TRBONET
Dispatch Systems

neocom software

AUTHORIZED APPLICATION PROVIDER DIMETRA™ MOTOROLA SOLUTIONS

AUTHORIZED APPLICATION PROVIDER MOTOTRBO™ MOTOROLA SOLUTIONS

TRBOnet Watch

User Manual

Version 4.3

Last revised on 29 September 2026

USA Office
Neocom Software
150 South Pine Island Rd., Suite 300
Plantation, FL 33324, USA

Sales
EMEA: +44 203 608 0598
Americas: +1 872 222 8726
APAC: +61 28 607 8325

www.trbonet.com
info@trbonet.com

© Neocom Software Corporation

Contents

1 Introduction 4
1.1 About This Guide 4
1.2 About TRBOnet 4
1.3 Contacts 4
2 Overview 5
2.1 About TRBOnet Watch 5
2.2 Features 6
2.3 Architecture 6
2.4 Hardware and Software Requirements 7
2.5 Compatibility with MOTOTRBO Firmware Versions 7
2.6 Licensing 8
2.7 System Monitoring Levels 8
3 Installation and Upgrade 11
3.1 Installing TRBOnet Watch 11
3.2 Repairing TRBOnet Watch 11
3.3 Uninstalling TRBOnet Watch 12
3.4 Upgrading TRBOnet Watch 12
4 TRBOnet Watch Server 13
4.1 Launching TRBOnet Watch Server 13
4.2 Managing the Software License 13
4.3 Creating a TRBOnet Watch Database 14
4.4 Data Types 19
4.5 Network Parameters 19
4.6 Advanced Settings 20
4.7 Systems 22
4.8 SNMP Communication 22
4.9 Mobile Gateways 24
4.10 Installing and Starting the Service 25

5 TRBOnet Watch Console 28
5.1 Connecting to TRBOnet Watch Server 28
5.2 Main Window Overview 29
5.3 Console Settings 31
5.4 Radio Systems 34
5.5 Server Settings 54
5.6 Dashboard 70
5.7 Channels 71
5.8 Health Monitor 77
5.9 Topology 83
5.10 Map 86
5.11 Incident Management 92
5.12 Reports 99
6 TRBOnet Watch Mobile 103
6.1 Installation 103
6.2 Connection to TRBOnet Watch Server 103
6.3 Operation 105
Appendix A: Charts and Reports 110
A.1 Charts 110
A.2 Reports 125
Appendix B: SNMP Support 137
B.1 MIB Files 137
B.2 MIB Objects 138
B.3 Alarms 139
B.4 Examples 141
Appendix C: RCM Messages 143
Appendix D: Glossary of Acronyms 145

1 Introduction

1.1 About This Guide

This document is intended for the radio network control room personnel in charge of the radio system monitoring and maintenance. It introduces the user interface and functionality of the TRBOnet Watch Server and TRBOnet Watch Console applications.

1.2 About TRBOnet

TRBOnet is a suite of professional applications for the MOTOTRBO digital two-way radio networks. TRBOnet manages voice, text and data communication paths to network endpoints and provides a unified graphical dispatcher workbench interface for all the messaging and workforce orchestration tasks.

1.3 Contacts

Region	Phone	Email & Support
EMEA	+44 203 608 0598	info@trbonet.com — general and commercial inquiries support@trbonet.com — technical support https://trbonet.com/kb/ — online knowledge base
Americas	+1 872 222 8726	
APAC	+61 28 607 8325	

2 Overview

2.1 About TRBOnet Watch

TRBOnet Watch is an advanced software packet sniffer designed for logging and analyzing data streams in your MOTOTRBO radio networks. This solution also gives you an integrated view into the health of your network. The application monitors infrastructure resource usage and allows a user to detect topology problems and verify that all components of the system are configured correctly.

The software provides views of system performance from every perspective. Built-in tools and monitors greatly reduce time required for data analysis and eliminate the necessity for on-site visits. This cutting-edge technology enables a simple setup procedure and does not require NAI Data licenses.

The **Channels** tab shows activity on each slot of your system. TRBOnet Watch is capable of determining what kind of data is transmitted on available channels. You can easily verify that radios send registration statuses and GPS data to the system. This software can recognize voice calls, telemetry, and option board data, as well as text messages and system packets. The log contains detailed information about each entry including sender and recipient identifiers, slots, talk groups and signal strength for calls.

The **Topology** tab gives you an insight into MOTOTRBO networks connected to TRBOnet Watch. It helps you pinpoint configuration problems and check if there have been any alarms from the repeaters. This is especially useful for large multi-site systems. It also allows you to check if new repeaters have been successfully added to your network. The Topology screen allows you to verify that all components of the system have unique identifiers and there are no conflicting identifiers.

The **Health Monitor** tab provides full information about IP connections in the system and the uptime for each repeater. This tab offers enhanced features such as remote channel change or disabling repeaters.

The **Reports** tab is used to visualize megabytes and gigabytes of information obtained from the radio network. Advanced filters help you get a clear understanding of system performance by system name, slot, frequency, unit ID or talk group. This information can be used to bill customers using your radio infrastructure. The Channel Usage and Frequency Usage reports are of interest to those who want to ensure their systems have sufficient capacity for efficient communications. The All Channels Busy report shows how often the radio channels have not been available for radio users within a user defined time interval.

2.2 Features

TRBOnet Watch features include:

- Support for all MOTOTRBO platforms
- Multiple systems monitoring
- Topology problem detection
- Real-time traffic capture
- Network usage by system, site, slot, channel, talk group, radio user
- Hardware alarms
- Signal strength
- RSSI level map
- SNMP integration
- No NAI Data licenses required

2.3 Architecture

TRBOnet Watch is a client-server solution that does not require additional hardware and can be added to a MOTOTRBO radio system of any size and architecture.

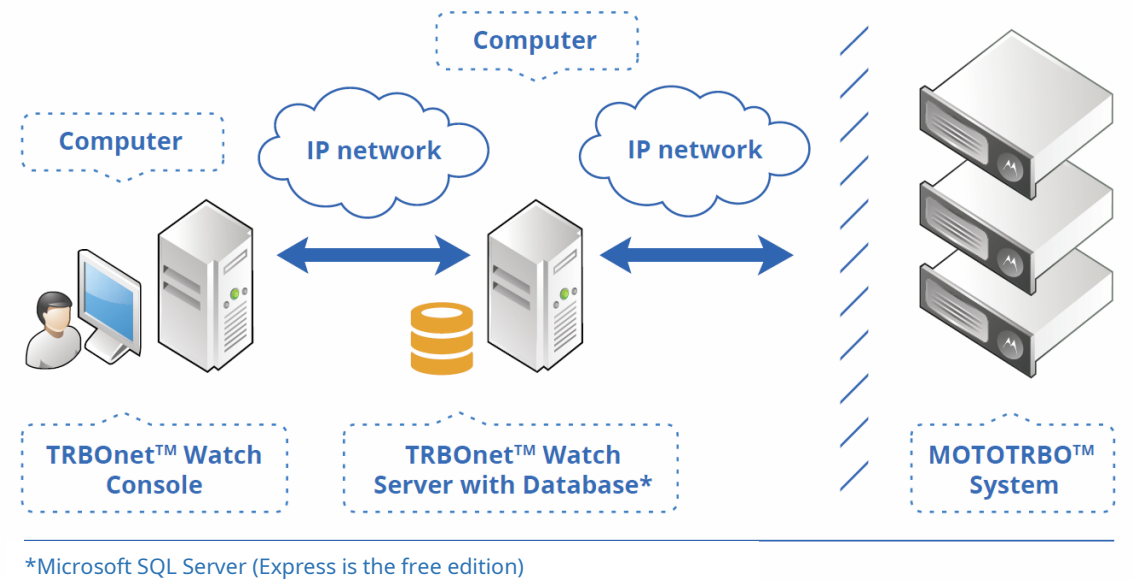


Figure 1: TRBOnet Watch architecture

The server part of the application is installed on any networked computer that meets the hardware and software requirements. The TRBOnet Watch Server implements the MOTOTRBO protocols, manages IP connection to repeaters, and stores data.

The client software can run on any remote computer and receives all the information about the system from anywhere over an IP connection.

2.4 Hardware and Software Requirements

Table 1: TRBOnet Watch hardware and software requirements

TRBOnet Watch Server			
Channels	Less than 50	Greater than 51 but less than 250	250+
CPU	Intel Core i3/i5	Intel Core i7	Contact technical support
Memory	4 GB	8 GB	
HDD	2 GB for installation files		
Sound Card	No		
Supported OS	Windows 10 (x64)/11, Windows Server 2016/2019/2022 (x64) Note: Windows Server 2016/2019/2022 requires Desktop Experience Role/Feature installed.		
Software	.NET Framework 4.8, MS SQL Server 2016 or higher		
TRBOnet Watch Console			
CPU	Intel Core i5		
Memory	4 GB		
HDD	2 GB for installation files		
Sound Card	Yes		
Display	1600x900 minimum resolution, 1920x1080 and higher resolution is recommended		
Additional Devices	Speakers		
Supported OS	Windows 10 (x64)/11		
Software	.NET Framework 4.8		

2.5 Compatibility with MOTOTRBO Firmware Versions

TRBOnet Watch can monitor all kinds of traffic on MOTOTRBO systems IP Site Connect, Capacity Plus Single Site, Capacity Plus Multi-Site, Extended Range Direct Mode (ERDM), and Capacity Max. The following table describes the compatibility between TRBOnet Watch product versions and MOTOTRBO firmware versions for each supported system type.

Table 2: MOTOTRBO firmware versions compatible with TRBOnet Watch

TRBOnet Watch version	IPSC	Capacity Plus Single Site	Capacity Plus Multi-Site	ERDM	Capacity Max
2.3.5	02.40.12			Not supported	
2.5	02.06.00.07			02.07.00.03	
3.0	02.08.00.07			02.08.00.07	

TRBOnet Watch version	IPSC	Capacity Plus Single Site	Capacity Plus Multi-Site	ERDM	Capacity Max
3.2	2.10.0.13			2.10.0.13	
4.0	2.10.0.13			2.10.0.13	

2.6 Licensing

When you purchase TRBOnet Watch, you obtain a permanent (non-expiring) license that specifies functional modules and types of radio networks available for users. All repeaters that need to be monitored must be included in the license. If the actual number of repeaters exceeds the license limits, extra connections are ignored.

The list of optional features includes:

- Additional repeater connections
- Additional consoles
- RSSI monitoring
- Watch for mobile devices

2.7 System Monitoring Levels

TRBOnet Watch can monitor a MOTOTRBO system on one of the following levels:

- Level 1: Link Establishment: Watch monitors all IP connections in the system.
- Level 2: Diagnostics: Watch monitors all IP connections in the system and RDAC connections of all repeaters in the system.
- Level 3: Call Monitoring: Watch monitors all IP and RDAC connections in the system and air traffic in the system channels. Traffic is not parsed.
- Level 4: Call Parsing: Watch monitors all IP and RDAC connections in the system and air traffic in the system channels. Traffic is parsed, all types of traffic are recognized.

The features available in TRBOnet Watch Console depend on the system type as well as on the monitoring level specified for each system in the TRBOnet Watch Server configuration tool. Some features require a special license.

The following table summarizes the functionality available in TRBOnet Watch Console for each system type and at each level of system monitoring.

Table 3: TRBOnet Watch Console functionality available on each level of system monitoring

TRBOnet Watch feature	IP Site Connect	ERDM	Capacity Plus	LCP	Capacity Max
Level 1: Link establishment					
Diagnostics	IP connection status				
Topology	IP connections only				
Reports	Event Viewer only. Other reports display no information.				
Level 2: Diagnostics					
Diagnostics	Full support				Level 2 is not supported
Topology	Full support				
Reports	Event Viewer only. Other reports display no information				
Level 3: Call monitoring					
Diagnostics	Full support				-
Topology	Full support				
Real-time traffic monitoring	Slots, channels	Slot	Channels	Channels	Channels
Recognized traffic:					
▪ Location	-	-	-	-	Yes
▪ System	Yes	Yes	Yes	Yes	Yes
▪ Voice	Yes	Yes	Yes	Yes	Yes
▪ Data	Yes	Yes	Yes	Yes	Yes
Call parsing	Not supported				
Reports:					
RSSI Levels: GPS	Yes	Yes	Yes	Yes	Yes
RSSI Levels: Map	Yes	Yes	Yes	(with TRBOnet PLUS only)	(with TRBOnet PLUS only)
GPS Data	-	-	-	-	-
Text Messages	-	-	-	-	-
Charts	All	All	All	All	All

TRBOnet Watch feature	IP Site Connect	ERDM	Capacity Plus	LCP	Capacity Max
Level 4: Call Parsing					
Diagnostics	Full support			Level 4 is not supported	
Topology	Full support				
Reports	All	All	All		
Charts	All	All	All		
Real-time traffic monitoring	Slots, channels	Slot	Channels		
Recognized traffic:					
▪ Registration	Yes	Yes	Yes		
▪ Telemetry	Yes	Yes	Yes		
▪ Text	Yes	Yes	Yes		
▪ Location	Yes	Yes	Yes		
▪ System	Yes	Yes	Yes		
▪ Voice	Yes	Yes	Yes		
▪ User	Yes	Yes	Yes		
▪ Data	Yes	Yes	Yes		
▪ Option Board	Yes	Yes	Yes		
Call parsing	Yes	Yes	Yes		
Listening to voice transmitted on the channel (Mute button)	Yes	Yes	Yes		

3 Installation and Upgrade

This section describes how to install, repair, uninstall, and upgrade your TRBOnet Watch software to the higher version.

3.1 Installing TRBOnet Watch

Before you start installing TRBOnet Watch, make sure that your computer meets the minimum hardware and software requirements. For more information, refer to section 2.4, Hardware and Software Requirements (page 7).

To install TRBOnet Watch:

1. Double-click the *TRBOnet.Watch_<version>.exe* file to run the TRBOnet Watch setup wizard. Click **Next**.
2. Accept the terms in the license agreement. Click **Next**.
3. Select the installation type:
   - **TRBOnet Watch Console and Server**: Choose to install both the server and client software on one computer.
   - **TRBOnet Watch Console**: Choose to install only the client software on the computer, for instance, on the dispatcher's desktop.
4. Click **Next**.
5. Click **Install**, then click **Finish** to exit the setup wizard.

After the installation is finished, you need to specify several configuration settings as described in section 4, TRBOnet Watch Server (page 13).

3.2 Repairing TRBOnet Watch

To repair the TRBOnet Watch installation:

1. Double-click the *TRBOnet.Watch_<version>.exe* file to run the TRBOnet Watch setup wizard. Click **Next**.
2. Select the **Repair** option.
3. Click **Repair**, then click **Finish** to exit the setup wizard.
4. Run the TRBOnet Watch Server as a Windows service as described in section 4.10, Installing and Starting the Service (page 25).

Except for the Windows service, the repaired installation keeps all configuration settings unchanged.

3.3 Uninstalling TRBOnet Watch

To uninstall TRBOnet Watch from your computer:

1. Double-click the *TRBOnet.Watch_<version>.exe* file to run the TRBOnet Watch setup wizard. Click **Next**.
2. Select the **Remove** option.
3. Click **Remove**. TRBOnet Watch is removed from your desktop.

Note: Log files, configuration files, and folders are not removed from the disk automatically. Uninstalling TRBOnet Watch does not affect the TRBOnet Watch database.

3.4 Upgrading TRBOnet Watch

To upgrade TRBOnet Watch:

1. Uninstall the current version of TRBOnet Watch as described in section 3.3, Uninstalling TRBOnet Watch (page 12).
2. Install the TRBOnet Watch as described in section 3.1, Installing TRBOnet Watch (page 11).
3. Launch the TRBOnet Watch Server.

   The configuration settings of the uninstalled server are preserved in the configuration file and are displayed in the **TRBOnet Watch Server** window after the upgrade.
4. Run TRBOnet Watch Server as a Windows service as described in section 4.10, Installing and Starting the Service (page 25).
5. Click **Database** in the **Configuration** pane. Then click **Upgrade Database** in the right pane.

4 TRBOnet Watch Server

This section describes how to configure your TRBOnet Watch for radio network monitoring and diagnostics.

4.1 Launching TRBOnet Watch Server

To launch the TRBOnet Watch Server, double-click the **Watch Server** icon on the desktop, or click **All Programs** and then navigate to **Neocom Software** and **Watch Server** on the **Start** menu.

When the TRBOnet Watch Server is launched for the first time, the main configuration window appears.

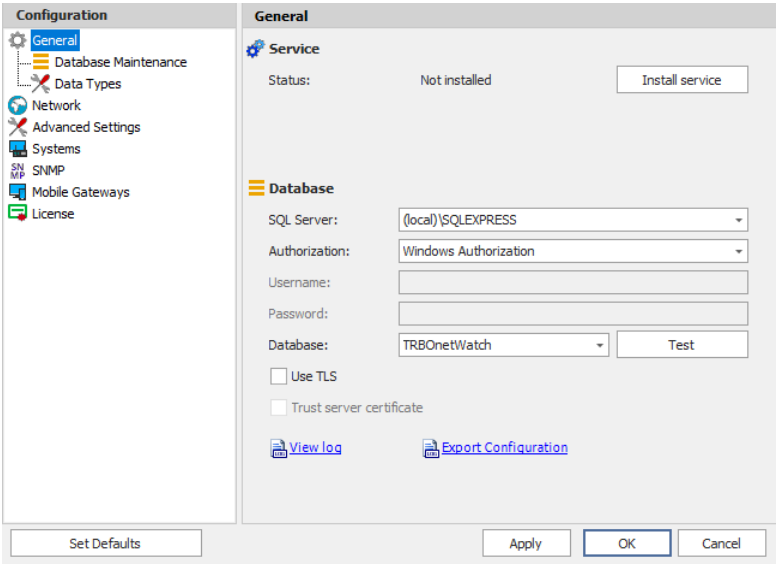


Figure 2: TRBOnet Watch Server – General

4.2 Managing the Software License

TRBOnet Watch contains a free trial license that allows you to evaluate the product.

To use the product after the evaluation period, order a license from a reseller or Neocom Software directly. Include the information about your current license in the request. This can be done by opening the **License** tab, clicking **Copy to Clipboard**, and inserting the copied details to the request.

To apply a new license:

1. Copy the new license file to a local folder. If this folder contains other license files, delete them.
2. In the **TRBOnet Watch Server** window, select **License** in the **Configuration** pane.
3. Click **License Manager**. The **License Manager** dialog box appears.

4. Click **Next**. Click the search button next to the **License file** field and navigate to the license file.
5. Click **Next**, then click **Finish**.

4.3 Creating a TRBOnet Watch Database

Perform the following steps to create a TRBOnet Watch database.

Note: Before creating a database, make sure that an SQL Server application is installed on your server or on a networked storage device. For the list of SQL Server editions compatible with the current version of TRBOnet Watch, refer to section 2.4, Hardware and Software Requirements (page 7).

To create a TRBOnet Watch database:

1. In the **TRBOnet Watch Server** window, select **Database** in the Configuration pane.
2. Specify the following database connection properties:

Table 4: TRBOnet Watch Database connection properties

Property	Description
SQL Server	The SQL Server. Select an instance from the list of the database management systems found on your network.
Authorization	The authorization method. Select the preferred option: ▪ **Windows Authorization**: TRBOnet Watch will use your Windows credentials to access the database. To use Windows authorization, the Local System account must be granted MS SQL Server administrator privileges. For details, refer to section 4.3.2, Configuring the Local System Account (page 16). ▪ **SQL Server Authorization**: TRBOnet Watch will use an MS SQL Server user account to access the database. To use SQL Server Authorization, the MS SQL Server user account must be granted MS SQL Server administrator privileges.
Username	The MS SQL Server username. Required for SQL Server Authorization.
Password	The MS SQL Server user password. Required for SQL Server Authorization.

Property	Description
Database	The preferred database name. Follow the naming rules specific to the selected SQL Server edition. Type the new database name and click **Create**. You can also use one of the following two options: Click **Create and import configuration** to set up a new database using an existing configuration file. Click **Create using current configuration** to create a new database using the configuration of the current database. Note: This option may be useful if the database of TRBOnet Watch 4.0 reaches its maximum size and you want to create a new database using the same settings.
Use TLS	Select this option to enable TLS encryption for database connections.
Trust server certificate	Select this option to skip certificate verification.

3. Configure how the TRBOnet Watch database will be maintained. For details, refer to section 4.3.3, Configuring Database Maintenance (page 17).

Once the database connection is established, you will be able to configure server parameters.

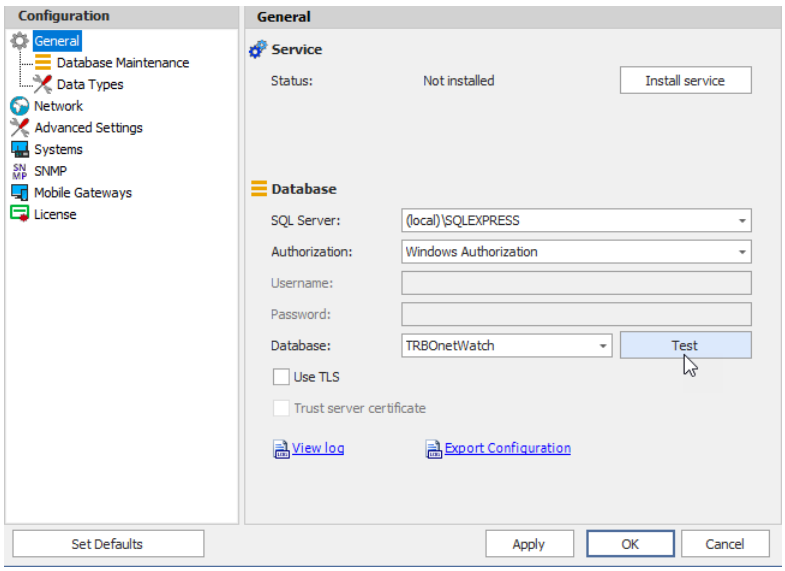


Figure 3: TRBOnet Watch Server – Database created

4.3.1 Updating TRBOnet Watch Database

To update a previously created TRBOnet Watch database:

- Click the arrow on the right of the **Database** box, and from the list, select the Watch database, and click **Test**.

> Note: If the test fails because of an incorrect database version, you will be prompted to start the wizard to update the database to the correct version (**Fix with the wizard**).

4.3.2 Configuring the Local System Account

If the TRBOnet Watch database connection uses Windows authentication, verify that the list of MS SQL Server administrators includes the Local System account. Otherwise, the following error message will be displayed when attempting to connect to the database:

Cannot open the database requested by the login. The login failed. Login failed for user 'NT AUTHORITY\SYSTEM'.

Privileges for the Local System account can be configured (granted) during or after the MS SQL Server installation.

To grant administrator rights to Local System when installing MS SQL Server:

1. Run MS SQL Server setup. Click **Database Engine Configuration** and then the **Server Configuration** tab.
2. Under **Specify SQL Server administrators**, click **Add**.
3. In the **Select Users or Groups** window, click **Advanced**.
4. Click the **Find** button and select the LOCAL SERVICE account. Click **OK** to add the user and close the window. The NT AUTHORITY\LOCAL SERVICE(LOCAL SERVICE) user appears in the list of SQL Server administrators.
5. Click **Next** and follow the prompts to finish setup.

To grant administrator rights to Local System after MS SQL Server installation:

1. Launch MS SQL Server Management Studio.
2. In the **Connect to Server** dialog box, expand the **Server name** menu and point the SQL Server instance on which the TRBOnet Watch database is created. Click **Connect**.



Figure 4: Connecting to the SQL Server instance

3. In the **Object Explorer** pane, expand the SQL Server instance to which you have just connected.
4. Go to the **Security** node and select **Logins**.
5. Under the **Logins** node, right-click **NT AUTHORITY\SYSTEM** and click **Properties**.
6. In the **Login Properties** window, click **Server Roles** in the left pane. Select the **sysadmin** checkbox in the right pane.
7. Click **OK** to add sysadmin privileges to the selected user.

4.3.3 Configuring Database Maintenance

To prevent data loss and reduce the size of the TRBOnet Watch database, regularly create database backups and delete old data. You can do it at your convenience (unscheduled), or you can schedule regular database maintenance.

To configure database maintenance:

- In the **Configuration** pane, select **General** > **Database Maintenance**.

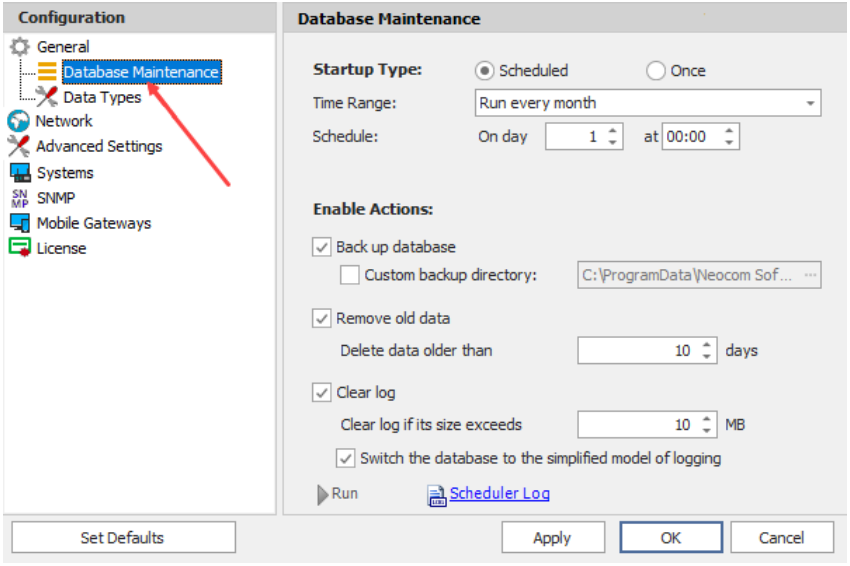


Figure 5: Configuring database maintenance

In the **Enabled Actions** section of the right pane, enable the required options:

- **Back up database**
  Select this option to back up the database to the default local folder. To save the backup to a particular folder, select **Custom backup directory**, click the **Search** button in the edit box, and select the preferred folder.
- **Remove old data**
  Select this option to remove old data from the database. Configure the options:
  - **Delete data older than**
    For scheduled maintenance, specify the number of days to keep the data.
  - **Delete data created before**
    For occasional maintenance, specify the date before which all data should be cleared.
- **Clear log**
  Select this option to clear the transaction log. Configure the options:
  - **Clear log if its size exceeds**
    Specify the maximum allowed log size (in MB). If the threshold is exceeded, the transaction log is cleared.
  - **Switch the database to the simplified model of logging**
    If your database uses the full transaction logging model, select this option to switch to the simplified model in order to reduce the volume of logged transactions.

    If the database uses the simplified logging model, this option is unavailable.

The database maintenance options are executed in the order they appear in the **Database Maintenance** pane. If backup is enabled, the data is backed up and then removed.

To schedule database maintenance:

1. In the right pane, click the **Scheduled** option.
2. On the **Time Range** menu, select to run database maintenance every hour, day, week, or month.
3. Specify the day and/or time for maintenance to be started.
4. Select the actions to be executed.
5. Click **Apply** to save the changes.

To run database maintenance immediately:

1. In the right pane, click the **Once** option.
2. Select the actions to be executed.

3. Click **Run** to start maintenance. The progress of the selected operations is displayed in the **Database Maintenance** window.

When maintenance is complete, the **Results** area displays the maintenance log record.

To view all records in the database maintenance log, click the **Scheduler Log** link and click the **Scheduler** tab in the **View log entries** window.

4.4 Data Types

If your radio systems use protocols other than standard MOTOTRBO protocols (ARS, Location, Text Messaging, and Telemetry), you can configure the appropriate ports.

- In the **Configuration** pane, select **General > Data Types**.

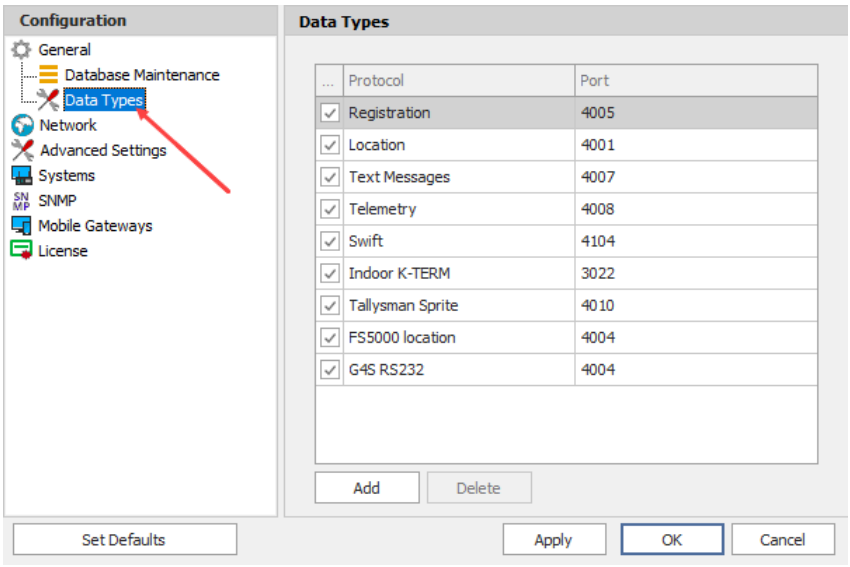


Figure 6: Configuring data ports

- **Protocol**
  From the list, select the protocol name.
- **Port**
  Specify the port number that will be used for the selected protocol.

4.5 Network Parameters

Perform the following steps to configure IP communications between TRBOnet Watch Server and TRBOnet Watch Consoles.

To specify the IP network settings:

- In the **TRBOnet Watch Server** window, select **Network** in the **Configuration** pane.

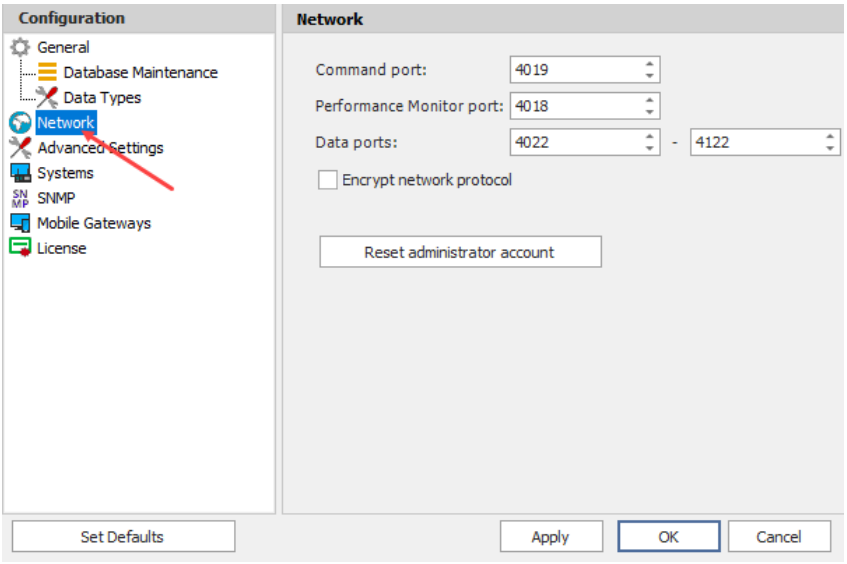


Figure 7: Configuring the Network settings

- In the **Network** pane, specify the following settings:
  - **Command Port**
    Specify the IP port for communications with TRBOnet Watch Console (default value: 4019).
  - **Performance Monitor port**
    Specify the port that will be used to monitor computers with running TRBONET Enterprise | PLUS software.
  - **Data ports**
    Specify the ports for transferring data.
  - **Encrypt network protocol**
    Select this option for TRBOnet Watch Server to communicate via encrypted data with TRBOnet Watch Console.
  - **Reset administrator account**
    Click this button to reset the administrator's login and password to their default values.

4.6 Advanced Settings

- In the **TRBOnet Watch Server** window, select **Advanced Settings** in the **Configuration** pane.

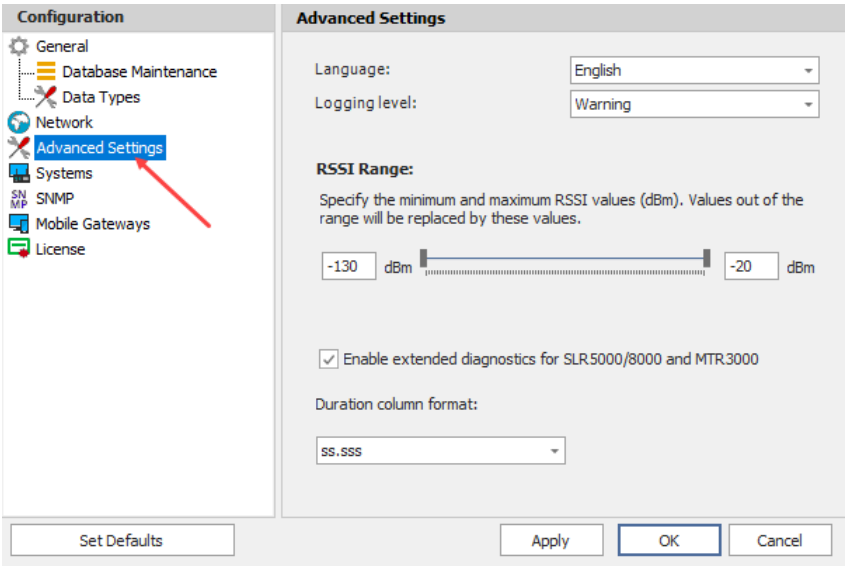


Figure 8: Advanced settings

- **Language**
  From the drop-down list, select one of the supported interface languages.
- **Logging level**
  From the drop-down list, select the preferred level of detail in the system log: **Debug**, **Information**, **Warning** (default), or **Error**. Use the default **Warning** option unless you are requested by the technical support team to select a different level.

  Note: The TRBOnet Watch Server logs specific information that can help the technical support team to investigate a customer reported issue. The level of detail in the system log depends on the Logging level settings.
  The **Debug** level of detail is recorded to the TRBOnet Watch database, which quickly increases the database size.
- **RSSI Range**
  Specify the minimum and maximum RSSI values (dBm). Values out of the range will be replaced by these values.
- **Enable extended diagnostics for SLR5000/8000 and MTR3000**
  Select this option so that TRBOnet Watch will show the extended diagnostic information about SLR/MTR repeaters in all monitored systems. This information is displayed in additional fields on the **Health Monitor** tab.
- **Duration column format**
  From the list, select the format used for displaying duration time.

4.7 Systems

Radio systems are now managed through the TRBOnet Watch Console.

From the Channels tab, right-click the Watch Server in the left pane and select Systems. See section 5.4, Radio Systems.

All radio systems will become available after the database has been updated to the latest version.

4.8 SNMP Communication

The TRBOnet Watch Server includes the SNMP Agent module that sends notifications and allows for polling tables with information about system topology, current alarm status, and alarm history. For more information, refer to Appendix B: SNMP Support (section B.2 MIB Objects, page 138).

You can optionally configure the TRBOnet Watch Server to send notifications to a remote NMS using the SNMPv2 or SNMPv3 protocol. The SNMP Agent module supports all security levels for SNMPv3: "no authentication and no privacy", "authentication no privacy", and "authentication and privacy".

To configure a remote NMS for communication with the TRBOnet Watch SNMP Agent, you need to load the MIB files to a remote NMS and configure it. The MIB files are located at the following URL:

https://cdn.trbonet.com/download/tools/NeocomMIBs.zip

Note: To learn more about configuring an NMS, refer to Appendix B: SNMP Support (page 137).

Next, you need to configure the SNMP Agent for sending notifications to the NMS as further described in this topic.

To configure the SNMP Agent for communication with an NMS:

1. In the **TRBOnet Watch Server** window, click **SNMP** in the **Configuration** pane. The **SNMP** pane loads the default SNMP communication settings.
2. Update the following settings where necessary:

Table 5: SNMP configuration settings

Setting	Description
System Parameters section: Includes basic settings that will be visible in an NMS. Except **sysObjectID**, these settings can be modified in NMS.	
sysDescr	Specify a description of the TRBOnet Watch solution. Default: The full name and version of TRBOnet Watch.
sysObjectID	TRBOnet Watch OID. Read-only. Value: 1.3.6.1.4.1.40730.1.1.

