ABB MEASUREMENT & ANALYTICS | USER MANUAL

Extendable IO (XIO)

XIO-00, XIO-04, XIO-08

Smart, extendable IO
Measurement made easy

Contents

List of tables

Additional information

Additional free publications are available for download at www.abb.com/upstream or by scanning this code:
XIO Product page

Table 0-1: Related documents

Document	Document number
XIO Data sheet	DS_2102774-EN
XIO Quick Start Guide (tri-fold leaflet)	2106425
XIO Interface Application Guide	2107011
Ethernet-Serial Passthrough Application Guide	2107010
Network Communication Application Guide	2107013
I/O Interface Application Guide	2107012
RMC User Manual	2105552
TFIO Module User Manual	2101226
Wi-Fi Antenna Kit Installation Guide	2106123

Cyber security

This product is designed to be connected, and communicate information and data, via a network interface. All Totalflow products should be connected to a secure network. It is the customer's sole responsibility to provide and continuously ensure a secure connection between the product and the customer network or any other network (as the case may be). The customer shall establish and maintain appropriate measures (such as, but not limited to, the installation of firewalls, application of authentication measures, encryption of data, or installation of antivirus programs) to protect this product, the network, its system and interfaces against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB Inc. and its affiliates are not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

Although ABB provides functionality testing on the products and updates that it releases, the customer should institute its own testing program for any product updates or other major system updates (to include, but not limited to, code changes, configuration file changes, third party software updates or patches, hardware change out) to ensure that the security measures that the customer has implemented have not been compromised and that system functionality in the customer's environment is as expected.

Malware Prevention

Recommendation: As with any downloaded software, scan ABB embedded software packages using a malware prevention solution.

Safety

Read these instructions carefully before installation and commissioning. These instructions do not contain all details on all types of products and do not explain all assembly, operating, or maintenance scenarios. Ask the manufacturer for further information.

Observe warning signs on packaging and on the device. Safety symbols are in accordance with IEC 60417 or ISO 7000.

Assign only qualified and authorized specialists for the assembly, electrical connection, commissioning, and maintenance of the equipment. Specialist qualifications include:

- Training or instruction and/or authorization to operate and maintain devices or systems according to safety engineering standards for electrical circuits, high pressures, and aggressive media
- Training or instruction in accordance with safety engineering standards regarding maintenance and use of adequate safety systems

WARNING: According to ISO 9996, use only sufficiently insulated tools for electrical connection.

Also consider the following regulations:

- The applicable standards and safety regulations concerning the construction and operation of electrical installations
- The regulation on technical working materials (safety guidelines for tools)
- The regulations and recommendations relating to explosion protection
- The recommendations for safe working in the case of installation in a Safety Integrity Level (SIL) loop.
- The regulations that apply in the country of use

Potential safety hazards

The XIO uses voltages in the range of 12 - 24 Vdc plus some percent of tolerance. There are no hazardous voltages present in the device. However, some optional power sources might convert power from Vac to - Vdc.

Pressurized natural gas is present in the measurement pipeline. Natural gas can escape from the pipeline during installation, calibration, or following damage to the pipeline. Only properly trained and authorized personnel should work in hazardous locations.

WARNING – Bodily injury. Apply power only after the procedures are complete. Technicians must perform the procedures in order: plan, install, wire, verify the power-on sequence, and configure.

WARNING – Bodily injury. The device can be operated at high levels of pressure and with aggressive media. Serious injury and/or considerable material damage can be caused if this device is handled incorrectly.

WARNING – Bodily injury. Read and follow instructions contained in this guide before and during equipment installation. Failure to do so could result in bodily injury or equipment damage.

WARNING – Bodily injury. Ensure there is no hazardous atmosphere present when performing maintenance on the unit. Do not separate components when energized. This applies to all connectors and connections, cabling and wiring.

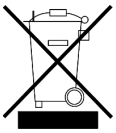
NOTICE – Equipment damage or loss of data. Potential electrostatic charging hazard: clean only with a damp cloth.

Compliance

Waste Electrical and Electronic Equipment (WEEE)

EU Directive 2012/19/EU

ABB Industrial Automation, Measurement and Analytics is committed to actively protecting the environment. Do not dispose of WEEE as unsorted municipal waste. Collect WEEE separately. WEEE management participation is critical to the success of WEEE collection.



Do not mix electrical and electronic equipment with general household waste if it displays the crossed-out wheeled bin symbol. Dispose of it correctly at a recycling facility to save valuable resources and prevent potential negative effects on health and the environment. These steps ensure compliance with the Waste Electrical and Electronic Equipment (WEEE) Directive.

Treat waste electrical and electronic equipment (WEEE) separately. Use the national collection framework available to customers for the return, recycling, and treatment of WEEE.

FCC RF Compliance

CONTAINS FCC CERTIFIED TRANSMITTER MODULE(S).
THIS PRODUCT CONTAINS FCC ID: Z64-WL18DBMOD.
THIS DEVICE COMPLIES WITH PART 15 OF THE FCC RULES.

THIS PRODUCT CONTAINS IC: 5530C-WL1837MOD. THIS DEVICE COMPLIES WITH RSS-GEN OF THE IC RULES

OPERATION IS SUBJECT TO THE FOLLOWING 2 CONDITIONS:
THIS DEVICE MAY NOT CAUSE HARMFUL INTERFERENCE.
THIS DEVICE MUST ACCEPT ANY INTERFERENCE RECEIVED, INCLUDING ANY INTERFERENCE THAT MAY CAUSE UNDESIRED OPERATION.

FC IC

1 Product overview

The ABB XIO is a microprocessor-based device with built-in, pre-engineered applications for expanding serial communication and IO over Ethernet to a host controller. The devices are extendable, supporting hardware expansion using TFIO modules.

The XIO may be located remotely from the controller (RTU) using Ethernet for communication. Configuration of the device may be performed using USB, Wi-Fi, Bluetooth, or an Ethernet connection depending on the XIO model. It has extendable IOs, using TFIO modules and up to 8 onboard COM serial ports (depending on the model) to communicate with measurement transmitters, additional automation or control equipment, flow computers, etc.

There are 3 models of the XIO based on the number of serial communication interfaces they support. Figure 1-1 shows the XIO-08 which has 8 COM ports. Figure 1-2 shows the XIO-04 which has 4 COM ports. Figure 1-3 shows the XIO-00 with no serial COM support (used only for extending IOs).

Figure 1-1: XIO-08

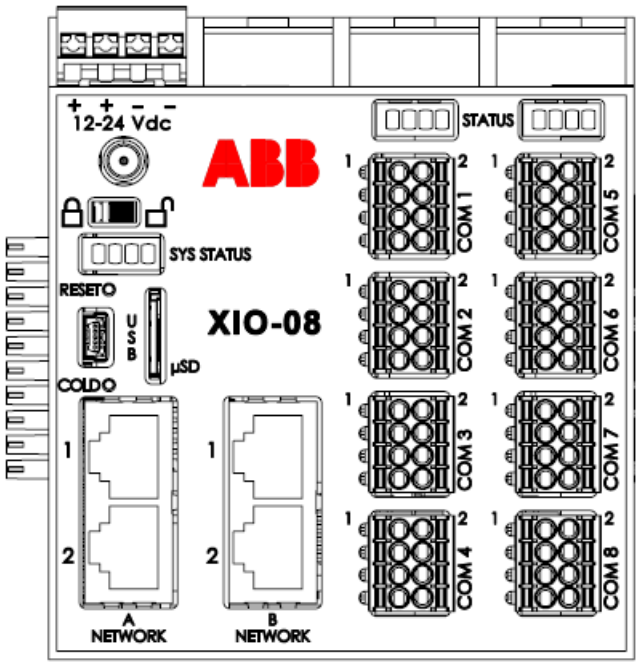


Figure 1-2: XIO-04

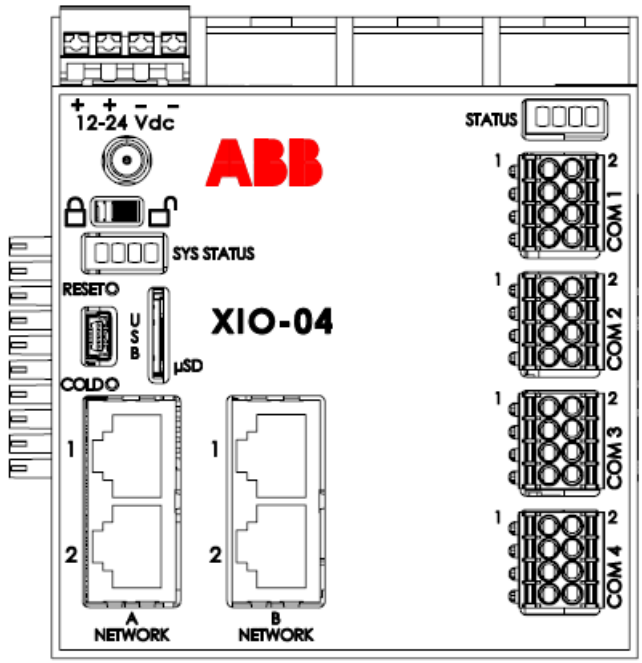


Figure 1-3: XIO-00

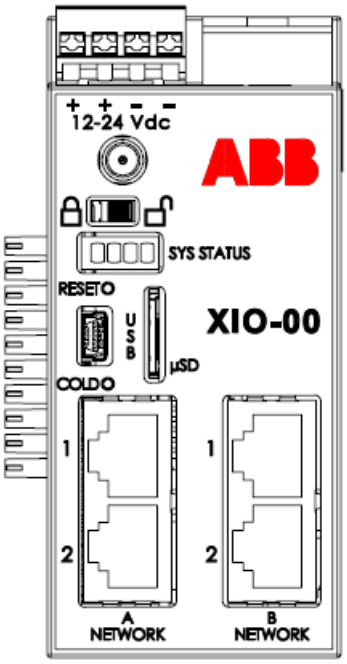


Table 1-1 provides a general description of each XIO model. All XIO models provide backward-compatible functionality based on ABB Totalflow software, communications, and IO technologies. They support IO and serial communication expansion. All models support a single backward-compatible TFIO bus, with an IO module capacity of up to 22 modules.

Table 1-1: XIO models

Model	Description	Use
XIO-08	4 Ethernet ports, 8 COM ports, 1 TFIO I^2C bus interface Dimensions: 3.90 x 3.96 x 4.375 inches (9.91 x 10.06 x 11.11 cm)	Extends both serial and I/O capacity
XIO-04	4 Ethernet ports, 4 COM ports 1 TFIO I^2C bus interface Dimensions: 3.90 x 3.96 x 4.375 inches (9.91 x 10.06 x 11.11 cm)	Extends both serial and I/O capacity
XIO-00	4 Ethernet ports, 1 TFIO I^2C bus interface Dimensions (This model is narrower since no COM ports are supported): 2.04 x 3.96 x 4.375 inches (5.18 x 10.06 x 11.11 cm)	Extends I/O capacity only

IMPORTANT NOTE: For general specifications, refer to the Data sheet on the XIO Product page.

2 Physical Description

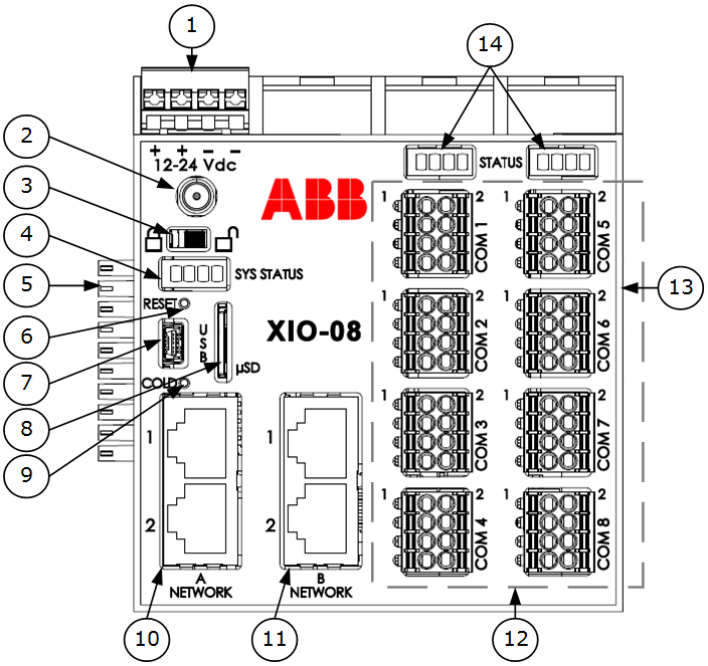
2.1 XIO Housing

A DIN rail mountable plastic housing packages the XIO electronic boards and components.

IMPORTANT NOTE: The XIO must be installed on an interior wall, or in an enclosure that meets the environmental ratings for the location. See section 2.1.1 Enclosures for information about ABB enclosures. See section 3.1.1 Enclosure requirements for information about third-party enclosures.

The housing is an interlocked top cover and a base. The following figures illustrate the XIO components and interfaces (ports). The XIO-08 is used for the illustrations.

Figure 2-1: XIO housing cover

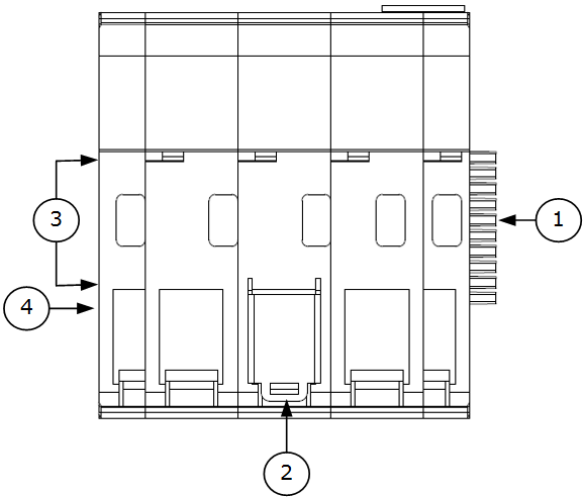


Legend: XIO housing cover

ID	Description	ID	Description
1	External power supply input (12 or 24 Vdc)	8	Micro SD holder
2	Wi-Fi antenna connector	9	Cold button (paperclip actuated)
3	Security switch	10	A Network Ethernet ports 1 and 2
4	System status LEDs	11	B Network Ethernet ports 1 and 2
5	TFIO Module interface (male)	12	COM 1 – COM 8 Serial communication ports (XIO-08 and XIO-04 only)
6	Reset button (paperclip actuated)	13	TFIO Module interface (female) (on the side)
7	USB mini port	14	Communication card status LEDs

The electronic boards are inserted into a backplane at the base and the mounting clips are accessible on the exterior. Figure 2-2 illustrates the exterior of the housing base.

Figure 2-2: XIO housing base



Legend: XIO housing base

ID	Description	ID	Description
1	Male TFIO interface	3	DIN rail channel
2	DIN rail clip	4	Female TFIO interface

IMPORTANT NOTE: The XIO has grounding clips attached to the bottom of the electronic board. The grounding clips fit through the base grounding slots to contact the DIN rail when mounted. Be sure to ground the DIN rail.

2.1.1 Enclosures

The XIO can be purchased installed in an enclosure. ABB offers the *X*CORE enclosures described in Table 2-1. For more information and complete specifications, see www.abb.com/upstream.

Table 2-1: XCORE enclosures available

Part number	Size	Weight
2424	24 x 24 x 12 inches (61 x 61 x 30 cm)	45 pounds maximum (fully loaded system)
3630	36 x 30 x 12 inches (91 x 76 x 30 cm)	75 pounds maximum (fully loaded system)

Figure 2-3: *X*CORE 3630 medium size enclosure (front view)

Figure 2-4: *X*CORE 2424 small size enclosure (internal view displays an installed XIO-08 as an example)

2.2 Electronic board

The electronic board component specifications are listed in this section.

DANGER – Serious damage to health / risk to life. **Explosion Hazard:** Do not connect or disconnect connectors or their terminations while energized unless the area is known to be non-hazardous.

IMPORTANT NOTE: For general specifications, refer to the Data sheet listed under Additional information.

2.2.1 Communication ports

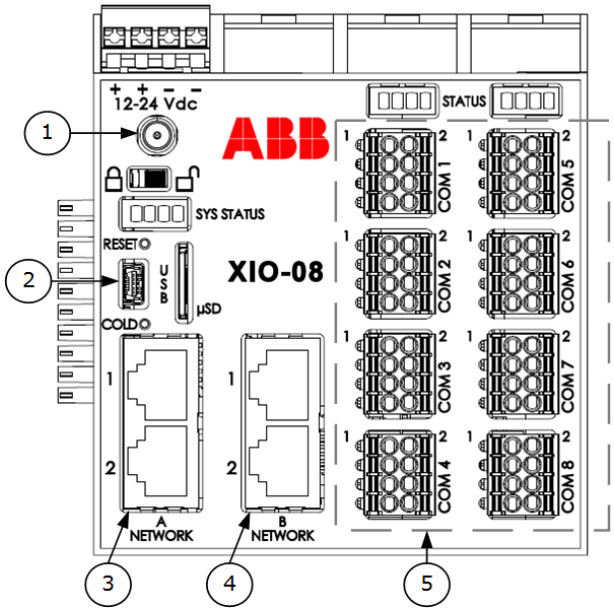
Communication ports provide communication between the XIO and host systems or external devices. Factory preconfigured ports support typical communication scenarios. The ports support several available communication protocols.

Ports configured for local communication (direct connection) support either local access from a host system, or connection to external devices or peripherals including:

- Measurement transmitters
- Additional automation or control equipment
- Flow computers
- Analyzers

The XIO has several communication ports. Figure 2-5 illustrates the ports and communication expansion interfaces for the XIO-08. Models differ on the number of COM ports, but the other ports are the same on all models.

Figure 2-5: Communication ports (XIO-08)



Legend: Communication ports (data speed and use)

ID	Port name	Connector type	Data transfer rate (port speed)	Use (connections)
1	Wi-Fi /Bluetooth	SMA connector for Wireless Antenna (optional)	54 Mbps over Wi-Fi maximum 3 Mbps over Bluetooth. Actual throughput-rate will be less depending on number of devices connected, distance and obstacles between device antennas.	(Optional) Local communication over Wi-Fi or Bluetooth. XIO can be a Wi-Fi client or Wi-Fi Access point.
2	USB	USB Type Mini B	Supports USB 2.0 full speed mode and high-speed mode	Local communication (high-speed serial local operator interface)
3	Ethernet A Network 1, 2	RJ-45	10/100 Mbps Full Duplex (auto-negotiable, not user-configurable)	Two ports: A1 and A2. Connection to the corporate network for data collection and local connection
4	Ethernet B Network 1, 2	RJ-45	100 Mbps Full Duplex	Two ports: B1 and B2. Realtime data communication between XIO and RMC
5	Serial communication COM 1 - COM 8	Removable Terminal connector (8 POS), spring-cage termination	Baud Rate: 2,400 to 115,200 bps Manually configurable from the user interface	XIO-04 and XIO-08 only. The XIO-00 does not support serial (COM) ports. Remote or local serial communication configurable for either RS-232, RS-422 or RS-485

2.2.1.1 Serial communication ports (XIO-04 and XIO-08 only)

COM 1 to COM 8 are software-configurable for serial (RS-232, RS-485, or RS-422) communication between the XIO and external measurement equipment such as pressure or temperature transmitters.

DANGER – Serious damage to health / risk to life. Explosion Hazard: Do not connect or disconnect connectors or their terminations while energized unless the area is known to be non-hazardous.

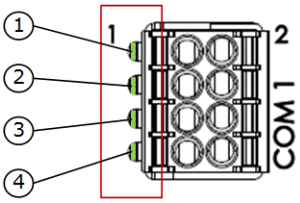
The configured interface type and the distance between the XIO and the connected external device determine maximum serial communication speed. The supported port speed ranges from 2,400 bps to 115,200 bps.

2.2.1.2 XIO COM LEDs (XIO-04 and XIO-08 only)

There are two kinds of COM LED on the front of the XIO device.

- COM LEDs
- STATUS LEDs

Figure 2-6: COM LEDs



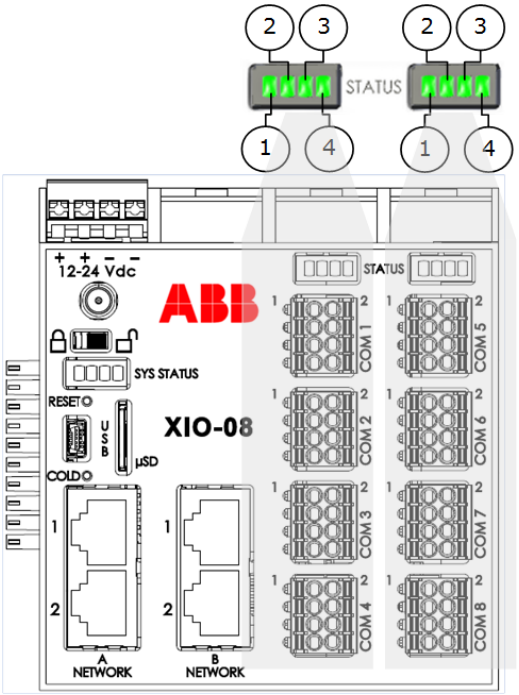
Legend: COM LEDs

LED	ON	OFF
1	Port Enabled	Port Disabled
2	Port Power Output ON	Port Power Output OFF
3	Port TXD Activity	
4	Port RXD Activity	

2.2.1.3 Communications Port Group STATUS LEDs (XIO-04 and XIO-08 only)

During normal operation, LEDs 1-3 should be ON and LED 4 should be OFF.

Figure 2-7: STATUS LEDs



Legend: Status LEDs for all COMS

LED	ON	OFF
1	Port Group Power On	Port Group Power OFF (LED is OFF. No other LEDs should be ON)
2	Port Group Enabled	Port Group Disabled (LED is OFF. No Port LEDs should be ON)
3	Port Group Normal operation	Port Group Suspend Mode
4	Port Group Suspend Mode	Port Group Normal Operation

2.2.1.4 USB port

The USB type mini B port provides high-speed serial communications between the XIO and equipment, host systems or computers with USB interfaces. The port supports local operator access through PCCU32.

The USB port has two speed modes: full speed and high speed. The XIO automatically negotiates data transmission rates with the host system.

2.2.1.5 Ethernet ports

The XIO supports embedded managed Ethernet switch capabilities through its 2-port sets of Ethernet ports. One set is labeled as A Network and the other as B Network on the device. The A Network ports, also referred to as Enterprise Network ports, can be used for connections to the corporate wide area network or for connections to the field network for device management. The B Network ports, also referred to as Industrial Network ports, can be used for connections carrying real time measurement traffic. The XIO has the flexibility to support connections as a 4-port Ethernet switch (A Network and B Network interfaces are combined into a single logical network) or provide separate Ethernet interfaces (A Networks are separate from B Networks). The XIO also supports port forwarding when not in 4-port switch mode. All options are configurable from the user interface (PCCU).

Table 2-2 shows the typical use of the Ethernet ports. All ports can be used for star or daisy-chain connections. The topology depends on the actual configuration of the interfaces which depends on field requirements.

Note that all ports can be used for direct local connection by operators and field technicians.

Table 2-2: Ethernet ports

Port name	Data transfer rate (port speed)	Typical use
A Network (1, 2)	10/100 Mbps Full Duplex (Supports auto-negotiation and uses standard or straight-through Ethernet cable)	Connection to the corporate network for data collection and local connection. Two physical ports: 1 and 2. Two possible interfaces labeled: A1 and A2. Two Ethernet Modes: – The 1 Network mode provides a single interface (A1+A2). The XIO behaves like a 2-port switch. – The 2 Network mode provides two separate interfaces (A1, A2). Each interface can be assigned its own network.
B Network (1, 2)	10/100 Mbps Full Duplex (Supports auto-negotiation and uses standard or straight-through Ethernet cable)	Real-time data communication between XIO and RMC or other devices. Two physical ports: B1 and B2. One Ethernet Mode only: 2 Network mode provides two separate interfaces (B1, B2). Each interface can be assigned its own network.

IMPORTANT NOTE: All ports can be configured for any desired connection based on field requirements. A Network ports are not restricted to WAN or field LAN connections. B Network ports are not restricted to local field connections. Configuration of the associated interfaces is flexible. Table 2-2 above provides only basic examples for the intended use of the ports. For additional details on Ethernet connections, refer to section 9 Ethernet connectivity scenarios, or click **Help** on the Networking tab when connected to the device with the user interface (PCCU32).

2.2.2 TFIO expansion interfaces

The XIO provides two interfaces to add modular I/Os. The XIO supports up to 22 TFIO modules.

The XIO uses an independent bus to communicate with the modules. Totalflow has an I/O protocol to exchange information between the modules and the XIO. The bus operates in a master/slave mode, with the main board acting as master.

The TFIO modules are DIN rail mountable and employ contact technology for field wiring. The modules interconnect to each other to provide the necessary power and interface signals along the bus.

The TFIO modules are hot-pluggable and can be inserted, replaced or removed during the normal operation of the device with no restart required. The system will detect any changes to the modules on the TFIO bus and the module states can be verified with PCCU.

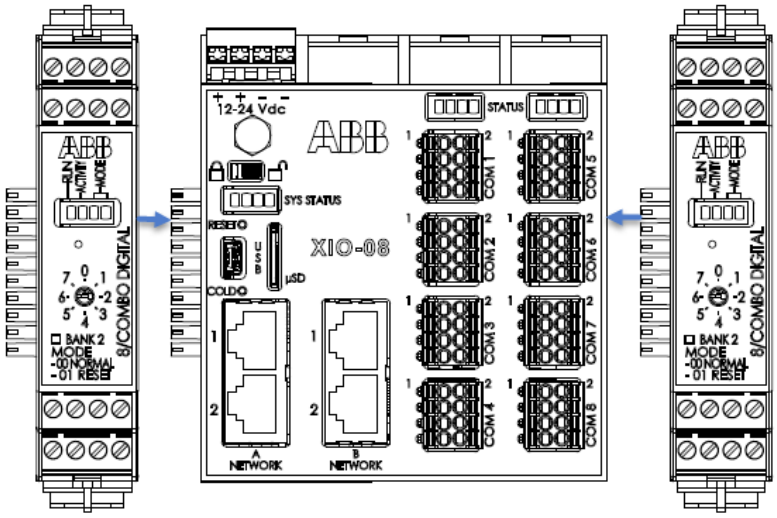
DANGER – Serious damage to health / risk to life. Explosion Hazard: Do not connect or disconnect TFIO modules, connectors or their terminations while energized unless the area is known to be non-hazardous.

IMPORTANT NOTE: Power compatibility for TFIO modules depends on module type:

- Older green modules must only use 12 Vdc.
- M2 modules and newer grey modules can use 24 Vdc.
- A combination of green modules, and M2 modules or grey modules, must only use 12 Vdc.

Figure 2-8 shows the location of the XIO TFIO connectors for attachment of the TFIO Modules. All XIOs and TFIO modules support a male TFIO connector on the left and a female connector on the right (not visible in the illustration). A TFIO module can be attached to either side of the XIO. The location depends on the location of the XIO and the space on DIN rails inside an enclosure. See Figure 2-4 which shows an XIO with two modules attached inside an enclosure.

Figure 2-8: TFIO module connections to XIO

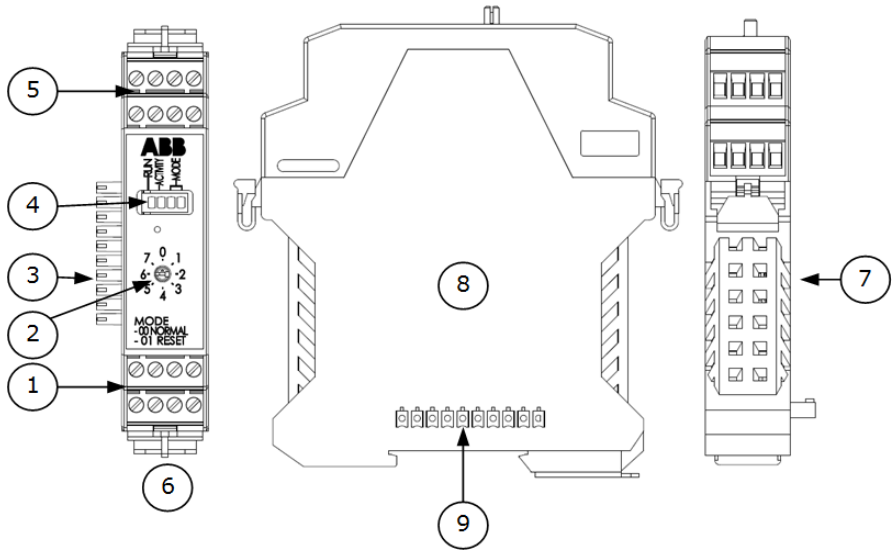


All modules have four LED lights, a manual reset button, and a selectable address from zero through seven (Figure 2-9). The faceplate of each module shows:

- Type of module
- LED light panel
- Reset button
- Module address selector

For additional information, refer to the TFIO Module User Manual. See Additional information for a link to the online manual.

Figure 2-9: TFIO module



Legend: TFIO module

ID	Description	ID	Description
1	4 pin terminals	**6**	TFIO front face
2	Bus address rotary switch	**7**	TFIO top view
3	Bus interface (male)	**8**	TFIO side face
4	Activity LEDs	**9**	Bus interface (female)
5	4 pin terminals		

2.2.3 External power supply requirements

Comply with the following specifications when powering the controller with an external power source.

A customer-provided and installed 5 A fuse in the "+" side circuit of the power source is required to protect the XIO power circuits.

Table 2-3: Power source requirements

Source type	Requirement	Temperature
External power supply	Power source: 12 Vdc to 24 Vdc, 5 A	Rating for ambient temperature is Ta = -40 °C to +60 °C (-40 °F to 140 °F).
External power fuse	Power to the XIO must be fused at 5A	

2.2.4 Power port

The XIO has a single port for connection to an external power source. The port supports reverse polarity protection.

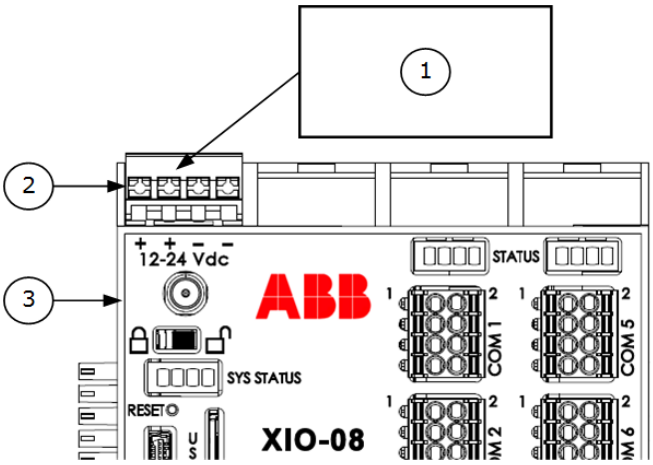
Table 2-4: Power connector specifications

Port	Terminal type
Power	Removable terminal connector (4 POS), spring cage termination. Wire gauge 12 AWG to 22 AWG

IMPORTANT NOTE: Select wire gauges based on the voltage and current requirements of the circuitry and the expected length of the wires. The gauge differs for each application.

The external power supply is the sole source of power to the XIO. The power supply may be one of several different devices, represented as a rectangle in the following drawing.

Figure 2-10: External power mode



Legend: External power mode

ID	Description
1	External power supply
2	External power terminal connector
3	XIO device

IMPORTANT NOTE: If you do not use ABB-approved power sources, verify that the customer-supplied power source meets these requirements. For additional details about requirements, see section 3.1 Site planning and requirements.

IMPORTANT NOTE: The XIO does not have a hardware circuit to monitor the 12-24V incoming line voltage like other ABB Totalflow devices. For this reason:

- The XIO embedded software does not support sleep mode when the line voltage drops below minimum input value (10.9 V). There is no support for configuration for low power use.
- The AGA 3 application always provides a value of 0 V for the XIO Battery / External voltage.

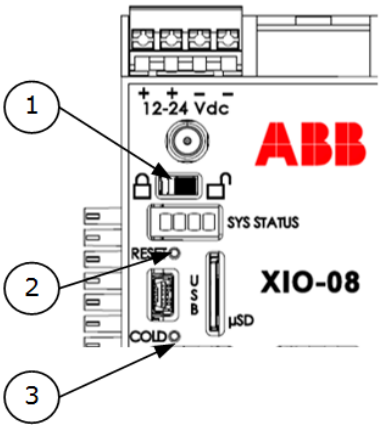
2.2.5 Security switch

The XIO has a security switch located between the Wireless Antenna Connector and the System Status LEDs (Figure 2-11).

DANGER – Serious damage to health / risk to life. Explosion Hazard: Once the device is installed and in operation, the security switch position shall not be changed unless the area is known to be non-hazardous.

When the security switch is in the ON position, PCCU requires security codes to connect with the device. For more security information, see section 7 Configure security (recommended).

Figure 2-11: Security switch



Legend: Security switch

ID	Description
1	Security switch
2	Reset (paperclip actuated)
3	Cold (paperclip actuated)

2.2.6 Reset button

The XIO has a reset button located above the USB connector (Figure 2-11).

DANGER – Serious damage to health / risk to life. Explosion Hazard: The RESET button must not be pressed unless the area is known to be non-hazardous.

Press the reset button to restart the XIO with the running (warm) configuration.

2.2.7 COLD button

DANGER – Serious damage to health / risk to life. Explosion Hazard: The COLD button must not be pressed unless the area is known to be non-hazardous.

Press and hold the cold button while resetting the XIO to restart with the cold configuration restored. Power cycle the device to restart the XIO.

2.2.8 Super capacitor

The XIO design includes an onboard super capacitor (Super CAP) that serves as a short-term power reservoir. In the event of a loss of power or a reset, the charged capacitor prevents the supply voltage from falling to zero for 2.5 seconds. This delay allows the system time to save data, such as trending files, and restart configuration. The capacitor charges automatically when the controller is powered on for the first time, or after the controller is powered off for several hours or longer. The capacitor remains charged if the controller is powered on. The capacitor takes two minutes to first charge when completely discharged.

2.3 Embedded software and data

The XIO non-volatile memory contains the software required for operation and provides storage space for customer data.

The embedded software has the following components:

- Operating system: Required for system boot, operation, and execution of all applications
- Applications: Totalflow applications that define the XIO functions for the required scenarios
- Configuration: Files that contain factory default and user-defined settings and parameters required by the applications active on the XIO

The stored data depends on the configured applications for the specific site requirements.

2.3.1 Operating system

The XIO uses a thread-priority preemptive real-time operating system (Linux-based OS). The software architecture prioritizes real-time functionality (communication applications) before executing non-real-time functions (post communication data processing and file system access). The XIO OS supports:

- Execution of the communication suite of applications
- Backward-compatible protocol transactions for all applications
- Improved real-time performance metrics

The OS file system has a RAM file system and an embedded multimedia card (eMMC) data journaling file system. The applications access the RAM file system, which provides increased performance. The RAM file system is backed up into the eMMC file system for the following triggers:

- Once a minute at the fourth second of each minute
- Prior to all warm restarts (triggered from PCCU Station Setup, terminal mode, the device loader, or the reset button)

2.3.2 Applications

The XIO supports all Totalflow communication applications and the I/O Interface application for interfacing with peripherals. All applications have real-time performance metrics that monitor the overall health of the system.

2.3.2.1 Applications supported on the XIO

Table 2-5 identifies the subset of Totalflow applications supported by the XIO.

To view the most up-to-date list of supported applications by the XIO:

1. Connect the laptop or PC to a USB or Ethernet port on the XIO. See Figure 9-2: Local connection to XIO on 4-port switch mode for more information.
2. Launch PCCU and click **Entry** to connect with the controller in Entry mode.
3. Click Application/License Management>Credit/App Info.
4. Click **Help** for additional information.

Table 2-5: Applications available on the XIO

Application	Exportable	Application	Exportable
Alarm System	No	Operations	No
AGA3 Measurement	No	PID Controller	No
Coriolis Interface	Multiple instances	Plunger Control	No
Data Transfer	Single instance	Shutdown System	No
Ethernet-Serial Passthrough	No	System	Always exported automatically. Single instance
Gas Lift	No	Therms Master	Multiple instances
Generic Communication App	No	Trend System	No
Holding Registers	No	Wireless Remote IO	Multiple instances
IO System	Single instance	XIO Server	Always exported automatically. Single instance
LevelMaster	Multiple instances	XIO Write Server	No

Application	Exportable	Application	Exportable
Liquid Coriolis Interface	Multiple instances	XIO Interface	No
		XMV Interface	Multiple instances

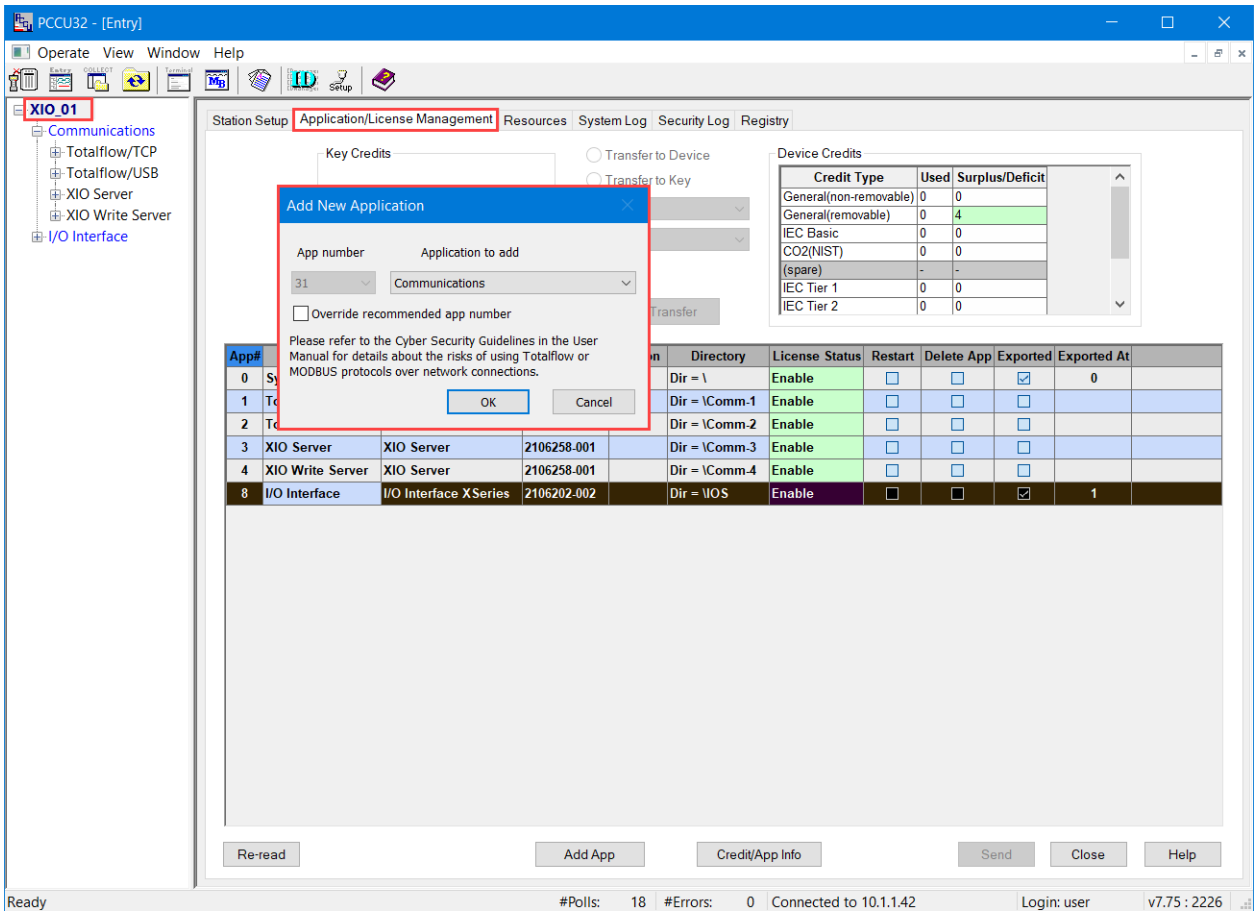
2.3.2.2 Verify or add applications on the XIO

Complete these steps in PCCU Expert view. Click **View** on the PCCU32 menu and select **Expert** from the drop-down list.

To verify the installed applications:

1. Connect to the XIO using PCCU.
2. At the top of the navigation tree, click the station ID name. The Station Setup tab displays.
3. Select the Application/License Management tab.
4. Verify instantiated applications in the table.
5. Click **Add App** to add required or additional applications. The Add New Application dialog displays.

Figure 2-12: Adding applications on the XIO – Application/License management tab



6. Click **Application to Add** and select the application from the drop-down list.
7. Click **OK**.
8. Click **Send** to save the application.

2.3.3 Configuration files

The configuration files contain the configuration or settings required for the operation of the XIO and applications. Configuration files can include initial (factory-defined) or user-defined settings or parameters. The XIO contains the following configuration files:

- Factory configuration is the ABB default factory configuration, or a customer-specific configuration programmed into the factory folder during final assembly. The factory configuration is read-only and stored in persistent memory. It can only be updated at the factory.
- Startup (cold) configuration is used for a cold restart of the device or when a configuration package is sent to the device by the PCCU loader. The startup configuration is stored in the tfCold directory and can be modified or updated as needed.
- Running (warm) configuration is used by the device during normal operation. The running configuration is stored in the tfData directory and can be modified or updated as needed.

2.3.4 Customer data collection files

The data collection files contain all the trend data the XIO generates. These data files are in the tfData directory with the running configuration files. The type and amount of collection data depend on the number and type of trends active on the device.

IMPORTANT NOTE: The tfData directory also contains the calibration files if the controller has been field-calibrated.

2.4 User interface

The PCCU32 software running in a Windows® environment is the main user interface to the XIO. PCCU32 supports several view levels and can be configured to provide role-based secure access to the controller for the following tasks:

- Initial configuration and commissioning (setup)
- Monitor the controller operation and performance
- Add, configure, and optimize applications (configuration)
- Calibration
- Data collection

2.5 Secure service access interface

The Secure Shell (SSH) and Secure File Transfer Protocol (SFTP) on the XIO allow secure login access and file transfer capability for advanced service access. SSH provides an encrypted communication channel, which requires private key authentication for access to the controller. Secure access is available for troubleshooting purposes only and is reserved for advanced users and ABB technical support or development personnel.

3 Installation

This chapter provides information for XIO installation and setup.

IMPORTANT NOTE: Read the installation chapter and review user drawings before beginning installation. Make sure to review safety warnings carefully.

WARNING– Bodily injury. Although there may be alternate methods of installation and commissioning of the XIO, ABB recommends that technicians perform the procedures in the order presented: plan, install, wire, then apply power, verify power-on sequence, and configure.

3.1 Site planning and requirements

XIO installation requires that customer-supplied enclosures, power sources, wiring, and location comply with the specifications described in this section.

WARNING– Bodily injury. Carefully review the specifications in this section to select compliant equipment. Failure to comply with these specifications may create unsafe conditions, resulting in bodily injury and equipment damage.

3.1.1 Enclosure requirements

Install an XIO standalone on a DIN rail on an interior wall, in an *X*CORE enclosure, or in a customer-supplied enclosure.

For general purpose nonhazardous locations, the XIO must be installed in an enclosure that complies with the following specifications:

- For general purpose locations, the enclosure must protect the XIO against shock and impact.

For hazardous locations, the XIO must be installed in an enclosure that complies with the following specifications:

- For Class I, Division 2, the enclosure must be rated at least Type 3R, according to the environment.
- Class I, Zone 2 requires an enclosure that meets IP54 rating and according to IEC 60529 and IEC 60079-0.

Verify that customer-supplied enclosures meet these requirements.

3.1.2 Location requirements

The installation location should:

- Allow access to the enclosure, XIO, power sources, cables and connections
- Be at a distance that does not exceed the maximum or recommended field wiring lengths for connections to peripherals or external equipment. Field wiring requirements depend on the type of connection. See section 3.1.4.

3.1.3 Mounting requirements

Mounting surfaces or walls require enough strength to support the hanging weight of the enclosure, and associated equipment to meet the requirements of IEC715.

3.1.4 Install antenna (for wireless functionality)

Wireless support is optional on the XIO. If your device has a wireless interface connector, make sure to obtain the antenna required to enable communication.

IMPORTANT NOTE: A Wi-Fi Antenna Kit (part number 2106049) is required for antenna installation. Order the kit option with the cable length appropriate for the size of the XIO enclosure. See the link to the Antenna Kit Installation Guide in Additional information.

1. Install the antenna to support onboard Bluetooth® and Wi-Fi® wireless interfaces.
2. Use the SMA connector on the XIO to connect the antenna (see Figure 2-1: XIO housing cover).

3.2 Wiring requirements

Field wiring must meet the following requirements:

- All wiring connections and the screw terminals for power support 14 – 24 AWG and communications support 16 - 24 AWG. Select the wire gauge according to the voltage and current requirements of the circuitry. The gauge differs for each application.
- Follow local electrical codes to select the appropriate wire gauge and type based on the load current, voltage, signal type, and indoor or outdoor environment.

NOTICE – Equipment damage. Field installation cable and conductors must be rated greater than 70 °C (158 °F) when installed in an ambient temperature of 60 °C (140 °F).

3.3 Unpack and inspect

The XIO and additional parts ship in a specially designed shipping carton with a Quick Start Guide, Safety and Compliance notice, and packing list.

IMPORTANT NOTE: If there is any damage to the shipping carton, keep it and the packing materials until the contents are inspected and found to be free of damage.

To unpack the XIO and inspect for damaged, missing, or incorrect parts:

- Inspect the shipping carton for damage.
- Carefully remove items from the carton.
- Keep all shipping materials to return parts.
- Compare the packing list with the materials received. Check for any missing or incorrect parts.
- Inspect each item for damage: XIO exterior and optional equipment, if purchased.

If there are missing, incorrect, damaged parts or noticeable defects, call the ABB main office number listed on the last page of this manual.

3.4 Basic hardware installation

This is an overview of a typical hardware installation. For different installations, call the ABB main office number listed on the last page of the manual.

NOTICE – Equipment damage. The XIO must always be mounted on a horizonal DIN rail, never vertically.

NOTICE – Equipment damage. Before powering the XIO, perform all the procedures in the order presented in this section.

DANGER – Serious damage to health / risk to life. Use properly insulated tools and wear a grounding strap to eliminate static electricity when connecting or disconnecting wires. Mishandling may cause a static electric discharge resulting in bodily injury and damage to the electronic components.

3.4.1 Ground the controller

The XIO must be mounted on a grounded DIN rail.

NOTICE – Equipment damage. The controller must be mounted on a DIN rail bonded to an earthing terminal. The bonding conductor must have a cross sectional area of at least 4 mm^2 (12 AWG).

To ground the DIN rail:

1. Screw the DIN rail onto the mounting surface.

2. Attach a grounding wire to the DIN rail.
3. Attach the other end of the wire to an electrical ground.

3.4.2 Standalone mounting

To mount the XIO:

1. Position the XIO on the DIN rail.
2. Push the XIO onto the DIN rail until it snaps into place.

IMPORTANT NOTE: To remove the XIO, insert a slotted screwdriver into the access slot of the DIN rail and release the clip to loosen. See section 8.6.3 Remove the XIO from the DIN rail.

3.4.3 Mounting when using an enclosure

The *X*CORE enclosure has tags for wall-mounting (Figure 3-1). Mount the enclosure per field specifications. The XIO is usually already mounted on an internal DIN rail inside the enclosure.
To use non-ABB enclosures, follow the vendor's mounting instructions. The DIN rail can be installed on a wall or in an enclosure that meets the environmental ratings for that location. It is recommended that 4 inches of clearance be available above and below the device, and 1 inch to the left and right of the XIO, or the XIO and any TFIOs connected.

Figure 3-1: *X*CORE enclosure top mounting tabs and interior view

3.4.4 Wire serial communication ports

Wire the XIO serial communication (COM) ports to communicate with and power external devices. Wire for communication according to the type of serial interface with the external device. Wire for power if there is no external supply powering the external device.

IMPORTANT NOTE: The maximum amount of current draw is 5A for all connected devices (XIO/RMC, TFIO modules, and auxiliary field wired equipment).

This section provides wire length specifications per serial interface type, tables for port pinouts and generic instructions for field wiring. There are also two examples of serial communication in the following table.

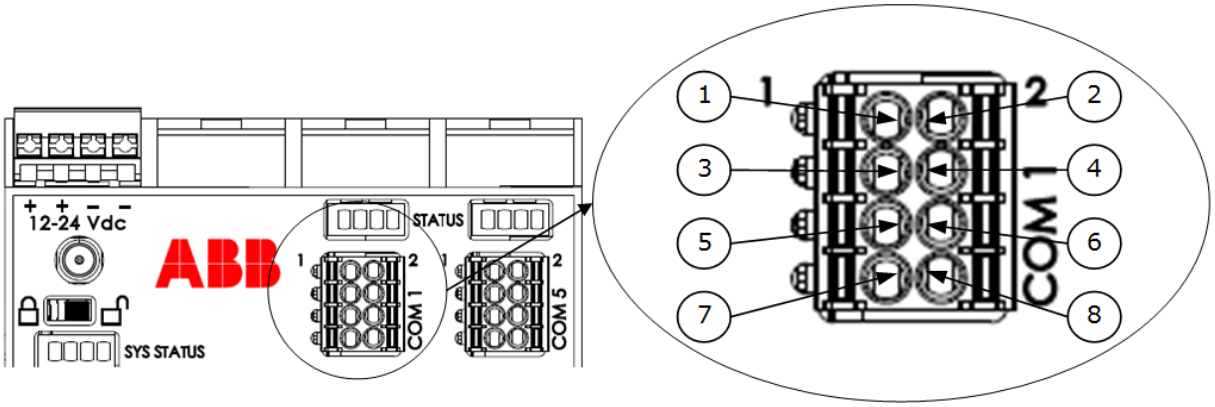
Table 3-1: Serial communications specifications

Communication type	Maximum wire length	Termination
RS-232	50 ft (15 m)	Removable Terminal connector (8 POS), spring-cage termination. Wire Gauge 16 AWG to 24 AWG. Use ferrules without insulating collar, according to DIN 46228-1 as specified in Table 3-2.
RS-485 or RS-422	4000 ft (1220 m)	

Table 3-2: Ferrule specifications

Cross section	Length
0.25 mm²	5 mm to 7 mm
0.5 mm²	8 mm to 10 mm
0.75 mm²	8 mm to 10 mm
1 mm²	8 mm to 10 mm
1.5 mm²	10 mm

Figure 3-2: COM 1 to COM 8 serial communication port pinouts



Legend: COM 1 to COM 8 serial communication port pinouts

PIN	RS-232	RS-485	RS-422
1	Voltage out (VOUT)	Voltage out (VOUT)	Voltage out (VOUT)
2	Ground (GND)	Ground (GND)	Ground (GND)
3	Switched voltage (SW VOUT)	Switched voltage (SW VOUT)	Switched voltage (SW VOUT)
4	Ground (GND)	Ground (GND)	Ground (GND)
5	Request to send (RTS)	Transmit/Receive (BUS+)	Transmit Bus + (TBUS+)
6	Transmit data (TX)	Transmit/Receive (BUS-)	Transmit bus – (TBUS-)
7	Request to send (RX)	Not Used	Receive bus + (RBUS+)
8	Clear to send (CTS)	Not Used	Receive bus – (RBUS-)

To wire the serial communication port:

NOTICE – Equipment damage. Pin 1 (VOUT) or pin 3 (SW VOUT) can power an external device on all COM ports. The external power supply connected to the power port determines the output voltage at these pins.

Verify that the device is compatible with the input voltage at the power port before connecting to these pins. Connection to an incompatible device can result in damage to the device.

1. Pry the terminal connector off the electronic board by hand (use a slotted screwdriver if necessary).
2. Trim the wire covering back 10 mm (0.400 in) on each wire.
3. Place the trimmed end of the wire in the ferrule and crimp the metallic portion of the ferrule with a crimping plier.
4. Insert the ferrule into the cage available for wire and push until it latches on. Ensure the wire is securely latched.
5. Insert the wires at the correct pin according to Figure 3-2: COM
6. Insert the wires into the required pins if the device is powered from the COM port:
   - Use pin 1 (VOUT) and pin 2 (GND) to provide constant voltage.
   - Use pin 3 (SW VOUT) and pin 2 (GND) to provide switched voltage.

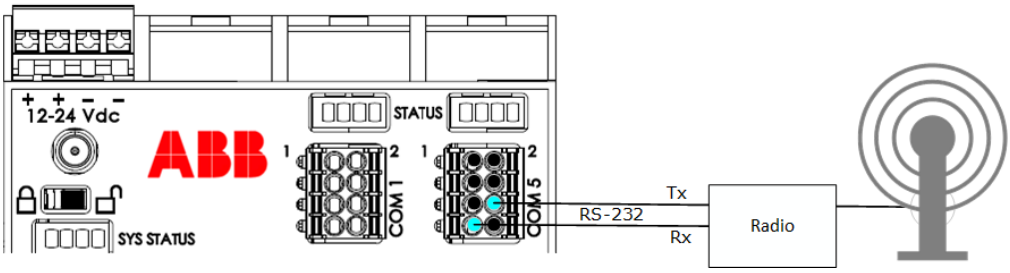
NOTICE – Equipment damage. Do not push the ferrules too hard into the terminal connector. This can damage the connector or the ferrule.

7. Insert the terminal connector onto the COM port if it was removed.

3.4.4.1 Wire remote communications equipment (radio)

The serial communication (COM) ports can be wired with remote communication equipment, such as a radio. Figure 3-3 shows the connection between radio equipment and one of the COM ports. In this example, the COM port is configured as an RS-232 port, which provides point-to-point communication.

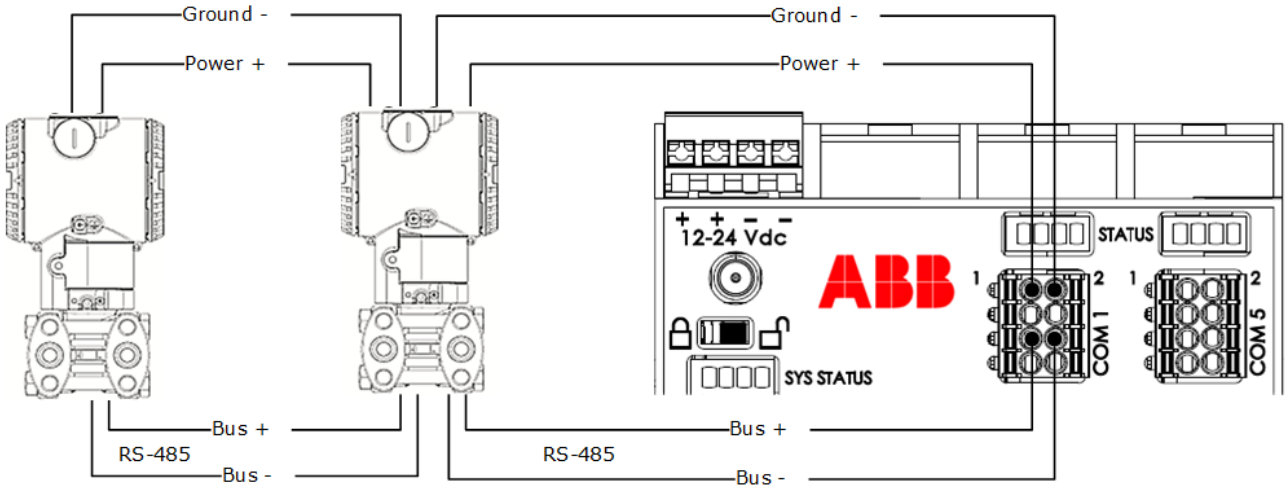
Figure 3-3: Serial communication with radio equipment



3.4.4.2 Wire multiple peripheral measurement devices

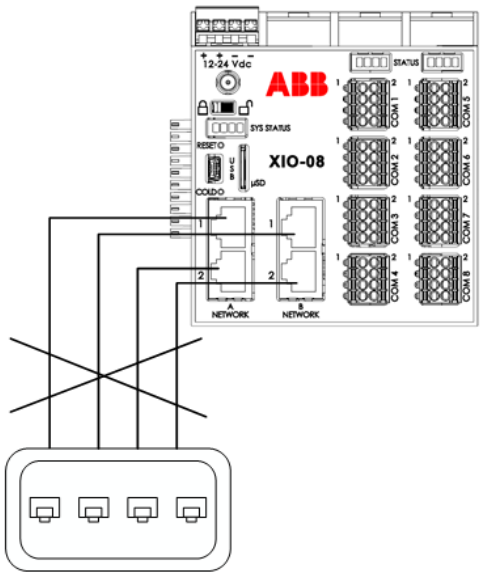
The controller serial communication (COM) ports can connect to peripheral measurement devices, such as multivariable transmitters. Figure 3-4 shows the connection between one of the COM ports and two multivariable transmitters. In this example, the COM port is configured as an RS-485 port, which provides both point-to-point or multi-point communication. The example shows the two transmitters connected to the controller for communication and power. This is controlled by the comm application using SW VOUT.

Figure 3-4: COM 1 for RS-485 communication with multiple devices



As illustrated in the following drawing, do not connect A1 and A2 or B1 and B2 to the same Ethernet switch if they are in 1 Network Mode. Connecting both sets of ports to the same switch disables the ports.

Figure 3-5: Wrong Ethernet connection



3.4.5 Connect TFIO modules

TFIO modules connect directly to the TFIO ports on either side of the XIO. For additional information, refer to the TFIO Module User Manual under Additional information.

DANGER – Serious damage to health / risk to life. Do not connect or disconnect TFIO modules, connectors or their terminations while energized unless the area is known to be non-hazardous.

NOTICE – Equipment damage. When the TFIO interface is disabled, the modules remain powered. Remove the power from the XIO before connecting or disconnecting additional TFIO modules. Failure to power down the XIO can result in damage to the module. The procedure in this section assumes the XIO is powered off.

Table 3-3 identifies the different module types available with the XIO that supports 12 volts to 24 volts operation. The XIO does not support the TFIO CIM module, part number 2100421.

Table 3-3: TFIO modules

TFIO module	Part number
Valve Control Combo IO	2100412
4-20 mA Analog Output	2100415
Type II Analog Input	2100418
Combo Digital	2100543
Thermocouple Input	2100869
RTD Input	2101018

NOTICE – Equipment damage. Power compatibility for TFIO modules depends on module type:

- Older green modules must only use 12 Vdc.
- M2 modules and newer grey modules can use 24 Vdc.
- A combination of green modules, and M2 modules or grey modules, must only use 12 Vdc.

The TFIO modules are hot-pluggable and can be removed or detached when the XIO is powered. However certain locations and conditions may require powering off the XIO before TFIO module insertion or removal.

DANGER – Serious damage to health / risk to life. Do not perform any wiring or removal/insertion of modules unless it is known that a potentially explosive atmosphere condition does not exist.

These instructions do not address the requirements for installations in potentially explosive atmospheres.

Wiring between the XIO, TFIO modules and field equipment must meet the requirements for installation in accordance with the local and national electrical codes.

IMPORTANT NOTE: This procedure assumes that the XIO power and TFIO-IO modular connectors have been correctly wired. The XIO and I/O connectors can be attached or removed without removal of wiring. Always remove the wired connectors attached to the TFIO modules prior to insertion or removal on the XIO.

To connect the TFIO module(s):

NOTICE – Equipment damage. The output voltage at the following pins depends on the external power supply connected to the power port:

- J2-1, J4-1 and J4-3 (on the TFIO valve control interface module)
- J1-1, J2-1, J3-1, J4-1 (on the TFIO analog output module)

Before connecting to these pins, verify that the external device is compatible with the input voltage at the power port.

1. Remove the power connector from the XIO (see 4.9.1 Connect the TFIO modules to the XIO).
2. Remove wired connectors from the TFIO(s).
3. Attach the TFIO module to the DIN rail.
4. Position it beside the XIO and snap them together.
5. Attach the next TFIO module to the DIN rail.
6. Position it beside the previously attached module and snap them together.
7. Repeat steps 3 and 4 to attach the additional TFIO modules as required.
8. Attach I/O wired connectors to the TFIO(s).
9. Reconnect power to the XIO.
10. Wait for the XIO to reinitialize.

IMPORTANT NOTE: TFIO port supports a maximum of 22 modules.

11. Loosen the terminal connector screws for the correct pin.
12. Insert the wires in the required TFIO pins.
13. Tighten the terminal connector screws.

Proceed to configure the I/O Interface application next.

To configure the TFIO, see section 4.9 Configure the I/O Interface.

3.5 Power the XIO

This section describes the power-on sequence and instructions to set up the external power supply.

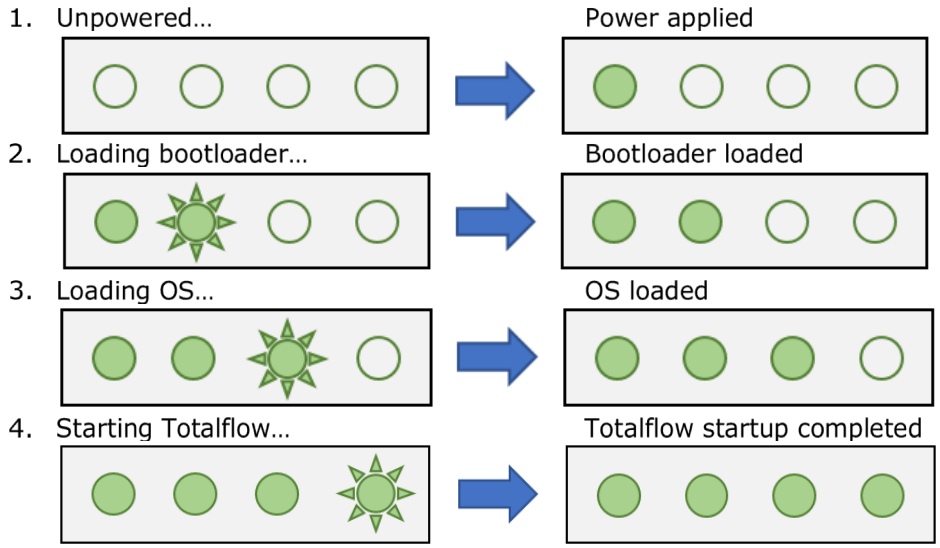
NOTICE – Equipment damage. Before applying power to an XIO with TFIO modules attached, be sure to check the module's sale/data sheet for power rating compatibility. Some modules are rated for 12 Vdc while others are rated for 24 Vdc. When combining modules that include those rated for 12 Vdc operation, do not apply power that exceeds 12 Vdc.

IMPORTANT NOTE: Externally fuse the power input for the load. This consists of the equipment plus any external devices powered by the XIO. The wire gauge should be appropriate (in some applications a minimum of 16 AWG gauge is advisable).

3.5.1 Power-on sequence

The XIO power-on sequence initiates when power is connected. The SYS STATUS LEDs display the following information as the controller completes its startup:

Figure 3-6: LED power on sequence



IMPORTANT NOTE: The XIO design has a super capacitor (Super CAP) that is a short-term power reservoir (see section 2.2.8 Super capacitor for more details). The first time the unit powers on, or if the XIO is left powered off for several hours or longer, the boot time is approximately two minutes to allow charging of the super capacitor. The boot time is considerably less once the capacitor is fully charged.

3.5.2 Power with external power source

The unit receives power from an external power supply (12 to 24 Vdc). Remove the power terminal connector to wire the power cable before connecting the power supply to the board.

DANGER – Serious damage to health / risk to life. Explosion Hazard: A customer provided and installed 5 A fuse in the power source line is required. Components on the boards that overheat due to higher fuse rating could ignite in the presence of explosive gas.

WARNING – Bodily injury. To prevent injury, only permit a licensed electrician to install Vac wiring.

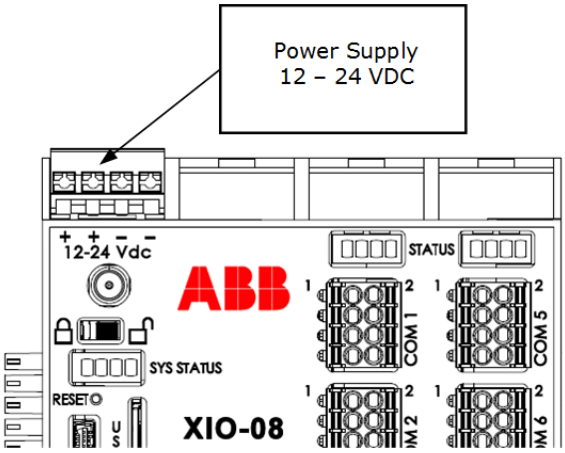
IMPORTANT NOTE: The external power supply must meet the specifications in section 2.2.3 External power supply requirements.

All wiring must comply with national and local electrical codes and applicable ABB certification drawings to maintain system certification.

To wire an external power source to the XIO:

1. Follow the manufacturer's instructions supplied with the external power supply to install and connect the power source.
2. Pry the power port removable terminal connector off the electronic board with a slotted screwdriver.
3. Trim back the covering on the end of the power cable that connects to the controller 10 mm on each wire.
4. Place the trimmed end of the wire in the ferrule and crimp the metallic portion of the ferrule with a crimping plier.
5. Press the orange-colored spring-cage latch at the top of the terminal connector, insert the ferrule inside the cage and release the latch. Make sure the wire is securely latched.
6. Repeat Step 5 for other wires. Observe the polarity (+ and -).
7. Insert the wired terminal connector into the power port.

Figure 3-7: Connect the external power supply



8. Apply power to the external power supply.
9. Observe the power-on sequence on the SYS STATUS LEDs to verify that the XIO is receiving power. See details in section 3.5.1, Power-on sequence. When all four LEDs are solid green, the sequence is complete.
10. Press **Reset** if the power-on sequence fails to initiate or complete.

4 Startup

This chapter describes the setup and configuration procedures to activate a newly installed XIO system. Complete the XIO configurations through the Windows®-based interface software PCCU32.

IMPORTANT NOTE: The XIO equipment requires PCCU32 version 7.68 or newer. Previous versions of PCCU32 are not compatible. PCCU32 must be installed in the PC or laptop used to configure the XIO. To download and install the latest PCCU32 version, see the next section. Click **Help** on any screen used for configuration. Online help topics are available for each PCCU screen.

4.1 Download PCCU32 from the ABB global website

The latest PCCU version is available on the ABB website. Please note that the major version of PCCU is used to list the available software on the site, but the installation package file name contains the part and revision numbers: 2103445-XXX, where 2103445 is the unique part number for PCCU, and XXX is the

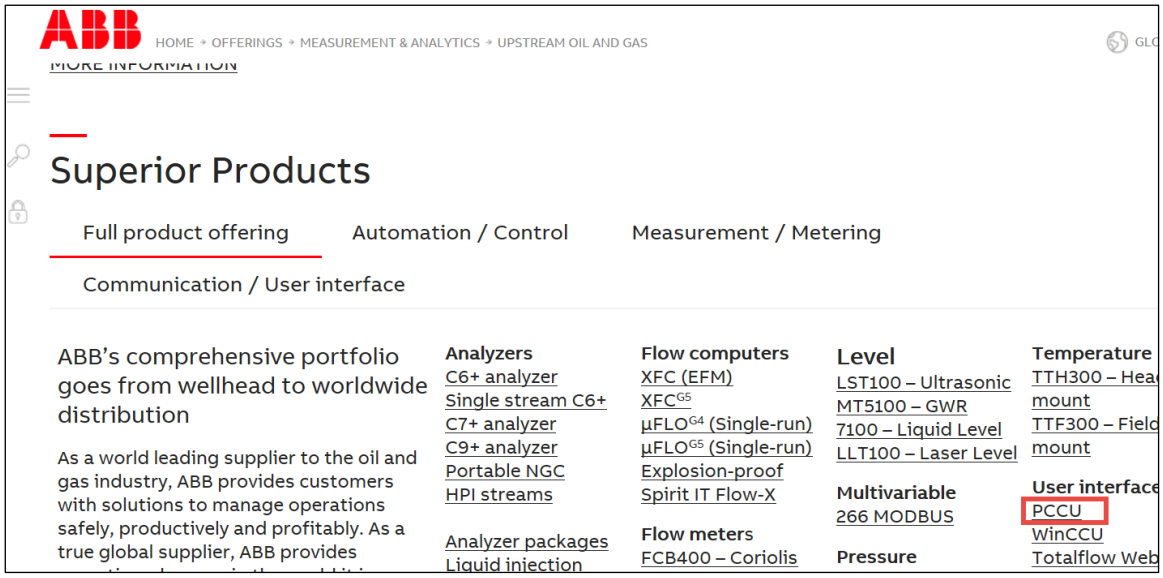
revision number. For example, the installation package for PCCU 7.74 has the number 2103445-098 in the file name.

Always review release notes for new features or bug fixes before installing and using new versions.

To review release notes and download PCCU:

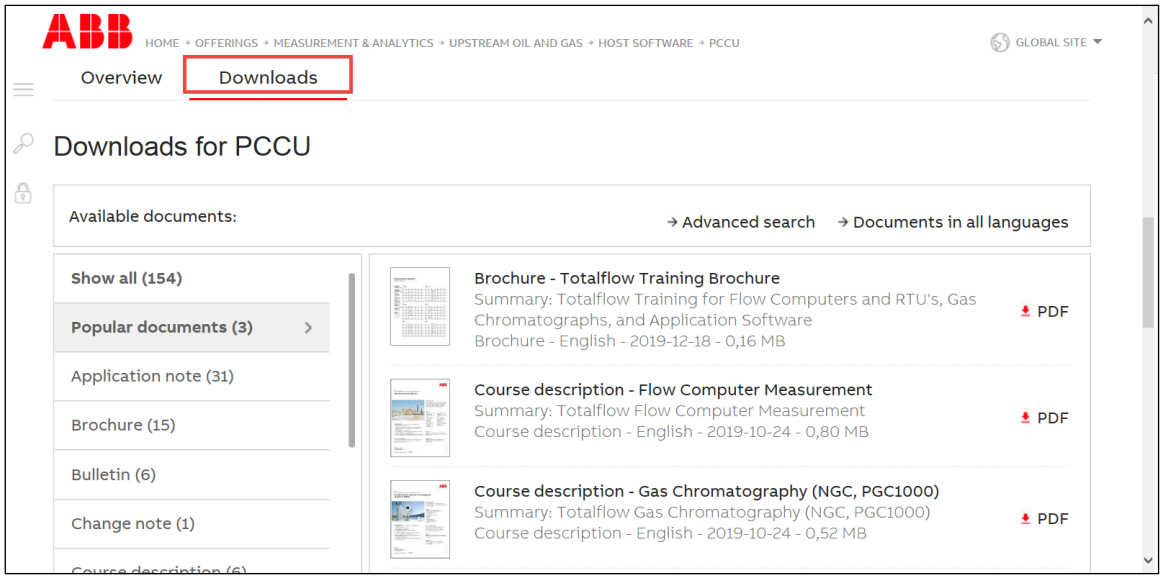
1. Go to www.abb.com/upstream.
2. Under Products, select **PCCU** from the User Interface category.

Figure 4-1: ABB Upstream home page



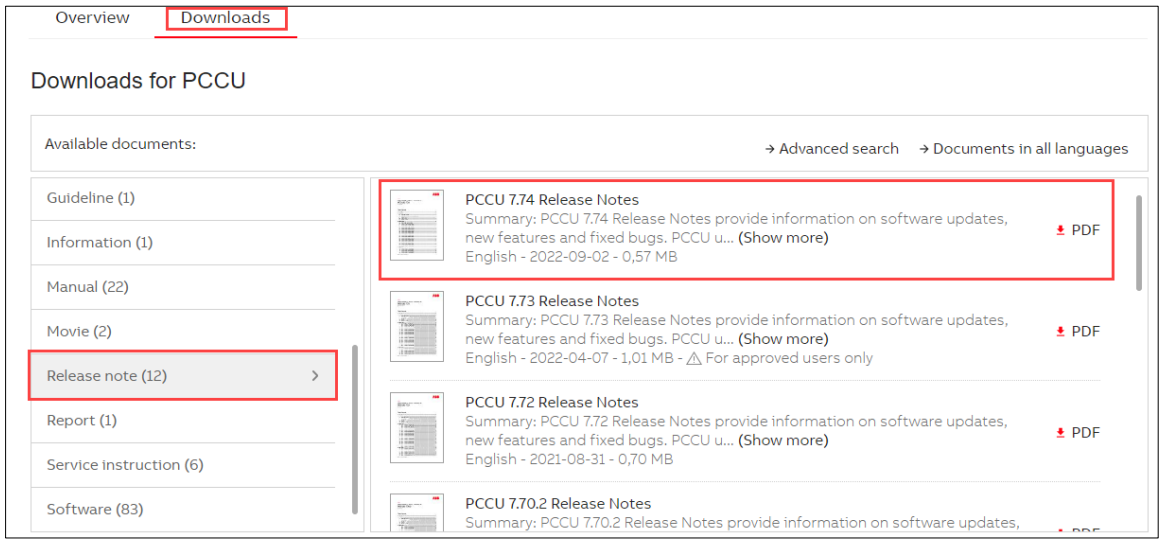
3. On the PCCU page, scroll down and select the **Downloads** tab.

Figure 4-2: PCCU page - document downloads



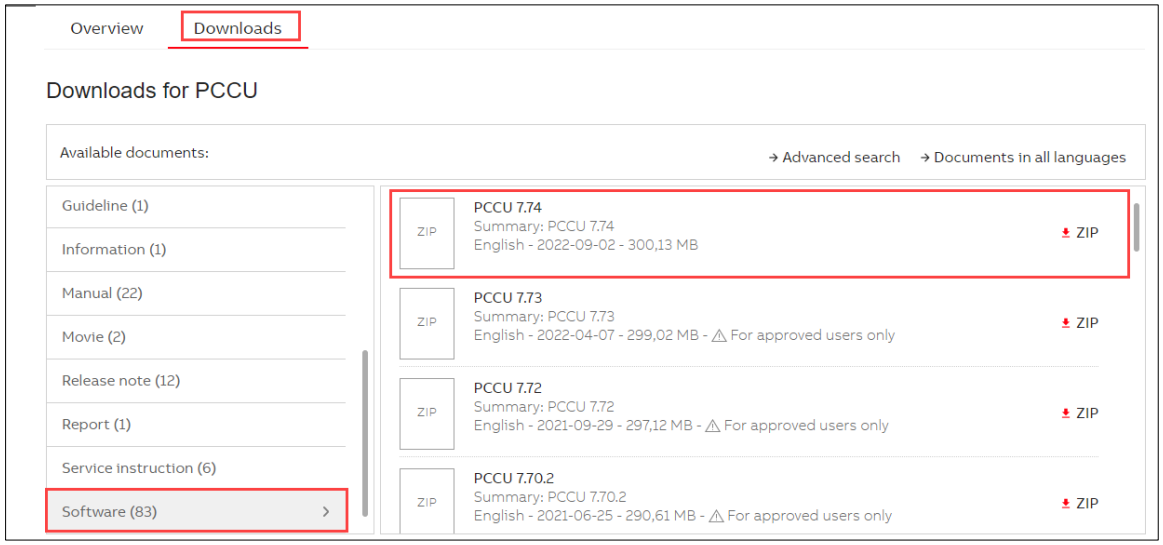
4. On the Downloads for PCCU page, scroll down on the left menu of available documents, locate, and select **Release note** (Figure 4-3).

Figure 4-3: Release notes list



5. Locate the release notes for the latest revision on the displayed list. There may be release notes for other versions. Make sure to select the required one.
6. Select the release notes to view from the browser.
7. Scroll down on the left menu again to locate and select **Software** (Figure 4-4).

Figure 4-4: PCCU installation software revisions list



8. Locate and select the latest software version in the displayed list (identified by major revision number, such as PCCU 7.74).
9. Select the **ZIP** icon to download. The installation package file name has the part and rev number, for example: 2103445-098EX.ZIP.
10. Select **Save** at the download prompt.
11. Save the file on the laptop used to configure the device.

4.2 Install PCCU32

PCCU32 software operates in a Windows® environment. To install PCCU32:

12. Locate the downloaded compressed file on the PC or laptop.
13. Unzip (Extract files) the downloaded installation file and save files in desired folder.
14. Open created folder.

15. Double-click **setup.exe** to run the installation program. Follow the screen prompts during installation.
16. Click **Finish** when installation completes.

4.3 Establish local communication

Connect the laptop to the USB or Ethernet ports to establish initial local communication. These ports are configured at the factory for local operator access. Configure PCCU to use any of these ports.

- To use USB, see section 4.3.1 Using the USB port
- To use Ethernet, see section 4.3.2 Using the Ethernet ports

IMPORTANT NOTE: External weatherproof local communication connectors (USB or Ethernet) are available on *X*CORE enclosures, if purchased. Use external ports to connect locally if the XIO is inside an enclosure. If the XIO is a standalone device, use the USB or Ethernet ports.

Do not use external enclosure connectors for permanent field connections. These connectors are only for local access during configuration or maintenance.

4.3.1 Using the USB port

The following instructions apply to USB port connections. Table 4-1: USB cabling provides cabling details to connect to the USB port.

