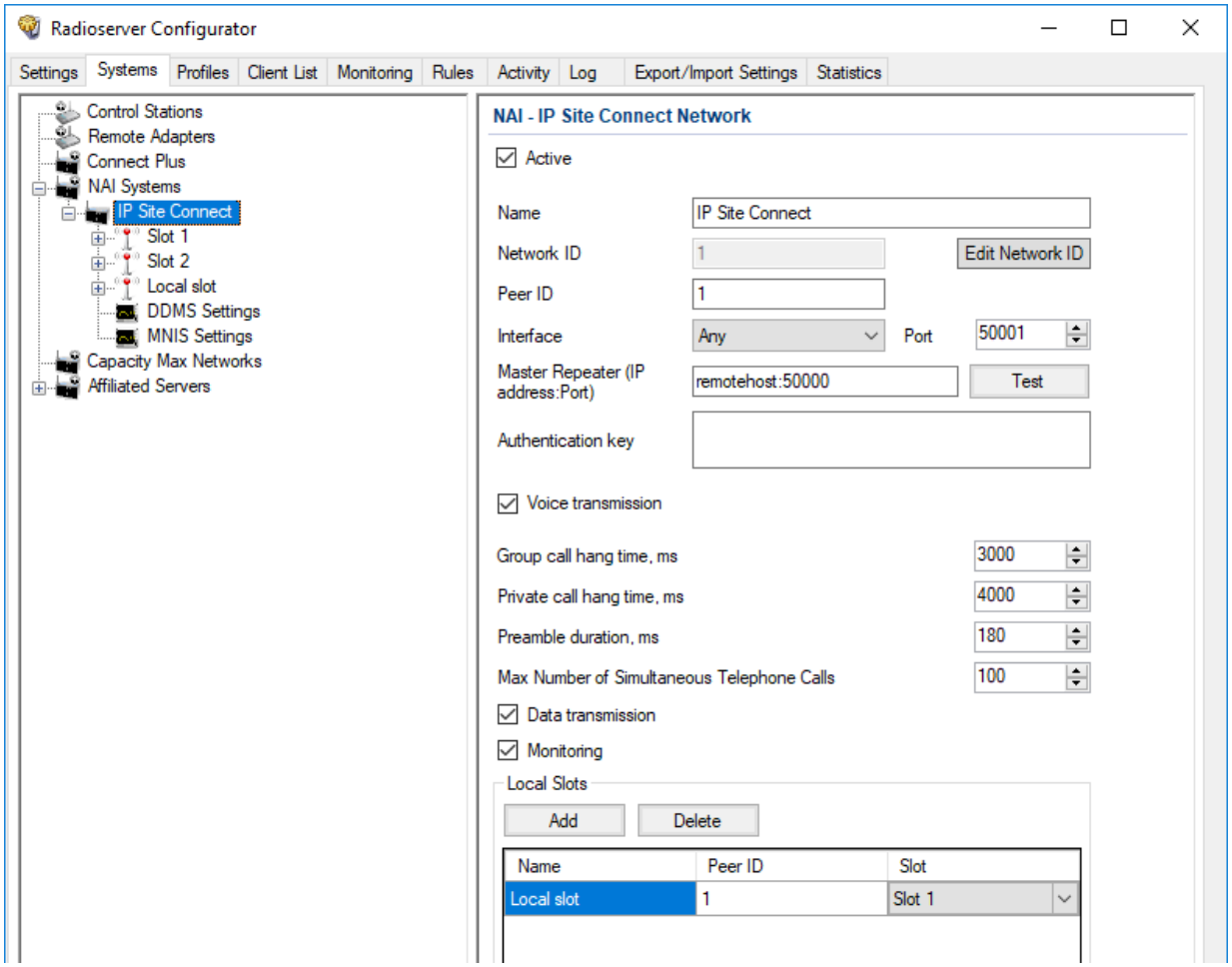
Follow the procedure to add new or edit an existing local slot (site-specific voice channel) in IP Site Connect.

Prerequisites:

- Set the network settings. For details, see Adding and Editing IP Site Connect.
- Ensure that SmartPTT has the license for voice transmissions. For details, see Viewing License Items.
- From repeater codeplugs, obtain information which time slot of the desired repeater is excluded from the IP Site Connect system (is configured as site-specific).

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***NAI Systems*** → ***<network name>***.



3. In the right pane, in the ***Local Slots*** area, perform the following actions:

To add a new local slot,	click ***Add***. The node for the added local slot appears on the left.
To edit an existing local slot,	proceed to the next step of the procedure.

4. In the table, in the desired row, perform the following actions:
   a. In the ***Name*** column, double-click the current slot name, and then type the desired name.
   b. In the ***Peer ID*** column, double-click the current repeater ID value, and then type the desired ID value.
   c. In the ***Slot*** column, select the desired time slot to be used by the local slot:

To use the first time slot of the repeater,	from the list, select *Slot 1*.
To use the second time slot of the repeater,	from the list, select *Slot 2*.

5. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Set the local slot settings. For details, see Configuring SmartPTT Identification.
- Configure talkgroups. For details, see Adding and Editing Talkgroups in IPSC.
- Configure encryption of transmissions in the network. For details, see Configuring Encryption in IPSC.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

6.2.3.3 Configuring SmartPTT Identification

Follow the procedure to configure SmartPTT identification on a slot or local slot of the IP Site Connect network.

Prerequisites:

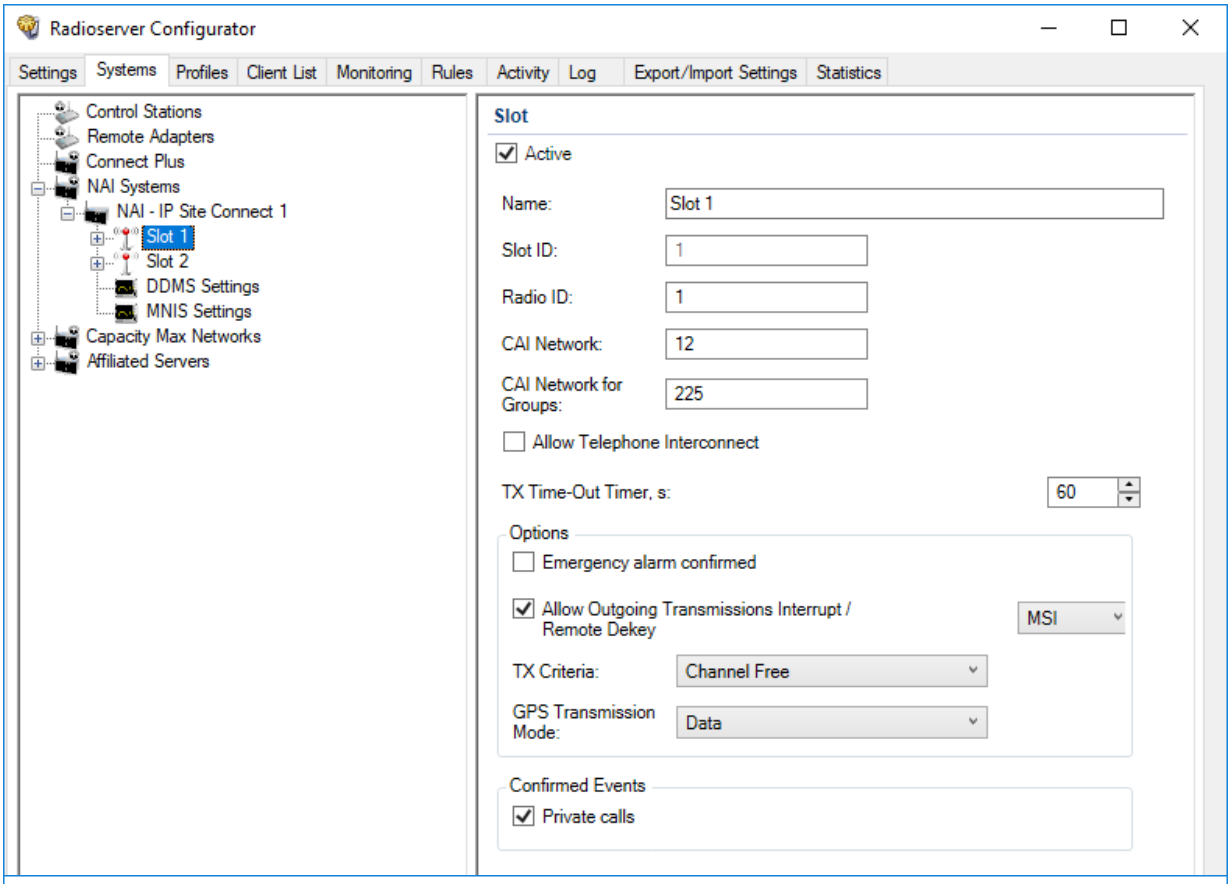
- Set the network settings. For details, see Adding and Editing IP Site Connect.
- Determine the radioserver ID as a virtual radio.
- From radio codeplugs, obtain the following data:
  - CAI and CAI group values.
  - Voice transmission duration.
  - Outgoing transmissions interrupt settings.
  - CSBK data settings (active or inactive).
- From the MNIS configuration file, obtain information on site coordinates (configured or not).
- Determine the necessity for the following radioserver functions:
  - Radio system integration with phone systems.
  - Emergency alarms and calls acknowledgment.
- For local slots, determine the identifier of the desired repeater.

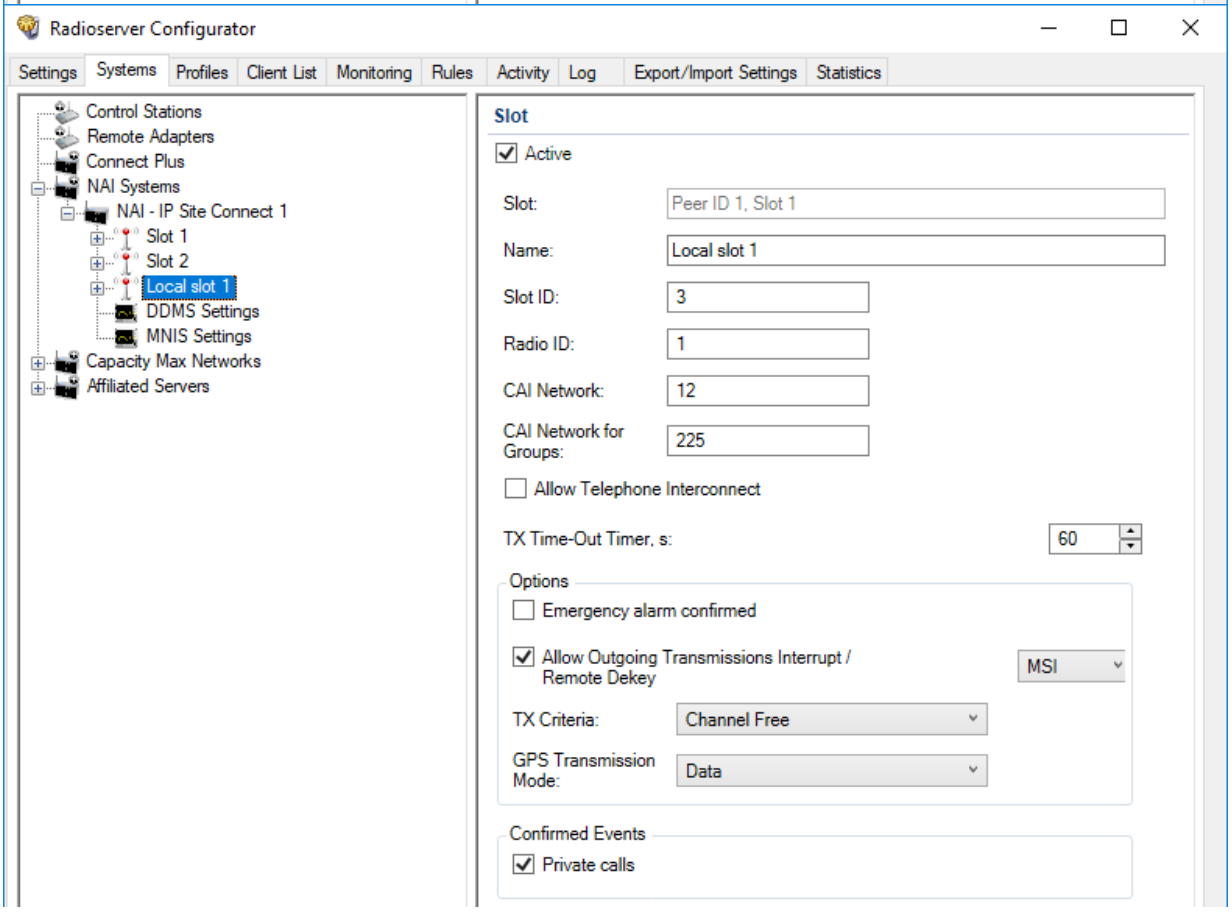
Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***NAI Systems*** → ***<network name>***.
3. Select the desired slot for identification:

To identify SmartPTT on the first time slot,	click the first (upper) node of the slot.
To identify SmartPTT on the second time slot,	click the second (lower) node of the slot.
To identify SmartPTT on a local slot,	click the node of the desired local slot.

In the right pane, the slot settings appear.





4. In the right pane, select the ***Active*** check box.
5. In the ***Name*** field, type the slot name.
6. If available, in the ***Slot ID*** field, enter an identifier of the local slot.

Important
The value must not be 1 or 2, because these values are reserved for time slots.

7. Type the SmartPTT Radioserver identification parameters:
    a. In the ***Radio ID*** field, type the identifier of the radioserver as a virtual radio.

Important
Do not assign this ID to a client or radio in any radio network.

    b. In the ***CAI Network*** field, type the CAI ID.
    c. In the ***CAI Network for Groups*** field, type the CAI Group ID.
8. Select the ***Allow Telephone Interconnect*** check box to allow voice calls between radios registered on the slot and telephone subscribers.
9. In the ***TX Time-Out Timer, s*** field, enter the maximum duration (in seconds) of voice transmissions in the radio network.
10. In the ***Options*** area, select the ***Emergency alarm confirmed*** check box to enable emergency confirmation by SmartPTT Radioserver.
11. Configure the possibility to interrupt voice transmissions from a dispatcher with voice transmissions from a radio:
    a. Select the ***Allow Outgoing Transmissions Interrupt / Remote Dekey*** check box.
    b. Next to the check box, from the list, select the interruption protocol:

To use the protocol developed by Motorola Solutions,	select *MSI*.
To use the protocol included in the DMR digital communication standard,	select *DMR*.

Important
The ***Allow Outgoing Transmissions Interrupt / Remote Dekey*** parameter does not affect the ability of emergency transmissions to interrupt outgoing transmissions from a dispatcher.

12. From the ***TX Criteria*** list, select one of the following options:

If the call initiator must transmit only when no other transmissions are detected over the radio channel,	select *Channel Free*.
If the call initiator must interrupt another participant of the radio network in accordance with the selected MSI or DMR protocol,	select *Tx Interrupt*.
If the call initiator must completely ignore other transmissions over the radio channel,	select *Always*.

13. From the ***GPS Transmission Mode*** list, select one of the following options:

If CSBK data is used in the radio system and site coordinates are configured in MNIS,	select *Enhanced CSBK*.
If CSBK data is used in the radio system but site coordinates are ***not*** configured in MNIS,	select *CSBK*.
In CSBK data is ***not*** used in the radio system or outdoor positioning service is used together with indoor positioning service,	select *Data*.

14. In the ***Confirmed Events*** area, select the ***Private calls*** check box to support private call request confirmation.
15. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (***  ***)***.

Postrequisites:

- Configure talkgroups. For details, see Adding and Editing Talkgroups in IPSC.
- Configure encryption of transmissions in the network. For details, see Configuring Encryption in IPSC.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (***  ***)*** or ***Restart (***  ***)***.

6.2.3.4 Adding and Editing Talkgroups in IPSC

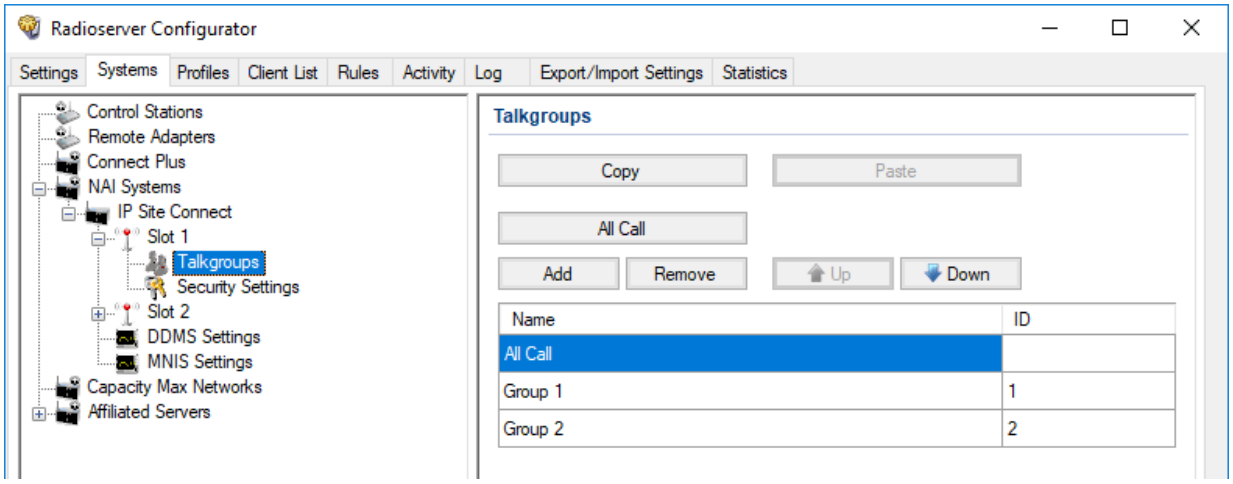
Follow the procedure to add or edit talkgroups or All Call on the selected slot.

Prerequisites:

- Set the selected slot settings. For details, see Configuring SmartPTT Identification.
- From repeater codeplugs, obtain talkgroup IDs.
- If SmartPTT license allows voice calls in the system, determine the All Call necessity.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***NAI Systems*** → ***<network name>*** → ***<slot name>***, and then select ***Talkgroups***.



3. In the right pane, perform one of the following actions:

To add a new talkgroup,	click ***Add***.
To add an All Call,	click ***All Call***.
To edit an existing entry,	proceed to the next step of the procedure.

4. In the table, in the desired entry, perform the following actions:
   a. In the ***Name*** column, double-click the current talkgroup or All Call name, and then type the desired name.
   b. In the ***ID*** column, double-click the current talkgroup ID, and then type the desired ID.

Important
The group ID must be unique across all slots of NAI systems.

NOTE
SmartPTT Radioserver Configurator does not show the All Call ID.

5. *(Optional)* Using ***Up*** and ***Down*** buttons, reorder entries in the table.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- Duplicate the list of groups for other slots of the system. For details, see Settings Duplication.

6.2.3.5 Configuring Encryption in IPSC

Follow the procedure to add security keys to SmartPTT Radioserver that will be used to encrypt and decrypt transmissions.

Prerequisites:

- Ensure that SmartPTT license allows the following features:
  - Voice calls in the systems.
  - *(Optional)* AES-compliant security keys.

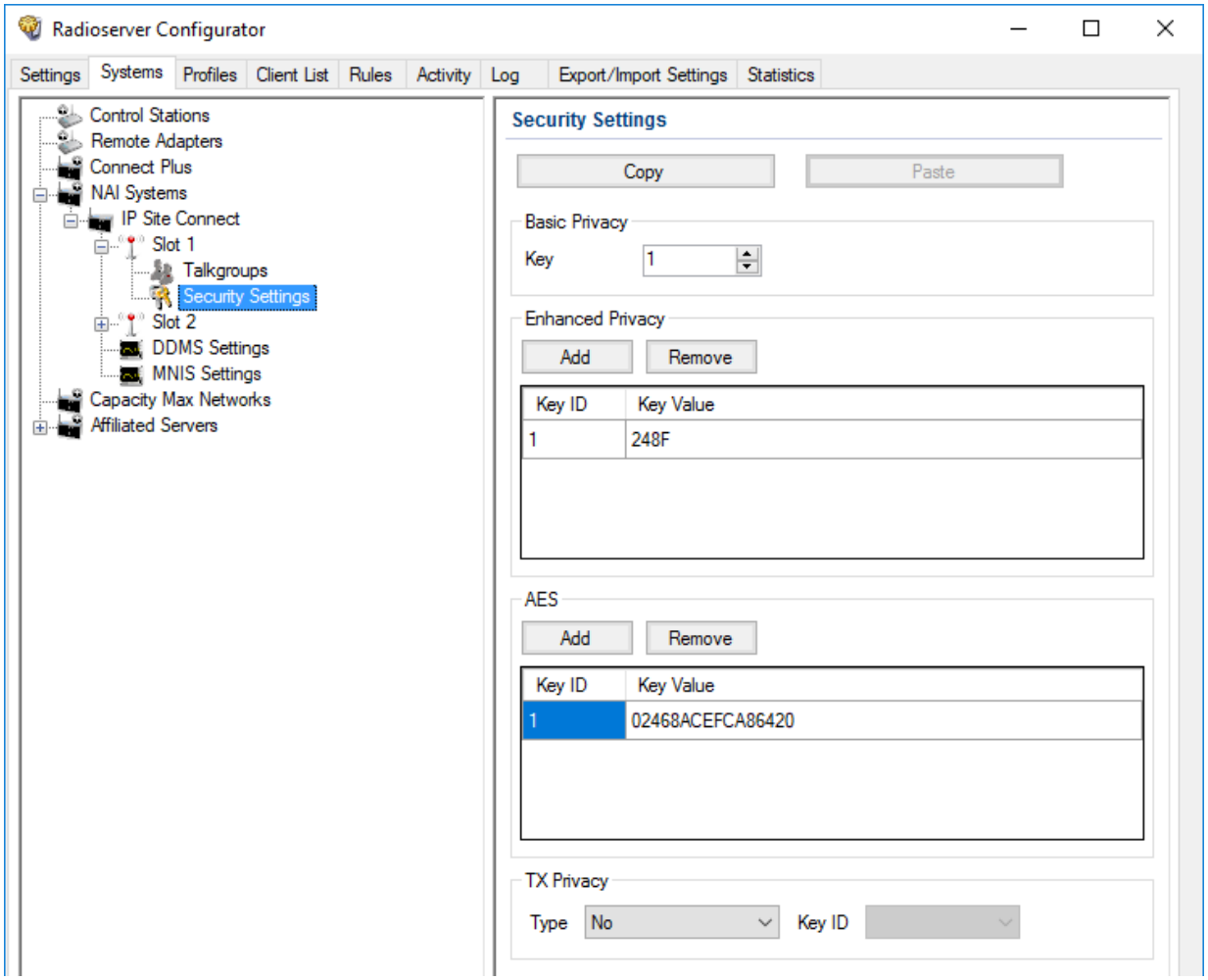
  For details, see Viewing License Items.
- From radio codeplugs, obtain security key IDs and values for all encryption types used in the radio system.

Important
MOTOTRBO configuration tools do not show the configured security/privacy keys for security reasons.

- Determine the key that will be used to encode dispatcher transmissions.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***NAI Systems*** → ***<system name>*** → ***<slot name>***, and then select ***Security Settings***.



3. Configure the desired encryption type:

To configure basic encryption,	in the ***Basic Privacy*** area, in the ***Key*** field, enter the key value.
To configure enhanced encryption,	in the ***Enhanced Privacy*** area, perform the following actions: 1. Click ***Add*** to add a new key. 2. In the corresponding row of the table, in the ***Key ID*** column, double-click the default value, and then type the key ID. 3. In the same row, in the ***Key Value*** column, double-click the cell, and then type the key value.
To configure AES encryption,	in the ***AES*** area, perform the following actions: 1. Click ***Add***.

	2. In the corresponding row of the table, in the ***Key ID*** column, double-click the current ID, and then type the desired ID. 3. In the same row, in the ***Key Value*** column, double-click the current value, and then type the desired value.

4. In the ***Tx Privacy*** area, configure the encryption of dispatcher transmissions:

To use basic encryption,	from the ***Type*** list, select *Basic*.
To use enhanced encryption,	perform the following actions: 1. From the ***Type*** list, select *Enhanced*. 2. From the ***Key ID*** list, select the desired key ID.
To use AES encryption,	perform the following actions: 1. From the ***Type*** list, select *AES (Symmetric Key)*. 2. From the ***Key ID*** list, select the ID of the desired key.
To transmit without encryption,	from the ***Type*** list, select *No*.

5. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

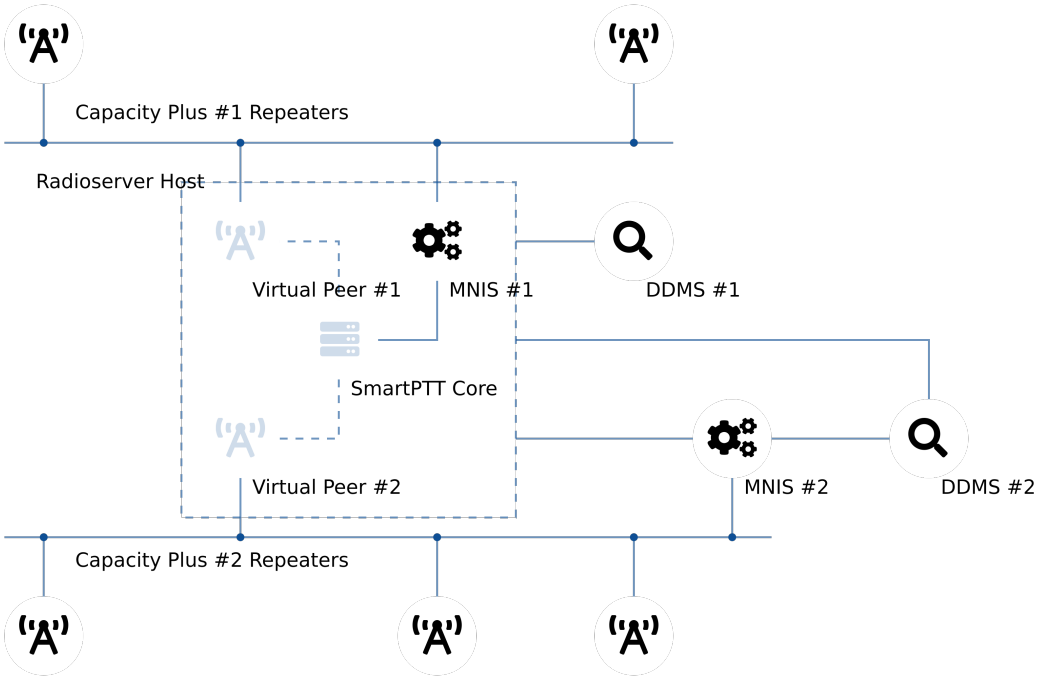
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- Duplicate security keys for other slots of the system. For details, see Settings Duplication.

6.3 Capacity Plus

Capacity Plus is a family of digital trunked radio systems by Motorola Solutions. The family includes single-site and multisite systems. Multisite systems may be referred to as Linked Capacity Plus or Capacity Plus Multi-Site.

In SmartPTT, single-site and multisite systems are configured differently. The current section describes the single-site solution (Capacity Plus). For information on the multisite system, see Linked Capacity Plus.

MOTOTRBO™ Capacity Plus is a digital (DMR) trunked radio system. It is a single-site system with high channel capacity (up to 12 simultaneous voice calls). This is achieved by the use of multiple repeaters installed on the site. Each repeater is configured to the unique duplex channel. For details, see MOTOTRBO™ Capacity Plus on the Motorola Solutions website.



SmartPTT is able to connect to multiple Capacity Plus systems at a time. If bridging is configured between those systems, SmartPTT will provide increased RF coverage. The size of the zone will be proportional to the number of the bridged Capacity Plus systems.

SmartPTT connects to Capacity Plus over the Network Application Interface (NAI) that is provided by Motorola Solutions. It requires to use the following additional software:

- MOTOTRBO Network Interface Service (MNIS) provides data communication between the radio system and SmartPTT.
- Device Discovery and Mobility Service (DDMS) provides the radio presence (ARS) information to SmartPTT.

In SmartPTT, Capacity Plus connection requires the following licenses:

- Voice and radio commands license (includes emergency alarms and calls).
- Data exchange license.

6.3.1 SmartPTT Features in Capacity Plus

Capacity Plus provides SmartPTT with access to the following features:

- Information on radio presence in the network (ARS).
- Radio user identification.
- Voice call reception and initiation (includes group calls and private calls).
- Emergency alarms and calls.
- Radio location updates (includes revert channel support).
- Text messaging and job ticketing.

- Radio commands.
- Telemetry and remote control over radios.

SmartPTT provides the following features for Capacity Plus users:

- Simultaneous access to multiple systems.
- Integration with other radio systems using cross patches, bridging, and conference calls.
- Telephone interconnect over SIP trunk.
- Event logging and voice recording.
- Per-console and system-wide rules.
- Availability for Web Client users, SmartPTT Mobile users, and third-party applications.

For network monitoring purposes, SmartPTT provides the following features:

- Network device monitoring over SNMP (includes control stations).
- Integral radio channel monitoring (also referred to as “air monitoring”).
- Repeater control over RDAC.
- Network topology visualization and update.

NOTE
SmartPTT does ***not*** show on-site/fielded radios on topology diagrams.

- Statistical information gathering (system performance, alarm statistics), reports generation.

6.3.2 Capacity Plus Configuration

Connection to Capacity Plus requires additional radio devices configuration, MNIS configuration, DDMS configuration, and dispatch software configuration.

Radio Devices Configuration

To support SmartPTT connection, the following actions must be performed:

- Radio IDs must be reserved for the following needs:
  - Dispatch subsystem (SmartPTT) identification.
  - MNIS identification.
  - *(Optional)* Individual dispatcher (operator) identification.
- To update the location when the radio sends telemetry data, the ***GNSS Report*** check box must be selected for the desired GPIO physical pins in the radio codeplugs.
- Peer IDs (Repeater Radio IDs) must be reserved for the following needs:
  - SmartPTT identification as a software peer.
  - MNIS identification.
- MNIS Radio ID (***not*** SmartPTT Radio ID) must be configured as the ARS ID in all radio codeplugs.

- All radios and repeaters must have equal CAI IDs and CAI Group IDs.
- IP address and UDP port of the master repeater must be obtained.
- Security keys must be obtained from radio codeplugs.

If you need assistance in the MOTOTRBO devices configuration, contact Motorola Solutions representatives in your region.

MNIS and DDMS Configuration

To configure MNIS and DDMS, the following actions must be performed:

- Dedicated IDs (Radio ID and Peer ID) must be assigned to MNIS.
- MNIS must be connected to the Capacity Plus master repeater.
- *(Optional)* RF site latitude and longitude must be configured in MNIS to increase the rate of radio location updates.
- Security keys must be configured in MNIS.
- DDMS address must be configured in MNIS.
- ARS ports must be synchronized in MNIS and DDMS.

If you need assistance in the MOTOTRBO software configuration, contact Motorola Solutions representatives in your region.

SmartPTT Configuration

To configure SmartPTT to work with Capacity Plus, the following actions must be performed:

- Connection to the master repeater must be configured. For details, see Adding and Editing Capacity Plus.
- SmartPTT Radioserver must be identified in the radio system. For details, see Configuring SmartPTT Identification in Capacity Plus.
- Talkgroups and All Call must be configured. For details, see Adding and Editing Talkgroups in Capacity Plus.
- Security keys must be configured in SmartPTT. For details, see Configuring Encryption in Capacity Plus.
- DDMS connection must be configured in SmartPTT. For details, see Configuring DDMS Connection.
- SmartPTT must be connected to the MNIS server. For details, see Configuring MNIS Connection.

If you need assistance in the SmartPTT configuration, submit a request to SmartPTT Technical Support Center.

Network Monitoring

For network monitoring configuration in SmartPTT, the following actions must be performed:

- IP addresses of all repeaters in the system must be obtained.
- IP addresses of all other network devices must be obtained. This includes uninterruptible power supplies (UPS), switches, routers, etc.

For information on network monitoring configuration, see Network Monitoring.

6.3.2.1 Configuring Connection to Capacity Plus

Follow the procedure to add new or edit an existing connection to the radio system.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure that SmartPTT has the license for voice and data exchange in the network. For details, see Viewing License Items.
- From codeplugs of repeaters, obtain the following data:
  - IP address and UDP port of a master repeater.
  - Repeater private authentication key.
- From radio codeplugs, obtain the following data:
  - Duration of the group and private call hangtime.
  - Duration of the voice transmission delay (preamble duration).
- If the repeater and radioserver are in different networks controlled by different routers over the router that supports Network Address Translation (NAT), obtain the IP address and UDP port that will be translated to the master repeater IP address and UDP port number.
- *(Optional)* Turn on SmartPTT monitoring. For details, see Configuring Monitoring Database Connection.

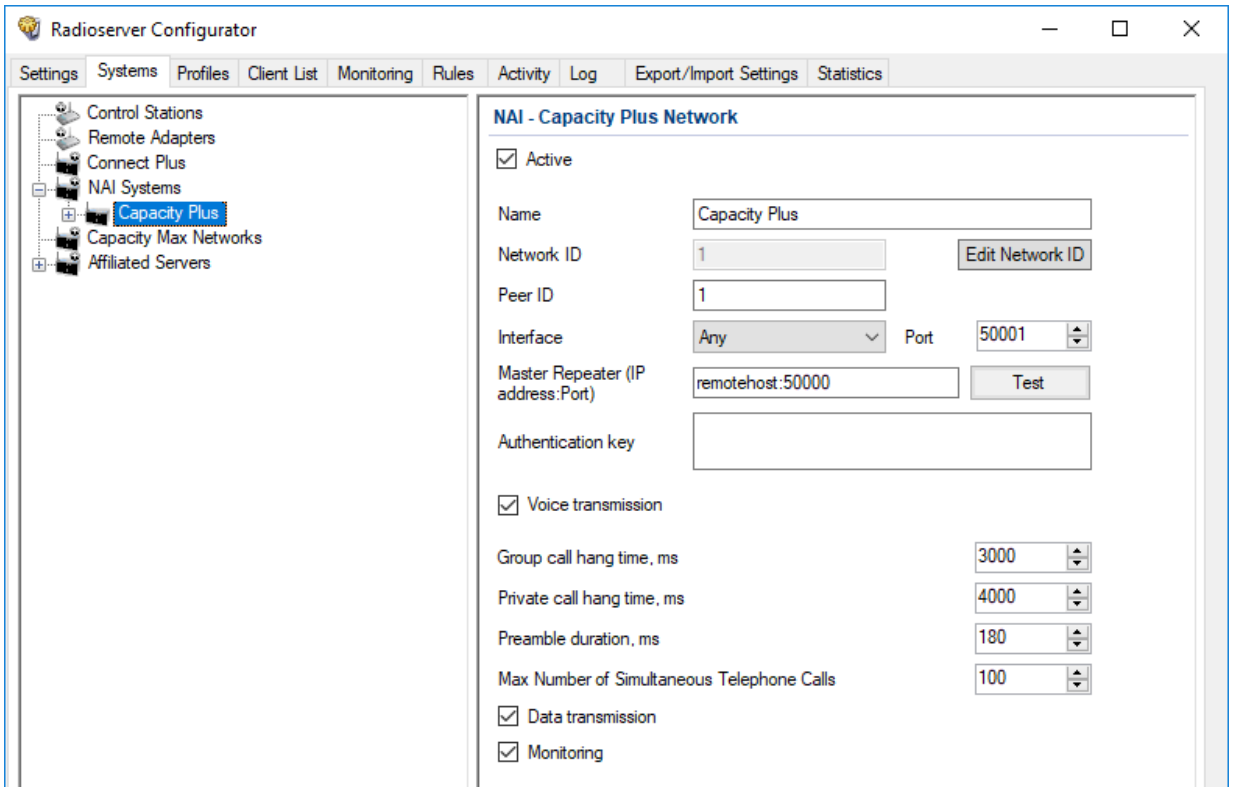
Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.

2. In the left pane, perform one of the following actions:

To add a new network,	right-click the ***NAI Systems*** node, point to ***Add***, and then select ***NAI - Capacity Plus***.
To edit an existing network,	expand the ***NAI Systems***, and then click the desired network.

The connection settings appear in the right pane of the tab.



3. In the right pane, configure the general connection settings:
   a. Select the ***Active*** check box.
   b. In the ***Name*** field, type the radio system name.
   c. Leave the value in the ***Network ID*** field unchanged.
4. Configure the master repeater connection:
   a. In the ***Peer ID*** field, type the ID of the virtual repeater reserved for a radioserver.
   b. From the ***Interface*** list, select one of the following options:

To use any of the radioserver host IP addresses,	select *Any*.
To fix the IP address,	select the desired IP address.

Important
If a radioserver and MNIS are installed on the same computer, use fixed IP address that is different from the MNIS Tunnel IP address (by default, *192.168.56.1*).

Important
If a radio or control station is connected to the computer, use fixed IP address that is different from the radio or control station IP address (by default, *192.168.10.1*).

c. In the ***Port*** field, enter the radioserver host port that will be used to connect to the repeater.

d. In the ***Master Repeater (IP address:Port)*** field, type the IP address and UDP port that a radioserver will use to connect to the master repeater (includes the potential NAT use). Input format is <IP address in dot-decimal notation>:<UDP port>.

e. In the ***Authentication key*** field, type the repeater private authentication key. To view the entered key, click the eye icon ( ). For security reasons, the key will not be available for viewing in subsequent sessions.

f. *(Optional)* Click ***Test*** to check the repeater connection.

5. Configure voice call parameters in the radio system:

a. Select the ***Voice transmission*** check box to allow voice reception and transmission for SmartPTT.

b. In the ***Group call hang time, ms*** field, enter the hangtime duration (in milliseconds) for group calls.

c. In the ***Private call hang time, ms*** field, enter the hangtime duration (in milliseconds) for private calls.

d. In the ***Preamble duration, ms*** field, enter the transmission start delay (in milliseconds).

e. In the ***Max Number of Simultaneous Telephone Calls*** field, enter the maximum number of voice calls between radio system and phone system.

6. Select the ***Data transmission*** check box to allow SmartPTT data exchange with MNIS and DDMS services.

7. *(Optional)* Select the ***Monitoring*** check box to turn on the radio system devices diagnostics.

8. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Identify a radioserver in the system. For details, see Configuring SmartPTT Identification in Capacity Plus.
- Configure talkgroups and All Call in the network. For details, see Adding and Editing Talkgroups in Capacity Plus.
- Configure security keys. For details, see Configuring Encryption in Capacity Plus.
- If data transmission is allowed, configure DDMS service. For details, see Configuring DDMS Connection.
- If data transmission is allowed, configure MNIS service. For details, see Configuring MNIS Connection.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- In the firewall software on the computer, unlock the specified UDP port. For details, see Radioserver Host.
- *(Optional)* Configure network device monitoring. For details, see Network Monitoring.

6.3.2.2 Configuring SmartPTT Identification in Capacity Plus

Follow the procedure to configure SmartPTT identification in the radio network.

Prerequisites:

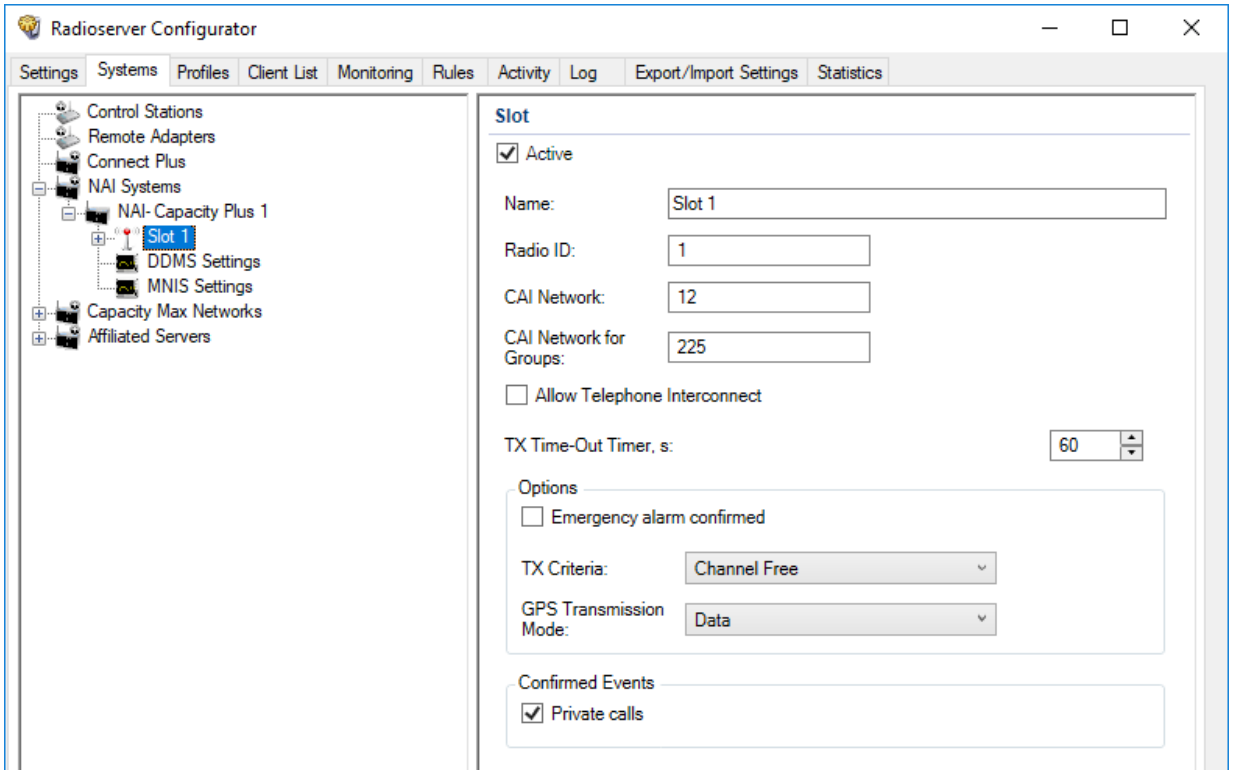
- Configure the network settings. For details, see Adding and Editing Capacity Plus.
- From radio codeplugs, obtain the following data:

- CAI and CAI group values.
- Voice transmission duration.
- CSBK data settings (active or inactive).

- From the MNIS configuration file, obtain information on the repeater location (configured or not).
- Determine the necessity for the following radioserver functions:
  - Radio system integration with phone systems.
  - Emergency alarms and calls acknowledgment.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***NAI Systems*** → ***<system name>***, and then click ***<slot name>***.
   The identification parameters appear in the right pane of the tab.



3. In the right pane, select the ***Active*** check box.
4. In the ***Name*** field, type the title that will represent the radio network in SmartPTT Dispatcher.
5. Type the SmartPTT Radioserver identification parameters:
   a. In the ***Radio ID*** field, type the radio ID that is reserved for SmartPTT Radioserver.
   b. In the ***CAI Network*** field, type the CAI ID.
   c. In the ***CAI Network for Groups*** field, type the CAI Group ID.
6. Select the ***Allow Telephone Interconnect*** check box to provide voice calls feature between the radio system and phone system.
7. In the ***TX Time-Out Timer, s*** field, enter the maximum duration (in seconds) of voice transmissions in the radio network.

8. In the ***Options*** area, select the ***Emergency alarm confirmed*** check box to enable emergency confirmation by SmartPTT Radioserver.
9. From the ***TX Criteria*** list, select one of the following options:

If the call initiator must transmit only when no other transmissions are detected over the radio channel,	select *Channel Free*.
If the call initiator must interrupt another participant of the radio network according to the selected MSI or DMR protocol,	select *Tx Interrupt*.
If the call initiator must completely ignore other transmissions over the radio channel,	select *Always*.

10. From the ***GPS Transmission Mode*** list, select one of the following options:

If CSBK data is used in the radio system and site coordinates are configured in MNIS,	select *Enhanced CSBK*.
If CSBK data is used in the radio system but site coordinates are not configured in MNIS,	select *CSBK*.
In CSBK data is not used in the radio system or outdoor positioning service is used together with indoor positioning service,	select *Data*.

11. In the ***Confirmed Events*** area, select the ***Private calls*** check box to support private call request confirmation.
12. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (***  ***)***.

Postrequisites:

- Configure talkgroups. For details, see Adding and Editing Talkgroups in Capacity Plus.
- Configure security keys. For details, see Configuring Encryption in Capacity Plus.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (***  ***)*** or ***Restart (***  ***)***.

6.3.2.3 Adding and Editing Talkgroups in Capacity Plus

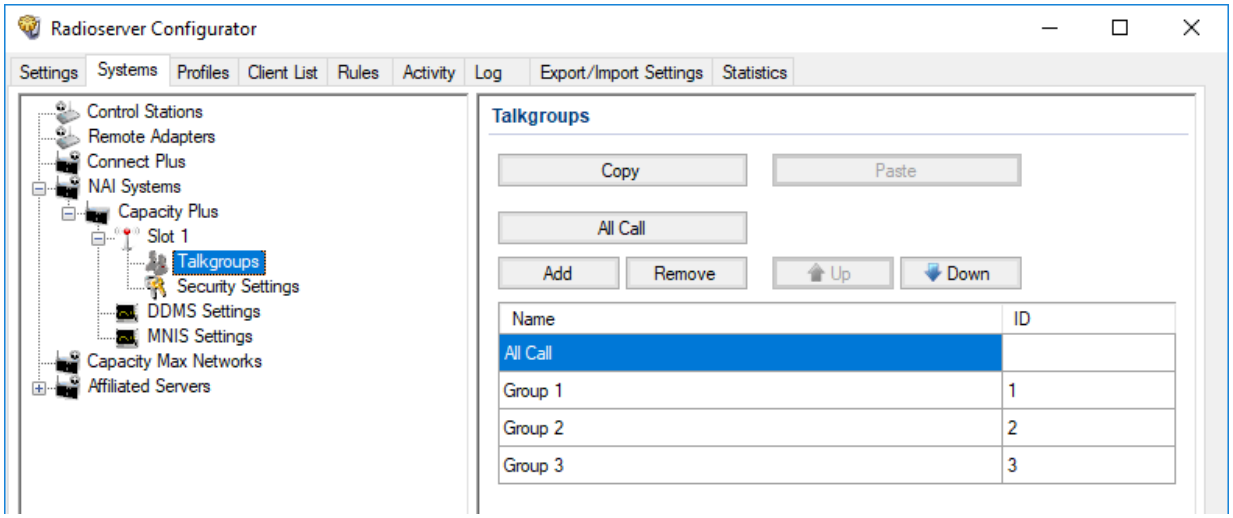
Follow the procedure to add or edit talkgroups or All Call available in the system.

Prerequisites:

- Configure SmartPTT identification in the radio network. For details, see Configuring SmartPTT Identification in Capacity Plus.
- From repeater codeplugs, obtain talkgroup IDs.
- If SmartPTT license allows voice calls in the system, determine the All Call necessity.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***IP Site Connect Networks*** → ***<network name>*** → ***<slot name>***, and then select ***Talkgroups***.



3. In the right pane, perform one of the following actions:

To add a new talkgroup,	click ***Add***.
To add an All Call,	click ***All Call***.
To edit an existing entry,	proceed to the next step of the procedure.

4. In the table, in the desired entry, perform the following actions:
   a. In the ***Name*** column, double-click the current talkgroup or All Call name, and then type the desired name.
   b. In the same row, in the ***ID*** column, double-click the current talkgroup ID, and then type the desired ID.

Important
The group ID must be unique across all slots of NAI systems.

NOTE
SmartPTT Radioserver Configurator does not show All Call IDs.

5. *(Optional)* Using ***Up*** and ***Down*** buttons, reorder entries in the table.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (*** ***)***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (*** ***)*** or ***Restart (*** ***)***.

6.3.2.4 Configuring Encryption in Capacity Plus

Follow the procedure to support encrypted transmissions decoding and encoding in SmartPTT.

Prerequisites:

- Ensure that SmartPTT license allows the following features:
  - Voice calls in conventional (IPSC) systems.
  - *(Optional)* AES-compliant security keys.

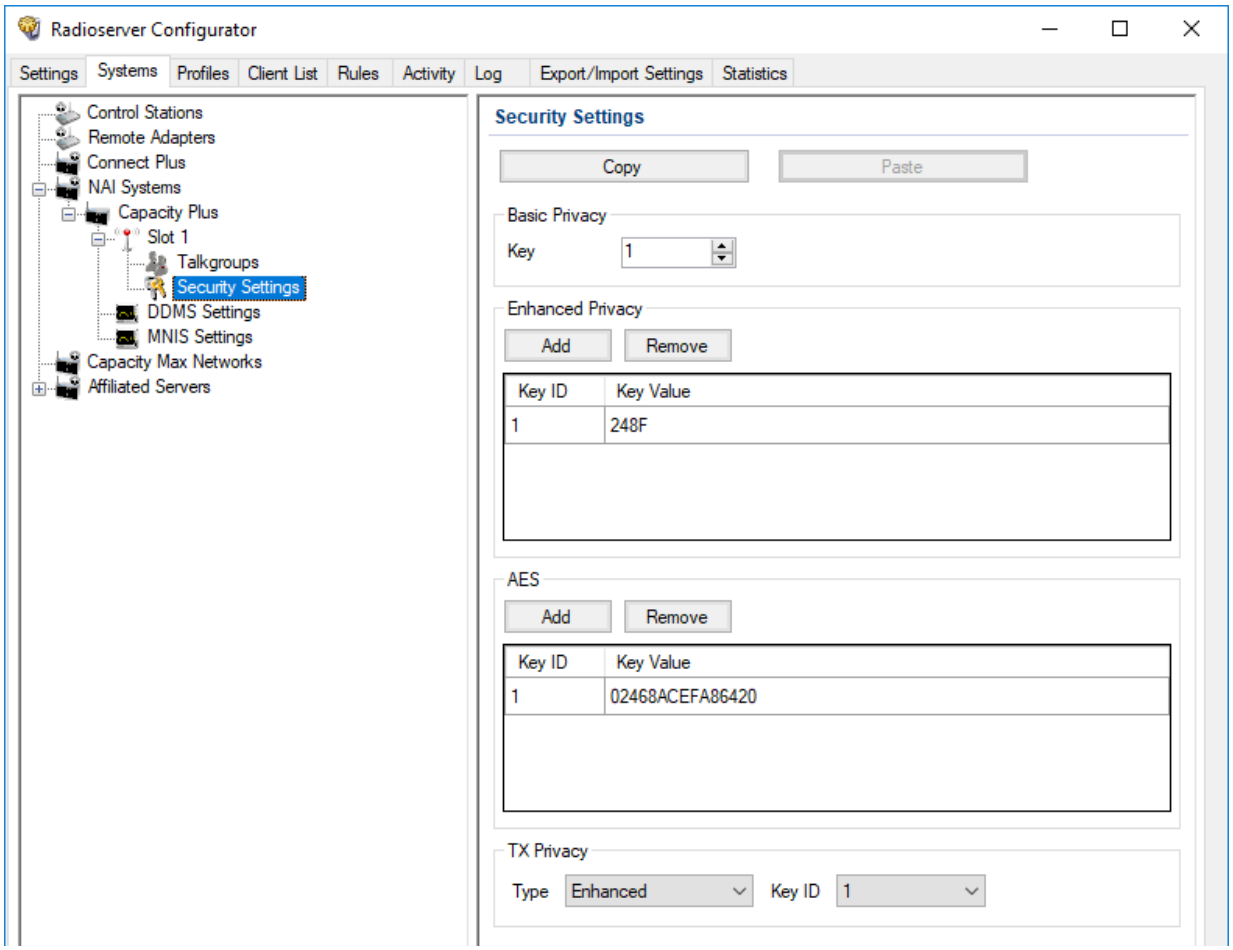
  For details, see Viewing License Items.
- Obtain security key IDs and values for all encryption types used in the radio system.

Important
MOTOTRBO configuration tools do ***not*** show the configured security/privacy keys for security reasons.

- Determine the key that will be used to encode dispatcher transmissions.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***NAI Systems*** → ***<system name>*** → ***<slot name>***, and then select ***Security Settings***.
   The security key settings appear in the right pane.



3. Configure the desired encryption type:

To configure basic encryption,	in the ***Basic Privacy*** area, in the ***Key*** field, enter the key value.
To configure enhanced encryption,	in the ***Enhanced Privacy*** area, perform the following actions: 1. Click ***Add*** to add a new key. 2. In the corresponding row of the table, in the ***Key ID*** column, double-click the default value, and then type the key ID. 3. In the same row, in the ***Key Value*** column, double-click the cell, and then type the key value.
To configure AES encryption,	in the ***AES*** area, perform the following actions: 1. Click ***Add***. 2. In the corresponding row of the table, in the ***Key ID*** column, double-click the current ID, and then type the desired ID. 3. In the same row, in the ***Key Value*** column, double-click the current value, and then type the desired value.

4. In the ***Tx Privacy*** area, configure the encryption of dispatcher transmissions:

To use basic encryption,	from the ***Type*** list, select *Basic*.
To use enhanced encryption,	perform the following actions: 1. From the ***Type*** list, select *Enhanced*. 2. From the ***Key ID*** list, select the desired key ID.
To use AES encryption,	perform the following actions: 1. From the ***Type*** list, select *AES (Symmetric Key)*. 2. From the ***Key ID*** list, select the ID of the desired key.
To transmit without encryption,	from the ***Type*** list, select *No*.

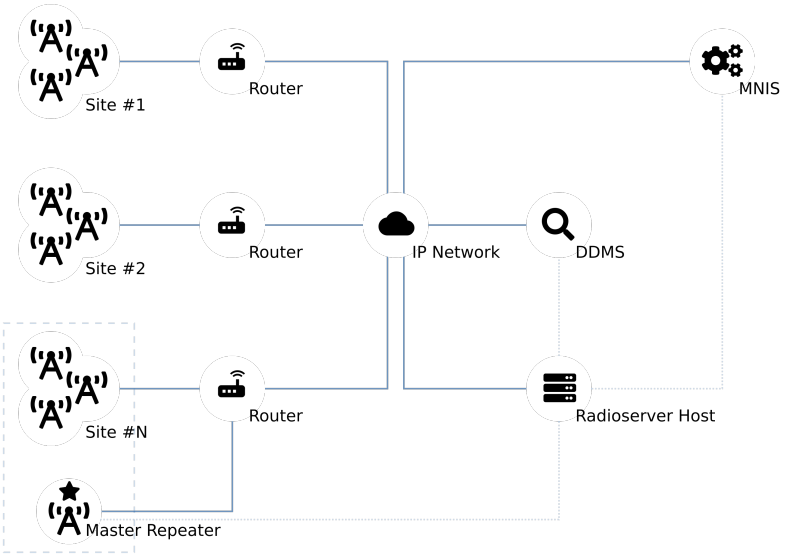
5. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- Duplicate security keys for other slots of the system. For details, see Settings Duplication.

6.4 Linked Capacity Plus

Linked Capacity Plus (Capacity Plus Multi-Site) is a digital (DMR) trunked radio system. It is a multisite system (provides great RF coverage) that provides several simultaneous voice calls on the site.
For information on the radio system and its capabilities, see MOTOTRBO™ Capacity Plus Multi-Site on the Motorola Solutions website.



SmartPTT is able to connect to multiple Linked Capacity Plus radio systems at once. To provide this connection, use Network Application Interface (NAI) developed by Motorola Solutions. Using NAI requires to use the following additional software:

- MOTOTRBO Network Interface Service (MNIS) provides data communication between the radio system and SmartPTT.
- Device Discovery and Mobility Service (DDMS) provides ARS information to SmartPTT.

SmartPTT Radioserver requires simultaneous connection to master repeater, MNIS, and DDMS (see dotted lines on the diagram).

In Linked Capacity Plus, master repeater is a real radio system repeater. It can be installed on any site of the system.

6.4.1 SmartPTT Features in LCP

Linked Capacity Plus provides the following features to SmartPTT:

- Information on radio presence in the network (ARS)
- Radio user identification
- Voice call reception and initiation (includes group calls and private calls)
- Emergency alarms and calls
- Radio location updates (includes revert channel support)
- Text messages and job tickets
- Radio commands
- Telemetry and remote control over radios

For Linked Capacity Plus, SmartPTT provides the following features:

- Simultaneous connection to multiple Linked Capacity Plus radio systems.
- Connecting multiple Linked Capacity Plus networks to one MNIS service.
- Integration with other radio systems using bridging and conference calls.
- Integration between phone systems and radio systems.
- Event logging and voice recording.
- Rules configuration.

For network monitoring, the following features are provided:

- Network device monitoring over SNMP.
- Over-the-air traffic monitoring (without splitting by radio channels).
- Network topology visualization.

NOTE
SmartPTT does ***not*** show on-site/fielded radios on the topology diagram.

- Statistical information gathering (system performance, alarm statistics), reports generation.

6.4.2 Linked Capacity Plus Configuration

Linked Capacity Plus connection requires additional radio devices configuration, MNIS configuration, DDMS configuration, and dispatch software configuration.

Radio Devices Configuration

To support SmartPTT connection, the following actions must be performed:

- Radio IDs must be reserved for the following needs:
  - Dispatch subsystem (SmartPTT) identification.
  - MNIS identification.
  - *(Optional)* Individual dispatcher (operator) identification.
- Peer IDs must be reserved for the following needs:
  - SmartPTT identification as a software peer.
  - MNIS identification.
- MNIS Radio ID (***not*** SmartPTT Radio ID) must be configured as the ARS ID in all radio codeplugs.
- All radios and repeaters must have the same CAI IDs and CAI Group IDs.
- IP address and UDP port of the master repeater must be obtained.
- Security keys configured in radio codeplugs must be obtained.

NOTE
All radio stations, MNIS, and the radioserver must have the same security keys in order for voice calls to work correctly.

If you need assistance in the MOTOTRBO devices configuration, contact Motorola Solutions representatives in your region.

MNIS and DDMS Configuration

To configure MNIS and DDMS, the following actions must be performed:

- Dedicated IDs (Radio ID and Peer ID) must be assigned to MNIS.
- MNIS must be connected to the master repeater.
- *(Optional)* Repeater coordinates must be configured in MNIS to increase the rate of radio location updates.
- Security keys that are configured in radio codeplugs must be configured in MNIS.
- DDMS address must be configured in MNIS.
- ARS ports must be synchronized in MNIS and DDMS.

If you need assistance in the MOTOTRBO software configuration, contact Motorola Solutions representatives in your region.

SmartPTT Configuration

To configure SmartPTT to work in Linked Capacity Plus, the following actions must be performed:

- Connection to the master repeater must be configured. For details, see Adding and Editing LCP Connection.
- SmartPTT Radioserver must be identified in the radio system. For details, see Configuring SmartPTT Identification.
- Talkgroups and All Calls must be configured. For details, see Adding and Editing Groups in LCP.
- Call routing between the phone and radio system must be configured. For details, see Configuring Phone Calls Routing.
- Security keys must be configured in SmartPTT. For details, see Configuring Encryption in LCP.
- SmartPTT must be connected to DDMS. For details, see Configuring DDMS Connection.
- SmartPTT must be connected to MNIS. For details, see Configuring MNIS Connection.

If you need assistance in the SmartPTT configuration, submit a request to SmartPTT Technical Support Center.

Network Monitoring

For network monitoring configuration in SmartPTT, the following actions must be performed:

- IP addresses of all repeaters in the system must be obtained.
- IP addresses of all other network devices must be obtained. This includes uninterruptible power supplies (UPS), switches, routers, etc.

For information on network monitoring configuration, see Network Monitoring.

6.4.2.1 Phone Call Routing Priority

SmartPTT provides the ability to configure routing priority for voice calls from the phone system to Linked Capacity Plus. Prioritization is applicable to group calls only. Private calls are routed automatically to the site where the radio is registered.

For priority configuration, the following conditions must be met:

- Talkgroup and/or All Call must be site-specific, ***not*** system-wide.
- Same talkgroup ID and/or All Call must be available on multiple sites.
- Phone call mask must ***not*** have a site ID substitution.

If these conditions are met, radioserver will try to initiate a group call on the site that is available in the first row of the table. If the group call is successfully initiated, it will ***not*** be initiated on other sites. If the group call initiation fails, radioserver will try to initiate a group call on the site that is in the next row of the priority table.

For instructions on the phone call routing priority configuration, see Configuring Phone Calls Routing.

6.4.2.2 Configuring Connection to LCP

Follow the procedure to add a new or edit an existing connection to the radio system.

Prerequisites:

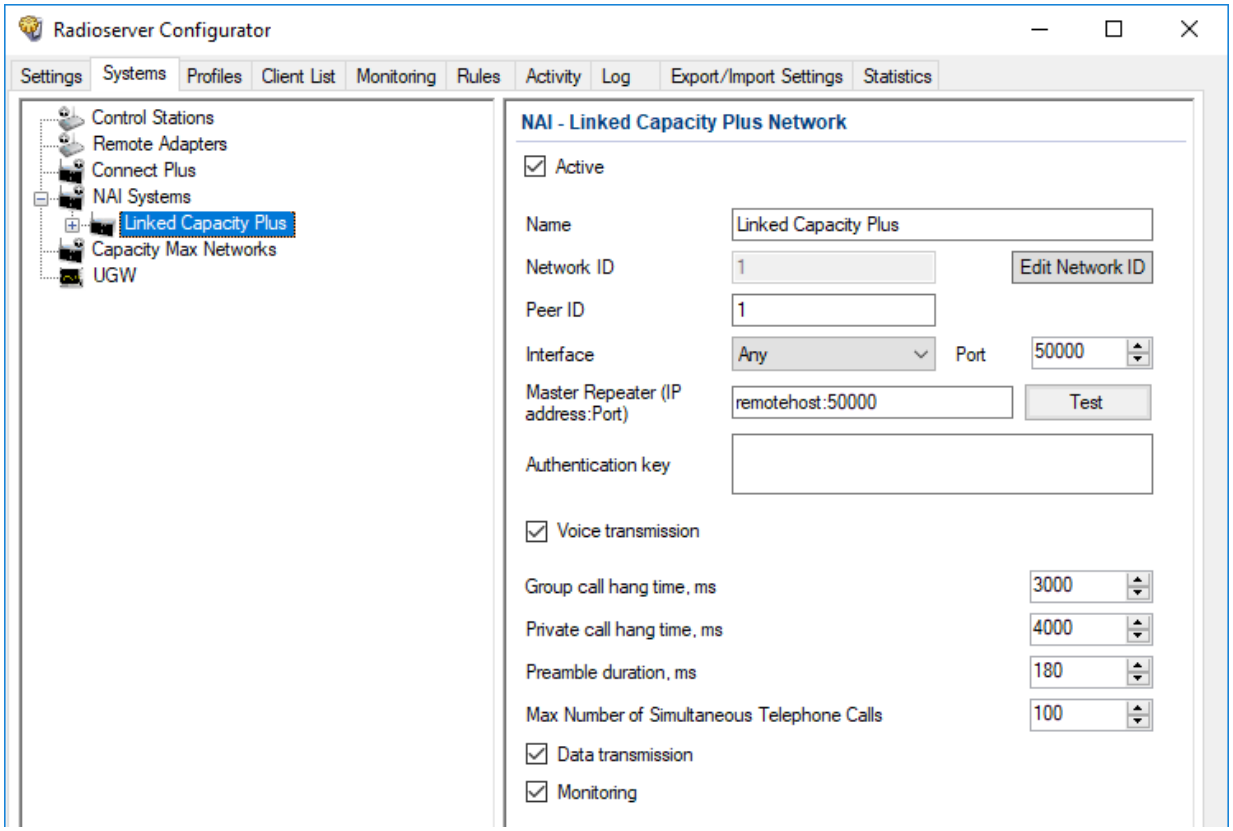
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- From repeater codeplugs, obtain the following data:
  - Master repeater IP address and UDP port number.
  - Repeater private authentication key.
- From radio codeplugs, obtain the following data:
  - Duration of the group and private call hangtime.
  - Duration of the voice transmission delay (preamble duration).
- Determine the maximum number of voice calls between the radio system and the phone system.
- If the master repeater and radioserver are connected over the router that supports Network Address Translation (NAT), obtain the IP address and UDP port that will be translated to the master repeater IP address and UDP port number.
- *(Optional)* Turn on SmartPTT monitoring. For details, see Configuring Monitoring Database Connection.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, perform one of the following actions:

To add a new network,	right-click the ***NAI Systems*** node, then select ***Add → NAI - Linked Capacity Plus***.
To modify an existing network,	expand the ***NAI Systems*** node, and then click ***<network name>***.

The connection settings appear in the right pane of the tab.



