

Intelligent control

Table of contents

1	About this manual	4
1.1	Intended audience and use	4
1.2	Related documentation	4
1.3	Copyright notice	4
1.4	Trademarks	4
1.5	Notice of liability	4
2	Introduction	5
3	Getting started	6
3.1	Log on to the PXI-CORE edge controller	6
3.2	Licensing	6
3.3	Installing	7
3.4	Activating the licenses	7
4	Configuration	9
4.1	Overview	9
4.2	System definition	9
4.3	Event definition	11
4.3.1	Date/Time system	12
4.4	Action definition	13
4.5	MQTT support	14
4.5.1	Introduction	14
4.5.2	Add an MQTT user	14
4.5.3	MQTT Topic	15
4.5.4	Connect the client to the broker	15
4.5.5	Add MQTT devices to Intelligent Controller	15
4.5.6	MQTT broker certificate	16
4.6	Activity log	19
4.7	License management	19
4.8	Save & restore	19
5	Related applications	21
5.1	MQTT Broker	21
5.2	Node-RED	21
6	Troubleshooting	22

1 About this manual

The purpose of this manual is to provide all required information needed for the installation and configuration of the Bosch Intelligent Control application software on the Bosch PXI-CORE edge controller.

- Unless required for the installation and configuration of the Intelligent Control application, and installed applications, this manual does not describe PXI-CORE edge controller installation, configuration and operating/user instructions. Refer to *Related documentation, page 4*.
- This manual, or an update, in pdf format is available for download from www.boschsecurity.com.

1.1 Intended audience and use

This manual is intended for system integrators authorized to create interfaces between the various Bosch Building Technology systems and devices.

System integrators must be knowledgeable about:

- The functionality and configuration of the supported systems.
- IP network communication.

1.2 Related documentation

The Bosch Intelligent Control application requires the following documentation for installation, configuration and use:

- PXI-CORE edge controller Installation and configuration manual.
See the download section of the PXI-CORE product page, on www.boschsecurity.com.

1.3 Copyright notice

Unless otherwise indicated, this publication is the copyright of Bosch Security Systems B.V. All rights are reserved.

1.4 Trademarks

Throughout this document trademark names may have been used. Rather than put a trademark symbol in every occurrence of a trademark name, Bosch Security Systems states that the names are used only in an editorial fashion and to the benefit of the trademark owner with no intention of infringement of the trademark.

1.5 Notice of liability

While every effort has been taken to ensure the accuracy of this document, neither Bosch Security Systems nor any of its official representatives shall have any liability to any person or entity with respect to any liability, loss or damage caused or alleged to be caused directly or indirectly by the information contained in this document.

Bosch Security Systems reserves the right to make changes to features and specifications at any time without prior notification in the interest of ongoing product development and improvement.

2 Introduction

The Intelligent control is a PXI-CORE Edge controller application that offers smart IP-based integration between various Bosch Security and Safety products by making use of the available IP interfaces. Additionally, it seamlessly integrates with MQTT-supported devices, allowing for extended connectivity and compatibility. In this way, Intelligent control can effortlessly interact with a broad range of systems and devices.

The configuration is done via an intuitive web-based user interface. Through the use of events and actions, the user has total control over the configuration. The action defines what needs to happen in one of the connected systems. The event defines when it happens. You can combine multiple inputs using logical AND/OR operations, and you can start various actions based on the same event.

3 Getting started

Configuration of the Intelligent Control application is done using the GUI of the Intelligent Control application, which is accessible via the PXI-CORE edge controller web browser. To install and configure the Intelligent Control application, the following order is recommended:

1. *Log on to the PXI-CORE edge controller, page 6*
2. *Licensing, page 6*
3. *Installing, page 7*
4. *Configuration, page 9*

3.1 Log on to the PXI-CORE edge controller

To log on to the PXI-CORE edge controller:

1. Open your web browser, and enter the IPv6-address of the PXI-CORE in your web browser.
2. Enter your username and password.

Supported browsers:

- Chrome
- Safari
- Firefox
- Microsoft Edge

For troubleshooting, refer to the PXI-CORE Edge controller user manual.