Setting	Description
sysContact	Specify the contact information of the person or organization responsible for solving SNMP Agent issues.
sysName	The name of the SNMP Agent.
sysLocation	The descriptive physical location of the SNMP Agent. Default: "Default location".
Engine ID	The identifier of the SNMP Agent. Specify the value that contains 10 to 64 hex characters, or use the default value. Default: 80000AD0431AF108. Note: If SNMPv3 is enabled, the **Engine ID** value must match the appropriate setting in NMS.
SNMP Agent section: Enable the SNMP Agent and configure the NMS connection.	
Enabled	Select to run the SNMP Agent.
SNMPv3 Only	Select to use the SNMPv3 protocol for (encrypted if required) communication between the remote NMS and TRBOnet Watch. The SNMPv3 Agent will ignore all unauthorized requests, including notification requests (if configured to do so). Note: If you select this option, fill out the fields in the **SNMPv3 User** section and the **Engine ID** field.
Notification section: Configure the SNMP Agent to notify the recipient about unauthorized connection attempts.	
SNMP	Select to enable the SNMP Agent to send notifications.
Authentication	Select to enable the SNMP Agent to send notifications in case of unsuccessful authentication on the agent. Note: This option also requires that the **SNMPv3 Only** option is selected.
To	The IPv4 address to which the SNMP Agent sends notifications. The UDP port is 162. Note: Click **Test** to send a test notification to the recipient.
Version	The SNMP protocol version for sending notifications. Values: SNMPv2, SNMPv3. Note: If you select **SNMPv3**, fill out the fields in the **SNMPv3 User** section.
SNMPv3 User section: If SNMPv3 is enabled, specify the SNMP Agent user credentials.	

Setting	Description
User	Specify the user of the SNMP Agent with the required security level (noAuthNoPriv, authNoPriv, or authPriv).
Auth Password	Specify the authentication password if required by the user's security level.
Privacy Password	Specify the privacy password if required by the user's security level.
Auth Protocol	If the authentication password is used, specify the authentication protocol. Values: None, MD5, SHA.
Privacy Protocol	If the privacy password is used, specify the privacy protocol. Values: None, DES, TripleDES, AES128, AES192, AES256.

4.9 Mobile Gateways

To enable connections of Mobile Client applications to TRBOnet Watch Server, you must configure at least one dedicated gateway.

- In the **Configuration** pane, select **Mobile Gateways**.
- In the **Mobile Gateways** pane, select **Enable Mobile Gateways.**
- In the **Configuration** pane, under **Mobile Gateways** select **Mobile Gateway**. Click the **Add** button.
- In the **Mobile Gateway** pane, specify the following parameters:

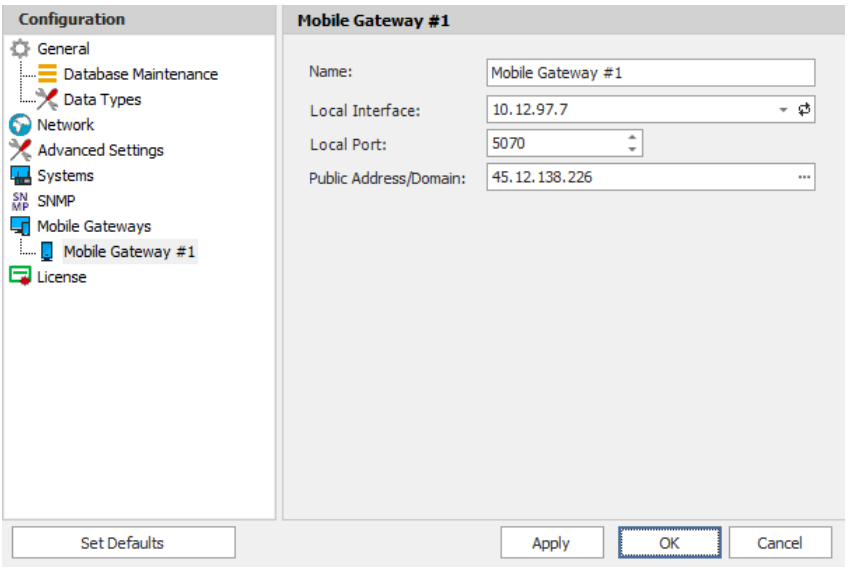


Figure 9: Mobile Gateway pane

- **Name**
  Enter a name for the mobile gateway.
- **Local Interface**
  Enter the IP address of the PC with TRBOnet Watch Server.

- **Local Port**
  Enter the local UDP port number for the Mobile service (5070, by default).
- **Public Address/Domain**
  This is the public IP address of your PC. Enter the Public Address if your TRBOnet Server is behind a router. To detect the public address, click the ellipsis (**...**) button.

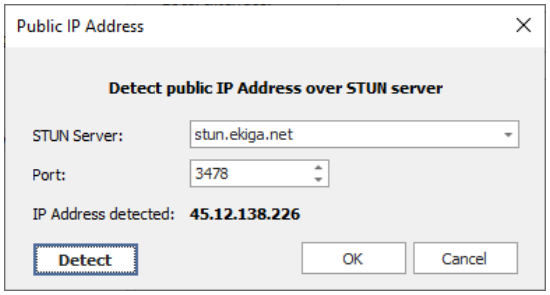


Figure 10: Public IP Address

- **STUN Server**
  From the drop-down list, select the STUN Server.
- **Detect**
  Click this button to detect your public IP address.

4.10 Installing and Starting the Service

TRBOnet Watch runs as a Windows service and this is a mandatory configuration step.

To run the TRBOnet Watch Server as a Windows service:

1. In the **Configuration** pane, select **General**.
2. Click **Install Service** in the **Service** pane.
   As a result, the Windows service will be created.

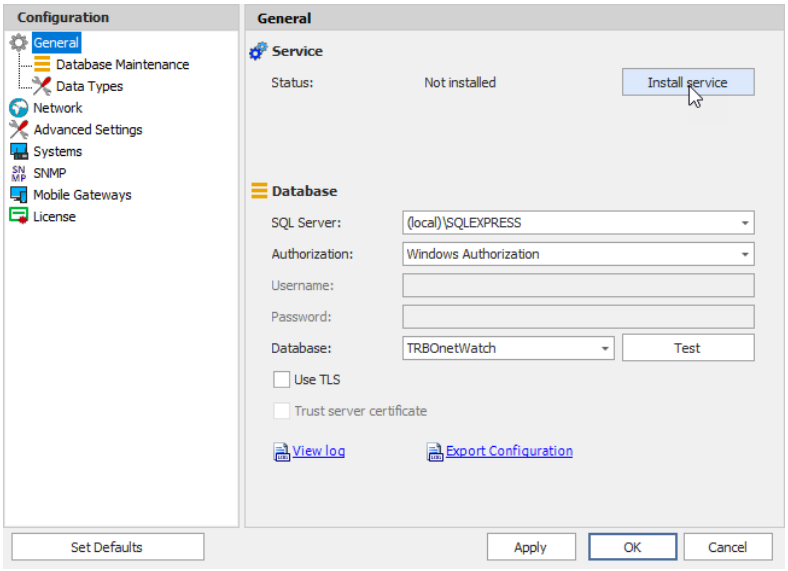


Figure 11: Service not installed

3. Click the **Start service** link.

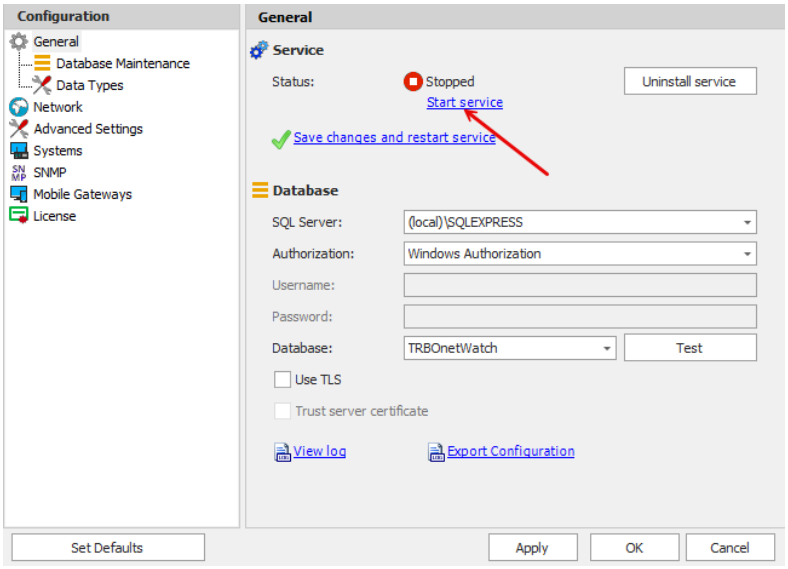


Figure 12: Service not started

Once the Windows service is started, you won't be able to configure server parameters until the service is stopped.

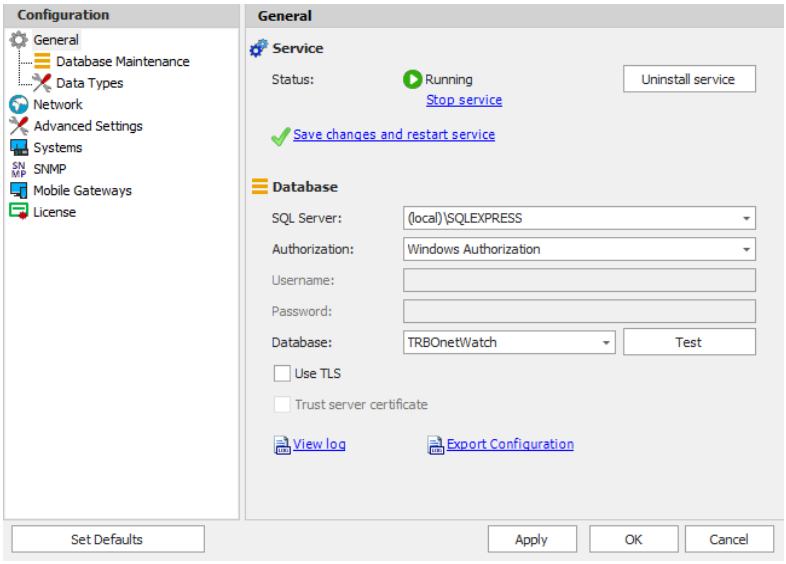


Figure 13: Service started

The following links and buttons and commands are available in the **General** pane:

- **Stop**
  Click to stop the Windows service.
- **Uninstall service**
  Click to remove the service.
- **View log**
  Click this link to open the TRBOnet Watch Server system log in the **View log entries** dialog box. The log may be requested by our technical support team, should the customer report any TRBOnet Watch issue.
- **Export Configuration**
  Click to export the server configuration to a .config file.

5 TRBOnet Watch Console

This section describes how to configure, manage, and use the TRBOnet Watch Console for monitoring different system types, building analytics and reports, and diagnostics.

5.1 Connecting to TRBOnet Watch Server

When you launch the TRBOnet Watch Console for the first time, the dialog box appears.

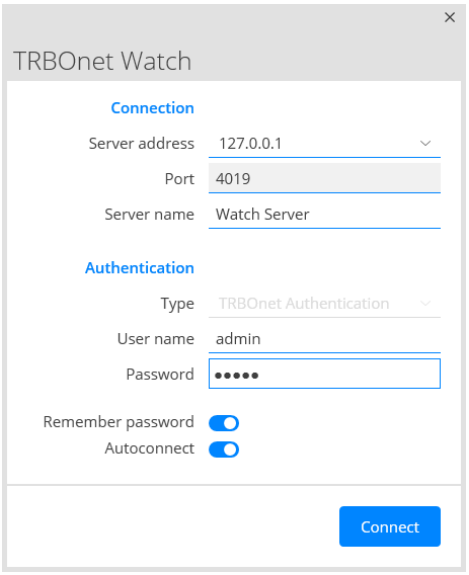


Figure 14: The Connect to Server dialog box

Connection

- **Server address**
  The IP address of the TRBOnet Watch Server you are connecting to. Select this address from the drop-down list or type it in manually.
- **Port**
  Enter the local port of the TRBOnet Watch Server PC to accept connections from the TRBOnet Watch Console.

  Note: This is the **Command Port** parameter of TRBOnet Watch Server configured in section 4.5, Network Parameters (page 19).
- **Server name**
  Enter a name for the server that will be displayed in the TRBOnet Watch Console.

Authentication

- **User name**
  Enter the User Name registered in the TRBOnet Watch Console Users list.

- **Password**
  Enter the User Password.

  Note: The default Administrator credentials are ***admin*** for the user name and ***admin*** for the password.

- **Remember password**
  Select this option to have the Dispatch Console application remember your password.
- **Autoconnect**
  Select this option to launch the Dispatch Console application without having to type the User Name and Password every time. Use this option if you regularly connect to the same TRBOnet Server and your workstation is in a secure location.

- Once you have completed the required fields, click **Connect**.

5.2 Main Window Overview

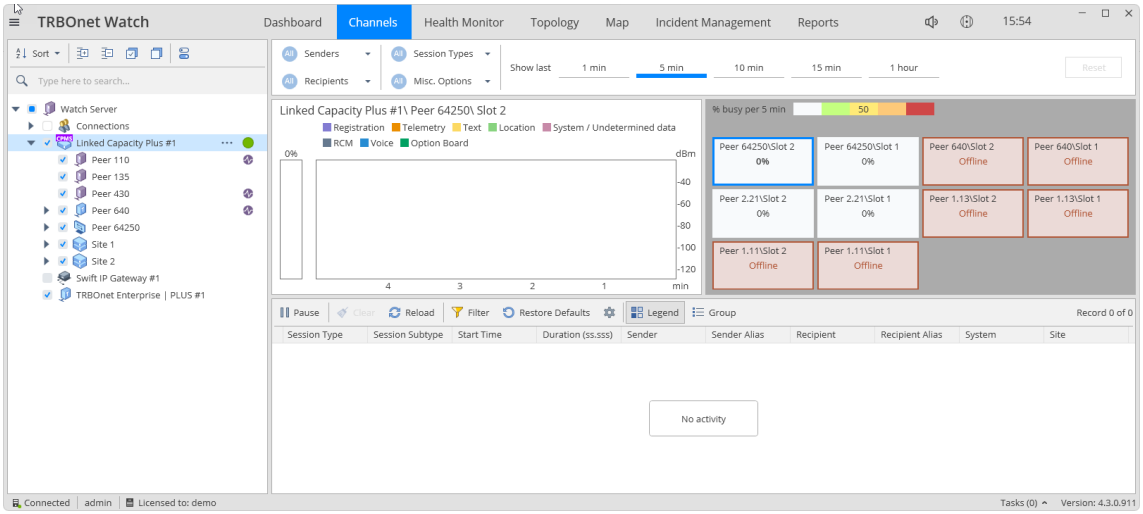


Figure 15: Main window overview

In the upper bar of the main window, you see the following tabs:

- Dashboard
- Channels
- Health Monitor
- Topology
- Map
- Incident Management
- Reports
- Radio Systems
  *Appears if you are in the mode of adding/editing radio systems

5.2.1 Moving/Hiding Tabs

If you right-click on a tab, the context menu will appear, allowing you to do the following:

- **Move tab to new window**
  Select this item to move the tab to a new window.
- **Move tab to main window**
  Select this item to return the tab to the main window.
- **Move tab to another window**
  Select this item to move the tab to an existing window.
- **Move all tabs to main window**
  Select this item to return all tabs to the main window.
- **Hide tab**
  Select this item to hide the tab.
- **Restore hidden tabs**
  Select this item to restore all hidden tabs.

Note: You can perform some of the above actions just by dragging and dropping tabs.

5.3 Console Settings

This section describes how to set up the TRBOnet Watch Console.

- Click the **Menu** button ( ) in the upper-left corner of the main window.
- On the slide-out menu, click **Settings**.
  As a result, the **Settings** window will appear.

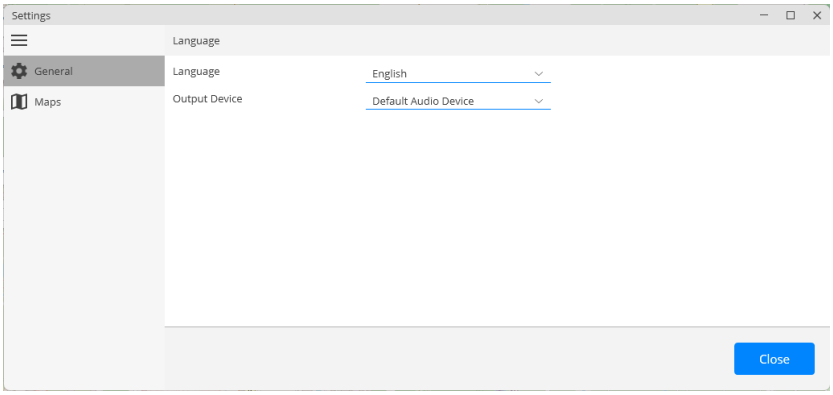


Figure 16: The Console Settings window

5.3.1 Changing the Language

You can configure the TRBOnet Watch Console to display all labels and messages in one of the supported languages.

To select a different language for the console:

- In the **Settings** window, in the **General** tab, from the drop-down list, select the preferred language.

5.3.2 Selecting the Output Device

- In the **Settings** window, in the **General** tab, from the drop-down list, select the output device for playing the sound.

5.3.3 Configuring the Maps

- In the **Settings** window, select the **Maps** tab.
- To add a map, in the **Maps** pane, click the **Add** button.
  Or, click the **Edit** button to edit the selected map.

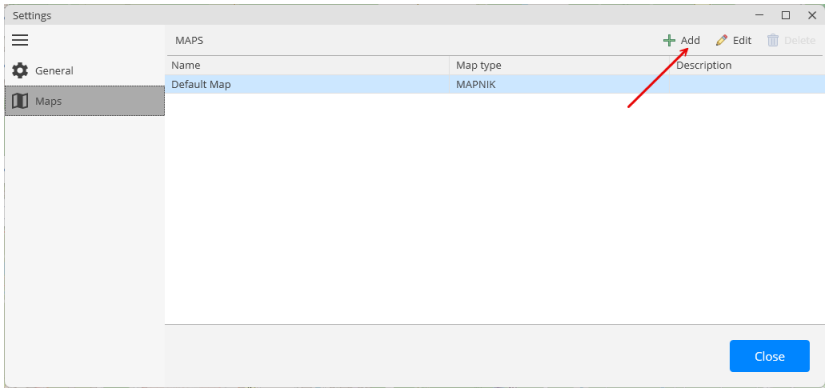


Figure 17: Console settings - Maps

In the **Add map** (or, **Edit map**) window that opens, enter the following information:

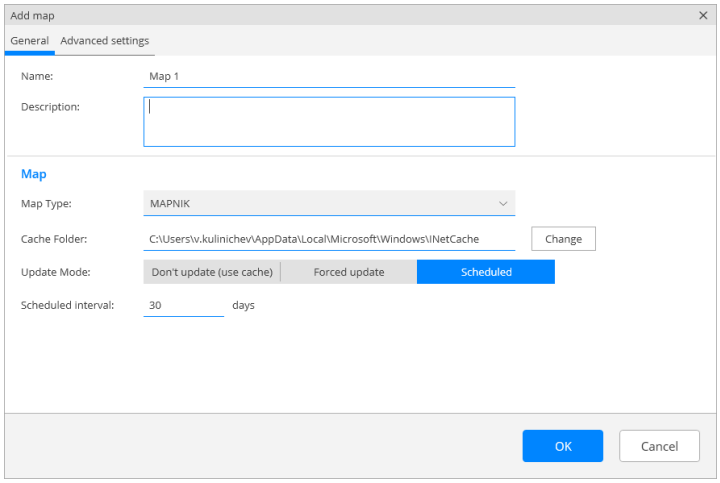


Figure 18: Maps – General tab

- **Name**
  Enter a name for the map.
- **Description**
  Enter a description for the map.
- **Map Type**
  From the drop-down list, select the map type. For available map types, refer to section 5.3.2.1, Supported Map Types.
- **Map API Key**
  Enter the API key for the selected map type.

  Note: To obtain the API key, click the **API Key info** link on the right and follow the instructions.
- **Cache folder**
  Click the ellipsis (**...**) button and locate the folder on the PC where you want to store map data.

- **Update Mode**
  Select the mode for updating the map tiles stored in the specified Cache folder ('Don't update', 'Forced update', or 'Scheduled').

- Click the **Advanced settings** tab.

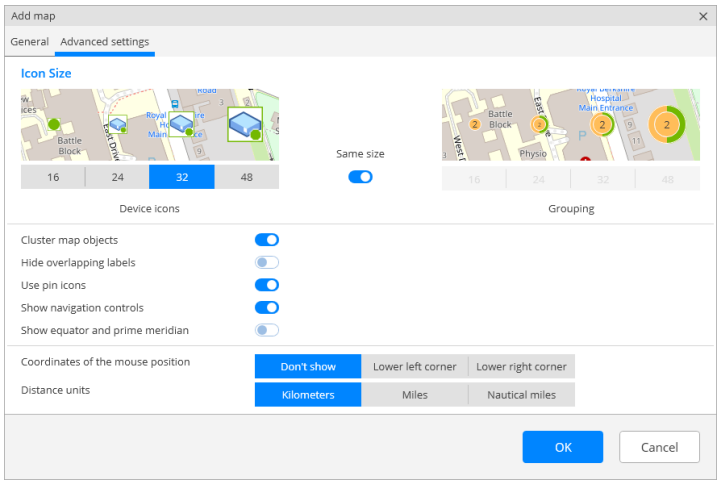


Figure 19: Maps – Advanced Settings tab

- In this tab, you can select what to show on the map by turning on the appropriate toggle switches.

5.3.3.1 Supported Map Types

- **MAPNIK** – free online map. For more details on OpenStreetMaps, visit the official the website: https://www.openstreetmap.org/
- **Thunderforest** – commercial online maps. Visit https://www.thunderforest.com/docs/apikeys/ to get a key.
- **Microsoft BING** – commercial maps from Microsoft. Includes BING_ROAD, BING_AREA, and BING_HYBRID subtypes. A user may use BING maps for 90 days and then they must get a Basic Key. Visit https://msdn.microsoft.com/en-us/library/ff428642.aspx to get a Basic Key.
- **Google Maps** – online mapping service from Google. Visit https://developers.google.com/maps/documentation/javascript/get-api-key#key to get a key.
- **Custom Maps** – online mapping services such as TRBOnet Map Server, WMS and WMTS services. For more details, refer to *TRBOnet Map Server User Guide*. For more details on the WMS/WMTS services, visit https://www.opengeospatial.org/standards/wms/introduction.

5.3.4 Viewing the License Information

To see the current license permissions in the TRBOnet Watch Console

- Click the **Menu** button ( ) in the upper-left corner of the main window.
- On the slide-out menu, click **License**.
  As a result, the **Help** window opens with the **License** tab selected.

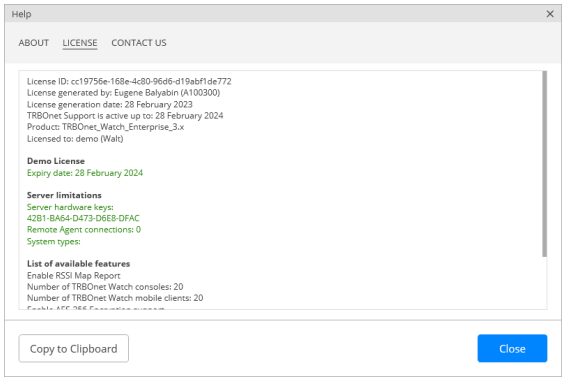


Figure 20: License

5.3.5 Color Themes

To switch between the dark/light themes, and then back to the gray theme:

- Click the **Change theme** icon ( ) on the right side of the title bar.
  When clicked, the icon will be successively changed to , , and back to .

5.4 Radio Systems

Radio systems are now configured in TRBOnet Watch Console.

- In the left pane, click the ellipsis button on the right of the Watch Server item, and from the context menu select **Radio Systems**.
  Or, click the icon on the left pane's toolbar.

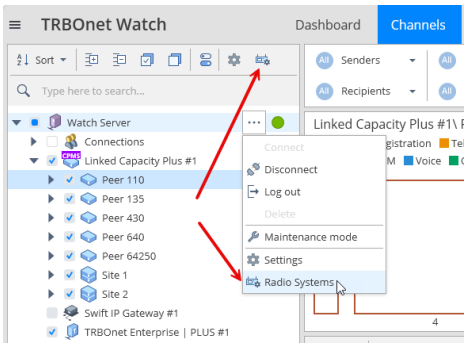


Figure 21: Watch Server – Radio Systems

5.4.1 MOTOTRBO IPSC, CP, LCP, and ERDM

In the right pane (under the **Radio Systems** tab), click one of the following links:

- Add IP Site Connect
- Add Extended Range Direct Mode
- Add Capacity Plus
- Add Linked Capacity Plus

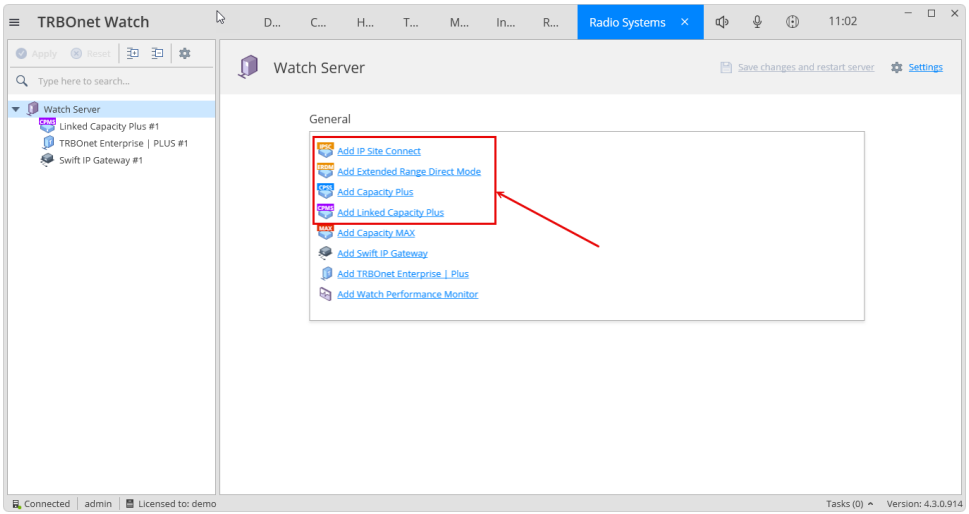


Figure 22: Adding MOTOTRBO systems

5.4.1.1 General Settings

In the **General** section, specify the following parameters:

Table 6: MOTOTRBO General settings

Property	Description
System Name	The name of the system that uses the master repeater. The system name will be displayed in the TRBOnet Watch Console. Valid characters: spaces, alphanumeric and special characters.
TRBOnet Peer ID	The peer ID of the TRBOnet Watch Server in the system. Range: 1 to 16777215. Range for LCP and Capacity Plus: 1-65535. Default: 200. This value must be unique among the repeaters and software agents in the radio system.
TRBOnet Local Port	The IP port of the TRBOnet Watch Server used for connection with a radio network. Use a unique port for each master repeater in the system.
SNMP ID	Any value within the valid range used to generate the repeater's physical index. Valid range: 1 to 127. Move the mouse cursor over the **SNMP ID** label to see the generated physical index stored in the physical entity table (object entPhysicalTable) of the SNMP Agent. To learn more about SNMP communication with TRBOnet Watch, refer to Appendix B: SNMP Support (page 137).

Property	Description
Master Peer subsection	
Master IP Address	The static IP address of the master repeater. Default: 192.168.0.100.
Master UDP Port	The UDP port of the master repeater. Range: 1024 to 65535. Default: 50000.
Authentication Key	The private key value of the master repeater as specified in the repeater's configuration. Valid characters: 0-9 and A-F. Max length: 40 characters. Leave this field blank if the repeater authentication is disabled.
System Type	Displays the topology of a MOTOTRBO system.
Connection	Select the level of monitoring in the system. Choosing a low level helps reduce traffic and the database volume. Options: ▪ **Level 1: Link Establishment**: Select to monitor the IP connections in the system. ▪ **Level 2: Diagnostics**: Select to monitor the IP and RDAC connections in the system. ▪ **Level 3: Call Monitoring**: Select to monitor the IP and RDAC connections in the system and non-parsed traffic in the channels. ▪ **Level 4: Call Parsing**: Select to leverage the full-featured monitoring in the system. For details, refer to section 2.7, System Monitoring Levels (page 8).

- Click **Test** to check the IP connection to the master repeater. The result appears in a popup window. If successful, the firmware version and serial number are displayed. Click **Close** to close the popup window.

Adding Peers

Indicate all system peers that you may need to include in reports and charts. Peers added on this tab can be selected as filter settings in the Reports tab. For details, refer to section 5.12, Reports (page 99).

To add system peers:

- Click the **Load Peers from Repeater** link in the right pane to automatically find all system peers, including all connected software peers.
- Click the **Add Peer** link to add a new peer to the list.
  Edit the **Peer ID** and **Alias**, if necessary.

5.4.1.2 Privacy Settings

In the **Privacy** section, specify the following parameters:

Table 7: Privacy settings of the MOTOTRBO repeater

Property	Description
Privacy Type	The type of privacy as specified in the repeater configuration. Options: ▪ **None**: Privacy is disabled. ▪ **Basic**: Basic Privacy (utilizes a Motorola proprietary non-cryptographic algorithm to encrypt and protect voice and data). ▪ **Enhanced**: Enhanced Privacy (utilizes a cryptographic algorithm to encrypt and protect voice and data).
Basic Privacy Key ID	Applies to Basic Privacy only. The privacy key specified in the repeater configuration. Valid range: 1 to 255.
Enhanced Algorithm	Applies to Enhanced Privacy only. The encryption algorithm specified in the repeater configuration. Options: ARC4, DES, AES 128, AES 256.
Enhanced Privacy Keys	The Enhanced Privacy keys specified in the repeater configuration. Applies to Enhanced Privacy only. Click the **+ New key** button and add up to 16 Enhanced Privacy keys. Each key appears in the table with the following properties: ▪ **ID**: A unique index key within the range of 1 to 255. ▪ **Key Name**: A unique 16-character alias of the encryption key ID. ▪ **Key Value**: The encryption value that maps the key ID. Range: 1 to FFFFFFFFFE.

5.4.1.3 Data Storage

By default, the TRBOnet Watch Console stores traffic from all monitored radio channels in the database.

In order to save storage space, you can set up filtering rules. Using the filter, select the type of data that will be added to the database. The filtering rules allow you to define:

- Groups and radios whose activity needs to be monitored.
- Groups and radios whose activity should be added to the database.
- Whether the All Calls log should be displayed in the console.
- Whether repeater control messages should be stored in the database.

To configure monitoring and data storage in a system:

In the **Data Storage** section, specify the following parameters:

- Select the required tab and adjust the settings as follows:

Table 8: Call filtering and data storage settings of the MOTOTRBO repeater

Tab name	Instructions
Group Call/ Private Call	On each tab, do any of the following: ▪ Select **Enable Group call filter** to enable filtering. Then add filtering rules for the selected type of calls as described in section Creating Rules (page 38).
All Call	Configure monitoring and data storage of All Call calls. ▪ **Show All Call in console**: Select to display All Calls in the console. ▪ **Store Voice All Call**: Select to store All Call voice data.
Advanced	Configure storage of repeater call monitoring (RCM) messages. ▪ **Allow Sync Undetect messages** ▪ **Store RCM messages**: Select to store the RCM messages in the database. Enable this option to show RCM data for the given system in the Channels tab and in charts and reports. ▪ **All channels busy threshold** Enter the time interval, in seconds, that will be used as a threshold for channel busy level.

Creating Rules

To add filtering rules for group calls or private calls:

- in the **Data Storage** section, click the **Group call** or **Private call** tab, respectively.

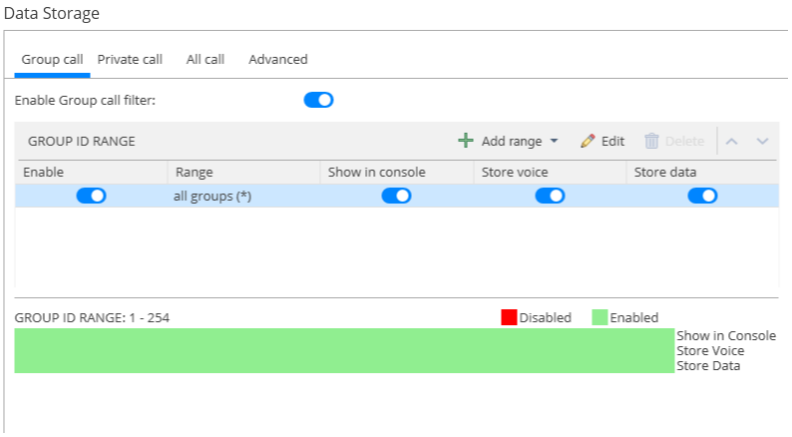


Figure 23: Filtering rules for group calls

Filtering is enabled if the **Enable Group call filtering** option is selected. By default, the selected tab shows the default rule. The title of this rule indicates the range of group IDs (*all groups*) or radio IDs (*all radios*) covered by this rule.

If necessary, create custom rules for smaller ranges or for individual IDs and set options for each ID or range.

To create a new rule:

1. Click **Add Range**. On the **Group Call** tab, click **Specified Group** or **Group Range** to filter calls made in a particular talk group or a in group range, respectively. On the **Private Call** tab, click **Specified Radio** or **Radio Range** to filter calls initiated by a particular radio or a radio range.
2. In the popup dialog box, specify the group ID or the radio ID, or the first and last ID in the range. Click **OK**.

   Table 9: Number ranges allowed in MOTOTRBO system types

System	Group range	Radio range
IP Site Connect, Extended Range Direct Mode	1-16,776,415	1-16,777,215
Capacity Plus, LCP	1-254	1-65,535

3. Enable or disable options in the rule. These options apply to a call if the calling number matches the number or range specified in the rule:
   - **Show in Console**: If enabled (selected), the call is displayed in the console.
   - **Store Data**: If enabled, the data call is stored in the database.

   The storage options are available only when the **Show in Console** option is enabled.
4. Set the priority of the rule by using the arrow keys. The top entry in the list has the higher priority.

   At runtime, when a group call or a private call is initiated in the system, the filtering rules for this call type are checked one after another in the order they follow on the respective tab. If the calling ID matches a rule, this rule is applied and the rules with lower priority are not checked. If the calling ID does not match a rule in the list, the default rule will be applied. The default rule always takes the last position in the list and cannot be moved.

Note: If some rules have overlapping ranges, set their priority as described in section Ordering Rules with Overlapping Ranges (page 40).

To edit the rules, do the following:

- Click **Edit** to modify the rule.
- Click **Delete** to delete the rule.
- Clear the checkbox to disable the rule. Disabled rules are ignored at runtime.

The default rule (*all groups* or *all radios*) cannot be removed or disabled.

Ordering Rules with Overlapping Ranges

The order of rules on the tab is important if the rule ranges overlap. For instance, you need to monitor group calls in the IP Site Connect system as follows:

- In the range of 5,000,000 to 10,000,000 you need to store data
- In the range of 8,000,000 to 11,000,000 you need to store voice
- For the remaining numbers, you do not monitor calls

You need to create the following rules:

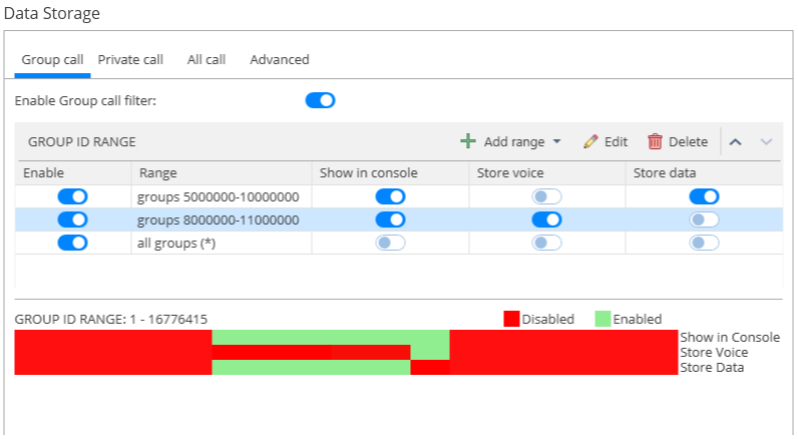


Figure 24: Ordering rules with overlapping ranges

In this example, ranges 5,000,000 - 10,000,000 and 8,000,000 - 11,000,000 overlap. Calls in the range of 8,000,000 - 10,000,000 will be handled as specified in the rule that works first. If you stay with the above rule order, data will be stored in this range. If you move the rule "groups 8000000-11000000" to the top position, voice will be stored.

The color band below the rules visualizes the expected effect of the rule options. Options appear in the color band as three horizontal-colored stripes: **Show in Console**, **Store Voice**, and **Store Data**. The length of each stripe stretches from group 1 (left) to the maximum possible ID in the system. In case of private calls, the horizontal axis shows radio IDs from 1 (left) to the maximum possible ID. Rules break the horizontal axis into ranges. Within each range, the color stripes are green or red, depending on the status of the respective rule option – enabled or disabled. If you move the mouse cursor over the colored stripe, the tip shows the range of IDs where the option applies.