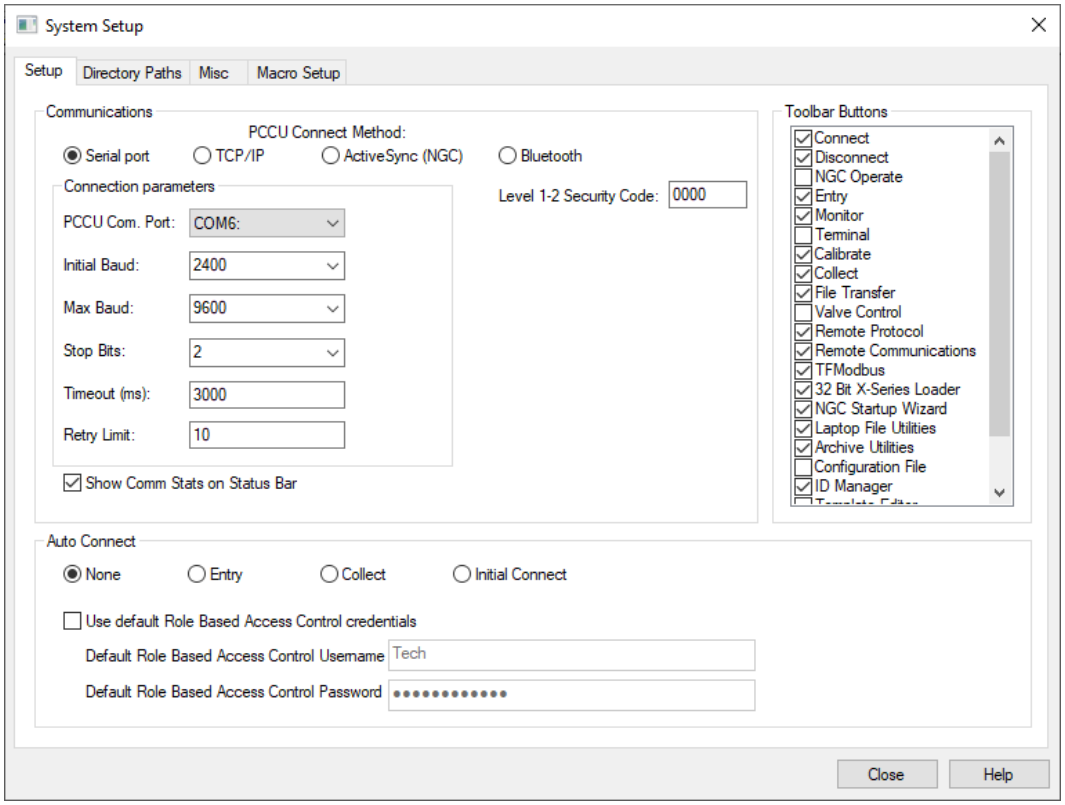
Table 4-1: USB cabling

Host system interface type	Required cabling termination (connectors) or adaptors	ABB part number
USB 2.0 Type A receptacle	USB 2.0 Type mini-B plug to USB 2.0 Type A plug cable (referred as USB PCCU32 cable)	1801800-xxx

To set up communication using the USB port:

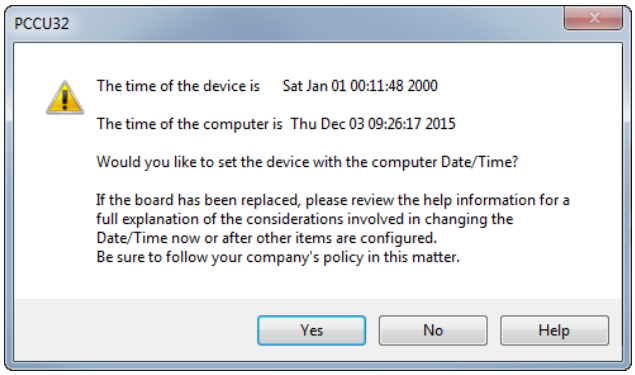
1. Power on the XIO and the laptop or PC. All the SYS status LEDs display green when the XIO completes startup.
2. Connect the laptop to the USB port.
3. Launch PCCU.
4. Click **Setup** on the PCCU32 toolbar menu. The System Setup window displays (Figure 4-5).

Figure 4-5: PCCU system setup (USB communication)



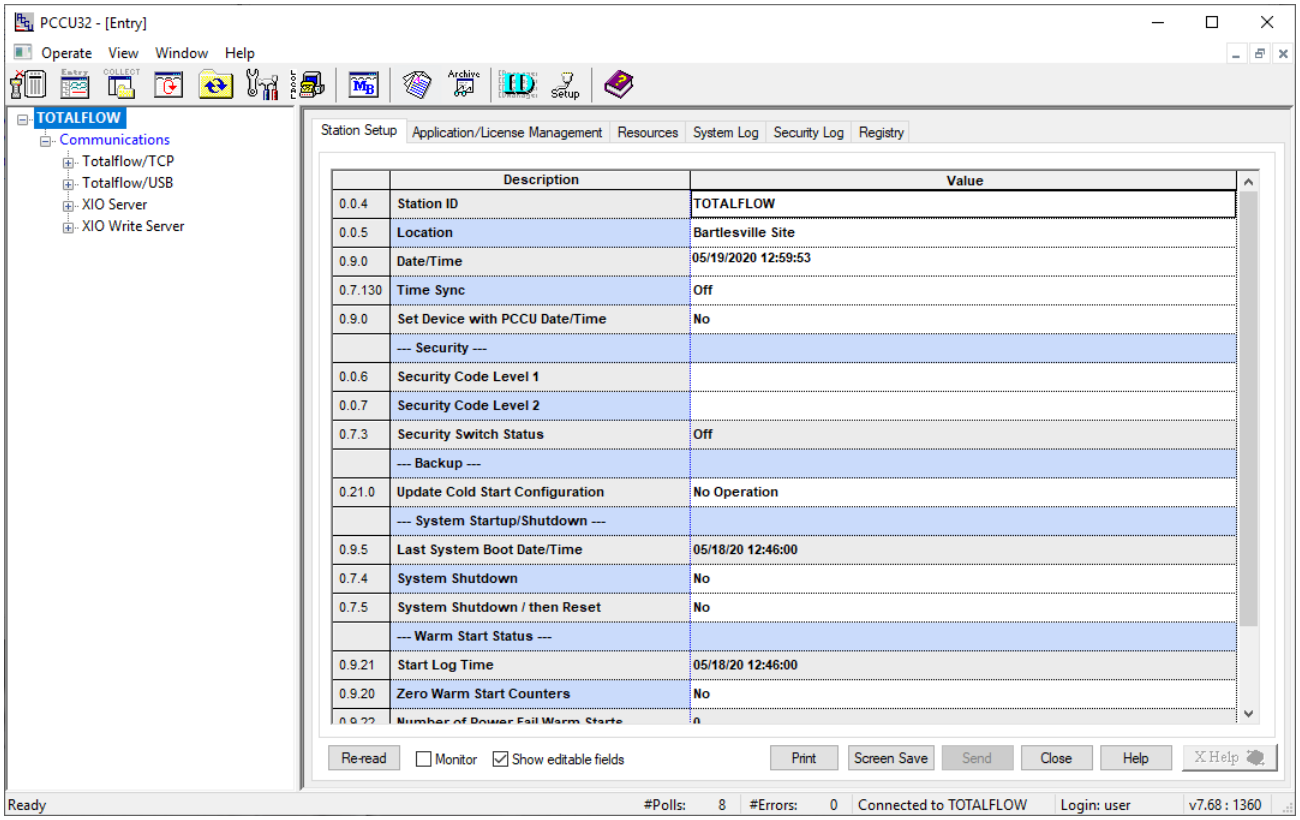
5. Under PCCU Connect Method, select **Serial port**.
6. From the **PCCU Com. Port** drop-down list, select the computer USB port where the cable connects.
7. Click **Close**.
8. Click **Entry** on the PCCU32 toolbar to connect to the device.
9. Click **Yes** if the message to synchronize the date and time displays. This message displays if the XIO calendar clock does not match the laptop's date and time which is usually the case with a new system.

Figure 4-6: Synchronize date and time



10. Verify that the connection is successful when the PCCU32 Entry screen displays.

Figure 4-7: XIO default screen – Entry mode (Advanced view)

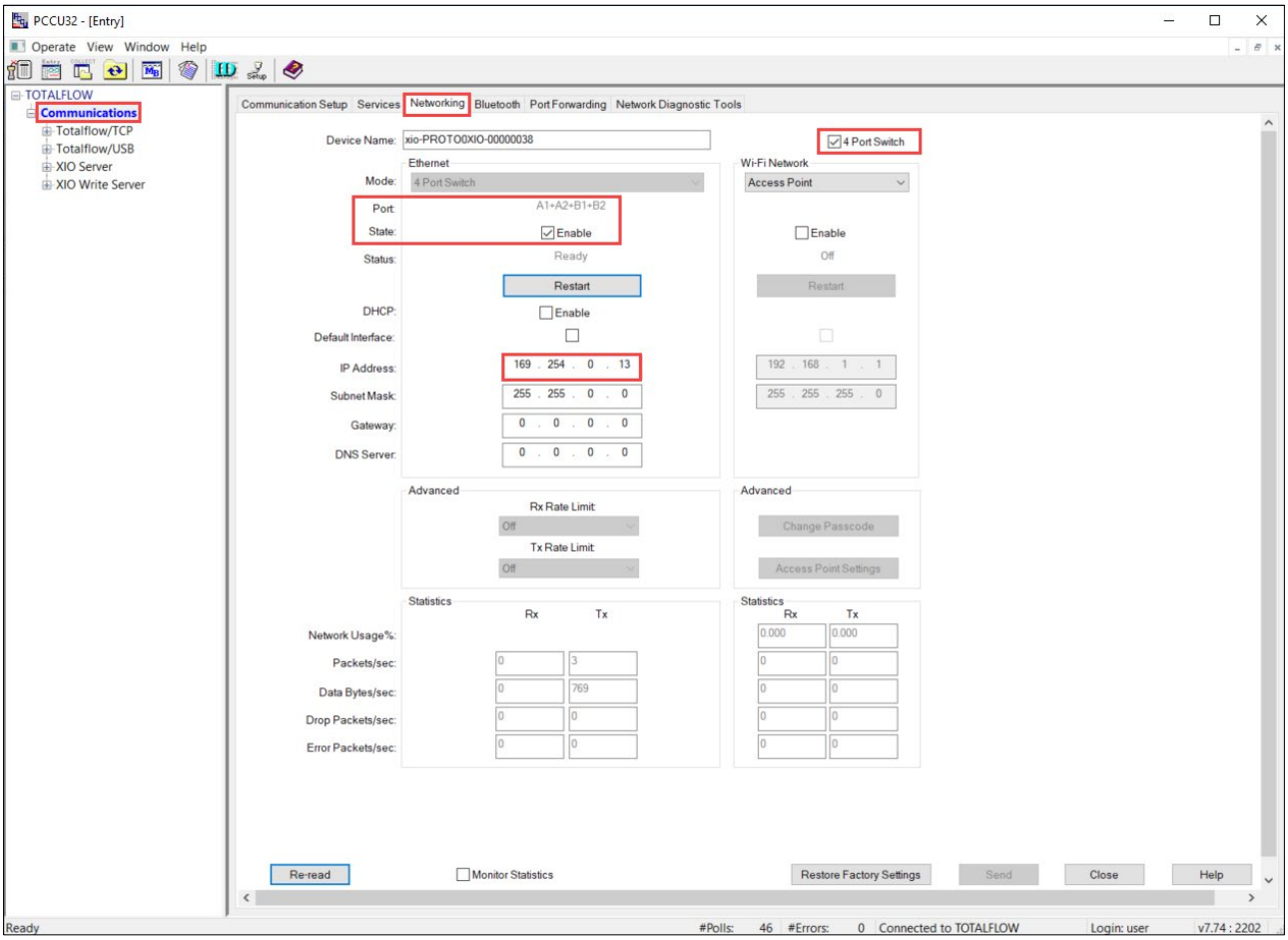


11. Proceed to configure the XIO:
    a. To use Ethernet, complete the steps in section 4.3.2 Using the Ethernet ports first, change to expert view (section 4.4 Change PCCU to Expert view), and then proceed to section 4.5 Configure basic XIO parameters.
    b. To use USB, remain on the current USB connection, change to expert view (section 4.4 Change PCCU to Expert view), and then proceed to section 4.5 Configure basic XIO parameters.

4.3.2 Using the Ethernet ports

The XIO Ethernet interface supports local TCP/IP communications and is configured as a 4-port switch from the factory. A default IP address (**169.254.0.13**) is ready for initial local communication using any of the 4 ports. All ports are enabled by default.

Figure 4-8: Default IP configuration



The following table lists the cabling details for connecting to the XIO Ethernet ports.

Table 4-2: Ethernet cabling

Supported devices (with Ethernet 10/100 BaseT ports)	Required cabling termination (connectors) or adaptors	ABB part number
Host system (operator laptop or computer) Network device (Ethernet hub, switch or router) Other Totalflow devices: additional XIOs, RMCs, flow computers, and analyzers	Straight-through Ethernet CAT 5 cable with RJ-45 connectors at both ends.	1681011 Maximum distance: 100 meters (328 feet)

IMPORTANT NOTE: Operators can initially connect to any of the 4 ports and use the same factory default address when the XIO is configured in 4-port switch mode. For other modes and configurations, use the appropriate IP address and port for local communication. Access to an Ethernet port for direct connection depends on the final connection topology of the XIO and other devices after the installation is complete.

4.3.2.1 Configure the host system

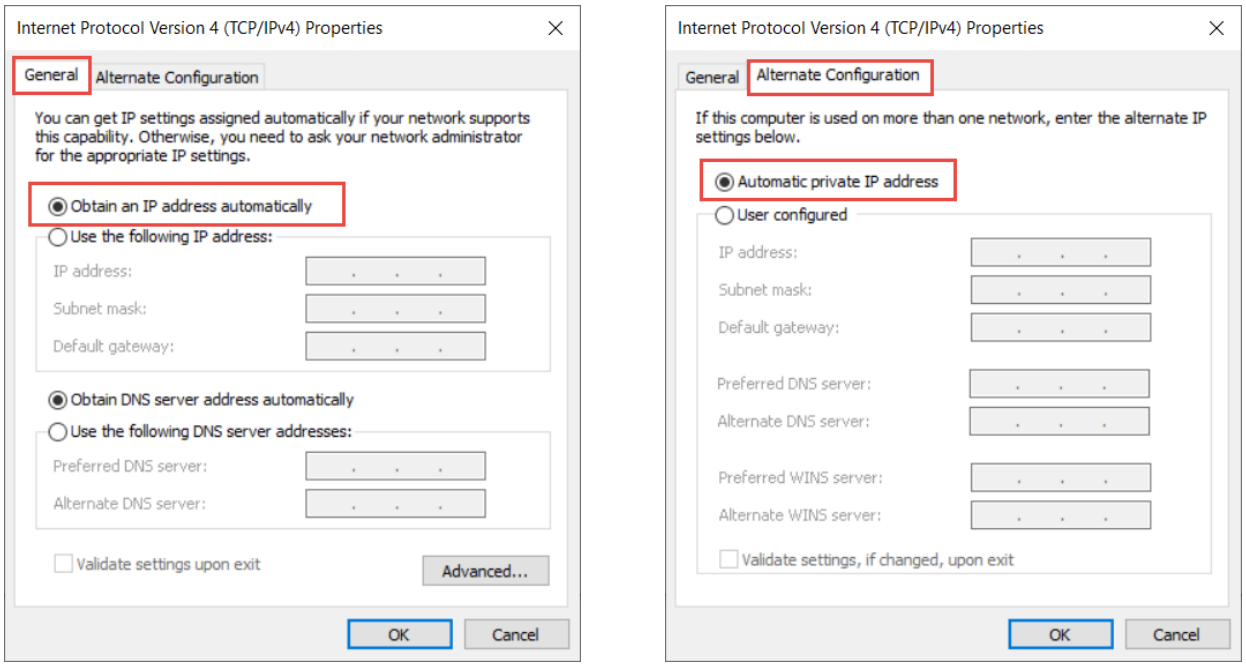
Configuration of the host system may or may not be needed:

- If the laptop is configured to automatically obtain the IP address, do not change the TCP/IP configuration. Proceed to section 4.3.2.2 Set up PCCU32 and connect.

– If the laptop has a static TCP/IP configuration, configure it for dynamic IP addressing and private addressing as the example shows in figure (Figure 4-9).

IMPORTANT NOTE: Detailed configuration steps for the host system vary depending on the operating system version. Typically, you can configure IP properties from the Windows® **Control panel**>**Network and Internet**>**Network Connection** screen. Configure IP properties for the **Local Area Connection** Ethernet interface. Review Microsoft Windows help topics if unable to locate the configuration options.

Figure 4-9: IP configuration for host system

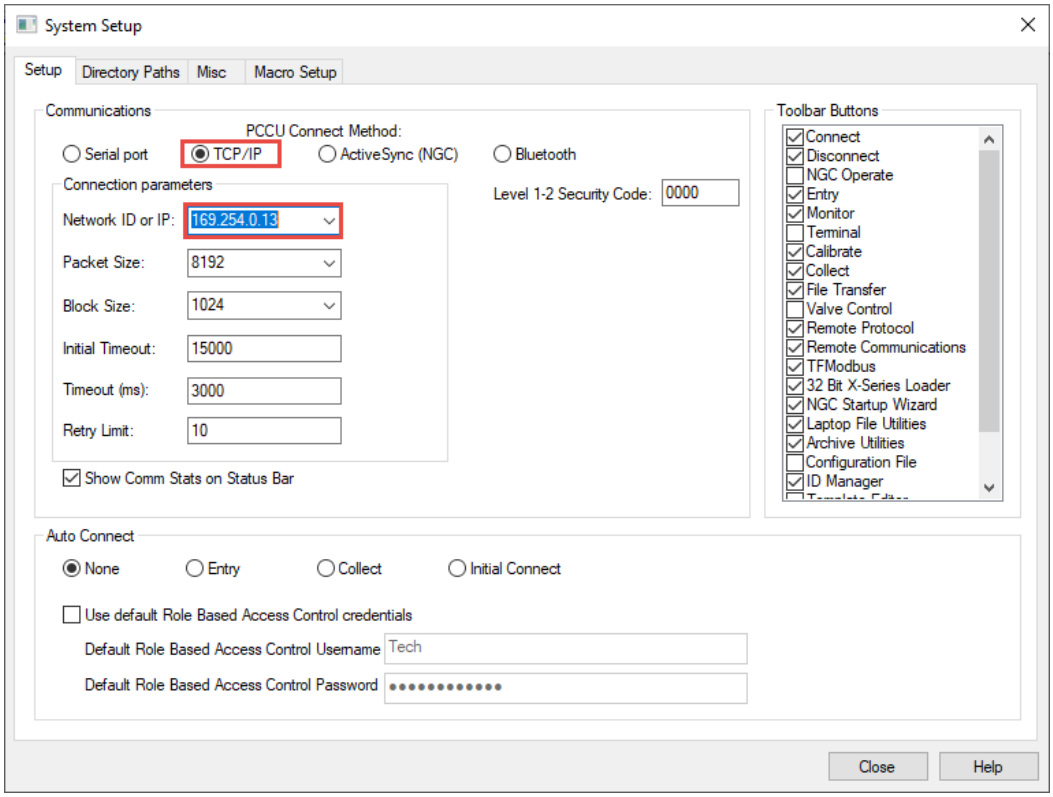


4.3.2.2 Set up PCCU32 and connect

To configure PCCU32 for TCP/IP communication:

1. Power on the XIO and the laptop or PC.
2. Connect the Ethernet cable.
3. Launch PCCU.
4. Click **Setup** on the PCCU32 toolbar menu. The System Setup window displays.
5. Click **TCP/IP**.
6. Under Connection Parameters in the Network ID or IP field (Figure 4-10), type the default IP address (**169.254.0.13**).

Figure 4-10: PCCU setup for local Ethernet communication



7. Click **Close**.
8. Click **Entry** on the PCCU32 menu bar to connect to the device. When the connection is successful the PCCU32 Entry screen displays.
9. Proceed to section 4.4 Change PCCU to Expert view.

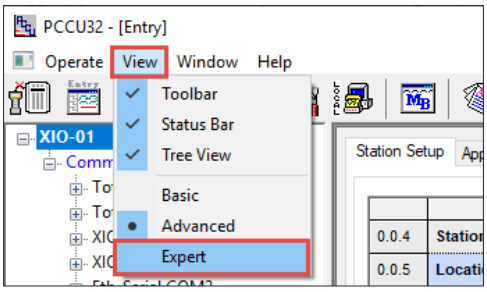
4.4 Change PCCU to Expert view (required)

Change the PCCU Entry screen to Expert view to complete the XIO startup and configuration procedures. This procedure assumes a successful PCCU connection with the device is already established.

To change to Expert view from the Entry screen:

1. Select **View** > **Expert** on the top PCCU menu.

Figure 4-11: Expert View screen



2. Wait for the screen to refresh to Expert view.
3. Stay on Expert view through the startup and configuration process.

IMPORTANT NOTE: The **Show editable fields** option is available at the bottom of PCCU entry screens. When you select this option, user-configurable fields display white. Please note that when this option is selected, some fields that display function statuses may not show color. If you wish to show colors, then clear this option and always remember to click **Re-read** to refresh the screen.

Proceed to configure the device in section 4.5.

4.5 Configure basic XIO parameters

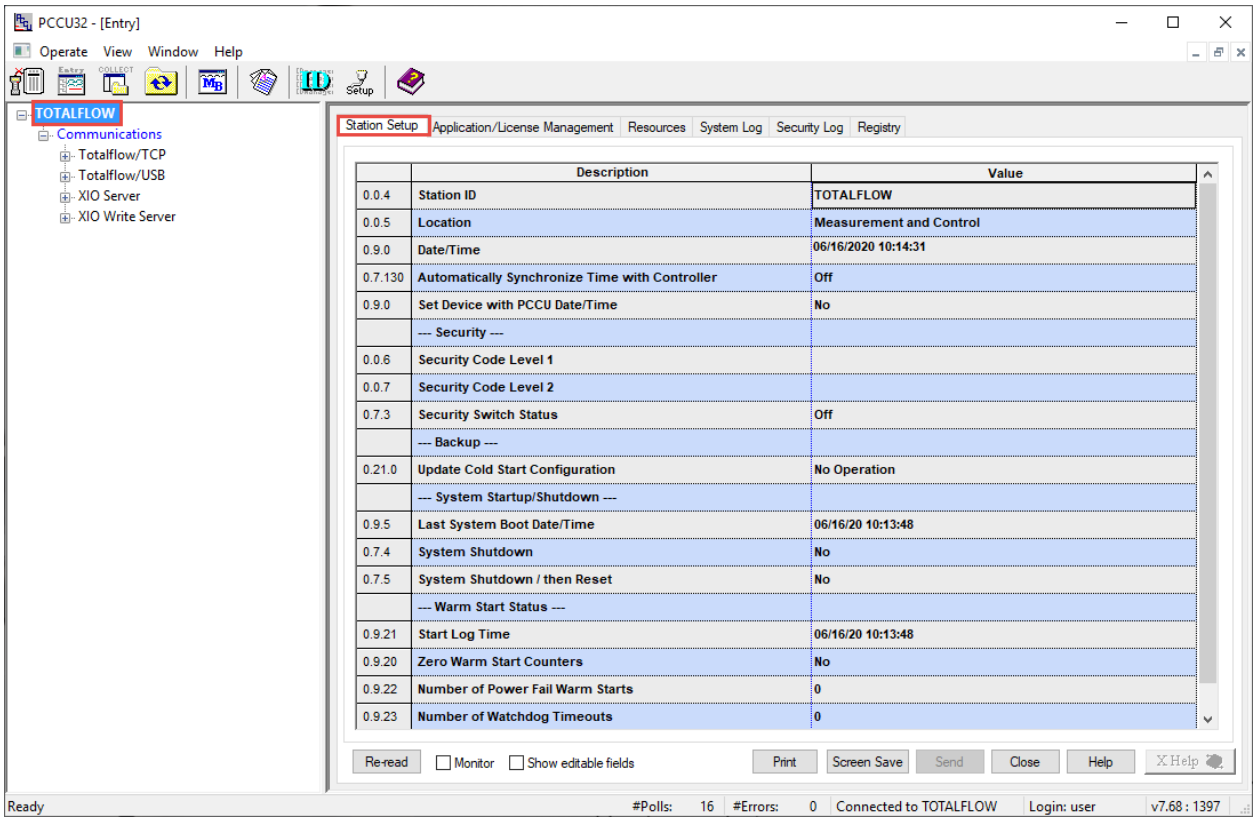
This section covers basic setup and configuration of the XIO after the local connection is established. This procedure assumes that PCCU communication setup is already configured for the appropriate port type: USB or Ethernet.

IMPORTANT NOTE: You must change the XIO factory default Station ID at first time installation. Unique Station IDs differentiate every XIO and their advertised services on a network. In multi-XIO installations, ensure all assigned IDs are unique before connecting the XIOs to the same network. Station ID updates after the remote controller and the XIO have established connection and are operational causes communication failure and service disruption.

To configure the XIO:

1. Click **Entry** to display the Entry screen.
2. Click the station ID (default name is TOTALFLOW) at the top of the navigation tree. The Station Setup tab displays.

Figure 4-12: XIO Station Setup default screen



3. Set up the basic settings identified in Table 4-3. See Figure 4-13 which shows an XIO with a unique ID. Refresh the navigation screen for the new XIO ID to show after configuration. It is very important that a unique ID is defined before attempting to configure communications with an RMC. The XIO ID is automatically detected by the RMC over the network and eases configuration.

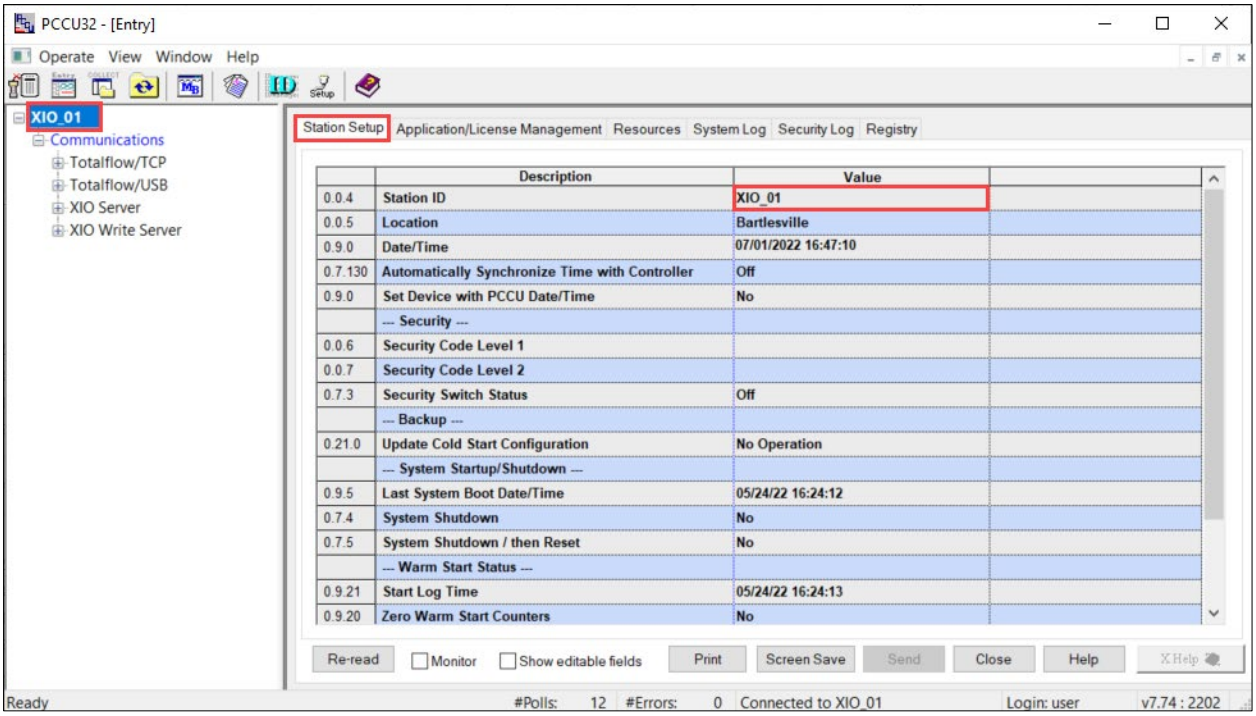
IMPORTANT NOTE: Use a unique Station ID for each XIO. The ID is limited to ten characters. It is recommended to limit special characters to spaces or underscores (_).

Table 4-3: Required station setup

Required entry	Format	Description
Station ID	10-digit alphanumeric	Name that uniquely identifies each installed XIO. This name is detected by remote controllers (using Auto Discovery) and must be unique. It is recommended not to leave the factory default name even when installing a single XIO.
Location	24-digit alphanumeric	Describes the physical location of the device, such as the county name or road number.
Date/Time	MM/DD/YYYY HH:MM:SS (24-hour clock)	Date and time must agree with the collection equipment. For initial installations, if you replied "yes" to the request to synchronize data and time with your laptop when you connected with the device for the first time, you do not need to change these values.

IMPORTANT NOTE: The XIO Station Setup function: Automatically Synchronize Time with Controller, sets the time of the XIO to match that of the remote controller it connects to (within a small margin of error). The purpose for this synchronization is to correlate events and logs on both devices. The recommendation is to turn synchronization on. If installing several XIOs for connection to an ABB remote controller, synchronizing each XIO to the controller means there is no need to individually synchronize each XIO to the laptop at first time connection.

Figure 4-13: Basic XIO configuration (unique XIO Station ID required)



4.6 Configure network communication (4-port switch mode)

The XIO network communication configuration depends on field scenarios. The XIO Ethernet ports support several options. Network configuration provides TCP/IP based communication for:

- Remote management and access to the device from the corporate network: The XIO configured with a valid IP address is available for remote monitoring connections and data collection.
- Measurement data transmission in the field: The XIO configured with a valid IP address is discoverable and available for connection with Totalflow remote controllers polling for measurement data.

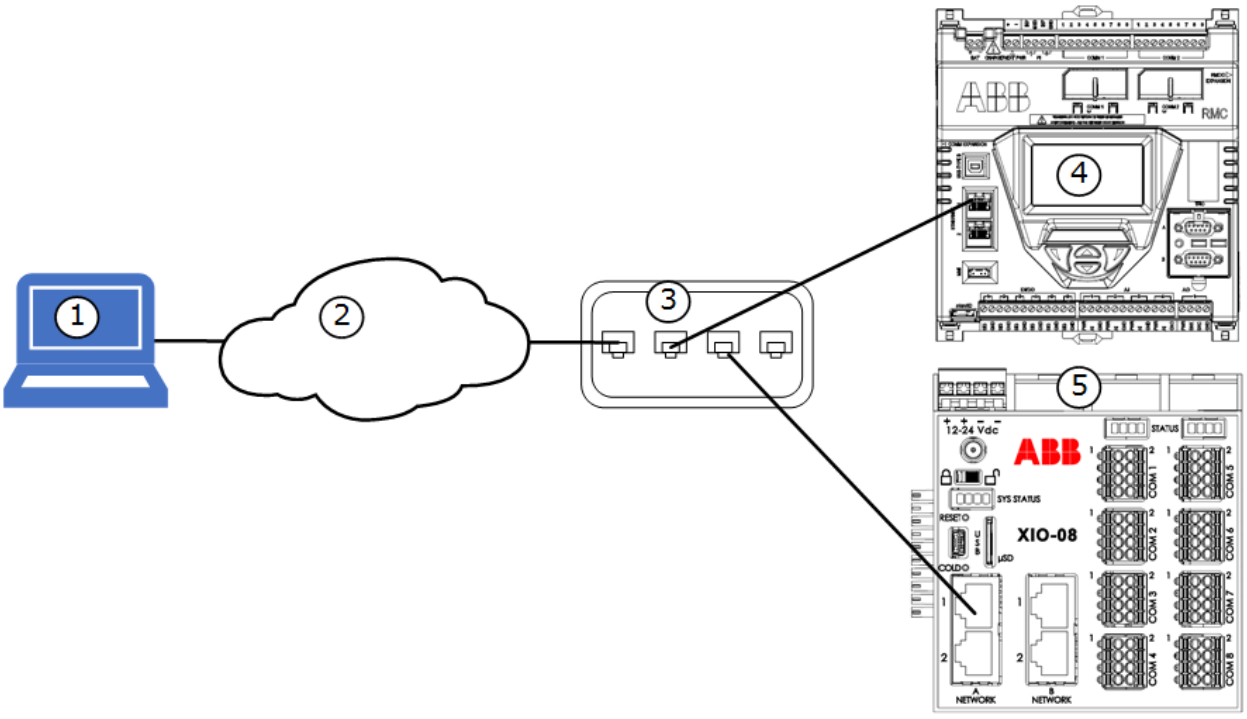
IMPORTANT NOTE: For additional details on network configuration, see section 9 Ethernet connectivity scenarios or the Network Communication Application Guide listed in Additional information.

4.6.1 Sample connections

The following figures show high-level examples of XIO network connections. In these scenarios, the RMC is the remote controller installed at the site. The XIO may be in the same cabinet as the RMC or standalone in another cabinet at a distance from the RMC. Ethernet connection options depend on the available network equipment, distance between devices, and number of devices.

In Figure 4-14, both the XIO and RMC connect to their own ports on a network switch. Each can be accessed remotely for management. Measurement data traffic flows between the RMC and the XIO.

Figure 4-14: Ethernet connection – XIO / RMC (star topology)



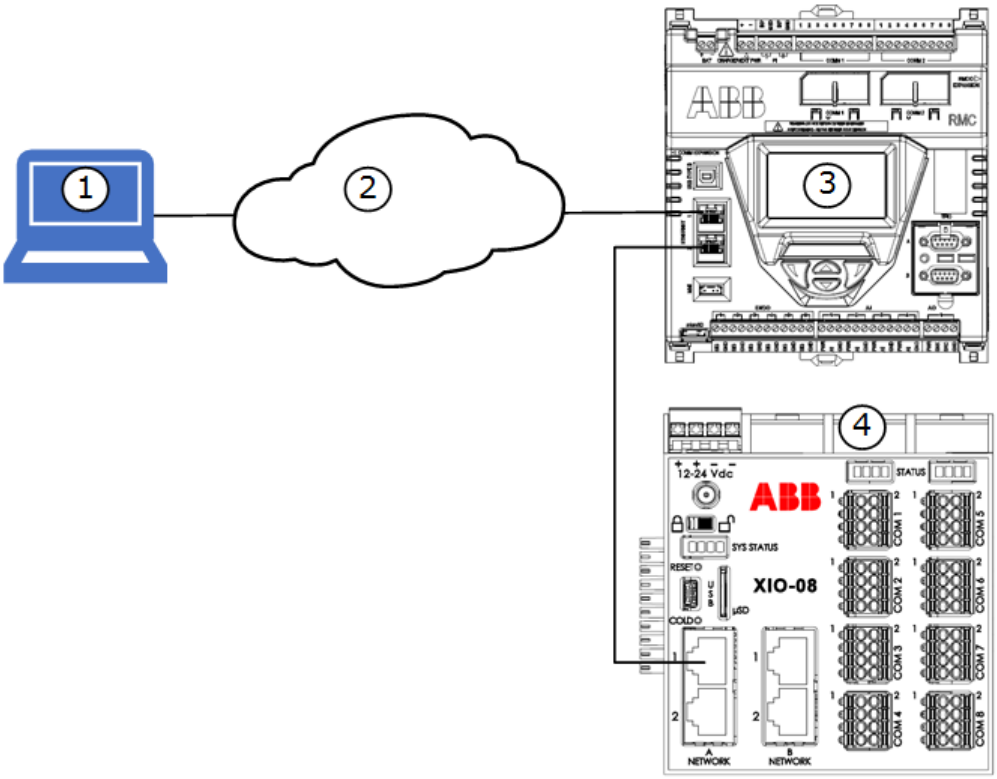
Legend: Ethernet connection (Star topology)

ID	Name	ID	Name	ID	Name
1	Host System with PCCU	3	Ethernet switch or hub	5	XIO
2	TCP/IP network	4	RMC		

In Figure 4-15, the XIO connects directly to the RMC. Access to the XIO for remote management is through the RMC which performs the role of a switch.

IMPORTANT NOTE: The RMC must be configured as a 2-port switch to support this connection scenario (Ethernet port 1 and 2 are configured in 1-Network mode). When the RMC is configured for 2-Network mode (E1 and E2 are configured as separate networks), it is not possible to manage the XIO from the same network as the RMC. For additional information on different scenarios, see section 9 Ethernet connectivity scenarios.

Figure 4-15: Ethernet connection – XIO / RMC (daisy chain topology)



Legend: Ethernet connection (daisy chain topology)

ID	Name	ID	Name
1	Host System with PCCU	3	RMC (Ethernet ports configured in 1-Network Mode)
2	TCP/IP network	4	XIO

4.6.2 Configuration overview

The configuration procedures assume the following:

- The XIO has its factory default configuration. This configuration combines all Ethernet ports into a single 4-port switch configuration.
- A single valid IP address will be assigned to the XIO. This IP address is unique in the field network and replaces the factory default.
- The Totalflow remote controller is the RMC-100 which is configured as a 2-port switch and already has a unique and valid IP address compatible with that of the XIO (same subnet).

IMPORTANT NOTE: TCP/IP based communication can take place between a Totalflow controller and an XIO when both have their factory default IP addresses intact. However, it is best practice to use unique IP addresses even if only one XIO is installed.

All XIOs have the same factory IP address. Installations with multiple XIOs must replace the default IP address with a unique address for each device.

To configure the XIO for network communication, follow the applicable procedures:

- If the XIO connects to a third-party controller, follow steps in section 4.6.3 Configure the XIO and then, 4.8 Configure Ethernet-Serial Passthrough. The configuration of a third-party controller is beyond the scope of this manual. Consult the vendor documentation.
- If the XIO connects to a Totalflow controller, such as the RMC-100, follow steps in section 4.8.1 Configure the XIO first, and then complete steps in section 4.8.2 Configure the RMC.

4.6.3 Configure the XIO

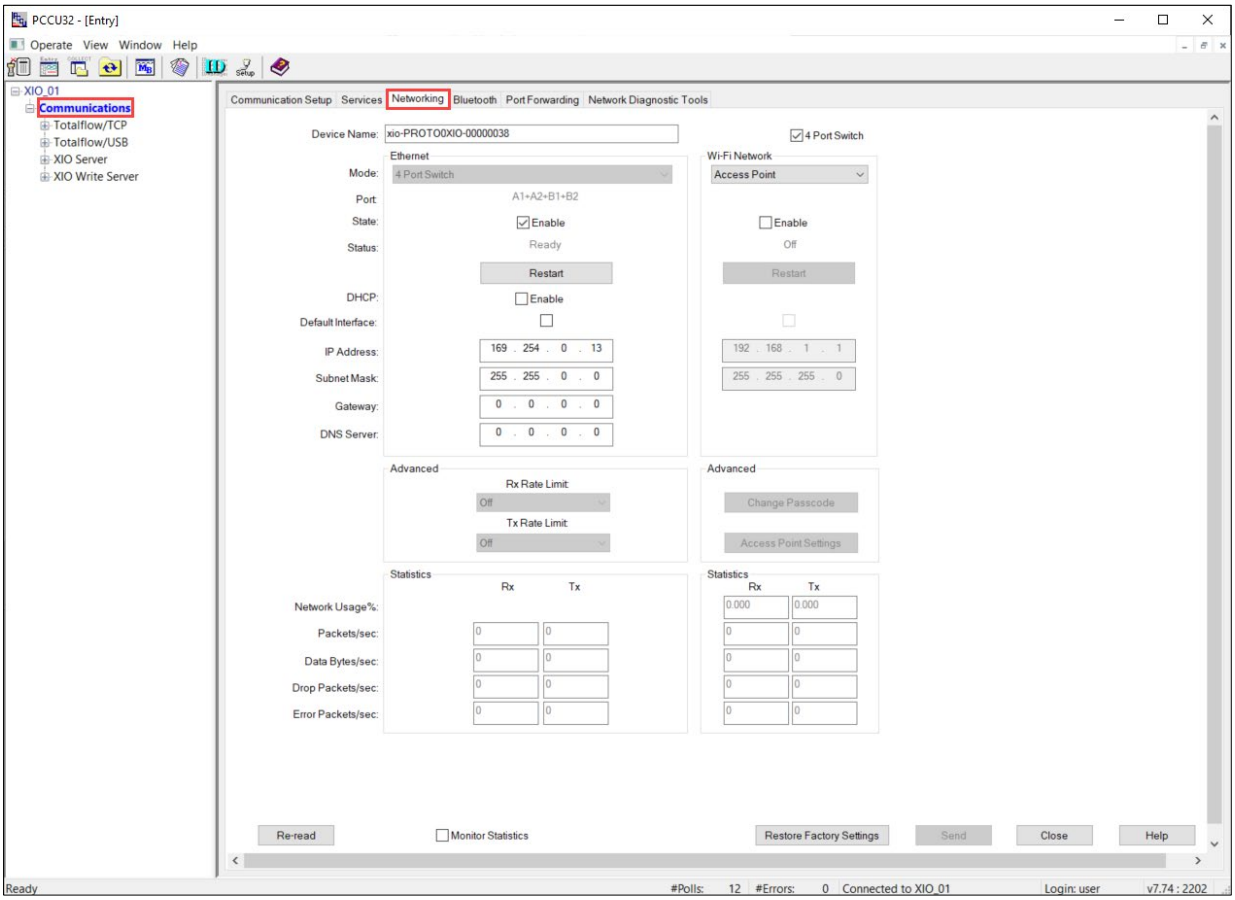
Configure the XIO with valid IP parameters. The XIO supports static (manual) or dynamic (DHCP) IP addressing on both A and B network ports. If possible, it is preferable to configure the XIO with static IP addresses. These addresses remain in the configuration and do not depend on a connection to a DHCP server. Loss of the IP address causes loss of existing connections on the Ethernet ports.

IMPORTANT NOTE: A change to the state of Ethernet (enable or disable) or any other parameter will restart that Ethernet interface. This will cause existing connections on that IP address to be lost.

To configure the XIO:

1. On the navigation tree, click **Communications**. The Communications Setup tab displays.
2. Select the **Networking** tab. The Networking screen displays the XIO default networking configuration as a 4-port switch.

Figure 4-16: XIO default network configuration (4-port switch)



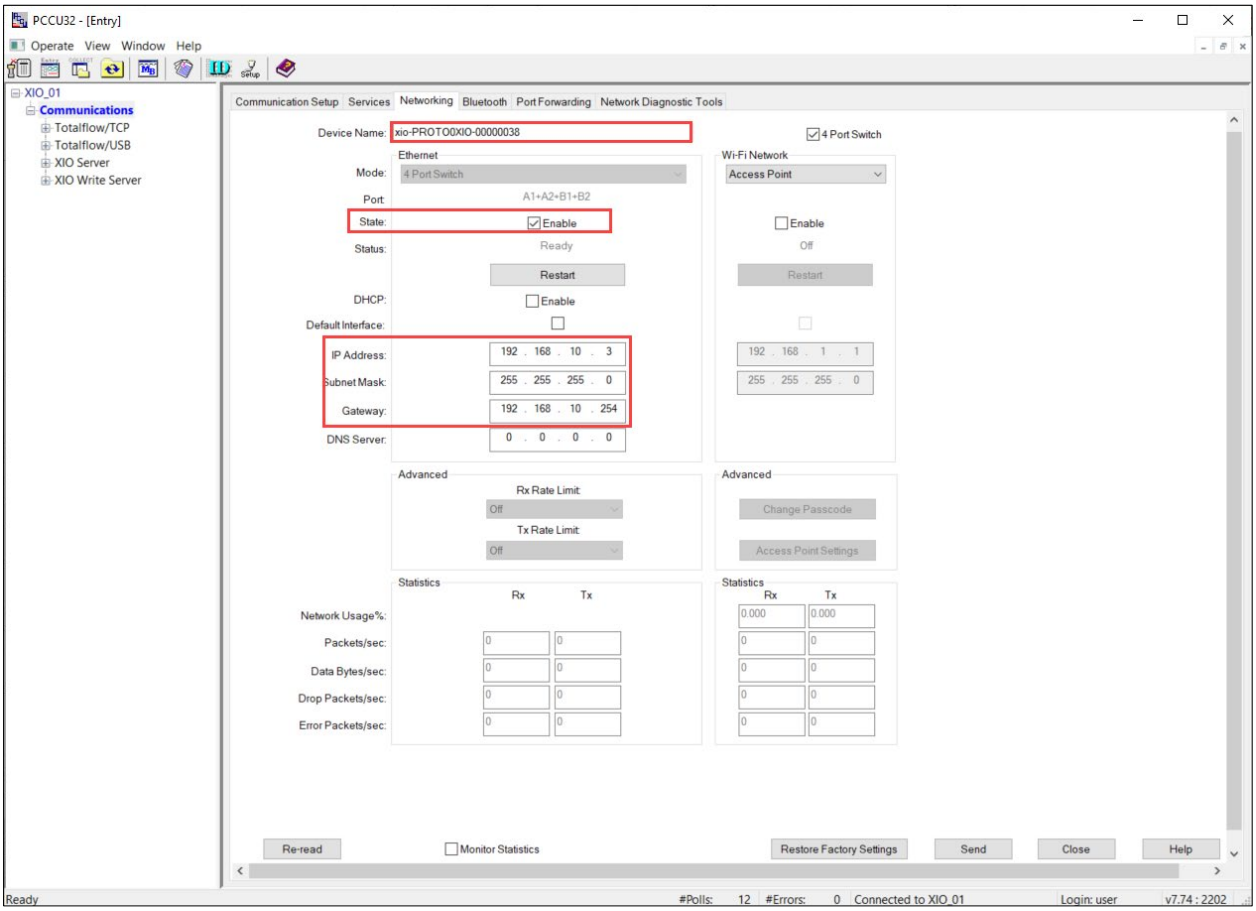
3. Configure the following (Figure 4-17):
   a. In the Device Name field, accept the factory default name or type a different name. If using a non-default name, make sure that the name is unique.

IMPORTANT NOTE: The factory default device name is a unique name specific to each XIO. While the name is user-configurable, it is recommended to leave the default to ensure that the name is always unique. The device name is the same as the Network ID (displayed in the Services tab). When the XIO wireless interface is enabled (for example, in the role of a Wi-Fi access point), it broadcasts this name. Wireless clients detect this name as the network available for connection. If the name is not unique and there are multiple XIOs in the field, wireless clients have no way to determine if they are connecting to the desired XIO. Changing the device name from the Networking tab automatically updates the Network ID in the Services tab.

   b. Select the **State** checkbox to enable the Ethernet ports.
   c. Configure IP parameters:
      i. Select **Enable** DHCP for automatic addressing if there is DHCP Service available in the network, or

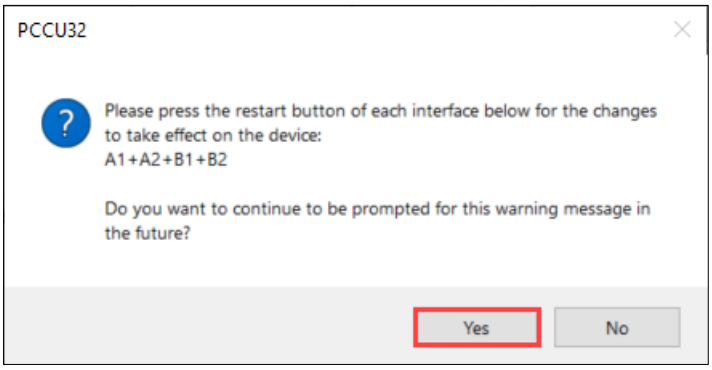
      ii. Type each of the parameters for static addressing into IP Address, Default Gateway, and Subnet Mask. (This is recommended, since static addresses remain even if connection to the corporate network or local router is lost).

Figure 4-17: Enable XIO for network communication with valid IP address



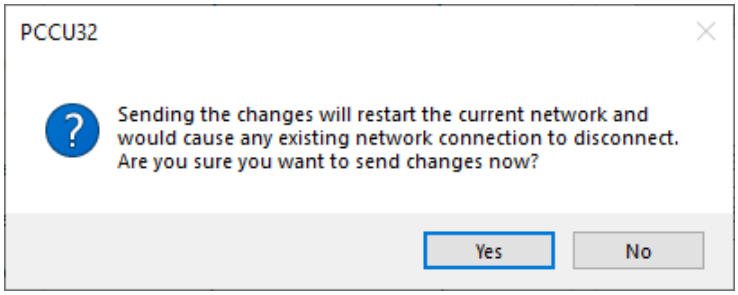
4. Click **Send**.
5. Click **Yes** (recommended) if you need the reminder to restart interfaces to display every time configuration is changed. If you don't need a reminder click **No**.

Figure 4-18: Restart reminder



6. Click **Restart**. A message to confirm the restart displays.

Figure 4-19: Restart message



7. Click **Yes**. If you have enabled DHCP, wait for the device to obtain its IP configuration. The IP configuration fields automatically populate when the device receives the IP configuration values from the DHCP. Check the local router providing DHCP services if these fields do not populate. Unless the device has the correct IP configuration, it cannot communicate on Ethernet.

IMPORTANT NOTE: Any existing TCP/IP connection is lost when the XIO IP address changes and the network interface restarts. If you are using one of the Ethernet ports to connect locally, reconfigure the laptop or PC with an IP address compatible with the new XIO IP address to reestablish connection.

8. Connect any of the XIO Ethernet ports to the controller's Ethernet port or field network switch.
9. Ping the XIO from network to verify that it has the proper configuration. The XIO replies to the ping when IP parameters are correct.
10. Remain connected to the XIO.
11. If the XIO communicates with a Totalflow remote controller, proceed to section 4.6.4.
12. If the XIO communicates with a third-party controller, proceed to section 4.8 Configure Ethernet-Serial Passthrough.

4.6.4 Configure the RMC

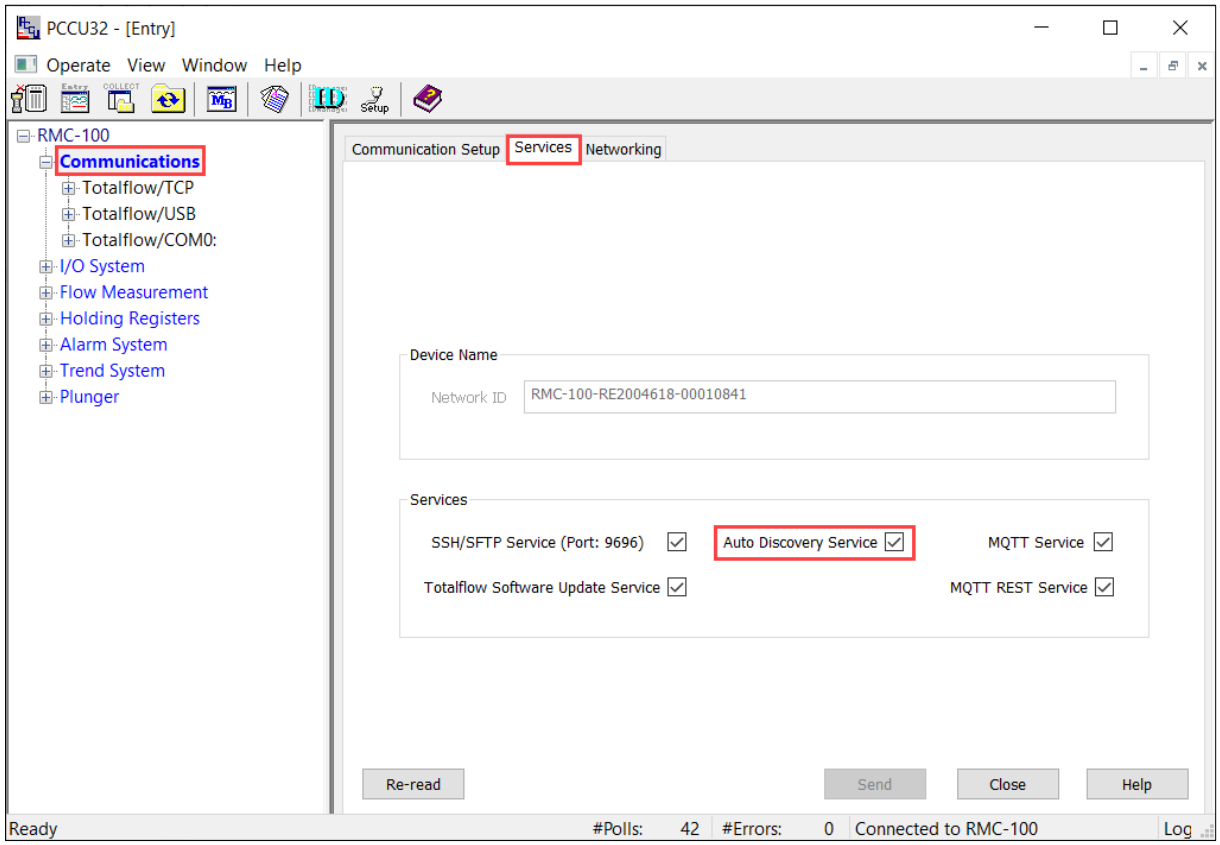
This procedure describes how to configure the RMC to establish communication with the XIO. The RMC supports automatic discovery of XIOs on the field network when they are configured with valid and compatible addresses. It is assumed that the RMC has already been configured with a valid IP address and that the Auto Discovery Service is enabled (factory default).

The XIO interface on the RMC is the application that handles the detection and communication with the XIO.

To configure the RMC:

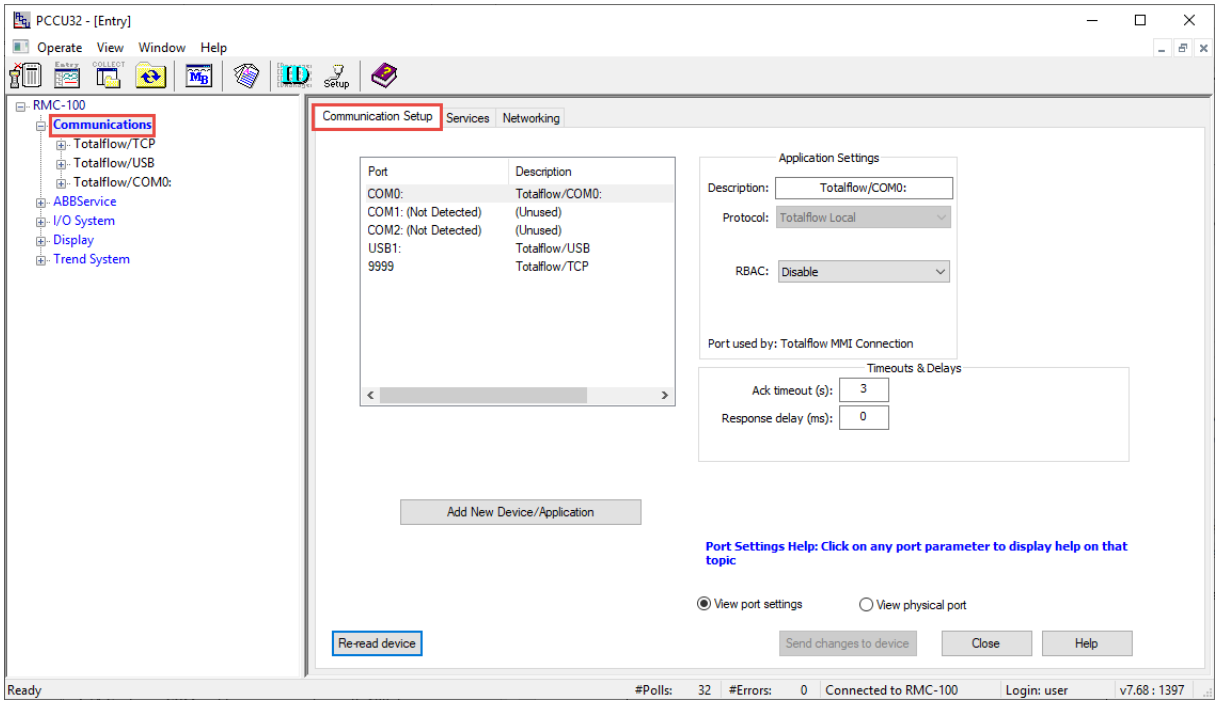
1. Launch another instance of PCCU to connect to the RMC.
2. Click **Entry**.
3. On the navigation tree, select **Communications**, then select the **Services** tab.
4. Verify that **Auto Discovery Service** is enabled.

Figure 4-20: Auto Discovery service enabled in the RMC



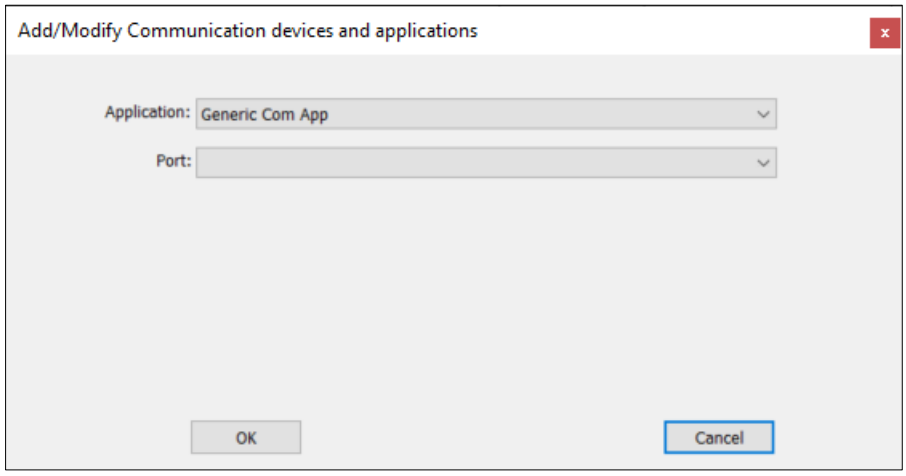
5. Select the Communications Setup tab.

Figure 4-21: Communication Setup (default screen)



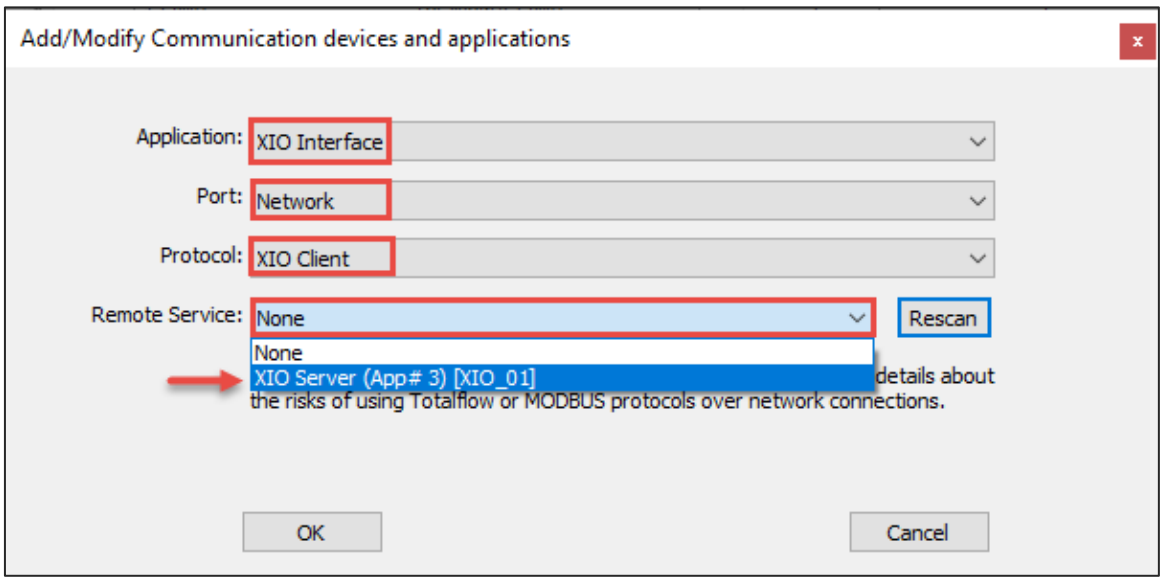
6. Click **Add New Device/Application**. The Add/Modify Communications devices and applications window displays.

Figure 4-22: Add/Modify Communications devices and application



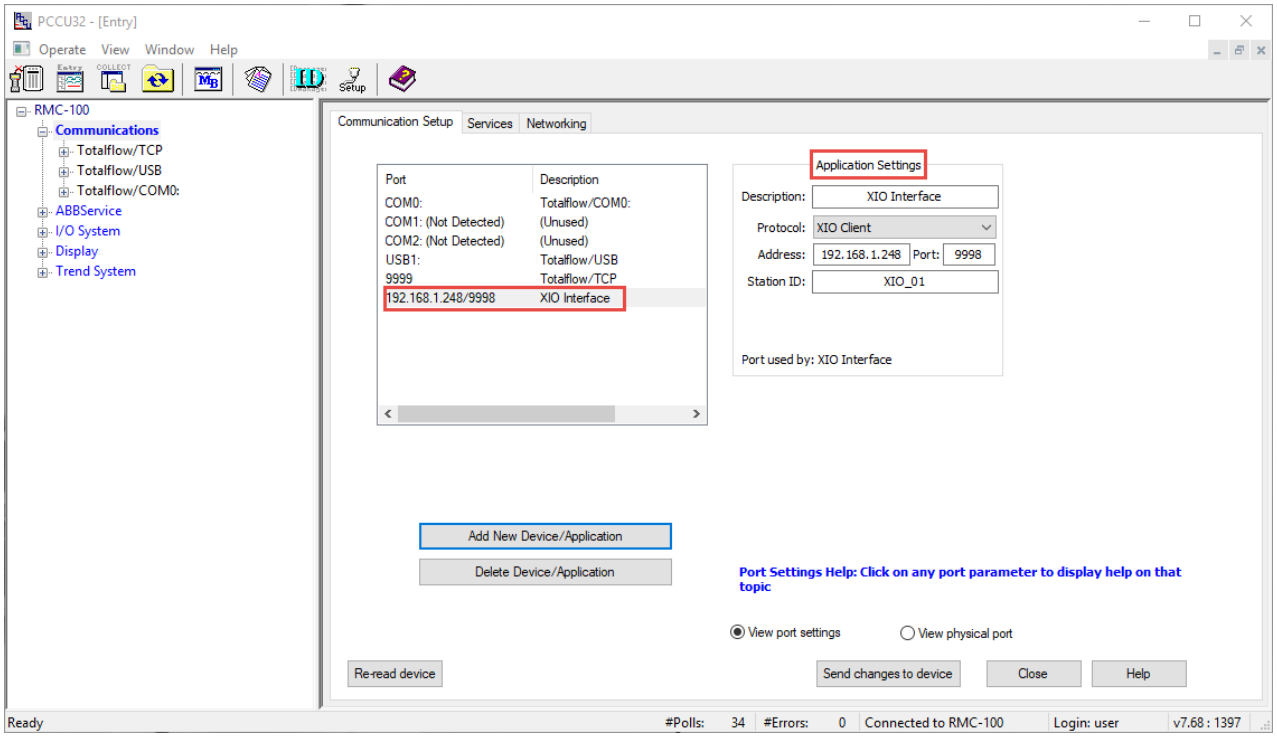
7. Configure the following (see Figure 4-23):
   a. Select **XIO Interface** from the Application drop-down list.
   b. Select **Network** from the Port drop-down list.
   c. Leave the **XIO Client** (default) on the Protocol drop-down list.
   d. Click the **Remote Service** drop-down list. The list of detected XIOs in the field network displays: The XIO Server application displays with each associated XIO ID. In the example, a single XIO is identified as XIO Server [XIO_01]. Identify the correct XIO when multiple XIOs display. The App# assigned to the XIO Server application on the XIO also displays. It helps identify the specific instance when the application names are the same. In the example shown the App# is 3 which is the slot number the XIO Server is instantiated at.
   e. Locate and select the XIO on the list. The selected XIO displays in the Remote Service field.

Figure 4-23: Add XIO Interface for detected XIO (shown in Remote Service field)



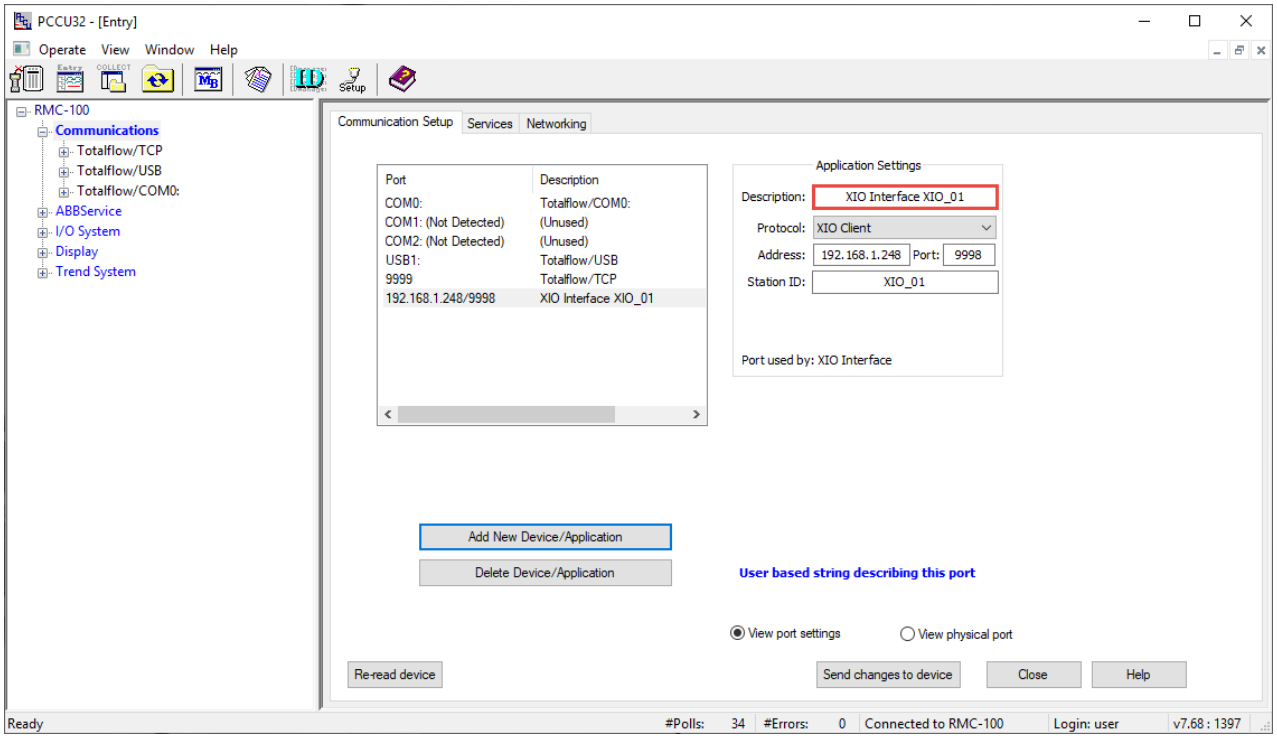
8. Click **OK**. The communication port and application (XIO Interface) for communication with the XIO displays in the port list. Note that while the network port was selected in the previous configuration dialog box, the list does not display the network port, but an IP/TCP number combination (in the example, 192.168.1.248/9998). The IP address is that of the detected XIO, and the TCP port is the logical port that the XIO reserves to grant connection requests from the RMC XIO Interface client. The default XIO TCP port is 9998.

Figure 4-24: Default XIO Interface configuration



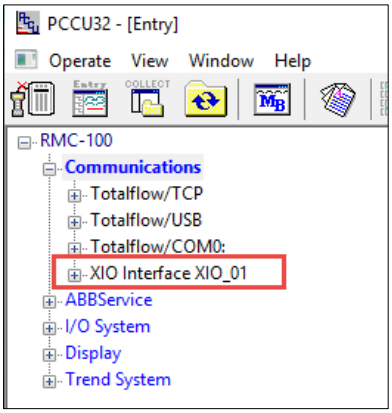
9. Verify the values of the additional configuration fields. The Application Settings section displays the generic description of the XIO Interface, default protocol, detected TCP parameters and XIO Station ID. These values are automatically populated when the XIO Interface was added.
10. For a multiple XIO installation, change the description field to a name that helps identify the XIO. A unique description that includes the XIO Station ID is easier to locate on the navigation tree than the generic default description (XIO Interface or XIO Interface-n).

Figure 4-25: XIO Interface application on network port



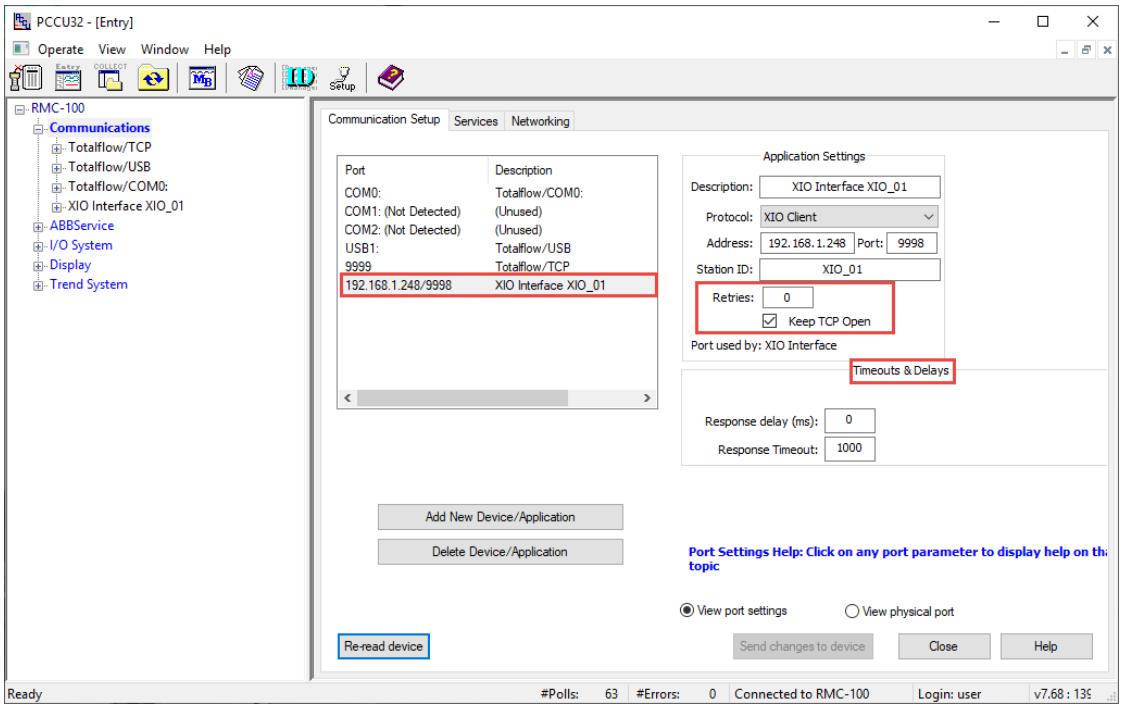
11. Click **Send changes to device**. The XIO Interface application displays in the navigation tree.

Figure 4-26: XIO Interface on the RMC navigation tree



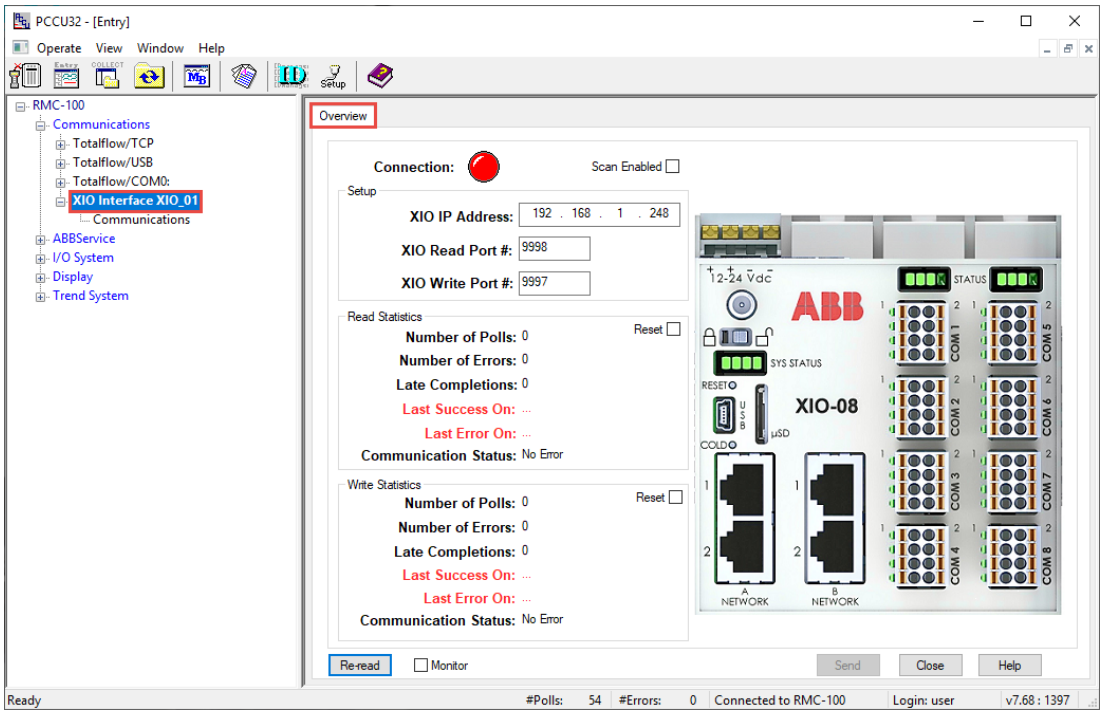
12. If unable to see the XIO interface on the navigation tree, refresh the navigation tree or click Close. View or reconnect to verify the navigation tree displays the XIO Interface application.
13. On the communication setup tab, select the XIO Interface port from the list. Notice that the Application Settings section displays additional configuration parameters. The Timeouts & Delays section also displays. These parameters are user-configurable, but default values can be used.
14. Change the default configuration of these parameters if necessary. Additional parameters are available on the XIO interface screens.

Figure 4-27: XIO Interface application on network port – additional settings



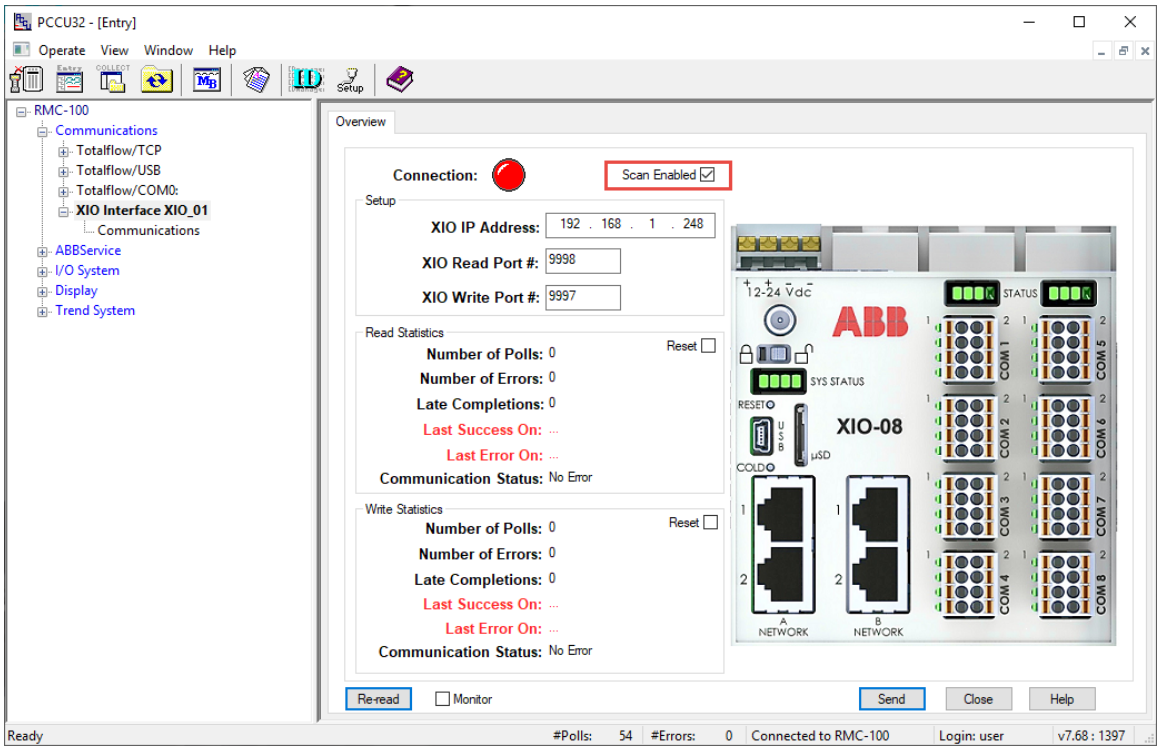
15. If you prefer to configure communication parameters on the XIO Interface instance screens, select the **XIO Interface** instance on the navigation tree. (If you have configured a different instance name in the communication setup TCP/IP description field, select that name on the tree.) The Overview tab displays (Figure 4-28) and provides quick visual connection status between the RMC and the XIO. At first installation, the connection status is red because the RMC is not yet enabled to begin communicating with the XIO.

Figure 4-28: XIO Interface Overview screen



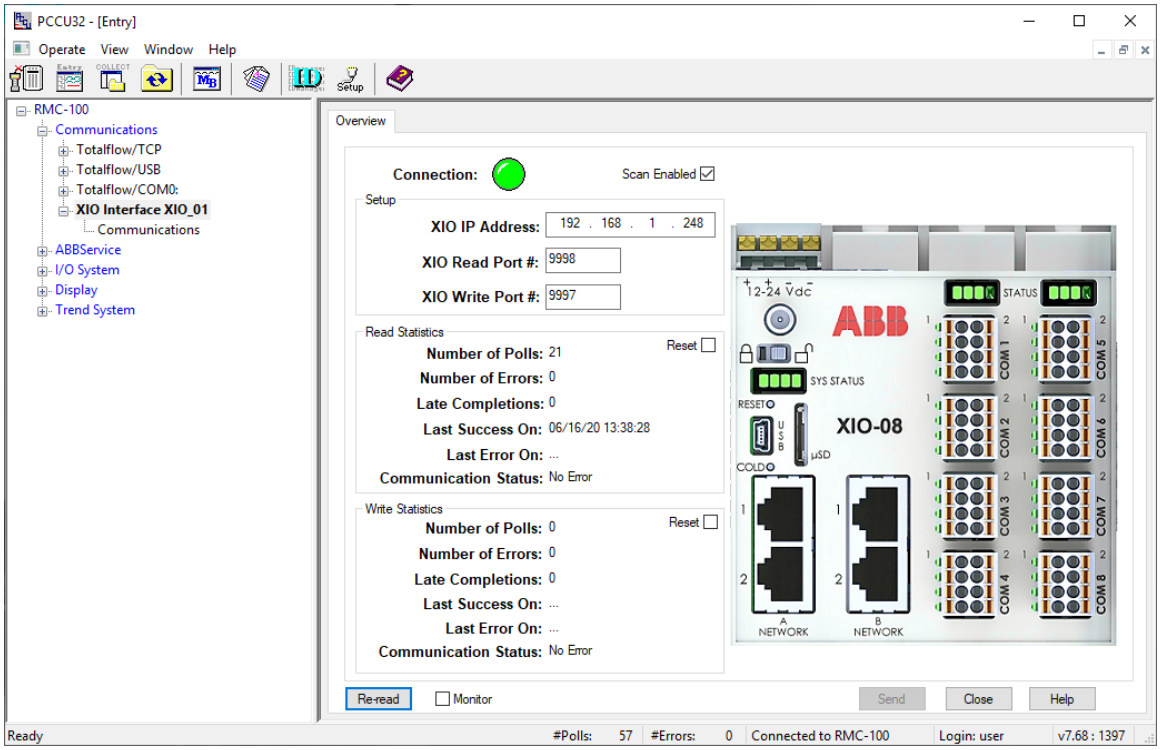
16. Select Scan Enabled.

Figure 4-29: Enable the XIO Interface scan function



17. Select **Send**.
18. Select **Re-read** to refresh the screen.
19. Verify the status of the RMC-XIO connection:
    a. The connection is successful if the Connection indicator is green. The Communication Status under the Read Statistics section should display: No Error.
    b. The connection failed if the Connection indicator is red. The Communication Status under the Read Statistics section displays: Connection Timeout. Additional information on screen parameters is available in the PCCU help topics. Click **Help** to display topic for the screen.

Figure 4-30: Successful RMC-XIO connection



20. Repeat steps 5 through 19 for additional XIOs.

4.7 Configure serial communication applications (COM ports on XIO-04 and XIO-08)

This section describes how to configure the XIO and its communication applications to add serial port capacity to the RMC. Communication applications assigned to COM ports are instantiated in the XIO but are managed (visible) from the RMC.

