ENGLISH

Configuration Guide for Panasonic 771

700 Series Air - IN771AIR00L0000 Gateway

Version 1.0.5
Publication date 2026-01-15

Intesis MAPS

Disclaimer

The information in this document is for informational purposes only. Please inform HMS Networks of any inaccuracies or omissions found in this document. HMS Networks disclaims any responsibility or liability for any errors that may appear in this document.

HMS Networks reserves the right to modify its products in line with its policy of continuous product development. The information in this document shall therefore not be construed as a commitment on the part of HMS Networks and is subject to change without notice. HMS Networks makes no commitment to update or keep current the information in this document.

The data, examples and illustrations found in this document are included for illustrative purposes and are only intended to help improve understanding of the functionality and handling of the product. In view of the wide range of possible applications of the product, and because of the many variables and requirements associated with any particular implementation, HMS Networks cannot assume responsibility or liability for actual use based on the data, examples or illustrations included in this document nor for any damages incurred during installation of the product. Those responsible for the use of the product must acquire sufficient knowledge in order to ensure that the product is used correctly in their specific application and that the application meets all performance and safety requirements including any applicable laws, regulations, codes and standards. Further, HMS Networks will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features or functional side effects found outside the documented scope of the product. The effects caused by any direct or indirect use of such aspects of the product are undefined and may include e.g. compatibility issues and stability issues.

Table of Contents

1. Introduction to Intesis MAPS

Intesis MAPS© is a software tool for configuring and monitoring the Intesis® gateways. Intesis MAPS has been designed and developed in-house, assuring an up-to-date tool to get all the potential of Intesis gateways.

The design of this configuration tool focuses on four main pillars:

- A user-friendly interface.
- Multiple ways to create your project:
  - From scratch, using a template.
  - Importing data from your computer.
  - Downloading the settings from an already configured gateway.
- Full linkage between the control system and the HVAC installation signals.
- Real-time monitoring of the HVAC network.

2. Prerequisites

To configure the gateway, you need:

- The items supplied by HMS Networks:
  - Intesis IN771AIR00LO000 gateway
  - Gateway documentation:
    - Installation guide
    - User manual
- A computer to run the configuration tool Intesis MAPS.

RECOMMENDED REQUIREMENTS:

- OS: Windows 11
- Display resolution:
  - minimum supported: 1280×720 at 100% scaling (no scaling applied)
  - Recommended resolution: 1920×1080
    (Optimized for 100% scaling; higher scaling may cause layout issues)
- Storage: Minimum 1 GB free space
- RAM: 4 GB

- A compatible USB cable.

NOTICE
The type of cable required may vary depending on the gateway version. Earlier models use a Mini-B type connector, while the latest models use a USB Type-C connector.

NOTICE
You can use an Ethernet cable instead (not included).

3. Installation

Downloading the software

1. Enter the Intesis MAPS webpage.
2. Click the **Download now** button. The page will scroll down to the download form.
3. Fill out the form.

> **NOTICE**
> You can review the privacy policy section for more information about how HMS processes the form data.

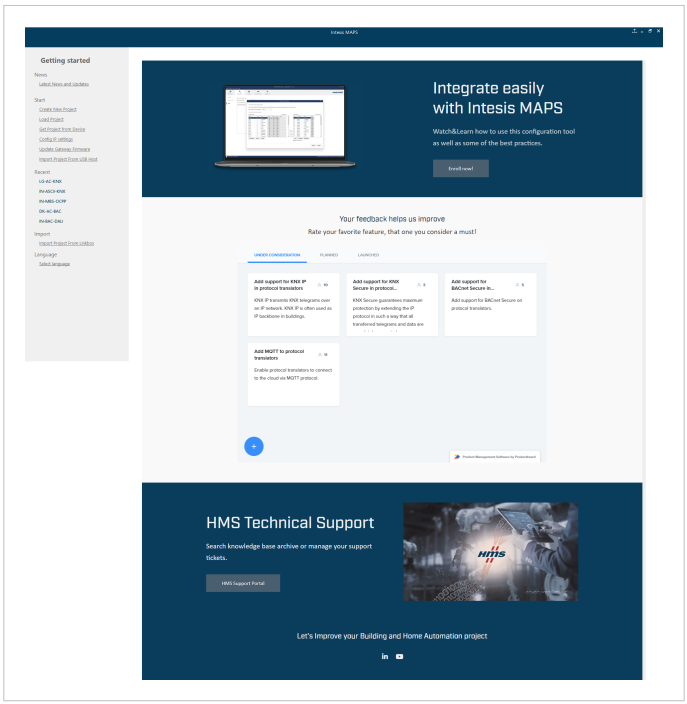
4. Click the **Download** button.
5. A .zip file will be downloaded to your computer.

Installing the software

1. Click the .zip file to open it.
2. Double-click the EXE file.
3. The Intesis MAPS Setup Wizard will guide you through the steps required to install Intesis MAPS on your computer:
   a. Read the license agreement and select **I Agree**.
   b. Select the installation folder.
4. Once the installation is completed, click the **Close** button.

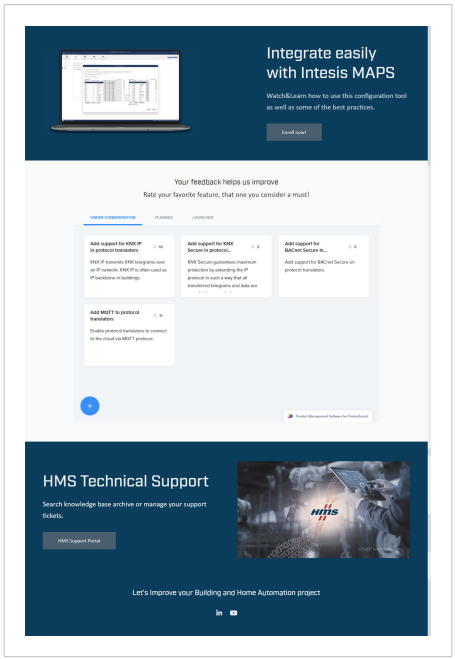
4. First steps in Intesis MAPS

Upon launching Intesis MAPS, you will be greeted with the home screen. This window is divided into two sections: The **Getting Started** column on the left and the **Latest News and Updates** section in the main body.



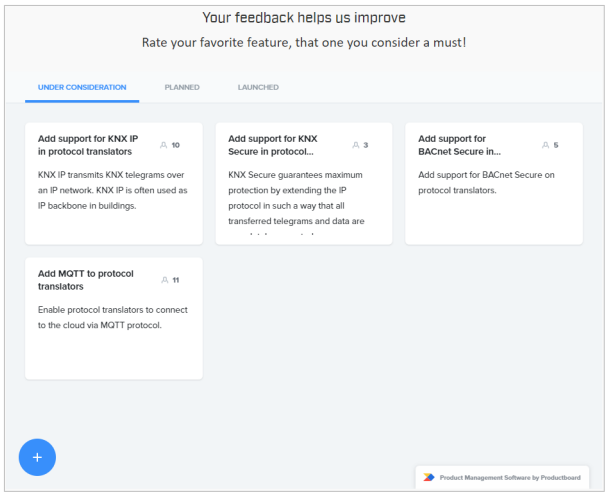
4.1. Latest News and Updates

This section contains useful information related to Intesis MAPS.



Through this section, you can:

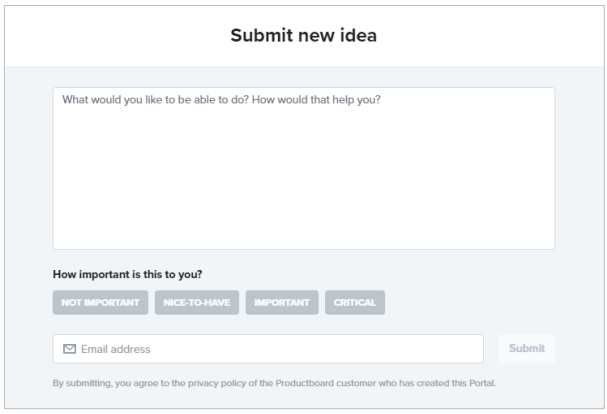
- Get access to an Intesis MAPS online course in the top section.
- Get information about features under consideration for implementation, planned, or recently launched in the features board of the middle section.



NOTE

Click a feature to expand it and rate it. To share a feature, expand it, click the icon, and click on **Copy private link**.

This board also gives the option to submit ideas and suggestions for future features. To submit an idea, click the button and fill out the form.



- You can also enter the HMS Support Portal by clicking the **HMS Support Portal** button at the bottom section.

4.2. Getting Started

This section allows direct access to some of the most commonly used features of Intesis MAPS. These are:

NEWS

- **Latest News and Updates**: Click this option to load the **Latest News and Updates** section.

START

- **Create New Project**: Click this option to open the **New Project** menu.

> **NOTE**
> To know more about creating a new project, consult the section Create a New Project from a Template (page 9).

- **Load Project**: Click this option to load an Intesis MAPS project (.ibmaps file) to Intesis MAPS.

1. Use the new dialog to look for the file and select it.
2. Click **Open** or double-click the file.
3. The project will be loaded to Intesis MAPS.

> **NOTE**
> For more information about file management, consult the section Saving, Opening, Importing, and Exporting the Project (page 10).

- **Get Project from Device**: Click this option to import the Intesis MAPS project file (.ibmaps file) directly from a gateway.

1. Connect the gateway to the computer.
2. On the **Discovered Devices** dialog, select the way you connected the gateway:
   a. **IP**: If you are using the **Ethernet Port** of the gateway.
   b. **USB**: If you are using the **USB** port of the gateway.
3. Select the gateway name (for IP) or the computer COM port (for USB) from the list.

> **NOTICE**
> If the gateway name or the computer COM port does not appear, click the **Refresh** button.
>
> If the problem persists, ensure the gateway and the computer are correctly connected.

4. Once selected, the options on the right will autofill.
5. Click **Import Project**.
6. Once downloaded, use the **Save file** dialog to type a name for the file and select a folder to save it.

> **NOTE**
> For more information on connecting the gateway to your computer, consult the section Connection Tab (page 25).

- **Config IP settings**: This section lists the discovered devices in the network. Select a gateway from the list to check its properties and to gain direct access to the **Identify** and **Edit** functions.

> **NOTE**
> These two functions are covered in the section Connection Tab (page 25).

- **Import Project From USB Host**: Opens a file browser to select an Intesis MAPS project file in USB MAPS Project format (.expmaps) to load.

> **NOTE**
> For more information about file management, consult the section Saving, Opening, Importing, and Exporting the Project (page 10).

RECENT

- **Recent**: A list of up to the last five saved projects is available here. To load any of these last projects, click on its name.

> **NOTICE**
> To check the location path of a recent file, simply hover your cursor over it.

IMPORT

- **Import Project From Linkbox.**

> **NOTICE**
> This option does not apply to the IN771AIR00LO000 gateway.

UPDATES

- **Update Gateway Firmware**: Use this option to check for updates and load a new firmware version to your gateway.

> **NOTE**
> When connecting to the gateway, Intesis MAPS will automatically detect if a new firmware version is available. If so, a new dialog appears showing the firmware version number, the release date, and what's new for this version. Through the **Download** and **Later** buttons, you can update the firmware immediately or postpone the update.

1. Click **Update Gateway Firmware**.
2. On the **Discovered Devices** dialog, select the way you connected the gateway to your computer:
   a. **IP**: If you are using the **Ethernet Port** of the gateway.
   b. **USB**: If you are using the **USB C** port of the gateway.
3. Select the gateway name (for IP) or the computer COM port (for USB) from the list.

> **NOTICE**
> If the gateway name or the computer COM port does not appear, click the **Refresh** button.
>
> If the problem persists, ensure the gateway and the computer are correctly connected.

4. Once selected, the options on the right will autofill.
5. Click **Update Firmware**.

6. The **Firmware Manager** dialog offers two options to update the gateway's firmware:
   - **Update from File**: Use this option if you have a file with the new firmware version stored locally on your computer.
   - **Check for Update**: Use this option if you want to update the firmware online:

> **IMPORTANT**
> You need an internet connection to use this option.

> **NOTE**
> After creating or loading a project, the firmware manager is also available through the **Tools - Firmware** option in the top menu.

- **Software Update**: Click this option to update Intesis MAPS.
  - If you are already using the latest version available, a dialog appears informing you that the software is up to date.
  - If there is a new version available, a dialog will show the information about the new version and three options:
    - **Skip this version**: Click this option to avoid the software update.

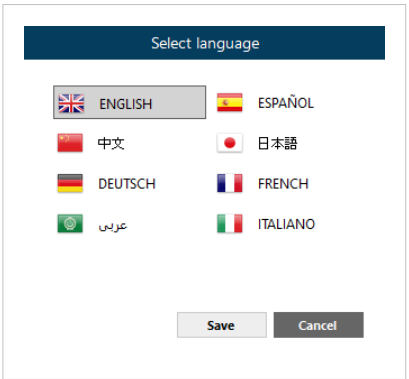
> **IMPORTANT**
> Each new version of Intesis MAPS includes improvements, issue fixes, support for new products, and more. It is recommended to keep the software up to date.

    - **Remind me later**: When clicking this option, a new dialog appears, allowing you to select the time lapse for the reminder or to download the update now.
    - **Update**: The new software version will be downloaded to your computer, and the setup wizard will be launched.

LANGUAGE

- **Select language**: Click this option to change the language.

1. Select a language from the dialog.
2. Click **Save**.
3. To apply the new selected language, close Intesis MAPS and open it again.



5. Create a New Project from a Template

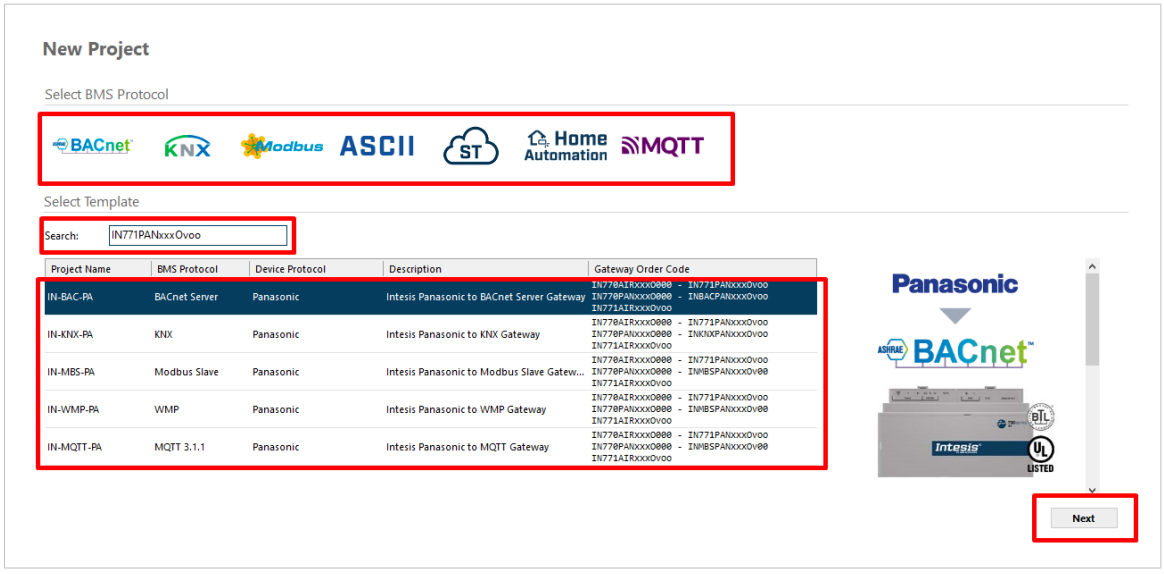
1. Open Intesis MAPS.
2. Click **Create New Project** in the **Start** menu on the left.
   Create a new project using a template. To find the appropriate template, filter the search by:
   - Clicking on the protocol logos.
   - Typing the order code IN771PANxxxOv00 in the **Search** field.

   NOTE
   The order code is printed on the silver label located on either side of the gateway.

   Besides the order code, you can also search by any value from the other columns: **Project Name**, **BMS Protocol**, **Device Protocol**, or **Description**.

   NOTE
   Selecting a **BMS protocol** will limit the search results to that protocol.

   - Looking for the **Project Name** on the list: IN-BAC-PA (for BACnet), IN-MBS-PA (for Modbus), IN-KNX-PA (for KNX), IN-MQTT-PA (for MQTT), IN-WMP-PA (for Home Automation).

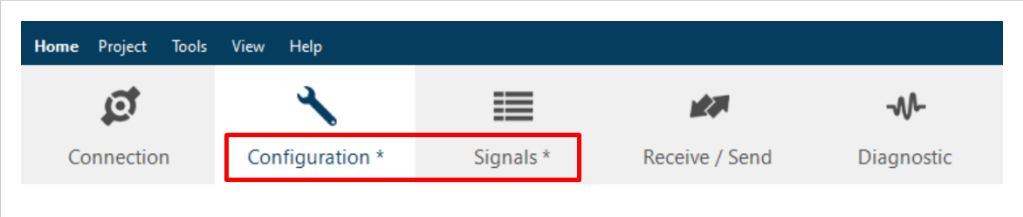


3. Select the desired template.
4. Click **Next** or **double-click the template** on the list.

NOTE
Templates are just a starting point for your integration. Depending on the type of integration, you may have to modify some parameters.

6. Saving, Opening, Importing, and Exporting the Project

After editing any option from the **Configuration** and **Signals** tabs, an asterisk appears to indicate that you have made changes to the project but have not saved them or sent the project to the gateway yet:

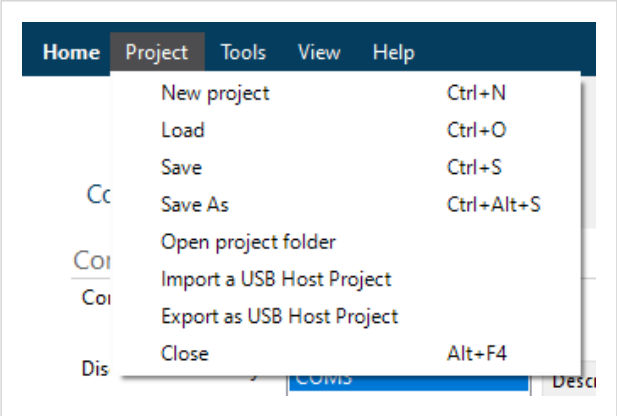


To know how to send your project to the gateway, see Receive/Send Tab (page 32).

- **SAVING YOUR INTESIS MAPS PROJECT**

> **IMPORTANT**
> Remember to save your project periodically to keep your changes.

1. Click **Project**.



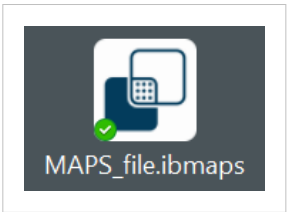
2. Click **Save** or **Save As**.

> **TIP**
> Instead, you can use the shortcut **Ctrl+S** (Save) or **Ctrl+Alt+S** (Save As).

3. On the **Save file** menu, type a **File name** and select where to save the file.
4. Click **Save**.

- **OPENING AN INTESIS MAPS PROJECT FROM YOUR COMPUTER**

> **TIP**
> Double-click a .ibmaps file saved on your computer to automatically open it in Intesis MAPS.

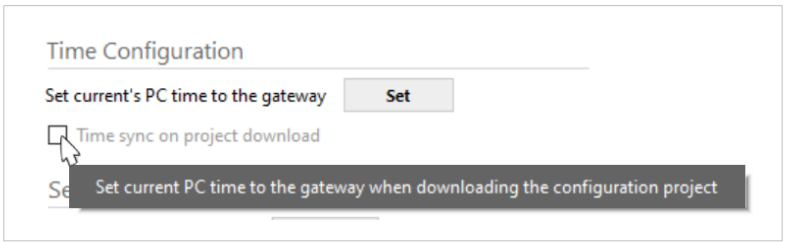


1. Click **Project**.
2. Click **Load**.
3. On the emergent window, select the desired file from your computer.
4. Click **Open**.

7. Main Menu Overview

The following sections provide an overview of the five tabs that compose the Intesis MAPS main menu. Through these options, you will establish a connection between the gateway and the computer, set up your project through the **Configuration** and **Signals** tabs, send it to the gateway, and monitor that everything works fine using the **Diagnostic** tab.

TIP
Tooltip: Hover the cursor over a field, and a message will appear indicating the purpose of the parameter.