5.4.2 MOTOTRBO Capacity Max

To monitor a Capacity Max system, you need to add the system, all RF sites, and Trunk Controllers in TRBOnet Watch. Registering other system components, such as Data Gateways and VRC Gateways, is optional.

Note that once you have added/changed Capacity Max components in TRBOnet Watch, you must specify the IP address/UDP Port of the TRBOnet Watch Server in **Call Monitor Application 1 IP/UDP Port** settings and rewrite the

configuration (Trunking Controller, VRC Gateway, RF Site and Peers) in Motorola's RM Software.

5.4.2.1 TRBOnet Watch

To add a Capacity Max:

- In the right pane, click **Add Capacity Max**.

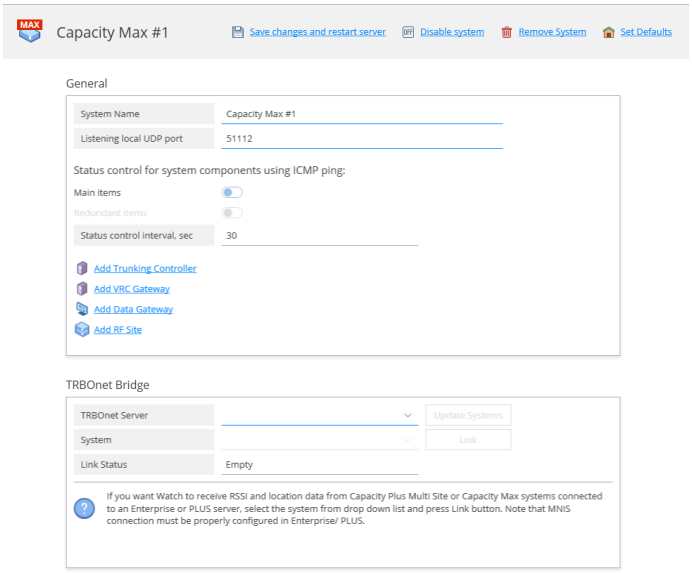


Figure 25: Adding Capacity Max

- In the **General** section, specify the following parameters:

Table 10: Capacity Max IP connection settings

Property	Description
System Name	The name of the Capacity Max system to be displayed in the TRBOnet Watch Console. Valid characters: spaces, alphanumeric and special characters.
Listening local UDP port	The UDP port of the TRBOnet Watch Server host for listening to the Capacity Max system. This setting must match the **Call Monitor Application 1 UDP Port** setting in the Radio Management tool.
Status control for system components using ICMP ping	
Main items	If this option is selected, the system components will be periodically pinged to check their status.
Redundant items	If this option is selected (available only if the above option is selected), the redundancy system components will also be pinged to check their status.
Status control interval	Specify the ping interval, in seconds

- Add Trunking Controller, Data Gateway, and VRC Gateway components.

- Add all RF sites as described in section RF Site (page 46).

Trunking Controller

Perform the following steps to add a Trunking Controller:

- In the right pane, click the **Add Trunking Controller** link.

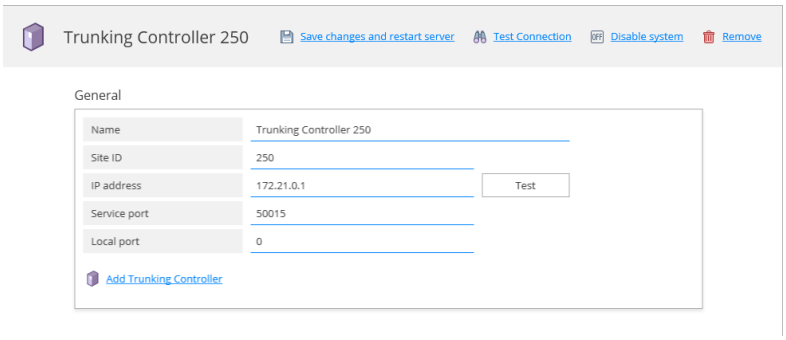


Figure 26: Adding Trunking Controller

- In the **General** section, specify the following properties:

Table 11: Trunking Controller connection settings

Property	Description
Name	The name of the Trunking Controller to be displayed in the TRBOnet Watch Console.
Site ID	Enter the ID of a non-existing site (for example, 250 if it has not yet been assigned to another site).
IP address	The IP address of the Trunking Controller as specified in the Capacity Max system configuration (Figure 35).
Service port	Specify the service port number (50015, by default).
Local port	Specify the local port number (0 means any free port).

Data Gateway

Perform the following steps to add a Data Gateway:

- In the right pane, click the **Add Data Gateway** link.

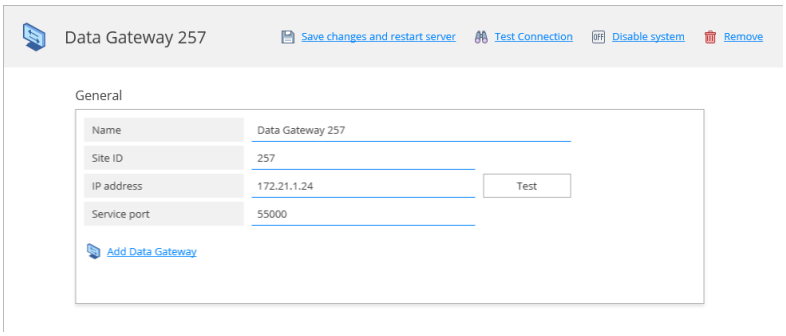


Figure 27: Adding Data Gateway

- In the **General** section, specify the following properties:

Table 12: Data Gateway connection properties

Property	Description
Name	A user-friendly name of the Data Gateway to be displayed in the TRBOnet Watch Console. Valid characters: spaces, alphanumeric and special characters.
Site ID	The site ID on which the Data Gateway is deployed. Enter the site ID specified in the Capacity Max system configuration. Note: Open the Capacity Max configuration on any system repeater as described in section RF Site (page 46).
IP address	The IP address of the host on which the MNIS Data Gateway is installed.
Service port	Specify the service port number (55000, by default).

VRC Gateway

Perform the following steps to add a VRC Gateway:

- In the right pane, click the **Add VRC Gateway** link.

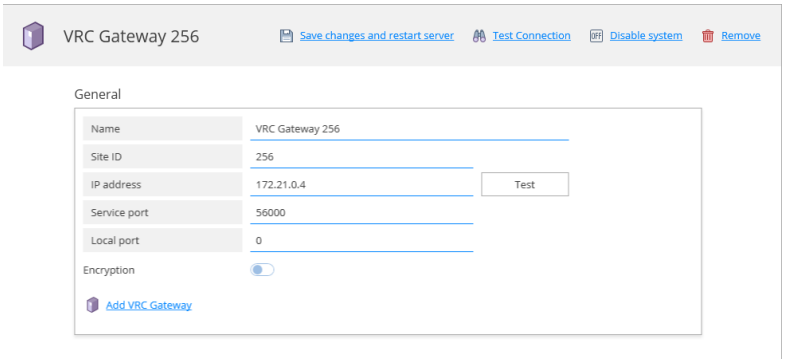


Figure 28: Adding VRC Gateway

- In the **General** section, specify the following properties:

Table 13: VRC Gateway connection properties

Property	Description
Name	A user-friendly name of the VRC Gateway to be displayed in the TRBOnet Watch Console. Valid characters: spaces, alphanumeric and special characters.
Site ID	The site ID on which the VRC Gateway is deployed. Enter the site ID specified in the Capacity Max system configuration. Note: Open the Capacity Max configuration on any system repeater as described in section RF Site (page 46).
IP	The IP address of the VRC Controller as specified in the Capacity Max system configuration (Figure 36).
Service port	Specify the service port number (56000, by default).
Local port	Specify the local port number (0 means any free port).

Property	Description
Encryption	Select this option to enable encryption on the VRC Gateway.

RF Site

Perform the following steps to add an RF Site and peers:

- In the right pane, click the **Add RF Site** link.

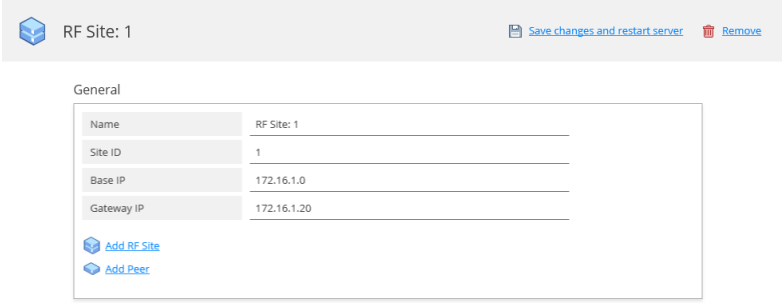


Figure 29: Adding RF Site

- In the **General** section, specify the following RF Site connection properties:

Table 14: RF site connection settings

Property	Description
Name	A user-friendly name of the RF site to be displayed in the TRBOnet Watch Console. Valid characters: spaces, alphanumeric and special characters.
Site ID	The site ID. This setting must match the **Site ID** value in the Radio Management tool (Figure 34).
Base IP	The base IP address of the RF site. This setting must match the **Base IP** value in the Radio Management tool (Figure 34).
Gateway IP	The IP address for the site router. This setting must match the **Gateway IP** value in the Radio Management tool (Figure 34).

- Click the **Add Peer** link.

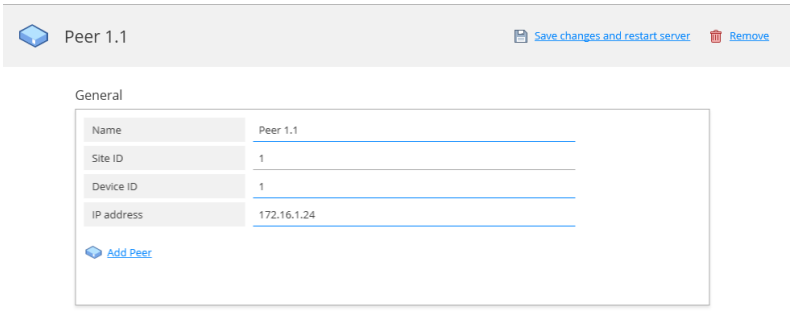


Figure 30: Adding Peers to RF Site

- In the **General** section, add information for the repeater belonging to the RF site. To edit the properties of the peer, click the respective field and type the required value.

5.4.2.2 Motorola's RM Software

To register a Capacity Max system, you need to open the system configuration in Motorola's Radio Management (RM) software.

To open the Capacity Max configuration:

1. Launch the Radio Management software. Click **Radios**.

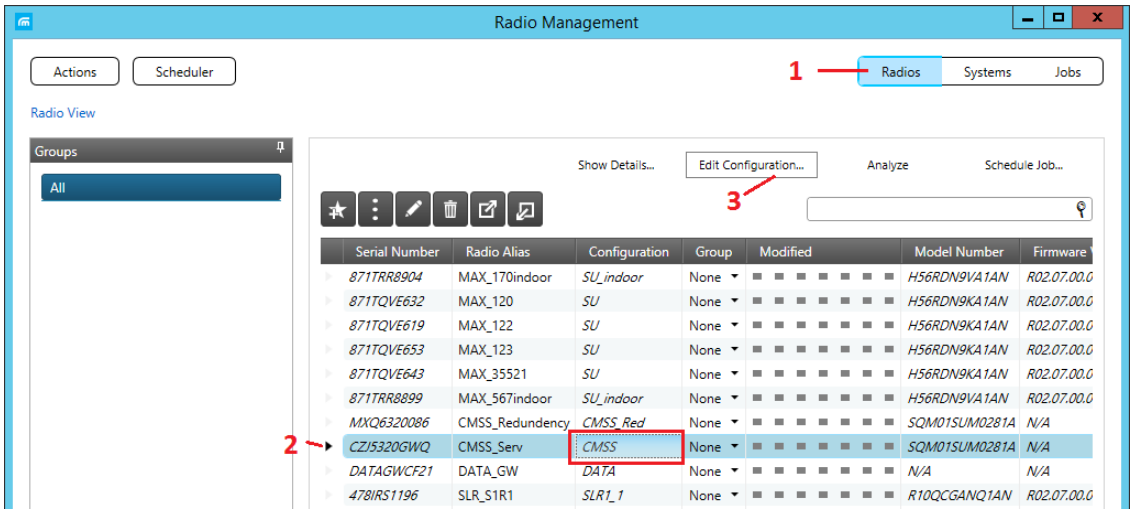


Figure 31: Opening the Capacity Max system configuration

2. In the list, click the arrow in front of the entry with the CMSS configuration.
3. Click the **Edit Configuration** button.

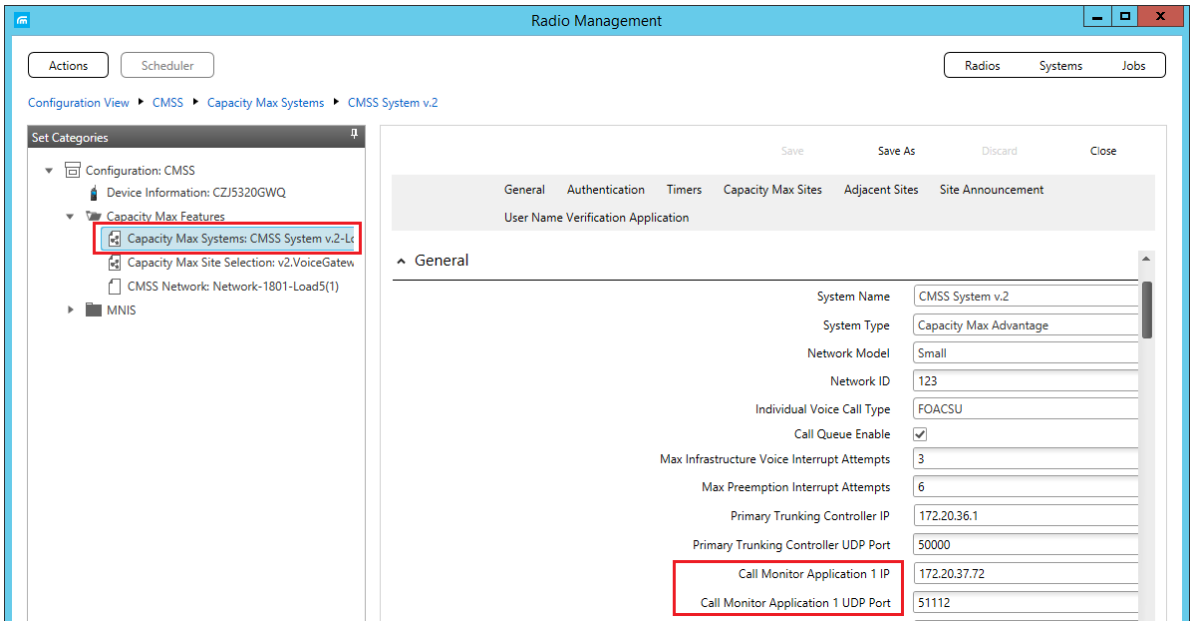


Figure 32: Opening the general settings of the Capacity Max system

4. In the left pane, expand **Capacity Max Features** and click **Capacity Max Systems**.

For your TRBOnet Watch to receive traffic from the Capacity Max system, the **Call Monitor Application 1 IP** setting must specify the IP address of the TRBOnet Watch Server.

RF Site

To register all RF sites from your Capacity Max system, use Radio Management to open the system configuration for all the any repeaters registered in that system to view the information about those repeaters.

To open the Capacity Max configuration for a repeater:

1. Launch the Radio Management software. Click **Radios** (Figure 33, step 1).
2. In the right panel, click the arrow in front of an entry with the repeater configuration (Figure 33, step 2). Make sure that the entire line is selected.
3. Click the **Edit Configuration** button (Figure 33, step 3).

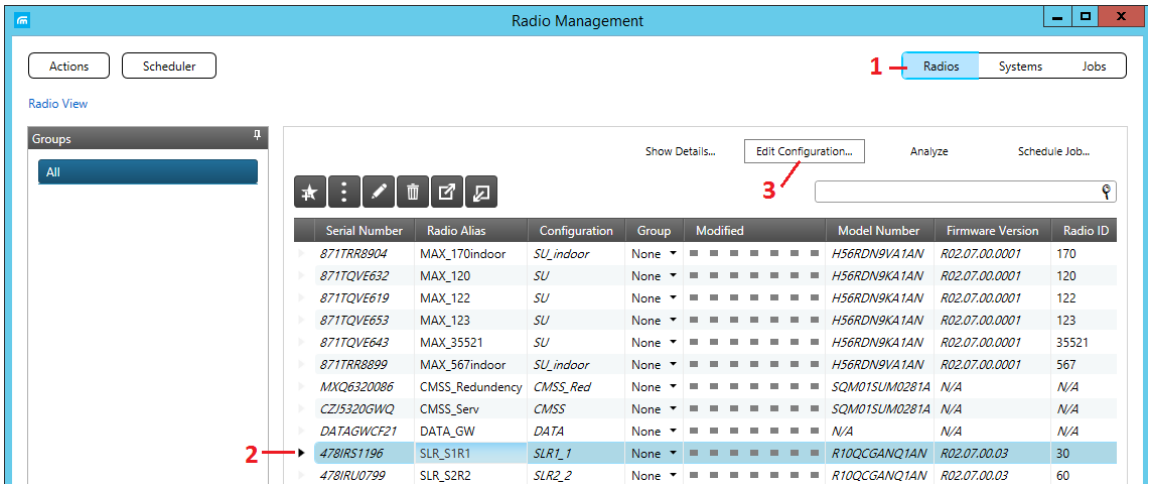


Figure 33: Opening the Capacity Max configuration for a repeater

4. In the left pane, expand **Capacity Max Features** and click **Capacity Max Systems** (Figure 34, step 1).
5. In the right pane, click **Capacity Max Sites** (Figure 34, step 2).

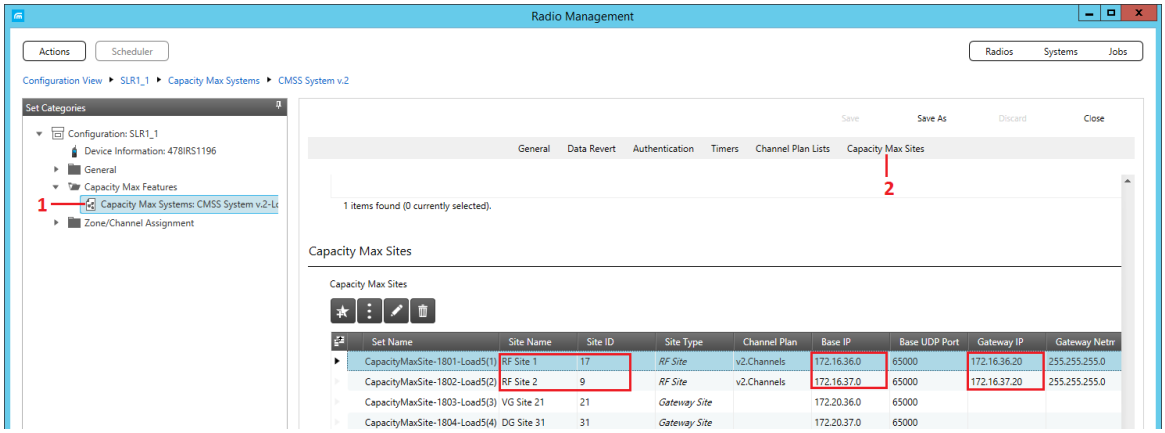


Figure 34: Opening the system sites

Register the repeater information in TRBOnet Watch for all RF sites that are displayed in the **Capacity Max Sites** list.

Trunking Controller

Perform the following steps to register a Trunking Controller:

1. Open the Capacity Max system configuration as described in section 5.4.2.2, Motorola's RM Software (page 45).

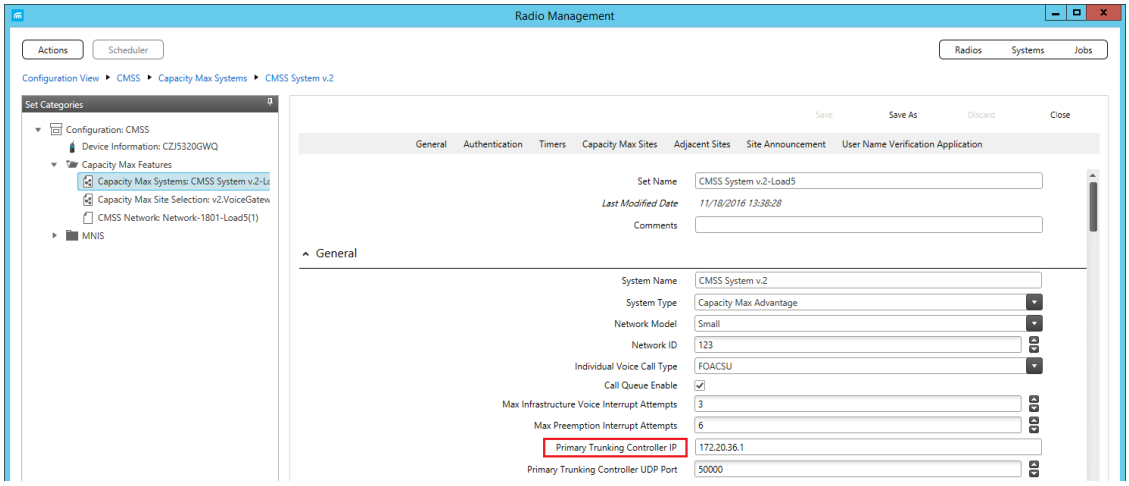


Figure 35: The IP address of the Trunking Controller

VRC Gateway

Perform the following steps to register a VRC Gateway:

1. Open the Capacity Max system configuration as described in section 5.4.2.2, Motorola's RM Software (page 45).
2. In the left panel, click **CMSS Network** under **Capacity Max Features** (Figure 36).

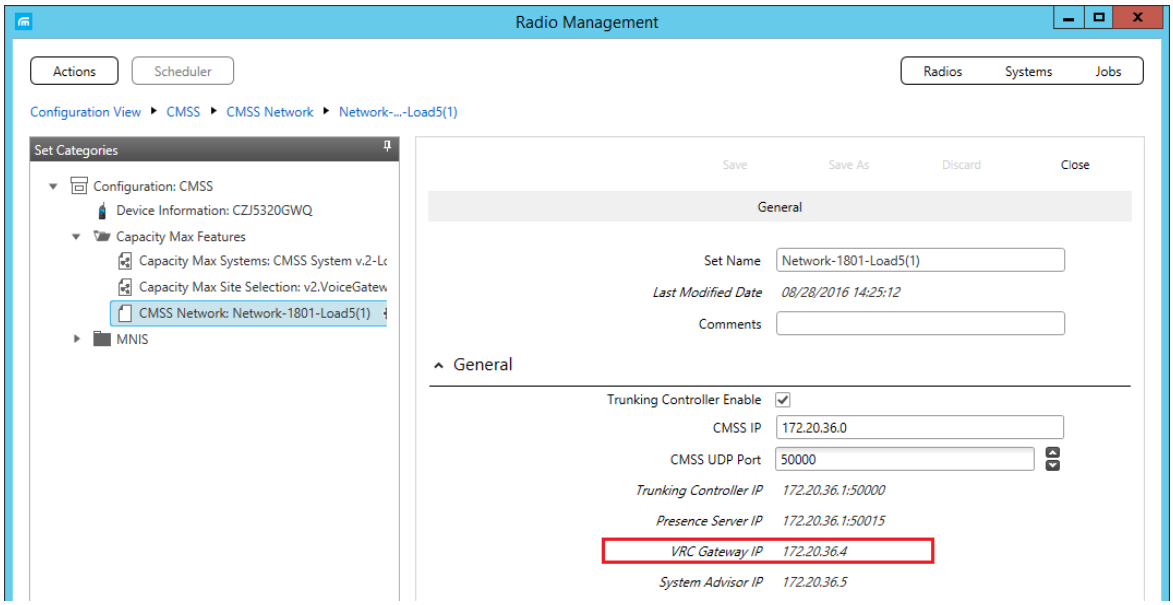


Figure 36: The IP address of the VRC Controller

5.4.3 Swift IP Gateway

TRBOnet Watch can monitor the traffic of a hardware RoIP gateway that connects a MOTOTRBO two-way radio to the system's IP network. To monitor a RoIP gateway, register the respective hardware unit - Swift IP Gateway A100/A200.

Perform the following steps to register a Swift IP Gateway:

- In the right pane, click **Add Swift IP Gateway**.
- In the **General** section, specify the following properties:

Table 15: Swift IP Gateway settings

Property	Description
System Name	The name of the RoIP gateway. Valid characters: spaces, alphanumeric and special characters.
IP Address	The IP address of the TRBOnet Swift Agent. The expanded list shows all TRBOnet Swift Agent units available on the network. Default: 192.168.0.100.
Port	The IP port of the TRBOnet Swift Agent. Default: 8002.
Local Port	The local port number that will be used by TRBOnet Watch to establish a connection to the Swift Agent. The value 0 (default) means that a random port will be used.
Ignore voice data	Select to ignore voice traffic from the TRBOnet Swift Agent. If this option is enabled, the TRBOnet Watch Console does not receive voice calls from this RoIP gateway.
VoIP port	The local port of the TRBOnet Swift Agent for voice-over-IP communication. Default: 4000.
Audio Format	From the drop-down list, select the format to transmit audio data.

- Click **Test** to see information about the connected Swift IP Gateway (radio ID, Serial Number, Firmware version, etc.)

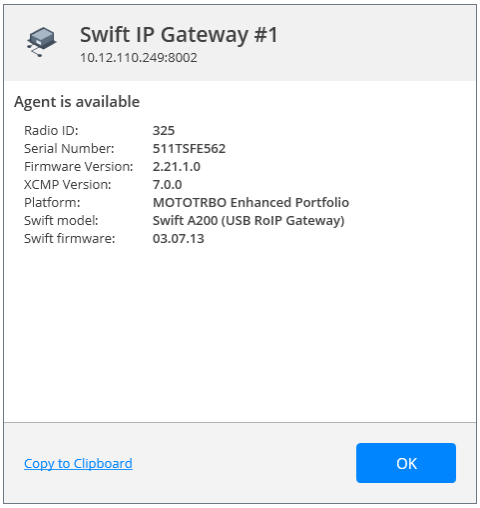


Figure 37: Testing Swift IP Gateway

5.4.4 TRBOnet Enterprise | PLUS

If your Linked Capacity Plus or Capacity MAX radio systems are using the NAI protocol to transfer data (Location, ARS, TMS), then in order to build reports and RSSI analytics, you'll have to connect to the appropriate TRBOnet Enterprise | PLUS.

You can also monitor the performance of the PC hosting the TRBOnet Enterprise | PLUS. Hardware performance includes CPU usage, Memory usage and Disk space usage. In addition, you will find information about the installed operating system, and the version of TRBOnet Enterprise | PLUS.

Note: Before connecting to TRBOnet Enterprise | PLUS, make sure that the required radio systems are properly registered in. Also note that the TRBOnet Enterprise | PLUS must be of version 6.2 or later.

- In the right pane, click **Add TRBOnet Enterprise | PLUS**.
- In the **General** section, specify the following properties:

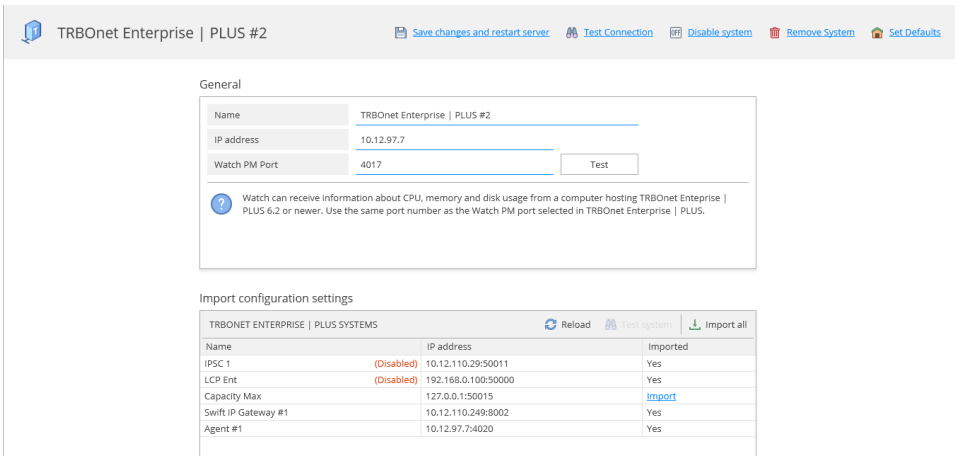


Figure 38: Adding TRBOnet Plus/Enterprise

- In the 'TRBOnet Enterprise | PLUS' pane, specify the following parameters:
  - **Name**
    Enter a name for the TRBOnet Enterprise | PLUS you are connecting to.
  - **IP address**
    Enter the IP address of the PC hosting the TRBOnet Enterprise | PLUS Server or TRBOnet Enterprise | PLUS Agent.
  - **Watch PM port**
    Enter the port number to be used by TRBOnet Watch to connect to the PC hosting the TRBOnet Enterprise | PLUS. Use the same port number as the **Watch PM port** selected in TRBOnet Enterprise | PLUS.

    Note: If you are adding both TRBOnet Enterprise | PLUS Server and TRBOnet Enterprise | PLUS Agent, make sure they have different Watch PM port numbers.

  - **Test**
    Click this button to see information about the connected TRBOnet Enterprise | PLUS and available Location services.

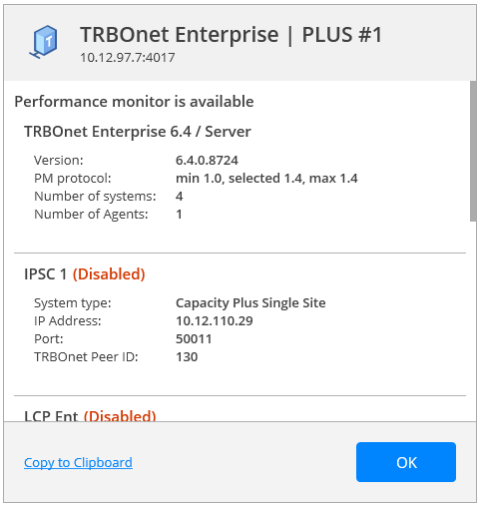


Figure 39: Testing TRBOnet Enterprise

5.4.4.1 Importing Settings

- In the **Import configuration settings** section, click **Import all**.
  As a result, you will see the imported systems in the table below.

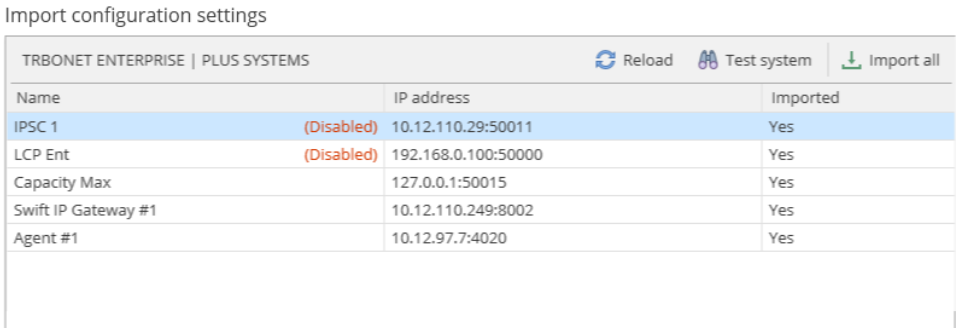


Figure 40: Imported TRBOnet Enterprise settings

5.4.4.2 TRBOnet Bridge

If you want TRBOnet Watch to receive RSSI and location data from Linked Capacity Plus or Capacity Max systems connected to an Enterprise or PLUS server, you should link these systems together. Note that MNIS connection must be properly configured in Enterprise | PLUS.

This section describes how to configure a bridge between the Watch systems and the corresponding Enterprise | PLUS systems.

Go to the Linked Capacity Plus or Capacity Max system you have imported from TRBOnet Enterprise | PLUS.

- In the **TRBOnet Bridge** section, specify the following parameters:

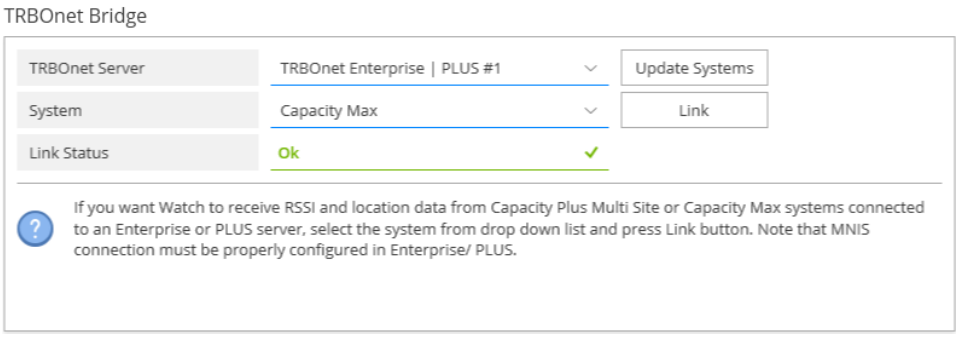


Figure 41: TRBOnet Bridge

- **TRBOnet Server**
  Select the connected Enterprise | PLUS server.
- **System**
  Select the name of the radio system in TRBOnet Watch.
- **Lins Status**
  Indicates the link status of the radio system.

5.4.5 Watch Performance Monitor

The Watch Performance Monitor is used to monitor the performance of the remote PC hosting the TRBOnet Watch Server or TRBOnet Enterprise | PLUS Server.

Hardware performance includes CPU usage, Memory usage and Disk space usage. In addition, you will see information about the installed operating system, and the version of TRBOnet Watch Server or TRBOnet Enterprise | PLUS. If the remote PC is hosting the TRBOnet Watch Server, you will also see information about the MS SQL database (database name, size, version).

Note: To view performance monitor information, hover over the corresponding item in the left pane of the TRBOnet Watch Console.

- In the right pane, click **Add Watch Performance Monitor**.

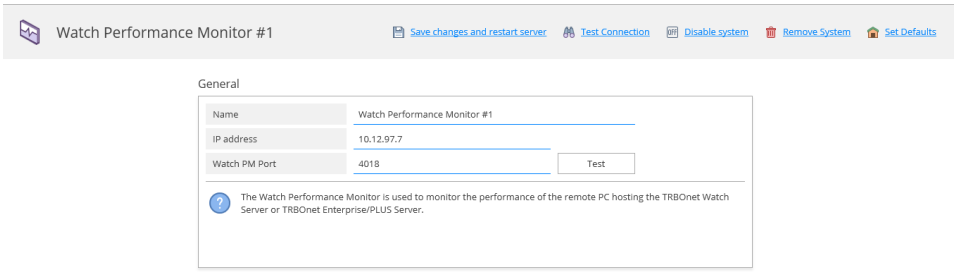


Figure 42: Adding TRBOnet Watch Performance Monitor

- In the **General** section, specify the following parameters:
  - **Name**
    Enter a name for the TRBOnet Watch (or, TRBOnet Enterprise | PLUS) you are connecting to.
  - **IP address**
    Enter the IP address of the PC hosting the TRBOnet Watch Server (or, TRBOnet Enterprise | PLUS).
  - **Watch PM port**
    Enter the port number to be used to connect to the PC hosting the TRBOnet Watch Server (or, TRBOnet Enterprise | PLUS).
  - **Test**
    Click this button to see information about the connected TRBOnet Watch Server (or, TRBOnet Enterprise | PLUS).

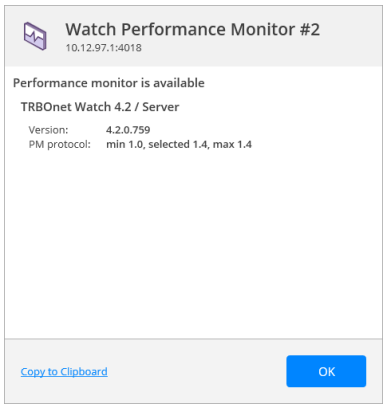


Figure 43: Testing TRBOnet Watch Performance Monitor

5.4.6 Applying Changes

Once you have added required systems to TRBOnet Watch, you see them in green with a plus sign on the right.

To apply changes and restart the server, click the **Apply** button on top of the left pane.