RMC-XIO communication takes place through the XIO Interface (client) – XIO Server connection. This connection must be successfully established and stable as described in section 4.6.4 Configure the RMC. The RMC retrieves measurement data captured on the XIO COM ports and feeds it to its local measurement applications.

IMPORTANT NOTE: A single XIO Interface instance on the RMC can manage communication with all COM ports on an XIO. Additional XIO Interface instances are required for additional XIOs. Use a naming convention for the XIO interface instances which allows easy identification of the associated XIO.

Configure COM 1 - COM 8 communication ports to connect one or more peripheral serial devices. These ports are software-configurable to support RS-232, RS-422, and RS-485.

Configure the ports with the application that supports the type of peripheral. For ABB Totalflow peripherals, use special-purpose communication applications such as the XMV Interface.

IMPORTANT NOTE: The Totalflow Generic Com App supports third-party peripherals. It is recommended to configure the COM port for Ethernet-Serial Passthrough when connecting to third-party peripherals. Refer to section 4.8 Configure Ethernet-Serial Passthrough.

The procedures in these sections assume that the COM ports are already wired for the type of peripheral attached.

IMPORTANT NOTE: During these procedures, pay close attention to the four LED lights on the left side of the COM Ports. The LEDs are indicators for PWR (VBatt, Switched VBatt), TXD, and RXD. Blinking TXD and RXD LEDs indicate that the XIO is transmitting and receiving traffic. The PWR LEDs turn on only if the respective COM port is assigned to an application. They remain off when the port is unused (unassigned to any application).

4.7.1 Configure COM port for communication with ABB devices

This procedure describes the configuration of an XIO COM port for connection with an ABB peripheral. The example in this procedure connects an ABB multivariable transmitter to XIO COM1. The XMV Interface is the application that handles communication with the multivariable. It is added and assigned to COM1. There are two ways to add the application and assign it to the required COM port:

- Add the application from the Application/License Management tab, then assign and configure the COM port from the XMV Interface Communications Setup tab or,
- Add and assign the COM port from the Communication Setup tab (Recommended). The Communication Setup tab handles automatic configuration of optimal parameter for the application/device type. You can configure all required parameters for successful first-time communication from the same screen.

IMPORTANT NOTE: Use a naming convention for the communication application instances which allows for easy identification of the assigned XIO COM port.

Adapt the procedures for other types of devices and communication applications. Click **Help** on the application screens for detailed configuration parameter information.

The procedure in these sections assume that the peripherals are correctly wired to the COM ports.

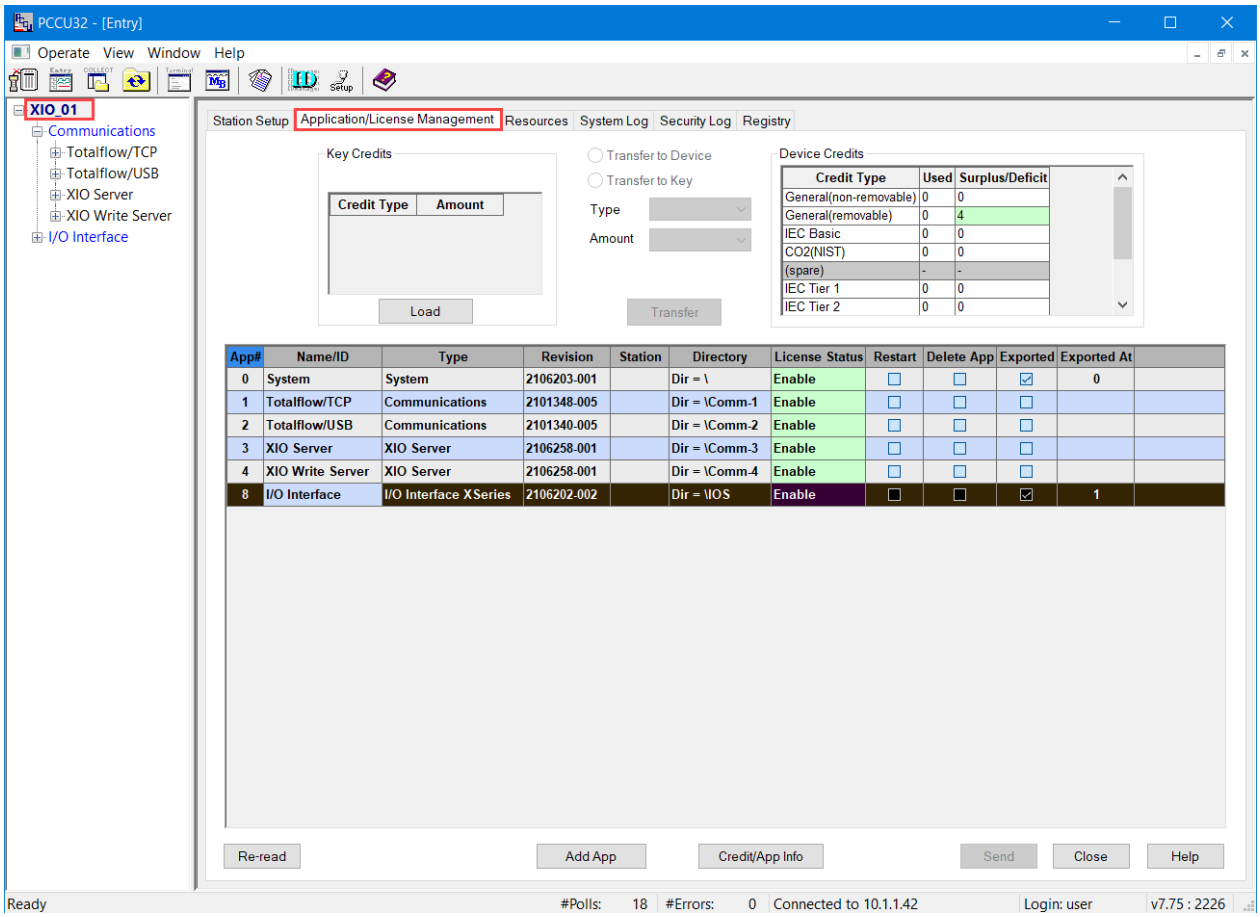
4.7.1.1 Assign and configure the port from the XMV Interface

This procedure adds the XMV interface from the Application/License Management tab first, and then assigns and configures the port from the XMV Interface Communications Setup tab.

To configure COM port with XMV Interface:

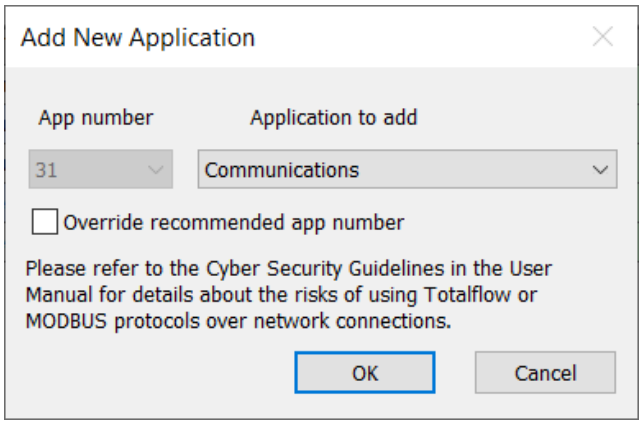
1. Verify that the status LEDs on the corresponding COM port column displays solid green on first 3 LEDs. The 4th LED should not be lit.
2. On the navigation tree, select the Station ID (XIO ID). The Station Setup tab displays.
3. Select the **Application/License Management** tab. The list of applications displays.

Figure 4-31: XIO Application/License Management tab



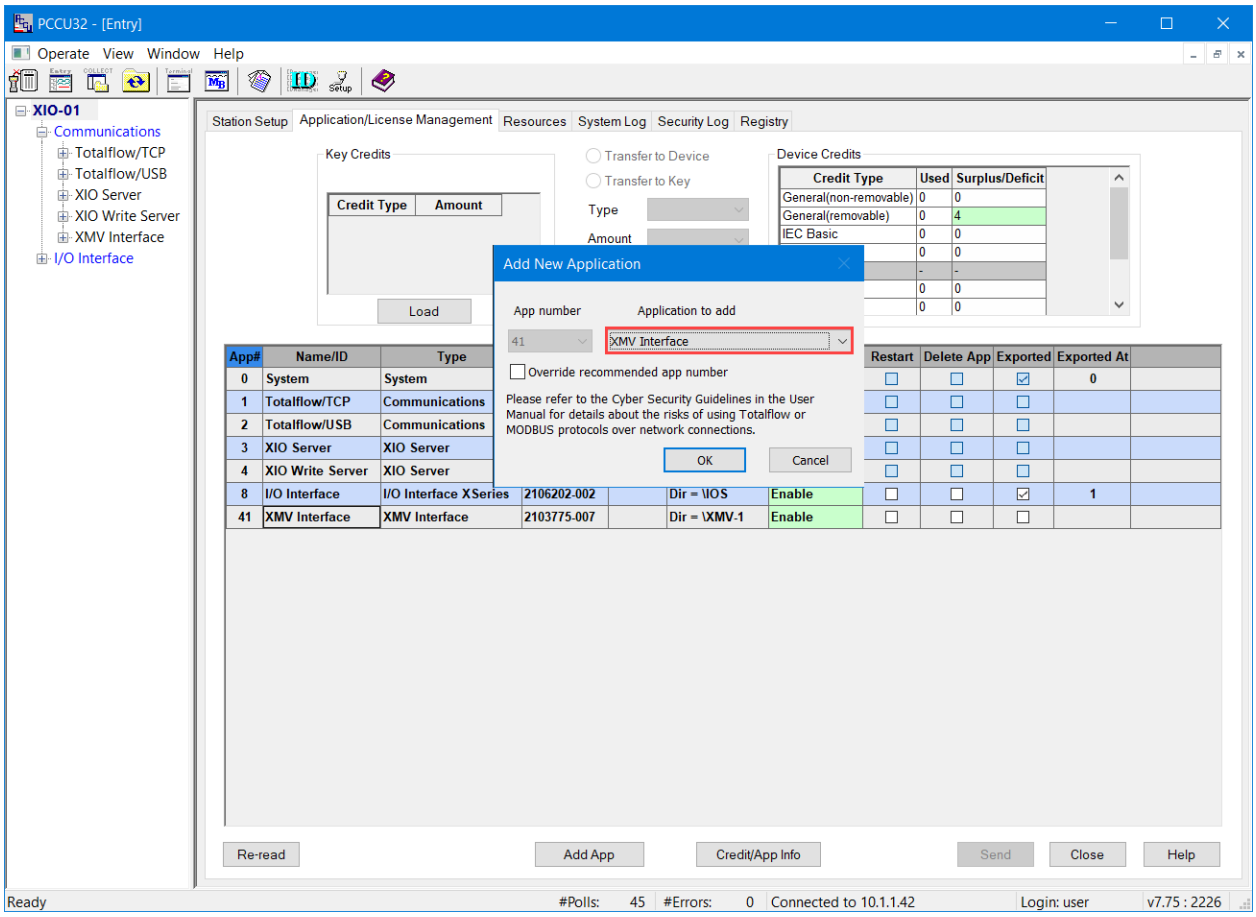
4. Click **Add App**. The Add New Application window displays.

Figure 4-32: Add New Application



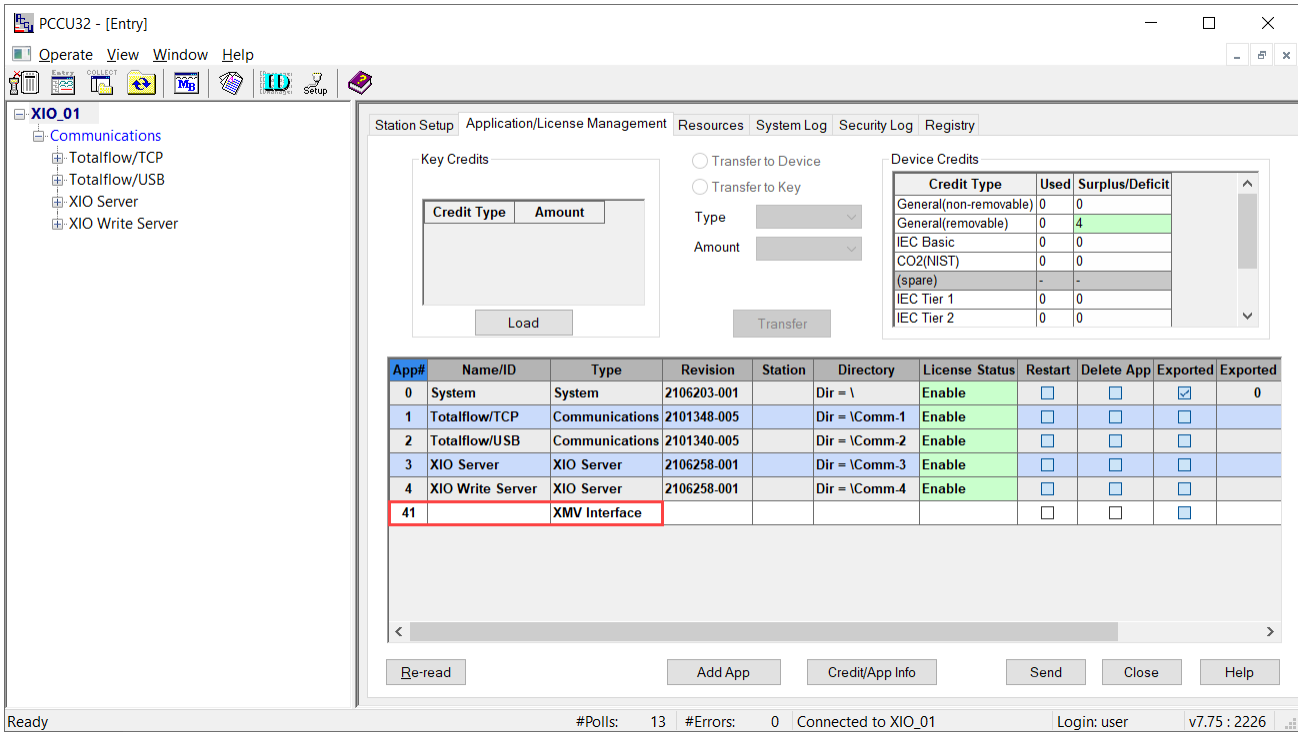
5. Select **XMV Interface** from the **Application to add** drop-down list.

Figure 4-33: XMV Interface selected from the application list



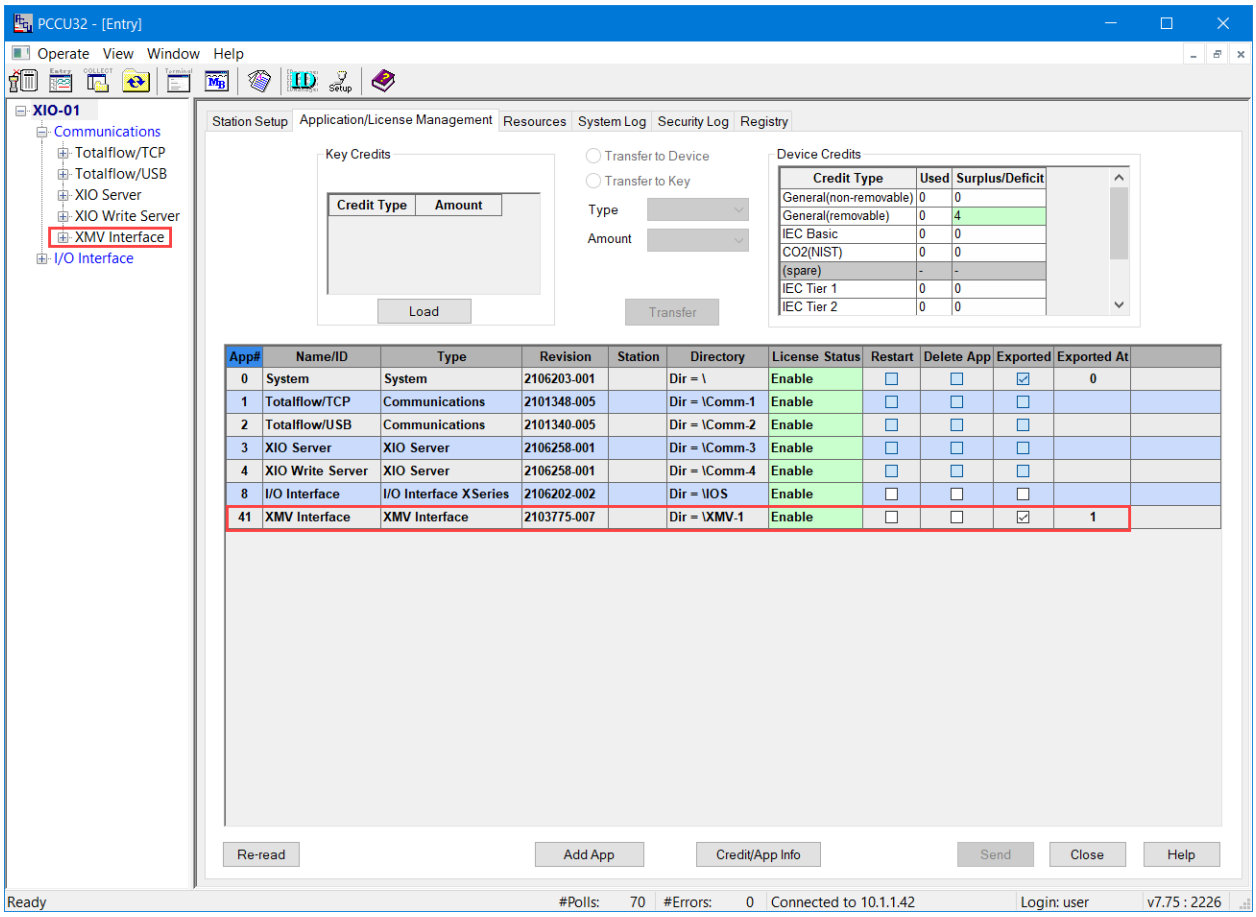
6. Click **OK**. The XMV Interface displays in the application table with the default application slot number (41, in this example).

Figure 4-34: XMV Interface instance on default application slot number



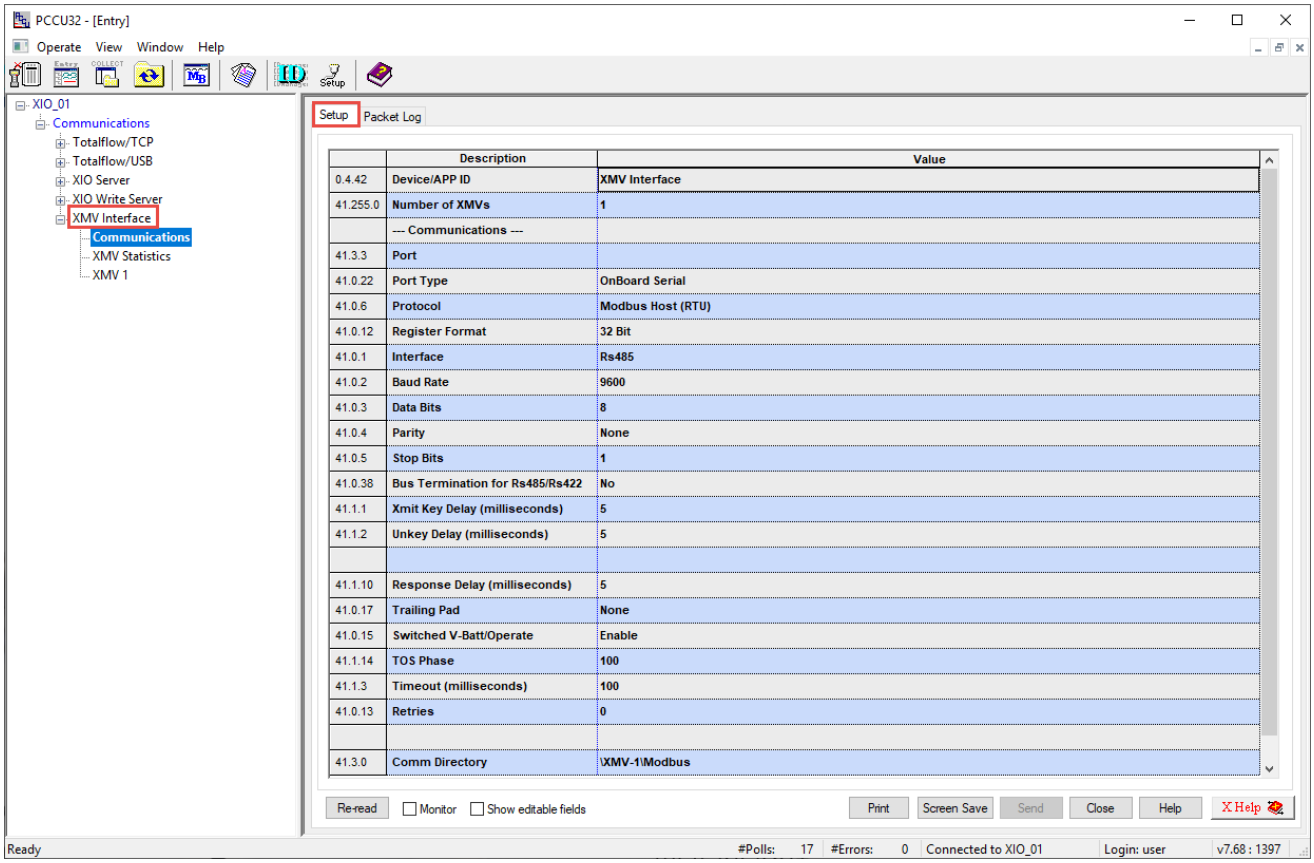
7. Click **Send**. The XMV Interface application displays in the application table and on the navigation tree. If the navigation does not refresh to show the application, click **Close** to disconnect, and then **Entry** to re-connect. The navigation should display the application when it refreshes after reconnecting.

Figure 4-35: XMV Interface on the XIO navigation tree



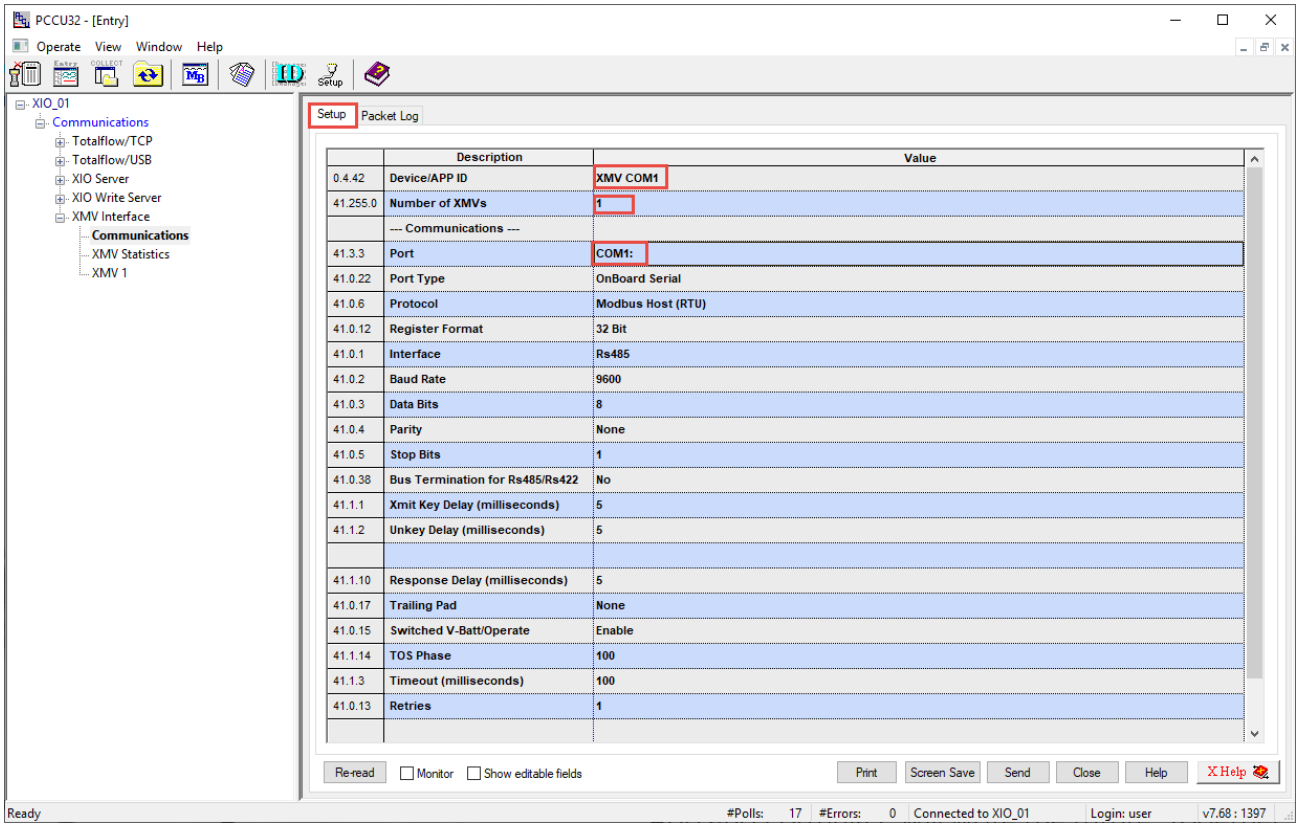
8. On the navigation tree, expand **XMV Interface** and select **Communications**. The Setup tab displays with the default port settings. The example used for the next steps shows the assignment of COM1 to an XMV Interface Instance.

Figure 4-36: XMV Interface communication setup (default screen)



9. Configure the port (Figure 4-37):
   a. Type a different description in the Device/APP ID value column. Use unique names that help identify the port when multiple ports are used.
   b. Configure the number of XMVs if greater than one.
   c. Type the port number in the Port value column. Add a colon after the number. For example, type **COM1:** for the XIO COM1 port.

Figure 4-37: XMV Interface Communication Setup – Description and port assignment

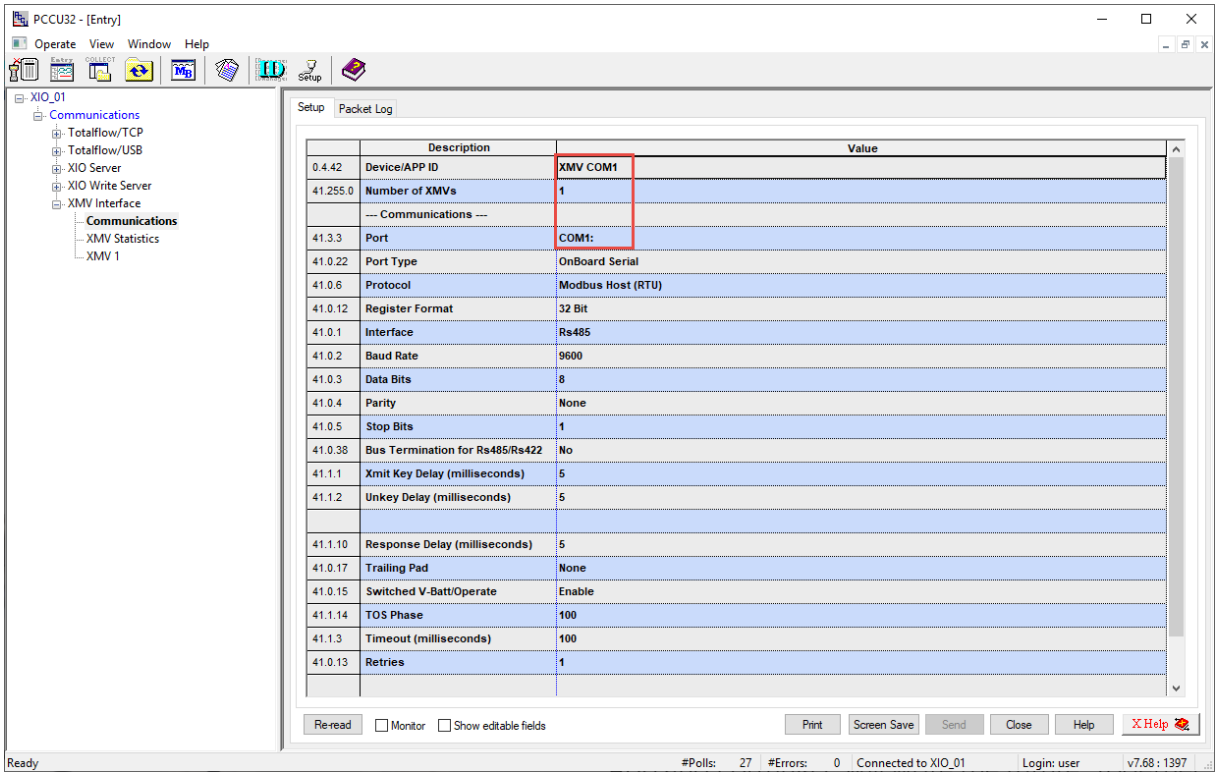


d. Configure the serial port settings to match the settings of the external device. When the XMV application is added from the Application/License Management tab, the default settings may not require change. Some of these default settings have been optimized to work with ABB peripherals with only minor modification at first-time connection.
e. Select the **Bus Termination** drop-down and then select **Yes** if the XIO is the last device on the RS-422 or RS-485 communication bus.
f. Configure Retries as necessary. Suggested value: 1.

10. Click **Send**. The port displays the new configuration. The following figure displays the configured port with typical values; but it may require some fine-tuning.

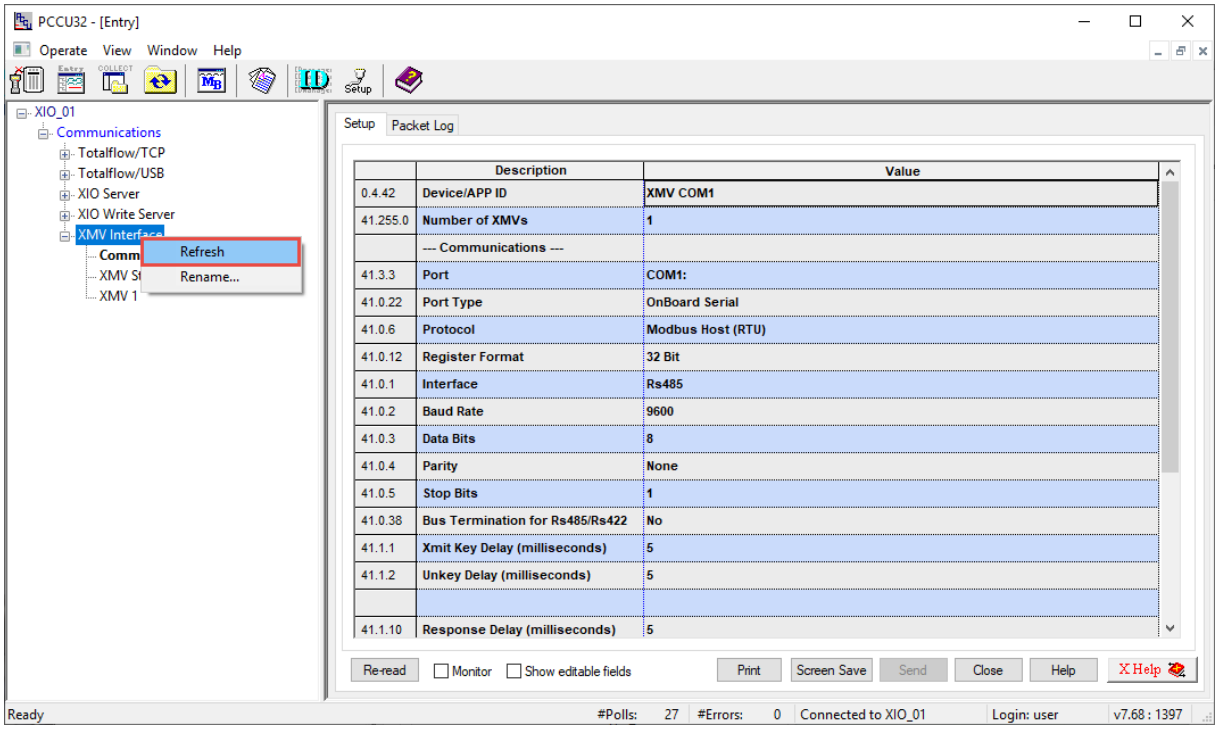
IMPORTANT NOTE: After clicking **Send** to save the communication setup, the configured COM port 1st and 2nd LEDs lit up to indicate that the application has been assigned to the port and is activated or turned on. The port supplies power from its power pins and is ready to communicate (receive and transmit).

Figure 4-38: XMV Interface Communication Setup for XIO COM1



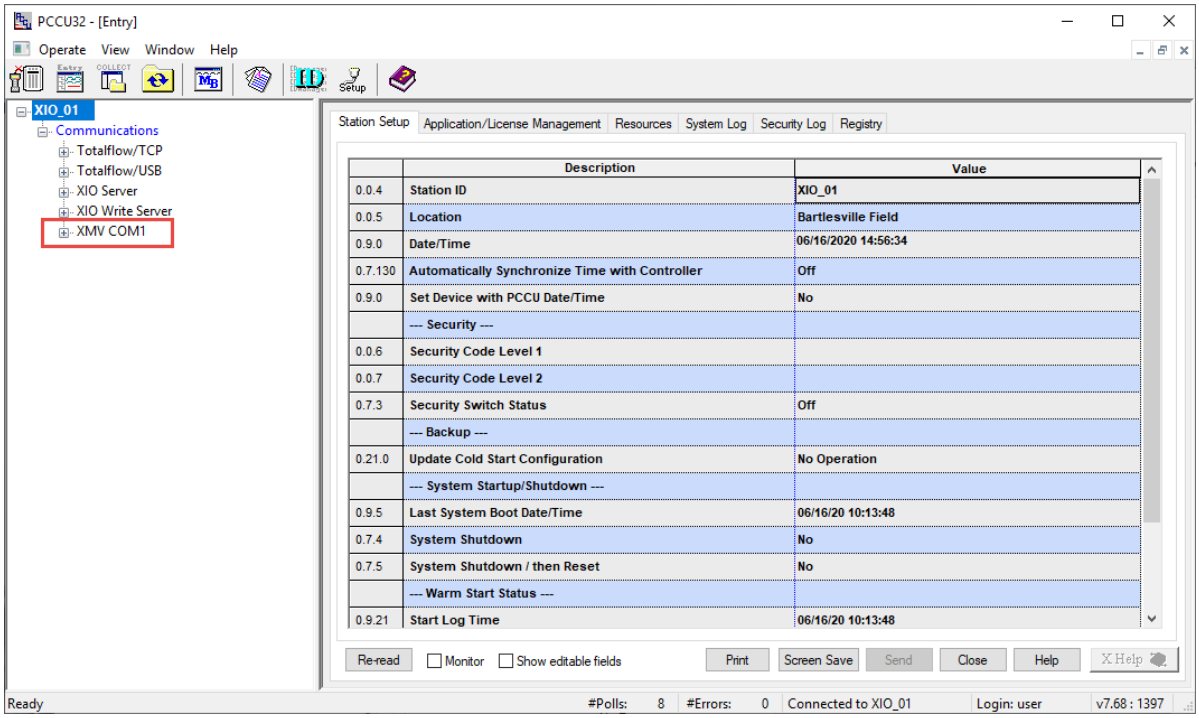
11. On the navigation tree, select the XMV Interface instance just configured, right click and select **Refresh**. The new name for the XMV Interface should display in the tree under **Communications**.

Figure 4-39: Refresh generic XMV Interface application to reflect associated port (XIO COM1)



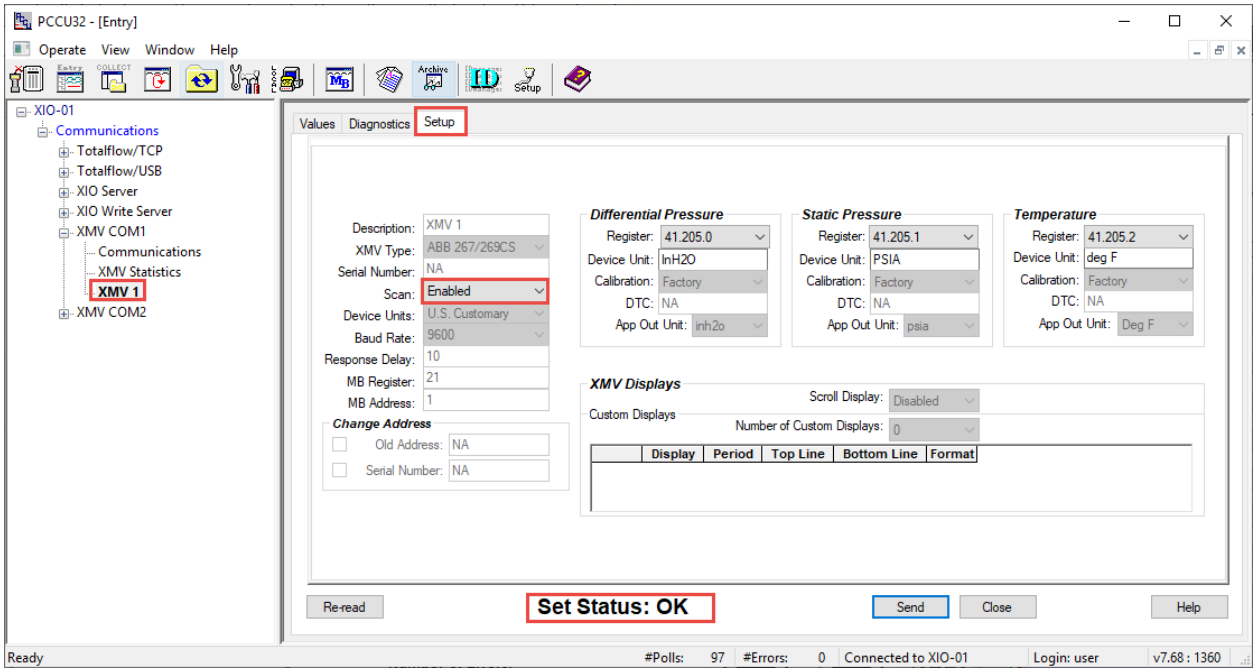
12. If the navigation tree does not refresh, click **Close** to exit connection, and then click **Entry.** The navigation tree refreshes reflecting the change. In this example, the default XMV Interface was renamed "XMV COM1" to reflect the XMV application and the port it is assigned to. Use a naming convention that meets your site requirements.

Figure 4-40: XMV Interface application associated with XIO COM1 (navigation tree)



13. On the XIO, verify that the PWR LEDs to the left of the port are on. These LEDs indicate that the port is active. These LEDs turn on only when the port is assigned to an application. They remain off when the port is unused.
14. Configure the XMV:
    a. On the navigation tree, expand the XMV Interface instance and then select **XMV1**.
    b. Select **Setup** tab.
    c. If the **Scroll Displays** field, in the XMV Displays section is enabled, change to **Disabled**.
    d. Click **Send**. This activates parameter fields for configuration.
    e. Configure the required parameters.
    f. Select **Enable** in the Scan drop-down list.
    g. Click **Send**.
    h. Verify that the Set Status displays **OK** at the bottom of the screen.

Figure 4-41: XMV Setup (Set Status OK)



15. Select the **Values** tab.
16. Verify the values for measured variables display and that the Scan Status displays **OK**.
17. On the navigation tree, select the XMV interface instance for the port. The multivariable displays with current values for the measured variables. The number of polls and the number of errors display.
18. Verify that values display and that the error count does not increase. There may be some errors due to an initial lack of communication, but errors should not increase once communication is successfully established. Click **Re-read** or select **Monitor** to verify communication with the peripheral is taking place.
19. When the XIO-peripheral communication is successful, proceed to section 4.7.2 Configure XIO application export.

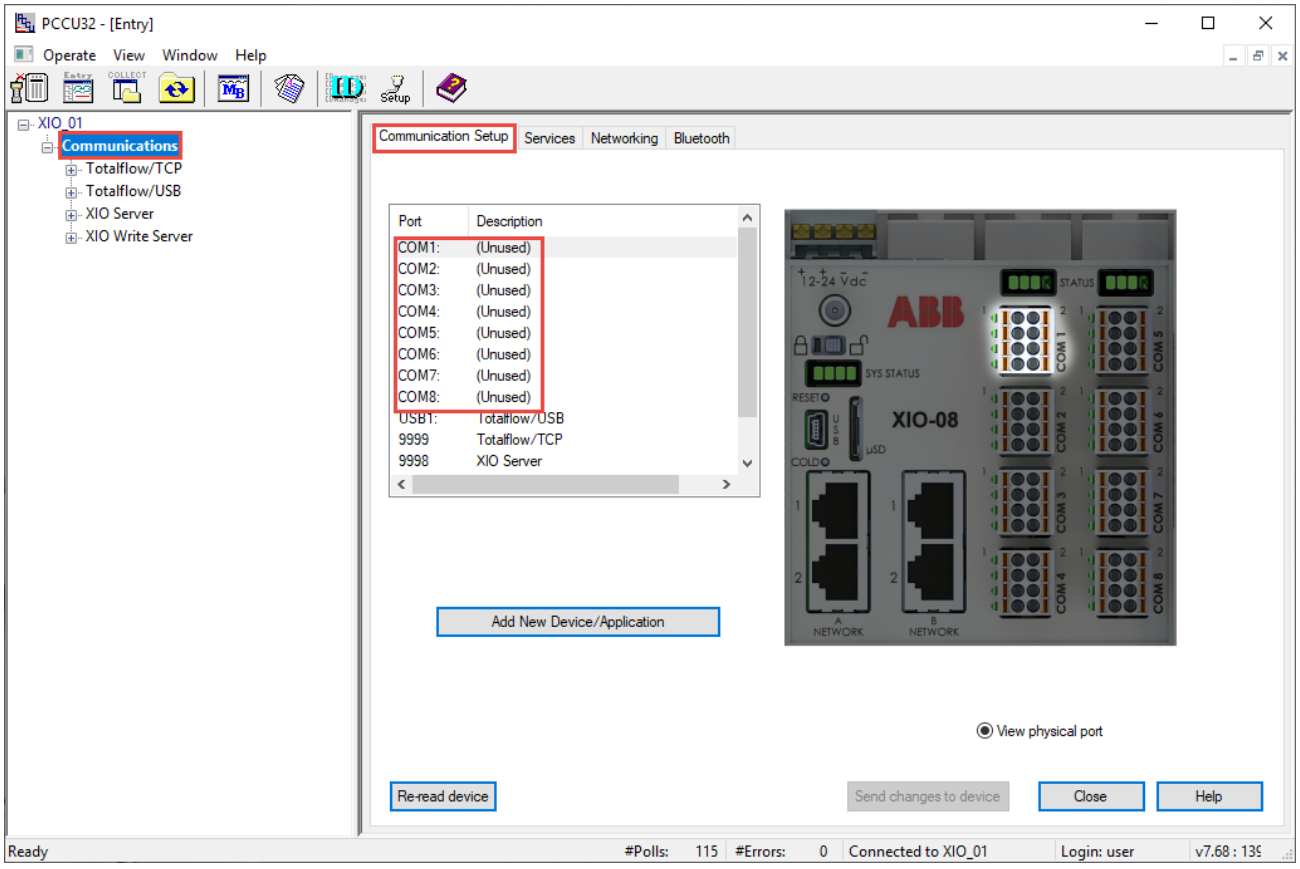
4.7.1.2 Assign and configure port from the Communication Setup tab

This procedure adds, assigns, and configures the COM port with the XMV interface from the Communication Setup tab. When the port and application are assigned and added in this way, the default settings need to be updated. The default settings on this screen do not reflect the optimal values for ABB multivariable transmitters. Optimal values to complete the configuration of the port are provided in this procedure.

To configure the COM port:

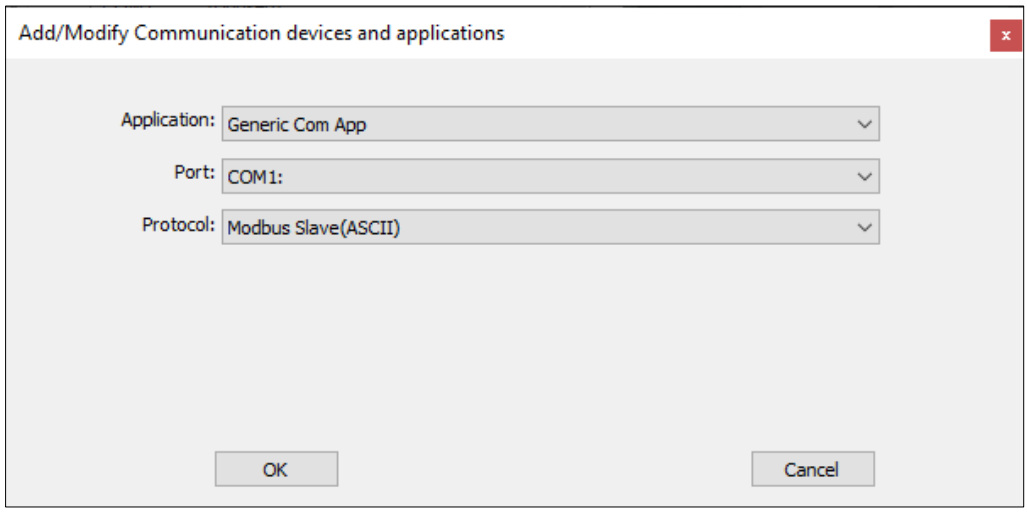
1. Verify that the status LEDs on the corresponding COM port column display solid green on first 3 LEDs. The 4th LED should not be lit.
2. On the PCCU navigation tree, click **Communications**. The Communications Setup tab displays (Figure 4-42).
3. View the list of ports. In new devices, all COM ports display as unused (when ports are already assigned to applications the application instance Name or ID displays in the port description). The figure below shows a new XIO with unused or unassigned ports.

Figure 4-42: XIO Communication setup tab



4. Add communication application to a COM port:
   a. Select the **COM** port.
   b. Click **Add New Device/Application**. The Add/Modify Communication device and applications window displays (Figure 4-43).

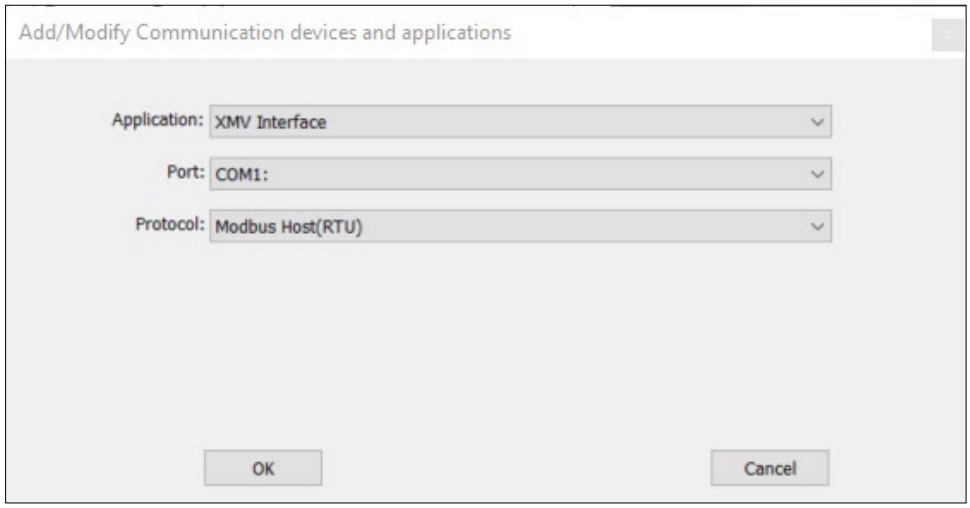
Figure 4-43: Add/Modify Communication devices and applications



   c. Select the appropriate application from the **Application** drop-down list. In this example, the selected application is the XMV Interface (Figure 4-44).

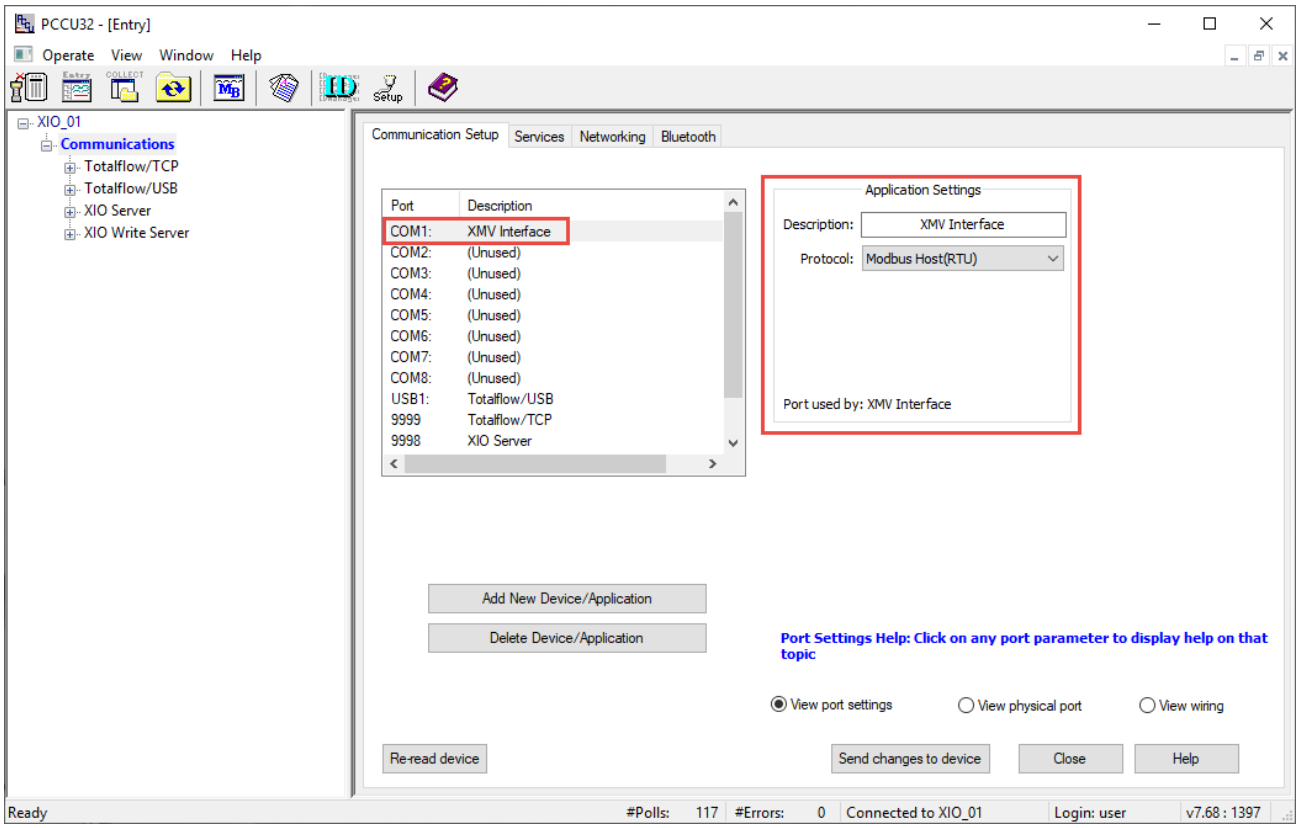
d. Select a port (COM1 – COM8) from the **Port** drop-down list.
e. Select the appropriate protocol from the **Protocol** drop-down list.

Figure 4-44: Add Application, Port, and Protocol



5. Click **OK**. The port list displays the XMV Interface assigned to the selected port (COM1 in this example, Figure 4-45). The description and protocol display also. These are configurable fields and can be changed before saving the configuration, if desired.

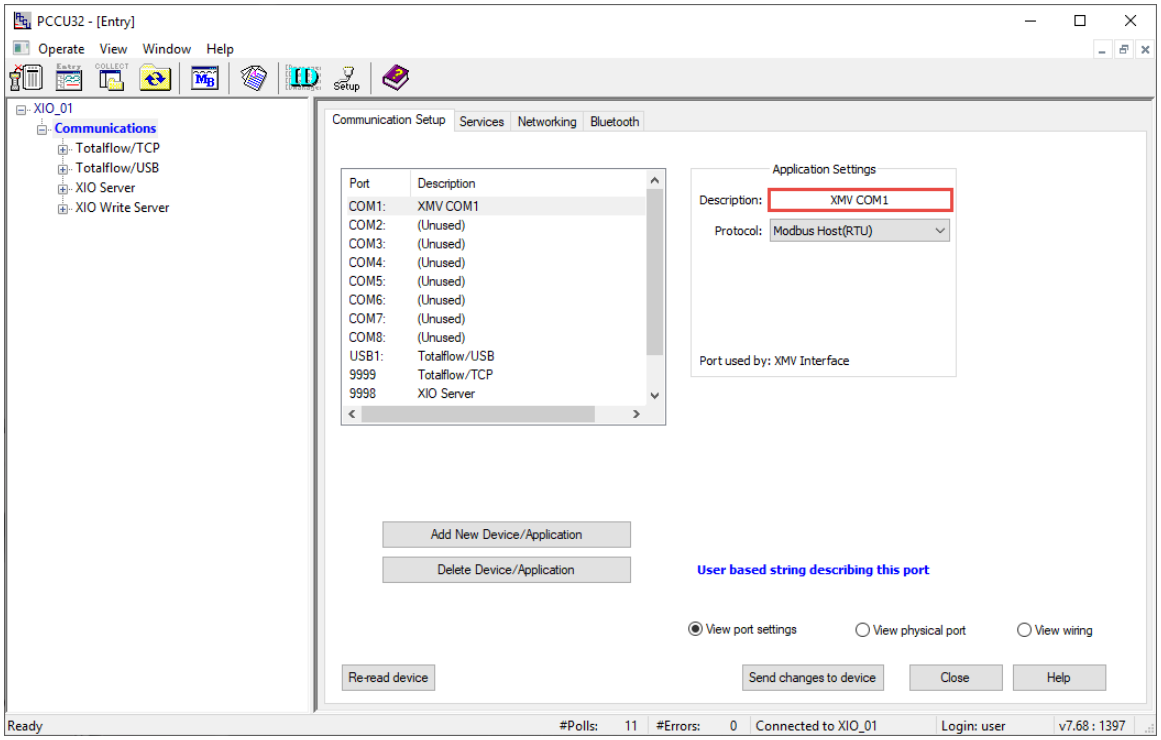
Figure 4-45: Add XMV Interface for COM1 – default app name



6. Configure the application:

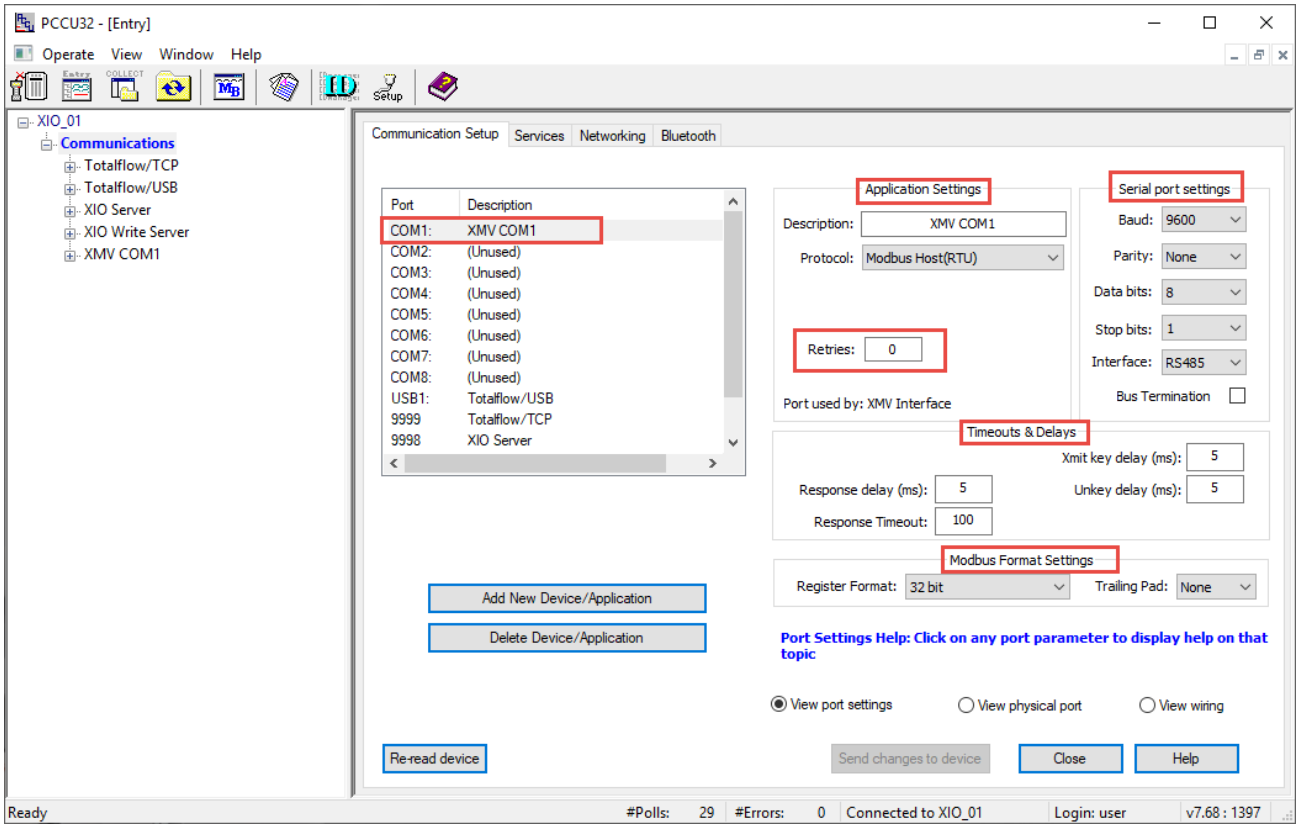
a. Type a unique port description in the Description field. The default description is the application name. If planning to add additional COM ports, type a description that helps identify the port.
b. Configure the desired protocol if needing to change the initial selection.

Figure 4-46: XMV Interface for XIO COM1



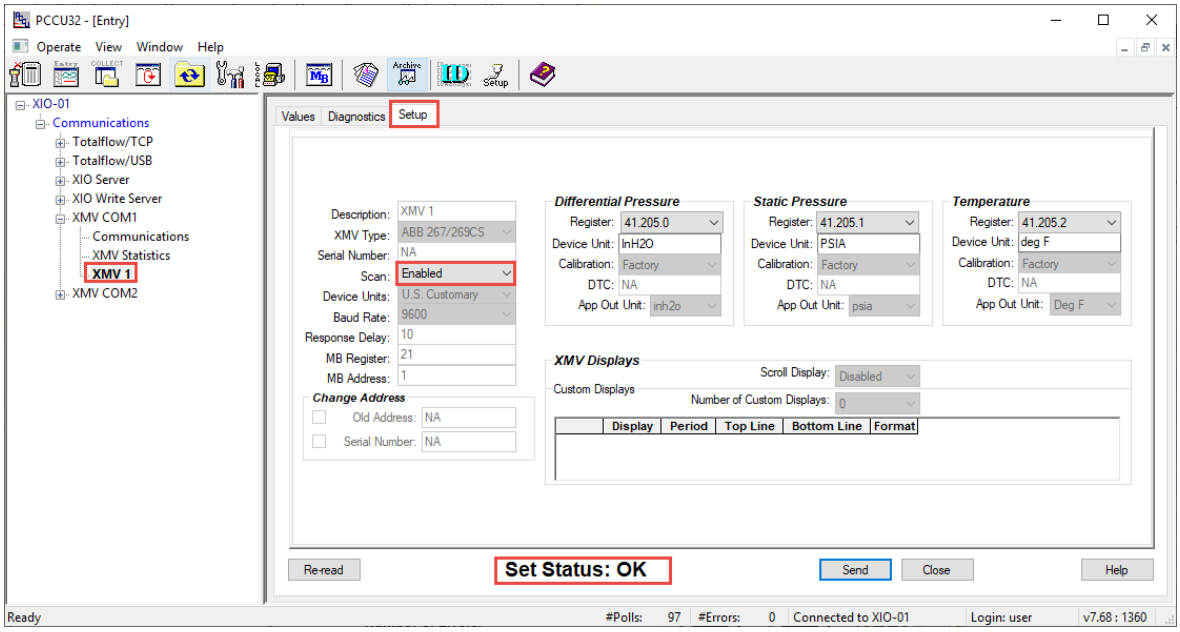
7. Click **Send changes to device**. The port displays its new description and displays additional settings with default values: Application, Serial port, Timeout & Delays, and Modbus Format Settings.

Figure 4-47: XMV Interface for XIO COM1 – default communication and format settings



8. On the XIO, verify that the PWR LEDs to the left of the COM port turn on indicating that the port is active. PWR LEDs light only after the COM port is assigned to a communication application. They remain off for unassigned ports.
9. Refresh the navigation tree to verify that the XMV Interface displays under Communications. If the application does not display, click **Close** to disconnect and then click **Entry** to re-connect. The navigation refreshes and displays the XMV Interface.
10. Configure the port:
    a. Expand the **XMV Interface** instance, then select **Communications**. The Setup tab displays with the port parameters for communication with the peripheral.
    b. Verify the configuration parameters. The Setup screen reflects the default parameter values from the Communication Setup tab and additional parameters.
    c. Configure parameters as required.
11. Configure the XMV:
    a. On the communication tree, select **XMV1**, then select the **Setup** tab.
    b. If the **Scroll Displays** field, under the XMV Displays section is enabled, change to **Disabled**.
    c. Click **Send**. This activates parameter fields for configuration.
    d. Configure the required parameters.
    e. Select **Enable** in the Scan drop-down list.
    f. Click **Send**.
    g. Verify that the Set Status displays **OK**.

Figure 4-48: XMV1 configuration



12. Select the **Values** tab. Verify that measured variables display values and the Scan Status displays: OK.
13. Verify the XIO-XMV connection:
    a. On the navigation menu, select the XMV application instance. The main XMV screen displays.
    b. Verify that variable values display and that the poll counter displays polls. Click **Re-read** or select **Monitor** to update screen values. The number of errors counter should display zero or should not be increasing. A certain number of errors could be present due to lack of initial communication prior to XMV configuration.
14. When the XIO-peripheral communication is successful, proceed to section 4.7.2.

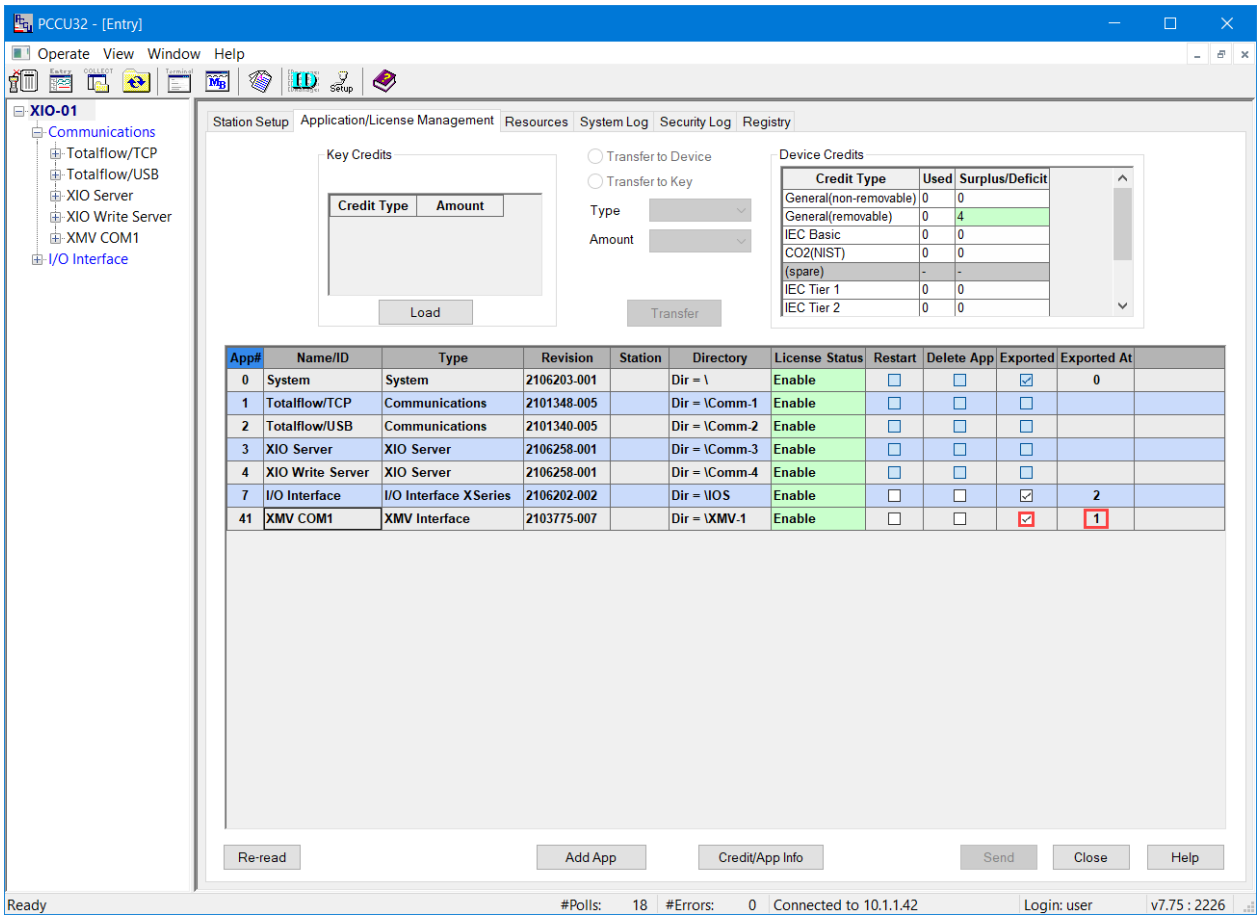
4.7.2 Configure XIO application export

Configure XIO communication applications to export their information and data to the remote controller. The application must be set to export to be visible from the remote controller.

To export the application:

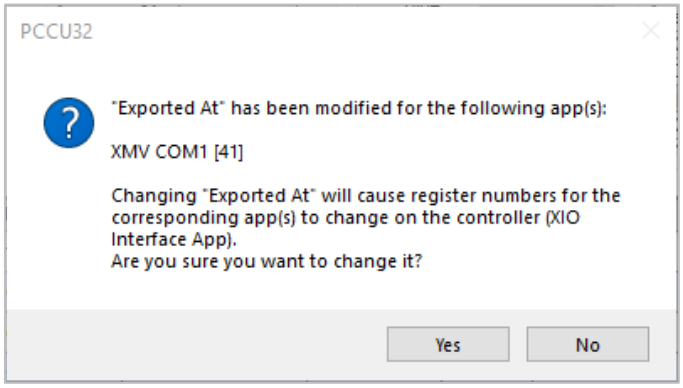
1. On the navigation tree, select the Station ID (XIO ID). The Station Setup tab displays.
2. Select the **Application/License Management** tab. The application list displays.
3. Locate the application to export.
4. Select the **Exported** check box for the application. The next field, under the Export At column, automatically displays the next available index number (in the example, it is 1).
5. Accept the index number provided (easiest) or select a different one by selecting the field and choosing another number from the drop-down list. Available values are 1-15.

Figure 4-49: Example of selected application to export – exported at application index 1



6. Click **Send.** A warning message to confirm the application index assignment displays. This message also displays if the index is changed once the XIO is operational. Because this is the first time installing the device, the change is confirmed. Once the application is operational, be aware that changes cause register number change as indicated. Update the application index with caution.

Figure 4-50: Warning before exporting application



7. Click **Yes**.
8. Proceed to section 4.7.3 to verify that the application is visible and data is received at the remote controller.

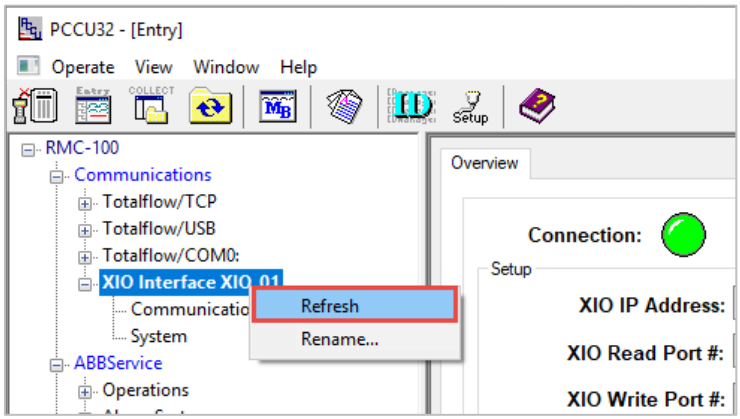
4.7.3 Verify XIO application export on the RMC

Exported XIO applications display under the XIO Interface on the RMC navigation tree to help distinguish the XIO remote applications from the local applications. Access to the remote applications from the RMC provides visibility into the application values and configuration without needing to connect to the XIO.

To verify application export:

1. On the RMC navigation tree, expand the XIO Interface instance. Notice that the exported application may still not be visible under the XIO Interface.
2. Right-click the **XIO Interface** instance and select **Refresh**.

Figure 4-51: Refresh the navigation tree



3. Verify that the exported XIO COM application (XMV COM1 in this example) displays on the navigation tree (Figure 4-52).

Figure 4-52: Verify the XIO application displays on the RMC navigation tree

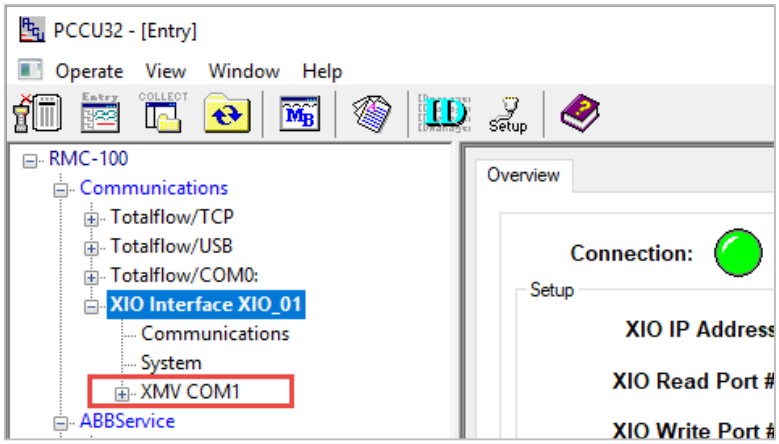
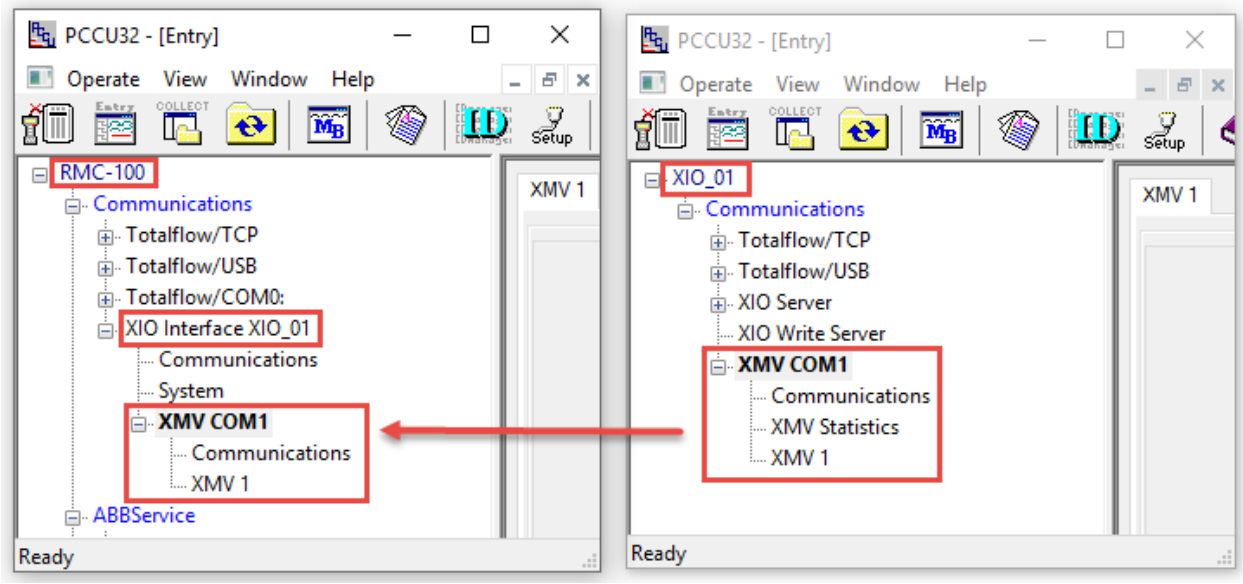


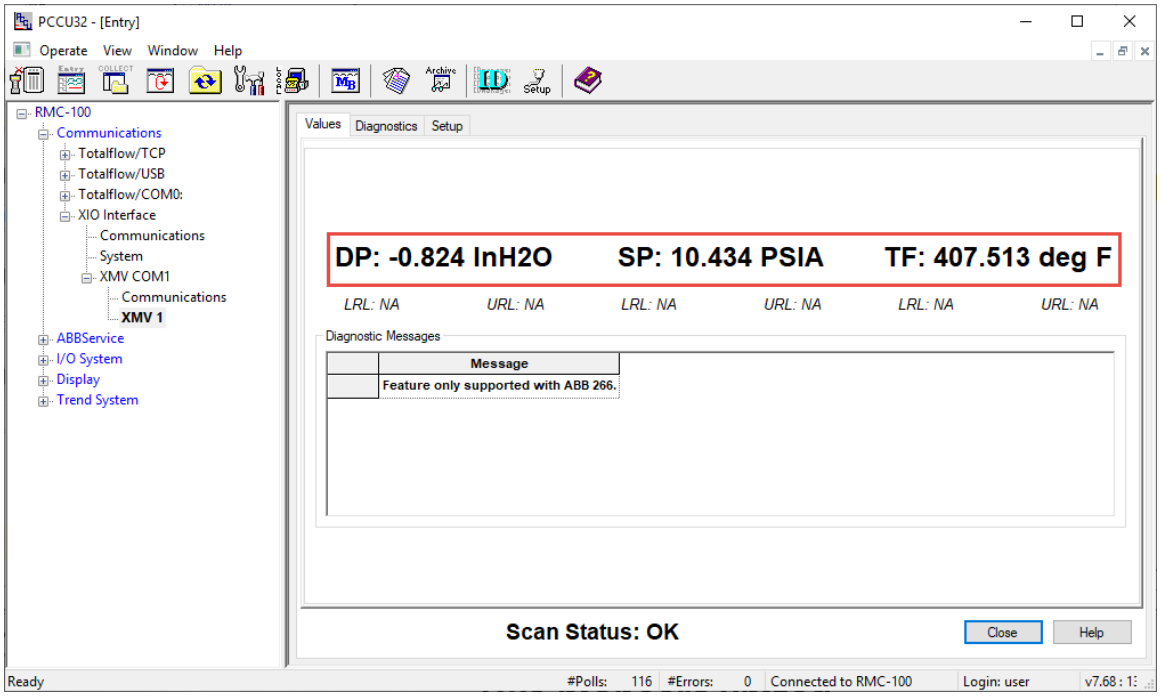
Figure 4-53 displays both RMC and XIO navigation trees. The RMC should display all exported XIO applications.

Figure 4-53: Exported XIO application visible on the RMC (left screen)



4. View current measurement values sent by the remote peripheral. For the example used in this procedure:
   a. Expand the XMV application for the port of interest.
   b. Select the remote multivariable of interest. For example, **XMV1** (there may be multiple XMVs connected to a single COM port).
   c. View the values for DP, SP, and TF. Click **Re-read** to refresh to the latest values or select **Monitor** to keep track of latest values as they change.

Figure 4-54: Verify RMC is receiving measurement data from remote peripheral

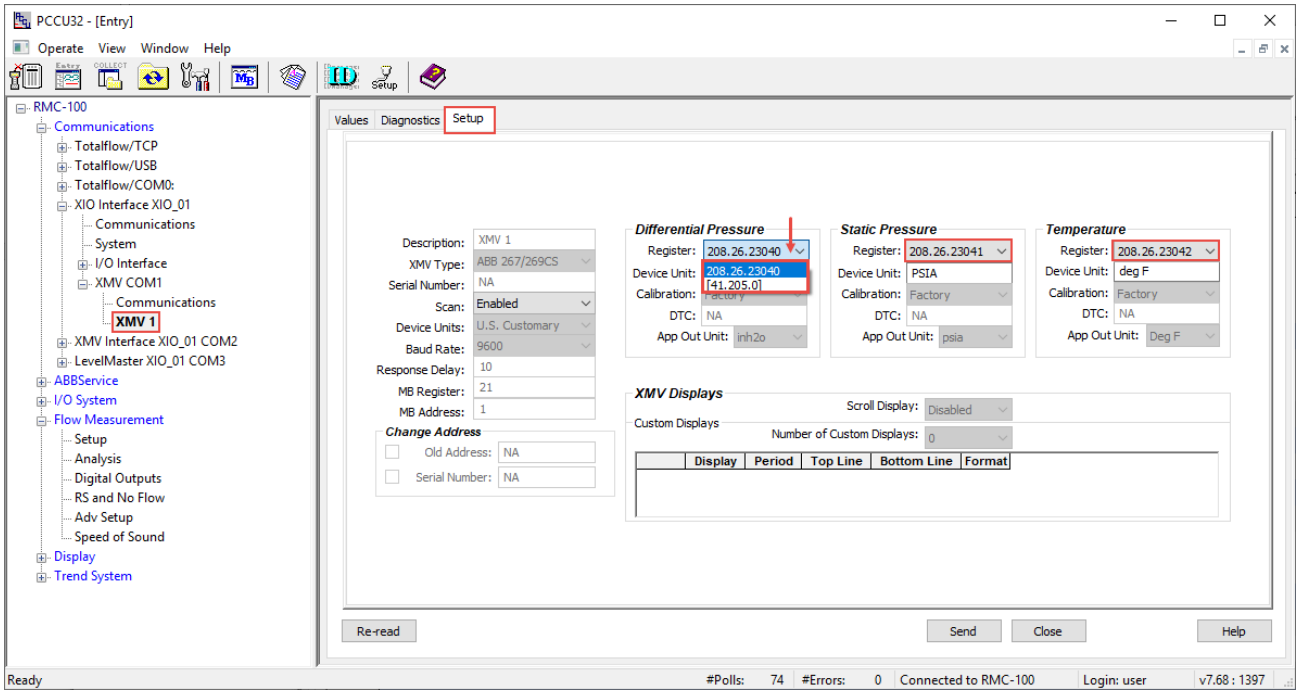


4.7.4 Configure measurement applications to use XIO values

To make data available for applications on the RMC, configure the RMC register numbers assigned to store the measurement values received from the remote device. For example, configure registers with XMV values on a measurement tube on the RMC:

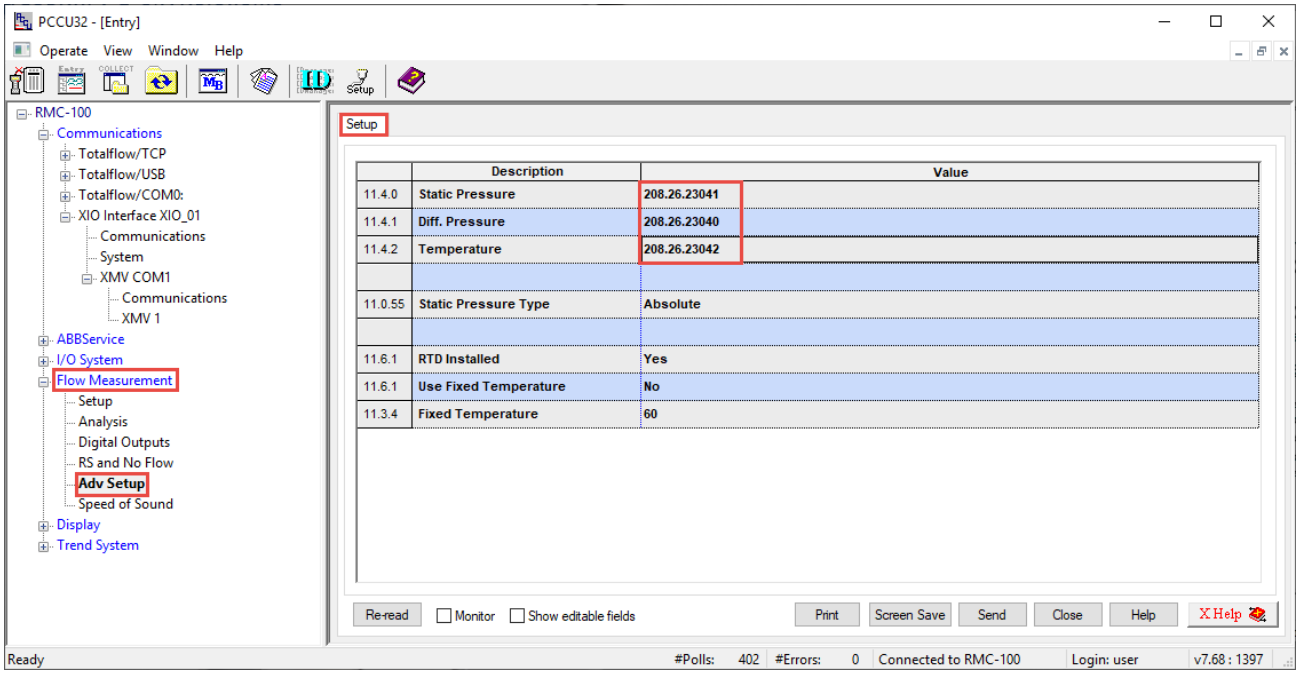
1. On the navigation tree, under the exported XMV Interface, select the XMV of interest and then select the **Setup** tab.
2. Take note of the register values displayed in the variable register fields. These fields display the registers on the RMC by default. Select the register field to view registers on the XIO. The RMC registers display on top. The registers on the XIO display below, in brackets.