3. In the right pane, configure the general connection settings:
   a. Select the ***Active*** check box.
   b. In the ***Name*** field, type the radio system name.
   c. Leave the value in the ***Network ID*** field unchanged.
4. Configure the master repeater connection:
   a. In the ***Peer ID*** field, type the ID of the virtual repeater reserved for a radioserver.
   b. From the ***Interface*** list, select one of the following options:

To use any of the radioserver host IP addresses,	select *Any*.
To select the specific IP address,	select one of the available IP addresses.

Important
If a radioserver and MNIS are installed on the same computer, use fixed IP address that is different from the MNIS Tunnel IP address (by default, *192.168.56.1*).

Important
If a radio or control station is connected to the radio server computer, use fixed IP address that is different from the radio or control station IP address (by default, *192.168.10.1*).

c. In the ***Port*** field, enter the radioserver host port that will be used to connect to the repeater.

d. In the ***Master Repeater (IP address:Port)*** field, type the IP address and UDP port that a radioserver will use to connect to the master repeater (includes the potential NAT use). Use the following format: <IP address in dot-decimal notation>:<UDP port>.

e. In the ***Authentication key*** field, type the repeater private authentication key.

f. *(Optional)* Click ***Test*** to check the repeater connection.

5. Configure voice call parameters in the radio system:

a. Select the ***Voice transmission*** check box to allow voice reception and transmission for SmartPTT.

b. In the ***Group call hang time, ms*** field, enter the hangtime duration (in milliseconds) for group calls.

c. In the ***Private call hang time, ms*** field, enter the hangtime duration (in milliseconds) for private calls.

d. In the ***Preamble duration, ms*** field, enter the transmission start delay (in milliseconds).

e. In the ***Max Number of Simultaneous Telephone Calls*** field, enter the maximum number of voice calls between the radio system and phone system.

6. Select the ***Data transmission*** check box to allow SmartPTT data exchange with MNIS and DDMS services.

7. *(Optional)* Select the ***Monitoring*** check box to turn on the radio system devices diagnostics.

8. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Identify a radioserver in the system. For details, see Configuring SmartPTT Identification.
- Configure talkgroups and All Call in the network. For details, see Adding and Editing Groups in LCP.
- Configure phone calls routing. For details, see Configuring Phone Calls Routing.
- Configure security keys. For details, see Configuring Encryption in LCP.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- In the firewall software on the computer, unlock the specified UDP port. For details, see Radioserver Host.
- *(Optional)* Configure network device monitoring. For details, see Network Monitoring.

6.4.2.3 Configuring SmartPTT Identification

Follow the procedure to configure SmartPTT identification in the radio network.

Prerequisites:

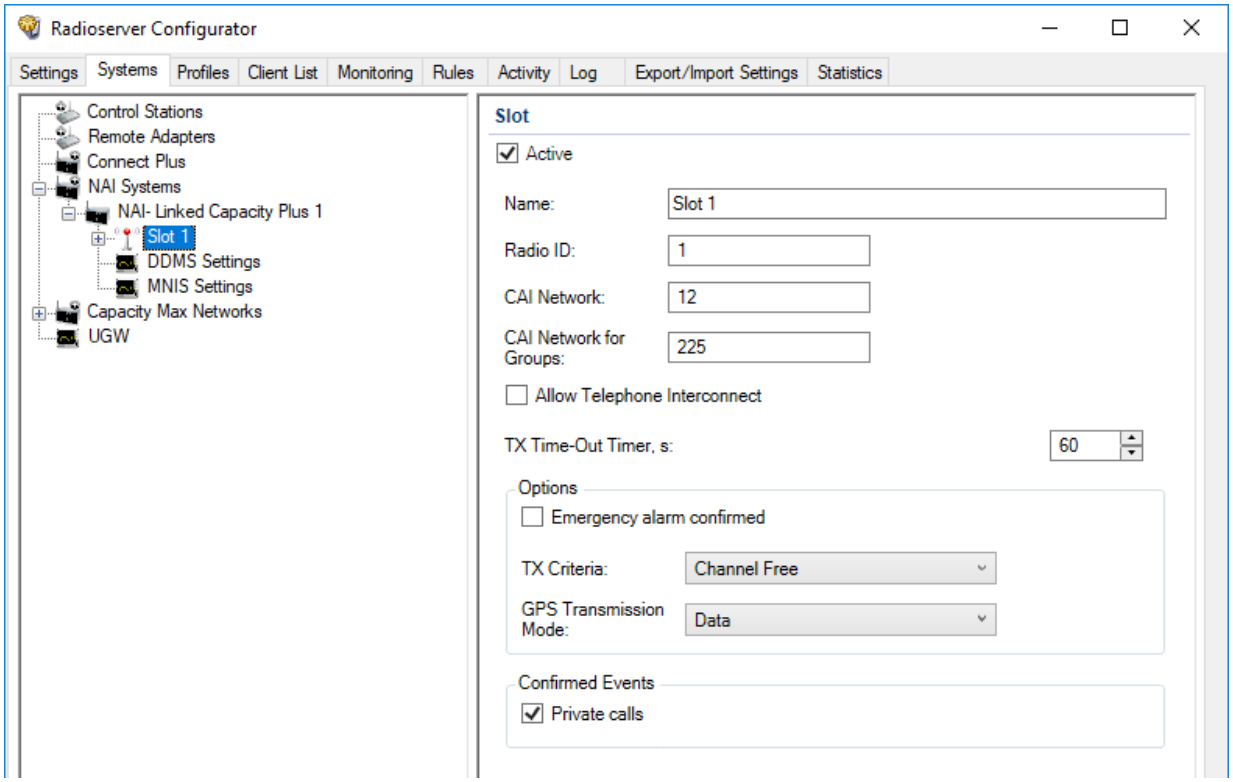
- Configure the network settings. For details, see Adding and Editing LCP Connection.
- From radio codeplugs, obtain the following data:

- CAI and CAI group values.
- Voice transmission duration.
- CSBK data settings (active or inactive).

- From the MNIS configuration file, obtain information on the site coordinates (configured or not).
- Determine necessity for the following radioserver functions:
  - Radio system integration with phone systems.
  - Emergency alarms and calls acknowledgment.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***NAI Systems*** → ***<system name>***, and then click ***<slot name>***.
   The identification parameters appear in the right pane of the tab.



3. In the right pane, select the ***Active*** check box.
4. In the ***Name*** field, type the title that will represent the radio network in SmartPTT Dispatcher.
5. Type the SmartPTT Radioserver identification parameters:
   a. In the ***Radio ID*** field, type the radio ID that is reserved for SmartPTT Radioserver.
   b. In the ***CAI Network*** field, type the CAI ID.
   c. In the ***CAI Network for Groups*** field, type the CAI Group ID.
6. Select the ***Allow Telephone Interconnect*** check box to provide voice calls feature between the radio system and phone system.
7. In the ***TX Time-Out Timer, s*** field, enter the maximum duration (in seconds) of voice transmissions in the radio network.

8. In the ***Options*** area, select the ***Emergency alarm confirmed*** check box to enable emergency confirmation by SmartPTT Radioserver.
9. From the ***TX Criteria*** list, select one of the following options:

If the call initiator must transmit only when no other transmissions are detected over the radio channel,	select *Channel Free*.
If the call initiator must interrupt another participant of the radio network according to the selected MSI or DMR protocol,	select *Tx Interrupt*.
If the call initiator must completely ignore other transmissions over the radio channel,	select *Always*.

10. From the ***GPS Transmission Mode*** list, select one of the following options:

If CSBK data is used in the radio system and site coordinates are configured in MNIS,	select *Enhanced CSBK*.
If CSBK data is used in the radio system but site coordinates are not configured in MNIS,	select *CSBK*.
In CSBK data is not used in the radio system or outdoor positioning service is used together with indoor positioning service,	select *Data*.

11. In the ***Confirmed Events*** area, select the ***Private calls*** check box to support private call request confirmation.
12. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (***  ***)***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (******)*** or ***Restart (******)***.

6.4.2.4 Adding and Editing Groups in LCP

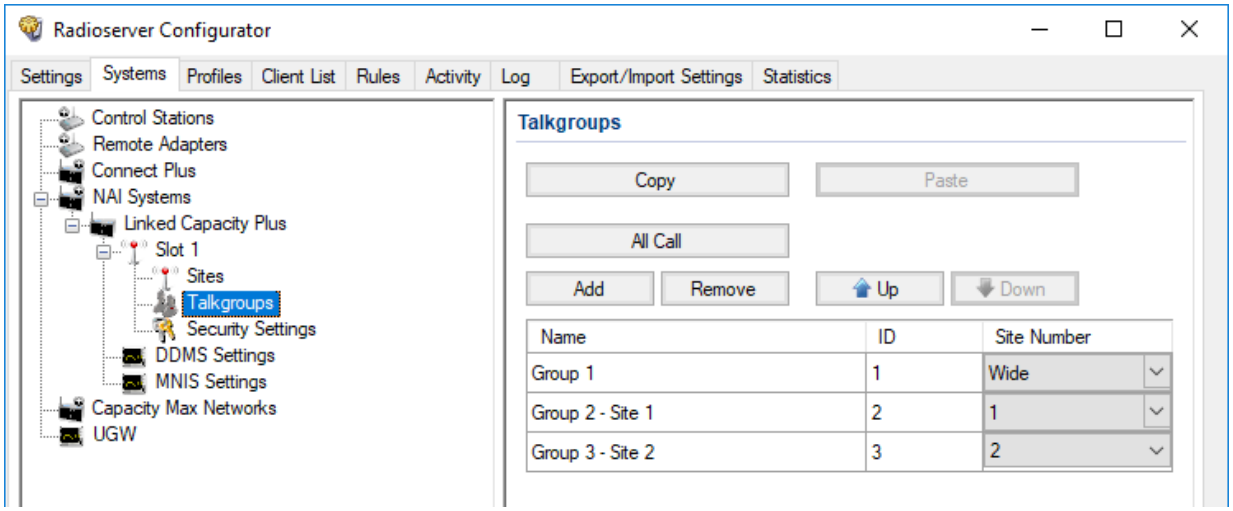
Follow the procedure to configure talkgroups and All Calls in the radio system.

Prerequisites:

- From repeater codeplugs, obtain the list of talkgroups for each radio system site.
- Determine system-wide and site-specific All Calls necessity.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***NAI Systems*** → ***<system name>*** → ***<slot name>***, and then select ***Talkgroups***.
   The group settings appear in the right pane.



3. In the right pane, perform one of the following actions:

To add a new talkgroup,	click ***Add***.
To add a new All Call,	click ***All Call***.
To edit an existing talkgroup or All Call,	proceed to the next step of the procedure.

4. In the table, in the desired row, perform the following actions:
   a. In the ***Name*** column, double-click the current name, and then type the desired name.
   b. In the same row, in the ***ID*** column, double-click the current ID, and then type the desired ID.

Important
The group ID must be unique across all slots of NAI systems.

NOTE
SmartPTT Radioserver Configurator does not show All Call IDs.

   c. In the same row, from the ***Site Number*** list, select one of the following options:

To configure system-wide talkgroup or All Call,	select *Wide*.
To configure site-specific talkgroup or All Call,	select the desired site number (site ID).

5. *(Optional)* Using ***Up*** and ***Down*** buttons, reorder rows in the table.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (*** ***)***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (*** ***)*** or ***Restart (*** ***)***.

6.4.2.5 Configuring Voice Calls on Sites

Follow the procedure to configure voice call routing prioritization from the phone system to the radio system. The procedure is applicable for group calls only, for site-specific groups that have no site ID in the call request. For details, see Phone Call Routing Priority.

Prerequisites:

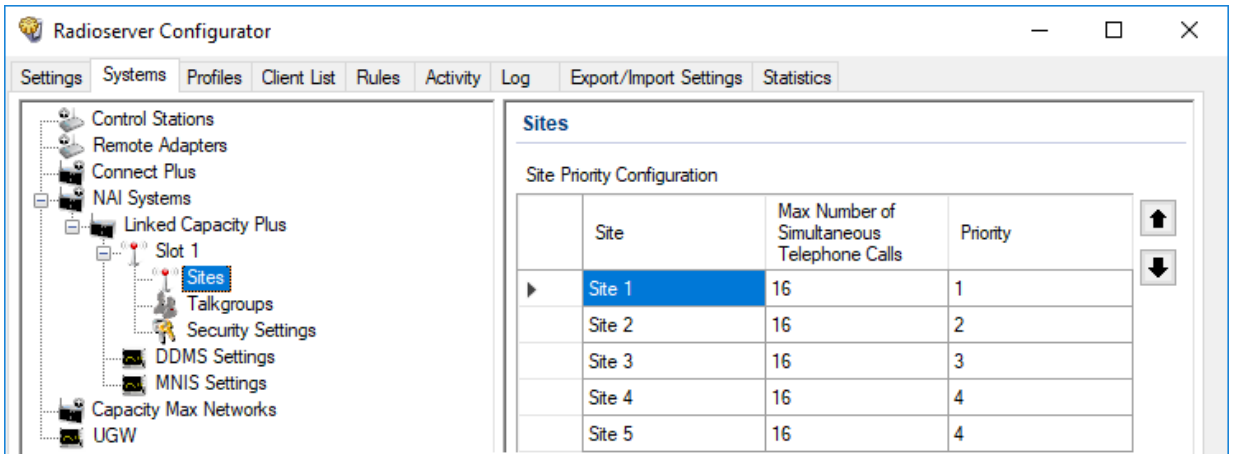
- Determine the maximum number of simultaneous phone calls on each radio system site.

Important
Maximum number of calls must be 2S−1, where S is a number of repeaters on the site.

- Determine per-site priority for group call routing.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***NAI Systems*** → ***<system name>***, and then click ***Sites***.
   The site settings appear in the right pane.



3. In the right pane, in the ***Max Number of Simultaneous Voice Calls*** column, for the desired site, double-click the current number of simultaneous calls, and then type the desired number of calls.
4. Repeat step 3 for all the desired sites.
5. Configure call routing prioritization:
   a. Click the empty cell on the left of the site name.
   b. Perform one of the following actions:

To increase the routing prioritization for the site,	on the right of the table, click ***Increase priority*** ( ).
To decrease the routing prioritization for the site,	on the right of the table, click ***Decrease priority*** ( ).

6. Repeat step 5 for all of the sites.
7. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration*** ( ).

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start*** ( ) or ***Restart*** ( ).

6.4.2.6 Configuring Encryption in LCP

Follow the procedure to support encrypted transmissions decoding and encoding in SmartPTT.

Prerequisites:

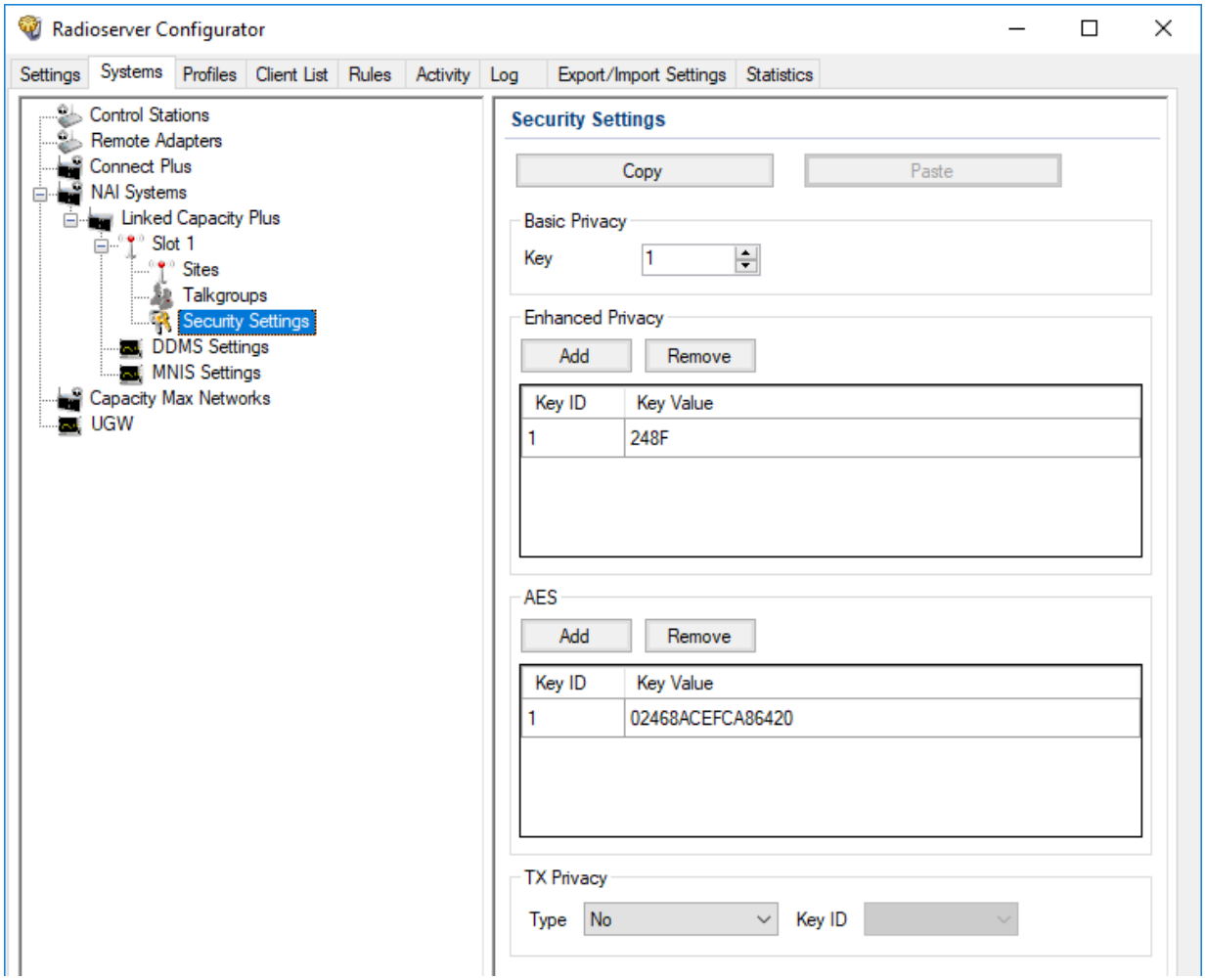
- Obtain security key IDs and values for all encryption types used in the radio system.

Important
MOTOTRBO configuration tools do not show the configured security/privacy keys for security reasons.

- Determine the key that will be used to encode dispatcher transmissions.
- To configure symmetric keys, install the corresponding SmartPTT license.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***NAI Systems*** → ***<system name>*** → ***<slot name>***, and then select ***Security Settings***.
   The security key settings appear in the right pane.



3. In the right pane, in the ***Basic Privacy*** area, perform the following actions:

If basic encryption is used in the radio system,	in the ***Key*** field, enter the value of the basic security key.
If basic encryption is not used in the radio system,	proceed to the next step of the procedure.

4. Add a new security key to the dispatch subsystem:

To add a new enhanced key,	perform the following actions: 1. In the ***Enhanced Privacy*** area, click ***Add***. 2. In a new row of the table, in the ***Key ID*** column, double-click the current ID, and then type the desired ID. 3. In the same row, in the ***Key Value*** column, double-click the current value, and then type the desired value.
To add a new symmetric (AES-compliant) key,	perform the following actions: 1. In the ***AES*** area, click ***Add***. 2. In a new row of the table, in the ***Key ID*** column, double-click the current ID, and then type the desired ID. 3. In the same row, in the ***Key Value*** column, double-click the current value, and then type the desired value.

5. *(Optional)* Modify an existing security key:

To edit the basic security key,	in the ***Basic Privacy*** area, in the ***Key*** field, enter the desired basic security key.
To modify an existing enhanced security key,	perform the following actions: 1. In the ***Enhanced Privacy*** area, in a desired row of the table, in the ***Key ID*** column, double-click the current ID, and then type the desired ID. 2. In the same row, in the ***Key Value*** column, double-click the current value, and then type the desired value.
To modify an existing symmetric (AES-compliant) key,	perform the following actions: 1. In the ***AES*** area, in a desired row of the table, in the ***Key ID*** column, double-click the current ID, and then type the desired ID. 2. In the same row, in the ***Key Value*** column, double-click the current value, and then type the desired value.

6. Configure outgoing transmission encryption (from dispatchers to the radio network):

To use basic security key,	from the ***Type*** list, select *Basic*.
To use one of enhanced security keys,	perform the following actions: 1. From the ***Type*** list, select *Enhanced*. 2. From the ***Key ID*** list, select the ID of the desired key.

To use one of symmetric (AES-compliant) security keys,	perform the following actions: 1. From the ***Type*** list, select *AES (Symmetric Key)*. 2. From the ***Key ID*** list, select the ID of the desired key.
To perform unencrypted (clear) transmissions,	from the ***Type*** list, select *No*.

7. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

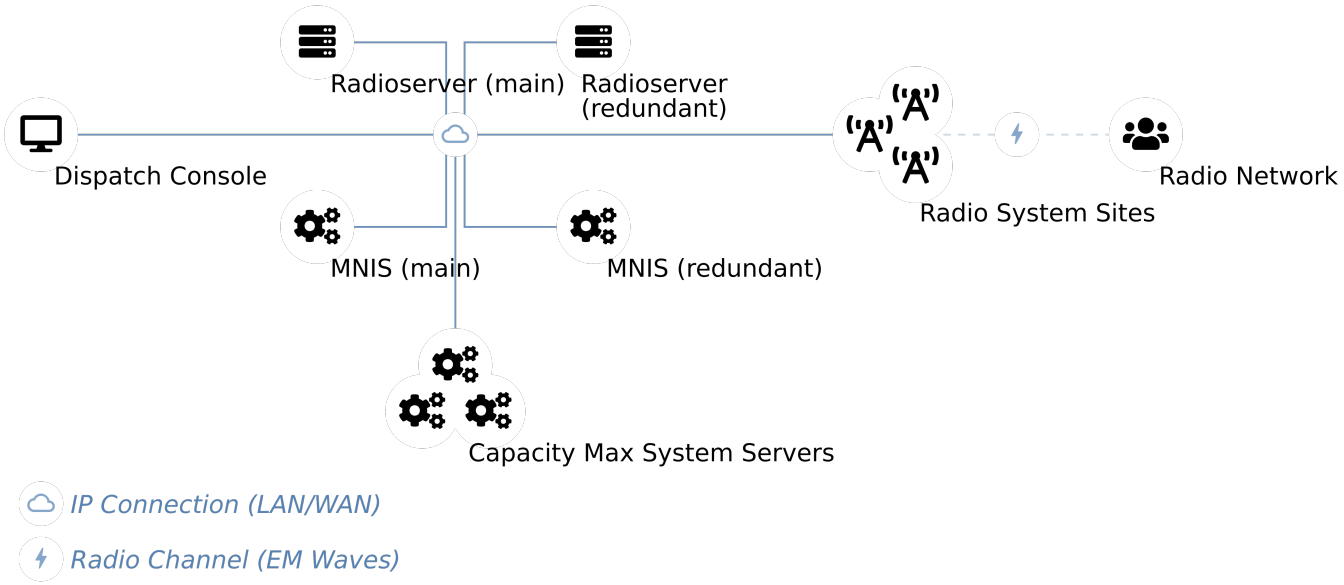
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- Duplicate security keys for other slots of the system. For details, see Settings Duplication.

6.5 Capacity Max

MOTOTRBO™ Capacity Max is a multisite trunked radio system from Motorola Solutions. The system is compliant with ETSI DMR Tier III standards, supports up to 900 sites with up to 3,000 users per site. It provides connections alternation/redundancy and information security. For details, visit the MOTOTRBO™ Capacity Max web page of the Motorola Solutions website.

Capacity Max is available to SmartPTT over the Capacity Max System Server device (CMSS) connection. CMSS is a controller that provides the following communication interfaces:

- Presence Server (information about radios and their online/offline status)
- MNIS VRC Gateway (voice calls and radio signaling commands)



Each CMSS provides only one Presence Server and/or one MNIS VRC Gateway interfaces. For each alternate/redundant or additional interface, another CMSS is required.

Text messages, positioning information, and telemetry data are provided by the MNIS Data Gateway. It is represented by the MOTOTBRO Network Interface Service (MNIS), a Windows service from Motorola Solutions that is hosted on a regular computer outside CMSS.

6.5.1 Capacity Max Feature Overview

Capacity Max provides and supports the following features:

- Private and group voice calls (including system-wide and site-specific All Calls)
- Radio commands
- Telephone interconnect
- Voice notifications
- Voice recording
- Text messaging.
- Outdoor (GNSS) positioning services, including coordinates transfer over the control channel (USBD Polling).

NOTE
The number and frequency of location updates over the control channel is limited. Also, keep in mind that these updates cannot be used for building the coverage map.

- Temporary Talkgroup creation over the Dynamic Group Number Assignment.
- Data acquisition and remote control over MOTOTRBO radios.
- Wireless traffic encryption using MOTOTRBO enhanced privacy or AES-compliant privacy.
- Presence Server, MNIS VRG Gateway, and MNIS Data Gateway alternation/redundancy.
- Secure connection between SmartPTT Radioserver and CMSS.

For network monitoring, the following features are provided:

- Over-the-air traffic monitoring (without splitting by radio channels).
- Network topology visualization.

NOTE
SmartPTT does ***not*** show on-site/fielded radios on the topology diagram.

- Statistical information gathering (system performance, alarm statistics), reports generation.

Licensing

To support Capacity Max, SmartPTT Radioserver requires the following licenses:

Capacity Max Presence Connectivity
Each license unlocks the connection to the Presence Server and up to 4 alternate/redundant Presence Servers (optional).

Capacity Max Voice Connectivity
Each license unlocks the connection to 15 MNIS VRC Gateways. Such a great amount of gateways may be needed in systems with high call rate. Each gateway may have an optional alternate/redundant gateway.

Capacity Max Data Connectivity
Each license unlocks the connection to the MNIS Data Gateway and the alternate/redundant MNIS Data Gateway (optional).

AES Encryption Support
The license makes symmetric security keys available for configuration.

For information on CMSS licenses, contact the Motorola Solutions representative in your region.

SmartPTT Radioserver ignores Radio Stun, Radio Revive, and Radio Kill commands sent to SmartPTT Radioserver ID and SmartPTT client IDs.

6.5.2 Capacity Max Configuration Brief

The following information is required to start Capacity Max Configuration in SmartPTT.

Identifier Reservation

In Capacity Max, SmartPTT Radioserver requires a numeric ID that must be unique across all Radio IDs in the whole radio system. The ID should be the same for main and alternate/redundant SmartPTT Radioserver. If radio subscribers call to this ID, SmartPTT Radioserver will accept the call and will share/retransmit it to all active operators.

To deliver a private communication between dispatchers and radio subscribers, unique IDs must be reserved to dispatchers. IDs must be set on the ***Clients*** tab of SmartPTT Radioserver Configurator. In the document, these IDs are referred to as “Dispatcher IDs”.

Configuration Software

Configuration of Capacity Max in SmartPTT requires the following software:

- SmartPTT Radioserver Configurator that provides SmartPTT Radioserver settings.
- Radio Management Configuration Client (RMCC) that provides the radio system settings and CMSS settings.
- *(Optional)* If you do not use connection over TCP, you need SmartPTT MNIS Data Gateway Relay that routes data between the remote MNIS Data Gateway and SmartPTT Radioserver.

Configuration Process

The process includes the following actions:

1. Radio system addition and general SmartPTT Radioserver configuration. For details, see Configuring Connection to Capacity Max.
2. Presence Server connection. For details, see Connecting to Presence Servers.
3. MNIS Data Gateway connection. For details, see Connecting to Data Gateways.
4. MNIS VRC Gateway connection. For details, see Connecting to MNIS VRC Gateways.
5. Group call recipients configuration. For details, see Adding and Editing Groups in Capacity Max.
6. Temporary Talkgroup configuration. For details, see Adding and Editing Temporary Talkgroups.
7. Security keys addition. For details, see Configuring Encryption in Capacity Max.
8. Correct settings synchronization between the main and alternate/redundant SmartPTT Radioservers.

Instructions provide an information on how to obtain CMSS settings if required.

6.5.3 Configuring Connection to Capacity Max

Follow the procedure to add Capacity Max to the SmartPTT Radioserver configuration.

Prerequisites:

- Determine the radioserver ID as a virtual radio.
- From Capacity Max configuration, obtain the following information:
  - SmartPTT Radioserver ID
  - Availability of the voice and data services
  - If CSBK Data are used or not
  - Voice transmit settings
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- To configure the monitoring of voice calls and data transmissions in the Capacity Max network, first enable the monitoring service. For details, see Monitoring.

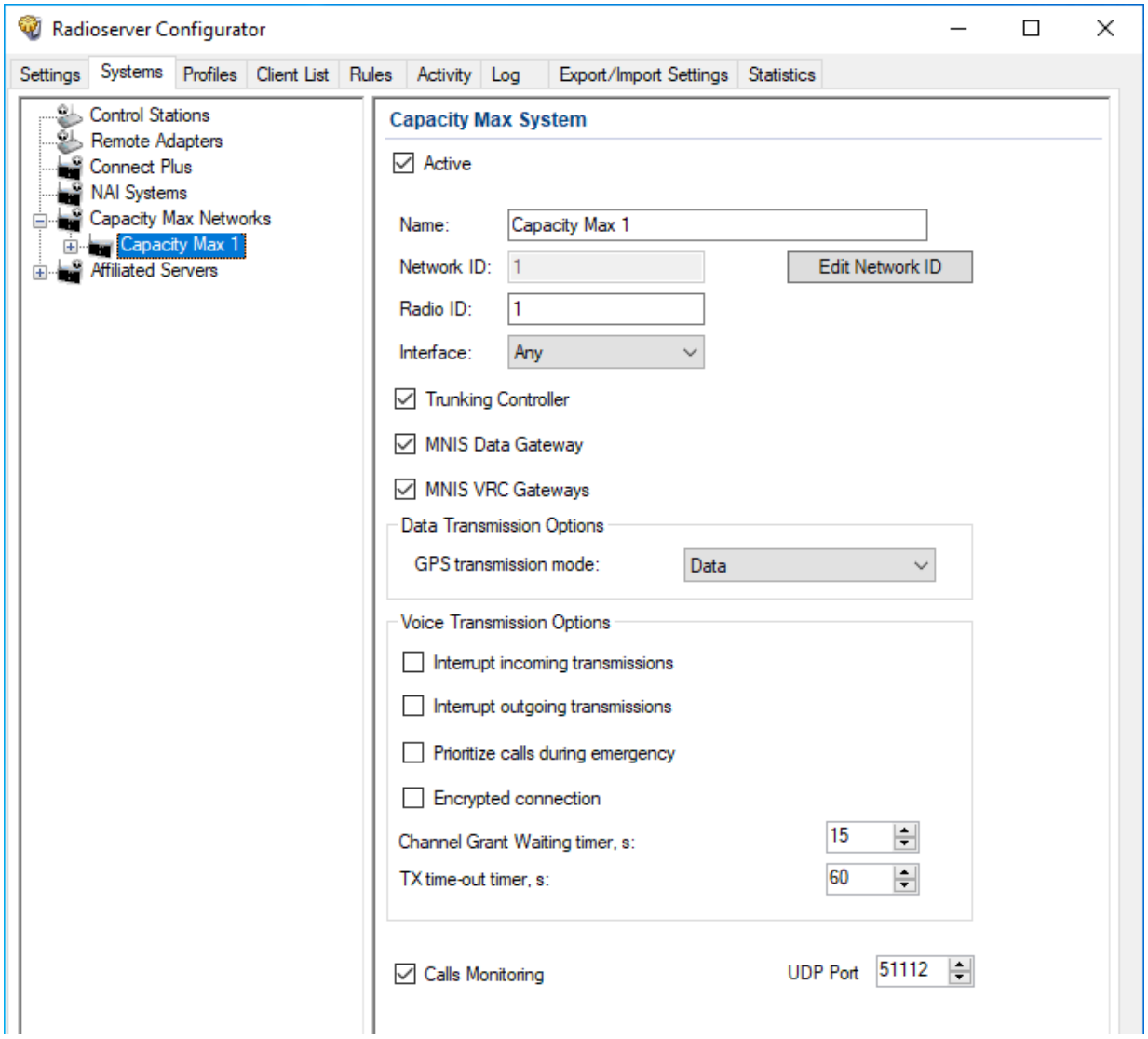
Contact the Motorola Solutions representative in your region to obtain the configured parameters.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. Perform one of the following actions:

To add a new Capacity Max network,	right-click ***Capacity Max Networks***, and then click ***Add***.
To edit an existing Capacity Max network,	expand ***Capacity Max Networks***.

3. Under the expanded ***Capacity Max Networks*** node, click the desired network.
   The general network settings appear in the right panel.



4. Click a new subnode.
5. In the right pane, configure the general SmartPTT Radioserver settings:
   a. Select the ***Active*** check box.
   b. In the ***Name*** field, type the radio network name.
   c. Leave the ***Network ID*** parameter unchanged.
   d. In the ***Radio ID*** field, type the identifier of the radioserver as a virtual radio.

Important
Do not assign this ID to a client or radio in any radio network.

6. Show Capacity Max service settings:
   a. Select the ***Trunking Controller*** check box to show the Presence Server connection settings.
   The ***Trunking Controller*** subnode appears.
   b. Select the ***MNIS Data Gateway*** check box to show the MNIS Data Gateway connection and communication settings.
   The ***MNIS Settings*** subnode appears.
   c. Select the ***MNIS VRC Gateway*** check box to show the MNIS VRC Gateway connection and communication settings.
   The ***MNIS VRC Gateways*** subnode appears.

7. To configure GPS data format, in the ***Data Transmission Options*** area, perform one of the following actions:

If CSBK Data are configured in the radio network,	from the ***GPS Transmission mode*** list, select *Enhanced CSBK*.
If no CSBK Data are configured,	from the ***GPS Transmission mode*** list, select *Data*.
If no data gateway will be used in Capacity Max,	leave the ***GPS Transmission mode*** parameter unchanged.

8. In the ***Voice Transmission Options*** area, configure voice features in Capacity Max:
   a. To enable the capability to interrupt voice transmissions from radios with dispatcher voice transmissions or voice notifications, select the ***Interrupt incoming transmissions*** check box.
   b. To enable the capability to interrupt voice transmissions or voice notifications from dispatcher with voice transmissions from radios, select the ***Interrupt outgoing transmissions*** check box.
   c. To increase call priority for radios in the emergency mode, select the ***Prioritize calls during emergency*** check box.
   d. To secure voice traffic between SmartPTT Radioserver host and CMSS, select the ***Encrypted connection*** check box.
   e. In the ***Channel Grant Waiting Timer, s*** field, enter the channel grant timeout.
   f. In the ***TX time-out timer field, s***, enter the voice transmission timeout.
9. *(Optional)* To enable the monitoring of voice calls and data transmissions, perform the following actions:
   a. Select the ***Calls Monitoring*** check box.
   b. In the ***UDP Port*** field, enter the number of the UDP port that the SmartPTT radioserver will use to receive data from the Capacity Max network. The default value is *51112*.
10. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

6.5.4 Connecting to Presence Servers

Follow the procedure to connect the SmartPTT Radioserver to the Presence Server.

Prerequisites:

From the Capacity Max configuration, obtain the following information:

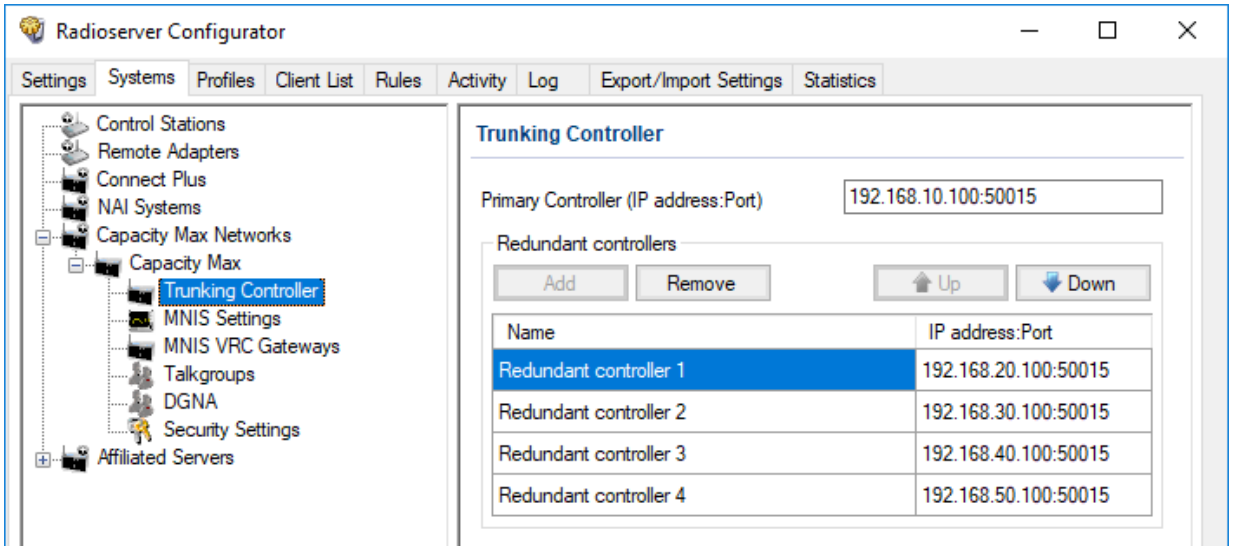
- IPv4 address and port number of the main/primary Presence Server interface.
- IPv4 addresses and port numbers of the all alternate/redundant Presence Server interfaces.

Contact the Motorola Solutions representative in your region to obtain the configured parameters.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. Access Presence Server connection settings:
   a. On the tab, in the left pane, expand ***Capacity Max Network***, and then select ***<your network>***.
   b. In the right pane, select the ***Trunking Controller*** check box, or ensure that it is already selected.

c. In the left pane, expand ***<your network>***, and then select ***Trunking Controller***.
The Presence Server settings appear in the right pane.



3. In the right pane, in the ***Primary Controller*** field, type <Main Presence Server IP>:<Main Presence Server Port>.
4. In the ***Redundant controllers*** area, configure the connection to alternate/redundant Presence Servers:
   a. Perform one of the following actions:

To add a new connection,	click Add.
To edit an existing connection,	proceed to the next step of the procedure.

   b. In the new row, in the ***IP address:Port*** column, double-click the default value, and type <Alt. Presence Server IP>:<Alt. Presence Server Port>.
   c. *(Optional)* In the ***Name*** column, double-click the default value, and type the ***Presence Server*** name.

NOTE
Names of the alternate/redundant Presence Servers are used in the system messages of SmartPTT Dispatcher.

5. If more than one alternate Presence Server is configured in Capacity Max, repeat the previous step for the remaining Presence Servers.
6. *(Optional)* Using ***Up*** and ***Down*** buttons, reorder rows in the table.
7. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (*** ***)***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (*** ***)*** or ***Restart (*** ***)***.
- In the firewall software on the radioserver computer, unlock the set TCP ports. For details, see Radioserver Host.

6.5.5 Connecting to Data Gateways

Follow the procedure to connect SmartPTT Radioserver to the MNIS Data Gateway.

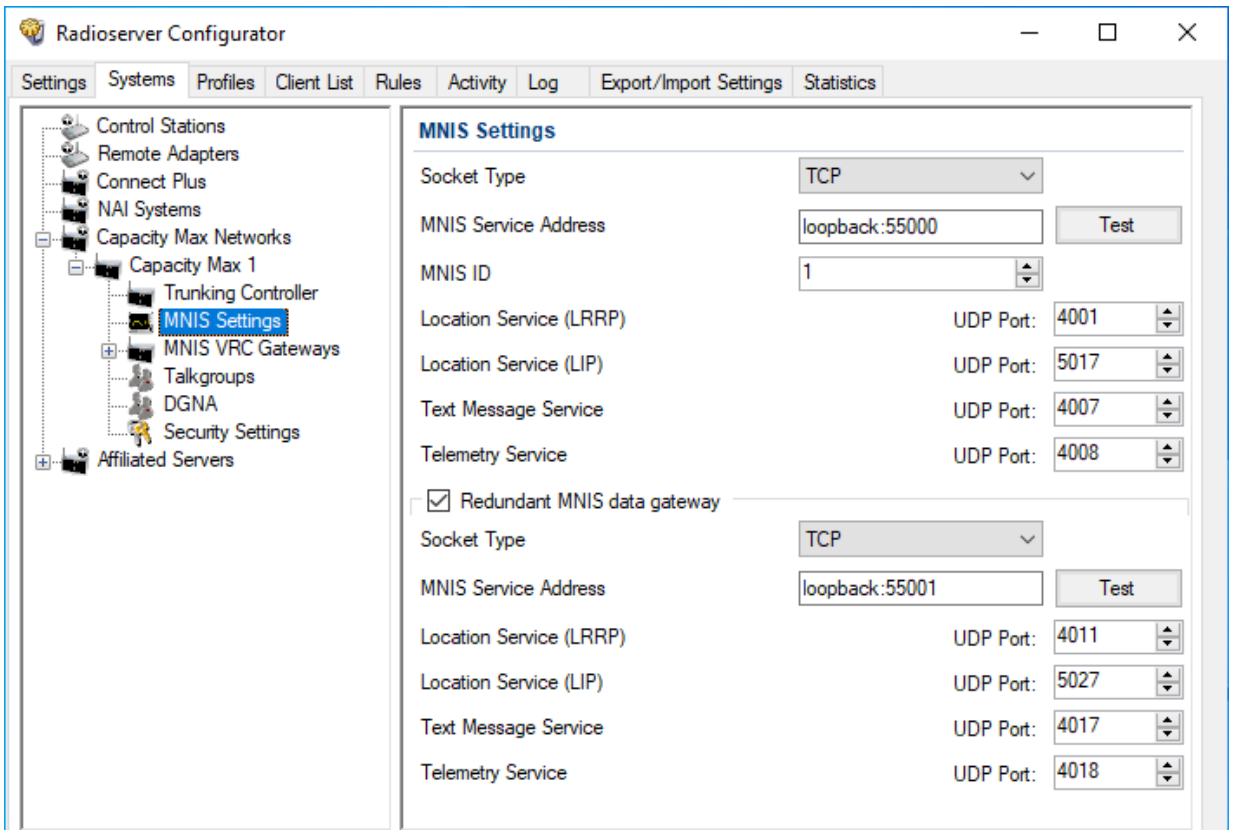
Prerequisites:

- From the Capacity Max configuration, obtain the following information:
  - Main/primary data gateway settings.
  - If available, alternate/redundant data gateway settings.

  Contact the Motorola Solutions representative in your region to obtain the configured parameters.
- For connection using SmartPTT MNIS Data Gateway Relay, from its configuration, obtain the IP address and port. For details, see Configuring MNIS Data Gateway Relay.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. Access data gateway settings:
   a. On the tab, in the left pane, expand ***Capacity Max Networks***, and then select ***<your network>***.
   b. In the right pane, select the ***MNIS Data Gateway*** check box, or ensure that it is selected.
   c. In the left pane, expand ***<your network>***, and then select ***MNIS Settings***.
   The data gateway settings appear in the right pane.



3. Connect to the main MNIS Data Gateway:

To connect over the TCP interface,	perform the following actions: 1. From the ***Socket Type*** list, select *TCP*. 2. In the ***MNIS Service Address*** field, type <MNIS host IP address or domain name>:<MNIS Control Interface TCP Port>. 3. *(Optional)* To check connection between the radioserver and MNIS service, click ***Test***, then, in the ***Test Connection*** window, wait for the check result and click ***Close***.
To connect over the virtual network interface if the MNIS service and SmartPTT Radioserver are hosted on the same computer,	perform the following actions: 1. From the ***Socket Type*** list, select *Tunnel Interface (Legacy)*. 2. From the ***Interface*** list, select the MNIS Tunnel IP address. The default MNIS Tunnel IP is *192.168.10.1*. 3. In the ***MNIS Service Address*** field, type <SmartPTT Radioserver host IP address or domain name>:<MNIS Control Interface TCP Port>. 4. *(Optional)* To check connection between the radioserver and MNIS service, click ***Test***, then, in the ***Test Connection*** window, wait for the check result and click ***Close***.
To connect using SmartPTT MNIS Data Gateway Relay if the MNIS service and SmartPTT Radioserver are hosted on different computers,	perform the following actions: 1. From the ***Socket Type*** list, select *Data Gateway Relay (Legacy)*. 2. In the ***MNIS Service Address*** field, type <MNIS host IP address or domain name>:<MNIS Control Interface TCP Port>. 3. In the ***MNIS Relay Server network address*** field, type <MNIS host IP>:<SmartPTT MNIS Data Gateway Relay Port>. 4. *(Optional)* To check connection between the radioserver and MNIS service, click ***Test***, then, in the ***Test Connection*** window, wait for the check result and click ***Close***.

4. Configure MNIS Data Gateway settings:
   a. In the ***MNIS ID*** field, enter MNIS Application ID.
   b. In the ***Location Service (LRRP)*** field, enter the number of the MNIS port used to receive radio coordinates over LRRP and send location requests.
   c. In the ***Text Message Service*** field, enter the number of the MNIS port used to receive and send text messages.
   d. In the ***Telemetry Service*** field, enter the number of the MNIS port used for data acquisition and remote control commands.

5. Configure the alternate/redundant MNIS Data Gateway:
   a. Select the ***Redundant MNIS data gateway*** check box.
   b. With controls in the ***Redundant MNIS data gateway*** area, perform the actions described in step 3.

Important
The *Tunnel Interface (Legacy)* socket type cannot be selected for the alternate/redundant data gateway, if it is already selected for the main MNIS Data Gateway.

   c. With the remaining controls of the area, perform the actions described in step 4.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- In the firewall software on the radioserver computer, unlock the set TCP and UDP ports. For details, see Radioserver Host.

6.5.6 Connecting to MNIS VRC Gateways

Follow the procedure to connect SmartPTT Radioserver to MNIS VRC Gateway.

Prerequisites:

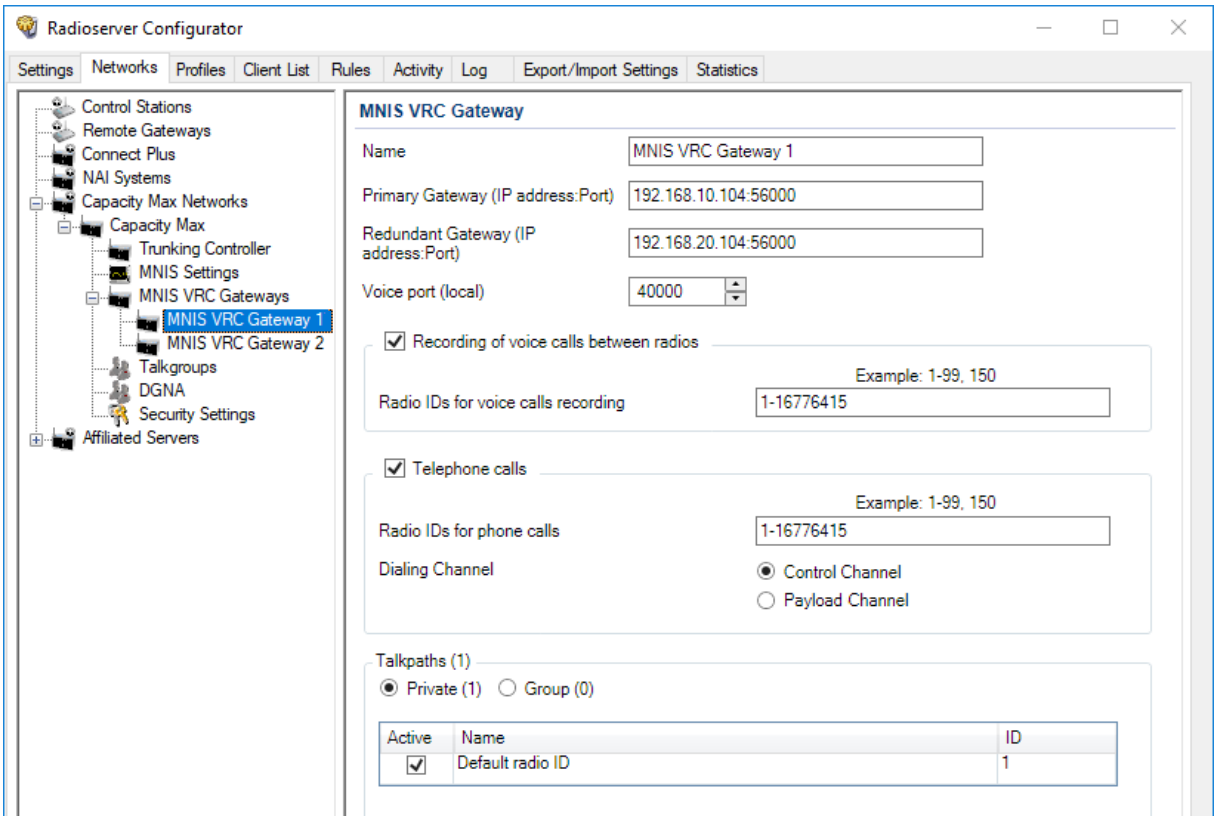
- From Capacity Max configuration, obtain the following information:
  - IP address and port for each main/primary MNIS VRC Gateway.
  - IP address and port for each alternate/redundant MNIS VRC Gateway.
  - Radio IDs affiliated to voice logging, phone interconnect, and call initiation over the gateways.
- *(Optional)* Select the mode for telephone calls in the radio system. Make sure that in the MOTOTRBO™ trunking controller configuration file, the corresponding option is selected for the ***Phone Call Setup Method*** parameter: ***Dialing Digits on Control Channel (as per DMR3)*** or ***Dialing Digits on Payload Channel***.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. Access MNIS VRC Gateway settings:
   a. On the tab, in the left pane, expand ***Capacity Max Networks***, and then select ***<your network>***.
   b. In the right pane, select the ***MNIS VRC Gateway*** check box, or ensure that it is selected.
   c. In the left pane, expand ***<your network>***.
   The ***MNIS VRC Gateways*** subnode appears.
3. Perform one of the following actions:

To add a new gateway,	right-click ***MNIS VRC Gateways***, and then select ***Add***.
To edit the existing gateway settings,	expand ***MNIS VRC Gateways***.

4. Under the expanded ***MNIS VRC Gateways*** node, click the desired subnode.



5. Modify the gateway connection settings:

   a. In the right pane, in the ***Name*** field, type the gateway name.

NOTE
Gateway names are used in system messages in SmartPTT Dispatcher.

   b. In the ***Primary Gateway (IP address:Port)*** field, type <Main Gateway IP>:<Main Gateway Port>.

   c. In the ***Redundant Gateway (IP address:Port)*** field, type <Alt. Gateway IP>:<Alt. Gateway Port>.

   d. In the ***Voice port (local)*** field, enter the free UDP port of the SmartPTT Radioserver host.

6. Configure voice recoding for the gateway:

   a. Select the ***Recoding of voice calls between radios*** check box.

   b. In the ***Radio IDs for voice calls recording*** field, type Radio IDs which calls must be recorded.

Important
For voice recording, SmartPTT must have the “Voice Recording” or “NexLog” license. For details, contact Elcomplus, Inc. representative in your region.

7. Configure telephone line access for radio users over the gateway:

   a. Select the ***Telephone calls*** check box.

   b. In the ***Radio IDs for phone calls*** field, type IDs of radios that must be able to receive and initiate phone calls.

   c. Select a mode for telephone calls:

To use a control channel for telephone calls between radio and telephone subscribers,	select ***Control Channel***. This mode is DMR Tier III standard and available for any DMR-compliant radios. The mode is

	selected by default.
To use a payload channel for telephone calls between radio and telephone subscribers,	select ***Payload Channel***. This mode is a proprietary Motorola Solutions standard and only available for MOTOTRBO™ radios.

Important
For telephone calls, SmartPTT must have the “Telephone Interconnect Service” license. For details, contact Elcomplus, Inc. representative in your region.

8. In the ***Talkpaths*** area, perform one of the following actions:

To configure talkpaths for specific IDs,	click ***Private***.
To view group talkpaths,	click ***Group***.

9. Configure the talkpaths utilization on the gateway:

To provide the talkpath for the ID,	in the table, in the ***Active*** column, select check boxes for the corresponding IDs.
To reject the talkpath provision for the ID,	in the table, in the ***Active*** column, clear check boxes for the corresponding IDs.

10. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Repeat the procedure to connect other MNIS VRC gateways.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- In the firewall software on the radioserver computer, unlock the set TCP and UDP ports. For details, see Radioserver Host.

6.5.7 Adding and Editing Groups in Capacity Max

Follow the procedure to add talkgroups to SmartPTT Radioserver, and configure site-specific and system-wide All Calls.

Prerequisites:

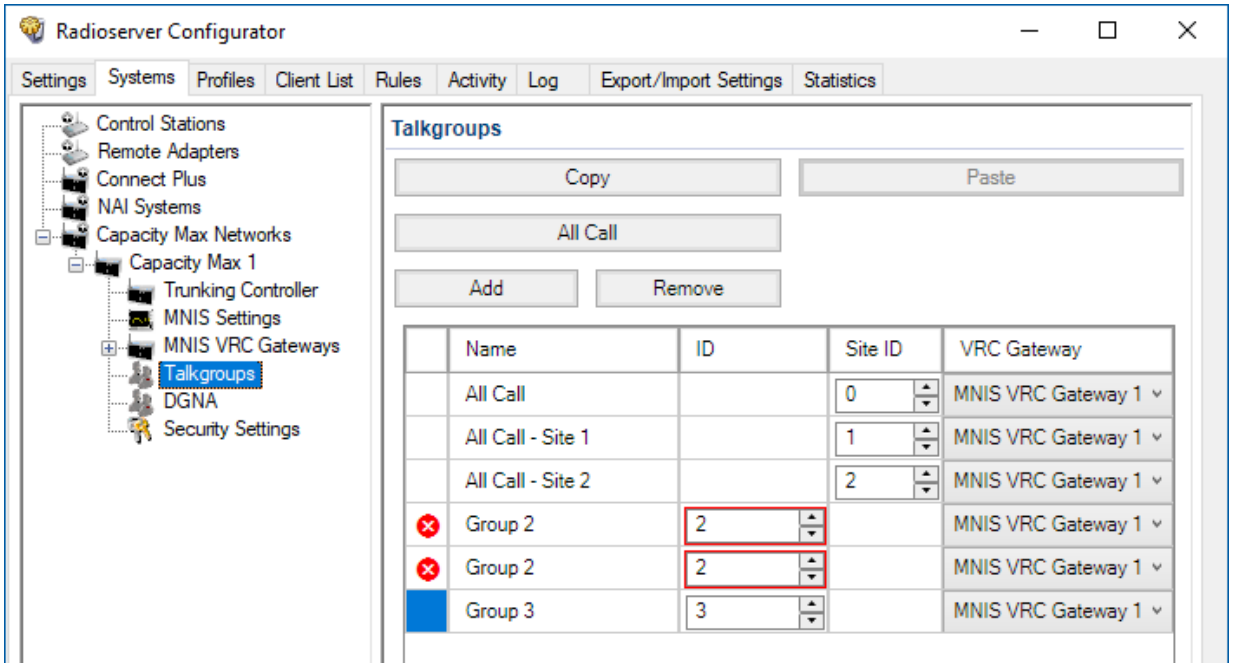
From the Capacity Max configuration, obtain the following information:

- Talkgroup IDs and their affiliation to Capacity Max sites and gateways.
- List of Site IDs to configure All Calls.

Contact the Motorola Solutions representative in your region to obtain the configured parameters.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. On the tab, in the left pane, expand ***Capacity Max Networks*** → ***<Your network>***, and then select ***Talkgroups***.



3. Perform the desired action:

To add a new talkgroup,	click ***Add***.
To add a new All Call,	click ***All Call***.
To edit the existing group or All Call,	proceed to the next step of the procedure.
To remove a talkgroup or All Call,	in the table, select the desired entry, and then click ***Remove***. Proceed to the next step of the procedure.

4. In the desired entry of the table, perform the following actions:
   a. In the ***Name*** column, double-click the current name of the talkgroup or All Call, and then type the desired name. Under this name, the talkgroup or All Call appear in SmartPTT Dispatcher.
   b. In the ***ID*** column, specify a unique talkgroup identifier obtained from the repeater configuration. The All Call identifier is hidden in the table and not editable. The range of possible values is from *0* to *16777214*.
   c. In the ***Site ID*** column, specify unique identifier of the site where the corresponding All Call will be available. The range of possible values is from *0* to *900*.
   d. In the ***VRC Gateway*** column, select the MNIS VRC Gateway that will route the talkgroup calls to SmartPTT Radioserver.
5. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

6.5.8 Adding and Editing Temporary Talkgroups

Follow the procedure to add a new temporary talkgroup or edit the parameters of an existing one.

Prerequisites:

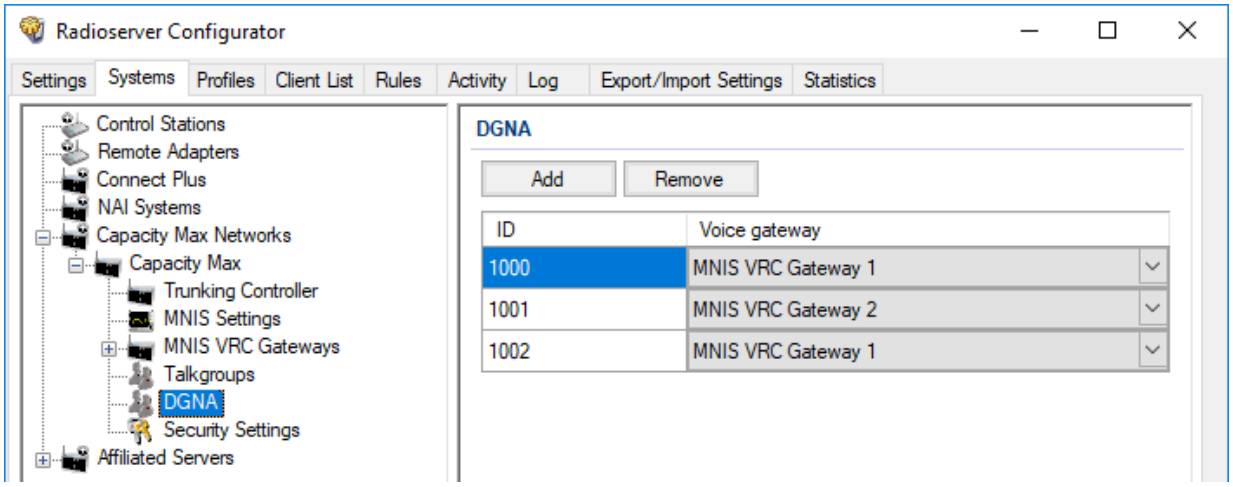
Ensure the following:

- DGNA is configured in Capacity Max.
- SmartPTT Radioserver has access to DGNA in Capacity Max. and, in particular, allowed for SmartPTT.
- Talkgroup IDs allocated in Capacity Max to be used as IDs of temporary talkgroups.

Contact the Motorola Solutions representative in your region to obtain the configured parameters.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. On the tab, in the left pane, expand ***Capacity Max Networks*** → ***<your network>***, and then select ***DGNA***.



3. Perform one of the following actions:

To add a new talkgroup,	in the right pane, click ***Add***.
To edit an existing talkgroup,	proceed to the next step of the procedure.

4. In the ***ID*** column, specify the Talkgroup ID that can be further assigned to a TTG.
5. In the same entry, in the ***Voice gateway*** column, select the desired voice gateway from the expandable list.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

6.5.9 Configuring Encryption in Capacity Max

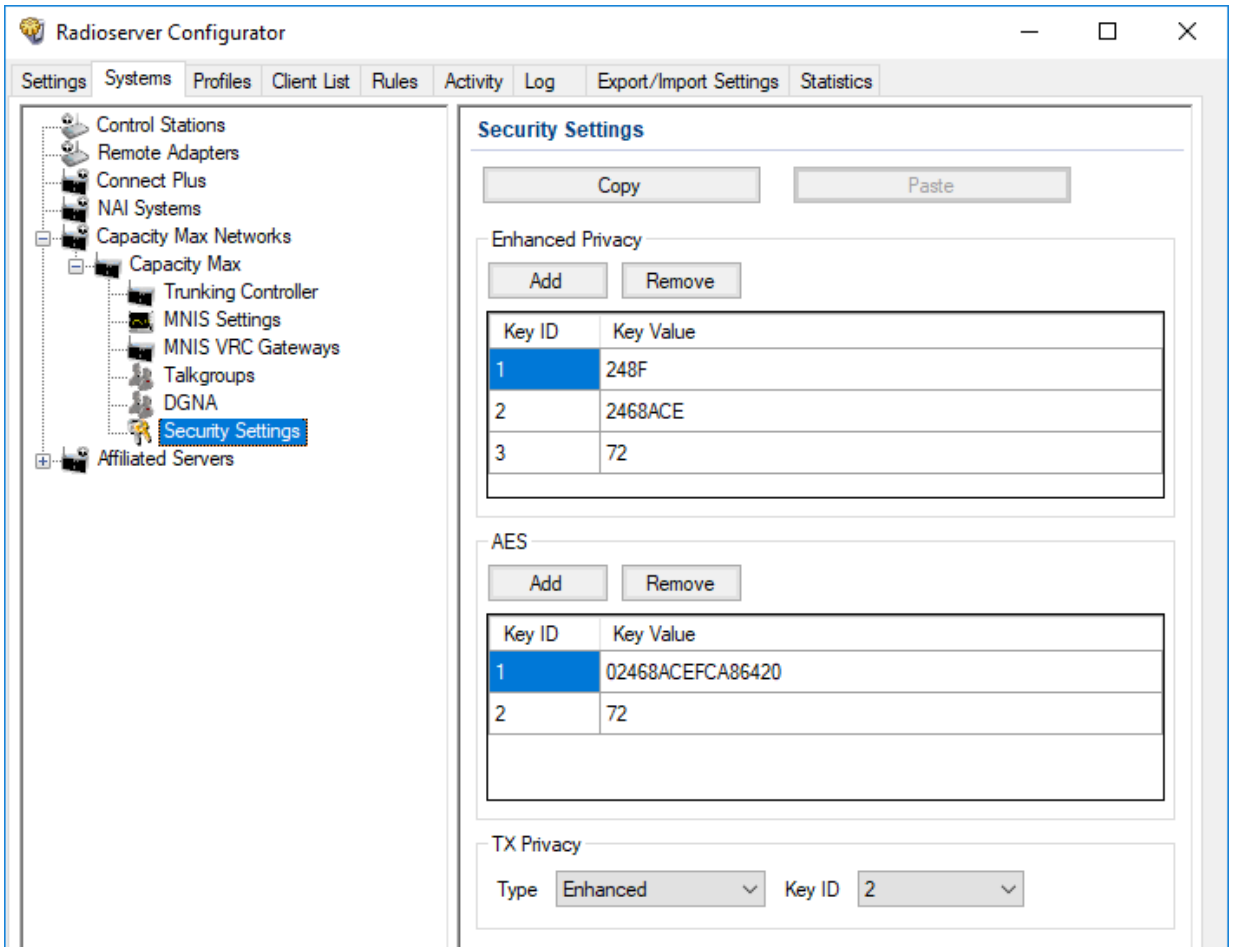
Follow the procedure to add security keys to SmartPTT Radioserver that will be used to decrypt incoming voice calls and encrypt outgoing voice calls.

Prerequisites:

- From the Capacity Max configuration, obtain security key IDs and values for all the supported encryption types. Contact the Motorola Solutions representative in your region to obtain the configured parameters.
- Determine the key that will be used to encrypt outgoing calls from SmartPTT Dispatcher users.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***System*** tab.
2. On the tab, in the left pane, expand ***Capacity Max Networks*** → ***<your network>***, and then select ***Security Settings***.



3. In the right pane, add the enhanced security keys:
   a. In the ***Enhanced Privacy*** area, perform one of the following actions:

To add a new key,	click ***Add***.
To edit an existing key,	proceed to the next step of the procedure.

   b. In the corresponding row of the table, in the ***Key ID*** column, double-click the default value, and then type the key ID.
   c. In the same row, in the ***Key Value*** column, double-click the default value, and then type the desired key value.

4. Add the AES security keys:
   a. In the ***AES*** area, perform one of the following actions:

To add a new key,	click ***Add***.
To edit an existing key,	proceed to the next step of the procedure.

   b. In the corresponding row of the table, in the ***Key ID*** column, double-click the default value, and then type the desired key ID.
   c. In the same row, in the ***Key Value*** column, double-click the default value, and then type the desired key value.
5. In the ***TX Privacy*** area, configure the encryption of dispatcher-initiated transmissions:

To use enhanced security keys,	perform the following actions: 1. From the ***Type*** list, select *Enhanced*. 2. From the ***Key ID*** list, select the desired key ID.
To use AES security keys,	perform the following actions: 1. From the ***Type*** list, select *AES (Symmetric Key)*. 2. From the ***Key ID*** list, select the desired key ID.
To perform clear transmissions,	from the ***Type*** list, select *No*.