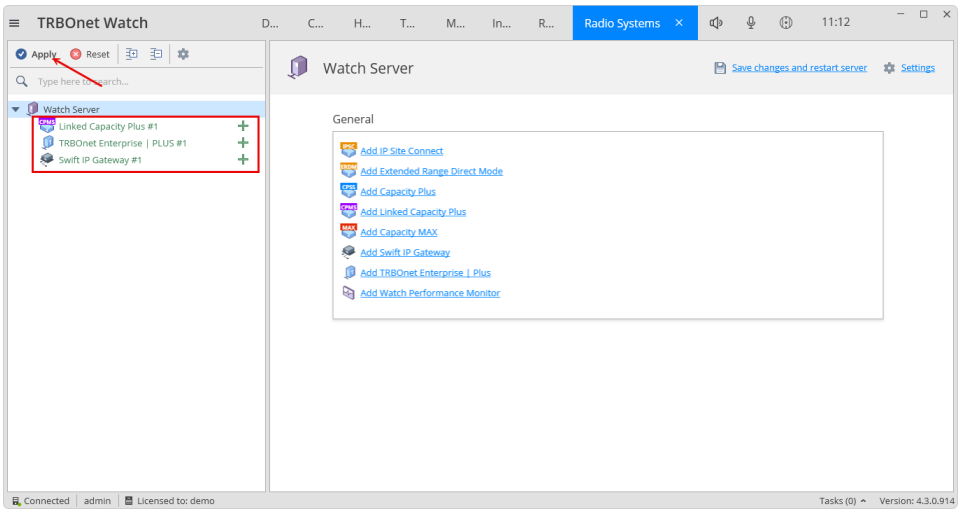


Figure 44: Added radio systems

To exclude a system from monitoring, click the ellipsis button on the right of the corresponding item in the left pane and click **Disable system** on the context menu.

Note: The license limits the number of systems that TRBOnet Watch can monitor simultaneously. To determine how many systems you can enable, check the number of repeaters specified in your license. If you enable more systems and exceed the limit, TRBOnet Watch will only monitor the allowed number of systems, and the remaining enabled systems will be ignored.

To view and edit the configuration settings of any system, select it in the left pane, and in the right pane, modify the required system settings.

Using the Context Menu

- Right-click on a system in the left pane to access the menu.

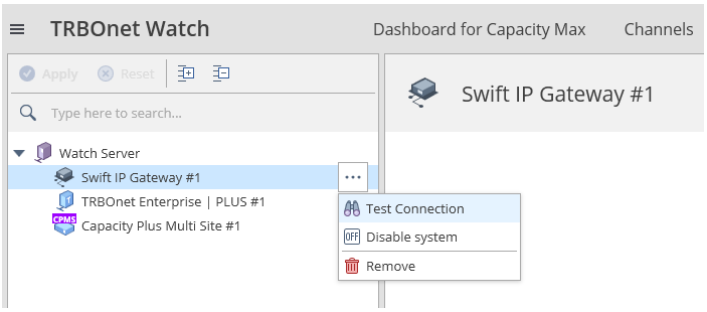


Figure 45: The context menu of a radio system

Use the context menu commands as follows:

- **Test connection**: Click to test the IP connection between the system and the TRBOnet Watch Server.
- **Enable system/Disable system**: Click to enable or disable monitoring of the selected system.
- **Remove**: Click to remove the selected system or the system component from.

5.5 Server Settings

This section describes the Server settings that can be specified in TRBOnet Watch Console.

To access the server settings:

- In the left pane, click the ellipsis button on the right of the Watch Server item, and from the context menu select **Settings**.

  Or, click the  icon on the left pane's toolbar.

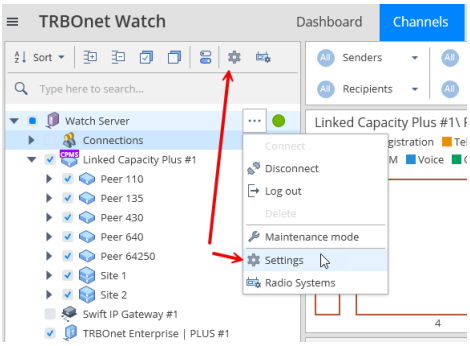


Figure 46: Accessing server settings

As a result, the **Settings** dialog box opens.

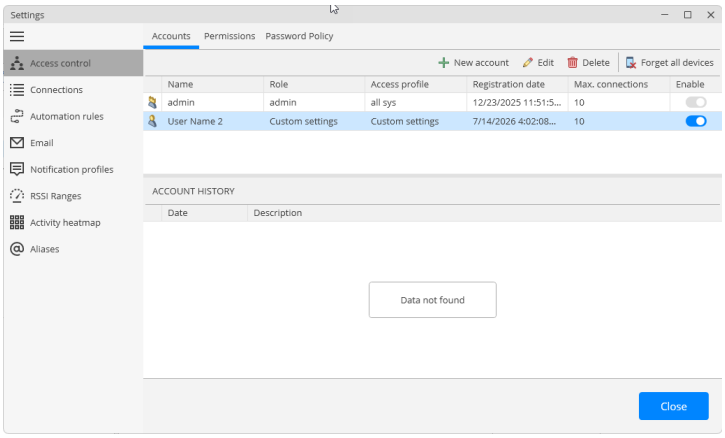


Figure 47: Server settings – Access Control

5.5.1 Access Control

This tab contains information about access control in TRBOnet Watch.

5.5.1.1 Accounts

The administrator can add, edit, and delete user accounts in the system.

- Click the **Accounts** tab.

Creating an Account

- To create an account, click **+ New account**.
  In the 'Account' dialog box, specify the following parameters:

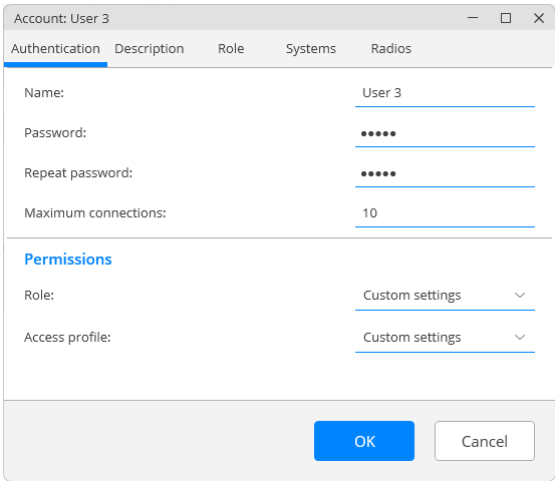


Figure 48: Adding user account

- **Name**
  Enter a name for the user.
- **Password**
  Enter a password for the user.
- **Repeat password**
  Enter the password again to confirm.
- **Maximum connections**
  Specify the maximum number of connections to the Watch Console from the user account.

Permissions

- **Role**
  From the drop-down list, select the role of the user. If you select 'Custom settings', you can specify required permissions on the **Role** tab that appears in the dialog box.
- **Access profile**
  Choose the access profile for the user. If you select 'Custom settings', you can specify required permissions on the **Systems** and **Radios** tabs that appear in the dialog box.

- On the **Description** tab, enter the **Email** and **Description** for the account.
- **Role** tab
  This tab will appear if you have selected 'Custom settings' in the 'Role' field. On this tab, select the modules that will be available to the user.
- **Systems** and **Radios** tabs
  These tabs will appear if you have selected 'Custom settings' in the 'Access profile' field. On these tabs, select systems and radios that will be available to the user.

Disabling/Enabling a User Account

To disable an account:

- Select an account in the Accounts table and turn off the toggle switch in the Status column.

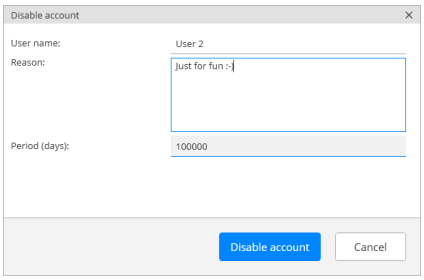


Figure 49: Disabling user account

In the 'Disable User Account' dialog box, specify the following parameters:

- **Reason**
  Enter the reason you are disabling the user.
- **Period (days)**
  Enter the number of days during which the user will not be allowed to connect to the Watch Console.

To enable an account:

- Select an account in the Accounts table and turn on the toggle switch in the Status column.

Account History

The table below shows the history of the selected account.

Detaching Mobile Devices from a User Account

In addition, you can detach mobile devices that have ever been used to connect to TRBOnet Watch Server via the given user account.

- Just select an account in the list and click the **Forget all devices** button. As a result, all mobile devices will be detached from the account and thus won't receive any push notifications configured for this account.

5.5.1.2 Permissions

The **Permissions** tab contains information about the roles and access profiles available to the user accounts.

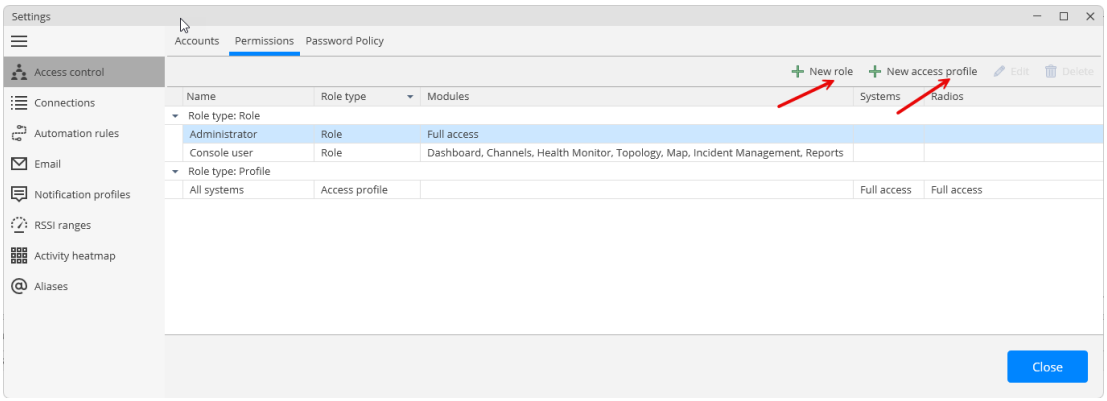


Figure 50: Server settings – Access control > Permissions

Creating a Role

- To create a role, click **+ New role**.
  In the 'Role' dialog box, specify the following parameters:
  - On the **General** tab, specify the Name and Description of the role.
  - On the **Role** tab, select the modules that will be available to this role.

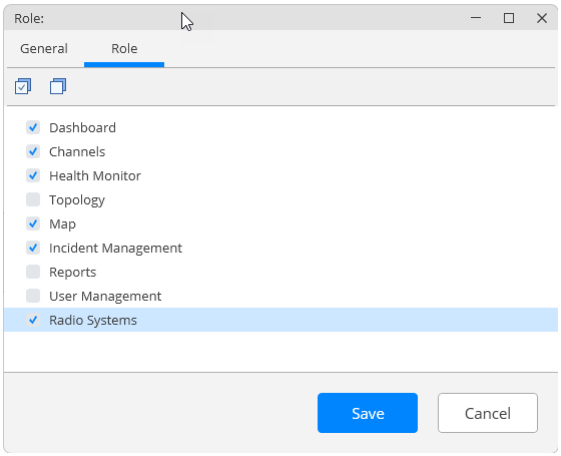


Figure 51: Creating role

Creating an Access Profile

- To create an access profile, click **+ New access profile**.
  In the 'Access profile' dialog box, specify the following parameters:
  - On the **General** tab, specify the Name and Description of the access profile.
  - On the **Systems** and **Radios** and tabs, select the systems and radios that will be available to this profile.

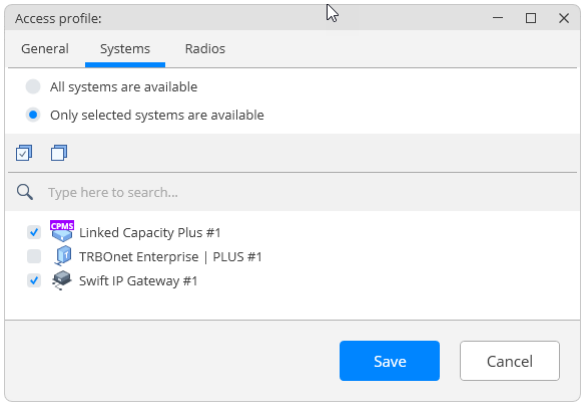


Figure 52: Access profile – Systems

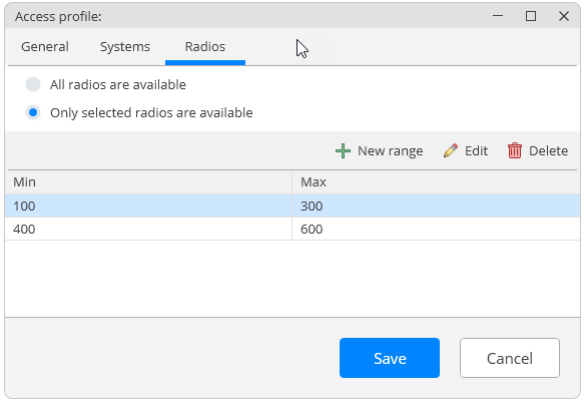


Figure 53: Access profile – Radios

5.5.1.3 Password Policy

The **Password Policy** tab contains information about password requirements.

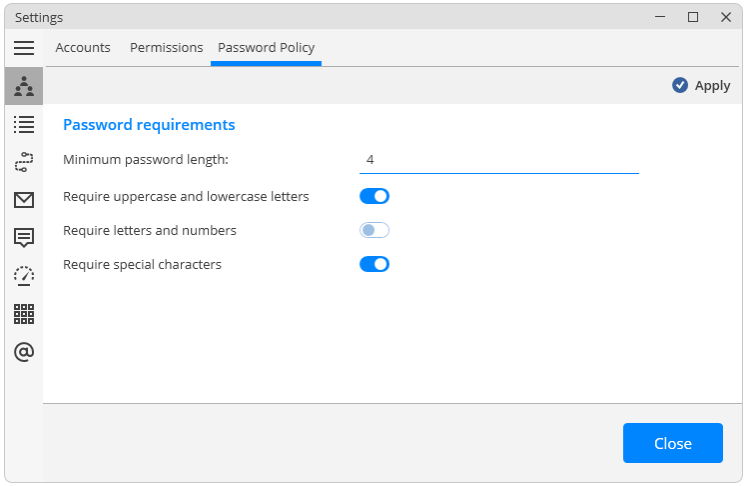


Figure 54: Password policy

- **Minimum password length**
  Enter the minimum password length, in characters.
- **Require uppercase and lowercase letters**
  Select this checkbox to require that a password include at least one uppercase letter (A-Z) and one lowercase letter (a-z).

- **Require letters and numbers**
  Select this checkbox to require that a password include at least one character from [A-Za-z] and at least one from [0-9].
- **Require special characters**
  Select this checkbox to require that a password include at least one non-alphanumeric character.

5.5.2 Connections

This tab contains information about current connections to the server.

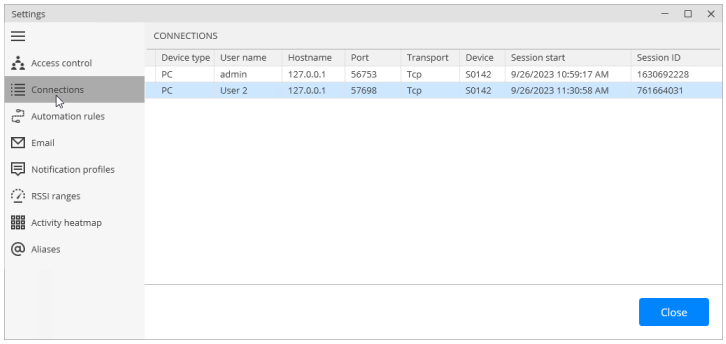


Figure 55: Server settings - Connections

5.5.3 Automation Rules

This tab contains information about the configured incident detection rules.

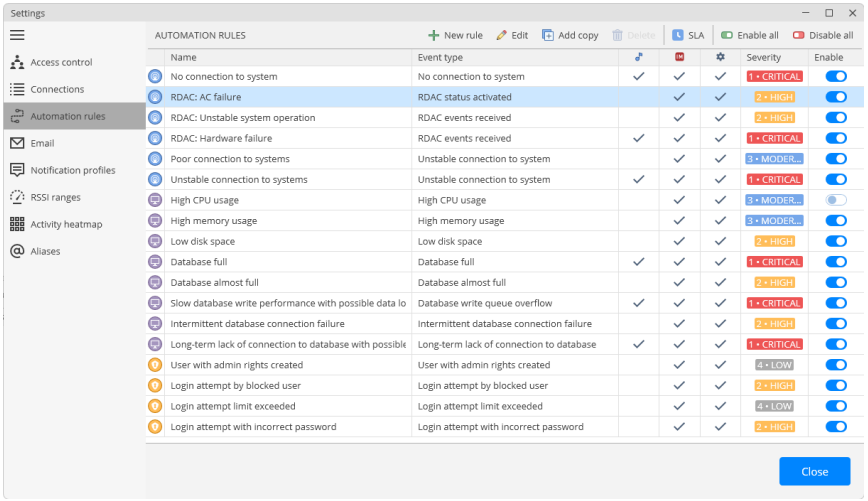


Figure 56: Server settings – Automation rules

For more information about adding/editing rules, refer to section 5.11.1, Incident Automation Rules (page 92).

5.5.4 Email Settings

To be able to send and receive email notifications, configure the following email-settings.

- In the **Settings** window, select the **Email** tab.

5.5.4.1 Email groups

In this section, you define the email groups that will be used for notification purposes.

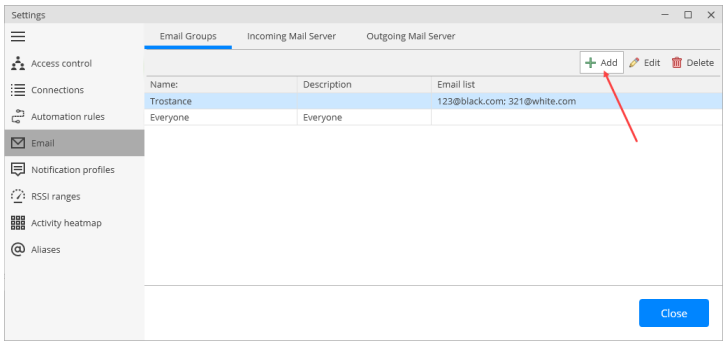


Figure 57: Server settings – Email settings

- In the right pane, click the **Email Groups** tab.
- To add an email group, click the **Add** button.

  In the dialog box that opens:

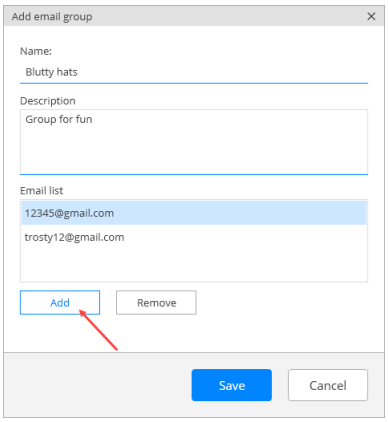


Figure 58: Adding an email group

  - Enter the **Name** and **Description** of the group.
  - To add an email address to the group, click the **Add** button and in the dialog box that opens enter the desired address.

5.5.4.2 Incoming mail server

In this section, you configure the incoming mail server parameters.

- In the right pane, click the **Incoming Mail Server** tab.

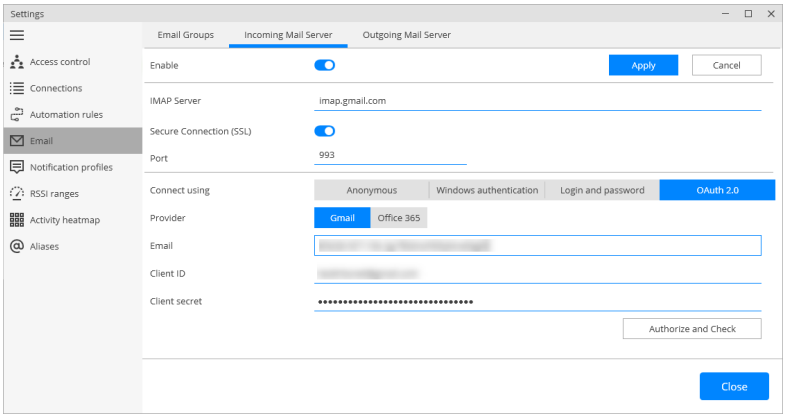


Figure 59: Email settings – Incoming mail server

- **Enable**
  Select this option to enable Incoming Mail Server.
- **IMAP Server**
  Enter the server hostname or IP address.
- **Secure connection (SSL)**
  Select this option to enable a secure connection. Note that a dedicated port will be used to connect to the mail server via SSL.

  Note: The port number will automatically change from **143** to **993** when you select this option.
- **Port**
  The port number to be used for the connection.

  Note: This box is populated automatically depending on whether a secure connection is selected or not.
- **Connect Using**
  Choose one of the following options:
  - **Anonymous access**
    Choose this option to use an anonymous access to the incoming mail server.
  - **Windows authentication**
    Choose this option to connect via TRBOnet Service Windows Account, if it is running under a specific account;
  - **Use login and password**
    Choose this option and specify the credentials for the mailbox:
    - ✓ **Login**
      Enter the incoming mail server login.
    - ✓ **Password**
      Enter the incoming mail server password.

- **OAuth 2.0**
  Choose this option if the email server requires OAuth 2.0 authorization.
  - ✓ **Provider**
    Choose either **Office 365** or **Gmail**.
  - ✓ **Email**
    Enter the email address.
  - ✓ If **Gmail** is selected as the email provider, enter the **Client ID** and **Client secret**.
    If **Office 365** is selected as the email provider, enter the **Client ID** and **Tenant ID**.
  - ✓ **Authorize and Check**
    Click this button to authorize your email account and check for new emails.

Notes: You must log into your email account on the same computer where TRBOnet Watch Server is running.
Also note that only a single IMAP server account can be associated with a single TRBOnet Watch Server.

5.5.4.3 Outgoing mail server

The SMTP Server is used to send emails from users to mail servers as well as between mail servers to deliver emails to the final destination.

- In the right pane, click the **Outgoing Mail Server** tab.

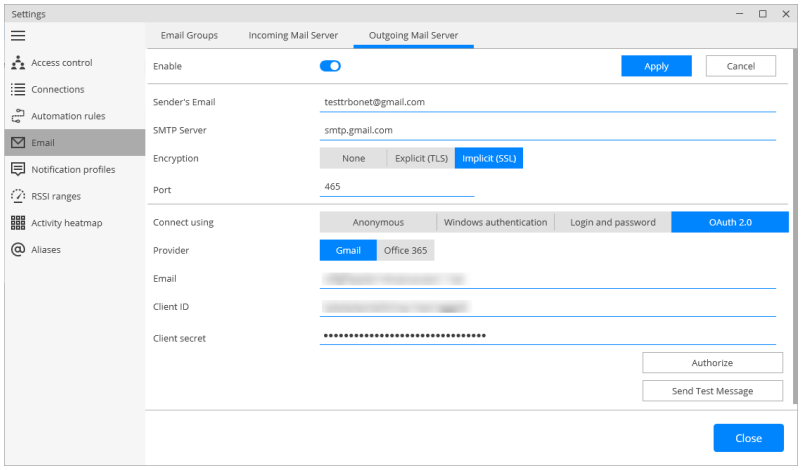


Figure 60: Email settings – Outgoing mail server

- **Enable**
  Select this option to enable Outgoing Mail Server.
- **Sender's Email**
  Enter the email address (optional) of the sender.

- **SMTP Server**
  Enter the server hostname or IP address of the SMTP server.
- **Encryption**
  Choose one of the encryption protocols (**TLS** or **SSL**) if a secure connection is required, or select **None** if not. Note that three different dedicated ports will be used to connect to the mail server: via SSL, TLS, or with no encryption.

  Note: The port number will automatically change when you select the encryption protocol. For example, from **25** (no encryption) to **465** for SSL, and to **587** for TLS.
- **Port**
  The port number to be used for the connection.

  Note: This box is populated automatically depending on the selected encryption protocol.
- **Connect using**
  Choose one of the following options:
  - **Anonymous access**
    Choose this option to use an anonymous access to the SMTP server.
  - **Windows authentication**
    Choose this option to connect via TRBOnet Service Windows Account, if it is running under a specific account;
  - **Login and password**
    Choose this option and specify the credentials for the mailbox:
    - ✓ **Username**
      Enter the SMTP server user name.
    - ✓ **Password**
      Enter the SMTP server password.
    - ✓ **Type**
      Choose the SMTP login type.
  - **OAuth 2.0**
    Choose this option if the email server requires OAuth 2.0 authorization.
    - ✓ **Provider**
      Choose either **Office 365** or **Gmail**.
    - ✓ **Provider**
      Choose either **Office 365** or **Gmail**.
    - ✓ **Email**
      Enter the email address.

✓ If **Gmail** is selected as the email provider, enter the **Client ID** and **Client secret**.
If **Office 365** is selected as the email provider, enter the **Client ID** and **Tenant ID**.

✓ **Authorize**
Click this button to authorize your email account.

✓ **Send Test Message**
Click this button to send a test message from the Sender Email address.
As a result, you will receive a response to your message with the same subject.

Note: You must log into your email account on the same computer where TRBOnet Watch Server is running.

5.5.5 Notification Profiles

In this tab, you can configure notification profiles that will be used in the Incident Detection Rules (see section 5.11.1, Incident Automation Rules)

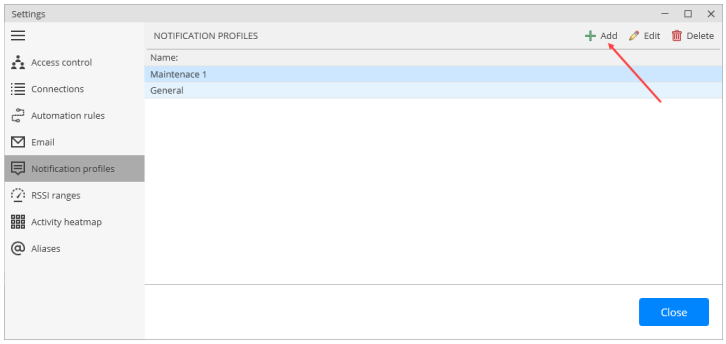


Figure 61: Server settings – Notification profiles

To add a notification profile:

- Click the **Add** button.

In the dialog box that opens, specify the following parameters:

- **Name**
  Enter a name for the notification profile

Email Groups tab

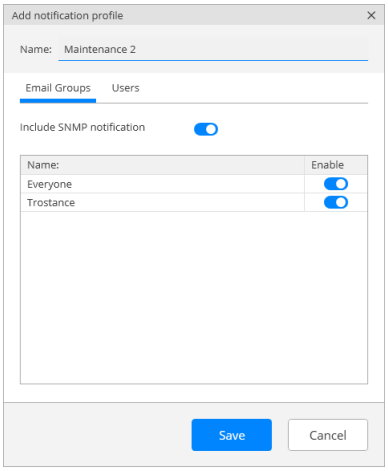


Figure 62: Notification profile – Email groups

- **Include SNMP notifications**
  Select this option to include SNMP notifications in the notification profile.
- Add email groups by turning on the appropriate toggle switches.

Users tab

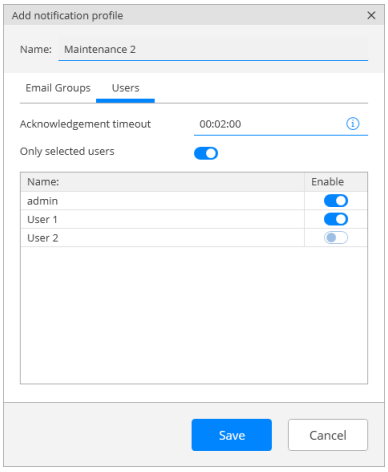


Figure 63: Notification profile – Users

- **Acknowledgement timeout**
  Enter the timeout for waiting for an acknowledgement. If an incident is not acknowledged during this time, TRBOnet will resend it using a different delivery option (push notification and/or email message).
- **Only selected users**
  Select this option to send notifications only to selected users, and turn on the appropriate toggle switches.

5.5.6 RSSI Ranges

On this tab, you can define the colors for RSSI zones depending on the RSSI level, in dBm. These colored zones will be displayed on the map, as well as in the RSSI Levels report. In addition, you can introduce your own RSSI zones with their respective colors.

See also section 5.10.1, Loading RSSI data.

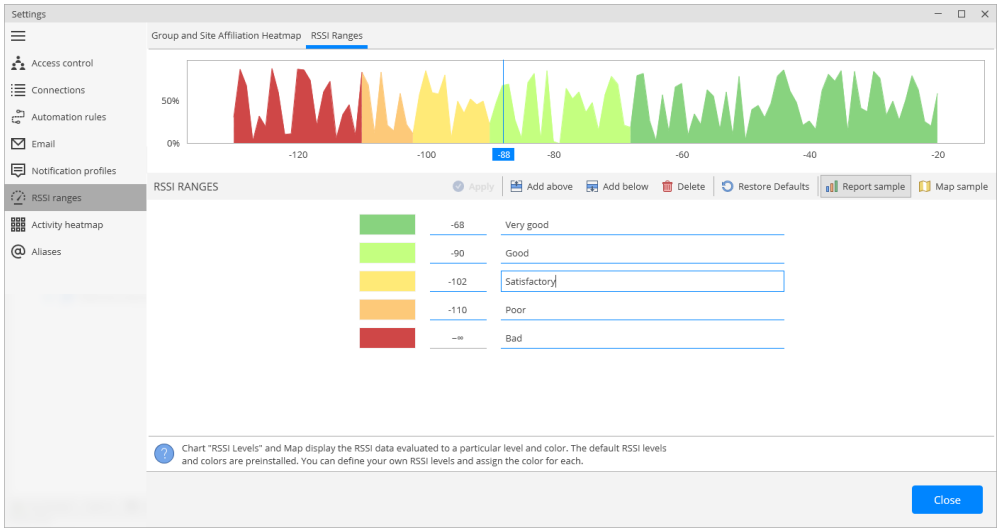


Figure 64: : Server settings – RSSI Ranges

5.5.7 Activity Heatmap

On this tab, you can define the colors for displaying group and site affiliation levels on the **Dashboard** tab. In addition, you can introduce your own levels with their respective colors.

See also section 5.6, Dashboard.



Figure 65: : Server settings – Radio activity heatmap

5.5.7.1 Advanced

On this tab, you configure how radio activity is displayed in the Dashboard screen.

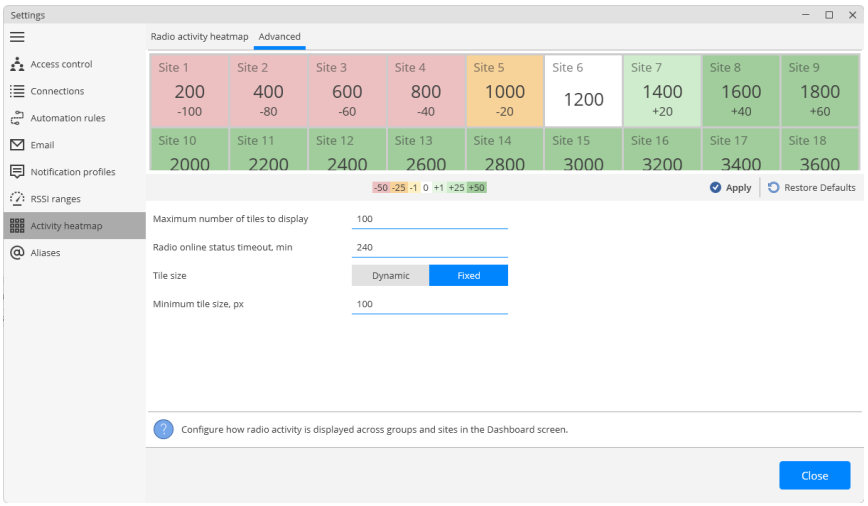


Figure 66: Activity heatmap – Advanced

- **Maximum number of tiles to display**
  Enter the maximum number of tiles that will be displayed. If the number of sites/groups exceeds this number, the remaining sites/groups will be placed in a separate tile named 'Other'.
- **Radio online status timeout, min**
  Enter the timeout for the radio online status. If the radio gets offline, it will be displayed as offline after this timeout expires.
- **Tile size**
  - **Dynamic**
    Choose this mode so that the tiles will be scaled according to their corresponding site/group load.
  - **Fixed**
    Choose this mode so that all tiles will have the same size regardless of the site/group load.
- **Minimum tile size**
  Enter the minimum size for the same-sized tiles.

5.5.8 Aliases

In this tab, you can configure the aliases that will be used for radios and radio groups. In addition, you can add tags and assign them to radios.

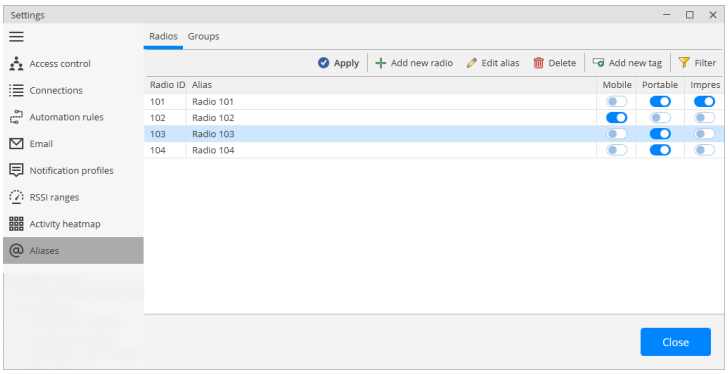


Figure 67: Aliases for radios and talk groups

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

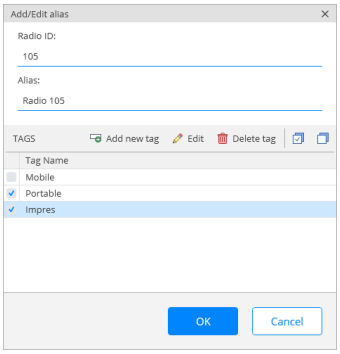


Figure 68: Aliases for radios and talk groups

In the **Add/Edit Alias** dialog box, specify the following parameters:

- **Radio ID**
  Enter the ID of the radio.
- **Alias**
  Enter the alias for the radio.
- **Add new tag**
  Click this button and enter the tag name.
  In the list of tags, select the tag(s) that can be assigned to the radio.

In a similar way, you can add aliases for radio groups (except for tags). Just go to the **Groups** tab and add aliases for groups.

5.5.8.1 Importing Radios and Groups

You can also import aliases of radios and radio groups from the connected TRBOnet Enterprise | PLUS systems.

- While on the **Channels** tab, in the left pane, select **TRBOnet Enterprise | PLUS** you have added to Watch server.
- In the right pane, go to **Import aliases** section, and click the **Reload Radios and Groups** link.
  Click **Import** buttons for radios and groups.

Note: If radios or radio groups with the same IDs already exist, you will be prompted to overwrite or skip them.

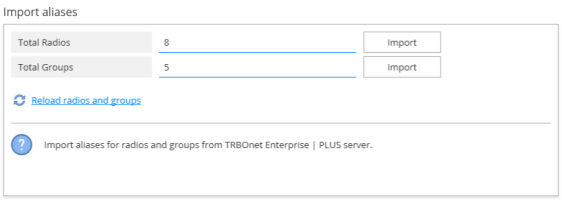


Figure 69: Importing aliases for radios and talk groups

Once you have imported radios and talk groups, you can assign to them required tags.

5.6 Dashboard

This tab displays the visual representation of the connected radio system, such as controllers, repeaters, RF sites, radio units, etc.

To configure the display of radio systems in the Dashboard screen, see section 5.5.7, Activity Heatmap.

To highlight the site the radio is on, select the **Find Radio** button and enter the ID of the radio.