Figure 4-55: Obtain RMC registers storing remote peripheral measurement values



3. On the navigation tree, expand the measurement application instance and then select **Adv Setup**. The Setup screen displays.
4. Type the register numbers for each variable.

Figure 4-56: Configure registers storing remote peripheral measurement values



5. Click **Send**. The measurement application instance can use the values in the calculations as required.

4.8 Configure Ethernet-Serial Passthrough

This section describes how to configure the XIO-04 or XIO-08 and the Ethernet-serial passthrough function in order to extend serial port capacity to an RMC.

Both the RMC and the XIO must connect either directly using Ethernet ports or to the field area network switch. In this scenario, the XIO performs the role of an Ethernet-serial converter and makes COM ports available to applications on the RMC. The XIO relays all communications from the attached serial devices to the controller on the Ethernet port (network connection). Both must have valid IP addresses. Serial communication protocols are used transparently (encapsulated) over the Ethernet interface.

The RMC manages communication with the peripherals on the XIO with communication applications instantiated and configured locally. The RMC manages and monitors the XIO COM ports as if they were its own onboard ports.

IMPORTANT NOTE: As an example, the scenario described in this section describes the configuration of an XIO COM port connecting to an ABB multivariable (XMV). An XMV Interface application instance is added on the RMC for communication with that device. Other scenarios might include multiple XMVs on the same COM port or additional XMVs connected to other ports. The RMC uses an XMV Interface instance for every COM port configured in passthrough mode. Adapt the following steps for the type of peripheral and associated communication application:

- To communicate with other types of ABB devices, use their specific communication application.
- To communicate with third-party peripherals, use the Generic Com App.

IMPORTANT NOTE: The Ethernet-Serial Passthrough function activates on a per-port basis. If all XIO COM ports require passthrough, each port requires its own Ethernet-Serial Passthrough instance. Use a naming convention for the instances that makes XIO COM port identification easy. Both the Ethernet-Serial Passthrough and the XIO server can be active on the XIO, but each owns the ports assigned to it.

IMPORTANT NOTE: For additional details on the passthrough functionality and configuration, see the Ethernet-Serial Passthrough Application Guide listed in Additional information.

The procedures in these sections assume that the COM ports are wired correctly.

4.8.1 Configure the XIO

This procedure configures the XIO Ethernet port to act as a passthrough for the specified serial port. It also configures the serial port for communication with the attached peripheral.

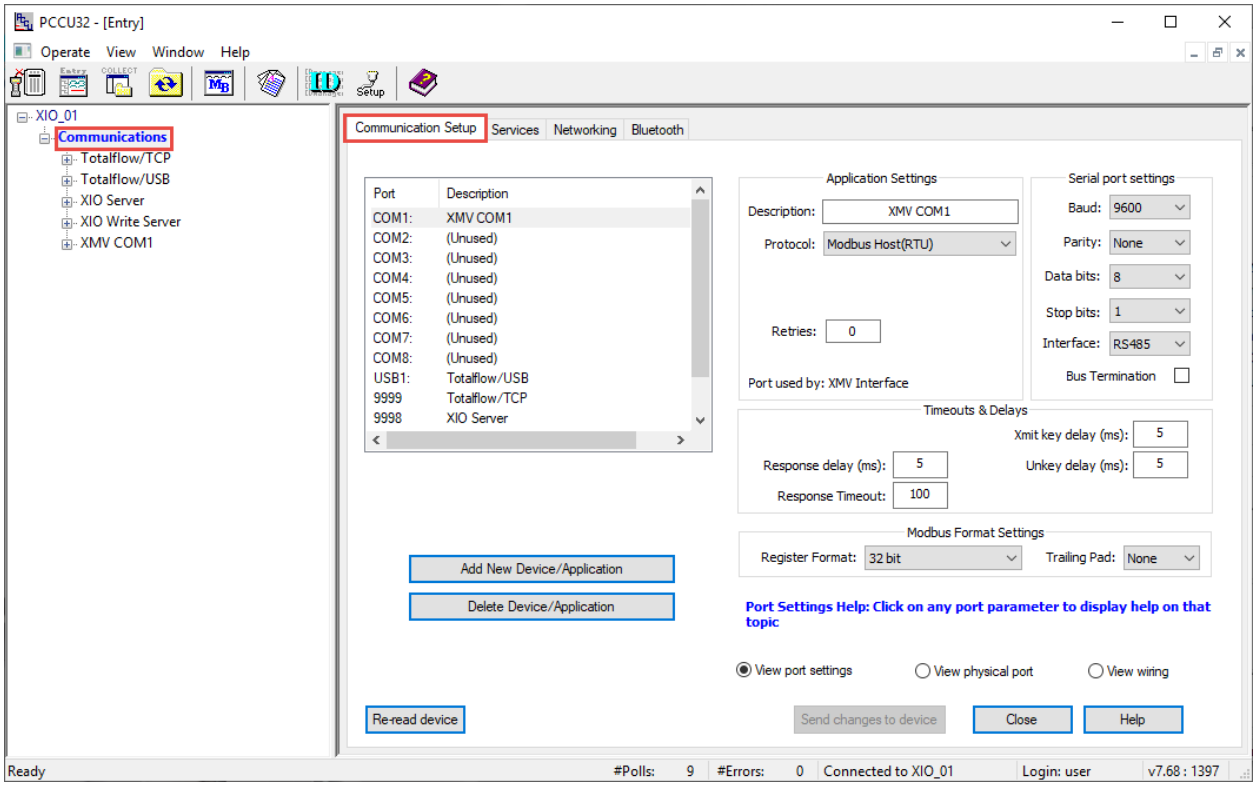
The serial port on the XIO can connect external devices such as XMVs and other transmitters while the corresponding interface application (for example, XMV Interface) runs on the RMC.

Use any of the serial (COM) ports on the XIO to connect with any external serial device, such as radios and measurement transmitters. This scenario shows a single ABB multivariable transmitter (XMV) connected to the XIO. Other scenarios might include multiple XMVs on the same COM port.

To configure Ethernet-Serial passthrough for an XIO COM port:

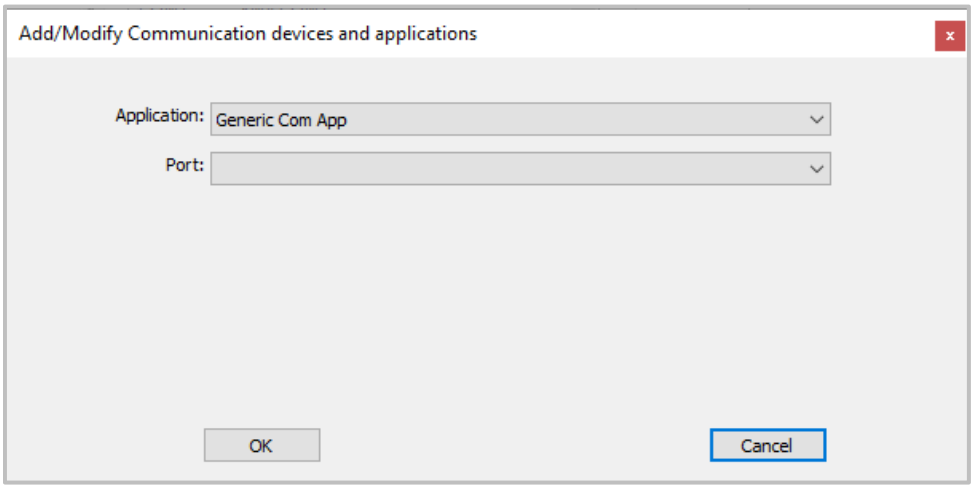
1. On the Navigation tree, select **Communications**. The Communication Setup displays.

Figure 4-57: Communication Setup



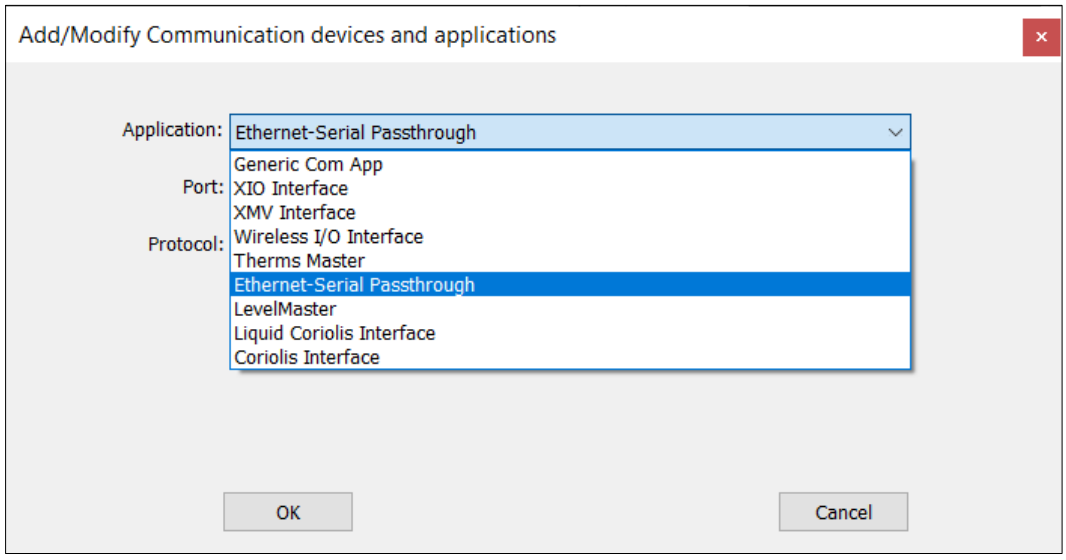
2. Click Add New Device/Application.

Figure 4-58: Add/Modify Communication devices and applications



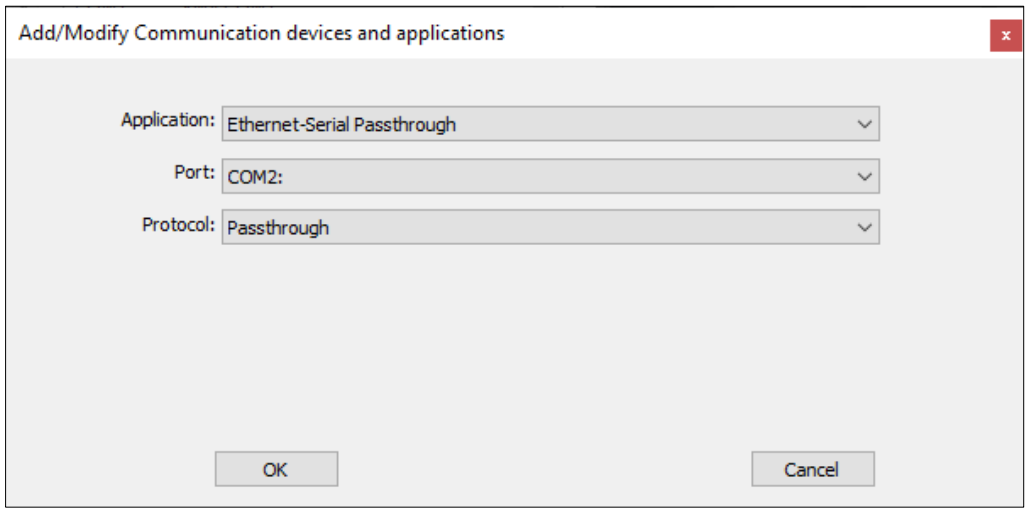
3. Select **Ethernet-Serial Passthrough** from the Application drop-down list

Figure 4-59: Adding Ethernet-Serial Passthrough application



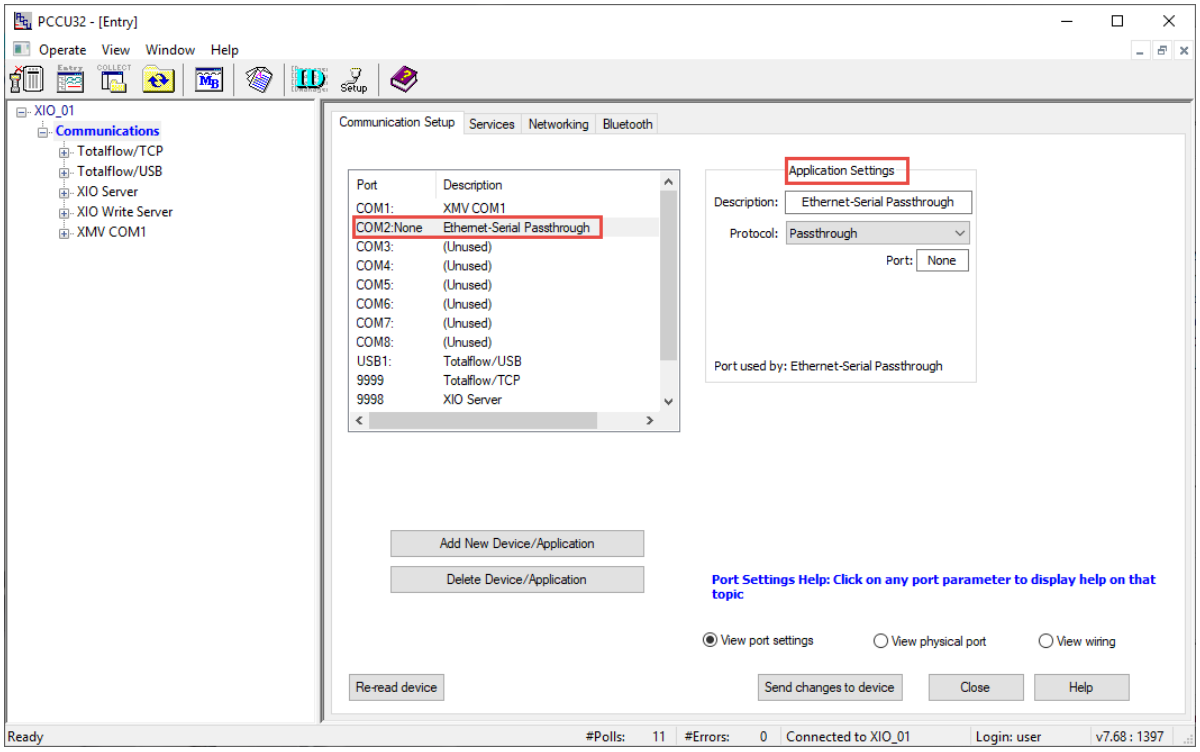
4. Select the required COM port from the **Port** drop-down list.
5. Select the required protocol from the **Protocol** drop-down list.

Figure 4-60: Assign COM port and protocol to Ethernet-Serial Passthrough



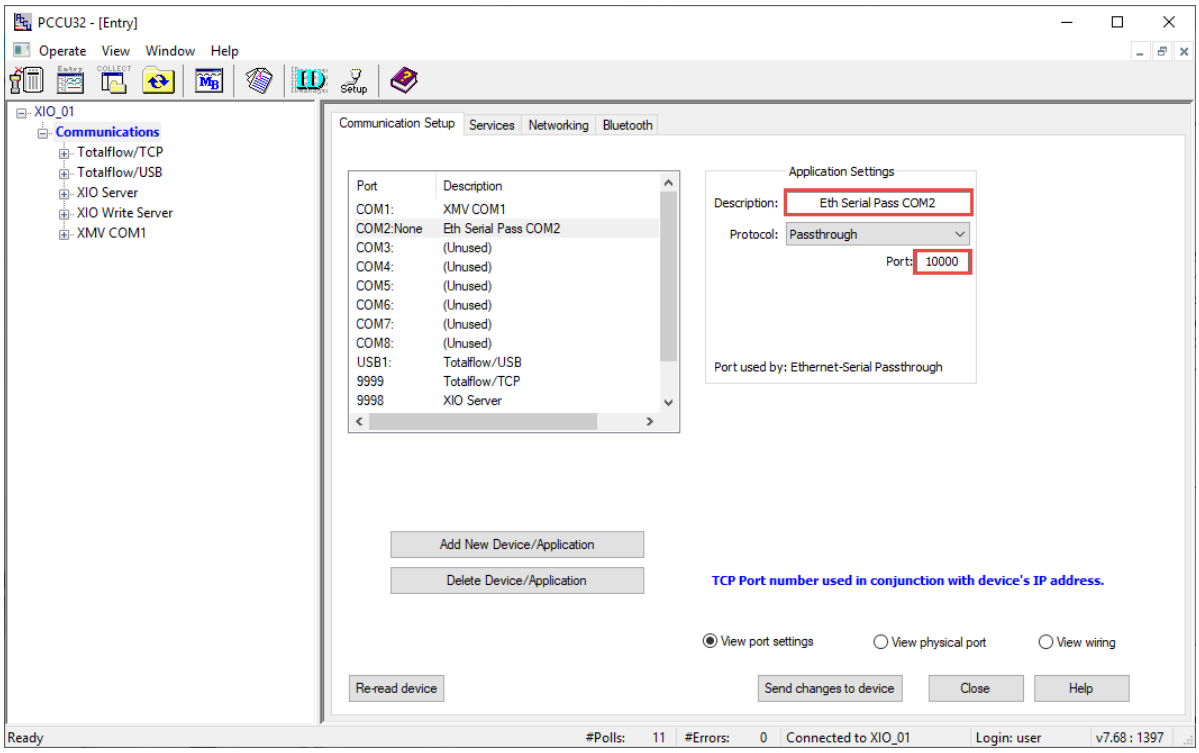
6. Click **OK** to complete selections and return to the Communication Setup screen. The serial port to which the Ethernet-serial passthrough is applied displays in the port list. In the example below, the port shows as COM2:None. "None" indicates that the port and application do not have a TCP port assigned yet. The field: Port, in the Application Settings section is the TCP port and the default is: None. Configure the port in the next steps. A unique TCP port is a required parameter for each Ethernet-Serial Passthrough instance.

Figure 4-61: Ethernet-Serial Passthrough COM port assignment – Default settings



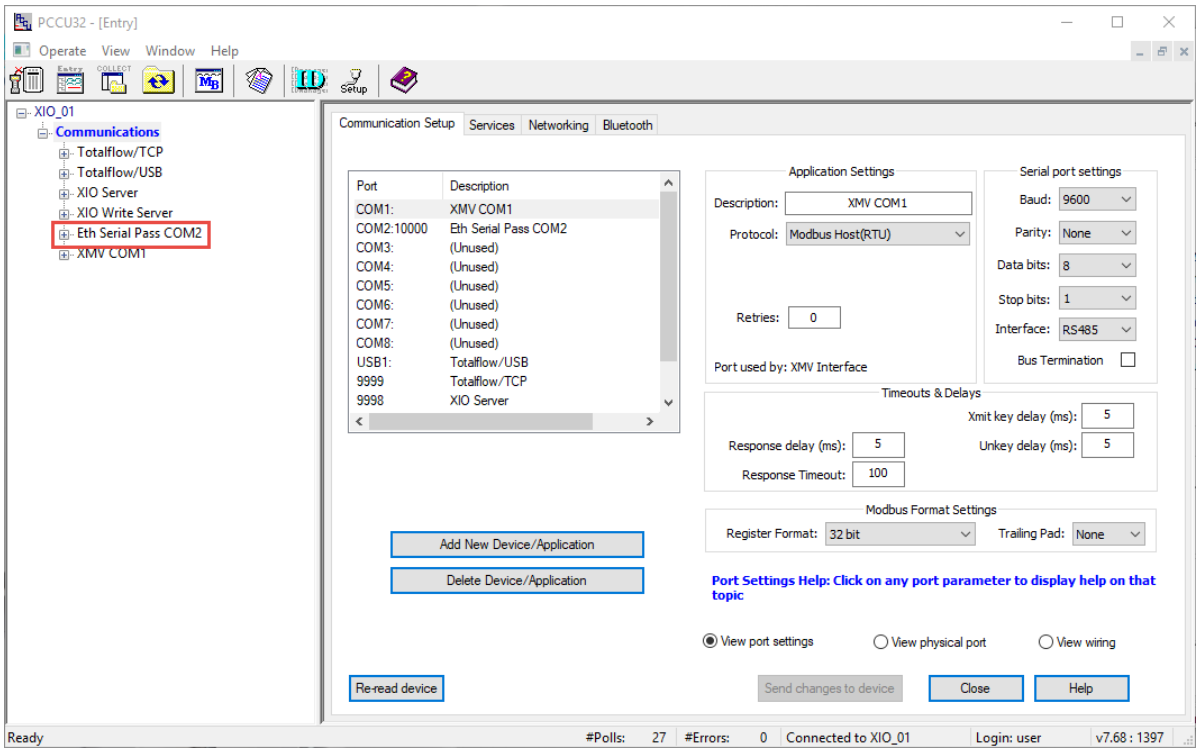
7. Configure Application Settings:
   a. Configure a new description that helps identify the assigned COM port, if desired.
   b. Configure the TCP port in the Port field.

Figure 4-62: Ethernet-Serial Passthrough TCP port assignment



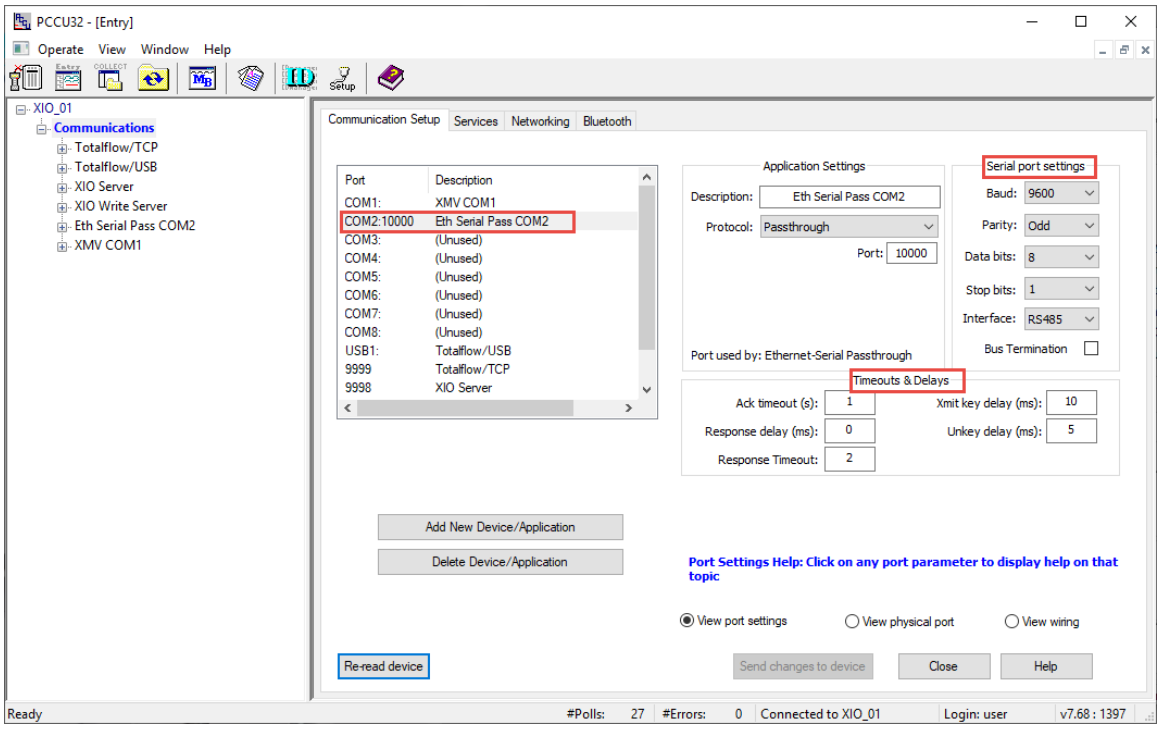
8. Click **Send changes to device**. The Ethernet-Serial Passthrough application displays on the navigation tree.

Figure 4-63: Ethernet-Serial Passthrough on the navigation tree – instance renamed



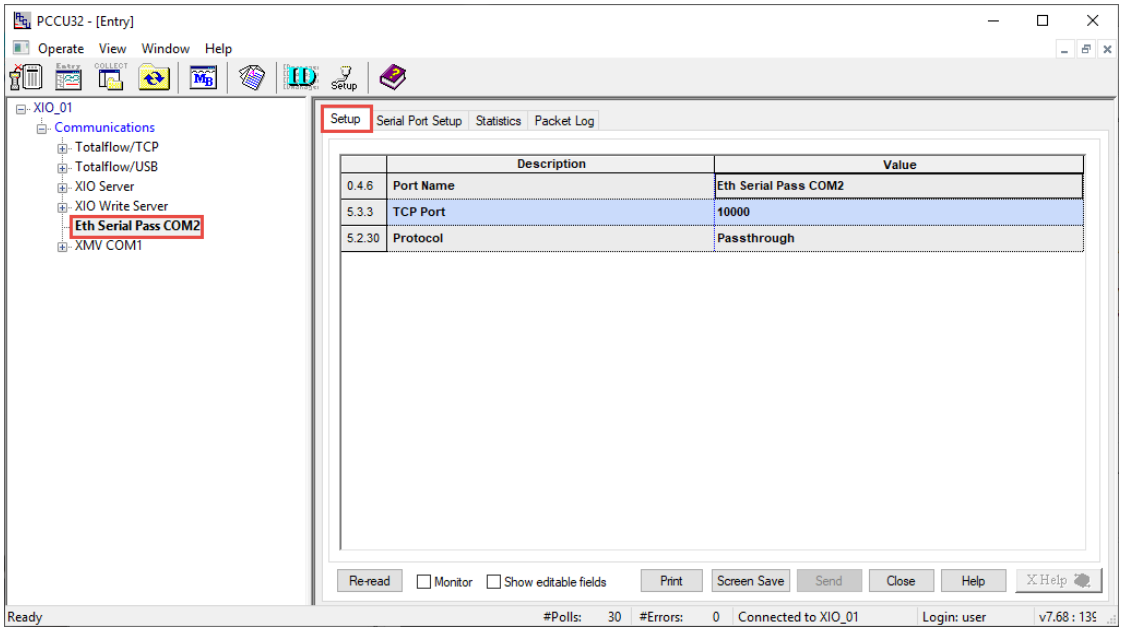
9. On the Communication Setup screen, select the Ethernet Serial Passthrough port from the list. Additional settings display with default values in sections: Serial port and Timeout & Delays settings.

Figure 4-64: Ethernet-Serial Passthrough application on XIO navigation tree



10. Configure settings as required on the Communication Setup screen or by selecting the Ethernet-Serial Passthrough application from the navigation tree as in the next steps.
11. On the Navigation tree, select the Ethernet-Serial Passthrough instance created above. The Setup tab displays with the Application settings configured above.

Figure 4-65: Ethernet-Serial Passthrough Setup – User defined Application Settings

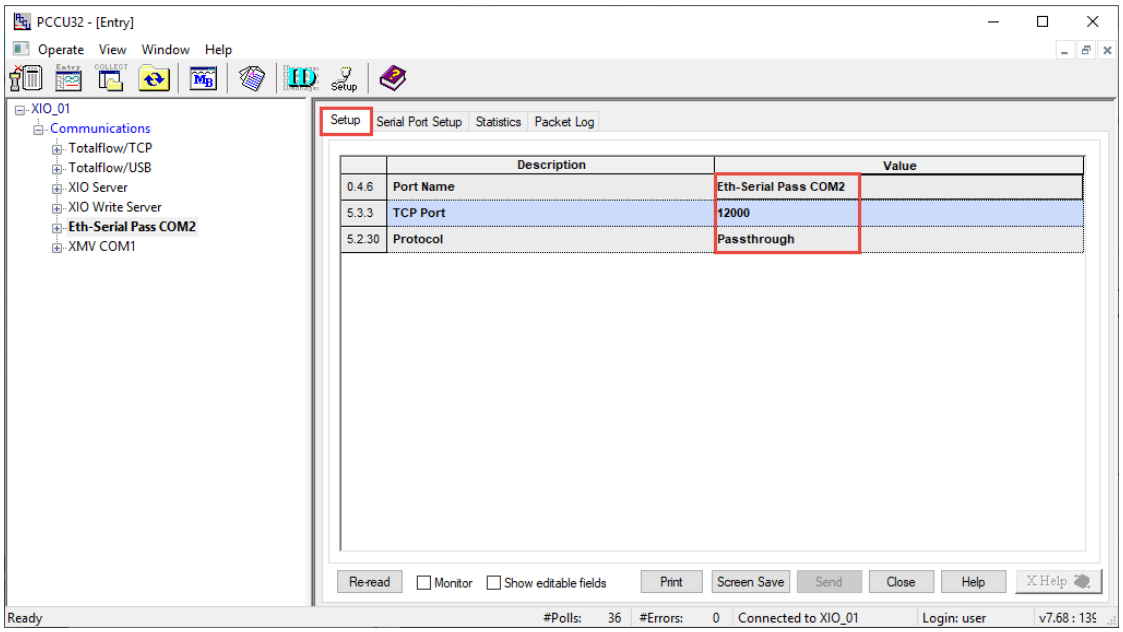


12. If you need to update the configuration (Figure 4-66):

a. Type a new descriptive port name if necessary. Ideally, the description identifies the port the passthrough function is associated with. This will make port selection easier when configuring the communication application on the remote controller.
b. Configure the TCP port. Type a number from the valid TCP range of 0-32768 (excluding ports already in use). In this example the TCP port number is updated to 12000.
c. Verify that the protocol selected at the time the application was added is correct. Change the protocol if required.

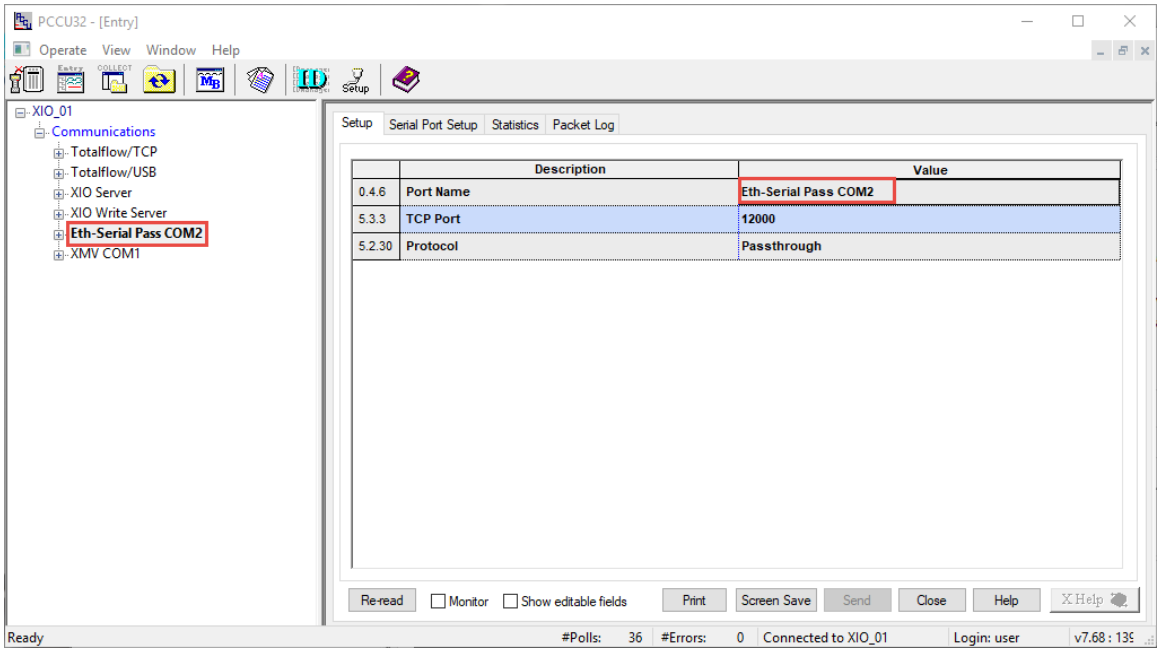
13. Click **Send**. Configuration updates display.

Figure 4-66: Ethernet-Serial Passthrough – Application Settings update from Setup tab



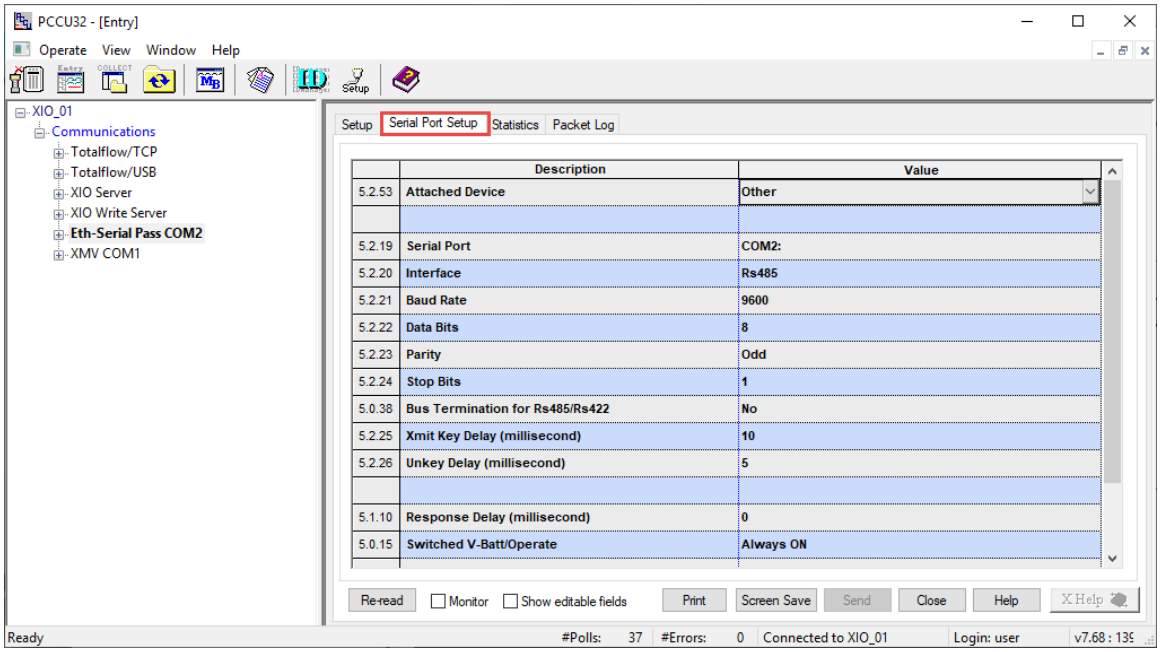
14. Click **Re-read** or refresh the navigation tree if there were configuration updates for application name. The new port or application instance name displays on the navigation tree.

Figure 4-67: Ethernet-Serial Passthrough for XIO COM2 (with user-defined name)



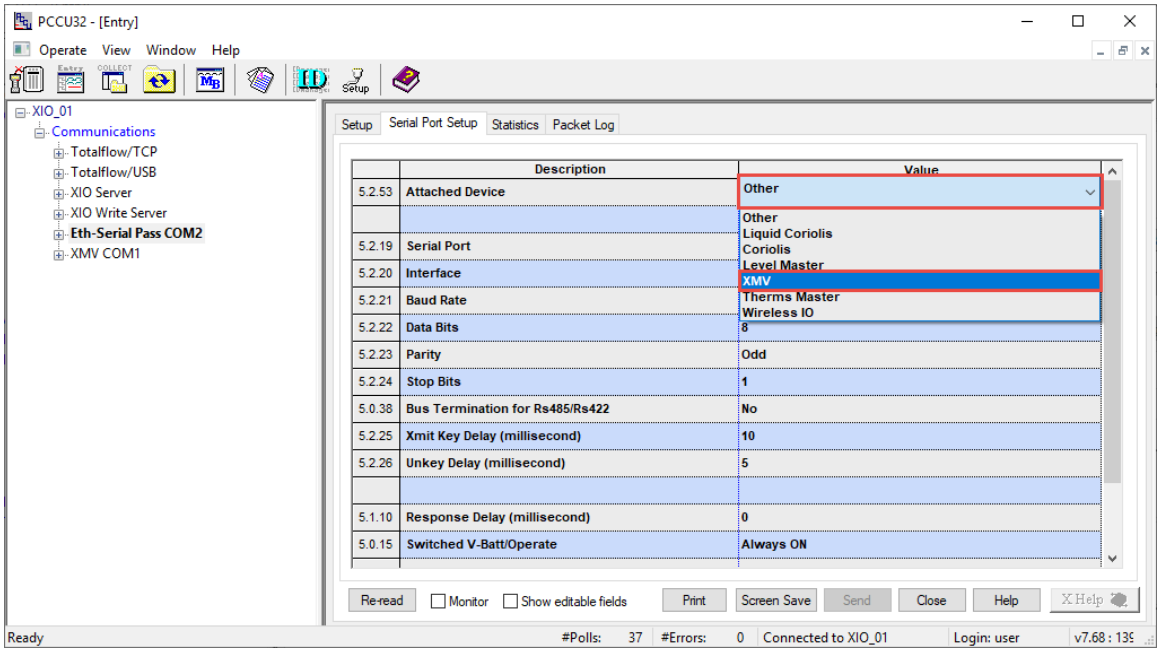
15. Select the Serial Port Setup tab.

Figure 4-68: Ethernet-Serial Passthrough (COM2) - Serial Port Setup



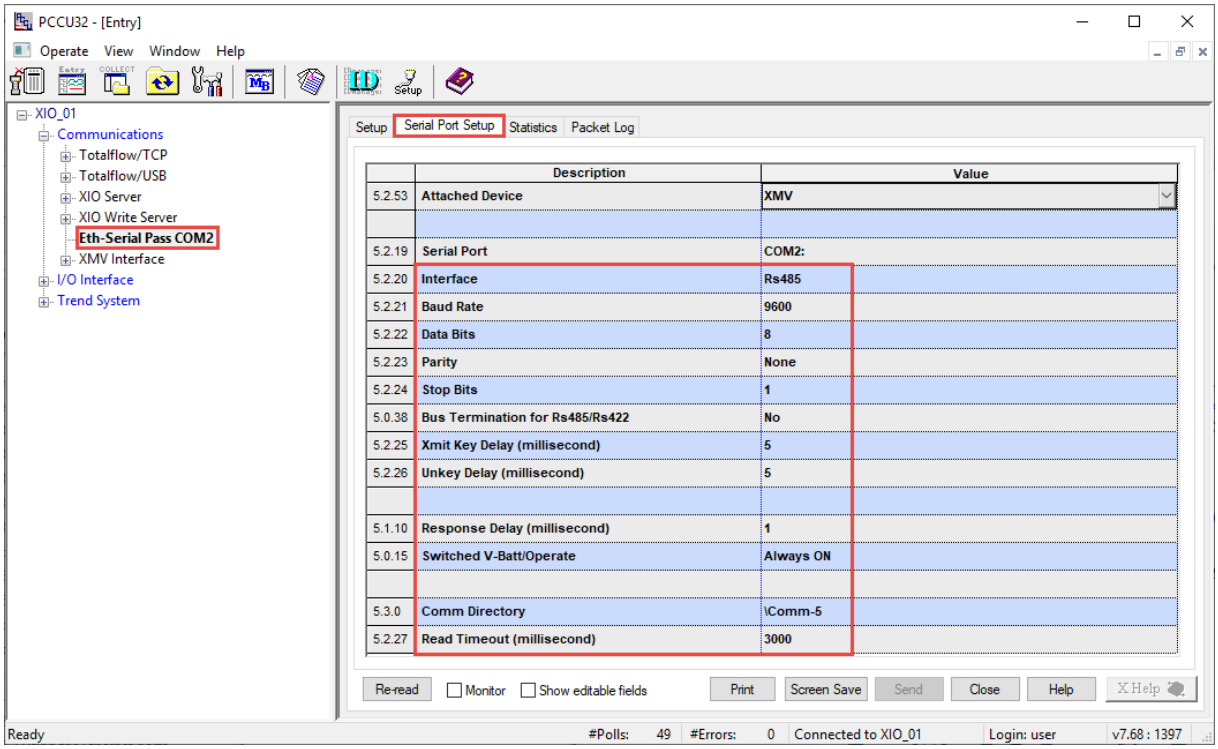
16. Select the type of device connected to the COM port from the **Attached Device** drop-down list. For this example, the XMV.

Figure 4-69: Attached Device drop-down list



17. Configure communication parameters to match those required by the attached device. These parameters must also match those configured on the application on the RMC-100.
18. Click **Send**.

Figure 4-70: Configure XIO COM port communication values (Default values for the XMV)



19. Proceed to configure the communication application on the remote controller in section 4.8.2 Configure the RMC.

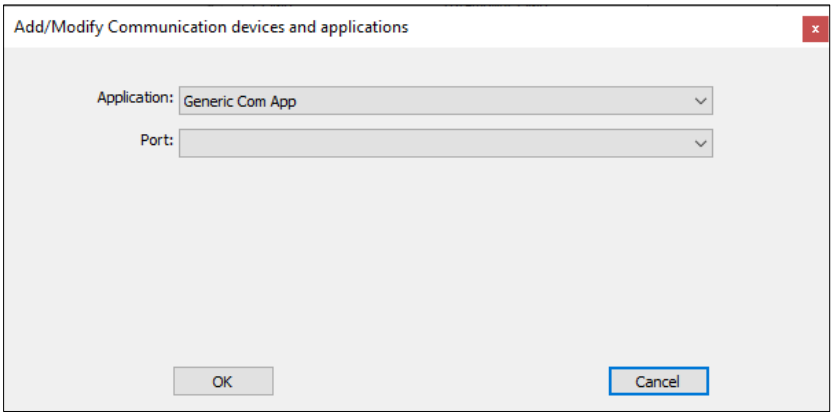
4.8.2 Configure the RMC

The RMC detects the Ethernet-Serial passthrough application instance(s) when activated on the XIO. This procedure takes advantage of the RMC Auto Discovery feature to assign a local communication application to a remote COM port on the XIO.

To configure a serial communication application on the RMC for an XIO COM port:

1. On the Navigation tree, select **Communications**. The Communication Setup displays.
2. Click **Add New Device/Application**. The Add/Modify Communication devices and applications window displays.

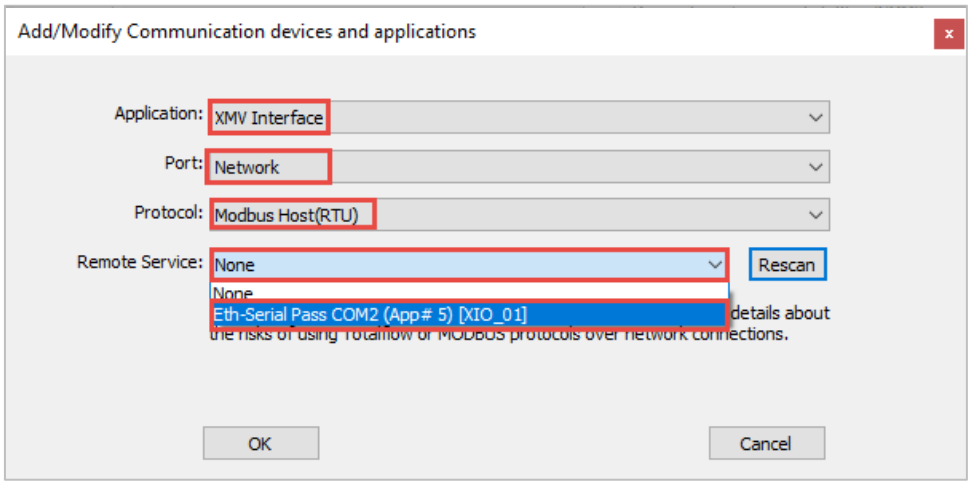
Figure 4-71: Add/Modify Communication devices and applications



3. Select the serial communication application required from the **Application** drop-down list (Figure 4-72). In this example, the XMV Interface application is selected for the XMV connected to the XIO.
4. Select **Network** from the Port drop-down list. The network port here refers to the Ethernet port.

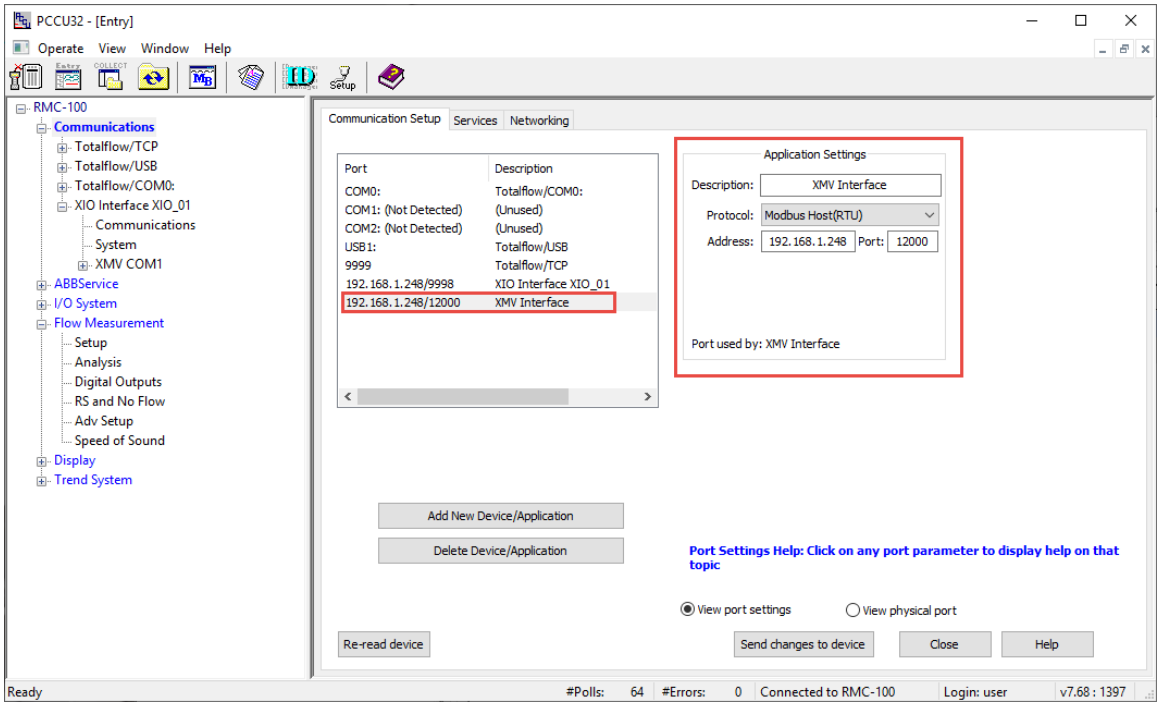
5. Select the required protocol from the **Protocol** drop-down list. This protocol is the serial protocol required for communication with the peripheral attached to the XIO COM port. Select the protocol that applies to the peripheral and type of communication.
6. Select the XIO Ethernet-Serial Passthrough instance from the **Remote Service** drop-down list. The XIOs with the active Ethernet-serial passthrough function display automatically (they are detected by the RMC Auto Discovery feature). If you have changed the default Ethernet-Serial Passthrough description as recommended, each instance uniquely identifies the associated port. The slot number assigned to the Ethernet to Serial Passthrough application on the XIO displays also. In the example the application has slot number 5.

Figure 4-72: Assign XMV Interface to detected XIO port (shown in Remote Service field)



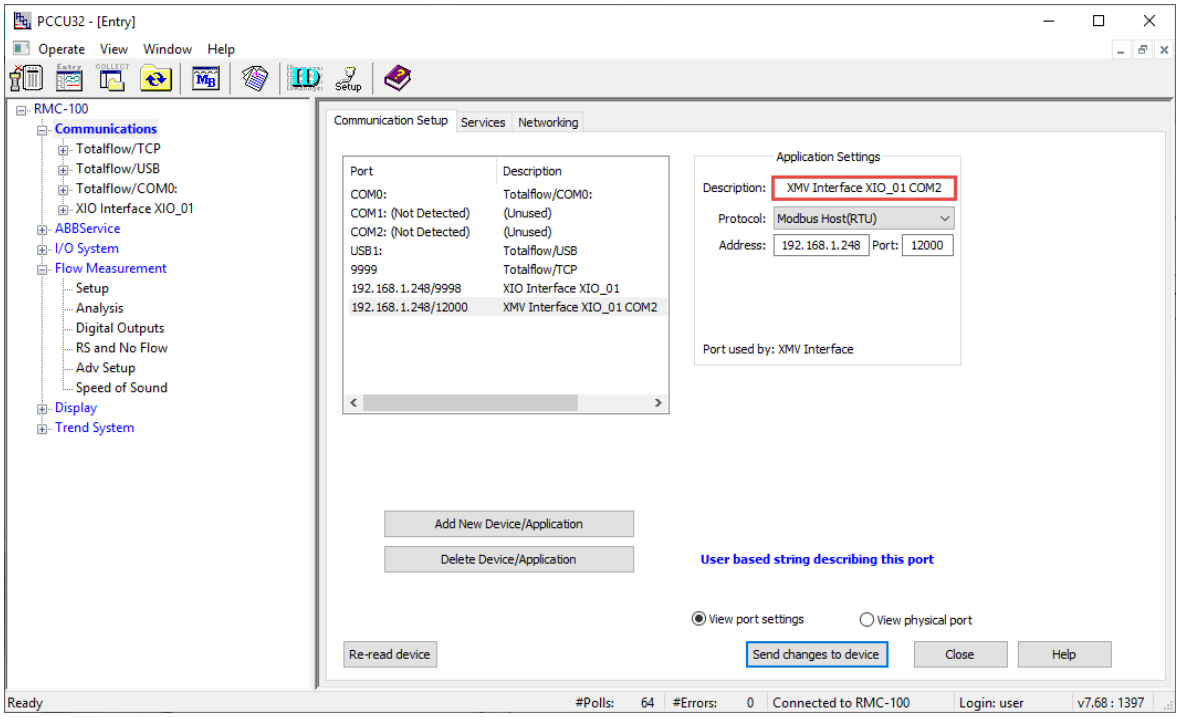
7. Click **OK** to complete selections and return to the Communication Setup screen. A new port displays in the port list with the associated application (XMV Interface in this example). The port is the destination's logical port on the XIO: the combination of the XIO's IP address and the specific TCP port used to handle the communication to the associated serial port. The RMC automatically detects the TCP port assigned on the XIO. In this example, the TCP port is 12000.

Figure 4-73: XMV Interface assigned to XIO port – Default Application settings



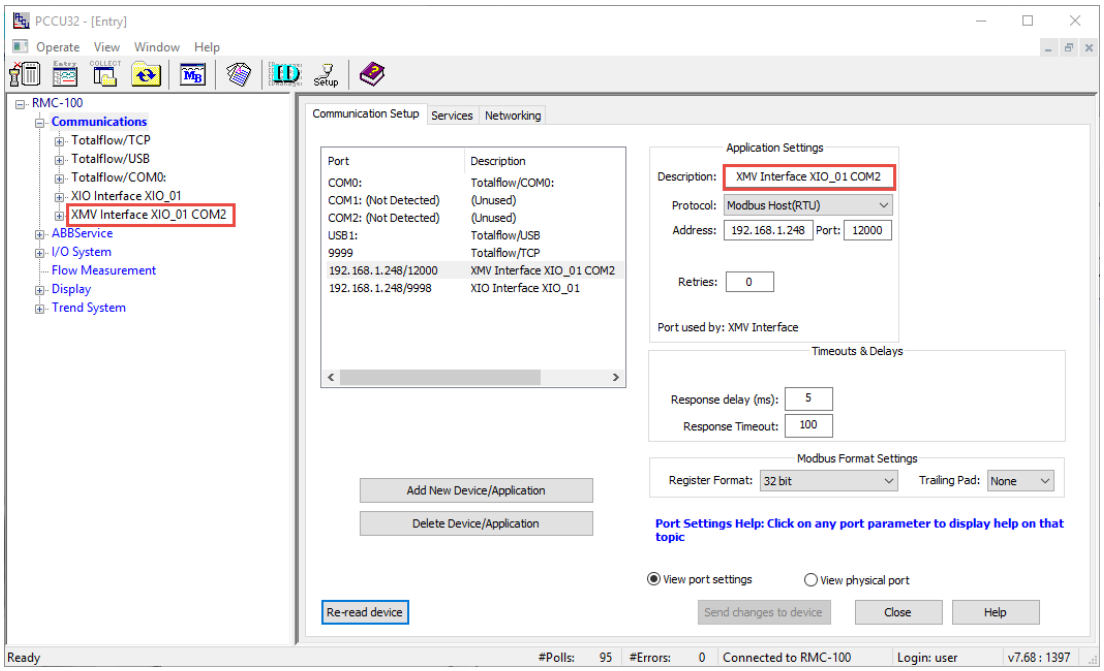
8. Verify Application settings and their default configuration (Figure 4-74)
9. Under the Application settings section, type a unique description. A unique description that identifies the communication application, associated XIO, and specific COM port helps identify the port when multiple applications are added.

Figure 4-74: XMV Interface assigned to XIO port – User-defined application description



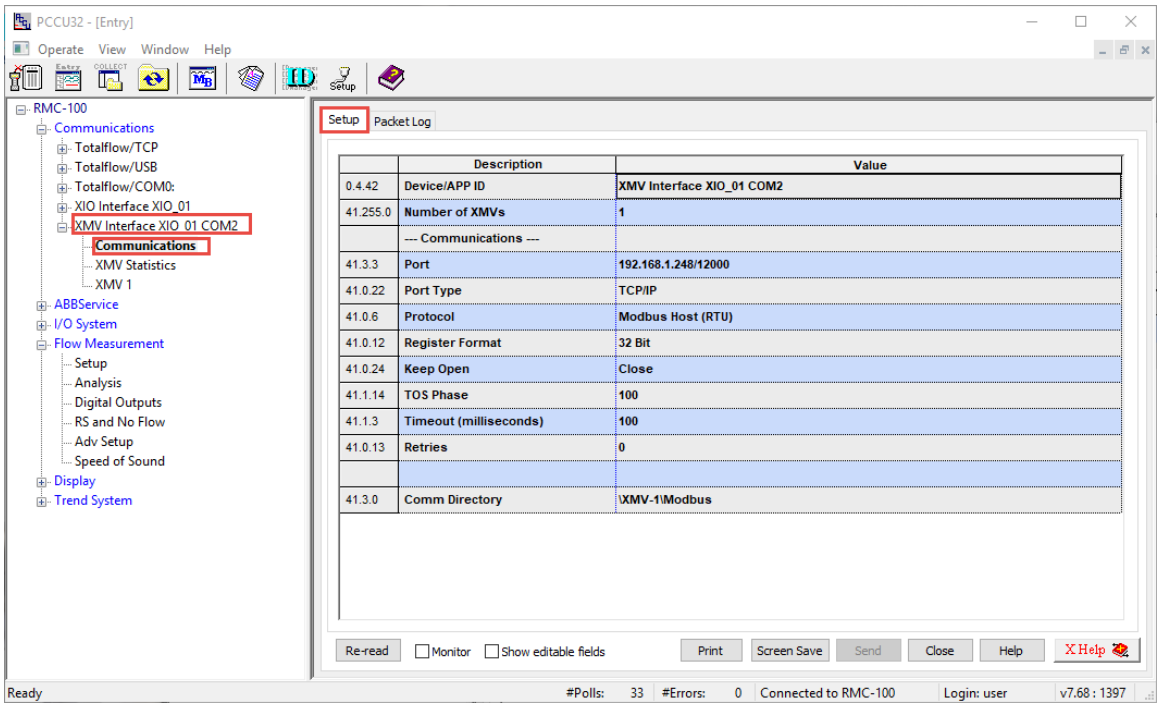
10. Click **Send changes to device**. The description of the port reflects the user-given name under the Application Settings section. This name is also displayed on the navigation tree. In this example, the XMV interface user-defined name identifies the XIO_01 and the port COM2. Note that additional configuration parameters display on the Communication Setup screen: The Retries field under Application Settings, Timeout & Delays, Modbus Format settings.

Figure 4-75: XMV Interface on RMC navigation tree (with user-defined name)



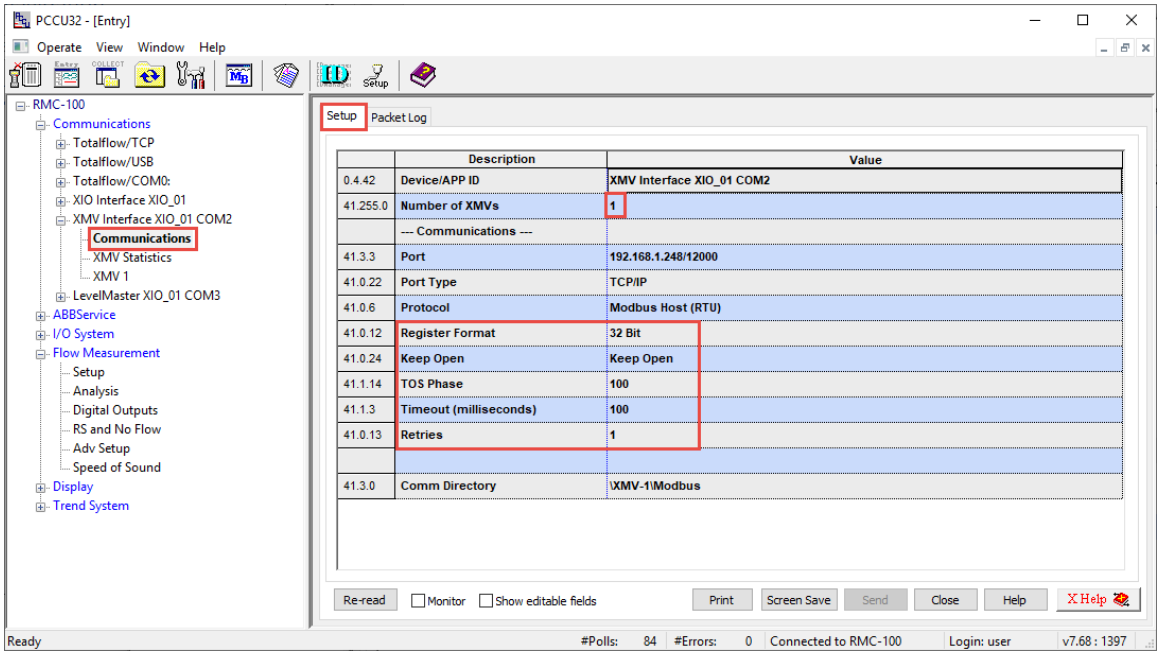
11. Configure application, communication or format parameters in this screen or from the application-specific screens in the next steps.
12. Configure the communication application (Figure 4-77):
    a. On the navigation tree, select the application instance and then **Communications**. The Setup tab displays.

Figure 4-76: XMV Interface Communications Setup with assigned XIO and COM port



b. Configure the number of XMVs (if more than 1). When multiple XMVs connect to the port, each of the XMVs must display on the navigation tree for individual configuration and management.
c. Verify that the Port, Port Type and Protocol parameters reflect the values selected when the application was added in the Communication Setup screen.
d. Configure or fine tune the communications parameters (if you configured them in step 11, skip this step). The values for parameters must match those configured on the XIO COM port where applicable.
e. If the Keep Open value field is: Close, select the field and select **Keep Open**.

Figure 4-77: XMV Interface communication parameters (user-defined)



13. Click **Send**.
14. Configure the XMV(s) next.

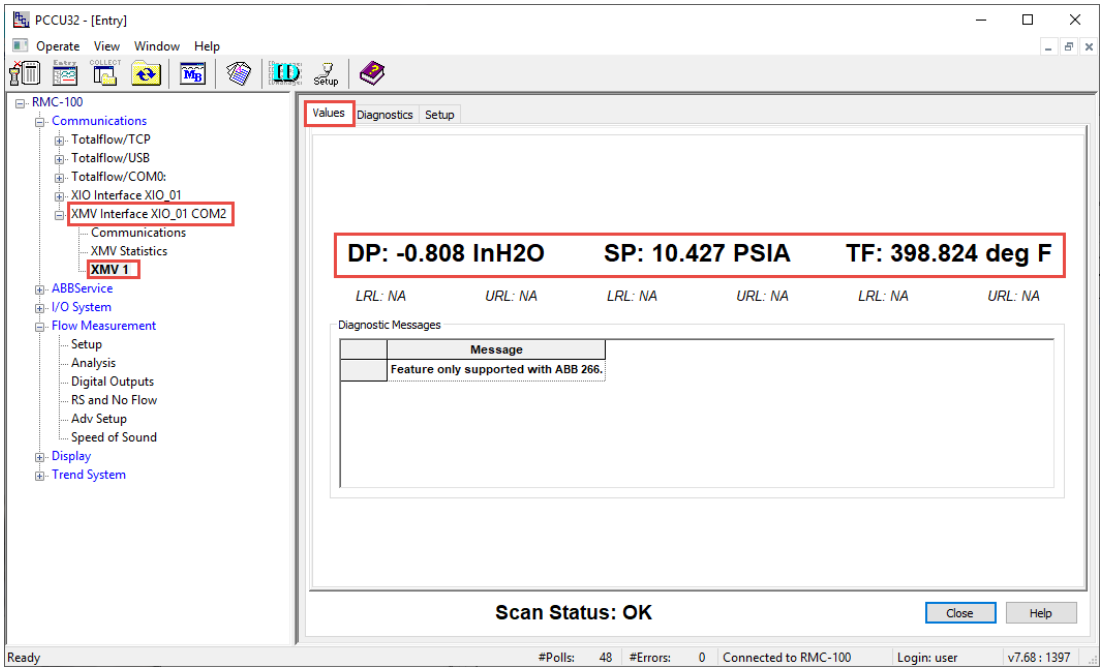
4.8.3 Configure the peripheral

For ABB Totalflow peripherals, the controllers or flow computers may support peripheral configuration options within the applications assigned to those peripherals. In this example, the XMV Interface application on the RMC supports the XMV configuration of the multivariable connected to the XIO COM port. Configure the peripheral from the controller, if available. If the controller does not support the peripheral, configure from the peripheral HMI. For third-party peripherals, consult vendor documentation. For additional details and troubleshooting tips for the XMV, see the XMV User Manual.

To configure the XMV:

1. On navigation tree, select the XMV to configure. The Values tab displays. No values display until the XMV configuration is complete.
2. Select the **Setup** tab.
3. Configure XMV parameters:
   a. Under XMV Displays, if Scroll Displays is enabled, change to Disabled.
   b. Click **Send**. This activates parameter fields for configuration.
   c. Configure the required parameters.
   d. Select **Enable** in the Scan drop-down list.
   e. Click **Send**.
   f. Verify that the Set Status displays OK.
4. Select the **Values** tab.
5. Verify that the XMV measurement values (DP, SP, TF) display and that the message "Scan Status: OK" displays.

Figure 4-78: Verify RMC receives remote peripheral measurement values

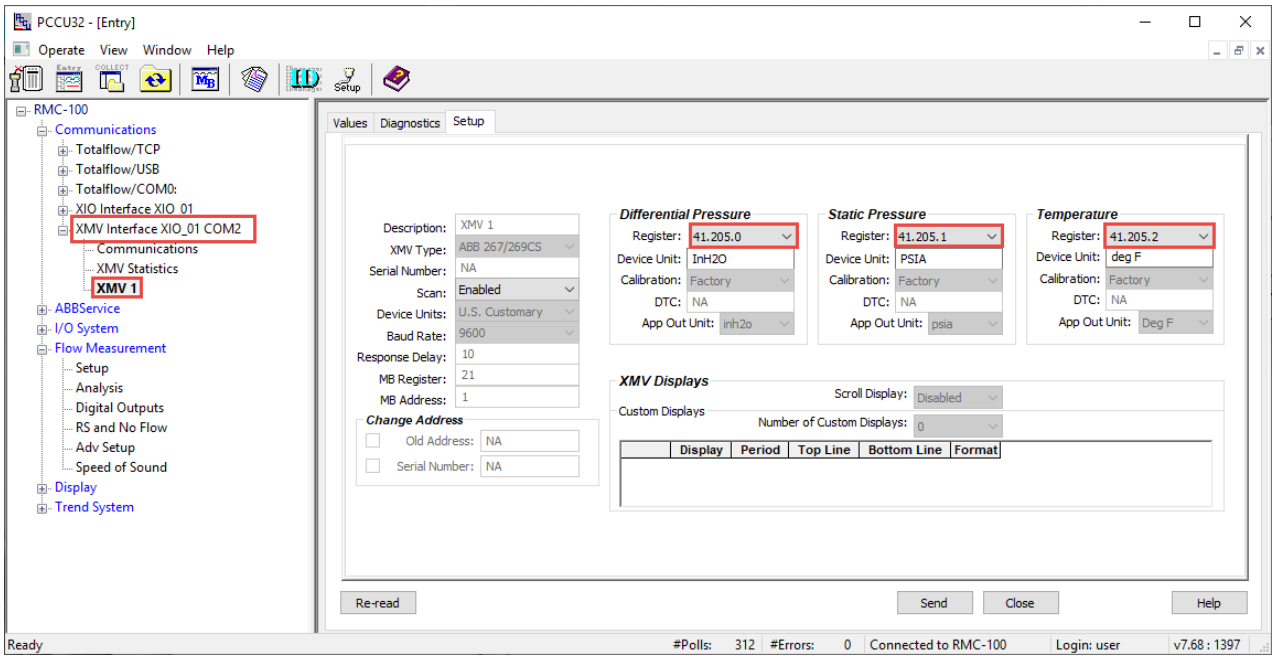


4.8.4 Configure measurement applications to use XIO values

To configure measurement applications with the remote XMV measurement values:

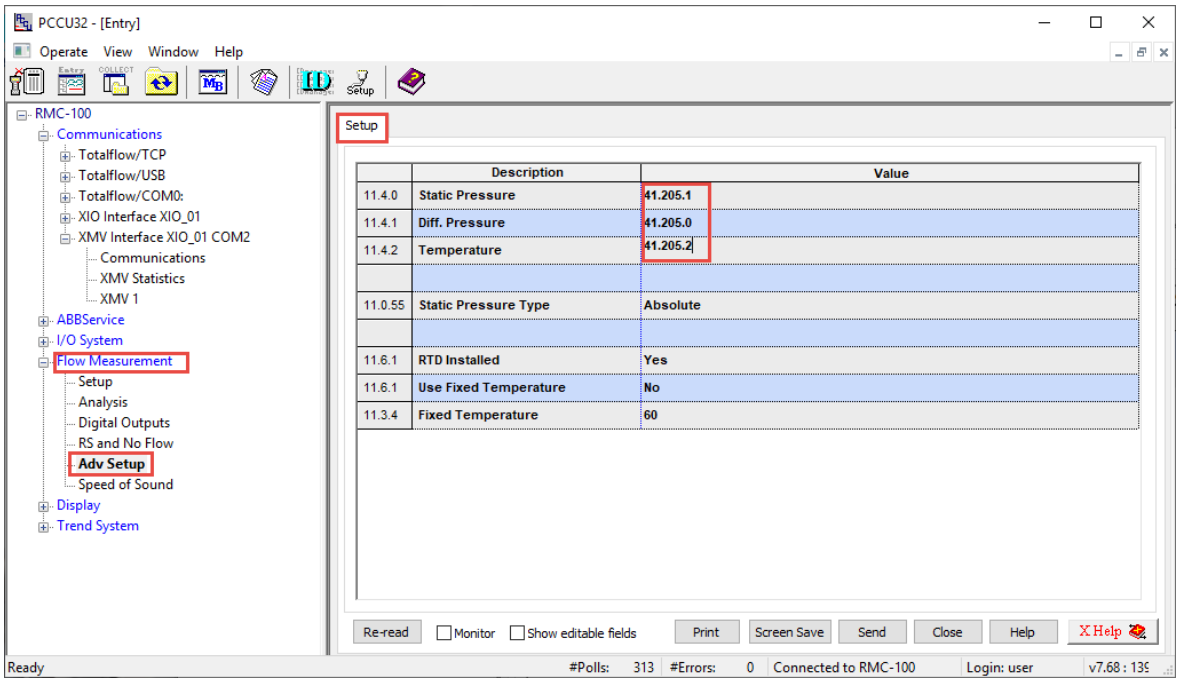
1. Obtain register values used by the RMC communication application. In this example, the XMV application stores the remote peripheral values in local RMC registers (Figure 4-79).
2. For multiple XMVs, select each XMV and obtain the specific registers from each respective Setup tab.

Figure 4-79: RMC application registers storing remote peripheral measurement values



3. On the navigation tree, expand the desired measurement application instance, and then select **Adv Setup** (Figure 4-80). The Setup screen displays. In this example the instance: **Flow Measurement** is an AGA3 Gas measurement instance.
4. Configure register values for the measured variables. In this example, the register values of XMV1 are used.

Figure 4-80: Configure measurement value registers for measurement application



5. Click **Send**. The measurement application instance can use the remote peripheral values in the calculations as required.

IMPORTANT NOTE: Configure other applications as required. Application configuration details are beyond the scope of this manual. Application-specific topics are available on each application screen. Click **Help** on the for specific topics.

4.9 Configure the I/O Interface for TFIO module support

The XIO supports I/O expansion with TFIO modules. This section provides steps to connect the TFIO modules and to add and configure the I/O Interface application. The I/O Interface application manages the communication with the modules.

IMPORTANT NOTE: For additional details supporting TFIO modules, see the link to the I/O Interface Application Guide listed in Additional information, or click **Help** on any of the I/O Interface screens in PCCU for specific configuration information.

4.9.1 Connect the TFIO modules to the XIO

IMPORTANT NOTE: The TFIO port on the XIO supplies power to the modules. The port is always on when the XIO is powered. Plan connection or removal of the TFIO modules and wired connectors based on your site requirements:

- If the installation area is potentially explosive, remove power to the XIO before module insertion/removal.
- If the installation area is not potentially explosive, it is not necessary to remove power from the XIO. Connect modules and proceed to section 4.9.2 Add and export the I/O Interface application.

The TFIO modules are hot-pluggable and can be removed or detached when the XIO is powered. However certain locations and conditions may require powering off the XIO before TFIO module insertion or removal.

IMPORTANT NOTE: The Valve Control TFIO module is not currently supported by the XIO. Contact ABB technical support for additional information.

DANGER – Serious damage to health / risk to life. Do not perform any wiring or removal/insertion of modules unless it is known that a potentially explosive atmosphere condition does not exist.

These instructions do not address the requirements for installations in potentially explosive atmospheres.

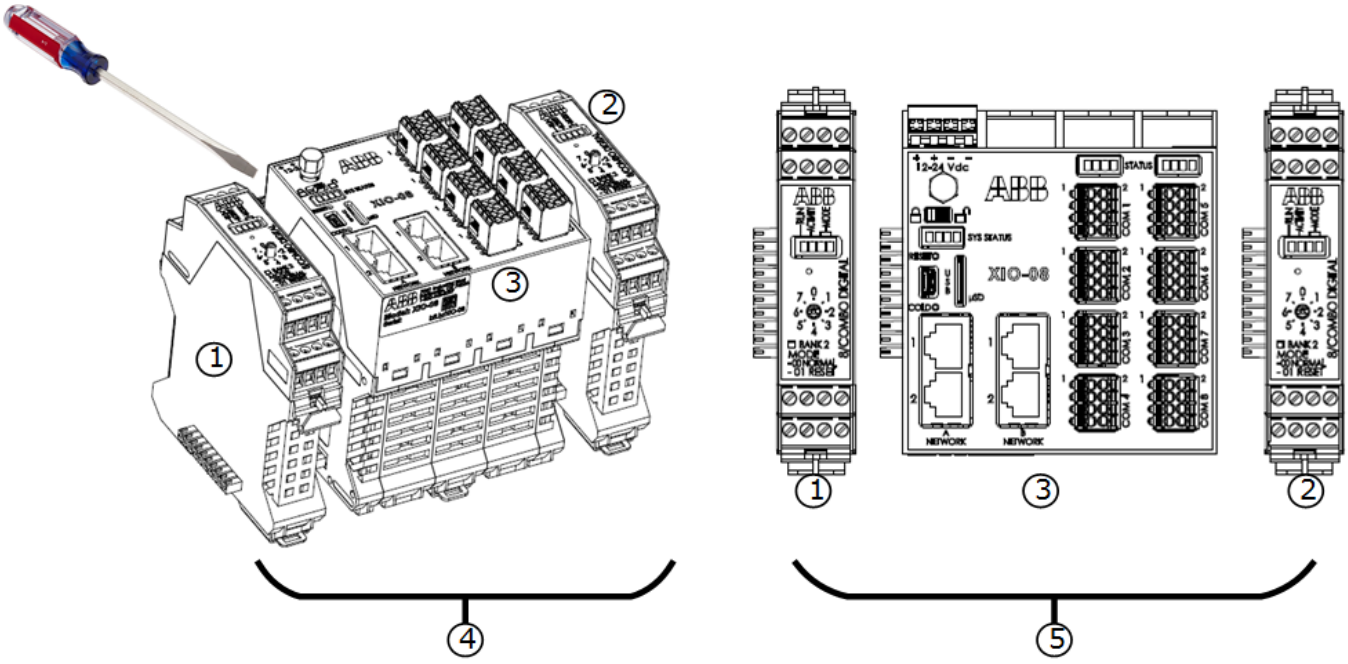
Wiring between the XIO, TFIO modules and field equipment must meet the requirements for installation in accordance with the local and national electrical codes.

IMPORTANT NOTE: This procedure assumes that the XIO power and TFIO I/O modular connectors have been correctly wired. The power and I/O connectors can be attached or removed without removal of wiring. Always remove the wired connectors attached to the TFIO modules prior to insertion or removal on the XIO.

To connect modules:

1. Remove the power connector from the XIO.
2. Remove wired connectors from the TFIO(s).
3. Connect the TFIO module or module set to the TFIO connector on the side of the XIO.

Figure 4-81: TFIO to XIO connections



Legend: TFIO to XIO connections

ID	Name	ID	Name
1	Side of TFIO	4	Side view of connections
2	Face of TFIO	5	Face view of connections
3	XIO		

IMPORTANT NOTE: To remove TFIO modules, insert a small, slotted screwdriver between the connector and the housing and gently pry the module away from the XIO.

4. Attach I/O wired connectors to the TFIO(s).
5. Reconnect power to the XIO.
6. Wait for the XIO to reinitialize.
7. Proceed to configure the I/O Interface application next.

4.9.2 Add and export the I/O Interface application

The I/O Interface application, which handles communication with TFIO modules, may not be already added or enabled from the factory.

The I/O Interface application is required, whether the TFIO modules are controlled locally by an XIO application or remotely by an RMC application.

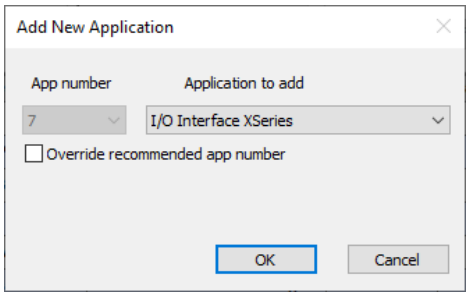
This procedure adds the I/O Interface on the XIO and sets it to export. Export of the I/O Interface is required when the XIO TFIO modules are controlled by remote applications. Exporting the I/O Interface allows control and management of the TFIO modules from the RMC. If not exported when required, the XIO may issue an alarm.

IMPORTANT NOTE: It is assumed that the majority of installed XIOs will be used to expand the I/O or serial capability of an RMC, and therefore TFIO modules will be controlled remotely. In some cases, however, the XIO may be used as a standalone controller and the TFIO modules would be driven locally by XIO applications. In this case, the export of the I/O interface is not required. For local control, the Enable Watchdog on an XIO must be set to **Module Control** mode.