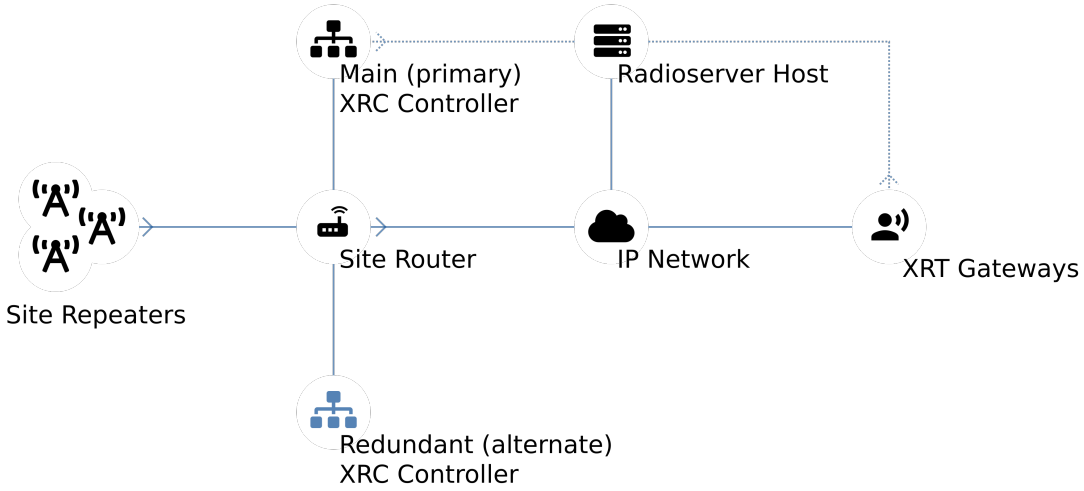
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

6.6 Connect Plus

Connect Plus is a digital (DMR) trunked radio system. It is a multisite system (provides great RF coverage) that hosts up to 2900 radios per site and provides up to 29 simultaneous voice calls per site. For details on the system and its capabilities, see MOTOTRBO™ Connect Plus on the Motorola Solutions website.



Each site hosts up to 15 repeaters controlled by XRC controller. Controller provides channel management and dispatch subsystems integration to the site. For inter-site and system-wide transmissions, controller accesses another XRC controller (on another site) and provides all the information to it over IP.

SmartPTT must be connected to at least one XRC controller of the system. If a site hosts two controllers (main and alternate), SmartPTT must be connected to the main controller only. It does ***not*** support the connection to alternate/redundant XRC controllers.

To increase the system connection reliability, SmartPTT can be connected to multiple XRC controllers at once. In this case, if one controller becomes unavailable, SmartPTT will automatically connect to another controller.

To access voice and radio command features, SmartPTT must connect not only to XRC controllers, but to XRT gateways as well. Each gateway provides a limited number of simultaneously monitored voice calls in the system. If required, SmartPTT is able to connect to multiple gateways at once.

6.6.1 SmartPTT Features in Connect Plus

Connect Plus provides the following features to SmartPTT:

- Information on radio presence in the network (ARS)
- Voice call reception and initiation (includes group calls and private calls)
- Emergency alarms and calls
- Radio location updates (includes revert channel support)
- Text messaging and job ticketing
- Radio commands

Important
Connect Plus does ***not*** support over-the-radio telemetry and over-the-radio remote control.

For Connect Plus, SmartPTT provides the following features:

- Simultaneous connection to multiple Connect Plus systems
- Integration with other radio systems using cross patches and bridging
- Event logging and voice recording
- Rules configuration

Important
Connect Plus does ***not*** allow integration with phone systems over SmartPTT. It uses XRI gateway for this purposes.
XRI gateways do ***not*** support dispatch software connection.

For network monitoring, the following features are provided:

- Network device monitoring over SNMP.
- Over-the-air traffic monitoring (without splitting by radio channels).
- Network topology visualization.

NOTE
SmartPTT does ***not*** show on-site/fielded radios on the topology diagram.

- Statistical information gathering (system performance, alarm statistics), reports generation.

6.6.2 Connect Plus Configuration

SmartPTT connection to the Connect Plus requires the following:

- Radio system compliance with the planning requirements
- Additional radio devices configuration.
- Dispatch software configuration.

Planning Requirements

To support SmartPTT connection, the radio system must comply with the following requirements:

- All radios and repeaters must have the same CAI IDs and CAI Group IDs.
- At least one repeater radio ID must be unused.
- At least one radio ID must be unused.
- Router that connects XRC controller and a radioserver must support Network Address Translation (NAT).
- Router that connects XRT gateways and a radioserver must support NAT.
- Security key IDs and values must be known to SmartPTT configuration engineers since MOTOTRBO software and firmware hides them immediately after configuration and does ***not*** provide tools to view them.

Additional Radio Devices Configuration

To support SmartPTT connection to the radio system, the following actions must be performed:

- In each XRC controller, new console users must be created:
  - Dispatch subsystem (radioserver).
  - *(Optional)* Individual dispatchers (operators).
- To update the location when the radio sends telemetry data, the ***GNSS Report*** check box must be selected for the desired GPIO physical pins in the radio codeplugs.
- If XRC controllers and a radioserver are connected over the router, network address translation must be configured for all XRC services that will be used by a radioserver.
- If XRT gateways and a radioserver are connected over the router, network address translation must be configured to provide the connection.

If you need assistance in the MOTOTRBO devices configuration, contact Motorola Solutions representatives in your region.

SmartPTT Configuration

To configure SmartPTT connection to Connect Plus, the following actions must be performed:

- General connection parameters must be configured. For details, see Configuring Connection to Connect Plus.
- XRC controller connection must be configured. For details, see Adding and Editing XRC Controllers.
- *(Optional)* List of talkgroups must be configured. For details, see Adding and Editing Talkgroups in Connect Plus.

- XRT gateway connection must be configured. For details, see Adding and Editing XRT Gateways.
- Talkpaths must be configured. For details, see Configuring Talkpaths.
- Security keys must be configured. For details, see Configuring Encryption in Connect Plus.
- Network traffic must be unlocked for voice calls. For details, see Connect Plus Ports.

6.6.2.1 Configuring Connection to Connect Plus

Follow the procedure to add a new or edit an existing Connect Plus Connection.

Prerequisites:

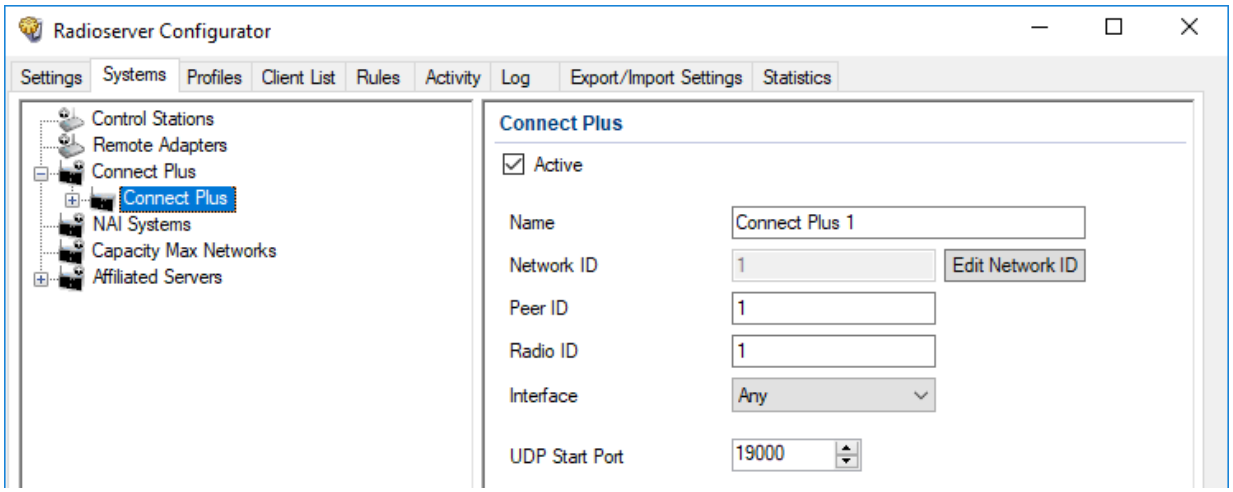
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Install SmartPTT license that allows voice and/or data communication with Connect Plus. For details, see Installing License.
- From codeplugs of XRC controllers, obtain the following data:
  - Console User ID for a radioserver.
  - Repeater Radio ID for a radioserver.
- Determine IP address of the radioserver that will be used to connect to the system.
- For voice and radio command transmission, determine the UDP port number that will be related to the beginning of the port range allocated for talkpaths.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, perform the following actions:

To add a new network,	right-click the ***Connect Plus*** node, and then select ***Add***.
To edit an existing network,	expand the ***Connect Plus*** node, and then click the desired node.

Connection settings appear in the right pane.



3. In the right pane, select the ***Active*** check box.
4. In the ***Name*** field, type the radio network name.
5. Leave the value in the ***Network ID*** field unchanged.
6. In the ***Peer ID*** field, type the Repeater Radio ID for a radioserver.
7. In the ***Radio ID*** field, type the radioserver ID that matches the Console User ID parameter in the XRC controller codeplug.

Important
Do not assign this ID to a client or radio in any radio network.

8. From the ***Interface*** list, select one of the following options:

To use any of the active IP addresses of the computer,	select *Any*.
To use the fixed IP address of the computer,	select the desired address.

9. In the ***UDP Start Port*** field, enter the UDP port number that will be related to the beginning of the port range allocated for talkpaths.
10. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (*** ***)***.

Postrequisites:

- Configure XRC controller connection. For details, see Adding and Editing XRC Controllers.
- Configure talkgroups if your SmartPTT license does not allow voice calls in Connect Plus. For details, see Adding and Editing Talkgroups in Connect Plus.
- Configure XRT gateway connection. For details, see Adding and Editing XRT Gateways.
- Configure talkpaths. For details, see Configuring Talkpaths.
- Configure voice encryption. For details, see Configuring Encryption in Connect Plus.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (*** ***)*** or ***Restart (*** ***)***.

6.6.2.2 Adding and Editing XRC Controllers

Follow the procedure to add a new or edit an existing connection to the main/primary site controllers (XRC controllers) of the Connect Plus system.

Prerequisites:

- Add and configure the Connect Plus connection. For details, see Configuring Connection to Connect Plus.
- Ensure that SmartPTT license allows data communication with Connect Plus. For details, see Viewing License Items.
- From the controller configuration files, obtain the following data:
  - Presence notification service (ARS) port number.
  - Location service port number.
  - Port number of the text message service.
  - *(Optional)* Port number of the network device monitoring service.

- Determine the radioserver port number used to access the services.

Important
Each service of each XRC controller requires the unique local port number.

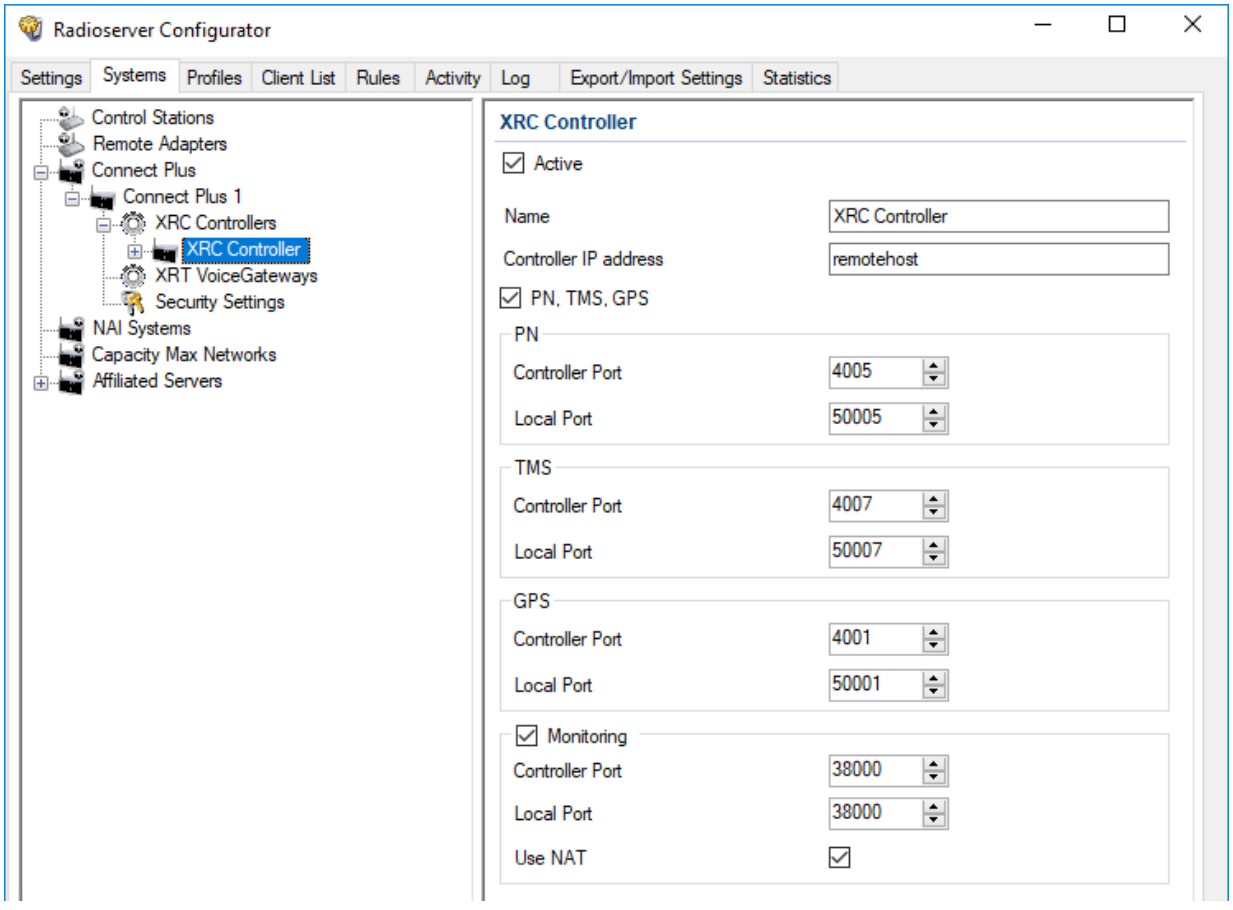
- If the controller and a radioserver are connected over the router that supports Network Address Translation (NAT), obtain the router IP address that is translated to the controller IP address.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane of the tab, expand ***Connect Plus*** → ***<network name>***.
3. Perform one of the following actions:

To add a new XRC controller,	right-click the ***XRC Controllers*** node, and then select ***Add***.
To edit an existing XRC controller connection,	expand the ***XRC Controllers*** node, and then click the desired node.

The controller connection settings appear in the right pane.



4. In the right pane, select the ***Active*** check box.
5. In the ***Name*** field, type the controller name that will be used as the name of the corresponding Location element on the ***Monitoring*** tab.

6. In the Controller IP address field, type the IP address of the controller or router that provide access to the controller. Input format is
<IP address in dot-decimal notation>.
7. Select the ***PN, TMS, GPS*** check boxes to allow connection configuration to the controller services.
8. Configure the controller services connection:

To connect to the radio registration service (ARS/DDMS/PN),	perform the following actions: 1. In the ***PN*** area, in the ***Controller Port*** field, enter the corresponding controller port number. 2. In the same area, in the ***Local Port*** area, enter the radioserver port number.
To connect to the text message service,	perform the following actions: 1. In the ***TMS*** area, in the ***Controller Port*** field, enter the controller port number that is related to TMS. 2. In the same area, in the ***Local Port*** area, enter the radioserver port number.
To connect to the radio location service,	perform the following actions: 1. In the ***GPS*** area, in the ***Controller Port*** field, enter the corresponding controller port number. 2. In the same area, in the ***Local Port*** area, enter the radioserver port number.
To connect to the network device monitoring service,	perform the following actions: 1. Select the ***Monitoring*** check box. 2. In the ***Monitoring*** area, in the ***Controller Port*** field, enter the corresponding controller port number. 3. In the same area, in the ***Local Port*** area, enter the radioserver port number. 4. Select the ***Use NAT*** check box if a radioserver connects to the controller over the router with active NAT.

9. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Configure talkgroups if your SmartPTT license does not allow voice calls in Connect Plus. For details, see Adding and Editing Talkgroups in Connect Plus.
- Configure network device monitoring. For details, see Network Monitoring.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

- In the firewall software on the radioserver computer, unlock the set ports. For details, see Radioserver Host.

6.6.2.3 Adding and Editing Talkgroups in Connect Plus

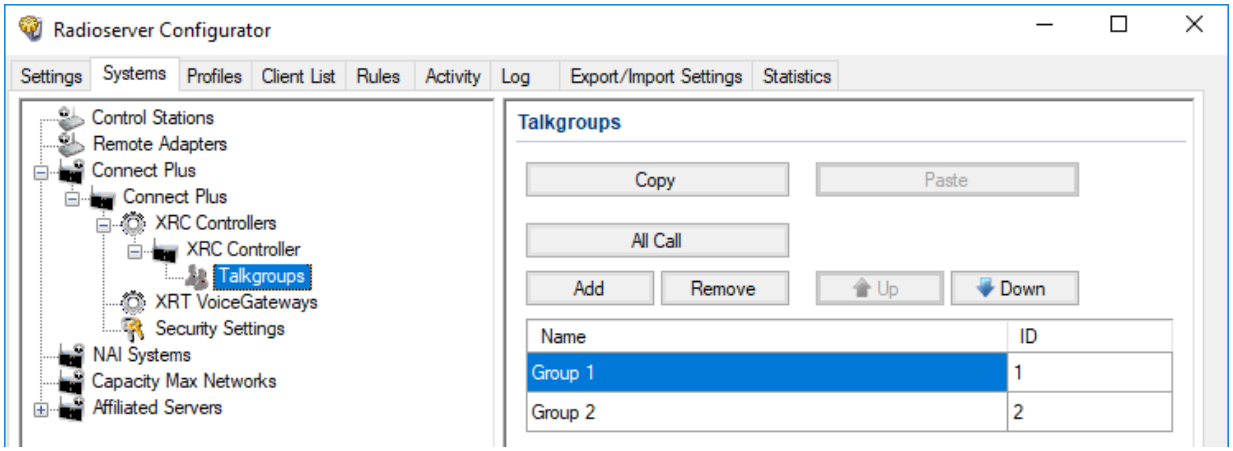
Follow the procedure to edit the list of talkgroups that are configured in the XRC controller configuration file.

Prerequisites:

- From the XRC controller configuration file, obtain the list of talkgroup IDs.
- Add and configure SmartPTT connection to all the desired XRC controllers. For details, see Adding and Editing XRC Controllers.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***Connect Plus*** → ***XRC Controllers*** → ***<controller name>***, and then click ***Talkgroups***.
   The list of talkgroups appear in the right pane.



3. In the right pane, perform one of the following actions:

To add a new talkgroup,	click ***Add***.
To edit an existing talkgroup,	proceed to the next step of the procedure.

4. In the desired table entry, in the ***Name*** column, double-click the current name, and then type the desired name.
5. In the same entry, in the ***ID*** column, double-click the current ID, and then type the desired ID.
6. *(Optional)* Using ***Up*** and ***Down*** buttons, reorder entries in the table.
7. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (*** ***)***.

Postrequisites:

- If talkgroups are configured equally in several XRC controllers, copy them to the corresponding controller lists. For details, see Copying Talkgroups Between Controllers.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (*** ***)*** or ***Restart (*** ***)***.

6.6.2.3.1 Copying Talkgroups Between Controllers

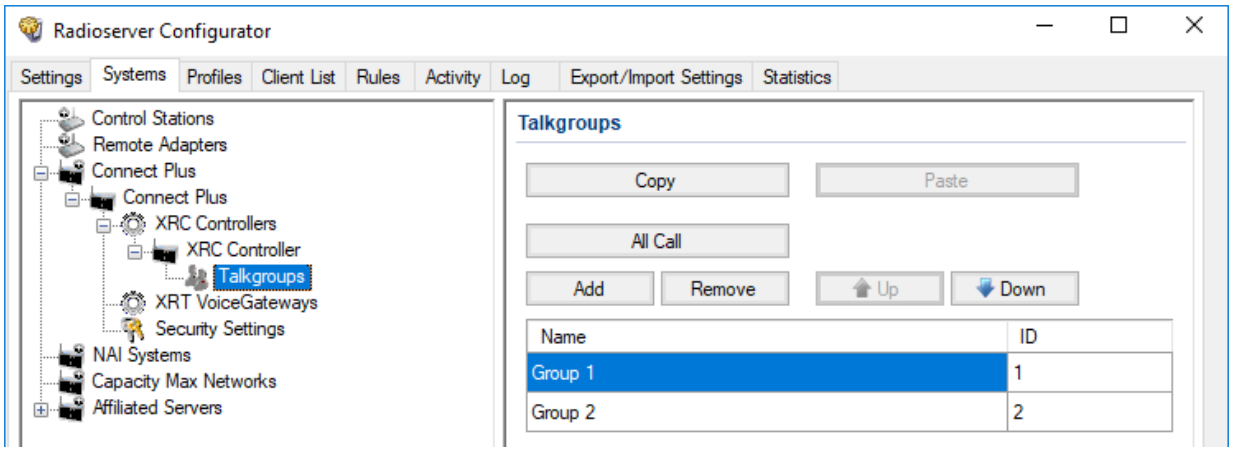
Follow the procedure to copy talkgroup list from an XRC controller to another controller within SmartPTT. The procedure is valid if several controllers have equal or slightly different lists of groups.

Prerequisites:

- Configure SmartPTT connection to multiple XRC controllers. For details, see Adding and Editing XRC Controllers.
- Ensure that controller lists of talkgroups are equal or slightly different.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***Connect Plus*** → ***XRC Controllers*** → ***<controller name>***, and then click ***Talkgroups***.
   The list of talkgroups appears in the right pane.



3. In the right pane of the tab, click ***Copy*** to copy the list of talkgroups to the SmartPTT Radioserver Configurator clipboard.
4. In the left pane of the tab, under the ***XRC Controllers*** node, expand ***<other controller name>***, and then click ***Talkgroups***.
5. In the right pane, click ***Paste***.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- *(Optional)* Edit the copied list of talkgroups. For details, see Adding and Editing Talkgroups in Connect Plus.

6.6.2.4 Adding and Editing XRT Gateways

Follow the procedure to add a new or edit an existing connection to XRT gateways of the Connect Plus radio system.

Prerequisites:

- Ensure that SmartPTT license file allows voice calls in Connect Plus. For details, see Viewing License Items.
- Add and configure SmartPTT connection to Connect Plus. For details, see Configuring Connection to Connect Plus.
- From configuration files of XRT gateways, obtain the following data:
  - IP address and the port number for SmartPTT connection.

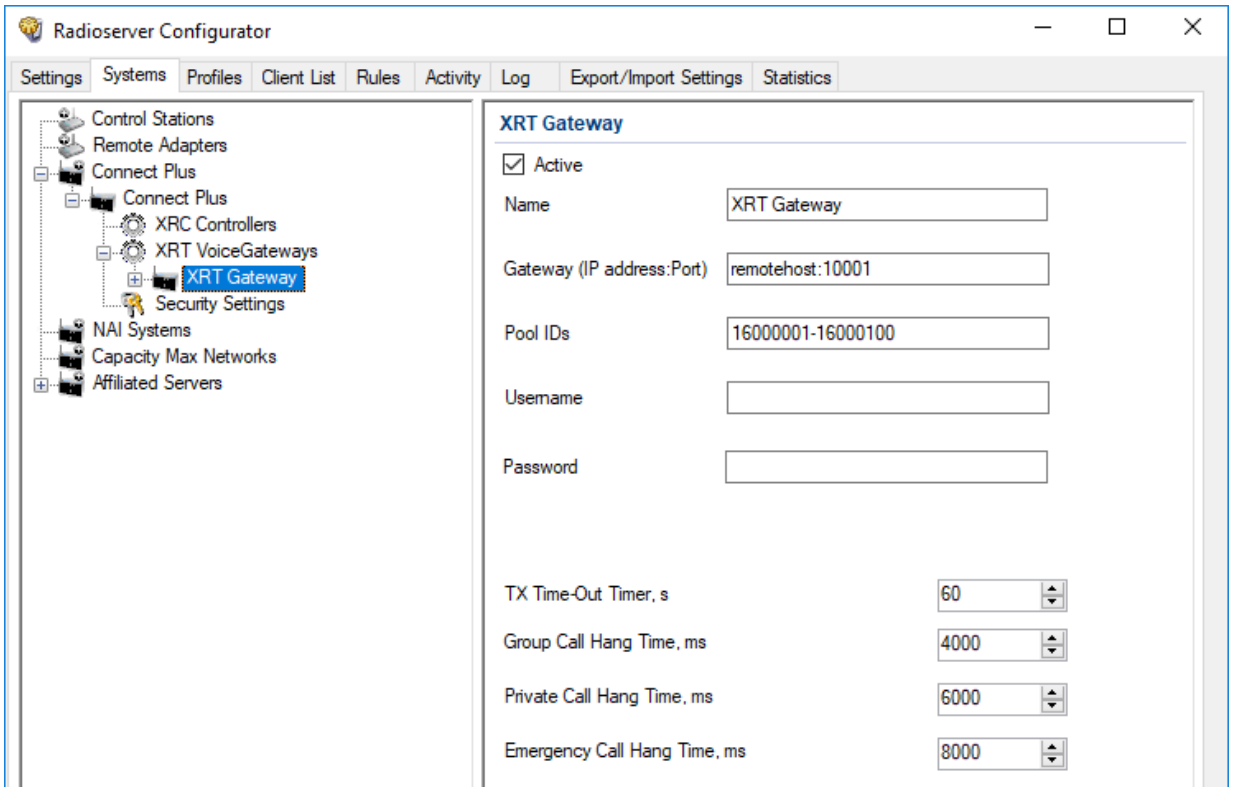
  - User credentials (login and password) used for SmartPTT authentication in gateways.
  - Range of voice call IDs provided by the gateway for dispatch subsystem.
- From radio codeplugs, obtain the following data:
  - Maximum duration of voice transmissions.
  - Hangtime durations for group calls, private calls, and emergency calls.
- If the gateway and a radioserver are connected over the router that supports Network Address Translation (NAT), obtain the router IP address and port number that will be translated to the gateway IP address and port number.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***Connect Plus*** → ***<network name>***.
3. Perform one of the following actions:

To add a new gateway,	right-click the ***XRT VoiceGateways*** node, and then select ***Add***.
To edit an existing gateway,	expand the ***XRT VoiceGateways***, node, and then click the desired child node.

   The gateway connection settings appear in the right pane.



4. In the right pane, select the ***Active*** check box.
5. In the ***Name*** field, type the gateway name.

6. In the ***Gateway (IP address:Port)*** field, type the IP address and port number that provide the gateway connection (considering NAT). Input format is <IP address in dot-decimal notation>:<port number>.
7. In the ***Pool IDs*** field, type the range of voice call IDs that is configured in the gateway for SmartPTT. Input format is <minimum>-<maximum>.
8. In the ***Username*** field, type the login of the user account that is used for SmartPTT authentication in the gateway.
9. In the ***Password*** field, type the password of the user account that is used for SmartPTT authentication in the gateway. To view the entered password, click the eye icon ( ). For security reasons, the password will not be available for viewing in subsequent sessions.
10. Configure voice call parameters:
    a. In the ***TX Time-Out Timer, s*** field, enter the maximum duration of voice transmissions.
    b. In the ***Group Call Hang Time, ms*** field, enter hangtime duration for non-emergency group calls.
    c. In the ***Private Call Hang Time, ms*** field, enter hangtime duration for private calls.
    d. In the ***Emergency Call Hang Time, ms*** field, enter hangtime duration for emergency calls.
11. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Configure talkpaths. For details, see Configuring Talkpaths.
- Configure gateway monitoring as a network device. For details, see Adding and Configuring Devices.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- In the firewall software on the radioserver computer, unlock the specified port. For details, see Radioserver Host.

6.6.2.5 Configuring Talkpaths

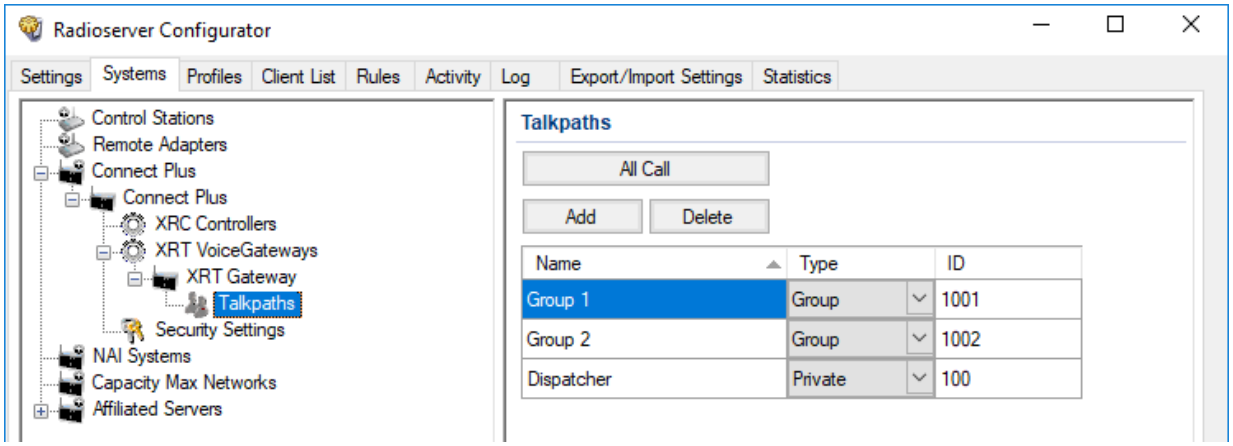
Follow the procedure to configure talkpaths that XRT gateway will provide to SmartPTT.

Prerequisites:

- Connect SmartPTT to the desired XRT gateways. For details, see Adding and Editing XRT Gateways.
- From configuration files of XRC controllers, obtain the following data:
  - Console User ID of the radioserver.
  - *(Optional)* Console User IDs of dispatchers.
- From configuration files of XRT gateways, obtain the following data:
  - Talkgroup IDs.
  - Information on the system-wide All Calls (available or not).

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***Connect Plus***. → ***XRT VoiceGateways*** → ***<gateway name>***, and then click ***Talkpaths***.
   The list of talkpaths appears in the right pane.



3. In the right pane of the tab, perform one of the following actions:

To add a new talkpath (except for All Call),	click ***Add***.
To add a new talkpath for All Call,	click ***All Call***.
To delete an existing talkpath,	perform the following actions: 1. In the table, click the desired talkpath. 2. Click ***Delete***.
To edit an existing talkpath,	proceed to the next step of the procedure.

4. In the desired table entry, in the ***Name*** column, double-click the current talkpath name, and then type the desired name.
5. In the same entry, configure the talkpath:

To configure talkpath for group calls,	perform the following actions: 1. From the ***Type*** list, select *Group*. 2. In the ***ID*** column, double-click the current value, and then type the desired talkgroup ID.
To configure talkpath for private calls,	perform the following actions: 1. From the ***Type*** list, select *Private*. 2. In the ***ID*** column, double-click the current value, and then type Console User ID of the radioserver or one of dispatchers.

NOTE
Talkpaths for All Calls do not require configuration.

6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (***  ***)***.

Postrequisites:

- Configure security keys for voice transmissions. For details, see Configuring Encryption in Connect Plus.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (***  ***)*** or ***Restart (******)***.

6.6.2.6 Configuring Encryption In Connect Plus

Follow the procedure to support transmission decryption and encryption in SmartPTT.

Prerequisites:

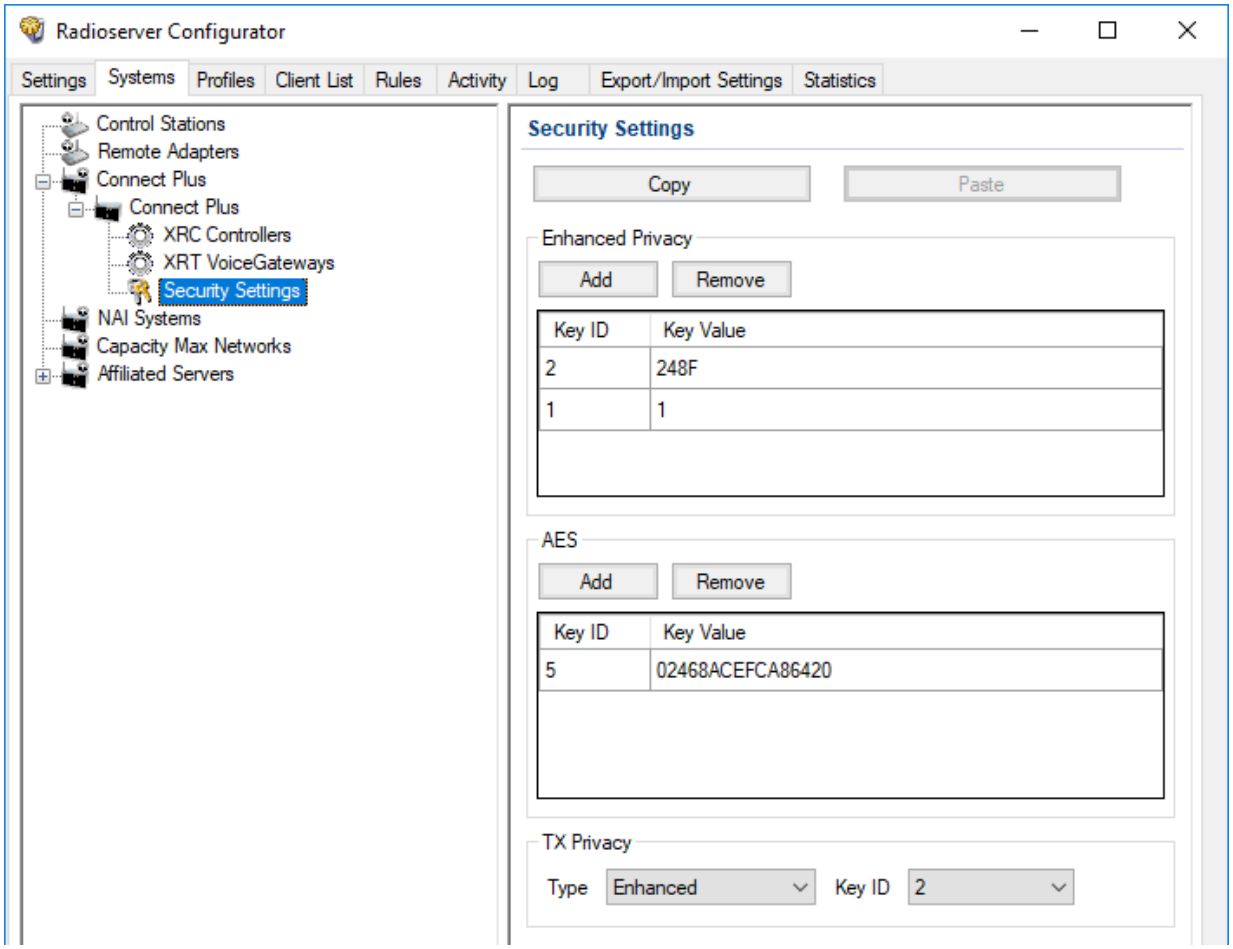
- Add and configure Connect Plus connection. For details, see Configuring Connection to Connect Plus.
- Ensure that the SmartPTT license allows voice calls in Connect Plus. For details, see Viewing License Items.
- Obtain security key IDs and values for all encryption types used in the radio system.

Important
MOTOTRBO configuration tools do not show the configured security/privacy keys for security reasons.

- Determine the key that will be used to encode dispatcher transmissions.
- To configure symmetric (AES-compliant) keys, install the corresponding SmartPTT license. For details, see Installing License.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***Connect Plus*** → ***<network name>***, and the select ***Security Settings***.
   The security key settings appear in the right pane.



3. Add a new security key to the dispatch subsystem:

To add a new enhanced key,	perform the following actions: 1. In the ***Enhanced Privacy*** area, click ***Add***. 2. In a new entry of the table, in the ***Key ID*** column, double-click the current ID, and then type the desired ID. 3. In the same entry, in the ***Key Value*** column, double-click the current value, and then type the desired value.
To add a new symmetric (AES-compliant) key,	perform the following actions: 1. In the ***AES*** area, click ***Add***. 2. In a new entry of the table, in the ***Key ID*** column, double-click the current ID, and then type the desired ID. 3. In the same entry, in the ***Key Value*** column, double-click the current value, and then type the desired value.

4. *(Optional)* Modify an existing security key:

To modify an existing enhanced security key,	perform the following actions: 1. In the ***Enhanced Privacy*** area, in a desired entry of the table, in the ***Key ID*** column, double-click the current ID, and then type the desired ID. 2. In the same entry, in the ***Key Value*** column, double-click the current value, and then type the desired value.
To modify an existing symmetric (AES-compliant) key,	perform the following actions: 1. In the ***AES*** area, in a desired entry of the table, in the ***Key ID*** column, double-click the current ID, and then type the desired ID. 2. In the same entry, in the ***Key Value*** column, double-click the current value, and then type the desired value.

5. Configure outgoing transmission encryption (from dispatchers to the radio network):

To use one of enhanced security keys,	perform the following actions: 1. From the ***Type*** list, select *Enhanced*. 2. From the ***Key ID*** list, select the ID of the desired key.
To use one of symmetric (AES-compliant) security keys,	perform the following actions: 1. From the ***Type*** list, select *AES (Symmetric Key)*. 2. From the ***Key ID*** list, select the ID of the desired key.

To perform unencrypted (clear) transmissions,	from the ***Type*** list, select *No*.

6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

6.6.3 Connect Plus Glossary

This section provides interpretations for various terms used in SmartPTT to describe the Connect Plus connection and configuration. The terms may slightly differ from those in the Connect Plus documentation. If you need more information, submit a request to SmartPTT Technical Support Center.

Control Channel

Specific time slot of the specific site repeater (logical site channel) that is used by radios as a reference channel. It is used to deliver commands and notifications including the channel selection for transmission reception and/or initiation.

Presence Notifier (PN)

Radio network service that provides information about radio registration in the system and availability for transmissions. It is synonymous to ARS (automatic registration service) and similar to DDMS (device discovery and mobility service).

Voice Call ID

Identifier that allows XRT gateway to control and limit the number of simultaneous voice calls over the gateway. ID is not related to the call initiator and target.

Talkpath

Voice call that is allowed to be received and/or initiated by SmartPTT. Talkpath is characterized by type and ID. If the talkpath type is “group”, the ID must be related to the talkgroup ID. Such talkpaths provide the ability to receive and initiate group calls.

If the talkpath type is “private”, the ID must be either radioserver Radio ID, or dispatcher ID (assigned on the ***Clients*** tab of SmartPTT Radioserver Configurator). Such talkpaths provide the ability to receive and initiate private calls.

Important
Configuring talkpaths for on-site radios is ***not*** required.

6.7 Universal SmartPTT Configuration

Current section provides information on SmartPTT configuration that can be implemented for various radio systems:

- Configuration of the DDMS and MNIS access for NAI systems
- Configuration of the SmartPTT MNIS Data Gateway Relay connection for NAI systems and Capacity Max

To specifically configure MNIS and DDMS for different networks, see the sections on configuring the corresponding radio systems.

DDMS Connection

The MOTOTRBO™ Device Discovery and Mobility Service (DDMS) software gateway delivers the radio presence (ARS) information and radio user ID to SmartPTT dispatchers. On the computer, DDMS is represented as a Windows service.

For information on configuring the DDMS access, see Configuring DDMS Connection.

MNIS Connection

The MOTOTRBO™ Network Interface Service (MNIS) software gateway provides SmartPTT dispatchers with data reception and transmission in the radio network. Data includes:

- Text messages and job tickets
- Location requests and reports
- Telemetry data and remote control commands

On the computer, MNIS is represented as a Windows service.

SmartPTT provides three types of the SmartPTT Radioserver connection to the MNIS service:

- Over the virtual network interface (tunnel) of the MNIS service if SmartPTT Radioserver and MNIS are running on the same computer.
- Using the SmartPTT MNIS Data Gateway Relay service if SmartPTT Radioserver and MNIS are hosted on different computers.
- Over the TCP control interface of the MNIS service, regardless of its hosting.

Important
For MNIS version 2.10 or later, connection over the TCP interface must be used.

The same MNIS service can be used by multiple Linked Capacity Plus (TCP interface only) and IP Site Connect networks. To simplify the configuration of NAI systems, duplication of the MNIS settings is implemented in SmartPTT. For details, see Settings Duplication.

Configuring MNIS connection can include the following:

- Configuration of the MNIS access for NAI systems. For details, see Configuring MNIS Connection.
- Configuration of the MNIS access for Capacity Max. For details, see Connecting to Data Gateways.
- Configuration of the SmartPTT MNIS Data Gateway Relay connection. For details, see Configuring MNIS Data Gateway Relay.

NOTE
SmartPTT and MNIS do not provide any security means for data traffic if connected remotely. To secure the data exchange between SmartPTT and MNIS, it is recommended to use third-party solutions such as VPN.
If you need assistance in configuring a secure MNIS connection, submit a request to SmartPTT Technical Support Center.

6.7.1 Configuring DDMS Connection

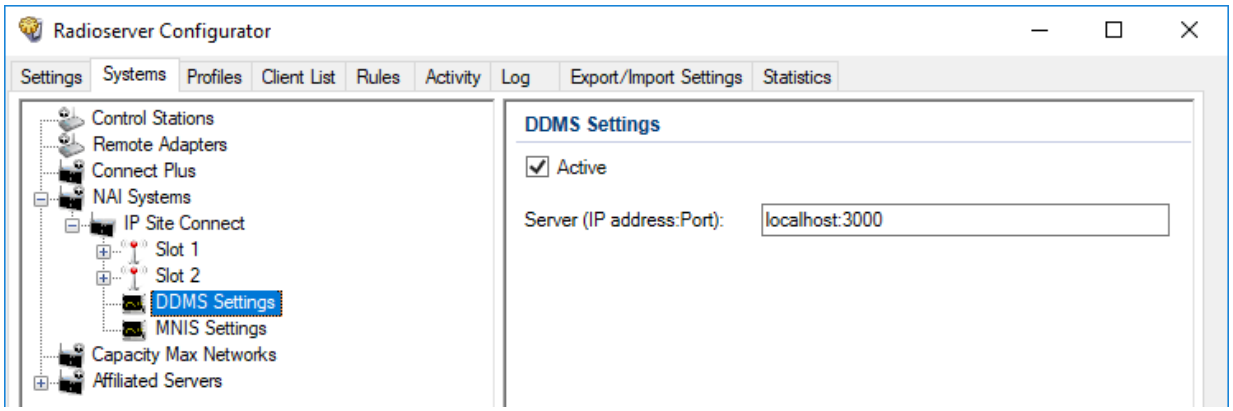
Follow the procedure to connect SmartPTT Radioserver to the DDMS service.

Prerequisites:

- From the MNIS Configuration Utility, obtain the DDMS host IP address.
- From the DDMS Configuration Utility, obtain the watcher port number (value in the ***PortWatcher*** field).

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane of the tab, expand ***NAI Systems*** → ***<system name>***, and then select ***DDMS Settings***.
   The DDMS connection settings appear in the right pane.



3. In the right pane, select the ***Active*** check box.
4. In the ***Server (IP address:Port)*** field, type DDMS host IP address and watcher port number. Input format is <IP address in dot-decimal notation>:<port number>.
5. *(Optional)* If available, select the ***DDMS Mode Control*** check box to establish dependence of the redundant server DDMS activity from the DDMS activity of the primary server.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (*** ***)***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (*** ***)*** or ***Restart (*** ***)***.
- In the firewall software on the radioserver computer, unlock the specified UDP port. For details, see Radioserver Host.

6.7.2 Configuring MNIS Connection

Follow the procedure to connect SmartPTT Radioserver to the MNIS service.

The procedure is not applicable to Capacity Max. For the applicable procedure, see Connecting to Data Gateways.

Prerequisites:

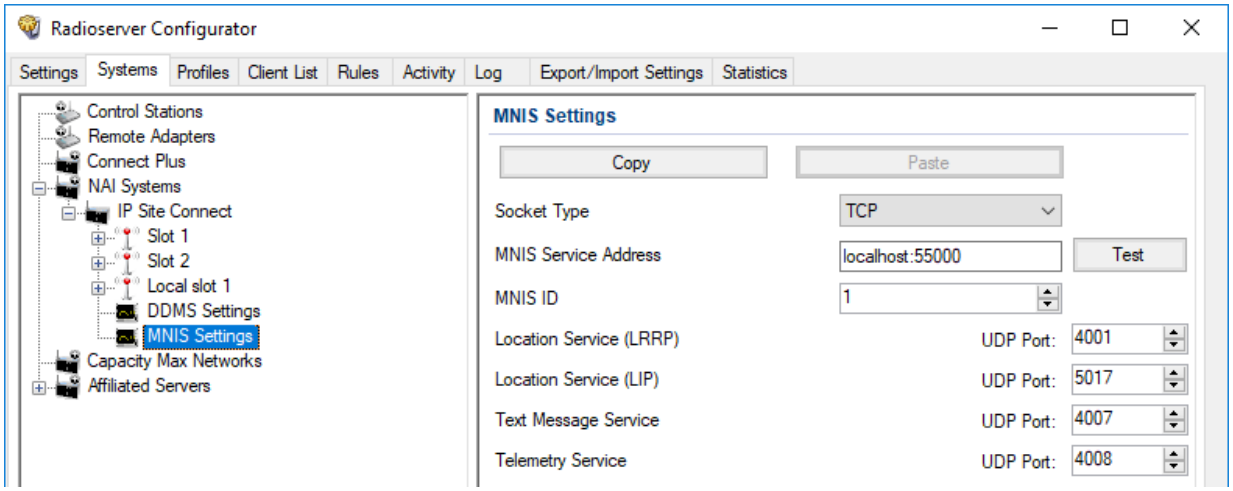
- Obtain IP address or domain name of the MNIS host.
- From the MNIS Configuration Utility, obtain the following information:
  - MNIS Application ID.

- TCP port of the MNIS control interface.
- MNIS ports used for different types of data.
- For connection over the virtual network interface, MNIS Tunnel IP address.

- For connection using SmartPTT MNIS Data Gateway Relay, configure the corresponding service. For details, see Configuring MNIS Data Gateway Relay.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. Access data gateway settings:
   a. On the tab, in the left pane, expand ***NAI Systems***, and then select ***<system name>***.
   b. In the right pane, select the ***Data Transmission*** check box, or ensure that it is selected.
   c. In the left pane, expand ***<system name>***, and then select ***MNIS Settings***.
   The data gateway settings appear in the right pane.



3. Connect SmartPTT Radioserver to the MNIS service:

To connect over the TCP interface,	perform the following actions: 1. From the ***Socket Type*** list, select *TCP*. 2. In the ***MNIS Service Address*** field, type <MNIS host IP address or domain name>:<MNIS Control Interface TCP Port>. 3. *(Optional)* To check connection between the radioserver and MNIS service, click ***Test***, then, in the ***Test Connection*** window, wait for the check result and click ***Close***.

To connect over the virtual network interface if MNIS is installed on the current computer,	perform the following actions: 1. From the ***Socket Type*** list, select *Tunnel Interface*. 2. From the ***Interface*** list, select the MNIS Tunnel IP address. The default MNIS Tunnel IP is *192.168.10.1*. 3. In the ***MNIS Service Address*** field, type <SmartPTT Radioserver host IP address or domain name>:<MNIS Control Interface TCP Port>. 4. *(Optional)* To check connection between the radioserver and MNIS service, click ***Test***, then, in the ***Test Connection*** window, wait for the check result and click ***Close***.
To connect using SmartPTT MNIS Data Gateway Relay if MNIS is installed on another computer,	perform the following actions: 1. From the ***Socket Type*** list, select *Data Gateway Relay (Legacy)*. 2. In the ***MNIS Service Address*** field, type <MNIS host IP address or domain name>:<MNIS Control Interface TCP Port>. 3. In the ***MNIS Relay Server network address*** field, type <MNIS host IP>:<SmartPTT MNIS Data Gateway Relay Port>. 4. *(Optional)* To check connection between the radioserver and MNIS service, click ***Test***, then, in the ***Test Connection*** window, wait for the check result and click ***Close***.
To use connection parameters set in other IP Site Connect or Linked Capacity Plus network and copied to the SmartPTT Radioserver Configurator clipboard,	perform the following actions: 1. Click ***Paste***. 2. Proceed to the last step of the procedure.

4. In the ***MNIS ID*** field, enter MNIS Application ID.
5. In the ***Location Service (LRRP)*** field, enter the number of the MNIS port used to receive radio coordinates over LRRP and send location requests.
6. In the ***Location Service (LIP)*** field, enter the number of the MNIS port used to receive radio coordinates over LIP.
7. In the ***Text Message Service*** field, enter the number of the MNIS port used to receive and send text messages.
8. In the ***Telemetry Service*** field, enter the number of the MNIS port used for data acquisition and remote control commands.
9. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- To copy the specified parameters for configuring MNIS connection in other IP Site Connect or Linked Capacity Plus systems, click ***Copy***.
- In the firewall software on the radioserver computer, unlock the set TCP and UDP ports. For details, see Radioserver Host.

6.7.3 Configuring MNIS Data Gateway Relay

Follow the procedure to configure the SmartPTT MNIS Data Gateway Relay service. The service forwards network traffic between the virtual network interface (tunnel) of the MNIS service and the MNIS host interface. It is required if MNIS is hosted on the computer that is different from the radioserver host.

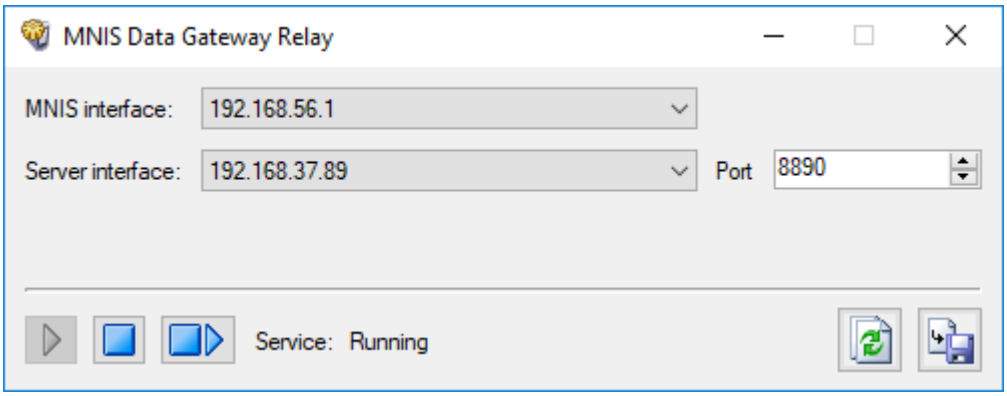
NOTE
For MNIS version 2.10 or later, connecting SmartPTT Radioserver to a remote data gateway using the SmartPTT MNIS Data Gateway Relay service is not recommended. Use connection over the TCP interface instead.

Prerequisites:

Obtain the SmartPTT MNIS Data Gateway Relay installation file, start it on the same computer where MNIS is installed and configured, and install the service by following the Setup Wizard instructions.
To obtain the installation file, submit a request to SmartPTT Technical Support Center.

Procedure:

1. Start the service configurator (MNIS Data Gateway Relay.exe) on the MNIS host.
   The ***MNIS Data Gateway Relay*** window appears.



2. From the ***MNIS interface*** list, select the MNIS Tunnel IP address.
3. Perform one of the following actions:

To forward SmartPTT Radioserver requests and responses only for the specific IP address of the MNIS host,	from the ***Server interface*** list, select the desired IP address.
To forward SmartPTT Radioserver requests and responses for any IP address of the MNIS host,	from the ***Server interface*** list, select *Any*.

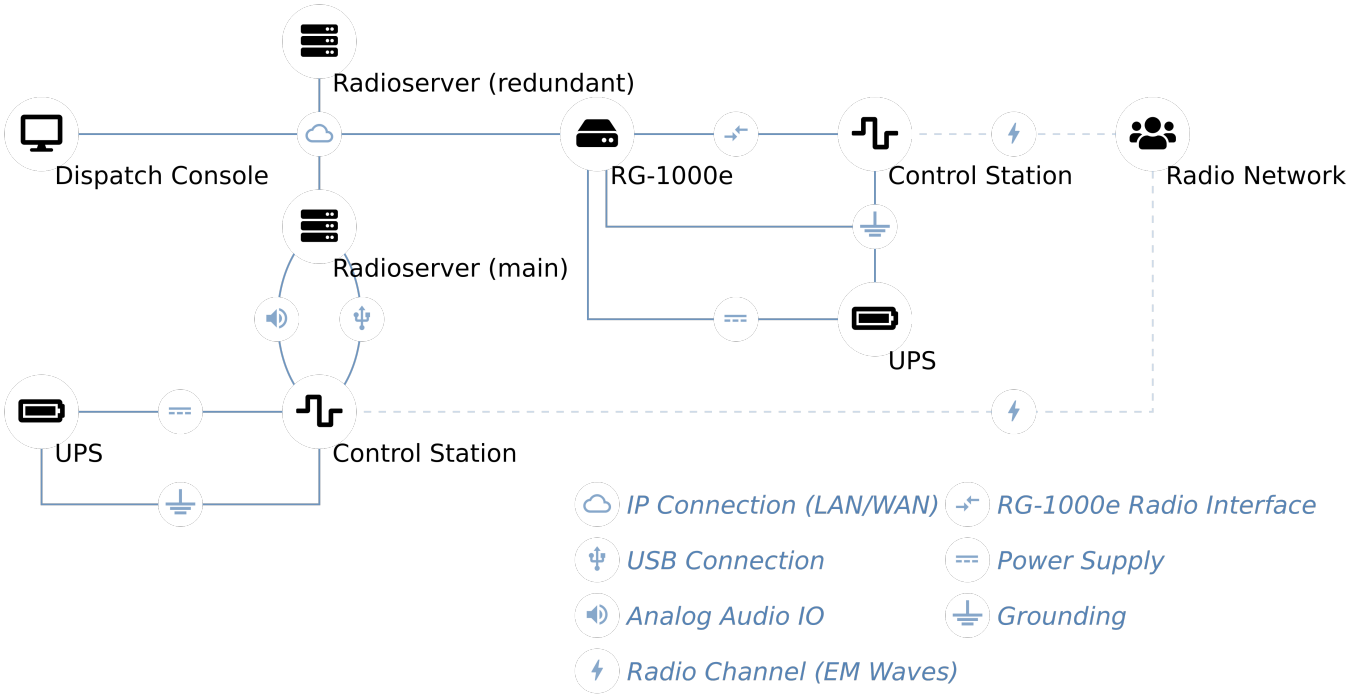
4. In the ***Port*** field, type the number of a free computer UDP port (default port is *8890*).
5. To save changes, at the bottom of the Relay window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the Relay window, click ***Start ( )*** or ***Restart ( )***.

6.8 MOTOTRBO Control Stations

SmartPTT supports MOTOTRBO control stations, MOTOTRBO-compliant mobile or base radios that act as access points to the radio network.



In SmartPTT, MOTOTRBO control stations are intended for direct communication between radios. If you have questions on control stations application in repeater systems, contact Elcomplus, Inc. representatives in your region.

SmartPTT supports the following interfaces for MOTOTRBO control stations connection:

- Digital-and-analog interface (USB+audio). For details, see MOTOTRBO Station Access over USB+Audio.
- Over the RG-1000e/RG-2000 remote adapter. For details, see MOTOTRBO Station Access over RG-1000e.

Using MOTOTRBO radios as control stations implies that they are ***not*** operated directly. This includes the following:

- No person must switch channels on the control station using Control Head buttons or other controls.
- No person must transmit from the radio using Control Head buttons or handsets.

Violation of such requirements results in the data desynchronization between SmartPTT and a control station.

6.8.1 Control Station Features

MOTOTRBO control stations provide the following features to SmartPTT:

- Direct communication with digital radios.
- Limited support for analog radio systems (MDC-1200 and Select 5). For details, submit a request to the SmartPTT Technical Support Center.
- Radios registration (includes on-activity registration).
- Incoming and outgoing voice calls (group and private calls).

- Incoming emergency alarms and calls.
- Voice encryption and decryption.
- Radio location reports reception.
- Text messages and job tickets.
- Telemetry data acquisition and remote control using on-site radios.

Based on provided features, SmartPTT implements the following features:

- Simultaneous connection to multiple control stations.
- Phone calls.
- Voice integration with other radio systems using cross patches, bridging, and conference calls.
- Events and voice logging.
- Rules configuration.
- Control station accessibility over the Server API. For details, see Third-Party Apps.

For station control purposes, SmartPTT provides the channel selection feature for control stations.

For network monitoring purposes, SmartPTT provides the following features:

- Connection monitoring between radioserver and the control station.
- Supplementral network devices monitoring (UPS, switches etc.).
- Automatic alarm notifications.
- Radio channel monitoring (may be referred to as “air monitoring”).
- Open Voice Channel Mode (OVCM) calls.
- Availability on the topology diagram.

NOTE
SmartPTT does ***not*** show on-site/fielded radios on the topology diagram.

6.8.2 MOTOTRBO Stations Configuration

Configuration of control stations and fielded radios requires the following:

- Compliance with planning requirements. For details, see “Planning Requirements” below.
- Additional control station configuration. For details, see “Control Station Configuration” below.
- Additional digital radios configuration. For details, see “Digital Radios Configuration” below.

Important
Information below provides the minimum required changes in radio equipment settings. It is ***not*** sufficient for operation. For configuration assistance, submit a request to SmartPTT Technical Support Center.

Planning Requirements

To support the direct mode communication, all radios (including control stations) must comply with the following requirements:

- All radios (including control stations) must have unique Radio IDs.
- All radios (including control stations) must have equal radio network IDs (CAI ID) and group ID in the radio network (CAI Group ID).
- All radios (including control stations) must use equal security keys.
- All radios (including control stations) must have equal set of properly configured channels. Proper channel configuration includes the following aspects:
  - Receive and transmit frequencies.
  - Default groups on each channel.
  - Security systems.

Control Station Configuration

To configure mobile/base radios to operate as control stations, their codeplugs must be modified in the following way:

- Private calls must be allowed.
- Radio network services must be activated:
  - Location (GNSS) service.
  - Text message service.
- Control station interface must be configured:
  - Voice and non-voice information must be routed over the cable.
  - Information forwarding to PC must be activated.
- Control station channels must be configured:
  - Each digital channel must have a different default talkgroup
  - *(Optional)* One of digital channels must have the All Call as a default group.
- Emergency alarm acknowledgment must be activated on each digital radio channel.
- *(Optional)* Voice/transmit interruption must be configured. It is recommended to allow voice/transmit interruption for control station despite of the color code or channel accessibility.

Digital Radios Configuration

To configure digital radios, their codeplugs must be modified in the following way:

- They must send registration reports to the control station Radio ID.
- They must send their location reports to the control station Radio ID.
- Their emergency group must be the default talkgroup of the control station.
- To update the location when the radio sends telemetry data, the ***GNSS Report*** check box must be selected for the desired GPIO physical pins in the radio codeplugs.

6.8.3 MOTOTRBO Station Access over USB+Audio

To connect a MOTOTRBO control station to the radioserver host, the following elements must be connected to each other:

- Control station must be connected to the power supply that is ***disconnected*** from the power system.
- Control station must be connected to the radioserver host using Elcomplus, Inc. cable.
- Power supply must be connected to the power system.

WARNING
Power connection may result in the unintended personnel injury or equipment damage. The connection must be performed with a qualified engineer who have the corresponding license.

To configure the control station connection to the radioserver, the following actions must be performed:

- SmartPTT license with MOTOTRBO control stations permission must be installed. For details, see Installing License.
- Radioserver must be connected to the control station. For details, see Configuring MOTOTRBO Control Station Connection.
- *(Optional)* 5-tone telegrams must be configured.
- Talkgroups and All Call must be added. For details, see Configuring MOTOTRBO Control Station Groups.
- Control station channels must be configured. For details, see Configuring MOTOTRBO Control Station Channels.
- Voice processing must be configured. For details, see Configuring MOTOTRBO Control Station Audio Settings.

6.8.3.1 Configuring MOTOTRBO Control Station Connection

Follow the procedure to add a new or edit an existing connection to the local MOTOTRBO control station.

Prerequisites:

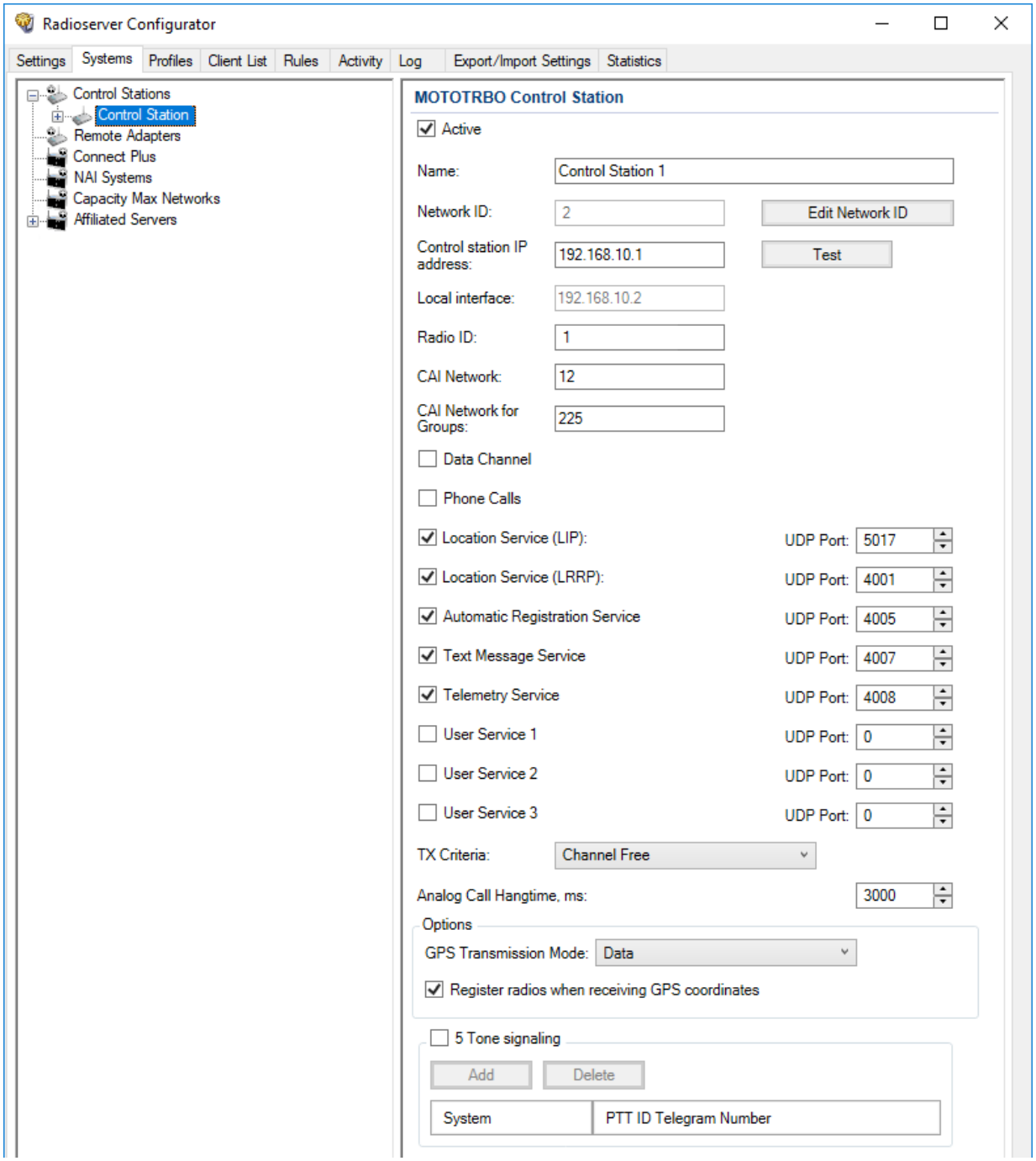
- Ensure that the control station is connected to the SmartPTT Radioserver host using the dedicated Elcomplus, Inc. cable, connected to the power supply, and turned on.
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure that SmartPTT has the license that unlocks the use of MOTOTRBO control station. For details, see Viewing License Items.
- From the control station codeplug, obtain the following information:
  - Radio ID, CAI network ID, and CAI Group ID.
  - Control station ports used to receive and transmit various data types.
  - Transmit interruption parameters.
  - Location provision settings that depend on data transmission settings on channel.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, perform one of the following actions:

To add a new connection,	perform the following actions: 1. Right-click ***Control Stations***. 2. Point to ***Add***, and then select ***MOTOTRBO control station***.
To edit an existing connection,	expand ***Control Stations***, and then select the desired control station.