To use the Intelligent Control application, PXI-CORE edge controller permission **Manage Intelligent Control** is required. The PXI-CORE **Full access** permission is already set at initial delivery.

It is possible to create user accounts in PXI-CORE edge controller just for the Intelligent Control application. You can set up Manage and View only permissions of the Intelligent Control when adding or editing users in the PXI-core edge controller:

- **Manage Intelligent Control** allows full control and configuration of the Intelligent Control application.
- **View Intelligent Control** only allows you to view certain menus of the Intelligent Control application. It is not possible to change any configuration.

3.2 Licensing

To use the Intelligent Control application, the base PXI-LICB license is required. You also need the correct licenses for the system to which you want to interface.

For the complete set of licenses available, see the datasheet on www.boschsecurity.com.

Obtaining your activation ID

You can buy the required licenses individually or all at once. After your purchase, you receive an e-mail confirmation with a 35-character activation ID.



Notice!

The activation ID in the confirmation e-mail is required to activate the license.

See *Activating the licenses, page 7*, for further information.

3.3 Installing

You can find and download the Intelligent Control related application from the product page. You can also find and download the Release Notes that contain the latest information of the Intelligent Control version.

To install or upgrade the Intelligent Control application in your PXI-CORE edge controller:

1. In the **Settings** menu, select Apps. The apps screen opens.
2. Click the **Install from file** button.
3. Navigate to the folder containing the installation files.
4. Select following four applications (You can select them all at once):
 - Node-Red
 - Licensing server
 - MQTT broker
 - Intelligent Control
5. Click **Open**.
6. Click **Install** to install (or update) the selected applications.

**Notice!**

You can deselect applications that you do not want to install by clearing the check box next to the application. We suggest you check the versions.

**Notice!**

Updating the installed version of the Intelligent Control, MQTT Broker or Node-Red applications interrupts the current operation of the Intelligent Control application. Only update applications when it will not impact the operation.

3.4 Activating the licenses

After installing Intelligent Control and the other necessary applications, activate the licenses you purchased. Refer to *Licensing, page 6*.

**Notice!**

If you do not have a license when you start the Intelligent Control, the system redirects you to the **License** menu automatically.

To add and activate a license:

1. Navigate to the **License management** menu of the Intelligent Control application.
2. Click the + icon. The **Add licenses** window appears.
3. Fill in the required fields for adding a new license.

**Notice!**

Enter the requested information according to your preferences. Use detailed information since this is meant to easily recognize which system and user the licenses belong to.

4. Under **Activation information**, copy/paste your Activation ID from the confirmation e-mail to the **Activation ID** field.

**Notice!**

Entering the wrong ID does not alert the user of any errors in the Activation ID. If the ID is incorrect, it is not recognized by the license activation website.

5. Click the **Create request** button.
A request file with the extension .bin downloads to your default download folder. The request file name contains the serial number of the device, current date and time.
 6. Click the **System Activation Site** button on the **Licenses** menu and you will be redirected to the Bosch System Activation Site.
 7. Enter your credentials to log in to the System Activation site.
 8. Click the **Manage Licenses** tab.
 9. Click the **Upload** button. A file explorer window opens.
 10. Browse to the file and upload the .bin request file previously generated. When the upload is complete, you receive a response request file (license_<serialnumber>.bin) that is saved in your default download folder.
-

**Notice!**

If you do not have internet access on the current device, use a different device with an internet connection and go to <https://licensing.boschsecurity.com/>. Alternatively, you can move the file using a USB memory device to a different Internet connected device.

11. Return to the **Licenses** menu in the Intelligent Control application.
12. Click the **Upload response** file button.
13. Click the **Select file** button.
14. Browse to the file and select the Response request file to upload.
15. Click **Upload**.
Your activated licenses are now visible and you are able to use the Intelligent Control application.

4 Configuration

Assuming that the required applications are correctly installed on the PXI-CORE, they become available on the left hand-side navigation bar, and mid-section as a tile.