To add the I/O Interface application and configure for export:

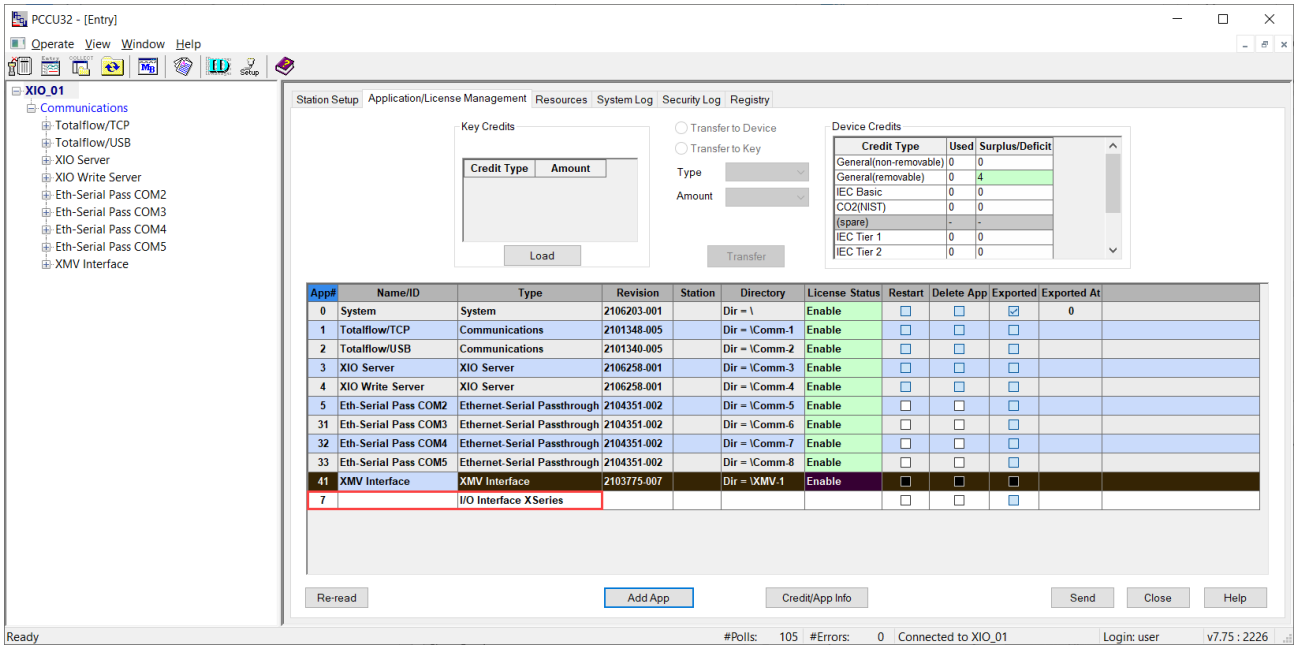
1. Connect with the XIO on PCCU Entry mode.
2. On the navigation tree, select the Station ID (XIO ID) and then the **Application/License Management** tab.
3. Click **Add App**.
4. Select **I/O Interface XSeries** from the Application to add drop-down list.

Figure 4-82: Add New Application: I/O Interface XSeries



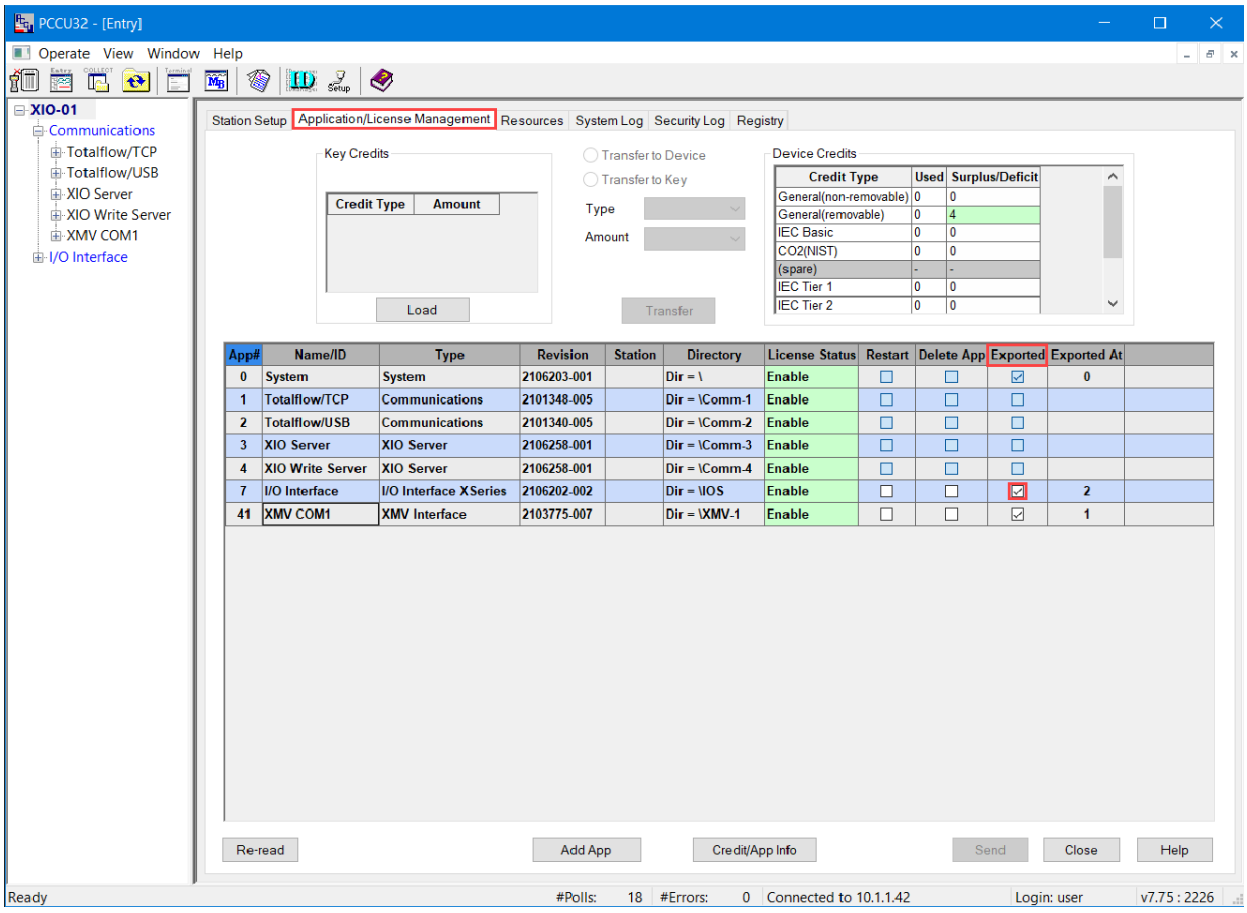
5. Click **OK**. The application displays in the last row of the application table (Figure 4-83).

Figure 4-83: I/O Interface in the XIO application table



6. Click **Send**. Additional I/O Interface application attributes display in the table. Note that the application may display in a different row depending on the application slot number. The table organizes applications based on the slot number in ascending order. The navigation tree refreshes and displays the application.
7. Select the check box under the Exported column (Figure 4-84). The **Exported at** value next to the Export checkbox automatically displays. This is an index number for the application. Keep the default selected or select an unused number from the range: 1-15.

Figure 4-84: Export I/O Interface application



IMPORTANT NOTE: The index number an application is exported at affects register numbers for the XIO Interface application on the remote controller (RMC). If you change this number after the application has been added and configured, it changes its existing register numbers. Register number change for an application already in-service may disrupt operation.

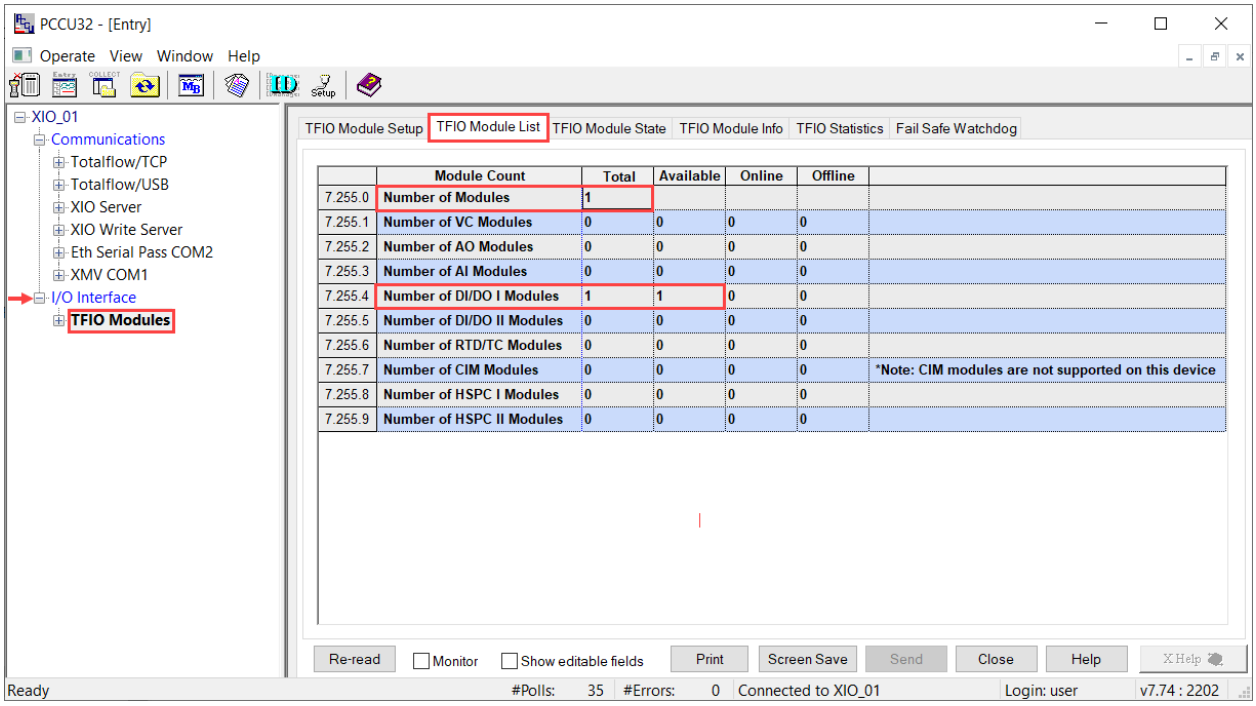
8. Click **Send**. The I/O Interface displays as an exported application in the application table. The application export index also displays.
9. Proceed to section 4.9.3 Verify TFIO module detection on XIO.

4.9.3 Verify TFIO module detection on XIO

To verify that the TFIO interface recognizes the connected modules:

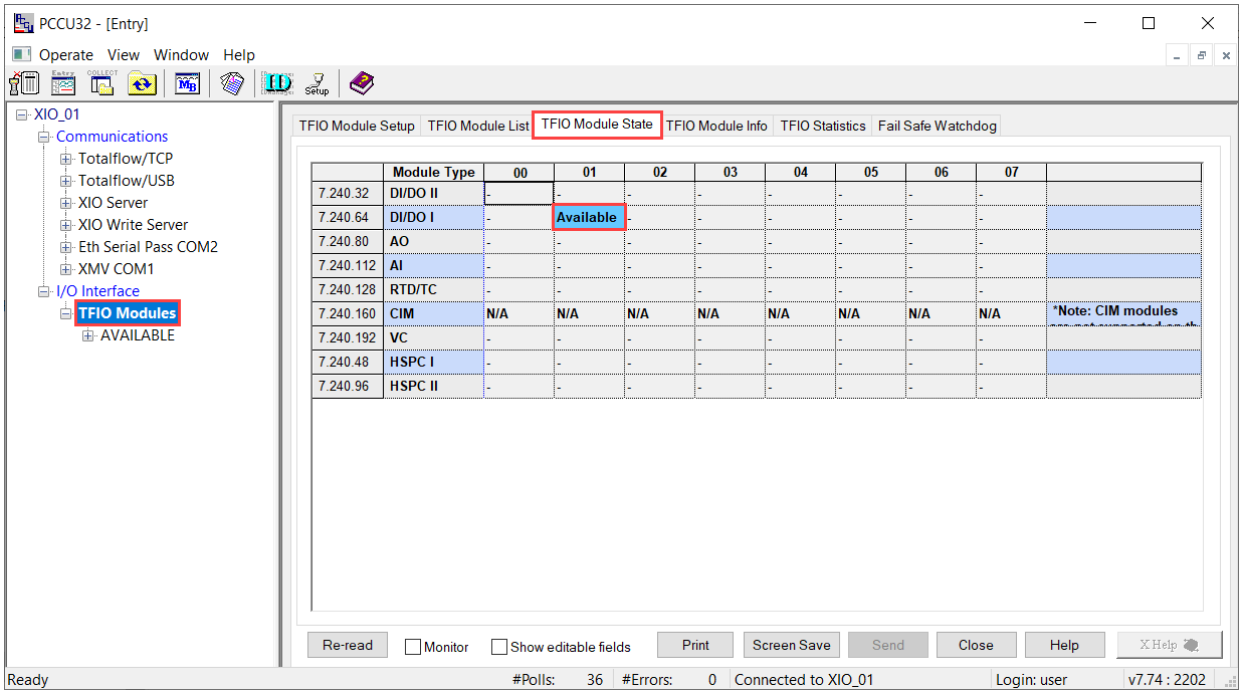
1. On the navigation tree, expand **I/O Interface**. Then select **TFIO Modules** (Figure 4-85).
2. Select the **TFIO Module List** tab.
3. Verify that the XIO detected the correct number and type of the connected module(s).

Figure 4-85: TFIO detection on the XIO – TFIO Module List tab



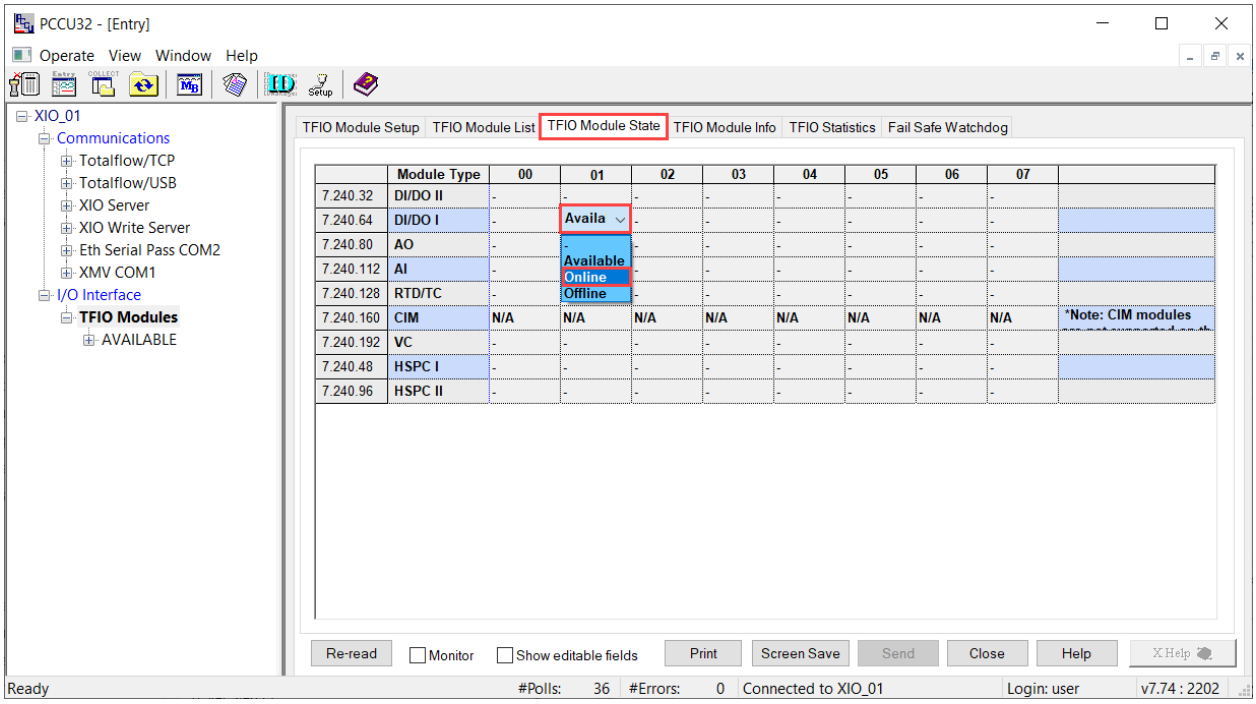
4. Select the **TFIO Module State** tab. The connected module displays the status: Available (blue) (Figure 4-86). This means that the XIO has detected the TFIO module in its communication bus, but the module is not ready for use yet.

Figure 4-86: TFIO Module State for new module - Available



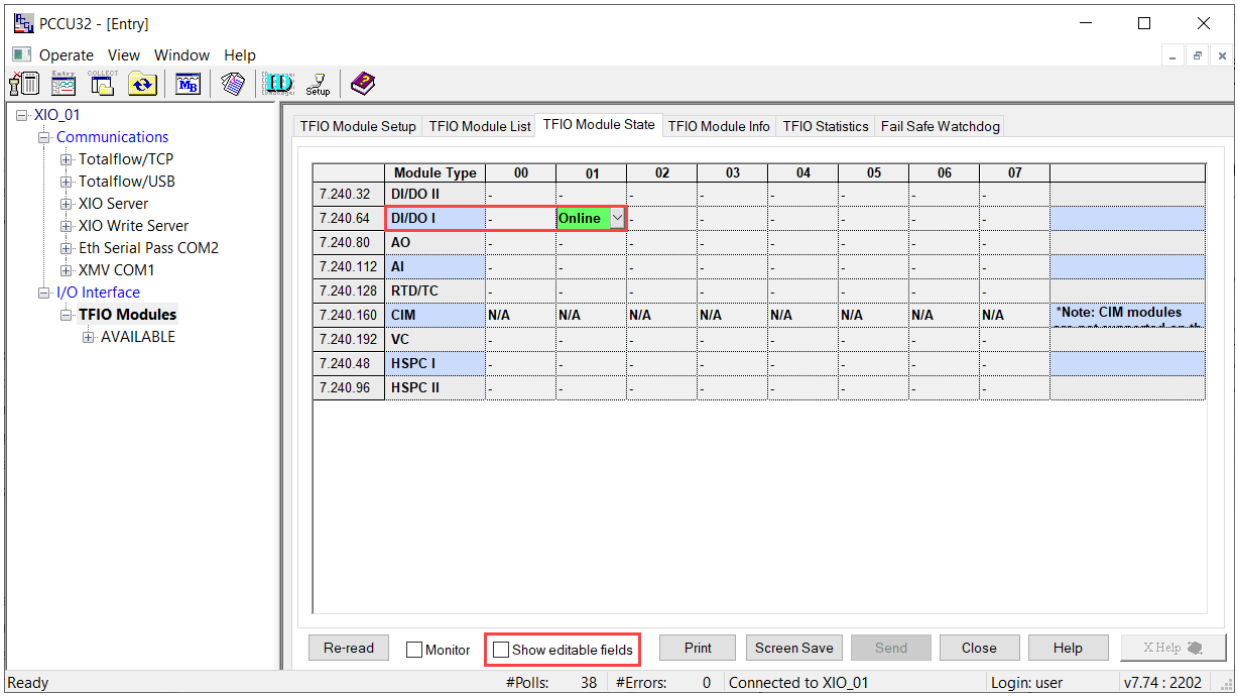
5. Set the TFIO module to **Online** (Figure 4-87) to enable the TFIO module for communication.

Figure 4-87: TFIO Module State – Select Online mode



6. Click **Send**. The State of the TFIO module displays: Online. Refresh the screen to see the state change to green. If color is not showing in the state field, clear **Show editable fields** at the bottom of the screen. Changing the module state to Online places the module in service. The module is ready for use.

Figure 4-88: TFIO Module State – Online mode



4.9.4 Clear the Fail Safe Watchdog alarm (remote TFIO control)

The XIO supports a watchdog function to define module output fail-safe states in case of XIO-remote controller Ethernet communication failure. The watchdog function is enabled for all modules from the factory. The watchdog is in an alarm state if:

- The I/O Interface on the XIO is not exported to the RMC
- The XIO-RMC connection has not been established or has failed
- The XIO needs a reset. The alarm may display during the first-time installation of the modules.

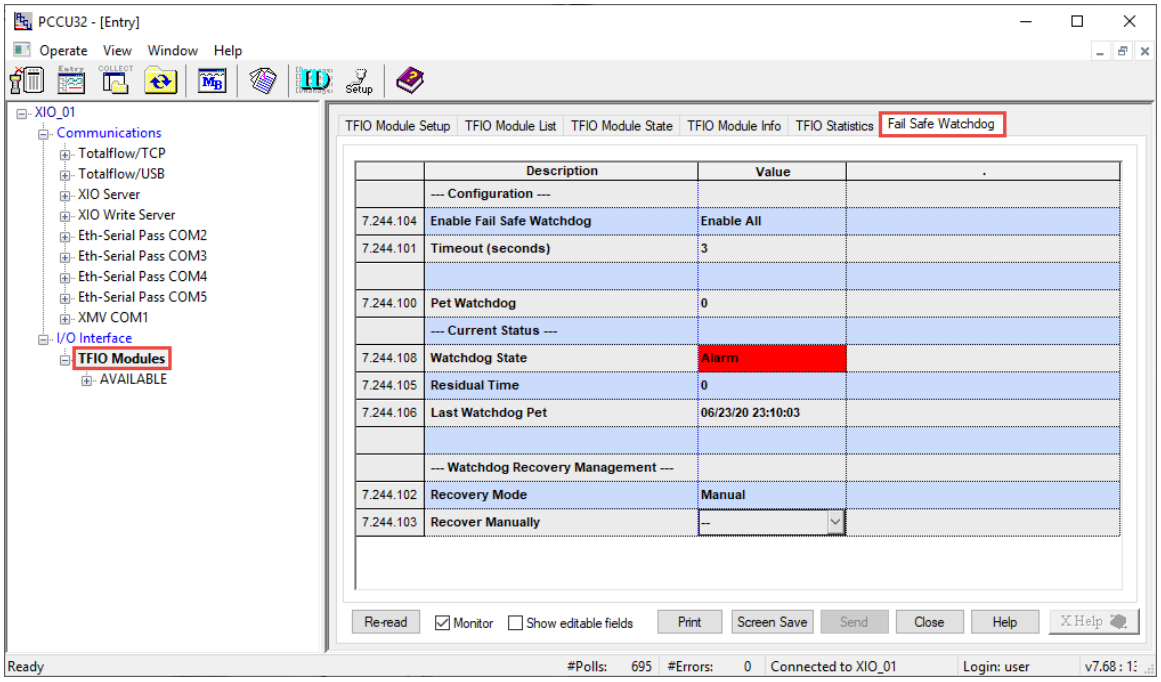
This procedure assumes the XIO is connected to an RMC and TFIO modules on the XIO are controlled by applications on the RMC. It clears the alarm after a module is first connected to the XIO and is set to Online state.

To clear the watchdog alarm:

1. Select the **Fail Safe Watchdog** tab (Figure 4-89). Locate the Watchdog State parameter and verify the state:
   a. If the state displays Normal (green), the XIO is successfully communicating with the remote controller and the TFIO is ready for use (successful network connectivity).
   b. If the state displays Alarm (red), the XIO is not successfully communicating with the remote controller or needs a reset.

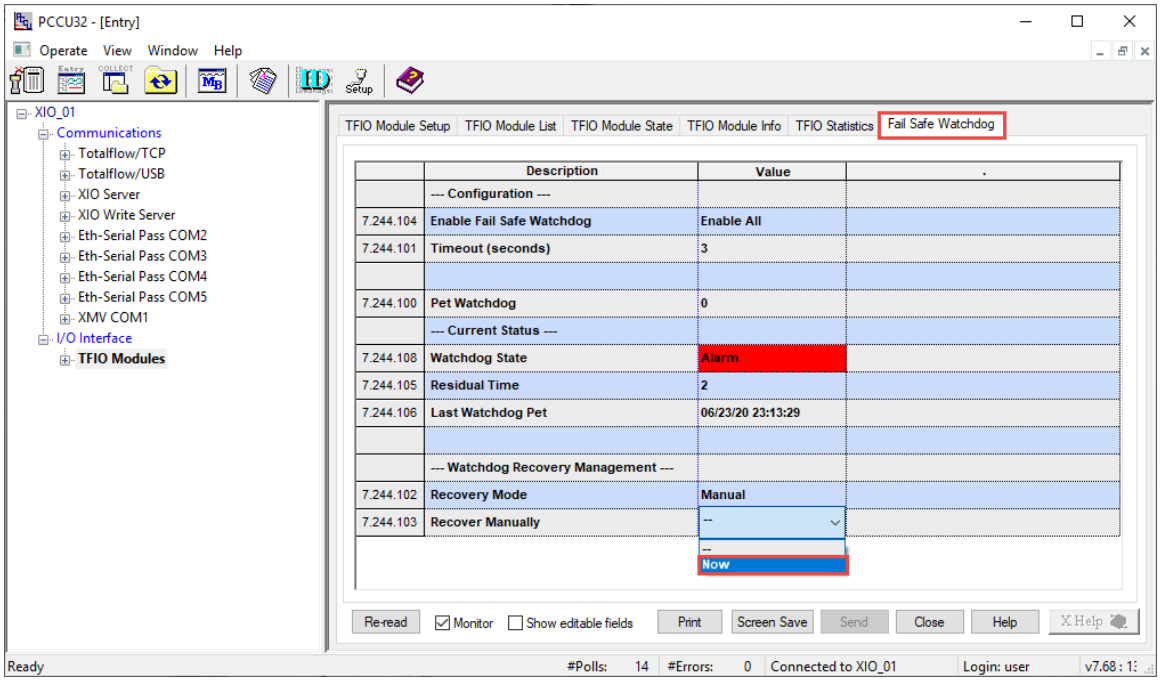
IMPORTANT NOTE: The Fail Safe Watchdog is enabled for all TFIO modules by default. Connecting a TFIO module without exporting the I/O Interface to the RMC sets the Watchdog state to alarm. The 3rd and 4th Sys Status LEDs (located below the XIO security switch) blink to indicate this condition. The Watchdog state remains in alarm until the I/O Interface app is exported while the Watchdog is enabled.

Figure 4-89: Fail Safe Watchdog tab – Watchdog on Alarm State



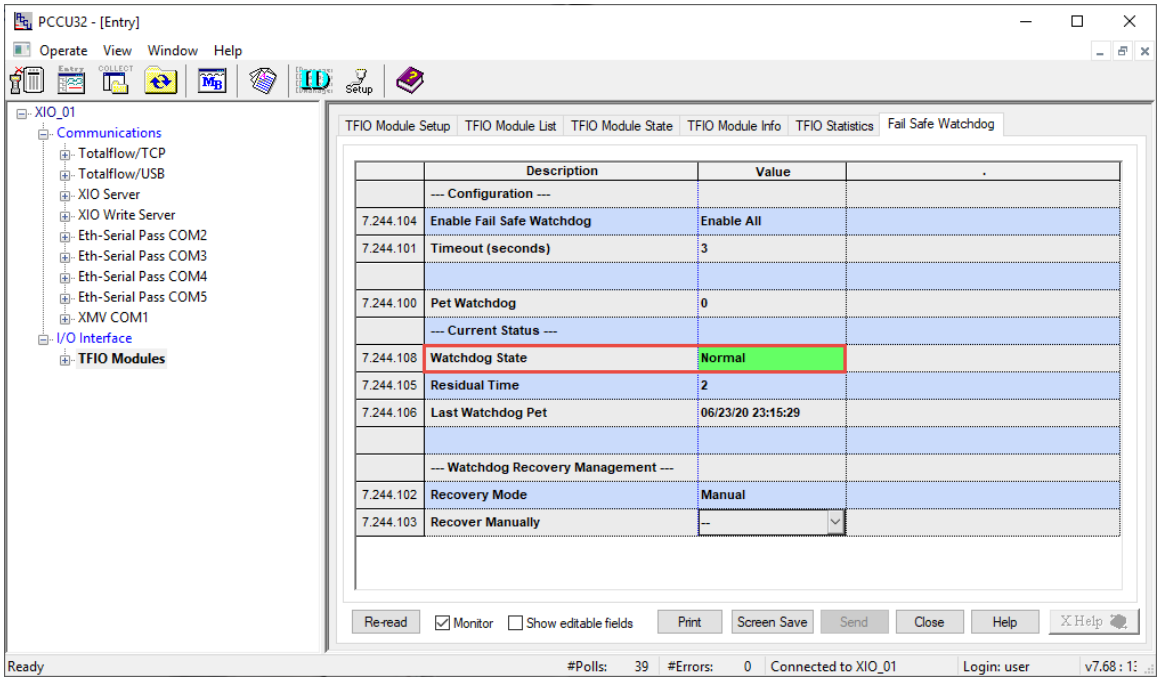
2. To clear the alarm:
   a. Select **Now** on the Recover Manually value field (Figure 4-90).

Figure 4-90: Recover Watchdog Manually



b. Click **Send**.
c. Verify that the Watchdog State displays Normal (green).

Figure 4-91: Fail Safe Watchdog tab – Watchdog in Normal state (Alarm cleared)



3. Verify that the SYS STATUS 3rd and 4th LEDs stop blinking and remain lit. This indicates that the XIO and remote controller are communicating and therefore the RMC applications can control the TFIO modules as necessary.
4. Click **Help** to display the TFIO Module List topic for more information.

4.9.5 Clear the Fail Safe Watchdog alarm (local TFIO control)

If the XIO is used as a standalone remote controller, you can clear the Ethernet Fail Safe Watchdog alarm by setting the XIO Fail Safe Watchdog function to **Module Control** or **Disable All**. Follow one of the two procedures in this section if the XIO is used as a standalone controller. That is, TFIO module outputs are controlled by local XIO applications only.

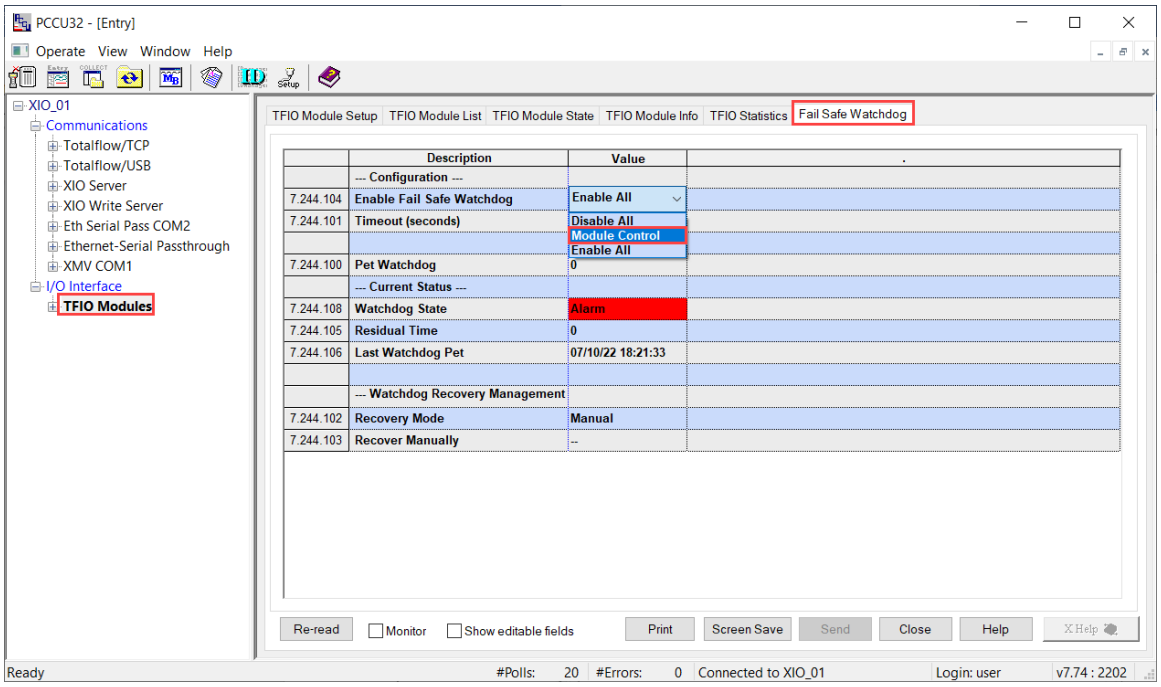
4.9.5.1 Set the Fail Safe Watchdog to Module Control

The Module Control mode allows setting the local watchdog function at a DO level. The watchdog can be enabled or disabled for each module output. Make sure that the I/O Interface application is not exported.

To set the watchdog to module control and clear the alarm state:

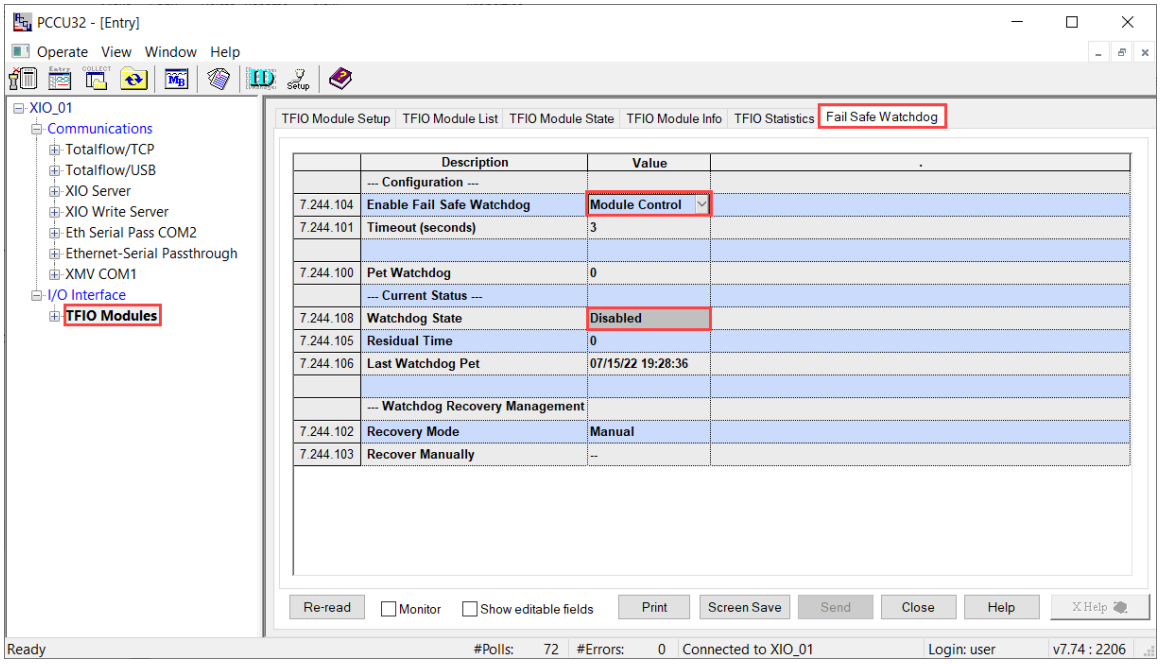
1. Select the **Enable Fail Safe Watchdog** drop-down list and select **Module Control**.

Figure 4-92: Set Fail Safe Watchdog to Module Control mode



2. Click **Send**.
3. Clear the **Show editable fields** checkbox.
4. Verify that the Watchdog state is not in Alarm state. The parameter should display: **Disabled**.

Figure 4-93: Clear Watchdog State from Alarm to Disabled (Module Control mode)



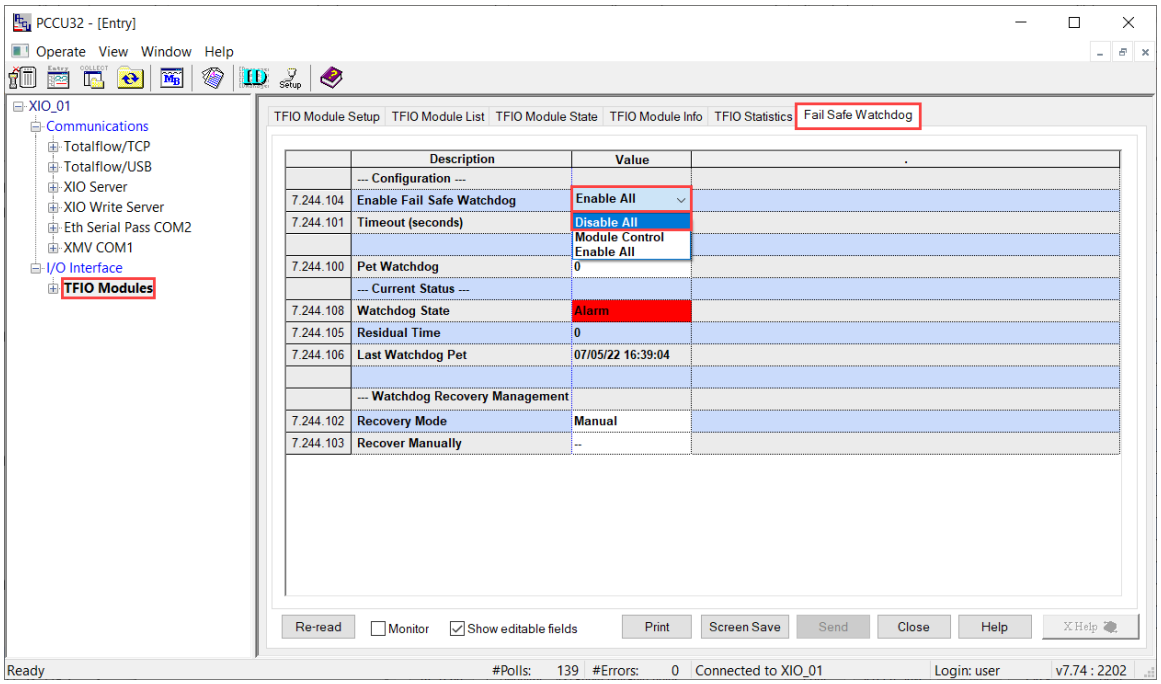
4.9.5.2 Disable the Fail Safe Watchdog

If you do not wish to enable the Fail Safe Watchdog function, disable it for all outputs on the modules.

To disable the watchdog and clear the alarm state:

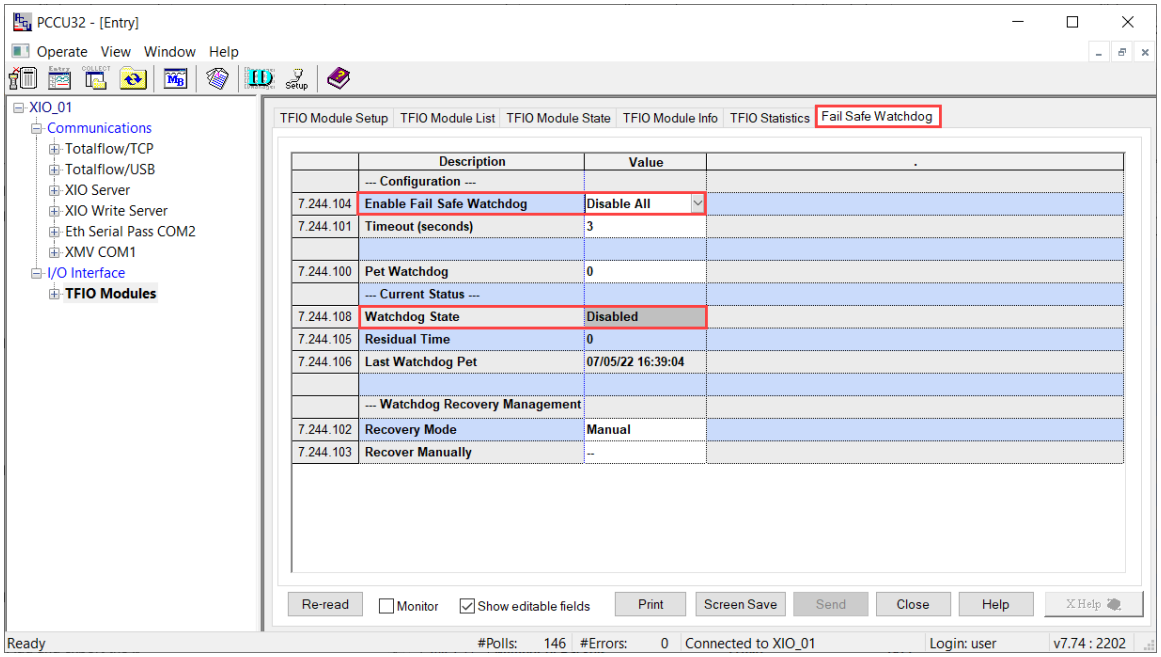
1. Select the **Enable Fail Safe Watchdog** drop-down list and select **Disabled**.

Figure 4-94: Disable Fail Safe Watchdog on XIO TFIO modules



2. Click **Send**.
3. Clear the **Show editable fields** checkbox.
4. Verify that the Watchdog state is not in Alarm state. The parameter should display: **Disable All**.

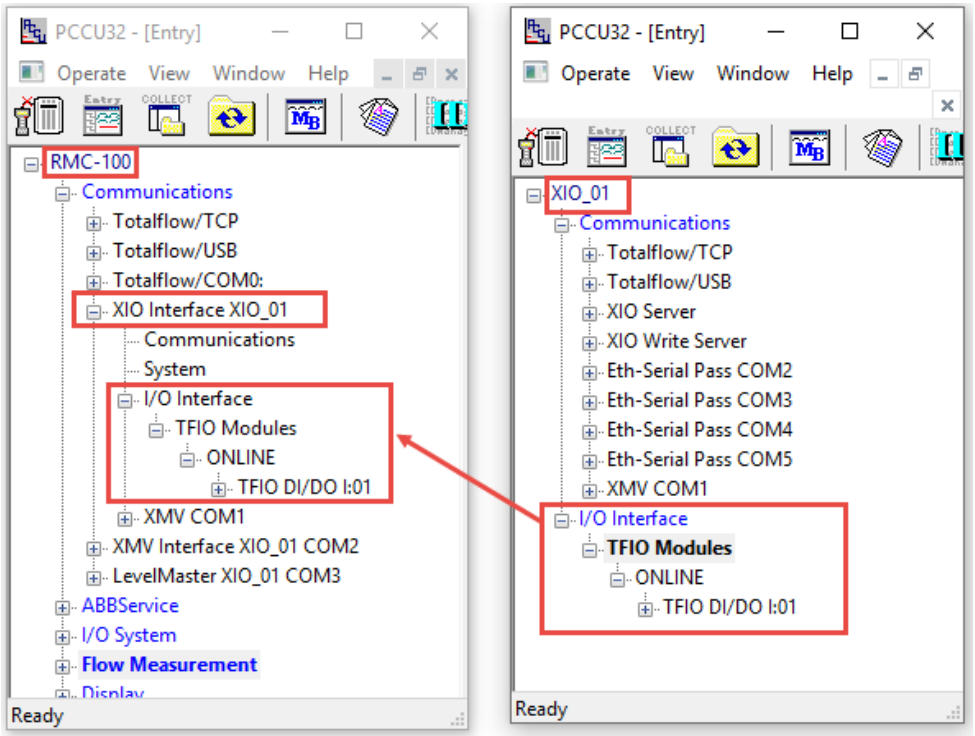
Figure 4-95: Clear Watchdog State from Alarm to Disabled (Disable All mode)



4.9.6 Verify I/O interface application export on RMC

Refresh the navigation trees (Figure 4-96) to verify that the I/O Interface application displays (XIO tree view on the right). The application should also display on the navigation tree of the RMC, under the XIO Interface (left screen). The views on the tree are identical and show the detected TFIO module.

Figure 4-96: XIO I/O Interface application exported to RMC – Remote TFIO Module detected



5 Calibration

Calibration procedures vary depending on application scenarios. The XIO supports the same calibration utility as other Totalflow devices.

Calibration depends on where the involved applications are in operation and the communication method between the XIO and the remote controller. The table below describes where the calibration must be performed from per application scenario. The table also details where the calibration files are stored.

IMPORTANT NOTE: I/O calibration (shown in the last row) can be performed from either the XIO or the RMC. When calibration is done from the XIO, there is a pop-up message to notify the user that the IO point they are calibrating may be used in a tube and if that is the case, calibration should be done from the RMC instead. Regardless of where the calibration takes place, I/O calibration files are stored on the XIO. The calibration method is the same from XIO or RMC.

Table 5-1: Calibration per application scenario

Application	Physical Location	Application Location	Application Exported	Communication Method	Calibration File Location	Calibration from device
Comm (XMV Interface)	XIO	RMC	Yes	Ethernet-Serial Passthrough	RMC	RMC
Comm (XMV Interface)	XIO	XIO	Yes	XIO Interface	XIO	RMC
Comm (XMV Interface)	XIO	XIO	No	Local serial	XIO	XIO
Comm (XMV Interface)	RMC	RMC	No	Local serial	RMC	RMC
I/O System (TFIOs)	XIO	XIO	Yes	XIO Interface	XIO	RMC/XIO

6 Basic troubleshooting

The following sections describe issues that may arise during basic installation. For support, call the ABB main office number on the last page of this manual.
Before calling:

- Take note of the model and serial number. The serial number is on a label affixed to the bottom of the unit.
- Prepare a detailed description of the problem for the Technical Support representative.
- Prepare a written description of the problem.
- Take note of any alarms or messages as they appear.
- Know the software version and optional part numbers.

IMPORTANT NOTE: For additional details on the XIO Interface, Ethernet-Serial Passthrough or IO Interface, see links to application guides listed in Additional information.

6.1 Use LED states for troubleshooting

The XIO LEDs provide quick visual indication of the health of the system during power on or after power is applied to the XIO. The XIO has 3 sets of LEDs:

- SYS STATUS LEDs: Indicate power to the XIO and status of connection with the host controller
- COM Port group STATUS LEDs: 4 LEDs to indicate COM port group status (XIO-08 has two 4-port groups, XIO-04 has one 4-port group)
- Individual COM port LEDs: 4 LEDs for each COM port (XIO-08 and XIO-04 only) located at the left of the port.

6.1.1 SYS STATUS LEDs

During power up, the SYS STATUS LEDs provide the status of the power up sequence and indicate when the different embedded software components are being loaded or started on the XIO. Observe the LEDs during power up (see Table 6-1) to ensure the sequence is completed.

Table 6-1: SYS STATUS LED States during power up*

LED	ON	OFF	Blinking
1	Power detected	No power detected	Not applicable
2	Completed Bootloader loading	No Power detected	Loading Bootloader
3	Completed OS loading	No Power detected	Loading OS
4	Completed Application Startup	No Power detected	Application startup in progress

* See Figure 3-6 for an illustration of the power on sequence.

After the XIO power up sequence completes, the SYS STATUS LEDs can indicate the status of the connection of the XIO to the host controller if connection monitoring is enabled. Table 6-2 shows how LED 3 and 4 are used to indicate connection health.

Table 6-2: SYS STATUS LED states after power on sequence completes

LED	ON	OFF	Blinking
1	Power on	No power detected	Not applicable
2	Power on	No power detected	Not applicable
3	– If the XIO Fail Safe Watchdog is enabled, it indicates that the Host Controller-XIO connection is successfully established. – If the XIO Fail Safe Watchdog is disabled, the Host Controller-XIO connection is not monitored. Please note that a lit LED does not indicate a successful connection.	No power detected	Indicates that the host controller-XIO connection has failed. This condition is detected and indicated only when the XIO Fail Safe Watchdog is enabled.
4	– If the XIO Fail Safe Watchdog is enabled, it indicates that the Host Controller-XIO connection is successfully established. – If the XIO Fail Safe Watchdog is disabled, the Host Controller-XIO connection is not monitored. Please note that a lit LED does not indicate a successful connection.	No power detected	Indicates that the host controller-XIO connection has failed. This condition is detected and indicated only when the XIO Fail Safe Watchdog is enabled.

If the XIO I/O Interface is remotely controlled by a host controller (RMC), a successful XIO-remote controller connection is always required. The XIO Watchdog function is enabled by default to monitor this connection. LED 3 and 4 will indicate an alarm at first-time installation. See section 4.9.4 Clear the Fail Safe Watchdog alarm (remote TFIO control) and 4.9.5 Clear the Fail Safe Watchdog alarm (local TFIO control) to clear the alarm if necessary. If the XIO is running as a standalone system, then the watchdog must be disabled.

6.1.2 COM port LEDs

COM port LEDs provide the status of the COM port groups (a group of 4 COM ports, Table 6-3) or for each port individually (Table 6-4).

Correct operation of the COM groups is indicated by lit LEDs 1-3.

Table 6-3: COM port group STATUS LED states

LED	ON	OFF	Blinking
1	Port Group Power On	Port Group Power OFF (LED is OFF. No other LEDs should be ON)	Not applicable
2	Port Group Enabled	Port Group Disabled (LED is OFF. No Port LEDs should be ON)	Not applicable
3	Port Group Normal operation	Port Group Suspend Mode	Not applicable
4	Port Group Suspend Mode	Port Group Normal Operation	Not applicable

Each COM port has its own LEDs, four LEDs for each COM port (Table 6-4). Note that the LEDs are lit when the port is enabled. That is, the port is assigned to an application during configuration and initialized for communication.

At initial installation, the LEDs will be OFF. When the port is enabled and configured for operation, LED 1 and 2 turn on. When communication with the device attached to the COM port is established successfully, then LED 3 and 4 indicate activity as the port transmits or receives data.

Table 6-4: COM port status LED states

LED	ON	OFF
1	Port Enabled	Port Disabled
2	Port Power Output ON	Port Power Output OFF
3	Port TXD activity (port transmitting data)	No TXD activity (no data is being transmitted)
4	Port RXD activity (port receiving)	No RXD activity (no data is being received)

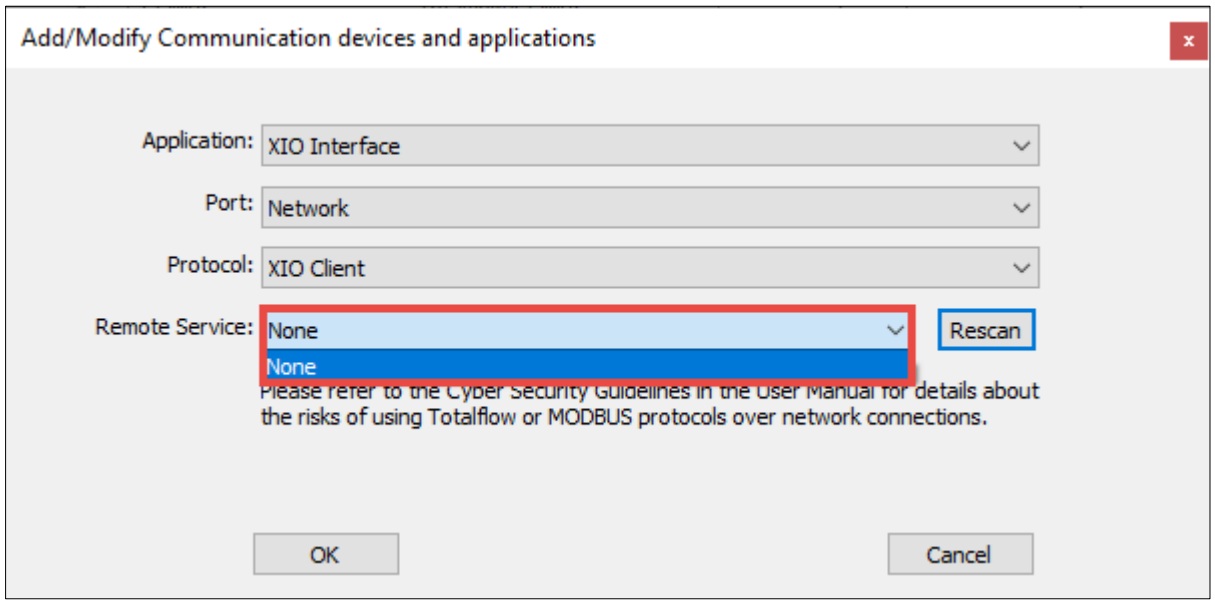
Section 4.7.1 Configure COM port for communication with ABB devices and section 4.8 Configure Ethernet-Serial Passthrough provide details on COM port setup. Monitor LEDs closely during port configuration to ensure COM ports are enabled and active. Assigning serial communication applications to the COM ports automatically enables the port.

6.2 RMC unable to detect or communicate with the XIO

The XIO advertises its services (XIO server or Ethernet-Serial Passthrough) on its network connection. Proper connections, and the correct configuration of every device on that network, ensure that the RMC detects the advertised services for each XIO and receives measurement data. The inability of the RMC to detect or communicate with the XIO can be due to many reasons. Communication failure can be determined from the RMC in different screens.

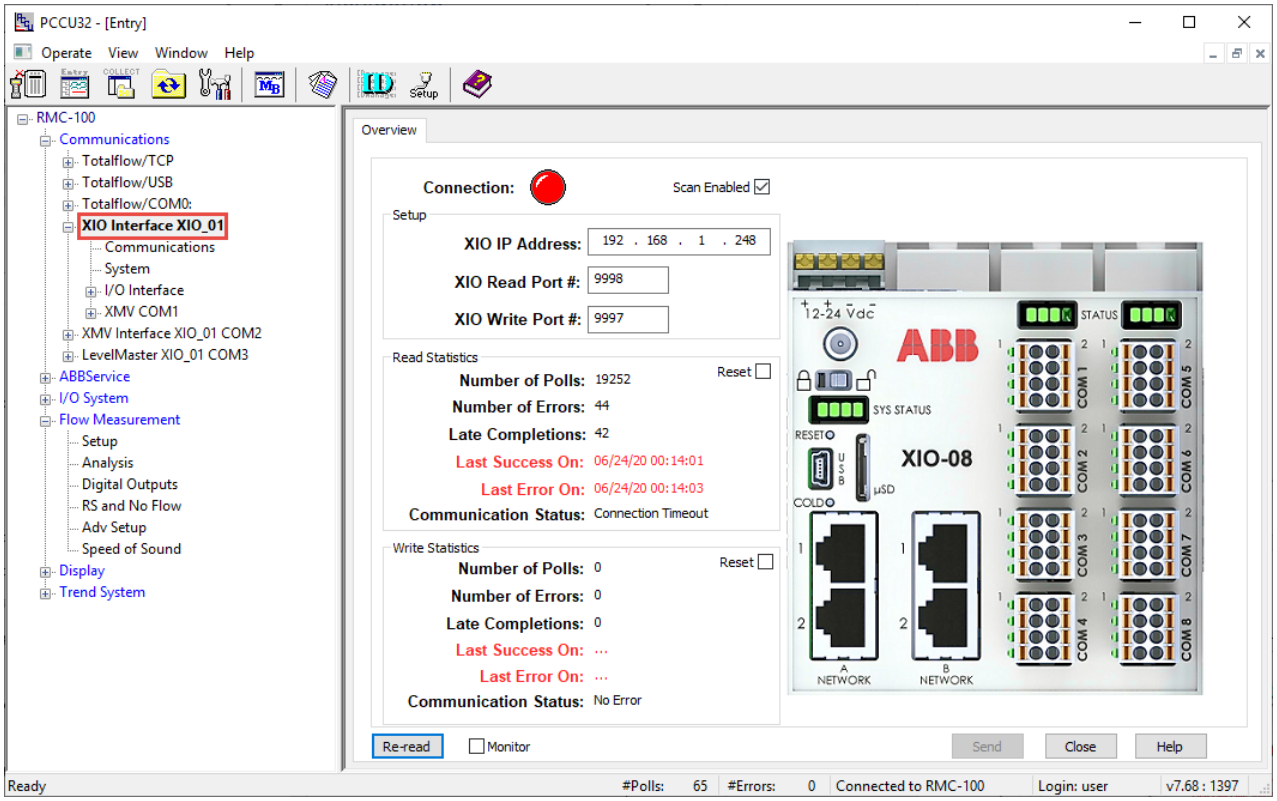
- Connectivity failure at initial setup prevents detection of the XIO when trying to activate and configure the XIO Interface application. The figure below shows no XIO in the Remote Service list. The Rescan function triggers the discovery of undetected XIOs. In single or multi-XIO installations:
  - If some XIOs display, but not others, verify the connection or configuration of the missing XIOs. Click **Rescan** and verify if the RMC detects new XIOs.
  - If no XIOs display at all, verify the RMC connection and configuration.

Figure 6-1: RMC unable to detect XIO



– Connectivity failure after an initially successful connection results from a change of connection status. The XIO Interface Overview screen displays information about the last successful communication polls in addition to the red indicator for connection loss.

Figure 6-2: XIO Interface Overview screen (connection failure)



6.2.1 Verify RMC-XIO connection (physical connection)

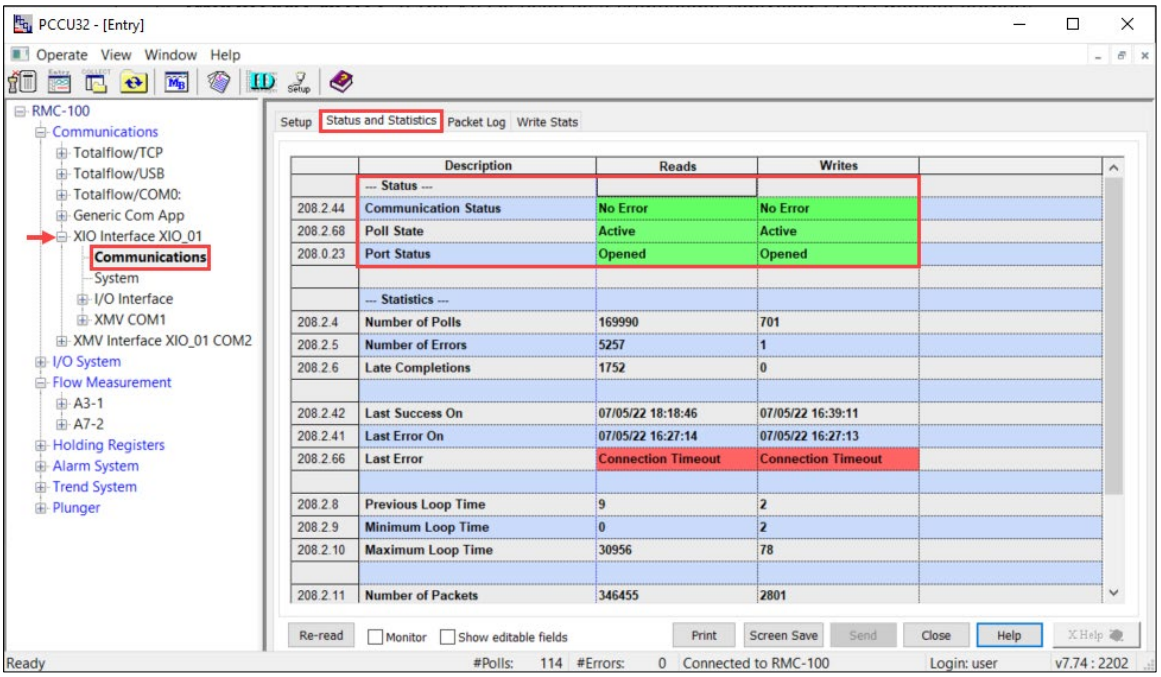
Depending on the connection scenario, the XIO may connect to the field network switch (star topology), to the RMC, or to another XIO (daisy chain). Loss of physical connection is detected and displayed on the XIO Interface Overview screen.

This procedure verifies if the RMC has successfully established a connection with the XIO. Verify connection status from the **Status and Statistics** tab. This procedure describes how to check connection status.

To verify that the RMC-XIO link is established:

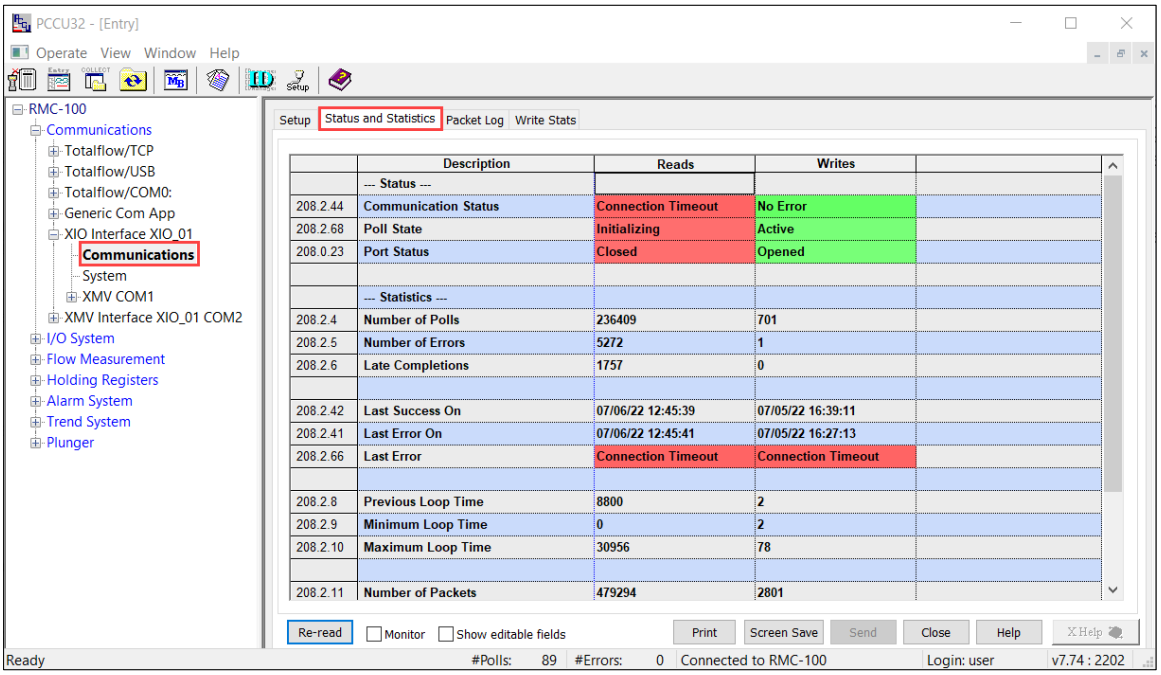
1. When physically close to the XIO, visually check the Ethernet ports LEDs. The Ethernet port LEDs should be lit.
2. From the RMC:
   a. On the navigation tree, expand the **XIO interface** and select **Communications**.
   b. Select the **Status and Statistics** tab (Figure 6-3).
   c. Verify Communication Status displays: No Error, for both reads and writes.
   d. Verify that the Poll State displays: Active, for reads. Note that the Poll State for writes may display: Inactive, during initial configuration. This does not indicate connection failure. An Inactive state indicates that RMC applications have not sent writes to the XIO yet. Reads are sent periodically. Writes are sent based on the applications and their programming.
   e. Verify that the Port Status is Opened for both reads and writes.

Figure 6-3: RMC-XIO connection successful



A broken connection, or one with excessive errors, displays communication status errors, poll state for reads constantly initializing but never reaching the Active state, and port status closed. Figure 6-4 shows the state of the status parameters when the connection is broken.

Figure 6-4: RMC-XIO Connection failure



If the connection status displays errors:

1. Ensure that the Ethernet cables and connectors for both the RMC and XIO are not damaged or broken. Verify that the cable connectors are firmly inserted in the Ethernet ports used for the network connections.
2. Verify the link status again if cabling has been replaced or connections made.

If the Communication Status, Poll State and Port Status errors do not resolve and all the physical connections are correct. Proceed to verify the IP parameters in the next section.

6.2.2 Verify the IP parameter configuration (IP communication)

Correct IP parameter configuration is required for RMC-XIO communication to work. This procedure describes how to verify the IP parameters on the XIO. It assumes the RMC IP configuration is correct.

Consider the following:

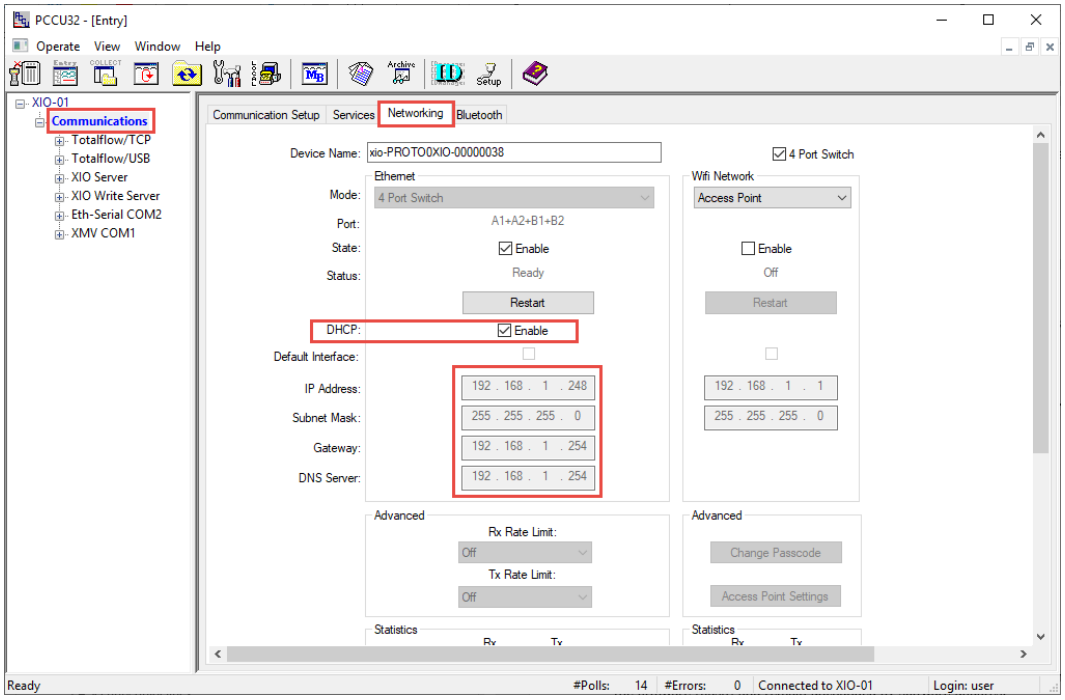
- The IP address of the XIO is automatically discovered by the RMC when the XIO interface is added from the Communication Setup screen (RMC uses Auto Discovery function and displays detected XIOs). The RMC configures this IP address in its communication parameters to establish and maintain connection with the XIO. If the detected IP address is not valid or compatible with the RMC, connection will not be possible. Verify the XIO IP parameters as described in this section. An invalid XIO address must be corrected in the XIO.
- The IP address must be manually added to the RMC XIO Interface communication parameters when the interface is added from the Application and License Management screen. Ensure that the XIO IP address configured in the RMC is correct. An incorrect address in the RMC (even if the XIO configuration is valid) must be corrected in the RMC.

6.2.2.1 Verify that the XIO has a valid IP configuration

To verify IP configuration in the XIO:

1. If the XIO has static IP parameters, verify that the parameters are valid for the field network. Obtain valid static IP parameters from your network administrator.
2. If the XIO is using DHCP for automatic IP parameters configuration, verify the XIO has obtained the values. Figure 6-5 shows an XIO with DCHP enabled and with IP parameters obtained from the DHCP server.

Figure 6-5: XIO with IP parameters obtained from DHCP server



3. If DHCP is enabled and the IP parameter fields show zeroes:
   a. Verify that the connection to the network switch or router is not broken or damaged and that the link is up.
   b. Verify that the DHCP server is enabled on the field switch or router.

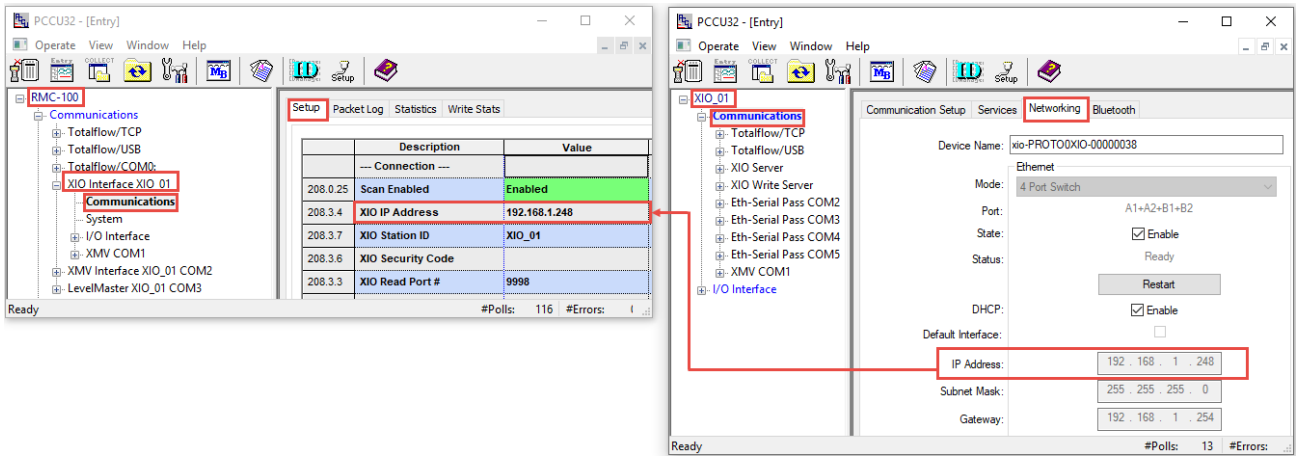
6.2.2.2 Verify that the RMC has the correct XIO IP address

If the XIO has a valid configuration, verify that the XIO IP address has been correctly configured on the RMC. A mismatch in configuration prevents connection. Follow this procedure if you added the XIO Interface from the RMC Application and License management tab and configured the IP address manually. It is possible to type an incorrect address.

To verify:

1. On the RMC navigation tree, expand the XIO interface and select **Communications**.
2. On the **Setup tab**, verify the XIO IP address value.
   a. Verify that the value matches the IP address in the XIO.

Figure 6-6: Correct XIO IP address – IP address match on both the RMC and XIO



b. If the IP value for the RMC does not match the value for the XIO (Figure 6-7), the RMC-XIO status reflects connection failure (Figure 6-8).

Figure 6-7: Incorrect XIO IP address configured on the RMC

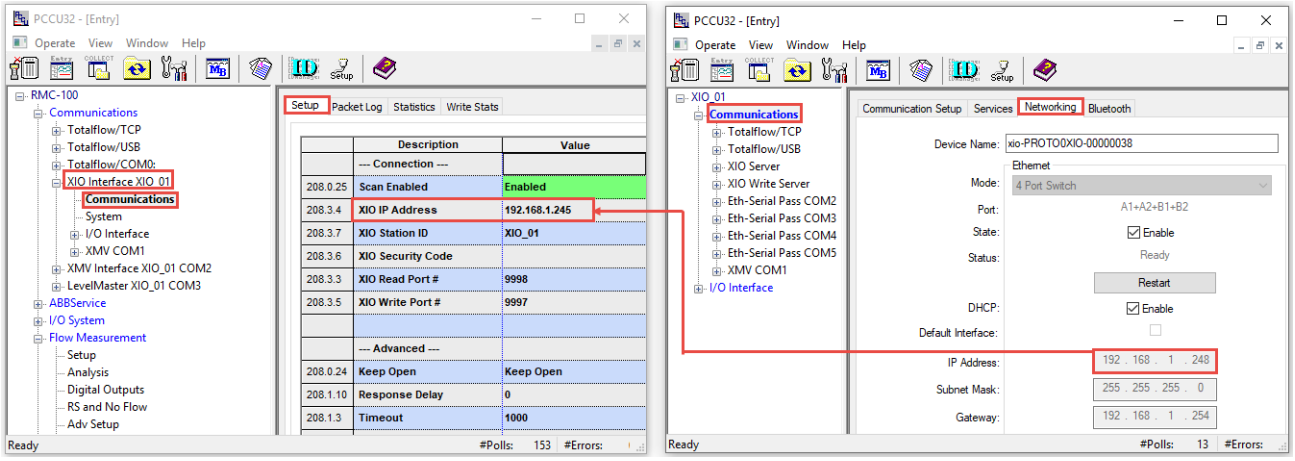
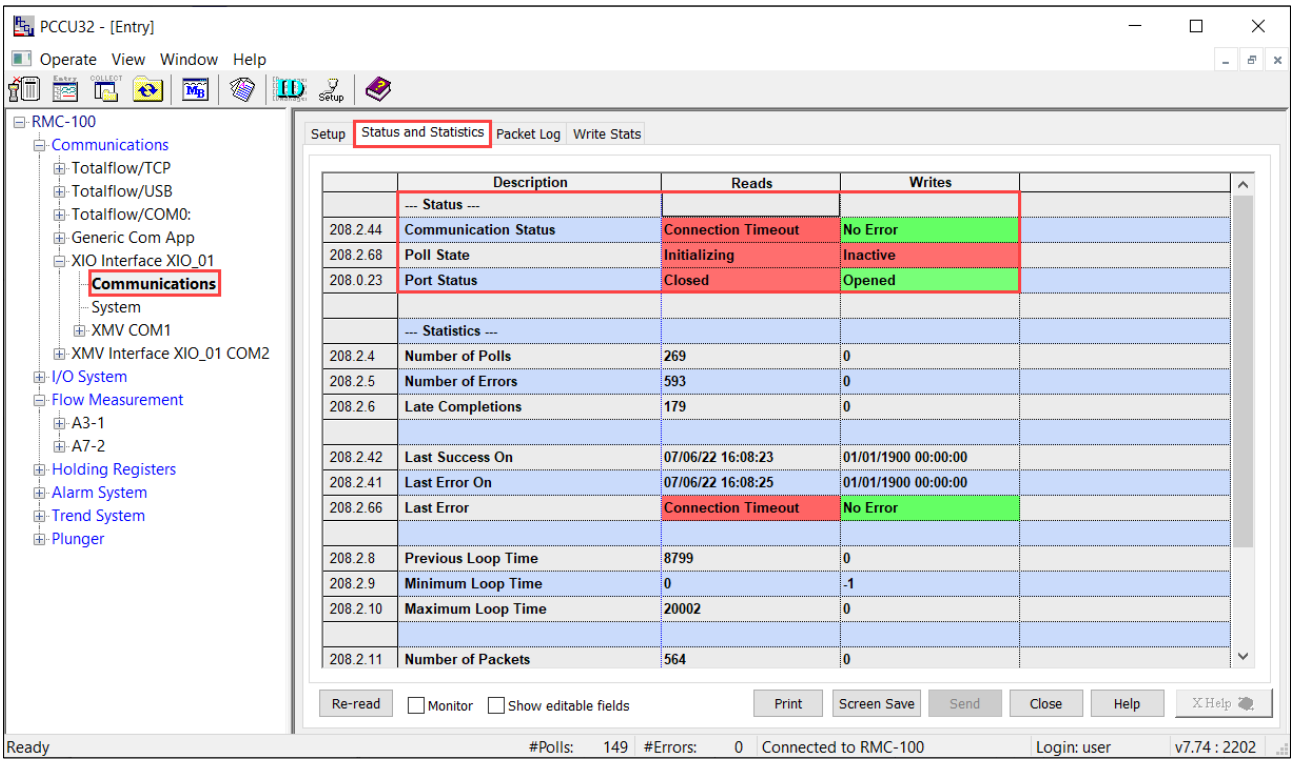
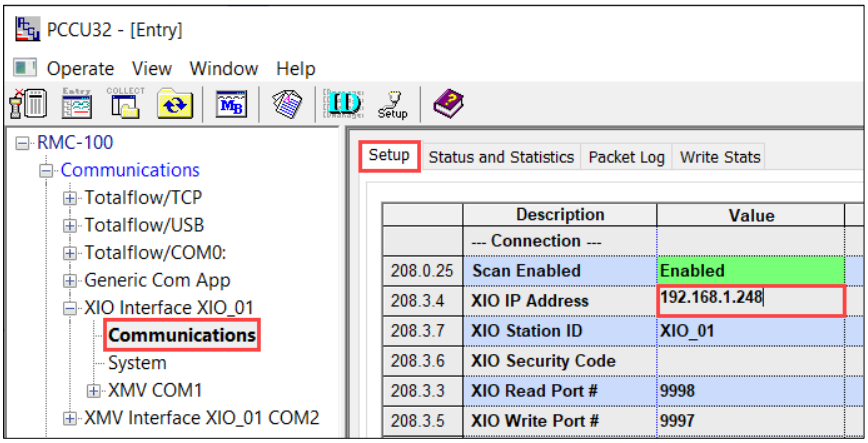


Figure 6-8: Connection failure - incorrect XIO IP in the RMC XIO Interface setup



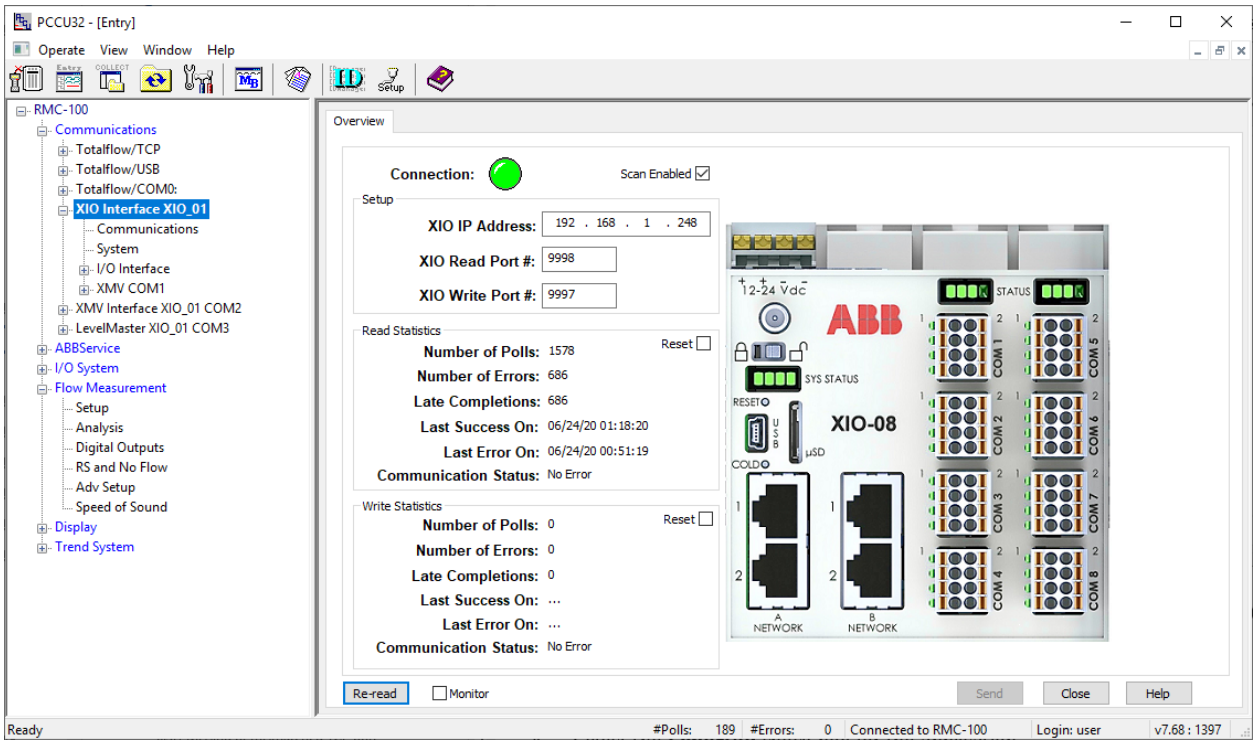
3. Correct the IP address to match the IP address in the XIO (Figure 6-9).

Figure 6-9: Manual correction of the XIO IP address in the RMC



4. Click **Send** to save the updated address.
5. On the navigation tree, select **XIO Interface** to verify that the connection is established. The connection status indicator should display green.

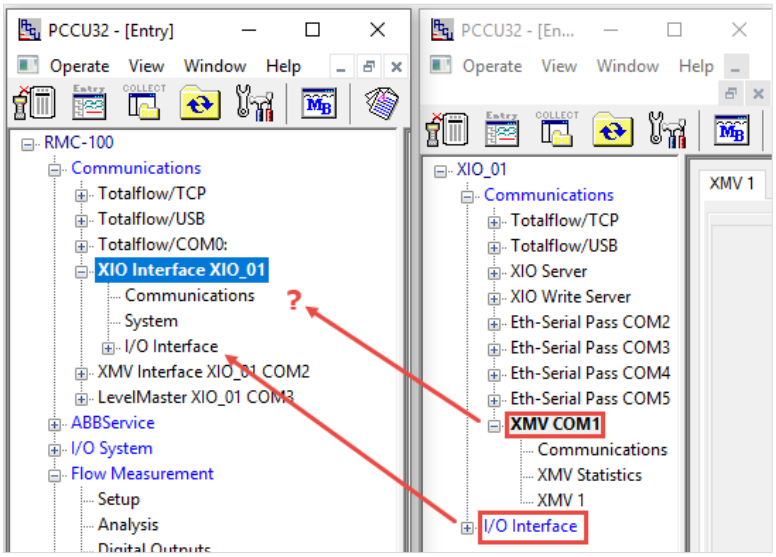
Figure 6-10: XIO Interface overview screen - RMC-XIO connection successfully established



6.3 XIO applications not displaying on the RMC

Non-exported applications may not display under the XIO Interface on the RMC (Figure 6-11). To manage the remote XIO applications from the RMC, those applications must be exported.