The control station parameters appear in the right pane.



3. In the right pane, select the ***Active*** check box to unlock control station settings.
4. In the ***Name*** field, type the control station name.
5. Leave the value in the ***Network ID*** field unchanged, or edit the value after clicking the ***Edit Network ID*** button.
6. In the ***Control station IP address*** field, type the IP address of the local network interface associated with the connected control station.
7. *(Optional)* To check if you have specified the control station IP address correctly, click ***Test***. After checking you will see a message with the result.
8. Leave the value in the ***Local interface*** field unchanged.

9. Type the control station identification parameters:
    a. In the ***Radio ID*** field, type the control station ID specified in its codeplug

Important
Do not assign this ID to a client or radio in any radio network.

    b. In the ***CAI Network*** field, type the ID of the CAI network that is set in the control station codeplug.
    c. In the ***CAI Network for Groups*** field, type the ID of the CAI network for groups that is set in the control station codeplug.
10. Select the ***Data Channel*** check box if the control station is used to receive location coordinates from other radio only.

Important
All other parameters must be configured only if the ***Data Channel*** check box is cleared.

11. Select the ***Phone Calls*** check box to allow other radios to receive and initiate phone calls over the control station.
12. Configure data transmission over the control station:

To receive coordinates over LIP,	perform the following actions: 1. Select the ***Location Service (LIP)*** check box. 2. In the field to the right of the check box, enter the port number used to receive this data.
To receive coordinates over LRRP,	perform the following actions: 1. Select the ***Location Service (LRRP)*** check box. 2. In the field to the right of the check box, enter the port number used to receive this data.
To receive information about radio presented in the radio network,	perform the following actions: 1. Select the ***Automatic Registration Service*** check box. 2. In the field to the right of the check box, enter the port number used to receive the data.
To support text messages and job tickets in the radio network,	perform the following actions: 1. Select the ***Text Message Service*** check box. 2. In the field to the right of the check box, enter the port number used to receive and transmit the data.
To receive telemetry data and send telemetry commands,	perform the following actions: 1. Select the ***Telemetry Service*** check box. 2. In the field to the right of the check box, enter the port number used to receive and transmit the data.

To receive client services data,	perform the following actions: 1. Select the ***User Service*** check box that corresponds to the control station configuration. 2. In the field to the right of the check box, enter the port number used to receive this data.

13. From the ***TX Criteria*** list, select one of the following options:

If the control station is configured to transmit only when no other transmissions is detected over the radio channel,	select *Channel Free*.
If the control station is configured to notify other radios on transmissions interruption,	select *Tx Interrupt*.
If the control station is configured to completely ignore other transmission over the radio channel,	select *Always*.

Important
SmartPTT does not support color code criteria for outgoing transmissions.

13. In the ***Analog Call Hangtime, ms*** field, enter the maximum time interval between transmissions over analog channels that will be considered as transmissions within the same call in SmartPTT.
14. From the ***GPS Transmission Mode*** list, select one of the following options:

If all the digital channels support both CSBK data and enhanced GNSS,	select *Enhanced CSBK*.
If all the digital channels support CSBK data, and do not support Enhanced GNSS,	select *CSBK*.
If digital channels have different settings,	select *Data*.

15. Select the ***Register radios when receiving GPS coordinates*** check box to allow SmartPTT Radioserver register radios on the control station when it receives their GPS coordinates.
16. Clear the ***5 Tone signaling*** check box.

NOTE
For information on five-tone signaling support in SmartPTT, submit a request to the SmartPTT Technical Support Center.

17. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Configure groups. For details, see Configuring MOTOTRBO Control Station Groups.
- Configure control station channels.For details, see Configuring MOTOTRBO Control Station Channels.
- Configure audio settings. For details, see Configuring MOTOTRBO Control Station Audio Settings.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

- In the firewall software on the computer, unlock the set UDP ports. For details, see Radioserver Host.

6.8.3.2 Configuring MOTOTRBO Control Station Groups

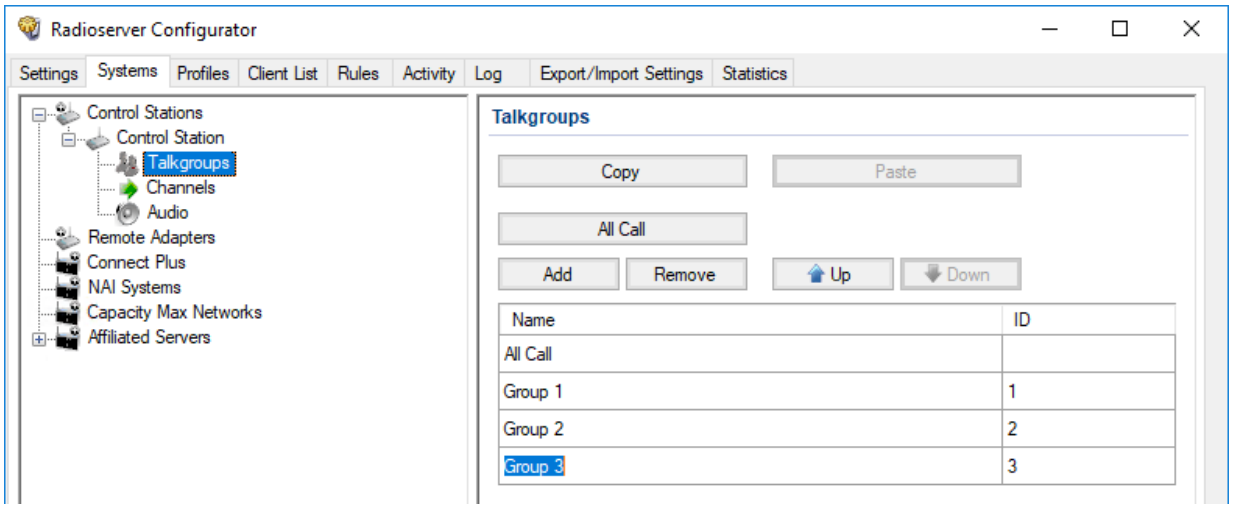
Follow the procedure to add new or edit existing talkgroups and All Call entries that will be available to SmartPTT dispatchers.

Prerequisites:

From the control station codeplug, obtain talkgroup IDs. To obtain the information, use the compatible MOTOTRBO CPS application.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***Control Stations*** → ***<your control station>***, and then select ***Talkgroups***.
   The list of groups appears in the right pane.



3. In the right pane, perform one of the following actions:

To add a new talkgroup,	click ***Add***.
To add an All Call,	click ***All Call***.
To edit an existing entry,	proceed to the next step of the procedure.

4. In the table, in the desired entry, perform the following actions:
   a. In the ***Name*** column, double-click the current name, and then type the desired name.
   b. In the ***ID*** column, double-click the current Talkgroup ID, and then type the desired ID.

NOTE
For All Call, no ID is shown.

5. *(Optional)* Using ***Up*** and ***Down*** buttons, reorder entries in the table.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (*** ***)***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (*** ***)*** or ***Restart (*** ***)***.

6.8.3.3 Configuring MOTOTRBO Control Station Channels

Follow the procedure to add new or edit existing control station channels.

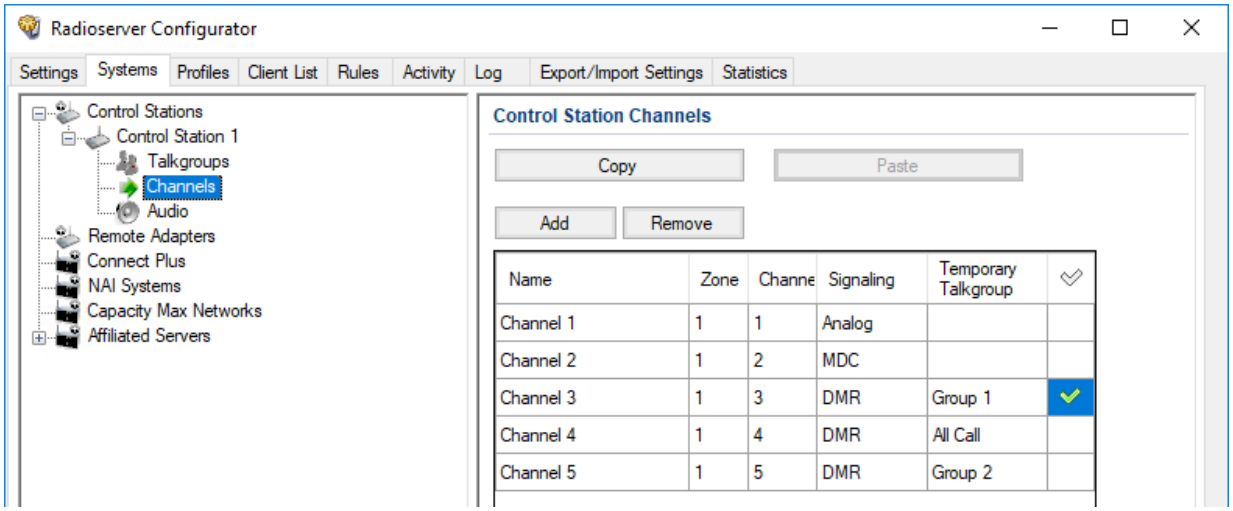
Prerequisites:

- From the control station codeplug, obtain the following information:
  - List of channels and their identification information (zone IDs and channel IDs).
  - Radio signaling type used on each channel.
  - Channel default contract (talkgroup ID or All Call).

  To obtain the information use the compatible MOTOTRBO CPS application.
- Ensure that talkgroups and All Calls are added to SmartPTT Radioserver Configurator. For details, see Configuring MOTOTRBO Control Station Groups.
- If required, ensure that the necessary 5-tone telegrams are added to SmartPTT Radioserver Configurator.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***Control Stations*** → ***<your control station>***, and then select ***Channels***.
   The list of channels appears in the right pane.



3. In the right pane, perform one of the following actions:

To add a new channel,	click ***Add***.
To edit an existing entry,	proceed to the next step of the procedure.

4. In the table, in the desired entry, perform the following actions:
   a. In the ***Name*** column, double-click the current channel name, and then type a new name.
   b. In the ***Zone*** field, double-click the current zone ID, and then type the desired ID.
   c. In the ***Channel*** column, double-click the current channel ID, and then type the desired ID.
   d. In the ***Signaling*** column, configure the desired signaling type on the channel:

To configure a digital channel,	perform the following actions: 1. From the list, select ***DMR***. 2. In the ***Temporary Talkgroup*** column, from the list, select the desired talkgroup or All Call.
To configure an analog channel,	from the list, select the desired option.

5. After all channels are configured, in the ***Default Channel ( )*** column, select the check box next to the channel that will be selected on the control station each time SmartPTT Radioserver is started or restarted.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

6.8.3.4 Configuring MOTOTRBO Control Station Audio Settings

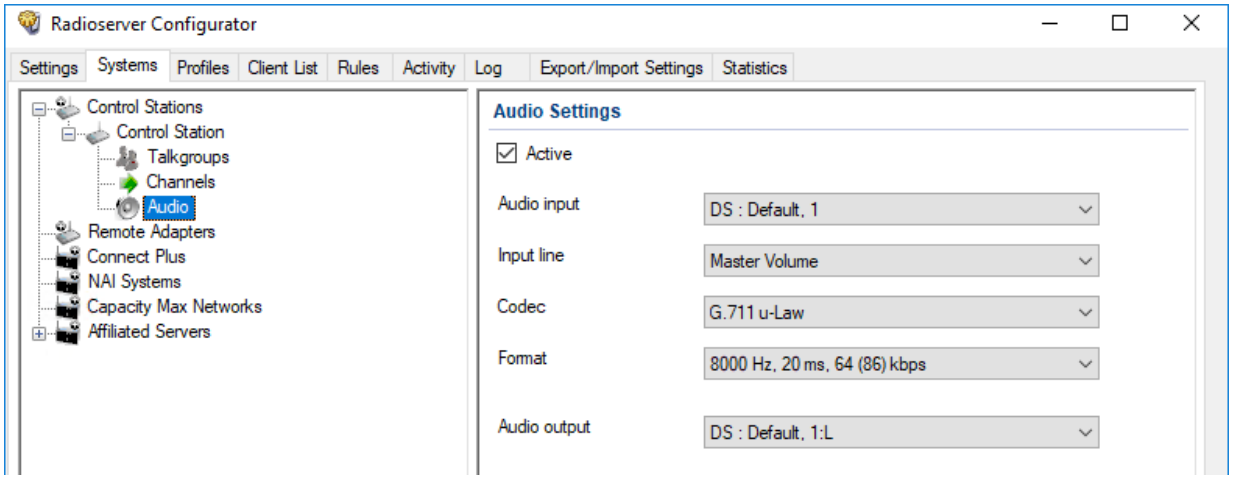
Follow the procedure to edit audio settings required to receive voice from the control station and send dispatcher voice to it.

Prerequisites:

From the SmartPTT Radioserver host, obtain the identification information on audio inputs and outputs used to connect the control station.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***Control Stations*** → ***<your control station>***, and then select ***Audio***.
   The audio settings appear in the right pane.



3. In the right pane, select the ***Active*** check box to unlock audio settings.
4. From the ***Audio*** input list, select the proper microphone input.
5. Leave the value in the ***Input line*** unchanged until you are using the sound card with multiple audio processing lines for each input.
6. From the ***Codec*** list, select the desired codec. The recommended options are *G.711 u-Law* and *G.711 A-Law*.

7. From the ***Format*** list, select the desired values of sampling frequency and frame length. The selected option will affect the IP channel loading between SmartPTT Radioserver and SmartPTT Dispatcher.
8. From the ***Audio output*** list, select the proper speaker output.
9. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

6.8.4 MOTOTRBO Station Access over RG-1000e

RG-1000e is a remote adapter intended to provide the remote access to control stations for SmartPTT. It may also used for other purposes (like radio system bridging, “distributed repeaters” etc). For details, visit the SmartPTT RG-1000e webpage of the SmartPTT website.

Additional Features

If MOTOTRBO control station is connected over RG-1000e, if provides the following additional features to SmartPTT:

- Alternate/redundant radioserver support.
- Configurable session initiator.

Using RG-1000e does ***not*** provide the following features:

- Secure connection between the remote adapter and radioserver.
- Location reporting using option boards. For details, see Location with Option Boards.

Remote Adapter Configuration

To configure the remote adapter to support MOTOTRBO control stations connected over the digital-and-analog interface, the following actions must be performed:

- Control station must be connected to the adapter using Elcomplus, Inc. cable.
- Power supply and grounding must be configured correctly for control station gateway.

WARNING
Power connection may result in the unintended personnel injury or equipment damage. The connection must be performed with a qualified engineer who have the corresponding license.

- In remote adapter configuration file, the correct connection mode must be configured:
  - MOTOTRBO radio connection.
  - Control station connection.
- Remote adapter IP channel association with a physical radio port must be configured.
- *(Optional)* Audio gain/attenuation must be configured on the radio port.

For information on the adapter settings, see *RG-1000e Installation and Configuration Guide*.

For information on the analog connection of the MOTOTRBO control station to the adapter, see Analog Interfaces.

SmartPTT Configuration

To configure the control station connection over RG-1000e to the radioserver, the following actions must be performed:

- SmartPTT license with MOTOTRBO control station permissions must be installed. For details, see Installing License.
- Connection to the control station must be configured. For details, see Configuring Remote MOTOTRBO Control Station Connection.
- *(Optional)* 5-tone telegrams must be configured.
- Talkgroups and All Call must be added. For details, see Configuring Remote MOTOTRBO Control Station Talkgroups.
- Control station channels must be configured. For details, see Configuring Remote MOTOTRBO Control Station Channels.
- Voice processing must be configured. For details, see Configuring Remote MOTOTRBO Control Station Audio Settings.

6.8.4.1 Configuring Remote MOTOTRBO Control Station Connection

Follow the procedure to add a new or edit an existing connection to a remote MOTOTRBO control station.

Prerequisites:

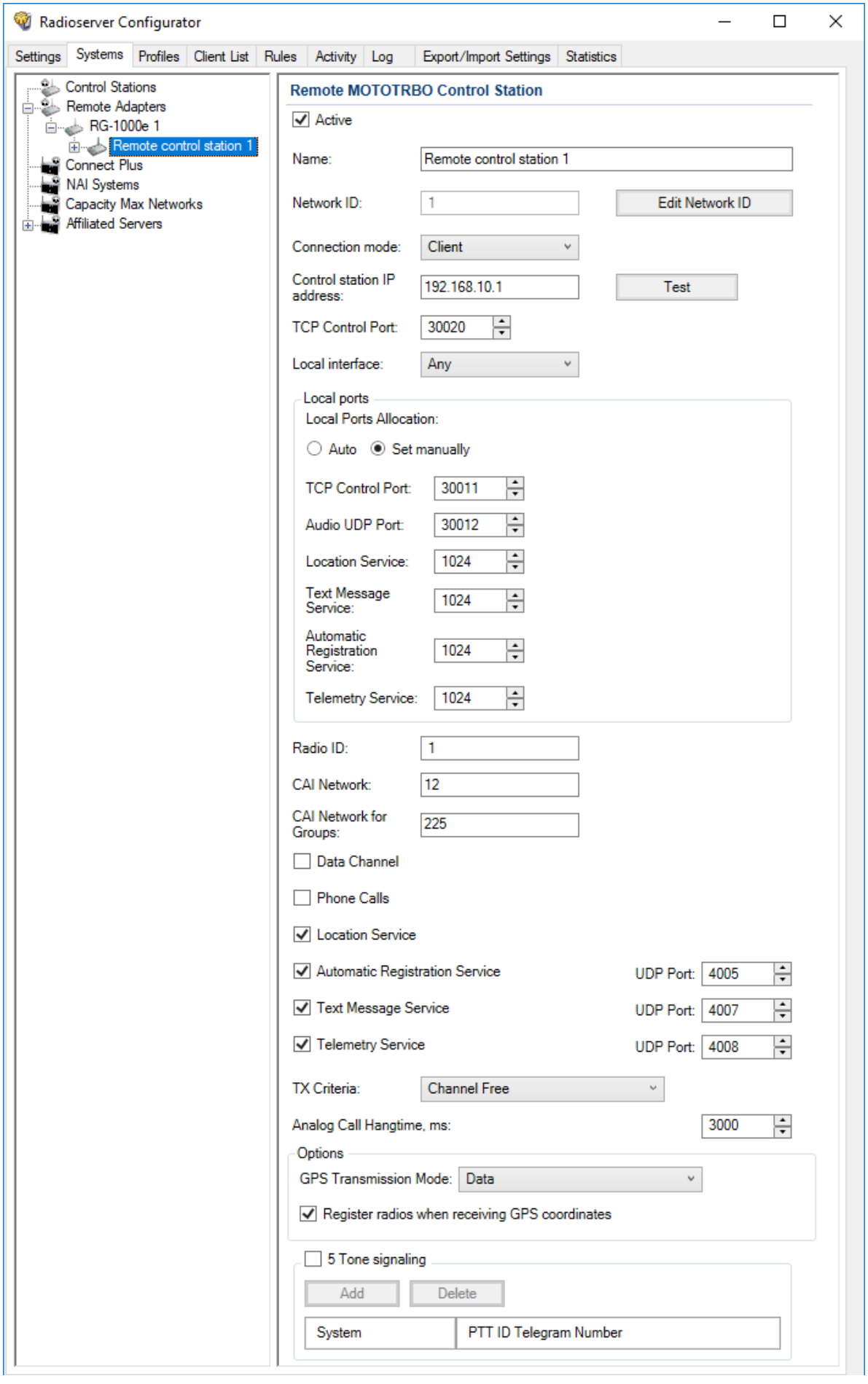
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure SmartPTT license allows remote control stations access. For details, see Viewing License Items.
- From the control station codeplug, obtain the following information:
  - Radio ID, CAI network ID, and CAI Group ID
  - Transmit interruption parameters
  - The format of location data transmission in the control station
- Determine whether SmartPTT Radioserver or RG-1000e will initiate the connection.
- *(Optional)* If RG-1000e is configured to act as a server, from the RG-1000e configuration, obtain the IP address and port number configured for the desired control station.
- From the RG-1000e configuration, obtain control station ports used to receive and transmit various data types.
- *(Optional)* Determine SmartPTT Radioserver host ports that will be used to receive different data types from the control station.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, perform one of the following actions:

To add a remote MOTOTRBO control station to a new remote adapter,	perform the following actions:

	1. Right-click ***Remote Adapters***, and then click ***Add*** → ***RG-1000e***. The ***<Adapter Name>*** node appears. 2. In the right pane, select the ***Active*** check box. 3. *(Optional)* In the ***Name*** field, type the adapter name. 4. In the left pane, right-click the ***<Adapter Name>*** node, point to ***Add***, and then select ***Remote MOTOTRBO Control Station***.
To add a remote MOTOTRBO control station to an existing remote adapter,	perform the following actions: 1. Expand the ***Remote Adapters*** node. 2. Right-click the desired adapter name, point to ***Add***, and then select ***Remote MOTOTRBO Control Station***.
To edit an existing remote MOTOTRBO control station connection settings,	expand ***Remote Adapters*** → ***<Adapter Name>***, and then click the desired control station.
To delete a remote MOTOTRBO control station connection,	perform the following actions: 1. Expand ***Remote Adapters*** → ***<Adapter Name>***. 2. Right-click the desired control station, and then select ***Delete***. 3. Proceed to the last step of the procedure.


Radioserver Configurator
Settings
Systems
Profiles
Client List
Rules
Activity
Log
Export/Import Settings
Statistics
Control Stations
Remote Adapters
RG-1000e 1
Remote control station 1
Connect Plus
NAI Systems
Capacity Max Networks
Affiliated Servers
Remote MOTOTRBO Control Station
Active
Name:
Remote control station 1
Network ID:
1
Edit Network ID
Connection mode:
Client
Control station IP address:
192.168.10.1
Test
TCP Control Port:
30020
Local interface:
Any
Local ports
Local Ports Allocation:
Auto
Set manually
TCP Control Port:
30011
Audio UDP Port:
30012
Location Service:
1024
Text Message Service:
1024
Automatic Registration Service:
1024
Telemetry Service:
1024
Radio ID:
1
CAI Network:
12
CAI Network for Groups:
225
Data Channel
Phone Calls
Location Service
Automatic Registration Service
UDP Port:
4005
Text Message Service
UDP Port:
4007
Telemetry Service
UDP Port:
4008
TX Criteria:
Channel Free
Analog Call Hangtime, ms:
3000
Options
GPS Transmission Mode:
Data
Register radios when receiving GPS coordinates
5 Tone signaling
Add
Delete
System
PTT ID Telegram Number

3. In the right pane, select the ***Active*** check box to unlock control station settings.
4. In the ***Name*** field, type the control station name.
5. Leave the value in the ***Network ID*** field unchanged, or edit the value after clicking the ***Edit Network ID*** button.
6. Configure the connection mode to the control station:

If RG-1000e is configured to accept SmartPTT connection (acts as a server),	perform the following actions: 1. From the ***Connection mode*** list, select *Client*. 2. In the ***Control station IP address*** field, type the adapter IP address to receive radioserver connections. 3. *(Optional)* To check if you have specified the control station IP address correctly, click ***Test***. After checking you will see a message with the result. 4. In the ***TCP Control Port*** field, enter the port number to receive radioserver connections. ***Important*** The IP address and port number in the fields above must match the IP address and port number in the ***IP address*** and ***Port XCMP protocol*** fields in the ***Gateway IP settings*** area of the RG-1000e configuration. For details, see "IP channel" in *RG-1000e Installation and Configuration Guide*.
If RG-1000e is configured to initiate SmartPTT connection (acts as a client),	perform the following actions: 1. From the ***Connection mode*** list, select *Server*. 2. In the ***Local TCP Control Port*** field, enter the SmartPTT Radioserver port number to listen to incoming connections. ***Important*** The port number in this field must match the port number in the ***Port XCMP protocol*** field in the ***Remote Gateway IP settings*** area of the RG-1000e configuration. For details, see "IP channel" in *RG-1000e Installation and Configuration Guide*.

7. From the ***Local interface*** list, select the desired option:

To use any radioserver IP address for the remote adapter connection,	select *Any*.
To use a fixed IP address for the remote adapter connection,	select the desired IP address.

Important
If you select *Server* from the ***Connection mode*** list, a fixed IP address must match the IP address in the ***IP address*** field in the ***Remote Gateway IP settings*** area of the corresponding IP channel in the RG-1000e configuration.

8. *(Optional)* In the ***Local ports*** area, set SmartPTT Radioserver host ports for different types of data:

To set local ports automatically,	select *Auto*.
To set specific local port values,	perform the following actions: 1. Select *Set manually*. 2. If available, in the ***TCP Control Port*** field, enter the port number used to receive commands and service messages from the remote control station, and send commands and service messages to it. 3. In the ***Audio UDP Port*** field, enter the port number used to receive voice from the remote control station and send dispatcher voice to it. 4. In the ***Location Service*** field, enter the port number used to receive location updates from radios and send location update requests to them over the remote control station. 5. In the ***Text Message Service*** field, enter the port number used to receive text messages from radio, and send text messages from dispatchers over the remote control station. 6. In the ***Automatic Registration Service*** field, enter the port number used to receive presence information on radios within the RF coverage zone of the remote control station. 7. In the ***Telemetry Service*** field, enter the port number used to receive telemetry data and send telemetry commands.

9. Type the control station identification parameters:
   a. In the ***Radio ID*** field, type the control station ID specified in its codeplug

Important
Do not assign this ID to a client or radio in any radio network.

   b. In the ***CAI Network*** field, type the ID of the CAI network that is set in the control station codeplug.
   c. In the ***CAI Network for Groups*** field, type the ID of the CAI network for groups that is set in the control station codeplug.

10. If the control station is only used to receive location coordinates from other radios, select the ***Data Channel*** check box.

NOTE
If the ***Data Channel*** check box is selected, the call parameters become unavailable.

11. Select the ***Phone Calls*** check box to allow other radios to receive and initiate phone calls over the control station.

NOTE
To make this feature work correctly, configure radios to interrupt control station transmissions and set a long hangtime in the radio system to which the control station belongs.

12. Configure data transmission over the control station:

To receive location updates from radios,	select the ***Location Service*** check box. ***Important*** SmartPTT assumes that the control station always uses the port *4001* to send radio location updates to SmartPTT Radioserver.
To receive information about radio presence in the network,	perform the following actions: 1. Select the ***Automatic Registration Service*** check box. 2. In the field to the right of the check box, enter the number of the port used to send presence check requests and receive presence data.
To support text messages and job tickets in the radio network,	perform the following actions: 1. Select the ***Text Message Service*** check box. 2. In the field to the right of the check box, enter the number of the port used to send and receive text messages.
To receive telemetry data and send telemetry commands,	perform the following actions: 1. Select the ***Telemetry Service*** check box. 2. In the field to the right of the check box, enter the number of the port used to send telemetry commands and receive telemetry data.

Important
The port numbers in the ***Automatic Registration Service***, ***Text Message Service***, and ***Telemetry Service*** fields must match the port numbers in the ***ARS***, ***Text messages***, and ***Telemetry*** fields in the ***Radio network services ports*** area of the RG-1000e remote adapter configuration. For details, see “Settings” in *RG-1000e Installation and Configuration Guide*.

13. From the ***TX Criteria*** list, select one of the following options:

If the control station is configured to transmit only when no other transmissions are detected over the radio channel,	select *Channel Free*.

If the control station is configured to notify other radios on interrupting their transmissions,	select *Tx Interrupt*.
If the control station is configured to completely ignore other transmissions over the radio channel,	select *Always*.

Important
SmartPTT does not support color code for outgoing transmissions.

14. In the ***Analog Call Hangtime, ms*** field, enter the maximum interval between transmissions over analog channels within one call.
15. From the ***GPS Transmission Mode*** list, select one of the following options:

If all digital channels support both CSBK data and enhanced GNSS,	select *Enhanced CSBK*.
If all digital channels support CSBK data, but not all of them support Enhanced GNSS,	select *CSBK*.
If digital channels have different settings,	select *Data*.

16. *(Optional)* To allow SmartPTT Radioserver register radios on the control station when it receives their GPS coordinates, select the ***Register radios when receiving GPS coordinates*** check box.

NOTE
When the ***Data Channel*** check box is selected, the ***Register radios when receiving GPS coordinates*** check box becomes automatically selected and unavailable to clear.

17. If you use the control station in analog radio systems with 5 Tone signaling, in the ***5 Tone signaling*** area, configure 5 Tone telegrams.

NOTE
At the moment, support for 5 Tone signaling in SmartPTT is carried out in a limited mode, therefore you should contact the SmartPTT Technical Support Center regarding the use of 5-tone signaling.

18. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (*** ***)***.

Postrequisites:

- Configure control station talkgroups. For details, see Configuring Remote MOTOTRBO Control Station Talkgroups.
- Configure control station channels. For details, see Configuring Remote MOTOTRBO Control Station Channels.
- Configure audio settings. For details, see Configuring Remote MOTOTRBO Control Station Audio Settings.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (*** ***)*** or ***Restart (*** ***)***.
- In the firewall software on the computer, unlock the set ports. For details, see Radioserver Host.

6.8.4.2 Configuring Remote MOTOTRBO Control Station Talkgroups

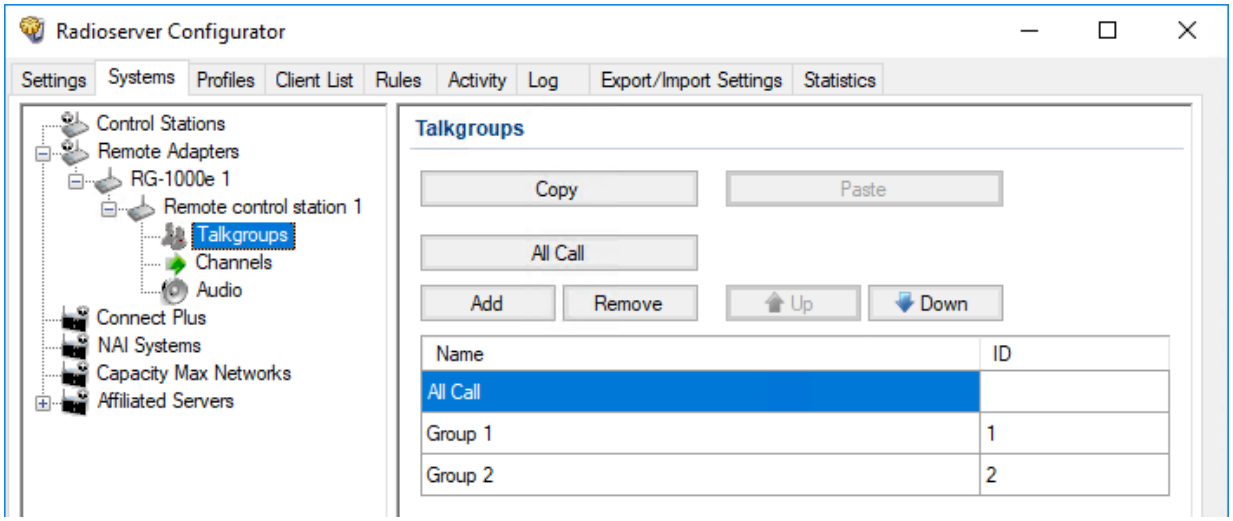
Follow the procedure to add new or edit existing talkgroups and an All Call entry that will be available to SmartPTT dispatchers.

Prerequisites:

- Configure the remote MOTOTRBO control station connection. For details, see Configuring Remote MOTOTRBO Control Station Connection.
- From the remote control station codeplug, obtain talkgroup IDs. To obtain the information, use the compatible MOTOTRBO CPS application.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***Remote Adapters*** → ***<Adapter Name>*** → ***<Control Station Name>***, and then select ***Talkgroups***. The list of groups appears in the right pane.



3. In the right pane, perform one of the following actions:

To add a new talkgroup,	click ***Add***.
To add an All Call entry,	click ***All Call***.
To edit an existing entry,	proceed to the next step.
To remove an existing entry,	perform the following actions: 1. Click the desired entry. 2. Click ***Remove***. 3. Proceed to the last step of this procedure.

4. For the desired entry in the table, perform the following actions:
   a. In the ***Name*** column, double-click the current name, and then type the desired name.

NOTE
The entered talkgroup names will be displayed in SmartPTT Dispatcher, SmartPTT Web Client, and SmartPTT Mobile.

   b. In the ***ID*** column, double-click the current talkgroup ID, and then type the desired ID.

NOTE
For All Call, the ID cell is empty.

5. *(Optional)* Using ***Up*** and ***Down*** buttons, reorder entries in the table. The order of talkgroups in SmartPTT Radioserver Configurator determines the order of talkgroups in SmartPTT Dispatcher and SmartPTT Web Client.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

6.8.4.3 Configuring Remote MOTOTRBO Control Station Channels

Follow the procedure to add new or edit existing channels of a remote MOTOTRBO control station.

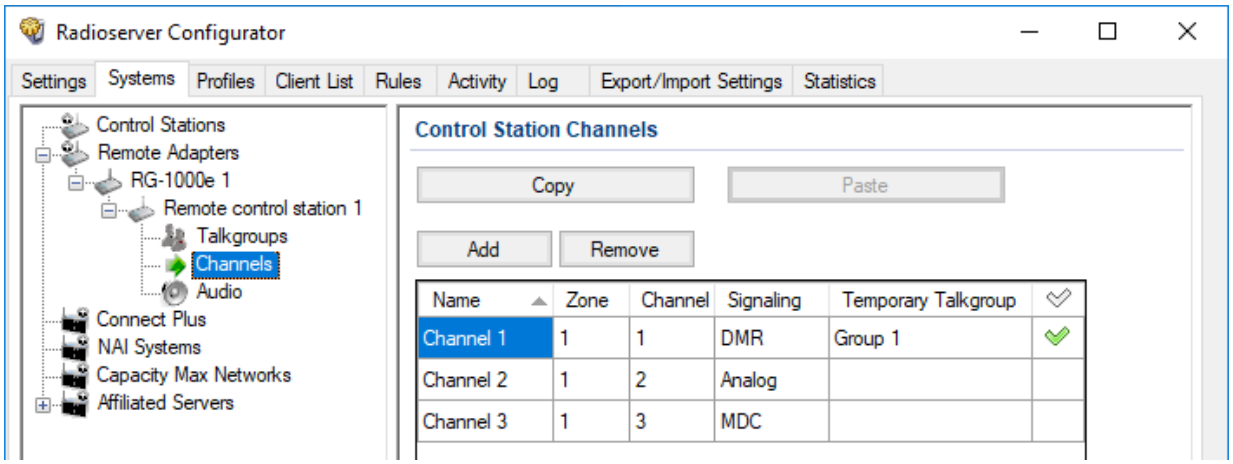
Prerequisites:

- Configure the remote MOTOTRBO control station connection. For details, see Configuring Remote MOTOTRBO Control Station Connection.
- From the control station codeplug, obtain the following information:
  - List of channels and their identification information (zone IDs and channel IDs).
  - Radio signaling type used on each channel.
  - Channel default contact (talkgroup ID or All Call).

  To obtain the information, use the compatible MOTOTRBO CPS application.
- Ensure that talkgroups and All Call are added to SmartPTT Radioserver Configurator. For details, see Configuring Remote MOTOTRBO Control Station Talkgroups.
- *(Optional)* Ensure that the necessary 5-tone telegrams are added to SmartPTT Radioserver Configurator.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***Remote Adapters*** → ***<Adapter Name>*** → ***<Control Station Name>***, and then select ***Channels***.
   The list of channels appears in the right pane.



3. In the right pane, perform one of the following actions:

To add a new channel,	click ***Add***.

To edit an existing entry,	proceed to the next step of the procedure.
To remove an existing channel,	perform the following actions: 1. Click the desired entry. 2. Click ***Remove***. 3. Proceed to the last step of this procedure.

4. For the desired entry in the table, perform the following actions:
   a. In the ***Name*** column, double-click the current channel name, and then type a new name.
   b. In the ***Zone*** field, double-click the current zone ID, and then type the desired ID.
   c. In the ***Channel*** column, double-click the current channel ID, and then type the desired ID.
   d. From the list in the ***Signaling*** column, select the radio signaling used on the radio channel or the desired 5-tone telegram.
   e. From the list in the ***Temporary Talkgroup*** column, select the talkgroup or All Call that is set as default contact on the channel.
5. After all channels are configured, in the Default Channel ( ) column, select the check box next to the channel that will be selected on the remote control station each time SmartPTT Radioserver is started or restarted.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

6.8.4.4 Configuring Remote MOTOTRBO Control Station Audio Settings

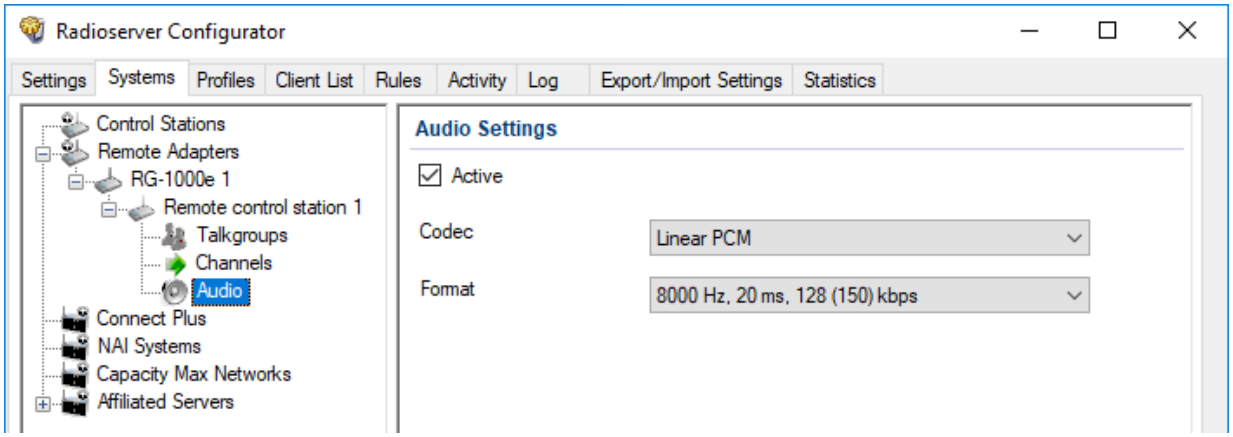
Follow the procedure to edit audio settings required to receive voice from a remote MOTOTRBO control station and send dispatcher voice to it.

Prerequisites:

Configure the remote MOTOTRBO control station connection. For details, see Configuring Remote MOTOTRBO Control Station Connection.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***Remote Adapters*** → ***<Adapter Name>*** → ***<Control Station Name>***, and then select ***Audio***.
   The audio settings appear in the right pane.



3. In the right pane, select the ***Active*** check box to unlock audio settings.
4. From the ***Codec*** list, select the desired voice transcoding algorithm.
5. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

6.8.5 MOTOTRBO Station Access over RG-2000

RG-2000 is a remote adapter intended to provide the remote access to control stations for SmartPTT.

Additional Features

If MOTOTRBO control station is connected over RG-2000, if provides the following additional features to SmartPTT:

- Alternate/redundant radioserver support.
- Configurable session initiator.
- Location reporting using option boards. For details, see Location with Option Boards.

Remote Adapter Configuration

To configure the adapter to support MOTOTRBO control stations connected over the digital-and-analog interface, the following actions must be performed:

- Control station must be connected to the adapter using Elcomplus, Inc. cable.
- Power supply and grounding must be configured correctly for control station gateway.

WARNING
Power connection may result in the unintended personnel injury or equipment damage. The connection must be performed with a qualified engineer who have the corresponding license.

- In remote adapter configuration file, the correct connection mode must be configured:

    - MOTOTRBO radio connection.
    - Control station connection.
- Adapter IP channel association with a physical radio port must be configured.
- *(Optional)* Audio gain/attenuation must be configured on the radio port.

For information on the remote adapter settings, see RG-2000 *Installation and Configuration Guide*.

For information on the analog connection of the MOTOTRBO control station to the remote adapter, see Analog Interfaces.

SmartPTT Configuration

To configure the control station connection over RG-2000 to the radioserver, the following actions must be performed:

- SmartPTT license with MOTOTRBO control station permissions must be installed. For details, see Installing License.
- Connection to the control station must be configured. For details, see Configuring Remote MOTOTRBO Control Station Connection.
- Talkgroups and All Call must be added. For details, see Configuring Remote MOTOTRBO Control Station Talkgroups.
- Control station channels must be configured. For details, see Configuring Remote MOTOTRBO Control Station Channels.
- Voice processing must be configured. For details, see Configuring Remote MOTOTRBO Control Station Audio Settings.

6.8.5.1 Configuring Remote MOTOTRBO Control Station Connection

Follow the procedure to add a new or edit an existing connection to a remote MOTOTRBO control station.

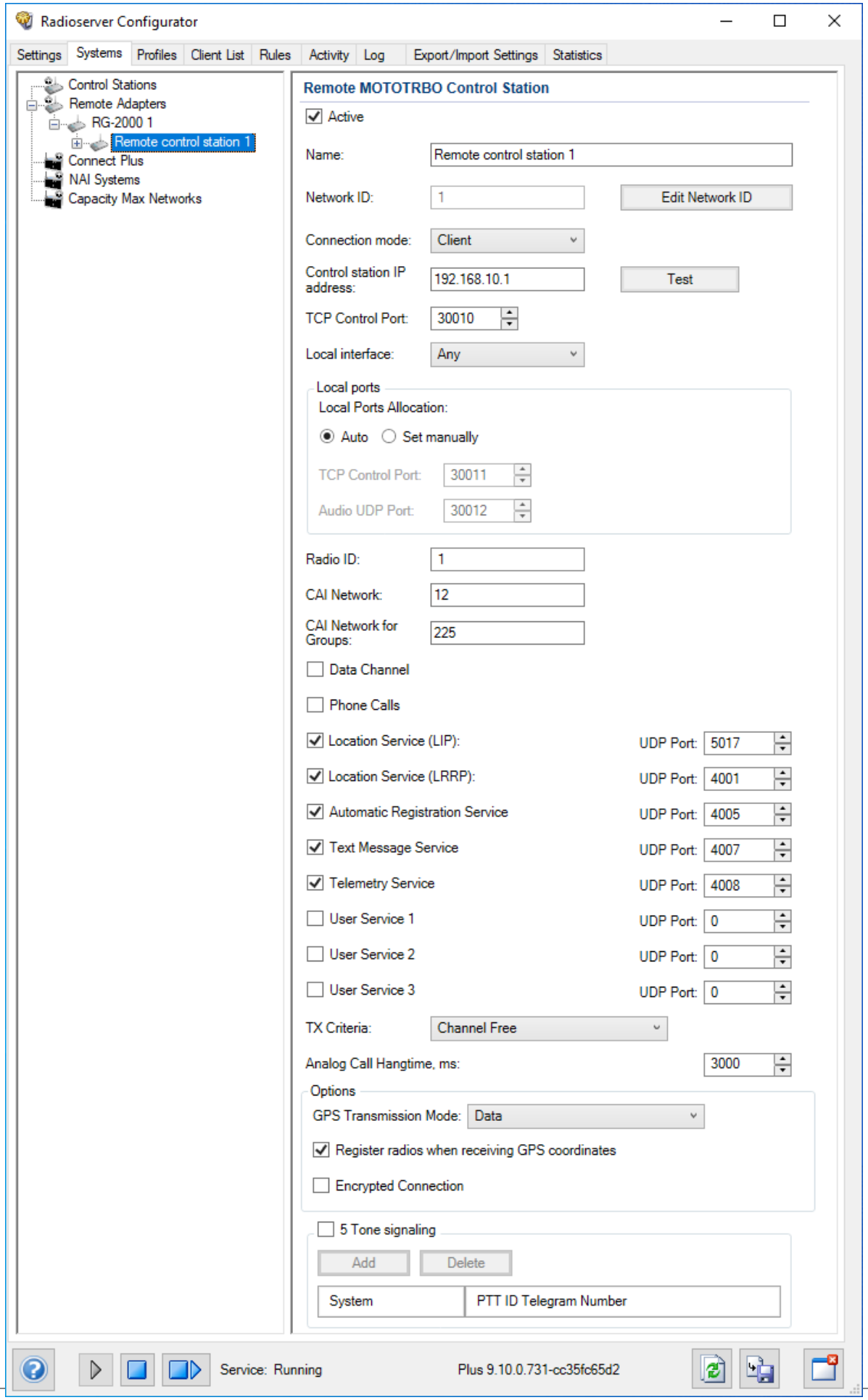
Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure SmartPTT license allows remote control stations access. For details, see Viewing License Items.
- From the control station codeplug, obtain the following information:
    - Radio ID, CAI network ID, and CAI Group ID
    - Transmit interruption parameters
    - The format of location data transmission in the control station
- Determine whether SmartPTT Radioserver or RG-2000 will initiate the connection.
- *(Optional)* If RG-2000 is configured to act as a server, from the RG-2000 configuration, obtain the IP address and port number configured for the desired control station.
- From the RG-2000 configuration, obtain control station ports used to receive and transmit various data types.
- *(Optional)* Determine SmartPTT Radioserver host ports that will be used to receive different data types from the control station.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, perform one of the following actions:

To add a remote MOTOTRBO control station to a new remote adapter,	perform the following actions: 1. Right-click ***Remote Adapters***, and then click ***Add → RG-2000***. The ***RG-2000*** node appears. 2. In the right pane, select the ***Active*** check box. 3. *(Optional)* In the ***Name*** field, type the adapter name. 4. In the left pane, right-click the ***RG-2000*** node, point to ***Add***, and then select ***Remote MOTOTRBO Control Station***.
To add a remote MOTOTRBO control station to an existing adapter,	perform the following actions: 1. Expand the ***Remote Adapters*** node. 2. Right-click the desired adapter name, point to ***Add***, and then select ***Remote MOTOTRBO Control Station***.
To edit an existing remote MOTOTRBO control station connection settings,	expand ***Remote Adapters → RG-2000***, and then click the desired control station.
To delete a remote MOTOTRBO control station connection,	perform the following actions: 1. Expand ***Remote Adapters → <Adapter Name>***. 2. Right-click the desired control station, and then select ***Delete***. 3. Proceed to the last step of the procedure.


Radioserver Configurator
Settings
Systems
Profiles
Client List
Rules
Activity
Log
Export/Import Settings
Statistics
Control Stations
Remote Adapters
RG-2000 1
Remote control station 1
Connect Plus
NAI Systems
Capacity Max Networks
Remote MOTOTRBO Control Station
Active
Name:
Remote control station 1
Network ID:
1
Edit Network ID
Connection mode:
Client
Control station IP address:
192.168.10.1
Test
TCP Control Port:
30010
Local interface:
Any
Local ports
Local Ports Allocation:
Auto
Set manually
TCP Control Port:
30011
Audio UDP Port:
30012
Radio ID:
1
CAI Network:
12
CAI Network for Groups:
225
Data Channel
Phone Calls
Location Service (LIP):
UDP Port:
5017
Location Service (LRRP):
UDP Port:
4001
Automatic Registration Service
UDP Port:
4005
Text Message Service
UDP Port:
4007
Telemetry Service
UDP Port:
4008
User Service 1
UDP Port:
0
User Service 2
UDP Port:
0
User Service 3
UDP Port:
0
TX Criteria:
Channel Free
Analog Call Hangtime, ms:
3000
Options
GPS Transmission Mode:
Data
Register radios when receiving GPS coordinates
Encrypted Connection
5 Tone signaling
Add
Delete
System
PTT ID Telegram Number
Service: Running
Plus 9.10.0.731-cc35fc65d2

3. In the right pane, select the ***Active*** check box to unlock control station settings.
4. In the ***Name*** field, type the control station name.
5. Leave the value in the ***Network ID*** field unchanged, or if necessary, edit the value after clicking the ***Edit Network ID*** button.
6. Configure the connection mode to the control station:

If RG-2000 is configured to accept SmartPTT connection (acts as a server),	perform the following actions: 1. From the ***Connection mode*** list, select *Client*. 2. In the ***Control station IP address*** field, type the remote adapter IP address to receive radioserver connections. 3. In the ***TCP Control Port*** field, enter the port number to receive radioserver connections.
If RG-2000 is configured to initiate SmartPTT connection (acts as a client),	perform the following actions: 1. From the ***Connection mode*** list, select *Server*. 2. In the ***Local TCP Control Port*** field, enter the SmartPTT Radioserver port number to listen to incoming connections.

7. From the ***Local interface*** list, select the desired option:

To use any radioserver IP address for the remote adapter connection,	select *Any*.
To use a fixed IP address for the remote adapter connection,	select the desired IP address.

8. *(Optional)* In the ***Local ports*** area, set SmartPTT Radioserver host ports for different types of data:

To set local ports automatically,	select *Auto*.
To set specific local port values,	perform the following actions: 1. Select *Set manually*. 2. If available, in the ***TCP Control Port*** field, enter the port number used to receive commands and service messages from the remote control station, and send commands and service messages to it. 3. In the ***Audio UDP Port*** field, enter the port number used to receive voice from the remote control station and send dispatcher voice to it.

9. Type the control station identification parameters:
    a. In the ***Radio ID*** field, type the control station ID specified in its codeplug

Important
Do not assign this ID to a client or radio in any radio network.

b. In the ***CAI Network*** field, type the ID of the CAI network that is set in the control station codeplug.

c. In the ***CAI Network for Groups*** field, type the ID of the CAI network for groups that is set in the control station codeplug.

10. If the control station is only used to receive location coordinates from other radios, select the ***Data Channel*** check box.

NOTE
If the ***Data Channel*** check box is selected, the call parameters become unavailable.

11. Select the ***Phone Calls*** check box to allow other radios to receive and initiate phone calls over the control station.

NOTE
To make this feature work correctly, configure radios to interrupt control station transmissions and set a long hangtime in the radio system to which the control station belongs.

12. Configure data transmission over the control station:

To receive radio coordinates over LIP,	perform the following actions: 1. Select the ***Location Service (LIP)*** check box. 2. In the ***UDP Port*** field to the right of the ***Location Service (LIP)*** check box, enter the port number used to receive and send this data.
To receive radio coordinates over LRRP,	perform the following actions: 1. Select the ***Location Service (LRRP)*** check box. 2. In the ***UDP Port*** field to the right of the ***Location Service (LRRP)***, enter the port number used to receive and send this data. ***Important*** SmartPTT assumes that the control station always uses the port *4001* to send radio location updates to SmartPTT Radioserver.
To receive information about radio presence in the network,	perform the following actions: 1. Select the ***Automatic Registration Service*** check box. 2. In the ***UDP Port*** field to the right of the ***Automatic Registration Service*** check box, enter the number of the port used to send presence check requests and receive presence data.
To support text messages and job tickets in the radio network,	perform the following actions: 1. Select the ***Text Message Service*** check box. 2. In the ***UDP Port*** field to the right of the ***Text Message Service*** check box, enter the number of the port used to send and receive text messages.
To receive telemetry data and send telemetry commands,	perform the following actions:

	1. Select the ***Telemetry Service*** check box. 2. In the ***UDP Port*** field to the right of the ***Telemetry Service*** check box, enter the number of the port used to send telemetry commands and receive telemetry data.
To receive client services data,	perform the following actions: 1. Select the ***User Service <Number>*** check box that corresponds to the control station configuration. 2. In the ***UDP Port*** field to the right of the ***User Service <Number>*** check box, enter the port number used to receive this data.

13. From the ***TX Criteria*** list, select one of the following options:

If the control station is configured to transmit only when no other transmissions are detected over the radio channel,	select *Channel Free*.
If the control station is configured to notify other radios on interrupting their transmissions,	select *Tx Interrupt*.
If the control station is configured to completely ignore other transmissions over the radio channel,	select *Always*.

Important
SmartPTT does not support color code for outgoing transmissions.

14. In the ***Analog Call Hangtime, ms*** field, enter the maximum interval between transmissions over analog channels within one call.
15. From the ***GPS Transmission Mode*** list, select one of the following options:

If all digital channels support both CSBK data and enhanced GNSS,	select *Enhanced CSBK*.
If all digital channels support CSBK data, but not all of them support Enhanced GNSS,	select *CSBK*.
If digital channels have different settings,	select *Data*.

NOTE
The ***GPS Transmission Mode*** list is unavailable if the ***Location Service (LRRP)*** check box is cleared.

16. *(Optional)* To allow SmartPTT Radioserver register radios on the control station when it receives their GPS coordinates, select the ***Register radios when receiving GPS coordinates*** check box.

NOTE
If the ***Data Channel*** check box is selected, the ***Register radios when receiving GPS coordinates*** check box becomes automatically selected and unavailable for clearing.
The ***Register radios when receiving GPS coordinates*** check box is unavailable if the ***Location Service (LRRP)*** check box is cleared.

17. *(Optional)* To enable encrypted connection between SmartPTT and the RG-2000, select the ***Encrypted Connection*** check box.

    NOTE
    The ***Encrypted Connection*** check box is unavailable if the ***Location Service (LRRP)*** check box is cleared.

18. If you use the control station in analog radio systems with 5 Tone signaling, in the ***5 Tone signaling*** area, configure 5 Tone telegrams.

NOTE
At the moment, support for 5 Tone signaling in SmartPTT is carried out in a limited mode, therefore you should contact the SmartPTT Technical Support Center regarding the use of 5-tone signaling.

19. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Configure control station talkgroups. For details, see Configuring Remote MOTOTRBO Control Station Talkgroups.
- Configure control station channels. For details, see Configuring Remote MOTOTRBO Control Station Channels.
- Configure audio settings. For details, see Configuring Remote MOTOTRBO Control Station Audio Settings.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- In the firewall software on the computer, unlock the set ports. For details, see Radioserver Host.

6.8.5.2 Configuring Remote MOTOTRBO Control Station Talkgroups

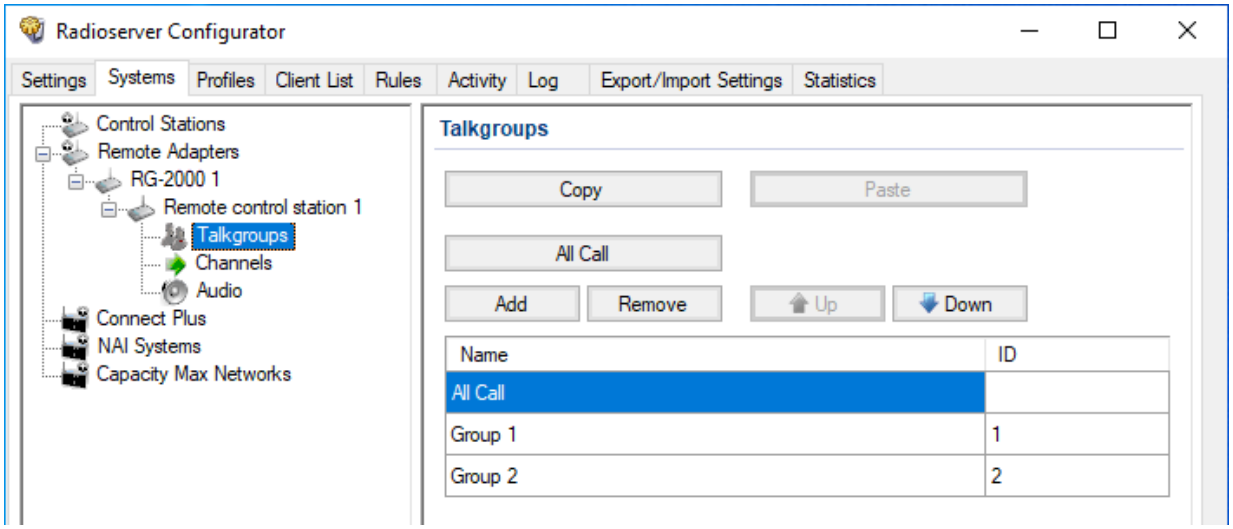
Follow the procedure to add new or edit existing talkgroups and an All Call entry that will be available to SmartPTT dispatchers.

Prerequisites:

- Configure the remote MOTOTRBO control station connection. For details, see Configuring Remote MOTOTRBO Control Station Connection.
- From the remote control station codeplug, obtain talkgroup IDs. To obtain the information, use the compatible MOTOTRBO CPS application.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***Remote Adapters*** → ***RG-2000*** → ***<Control Station Name>***, and then select ***Talkgroups***.
   The list of groups appears in the right pane.



3. In the right pane, perform one of the following actions:

To add a new talkgroup,	click ***Add***.
To add an All Call entry,	click ***All Call***.
To edit an existing entry,	proceed to the next step.
To remove an existing entry,	perform the following actions: 1. Click the desired entry. 2. Click ***Remove***. 3. Proceed to the last step of this procedure.

4. For the desired entry in the table, perform the following actions:
   a. In the ***Name*** column, double-click the current name, and then type the desired name.

NOTE
The entered talkgroup names will be displayed in SmartPTT Dispatcher, SmartPTT Web Client, and SmartPTT Mobile.

   b. In the ***ID*** column, double-click the current talkgroup ID, and then type the desired ID.

NOTE
For All Call, the ID cell is empty.

5. *(Optional)* Using ***Up*** and ***Down*** buttons, reorder entries in the table. The order of talkgroups in SmartPTT Radioserver Configurator determines the order of talkgroups in SmartPTT Dispatcher and SmartPTT Web Client.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

6.8.5.3 Configuring Remote MOTOTRBO Control Station Channels

Follow the procedure to add new or edit existing channels of a remote MOTOTRBO control station that is used to receive and initiate calls into a talkgroup.

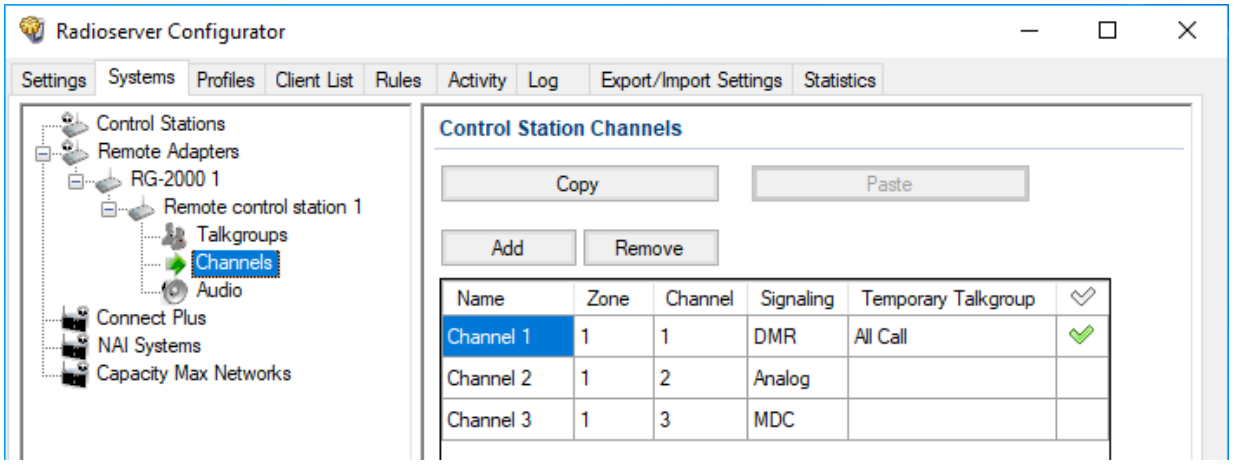
Prerequisites:

- Configure the remote MOTOTRBO control station connection. For details, see Configuring Remote MOTOTRBO Control Station Connection.
- From the control station codeplug, obtain the following information:
  - List of channels and their identification information (zone IDs and channel IDs).
  - Radio signaling type used on each channel.
  - Channel default contact (talkgroup ID or All Call).

  To obtain the information, use the compatible MOTOTRBO CPS application.
- Ensure that talkgroups and All Call are added to SmartPTT Radioserver Configurator. For details, see Configuring Remote MOTOTRBO Control Station Talkgroups.
- *(Optional)* Ensure that the necessary 5-tone telegrams are added to SmartPTT Radioserver Configurator.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***Remote Adapters*** → ***RG-2000*** → ***<Control Station Name>***, and then select ***Channels***.
   The list of channels appears in the right pane.



3. In the right pane, perform one of the following actions:

To add a new channel,	click ***Add***.
To edit an existing entry,	proceed to the next step of the procedure.
To remove an existing channel,	perform the following actions: 1. Click the desired entry. 2. Click ***Remove***. 3. Proceed to the last step of this procedure.

4. For the desired entry in the table, perform the following actions:
   a. In the ***Name*** column, double-click the current channel name, and then type a new name.
   b. In the ***Zone*** field, double-click the current zone ID, and then type the desired ID.
   c. In the ***Channel*** column, double-click the current channel ID, and then type the desired ID.
   d. From the list in the ***Signaling*** column, select the radio signaling used on the radio channel or the desired 5-tone telegram.
   e. From the list in the ***Temporary Talkgroup*** column, select the talkgroup or All Call that is set as default contact on the channel.
5. After all channels are configured, in the Default Channel ( ) column, select the check box next to the channel that will be selected on the remote control station each time SmartPTT Radioserver is started or restarted.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

6.8.5.4 Configuring Remote MOTOTRBO Control Station Audio Settings

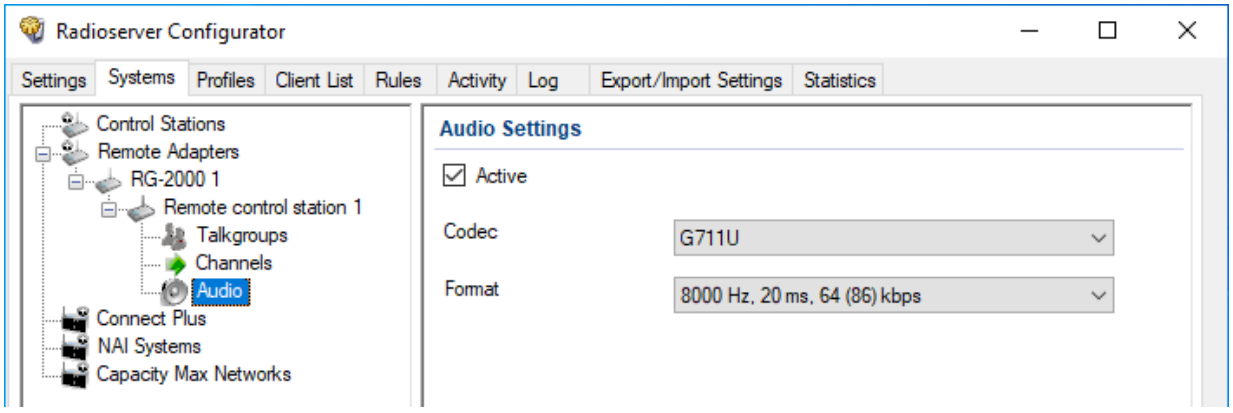
Follow the procedure to edit audio settings required to receive voice from a remote MOTOTRBO control station and send dispatcher voice to it.

Prerequisites:

- Configure the remote MOTOTRBO control station connection. For details, see Configuring Remote MOTOTRBO Control Station Connection.
- From the RG-2000 configuration file, obtain the voice transcoding algorithm.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***Remote Adapters*** → ***RG-2000*** → ***<Control Station Name>***, and then select ***Audio***.
   The audio settings appear in the right pane.



3. In the right pane, select the ***Active*** check box to unlock audio settings.
4. From the ***Codec*** list, select the desired voice transcoding algorithm.

Important
The algorithm must match the codec selected in the RG-2000 configuration.

5. *(Optional)* If you selected *Opus* from the ***Codec*** list, select the desired values of sampling frequency and frame length from the ***Format*** list.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

6.9 Settings Duplication

To significantly simplify the network configuration, you can duplicate various settings in control stations, conventional, and trunked radio systems. These settings include:

- Talkgroups and All Calls
- Security keys
- MNIS connection parameters (only for Linked Capacity Plus and IP Site Connect systems)

For duplication, each ***Talkgroups***, ***Security Settings*** and ***MNIS Settings*** pane of the SmartPTT Radioserver Configurator provides the ***Copy*** and ***Paste*** buttons. Copying and pasting are available within SmartPTT Radioserver Configurator only. No settings can be pasted to a text file that is opened in the operating system.

SmartPTT does ***not*** provide tools to import settings from radio codeplugs, repeater codeplugs, configuration files of the MOTOTRBO software, and trunked radio system controllers (Connect Plus and Capacity Max).