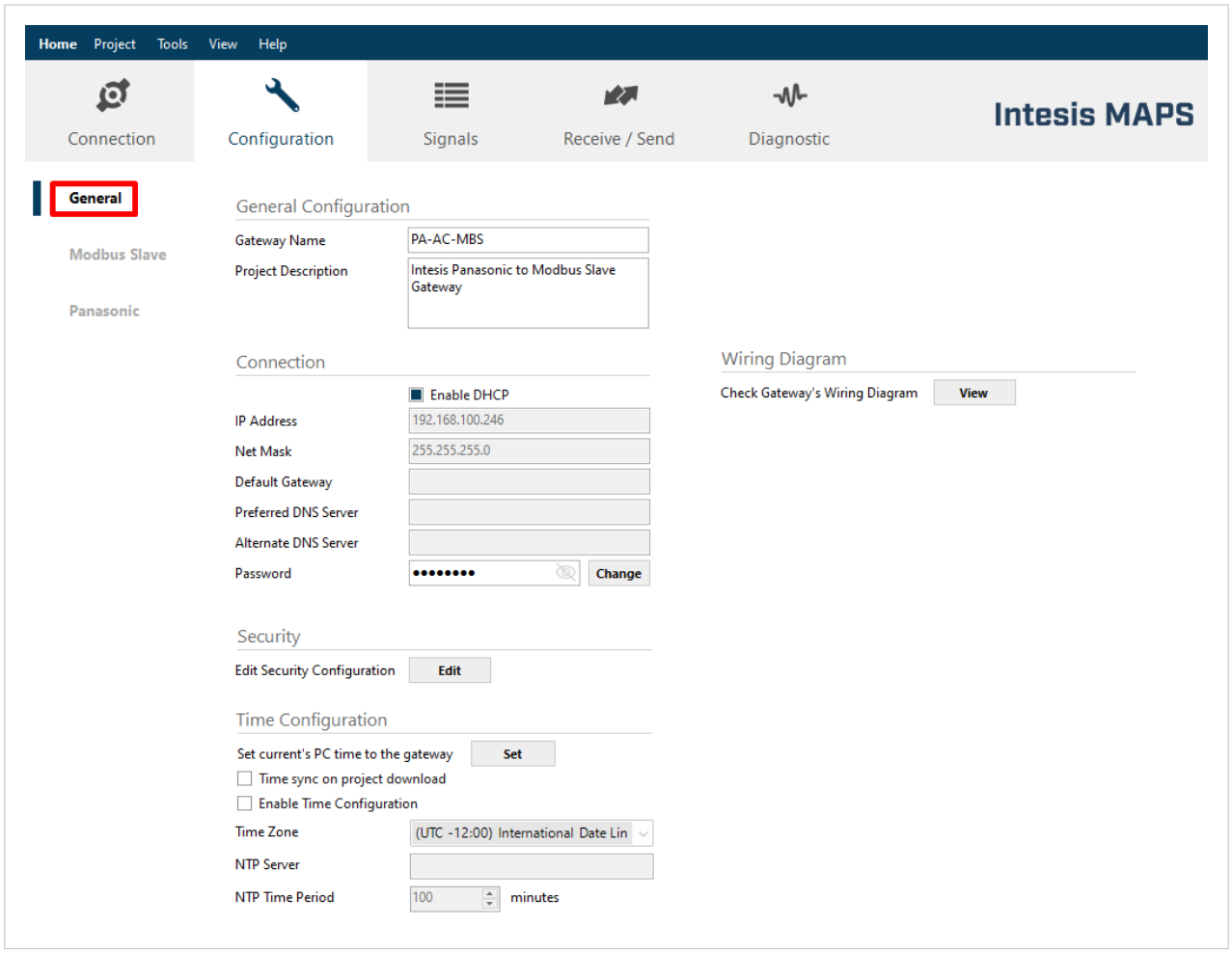
8. Configuration Tab

A menu with some options appears on the left side of the window:

- **General**: Configure the general parameters of the gateway.
- **Building management system (BMS) protocol**: Modbus, KNX, BACnet, MQTT, or Home Automation, depending on your project's current protocol combination. In the case of the image on the left, the control system is based on Modbus.
- **Panasonic:** Protocol of the AC installation.

NOTE
The order of these elements may change depending on the protocol combination, and additional subsections may appear.

8.1. General Configuration Menu



Use this section to configure some general parameters of the gateway.

NOTICE
The available options may vary depending on the active protocol.

8.1.1. General Configuration

- **Gateway Name**: Type a descriptive name for your gateway (max. 32 characters).
- **Project Description**: Type a short description of your project (max. 255 characters).

8.1.2. Connection

- **Enable DHCP (selected by default)**.
  When sending the project to the gateway, the status of this parameter determines how the IP address is assigned:
  - The parameter is selected: No IP address is assigned to the gateway, which will be permanently waiting for a DHCP server to assign an IP address.
  - The parameter is deselected: A static IP address must be assigned to the gateway through the following parameters:
    - **IP Address**: Set the static IP address (default value: **192.168.100.246**).

      IMPORTANT
      Change the gateway's default IP address before integrating it at the final installation site to prevent security issues and IP conflicts.

    - **Net Mask**: Set the subnet mask (default value: **255.255.255.0**).
    - **Default Gateway**: Type the access point/router IP address.

      NOTE
      The **Default Gateway** parameter is a networking concept that is not related to the Intesis gateway. It refers to the IP address of the device (usually a router) that serves as the access point for sending data from the local network to other networks, including the Internet. Therefore, this field only needs to be filled in if the Intesis gateway is connected outside the local network.

    - **Preferred DNS Server**: Type the DNS server IP address.
    - **Alternate DNS Server**: Type the IP address of an alternative DNS server.

      NOTE
      The gateway connects with this alternative DNS server if there is no communication with the **Preferred DNS Server**.

- **Password**. Use this option to visualize the gateway's password and set a new one.

> **IMPORTANT**
> Change the default password before sending the project to the gateway. Follow the instructions below.

1. Click the **Change** button.
2. Type a new password.
3. Go to the **Receive/Send** tab.
4. In the **Send** menu, click the **Send** button.
5. Go to the **Connection** tab.
6. Select the gateway from the **Discovered Gateways** window.
7. Click **Connect**.

8.1.3. Security

- **Edit Security Configuration**: Click the **Edit** button to open the **Security Configuration** window.

> **IMPORTANT**
> We recommend keeping the predetermined configuration.

  - **Disable UPD Discover Service** (disabled by default): If selected, the gateway is not discoverable through UDP communication.
  - **Disable TCP Console Service** (disabled by default): If selected, the gateway stops communicating with the configuration and diagnostic software through TCP. This only applies to gateways supporting connection to the computer via both Ethernet and console ports.
  - **Use custom UDP/TCP port** (disabled by default): Enable to set the UDP/TCP port manually.
  - **Disable HTTPS Certificates Auto Update** (enabled by default): If selected, automatic updates for HTTPS certificates are not allowed. If deselected, you can set the update time period using the parameter below.

Click **Save** to save the changes.

8.1.4. Time Configuration

- **Set current PC time to the gateway**: Connect the gateway to your computer and click the **Set** button to set the gateway's time to your computer's current time.
- **Time sync on project download** (disabled by default): The gateway's time is set to your computer's time when downloading the project to the gateway.

This gateway supports Network Time Protocol (NTP) time servers. To define a time server, check the **Enable Time Configuration** checkbox and use the following parameters:

- **Time Zone**: Select the correct time zone for your project.
- **NTP Server**: You can define an NTP server using either an IPv4 address or a domain name.

  NOTICE
  The domain name format requires an operative DNS server. This server must be defined manually when DHCP is disabled. See Connection (page 14).

- **NTP Time Period**: Select the interval, in minutes, at which the gateway synchronizes its internal clock with the NTP server. Valid range: 1 to 65535 minutes. Default value: **100 minutes**.

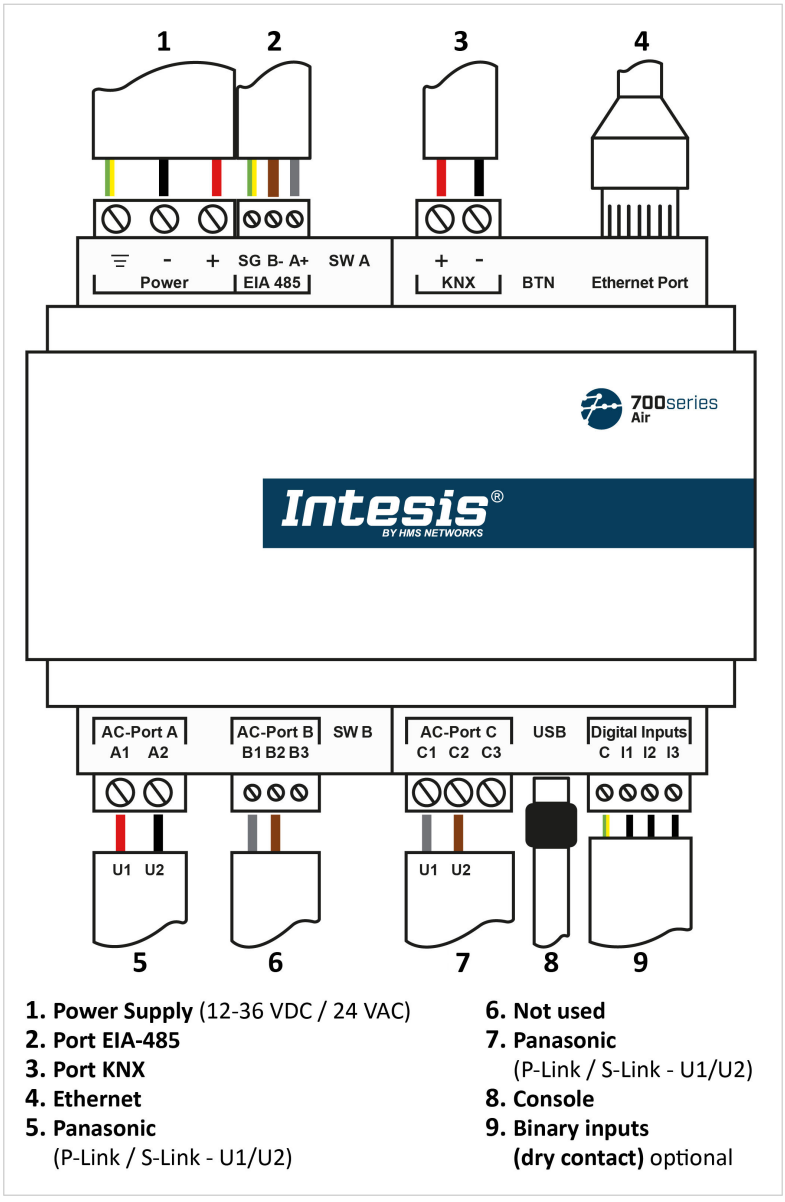
TIP
Having configured this section, synchronization with the NTP server can be triggered at any time through the **Console** viewer in the **Diagnostic** tab. To do so, enter **ntpsync** in the console. The possible responses are:

- **NTP - SUCCESS [timestamp]**: Synchronization successful. Gateway time updated to *[timestamp]*.
- **NTP - ERROR [error description]**: Synchronization failed. Reason: *[error description]*.

For more information about the **Diagnostic** tab, see Diagnostic Tab (page 33).

8.1.5. Wiring Diagram

- **Check Gateway's Wiring Diagram**: Click the **View** button to open the schematic image showing how to wire the gateway.



1. **Power Supply** (12-36 VDC / 24 VAC)
2. **Port EIA-485**
3. **Port KNX**
4. **Ethernet**
5. **Panasonic**
   (P-Link / S-Link - U1/U2)
6. **Not used**
7. **Panasonic**
   (P-Link / S-Link - U1/U2)
8. **Console**
9. **Binary inputs**
   (dry contact) optional

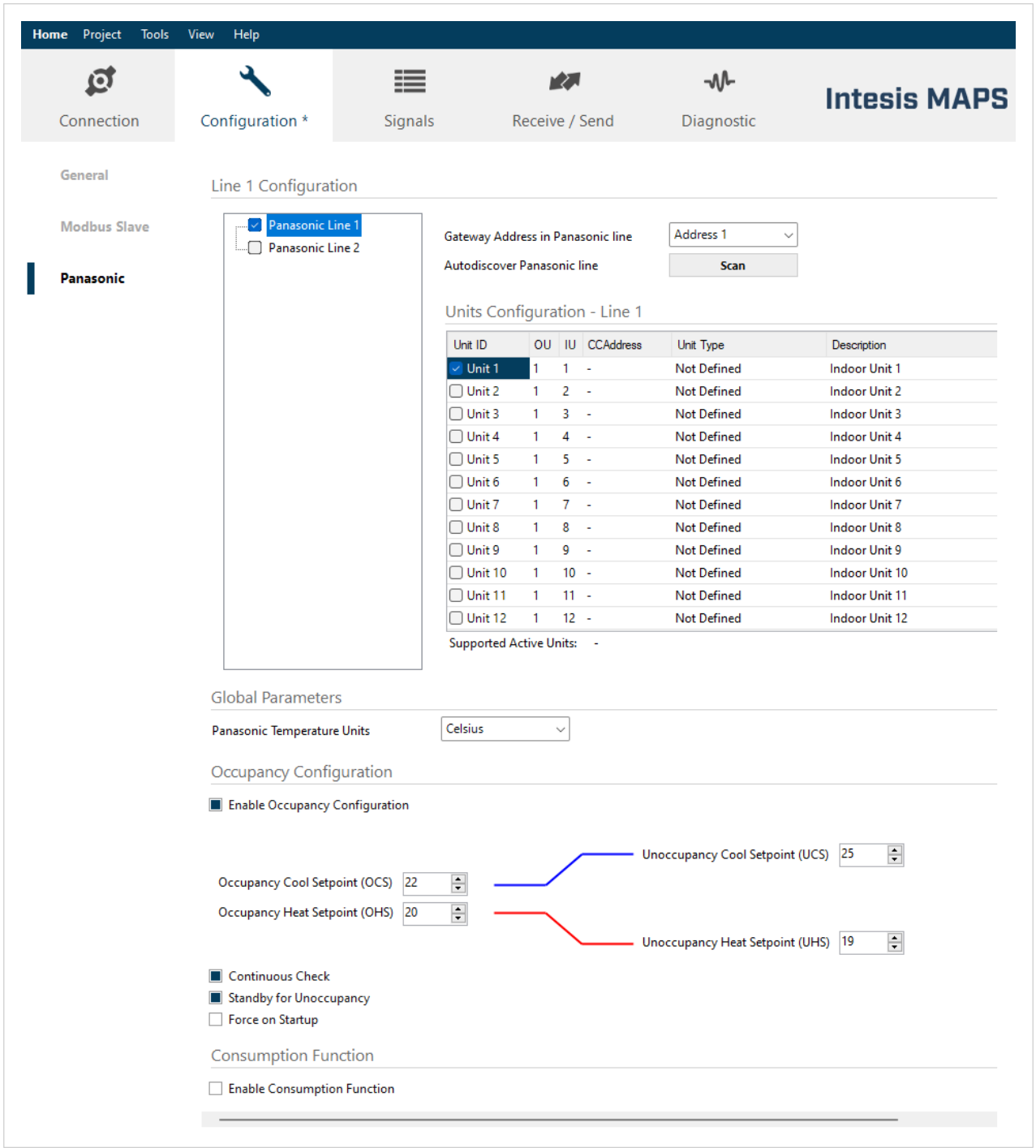
8.2. BMS Protocol

The parameters in this menu vary depending on the current protocol combination. Consult these sections for each protocol:

- Modbus (page 38)
- KNX (page 41)
- BACnet (page 44)
- MQTT 3.1.1 (page 57)
- Home Automation (page 67)

8.3. Panasonic Protocol (Device Protocol)

Figure 1. Panasonic protocol parameters inside the Configuration tab



Use this menu to integrate AC indoor and outdoor units into your project and configure some Panasonic protocol parameters.

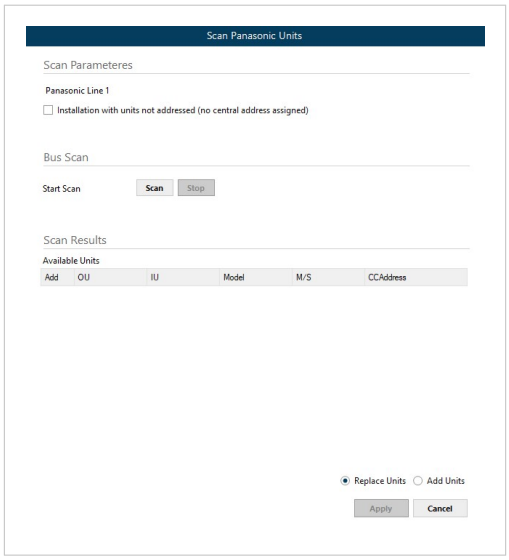
8.3.1. Lines Configuration

1. Select the **Panasonic Line**.
2. Select the **Gateway Address in Panasonic line**: **Address 1** or **Address 2**.

- **Autodiscover Panasonic Line**: This function discovers all indoor and outdoor units connected to the installation.

  1. Click the **Scan** button to open the Scan Panasonic Units window:

Figure 2. Bus Scan window



  2. Click the **Installation with units not addressed (no central address assigned)** checkbox if applicable. If so, set the **OU Scan range** by selecting its low and high limits.
  3. Start the bus scanning by clicking the **Scan** button.
  4. Once the scanning has finished, you can select or deselect which units you want to integrate.
     - Check the **Replace Units** option if you want the units you have now selected to replace the previously listed units.
     - Check the **Add Units** option if you want to add the units you have now selected to the previously listed units.
  5. Click **Apply** to replace/add the discovered units you have selected.

- **Units Configuration**: Use this table to configure some parameters related to the AC units of your project:
  - **Unit ID**: Check which units you want to integrate.
  - **OU**: Set a number for each outdoor unit (1..31).
  - **IU**: Set a number for each indoor unit (1..64).
  - **Description**: Type a description for each unit.

8.3.2. Global Parameters

NOTE
This section is not available for the Home Automation protocol.

- **Panasonic Temperature Units**: Temperature unit in Celsius or Fahrenheit degrees.

8.3.3. Occupancy Configuration

- **Enable Occupancy Configuration**: Click the checkbox to enable this functionality.
- **Occupancy Cool Setpoint (OCS)**: Set the temperature for the cool mode when the room is occupied (1..100°C / 33..212°F. Default value: **22°C / 71°F**).
- **Unoccupancy Cool Setpoint (UCS)**: Set the temperature for the cool mode when the room is unoccupied (1..100°C / 33..212°F. Default value: **25°C / 77°F**).

IMPORTANT
UCS must always be higher than or equal to OCS.

- **Occupancy Heat Setpoint (OHS)**: Set the temperature for the heat mode when the room is occupied (1..100°C / 33..212°F. Default value: **20°C / 68°F**).
- **Unoccupancy Heat Setpoint (UHS)**: Set the temperature for the heat mode when the room is unoccupied (1..100°C / 33..212°F. Default value: **19°C / 66°F**).

IMPORTANT
UHS must always be lower than or equal to OHS.

IMPORTANT
The minimum difference between the Cool and Heat setpoints must be 2°C / 4°F.

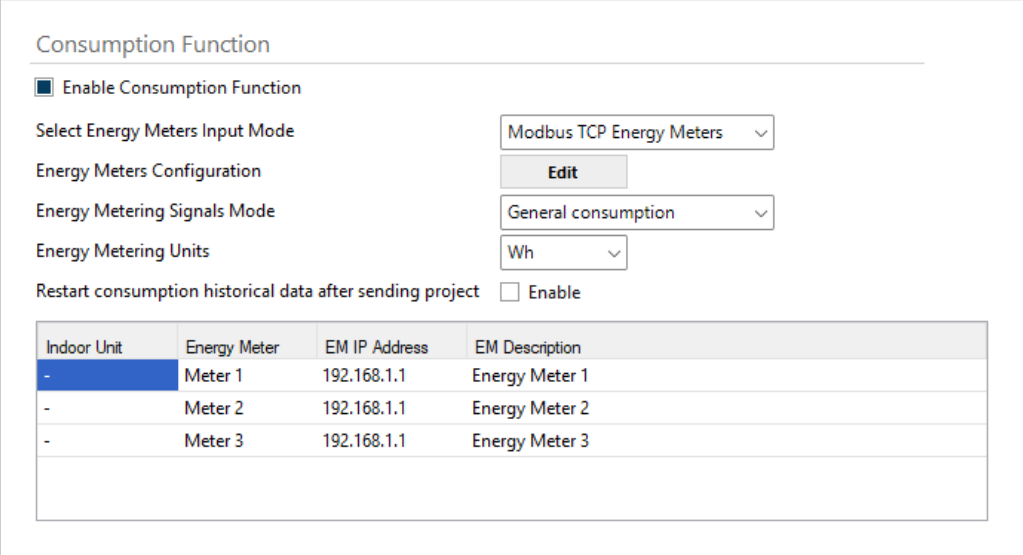
- **Continuous Check**: Click the checkbox to enable or disable this parameter. When enabled, the gateway checks the occupancy when there's any change in the room's temperature. If the parameter is unchecked, it only checks the occupancy when the occupancy status changes.
- **Standby for Unoccupancy**: Click the checkbox to enable/disable this parameter, which determines the indoor unit's behavior while the ambient temperature is in between the deadband. If enabled, the indoor unit will turn off; if disabled, it will remain on.
- **Force on startup**: Click the checkbox to enable/disable this parameter. If enabled, the values you set in the configuration screen will be loaded after a reset. If disabled, the last selected values will be loaded after a reset.

8.3.4. Consumption Function

NOTE
This function is available only for Modbus, KNX, and BACnet.

With this function, you can monitor the energy consumption of the integrated indoor units.