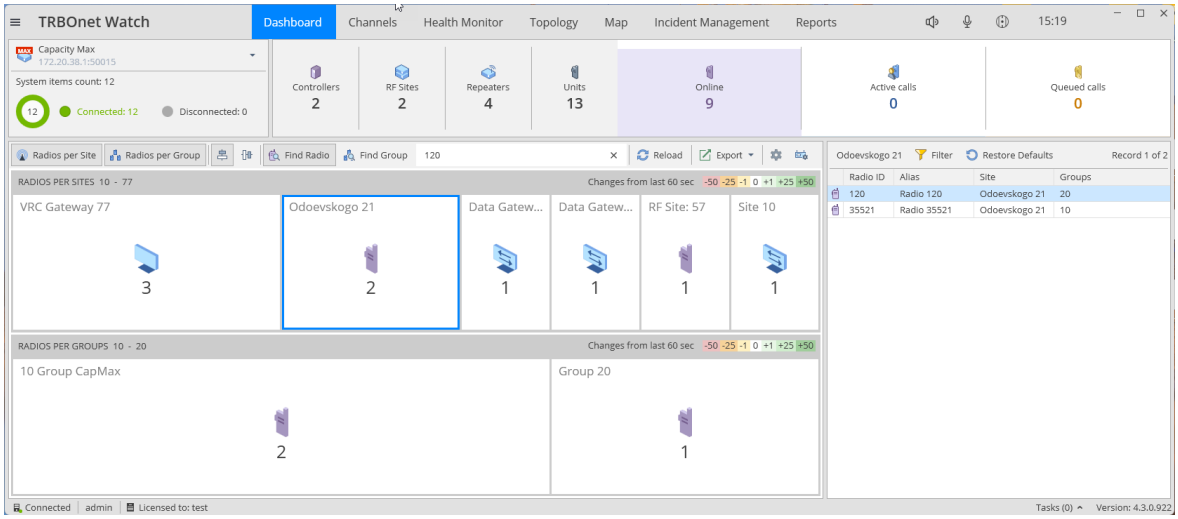


Figure 70: Dashboard tab – Highlighting a Site

To highlight the radio group, select the **Find Group** button and enter the ID of the radio group.

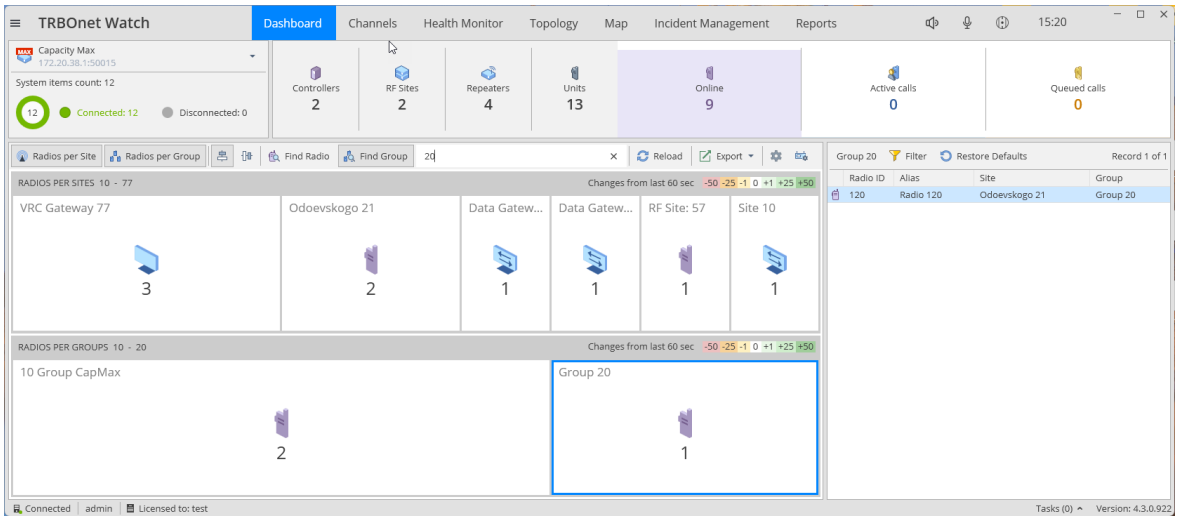


Figure 71: Dashboard tab – Highlighting a Gadio Group

5.7 Channels

Channels Monitoring is used for real-time monitoring of MOTOTRBO systems and Radio-over-IP gateways.

Note: The time on the computer hosting the TRBOnet Watch Console must be synchronized with the time on the computer hosting the TRBOnet Watch Server.

- Click the **Channels** tab in the upper bar.

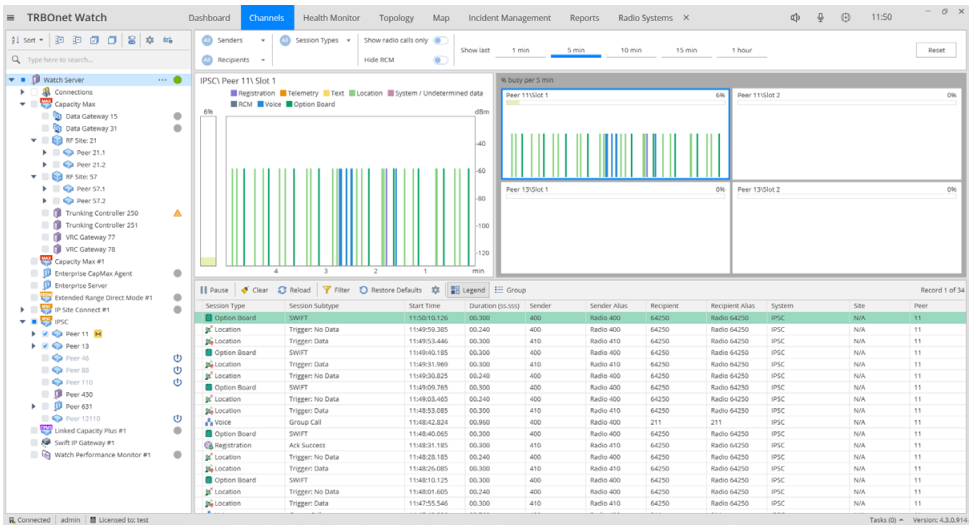


Figure 72: Channels tab

5.7.1 Left pane

In the left pane, you see the connected Watch Server and the associated radio systems. Select the checkboxes of the corresponding systems, repeaters, or slots to monitor their traffic in the right pane.

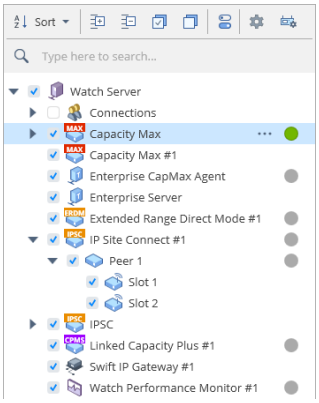


Figure 73: Left pane

In the upper part of the left pane, there is a toolbar from where you can manage elements as follows:

- 
  Click this button and select to sort elements in ascending or descending order.
- 
  Click this button to expand all elements.
- 
  Click this button to collapse all elements.
- 
  Click this button to select all elements.
- 
  Click this button to unselect all elements.
- 
  Click this button and on the menu that opens select the following options:
  - **Notify Watch users when new elements are added in server**
    Select this option so that notifications will arrive when new elements are added on the server.
  - **Enable monitoring of new elements**
    Select this option so that new elements will be automatically checked for monitoring.
- 
  Click this button to access the server settings.
  See section 5.5, Server Settings.
- 
  Click this button to configure radio systems.
  See section 5.4, Radio Systems.
- 
  In the text box next to this icon, type the text to search for in the names of systems, repeaters, slots, etc.

5.7.1.1 Watch Server

When a Watch server is connected, its status icon is displayed as a green circle.

If you click the ellipsis (...) button on the right of the server, the server's context menu will appear.

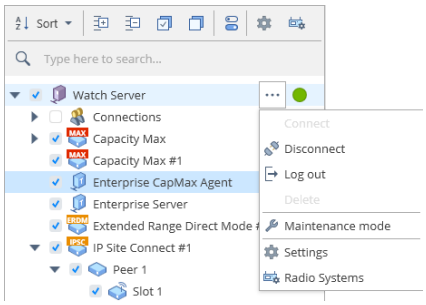


Figure 74: Watch Server's context menu

- **Disconnect**
  Select this menu item to disconnect from the server.
- **Log out**
  Select this menu item to log out and then log in as a different user. See also section 5.1, Connecting to TRBOnet Watch Server.
- **Maintenance mode**
  Select this menu item to start/stop the maintenance mode for Watch Server. In the dialog box that opens, select the duration of the maintenance mode, and whether to apply this mode to nested elements (systems and repeaters).
- **Settings**
  Select this menu item to open the Server Settings window. See section 5.5, Server Settings.
- **Radios systems**
  Select this menu item to configure radio systems. See section 5.4, Radio Systems.

5.7.1.2 Repeaters

If you click the ellipsis (...) button on the right of the repeater, the repeater's context menu will appear.

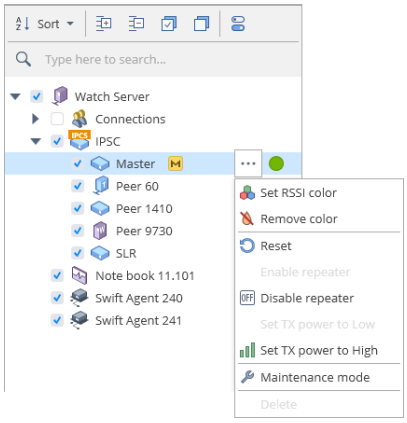


Figure 75: Repeater's context menu

- **Set RSSI color**
  Select this menu item to change the RSSI color for the selected repeater.
- **Reset**
  Select this menu item to reboot the repeater.
- **Disable/enable repeater**
  Select this menu item to disable/enable the repeater. A disabled repeater won't be able to receive and transmit data.
- **Set TX power to High/Low**
  Select this menu item to set the appropriate TX power level for the repeater.

- **Maintenance mode**
  Select this menu item to start/stop the maintenance mode for the repeater. In the dialog box that opens, select the duration of the maintenance mode, and whether to apply this mode to nested elements (repeaters).

  Note: When the repeater is in the maintenance mode, Watch won't generate any incidents on the repeater's alarms.

Note: For more information on how to remotely control repeaters, refer to section 5.8.3, Repeater Remote Control (page 80).

5.7.2 Filters

The filters are located on the upper toolbar on the right panel.



Figure 76: Channels - Filter toolbar

Senders / Recipients

Click the arrow on the right and choose one of the following options:

- **All**
- **Specified**
  Enter the ID of the radio.
  Here you can also enter multiple radios. Just separate each ID by a comma, or enter the range, like: 12, 35, 105-111, 249.
- **Range**
  Enter the **From** and **To** values to define the range of radio IDs.
- **By mask**
  To specify a mask, use digits and the following wildcards:
  - % to replace any number of digits in the radio ID
  - _ (underscore) to replace one digit in the radio ID

  For instance, enter the mask _12%34_6 to filter out IDs 112003406, 91263476, and others.

Session Types

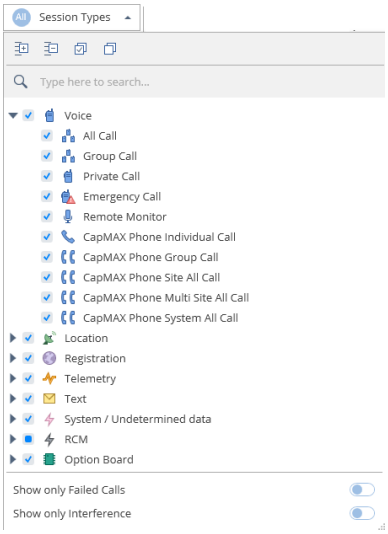


Figure 77: Session types

Select the **Show only Failed Calls** and **Show only Interference** options to select the respective messages in the **RCM** section.

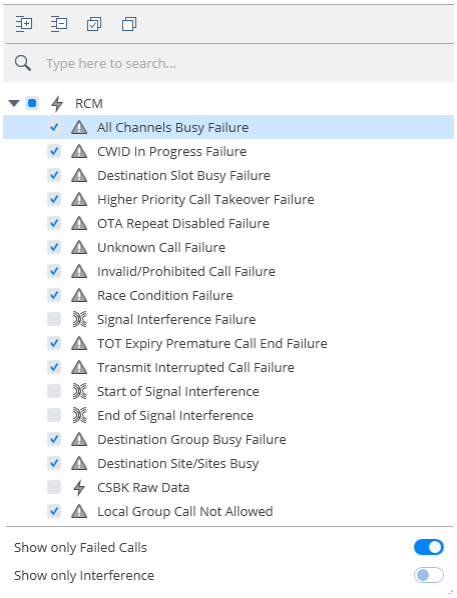


Figure 78: RCM section

Misc. Options

- **Show only calls from radios**
  Select to avoid duplication of calls in a report for the case when a multi-site system is used and radio calls are routed to multiple sites.
- **Show RCM**
  Select to include RCM messages.

Show last

Select the data collection time period (last 1 min, 5 min, 10 min, 15 min, or 1 hour).

Reset Filters

Click the **Reset** button to clear the selected filters.

5.7.3 Slot's traffic

In the right pane, you see the slots of the systems selected in the left pane.

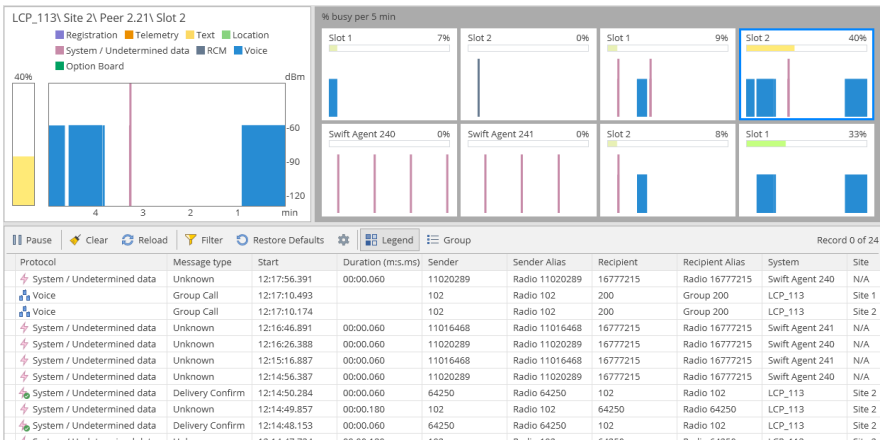


Figure 79: Channels – Slot's traffic

The real-time traffic monitor displays activity in the slot in real time. The received calls are displayed as vertical-colored bars moving across the monitor.

- The height of the bar indicates the RSSI level (in dBm) of the received signal relative to the Y-axis.
- The width of the bar corresponds to the duration of the signal (in milliseconds) relative to the X-axis.
- The color of the bar indicates the type of the transmitted data. The legend above the bars shows the meaning of each color: Registration (ARS), Telemetry, Text, Location (GPS), System, Voice, User (user-defined data format), Data (all non-voice calls in LCP systems), Option Board.

The color-graded bar is located on the left of the image of each slot, and the percentage value in each monitor indicates the workload of the slot.

5.8 Health Monitor

The **Health Monitor** tab displays the diagnostic information from all MOTOTRBO systems registered in your TRBOnet Watch. This tab shows alarms from repeaters and helps to pinpoint configuration problems.

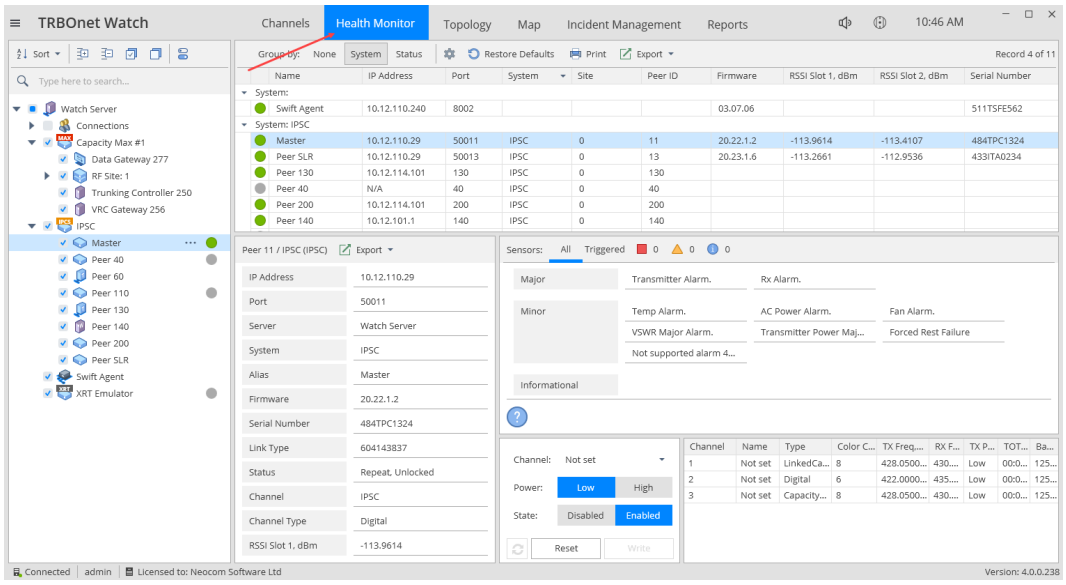


Figure 80: The Health Monitor tab

Additionally, you can use the **Health Monitor** tab to manage repeaters remotely. To learn more about this option, refer to section 5.8.3, Repeater Remote Control (page 80).

Note: The **Health Monitor** functionality is unavailable for Capacity Max systems.

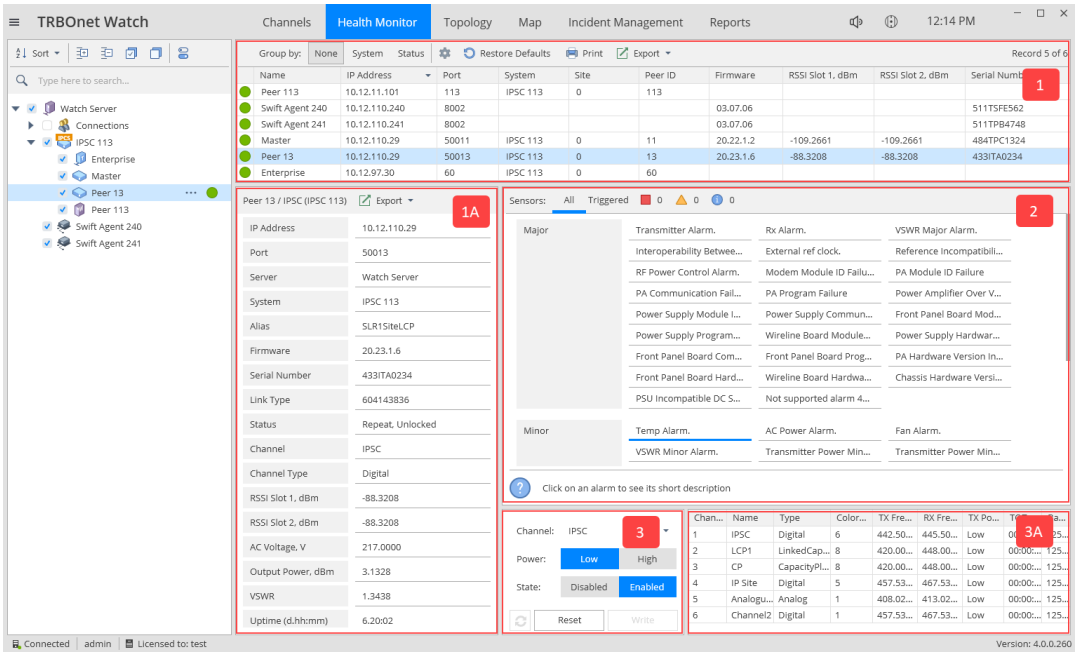


Figure 81: The Health Monitor panels

5.8.1 Repeaters

The **Repeaters, Controllers and Software Applications** list displays the diagnostic information about repeaters and peers in all registered MOTOTRBO systems. This panel is shown in Figure 80 as number 1.

You can also select which columns to display in this panel. Just click the gear button () on the top of the panel and select/unselect required columns.

The form (1A) shows more detailed information about the peer.

Table 16: Repeaters, Controllers and Software Applications list - settings

Setting	Description
IP Address	The IP address of the peer.
Port	The UDP port of the peer.
System	The radio system the peer belongs to.
Site	The site ID of the peer. Applies to Linked Capacity Plus systems, and RF sites (Capacity Max). Otherwise, displays 0.
Peer ID	The peer ID.
Alias	The peer alias (if defined). To learn more about adding aliases, refer to section Adding Peers (page 36).
Firmware	The firmware version of the repeater. Not applicable to software peers.
Serial Number	The serial number of the hardware.
Status	The operational state of the repeater. The normal state is "Repeat, Unlocked". Not applicable to software peers.
Channel	The channel name of the repeater specified in MOTOTRBO CPS. Not applicable to software peers (displays "No Data").
Channel Type	The channel type. Values: Digital, Capacity Plus Voice, Capacity Plus Data, Linked Capacity Plus Voice, Linked Capacity Plus Data. Not applicable to software peers.
RSSI Slot 1 (dBm)	The signal strength level on Slot 1 of the repeater.
RSSI Slot 2 (dBm)	The signal strength level on Slot 2 of the repeater.
AC Voltage (V)	The AC voltage of the repeater (when not powered from the battery). Supported by New Generation repeaters only.
Output Power (dBm)	The output power. Supported by New Generation repeaters only.

Setting	Description
VSWR	Voltage Standing Wave Ratio of the repeater. Display format: X:1. Supported by New Generation repeaters only.
Uptime (d.h:m)	The total time the repeater is up and running.

5.8.1.1 Exporting repeater data

To export repeater data to a different format, click the Export button and from the drop-down menu, select the desired format.

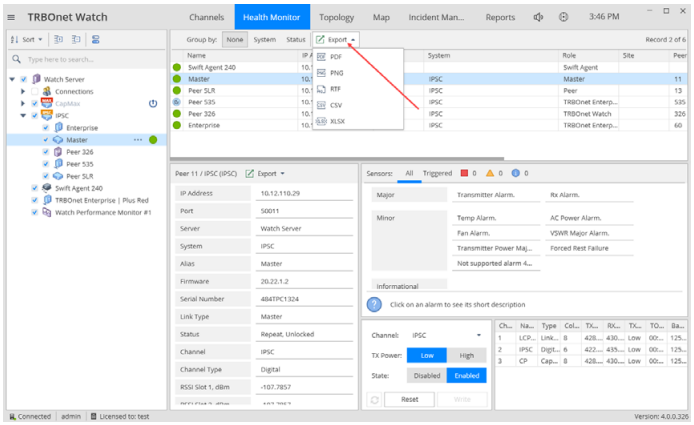


Figure 82: Exporting repeater data

5.8.2 Sensors

The **Sensors** panel is shown in Figure 80 as number 2. It displays alarms of the repeater selected in the **Repeaters, Controllers and Software Applications** list.

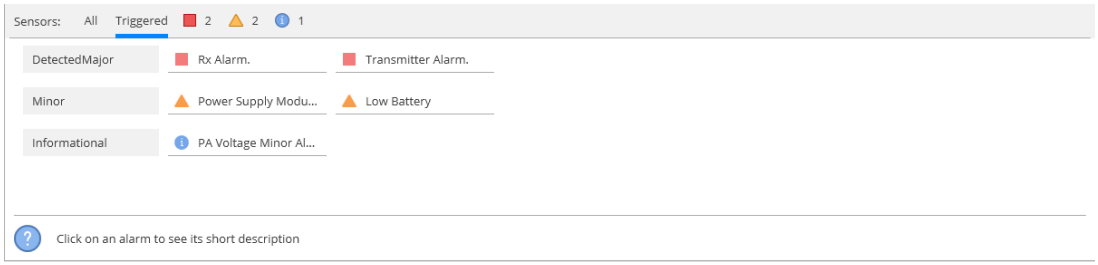


Figure 83: The Sensors panel for a repeater

5.8.2.1 Alarm icons

The following icons are used to indicate alarm severity levels:

- The "red box" icon indicates a major alarm.
- The "attention" icon (yellow triangle) indicates a minor alarm.
- The "information" icon (blue circle with the "i" character) indicates an information alarm.

If a repeater generates several alarms of different severity levels (major, minor, and/or information), the highest of these severity levels is indicated by the icon.

Click on a particular alarm to see its short description.

5.8.3 Repeater Remote Control

The **Remote Control** panel (number 3 in Figure 80) displays the current settings of the repeater that you can modify remotely:

- **Channel**: The selected channel.
- **TX Power**: The transmission power configured for the selected channel.
- **State**: The operational status of the repeater.

The **Repeater preprogrammed channels** panel (number 3A in Figure 80) displays the list of channels available for use with this repeater.

The information in the list is read-only. The settings of the programmed channel are as follows:

- **Channel**: The ordinal number of the channel programmed in the repeater configuration.
- **Name**: The channel name programmed in the repeater configuration.
- **TX Freq, MHz**: The TX frequency of the channel.
- **RX Freq, MHz**: The RX frequency of the channel.
- **Bandwidth, Hz**: The bandwidth of the channel.
- **Color Code**: The color code of the channel.
- **Type**: The type of the channel programmed in the repeater configuration. Allowed values: Digital, Capacity Plus Voice, Capacity Plus Data, Linked Capacity Plus Voice, Linked Capacity Plus Data.
- **TX Power**: The transmission power programmed in the repeater configuration.
- **TOT, sec**: The timeout, in seconds, during which the radio can continuously transmit before transmission terminates automatically.

You can perform the following remote operations with a repeater.

Use a different channel on the repeater:

- Select the repeater in the **Repeaters, Controllers and Software Applications** list (number 1 in Figure 80).
- In the **Remote Control** panel (number 3 in Figure 80), expand the **Channel** drop-down menu and click a different channel.
- Click the **Write** button. The repeater configuration update may take more than a minute.
- If the channel type has changed after the update, launch the TRBOnet Watch Server and specify the **System Type** setting accordingly, as described in section 5.4.1, MOTOTRBO IPSC, CP, LCP, and ERDM (page 35).

Change the TX Power of the repeater:

High transmission power is required to get a stronger signal and extend transmission distances. Low transmission power is preferred for communication in close proximity; it also serves to prevent transmissions into other geographical groups.

- Select the repeater in the **Repeaters, Controllers and Software Applications** list (number 1 in Figure 80).
- In the **Remote Control** panel (number 3 in Figure 80), click the desired **TX Power** option: **High** or **Low**.
- Click the **Write** button.

Enable/disable the repeater:

When enabled, the repeater transmits, receives, and repeats operations.

When disabled, the repeater cannot transmit, receive, or repeat. In the disabled mode, the repeater responds to GPIO controls such as channel steering and diagnostics to sending alarms.

- Select the repeater in the **Repeaters, Controllers and Software Applications** list (number 1 in Figure 80).
- In the **Remote Control** panel (number 3 in Figure 80), click the desired **Status** option: **Enabled** or **Disabled**.
- Click the **Write** button.

Reboot the repeater remotely:

- Select the repeater in the **Repeaters, Controllers and Software Applications** list (number 1 in Figure 80).
- Click the **Reset** button in the **Remote Control** panel (number 3 in Figure 80).

Note: You can also use the context menu of a repeater in the left pane (see Figure 74: Repeater's context menu) to remotely modify the repeater's transmission power and operational status, as well as to remotely reboot the repeater.

Reload the configuration settings:

- Select the repeater in the **Repeaters, Controllers and Software Applications** list (number 1 in Figure 80).
- Click  in the **Remote Control** panel (number 3 in Figure 80).

The latest configuration settings of the repeater are loaded to the **Remote Control** panel and to the **Repeater Preprogrammed Channels** list.

5.8.4 RoIP gateways

If you select a RoIP gateway, you will see the following information:

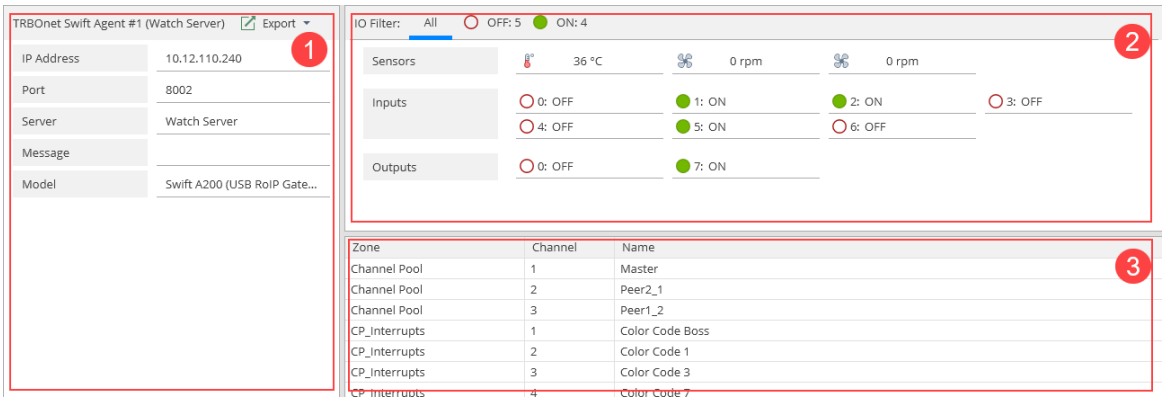


Figure 84: Diagnostic information for a RoIP gateway

On panel 1:

- **IP Address**
  The IP address of the RoIP gateway.
- **Port**
  The IP port of the RoIP gateway.
- **Model**
  The model number of the RoIP gateway.

On panel 2:

- **Sensors**
  - Temperature, °C
    The temperature measured inside the hardware RoIP gateway (TRBOnet Swift Agent).
  - Cooler 1, rpm
    The speed of cooler 1 connected to the TRBOnet Swift Agent (rotations per minute)
  - Cooler 2, rpm
    The speed of cooler 2 connected to the TRBOnet Swift Agent (rotations per minute)
- **Inputs**
  The statuses of the input pins configured on the TRBOnet Swift Agent.
- **Outputs**
  The statuses of the output pins configured on the TRBOnet Swift Agent.

On panel 3, you see information on the channels configured on the TRBOnet Swift Agent.

5.9 Topology

The **Topology** tab allows you to inspect the topology and connection statuses of all MOTOTRBO system peers and RoIP gateways monitored in TRBOnet Watch.

To show/hide an element, select/deselect it in the left pane.

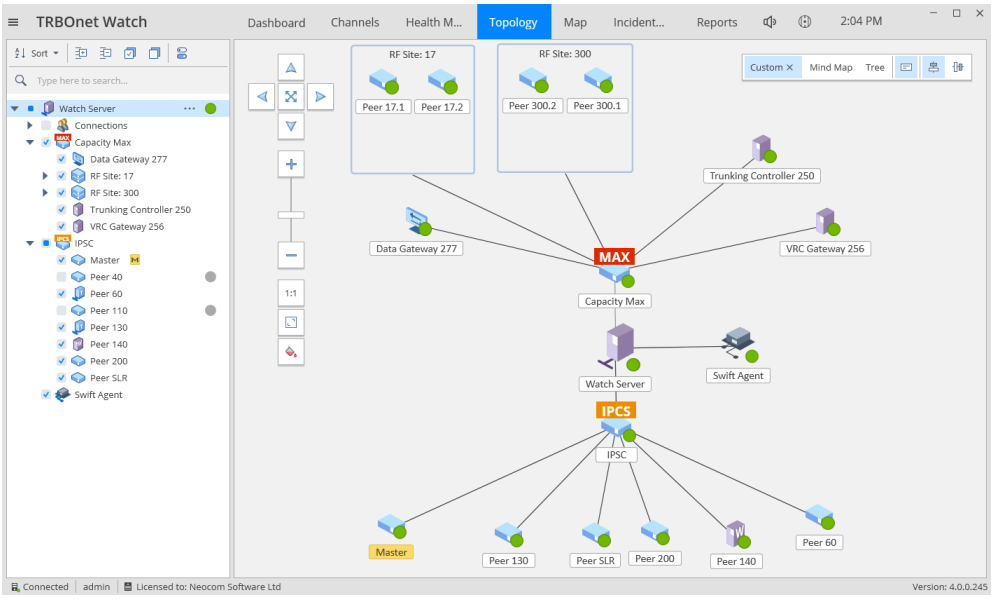
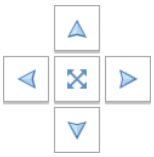


Figure 85: Topology of connected systems

Navigation

- Use the navigation arrows:

  Or, drag the mouse.

Scale

- Drag the slider or use the plus or minus button to scale the layout.

  Or, use the mouse wheel to zoom in/out.

- 

  Click this button to use the original scale.

- 
  Click this button to fit the displayed system(s) to the window.

Background

- 
  Click this button and select the background for the Topology view.

Layout

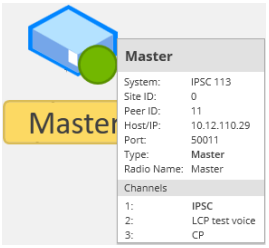
- **Custom**
  Click the Plus button and define your own topology layout by dragging the nodes to the desired positions.
- **Mind Map**
  Click this button to represent the topology layout as a mind map.
- **Tree**
  Click this button to represent the topology layout as a tree.
-
  Toggle this button to show/hide labels on the topology layout.
- 
  Click this button to center the topology layout horizontally.
- 
  Click this button to center the topology layout vertically.

5.9.1 Topology elements

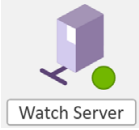
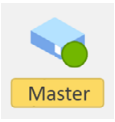
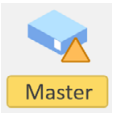
MOTOTRBO system elements are represented with the help of images, labels, and icons:

- Images classify elements as a repeater, hardware, software, or an unknown item (a non-registered element detected in the IP network).
- Labels identify elements.
- Icons provide information about the connection status of the elements.

If you point at an element with the mouse cursor, the tooltip shows the information about the element (ID and alias), the IP connection settings, and system settings.



The following examples explain how to read the information in the topology view.

	Image: Server ▪ TRBOnet Watch Server (key element) Icon: Normal IP connection
	Image: Repeater ▪ MOTOTRBO system Icon: Normal IP connection
	Image: Repeater ▪ Master repeater Icon: Normal IP condition, no RDAC issues
	Image: Repeater ▪ Peer repeater Icon: Normal IP connection, no RDAC issues
	Image: Repeater Icon: RDAC issue, minor severity level ("attention")
	Image: Repeater Icon: Repeater disabled (no transmission)
	Image: Repeater Icon: No RDAC connection
	Image: Repeater Icon: Maintenance mode
	Image: Repeater Icon: Not licensed
	Image: Swift Agent Icon: Normal IP connection
	Image: Software peer ▪ TRBOnet Watch application Icon: Normal IP connection
	Image: Software peer ▪ TRBOnet Enterprise application Icon: Normal IP connection
	Image: Software peer ▪ TRBOnet Enterprise application Icon: Redundancy - Active

5.10 Map

In the **Map** tab, the dispatcher can monitor the location of the selected radio systems, display RSSI levels, etc.

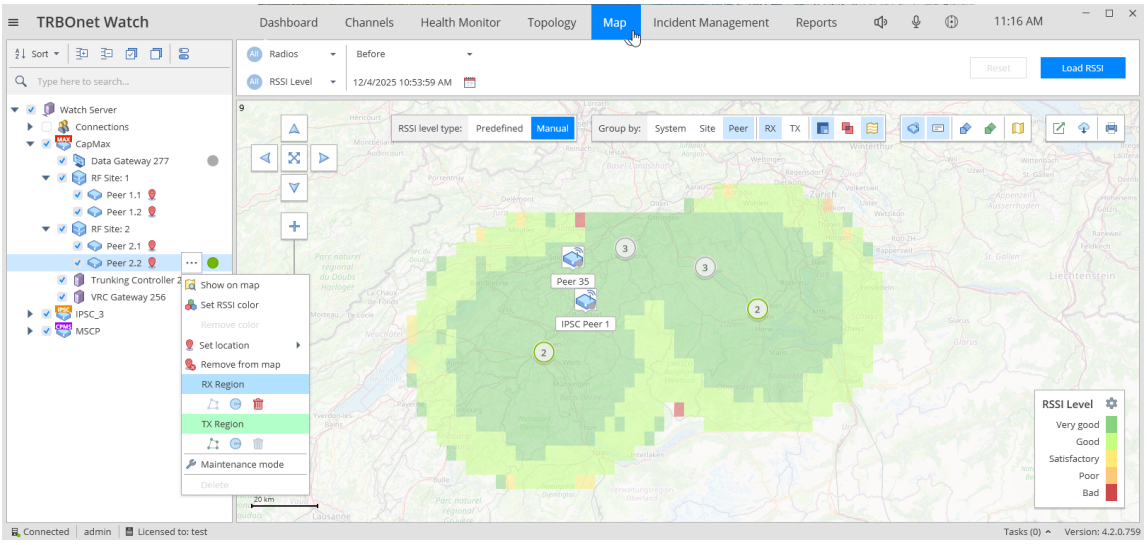


Figure 86: Map

In the left pane, you see the connected Watch Server and the associated radio systems.

To open the context menu, right-click on an item or click the ellipsis (...) button on the right of an item:

- **Show on map**
  Select this menu item to view the selected system/site/peer in the center of the map.
- **Set RSSI color**
  Select this menu item to change the RSSI color for the selected system/site/peer.