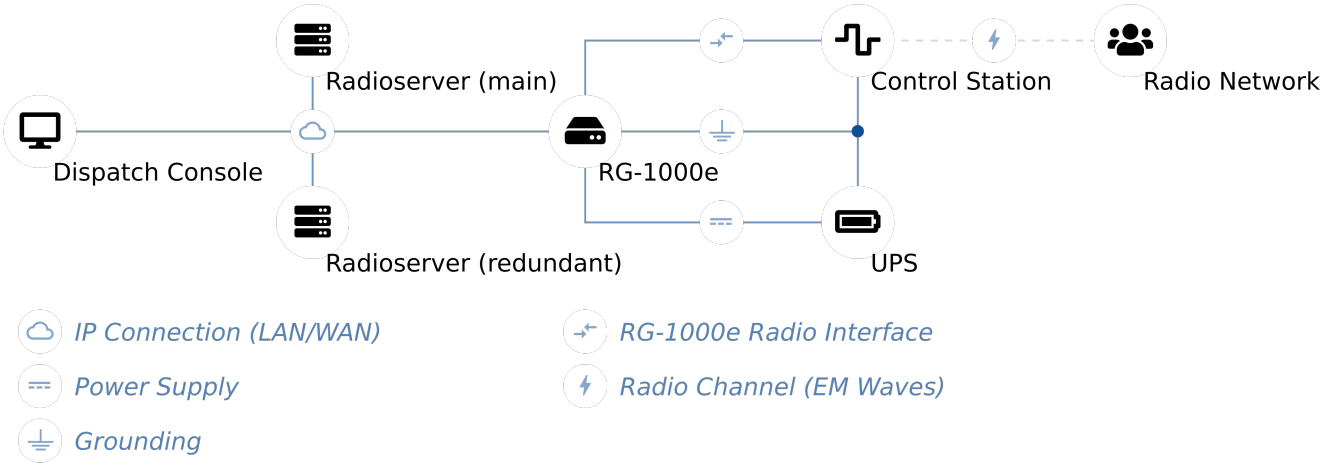
7 Other VoIP Systems

In addition to MOTOTRBO, SmartPTT supports the following communication systems with VoIP capabilities:

- Analog radio systems. For details, see Analog Radio Systems.
- P25 radio systems. For details, see P25 Radio Systems.
- Phone systems over SIP trunk. For details, see SIP Telephony.

7.1 P25 Radio Systems

P25 (also known as Project 25 or APCO) is a digital mobile radio standard designed for use by public safety organizations. SmartPTT is able to access such systems using control stations. In particular, it uses APX™ mobile radios for such purposes. For details, visit APX™ Series P25 Two-Way Radios on the Motorola Solutions website.



SmartPTT supports Analog 4-wire connection over RG-1000e. This involves the use of the C-APX ver 1-1 cable and operation in the *Radio I/O* mode. For details, see Analog Interfaces.

Important
Analog connection only supports voice. It does ***not*** support analog signaling.

Important
For information on the supported models of APX control stations, contact Elcomplus, Inc. representatives in your region.

Using APX radios as control stations implies that they are not operated directly. This includes the following:

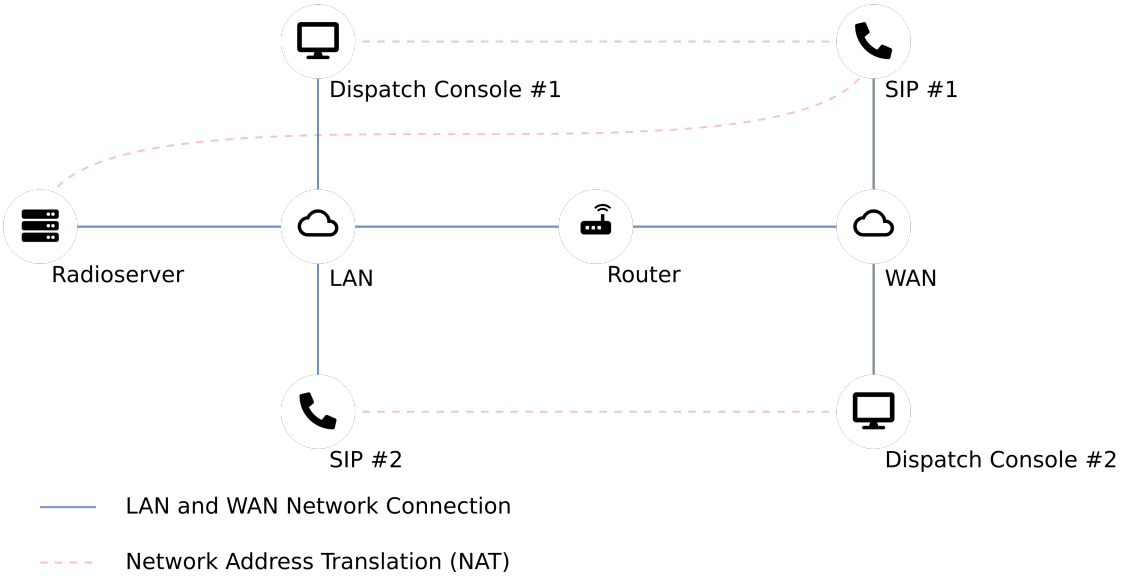
- No person must switch channels on the control station using Control Head buttons or other controls.
- No person must transmit from the radio using Control Head buttons or handsets.

Violation of these requirements results in data desynchronization between SmartPTT and the control station.

7.2 SIP Telephony

SmartPTT supports voice communication between any digital radio system and the Customer's phone system that is based on the Session Initiation Protocol (SIP trunk) and supports user agent connections (radioserver and dispatch consoles).

NOTE
In telephony, user agent connections are client connections based on SIP trunk.



SmartPTT Dispatcher can also have connection to a PBX separately from SmartPTT Radioserver (to the same or another PBX). For details, see "Telephone Interconnect" in *SmartPTT Dispatcher Guide*.

General Requirements for PBX

To support SmartPTT Radioserver connection, the private branch exchange (PBX) must comply with the following requirements:

- Radioserver account must belong to the known domain/workgroup in the PBX settings.
- *(Optional)* SmartPTT Radioserver must have the dedicated user account in PBX.
- All phone devices that are connected to PBX must use the same vocoder.

For detailed information on requirements for PBX, submit a request to the SmartPTT Technical Support Center.

7.2.1 Telephony Features

SmartPTT provides the following features when integrates phone systems and radio systems:

- Various call types:
  - Voice call from a radio network to a phone number.
  - Voice call from a telephone number to a talkgroup or the All Call ID.
  - Voice call from a telephone number to a radio.
- Call initiation request using text messages.
- Calling party authentication. For details, see Telephony Connection Overview.

- Service tones playback (grant tones, hang up tones).
- Software-based volume gain for calls.
- Call masks for private and group calls from a telephone number. For details, see Call Masks.
- Radioserver autoreply. For details, see Configuring Autoreply.

7.2.1.1 Call Process

Phone call between a radio and a telephone number is a complex type of call for the following reasons:

- Radios operate in half-duplex mode (either receive or transmit voice).
- Phones operate in full-duplex mode (receive and transmit at once).

As a result, the call is performed in the following way:

- When the call is established, radio starts receiving audio from the phone.
- When the radio user wants to transmit, they press PTT. At this, the following changes occur:
  - Radio stops hearing phone user and starts transmitting.
  - Phone user starts hearing radio user's voice.
  - Phone user's voice is ignored (not sent to the radio network).
- When the radio user stops transmitting, they release PTT. At this, the following changes occur:
  - Radio starts receiving audio from the phone again.
  - Phone user stops hearing radio user's voice.

If the radio that is involved in the phone call receives a call from another radio, it ends the phone call and starts receiving incoming call from the radio network.

7.2.2 Telephony Connection Overview

SmartPTT connection to PBX for the following phone system and radio system integration, requires the following:

- Planning requirements compliance.
- Additional radio devices configuration.
- Dispatch software configuration.

Important
All of the following information (except SmartPTT configuration) is the minimum required modification. It is not sufficient for system integration. For more information and/or configuration assistance, submit a request to SmartPTT Technical Support Center.

Planning Requirements

To implement the system integration, all communication parties must have unique Radio IDs. This includes the following:

- Radios.

- Radioserver (if accesses repeater-based systems).
- Control stations.
- Dispatchers (if authentication is turned on in desktop clients).

If radioserver accesses repeater-based systems, the following system elements must have unique peer IDs (may also be referred to as “repeater radio IDs”):

- Repeaters.
- Radioserver.
- MNIS VRC service of the Capacity Max radio system.

Except this, masks must be determined for phone calls. For details, see Call Masks.

Additional Radio Devices Configuration

In networks with control stations, radios must be able to interrupt incoming calls.

In repeater-based systems, perform the following actions:

- Call start and call end codes must be configured. For details, see Phone Call Codes.
- Phone gateway ID must be configured:
  - For IP Site Connect — gateway ID must be equal to Peer ID of SmartPTT Radioserver.
  - For networks over NAI — gateway ID must be equal to Radio ID.

In the Capacity Max radio system, telephone calls between radio and telephone subscribers can occur in one of the two modes: on the control channel or on the voice channel. You can select the desired mode in the trunking controller.

If you use MOTOTRBO™ equipment, you can select the desired mode in the trunking controller configuration file, in the ***Phone Call Setup Method*** parameter:

- To make phone calls on the control channel, in the ***Phone Call Setup Method*** parameter, select the ***Dialing Digits on Control Channel (as per DMR3)*** option, and in SmartPTT Radioserver Configurator, in Capacity Max settings, select the ***Control Channel*** mode.
- To make phone calls on the voice channel, in the ***Phone Call Setup Method*** parameter, select the ***Dialing Digits on Payload Channel option*** option, and in SmartPTT Radioserver Configurator, in Capacity Max settings, select the ***Voice Channel*** mode.

Important
Telephony is unavailable in Connect Plus.

SmartPTT Configuration

To configure SmartPTT Radioserver, perform the following actions:

- Install SmartPTT license with the Telephone Interconnect permission. For details, see Installing License.
- Configure phone call parameters. For details, see Configuring Phone Calls.
- Connect Radioserver to PBX. For details, see Connecting to PBX.
- *(Optional)* Limit radio access to phone system. For details, see Limiting Access to PBX.

- Configure phone call processing for calls from the telephone network to the radio network. For details, see Configuring Incoming Calls.
- *(Optional)* Configure radioserver autoreply. For details, see Configuring Autoreply.
- Configure phone call processing for calls from the radio network to the telephone network. For details, see Configuring Outgoing Calls.

7.2.2.1 Call Masks

Call masks are used by radioserver for different call types:

- Group phone calls (from a phone to a talkgroup or All Call).
- Private phone calls (from a phone to a radio).

Private Call Mask

To provide private phone calls, no mask is recommended to be used. In this case, phone user must perform the following actions:

1. User dials the radioserver number (as configured in PBX).
2. When radioserver is accessed, user dials the Radio ID of the required radio.

Group Call Masks

Group call masks is the required mask type, especially if the private call mask is not configured. Otherwise, any call from the phone to a radio network will be considered as a private call.

For group phone calls, one of the following masks is recommended to be used:

Mask	Description
0 or 0T	Contains the following expressions: • 0 is a number that never appears in the first position of the Radio ID number. • T is an expression for “any number of digits”. Recommended to be used when radioserver connects to a single radio system.
0NT	Contains the following expressions: • 0 is a number that never appears in the first position of the Radio ID number. • N is a network ID. • T is an expression for “any number of digits”. Recommended to be used when radioserver connects to multiple radio systems that have the same talkgroup IDs or All Call ID.
0ST	Contains the following expressions: • 0 is a number that never appears in the first position of the Radio ID number. • S is the slot ID.

Mask	Description
	• T is an expression for “any number of digits”. Recommended to be used when the following conditions are fulfilled: • Radioserver connects to IP Site Connect with two or more slots that are not used as data channels. • List of talkgroups is equal on those slots.
0NST	Contains all the expressions described above. Recommended to be used when SmartPTT integrated multiple complex systems. ***NOTE*** Radioserver automatically determines number of positions for each ID.

To initiate a group call using the 0NST mask, phone users must perform the following actions:

1. Dial the radioserver number (as configured in PBX).
2. When radioserver is accessed, dial *0*.
3. Identify a network:

To specify a network,	dial network ID.
To avoid the network specification,	dial *0*.

4. If a call is intended to IP Site Connect, identify a slot:

To determine the first wide slot,	dial *1*.
To determine the second wide slot,	dial *2*.
To determine another (local slot),	dial slot ID.
To avoid the network specification,	dial *0*.

5. Enter the required target ID:

To initiate a call to a talkgroup,	dial talkgroup ID.
To initiate an All Call,	dial *0*. ***NOTE*** Do not use a standard All Call ID.

Masks Syntax

Call masks may include one or several of the following expressions:

Expression	Description
.	Any single digit in the specific position.

[a-f]	A single Latin letter from the specified range may occur in this particular position. ***Important*** Lowecase letters must be used.
[a,b,c]	One of the specified Latin letters may occur in a position. ***Important*** Lowecase letters must be used.
[abc]	Same as [a,b,c].
T	Starting the current position, any amount of digits can be entered that will be interpreted as a single parameter.
(.)	OR operator for multiple masks.
{}	Content of such brackets must be included in the parameter.
N	Specific network ID or the *0* value that is equivalent to “ANY”. Applicable to group phone calls only.
S	Specific slot ID or the *0* value that is equivalent to “ANY”. Applicable to group phone calls only.

7.2.2.2 Phone Call Codes

To initiate and end phone calls, specific codes must be configured in radio codeplugs. They are configured in the Dual-Tone Multi-Frequency (DTMF) format. The format determines the following set of characters to be used:

- All arabic digits (from 0 to 9).
- Latin letters “A”, “B”, “C”, and “D”.
- The asterisk character (*).
- The number/hash/pound character (#).

Codes are recommended to comply with the following requirements:

- Each code must consists of at least two characters.
- Each code must include either asterisk, or hash.

EXAMPLE

Call initiation code: *1

Call end code: #1

7.2.3 Configuring Phone Calls

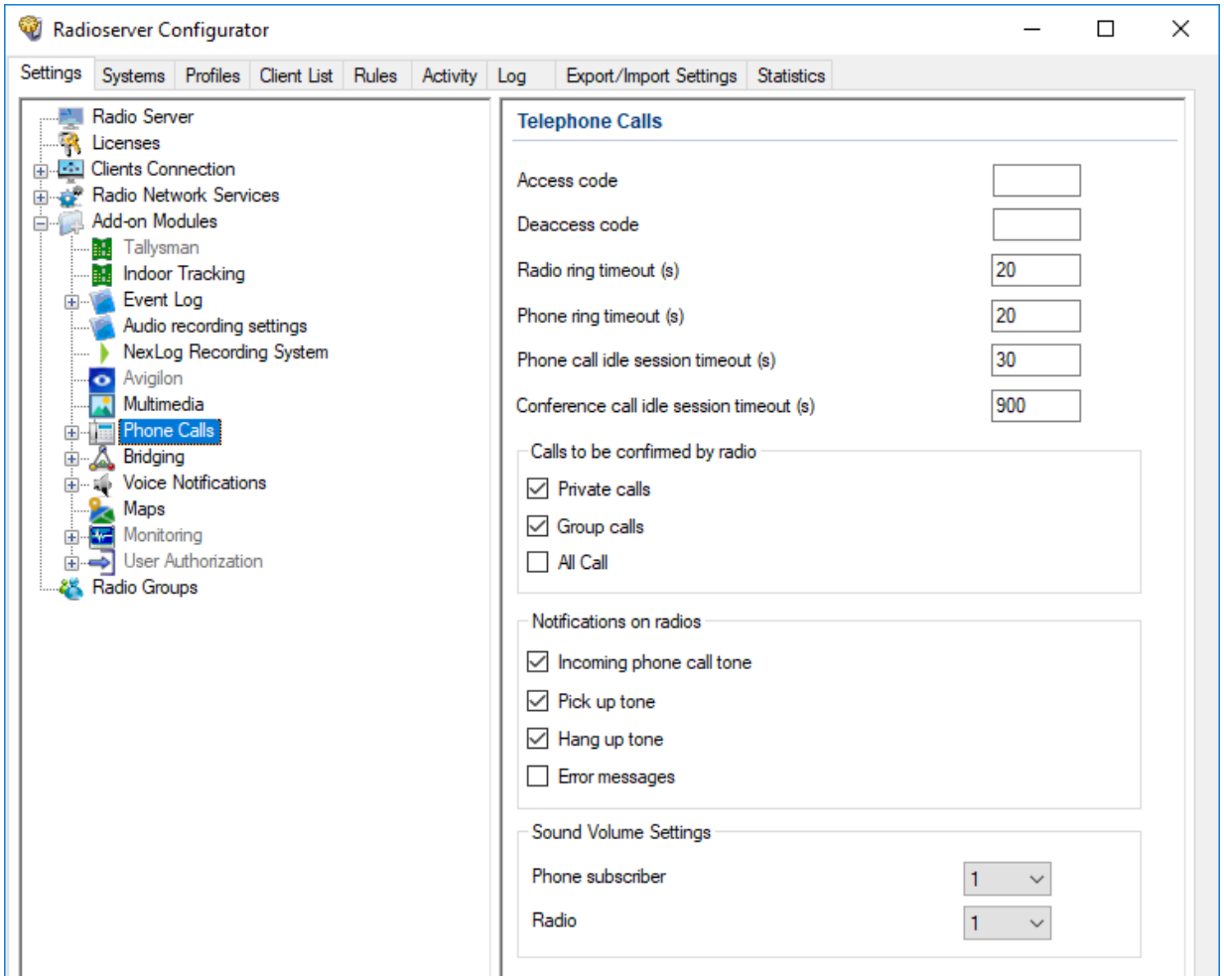
Follow the procedure to configure phone call processing in SmartPTT.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure that SmartPTT license allows telephone interconnect. For details, see Viewing License Items.
- Obtain access and deaccess codes configured in radios.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Add-on Modules***, and then click ***Phone Calls***.
   The phone call settings appear in the right pane.



3. In the right pane, in the ***Access code*** field, type the code to initiate a phone call from the radio.
4. In the ***Deaccess code*** field, type the code to end a phone call from the radio.
5. In the ***Radio ring timeout (s)*** field, type the maximum wait time for a radio to accept a call from a phone subscriber.
6. In the ***Phone ring timeout (s)*** field, type the maximum wait time for a phone subscriber to accept a call from a radio.
7. In the ***Phone call idle session timeout (s)*** field, type the maximum wait time for a radio to transmit during a phone call.

8. In the ***Conference call idle session timeout (s)*** field, type the maximum wait time for a radio to transmit during a conference call.
9. In the ***Calls to be confirmed by radio*** area, perform the following actions:

To require confirmation of private calls by radios,	select the ***Private calls*** check box.
To require confirmation of group calls by radios,	select the ***Group calls*** check box.
To require confirmation of all calls by radios,	select the ***All Calls*** check box.

10. Configure notification of radios about phone call status:

To notify radios about waiting for the phone subscriber to pick up,	select the ***Incoming phone call tone*** check box.
To notify radios that the phone subscriber has accepted the call (picked up),	select the ***Pick up tone*** check box.
To notify radios that the phone subscriber has ended the call (hung up),	select the ***Hang up*** check box.
To notify radios that SmartPTT Radioserver has failed to initiate the call,	select the ***Error messages*** check box.

11. *(Optional)* Configure software-based volume gain for call participants:
    a. From the ***Phone subscriber*** list, select the desired amplification factor for phone subscriber voice transmissions.
    b. From the ***Radio*** list, select the desired amplification factor for radio user voice transmissions.
12. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

7.2.4 Connecting to PBX

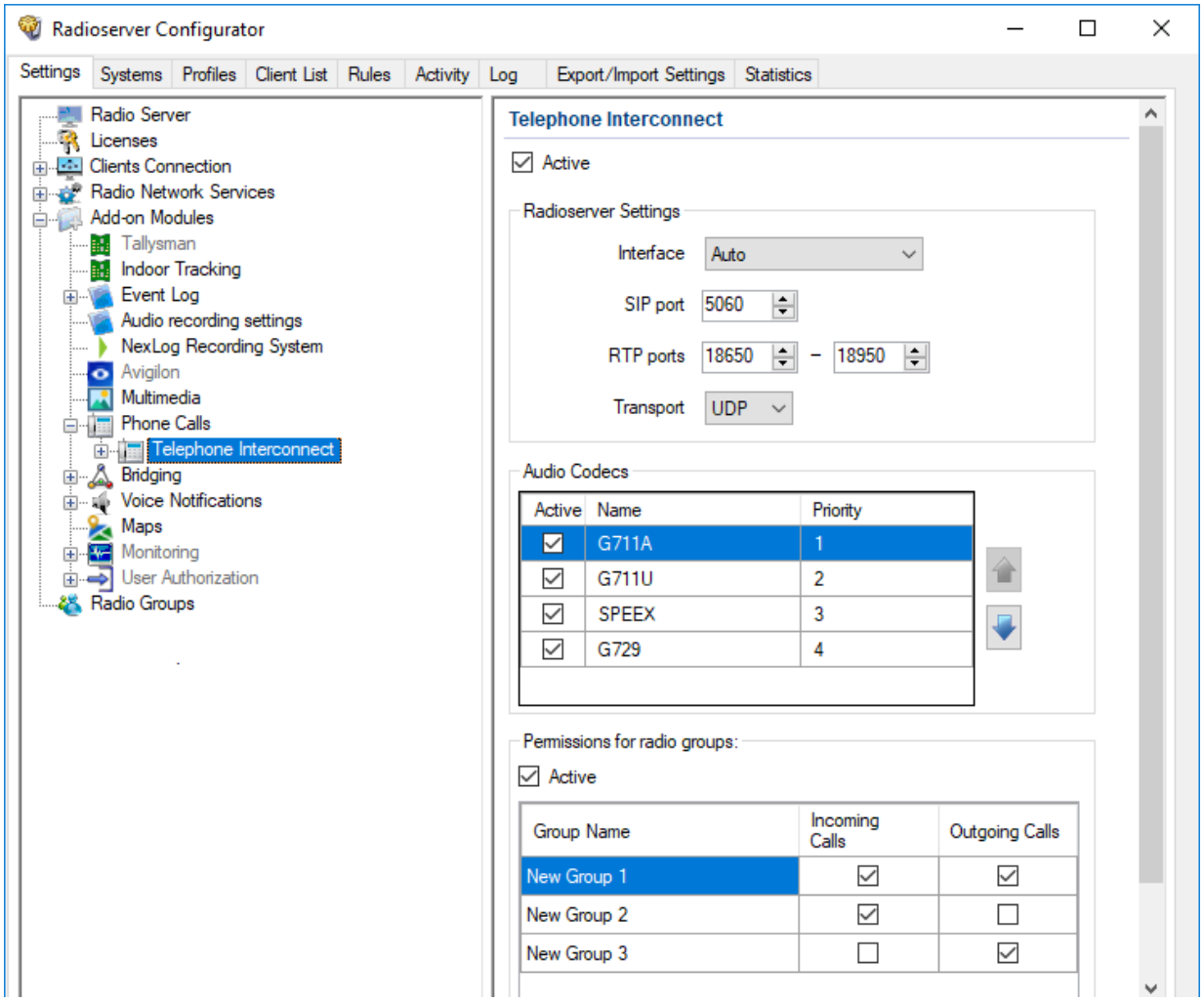
Follow the procedure to configure the connection between SmartPTT Radioserver and PBX.

Prerequisites:

- Ensure that SmartPTT license allows Telephone Interconnect. For details, see Viewing License Items.
- Obtain the IP address, network ports and communication protocols used to connect SmartPTT Radioserver to PBX.
- Obtain the list of voice codecs supported by PBX, telephones and telephone gateways.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Add-on Modules*** → ***Phone Calls***, and then click ***Telephone Interconnect***.
   The PBX connection settings appear in the right pane.



3. In the right pane, select the ***Active*** check box.
4. In the ***Radioserver Settings*** area, perform the following actions:
   a. From the ***Interface*** list, select the desired option:

To use any radioserver IP address,	select *Auto*.
To use fixed radioserver IP address,	select the specific IP address.

   b. In the ***SIP port*** field, enter the radioserver port number to be used for PBX connection.
   c. In the ***RTP ports*** fields, enter the lower and upper boundary of the UDP port range to be used for voice traffic between SmartPTT Radioserver and PBX.

Important
Number of ports in the range must be equal to the maximum number of simultaneous phone calls over a radioserver.

   d. From the ***Transport*** list, select the desired transport protocol:

If TCP is configured in PBX,	select *TCP*.
If UDP is configured in PBX,	select *UDP*.

5. In the ***Audio Codecs*** area, perform the following actions:

a. In the table, in the ***Active*** column, select the check boxes of codecs supported by PBX and telephone gateways (if available).

b. Configure codec priority:

To increase vocoder use priority,	perform the following actions: 1. Click the desired codec in the table. 2. Click ***Increase priority (*** ***)*** to move the codec up in the table.
To decrease vocoder use priority,	perform the following actions: 1. Click the desired codec in the table. 2. Click ***Decrease priority (*** ***)*** to move the codec down in the table.

6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (*** ***)***.

Postrequisites:

- *(Optional)* Limit access to the telephone network for radios. For details, see Limiting Access to PBX.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (*** ***)*** or ***Restart (*** ***)***.
- In the firewall software on the computer, unlock the set ports. For details, see Radioserver Host.

7.2.4.1 Limiting Access to PBX

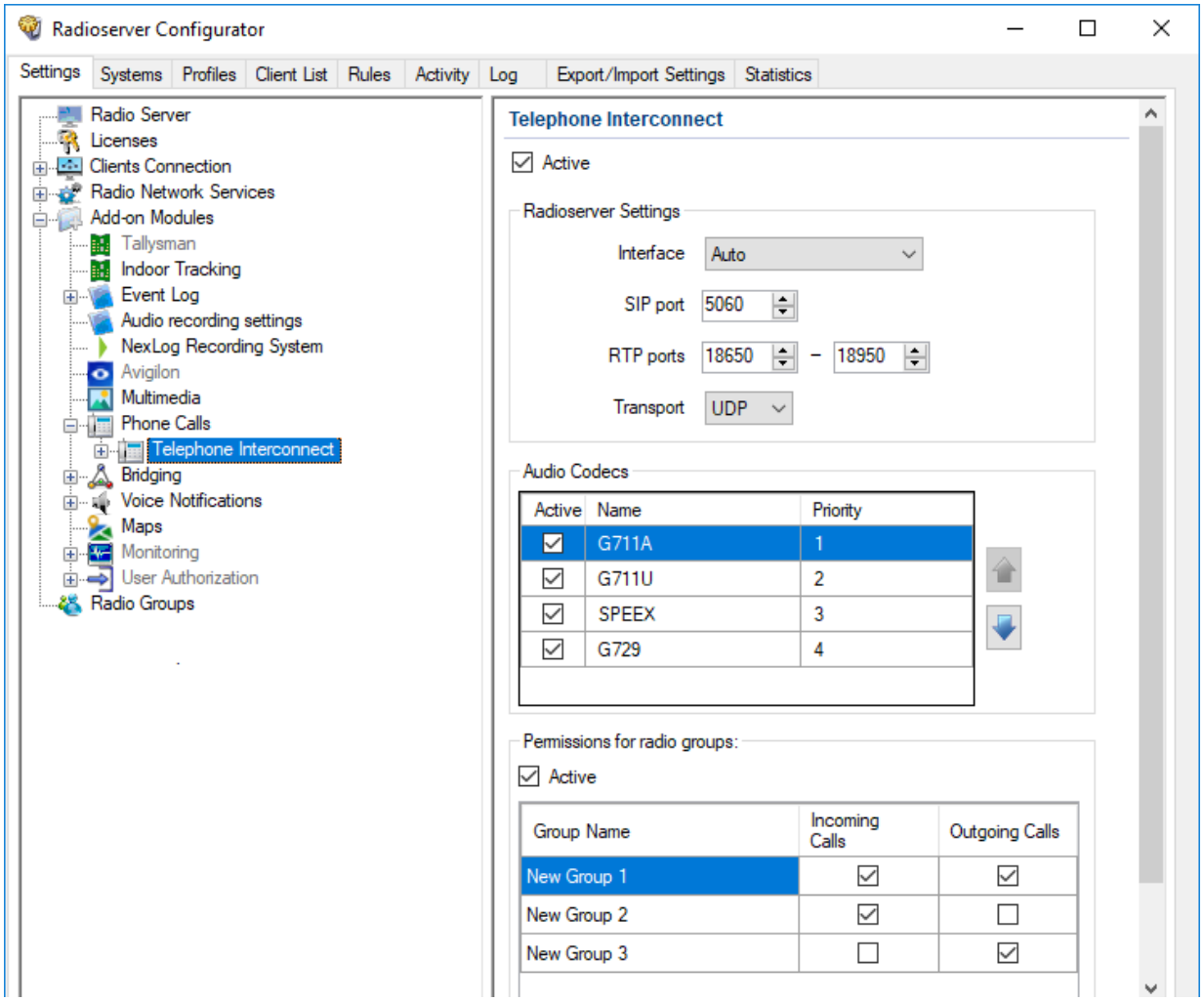
Follow the procedure to limit radios access to the phone system.

Prerequisites:

- Configure radioserver connection to PBX. For details, see Connecting to PBX.
- Create and configure desired groups of radios. For details, see Managing Radio Groups.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Add-on Modules*** → ***Phone Calls***, and then click ***Telephone Interconnect***.
   The PBX connection settings appear in the right pane.



3. In the right pane, in the ***Permissions for radio groups*** area, select the ***Active*** check box.
4. For each radio group in the table, perform the following actions:

To allow private phone calls to radios,	in the ***Incoming Calls*** column, select the check box.
To allow group phone calls confirmation to radios,	in the ***Incoming Calls*** column, select the check box.
To allow radios in the group to initiate calls to phone subscribers,	in the ***Outgoing Calls*** column, select the check box.

5. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

7.2.5 Configuring Incoming Calls

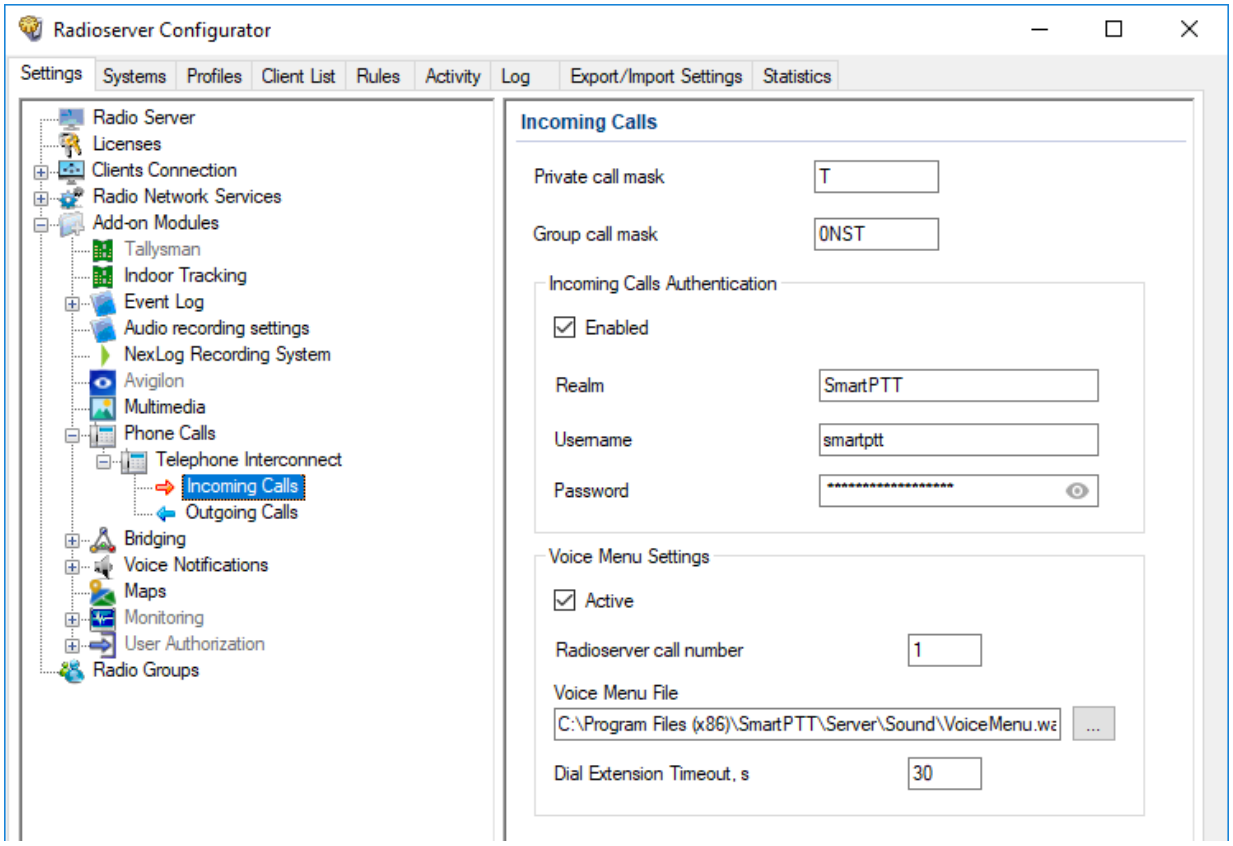
Follow the procedure to configure handling of phone calls from telephone network to the radio network.

Prerequisites:

- Configure PBX connection. For details, see Connecting to PBX.
- From PBX configuration, obtain the credentials (username, password, and realm) to use for authentication.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Add-on Modules*** → ***Phone Calls*** → ***Telephone Interconnect***, and then click ***Incoming Calls***. Incoming phone calls settings appear in the right pane.



3. *(Optional)* In the right pane, in the ***Private call mask*** field, type the desired mask.
4. In the ***Group call mask*** field, type the desired mask (the recommended mask is *0NST*).
5. In the ***Incoming Calls Authentication*** area, configure phone subscriber authentication:
   a. Select the ***Enabled*** check box.
   b. In the ***Realm*** field, type the name of the realm the phone user must belong to.
   c. In the ***Username*** field, type the name of the account to be used for authentication.
   d. In the ***Password*** field, type the corresponding password. To view the entered password, click the eye icon ( ). For security reasons, the password will not be available for viewing in subsequent sessions.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Configure SmartPTT Radioserver voice menu for incoming calls from the telephone network. For details, see Configuring Autoreply.
- Configure outgoing calls (from radio network to the telephone network). For details, see Configuring Outgoing Calls.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

7.2.6 Configuring Autoreply

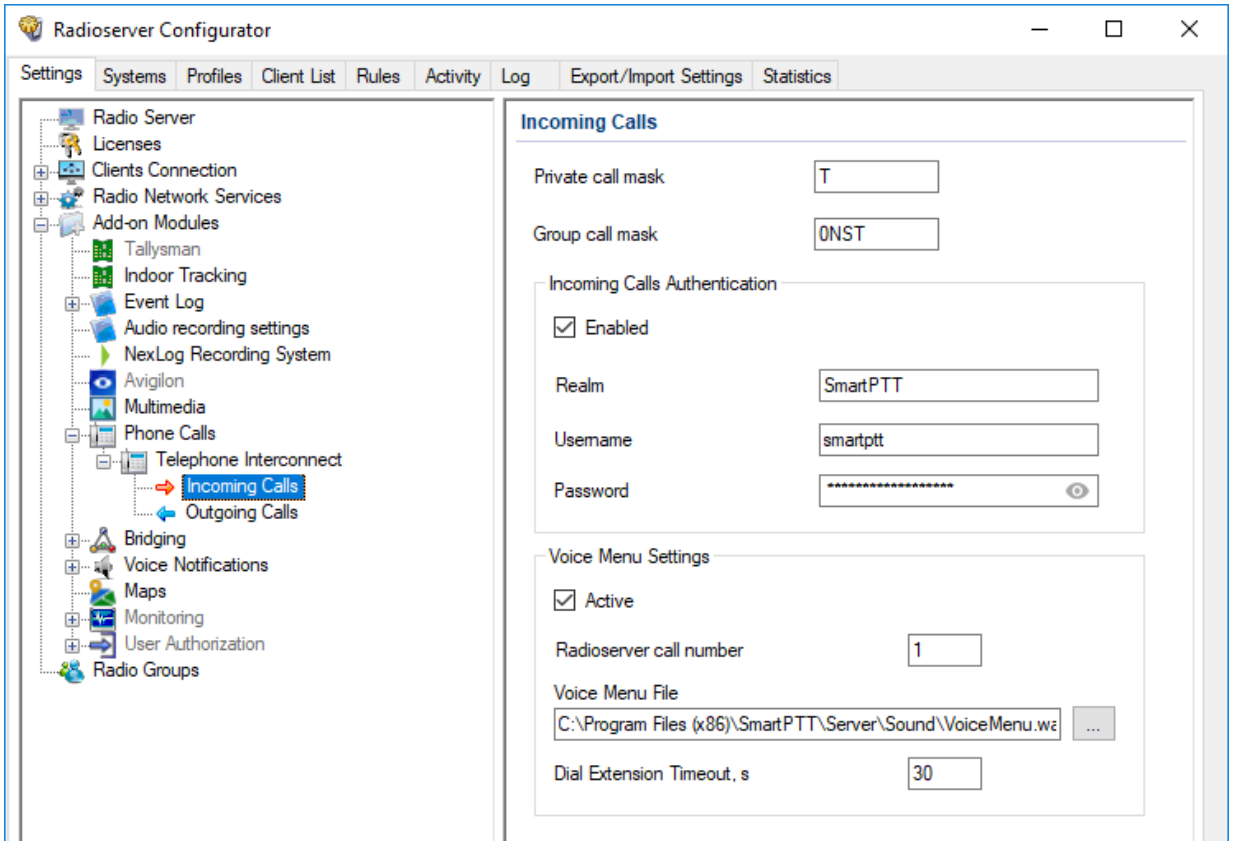
Follow the procedure to configure the radioserver autoreply to phone users when they initiate a phone call.

Prerequisites:

- In PBX, configure the radioserver dial number.
- Create an audio file to use as an autoreply. For details, see Audio File Requirements.
- Determine the maximum wait time for a telephone subscriber to dial the number for calls to the radio network.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Add-on Modules*** → ***Phone Calls*** → ***Telephone Interconnect***, and then click ***Incoming Calls***.
   The incoming calls settings appear in the right pane.



3. In the right pane, in the ***Voice Menu Settings*** area, select the ***Active*** check box.
4. In the ***Radioserver call number*** field, type the radioserver dial number.
5. Configure the audio file:
   a. Next to the ***Voice Menu File*** heading, click the Browse (...) button.
      The dialog box appears.
   b. In the dialog box, select the desired file.
6. In the ***Dial Extension Timeout, s*** field, type the maximum wait time for the phone user to dial the number that initiates a call to the radio network.

Important
The phone subscriber must dial the extension number after the voice menu audio file finishes playing, and then press #.

7. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

7.2.7 Configuring Outgoing Calls

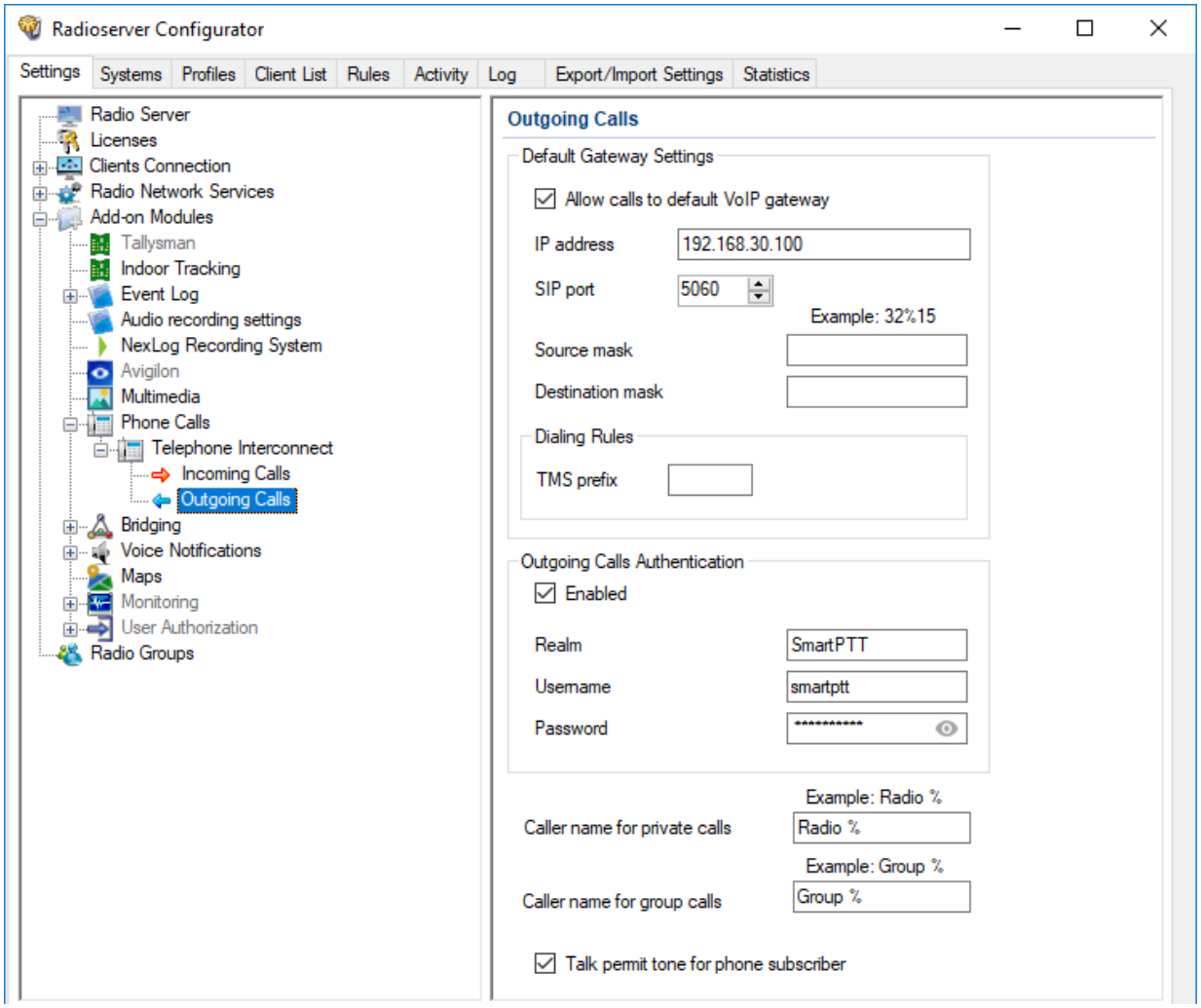
Follow the procedure to configure the handling of calls from radio network to telephone network.

Prerequisites:

- Configure PBX connection. For details, see Connecting to PBX.
- Obtain the PBX connection settings (IP address and port number).
- From the PBX settings, obtain the credentials (realm, username and password) required for SmartPTT Radioserver authentication.
- From the PBX settings, obtain the codes used to access the desired telephone network as well as prefixes and/or postfixes for callbacks.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Add-on Modules*** → ***Phone Calls*** → ***Telephone Interconnect***, and then click ***Outgoing Calls***.
   The outgoing call settings appear in the right pane.



3. In the right pane, configure radioserver connection to PBX:
   a. Select the ***Allow calls to default VoIP gateway*** check box.
   b. In the ***IP address*** field, type PBX IP address in dot-decimal notation.
   c. In the ***SIP port*** field, type the PBX port number to which SmartPTT Radioserver will connect.
   d. In the ***Source mask*** field, type the expression to be dialed by phone subscribers to call back radios. Use the "%" character to be substituted by the caller radio ID.
   e. In the ***Destination mask*** field, type the expression to be entered by radios to call back phone subscribers. Use the "%" character to be substituted by the caller phone number.
4. *(Optional)* To configure outgoing call initiation by sending a text message to radioserver ID, in the ***Dialing Rules*** area, type the TMS text.
5. In the ***Outgoing Calls Authentication*** area, configure SmartPTT Radioserver authentication:

If PBX requires authentication,	perform the following actions: 1. Select the ***Enabled*** check box. 2. In the ***Realm*** field, type the name of the realm that SmartPTT Radioserver account belongs to.

	3. In the ***Username*** field, type the name of SmartPTT Radioserver account in PBX. 4. In the ***Password*** field, type the password of SmartPTT Radioserver account in PBX. To view the entered password, click the eye icon ( ). For security reasons, the password will not be available for viewing in subsequent sessions.
If PBX does ***not*** require authentication,	clear the ***Enabled*** check box.

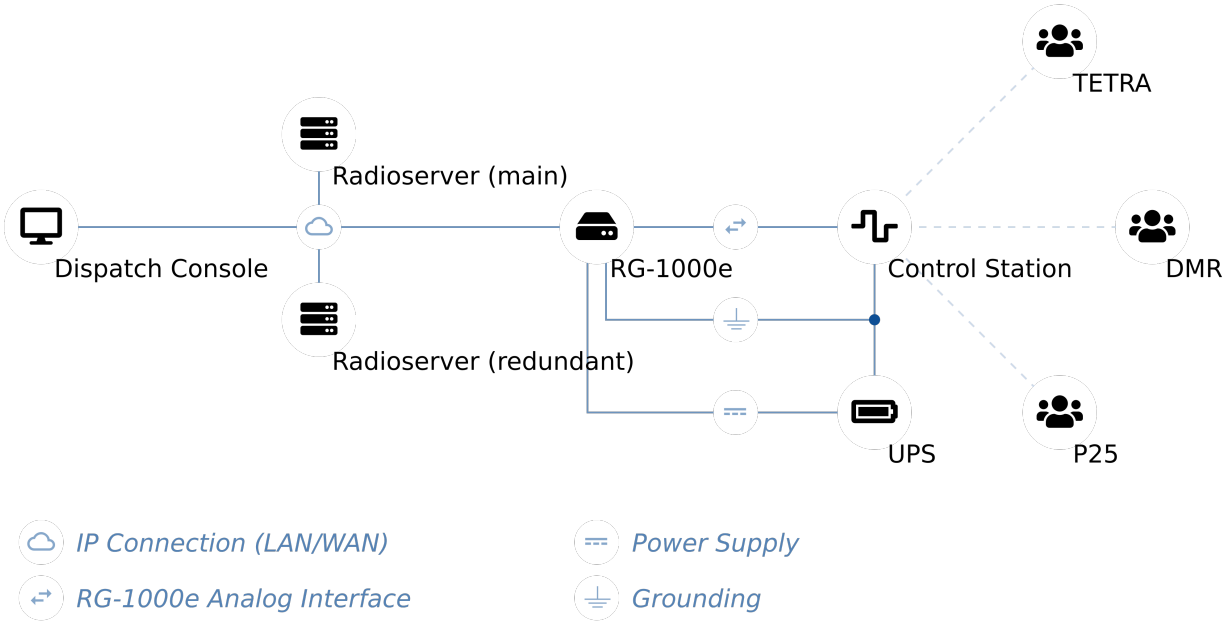
6. *(Optional)* Configure the caller name format (appears on the phone display):
   a. In the ***Caller name for private calls*** field, type the caller name format for private calls.
   b. In the ***Caller name for group calls*** field, type the caller name format for group calls.
7. Select the ***Talk permit tone for phone subscriber*** check box to play a call permit tone/grant tone that informs phone users that they can speak.
8. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

7.3 Analog Interfaces

In SmartPTT, “analog interface“ refers to the control station connection interface that provides only voice reception and transmission. The interface is completely provided by the RG-1000e remote adapter only.



Interface provides the following features:

- Control station channel selection.
- Voice reception on the channel (incoming transmission).

- Voice transmission on the channel (outgoing transmission).

The interface does ***not*** support PTT ID (call target), Call ID (initiator), radio commands, and the wireline control station operation. For details, submit a request to the SmartPTT Technical Support Center.

Analog interface may be referred to as “E&M”. The reference is incorrect. E&M implies specific connection types and voltage levels on the interface pins.

Information on radio models and the corresponding radio systems is available in the RG-1000e documentation. For additional information, contact Elcomplus, Inc. representative in your region.

Using mobile/base radios as control stations implies that they are ***not*** operated directly. This includes the following:

- No person must switch channels on the control station using Control Head buttons or other controls.
- No person must transmit from the radio using Control Head buttons or handsets.

Violation of such requirements results in the data desynchronization between SmartPTT and a control station.

7.3.1 Analog Interface Configuration over RG-1000e

Analog interface configuration requires the following:

- Control station configuration. For details, see “Control Station Configuration” below.
- Additional digital radios configuration. For details, see “Remote Adapter Configuration” below.
- SmartPTT configuration. For details, see “SmartPTT Configuration” below.

Important
Information below provides the minimum required changes in radio equipment settings. It is ***not*** sufficient for operation. For configuration assistance, submit a request to SmartPTT Technical Support Center.

Control Station Configuration

To connect a base/mobile radio to SmartPTT over the analog interface and use in as a control station, the following changed must be performed:

- Control station GPIO pins must be configured for the following purposes:
  - Audio output
  - Audio input
  - PTT signal reception
  - Incoming call detection (VOX, CSQ, or other)
- If channel selection is required, the following actions must be performed:
  - Up to 4 additional pins must be configured for channel selection.
  - All control station channels must be configured in the zone with ID = 1 (if multiple zones are supported).

Remote Adapter Configuration

To configure RG-1000e for analog interface support, the following actions must be performed:

- Control station must be connected to the adapter using the dedicated cable. For details, see *RG-1000e Installation and Configuration Guide*.
- Power supply and grounding must be configured correctly for control station gateway.

WARNING
Power connection may result in the unintended personnel injury or equipment damage. The connection must be performed with a qualified engineer who have the corresponding license.

- In the remote adapter configuration file, the correct connection mode must be configured:
  - IO connection mode.
  - Control station connection.
- Adapter IP channel must be associated with the corresponding radio port.
- Radio port pinout must be configured in accordance with the control station model and voice detection mode in the control station.
- *(Optional)* Audio gain/attenuation must be configured for the radio port.

For information on the adapter settings, see *RG-1000e Installation and Configuration Guide*.

SmartPTT Configuration

To configure the control station connection over the analog interface, the following actions must be performed:

- SmartPTT license with RG-1000e permission must be installed. For details, see Installing License.
- Connection to the control station must be configured. For details, see Configuring Station Connection over Analog Interface.
- Control station channels must be configured. For details, see Configuring Channels for Analog Interface.
- Voice processing must be configured. For details, see Configuring Audio Processing over Analog Interface.

7.3.1.1 Configuring Station Connection over Analog Interface

Follow the procedure to add a new or edit an existing connection to a remote I/O control station.

Prerequisites:

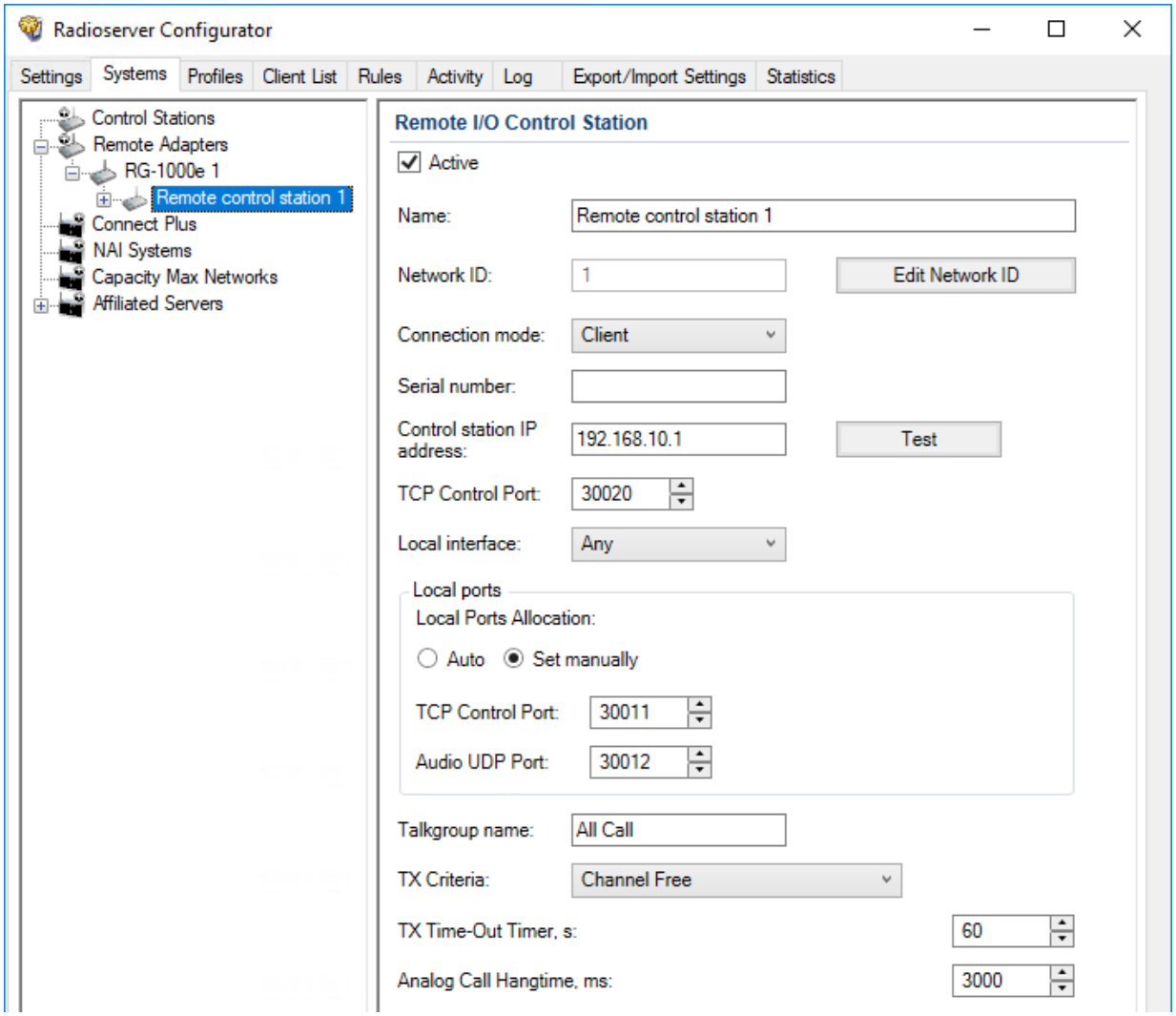
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure that SmartPTT license allows control station connection over analog interface. For details, see Viewing License Items.
- Determine whether SmartPTT Radioserver or RG-1000e will initiate the connection.
- *(Optional)* If RG-1000e is configured to act as a server, from the RG-1000e configuration file, obtain the IP address and port number configured for the desired control station.

- *(Optional)* From the control station codeplug, obtain the control station serial number.
- *(Optional)* Determine SmartPTT Radioserver host ports that will be used to receive XCMP and audio data from the control station.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, perform one of the following actions:

To add a remote I/O control station to a new adapter,	perform the following actions: 1. Right-click the ***Remote Adapters*** node, and then click ***Add → RG-1000e***. 2. In the right pane, select the ***Active*** check box. 3. *(Optional)* In the ***Name*** field, type the adapter name. 4. In the left pane, right-click the ***<Adapter Name>*** node, point to ***Add***, and then select ***Remote I/O Control Station***.
To add a remote I/O control station to an existing adapter,	perform the following actions: 1. Expand the ***Remote Adapters*** node. 2. Right-click the desired adapter name, point to ***Add***, and then select ***Remote I/O Control Station***.
To edit an existing remote I/O control station connection settings,	expand ***Remote Adapters → <Adapter Name>***, and then click the desired control station.
To delete a remote I/O control station connection,	perform the following actions: 1. Expand ***Remote Adapters → <Adapter Name>***. 2. Right-click the desired control station, and then select ***Delete***. 3. Proceed to the last step of the procedure.



3. In the right pane, select the ***Active*** check box to unlock control station settings.
4. In the ***Name*** field, type the control station name.
5. Leave the value in the ***Network ID*** field unchanged, or edit the value after clicking the ***Edit Network ID*** button.
6. Configure the connection mode to the control station:

If RG-1000e is configured to accept SmartPTT connection (server),	perform the following actions: 1. From the ***Connection mode*** list, select *Client*. 2. In the ***Control station IP address*** field, type the remote adapter IP address to receive radioserver connections. 3. *(Optional)* To check if you have specified the control station IP address correctly, click ***Test***. After checking you will see a message with the result. 4. In the ***TCP Control Port*** field, enter the port number to receive radioserver connections.

Important
The IP address and port number in the fields above must match the IP address and port number in the ***IP address*** and ***Port XCMP protocol*** fields in the ***Gateway IP settings*** area of the RG-1000e configuration. For details, see "IP channel" in *RG-1000e Installation and Configuration Guide*.

If RG-1000e is configured to initiate SmartPTT connection (client),	perform the following actions: 1. From the ***Connection mode*** list, select the *Server* mode. 2. In the ***Local TCP Control Port*** field, enter the SmartPTT Radioserver port number to listen to incoming connections. ***Important*** The port number in this field must match the port number in the ***Port XCMP protocol*** field in the ***Remote Gateway IP settings*** area of the RG-1000e configuration. For details, see "IP channel" in *RG-1000e Installation and Configuration Guide*.

7. From the ***Local Interface*** list, select the desired option:

To use any radioserver IP address for the adapter connection,	select *Any*.
To use a fixed IP address for the remote adapter connection,	select the desired IP address. ***Important*** If you select *Server* from the ***Connection mode*** list, a fixed IP address must match the IP address in the ***IP address*** field in the ***Remote Gateway IP settings*** area of the corresponding IP channel in the RG-1000e configuration.

8. *(Optional)* In the ***Local ports*** area, set SmartPTT Radioserver host ports to receive data:

To set local ports automatically,	select *Auto*.
To set specific local port values,	perform the following actions: 1. Select *Set manually*. 2. In the ***TCP Control Port*** field, enter the port number to use for commands and service messages exchange between the radioserver and the adapter. 3. In the ***Audio UDP Port*** field, enter the port number to use for voice receiving and transmission.

9. *(Optional)* Configure the following options:
   a. In the ***Serial number*** field, enter the control station serial number.

b. In the ***Talkgroup name*** field, enter the control station talkgroup name.

10. From the ***TX Criteria*** list, select one of the following options:

If the control station is configured to transmit only when no other transmissions are detected over the radio channel,	select *Channel Free*.
If the control station is configured to completely ignore other transmission over the radio channel,	select *Always*.

Important
SmartPTT does not support color code criteria for outgoing transmissions.

11. In the ***TX Time-Out Timer, s*** field, enter the maximum duration of voice transmission on the channel.
12. In the ***Analog Call Hangtime, ms*** field, enter the maximum interval between transmissions over analog channels within one call.
13. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Configure control station channels. For details, see Configuring Channels for Analog Interface.
- Configure audio settings. For details, see Configuring Audio Processing over Analog Interface.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- *(Optional)* In the firewall software on the computer, unlock the set ports. For details, see Radioserver Host.

7.3.1.2 Configuring Channels for Analog Interface

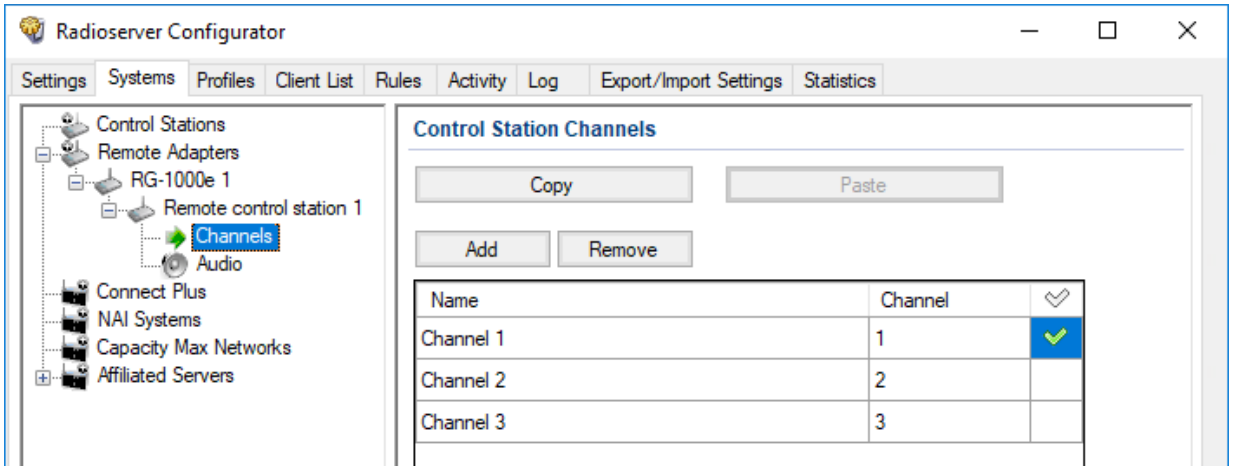
Follow the procedure to add new or edit existing channels of a remote I/O control station.

Prerequisites:

- Configure the control station connection. For details, see Configuring Station Connection over Analog Interface.
- Configure the control station GPIO pins to switch channels.
- Configure all control station channels in the first zone.
- Determine the default control station channel.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***Remote Adapters*** → ***<Adapter Name>*** → ***<Control Station Name>***, and then select ***Channels***.
The list of channels appears in the right pane.



3. In the right pane, perform one of the following actions:

To add a new channel,	click ***Add***.
To edit an existing entry,	proceed to the next step of the procedure.
To remove an existing channel,	perform the following actions: 1. Click the desired entry. 2. Click ***Remove***. 3. Proceed to the last step of this procedure.

4. For the desired entry in the table, perform the following actions:
   a. In the ***Name*** column, double-click the current channel name, and then type a new name.
   b. In the ***Channel*** column, double-click the current channel ID, and then type the desired channel ID.
5. When all channels are added, in the Default Channel ( ) column, select the check box next to the channel that will be selected on the remote control station each time SmartPTT Radioserver is started or restarted.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

7.3.1.3 Configuring Audio Processing over Analog Interface

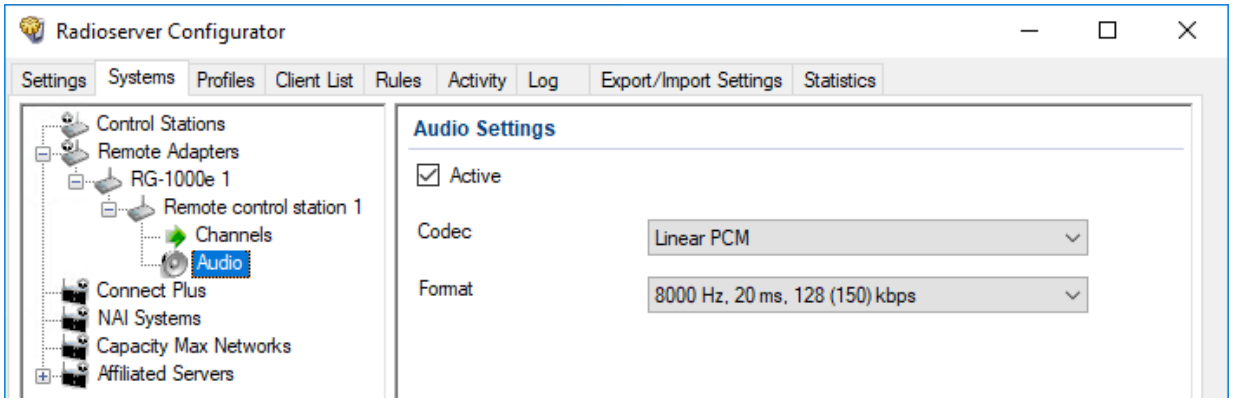
Follow the procedure to edit audio processing settings required to receive voice from an I/O control station and send dispatcher voice to it.

Prerequisites:

Configure the control station connection. For details, see Configuring Station Connection over Analog Interface.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***Remote Adapters*** → ***<Adapter Name>*** → ***<Control Station Name>***, and then select ***Audio***.
   The audio settings appear in the right pane.



3. In the right pane, select the ***Active*** check box to unlock audio settings.
4. From the ***Codec*** list, select the desired voice transcoding algorithm.
5. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (***  ***)***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (******)*** or ***Restart (******)***.

7.3.2 Analog Interface Configuration over RG-2000

Analog interface configuration requires the following:

- Control station configuration. For details, see “Control Station Configuration” below.
- Additional digital radios configuration. For details, see “Remote Adapter Configuration” below.
- SmartPTT configuration. For details, see “SmartPTT Configuration” below.

Important
Information below provides the minimum required changes in radio equipment settings. It is ***not*** sufficient for operation. For configuration assistance, submit a request to SmartPTT Technical Support Center.