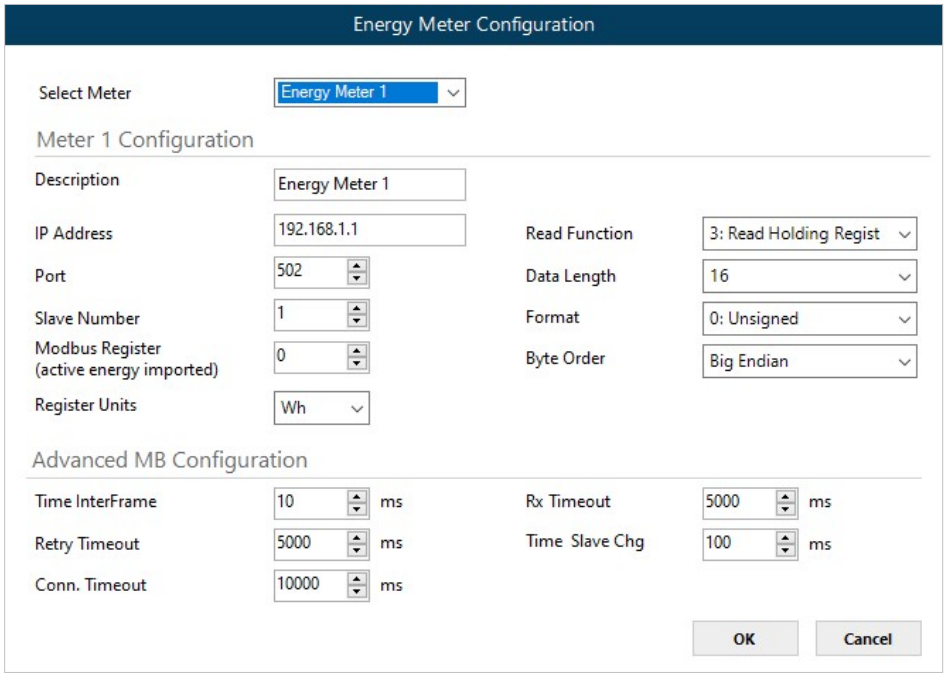
IMPORTANT
Before using this function, ensure the AC system and the pulse/Modbus energy meters are already installed, wired, configured, and properly working.



- **Enable Consumption Function**: Click the checkbox to enable this parameter.
- **Select Energy Meters Input Mode:** Select **Modbus TCP Energy Meters** or **Pulse Meters & Binary Inputs**.
- **Energy Meters Configuration**: Click the **Edit** button to open the **Energy Meter Configuration** window.

NOTE
The configuration parameters will vary depending on the energy meter type selected.

– Energy meter configuration for **Modbus TCP Energy Meters**.



Use the **Select Meter** parameter to choose the energy meter you want to configure.

NOTE
Up to three energy meters are available.

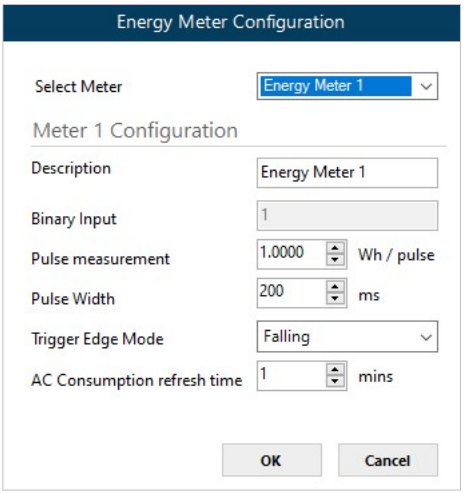
- **Meter 1 Configuration**:
  - **Description**: Type a description for the meter.
  - **IP Address**: It shows the IP address where the meter is located.
  - **Port**: Port for the Modbus TCP/IP connection. (**502** port by default).
  - **Slave Number**: Energy meter slave Modbus address (1 to 254).
  - **Modbus Register (active energy imported)**: Modbus register to read (1 to 65535).
  - **Register Units**: Choose **Wh** or **kWh**.
  - **Read Function**: Read register type for this function. Choose between function **3: Read Holding Registers** and function **4: Read Input Registers**.
  - **Data Length:** Number of bits for the Modbus register (16, 32, or 64 bits).
  - **Format**: Select the data type between **0: Unsigned**, **1: Signed (C2)**, **2: Signed (C1)**, **3: Float**.
  - **Byte Order**: Choose **Big Endian**, **Little Endian**, **Word Inv BE**, **Word Inv LE**.
- **Advanced MB Configuration**:
  You can modify these Modbus parameters to adapt the Modbus communication to every installation.

  IMPORTANT
  These parameters are for advanced users only. As a general rule, keep the default values for proper communication with the meter.

  - **Time InterFrame**: Select the minimum time between received and sent frames (0 to 100000 ms. Default value: **10 ms**).
  - **Retry Timeout**: Select the minimum time between retry frames after no response on the TCP connection (0 to 30000 ms. Default value: **5000 ms**).

- **Conn. Timeout**: Select the minimum time before launching an error message after no response on the TCP connection (100 to 30000 ms. Default value: **10000 ms**).
- **RX Timeout**: Select the minimum time before launching an error message when no TCP frames are received but the TCP connection is OK (100 to 30000 ms. Default value: **5000 ms**).
- **Time Slave Chg**: Select the minimum time of silence when changing from one slave device to another one (100 to 10000 ms. Default value: **100 ms**).

- Energy meter configuration for **Pulse Meters & Binary Inputs**.



Use the **Select Meter** dropdown menu to choose the energy meter you want to configure.

- **Meter 1 Configuration**.
  - **Description**: Type a description for the meter.
  - **Binary Input (not editable)**: It shows the gateway's digital input where the meter is connected.
  - **Pulse Measurement**: Set the equivalence between pulses and energy.

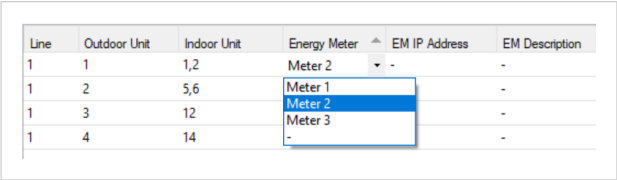
    IMPORTANT
    This value must match the configuration of the energy meter device.

  - **Pulse Width**: It defines the width of each pulse.

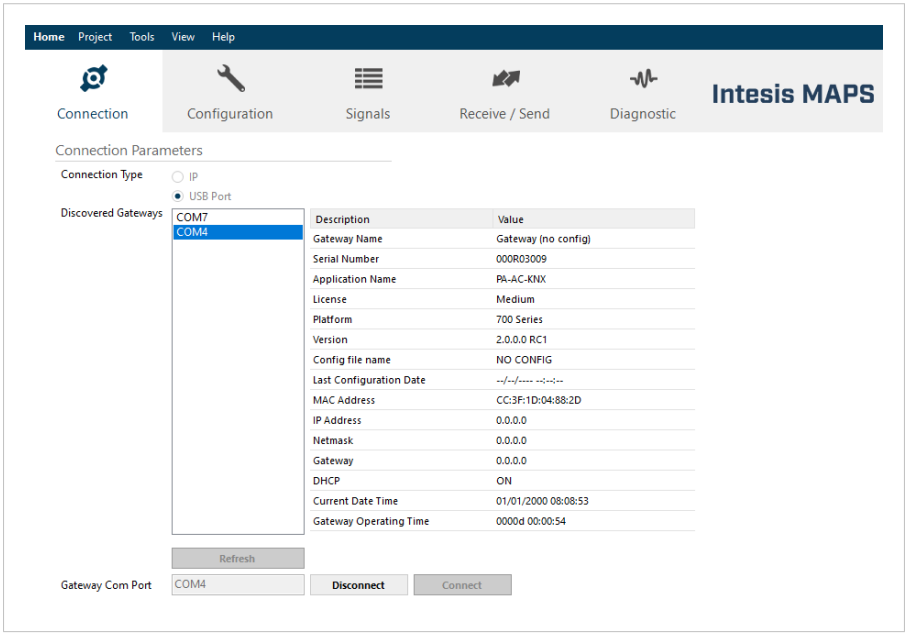
    IMPORTANT
    This value must match the configuration of the energy meter device.

  - **Trigger Edge Mode**: Choose between **Falling** or **Rising** mode.
  - **AC Consumption refresh time**: It defines the time to refresh the consumption values for this energy meter.

- **Energy Metering Signals Mode**. Choose between:
  - **General Consumption**. It activates three signals for each indoor unit:
    - Consumption Yesterday
    - Consumption Today
    - Consumption Total
  - **Cool/Heat modes consumption**. It activates six signals for each indoor unit:
    - Consumption Yesterday Heat
    - Consumption Today Heat
    - Consumption Total Heat
    - Consumption Yesterday Cool
    - Consumption Today Cool
    - Consumption Total Cool
- **Energy Metering Units**: Choose between **Wh** or **KWh**.
- **Restart consumption historical data after sending project**: If checked, consumption historical data will be restarted every time a project is sent to the gateway.
- **Assignation table**. Use this table to assign the previously selected units to each **Energy Meter**.
  - Select the **Energy Meter** for each **Outdoor Unit**.



9. Connection Tab



1. Connect the gateway to your computer. Two possibilities are available:

   - Use the **USB** port and an appropriate USB cable.

   NOTICE
   The type of cable required may vary depending on the gateway version. Earlier models use a Mini-B type connector, while the latest models use a USB Type-C connector.

   TIP
   This type of connection is recommended.

   - Use the gateway's **Ethernet port**.

   IMPORTANT
   When using this type of connection, some considerations must be taken into account. Consult the Troubleshooting section at the end of the document. See Connecting the Gateway to the Computer through Ethernet (page 71).

2. If the gateway is not powered on yet, turn it on.

   IMPORTANT
   Use an adequate power supply. Consult the gateway's User Manual or Installation Guide.

   TIP
   If the gateway still has its factory settings or has been factory reset, wait a few seconds for it to initialize and become ready before continuing.

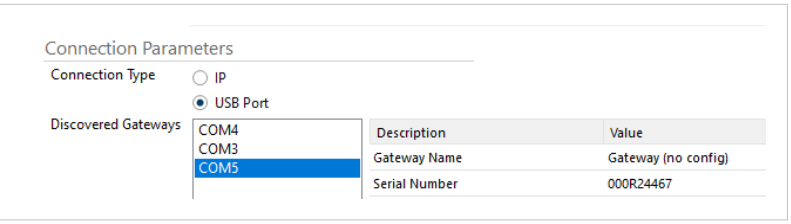
3. On the **Connection Type** parameter, select the way you connected the gateway to your computer:

   a. Select **USB Port** if you are using the **USB** port of the gateway.

> **TIP**
> No password is needed when connecting via USB.

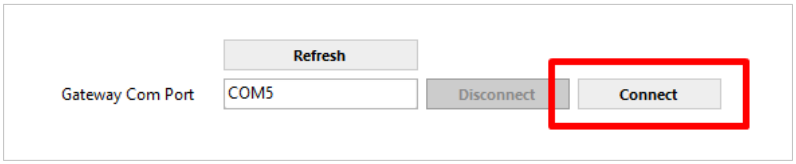
> **NOTICE**
> When using the USB connection, the active ports of your computer will appear in the **Discovered Gateways** field as **COM** + the number of the port (**COM5** in the image below).

   i. In the **Discovered Gateways** field, select the port of the computer where the gateway is connected.

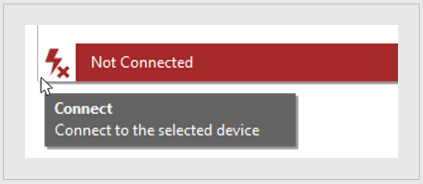


> **NOTICE**
> All data from the **Value** column on the right will be automatically populated when the correct gateway is selected.

   ii. Click the **Connect** button.



> **TIP**
> You can also connect to the gateway using the button from the lower bar:

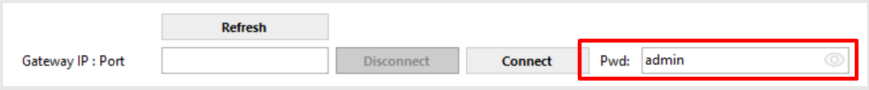


> **NOTICE**
> When the connection is established, the lower red bar will turn blue.

b. Select **IP** if you are using the **Ethernet port** of the gateway.

NOTE

- The default password when connecting via IP is **admin**.



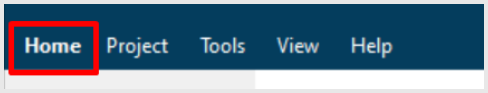
  You can change this password as explained in Configuration Tab → General → Connection (page 14).

- When the gateway still has its factory settings or has been factory reset, it appears in the **Discovered Gateways** field as **Gateway (no config)**.

IMPORTANT

When using the IP connection, the gateway's name should appear in black. If it appears in red:

- The gateway is not compatible with the selected template. To solve the problem, click **Home** in the upper menu to go to the **New Project** page, and make sure you select the correct template, as explained in Create a New Project from a Template (page 9).



- There is a problem with the gateway IP address. Consult the Troubleshooting section at the end of the document. See Connecting the Gateway to the Computer through Ethernet (page 71).
- If the problem persists, try to update the gateway's firmware as explained in Getting Started → UPDATES → Update Gateway Firmware (page 7).

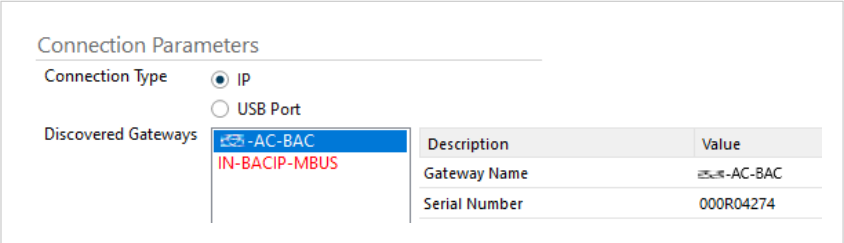
TIP

If your gateway does not appear in the **Discovered Gateways** field:

- Wait a minute for the gateway to initialize and become ready.
- Click the **Refresh** button.

- Deactivate the Wi-Fi connection on your computer.
  - On rare occasions, having the Wi-Fi connection activated causes the Windows system to bypass the Ethernet connector, preventing the computer from finding the gateway.
- If the problem persists, follow the instructions explained in Troubleshooting - Connection Tab (page 71).

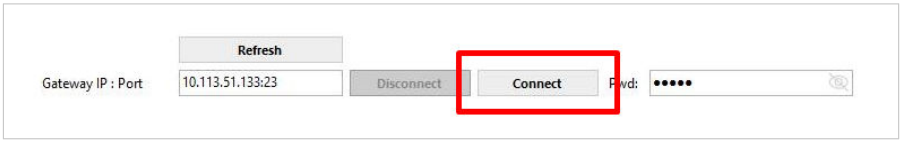
i. Select your gateway from the **Discovered Gateways** field.



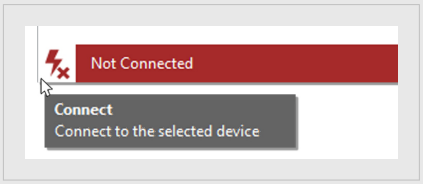
NOTICE
All data from the **Value** column on the right will be automatically populated when the correct gateway is selected.

The IP address and port of the gateway will also be displayed in the **Gateway IP : Port** option below the **Refresh** button.

ii. Click the **Connect** button.



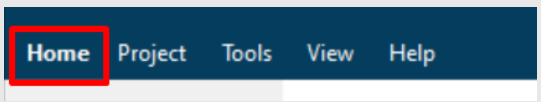
TIP
You can also connect to the gateway using the button from the lower bar:



NOTICE
When the connection is established, the lower red bar will turn blue.

IMPORTANT
If your Intesis gateway doesn't match the selected template, a warning message will emerge.

- Go back to **Home** and ensure you selected the correct template.



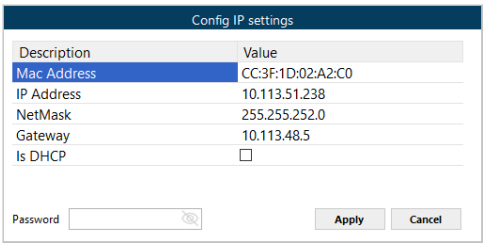
The IN771AIR00LO000 gateway is compatible with the following templates:

  - For BACnet: IN-BAC-PA
  - For KNX: IN-KNX-PA
  - For Modbus: IN-MBS-PA
  - For MQTT: IN-MQTT-PA
  - For Home Automation: IN-WMP-PA

- If the problem persists, try to update the gateway's firmware as explained in Getting Started → UPDATES → Update Gateway Firmware (page 7).

When selecting IP as the connection type, two additional buttons will appear once the connection is established:

- **Identify**: Click the **Identify** button and then enter the project password to make the gateway's LEDs blink for 10 seconds.
- **Edit**: Click the **Edit** button to open the **Config IP settings** window.



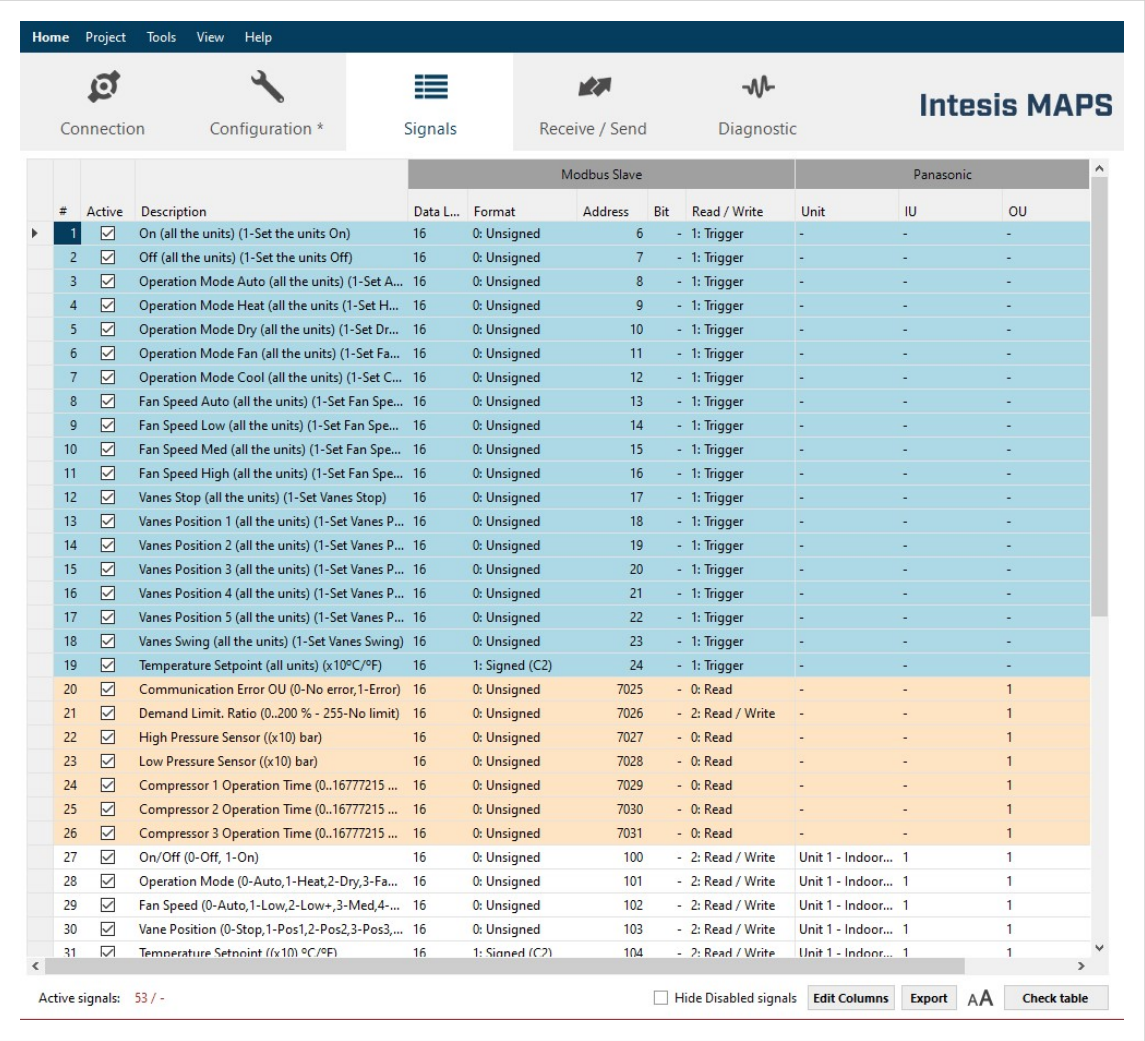
When DHCP is not enabled, you can edit the **IP Address**, **NetMask**, and Default **Gateway** IP. Enter the project password and click the **Apply** button to save the changes.

NOTICE
These parameters can also be edited in the **Configuration** tab. See Configuration Tab → Connection (page 14).

10. Signals Tab

This menu lists all available signals and their parameters for both BMS and Device protocols.

Figure 3. Signals tab for the Modbus server protocol combination



Regardless of the protocol, all signals share some common characteristics and parameters:

Signals background color meaning:

- **Blue**: General system signals.
- **Orange**: Signals for the outdoor units.
- **White**: Signals for the indoor units.

NOTICE

The number of available signals depends on different factors, such as the current protocol, the unit types, and the functions enabled.

Below the list of signals, these options are available:

- **Auto BACname**: Uncheck this parameter to edit signal names.

> **NOTE**
> This parameter is available only for **BACnet**.

- **Active signals**: Number of active signals / total number of signals.

> **TIP**
> You can use the checkbox at the column header to select or deselect all signals at once.