To start the configuration:

- ▶ On the PXI-CORE home page, click on the Intelligent Control application name or tile, to open the App.

4.1 Overview

Overview is the Intelligent Control application landing page. Use the **Overview** menu to view the main functions of Intelligent Control and to quickly navigate to these functions in the system through the use of informative graphical tiles. Each tile displays real-time data and possible issues in the current configuration.

Elements of the Overview page

Function tiles		
For a new configuration, it is recommended to start in the following order:		
1	License management	
2	<i>System definition, page 9</i>	To define the interconnection with systems/devices. The System definition tile displays the current number of (dis)connected systems. Systems disconnected are displayed in yellow and with the \triangle sign.
3	<i>Event definition, page 11</i>	To define a state change in the connected system(s)/device(s) which can start an action. The Event definition tile displays the current number of events definitions in the system. Events with issues needing attention are displayed in yellow and with the \triangle sign.
4	<i>Action definition, page 13</i>	To define a specific instruction for the connected system(s)/device(s) when at least one event is triggered. The Action definition tile displays the number of action definitions currently in the system. Actions with issues needing attention are displayed in yellow and with the \triangle sign.
5	Activity log	The Activity log tile displays the latest activity logged.

To navigate directly to the functions from this screen:

- ▶ Click on the tile you want to access. Alternatively, you can use the menu on the left side.

4.2 System definition

The **System definition** menu displays an overview of the systems currently configured and their current connection status.

A chain icon on the left side of the screen switches from broken (disconnected) to non-broken (connected) to show that the system/device connection state is being monitored.

Each system definition contains the system name, system type and how many events and actions are currently being used in this system.

In the System definition menu, you can add and configure new system definitions, remove system definitions, and enable/disable systems and definitions.

Adding a new system definition

To add a new system definition:

1. Click the + icon.
2. Enter a unique name for the system.
3. Select the type of system from the dropdown menu.



Notice!

A system of any type can be added, even if there are no (more) licenses activated for that system type.

-
4. Enter the required information for each field.
 5. Test the connection.

NOTE: Testing the connection does not require a license. The test will be successful if you entered the correct configuration.

6. Click **Save** to submit your changes or **Cancel** to discard the changes.

All systems added display in the first column. If there is no active license available, the chain icon displays broken, meaning the system is not connected.


Editing a system definition

To edit a system definition:

1. Click the system you want to modify. The system definition screen opens.
2. Make the necessary changes to the system.
3. Click **Save** to submit your changes or **Cancel** to discard the changes.


Deleting an existing system definition

To remove an existing system definition:

1. Click the  icon of the system definition you want to delete.
2. Click **Delete** to remove the entry or **Cancel** to discard the changes.



Notice!

You can only remove a system when it is not used in any event or action!
If the delete icon () is grayed out, the system/device is still in use.



Notice!

It is not possible to delete a system that is still present on the network and supports automatic discovery. The system still shows in the left menu.

Testing the connection

To ensure the information you entered is correct (IP address, password, username, etc.), you can test your settings before saving the system definition.

To test the connection between the added system and the Intelligent Control application:

- Click the **Test connection** button when adding or editing a system definition. This button is only active if all requested settings are inserted/selected.
- If the connection fails, verify the system/device is on and review all settings to make sure everything is correct. Test the connection again.
- A test is successful if Intelligent Control can create a connection to the designated system using the provided information. A successful test displays a **Connection successful** message.
- After a successful test connection, the system automatically connects.

Using a secure connection

- Automatic detection of a secure connection is available for supported systems. The connection to the system/device uses the best possible secure connection offered.
- To use an unsecured (http) communication protocol, clear (disable) the **Use a secure connection** checkbox.

4.3

Event definition

An event is a change of state in one of the Intelligent Control defined systems/devices, which can start an action in the same, or another, defined system/device. Refer to *System definition, page 9*.

Use the **Event definition** menu to view the state of the event, the number of triggers the system monitors, and the number of actions the event is currently using. A search field is available to quickly filter by the name of existing event definitions.

Event definition limits

- It is possible to configure up to 250 different events within an event definition.