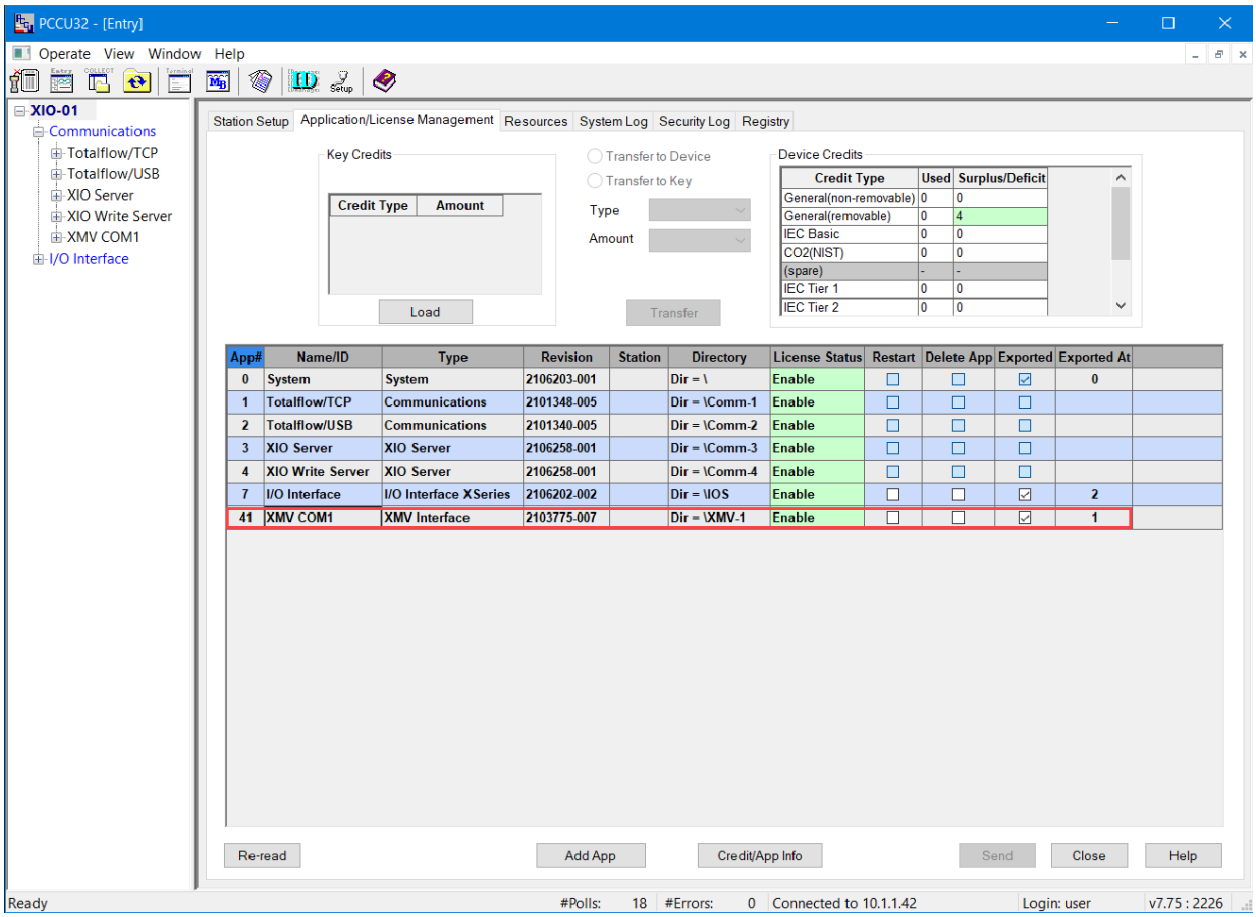
Figure 6-11: Missing remote applications on the RMC XIO Interface



To verify the application export setting:

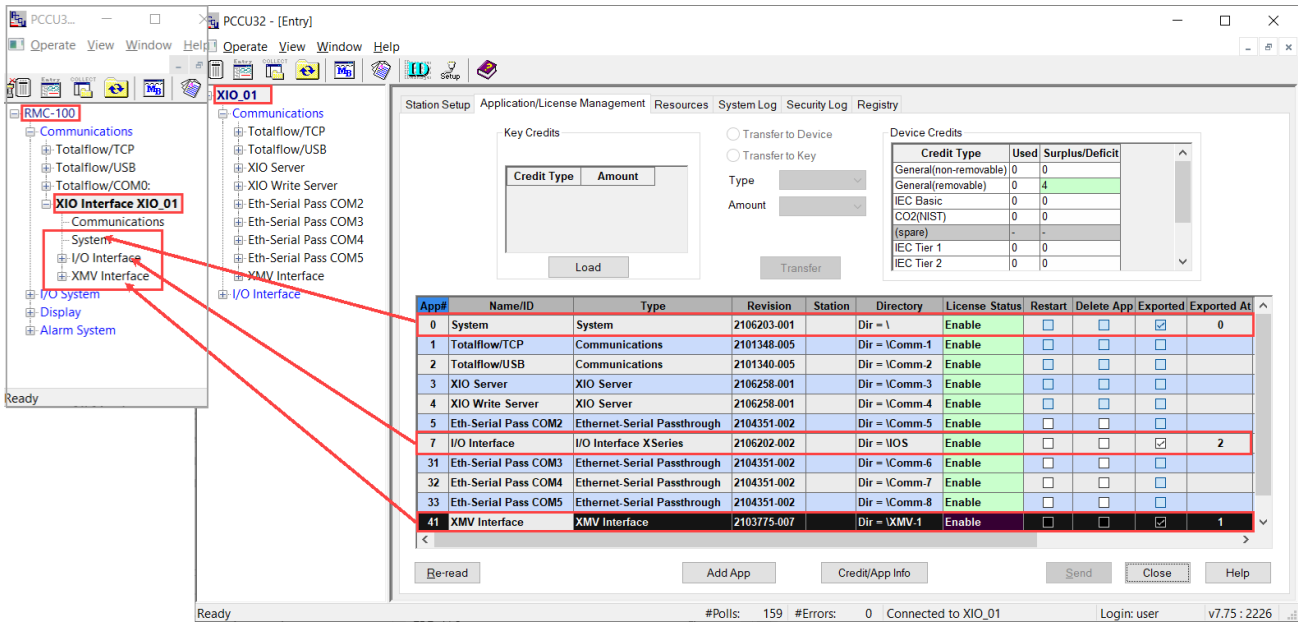
1. On the navigation tree, select the XIO Station ID.
2. Select the Application/License Management tab.
3. Locate the application of interest in the application table.
4. If not set for export, select the **Exported** check box for the application.
5. Accept default or select value for application index in the Exported at column.

Figure 6-12: Exported check box



6. Click **Send**.
7. On the RMC, refresh the corresponding XIO Interface instance and verify that the exported applications display (Figure 6-13).

Figure 6-13: Exported XIO applications available on the RMC

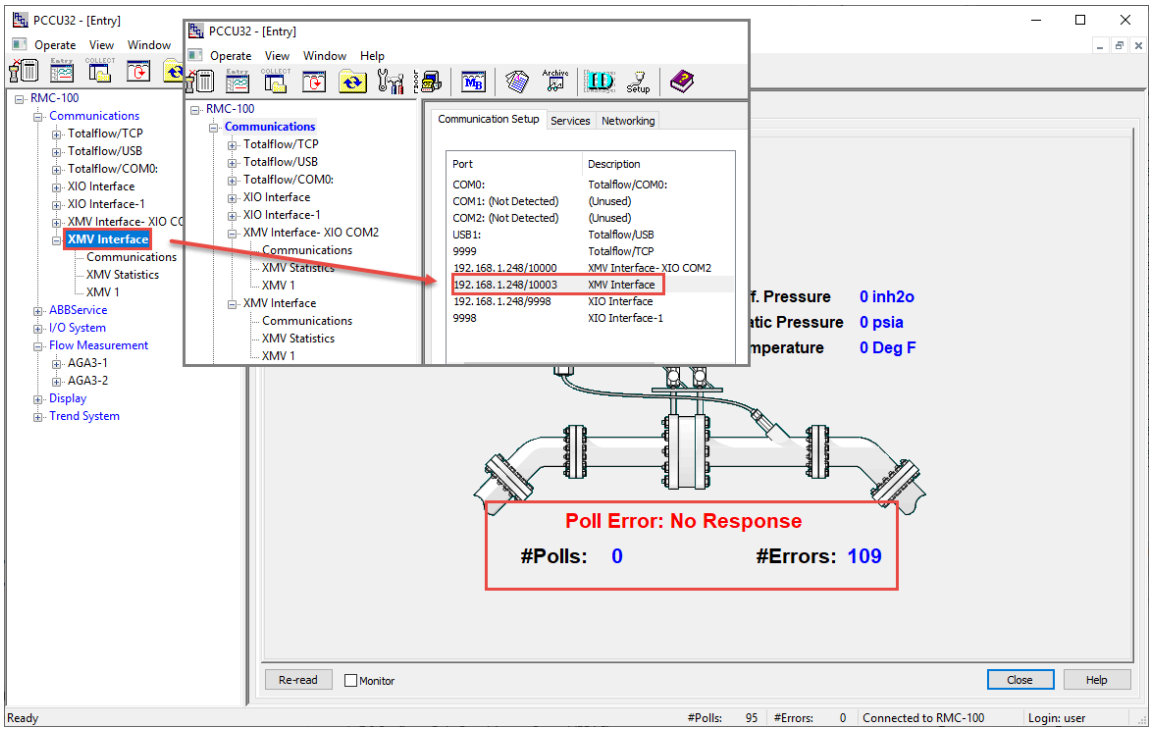


6.4 RMC failure to receive data from XIO passthrough

The RMC-XIO communication through Ethernet-Serial passthrough requires assigning the desired COM port, assigning a unique TCP port, and configuring the correct serial communication parameters. As with any serial communication setup, parameters on the XIO must match the parameters of the RMC application that is processing the data received from the XIO COM port.

If you are experiencing issues communicating when using the Ethernet-serial passthrough function, verify the configuration on the XIO first and then troubleshoot serial communication. The following figure shows an RMC XMV application configured for communication with an XIO which is unable to receive XMV data.

Figure 6-14: RMC failure to receive data – XMV Interface does not have XMV values

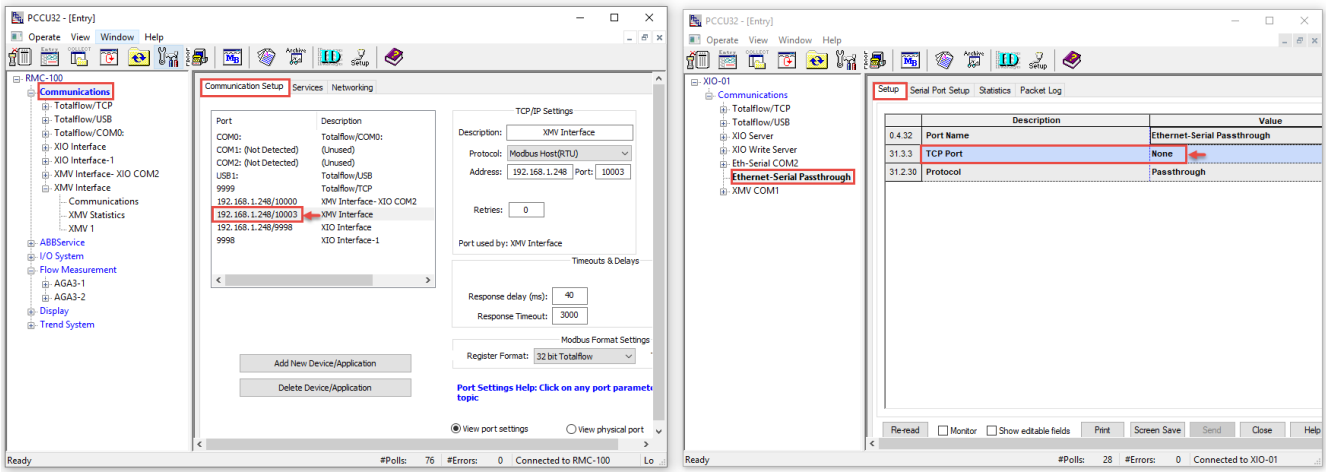


The procedures in this section assume that the serial device is properly wired to the XIO COM port. If none of the procedures included in this section resolves communication failure, be sure to check the wiring again.

6.4.1 Missing or mismatched TCP port

A mismatched or missing TCP port on either the RMC or XIO prevents communication. Figure 6-15 shows the example of an RMC XMV application (left) using Ethernet-Serial Passthrough to communicate to a port on an XIO (right). Note that the RMC has a destination IP and TCP port, but the TCP port in the XIO is missing. The RMC will be unable establish a connection until the XIO has a matching and valid TCP port.

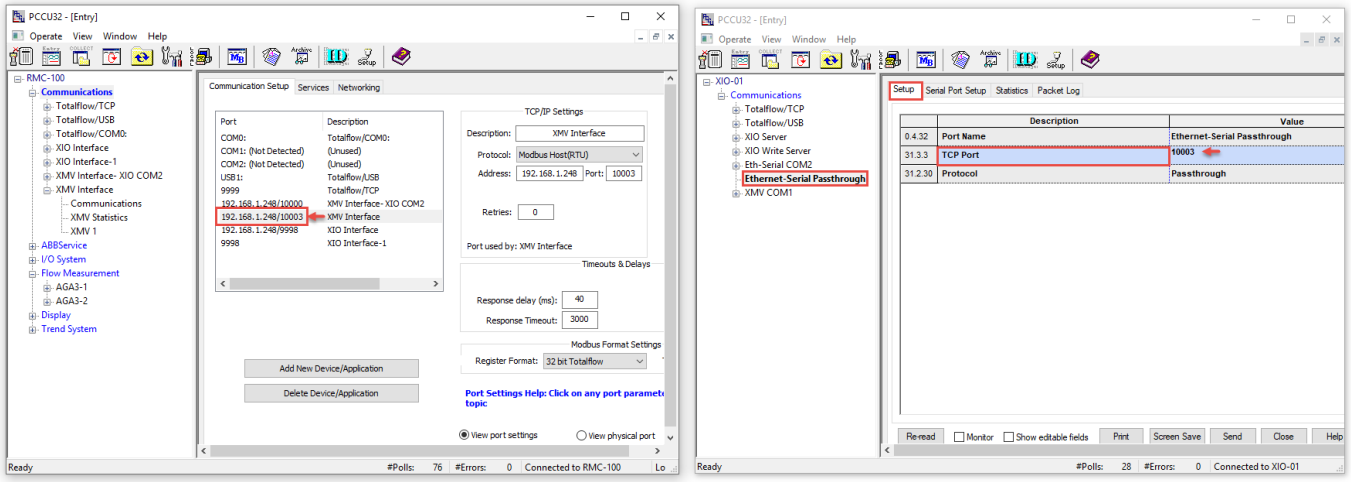
Figure 6-15: Missing TCP port



To verify or configure the TCP port on the XIO (Figure 6-16):

1. On the navigation tree, select the **Ethernet – Serial passthrough** instance (Right image).
2. On the Setup screen, verify that the TCP port parameter has a valid port number and that it matches the one configured in the RMC.

Figure 6-16: Configure TCP port



3. Click **Send** to save changes.

6.4.2 Missing or incorrect XIO serial port

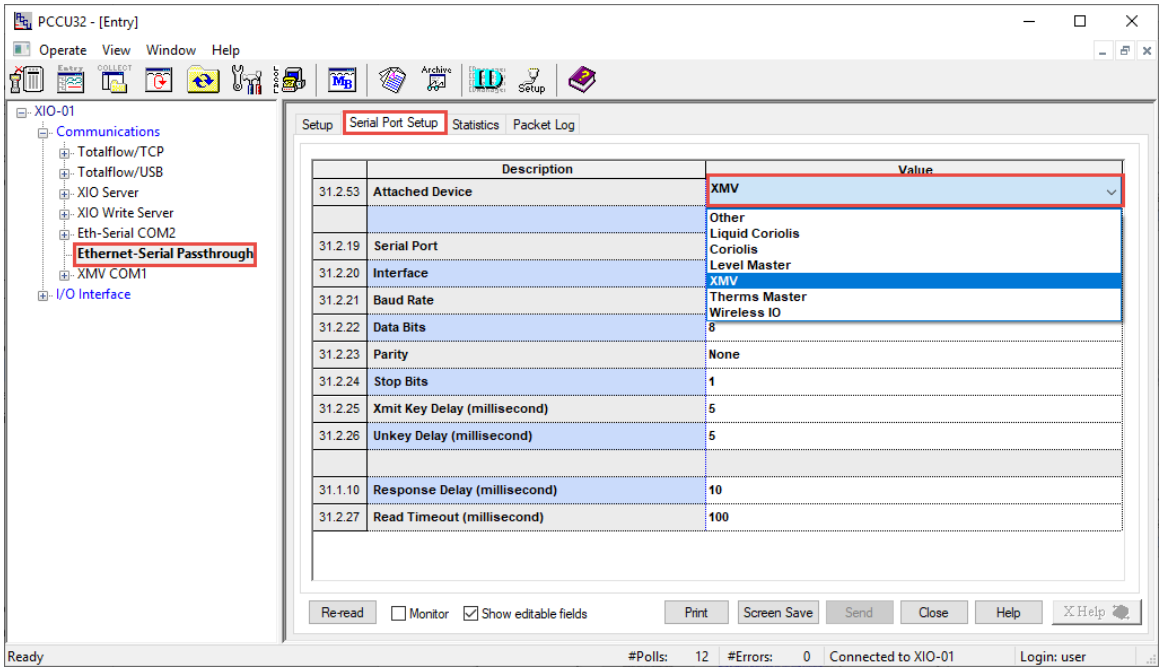
Configure the Ethernet-Serial Passthrough instance for the correct port and attached device type.

To verify or assign the correct XIO COM port and device type:

1. On the navigation tree, select the **Ethernet – Serial Passthrough** instance.
2. Select the **Serial Port Setup** tab.
3. Select the device type from the **Attached Device** drop-down list.

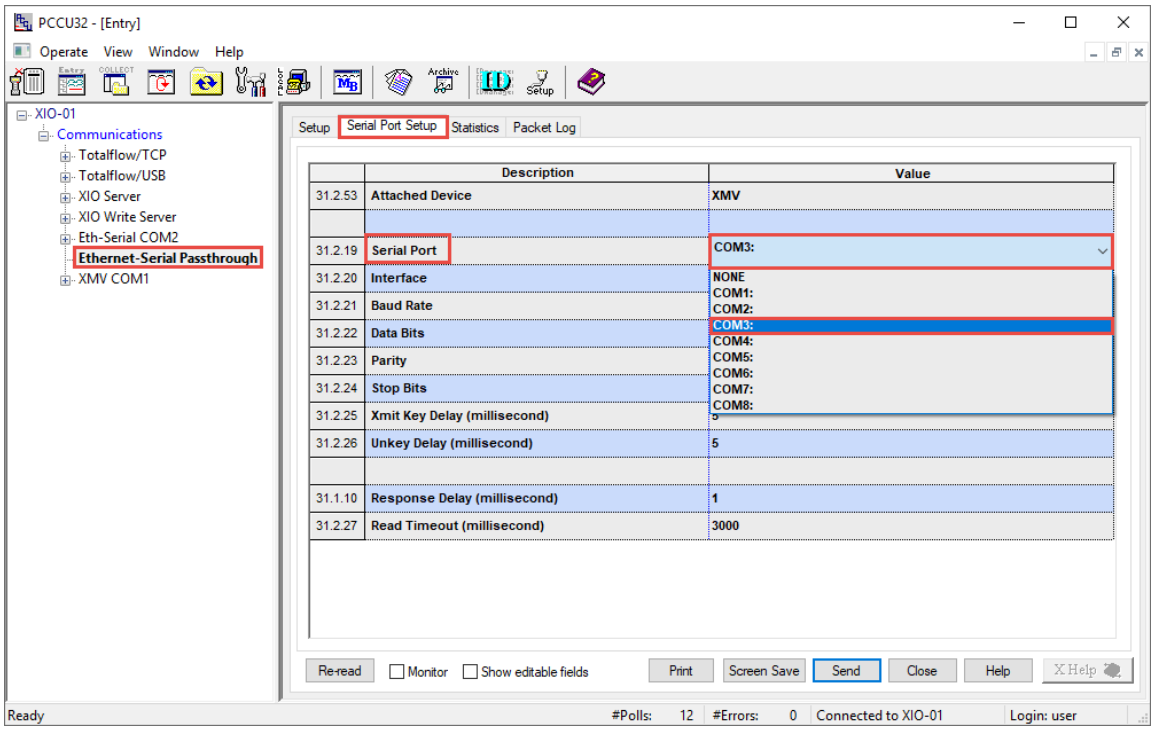
IMPORTANT NOTE: The XIO supports pre-configured communication parameter values for several ABB peripherals. When connecting the XIO COM port to one of these devices, selecting the correct attached device type uses the optimal values to communicate with that device. For third-party peripherals, select **Other** and consult the vendor documentation for optimal values. Incorrect device type configuration prevents communication because of mismatched device and port settings.

Figure 6-17: Configure attached device type



4. Ensure the Serial Port displays the desired COM port. If none displays, select the port from the drop-down list.

Figure 6-18: Configure COM port



5. Click **Send**.

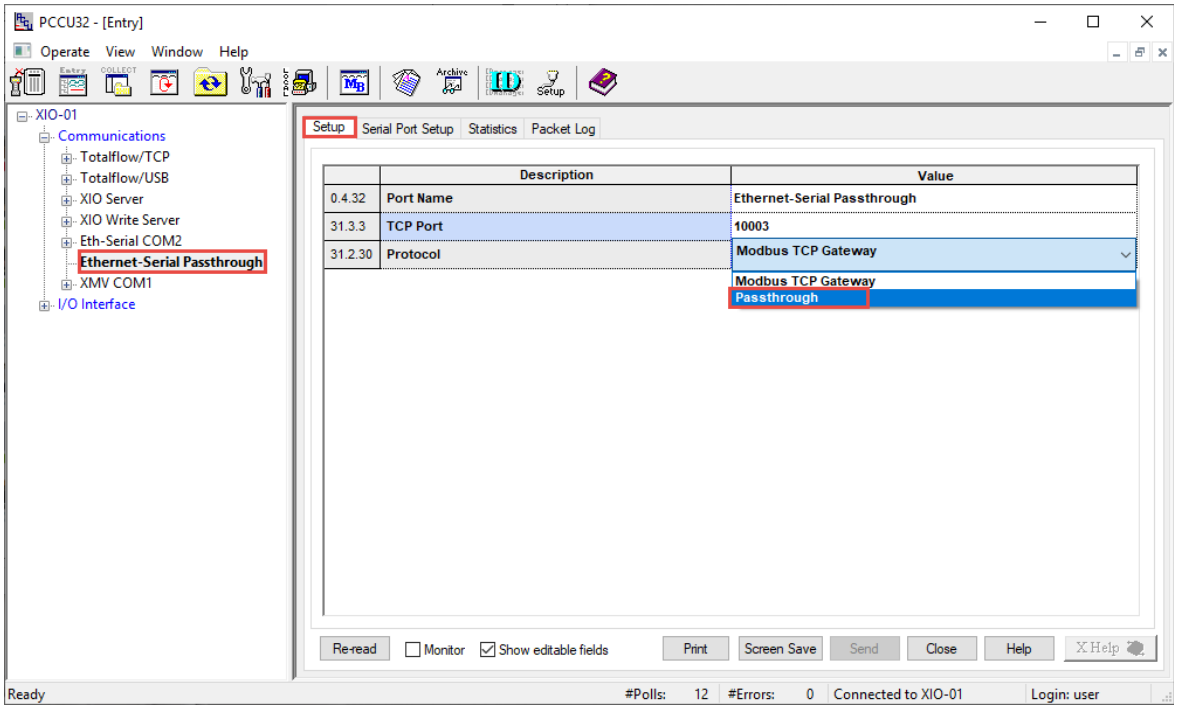
6.4.3 Incorrect protocol selection

Ethernet-Serial Passthrough supports the Passthrough or Modbus TCP Gateway protocols. Set the XIO for the Modbus TCP Gateway protocol only if the RMC communication application is setup as a Modbus TCP client. Otherwise, use Passthrough. Mismatch in protocol configuration prevents communication.

To verify or configure the correct protocol:

1. On the navigation tree, select the **Ethernet – Serial passthrough** instance.
2. On the **Setup** tab, verify the current protocol.
3. Select the correct option from the **Protocol** drop-down list.

Figure 6-19: Configure Protocol



4. Click **Send**.
5. Verify that the RMC application receives data from the XIO COM port.

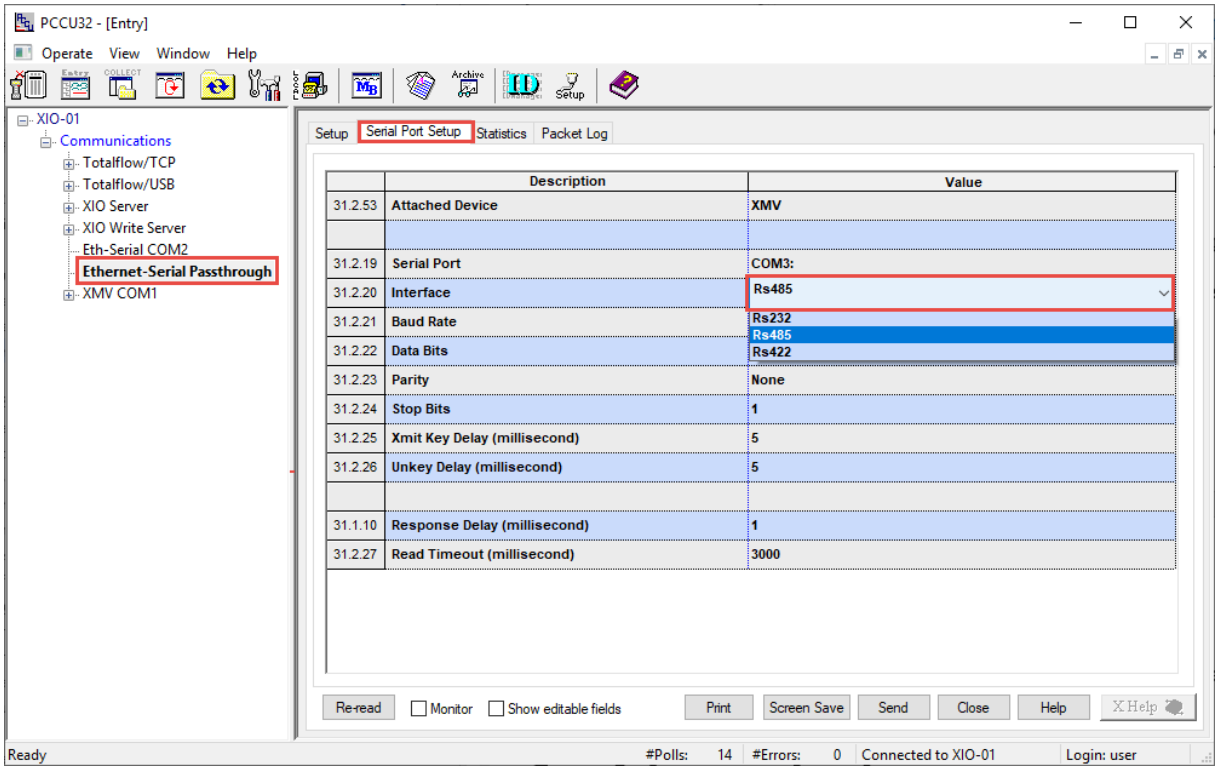
6.4.4 Mismatched serial communication parameters

If the configuration corrections in the previous sections do not resolve the communication failure, verify or correct the serial communication parameters.

To verify or configure serial communication parameters:

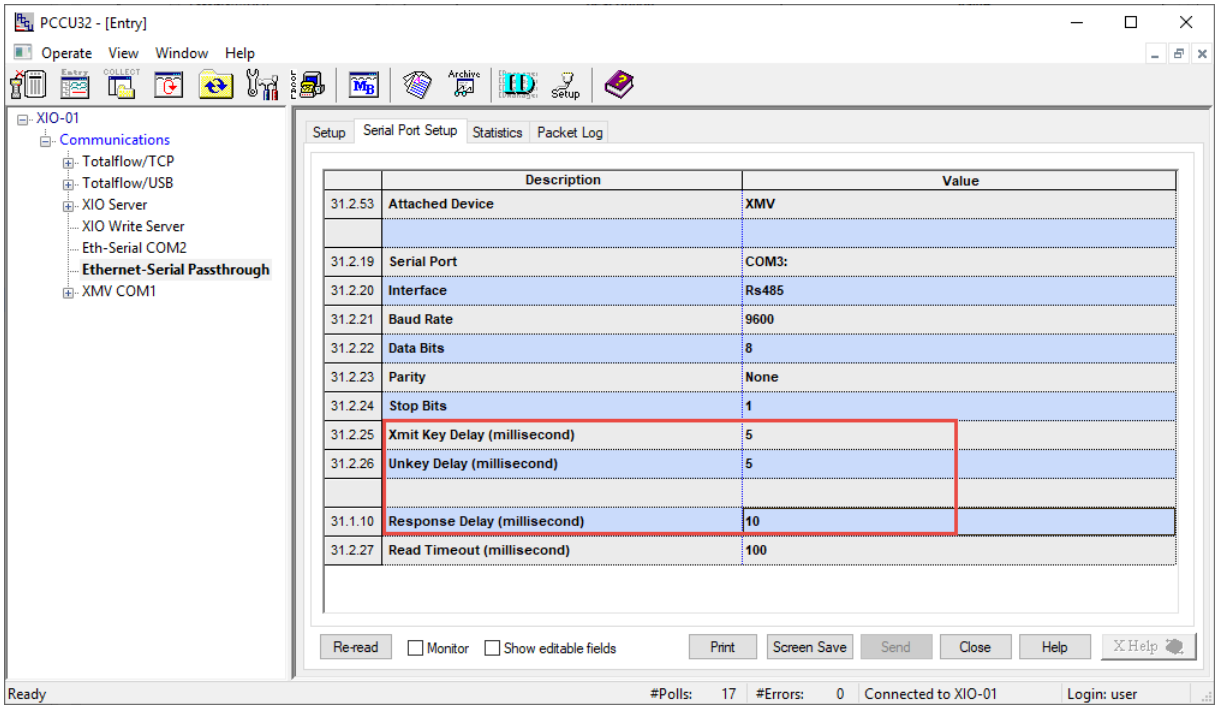
1. On the navigation tree, select the **Ethernet – Serial passthrough** instance.
2. Select the **Serial Port Setup** tab.
3. Configure the correct interface. Select from the Interface drop-down menu. It must match that of the peripheral connected to the port.

Figure 6-20: Configure COM port Interface type



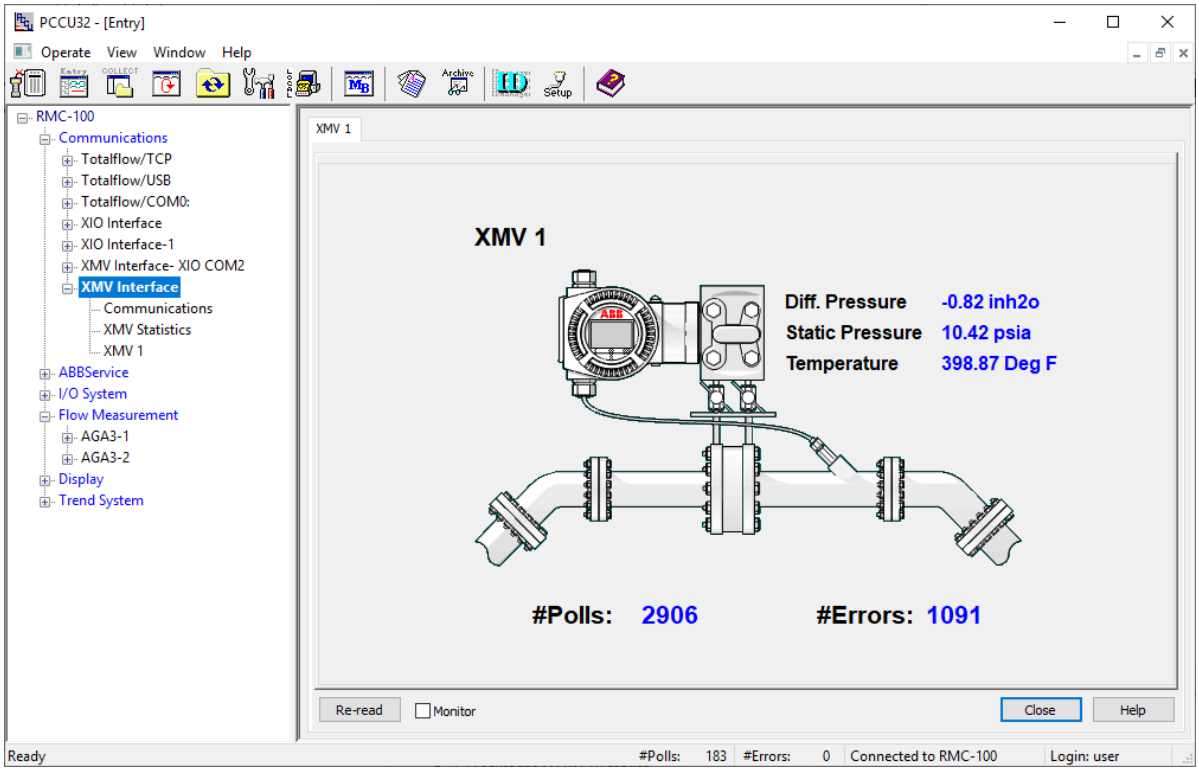
4. Configure additional parameters as applicable for the type of peripheral. For XMV optimal values, see the example in the figure below. The parameters on the RMC application should have the same values.

Figure 6-21: Configure additional COM port parameters



5. Verify that the connection is successful. The RMC should be able to receive data.

Figure 6-22: RMC application able to receive data – XMV Interface displays XMV values



6.5 Fail Safe Watchdog alarm does not clear

Follow this procedure if the Fail Safe Watchdog state remains in an alarm condition even after an attempt at manual recovery (the alarm won't clear from Manual or Auto mode).

IMPORTANT NOTE: The Fail Safe Watchdog feature monitors network connectivity between the RMC and the XIO. This procedure assumes that the RMC and the XIO are successfully connected. For additional information on the Fail Safe Watchdog feature, click **Help**.

Figure 6-23: Fail Safe Watchdog in Alarm State (Manual recovery mode)

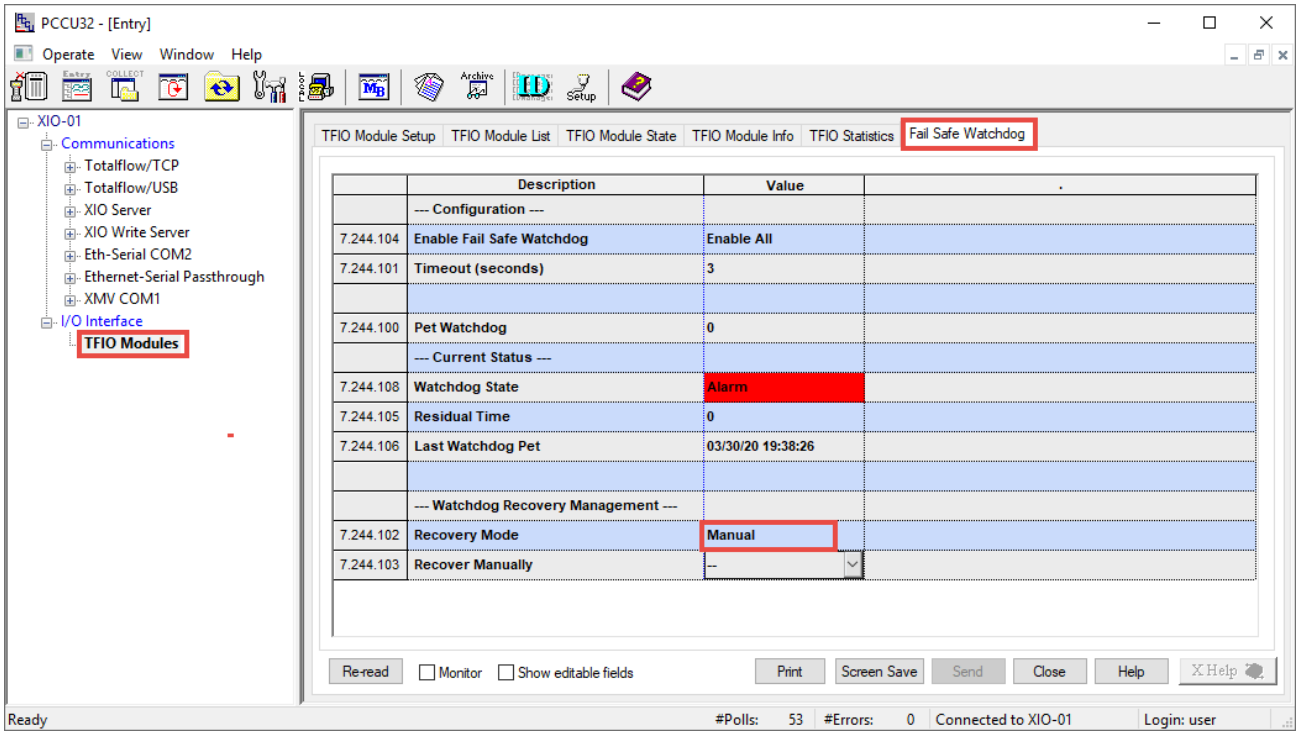
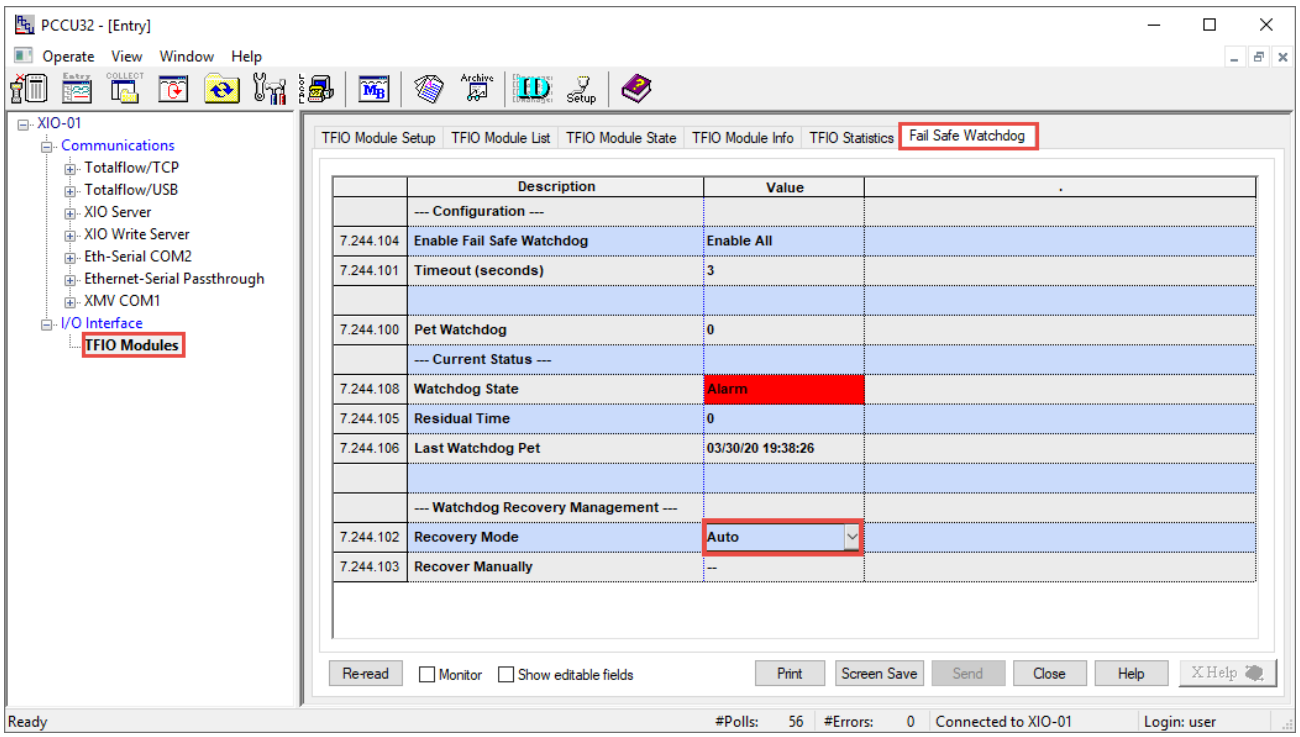


Figure 6-24: Fail Safe Watchdog in Alarm State (Auto recovery mode)

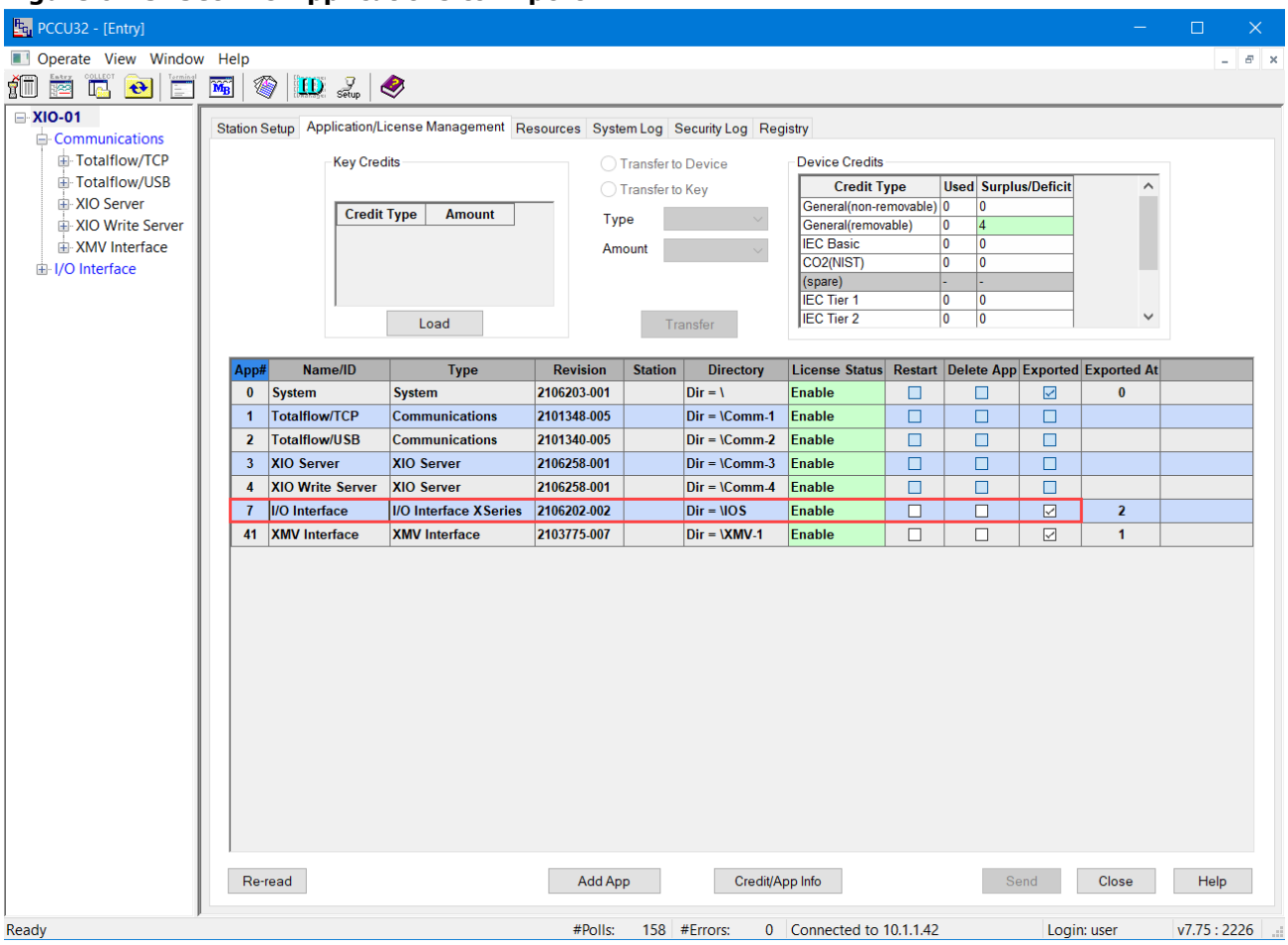


To clear the alarm:

1. Ensure there is network connectivity between the RMC and the XIO. If connectivity has been lost, restore communication before attempting to clear the watchdog alarm.
2. Set the I/O interface application for export to the RMC.

a. On the navigation tree, select the XIO ID.
b. Select the **Application and License Management** tab.
c. Locate the IO Interface application in the application table.
d. Select the **Exported** check box.

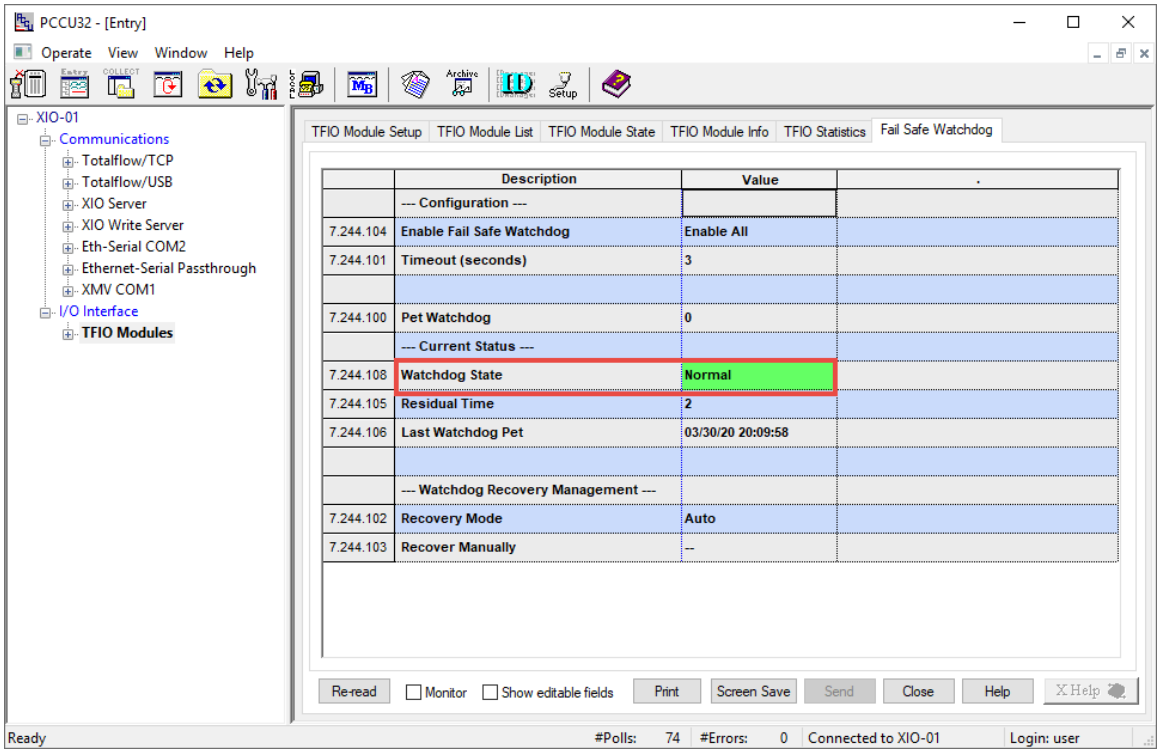
Figure 6-25: Set XIO Applications to Export



e. Click **Send**.

3. On the navigation tree, expand the **I/O Interface** and select **TFIO Modules**.
4. Select the Fail Safe Watchdog tab.
5. Verify that the Watchdog State Alarm status cleared. The Watchdog State should display: Normal.

Figure 6-26: Normal Watchdog State



6.6 Network Diagnostic Tools

Network communications diagnostic tools are available on the Network Diagnostic tools tab from PCCU. This tab provides the ability to run the well-known PING and Traceroute network utilities. These two utilities are used to determine packet delay and routes between the XIO and a host or another device.

IMPORTANT NOTE: Running PING and Traceroute require that Ethernet Interfaces are enabled, active, and configured with correct IP parameters. Be sure to configure the appropriate interfaces on the Networking tab before running these commands. Click **Help** from the Network Diagnostic Tools tab for additional parameter details and for interpreting results.

To run diagnostics:

1. Connect to the XIO using PCCU.
2. Click **Communications** on the PCCU navigation tree.
3. Click the Network Diagnostic Tools tab.
4. Select the utility from the Tools Type drop-down list.
5. Configure required parameters.
6. Click the **Start** button to run the utility.
7. Review results.

7 Configure security (recommended)

To secure access to the XIO, review the security features implemented.

7.1 Access points

Totalflow user interfaces and host products support connection with the XIO through several types of communication ports, protocols, and services. These are points of entry that could be subject to inexperienced, unauthorized or malicious access through a point-to-point connection or a network connection. Physical access to the ports must be controlled to protect local and remote access. Enable on-board security or enforce authentication before establishing a connection with any of the ports.

This section lists the communication ports, services, protocols, and the open Transmission Control Protocol (TCP) ports that must be considered when securing devices.

7.2 Communication interfaces

The table below lists the default communication ports available in the XIO with standard configuration. These ports are pre-configured from the factory. When enabled, these ports are ready for use, but are not secured.

Unprotected ports make the full functionality of the device available to any user. Configure security passcode or role-based authentication to prevent unauthorized access.

Table 7-1: Default communication ports on the XIO

Wired connections communication ports, default names	Default state	Default protocol	Security feature available
USB, port name: Totalflow/USB	Enabled	Totalflow Local (Read-only)	Bi-Level Security code authentication or Role-base Authentication (Role-base Authentication, RBAC)
Ethernet, port name: Totalflow/TCP	Enabled	Totalflow/TCP (Read-only)	Bi-Level Security code authentication or Role-base Authentication (Role-base Authentication, RBAC)
COM1-COM8, port name: TF – Remote	Disabled	Totalflow Remote (Configurable)	Bi-Level Security code authentication or Role-base Authentication (Role-base Authentication, RBAC)

IMPORTANT NOTE: The Totalflow protocol is an unsecured protocol. As such, the intended application should be assessed to ensure that these protocols are suitable before implementation.

IMPORTANT NOTE: The Ethernet ports on the XIO might connect to a network and peripheral devices. If the peripheral devices send real-time measurement data to the XIO, configure connections correctly to prevent loss of this data due to network issues. See section 9 Ethernet connectivity scenarios.

The table below lists the wireless interfaces available in XIO devices with standard configuration.

Table 7-2: Wireless interfaces in XIO

Wireless connections communication interfaces	Default state	Protocol	Security feature available
Wi-Fi, Wi-Fi Access Point functionality	Disabled	Totalflow Local/TCP	Passcode protection and standards-based Wi-Fi security modes (WPA, WPA2)
Onboard Bluetooth, Port Name: Bluetooth	Disabled	Totalflow Local	Role-Based Authentication (RBAC)

7.2.1 User-enabled services

Services are software processes that run on the XIO device. The table below lists user-enabled services that open access to the embedded software file system. Unauthorized or malicious use of these services can cause file corruption and render a device inoperable.

Table 7-3: User-enabled services on the XIO

Service Name	Default state	Description	Security feature available
SSH/SFTP Service	Disabled	Serves connection requests for secure login shell and file transfer. Supports connection requests from third-party SSH/SFTP clients.	Authentication based on private-public key pairs, passphrase-protected keys
Totalflow Software Update Service	Enabled	Enables or blocks the ability of the device loader to update the embedded software.	None specific to the service. Must use Bi-level security passcode or Role-Based Authentication (RBAC)
Auto Discovery Service	Enabled	Enables publishing and discovery of server applications running on XIO and other devices in the network.	None specific to the service.

7.2.2 Open Transmission Control Protocol (TCP) ports

The table below lists the open TCP ports on the XIO. These ports are used for all TCP/IP based connections which are supported by the Ethernet ports.

Protocols over TCP can be standard like SSH, or proprietary like Totalflow (Remote or Local).

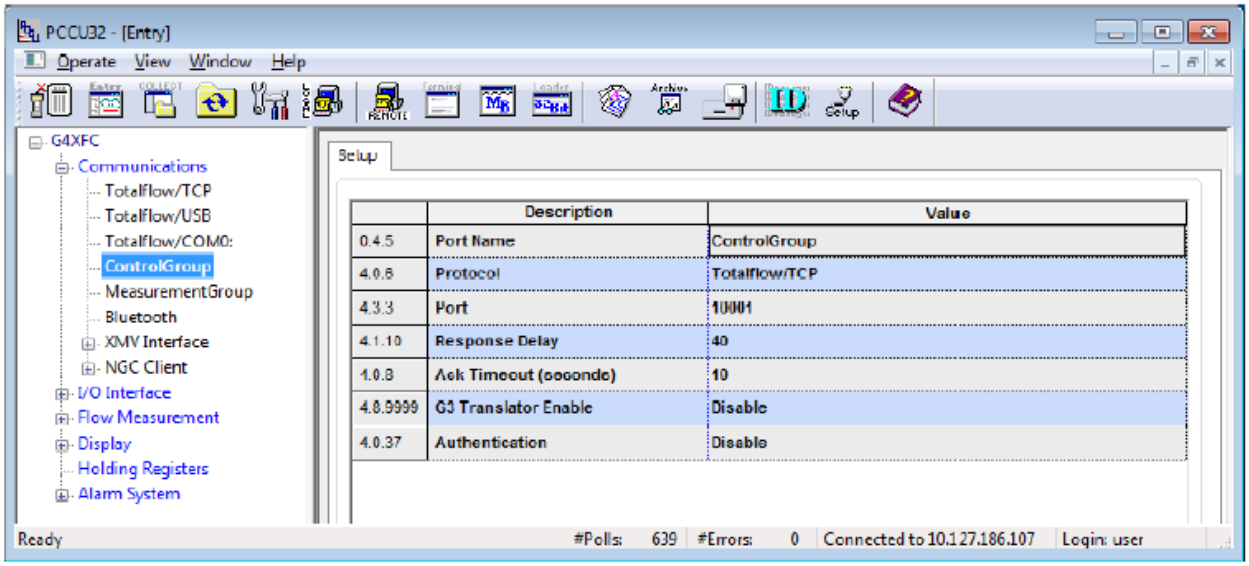
Table 7-4: Open TCP ports on the XIO

Default port	User-configurable	Port can be closed	Protocol using the port	Description
9999	Yes	No	Totalflow/TCP	Assigned to connections used for device monitoring, configuration and data collection or polling. PCCU, WinCCU, TDS and third-party SCADA systems request these connections.
9997	Yes	No	Totalflow/TCP	XIO Write Server: Assigned to connections used to control data points by other remote controllers like RMC through XIO Interface App.
9998	Yes	No	Totalflow/TCP	XIO Server: Assigned to connections used for data polling by other remote controllers like RMC through XIO Interface App.
65535	No	Yes	Device Loader/ TCP	Assigned to the device loader connections for device software update. PCCU requests this type of connection.
9696	No	Yes	SSH/TCP	Assigned to secure shell (SSH/SFTP) connections. Third-party SSH/SFTP clients request these connections.
5353	No	Yes	mDNS/UDP	Used by Auto Discovery service to detect Totalflow services present on the network

IMPORTANT NOTE: The TotalFlow/TCP and Modbus protocols are unsecured protocols, as such the intended application, should be assessed to ensure that these protocols are suitable before implementation.

IMPORTANT NOTE: For connections with user-configurable ports, use the default value or assign a different port number from the range of 1024 to 65534. Connections using non-default TCP ports are handled by additional Totalflow/TCP communication or Modbus TCP applications configured with different TCP ports. For example, the figure below shows an additional Totalflow/TCP application (named ControlGroup) with a different TCP port (10001).

Figure 7-1: Totalflow/TCP application instance with non-default TCP port



IMPORTANT NOTE: TCP port numbers from 0 to 1023 are universally reserved for well-known ports. Never use these port numbers.

7.3 Denial of service (DOS) threshold rates

Protection of ports used for TCP/IP communication, such as Ethernet, is very important. Cybersecurity threats can make a device unavailable for connection.

If the Totalflow device has a Denial of Service (DOS) attack, the device cannot grant requests for connection. It stops responding. The following table provides the DOS threshold rates per packet type. The device stops responding at these thresholds.

Table 7-5: Denial of Service (DOS) threshold rates

Packet type	Description
Ethernet	9 Mbps (13393 packets/sec)
ARP	9 Mbps (13393 packets/sec)
IP	9 Mbps (13393 packets/sec)
ICMP	27 Mbps (40179 packets/sec)
UDP	10 Mbps (14881 packets/sec)
TCP	10 Mbps (14881 packets/sec)

7.4 Security guidelines

The following table contains recommended guidelines to secure access to the XIO. Find procedures for secure configuration throughout this manual, in Quick Start Guides, and in online PCCU help files.

Table 7-6: XIO security guidelines

Recommendation	Description
Secure physical access to the device	Control access to the device, internal components, and connected peripherals.
Secure access with security switch	Turn the onboard security switch on to enforce authentication through bi-level security codes or RBAC. See section 7.5.
Configure bi-level security codes	Change default security codes to private codes (the default security code for both level 1 and level 2 is 0000). See section 7.5.
Enable Role-Based Access Control (RBAC)	Configure RBAC. See section 7.6. Enable role-based access and enable authentication for each of the communication ports. Change the default RBAC passwords and security codes.
Secure network connection	The device only connects to a firewall-protected private network. Do not connect directly to the Internet.
Secure Bluetooth® access	Enable Bluetooth only when required. Enable RBAC authentication on the port. See section 7.6.
Secure SSH/SFTP access	Enable the SSH/SFTP service only when required. Change the default SSH/SFTP private keys for all accounts. The SSH/SFTP private keys should always be passphrase-protected. See section 7.7 Secure the SSH/SFTP service.
Secure software updates	Enable the Totalflow Software Update service only when required. Use RBAC to limit the ability to enable/disable this service.
Manage credentials	Store all private credentials, keys, and security codes in safe locations and share this information only with properly trained and authorized personnel. Change or update as needed.

7.5 Configure bi-level security with security switch

This procedure activates secured access to the XIO by changing the default (OFF) position of the security switch and configuring bi-level security codes.

Switch-enforced security applies to access from PCCU. Access for remote controllers through the XIO Interface requires that the controller has the XIO level 2 security code before connection attempt. The security code is required regardless of security switch position. If you change the default security codes on the XIO (default code is 0000 for both levels), to private customer codes, make sure you configure the same level 2 code on the RMC. Refer to section 7.5.1 Configure non-default XIO security code on the RMC.

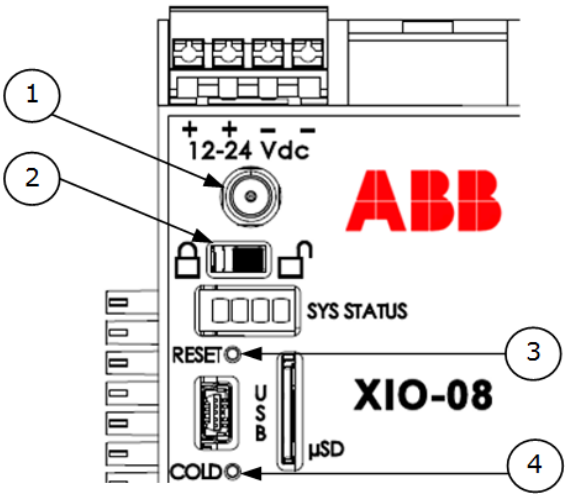
IMPORTANT NOTE: After this procedure is completed, connection to the XIO is restricted to users with the correct security codes.

This procedure requires access to the XIO security switch. If the XIO is installed inside an enclosure, access to the interior of the enclosure is required.

To enable security:

1. Open the enclosure door (if the XIO is installed inside one).
2. Locate the security switch between the Wireless Antenna and SYS STATUS LED (Figure 7-2).

Figure 7-2: XIO security switch

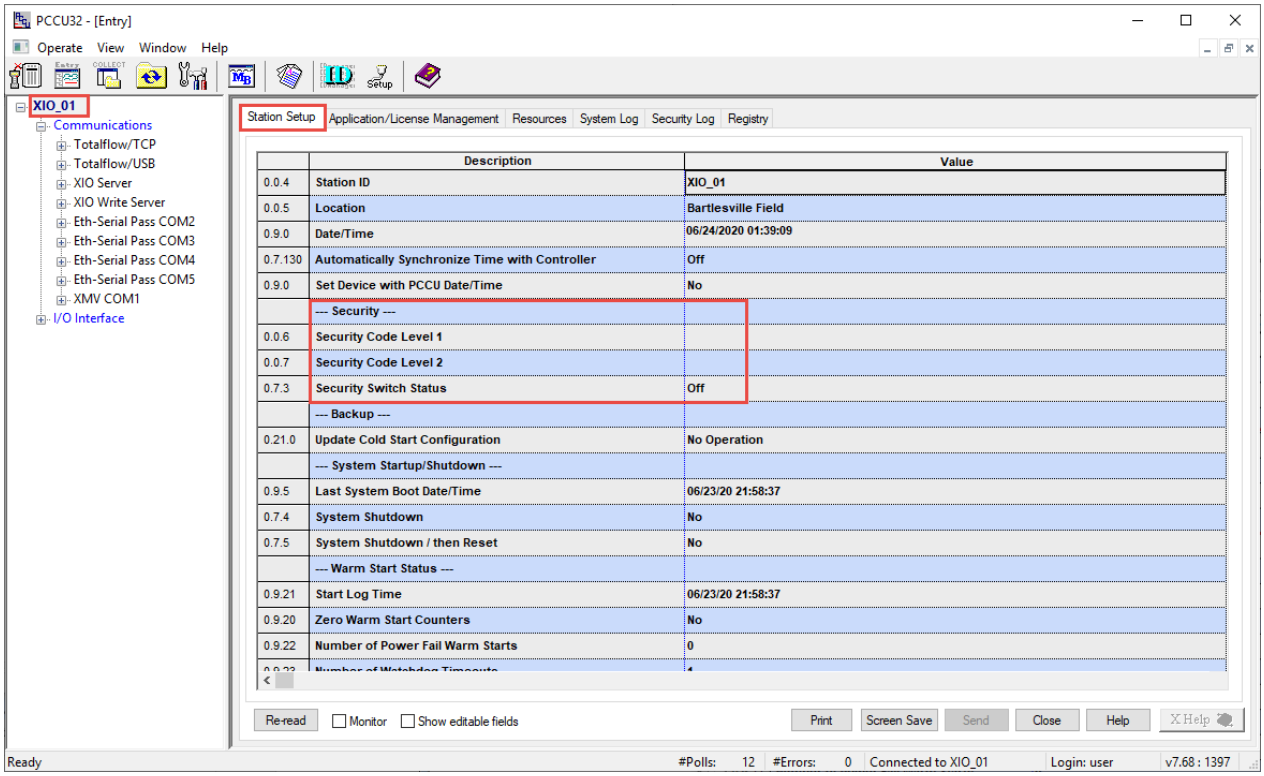


Legend: XIO security switch

ID	Description	ID	Description
1	Antenna socket	**3**	Reset button
2	Security switch	**4**	Cold button

3. Verify that the security switch is off (unlock icon).
4. Display the Station Setup tab and verify that Security Switch Status is **Off**. Note that while no security codes are visible, this does not indicate security codes are not configured. The default security codes are 0000 for both levels.

Figure 7-3: Station Setup tab – Security switch status



5. Type a four-digit security code into Security Code Level 1 (Level 1 access grants read-only access to the device).
6. Type a four-digit security code for Security Code Level 2 (Level 2 access grants read and write access to the device).

IMPORTANT NOTE: Record the security codes. They are not visible on the Station Setup tab after you save them.

7. Click **Send**.
8. On the XIO, set the security switch to on (lock icon).
9. On the Station Setup tab, click **Re-read.** Verify that the security switch status is **On**.

Enforcement of the security codes is in effect.

IMPORTANT NOTE: PCCU32 requires the security codes the next time it attempts to connect to the device. The security codes in PCCU32 version 7.68 or later do not prevent MODBUS® access to the XIO.

7.5.1 Configure non-default XIO security code on the RMC

The XIO Interface application requires read and write privileges to work properly with the XIO. If the XIO security level 2 code (write protection) is non-default, you must configure this code in the XIO Interface Communications Setup (in the XIO Security Code field). The position of the security switch does not remove the requirement for the XIO Interface App to be configured for level 2 access.

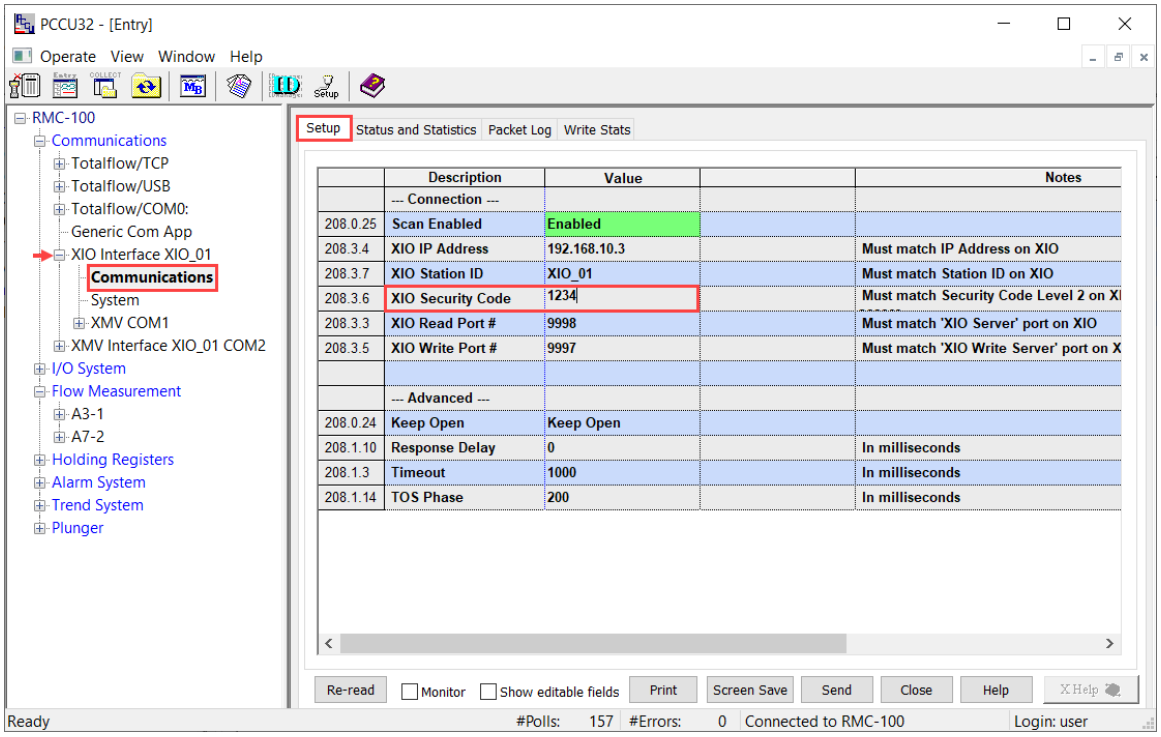
This procedure configures the XIO level 2 security code in the XIO Interface to allow the RMC to perform writes on the XIO. Connection failure occurs when the incorrect security code is configured in the XIO Interface.

This procedure assumes that the XIO level 2 security code has already been configured on the XIO **Station Setup** tab, and that the code was recorded for safe keeping. Once configured, the security code is not visible on the screen. Before proceeding, obtain the correct code.

To configure the security code on the RMC:

1. On the navigation tree, expand the XIO Interface instance and then select **Communications**.
2. Select the **Setup** tab.
3. Under the Connection section, locate the XIO Security Code parameter (Figure 7-4).
4. Type the XIO level 2 security code. It should match the security code configured in the XIO.

Figure 7-4: Configuration of XIO Security Code on the XIO Interface



5. Click **Send**.
6. Click **Yes** to confirm. Stay on the Setup screen.
7. Monitor the connection in the Status section. The connection should be restored once the XIO Interface reestablishes connection with the correct code. The Communication Status, Poll State (reads) and Port Status should display: No Error, Active, and Opened respectively.

7.6 Configure Role-Based Access Control (RBAC)

Role Based Access Control (RBAC) is a feature in PCCU32 that allows an administrator to designate roles and control access levels for various applications and processes in the device. The XIO supports RBAC security files. Each security file is configurable for the specific device type.

When designing an RBAC security system, consider all required user access to the system. Create the users and an administrator and assign a default role to each.

RBAC security configuration restricts or disables unapproved applications and functions for the current user. Restricted applications and restricted functions are not visible on the PCCU32 navigation tree. The Send button is grayed out on applications with read-only functionality.

NOTICE – Security override: Once implemented, RBAC overrides the device-enforced bi-level security and PCCU32-enforced security. RBAC replaces all other security and specifically implements on a port-by-port basis.

7.6.1 Default access roles

Default roles are automatically available in PCCU32:

- Administrator
- Expert
- Advanced
- Basic
- File Admin

The Administrator role has the highest-level access rights to all functions. Administrators add users, define roles, and save security configuration files to a PC. Expert, Advanced, and Basic roles have decreasing levels of access rights. The File Admin role has the access rights of the Basic role plus minimum rights required for sending and reading RBAC security files to and from devices. The security files can upload to multiple flow computers for implementation.

7.6.2 Set up and create a new RBAC security control file

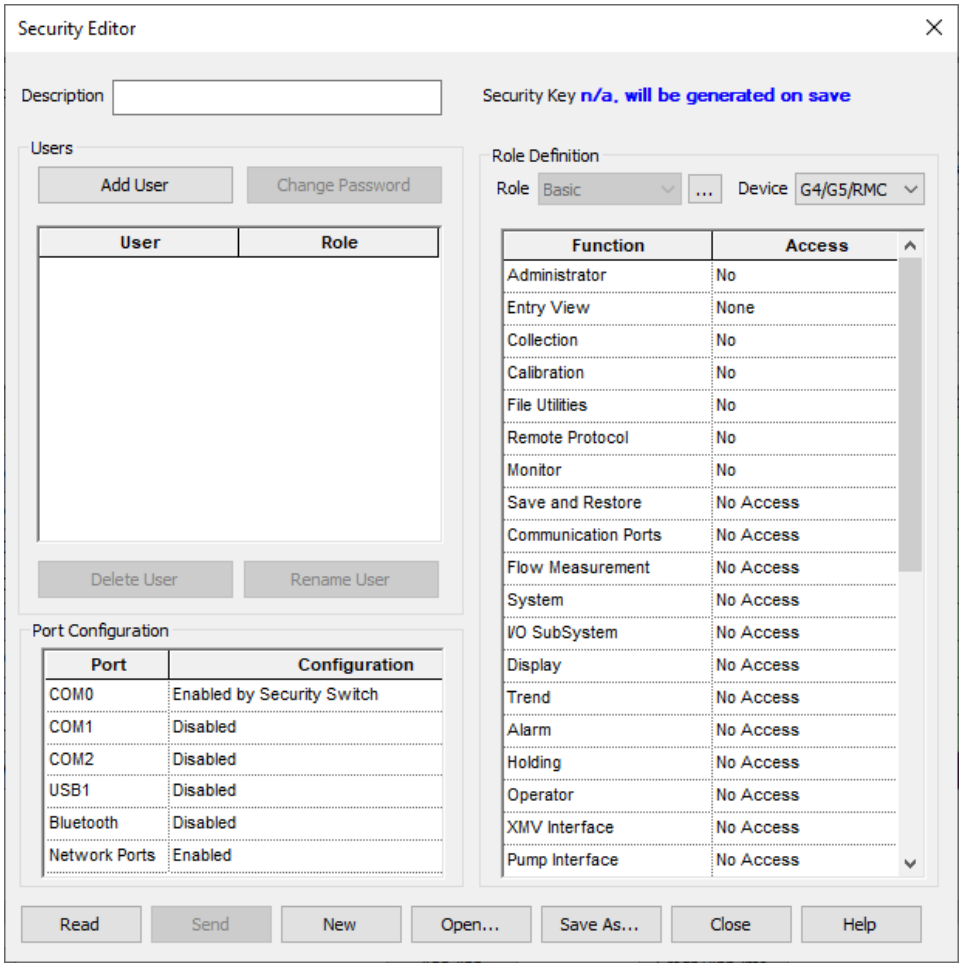
This section explains how to set up a new RBAC security system and includes:

- Create a security control file.
- Create an administrator account.
- Create individual user accounts and assign default roles.
- Create customized roles if necessary.
- Configure communication ports.
- Save the security file.

To set up a new RBAC security system:

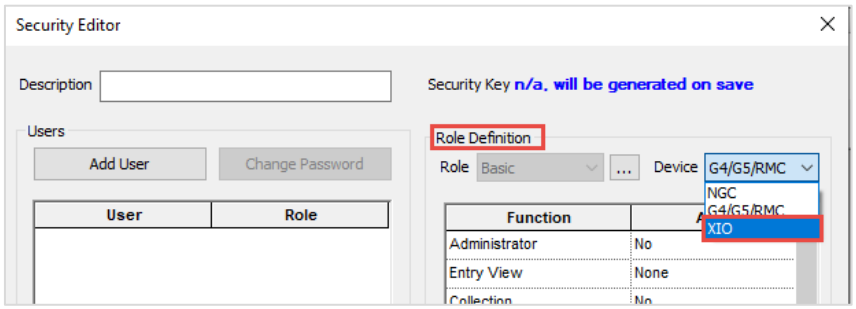
1. Launch PCCU32.
2. Click **Operate** > **Security** > **Role Based Access Control** > **Role Administration** on the toolbar. The Security Editor window displays.

Figure 7-5: Role based access control security editor



3. Under the Role Definition section, click the **Device** drop-down list and select: **XIO**.

Figure 7-6: RBAC role definition for XIO



4. Click **Yes** to confirm device type change.
5. Create the RBAC:
   a. Verify that the Role displays **Administrator**.
   b. Click **Add User**.
   c. Type the user name into the Name field.
   d. Type the password into the Password field.
   e. Click **OK**.
5. Follow the procedures detailed in section 7.6.4 Create a new user account to create user accounts with standard roles or to define or customize a role. Return here to complete this procedure.

6. To assign RBAC security to a communication port, see section 7.6.5 Enable RBAC authentication on communication ports.
7. Type a description of the security file into the Description field.
8. Click **Save As** to save the new security control file.
9. Type a password for the security file and click **OK**. The Save Security File dialog displays.
10. Navigate to the appropriate folder, then rename the file as necessary.
11. Click **Save**.

IMPORTANT NOTE: The Security Key displays at the top right corner of the Security Editor dialog. This key displays "n/a will be generated on save" before the security file is saved for the first time, or after changes. After saving, a new security key is assigned and logged into the Security Log. A copy of the security file is saved to the PC connected to the device. The previous key disappears after modification, and a new one replaces it. The new key and the security control file are automatically logged and saved to the PC. The security control file saves to the PCCU > RBAC folder on the PC and has a default file name tfsrf.rba.

7.6.3 Edit the security file

To edit an existing security control file:

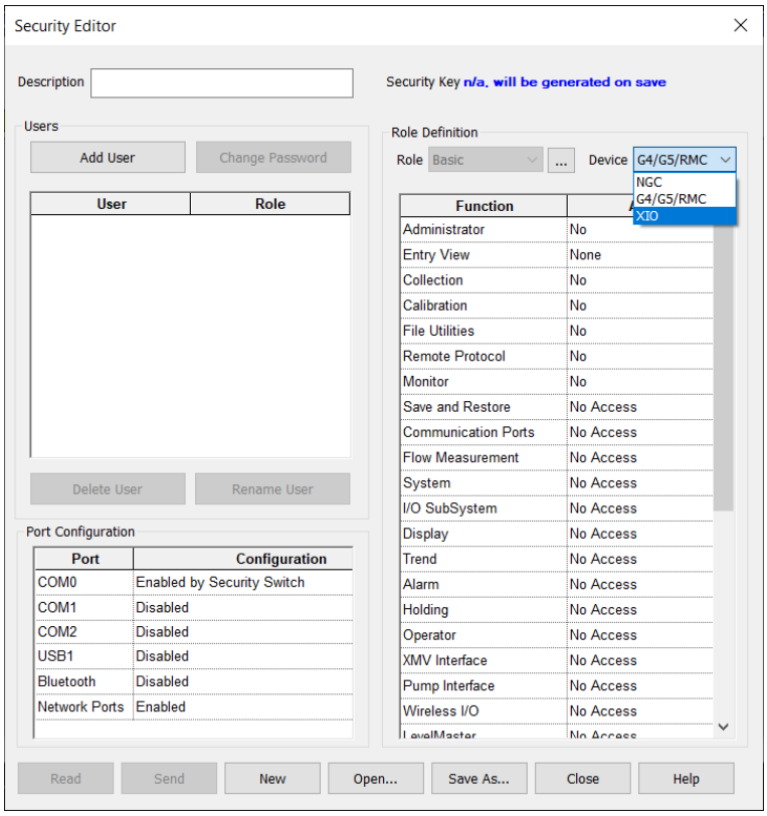
1. Launch PCCU32.
2. Click **Operate** > **Security** > **Role Based Access Control** > **Role Administration** on the toolbar. The Security Editor window displays.
3. Click **Open** to display the Open Security File navigation dialog.
4. Browse to **PCCU** > **RBAC** > [file name.rba]. Click **Open**.
5. Make the necessary changes.
6. Click **Save As**. The Security File Password dialog displays.
7. Type a password for the security file. Click **OK**.
8. Navigate to the folder, then rename the file. Click **Save**.

7.6.4 Create a new user account

To add a new user to the RBAC security system:

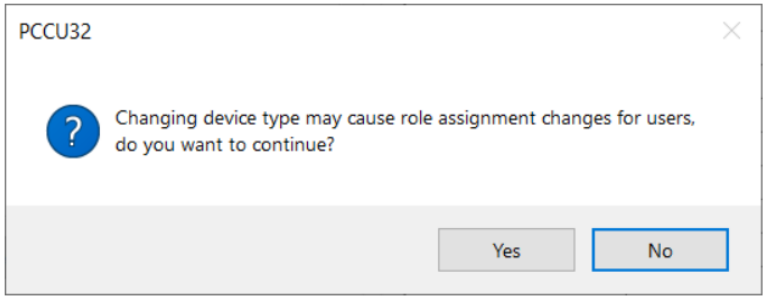
1. On the Security Editor screen, select **XIO** from the Device drop-down list.