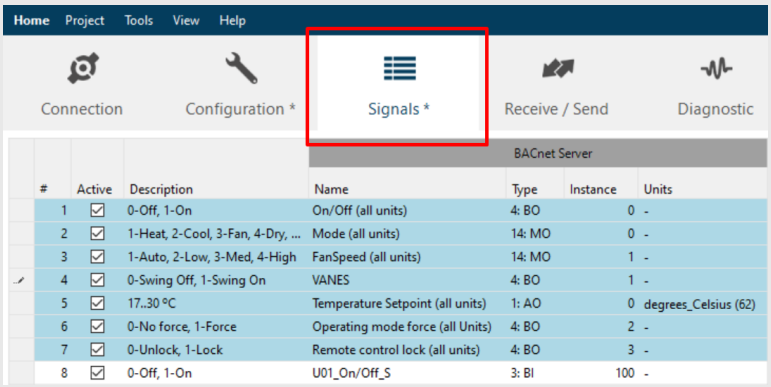
- **Hide Disabled signals (disabled by default)**: Show/hide all disabled signals from the list.
- **Edit Columns**: Click this button to hide/show any column of the table.
- **Export**: Click this button to export the current signals' configuration to an XLSX file for later import, helping to reduce commissioning time.

> **TIP**
> The **Import** and **Export** options can help you reduce commissioning time. However, you can also export and import the whole project's configuration, including the signal's settings, as explained in Saving, Opening, Importing, and Exporting the Project (page 10).

- **AA**: Increases or decreases the font size.
- Click the **Check table** button to review the signals' configuration.

> **NOTE**
> If any signal parameter is incorrect, a message will pop up with specific error information.

> **IMPORTANT**
> After editing a parameter or enabling or disabling a signal, an asterisk appears on the **Signals** tab icon as a reminder that you have made changes to the project but have not saved them or sent the project to the gateway yet.



To know how to save your project, see Saving, Opening, Importing, and Exporting the Project (page 10).

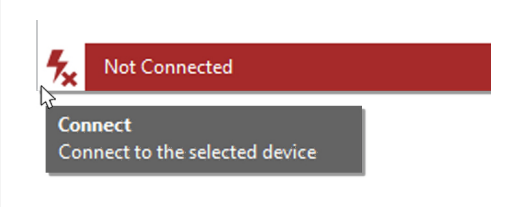
To know how to send your project to the gateway, see Receive/Send Tab (page 32).

11. Receive/Send Tab

SEND

NOTE
Once you have finished setting all the necessary parameters for your Intesis MAPS project, you must load the project onto the gateway to configure it. The gateway will not be configured until the Intesis MAPS project is sent to it.

1. Click the **Send** button.
   a. If the gateway is still factory-set, you will be prompted to save the project on your PC. Once saved, the configuration is automatically sent to the gateway.
   b. If you have already saved the project, the configuration is automatically sent to the gateway.
2. Connect again with the gateway after sending the file.



NOTICE
The gateway reboots automatically once the new configuration is loaded. This process may take a few seconds.

Once the configuration is completed and sent, the gateway is already operative. Even so, you should review that everything works correctly by entering the **Diagnostic** tab.

RECEIVE

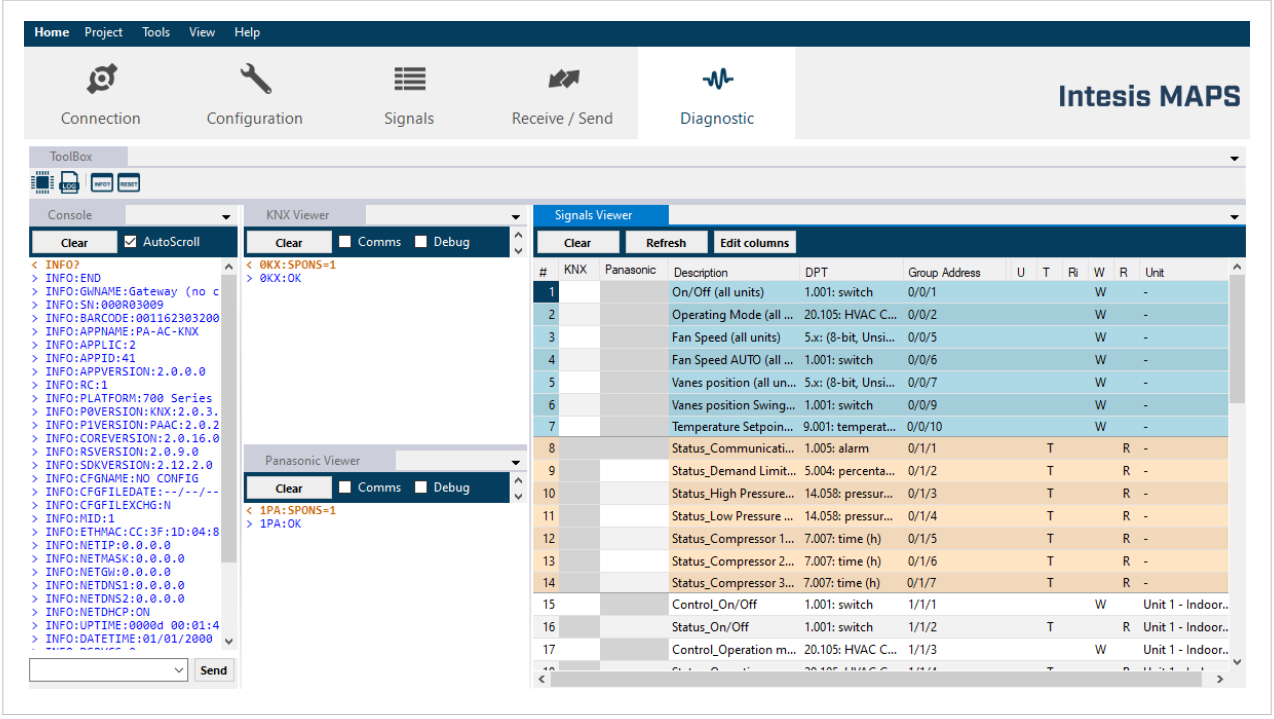
Use this function to load the configuration of a gateway to Intesis MAPS.

TIP
This function may be helpful when you need to change some parameters of an already configured gateway or to clone the project loaded in a gateway.

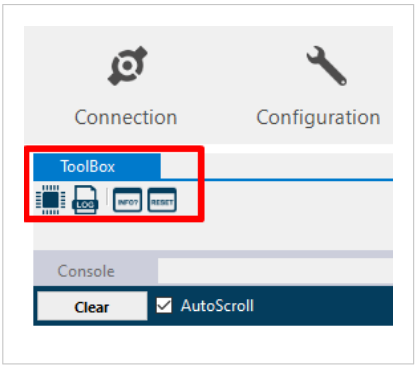
12. Diagnostic Tab

IMPORTANT
Connection with the gateway is required to use the diagnostic tools.

Figure 4. Diagnostic tab window. Find the ToolBox between the upper tabs bar and the Console view. Below it, from left to right: Console viewer, Protocol viewers (one above the other), and the Signals viewer



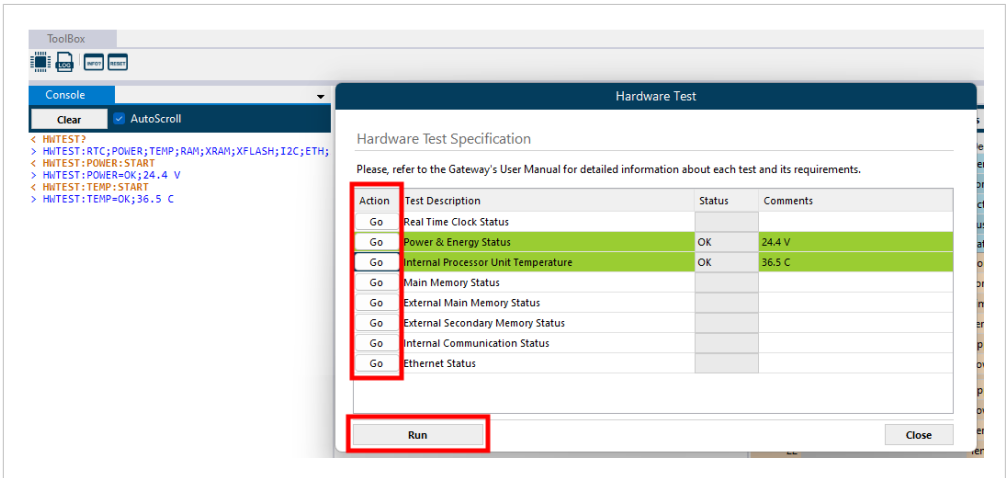
TOOLBOX



NOTE
Depending on your screen resolution, the **ToolBox** icons may appear partially hidden behind the **Viewers** window.

Options in the **ToolBox** menu, from left to right:

- **Microprocessor icon**: Run a hardware test for each component of the gateway.



  - Use the **Go** buttons to run a test for each specific element.
  - Use the **Run** button to run a test for all hardware elements.

> **NOTICE**
> The information will be displayed in both the **Hardware Test** dialog and the **Console** viewer.

- **LOG**: Set Intesis MAPS in logging mode to record all the information present in the viewers and save it in a .zip file.

> **NOTICE**
> - Once the recording starts, the **LOG** icon turns red.
> - You can stop the recording at any moment by clicking the **LOG** icon.
> - When the recording stops, a dialog appears allowing you to run a hardware test and include it in the log file.

- **INFO?**: This option shows the gateway information in the **Console** viewer.
- **RESET**: Reset the gateway.

VIEWERS

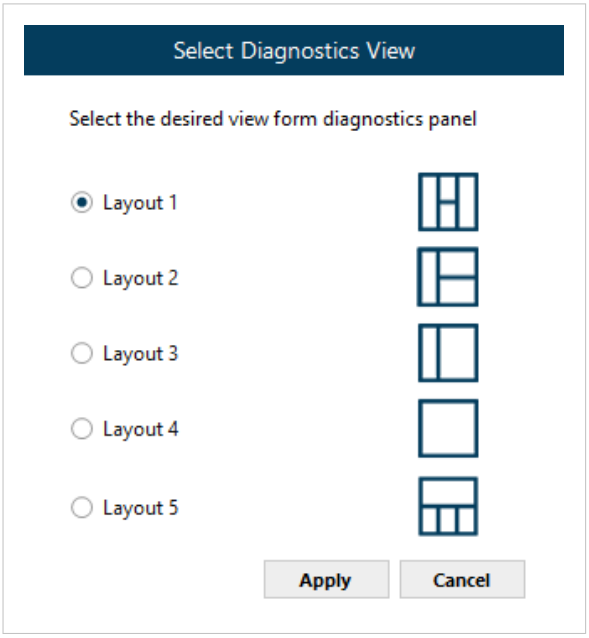
Intesis MAPS provides several viewers:

- A generic console viewer for general information about communications and the gateway status.
- A viewer for both protocols to check their current status.
- A signals viewers to simulate the BMS behavior or check the system's current values.

> **NOTE**
> Use the refresh button to get updated values on the signals viewer.

The layout of these viewers can be modified:

- Using the **Select Diagnostics View** option from the **View** menu:



NOTE
Layouts 3 and 4 offer two different tabbed options:

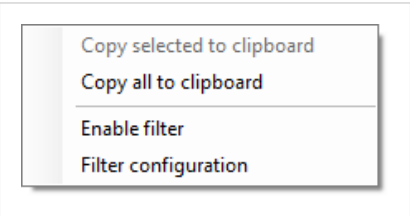
- Fixed console to the left and tabbed browser for the other viewers
- Full tabbed browser

- Clicking and dragging the border of a viewer. To do so, place the cursor over the edge of a viewer. On the vertical edges, the cursor changes to ↔ to adjust the width, and on the horizontal edges, the cursor changes to ↕ to adjust the height.

Viewers can also be arranged manually by clicking and dragging them from their title bar, to use them as independent windows or to position them in relation to other viewers.

FILTERING

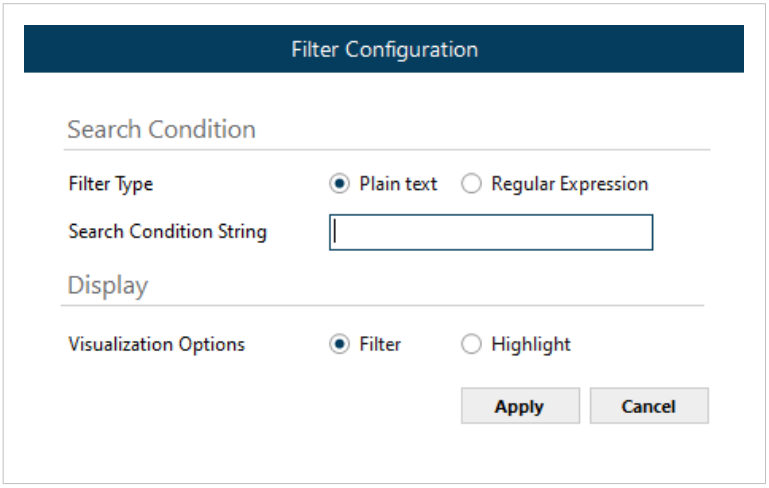
A filtering tool is available for the console and the bus viewers to find the desired information more efficiently. To use this tool, right-click on the viewer.



The options available for this tool are:

- **Copy selected to clipboard**: It copies the selected text into the clipboard. If no text is selected, this option is disabled.
- **Copy all to clipboard**: It copies all the information from the viewer to the clipboard.

- **Enable filter**: This option enables or disables the configured filter. To use this option, a filter must be defined beforehand under Filter configuration.



- **Filter configuration**: The filter itself is defined here, using some additional options:
  - **Search Condition**:
    - **Filter Type**:
      - **Plain text**: It searches all the communication frames that include the text specified in the **Search Condition String** below.
      - **Regular Expression**: It searches all the communication frames that match the regular expression specified in the **Search Condition String** below.

> **NOTE**
> A regular expression is a sequence of characters that specifies a match pattern in text. If you are not familiar with regular expressions, use the **Plain text** option instead.

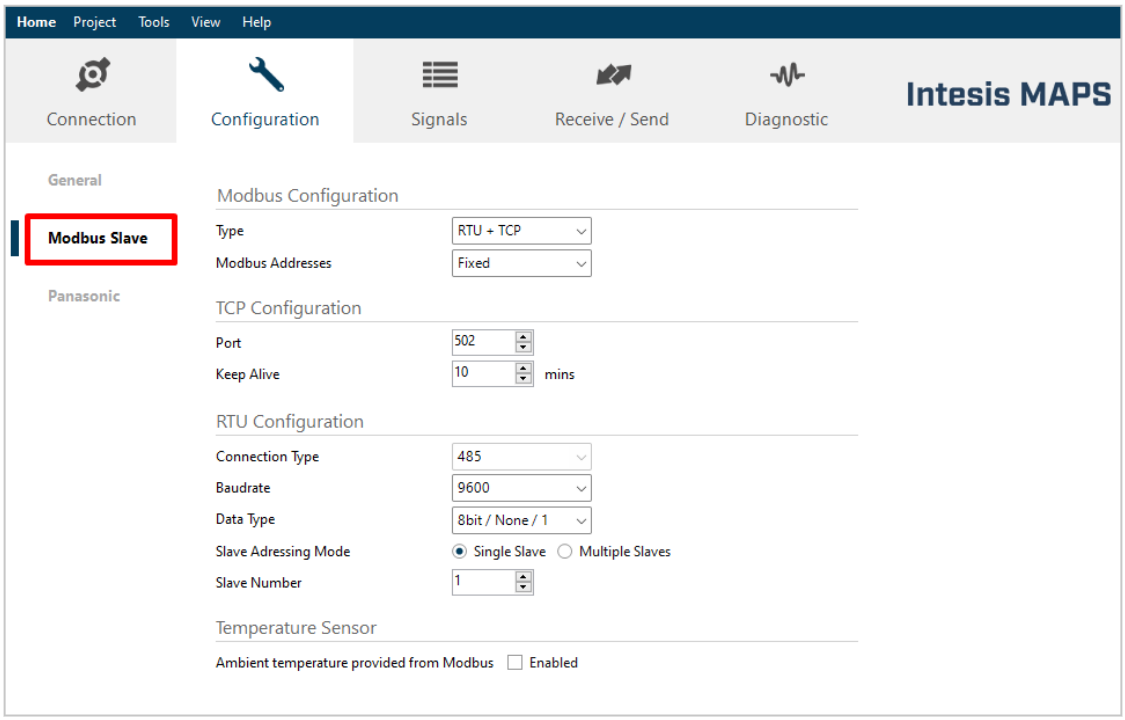
  - **Display**:
    - **Visualization Options**:
      - **Filter**: It removes all the communication frames that do not fulfill the filter condition specified in the **Search Condition String**.
      - **Highlight**: It highlights the communication frames that fulfill the filter condition specified in the **Search Condition String**.

13. BMS Protocols Available

The Intesis IN771AIR00LO000 gateway supports Modbus TCP and RTU, KNX, BACnet/IP and MS/TP, MQTT 3.1.1, and Home Automation communication protocols. The following sections provide the most relevant information for each one.

14. Modbus

Figure 5. Modbus configuration parameters



14.1. Modbus Configuration

- **Type**: Select the communication type.
  - **RTU**: Serial communication over the EIA-485 bus.
  - **TCP**: IP communication over Ethernet.
  - **RTU + TCP**: Simultaneous communication: serial over the EIA-485 bus and IP over Ethernet.
- **Modbus Addresses:** Define the type of Modbus register list.
  - **Fixed:** Addresses cannot be modified.
  - **Custom**: The Modbus register list can be freely edited.

14.2. RTU Configuration

The RTU communication type is configured through the following parameters:

- **Connection type**:
  - **485** (default value): EIA-485 port of the gateway.

> **NOTICE**
> This dropdown menu is locked and cannot be interacted with, because it contains only a single value. Since there are no alternative options to choose from, the menu is disabled to streamline your experience and avoid unnecessary interactions.

- **Baudrate**: Select the communication speed: 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200 bps.

> **NOTE**
> The baud rate is set to 9600 bps by default.

- **Data type**: Select the frame format (Default format: **8bit/None/1**).

Data bits	Parity	Stop bits
8bit	None Even Odd	1 2

- **Slave Addressing Mode**:
  - Select the **Single Slave** option if you have one single server.
  - Select the **Multiple Slaves** option if you have multiple servers.
- **Slave Number**: Set the server starting address (1..255. Default value: **1**).

14.3. TCP Configuration

By selecting TCP as the communication type, you can configure:

- **Port**: Set the port for communication between the gateway and the Modbus TCP system (1..65535).

> **NOTE**
> The default port is 502.

- **Keep Alive**: Set the time in minutes before sending a keep-alive message (1..1440. Default value: **10 minutes**).

> **NOTE**
> Set the parameter to 0 to disable this function.

- **Slave Addressing Mode**:
  - Select the **Single Slave** option if you have one single server.
  - Select the **Multiple Slaves** option if you have multiple servers.
- **Slave Number**: Set the server address (1..255. Default value: **1**).

14.4. Temperature Sensor

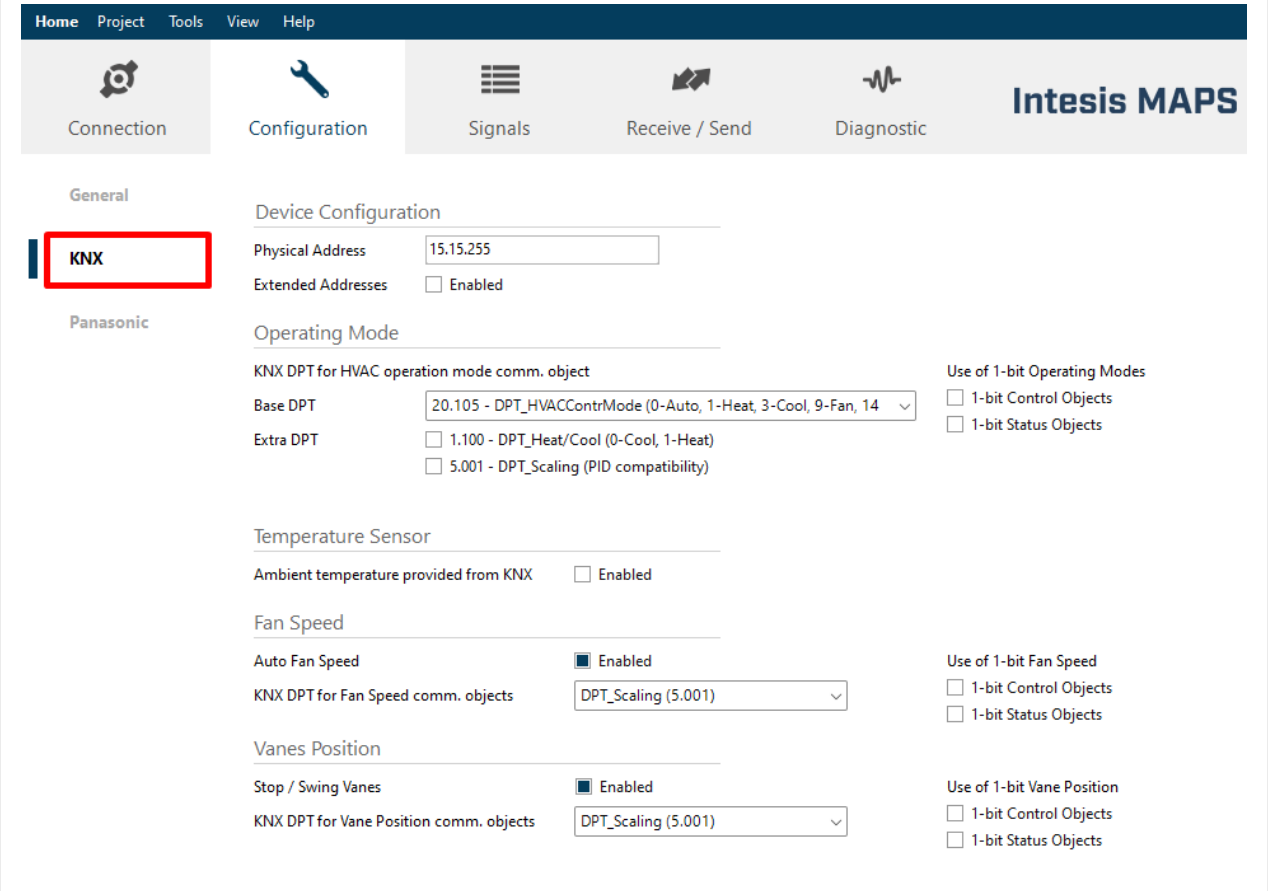
- **Ambient temperature provided from Modbus**: Enables the object **Modbus ambient temperature (x10)** and **AC Real Temperature Setpoint (x10)**, which allow writing the temperature received from a sensor from the Modbus side as the indoor unit reference temperature.
  When enabling this function, the gateway uses a formula to establish which temperature must be sent to the indoor unit:
  $S_{AC} = T_{AC} - (T_{BMS} - S_{BMS})$
  Where:
  - **S_{AC}:** AC indoor unit setpoint temperature.
  - **T_{AC}:** AC indoor unit return temperature.
  - **T_{BMS}:** Ambient temperature provided from Modbus.
  - **S_{BMS}:** Setpoint temperature provided from Modbus.