Adding a new event definition:

To add a new event definition:

1. Click the + icon.
2. Enter a unique and useful name for the event.
3. Select the system for which you want to add the event definition.
4. Select the sensor type to define the trigger you want to use.
5. Select the sensor which monitors for the event trigger.



Notice!

The sensor name is the name defined in the connected system.

6. Select the desired trigger condition from the **Condition** and **Status** dropdown menus.



Notice!

For some options you are required to input values and will not get a dropdown menu. Enter the value directly into the corresponding field.

7. (Optional) Repeat steps 3-6 to add more triggers as AND/OR conditions.
8. Click **Save** to submit your changes or **Cancel** to discard the changes.


Editing an event definition

To edit or modify an event definition:

1. Click the event you want to modify. The event definition settings screen opens.
2. Make the necessary changes to the event definition.
3. Click **Save** to submit the changes or **Cancel** to discard the changes.


Deleting an existing event

To remove an existing event:

1. Click the  icon of the event definition you want to remove. A confirmation message opens.
2. Click **Delete** to remove the entry or **Cancel** to discard the changes.



Notice!

You can only remove an event if it is not being used! If the  icon is grayed out, the event is used in one or more actions elsewhere in the system.

4.3.1

Date/Time system

Define one, or a combination of, Date/Time event(s) when one, or more, action definition(s) must take place.

To define a Date/Time event:

1. From the **System** dropdown menu, select **Date/Time**.
2. After selecting the frequency of the event, select the **Sensor, Condition** and **Status** according the table below:
 - If more than one sensor type is required, use the “AND” and/or “OR” statements.

Sensor type	Condition	Status	Event description
Time	Is equal to	Hours (0-23) : Minutes (0-59)	To trigger an action definition on the selected Status time. E.g., at 09:00, play background music in zone x /zone group y.
	Is greater than or equal to		To trigger an action definition after a selected time set. E.g., at 18:00 and after, stop background music in zone x /zone group y.
	Is less than		To trigger an action definition before a selected time set.
Week day	Is equal to	Sunday up to Saturday	To trigger an action definition on the selected day(s) in a week. E.g., on all weekdays, except on a Monday.
Month day	Is equal to	1 up to 31	To trigger an action definition on the selected day(s) in a month. E.g., on all month days, except the 10 th of the month.

Sensor type	Condition	Status	Event description
Month	Is equal to	January up to December	To trigger an action definition on the selected month(s). E.g., on all months, except the month of February.

4.4 Action definition

Actions are executed at the moment the selected event triggers. This means the event condition becomes true. In an action, you define what has to happen when the event is true. Use the **Action definition** menu to view the state of the action and a short description of what the action does. You can add and configure new action definitions, remove and modify action definitions. You can temporarily disable an action with the enable switch. A search field is available to quickly filter by the name of existing action definitions.

Action definition limits

- It is possible to configure up to 250 different action definitions.

Adding a new action definition

To add a new action definition:

1. Click on the + icon.
2. Enter a unique and useful name for the action.
3. Select the event that you want to trigger the action.
4. Select the system that will execute the action.
5. Select the action that will be executed.
6. Select the Abort this action when the event is no longer active check box if an action should be aborted when the related event is no longer true.
7. Click **Save** to submit your changes or **Cancel** to discard the changes.

Testing the action

To ensure all the settings of the action are correct, you can test your action before saving the action definition. This triggers the selected event, even if the conditions of the event are not currently met. You can verify if the connected system executes the desired action. If the test is successful, all settings are correct and you can save the action definition.


1. To test the functionality of the configured action to perform, click the **Test action** button.
 - A passed or failure test result appears.
 - At a failure, check all items again.

Editing an action definition

To edit or modify an action definition:

1. Click the action you want to modify. The action definition setting screen opens.
2. Make the necessary changes to the action definition.
3. Click **Save** to submit the changes or **Cancel** to discard the changes.

Deleting an existing action definition

1. Click the  icon of the action definition you want to remove. A confirmation message opens.
2. Click **Delete** to remove the entry or **Cancel** to discard the changes.