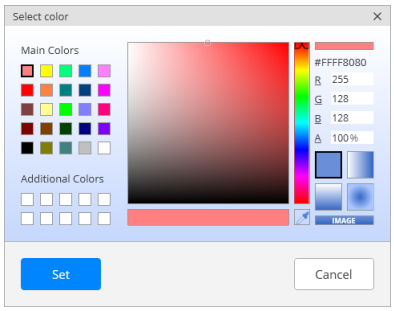


Figure 87: Selecting RSSI color

  - In the dialog box that opens, select the desired color, and click **Set**.
- **Remove color**
  Select this menu item to restore the RSSI color to its default value.

- **Set location**
  - **Position on map**
    Select this menu item and in the right pane click on the map where you want to place the selected system/site/peer.
  - **Use coordinates**
    Select this menu item and in the dialog box that opens select the coordinate system and enter the desired coordinates.
- **Remove from map**
  Select this menu item to remove the selected system/site/peer from the map.
- **RX region**
  Under this menu item, select one of the tools for drawing regions with the expected RX signal reception:
  - 
    Select this tool to draw a rectangular region around the selected site/peer.
  - 
    Select this tool to draw a circular region around the selected site/peer.
  - 
    Select this tool to delete the region around the selected site/peer.
- **TX region**
  Under this menu item, select one of the tools for drawing regions with the expected TX signal reception:
  - 
    Select this tool to draw a rectangular region around the selected site/peer.
  - 
    Select this tool to draw a circular region around the selected site/peer.
  - 
    Select this tool to delete the region around the selected site/peer.

5.10.1 Loading RSSI data

RSSI data is used to vizualize the actual coverage zone of your radio network on the electronic map. You can see on the map the RSSI levels measured in the selected system(s) during the predefined date and time range.

To load RSSI data:

- Click the **Load RSSI** button.

The coverage zone is represented on the map by colored rectangles. A rectangle is an area where the RSSI signals are measured. The map is divided into

rectangles of equal size. A rectangle is colored if any RSSI signal is detected in this area.

When pointed to with a mouse cursor, the rectangle shows its square outline, the number of RSSI signals, and the average RSSI level.

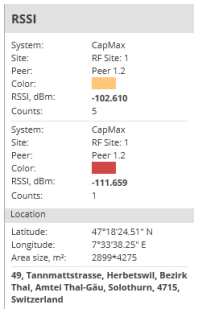


Figure 88: RSSI information

See also section 5.10.2, Display filters (RSSI level type).

5.10.1.1 Filter settings

The filters are located on the upper toolbar on the map panel.

Senders

Click the arrow on the right and choose one of the following options:

- **All**
- **Specified**
  Enter the ID of the radio.
  Here you can also enter multiple radios. Just separate each ID by a comma, or enter the range, like: 12, 35, 105-111, 249.
- **Range**
  Enter the **From** and **To** values to define the range of radio IDs.
- **By mask**
  To specify a mask, use digits and the following wildcards:
  - % to replace any number of digits in the radio ID
  - _ (underscore) to replace one digit in the radio ID

  For instance, enter the mask _12%34_6 to filter out IDs 112003406, 91263476, and others.

RSSI Level

Click the arrow on the right and choose of the following items:

- **All**
  Choose this item to load data with all available RSSI signal levels.
- **Show data with RSSI level lower than**
  Choose this item to load only data with the RSSI signal level lower than the specified value, in dBm.

- **Show data with RSSI level from ... to ...**
  Choose this item to load only data where the RSSI signal level falls within the specified range, in dBm.
- **Show data with RSSI higher than**
  Choose this item to load only data with the RSSI signal level higher than the specified value, in dBm.

Date and Time

Click the arrow on the right and choose one of the following options:

- **Between**
  Choose this option and select the **From**, **To**, and **Timeframe** values for the desired time period.
- **Before**
  Choose this option and select the date before which you want data to be included in the report.
- **Since**
  Choose this option and select the date since which you want to include data in the report.
- **Specific date**
  Choose this option and select the date.
- **Predefined values**
  Choose this option, then click the arrow on the right of the box below and choose the data collection time period (last x minutes/hours, today, yesterday, etc.).

5.10.2 Display filters

The map display filters are located in the upper part of the map pane.

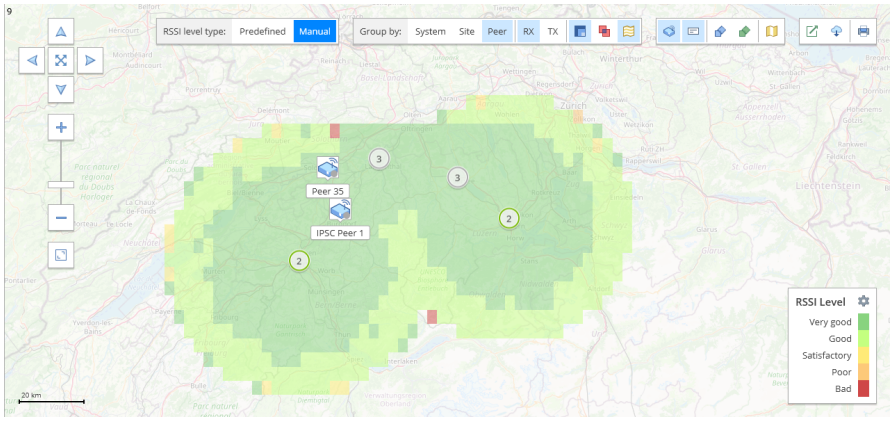


Figure 89: Map – Display filters

- **RSSI level type**
  Select how to display RSSI levels.

- **Predefined**
  RSII levels are represented in graduation of green. The brighter the color, the higher the RSSI level. The corresponding color legend is displayed in the lower-right corner of the Map pane.
- **Manual**
  RSII levels are represented according to the color scheme defined in Server Settings > RSSI ranges (see section 5.5.6, RSSI Ranges). The corresponding color legend is displayed in the lower-right corner of the Map pane.

- **Group by**
  Select how to group RSSI levels: by System, by Site, or by Peer.
- **RX/TX**
  Select which RSSI data to display: **RX** or **TX**. Where,
  RX is the signal received by the repeater.
  TX is the signal received by the radio equipped with the option board.

  Note: The minimum firmware versions that support RSSI TX data are as follows:

Swift GOB option board	04.00.38
Swift GOB R7 option board	07.00.14
Swift ST002m option board	06.00.17

- 
  Toggle this button to show/hide loaded RSSI data.
- 
  Select this button to show only intersections of RSSI regions.
- 
  Select this button to blur the underlying map.
- 
  Toggle this button to show/hide repeaters and systems.
-
  Toggle this button to show/hide labels for the repeaters and systems.
- 
  Toggle this button to show/hide RX regions.
- 
  Toggle this button to show/hide TX regions.
- 
  Click this button and select one of the following commands:
  Add Map, **Manage Maps**, or **Default Map**.
  For details, refer to section 5.3.2, Configuring the Maps.

5.10.3 Map toolbar

The map toolbar is located in the upper-right corner of the map pane.

- 
  Click this button to export RSSI data.
  Navigate to where you want to save the file, enter a **File name** and from the **Save as type** list, select either CSV or KML.
- 
  Click this button to download the tiles of the map currently displayed in the Map pane.

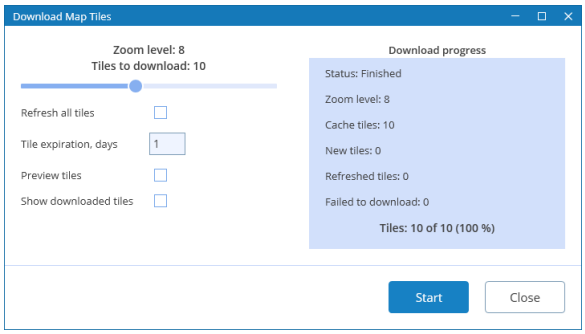


Figure 90: Downloading map tiles

In the dialog box, specify the following parameters:

- **Zoom level**
  Move the slider from left to right to increase the detail level of the map.
- **Refresh all tiles**
  Select this option to refresh the map tiles before saving to your PC.
- **Tile expiration, days**
  Enter the time the saved offline map will be stored before it is automatically updated.
- **Preview tiles**
  Select this option to show borders around the tiles to be downloaded.
- **Show downloaded tiles**
  Select this option to show how the tiles are being downloaded.
- Click **Start** and wait for the system to save the files. This may take several minutes.

- 
  Click this button to print the map region currently displayed in the Map pane.

5.11 Incident Management

Incidents are generated based on the detection rules specified.

For more information on the rules, refer to section 5.11.1, Incident Automation Rules.

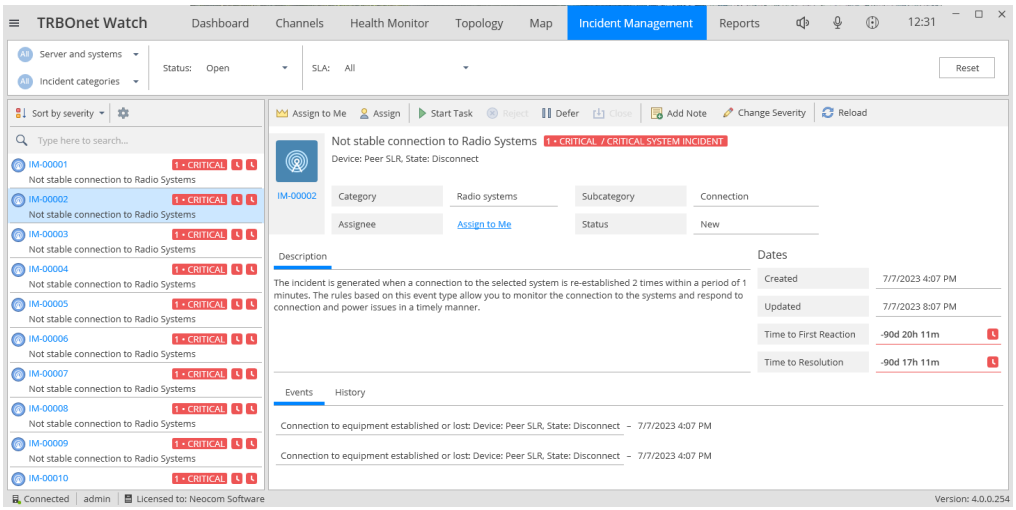


Figure 91: Incident Management tab

5.11.1 Incident Automation Rules

To add/edit incident detection rules, click the gear button on the left pane:

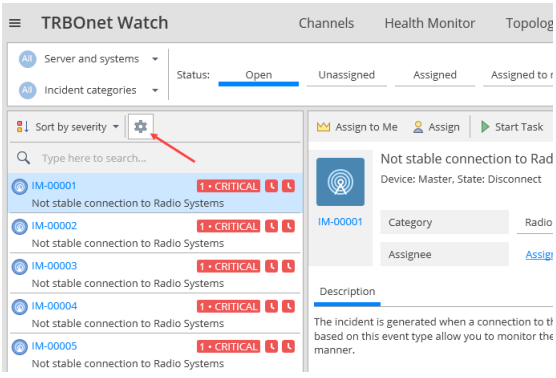


Figure 92: Accessing Incident Detection Rules

As a result, the **Settings** window appears with the **Automation rules** tab selected.

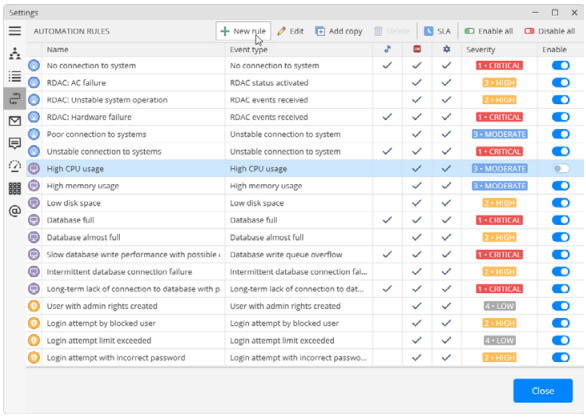


Figure 93: Server settings – Automation rules

To enable a rule:

- Turn on the toggle switch in the **Enable** column.

To create a rule:

- Click the **+ New rule** button.
  As a result, the **Rule** window opens.

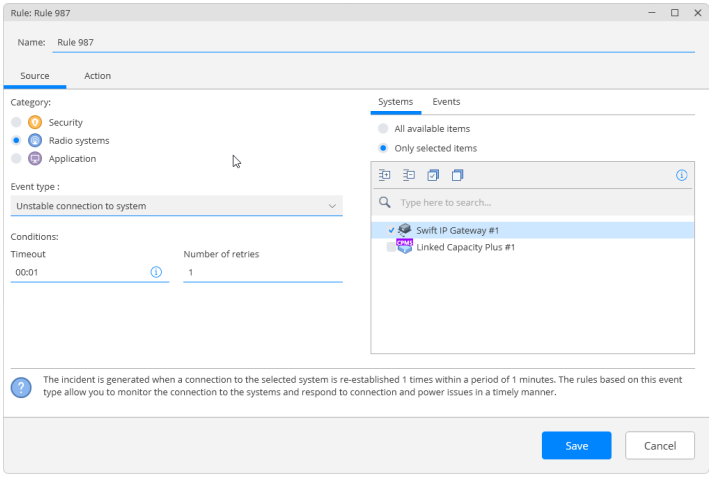


Figure 94: Incident automation rules - Adding a rule - Source

- **Name**
  Enter a name for the rule.

Source

- **Category**
  Choose the desired category for the rule (Security, Radio systems, or Application).
- **Event type**
  From the list, select an event type for the chosen category.
- **Conditions**
  - **Timeout**
    Enter the time period within which to count the events.

- **Number of the retries**
  Enter the number of times for the event to happen within the specified timeout.

- **Systems**
  Under this tab, select the radio systems.
- **Events**
  Under this tab, select the events to be expected.

Note: The **Systems** and **Events** tabs are available if the **Radio systems** item is chosen in the **Category** section.

Action

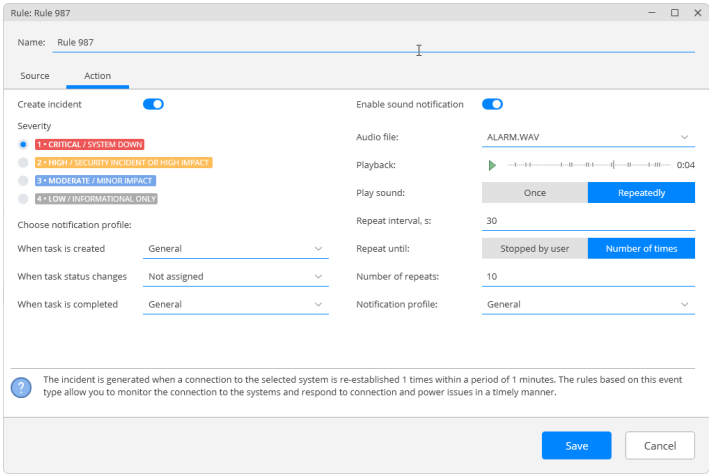


Figure 95: Incident automation rules - Adding a rule - Source

- **Create incident**
  Select this item to create an incident task.
  - **Severity**
    Choose the severity of the incident (Critical, High, Moderate, or Low).
  - **Choose notification profile**
    Select the notification profiles that will be used to send appropriate notifications in the following three cases: when the associated task is created, changed, or completed.

Note: For how to create notification profiles, refer to section 5.5.5, Notification Profiles (page 64).

- **Enable sound notification**
  Select this item to enable sound notification.
  - **Audio file**
    From the list, select the audio file to be played back.
  - **Playback**
    Click the green arrow icon to listen to the selected audio file.

- **Play sound**
  - **Once**
    Select this item to play the notification sound only once.
  - **Repeatedly**
    Select this item to play the notification sound repeatedly.
- **Repeat interval**
  Enter the repeat interval, in seconds.
- **Repeat until**
  - **Stopped by user**
    Select this item to play the notification sound util the console user stops playback manually by clicking the flashing bell icon ( ) on the console's upper bar.
  - **Number of times**
    Select this item to play the notification sound the specified number of times.
- **Number of repeats**
  Enter the number of repeats for the sound notification.
- **Notification profile**
  Select the notification profile that will be used for this sound notification.

-
  Here you see a description of the rule you are creating.

5.11.1.1 Changing SLA terms

- Click the **SLA** button.

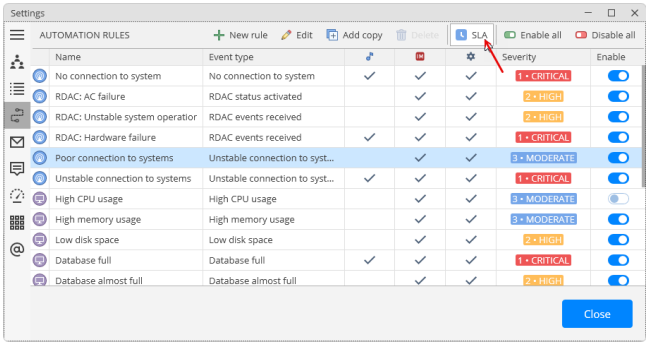


Figure 96: Automation rules – Accessing SLA terms

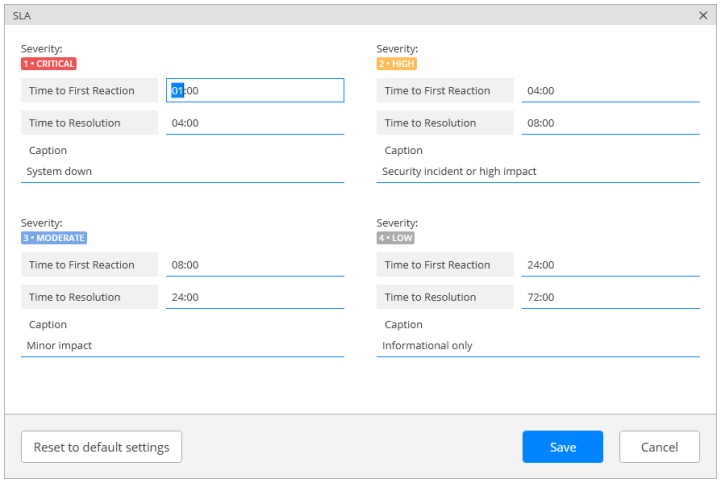


Figure 97: Incident detection rules – Editing SLA terms

For each of the severities, you can modify the following SLA parameters:

- **Time to First Reaction**
  Time before the task is started.
- **Time to Resolution**
  Time before the task is resolved (closed).
- **Caption**
  Caption that is displayed for the severity.

5.11.2 Incident Workflow

When an incident occurs, the corresponding notification will appear at the bottom right of the screen. In addition, the incident will appear in the left pane of **TRBOnet Watch** window when the **Incident Management** tab is selected.

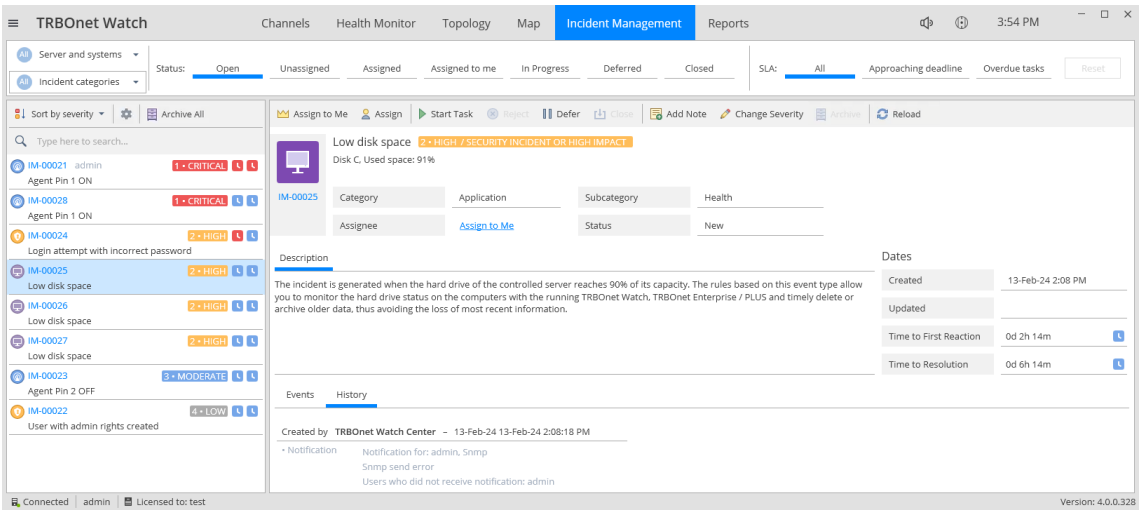


Figure 98: Incident Management - Workflow

5.11.2.1 View filters

The view filters are located on the upper toolbar.

- **Servers and systems**
  Select the radio systems which incidents you want to display.
- **Incident categories**
  Select the categories/subcategories you want to display.
- **Status**
  Choose one of the incident statuses you want to display.
  The statuses are as follows:
  Open, **Unassigned**, **Assigned**, **Assigned to Me**, **In Progress**, **Deferred**, **Closed**
- **SLA**
  Choose one of the SLA statuses you want to display.
  The SLA statuses are as follows:
  All, **Approaching deadline**, **Overdue tasks**
- To reset the filters, click the **Reset** button,

5.11.2.2 Incident handling

In the right pane, you see the detailed information on the incident selected in the left pane. To handle incidents, use the upper toolbar buttons in the right part of the window.

To assign the incident:

- Click the **Assign** button.
  In the dialog box that opens select an assignee for the task and enter the note, if required.
- To assign a task to yourself, just click the **Assign to Me** button.

To start the task:

- Click the **Start Task** button.
  The incident status will change to **In progress**.

To reject the task:

- Click the **Start Task** button.
  The incident status will change to **New**.

To defer the task:

- Click the **Defer** button.
  The incident status will change to **Deferred**.

To close the task:

- Click the **Close** button.
  The incident status will change to **Closed**.

To change incident's severity:

- Click the **Change Severity** button.
  In the dialog box that opens, choose the desired new severity for the incident.

  Note: Once you have changed the incident's severity, the **Time to First Reaction** and **Time to resolution** parameters will correspondingly change for the incident.

To archive the closed task:

- Click the **Archive** button.
  In the confirmation dialog box that opens, click **Confirm**.

  Note: The archived incidents won't be displayed in the tree of incidents. The archived incidents can be viewed in the Incidents report.

SLA times

The **Time to First Reaction** and **Time to Resolution** parameters are displayed in the right part of the window.

The following icons are used to indicate the SLA times for the incident:


This icon indicates that the remaining time meets the SLA requirements.


This icon indicates that the remaining time is less than 10% to meet the SLA requirements.


This icon indicates that the SLA time has already been exceeded.


This icon indicates that the incident has been closed within the SLA time frame.

This icon indicates that the incident has been closed with SLA overdue.

5.12 Reports

TRBOnet Watch comes with a set of predefined reports and charts to help you instantly retrieve and visualize the database information of any aspect of system monitoring. By setting filters, you can adjust reports and charts to include specific channels, types of traffic, and time settings.

This section describes how to build and analyze reports and charts, and how to retrieve the required scope using filters.

- Click the **Reports** tab in the upper bar.

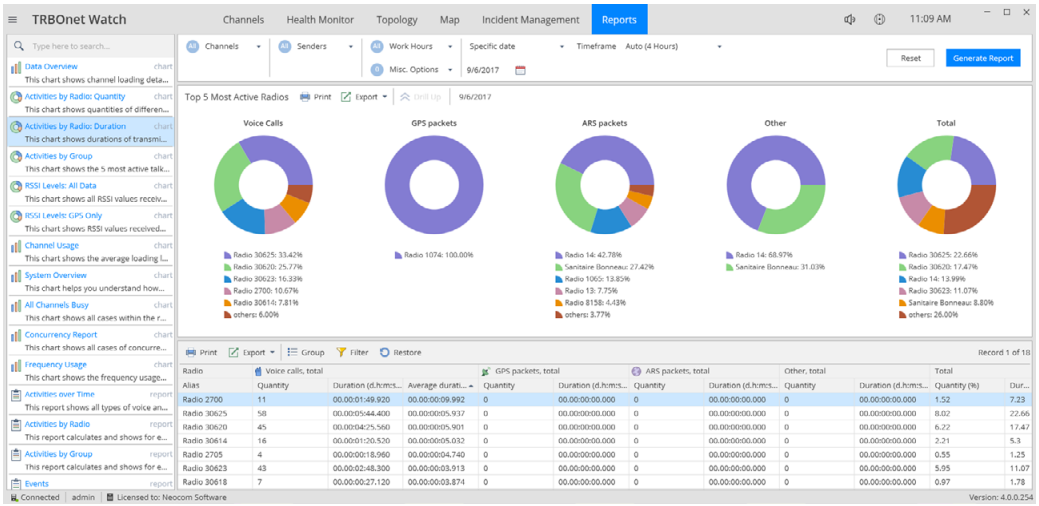


Figure 99: Charts and reports

The left pane displays the list of predefined charts and reports. You cannot add custom reports/charts or delete any report/chart from this list. Use the search bar on top of the left pane to quickly find a report/chart by its name/description.

The filter toolbar provides controls for managing filters and for building charts and reports. Learn more about filters in section 5.12.1, Filters below.

The right pane displays the generated report. The message line (yellow) displays a warning about the generated report.

For a detailed description of each report and chart, refer to Appendix A: Charts and Reports

5.12.1 Filters

The filter settings are configured in the upper toolbar on the right panel.

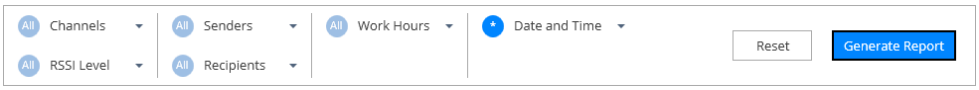


Figure 100: Reports and Charts – Filter toolbar

Channels

Click the arrow on the right and select the channels whose traffic will be included in the report/charts.

RSSI Level

Click the arrow on the right and choose of the following items:

- **All**
  Choose this item to load data with all available RSSI signal levels.
- **Show data with RSSI level lower than**
  Choose this item to load only data with the RSSI signal level lower than the specified value, in dBm.
- **Show data with RSSI level from ... to ...**
  Choose this item to load only data where the RSSI signal level falls within the specified range, in dBm.

Senders / Recipients

Click the arrow on the right and choose one of the following options:

- **All**
- **Specified**
  Enter the ID of the radio.
  Here you can also enter multiple radios. Just separate each ID by a comma, or enter the range, like: 12, 35, 105-111, 249.
- **Range**
  Enter the **From** and **To** values to define the range of radio IDs.
- **By mask**
  To specify a mask, use digits and the following wildcards:
  - % to replace any number of digits in the radio ID
  - _ (underscore) to replace one digit in the radio ID

  For instance, enter the mask _12%34_6 to filter out IDs 112003406, 91263476, and others.

Work Hours

Click the arrow on the right and choose one of the work schedules:

- **24x7**
  Choose this schedule for 24x7 hours.
- **Same each day**
  Choose this schedule and set the From and To times for the schedule.
- **Vary by day**
  Choose this schedule and select specific days of the week and hours for each day.

Date and Time

Click the arrow on the right and choose one of the following options:

- **Between**
  Choose this option and select the **From**, **To**, and **Timeframe** values for the desired time period.
- **Before**
  Choose this option and select the date before which you want data to be included in the report.
- **Since**
  Choose this option and select the date since which you want to include data in the report.
- **Specific date**
  Choose this option and select the date and the **Timeframe** value.
- **Predefined values**
  Choose this option, then click the arrow on the right of the box below and choose the data collection time period (last x minutes/hours, today, yesterday, etc.).

5.12.2 Drilling down in Charts

If the mouse is pointed to a section of a pie or bar chart and that section changes to a different pattern (for example, striped), then clicking on this section will open a new chart with additional details about the pointed section.

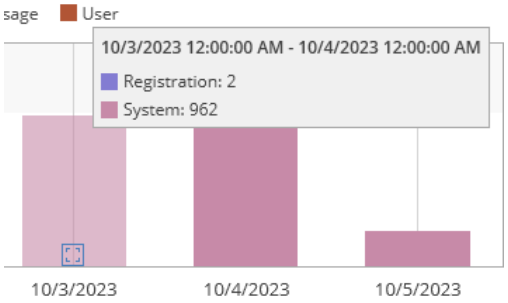


Figure 101: Drill-down in a bar chart

In a line chart, if a pointed section shows the frame with a "drill down" button ( ), click the line within the frame to drill down into the highlighted section.

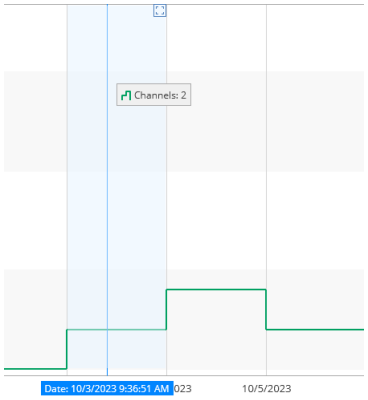


Figure 102: Drill-down in a line chart

Or, click the "drill down" button and select the preferred timeframe of the new chart on the context menu.

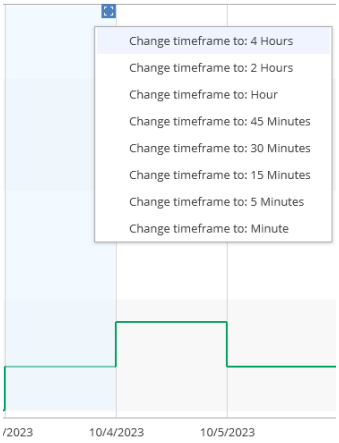


Figure 103: Drill-down with the preferred timeframe

The time axis's scale in the new chart equals to the length of the clicked (selected) timeframe.

Or, if you click the line rather than the "drill down" button, the new timeframe will be one scale smaller than the clicked timeframe.

Note: The timeframes are ranged as follows: Week, Day, 4 Hours, 2 Hours, Hour, 45 Minutes, 30 Minutes, 15 Minutes, 5 Minutes, Minute.

6 TRBOnet Watch Mobile

This section describes how to install and configure TRBOnet Watch Mobile which is a software application for Android and iOS smartphones that provides important TRBOnet Watch information.

6.1 Installation

The latest version of the TRBOnet Watch Mobile 4.0+ software application is available for download on the Google Play Store or the Apple App Store.

To install TRBOnet Watch Mobile:

1. Visit Google Play Store or Apple App Store from your mobile device.
2. Tap the TRBOnet Watch Mobile 4.0+ **Install** button.

6.2 Connection to TRBOnet Watch Server

On the login page, make sure the connection profile and credentials are correct, and tap **Connect**.

Note: If the connection cannot be established, make sure that your mobile device is connected to the network.

6.2.1 Adding Connection Profile

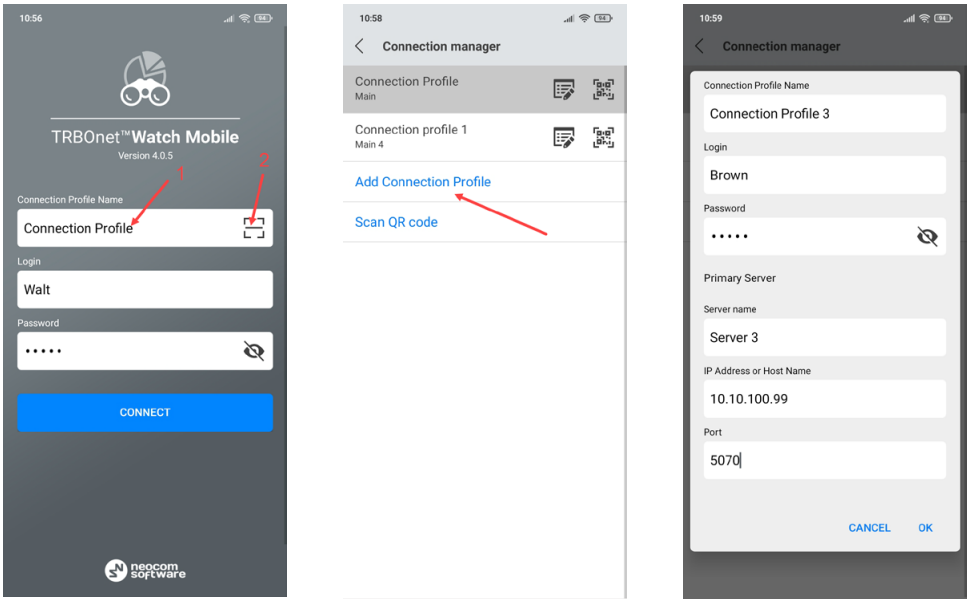


Figure 104: TRBOnet Watch Mobile - Adding a connection profile

- Tap on the **Connection Profile Name** (1).
- In the **Connection Manager** page:
  - Tap **Add Connection Profile**, and in the box that pops up, enter the following information:

- **Connection Profile Name**
  Enter the name of the profile.
- **Login**: The login for your TRBOnet Watch Mobile application. See also section 5.5.1, Access Control.
- **Password**: The password for your TRBOnet Watch Mobile application.

Note: The connection settings in the figure serve as an example. Contact your administrator to get the actual connection settings.

Primary Server

- **Server Name**
  Enter the name of the server.
- **IP Address or Host Name**: The IP address or the host name of the TRBOnet Mobile Gateway.
- **Port**: The local port of the TRBOnet Mobile Gateway (by default, 5070, see section 4.9, Mobile Gateways).
- Tap **OK**.

Or, to add a connection profile with the QR code:

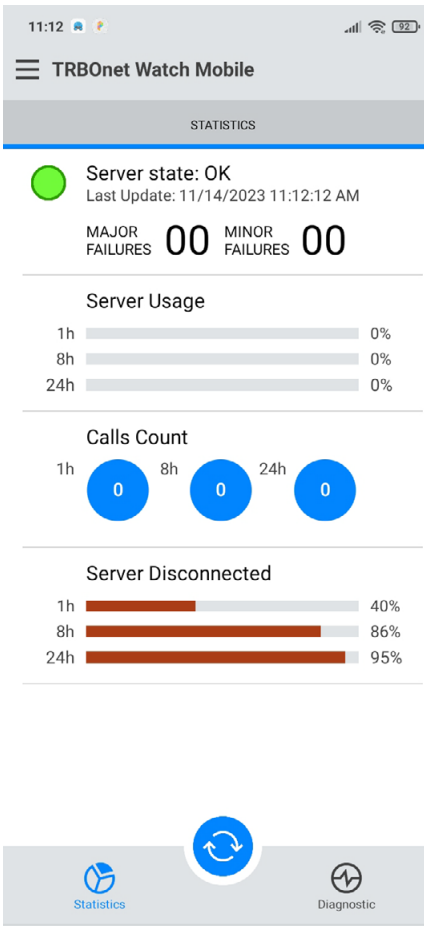
- Tap the button on the right (2).
- While in the **Scan QR code** page,
  - Point the camera at the QR code and wait for the QR code to scan.
    As a result, the corresponding connection profile will be added to the list of connection profiles.

6.3 Operation

Once you have connected to TRBOnet Watch Server, you'll see the following screens.

6.3.1 Statistics

On the **Statistics** screen, you will see the following information:



- **Server state**
  Displays the state of the radio systems connected to TRBOnet Watch Server. If there are any failures, their number and severity will be displayed.
- **Server Usage**
  Displays the statistics for busy channels in the radio systems during the specified periods (1 h, 8 h, and 24 h), in percent.
- **Calls Count**
  Displays the total number of voice calls made over the radio systems during the specified periods (1 h, 8 h, and 24 h), in amount.
- **Server Disconnected**
  Displays the statistics for disconnected channels in the radio systems during the specified periods (1 h, 8 h, and 24 h), in percent.

Figure 105: TRBOnet Watch Mobile - Statistics

6.3.2 Diagnostics

On the **Diagnostics** screen, you will see a list of radio systems connected to TRBOnet Watch Server.

6.3.2.1 Repeater

- Tap the desired system and then tap the repeater to be diagnosed.