NOTE
Due to this function, the indoor unit and the Modbus temperature setpoints may differ.

IMPORTANT
When using this function, the user won't be able to use any external device, such as a remote controller, to set the AC indoor unit temperature.

15. KNX

Figure 6. KNX configuration parameters



15.1. Device Configuration

- **Physical Address**: Sets the gateway's KNX physical address in the network. This is a unique identifier for the gateway inside a single KNX TP-1 segment. The maximum value is 15.15.255 (default).
- **Extended Addresses**: Select it to extend the range of available KNX group addresses from the standard 15/7/255 to 31/7/255.

15.2. Operating Mode

These parameters are related to the control and monitoring of the AC unit operating mode.

- **KNX DPT for HVAC operation mode comm. object:**
  - **Base DPT**: Datapoint Type to control and monitor the operating mode.
    - DPT_20.105. DPT_HVACContrMode: 0-Auto, 1-Heat, 3-Cool, 9-Fan, 14-Dry.
    - DPT_5.x (non-standardized): 0-Auto, 1-Heat, 2-Dry, 3-Fan, 4-Cool.
    - Legacy DPT_5.x (non-standardized): 0-Cool, 1-Heat, 2-Fan, 3-Dry, 4-Auto

  - **Extra DPT:** You can enable these additional Datapoint Types:
    - DPT_1.100. DPT_Heat/Cool: 0-Cool, 1-Heat.
    - DPT_5.001. DPT_Scaling (PID compatibility): It enables two objects: **Control_ Heat Mode & On** and **Control_ Cool Mode & On**, whose type is DPT_Scaling (0..100%). They provide compatibility with certain thermostats oriented to the operation of valves for heating and cooling. When these objects receive a value > 0%, the corresponding operating mode (heat or cool) and the status On are sent to the indoor unit. When the value received is 0%, the status sent for the operating mode is Off.

- **Use of 1-bit Operating Modes:**
  - **1-bit Control Objects**: Enables a bit-type object to control each operating mode.
  - **1-bit Status Objects**: Enables a bit-type object for the monitoring of each operating mode.

15.3. Temperature Sensor

- **Ambient temperature provided from KNX**: Enables the object **Control_KNX ambient temperature**, which allows writing the temperature received from a sensor from the KNX side as the indoor unit reference temperature.
  When enabled, the gateway uses a formula to establish which temperature must be sent to the indoor unit:
  $\mathbf{S_{AC} = T_{AC} - (T_{KNX} - S_{KNX})}$
  Where:
  - $\mathbf{S_{AC}}$**:** AC indoor unit setpoint temperature.
  - $\mathbf{T_{AC}}$**:** AC indoor unit return temperature.
  - $\mathbf{T_{KNX}}$**:** Ambient temperature provided from KNX.
  - $\mathbf{S_{KNX}}$**:** Setpoint temperature provided from KNX.

NOTE
Due to this function, the indoor unit and the KNX temperature setpoints may differ.

IMPORTANT
When using this function, the user won't be able to use any external device, such as a remote controller, to set the AC indoor unit temperature.

15.4. Fan Speed

These parameters are related to the control and monitoring of the AC unit fan speed.

- **Auto Fan Speed**: It enables the following additional objects:
  - **Fan Speed AUTO (all units)**: a global object for all units.
  - **Control_Fan speed Man/Auto**: an individual control object for each enabled unit.
  - **Status_Fan speed Man/Auto**: an individual status object for each enabled unit.
- **KNX DPT for Fan Speed comm. objects:**
  - **DPT_Scaling (5.001):** Percentage values are used to control/monitor the fan speed. Their value will vary according to the number of fan speeds available for the unit.
  - **DPT_Value_1_Ucount (5.010)**: Enumerated values are used to control/monitor the fan speed.
- **Use of 1-bit Fan Speed:**
  - **1-bit Control Objects**: Enables a bit-type object to control the fan speed.
  - **1-bit Status Objects**: Enables a bit-type object for the monitoring of each fan speed.

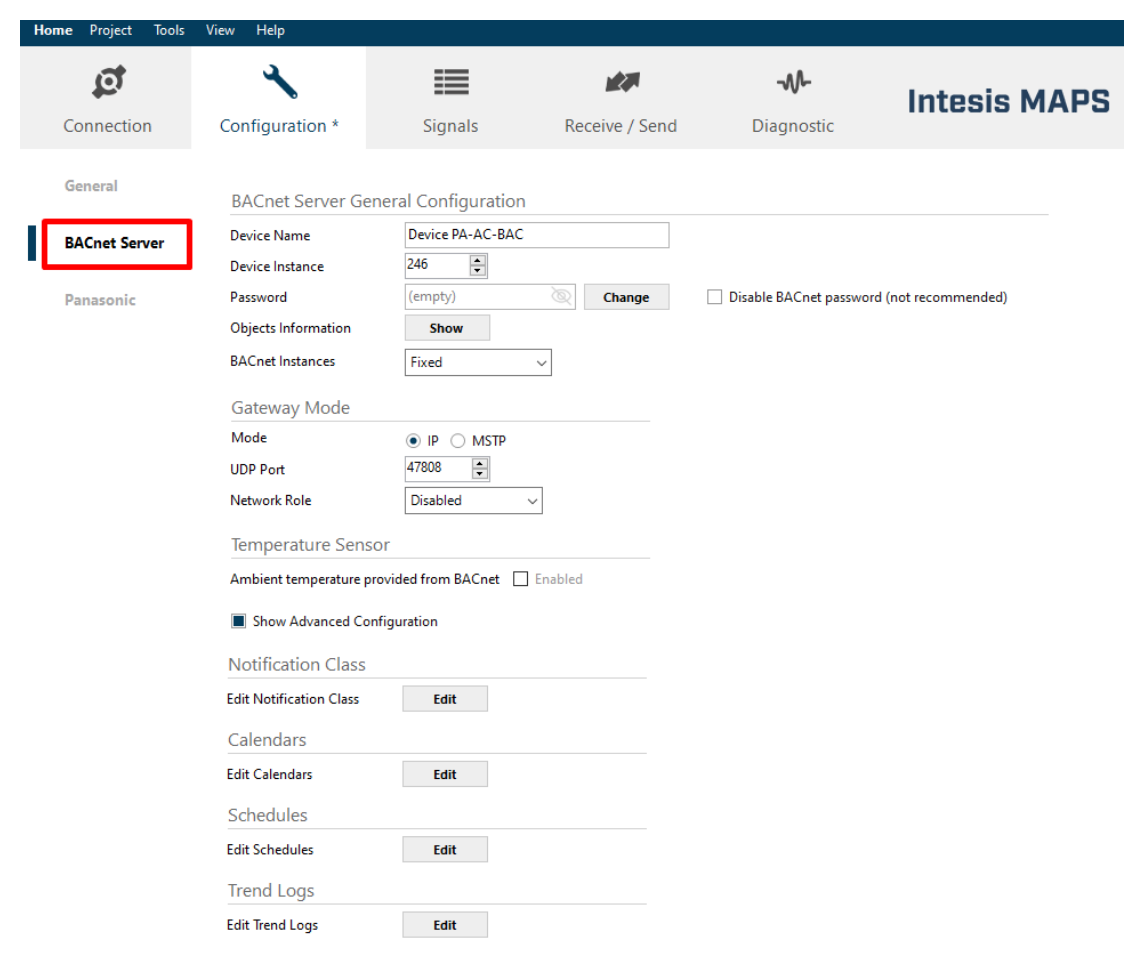
15.5. Vanes Position

These parameters are related to the control and monitoring of the AC unit vanes position.

- **Auto / Swing Vanes**: It enables Auto and Swing control and monitoring objects.
- **KNX DPT for Vane Position comm. objects**:
  - **DPT_Scaling (5.001):** Percentage values are used to control/monitor the vanes position. Their value will vary according to the number of positions available for the unit.
  - **DPT_Value_1_Ucount (5.010)**: Enumerated values are used to control/monitor the vanes position.
- **Use of 1-bit Vane Position:**
  - **1-bit Control Objects**: Enables a bit-type object to control the vanes position.
  - **1-bit Status Objects**: Enables a bit-type object for the monitoring of each vanes position.

16. BACnet

Figure 7. BACnet configuration parameters



16.1. BACnet Server General Configuration

- **Device Name**: Type a descriptive name for your gateway.
- **Device Instance**: Set the BACnet device object instance property. This is a unique identifier for the gateway inside a single BACnet network segment (0..4194302. Default value: **246**).
- **Password**: Click the **Change** button and follow the instructions to set a password for the gateway.
- **Objects Information**: Click **Show** to see a table with the type of objects available.
- **BACnet Instances:** Define the type of BACnet instances.
  - **Fixed:** Instances cannot be modified.
  - **Custom**: The BACnet instances list can be edited.
- **Disable BACnet password (not recommended)** (parameter disabled by default): Disable the BACnet password.

IMPORTANT
Keep the BACnet password enabled to ensure the security of the gateway and the installation.

16.2. Gateway Mode

- **Mode**: Select the communication type.
  - **IP** (default value): IP communication over Ethernet.
    - **UDP Port**: Select the UDP port for the BACnet/IP communication (1..65535).

      NOTE
      The UDP port is set to 47808 (BAC0 in hexadecimal) by default.

    - **Network Role** (disabled by default): Define the gateway behavior regarding other network elements.

      IMPORTANT
      If you are unfamiliar with these options, please leave the parameter as **Disabled** to avoid issues with the BACnet communication/configuration.

      - **Disabled**: The gateway provides no special service regarding network communication or settings.
      - **Foreign Device**: The gateway acts as a foreign device from the BACnet network point of view.
      - **BBMD**: The gateway acts as a BBMD in the BACnet network.
  - **MS/TP**: Serial communication over the EIA-485 bus.
    - **Baud rate**: Select the communication speed: Auto, 9600, 19200, 38400, 57600, 76800, or 115200 bps.

      NOTE
      The baud rate is set to Auto by default.

    - **Max. Masters**: Set the highest master MAC address in the MS/TP network (1..127. Default value: **127**).
    - **Max. Info Frames**: Set the maximum number of messages that can be sent onto MS/TP network per token pass (1..100. Default value: **1**).
    - **MAC Address**: Set the MAC address of the gateway in the MS/TP network (0..127. Default value: **1**).

16.3. Temperature Sensor

- **Ambient temperature provided from BACnet**: Enables the object **BACnet ambient temperature**, which allows writing the temperature received from a sensor from the BACnet side as the indoor unit reference temperature.
  When enabling this function, the gateway uses a formula to establish which temperature must be sent to the indoor unit:
  $S_{AC} = T_{AC} - (T_{BMS} - S_{BMS})$
  Where:
  - S_{AC}: AC indoor unit setpoint temperature.
  - T_{AC}: AC indoor unit return temperature.
  - T_{BMS}: Ambient temperature provided from BACnet.
  - S_{BMS}: Setpoint temperature provided from BACnet.

NOTE
Due to this function, the indoor unit and the BACnet temperature setpoints may differ.

IMPORTANT
When using this function, the user won't be able to use any external device, such as a remote controller, to set the AC indoor unit temperature.

16.4. BACnet Advanced Configuration

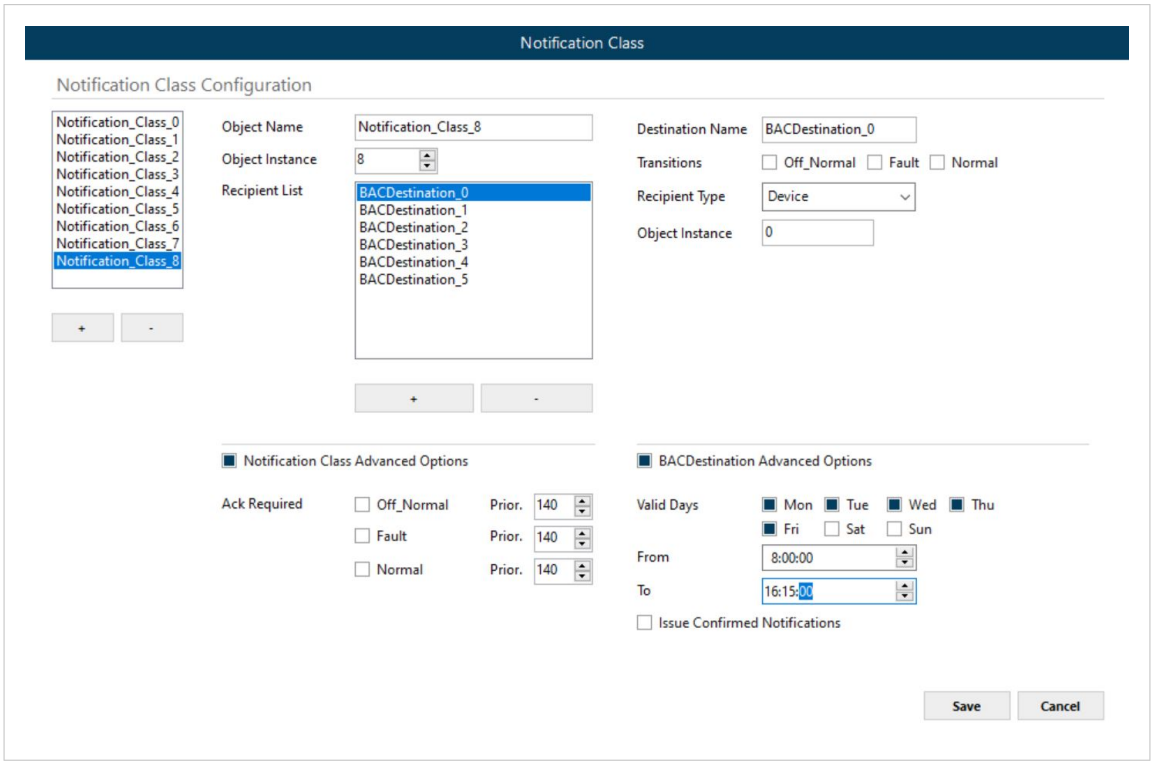
Show Advanced Configuration: Open advanced configuration parameters (disabled by default).

IMPORTANT
These menus provide advanced functionalities intended for expert users.

We recommend keeping these options set to their default values.

16.4.1. Notification Class

Click **Edit** to open the **Notification Class Configuration** parameters.



Click the + button to create up to ten Notification_Class objects. For each one, you can set:

- **Object Name**: Type a name for the Notification_Class.
- **Object Instance**: Set the BACnet object instance for the Notification_Class.
- **Recipient List**: Click the + button to create up to eight different BACnet destinations. For each one, you can set:
  - **Destination Name**: Type a descriptive name for the BACnet destination.
  - **Transitions**: Select which transitions will force this Notification_Class to be active:
    - **Off_Normal** (disabled by default): When the status changes from off to normal.
    - **Fault** (disabled by default): When the status changes to fault.
    - **Normal** (disabled by default): When the status changes from fault to normal.

  - **Recipient Type**: Select the type of destination:
    - **Device** (default value): The recipient is a device.
      - **Object Instance**: Select the device instance number for this device.
    - **Address (IP)**: The recipient is set using the specific address on BACnet/IP. Specify:
      - **Network Number** (0 .. 65535. Default value: **0**).
      - **IP** address (192.168.100.10 by default) and **Port** (47808 by default) for the destination.
      - Set the destination as a **Global Broadcast** (disabled by default).
      - Set the destination as a **Broadcast** (disabled by default).
    - **Address (MS/TP)**: The recipient is set using the specific address on BACnet MS/TP. You'll have to specify:
      - **Network Number** (0..65535. Default value: **0**).
      - **MS/TP MAC Address** (0..255. Default value: **0**).
      - Set the destination as a **Global Broadcast** (disabled by default).
      - Set the destination as a **Broadcast** (disabled by default).
    - **Address (Other):** The recipient is set using another type of address. You'll have to specify:
      - **Network Number** (0..65535. Default value: **0**).
      - **Other Address** (HEX string. Default value: **ff**).
      - Set the destination as a **Global Broadcast** (disabled by default).
      - Set the destination as a **Broadcast** (disabled by default).
- **BACDestination Advanced Options** (disabled by default): Check this option to show some advanced options.
  - **Valid days:** Sets the days for receiving the notification.
  - **From**: Sets the starting point for the valid period.
  - **To**: Sets the ending point for the valid period.
  - **Issue Confirmed Notifications** (disabled by default): Determines if notification events are sent as Confirmed or Unconfirmed to the BACnet destination.

    IMPORTANT
    Sending them as Confirmed requires Ack.

- **Notification Class Advanced Options** (disabled by default): Check this option to show the **Ack Required** options.
  - **Off_Normal** (disabled by default): Enable the acknowledgment for the TO_OFF_NORMAL event.
  - **Fault** (disabled by default): Enable the acknowledgment for the TO_FAULT event.
  - **Normal** (disabled by default): Enable the acknowledgment for the TO_NORMAL event.

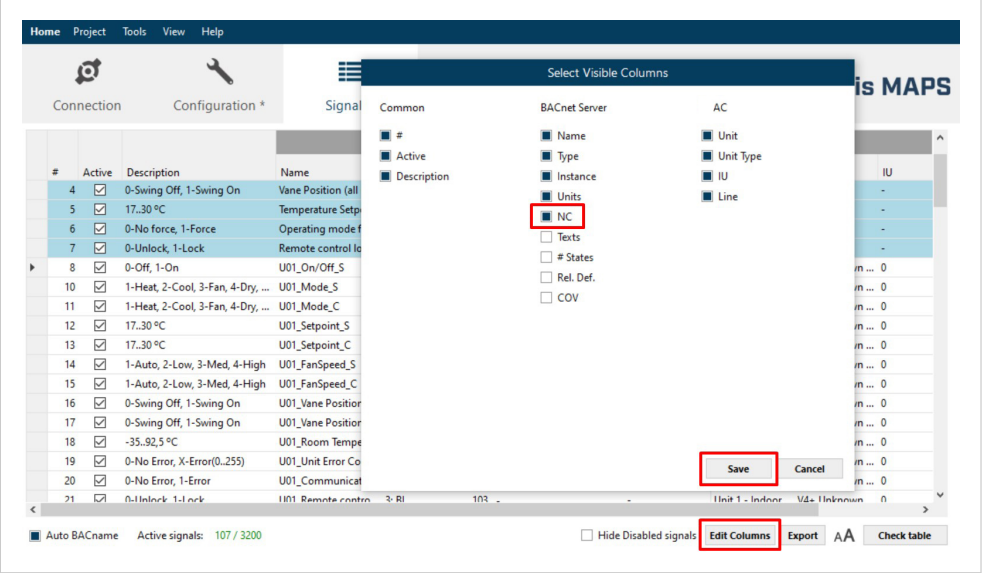
NOTE
Set the priority for each parameter (0..255. Default value: **140**).

After creating and configuring the needed Notification_Class objects, the next step is to assign them to signals:

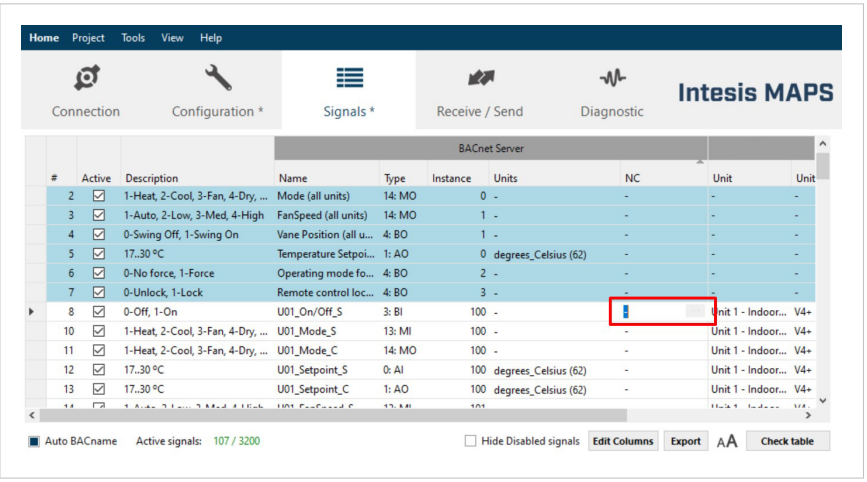
NOTICE
To better understand the assignment of Notification_Class objects to signals, we are moving from the **Configuration** tab to the **Signals** tab.

