



Version 9.2

# SmartPTT PLUS

## Radioserver Configurator User Guide

December 2017

# Contents

<b>1 Settings</b>	<b>6</b>
<b>1.1 Radio Server</b>	<b>7</b>
<b>1.2 Redundant Radio Server</b>	<b>9</b>
1.2.1 Adding Redundant Radio Server	10
1.2.2 Configuring Redundant Radio Server	11
1.2.3 Configuring the Correspondence Table	12
1.2.3.1 Configuring Values	13
1.2.3.2 Configuring Parameters	14
1.2.4 Displaying Redundant Radio Server in SmartPTT Dispatcher	15
<b>1.3 Licenses</b>	<b>16</b>
<b>1.4 Services</b>	<b>22</b>
1.4.1 ARS	22
1.4.2 GPS	25
1.4.3 TMS	27
1.4.4 Telemetry	28
1.4.5 Radio Blacklist	29
1.4.6 Email Gateway	38
1.4.6.1 Configuring Radioserver	40
Configuring Outgoing Messages Server	42
Configuring Incoming Messages Server	43
1.4.6.2 Sending Messages	46
Sending Messages to Radios	46
Sending Messages to Email Address	47
1.4.7 SMS Gateway	48
1.4.8 File Receive	55
<b>1.5 Add-on Modules</b>	<b>60</b>
1.5.1 Tallysman	60
1.5.2 Indoor Tracking	62
1.5.2.1 Configuring Indoor Tracking in MOTOTRBO CPS	65
1.5.2.2 Configuring Indoor Tracking	69
1.5.3 Event Log	71
1.5.3.1 Settings	85
1.5.3.2 Automatic Database Backup	87
1.5.4 Phone Calls	89
1.5.4.1 Telephone Interconnect	92

## Contents

---

1.5.5 Bridging	100
1.5.5.1 Multigroups	101
1.5.6 Voice Notifications	104
1.5.7 Clients Connection	106
1.5.7.1 Web Service	106
1.5.7.2 Third-Party Applications	107
1.5.8 Monitoring	108
1.5.8.1 Settings	123
1.5.8.2 Automatic Database Backup	124
1.5.8.3 SNMP Service	125
1.5.9 User Authorization	128
1.5.9.1 Users	145
1.5.9.2 Automatic Database Backup	149
<b>1.6 Profiles</b>	<b>152</b>
<b>1.7 Radio Groups</b>	<b>156</b>
<b>1.8 Metadata</b>	<b>158</b>
1.8.1 Radios	172
1.8.2 Automatic Database Backup	173
<b>2 Networks</b>	<b>175</b>
<b>2.1 Control Stations</b>	<b>175</b>
2.1.1 Configuring Channels	185
2.1.2 Configuring Talkgroups	186
2.1.3 Configuring Audio Settings	187
<b>2.2 Connect Plus</b>	<b>188</b>
2.2.1 Configuring Connect Plus	189
2.2.2 XRC Controller	191
2.2.2.1 Configuring Joint GPS and Indoor Data	193
Configuring Radio in MOTOTRBO CPS	194
Configuring Radio in SmartPTT Dispatcher	194
Configuring Repeater in MOTOTRBO CPS	194
2.2.3 XRT Gateway	194
2.2.4 Security Settings	197
<b>2.3 NAI Systems</b>	<b>205</b>
2.3.1 Adding and Configuring NAI Systems	207
2.3.2 Adding and Configuring NAI Control Stations	215
2.3.2.1 Audio Settings	220
2.3.3 Configuring NAI Slots	221

## Contents

---

2.3.3.1 Configuring Local Slots	224
2.3.3.2 Configuring Joint GPS and Indoor Data	226
Configuring Radio in MOTOTRBO CPS	226
Configuring Radio in SmartPTT Dispatcher	227
Configuring Repeater in MOTOTRBO CPS	227
2.3.3.3 Configuring Data Transmitting on CSBK/Enhanced CSBK channel	227
2.3.4 Configuring NAI Talkgroups	229
2.3.5 DDMS Service	233
2.3.5.1 Configuring DDMS in MOTOTRBO DDMS	234
2.3.5.2 Configuring DDMS in SmartPTT Radioserver Configurator	235
2.3.6 MNIS Data Gateway	236
2.3.6.1 Configuring MNIS in MOTOTRBO Network Interface Service Configuration Utility	238
2.3.6.2 Configuring MNIS Data Gateway for Local Socket	240
2.3.6.3 Configuring MNIS Data Gateway for Remote Socket	241
Configuring MNIS Data Gateway Relay	241
Configuring Radio Server	242
2.3.7 Security Settings	243
<b>2.4 Capacity Max</b>	<b>253</b>
2.4.1 Configuring Capacity Max	255
2.4.1.1 Configuring Joint GPS and Indoor Data	259
Configuring Capacity Max in Radio Management	259
Configuring Repeater in Radio Management	260
Configuring Radio in Radio Management	260
Configuring Radio in SmartPTT Dispatcher	261
2.4.2 Configuring Trunk Controller	261
2.4.3 Configuring MNIS Data Gateway	267
2.4.4 Configuring MNIS VRC Gateway	274
2.4.5 Adding Console in Radio Management	277
2.4.6 Configuring Talkgroups	279
2.4.7 Security Settings	280
<b>2.5 SIP/RTP Interfaces</b>	<b>290</b>
2.5.1 SIP/RTP Gateway	292
<b>3 Client List</b>	<b>293</b>
<b>4 Network Configuration</b>	<b>295</b>
<b>5 Rules</b>	<b>303</b>
<b>5.1 Adding Rule for Events on Radios</b>	<b>303</b>
<b>5.2 Adding Rule for Events on Dispatcher</b>	<b>306</b>



## Contents

---

<b>5.3 Modifying Rule</b>	<b>308</b>
<b>5.4 Deleting Rule</b>	<b>309</b>
<b>6 Activity</b>	<b>311</b>
<b>7 Log</b>	<b>313</b>
<b>8 Export/Import Settings</b>	<b>314</b>
<b>9 Statistics</b>	<b>316</b>

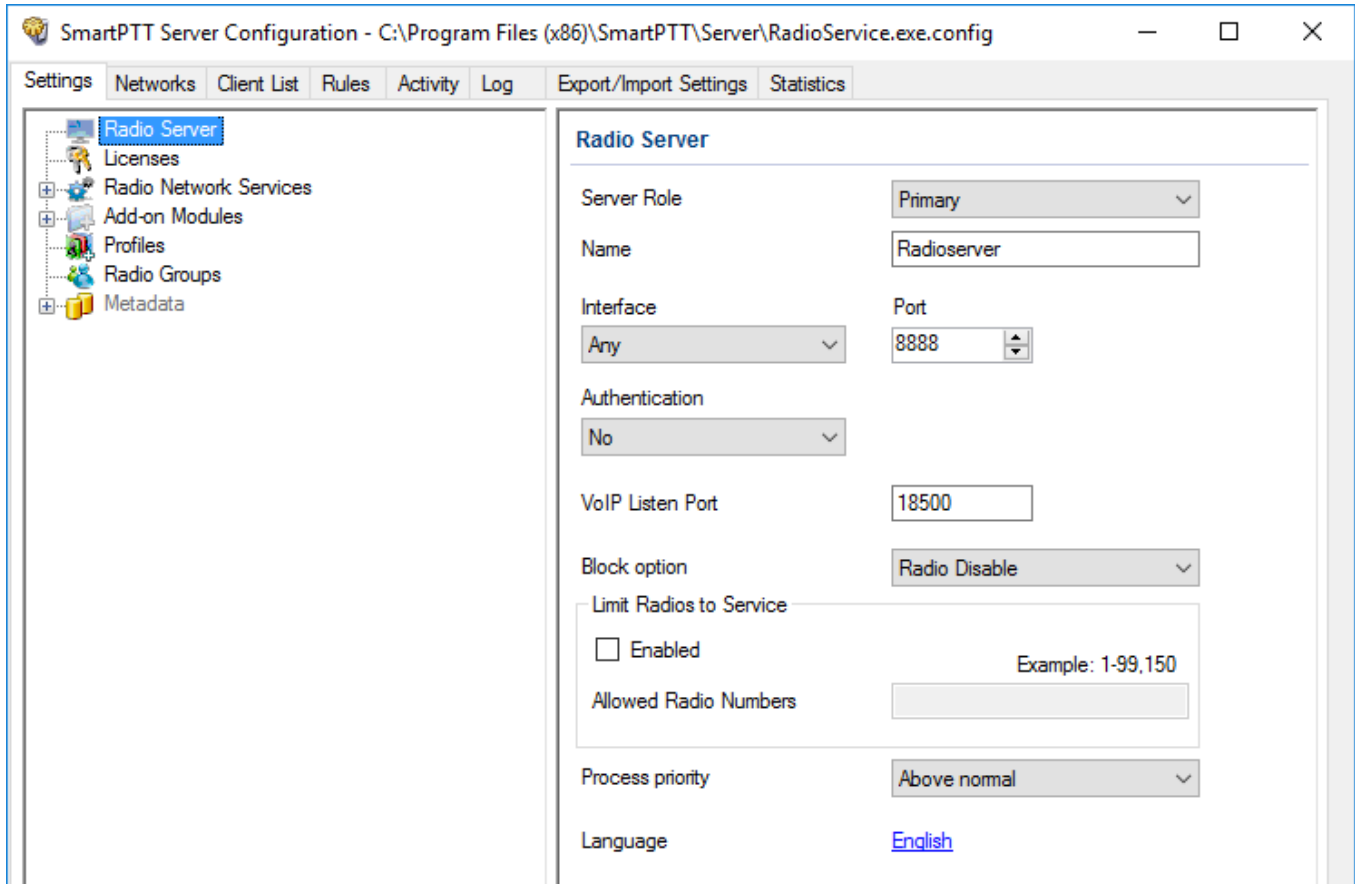
# 1 Settings

In this tab you can configure the general settings of SmartPTT Radioserver:

- [Radioserver](#)
- [Licenses](#)
- Radio network services
- Add-on Modules
- [Profiles](#)
- [Radio groups](#)
- [Metadata](#)

## 1.1 Radio Server

To set up the radioserver, click **Radio Server** in the left list of the *SmartPTT Radioserver Configurator* window. The **Radio Server** window appears:




**Server Role:** Sets the radioserver role (*Primary* or *Redundant*). Primary radioserver can have only one redundant radioserver and vice versa. To configure the redundant radioserver settings, see the Redundant Radio Server section.

**Name:** Radioserver alias. You cannot type more than 20 characters into this field.

**Interface** and **Port:** Radioserver IP address, i.e. the IP address of the PC where the radioserver is installed. Default port is 8888.

### NOTE

If the specified port is occupied, you will see the warning icon  next to the input field. Hover the mouse over the icon to see where the port is being used.

**Authentication:** Authentication parameters required for connection to the radioserver. Select *No* to set anonymous authentication. Select *Windows* to set Windows authentication.

**NOTE**

If *Windows* is selected, to connect, the dispatcher must use the user name and password of the account where the radioserver service was started.

**VoIP Listen Port:** Number of a UDP port for receiving voice data from the dispatcher.

**Block option:** Allows selecting the way of blocking the radio. When *Radio Disable* is applied, radioserver sends the *Radio Disable* command to block the radio. The *Deny Channel* option denies the radio to work on the given channel.!

**NOTE**

The Deny Channel option is applicable only to IP Site Connect (direct IP connection) or NAI based configurations.

**NOTE**

When the *Block Radio* command is sent from one radio to another, the radio will be blocked, even if *Deny Channel* is selected.

**Limit Radios to Service:** Allows to manage the number of radios allowed in the network. Here you can specify which radios are to be controlled by the system and which are not.

**Enabled:** Select to make this functionality active.





**Allowed Radio Numbers:** Enter IDs of radios which can be managed from a dispatch console.




**WARNING**

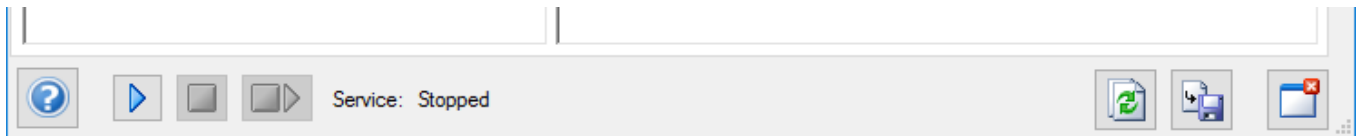
Dispatcher cannot connect radios whose IDs are not specified.

**Process priority:** Allows selecting the priority that the system associates with a process. By setting this parameter you can speed up or slow down SmartPTT performance. The highest possible priority is *Real time*. Use it wisely, because it may cause malfunctioning of the whole system. We recommend to use the *Normal* priority.

**Language:** Allows selecting languages of the user interface of the *SmartPTT Radioserver Configurator* program.

You can save changes made by clicking **Save** . If you want to cancel changes made, click **Restore** . All the changes made after the last save will be restored. To exit *SmartPTT Radioserver Configurator*, click **Close** . To view help, click **Help** .

The radioserver is implemented as Windows service SmartPTT Radio Service. To enable saved changes you must restart the service. Service is managed using the following buttons: **Start, Stop and Restart** , , .



## 1.2 Redundant Radio Server

Redundant radioserver is activated in case of primary server breakdown. Switching between the servers is made automatically, however, the redundant server is activated only if the last connection to the primary server was no later than 31 days ago.

### NOTE

To activate redundant radioserver, install the corresponding license. For more information on how to install licenses, see [Licenses](#).

Before configuring redundant radioserver, ensure all parameters of the primary server are configured properly. If the parameters are changed, save the changes and restart the primary server.

Values and parameters of primary and redundant servers must not be the same. You need to set new parameters for redundant radioserver. The primary radioserver settings are copied to the redundant server in accordance with the parameters set in the [Correspondence table](#).

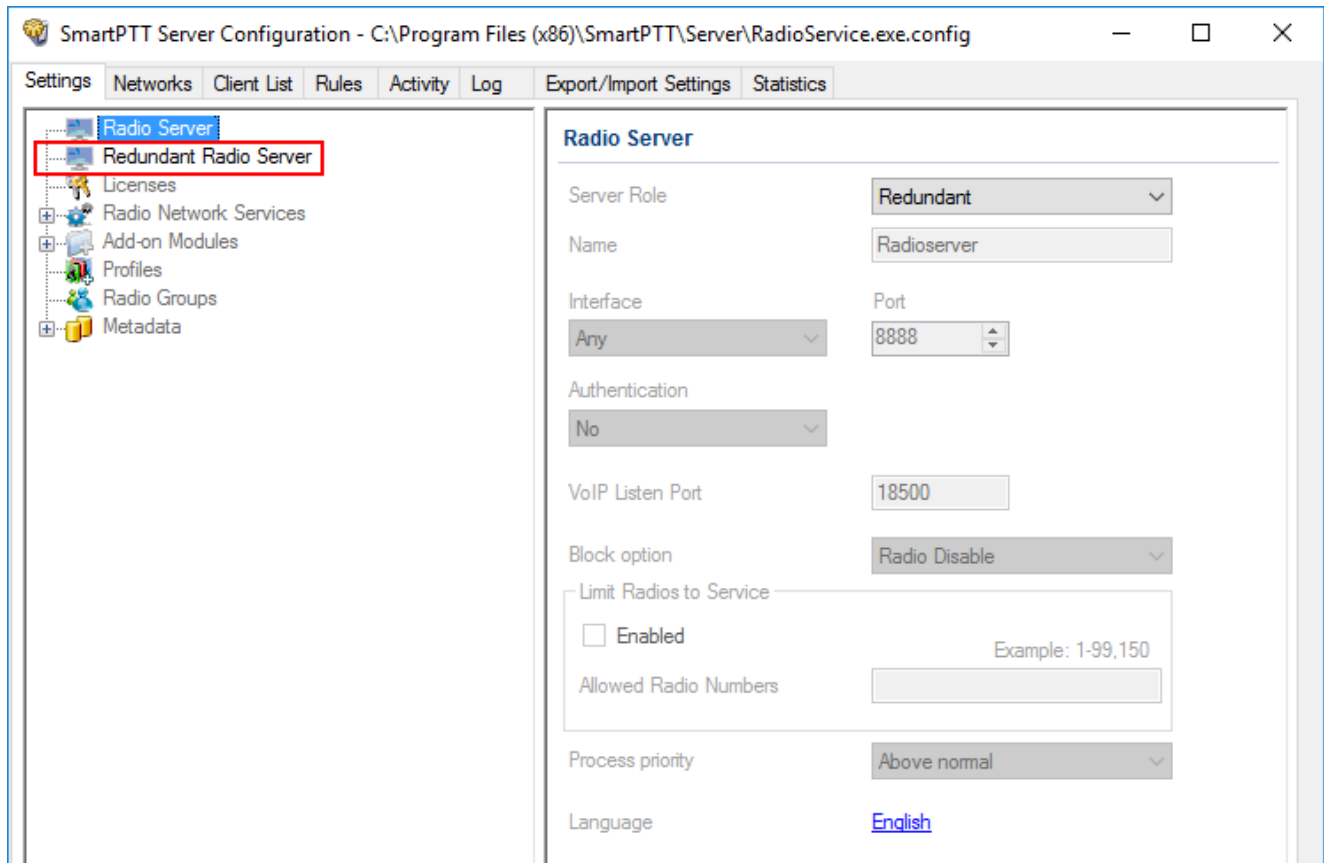
If the primary server parameters were changed after the redundant radioserver start, you need to update the [Correspondence table](#).

In the [Network Configuration](#) tab you can set up automatic radioserver redundancy error notifications.

## 1.2.1 Adding Redundant Radio Server

To add a redundant radioserver in SmartPTT Radioserver Configurator, follow these steps:

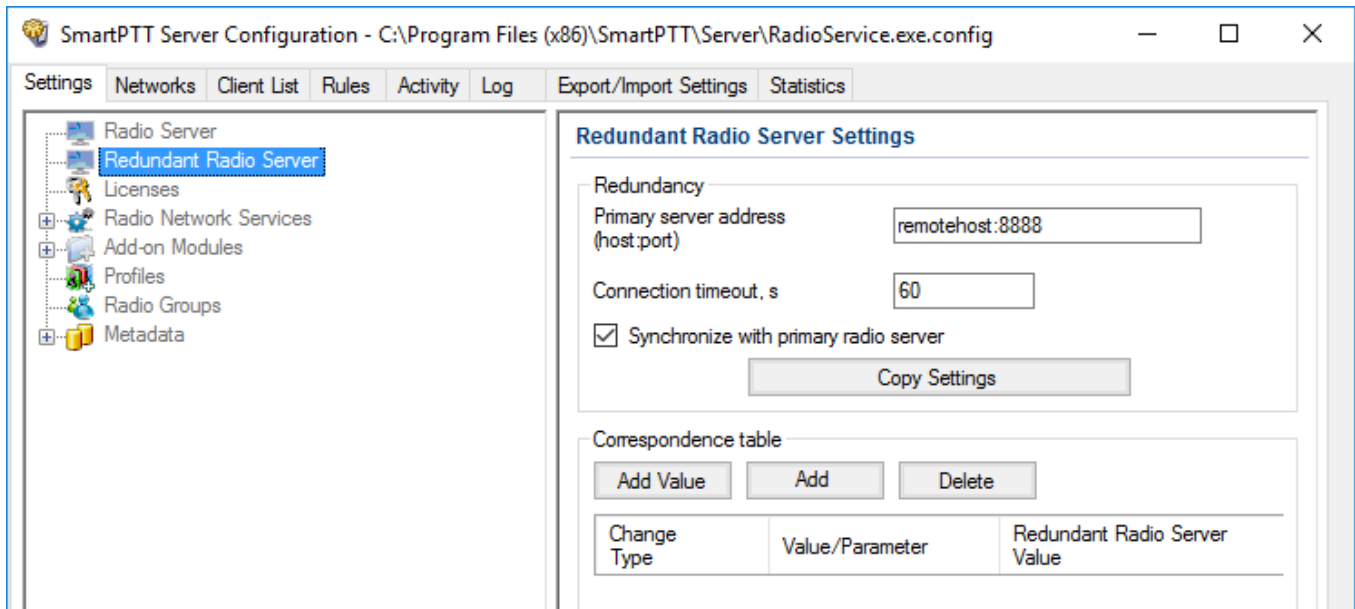
1. In the left pane of the **Settings** tab, click **Radio Server**.
2. In the **Radio Server** pane, from the **Server Role** list, select *Redundant*. In the left pane the **Redundant Radio Server** node appears.



## 1.2.2 Configuring Redundant Radio Server

To configure the redundant radio server in SmartPTT Radioserver Configurator, follow these steps:

1. In the left pane of the **Settings** tab, click **Redundant Radio Server**.



2. In the **Redundant Radio Server Settings** window, perform the following actions:
  - a. In the **Primary server address (host: port)** field, enter the primary radioserver IP address and port.
  - b. *Optional:* In the **Connection timeout (s)** field, enter time interval after which the redundant server becomes activate (starting from the primary server shutdown). The minimum value is 20 seconds.
  - c. Click **Copy Settings** to copy primary radioserver settings to the redundant server.
  - d. Select the **Synchronize with primary radio server** check box to activate the automatic synchronization of redundant server with primary server after the primary server restart.

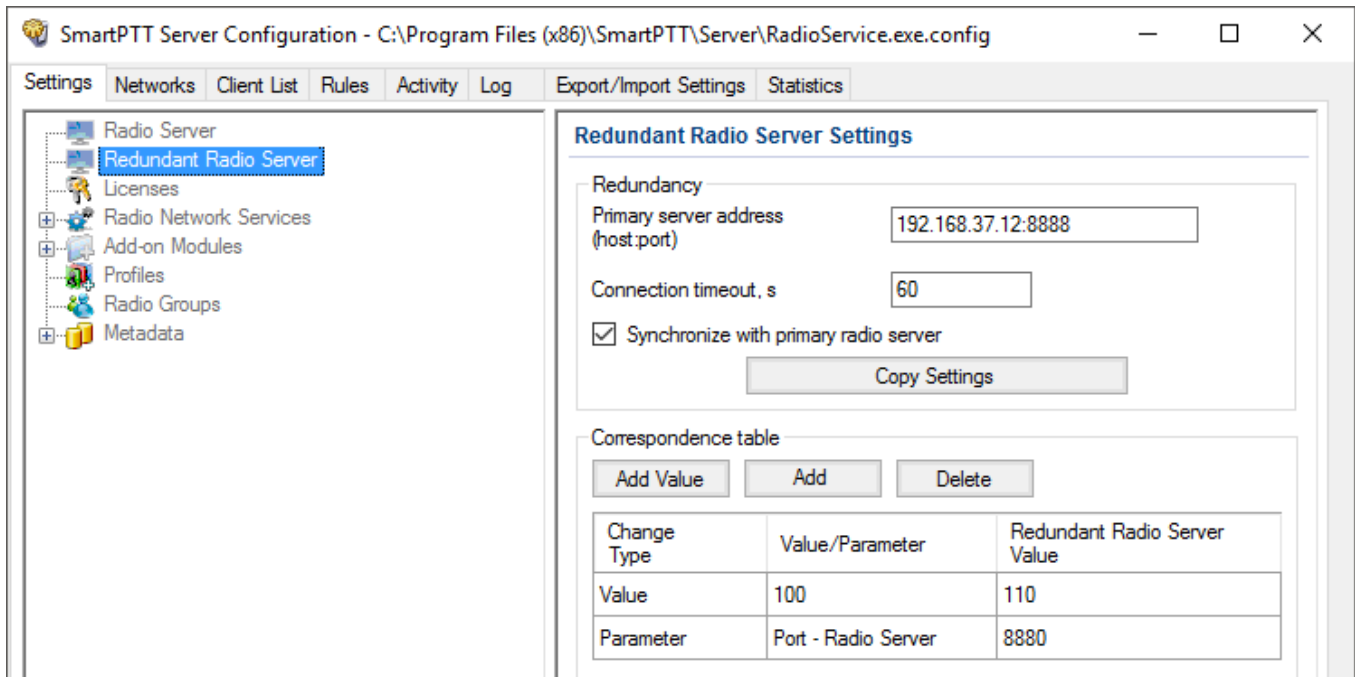
### NOTE



When the **Synchronize with primary server** check box is selected, only the **Activity**, **Export/Import Settings** and **Statistics** tabs are available for editing.

3. Configure the **Correspondence Table**. For more information on how to configure the table, see [Configuring the Correspondence Table](#).

## 1.2.3 Configuring the Correspondence Table

To configure the **Correspondence table** for the redundant radioserver, follow these steps:



1. Ensure the **Synchronize with primary radio server** check box in the **Redundancy** area is selected.
2. Set or edit the existing values or parameters for changing. To do it, see [Configuring Values](#) and [Configuring Parameters](#).
3. After setting values and parameters, click **Save**  to save changes.
4. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.



### 1.2.3.1 Configuring Values

To configure values for changing, in the **Correspondence table**, perform the following actions:

1. Click **Add Value**.
2. In the **Value/Parameter** field, type the value for changing.
3. In the **Redundant Radio Server Value** field, enter a new value for the redundant radioserver.

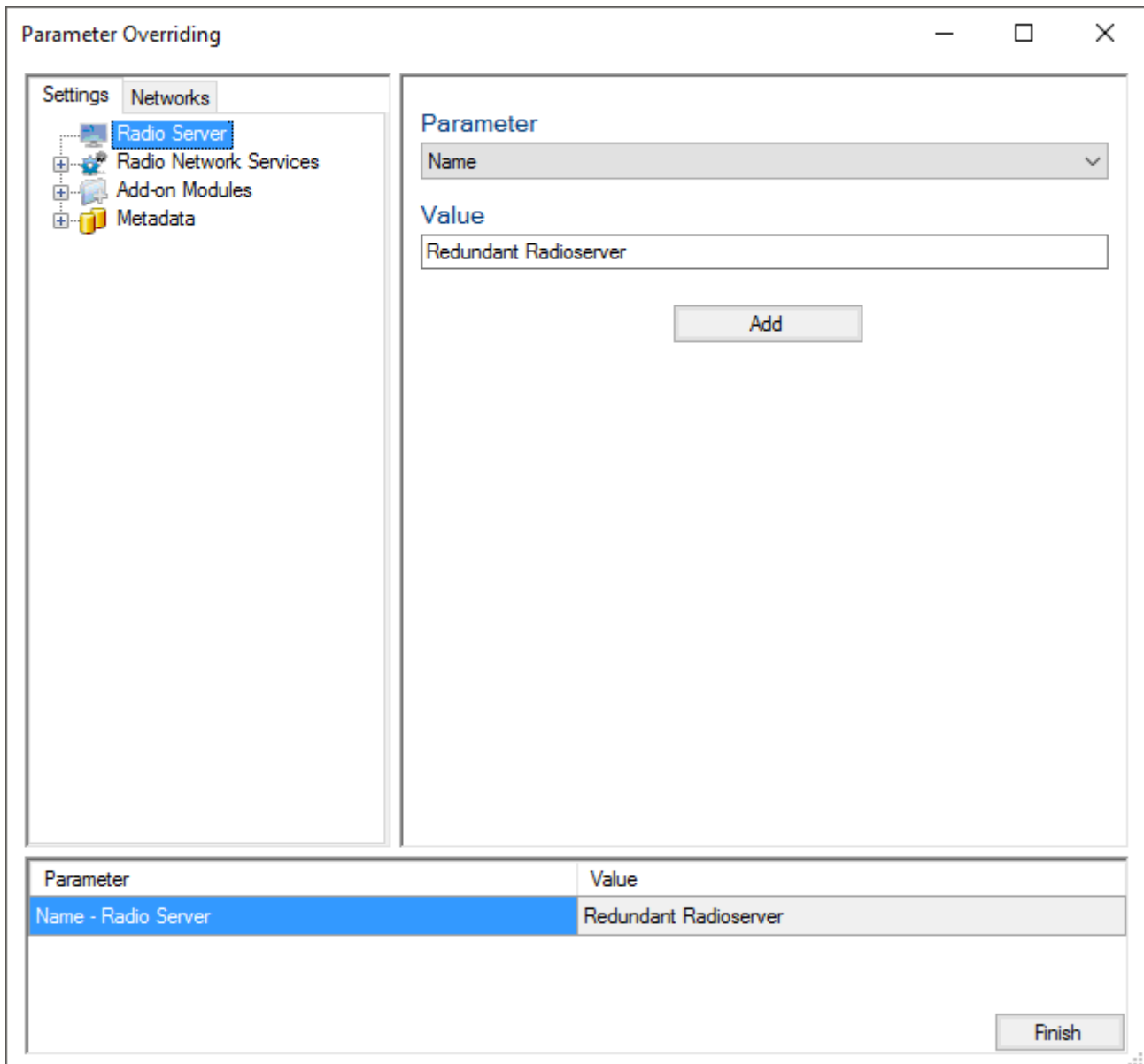
#### **WARNING**

The value in the **Correspondence table** changes all similar values copied from the primary server parameters.

### 1.2.3.2 Configuring Parameters

To configure parameters for changing, in the **Correspondence table**, perform the following actions:

1. Click **Add**.
2. In the open **Parameter Overriding** window, in the setting tree of the **Settings** or **Networks** tab, select the required node.



**NOTE**

The structure of the **Settings** and **Networks** tabs corresponds to the structure of the same SmartPTT Radioserver Configurator tabs.

3. From the **Parameter** list, select the required parameter.
  - For NAI - IP Site Connect, NAI - Capacity Plus and NAI - Linked Capacity Plus network topologies replace **Peer ID** parameters values.
  - *Optional*: IP-addresses.
  - *Optional*: Databases names.
4. In the **Value** area, enter the value, select the value from the list or select/clear the check box.
5. To add the parameter to the **Correspondence table**, click **Add**.
6. After adding all desired parameters, click **Finish**.

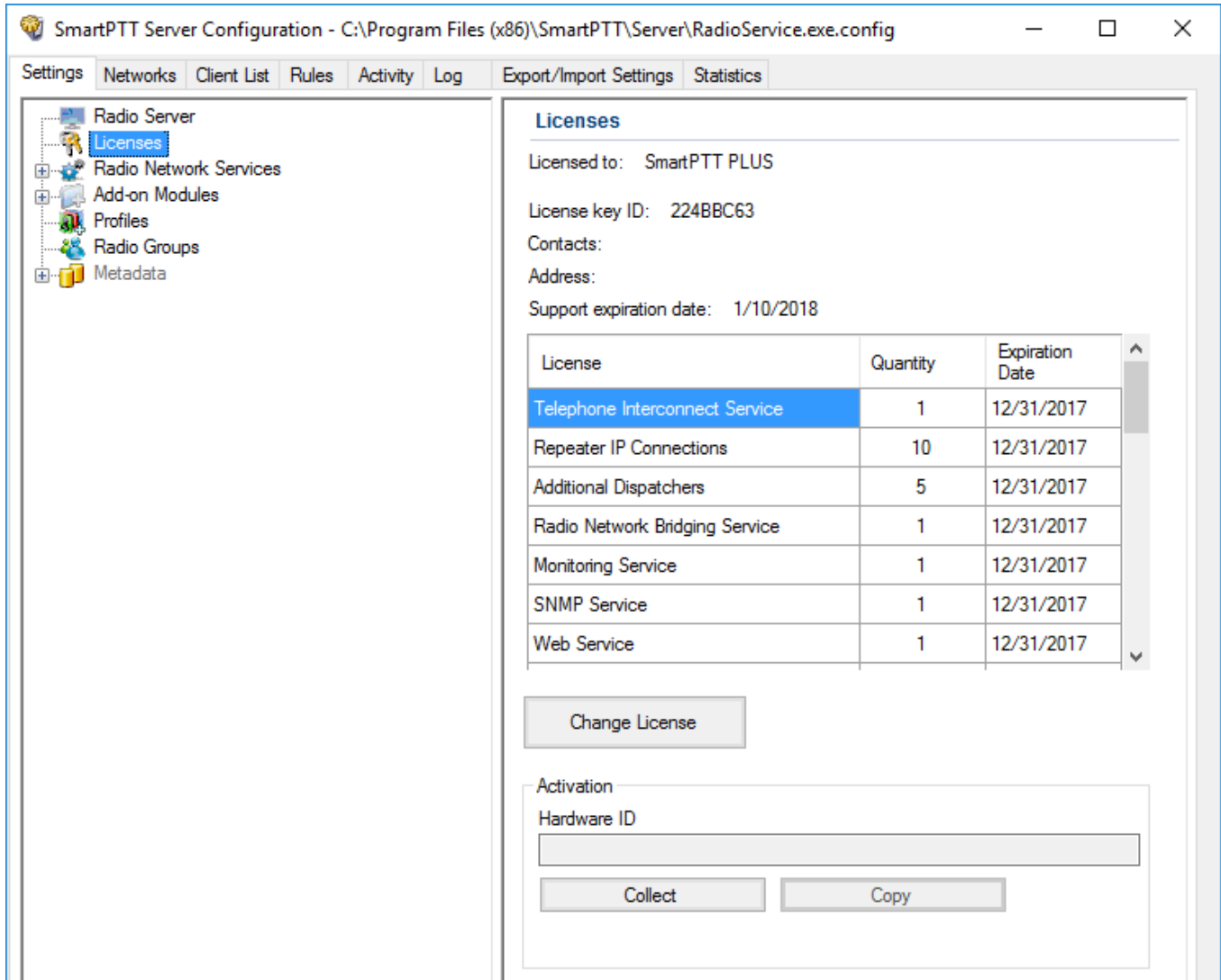
## 1.2.4 Displaying Redundant Radio Server in SmartPTT Dispatcher

To display the redundant server in SmartPTT Dispatcher, follow these steps:

1. Verify the redundant and primary radioservers are running and configured properly.
2. Add both radioservers into the dispatch console (**Settings** → **Radioservers**) and make them active.
3. Check that you can see both radioservers online in the **Radio Fleet** panel of *SmartPTT Dispatcher*.

## 1.3 Licenses

In the **Licenses** menu you can see the services which are available to you in SmartPTT and install a new license if needed.



Availability of the services is regulated by the license file. It contains licenses – permissions to use the particular number of particular services. They'll be Those licenses are being called here as services.

At the fresh start, SmartPTT generates demo license file which works for a small period of time. You cannot extent its activity period and you should obtain a regular license file.

Regular license file binds to the hardware of the primary radioserver PC or redundant radioserver PC. Hardware ID (HID) is required for the binding.

To obtain hardware ID via *SmartPTT Radioserver Configurator*:

1. Run *SmartPTT Radioserver Configurator*.
2. In the **Settings** tab click **Licenses**.
3. Click the **Collect** button in the **Activation** area of the **Licenses** window. The code which appears in the **Hardware ID** field is the hardware ID.
4. Click **Copy** to copy the hardware ID to the clipboard.

To obtain hardware ID without *SmartPTT Radioserver Configurator*, please, refer to the [following article](#) on the SmartPTT Technical Support Center website.

When you get the license file, you should install it.

To install a license file, follow these steps:

1. Run *SmartPTT Radioserver Configurator*.
2. In the **Settings** tab click **Licenses**.
3. Click **Change License**.
4. Open the received license file. The **License Installation** window appears:

Установка лицензии

Правом на лицензию обладает: SmartPTT Customer Name  
Идентификатор лицензионного ключа: 1BE7813E  
Дата окончания подписки на обновления: 12/31/2017  
Контакты:  
Адрес:

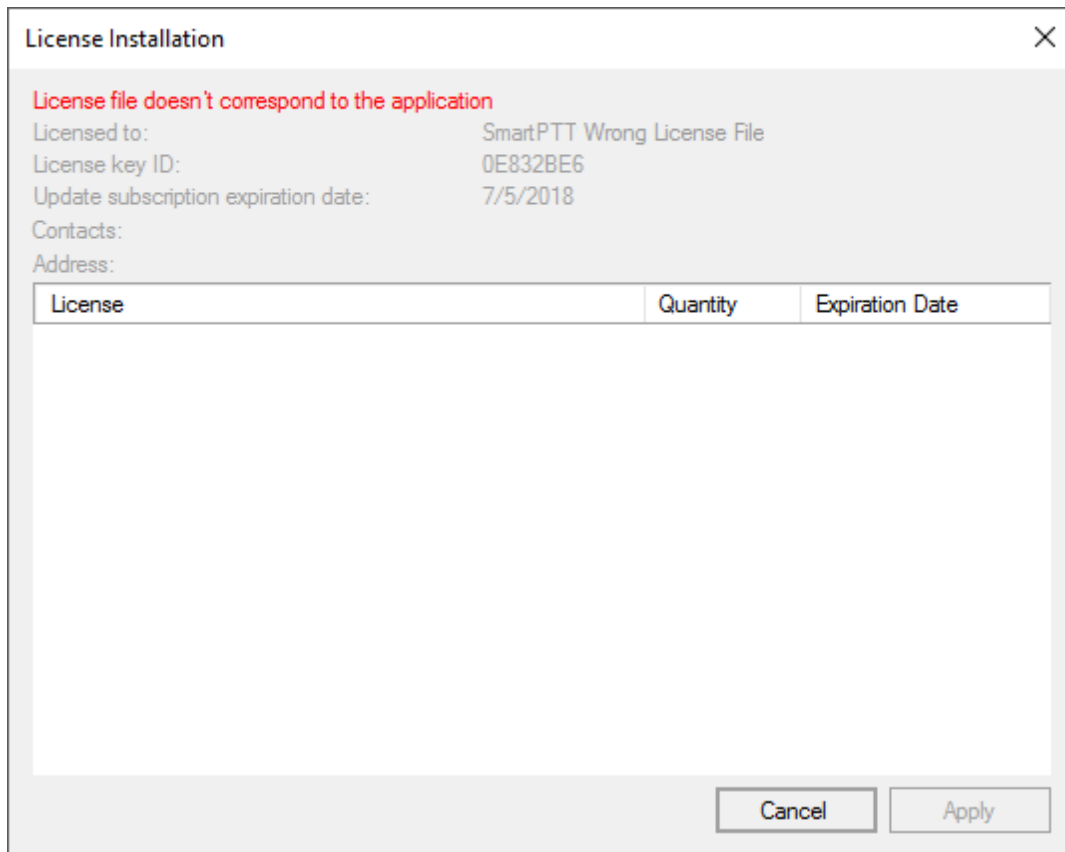
Лицензия	Кол-во	Действительно до
Веб-сервис	1	12/31/2017
Поддержка Indoor-позиционирования	1	12/31/2017
Поддержка голоса Connect Plus	2	12/31/2017
Поддержка данных Connect Plus	2	12/31/2017
Поддержка голоса NAI IPSC	10	12/31/2017
Поддержка голоса NAI Capacity Plus	10	12/31/2017
Поддержка голоса NAI LCP	10	12/31/2017
Поддержка GPS	1	12/31/2017
Поддержка аудиозаписи	1	12/31/2017
Поддержка данных NAI IPSC	10	12/31/2017



Отмена Применить

5. Check the information in the **License Installation** window. Pay attention to the table to check if you have all the services you need.

**NOTE**

If the license does not match the product or the hardware, **Licensed to** text will be red and the services table will be empty.



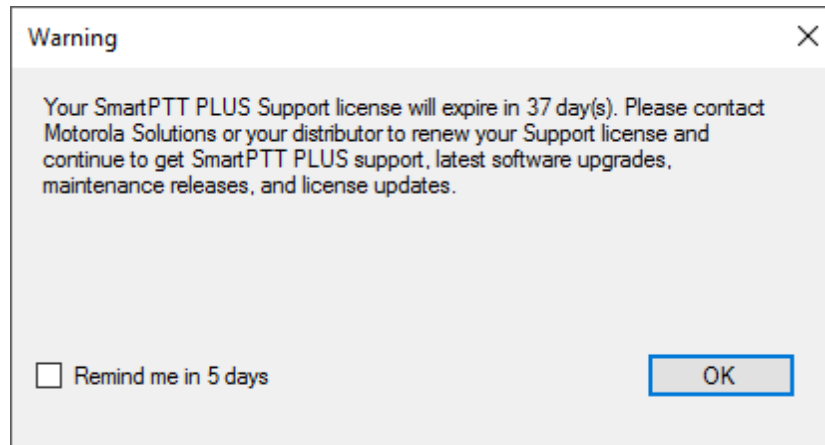
6. To accept the license click **Apply**. To cancel the license installation click **Cancel**.
7. Click **OK** in the notification window.
8. Click **Save**  to save changes.
9. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

After the license installation in the **Licenses** window the available services will appear as they were in the **License Installation** window.

Different services may have different expiration date. When the service is expired, it will be written red in the table.

When the expiration data approaches, you will start to get notifications at the start of *SmartPTT Radioserver Configurator*:

You can select the **Remind me in 5 days** check box to remind about the license updating in 5 days.





In addition, yellow triangle will appear near the dates, notifying about the approaching of the expiration date.

SmartPTT Server Configuration - C:\Program Files (x86)\SmartPTT\Server\RadioService.exe.config

Settings Networks Client List Rules Activity Log Export/Import Settings Statistics

Radio Server  
Licenses  
Radio Network Services  
Add-on Modules  
Profiles  
Radio Groups  
Metadata

### Licenses

Licensed to: SmartPTT Customer Name  
License key ID: 1BE7813E  
Contacts:  
Address:  
Support expiration date: 12/31/2017 ⚠

License	Quantity	Expiration Date
Telephone Interconnect Service	1	12/31/2017
Repeater IP Connections	15	12/31/2017
Additional Dispatchers	10	12/31/2017
Radio Network Bridging Service	1	12/31/2017
Monitoring Service	1	12/31/2017
SNMP Service	1	12/31/2017
Web Service	1	12/31/2017

Change License

Activation  
Hardware ID  
Collect Copy

Service: Stopped ⚠ PLUS 9.2.0.0

You cannot update or upgrade to SmartPTT released later of the expiration date of annual support. Nevertheless, your current software will continue to operate without any limitations until the licensed services are not expired. You could also be provided with the limited technical support for SmartPTT.

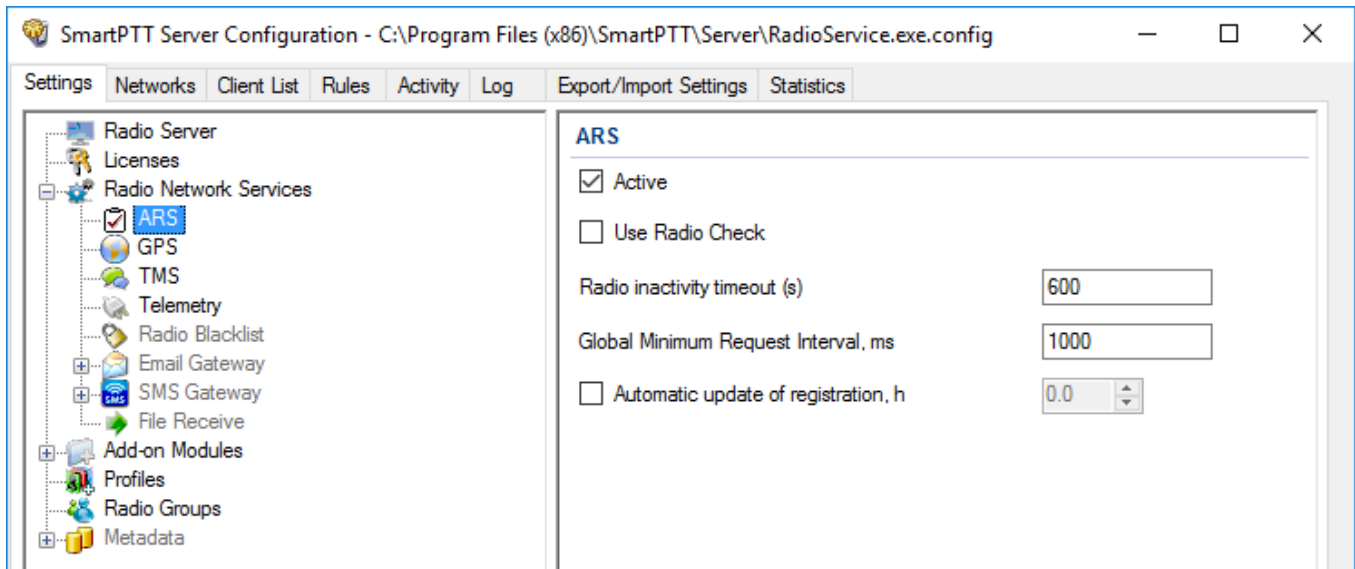
To use the newest version of SmartPTT with all new features, please, renew the annual support.

## 1.4 Services

### 1.4.1 ARS

ARS or registration service provides information on the availability of radios in the radio network.

To set up the registration service parameters, click **ARS** in the list in the left area of the SmartPTT Radioserver Configurator window. A new pane appears on the right:



**Active:** Select to enable the service.

**Use Radio Check:** This setting defines the mechanism used for checking radio presence in the network. If selected, the system uses the **Radio Check** command. This option was implemented for radios that do not support ARS.

**Radio Inactivity Timeout, s:** Time period, after which the radio that did not display any activity becomes potentially absent. In this case the system includes this radio into a special presence check process.

#### NOTE

Radio activity includes the following events: GPS location, telemetry signal, text message or voice call.

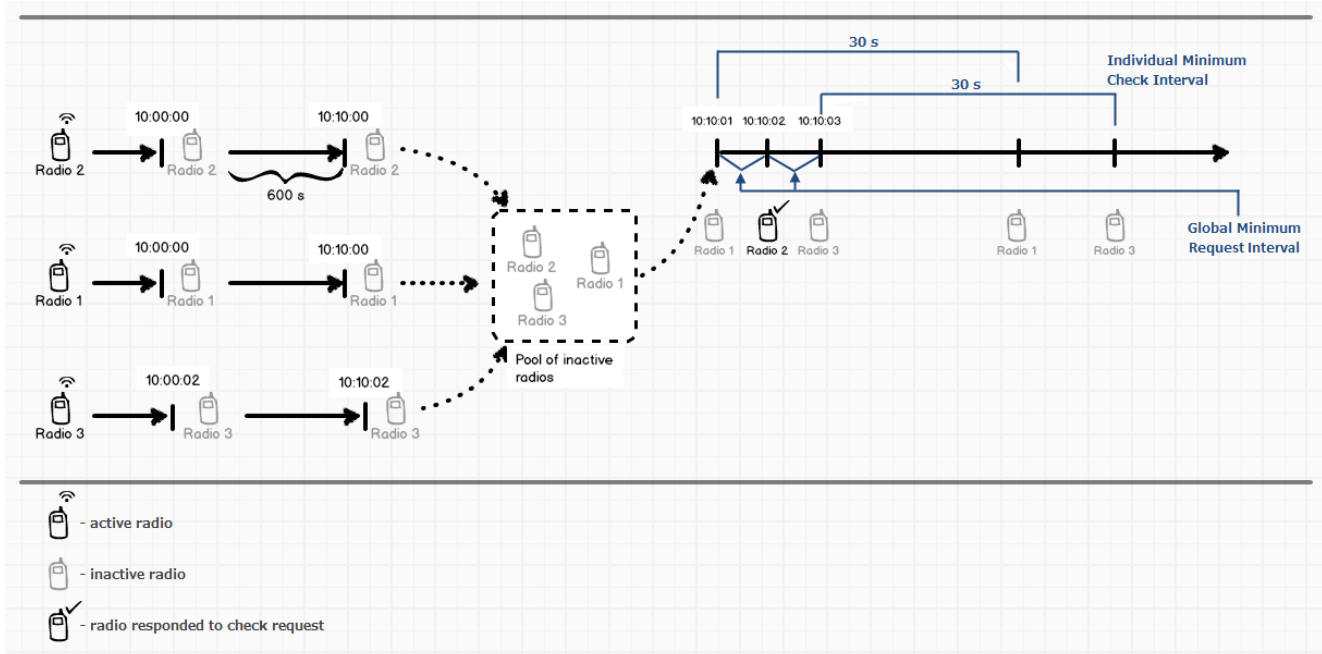
Generally, a radio can be sent 5 presence check requests successively with a 30-second interval. This parameter is called Individual Minimum Check Interval and equals to 30 s; it can't be changed in *SmartPTT Radioserver Configurator*. This parameter sets the interval between presence check requests sent to one radio. Therefore, it can be increased depending on the number of radios to

check. If the radio does not respond to the presence check requests and does not display any activity, it will acquire the Offline status after the 5th unsuccessful presence check request.

**Global Minimum Request Interval, ms:** Sets the minimum interval between presence check requests sent to all inactive radios in all networks. Instead of sending presence check requests to all inactive radios at one time, the system puts them on a queue and sends one presence check request to one radio at a time with the interval set in the Global Minimum Request Interval field. This method allows us to eliminate the risk of sending too many presence check requests at one time, thus removing traffic overload on the channel and spreading network load evenly.

### Example

There are three radios active till 10:00:00 and 10:00:02 (see figure below). Then, for the following 600s they do not display any activity. So, the radio activity timeout for Radios 1 and 2 runs out at 10:10:00 and for Radio 3 at 10:10:02. When it happens, the system creates a pool of inactive radios. The system puts the radios on a queue and starts sending presence check requests with the interval set in the **Global Minimum Request Interval** field. Radio 2 responds to the presence check request and is no longer regarded as potentially offline. Radios 1 and 3 do not respond to the presence check request and do not display any activity, so the system sends another request in 30s to each radio. After the 5th presence check request, the radios get the Offline status.



**Automatic update of registration, h:** If selected, the radio will send its ARS data to server at specified intervals.

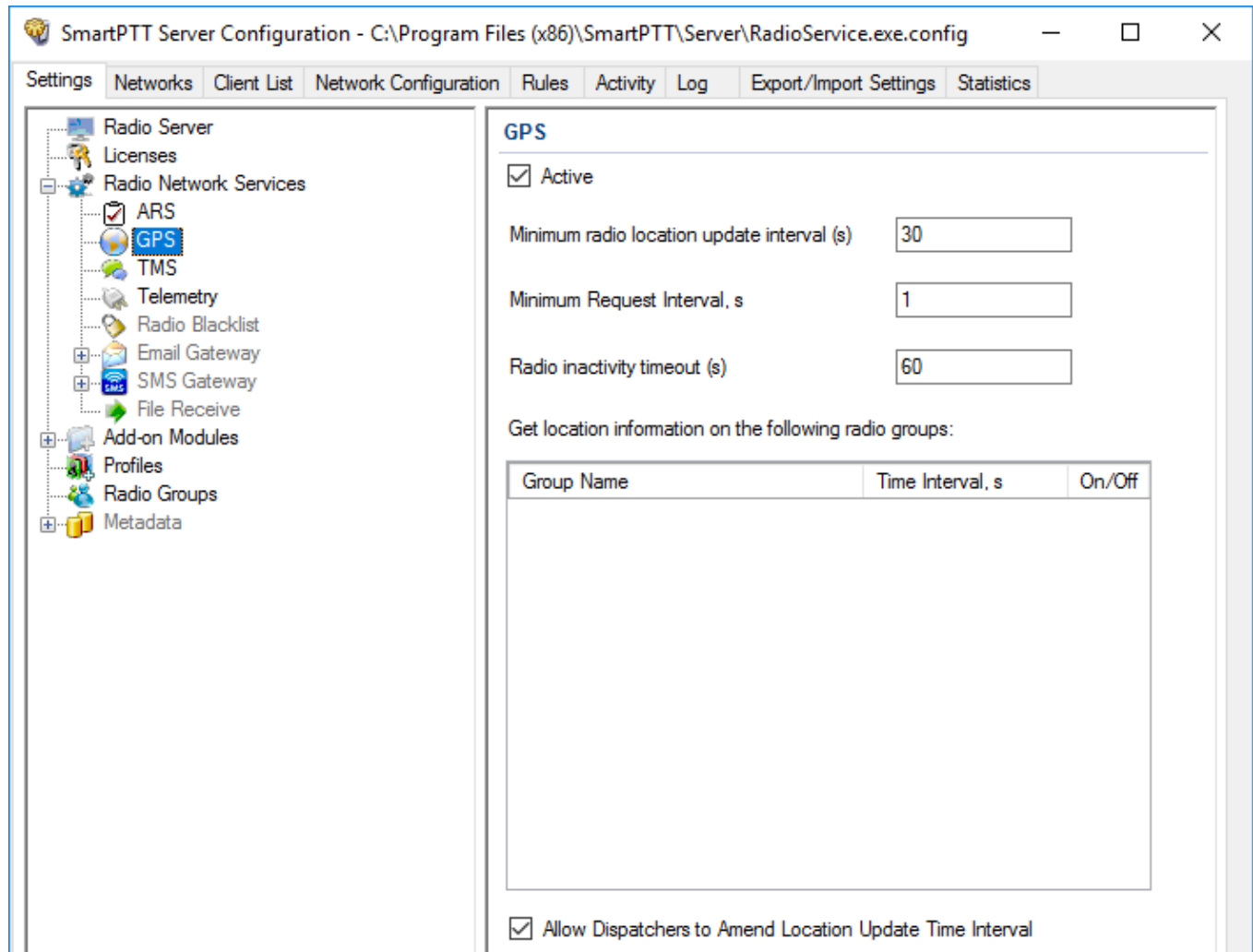
**NOTE**

We recommend to specify the [automatic registration update interval](#) larger than the [radio inactivity timeout interval](#).

## 1.4.2 GPS

GPS or location service provides coordinates of radios with a GPS receiver so you can determine their current location.

To set up location service parameters, in the **Settings** pane of the *SmartPTT Radioserver Configurator* window click **GPS**. The **GPS** pane appears:



**Active:** Select to activate the location service.

**Minimum location update interval, s:** Minimum update time interval. If the time interval specified by the dispatcher is less than **Minimum location update interval**, the new value set by the dispatcher will be ignored, and radio location will be updated within **Minimum location update interval**.

**Minimum Request Interval, s:** The minimum interval between GPS requests sent to the radios within one network. The requests can be sent automatically or initiated by the dispatcher. This method allows us to eliminate the risk of sending too many GPS requests at one time, thus removing traffic overload on the channel and spreading network load evenly.

**Radio Inactivity Timeout, s:** Time period, after which the radio that has not send GPS becomes potentially absent. In this case the radio receives a location update request.

The **Get location information on the following radio groups** table contains the radio groups added in the [Radio Groups](#) pane.

**Group Name:** The radio group name added in the [Radio Groups](#) pane.

**Time Interval, s:** The location update time interval for a certain radio group. It can be set in two ways:

- In the **Time Interval** field type the needed location update interval and press Enter.
- Select the **On/Off** check box and type the needed location update interval in the **Time Interval** field instead of the appeared default value.

You can set a range of fixed values for the location update time interval. The values for different [GPS transmission modes](#) can be the following:

- If the [Data](#) mode is on, you can set *30 s, 60 s, 120 s, 240 s* or *480 s* location update time interval.
- If the [CSBK](#) mode is on, you can set *15 s, 30 s, 60 s, 120 s, 240 s* or *480 s* location update time interval.
- If the [Enhanced CSBK](#) mode is on, you can set *7.5 s, 15 s, 30 s, 60 s, 120 s, 240 s* or *480 s* location update time interval.

#### NOTE

You can set 7.5 s interval using 7 or 8 values only.

**On/Off:** Select the check box to set location update time interval default value (*240 s*). If the check box is not selected, it will be selected automatically after typing the location update time interval in the **Time Interval** field.

#### NOTE

Each time you select or clear the **On/Off** check box again, the location update time interval in the **Time Interval** field automatically resets to its default value (*240 s*).

If **Allow Dispatchers to Amend Location Update Time Interval** is selected, dispatchers can reduce the location update time interval configured in the table above. However, if the time interval specified by the dispatcher is less than **Minimum location update interval**, the new value set by the dispatcher will be ignored, and radio location will be updated within **Minimum location update interval**. If **Allow Dispatchers to Amend Location Update Time Interval** is not selected, dispatchers won't be able to change the time interval for location update, and location will be updated within the time interval set in the table per each group.

### WARNING

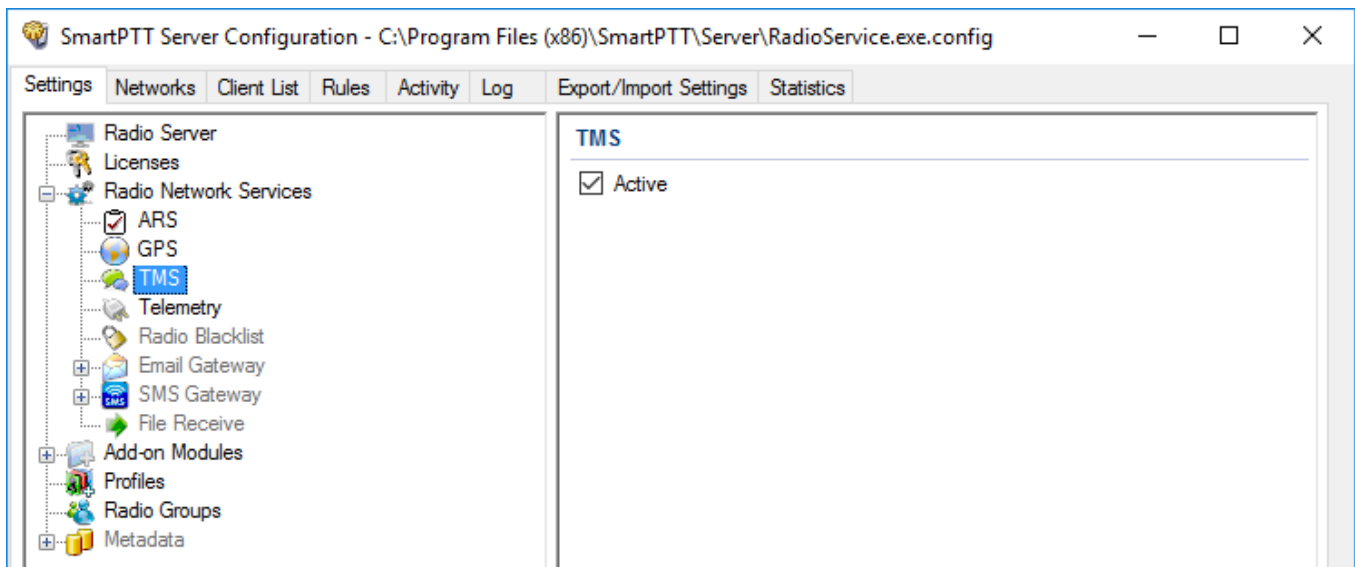
If **Allow Dispatchers to Amend Location Update Time Interval** check box is clear and the table is empty, the dispatcher will not receive any radio location data.

## 1.4.3 TMS

TMS or text messaging service is used to exchange text messages between radios and *SmartPTT Dispatcher*.

To set up the messaging service parameters, follow these steps:

1. In the left pane of the **Settings** tab click **TMS**.
2. In the **TMS** pane, select the **Active** check box.

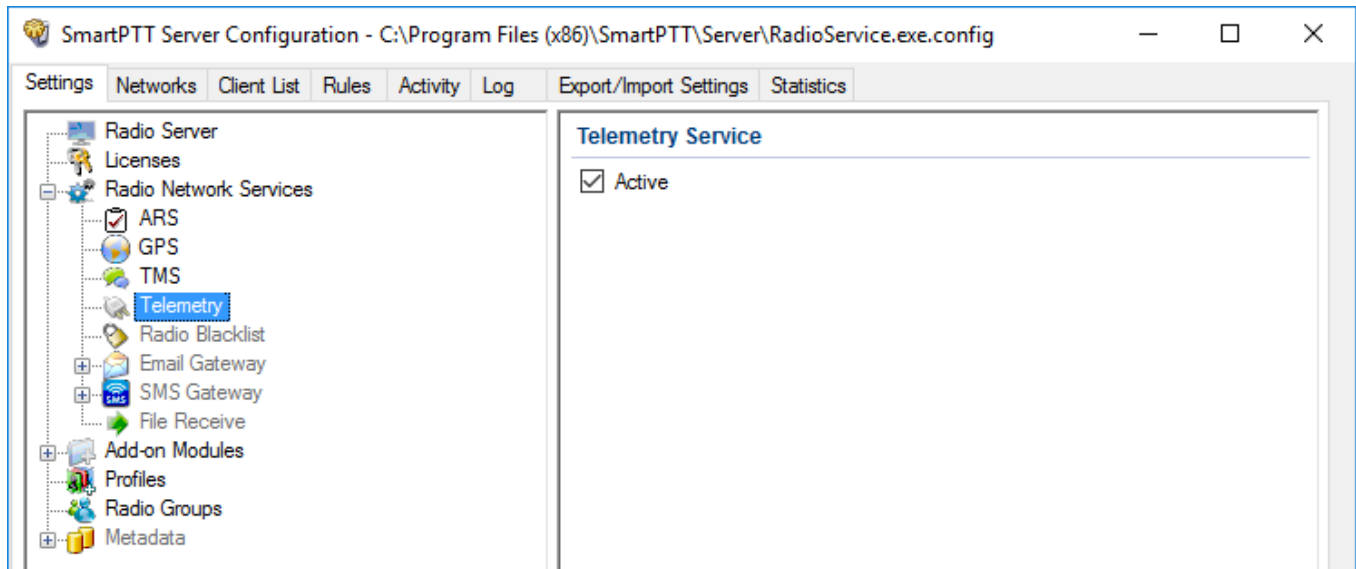


## 1.4.4 Telemetry

Telemetry is used for transmission and processing of telemetry signals between *SmartPTT Dispatcher* and radios.

To set up telemetry parameters, follow these steps:

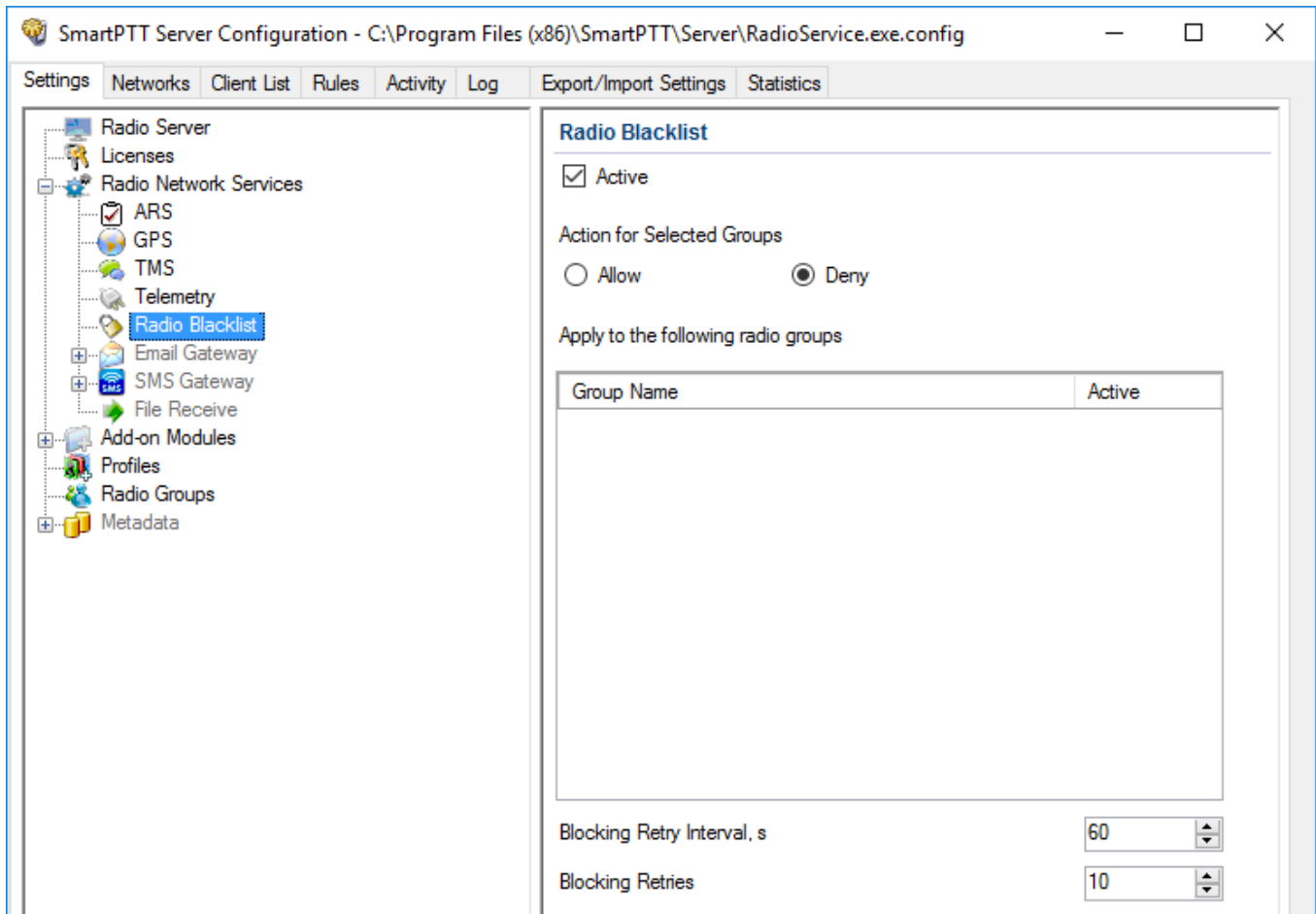
1. In the left pane of the **Settings** tab, click **Telemetry**.
2. In the **Telemetry Service** pane, select the **Active** check box.





## 1.4.5 Radio Blacklist

**Radio Blacklist** is used for blocking radios. You can block only registered radios when they go online and included into the certain [radio group](#). Besides the blacklist you can also create a “whitelist”, in other words to block all other radios except those who are in the selected groups.



To block the radio, you should preconfigure this feature using *MOTOTRBO CPS*.

If the radio is not blocked, *SmartPTT Radioserver Configurator* performs several attempts of blocking according to the settings.

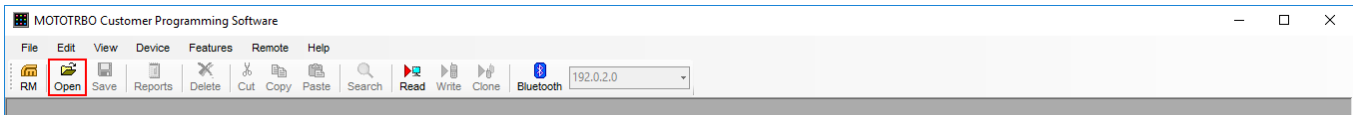
Configuration of the blacklist includes the following steps:

## Configuring the Firmware File

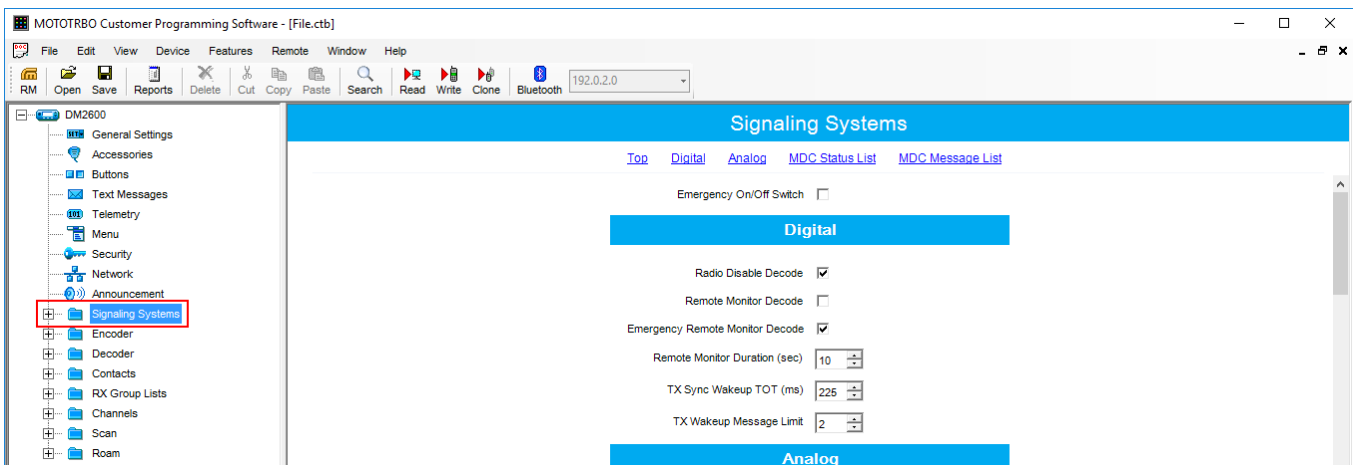
This topic contains information about the firmware file configuration. It is alternative to the Configuring the Radio procedure.

To configure a firmware file, follow these steps:

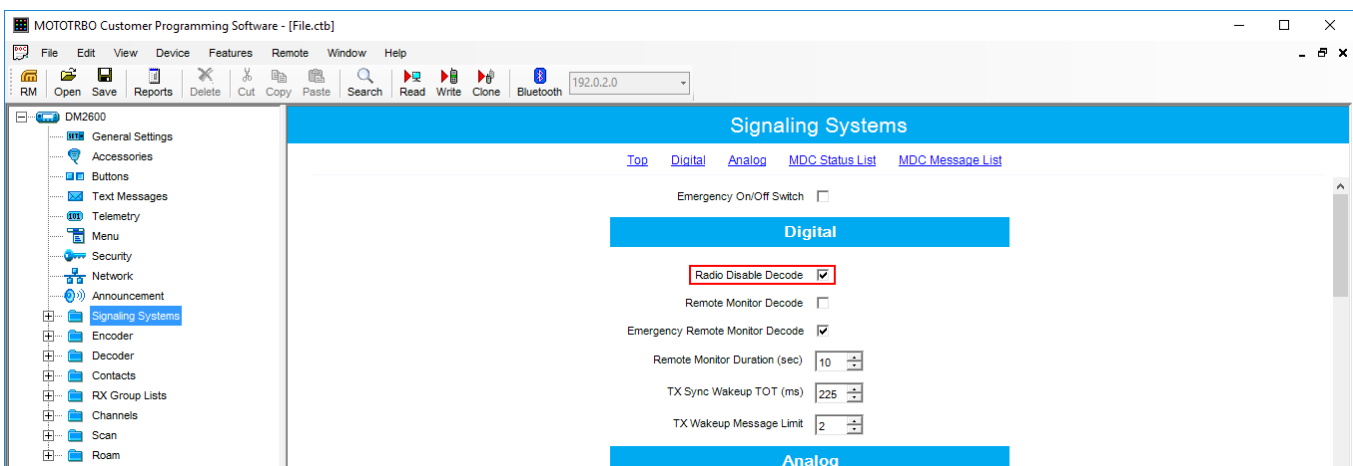
1. In *MOTOTRBO CPS*, click **Open** and select the firmware file.



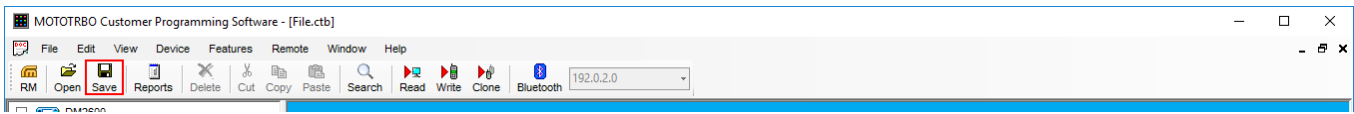
2. In the left pane, click **Signaling Systems**.



3. In the **Signaling System** pane, select **Radio Disable Decode**.



#### 4. Click **Save**.



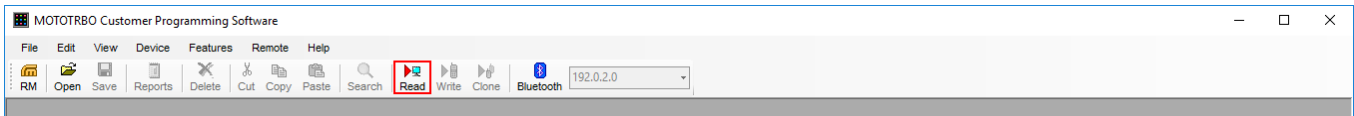
To allow blocking the radio, update the radio firmware using the saved file.

## Configuring Radio

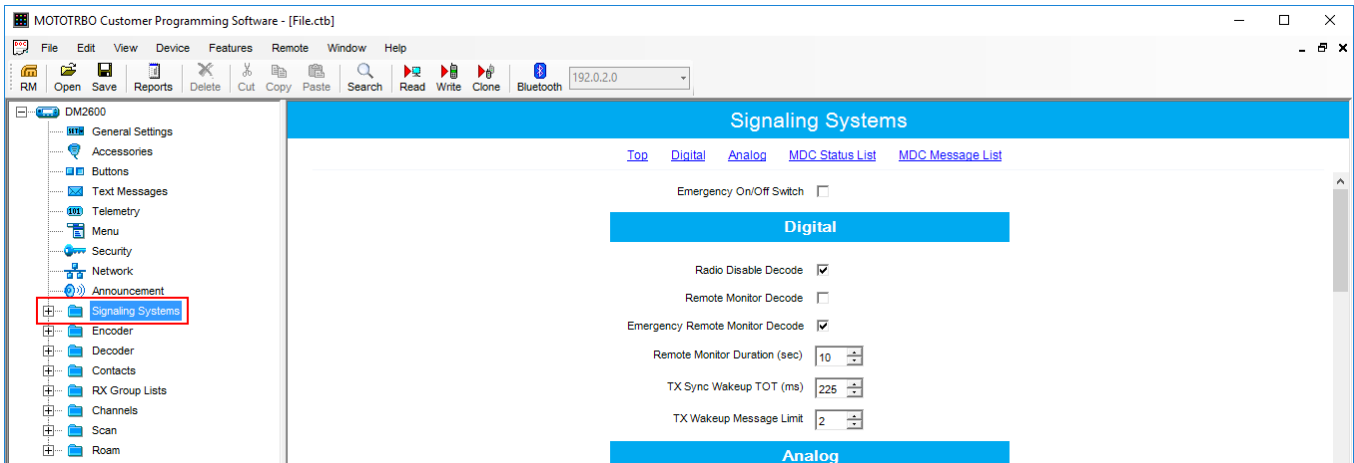
This topic contains information about radio configuring. It is alternative to the Configuring the Firmware File.

To configure Radio, follow these steps:

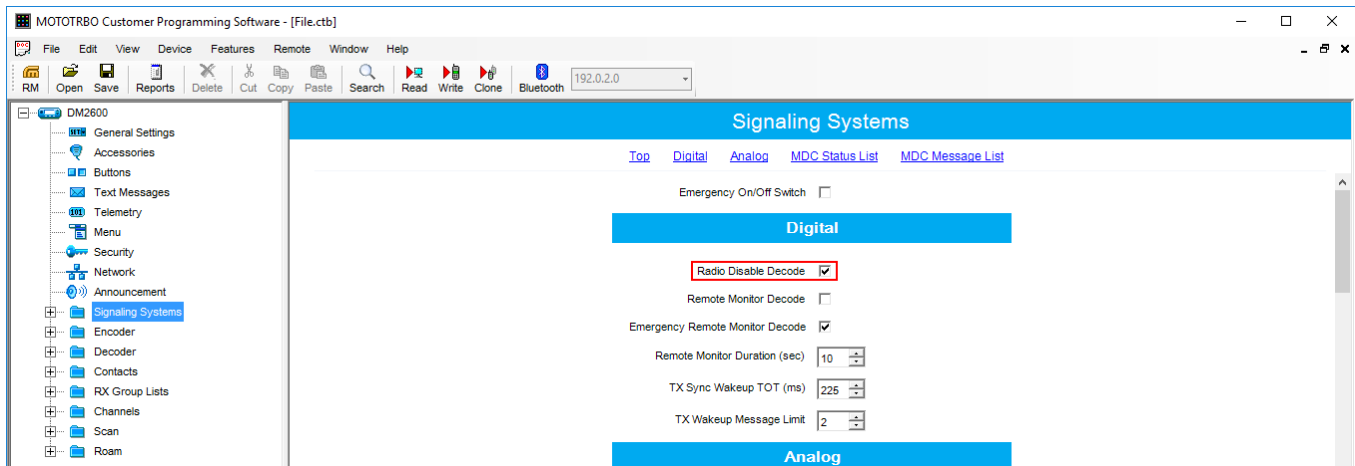
1. Connect the radio to the computer with special cable and wait for driver installation. *MOTOTRBO CPS* must be installed on the computer previously.
2. Run *MOTOTRBO CPS* and click **Read**.



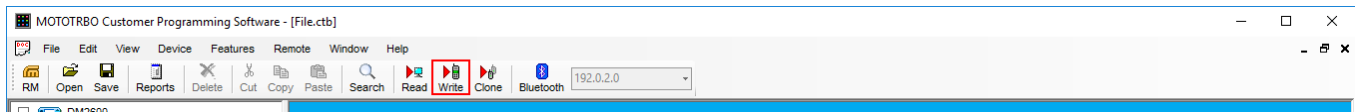
#### 3. In the left pane, click **Signaling Systems**.



- In the **Signaling System** pane, select **Radio Disable Decode**.



- Pause your antivirus software to provide successful firmware update.
- Click **Write** to update radio firmware.



### WARNING

Do not unplug your cable from the radio or computer until the radio firmware update complete.

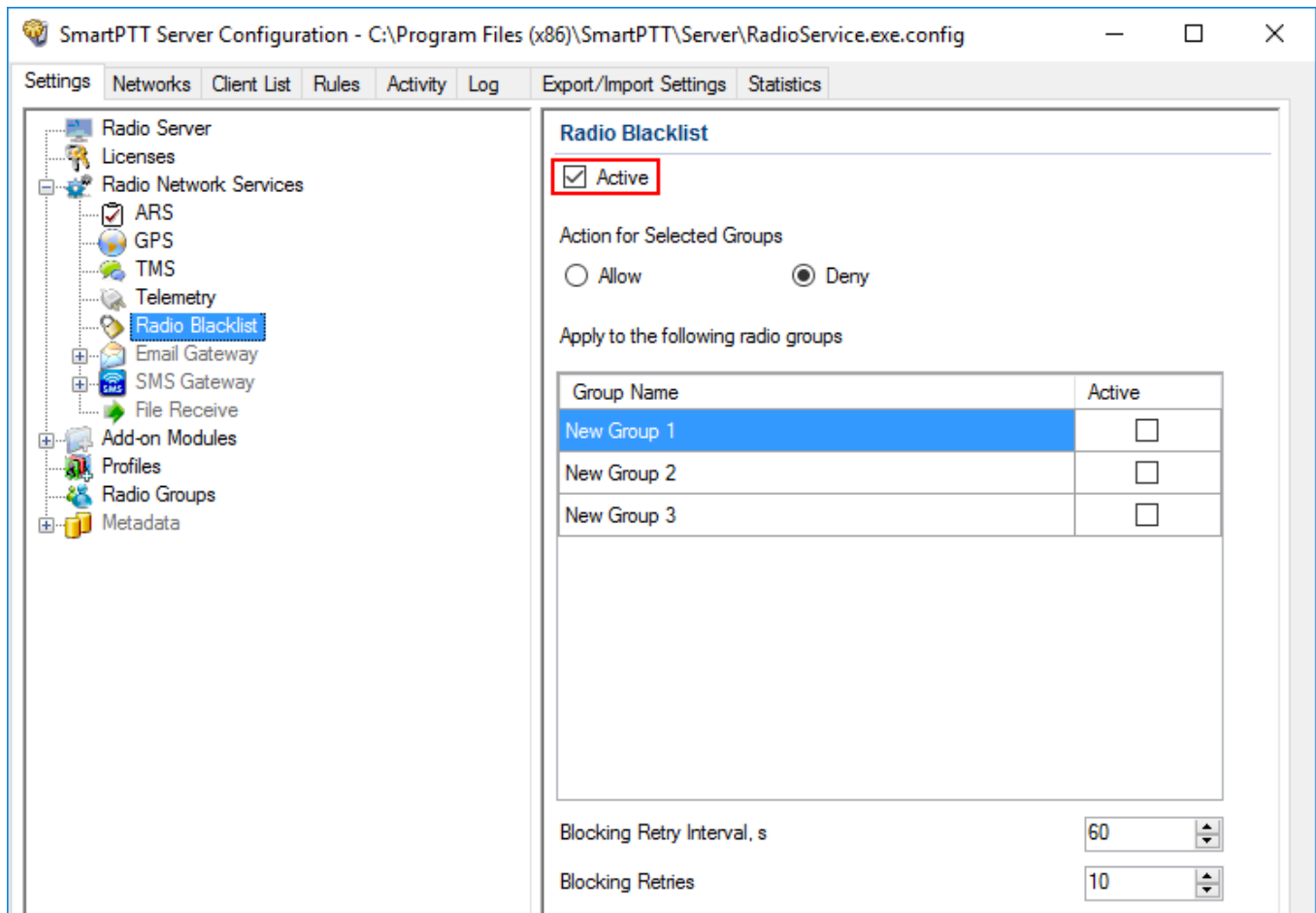
- Wait for the successful update and close *MOTOTRBO CPS*.
- Eject the radio properly and unplug the cable from your computer.

## Configuring Radio Blacklist

To begin the configuration of the Radio Blacklist you should create radio groups (see Adding Radio Groups).

To configure Radio Blacklist, follow these steps:

1. In the left pane of the **Settings** tab, click **Radio Blacklist**.
2. In the **Radio Blacklist** pane, select **Active**.

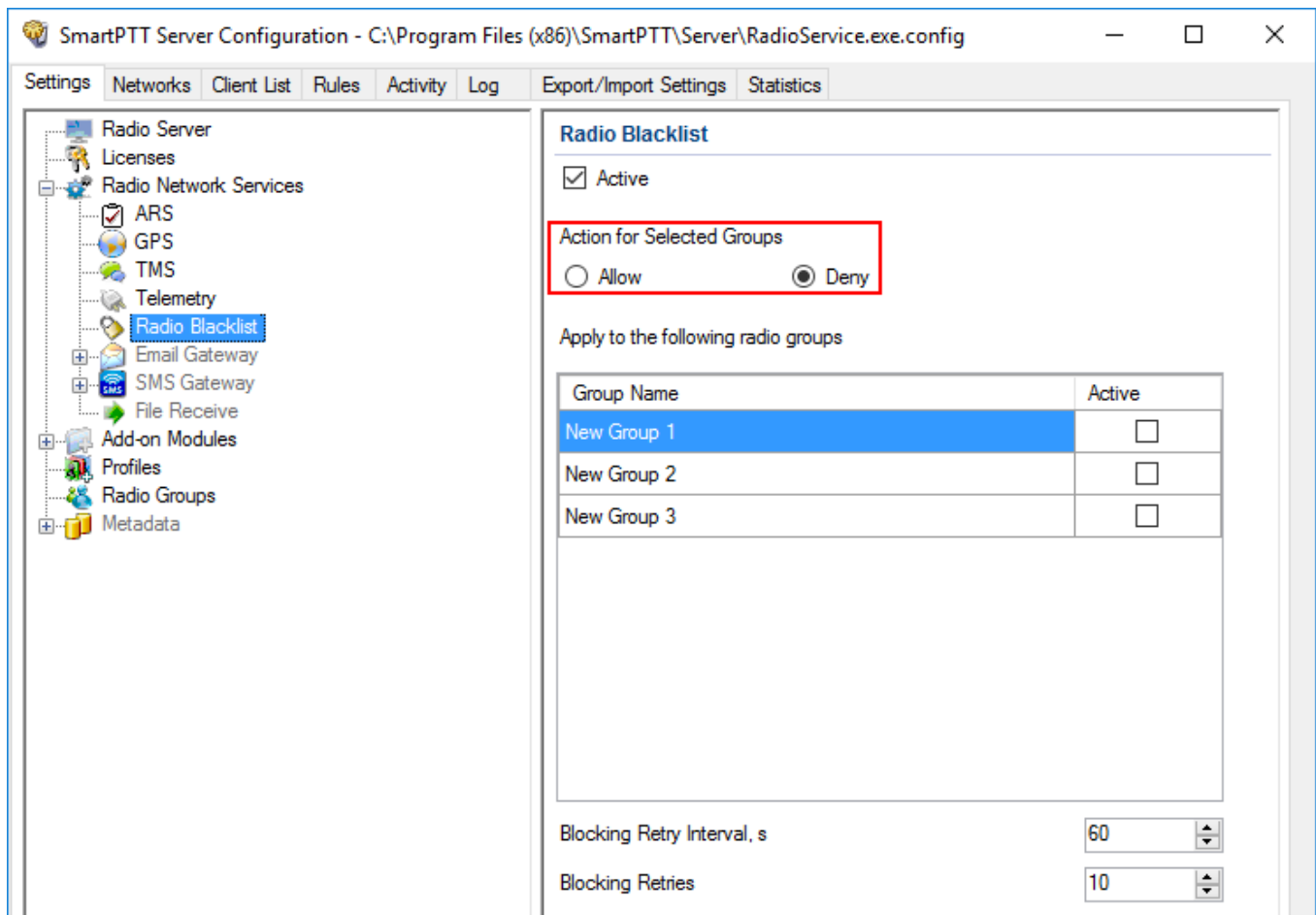


The screenshot shows the SmartPTT Server Configuration window with the 'Radio Blacklist' settings pane active. The left sidebar shows a tree view with 'Radio Blacklist' selected. The main pane has the following settings:

- Radio Blacklist**:  Active
- Action for Selected Groups**:  Allow,  Deny
- Apply to the following radio groups**: A table with 3 rows and 2 columns.
- Blocking Retry Interval, s**: 60
- Blocking Retries**: 10

Group Name	Active
New Group 1	<input type="checkbox"/>
New Group 2	<input type="checkbox"/>
New Group 3	<input type="checkbox"/>

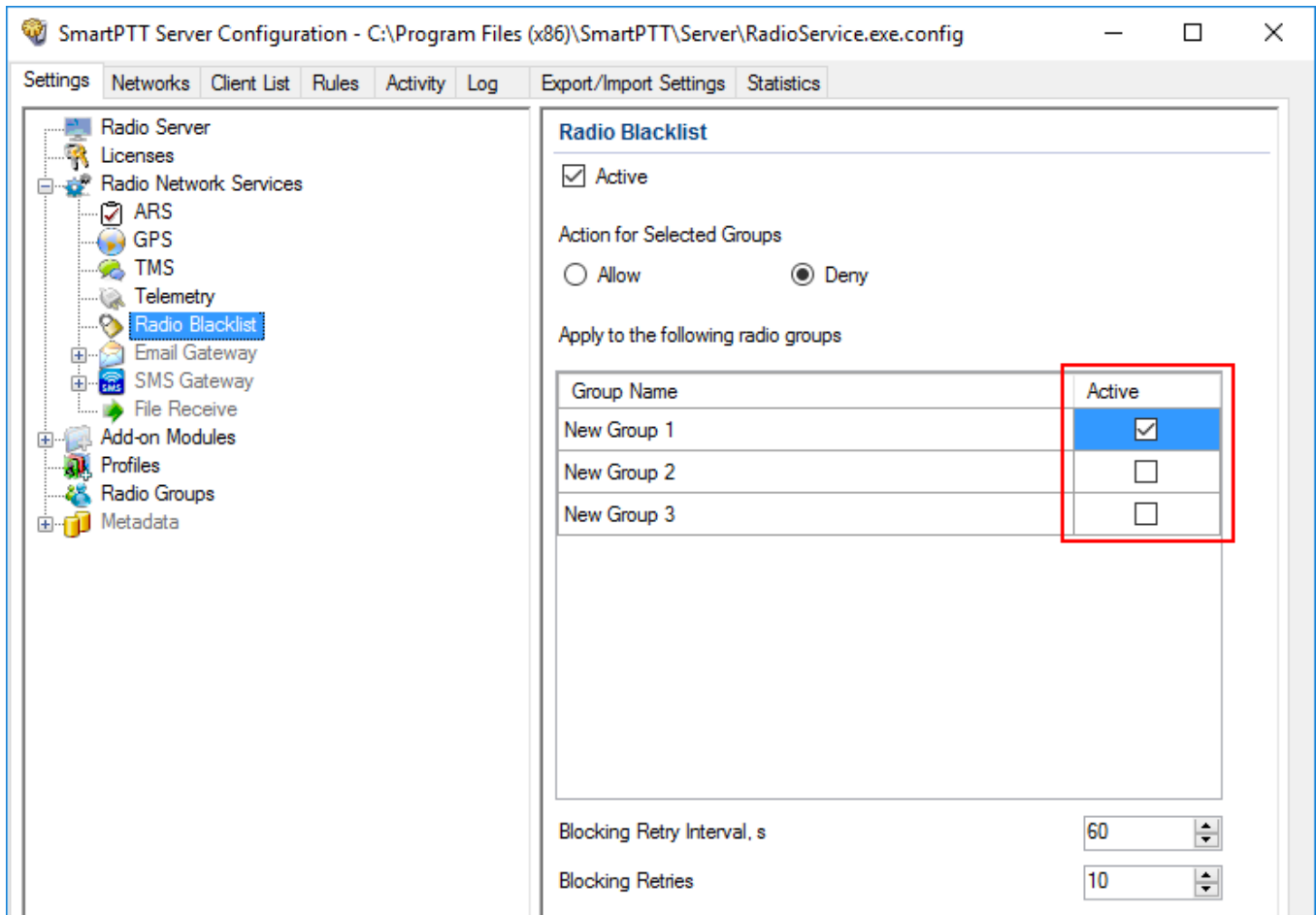
3. Select needed type of the list for radio groups.



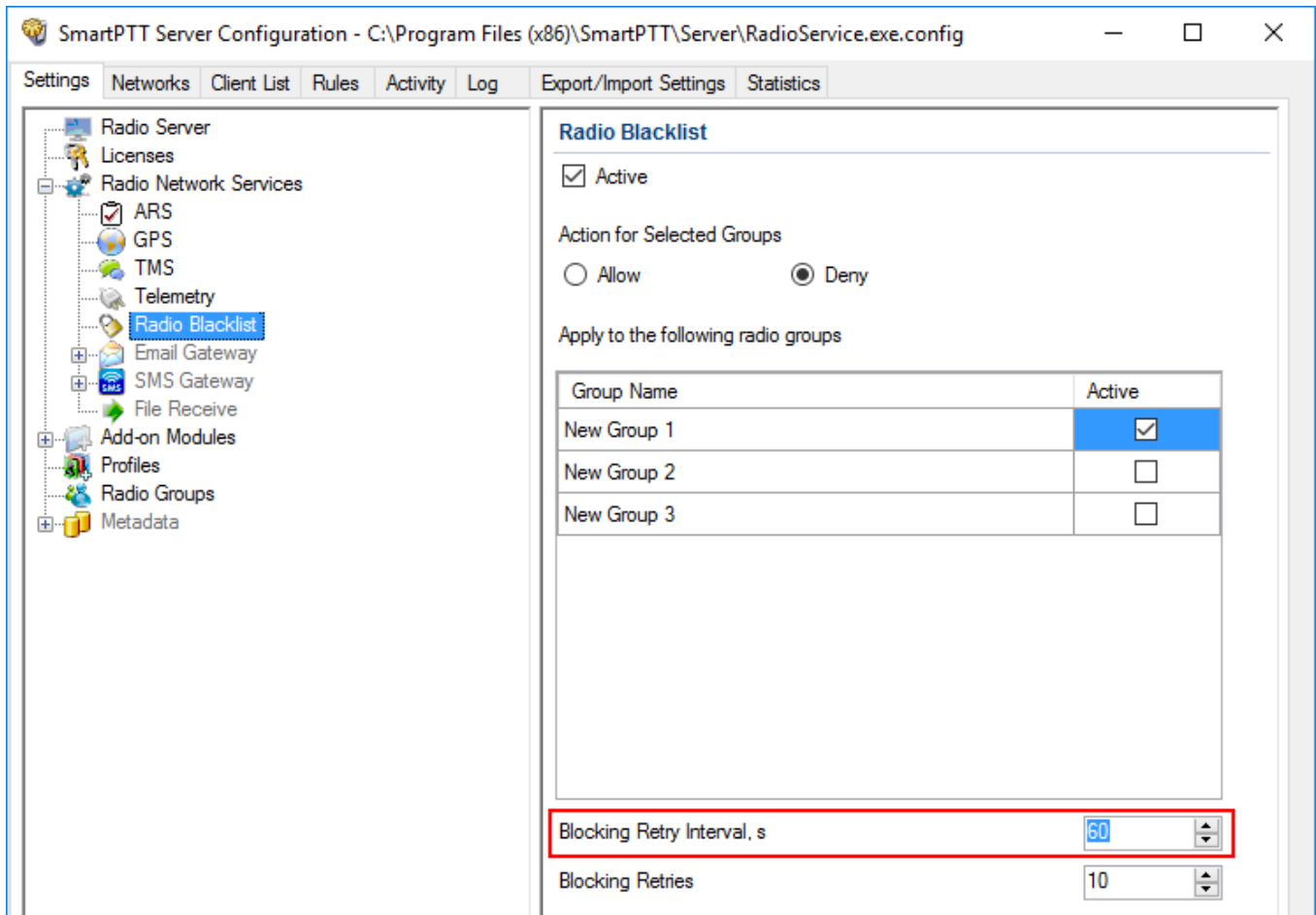
**Deny:** Blocks selected radio groups.

**Allow:** Blocks other groups except of the selected ones.

4. Select the desired radio groups.



5. In the **Blocking Retry Interval** field, enter an interval between attempts of blocking.





- In the **Blocking Retries** field enter a number of groups blocking retries.

The screenshot shows the 'Radio Blacklist' configuration window. The left sidebar contains a tree view with 'Radio Blacklist' selected. The main panel has the following settings:

- Active
- Action for Selected Groups:  Allow,  Deny
- Apply to the following radio groups:



Group Name	Active
New Group 1	<input checked="" type="checkbox"/>
New Group 2	<input type="checkbox"/>
New Group 3	<input type="checkbox"/>

At the bottom, there are two spinners:

- Blocking Retry Interval, s: 60
- Blocking Retries: 10** (highlighted with a red box)

**NOTE**

If blocking is failed after retry number, SmartPTT Radioserver Configurator stops attempting until the restart.

- Click **Save**  to save changes.
- Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

## 1.4.6 Email Gateway

Email gateway is used for exchanging digital messages between email users and MOTOTRBO radios. The following scheme displays how it is done:



To be able to exchange email messages between radios and email users you need to configure radioserver.

For text message exchange you can use POP3 or IMAP4 protocol.

Before configuring radioserver, ensure your email account is configured properly:

- POP is activated for all email (including downloaded)
- IMAP is activated

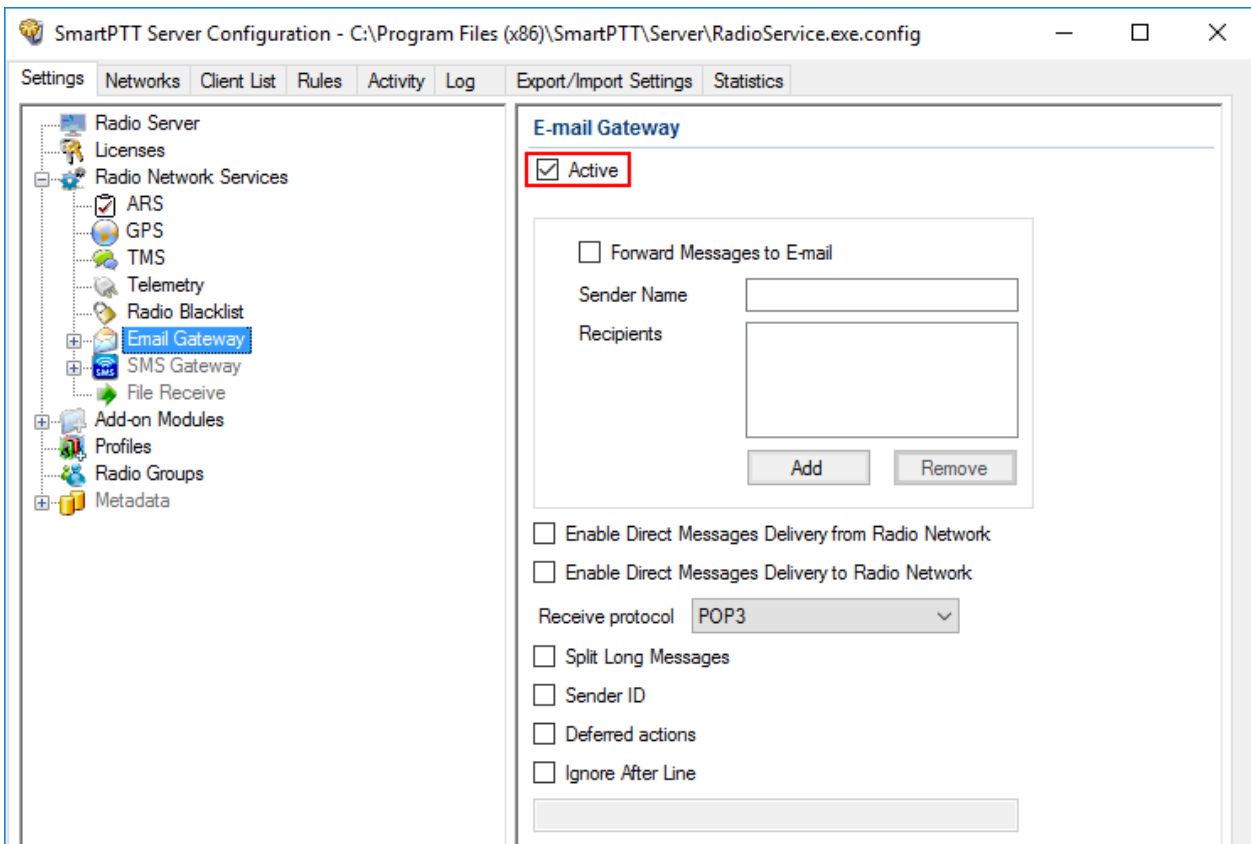
If you use an email client (for example, Microsoft Outlook), the following settings are required for the outgoing messages:

- Plain text as a message format
- Unicode (UTF-8) encoding for outgoing images (with Base64 encoding)

## 1.4.6.1 Configuring Radioserver

To configure SmartPTT Radioserver, follow these steps:

1. In the **Settings** tab of SmartPTT Radioserver, expand **Radio Network Services** and click **Email Gateway**.
2. In the **Email Gateway** pane, select the **Active** check box.





3. Select the **Forward Messages to E-mail** check box to activate message forwarding from radios to the email addresses specified in the **Recipients** list.

### NOTE

When a radio sends a text message to another radio and if it was successfully sent or/and delivered, all recipients added to the **Recipients** list receive the according confirmation messages.

4. In the **Sender Name** field, enter the domain name from which email messages are sent.
5. In the **Recipients** field, enter the list of email addresses to receive forwarded text messages.

6. *Optional:* Select the **Direct Message Delivery from Radio Network** check box to forward mail messages directly from radios.
7. *Optional:* Select the **Direct Message Delivery to Radio Network** check box to forward mail messages directly to radios.
8. *Optional:* From the **Receive protocol** list, select the protocol for email message receiving (*POP3* or *IMAP4*).
9. *Optional:* Select the **Split Long Messages** check box to split the original message into several packages during transmission without losing information.
10. *Optional:* Select the **Sender ID** check box to insert the sender email address to the received message.
11. *Optional:* Select the **Deferred actions** check box to deliver an information to the offline radio. When radio becomes online, it will immediately receive it.
12. *Optional:* Select the **Ignore After Line** check box to ignore everything after a certain string in the received email message.
13. Click **Save**  to save changes.
14. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

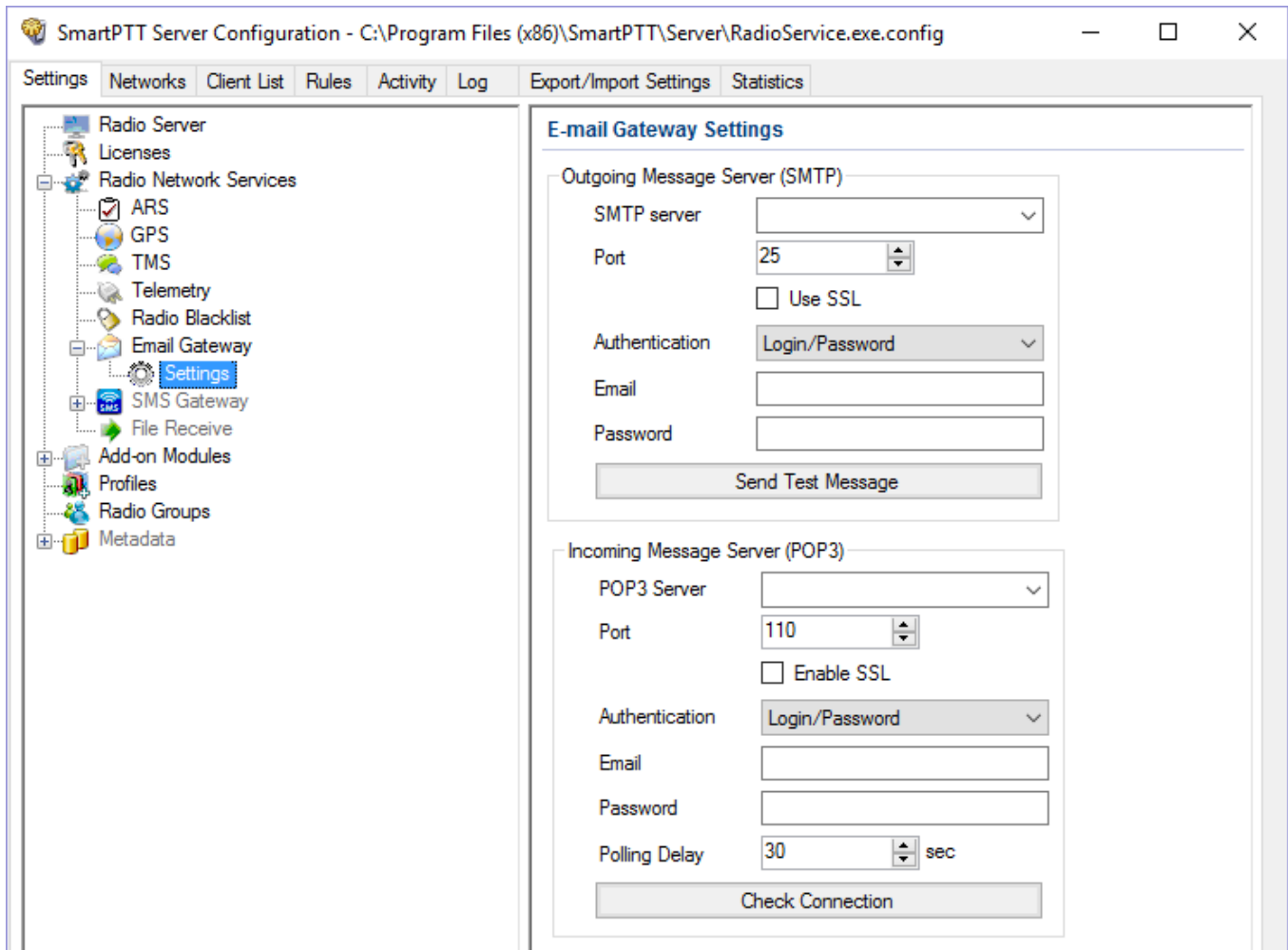
**NOTE**

When **Forward Messages to E-mail** is enabled together with the options of receiving messages from the radio network and from the email, all messages sent or received by email users will be duplicated to the specified email addresses.



### 1.4.6.1.1 Configuring Outgoing Messages Server

To configure outgoing message server settings in SmartPTT Radioserver Configurator, follow these steps:

1. In the **Settings** tab of SmartPTT Radioserver, expand **Radio Network Services** → **Email Gateway** and click **Settings**.



2. In the **Outgoing Message Server (SMPT)** area of the **E-mail Gateway Settings** pane, perform the following actions:
  - a. In the **SMTP server** field, enter the domain name of SMTP server which is used for delivering outgoing email messages.
  - b. In the **Port** field, enter the port number SMTP server.
  - c. *Optional:* If you want to establish a secure connection with SMTP server, select the **Use SSL** check box.

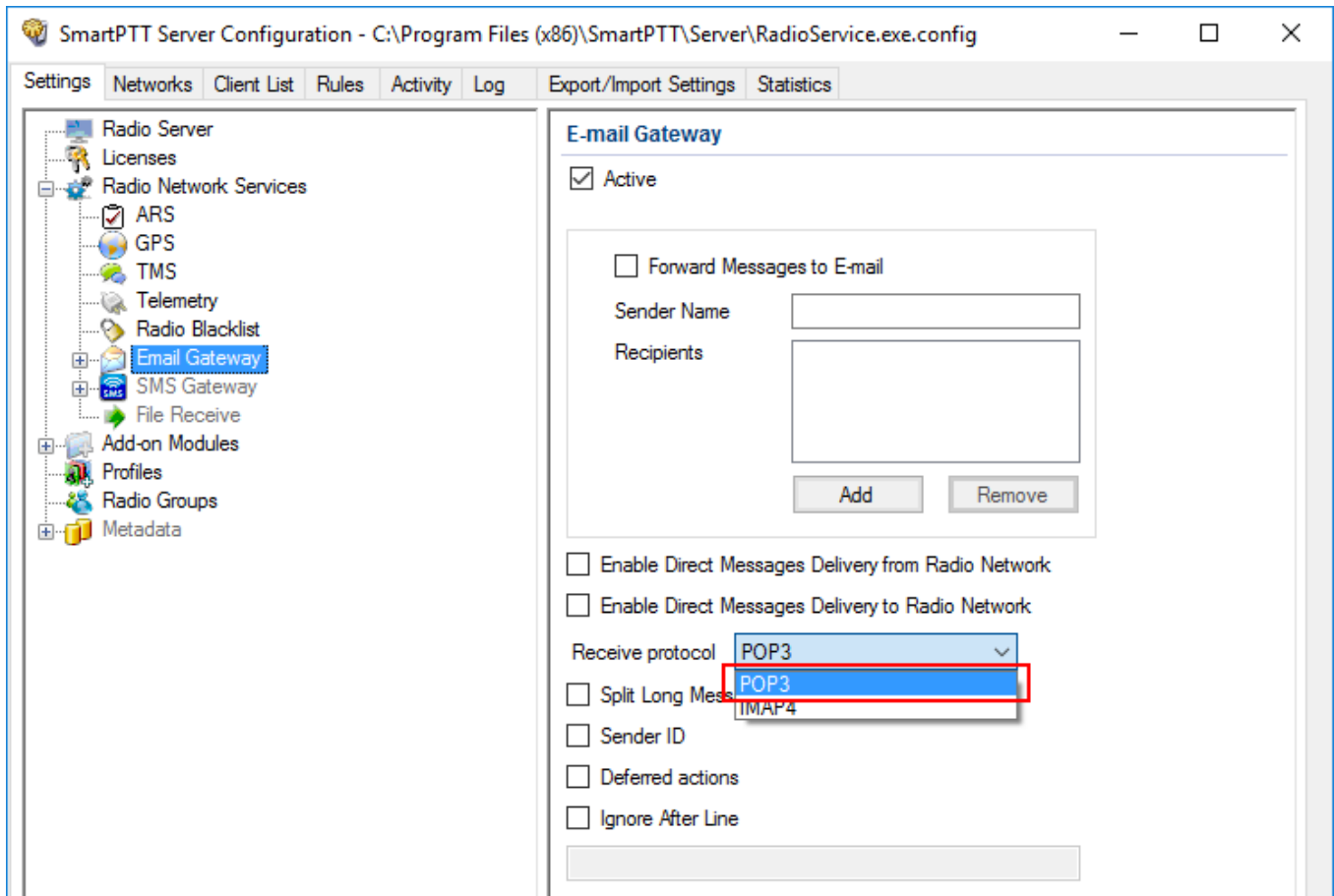
- d. From the **Authentication** list select the authentication method for SMTP server:
    - i. *Anonymous* – to connect to the SMTP server anonymously.
    - ii. *Windows* – to connect to the SMTP server using Windows Authorization.
    - iii. *Login/Password* – to connect to the SMTP server with Login/Password specified.
  - e. *If the Login/Password authentication is selected:* In the **Email** field, enter an email address required by the mail server.
  - f. *If the Login/Password authentication is selected:* In the **Password** field, enter the password.
3. Click **Send Test Message** to check server connection. If connection is successful and the settings are correct, the mail user specified above will receive a test email message.
  4. Click **Save**  to save changes.
  5. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

#### 1.4.6.1.2 Configuring Incoming Messages Server

To configure incoming message server settings in SmartPTT Radioserver Configurator, follow these steps:

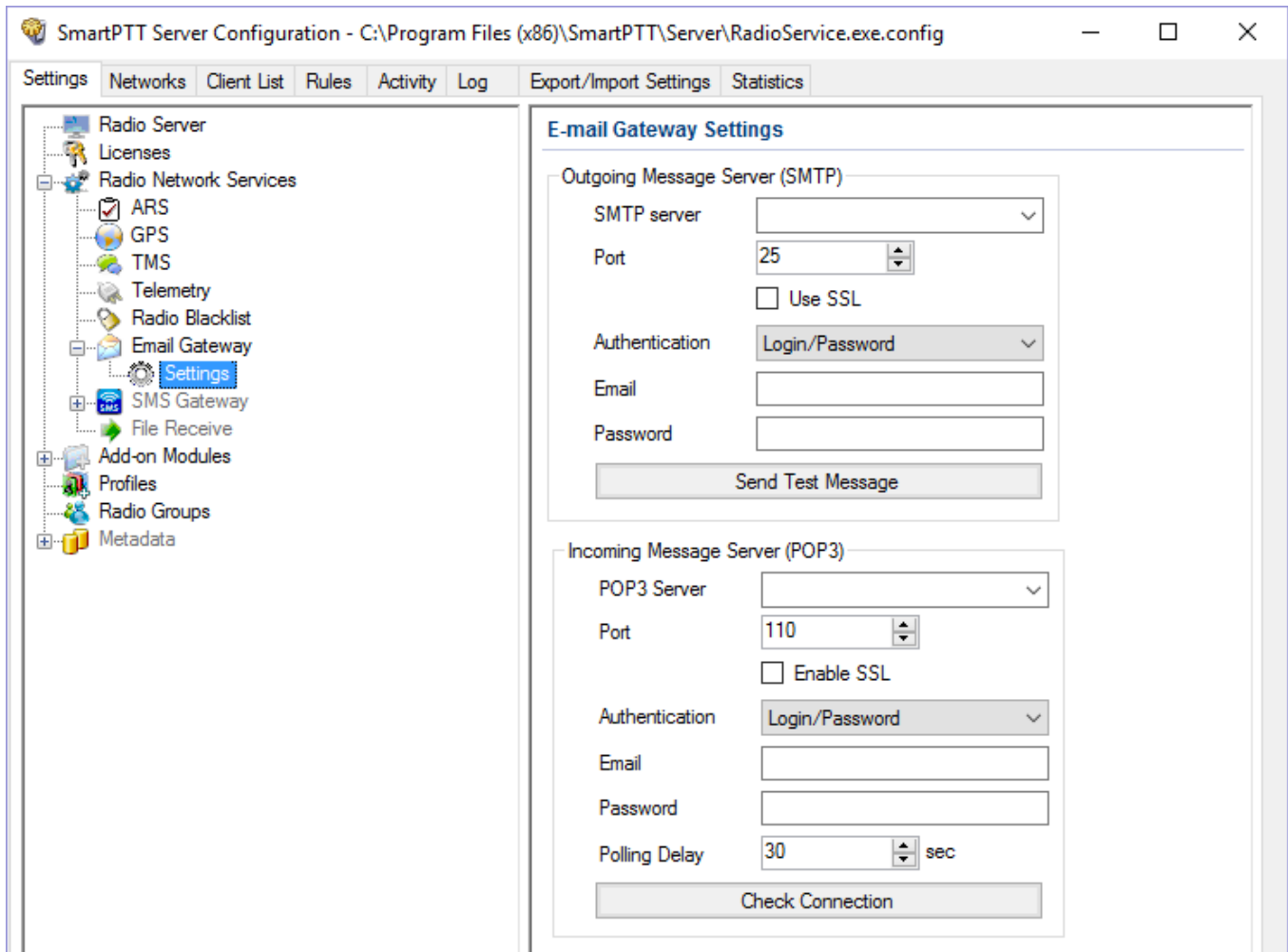
1. In the **Settings** tab of SmartPTT Radioserver, expand **Radio Network Services** and click **Email Gateway**.

2. In the **Email Gateway** pane, from the **Receive protocol** list, select *POP3* or *IMAP4*.







3. Expand **Email Gateway** and click **Settings**.



4. In the **Incoming Message Server** area of the **Email Gateway Settings** pane, perform the following actions:
- In the **POP3 Server** (or **IMAP4 Server**) field, specify domain name of the server which is used to deliver incoming email messages.
  - In the **Port** field, enter the port number server.
  - Optional:* If you want to establish a secure connection with server, select the **Use SSL** check box.
  - From the **Authentication** list select the authentication method for server:
    - Anonymous* – to connect to the server anonymously.
    - Login/Password* – to connect to the server with Login/Password specified.

- e. *If the Login/Password authentication is selected:* In the **Email** field, enter an email address required by the mail server.
  - f. *If the Login/Password authentication is selected:* In the **Password** field, enter the password.
  - g. In the **Polling Delay** field, specify the polling interval for the mail server.
5. Click **Check Connection**.

If connection is successful, the pop-up window displays the number of unread email messages in your email box.

6. Click **Save**  to save changes.
7. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

## 1.4.6.2 Sending Messages

### 1.4.6.2.1 Sending Messages to Radios

To send an email message to a radio, follow these steps:

1. Sign in to your email account.
2. Compose the message:
  - a. Enter the prefix : (colon symbol) indicating that this message is addressed to a radio or a talkgroup.
  - b. Enter the radio/talkgroup ID or IP address in the **<ID|IP>** format.

#### NOTE

If a radio or talkgroup ID is more than 255, you can send an email message only by entering the radio or talkgroup IP address.

- c. Enter the space symbol that indicates the beginning of a text message body.
- d. Enter your message.



## Example

- The email message `:12.0.0.77 Hello!` received from the mail server will be forwarded to the radio or talkgroup with IP `12.0.0.77`.
- The email message `:77 Hello!` received from the mail server will be forwarded to the radio with ID `77`.
- The email message `:12.0.0.80,12.0.0.81,12.0.0.82,12.0.0.50 Hello!` or `:80,81,82,50 Hello!` received from the mail server will be forwarded to the radios with corresponding IDs.

### 1.4.6.2.2 Sending Messages to Email Address

To send a message from a radio to an email user, follow these steps:

1. Open the **Messages** menu on the radio.
2. To enter the message text in the field, perform the following actions:
  - a. Enter the prefix `:` (colon symbol) indicating that this message is addressed to email user.
  - b. Enter the email address of the contact or several contacts, separated with the comma (`,`) symbol in the `<email_address>` format.
  - c. Enter the space symbol that indicates the beginning of the message body.
  - d. Enter your message.



## Example

- The message `:email_address@example.com Hello!` from a radio will be forwarded to the email user with the email address `email_address@example.com`.
- The message `:email_address1@example.com, email_address2@example.com Hello!` from a radio will be forwarded to the email users `email_address1@example.com` and `email_address2@example.com`.

## 1.4.7 SMS Gateway

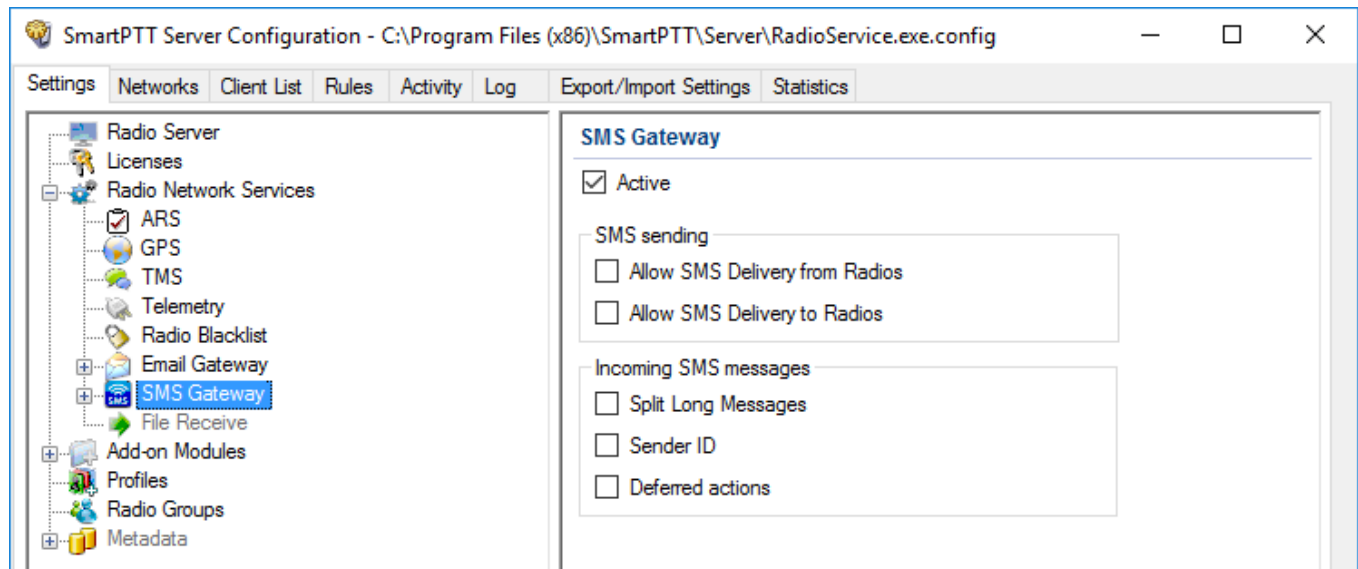
SmartPTT Radioserver has an integrated SMS Gateway service, which allows establishing communication between radios and mobile phones. There are two possible ways to communicate between each other:

- A radio sends an SMS to a phone subscriber
- A phone subscriber sends an SMS to a radio

To be able to send an SMS, it is necessary to do preliminary settings on both modem and SmartPTT Radioserver.

### Configuring SmartPTT Radioserver and Incoming Messages

In the left pane of the Settings tab, click **SMS Gateway**.



**Active:** Select to enable SMS Gateway service.

**Allow SMS Delivery from Radios:** Select this option if you need to forward SMS directly from radios.

**Allow SMS Delivery to Radios:** Select this option if you need to forward SMS directly to radios.

**Split Long Messages:** If selected, a long message, i.e. a message that contains more characters than allowed in one message in the radio network sent to a radio, will be split into several

messages. If not selected, a long message addressed to a radio is trimmed to not exceed the limit (some information will be lost).

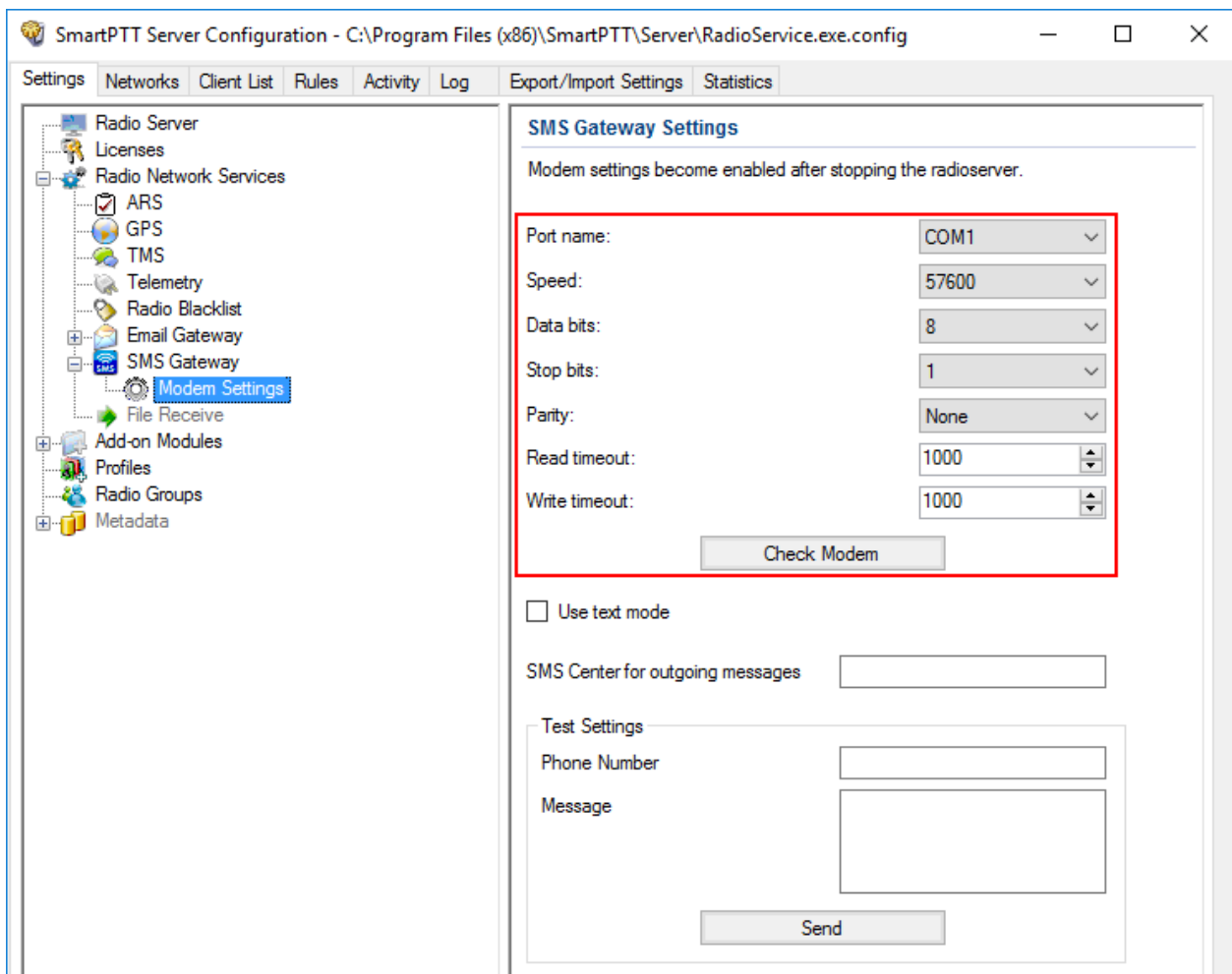
**Sender ID:** If selected, the phone number of the sender with the received SMS will be displayed on the radio.

**Deferred actions:** If selected, it allows to deliver an information to the offline radio. When radio becomes online, it will immediately receive it.

## Configuring a Modem and Outgoing Messages

### WARNING

To enable modem settings, stop SmartPTT Radioserver.



**Port name:** COM port number which modem is connected to. You can find the COM port number by opening modem properties in Windows Control Panel.

**Speed:** Data flow rate through COM port (in bits per second).

**Data bits:** Number of data bits to transmit. You can configure **Data Bits** to be 5, 6, 7, or 8. Data is transmitted as a series of five, six, seven, or eight bits (five and six bit data formats are used rarely for specialized communications equipment).

**Stop bits:** Number of bits used to indicate the end of a byte. You can configure **Stop Bits** to be 1, 1.5, or 2. If **Stop Bits** is 1.5, the stop bit is transferred for 150% of the normal time used to transfer one bit. Both the computer and the peripheral device must be configured to transmit the same number of stop bits.

**Parity:** Method of detecting errors in transmission. You can configure **Parity** to be **None**, **Odd** or **Even**:

**None:** Parity checking is not performed and the parity bit is not transmitted.

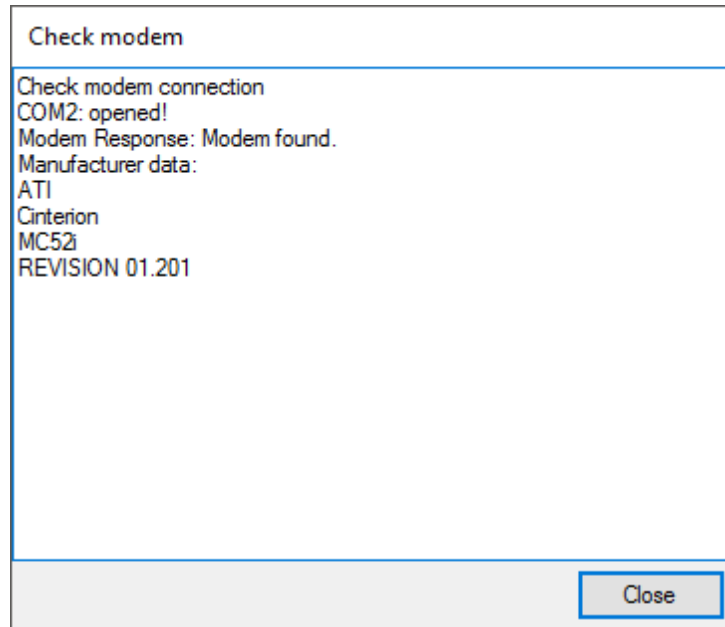
**Odd:** Number of mark bits in the data is counted, and the parity bit is asserted or unasserted to obtain an odd number of mark bits.

**Even:** Number of mark bits in the data is counted, and the parity bit is asserted or unasserted to obtain an even number of mark bits.