Control Station Configuration

To connect a base/mobile radio to SmartPTT over the analog interface and use in as a control station, the following changed must be performed:

- Control station GPIO pins must be configured for the following purposes:
  - Audio output
  - Audio input
  - PTT signal reception
  - Incoming call detection (VOX, CSQ, or other)
- If channel selection is required, the following actions must be performed:

- Up to 4 additional pins must be configured for channel selection.
- All control station channels must be configured in the zone with ID = 1 (if multiple zones are supported).

Remote Adapter Configuration

To configure RG-2000 for analog interface support, the following actions must be performed:

- Control station must be connected to the adapter using the dedicated cable. For details, see *RG-2000 Installation and Configuration Guide*.
- Power supply and grounding must be configured correctly for control station gateway.

WARNING
Power connection may result in the unintended personnel injury or equipment damage. The connection must be performed with a qualified engineer who have the corresponding license.

- In the remote adapter configuration file, the correct connection mode must be configured:
  - IO connection mode.
  - Control station connection.
- Adapter IP channel must be associated with the corresponding radio port.
- Radio port pinout must be configured in accordance with the control station model and voice detection mode in the control station.
- *(Optional)* Audio gain/attenuation must be configured for the radio port.

For information on the remote adapter settings, see RG-2000 *Installation and Configuration Guide*.

SmartPTT Configuration

To configure the control station connection over the analog interface, the following actions must be performed:

- SmartPTT license with RG-2000 permission must be installed. For details, see Installing License.
- Connection to the control station must be configured. For details, see Configuring Remote I/O Control Station Connection.
- Control station channels must be configured. For details, see Configuring Remote I/O Control Station Channels.
- Voice processing must be configured. For details, see Configuring Remote I/O Control Station Audio Settings.

7.3.2.1 Configuring Station Connection over Analog Interface

Follow the procedure to add a new or edit an existing connection to a remote I/O control station.

Prerequisites:

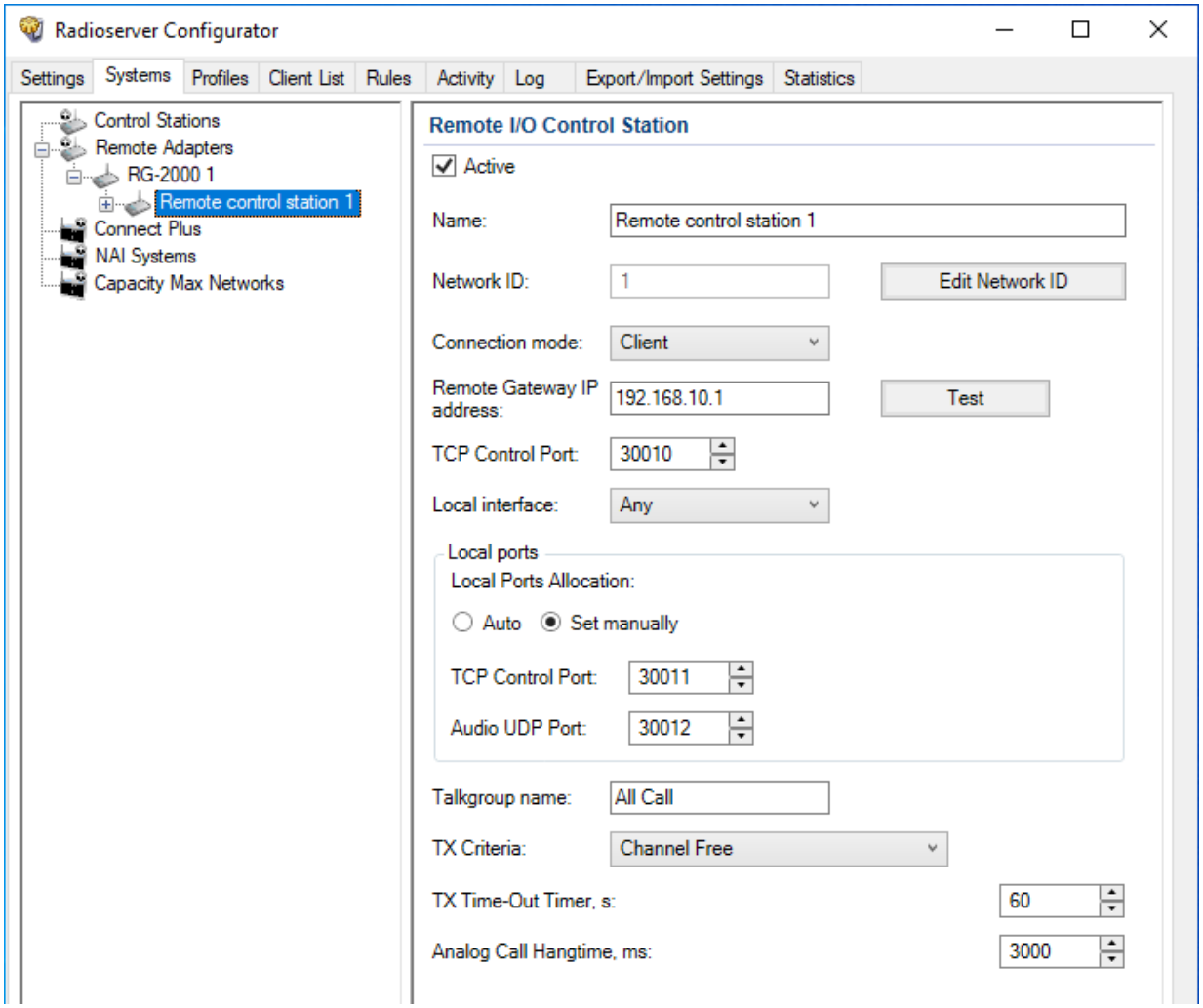
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure that SmartPTT license allows control station connection over analog interface. For details, see Viewing License Items.
- Determine whether SmartPTT Radioserver or RG-2000 will initiate the connection.

- *(Optional)* If RG-2000 is configured to act as a server, from the RG-2000 configuration file, obtain the IP address and port number configured for the desired control station.
- *(Optional)* From the control station codeplug, obtain the control station serial number.
- *(Optional)* Determine SmartPTT Radioserver host ports that will be used to receive XCMP and audio data from the control station.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, perform one of the following actions:

To add a remote I/O control station to a new remote adapter,	perform the following actions: 1. Right-click the ***Remote Adapters*** node, and then click ***Add → RG-2000***. 2. In the right pane, select the ***Active*** check box. 3. *(Optional)* In the ***Name*** field, type the remote adapter name. 4. In the left pane, right-click the ***RG-2000*** node, point to ***Add***, and then select ***Remote I/O Control Station***.
To add a remote I/O control station to an existing remote adapter,	perform the following actions: 1. Expand the ***Remote Adapters*** node. 2. Right-click the desired adapter name, point to ***Add***, and then select ***Remote I/O Control Station***.
To edit an existing remote I/O control station connection settings,	expand ***Remote Adapters → RG-2000***, and then click the desired control station.
To delete a remote I/O control station connection,	perform the following actions: 1. Expand ***Remote Adapters → RG-2000***. 2. Right-click the desired control station, and then select ***Delete***. 3. Proceed to the last step of the procedure.



3. In the right pane, select the ***Active*** check box to unlock control station settings.
4. In the ***Name*** field, type the control station name.
5. Leave the value in the ***Network ID*** field unchanged, or if necessary, edit the value after clicking the ***Edit Network ID*** button.
6. Configure the connection mode to the control station:

If RG-2000 is configured to accept SmartPTT connection (server),	perform the following actions: 1. From the ***Connection mode*** list, select *Client*. 2. In the ***Remote Gateway IP address*** field, type the remote adapter IP address to receive radioserver connections. 3. In the ***TCP Control Port*** field, enter the port number to receive radioserver connections.
If RG-2000 is configured to initiate SmartPTT connection (client),	perform the following actions: 1. From the ***Connection mode*** list, select the *Server* mode. 2. In the ***Local TCP Control Port*** field, enter the SmartPTT Radioserver port number to listen to incoming connections.

7. From the ***Local Interface*** list, select the desired option:

To use any radioserver IP address for the remote adapter connection,	select *Any*.
To use a fixed IP address for the remote adapter connection,	select the desired IP address.

8. *(Optional)* In the ***Local ports*** area, set SmartPTT Radioserver host ports to receive data:

To set local ports automatically,	select *Auto*.
To set specific local port values,	perform the following actions: 1. Select *Set manually*. 2. In the ***TCP Control Port*** field, enter the port number to use for commands and service messages exchange between the radioserver and the adapter. 3. In the ***Audio UDP Port*** field, enter the port number to use for voice receiving and transmission.

9. *(Optional)* In the ***Talkgroup name*** field, enter the control station talkgroup name.
10. From the ***TX Criteria*** list, select one of the following options:

If the control station is configured to transmit only when no other transmissions are detected over the radio channel,	select *Channel Free*.
If the control station is configured to completely ignore other transmission over the radio channel,	select *Always*.
If the control station is configured to notify other radios on interrupting their transmissions,	select *Tx Interrupt*.

Important
SmartPTT does not support color code criteria for outgoing transmissions.

11. In the ***TX Time-Out Timer, s*** field, enter the maximum duration of voice transmission on the channel.
12. In the ***Analog Call Hangtime, ms*** field, enter the maximum interval between transmissions over analog channels within one call.
13. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (***  ***)***.

Postrequisites:

- Configure control station channels. For details, see Configuring Remote I/O Control Station Channels.
- Configure audio settings. For details, see Configuring Remote I/O Control Station Audio Settings.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (***  ***)*** or ***Restart (***  ***)***.
- *(Optional)* In the firewall software on the computer, unlock the set ports. For details, see Radioserver Host.

7.3.2.2 Configuring Channels for Analog Interface

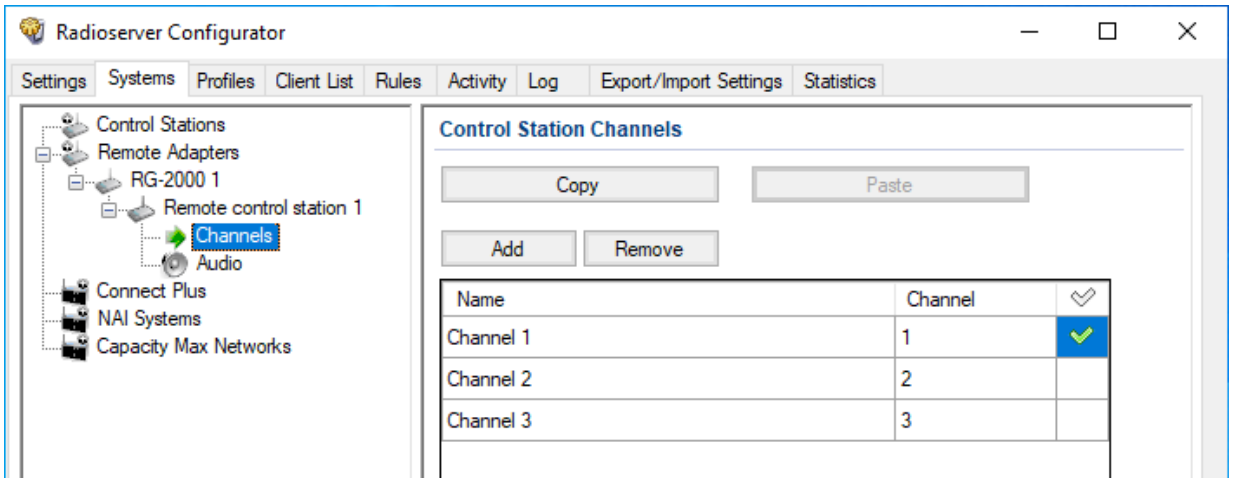
Follow the procedure to add new or edit existing channels of a remote I/O control station.

Prerequisites:

- Configure the control station connection. For details, see Configuring Remote I/O Control Station Connection.
- Configure the control station GPIO pins to switch channels.
- Configure all control station channels in the first zone.
- Determine the default control station channel.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***Remote Adapters*** → ***RG-2000*** → ***<Control Station Name>***, and then select ***Channels***.
   The list of channels appears in the right pane.



3. In the right pane, perform one of the following actions:

To add a new channel,	click ***Add***.
To edit an existing entry,	proceed to the next step of the procedure.
To remove an existing channel,	perform the following actions: 1. Click the desired entry. 2. Click ***Remove***. 3. Proceed to the last step of this procedure.

4. For the desired entry in the table, perform the following actions:
   a. In the ***Name*** column, double-click the current channel name, and then type a new name.
   b. In the ***Channel*** column, double-click the current channel ID, and then type the desired channel ID.
5. When all channels are added, in the Default Channel (✓) column, select the check box next to the channel that will be selected on the remote control station each time SmartPTT Radioserver is started or restarted.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

7.3.2.3 Configuring Audio Processing over Analog Interface

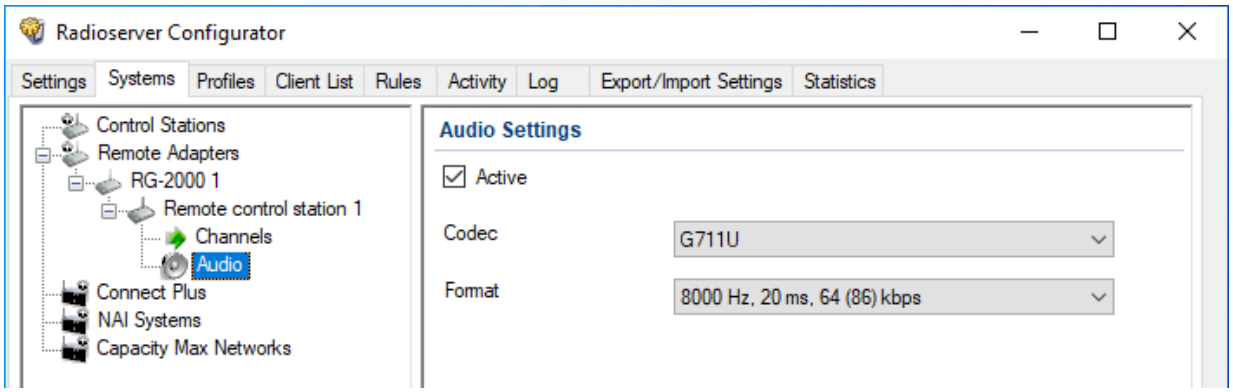
Follow the procedure to edit audio processing settings required to receive voice from an I/O control station and send dispatcher voice to it.

Prerequisites:

- Configure the control station connection. For details, see Configuring Remote I/O Control Station Connection.
- From the RG-2000 configuration file, obtain the voice transcoding algorithm.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, expand ***Remote Adapters*** → ***RG-2000*** → ***<Control Station Name>***, and then select ***Audio***.
   The audio settings appear in the right pane.



3. In the right pane, select the ***Active*** check box to unlock audio settings.
4. From the ***Codec*** list, select the desired voice transcoding algorithm.

Important
The algorithm must match the codec selected in the RG-2000 configuration.

5. *(Optional)* If you selected *Opus* from the ***Codec*** list, select the desired values of sampling frequency and frame length from the ***Format*** list.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

7.4 Analog Radio Systems

Analog systems are those that use frequency modulation and (optionally) various in-band audible signaling systems. For example, the following analog signaling can be used:

- MDC-1200.
- Five-tone signaling (for example, Select 5).

SmartPTT provides the limited support of analog radio systems and limited integration capabilities. Access to those systems is provided in one of the following ways:

MOTOTRBO Control Stations

MOTOTRBO control stations provide the partial voice and signaling transcoding and information provision to SmartPTT. For information on MOTOTRBO stations usage, see MOTOTRBO Control Stations.

Analog Interface

Analog interface provides the ability to receive voice transmissions, initiate voice transmissions, and switch station channels. The interface is provided by the RG-1000e remote adapter. For information on analog interfaces in SmartPTT, see Analog Interfaces.

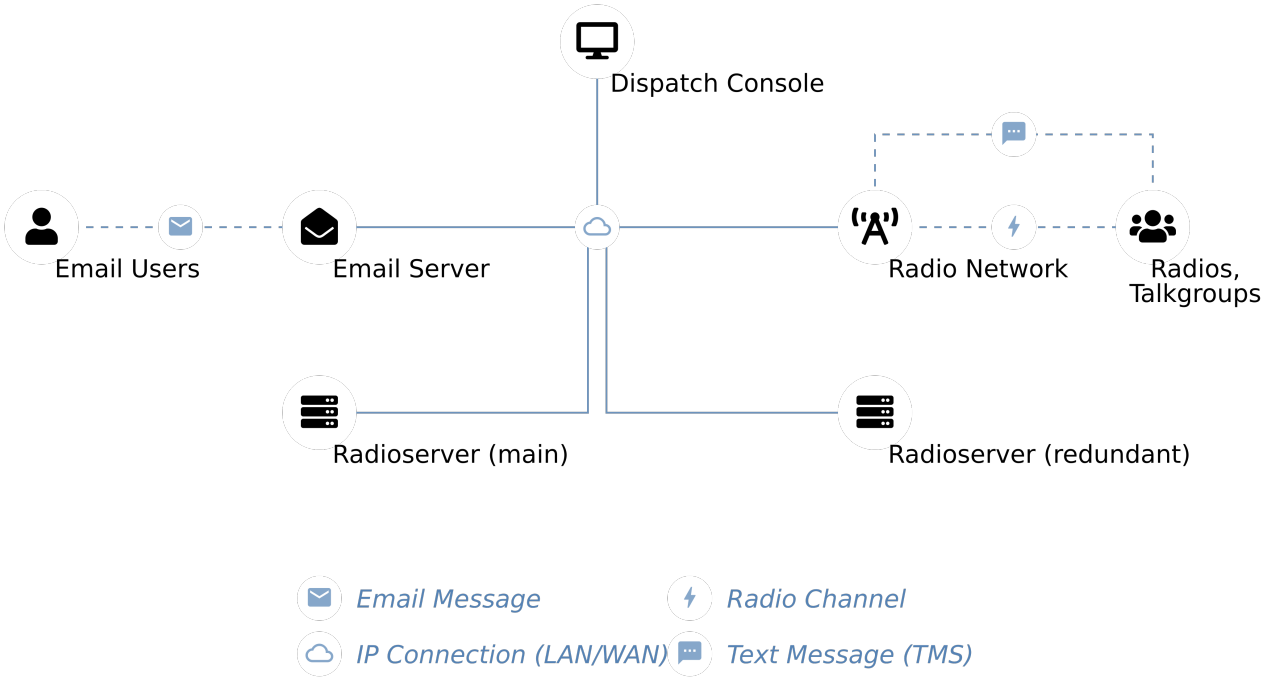
8 Data Exchange Systems

In addition to various VoIP communication systems, SmartPTT supports various data transferring systems. Those systems are as follows:

- Email Services. For details, see Email Services.
- Mobile Network Services. For details, see Mobile Phone Networks.
- Avigilon. For details, see Avigilon.

8.1 Email Services

SmartPTT supports email services connection to provide text messages delivery to email addresses for radios and dispatchers. It also provides the ability to send text messages from mailboxes.



SmartPTT implements the following features when connects email servers:

- Private text messages sent from email addresses.
- Text messages sent from radios to mailboxes.
- Automatic email notifications for pre-configured events:
  - Radio network events (including those related to the radio location). For details, see Rules.
  - Network device alarms. For details, see Configuring Alarm Notifications.
- Text messages monitoring in radio networks:
  - Forwarding text messages intended to be sent from radio network to mailbox.
  - Notifying on text messages in the radio network.
- Automatic deferred actions creation for private text messages which target is currently unavailable.

SmartPTT supports the following standard email communication protocols:

- Internet Message Access Protocol (IMAP4) that is used to receive email messages from email server.
- Post Office Protocol (POP3), an alternative email reception protocol.
- Simple Mail Transfer Protocol (SMTP) that is used to send email messages to email server.

8.1.1 Configuring Message Processing

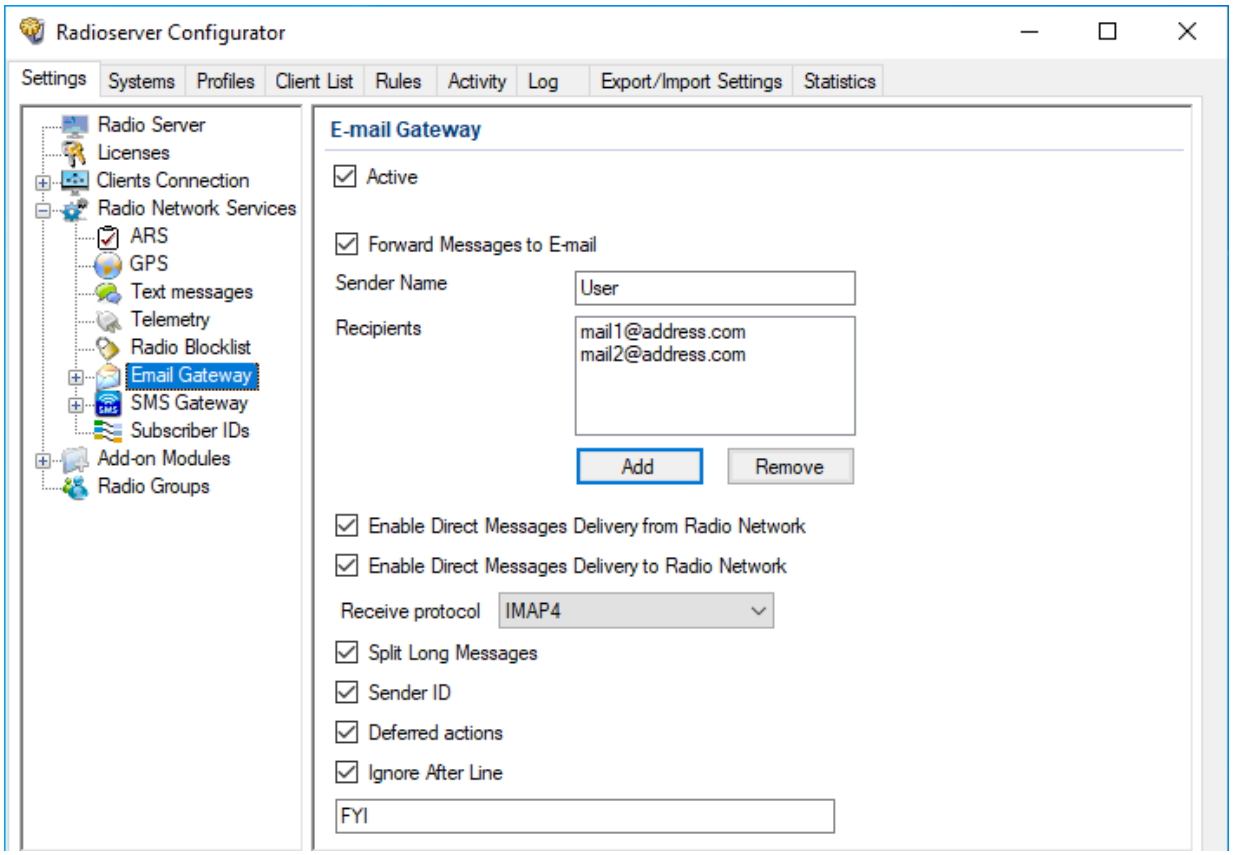
Follow the procedure to configure email message processing in SmartPTT Radioserver.

Prerequisites:

- Obtain email address that SmartPTT Radioserver uses to send and receive email messages.
- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Radio Network Services***, and then click ***Email Gateway***.
   The message processing settings appear in the right pane.



3. In the right pane, select the ***Active*** check box.
4. *(Optional)* To configure monitoring of text message exchange, perform the following actions::
   a. Select the ***Forward Messages to E-mail*** check box to allow forwarding text messages and notifications from radios to emails.

b. In the ***Sender Name*** field, type the SmartPTT Radioserver alias that will appear in forwarded email messages.

c. Configure the list of email addresses that will receive forwarded messages:

To add an email address,	perform the following actions: 1. Click ***Add***. The ***Add recipient*** window appears.  2. In the ***Recipient address*** field, type the email address. 3. Click ***Add***.
To delete an email address,	perform the following actions: 1. In the list of the ***Recipients*** area, click the email address that you want to delete. 2. Click ***Remove***.

5. Select the ***Enable Direct Message Delivery from Radio Network*** check box to enable delivering text messages from radios to email address.
6. Select the ***Enable Direct Message Delivery to Radio Network*** check box to enable delivering email messages to radios as TMS messages.
7. *(Optional)* To configure message processing parameters, perform the following actions::
   a. Select the ***Split Long Messages*** check box to allow splitting a long email message and delivering it as several TMS messages.
   b. Select the ***Sender ID*** check box to display a sender email addresses in the TMS messages.
   c. Select the ***Deferred actions*** check box to enable delayed message delivery to radios that are offline. If the email message is sent to the radio that is offline, SmartPTT Radioserver will store the message and send it only when the radio becomes online.
8. *(Optional)* To specify the email text that you want to hide in the TMS message, perform the following actions::
   a. Select the ***Ignore After Line*** check box.
   b. In the field below, type the text. The TMS will show only the text that is located before the text that you enter in this field.
9. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (***  ***)***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (***  ***)*** or ***Restart (***  ***)***.
- Connect SmartPTT Radioserver to the POP/IMAP service (incoming email service). For details, see Connecting to POP/IMAP Services.

- Connect SmartPTT Radioserver to the SMTP service (outgoing email service). For details, see Connecting to SMTP Services.

8.1.2 Connecting to POP/IMAP Services

Follow the procedure to connect SmartPTT Radioserver to the incoming email message server via POP3 or IMAP4.

Prerequisites:

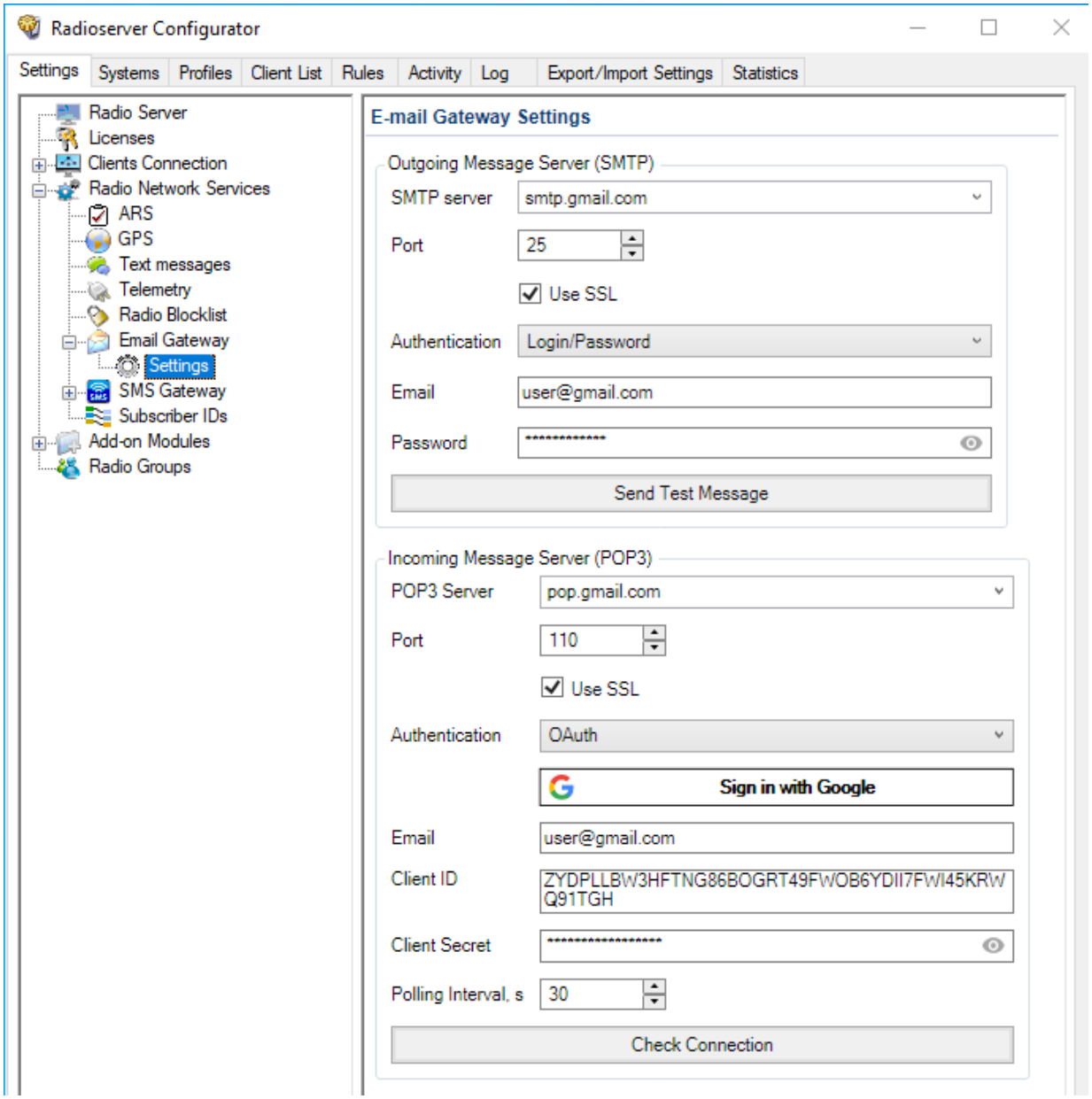
- Obtain the following information on the incoming message server:
  - Allowed protocol (POP or IMAP).
  - Domain name and port number for third-party applications.
  - TLS/SSL necessity.
  - SmartPTT Radioserver authentication credentials (email address and password) if you use the Login/Password authentication method.
- If you use the OAuth2 authentication, first register SmartPTT on the selected email server and obtain the Client ID and Client Secret. For details, see the online help:
  - Google: https://developers.google.com/gmail/imap/xoauth2-protocol
  - Microsoft: https://learn.microsoft.com/en-us/exchange/client-developer/legacy-protocols/how-to-authenticate-an-imap-pop-smtp-application-by-using-oauth
- If you want to use *OAuth* authentication with Office365, ensure that your web browser uses a direct Internet connection (do not use proxy). To check your connection type, go to the web browser settings.
- The Administrator of your Microsoft Outlook corporate email system must provide the user account access to POP, IMAP, and SMTP apps.
- In the firewall software, unlock the TCP port used for connection to the POP3 (or IMAP4) server. For details, see Radioserver Host.
- Activate email server support in SmartPTT. For details, see Configuring Message Processing.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Radio Network Services***, and then click ***Email Gateway***.
3. In the right pane, from the ***Receive protocol*** list, select the desired protocol:

If the incoming message service supports IMAP4,	select *IMAP4*.
If the incoming message service supports POP3,	select *POP3*.

4. In the left pane, expand the ***Email Gateway*** node, and then click ***Settings***.
   The service connection settings appear in the right pane.



5. In the ***Incoming Message Server (POP3)/(IMAP4)*** area, in the ***POP3 server/IMAP4 server*** field, enter the domain address of the incoming message server or select it from the list.
6. In the ***Port*** field, enter the port number that third-party applications use to connect to the server. The range of possible values is *1–65535*.
   For information on default port numbers, see Settings (Email).
7. *(Optional)* To enable secure connection (TLS/SSL) between SmartPTT Radioserver and the incoming message server, select the ***Enable SSL*** check box. Use the SSL protocol to ensure privacy and security of network communication.
8. In the ***Email*** field, type the email address through which SmartPTT Radioserver receives messages.
9. From the ***Authentication*** list, select the authentication mode that is configured on the POP3 (IMAP4) server:

If the server does not require authentication,	select *Anonymous*.

If the server requires authentication based on email address and its password,	perform the following actions: 1. Select *Login/Password*. 2. In the ***Password*** field, type the password for the SmartPTT Radioserver email address. To view the entered password, click the eye icon ( ). For security reasons, the password is not available for viewing in subsequent sessions.
To authenticate with an OAuth2 token,	perform the following actions: 1. Select *OAuth*. 2. In the ***Client ID*** field, enter the SmartPTT identifier that you obtain when registering SmartPTT on the email server. 3. In the ***Client Secret*** field, enter the SmartPTT secret that you obtain when registering SmartPTT on the email server. To view the entered secret, click the eye icon ( ). For security reasons, the secret is not available for viewing in subsequent sessions. 4. Click the authorization button. A web page with your email service appears in the web browser. 5. Select your account on the web page and return to SmartPTT Radioserver Configurator. If authorization is successful, a corresponding message displays in SmartPTT Radioserver Configurator.

10. In the ***Polling Delay (s)*** field, specify the period of service polling for checking new messages. The range of possible values is *30–3600* seconds. The default value is *30*.
11. *(Optional)* Click ***Check Connection*** to check connection to the incoming message server.
12. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

8.1.3 Connecting to SMTP Services

Follow the procedure to connect SmartPTT Radioserver to the outgoing message server.

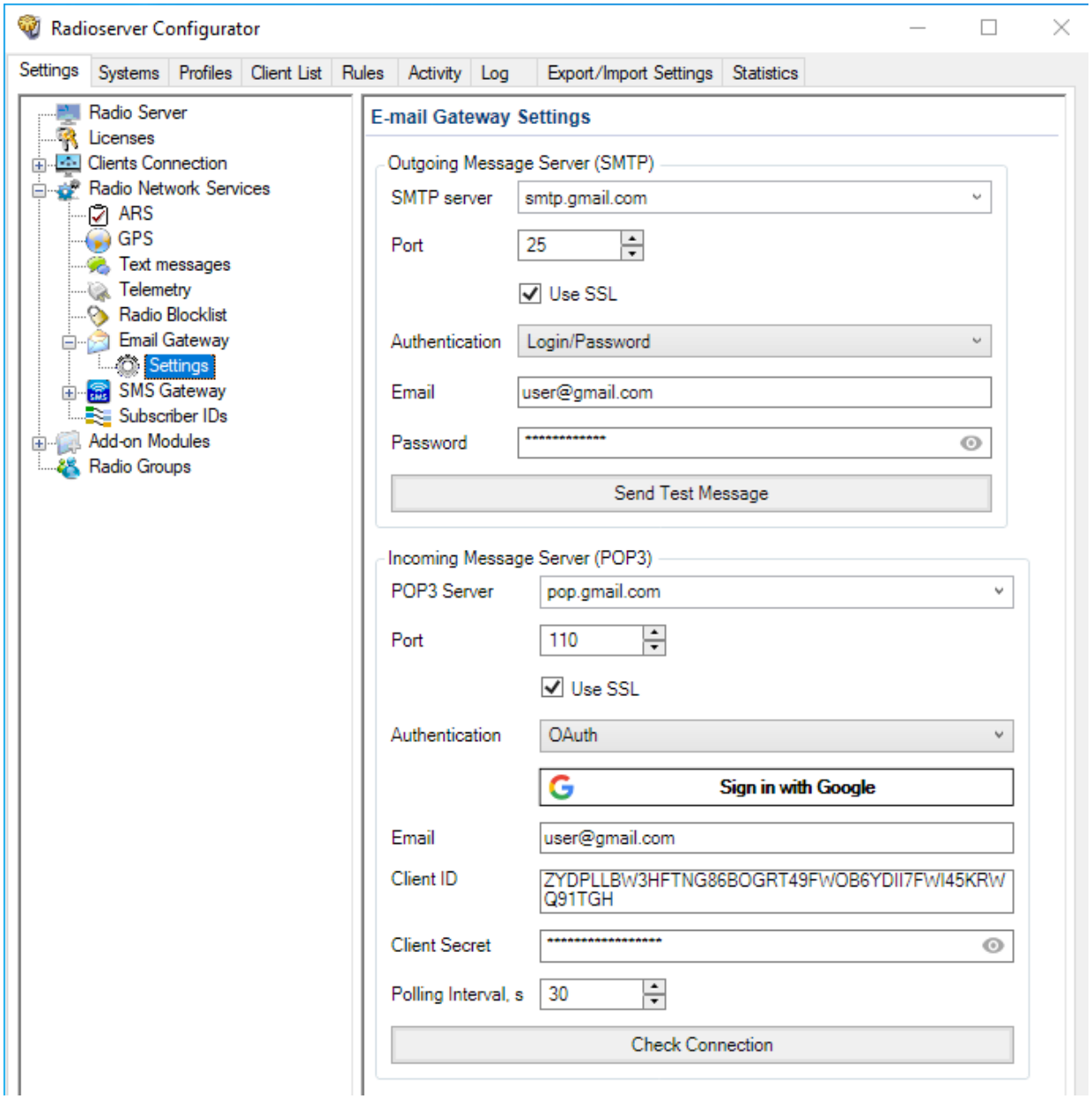
Prerequisites:

- Obtain the following information on the SMTP server:
  - Domain name and port number for third-party applications.
  - TLS/SSL necessity.
  - SmartPTT Radioserver authentication credentials (email address and password) if you use the Login/Password authentication method.

- If you use the OAuth2 authentication, first register SmartPTT on the selected email server and obtain the Client ID and Client Secret. For details, see the online help:
  - Google: https://developers.google.com/gmail/imap/xoauth2-protocol
  - Microsoft: https://learn.microsoft.com/en-us/exchange/client-developer/legacy-protocols/how-to-authenticate-an-imap-pop-smtp-application-by-using-oauth
- If you want to use *OAuth* authentication with Office365, ensure that your web browser uses a direct Internet connection (do not use proxy). To check your connection type, go to the web browser settings.
- The Administrator of your Microsoft Outlook corporate email system must provide the user account access to POP, IMAP, and SMTP apps.
- In the firewall software, unlock the TCP port used for connection to the server. For details, see Radioserver Host.
- Activate email server support. For details, see Configuring Message Processing.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Radio Network Services*** → ***Email Gateway***, and then click ***Settings***.
   The SMTP service connection settings appear in the right pane.



3. In the ***Outgoing Message Server (SMPT)*** area, in the ***SMTP server*** field, enter the SMTP service domain address or select it from the list.
4. In the ***Port*** field, enter the port number that third-party applications use to connect to the server. The range of possible values is *1–65535*.
   For information on default port numbers, see Settings (Email).
5. *(Optional)* To enable secure connection (TLS/SSL) between SmartPTT Radioserver and the server, select the ***Use SSL*** check box. Use the SSL protocol to ensure privacy and security of network communication.
6. In the ***Email*** field, type the email address through which SmartPTT Radioserver sends messages.
7. From the ***Authentication*** list, select the authentication mode that is configured on the server:

If the server does not require authentication,	select *Anonymous*.
If the server accepts domain and/or local credentials,	select *Windows*.
If the server requires authentication based on email address and its password,	perform the following actions: 1. Select *Login/Password*. 2. In the ***Password*** field, type the password for the SmartPTT Radioserver email address. To view the entered password, click the eye icon ( ). For security reasons, the password is not available for viewing in subsequent sessions.
To authenticate with an OAuth2 token,	perform the following actions: 1. Select *OAuth*. 2. In the ***Client ID*** field, enter the SmartPTT identifier that you obtain when registering SmartPTT on the email server. 3. In the ***Client Secret*** field, enter the SmartPTT secret that you obtain when registering SmartPTT on the email server. To view the entered secret, click the eye icon ( ). For security reasons, the secret is not available for viewing in subsequent sessions. 4. Click the authorization button. A web page with your email service appears in the web browser. 5. Select your account on the web page and return to SmartPTT Radioserver Configurator. If authorization is successful, a corresponding message displays in SmartPTT Radioserver Configurator.

8. *(Optional)* Click ***Send Test Message*** to check connection to the SMTP server.
9. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

8.1.4 Email Message Requirements

Email message can be sent to one or several radios as well as to one or several talkgroups. Email message that is sent from a mailbox to a radio network, must comply with the following requirements:

- Must be addressed to SmartPTT Radioserver mailbox.
- Must be a plain text message. No HTML or RTF formatting must be applied to it.

- Must use the UTF-8 encoding.
- Message text must have specific structure:
  - Message text must start with a colon (:).
  - Right after the colon, target ID must be entered.
  - Right after the ID, a space must be entered.
  - Right after the space, a character or message text must be entered.

Important
«New line» symbol must never be placed after or instead of the space.

  - If the email-message must be sent to several receivers, their identifiers must be divided by commas.

Target ID can be entered in different form (depends on the target type). To send a message to a radio, one of the following formation must be used:

- Decimal number (if radio ID ranges from 1 to 255).
- IP address in dot-decimal notation (applicable to any value). For details, see ID-to-IP Conversion.

To send a message to a talkgroup, IP address in dot-decimal notation (applicable to any value) must be used only. For details, see ID-to-IP Conversion.

Important
Messages addressed to the All Call ID will not be sent.

EXAMPLE

- The “call back to radio 1” message must be sent to the radio IDs = 200, 201, 202. Email text must be as follows
  :200,201,202 call back to radio 1
- The “call back to radio 1” message must be sent to the radio ID = 1001. Email text must be as follows
  :12.0.3.233 call back to radio 1
- The “call back to radio 1” message must be sent to the talkgroup ID = 1001. Email text must be as follows
  :225.0.3.233 call back to radio 1

8.1.5 TMS Requirements

Text message that is sent from radio and intended to be delivered to email, must be sent to the radio ID assigned to the radioserver.

Text message content must comply with the following requirements:

- Message must start with a colon (:).
- Target mailbox must be entered right after the colon. Input format is
  <user name>@<domain name>
- If a message must be sent to multiple email addresses, other mailboxes must be entered comma-separated. No spaces must be used between commas and mailboxes.
- After the last mailbox, a space must be entered.

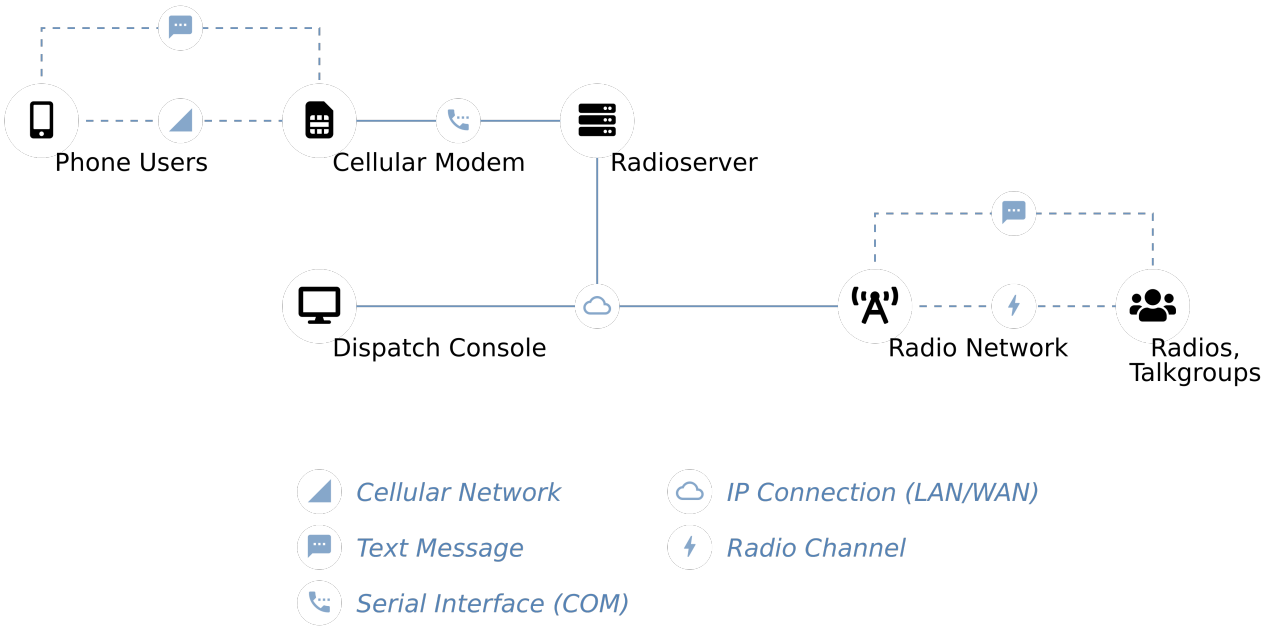
- Right after the space, a printed symbol or message text must be entered.

EXAMPLE

- The “available” text must be sent to a mailbox from a radio. TMS text must be as follows
  :user@mailbox.com available
- The “available” text must be sent to multiple mailboxes. TMS text must be as follows
  :user1@mailbox.com,user2@mailbox.com avaialbe

8.2 Mobile Phone Networks

SmartPTT supports the mobile phone network access for text-based communication and notifications.



Phone network access provides the following features in SmartPTT:

- Private and group text messages from the phone network to radio networks.
- Short text messages from radio networks to the phone network.
- Automatic notifications to the phone network for various events:
  - Specific events in the radio network (emergency alarms, specific location updates). For details, see Rules.
  - Radio network infrastructure alarms. For details, see Configuring Alarm Notifications.
- Private message delivery deference if the target radio is offline.

To access the phone network, SmartPTT uses phone network modems. The modems must be connected over the COM port of the radioserver host. For details, submit a request to the SmartPTT Technical Support Center.

8.2.1 Configuring SMS and TMS Processing

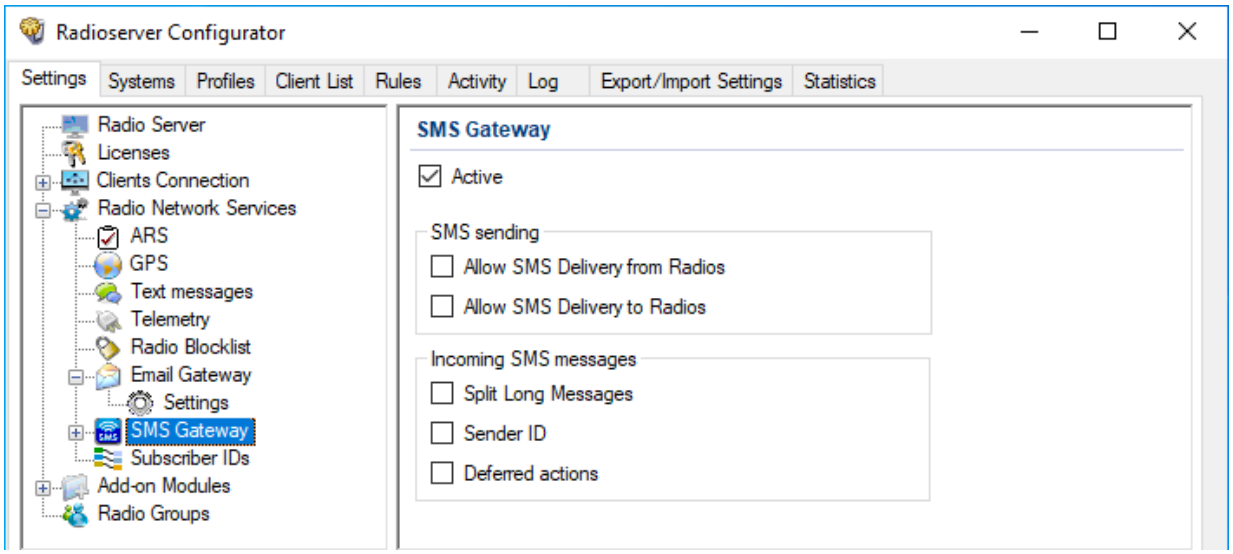
Follow the procedure to allow access to mobile networks and configure SMS exchange parameters.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure that the license for telephone interconnect service is installed in SmartPTT.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Radio Network Services***, and then click ***SMS Gateway***.
   The message processing settings appear in the right pane.



3. In the right pane, select the ***Active*** check box.
4. *(Optional)* Configure message exchange between the phone network and radio networks:
   a. Select the ***Allow SMS Delivery from Radios*** check box to allow sending TMS messages from a radio to a phone number as SMS messages.
   b. Select the ***Allow SMS Delivery to Radios*** check box to allow sending SMS messages from a phone number to a radio as TMS messages.
5. *(Optional)* Configure parameters of SMS message processing:
   a. Select the ***Split Long Messages*** check box to enable splitting a long SMS message and sending it as several TMS messages to the radio.
   b. Select the ***Sender ID*** check box to display the phone number of the SMS message sender in the TMS message.
   c. Select the ***Deferred Actions*** check box to enable delayed delivery of messages to offline radios. If you select the check box and send an SMS message to the offline radio, then the radioserver will store the message and send it when the radio becomes online.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

8.2.2 Connecting to Phone Modems

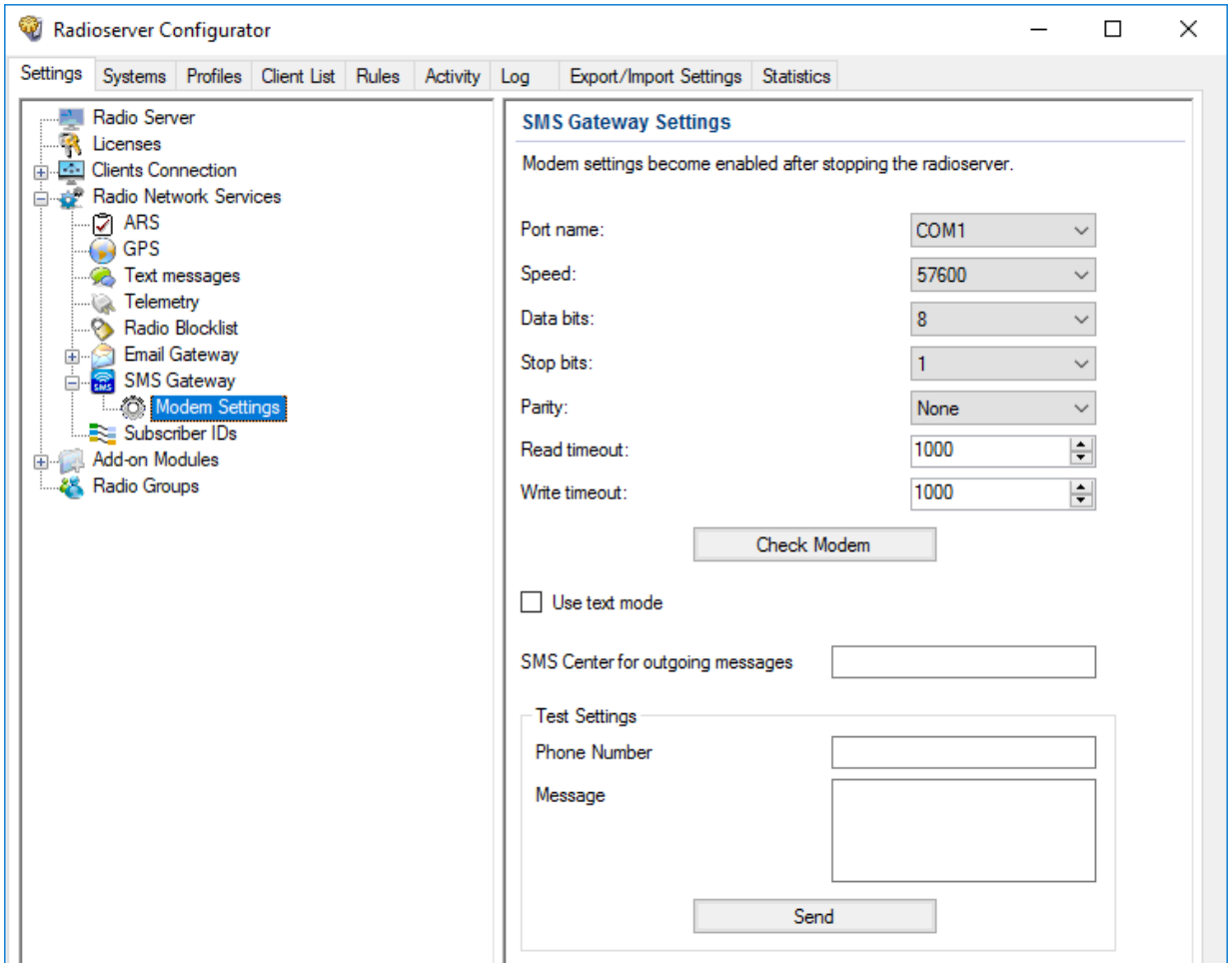
Follow the procedure to configure SmartPTT Radioserver connection to the phone modem that provides access to the mobile network.

Prerequisites:

- Determine the protocol parameters for SmartPTT Radioserver and modem communication over the COM port.
- Connect the modem to the SmartPTT Radioserver COM port.
- Stop SmartPTT Radioserver by clicking the ***Stop ( )*** button in the bottom part of SmartPTT Radioserver Configurator.
- In SmartPTT Radioserver Configurator, enable access to the cellular mobile network.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Radio Network Services*** → ***SMS Gateway***, and then click ***Modem Settings***.
   The modem settings appear in the right pane.



3. From the ***Port Name*** list, select the COM port name to which the modem is connected.
4. Configure the communication parameters for the port:

a. From the ***Speed*** list, select the bit rate for data exchange between SmartPTT Radioserver and the modem. The range of possible values is *110–921600* bits per second. The default value is *57600*.

b. From the ***Data bits*** list, select the number of bits encoded in each symbol of the protocol. The range of possible values is *5–8* bits. The default value is *8*.

c. From the ***Stop bits*** list, select the stop bits length. The following options are available: *1*, *1.5*, and *2*. The default value is *1*.

d. From the ***Parity*** list, select a bit added to a string of the binary code. The following options are available in the list: *None*, *Even*, and *Odd*. The default value is *None*.

e. In the ***Read timeout*** field, specify the timeout on waiting to read data. The range of possible values is *100–30000* milliseconds. The default value is *1000*.

f. In the ***Write timeout*** field, specify the timeout on waiting to write data. The range of possible values is *100–30000* milliseconds. The default value is *1000*.

5. *(Optional)* Click ***Check Modem*** to test SmartPTT Radioserver connection to the modem.

6. Configure the charset that will be used in SMS and TMS messages:

If you use only Latin characters and generally accepted punctuation marks,	select the ***Use text mode*** check box.
If you use languages other than English, or any Unicode characters,	clear the ***Use text mode*** check box.

7. In the ***SMS Center for outgoing messages*** field, type the service number of the mobile operator that SmartPTT Radioserver uses to forward text messages from radios to phone numbers. Enter the phone number in the international format with no spaces. Start with the "+" character.

NOTE
If the service number is specified in the SIM card installed in the modem, you can leave the field empty.

8. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (***  ***)***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (***  ***)*** or ***Restart (***  ***)***.
- Test connection to the modem by sending test messages. For details, see Testing Modem Operation.

8.2.2.1 Testing Modem Operation

Follow the procedure to test SmartPTT Radioserver connection to the modem by sending test messages.

Important
Sending SMS messages can be charged according to the terms of your phone network contract.

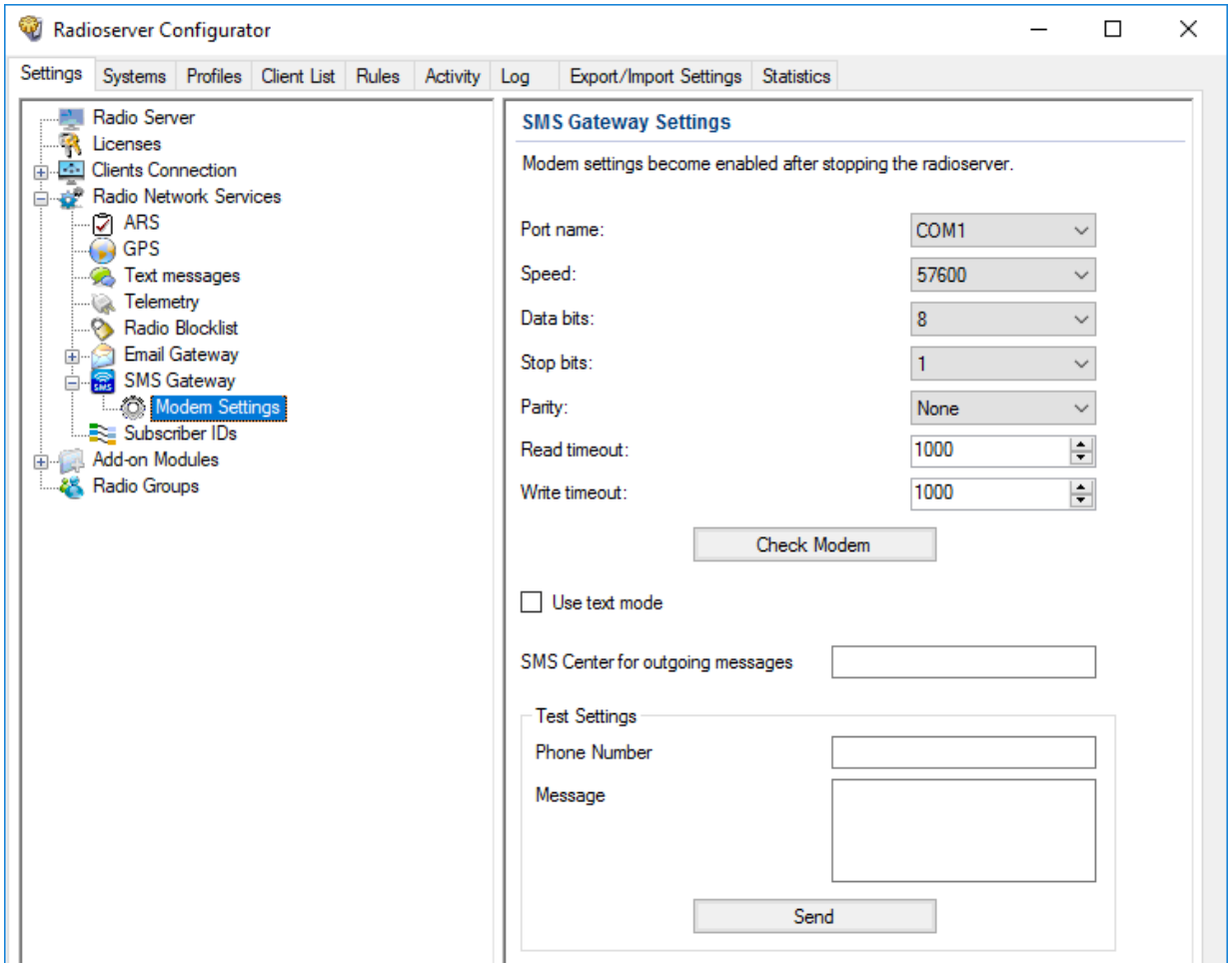
Prerequisites:

- Configure SmartPTT Radioserver connection to the modem. For details, see Connecting to Phone Modems.
- Ensure that the modem antenna is withing the phone network coverage zone.
- Decide a phone number to which you will send a test message.

- Stop SmartPTT Radioserver by clicking the ***Stop (*** ***)*** button at the bottom of the SmartPTT Radioserver Configurator window.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Radio Network Services*** → ***SMS Gateway***, and then click ***Modem Settings***.
   The connection settings appear in the right pane.



3. In the ***Test Settings*** area, in the ***Phone Number*** field, type the phone number to which you will send a test message. Enter the phone number in the international format with no spaces. Start with the "+" character.
4. In the ***Message*** field, type the text of the message.
5. Click ***Send*** and wait for the SMS message reception.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (*** ***)***.

8.2.3 SMS Messages for Radio Networks

If an SMS message must be delivered from the mobile network to a radio network, the message must comply with the following requirements:

- Message must be sent to the number that is programmed in the SIM card that is installed in the phone modem.
- Message text must be specific.

Message text must comply with the following requirements:

- It must start with the colon character (:).
- After the colon, a target must be entered. No spaces must be between the target and a colon.
- After the target, a space must be entered.
- After the space, any printed character or message text must be entered.

Important
You must ***not*** start a new line after or instead of the space character.

Depending on the target type, it must be specified differently. To send a message to a radio, one of the following formats must be used:

- Decimal number (if the radio ID is in the range of 1 to 255).
- IP address (for any radio ID values). For details, see ID-to-IP Conversion.

To send a message to a talkgroup, the talkgroup IP address must be used as a target. For details, see ID-to-IP Conversion.

Important
Text messages cannot be sent to All Call IDs.

EXAMPLE

- Message text is “call to radio 1” and the target radio ID is 200. SMS message text must be a follows:
  :200 call to radio 1
- Message text is “call to radio 1” and the target radio ID is 1001. SMS message text must be as follows:
  :12.0.3.233 call to radio 1
- Message text is “call to radio 1” and the target talkgroup ID is 1001. SMS message text must be as follows:
  :225.0.3.233 call to radio 1

8.2.4 TMS Messages for Phone Networks

If a text message must be delivered from a radio network to the phone network over the radioserver, it must be sent to the radio ID assigned to the radioserver.

Message text must comply with the following requirements:

- Message text must start with the colon character that follows with the ampersand characters (:&).
- Right after the ampersand, a phone number must be entered in the following format:
  - Only digits must be left. Other characters must be removed (includes, spaces, brackets, hyphens etc.).
  - Phone number prefix (+) must not be used.
- Right after the number, a space must be entered.
- Right after the space, any printed character or message text must be entered.

EXAMPLE

- The “available” message must be delivered to the phone number +1 909 909 9009. Message text must be as follows: :&19099099009 available

8.3 Avigilon

One more data exchange system (video) supported by SmartPTT is Avigilon. This video monitoring system helps dispatchers to monitor online what is happening at one or another object, for example, if alarm is received from a radio, thus allowing to know the situation at the object.

To integrate cameras with SmartPTT Dispatcher, Avigilon Control Center Server 7 Software must be installed. For details, see the Avigilon Control Center 7 Software web page on the Avigilon website.

To integrate with the Avigilon system, the corresponding license must be installed. For details, see Installing License.

To watch live video from cameras, perform the following:

- Install Avigilon Control Center Server 7 software.
- Add cameras to the Avigilon system.
- Instal the corresponding license.
- Connect SmartPTT to the Avigilon system. For details, see Configuring Avigilon Connection.
- Add cameras on a map in SmartPTT Dispatcher.
  For information on working with cameras, see the "Adding Cameras" section of *SmartPTT Dispatcher Guide*.

NOTE
Video recording in the SmartPTT system is not available.

8.3.1 Configuring Avigilon Connection

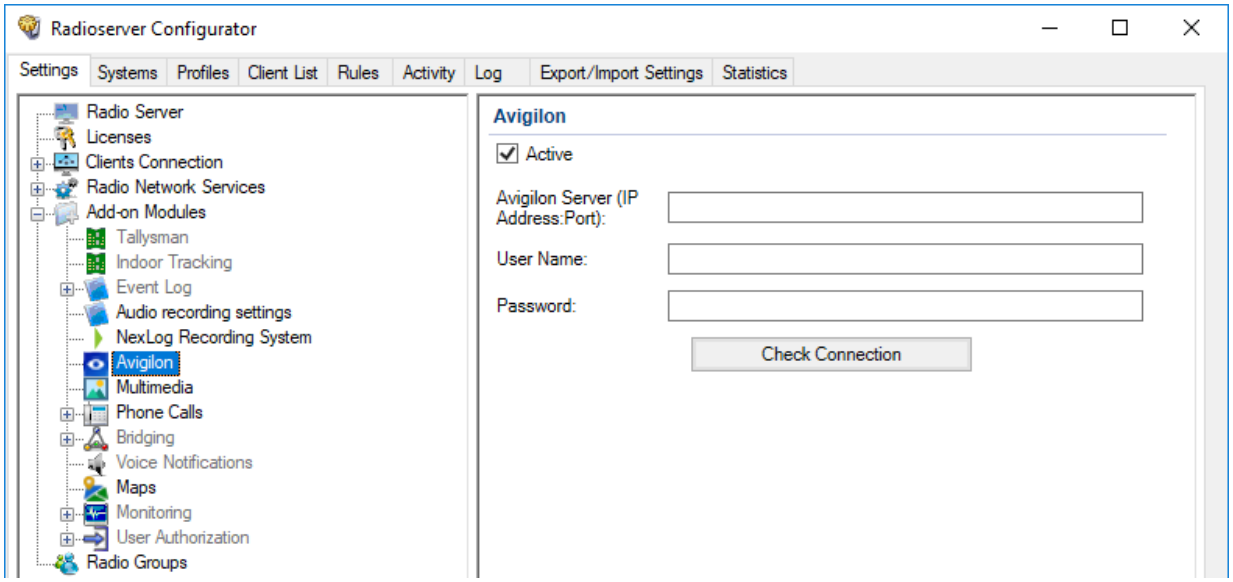
Follow the procedure to configure SmartPTT connection to the Avigilon system.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure the SmartPTT license allows connection to Avigilon. For details, see Viewing License Items.
- Obtain the user name and password that will be used for authentication in the Avigilon system.
- Obtain the Avigilon IP address and port to connect SmartPTT.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane of the tab, expand the ***Add-on Modules*** node, and then click ***Avigilon***.
   The system connection settings appear in the right pane of the tab.



3. In the right pane of the tab, select the ***Active*** check box.
4. In the ***Avigilon Server (IP Address:Port)*** field, type the IP address of the Avigilon server to connect SmartPTT to it.
5. In the ***User Name*** field, type the user name that SmartPTT will use for authentication on the Avigilon server.
6. In the ***Password*** field, type the password set for the specified user on the Avigilon server. To view the entered password, click the eye icon ( ). For security reasons, the password will not be available for viewing in subsequent sessions.
7. Press the ***Check Connection*** button to check the Avigilon server connection status.
8. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- In the firewall software on the radioserver computer, unlock the specified port. For details, see Radioserver Host.