4.5 MQTT support

4.5.1 Introduction

Intelligent control supports MQTT devices (clients) via the dedicated MQTT broker application. This MQTT broker is a related application part of the Intelligent control package. The MQTT broker enables a connection between generic MQTT clients and the Intelligent control application. By integrating MQTT devices, the Intelligent control application can recognize their messages as selectable sensors, considering the payload. Additionally, you can define actions in the Intelligent control application to send actions to the MQTT clients. Described below is an illustration of the principle of the MQTT support with Intelligent control. On one side it connects to the supported systems and on the other side it behaves as a MQTT client. Via the MQTT broker, it communicates with the external MQTT devices (clients). The communication (Publish, Subscribe and Deliver) between the Intelligent control application and the MQTT broker application is all done automatically, with no user configuration required.

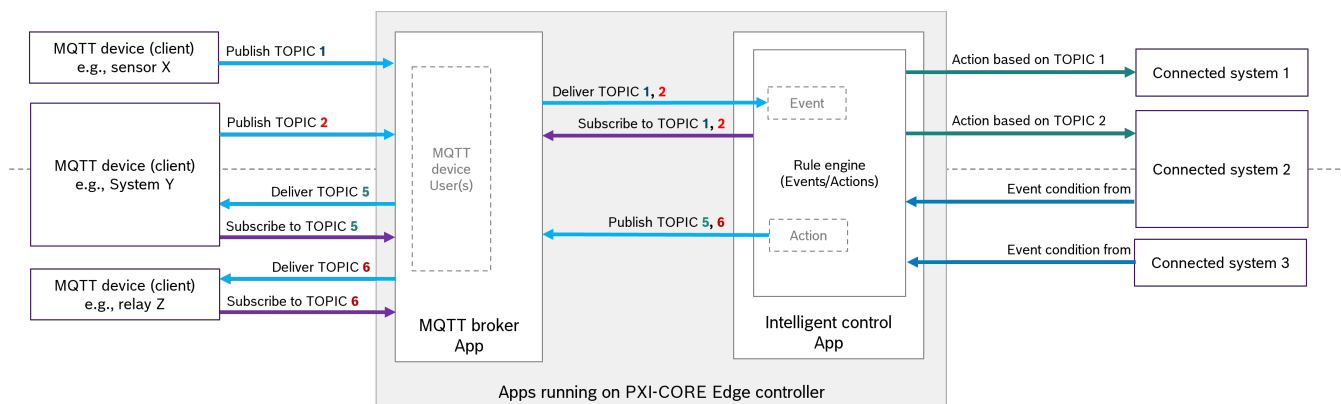


Figure 4.1: Principle overview of MQTT support with Intelligent control

If you are new to MQTT and want to learn more about it, please visit: <https://mqtt.org/getting-started/>.

4.5.2 Add an MQTT user

Adding a MQTT user

To allow MQTT clients to connect to the MQTT broker it is necessary to create a user. You can add as many user as you like using the **+** button in the right top corner.

To **add a user**:

1. Click the **+** button in the top right corner of the screen.
2. Enter your preferred username and password.
The password must follow the password rules as defined in settings (Users & Permissions | More settings | Password Policies of the PXI-CORE GUI).
3. Define the desired MQTT topic. For more information, see *MQTT Topic*, page 15.



Notice!

The password expiry and password history rules are not applicable for MQTT users!

4.5.3

MQTT Topic

MQTT topics are used to exchange information (read or set) between MQTT clients. MQTT topics are structured in a hierarchy level using the backslash (/) as a delimiter.

For security reasons, an MQTT topic must begin with "Ext/", everything else in the topic is entirely user-definable. You have the flexibility to define a specific topic for each MQTT device, as well as a root topic for multiple devices that share the same credentials.

For example, if you have three different temperature sensors, you can create a user with access rights to the "Ext/temperature" topic. Then, you select the options **Apply access rights to all sub-topics** and **Allow writing to the MQTT topic**.