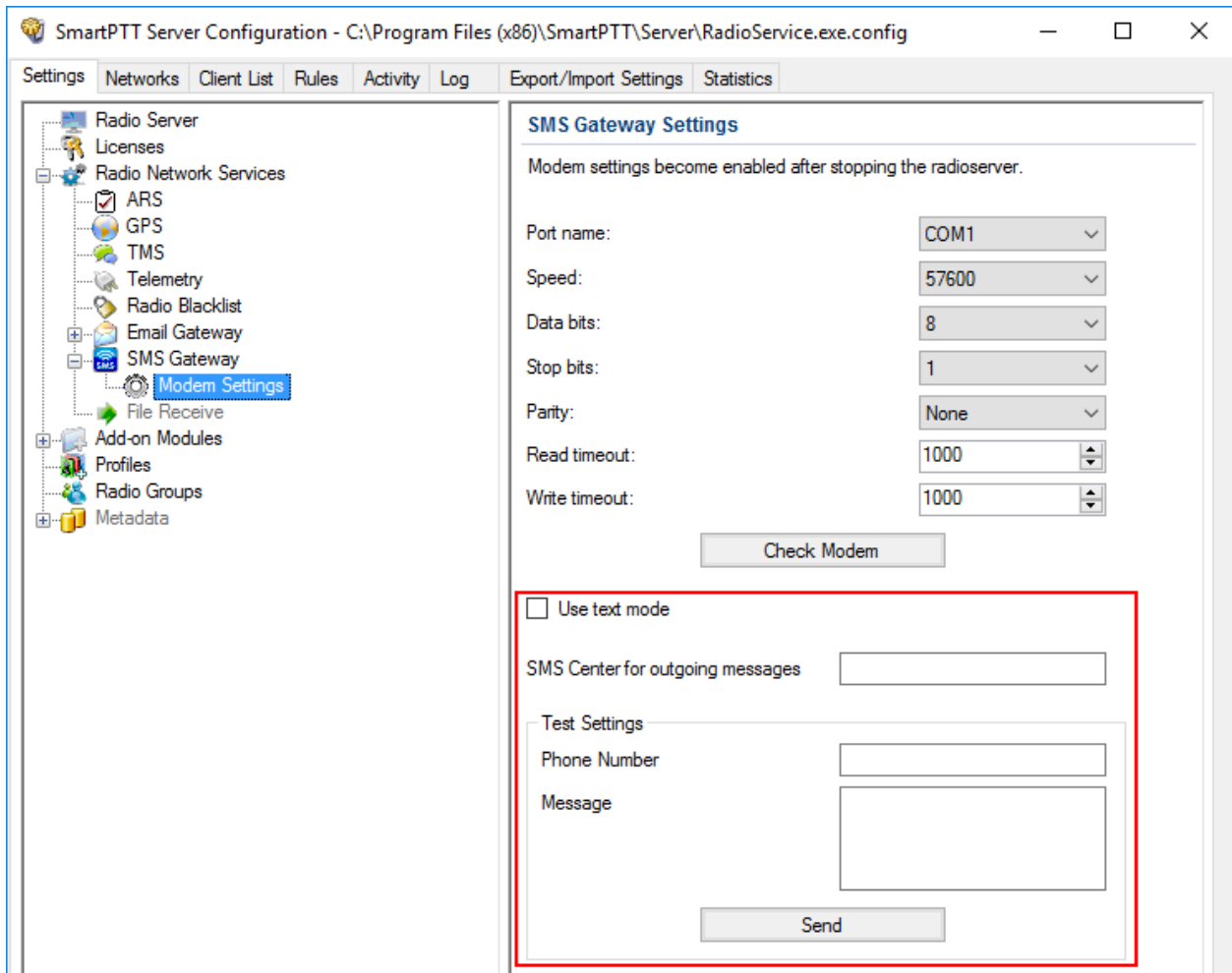
**Read timeout:** Number of milliseconds before a time-out occurs when a read operation does not finish.

**Write timeout:** Number of milliseconds before a time-out occurs when a write operation does not finish.

**Check Modem:** Modem operation test. If a modem is detected, you will see information regarding the type of modem installed on your system. If there is no modem detected, you will see “Modem not found” message.



The next step is to check settings for outgoing messages and to send a test message.



**Use text mode:** Allows selecting Text or PDU mode for SMS sending. There are two ways of sending and receiving SMS messages: in text mode (the check box selected) and in the protocol description unit (PDU) mode (the check box is not selected). The text mode (unavailable on some phones) is just an encoding of the bit stream represented by the PDU mode, and can be used only for English; PDU mode and Unicode are used for all languages. Unicode is the universal character encoding which provides the basis for the consistent encoding, representation and handling of text expressed in most of the world's writing systems.

**SMS Center for outgoing messages:** SMS message center number. If the number is registered on modem's SIM-card, there is no need to fill this field.



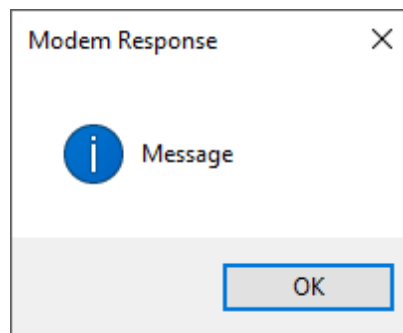
## Testing SMS Sending



Make sure SMS that messages can be sent to recipients from SmartPTT Radioserver. Use **Test Settings** to do it.

First, in the field **Phone Number** specify the phone number where you will send the test message.

Second, enter the text of the message in the field **Message**. And then click **Send**.

If the message is successfully sent, you will get a confirmation notification.



When modem is selected and test message is successfully sent, save the changes  and start the radioserver . After the radioserver is started, **Check modem** and **Send** (test message) will be unavailable. It will mean that now you are ready to send SMS messages from the radio and to the radio.

To send an SMS from the mobile phone to the radio, the message forwarded to the modem number should comply with one of the following formats.



The following symbols should be used:

- **Colon (:)** symbol: Prefix that indicates addressing the message to the specific recipient
- **<Radio/Talkgroup IP>**: Radio or talkgroup IP address of the recipient  
OR
- **<Radio ID>**: Radio ID of the target contact

- **Space symbol:** Indicates the beginning of the message text

Use the **Split Long Messages** option to guarantee that a message will not be cut.

#### Example

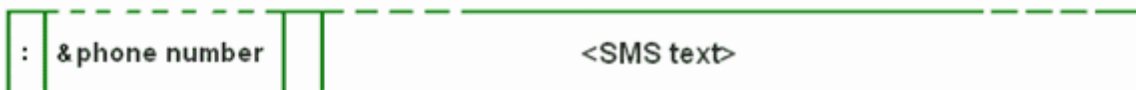
When SmartPTT Radioserver received the following message, it sends the message to radio 77 (or to talkgroup ID = 2):

- To the radio with radio ID = 77: *:12.0.0.77 SMS text*
- To the radio with radio ID = 77: *:77 SMS text*
- To talkgroup 2: *:225.0.0.2 SMS text*
- To multiple radios simultaneously: *:12.0.0.80,12.0.0.81,12.0.0.82,12.0.0.50 SMS text*
- To multiple radios simultaneously: *:9080,9081,9082,9050 SMS text*

#### NOTE

When only ID is specified (with no IP address of the radio or talkgroup), SMS can be sent only to the radio with the specified ID. To send a group SMS, it is necessary to use a full talkgroup IP address.

To send an SMS from a radio to a mobile phone, the message should comply with the following format.



The following symbols should be used:

- **Colon (:)** symbol: Prefix that indicates addressing the message to the specific telephone user.
- **<&phone number>**: Phone number of the SMS target (symbol "&" is used instead of "+" because there is no "+" symbol in the MOTOTRBO radios).
- **Space** symbol: Indicates the beginning of the message text.

#### Example

On receiving the message *:&71234567890 SMS text*, the radioserver sends it to the mobile radio

with the phone number +71234567890

- To several mobile subscribers simultaneously: `:&71234567890,&71234567890 SMS text`

## 1.4.8 File Receive

File Receive is used for sending files to MOTOTRBO radios. This function is even more necessary in field communication characterized by the absence of the Internet connection and other channels to transmit data.

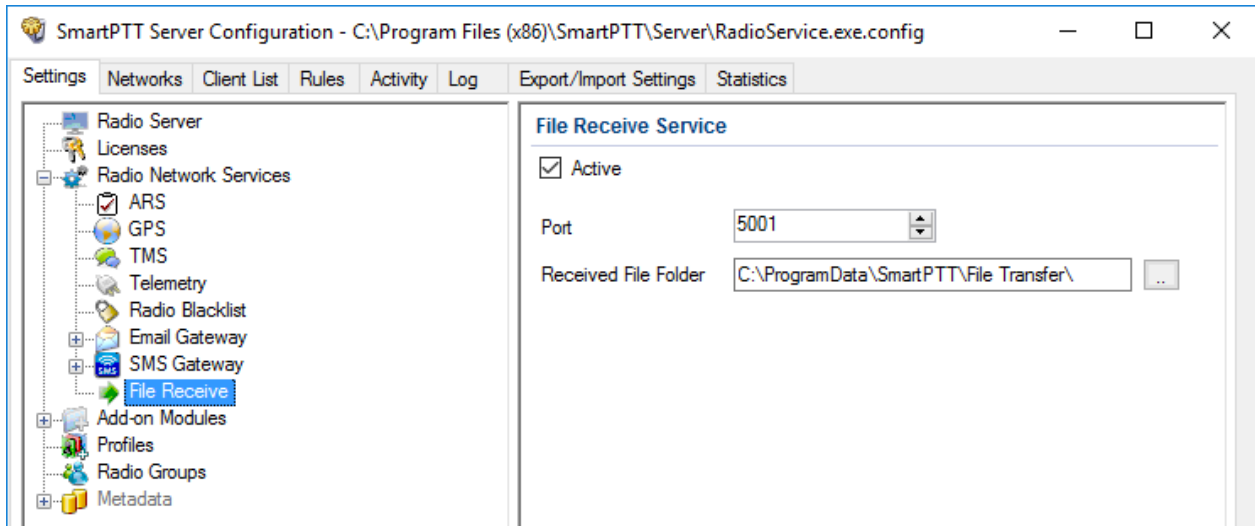
In version 2.0 SmartPTT File Transfer allows receiving files without the server application or base stations. You need to have only a radio connected to the PC by using USB port and the client application SmartPTT File Transfer version 2.0.

To enable this functionality, follow these steps:

1. Configure SmartPTT Radioserver settings.
2. Configure the radio with the help of *MOTOTRBO CPS*.
3. Configure routing settings for file transfer on a remote computer.
4. Configure the client application SmartPTT File Transfer 2.0.

## Configuring SmartPTT Radioserver

To configure the settings, select the **File Receive** menu item in the left setting tree of *SmartPTT Radioserver Configurator*. The **File Receive Service** pane opens:



**Active:** Enables the service.

**Port:** Port used by file receive service.

**Received File Folder:** Field to specify the folder name where received files are to be stored.

To apply the changes, save the new settings and restart the radioserver.

## Configuring Radio Settings in MOTOTRBO CPS

For the best file transfer rate a radio should be configured in the following way:

1. Open MOTOTRBO CPS and go to **General Settings** and configure the **TX Preamble Duration** parameter to be *60 ms*.
2. Go to **Network** and configure the **Max TX PDU Size** parameter to be *500 bytes*.
3. Clear **Data Call Confirmed** for the channel where the files are transmitted.

## Configuring Routing Settings for File Transmission

To configure file transmission correctly, add information on the new route for file transmission in the routing table of the PC to which a radio is connected.

To configure routing table, run Windows command prompt as Administrator:



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

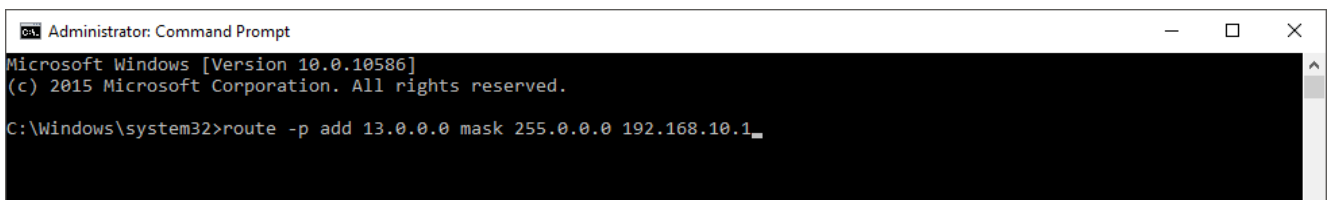
C:\Windows\system32>
```

To add the file transmission route, use Windows enter `route -p add 13.0.0.0 mask 255.0.0.0 192.168.X.X`. In this message the following is used:

- `route`: is a command to add a route
- `-p`: The key for adding a route into the list of fixed routes
- `add`: adding the route
- `13.0.0.0`: IP address of all radios available in the radio network
- `mask 255.0.0.0`: Network mask
- `192.168.X.X`: Radio IP address

### Example

To transmit data packets from the radio with IP address `192.168.10.1` (radio IP address can be found in the *MOTOTRBO CPS* application, **Network** menu), the following command needs to be entered: `route -p add 13.0.0.0 mask 255.0.0.0 192.168.10.1`



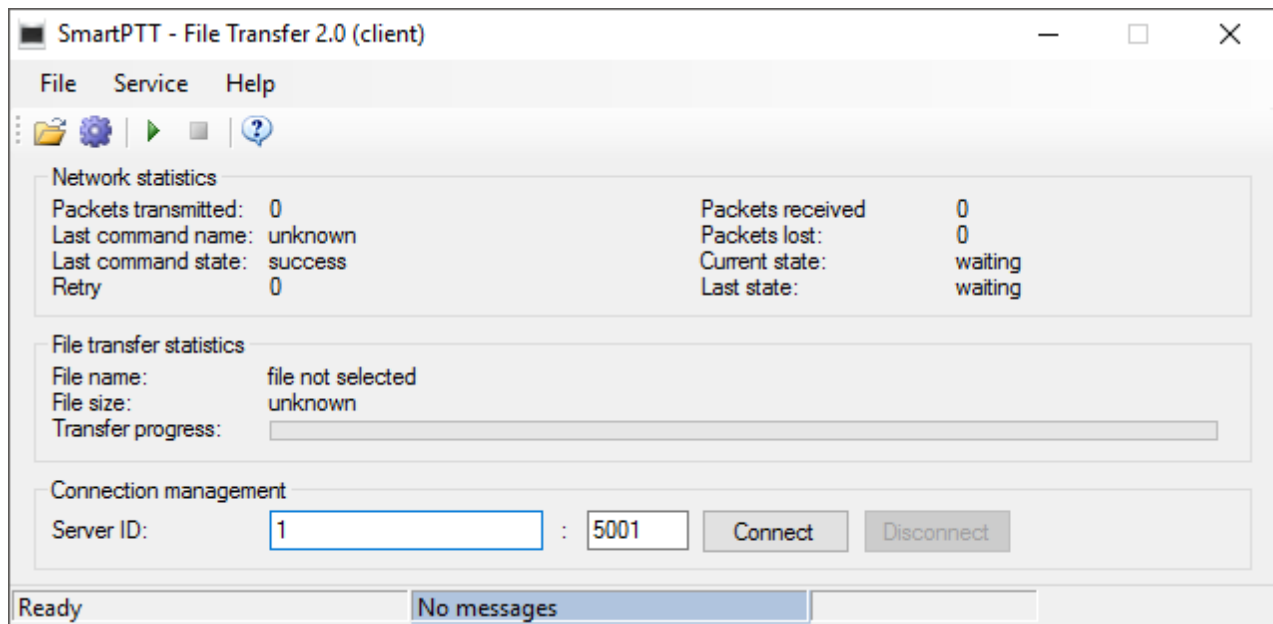
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>route -p add 13.0.0.0 mask 255.0.0.0 192.168.10.1
```

## Configuring SmartPTT File Transfer Settings

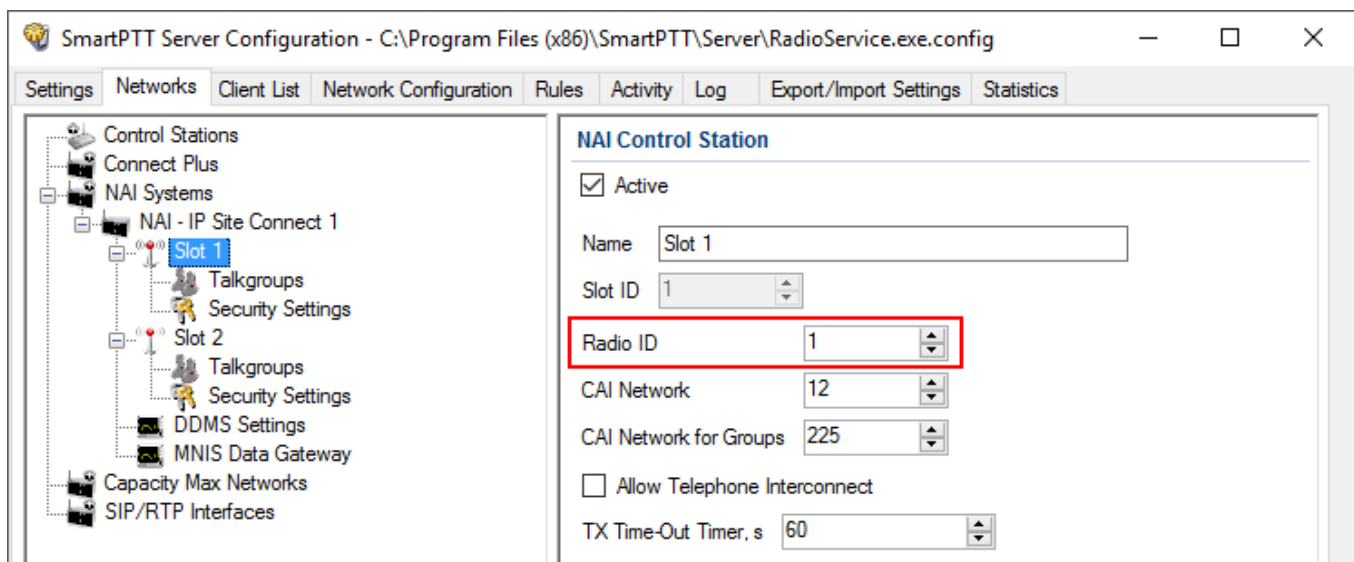
1. Download and install the latest version of the application SmartPTT File Transfer ([http://www.smartptt.com/demo\\_versija.html](http://www.smartptt.com/demo_versija.html)).

## 2. Launch **SmartPTT File Transfer Client**:

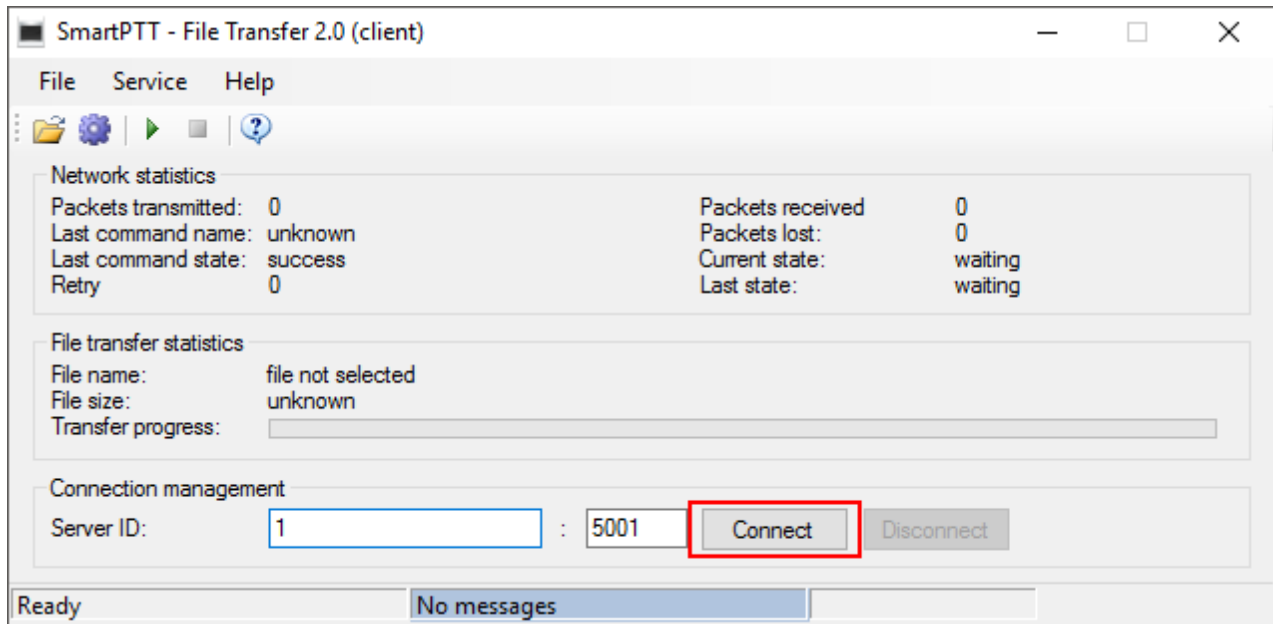


3. In the **Server ID** field, enter the radio ID of NAI - IP Site Connect, which will be used for file transmission.

The radio ID is set in *SmartPTT Radioserver Configurator*, in the **NAI - IP Site Connect** → **NAI Control Station** pane in the **Radio ID** field.

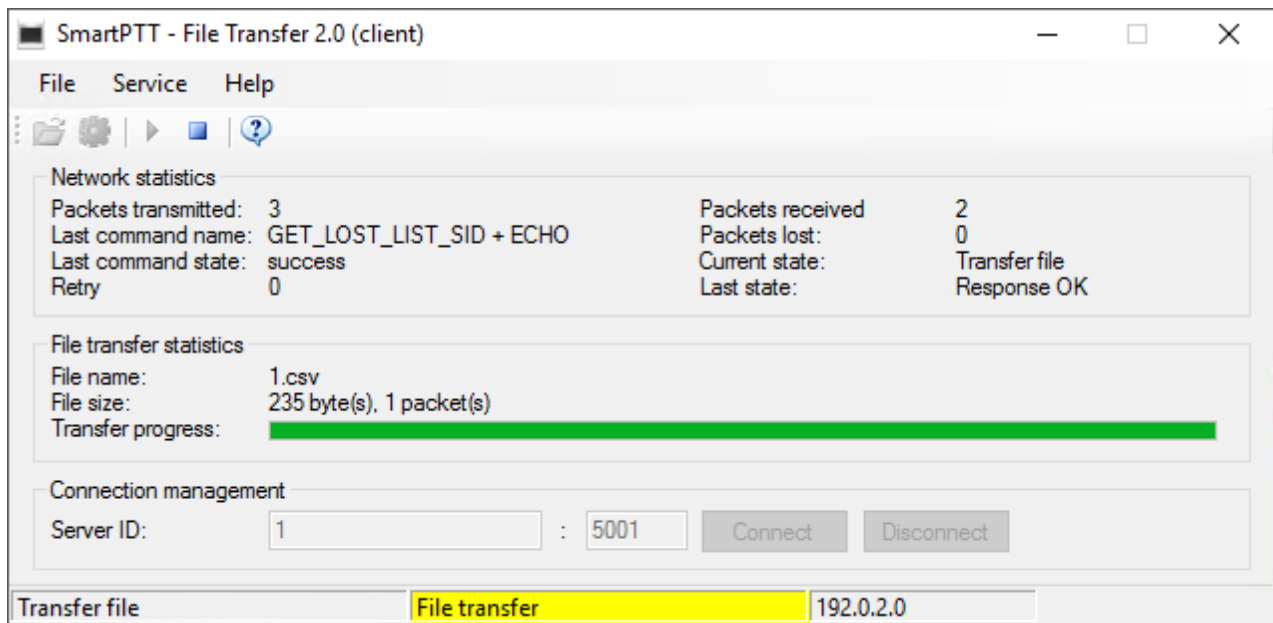


- In SmartPTT File Transfer, click **Connect** to connect to the radioserver.

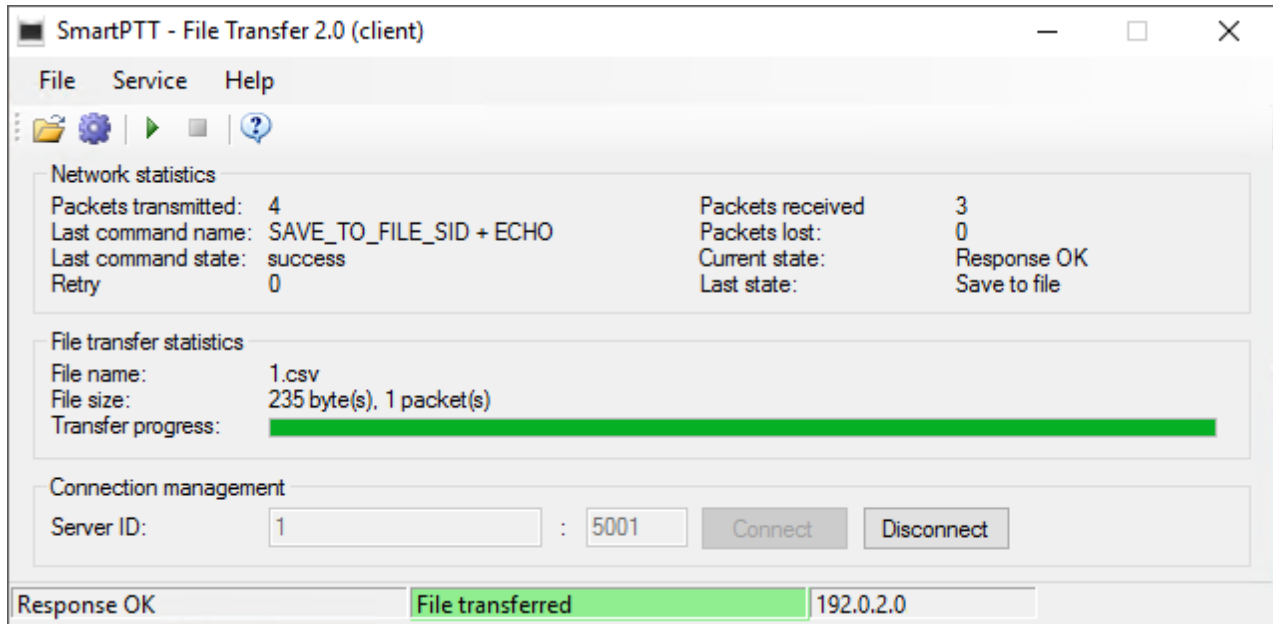


## File Transmitting

Select file to transmit (**File** → **Select File**) and click the **Start File Transfer** button ►. At the bottom of the window a record about the ongoing file transmission process appears.



As soon as the file is successfully transmitted, the corresponding notification appears at the bottom of the window.



## NOTE

For more information about the settings of SmartPTT File Transfer, see *SmartPTT File Transfer User Guide*.

## 1.5 Add-on Modules

### 1.5.1 Tallysman

SmartPTT provides a more efficient radio monitoring that works in the Lone Worker mode. The option is compatible with MOTOTRBO DM/DP 3000 and 4000 series radios.

SmartPTT ensures the following features for the generic option board with the Tallysman Sprite™ TW251 firmware:

- Mandown, or activating the alarm signal if the radio is tilted (its orientation does not corresponds to the parameters set for the option board in Tallysman Sprite Configurator).
- Heartbeat messages. Messages that provide information about radio presence in the radio network. If message delivery failed, *SmartPTT Dispatcher* is notified about the radio unavailability. The radio is also informed about radioserver unavailability (for example, when the channel is busy).



## Example

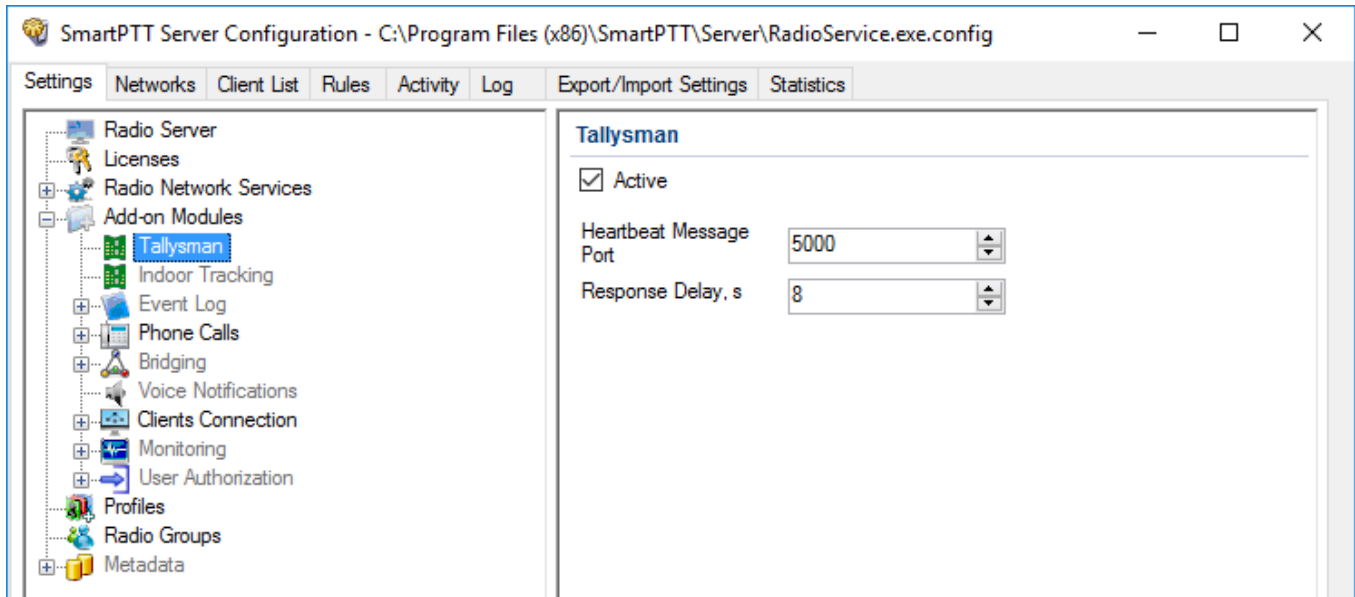
When the radio tilt changes, a signal is played on the radio. The signal stops after the radio is returned to its normal position. If not, an emergency alarm is sent to SmartPTT Radioserver. The emergency alarm LED on the radio can be turned off by a long press on the emergency alarm button (depends on the radio MOTOTRBO CPS settings).

For proper operation of the radios with the built-in option board with the Tallysman Sprite™ TW251 firmware, do the following radio settings in MOTOTRBO CPS:

1. Activate option board on the selected channel by selecting the **Option Board** check box.
2. Activate the Emergency Alarm Indication option and select digital signaling system from the list in the Emergency System field. To set up a signaling system, go to **Signaling Systems** → **Digital Emergency** item.

The screenshot displays the configuration page for 'Rep1\_SlotA' in the SmartPTT PLUS Radioserver Configurator. The interface is split into RX and TX configuration panels. In the RX panel, the 'Option Board' checkbox is checked, and the 'Emergency Alarm Indication' checkbox is also checked. In the TX panel, the 'Emergency System' dropdown menu is set to 'Sys1'. The left sidebar shows a tree view of settings categories, with 'Rep1\_SlotA' selected under 'Channels'.

To activate Tallysman, click **Tallysman** in the setting tree of *SmartPTT Radioserver Configurator* and select the **Active** check box.



**Heartbeat Message Port:** UDP port to receive messages about the radio presence in the network. This value must match Host UDP Port in the option board configurator (the Heartbeat item, the SmartPTT GOB Configurator application). Use the default value of *5000*.

**Response Delay, s:** The time period that passes before SmartPTT Radioserver sends heartbeat message confirmation to the radio. Set the value taking into consideration the network load. Otherwise, if the radio does not receive acknowledgment, the radio gets a signal about radioserver unavailability.

## 1.5.2 Indoor Tracking

Big organizations with huge premises require constant control over their employees displacement inside buildings. For this purpose Indoor Tracking system was implemented.

Indoor Tracking system allows getting data from special beacons and transmitting it to *SmartPTT Dispatcher* or any other client application using API. Contact our technical support (<http://support.smartptt.com/hc/en-us>) for SmartPTT Client API documentation.

Currently, SmartPTT system supports the following technologies and products:

- **iBeacon technology:** With MOTOTRBO radios with the firmware version 2.6 and above, and beacons that support iBeacon technology.

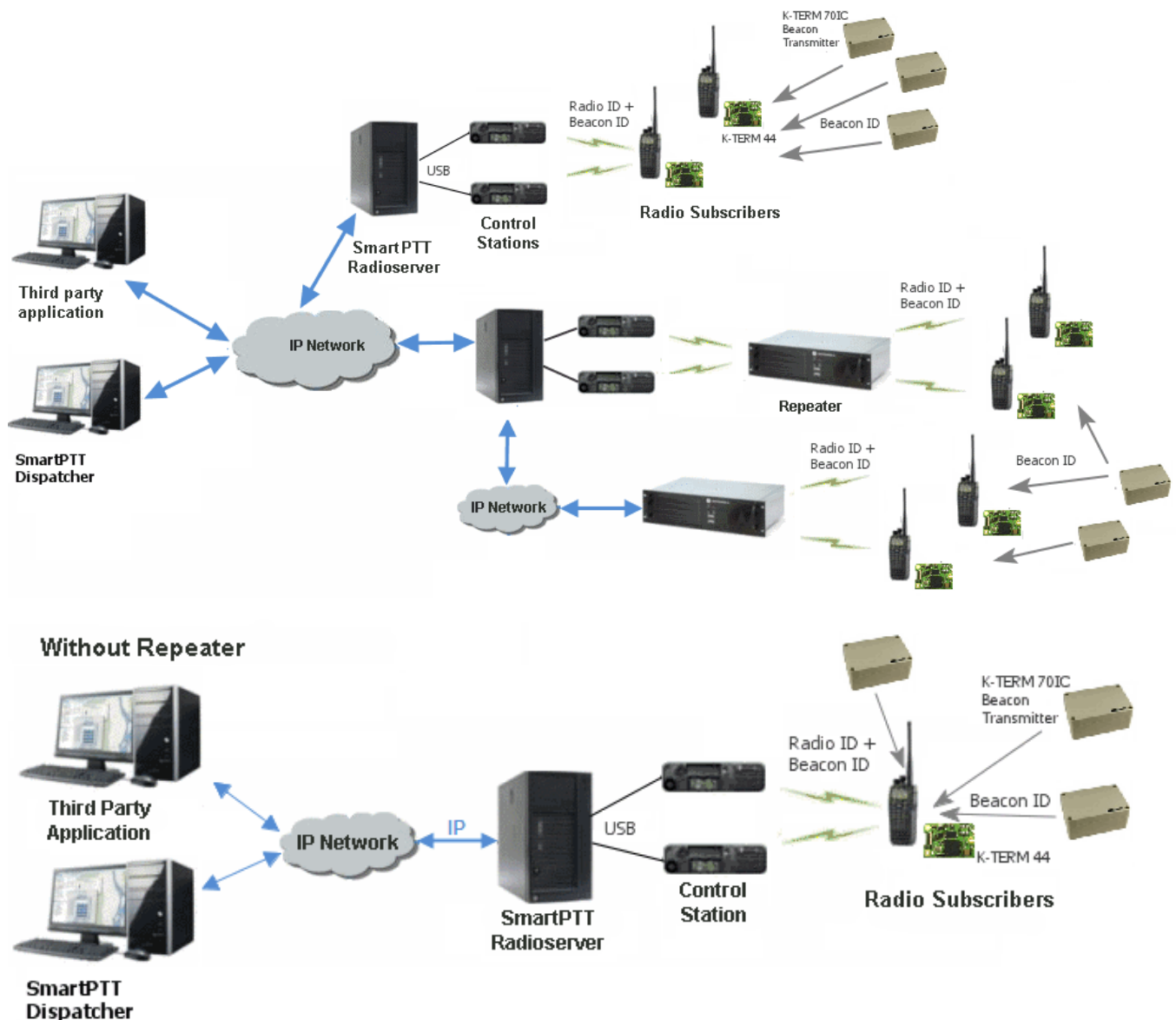
- **BluFi Wireless:** With option boards (Connect-RTL RF800) and beacons (Connect-RTL RF800).
- **Kilchherr Elektronik AG:** With option boards (K-TERM 44) and beacons (K-TERM 70IC Beacon Transmitter).

Connect Plus systems support Indoor Tracking based on the iBeacon technology only.

**NOTE**

Indoor Tracking functionality requires the corresponding license. For more information on how to install licenses, see [Licenses](#).

The following scheme shows how SmartPTT Radioserver gets radio location data:



## iBeacon-based technology scheme

Each installed beacon is transmitting at an interval ranging from a fraction of a second to several minutes the data packages in the following format:

- *iBeacon prefix*: A title of a package
- *UUID*: A unique identifier of the beacon
- *Major*: A group parameter of the beacon
- *Minor*: The individual parameter of the beacon in the group
- *Tx power*: The strength of the signal, transmitting by the beacon

The radio with the preconfigured CPS settings (see [below](#)) receives the data packages from the beacons which identifiers (UUID) are set in the CPS settings, and transmits them to SmartPTT Radioserver via repeater or control station.

## BluFi scheme

The RF800 beacons operate in a continual **Sleep** → **Transmit** → **Sleep** → **Transmit** mode. When a beacon awakes from its sleep cycle, it transmits its allocated code during the transmit phase, and then returns to sleep phase.

Portable radios operate in the **Sleep** → **Listen** → **Sleep** → **Listen** mode. When a portable radio awakes from its sleep cycle, it listens for any transmitted beacon codes during its listen phase, and then determines the current active beacon. If a new active beacon is different from the previous active beacon, a beacon update status message (a special TMS message) is sent via the radio network to SmartPTT Radioserver. For more information on BluFi beacons and option boards, see the manufacturer's documentation on the products.

### NOTE

Connect-RTL S RF800 option boards transmit data in TMS messages. Therefore, it is necessary to have TMS enabled.

## Kilchherr scheme

Each beacon installed is continually transmitting commands, like *Detect*, *Keep Alive*, *Lost*, which contain unique **Beacon ID** (set in K-Term CPS). When a radio gets closer to the beacon, the built-in option board receives **Beacon ID** and then transmits it with the **Radio ID** to SmartPTT

Radioserver via repeater or control station. Further data processing can be handled by *SmartPTT Dispatcher* or any third party application, connected to the radioserver using API. For more information on Kilchherr beacons and option boards see the manufacturer's documentation on the products.

**WARNING**

For the **Kilchherr** and **BluFi** option boards, in network systems with MNIS service enabled, make sure that the ID set in the option board settings (where data is to be sent) should match **MNIS Application ID**. In network systems without MNIS service enabled, any ID can be set in the option board settings (where data is to be sent). However, it is necessary that **Data call confirmed** should be unselected in the radio settings. In networks based on control stations it is necessary that the ID set in the option board settings should match **Radio ID** set in the control station settings.

To use the **Indoor Tracking** feature based on the iBeacon technology, ensure that the MOTOTRBO radio meets the following requirements:

- The radio has the firmware version 2.6 and above
- The radio [supports Indoor-positioning](#)
- The radio is [configured properly](#) in MOTOTRBO CPS

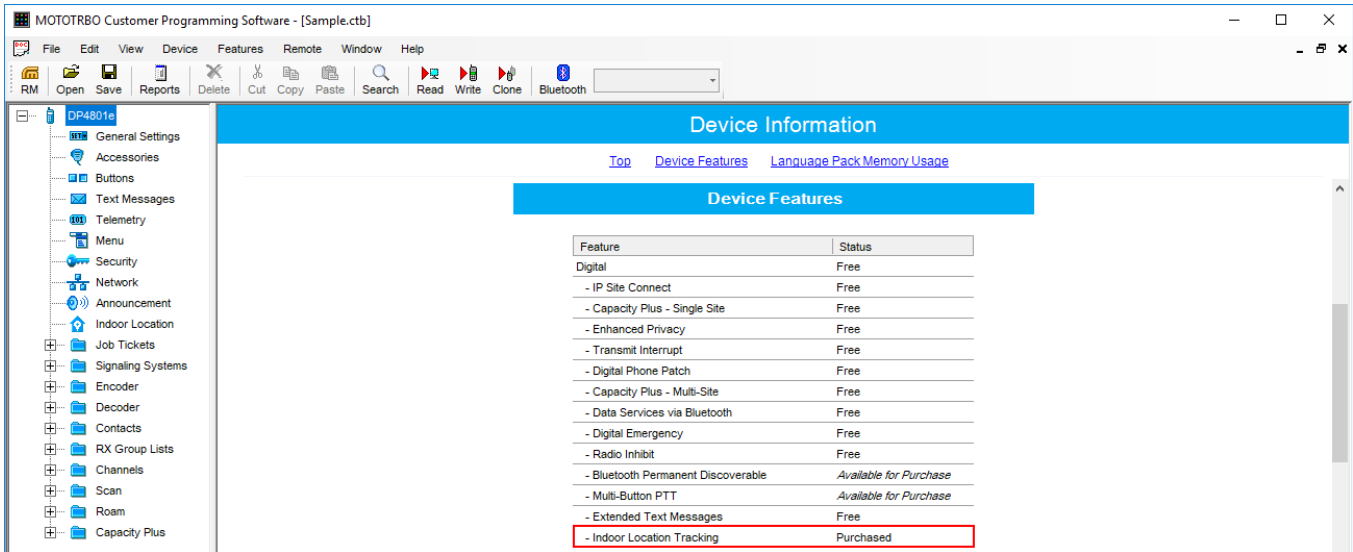
### 1.5.2.1 Configuring Indoor Tracking in MOTOTRBO CPS

**NOTE**

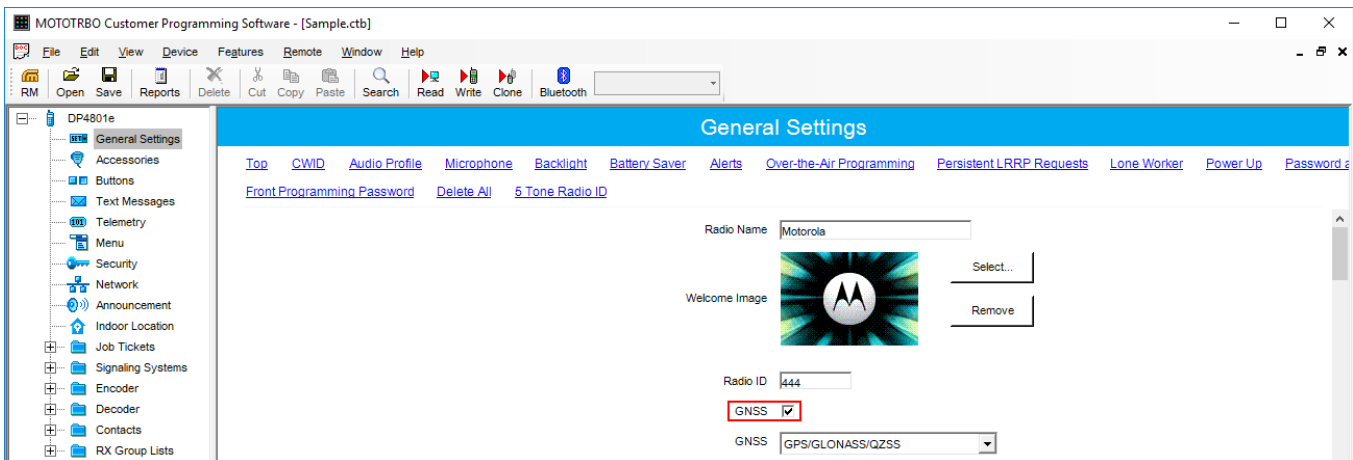
Below is a description of the Indoor settings only. The complete information on how to program the MOTOTRBO equipment step by step, please refer to *SmartPTT PLUS Installation & Configuration Guide*.

To configure the MOTOTRBO radio for use of the Indoor Tracking feature based on the iBeacon technology, follow these steps:

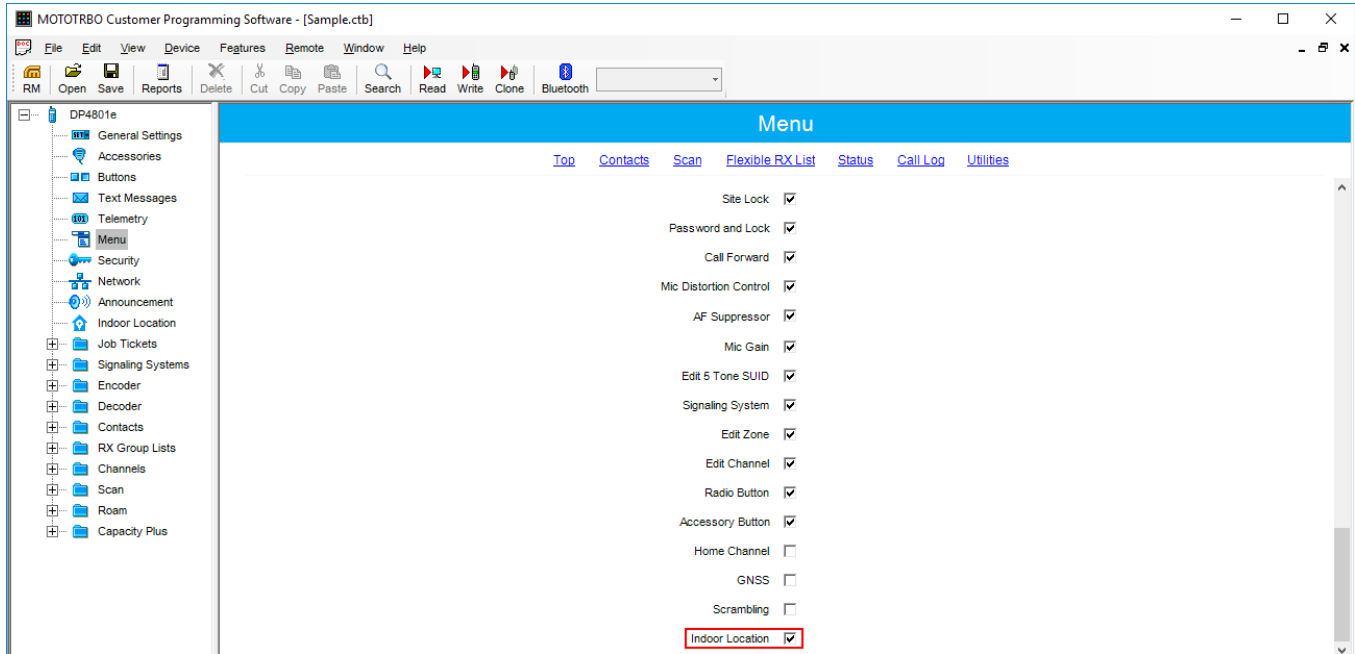
1. Launch MOTOTRBO CPS with the 13.0 version or above, and perform the following actions:
  - a. In the left pane, select the desired radio and in the **Device Information** tab verify the **Indoor Location Tracking** field has the *Purchased* value.



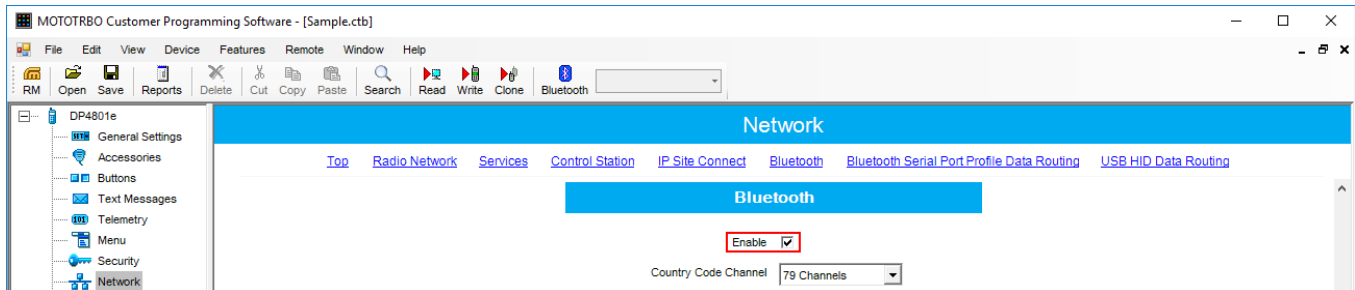
- b. In the left pane, select **General Settings**. In the **General Settings** window, select the **GNSS** check box.



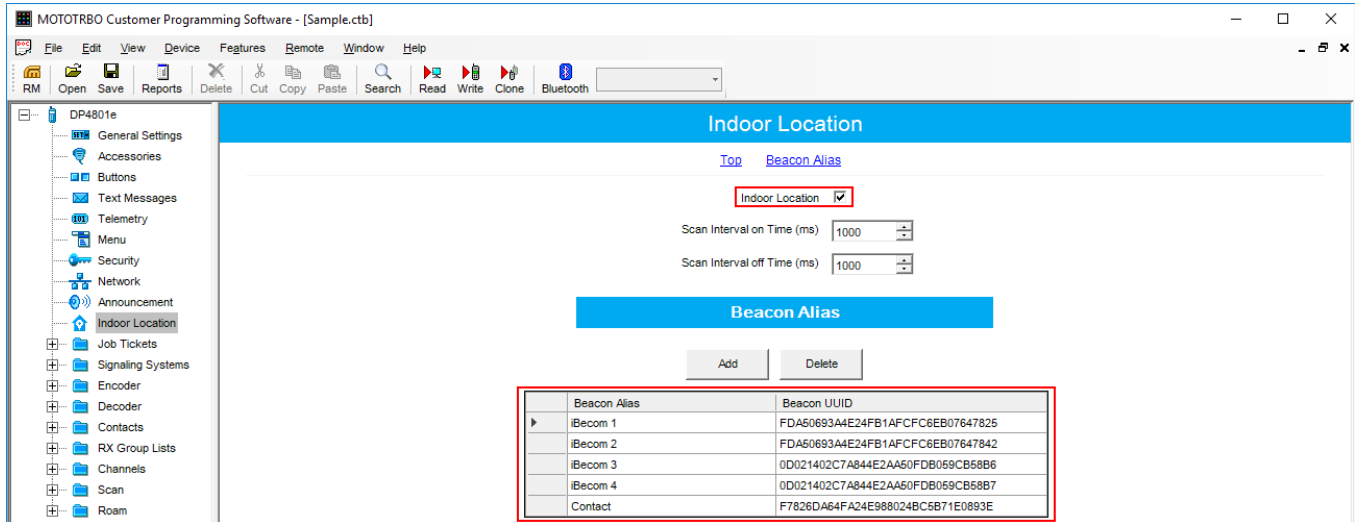
- c. In the left pane, select **Menu**. In the **Utilities** area of the **Menu** pane, select the **Indoor Location** check box.



- d. In the left pane, select **Network**. In the **Bluetooth** area of the **Network** pane, select the **Enable** check box.



- e. In the left pane, select **Indoor Location**. In the **Indoor Location** pane, select the **Indoor Location** check box.



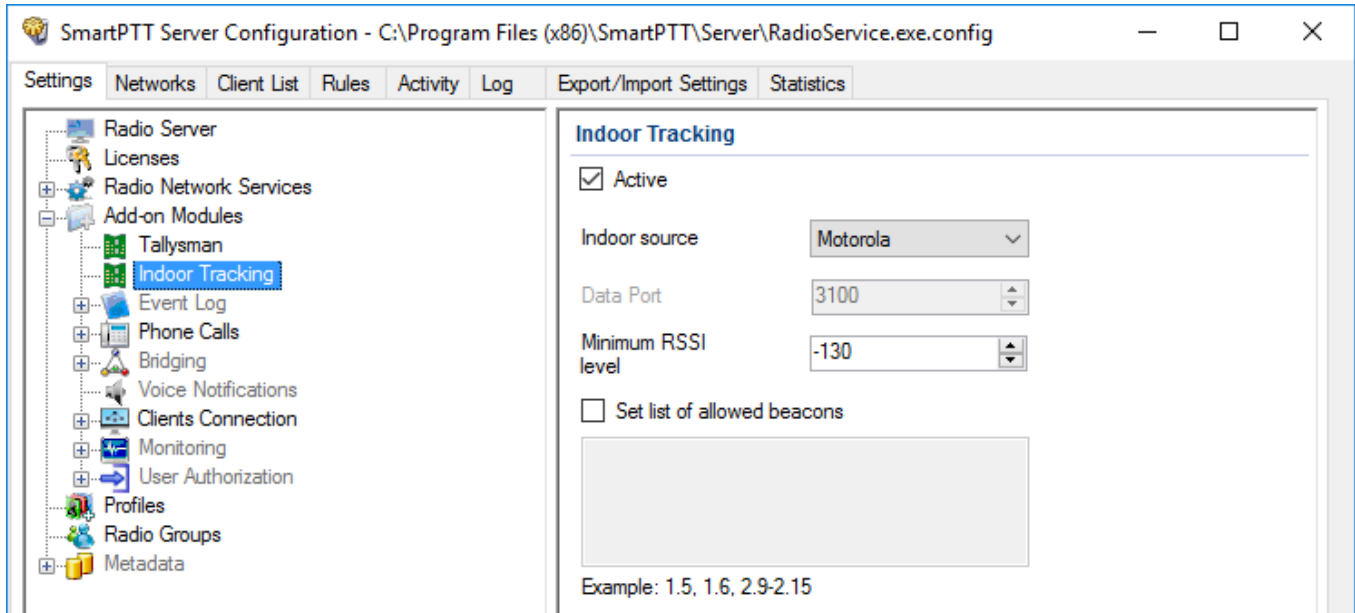
- f. In the **Beacon Alias** area, add the beacons and specify their names and identifiers (UUID).
2. Configure Bluetooth in the radio to activate Indoor-positioning. For that, with use of radio menu buttons, perform the following actions:
    - a. Set the parameter **Main Menu** → **Bluetooth** → **My Status** → **On**.
    - b. Set the parameter **Main Menu** → **Bluetooth** → **Indoor Location** → **Enabled**.



## 1.5.2.2 Configuring Indoor Tracking

To configure **Indoor Tracking** in SmartPTT Radioserver Configurator, follow these steps:

1. In the left pane of *SmartPTT Radioserver Configurator*, select **Indoor Tracking**.



2. In the **Indoor Tracking** pane, perform the following actions:
  - a. Select the **Active** check box to activate Indoor Tracking.
  - b. From the **Indoor source** list, select the desired Indoor-positioning technology:
    - *Motorola*: If you use iBeacon technology
    - *BluFi*: If you use BluFi Wireless technology
    - *Kilchherr*: If you use Kilchherr Elektronik AG technology
3. Only for *Kilchherr* technology: In the **Data Port**, enter the UDP port for listening to Beacon ID.
4. Only for *iBeacon* technology: In the **Minimum RSSI level**, enter the minimum value of the signal strength, that radio receives from the beacon.

### NOTE

SmartPTT Radioserver does not process the signals with power that is lower than the specified level.

5. *Optional:* Select the **Set list of allowed beacons** check box and specify the numbers of the beacons which data must be processed by SmartPTT Radioserver. Use the following format:
  - If you use *Motorola* technology: Specify the numbers of the beacons in the *Major.Minor* format, where the *Major* is the beacons number, *Minor* is the individual number of the beacon in the group.
  - For the *BluFi* or *Kilchherr* technology: Specify the Beacon IDs set in the beacons parameters.

**NOTE**

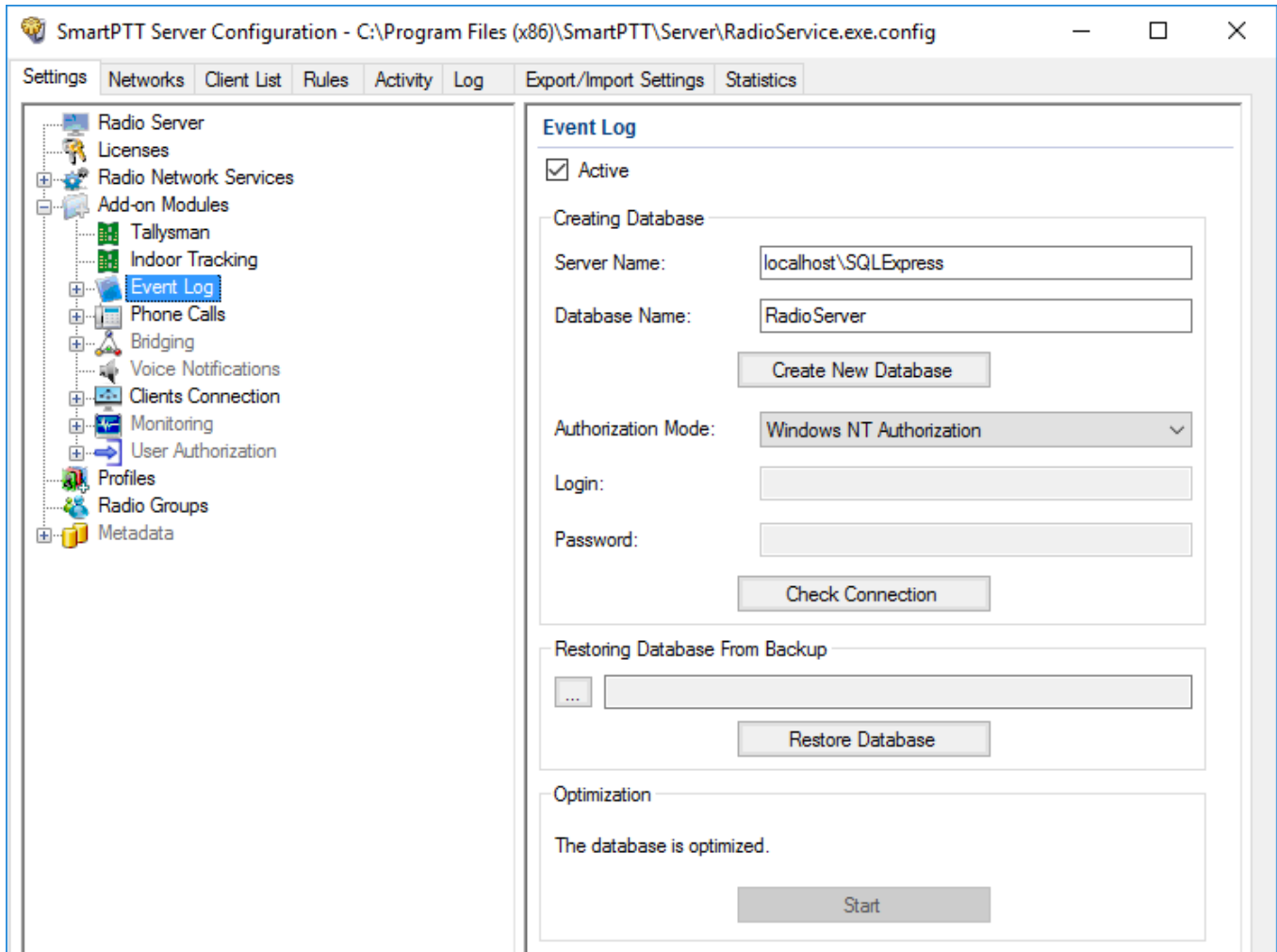
If the **Set list of allowed beacons** check box is not selected, the radioserver processes data from all the beacons.

## 1.5.3 Event Log

Event Log tracks all events from all dispatch systems connected to the radioserver. Events are registered in the event log even if *SmartPTT Radioserver Configurator* is closed.

To activate First activate the event log by checking off **Enable Event Logging**. To do it, select **Event Log** item in the setting tree in *SmartPTT Radioserver Configurator*.

Then create the database for the log.



### NOTE

To activate Event Log on radioserver, install the corresponding license. For more information on how to install licenses, see [Licenses](#).

To create a new database, enter the server name and the database name in the **Server Name** and the **Database Name** fields, and click **Create New Database**. If creation is successful, a message

about successful database creation appears. If a database is not created, the cause of failure will be displayed at the bottom of the window.

**NOTE**

Database creation process at SmartPTT Radioserver is similar to the database creation process at *SmartPTT Dispatcher*.

For the database server installed together with the SmartPTT Radioserver enter the name using the following format: *<Name of computer\SQLExpress>* (for example, *MYCOMP\SQLExpress*).

Select **Authorization Mode** between the two:

- **Windows NT Authorization:** The user who has logged into the Windows system, must be listed in the SQL server's list of users to make connection.
- **SQL Server Authorization:** You must have the login name and password of the account with SQL server access.

Click **Check Connection**. In case of successful authorization the message *"The connection is established successfully!"* appears. If authorization fails, the cause will be displayed at the bottom of the window.

To restore the event log database from the backup, select the required database backup file in the **Path** field and click **Restore Database**.

**NOTE**

To set up the auto backup of the event log database, go to the [Automatic Database Backup](#) window.

To optimize the event log database, click the **Start** button in the **Optimization** block. The optimization of the event log database accelerates the database query processing when getting a large amount of GPS data or events. For example, when building the **Radio Activity Reports**, **Radio Locations**, **Events for Period** and other reports in *SmartPTT Dispatcher*.

**NOTE**

The optimizing feature is applicable only to non-optimized event log databases created before the release of SmartPTT 9.0 and higher.

Before performing the optimization, ensure that the radioserver is stopped.

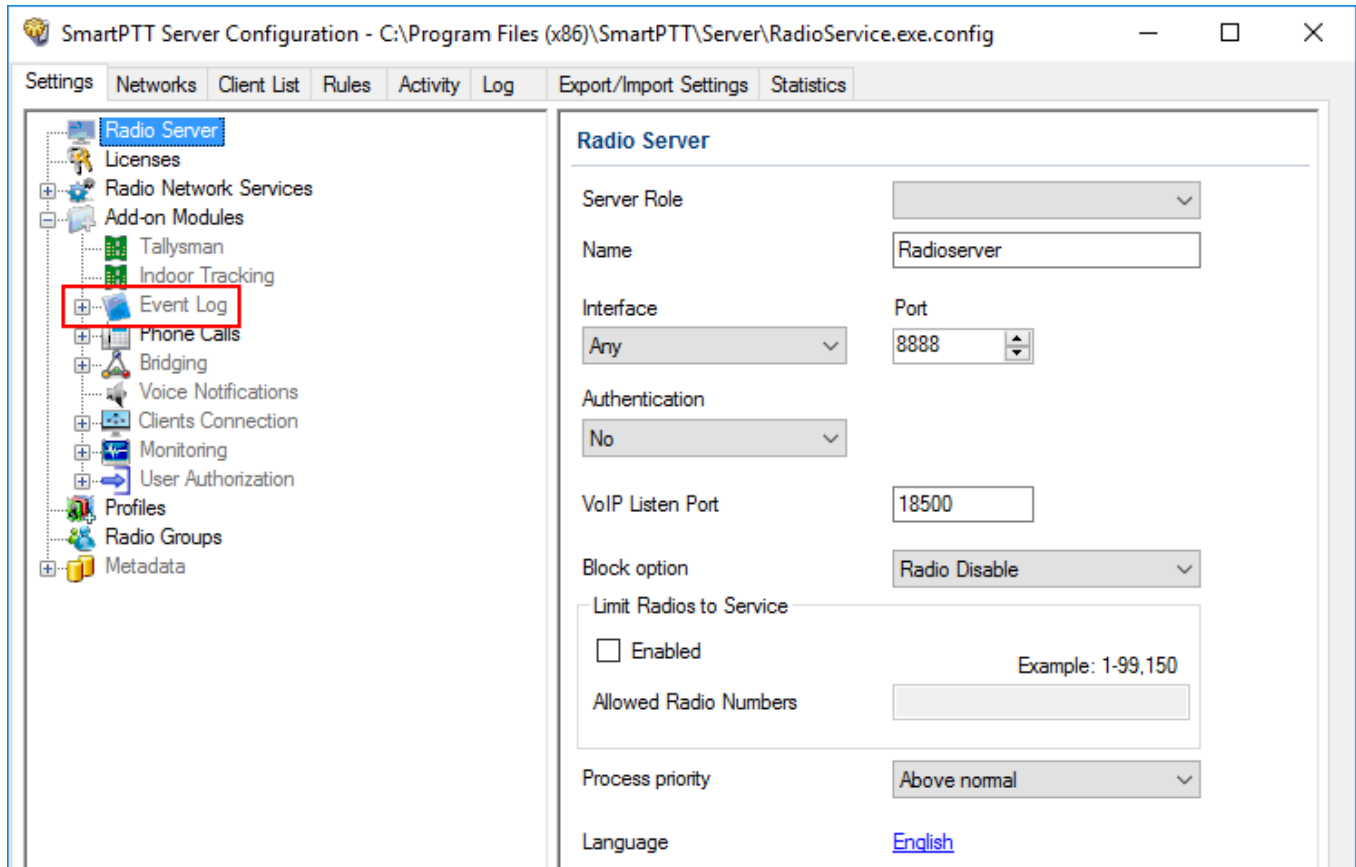
If the event log database is optimized, the **Optimization** block shows the corresponding message and the **Start** button is inactive.

The following instructions are related to the event log:

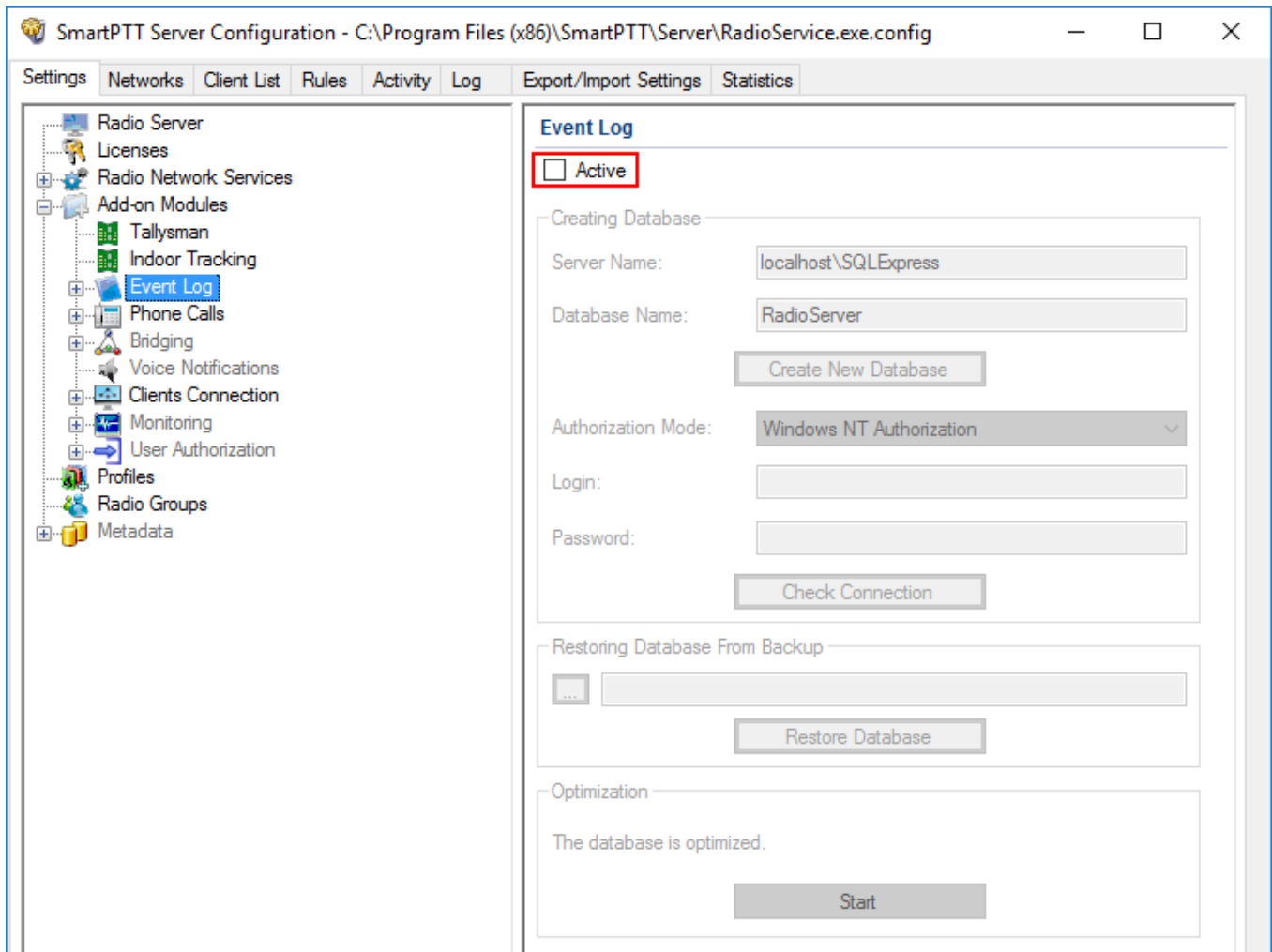
## Creating Database

To create the event Log database, follow these steps:

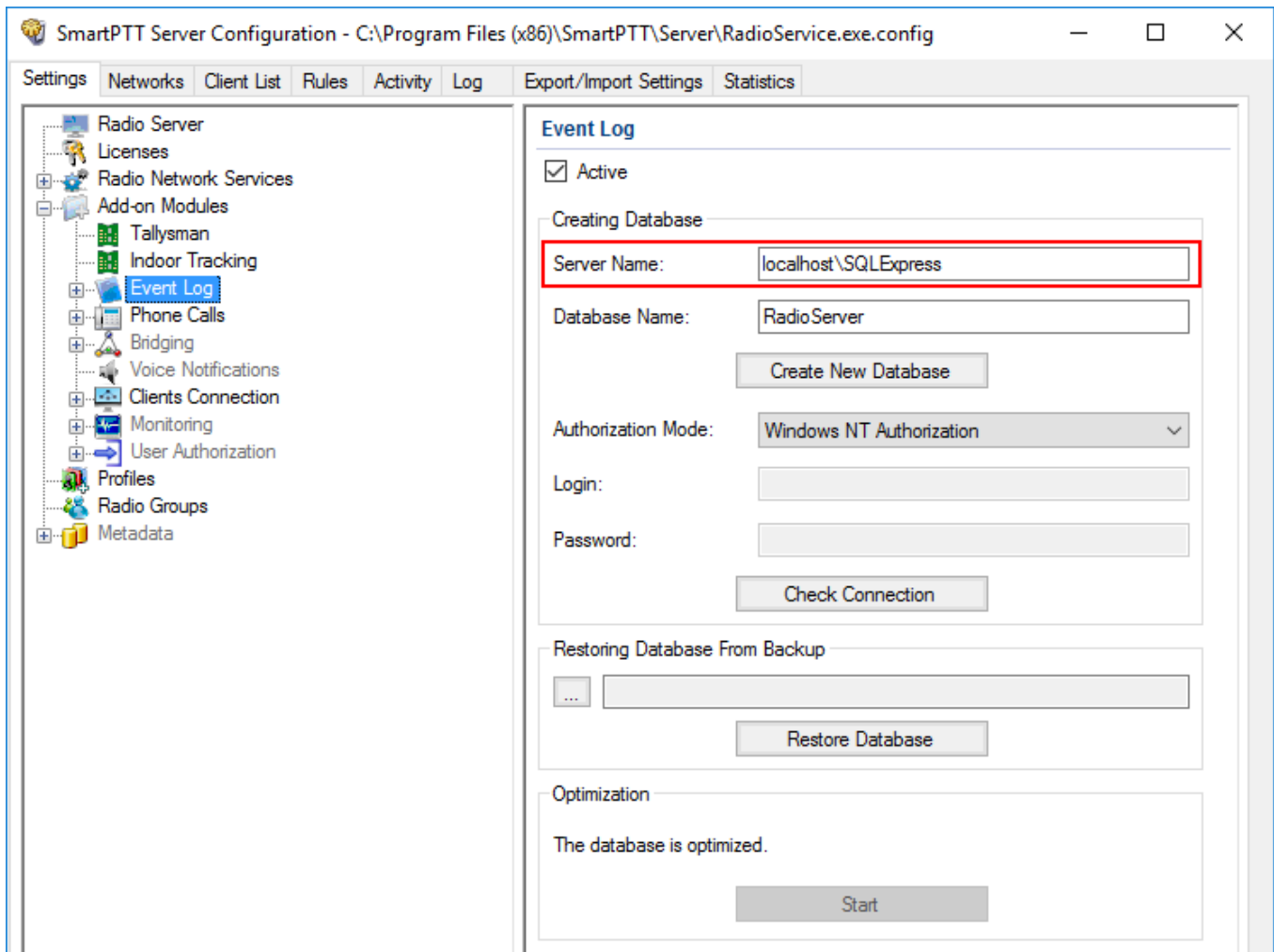
1. In the left pane of the **Settings** tab, expand **Add-on Modules** node and click **Event Log**.



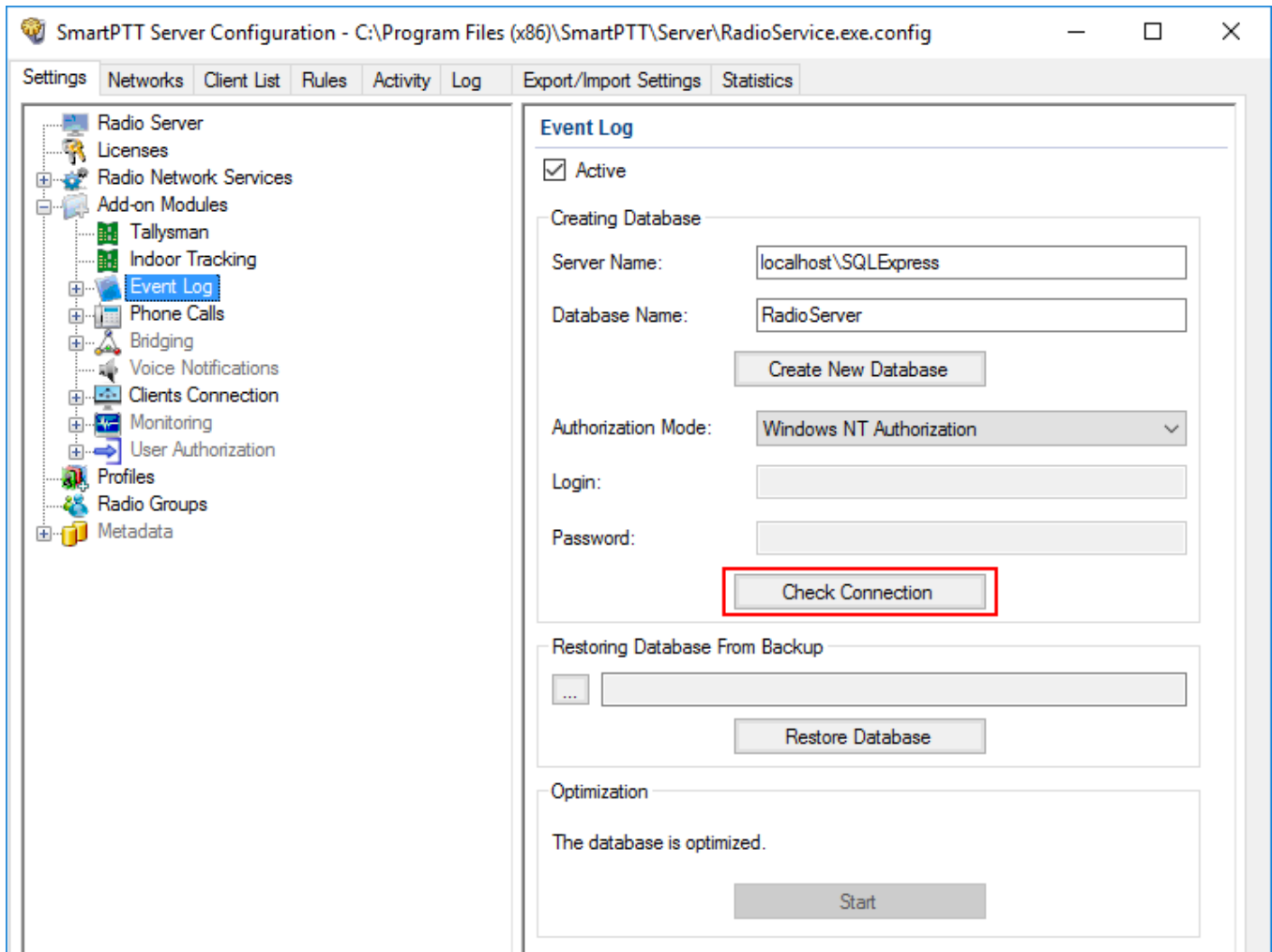
2. Make sure that the **Active** check box is selected in the **Event Log** pane.



3. In the **Server name** field, enter the name of the SQL Server. You can use either *<IP-address of your computer>\<Your SQL Server name>* or *localhost\<Your SQL Server name>* format:

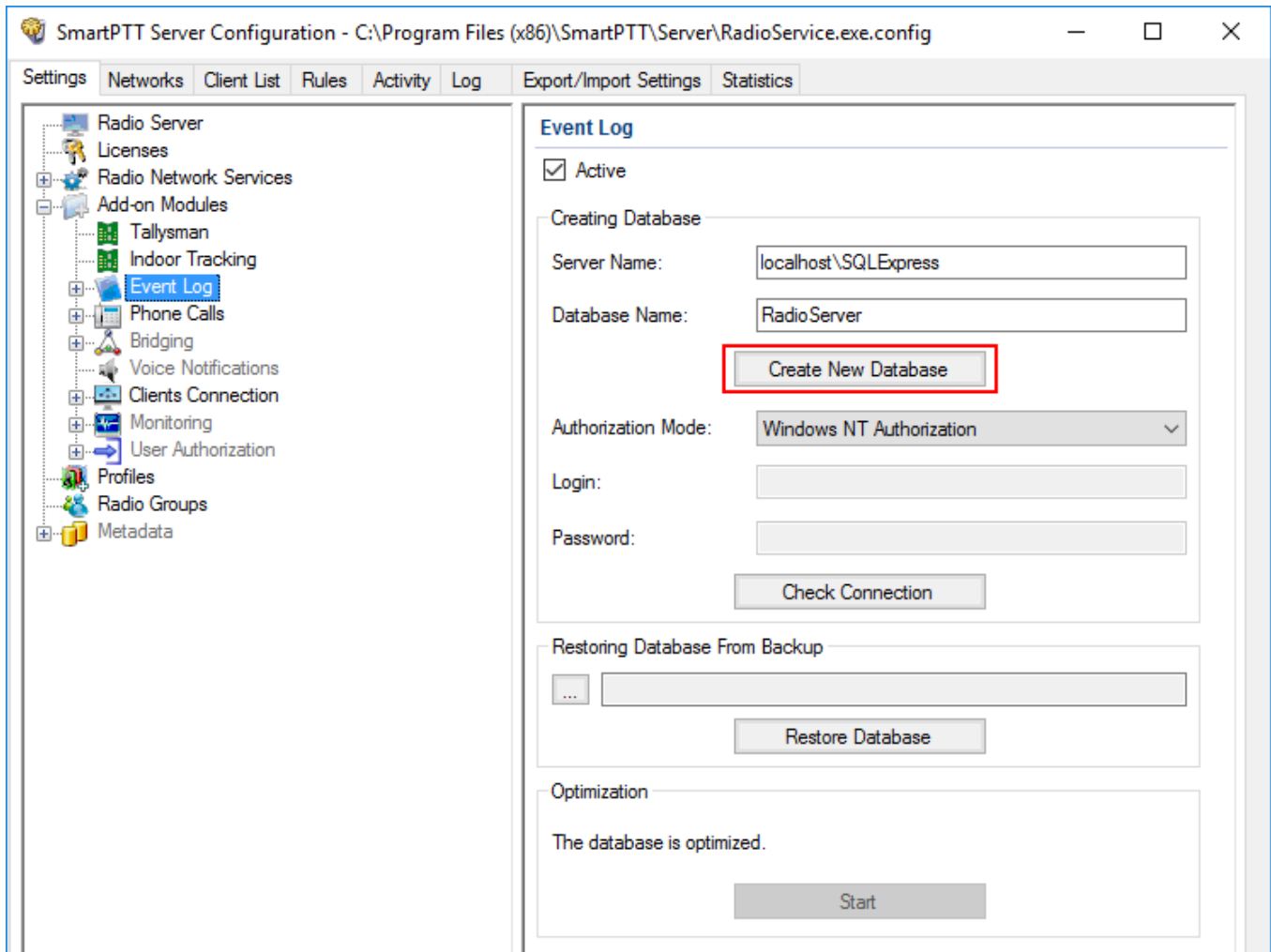


4. In the **Database Name** field, enter the name of a local event log database.

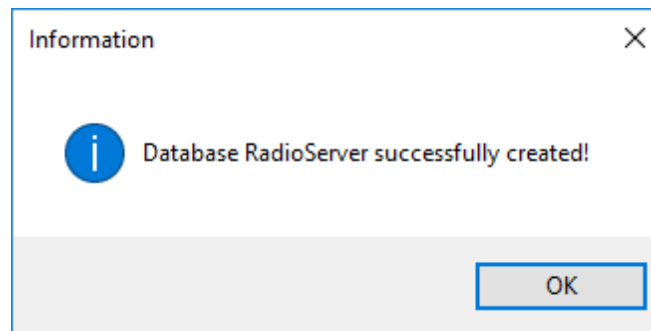





5. Click **Create New Database**.



If creation is successful, the following message appears.



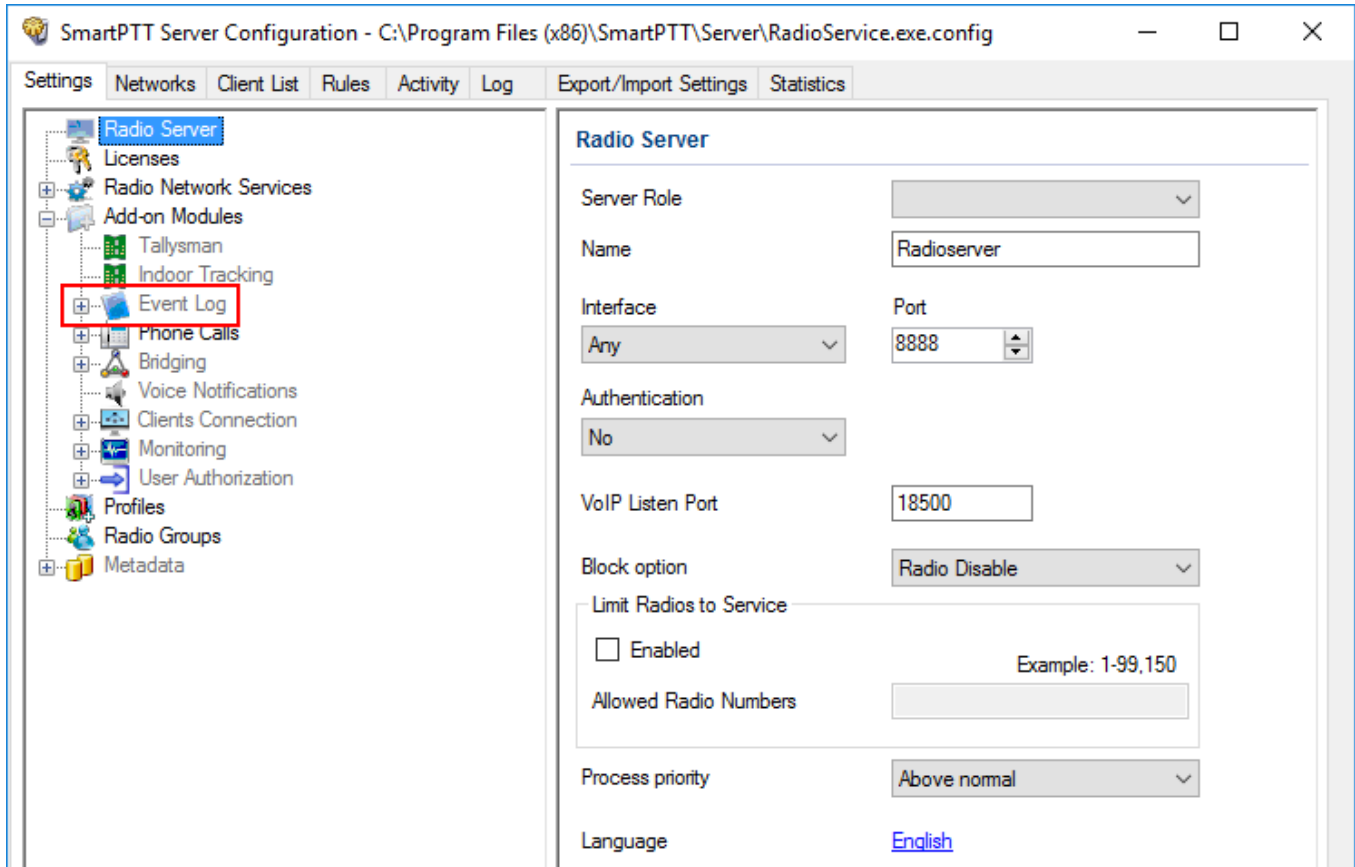
6. Click **Save**  to save changes.

7. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

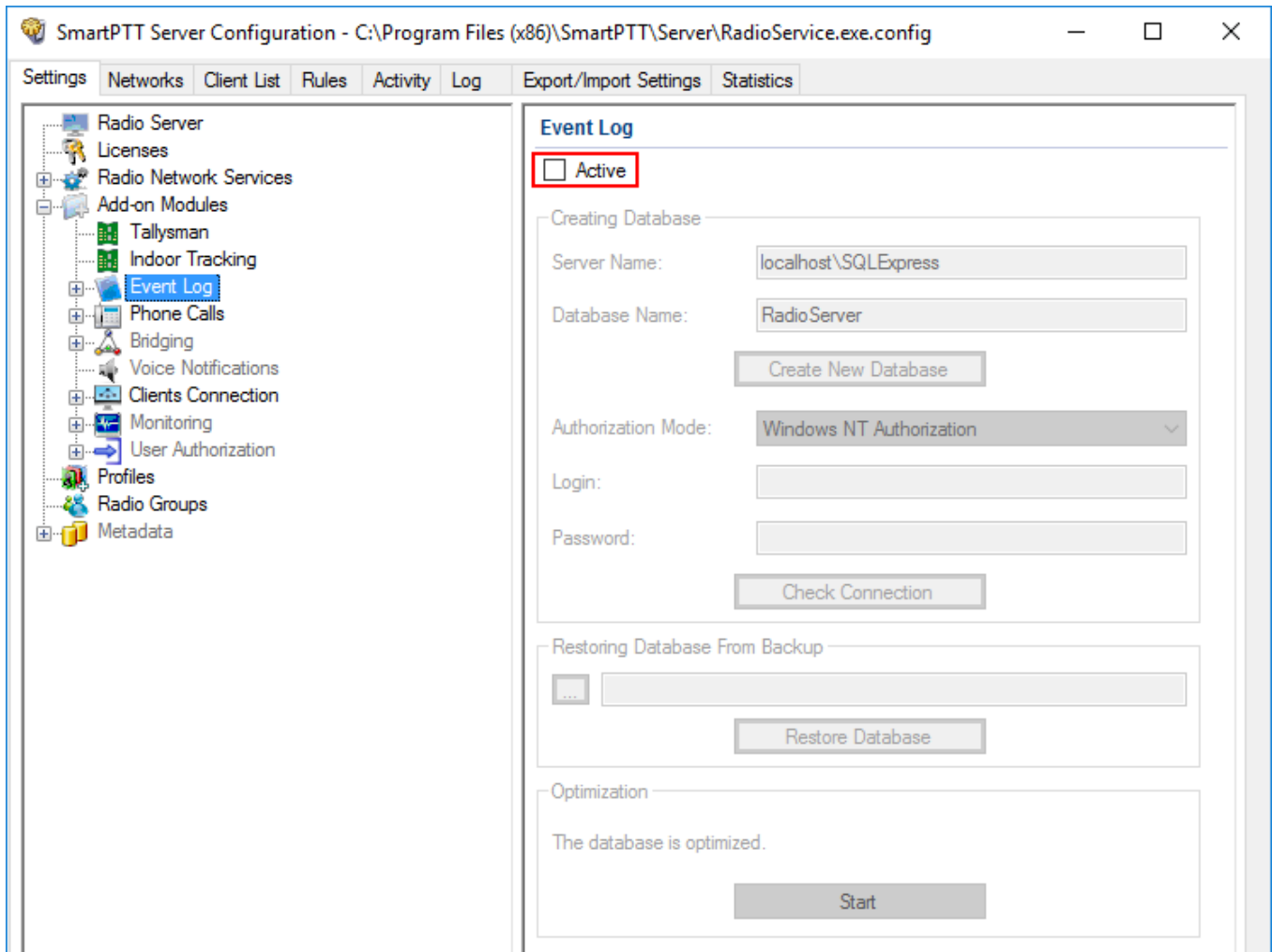
## Connecting Local Database

To connect to the local event Log database, follow these steps:

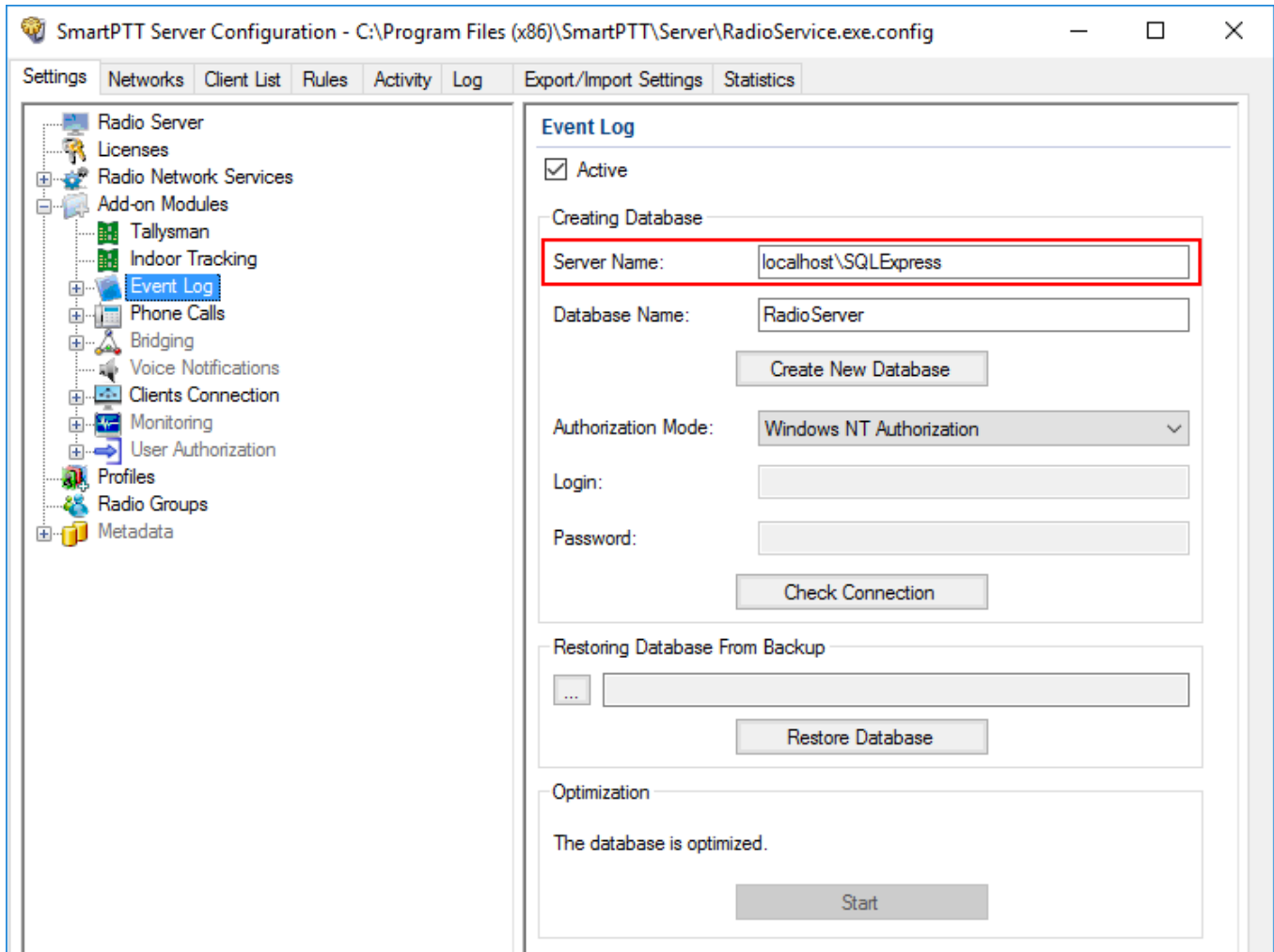
1. In the left pane of the **Settings** tab, expand **Add-on Modules** node and click **Event Log**.



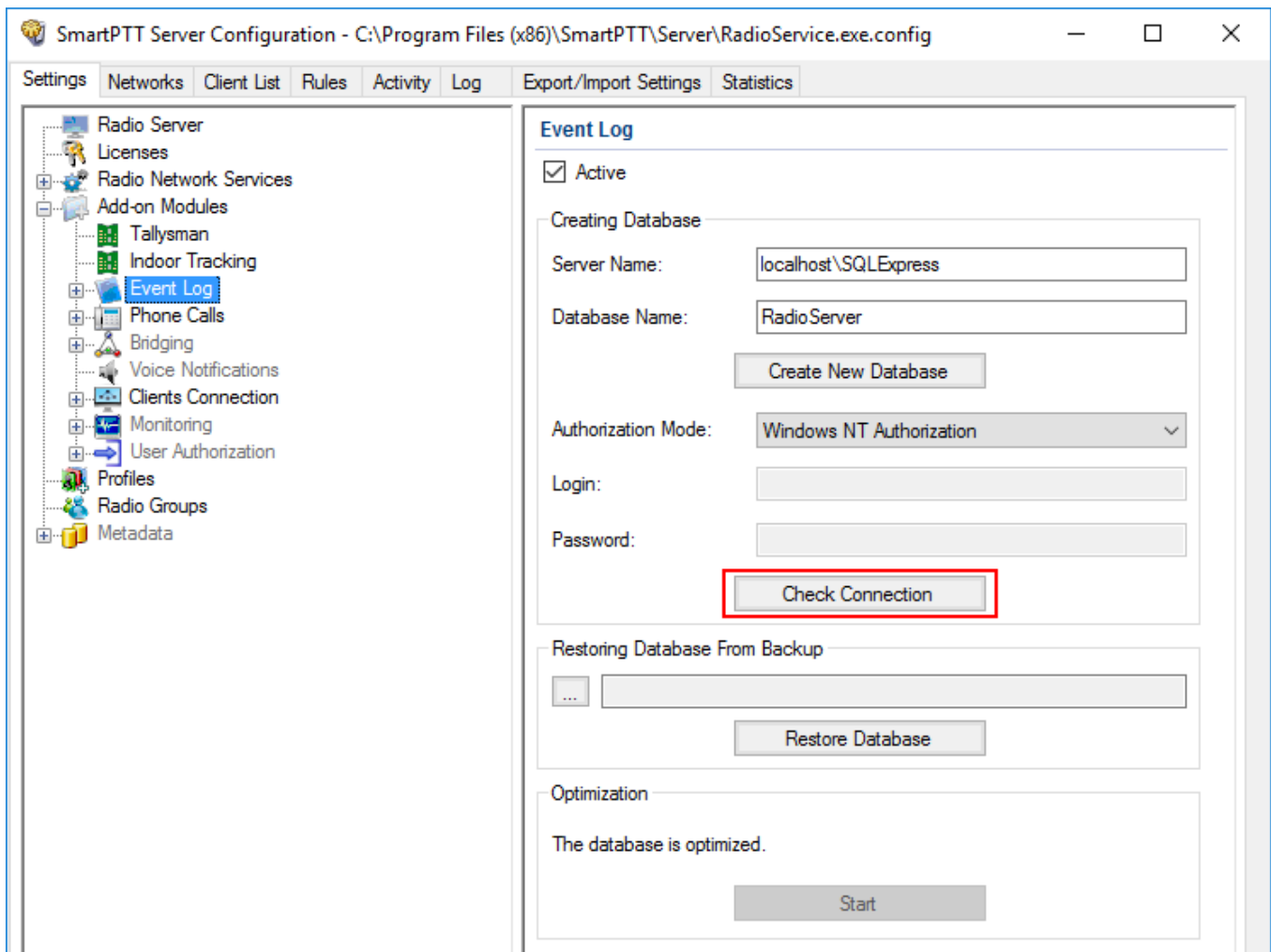
2. Make sure that the **Active** check box is selected in the **Event Log** pane.



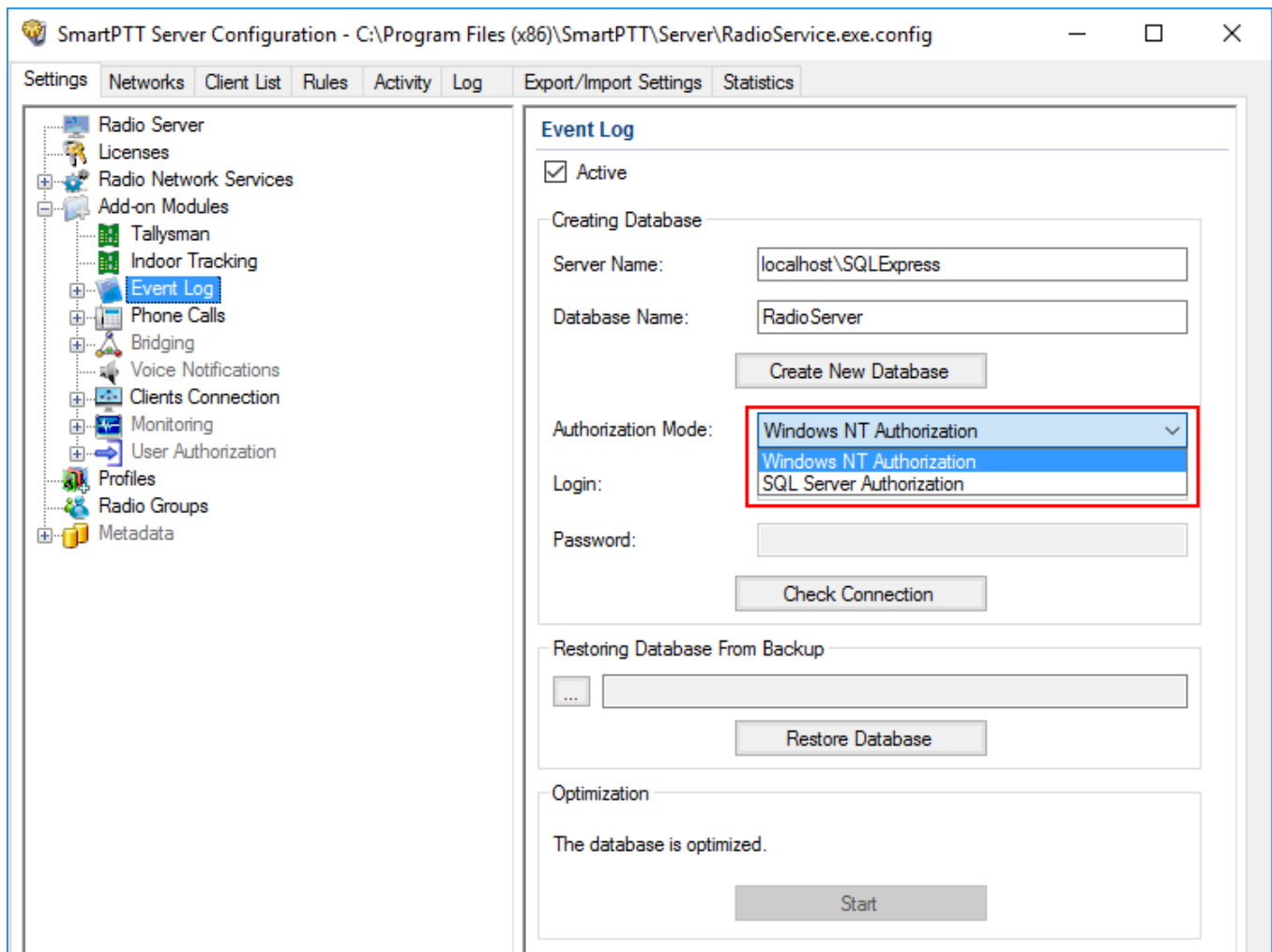
3. In the **Server name** field, enter the name of the SQL Server. You can use either *<IP-address of your computer>\<Your SQL Server name>* or *localhost\<Your SQL Server name>* format:



4. In the **Database Name** field, enter the name of a local Event Log database.



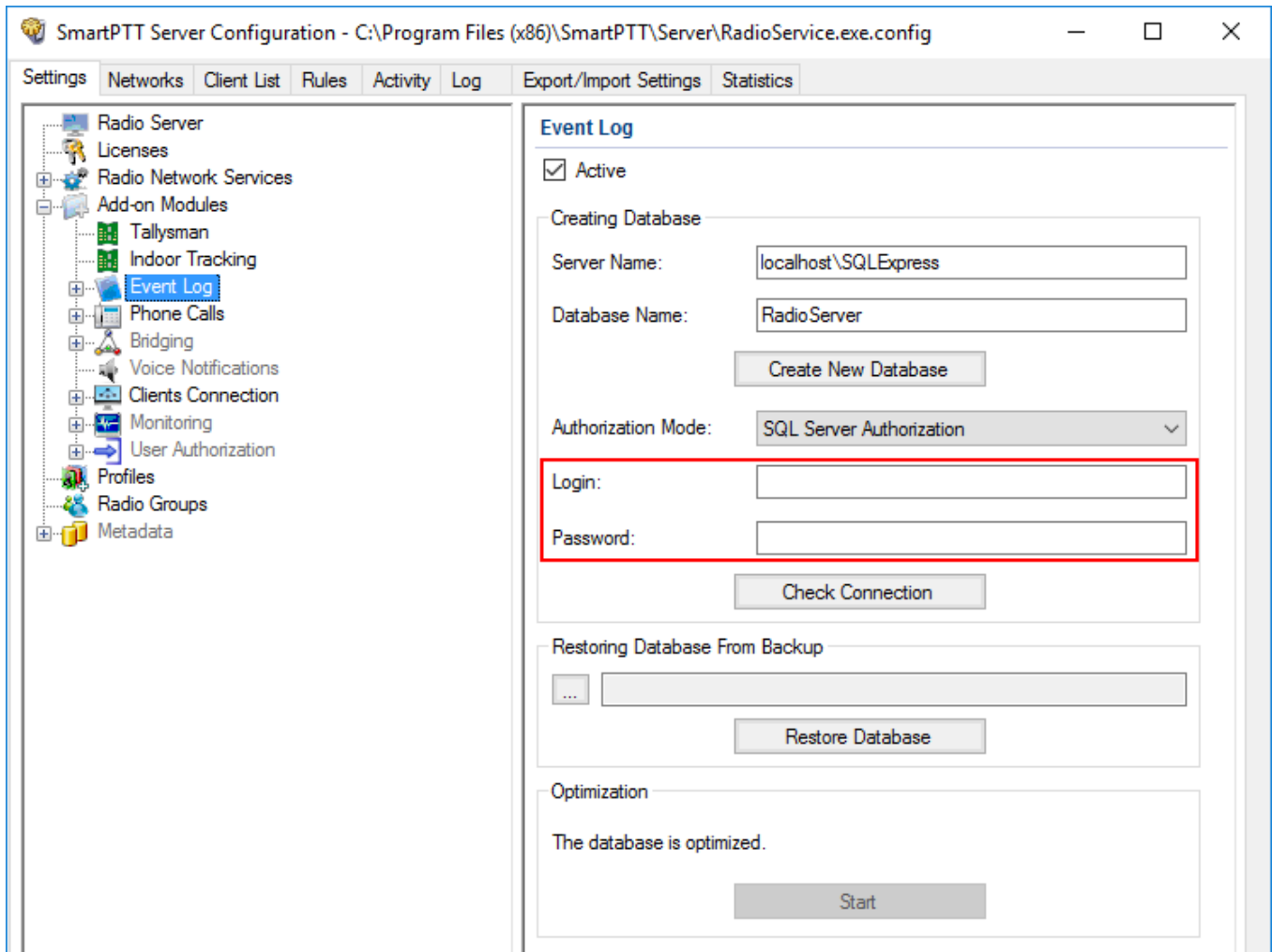
5. From the **Authorization Mode** list, select the needed authorization mode:



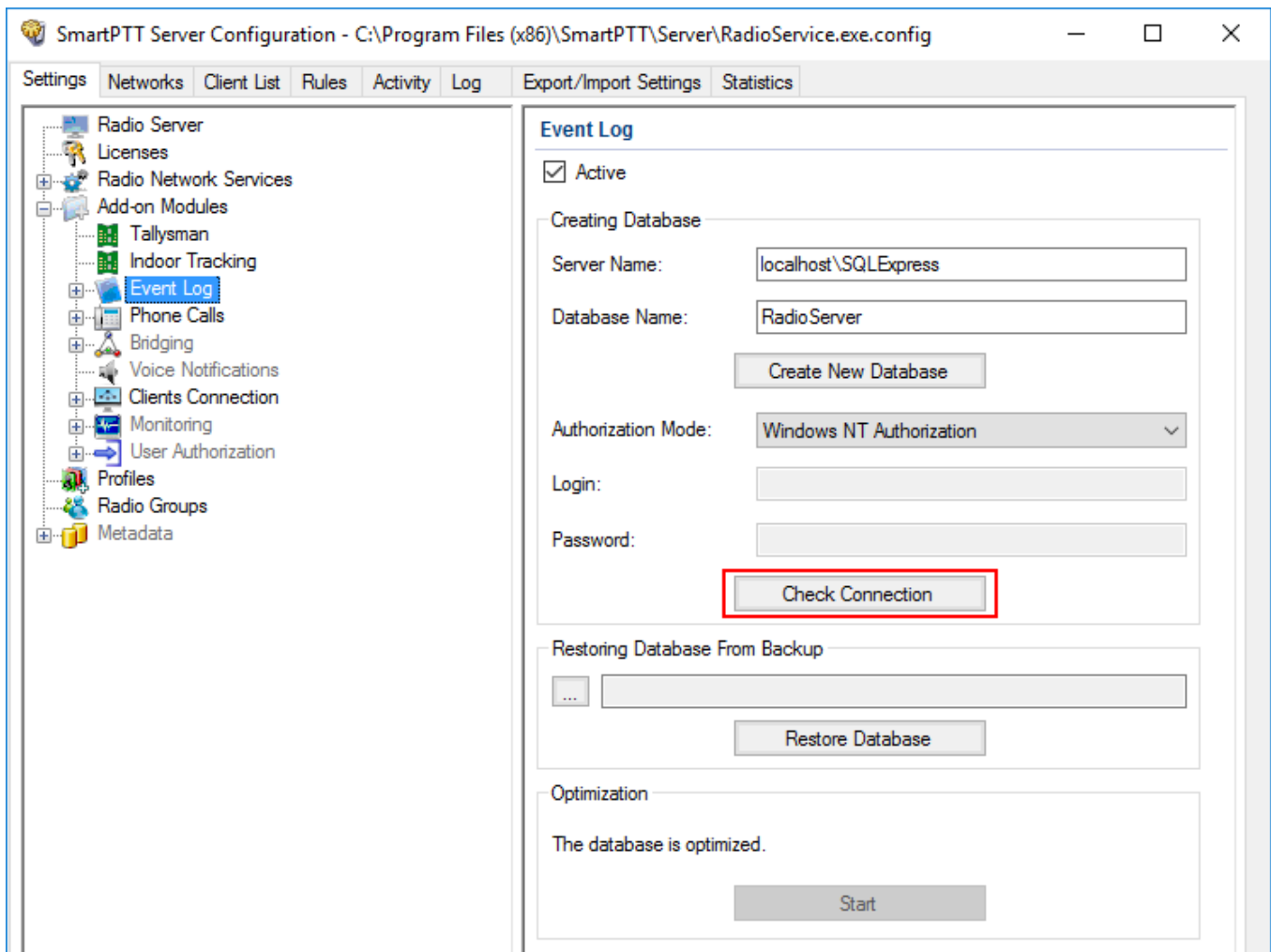
**Windows NT Authorization:** Select to use Windows account for connecting to the local SQL Server.

**SQL Server Authorization:** Select to use SQL Server account for connecting to the local SQL Server.

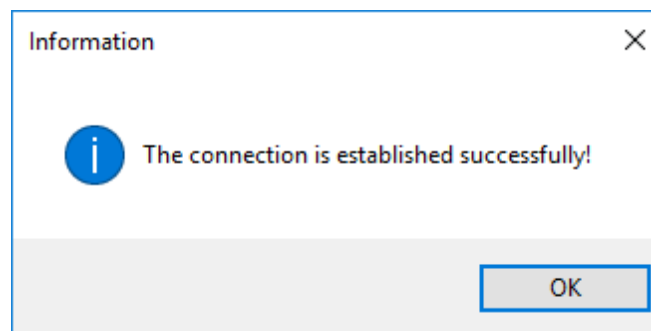
6. If **SQL Server Authorization** is selected, enter login and password.




7. Click **Check Connection**.



If the connection is successful, the following message appears.



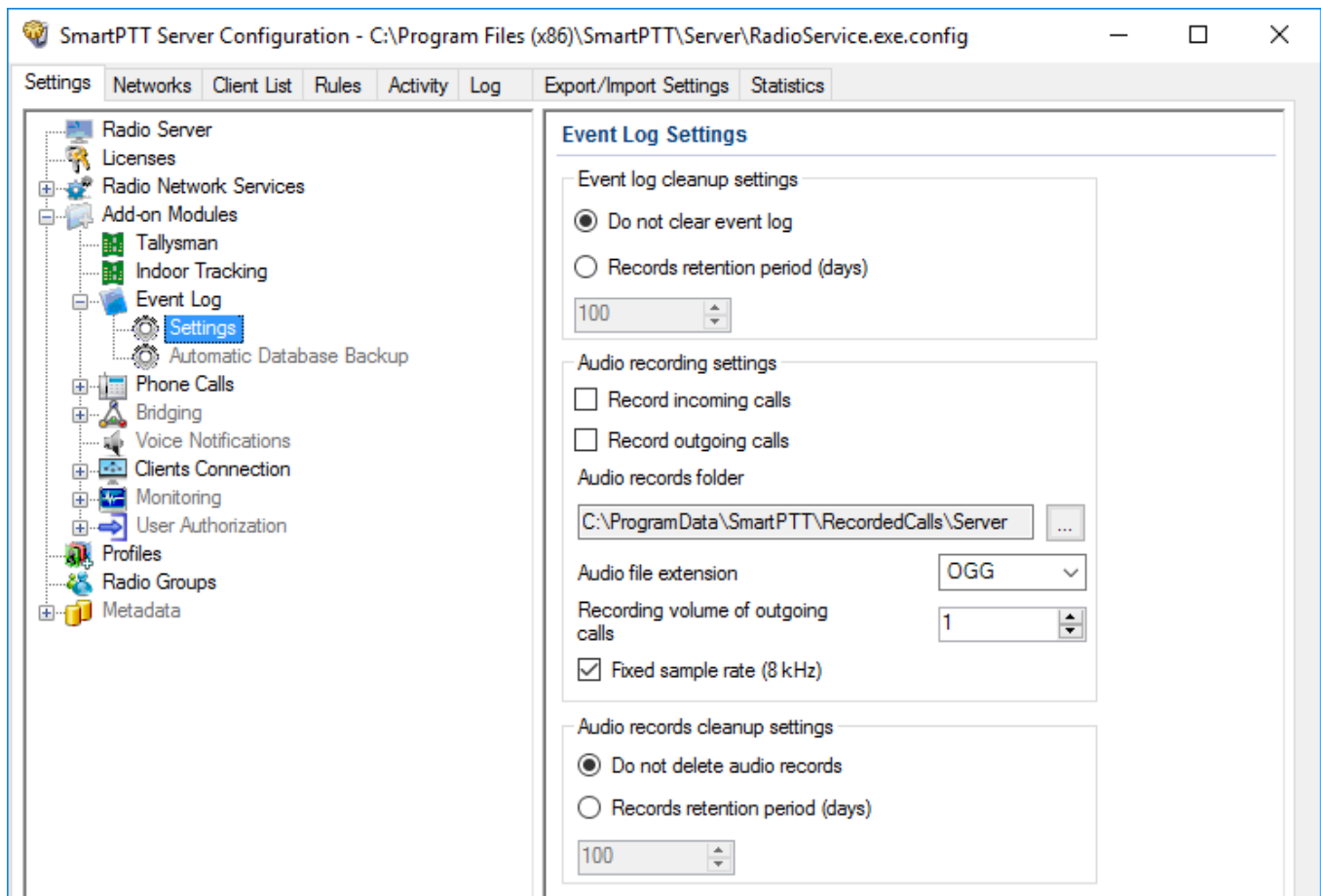
8. Click **Save**  to save changes.

9. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.



### 1.5.3.1 Settings

To configure the radioserver event log select **Settings** in the **Event Log** menu.



To access the settings you should select **Active** in the **Event Log** menu.

The following settings are available to you:

#### Event log cleanup settings

Select the proper variant:

**Do not clear event log:** Select to keep as much of events in the log as possible in the hard drive

**Records retention period (days):** Select to enter the maximum number of the last days to be logged.

#### NOTE

The following settings are available if server is running. To run it, click **Run** or **Restart** in the lower tool bar.

### Audio recording settings

Select the proper variant:

**Record incoming calls:** Select to record voice calls initiated by the radios.

**Record outgoing calls:** Select to record voice calls initiated by the dispatcher123.

**Audio records folder:** Select the absolute path to the folder where recorded voice calls will be stored.

**Audio file extension:** Select the proper extension of the file. Choose between the .mp3 (the default extension), .ogg and .wav extensions.

**Recording volume of outgoing calls:** Select the volume of the recorded voice call. Set the value between 1 and 5.

**Fixed sample rate (8 kHz):** Select to force the sample rate of the recorded voice calls (reduces size of the file).

### Audio records cleanup settings

Select the proper variant:

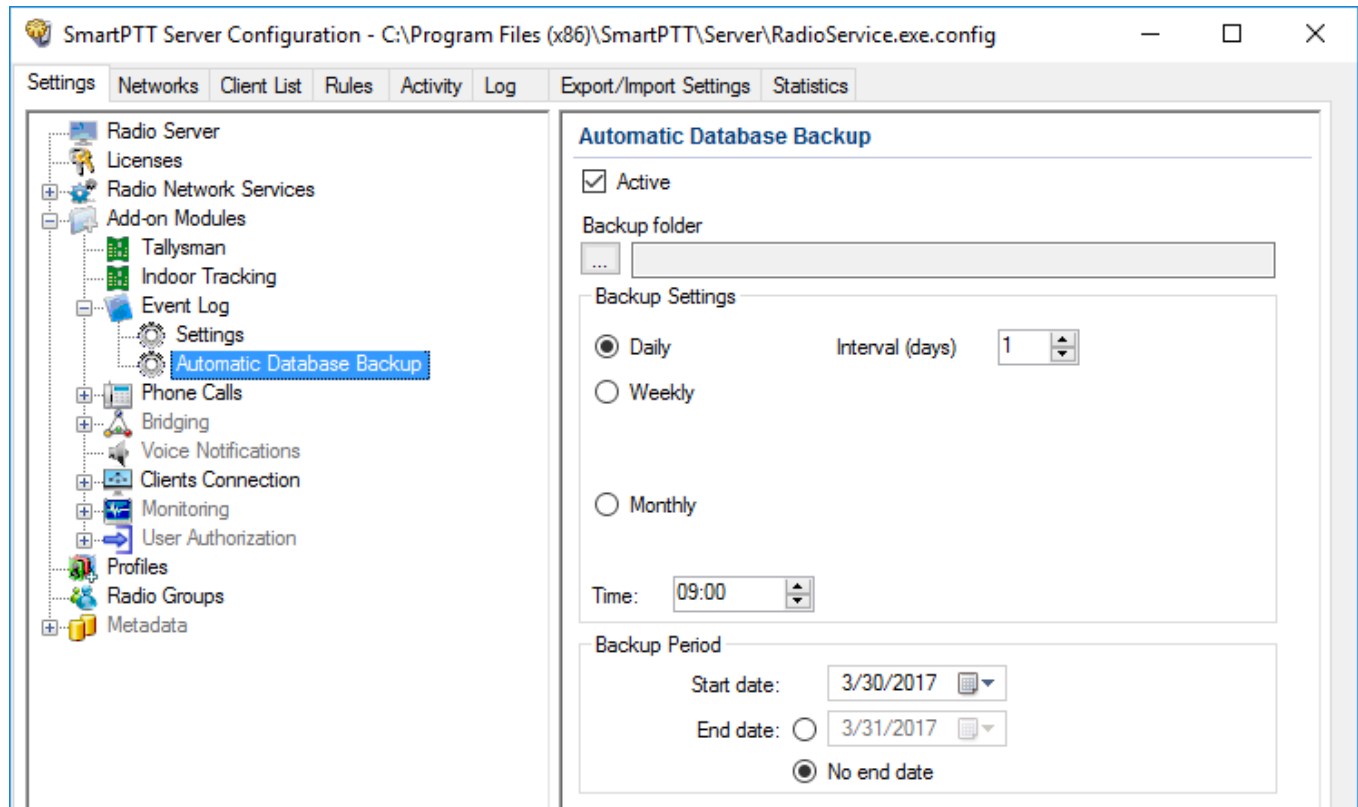
**Do not delete audio records:** Select to keep as much of recordings (audio files) as possible in the hard drive.

**Records retention period (days):** Select to enter the maximum number of days to be “voice-logged”.

### 1.5.3.2 Automatic Database Backup

Backing up data on a regular basis helps to protect it from being erased in case of the server hardware or software failure. SmartPTT Radioserver Configurator allows to back up the event log database automatically.

In order to set up automatic backup schedule of the event log database, select **Automatic Database Backup** under **Event Log** in the setting tree of SmartPTT Radioserver Configurator.



**Active:** Select the check box to enable the ability to create current event log database backups in the automatic mode.

**Backup Folder:** Full path to the file for saving the database backup.

**Daily:** Every fixed day at the specified time (for example, every day, every third day at 9:00 a.m.).

**Weekly:** Every fixed day of the week at the specified time (for example, every Monday, Wednesday and Friday at 11:00 p.m.).

**Monthly:** Once a month on the fixed day of the selected month and at the specified time.

**Time:** Sets the time for database backup. This setting is common to all database backup intervals.

**Backup Period:** Allows you to set time period when automatic database backup is to be made according to the selected backup settings.

**NOTE**

The number of stored backup files in the same folder is limited to 3. Otherwise, when creating a new copy, the old files are deleted.

**NOTE**

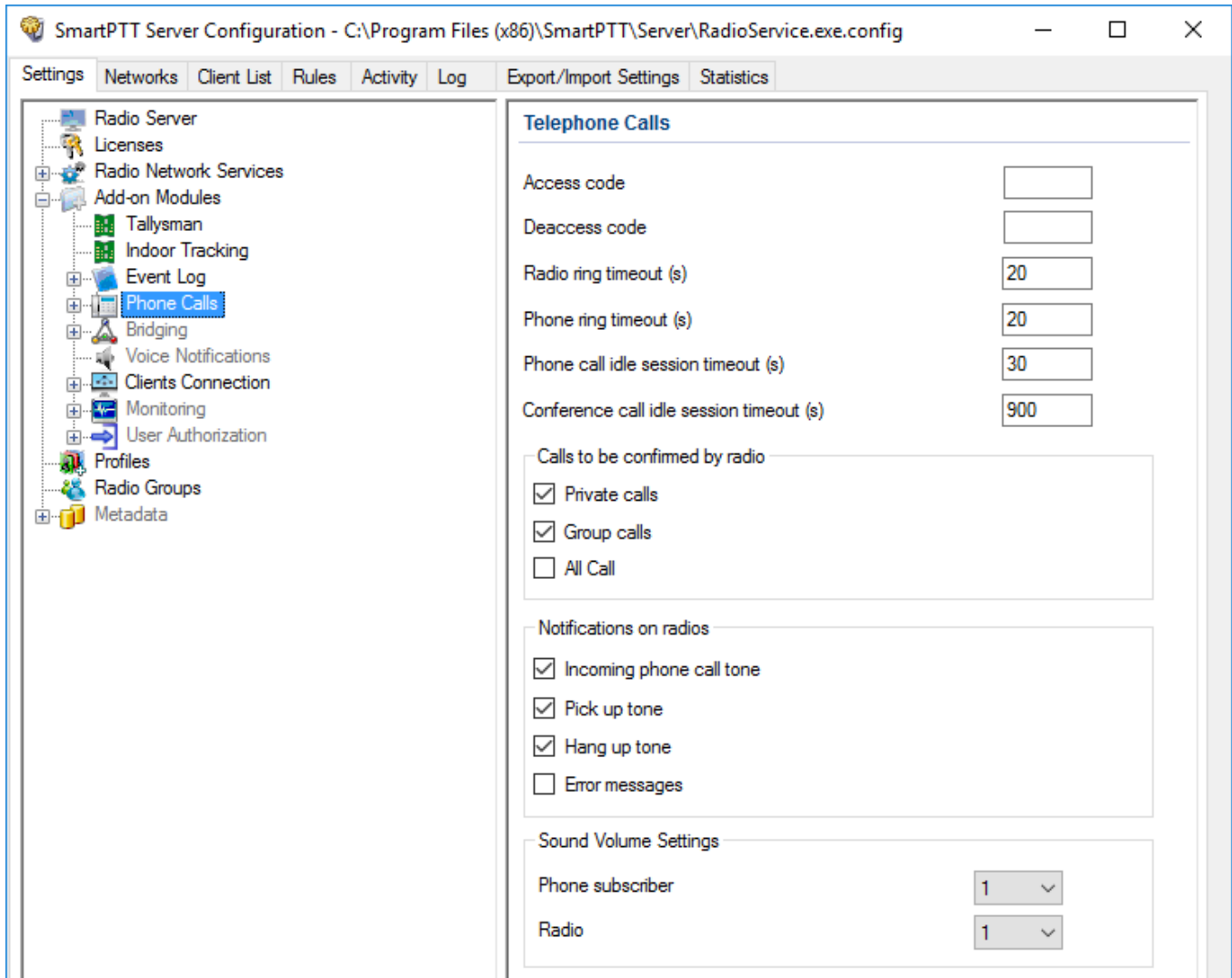
The event log database recovery from the automatically created backup is performed manually in the [Event Log](#) window.

## 1.5.4 Phone Calls

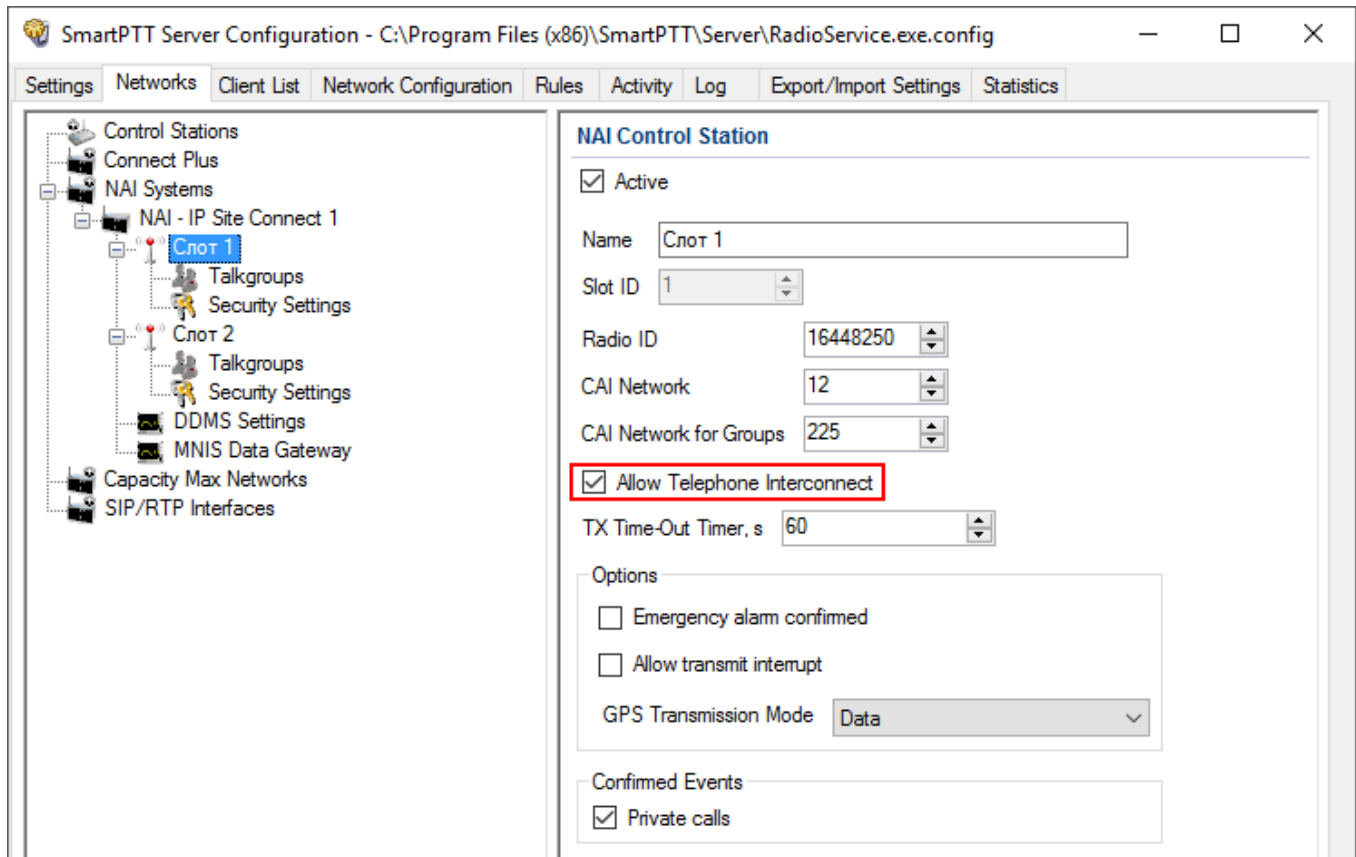
*SmartPTT Radioserver Configurator* is used for configuring conference calls between radios, dispatchers and telephone subscribers.