8.4 ID-to-IP Conversion

In some cases, radio IDs and talkgroup IDs must be represented as IP addresses. Examples of such cases is as follows:

- SMS messages sent from a mobile phone to the radio network over SmartPTT.
- During the SmartPTT Radioserver activity events analysis.

In SmartPTT, ID representation as an IP address implies the dot-decimal notation. It means that each ID is represented as four decimal numbers (octets) separated by dots. Each decimal number ranges from 0 to 255. Example of the IP address is 255.255.255.0.

Radio IDs

To convert a radio ID to IP address (using dot-decimal notation), the following actions must be performed:

1. Radio ID must be converted from a decimal number to a hexadecimal number.

EXAMPLE

Radio ID is equal to *1001*. In hexadecimal form, it is equal to *3E9*.

2. The converted ID must be represented as a six-position hexadecimal number.

EXAMPLE

The ID is equal to 3E9. In a six-position form, it is equal to *0003E9*.

3. The six-position ID must be split into three two-position hexadecimal numbers.

EXAMPLE

The six-position hexadecimal number *0003E9* can be split into the following two-position numbers:

- 00
- 03
- E9

4. Each two-position hexadecimal number must be converted to a decimal number.

EXAMPLE

- Hexadecimal bumber 00 is equal to decimal number 0.
- Hexadecimal number 03 is equal to decimal number 3.
- Hexadecimal number E9 is equal to decimal number 233.

Each decimal number is related to the second, third, and fourth octet of the IP address, respectively. The first octet is equal to the CAI of the corresponding radio network.

EXAMPLE

Radio ID is equal to *1001*. Radio is used in a radio network with CAI equal to *12*.

Radio IP address is equal to *12.0.3.233*.

Talkgroup ID

Conversion process for talkgroup IDs is almost the same as for radio IDs. The difference is that Group CAI must be used instead of CAI.

EXAMPLE

Talkgroup ID is equal to *1001*. Group CAI is equal to *225*.

Talkgroup IP address is equal to *225.0.3.233*.

9 Network Monitoring

In SmartPTT, network monitoring is a process of the information gathering about wireline network devices performance. Information gathering is performed by the radioserver over the Simple Network Management Protocol (SNMP). Data are saved to the dedicated database.

Important
Network monitoring is unavailable for Capacity Max.

When the monitoring is active, dispatch console receives the following capabilities:

- Network topology visualization.
- Network devices control.
- Information on device alarms.
- Monitoring reports generation.

SmartPTT gathers information for the following devices:

- Radioserver host.
- Repeaters, MNIS services, and other application peers.
- Routers and switches.
- Uninterruptible power supplies (UPS).
- Supermicro server platforms.
- Generic network devices (for example, dispatch console hosts).

All the devices can be grouped into Locations, a logical elements that can be associated with a site or a dispatch center.

NOTE
In Connect Plus, the Location element is created automatically per each XRC controller and, therefore, is associated with a system site.

9.1 External SNMP Services

SmartPTT provides integration with a third-party SNMP services. Radioserver connects to those services as a client application and provides information about all of the monitored devices.

To support SmartPTT connection, SNMP services must have specific MIB files uploaded to it. MIB files are the management information base files that define a device parameters and its attributes. If you need more information on MIB files utilization for your SNMP, submit a request to SmartPTT Technical Support Center.

MIB files that define radioserver as a network device, are available in the .\MIB directory of the radioserver installation directory.

9.1.1 Configuring SNMP Server Connection

Follow the procedure to configure SNMP server connection.

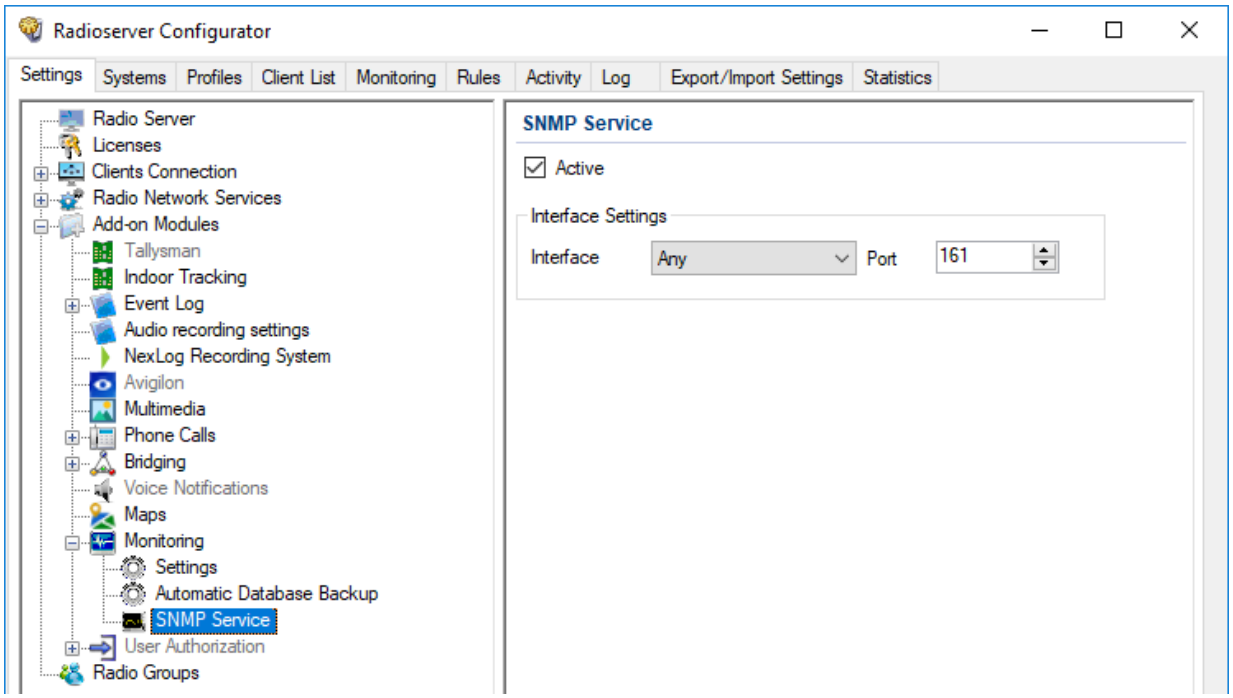
Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *Database Administrators* group. For details, see Loging in to Radioserver Configurator.

- Ensure that SmartPTT license allows SNMP connection. For details, see Viewing License Items.
- Configure SmartPTT connection to the monitoring database. For details, see Configuring Monitoring Database Connection.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Add-on Modules*** → ***Monitoring***, and then click ***SNMP Service***.
   The SNMP service settings appear in the right pane.



3. Select the ***Active*** check box.
4. If necessary, change ***Interface Settings***:
   a. From the ***Interface*** list, select the SmartPTT Radioserver IP address to which the SNMP server will connect.

To use any of the configured SmartPTT Radioserver host IP addresses,	select *Any*.
To use a specific IP address,	select the desired IP address.

   b. In the ***Port*** field, enter the port number for receiving requests from the SNMP server.

Important
Do not change ***Interface Settings*** without need.

5. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- In the firewall software on the radioserver computer, unlock the specified port. For details, see Radioserver Host.
- Configure external SNMP monitoring for SmartPTT Radioserver. For details, see Configuring SNMP for Radioserver.

- Configure external SNMP monitoring for radio network devices.
- Install the SNMP server and configure it, specifying the SmartPTT Radioserver IP address.
- In the SNMP server, install the MIB files located in the following folder: <SmartPTT installation path>\Server\MIB.
- Configure the desired devices in the SNMP server.

9.2 Configuring SNMP for Radioserver

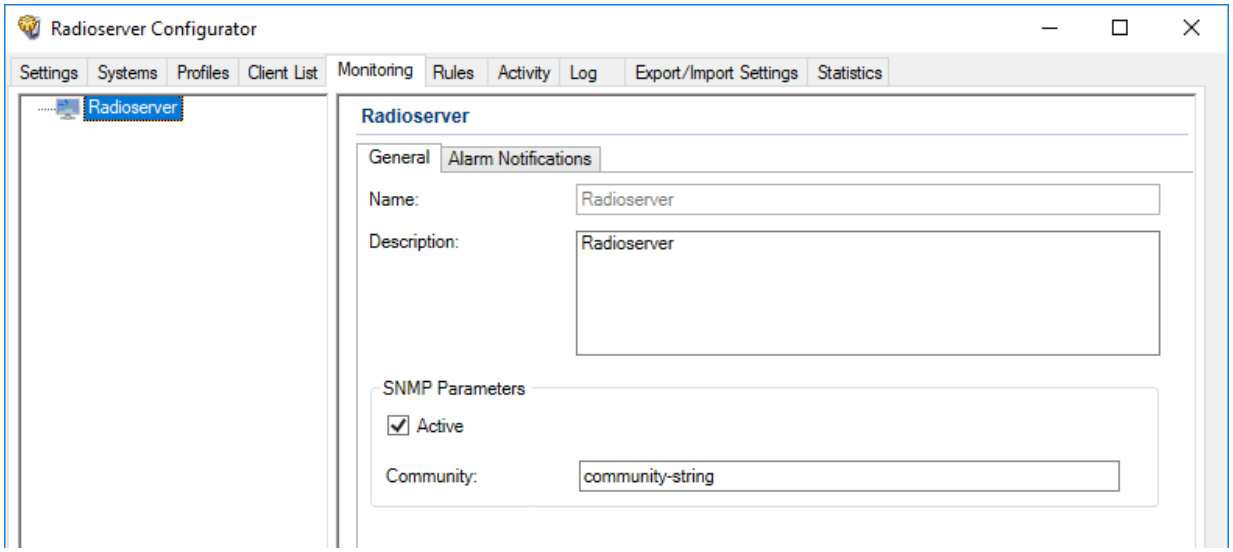
Follow the procedure to configure the SNMP monitoring of the SmartPTT Radioserver host as a separate network device that is not part of the radio network.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Configure SmartPTT connection to the monitoring database. For details, see Configuring Monitoring Database Connection.
- Configure SmartPTT interface for an external SNMP server. For details, see Configuring SNMP Server Connection.
- Obtain the community string for the SNMP server.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Monitoring*** tab.
2. In the left pane of the ***Monitoring*** tab, click ***<Radioserver name>***.



3. In the right pane of the ***Monitoring*** tab, open the ***General*** tab.
4. *(Optional)* In the tab, in the ***Description*** field, type the information about a radioserver.
5. In the ***SNMP Parameters*** area, select the ***Active*** check box.
6. In the ***Community*** field, type the community string of the SNMP server.
7. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Configure alarm notifications. For details, see Configuring Alarm Notifications.
- In the SNMP server settings, assign the read-only attribute to the community entry.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (▷)*** or ***Restart (▷)***.

9.3 Configuring Radioserver Monitoring in the Network

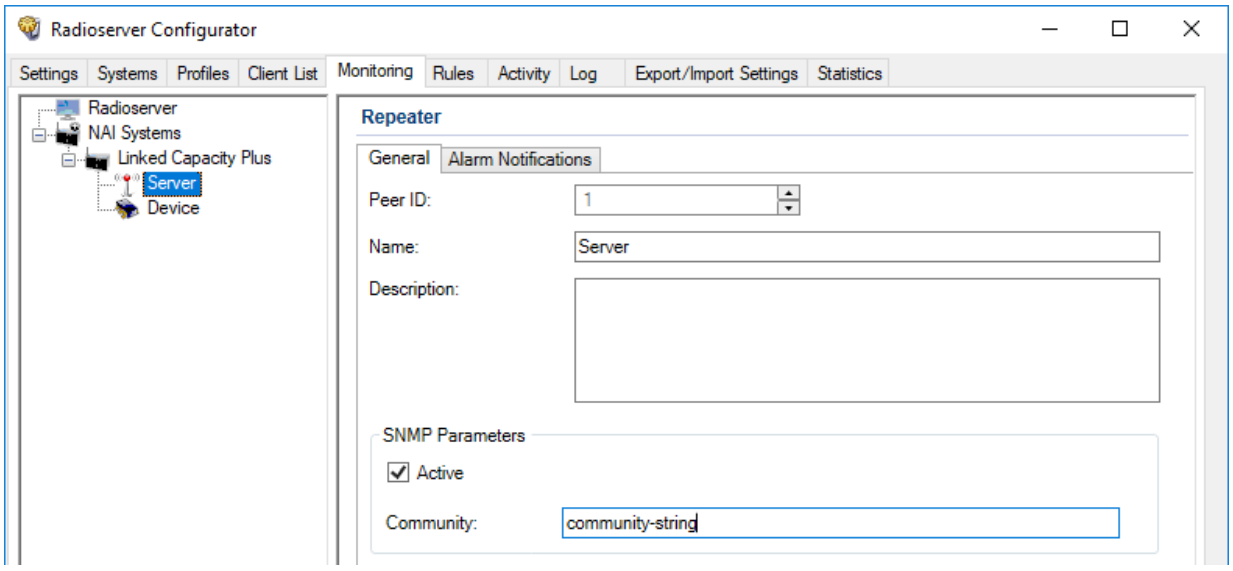
Follow the procedure to configure the radioserver monitoring as a virtual network device.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Connect a radioserver to the desired radio systems. For details, see MOTOTRBO Radio Systems.
- Configure SmartPTT connection to the monitoring database. For details, see Configuring Monitoring Database Connection.
- Configure SmartPTT interface for an external SNMP server. For details, see Configuring SNMP Server Connection.
- Obtain the community string for the SNMP server.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Monitoring*** tab.
2. In the left pane of the ***Monitoring*** tab, expand <***network type***> → <***network name***>. If the element corresponding to a radioserver misses, expand the <***location name***> node, and then click the node that corresponds to the radioserver element.



3. In the right pane of the ***Monitoring*** tab, in the ***Name*** field, type the name of a radioserver.
4. *(Optional)* In the ***Description*** field, type the short information about a radioserver.
5. In the ***SNMP Parameters*** area, select the ***Active*** check box.
6. In the ***Community*** field, type the community entry used for authentication on the SNMP server.
7. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (💾)***.

Postrequisites:

- Configure alarm notifications. For details, see Configuring Alarm Notifications.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (▷)*** or ***Restart (▷)***.

9.4 Adding and Configuring Peers

Follow the procedure to add or configure monitoring settings of a repeater, MNIS service, or other application peer.

Prerequisites:

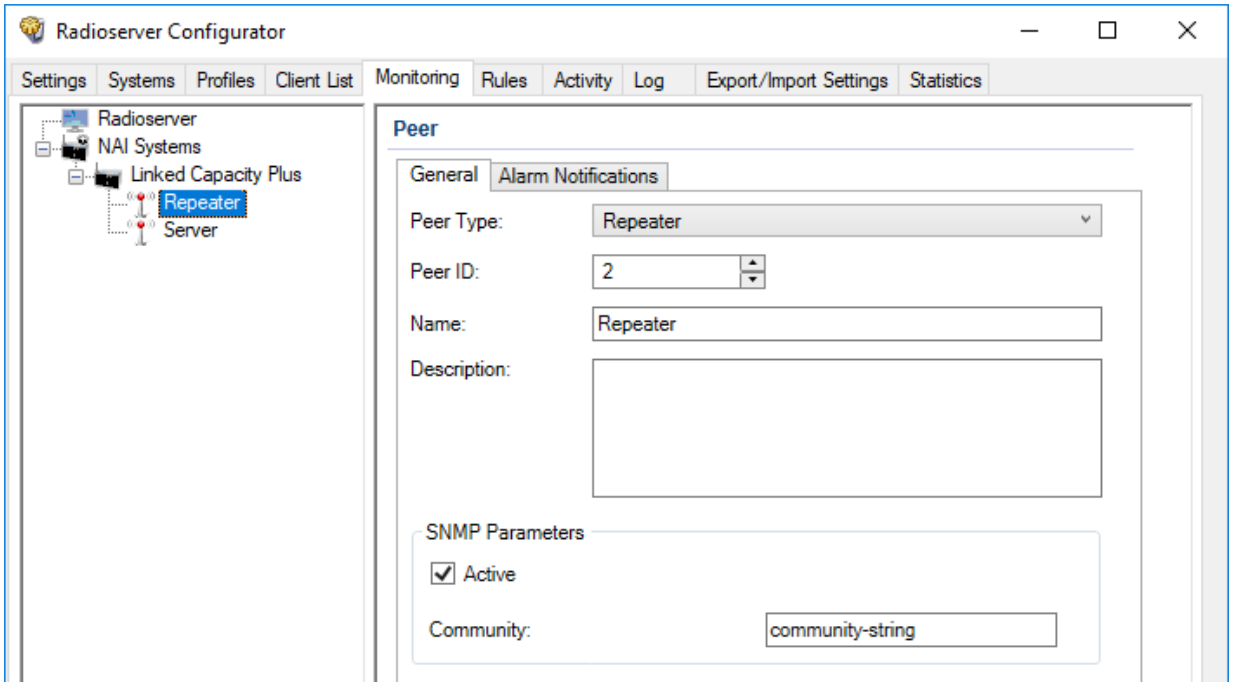
- Connect a radioserver to the desired radio systems. For details, see MOTOTRBO Radio Systems.
- Configure SmartPTT connection to the monitoring database. For details, see Configuring Monitoring Database Connection.
- Configure SmartPTT interface for an external SNMP server. For details, see Configuring SNMP Server Connection.
- Obtain the community string for the SNMP server.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Monitoring*** tab.
2. In the left pane of the ***Monitoring*** tab, expand <***network type***> → <***network name***>.
3. Perform one of the following actions:

To add a new peer,	right-click the network name, and then, from the actions menu, select ***Add Peer***.
To edit peer parameters,	click the desired peer. If the desired element misses, expand the <***location name***> node, and then click the element corresponding to a peer.

4. In the right pane of the ***Monitoring*** tab, open the ***General*** tab.



5. From the ***Peer Type*** list, select the desired peer type:

To configure monitoring of a repeater,	select *Repeater*.
To configure monitoring of a MNIS software gateway,	select *MNIS*.
To configure monitoring of an application peer other than MNIS,	select *Application Peer*.

6. In the ***Peer ID*** field, enter a unique identifier of a peer.
7. In the ***Name*** field, type the desired peer name.
8. *(Optional)* In the ***Description*** field, type the peer description that appears on a topology diagram in SmartPTT Dispatcher.
9. In the ***SNMP Parameters*** area, select the ***Active*** check box.
10. In the ***Community*** field, type the community entry of the SNMP server.
11. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Configure alarm notifications. For details, see Configuring Alarm Notifications.
- Update the topology. For details, see Updating Topology.
- To delete a peer, in the left pane of the ***Monitoring*** tab, right-click the peer name and select ***Remove Peer***.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

9.5 Adding and Configuring Devices

Follow the procedure to add and configure the device monitoring settings.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Connect to radio networks:
  - To access the MOTOTRBO radio systems, see MOTOTRBO Radio Systems.
  - To access the P25 radio systems, see P25 Radio Systems.
- Configure SmartPTT connection to the monitoring database. For details, see Configuring Monitoring Database Connection.
- Configure SmartPTT interface for an external SNMP server. For details, see Configuring SNMP Server Connection.
- Obtain the community string for the SNMP server.

Procedure:

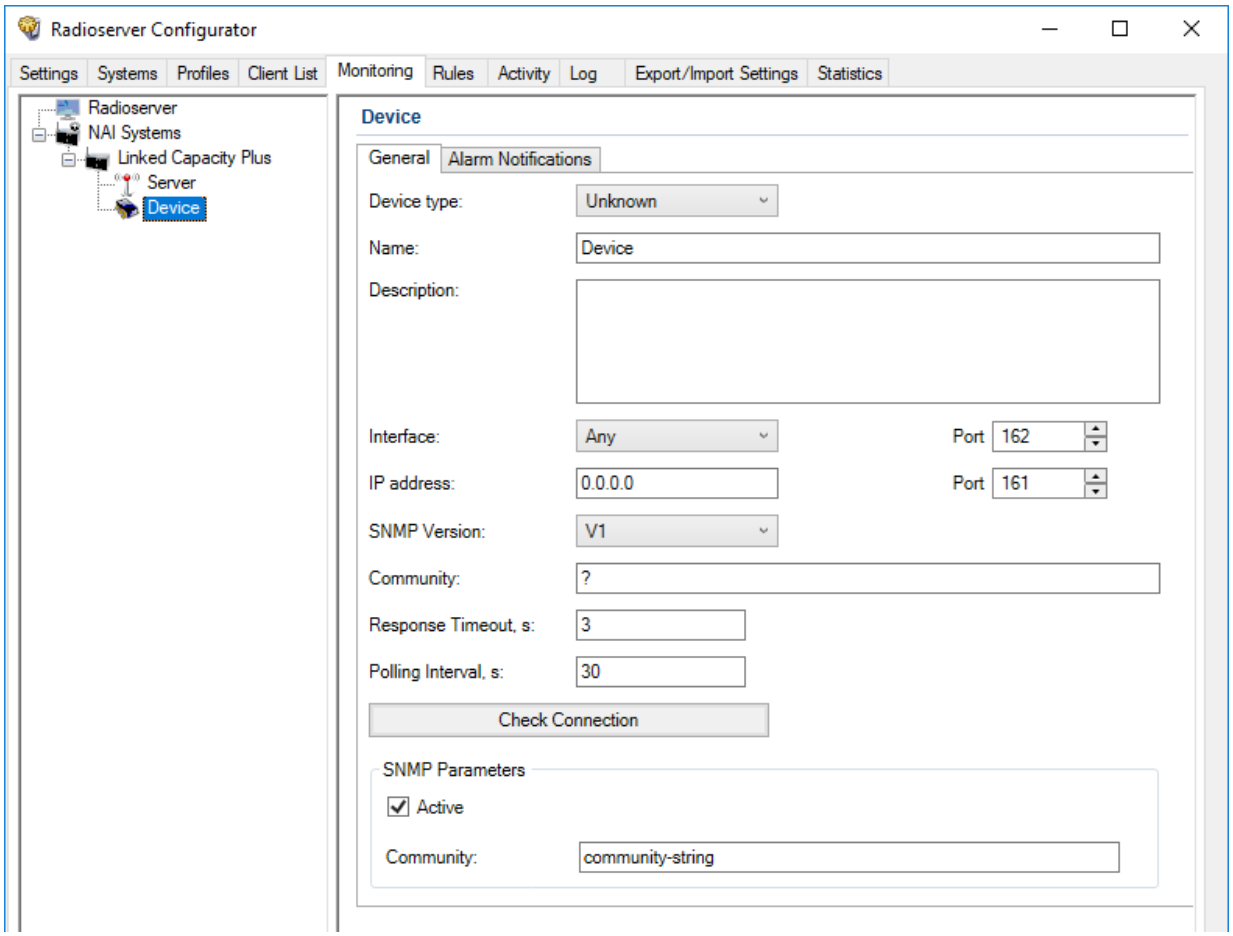
1. In SmartPTT Radioserver Configurator, open the ***Monitoring*** tab.
2. In the left pane of the ***Monitoring*** tab, perform one of the following actions:

To access devices operating with control stations,	expand ***Control Stations***.

To access devices of repeater systems,	expand ***<network type>*** → ***<network name>***

3. Perform one of the following actions:

To add a new device,	right-click the network name or the ***Control Stations*** node, and then from the actions menu select ***Add Device***.
To edit device parameters,	click the desired device. If the desired element misses, expand the ***<location name>*** node, and then click the element corresponding to a device.



4. In the right pane of the tab, open the ***General*** tab.
5. In the ***General*** tab, from the ***Type*** list, select the desired device type.
6. In the ***Name*** field, type the device name.
7. *(Optional)* In the ***Description*** field, type the device description that appears on a topology diagram in SmartPTT Dispatcher.
8. Configure connection to a device:
   a. From the ***Interface*** list, select the IP address of the SmartPTT Radioserver host for interacting with a device.
   b. In the ***Port*** field, enter the port number that a server will use for interacting with a device.
   c. In the ***IP-address*** field, type the IP address of a device.
   d. In the ***Port*** field, enter the device port number.

9. From the ***SNMP Version*** list, select the desired version of the SNMP protocol.
10. In the ***Community*** field, type the community name that is used for connection to a device over the SNMP protocol in the local network.
11. In the ***Response Timeout, s*** field, type the amount of time in seconds during which a radioserver expects a response from a device.
12. In the ***Polling Interval, s*** field, type the amount of time in seconds after which a radioserver sends a request to a device.
13. Click the ***Check Connection*** button to check the status of the device connection.
    A new window with information on the connection status appears.
14. In the ***SNMP Parameters*** area, select the ***Active*** check box.
15. In the ***Community*** field, type the community entry used for authentication on the SNMP server.
16. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (*** ***)***.

Postrequisites:

- Configure alarm notifications. For details, see Configuring Alarm Notifications.
- Update the topology. For details, see Updating Topology.
- In the firewall software on the radioserver computer, unlock the set ports. For details, see Radioserver Host.
- To delete a device, in the left pane of the tab, right-click the device name and select ***Remove Device***.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (*** ***)*** or ***Restart (*** ***)***.

9.6 Adding and Configuring Locations

Follow the procedure to add or configure location settings in the network configuration.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Connect to radio networks:
  - To access the MOTOTRBO radio systems, see MOTOTRBO Radio Systems.
  - To access the P25 radio systems, see P25 Radio Systems.
- Configure SmartPTT connection to the monitoring database. For details, see Configuring Monitoring Database Connection.
- Add the repeaters and devices to the network configuration:
  - To add a repeater, see Adding and Configuring Peers.
  - To add a device, see Adding and Configuring Devices.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Monitoring*** tab.
2. On the ***Monitoring*** tab, perform one of the following actions:

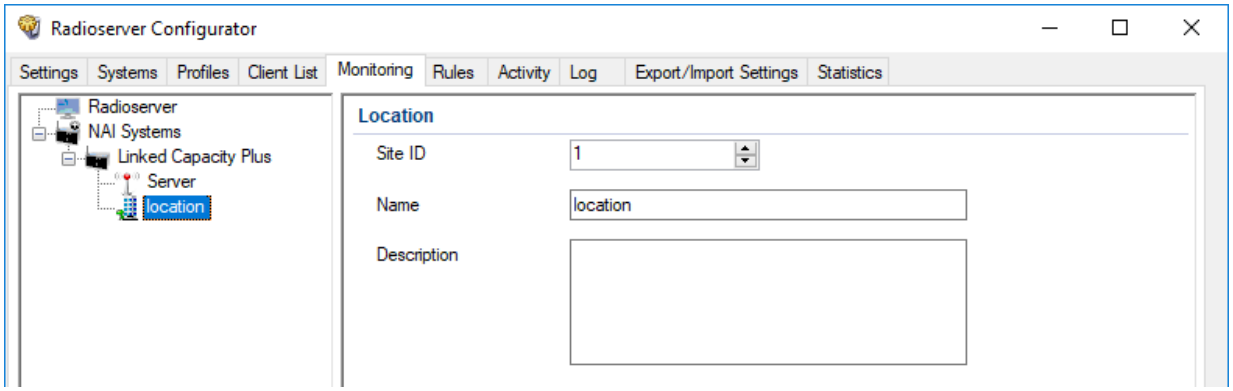
To access locations connected to control stations,	expand ***Control Stations***.

To access locations of repeater systems,	expand ***<network type>*** → ***<network name>***

3. Perform one of the following actions:

To add a new location,	right-click the network name, and then from the actions menu select ***Add Location***.
To edit location parameters,	click the desired location.

Important
Location adding is not available for Connect Plus systems.



4. In the right part of the tab, in the field ***Site ID*** (if available), type the site number.
5. In the right pane of the tab, in the ***Name*** field (if available), type the desired location name.
6. *(Optional)* In the ***Description*** field, type the location description.
7. Specify elements that should be grouped in this location:

To add an element to the location,	drag the desired element to the location.
To move an element from one location to another,	perform the following actions: 1. Expand the node corresponding to the location from which you want to move an element. 2. Expand the node corresponding to the location where you want to move an element. 3. Drag the desired element to the desired location.
To move an element from the location,	perform the following actions: 1. Expand the node corresponding to the desired location. 2. Drag the desired element to the network name or another location.

8. *(Optional)* Change the position of the location element in the network configuration:

To move the location up in the list,	right-click the desired location, and then from the action menu, select ***Up***.

To move the location down in the list,	right-click the desired location, and then from the action menu, select ***Down***.

9. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Update topology. For details, see Updating Topology.
- To delete location, in the left pane of the tab, right-click the location name and select ***Remove Location***.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

9.7 Configuring Local Stations Monitoring

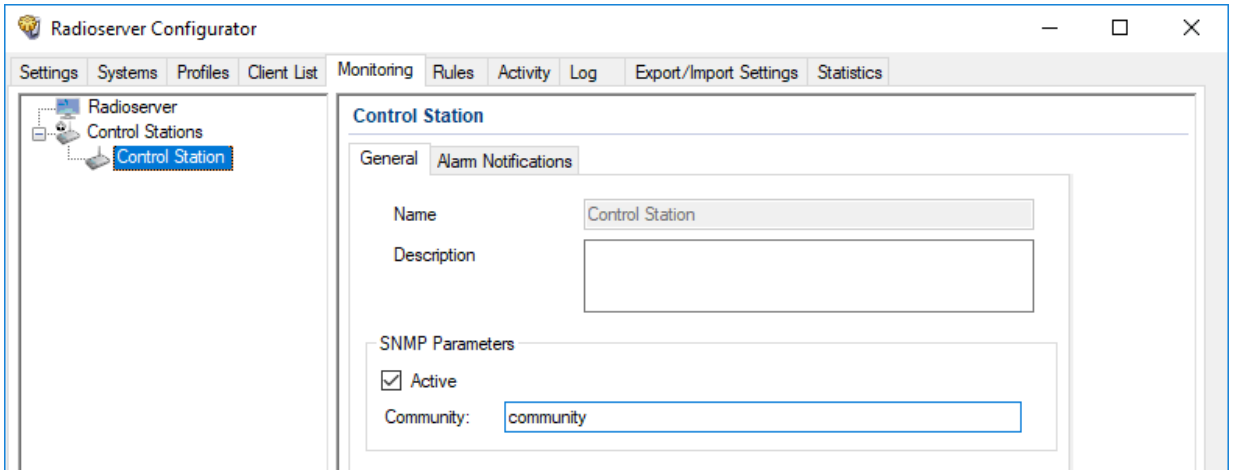
Follow the procedure to configure control stations monitoring that will be displayed on the topology diagram in SmartPTT Dispatcher.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Connect SmartPTT to local control stations. For details, see MOTOTRBO Control Stations.
- Configure SmartPTT connection to the monitoring database. For details, see Configuring Monitoring Database Connection.
- Configure SmartPTT connection to an external SNMP server. For details, see Configuring SNMP Server Connection.
- Obtain the community string for the SNMP server.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Monitoring*** tab.
2. In the left pane of the ***Monitoring*** tab, expand the ***Control Stations*** node, and then select the desired control station.



3. In the ***General*** tab, in the ***Description*** field, type the description of a control station that will be displayed on a topology diagram in *SmartPTT Dispatcher*.
4. In the ***SNMP parameters*** area, select the ***Active*** check box.
5. In the ***Community*** field, type the community string of the SNMP server.
6. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (***  ***)***.

Postrequisites:

- Configure alarm notifications. For details, see Configuring Alarm Notifications.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (***  ***)*** or ***Restart (***  ***)***.

9.8 Configuring Remote Gateway Monitoring

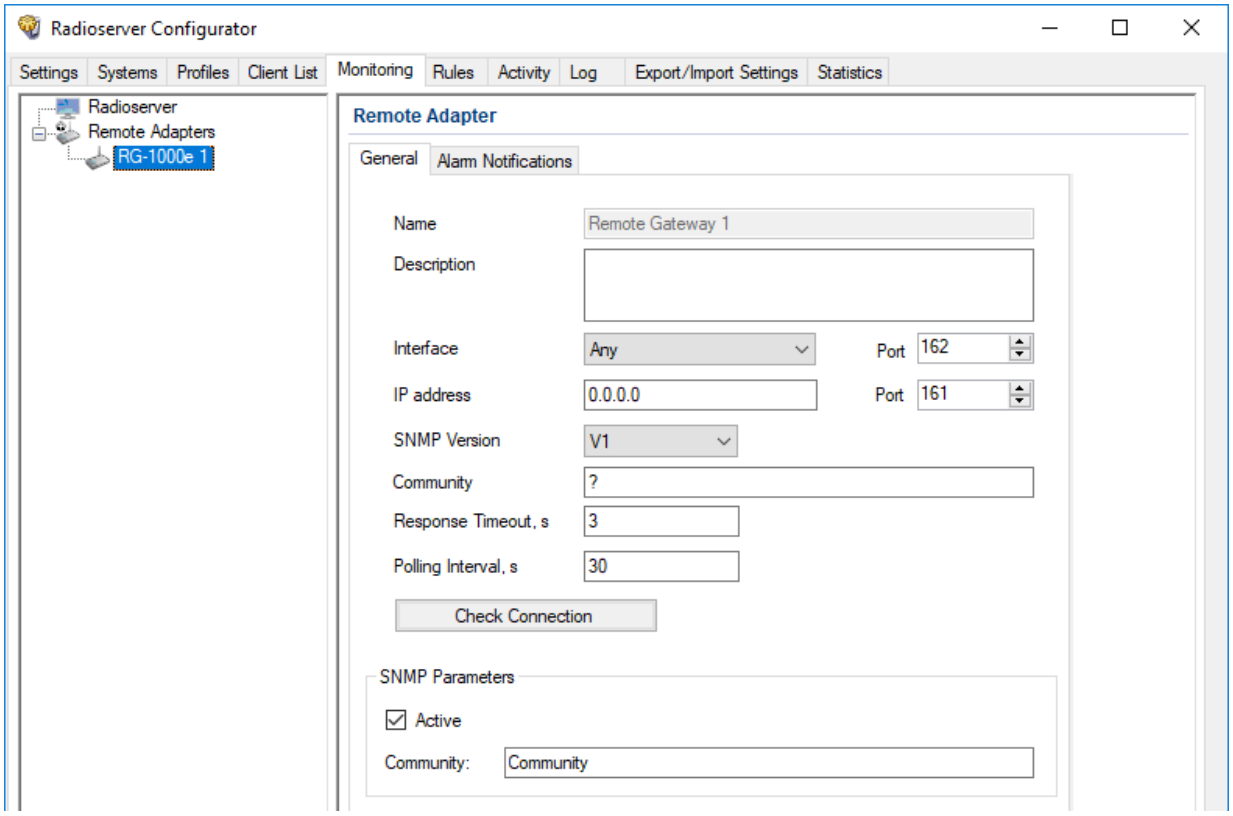
Follow the procedure to configure the remote adapter monitoring in SmartPTT.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Add the desired adapters and (if required) control station connections:
  - To connect MOTOTRBO stations, see MOTOTRBO Radio Systems.
  - To connect stations over analog interface, see Analog Interfaces.
- Configure SmartPTT connection to the monitoring database. For details, see Configuring Monitoring Database Connection.
- Configure SmartPTT interface for an external SNMP server. For details, see Configuring SNMP Server Connection.
- Obtain the community string for the SNMP server.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Monitoring*** tab.
2. In the left pane of the ***Monitoring*** tab, expand ***Remote Adapters***, and then select the desired adapter.
3. In the right pane of the ***Monitoring*** tab, open the ***General*** tab.



4. In the ***Description*** field, type the remote adapter description.
5. Configure the connection to a control station or a remote adapter:
    a. From the ***Interface*** list, select the IP address of the SmartPTT Radioserver host for interacting with a remote adapter.
    b. In the ***Port*** field, enter the SmartPTT Radioserver port number for interacting with a remote adapter.
    c. In the ***IP-address*** field, type the IP address of a remote adapter.
    d. In the ***Port*** field, enter the remote adapter port number.
6. From the ***SNMP Version*** list, select the SNMP protocol that is used in the radio system.
7. In the ***Community*** field, type a name of the community that is used for connection to a remote adapter over the SNMP protocol in the local network.
8. In the ***Response Timeout, s*** field, type type the amount of time in seconds during which SmartPTT Radioserver expects a response from a remote adapter.
9. In the ***Polling Interval, s*** field, type the amount of time in seconds after which SmartPTT Radioserver sends a request to a remote adapter.
10. Click the ***Check Connection*** button to check the status of the remote adapter connection. The window with information on the connection status appears.
11. Configure sending remote adapter data to the SNMP service:
    a. In the ***SNMP Parameters*** area, select the ***Active*** check box.
    b. In the field ***Community***, type the community entry of the SNMP server.
12. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Configure alarm notifications. For details, see Configuring Alarm Notifications.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (▷)*** or ***Restart (▣▷)***.
- In the firewall software on the radioserver computer, unlock the set ports. For details, see Radioserver Host.

9.8.1 Configuring Remote Control Stations Monitoring

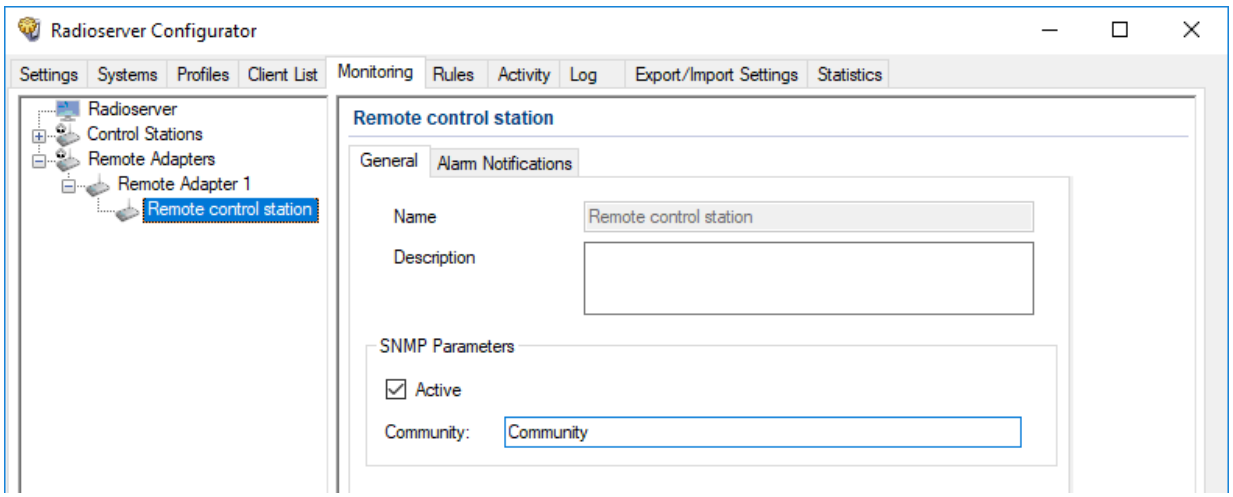
Follow the procedure to configure the remote control stations monitoring that will be displayed on the topology diagram in SmartPTT Dispatcher.

Prerequisites:

- Add remote adapters and the desired control stations:
  - To connect MOTOTRBO stations, see MOTOTRBO Radio Systems.
  - To connect stations over analog interface, see Analog Interfaces.
- Configure SmartPTT connection to the monitoring database. For details, see Configuring Monitoring Database Connection.
- Configure SmartPTT interface for an external SNMP server. For details, see Configuring SNMP Server Connection.
- Obtain the community string for the SNMP server.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Network Configuration*** tab.
2. In the left pane of the ***Network Configuration*** tab, expand ***Remote Adapters*** → ***<remote adapter name>***, and then select the desired control station.
3. In the right pane, select the ***General*** tab.



4. On the ***General*** tab, in the ***Description*** field, type the description of a control station.
5. In the ***SNMP parameters*** area, select the ***Active*** check box.
6. In the ***Community*** field, type the community string of the SNMP server.
7. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Configure alarm notifications. For details, see Configuring Alarm Notifications.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

9.9 Configuring Alarm Notifications

Follow the procedure to configure automatic sending of alarm notifications during malfunctions in the radio system.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Connect to radio systems:
  - To connect MOTOTRBO radio systems, see MOTOTRBO Radio Systems.
  - To connect P25 radio systems, see P25 Radio Systems.
- Connect SmartPTT to the monitoring database. For details, see Configuring Monitoring Database Connection.
- Configure SmartPTT interface for an external SNMP server. For details, see Configuring SNMP Server Connection.
- Configure SmartPTT connection to the mobile phone network. For details, see Connecting to Phone Modems.
- Configure SmartPTT connection to the Email server. For details, see Configuring Message Processing.
- Determine an object for which you want to configure alarm notifications. For details, see Network Monitoring.
- Obtain identification receiver data (Email, telephone number, radio ID, the community entry used for authentication on the SNMP server etc.) to enter the ***Receiver*** dialog box.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Monitoring*** tab.
2. In the left pane of the tab, perform one of the following actions:

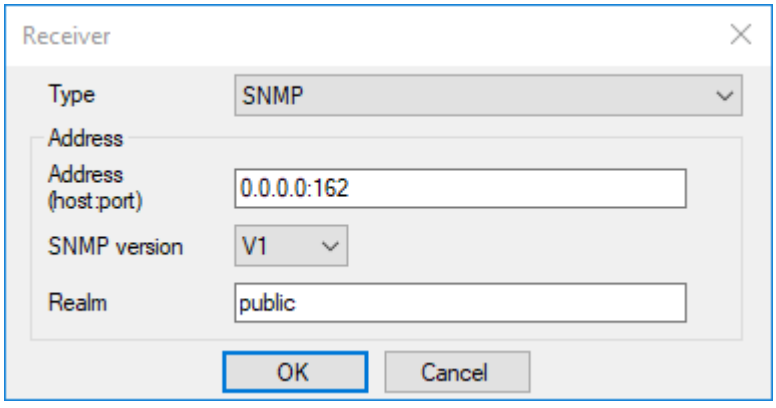
To configure notifications for a radioserver,	click ***<Radioserver name>***.
To configure notifications for individual repeater networks,	expand <***network type***> and then click the desired child node.
To configure notifications for individual nodes of repeater systems,	perform the following actions: 1. Expand <***network type***> → <***network name***>. 2. If the desired element misses, expand the <***location name***> node.

	3. Click the desired element.
To configure notifications for devices connected with control stations,	perform the following actions: 1. Expand ***Control Stations***. 2. Click the desired element.
To configure notifications for alarms connected with all control stations that are not part of repeater systems,	click ***Control Stations***.
To configure notifications for alarms connected with all control stations connected over the RG-1000e remote adapter,	expand the ***Remote Adapters*** node, and then click the desired ***<remote adapter name>*** subnode.
To configure notifications for separate control stations,	Expand ***Control Stations***, and then click the desired child node.
To configure notifications for separate remote control stations,	perform the following actions: 1. Expand the ***Remote Adapters*** node. 2. Expand the ***<remote adapter name>*** node. 3. Click the ***<control station name>*** node.

3. In the right pane of the ***Monitoring*** tab, open the ***Alarm Notifications*** tab.
4. In the ***Alarms*** area (if available), configure the desired alarms:

To configure sending of all alarm notifications,	click ***Select All***.
To cancel sending of all alarm notifications,	click ***Reset All***.
To configure manually the desired alarms about which notifications will be sent,	select or clear the desired alarms.
To configure alarms from network settings,	click ***Apply Network Settings***.

5. In the tab, click ***Add***.
The ***Receiver*** dialog box appears.



6. In the open dialog box, specify receivers of notifications:

To send notifications to Email,	perform the following actions: 1. From the ***Type*** list, select the desired *Email*. 2. In the ***Email*** field, type the Email of a receiver. ***NOTE*** To send notifications to several Emails, you have to configure several notifications.
To send notifications to talkgroups,	perform the following actions: 1. From the ***Type*** list, select *Message (Talkgroup)*. 2. From the ***Control Station*** list, select the desired slot, control station, or trunked system. 3. From the ***Talkgroup*** list, select the desired talkgroup.
To send notifications to radios,	perform the following actions: 1. From the ***Type*** list, select *Message (Radio)*. 2. In the ***Radio ID*** field, type ID of desired radios. Use hyphens to specify ranges and commas for enumeration of ID and ranges.
To send notification to SMS,	perform the following actions: 1. From the ***Type*** list, select *SMS*. 2. In the ***Telephone*** field, type the telephone number in international format. ***NOTE*** To send SMS to several telephone numbers you have to configure several notifications.
To send notifications to the SNMP server,	perform the following actions: 1. From the ***Type*** list, select *SNMP*. 2. In the field ***Address (host:port)***, type IP address and port number of the SNMP server in the following format: *<IP address in decimal format with dots>:<number of port>*. 3. From the list ***SNMP Version***, select the desired version of the SNMP protocol. 4. In the field ***Community***, type the community entry used for authentication.

7. In the ***Receiver*** dialog box, click ***OK*** to apply changes.
8. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- Repeat the procedure to add other receivers of notifications.
- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (***  ***)*** or ***Restart (***  ***)***.

9.10 Updating Topology

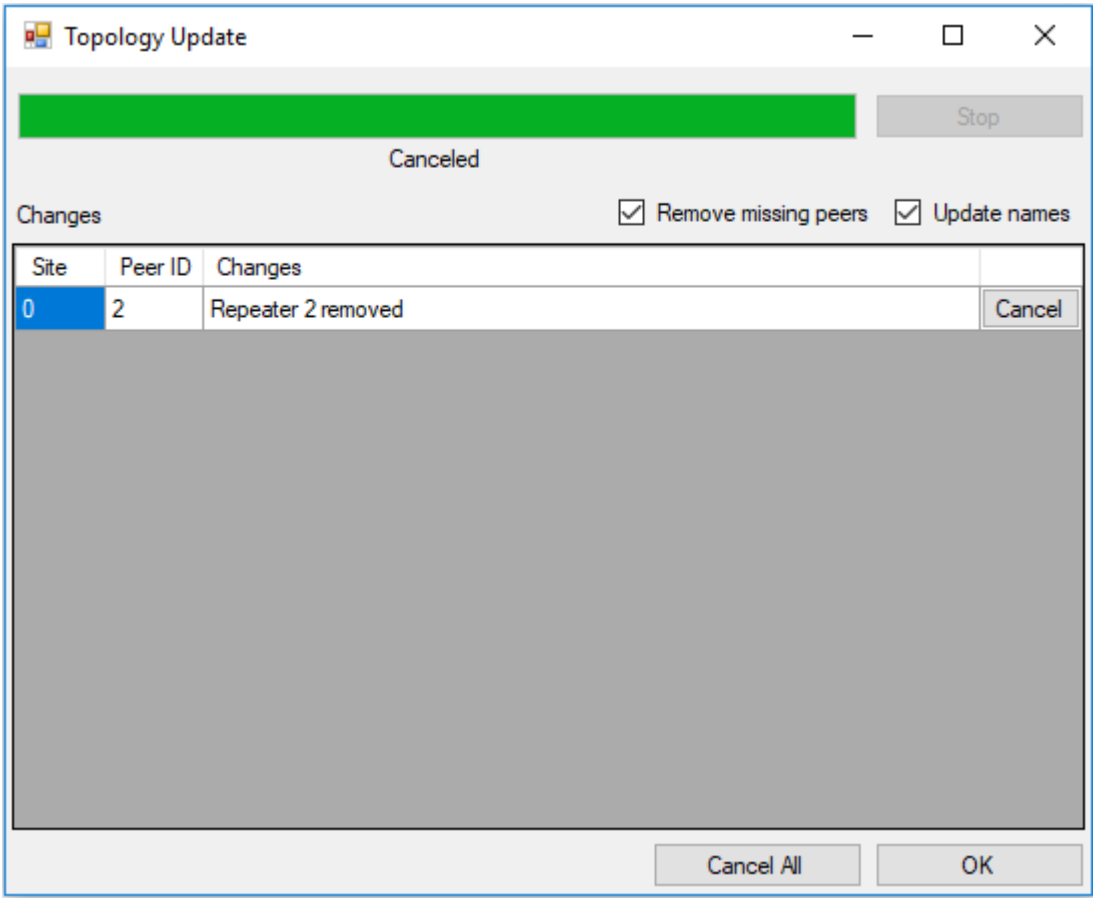
Follow the procedure to update topology.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Connect SmartPTT Radioserver to the desired radio systems:
  - To connect to a MOTOTRBO radio system, see MOTOTRBO Radio Systems.
  - To connect to a P25 radio system, see P25 Radio Systems.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Monitoring*** tab.
2. In the left pane of the ***Monitoring*** tab, expand <***network type***>, and then click <***network name***>.
3. In the right pane of the tab, open the ***System*** tab.
4. In the ***System*** tab, click ***Update Topology***.
   The ***Topology Update*** window appears and the update process starts automatically.



5. To change the topology update settings, perform the following actions:

To delete from topology missing nodes,	select the ***Remove missing peers*** check box.
To replace the current repeater names by those defined in their configuration files,	select the ***Update names*** check box.
To cancel changes for the desired node,	click ***Cancel*** next to the desired node.
To cancel all changes,	click ***Cancel All***.
To interrupt the update process,	click ***Stop***.

6. Click ***OK*** to apply changes.
7. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

10 Bridging and Cross Patching

SmartPTT provides features to route voice calls between radios and/or talkgroups from various sites, channels, radio systems, and servers.

Bridging

You can use the Bridging feature to connect radios and/or talkgroups from various sites and/or radio systems. SmartPTT provides two independent ways to configure bridging.

An administrator can configure bridging in SmartPTT Radioserver Configurator using multigroups. It is a convenient way to transmit voice calls between talkgroups in different radio systems and/or on different channels and slots. Multigroups automatically define routing directions using talkgroup IDs, but they cannot be used to transmit private calls.

Each multigroup is assigned a specific talkgroup ID. When you make a call to this talkgroup, the call will be received by all talkgroups with the same ID in all selected systems. You can also add IDs of the radios that also must receive this call regardless of the radio system. For details, see Bridging.

Operators can configure bridging in SmartPTT Dispatcher using routes. This way provides the ability to transmit both private and group calls, but an operator must manually configure routing directions that connect desired talkgroups and/or radios. For details, see “Bridging” in *SmartPTT Dispatcher Guide*.

Cross Patches (including Inter-Server Patching)

You can use cross patches to connect different talkgroups within one or several radioservers. A call made to a talkgroup included in a cross patch will be heard by all participants of the cross patch. It is also true for a call made by an operator or a telephone subscriber.

Important
You cannot combine several talkgroups from the same channel in one cross patch, or combine talkgroups from different non-affiliated radioservers in one cross patch.

To connect talkgroups within one radioserver, it is not required to purchase an additional license. An operator can create a cross patch directly in the SmartPTT Dispatcher interface. When you log out from the dispatch console, all the created cross patches will be saved, but they will not be available. For details, see “Cross Patches” in *SmartPTT Dispatcher Guide*.

If you want to connect talkgroups from different radioservers, you must have the Inter-Server Patching license. An administrator also must configure affiliated radioservers' connection in SmartPTT Radioserver Configurator. After the connection was configured, operators can select talkgroups from different affiliated radioservers to create cross patches in SmartPTT Dispatcher. For details, see Inter-Server Patching.

NOTE
You cannot make private calls using cross patches. For private calls between various radio systems, use bridging.

10.1 Bridging

In SmartPTT, bridging is a radioserver-controlled voice-only integration feature for radios and/or talkgroups from various radio systems. Typical cases of bridging implementation are as follows:

- Voice communication between VHF and UHF radio systems.
- Radio systems integration to increase the total voice communication coverage area.
- Privileged radios integration into multiple radio systems.

- Bridging does ***not*** depend on dispatch consoles (active or inactive).

Bridging has the following advantages over cross patches:

- Bridging provides the ability to integrate group and private calls.
- Bridging configuration rights can be provided to dispatchers.
- Bridging configuration changes do ***not*** require radioserver restart.

Important
Bridging does not provide text message exchange between radio systems.

Important
Bridging is unavailable for systems accessed over analog interfaces. For details, see MOTOTRBO Control Stations.

In SmartPTT, bridging includes the following configuration options:

- Radioserver-defined multigroups. For details, see Multigroups.
- Dispatcher-controlled routes. For details, see “Bridging” in *SmartPTT Dispatcher Guide*.

10.1.1 Multigroups

Multigroup is a SmartPTT wrapping over talkgroup that is provided within the Bridging feature. If radioserver receives a group call and the talkgroup ID is equal to the multigroup ID, radioserver will initiate a group call to the same ID in other radio systems.

To initiate a call in other radio systems, the following conditions must be fulfilled:

- Multigroup settings provide a list of control stations, conventional system slots, and trunked radio systems where the call must be initiated.
- Corresponding control stations, slots, and trunked radio systems must have the corresponding talkgroup.
- If talkgroups are unavailable, at least one radio from the list of radios must be registered on the corresponding control station, slot, or trunked radio system.

The following table provides the summary of the multigroup features:

Target System is Selected	***Talkgroup is Available***	***Radio is Registered***	***Result***
NO	any	any	call is ***not*** initiated
YES	NO	NO	call is ***not*** initiated
YES	NO	YES	call initiation succeeded
YES	YES	NO	call initiation succeeded
YES	YES	YES	call initiation succeeded

10.1.2 Managing Bridging

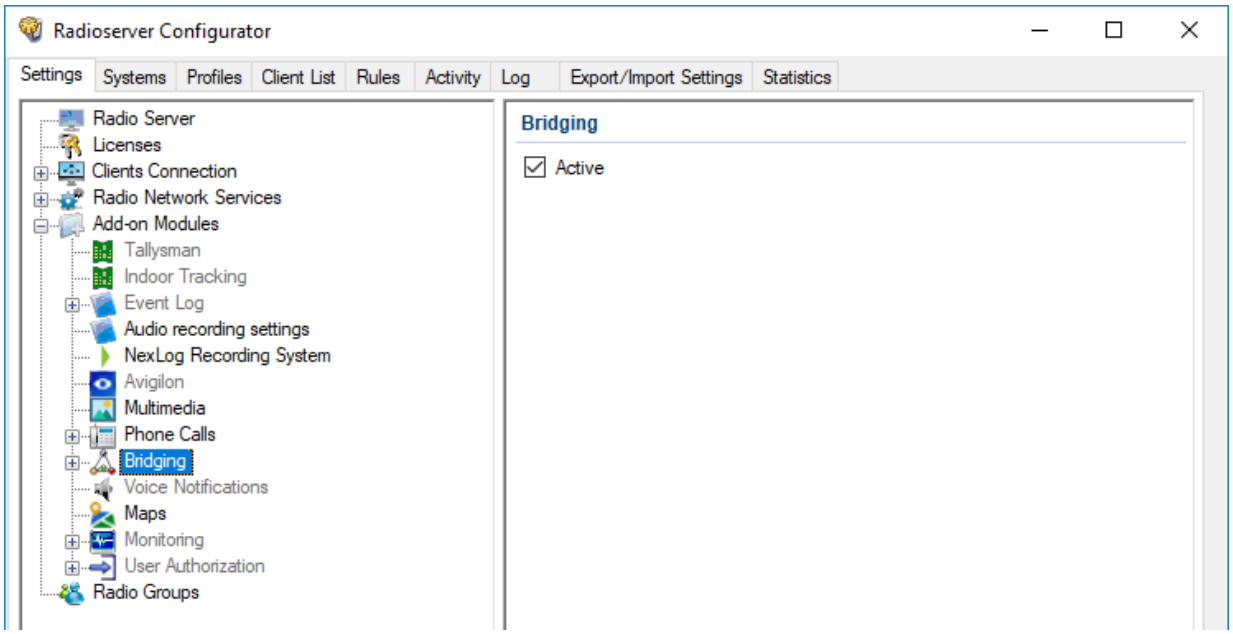
Follow the procedure to enable or disable bridging in SmartPTT.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure that the installed license includes the bridging feature. For details, see Viewing License Items.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Add-on Modules***, and then click ***Bridging***.



3. In the right pane, perform one of the following actions:

To enable bridging,	select the ***Active*** check box.
To disable bridging,	clear the ***Active*** check box.

4. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- Configure bridging in SmartPTT Dispatcher. For details, see “Bridging Service” in *SmartPTT Dispatcher Guide*.
- Add and configure multigroups. For details, see Managing Multigroups.

10.1.3 Managing Multigroups

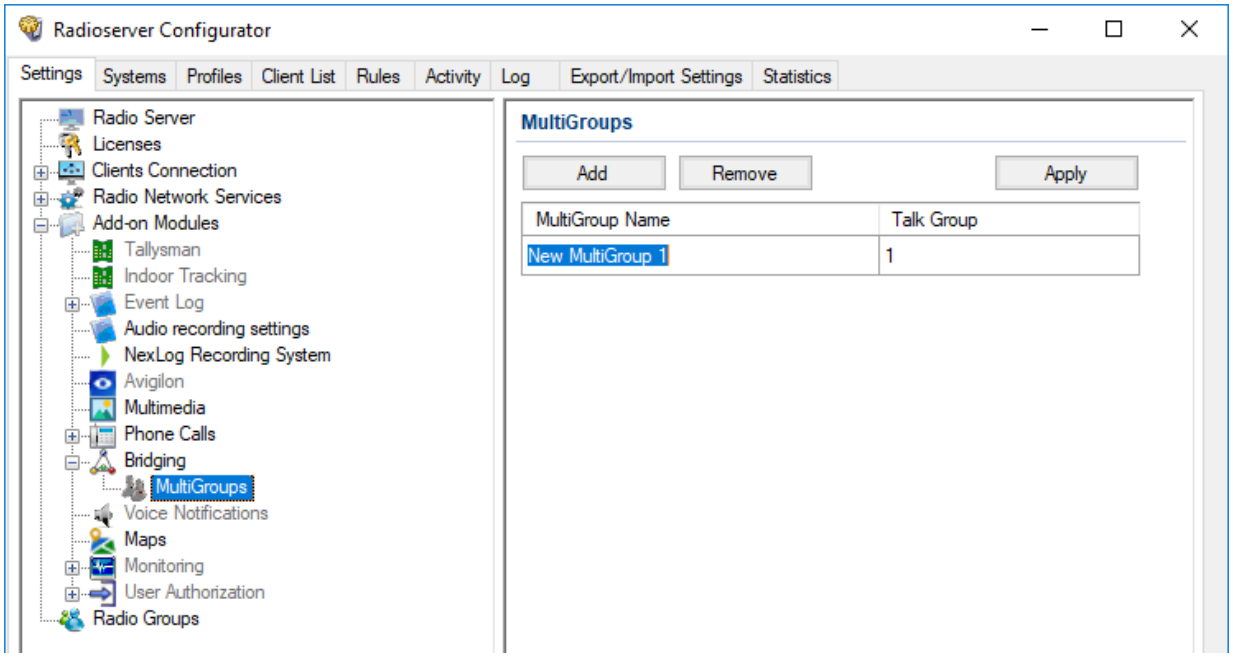
Follow the procedure to modify the list of multigroups supported by SmartPTT Radioserver.

Prerequisites:

Enable bridging. For details, see Managing Bridging.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Add-on Modules*** → ***Bridging***, and then click ***Multigroups***.



3. In the right pane, perform one of the following actions:

To add a new multigroup,	click ***Add***.
To delete an existing multigroup,	perform the following actions: 1. Click the desired multigroup in the table. 2. Click ***Remove***.

4. *(Optional)* Modify the parameters of the desired multigroup in the table:
   a. In the ***MultiGroup Name*** column, click twice the multigroup name, and then type a new name.
   b. In the ***Talk Group*** column, click twice the current ID, and then type a new ID.
5. *(Optional)* Configure the multigroups. For details, see Configuring Multigroups.
6. To immediately apply changes, click ***Apply***.
7. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration (***  ***)***.

10.1.4 Configuring Multigroups

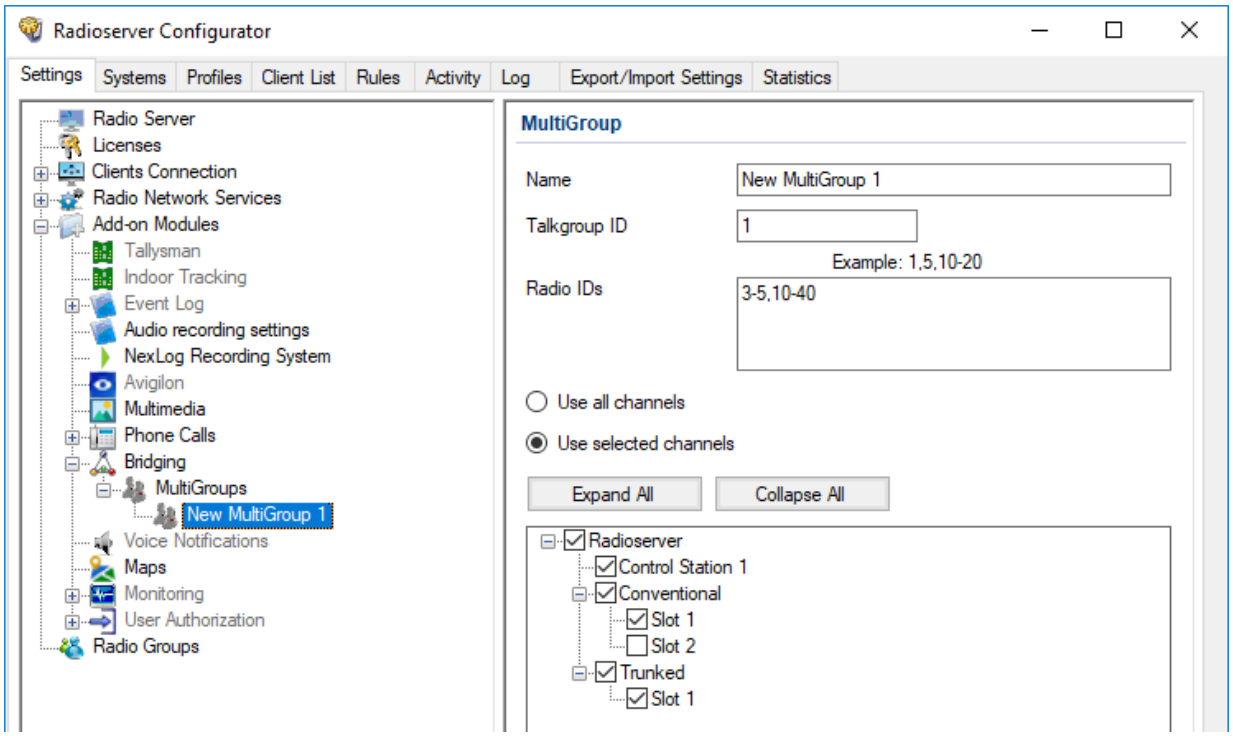
Follow the procedure to configure an existing multigroup.

Prerequisites:

- Connect to radio networks:
  - To access the MOTOTRBO radio systems, see MOTOTRBO Radio Systems.
  - To access the P25 radio systems, see P25 Radio Systems.
- Add multigroups. For details, see Managing Multigroups.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand ***Add-on Modules*** → ***Bridging*** → ***MultiGroups***, and then click the desired multigroup.



3. In the ***Name*** field, type the desired name for the multigroup.
4. In the ***Talkgroup ID*** field, type the talkgroup ID, calls to which will be interpreted by SmartPTT Radioserver as calls to the multigroup.
5. In the ***Radio IDs*** field, type the IDs of radios, whose registration in a radio system is required for calls to the multigroup to be bridged to that system.
6. Select bridging mode:

To bridge calls to any radio network if at least one radio listed in the ***Radio IDs*** field is registered there,	select the ***Use all channels*** option.
To bridge calls only to a limited set of radio networks,	perform the following actions: 1. Select the ***Use selected channels*** option.

2. Click ***Expand All*** to expand all nodes of the radio system object tree.
3. Select the check boxes next to the desired control stations, channels and systems.
4. Clear the check boxes next to the undesired control stations, channels and systems.

7. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.
8. To immediately apply changes, perform the following actions:
   a. In the left pane, click ***MultiGroups***.
   b. In the right pane, click ***Apply***.

10.2 Inter-Server Patching

The Inter-Server Patching feature provides the ability to connect each SmartPTT Radioserver to one or several other radioservers. To use Inter-Server Patching, you must install the Inter-Server Patching license on all radioservers that will be connected.