The next step involves configuring your MQTT temperature sensor to use the defined credentials and publish its data to specified sub-topics. For instance, you can use topics like "Ext/temperature/Hall," "Ext/temperature/outside," and "Ext/temp/Canteen."

Refer to the MQTT client documentation to learn how to define the MQTT topic it utilizes.

4.5.4

Connect the client to the broker

MQTT clients must use secure MQTT protocol (TLS) using TCP port 8883 of the broker. This prevents the client username and password from being sent to the broker in plaintext over the network.

Please refer to your MQTT device's instructions for guidance on connecting the client to the broker.

In addition, configure the defined username and password and make sure the MQTT client uses the defined topic for publishing and subscriptions.

4.5.5

Add MQTT devices to Intelligent Controller

To define each temperature sensor, like in the example in the **MQTT Topic** section, in Intelligent Control, do the following:

1. On the Systems Definitions page, click the **+ button**.
2. Enter a **logical name** for the system.
3. Select **Generic MQTT Device** as the system type.
4. In the Root topic field, enter a **specific topic** (e.g., Ext/temperature/Canteen).
5. Click **Save**.

The GUI displays an active connection, indicated by the closed chain icon, after it receives at least one MQTT message on the specified topic in the defined system.

For example, when the temperature sensor of the Canteen publishes its temperature every 5 minutes, it may take up to 5 minutes before you can see the connection status reflected in the GUI. Once the GUI shows an active connection, you can proceed to define an event that triggers at a specific temperature.



Notice!

It is only possible to define the event if the temperature sensor has at least once published its temperature to the MQTT broker!

4.5.6 MQTT broker certificate

Although communication between the MQTT client and the MQTT broker is always secured by encryption, it is advisable to further enhance the security of the system. If attackers gain access to your network, they might be able to hijack the IP address of the PXI-CORE. Consequently, an MQTT client could unknowingly offer its credentials to a fake device, mistaking it for the legitimate PXI-CORE device, thereby allowing an attacker to obtain sensitive information.

To mitigate this risk, you have two options.

- Use the existing self-signed certificate of the MQTT broker.
- Use your own CA-signed certificate.

Both options provide an added layer of security to protect against potential IP hijacking and unauthorized access.

Certificate	Advantage	Disadvantage	Use If...
Self-signed	The user does not need to obtain and maintain certificates.	The user must load the server CA certificate to each MQTT client separately. Requires manual updating when the server certificate is changed.	Only a few MQTT clients on the network and there is no need to revoke a certificate.
CA signed	The MQTT client automatically checks the certificate chain based on the configured server name.	The user must obtain a CA signed certificate for the MQTT broker. This certificate expires on a certain date, after which it must be renewed.	There is a possibility to get CA signed certificates for internal devices. Network allows resolving names to IP addresses.

Table 4.1: Certificate Types

4.5.6.1 Use the self-signed certificate

The MQTT broker automatically generates self-signed certificates after installation.

To see certificates in the PXI-CORE GUI:

- ▶ Go to **Settings | Certificates & Keys | MQTT broker**.

The self-signed certificate uses the PXI-CORE's hostname as the Common Name in the certificate. Therefore, the MQTT client must use this hostname instead of the IP address to establish a connection to the broker.

If you need to modify the hostname of the PXI-CORE, you can do so at Settings | Information.



Notice!

When you change the hostname, it becomes necessary to generate new self-signed certificates.

This process occurs automatically when you:

- Delete all certificates of the MQTT broker (Settings | Certificates & Keys | MQTT broker).
- Reboot the PXI-CORE via GUI Settings | Shutdown & reboot | Restart.