1. Go to the **Signals** tab.

2. Click the **Edit Columns** button from the bottom menu.

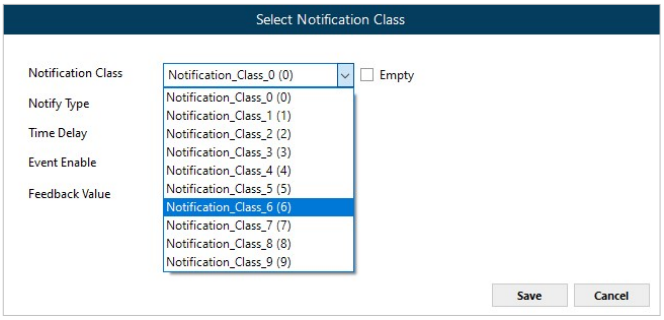


3. In the **Select Visible Columns** window, select **NC**.
4. Click **Save**.
   A new column named **NC** is now visible.
5. Look for the signal to which you want to assign the Notification_Class object and click the corresponding cell in the NC column.



6. Click the ... button.
7. In the **Select Notification Class** window, uncheck the **Empty** parameter.

8. Use the dropdown menu to select the Notification_Class object.



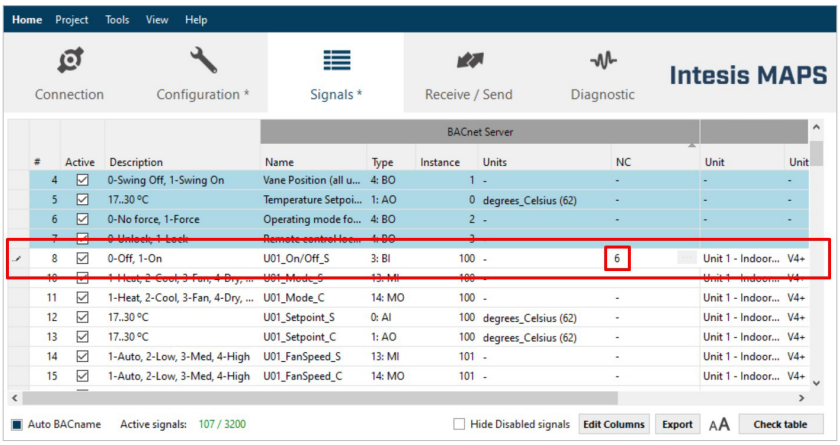
9. Set the rest of the parameters:

> **NOTE**
> These parameters vary depending on the signal type.

- **Notify Type**: Choose if the notification is sent as an **Alarm** (default) or an **Event**.
- **Time Delay**: Set the time in seconds before the notification launch (0 .. 65535. Default value: **0 seconds**).
- **Event Enable**: Click in the field to enable/disable the following options:
  - **TO_OFF_NORMAL** (enabled by default): Enable/disable the TO_OFF_NORMAL event.
  - **TO_FAULT** (enabled by default): Enable/disable the TO_FAULT event.
  - **TO_NORMAL** (enabled by default): Enable/disable the TO_NORMAL event.
- **Initial Feedback Value**: Set the initial feedback value (1..5. Default value: **2**)
- **Alarm Value**: Choose if the alarm value is **Active** or **Inactive** (default).
- **Alarm Value LUT**: Set an alarm value look-up table collection (use commas to separate values).
- **Fault Value LUT**: Set a fault value look-up table collection (use commas to separate values).
- **Feedback Value:** Choose if the feedback value is **Active** or **Inactive** (default).
- **High Limit** (Disabled by default): Enable this parameter to set the high limit for the notification.
- **Low Limit** (Disabled by default): Enable this parameter to set the low limit for the notification (0.00..999.00).
- **Deadband**: Set the deadband for the notification.

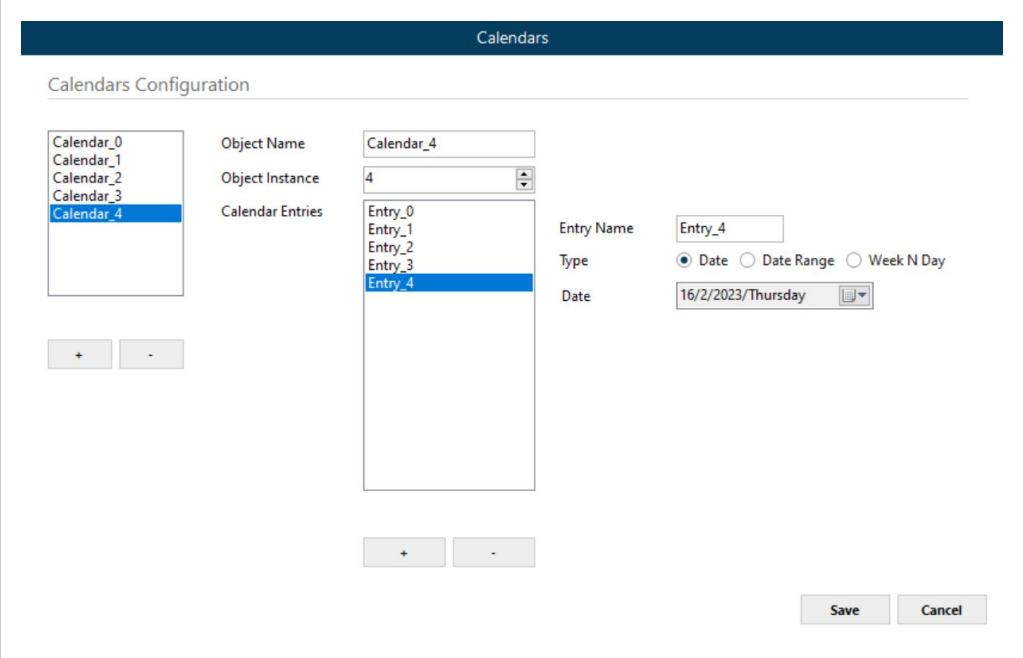
10. Click **Save** to save the changes.

Once assigned, the instance number of the Notification_Class object appears in the **NC** column.



16.4.2. Calendars

Click **Edit** to open the **Calendars Configuration** parameters.



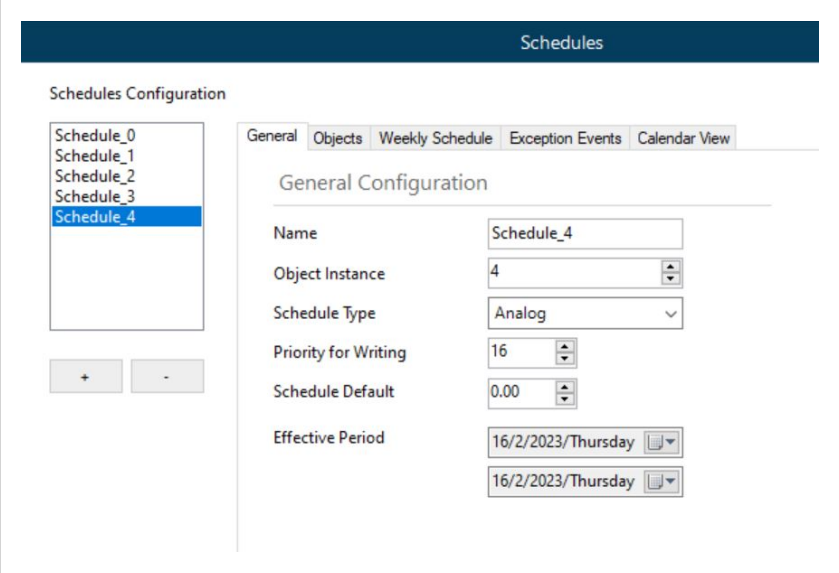
Click the + button to create up to 10 calendars. For each one, you can set:

- **Object Name**: Type a name for this calendar.
- **Object Instance**: Set the BACnet object instance for the calendar (0..4194303. Default value: **0**).
- **Calendar Entries**: Click the + button to determine the number of calendar entries (patterns). Create up to 32 different entries per calendar. For each entry, you can set:
  - **Entry Name**: Type the name for that pattern.
  - **Type**: Set the date type for that pattern:
    - **Date** (default value): The pattern applies to a specific day.
    - **Date Range**: The pattern applies within a date range. Set the starting day (**From**) and the ending day (**To**).
    - **Week N Day**: The pattern applies to a specific **Month**, **Week of the Month**, and/or **Day of the Week**.

> **NOTE**
> Select an asterisk (*) to apply the rule to all cases, i.e., an asterisk in the **Month** option will make the pattern apply to every month.

16.4.3. Schedules

Click **Edit** to open the **Schedules Configuration** parameters.



Click the + button to create up to ten schedules. For each one, you can set:

- **General Configuration**:
  - **Name**: Type a name for this schedule.
  - **Object Instance**: Set the BACnet object instance for the schedule (0 .. 4194303. Default value: **0**).
  - **Schedule Type**: Set it as an **Analog** (default), **Binary**, or **Multistate** object.

    IMPORTANT
    Use the type that best suits this particular schedule. For example, if this schedule is used to turn a device ON, select **Binary**.

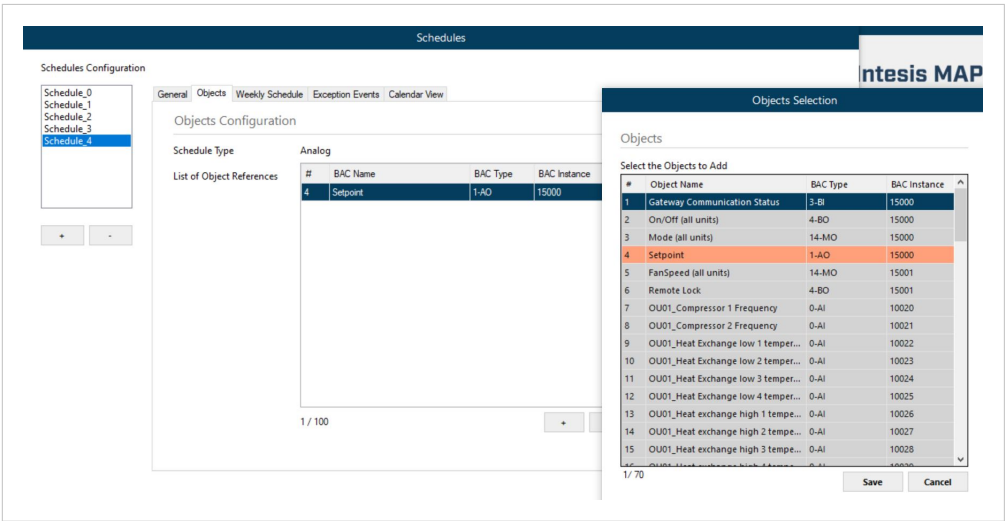
  - **Priority for Writing**: Select the writing priority of the schedule value (1..16. Default value: **16**).
  - **Schedule Default**: Set the default value for the schedule.

    NOTICE
    The range of values allowed depends on the type of object previously selected:

    - **Analog**: 0.00..65535.00
    - **Binary**: 0, 1
    - **Multistate**: 0..65535

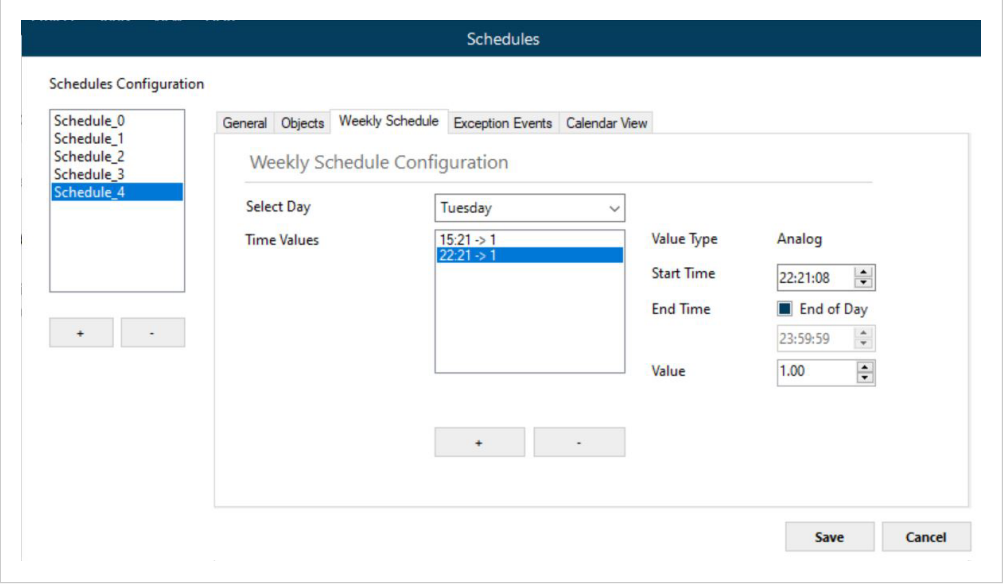
  - **Effective Period**: Set the starting and ending date. The schedule will be in effect during this period.

- **Objects Configuration**: Include BACnet objects in a specific schedule.



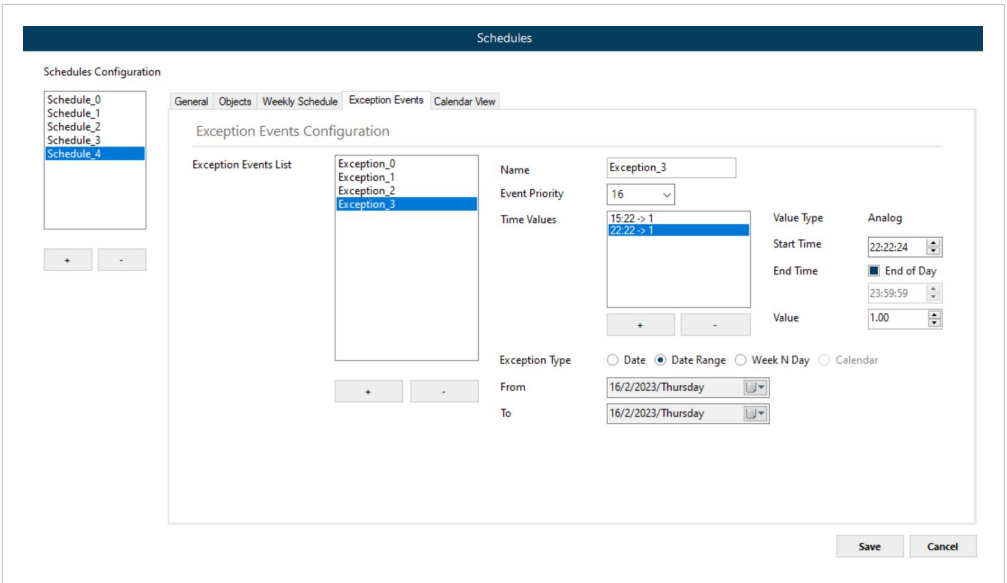
  - **Schedule Type**: It shows the previous **Schedule Type** object you selected: Analog, Binary, or Multistate.
  - **List of Object References**: Click the + button to open the **Objects Selection** dialog. The background color of each object indicates its status as follows:
    - **Grey**: Not allowed. This object type does not match the **Schedule Type** you previously selected.
    - **Yellow**: Allowed.
    - **Orange**: Already applied.

- **Weekly Schedule Configuration:**



  - **Select Day**: Select which day of the week the schedule applies.
  - **Time Values**: Click the + button to create up to six time periods. For each one, set the **Start Time**, the **End Time**, and the **Value**.

- **Exception Events Configuration**: Create exceptions to the schedules.



– **Exception Events List**: Click the + button to create up to 16 different exceptions. For each one, you can set:

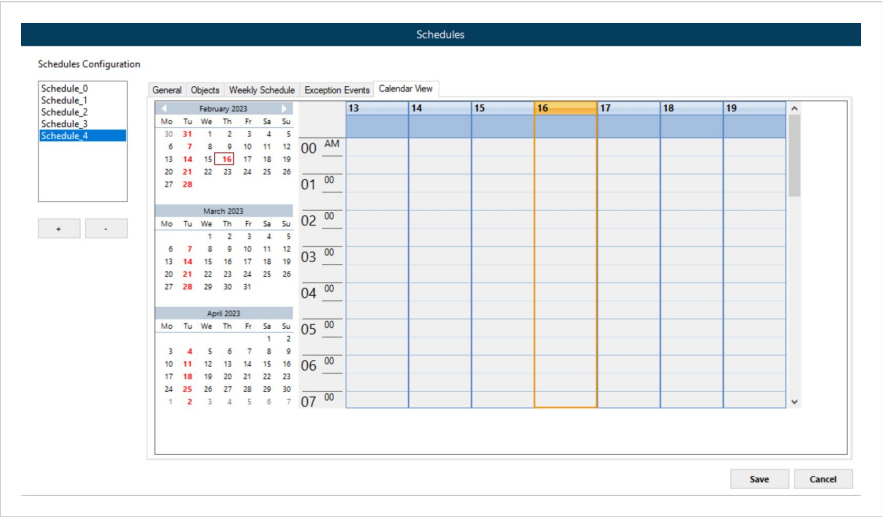
- **Name**: Type a name for the exception.
- **Event Priority**: Set a priority for the exception (1 [maximum priority] .. 16 [minimum priority]. Default value: **16**).
- **Time Values**: Click the + button to create up to six time periods. For each one, set the **Starting Time**, the **End Time**, and the **Value**.
- **Exception Type**: Set the type of date for the exception:
  – **Date** (default): Select a single day.
  – **Date Range**: Select a date range. Set the starting day (**From**) and the ending day (**To**). The exception will be in effect during this period.
  – **Week N Day**: Set the date by selecting a **Month**, a **Week of the Month**, and/or a **Day of the Week**.

> **NOTE**
> Select an asterisk (*) to apply the rule to all cases.

  – **Calendar**: Select a Calendar to apply its values to the exception event.

> **NOTE**
> This option is only enabled when at least one Calendar has been previously created. See Calendars (page 51).

- **Calendar View**: Display a calendar to consult all the configured schedules.

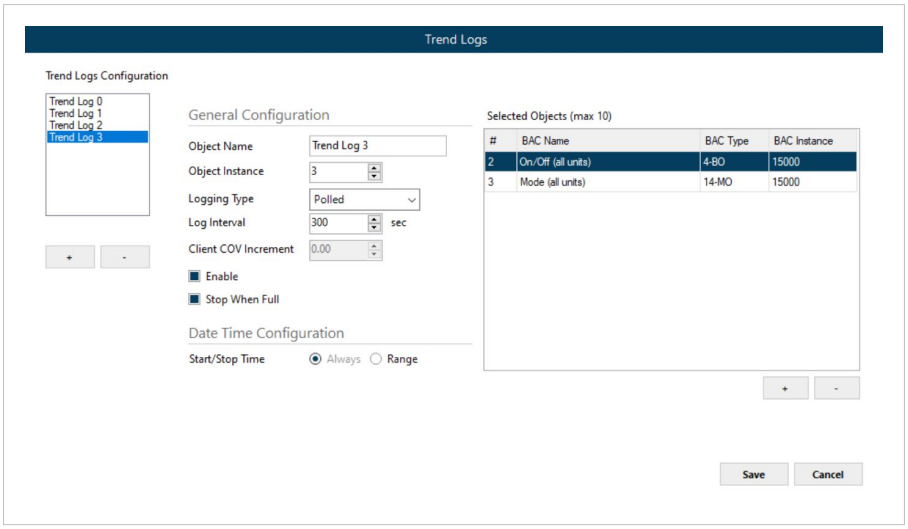


You can also create and modify **Weekly** and **Exception** schedules from this menu:

1. Use the calendar miniatures on the left to select the desired week.
2. Use the schedule view on the right to select the desired day and hour.
3. Right-click to open the settings menu. From this menu, the following options are available:
   - **Create Weekly Schedule**: Create a new weekly schedule.
   - **Create Exception Schedule**: Create a new exception event.
   - **Settings**: Edit an already created weekly schedule or exception event.
   - **Delete Event**: Delete the selected weekly schedule or exception event.

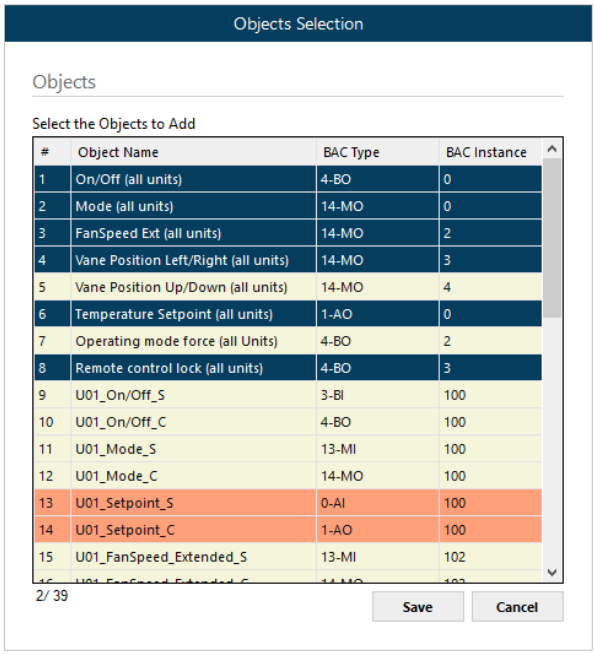
16.4.4. Trend Logs

Click **Edit** to open the **Trend Logs** parameters.