To configure these calls, follow these steps:

1. Define **Deaccess code**. Make sure that it matches the deaccess code specified in radio settings.



2. Enable **Allow Telephone Interconnect** in the slot settings.



The screenshot displays the SmartPTT Server Configuration interface. The left sidebar shows a tree view of the configuration structure, with 'Slot 1' selected under 'NAI - IP Site Connect 1'. The main window shows the 'NAI Control Station' configuration for 'Slot 1'. The 'Allow Telephone Interconnect' checkbox is checked and highlighted with a red box. Other settings include 'Active' checked, 'Name' 'Слот 1', 'Slot ID' 1, 'Radio ID' 16448250, 'CAI Network' 12, 'CAI Network for Groups' 225, 'TX Time-Out Timer, s' 60, and 'Confirmed Events' with 'Private calls' checked.

SmartPTT Server Configuration - C:\Program Files (x86)\SmartPTT\Server\RadioService.exe.config

Settings Networks Client List Network Configuration Rules Activity Log Export/Import Settings Statistics

Control Stations  
Connect Plus  
NAI Systems  
NAI - IP Site Connect 1  
Слот 1  
Talkgroups  
Security Settings  
Слот 2  
Talkgroups  
Security Settings  
DDMS Settings  
MNIS Data Gateway  
Capacity Max Networks  
SIP/RTP Interfaces

**NAI Control Station**

Active

Name Слот 1

Slot ID 1

Radio ID 16448250

CAI Network 12

CAI Network for Groups 225

Allow Telephone Interconnect

TX Time-Out Timer, s 60

Options

Emergency alarm confirmed

Allow transmit interrupt

GPS Transmission Mode Data

Confirmed Events

Private calls

3. In *SmartPTT Dispatcher*, go to **Settings** → **Telephone Interconnect** and set up the following parameters:

**Configuration**

**Telephone Interconnect**  
Telephone interconnect settings

General Settings | Codec Settings | SIP Trunk Authentication | SIP Accounts

Dispatcher Settings

Allow Calls to Telephone Subscribers

Transport: UDP

SIP Port: 5060

Phone Number: 100

Interface: 192.168.37.85

RTP Ports: 18700 - 18748

Displayed Subscriber Name:

VoIP Gateway Default Settings

Dial Prefix for Outgoing Calls: 12

Dial Prefix for Incoming Calls:

Default VoIP Gateway Address: 82.200.114.46 | SIP Port: 5060

Play Sound Alert for Incoming Call

Play Sound Alert for Outgoing Call

Sound Level: [Slider]

Help | Cancel | Finish

- a. Select **Allow Calls to Telephone Subscribers**.
  - b. In the **Interface** field define your radioserver **IP address**.
  - c. In the **RTP ports** field define RTP ports.
  - d. In the **Dial Prefix for Outgoing Calls** field enter the prefix for outgoing calls. It must match the same prefix that is set in the VoIP gateway.
  - e. Specify the IP address of the VoIP gateway.
4. To save the changes, click **Finish**.

Additional features, which are applied to telephone calls over SIP protocol:

**Radio ring timeout (s):** Sets the time interval during which the radioserver waits for pressing the PTT button on the radio.

**Phone ring timeout (s):** Sets the time interval during which the radioserver waits for the telephone subscriber to pick up the phone.

**Phone call idle session timeout (s):** Sets the time interval starting from the last time the PTT button is pressed on radio after which the telephone call will be automatically finished. This timeout must not exceed **TX Time-Out Timer** set in network settings in *SmartPTT Radioserver Configurator* and in repeater settings.

**Conference call idle session timeout (s):** Sets the time interval starting from the last time the conference call participant presses PTT button after which the conference call will be automatically finished.

**Calls to be confirmed by radio:** If enabled, when making a private call, group calls, All Call the telephone subscriber can hear the ring tone until you press PTT button on the radio. If these check boxes are not selected, the call will start immediately.

**Notifications on radios:** Sets notifications on radio of various events with a special tone: telephone calls, beginning and end of calls. The radio can also receive messages about errors.

**Sound Volume Settings:** Allows setting up sound volumes on a telephone and a radio during incoming or outgoing radio calls.

### 1.5.4.1 Telephone Interconnect

Telephone Interconnect service allows for communication between radio and telephone subscribers, and uses SIP and RTP protocols for signaling and voice data transmission. Voice data transmission is done in half-duplex mode. Switching between receiving and transmitting modes is carried out by voice interrupt initiated by a radio. There are several ways how to make the interconnection:

- A telephone subscriber makes a private call
- A telephone subscriber makes a group call
- A radio makes a call to a telephone subscriber



- The dispatcher connects telephone and radios
- The dispatcher connects a telephone subscriber and a talkgroup

To use Telephone Interconnect service, configure the radioserver and VoIP gateway settings. Also, make sure that **Allow Telephone Interconnect** is enabled in the network slot parameters.

## Configuring SmartPTT Radioserver

To configure SmartPTT Radioserver settings, go to *SmartPTT Radioserver Configurator* and select **Telephone Interconnect** as shown on the picture.

The screenshot shows the SmartPTT Server Configuration window with the following settings:

**Telephone Interconnect**

Active

**Radioserver Settings**

Interface: Auto

SIP port: 5060

RTP ports: 18650 - 18950

Transport: UDP

**Audio Codecs**

Active	Name	Priority
<input checked="" type="checkbox"/>	G711A	1
<input checked="" type="checkbox"/>	G711U	2
<input checked="" type="checkbox"/>	SPEEX	3
<input checked="" type="checkbox"/>	G729	4

**Permissions for radio groups:**

Active

Group Name	Incoming Calls	Outgoing Calls

**NOTE**

To activate telephone interconnect, install the corresponding license. For more information on how to install licenses, see [Licenses](#).

Under **Radioserver Settings** specify the interface that will be used for sending and receiving commands and voice data when working with VoIP gateway:

**SIP port:** UDP or TCP port number to receive and send SIP data packets. The default value is 5060. Accordingly, the specified port must be available for incoming and outgoing traffic.

**WARNING**

If both *SmartPTT Dispatcher* and SmartPTT Radioserver are installed on one computer, their SIP ports must differ. For example, 5060 for the radioserver and 5061 for the dispatch console.

**RTP ports:** Each connection with a phone subscriber occupies two UDP ports (even port numbers are used by RTP protocol, and odd port numbers – by RTCP protocol). The specified port must be available for incoming and outgoing traffic. The default range of values is from 18650 to 18660.

**WARNING**

The address and the port of the VoIP gateway must be real (NAT is not supported). If both *SmartPTT Dispatcher* and SmartPTT Radioserver are installed on one computer, the port ranges set in and the **RTP ports fields** in *SmartPTT Radioserver Configurator* and *SmartPTT Dispatcher* must differ.

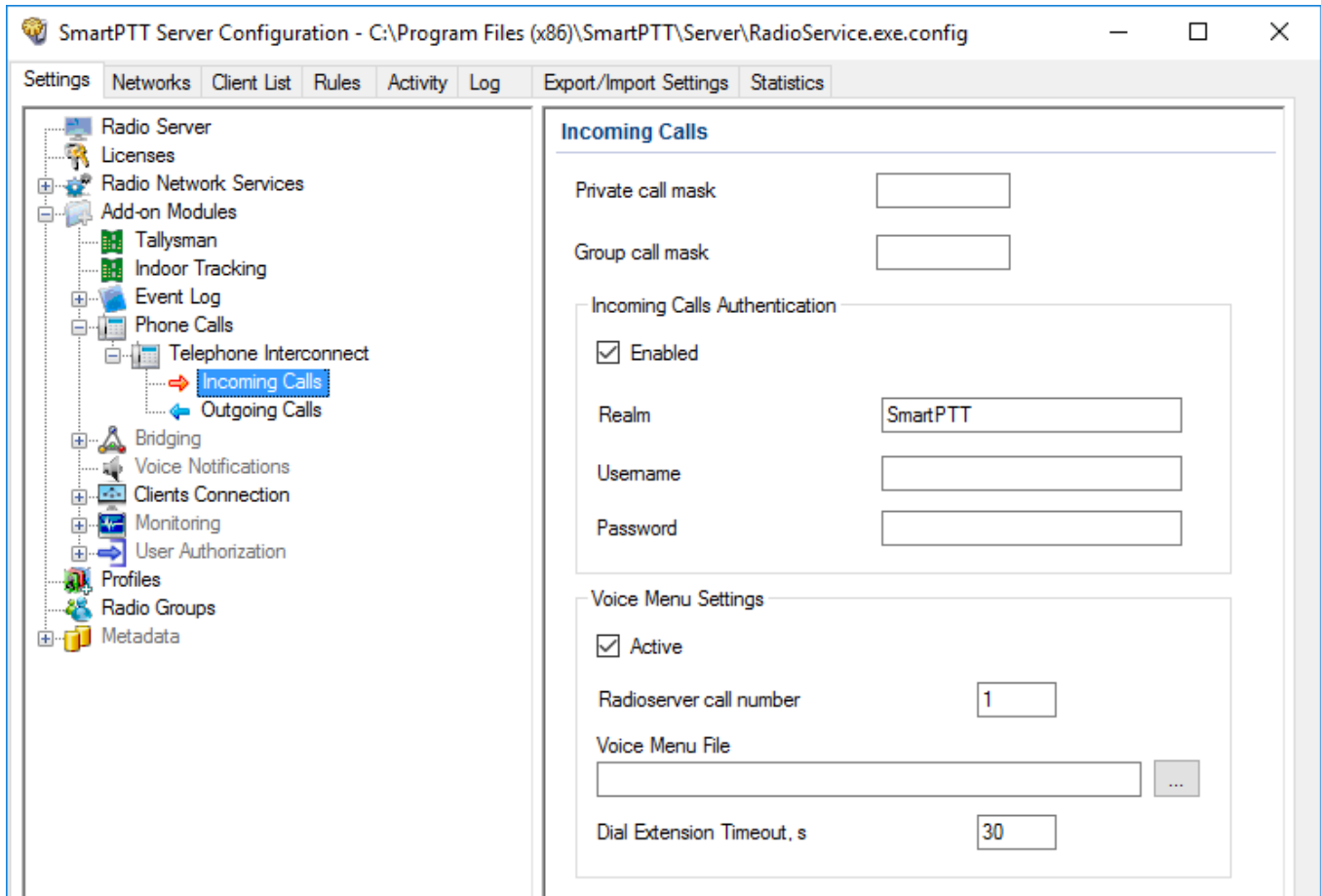
**Transport:** Allows selecting between TCP and UDP for SIP commands transmit.

**Audio Codecs:** You can activate or deactivate supported audio codecs, as well as change their priorities. Currently, there are 4 audio codecs: G711A, G711Q, SPEEX и G729. When connecting to PBX the radioserver always uses the codec priorities list set in the PBX settings, while the PBX can ignore the priorities list set in the radioserver. That is why codecs used by the call initiator and the responder can be different.

**Permissions for radio groups:** In this section you can allow or forbid particular groups of radios to make or answer telephone calls. These groups of radios can be created under [Radio Groups](#). If the **Active** check box is selected, and the table is empty, communication between radio and phone subscribers will be impossible.

## Incoming Calls

In terms of SmartPTT system “incoming calls” are calls that are made from telephone subscribers to radios.



A telephone subscriber can make two types of calls to radios.

- Private call is a call when the radioserver calls a radio. You can use **Private call mask** when making a private call.
- Group call is a call when the radioserver calls to a talkgroup. You can use **Group call mask** to make a group call.

A mask is a regular expression. In the following table you can find all the symbols used in masks.

Symbol	Description
.	Used for any figure

Symbol	Description
[m-n]	Used for any figure in the interval from <b>m</b> to <b>n</b>
[a,b,c] or [abc]	Used for any figure from the list
T	Used for any number of any figures
(.)	Used to unite regular expressions
{ }	Used to include everything inside the brackets into the resulting number
N	Used to denote network ID. <b>N=0</b> when there is only one network. Can be used only in <b>Group Call Mask</b> .
S	Used to denote <b>Slot ID</b> (IP Site Connect) or <b>Site ID</b> (Linked Capacity Plus). Can be used only in <b>Group Call Mask</b> .

### Example

- **Private Call Mask:** 31 or 31T
- **Group Call Mask:** 32NSST

Then the dialed numbers will mean the following:

- **31403**, i.e. **31 403**: private call to radio with ID = 403.
- **3200013**, i.e. **32 0 00 13**: wide group call to a talkgroup 13, which must be either unique for the radioserver, or located in the only network connected to the radioserver.
- **3210013**, i.e. **32 1 00 13**: wide group call to a talkgroup 13 located in network 1.
- 32112123, i.e. **32 1 12 123**: local group call to a talkgroup 123 in network 1, on site 12.

The **S** symbol can be assigned different values and they depend on the network type. Below is the list of values that can be used for the **S** symbol:

- In the IP Site Connect network the **S** symbol can be assigned values 1 or 2 only, which correspond to the number of the IP Site Connect slot.
- In the Capacity Plus network the **S** symbol can have only one value: 0.
- In the Linked Capacity Plus network the **S** symbol can be assigned any value. **S=0** stands for a wide group call. **S=1**, **S=2**, **S=any other figure** stand for a local group call specifying the LCP site number.

To make the All Call, use the following values:

- In the IP Site Connect network: **S=1/2** and talkgroup ID=0.
- In the Capacity Plus and Linked Capacity Plus networks: **S=0** and talkgroup ID=0.

Other settings mean the following:

**Incoming Calls Authentication:** Receiving an incoming call from a phone/softphone, the radioserver asks for the username and password corresponding to **Realm** in the described setting. The calling telephone subscriber must send back the username and password specified in this setting. To activate this ability, select **Enabled**.

- **Realm:** Parameter used for the incoming telephone calls authentication.
- **Username:** Username used for authentication.
- **Password:** Password used for authentication. It should correspond to the specified realm.

**Voice Menu Settings** is used for setting up interactive voice response (IVR), i.e., a technology that allows SmartPTT system to interact with radios through the use of voice and DTMF tones input via keypad. If enabled and set up properly, the telephone subscriber can make a call to the radioserver and then to the required radio or talkgroup using the information heard in the voice menu file.

- **Radioserver call number:** Number to call to the radioserver.

- **Voice Menu File:** The audio file which will be played to the telephone subscriber. The sampling frequency of the audio file must be 8000 Hz.
- **Dial Extension Timeout, s:** Period in seconds when the caller can dial the ID of the radio or talkgroup after listening to the voice menu file. If the caller has not dialed the ID before the time is out, the call will be dropped.

To make a call using voice menu, follow these steps:

1. Dial your PBX number.
2. Dial the radioserver call number.
3. Dial \* to turn on DTMF mode on the telephone (not obligatory, depends on the telephone parameters).
4. Dial the private or group call mask, and then the radio or talkgroup ID.
5. Dial #.

### Example

**The radio ID:** 120

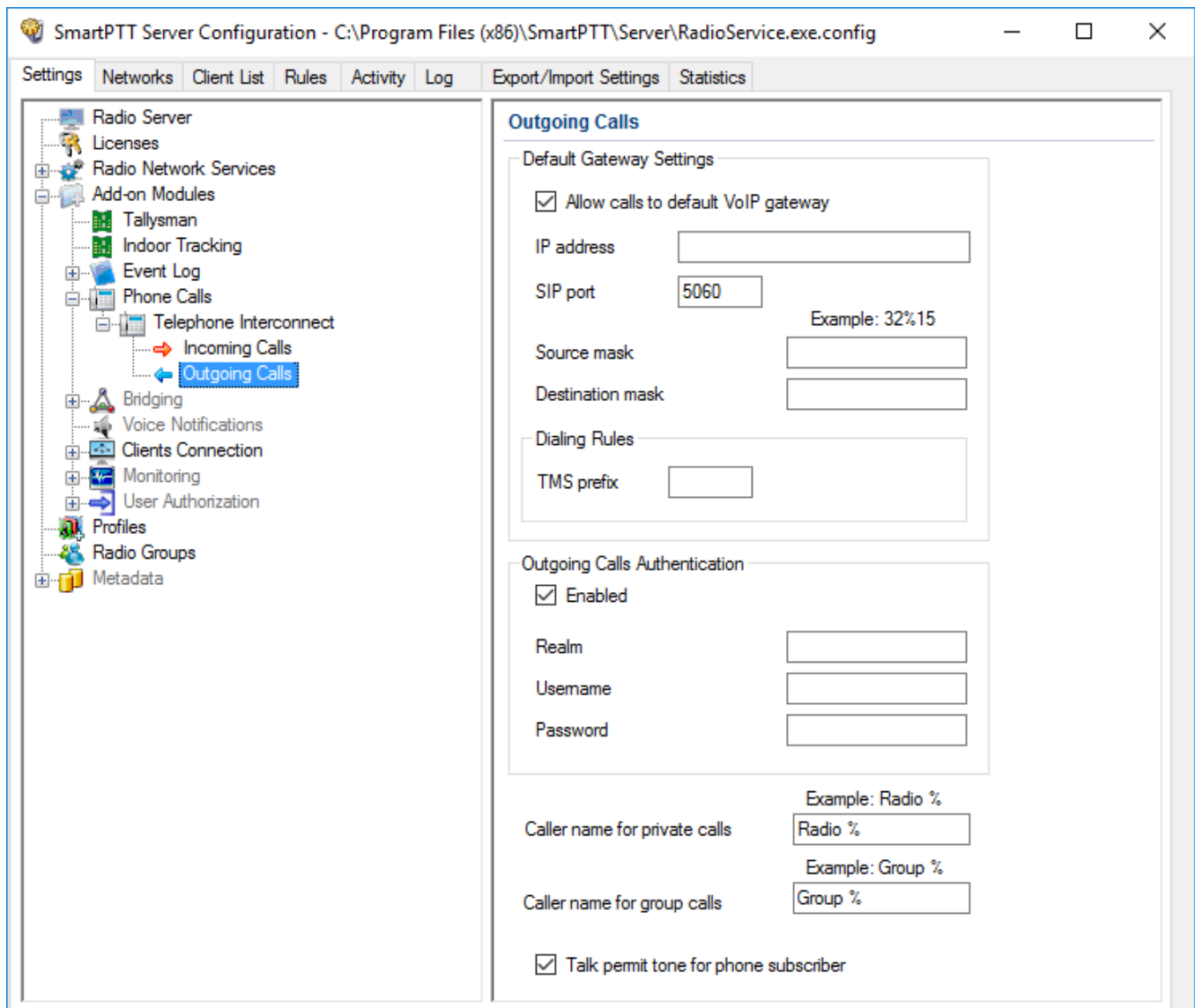
**The PBX number:** 9649

**The radioserver call number:** 10

**The private call mask:** 1

**The telephone subscriber will call:** 9649 10 (\*) 1 120 #

## Outgoing Calls



**Allow Calls to Default VoIP gateway:** If enabled, radio calls to telephone subscribers are made automatically, using all the data given, such as IP address of the automatic exchange,

Source and Destination masks, Dialing Rules. If the option is not selected, you will need to enter the IP address and the full number of the telephone subscriber to make a call.

**TMS prefix:** Used for making a call to a telephone subscriber with the help of a text message sent from a radio. **TMS Prefix** can contain any available symbol on the radio keyboard. Figures following the specified prefix are regarded as the telephone subscriber's number.

**Outgoing Calls Authentication:** The setting includes parameters required for outgoing call authentication. If Realm is left blank, the specified user name and password are used in response to any authentication request from the called party. Otherwise, Realm is checked whether it corresponds to the requesting user name and password. If it matches, user name and password are sent. If not, the authentication is failed immediately.

**Realm:** If the value is set, SmartPTT Radioserver responds to authentication requests with the matching **Realm** value. If the value is not set, SmartPTT Radioserver sends user name and password given in response to any authentication request.

**Username:** User name used for authentication.

**Password:** Password used for authentication.

**Caller name for private calls:** Name of the radio that will be shown to the telephone subscriber. The percent symbol (%) will be replaced automatically by the radio number.

**Caller name for group calls:** Name of the talkgroup that will be shown to the telephone subscriber. The percent symbol (%) will be replaced automatically by the talkgroup number.

**Talk permit tone for phone subscriber:** If selected, the phone subscriber will hear a special tone prompting to start speaking.

## 1.5.5 Bridging

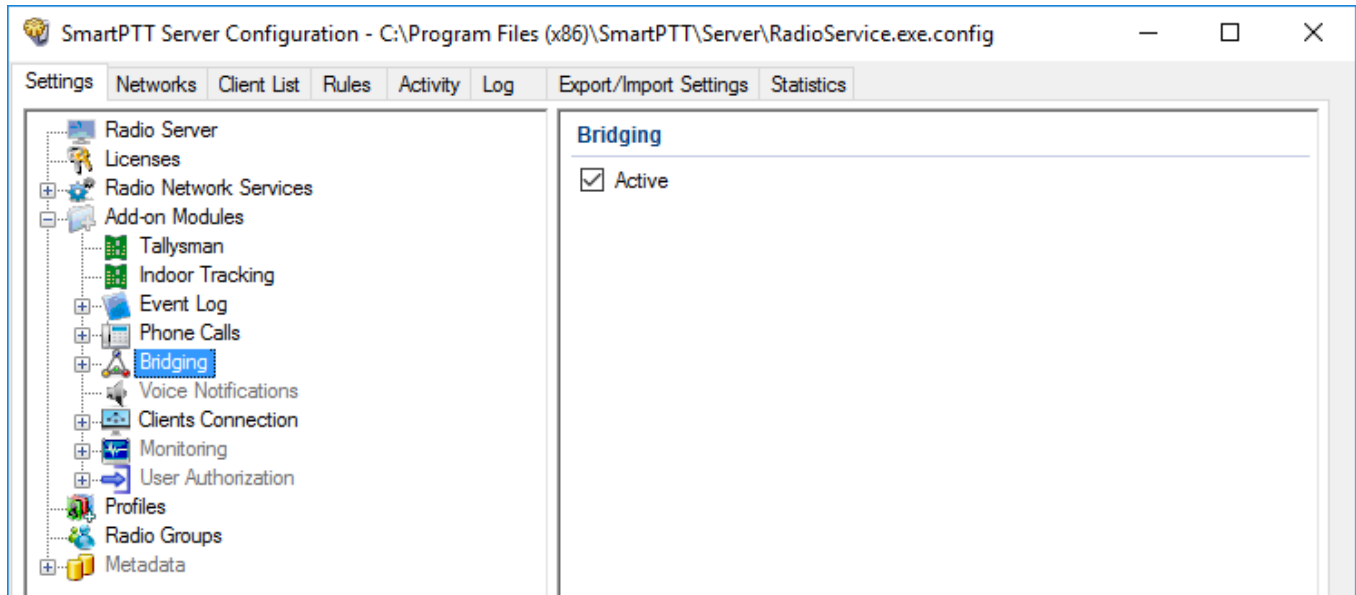
SmartPTT bridging service allows joining various network systems into a single radio network. The bridging service is implemented in the scope of SmartPTT PLUS Radioserver and provides intelligent means of redirecting voice and data streams among different network systems.

### NOTE

To activate bridging service, install the corresponding license. For more information on how to install licenses, see [Licenses](#).



To activate the Bridging service, click **Bridging** in the setting tree of *SmartPTT Radioserver Configurator*. In the opened window select the **Active** check box.

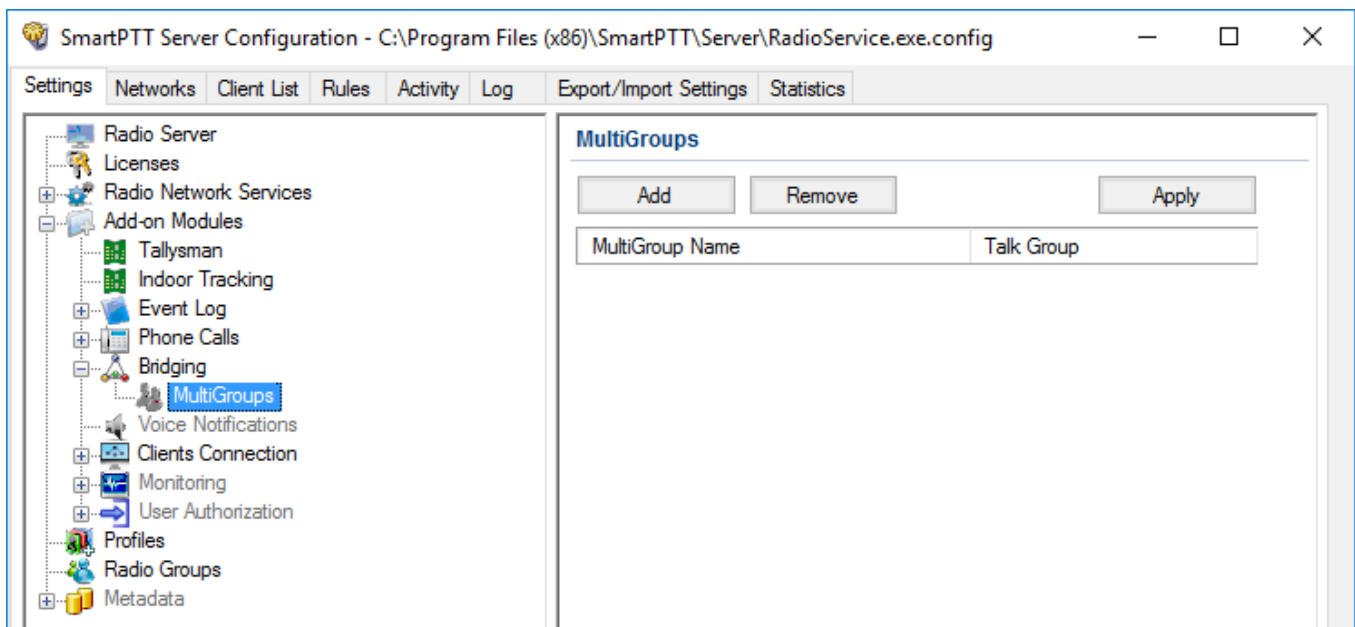


### 1.5.5.1 Multigroups

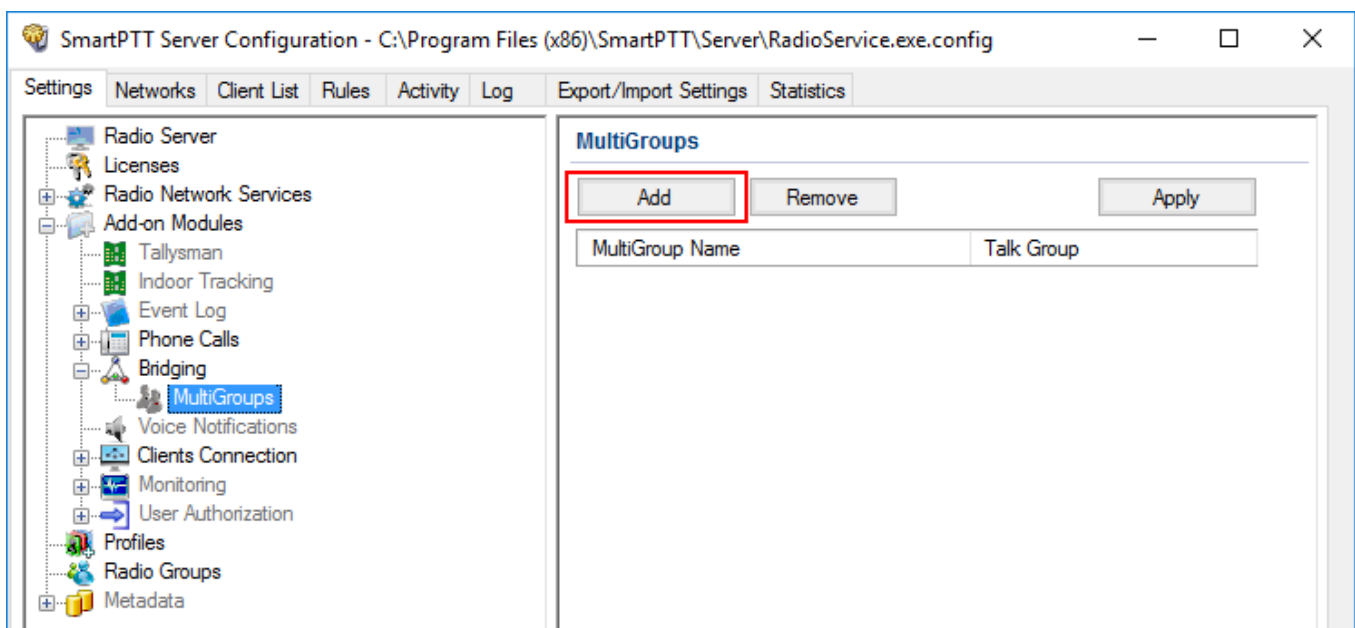
MultiGroups are used to organize dynamic routing of group calls between channels and different network systems. Routing of group calls can be global or limited to predefined channels. Configuration of MultiGroups does not require any bridging settings on *SmartPTT Dispatcher*, but **Bridging** must be enabled in *SmartPTT Radioserver Configurator*. If it is not activated, **MultiGroups** settings will be disabled.

To add and configure new multigroups, follow these steps:

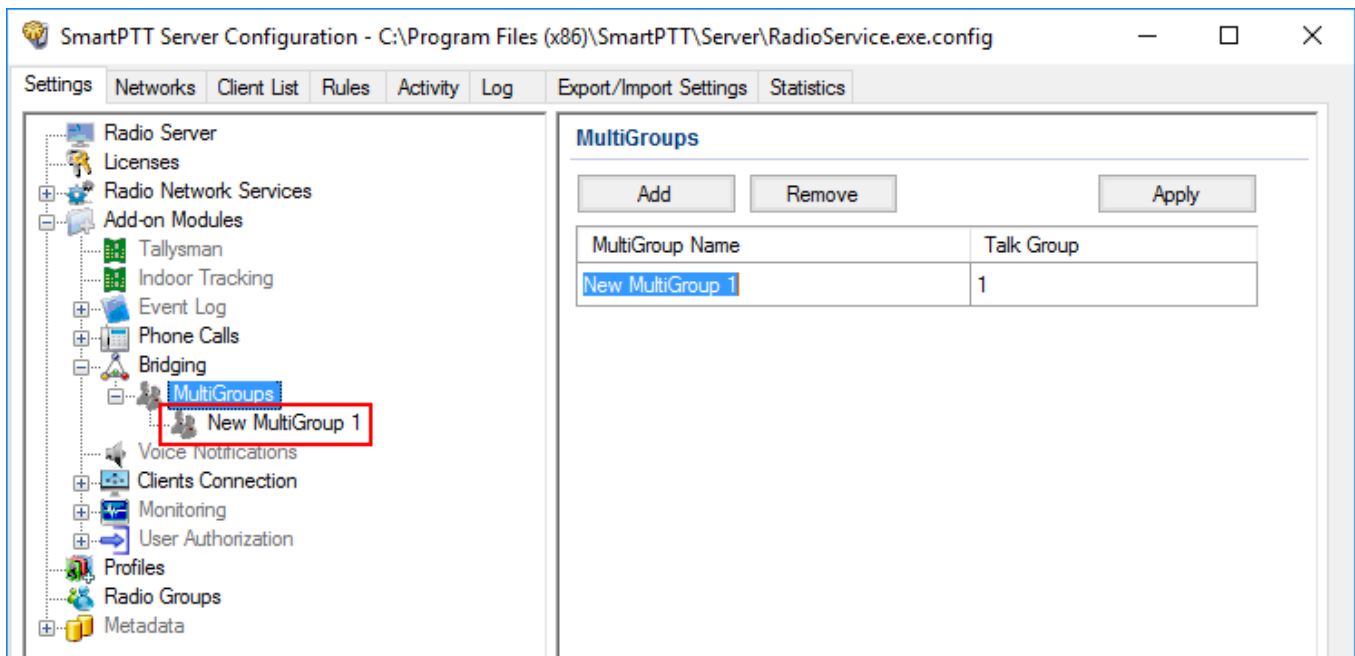
1. In the left pane of the **Settings** tab, expand the **Bridging** node and click **MultiGroups**.



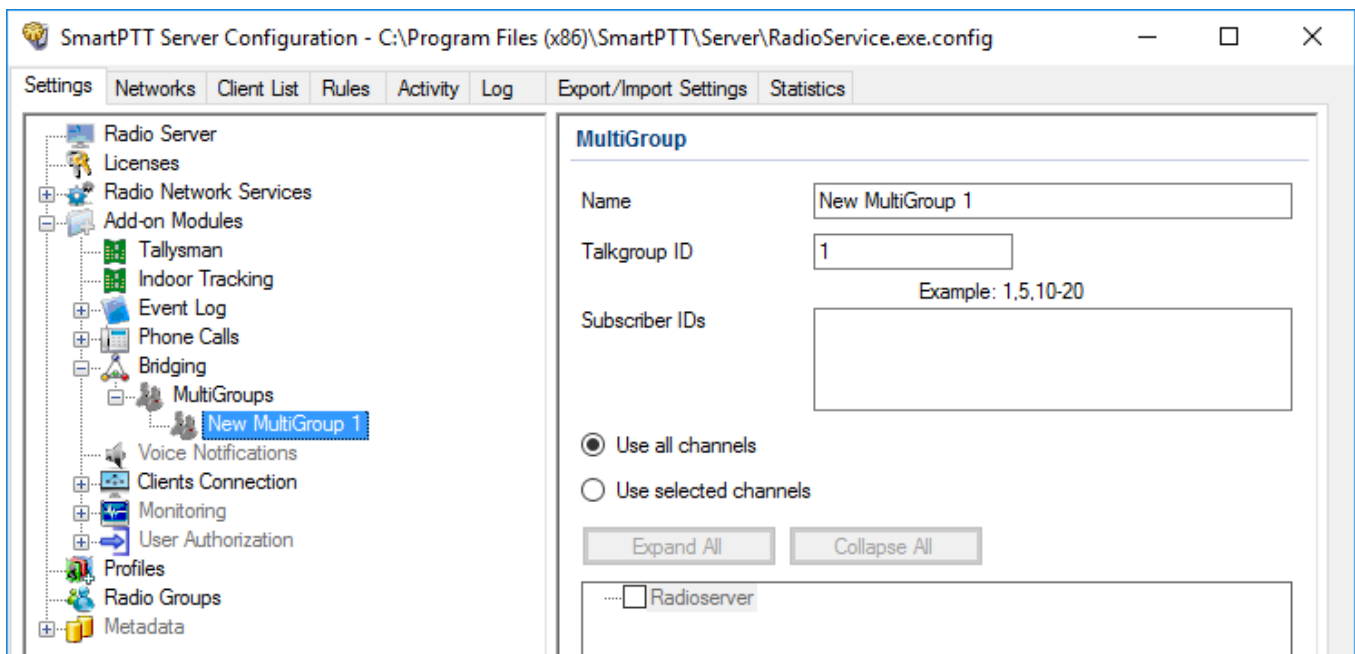
2. In the **MultiGroups** pane, click **Add**.



3. In the left pane, click the new multigroup name.



4. In the **MultiGroup** pane perform the needed configuration.



**Name:** Name of the multigroup.

**Talkgroup ID:** The ID of the talkgroup whose calls are to be routed.

**Radio IDs:** Radio IDs which will be included in the multigroup.

**Use all channels:** Select this option if you want the group call to be routed globally. It works in the following way. If a multigroup is created for a talkgroup, and a group call is made to this talkgroup, SmartPTT starts to look for all the talkgroups with this ID. Then SmartPTT checks if these groups have radios that were defined in the multigroup settings. The group call will be routed only to the talkgroups that include at least one of these radios.

**Use selected channels:** Select this option if you want the group call to be routed within selected channels.

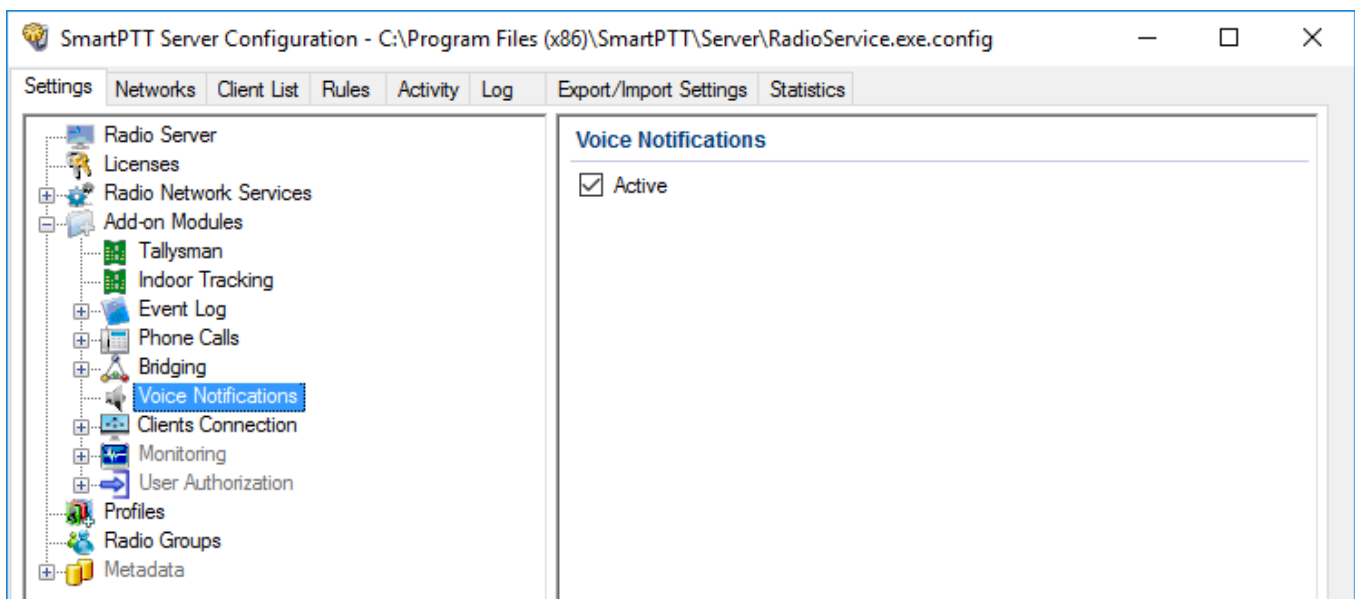
#### NOTE

When you add, change or delete a multigroup, it is not necessary to restart the radioserver. Click **Apply** to activate the multigroups.

## 1.5.6 Voice Notifications

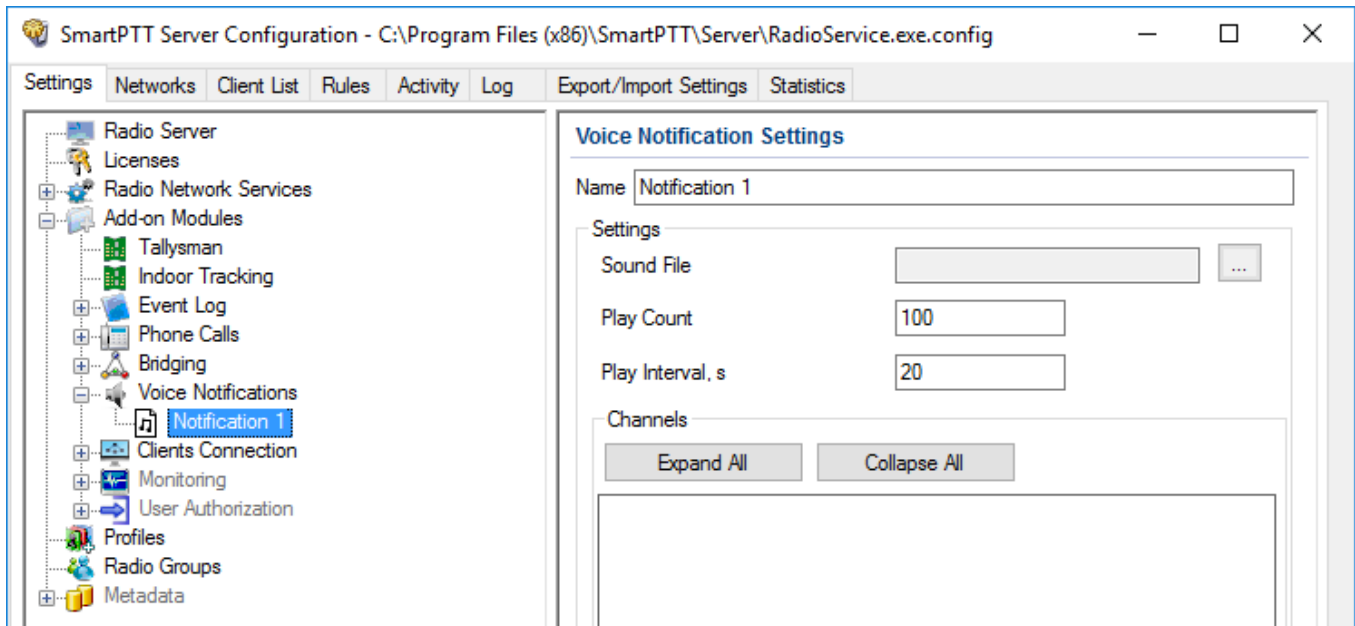
The main purpose of the voice notification functionality is to warn talkgroups about the fire or other emergency and to manage evacuation. However, in normal mode voice notifications can be used to transmit ordinary announcements.

To create a voice notification, select the **Voice Notifications** item in *SmartPTT Radioserver Configurator*. The **Voice Notifications** window appears on the right. To enable the service, select the **Active** check box.



To add a voice notification, right-click on **Voice Notifications** and select **Add**. The **Voice Notification Settings** window appears:

Set the following parameters in the **Voice Notification Settings** window.



**Name:** Name of the voice notification displayed in *SmartPTT Dispatcher*.

**Sound File:** Sound file in .wav, .mp3, or .ogg format. Only monophonic files can be used as voice notifications.

**Play Count:** Specifies how many times the voice notification will be played on the channel. To be set in the range from 1 to 9999.

**Play Interval, s:** Specifies the interval between the voice notification plays. To be set in the range from 5 to 216000.

Select channels of the hardware or/and virtual control stations in the **Channels** area (**All Call** or **Group Call**) that play the voice notification (after it was run in *SmartPTT Dispatcher*).

#### NOTE

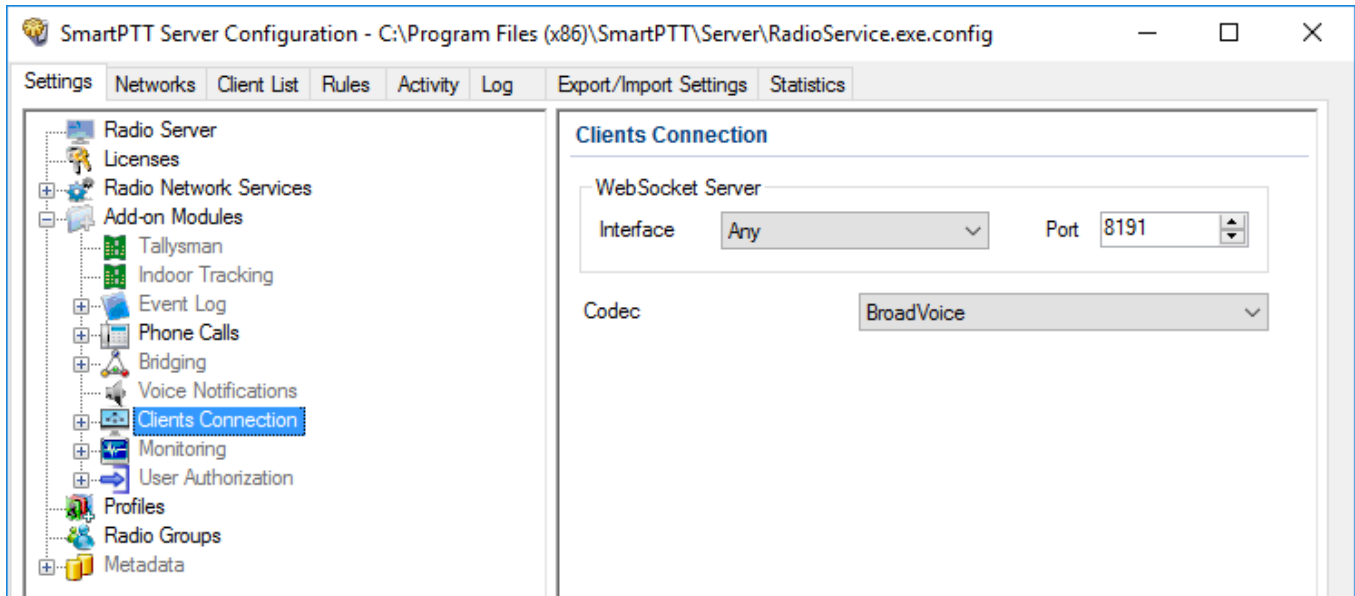
Playing voice notification on the channel corresponds to an outgoing call of SmartPTT Radioserver and fully occupies the selected channel. Thus, each control station (hardware or virtual) can have only one call type to be used for playing voice notifications on the channel – an all call or a group call.

To delete the voice notification profile, right-click on the selected profile and click **Delete**.

## 1.5.7 Clients Connection

*SmartPTT Radioserver Configurator* allows to enable support for web service and third-party applications.

To configure the parameters common for the described above applications, click **Clients Connection** in the setting tree of *SmartPTT Radioserver Configurator*. In the **Clients Connection** window set the required parameters.



**Interface/Port:** IP address and port used for connection of the web, mobile and third-party applications to SmartPTT Radioserver.

**Codec:** Outgoing audio stream compression method.

### 1.5.7.1 Web Service

This service expands SmartPTT bounds, as it allows the dispatchers to do their job without the desktop *SmartPTT Dispatcher*. Currently the web version provides the following functionality:

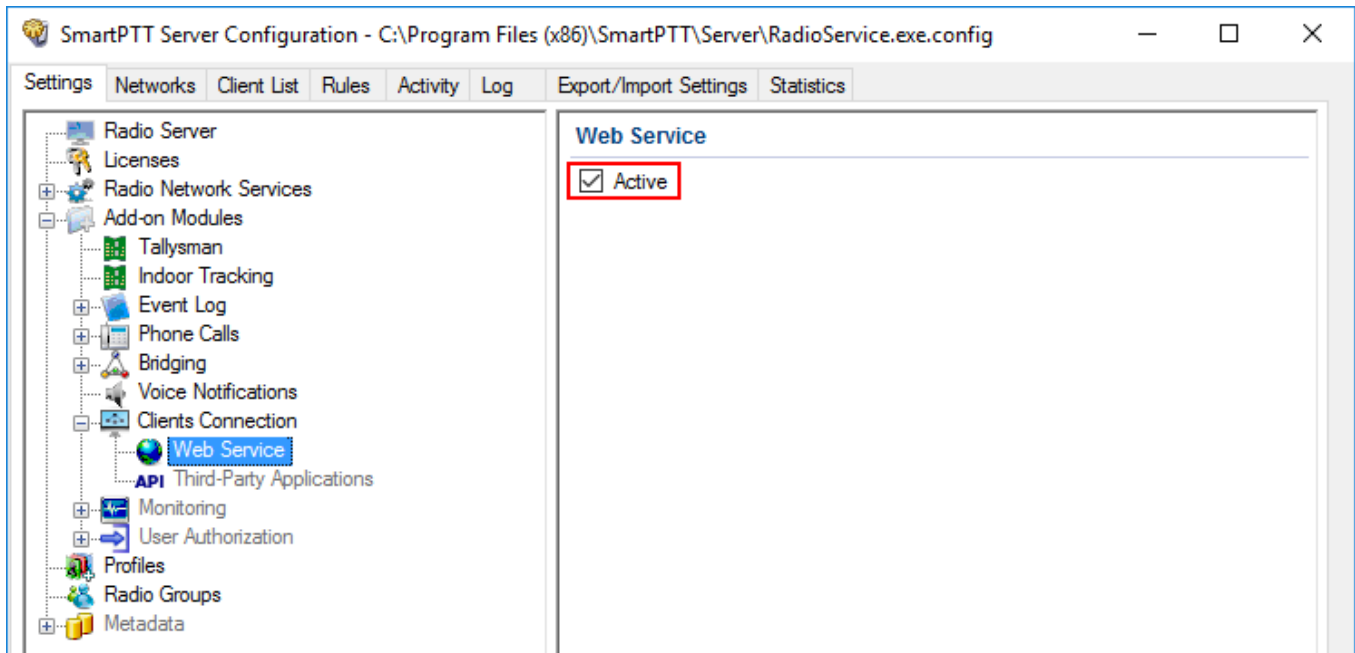
- Displaying radios on Google Maps
- Sending TMS messages to and from radios
- Getting ARS and GPS data
- Blocking and unblocking radios

**NOTE**

To activate web service, install the corresponding license. For more information on how to install licenses, see [Licenses](#).

For more detailed information on web client configuration, refer to SmartPTT Web Client Installation and Configuration Guide.

To enable support for web client, select the **Active** check box in the **Web Service** window of *SmartPTT Radioserver Configurator*.

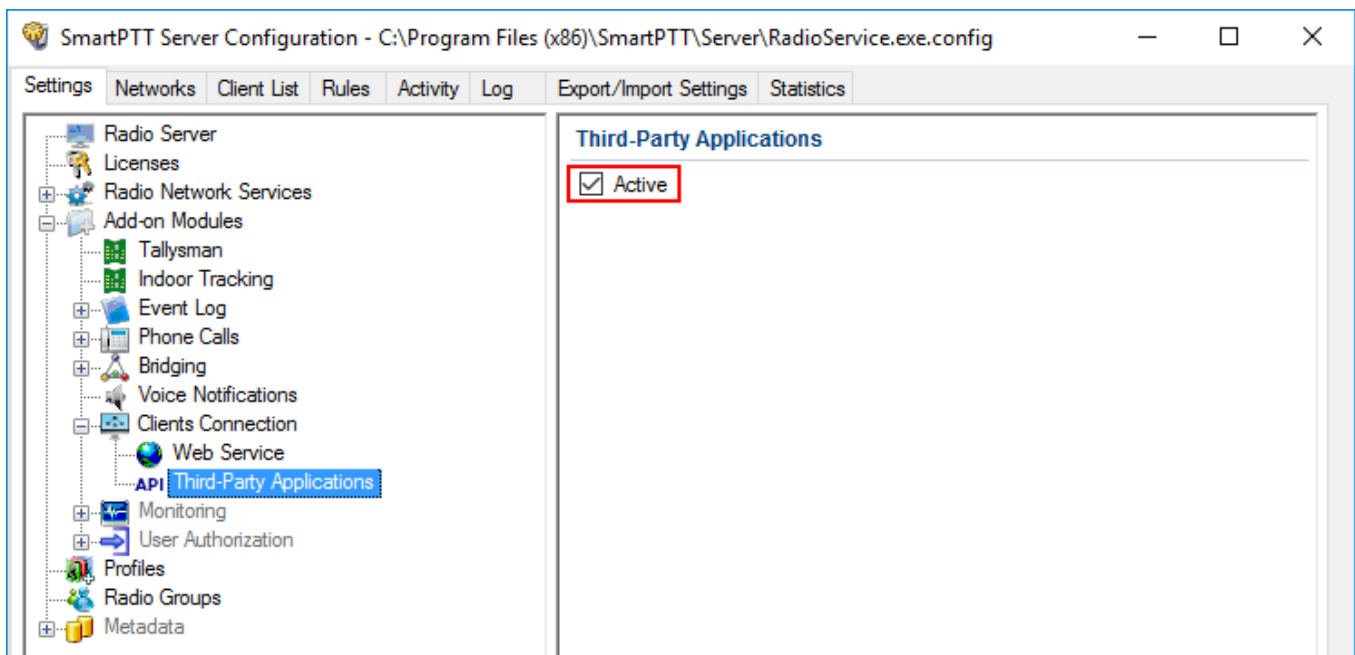


### 1.5.7.2 Third-Party Applications

To allow access to SmartPTT Server API, click **Third-Party Applications** in the setting tree of *SmartPTT Radioserver Configurator* and in the **Third-Party Applications** window select the **Active** check box.

**NOTE**

To get an access to third-party applications, install the corresponding license. For more information on how to install licenses, see [Licenses](#).



## 1.5.8 Monitoring

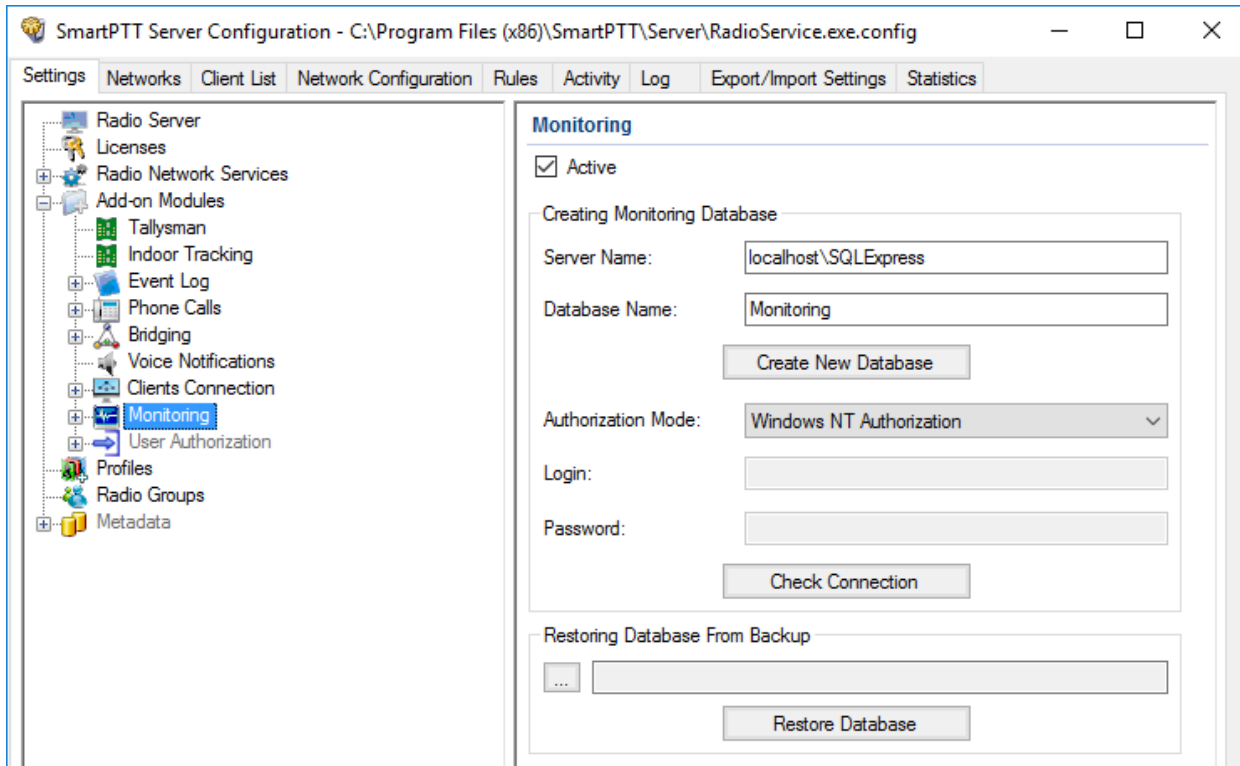
The Monitoring service gives an outlook for the whole radio system in the real time. With the help of this service the dispatcher can see what is happening on the channels and get information on the state of the devices.

### NOTE

Monitoring service requires the corresponding license. For more information on how to install licenses, see [Licenses](#).



By default, the Monitoring service is not active. Select **Monitoring** in the setting tree in *SmartPTT Radioserver Configurator* and select **Active** to enable it. If the **Monitoring** service is not activated, the radioserver and its network won't be displayed on the **Monitoring** panel.



To create a database for the monitoring purpose, type in the **Server Name** and **Database Name** fields, and click **Create New Database**. If creation is successful, a message about successful database creation is displayed. If the database is not created, the cause of the issue will be displayed at the bottom of the window.

#### NOTE

If the database server and SmartPTT Radioserver are installed on one computer, enter the name of the following format: *Computer Name\SQLEXPRESS* (for example, *MYCOMP\SQLEXPRESS*).

Select **Authorization Mode**:

- **SQL Server Authorization: Login and Password** must belong to the account with access to the SQL server.
- **Windows NT Authorization:** The user, who has logged into the Windows system, must be listed in the SQL server user list to make connection.

Click **Check Connection**. In case of successful authorization the message "*The connection is established successfully!*" is displayed. If authorization fails, the reason will appear at the bottom of the window.

**NOTE**

The radioserver event log database, the Monitoring database and the Dispatcher event log database must be different.

**NOTE**

To restore the monitoring database from the backup, select the required database backup file in the **Path** field and click **Restore Database**.

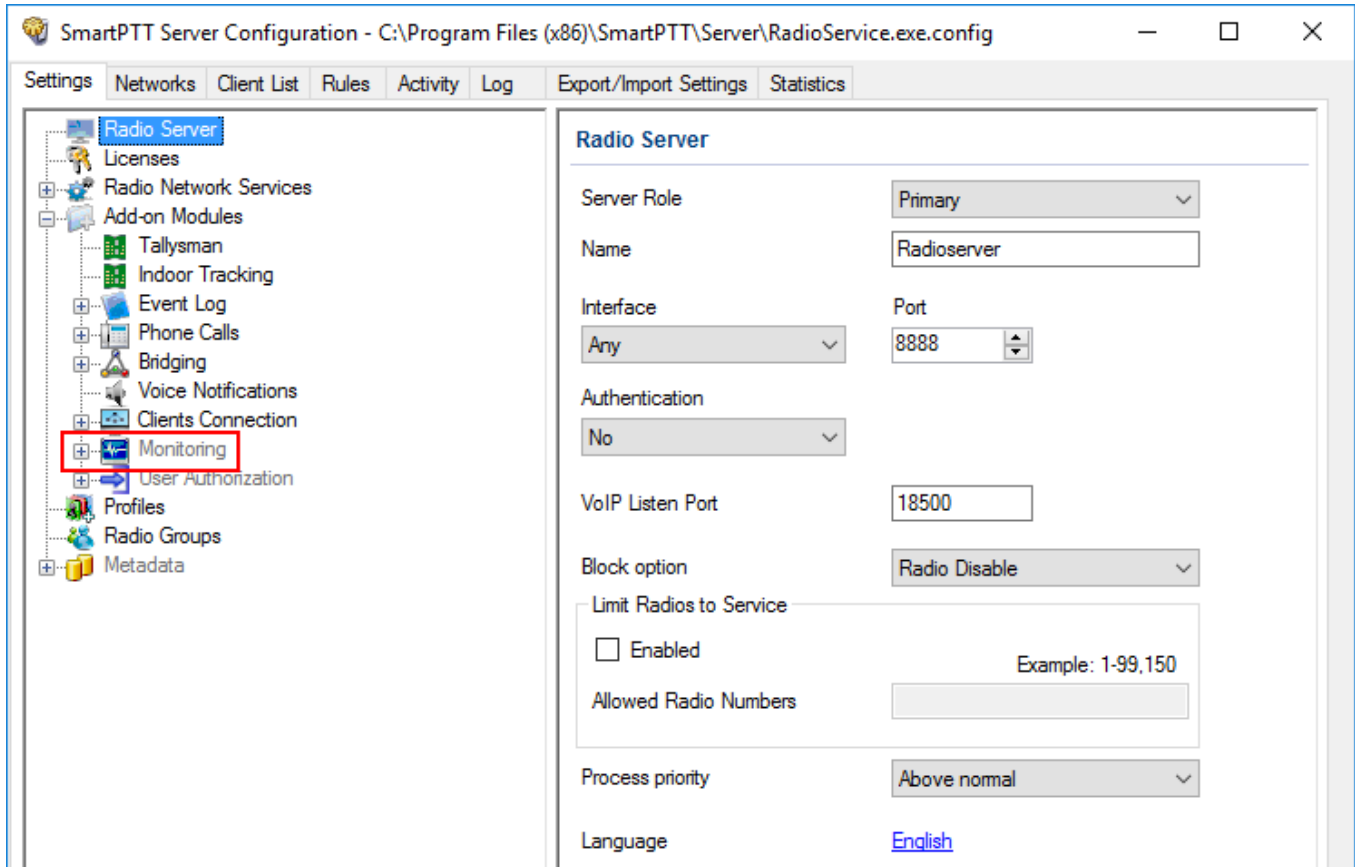
**NOTE**

To set up the auto backup of the monitoring database, go to the [Automatic Database Backup](#) window.

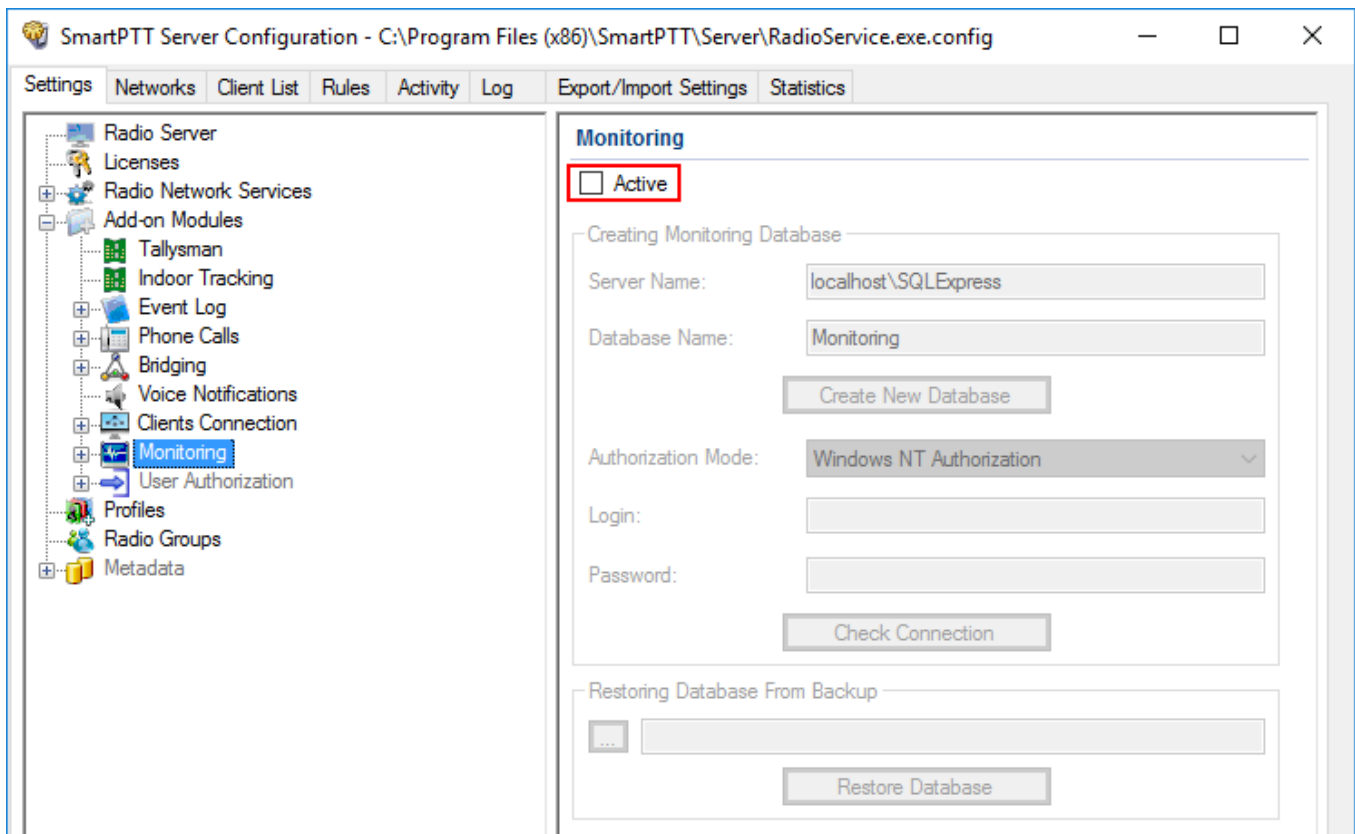
## Creating Database

To create the monitoring database, follow these steps:

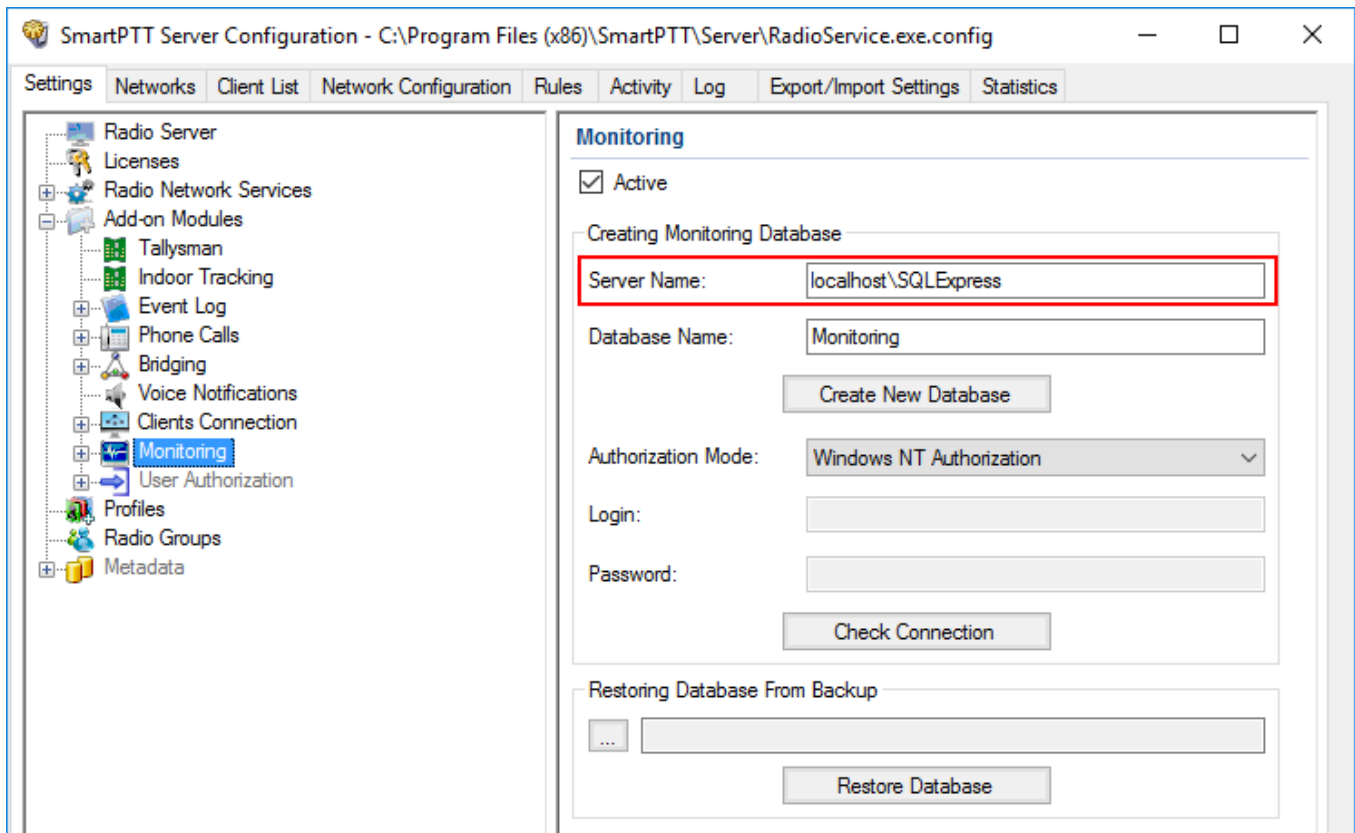
1. In the left pane of the **Settings** tab, expand **Add-on Modules** node and click **Monitoring**.



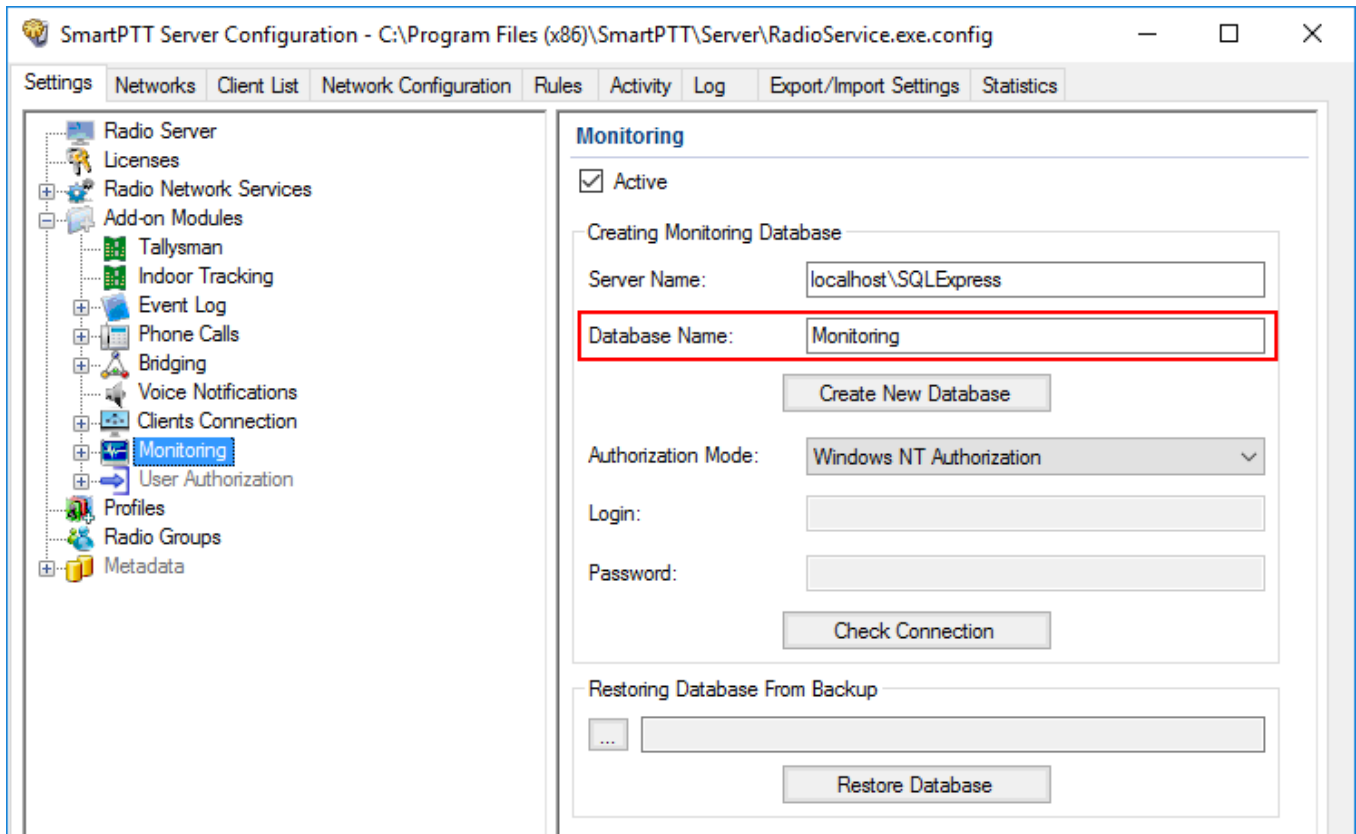
2. Make sure that the **Active** check box is selected in the **Monitoring** pane.



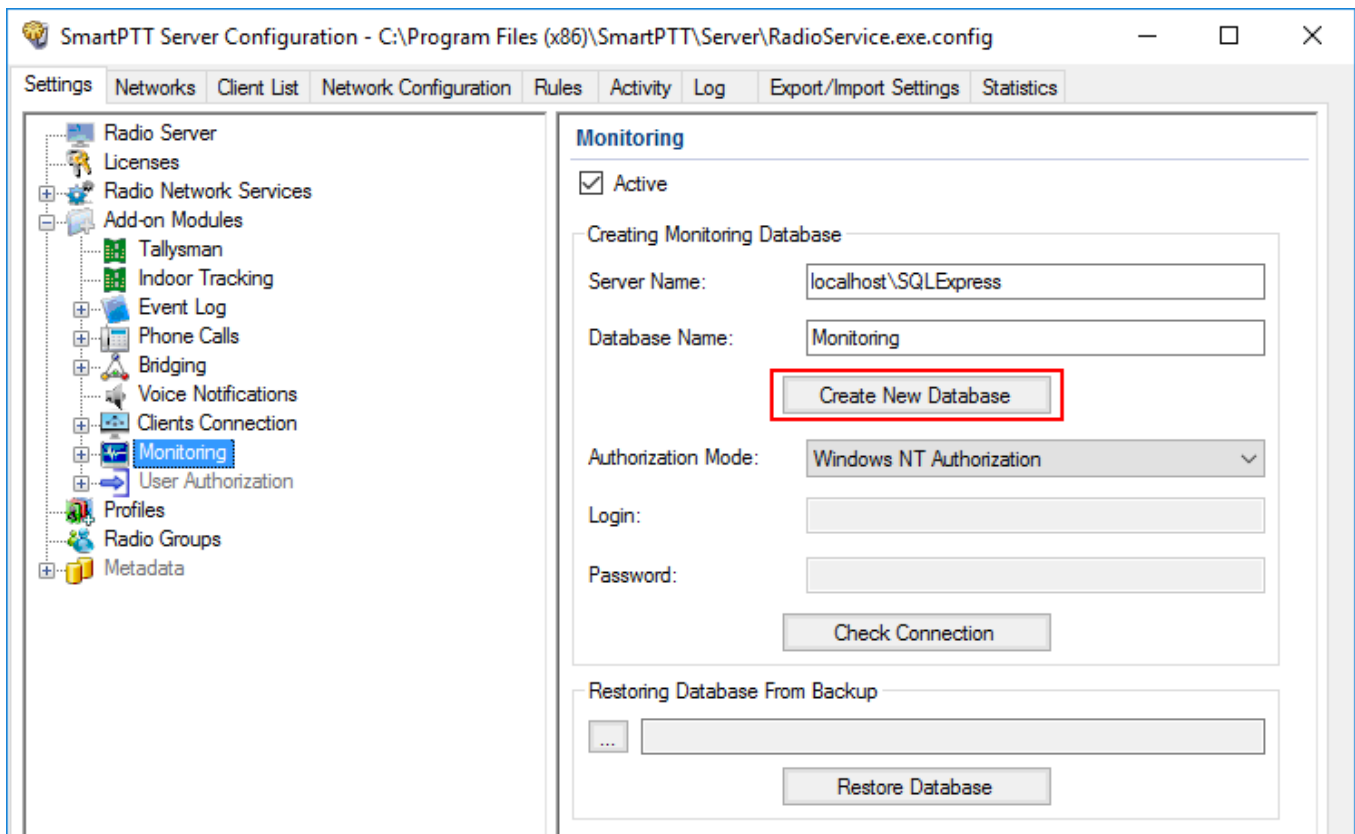
3. In the **Server name** field, enter the name of the SQL Server. You can use either *<IP-address of your computer>\<Your SQL Server name>* or *localhost\<Your SQL Server name>* format:



4. In the **Database Name** field, enter the name of a local monitoring database.



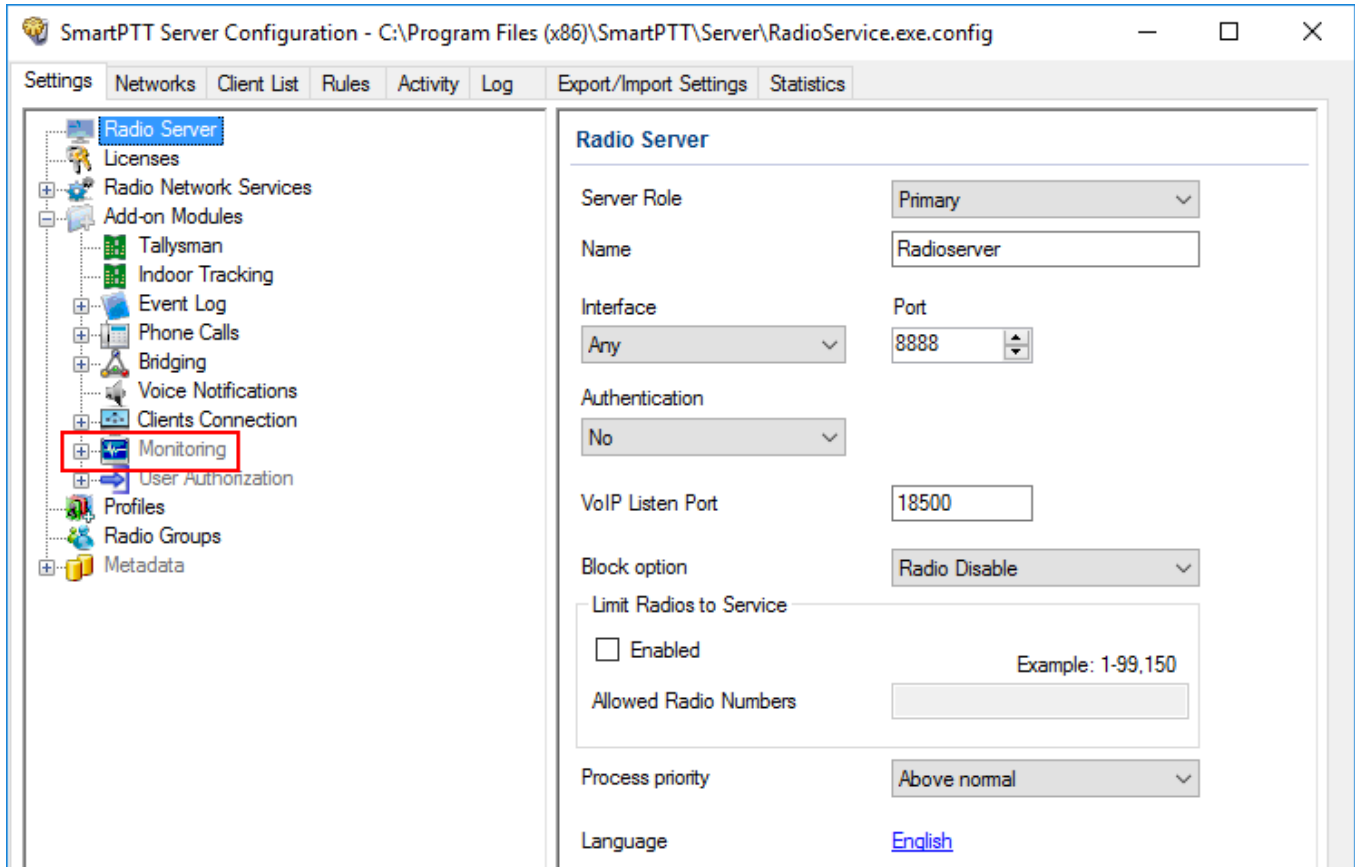
5. Click **Create New Database**.



## Connecting Local Monitoring Database

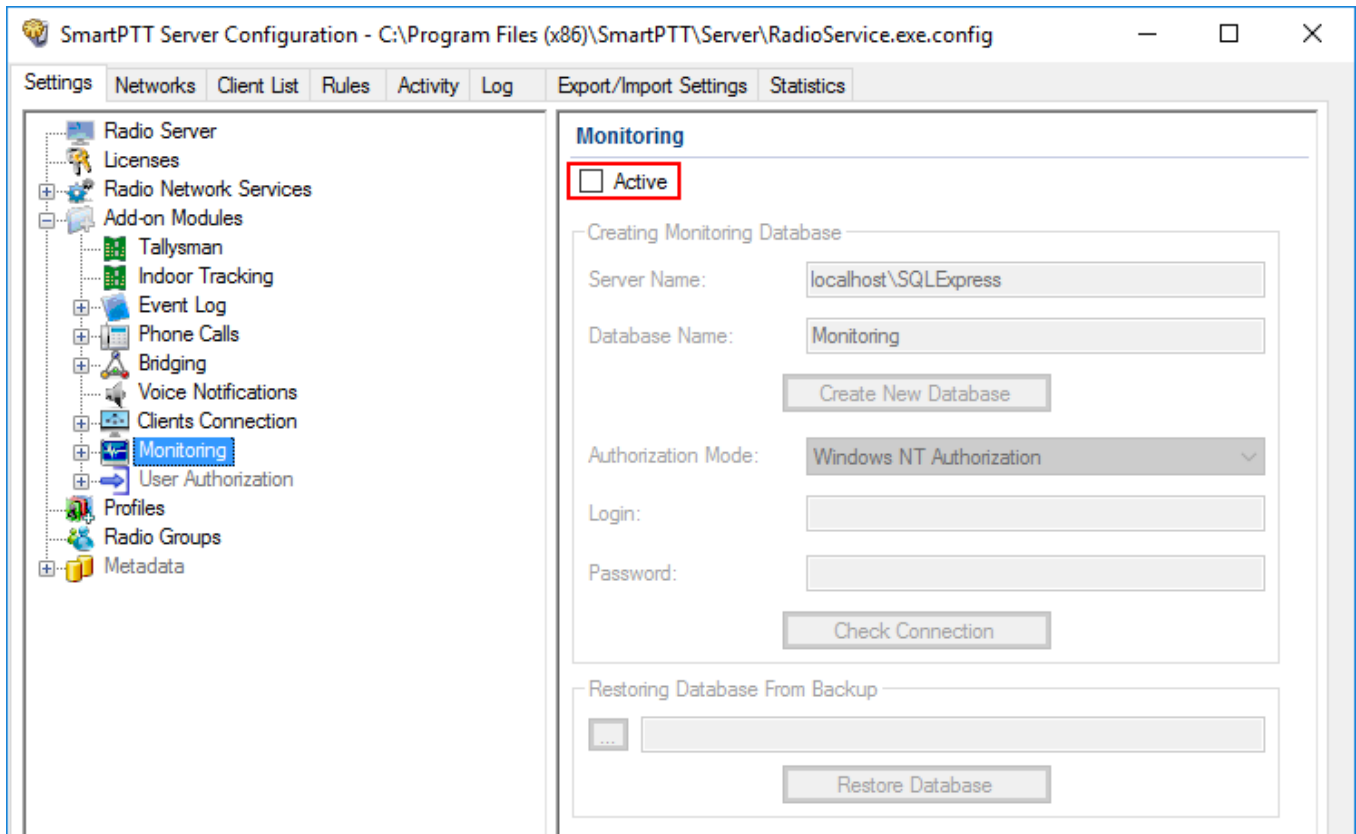
To connect to the local monitoring database, follow these steps:

1. In the left pane of the **Settings** tab, expand **Add-on Modules** node and click **Monitoring**.

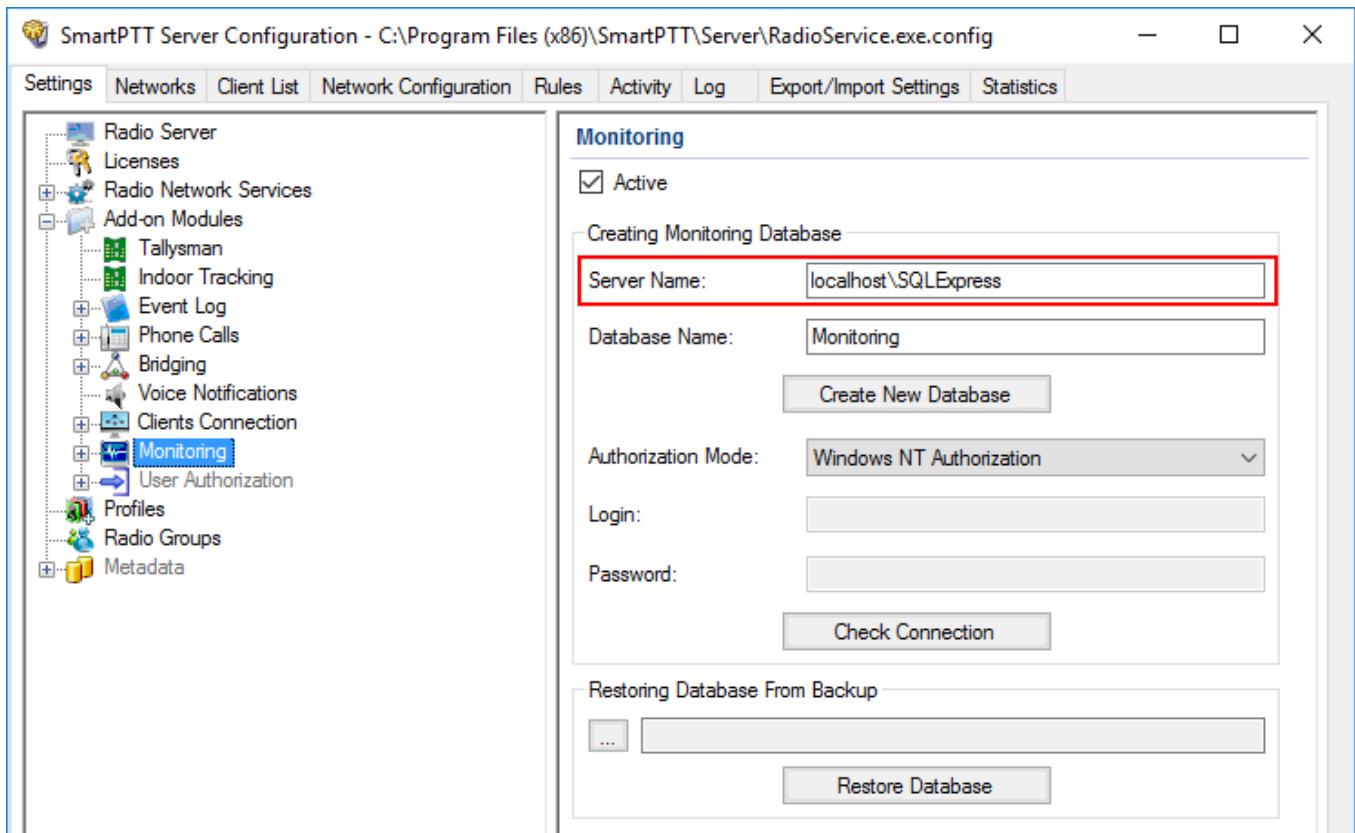




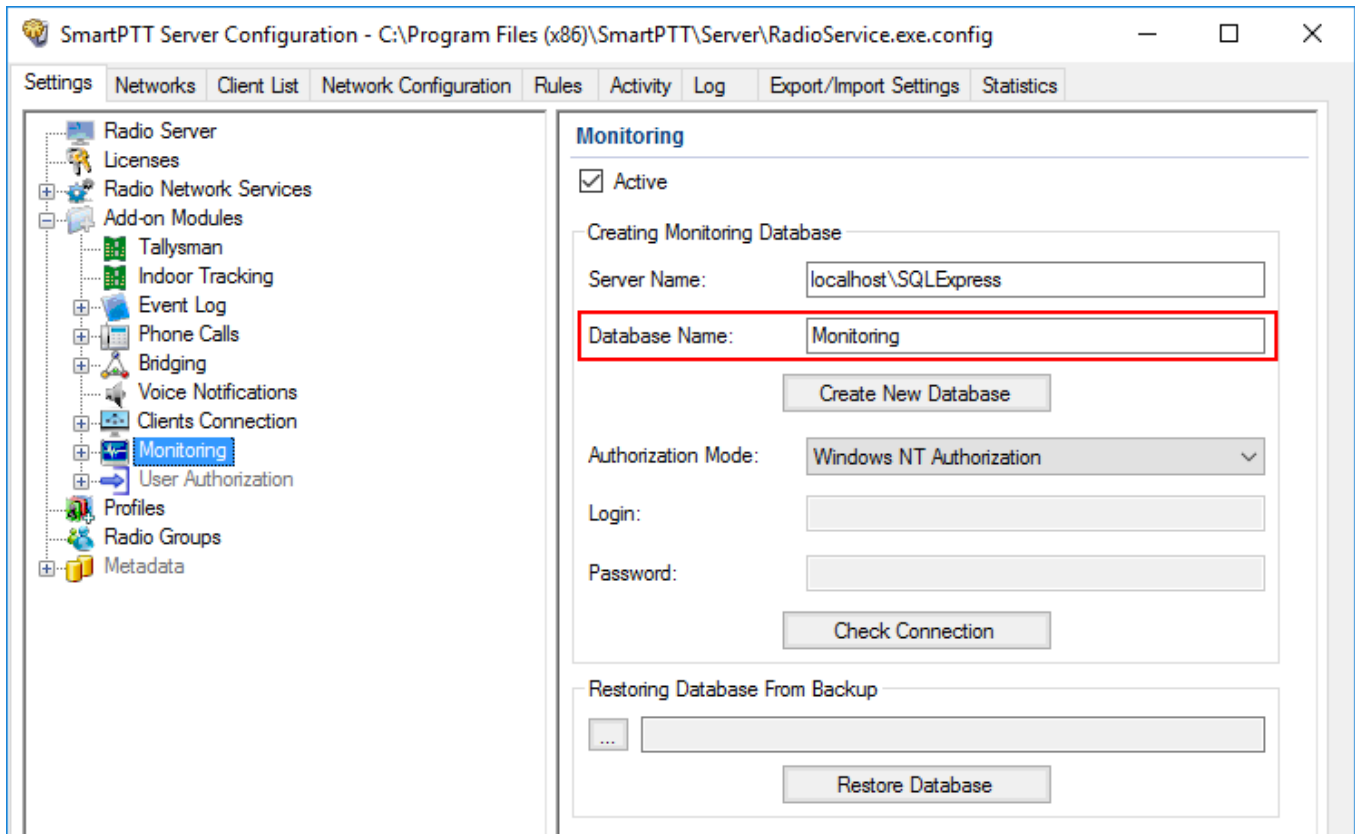
2. Make sure that the **Active** check box is selected in the **Monitoring** pane.



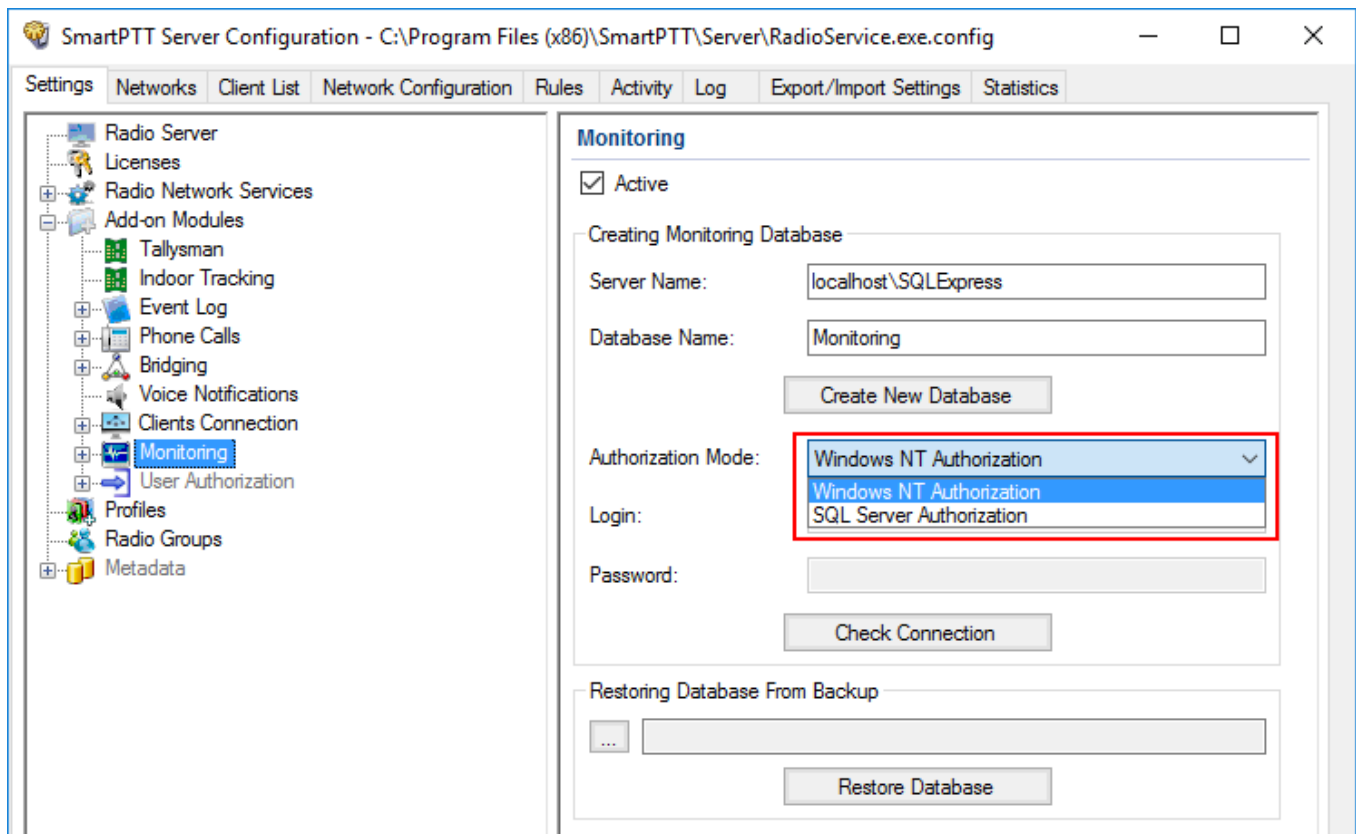
3. In the **Server name** field, enter the name of the SQL Server. You can use either *<IP-address of your computer>\<Your SQL Server name>* or *localhost\<Your SQL Server name>* format:



4. In the **Database Name** field, enter the name of a local Monitoring database.



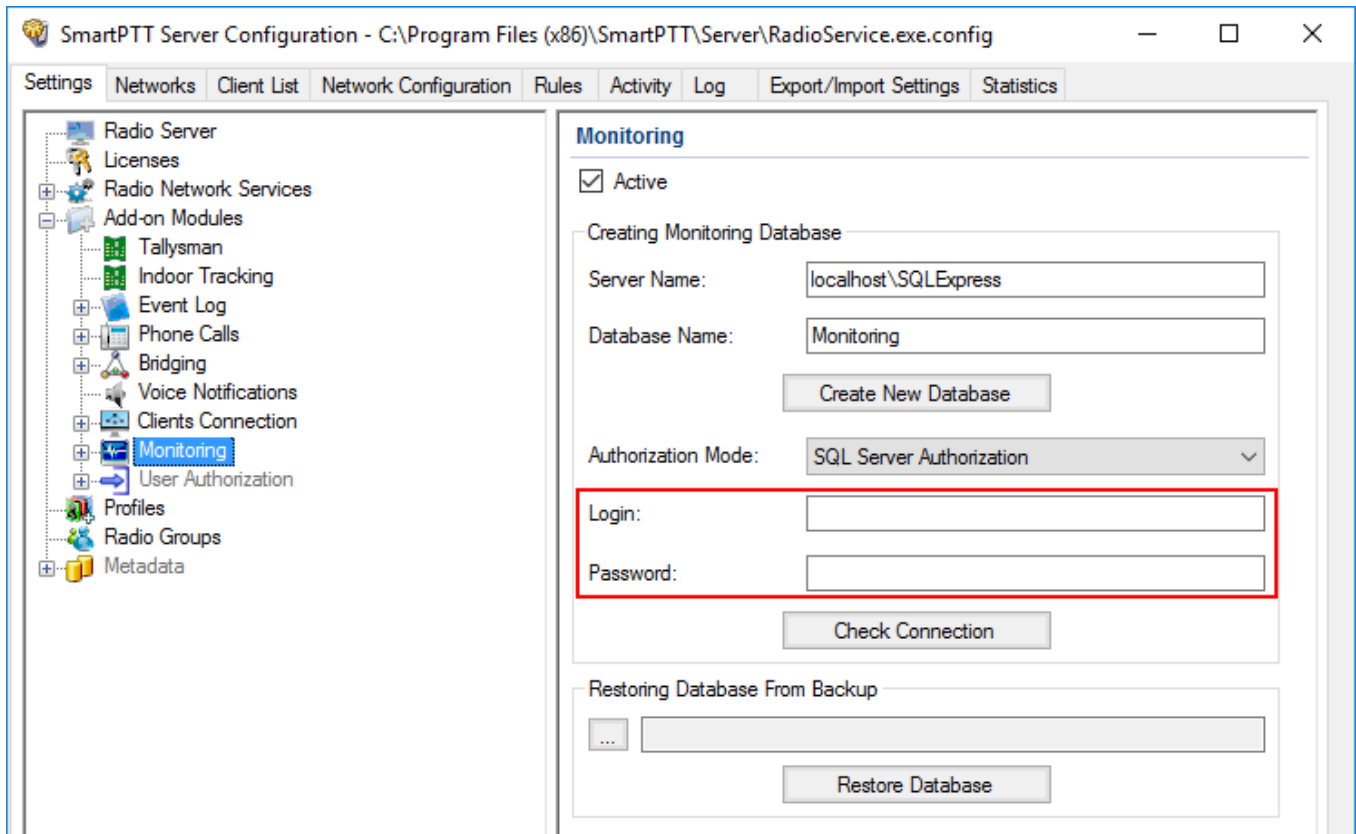
- From the **Authorization Mode** list, select the needed authorization type:



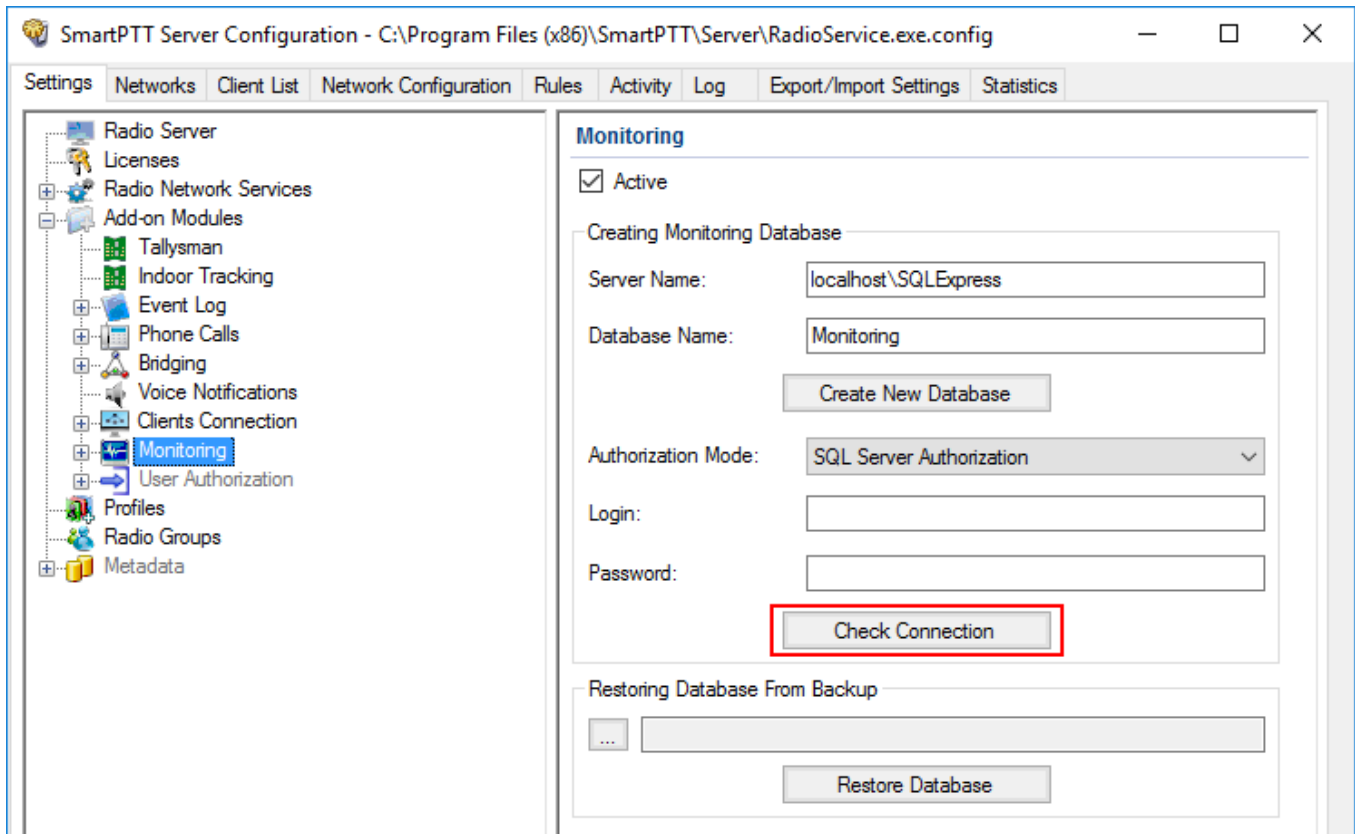
**Windows NT Authorization:** Select to use Windows account for connecting to the local SQL Server.

**SQL Server Authorization:** Select to use SQL Server account for connecting to the local SQL Server.

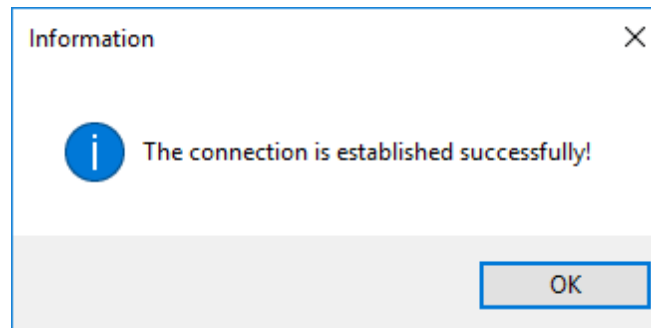
6. If **SQL Server Authorization** is selected, enter login and password.





7. Click **Check Connection**.



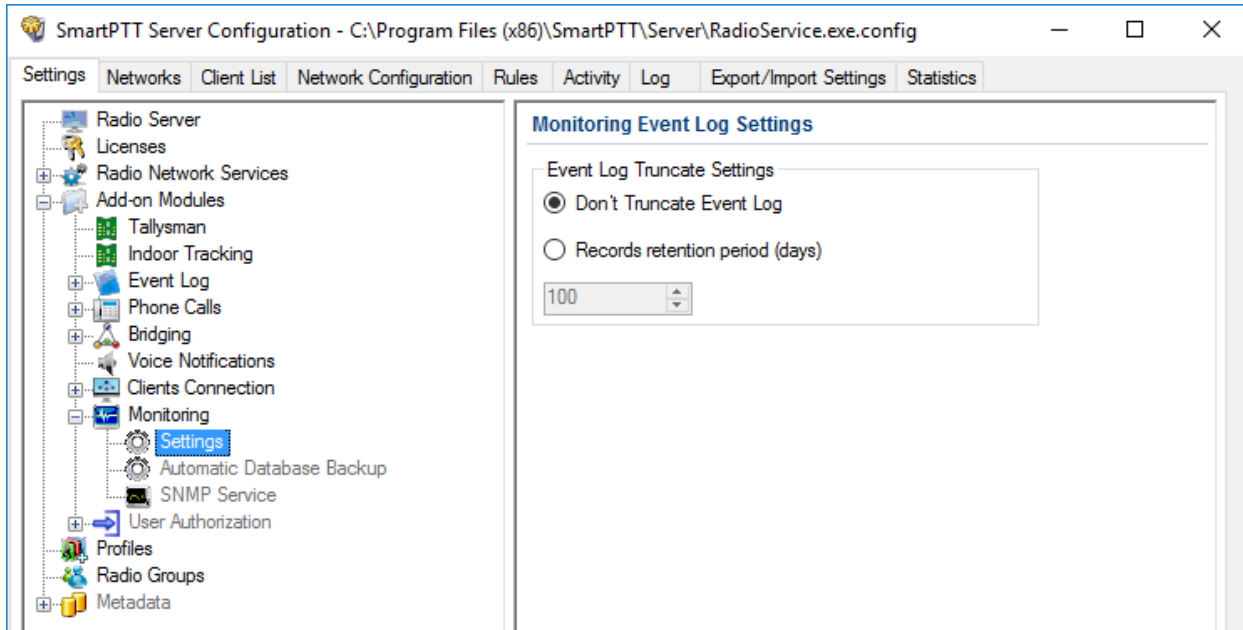
If the connection is successful, the following message appears.



8. Click **Save**  to save changes.
9. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

## 1.5.8.1 Settings

To configure automatic cleaning for the monitoring event log, go to the **Settings** section of the monitoring in *SmartPTT Radioserver Configurator*. The following window appears:



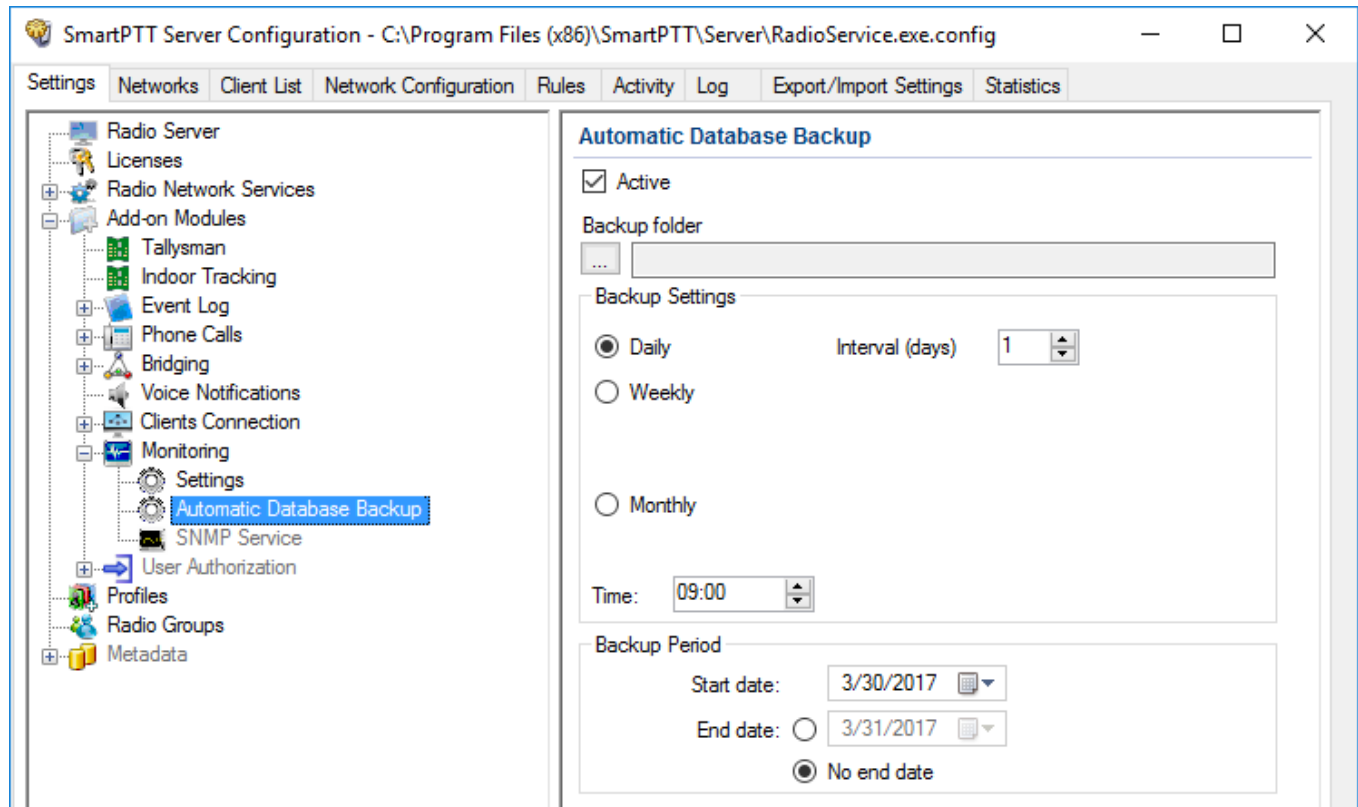
**Don't Truncate Event Log:** If selected, monitoring event log is not cleared automatically.

**Records retention period (days):** If selected, the system will delete records older than the number of days set in the field. By default, it is set to 100 days.

## 1.5.8.2 Automatic Database Backup

Backing up data on a regular basis helps to protect it from being erased in case of the server hardware or software failure. *SmartPTT Radioserver Configurator* allows to back up the monitoring database automatically.

In order to set up automatic backup schedule of the monitoring database, select **Automatic Database Backup** under **Monitoring** in the setting tree of *SmartPTT Radioserver Configurator*.



**Active:** Select the check box to enable the ability to create current monitoring database backups in the automatic mode.

**Backup folder:** Full path to the file for saving the database backup.

**Backup Settings:** Schedule for creating the current database backup.

**Daily:** Every fixed day at the specified time (for example, every day, every third day at 9:00 a.m.).

**Weekly:** Every fixed day of the week at the specified time (for example, every Monday, Wednesday and Friday at 11:00 p.m.).

**Monthly:** Once a month on the fixed day of the selected month and at the specified time.



**Backup Period:** Allows you to set time period when automatic database backup is to be made according to the selected backup settings.

**NOTE**

The number of stored backup files in the same folder is limited to 3. Otherwise, when creating a new copy, the old files are deleted.

**NOTE**

The monitoring database recovery from the automatically created backup is performed manually in the [Monitoring](#) window.

### 1.5.8.3 SNMP Service

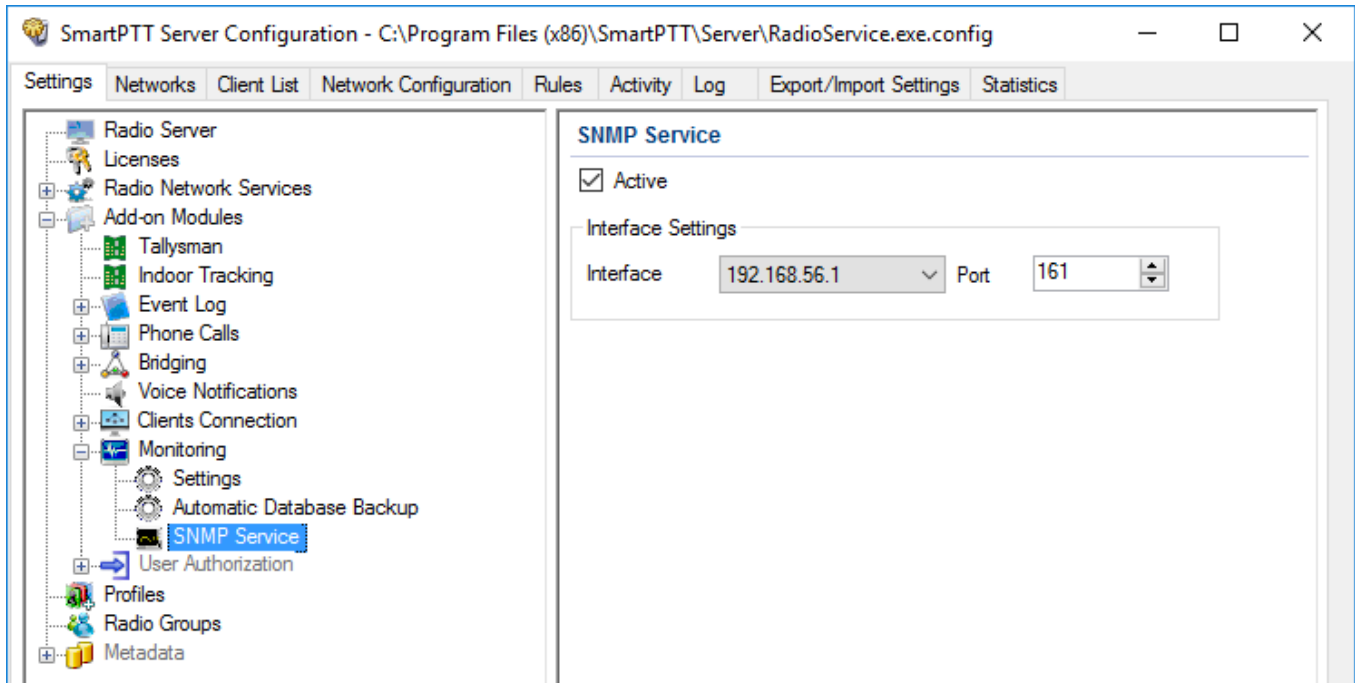
SNMP service allows to monitor network-attached devices such as repeaters, routers and uninterruptible power supplies (UPS).

To be able to get information about the state of a device, you need to have an SNMP client application installed. Use versions 1 and 2 of SNMP client applications. **Monitoring** must be activated, otherwise you won't be able to enable **SNMP Service**.

**NOTE**

SNMP service requires the corresponding license. For more information on how to install licenses, see [Licenses](#).

After you have obtained the license, enable SNMP service. To do that, select **Add-on Modules** → **Monitoring** → **SNMP Service**. The following window appears:

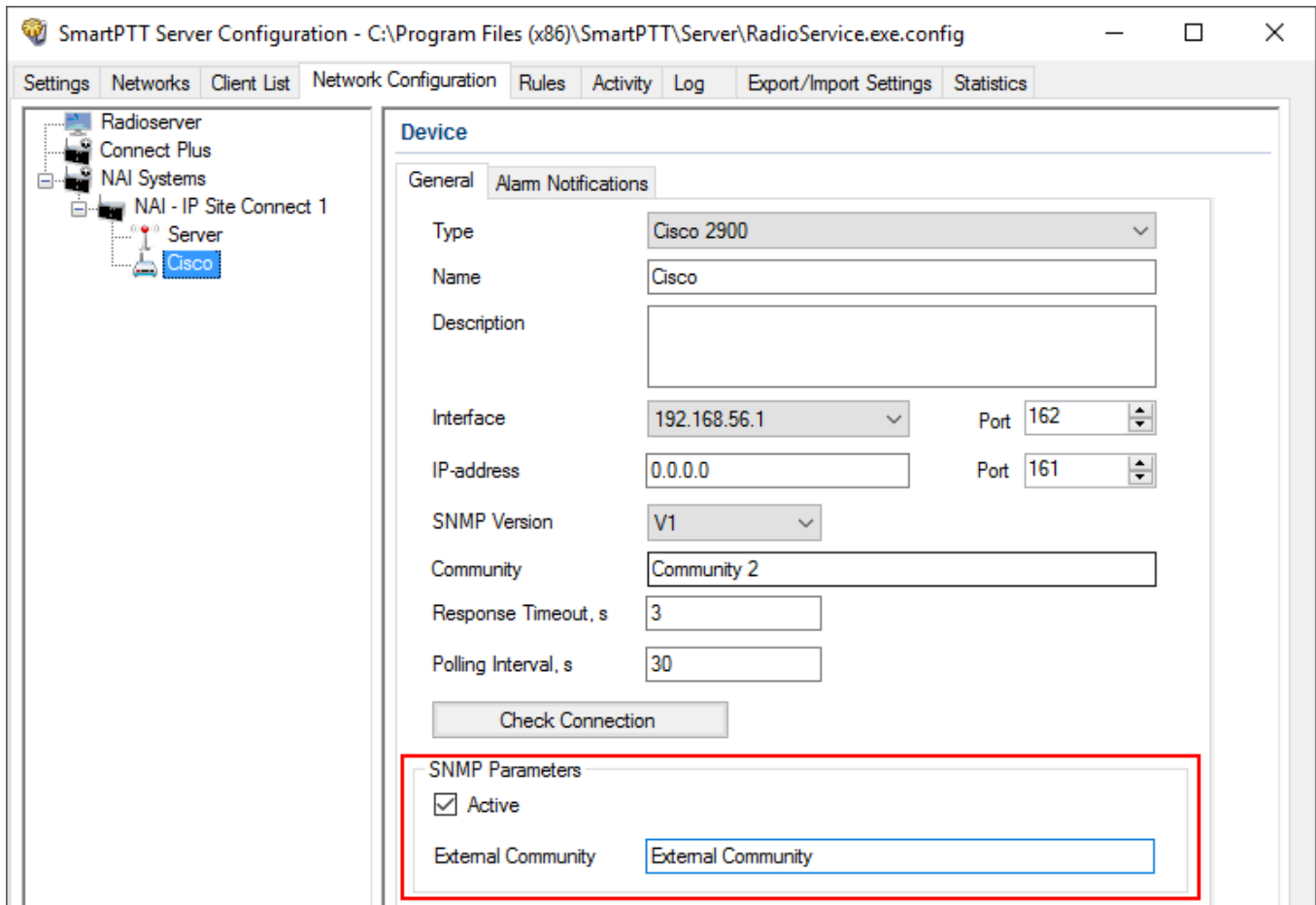


Select the **Active** check box to enable the service. The **Interface Settings** will become available.

**Interface:** The IP address of SmartPTT Radioserver.

**Port:** Port to listen to the data from the devices. By default, it is set to port 161.

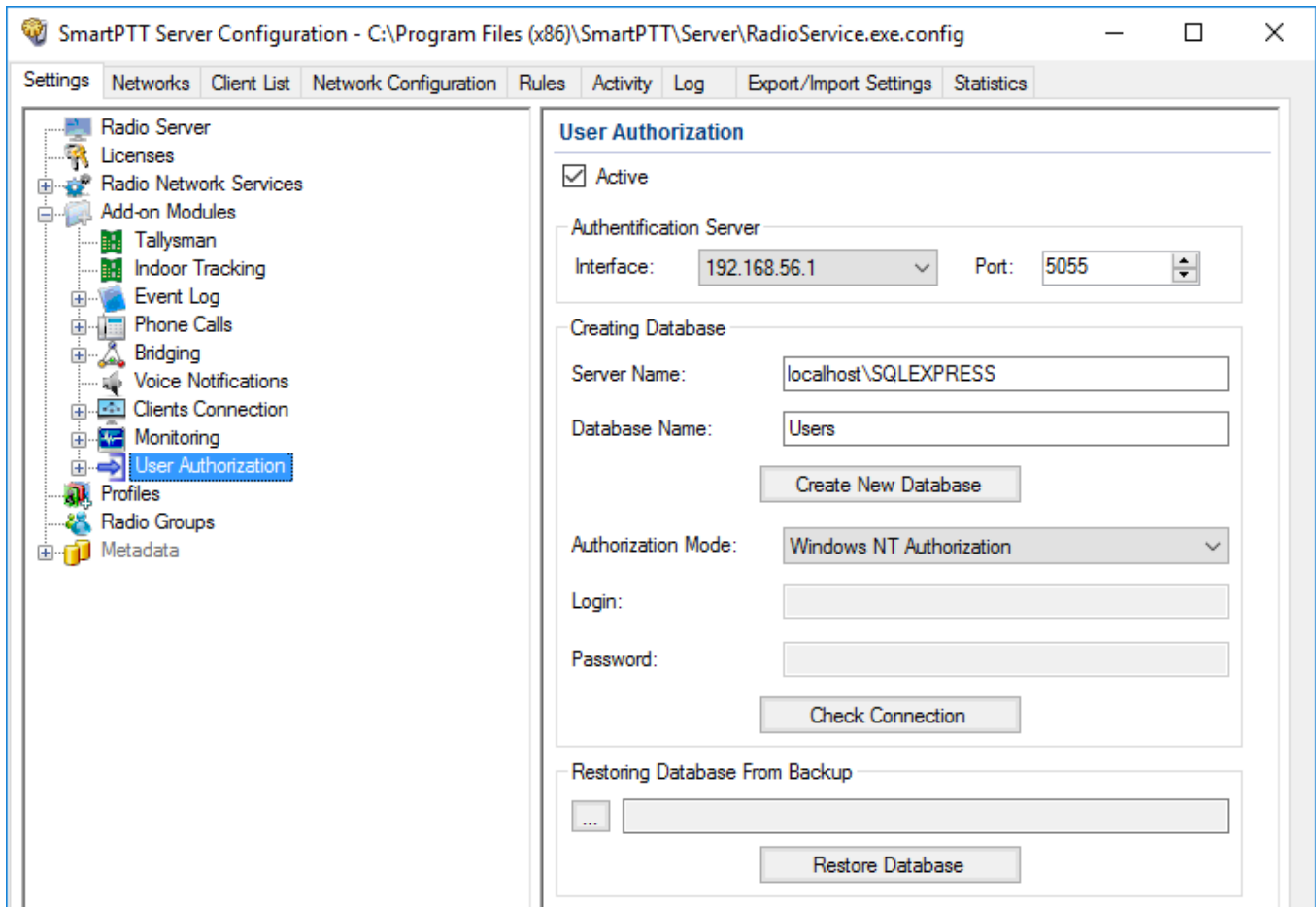
Then, install SNMP client application. Configure its settings to contain the IP address of the radioserver to get information on the devices, and the **External Community** to get information on particular device parameters. The **External Community** can be found in *SmartPTT Radioserver Configurator* in the **Network Configuration** tab for each device.

**NOTE**

For more information how to get device parameters, read documentation or review the corresponding MIB file of the device.

## 1.5.9 User Authorization

Companies with a great number of staff members often require control and accounting of radio use, namely to know the current radio user. For this purpose user authorization is implemented in SmartPTT Radioserver.



User authorization allows the dispatcher to identify the worker using the channel.

For proper work of the user authorization you should preconfigure the radio and set specific networks. The radio is configured in the *MOTOTRBO CPS* program. NAI networks are configured in the *MOTOTRBO DDMS* program and Capacity Max networks are configured in the *Radio Management* program.

---

*MOTOTRBO CPS*, *MOTOTRBO DDMS* and *Radio Management* settings include:

### **Configuring Radio**

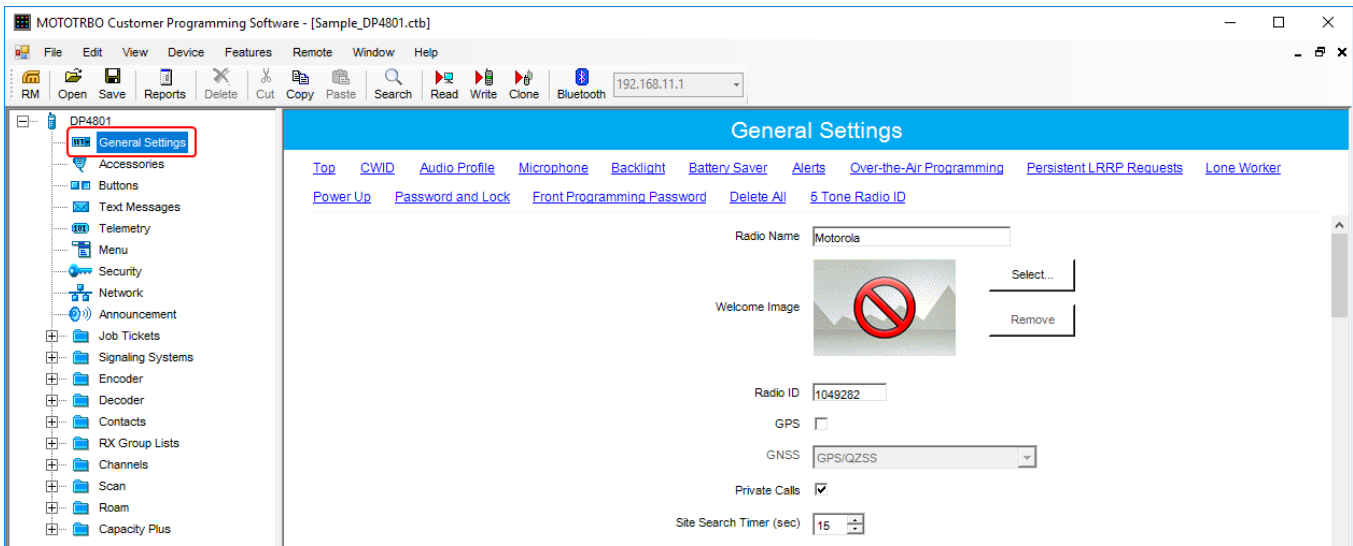
The following section describes the configuration of the radio in *MOTOTRBO CPS*. There are two ways to configure the radio:

- To connect the radio to the computer and to update its firmware.
- To preconfigure the firmware file and to use it for updating the radio firmware.

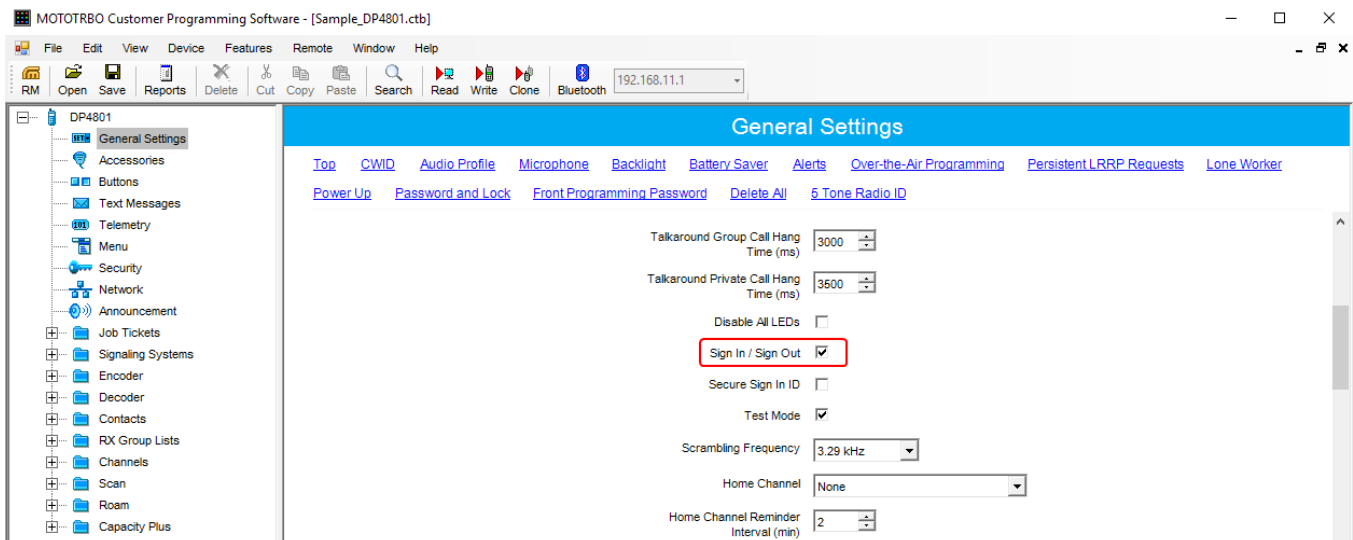
To configure the radio, follow these steps:

1. Run *MOTOTRBO CPS*.
2. Read the radio firmware or open the radio firmware file.

3. In the left pane, click **General Settings**.



4. In the **General Settings** pane, select the **Sign In/Sign Out** check box.



### WARNING


Do not unplug your cable from the radio or computer until the radio firmware update complete.