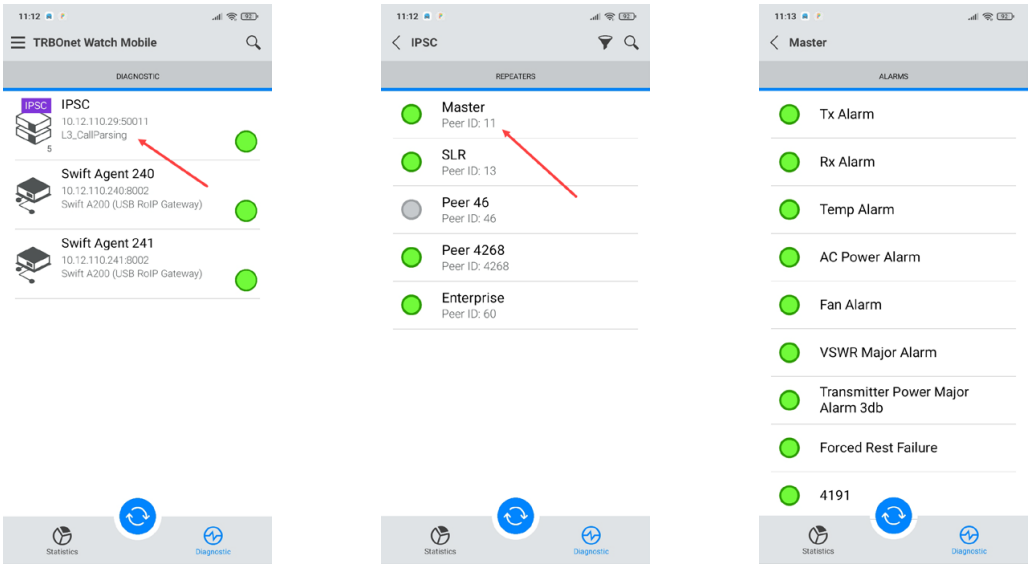


Figure 106: TRBOnet Watch Mobile – Repeater diagnostics

For the meaning of alarm icons, see section 5.8.2.1, Alarm icons (page 79).

6.3.2.2 RoIP gateway

If you tap on a hardware RoIP gateway (TRBOnet Swift Agent), you will monitor the statuses of its sensors (temperature and fans speed) and input/output pins in real time.

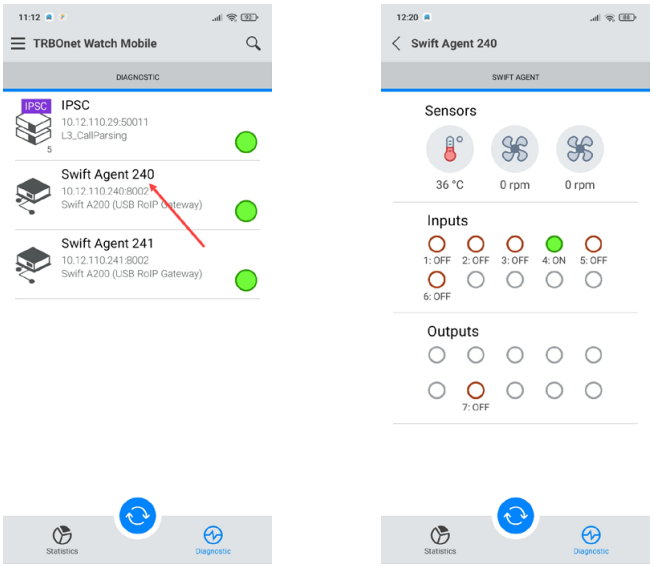


Figure 107: TRBOnet Watch Mobile – RoIP gateway diagnostics

6.3.3 Push notifications

The app system push shows the status of the connected TRBOnet Watch Server. If you tap on this notification, the running TRBOnet Watch Mobile app will open in the foreground. Or tap the Close button to close the app.

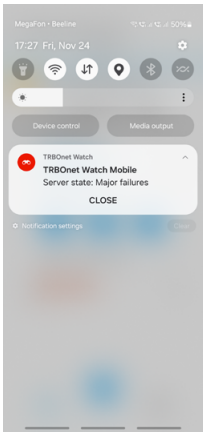


Figure 108: TRBOnet Watch Mobile – App system push notification

The TRBOnet Watch Mobile app can also receive push notifications about incidents and alarms occurring on the current and previously connected TRBOnet Watch Servers. A push notification consists of the following elements: connection profile name, message text, and a corresponding icon (see section 5.8.2.1, Alarm icons). There can be three types of notifications: Informational notification, Major failures notification, and Minor failures notification.

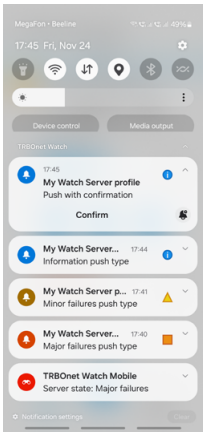


Figure 109: TRBOnet Watch Mobile – Push notifications

Notifications may also contain a Confirm button if there is a need to confirm the receipt of the push notification. If you tap on the Confirm button (or just on the notification area), the app will open and connect to the corresponding TRBOnet Watch Server. A confirmation request will be sent to the server and, as a result, you will get a successful delivery notification.

6.3.4 Settings

To configure your TRBOnet Watch Mobile application, tap the **Menu** button and then tap **Settings**. Scroll the **Settings** page and tap the option that you need to configure. Tap the **Back** button on the **Settings** page to save the settings and leave the page. The updated settings apply immediately.

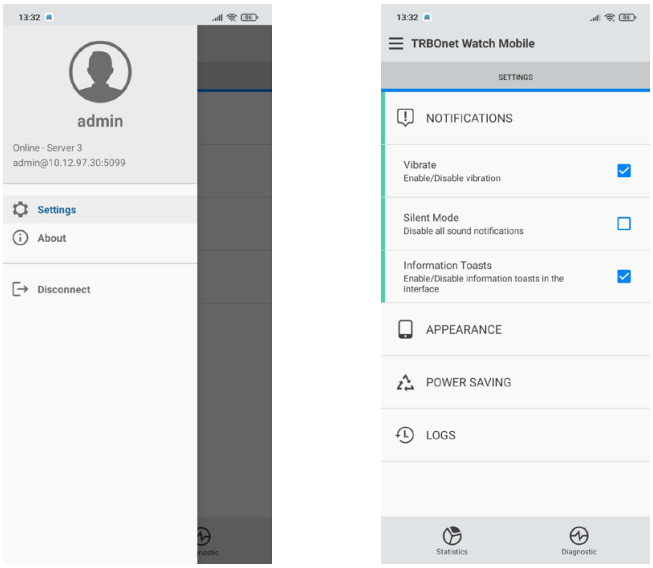


Figure 110: TRBOnet Watch Mobile – Settings

6.3.4.1 Notifications

- **Vibrate**
  Select this option to enable vibration for notifications, PTT button, etc.
- **Silent Mode**
  Select this option to disable all sound notifications.
- **Information Toasts**
  Select this option to display information toasts in the app.

6.3.4.2 Appearance

- **Language**
  Tap to choose the application language.
- **Show on Lock Screen**
  Select this option to show the app on the lock screen.

6.3.4.3 Power Saving

- **Background Mode**
  Choose one of the modes for running the app in the background:
  - **Full-time work**
    The service will work constantly until you manually disconnect it.
  - **Stops when closed in running apps list**
    The service will be stopped when you close the app from the Running Apps list.

- **Stops when minimized**
  The service will be stopped when you minimize the app.

- **Screen brightness**
  Select this option to decrease the screen brightness to a pre-defined value.

6.3.4.4 Logs

- **Incoming messages**
  Select this option to include incoming messages in the log file.
- **Outgoing messages**
  Select this option to include outgoing messages in the log file.
- **System info messages**
  Select this option to include Info messages in the log file.
- **Error messages**
  Select this option to include received error messages in the log file.
- **Send Logs**
  Tap this link to send the log file to TRBOnet Server.

Appendix A: Charts and Reports

A.1 Charts

This section describes all the predefined charts that TRBOnet Watch can generate. Presented below are the detailed descriptions of all the charts, including their goals, required filter settings, chart settings, and supported features.

A.1.1 Data Overview

The **Data Overview** charts summarize the workload of the specified channel(s) and displays traffic in these channels sorted by type.

Table 17: Data Overview charts – filter settings

Setting	Description
Channels	The channels whose traffic is shown in the charts.
RSSI Level	The RSSI signal levels that will be considered when building the charts.
Work Hours	The time interval(s) within the reported time that is used in the charts.
Date and Time	The reported time and the timeframe.

A.1.1.1 Messages by Type

The **Messages by Type** pie chart shows the percentage of each type of traffic in the monitored channel(s) during the reported time. The traffic in all monitored channels adds up to 100%.

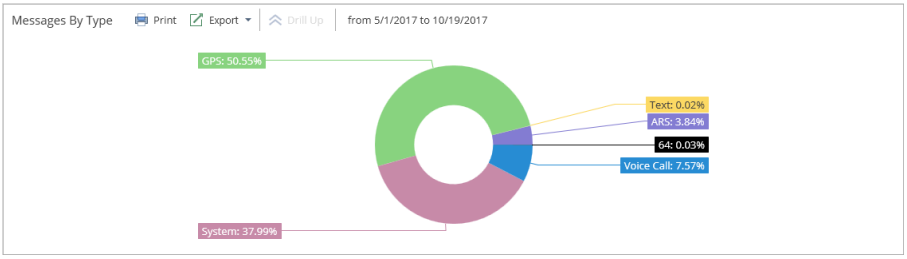


Figure 111: Messages by Type chart

- The reported time is displayed on the chart's toolbar.
- The colored sectors indicate the amount of each type of traffic.
- The legend shows the color, the type of traffic, and the percentage of this type of traffic.

A.1.1.2 Channel Load

The Loading Level of the Channels line chart shows the workload (%) of the selected channel(s) during the reported time.

The number of channels affects the layout of the chart:

- For a MOTOTRBO IPSC system, two charts (Slot 1 and Slot 2) are displayed.
- If a single IP gateway or multiple systems are selected, the chart calculates and displays the average workload for all channels.

Note: To get the individual workload of each channel in a multi-channel configuration, use the Channels Usage chart.

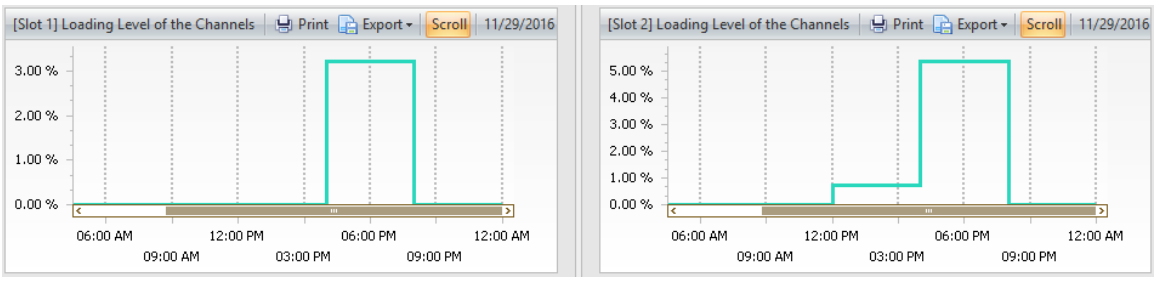


Figure 112: The loading level in the time slots of a MOTOTRBO IPSC system

- The X-axis shows the reported time divided into timeframes. These time settings are displayed on the chart's toolbar next to the **Scroll** button.
- The Y-axis shows the workload (%) of the selected channel(s). The workload is calculated in each timeframe as the total time when the channels were loaded, divided by the total time when they were connected.
- The color of the line indicates the connection status of the channel(s). A red line indicates that all reported channels were disconnected during the entire timeframe. If any channel was connected even for a minimum time interval within the timeframe, the line is blue.

Note: A channel is disconnected if the repeater is not connected to TRBOnet Watch over IP or if the IP gateway is not connected to a radio.

To drill down into a particular timeframe, click on the blue line in that timeframe. You cannot drill down into a timeframe where the line is red ("no connection").

A.1.2 Activities by Radio: Quantity

The **Activities by Radio: Quantity** charts show the quantities of different types of traffic produced by the most active radios on the specified channels during the reported time.

Table 18: Activities by Radio: Quantity charts – filter settings

Setting	Description
Channels	The channels whose traffic is included in the charts.
RSSI Level	The RSSI signal levels that will be considered when building the charts.
Senders	The radio ID whose outgoing traffic is included in the charts.
Work Hours	The time interval(s) within the reported time to be included in the charts.

Setting	Description
Date and Time	The reported time and the timeframe.

A.1.2.1 Top 5 Most Active Radios

The **Top 5 Most Active Radios** pie charts show information about the five most active radios that are sending the following types of traffic – voice, GPS, ARS, other types, and a total of all types (summary). Each pie chart shows the percentage of traffic generated by each radio in the monitored channel(s) within the reported time.

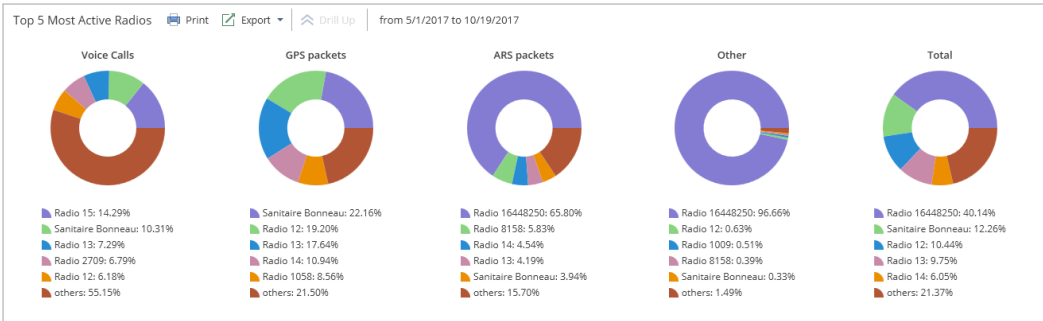


Figure 113: The percentage of call sessions initiated by the 5 most active radios

- In each chart, the total amount of all call sessions made by all active radios is 100%.
- Each radio is presented by a sector of a different color.
- The legend indicates the color and the radio ID, and the percentage of call sessions of a given type initiated by this radio.
- The reported time is displayed on the chart's toolbar.

To drill down into voice and data activity of a particular radio, click the respective sector in any chart.

A.1.2.2 Activity by Radio

The **Activity by Radio** list (located below the pie charts) shows in a tabular format the number and duration of call sessions (voice, GPS, ARS, all other, total) made by each top five active radio in the reported time.

Table 19: Activity by Radio list - fields

Field (level1)	Field (level 2)	Description
Radio	**ID**	The radio ID of the top five active radios.
Voice calls, total	**Quantity**	The number of voice calls made by the radio in the reported time.
	Duration	The duration of all voice calls initiated by the radio in the reported time. Format: dd.hh:mm:ss.ms

Field (level1)	Field (level 2)	Description
	Average duration	The average duration of a voice call made by the radio. Format: dd.hh:mm:ss.ms
GPS packets, total	**Quantity**	The number of GPS calls made by the radio in the reported time.
	Duration	The total duration of GPS calls made by the radio in the reported time. Format: dd.hh:mm:ss.ms
ARS packets, total	**Quantity**	The number of ARS transmissions made by the radio in the reported time.
	Duration	The total duration of ARS transmissions made by the radio in the reported time. Format: dd.hh:mm:ss.ms
Other, total	**Quantity**	The number of calls other than voice, GPS, and ARS, made by the radio in the reported time.
	Duration	The total duration of calls other than voice, GPS, and ARS, made by the radio in the reported time. Format: dd.hh:mm:ss.ms
Total	**Quantity (%)**	The total amount of all traffic (%) generated by the radio on the selected channel(s) during the reported time. Traffic generated by all most active radios makes 100%.
	Duration (%)	The total duration of all calls made by the radio in the reported time.

To drill down into details about a particular radio, click the respective line in the list. Two charts will be displayed for that particular radio: **Voice Activity for radio** and **Data Activity for radio**.

A.1.2.3 Voice Activity for Radio

The **Voice Activity for Radio** chart shows the number of Group calls, Private calls, and Broadcast (All) calls made by the radio in each timeframe of the reported time.

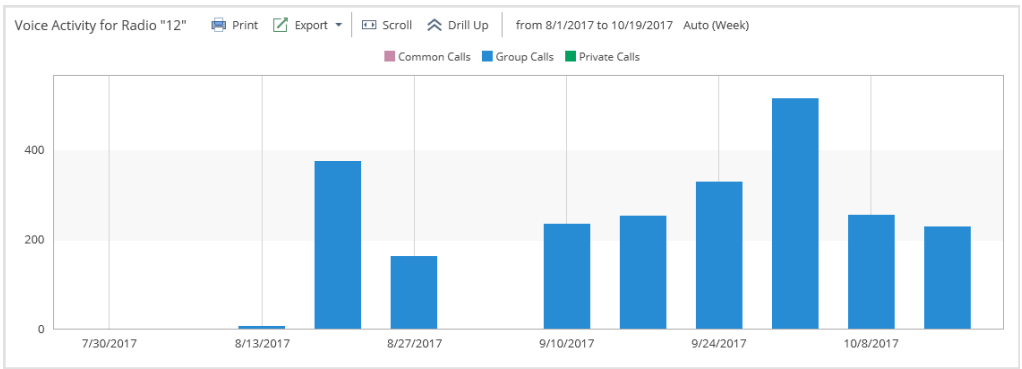


Figure 114: Voice activity of "radio 102"

- The legend indicates the color for each voice call type.
- The X-axis shows the reported time divided into timeframes.
- The Y-axis shows the number of voice calls.
- The height of each bar indicates the total number of calls made in the timeframe. Bars may include sections of different colors, indicating different call types made by the radio.
- If the cursor points on a bar, a pop-up tip will show the call details (the timeframe, the call type, the number of calls, and their total duration).

To drill down into a particular timeframe, click the respective bar. If the bar has sections of different color, click any section. To define the timeframe of the new chart to which you drill down, point on the bar and click the arrow. Click the preferred timeframe on the context menu.

A.1.2.4 Data Activity for Radio

The **Data Activity for Radio** chart shows the number of data calls of different types made by the radio in each timeframe of the reported time.

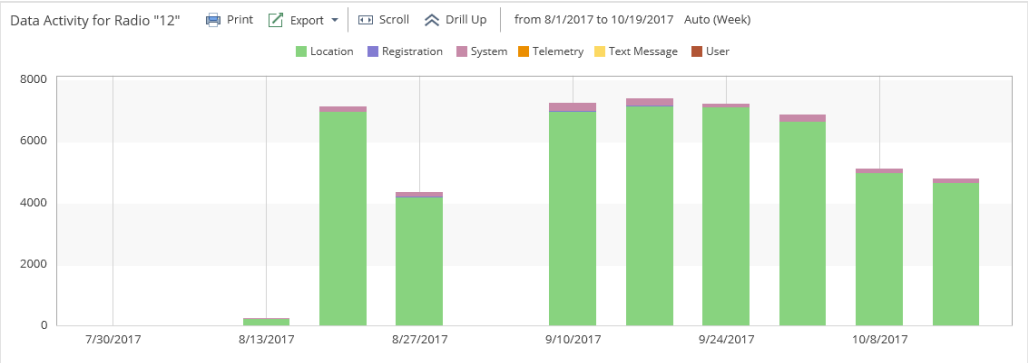


Figure 115: Data activity of "radio 102"

- The legend indicates the color for each data call type.
- The X-axis shows the reported time divided into timeframes.
- The Y-axis shows the number of data calls.
- The height of each bar indicates the total number of data calls made within the timeframe. Bars may include sections of different colors, indicating different call types made by the radio.
- If the cursor points on a bar, a pop-up tip will show the call details (the timeframe, the data call type, the number of calls and their total duration).

To drill down into a particular timeframe, click the respective bar. If the bar has sections of different color, click any section. To define the timeframe of the new chart to which you drill down, point the bar and click the arrow. Click the preferred timeframe on the context menu.

A.1.3 Activities by Radio: Duration

The **Activities by Radio: Duration** charts show how long the specified channels were busy with traffic from each of the five most active radios.

The filter settings and the included charts are similar to the ones described in section A.1.2, Activities by Radio: Quantity (page 111). The major difference is that the **Activities by Radio: Duration** charts show the duration of call sessions rather than their quantity. The **Activity by Radio** list is completely identical to the one included in the **Activities by Radio: Quantity** charts.

A.1.4 Activities by Group

The **Activities by Group** charts show the traffic of the most active talk groups in the selected channels during the reported time.

Table 20: Activities by Group chart – filter settings

Setting	Description
Channels	The channels whose traffic is included in the charts.
RSSI Level	The RSSI signal levels that will be considered when building the charts.
Work Hours	The time interval(s) within the reported time to be included in the charts.
Date and Time	The reported time and the timeframe.

A.1.4.1 Top 5 Most Active Groups

The **Top 5 Most Active Groups** pie chart shows the percentage of voice traffic generated by each of the most active talk groups on the selected channel(s) during the reported time. Traffic generated by all talk groups totals 100%.

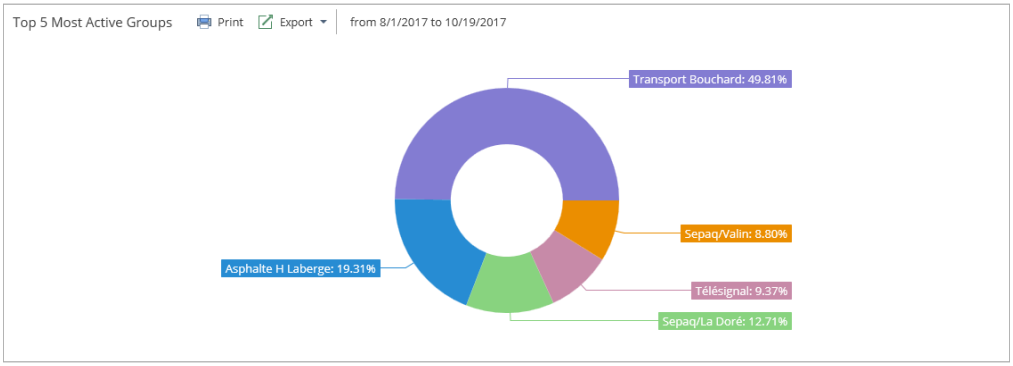


Figure 116: The percentage of traffic generated by the five most active groups

- Each talk group is represented by a sector of a different color.
- The legend indicates the color of the talk group, the talk group name, and the percentage of traffic generated in the talk group.
- The reported time is displayed on the chart's toolbar.

A.1.4.2 Group Activity

The **Group's Activity** list located below the pie chart shows the number and duration of group calls on each of the five most active talk groups during the reported time. The list also shows the share (%) of each talk group in the voice traffic generated by all of the most active groups.

Table 21: Group's Activity list - fields

Field (level1)	Field (level 2)	Description
Group	**ID**	The talk group number.
Voice calls	**Quantity**	The number of voice calls made by the talk group in the reported time.
	Duration (d.h:m:s.ms)	The duration of all voice calls made by the talk group during the reported time.
	Average duration (d.h:m:s.ms)	The average duration of a voice call made by the talk group.
Quantity	**%**	The percentage of voice traffic (%) generated by the talk group during the reported time. Traffic generated by all talk groups makes 100%.

A.1.5 RSSI Levels: All Data

The **RSSI Levels: All Data** charts show the quality of voice and data calls in the selected channels based on the signal strength. Calls with the measured signal strength are evaluated to one of the preconfigured RSSI levels and displayed in the charts with a particular color.

Table 22: RSSI Levels: All Data chart – filter settings

Setting	Description
Channels	The channels whose traffic is included in the charts.
RSSI Level	The RSSI signal levels that will be considered when building the charts.
Session Types	The types of traffic such as Voice, Data, Telemetry and other and, optionally, the types of calls included in the charts.
Recipients	The radio ID whose incoming traffic is included in the charts.
Work Hours	The time interval(s) within the reported time to be included in the charts.
Date and Time	The reported time and the timeframe.

Note: The **RSSI Levels: All Data** charts require at least 10 calls with a measurable signal strength. Otherwise, the "Data not found" message will be displayed.

A.1.5.1 RSSI by Thresholds

The **RSSI by Thresholds** pie chart shows the percentage of calls with different RSSI levels on the selected channels within the reported time.

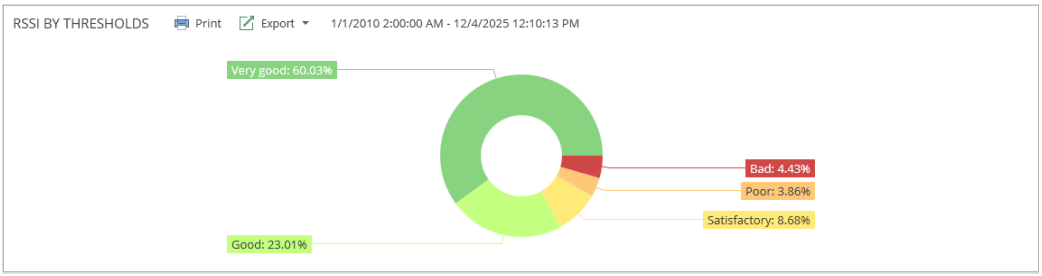


Figure 117: The amount of traffic per RSSI level band

- The colored sectors indicate calls at different RSSI levels.

  You can also click on a sector in the chart and see the filtered report on that RSSI level.

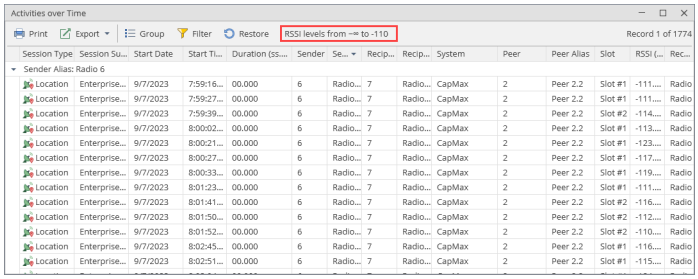


Figure 118: The filtered report on a selected RSSI level

- The legend indicates the color, the name of the RSSI level, and the percentage of voice and data calls with this RSSI level.

A.1.5.2 Relative RSSI Frequency by Thresholds

The **Relative RSSI Frequency by Thresholds** area chart shows the distribution of calls by RSSI levels in the selected channels(s) during the reported time.

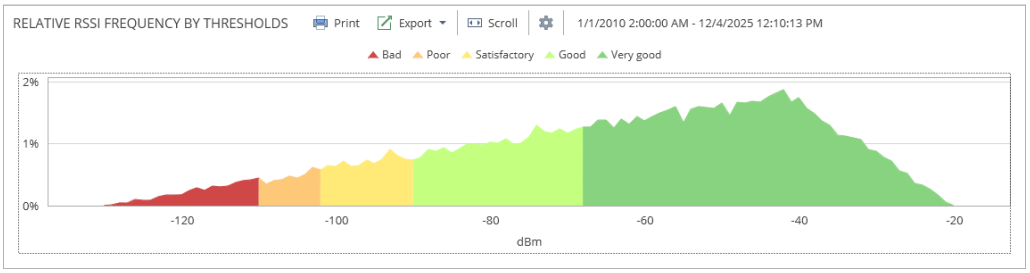


Figure 119: A MOTOTRBO IPSC system traffic ranged by RSSI level thresholds

- The X-axis shows the RSSI scale (dBm).
- The Y-axis shows the percentage of calls with the given RSSI level. All calls with the measured RSSI on the selected channels during the reported time add up to 100%.

- The color indicates a particular RSSI level. The legend indicates the colors of all RSSI levels. Click the ⚙ button to change the RSSI color scheme (see section 5.5.6, RSSI Ranges).

A.1.6 RSSI Levels: GPS Only

The **RSSI Levels: GPS Only** charts show the quality of GPS calls based on the signal strength. GPS calls with the measured signal strength are evaluated to one of the preconfigured RSSI levels and displayed in the charts with a particular color.

The displayed charts are identical to the **RSSI Levels: All Data** charts, except the traffic analyzed and displayed in the **RSSI Levels: GPS Only** charts is restricted to GPS calls only.

A.1.7 Channel Usage

The **Channel Usage** charts show the average loading level and individual levels for all selected channels within the reported time.

Table 23: Channels Usage charts – filter settings

Setting	Description
Channels	The channels whose traffic is included in the charts.
Work Hours	The time interval(s) within the reported time to be included in the charts.
Date and Time	The reported time and the timeframe.

A.1.7.1 Average and Individual Loading Levels of the Channels

The **Average and Individual Loading Levels** of the Channels line chart shows the average loading level of all selected channels during the reported time. The individual loading levels of all channels are displayed below as line charts.



Figure 120: Average and Individual Loading Levels of the Channels chart

- The X-axis shows the reported time divided into timeframes. The time settings are displayed on the chart's toolbar next to the **Scroll** button.

- The Y-axis shows the workload (%) of all selected channel(s). The workload is calculated in each timeframe as the total time when the channels were loaded, divided by the total time when they were connected.
- The color of the line indicates the connection status of the channel(s). A red line indicates that all reported channels were disconnected during the entire timeframe. If a channel was connected even for a short time interval within the timeframe, the line is blue.

Note: A channel is disconnected if the repeater is not connected to TRBOnet Watch over IP or if the IP gateway is not connected to a radio.

To drill down into a particular timeframe, click the blue line in that timeframe. You cannot drill down into a timeframe where the line is red ("no connection"). To define the timeframe of the new chart to which you drill down, point to the line and click the arrow. Point to the preferred timeframe on the context menu.

A.1.8 System Overview

The **System Overview** chart helps you understand how busy your system was for a selected period, from a few minutes to a year or even more. You can easily spot peak times when the system was used at its full capacity, which means that the available radio system might not be sufficient to handle all calls. The graph shows information about the number of channels that were disconnected or busy at any moment within the selected period, in other words, the number of channels that were not available for voice or data traffic.

The bar charts reflect the number of channels that were disconnected or busy, thus being unavailable for radio communication. The color saturation gives you an idea about the relative duration of time when this number of channels were disconnected (red) or busy (blue)- the darker the shade, the longer the period.

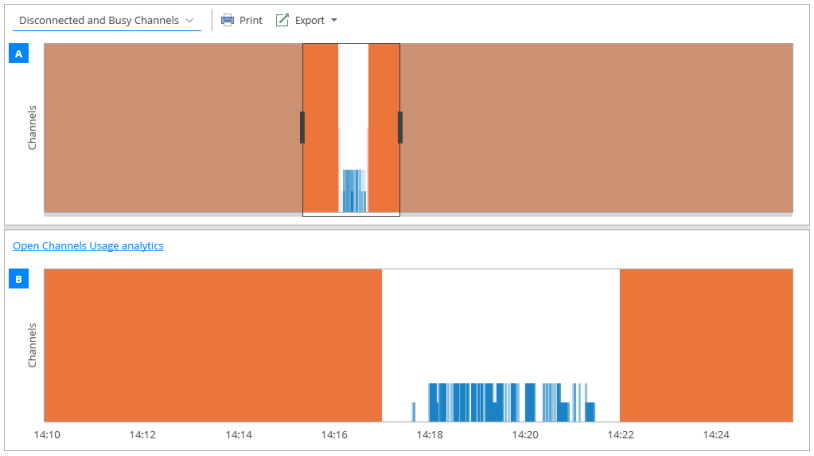


Figure 121 System Overview charts

Table 24: System Overview charts – filter settings

Setting	Description
Channels	The channels to be included in the charts. You need to indicate at least two channels for this type of analysis.
Work Hours	The time interval(s) within the reported time to be included in the charts.
Date and Time	The reported time and the timeframe.

Once you have generated the report, you will see two charts below: A and B. Chart A represents the whole time period specified in the chart filter. Chart B represents the time period selected in Chart A. To change a selection in a chart, drag a new selection and click on it. Clicking on a selection in chart B will open Chart C, and so on (D, E, etc.). As soon as you reach the most detailed time frame, you won't be able to make further selections in the chart. In this case, the **Open Detailed View** button will become active in the chart's toolbar.

A.1.8.1 Detailed View

The **Detailed View** can be used by an experienced user to perform a more detailed analysis of the channel states at a 1:1 timescale.

- Click the **Open Detailed View** link in the last, most detailed chart.

  As a result, the **Detailed View** window will open.

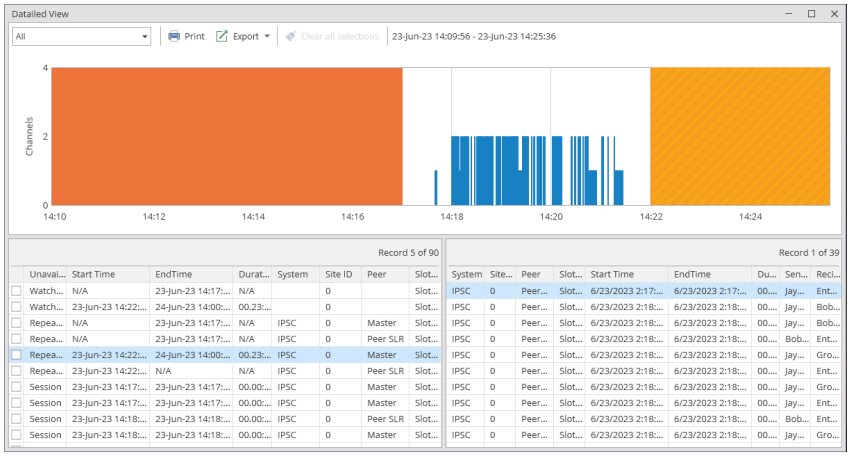


Figure 122: Detailed View window

- Make a selection or multiple selections (by clicking/dragging) in the upper chart.

  The collective selection in the chart will be represented in the **Channel states** table (information on the sessions, such as start/end times, duration, etc.). If you select a record or multiple records in the **Channel states** table, the **Calls** table will represent the calls (start/end times, duration, sender, recipient, session type, etc.) occurred within the selected session(s).

The contents of both tables can also be printed and exported to PNG bitmaps.

A.1.9 All Channels Busy

The **All Channels Busy** charts show all cases within the reported time when all selected channels were unavailable for radio users longer than the specified threshold value.

Table 25: All Channels Busy charts – filter settings

Setting	Description
Channels	The channels to be included in the charts. You need to indicate at least two channels for this type of analysis.
Threshold: Duration	The minimum duration (seconds) of an All Channels Busy event to be included in the charts. If set to 0, All Channels Busy events with any duration are included.
Threshold: Level	The minimum number of channels unavailable simultaneously that make an All Channels Busy event.
Work Hours	The time interval(s) within the reported time to be included in the charts.
Date and Time	The reported time and the timeframe.

A.1.9.1 Number of All Channels Busy

The **Number of All Channels Busy** chart is a sum of All Channels Busy events detected in each timeframe of the reported time. An event is added to this sum if the channels (in an amount not less than specified in the **Threshold: Level** filter setting) remain unavailable during the time specified by the **Threshold: Duration** filter setting, or longer.

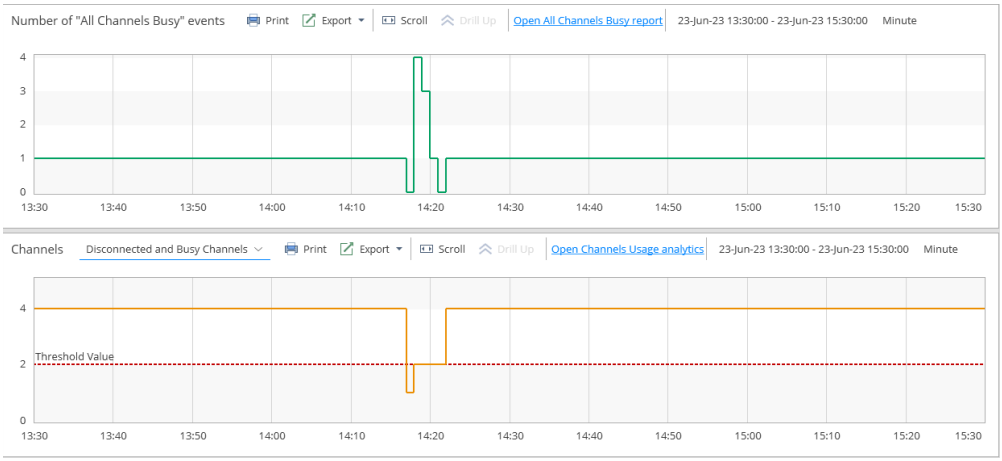


Figure 123: Number of All Channels Busy chart

- The X-axis shows the reported time divided into timeframes. The time settings are displayed on the chart's toolbar next to the **Scroll** button.

- The Y-axis shows the number of All Channels Busy events in each timeframe.
- If pointed to with the mouse cursor, a timeframe with All Channel Bus events displays a tooltip with the timestamps of the frame, the number of calculated All Channels Busy events, and the total duration of all calculated events.
- If an event lasts through several timeframes, it will be added to in each timeframe as an independent event.

To drill down into a particular timeframe, click on the blue line in that timeframe. You cannot drill down into a timeframe where the line lies on the X-axis ("no All Channel Busy events"). To define the timeframe of the new chart to which you drill down, point to the line and click the arrow. Click the preferred timeframe on the context menu.

To learn the details about the All Channel Busy events displayed in the chart, build the All Channels Busy report by clicking the **Go to All Channels Busy** button on the toolbar above the chart. To understand what caused an All Channels Busy event, build the Event Viewer report.