**Notice!**

The MQTT client must have the capability to resolve the PXI-CORE hostname to its current IP address. This functionality is provided by your network infrastructure. To check if it works, you can try pinging the device using its hostname (e.g., ping pxi-core). If you receive a response, it means the resolution is working correctly. However, if there is no response, it is essential to contact your network administrator, as certificates will not function without this crucial feature

Certificate & Keys	What it is	What to do with it
mqttbroker_ca.crt	This is the public part of the certificate used to sign the mqttbroker_server.crt certificate	<ul style="list-style-type: none"> – Download using the browse icon. – Import the CA-certificate it in your MQTT client which is configured to use self-signed certificates – Backup up the certificate at a safe place
mqttbroker_server.crt	This is the public part of the MQTT broker certificate	<ul style="list-style-type: none"> – Download from the certificate manager for backup reasons and store at a safe place
mqttbroker_server_private.key	This is the private key that belongs to the mqttbroker_server.crt	<ul style="list-style-type: none"> – Backup if you want to replace the PXI-CORE later without updating all the clients. <p>Keep your private key secure at all times! Anyone with access to the key can act as your MQTT broker!</p>

Table 4.2: The different certificates/keys and how to use them

4.5.6.2

Use a CA signed certificate

Using CA signed certificates provides enhanced security and simplifies the configuration of MQTT clients. To use this approach, you need to obtain the certificate from a [Certificate Authority \(CA\)](#).

Similar to the self-signed solution, the Common Name (CN) of the certificate must match the name the client uses to connect to the PXI-CORE.

Additionally, your network setup must be capable of resolving the Common Name to the IP address of the PXI-CORE. This resolution is essential to establish secure connections using the CA signed certificates effectively.

**Notice!**

It is enough if the Common Name only resolves to the PXI-CORE IP address in the network that has the MQTT clients. However, some CA's might require differently.

If you order a certificate from a Certificate Authority, you usually get:

- The certificate linked to the given Common Name
- The private key used to sign this certificate by the CA root certificate
- The root certificate from this CA

Use the ASCII versions of the certificate (.PEM)

The received certificates need to be renamed according the table below:

Certificate	Renamed to	Remarks
Requested certificate for the given CN	mqttbroker_server.crt	
Private key used to get this certificate signed	mqttbroker_server_private.key	
CA root certificate	mqttbroker_ca.crt	Optional not used by the MQTT broker intended for the clients

Once the certificates are renamed, go to Settings | Certificates & Keys | MQTT broker and upload them to PXI-CORE.

To upload certificates:

At the certificate tab:

1. Delete the mqttbroker_server.crt.
2. Upload the CA received and renamed server certificate.
3. (Optional) Delete the mqttbroker_ca.crt and upload the renamed CA root certificate.
4. On the Keys tab, delete the mqttbroker_server_private.key.
5. Upload the CA received and renamed private key.
6. Verify the correct certificate and key is uploaded (CN correct, Organization is the used CA)
7. If correct, reboot the PXI-CORE.
8. Verify the certificates are still unchanged.

If the certificates are unchanged after the reboot, the server uses a CA signed certificate.

Normally there is no need to make this certificate available to the client.

**Notice!**

CA signed certificates usually have an expiration date. After this date, your MQTT clients might not connect anymore to the MQTT broker!

4.6 Activity log

The Activity log is intended for troubleshooting the configuration. It registers all actions and triggers to assist you in troubleshooting when a specific action fails to start or stop.

Use the **Activity log** menu to look up entries of any trigger from any configured system when it occurs. You can monitor the start times and stop times of each action to validate the action runs as intended.

The start time and stop time of actions are logged indicating the action is performed in the intended system.

The activity log can hold a total of 50,000 entries, of which 1,000 are visible in the GUI. By using the filter button, you can specify a specific filter to narrow down the entries to those that interest you. Additionally, you have the option to download the full log, up to 50,000 entries as a .CSV file, using the Download button.

To download the .CSV file:

1. Click the **Download activity log** button. A download window opens. You can choose save or open the file.

4.7 License management

Use the **License management** menu to display the list of currently active licenses. You can add new licenses from this menu. Refer to *Activating the licenses, page 7*.

Refer to

– *Licensing, page 6*

4.8 Save & restore

Use the **Save & restore** menu to save and restore the current Intelligent Control configuration.



Notice!

Does not store any other PXI-CORE configuration.