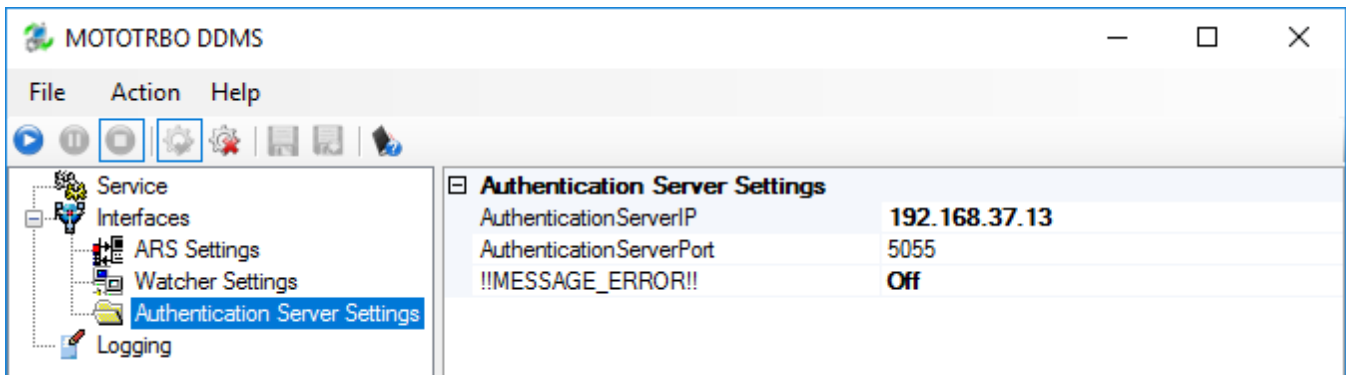
5. Update the radio firmware or save the radio firmware file for the following updating.

## Configuring DDMS service

To configure MOTOTRBO DDMS settings, follow these steps:

1. Run MOTOTRBO DDMS.

- Click **Stop**  to stop DDMS service.
- In the left pane, expand the **Interfaces** node and click **Authentication Server Settings**.



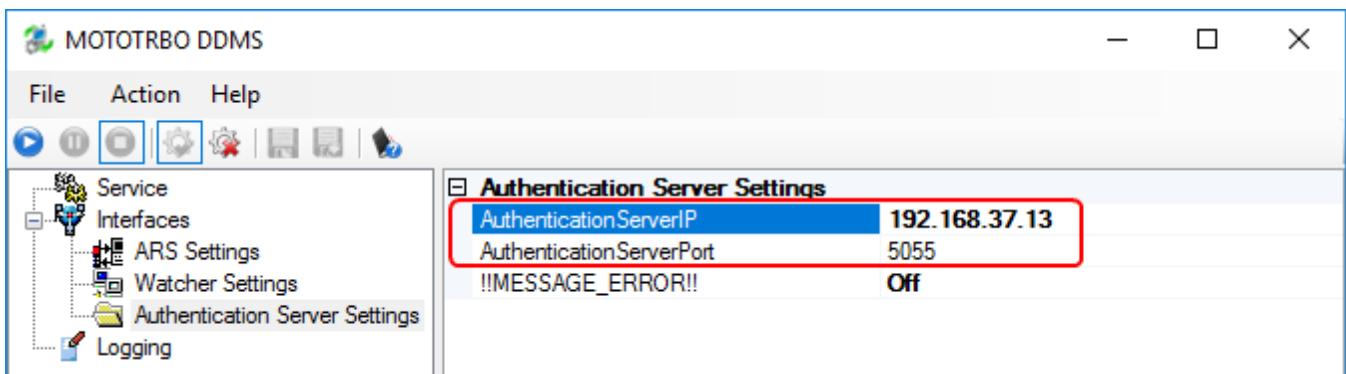
- In the **Authentication Server Settings** pane, specify the following parameters.

**Authentication Server IP:** Enter the [IP-address of the authentication server](#).

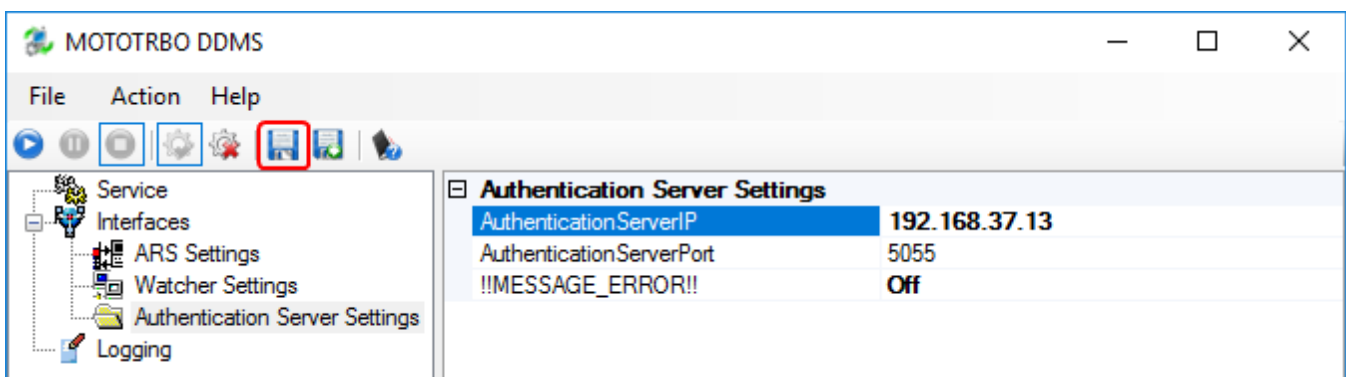
#### NOTE


By default, the authentication server has the IP address of the primary radioserver.

**Authentication Server Port:** Enter the port of the authentication server.



- Click **Save Configuration**.




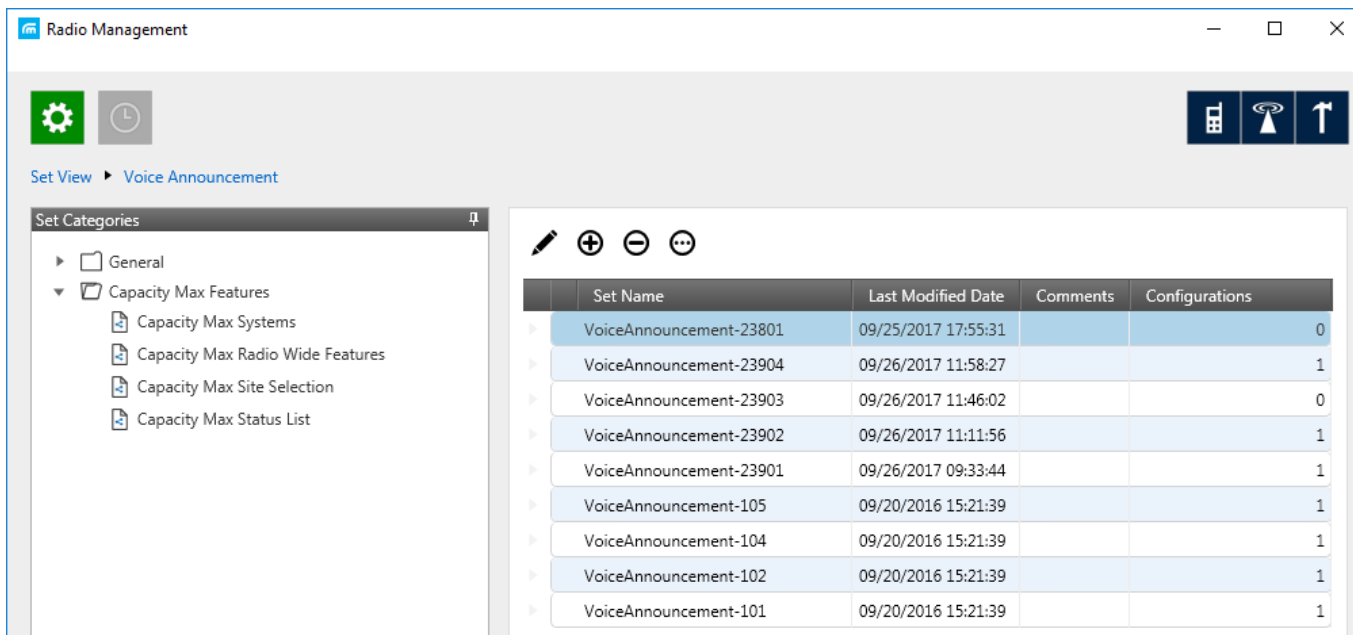
- Click **Start**  to start DDMS service.

## Configuring Capacity Max


For proper work of the authentication server, you should set Capacity Max networks. Capacity Max networks are configured in the program *Radio Management*.

To configure Capacity Max settings in *Radio Management*, follow these steps:

- Run *Radio Management*.
- Click **Actions** .
- From the **Manage** list, select **Sets**.
- In the **Set Categories** pane, expand the **Capacity Max Features** node.

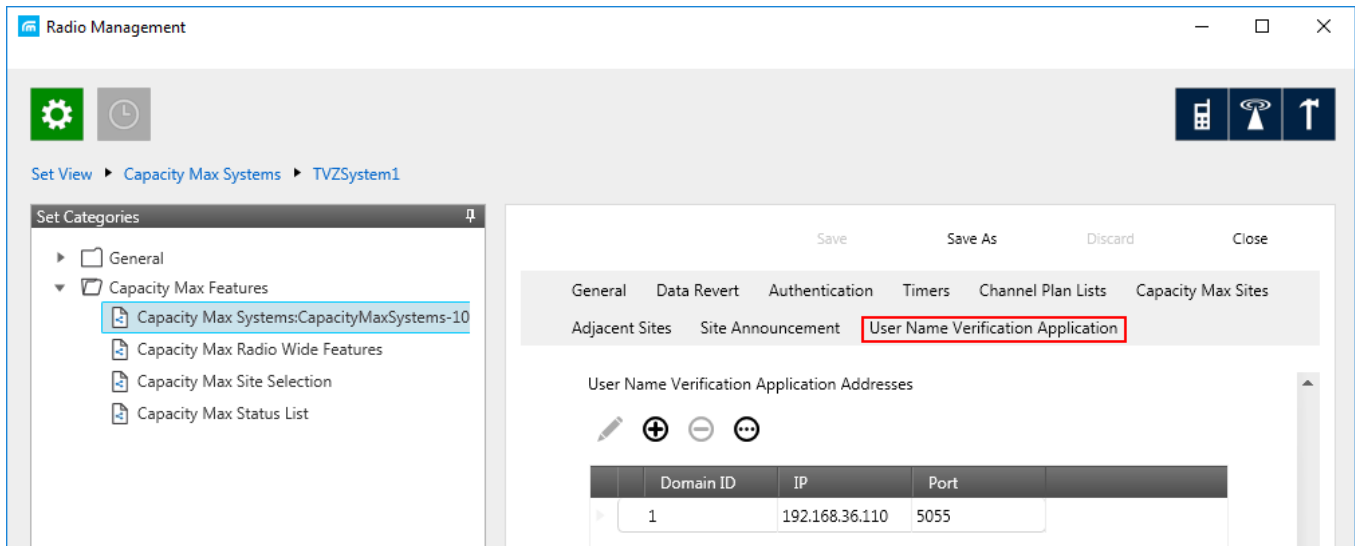


Set Name	Last Modified Date	Comments	Configurations
VoiceAnnouncement-23801	09/25/2017 17:55:31		0
VoiceAnnouncement-23904	09/26/2017 11:58:27		1
VoiceAnnouncement-23903	09/26/2017 11:46:02		0
VoiceAnnouncement-23902	09/26/2017 11:11:56		1
VoiceAnnouncement-23901	09/26/2017 09:33:44		1
VoiceAnnouncement-105	09/20/2016 15:21:39		1
VoiceAnnouncement-104	09/20/2016 15:21:39		1
VoiceAnnouncement-102	09/20/2016 15:21:39		1
VoiceAnnouncement-101	09/20/2016 15:21:39		1

- Click **Capacity Max Systems**.
- In the right pane, click the required Capacity Max System.
- Click **Edit** .



8. Click **User Name Verification Application**.



9. In **User Name Verification Application Addresses** pane, specify the following parameters:

**IP:** Enter the [IP-address of the authentication server](#).



**NOTE**

By default, the authentication server has the IP address of the primary SmartPTT Radioserver.

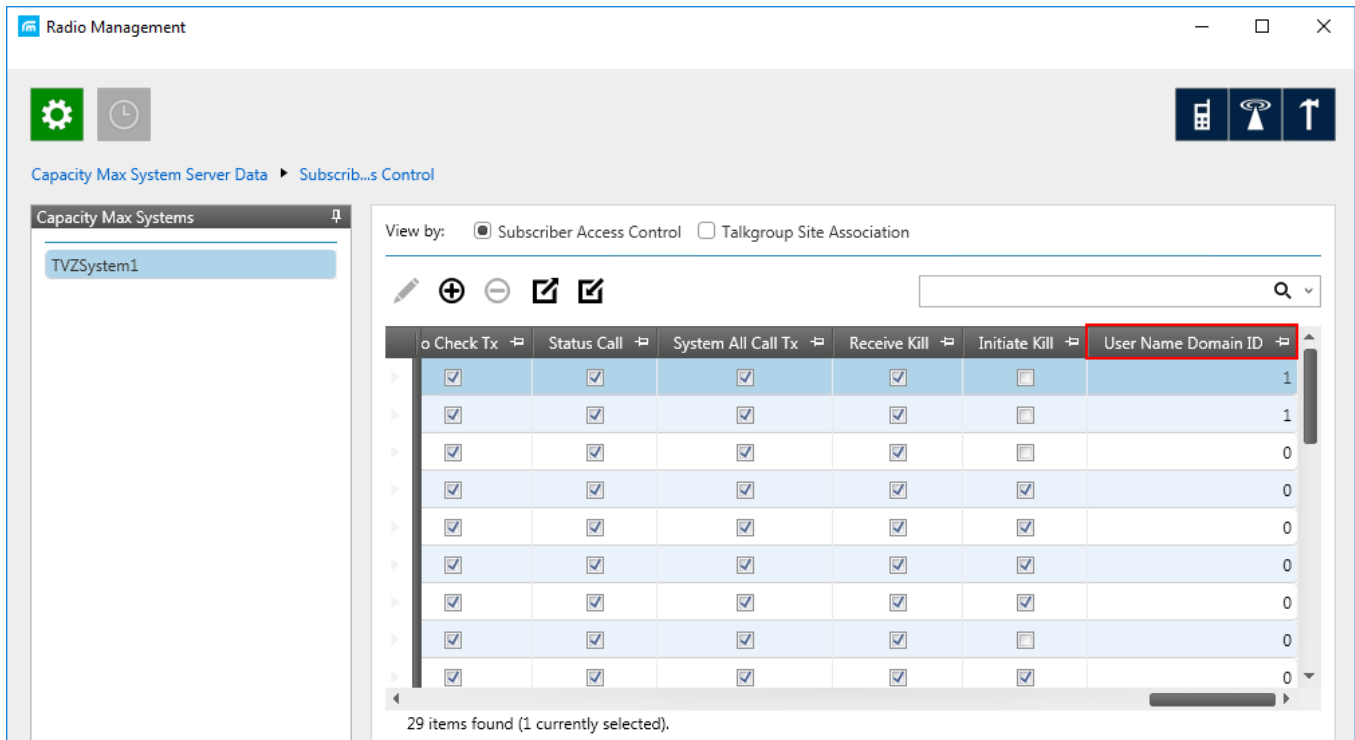
**Port:** Enter the port of the authentication server.

**Domain ID:** Specify ID for authentication server in Radio Management.

After this, perform the following actions to save the changes in the *Radio Management* program.

1. Click **Radio View**  to open the main menu.
2. Click **Actions** .
3. From the list, select **Manage** → **Capacity Max System Server Data**.
4. In the right pane, click the desired radio.


- In the **User Name Domain ID** field, specify the value from 0 to 16.



The screenshot shows the 'Radio Management' application window. On the left, there is a sidebar with 'Capacity Max Systems' and 'TVZSystem1' selected. The main area displays a table with the following columns: 'Check Tx', 'Status Call', 'System All Call Tx', 'Receive Kill', 'Initiate Kill', and 'User Name Domain ID'. The 'User Name Domain ID' column is highlighted in red. The table contains 29 rows of data, with the first row having a value of 1 and the others having values of 0. A search bar and view options are visible above the table.

Check Tx	Status Call	System All Call Tx	Receive Kill	Initiate Kill	User Name Domain ID
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0

29 items found (1 currently selected).

- Click **Radio View**  to open the main menu.
- Right click on the radiostation that was modified.
- Select **Schedule job**.

9. In the **Schedule job** window, click **OK**.

**Schedule Job**

**Job Type**

Write  No Switchover

Switchover

Read  Generate configuration

Apply to radio

**Connection Method**

USB + Wireless (LAN)  IP Program  Over the Air  Any

Suppress ARS after Switchover Switchover Timer (min):

**Job Name:**

**Time Zone:**

**Start after**

**End before**

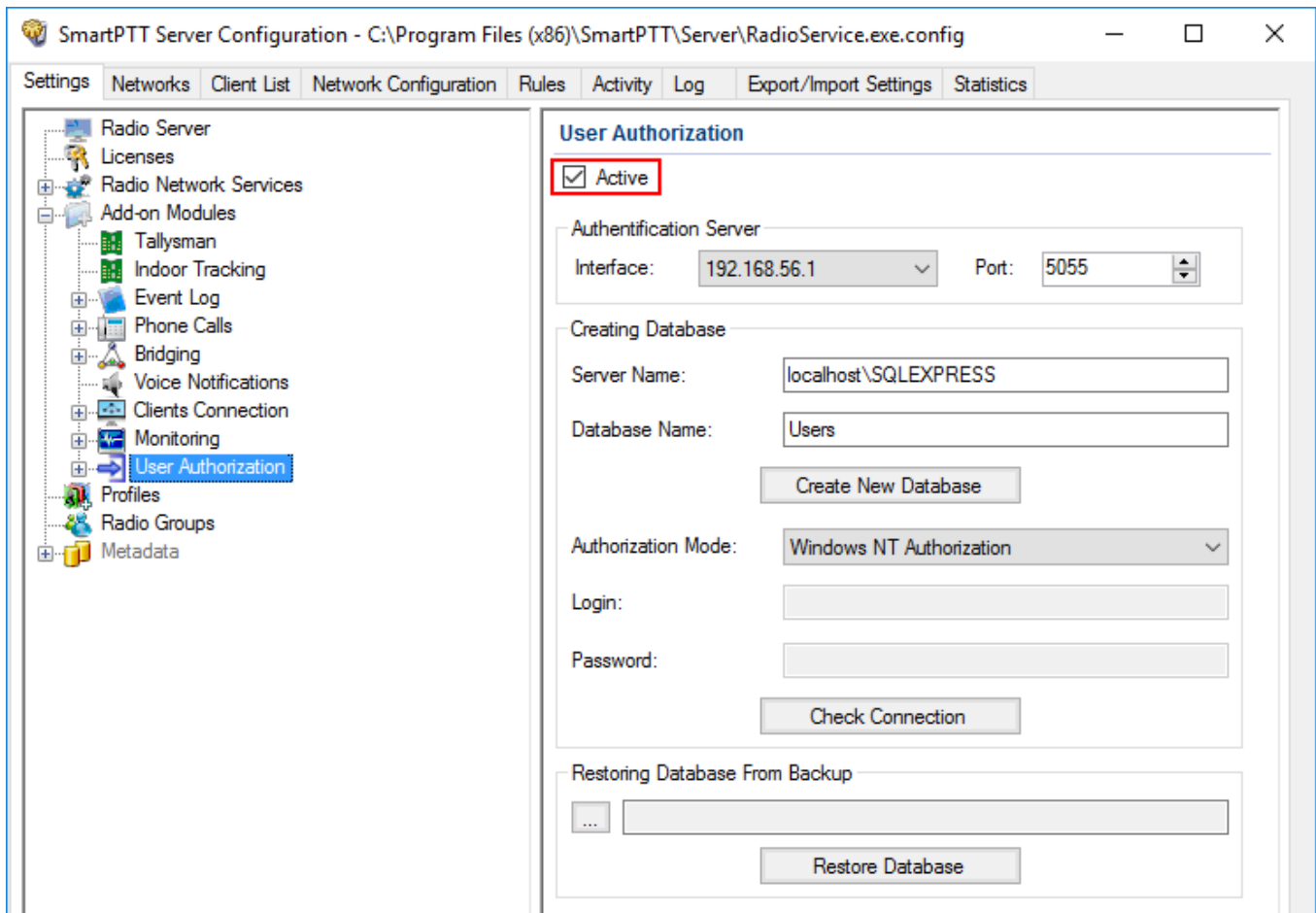
**OK** **Cancel**

When preliminary configuration of radio equipment complete, User authorization configuration should be made. This includes the following:

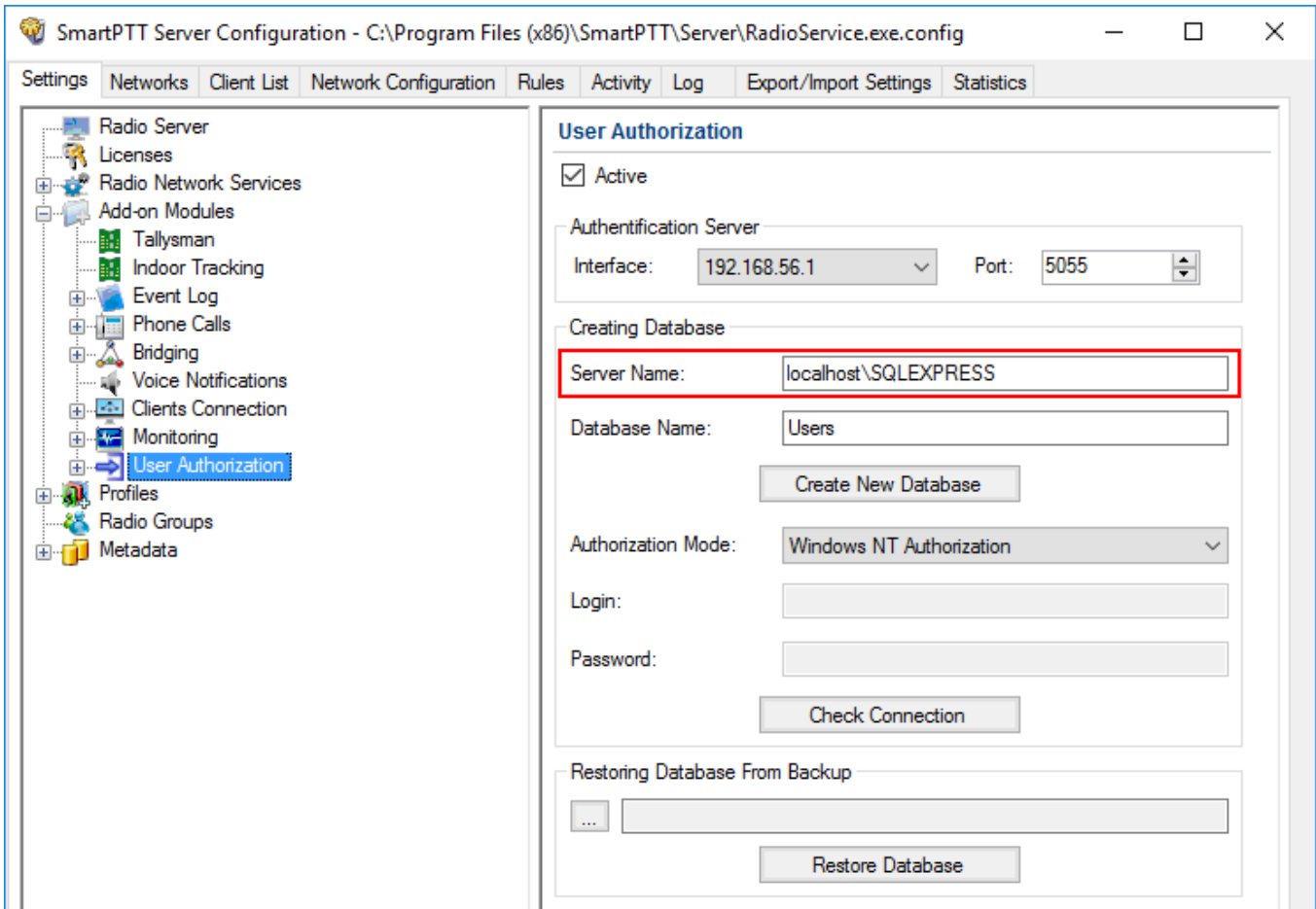
## Creating User Authorization Database

To create the authentication server database, follow these steps:

1. In the left pane of the **Settings** tab, expand the **Add-on Modules** node and click **User Authorization**.
2. In the **User Authorization** pane, select the **Active** check box.

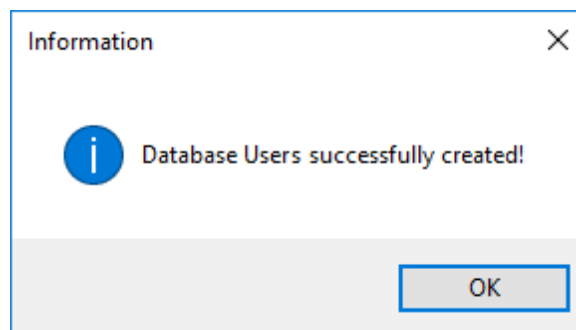




3. In the **Server Name** field of the **Creating Database** area, enter the name of the SQL Server. You can use either **<IP-address of your computer>\<Your SQL Server name>** or **localhost\<Your SQL Server name>** format:



4. In the **Database Name** field, enter the name of the authentication server database and click **Create New Database**.

If the creation is successful, the following message appears.

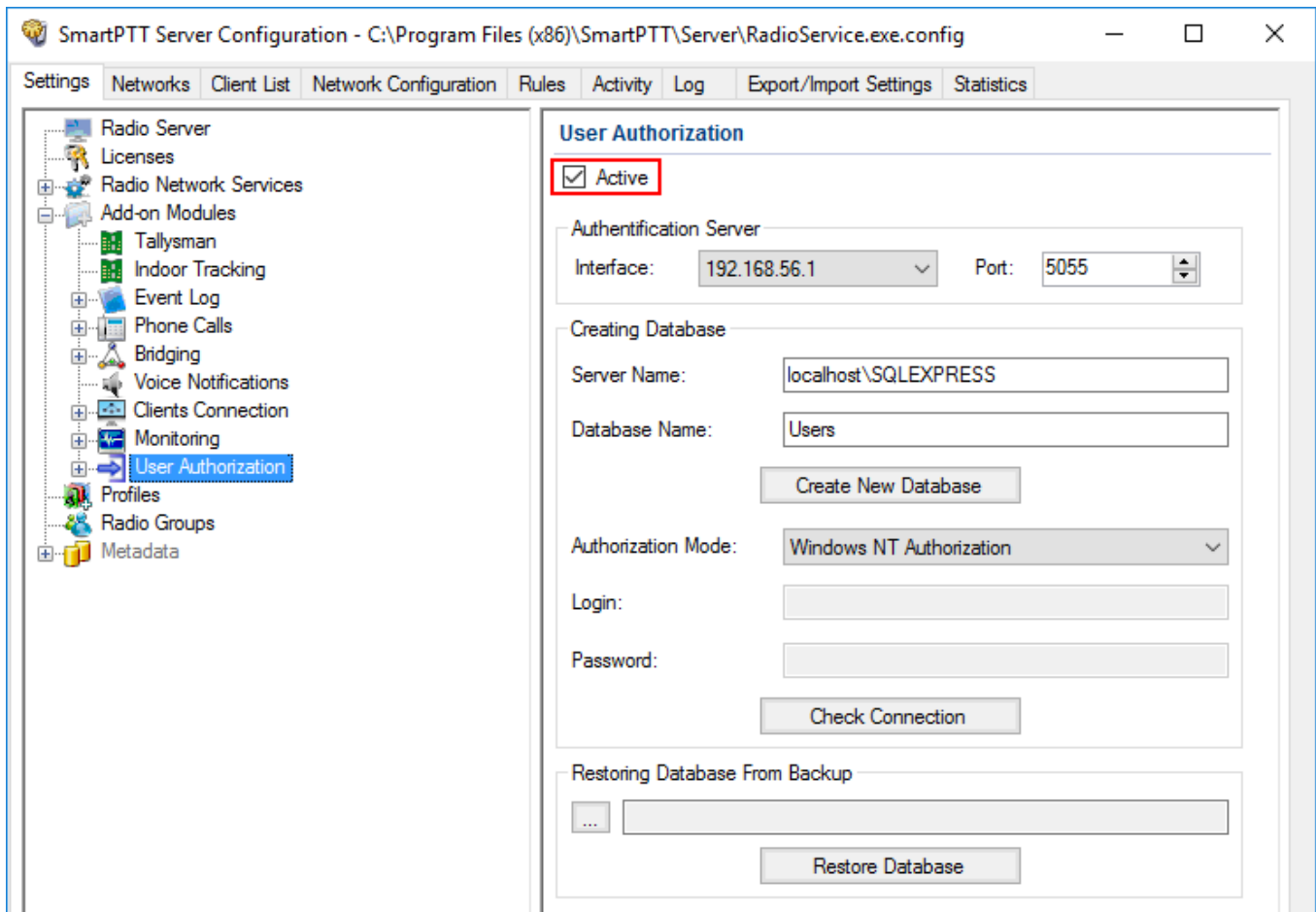


5. Click **Save**  to save changes.
6. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

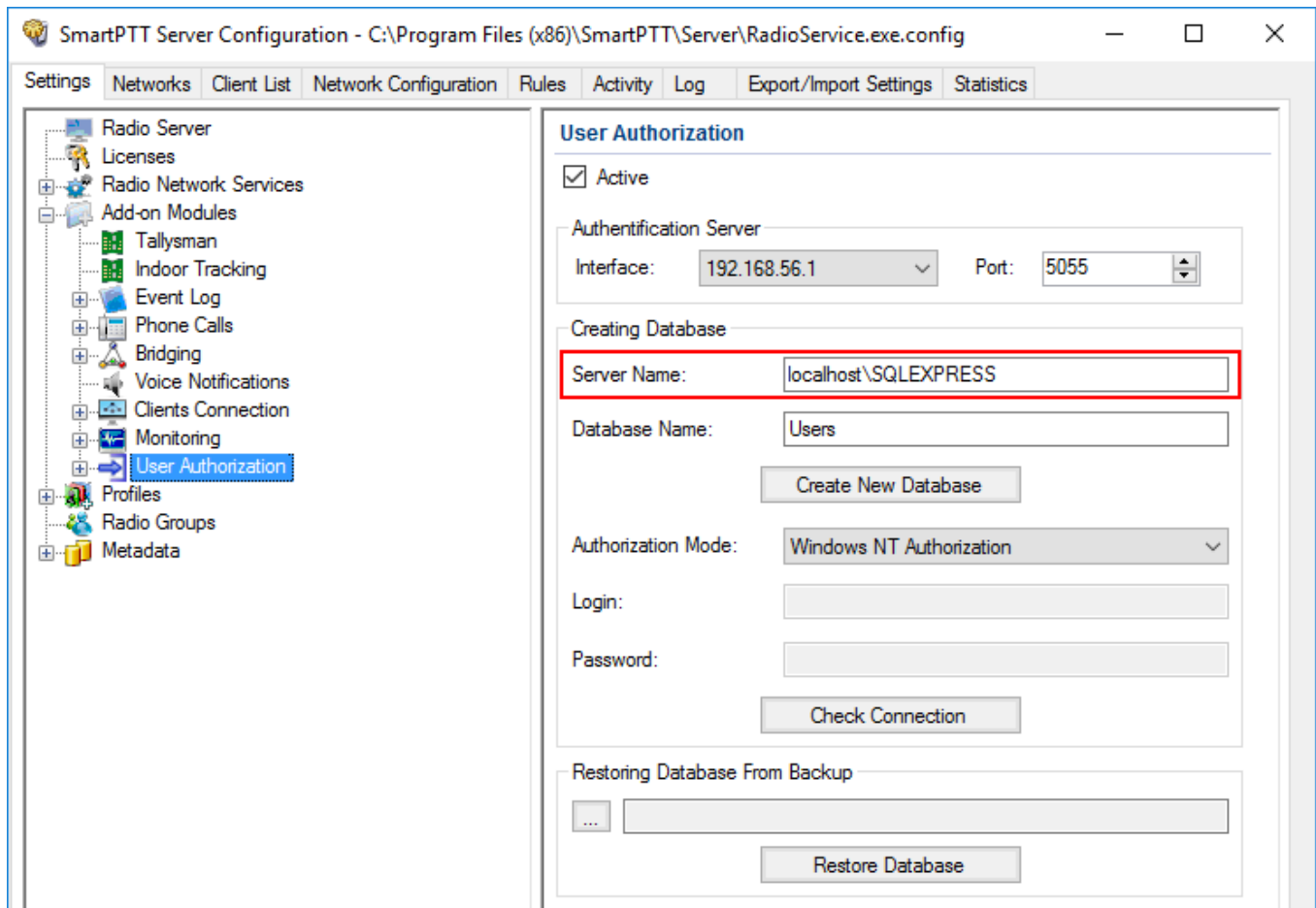
## Connecting User Authorization Database

To connect to the authentication server database, follow these steps:

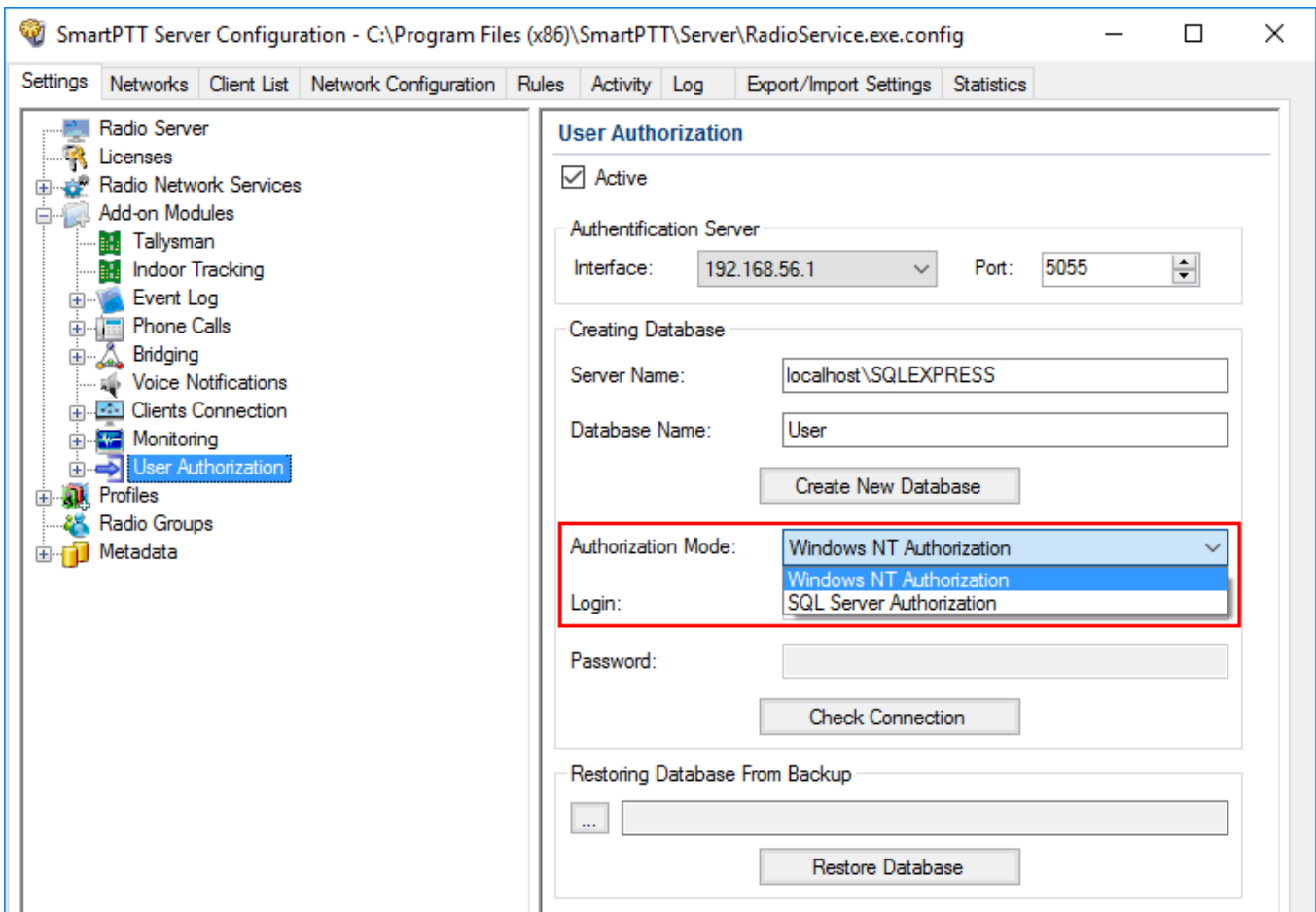
1. In the left pane of the **Settings** tab, expand the **Add-on Modules** node and click **User Authorization**.
2. In the **User Authorization** pane, select the **Active** check box.



3. In the **Server Name** field of the **Creating Database** area, enter the name of the SQL Server. You can use either **<IP-address of your computer>\<Your SQL Server name>** or **localhost\<Your SQL Server name>** format.
4. In the **Database Name** field, enter the name of the needed database.

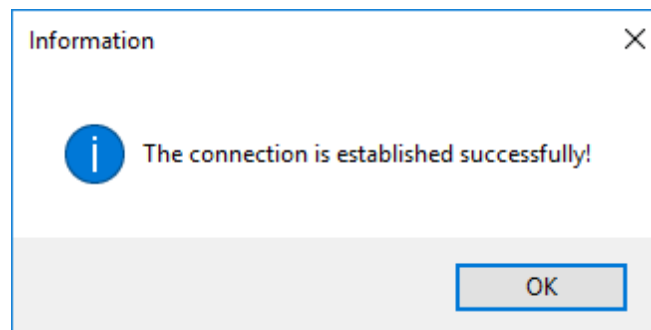




5. From the **Authorization Mode** list, select the needed authorization mode:
  - **Windows NT Authorization:** Select to use Windows account for connecting to the local SQL Server.
  - **SQL Server Authorization:** Select to use SQL Server account for connecting to the local SQL Server.



6. If **SQL Server Authorization** is selected, enter **Login** and **Password** and then click **Check Connection**.

If the connection is successful, the following message appears.



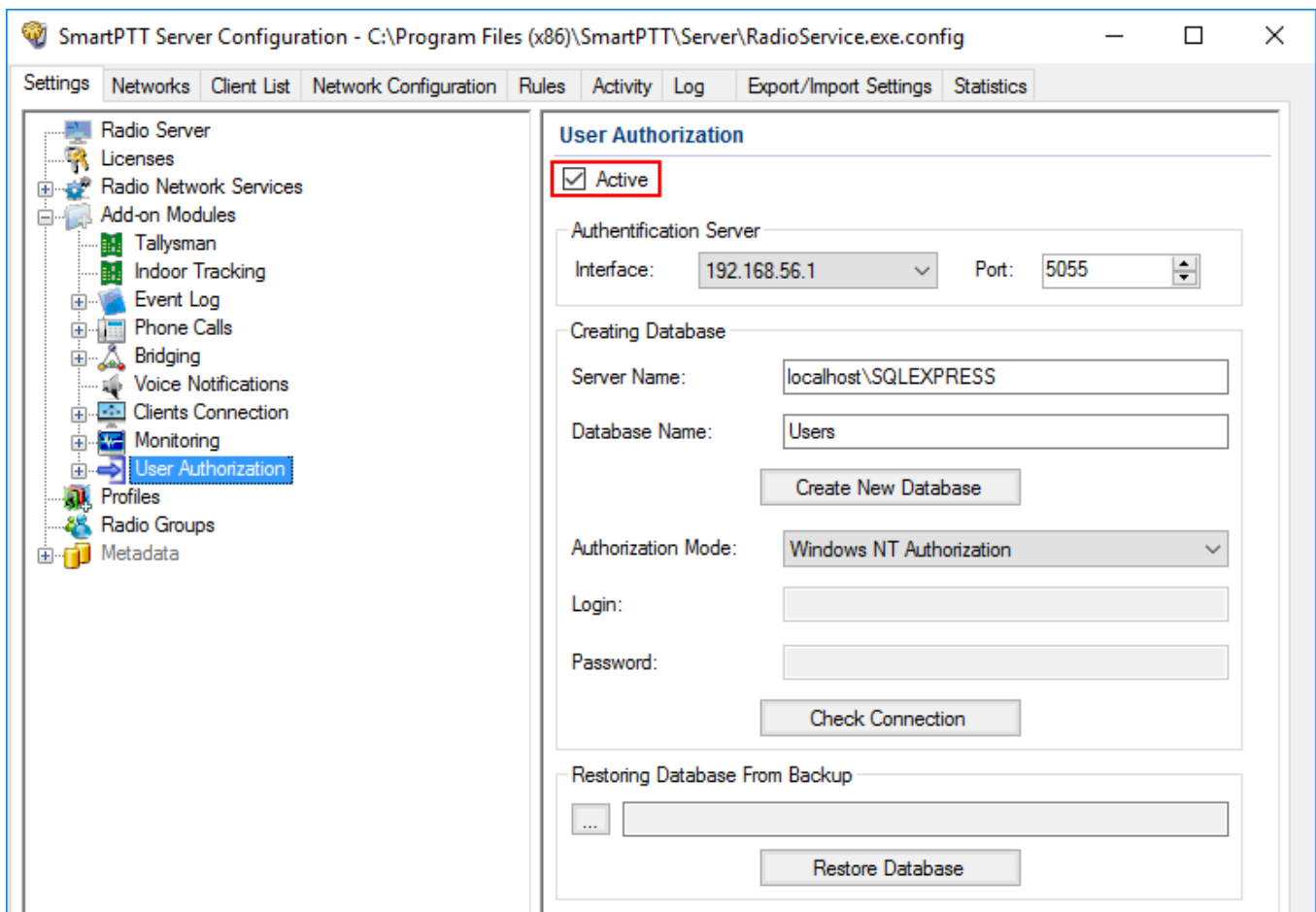
7. Click **Save**  to save changes.
8. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.



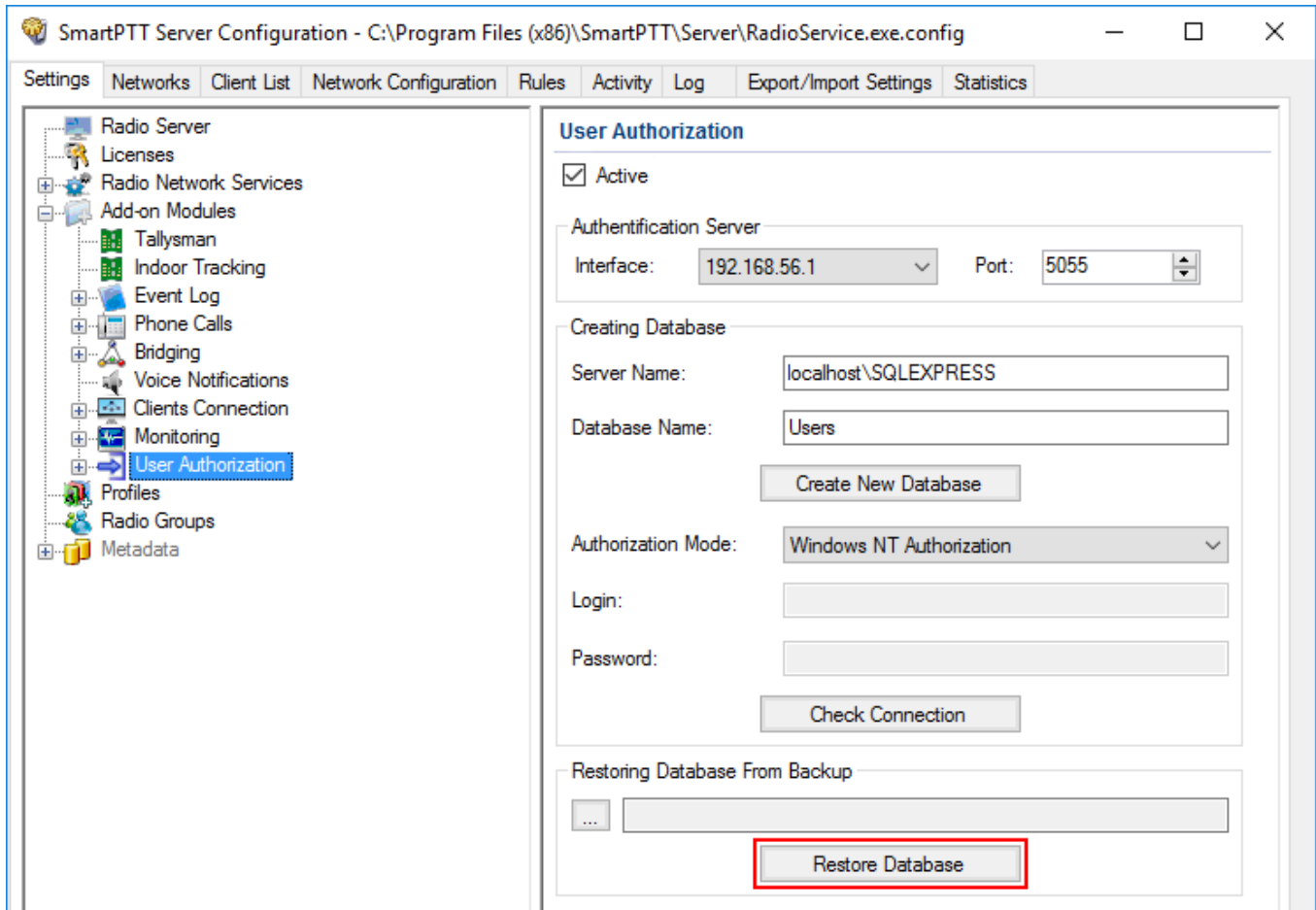
## Restoring Database from Backup

To restore database from backup, follow these steps:

1. In the left pane of the **Settings** tab, expand the **Add-on Modules** node and click **User Authorization**.
2. In the **User Authorization** pane, select the **Active** check box.



3. In the **Restoring Database Backup** area of the **User Authorization** pane, select the required database backup file and click **Restore Database**.

**NOTE**

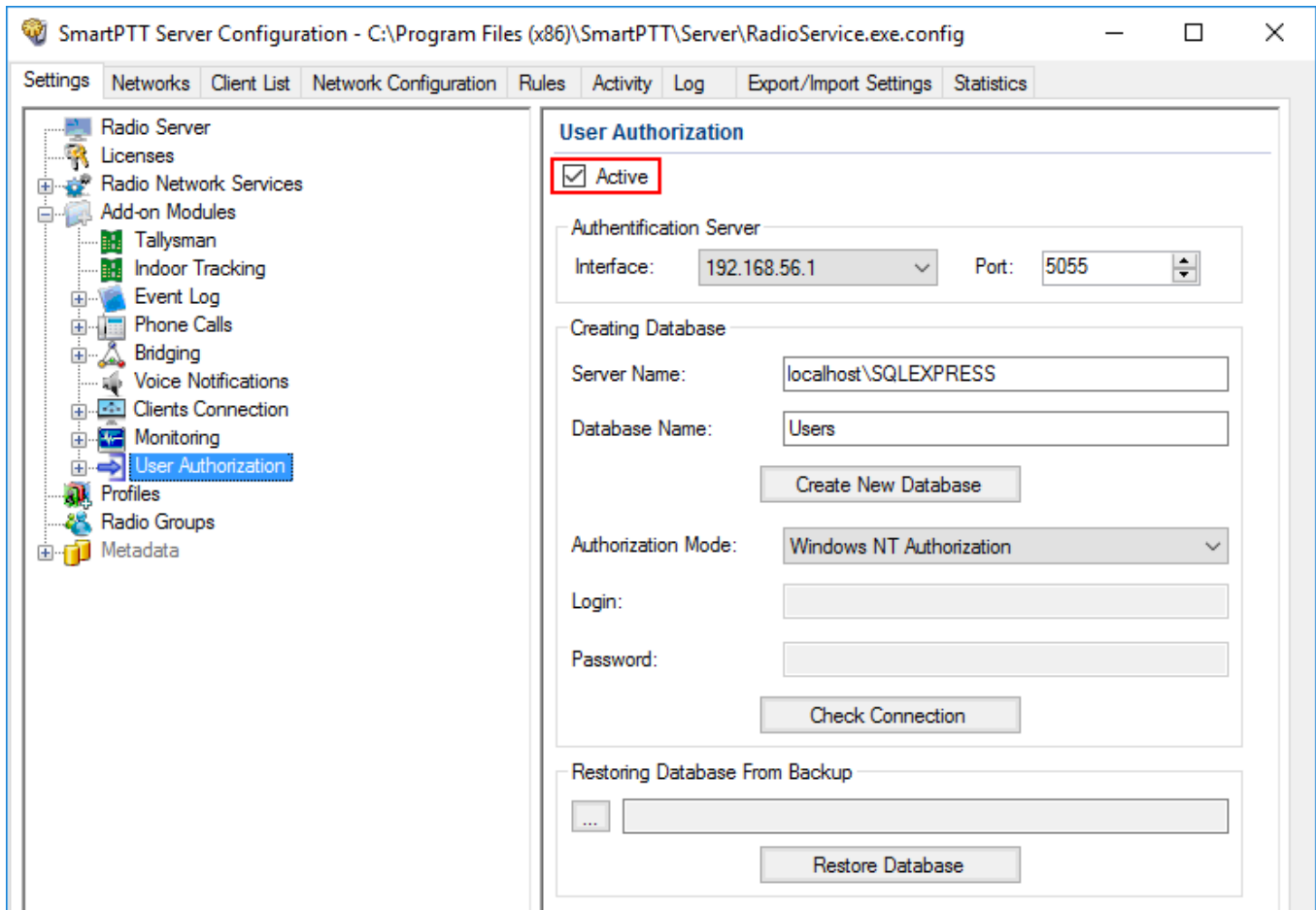
To set up the auto backup of the database, please refer to [Automatic Database Backup](#).

**Connecting User Authorization Database**

To connect to the authentication server, follow these steps:

1. In the left pane of the **Settings** tab, expand the **Add-on Modules** node and click **User Authorization**.

- In the **User Authorization** pane, select the **Active** check box.



- In the **Interface** field of the **Authentication Server** area, enter the IP-address of the SmartPTT Radioserver.

#### NOTE

By default the authentication server has the IP-address of the primary radioserver.

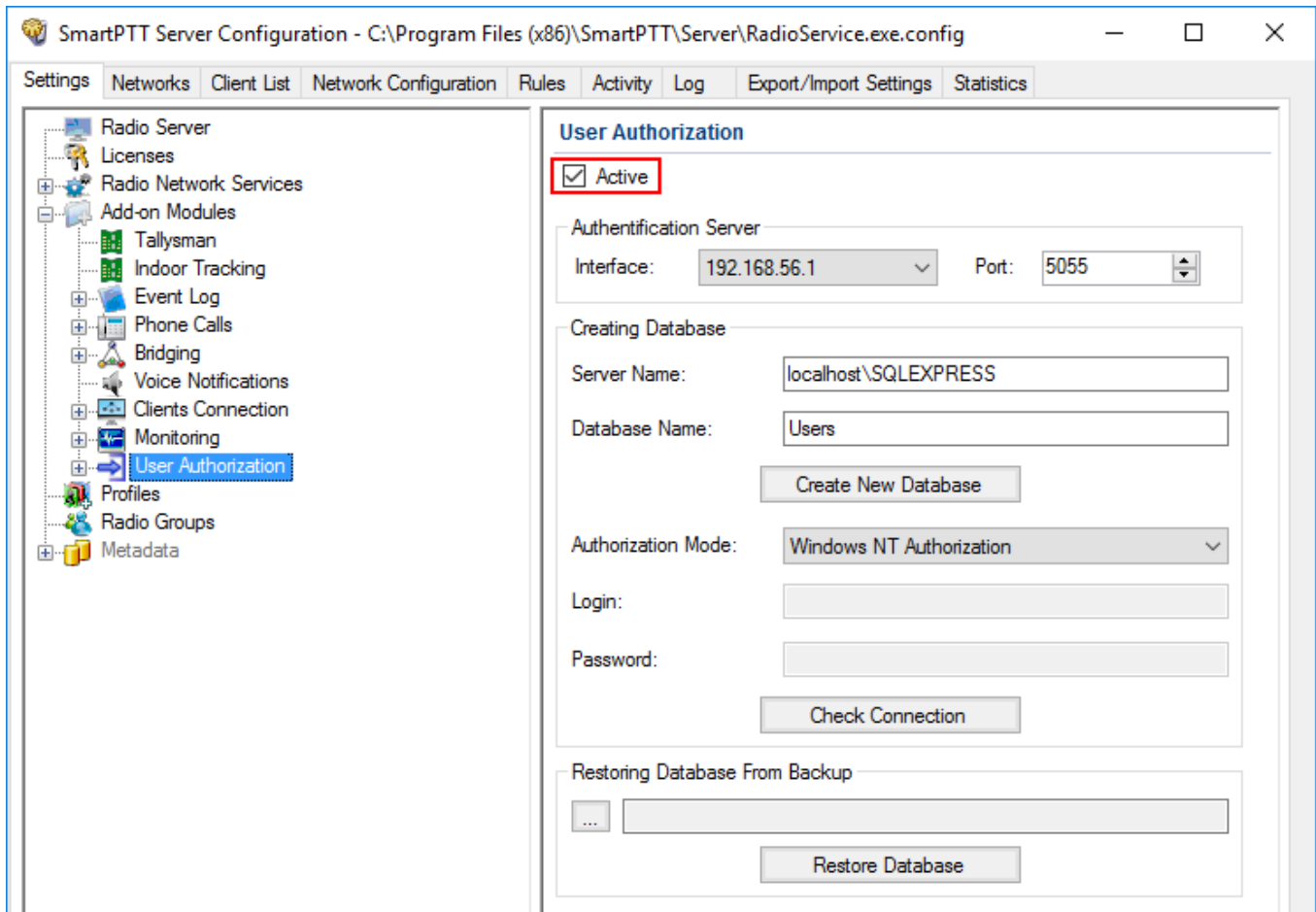
- In the **Port** field, enter the port number.



## Activating User Authorization

To activate the user authorization, follow these steps:

- In the left pane of the **Settings** tab, expand the **Add-on Modules** node and click **User Authorization**.

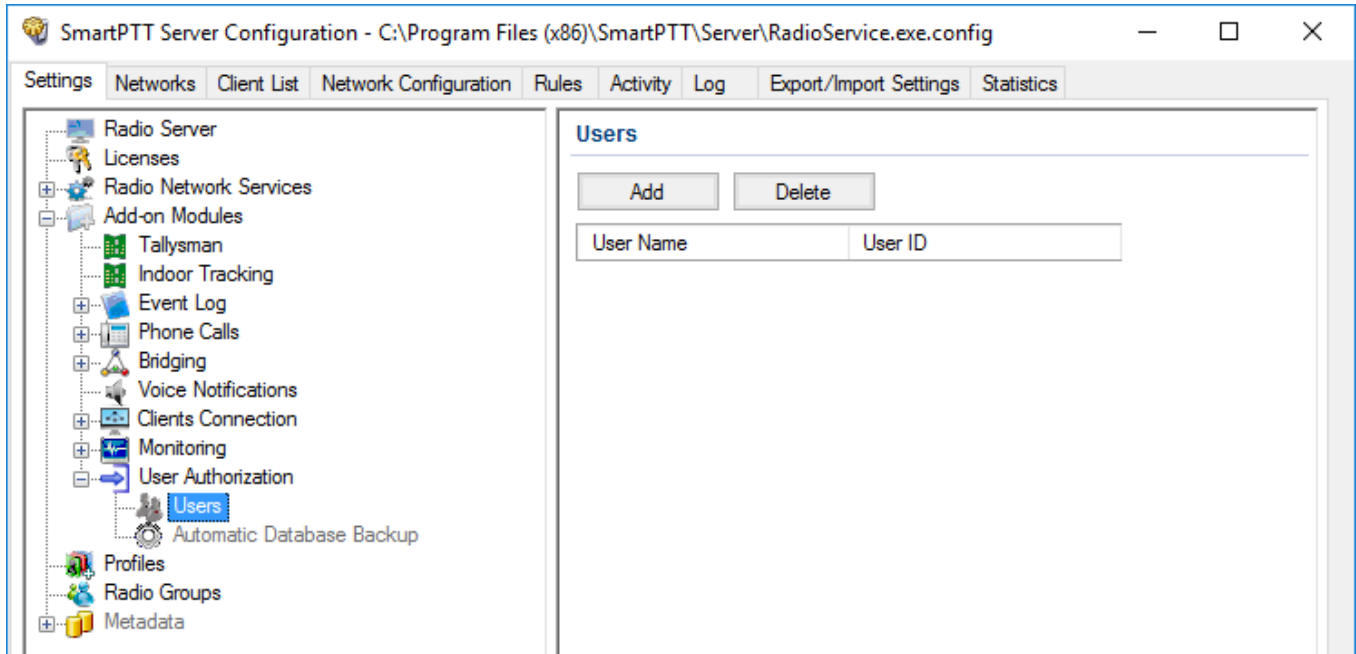
2. In the **User Authorization** pane, select the **Active** check box.



3. Click **Save**  to save changes.
4. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

## 1.5.9.1 Users

In *SmartPTT Radioserver Configurator* you can create a list of users. This list contains the names of the users with corresponding unique identifiers. When the radio user enters the unique identifier on the radio, the corresponding name becomes visible in *SmartPTT Dispatcher*.



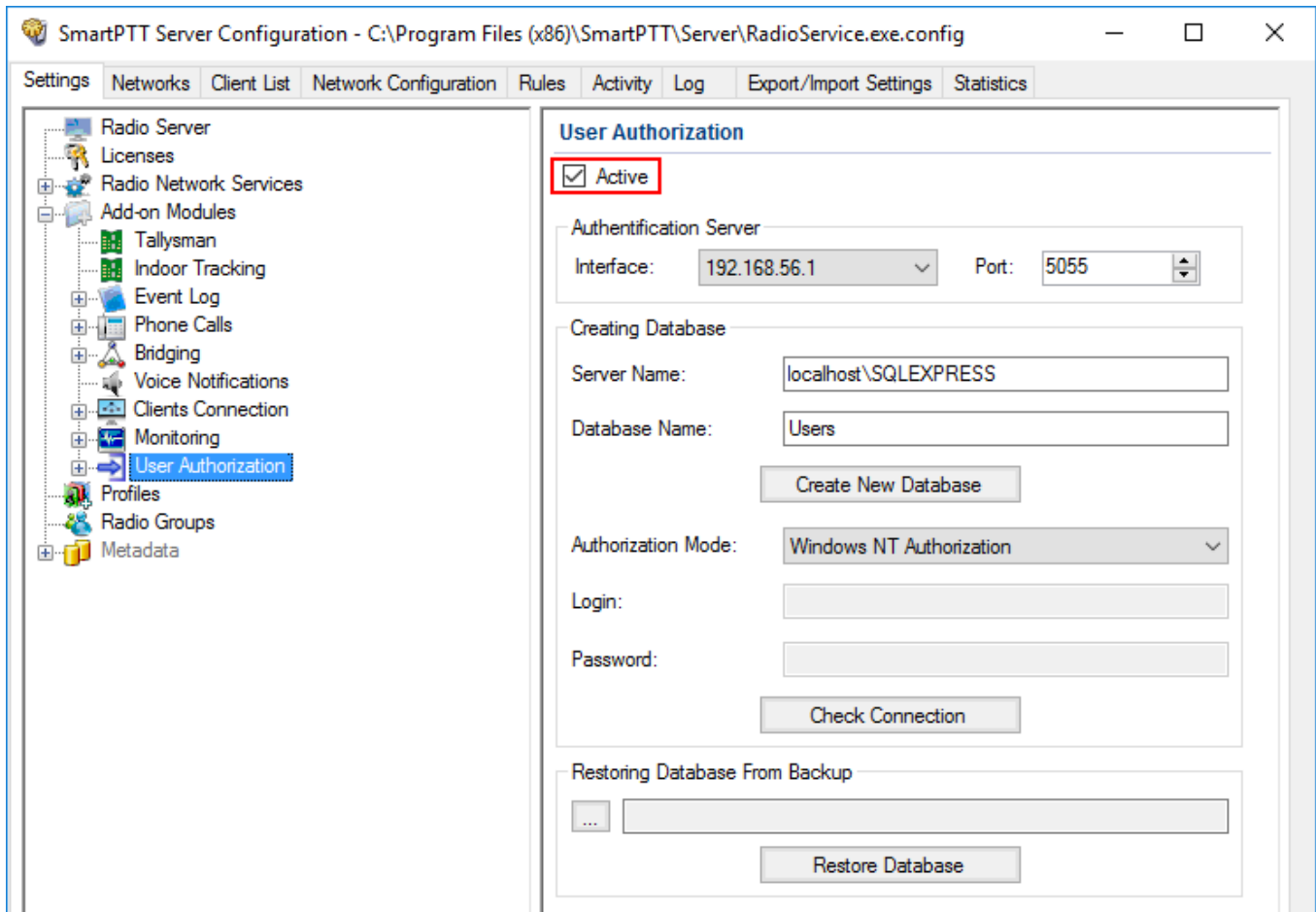
Configuration of the list of users includes:

### Adding users to the list

To add a user to the list, follow these steps:

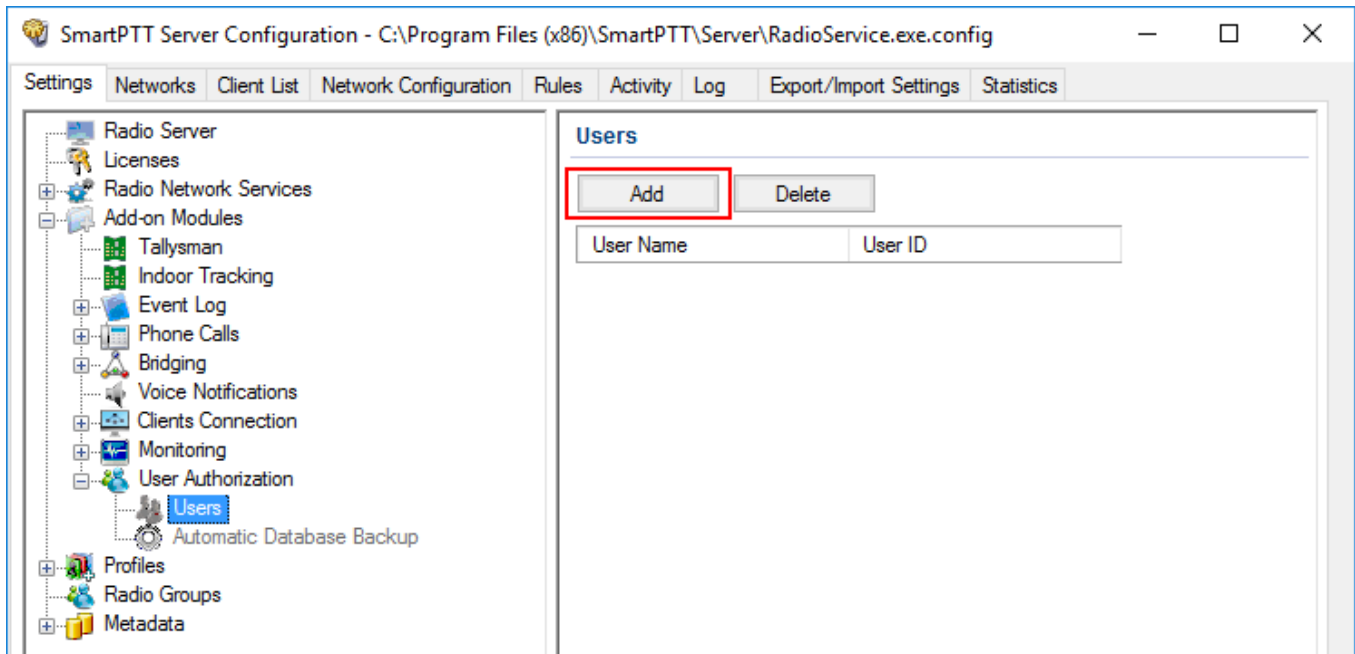
1. In the left pane of the **Settings** tab, expand the **Add-on Modules** node and click **User Authorization**.

2. In the **User Authorization** pane, select the **Active** check box.

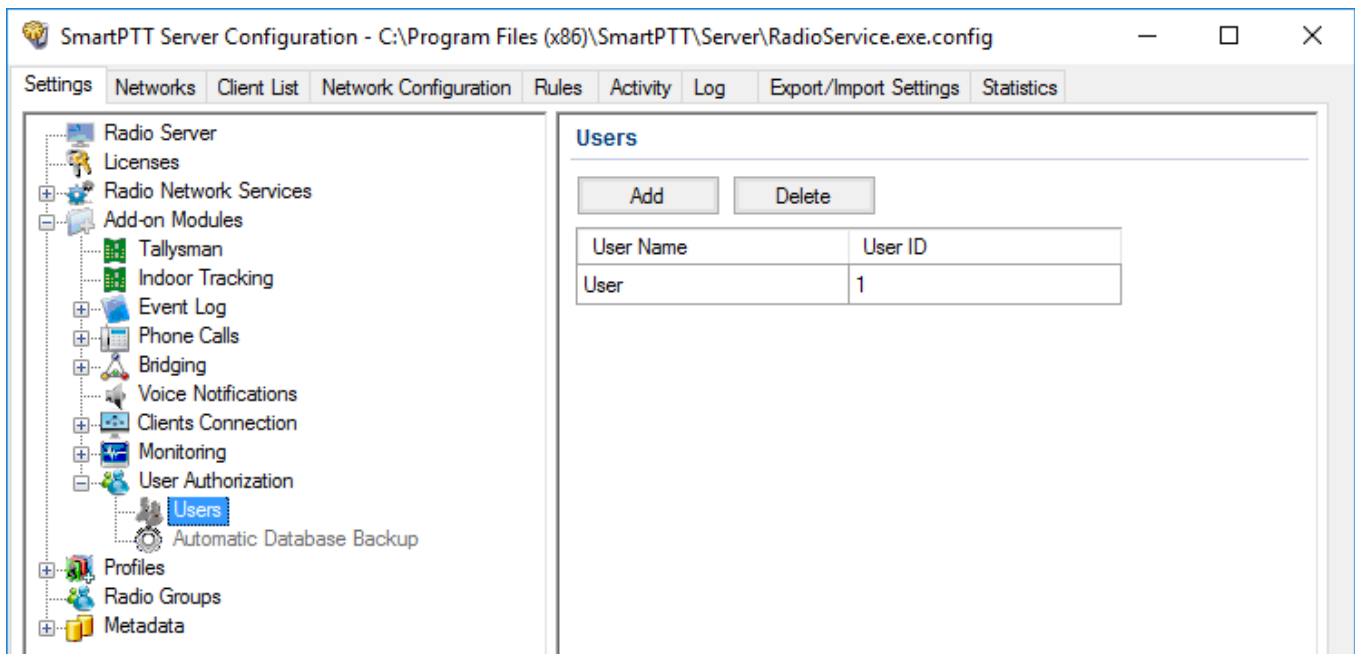


3. In the left pane of the **Setting** tab, expand the **User Authorization** node and click **Users**.

- In the **Users** pane, click **Add**.





- In the **Name** field, enter the name of a user.
- In the **ID** field, enter the radio ID.



- Add more users if needed.

#### NOTE

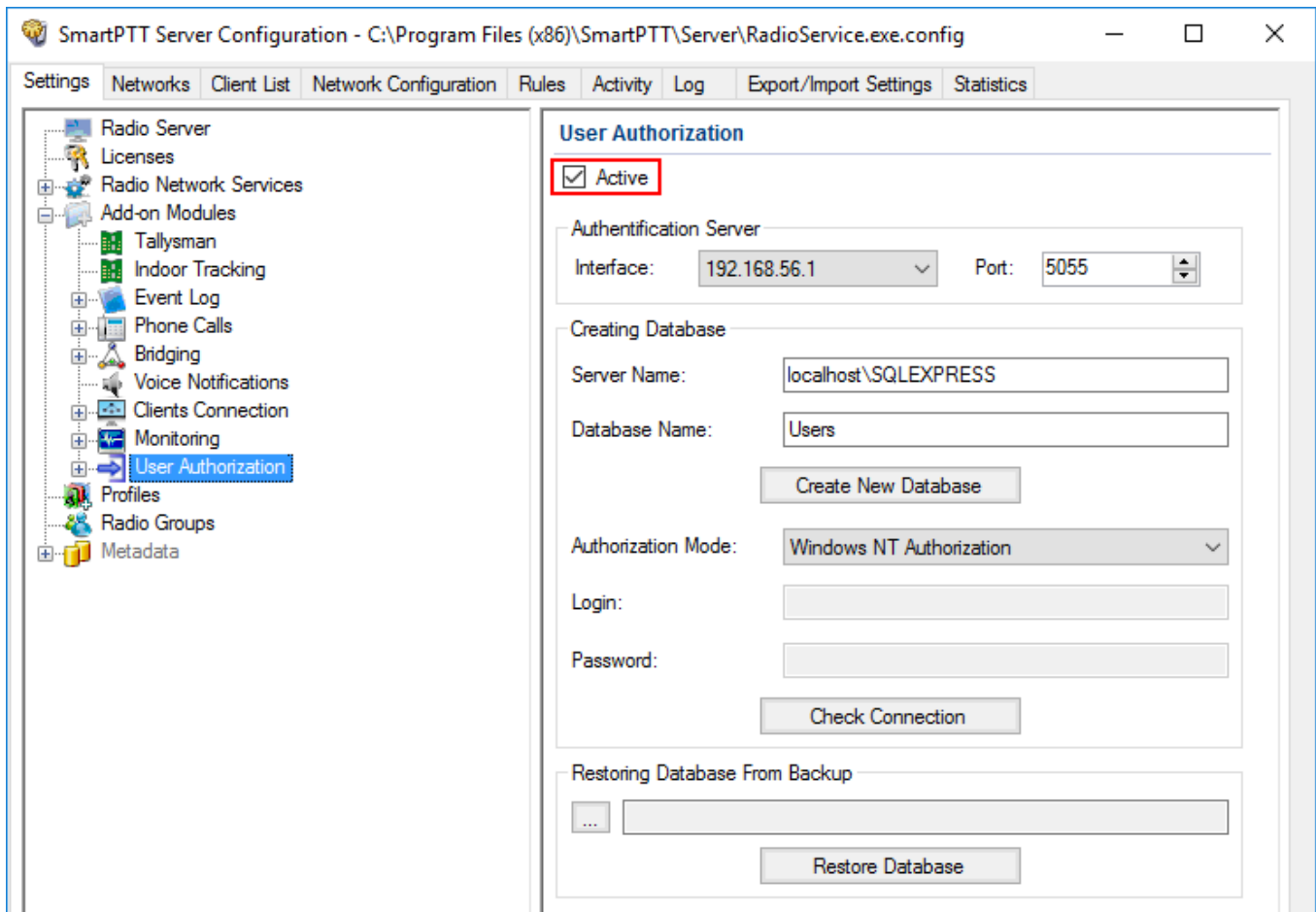
User names cannot be the same.

8. Click **Save**  to save changes.
9. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

## Removing users from the list

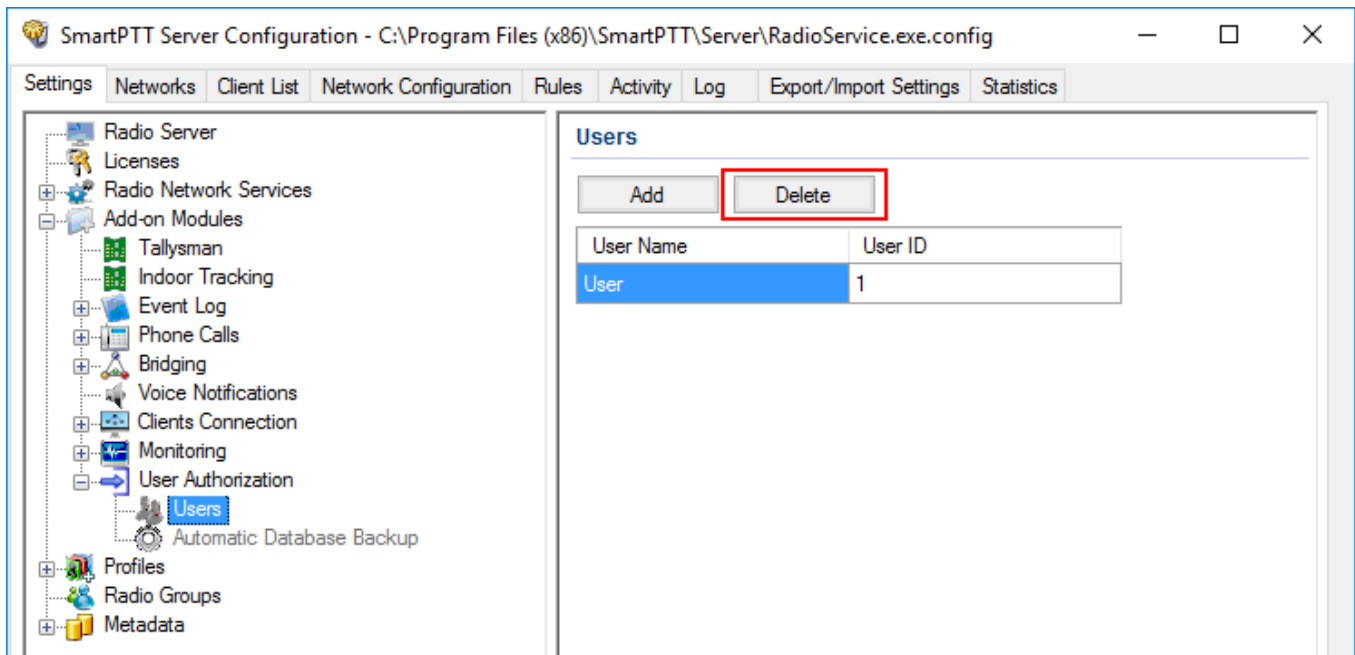
To remove a user from the list, follow these steps:

1. In the left pane of the **Settings** tab, expand the **Add-on Modules** node and click **User Authorization**.
2. In the **User Authorization** pane, select the **Active** check box.



3. In the left pane of the **Setting** tab, expand the **User Authorization** node and click **Users**.
4. In the **Users** window click the name of the user you want to delete and then click **Delete**.





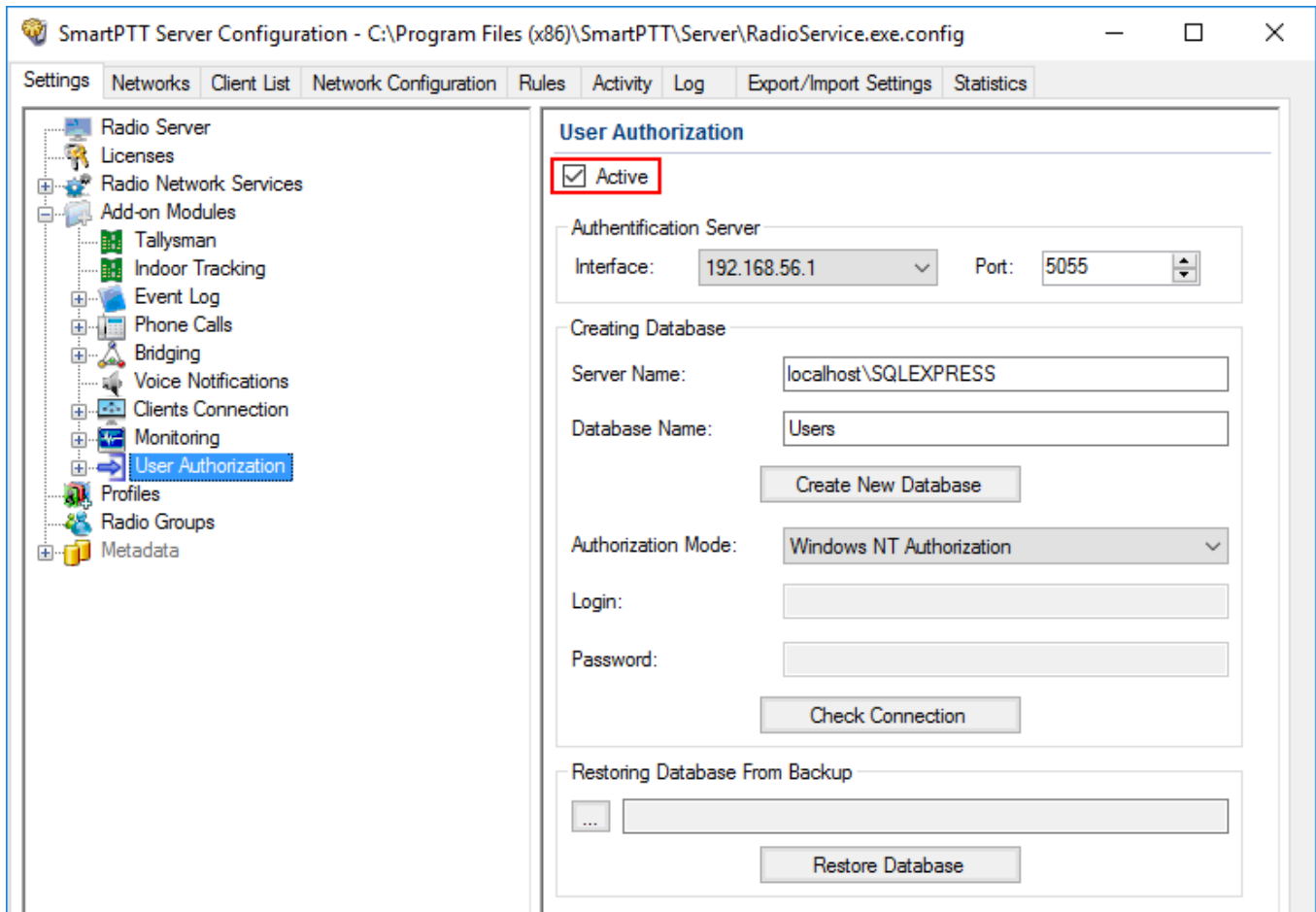
### 1.5.9.2 Automatic Database Backup

Backing up data on a regular basis helps to protect it from being erased in case of the server hardware or software failure. *SmartPTT Radioserver Configurator* allows to back up the authentication server database automatically.

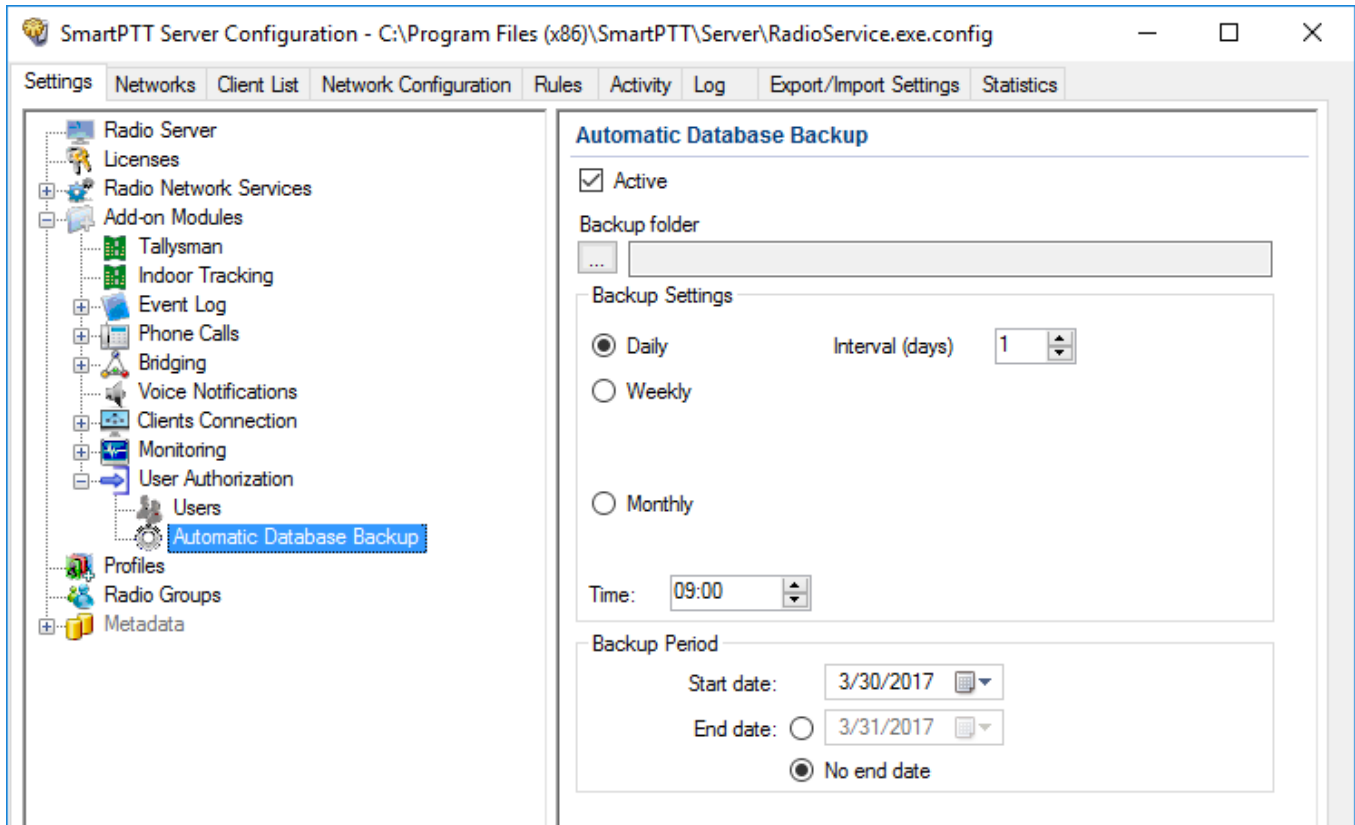
To set up automatic backup schedule of the authentication server, follow these steps:

1. In the left pane of the **Settings** tab, expand the **Add-on Modules** node and click **User Authorization**.

2. In the **User Authorization** pane, select the **Active** check box



- In the left pane of the **Setting** tab, expand the **User Authorization** node and click **Automatic Database Backup**.



- In the **Automatic Database Backup** pane, select the **Active** check box. The database backup becomes active in the automatic mode.
- In **Backup folder** enter the path to the file for saving the database backup.
- In the **Backup settings** area of the **Automatic Database Backup** pane, configure the following parameters:



**Daily:** Every fixed day at the specified time (for example, every day, every third day).

**Interval (days):** Set the interval for the database backup.

**Weekly:** Every fixed day of the week at the specified time (for example, every Monday and/or Wednesday).

**Monthly:** Once a month on the fixed day of the selected month and at the specified time.

**Time:** Set the time for the automatic database backup. This setting is common for all the intervals.

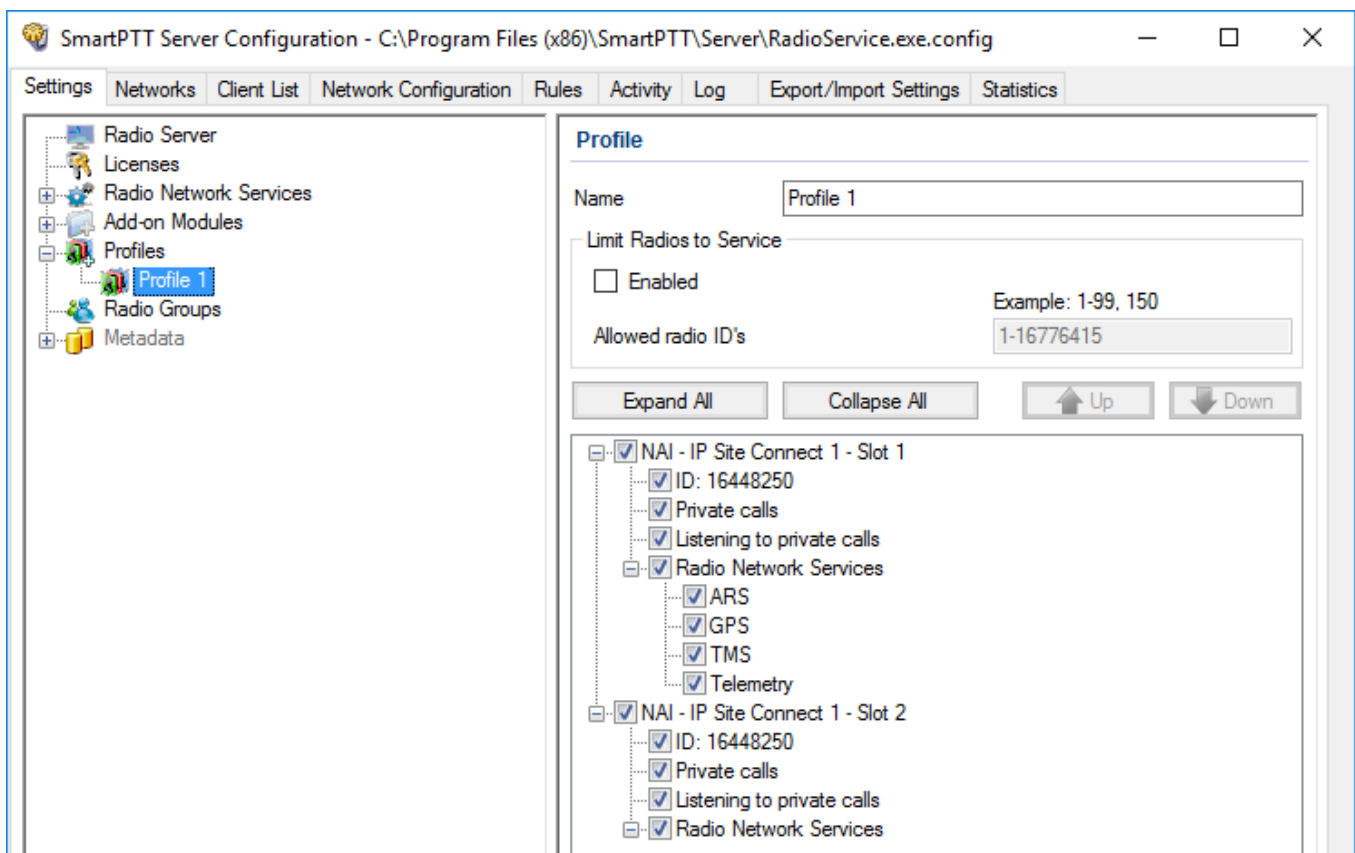
7. In the **Backup Period** area, set the time period when automatic database backup is to be made according to the selected backup settings. It can be either a restricted period of time or a period of time without end date.
8. Click **Save**  to save changes.
9. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

## 1.6 Profiles

*SmartPTT Radioserver Configurator* allows creating permission profiles. The permission profiles are used to limit the operator's access to objects managed by SmartPTT Radioserver (control stations, talkgroups, services, IP Site Connect slots), and to provide additional opportunities in the organization of calls between dispatchers and radios.

To create a profile right-click **Profiles** in the setting tree of *SmartPTT Radioserver Configurator* and click **Add**.

The following window appears:



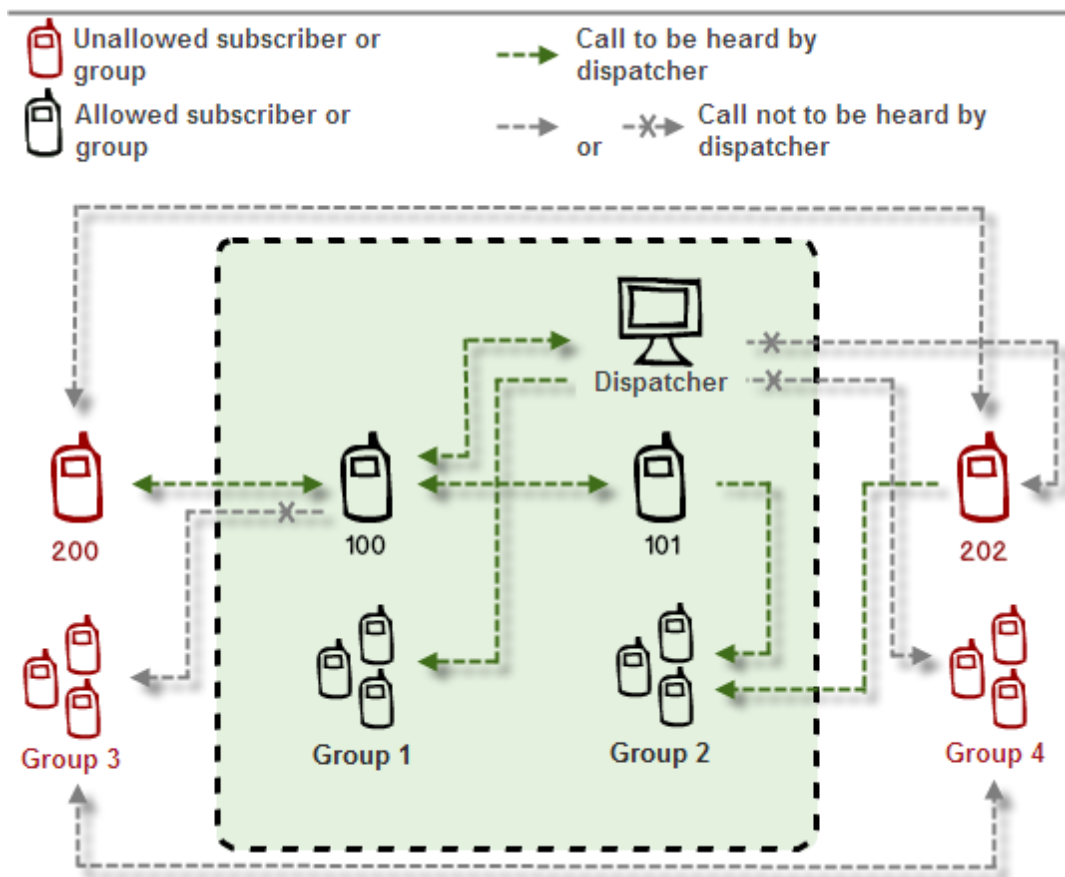
**Name:** The profile name.

The **Limit Radios to Service** area was designed to manage the number of radios allowed for this profile. Here you can specify which radios are to be controlled by the profile and which are not.

To make this functionality active select **Enabled**. Then, in the **Allowed radio ID's** field, enter the ID's of the radios which are to be controlled by the profile.

**WARNING**  
Not specified radio IDs will be ignored by SmartPTT system.

The following scheme shows how it works:



This is how this scheme can be presented in the table:

Call From	Call To				
	Allowed group	Unallowed group	Allowed radio	Unallowed radio	Dispatcher

Unallowed radio	Allowed	Not allowed	Allowed	Not allowed	Not allowed
Allowed radio	Allowed	Not allowed	Allowed	Allowed	Allowed
Dispatcher	Allowed	Not allowed	Allowed	Not allowed	Allowed

**NOTE**

When adding allowed radios make sure that the same radios are specified in **Radioserver** → [Limit Radios to Service](#). Otherwise, the radios not registered in both lists will be regarded as unallowed.

Upwards and downwards arrows are used for changing the order of head elements in the list. This order will be applied in *SmartPTT Dispatcher*, if this profile is used.

In the central list you can select all the elements which are to be controlled by the operator with this profile. If there are more than one operator on the same channel, set the unique **ID** for each operator. This will allow radios to make private calls to particular operators, dialing the specified ID.

**NOTE**

Operator can be assigned to the particular gateway of the network via ID. Therefore, it can be available to a fewer amount of talkgroups and radios.

To assign the ID to the profile in particular network:

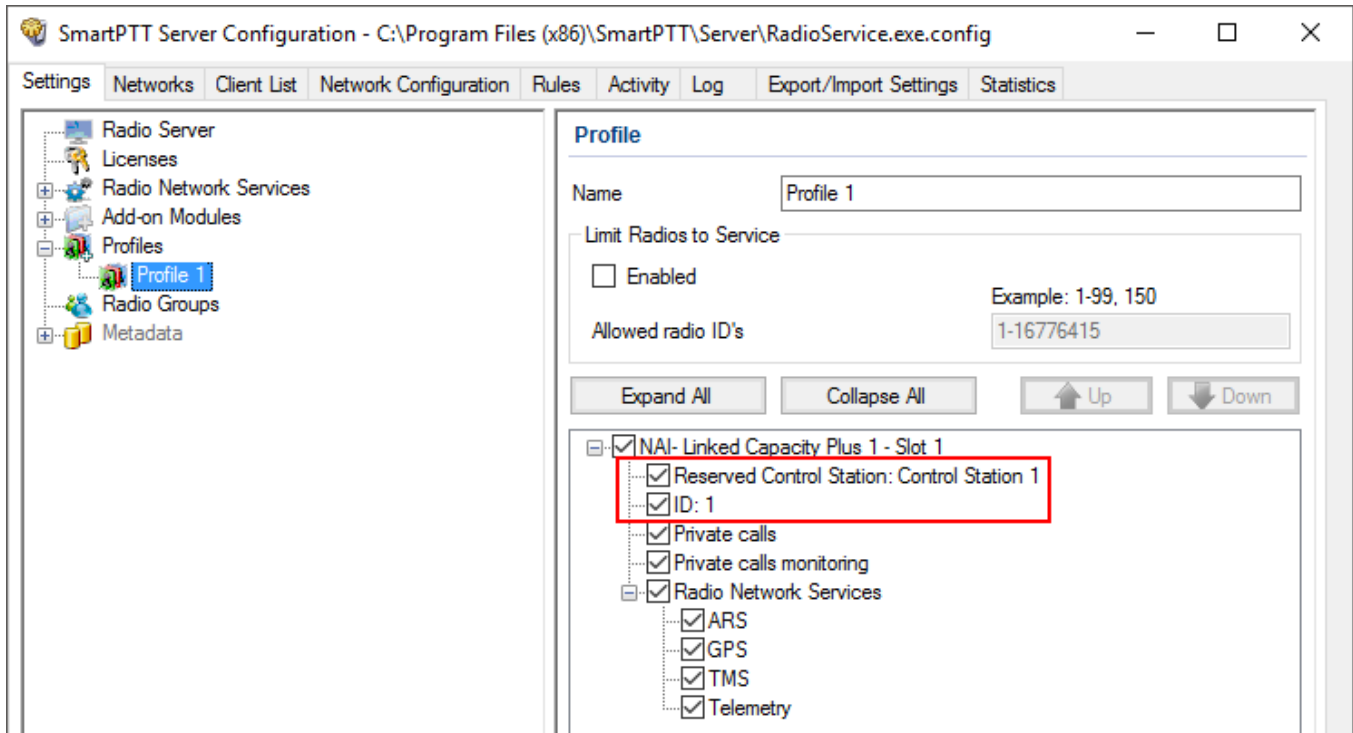
1. Select the **ID** check box in particular network.
2. Double-click ID to edit it.
3. Enter the proper ID for the network.

**NOTE**

If ID is unselected, **Network ID** will be used to identify the operator. In addition, it will be assigned to the gateway, for which default radio ID is assigned. For more information see the configuration settings of DDMS or VRC gateways in you networks.

If several dispatchers have the same ID, they will hear each other's private calls, even if **Private calls** check box is not selected.

In Capacity Plus and Linked Capacity Plus configurations based on NAI protocol, when using control stations reserved for dispatcher private calls, a new parameter **Reserved Control Station** appears and the ID value matches the reserved control station ID automatically:



**Private calls:** If enabled, it allows the dispatcher to initiate private calls to radio and telephone subscribers, and dispatchers.

**Private calls monitoring:** If enabled, it allows the dispatcher to hear private calls made from radios to other radios, dispatchers or telephone subscribers and vice versa, read their messages. This feature is available for networks with direct connection to repeater, e.g., IP Site Connect, Capacity Plus.

To allow the dispatcher to make an All Call or a group call, select the corresponding check box. If a group is selected, the dispatcher will hear all the calls made to this group.

To allow the dispatcher to use services like ARS, GPS, TMS, telemetry, select the corresponding check boxes under **Radio Network Services**.

Save changes and restart the server to apply the new profile.

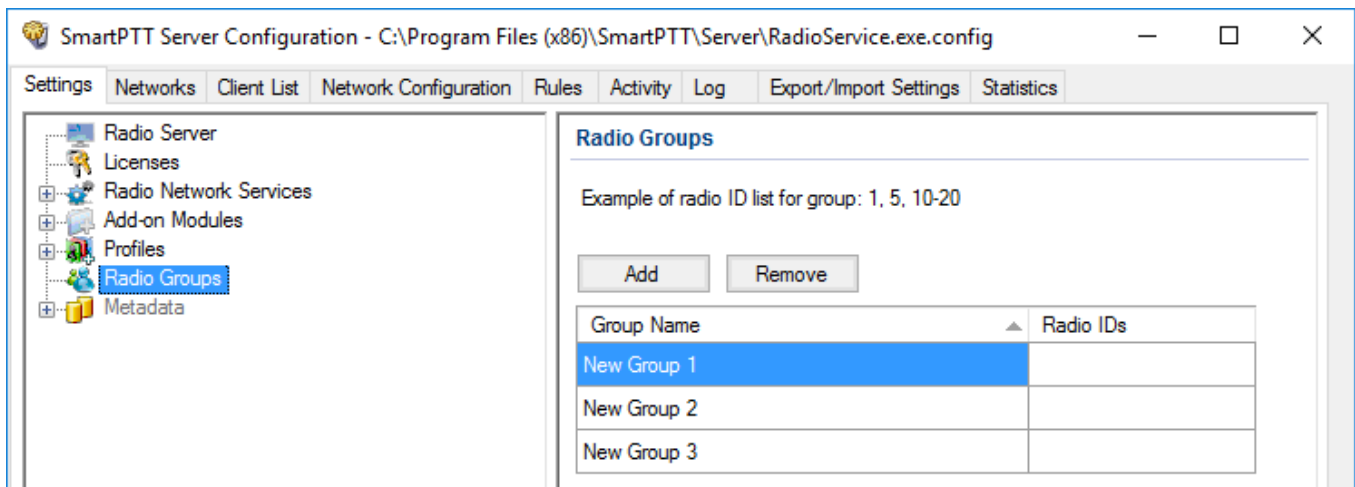
#### NOTE

To assign the created profile, open the dispatch console, **Settings** → **Radioservers**.

## 1.7 Radio Groups

Radio groups (do not confuse with talkgroups) are used to perform various tasks:

- Organization of a dynamic bridging of private calls (this feature is configured in *SmartPTT Dispatcher*)
- Telephone calls management
- Management of the intervals for receiving GPS coordinates of particular set of radios

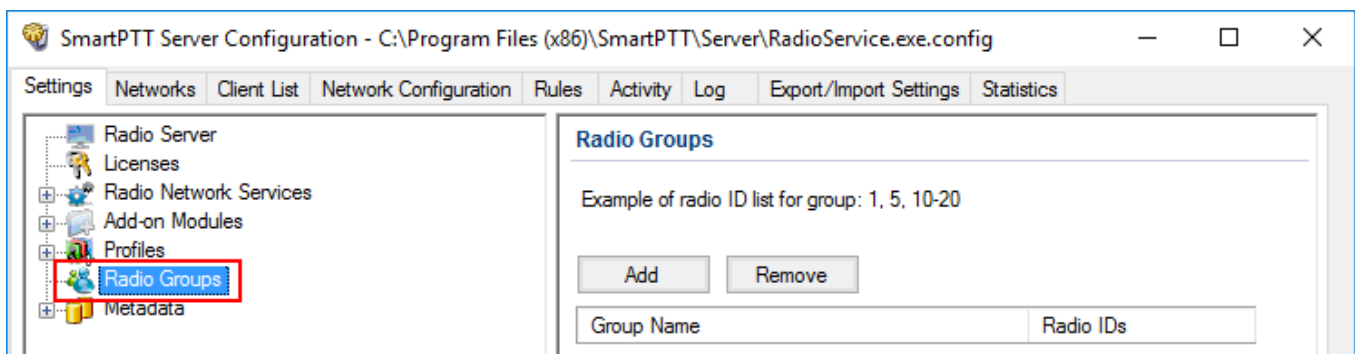


Configuration of radio groups includes:

### Adding Radio Group

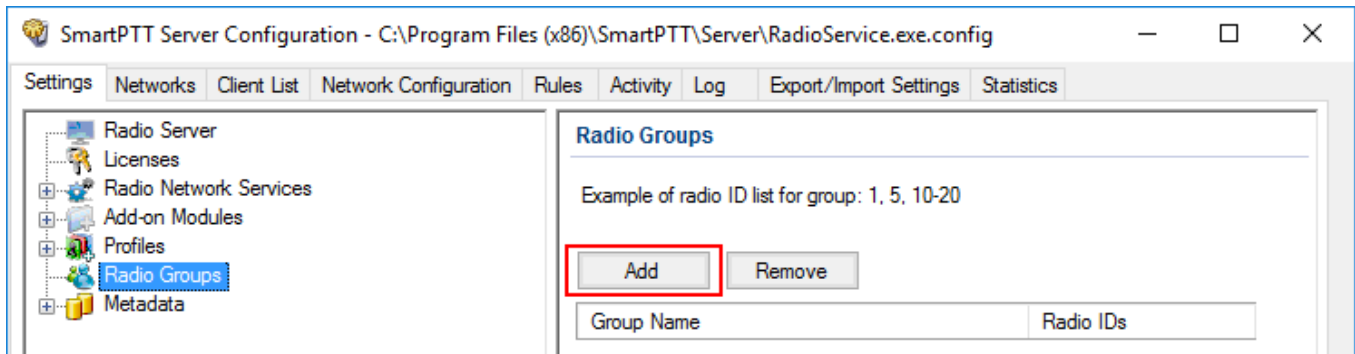
To add a radio group, follow these steps:

1. In the left pane of the **Settings** tab, click **Radio Groups**.

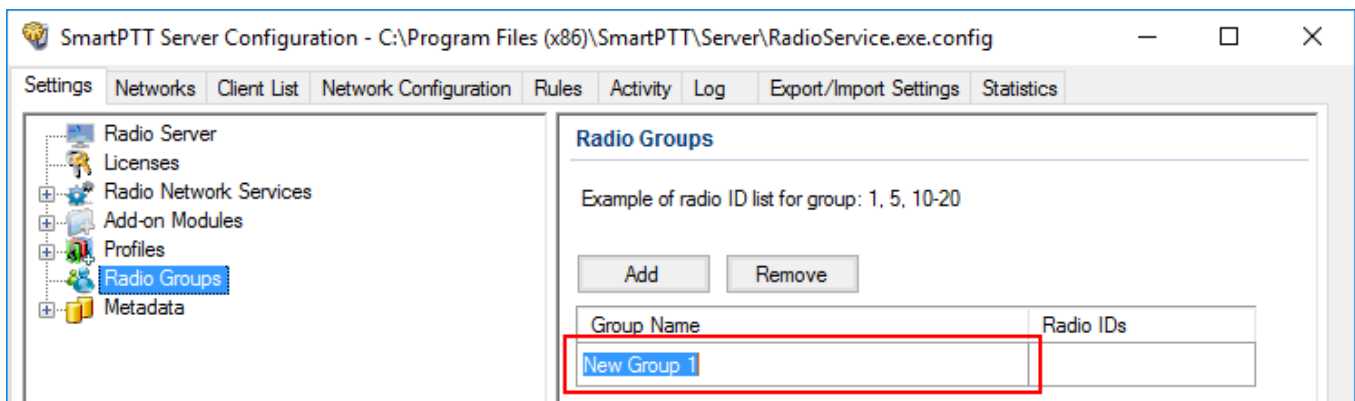




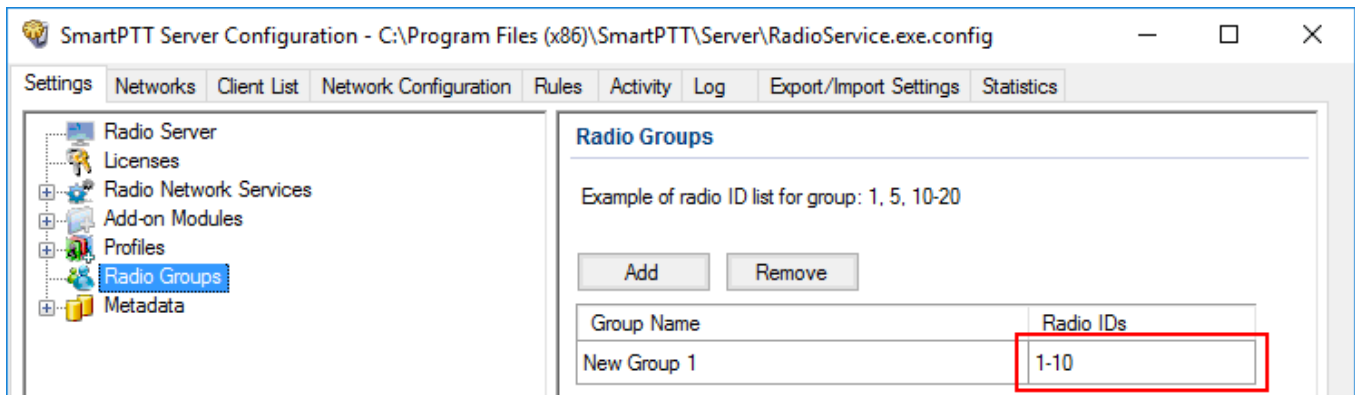
2. In the **Radio Groups** pane, click **Add**.



3. Change the name of the added group if needed.





4. Enter radio IDs which should be included to the group.



5. Add more groups if necessary.

#### NOTE

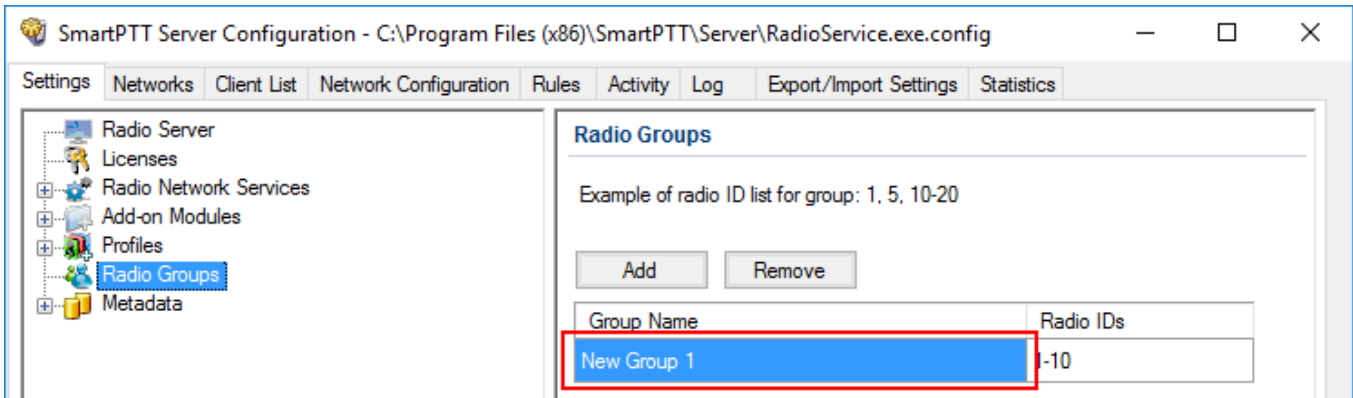
Different groups may include the same radio IDs.

6. Click **Save**  to save changes.
7. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

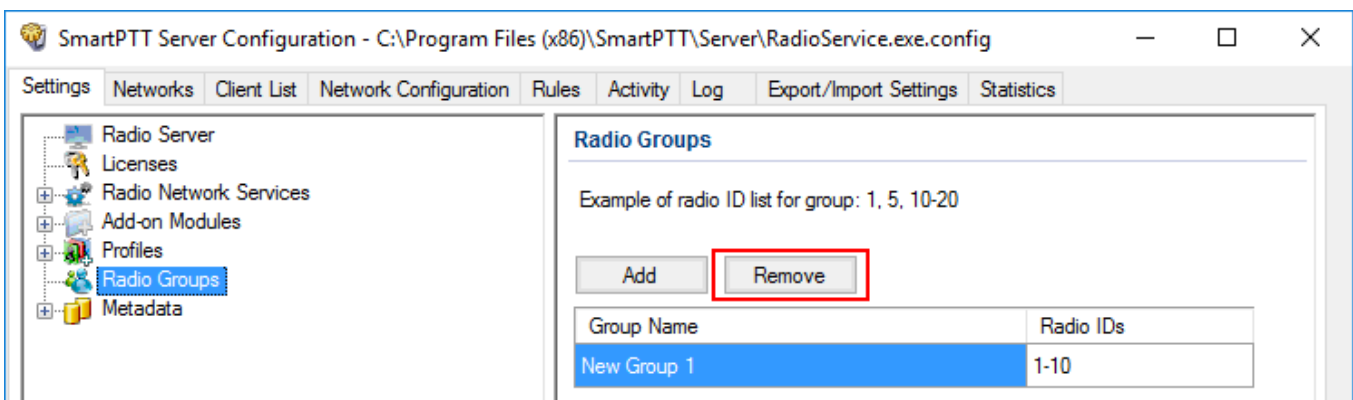
## Removing Radio Group



To remove a radio group, follow these steps:

1. In the left pane of the **Settings** tab click **Radio Groups**.
2. In the **Radio Groups** window click the name of the group that you want to remove.



3. Click **Remove**.



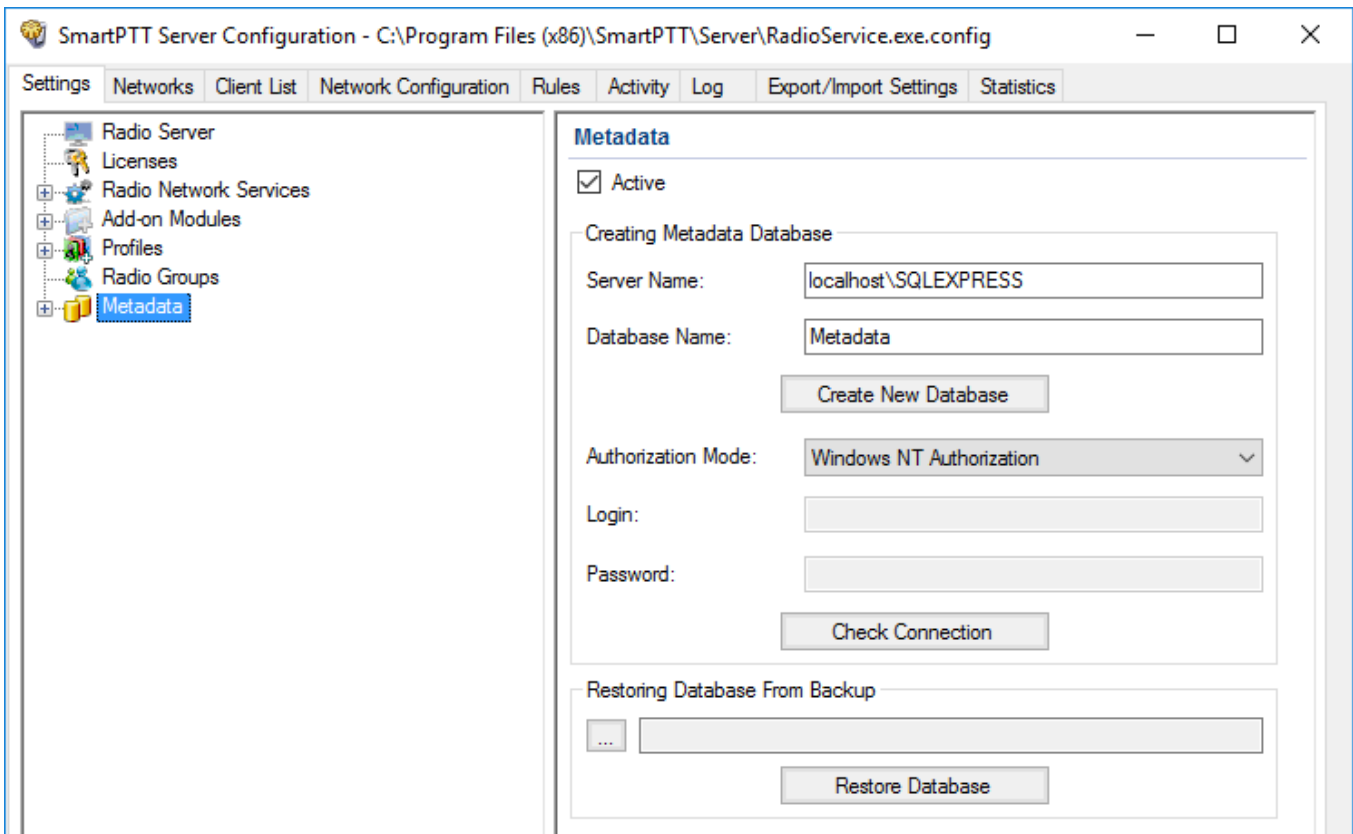
4. Click **Save**  to save changes.
5. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

## 1.8 Metadata

To provide several dispatch consoles with one consistent list of radios it was decided to keep radio metadata, e.g., radio ID, radio name, and whether it supports GPS or not. This data appears in *SmartPTT Dispatcher* automatically as soon as the radioserver is up and running. This refers only to online radios. If a radio is offline and is added to the [Radios](#) list, it won't appear in *SmartPTT Dispatcher*.

To create the database for radios metadata, follow these steps:

1. Click **Metadata** in *SmartPTT Radioserver Configurator* and click **Active**.



2. In the **Server Name** and the **Database Name** fields, enter the needed names and click **Create New Database**.

If creation is successful, a message about successful database creation is displayed. If a database is not created, the cause of failure will be displayed at the bottom of the window.

#### NOTE

For the database server installed together with the radioserver enter the name using the following format: *<Name of computer\SQLExpress>* (for example, *MYCOMP\SQLExpress*).

3. Select **Authorization Mode** between the two:
  - **SQL Server Authorization:** You must have the login name and password of the account with SQL server access.
  - **Windows NT Authorization:** The user who has logged into the Windows system, must be listed in the SQL server's list of users to make connection.
4. Click **Check Connection**.

If authorization is successful, the message "The connection is established successfully!" appears. If authorization fails, the cause will be displayed at the bottom of the window.

To restore the database from the backup folder, select the required database backup file in **Restoring Database Backup** and click **Restore Database**.

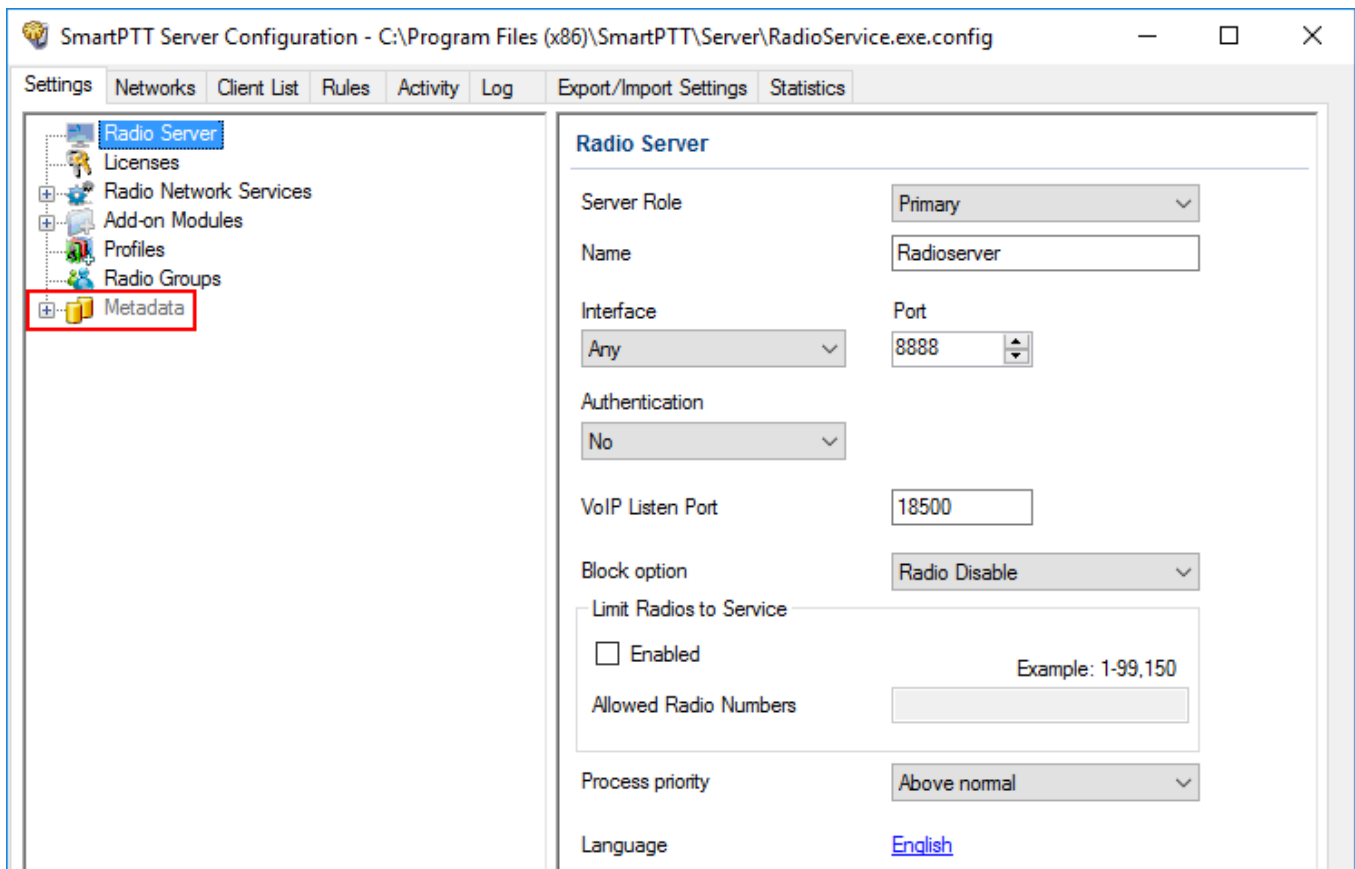
**NOTE**

To set up the auto backup of the database, go to the [Automatic Database Backup](#) window.

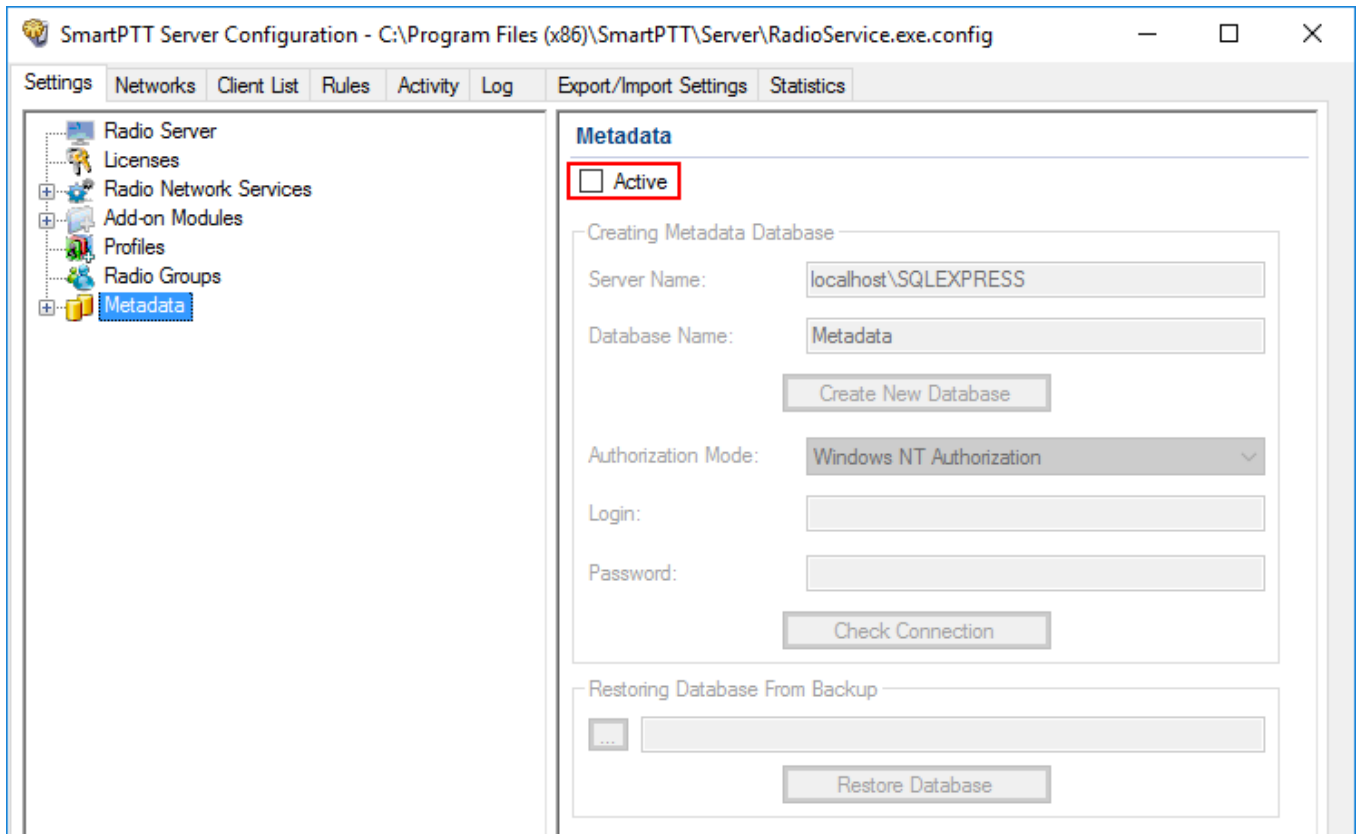
## Creating Database

To create metadata database, follow these steps:

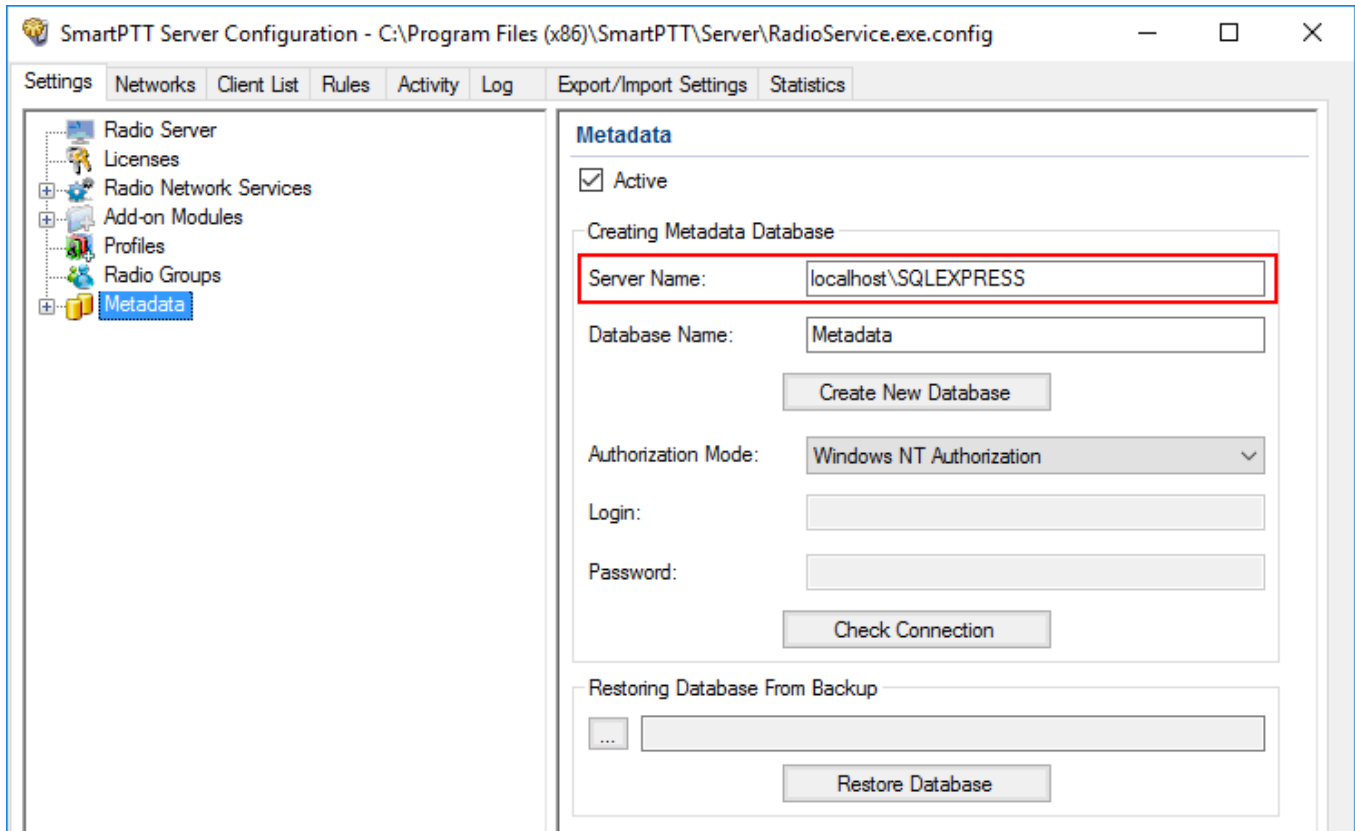
1. In the left pane of the **Settings** tab, click **Metadata**.