Figure 7-7: RBAC select XIO



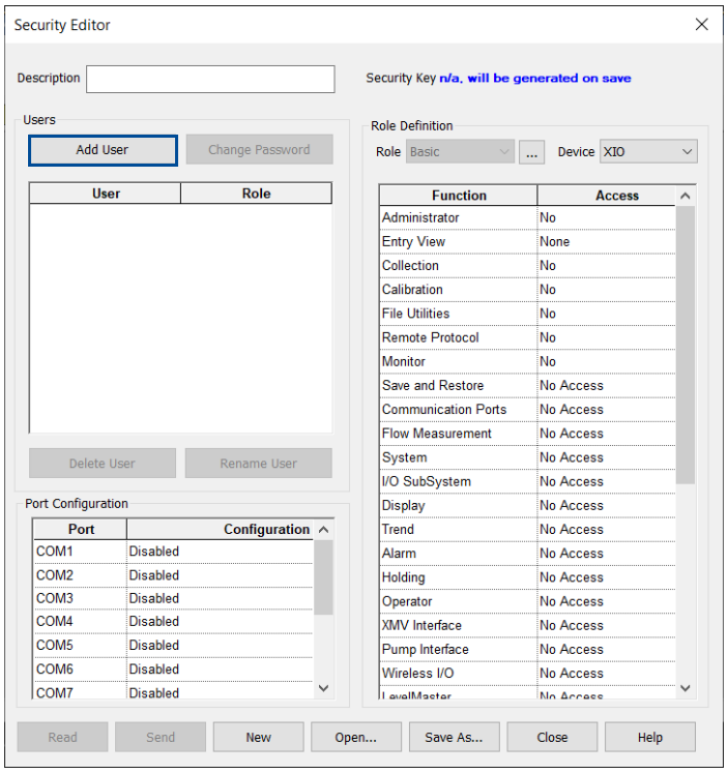
2. A dialog asks to confirm changing device type. Click **Yes**.

Figure 7-8: RBAC confirm XIO selection



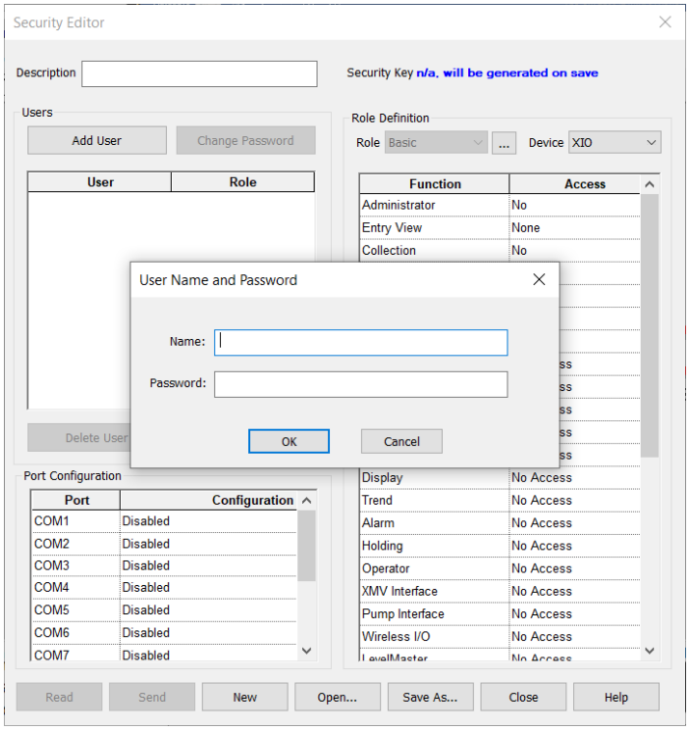
3. The Security Editor now displays the Device as XIO. Click **Add User**.

Figure 7-9: Add User in Security Editor



4. Type the user name into the Name field.

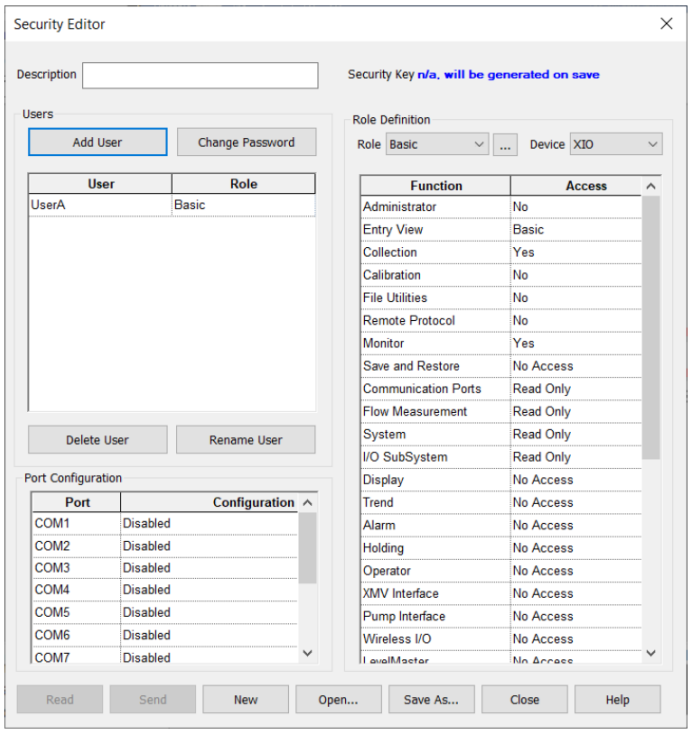
Figure 7-10: Type user name and password



5. Type the user password into the Password field.

6. Click **OK**. The new user account displays on the list of users.

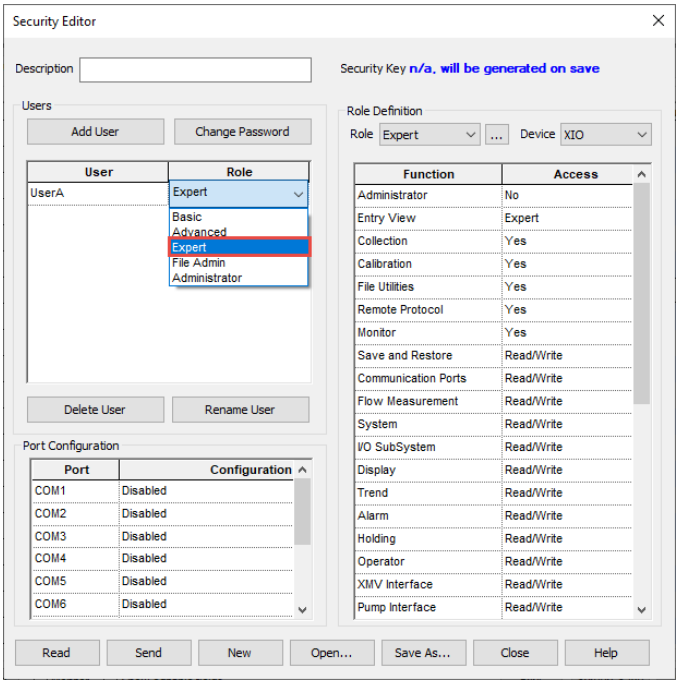
Figure 7-11: New user added to list in Security Editor



7. Click **Role** beside the new user account and select the appropriate role from the drop-down list.

IMPORTANT NOTE: During the initial setup, no customized roles exist. Create at least one additional user account before creating a customized role. Then assign the new role to a new or existing user account.

Figure 7-12: User role assignment



8. Repeat steps 3 through 7 for each user account.
9. Click **Save As** to save and name the new security control file.
10. Type a password for the security control file in the Password field and click **OK**.

7.6.5 Enable RBAC authentication on communication ports

Enabling RBAC authentication on communication ports secures access to the device. Connection to the ports requires authentication with correct credentials. Select one of the methods described in this section. Review the authentication options in Table 7-7.

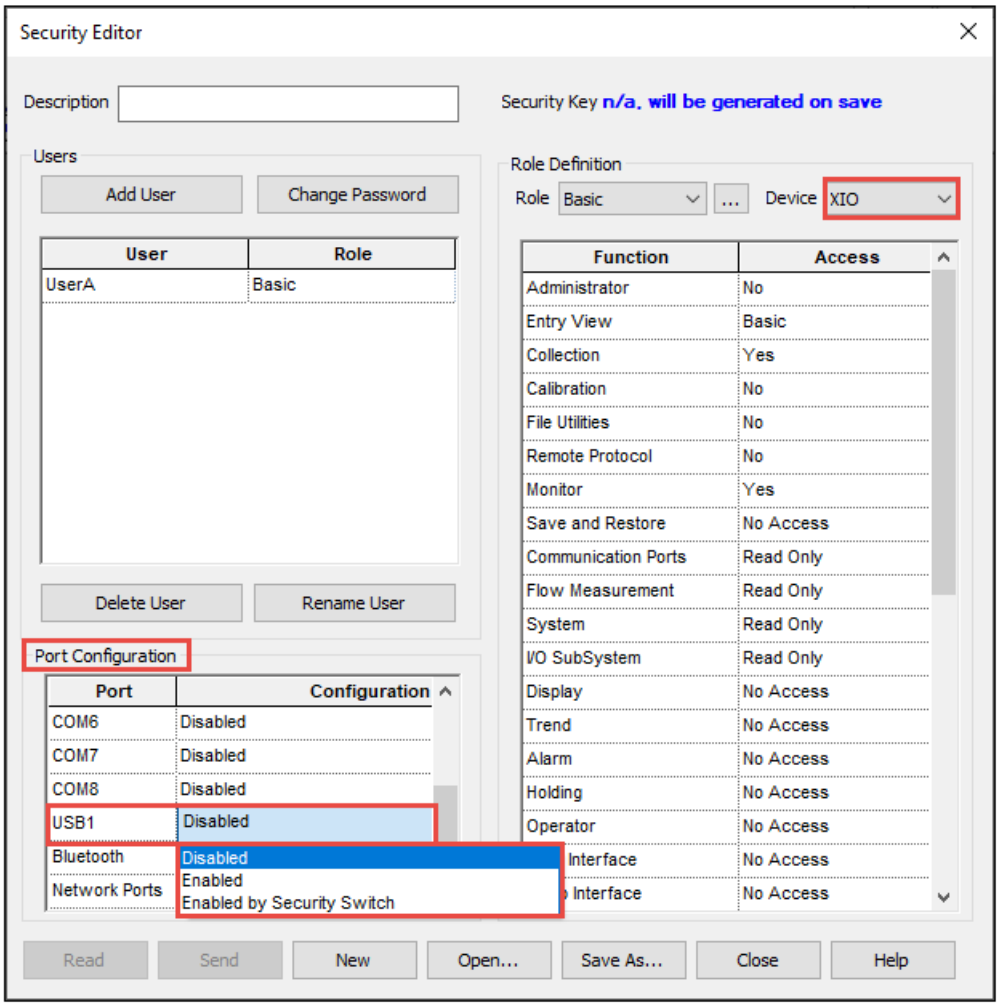
Table 7-7: Per-port RBAC authentication options

Port security setting	Functionality
Disable	Does not perform any RBAC security functions on the port.
Enable	Enable full security over the port for RBAC. Keep records of access credentials and safeguard them. If the administrator name or password are lost, you must reset the device with the factory default configuration. If you restore the factory defaults it deletes all data and the running configuration. See section 8.5.8 Factory restart from the device loader for additional details.
Enable by Security Switch	Enable security over the port for RBAC but allow the electronic board security switch to override RBAC security. If the administrator name or password are lost or forgotten, use the security switch to disable the RBAC. If the switch is off, log in and reconfigure the security access. No data is lost. See section 7.6.5.2.

7.6.5.1 Enable authentication from the RBAC security editor

1. Select the preferred authentication option for each port (see Figure 7-13).
2. Click **Save As** to save changes to the security control file.
3. Type the password for the security control file into the Current Password field. Click **OK**.

Figure 7-13: Enable port authentication from RBAC security editor



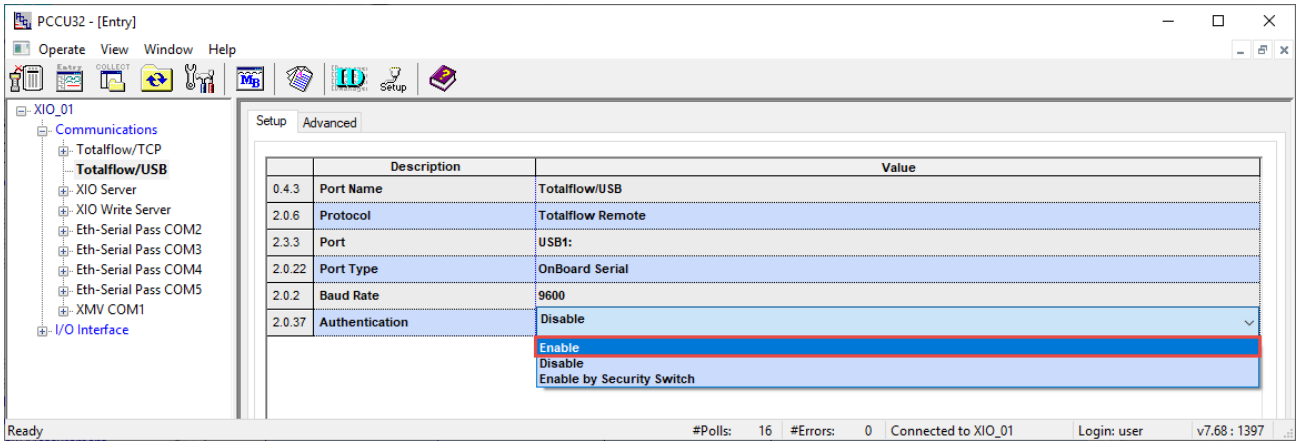
7.6.5.2 Enable authentication from the Entry mode

Enable RBAC authentication method for each required port.

Use entry mode in Advanced or Expert view to configure or override communication port security:

1. Launch PCCU and connect with the XIO in **Entry** mode. The navigation tree displays.
2. On the navigation tree, click the communication port. The Setup screen displays.
3. From the Authentication drop-down list, select **Enable** or **Enable by Security Switch** (Figure 7-14).
4. Click **Send**.
5. Repeat steps 2 through 4 for each of the communication ports.

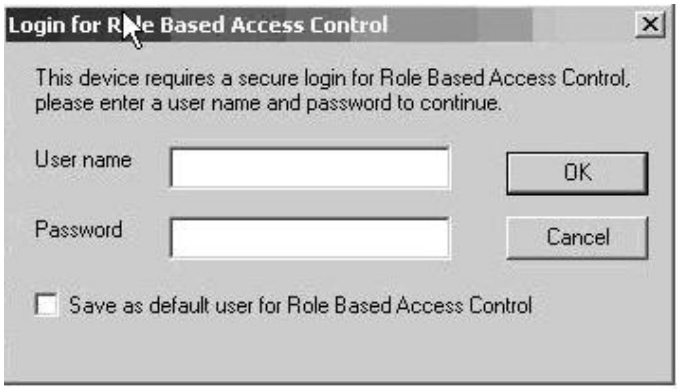
Figure 7-14: Enabling communication port authentication - Entry mode (on USB port)



7.6.5.3 Use default RBAC credentials

A login screen requires the User name and Password to connect PCCU to a flow computer through an RBAC-enabled port.

Figure 7-15: Login dialog box

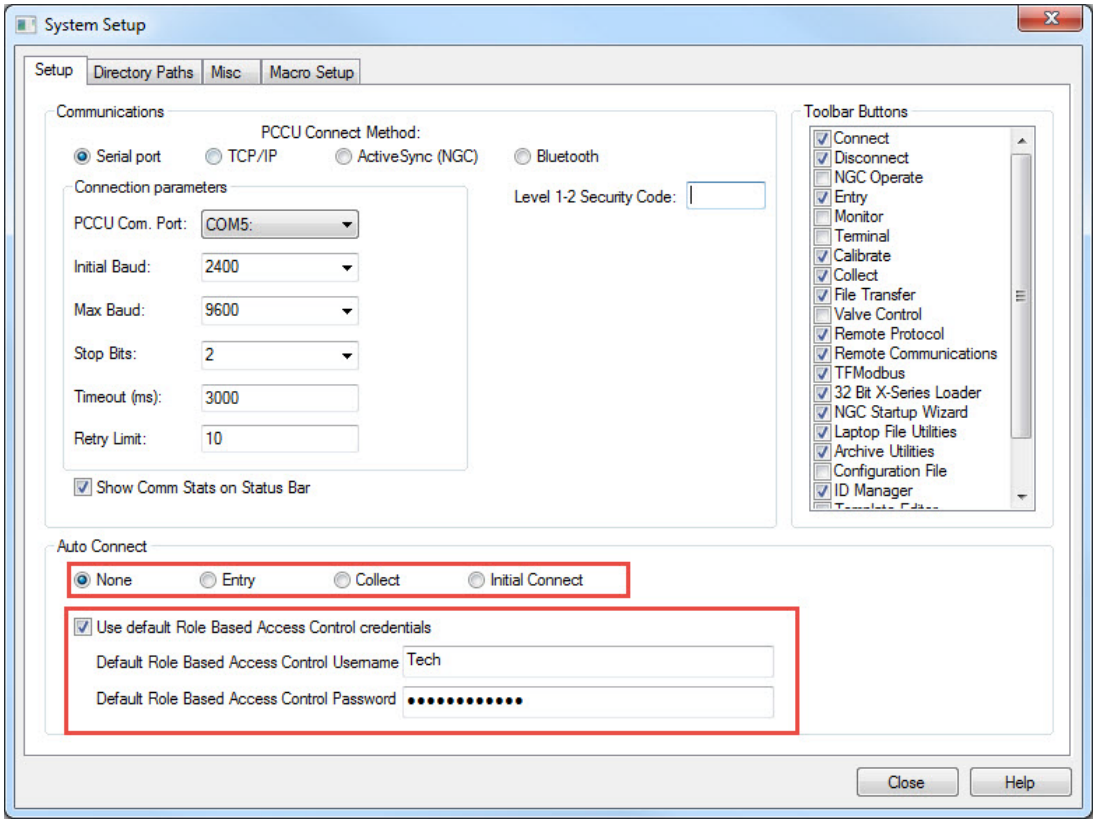


Set the User name and Password as default credentials in PCCU, if necessary. The User name and Password fields autofill with the default credentials on subsequent logins.

To create, change or disable the RBAC credentials in PCCU:

1. Click **Setup** on the toolbar or click **Operate** > **Setup** > **System Setup**.
2. In the Auto Connect section (Figure 7-16), set the defaults:
   a. Select **Entry**, **Collect**, or **Initial Connect**. Click **Help** for additional details.
   b. Select **Use Default Role Based Access Control credentials**.
   c. Type the user name into the Default Role Based Access Control Username field.
   d. Type the password into the Default Role Based Access Control Password field.

Figure 7-16: System Setup Auto Connect and RBAC credentials



3. Click **Close** to exit PCCU connection setup.

7.7 Secure the SSH/SFTP service

XIO devices implement the Secure Shell (SSH) and Secure File Transfer Protocol (SFTP) service. This provides SSH login access and file transfer capability from a client PC or laptop.

SSH/SFTP provides secure access, instead of the unsecured access of Telnet and FTP in earlier device generations.

SSH/SFTP communication is client-server based. The SSH/SFTP client is implemented in third-party software on the computer that communicates with the XIO device.

When the SSH/SFTP service is enabled, the SSH/SFTP server initializes and enters listening mode. In listening mode, the server can process requests for connection from SSH/SFTP clients. The service allows connections to properly authenticate clients.

7.7.1 Supported SSH/SFTP accounts

The table below lists the three SSH/SFTP accounts. Customers can access the Totalflow-user account, which is read-only. The developer and tech-support accounts are only available to ABB personnel for service and troubleshooting, or to advanced users and cybersecurity managers who want to generate private keys to replace factory default keys.

IMPORTANT NOTE: Call ABB Customer Support to request Totalflow-user account default private keys. See the SSH and SFTP service overview topic in PCCU online help for instructions to establish read-only SFTP connections.

Table 7-8: Security keys

Account Name	Access privileges	Default keys	Access
Totalflow-user	Only SFTP access (Read-only)	Totalflow-user private key	The following folders and contents are available for download: — Crash Dumps — Flash: Main Totalflow application (App), Factory configuration, Startup (cold) configuration — Logs: System and device loader log files — tfData: Running (warm) configuration files

7.7.2 SSH/SFTP authentication

Session keys encrypt the communication between the client and the SSH/SFTP server to provide security. Authentication requires specific private-public key pairs for the type of access. ABB provides default private keys and passphrases to customers upon request. ABB stores the default public keys at the factory in a protected storage location on the device's flash. They remain unchanged by updates.

To request a connection to the SSH/SFTP service, provide the private key and passphrase. The service compares the private key with the public key stored in the Totalflow device. If the keys pair correctly, the connection is successful.

IMPORTANT NOTE: Private keys do not ship with the product or user interface software. ABB keeps the keys and credentials safely stored. Request keys for SSH/SFTP access. Enable the service only if necessary.

7.7.3 Update default SSH/SFTP keys

ABB Totalflow generates default keys, but customers must generate their own private keys for security reasons. To update the private key, first update the corresponding public key stored on the XIO device. This procedure describes how to regenerate a private key and update the corresponding public key on the device.

IMPORTANT NOTE: Only permit an authorized expert user to perform this procedure. This procedure requires developer or tech-support access. Failure to follow the procedure in its entirety locks access to the SSH/SFTP service. To obtain default keys for this type of access, call ABB Customer Support.

7.7.3.1 Update requirements

The key update requires third-party software.

Obtain the following before update:

- Third-party software, such as PuTTYgen, to generate new keys. Download PuTTYgen as part of a putty package or as a standalone utility.
- Third-party SFTP client software to establish SFTP connections with the device (FileZilla).
- Latest PCCU from ABB. Download PCCU from www.abb.com/upstream.
- The private keys for developer or tech support accounts, and their respective passphrases for SFTP. To change the keys for the first time, request the default keys from ABB. Otherwise, use previously-updated keys.

IMPORTANT NOTE: There are other options for the third-party software. PuTTYgen and FileZilla are examples. The update procedure is similar with other software.

7.7.3.2 Generate private-public key pair

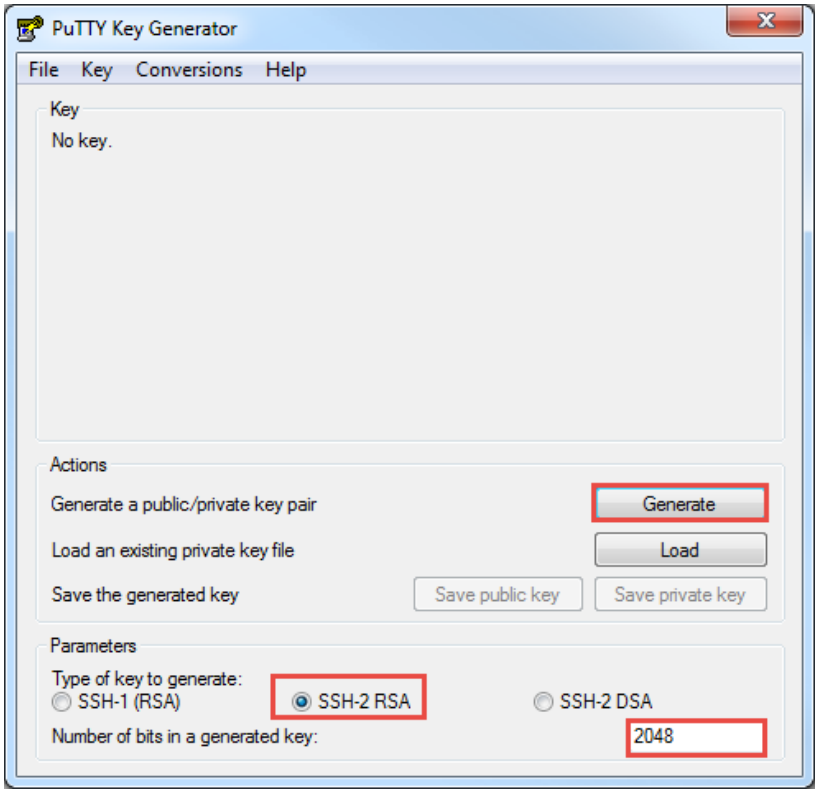
This procedure generates and saves a new private-public key pair. The private key, passphrase and public key are stored safely on the user’s laptop or PC. The public key must also be saved in the XIO device. The

new private key and its passphrase are necessary to access accounts after the update of a device's corresponding public key.

To generate new keys:

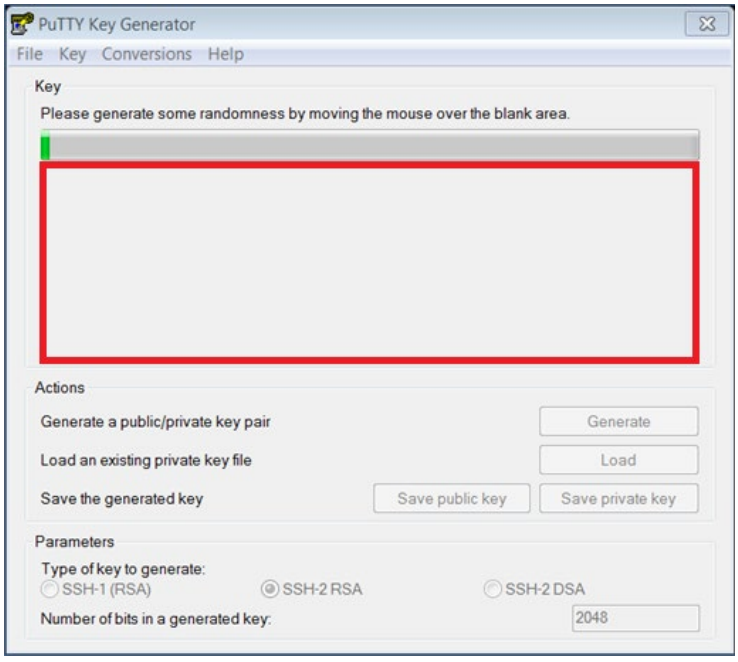
1. Download and install the latest version of PuTTYgen from the link in section 7.7.3.1, Update requirements.
2. Launch the PuTTYgen application. In the PuTTYgen Key Generator window, verify that the "Type of key to generate" is set to **SSH-2 RSA**, and "Number of bits in a generated key" is set to **2048**. Click **Generate**.

Figure 7-17: PuTTYgen Key Generator



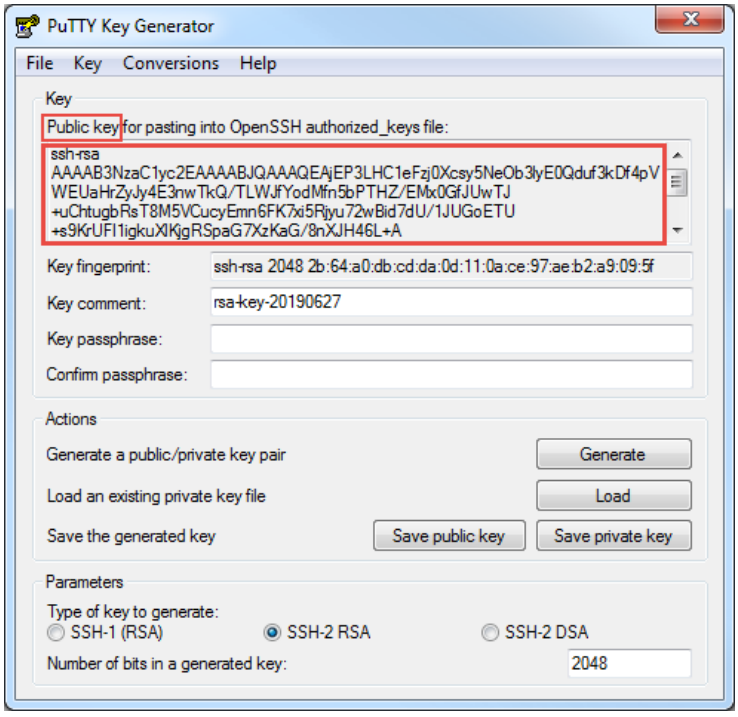
3. The image below illustrates the Key blank field. Hold the mouse over that field to prevent delays in key generation.

Figure 7-18: PuTTYgen Key Generator Key blank field



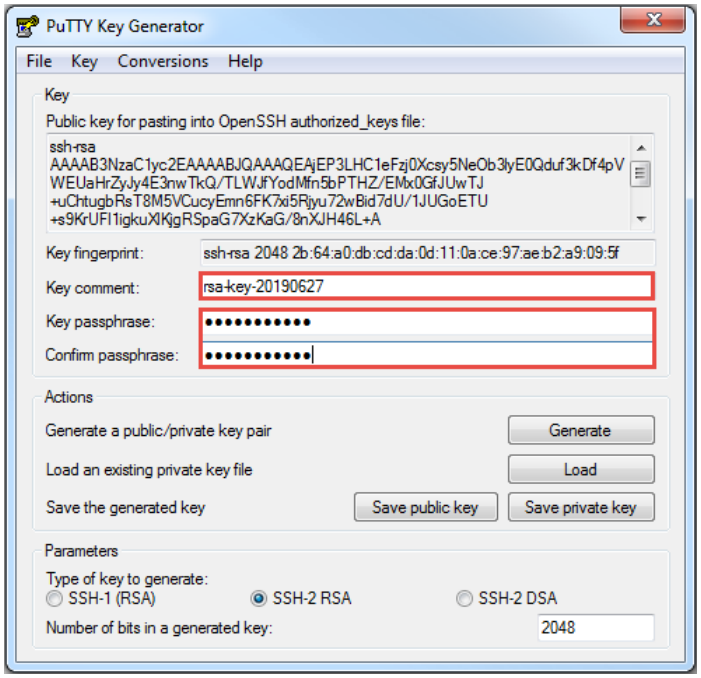
4. Allow the program to generate the new key. The progress bar reaches 100%. The Key field displays the new public key.

Figure 7-19: New public key



5. Accept the key description in Key comment or type a new one into the field.
6. Create a strong private passphrase and type it into the Key passphrase field and the Confirm passphrase field.

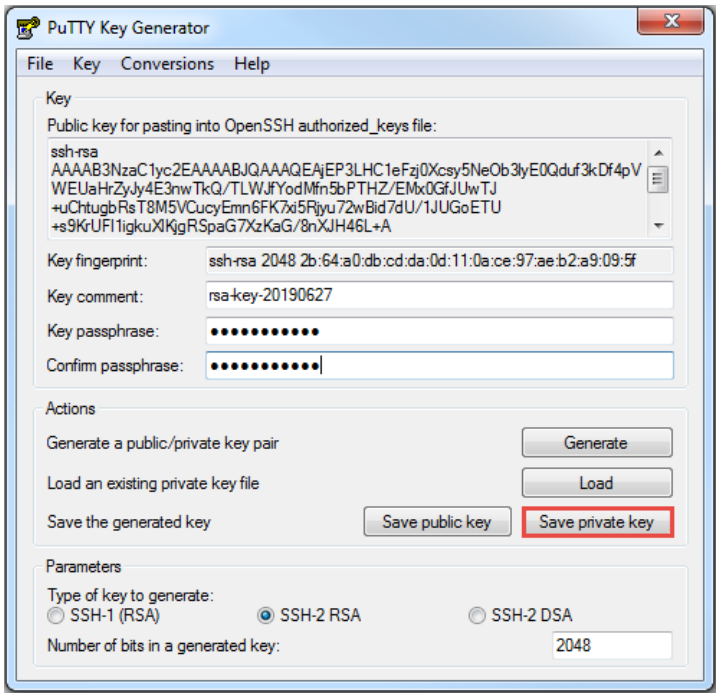
Figure 7-20: New private key comment and and passphrase



7. Click **Save private key** (Figure 7-21).

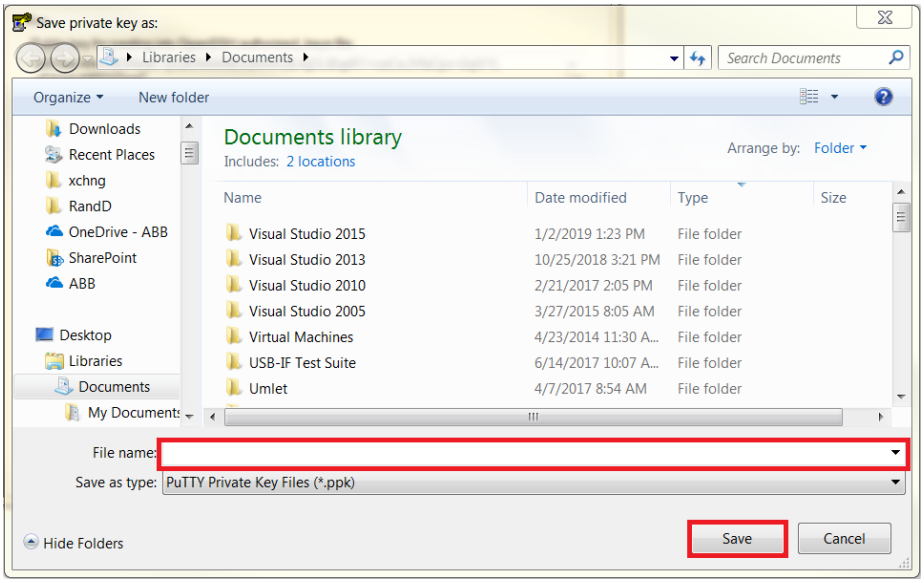
IMPORTANT NOTE: The PuTTY Key Generator generates the private key but does not display it on the screen.

Figure 7-21: Save private key and passphrase



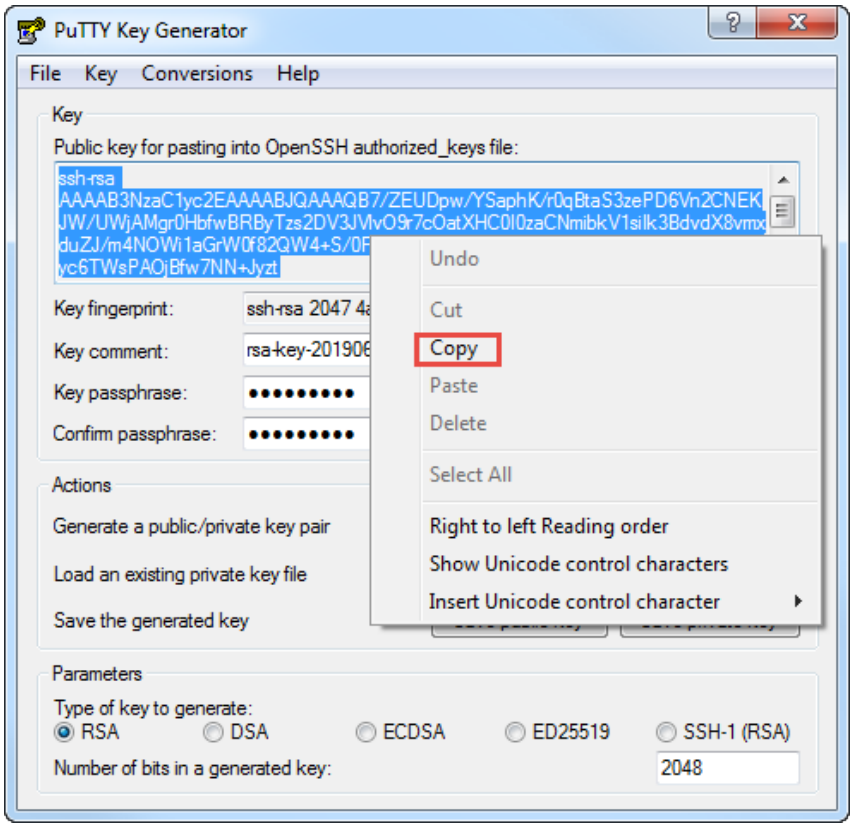
8. Navigate to the correct folder and type the File name. The private key file has a .ppk extension. Use this new private key and passphrase to access the accounts after an update to the public key.

Figure 7-22: Select location to save private key file



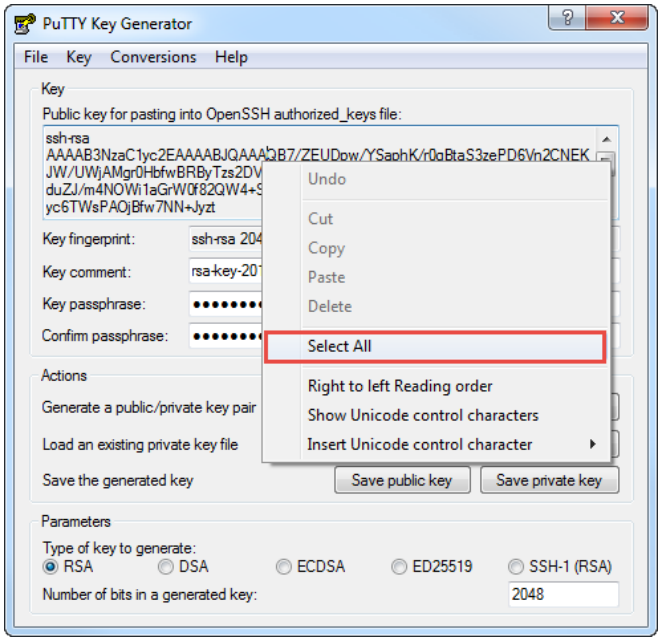
9. Click **Save**. The file browser closes.
10. Right-click the text in Public key for pasting into OpenSSH authorized key file. Click **Copy** (Figure 7-23).

Figure 7-23: Copy public key from the Key field



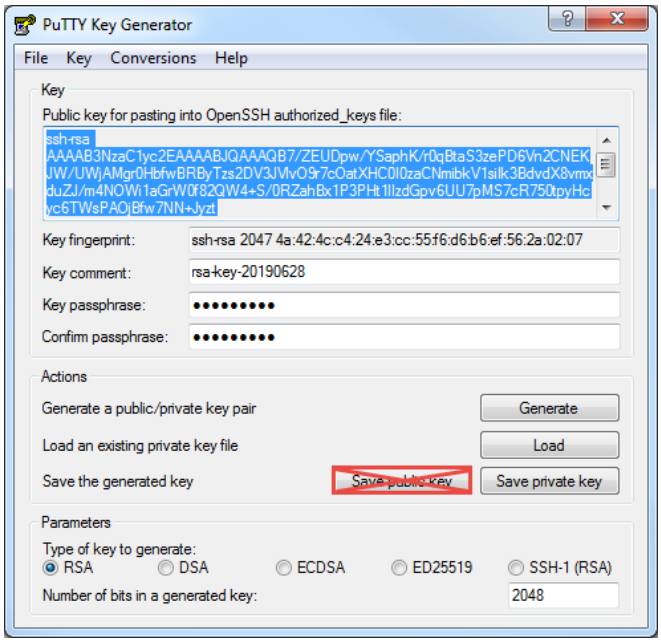
IMPORTANT NOTE: If the public key text is not highlighted, right-click the text and click **Select All** (Figure 7-24). Then click **Copy**.

Figure 7-24: Select generated public key text



IMPORTANT NOTE: Do not click Save public key on the PuTTY Key Generator dialog (Figure 7-25:).

Figure 7-25: Do not save public key from the PuTTY Generator dialog



11. Create a new text file on your laptop or PC and paste the copied public key contents into this file.
12. Save the text file. Use one of following file names based on the account type:
    - **userkey.txt**: A key with this name appends to the available Totalflow user public keys in the device. The Totalflow user account is accessible after the key update operation, either with the newly created private key or the previous set of private keys for the Totalflow user account.
    - **rootkey.txt**: A key with this name appends to the available developer and tech support public keys in the device. The developer and tech support accounts are accessible after the key update operation with either the newly created private key or the previous set of private keys for developer and tech support accounts.

The key generation is complete. A key file with the .ppk extension stores the new private key. A corresponding public key text file has one of the two names, above.

IMPORTANT NOTE: Follow steps 1 through 12 for each key to generate new user and root keys.

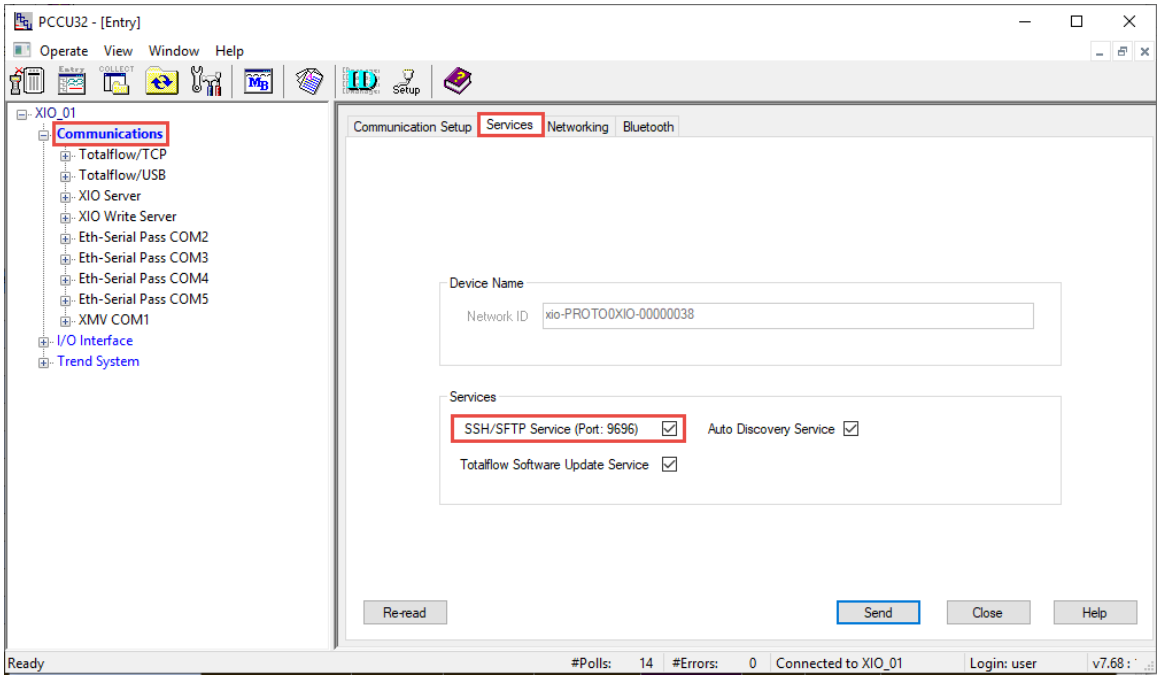
7.7.3.3 Update public keys on device

This procedure saves the new public key on the XIO device. The new key appends to an existing key. This procedure requires a TCP/IP-based connection with the device. Verify that the device has a valid IP configuration. The valid IP configuration depends on the type of connection. An Ethernet network or point-to-point connection may be used for this procedure.

To save the public key:

1. Download and install the latest version of FileZilla from the link provided in section 7.7.3.1, Update requirements.
2. Connect to the device's MMI or USB port.
3. Launch PCCU and click **Entry** on the toolbar.
4. On the navigation tree, select **Communications**.
5. Select **Services**.
6. Select **SSH/SFTP** service.

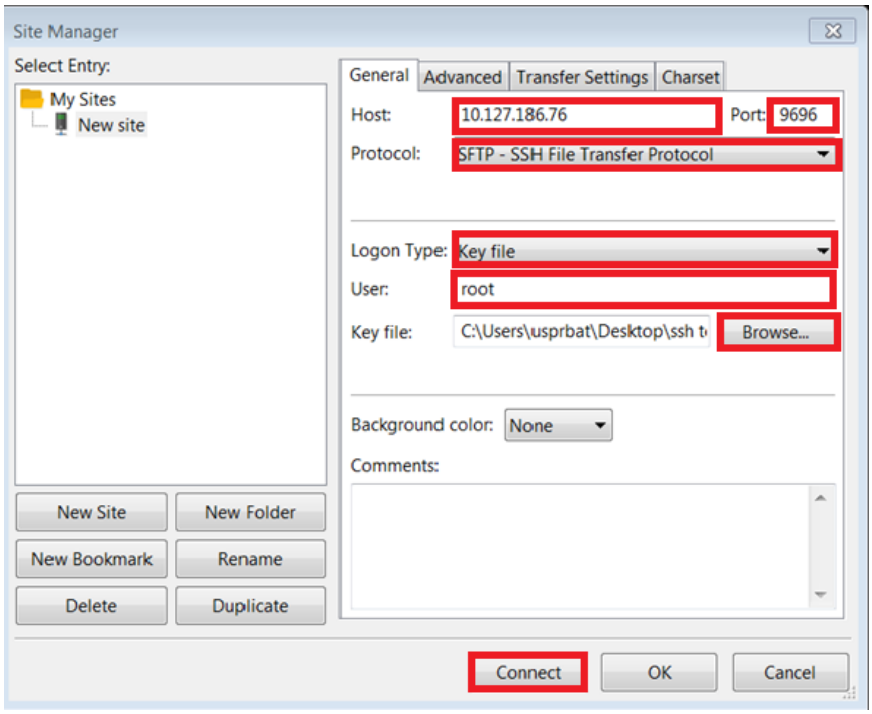
Figure 7-26: Enable the SSH/SFTP service



7. Click **Send**.

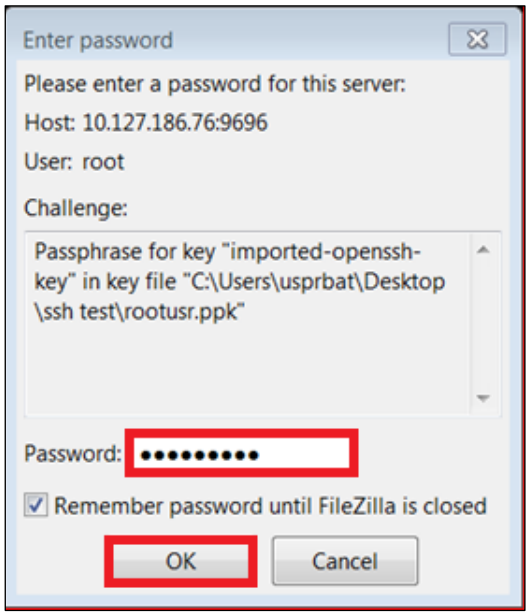
8. Click **Networking** to display the Networking tab and enable, verify, or configure IP parameters. Use a valid IP configuration to access the device over a network. Configure the device to use a local point-to-point to connection, as necessary. Click **Help** for additional details.
9. Click **Send** to save changes.
10. Connect the XIO device to the network, the laptop, or PC (if the Ethernet connection is local). Keep the serial or USB connection open.
11. Launch the FileZilla application.
12. Click **Open the Site Manager**. The Site Manager dialog displays (Figure 7-27).

Figure 7-27: FileZilla Site Manager connection setup



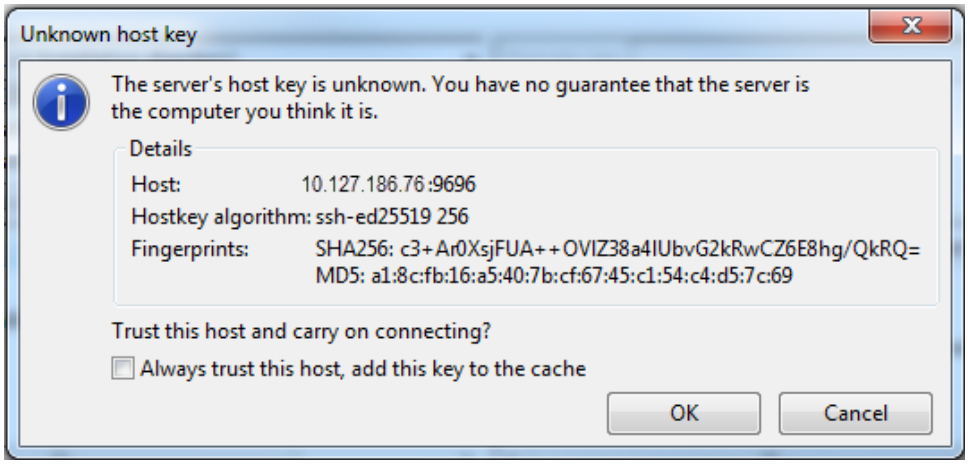
13. Configure the General tab parameters:
    - Host: Type the device's IP address.
    - Port: Type **9696**.
    - Protocol: Select **SFTP - SSH File Transfer Protocol** from the drop-down list.
    - Logon Type: Select **Key file** from the drop-down list.
    - User: Type **root**.
14. Click **Browse** to select the current private key. If this is the first time the keys are changed, use ABB's default developer or technical support private key.
15. Click **Connect**. If the private key is passphrase-protected, a window displays and requests the passphrase before allowing the connection (Figure 7-28).
16. Type the passphrase into **Password**. (Figure 7-28). Use the passphrase provided by ABB or update the key and create a unique passphrase.

Figure 7-28: Type private key passphrase (password)



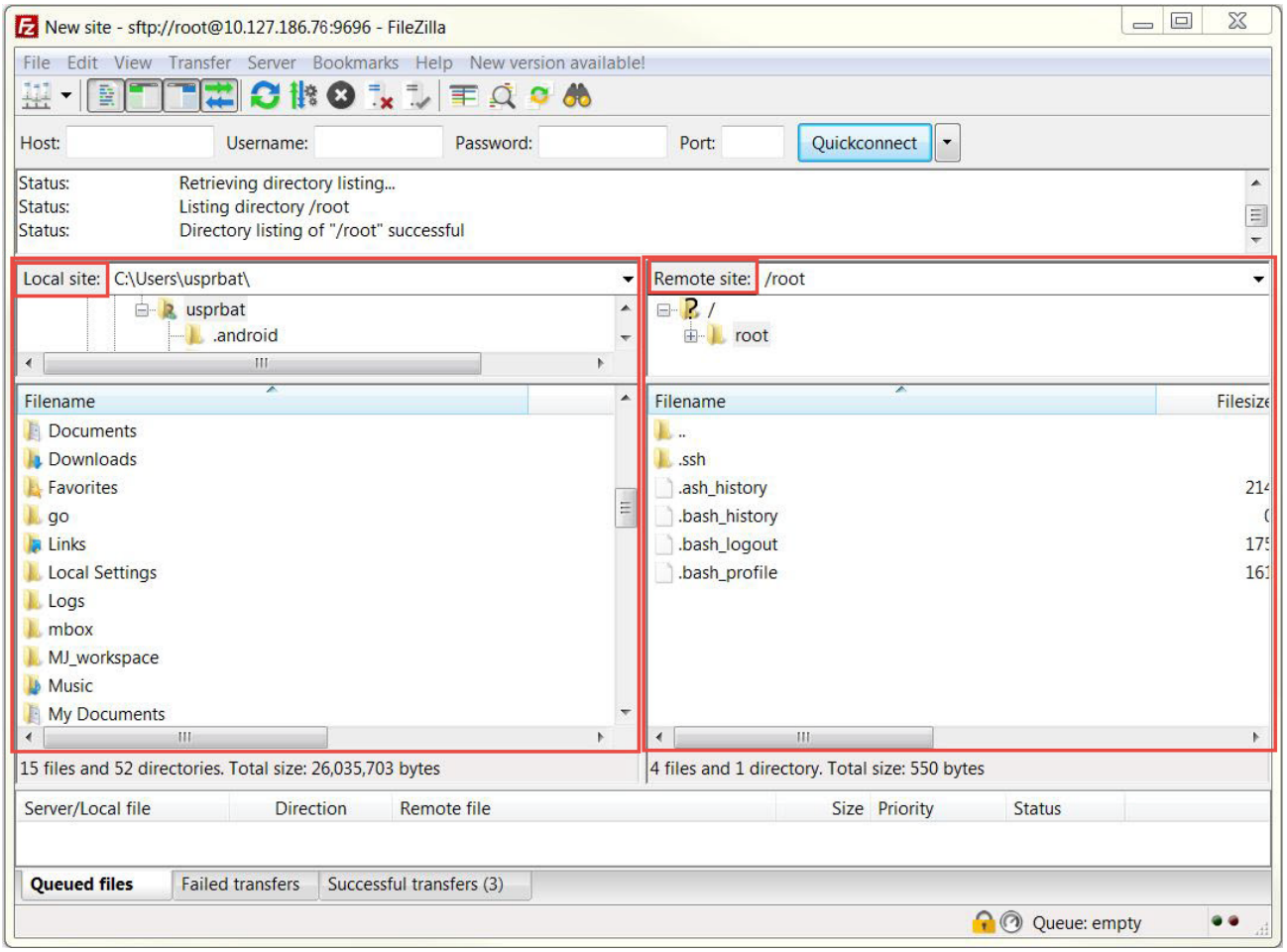
17. Click **OK.** The laptop issues a warning the first time it tries to connect to the device (Figure 7-29).

Figure 7-29: Unknown host key warning



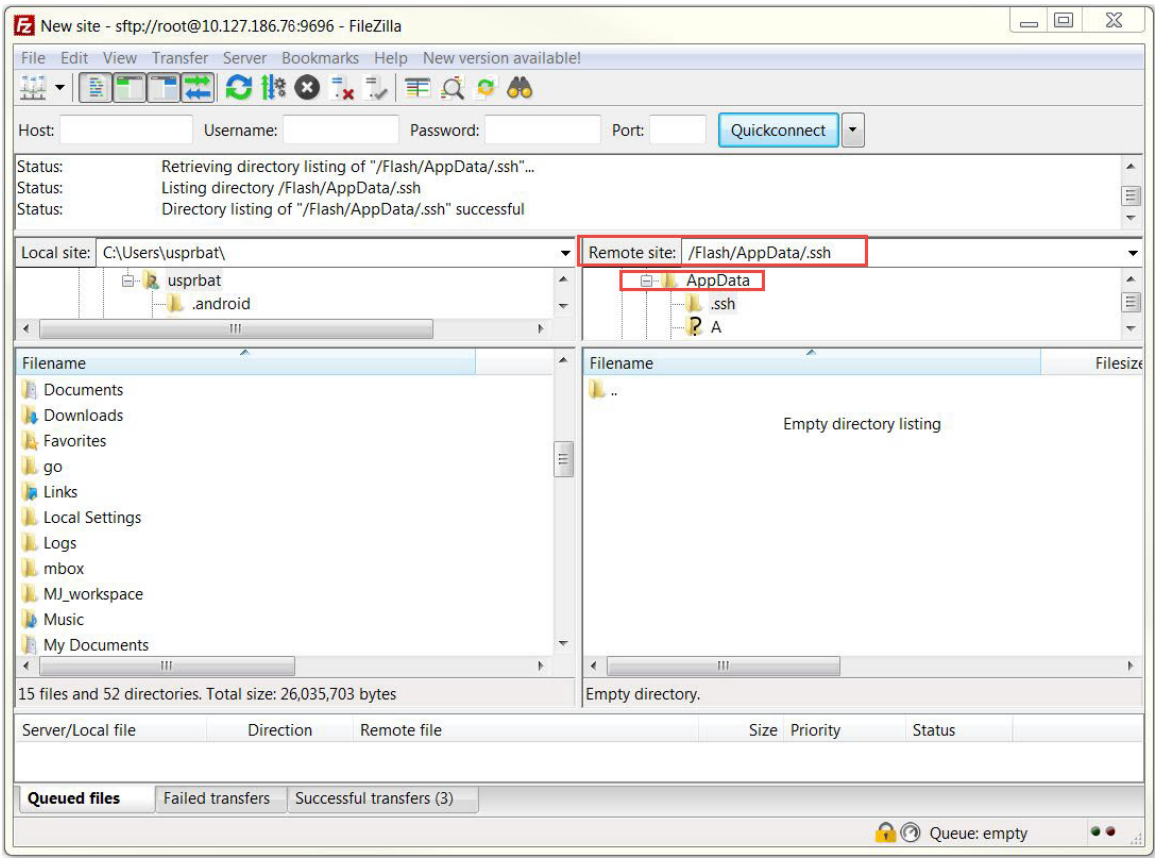
18. Click **OK.** The connection with the device is successful when FileZilla displays the file directories of the laptop or PC (Local Site, on the left) and the device (Remote site, on the right) (Figure 7-30).

Figure 7-30: FileZilla New Site window



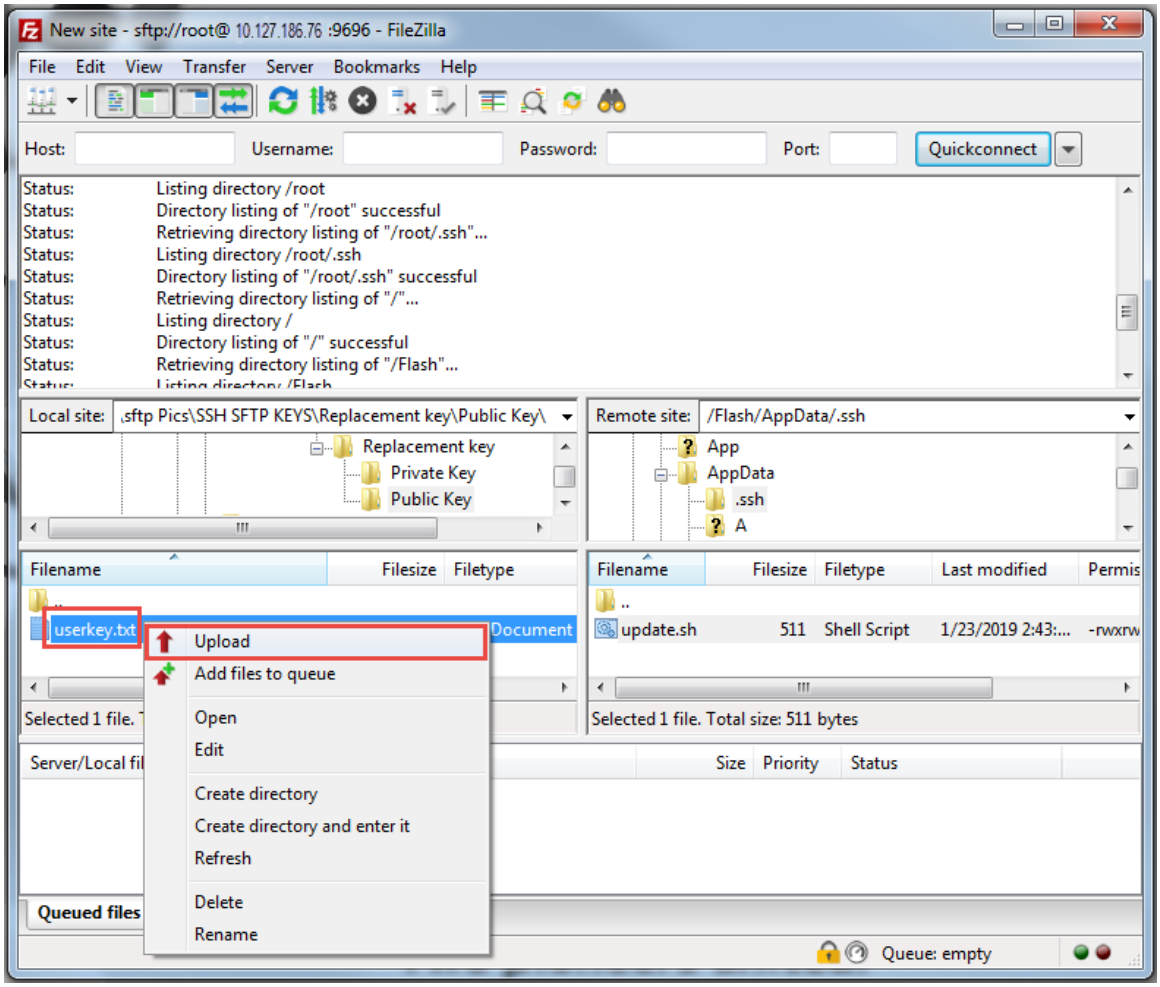
19. Navigate to the directory containing the newly created public key text file (on the left) and open it.
20. On the Totalflow device, navigate to the /**Flash**/**AppData**/.**ssh**/ directory. The device updates the keys only if it finds them in them in the specified directory.

Figure 7-31: Open the /Flash/AppData/.ssh/ directory



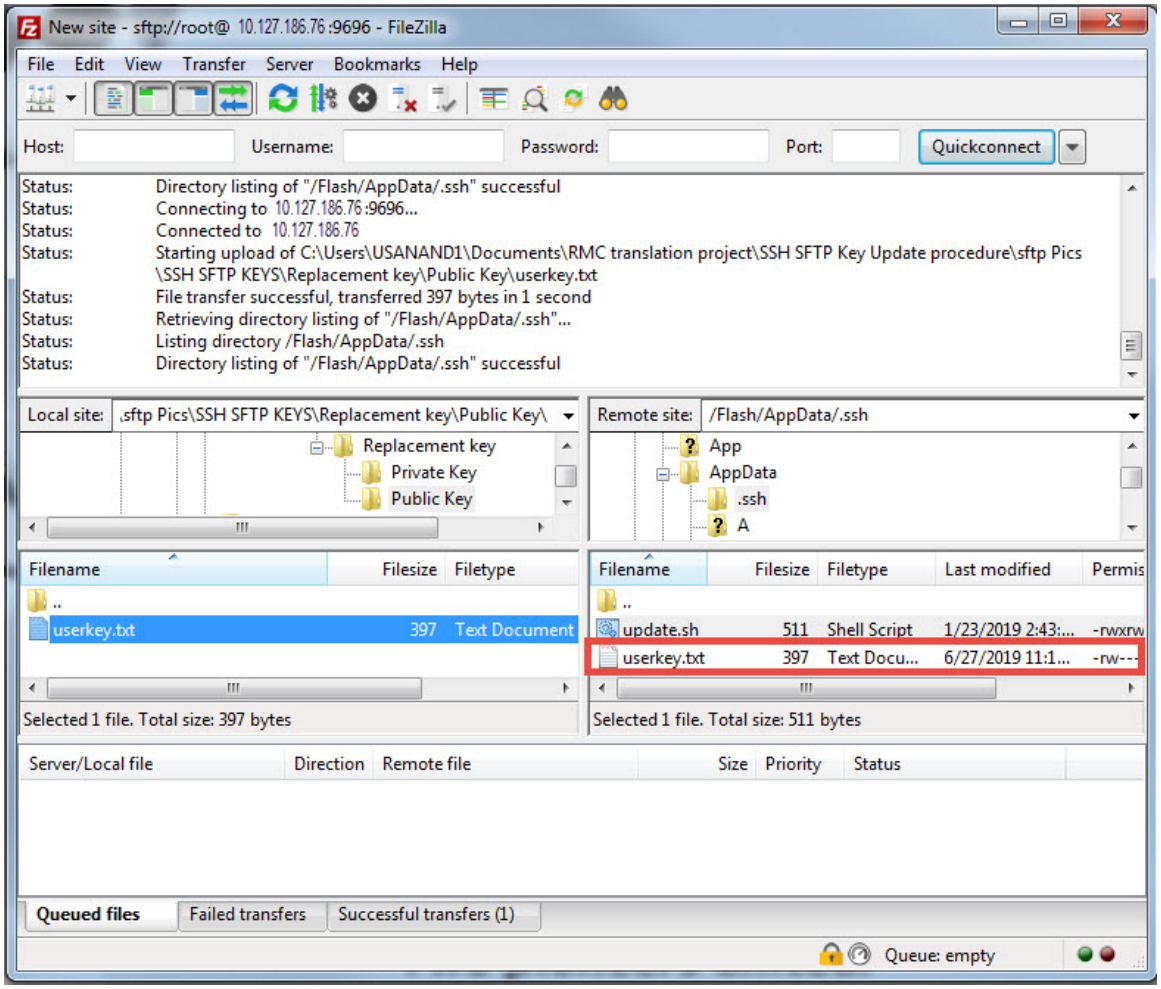
21. In the Filename window, right-click on the new public key file. Select **Upload** from the drop-down list.

Figure 7-32: Upload public key from laptop to device



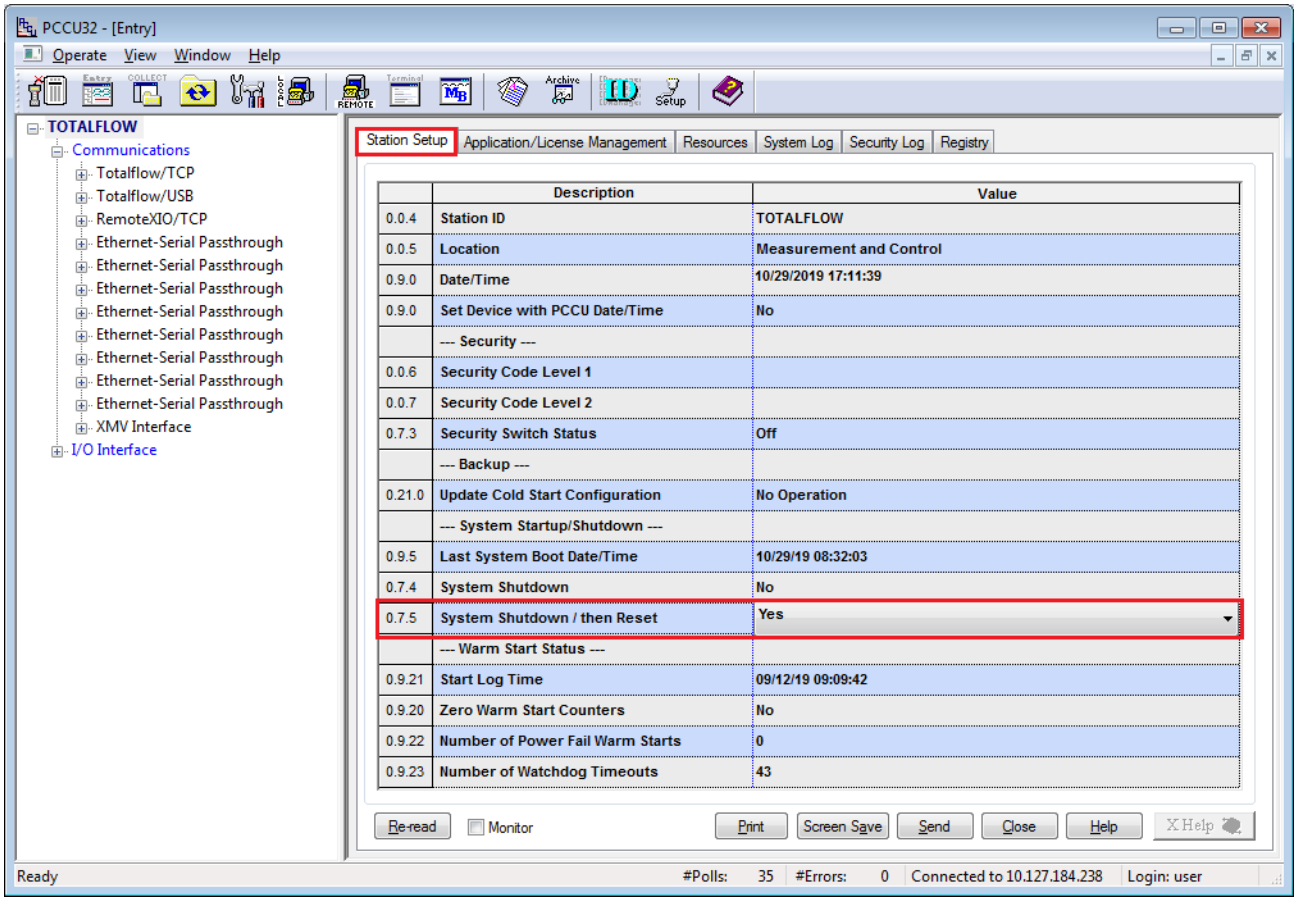
22. Verify that the file copied to the /Flash/AppData/.ssh/ directory. The name of the file displays under that directory when the upload is complete.

Figure 7-33: Verify public key upload is complete



23. Restart the device to activate the public key update (Figure 7-34).
24. Launch PCCU and click **Entry** to display the Entry Mode screen. The navigation tree displays.
25. Click **View>Expert**. Then click **Yes** to close the warning dialog.
26. At the top of the navigation tree, click the Station ID. The Station Setup tab displays.
27. Scroll down and click the **System Shutdown/then Reset** Value field. Select **Yes** from the drop-down list.
28. Click **Send**. The device restarts and the FileZilla SFTP connection closes.

Figure 7-34: Restart Totalflow device after public key update



With the key upload complete, a new private-public key pair is available for authentication. Test the authentication with these new keys next.

7.7.3.4 Verify authentication with new private-public key pair

Verify that the public key update successfully established a new FileZilla SFTP connection with the new key and passphrase.

To verify:

1. Restart FileZilla.
2. Click Open the Site Manager.
3. Configure the General tab:
   - Host: Type the device's IP address.
   - Port: Type **9696**.
   - Protocol: Select **SFTP - SSH File Transfer Protocol** from the drop-down list.
   - Logon Type: Select **Key file** from the drop-down list.
   - User: Type the user required per account type (For the Totalflow user account, type **totalflow**. For the developer or tech support accounts, type **root**.)
4. Click **Browse** to locate and select the newly created private key.
5. Click **Connect**.
6. Type the private key passphrase into the passphrase prompt. FileZilla displays the device's file system directories.

IMPORTANT NOTE: Keep private key files stored in a safe location accessible only to authorized personnel and security managers.

7.7.4 Enable SSH/SFTP

SSH/SFTP servers require a private key for authentication. The keys are in a protected storage location in the firmware (flash) and remain unchanged by software updates.

Customer access to the SFTP is read-only. SSH access is not available to the customer. Customers can copy files from the XIO but cannot write or send files to the XIO.

The following folders are available to copy or download:

- Crash dumps
- Firmware: Main Totalflow application (App), factory startup (cold) configuration, and startup (cold) configuration
- Logs: System and device loader log files
- tfData: Running (warm) configuration files

IMPORTANT NOTE: SSH/SFTP services are disabled by default for security. Perform this procedure only if required and you are an advanced user. Before enabling, see section 7 Configure security (recommended) or contact Technical support.

SSH/SFTP access is TCP/IP based. Enable and configure Ethernet with valid IP parameters.

Complete these steps in PCCU Expert view. Click **View** on the PCCU32 menu and select **Expert** from the drop-down list.

To enable the SSH/SFTP services on the XIO:

1. Connect to the XIO using PCCU.
2. On the navigation tree, click **Communications**.
3. Click **Services** to display the Services tab.
4. Click **SSH/SFTP Service (Port: 9696)** to enable the services.
5. Click **Send** to save the configuration.

Click **Help** to display the **Services** tab topic for more information to establish a read-only SFTP connection.

8 Service and maintenance

The Service and maintenance chapter provides:

- Standard maintenance procedures, including software backup, restoration and upgrade
- Additional procedures that are required before or after a maintenance procedure

DANGER – Serious damage to health / risk to life. Do not perform maintenance when an explosive atmosphere is present.

WARNING – Bodily injury / Equipment damage. Remove power from the XIO if unit servicing requires removal or disconnection of cables or wires. Failure to remove power during service can cause bodily injury or equipment damage. Review warnings in Potential safety hazards.

NOTICE – Loss of data. Collect the data and back up the configuration before performing service on the controller. Failure to collect data and save the configuration can result in a loss of data and require a complete system configuration.

NOTICE – Equipment damage. The external power connections must be removed before removing all other cables, boards, and field connections. Connecting or disconnecting cables and wires on the XIO while power is applied can damage the electronic components.

Do not reconnect the external power connections until all other cables, boards and field connections have been reconnected.

8.1 Preserve data and configuration

It is very important to preserve data and configuration files before performing maintenance procedures or software upgrades. Follow the procedures in this section to back up the data and device configuration. Move collected data files to other systems for safekeeping or import into customer databases.

Saved configuration files preserve the configuration of all the applications operating in the device. This saves a considerable amount of time reconfiguring complex applications in a device from scratch.

The procedure includes:

- Collect data (Trend data only)
- Update startup (cold) configuration
- Save startup (cold) configuration

8.1.1 Collect data

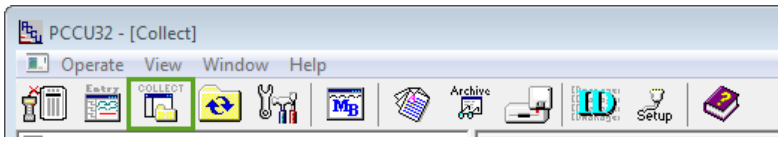
This procedure collects and saves the data to a file on a PC or laptop so that data in a device that has been in operation is not lost. The collect utility in the XIO supports saving trend data only. If no trends are configured on the XIO, skip this section.

IMPORTANT NOTE: Before collection, select the collected data from the several output types, including displaying the data on the screen. The system automatically creates a file containing the collected data and saves it for any output type selected. The default location of this file is the pccudata folder in the PCCU32 installation directory. The name of the collection file is the device station ID.

To collect the data from the XIO:

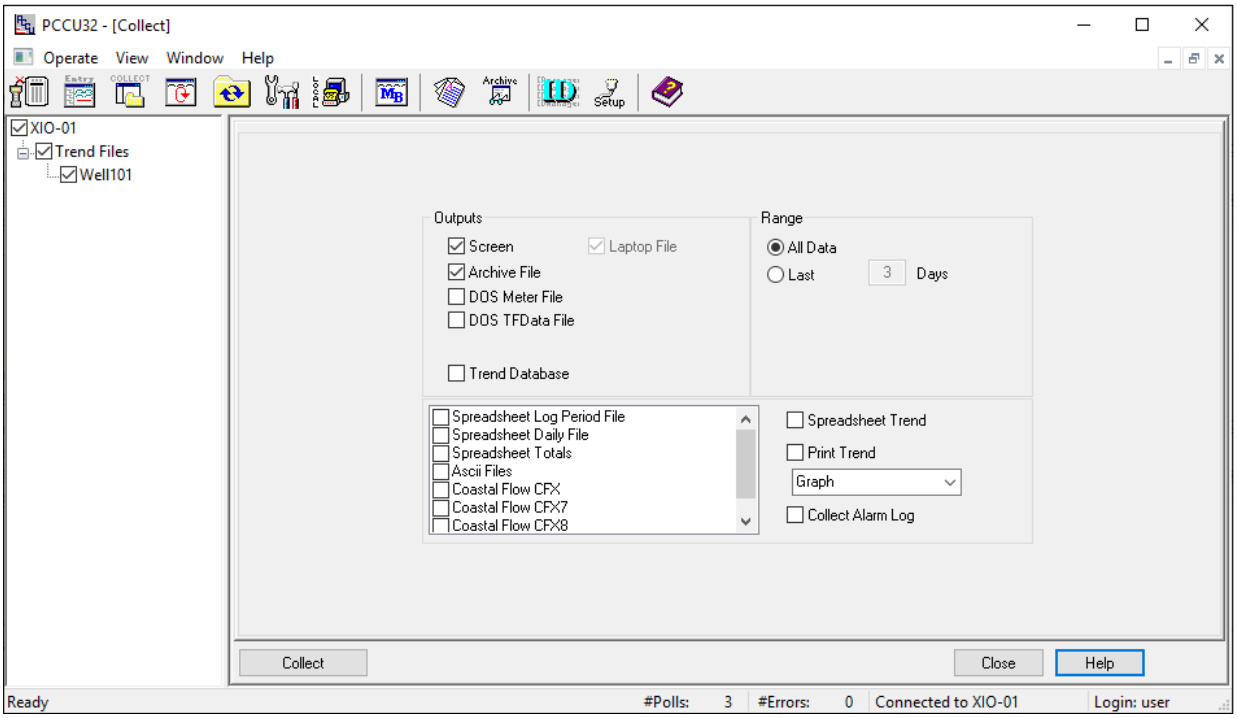
1. Connect the PC or laptop to the device (local communication) and launch PCCU32.
2. Click the **Collect** icon on the PCCU toolbar (Figure 8-1). The Collect screen displays (Figure 8-2).

Figure 8-1: Collect icon



3. Click one or more applications on the navigation tree to select them for data collection.
4. Click **Help** on the Collect screen for additional information.

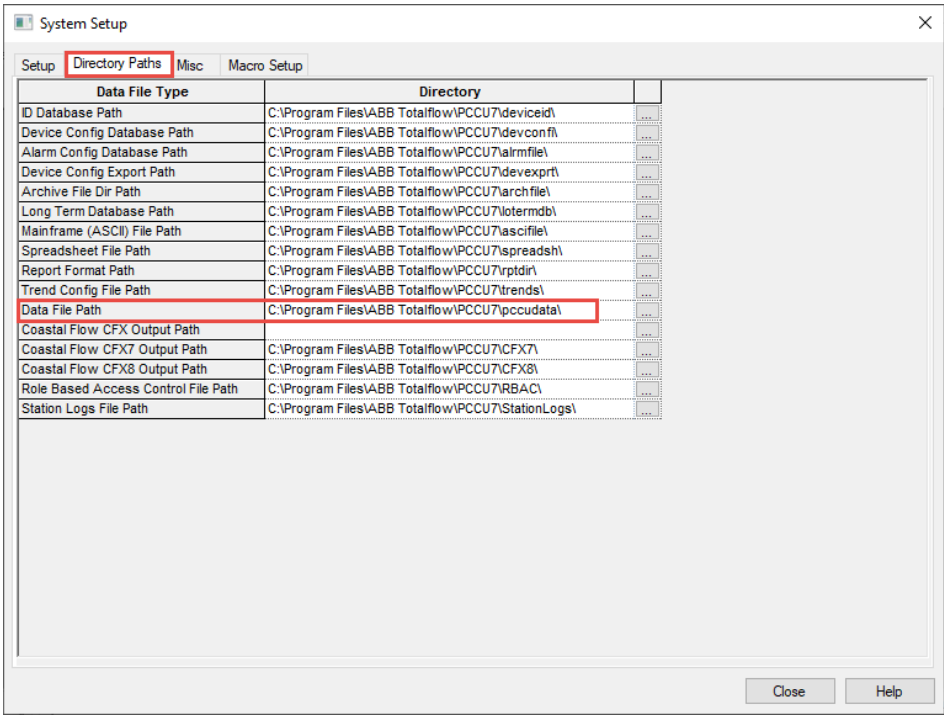
Figure 8-2: Collect screen



5. Click one or more output types from the Outputs list to send the data to other locations in addition to the laptop. The option to display the data on the screen is automatically selected.
6. Select the range of data to be collected.
7. Click **Collect**.
8. Click **Close** if the output screen displays.
9. Click **Close** to exit the Collect screen.