Click the + button to create up to five trend logs. For each one, you can set:

- **Object Name**: Type a name for the trend log.
- **Object Instance**: Set the BACnet object instance for the trend log (0..4194303. Default value: **0**).
- **Logging Type**: Select the trend log type:
  - **Polled** (default value): The trend log is triggered when polling.
    Use the **Log Interval** parameter to set the poll cadence in seconds (1..65535. Default value: **300 sec**).
  - **COV**: The trend log is triggered when there is a change of value.
    Use the **Client COV Increment** parameter to set (0.00..100000.00. Default value: **0.00**).
  - **Triggered**: The trend log is triggered by the BACnet system.
- **Enable** (enabled by default): Enable/disable the specific trend log even if the trend log is in the valid time range.
- **Stop When Full** (enabled by default):
  - If **enabled**, it will stop the trend log when the buffer is full.
  - If **disabled**, it will keep the last 2880 valid values.
- **Date Time Configuration**: Set the period when trend logs are active.
  - **Always** (default value).
  - **Range**: Use the **Start Time** and **End Time** parameters to set a time range.
- **Selected Objects (max 10)**: Click the + button to include up to ten BACnet objects in a trend log. To remove previously added objects, use the − button.



NOTE
To select multiple items in both the **Selected Objects** and the **Objects Selection** tables, press and hold the **Shift** key when clicking for consecutive objects or the **Control** key for non-consecutive objects. Objects that have already been added are displayed with an orange background.

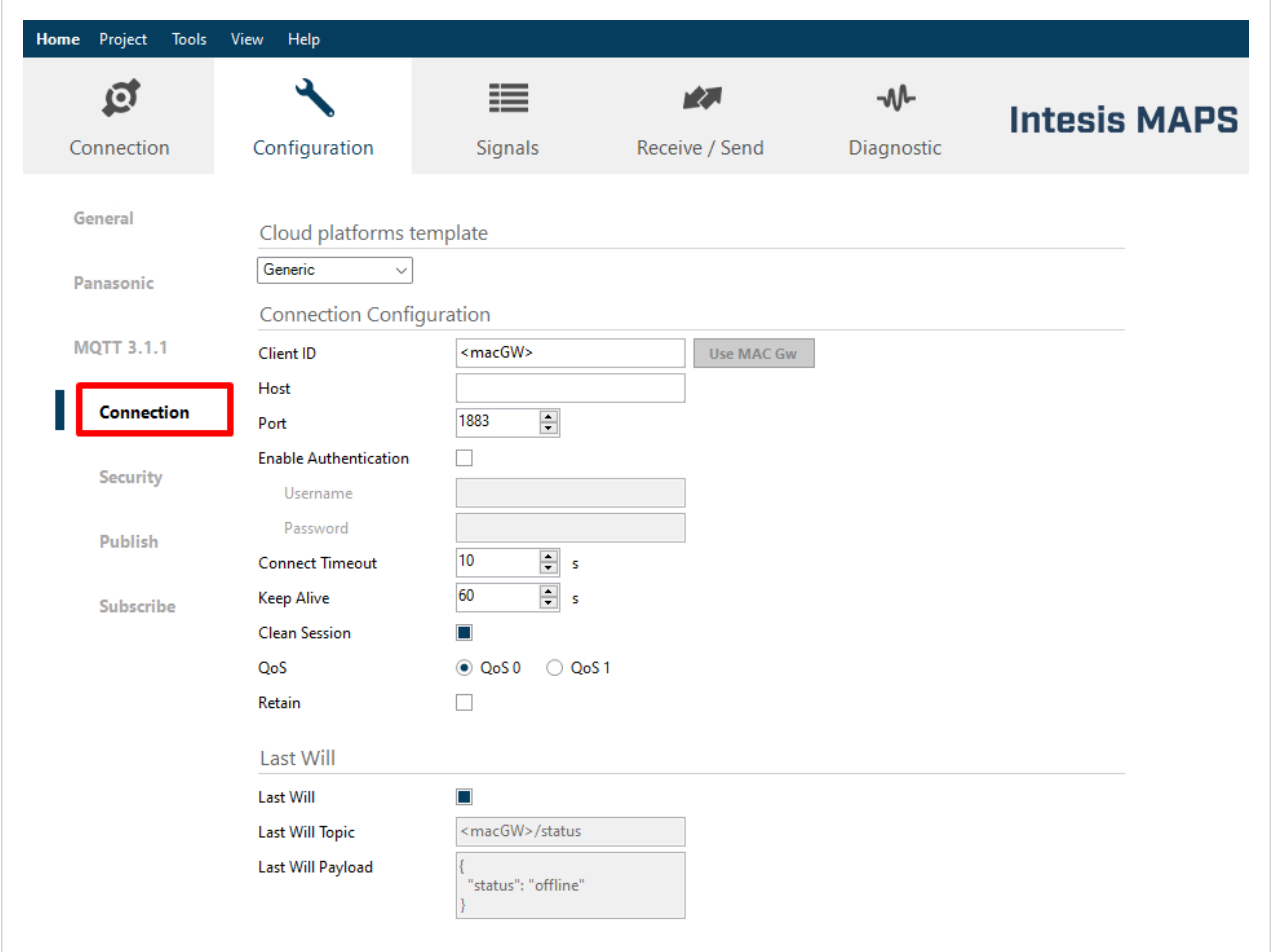
17. MQTT 3.1.1

The following configuration sections are used for MQTT:

- **Connection**: Parameters required to establish a connection with the MQTT broker.
- **Security**: This section enables secure communication via SSL/TLS, along with certificate management and renewal for authentication purposes.
- **Publish**: The signals used by the gateway to share its status information are listed here.
- **Subscribe**: These are the signals to which the gateway is subscribed. Therefore, these are the commands that the gateway can receive.

17.1. Connection

Figure 8. MQTT 3.1.1 connection parameters



17.1.1. Cloud Platforms Template

Select the cloud platform the gateway will establish a connection with:

- **Azure IoT Hub**: A service from Microsoft for securely connecting, managing, and monitoring IoT devices at scale.
- **AWS IoT Core**: A platform from Amazon for real-time device communication, management, and integration with AWS services.
- **Generic** (default value): Select this option if you are not using either of the platforms listed above.

17.1.2. Connection Configuration

- **Client ID**: A unique identifier for the gateway as an MQTT client. A simple way to ensure the uniqueness of the client ID is to use the MAC address of the gateway. To do so, press the **Use MAC Gw** button.
- **Host**: The IP address or the hostname of the MQTT broker. Enter the corresponding value as given by your service provider.
- **Port**: TCP port used to establish a connection (0..65535. Default value: **1883**).

NOTICE
The default ports defined for MQTT by convention are:

- **Port 1883**: Unencrypted communication. Data, including credentials, travels in plaintext, which can be intercepted if the network is compromised.
- **Port 8883**: Secure communication over TLS. Data, including credentials, is encrypted in transit, reducing the risk of interception or tampering even if the network is compromised. This port is required for the Azure IoT Hub platform.

Changes in the **Enable SSL/TLS** parameter of the **Security** section will modify this value automatically. Consult the Security (page 60) section for more information.

WARNING
Regardless of the port used, make sure that traffic through that port is allowed. As a general rule, the connection from the gateway to the broker must be fully permitted according to the configuration defined at the gateway.

For the reasons explained above, using secure communication is strongly recommended.

NOTICE
For secure operation in restricted networks, the gateway supports MQTT over TLS on port 443 using ALPN with brokers that provide this option (e.g., AWS IoT Core). For more information about the ALPN extension, refer to the Basic Configuration (page 61) section.

- **Enable Authentication**: Check this checkbox if the MQTT broker requires the use of credentials. Once checked, the following fields are enabled:
  - **Username** (required): The string used by the MQTT client to identify itself to the broker during authentication. Must match the credentials configured on the broker and is case-sensitive (max. 29 characters)
  - **Password**: The secret string used by the MQTT client to authenticate with the broker in combination with a username. It must match the credentials configured on the broker and is transmitted during the connection process. The use of a password may be optional depending on the broker's authentication settings.

NOTICE
Authentication over unencrypted MQTT is technically supported, but not secure. In that case, credentials such as usernames and passwords are transmitted in plain text, making them vulnerable to interception. For secure authentication, it is strongly recommended to use encrypted connections via SSL/TLS, which protect both credentials and data.

- **Connect Timeout**: Set the maximum time, in seconds, that the gateway will wait for an acknowledgement from the MQTT broker when attempting a connection (0..65535 seconds (18 hours 12 minutes and 15 seconds). Default value: **10 seconds**).

NOTICE
A value of 0 means the gateway will wait indefinitely.

- **Keep Alive**: Set the maximum time interval, in seconds, that is permitted to elapse between messages sent by the client to the broker (0..65535 seconds (18 hours 12 minutes and 15 seconds). Default value: **60 seconds**).

NOTICE
A **Keep Alive** value of zero effectively disables the keep alive mechanism. This means the MQTT broker is not required to disconnect the client due to inactivity. However, it is important to note that the broker is still entitled to disconnect the client at any time, regardless of the **Keep Alive** setting. This could be due, for example, to internal policies, resource constraints, or network issues.

- **Clean Session** (enabled by default): Determines whether the broker should treat each client connection as a new session or resume a previous one.
  - When enabled, the broker does not retain any session state (like subscriptions or undelivered messages) after the client disconnects.
  - When disabled, the broker retains session information, allowing the client to resume where it left off.

IMPORTANT
This setting cannot be disabled when using the Azure IoT Hub template.

- **QoS**: Set the Quality of Service (QoS) level for the overall communication. Two options are available:
  - **QoS 0** (default value): The MQTT broker sends messages once, with no acknowledgement. If delivery fails, the message is lost.
  - **QoS 1**: The MQTT broker ensures that messages are delivered at least once, requiring acknowledgment from the gateway. Duplicates may occur.

IMPORTANT
QoS 1 cannot be selected when using the Azure IoT Hub template.

- **Retain** (disabled by default): Determines whether published messages should be stored by the broker and delivered to future subscribers of the topic.

IMPORTANT
The **Retain** setting is not available when using the Azure IoT Hub template.

17.1.3. Last Will

An MQTT **Last Will** is a message that the gateway, as a client, asks the MQTT broker to publish on its behalf to an specific topic if it disconnects unexpectedly. By doing this, any other client subscribed to this topic will be notified of the disconnection.

IMPORTANT
The **Last Will** feature is not available when using the Azure IoT Hub template.

- **Last Will** (enabled by default): Determines whether a **Last Will** message will be transmitted to the broker. When enabled, this message is composed of the following fixed elements:
- **Last Will Topic**: Where the broker will publish the message if the gateway disconnects unexpectedly.

NOTICE
The topic used by the gateway for this function is: **<macGW>/status**, with the first node being the **client ID** of the gateway.

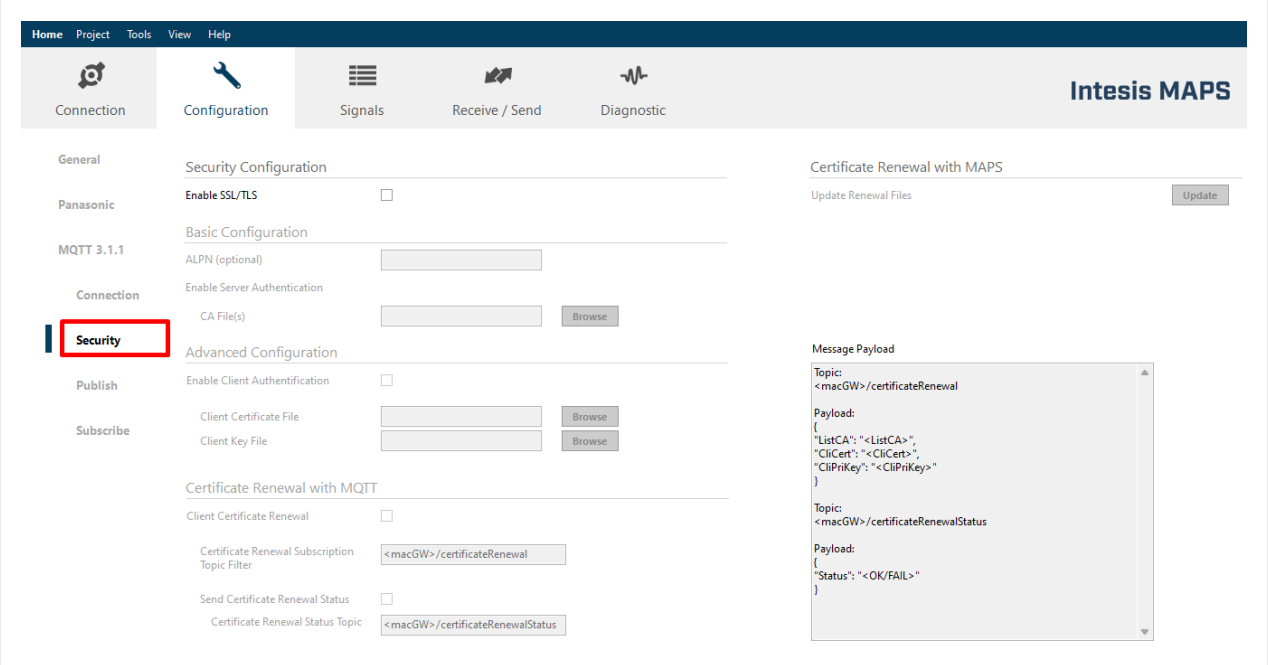
- **Last Will Payload**: The content of the message to publish.

NOTICE
The message provided by the gateway is handled in JSON format.

```
Payload:
{
    "status": "offline"
}
```

17.2. Security

Figure 9. MQTT 3.1.1 Security parameters



17.2.1. Security Configuration

Use this checkbox to enable or disable secure communication through SSL/TLS.

NOTICE
Changes in this setting will modify the **Port** value of the **Connection Configuration** section automatically:

- Checking the checkbox sets the port value to **8883**.
- Unchecking the checkbox sets the port value to **1883**.

When secure communication is enabled, the following subsections are also activated to provide the necessary certificates and additional settings.

17.2.2. Basic Configuration

- **ALPN (optional)**: If required, enter the string of text known as ProtocolName that identifies an application-layer protocol (like MQTT) during the TLS (Transport Layer Security) handshake, as defined by the ALPN extension.

  NOTICE
  As an example, the ALPN ProtocolName for AWS IoT Core is **x-amzn-mqtt-ca**.

- **Enable Server Authentication**: Use this option to allow the gateway, acting as a client, to verify the broker's identity using one or more CA files provided by the MQTT broker. When enabled, use the **Browse** button in the **CA File(s)** field below to select one or more certificates.

  NOTICE
  The number of required CA files may vary depending on the MQTT broker. Up to five CA files can be attached. To select multiple certificate files in the dialog file, use **Shift + click** for consecutive files or **Control + click** for non-consecutive files.

17.2.3. Advanced Configuration

- **Enable Client Authentication**: Use this option to allow the gateway to be authenticated by the broker. Two separate files, provided by the MQTT broker, are used for this purpose:
  - **Client Certificate File**: The public identity of the client. When the gateway connects securely to an MQTT broker, it presents this certificate to prove who it is.
  - **Client Key File**: The secret counterpart to the client certificate. It is used to digitally sign parts of the TLS handshake, proving that the gateway (as an MQTT client) owns the certificate.

  Use the **Browse** buttons on each section to upload the corresponding files.

IMPORTANT
Enabling client authentication but skipping server authentication allows the client to identify itself securely but not verify who it is talking to. This is a risky scenario that should be avoided unless you are in a fully trusted network. For more information about server authentication, refer to the previous section.

17.2.4. Certificate Renewal with MQTT

IMPORTANT
This feature is not available when using the Azure IoT Hub template.

- **Client Certificate Renewal**: It is possible for the renewal of the client certificates to occur directly via MQTT. In this case, the gateway subscribes to a predefined topic through which it receives the updated certificate. This topic structure can be seen in the following field:
  - **Certificate Renewal Subscription Topic Filter**: The topic used for the subscription is: **<macGW>/certificateRenewal**.

    IMPORTANT
    For the update to take place, the corresponding topic or filter must be correctly defined and configured on the MQTT broker side. Check your MQTT broker documentation for more information.

- **Send Certificate Renewal Status**: When **Client Certificate Renewal** is enabled, the gateway can publish to another predefined topic to communicate whether the renewal process has been successful (**OK**) or unsuccessful (**FAIL**). This topic structure can be seen in the following field:
  - **Certificate Renewal Status Topic**: The topic used for this publication is: **<macGW>/certificateRenewalStatus**.

  Any client subscribed to this topic will receive this information whenever an update takes place.
- **Message Payload**: This uneditable text field lists the two topics related to the renewal of certificates and the status of the renewal process, together with their corresponding payloads. Use this information to define the corresponding topics in the MQTT broker. (you can copy and paste directly).

17.2.5. Certificate Renewal with MAPS

In addition to updating the certificates remotely, as described in the previous section, it is also possible to update the certificate files on the gateway locally. To do so, press the **Update** button on **Update Renewal Files**.

NOTICE
Before proceeding, make sure that all needed files are already uploaded in their corresponding sections.

This procedure does not apply any change to the current gateway configuration besides replacing the existing certificates on the gateway with the ones selected in the corresponding Security subsections. To update the project configuration as a whole, see Receive/Send Tab (page 32).

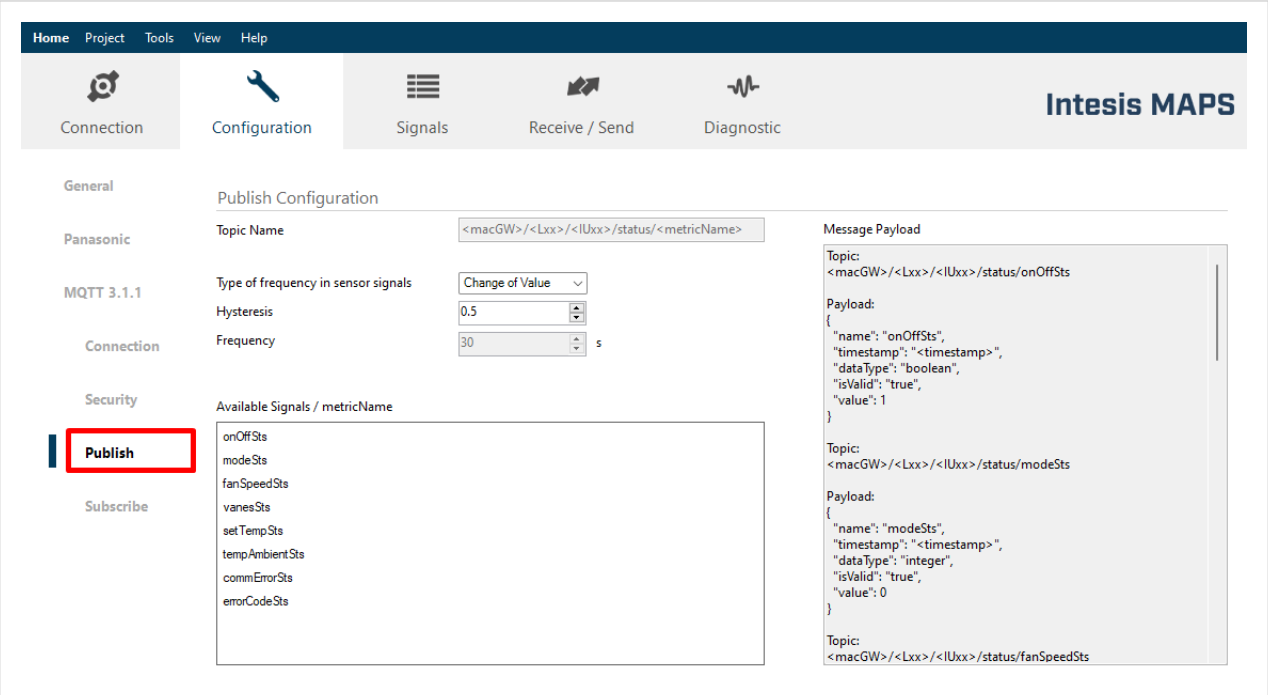
Two confirmation dialogs appear before proceeding with the update. The update can be stopped by clicking **Cancel** in either of these dialogs.

IMPORTANT
Always keep a backup of your certificate files in a safe location before making any changes.

Once the process is complete, a message will appear to confirm the success or failure of the process. Should the process not be completed successfully, review the certificate files and try again.

17.3. Publish

Figure 10. MQTT 3.1.1 Publish parameters



17.3.1. Publish Configuration

- **Topic Name**: An uneditable text field showing the current topic structure.
  The default topic structure varies depending on the cloud platform:
  - **AWS IoT Core / Generic**:
    - <macGW>/<Lxx>/<IUxx>/status/<metricName>

    Where:
    - **<macGW>** is the client ID of the gateway (use of the MAC address is recommended).
    - **<Lxx>** Identifies the communication bus that links multiple units to the same line.
    - **<IUxx>** refers to the indoor unit whose status signals are reported.
    - **<metricName>** is a placeholder representing the specific status metric published by the gateway for the specified indoor unit.
  - **Azure IoT Hub**:
    - devices/<macGW>/messages/events/&line=<Lxx>&IU=<IUxx>&metricName=<metricName>

    Where:
    - **<macGW>** is the client ID of the gateway (use of the MAC address is recommended).
    - **<Lxx>** Identifies the communication bus that links multiple units to the same line.
    - **<IUxx>** refers to the indoor unit whose status signals are reported.
    - **<metricName>** is a placeholder representing the specific status metric published by the gateway for the specified indoor unit.