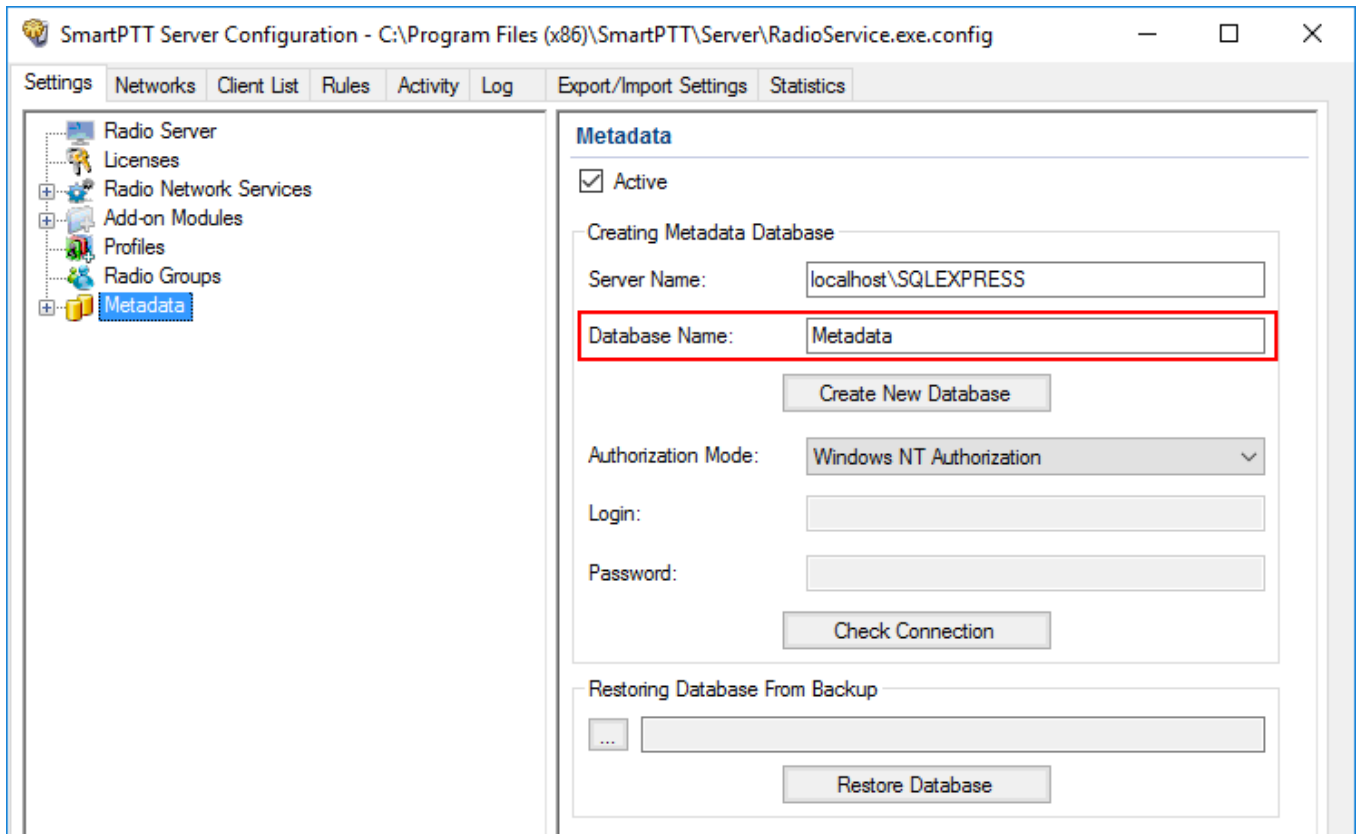
2. Make sure that the **Active** check box is selected in the **Metadata** pane.



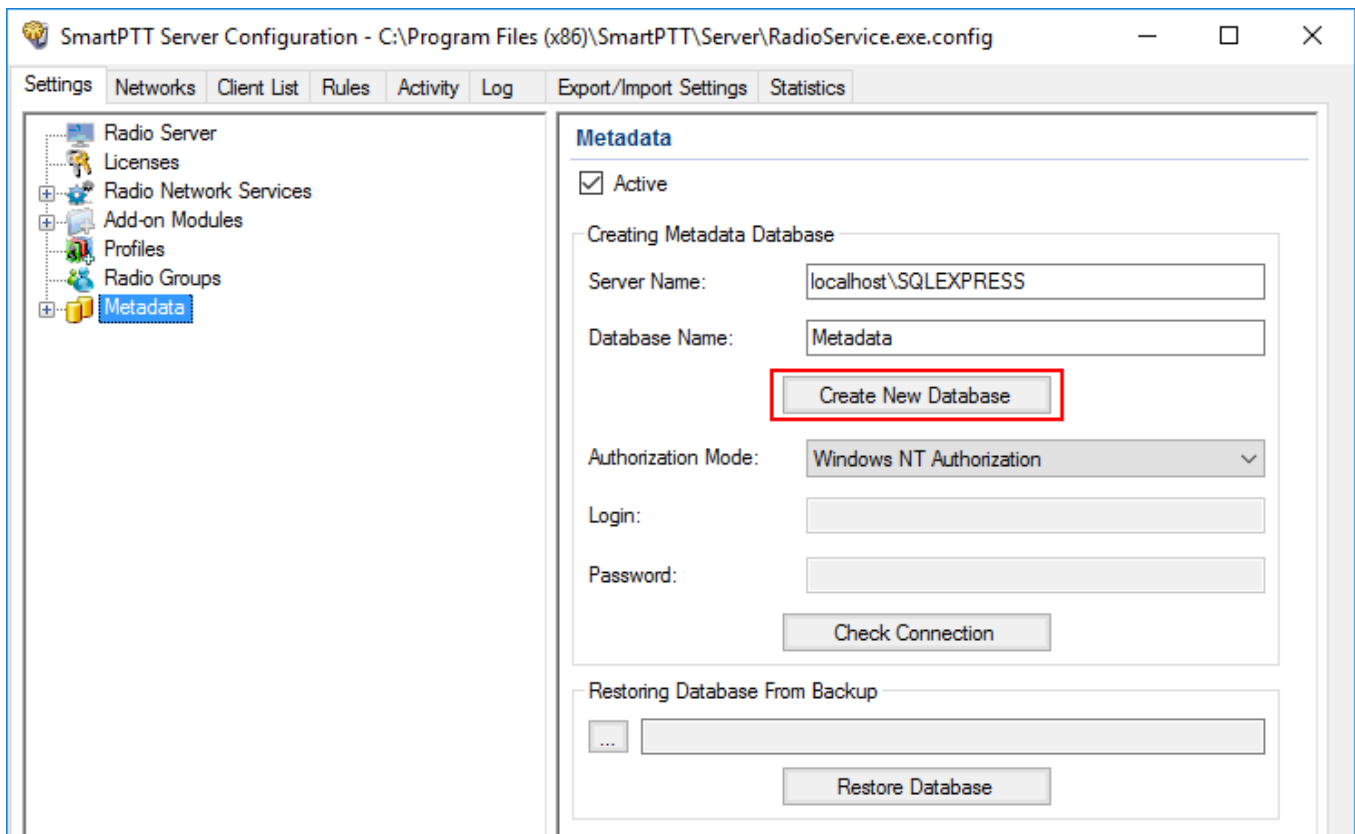
3. In the **Server name** field, enter the name of the SQL Server. You can use either *<IP-address of your computer>\<Your SQL Server name>* or *localhost\<Your SQL Server name>* format:



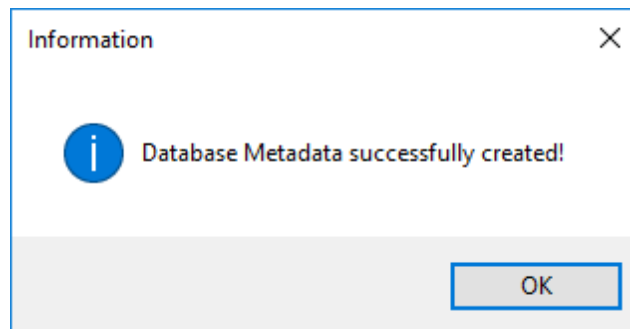
4. In the **Database Name** field, enter the name of a local metadata database.





5. Click **Create New Database**.



If creation is successful, the following message appears.



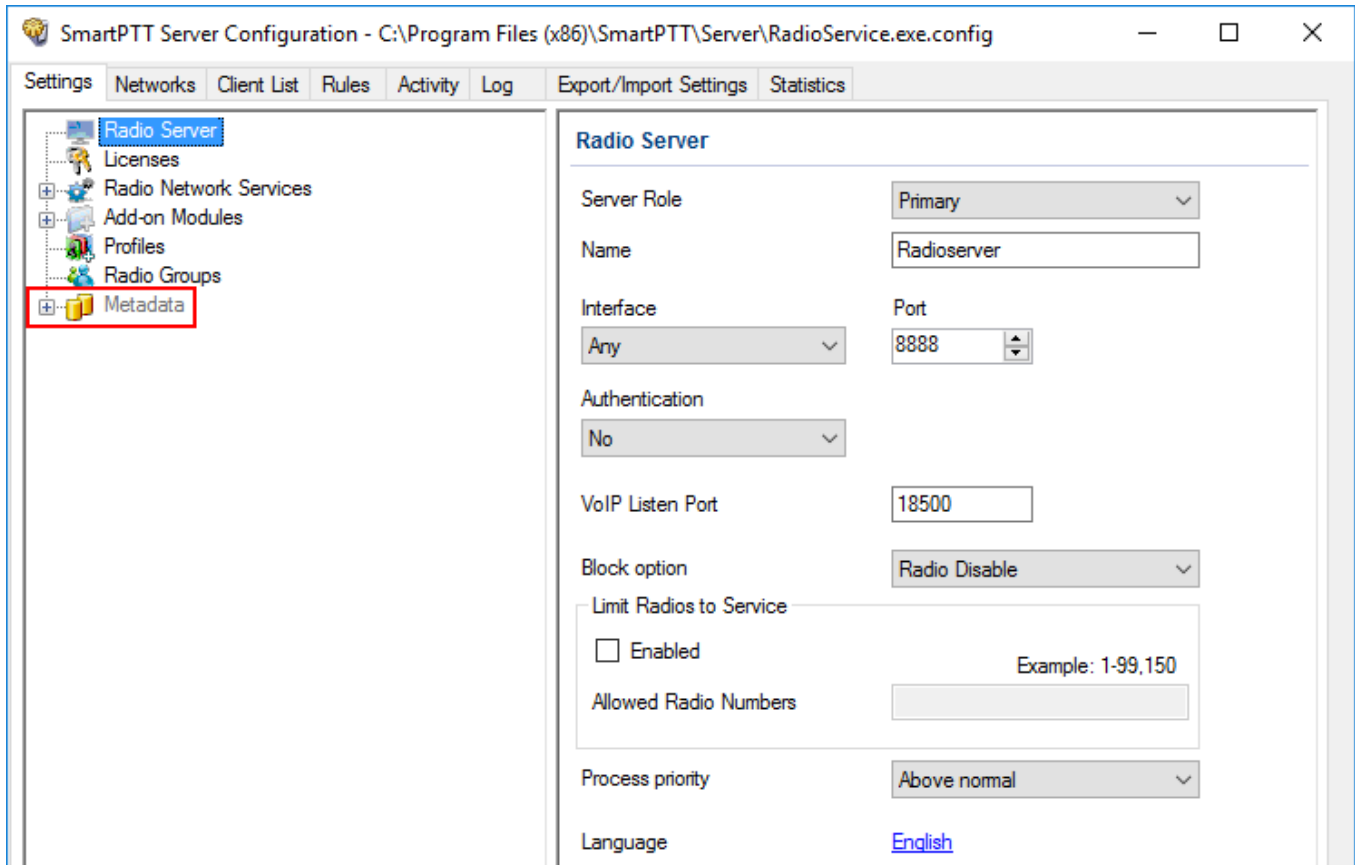
6. Click **Save**  to save changes.
7. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.



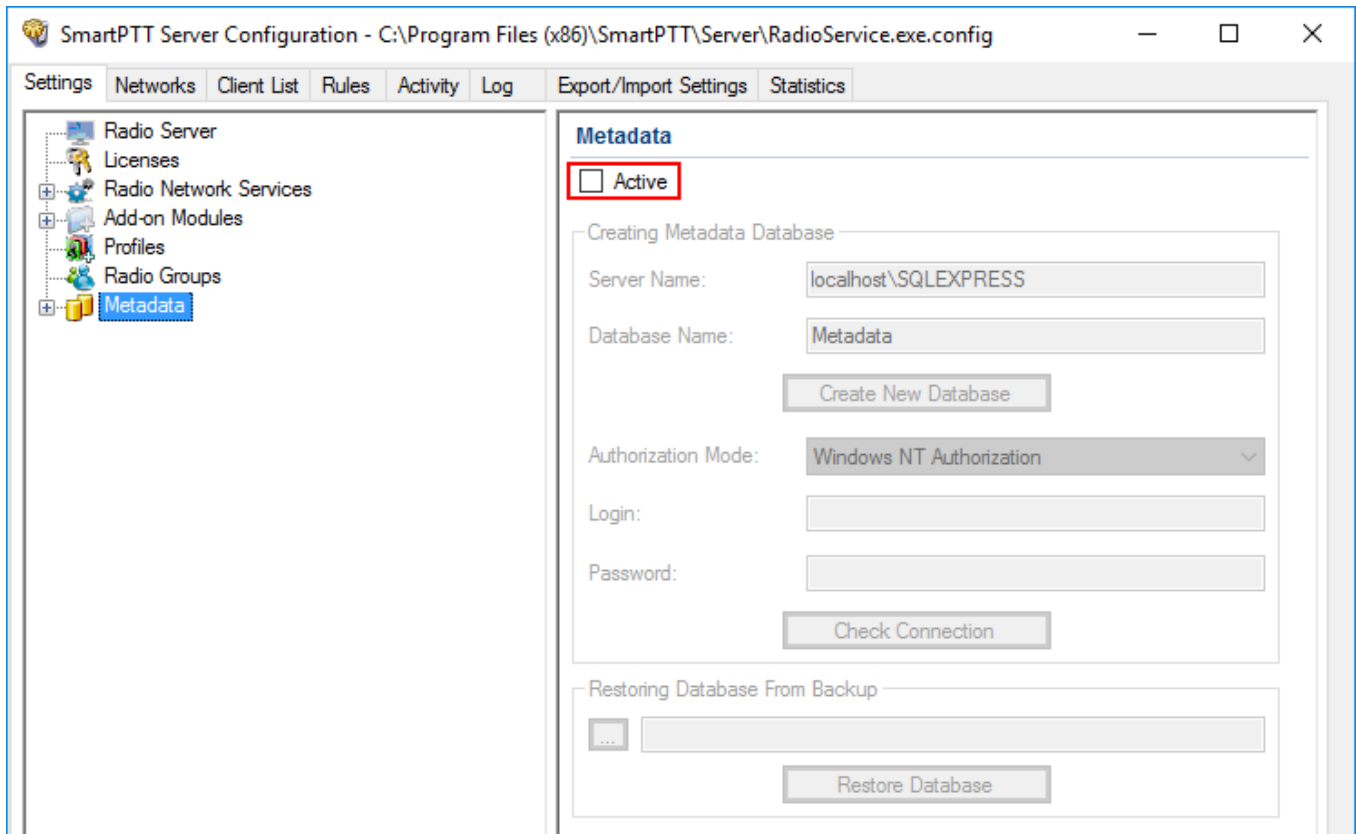
## Connecting Local Database

To connect to the local metadata database, follow these steps:

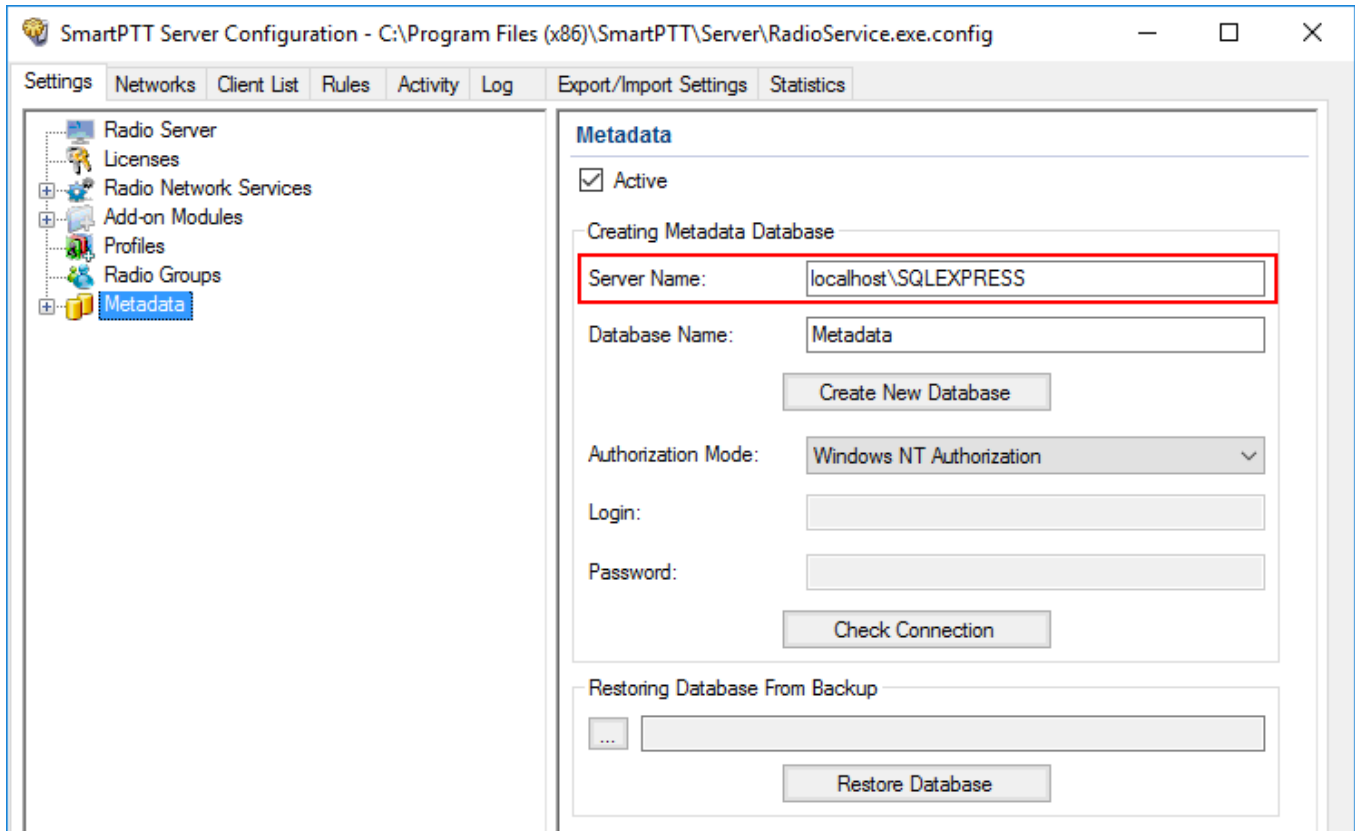
1. In the left pane of the **Settings** tab, click **Metadata**.



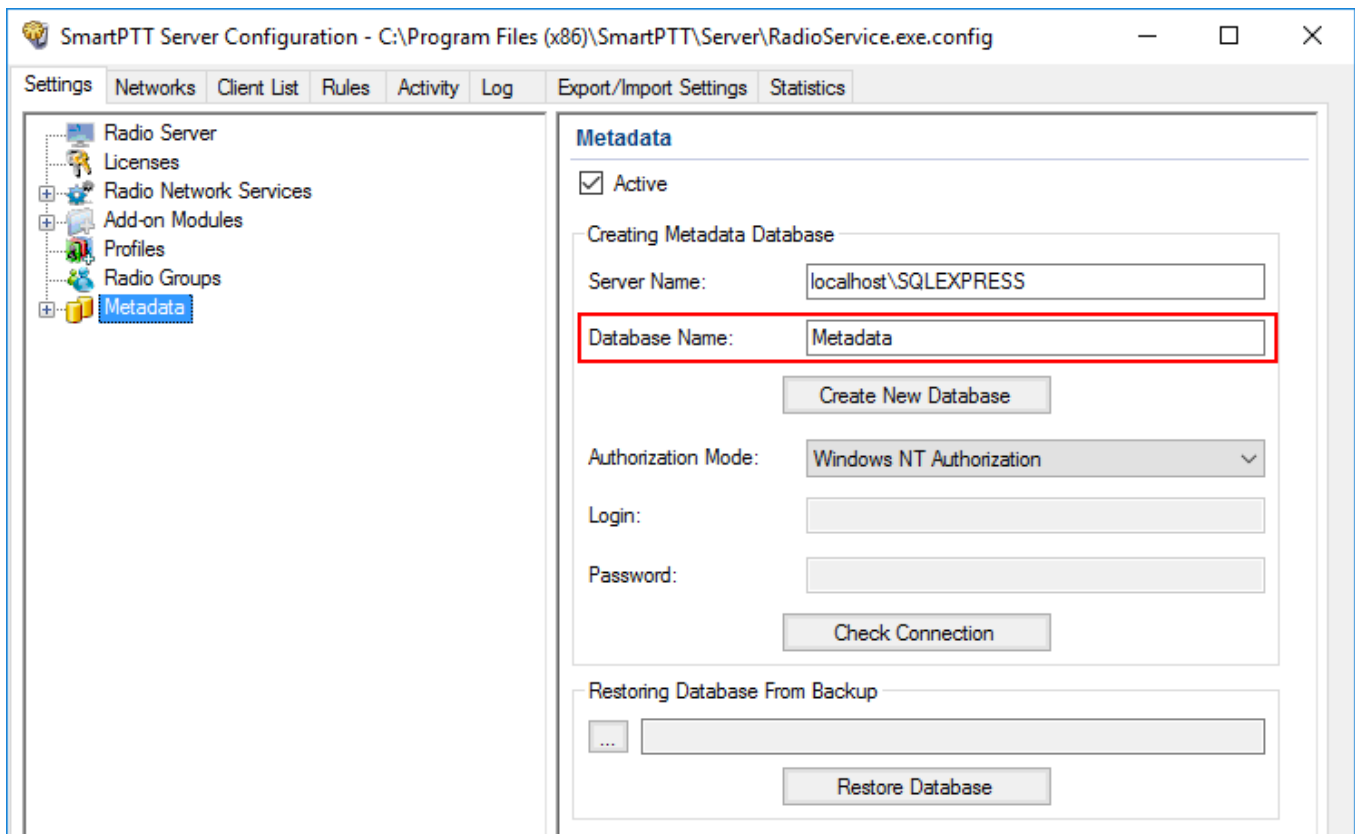
2. Make sure that the **Active** check box is selected in the **Metadata** pane.



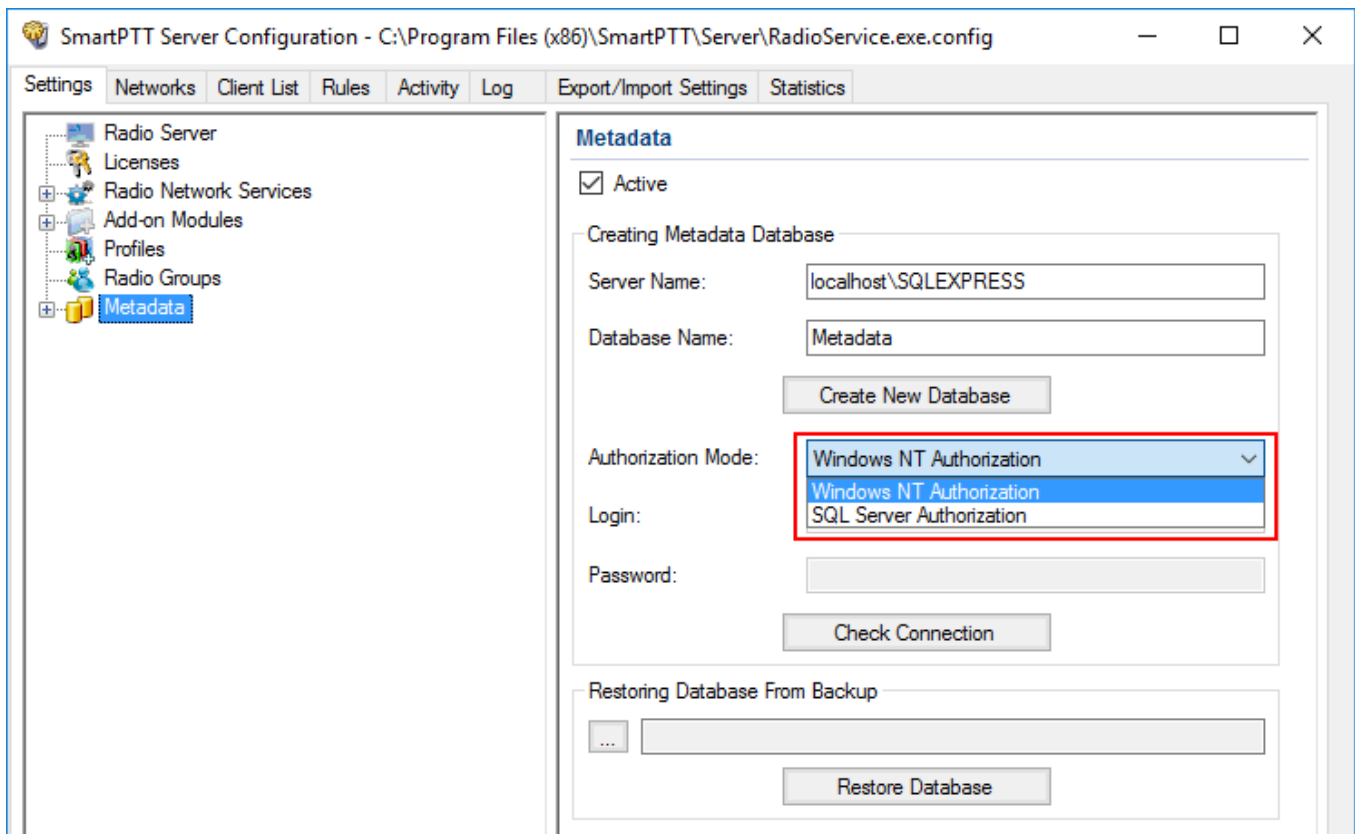
3. In the **Server name** field, enter the name of the SQL Server. You can use either **<IP-address of your computer>\<Your SQL Server name>** or **localhost\<Your SQL Server name>** format:



4. In the **Database Name** field, enter the name of a local Metadata database.



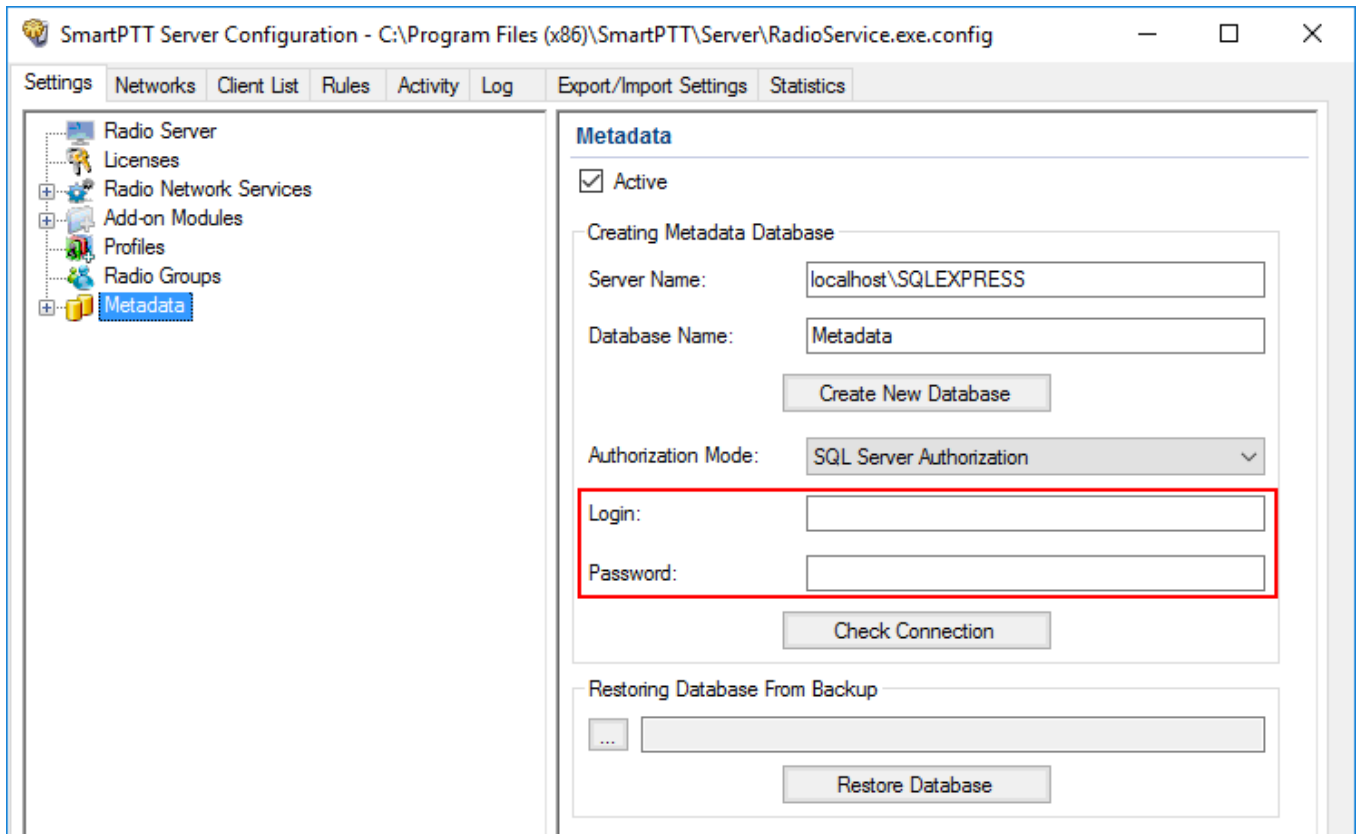
- From the **Authorization Mode** list, select the needed authorization type:



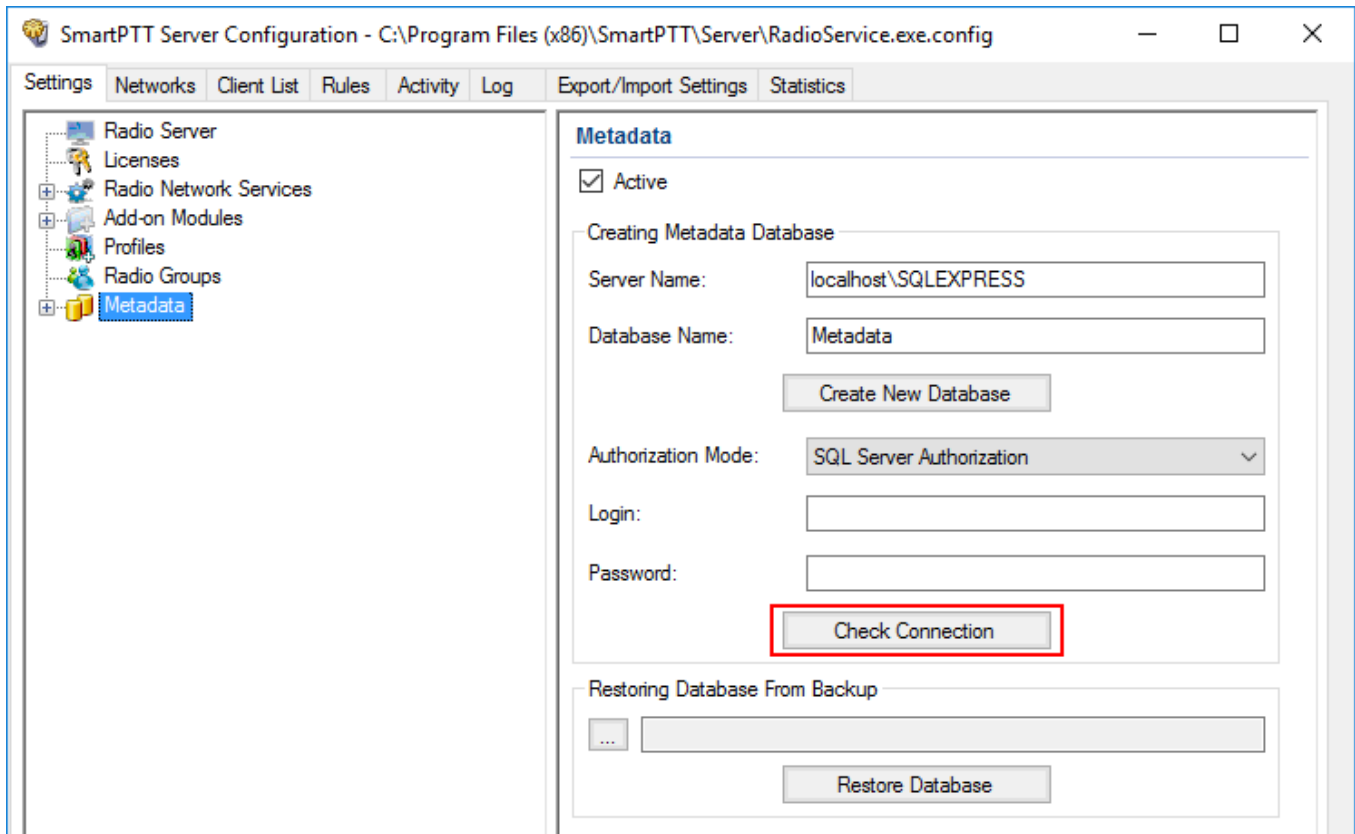
**Windows NT Authorization:** Select to use Windows account for connecting to the local SQL Server.

**SQL Server Authorization:** Select to use SQL Server account for connecting to the local SQL Server.

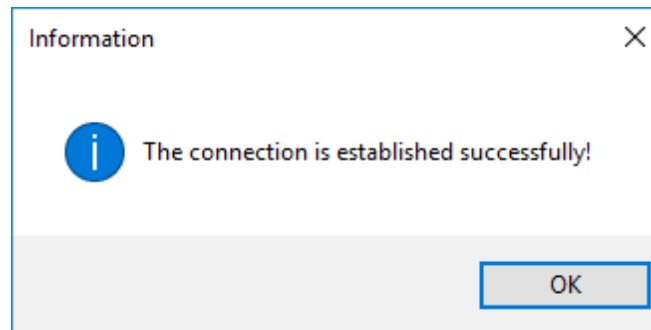
6. If **SQL Server Authorization** is selected, enter login and password.





7. Click **Check Connection**.



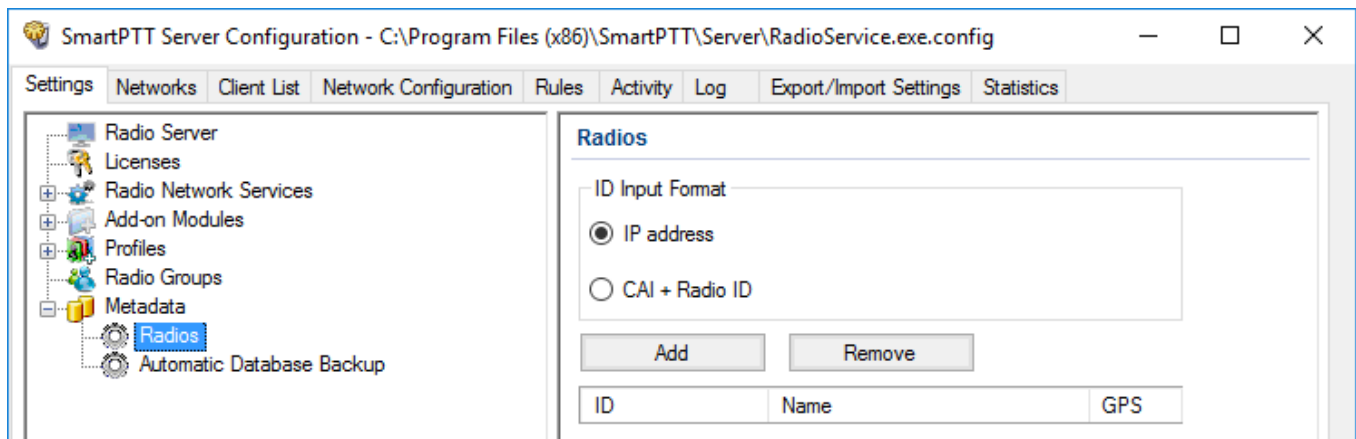
If the connection is successful, the following message appears.



8. Click **Save**  to save changes.
9. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

## 1.8.1 Radios

To add radio metadata, click **Radios**:



**ID Input Format:** Allows you to select the radio ID format to use.

To add a radio to the list, follow these steps:

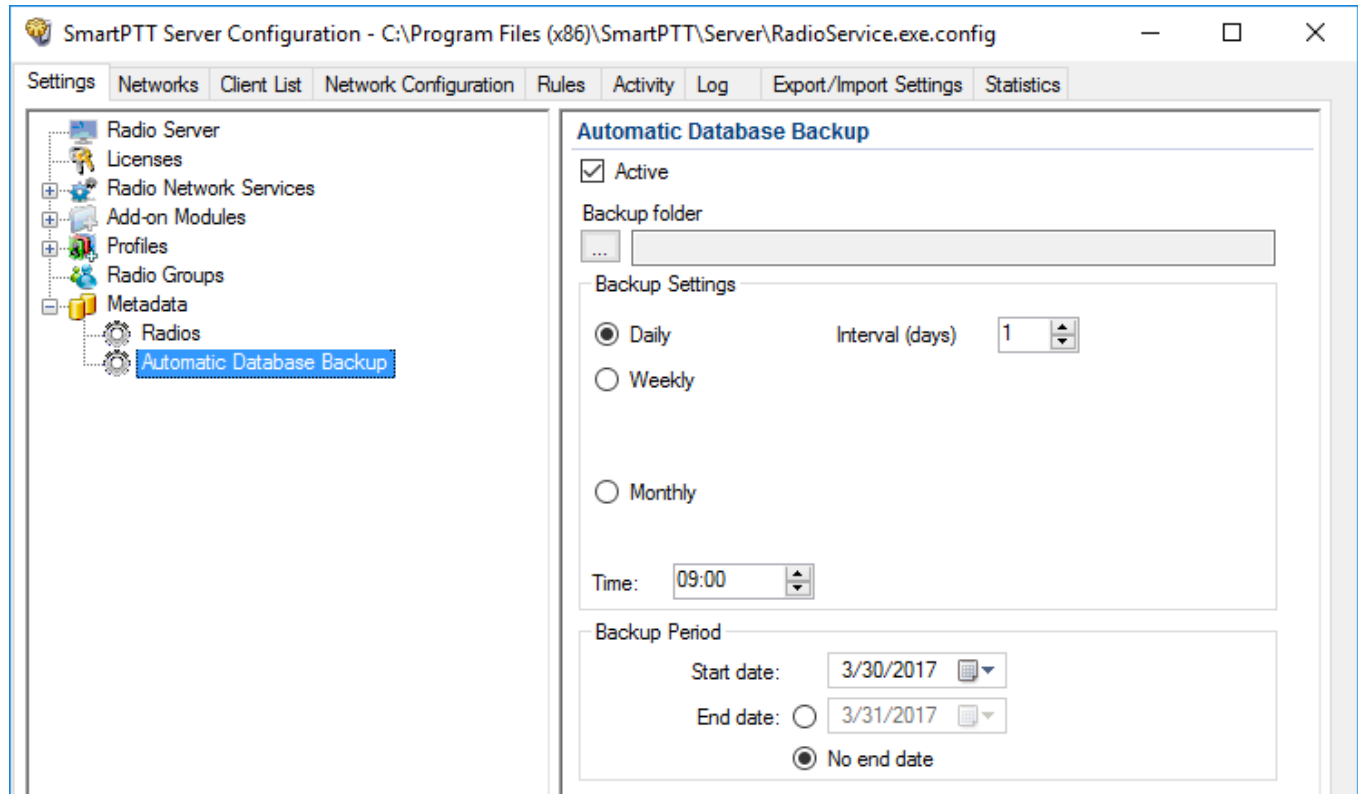
1. Click **Add**. The window for entering the radio ID opens up. The ID format depends on the selection in the **ID Input Format** section.
2. In the **Name** column, enter the name of the added radio.
3. In the **GPS** column, select whether the radio supports GPS.
4. To delete the radio from the database, select it in the list and click **Remove**.
5. Click **Save** to keep changes and restart the radioserver to see the newly added radios in the SmartPTT Dispatcher.



## 1.8.2 Automatic Database Backup

Backing up data on a regular basis helps to protect it from being erased in case of the server hardware or software failure. *SmartPTT Radioserver Configurator* allows to back up the metadata database automatically.

In order to set up automatic backup schedule of the metadata, select **Automatic Database Backup** under **Metadata** in the setting tree of *SmartPTT Radioserver Configurator*.



**Active:** Select the check box to enable the ability to create database backups in the automatic mode.

**Backup folder:** Full path to the file for saving the database backup.

**Backup Settings:** Schedule for creating the current database backup.

**Daily:** Every fixed day at the specified time (for example, every day, every third day at 9:00 a.m.).

**Weekly:** Every fixed day of the week at the specified time (for example, every Monday, Wednesday and Friday at 11:00 pm.).

**Monthly:** Once a month on the fixed day of the selected month and at the specified time.

**Backup Period:** Allows you to set time period when automatic database backup is to be made according to the selected backup settings.

**NOTE**

The number of stored backup files in the same folder is limited to 3. Otherwise, when creating a new copy, the old files are deleted.

## 2 Networks

This section contains the description of the following MOTOTRBO topologies and additional connections:

- [Control stations](#)
- [Connect Plus](#)
- [NAI systems](#)
- [Capacity Max](#)
- [SIP/RTP Interfaces](#)
- SmartPTT Radioservers

### 2.1 Control Stations

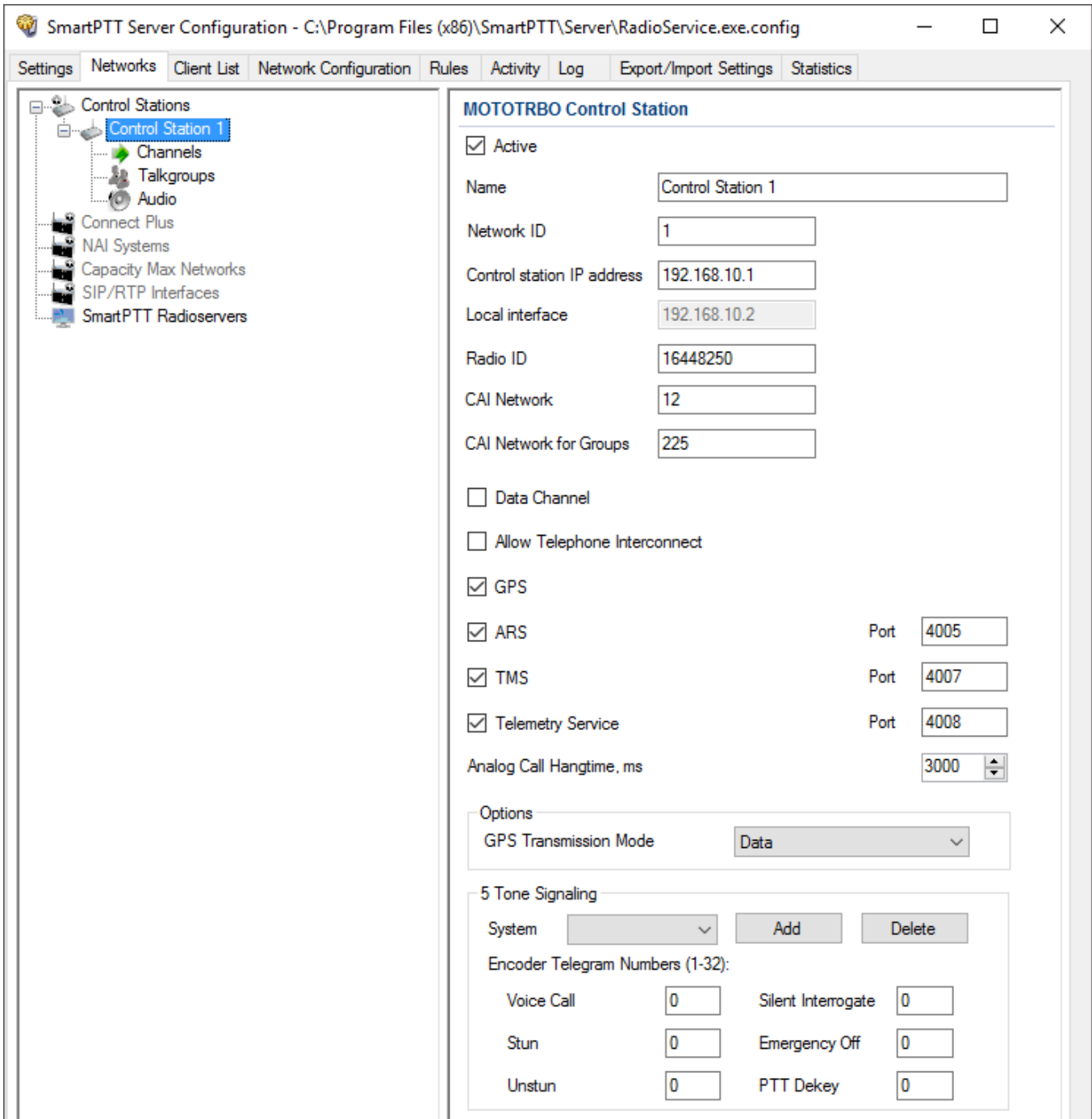
In this section you can configure MOTOTRBO, analog and remote control stations, which are used as a gateway to radio network.

The MOTOTRBO control station is a mobile or portable MOTOTRBO radio connected to the PC via USB and used as a gateway to radio network.

**NOTE**

To configure IP connectivity to MOTOTRBO control station , install the corresponding license. For more information on how to install licenses, see [Licenses](#).

To set up the MOTOTRBO control station, right-click **Control Stations** in the **Networks** tab of *SmartPTT Radioserver Configurator*, point to **Add** and click **MOTOTRBO Control Station**. The **MOTOTRBO Control Station** pane appears:



**Name:** Control station name.

**Network ID:** Unique identifier of the control station system among other systems.

**Control station IP address:** The IP address of the control station. The following address format and range are used: (001-223).(000-255).(000-255).(001-253). You can use any address except 127.x.x.x in the range from 1.x.x.x to 223.x.x.x. We recommend to use the address *192.168.10.1* by default, and in case of conflicts with other network interfaces you should select a different IP address.

**NOTE**

If two or more control stations are connected to the computer, one of the first three octets of the IP address must be unique for each control station.

**Local interface:** Local interface is used for connection to the control station. A question mark at the beginning of the field means that the control station was not defined.

**Radio ID:** Unique radio identifier used during communication with it. ID is to be set in the range from 1 to 16776415. It is highly recommended to use *16448250* as ID.

**CAI Network:** CAI-Network identifier. To be set in the range from 1 to 126. The default value is *12*.

**CAI Network for Groups:** The identifier of the group's CAI-Network. To be set in the range from 225 to 239. Use the default value is *225*.

**Data channel:** If selected, the control station is used for data transmission only and is not displayed in *SmartPTT Dispatcher*.

**Allow Telephone Interconnect:** Allows you to enable voice calls to telephone subscribers.

**GPS:** Activates location service which provides coordinates of a radio.

**ARS:** Activated registration service. Port *4005* is used as default. To register control station in the Capacity Max network, [start radioserver](#) and make a call. At that the radio will be registered in the network until [Radio Inactivity Timeout](#) runs out and the radioserver is restarted.

**TMS:** Activates the service for exchanging text messages amid dispatchers and radios. Port *4007* is used by default

**GPS Transmission Mode:** Allows you to select the way how to transmit location updates: as data packet in multiple bursts or as a single CSBK (Control Signaling Block).

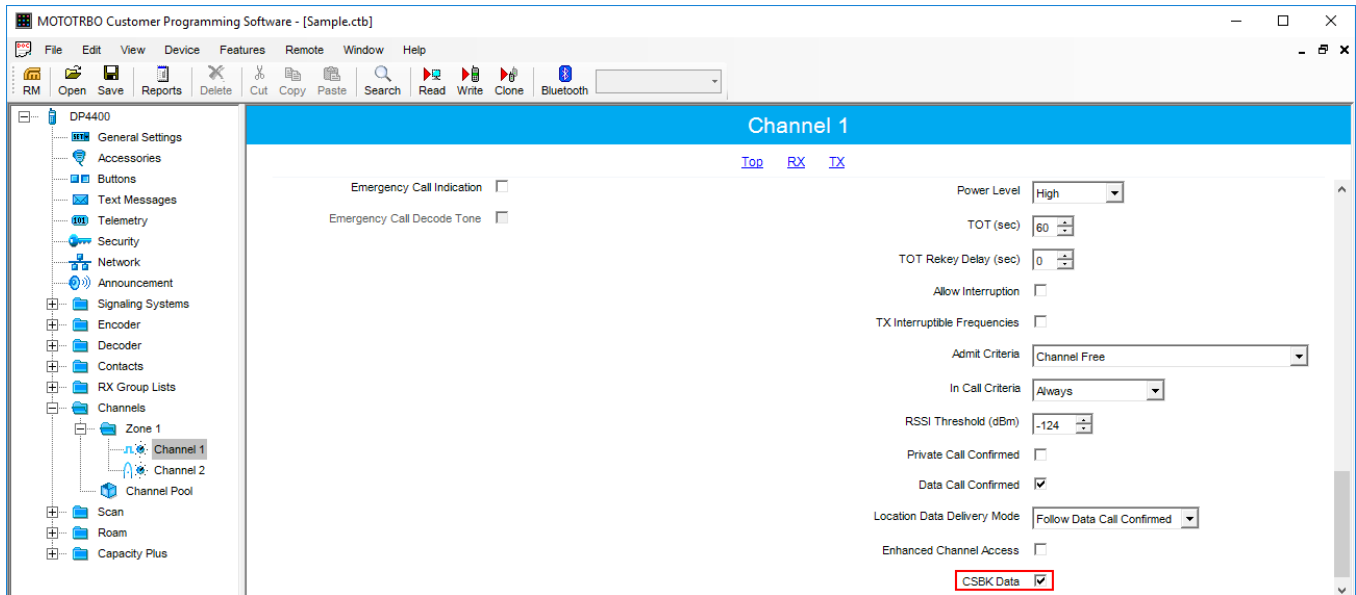
**NOTE**

The **GPS Transmission Mode** parameter is not applicable to the Capacity Plus systems.

Each solution has its own advantages and disadvantages:

GPS Transmission Mode	Advantages	Disadvantages
<b>Data</b>	No need to configure additional settings for receiving GPS data except for the Capacity Max settings. In the <i>Radio Management</i> program for all Capacity Max channels select the Trunked Channel type.	Increased traffic load on a channel
<b>CSBK</b>	Low traffic load on the channel and increased GPS transmission frequency rate — up to 4 times per minute.	Not all radios support CSBK commands
<b>Enhanced CSBK</b>	Low traffic load on the channel and increased GPS transmission frequency rate (up to 8 times per minute).	Not all radios support CSBK commands

To transmit location data using CSBK or Enhanced CSBK, enable **CSBK Data** in radio settings.



**NOTE**

Enhanced CSBK mode can be used on *Enhanced GPS* channels only.

**Analog Call Hangtime, ms:** Virtual hangtime which is used for uniting analog calls into one. This was done to not overload the event log with too many records of analog calls. During this hangtime the channel is not reserved, any one can start transmitting.

**NOTE**

Although the control station can't be seen in the **Radios** panel, you can still find it in **Report Wizard** and **Radio Activity Report**.

**5 Tone Signaling:** Settings for 5-Tone signaling, also known as SelectV. It is used in the analog networks to arrange selective calls. As a result, the analog channel provides additional services other than all call. For example, group and private calls to the radio, blocking or unblocking the radio, checking the radio presence on the channel.

**NOTE**

The current version of *SmartPTT Radioserver Configurator* supports SelectV signaling for MOTOTRBO DM 46xx Series radios and DP 46xx, DP 48xx Series radios used as control stations.

**NOTE**

Make sure that control stations and radios operating on the analog channel are configured properly in *MOTOTRBO CPS*.

Selective call is based on radio addressing, i.e., on assigning IDs to radios. At the beginning of each session the sound signals of different frequencies are transmitted and received by the radio. Such signals are called telegrams. Each telegram contains from one to three sequences. Every sequence may include up to 12 tones. The telegram formed in this way may include the calling radio or talkgroup address, the radio ID, a status message or a command. The radio receives all signals, but handles only its telegrams, i.e., telegrams addressed to this radio.

**NOTE**

You can specify one or several identifiers (**CAI + Radio ID** or **IP, MDC ID** or **5 Tone ID**) as a radio ID in *SmartPTT Dispatcher* in the **Properties** window. If the radio is used on the analog channel only, enter **5 Tone ID** or **MDC ID**; the **CAI** and **Radio ID** or **IP** fields must be left empty.

**System:** 5 Tone signaling system. Parameters in this section allow you to match the outgoing command from SmartPTT Radioserver and the telegram number.

**NOTE**

When decoded, telegrams are verified if the telegram sequences correspond to one of the definitions, and then the command of this definition is applied. To configure the command definition, use *MOTOTRBO CPS* (**Decoder** → **Definitions**, the **Matching Encode Telegram** field).

To create a 5-Tone signaling system in *SmartPTT Radioserver Configurator*, click **Add**. The several signaling systems can be added for each control station. To change the control station signaling system, select the required value from the list.

To delete the selected 5 Tone signaling system, click **Delete**.

**Voice Call:** The telegram number conforming to the private or group voice calls.

**Silent Interrogate:** The telegram number which corresponds to the check command of the radio presence on the network without notifying the radio.

**Stun:** The telegram number which stands for sending the **Block** command to the radio.

**Unstun:** The telegram number which stands for sending the **Unblock** command to the radio.

**Emergency Off:** When the radio receives the telegram number while in an emergency mode, the radio terminates the emergency mode.

**PTT Dekey:** When the radio receives the telegram number, the radio stops the current call session.

When the telegram encoding parameters are set, it is required to assign the signaling system for the channel (see the [Channels](#) tab).

If necessary, the control station can be disabled from the connection list. To do this, clear the **Active** check box.



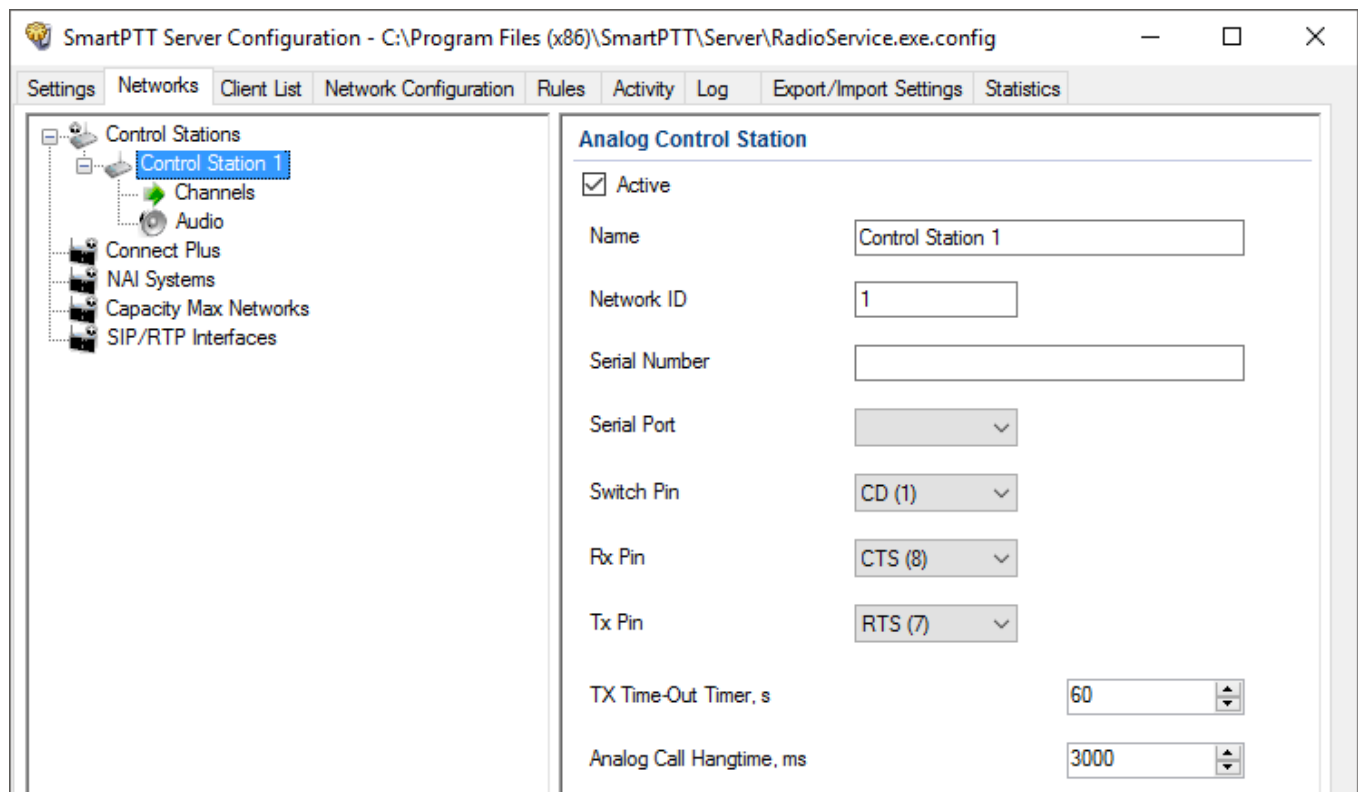
To delete the control station, right-click **Control Stations** entry in the setting tree of *SmartPTT Radioserver Configurator* and click **Delete**.

## Analog control station

To follow user evaluations and to facilitate migration from analog technology to digital technology, SmartPTT has been complemented with support of analog control stations.

Here you can find the configuration manual for the analog control station connected to the computer COM port via interface card. The interface card schematic is shown on the [website](#).

To add an analog control station, right-click **Control Stations** in the **Networks** tab of *SmartPTT Radioserver Configurator*, point to **Add** and click **Analog control station**. At that a new setting window appears on the right.



**Name:** Control station name.

**Network ID:** Unique ID of the network.

**Serial Number:** The control station serial number.

**Serial Port:** The port to which the control station is connected.

**Switch Pin:** (incoming) is set to 1 (< -3.0V) when the control station is switched on.

**Rx Pin:** (incoming) is set to 1 when a signal carrier is registered on the channel.

**Tx Pin:** (outgoing) is set to 1 to switch to transmit mode.

Change the display of the control signals of the control station to the pins of the socket RS323 (see the DE-9 pin numbers in brackets), if it is different from the one that is specified.

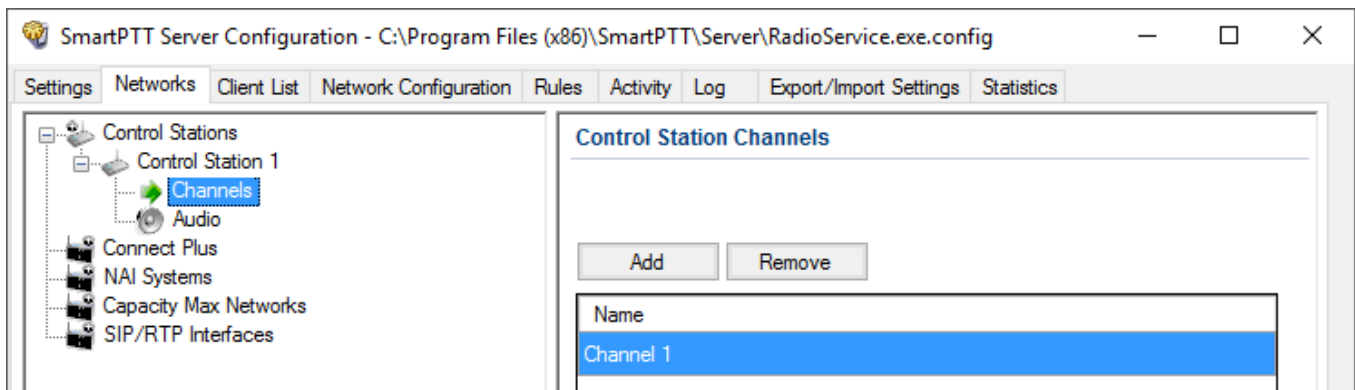
#### NOTE

The default values of the control signals are universal and usually do not require any changes.

**TX Time-Out Timer, s:** Continuous radio transmission timeout. After this time the transmission is interrupted.

**Analog Call Hangtime, ms:** A virtual hangtime which is used for uniting analog calls into one. This was done to not overload the event log with too many records of analog calls. During this hangtime the channel is not reserved, any one can start transmitting.

In the **Control Station Channels** window add a channel and name it (otherwise the dispatcher displays 1:1).



Audio is configured in the same way as for the control stations MOTOTRBO.

Save the changes and restart the service.

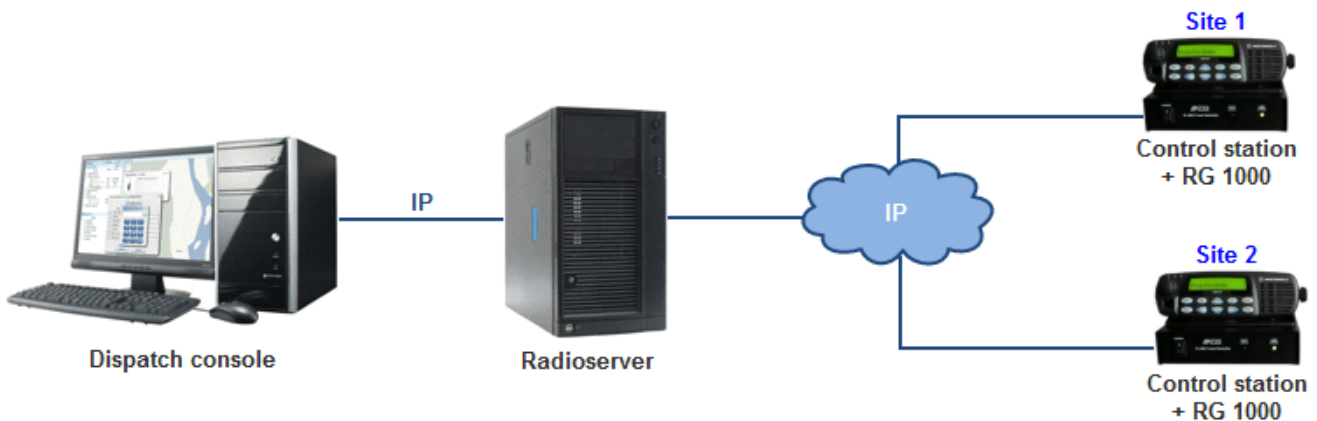
#### NOTE

In *SmartPTT Dispatcher* the operation of the analog control station is the same as for MOTOTRBO control stations in analog mode without signaling.

## Remote control station

Remote control station is a MOTOTRBO control station located anywhere else, and not connected to the radioserver PC by a USB cable.

The control station is connected to a special gateway for remote control (RG-1000) which provides IP connection to SmartPTT Radioserver. RG-1000 supports MOTOTRBO control stations (DM series) on both digital and analog channels.



To add a new remote control station, right-click **Control Stations**, point on **Add** and then click **Remote MOTOTRBO Control Station**. At that a new setting window appears on the right.

The screenshot shows the 'SmartPTT Server Configuration' application window. The 'Networks' tab is active, and the 'Remote MOTOTRBO Control Station' configuration is displayed. The left sidebar shows a tree view with 'Remote control station 1' selected under 'Control Stations'. The main configuration area includes the following fields and options:

- Active
- Name: Remote control station 1
- Network ID: 1
- Remote gateway IP address: 192.168.10.1
- XCMP port: 30010
- Local interface: 192.168.10.2
- Radio ID: 16448250
- CAI Network: 12
- CAI Network for Groups: 225
- Data Channel
- Allow Telephone Interconnect
- GPS
- ARS Port: 4005
- TMS Port: 4007
- Telemetry Service Port: 4008
- Analog Call Hangtime, ms: 3000
- Options:
  - GPS Transmission Mode: Data
- Set local ports
 

Service	Local port
XCMP	1024
Audio	1024
GPS	1025
TMS	1026
ARS	1027
Telemetry	1028

**Remote gateway IP address:** The IP address of the remote gateway RG-1000 which provides control over the remote control station.

**XCMP Port:** The port of the remote gateway, it should match the XCMP port set in the settings of the remote gateway.

**Local interface:** The local interface used for connection to the remote gateway.

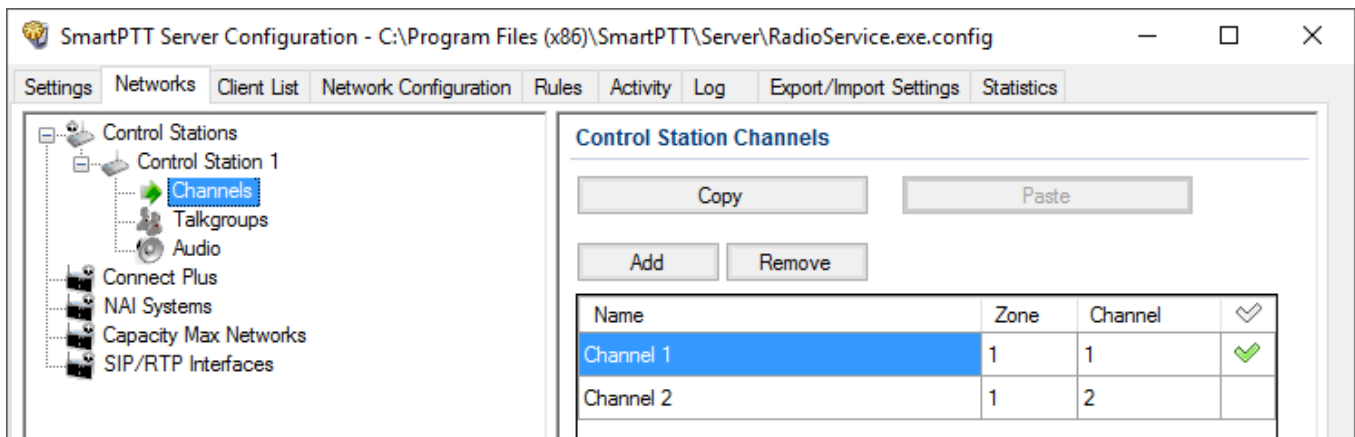
**Set local ports:** Local ports that can be used for connection to the gateway, if the default ports of the corresponding services are already in use. By default the system occupies local ports automatically, but you can define them manually.

Other parameters of the remote control station correspond to the parameters of an ordinary MOTOTRBO control station (see [here](#)).

## 2.1.1 Configuring Channels

After adding a control station, configure its channels. To set up and edit control station channels, click **Channels** in the setting tree of *SmartPTT Radioserver Configurator*. The following window is displayed.

To add a channel, click **Add**. At that, you will see a record of the added channel appear in the table.



**Name:** Channel alias visible to SmartPTT Dispatcher.

**Zone:** Serial number of a channel group. Information on the maximum possible number of zones and radio channels is shown in the following table.

Model	Maximum number of zones	Maximum number of channels per zone	Maximum total number of channels
Mobile radio with display	50	160	160

Model	Maximum number of zones	Maximum number of channels per zone	Maximum total number of channels
Mobile radio with seven segment display	2	32	32

**Channel:** Channel sequence number.

**Signaling:** 5 Tone signaling system taken from the [MOTOTRBO Control Station](#) settings window. The field is available only if the MOTOTRBO control station has at least one 5 Tone signaling system. When *Auto* is selected, the automatic detection of the channel type is set (analog, digital, IP Site Connect slot, etc.). The detection take place when you connect the control station.

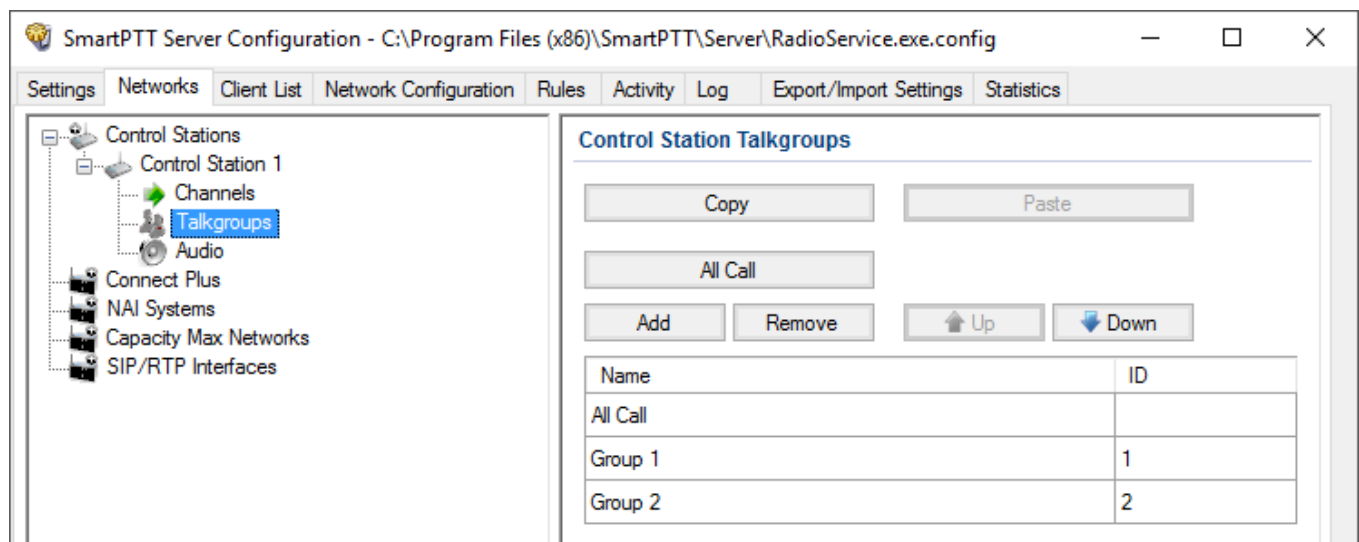
**NOTE**  
 If the channel type can't be determined automatically, you should specify the signaling system explicitly.

Selected channel will be set at the control station, when you start the radioserver.

To remove a channel, click **Delete**. To edit channel name, zone or channel number, place the cursor on the corresponding field and make changes.

## 2.1.2 Configuring Talkgroups

To set up and edit **Control Station Talkgroups**, click **Talkgroups** in the **Networks** tab of SmartPTT Radioserver Configuration. The following window appears:



To add a talkgroup, click **Add**. To add an all-call, click **All Call**. The added talkgroups will also appear in the **Profiles** window. To change the order of groups in the list, use the **Up** and **Down** arrows. The order defined in the window will be used in *SmartPTT Dispatcher*.

**Name:** Talkgroup alias displayed by the control station.

**ID:** Talkgroup unique identifier used during communications. It should be set in the range from 1 to 16776415.

**Remove:** Delete the selected talkgroup.

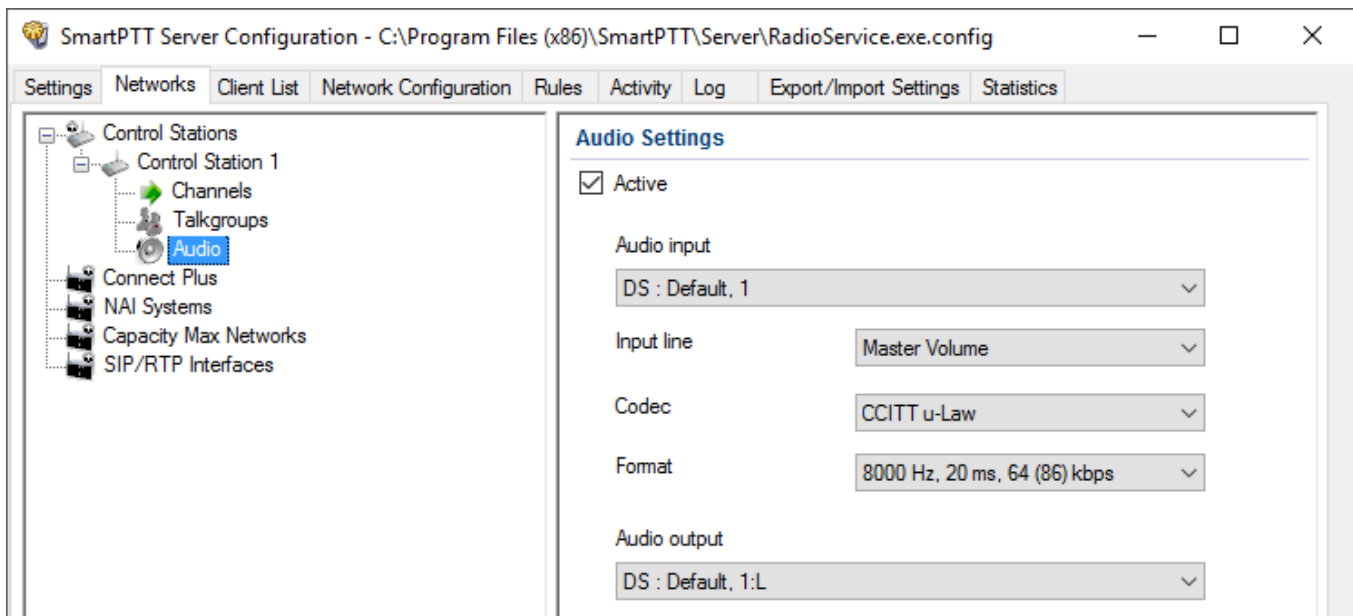
**Copy:** Copy added groups to the clipboard.

**Paste:** Paste copied groups from the clipboard.

To edit talkgroup name or ID, set the cursor on the corresponding field and make changes.

## 2.1.3 Configuring Audio Settings

To select audio devices and set up VoIP parameters, click **Audio** in the **Networks** tab of *SmartPTT Radioserver Configurator*.



**Active:** Allows disabling calls for a control station if it is used to transmit data only.

**Audio input:** An audio device to which the control station audio output is connected.

**Input line:** Audio mixer line used for connections. The control station audio output can be connected to the line input of the audio device.

**Codec:** Outgoing audio stream compression method.

**Format:** Sampling frequency of an outgoing audio stream.

### Example

Consider the following codec format: *8000 Hz, 20 ms, 64 (86) kbps*. Those settings mean:

- *8000Hz*: Sampling rate
- *20 ms*: Frame size
- *64 kbps*: Voice data bit rate
- *86 kbps*: Full bit rate (required network bandwidth)

**Audio output:** Audio device to which the control station audio input is connected.

## 2.2 Connect Plus

SmartPTT PLUS supports Connect Plus multi-site trunking system, which starting from version 8.5 can be used not only for ARS, TMS and GPS functionality, but also for voice communication between the dispatcher and radios.

Connect Plus network can include up to 15 repeaters (29 channels + 1 control channel) on each site. Each site must have at least one XRC Controller. It is the core of the Connect Plus network and its presence on each site is obligatory. The XRC Controller provides central call processing and real-time resource management for MOTOTRBO Connect Plus digital trunking systems. There can be two XRC Controllers per site if one of them serves as backup to the primary XRC. The secondary controller provides backup capability, but it does not increase the number of repeaters and calls that can be managed per site.

XRT Gateways are required for voice communication only. MOTOTRBO Connect Plus multi-site trunking network provides extended load capacity and provides digital communication to as many as 2,900 users per site.

When using Connect Plus network, SmartPTT Radioserver plays the role of a virtual repeater.

The Connect Plus network configuration includes the following stages:

- Adding new network and its basic configuration
- Setting up XRC Controller configurations



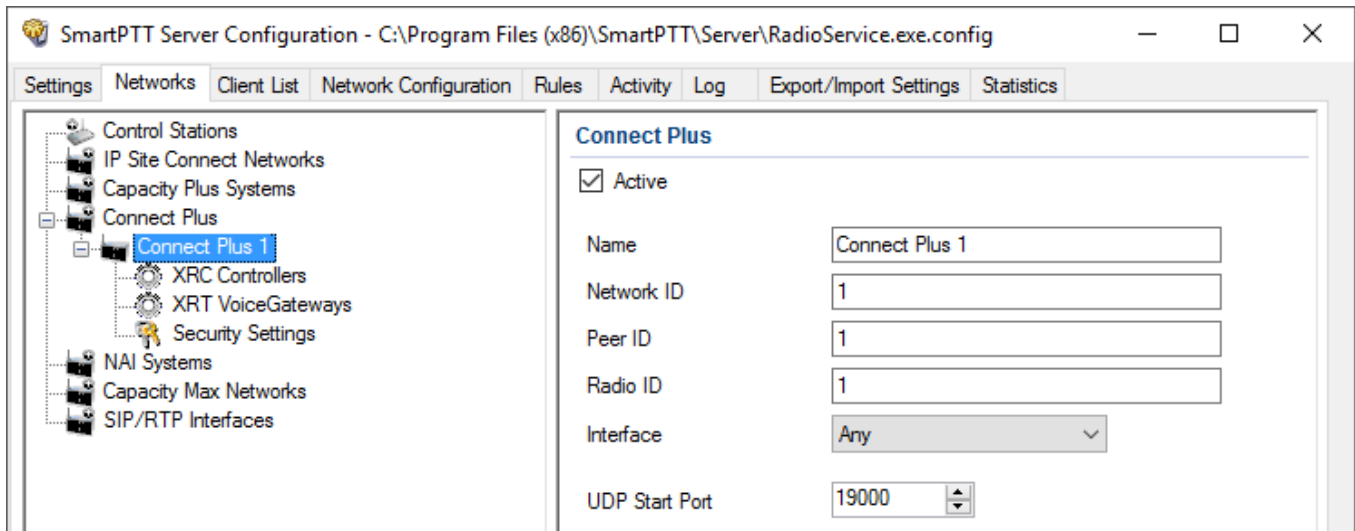
- Setting up talkgroups for group messages
- Setting up XRT Gateway parameters for voice communication
- Adding talk paths for voice calls

## 2.2.1 Configuring Connect Plus

First of all, make sure you have the necessary license for the Connect Plus network, i.e., Connect Plus Voice Support and Connect Plus Data Support.

To configure Connect Plus settings, add new Connect Plus system: right-click Connect Plus in the **Networks** tab of *SmartPTT Radioserver Configurator* and click **Add**.

The **Connect Plus** window appears:



**Active:** Activates Connect Plus System.

**Name:** Connect Plus network name.

**Network ID:** Unique ID of the Connect Plus network, that is used inside SmartPTT system. This is important if you have more than one Connect Plus network. Note that this ID is different from the Network ID defined in the XRC Controller codeplug.

**Peer ID:** Unique ID of the virtual repeater in the Connect Plus network. Make sure this ID is different from the repeater ID in the Connect Plus network.

**Radio ID:** The identifier of SmartPTT Radioserver. This identifier will be displayed on radios at receiving private calls and text messages from the dispatcher. If there are several dispatchers, you can create a profile for each operator ([Profiles](#)) and define a unique identifier for each operator. **Radio ID** set in this window must correspond to the **Console User ID** field in the XRT Gateway settings.

The screenshot shows a 'User Details' configuration window with the following fields and options:

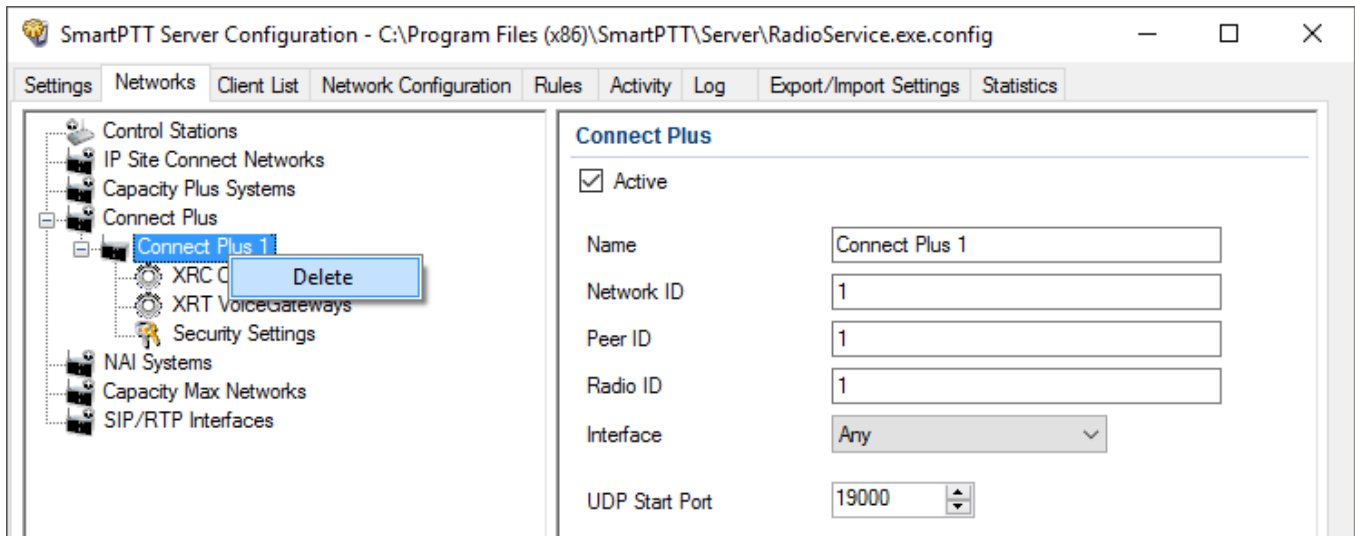
- Username: public
- Password: [masked]
- Max Talk Paths: 10
- Billing Enabled
- Network Wide All Call (NWAC) Enabled
- Group Talk Paths:
  - Group ID: 1001,1002
- Private Talk Paths (highlighted with a red box):
  - Console User ID: 100

At the bottom of the window are three buttons: 'New', 'Save', and 'Delete'.

**Interface:** IP address of the virtual repeater, i.e. SmartPTT Radioserver. Specify the IP address of the PC where the radioserver is installed.

**UDP Start Port:** Starting port number for local UDP ports that will be used by SmartPTT Radioserver for talk paths. It is recommended to use the default value of *19000*. If the created Connect Plus network should not transmit voice packets, this field can be ignored.

To delete the Connect Plus network, right-click the network you want to delete and click **Delete**.



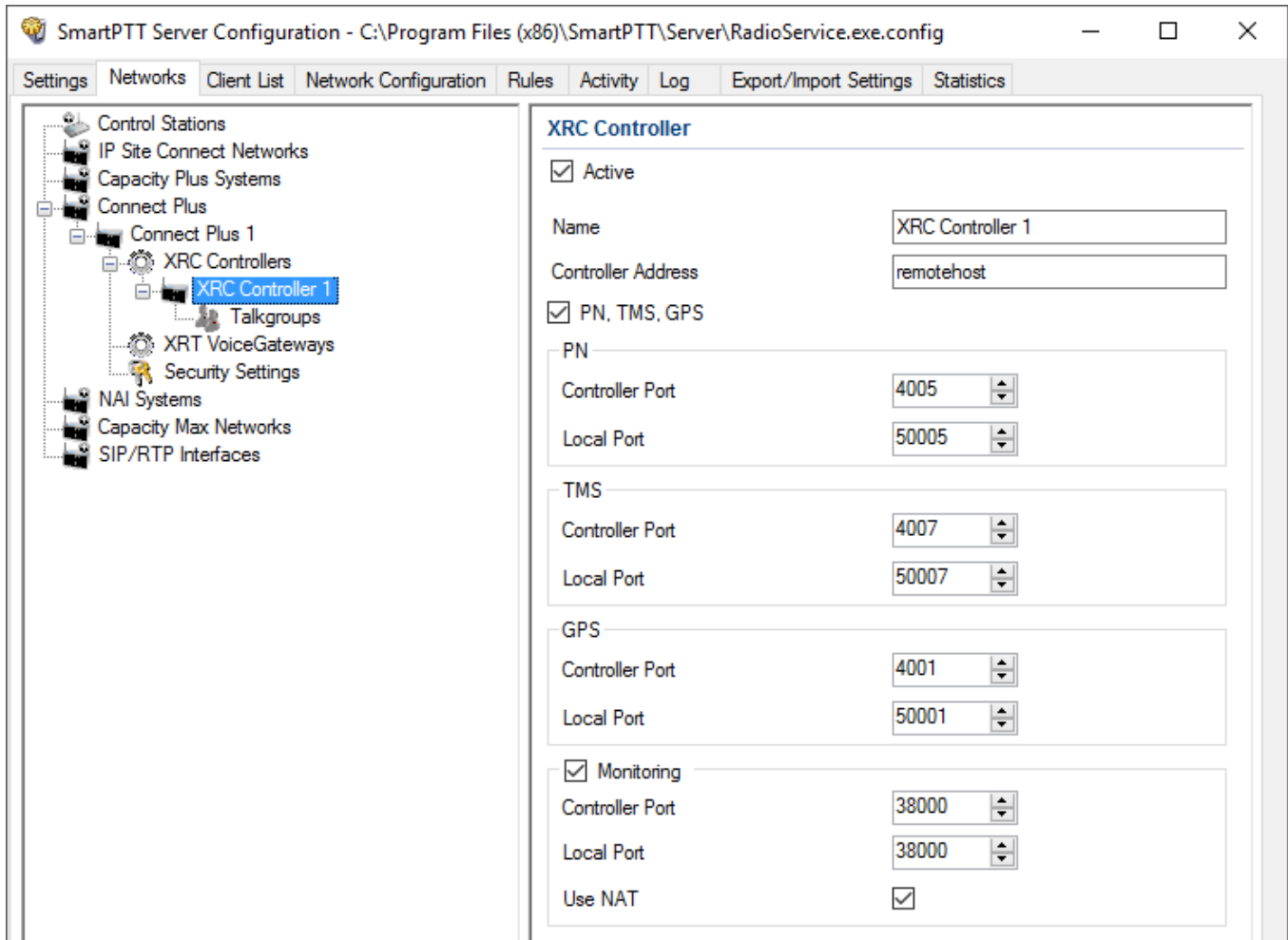
## 2.2.2 XRC Controller

The XRC Controller is necessary for transmitting registration and de-registration, GPS data, text messages. The XRC Controller is also required for making private calls, because without it, radios will be regarded as offline, and the dispatcher will not be able to make private calls.

### NOTE

To configure XRC Controller, install the corresponding license. For more information on how to install licenses, see [Licenses](#).

You can add only one XRC Controller per site. Right-click **XRC Controller** to add. The following window appears:



**Name:** XRC Controller name. This is used only in *SmartPTT Radioserver Configurator*.

**Controller Address:** IP address of the XRC Controller. Port is not required in this field.

In order to enable data services on the controller select **PN, TMS, GPS**.

**Controller port:** Port of XRC Controller for the corresponding service.

**Local port:** Port of the virtual repeater for the corresponding service.

#### NOTE

**PN Controller Port** should match the port of Presence Notification service set in XRC Controller.

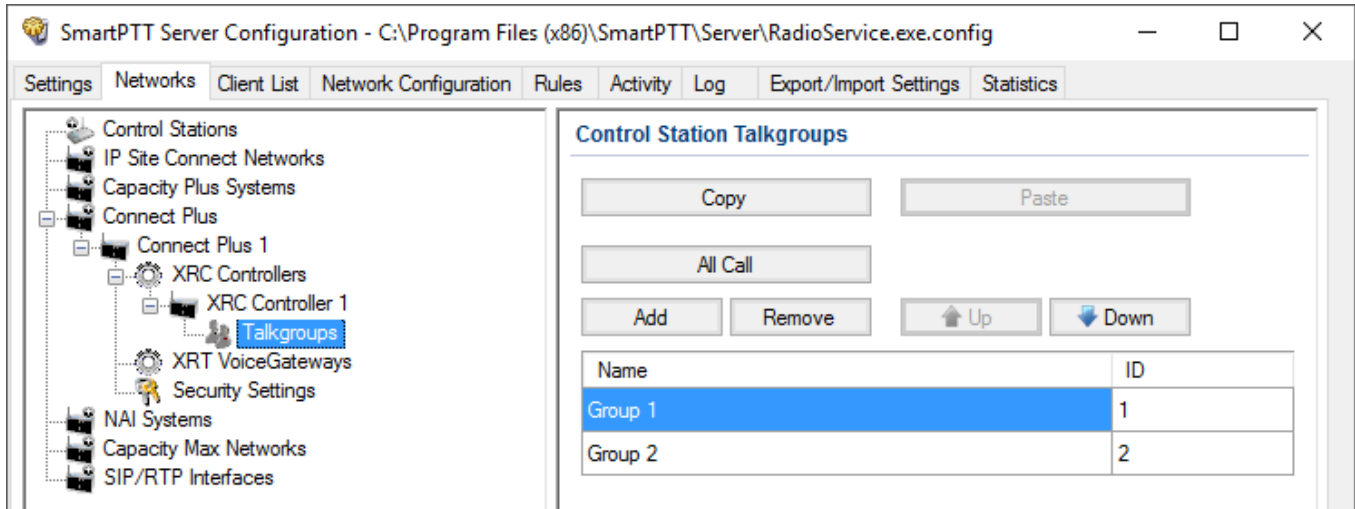
To be able to review the XRC Controller on the **Monitoring** panel in *SmartPTT Dispatcher*, select **Monitoring** and specify **Controller port** and **Local port**. If the XRC Controller is in one local

network with the radioserver, leave **Use NAT** clear. If the XRC Controller is outside the local network of the radioserver, select **Use NAT**.

#### NOTE

Make sure that general [Monitoring](#) is active.

In order to send group text messages, add talkgroups. Click **Talkgroups** under **XRC Controller**. The following window opens:



### 2.2.2.1 Configuring Joint GPS and Indoor Data

If you want to receive joint location data (GPS and indoor) in Connect Plus, configure the following settings:

- Radio settings in *MOTOTRBO CPS*
- Radio settings in SmartPTT Dispatcher
- Repeater settings in *MOTOTRBO CPS*

### 2.2.2.1.1 Configuring Radio in MOTOTRBO CPS

To configure radio in *MOTOTRBO CPS*, follow these steps:

1. In the radio firmware file, select **Channels** → **<Zone Name>** → **<Channel Name>**.
2. In the **<Channel Name>** pane, perform the following actions:
  - Select the **Enhanced GNSS** check box, and from the **Window Size** list, select *10*.
  - From the **Compressed UDP Data Header** list, select *MSI*.

### 2.2.2.1.2 Configuring Radio in SmartPTT Dispatcher

To configure radio in SmartPTT Dispatcher, follow these steps:

1. Open the radio properties window.
2. In the **Location** tab, perform the following actions:
  - a. Select the **Indoor Tracking** check box.
  - b. Select the **Update Interval** check box, and enter *30* in the field.

### 2.2.2.1.3 Configuring Repeater in MOTOTRBO CPS

To configure repeater in *MOTOTRBO CPS*, follow these steps:

1. In the repeater firmware file, select **Channels** → **<Zone Name>** → **<Channel Name>**.
2. In the **<Channel Name>** pane, in the **Enhanced GNSS area**, select the **Enable** check box.

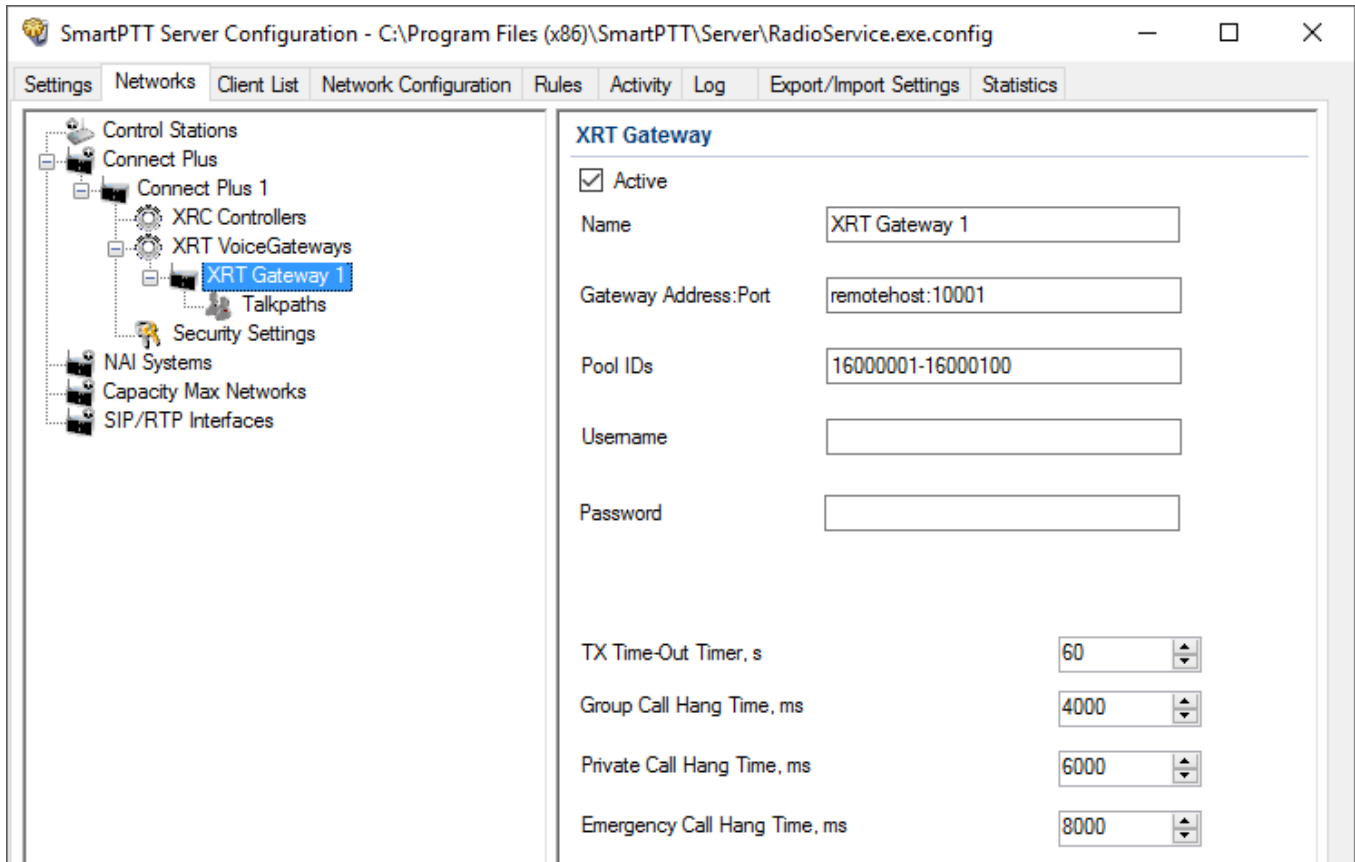
## 2.2.3 XRT Gateway

The XRT Gateway allows making voice calls and monitor call events in the Connect Plus system. You can have maximum 5 XRT Gateways working in one network. To support private voice communication, it is necessary to have an XRC Controller. Otherwise, radios will be regarded as offline, and private calls will be impossible.

#### NOTE

To configure XRT Gateway, install the corresponding license. For more information on how to install licenses, see [Licenses](#).

To add the gateway, right-click **XRT VoiceGateways** and click **Add**. The following window appears:

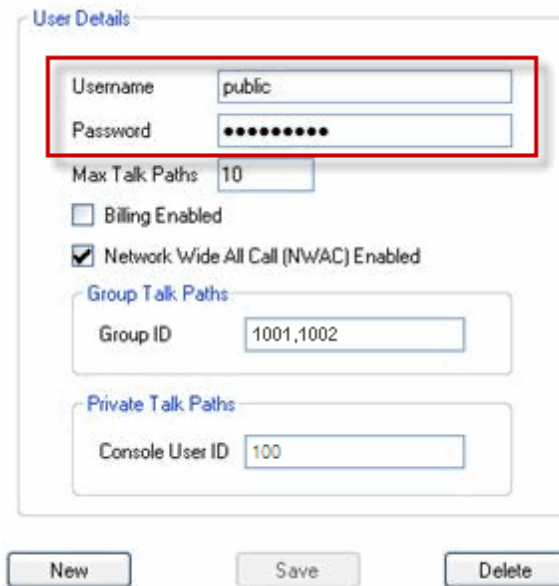


**Name:** XRT Gateway name, which is displayed only in *SmartPTT Radioserver Configurator*.

**Gateway Address:Port:** IP address and port of the XRT Gateway.

**Pool IDs:** It is recommended to use default values. The values must correspond to the range of IDs set in the XRT Gateway settings (**Pool ID**).

**Username and Password:** Used for authentication with the gateway and must equal the corresponding values in the XRT Gateway settings:



The screenshot shows a 'User Details' configuration window. The 'Username' field contains the text 'public'. The 'Password' field is masked with ten dots. Below these fields, 'Max Talk Paths' is set to '10'. There are two checkboxes: 'Billing Enabled' is unchecked, and 'Network Wide All Call (NWAC) Enabled' is checked. Under the 'Group Talk Paths' section, the 'Group ID' field contains '1001,1002'. Under the 'Private Talk Paths' section, the 'Console User ID' field contains '100'. At the bottom of the window are three buttons: 'New', 'Save', and 'Delete'.

**TX Time-Out Timer, s:** Time period during which the radio can transmit without interruptions. After this time is over, the transmission is interrupted.

**Group Call Hang Time, ms:** Time during which the channel is reserved for a group call after the end of transmission. During the timeout, only the participants of the talkgroup can transmit. This parameter should match the same parameter set in the XRC Controller.

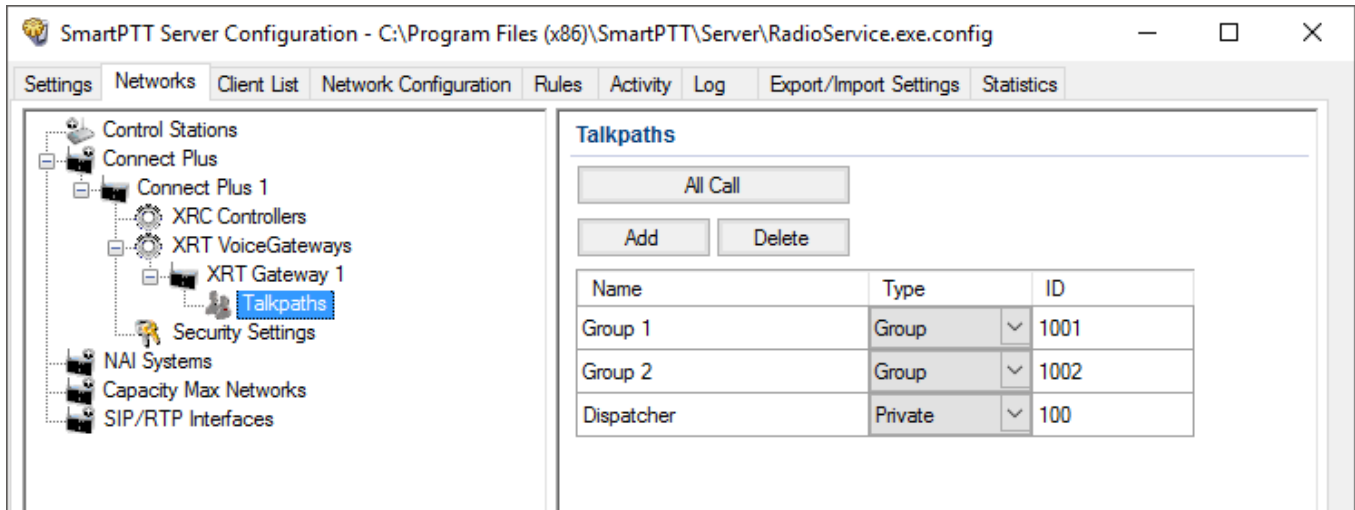
**Private Call Hang Time, ms:** Time during which the channel is reserved for a private call after the end of transmission. During the timeout, only the participants of the private call can transmit. This parameter should match the same parameter set in the XRC Controller.

**Emergency Call Hang Time, ms:** Time during which the channel is reserved for an emergency call after the end of transmission. During the timeout only the participants of the talkgroup can transmit. This parameter should match the same parameter set in the XRC Controller.

The next step is to add talk paths. They are necessary for voice communication. For each talkgroup or/and dispatcher add a talk path. This can be done in the **Talk Paths** window. Group IDs should match the IDs set in the **Group ID** field in the XRT Gateway settings (see above). If the **Group ID** field is empty in the XRT Gateway settings, the user should have permission for any Group Talk Path that it validly registers with the XRT 9000.



Dispatcher ID should match the ID set in the **Console User ID** in the XRT Gateway settings (see above).



#### NOTE

When adding talk paths make sure that talk paths with the same identifiers are specified in the XRT Gateway settings.

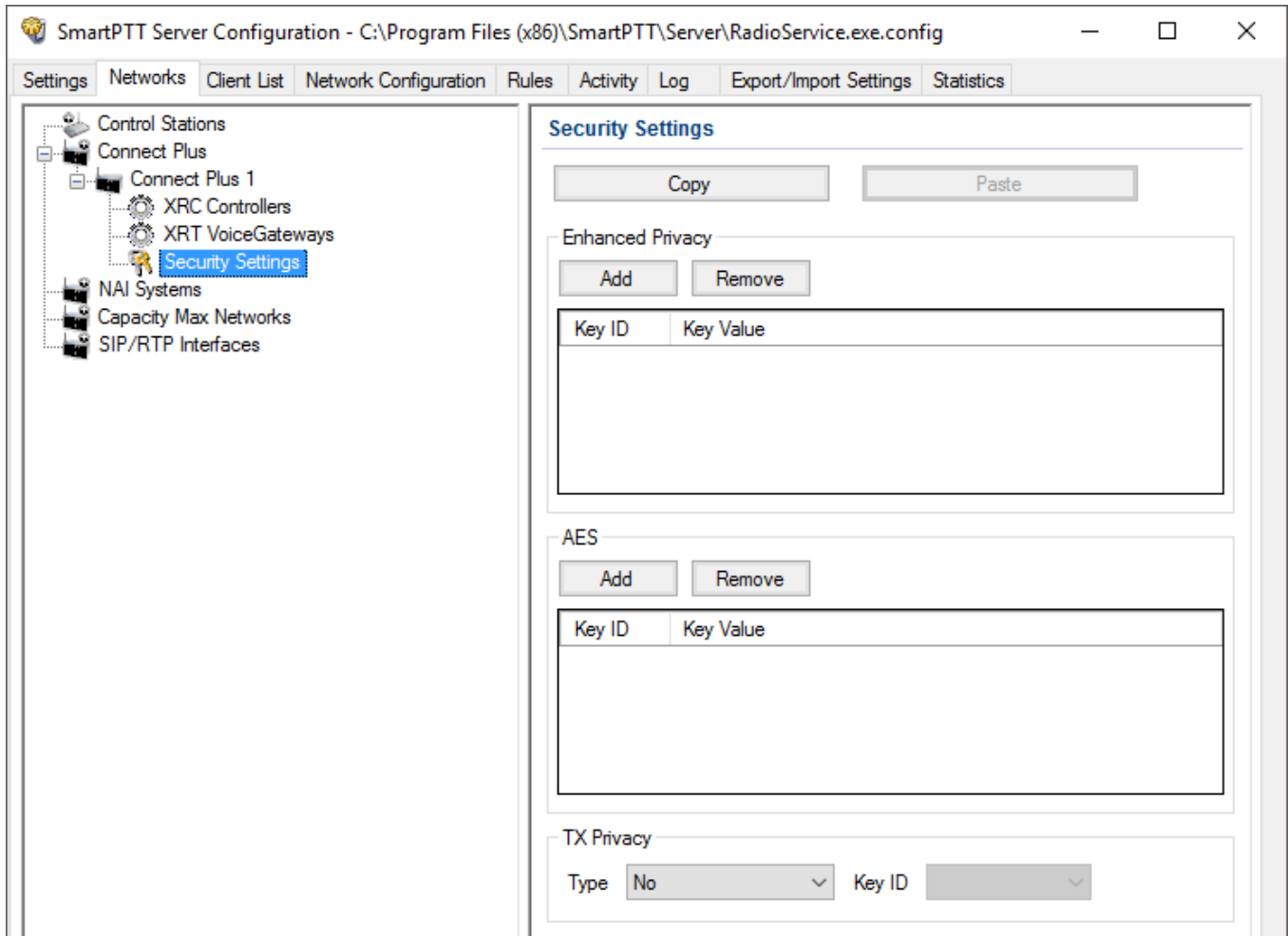
## 2.2.4 Security Settings

Connect Plus supports two types of privacy mechanisms – Enhanced and Advanced Encryption Standard (AES).

The Enhanced Privacy utilizes Motorola proprietary algorithms and therefore is not interoperable with other vendor's privacy offerings. The Enhanced Privacy provides high level of protection by means of 40-bit key length and supports multiple keys in a radio.

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST). The AES feature supports 256-bit key length, unlike Enhanced Privacy. Similar to Enhanced Privacy, the AES also supports multiple keys. For AES encryption a special license is required.

The **Security Settings** window allows you to specify the encryption keys for incoming and outgoing traffic on the digital channel.



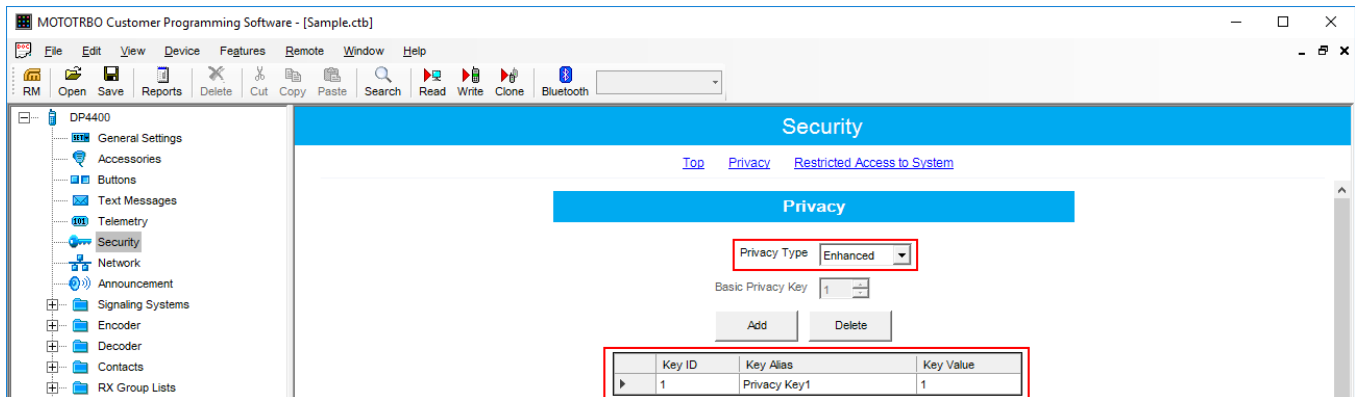
**Copy:** Copy encryption settings of the channel to the clipboard.

**Paste:** Paste encryption settings of the channel from the clipboard.

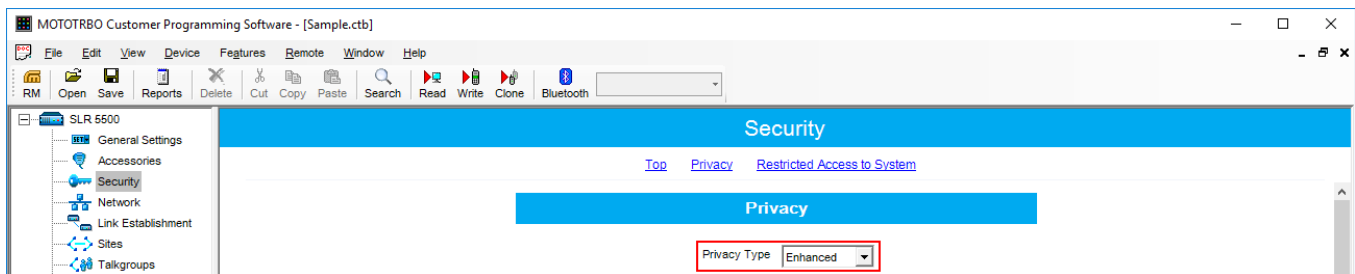
## Enhanced Privacy

To configure **Enhanced Privacy**, follow these steps:

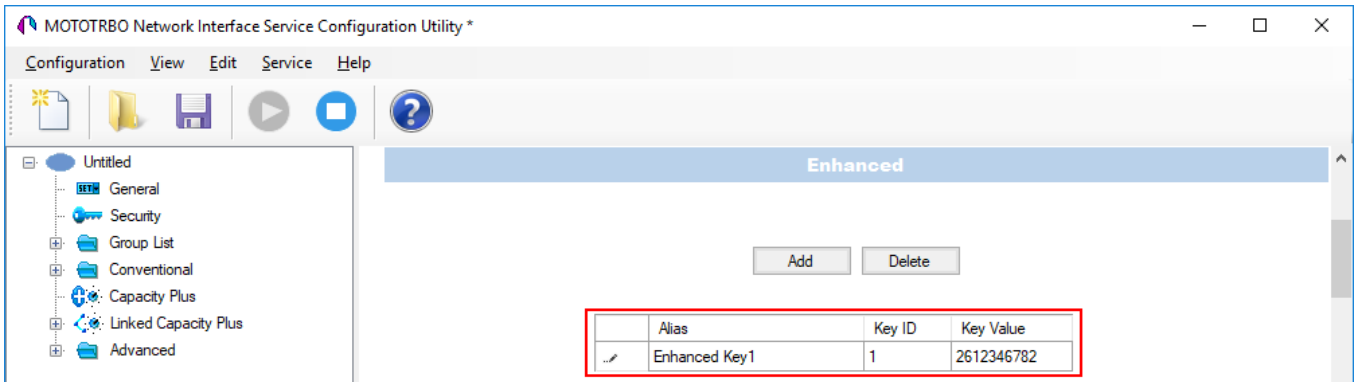
1. Run *MOTOTRBO CPS*.
2. In the **Security** window of the radio settings in *MOTOTRBO CPS* in the **Privacy Type** field select Enhanced and add the enhanced privacy key. Enter its ID and value in the corresponding fields.



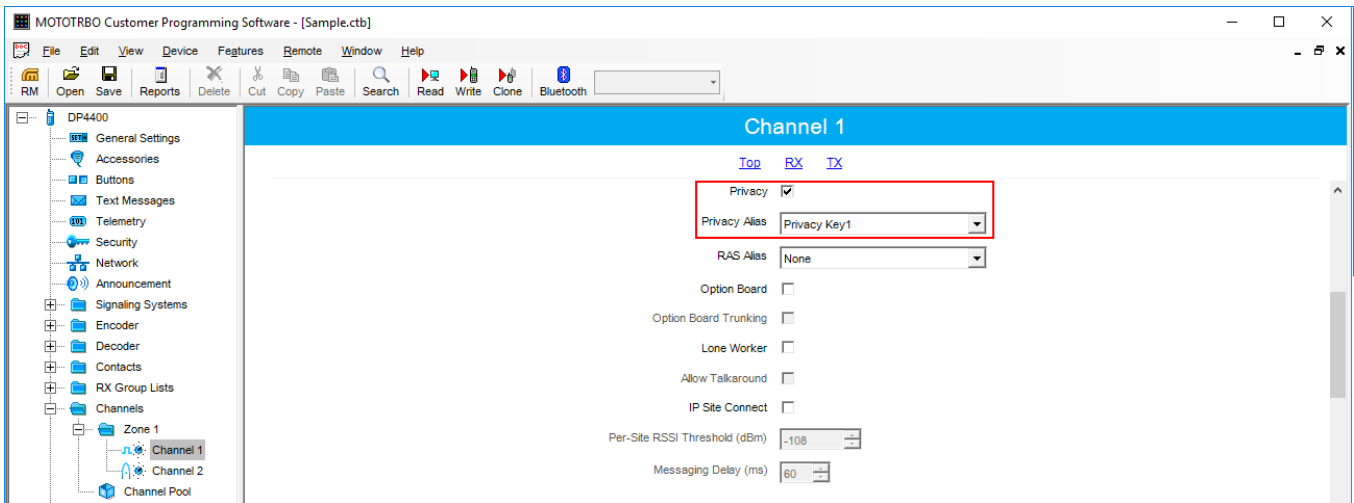
3. In the **Security** window of the repeater settings in *MOTOTRBO CPS* in the **Privacy Type** field select Enhanced.



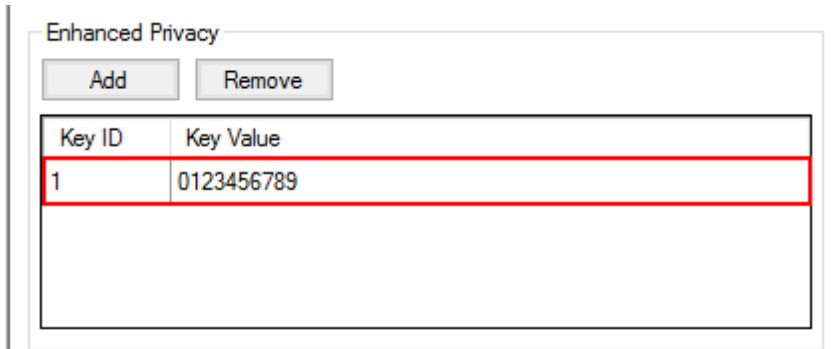
- In the **Security** window of *MOTOTRBO Network Interface Service Configuration Utility* in the **Enhanced** field add the enhanced privacy key. Enter its ID and value in the corresponding fields.



- In the radio settings in *MOTOTRBO CPS* to enable the encryption mode on the required channel select the **Privacy** check box and in the **Privacy Alias** field select the enhanced privacy key for this channel.



- In the **Security Settings** window of *SmartPTT Radioserver Configurator* add an enhanced privacy key for incoming traffic. Enter its ID and value in the corresponding fields.

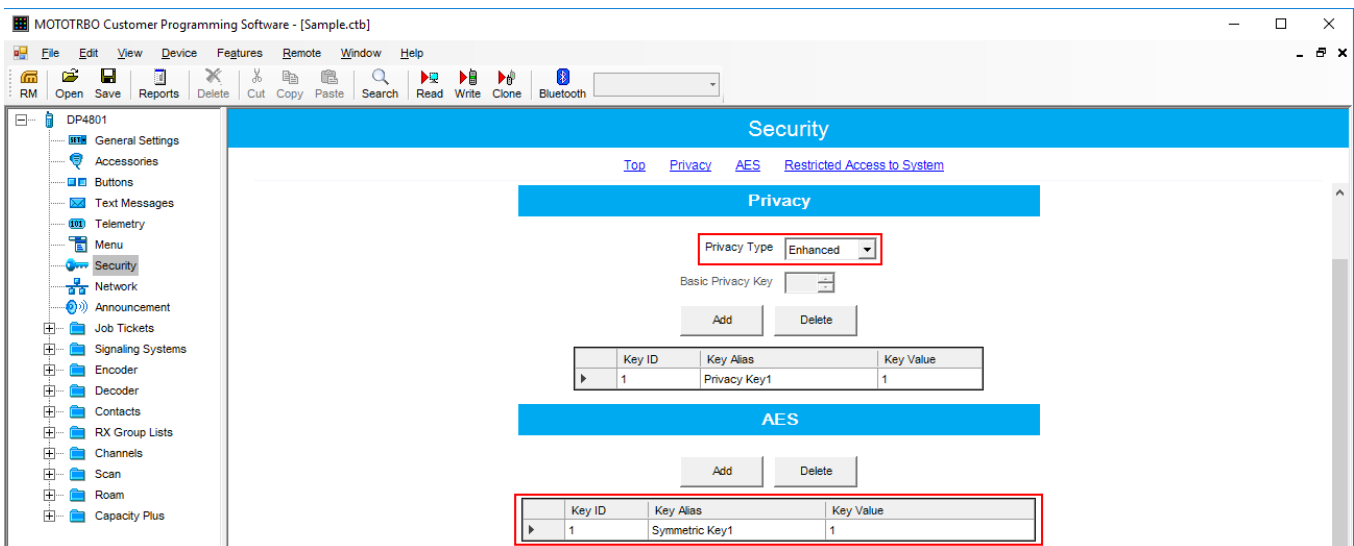


- Click **Save** to save changes.
- Click **Restart** to restart *SmartPTT Radioserver* and apply changes.

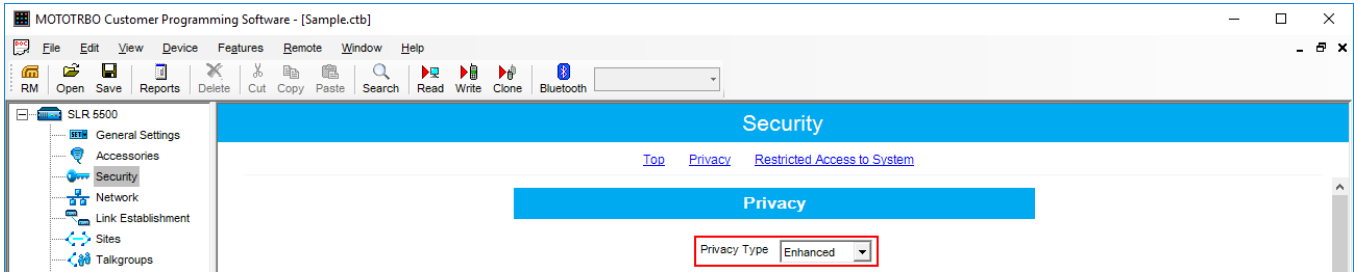
## AES Privacy

To configure the **AES** privacy, follow these steps:

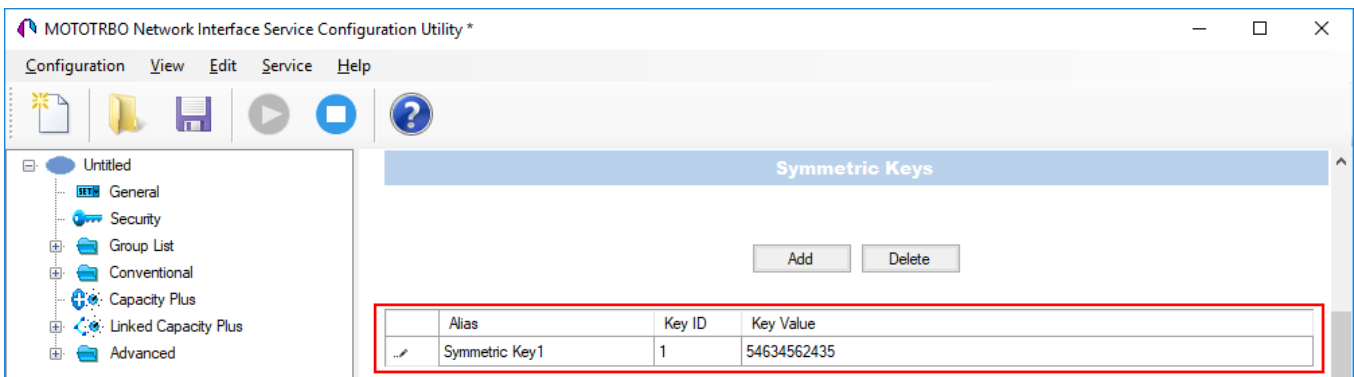
- Run *MOTOTRBO CPS*.
- In the **Security** window of the radio settings in *MOTOTRBO CPS* in the **Privacy Type** field select Enhanced and add the AES privacy key. Enter its ID and value in the corresponding fields.



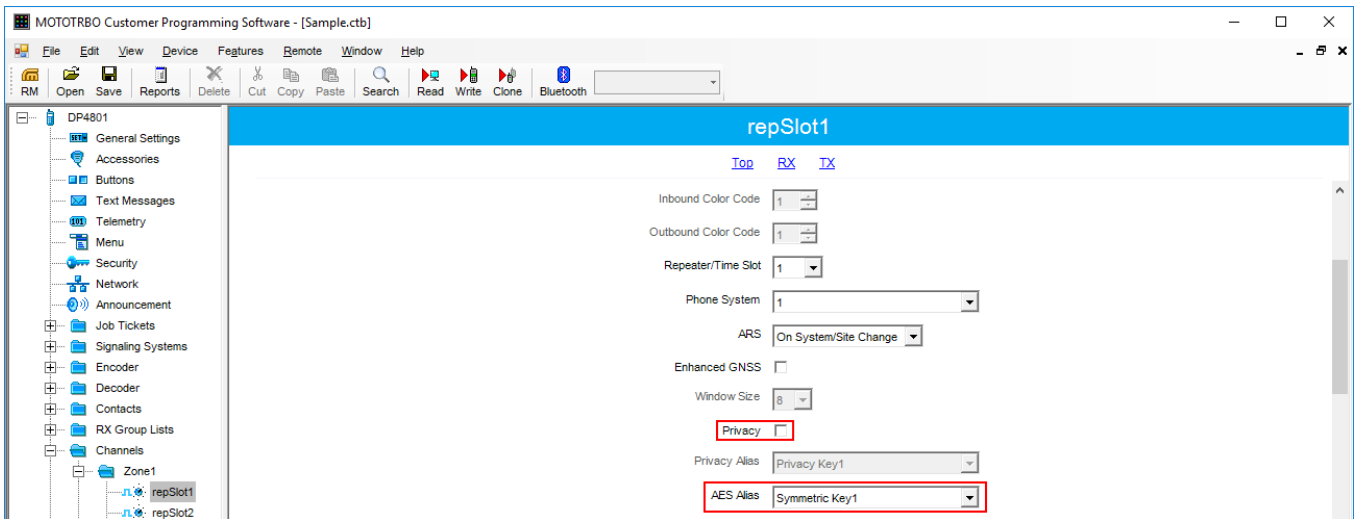
- In the **Security** window of the repeater settings in *MOTOTRBO CPS* in the **Privacy Type** field select **Enhanced**.



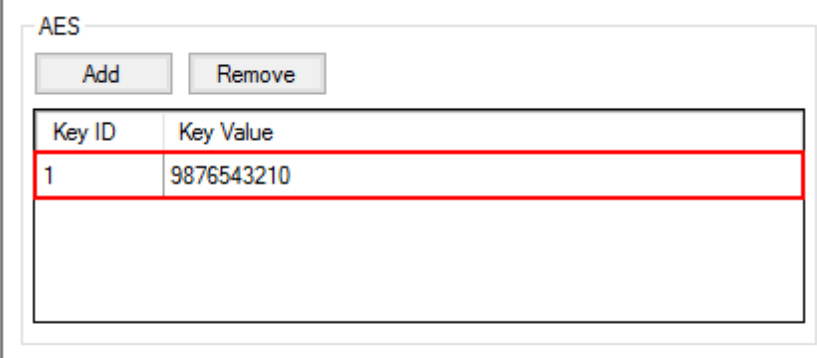
- In the **Security** window of MNIS in the **Symmetric Keys** field add the AES symmetric privacy key. Enter its ID and value in the corresponding fields.



- In the radio settings in *MOTOTRBO CPS* to enable the AES encryption mode on the required channel clear the **Privacy** check box and in the **AES Alias** field select the AES privacy key.





6. In the **Security Settings** window of *SmartPTT Radioserver Configurator* add an AES privacy key for incoming traffic. Enter its ID and value in the corresponding fields.



Key ID	Key Value
1	9876543210

**NOTE**

Key ID and Key Value must match the values set in the radio settings in the Radio Management program and in MOTOTRBO Network Interface Service Configuration Utility. If the values in the Key ID fields are the same, but the values in the Key Value fields do not match, the receiving side hears only a distorted voice. If the key identifier of the transmitting side does not coincide with one of the key identifiers in the list of the receiving side, then transfer to the receiving party will not be heard.