Save configuration

The **Save configuration** saves the current configuration with some exceptions:

Included	Excluded
System definitions	Activity log
Event definitions	Username and passwords ¹
Action definitions	

¹When restoring a previously stored configuration on the same PXI-CORE, usernames and passwords are restored. If you restore to a different PXI-CORE, usernames and passwords must be re-entered.

Restore configuration

Use **Restore configuration** to restore the full Intelligent Control configuration.

Restoring a previously saved configuration restores the configuration as it was in the moment it was saved. Any changes done afterwards will be lost.



Notice!

Restoring a configuration interrupts the current operation of the Intelligent Control application. Only update applications when it will not impact the operation.

5 Related applications

5.1 MQTT Broker

The MQTT Broker GUI allows you to create MQTT users for generic MQTT clients.
For more details, refer to *MQTT support, page 14*.

5.2 Node-RED

The Intelligent Control application uses Node-RED as its rule engine.

An advanced user can create additional Node-RED flows, using additional information.

For more details on how to use the Node-RED application, visit <https://nodered.org/>.

**Notice!**

Generated Node-RED flows starting with S2S... should not be changed.

6 Troubleshooting

Read this section in case the installation and/or the operation of the Intelligent Control application does not work as expected. This section presents the possible issues with maintenance actions focused on finding and solving the cause in a structured way. In large systems, it can be difficult to find the root cause of a problem. In that case, create a minimum size system with only the troubled device and the necessary devices to make it work, using short and proven cables. If the problem is absent, extend the system in steps until the problem shows up again.

This troubleshooting table gives a list of problems that you might face when using the Intelligent Control application. Column 2 and 3 contain possible causes and solutions.

Symptom	Possible cause	Possible solution
The configured system does not connect after a successful test.	No more licenses remaining for this system type.	Purchase more licenses to allow connection to all systems.
		Disable an already configured system.
Failure when testing a system connection.	The IP settings of the PXI-CORE do not allow communication to the IP address of the target system.	If both systems are in the same VLAN, make sure the IP address of the system to connect to matches the IP address of the PXI-CORE edge controller based on the subnet mask.
		If the systems are in different VLANs, make sure to set the correct default gateway and that you have routability between both VLANs.
A defined action is not executed.	The action is not enabled.	Enable the action in the Action definition menu.
	The trigger did not occur.	Check the Activity log to see if the trigger(s) were executed at a certain moment (the Activity log gives information on the triggers).
The GUI does not show all activated licenses.	New licenses types were introduced or internal bugs fixed.	Update the application.
	You might have accidentally removed the Bosch ST License Server and re-installed it (all licenses are gone).	Re-upload the RequestResponse_xxx.bin file containing the serial number of the PXI-CORE edge

Symptom	Possible cause	Possible solution
		controller. If the file is not available anymore, contact the service organization.
Missing all configured usernames and passwords upon restoring the system.	Restoring the configurations on a new PXI-CORE.	Re-configure all usernames and passwords manually.
The Activity log displays messages too fast.	Very active systems frequently updating the list with actions and triggers.	Download the Activity log as a .CSV file.
Date/time events are not triggering at the correct moment.	The time/date of trigger is not aligned with the internal clock on the PXI-CORE.	Set the correct time in the internal clock of the PXI-CORE (Settings -> Date & Time).
	Change of time zone.	Reboot the PXI-CORE so that all applications start using the new time zone.
Date and time are getting behind due to power down on the PXI-CORE edge controller.	Empty battery.	Replace the backup battery.
Cannot delete an unused system in System definition.	Some systems support automatic discovery and are added to the system definition overview.	Disconnect the non-used system of the network so it cannot be automatically discovered.
MQTT client does not want to connect when configured to validate the certificate.	Client does not use the correct CN of the certificate.	Use the certificate specified CN as host for the client.
	Client does not have the CA certificate in the case of self-signed certificates.	Supply the CA certificate from the certificate store to the client.
	Client has no access to the CA root certificate.	Supply the CA root certificate to the client.
	Client cannot resolve the hostname (CN) to the correct IP address.	Ping the MQTT broker using the configured hostname. If this does not work, contact your network administrator to set up hostname resolving.

Building solutions for a better life.

202309011128