- **Type of frequency in sensor signals**: Sensor signals represent the real-time values detected by physical sensors, which are then published for monitoring or control purposes. Select when this type of signal should be updated:
  - **Change of Value**: The topic is published when the signal value changes beyond the limit set by the **hysteresis** value. See **Hysteresis** below.
  - **Periodic**: The topic is published at a fixed time interval.

  NOTICE
  The only available sensor signal is **tempAmbientSts**. All other signals are non-sensor type and operate under the **Change of Value (CoV)** principle.

  Two additional settings are available, one for each option:
  - **Hysteresis**: Enabled when the **Change of Value** option is selected. Defines a margin range around a threshold to prevent rapid publishing caused by small fluctuations (0.0..5.0. Default value: **0.0**).
  - **Frequency**: Enabled when the **Periodic** option is selected. Defines how often the value is updated, in seconds (30..18000 seconds. Default value: **30 seconds**).
- **Available Signals / metricName**: All currently active publishing signals are listed here.

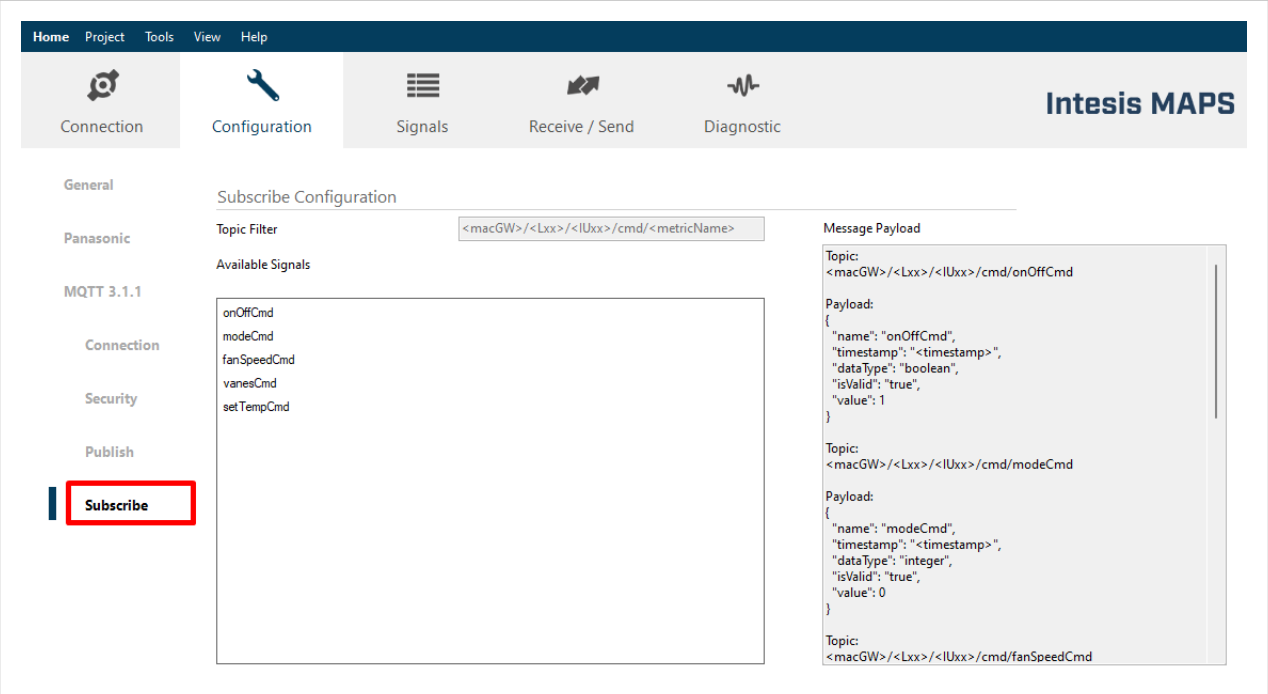
  NOTICE
  Signal selection occurs in the **Signals** tab. Refer to the Signals Tab (page 30) section for more information.
- **Message Payload**: This uneditable text field shows all current topics based on the active signals and their corresponding payloads. Other MQTT clients, such as a BMS, must subscribe to these topics to receive the status information.

  IMPORTANT
  Topic definitions in the message payload apply the Client ID value automatically, but the indoor unit must be set manually. When defining the subscriptions for MQTT clients, such as a BMS, to receive this status information, it is possible to either define individual topics for each indoor unit or status metric or use wildcards to reduce the number of topics to manage, leaving the handling of the received information to the internal logic of the MQTT client.

  TIP
  To select the whole text, click on the **Message Payload** text and press **Control + A**.

17.4. Subscribe

Figure 11. MQTT 3.1.1 Subscribe parameters



17.4.1. Subscribe Configuration

- **Topic Filter**: An uneditable text field showing the pattern used by the gateway, as a subscriber, to receive commands.
  The default topic filter structure varies depending on the cloud platform:
  - **AWS IoT Core / Generic**:
    - <macGW>/<Lxx>/<IUxx>/cmd/<metricName>

    Where:
    - **<macGW>** is the client ID of the gateway (use of the MAC address is recommended).
    - **<Lxx>** Identifies the communication bus that links multiple units to the same line.
    - **<IUxx>** refers to the indoor unit whose status signals are reported.
    - **<metricName>** is a placeholder representing the specific status metric published by the gateway for the specified indoor unit.
  - **Azure IoT Hub**:
    - devices/<macGW>/messages/devicebound/&line=<Lxx>&IU=<IUxx>&metricName=<metricName>

    Where:
    - **<macGW>** is the client ID of the gateway (use of the MAC address is recommended).
    - **<Lxx>** Identifies the communication bus that links multiple units to the same line.
    - **<IUxx>** refers to the indoor unit whose status signals are reported.
    - **<metricName>** is a placeholder representing the specific status metric published by the gateway for the specified indoor unit.

- **Available Signals**: All currently active subscribing signals are listed here.

> **NOTICE**
> Signal selection occurs in the **Signals** tab. Refer to the Signals Tab (page 30) section for more information.

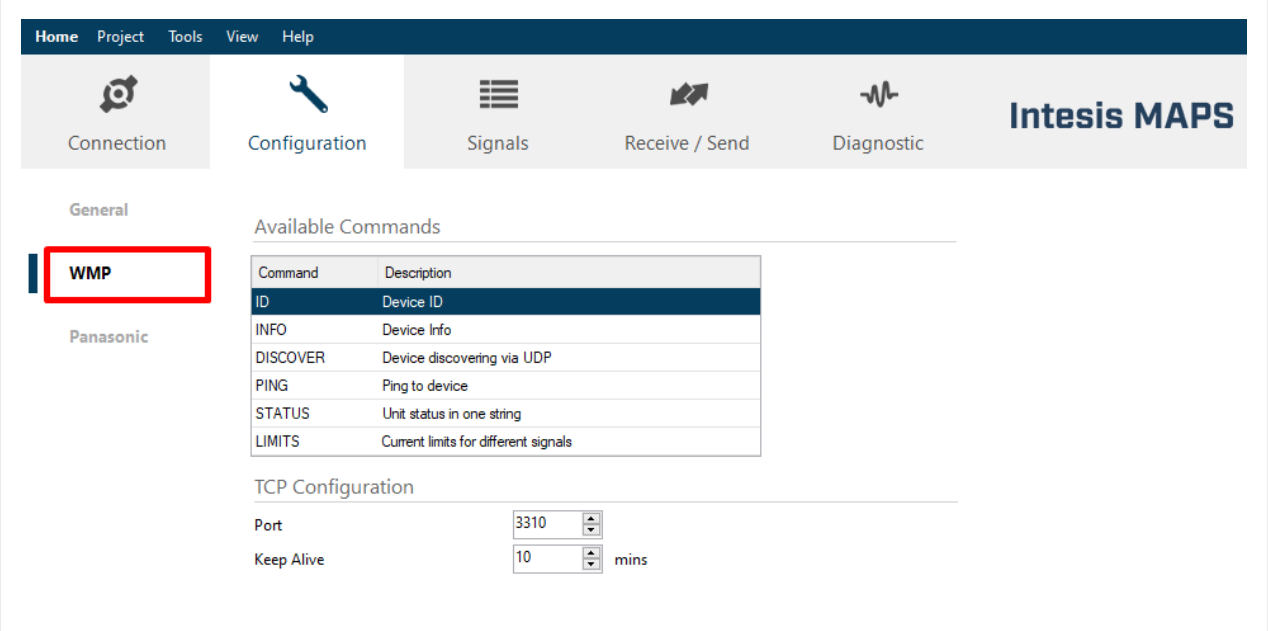
- **Message Payload**: This uneditable text field shows the structure of the message payload that the gateway requires to apply commands correctly. All MQTT clients that send commands through published topics, such as a BMS, must use this structure.

> **IMPORTANT**
> Topic definitions in the message payload apply the Client ID value automatically, but the indoor unit must be set manually. Remember to replace the **xx** in the **<IUxx>** segment with the desired indoor unit address (00-63), repeating the topic for as many indoor units as necessary. To reduce bandwidth usage, the number of topics should match the number of active indoor units.

> **TIP**
> To select the whole text, click on the **Message Payload** text and press **Control + A**.

18. Home Automation

Figure 12. Home Automation configuration parameters



18.1. Available Commands

This informative section displays all commands available for communication between the gateway and the Home Automation system:

- ID, INFO, DISCOVER, PING, STATUS, and LIMITS.

18.2. TCP Configuration

- **Port**: You can set the TCP port for the communication between the gateway and the Home Automation system.

> **NOTE**
> The default port is 3310.

- **Keep Alive**: Set the time in minutes before sending a keep-alive message (1..140. Default value: **10 min**).

> **NOTE**
> Set the parameter to 0 to disable this function.

19. Late Configuration: Change the Gateway's Protocol

Reconfiguring the gateway with a different protocol is very easy:

1. Connect the gateway to the computer and open Intesis MAPS.
2. Select the new template you need.
3. Click **Next** or double-click the template in the list.
4. Enter the **Connection** tab, select the gateway, and click the **Connect** button.
5. A dialog will inform you that the gateway has a different firmware version from the one required for the selected template, asking if you want to update the gateway's firmware.
6. Click **Yes**.
7. A dialog will ask if you want to save the project that is currently loaded in the gateway.
8. Click **Yes** or **No**, depending on your needs.
9. A new dialog appears showing the **Gateway Current Status** and the **Firmware Update Information**.
10. Click **Send** to load the new firmware into the gateway.
11. In the confirmation dialog, click **Yes**.
12. Once the firmware transfer is complete, click the **Connect** button to connect with the gateway again.
13. Configure the project as usual.

20. FAQ and Troubleshooting

20.1. Troubleshooting - General Questions

- **What is the best approach for configuring multiple gateways?**
  - If your project involves several gateways with the same configuration, you only need to create your project once and load it to each gateway by following the procedure explained just next.
- **Can I configure my project in Intesis MAPS if I don't have the gateway yet?**
  - Yes, you can create and complete your project with Intesis MAPS even without the gateway. Just proceed as follows:

    1. Create your project with Intesis MAPS.
    2. Save your project on your computer.

       NOTE
       The project will be saved in a file with the .ibmaps extension.

    3. Once you have the gateway, connect it to your computer.
    4. Open Intesis MAPS.
    5. On the home screen, click the **Load Project** option from the **Getting started** menu placed on the left side of the window.
    6. Select and open the .ibmaps file of your project.
    7. Once your project is loaded in Intesis MAPS, go to the **Connection** tab.
    8. Establish the connection with the gateway as explained in Connection Tab (page 25).
    9. Go to the **Receive / Send** tab.
    10. Click the **Send** button to load your Intesis MAPS project into the gateway.

- **What's the default password for the gateway?**
  - admin

    NOTICE
    This password is only necessary when connecting the computer to the gateway through an Ethernet connection.

    IMPORTANT
    Change the default password before sending the project to the gateway.

- **How do I change the gateway's password?**

  1. Go to the **General** section of the **Configuration** tab.
  2. In the **Connection** section, click the **Change** button next to the **Password** parameter.
  3. Type a new password.
  4. Go to the **Receive/Send** tab.
  5. In the **Send** menu, click the **Send** button.

6. Go to the **Connection** tab.
7. Select the gateway from the **Discovered Gateways** window.
8. Click **Connect**.

- **I forgot the gateway's password.**

> **TIP**
> If possible, connect the gateway to your computer using the USB connection. This way, the password won't be required.

– If you need to connect to the gateway over Ethernet and you have forgotten the password, a factory reset is required. (The procedure is explained below). The default password after a factory reset is **admin**.

> **NOTICE**
> If you exhaust all the attempts to write the correct password, after waiting for one minute, you will have three more attempts. If you exhaust these three new attempts, you'll need to wait another minute before having one more attempt. If you enter a wrong password again during this attempt, you'll have to wait ten minutes. After these ten minutes, the sequence starts anew.

- **How do I perform a factory reset?**

> **IMPORTANT**
> This action will restore the gateway to its original state, erasing all project data and settings.

1. Power off the gateway.
2. Locate the gateway's push button on the top side, between the KNX and the Ethernet connectors.

> **NOTICE**
> The button is hidden and only accessible using a thin object like a paper clip.

3. Push the button.
4. Power on the gateway.
5. Wait four seconds.
6. Release the button.

- **I can't find the template for the IN771AIR00LO000 in the Intesis MAPS New Project menu.**

– Make sure your Intesis MAPS version is 1.2.24.0 or higher. If you are running an older version, update the software as explained in Getting Started → UPDATES → Software Update (page 5).

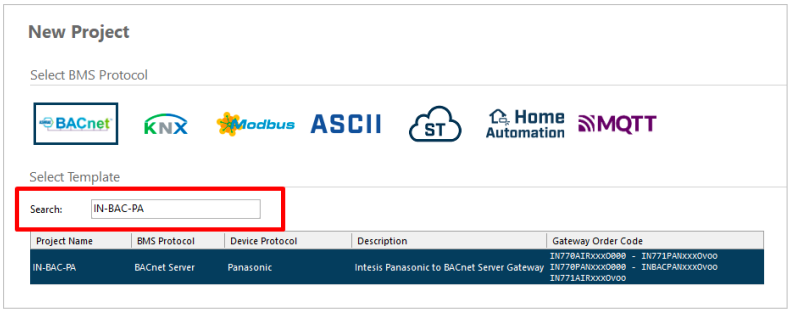
– If you are running the correct version of Intesis MAPS, follow these instructions:

1. Select the BMS protocol.

> **NOTE**
> Selecting a **BMS protocol** limits the search results to that protocol.

2. Use the **Search** field to locate the Project. Although all columns are searchable, the quickest way is to type the **Project Name** directly:

Protocol	BACnet	KNX	Modbus	MQTT	Home Automation
Template	IN-BAC-PA	IN-KNX-PA	IN-MBS-PA	IN-MQTT-PA	IN-WMP-PA



3. The template will be highlighted in blue.

20.2. Troubleshooting - Connection Tab

When establishing the connection between Intesis MAPS and the gateway using Ethernet, several considerations related to the presence of a DHCP server and the computer's Ethernet settings must be taken into account, as explained in the following sections.

20.2.1. Connecting the Gateway to the Computer through Ethernet

The method for connecting the gateway via Ethernet depends on whether a Dynamic Host Configuration Protocol (DHCP) server is being used.

IMPORTANT
The following topics apply whether the gateway still has its factory settings or has been factory reset.

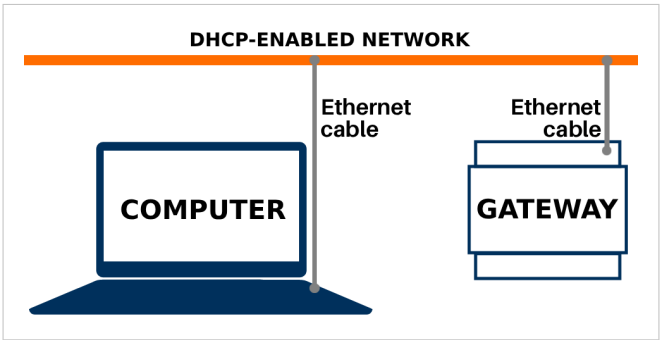
NOTE
The gateway includes a temporary DHCP mode that activates for 30 seconds each time an Ethernet link is detected[1]. If the gateway is connected to a DHCP-enabled network, the server will assign it a dynamic IP address. If no DHCP server is available, the default IP address **192.168.100.246** will be automatically assigned after 30 seconds.

[1] In practice, the temporary DHCP mode activates when:

- The Ethernet cable is unplugged and plugged back in.
- The gateway is powered off and then powered on.
- The gateway is reset.

NOTE
If the gateway has already been programmed (i.e., a project has been sent from Intesis MAPS to the gateway), the temporary DHCP mode will be deactivated. However, a permanent DHCP mode can be enabled using the **Enable DHCP** parameter, as explained in the section Configuration Tab → Connection (page 14).

20.2.1.1. Connecting the Gateway and the Computer through a DHCP-enabled Network



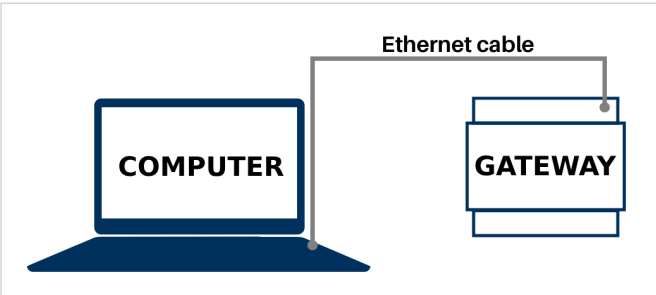
1. Connect the gateway to the DHCP-enabled network that your computer is also connected to.
2. Power on the gateway.
3. Set your computer's Ethernet configuration to **Automatic (DHCP)**. To do so, proceed as follows:
   a. Open the Ethernet settings on your computer.

> **TIP**
> These settings can usually be found in the **Network & Internet** menu.

   b. Set the **IP assignment** to **Automatic (DHCP)**.

At this point, you should be able to establish a connection between Intesis MAPS and the gateway as explained in Connection Tab (page 25).

20.2.1.2. Connecting the Gateway Directly to the Computer



1. Connect the gateway and your computer through their Ethernet ports.
2. Power on the gateway.
3. Open the Ethernet settings on your computer.

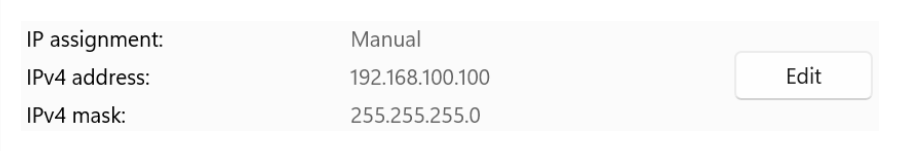
> **TIP**
> These settings can usually be found in the **Network & Internet** menu.

4. Set the **IP assignment** to **Manual**.
5. For the IP version, select **IPv4**.
6. Type an IP address within the range of the gateway.

> **NOTE**
> The gateway's default IP address is **192.168.100.246**

7. In the subnet mask parameter, type **255.255.255.0**, which is the gateway's default netmask.

Figure 13. Example of a computer's Ethernet configuration considering the gateway's default IP address and subnet mask.



At this point, you should be able to establish a connection between Intesis MAPS and the gateway as explained in Connection Tab (page 25).

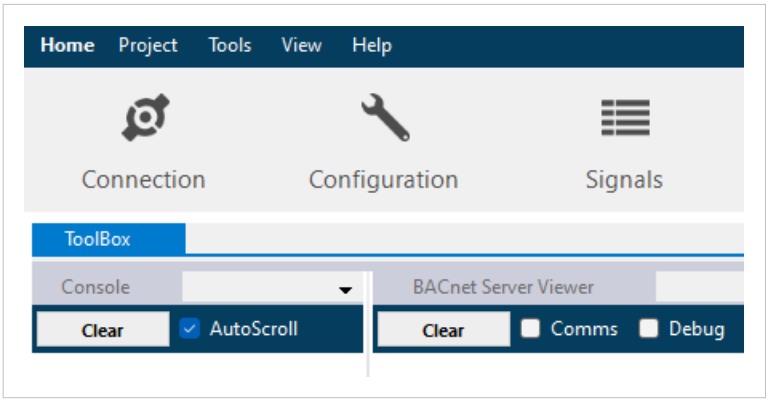
20.3. Troubleshooting - Receive / Send Tab

- **When should I send the MAPS project to the gateway?**
  - At a minimum, you should send the project once after completing the configuration. However, you can send the project to the gateway as many times as needed.

> **TIP**
> A good practice and time-saving approach is to save your project frequently and send it to the gateway only once it is complete. However, if you modify any parameter after completing the project, you must send it to the gateway again.

20.4. Troubleshooting - Diagnostic Tab

- **The ToolBox menu shows no buttons.**



– Depending on your screen resolution, the Console view may hide the Toolbox buttons. Just place the cursor between both views until its shape changes to a drag icon ⇳. Click and drag the Console view down until the Toolbox menu buttons appear.