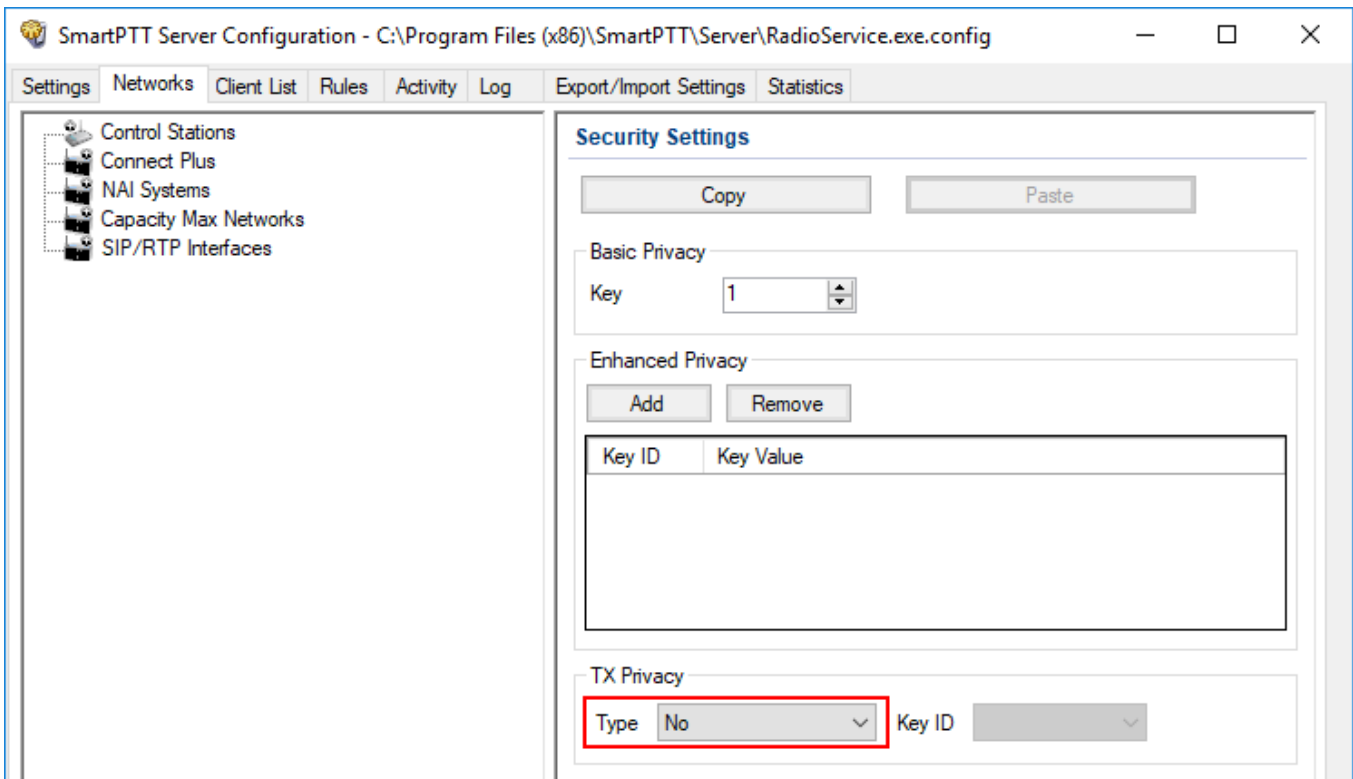
7. Click **Save**  to save changes.
8. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

**TX Privacy**

TX Privacy is used for selecting an encryption mode for outgoing traffic on the side of *SmartPTT Dispatcher*.

To configure the TX Privacy for a Connect Plus system, follow these steps:


1. In the **TX Privacy** area, from the **Type** list select the desired encryption type:



- Select *No* if encryption of outbound traffic from the radioserver is not required.
- Select *Enhanced* if you want to use enhanced encryption for outgoing traffic from the radioserver. Use the Key ID you specified in the **Enhanced Privacy** area.
- *AES license is required:* Select *AES (Legacy Key)* if you want to use AES (*Legacy Key*) encryption for outgoing traffic from the radioserver. Use the Key ID you specified in the **AES** area.
- *AES license is required:* Select *AES (Symmetric Key)* if you want to use AES (*Symmetric Key*) encryption for outgoing traffic from the radioserver. Use the Key ID you specified in the **AES** area.

#### NOTE

If from the **Type** field *No* is selected and you have AES encryption for incoming traffic configured, AES (*Symmetric Key*) is used for incoming traffic by default.

2. Click **Save**  to save changes.



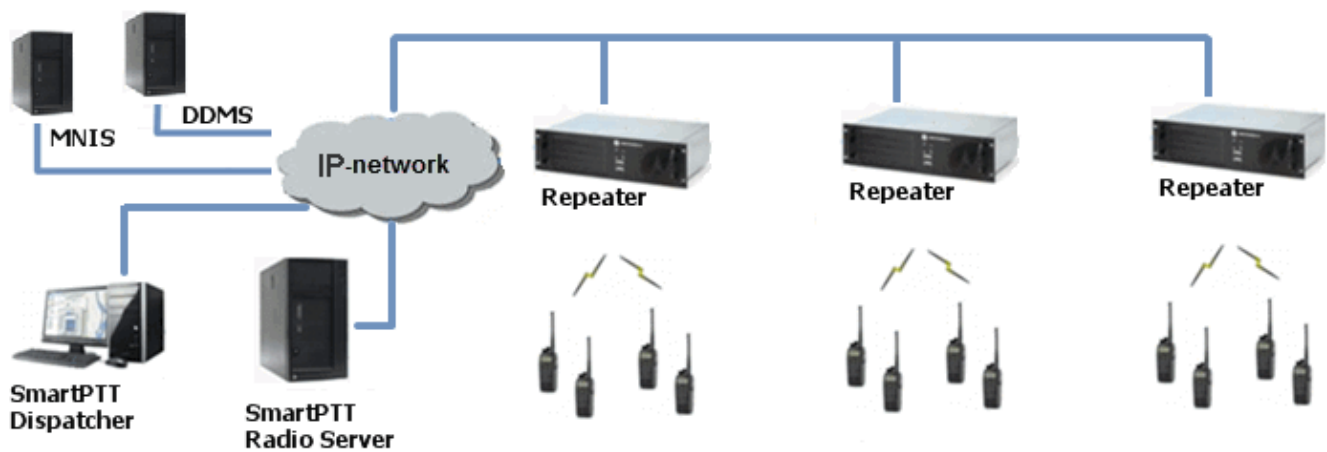
3. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

## 2.3 NAI Systems

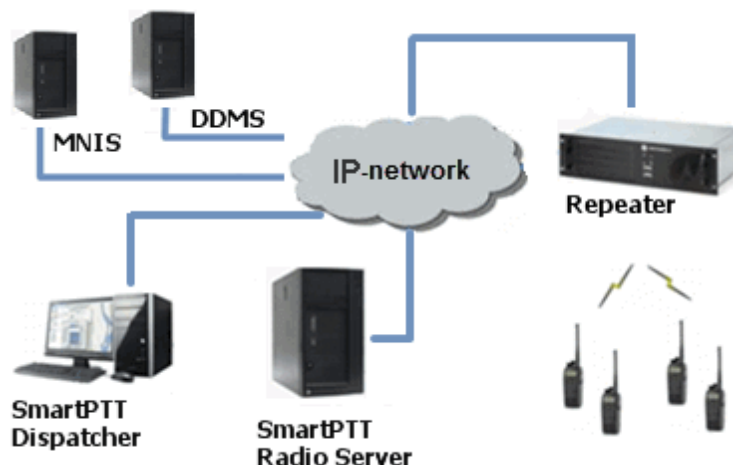
SmartPTT supports MOTOTRBO Network Application Interface (NAI) protocol for networks such as IP Site Connect, Extended Range Direct Mode, Capacity Plus, and Linked Capacity Plus. NAI network configuration uses this protocol for voice, data and monitoring data transmission.

Currently, you can configure four network types with the NAI protocol:

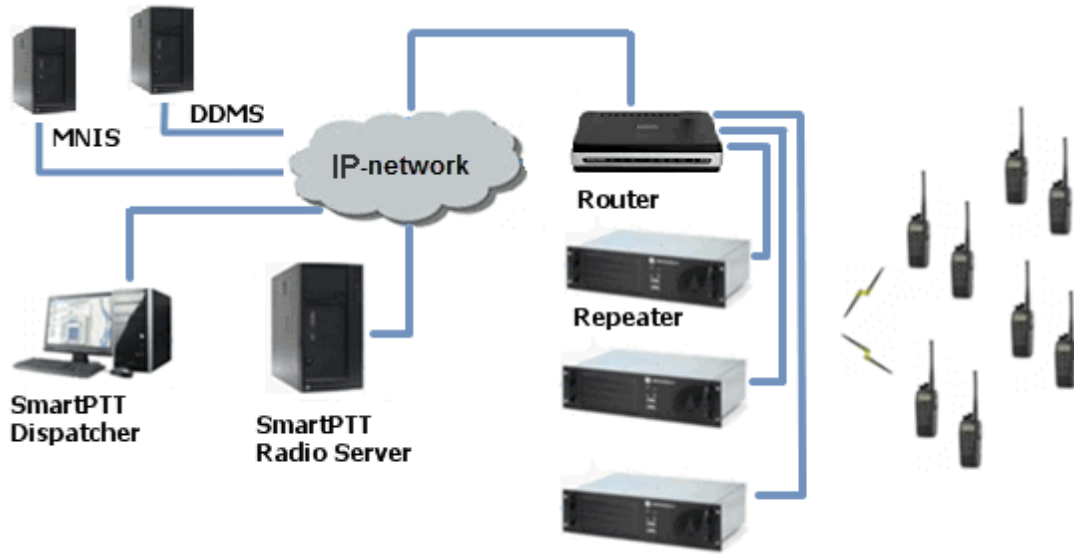
- NAI - IP Site Connect topology:



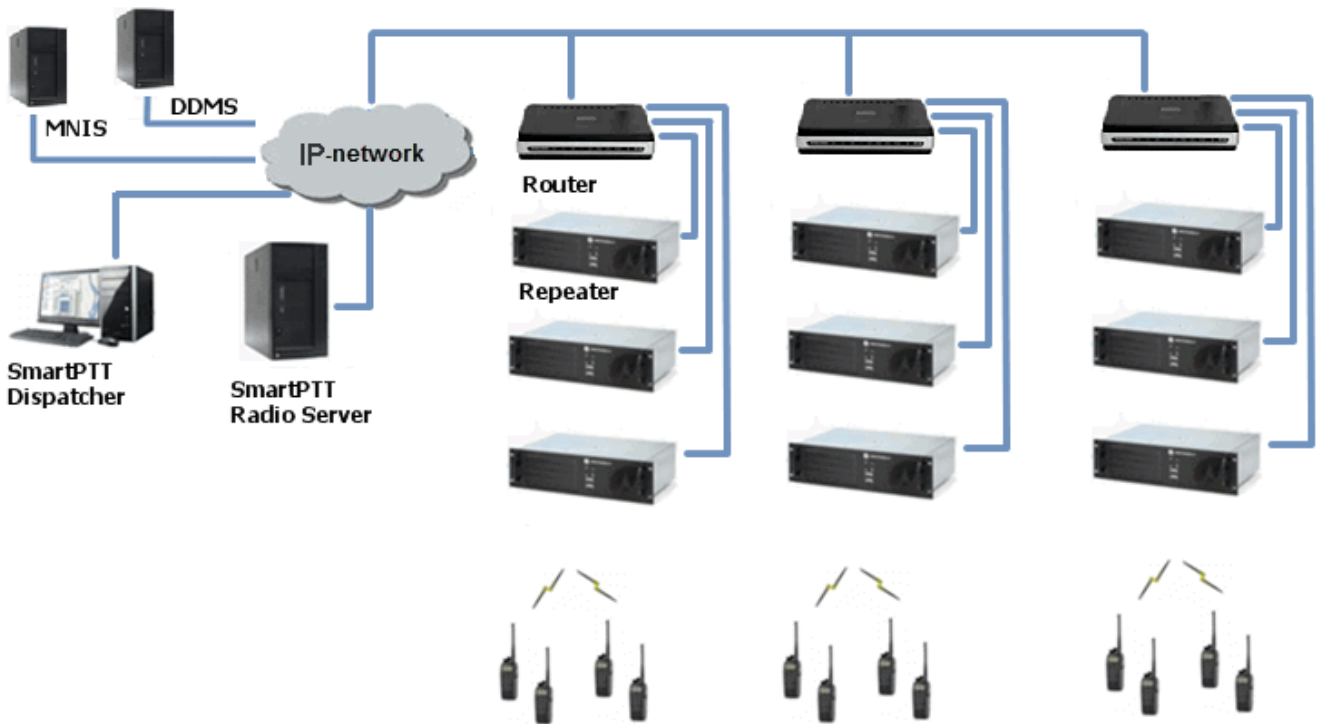
- NAI - Extended Range Direct Mode topology:



- NAI - Capacity Plus topology:



- NAI - Linked Capacity Plus topology:



**NOTE**  
You can install SmartPTT Radioserver, DDMS and MNIS on the same PC.

The MOTOTRBO Network Interface Service (MNIS) lets you transmit data (text messages, GPS, telemetry, etc.) without control stations. MNIS connects to the repeater system over IP and uses it to transmit and receive data packets.

To use the service, you need to install and configure *MOTOTRBO Network Interface Service Configuration Utility*.

**NOTE**

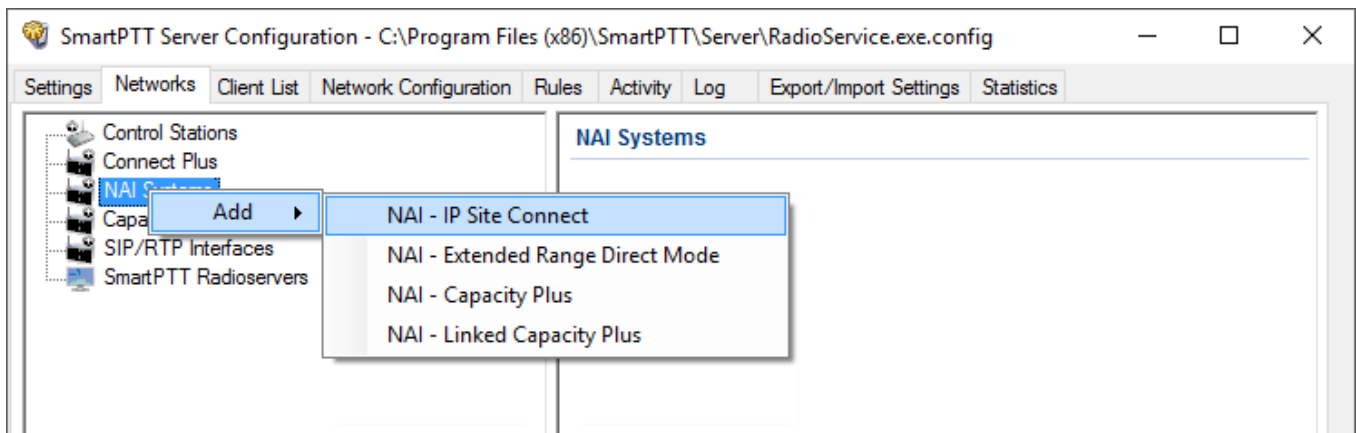
MNIS allows data transmission only. It does not support transmission of voice calls and CSBK commands (Radio Check, Call Alert commands and so on).

The Device Discovery and Mobility Service (DDMS) is a service that monitors the presence of ARS capable radio units and reports their parameters (IP address, Radio ID, etc.) to interested applications, such as SmartPTT Radioserver and MNIS.

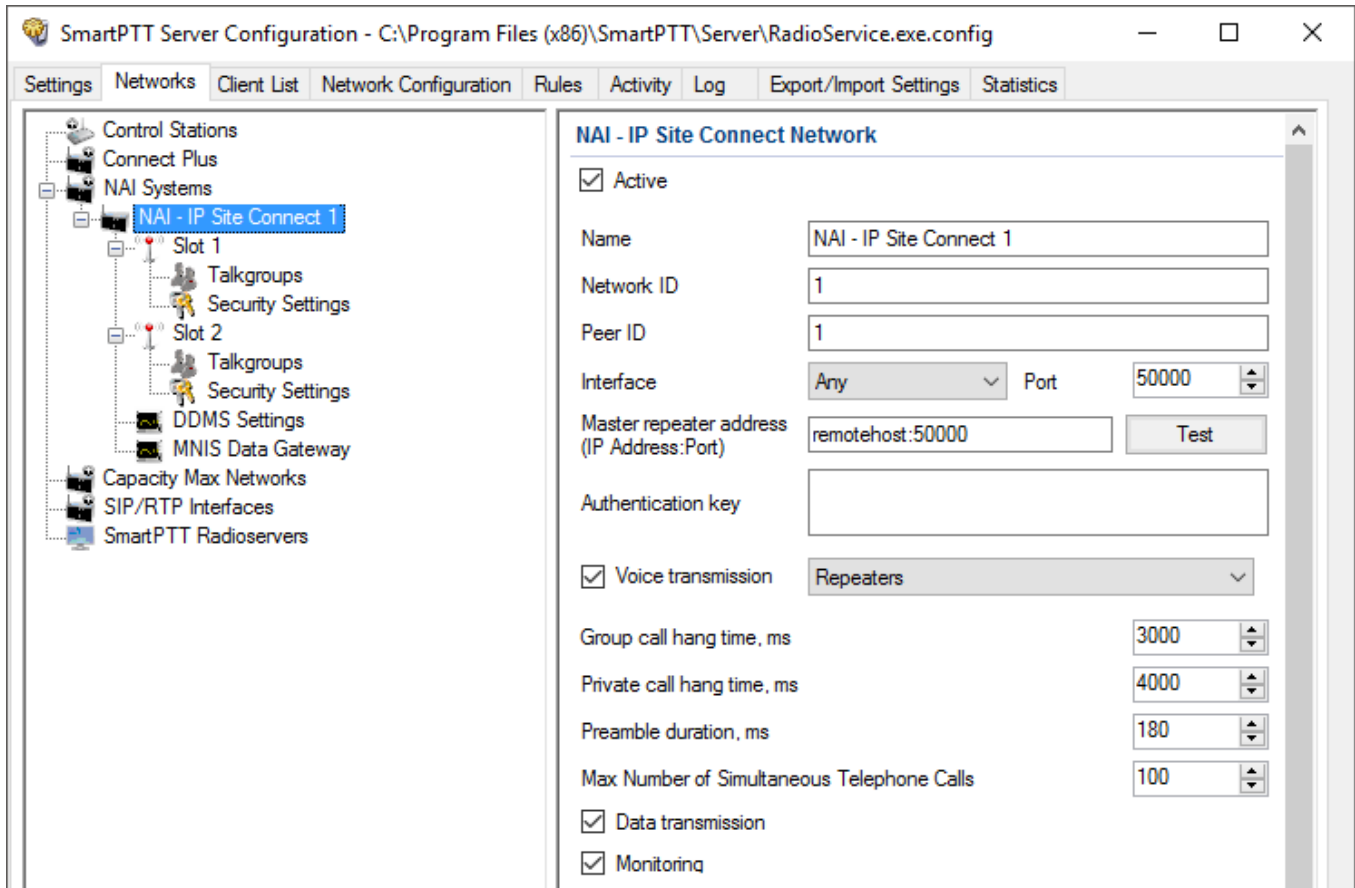
To use the service, you need to install and configure *MOTOTRBO DDMS*.

## 2.3.1 Adding and Configuring NAI Systems

To add a NAI system, on the **Networks** tab of SmartPTT Radioserver Configurator, right-click **NAI Systems**, point to **Add**, and select the desired network type (NAI - IP Site Connect, NAI - Extended Range Direct Mode, NAI - Capacity Plus or NAI - Linked Capacity Plus):



A new pane with network parameters opens. The network parameters differ depending on the selected network type:



**Active:** Activates a network.

**Name:** Name of the created system.

**Network ID:** Unique ID of the network. The network ID must not match any ID of the other SmartPTT Radioserver networks.

**Peer ID:** Unique ID of the radioserver in the network. This ID must not match any of the other repeater IDs in this network.

**Interface:** Local interface of the radioserver. The radioserver plays the role of a software peer.

**Port:** Port number of the radioserver. It should differ from the corresponding ports in other networks.

**Master repeater address (IP Address:Port):** IP address and port number of the network Master repeater. Click **Test** to check connection between the radioserver and the Master repeater.

**Authentication key:** Repeater authorization key (should be equal to the **Authentication key** in the repeater settings in *MOTOTRBO CPS*).

**Voice transmission:** Voice transmission can be carried by using repeaters or control stations.

**NOTE**

To activate **Voice transmission**, install the correspondence license. For more information on how to install licenses, see [Licenses](#).

To transmit voice via control stations, configure control station parameters and profiles for making private calls. To transmit voice via repeaters, configure virtual control station channels and talkgroups of the channel. The number of channels depends on the network type. To ensure data packets transmission over the network, configure the DDMS and MNIS services.

**Group call hang time:** Time during which the repeater reserves the channel for a group call after the end of transmission. During the timeout, only the participants of the talkgroup can transmit.

**Private call hang time:** Time during which the repeater reserves the channel for a private call after the end of transmission. During the timeout, only the participants of the private call can transmit.

**TX preamble duration (ms):** Duration of TX preamble. Increasing of preamble duration makes a message longer. It reduces the probability of missing the message by a scanning in battery save mode receiving radio. Increasing of preamble reduces the amount of data transmitted on the channel. Preamble duration must not exceed *8040 ms*.

**Max number of simultaneous telephone calls:** Sets the limit on the number of simultaneous telephone calls per system. The parameter is not applicable to the Extended Range Direct Mode systems.

**Data transmission:** Enables data transmission in the network.

**NOTE**

To activate **Data transmission**, install the correspondence license. For more information on how to install licenses, see [Licenses](#).

**Monitoring:** Enables monitoring of radio network equipment condition.

When selecting NAI - Linked Capacity Plus network with voice via repeaters, the new section **Site** with the **Site Priority Configuration** table appears:

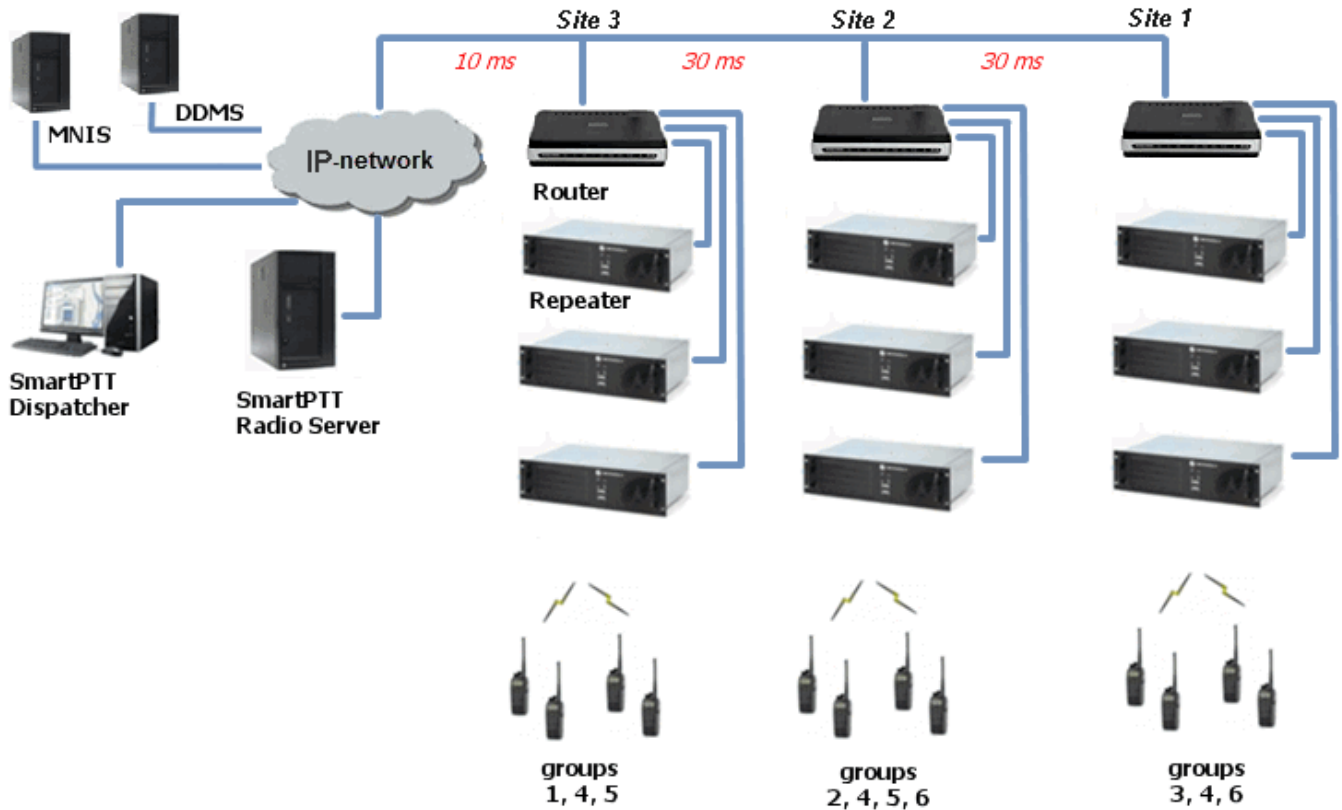
Site	Max Number of Simultaneous Telephone Calls	Priority
Site 1	16	1
Site 2	16	2
Site 3	16	3
Site 4	16	4
Site 5	16	5
Site 6	16	6
Site 7	16	7

**Site:** Name of the site.

**Max number of simultaneous telephone calls:** Sets the limit on the number of simultaneous telephone calls per site.

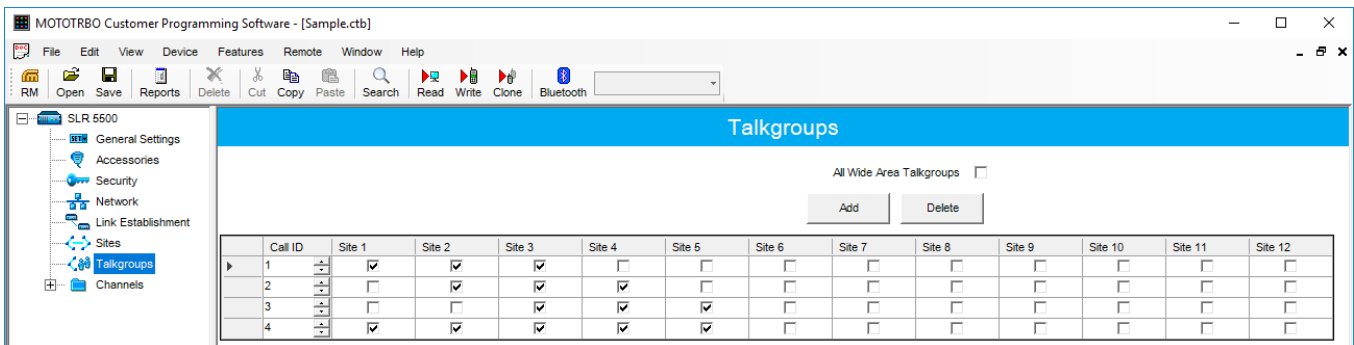
**Priority:** Priorities should be set on the basis of the radioserver proximity to the site. The closer the radioserver to the site, the higher priority it should have. Thus, you will be able to reduce data transmission delay.

The following scheme shows sites location in respect to the radioserver, and distribution of talkgroups on them:



Here, talkgroups 3, 4, 6 are assigned to Site 1; talkgroups 2, 4, 5, 6 – to Site 2; talkgroups 1, 4, and 5 – to Site 3.

The **Talkgroups** tab in repeater *MOTOTRBO CPS* settings allows you to configure group calls as wide area calls on specific sites:



By default, the repeater sends data to Site 1. Then, data goes from Site 1 to other sites. So, if you call to talkgroup 4, the total time delay is 130 ms.

Set up the site priorities so that sites with less time delay have a higher priority. It allows sending data to the nearest site, from which it is distributed to other sites. Ultimately, the total time delay in case of talkgroup 4 reduces up to 70 ms.

If connection with the site of the highest priority fails, the radioserver tries to work through the site of lower priority.

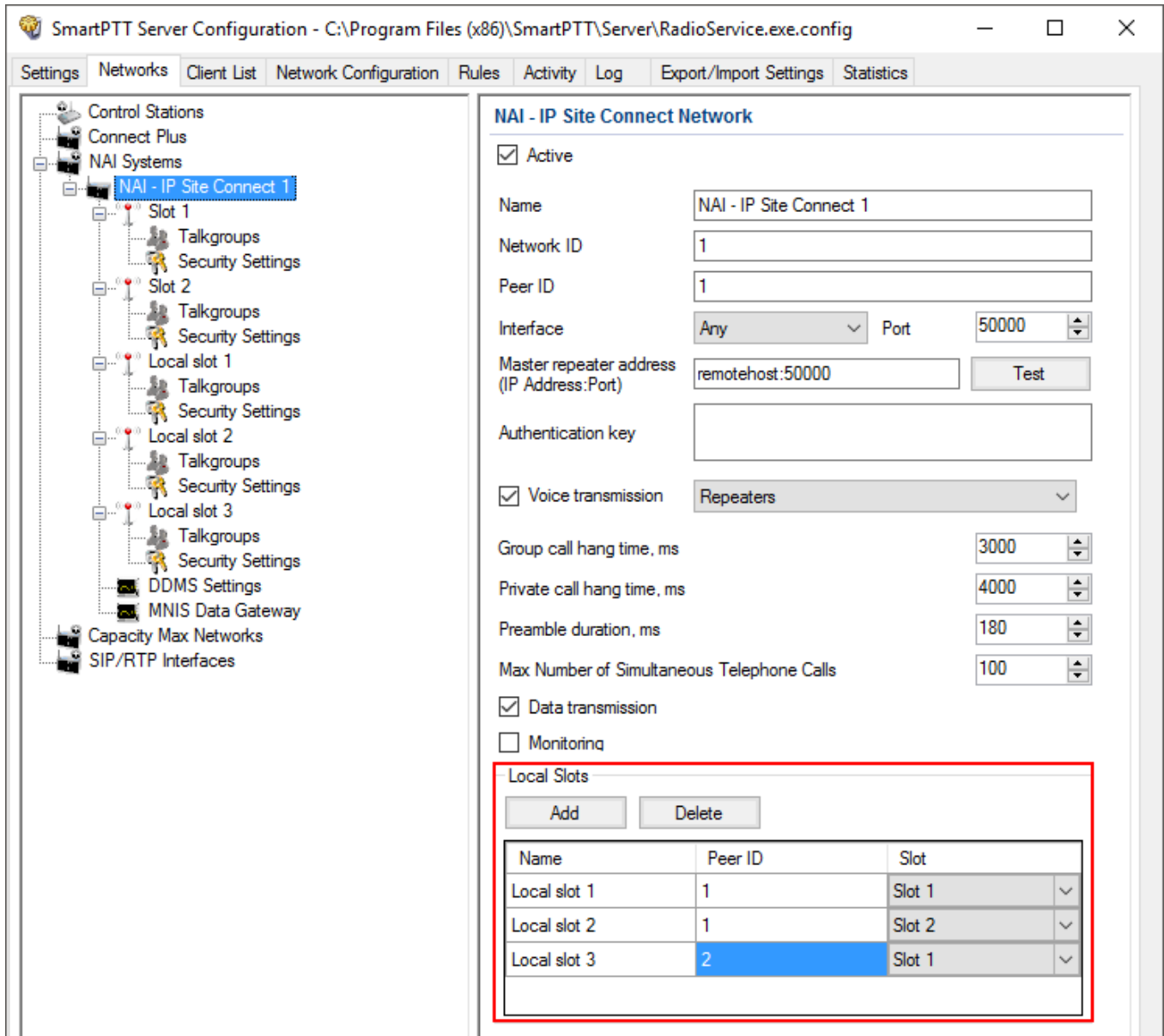
To assign site priority, drag the site name to the desired location or use arrows on the right to the table.

**NOTE**

Talkgroup distribution data is provided by the **Talkgroups** table on each site (repeater settings in *MOTOTRBO CPS*).



When selecting NAI - IP Site Connect with voice via repeaters, the **Local Slots** table appears. Local slots allow multiple communications at one time. To add a local slot, click the **Add** button above the table.



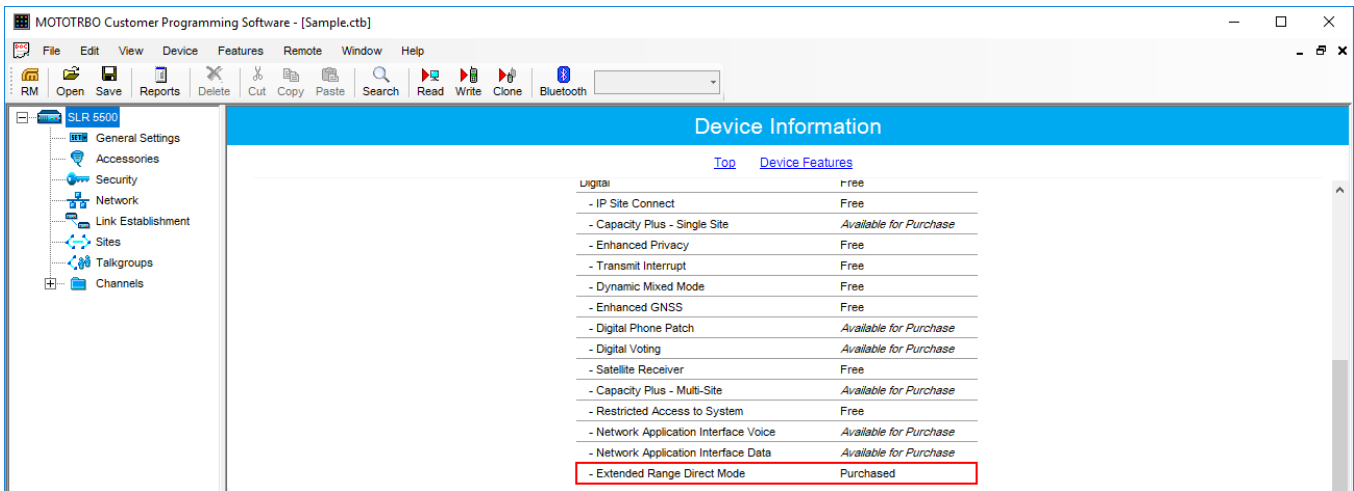
**Name:** Name of a local slot, which will be displayed in SmartPTT Radioserver Configurator and *SmartPTT Dispatcher*.

**Peer ID:** The identifier of a repeater.

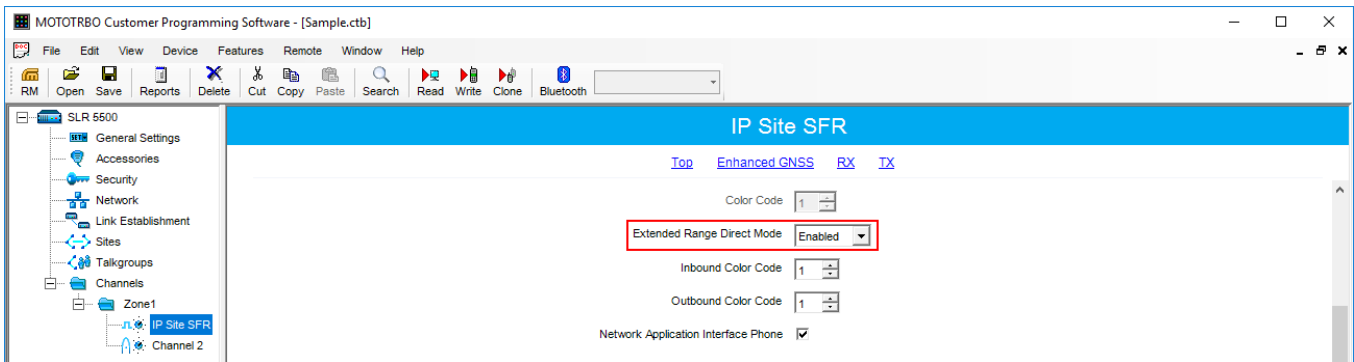
**Slot:** Selection between slots (*Slot 1* or *Slot 2*).

To configure NAI - Extended Range Direct Mode, ensure that the following settings are specified:

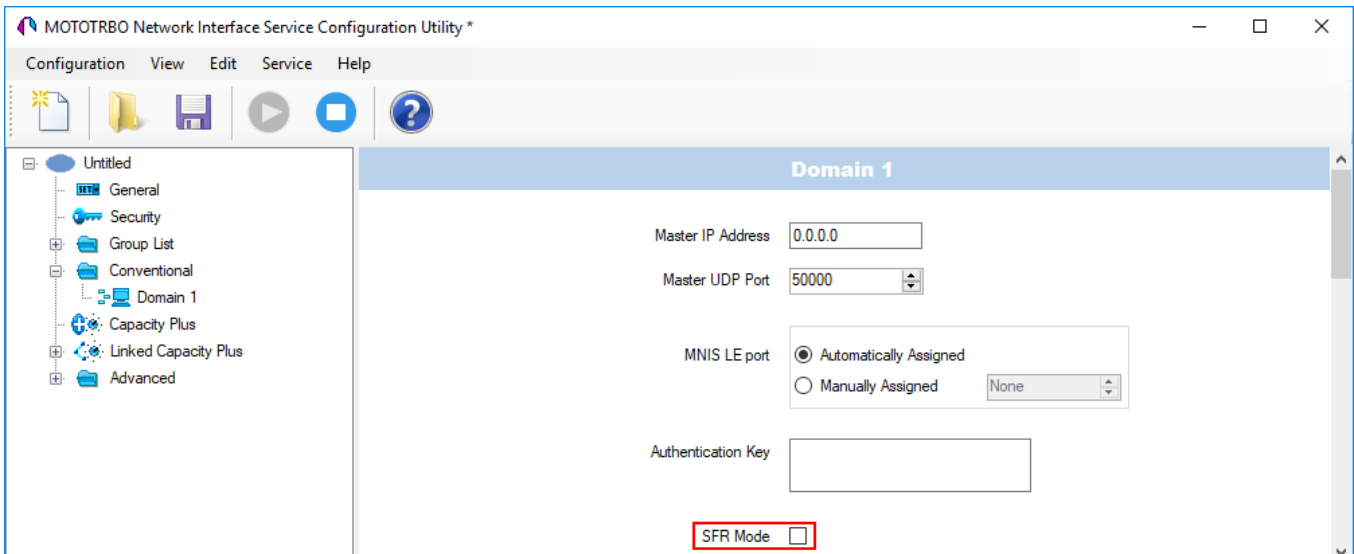
1. The repeater has the corresponding license in MOTOTRBO CPS.



2. Extended Range Direct Mode has the *Enabled* value in MOTOTRBO CPS.



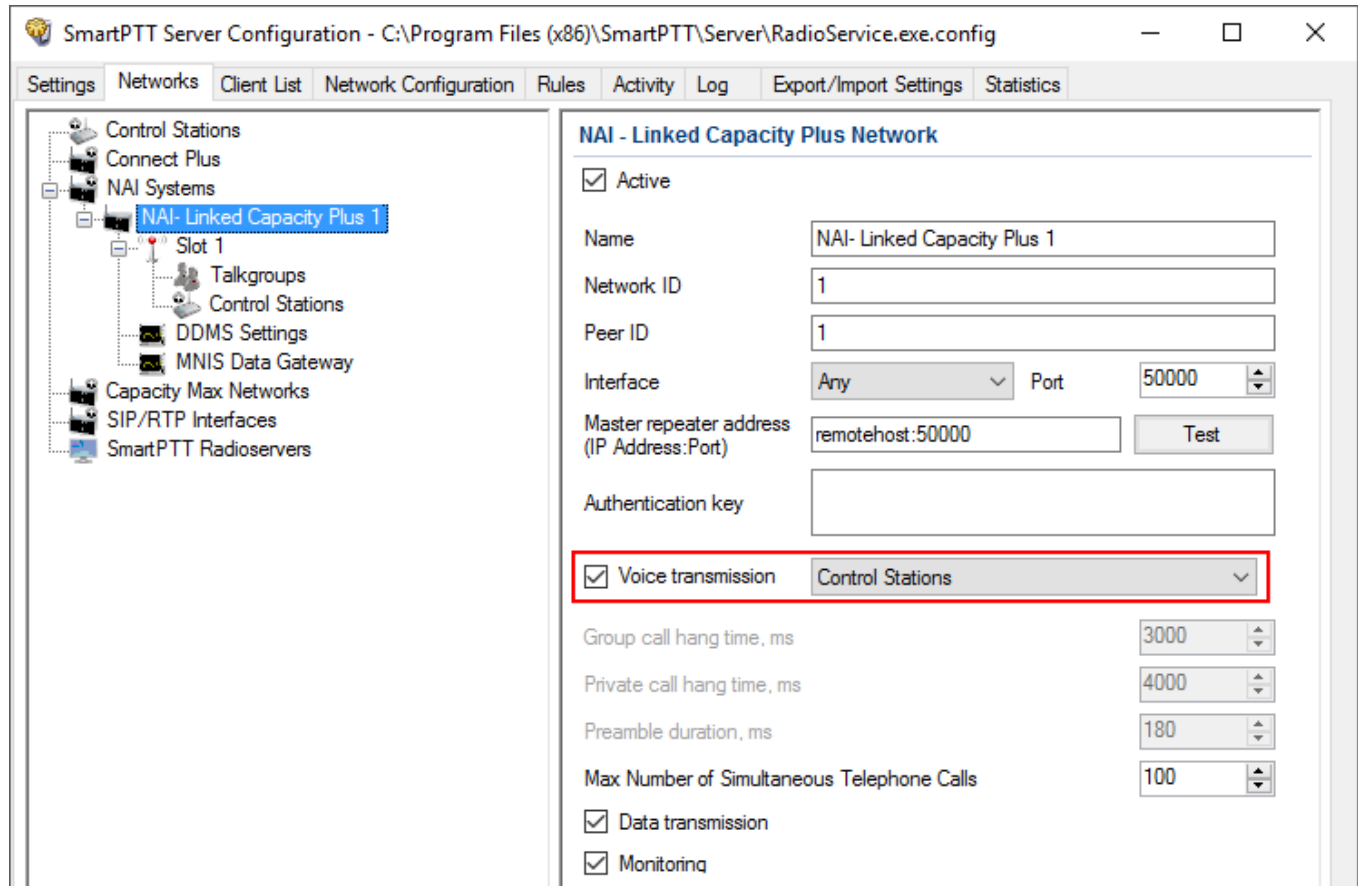
3. The **SFR Mode** check box is selected in the MNIS.



## 2.3.2 Adding and Configuring NAI Control Stations

To transmit voice packets over control station, you need to configure its settings.

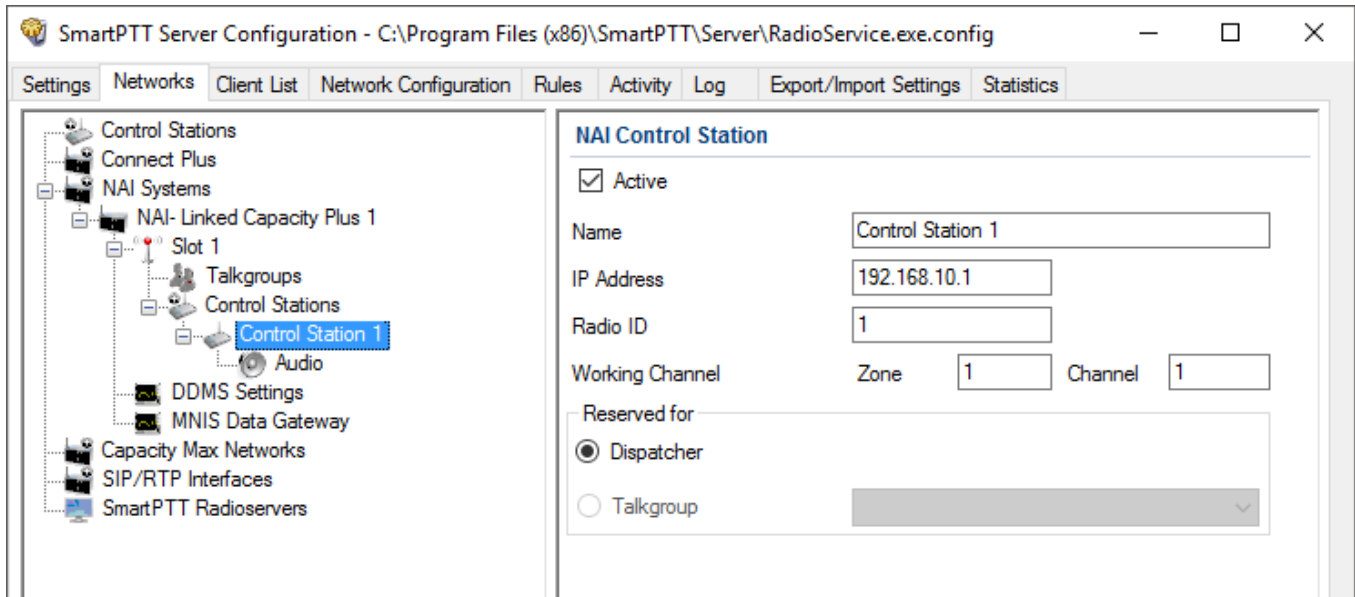
Control station settings become available, when you select voice packet transmission over control stations, not repeaters.



The screenshot displays the SmartPTT Server Configuration interface. The left sidebar shows a tree view with 'NAI - Linked Capacity Plus 1' selected under 'NAI Systems'. The main panel is titled 'NAI - Linked Capacity Plus Network' and contains the following settings:

- Active
- Name: NAI- Linked Capacity Plus 1
- Network ID: 1
- Peer ID: 1
- Interface: Any Port 50000
- Master repeater address (IP Address:Port): remotehost:50000 [Test]
- Authentication key: [Empty]
- Voice transmission: Control Stations (highlighted with a red box)
- Group call hang time, ms: 3000
- Private call hang time, ms: 4000
- Preamble duration, ms: 180
- Max Number of Simultaneous Telephone Calls: 100
- Data transmission
- Monitoring

To configure the control station settings, right-click **Control Station**, point to **Add**, and select **MOTOTRBO control station**. You can also add a remote control station, for more information about a remote control station see [this article](#).



**Active:** Activates a control station.

**Name:** Control station name.

**IP Address:** Local IP address of the control station. The following address format and range are used: (001-223).(000-255).(000-255).(001-253). Users can use any address except 127.x.x.x in the range from 1.x.x.x to 223.x.x.x. We recommend to use the address *192.168.10.1* by default, and in case of conflicts with other network interfaces you should select a different IP address.

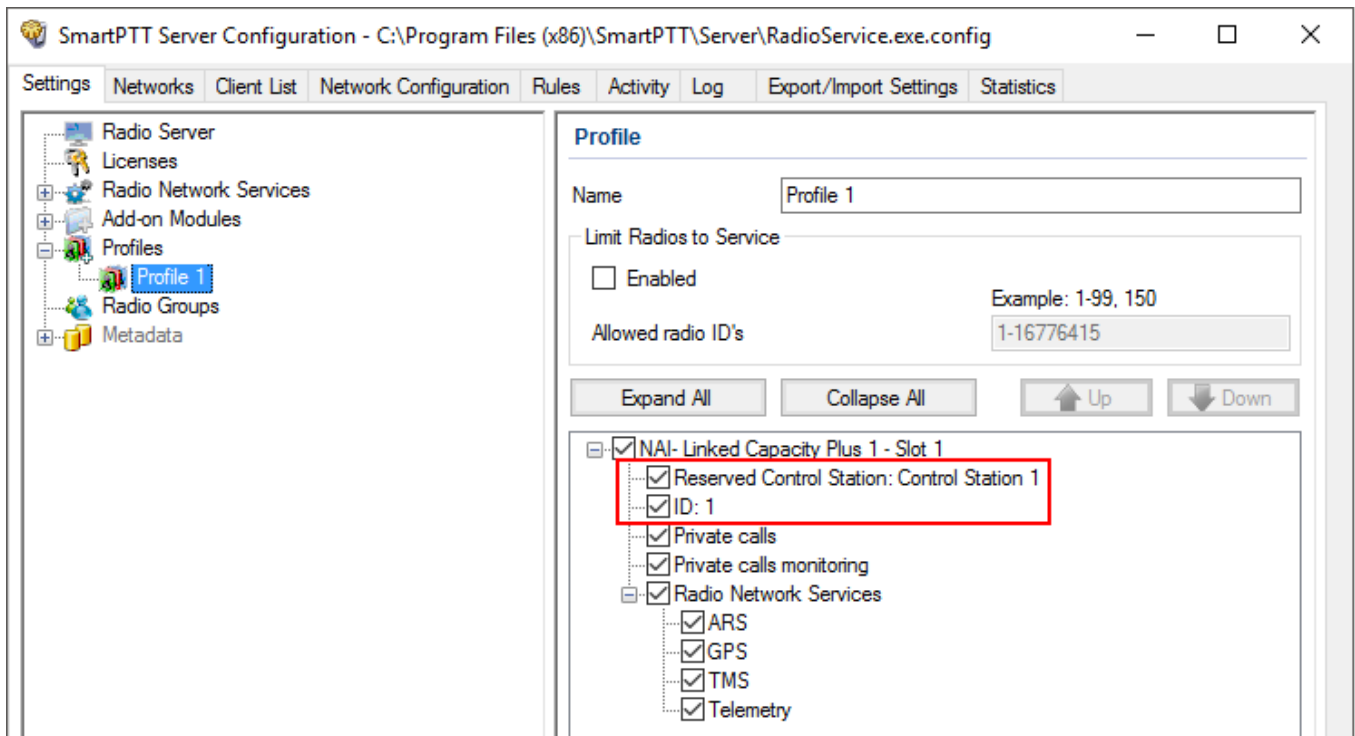
#### NOTE

If two or more control stations are connected to the PC, one of the first three octets of the IP address must be unique for each control station.

**Radio ID:** Unique radio identifier used during communication with it. In the IP Site Connect network, the ID is to be set in the range from 1 to 16776415. In the NAI - Capacity Plus or NAI - Linked Capacity Plus networks, the ID is to be set in the range from 1 to 65535.

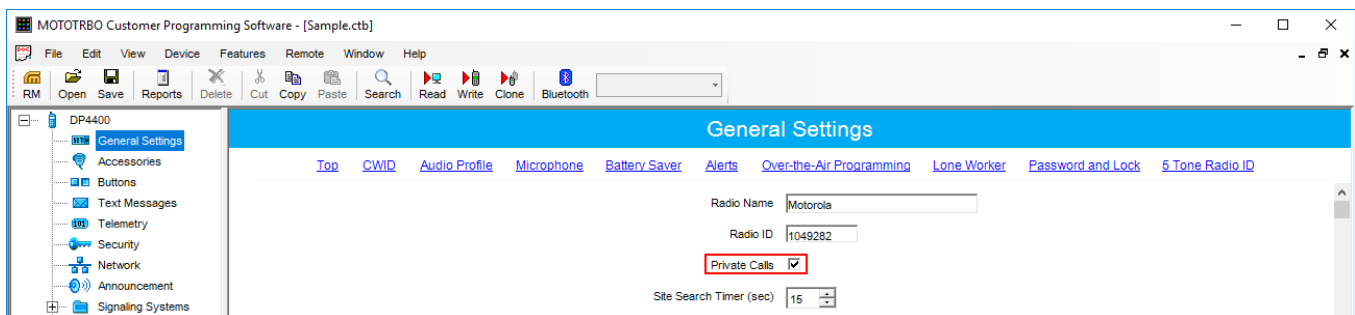
**Working Channel:** Select the channel and the zone to be set at the control station at the radioserver launch.

**Reserved for:** Allows you to define how the control station is to be used. It can be used for private calls (**Dispatcher**) or for group calls (**Talkgroup**). This parameter is available only for NAI - Extended Range Direct Mode, NAI - Linked Capacity Plus and NAI - Capacity Plus networks. You can use one control station per one dispatcher or per one talkgroup. To allow group calls, select **Talkgroup**. At that, the list with added talkgroups becomes enabled. To allow private calls to and from the dispatcher, select **Dispatcher** and add [profiles](#) – one per dispatcher. In the profile, select the reserved control station. At that, **ID** will change and will match **Radio ID** set in the **NAI Control Station** settings.

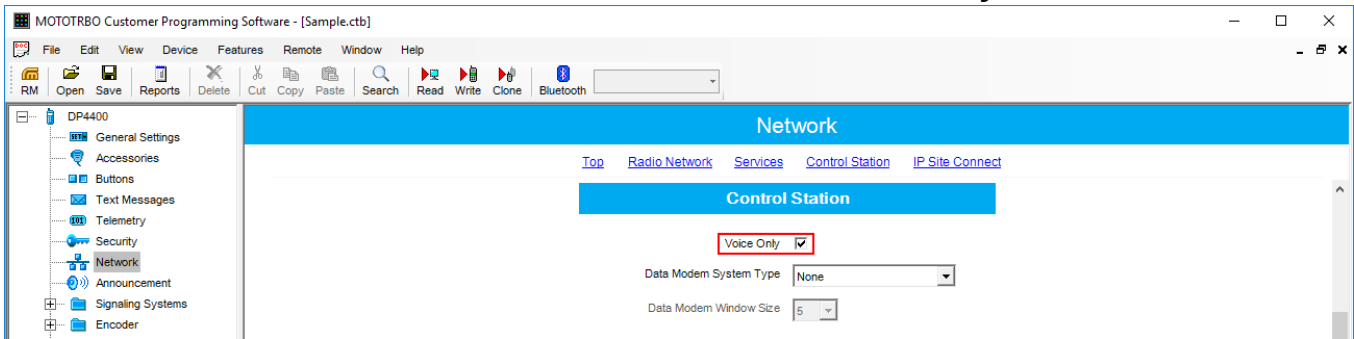


Also, make sure the following settings are made in CPS in control stations' configurations:

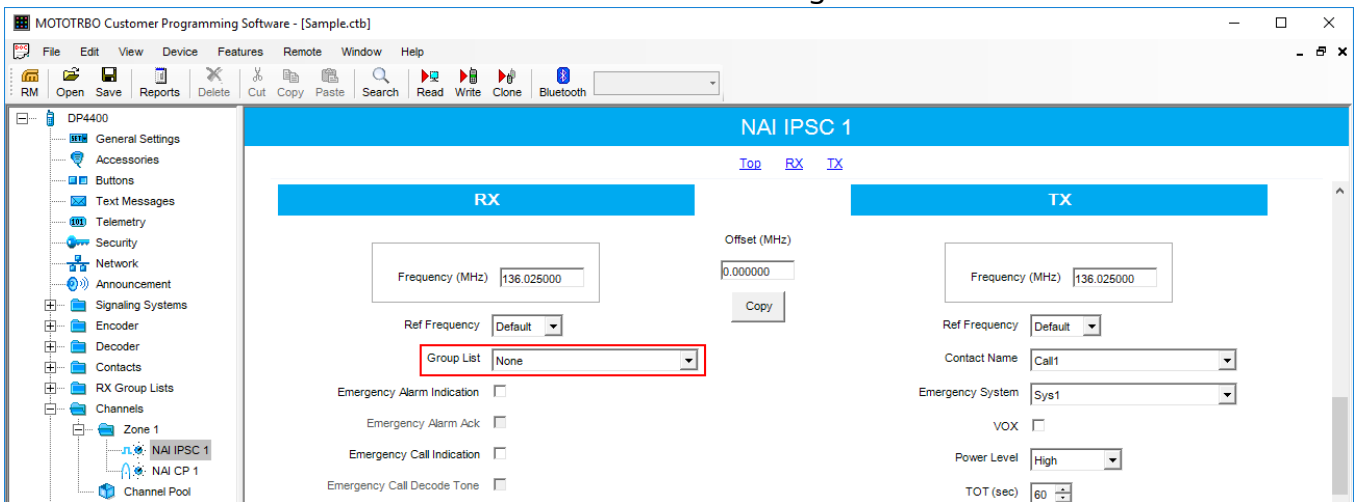
1. When using for talkgroups:
  - In **General Settings**, clear **Private Calls** check box.



- In **Network** under **Control Station** section, select **Voice Only**.

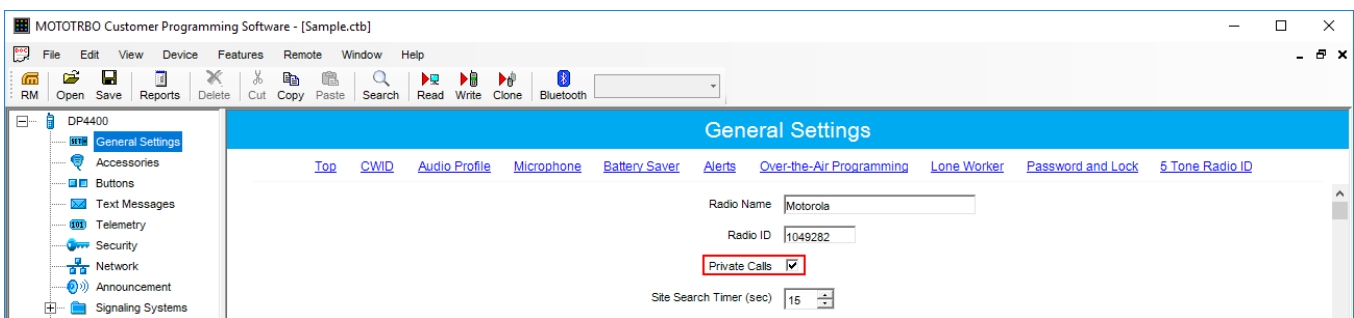


- In the **Channel** settings, in **RX Group List**, select the talkgroup, for which the control station is reserved in SmartPTT Radioserver Configurator.

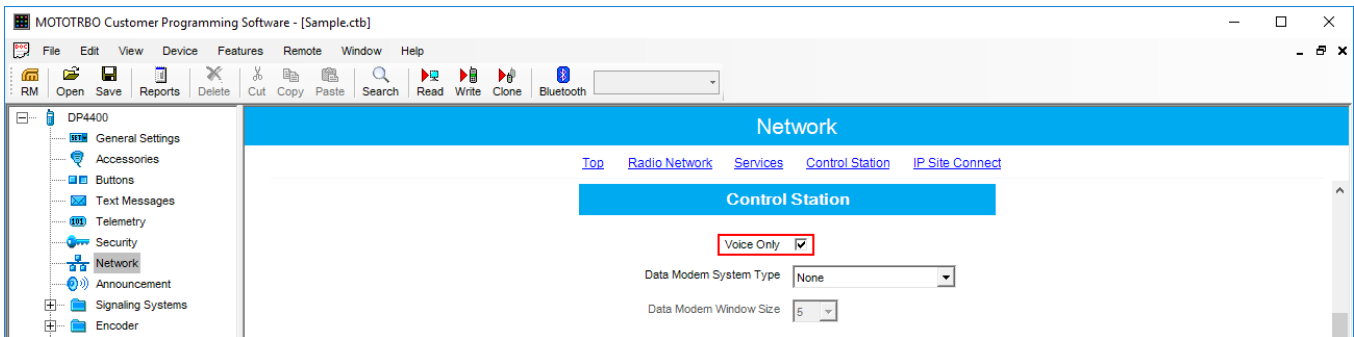


2. When using for dispatcher:

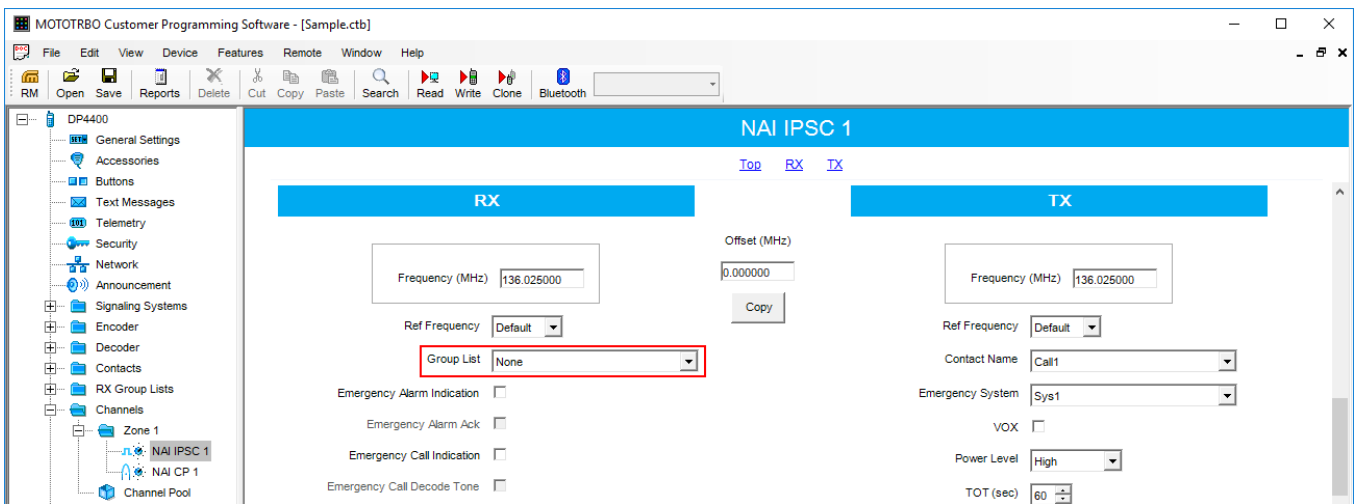
- In **General Settings**, select **Private Calls**.



- In **Network** under **Control Station** section, select **Voice Only**.



- In the **Channel** settings, in **RX Group List** select *None*.

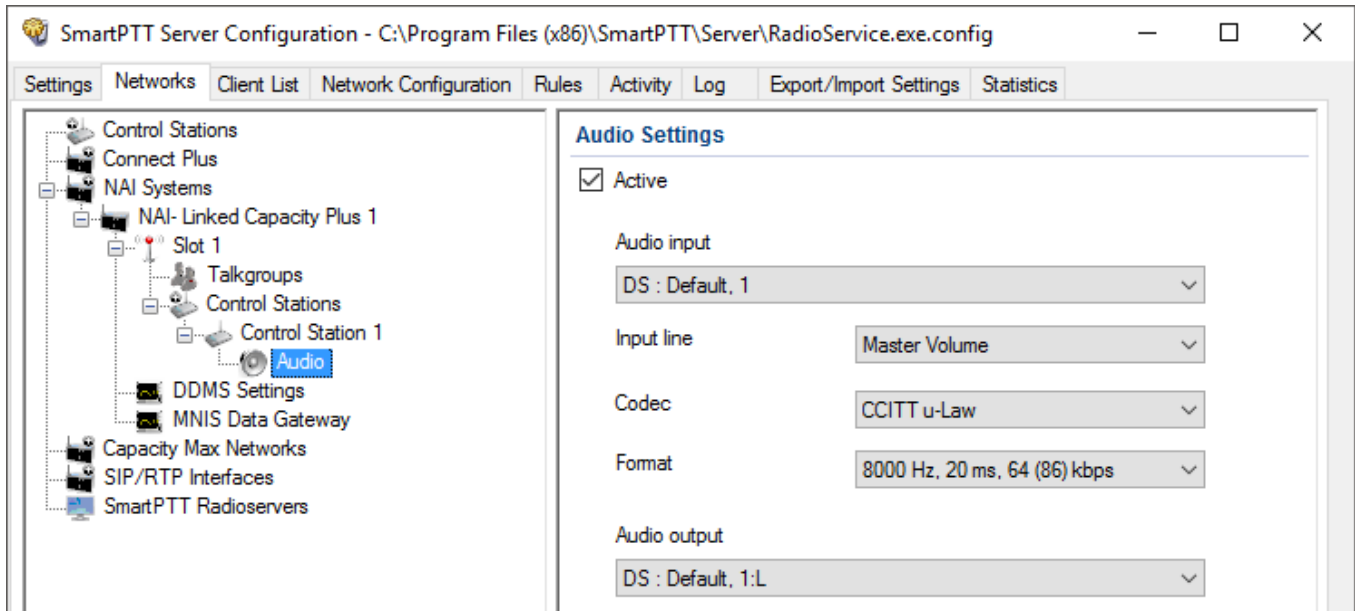


**NOTE**

All Calls can be initiated via a control station reserved for a group. If the control station is reserved for the dispatcher, you can only listen to **All Calls**.

### 2.3.2.1 Audio Settings

To select audio devices and set up VoIP parameters, click **Audio** in the **Networks** tab of *SmartPTT Radioserver Configurator*.



**Active:** Activates audio settings.

**Audio input:** An audio device to which the control station audio output is connected.

**Input line:** Audio mixer line used for connections. The control station audio output can be connected to the line input of the audio device.

**Codec:** Outgoing audio stream compression method.

**Format:** Sampling frequency of an outgoing audio stream.

#### Example

Specifications of the codec format **8000 Hz, 20 ms, 64 (86) kbps:**

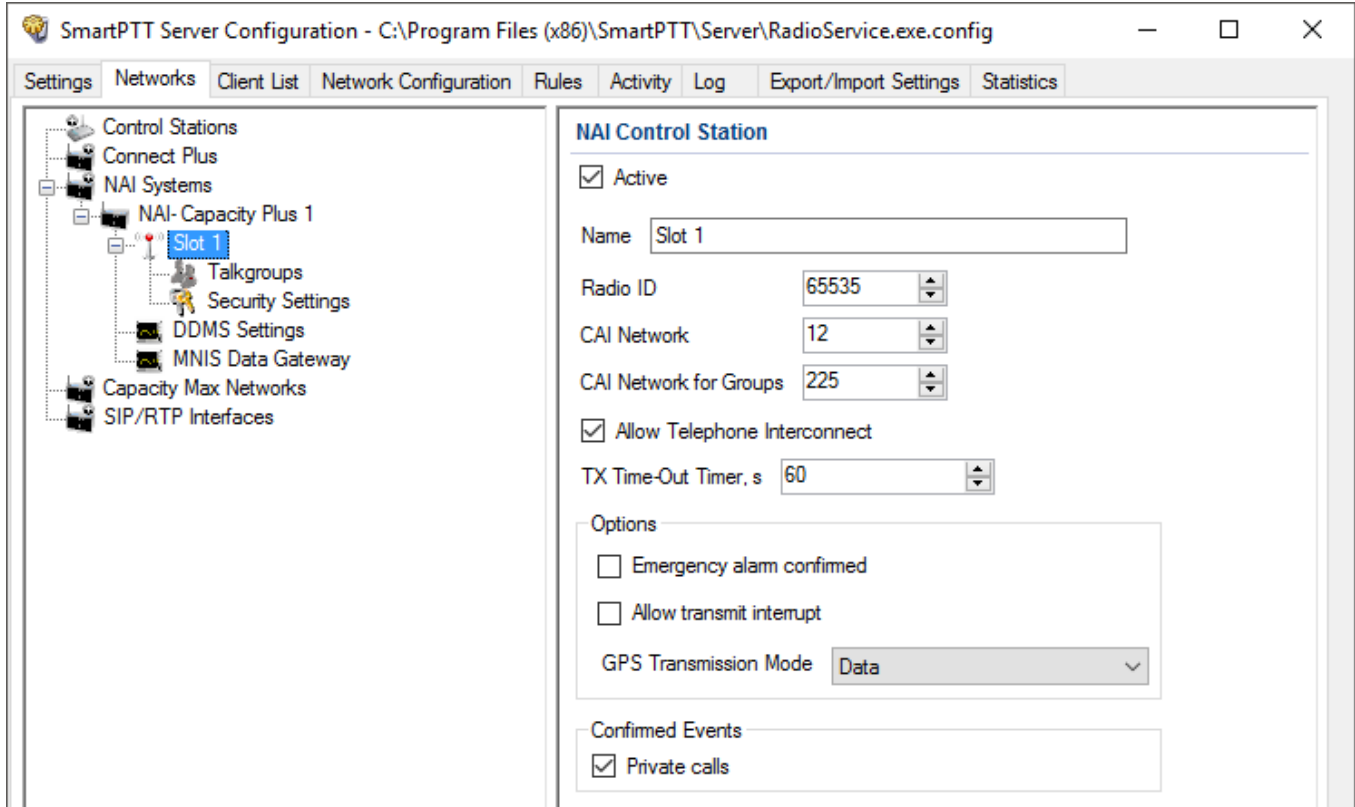
- **8000 Hz** is the sampling rate
- **20 ms** is the frame size
- **64 kbps** is the voice data bit rate
- **86 kbps** is a full bit rate (required network bandwidth)

**Audio output:** An audio device to which the control station audio input is connected.



## 2.3.3 Configuring NAI Slots

To configure the NAI Network slots, on the **Networks** tab of SmartPTT Radioserver Configurator, click the desired slot. The **NAI Control Station** pane appears:



### NOTE

For the NAI - Extended Range Direct Mode, NAI - Capacity Plus or NAI - Linked Capacity Plus networks, there is only one slot to configure.

**Active:** Activates a control station.

**Name:** Slot name.

**Slot ID:** Local slot identifier. This identifier is used in telephone calls (e.g., when there are many local slots to differentiate between them).

**Radio ID:** Unique identifier of a virtual control station corresponding to the network slot.

**CAI Network:** CAI-network identifier. The default value is 12 (must match *MOTOTRBO CPS* settings).

**CAI Network for Groups:** CAI-network for groups identifier. The default value is 225 (must match *MOTOTRBO CPS* settings).

**Allow Telephone Interconnect:** Enables telephone calls on the slot.

**NOTE**

**Allow Telephone Interconnect** is not applicable to the NAI - Extended Range Direct Mode systems.

**Emergency alarm confirmed:** Determines if the emergency alarm is allowed to be acknowledged.

**Allow transmit interrupt:** Enables or disables the ability to interrupt a radio.

**Private Calls:** Enables or disables the private calls confirmation.

**GPS Transmission Mode:** Allows you to select the way how to transmit location updates: as a data packet in multiple bursts or as a single CSBK (Control Signaling Block).

Each solution has its own advantages and disadvantages:

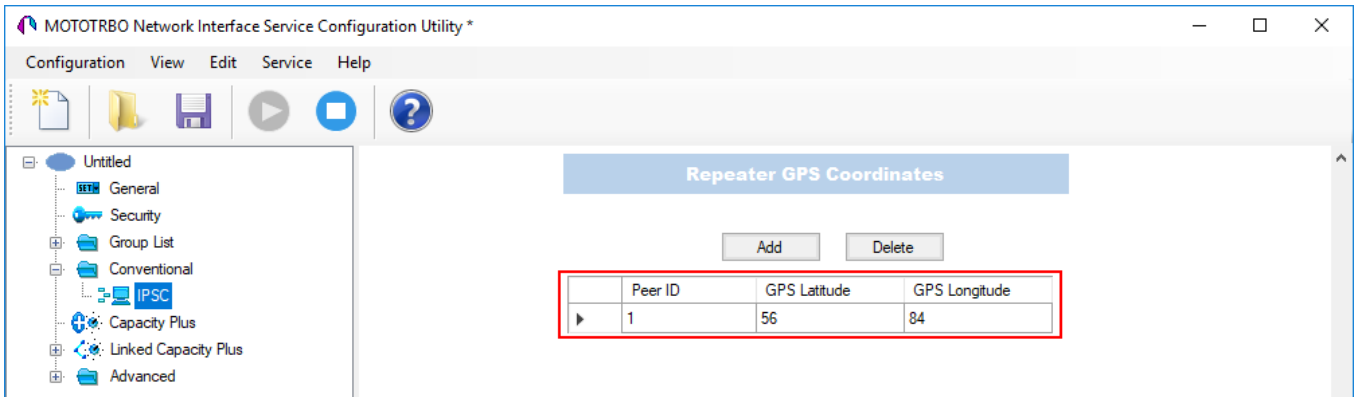
GPS Transmission Mode	Advantages	Disadvantages
<b>Data</b>	No need to configure additional settings for receiving GPS data	Increased traffic load on a channel
<b>CSBK</b>	<ul style="list-style-type: none"> <li>• Low traffic load on a channel</li> <li>• Increased GPS transmission frequency rate — once in 15 seconds</li> </ul>	<ul style="list-style-type: none"> <li>• Not all radios support CSBK commands</li> <li>• Additional MNIS settings*</li> </ul>
<b>Enhanced CSBK</b>	<ul style="list-style-type: none"> <li>• Low traffic load on a channel</li> <li>• Increased GPS transmission frequency rate — once in 7.5 seconds</li> </ul>	<ul style="list-style-type: none"> <li>• Not all radios support CSBK commands</li> <li>• Additional MNIS settings*</li> </ul>

**NOTE**

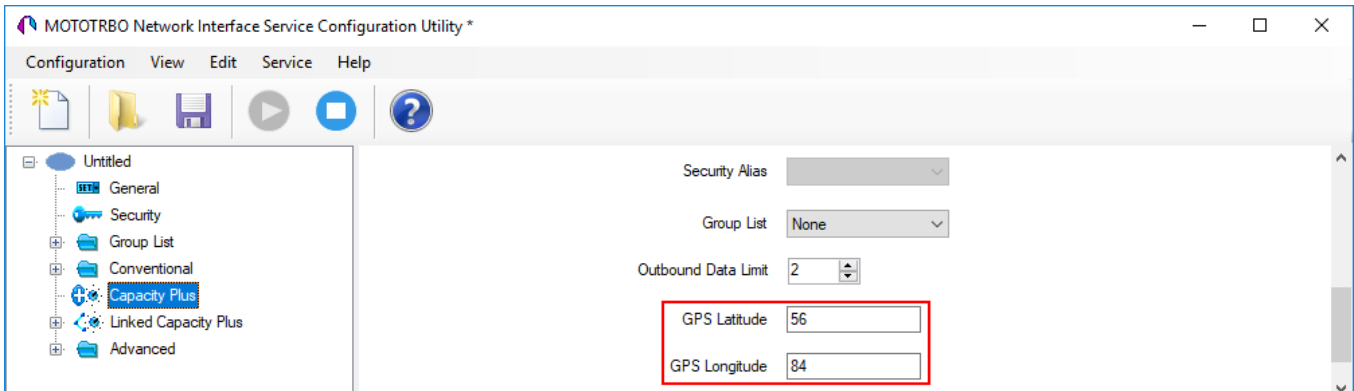
The Enhanced CSBK **GPS Transmission Mode** is not applicable to the NAI - Extended Range Direct Mode systems.

To transmit location data using CSBK and Enhanced CSBK, configure additional MNIS settings, which include adding repeater latitude and longitude. This information is used for calculation of radio locations.

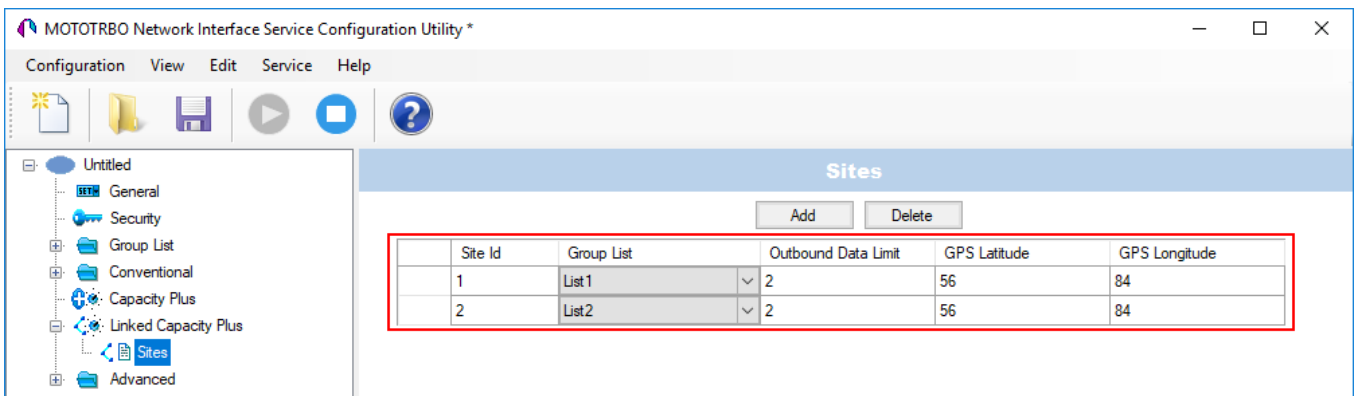
- For NAI - IP Site Connect configuration select **Conventional** → **IP Site Connect/Extended Range Direct Modedomain name** and in the **Repeater GPS Coordinates** area specify latitude and longitude for each network system:



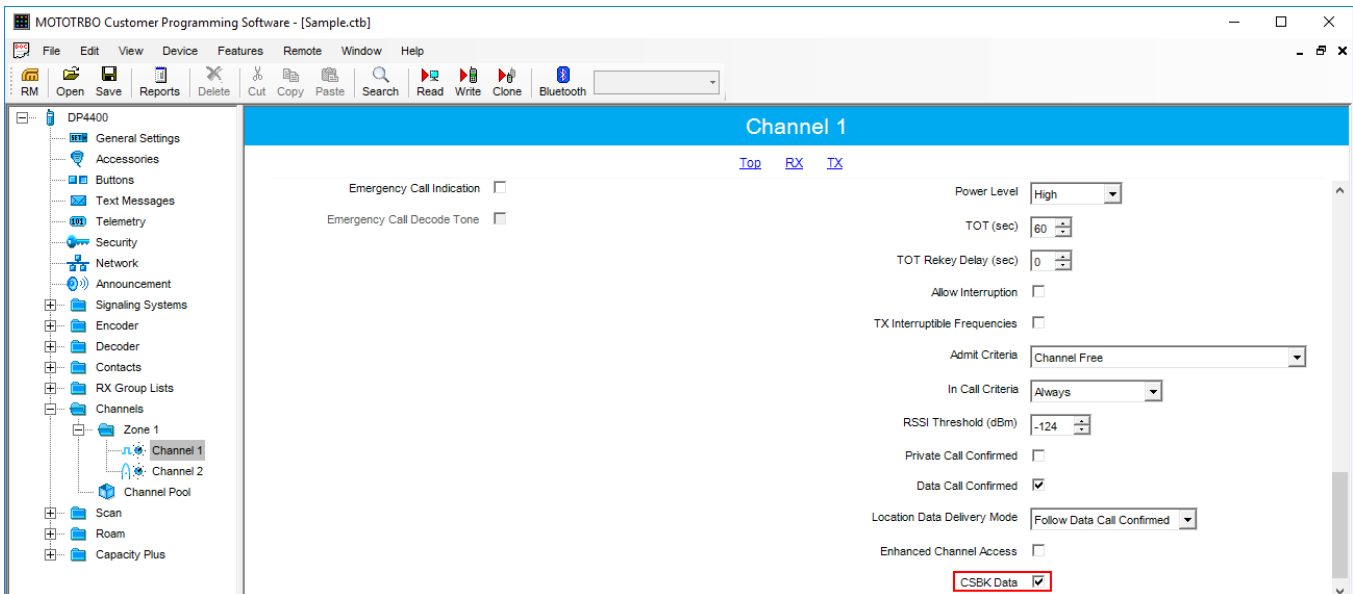
- For NAI - Capacity Plus configuration specify latitude and longitude just in one place:



- For NAI - Linked Capacity Plus configuration specify latitude and longitude for each site:



Also, to transmit location data using CSBK or Enhanced CSBK, select **CSBK Data** in radio settings:



#### NOTE

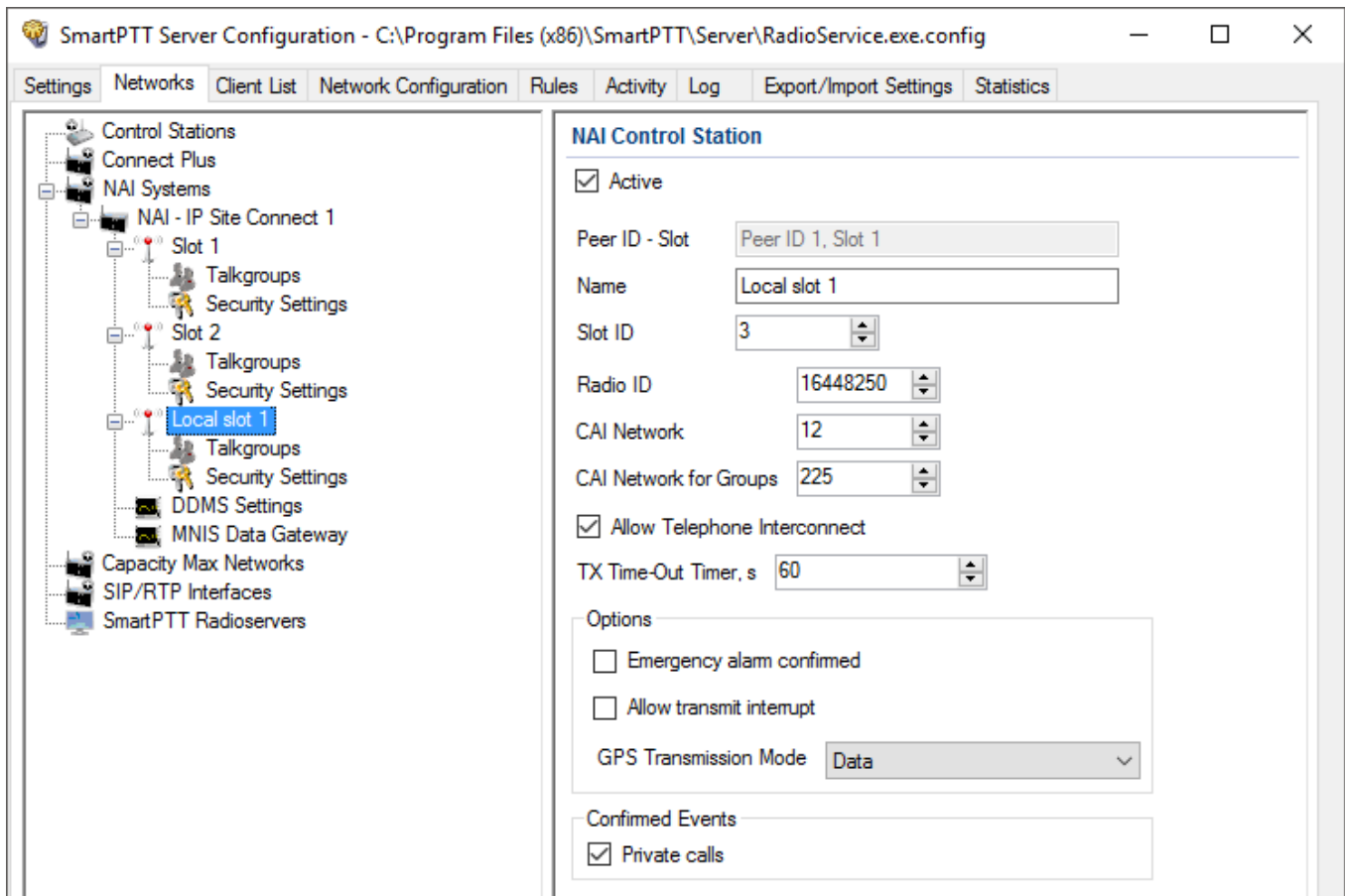
Remember that Enhanced CSBK can be used on **Enhanced GNSS** channels only.

### 2.3.3.1 Configuring Local Slots

As soon as the local slot is added to the **Local Slots** table, a new section appears in the settings tree.

#### NOTE

Local slots become available only when *Repeater* is selected for voice transmission.



**Active:** Allows you to enable or disable a local control station.

**Peer ID - Slot:** Peer identifier and slot number. Data is taken from the **Local Slot** table.

**Name:** Name of the local slot. It is used in *SmartPTT Radioserver Configurator* and in *SmartPTT Dispatcher*.

**Slot ID:** The identifier of the local slot, which will be used for group calls. This will be used in a group call mask. It must be unique in the system.

**Radio ID:** Unique radio identifier used during communication. It can match **Radio ID** of the virtual slots.

**CAI Network:** CAI-network ID. Use the default value of 12.

**CAI Network for Groups:** Group CAI-network ID. Use the default value of 225.

**Allow Telephone Interconnect:** Allows telephone calls on the slot.

**TX Time-Out Timer, s:** Time period during which the radio can transmit without interruptions. When time is out, the transmission is interrupted.

**Emergency alarm confirmed:** Determines if the emergency alarm is allowed to be acknowledged.

**Allow transmit interrupt:** Enables or disables the ability to interrupt a radio.

**Private calls:** This feature sets private calls on the current digital channel as confirmed.

**GPS Transmission Mode:** Allows you to select the way how to transmit location updates: as a data packet in multiple bursts or as a single CSBK (Control Signaling Block). For more information, see [GPS Transmission Mode](#).

To configure groups of the local slot, click **Talkgroups**. Configure talkgroup settings as ordinary IP Site Connect talkgroups.

If you use encryption, go to **Security Settings**. For more information on how to configure encryption settings, see [Security Settings in NAI systems](#).

## 2.3.3.2 Configuring Joint GPS and Indoor Data

If you want to receive joint location data (GPS and indoor) in NAI, configure the following settings:

- Radio settings in *MOTOTRBO CPS*
- Radio settings in SmartPTT Dispatcher
- Repeater settings in *MOTOTRBO CPS*

### 2.3.3.2.1 Configuring Radio in MOTOTRBO CPS

To configure radio in *MOTOTRBO CPS*, follow these steps:

1. In the radio firmware file, select **Channels** → **<Zone Name>** → **<Channel Name>**.
2. In the **<Channel Name>** pane, perform the following actions:
  - Select the **Enhanced GNSS** check box, and from the **Window Size** list, select *10*.
  - From the **Compressed UDP Data Header** list, select *MSI*.
  - Clear the **CSBK Data** check box.

### 2.3.3.2.2 Configuring Radio in SmartPTT Dispatcher

To configure radio in SmartPTT Dispatcher, follow these steps:

1. Open the radio properties window.
2. In the **Location** tab, perform the following actions:
  - a. Select the **Indoor Tracking** check box.
  - b. Select the **Update Interval** check box, and enter 30 in the field.

### 2.3.3.2.3 Configuring Repeater in MOTOTRBO CPS

To configure repeater in *MOTOTRBO CPS*, follow these steps:

1. In the repeater firmware file, select **Channels** → <Zone Name> → <Channel Name>.
2. In the <Channel Name> pane, in the **Enhanced GNSS area**, select the **Enable** check box.

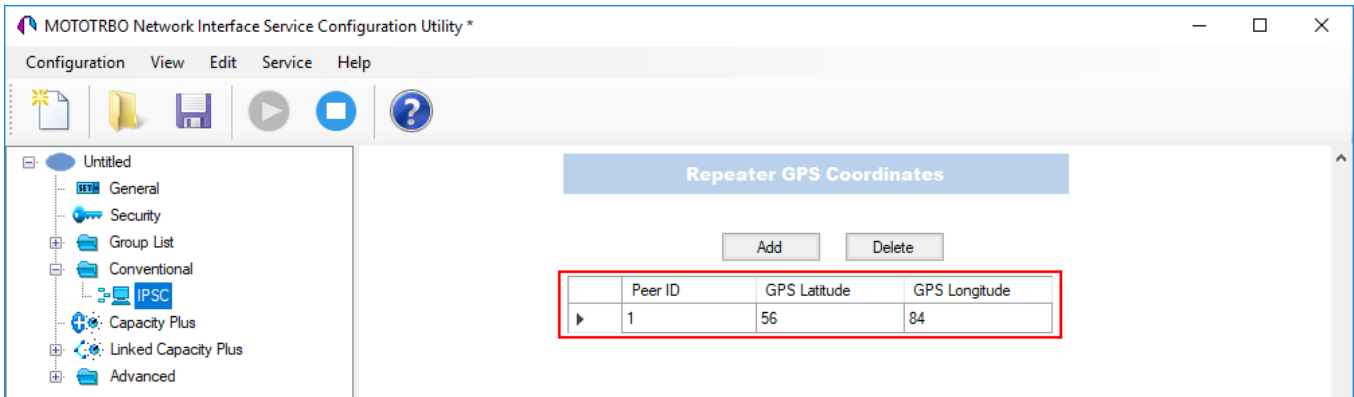
### 2.3.3.3 Configuring Data Transmitting on CSBK/Enhanced CSBK channel

#### NOTE

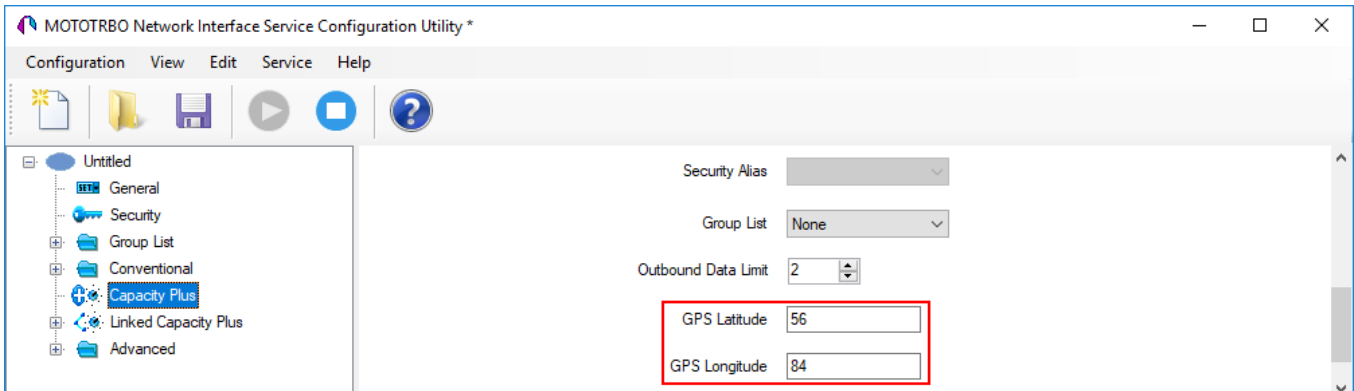
1. The Enhanced CSBK GPS Transmission Mode is not applicable to the NAI - Extended Range Direct Mode systems.
2. Enhanced CSBK can be used on **Enhanced GNSS** channels only.

To transmit location data using CSBK and Enhanced CSBK, configure additional MNIS settings, which include adding repeater latitude and longitude. This information is used for calculation of radio locations.

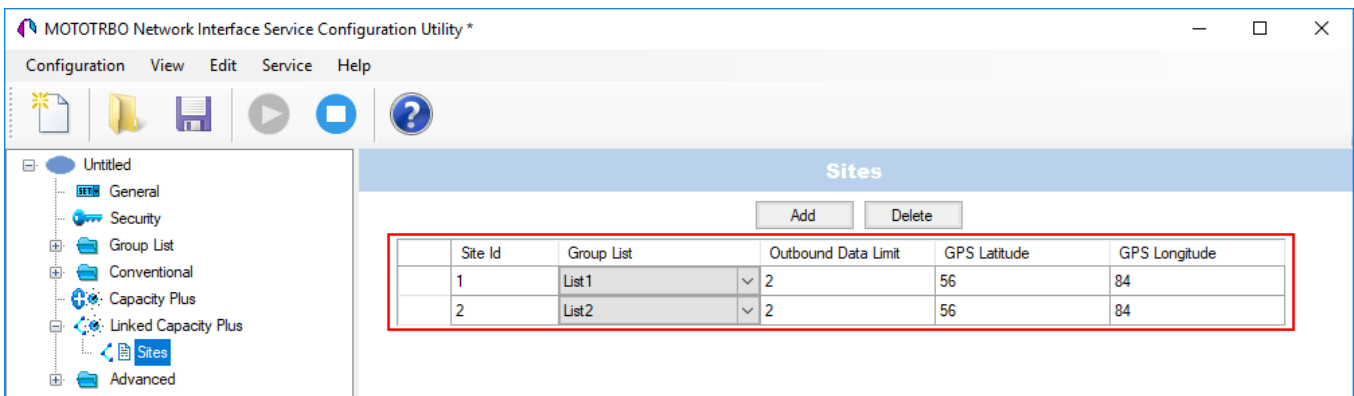
- For NAI - IP Site Connect configuration: Select **Conventional** → **IP Site Connect/Extended Range Direct Modedomain name** and in the **Repeater GPS Coordinates** area specify latitude and longitude for each network system:



- For NAI - Capacity Plus configuration: Specify latitude and longitude just in one place:

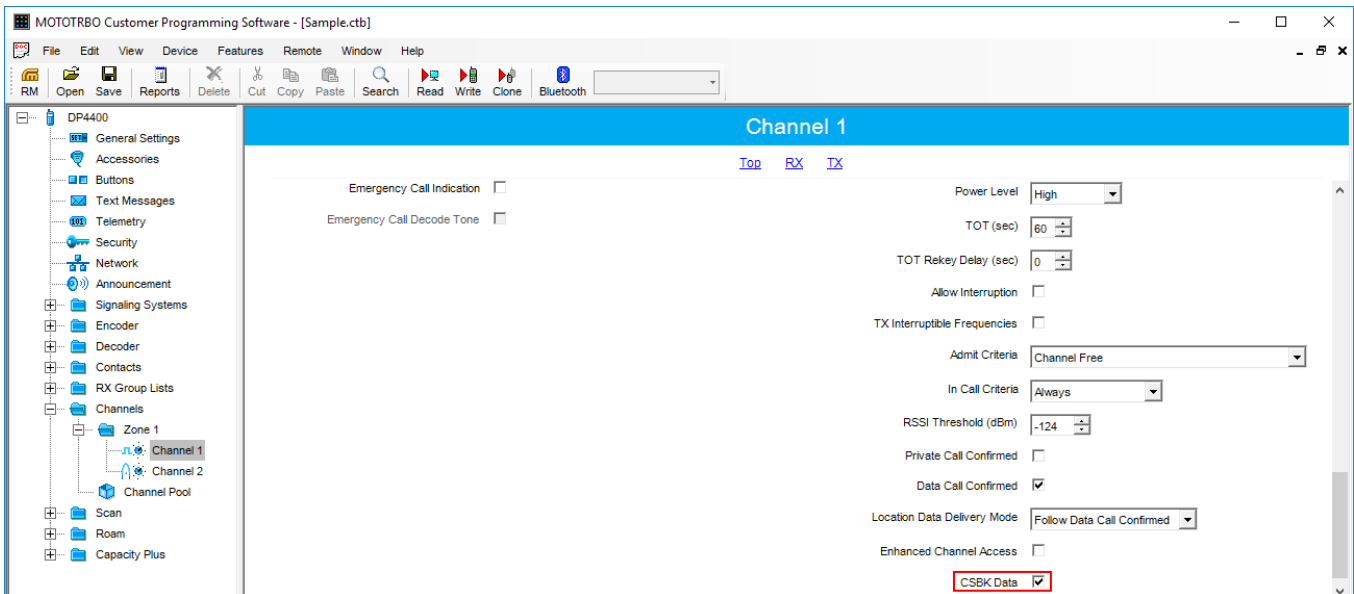


- For NAI - Linked Capacity Plus configuration: Specify latitude and longitude for each site:



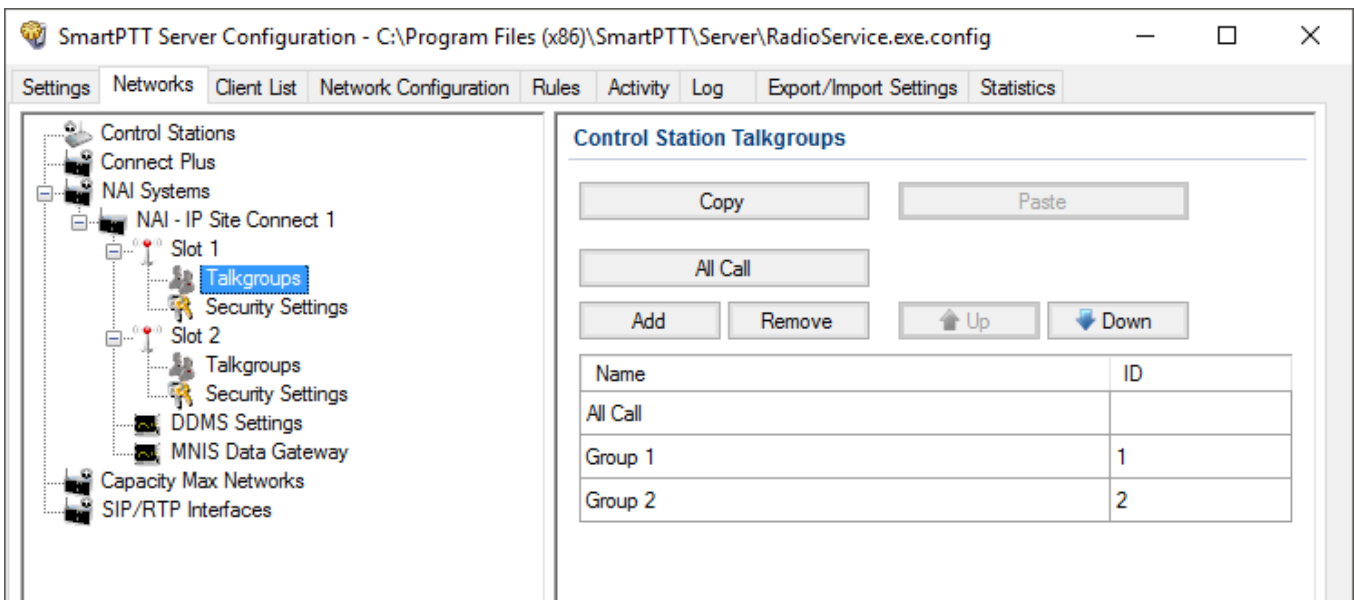


Also, to transmit location data using CSBK or Enhanced CSBK, select **CSBK Data** in radio settings:



### 2.3.4 Configuring NAI Talkgroups

To configure slot groups, in the **Networks** tab of *SmartPTT Radioserver Configurator*, click **Talkgroups**. The **Control Station Talkgroups** pane appears:

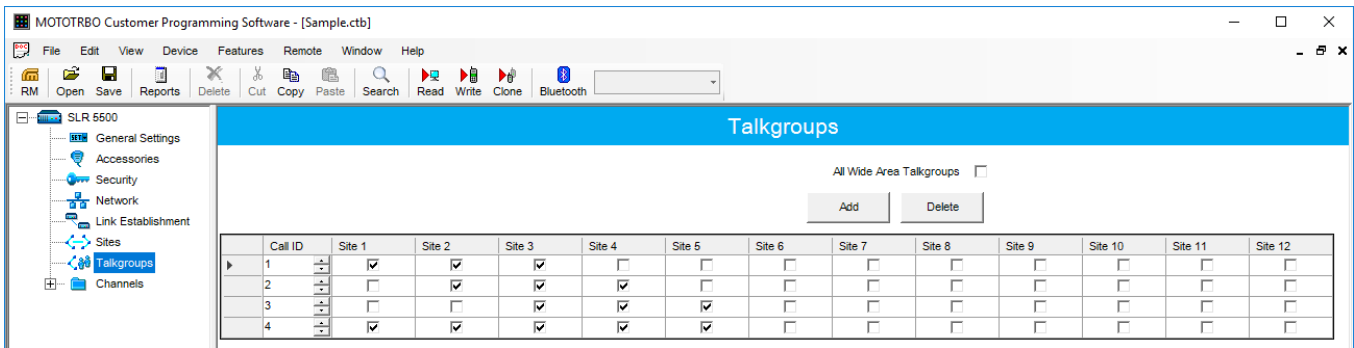


**NOTE**

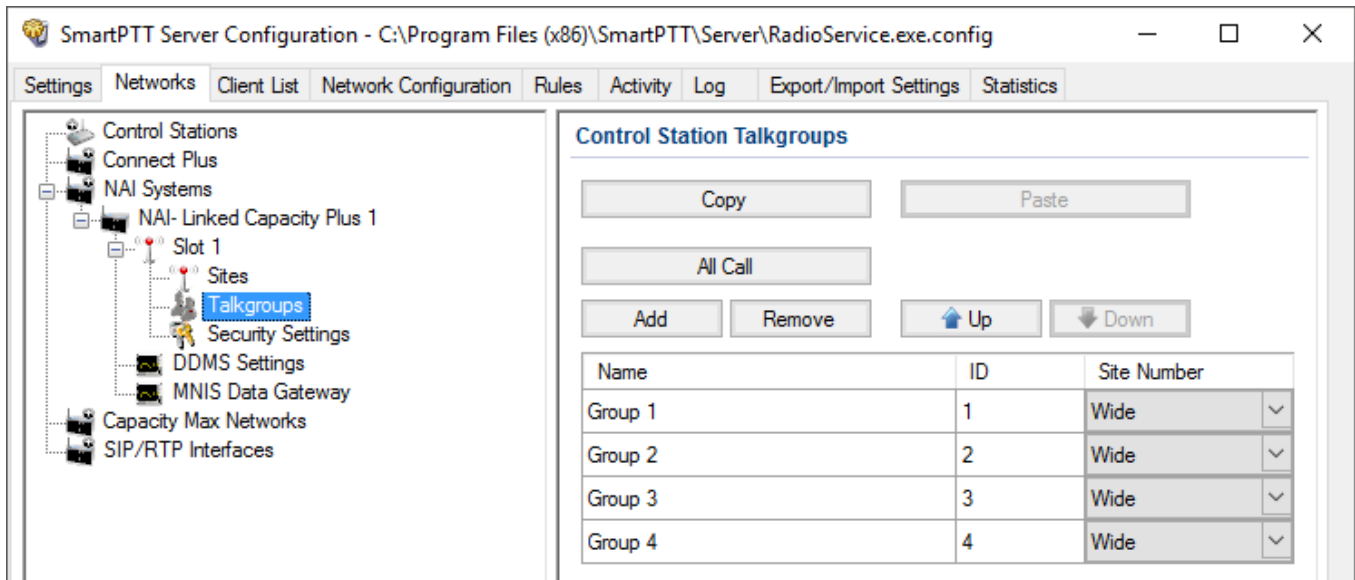
The configuration process of the virtual control station talkgroups for NAI - IP Site Connect, NAI - Extended Range Direct Mode or NAI - Capacity Plus networks is absolutely similar to the configuration of MOTOTRBO control station talkgroups.

For NAI - Linked Capacity Plus network type, parameters of wide area and local talkgroups are set in the **Control Station Talkgroups** window. All the configured talkgroups are displayed in *SmartPTT Dispatcher*.

Wide area talkgroup calls are available to the radios that are in the coverage area of sites designated in MOTOTRBO CPS for this talkgroup. Select check boxes in the required columns of the **Talkgroups** tab in the repeater MOTOTRBO CPS settings. Each column corresponds to the site where the talkgroup is available for a call.



In order to display wide area talkgroups in *SmartPTT Dispatcher*, add necessary talkgroups in *SmartPTT Radioserver Configurator*, define talkgroup identifiers that correspond to the identifiers of the wide area talkgroups in the repeater MOTOTRBO CPS settings and select *Wide* in the **Site Number** field.

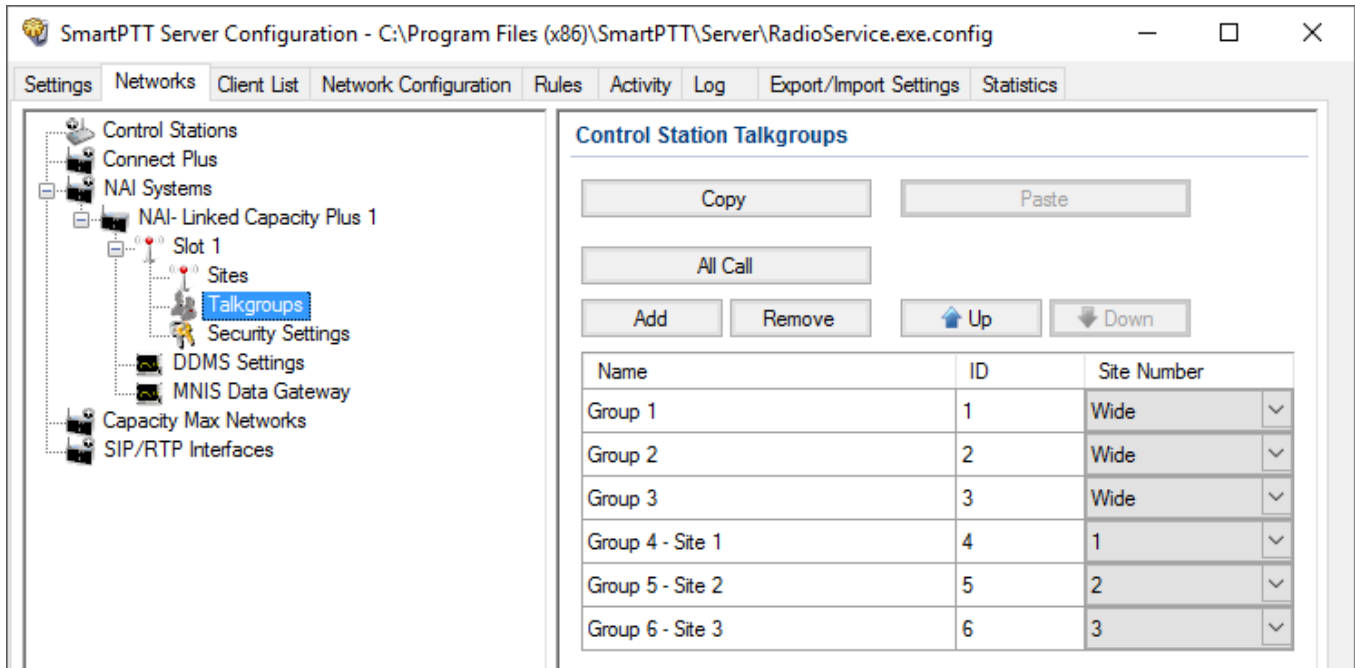


The talkgroups that are not specified in the repeater MOTOTRBO CPS settings are considered as local. The local talkgroup call does not go beyond the site where the call is initiated.

Add the required local talkgroups in *SmartPTT Radioserver Configurator*, define identifiers for them and select site number from the list in the **Site Number** field.

#### NOTE

Ensure that identifiers of wide area and local talkgroups do not match.



It is important to specify all talkgroups supported by the system in *SmartPTT Radioserver Configurator*. Otherwise, the operator can't initiate a call to such a talkgroup until the talkgroup member has made a group call to the operator.

To add the All Call, click **All Call**. In NAI - Linked Capacity Plus networks, you can add a wide All Call and a local All Call, which is limited to one site.

To add a wide All Call, which is available to all sites, click **All Call**. Ensure that **Site Number** is set to *Wide*.

To add an **All Call** limited to one site, click **All Call**, and in the **Site Number** column select the site number where the All Call will be heard. Please note, that you do not need any IDs for local All Calls. Only dispatchers can initiate the local All Call from the dispatch console.

**NOTE**

Local All Calls operate within one site in networks where voice transmission is carried out via a repeater. In hybrid networks, where voice transmission is carried out via a control station, a local All Call operates as the global All Call.

Name	ID	Site Number
All Call		Wide
All Call - Site 1		1
All Call - Site 2		2
Group 1	1	Wide
Group 2	2	Wide
Group 3	3	Wide
Group 4 - Site 1	4	1
Group 5 - Site 2	5	2
Group 6 - Site 3	6	3

## 2.3.5 DDMS Service

*Device Discovery and Mobility Service* (DDMS) is a service that monitors the presence of ARS capable radio units and reports their parameters (IP address, Radio ID, etc.) to interested applications, such as SmartPTT Radioserver and *MOTOTRBO Network Interface Service Configuration Utility* (MNIS).

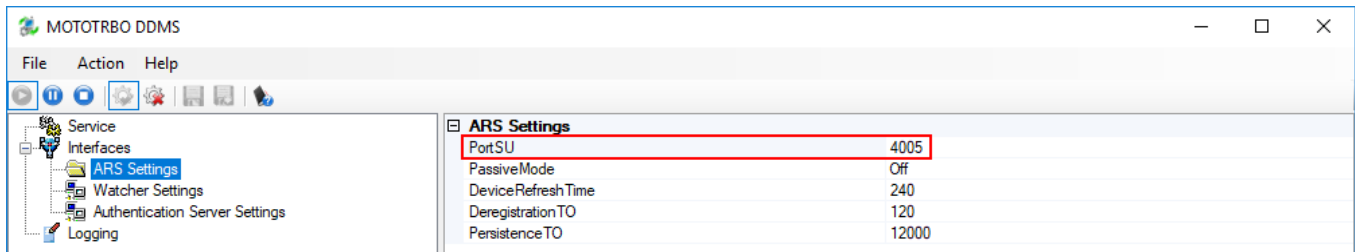
*Device Discovery and Mobility Service* is closely connected to MNIS. DDMS filters the registration service packets (ARS), received by the repeater, and information on the radio presence in the network is sent to all systems for further processing.

Before configuring *Device Discovery and Mobility Service*, ensure that *MOTOTRBO DDMS* and *MOTOTRBO Network Interface Service Configuration Utility* are installed on the computer.

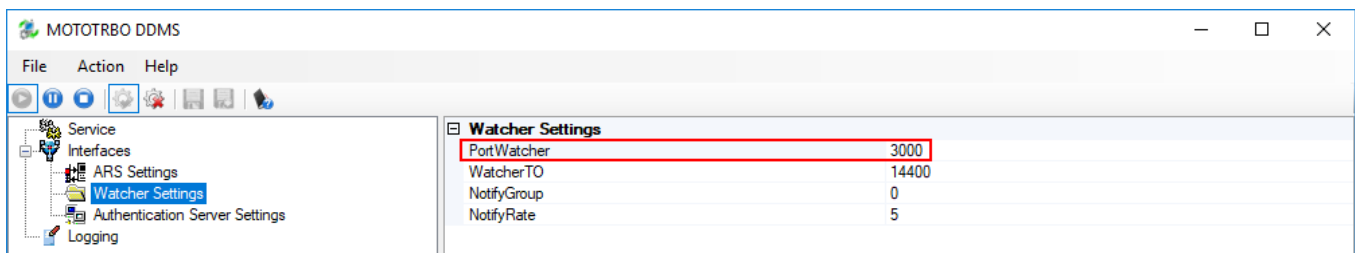
### 2.3.5.1 Configuring DDMS in MOTOTRBO DDMS

To configure DDMS in *MOTOTRBO DDMS*, follow these steps:

1. Run *MOTOTRBO DDMS*.
2. In the left pane, select **Interfaces** → **ARS Settings**.
3. Ensure the **PortSU** field value matches the **ARS UDP Port** field value in **Advanced** → **Networks** of *MOTOTRBO Network Interface Service Configuration Utility*.



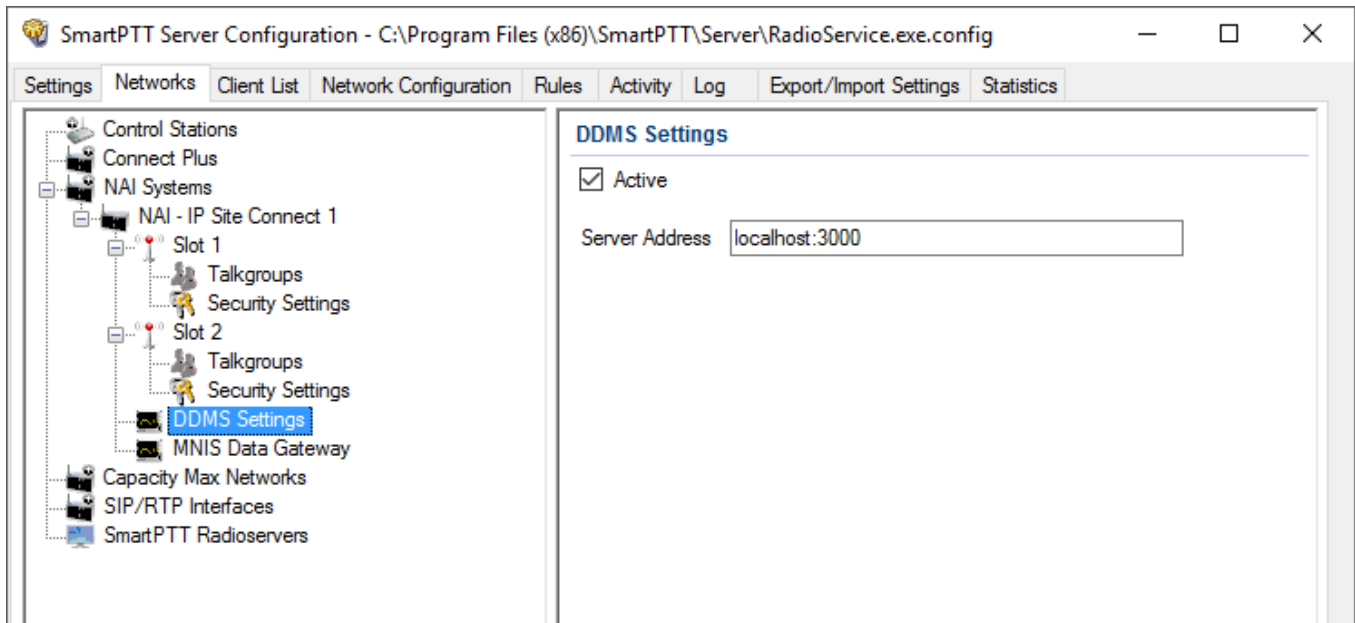
4. In the left pane, select **Interfaces** → **Watcher Settings**.
5. Ensure the **PortWatcher** field value matches the **WatcherPort** field in **Advanced** → **Networks** of *MOTOTRBO Network Interface Service Configuration Utility*.





## 2.3.5.2 Configuring DDMS in SmartPTT Radioserver Configurator

To configure DDMS settings in SmartPTT Radioserver Configurator, follow these steps:

1. In the left pane of the **Networks** tab, expand **NAI Systems** → **<Added NAI network>** and select **DDMS Settings**.



2. In the **DDMS Settings** pane, perform the following actions:
  - a. Select the **Active** check box.
  - b. In the **Server Address** field, type the IP address of the PC with the *MOTOTRBO DDMS* application installed on it, and port number of the DDMS server.  
The port number in this field must match the **PortWatcher** field value in **Interfaces** → **Watcher Settings**.of *MOTOTRBO DDMS*
3. Click **Save**  to save changes.
4. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

## 2.3.6 MNIS Data Gateway

MNIS is used for data exchange and serves as a DDMS watcher.

Before configuring MOTOTRBO Network Interface Service, ensure that the following applications are installed on the computer:

- *MOTOTRBO Network Interface Service Configuration Utility*
- *MOTOTRBO CPS*

You also should have an access to the *MOTOTRBO CPS* firmware file of a master repeater.

You can configure MNIS in the following programs:

- *MOTOTRBO Network Interface Service Configuration Utility*
- SmartPTT Radioserver Configurator

Remote socket is used for connecting more than one NAI - Capacity Plus or NAI - Linked Capacity Plus networks to SmartPTT Radioserver.

For proper functioning of all connected networks (voice and/or data transmission), ensure the following:

- [MOTOTRBO Network Interface Service Configuration Utility](#), [MOTOTRBO DDMS](#) and *MNIS Data Gateway Relay* are installed on multiple computers. The number of computers depends on the number of networks NAI - Capacity Plus or NAI - Linked Capacity Plus connected to SmartPTT Radioserver.

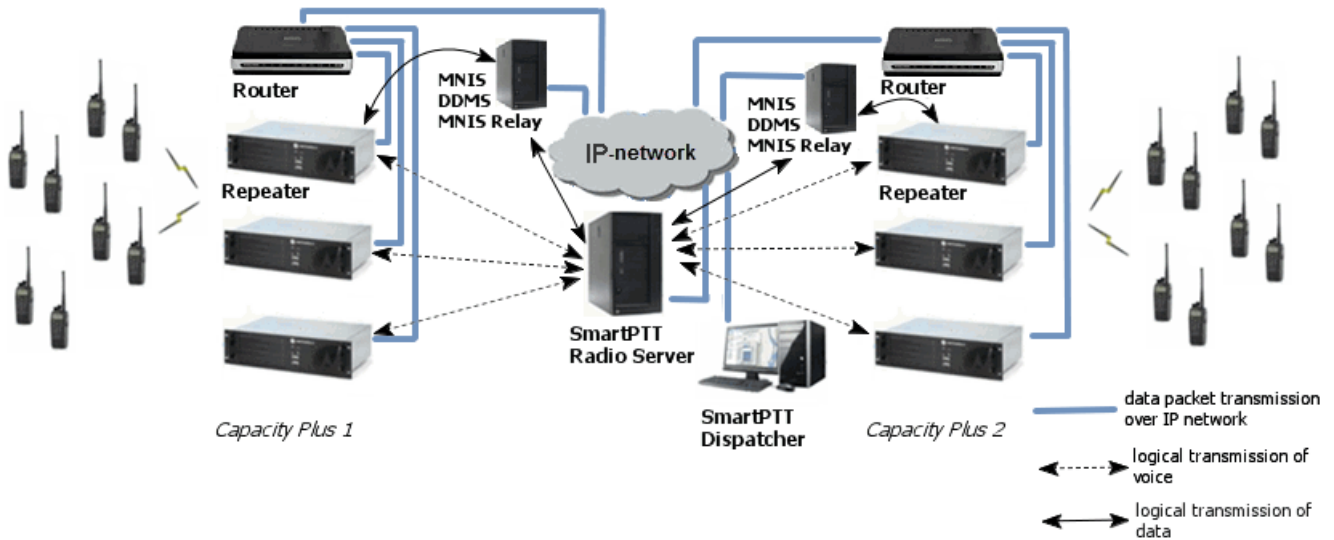
### **NOTE**

To get information on how to install and configure these applications, see the corresponding guides.



- Separate MNIS and DDMS services are configured by using the corresponding applications and started for each network.

Thus, voice data is transmitted from repeaters to SmartPTT Radioserver directly, and data is transferred via computer with MNIS Relay and the MNIS and DDMS service applications.



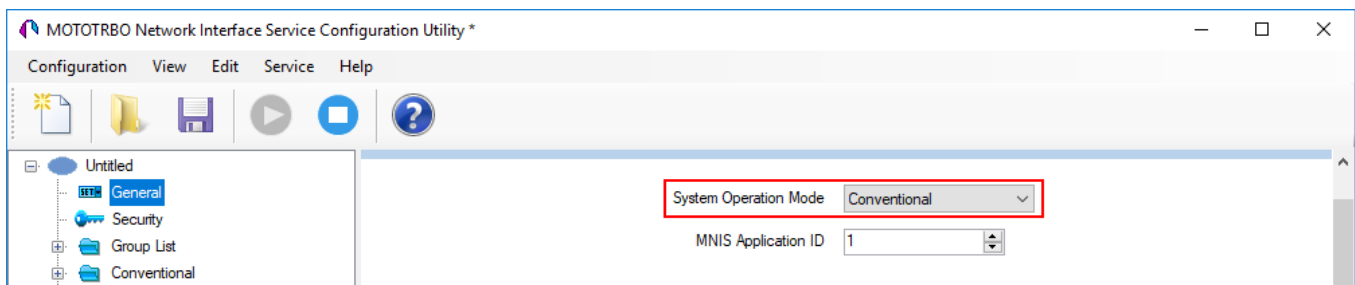
The section describes the configuration procedure of SmartPTT Radioserver Configurator and *MNIS Data Gateway Relay* for the remote socket.

You should repeat the configuration procedure of *MNIS Data Gateway Relay* and SmartPTT Radioserver Configurator for each separate network.

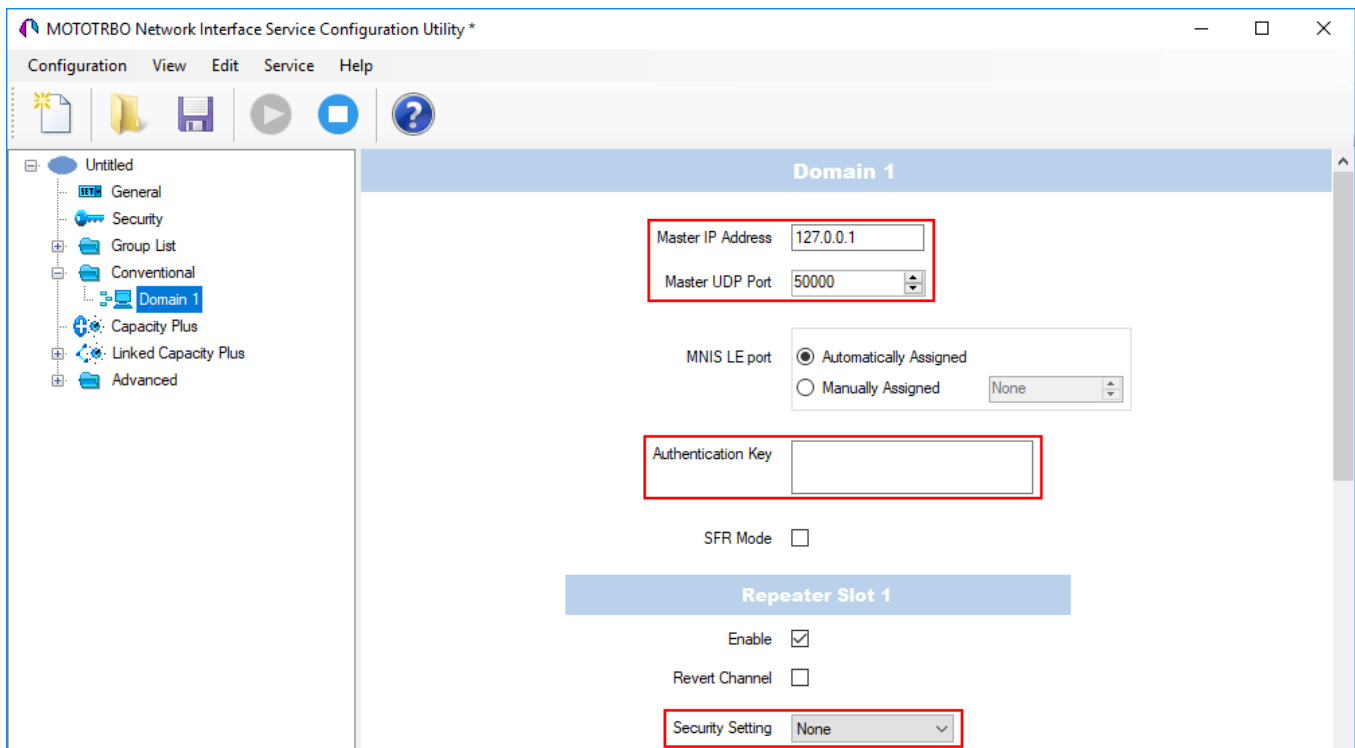
### 2.3.6.1 Configuring MNIS in MOTOTRBO Network Interface Service Configuration Utility

To configure MOTOTRBO Network Interface Service in *MOTOTRBO Network Interface Service Configuration Utility*, follow these steps:

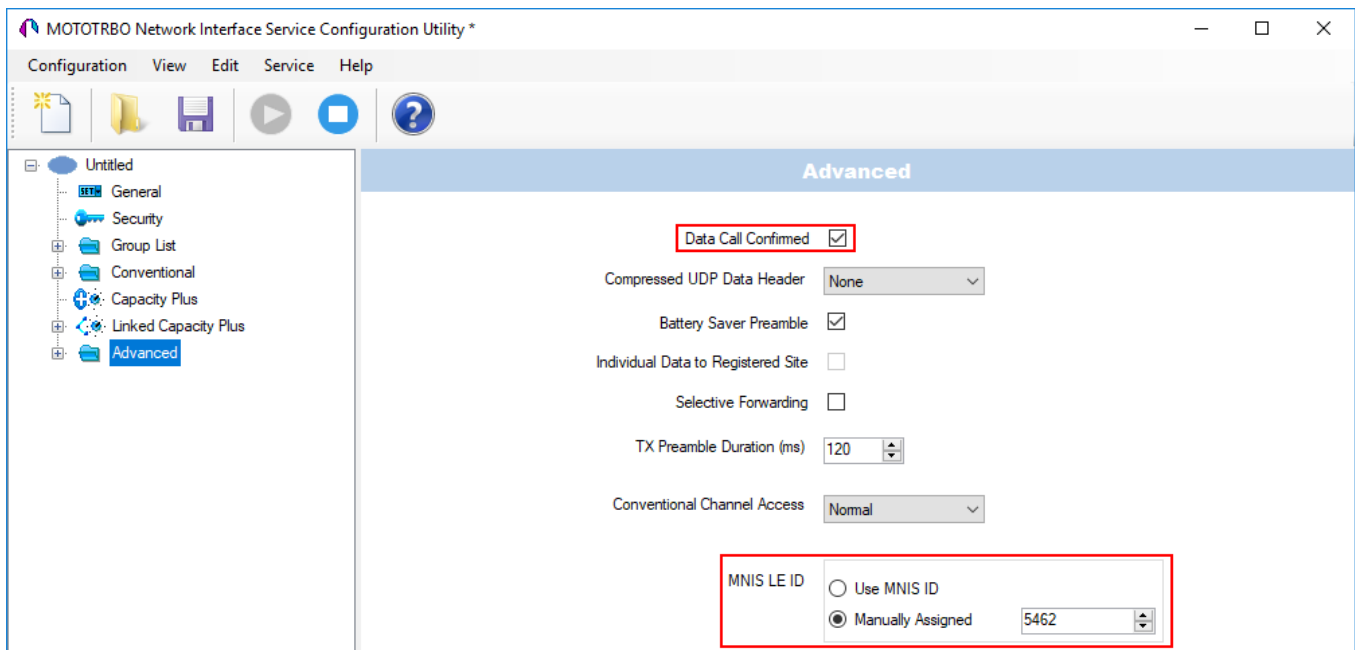
1. Run *MOTOTRBO Network Interface Service Configuration Utility*.
2. In the **System Operation Mode** field of the **General** node, select a mode depending on the network type selected in *SmartPTT Radioserver Configurator*.