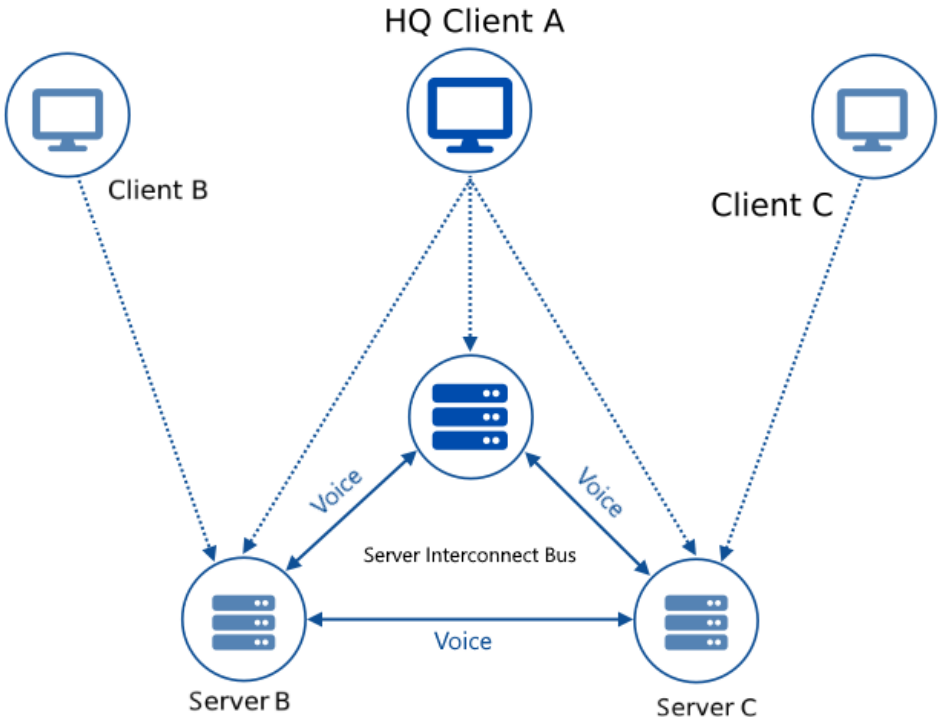
NOTE
The Inter-Server Patching feature provides additional capabilities for cross patches.
For information on cross patches in SmartPTT Dispatcher, see “Cross Patches” in *SmartPTT Dispatcher Guide*.

You can use this feature to combine talkgroups from affiliated radioservers in cross patches. The calls made to a talkgroup included in a cross patch will be retransmitted to all participants of the cross patch even if they belong to different radioservers. The connected radioservers can transmit voice to each other.

The Inter-Server Patching provides the following features:

- Connect two or more radioservers
- Make and receive group calls to/from other radioservers
- Use cross patches to connect talkgroups from different radioservers
- Log and record voice calls on affiliated radioservers

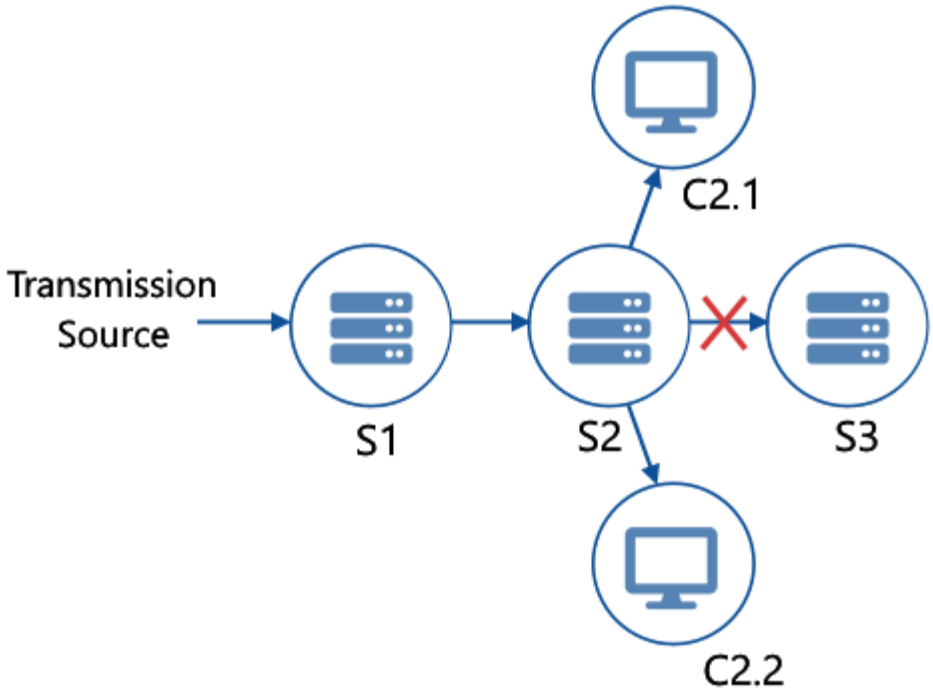
Important
Every radioserver in the system must have a unique ***Server ID***. Every radio system that will participate in inter-server cross patches must have a unique ***Network ID***.



NOTE

Only Client A can create cross patches with any available objects of Server A, B, and C, because it is the only client that is connected to all servers and can see their radio fleet objects.

A voice transmission can be retransmitted to another radioserver only from the radioserver that originally received this transmission. That means you cannot create a chain of cross patches. See the example below:



On the image, there are three radioservers (S1, S2, S3) combined into two cross patches (S1–S2, S2–S3). The radioserver S2 is also connected to two clients (C2.1 and C2.2). The radioserver S1 receives a transmission and retransmits it to the radioserver S2. The radioserver S2 cannot retransmit it further to radioserver S3. The clients connected to S2 will receive this transmission.

Important
If Web Clients are used in the Inter-Server Patching, in each Configurator of the affiliated radioservers, create accounts for Web Clients that differ from client accounts on other affiliated radioservers.

10.2.1 Configuring Affiliated Server Connection

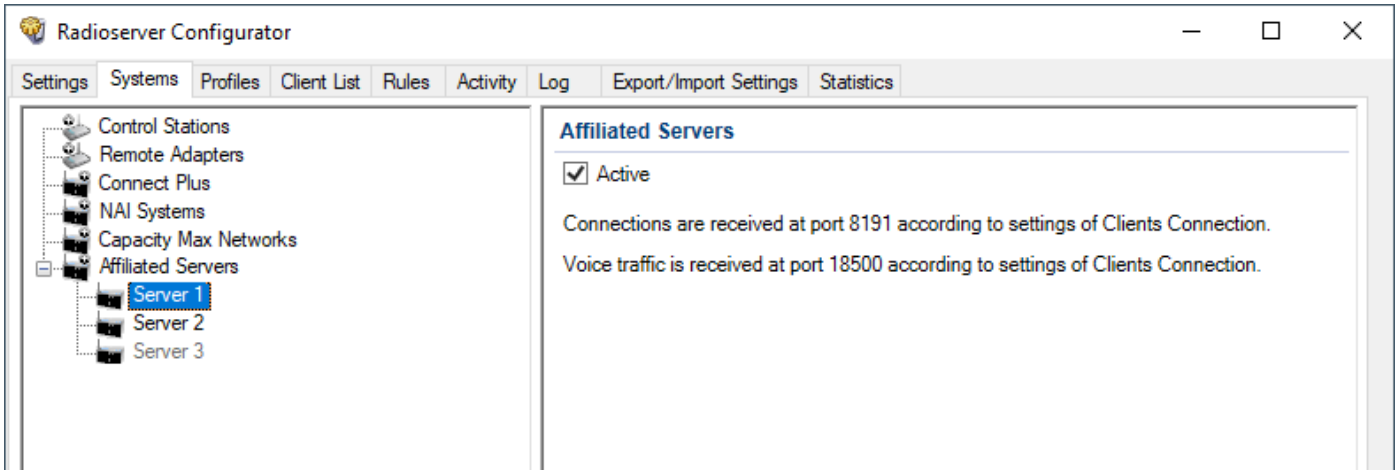
Follow the procedure to configure parameters of the radioserver to connect it to affiliated servers.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Install the Inter-Server Patching license on all radioservers that will be connected. For details, see Licensing.
- Ensure that every radioserver in the system has a unique ***Server ID***. For details, see Configuring Radioserver.
- Ensure that every radio system that will participate in inter-server cross patches has a unique ***Network ID***.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, click the ***Affiliated Servers*** node.
   The connection settings appear in the right pane.



3. Select the ***Active*** check box to enable the Inter-server Patching feature and unlock its settings.
4. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- Configure connection to affiliated servers.

10.2.2 Configuring Connection to Affiliated Server

Follow the procedure to configure the connection to an affiliated server.

Prerequisites:

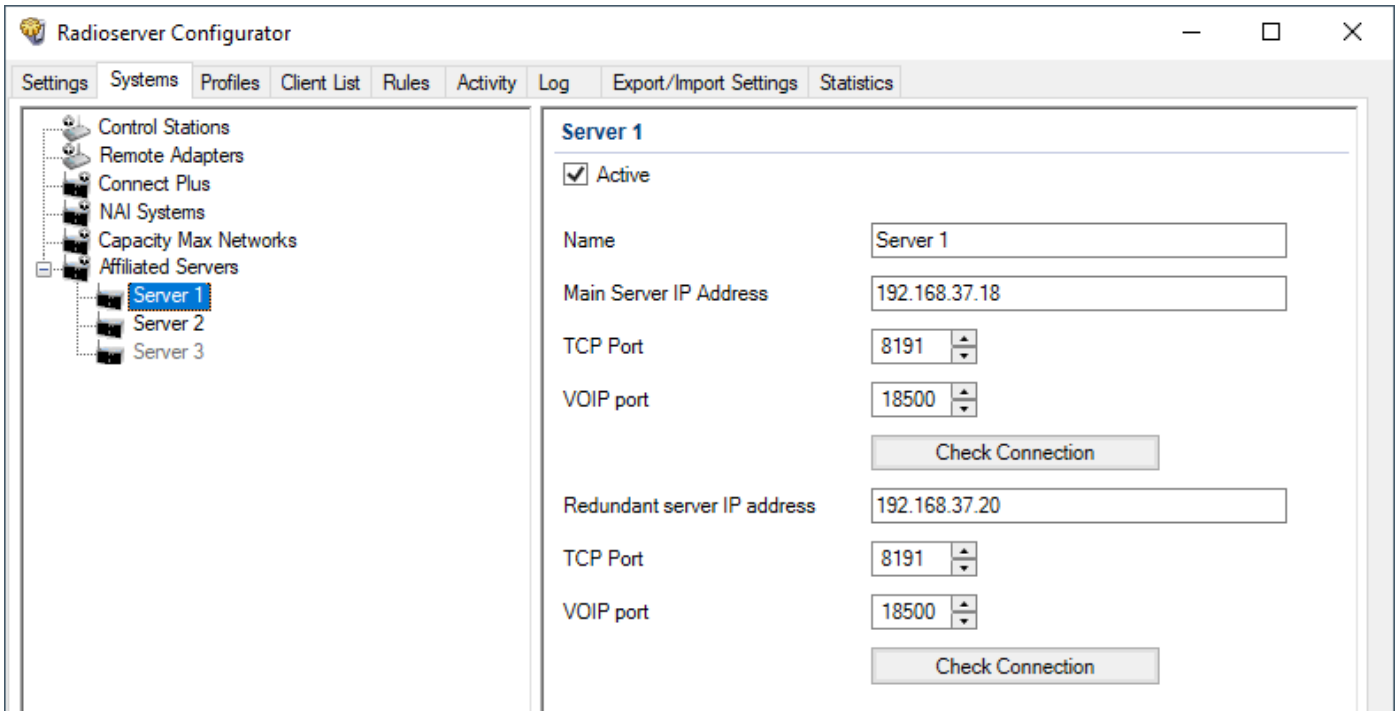
- Ensure that the Inter-Server Patching license is installed on the affiliated server that will be connected to the radioserver. For details, see Licensing.
- Configure connection parameters for your radioserver. For details, see Configuring Inter-server Patching.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Systems*** tab.
2. In the left pane, perform one of the following actions:

To add a new affiliated radioserver,	right-click the ***Affiliated Servers*** node, and then click ***Add***.
To edit an existing affiliated radioserver,	expand the ***Affiliated Servers*** node, and then click the desired affiliated radioserver subnode.

The affiliated radioserver settings will appear in the right pane.



3. Select the ***Active*** check box to enable connection to the desired radioserver.
4. In the ***Name*** field, type the radioserver name.
5. In the ***Main Server IP Address*** field, type the IP address of the main affiliated radioserver.
6. In the ***TCP Port*** field, type the TCP port number of the main affiliated radioserver. It must be the same as the ***HTTP port*** value in the ***Clients Connection*** node on the affiliated radioserver.
7. In the ***VOIP Port*** field, type the VOIP port number of the main affiliated radioserver. It must be the same as the ***VoIP Listen Port*** value in the ***Clients Connection*** node on the affiliated radioserver.
8. *(Optional)* Click the ***Check Connection*** button to check connection between radioservers.

9. *(Optional)* If the affiliated server has a redundant radioserver, enter the redundant radioserver IP address, TCP, and VOIP ports in the corresponding fields and click the ***Check Connection*** button to check connection between radioservers.
10. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

- To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.
- In the affiliated radioserver's configuration perform this procedure to create and configure the access to the current radioserver.

11 Alternation (Redundancy)

SmartPTT supports operation with the primary and redundant radioservers. The redundant radioserver is activated in case of primary radioserver breakdown. You can configure the inactivity time of the main radioserver after which switching to the redundant one takes place. The minimum value is *20* s.

Important
The redundant radioserver is not intended to be used permanently. If the redundant radioserver cannot synchronize with the primary one for 31 days, it is deactivated.

The primary radioserver can have only one redundant radioserver.

Important
To activate a redundant radioserver, install the corresponding license. For details, see Licenses.

If synchronization with primary radioserver is enabled, the redundant server settings are synchronized with the primary server in the continuous one way direction copy mode. The primary server operates in the normal mode, the backup server constantly synchronizes its settings with the settings of the primary one.

Important
If you use a certificate for the encrypted connection to Web Client, the certificate is not automatically copied to the redundant server when redundancy is enabled. On the redundant radioserver, use SmartPTT Radioserver Configurator to manually import the certificate. For details, see Configuring Web Client Connection.

For the proper operation of the redundant radioserver, certain values and parameters of primary and redundant radioservers must not be the same. For this, new parameter values must be specified in the correspondence table.
For information on the correspondence table, see Configuring the Correspondence Table.

If the primary radioserver settings were changed after the redundant radioserver start, you must update the correspondence table.

NOTE
After configuring redundant and primary radioservers, you must add them to SmartPTT Dispatcher.
For information on adding radioservers, see “Radioservers” in *SmartPTT Dispatcher Guide*.

Important
Automatic connection between the primary and redundant radioservers is available only for desktop clients and third-party applications.

11.1 Configuring Redundant Radioserver

Follow the procedure to add and configure the redundant radioserver.

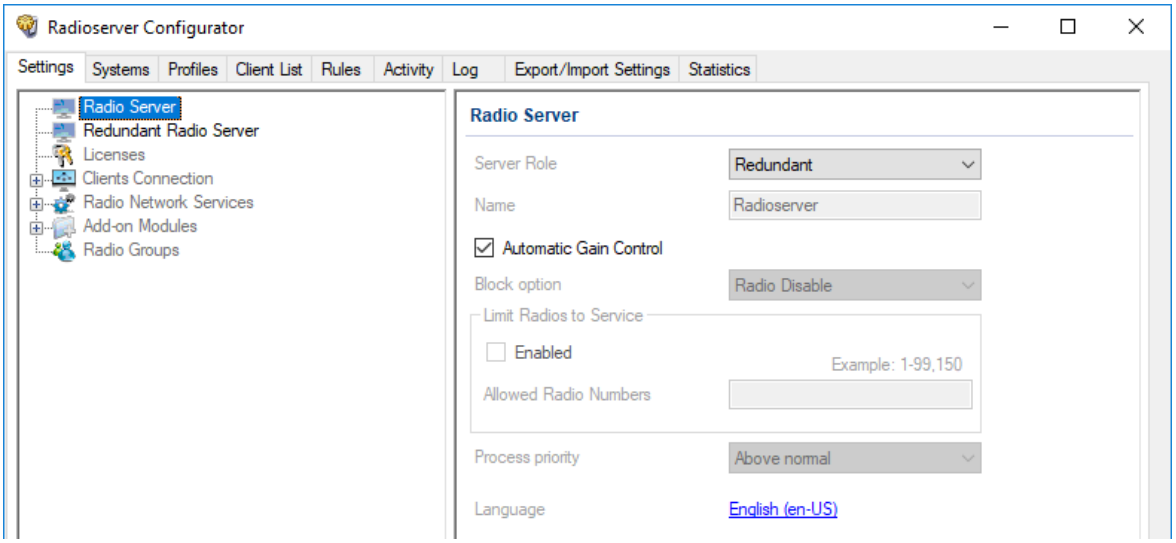
Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure all parameters of the primary radioserver are saved, and the radioserver is running. If the parameters were changed, save the changes and restart the primary radioserver to apply the changes to the redundant radioserver.
- Obtain the primary radioserver IP address.

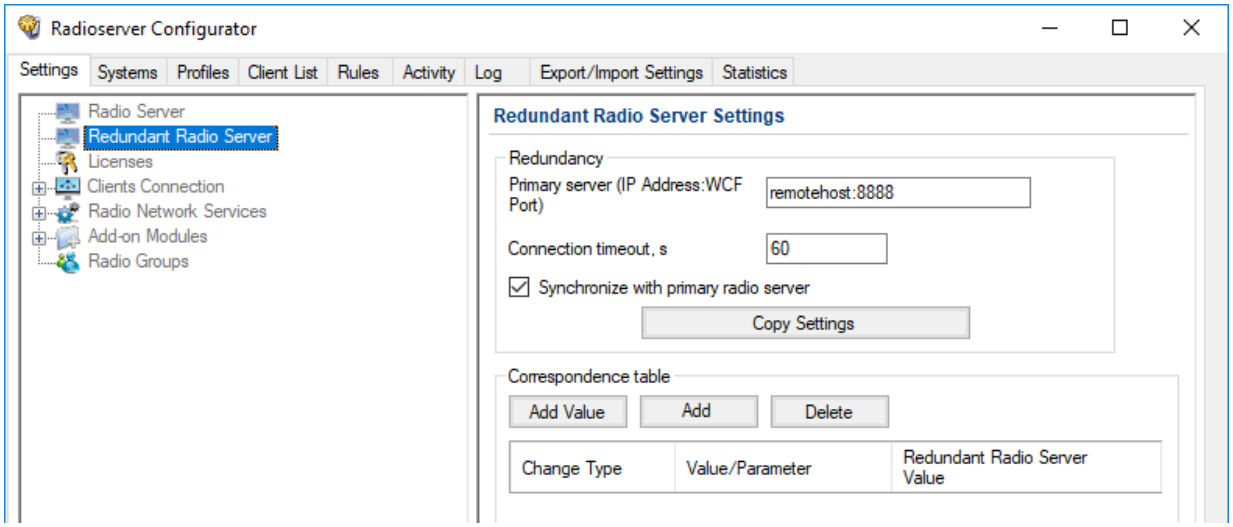
Procedure:

1. In the SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane of the ***Settings*** tab, click ***Radio Server***.

3. In the ***Radio Server*** pane, from the ***Server Role*** list, select *Redundant*.
   In the left pane, the ***Redundant Radio Server*** node appears.



4. In the left pane of the ***Settings*** tab, click ***Redundant Radio Server***.
   In the right pane of SmartPTT Radioserver Configurator, the redundant SmartPTT Radioserver settings appear.



5. In the ***Redundancy*** area, perform the following actions:

   a. In the ***Primary Server (IP Address:WCF Port)*** check box, type the primary SmartPTT Radioserver IP address and port.

   b. *(Optional)* In the ***Connection timeout, s*** field, type time interval after which the redundant SmartPTT Radioserver becomes active.

   c. Perform one of the following actions:

To copy primary SmartPTT Radioserver settings to the redundant one,	click ***Copy Settings***.
To activate the automatic synchronization of the redundant SmartPTT Radioserver with the primary one after the primary SmartPTT Radioserver restart,	select the ***Synchronize with primary radio server*** check box.

6. Configure the Correspondence table.
   For information on configuring the table, see Configuring the Correspondence Table.

11.1.1 Configuring the Correspondence Table

Follow the procedure to configure the Correspondence table for the redundant radioserver.

Prerequisites:

- Ensure all parameters of the primary radioserver are saved, and the radioserver is started.
- Ensure the ***Synchronize with primary radio server*** check box is selected in the ***Redundancy*** area.

Procedure:

1. In the Correspondence table, set or edit the existing values or parameters for replacing.
   For details, see Setting Values and Setting Parameters.
2. *(Optional)* To sort entries in the table, perform the following actions:

To sort entries ascending,	click the desired column heading until the Ascending Icon (▲) appears on the right of the heading.
To sort entries descending,	click the desired column heading until the Descending Icon (▼) appears on the right of the heading.

NOTE
Entries are sorted only by one column, clicking the name of another column automatically discards the sorting order applied earlier.

3. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.
4. To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

11.1.1.1 Setting Values

Follow the procedure to set a replacing value for the redundant radioserver in the Correspondence table.

Important
The the Correspondence table value replaces all similar values copied from the primary radioserver parameters.

Procedure:

1. In the ***Correspondence table*** area, click ***Add Value***.
   In the correspondence table below, a new entry appears.
2. In the desired entry, in the ***Value/Parameter*** column, type the desired value that will be replaced.
3. In the desired entry, in the ***Redundant Radio Server Value*** column, type a new value for the redundant radioserver.

Postrequisites:

To edit a value in the ***Value/Parameter*** or ***Redundant Radio Server Value*** columns, double-click the desired entry in the Correspondence table, and then type a new value.

11.1.1.2 Setting Parameters

Follow the procedure to set a replacing parameter for the redundant radioserver in the Correspondence table.

Procedure:

1. In the ***Correspondence table*** area, click ***Add***.
   The ***Parameter Overriding*** window appears.
2. In the left pane of the ***Parameter Overriding*** window, select the desired tab (***Settings*** or ***Systems***), and then expand the desired node.
   In the right pane, the area for selecting the parameter and its value appears.
3. From the ***Parameter*** list, select the desired parameter:
   - For NAI - IP Site Connect, NAI - Capacity Plus and NAI - Linked Capacity Plus replace ***Peer ID*** parameter values.
   - *(Optional)* Replace IP-addresses.
   - *(Optional)* Replace databases names.
   - For NAI - IP Site Connect, NAI - Capacity Plus, NAI - Extended Range Direct Mode and NAI - Linked Capacity Plus networks, select the ***Active*** check box for the ***DDMS mode control*** parameter to establish dependence of the redundant server DDMS activity from the DDMS activity of the primary server.

NOTE
If the ***Synchronize with primary radio server*** check box is cleared, this check box is transferred to the ***DDMS Settings*** node of each network respectively. If the ***DDMS Mode Control*** check box is cleared, the activity of the redundant server does not affect the activity of DDMS whose address is specified in the settings of the redundant server.

NOTE
If you configure ***Clients Connection***, you do not need to replace its parameters for the redundant radioserver.

4. In the ***Value*** area, set the value in one of the following ways:
   - Type the value in the field.
   - Select the value from the list.
   - Select/clear the check box.
5. Click ***Add*** to add the parameter to the Correspondence table.
6. Click ***Finish*** to close the window.

Postrequisites:

To edit a parameter or its value, double-click the desired entry in the Correspondence table, and then select another parameter, or change the selected value.

12 Maintenance

The chapter provides information on the operating SmartPTT observation as well as its configuration and database restoration.

12.1 Viewing System Events

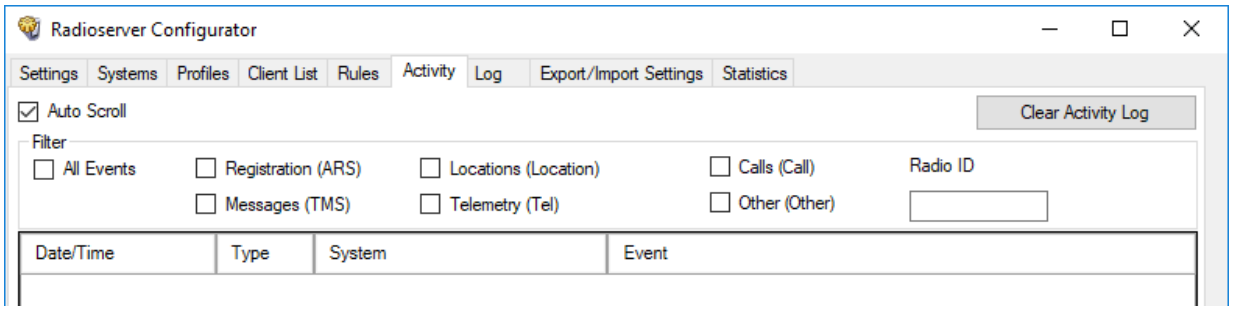
Follow the procedure to to view radioserver-detected events.

Prerequisites:

When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Activity*** tab.



2. *(Optional)* To turn on automatic event scrolling and show the most recent events, select the ***Auto Scroll*** check box.
3. In the ***Filter*** area, filter the desired events:

To show all events,	select the ***All Events*** check box.
To show registration events only,	select the ***Registration (ARS)*** check box.
To show text messaging events only,	select the ***Messages (TMS)*** check box.
To show location-related events only,	select the ***Locations (Location)*** check box.
To show telemetry and remote control events only,	select the ***Telemetry (Tel)*** check box. ***NOTE*** The check box does not affect Data Acquisition events.
To show voice reception/transmission events only,	select the ***Calls (Call)*** check box.
To show any other events,	select the ***Other (Other)*** check box.
To show events related to one or multiple Radio IDs only,	in the ***Radio ID*** field, type radio IDs. Use hyphens to type ID ranges; use commas to list IDs and ID ranges.

4. *(Optional)* To sort events by the ***Date/Time*** column and/or ***Type*** column, perform the following actions:

To sort events ascending,	click the column header until the Ascending (▲) icon appears in it.

To sort events descending,	click the column header until the Descending (▼) icon appears in it.

5. *(Optional)* To delete entries from the table (not from the database), clear ***Clear Activity Log***.

12.1.1 Event Types

SmartPTT provides information on the following types of events on the radio network:

- Radio registration
- Voice calls and their equivalents, for example, voice notifications
- Text messages
- Location reports
- Telemetry signals and remote control commands
- Various other types of events, such as radio commands

Description of these types of events is given below.

Registration (ARS)

Registration-related events are displayed on the ***Activity*** tab as follows:

- Event direction indicator (<–) (–>)
- Radio IP address and identifier (in decimal) in the format *<IP address> (<identifier>)*
- Additional information

> ***EXAMPLE***
>
> The attempt to obtain information about the radio with the 902 identifier presence in the network is failed:
>
> 12.0.3.134 (902) Inaccessible

Locations

Location-related events are displayed on the ***Activity*** tab as follows:

- Event direction indicator (<–) (–>)
- Radio IP address and identifier (in decimal) in the format *<IP address> (<identifier>)*
- Request number
- Additional information

EXAMPLE

Location coordinates of the radio with the 417 identifier on 2020.01.01 at 01:00:01 are latitude = 56,47907, longitude = 85,06649:

12.0.1.161 (417) Triggered Location Report id = 5 Latitude = 56,47907. Longitude = 85,06649 Timestamp: 01.01.2020 01:00:01

Calls

Call-related events are displayed on the ***Activity*** tab as follows:

- Voice transmission type
- Voice direction indicator in the format *<initiator ID> (<recipient ID>)*
- Additional information

EXAMPLE

Outgoing voice transmission from a dispatcher to the radio with the 445 identifier:

Private (Dispatcher) 1 –> 445 Tx

Messages (TMS)

Text message-related events are displayed on the ***Activity*** tab as follows:

- Message direction indicator in the format (*<sender ID> -> <recipient ID>*)
- The recipient and sender identifier in the format *<IP address> (<identifier>)*
  For IP addresses the following convention is applied:
  - If the first octet of the IP address corresponds to the CAI value of the network, then the recipient or sender is the radio.
  - If the first octet of the IP address corresponds to the CAI value of the group, then the recipient or sender is the talkgroup.
- Additional information

EXAMPLE

The radio with the 417 identifier sends a message to the radio with the 1 identifier:

- > 12.0.1.161 (417) – > 12.0.1.123 (1) SimpleTextMessage Need help

Telemetry

Telemetry-related events are displayed on the ***Activity*** tab as follows:

- Event subtype
- Radio IP address and identifier (in decimal) in the format *<IP address> (<identifier>)*
- Request number

- Additional information

> ***EXAMPLE***
>
> Incoming telemetry command when opening the door:
>
> Telemetry response. IP – 12.0.0.7; id= 54 type= Individual; opcode= QueryStatusResponse; payload= 00001000

Other

Other events can have different displaying structure on the ***Activity*** tab.

> ***EXAMPLE***
>
> Telephone call to the talkgroup:
>
> – > INVITE; From:sip: 1859@82.200.114.46:5060; To:sip:21@192.168.36.110:5060;
>
> < – Ringing(180); From:sip: 1859@82.200.114.46:5060; To:sip:21@192.168.36.110:5060;
>
> < – OK(200); From:sip: 1859@82.200.114.46:5060; To:sip:21@192.168.36.110:5060;
>
> – > ACK; From:sip: 1859@82.200.114.46:5060; To:sip:21@192.168.36.110:5060;
>
> – > BYE; From:sip: 1859@82.200.114.46:5060; To:sip:21@192.168.36.110:5060;
>
> < – OK(200); From:sip: 1859@82.200.114.46:5060; To:sip:21@192.168.36.110:5060;

12.1.2 Alarm Text Messages on Devices

Alarm text messages on devices are displayed in the following way:

- Outgoing text message direction indicator (<–)
- The recipient identifier in the format *<IP address> (<identifier>)*
  For IP addresses the following convention is applied:
  - If the first octet of the IP address corresponds to the CAI value of the network, then the recipient or sender is the radio.
  - If the first octet of the IP address corresponds to the CAI value of the group, then the recipient or sender is the talkgroup.
- Service text SimpleTextMessage
- The device name in the format
  Name : <device name>
- The device location in the format
  Location : <location name>
- The device ID as on the ***Network Configuration*** tab
- A multiple hyphen delimiter
- The list of alarms in the format
  <alarm name> : –

EXAMPLE

< – 12.0.2.88 (600) SimpleTextMessage Name : dms:rest@3.peers.55 Location : NAI– Linked Capacity Plus 213 Identifier : 3001 ---------- Repeater overheat : – Amplifier Fan Failure : –

12.2 Exporting Settings

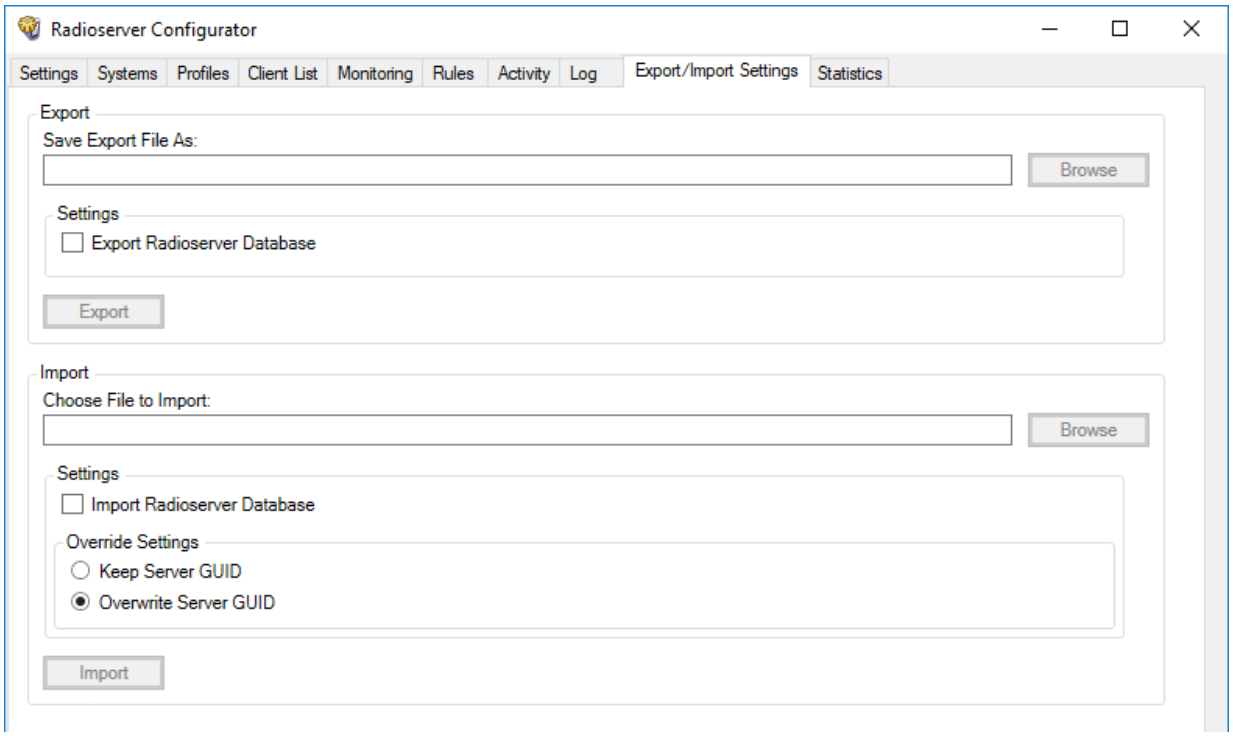
Follow the procedure to export SmartPTT Radioserver settings and its database (optional).

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Stop SmartPTT Radioserver by clicking the ***Stop (*** ***)*** button at the bottom of SmartPTT Radioserver Configurator.
- After you stop SmartPTT Radioserver, check the connection to all used databases. On the ***Settings*** tab, open settings of the desired database, and then in the ***Creating Database*** area, click ***Check connection***. For details, see Event Log, Monitoring, or User Authorization.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Export/Import Settings*** tab.



2. In the ***Export*** area at the top of the tab, specify the file to export settings into:
   a. Click the ***Browse*** button to the right of the ***Save Export File As*** field.
   b. In the window that appears choose the desired folder and type file name in the text field at the bottom of the window.
   c. Click the ***Save*** button at the bottom of the window.
   The specified path and file name are displayed in the ***Save Export File As*** field.

NOTE
You can also type or paste the full file path into this field.

3. *(Optional)* Select the ***Export Radioserver Database*** check box to include the SmartPTT Radioserver database into the same backup file.
4. Click the ***Export*** button.
   If the operation is successful, a notification appears.
5. After successful exporting, in the dialog box, click ***OK***.

12.3 Importing Settings

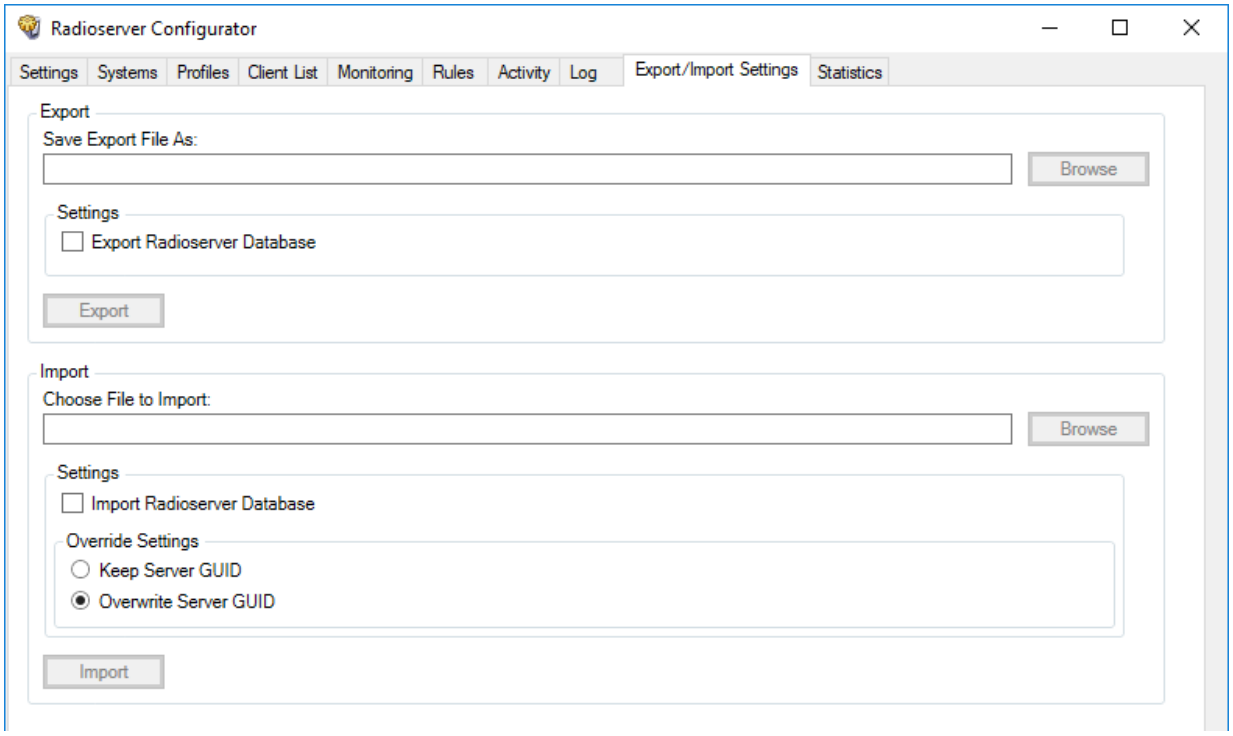
Follow the procedure to import SmartPTT Radioserver settings and database (optional).

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *System Administrators* group. For details, see Loging in to Radioserver Configurator.
- Stop SmartPTT Radioserver by clicking the ***Stop (*** ***)*** button at the bottom of SmartPTT Radioserver Configurator.
- After you stop SmartPTT Radioserver, check the connection to all used databases. On the ***Settings*** tab, open settings of the desired database, and then in the ***Creating Database*** area, click ***Check connection***. For details, see Event Log, Monitoring, or User Authorization.

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Export/Import Settings*** tab.



2. In the ***Import*** area, specify the file to import settings from:
   a. Click the ***Browse*** button to the right of the ***Choose File to Import*** field.
   b. In the window that appears choose the desired file containing exported server settings.

c. Click the ***Open*** button at the bottom of the window.
The specified path and file name are displayed in the ***Choose File to Import*** field.

NOTE
You can also type or paste the full file path into this field.

3. *(Optional)* Import radioserver database from the same file:

   a. Select the ***Import Radioserver Database*** check box to import the exported databases from the same file.

   b. In the ***Override Settings*** area, determine GUID restoration necessity:

If the current radioserver will work together with the one which settings are imported,	click ***Keep Server GUID***.
If the current radioserver completely replaces the previous radioserver or the current radioserver is a restored instance of the failed radioserver,	click ***All***.

4. Click the ***Import*** button, and then confirm the importing.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (***▷***)*** or ***Restart (***▣▷***)***.

12.4 Restoring Event Log Database

Follow the procedure to restore the SmartPTT Radioserver event log database from a backup.

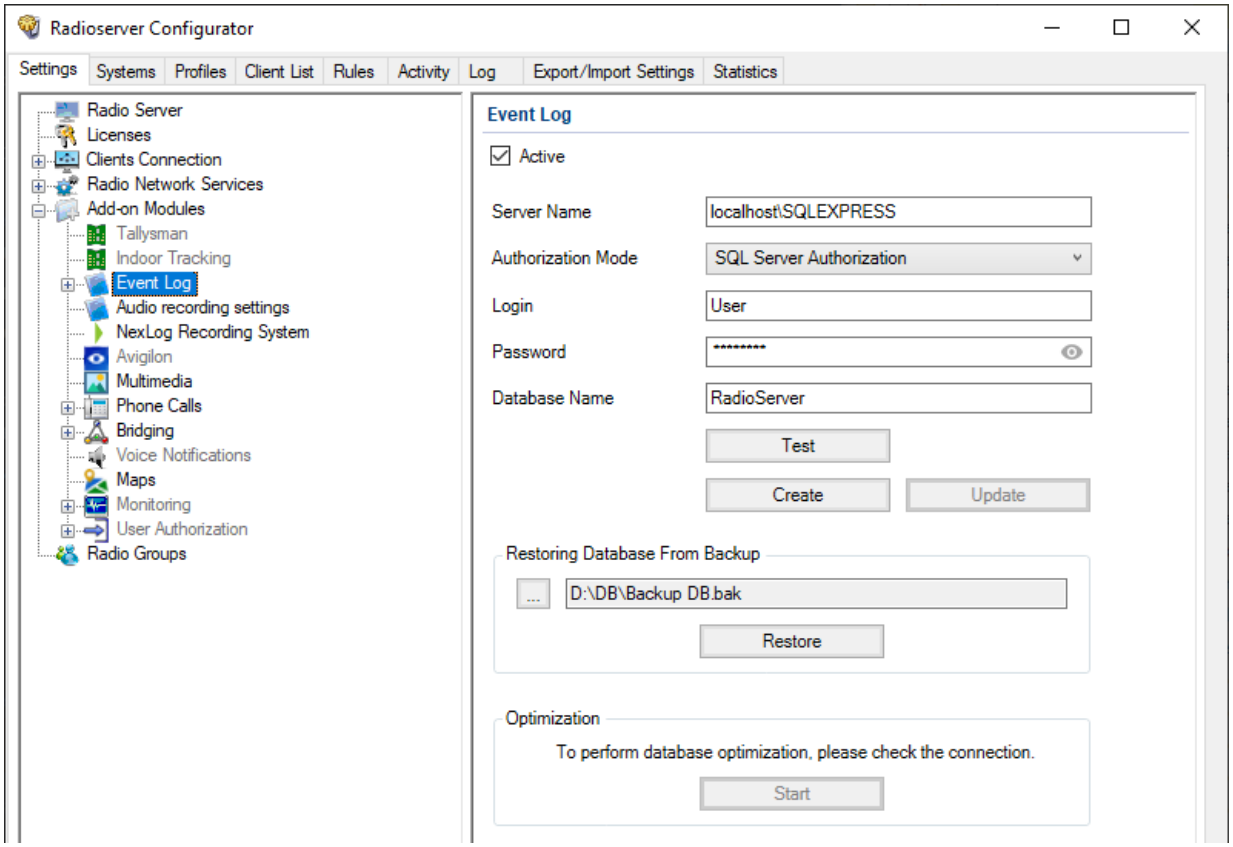
Important
If SQL Server was installed after SmartPTT, or if it is located on a remote computer, the database will not be available for configuration or use. Additionally, the database will be inaccessible if the user has created an account for database authorization instead of using Windows authentication.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *Database Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure that you have access to the desired backup file (.bak).

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand the ***Add-on Modules*** node, and then click ***Event Log***.
The database connection settings appear in the right pane.



3. In the ***Restoring Database From Backup*** area, specify the path to the backup file:
   a. Click the Browse ( ) button to the left of the text field.
   b. In the window that appears, select the file.
4. Click ***Restore***.
   A window with information if the database was restored appears.
5. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

12.5 Restoring Monitoring Database

Follow the procedure to restore the monitoring database from a backup.

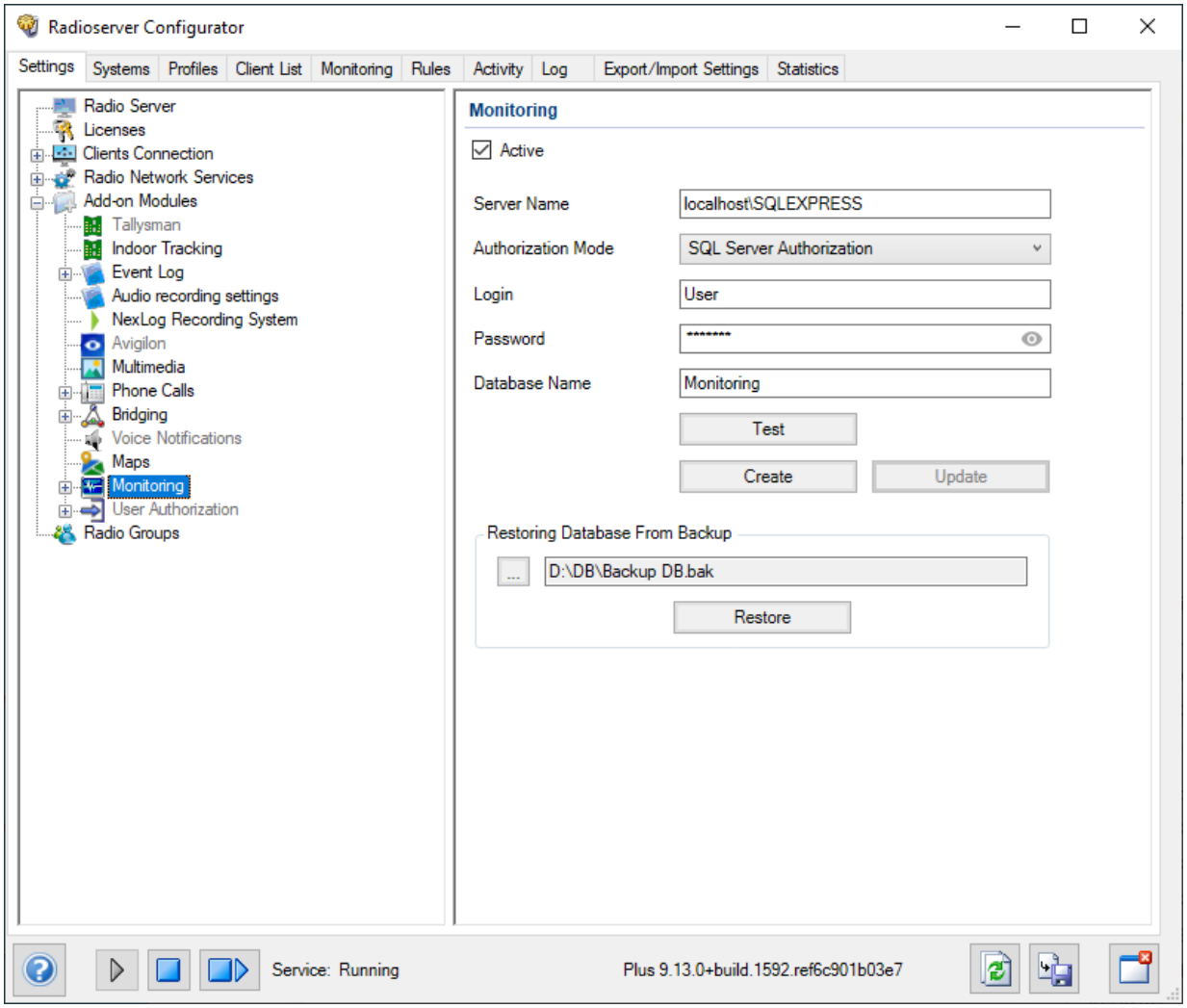
Important
If SQL Server was installed after SmartPTT, or if it is located on a remote computer, the database will not be available for configuration or use. Additionally, the database will be inaccessible if the user has created an account for database authorization instead of using Windows authentication.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *Database Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure that you have access to the desired backup file (.bak).

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand the ***Add-on Modules*** node, and then click ***Monitoring***.
   The database connection settings appear in the right pane.



3. In the ***Restoring Database From Backup*** area, specify the path to the backup file:
   a. Click Browse (...) to the left of the text field.
   b. In the window that appears, select the file.
4. Click ***Restore Database***.
   A window with information if the database was restored appears.
5. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start ( )*** or ***Restart ( )***.

12.6 Restoring User Database

Follow the procedure to restore the radio user database from a backup.

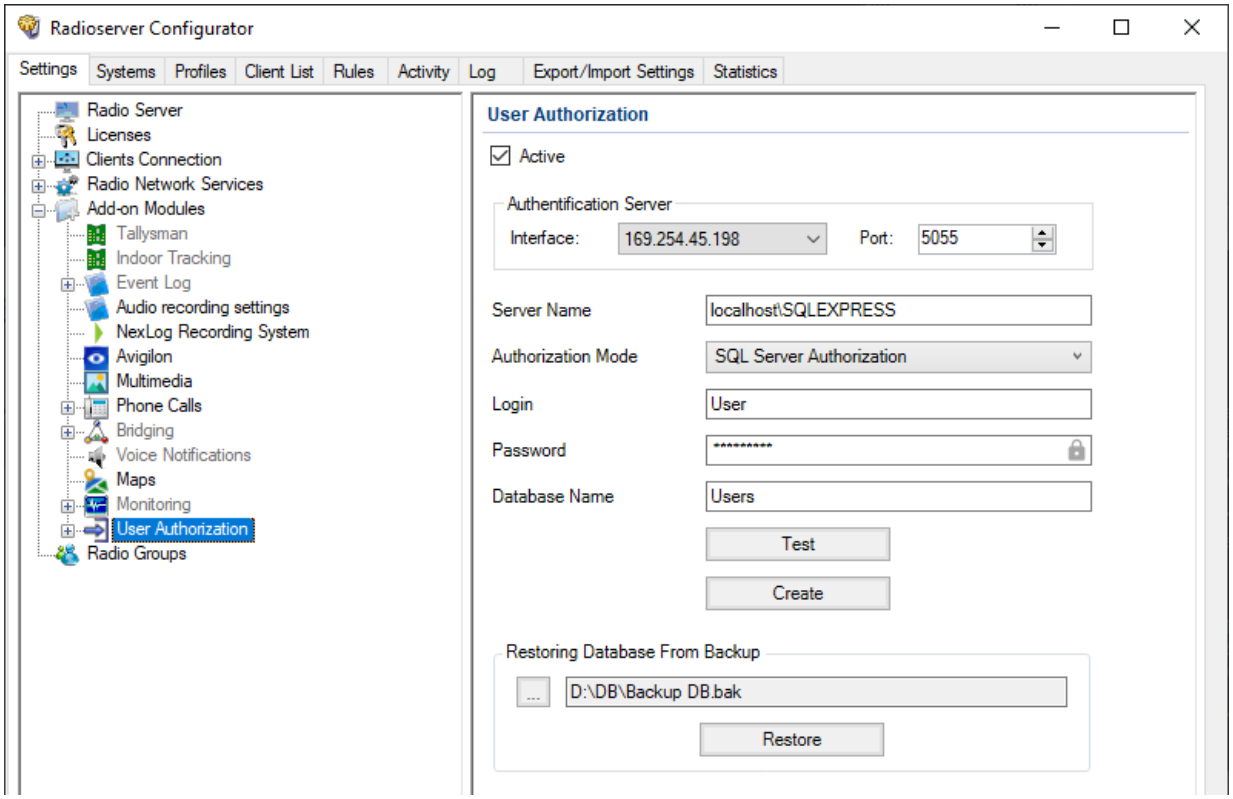
Important
If SQL Server was installed after SmartPTT, or if it is located on a remote computer, the database will not be available for configuration or use. Additionally, the database will be inaccessible if the user has created an account for database authorization instead of using Windows authentication.

Prerequisites:

- When using local or domain authentication, log in to SmartPTT Radioserver Configurator as a user from the *Database Administrators* group. For details, see Loging in to Radioserver Configurator.
- Ensure that you have access to the desired backup file (.bak).

Procedure:

1. In SmartPTT Radioserver Configurator, open the ***Settings*** tab.
2. In the left pane, expand the ***Add-on Modules*** node, and then click ***User Authorization***.
   The database connection settings appear in the right pane.



3. In the ***Restoring Database From Backup*** area, specify the path to the desired backup file:
   a. Click the Browse (...) button to the left of the text field.
   b. In the window that appears, select the desired file and click ***Open***.
4. Click ***Restore Database***.
   A window with information if the database was restored appears.
5. To save changes, at the bottom of the SmartPTT Radioserver Configurator window, click ***Save Configuration ( )***.

Postrequisites:

To apply changes immediately, at the bottom of the SmartPTT Radioserver Configurator window, click ***Start (*** ***)*** or ***Restart (*** ***)***.

13 Troubleshooting

The section provides description of typical problems you may encounter while installing and configuring SmartPTT software. It provides information on their possible reasons and ways of their resolving. If the suggested methods do not help to resolve your problem, contact SmartPTT Technical Support Center.

13.1 General Recommendations

Many problems related to the SmartPTT configuration and/or operation occur due to the incomplete infrastructure configuration. Such problems are usually appear as applications start failure.

To resolve such problems, the following recommendations must be followed:

- Always install drivers for sound cards, network cards, and other peripherals.
- Use compatible hardware and software.
- Always restart your computers after the operating system update installation and/or other software updates installation.

13.2 SmartPTT Installation Problems

If the installation of the SmartPTT software completed successfully, a message confirming successful installation appears. If the message does not appear, it means a problem occurred during the installation. It may occur for one of the following reasons:

- You logged on using a non-administrator account (standard or guest account).
- Microsoft .NET Framework is not installed on the computer.
- The components required for correct SmartPTT operation, such as MOTOTRBO Radio Driver or Microsoft SQL Server, were not installed.
- Installed Windows updates are not up-to-date or do not meet the system requirements.

To resolve installation-related problems, perform the following actions:

1. Log on as an Administrator.
2. Restart the installation of the SmartPTT software, and install all additional components offered by the installer:
   - If offered, agree to install Microsoft .NET Framework.
   - Install Microsoft SQL Server if it is not installed.

   For more information on the installation procedure, see SmartPTT Installation.
3. Ensure that Windows updates are up-to-date and meet the SmartPTT system requirements.
   For more information on Windows updates, see Microsoft Download Center and System Requirements.

13.3 SmartPTT Startup Problems

On successful launch of SmartPTT Dispatcher or SmartPTT Radioserver Configurator, the main window of the corresponding program opens automatically. If the window does not appear, the program did not launch because of a startup problem. It may occur for one of the following reasons:

- The computer was not restarted after the Microsoft .NET Framework installation.

- SmartPTT was installed to a folder other than ***Program Files*** on a computer with a 64-bit version of Windows.
- SmartPTT license period expired.
- Version of the installed Microsoft SQL Server does not correspond to the versions specified in Third Party Products.
- Multiple versions or multiple editions of Microsoft SQL Server are installed on the computer.
- SQL service is not running.

To resolve startup-related problems, check out the following measures:

- Restart your computer if it was not restarted after Microsoft .NET Framework installation.
  After restart, restart the installation, and then, in the ***Program Maintenance*** window, select ***Modify***. Follow the instructions provided by the SmartPTT installer.
- If SmartPTT was installed to a folder other than ***Program Files (x86)*** on a computer with a 64-bit version of Windows, uninstall it, and then reinstall to the ***Program Files (x86)*** folder.
- If SmartPTT license period expired, install a valid license. To order a license, contact the Elcomplus, Inc. representative in your region or SmartPTT Technical Support Center.
- Ensure that the Microsoft SQL Server version meets the system requirements.
- Ensure that only one version and edition of Microsoft SQL Server is installed on the computer (***Settings*** → ***Apps*** → ***Apps & features*** or ***Control Panel*** → ***Programs*** → ***Programs and Features***).
- Ensure that the SQL Server service is running (***Task Manager*** → ***Services***). If the service is not running, start it.

13.4 Web Console Connection Issues

At some configurations, users might be unable to launch Web Console (no loading screen appears). In particular, this occurs if Web Console and Server are behind the router. For example, this occurs when Operators access Web Console from the public network.

In the case, Customers need to contact their network administrators and check the fort forwarding configuration on the router. The following local ports of the Server computer shall be forwarded:

- WCF Port (default is 8888),
- HTTP Port (default is 8191),
- HTTPS Port (default is 8443),
- STUN Port (default is 3478),
- VoIP Port (default is 18500).

If the configuration above does not help, please submit a request to the Technical Support Center (support@smartptt.com).

13.5 Problems with Databases

A problem may occur when you connect the SmartPTT server or client to the database and in the course of further database-related activities in the SmartPTT system. It may occur for one of the following reasons:

- Version of the installed Microsoft SQL Server does not meet the requirements specified in Third Party Products.
- Multiple versions or multiple editions of Microsoft SQL Server are installed on the computer.

- The SQL Server service is not running.
- Incorrect SQL Server address in SmartPTT Radioserver Configurator.
- For the SQL authorization method, incorrect SQL user credentials.
- For systems connected to a remote database, the remote host is unavailable.

To resolve database-related problems, check out the recommendations below:

- Ensure that the Microsoft SQL Server version meets the system requirements.
- Ensure that only one version and edition of Microsoft SQL Server is installed on the computer (***Settings*** → ***Apps*** → ***Apps & features*** or ***Control Panel*** → ***Programs*** → ***Programs and Features***).
- Ensure that SQL Server service is running (***Task Manager*** → ***Services***). If the service is not running, start it.
- In SmartPTT Radioserver Configurator, specify the IP address of the computer on which SQL server is installed and running.
- For the SQL authorization method, specify correct SQL user credentials.
- Ensure that the remote host becomes available when using a remote database. For example, use the command *ping <host IP address>*.

13.6 Problem with Switching to Audio Node

The ASIO4ALL driver or a similar audio driver is installed on Windows. The selected audio playback device uses this audio driver. In SmartPTT Radioserver Configurator, in the control station settings, when you try to switch to the ***Audio*** node, Configurator suspends and audio playing from the device stops.

To solve the problem, perform the following actions on Windows:

1. Launch the Windows Devices and Printers program.
2. In the ***Devices*** section, for the desired audio playback device, open its properties window.
3. On the ***Advanced*** tab, clear the ***Give exclusive mode applications property*** check box.
4. Save the changes.

13.7 Audio Quality Issues

In some cases, subscribers may experience degraded audio quality for incoming voice calls from the operator. The sound may become "robotic", "metalized".

Root cause of those problems might be in audio devices configuration, repeater configuration, and conventions for use of microphones. Try the following solutions to resolve the problem.

Change Microphone Settings

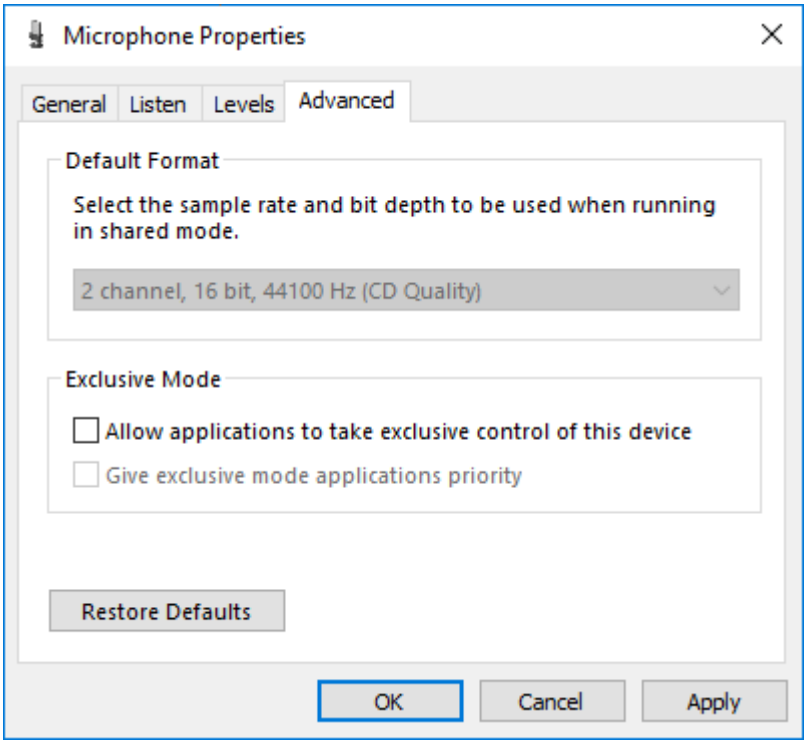
On the dispatcher's computer, change Windows sound settings:

1. In the Windows Control Panel, access sound settings:
   a. In the Control Panel, from the ***View by*** list, select ***Large icons*** or ***Small icons***.
   b. Click ***Sound***.
   The ***Sound*** window appears.

2. On the ***Recording*** tab, right click the input device (microphone) used in SmartPTT, and then click ***Properties***.
3. In the window that appears, on the ***Levels*** tab, adjust the ***Microphone Boost*** parameter by moving the slide bar.

To decrease the microphone sensitivity,	move the slider to the left.
To increase the microphone sensitivity,	move the slider to the right. The sound quality will be improved and the voice will sound clearer.

4. On the ***Advanced*** tab, clear the ***Allow applications to take exclusive control of this device*** check box.



5. Save the changes and close the properties window.
6. In the ***Sounds*** window, click ***OK***.

Change Repeater Settings

Audio quality degradation might occur due to the voice gain in repeaters. It is per-repeater option. To change it, perform the following actions:

1. Access repeater settings.
2. In the ***General Settings*** section, in the ***General*** area, decrease the value of the ***Repeater Gain*** parameter.
3. Save changes.

Adjust Distance to Microphone

Some microphones may have high audio sensitivity. If operators speak closely to such microphones, they send an overloaded voice to SmartPTT. Such voice may be poorly encoded.

To resolve the problem, increase the distance between the operator's mouth and microphone.

Additionally, install pop filters in front of microphones.

13.8 SmartPTT Mobile Using Problems

Problems may occur when using SmartPTT Mobile.

Insufficient sound volume

When using SmartPTT Mobile on iOS devices, such problem as insufficient sound volume of the incoming All Call and group calls may occur.

To eliminate the problem with the insufficient volume, in SmartPTT Radioserver Configurator, in the SmartPTT Radioserver settings, select the ***Automatic Gain Control*** check box to ajust the volume of incoming calls.

Unable to answer a call using a hardware PTT button

When using SmartPTT Mobile on a Sonim XP8800 device with Android, such problem as impossibility to answer a call during hangtime with a device screen turned off using the hardware PTT button may occur (if the device is in high priority mode).

To eliminate the problem, set the Hold timer parameter on the device to *Off* (this parameter is located in the programmable button settings of the device).

13.9 Export Issues

Sometimes you may experience issues when export SmartPTT configuration and database at once. That option is available in the ***Import/Export Settings*** tab of the SmartPTT Radioserver Configurator and described in Exporting SmartPTT Radioserver Settings.

If you have those issues, perform the following actions:

1. Ensure you stop SmartPTT Radioserver since you cannot export configuration and/or database while the service is running. For this, ensure that the “Stopped” text appears in the bottom part of the SmartPTT Radioserver Configurator.
2. Ensure SmartPTT Radioserver Configurator is connected to the event/activity log database.

To ensure if SmartPTT Radioserver is stopped, perform the following actions:

1. In SmartPTT Radioserver Configurator, check if the “Stopped” text appears in the bottom part of the SmartPTT Radioserver Configurator.
2. If “Running” appears, click ***Stop*** to stop the SmartPTT Radioserver.

To ensure the database connection, perform the following actions:

1. On the ***Settings*** tab, expand ***Add-on Modules***, and then click ***Event Log***.
3. In the right pane, click ***Check Connection***.
   The connection establishment notification appears.
4. Close the notification, and then repeat the exporting procedure. For details, see Exporting SmartPTT Radioserver Settings.

If you experience other issues, submit a request to the Technical Support Center.

13.10 Tracks Visualization Issues

At some configurations, Operators might be unable to visualize subscriber tracks on maps. In particular, this occurs when Operators use server-side database as data source.

Usually, the problem occurs if Desktop Console and Server are behind the router with respect to each other. In that case, Customers need to contact their network administrators and check the fort forwarding configuration on the router. The following local ports of the Server computer shall be forwarded:

- WCF Port (default is 8888),
- HTTP Port (default is 8191),
- HTTPS Port (default is 8443),
- STUN Port (default is 3478),
- VoIP Port (default is 18500).

If the configuration above does not help, please submit a request to the Technical Support Center (support@smartptt.com).

13.11 Reports Creation Issues

At some configurations, Operators might be unable to create reports when use Server database as a data source.

Usually, the problem occurs if Desktop Console connects to Server that is behind the router. In that case, Customers need to contact their network administrators and check the fort forwarding configuration on the router. The following local ports of the Server computer shall be forwarded:

- WCF Port (default is 8888),
- HTTP Port (default is 8191),
- HTTPS Port (default is 8443),
- STUN Port (default is 3478),
- VoIP Port (default is 18500).

If the configuration above does not help, please submit a request to the Technical Support Center (support@smartptt.com).

Contact Us

If you have a request or want to learn more about our solutions, please contact our sales managers via email sales@smartptt.com

Information about the product's features and settings is also available on the website smartptt.com/wiki/

Customer support is provided by SmartPTT Technical Support Center. You can contact a support engineer via email support@smartptt.com or by submitting a request on the official support website support.smartptt.com

You can find the full SmartPTT Terms of Technical Support on the official website smartptt.com

SmartPTT Technical Support Center does not consult on deployment and maintenance of Motorola Solutions products except on settings related to SmartPTT connection and data communication.

For technical support on Motorola Solutions products, please contact an authorized Motorola Solutions representative in your region.

To share your feedback on the product, documentation, and services, email us at feedback@smartptt.com

Web: smartptt.com
Email: info@smartptt.com
Tel.: +1-786-362-5525
Mailbox: 290 Northwest 165th St, # P-800A, Miami, FL, 33169, USA