A.1.9.2 Channels

The **Channels** chart displays the number of disconnected and/or busy channels in each timeframe of the reported time. The line chart is built for all selected channels. When building the chart, the threshold filter settings are not considered. The **Threshold: Level** is displayed in the chart as a dotted line.

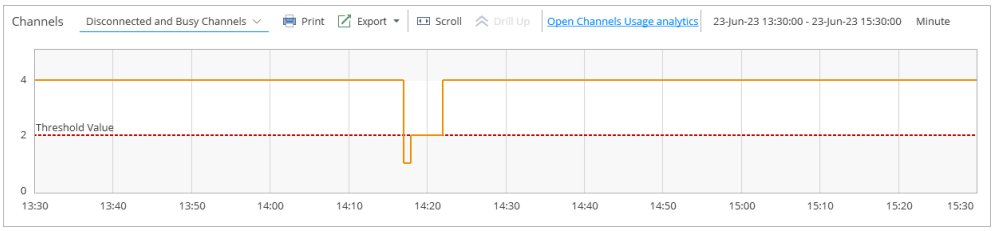


Figure 124: Channels chart (Disconnected and Busy Channels mode)

- The X-axis shows the reported time divided into timeframes. The time settings are displayed on the chart's toolbar next to the **Scroll** button.
- The Y-axis shows the number disconnected and/or busy channels within each timeframe.
- The **Views** button opens the menu where you can select the preferred view mode. The name of the selected mode appears near the Y-axis.
  - In the **Disconnected Channels** mode, the red line in each timeframe is the number of channels that were disconnected (not necessarily all together) for any time within the timeframe.
  - In the **Busy Channels** mode, the green line in each timeframe is the number of channels that were busy (simultaneously or not) for any time during the timeframe.

- In the **Disconnected and Busy Channels** mode, the yellow line in each timeframe is the number of channels that were unavailable (disconnected or busy) for the radios for any time during the timeframe.

To drill down into a particular timeframe, click on the line in that timeframe. To choose the timeframe of the new chart to which you drill down, point to the line and click on the arrow. Click the preferred timeframe on the context menu.

To learn the details about the usage of the selected channels, build the Channels Usage charts by clicking the **Go to Channels Usage Analytics** button on the toolbar above the chart.

A.1.10 Concurrency Report

The **Concurrency Report** charts show all cases of concurrent usage of the disconnected and/or busy channels over the reported time range.

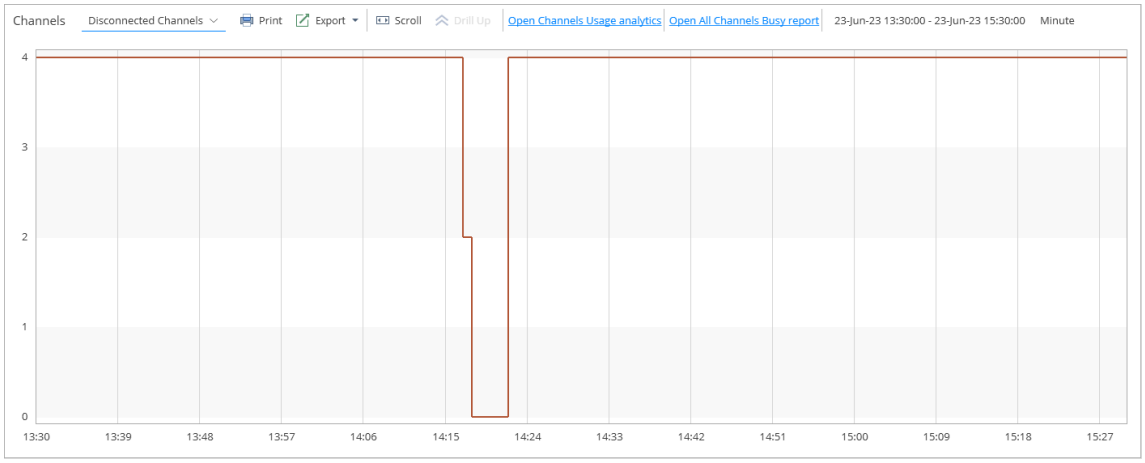


Figure 125: Concurrency Report chart (Disconnected and Busy Channels mode)

- The X-axis shows the specified time range. The time settings are displayed on the chart's toolbar next to the **Export** button.
- The Y-axis shows the total number of simultaneously disconnected and/or busy channels.
  The total number of simultaneously disconnected and/or busy channels is computed at each timepoint. The obtained function is then divided into time segments of a length equal to the specified timeframe. Note that for each time segment, a maximum number of the simultaneously used channels is obtained. Also note that for a series of disconnected and busy channels, the maximum number on each time segment is obtained after totaling the series of disconnected and busy channels.
- The **Views** button opens the menu where you can select the preferred view mode. The name of the selected mode appears along the Y-axis.
  - In the **Disconnected Channels** mode, the red line in each timeframe is the number of channels that were disconnected for any time within the timeframe.

- In the **Busy Channels** mode, the green line in each timeframe is the number of channels that were simultaneously busy for any time during the timeframe.
- In the **Disconnected and Busy Channels** mode, the yellow line in each timeframe is the number of the channels that were simultaneously unavailable (disconnected or busy) for the radios for any time during the timeframe.

A.1.11 Frequency Usage

The **Frequency Usage** chart shows the frequency usage (%) of each selected peer in the reported time.

Table 26: Frequency Usage chart – filter settings

Setting	Description
Peers	Peers included in the chart.
Work Hours	The time interval(s) within the reported time to be included in the charts.
Date and Time	The reported time and the timeframe.



Figure 126: Frequency usage by two peers

Each selected peer is displayed in a separate line chart. The name of the peer is displayed near the Y-axis in each chart.

- The X-axis shows the reported time divided into timeframes. The time settings are displayed on the chart's toolbar next to the **Scroll** button.
- The Y-axis shows the frequency usage (%). The value is calculated in each timeframe as activity time divided by the time when the peer stayed connected.
- The color of the line indicates the connection status of the peer. A red line means that the peer was disconnected during the entire timeframe. If the peer was connected even for a short time within the timeframe, the line is blue.

To drill down into a particular timeframe, click the blue line in that timeframe. To choose the timeframe of the new chart to which you drill down, point to the line and click the arrow. Click the preferred timeframe on the context menu.

Note: You cannot drill down into a timeframe where the line is red ("no connection") or where the frequency usage equals to 0.00% ("no activity").

A.2 Reports

This section includes the description of each table report that can be generated in the TRBOnet Watch Console. For each report, the section describes its goal, filter settings, and included fields.

A.2.1 Activities over Time

The **Activities over Time** report shows all types of voice and data calls transmitted on the radio channels between the parties (radios and software). For each transmission, the report shows when it happened, how long the channel was busy, which peers were involved, which system channel was used, and what signal strength was detected.

Table 27: Activities over Time report – filter settings

Setting	Description
Channels	The system channels whose traffic is included in the report.
RSSI Level	The RSSI signal levels that will be considered when building the report.
Session Types	The types of traffic such as Voice, Data, Telemetry and other and, optionally, the types of calls included in the report.
Senders	The radio ID of radios whose outgoing traffic is included in the report.
Recipients	The radio ID of radios whose incoming traffic is included in the report.
Work Hours	The time intervals within the reported time to be included in the report.
Date and Time	The reported time.

Table 28: Activities over Time report – fields

Field	Description
Session Type	The type of traffic.
Session Subtype	The type of call.
Start Time	The start time of call transmission.
Duration (m:s.ms)	The duration of the call (including hang time).
Sender	The radio ID of the sender.

Field	Description
Recipient	The radio ID of the recipient (if applicable).
System	The name of the system whose channel was used to transmit the call.
Peer	In MOTOTRBO systems, the ID of the peer that repeated the call. Is set to 0 for other systems.
Slot ID	The time slot of the repeater in which the call was repeated.
RSSI (dBm)	The incoming signal strength measured in the MOTOTRBO repeater slot. Is set to "N/A" if not applicable.
Received from	The type of the call sender ("Radio" or "Site").

A.2.2 Activities by Radio

The **Activities by Radio** report calculates and shows for each radio how many voice calls and GPS and ARS messages were transmitted and how much time it took to transmit each type of traffic during the reported time. The report also summarizes all types of traffic initiated by each radio and the share (%) of each radio in the overall system traffic.

Table 29: Activities by Radio report – filter settings

Setting	Description
Channels	The system channels whose traffic is included in the report.
RSSI Level	The RSSI signal levels that will be considered when building the report.
Session Types	The types of traffic such as Voice, Data, Telemetry and other and, optionally, the types of calls included in the report.
Senders	The radio ID of radios whose outgoing traffic is included in the report.
Recipients	The radio ID of radios whose incoming traffic is included in the report.
Work Hours	The time intervals within the reported time to be included in the report.
Date and Time	The reported time.

Table 30: Activities by Radio report – fields

Field (level1)	Field (level 2)	Description
Radio	**ID**	The radio whose outgoing traffic is reported.
Voice calls, total	**Quantity**	The number of voice calls initiated by the radio during the reported time.
	Duration (d.h:m:s.ms)	The total duration of voice calls initiated by the radio.
	Average duration (d.h:m:s.ms)	The average duration of a voice call initiated by the radio.

Field (level1)	Field (level 2)	Description
GPS packets, total	**Quantity**	The number of GPS messages sent by the radio during the reported time.
	Duration (d.h:m:s.ms)	The total duration of GPS traffic initiated by the radio.
ARS packets, total	**Quantity**	The number of ARS messages sent by the radio during the reported time.
	Duration (d.h:m:s.ms)	The total duration of ARS traffic initiated by the radio.
Other, total	**Quantity**	The number of other data calls sent by the radio during the reported time.
	Duration (d.h:m:s.ms)	The total duration of other data calls initiated by the radio.
Total	**Quantity (%)**	The share of traffic (%) generated by the radio in the system during the reported time. The value is calculated for all kinds of traffic.
	Duration (%)	The total duration of calls (%) initiated by the radio in the system during the reported time.

A.2.3 Activities by Group

The **Activities by Group** report calculates and shows for each talk group how many voice calls were made during the reported time. Also, the report calculates the share (%) of each talk group in the overall voice traffic transmitted in the system.

Table 31: Activities by Group report – filter settings

Setting	Description
Channels	The system channels whose traffic is included in the report.
RSSI Level	The RSSI signal levels that will be considered when building the report.
Messages	The types of traffic such as Voice, Data, Telemetry and other and, optionally, the types of calls included in the report.
Work Hours	The time intervals within the reported time to be included in the report.
Date and Time	The reported time.

Table 32: Activities by Group report – fields

Field (level1)	Field (level 2)	Description
Group	**ID**	The talk group whose outgoing voice traffic is summarized.

Field (level1)	Field (level 2)	Description
Voice calls	**Quantity**	The number of voice calls initiated by the talk group members during the reported time.
	Duration (d.h:m:s.ms)	The total duration of voice calls initiated by the talk group members.
	Average duration (d.h:m:s.ms)	The average duration of a voice call initiated in the talk group.
Total	**%**	The share (%) of the talk group in the overall voice traffic transmitted in the system during the reported time.

A.2.4 Events

The **Events** report allows you to trace all events that occurred in particular systems during the reported time.

Table 33: Events report – filter settings

Setting	Description
Systems and peers	The list of systems and peers.
Event type	The event types to be included in the report.
Date and Time	The reported date/time.

Table 34: Events report – fields

Field	Description
System	The name of the system where the event occurred.
Timestamp	The date and time when the event occurred.
Peer ID	The system peer related to the event. Is set to "N/A" if not a peer event.
Peer Type	The type of the system peer related to the event. Options: Hardware, Software, N/A (if not a peer event or the peer is unknown).
Event Type	The type of event.
Description	The description of the event.

A.2.5 Call Interruptions

The **Call Interruptions** report shows all call interrupt events occurred in the systems during the reported time.

Note: The **Call Interruptions** reports are supported only for **IPSC** and **Capacity Plus** systems with the **Level 4: Call Parsing** monitoring level.

Table 35: Call Interruptions report – filter settings

Setting	Description
Systems	The list of system names.
Work Hours	The time intervals within the reported time to be included in the report.
Date and Time	The reported time.

Table 36: Call Interruptions report – fields

Field	Description
Event type	The type of event (Interrupt or Dekey). Note: The Interrupt type means stopping a transmission and placing one's own voice transmission on the current channel, whereas the Dekey type means stopping a transmission in order to free up the channel.
Interrupter	The radio that interrupted a voice transmission.
Source	The radio that initiated the transmission that was interrupted.
Target	The target ID of the transmission that was interrupted.
Duration	The duration of the voice transmission that was interrupted.
Timestamp	The date and time when the interrupt event occurred.
System	The name of the system where the interrupt event occurred.
Site	The site where the interrupt event occurred.
Peer ID	The system peer related to the event. Is set to "N/A" if not a peer event.
Session Type	The type of traffic that was interrupted.
Session Subtype	The subtype of the interrupted traffic.
Result	The result of the event (Success or Failure).

A.2.6 Text Messages

The **Text Messages** report shows all text messages sent by radios on the selected system channels. For each message, the report shows the sender, the recipient, the time when the message was sent, the system slot that was used, and the text.

Table 37: Text Messages report – filter settings

Setting	Description
Channels	The system channels whose traffic is included in the report.
RSSI Level	The RSSI signal levels that will be considered when building the report.
Senders	The radio ID of radios whose outgoing traffic is included in the report.
Recipients	The radio ID of radios whose incoming traffic is included in the report.
Work Hours	The time intervals within the reported time to be included in the report.

Setting	Description
Date and Time	The reported time.

Table 38: Text Messages report – fields

Field	Description
Sender	The radio ID of the sender.
Recipient	The radio ID of the recipient.
Start Time	The timestamp of the message.
System	The name of the system in which the message was sent.
Peer	The ID of the peer that repeated the text message.
Slot ID	The channel that transmitted the message.
Text	The text of the message (appears if the message can be parsed).

A.2.7 RCM Messages

The **RCM Messages** report shows Repeater Call Monitoring (RCM) messages transmitted in the selected system(s) during the reported time.

Note: MOTOTRBO systems included in this report should have the "Store Repeater Call Monitoring messages" feature enabled in the TRBOnet Watch configuration settings. For details, refer to section 5.4.1.3, Data Storage (page 37).

Table 39: RCM Messages report – filter settings

Setting	Description
Channels	The system channels whose traffic is included in the report.
Senders	The radio ID of radios whose outgoing traffic is included in the report.
Recipients	The radio ID of radios whose incoming traffic is included in the report.
RCM Messages	The RCM messages to be included in the report.
Work Hours	The time intervals within the reported time to be included in the report.
Date and Time	The reported time.

Table 40: RCM Messages report – fields

Field	Description
Session Subtype	The type of RCM. For a brief description of all RCM messages, refer to Appendix C: RCM Messages (page 143).

Field	Description
Start Time	The time when the message was sent.
Duration (m:s.ms)	The duration of the message transmission.
System	The name of the MOTOTRBO system in which the repeater sent the RCM message.
Peer	The peer ID of the repeater that sent the RCM message.
Slot ID	The time slot in which the message was transmitted.

A.2.8 All Channels Busy

The **All Channels Busy** report shows the occurrences of All Channels Busy cases in the selected channels during the reported time.

Table 41: All Channels Busy report – filter settings

Setting	Description
Channels	The system channels to be included in the report. You need to indicate at least two channels for this report.
Threshold: Duration	The minimum duration (in seconds) of an All Channels Busy event to be included in the report. If set to "0", any duration is included.
Threshold: Level	The number of channels that should be busy at the same time to report an All Channels Busy event.
Work Hours	The time intervals within the reported time to be included in the report.
Date and Time	The reported time.

Table 42: All Channels Busy report – fields

Field	Description
Radio activity while all channels are busy	Click the **Load...** value to see activity of radios in the busy channels. The selected field can show any of the following: ▪ **No activity**: No radio activity was registered in the busy channels. ▪ **Collapse**: The expanded list shows the radios whose traffic made the channels busy. The included fields are: ▪ Protocol: The type of traffic. ▪ Subprotocol: The type of call or message. ▪ Start: The start time of the transmission. ▪ Duration: The duration of the transmission (including hang time). ▪ Sender: The radio ID of the sender. ▪ Recipient: The radio ID of the recipient. ▪ System: The system that transmitted the call or message. ▪ Site: For Linked Capacity Plus systems, the site where the transmission occurred. Not relevant to other system types (set to 0). ▪ Peer: The peer ID of the repeater that transmitted the call or message.

Field	Description
	▪ Slot: The time slot that was busy.
Start Time	The date and time when all selected channels became busy.
End Time	The date and time when any selected channel became available after all of them were busy.
Duration	The total time during which the selected channels were busy. Format: DD.HH:MM:SS

A.2.9 GPS Data

The **GPS Data** report shows all GPS messages transmitted in the selected channels during the reported time.

Table 43: GPS Data report – filter settings

Setting	Description
Channels	The channels included in the report.
RSSI Level	The RSSI signal levels that will be considered when building the report.
Senders	The radio ID of radios whose outgoing traffic is included in the report.
Recipients	The radio ID of radios whose incoming traffic is included in the report.
Work Hours	The time intervals within the reported time to be included in the report.
Date and Time	The reported time.

Table 44: GPS Data report – fields

Field	Description
Session Type	GPS transmission.
Session Subtype	The type of GPS message.
Start Time	The start time of the GPS transmission.
Duration	The total time during which the repeater used the channel to transmit the GPS message. Hang time is included.
Sender	The radio ID that sent the GPS message.
Recipient	The radio ID that received the GPS message.
System	The name of the system that transmitted the GPS message.
Peer	The peer ID of the repeater that transmitted the GPS message.
Slot ID	The time slot that transmitted the GPS message.
RSSI (dBm)	The incoming signal strength detected by the repeater.
Longitude	The GPS longitude of the sender.
Latitude	The GPS latitude of the sender.

Field	Description
Radius, m	The tracking inaccuracy (in meters) of the GPS coordinates. This report includes all GPS transmissions where the tracking inaccuracy does not exceed 15 meters; records with greater inaccuracy are not included in the report.

A.2.10 Frequency Usage

The **Frequency Usage** report shows for all selected peers:

- The total time during which every peer was connected to the network, and the duration (%) of the connected state
- The total time during which every peer was active
- The percentage of the "activity" time relative to the connection time

Table 45: Frequency Usage report – filter settings

Setting	Description
Peers	The system peers included in the report.
Work Hours	The time intervals within the reported time to be included in the report.
Date and Time	The reported time and the timeframe.

Table 46: Frequency Usage report – fields

Field (level1)	Field (level 2)	Description
Timeframe		The timeframe of the report per which the activity and connection of each peer is evaluated.
State		The state of the peer in each timeframe. Values: ▪ **Activity**: The peer transmits traffic. ▪ **Connection**: The peer is connected to TRBOnet Watch over IP. A RoIP getaway is connected to the radio. Note: If the peer had no activity during the reported timeframe, the Activity status is not displayed.
<Peer ID> (<system >)	**Duration h:m:s.ms**	The total time the peer was active or connected within the timeframe.
	Duration %	The meaning depends on the state of the peer: ▪ **Connection**: The percentage of time in the timeframe when the peer was connected. ▪ **Activity**: The percentage of the connection time within the given timeframe when the peer was active.

A.2.11 Incidents

The **Incidents** report shows incidents created by Watch based on alarms that occurred in selected systems within a selected time period. You can select incident categories, processing and SLA statuses.

Table 47: Incidents report – filter settings

Setting	Description
Systems and peers	The systems and peers included in the report.
Incident categories	The categories of incidents to be included in the report.
Severity	The incident severities (Critical, High, Moderate, and/or Low) to be included in the report.
Assignee	The assignees of the incidents to be included in the report.
Status	The status(es) of the incidents to be included in the report.
SLA	The SLA statuses (In progress, Success, and/or Overdue) of the incidents to be included in the report.
Date and Time	The reported time.

Table 48: Incidents report – fields

Field	Description
Category	The incident' category.
ID	The incident's ID. Click it and see the detailed information of the incident.
Name	The incident's name.
Created	The date/time the incident was created.
Updated	The date/time the incident was last updated.
Closed	The date/time the incident was closed (if closed).
Severity	The incident's severity.
Status	The incident's status.
SLA Reaction	Shows if the ticket was reacted in time or not.
SLA Close	Shows if the ticket was reacted in time or not.
Assignee	The ticket's assignee.

A.2.12 Call Queues (Capacity Max)

This **Call Queues** report shows all queued voice and data calls in Capacity Max within a selected time period. You can select specific types of calls.

Table 49: Call Queues report – filter settings

Setting	Description
Capacity Mas systems	The Capacity Max systems included in the report.
Session Types	The session types to be included in the report.
Date and Time	The reported time and the timeframe.

Table 50: Call Queues report – fields

Field	Description
Session Type	The session type.
Session Subtype	The session subtype.
Timestamp	The date and time when the call was queued.
Time in queue	The time the call was standing in a queue.
Sender	The sender of the queued call.
Sender Alias	The alias of the sender of the queued call.
Recipient	The recipient of the queued call.
Recipient Alias	The alias of the recipient of the queued call.
System	The Capacity Max system.
Site	The site in the Capacity Max system.

A.2.13 AC Voltage

The **AC Voltage** report shows AC voltages of connected repeaters within a selected time period. You can apply filters to view voltages within a specific range.

Note: Only SLR repeaters can be used in AC Voltage reports.

Table 51: AC Voltage report – filter settings

Setting	Description
Peers	The repeaters whose voltage values will be included in the report.
AC Voltage	The voltage values (higher than, lower than, and in the range of) to be included in the report.
Date and Time	The reported time and the timeframe.

Table 52: AC Voltage report – fields

Field	Description
Timestamp	The date and time the AC voltage was measured on the repeater.
System	The system of the repeater.

Field	Description
Site	The site of the repeater.
Peer	The repeater on which the AC voltage is measured.
Peer Alias	The repeater's alias.
AC Voltage (V)	The AC voltage measured on the repeater.

A.2.14 RSSI Noise

The **RSSI Noise** report shows RSSI level values when selected radio channels are idle within a selected time period.

Table 53: RSSI Noise report – filter settings

Setting	Description
Channels	The channels included in the report.
RSSI Level	The RSSI levels (higher than, lower than, and in the range of) to be included in the report.
Date and Time	The reported time and the timeframe.

Table 54: RSSI Noise report – fields

Field	Description
Timestamp	The date and time the RSSI level was measured on the repeater's slot.
System	The system of the repeater.
Site	The site of the repeater.
Peer	The repeater.
Peer Alias	The repeater's alias.
Slot	The slot of the repeater on which the RSSI level is measured.
RSSI (dBm)	The RSSI level measured on the slot.

Appendix B: SNMP Support

B.1 MIB Files

To configure communication with the TRBOnet Watch SNMP Agent, you need to upload and install on the NMS system the following MIB files:

- *common\ns_00_INET-ADDRESS-MIB.mib*
- *common\ns_01_CISCO-SMI.mib*
- *common\ns_02_CISCO-TC.mib*
- *common\ns_03_RMON-MIB.mib*
- *common\ns_04_TOKEN-RING-RMON-MIB.mib*
- *common\ns_05_SNMP-FRAMEWORK-MIB.mib*
- *common\ns_06_RMON2-MIB.mib*
- *common\ns_07_ENTITY-MIB.mib*
- *common\ns_08_CISCO-ENTITY-ALARM-MIB.mib*
- *common\ns_09_ALARM-MIB[rfc3877].mib*
- *ns_10_NEOCOM-SMI.MIB*
- *ns_11_NEOCOM-PRODUCTS-MIB.MIB*

The latest version of MIB files can be obtained at the following URL:

https://cdn.trbonet.com/download/tools/NeocomMIBs.zip

MIBs numbered 08-09 and all references (00-07 files) are contained in the *MIB\Common* folder. The number in the file name indicates the compilation order on a remote NMS.

NEOCOM-PRODUCTS-MIB (11) describes TRBOnet Watch and determines the scope of ENTITY-MIB and CISCO-ENTITY-ALARM-MIB (08) functionality implemented in the current version of the product.

ENTITY-MIB (07) contains information for managing physical entities in the system. It also arranges the entities into a containment tree that depicts their hierarchy and relationship to each other. The MIB supports the entPhysicalTable table.

The entPhysicalTable describes each physical component (entity) in the system. The table contains an entry for the top-level entity (master repeater) and for each entity connected to the master (hardware peers, applications, and other). Each entry provides information about the entity: its name, type, vendor, and a description, and describes how the entity fits into the hierarchy of system entities.

CISCO-ENTITY-ALARM-MIB (08) provides the information about all types of alarms in the system. This information serves for the following:

- Monitoring when alarms are asserted and cleared.
- Obtaining alarm history information.

- Tracking alarm statistics and counts.
- Generating SNMP traps and syslog messages in response to alarms.

B.2 MIB Objects

TRBOnet Watch works with the MIB objects listed in the table below.

Table 55: MIB objects related to TRBOnet Watch

Object Name	Object ID	Description	MIB file
entPhysicalTable	1.3.6.1.2.1.47.1.1.1	The Physical Entity (Overall System Topology) Table. Describes each physical component (entity) in the system.	ENTITY-MIB
ceAlarmDescrMapTable	1.3.6.1.4.1.9.9.138.1.1.1	The mapping between an alarm description and a vendor type.	CISCO-ENTITY-ALARM-MIB
ceAlarmDescrTable	1.3.6.1.4.1.9.9.138.1.1.2	Alarm Description Table.	CISCO-ENTITY-ALARM-MIB
ceAlarmTable	1.3.6.1.4.1.9.9.138.1.2.5	Alarm control and status information related to the corresponding physical entity, including a list of alarms currently being asserted by that physical entity.	CISCO-ENTITY-ALARM-MIB
ceAlarmHistTable	1.3.6.1.4.1.9.9.138.1.3.3	This table contains a history of ceAlarmIndicate and ceAlarmClear traps generated by the agent.	CISCO-ENTITY-ALARM-MIB
The following objects are the notifications expected on a remote NMS if SNMP notification is enabled in the TRBOnet Watch Server configuration. For details, refer to section 4.8, SNMP Communication (page 22).			
ceAlarmAsserted	1.3.6.1.4.1.9.9.138.2.0.1	Alarm Enabled	CISCO-ENTITY-ALARM-MIB
ceAlarmCleared	1.3.6.1.4.1.9.9.138.2.0.2	Alarm Disabled	CISCO-ENTITY-ALARM-MIB

Object Name	Object ID	Description	MIB file
entConfigChange	1.3.6.1.2.1.47.2.0.1	Generated when entPhysicalTable modified	ENTITY-MIB

B.3 Alarms

An alarm contains the following information:

- Type: A unique code that identifies the alarm
- Severity: The severity of the condition causing the alarm
- Description: The information about the condition that caused the alarm

Alarm state

The alarm state indicates the current state of the condition that caused the alarm:

- Asserted: The condition currently exists.
- Cleared: The condition has been resolved.

Alarm severity

The severity of the alarm indicates the type of condition the alarm represents.

- Critical (1): A severe, service-affecting condition that requires immediate corrective action.
- Major (2): A hardware or software condition that indicates a serious disruption of service or the malfunctioning or failure of important hardware. Although less serious than a critical alarm, a major alarm requires immediate attention and response of a technician to restore or maintain system capability.
- Minor (3): A condition or problem that does not seriously affect customer service, or occurs on nonessential hardware.
- Info (4): The information message concerning the event that improves operation, or the indication of a condition that could cause a problem.

Interpreting alarm information in CISCO-ENTITY-ALARM-MIB

To determine if any alarms are currently being asserted, read the ceAlarmTable object values.

Each entry in the table contains information about the alarms currently being asserted by each physical entity. Each entry is indexed by object entPhysicalIndex (ENTITY-MIB) of the entity.

To obtain information about individual alarms, read the ceAlarmDescrSeverity and ceAlarmDescrText object values.

TRBOnet Watch Alarm Codes

Table 56: TRBOnet Watch alarm decimal codes

Alarm	Decimal code
TxAlarm	1
RxAlarm	2
Temp_Alarm	3
AC_Power_Alarm	4
FanAlarm	5
PA_EEPROM_Corruption_Type_1	6
PA_EEPROM_Corruption_Type_2	7
PA_EEPROM_Corruption_Type_3	8
Exciter_EEPROM_Corruption_Type_1	9
Exciter_EEPROM_Corruption_Type_2	10
Exciter_EEPROM_Corruption_Type_3	11
Receiver_EEPROM_Corruption_Type_1	12
Receiver_EEPROM_Corruption_Type_2	13
Receiver_EEPROM_Corruption_Type_3	14
PA_Voltage_Alarm_High	16
PA_Voltage_Minor_Alarm	17
PA_Voltage_Major_Alarm	18
VSWR_Minor_Alarm	19
VSWR_Major_Alarm	20
Transmitter_Power_Minor_Alarm_2db	21
Transmitter_Power_Minor_Alarm_3db	22
Transmitter_Power_Major_Alarm_3db	23
Interoperability_Between_Exciter_and_PA	24
Incorrect_Carrier_Frequency	25
Incorrect_Codeplug_for_MTR2000_PA	26
Reference_Incompatibility	30
Exciter_Driver_Amp_Alarm	31
Exciter_Final_Amp_Alarm	32
Volt_8_Supply_Alarm	33

Alarm	Decimal code
Volt_10_Supply_Alarm	34
RF_Power_Control_Alarm	35
PA_Gain_Alarm	36
Ext_Circulator_Temp	37
PA_Revision	38
Exciter_Revision	39
RxRevision	40
PeerDisconnected	107

B.4 Examples

The following examples demonstrate how to configure an NMS for SNMP communication with TRBOnet Watch.

Note: All examples use SNMPc Enterprise by Castle Rock Computing. For details, refer to https://www.castlerock.com/products/snmpc/.

Table 57: Examples of configuring an NMS for SNMP communication with TRBOnet Watch

To do this:	Take these steps:
Install custom MIBs in the SNMP management console	1. Copy all MIB files from the MIB folder to the *...\SNMPc Network Manager\mibfiles* folder. 2. Launch the management console. 3. On the main menu, choose **Config** and then **Mib Database**. 4. In the dialog box, click **Add** and choose all necessary files from the list. Click **OK**. 5. Click the **Compile** button to recompile the MIB database.
Add TRBOnet Watch to the list of monitored entities	1. Launch the management console. 2. On the main menu, select **Insert** and then **Map Objects** and **Device**. 3. In the dialog box, specify the IP address and the name of TRBOnet Watch. Click **OK**.
Configure SNMPv3 protocol for authentication and confidentiality	1. Launch the management console. 2. In **Root Subnet**, right-click the Watch object and select **Properties**. 3. In the dialog box, click the **Access** tab and specify the following fields. For instance, you can show the following values: ▪ **Read Access Mode**: Set to SNMP V3 Priv-DES Auth-MD5.

To do this:	Take these steps:
	▪ **Read/Write Access Mode**: Set to SNMP V3 Priv-DES Auth-MD5. ▪ **V3 Engineid**: Show the value specified in TRBOnet Watch configuration (default: 80000AD0431AF108). ▪ **V3 Auth/Prive Security Name**, **V3 Auth Passwd**, **V3 Priv Passwd**: Show the values specified in TRBOnet Watch configuration. Note: For the description of TRBOnet Watch SNMP configuration settings, refer to section 4.8, SNMP Communication (page 22). 4. Click **OK**.
Read the list of alarms from a ceAlarmList	The ceAlarmList object (ceAlarmTable, Oid: 1.3.6.1.4.1.9.9.138.1.2.5.1.3) contains alarms as 32-byte strings in hexadecimal format. Note: If no alarm is set, ceAlarmList will contain an empty string (zero length). The ordinal bits in the string specify the alarm code. For example, you get an alarm encoded in the following string: 00 00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 You see 13 bytes holding zeroes and then a byte holding information. In this byte, (08) stands for (00001000) in binary format. Bits in the byte '08' are indexed from right to left, so the position of the ordinal bit is 3. Calculate the alarm code: 13*8 (the number of 'zero' bits prior to byte '08') + 3 (00001000)= 107 Look for code 107 in Table 70 (page 140). This code indicates the PeerDisconnected alarm.

Appendix C: RCM Messages

When the system is unable to set up the call or continue the requested call, it declines the call setup request with the reason code. TRBOnet Watch Console displays such reason codes in the Channels tab and includes them in reports as RCM messages.

The following table describes all RCM messages that can be displayed in the TRBOnet Watch Console.

Table 58: RCM messages

RCM Message (Reason Code)	Failure Scenario
CALL TRANSMISSION STATUSES	
Race Condition Failure	The Call Setup request is rejected during Arbitration.
Invalid/Prohibited Call Failure	Incorrect or forbidden format.
Destination Slot Busy Failure	The destination channel is busy.
Destination Group Busy Failure	The Call Setup request is declined because the destination Group is busy on another channel. This scenario applies to setting up a new call on the rest channel in Capacity Plus/LCP systems only.
All Channels Busy Failure	The Call Setup request is declined because all the channels at the site are busy. The rest channel is busy. This scenario applies to setting up a new call on the rest channel in Capacity Plus /LCP systems only.
OTA Repeat Disabled Failure	The Call Setup request is declined because the repeater where the request is sent is momentarily disabled by a system monitoring application.
Signal Interference Failure	The Call Setup request is declined because the repeater where the request is sent is experiencing an FCC type I or II interference. In Capacity Plus /LCP systems, this scenario applies to setting up a new call on the rest channel only.
CWID In Progress Failure	The Call Setup request is declined because the repeater where the request is sent is transmitting CWID. In Capacity Plus /LCP systems, this scenario applies to setting up a new call on the rest channel only.
TOT Expiry Premature Call End Failure	The call ended because the TOT timer expired.
Transmit Interrupted Call Failure	The Call Setup request with interrupt access failed to interrupt the ongoing OTA voice call.
Higher Priority Call Takeover Failure	The call is preempted by another call with higher priority such as Emergency call.

RCM Message (Reason Code)	Failure Scenario
Local Group Call Not Allowed	The Call Setup request for starting a Local Group call is declined because the site where the request is sent is reserved for Wide Area or Private calls. This scenario applies to setting up a new call on the rest channel in Capacity Plus /LCP systems only.
Non-Rest Channel Repeater	The Call Setup request is received on the non-rest channel repeater. This scenario applies to Capacity Plus /LCP systems only.
Destination Site/Sites Busy	The Call Setup request to start a wide area group call is declined because the destination sites of the group do not have channels available. This scenario applies to setting up a new call on the rest channel in Capacity Plus /LCP systems only.
Long Under Run Condition	The repeater ends the call due to jitter buffer under-runs occurring continuously for over 720 ms. This may be due to network congestion.
Undefined Call Failure	Any other failures.
All Call Ongoing or In-progress	The Call Setup request is declined because All Call is ongoing. This scenario applies to setting up a new call on the rest channel in Capacity Plus /LCP systems only.
RCM REPEAT BLOCKED INDICATION	
Start of Signal Interference (FCC Type I)	Signal interference is strong enough and blocks the repeater operation (FCC Type I).
End of Signal Interference (FCC Type I)	Signal interference is weak enough where the repeater resumes over-the-air operation (FCC Type I).
Start of Signal Interference (FCC Type II)	Signal interference is strong enough and blocks the repeater operation (FCC Type II).
End of Signal Interference (FCC Type II)	Signal interference is weak enough where the repeater resumes over-the-air operation (FCC Type II).
Start of CWID/BSI Repeat	The repeater has to transmit CWID/BSI and begins to block the repeater operation.
End of CWID/BSI Repeat	The repeater has ended its transmission of the CWID/BSI and resumes normal repeater operation.
Signal Interference Failure	Broadcast of the calls into the air is intermitted.

Appendix D: Glossary of Acronyms

Table 59: Acronyms

Term	Description
ARS	Automatic Registration Service
BSI	Base Station Identification
CPU	Central Processing Unit
CWID	Continuous Wave Identification
ERDM	Extended Range Direct Mode
GPIO	General Programmable Input Output
GPS	Global Positioning System
HDD	Hard Disk Drive
IP	Internet Protocol
IPSC	IP Site Connect
LCP	Linked Capacity Plus (also known as 'Capacity Plus Multi-Site')
MIB	Management Information Base
NAI	Network Application Interface
NMS	Network Management Station
NSCP	Neocom Software Control Protocol
OID	Object Identifier
OS	Operating system
OTA	Over the Air
RCM	Repeater Call Monitoring
RDAC	Repeater Diagnostics And Control
RoIP	Radio-over-IP
RSSI	Received Signal Strength Indicator
SLA	Service Level Agreement
SMS	Short Message Service
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TOT	Time-Out Timer
UDP	User Datagram Protocol
URL	Uniform Resource Locator
XCMP	Extended Command and Management Protocol
XNL	XCMP Network Layer