3. In the **Security** node, set the encryption keys that match the keys specified in the radio *MOTOTRBO CPS* settings.
4. For IP Site Connect/Capacity Plus/Linked Capacity Plus set up the following parameters in the **Conventional/Capacity Plus/Linked Capacity Plus** sections respectively:



- a. In the **Master IP address** field, type the Master repeater IP address.  
This value should match **Master IP** value in *MOTOTRBO CPS* in the **Link Establishment** pane.
  - b. In the **Master UDP Port** field, type the Master repeater UDP port.  
This value should match **Master UDP Port** value in *MOTOTRBO CPS* in the **Link Establishment** pane.
  - c. In the **Authentication Key** field, type the authentication key, if it is set in MOTOTRBO CPS in the **Link Establishment** pane.
  - d. From the **Security Settings** list, select the desired encryption mode.  
The privacy settings should match the repeater security settings in *MOTOTRBO CPS*.
5. In the **Advanced** node, perform the following actions:

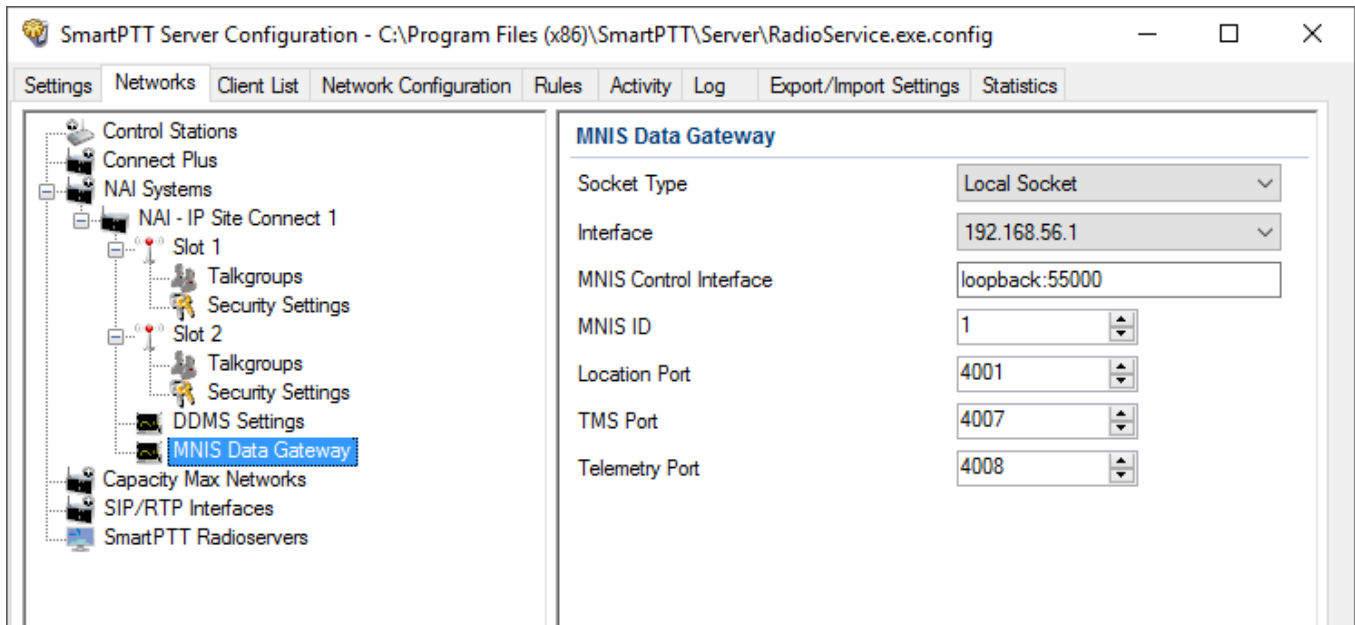


- a. Clear the **Data Call Confirmed** check box.
  - b. In the **MNIS LE ID** area, click **Manually Assigned** and enter a unique identifier MNIS.
6. Save changes.



## 2.3.6.2 Configuring MNIS Data Gateway for Local Socket

To configure MNIS Data Gateway for a local socket, follow these steps:

1. In the left pane of SmartPTT Radioserver Configurator, select **NAI Systems** → **NAI - Capacity Plus/NAI - Linked Capacity Plus Network** → **MNIS Data Gateway**.



2. In the **MNIS Data Gateway**, perform the following actions:
  - a. From the **Socket Type** list, select *Local Socket*.
  - b. From the **Interface** list, select the IP address specified in the **Tunnel IP Address** field in the **General** node of *MOTOTRBO Network Interface Service Configuration Utility*.  
The IP address should not match the IP address of the computer on which *MOTOTRBO Network Interface Service Configuration Utility* is installed.
  - c. In the **MNIS Control Interface**, type the following data:
    - i. The local IP-address of a computer.
    - ii. MNIS server port.  
The server port value should match the **Control Interface TCP Port** value in **Advanced** → **Network** of *MOTOTRBO Network Interface Service Configuration Utility*

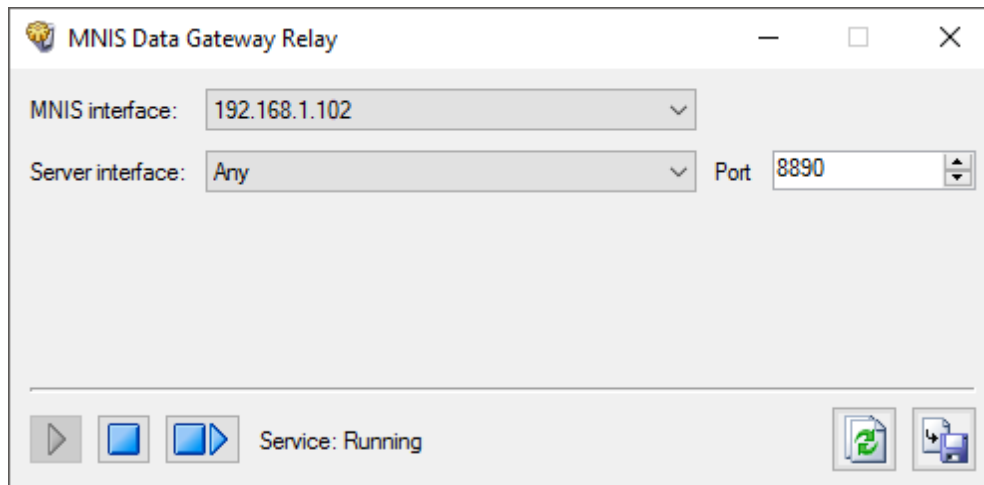
- d. In the **MNIS ID** field, enter the Common Air Interface (CAI) ID of the MNIS in the radio network.  
The value should match **MNIS Application ID** field in the **General** node of MOTOTRBO Network Interface Service Configuration Utility.  
It is also recommended that **MNIS ID** matches **Radio ID** in the radioserver slot settings.
  - e. *Optional:* Enter the port values for GPS, text messages and telemetry services.  
The ports values should match the ports set in the **TMS UDP Port, Telemetry UDP Port** and **Location Server UDP Port** fields in the **Advanced** → **Network** of *MOTOTRBO Network Interface Service Configuration Utility*.
3. Click **Save**  to save changes.
  4. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

## 2.3.6.3 Configuring MNIS Data Gateway for Remote Socket



### 2.3.6.3.1 Configuring MNIS Data Gateway Relay

To configure *MNIS Data Gateway Relay*, follow these steps:

1. Run *MNIS Data Gateway Relay*.



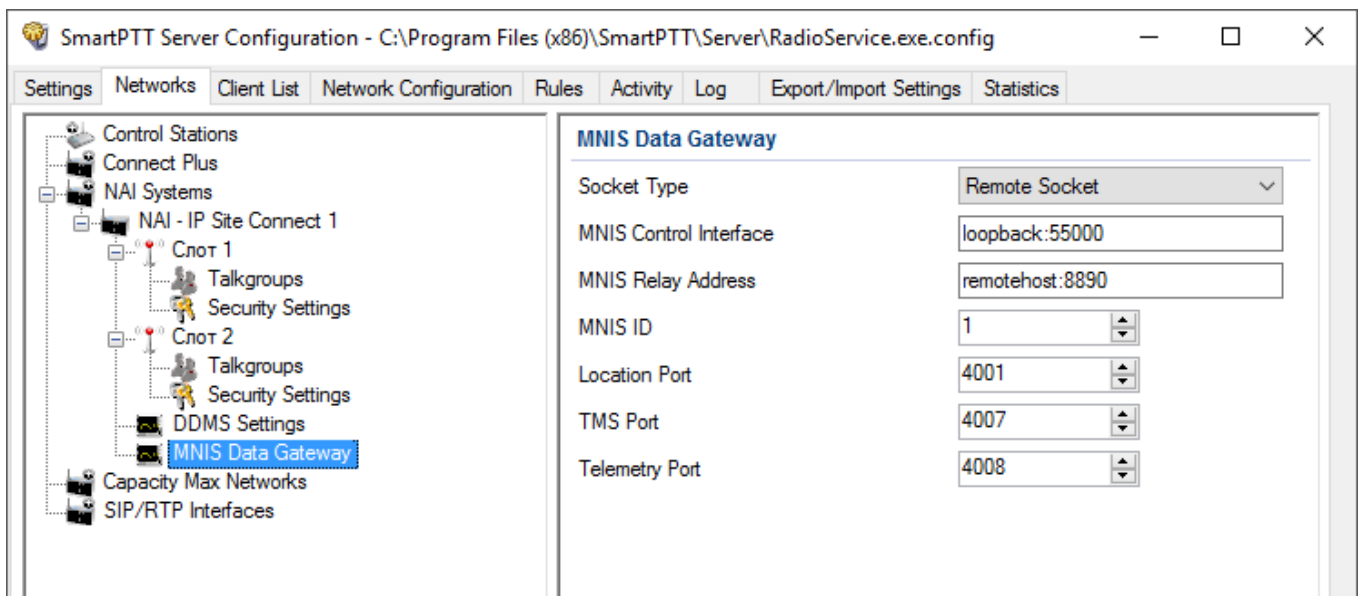
2. In the *MNIS Data Gateway Relay* program window, perform the following actions:

- a. From the **MNIS Interface** field, select the same IP address as in the **Tunnel IP Address** in the **General** node of *MOTOTRBO Network Interface Service Configuration Utility*.
  - b. From the **Server Interface** field, select the local computer IP address on which MOTOTRBO Network Interface Service is started and *MNIS Data Gateway Relay* is installed.
  - c. In the **Port** field, enter the port number through which the data is transmitted.
  - d. Click **Save**  to save changes.
  - e. Click **Restart**  to restart *MNIS Data Gateway Relay* and apply changes.
3. *Optional:* If needed, configure the port forwarding on the router to which your computer is connected.

### 2.3.6.3.2 Configuring Radio Server

To configure a remote socket in SmartPTT Radioserver, follow these steps:

1. In the left pane of *SmartPTT Radioserver Configurator*, select **NAI Systems** → **NAI - Capacity Plus/NAI - Linked Capacity Plus Network** → **MNIS Data Gateway**.





2. In the **MNIS Data Gateway** pane, perform the following actions:
  - a. From the **Socket Type** list, select *Remote Socket*.

- b. In the **MNIS Control Interface (IP address:Port)** field, enter an IP address and a port of the computer that has MOTOTRBO Network Interface Service installed.
- c. In the **MNIS Relay Address (IP address:Port)** field, enter an IP address and a port specified in MNIS Data Gateway Relay.

**NOTE**

IP addresses entered in the **MNIS Control Interface (IP address:Port)** and **MNIS Relay Address (IP address:Port)** fields should be the same and ports should differ.

- d. In the **MNIS ID** field, enter the Common Air Interface (CAI) ID of the MNIS in the radio network.  
The value should match **MNIS Application ID** field in the **General** node of MOTOTRBO Network Interface Service Configuration Utility.
  - e. *Optional:* Enter the port values for GPS, text messages and telemetry services.  
The ports values should match the ports set in the **TMS UDP Port, Telemetry UDP Port** and **Location Server UDP Port** fields in the **Advanced** → **Network** of *MOTOTRBO Network Interface Service Configuration Utility*.
3. Click **Save**  to save changes.
  4. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

## 2.3.7 Security Settings

The NAI systems support three types of privacy mechanisms – Basic, Enhanced, and Advanced Encryption Standard (AES).

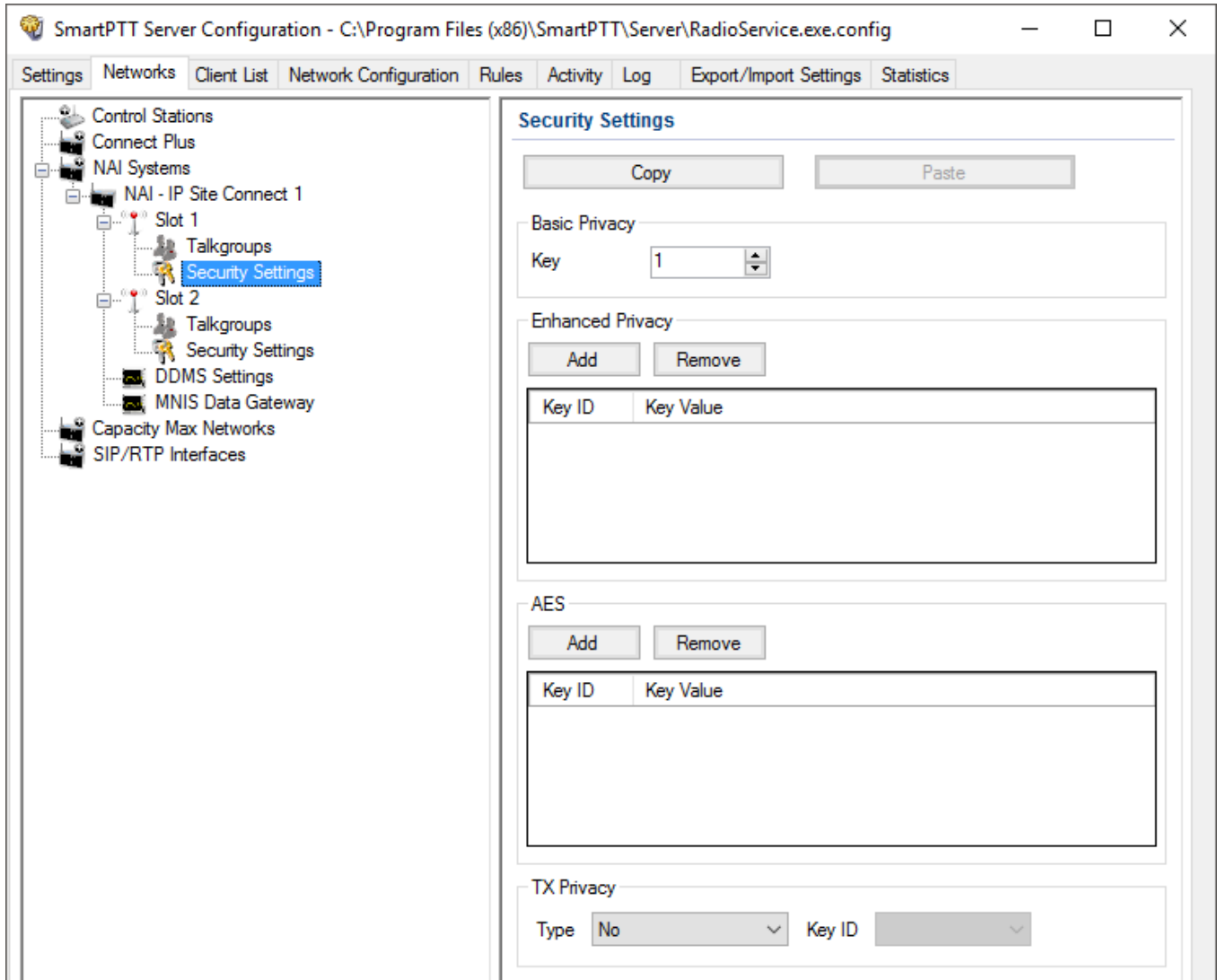
Both Basic and Enhanced Privacy utilize Motorola proprietary algorithms and therefore are not interoperable with other vendor's privacy offerings. The main differences between Basic and Enhanced Privacy are that the Enhanced Privacy provides higher level of protection by means of 40-bit key length. Enhanced Privacy supports multiple keys in a radio compared to one key in the case of Basic Privacy.

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST). The AES feature supports 256-bit key length. Similar to Enhanced Privacy, the AES also supports multiple keys.

**NOTE**

To use the AES encryption, install the correspondence license. For more information on how to install licenses, see [Licenses](#).

The **Security Settings** window allows you to specify the encryption keys for incoming and outgoing traffic on the digital channel.



**Copy:** Copy encryption settings of the channel to the clipboard.

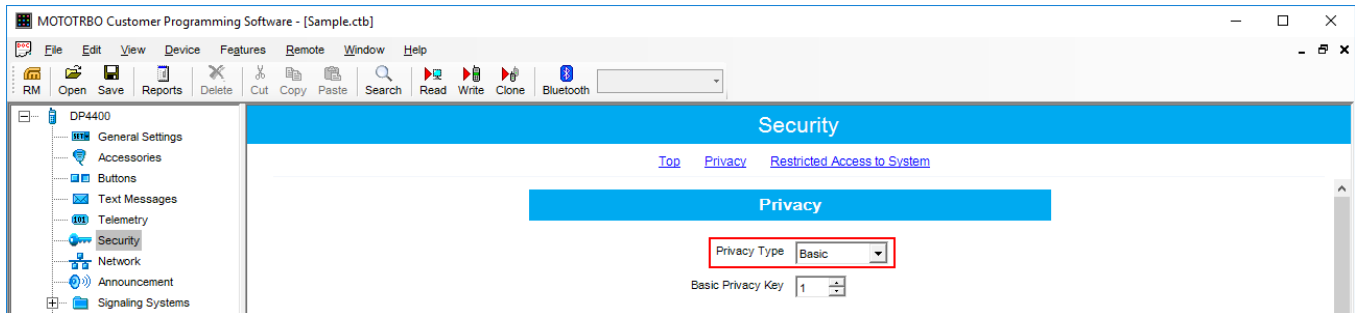


**Paste:** Paste encryption settings of the channel from the clipboard.

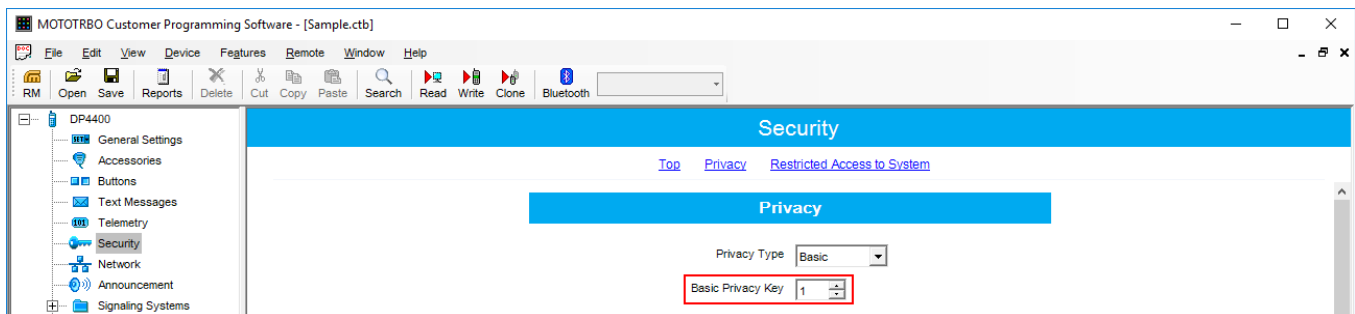
## Basic Privacy

To configure **Basic Privacy**, follow these steps:

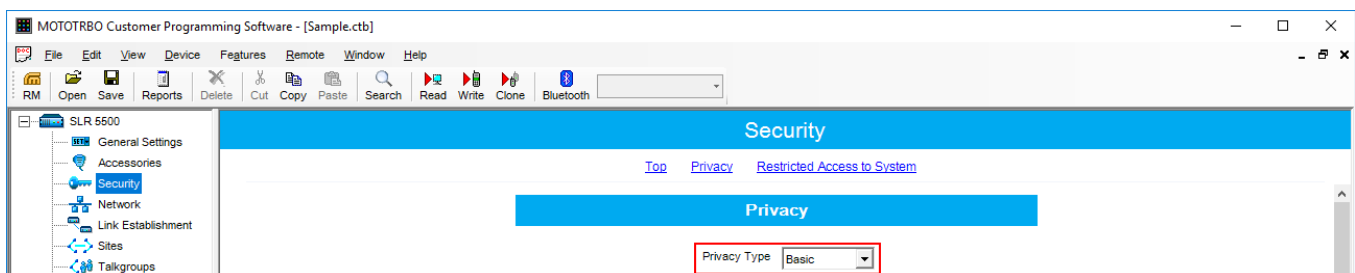
1. Run *MOTOTRBO CPS*.
2. In the **Security** window of the radio settings in *MOTOTRBO CPS* in the **Privacy Type** field, select *Basic*.



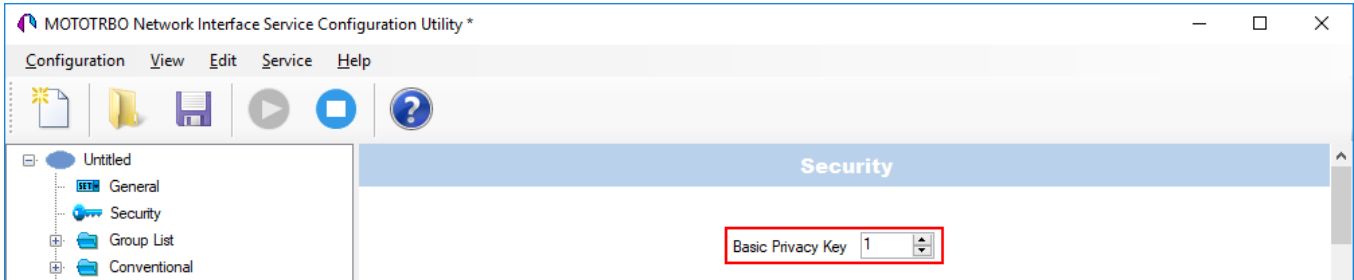
2. In the **Basic Privacy Key** field specify the key for the basic encryption mode. The value ranges from 1 to 255.



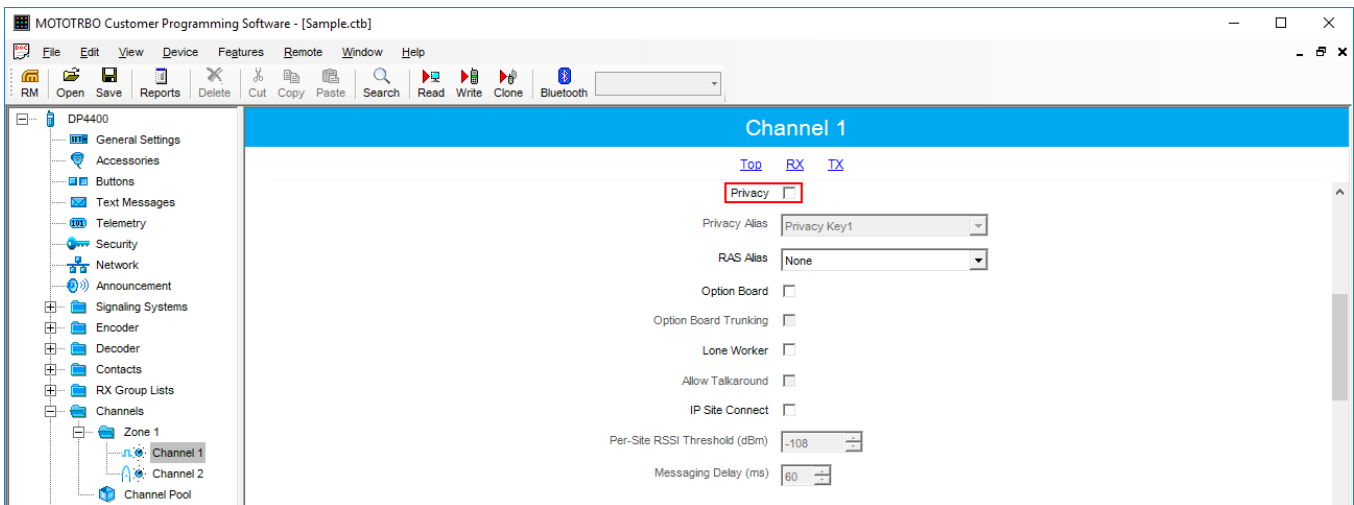
3. In the **Security** window of the repeater settings of *MOTOTRBO CPS* in the **Privacy Type** field, select *Basic*.



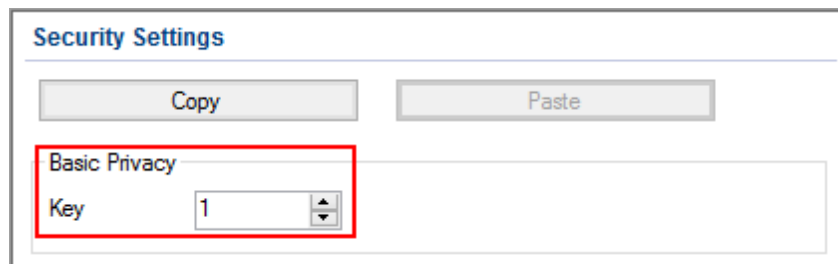
- In the **Security** window of the MNIS in the **Basic Privacy Key** field, specify the key for the basic encryption mode. The value ranges from 1 to 255.



- In the radio settings in *MOTOTRBO CPS*, select the **Privacy** check box to enable the encryption mode on the required channel.





- In the **Security Settings** window of *SmartPTT Radioserver Configurator* in the **Key** field specify the key for the basic encryption mode. The value ranges from 1 to 255.



**NOTE**

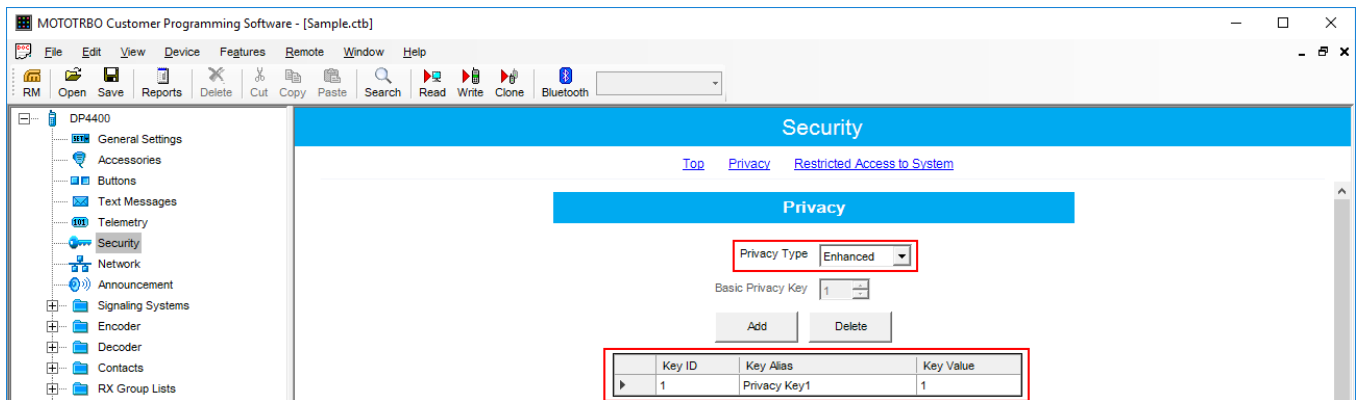
Ensure that the **Key** set in *SmartPTT Radioserver Configurator* matches **Basic Privacy Key** set in the radio settings in *MOTOTRBO CPS* and MNIS. If basic encryption keys of receiving and transmitting sides do not match, the receiving side hears only a distorted voice.

7. Click **Save**  to save changes.
8. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

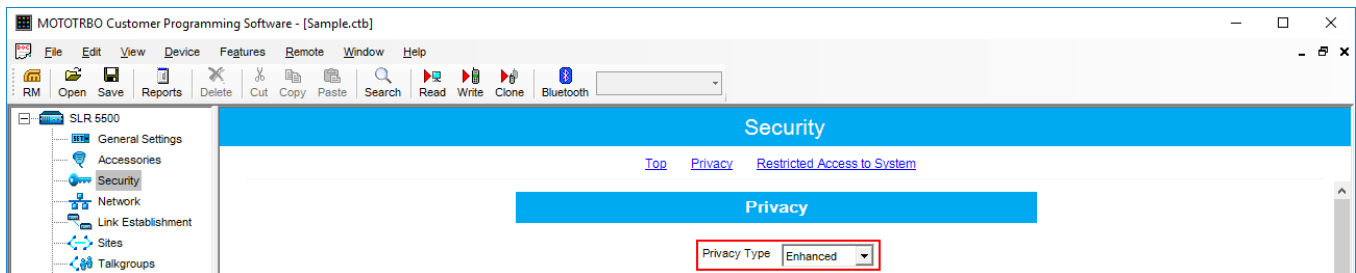
## Enhanced Privacy

To configure **Enhanced Privacy**, follow these steps:

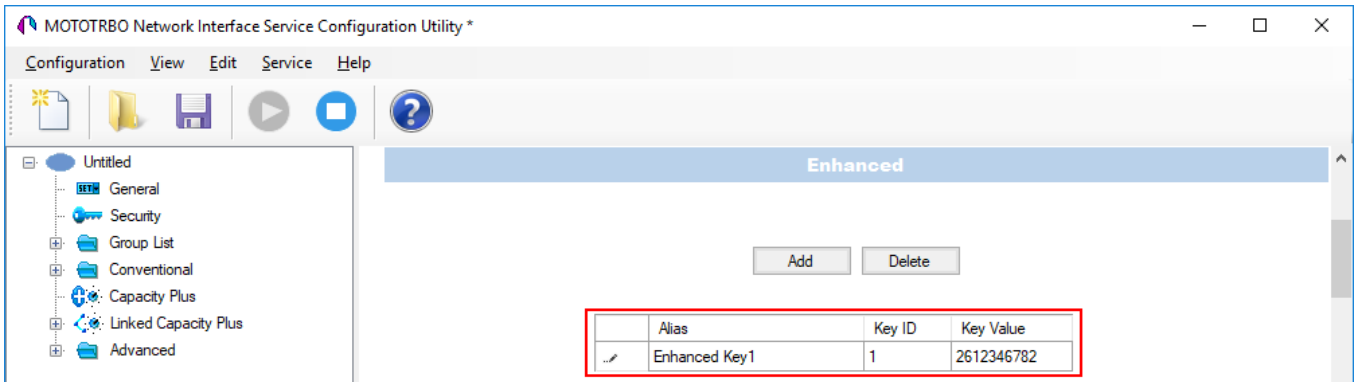
1. Run *MOTOTRBO CPS*.
2. In the **Security** window of the radio settings in *MOTOTRBO CPS* in the **Privacy Type** field select Enhanced and add the enhanced privacy key. Enter its ID and value in the corresponding fields.



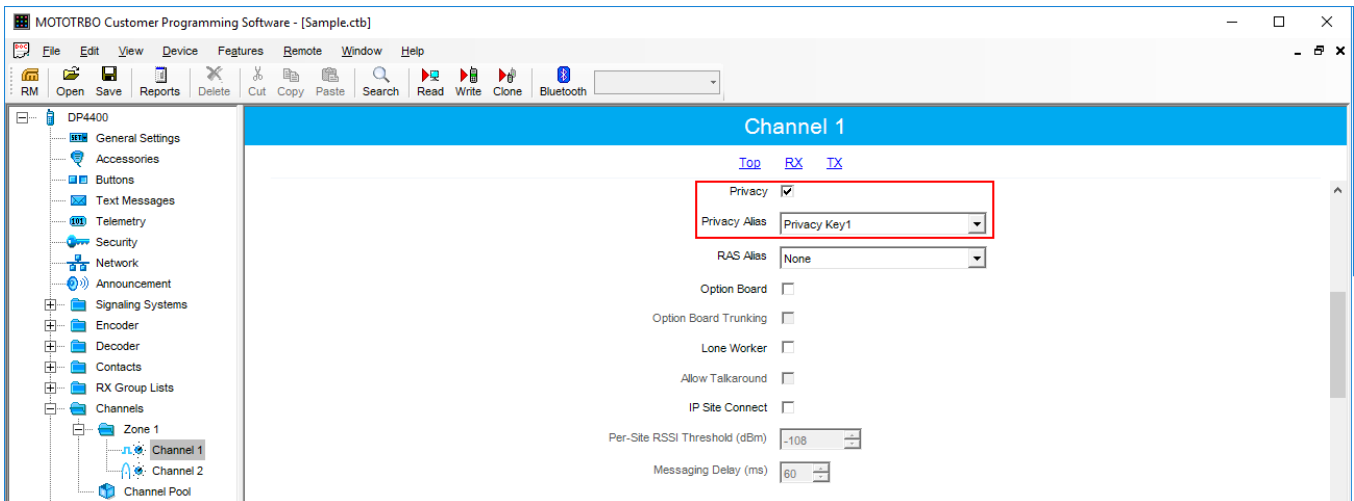
3. In the **Security** window of the repeater settings in *MOTOTRBO CPS* in the **Privacy Type** field select Enhanced.



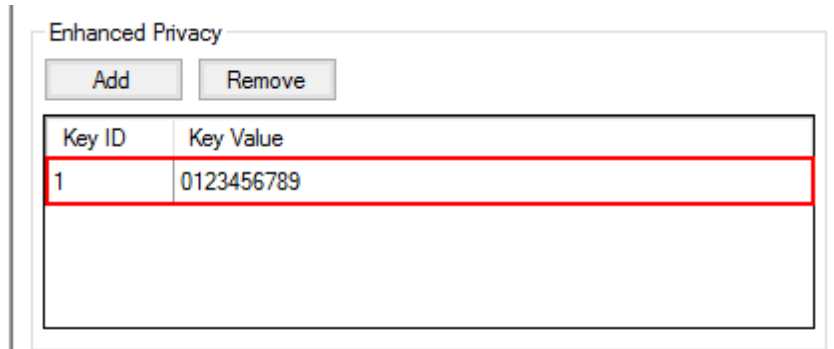
- In the **Security** window of *MOTOTRBO Network Interface Service Configuration Utility* in the **Enhanced** field add the enhanced privacy key. Enter its ID and value in the corresponding fields.



- In the radio settings in *MOTOTRBO CPS* to enable the encryption mode on the required channel select the **Privacy** check box and in the **Privacy Alias** field select the enhanced privacy key for this channel.



- In the **Security Settings** window of *SmartPTT Radioserver Configurator* add an enhanced privacy key for incoming traffic. Enter its ID and value in the corresponding fields.

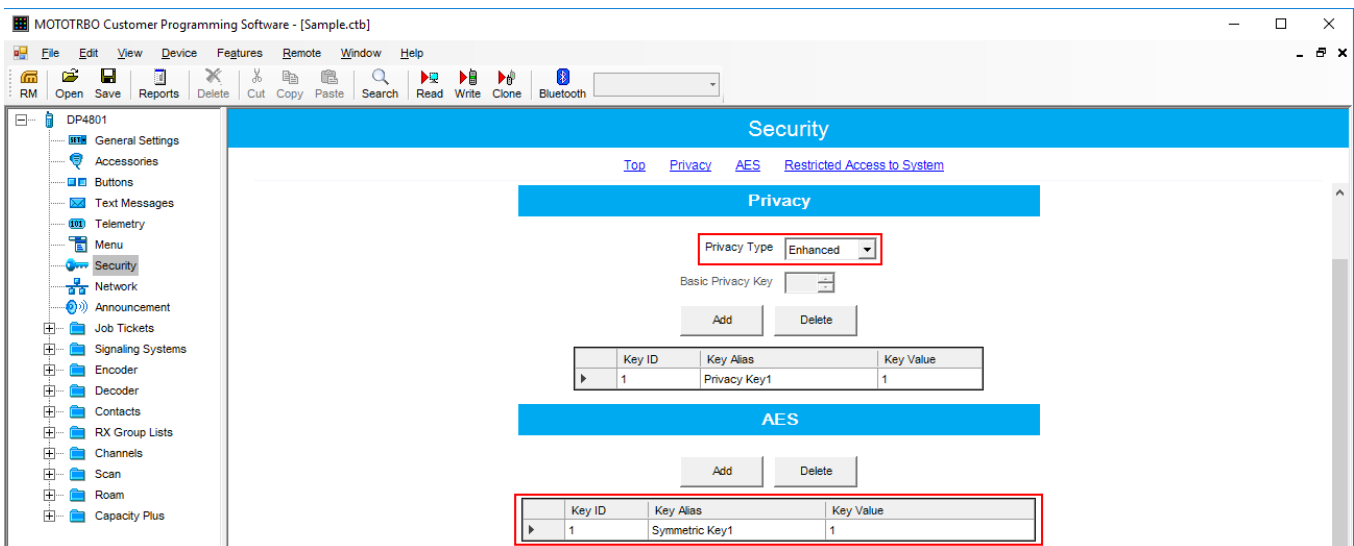


- Click **Save** to save changes.
- Click **Restart** to restart *SmartPTT Radioserver* and apply changes.

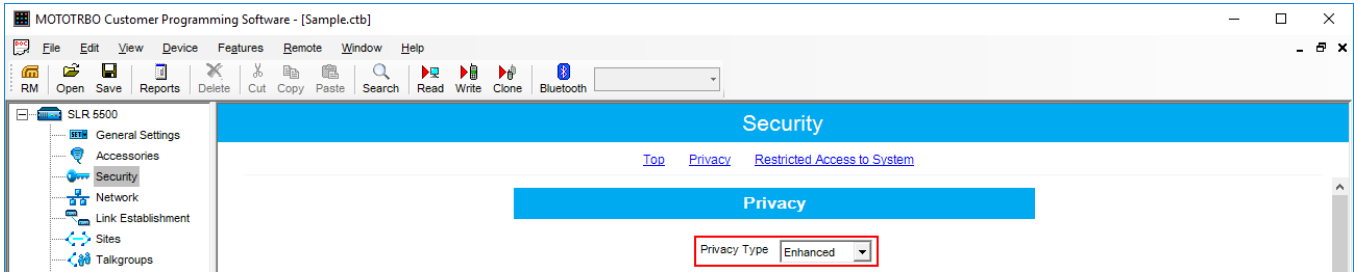
## AES Privacy

To configure the **AES** privacy, follow these steps:

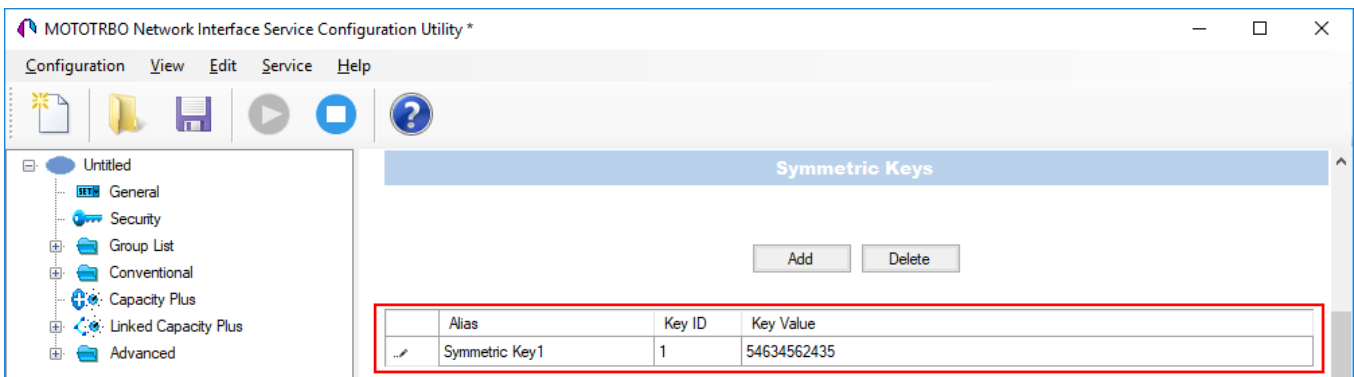
- Run *MOTOTRBO CPS*.
- In the **Security** window of the radio settings in *MOTOTRBO CPS* in the **Privacy Type** field select Enhanced and add the AES privacy key. Enter its ID and value in the corresponding fields.



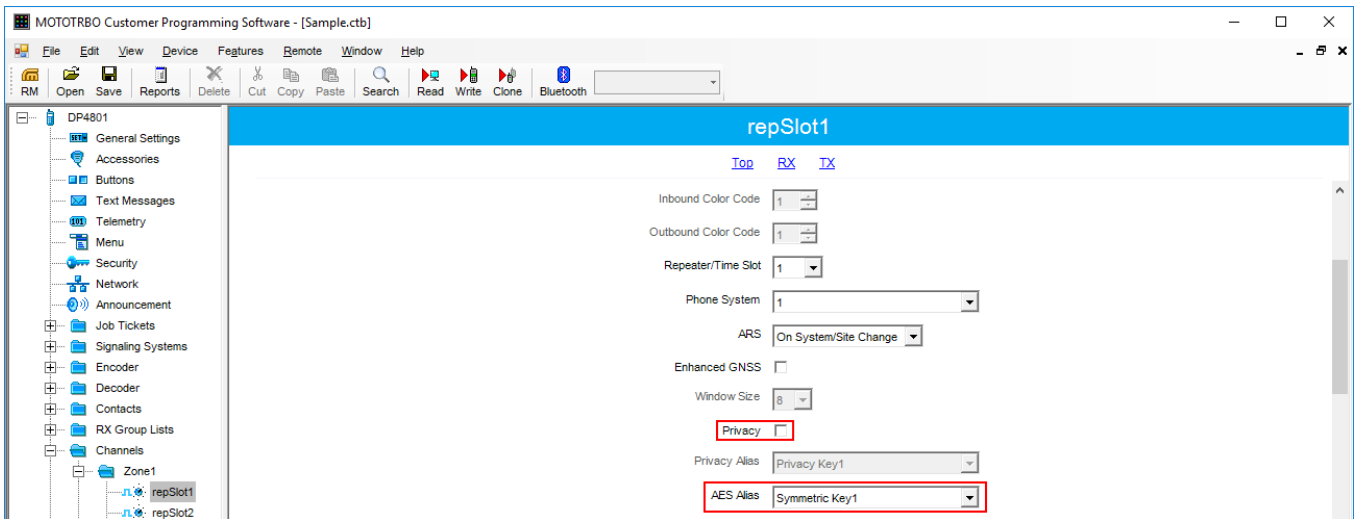
- In the **Security** window of the repeater settings in *MOTOTRBO CPS* in the **Privacy Type** field select **Enhanced**.



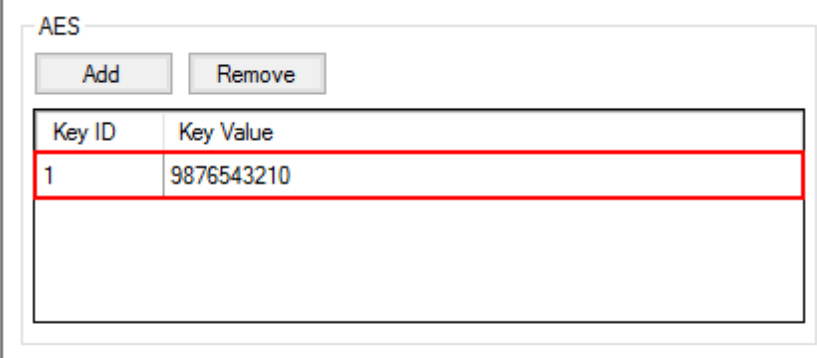
- In the **Security** window of MNIS in the **Symmetric Keys** field add the AES symmetric privacy key. Enter its ID and value in the corresponding fields.



- In the radio settings in *MOTOTRBO CPS* to enable the AES encryption mode on the required channel clear the **Privacy** check box and in the **AES Alias** field select the AES privacy key.





- In the **Security Settings** window of *SmartPTT Radioserver Configurator* add an AES privacy key for incoming traffic. Enter its ID and value in the corresponding fields.



Key ID	Key Value
1	9876543210

**NOTE**

Key ID and Key Value must match the values set in the radio settings in the Radio Management program and in MOTOTRBO Network Interface Service Configuration Utility. If the values in the Key ID fields are the same, but the values in the Key Value fields do not match, the receiving side hears only a distorted voice. If the key identifier of the transmitting side does not coincide with one of the key identifiers in the list of the receiving side, then transfer to the receiving party will not be heard.

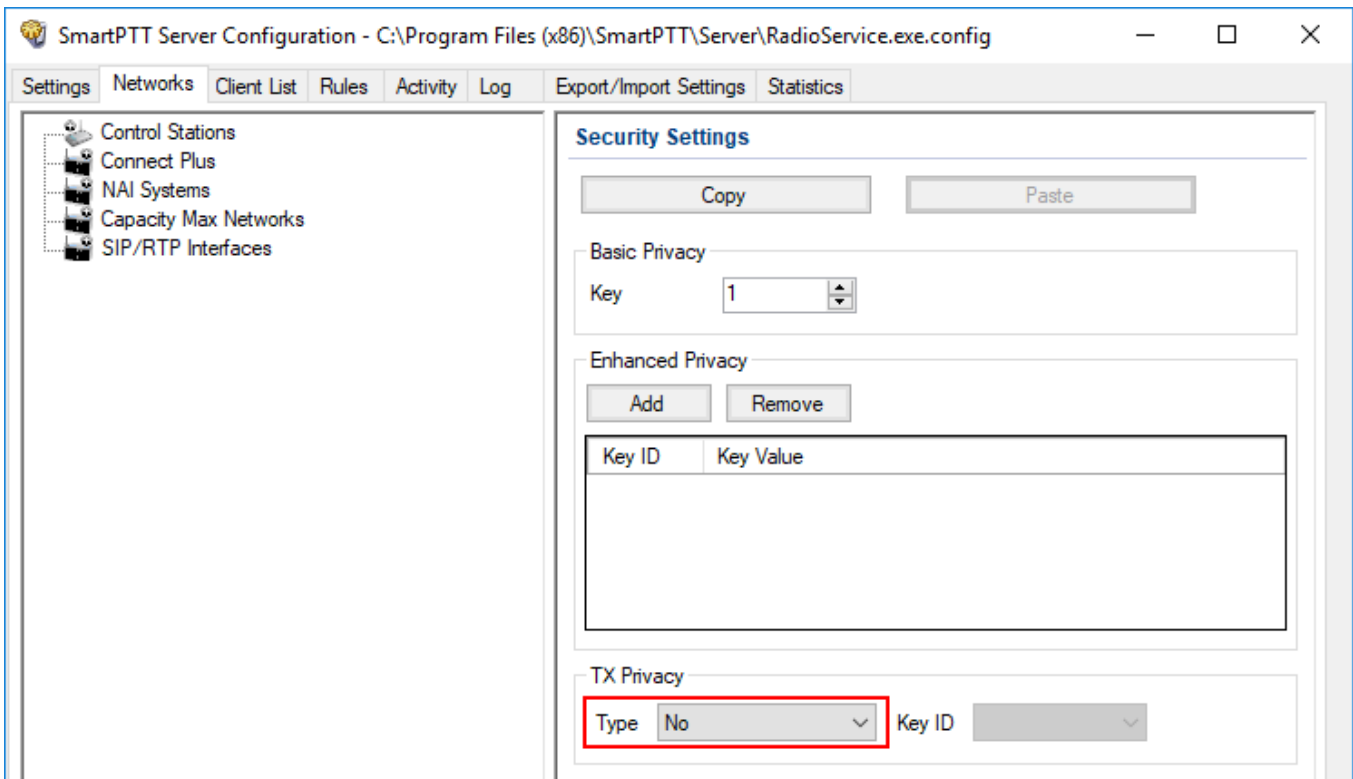
- Click **Save**  to save changes.
- Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

**TX Privacy**

TX Privacy is used for selecting an encryption mode for outgoing traffic on the side of *SmartPTT Dispatcher*.

To configure the TX Privacy for a NAI system, follow these steps:



1. In the **TX Privacy** area, from the **Type** list select the desired encryption type:



- Select *No* if encryption of outbound traffic from the radioserver is not required.
- Select *Basic* if you want to use basic encryption for outgoing traffic from the radioserver. Use the Key ID you specified in the **Basic Privacy** area.
- Select *Enhanced* if you want to use enhanced encryption for outgoing traffic from the radioserver. Use the Key ID you specified in the **Enhanced Privacy** area.
- *AES license is required:* Select *AES (Symmetric Key)* if you want to use AES (Symmetric Key) encryption for outgoing traffic from the radioserver. Use the Key ID you specified in the **AES** area.

#### NOTE

If from the **Type** field *No* is selected and you have AES encryption for incoming traffic configured, AES (Symmetric Key) is used for incoming traffic by default.

2. Click **Save**  to save changes.
3. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.



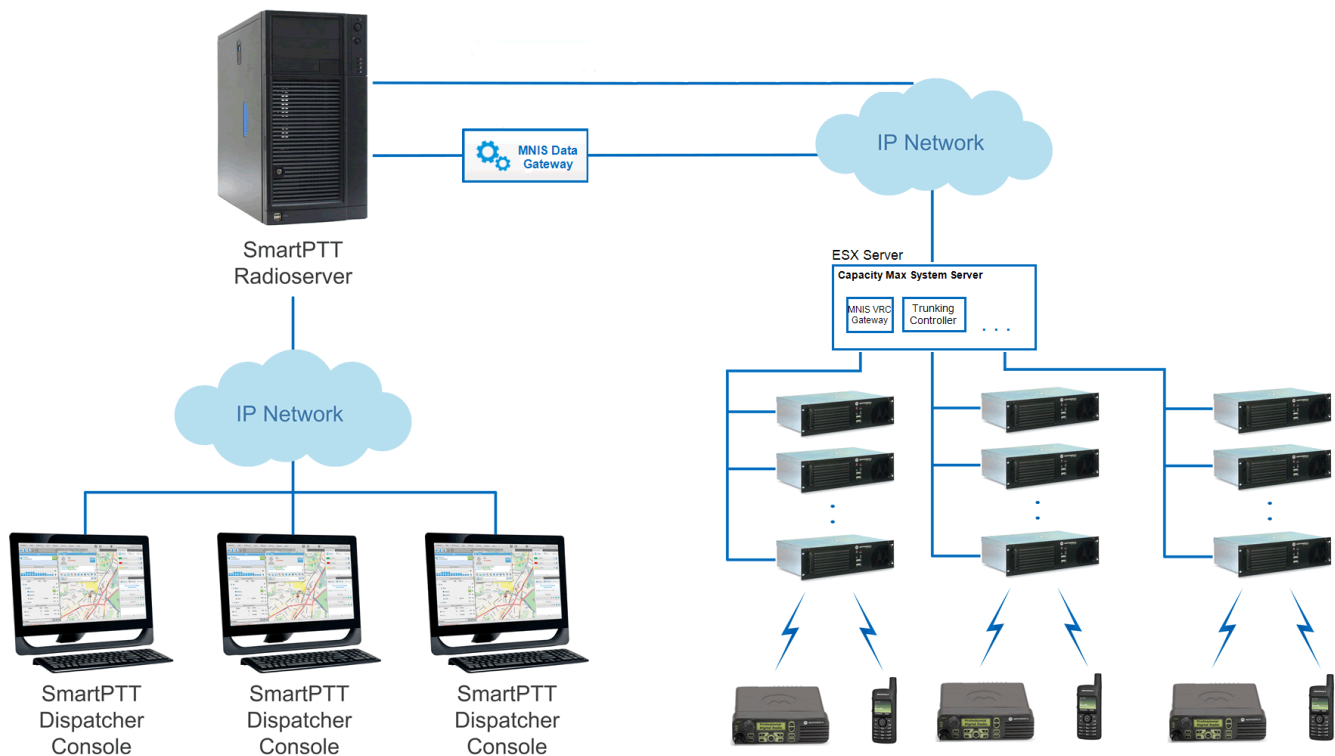
## 2.4 Capacity Max

Capacity Max is a trunking MOTOTRBO system that supports the European Telecommunications Standards Institute (ETSI) Digital Mobile Radio (DMR) Tier III operation.

Capacity Max system represents the enhancement of the Linked Capacity Plus functionality. It can include up to 15 sites and up to 15 trunked repeaters with up to 3,000 users per site. One slot on each site is allocated as a control channel. Capacity Max also supports data revert repeaters: up to 6 per site and 12 time channels per site.

Capacity Max system supports connection by using control stations. The parameters of the control station correspond to the parameters of an ordinary [MOTOTRBO control station](#).

Capacity Max system offers the simple and efficient system architecture that utilizes standard Internet protocol (IP) network with a centralized Capacity Max System Server (CMSS).



CMSS represents the VMware Sphere version 5.5 ESX server and includes the following virtual resources:

- Trunking Controller based on the Red Hat Linux
- MNIS VRC gateway

- Radio Management application that is used instead of *MOTOTRBO Customer Programming Software* (MOTOTRBO CPS) to configure the system

The system architecture also includes the MNIS Data Gateway, which is installed separately.

- High security. All voice, data and control traffic within the IP network is encrypted, and all radios are securely authenticated
- High level of reliability and resilience. The system can include an optional redundant server in addition to the main server and up to three alternate control channels per site

Capacity Max is compatible with all MOTOTRBO repeaters, except DR3000 series with the 8MB RAM, and all MOTOTRBO 4000 series portable and/or mobile radio stations.

To configure the Capacity Max system in *SmartPTT Radioserver Configurator*, you should have the following programs installed:

- *Radio Management* – to get the settings of the preconfigured virtual resources
- *MOTOTRBO Network Interface Service Configuration Utility* – to set up the MNIS Data Gateway

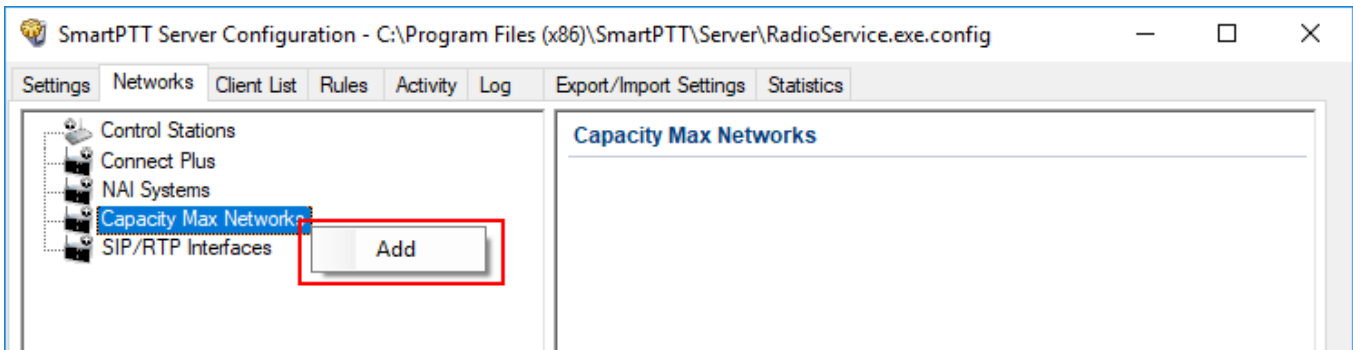
Capacity Max configuration in *SmartPTT Radioserver Configurator* includes the following steps:

- [Adding a new network and performing its basic configuration](#)
- Setting up the [Trunking Controller](#)
- Setting up [MNIS Data Gateway settings](#) for data transfer
- Setting up the [MNIS VRC Gateway](#) and the talkgroups
- Setting up the [security settings](#)

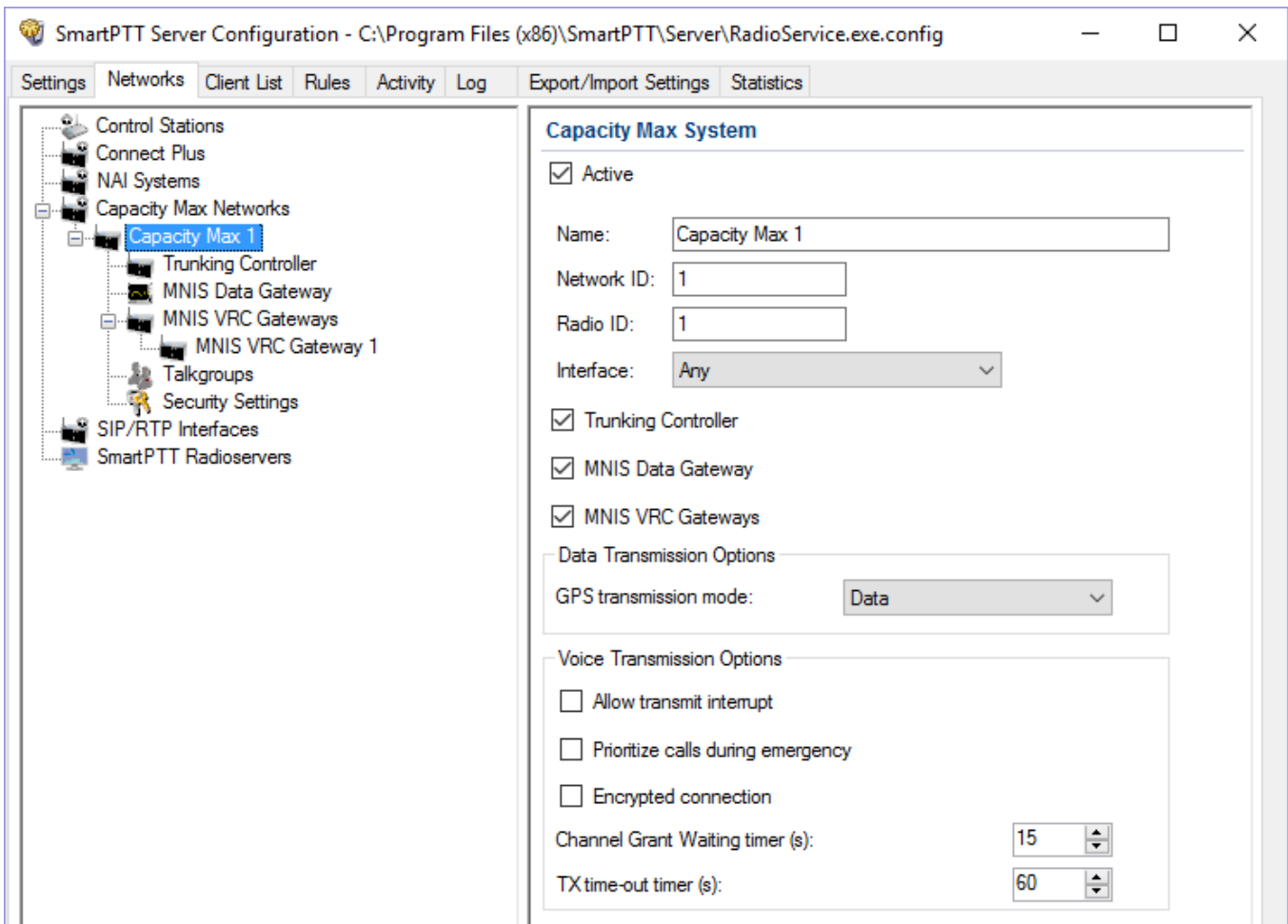
## 2.4.1 Configuring Capacity Max

To connect a new Capacity Max system to the SmartPTT Radioserver, follow these steps:

1. On the **Networks** tab, right-click **Capacity Max Networks** and then click **Add**.



2. Select the created Capacity Max system. The **Capacity Max System** pane appears:




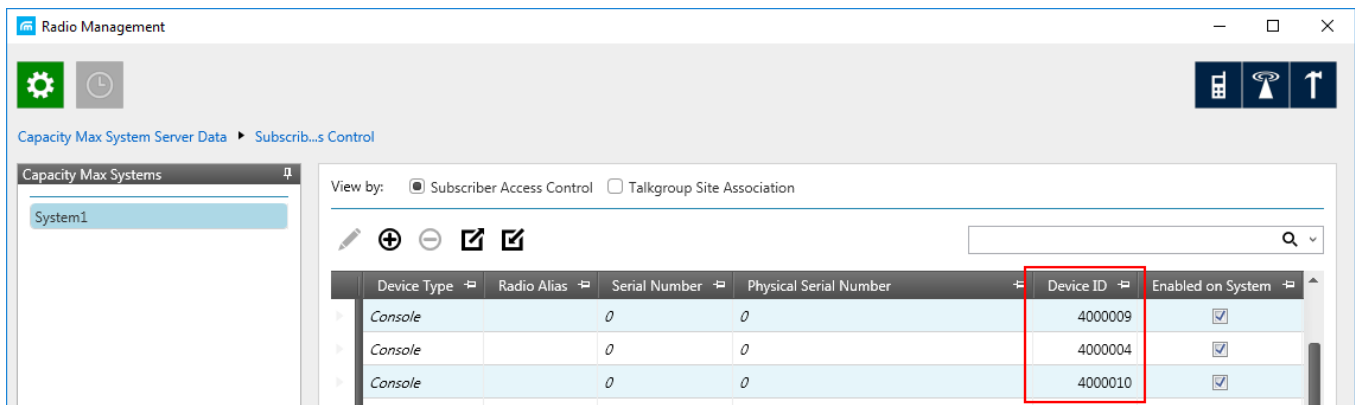
3. In the **Capacity Max System** pane, configure the available options:

**Name:** Name of the created system.

**Network ID:** Unique ID of the network. The network ID must not match any ID of other SmartPTT Radioserver networks

**Radio ID:** The identifier of the radioserver. This identifier is displayed on a radio when it receives private calls and text messages from the dispatcher. If there are several dispatchers, you can create a profile for each operator and define a unique identifier for each operator. **Radio ID** set in this window must correspond to the value set in the **Device ID** field for the preconfigured radioserver device in the *Radio Management* application (see the **Capacity Max Systems** settings, viewed by the **Subscriber Access Control** value).

To open the **Capacity Max System** settings in the *Radio Management* application, click **Action**  → **Manage** → **Capacity Max System Server Data** or press Ctrl+Alt+S.



**Interface:** The IP address of the computer where SmartPTT Radioserver is installed.

**Trunking Controller:** Select to allow the connection to [Trunking Controllers](#).

**MNIS Data Gateway:** Select to allow a connection to a [MNIS Data Gateway](#) and its use.

**MNIS VRC Gateways:** Select to allow a connection to a [MNIS VRC Gateway](#) and its use.



**Allow transmit interrupt:** Select if you want to interrupt a radio.

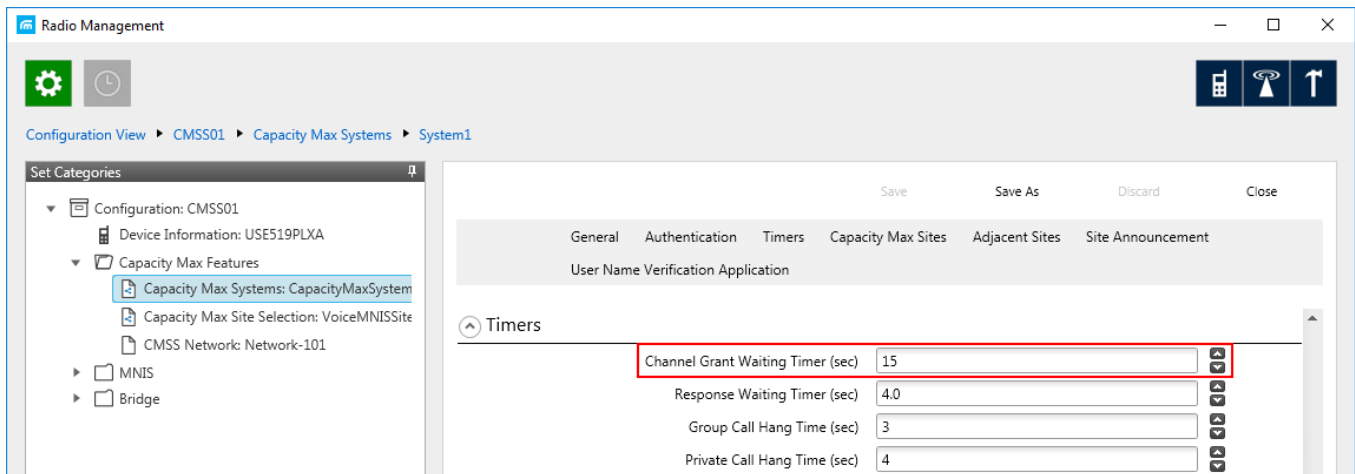
**Prioritize calls during emergency:** Sets a priority of the dispatcher call during the Emergency Call. If the check box is selected, the dispatcher call has the highest priority during the Emergency Call in relation to other calls and interrupts them in case of lack of resources.

**Encrypted connection:** Select to activate encrypted TLS connection between radioserver and voice gateway.

**Channel Grant Waiting timer (s):** Time period in seconds during which the caller expects a response from the called party (the FOACSU strategy). It is recommended to use the default value of 15 seconds that is set in *Radio Management* (see the **Capacity Max Systems:...** settings in the Capacity Max Features menu of the CMSS configuration, the **Channel Grant Waiting timer** field in the **Timers** tab).

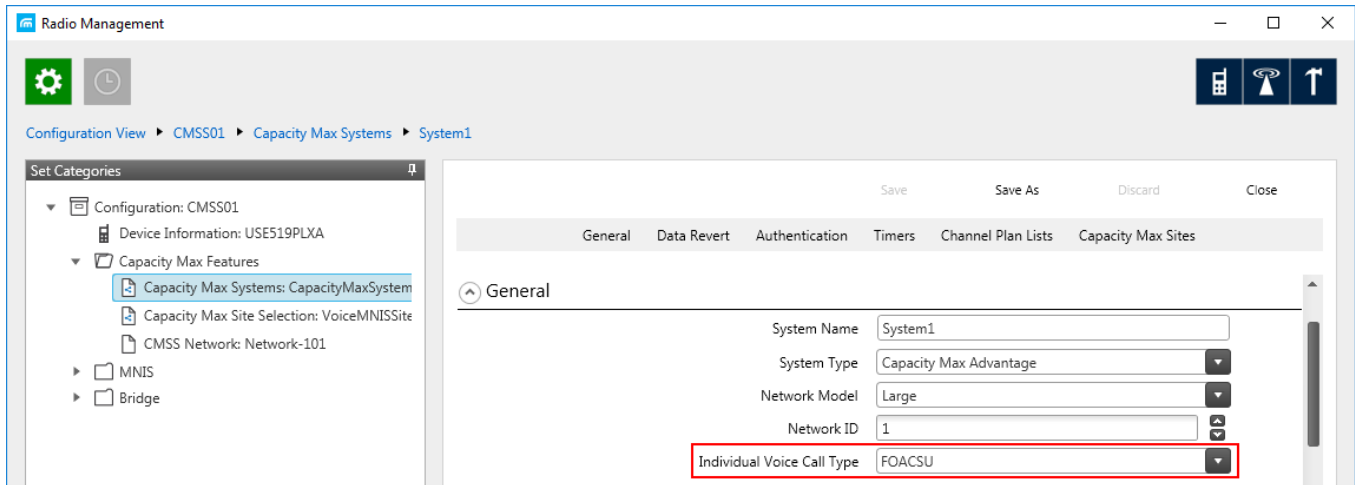
#### NOTE

To open the **Capacity Max Features** of the of the CMSS configuration in the *Radio Management* application, click **Action**  → **Manage** → **Configurations** or press Alt+C. In the open table, select the CMSS configuration and click **Edit** . In the open **Set Categories** pane, expand **Configuration:<CMSS configuration name>** and select **Capacity Max Features**.



FOACSU (Full Off Air Call Set Up) stands for the strategy of assigning the traffic channel only when the called party user answered the call specifically. During the timeout the traffic channel is not allocated for the call.

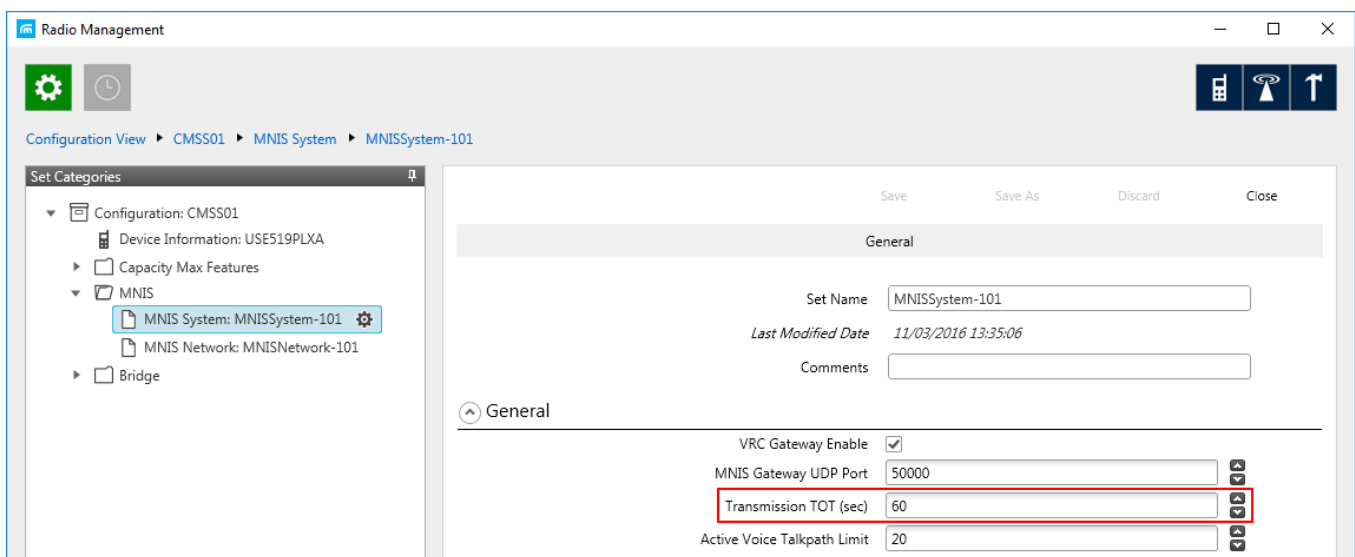
For the correct work of the FOACSU private calls, ensure it is configured in *Radio Management* (see the **Capacity Max Systems:...** settings in the [Capacity Max Features](#) menu of the CMSS configuration, the **Individual Voice Call Type** field in the **General** tab).



**TX time-out timer (s):** Time period during which the radio can transmit without interruptions. After this time is over, the transmission is interrupted. We recommend you to use the default value of 60 seconds, which is set in *Radio Management* (see the **MNIS System** settings in the **MNIS** menu of the CMSS configuration, the **Transmission TOT** field in the **General** tab).

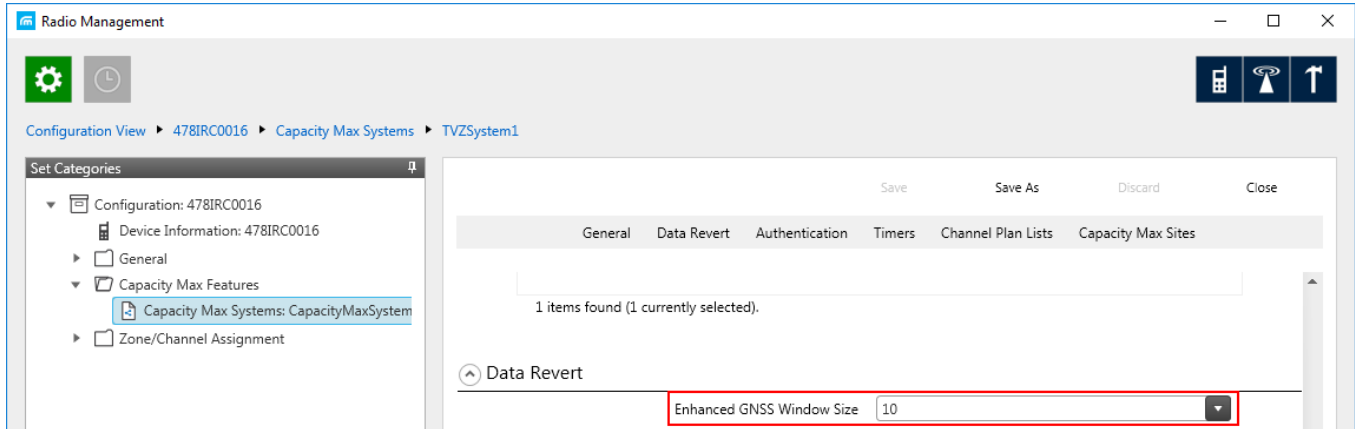
#### NOTE

To open the **MNIS** menu of the **CMSS configuration** in the *Radio Management* application, click **Action** → **Manage** → **Configurations** or press Alt+C. In the open table, select the CMSS configuration and click **Edit** . In the open **Set Categories** pane, expand **Configuration: <CMSS configuration name>** and select **MNIS** → **MNIS System**.



**GPS Transmission Mode:** Select the suitable mode:

- **Data:** GPS coordinates will be received in several packets. This mode is working only if **Trunking channel** is set in *Radio Management*. However, traffic is consumed in this mode.



- **Enhanced CSBK:** GPS coordinates will be sent as a single Control Signaling Block. This is traffic-effective option and it allows to increase GPS request rate up to 7.5 s. However, you should make sure that radio units in your system support CSBK commands.


## 2.4.1.1 Configuring Joint GPS and Indoor Data

If you want to receive joint location data (GPS and indoor) in Capacity Max, configure the following settings:

- Radio settings in *Radio Management*
- Radio settings in SmartPTT Dispatcher
- Repeater settings in *Radio Management*
- Capacity Max settings in *Radio Management*

### 2.4.1.1.1 Configuring Capacity Max in Radio Management

To configure Capacity Max in *Radio Management*, follow these steps:

1. Click **Actions** , and select **Manage** → **Sets**, or press Alt+S.
2. In the **Set Categories** pane, select **Capacity Max features** → **Capacity Max Systems**.

3. In the left column of the table, click ▶ to select the desired **Capacity Max** system.
4. Click **Edit** ✎.
5. In the **Data Revert** tab, from the **Enhanced GNSS Window Size** list, select the value *10*.
6. Save changes.

### 2.4.1.1.2 Configuring Repeater in Radio Management

To configure Capacity Max in *Radio Management*, follow these steps:

1. Click **Actions** ⚙️, and select **Manage** → **Sets**, or press Alt+S.
2. In the **Set Categories** pane, select **Capacity Max features** → **Capacity Max Systems**.
3. In the left column of the table, click ▶ to select the desired **Capacity Max** system.
4. Click **Edit** ✎.
5. In the **Capacity Max Sites** tab, perform the following actions:
  - a. In the left column of the table, click ▶ to select the desired **Capacity Max** system.
  - b. Click **Edit** ✎.
6. In the **Capacity Max Channels** tab, perform the following actions:
  - a. In the left column of the table, click ▶ to select the desired **Capacity Max** system.
  - b. Click **Edit** ✎.
7. In the **General** tab, from the **Channel Type** list, select *Data Revert Channel*.
8. Save changes.

### 2.4.1.1.3 Configuring Radio in Radio Management

To configure radio in *Radio Management*, follow these steps:

1. Click **Radio View** 📄.
2. In the left column of the table, click ▶ to select the desired radio.
3. Click **Edit** ✎.



4. In the **Set Categories** pane, perform the following actions:
  - a. Expand **Configuration** → **Zone/Channel Assignment** → **Zone**.
  - b. Select the desired Capacity Max zone.
5. In the left column of the table **Zone Items**, click ▶ to select the desired channel.
6. Click **Edit** ✎.
7. In the **General** tab, from the **Compressed UDP Data Header** list, select *DMR Standard*.
8. In the **RX/TX** tab, clear the **CSBK Data** check box.
9. Save changes.

#### 2.4.1.1.4 Configuring Radio in SmartPTT Dispatcher

To configure radio in SmartPTT Dispatcher, follow these steps:

1. Open the radio properties window.
2. In the **Location** tab, perform the following actions:
  - a. Select the **Indoor Tracking** check box.
  - b. Select the **Update Interval** check box, and enter 30 in the field.

## 2.4.2 Configuring Trunk Controller

Trunking controller of the Capacity Max network provides actual information about the network status (registered radios).

### NOTE

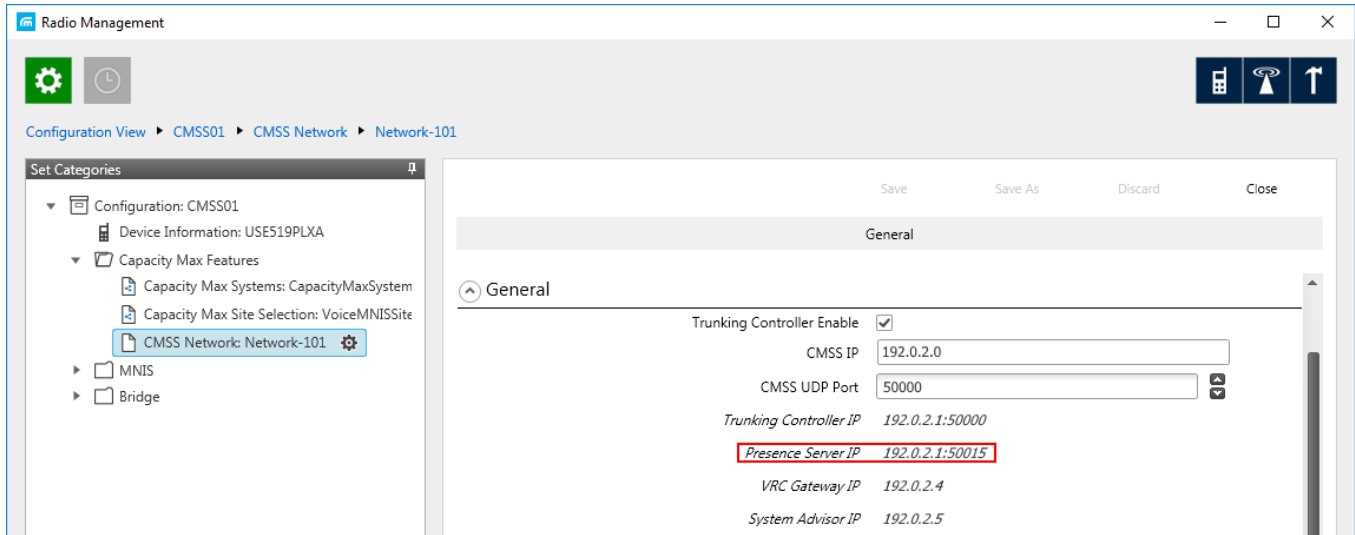
To configure trunk controller, install the corresponding license. For more information on how to install licenses, see [Licenses](#).

To configure a primary trunking controller, follow these steps:

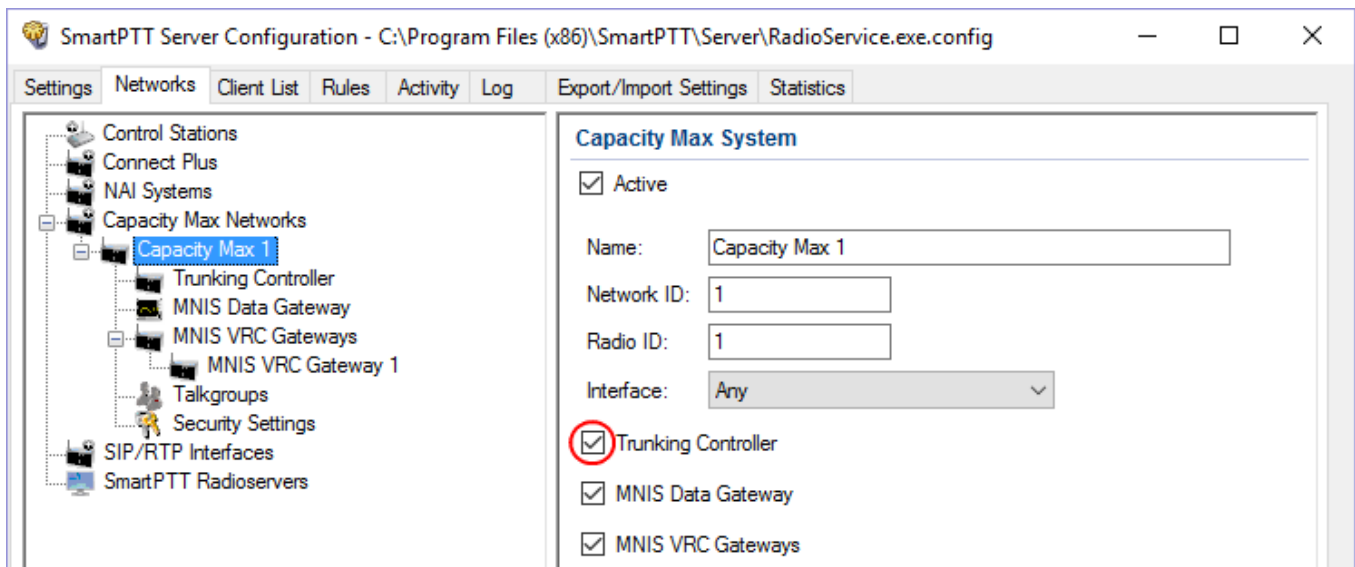
1. Ensure trunking controller is configured by using the *Radio Management* application, in particular, you can obtain IP address and port from the **Presence Server IP** field.

## NOTE

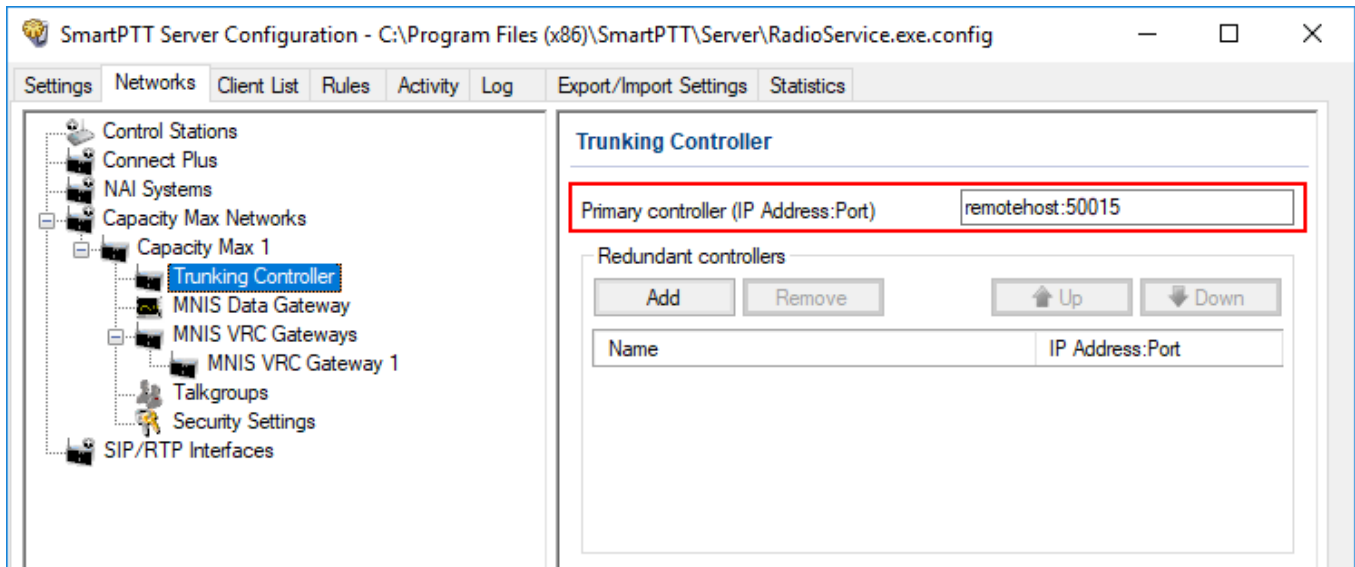
For more information on how to configure Radio Management application, see *Motorola Radio Management User Guide*.



2. [Add a new Capacity Max network](#) or select the existing one.
3. In the **Capacity Max System** pane, select the **Trunking Controller** check box to make trunking controller settings available.



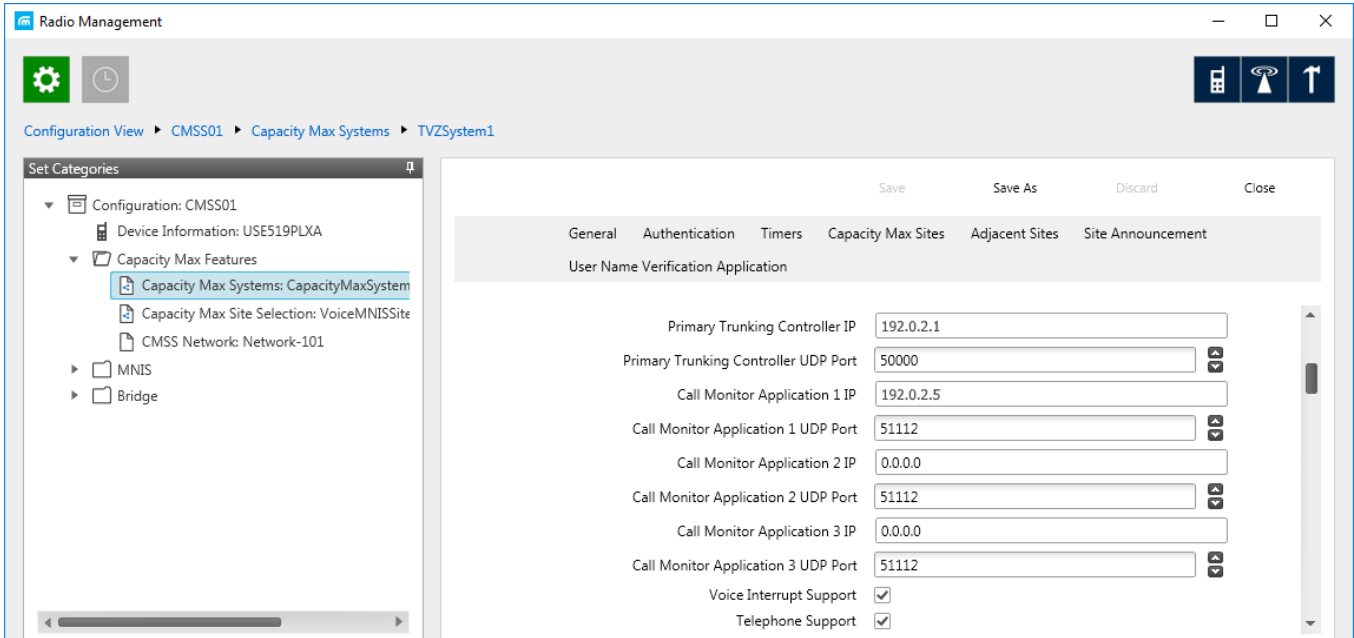
4. In the left pane, select **Trunking Controller** and in the **Trunking Controller** pane replace the default text "*remotehost:50015*" in the **Primary controller (IP address:Port)** field with IP address and port of the Presence Server from the *Radio Management* application.



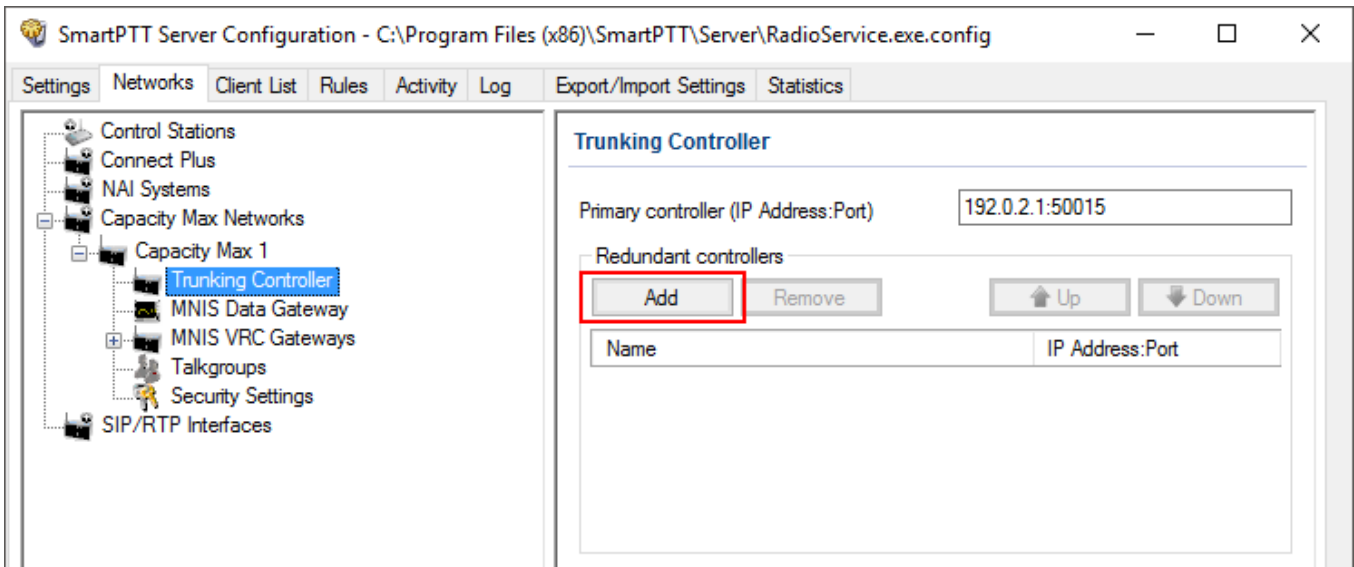
Capacity Max supports up to 4 redundant trunking controllers to keep the radios online when the primary controller goes offline. The order of redundancy is defined by the settings in the *Radio Management* application.

To configure additional trunking controllers:

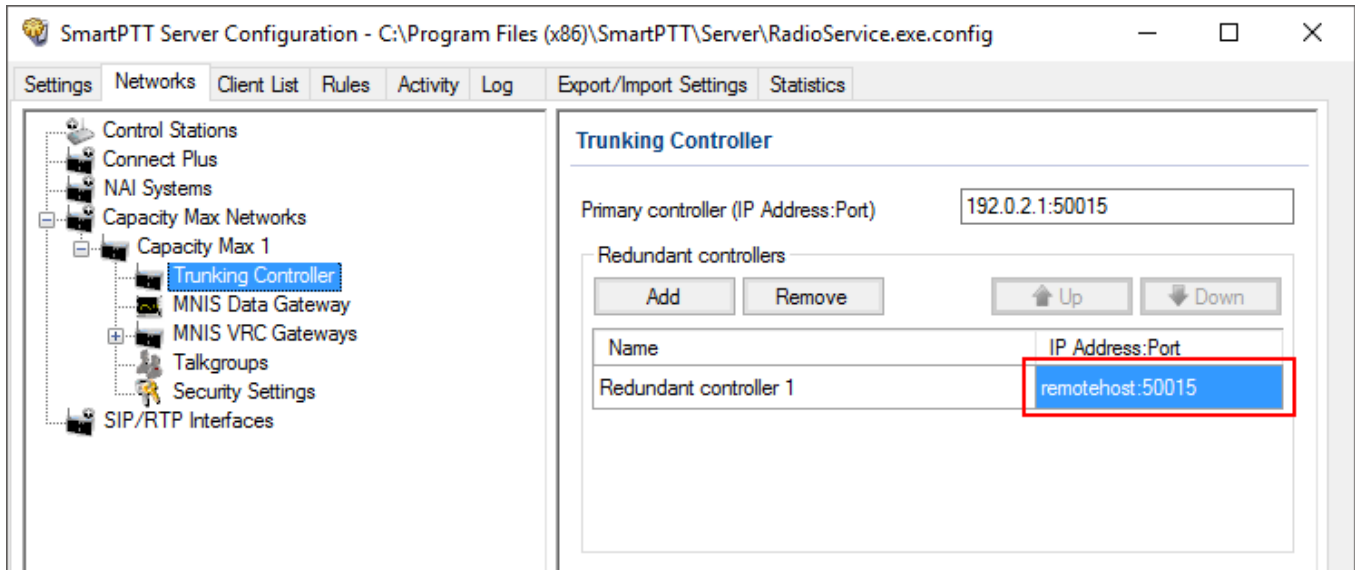
1. Make sure that redundant trunking controllers are configured in the *Radio Management* application.



2. In your Capacity Max network select **Trunking controller**.
3. In the **Redundant controllers** area, click **Add** to add a new controller to the table.



- Change the redundant controller IP address and port according to the settings in the *Radio Management* application. Rename the controller if needed. You should name controllers differently.



- Add more redundant controllers if needed. Change their IP addresses and ports according to the settings in the *Radio Management* application.

#### NOTE

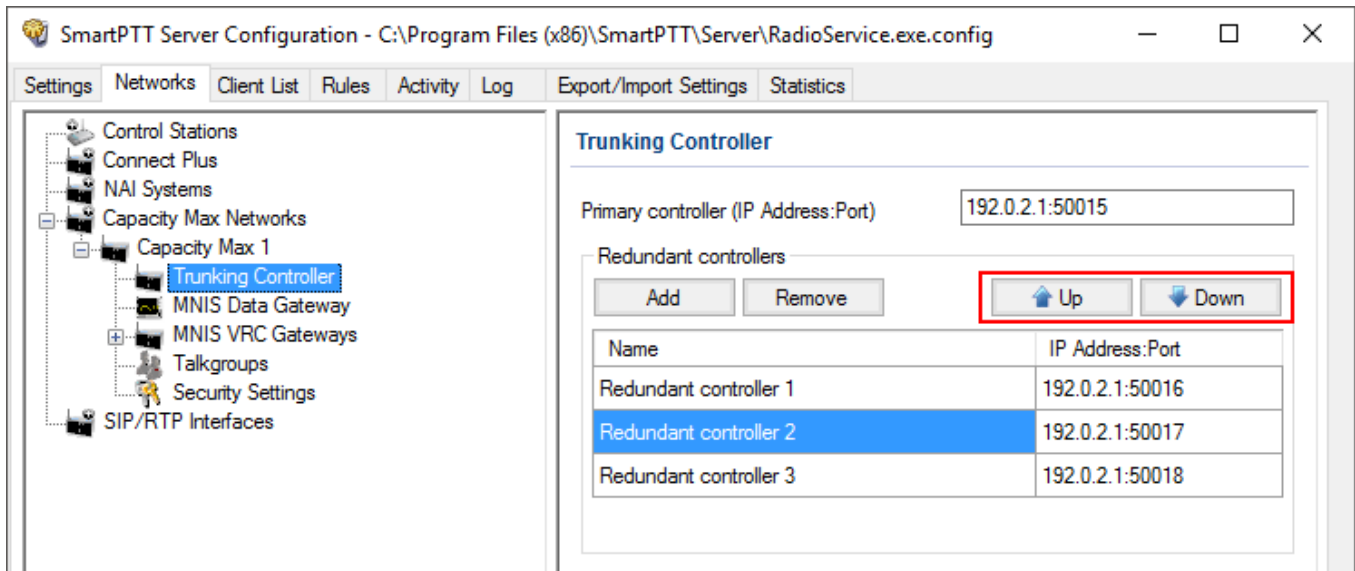
If ports of some controllers are the same, the exclamation mark **!** appears near them. You cannot switch to another menu until you change the ports.

You can change the order of the redundant controllers in the table. This helps to assign a new active controller in case when others disconnect from each other.

To change the order of the controllers in the table, follow these steps:

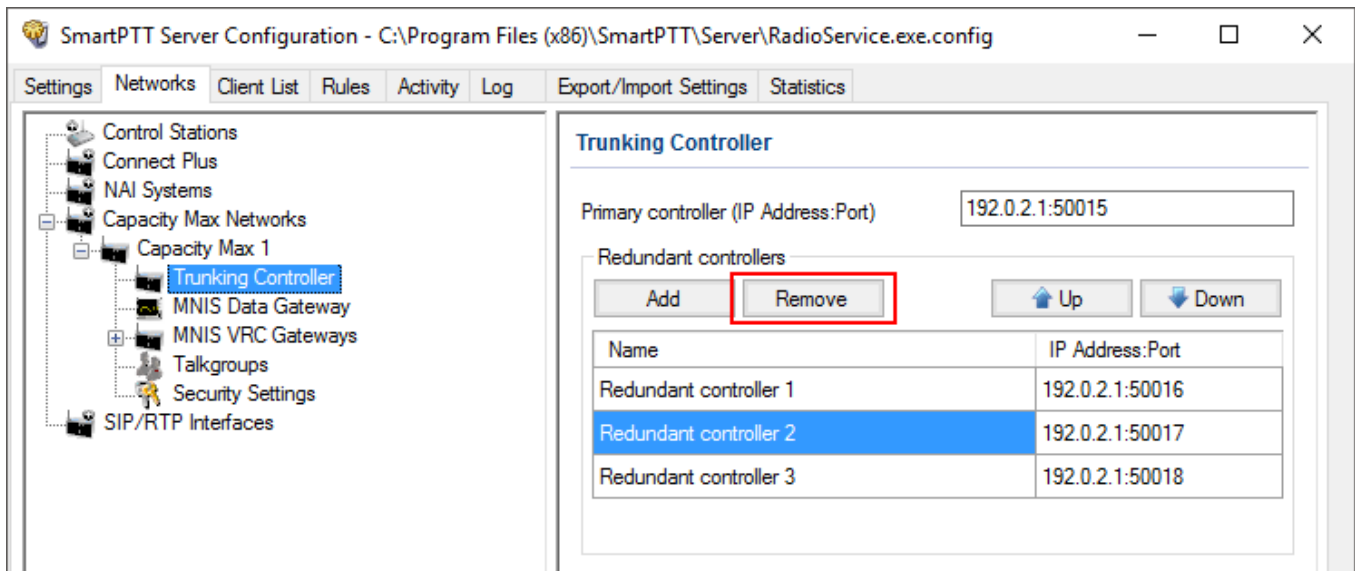
- Select the desired redundant controller.

2. Click **Up** or **Down** to move the redundant controller up and down.



To delete a redundant trunking controller from the table, follow these steps:

1. In your Capacity Max network select **Trunking Controller**.
2. In the **Redundant Controller** area, in the table select a redundant controller and click **Remove**.



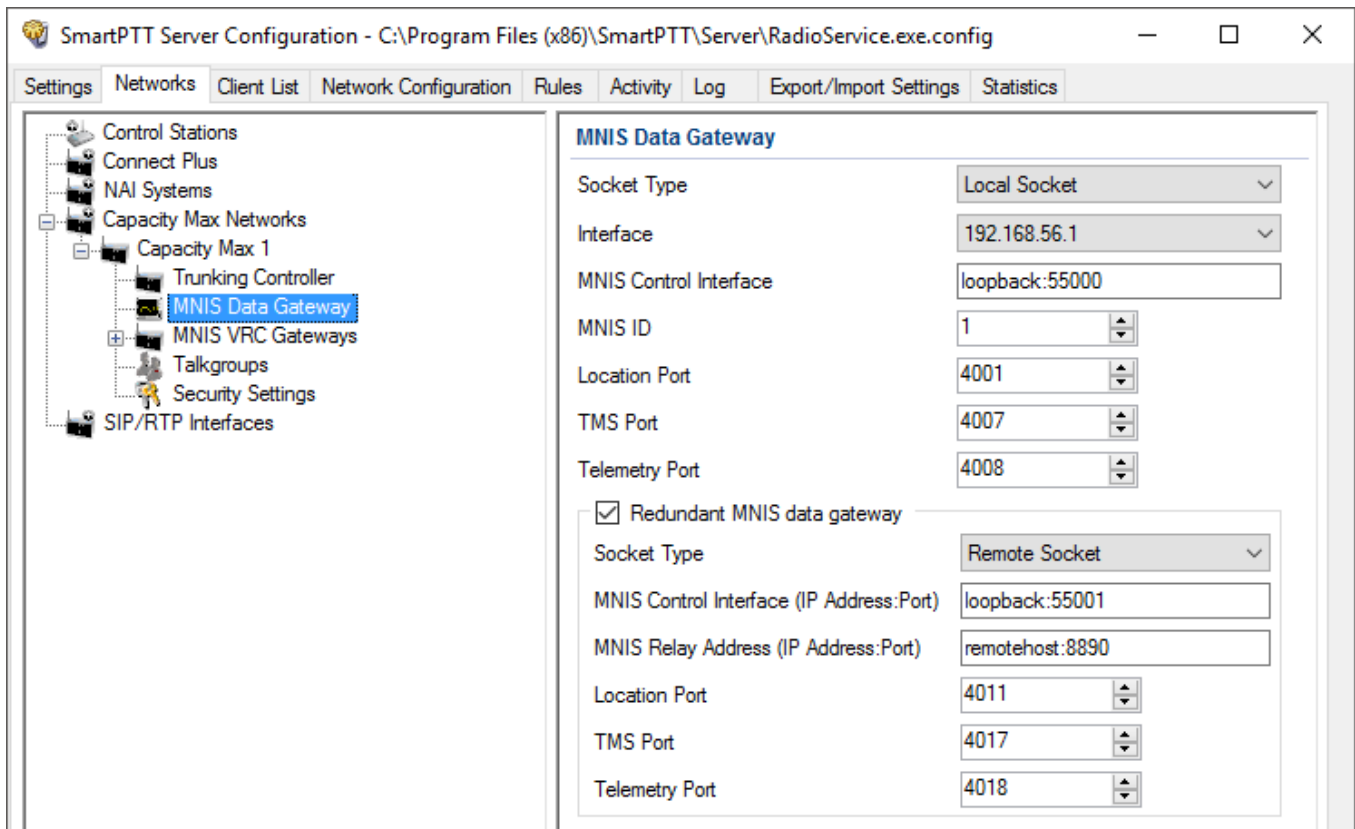
## 2.4.3 Configuring MNIS Data Gateway

To configure data transfer over Capacity Max network, configure MNIS Data Gateway settings in *SmartPTT Radioserver Configurator* and in *MOTOTRBO Network Interface Service Configuration Utility*.

### NOTE

To configure data transfer, install the corresponding license. For more information on how to install licenses, see [Licenses](#).

To configure MNIS Data Gateway settings in SmartPTT Radioserver, click **Capacity Max Networks** → **Capacity Max** → **MNIS Data Gateway**.



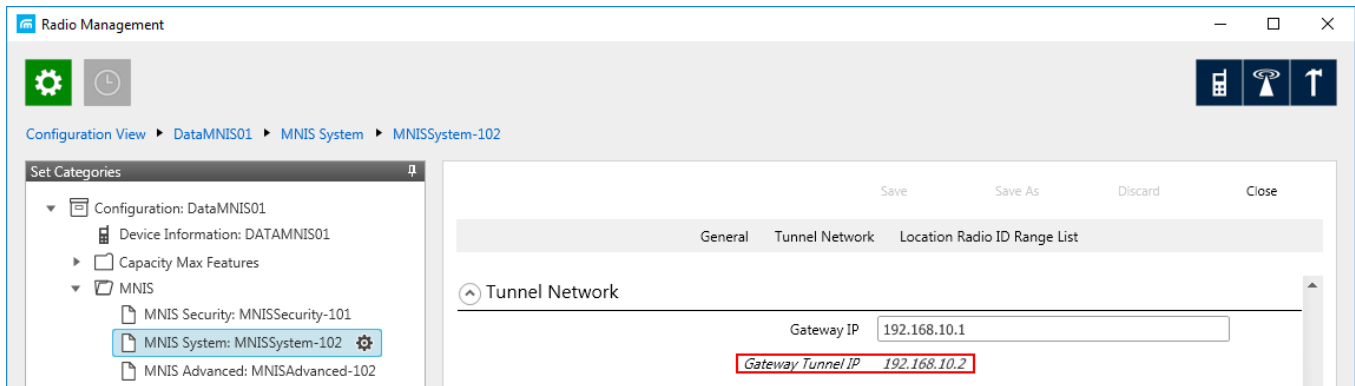
### NOTE

The **Data transmission** check box in the **Capacity Max** window should be selected. Otherwise, the **MNIS Data Gateway** parameter will not be shown.

**Socket Type:** Defines the software interface type to enable communication between processes. Select the *Local Socket* value if the *MOTOTRBO Network Interface Service Configuration Utility* is installed on the same PC as SmartPTT Radioserver. Select *Remote Socket* if the *MOTOTRBO Network*

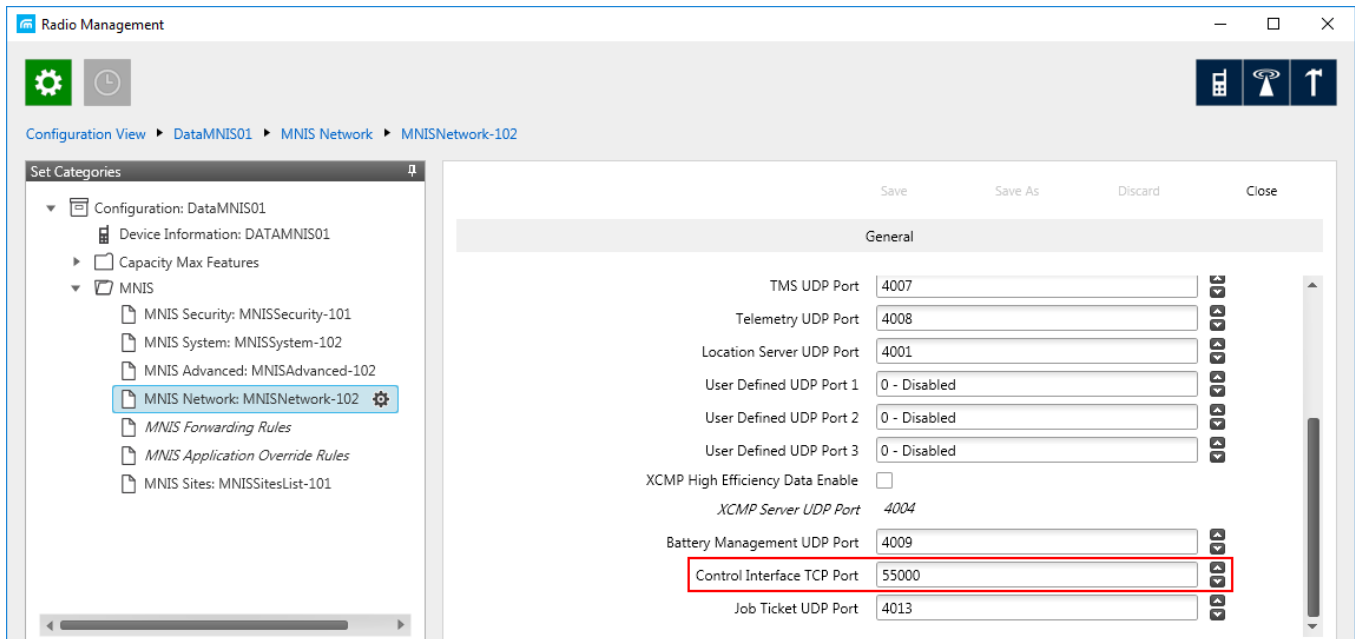
*Interface Service Configuration Utility* and SmartPTT Radioserver are installed on a different PCs. In this case, information exchange between the processes is supported by the MNIS Relay application.

**Interface:** MNIS interface. It must match the interface specified in the *Radio Management* application (see the **MNIS System** settings in the MNIS menu of the **DataMNIS\_Config** configuration, the **Gateway Tunnel IP** field in the **Tunnel Network** tab).






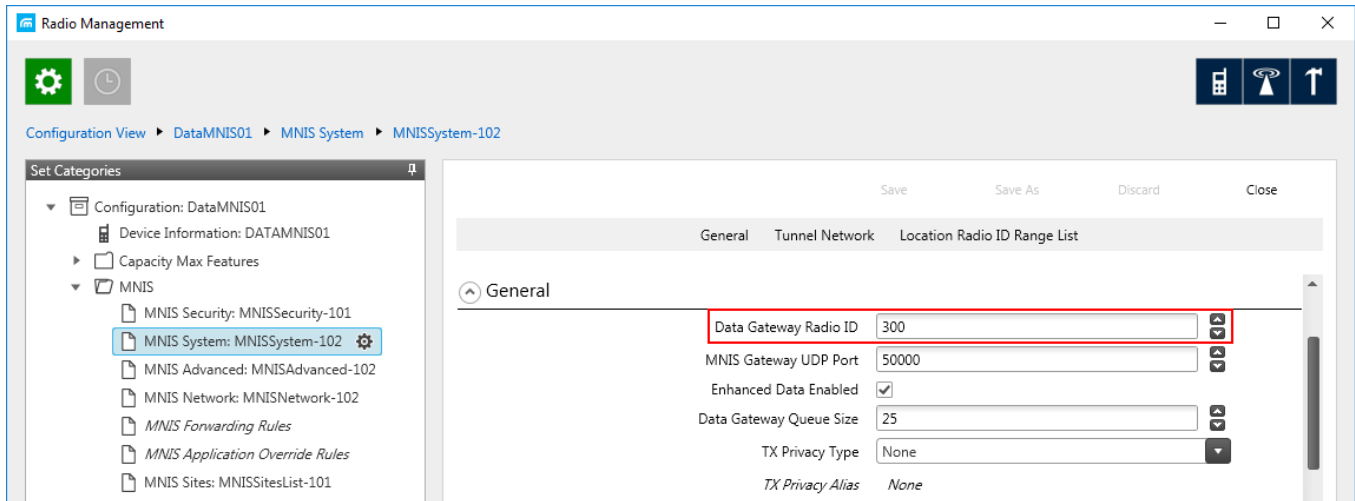
**MNIS Control Interface:** Use *localhost*, if *MOTOTRBO Network Interface Service Configuration Utility* is installed on the same PC as the radioserver. If *MOTOTRBO Network Interface Service Configuration Utility* and the radioserver are installed on different PCs, enter the IP address of the PC where *MOTOTRBO Network Interface Service Configuration Utility* is installed. The port should match the port number specified in the *Radio Management* application (see the **MNIS Network** settings in the **MNIS** menu of the **DataMNIS\_Config** configuration, the **Control Interface TCP Port** field in the **General** tab).



## NOTE

To open the **MNIS** menu of the DataMNIS configuration in the *Radio Management* application, click **Action**  → **Manage** → **Configurations** or press Alt+C. In the open table, select the DataMNIS and click **Edit**. In the **Set Categories** pane that opened, click **Configuration: <DataMNIS name>** → **MNIS**.

**MNIS ID:** The Common Air Interface (CAI) ID of the MNIS in the radio network. The ID is used by other calling radios when addressing *MOTOTRBO Network Interface Service Configuration Utility*. Verify **MNIS ID** matches the corresponding field in the *Radio Management* application (see the **MNIS System** settings in the **MNIS** menu of the DataMNIS configuration, the **Data Gateway Radio ID** field in the **General** tab).

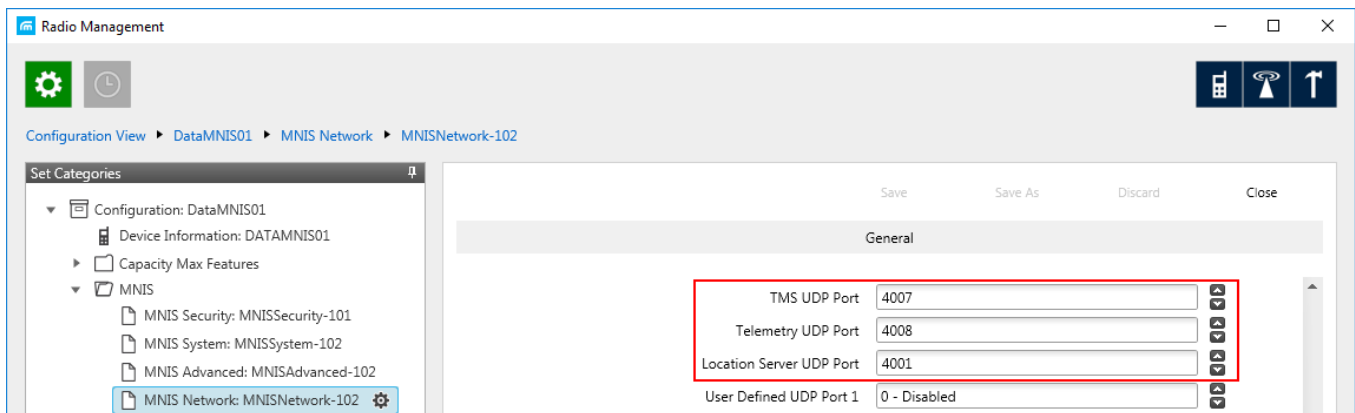


**Location Port:** The port where the radioserver will expect GPS data.

**TMS Port:** The port where the radioserver will expect text messages.

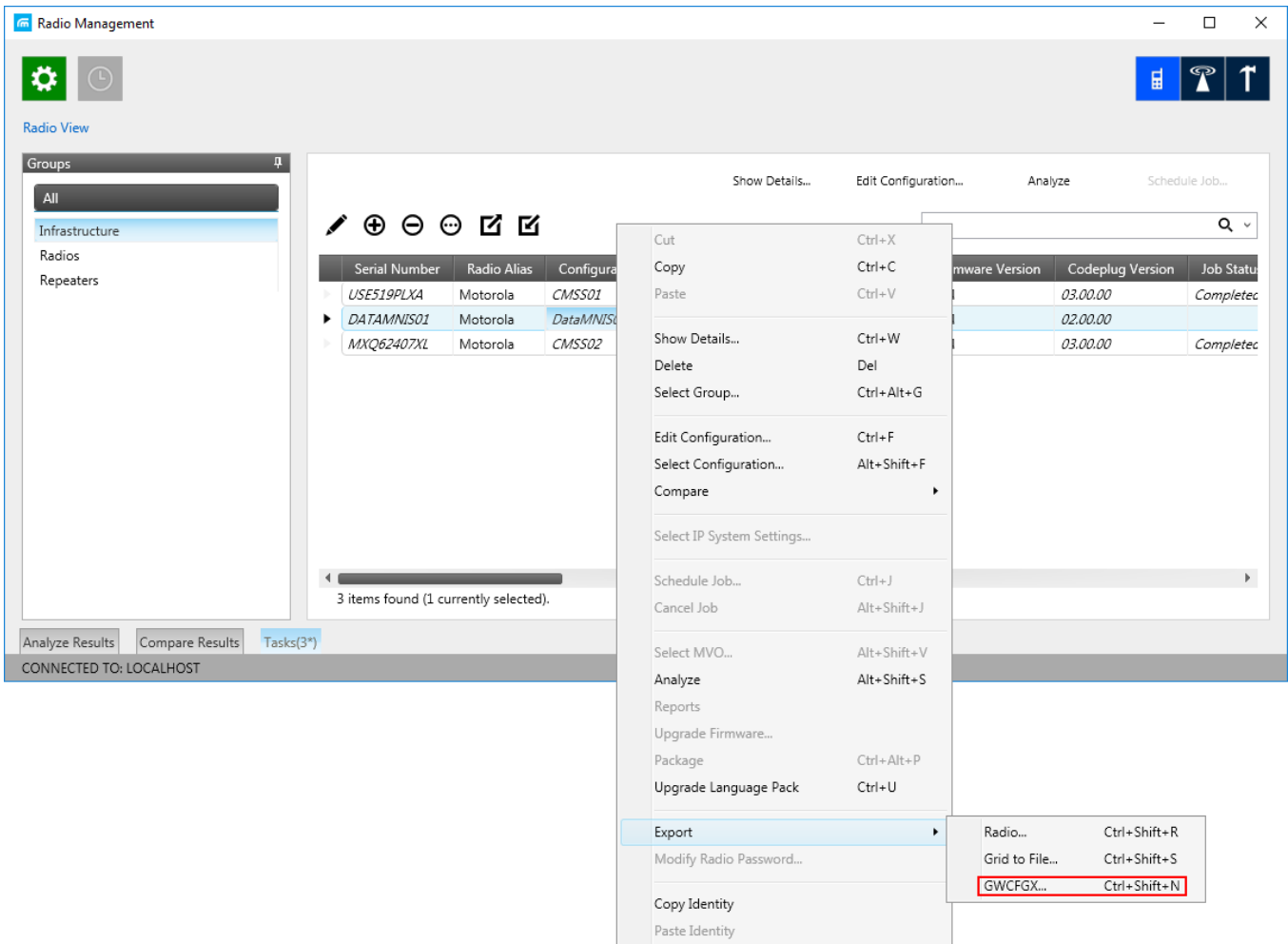
**Telemetry Port:** The port where the radioserver will expect telemetry data.

The ports should match the ports set in the corresponding fields in the *Radio Management* application (see the **MNIS Network** settings in the **MNIS** menu of the DataMNIS configuration, the **Location Server UDP Port** field, the **TMS UDP Port** field, the **Telemetry UDP Port** field in the **General** tab).

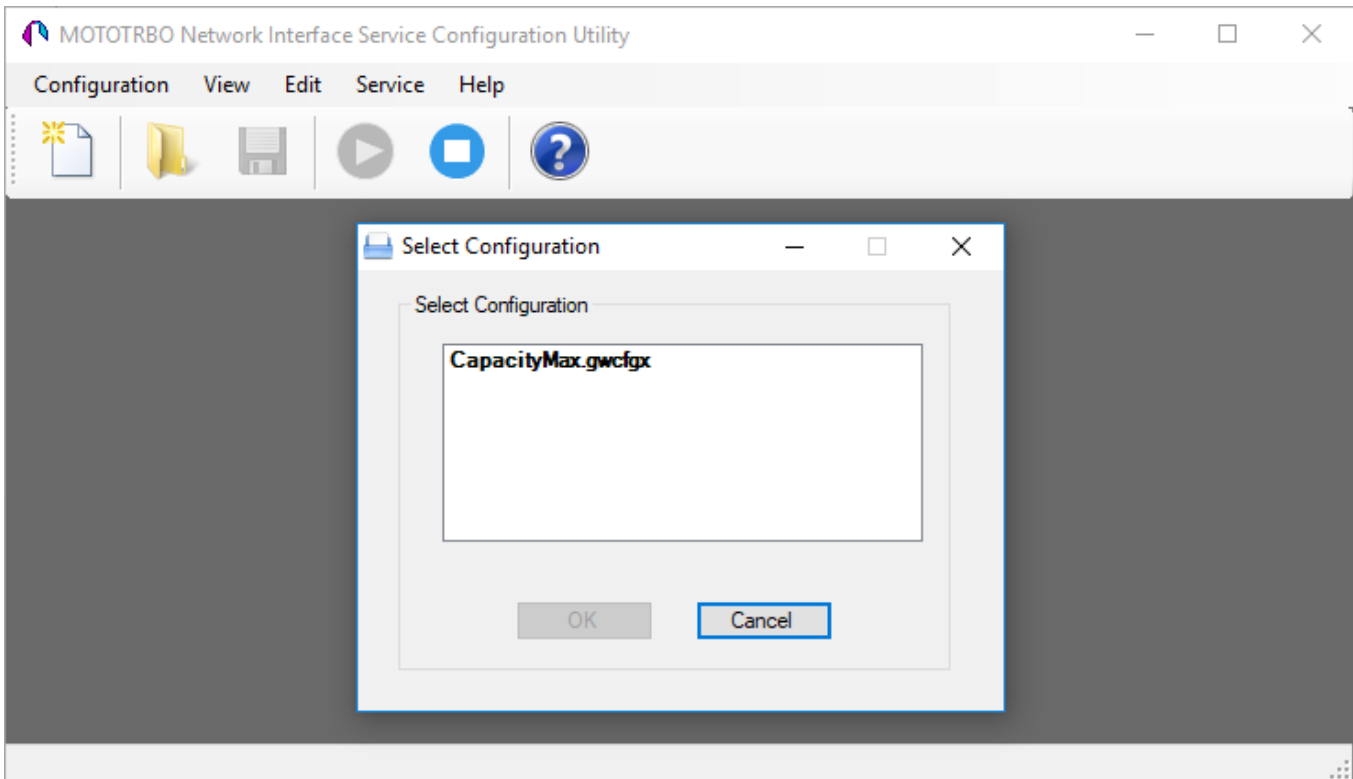


To set up MNIS Data Gateway settings in the *MOTOTRBO Network Interface Service Configuration Utility*, follow these steps:

1. Save MNIS Data Gateway settings from the *Radio Management* application as GWCFGX file. For that, click **Radios**, right click the **DATA MNIS...** item in the table that opened and click **Export** → **GWCFGX...** or press Ctrl+Shift+N. In the open **Export GWCFGX** window, select the file and click **OK**.



2. Transfer the saved GWCFGX file to your PC where the *MOTOTRBO Network Interface Service Configuration Utility* is installed, to the **Config** folder that is located on the local disk *C:/ProgramData/Motorola/Wireline Gateway*.
3. Launch the *MOTOTRBO Network Interface Service Configuration Utility* and click **Configuration** → **Select Active Configuration**. In the **Select Configuration** window that opened, select the GWCFGX file saved before and click **OK**.

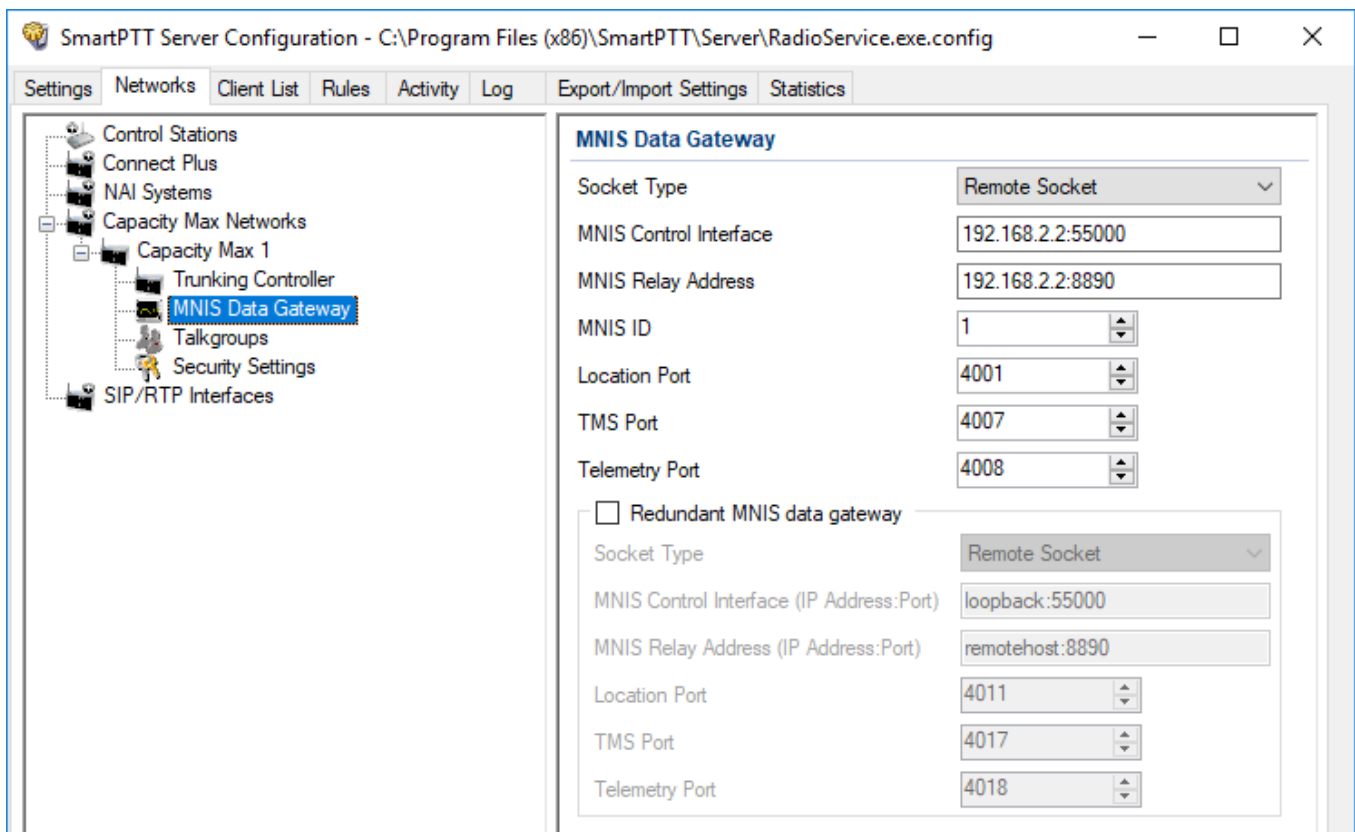


If *MOTOTRBO Network Interface Service Configuration Utility* and the SmartPTT Radioserver are running on different computers, or you configure several MNIS Data Gateways, follow these steps:



1. Install and run MNIS Data Gateway Relay on the computer where *MOTOTRBO Network Interface Service Configuration Utility* is running.
2. Run the MNIS Data Gateway Relay Configurator.



3. In the **MNIS interface** field enter the same address as it is in the **Tunnel IP Address** of MNIS.
4. In the **Server interface** field enter the same address as you did in the previous step.
5. In the **Port** type the available port of the computer.
6. Save changes and restart MNIS Data Gateway Relay.
7. In SmartPTT Radioserver Configurator double-click your network and click **MNIS Data Gateway**.



8. In the **Socket Type** field select *Remote Socket*.
9. In the **MNIS Control Interface** field, enter the IP address of the computer where MNIS service is running and the port from the **MNIS Control Interface TCP Port** field of the *MOTOTRBO Network Interface Service Configuration Utility*.

10. In the **MNIS Relay Address** field, enter the IP address of the computer where *MNIS Data Gateway Relay* service is running and the port from the **Port** field of *MNIS Data Gateway Relay*.
11. Configure other settings as described previously.
12. Click **Save**  to save changes.
13. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

## 2.4.4 Configuring MNIS VRC Gateway

Every Capacity Max network supports up to 15 MNIS VRC gateways. The first gateway is created always exists in the network, so you can add 14 gateways more.

### NOTE

To configure MNIS VRC gateway, install the corresponding license. For more information on how to install licenses, see [Licenses](#).

The order of the gateways matters a lot. All newly created profiles and talkgroups for your Capacity Max network will be assigned for the first MNIS VRC Gateway in the list. Therefore, you should be careful when configure several MNIS VRC Gateways.

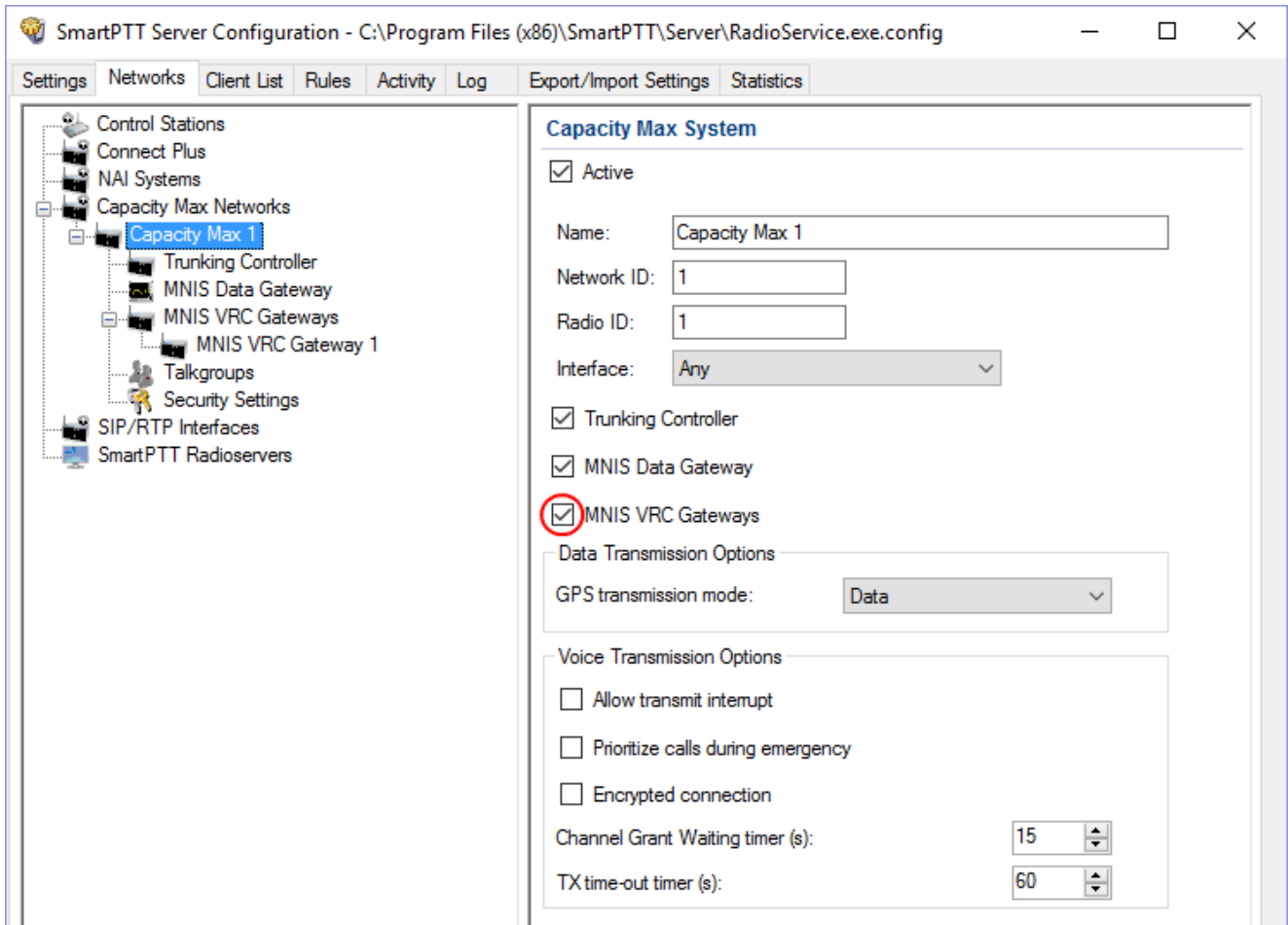
To configure MNIS VRC gateway, follow these steps:

1. Make sure that VRC Gateway is configured in the *Radio Management*.

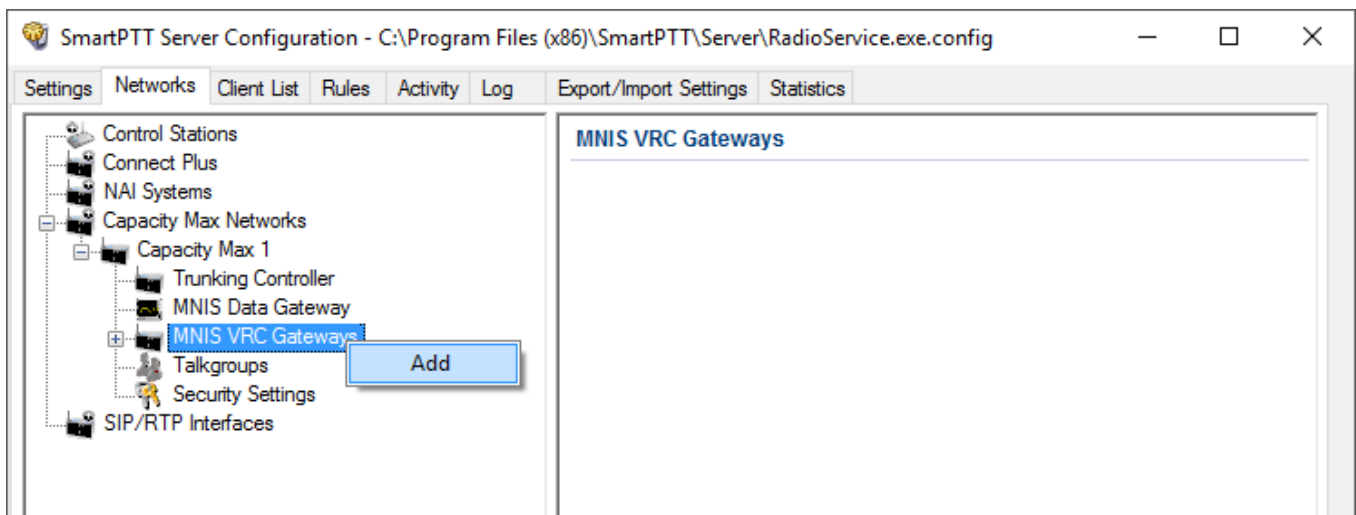
### NOTE

For more information on how to configure Radio Management application, see *Motorola Radio Management User Guide*.

- In your Capacity Max network select **MNIS VRC Gateways** to show and allow to configure MNIS VRC Gateways.



- To add a new MNIS VRC Gateway right-click **MNIS VRC Gateway** and click **Add**.

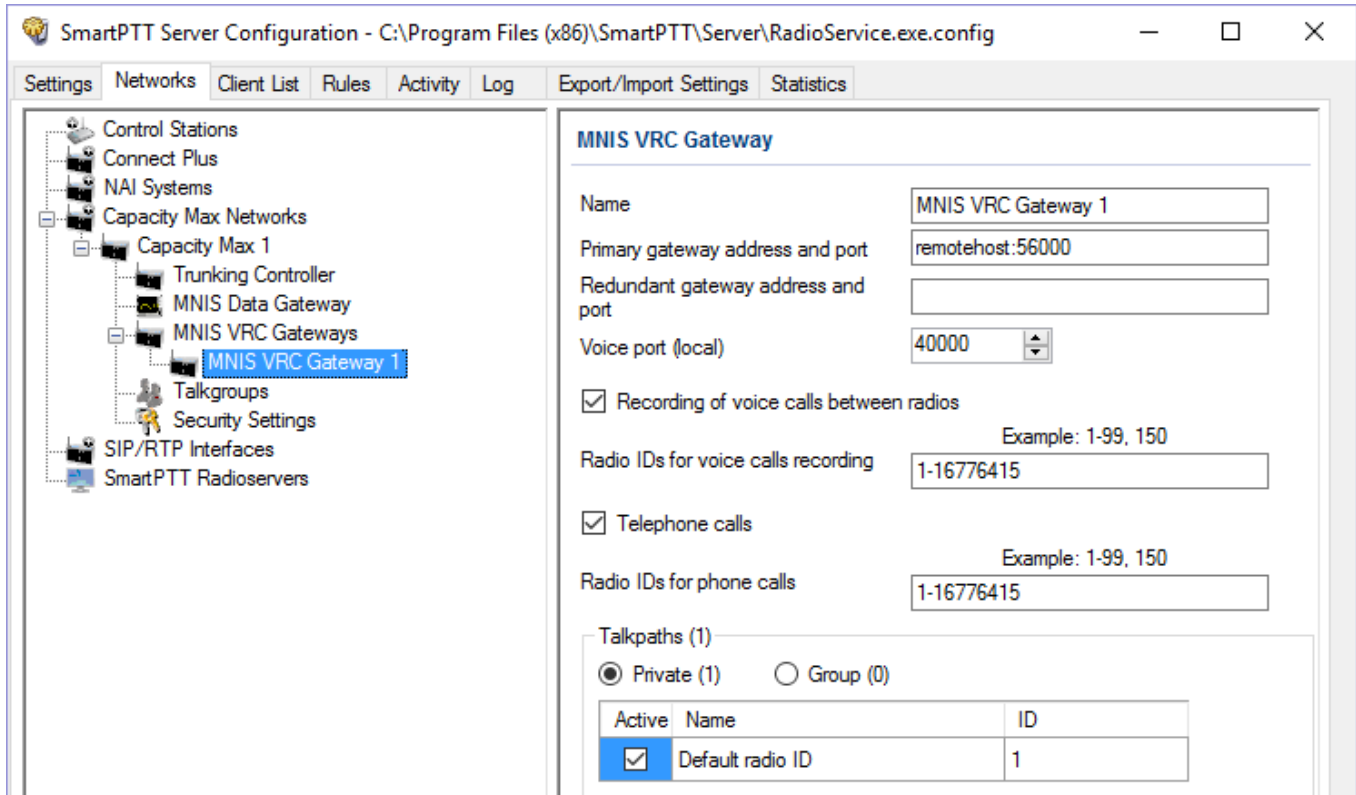


- Select the newly created or existing gateway.

**NOTE**

By default, all new gateways obtain equal IP addresses and ports. When you select one of those, you will not be able to leave the menu until you make its IP address and port unique within the site.

5. Configure the gateway options.



**Name:** The name of the gateway in SmartPTT Radioserver Configurator. Rename your gateway if needed.

**Primary gateway address and port:** IP address from **VRC Gateway IP** and port from **Server TCP port** which were configured in your CMSS Network in *Radio Management*.

**Redundant gateway address and port:** IP address of **VRC Gateway IP** and port from **Server TPC port** of the additional CMS server you assign to be redundant. You can leave this field empty if you do not have redundant VRC gateway.

**Voice port (local):** The port at which SmartPTT Radioserver will expect the voice data.

**Recording of voice calls between radios:** Select this to activate voice recording feature, that allows the dispatcher to hear private calls made from radios to other radios, dispatchers or telephone subscribers.



**Radio IDs for voice call recording:** Enter radio IDs for which the recording should be active. Follow the example, to specify the IDs.

**Phone calls:** Select this if you want to allow telephone calls for this gateway.

**Radio IDs for phone calls:** Enter radio IDs for which phone calls should be available. Follow the examples, to specify the IDs.

**Talk paths:** You can reorganize the default gateway for radios and profiles here.



**Private:** Click this to view the radio profiles which assigned to the current gateway. Profiles can be assigned to the gateway (**Active** is selected), not assigned (**Active** is clear) and unavailable on it (**Active** is clear, profile name is discolored). If the profile is unavailable, it means that it is selected on the other gateway. By default all new profiles will be selected on the first gateway in the list and their ID will be the same as that of the first gateway in the list.

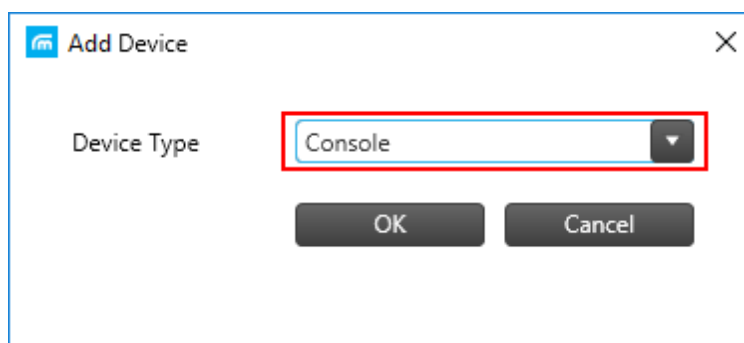
**Group:** Select this to view talkgroups created for the current site. For more information see Capacity Max [Talkgroups](#).

## 2.4.5 Adding Console in Radio Management

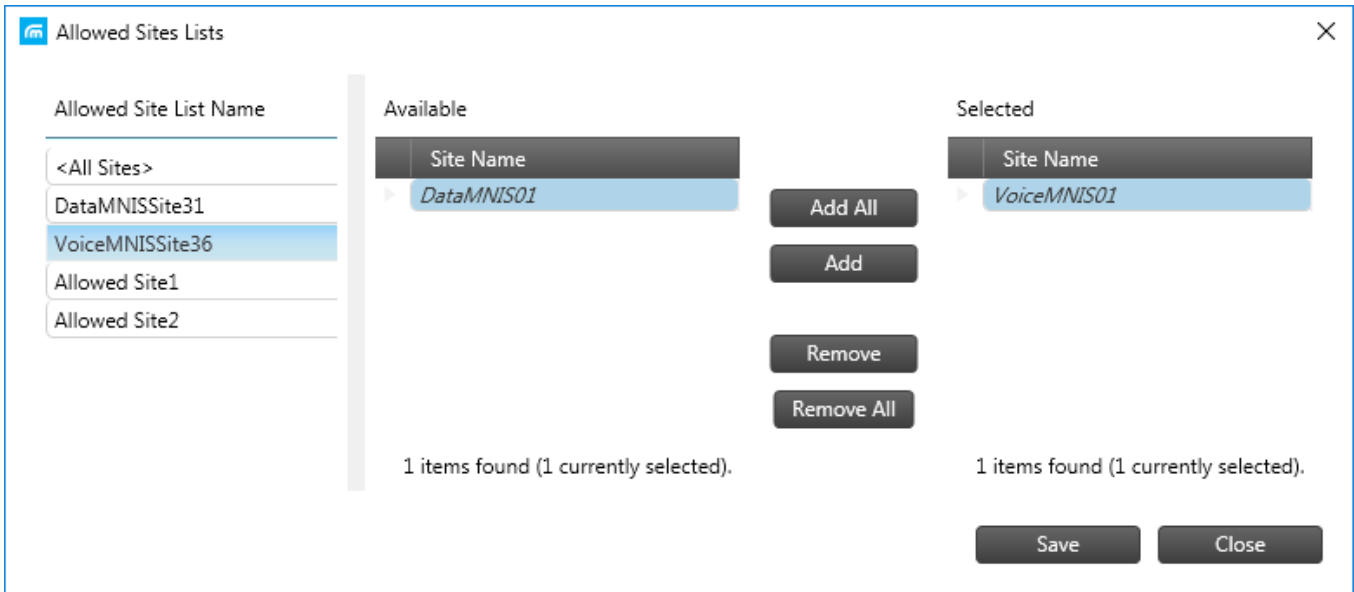
*Radio Management* dispatch console is used for providing a dispatcher with an access to the Capacity Max network.

To add console in *Radio Management*, follow these steps:

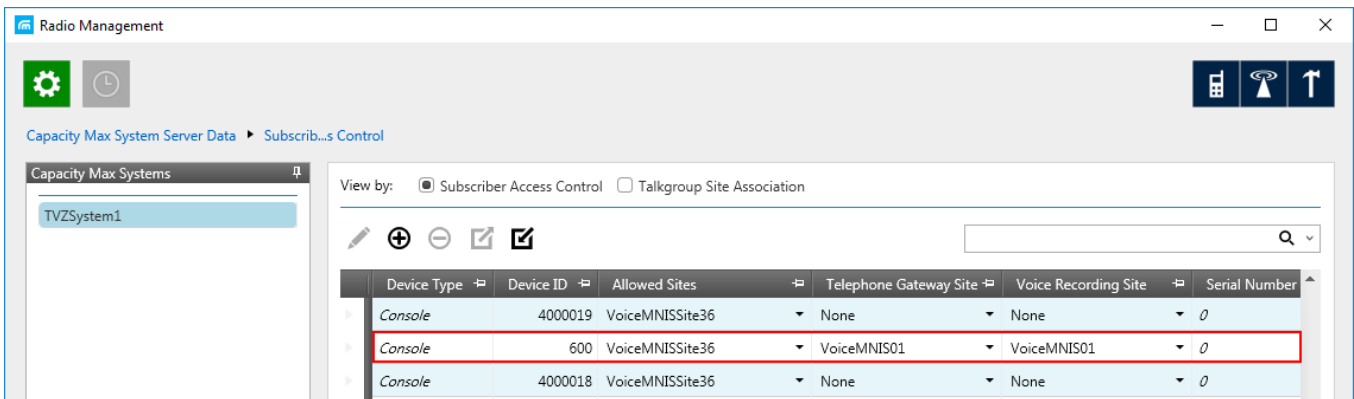
1. Click **Actions** , and select **Manage** → **Capacity Max System Server Data**.
2. Click **Add** .
3. In the open **Add Device** window, from the **Device Type** list, select *Console* and click **OK**.



4. In the table, in the added console row, perform the following actions:
  - a. In the **Device ID** column, enter radio ID for the console.
  - b. In the **Allowed Sites** column, from the list select **Edit**.
    - i. In the **Allowed Sites Lists** window, from the **Allowed Site List Name**, select the desired site for registering.
    - ii. Click **Save**.

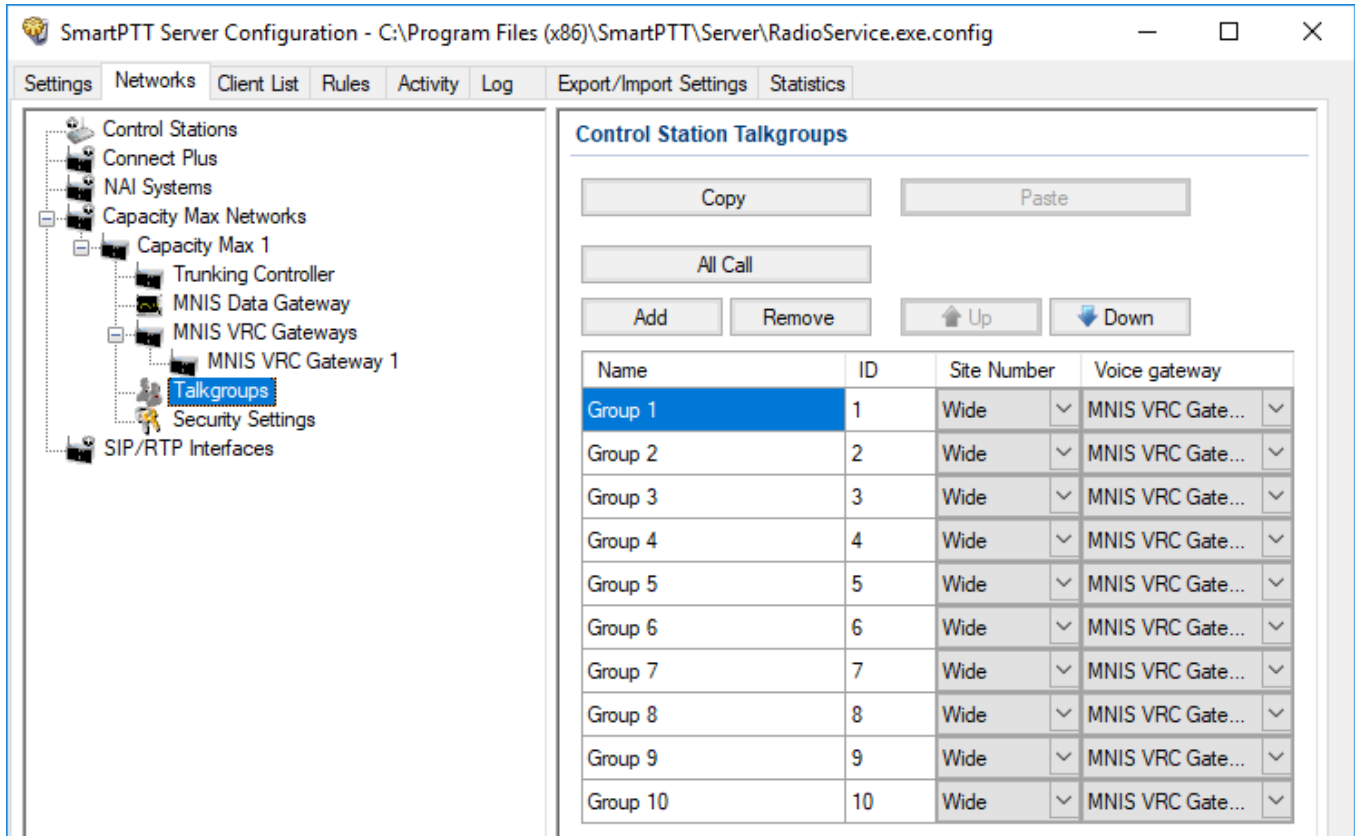


- c. In the **Telephone Gateway Site** column, from the list select the desired site for telephone recording.
- d. In the **Voice Recording Site** column, from the list select the desired site for voice recording.



## 2.4.6 Configuring Talkgroups

To configure Capacity Max talkgroups, click **Talkgroups**. The **Control Station Talkgroups** window appears:



To add a talkgroup, click **Add**. To add an All Call, click **All Call**. The added talkgroups will also appear in the **Profiles** window. To change the order of groups in the list, use the **Up** and **Down** arrows. The order defined in the window will be used in *SmartPTT Dispatcher*. To copy added groups to the clipboard, click **Copy**. To paste copied groups from the clipboard, click **Paste**. To delete the selected talkgroup, click **Remove**.

**Name:** Talkgroup alias displayed by the control station.

**ID:** Talkgroup unique identifier used during communications. To be set in the range from 1 to 65535 for a talkgroup, and in the ranges from 1 to 16776415, from 16777056 to 16777183 or be equal to 16777214 for an All Call.

To edit the talkgroup name or ID, set the cursor on the corresponding field and make changes.

**Site Number:** Site number list allowed for transmitting. In the Capacity Max network the talkgroups can be only wide-area, while All Call can be wide-area or local.

**NOTE**

In the Capacity Max network you can add only wide-area talkgroups, so only the *Wide* value is available for groups in the **Site Number** field. In order to display wide area talkgroups in *SmartPTT Dispatcher*, add necessary talkgroups in *SmartPTT Radioserver Configurator*, define talkgroup identifiers that correspond to the identifiers of the wide-area talkgroups in the *Radio Management* settings. You can add a wide-area All Call and a local All Call, which is limited to one site. To add a wide-area All Call, which is available to all sites, click **All Call**. Verify that **Site Number** is set to *Wide*. To add an All Call limited to one site, click **All Call**, and in the **Site Number** field select the site number where the All Call will be heard. Please note, that you do not need any IDs for All Calls.

**Voice gateway:** List of available voice gateways. You can assign a certain voice gateway for each talkgroup.

**NOTE**

If there are some available voice gateways, all talkgroups use by default the first voice gateway in the list. If the talkgroup is not registered on any voice gateway, the **Voice gateway** field will be empty. If [Voice transmission](#) is not selected in the Capacity Max network settings, the **Voice gateway** column will be hidden.

You should create talkgroups in accordance with the settings in the Radio Management application (see the **Capacity Max Systems** settings, sorted by the **Talkgroup Site Association** value). For more information, see *Motorola Radio Management User Guide*.

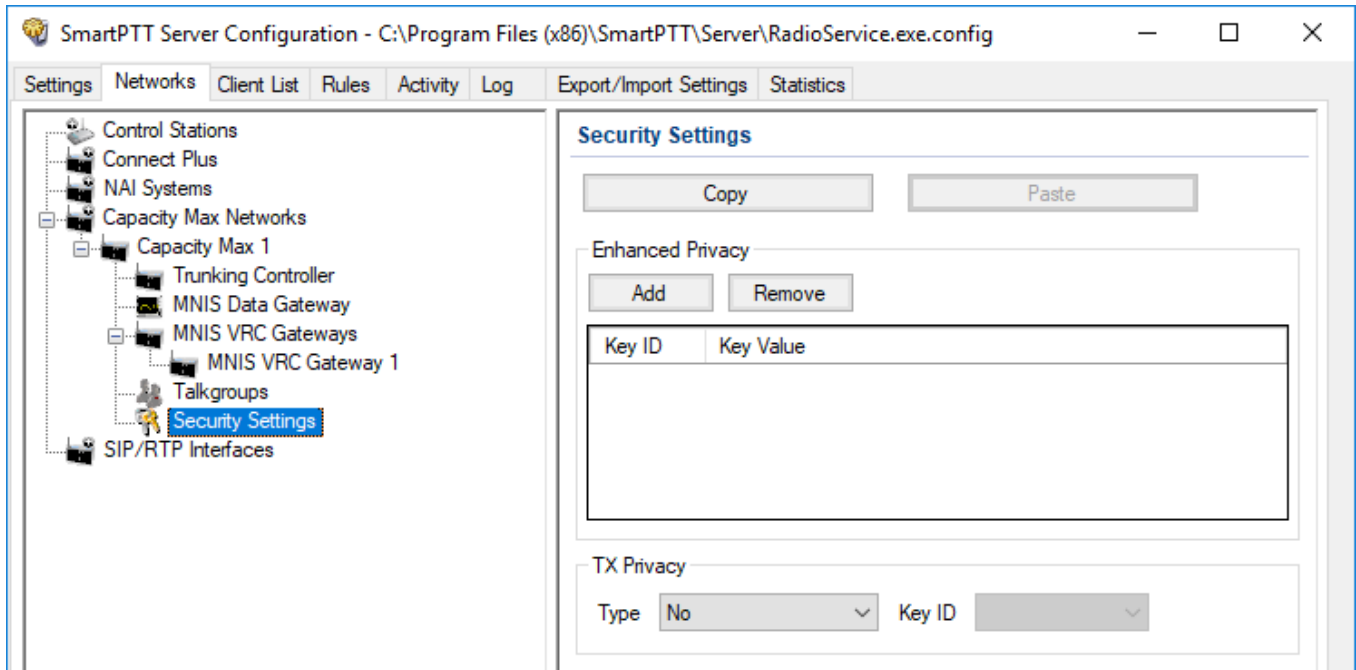
## 2.4.7 Security Settings

Capacity Max network supports two types of privacy mechanisms – Enhanced and Advanced Encryption Standard (AES).

The Enhanced Privacy utilizes Motorola proprietary algorithms and therefore is not interoperable with other vendor's privacy offerings. The Enhanced Privacy provides high level of protection by means of 40-bit key length and supports multiple keys in a radio.

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST). The AES feature supports 256-bit key length, unlike Enhanced Privacy. Similar to Enhanced Privacy, the AES also supports multiple keys. For AES encryption a special license is required.

You can specify the encryption keys for incoming and outgoing traffic on the digital channel in the **Security Settings** window.



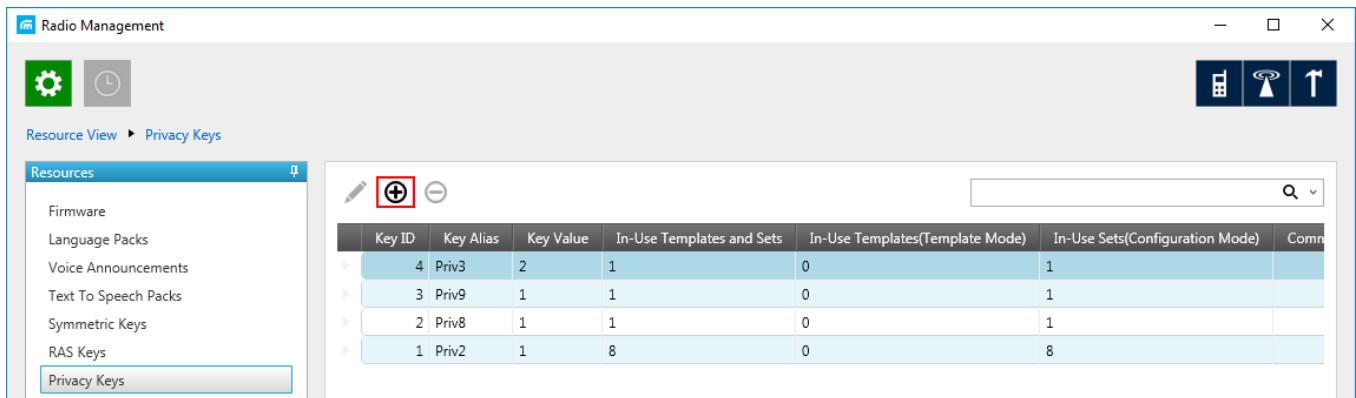
**Copy:** Copy encryption settings of the channel to the clipboard.

**Paste:** Paste encryption settings of the channel from the clipboard.

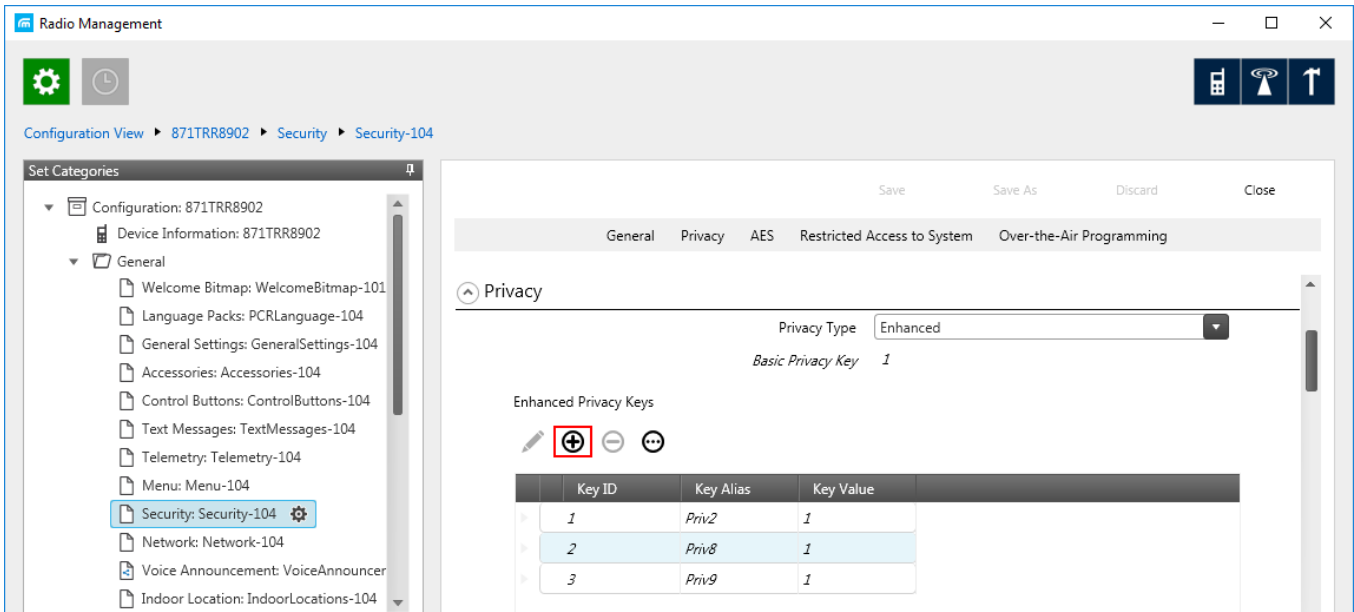
### Enhanced Privacy

To configure **Enhanced Privacy**, follow these steps:

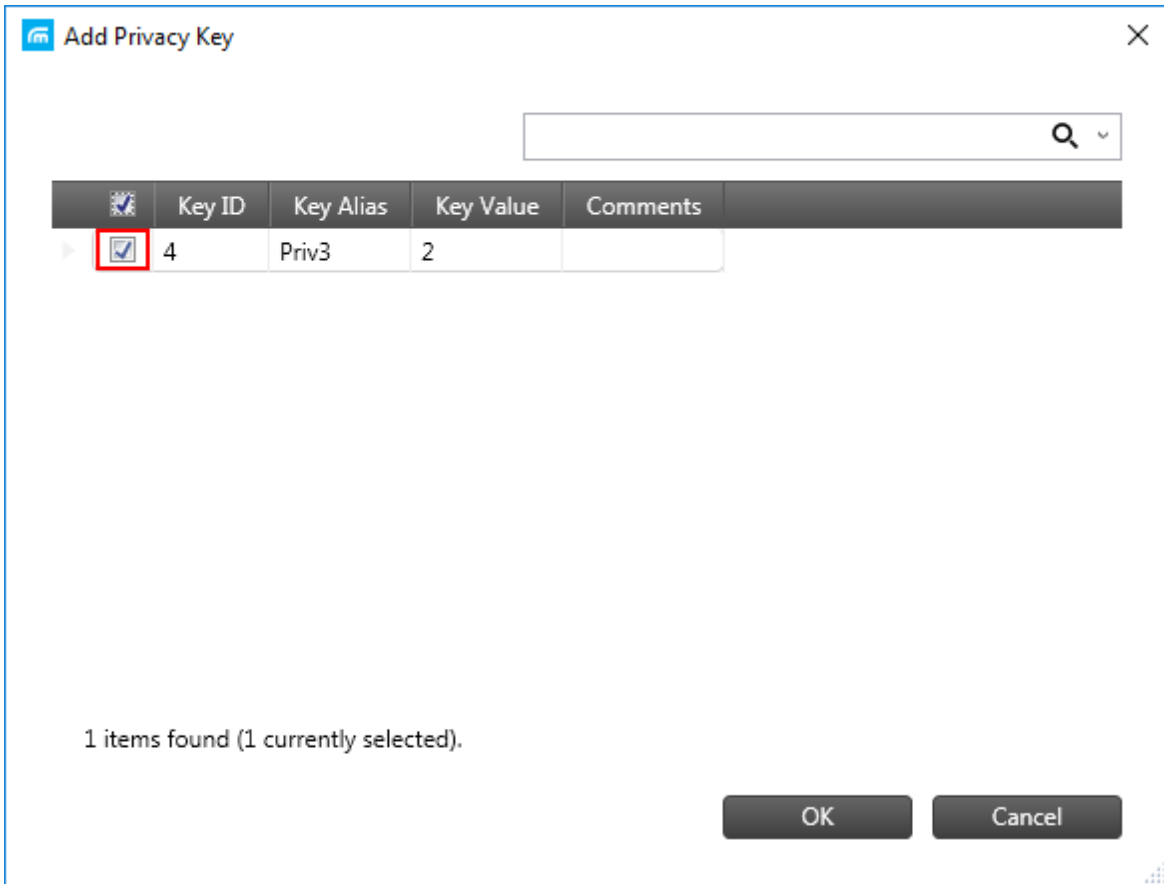
1. Run the *Radio Management* application.
2. In the **Privacy Keys** tab of the Radio Management application add the enhanced privacy key. Enter its ID and value in the corresponding fields.



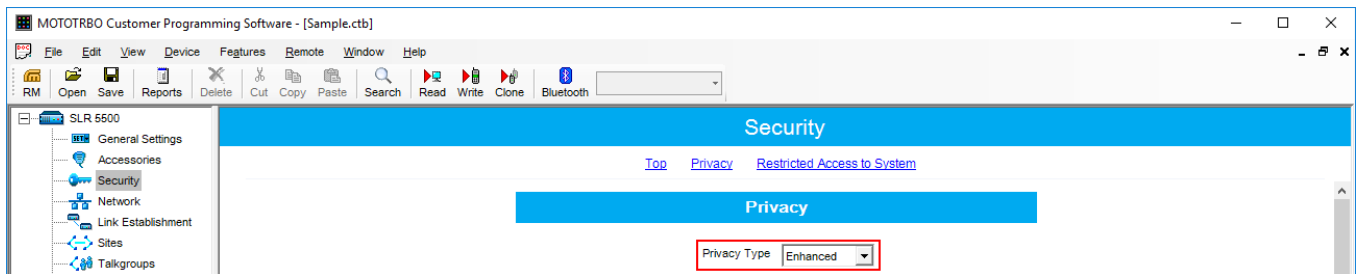
- Open the configuration of the required radio station and in the **Set Categories** menu click **General** → **Security**. To make the added enhanced privacy keys available for selection, add them in the selection set. To do that, in the **Privacy** tab click the **Add**.



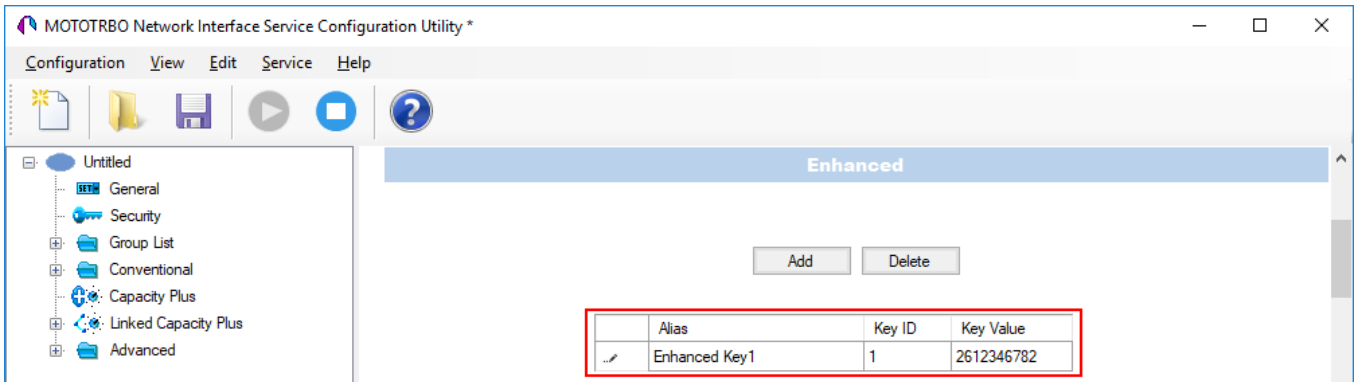
- In the **Add Keys** window, select the required keys, which you want to be available for selection in the **Privacy Alias** field when specifying the enhanced key on the channel and click **OK**.



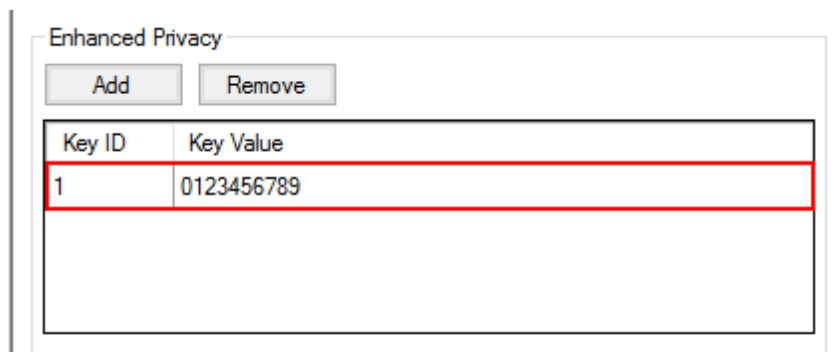
- In the **Security** window of the repeater settings in *MOTOTRBO CPS* in the **Privacy Type** field select **Enhanced**.



- In the **Security** window of *MOTOTRBO Network Interface Service Configuration Utility* in the **Enhanced** field add the enhanced privacy key. Enter its ID and value in the corresponding fields.





- In the **Security Settings** window of *SmartPTT Radioserver Configurator* add an enhanced privacy key for incoming traffic. Enter its ID and value in the corresponding fields.



**NOTE**

Key ID and Key Value must match the values set in the radio settings in the *Radio Management* program and *MOTOTRBO Network Interface Service Configuration Utility*. If the values in the Key ID fields are the same, but the values in the Key Value fields do not match, the receiving side hears only a distorted voice. If the key identifier of the transmitting side does not coincide with one of the key identifiers in the list of the receiving side, then transfer to the receiving party will not be heard.

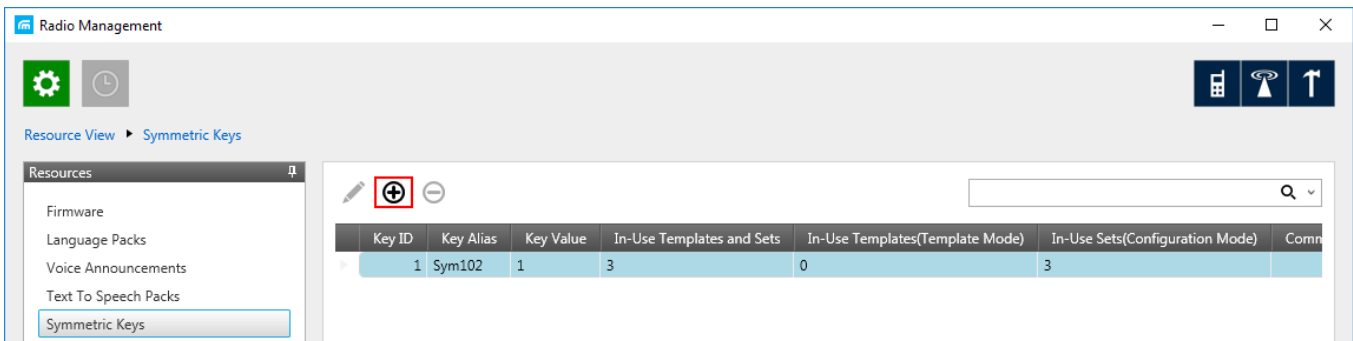
- Click **Save**  to save changes.
- Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.



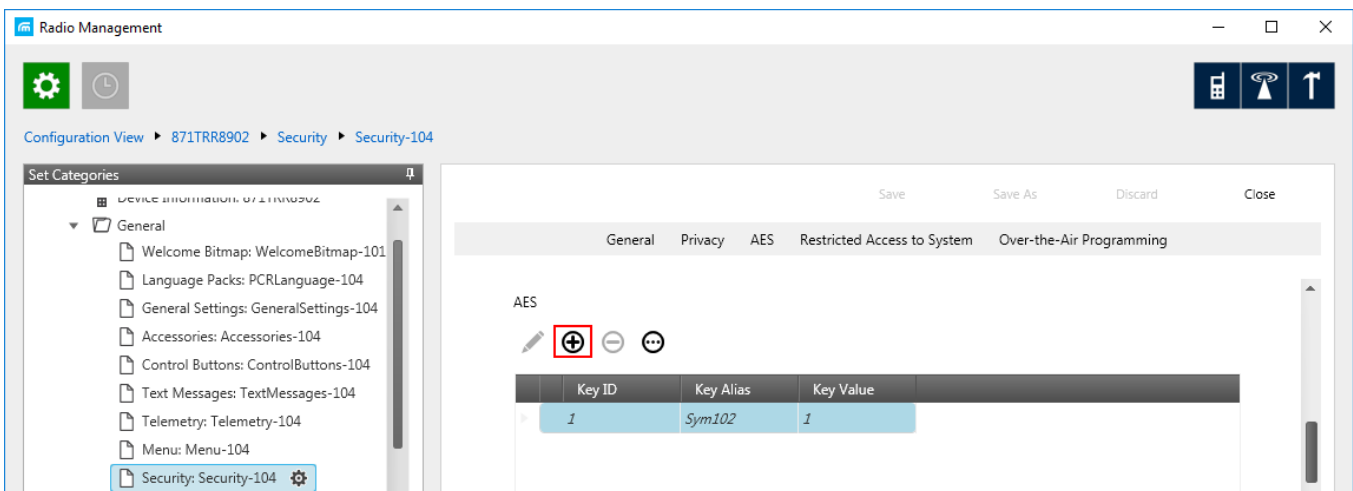
## AES Privacy

To configure the **AES** privacy, follow these steps:

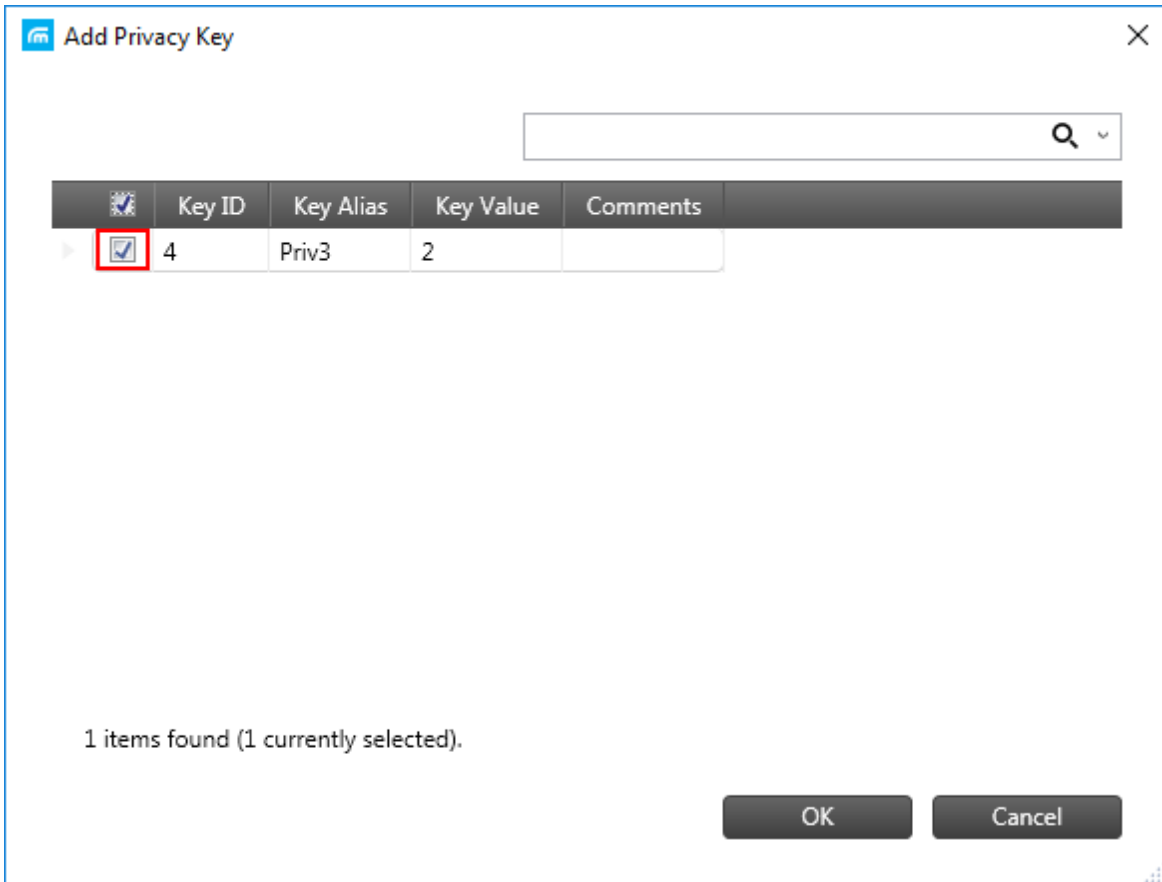
1. Run the *Radio Management* application.
2. In the **Symmetric Keys** tab of the *Radio Management* application add the AES privacy key. Enter its ID and value in the corresponding fields.



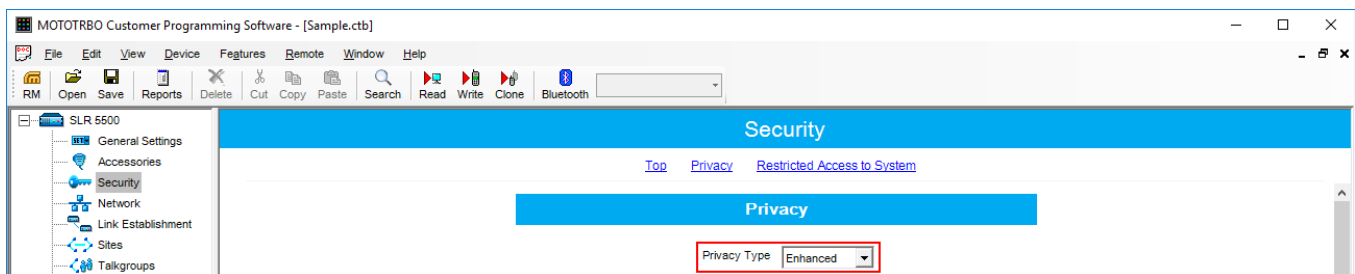
2. Open the configuration of the required radio station and in the **Set Categories** menu click **General** → **Security**. To make the added AES privacy keys available for selection, add them in the selection set. To do that, in the **AES** field, click **Add**.



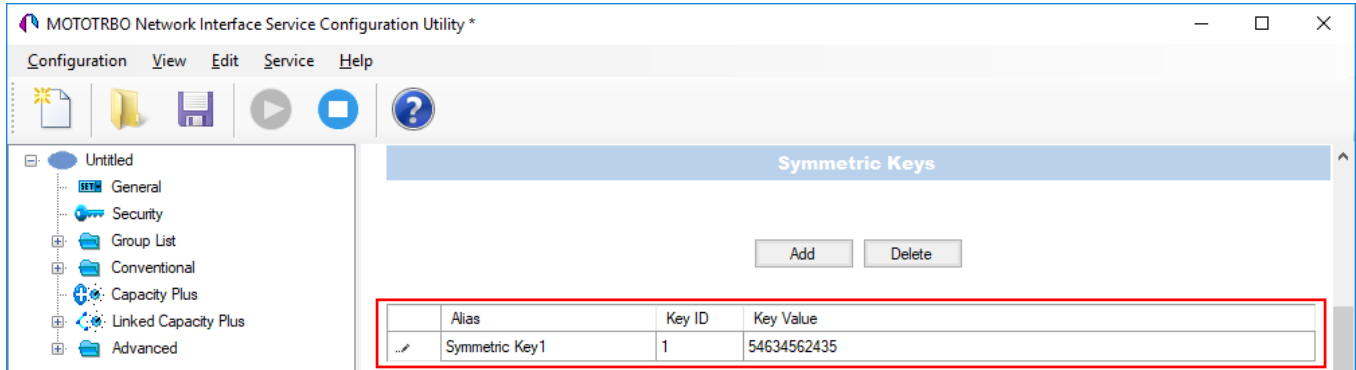
- At that the **Add Keys** window appears: Select the required keys, which you want to be available for selection in the **AES Alias** field when specifying the AES privacy key on the channel and click **OK**.



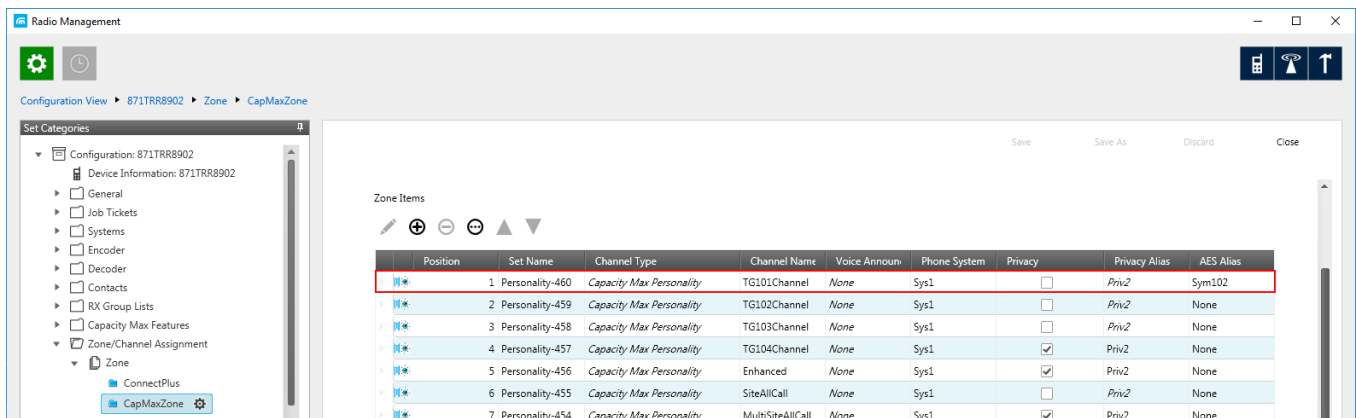
- In the **Security** window of the repeater settings in *MOTOTRBO CPS* in the **Privacy Type** field select **Enhanced**.



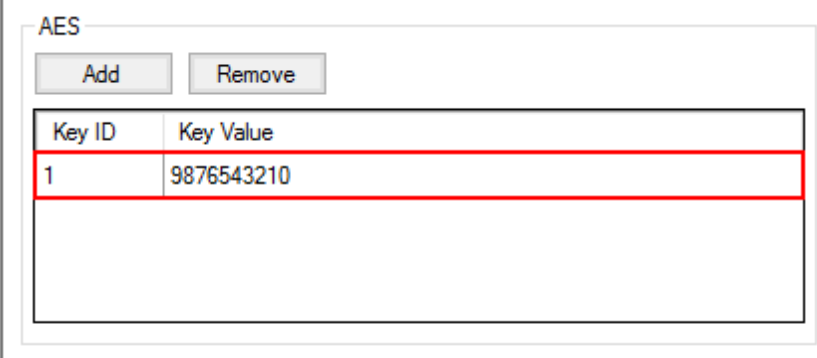
- In the **Security** window of MNIS in the **Symmetric Keys** area, add the AES symmetric privacy key. Enter its ID and value in the corresponding fields.



- In the radio settings in the *Radio Management* application to enable the AES encryption mode on the required channel, clear the **Privacy** check box and in the **AES Alias** field select the **AES privacy key**.





7. In the **Security Settings** window of *SmartPTT Radioserver Configurator* add an AES privacy key for incoming traffic. Enter its ID and value in the corresponding fields.



Key ID	Key Value
1	9876543210

**NOTE**

Key ID and Key Value must match the values set in the radio settings in the Radio Management program and in MOTOTRBO Network Interface Service Configuration Utility. If the values in the Key ID fields are the same, but the values in the Key Value fields do not match, the receiving side hears only a distorted voice. If the key identifier of the transmitting side does not coincide with one of the key identifiers in the list of the receiving side, then transfer to the receiving party will not be heard.

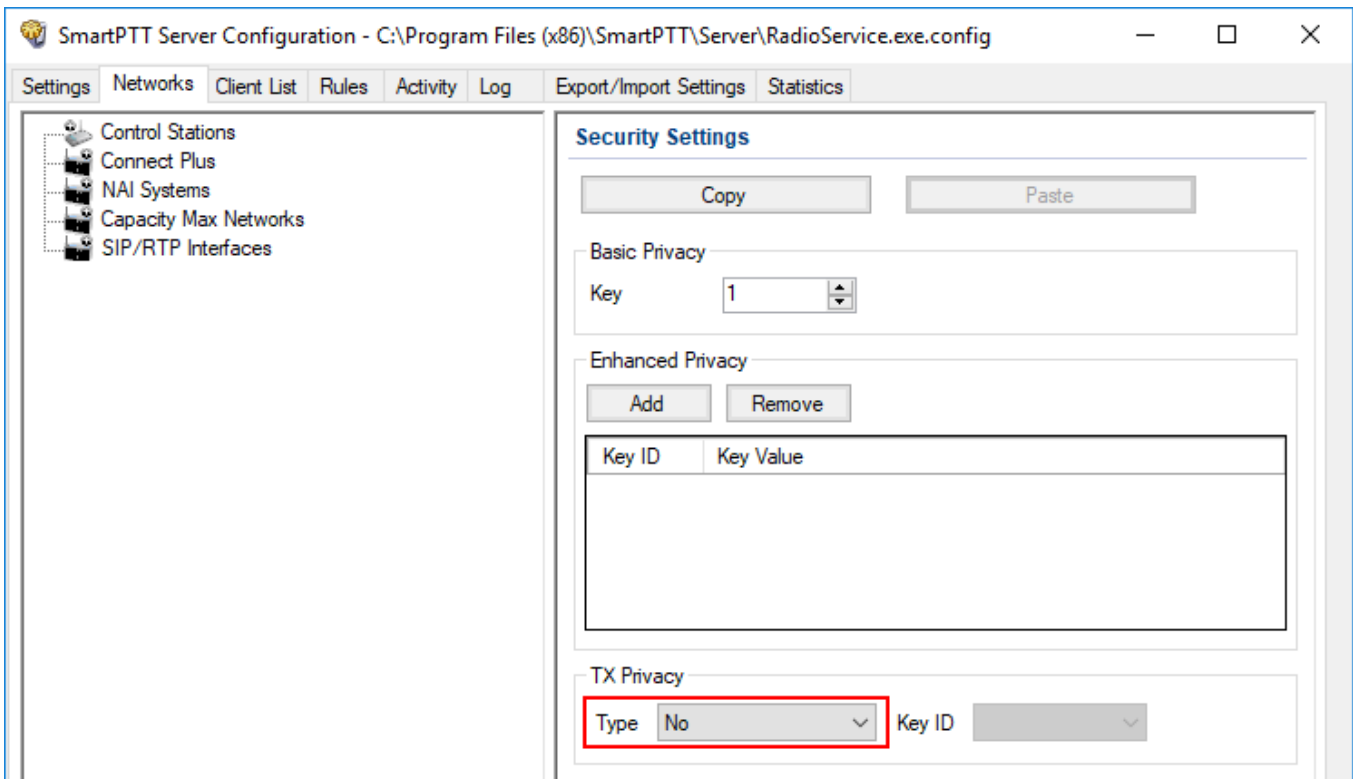
8. Click **Save**  to save changes.
9. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

**TX Privacy**

TX Privacy is used for selecting an encryption mode for outgoing traffic on the side of *SmartPTT Dispatcher*.

To configure the TX Privacy for a Capacity Max system, follow these steps:



1. In the **TX Privacy** area, from the **Type** list select the desired encryption type:



- Select *No* if encryption of outbound traffic from the radioserver is not required.
- Select *Enhanced* if you want to use enhanced encryption for outgoing traffic from the radioserver. Use the Key ID you specified in the **Enhanced Privacy** area.
- *AES license is required:* Select *AES (Symmetric Key)* if you want to use AES (Symmetric Key) encryption for outgoing traffic from the radioserver. Use the Key ID you specified in the **AES** area.

#### NOTE

If from the **Type** field *No* is selected and you have AES encryption for incoming traffic configured, AES (Symmetric Key) is used for incoming traffic by default.

2. Click **Save**  to save changes.
3. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

## 2.5 SIP/RTP Interfaces

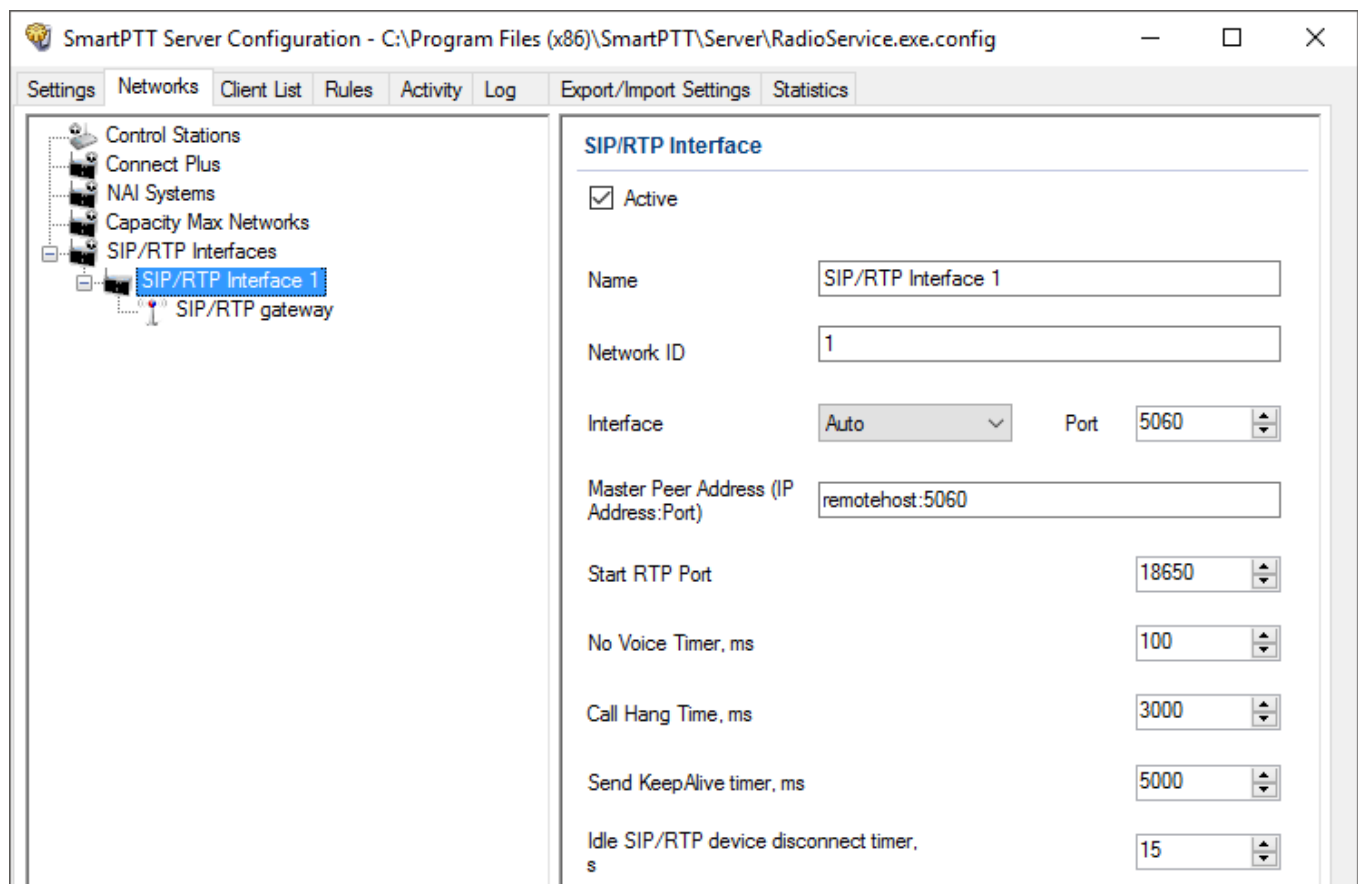
Backed up with Cisco special hardware, SmartPTT can operate with cable radio networks. The cable radio network interface is used for converting analog voice signals into digital IP packets. So far, we have run successful tests on Cisco 2900 only.

Cable radio networks allow SmartPTT to connect to analog radio systems and other systems supporting cable radio network interfaces. The dispatcher can monitor calls from and to these systems. In this version, only All Calls and Group Calls are supported. Group Calls require additional bridging configurations.

### NOTE

Wireline radio network support requires a correspondence license. For more information on how to install licenses, see [Licenses](#).

To add a cable radio network interface, right-click **SIP/RTP Interfaces** and click **Add**. The following window will open:



**Active:** Enables the network.

**Name:** Network name, which will be used in *SmartPTT Dispatcher*.

**Network ID:** Unique ID of the network, which is used inside SmartPTT system. It is important that you have no other network with the same **Network ID**.

**Interface:** A local IP address which is used as gateway between the radioserver and Cisco hardware. This IP address must also be defined in the Cisco device settings.

**Port:** Port number used for interconnection between the radioserver and Cisco hardware. This port must not be used in any other networks. The default value is *5060*.

**Master Peer Address (IP Address:Port):** The IP address and port of the SIP/RTP device (Cisco hardware), which is used as the network master peer.

**Start RTP Port:** This is the first RTP port is to be used by the SIP/RTP device for voice channels. The default value is *18650*.

**No Voice Timer, ms:** Time period for which the radioserver reserves the channel for a call session. If during this time period the SIP/RTP device has not sent any voice packet, the radioserver activates **Call Hang Time**.

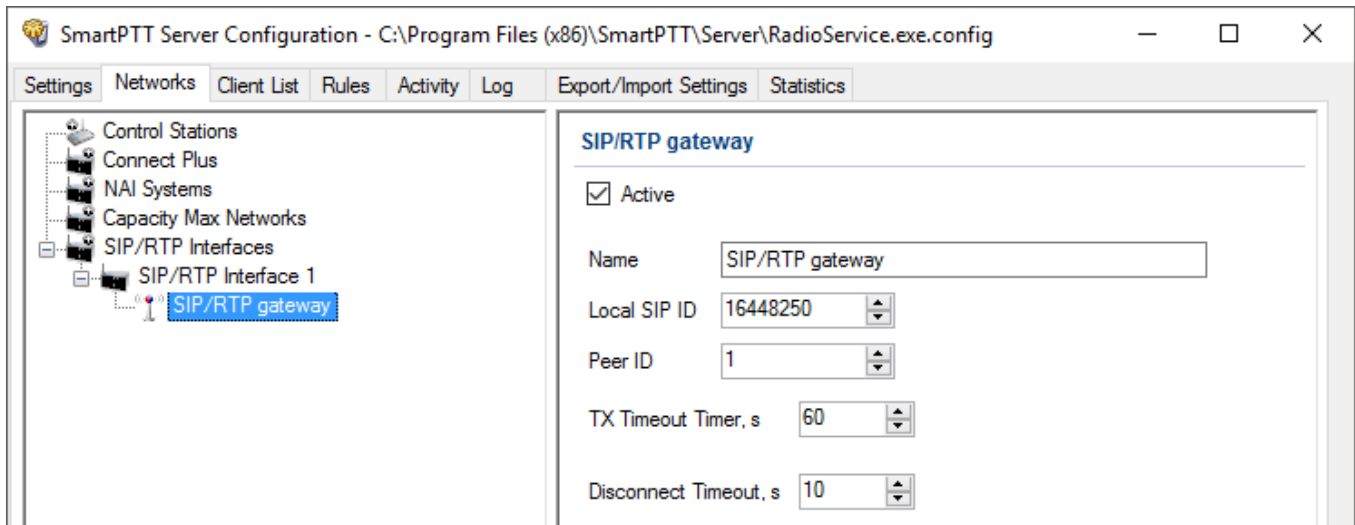
**Call Hang Time, ms:** Time period during which the radioserver reserves the channel for a call after the end of transmission. During the timeout, only the participants of the call can transmit.

**Send KeepAlive timer, ms:** Time interval for the radioserver to send a special packet (keepalive) to the SIP/RTP device to notify that the radioserver is active and running.

**Idle SIP/RTP device disconnect timer, s:** Time interval when the radioserver waits for a special packet (keepalive) from the SIP/RTP device to notify that the device is active and running. If the radioserver has not received this packet from the SIP/RTP device during this time period, the device gets the Offline status.

## 2.5.1 SIP/RTP Gateway

To set up the SIP/RTP gateway, click **SIP/RTP gateway**. The following window will open:



**Active:** Enables the SIP/RTP gateway.

**Name:** Any random name of the SIP/RTP gateway. It is used only in *SmartPTT Radioserver Configurator*.

**Local SIP ID:** The identifier of the radioserver. This will be used as a Radio ID by radios wishing to make the incoming All Call.

**Peer ID:** The identifier of the Cisco device. This will be used as a Radio ID for outgoing calls.

**TX Timeout Timer, s:** Time period during which the radio can transmit without interruptions. After this time is over, the transmission is interrupted.

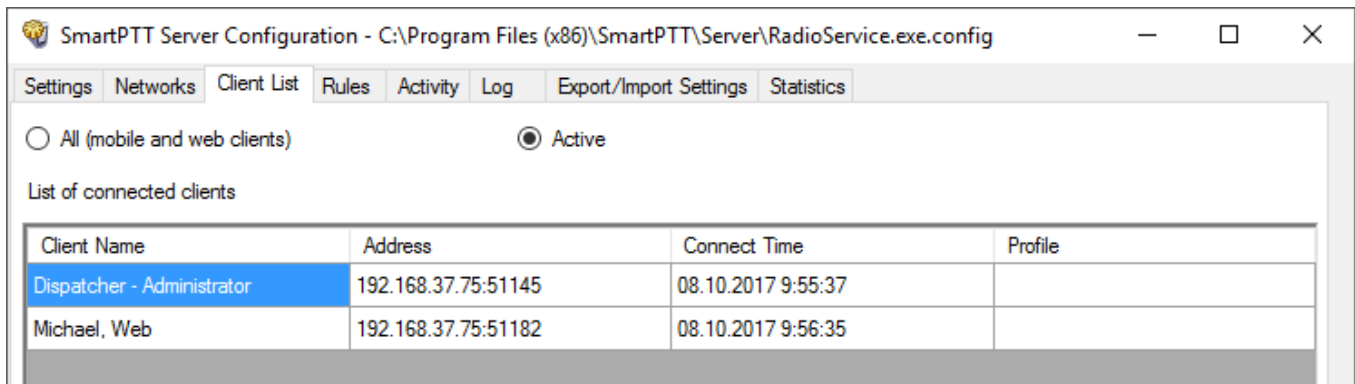
**Disconnect Timeout, s:** Time period during which the channel is blocked one way after **TX Timeout Timer** expiration. After this time period is over, the channel becomes available for transmission. While the channel is blocked, calls going in the opposite direction are not affected.



## 3 Client List

The **Client List** tab enables you to see the lists of client applications connected to the radioserver and to manage the settings of the users created to work with the web application.

To open the list of client applications connected to the radioserver, click the **Client List** tab and click **Active**.



**Client Name:** Name of the desktop version of the dispatch console, the operator's name, or web application connected to SmartPTT Radioserver. If **Windows Authentication** is enabled in SmartPTT Dispatcher **Settings** → **General Settings**, you can also see the name of the Windows group (which, in this case, corresponds to the name of the operator) and the name of the Windows user logged into Windows.

**Address:** The IP address of the client application.

**Connect Time:** Time of the last session.

**Profile:** Assigned profile to the dispatcher or to the user of the web application.

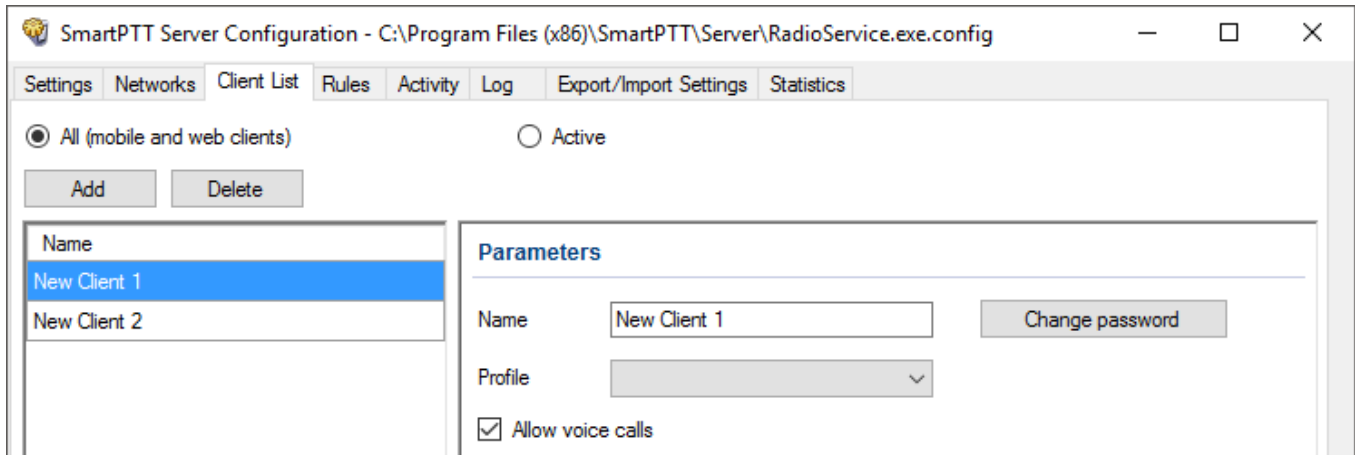
### NOTE

To assign a profile to the dispatcher, click **Settings** → **Radioservers** in *SmartPTT Dispatcher*. For more information about profiles see [Profiles](#) in the Help document.

To connect the desktop version of the dispatch console to the radioserver, go to **Settings** → **Radioservers** in SmartPTT Dispatcher and select the radioserver to which you want to be connected. At that, in the **Client List** tab of SmartPTT Radioserver Configurator the connected dispatch console will show up.

How to connect the user of the web application to the radioserver, please check WebClient Installation & Configuration for SmartPTT.

To open the list of users created to work with the mobile and web clients, click **All (mobile and web clients)**.



The **Login** list: The list of users of the SmartPTT web application.


To add new user, click the **Add** button. In the **Parameters** section specify the user name in the **Login** field and set the password by clicking the **Change password** button. The user name and password are case sensitive.

**Profile:** It contains the list of profiles created in *SmartPTT Radioserver Configurator* (see the **Settings** tab → **Profiles**). Assigning a profile to the user is not obligatory, but enables you to limit the user's access to objects and to provide additional opportunities in the organization of calls between user and radios. For more information about profiles, see [Profiles](#) in the Help document.

**Allow voice calls:** Select it to enable the user to make voice calls.

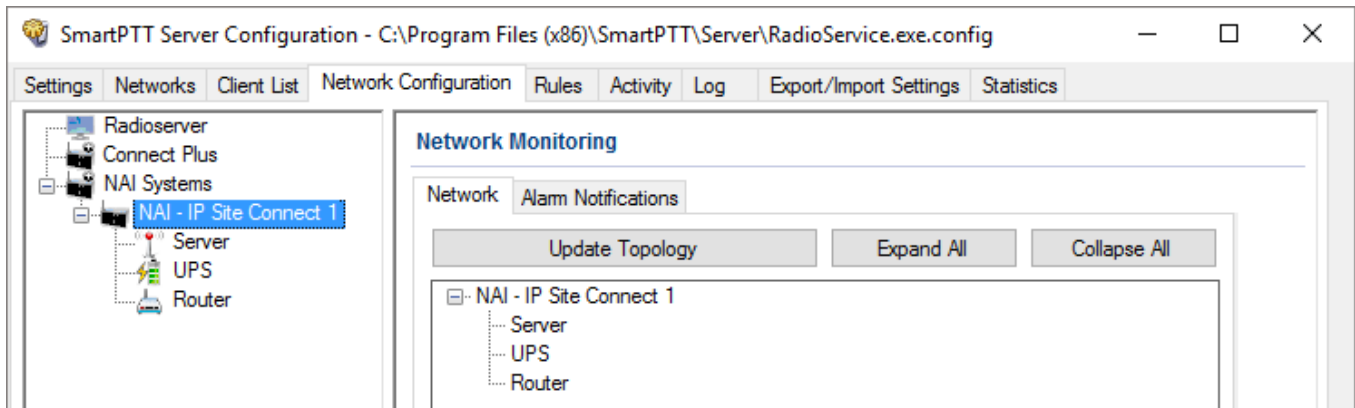
To edit the parameters of the existing user, click this user in the **Login** list, and edit the necessary fields in the **Parameters** section.

To delete user, click this user in the **Login** list, and click the **Delete** button.

To save the changes, click the **Save** button  in the bottom right corner of the *SmartPTT Radioserver Configurator*.

## 4 Network Configuration

In the **Network Configuration** tab you can set up elements of the networks used in the system. The added elements will be displayed in the **Topology** tab of *SmartPTT Dispatcher*. You can also set up sending of alarm notifications to predefined addresses.



### NOTE

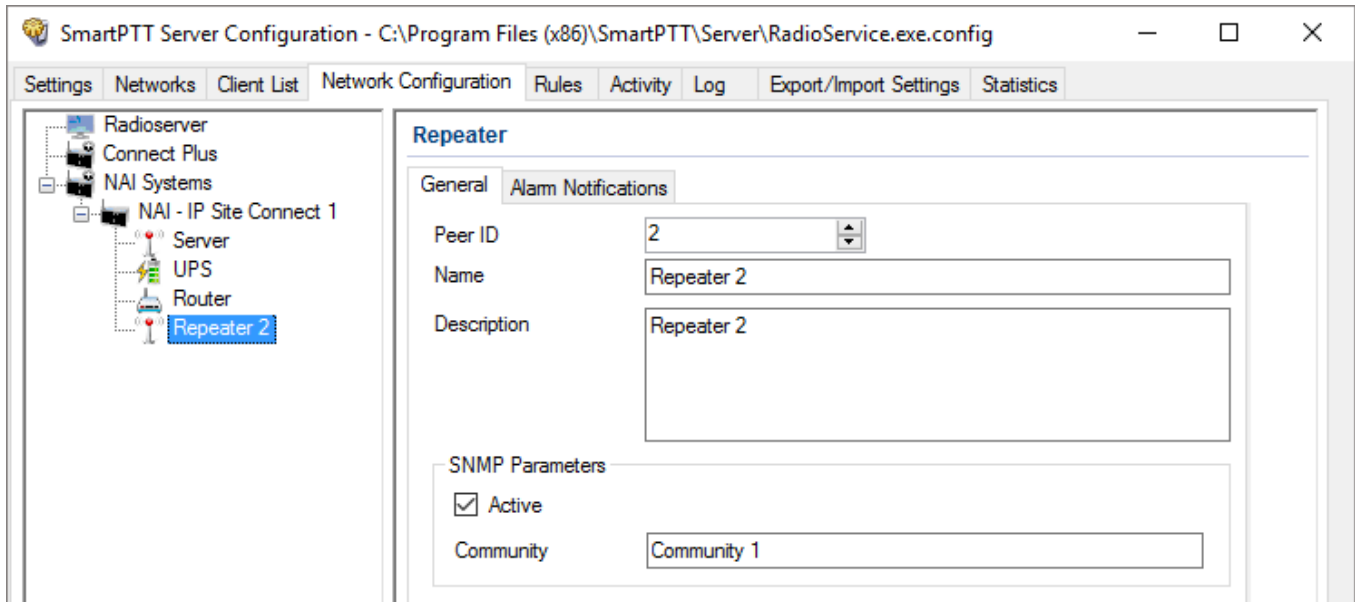
This tab is available only if there is a license for monitoring. If you have it, make sure you have selected the **Active** check box in the [Monitoring](#) window.

To add elements of the network, select the network in the list. The supported network elements include: repeaters, routers, UPS and location. To add devices, open the context menu by right-clicking on the existing network. Radioservers are added automatically with the name **Server**.

To delete the created object, right-click on the object and then click **Remove Repeater**, **Remove Device** or **Remove Location** respectively.

## Adding Repeater

To add a repeater, click **Add Repeater** in the context menu. The window for setting up repeater parameters will open.



**Peer ID:** Unique identifier of the repeater.

**Name:** Any random name of the repeater. The name will be used in the **Topology** tab in *SmartPTT Dispatcher*. If the name is not set, the name from the repeater codeplug will be displayed.

**Description:** Random description of the repeater.

**SNMP Parameters:** Here you can set up the community name, which is used as a password for the external SNMP client to connect to the repeater.

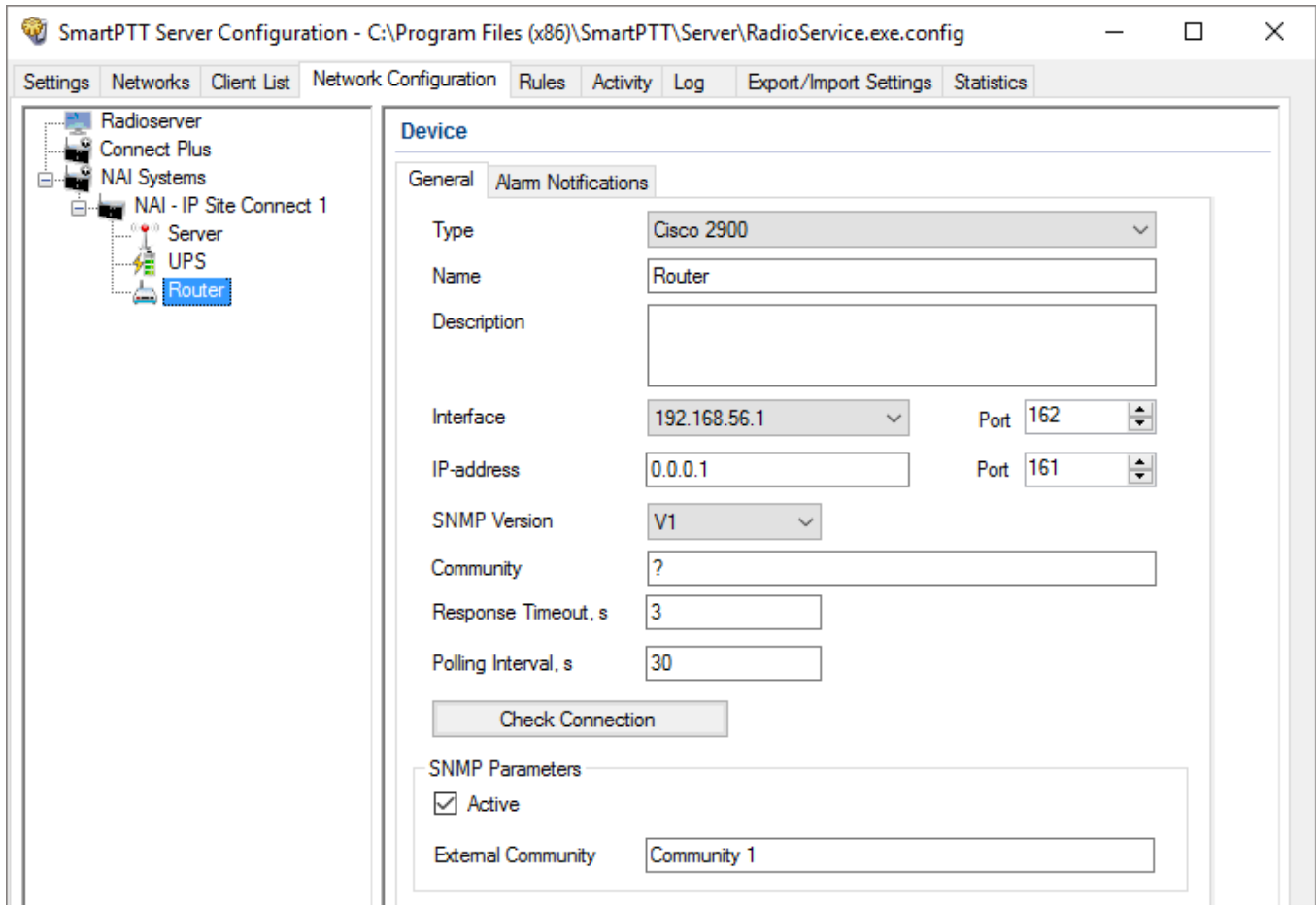
**Active:** Enable/Disable the external SNMP client.

**Community:** Community name used as a password for the external SNMP client to connect to the repeater.

In the **Alarm Notifications** tab you can set up automatic notification of alarms or errors occurred in the repeater. You can have the notifications sent to your email address, to your cell phone, to an SNMP client or to radios.

## Adding UPS and Routers and other devices

The supported devices include a router and an uninterruptible power supply (UPS). To add a device, click **Add Device** in the context menu. The following window appears:



**Type:** Device type. There are the following devices to choose from:

- Cisco2900 (router)
- Eaton9130 (UPS)
- Huawei Router
- UPS ATS-Convers
- Supermicro Server. This server allows you to receive information about the state of the radioserver and errors occurred on the radioserver. To be able to receive alarms from the radioserver, add Supermicro Server. If there are any alarms on the radioserver, you will see them in Monitoring event log in *SmartPTT Dispatcher*

- Apc 5000
- Unknown (for other devices not specified in the list)

**Name:** Random name of the device which is displayed in **Topology** in *SmartPTT Dispatcher*.

**Description:** Random description of the device.

**Interface:** The radioserver IP address used for interacting with the device.

**IP-address:** IP address of the device.

**SNMP Version:** Version of SNMP protocol used in the system. There are two options: versions 1 and 2 (V1 and V2).

**Community:** Community name, which is used as password to locally connect to the device over SNMP protocol.

**Response Timeout, s:** Time during which the server expects a response from the device. The maximum value is 10 sec.

**Polling Interval, s:** Time period at the end of which the radioserver sends a request to the device. The default value is 30 sec.

**Check Connection:** Checks if there is a connection to the device. At clicking the button a new window with the information on the connection status opens.

#### **SNMP Parameters:**

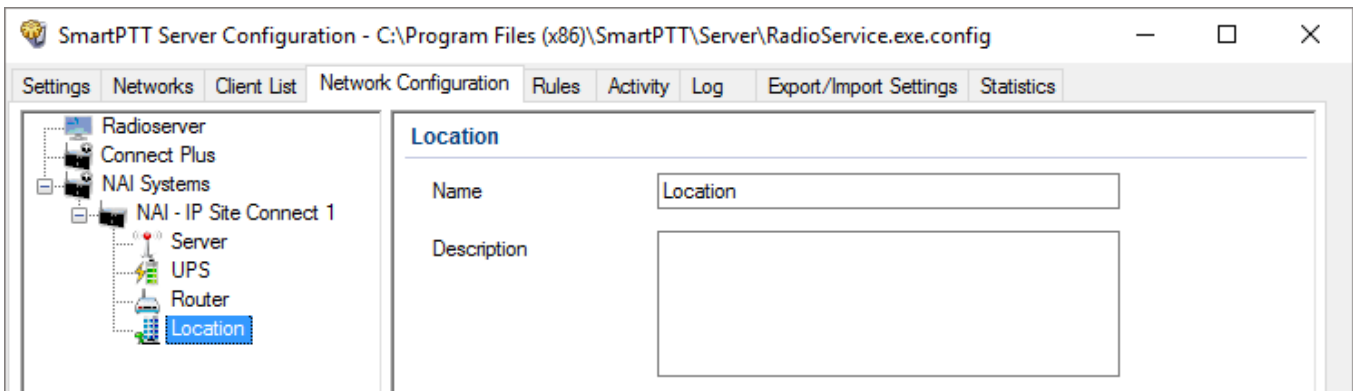
**Active:** Enable/Disable the external SNMP client.

**External Community:** Special community name which is used as password to connect to the device via external SNMP client.

To set up the automatic alarm notifications from the device, go to the **Alarm Notifications** tab.

## Adding Location

If there are many repeaters and devices, they can be grouped by location. In LCP systems a location represents a site (you can define **Site ID**). In Connect Plus systems a location can be used for added XRC controller. To add a location, select the **Add Location** option in the context menu. The following window appears:



**Name:** Any random name of the location. The name is displayed in the **Topology** tab in *SmartPTT Dispatcher*.

**Description:** Random description of the location which is displayed in the **Topology** tab in *SmartPTT Dispatcher* when hovering the mouse pointer over the object.

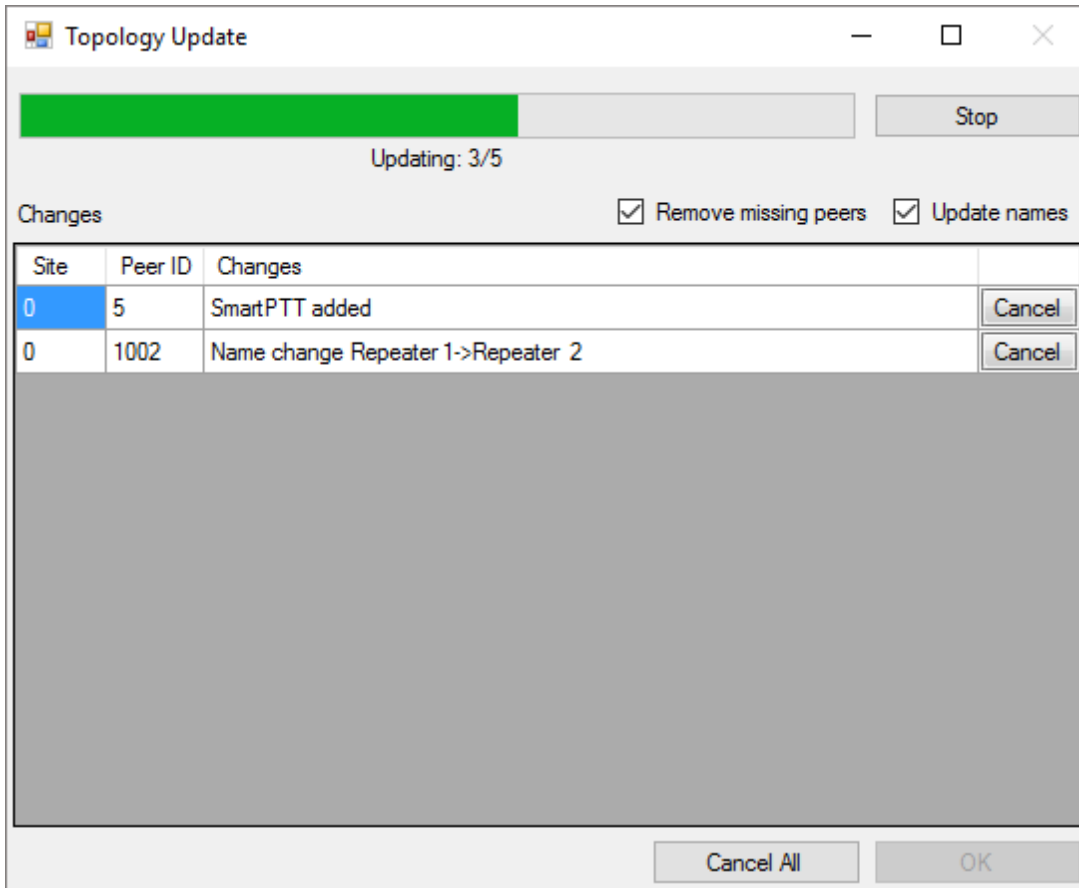
**Initial State:** Defines how the location object is to be displayed in the **Topology** tab in *SmartPTT Dispatcher*. If the check box is selected, all the devices and repeaters allocated to the location will be displayed by default. If the check box is not selected, the devices won't be seen inside the location by default. In this case, to see the devices, you will need to click on the location object in the **Topology** tab.

To add or remove a device or repeater from the location, simply drag it to another place.

### NOTE

When deleting a location with devices and repeaters allocated to it, all the devices will be deleted together with the location.

You can upload the network elements, instead of adding them manually. To do it, click **Update Topology**. At that, a pop-up window will open and the update process will start:



**Stop:** Interrupts the ongoing update process. All the changes that were made prior interruption—these you can see in the **Changes** table – will be applied after clicking **OK**.

**Remove missing peers:** Checks if there are any missing peers to exclude them from network topology.

**Update names:** Replaces names of repeaters by those defined in MOTOTRBO CPS.

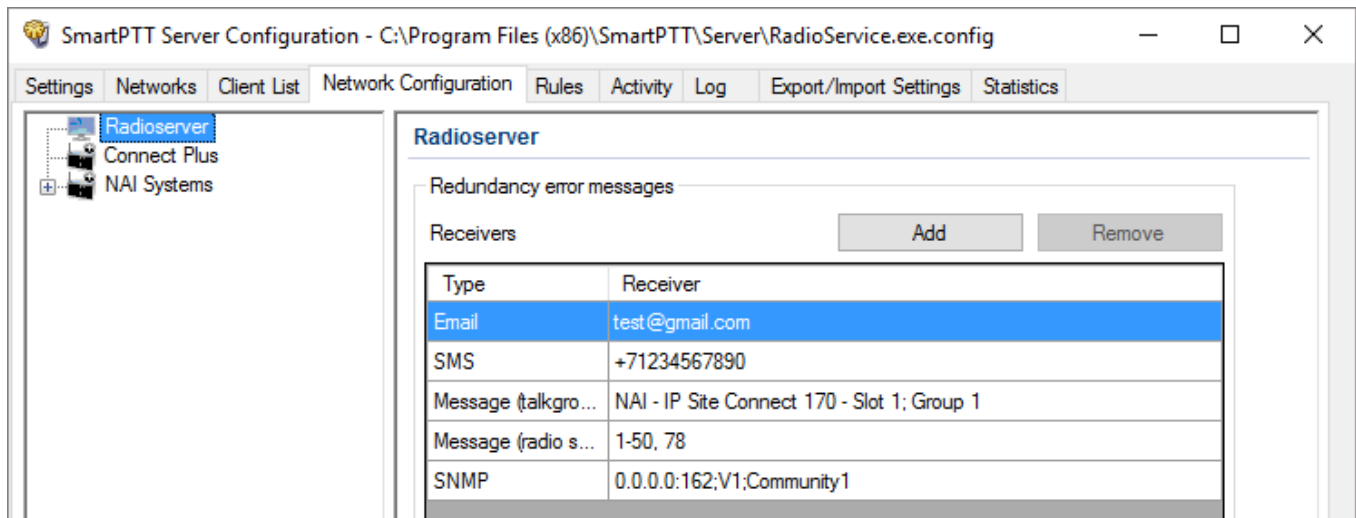
The **Changes** table shows all the changes made during the update process. You can discard changes by clicking **Cancel**. To discard all changes, click **Cancel All**. To apply the changes, click **OK**.

## Alarm Notifications

SmartPTT can notify radio and telephone subscribers, and other users about errors or other malfunctions occurred on devices used in the system or occurred during the redundancy.

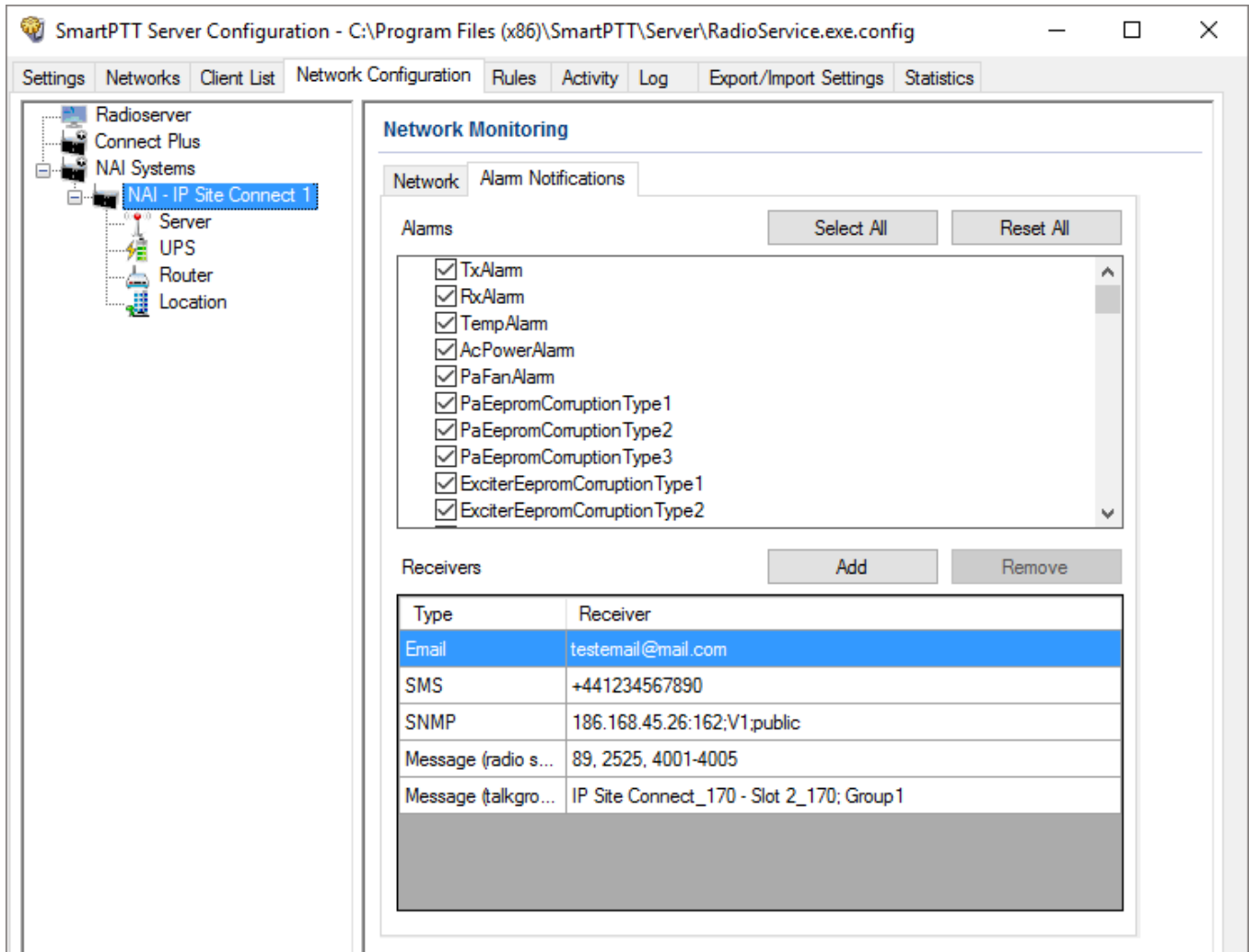


To set up automatic radioserver redundancy error notifications, in the left list of the **Network Configuration** tab click **Radioserver** (here your radioserver name is displayed) and create the list of notifications receivers.



To do it, click **Add**. There are several types of receivers: individual radios, talkgroups, telephone subscribers, email users, SNMP clients.

To set up automatic alarm notifications, click **Alarm Notifications** in the **Network Monitoring** window:



Select all the alarms you want to be notified about. Then create the list of notifications receivers. To do it, click **Add**. There are several types of receivers: individual radios, talkgroups, telephone subscribers, email users, SNMP clients.

The alarm notifications set in the **Network Monitoring** tab are applied to all elements of the radio network, but you can change them for each element of the network.

## 5 Rules

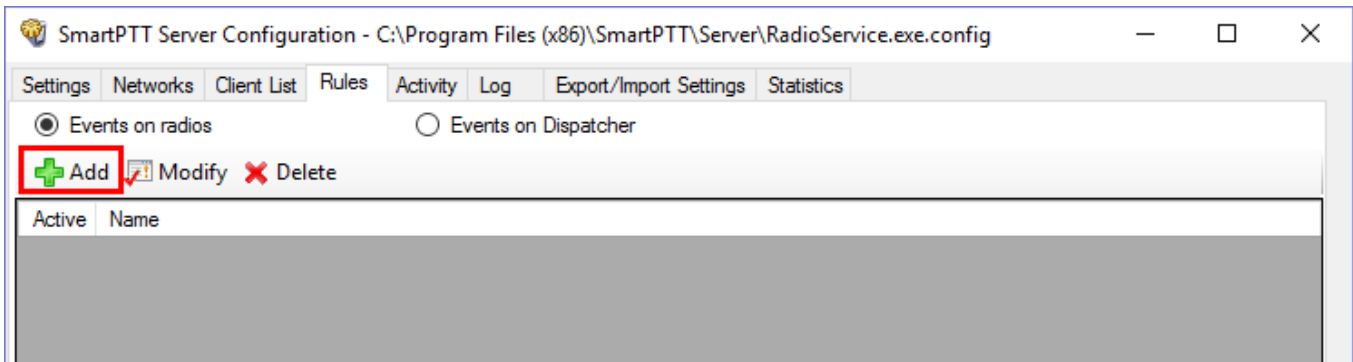
SmartPTT Radioserver allows you to set up rules for events on radios or Dispatcher. Rules allow the system to perform automatic actions (for example, playback sounds, send messages, play predefined voice notifications).

You can add new rules and modify or delete the existing rules.

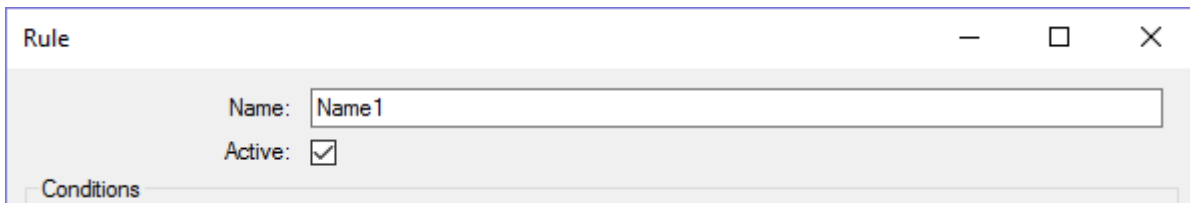
### 5.1 Adding Rule for Events on Radios

To create a rule for events on radios, follow these steps:

1. On the **Rules** tab, click **Events on radios** and then click **Add**.



2. In the window for creating a new rule type any rule name in the **Name** field.
3. Select the **Active** check box to make the rule active right after the creation.



4. Set the needed conditions of the rule:

**Conditions**

Direction:  Equal to Incoming

Event Type:  Equal to Telemetry Block Alarm

Date:

Additional Information:

Control Station:

Talkgroup:

Radio:  Equal to 0 0 0

User:

Status:  Equal to Call Alert Incoming Telem Unlocked

Duration:  Equal to 0

Name	Operation	Comment
<b>Direction</b>	Equal to	Select Incoming or Outgoing event
<b>Event Type</b>	Equal to	Select the event type
	Not equal to	
<b>Date</b>	Between	Set the start date and the end date
<b>Additional Information</b>	Equal to	Type any additional information, for example text message, task title and description, group call participant, etc.
	Contains	
<b>Control Station</b>	Equal to	Set the control stations names (see <a href="#">Control stations</a> )
	Contains	
<b>Talkgroup</b>	Equal to	Select the talkgroup name from the needed network
	Contains	
<b>Radio</b>	Equal to	Set the radio ID
	Not equal to	
<b>User</b>	Equal to	Select the radio users (see <a href="#">User Authorization</a> )
	Not equal to	

Name	Operation	Comment
<b>Status</b>	Equal to Not equal to	Select the system status
<b>Duration</b>	Equal to Not equal to Greater than Greater than or equal to Less than Less than or equal to Between	Set the duration of time in seconds

5. Set the needed actions of the rule:

**Actions**

Play Sound:   ..

Send Message:   ^ v

Example: 1-99, 150

Radios

User

Talkgroup

Send Message To Initiator

Start Voice Notification:

Stop Current Voice Notification:  Any

Name	Comment
<b>Play Sound</b>	Specify the audio file for the selected radios, users or talkgroups by clicking <b>Browse</b> [...] and selecting the needed .ogg, .wav or .mp3 file.

<b>Send Message</b>	<p>You can send a text message to the selected radio, user or talkgroups by typing the text in the Send Message field.</p> <p>Select the addressee by typing Radios ID or selecting the User or the Talkgroup.</p> <p>You can also send a message to the initiator if to select <b>Send Message To Initiator</b>.</p>
<b>Start Voice Notification</b>	<p>Specify the voice notification to play. If unavailable, add the voice notification in <a href="#">Voice Notification</a> on the <b>Settings</b> tab.</p> <p>If at the moment of adding the rule the system already has voice notification, the notification specified in the rule will not play.</p>
<b>Stop Current Voice Notification</b>	<p>Select any or specified current notification you want to stop.</p>

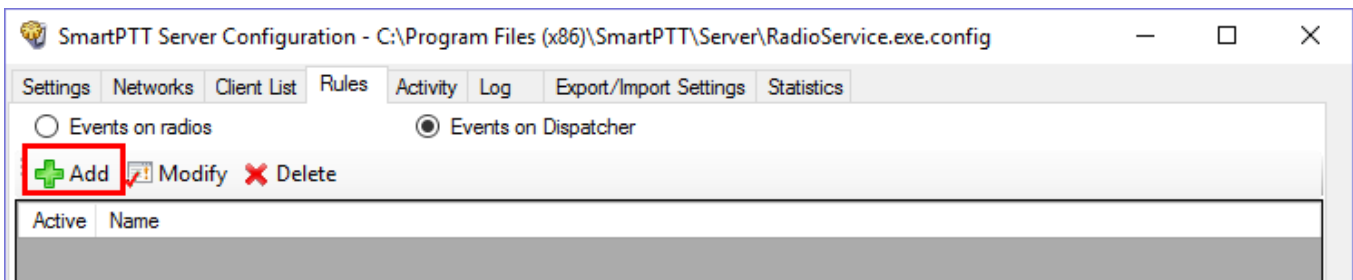
6. Click **Save** to save the created rule or click **Cancel** to cancel the rule adding.



## 5.2 Adding Rule for Events on Dispatcher

To create a rule for Events on Dispatcher, follow these steps:

1. On the **Rules** tab click **Events on Dispatcher** and then click **Add**.



2. In the window for creating a new rule type any rule name in the **Name** field.

3. Select the **Active** check box to make the rule active right after the creation.

4. Set the needed conditions of the rule:

Name	Operation	Comment
<b>Connection to Radioserver</b>	Lost	The rule works when the connection between SmartPTT radioserver and last dispatch console is terminated.
	Restored	The rule works when at least one SmartPTT Manager connects to radioserver.
<b>Timeout (s)</b>	Set time period	Time period in seconds, after which SmartPTT radioserver performs the selected actions.

5. Set the needed actions of the rule:

Name	Comment
------	---------

<b>Play Sound</b>	Specify the audio file for the selected radios, users or talkgroups by clicking <b>Browse [...]</b> and selecting the needed .ogg, .wav or .mp3 file.
<b>Send Message</b>	You can send a text message to the selected radio, user or talkgroups by entering the text in the <b>Send Message</b> field.  Select the addressee by typing Radios ID or selecting the User or the Talkgroup.
<b>Start Voice Notification</b>	Specify the voice notification to play. If unavailable, add the voice notification in <a href="#">Voice Notification</a> on the <b>Settings</b> tab.  If at the moment of adding the rule the system already has voice notification, the notification specified in the rule will not play.
<b>Stop Current Voice Notification</b>	Select any or specified current notification you want to stop.

6. Click **Save** to save the created rule or click **Cancel** to cancel the rule adding.



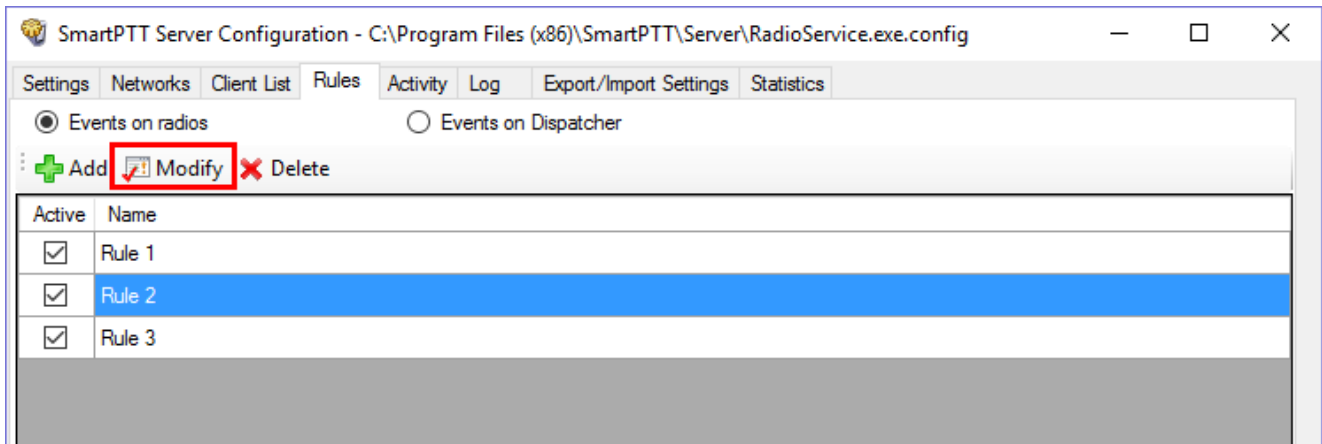
## 5.3 Modifying Rule



If you want to edit the existing rule, follow these steps:

1. On the **Rules** tab click **Events on radios** or **Events on Dispatcher**, depending on the rule you want to modify.
2. In the list of rules click the rule you want to modify.



3. Click **Modify** or double-click the rule.

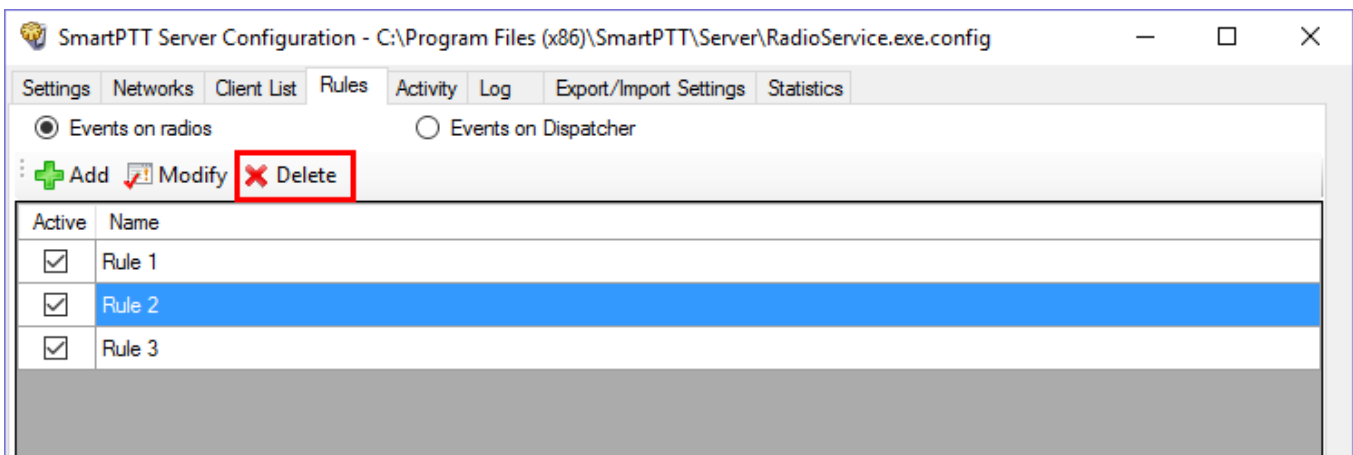


4. Make the needed changes in the rule in the opened window (see [Adding Rule for Events on Radios](#) or [Adding Rule for Events on Dispatcher](#)).
5. Click **Save**  to save changes.
6. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

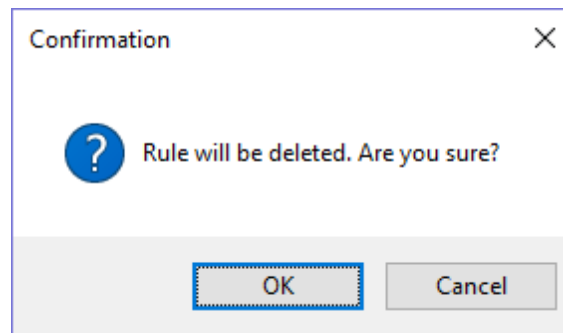
## 5.4 Deleting Rule



If you want to delete the rule, follow these steps:

1. On the **Rules** tab click **Events on radios** or **Events on Dispatcher**, depending on the rule you want to delete.
2. In the list of rules click the rule you want to delete.
3. Click **Delete**.



4. In the confirmation window click **OK** to delete the rule.

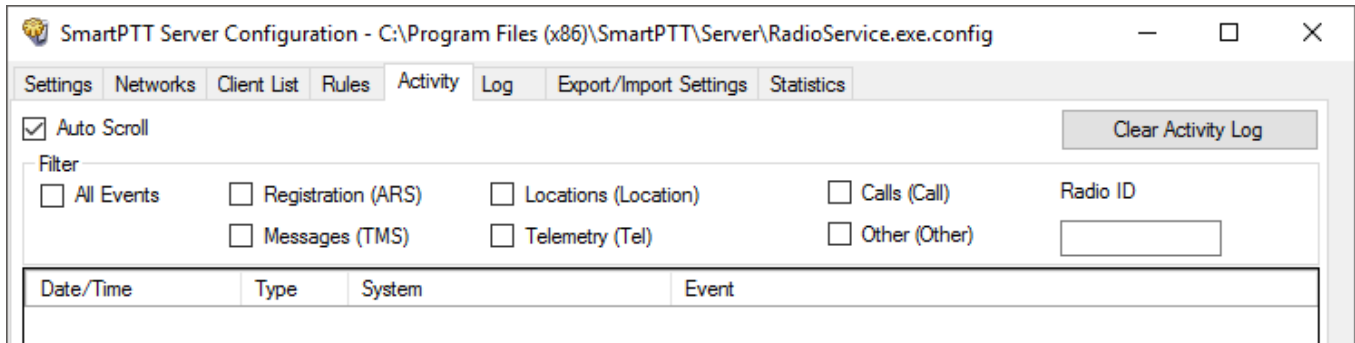


5. Click **Save**  to save changes.
6. Click **Restart**  to restart *SmartPTT Radioserver* and apply changes.

## 6 Activity

The **Activity** tab displays events that happen in the radio network. Mostly, it is used for debugging purposes, but it can be useful for system administrators as well.

To open **Activity**, click the **Activity** tab in SmartPTT Radioserver Configurator.



There are six types of events logged:

- Registration
- Messages
- Locations
- Telemetry
- Calls
- Other (includes connection or disconnection of slots or control stations)

You can enter the radio ID into the **Radio ID** field to view the events related to the particular radio.

You should select one or several of those check boxes to view events in the list.

All events are listed in the table with the following columns:

- **Date/Time:** The date and time of the event
- **Type:** The one of the listed types above
- **System:** The network where event happened
- **Event:** The brief description of the event and its status

You can apply the following settings for the list of events:

**Auto Scroll:** Select to make auto refresh of the list of events. When a new event will happen in the system, it will occur in the top of the list.

**Clear Activity Log:** Click to remove all events from the table. Events will be kept in the log files, they would be unavailable in the table of the **Activity** tab.

**Example**

Date and time in the regional format	Type of the event	Source of the event	Information on the event
Date/Time	Type	System	Event
9/1/16 9:40:00 AM	Location	Control Station 1	<span data-bbox="537 527 553 548">➤</span> 12.0.0.111 (111) TriggeredLocationReport id = 1, Latitude = 25.77528, Longitude = 80.20889, Timestamp: 9/1/16 9:40:00 AM

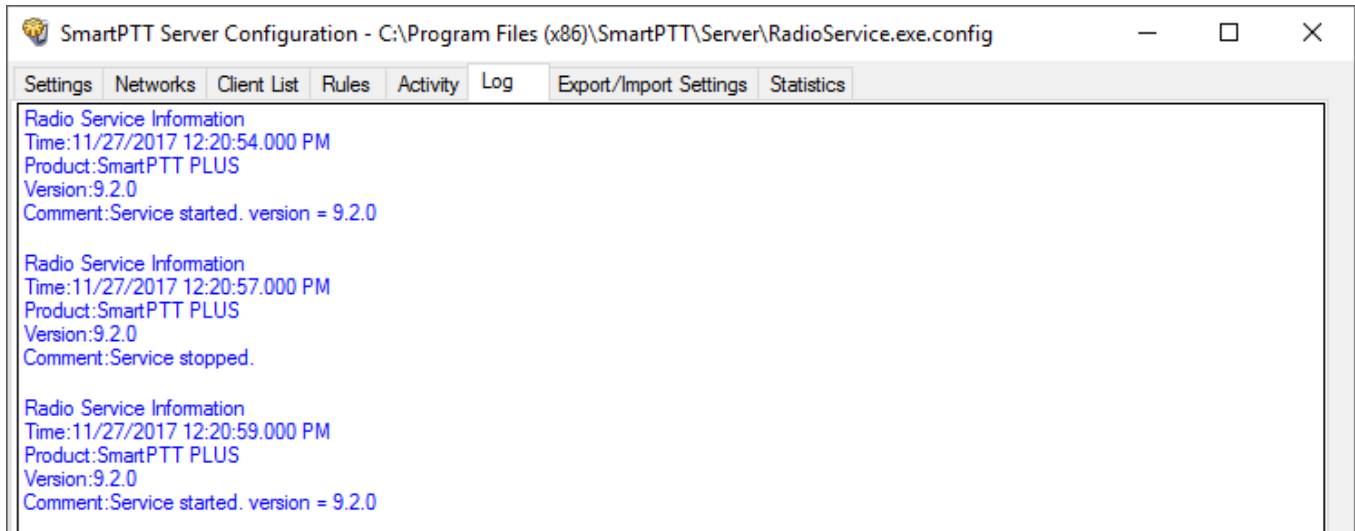
  

Initiator of the event	ID of the event initiator	Timestamp in the regional format
Incoming event	Description of the event	Content of the event

## 7 Log

The **Log** tab was designed to give information about the radio service system events. Mostly it is used for debugging purposes.

To see the log of the radio service, open the **Log** tab.



## 8 Export/Import Settings

SmartPTT Radioserver allows exporting configuration settings and database from one radioserver and importing them into another. Thus, the process of setting up new radioserver(s) with similar configuration settings becomes much easier and quicker.

### How to Export or Import Settings

To export or import the radioserver settings or/and the database, click **Export/Import Settings**.

The screenshot shows the 'SmartPTT Server Configuration' window with the 'Export/Import Settings' tab selected. The window title is 'C:\Program Files (x86)\SmartPTT\Server\RadioService.exe.config'. The interface is divided into two main sections: 'Export' and 'Import'.

**Export Section:**

- 'Save Export File As:' text box with a 'Browse' button.
- 'Settings' section with a checkbox for 'Export Radioserver Database'.
- 'Export' button.

**Import Section:**

- 'Choose File to Import:' text box with a 'Browse' button.
- 'Settings' section with a checkbox for 'Import Radioserver Database'.
- 'Override Settings' section with two radio buttons: 'Keep Server GUID' (selected) and 'All'.
- 'Import' button.

#### NOTE

Before exporting or importing the radioserver configuration settings and the database, stop the server. Otherwise, the buttons **Browse**, **Export** and **Import** will be unavailable.

### Exporting Settings and/or Database

To export the settings and/or the database of the radioserver, take the following steps:

1. Stop the radioserver.

2. Select the file where you want the settings to be exported by entering the path to the file in the **Save Export File As** field or by clicking **Browse**.
3. Select **Export Radioserver Database** if you want the database to be exported too.
4. Click **Export**.

**NOTE**

You cannot export the radioserver database separately (without the settings).

## Importing the Settings and/or the Database

To import the settings and/or the database to the radioserver, take the following steps:

1. Stop the radioserver.
2. Select the file from where you want the settings to be imported by entering the path to the file in the **Choose File to Import** field or by clicking **Browse**.
3. Select **Import Radioserver Database** if you want the database to be imported too.
4. Select the import mode:
  - **Keep Server GUID:** Import mode when the server globally unique ID is left unchanged. After importing, there are two servers with same configuration settings, but different globally unique GUID's. Use this mode if you need to copy settings to another server which is connected to the same dispatch console.
  - **All:** Import mode when all the server configuration settings, including the GUID, are replaced with the imported values. After importing, there are two servers with absolutely identical settings and GUID's. Use this mode if you need to restore your current server settings.
5. Click **Import**.

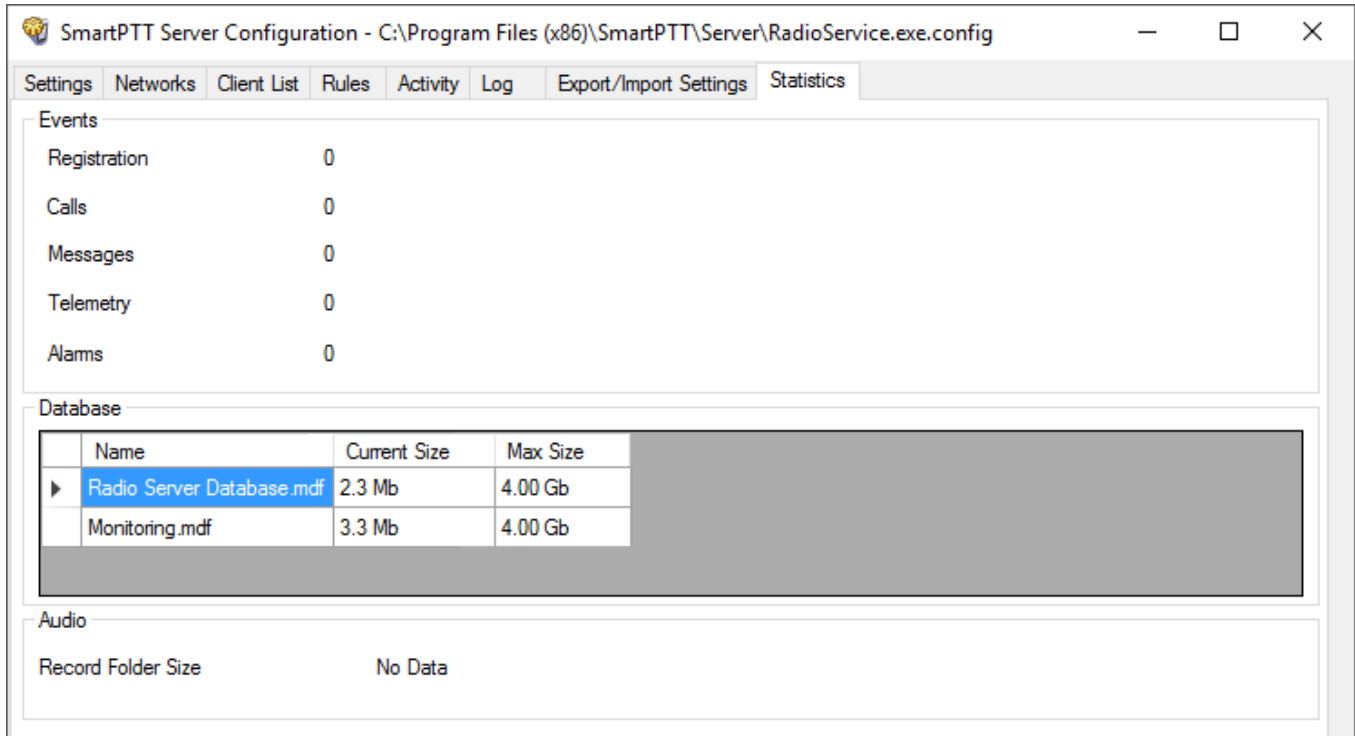
**NOTE**

After importing the radioserver settings with the option to override all the existing settings (**All**), it is important to delete one of the two servers to avoid GUID conflict.

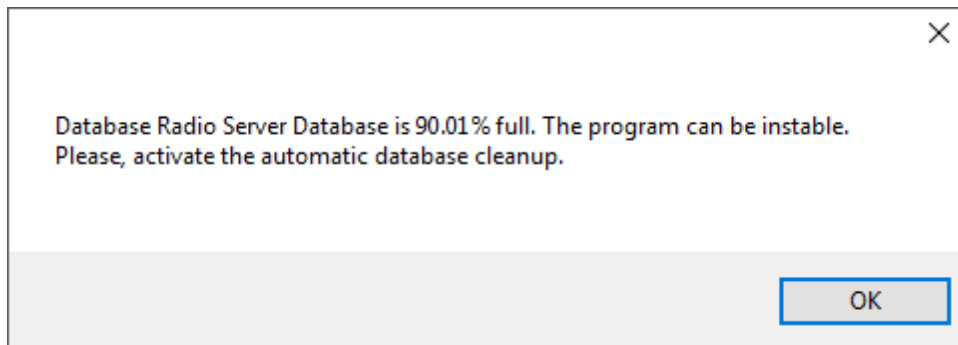
## 9 Statistics

The **Statistics** tab demonstrates you the following information:

- The total number of events on the radioserver (the Events field)
- The space on the hard drive used by the databases (the Database field)
- The space on the hard drive used by the audio records (the **Audio** field)



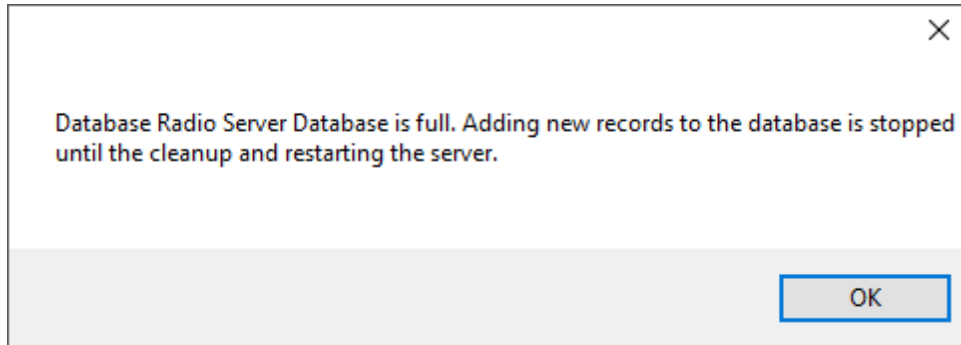
When the total size of records in your database exceeds 90% of the maximal size, a message will appear:





From this message you can learn the size of the records in your database. This message will appear at the every start of *SmartPTT Radioserver Configurator*. Then, if database is not cleaned up, it will appear every 30 min.

When the total size of records in your database reaches its maximum, another message will appear:



This message will appear at the every start of *SmartPTT Radioserver Configurator*. Then, if database is not cleaned up, it will appear every 30 min.

**NOTE**

In rare cases you may see the message that database is 100.00% full. It actually means that database is 99.995% full.