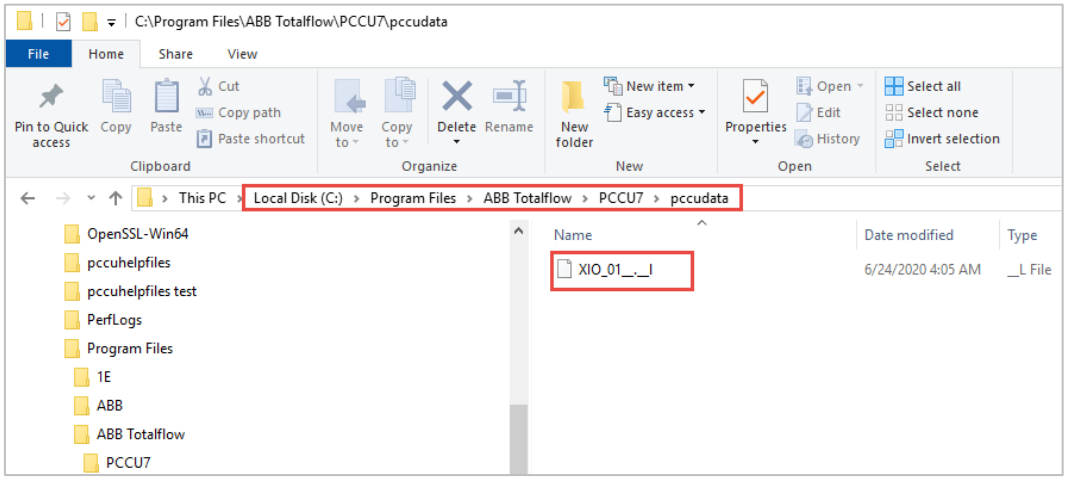
IMPORTANT NOTE: The data file might be in a default or user-defined location based on the PCCU directory path setup (Figure 8-3). The path for collected data is the Data File Path. The default location for data or laptop files is the pccudata directory in PCCU the installation directory.

Figure 8-3: Data file path



10. Navigate to the collected data file on the laptop.
    a. Open File Explorer.
    b. Navigate to the data file path. (Figure 8-4).
    c. Locate the data file. The data file is named with the device's station ID.

Figure 8-4: Locate laptop file (collected data)



IMPORTANT NOTE: PCCU creates a new laptop file the first time it collects data from a device. PCCU overwrites the data on the existing laptop file in subsequent collections from the same device. To preserve the laptop file for each collection, move and store the file in a safe location as soon as the collection is complete.

8.1.2 Save the device configuration

The following procedures are required to save the configuration of the Totalflow device for backup purposes. The device stores a running (warm) and a startup (cold) configuration that contain configuration files for all enabled and active applications. Configurations performed after the device starts for the first time continue to run in the running configuration. The startup configuration does not automatically update to reflect those configuration changes.

To perform a backup of the most up-to-date configuration, first update the startup configuration and save it on a laptop or PC.

Use backup configuration files to restore service in the event of equipment failure, part replacement, or to replicate the configuration in other devices.

IMPORTANT NOTE: tfData and tfCold, warm and cold, are terms used to refer to the running and startup configuration respectively.

8.1.2.1 Update the startup (cold) configuration

This procedure saves the running (warm) configuration to the startup (cold) configuration. With this procedure both the startup and the running configuration reflect the most current configuration. A cold restart event with the most-up-to-date configuration resumes device operation without the need to reconfigure the device. The update is a manually triggered action.

IMPORTANT NOTE: This procedure updates the startup configuration on the device. It does not create a configuration package in a separate location from the device.

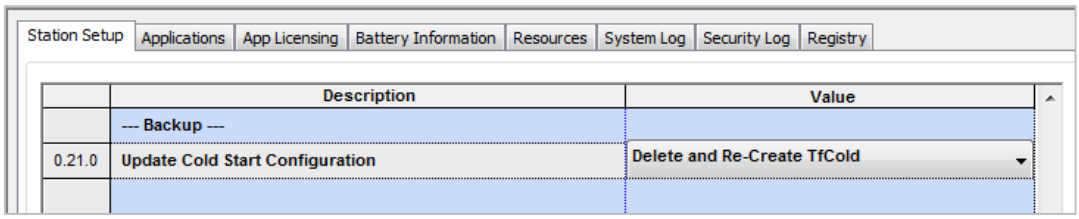
Perform this procedure when there are configuration changes. The startup configuration always contains the most up-to-date configuration.

The running (warm) configuration might contain calibration files. These files also save to the startup configuration during the update. Calibration files link with the device's electronic board serial number and do not apply to any other device.

To update the startup configuration:

1. Launch PCCU32 and click **Entry** on the toolbar.
2. Click the top item on the navigation tree. The Station Setup tab displays.
3. Scroll down to the Backup section (Figure 8-5).

Figure 8-5: Update cold start configuration



4. Click Update Cold Start Configuration and select Delete and Re-create TfCold from the drop-down list.
5. Click **Send**.
6. Click **Close** to exit the Station Setup screen and Entry Setup mode.
7. Click **Close** to disconnect PCCU32 from the device.

Proceed to the next section.

8.1.2.2 Save the startup (cold) configuration to the PC or laptop

This procedure saves the startup (cold) configuration from the device to a laptop or PC using the 32-Bit Loader. This requires a separate connection established from the loader, not from Entry mode.

IMPORTANT NOTE: If calibration files are in the startup configuration, they are automatically in the configuration package.

The saved calibration files link to the device's electronic board serial number and do not apply to any other device.

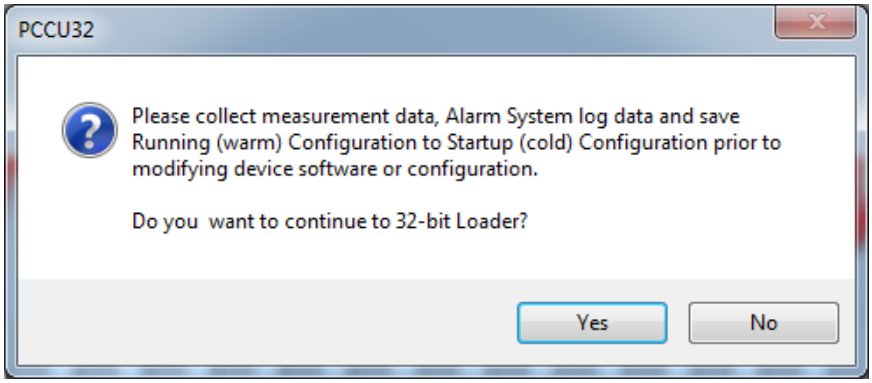
To save the device configuration:

1. Verify that PCCU32 is not connected to the device. If it is still connected, click **Disconnect**.
2. Click **32-Bit Loader** (Figure 8-6).

Figure 8-6: 32 Bit Loader icon

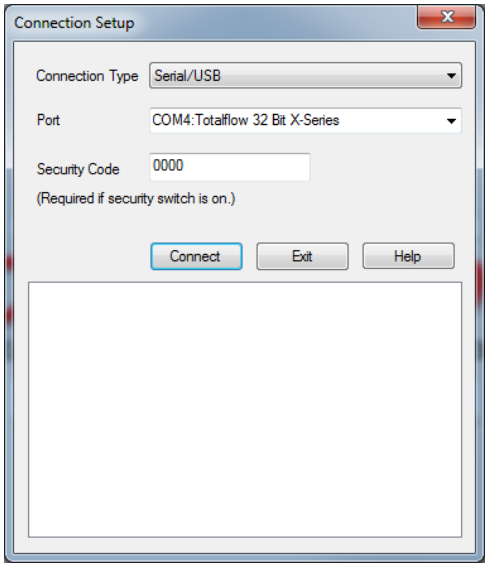
A message box displays (Figure 8-7).

Figure 8-7: Warning to collect data and update configuration



3. Click **Yes**. The Connection Setup dialog displays (Figure 8-8).

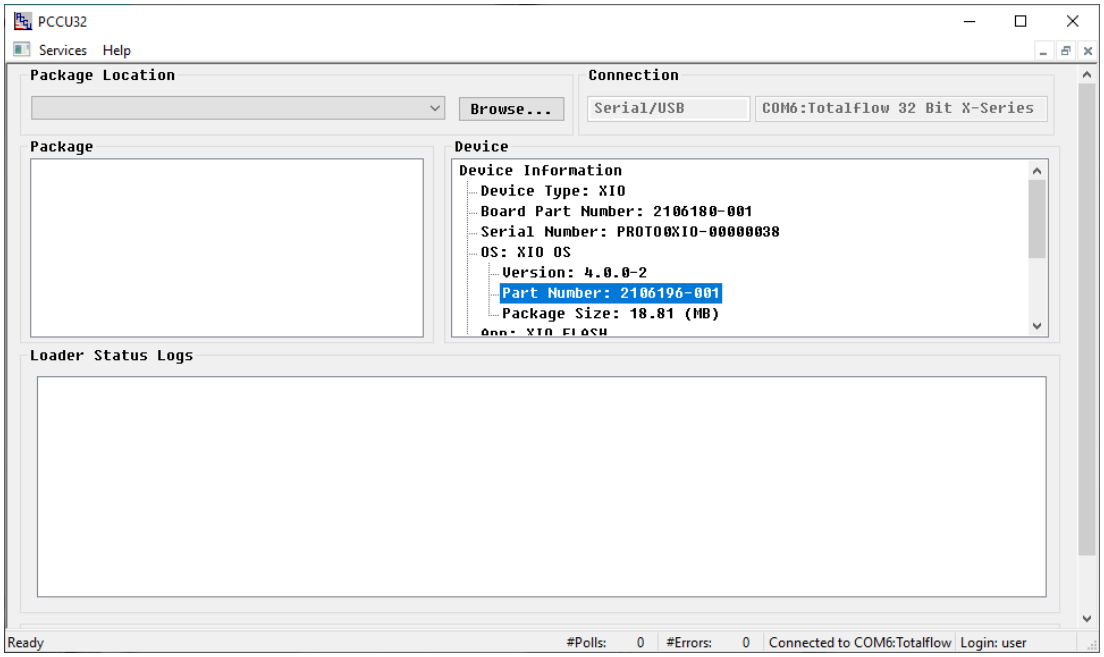
Figure 8-8: Device loader connection setup



4. Verify or type the connection setup parameters. Click **Connect**. When the device connects, the main loader screen displays (Figure 8-9).

IMPORTANT NOTE: Click **Help** on the 32-Bit Loader screens for additional details.

Figure 8-9: Device loader



5. On the loader screen, click **Services** on the menu bar.
6. Click **Save**... (Figure 8-10). The Save Software From Device dialog displays (Figure 8-11).

Figure 8-10: Device loader Save service

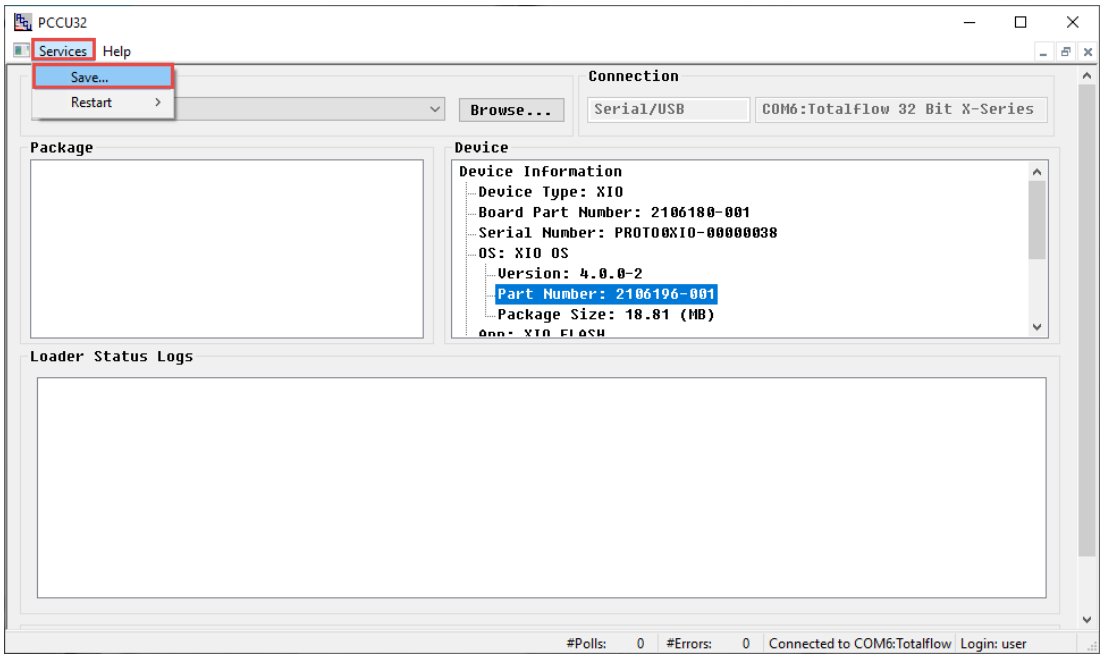
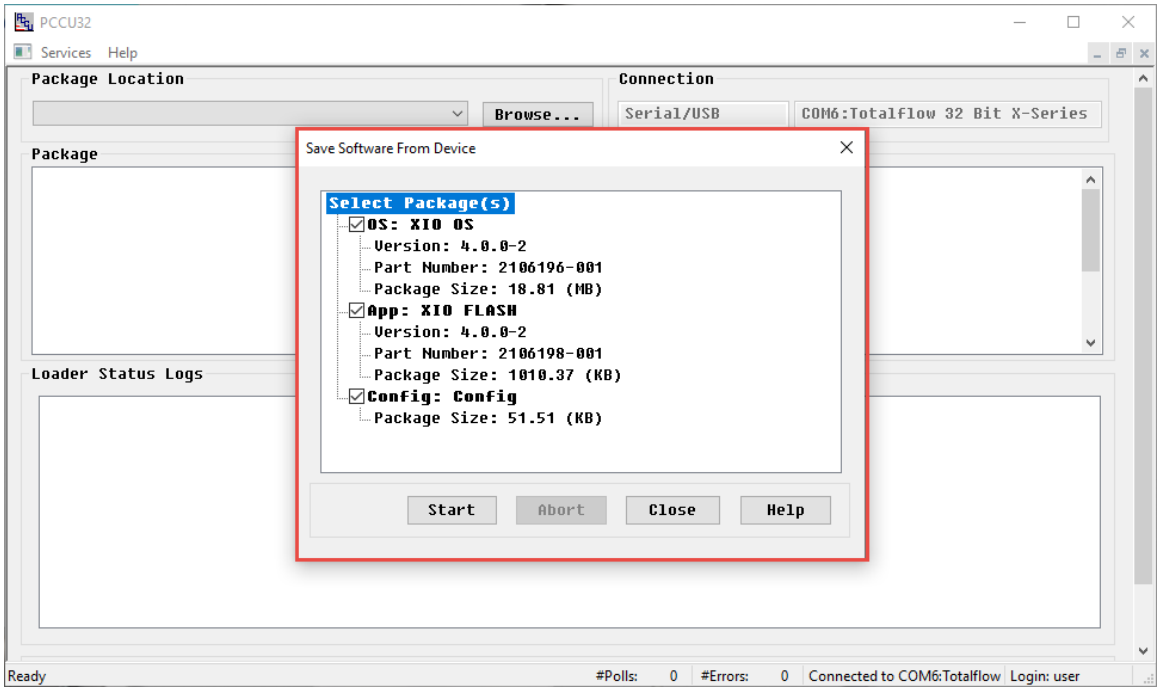
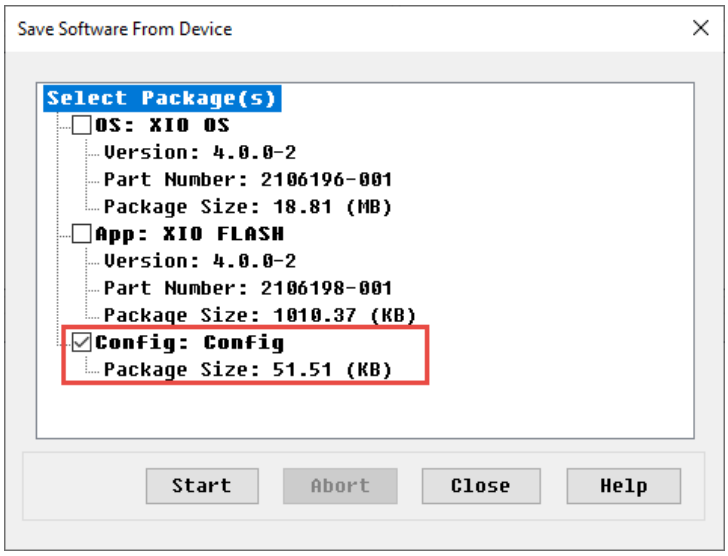


Figure 8-11: Save Software From Device dialog



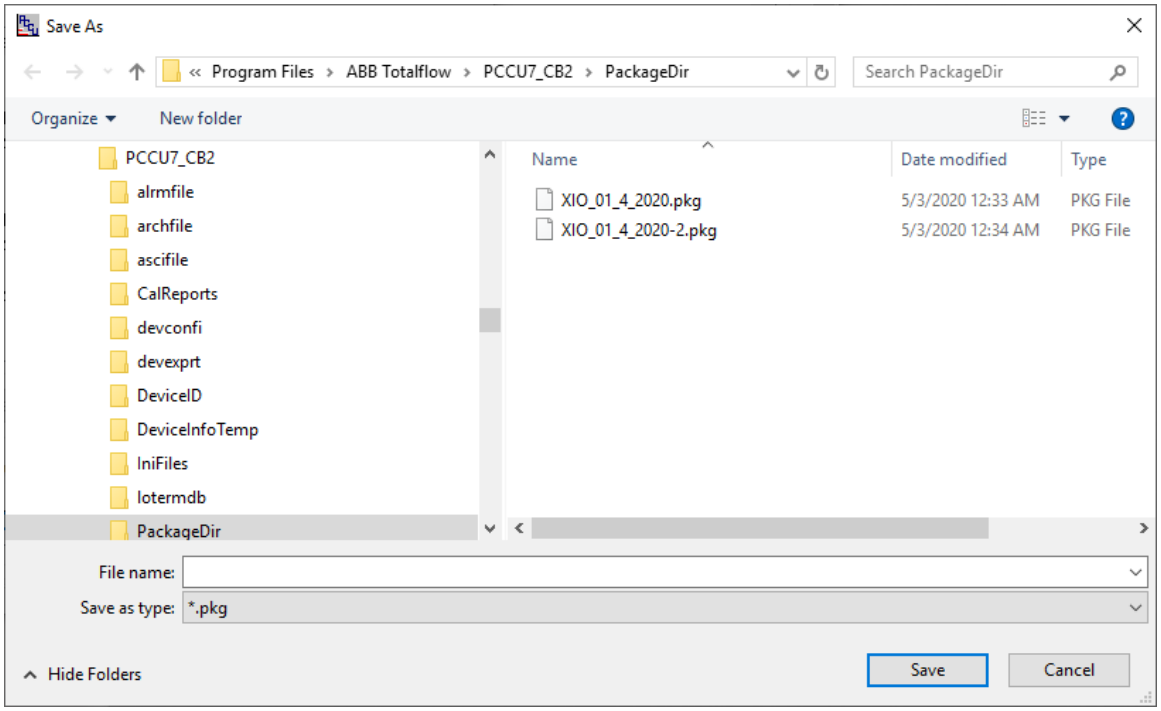
7. Click the **Config** checkbox. Clear the other checkboxes (Figure 8-12).

Figure 8-12: Save the startup (cold) configuration from the loader



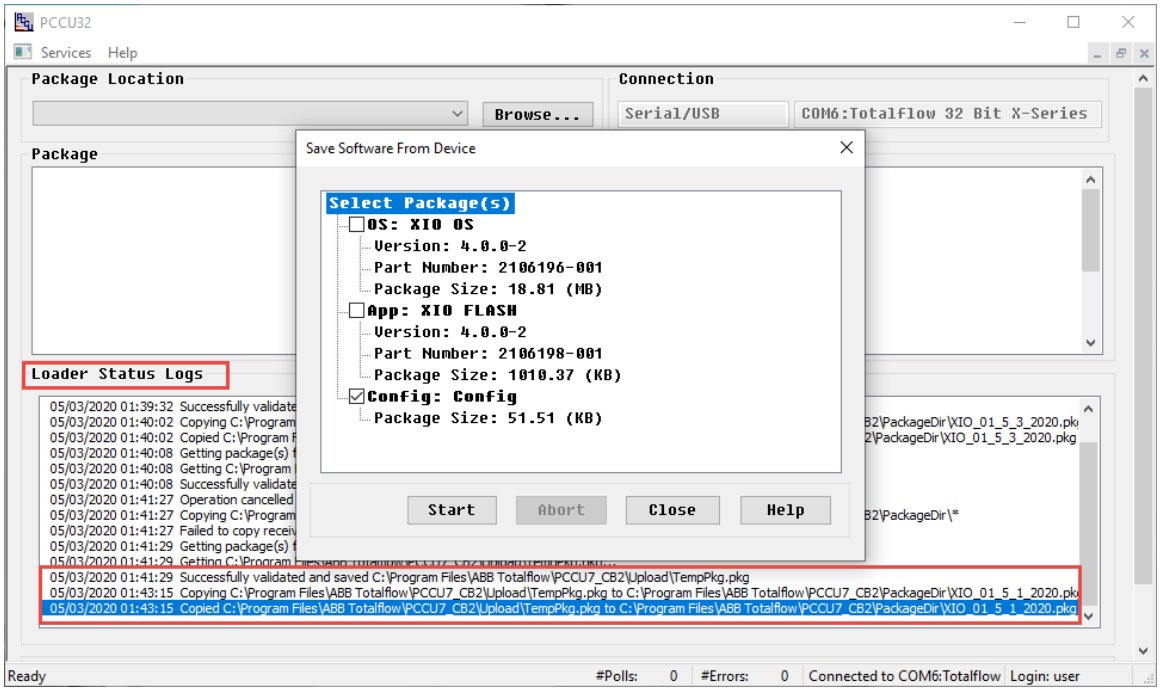
8. Click **Start**. The Save As window displays.

Figure 8-13: Default destination folder to save configuration (PackageDir)



9. Type the file name. Click **Save**. The loader assigns the .pkg extension automatically. The default location is the PackageDir folder in the PCCU installation directory.
10. View the Loader Status Logs field for status messages. When the configuration is successfully saved, several messages display to indicate that the configuration came from the device and that it successfully copied to the correct destination folder.

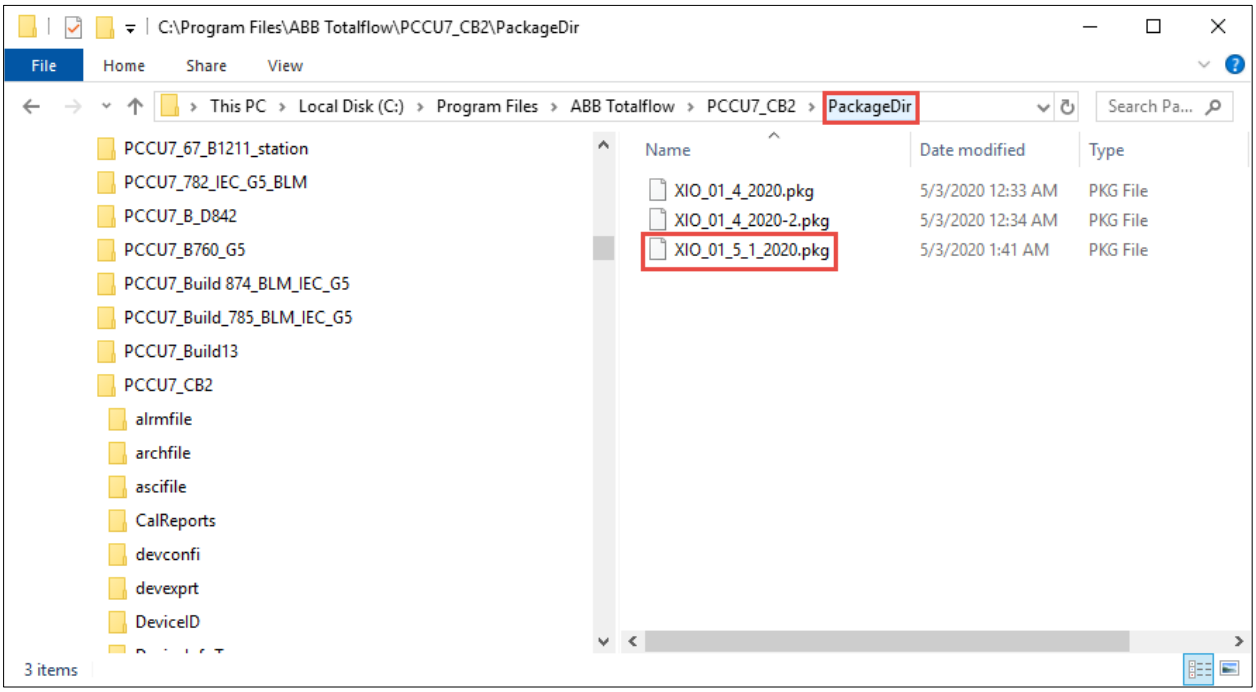
Figure 8-14 : Loader status logs – config file save successful



11. On the Save Software from Device window, click **Close** to return to the loader main screen.

12. Click **Close** to exit the device loader.
13. Locate the saved package in the destination folder. The file name format is <user-defined-name>.pkg (Figure 8-15).

Figure 8-15: Locating saved configuration (default directory)



8.2 Restore the device configuration

Use the device loader to restore the configuration on the device with a previously saved configuration package. Verify that the configuration package originated from the same unit. Then restore the device in the event of file corruption or other problems.

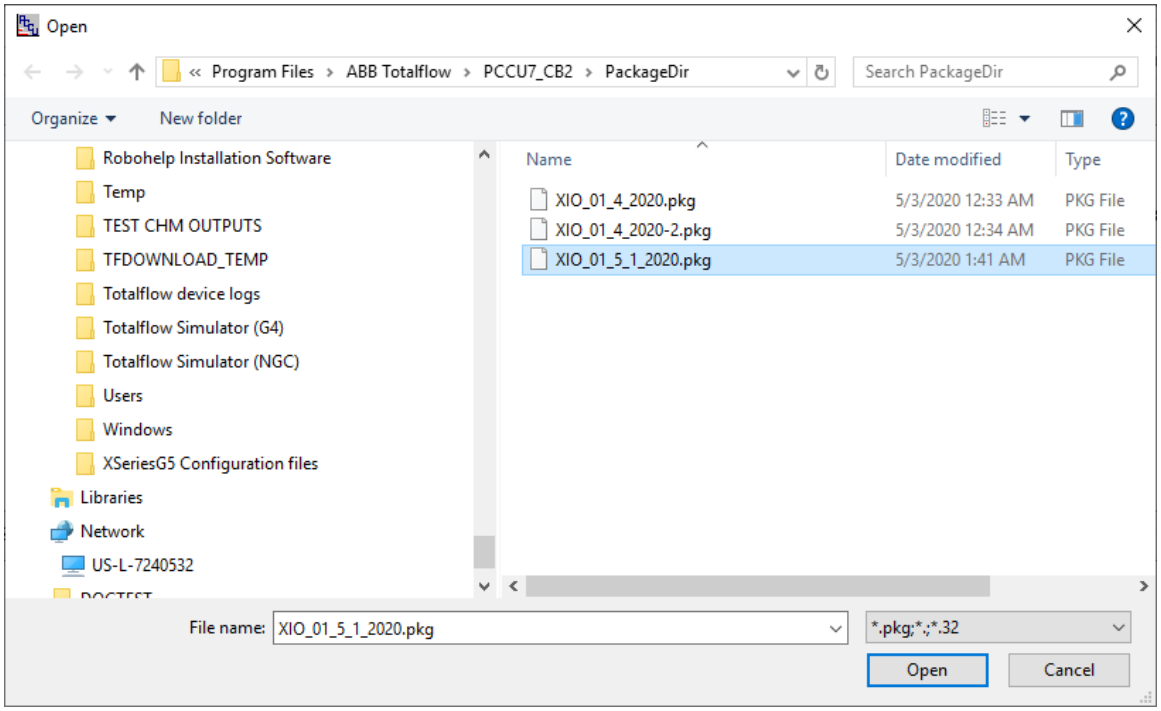
To restore the device configuration file:

NOTICE – Loss of data. When you restore the configuration, the loader sends the configuration package to replace the device's existing startup configuration. The device automatically uses the new startup configuration to restart (cold restart) and removes the previous startup configuration.

Before restoring the configuration on the device, perform the procedure in section 8.1.1 Collect data to collect the trend data (if trends are configured) and avoid data loss. It might be necessary to preserve the existing configuration if technical support needs to troubleshoot configuration issues. If necessary, perform the procedures in section 8.1.2.1 Update the startup (cold) configuration and section 8.1.2.2 Save the startup (cold) configuration to the PC or laptop.

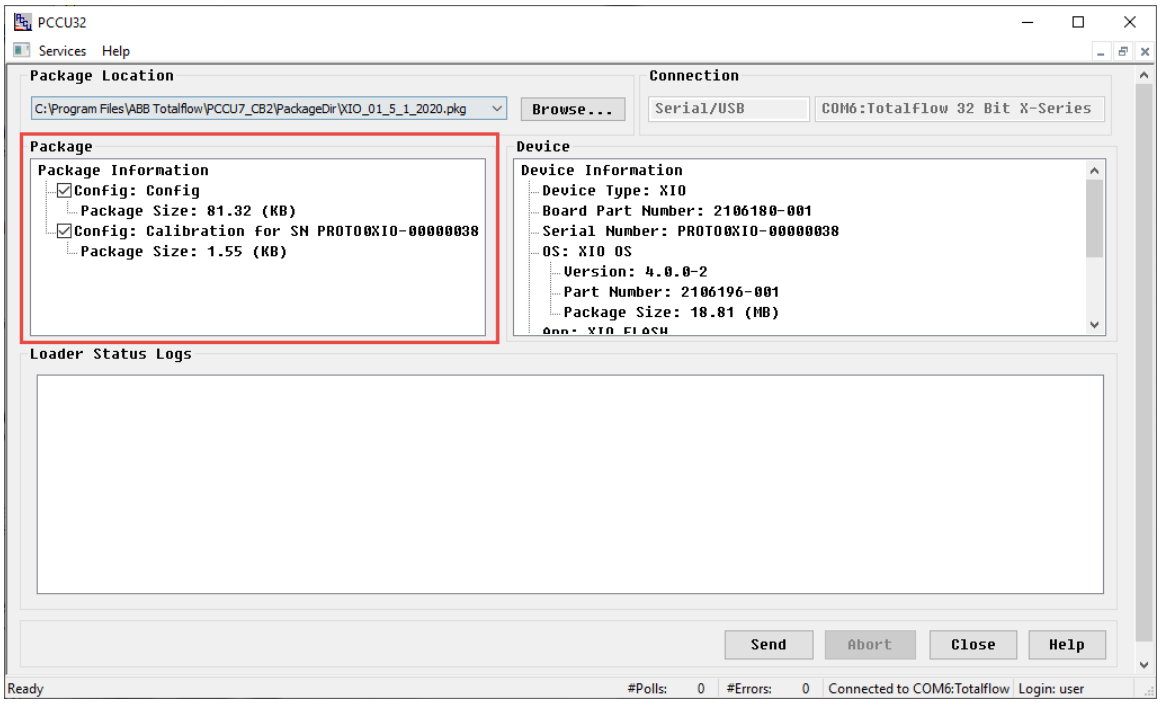
1. Verify that PCCU32 is not connected to the device. If it is still connected, click **Close**.
2. On the toolbar, click the 32-Bit Loader icon. A warning dialog to collect data displays.
3. Click **Yes**. The Connection Setup dialog displays.
4. Verify, select or type the connection setup parameters into the entry fields and click **Connect**. The main loader screen displays when the device connects.
5. Click **Browse**. The file explorer window displays.

Figure 8-16: Browse for configuration package



6. Locate and select the configuration file package, then click **Open**. The package details display in the Package field (Figure 8-17).

Figure 8-17: Loader screen configuration package to restore

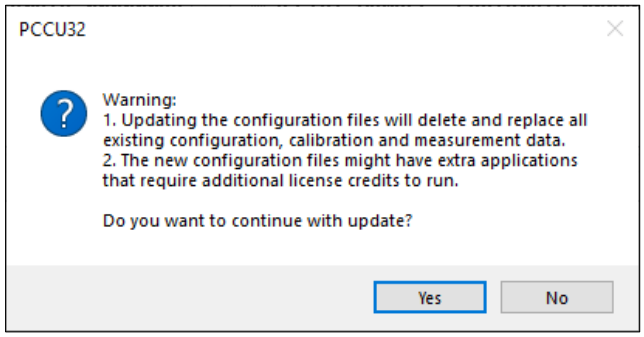


7. Select Config: Config.
8. Select **Config: Calibration** if the configuration file contains calibration files.

NOTICE – Tainted results. Do not select the calibration configuration in the Package field if the configuration package came from another XIO. Calibration files from a different device corrupt the last calibration records and skew the results. Only restore calibration files to the unit that generated them.

9. Click **Send**. A warning displays to indicate that existing configuration and device data will be overwritten and that extra credits may be needed to run the applications.

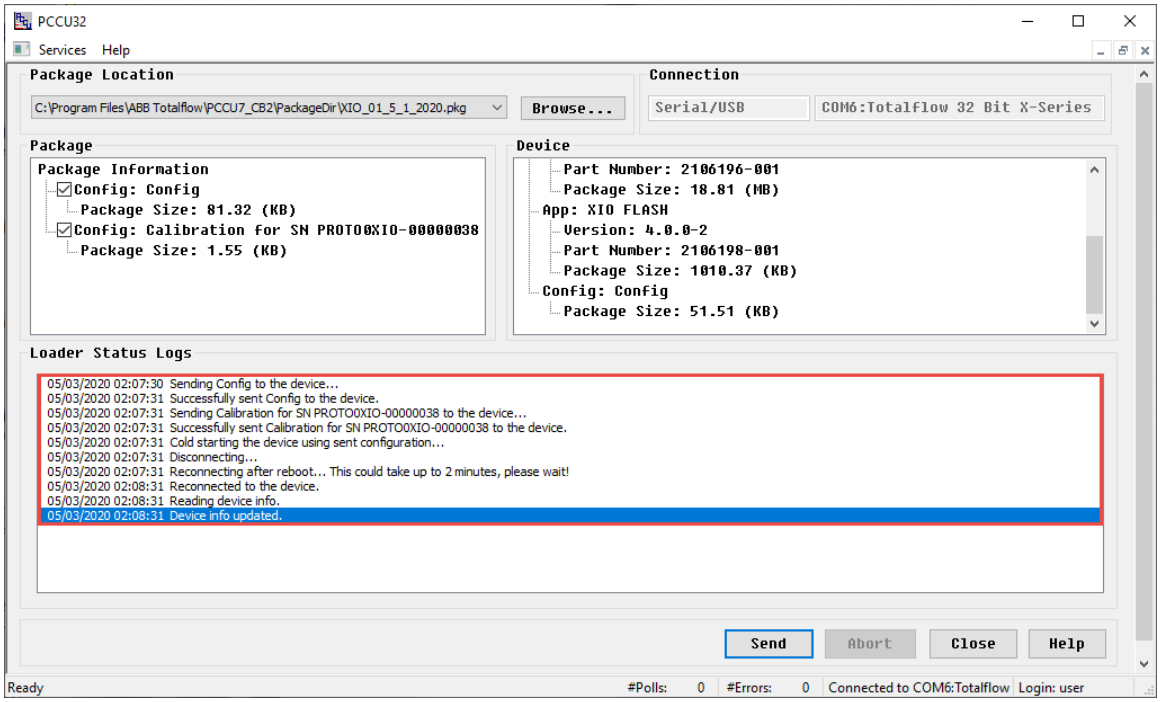
Figure 8-18: Warning before restoring device config



10. Click **Yes**.
11. View the status messages in the Loader Status Logs. A successful configuration file upload prompts messages to indicate:
    - The package was sent.
    - The system restarted.
    - The new configuration is active.

Successful completion of the configuration file update displays the message "Device info updated."

Figure 8-19: Configuration upload complete



12. Verify that the Device field displays the new configuration package information.

8.3 Use the configuration from another XIO

This procedure uses the device loader to copy a configuration saved from one device to another unit. Use this procedure if the configuration in several devices is similar. The configuration can be shared from one unit to another but not the calibration.

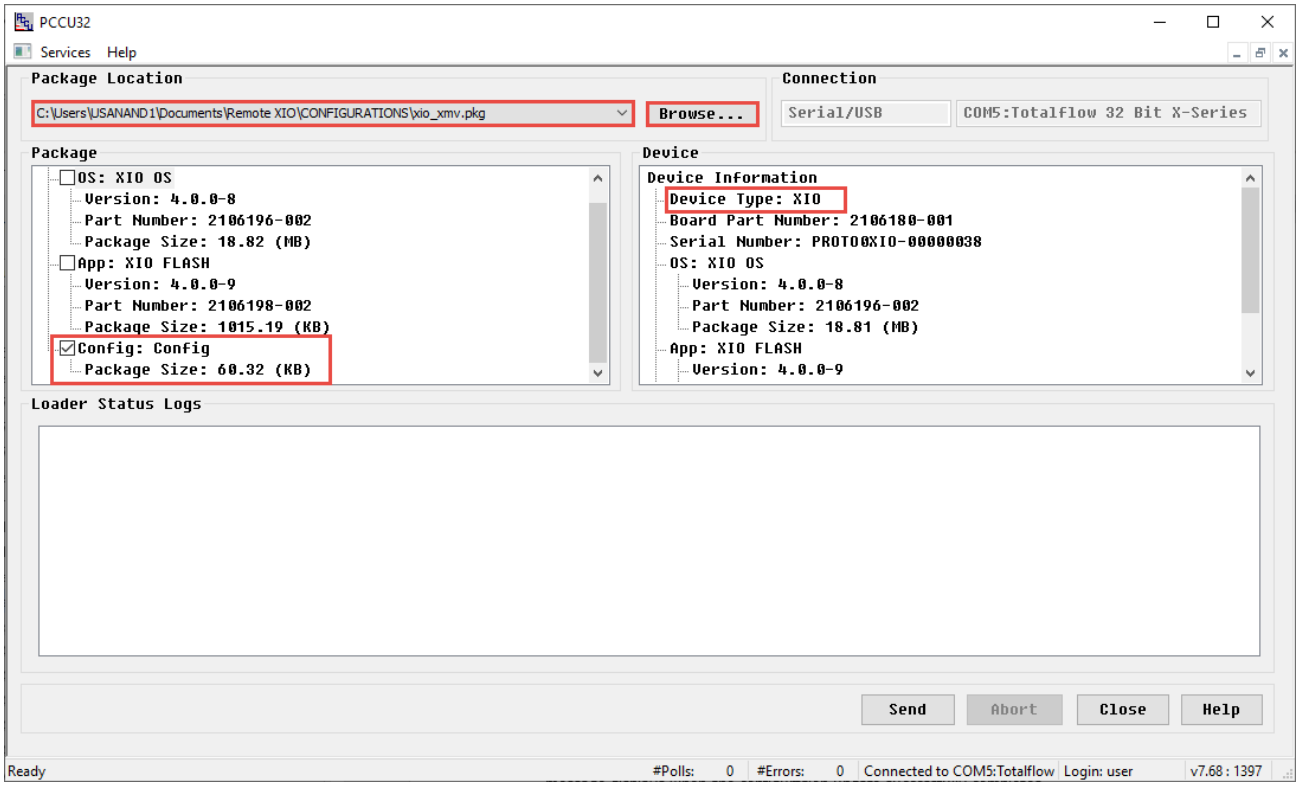
IMPORTANT NOTE: Do not use calibration data in a configuration package that was generated from another device. Calibration data is specific to each device and links to a device's electronic board serial number.

To send the device configuration:

NOTICE – Loss of data. After a configuration package from another unit replaces the existing package, the device automatically uses the new startup configuration to restart (cold restart). The previous Startup Configuration is overwritten.
To avoid loss of data and complete system reconfiguration, perform the procedures in section 8.1, Preserve data and configuration, to collect the data before sending a new configuration to the device.

1. Verify that PCCU32 is not connected to the device. If it is still connected, click **Close**.
2. Click the 32-Bit Loader icon in the toolbar. A warning dialog to collect data displays.
3. Click **Yes**. The Connection Setup dialog displays.
4. Verify, select, or type the connection setup parameters into the entry fields and click **Connect**. The main loader screen displays when the device connects.
5. Click **Browse**.
6. On the file browser window, locate and select the configuration file package then click **Open**. The package details display in the Package field (Figure 8-20). The configuration file may also contain the source device's OS and flash.

Figure 8-20: Loader screen configuration package from another XIO



7. Verify that the **Config: Config** checkbox is selected.
8. Clear other checkboxes so only **Config: Config** is selected.

NOTICE – Tainted results. If calibration files from the source device display, do not select them. Calibration files from a different device corrupt the last calibration records and skew the results. Only restore calibration files to the unit that generated them.

9. Click **Send**.
10. View the status messages in the Loader Status logs to verify that the package was sent successfully, the system restarted, and the new configuration is active. The "Device info updated" message displays when the configuration update successfully completes.
11. Verify that the Device field displays the new configuration package information.

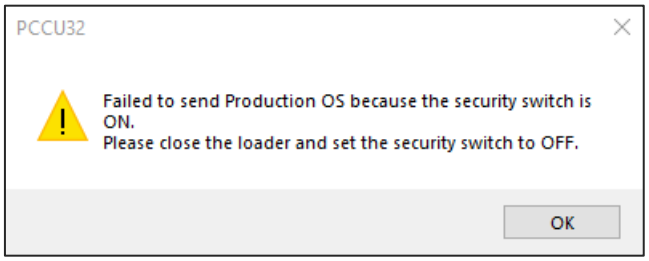
8.4 Update device software

ABB periodically releases software update packages. Use the device loader to update the controller with new software packages when required.

8.4.1 Security requirements before upgrade

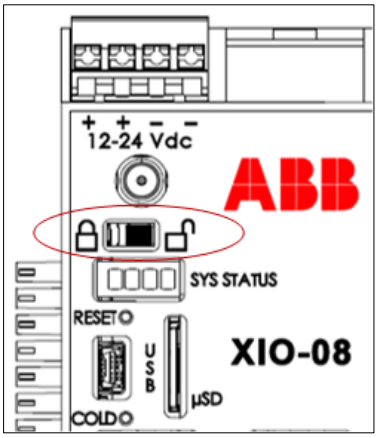
Before upgrade, disable the physical security switch on the device (set to **unlock/off**). If this is not done the following error message will be prompted.

Figure 8-21: Security ON error



After performing the upgrade, reset the Security switch to **Lock/on.**

Figure 8-22: XIO Security switch



8.4.2 When to upgrade

Software updates occur when:

- New major functionality or applications are added.
- Enhancements to existing application are added.
- Software bugs are fixed.

IMPORTANT NOTE: Devices might not require an update every time a new software package is released. Review the release notes to determine if an update is appropriate for your scenario and application requirements. In the case of critical bug fixes, a technical bulletin might be issued to indicate that an update is required. Technical bulletins identify the product hardware or software versions impacted.

Follow your company policies for the evaluation or testing of software updates before updating devices already in service.

8.4.3 Software packages

Software packages typically contain the main Totalflow application (Totalflow.exe, also referred to as flash in our download sites). If the main application also requires an updated version of the operating system (OS) or boot software, the package also includes the boot and OS software.

Software updates should not affect the configuration of a device. However, always collect data and save the configuration before any updates.

IMPORTANT NOTE: If you attempt an application-only (flash) update when an OS/boot update is also required, the loader rejects the update until you use the correct package and select all required items. The loader determines if the flash is compatible with the OS/Boot software currently in the device. See the Loader help topics in PCCU for additional details.

Software packages are available for download at www.abb.com/upstream. Software packages have a base part number followed by 3 digits to indicate the build version of the package. For example, the number of the XIO package containing both OS and Flash is 2106200. A package numbered 2106200-029 reflects build 29 of that package type.

Package part numbers are different for each product type. To locate packages on the ABB website, select the product and the applicable package.

IMPORTANT NOTE: If you have any questions or are unable to locate or download a software update package, call Technical Support.

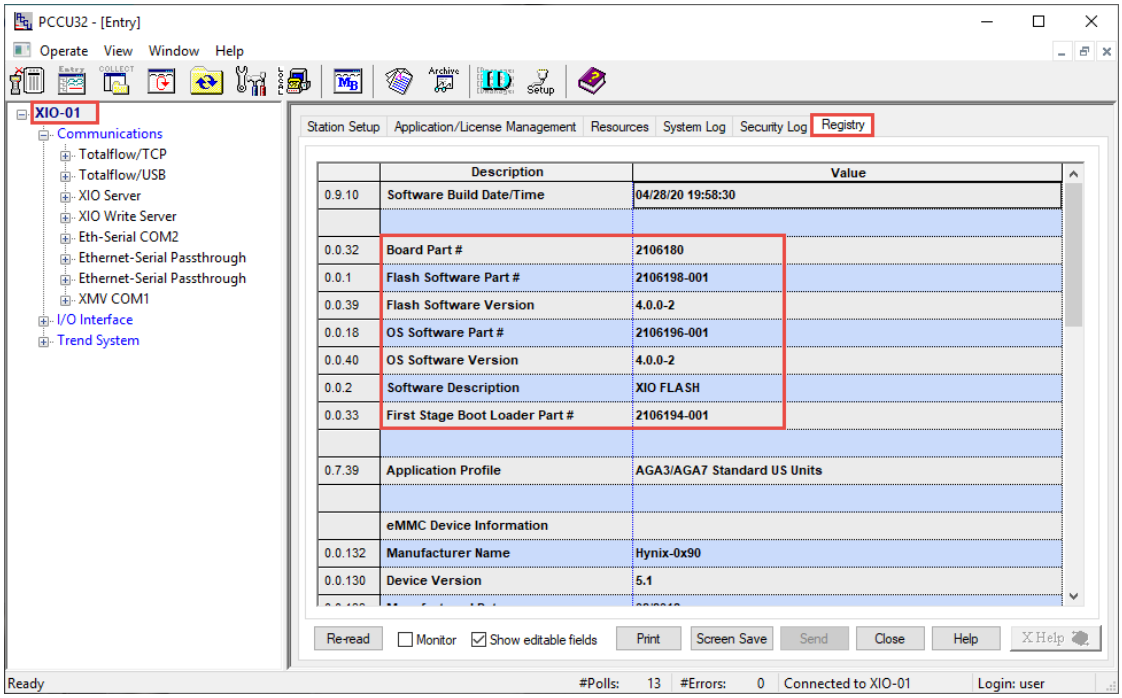
8.4.4 Determine device software part number/version

This procedure describes how to determine the software part numbers from PCCU. This information is helpful to determine if updates are necessary, or when ABB technical support requests them during troubleshooting.

To determine the current software on the device:

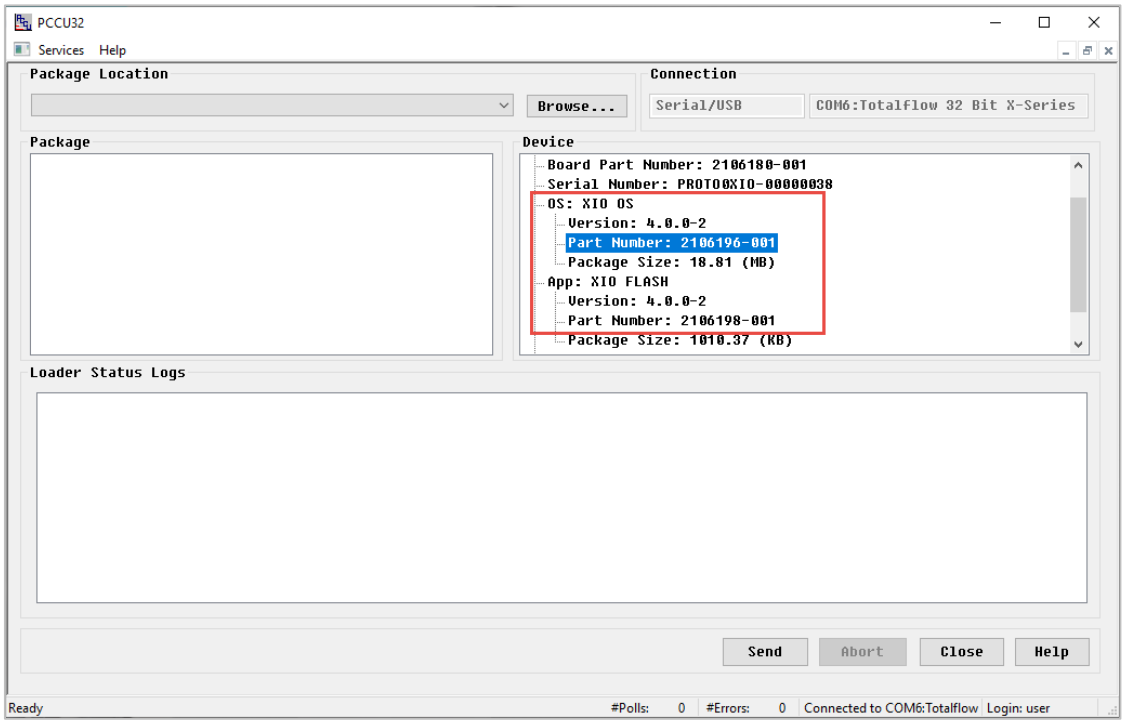
1. Connect to the device in PCCU entry mode.
2. Select the Station ID at the top of the navigation tree. The Station Setup screen displays.
3. Click **Registry** (Figure 8-23).
4. View and take note of the current part numbers and versions in the Value column. Part numbers in this list match the software package numbers released by ABB. Different numbers may apply for packages that combine more than one component. Carefully review software release notes to determine what to download.

Figure 8-23: XIO registry tab



IMPORTANT NOTE: Software part number and version information is also available from the loader. The loader screens use "App" to refer to the flash. See (Figure 8-24).

Figure 8-24: XIO software part numbers from the Loader



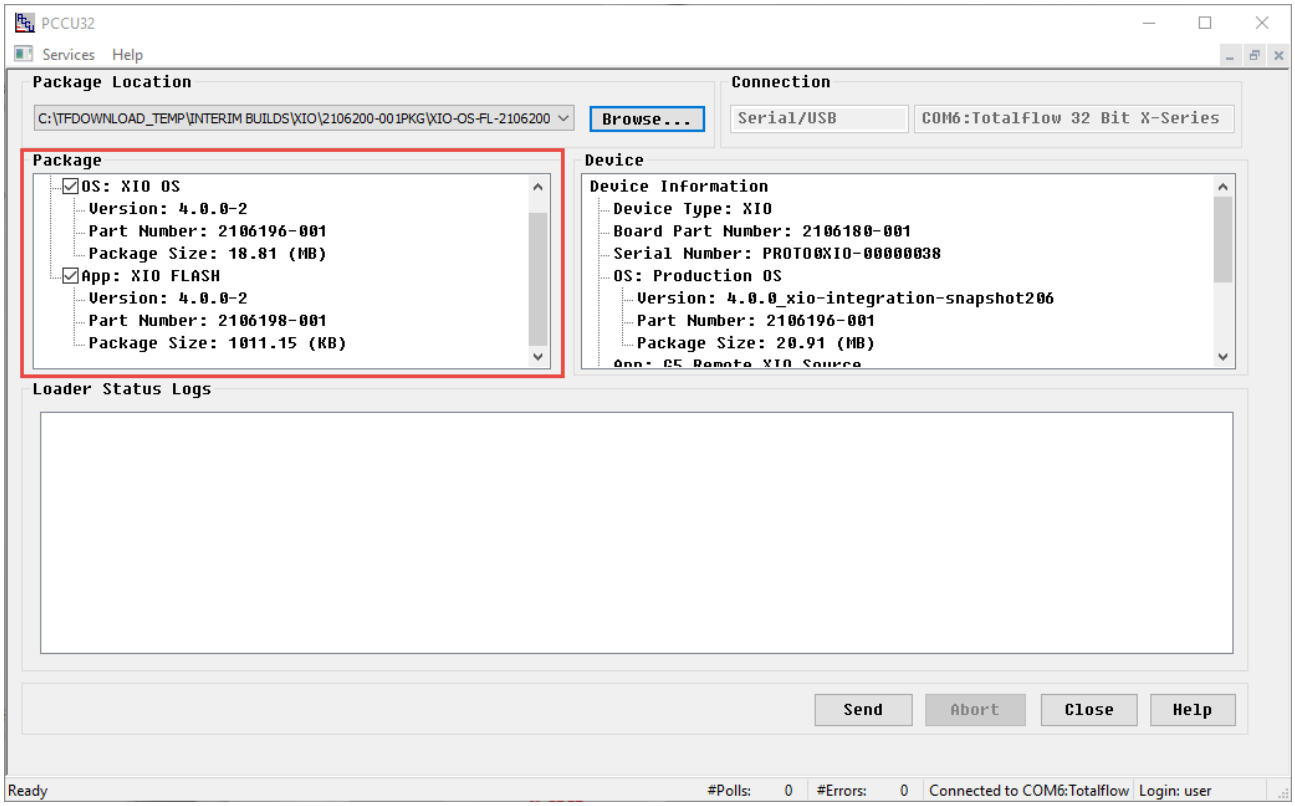
8.4.5 Update software

To update the software:

NOTICE – Loss of data. Collect the data and perform the procedures in section 8.1 Preserve data and configuration to back up the customer data and device configuration before performing any service on the device. Failure to collect data and save the configuration can result in a loss of data and require a complete system configuration.

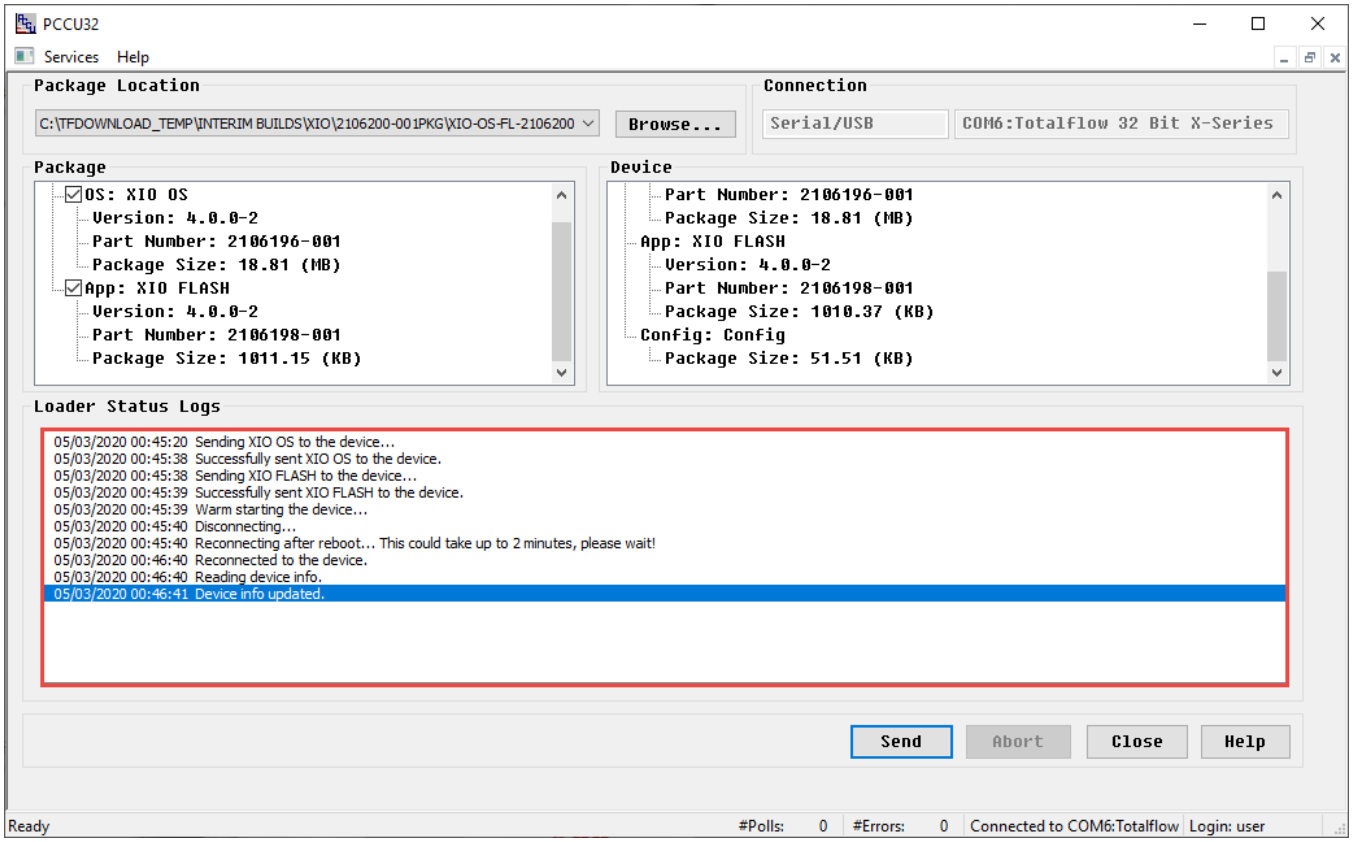
1. Download the software package from the ABB website to a laptop or PC.
2. Launch PCCU32 and click the **32-Bit Loader** icon in the toolbar. A message to confirm PCCU launch displays.
3. Click **Yes**.
4. Verify or type the connection setup parameters into the entry fields and click **Connect**. The Loader screen displays.
5. Click **Browse**. The browser window displays.
6. Locate and select the software package and click **Open**. The package details display in the Package field (Figure 8-25).

Figure 8-25: Update device software with package information



7. View the Package Information field to verify that the XIO package version is the required version for the update.
8. Verify that **OS: XIO OS** and **App: XIO FLASH** are checked. Clear unnecessary items in the package.
9. Click **Send**.
10. View the status messages in the **Loader Status Logs** field. The "Device info updated" message displays indicating that the package has been sent and activated successfully (Figure 8-26).

Figure 8-26: Software update complete (OS and Flash)



IMPORTANT NOTE: Updates to the main application (App) might require an update to PCCU32. In these cases, download a new version of PCCU32.

8.5 System restart

The XIO has several options for restart. This section provides an overview of those options and the corresponding procedures for manually-triggered restarts.

NOTICE – Data loss. Some of the restart procedures in this section cause customer data, device configuration or calibration data loss. To back up data and configuration, see section 8.1 Preserve data and configuration.

8.5.1 Restart type overview

There are several ways to restart an XIO. Restarts can be manually triggered or performed automatically after software updates, power removal, or other system events. Perform manually triggered restarts onboard or from the user interface (PCCU).

Table 8-1 describes device restarts. Review the implications of each restart type carefully to select the appropriate method. There may be several methods for the same type of restart.

IMPORTANT NOTE: While there are several methods for the warm and cold restarts, ABB recommends restarts from PCCU32 (Entry mode or device loader).

Table 8-1: Restart types

Restart type	Description	Use	User-triggered restart procedures
Warm restart	The device: Shuts down all applications. Backs up the running data, configuration, and logs to persistent memory. Restarts with running (warm) configuration.	Automatic trigger: After software update Manual trigger: A warm restart might be required as part of general installation, maintenance or troubleshooting procedures. For example, a warm restart restores operation if the device locks up due to power or communication interruption.	8.5.2 Warm restart with the RESET button 8.5.3 Warm restart from the device loader 8.5.4 Warm restart from PCCU Entry mode 8.5.5 Warm restart from terminal mode
Cold restart	The device: Shuts down all applications. Deletes the running configuration and repopulates it using the startup (cold) configuration. Restarts with startup (cold) configuration.	Automatic trigger: Following a startup configuration update Manual trigger: Only as part of a service or maintenance procedure or when ABB technical support specifically directs it. A cold restart causes running configuration loss (this might also include calibration files). To back up before restart, follow procedures in section 8.4.5 Update software.	8.5.6 Cold restart from the device loader 8.5.7 Cold restart from terminal mode
Factory restart	The device: Shuts down all applications. Deletes the running configuration and repopulates it using the factory configuration. Restarts with factory defaults	Manual trigger: Use Factory Restart when it is necessary or desirable to return the device to the original configuration as shipped from the factory. For example, do this when the device is relocated, or to start a configuration from scratch after file corruption or failed update. A reset to factory defaults causes data, running, and startup configuration loss (this might also include calibration files). To back up before going back to factory defaults, follow procedures in section 8.4.5 Update software.	8.5.8 Factory restart from the device loader
Restart due to power loss	All data logs and configurations within the current minute are lost.		Power removal is not a recommended method for restart.

8.5.2 Warm restart with the RESET button

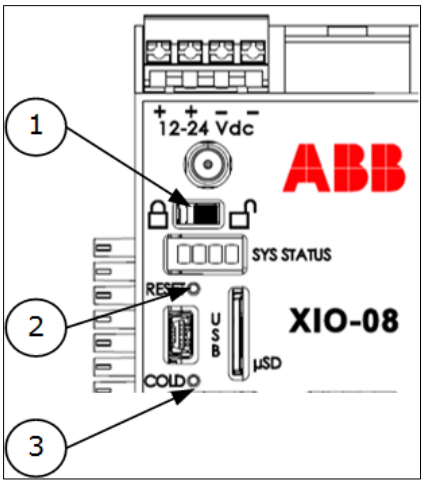
The warm restart resets the XIO microprocessor. Use a warm restart to take the XIO out of service for maintenance or troubleshooting. Only use a warm restart when a power or communication interruption causes the microprocessor to lock up.

This procedure uses the RESET button on the XIO to restart the device. It causes the device to restart with the running (warm) configuration. If the XIO is installed inside an enclosure, you must have access to the interior of the enclosure to access the XIO reset button.

To complete a warm restart using the reset button:

1. Press and release the **Reset** button (Figure 8-27).
2. Observe the System LEDs. The System LEDs show that the unit is shutting down and restarting.

Figure 8-27: Security switch



Legend: Security switch

ID	Description
1	Security switch
2	Reset (paperclip actuated)
3	Cold (paperclip actuated)

IMPORTANT NOTE: If the XIO does not restart, press and hold the **Reset** button for eight seconds.

8.5.3 Warm restart from the device loader

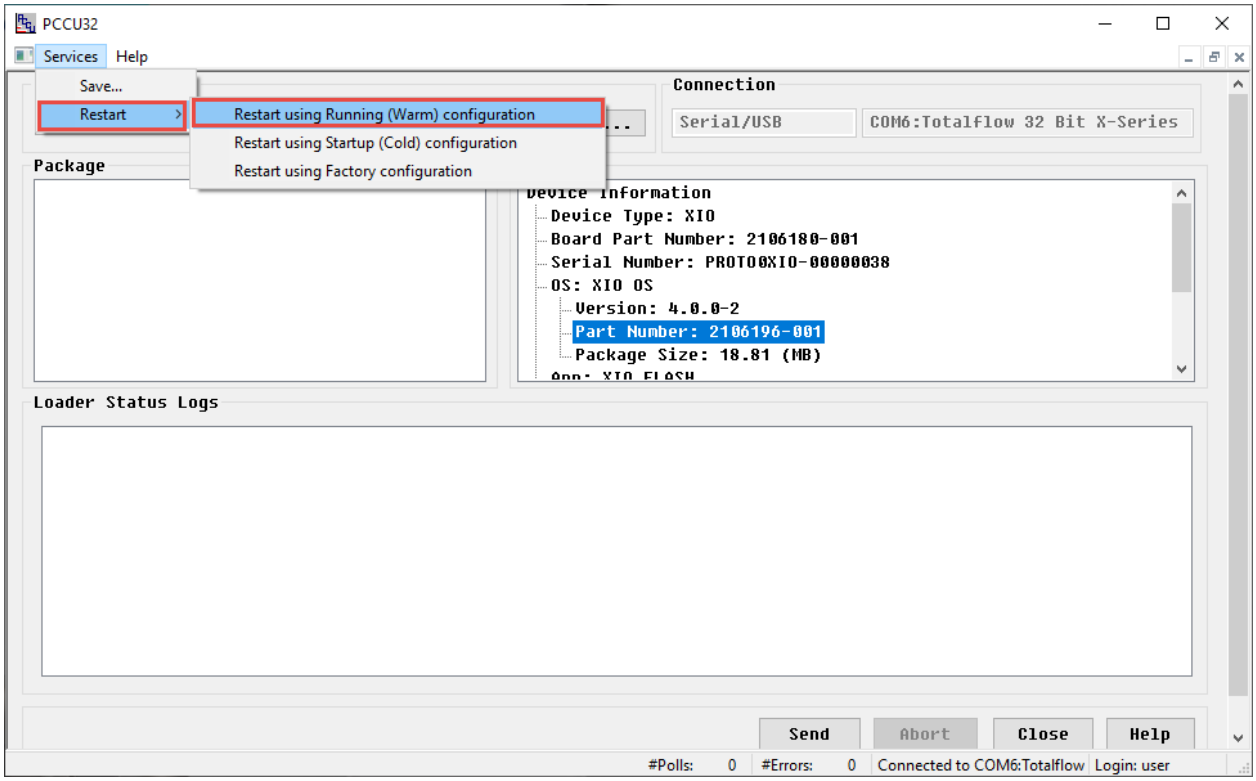
This procedure performs the warm restart from the 32-bit loader. The procedure can be performed while on a local or remote loader connection.

The procedure causes the device to restart with the running (warm) configuration.

To complete a warm restart from the device loader:

1. Launch PCCU.
2. Click **32 Bit Loader**. A message to confirm PCCU launch displays.
3. Click **Yes**.
4. Verify or type the connection setup parameters. Click **Connect**. The Loader screen displays.
5. Click **Services>Restart**. Select **Restart using Running (Warm) configuration** from the drop-down list (Figure 8-28).

Figure 8-28: Warm restart with device loader



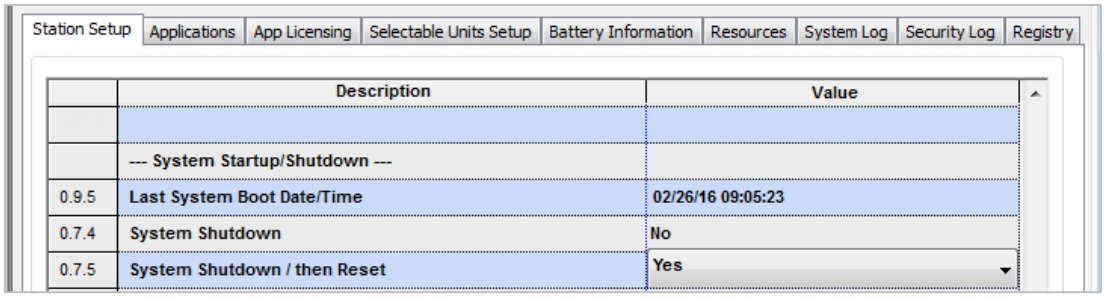
6. Click **Help** for more information.

8.5.4 Warm restart from PCCU Entry mode

To restart the device from PCCU Entry mode:

1. Launch PCCU32 and click **Entry**.
2. Click **View** on the PCCU32 menu and select **Expert** from the drop-down list.
3. At the top of the navigation tree, click the Station ID. The Station Setup tab displays.
4. Scroll down to **System Startup/Shutdown** (Figure 8-29).
5. Select **Yes** from the **System Shutdown / then Reset** drop-down list.
6. Click **Send**.
7. Click **OK** to confirm.

Figure 8-29: Warm restart on the Station Setup tab (Expert view)



8.5.5 Warm restart from terminal mode

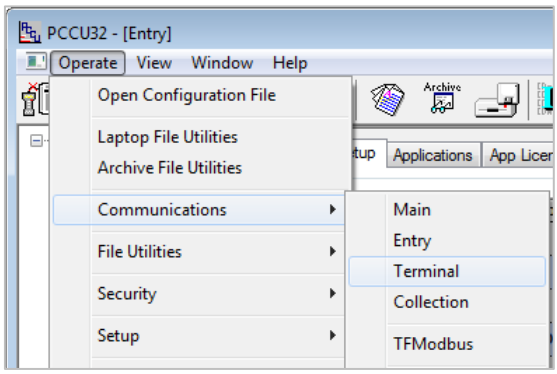
This procedure performs the warm restart from the terminal mode. It causes the device to restart with the running (warm) configuration.

Follow this procedure remotely or while physically connected to the device. Invoke Terminal mode from entry mode or from the PCCU main screen. This method of warm restart requires command entry.

To restart the controller using terminal mode:

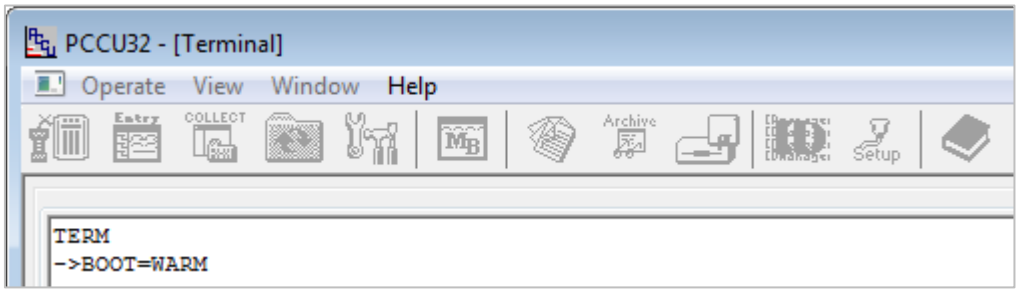
1. Launch PCCU32.
2. Click **Entry**.
3. Click **Operate>Communications** and select **Terminal** from the drop-down list (Figure 8-30). The Terminal screen displays.

Figure 8-30: Terminal menu option



4. Type the **BOOT=WARM** command at the terminal prompt (->) (Figure 8-31).

Figure 8-31: Terminal mode warm restart



5. Press **Enter**.

8.5.6 Cold restart from the device loader

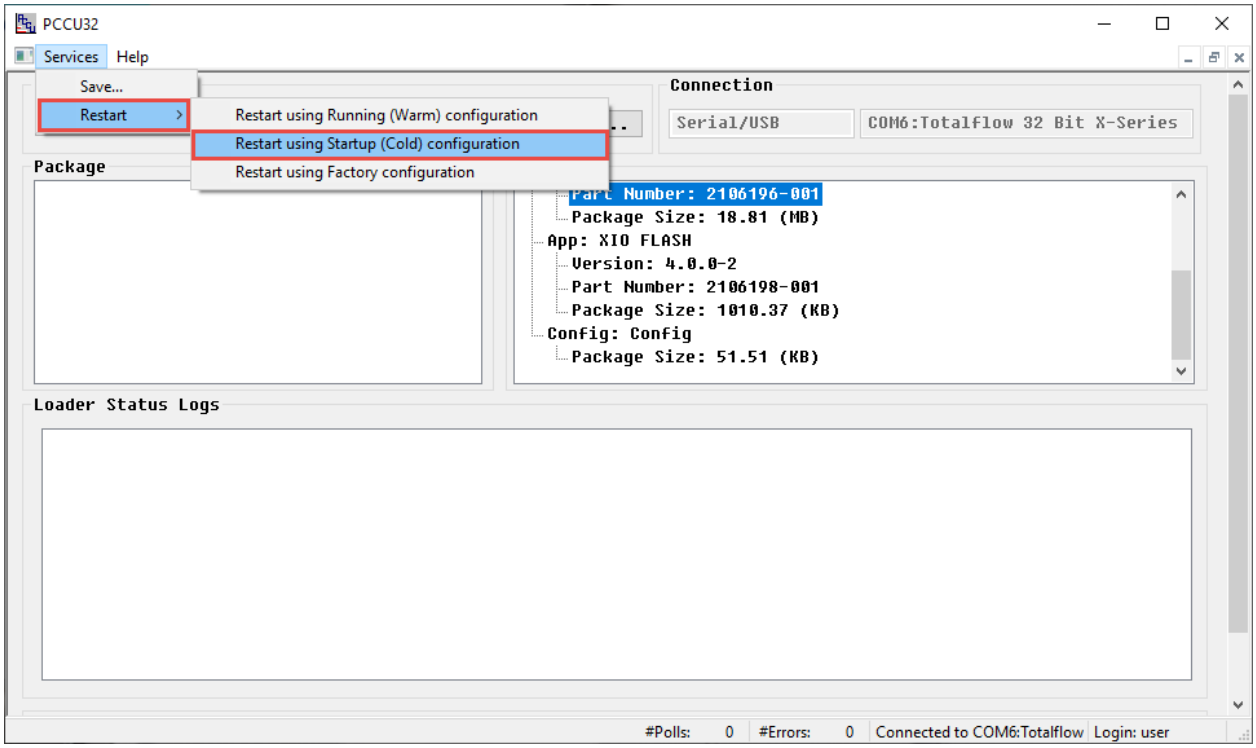
This procedure performs the cold start from the 32-bit loader. Follow this procedure on a local or remote loader connection. However, ABB highly recommends performing the cold restart locally. The cold restart causes the device to restart using the startup (cold) configuration.

NOTICE – Data Loss. Perform the procedures in section 8.1 Preserve data and configuration before a cold start. This avoids loss of the data and the need for a complete system reconfiguration. If the startup (cold) configuration does not have the latest network connection configuration, the restart causes loss of network connectivity. Update the startup configuration (tfCold) to avoid loss of network connection and required reconfiguration.

To complete a cold restart using the startup (cold) configuration:

1. Launch PCCU.
2. Click the **32 Bit Loader** icon in the toolbar. A message to confirm PCCU launch displays.
3. Click **Yes**.
4. Verify or type the connection setup parameters and click **Connect**. The Loader screen displays.
5. Click **Services>Restart** in the menu bar and select **Restart using Startup (Cold) configuration** from the drop-down list (Figure 8-32).

Figure 8-32: Cold restart using the device loader



6. Click **Help** for more information.

8.5.7 Cold restart from terminal mode

This procedure performs the cold start from the terminal mode. It causes the device to restart using the startup (cold) configuration.

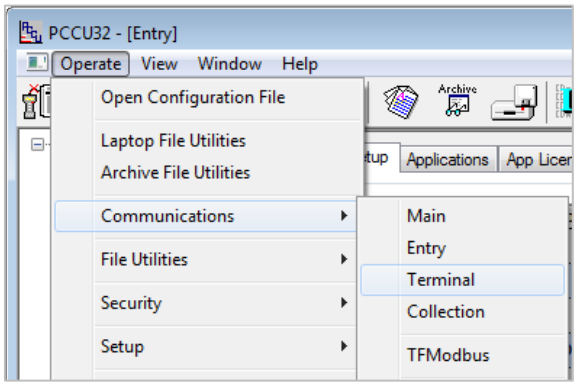
Perform the procedure on either a local or remote connection. However, ABB highly recommends local cold restarts with this method. Invoke Terminal mode from entry mode or from the PCCU main screen. This method of cold restart requires command entry.

NOTICE – Data Loss. Perform the procedures in section 8.1 Preserve data and configuration before a cold start. This avoids loss of the data and the need for a complete system reconfiguration. If the startup (cold) configuration does not have the latest network connection configuration, the restart causes loss of network connectivity. Update the startup configuration (tfCold) to avoid loss of network connection and required reconfiguration.

To restart from terminal mode:

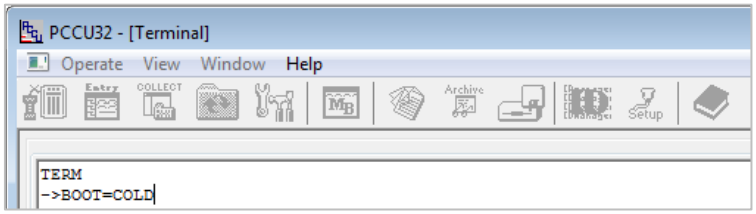
1. Launch PCCU.
2. Click the **Entry** icon in the toolbar. The Entry screen displays.
3. Click **Operate** in the menu bar and select **Communications>Terminal** from the drop-down list (Figure 8-33). The Terminal screen displays.

Figure 8-33: Terminal menu option



4. Type the command **BOOT=COLD** at the terminal prompt (->) (Figure 8-34).

Figure 8-34: Terminal screen – cold boot



5. Press **Enter**.

8.5.8 Factory restart from the device loader

This procedure uses the 32-bit loader to restore the device's startup configuration to its factory defaults. Factory defaults can include a generic base configuration or a custom configuration. Customers can request custom configurations to address specific requirements in addition to the basic configuration.

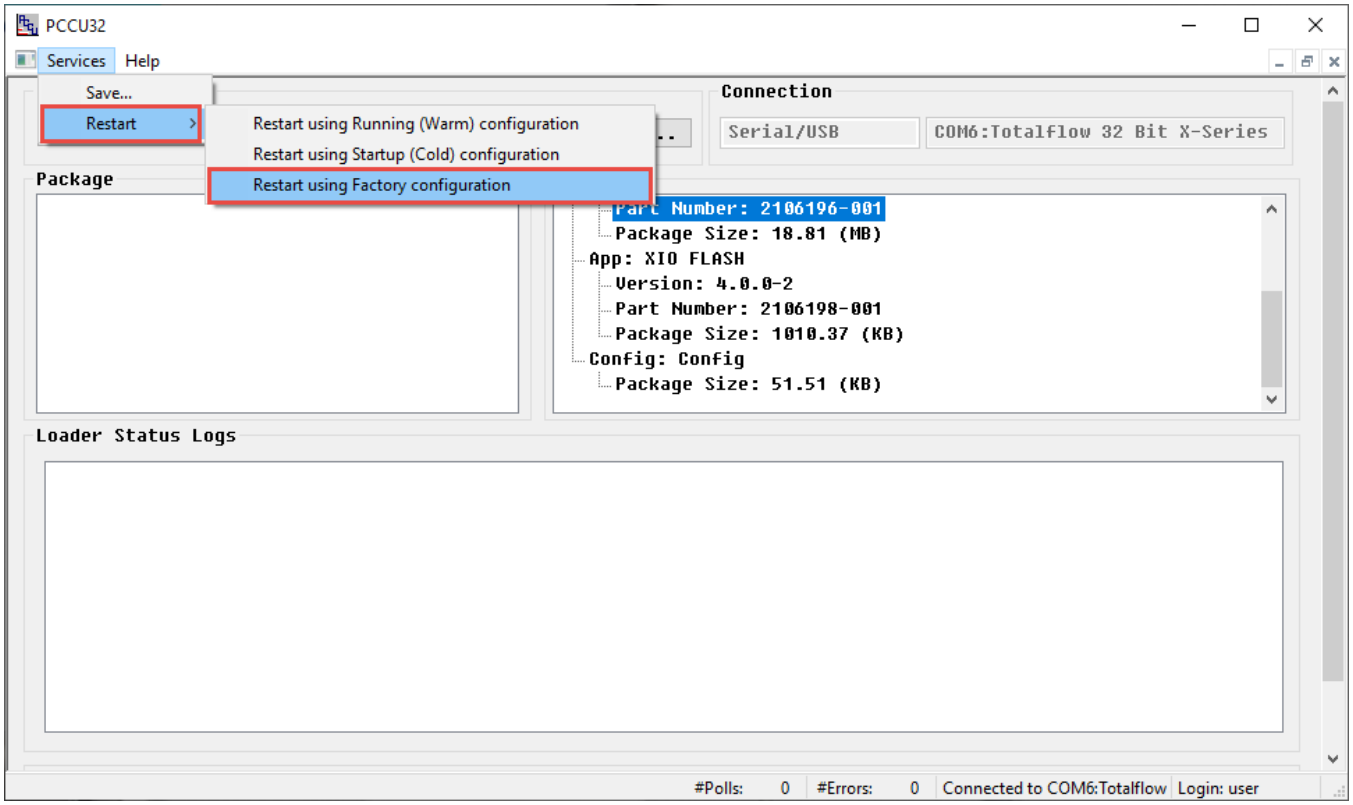
Restoring to factory configuration on a device already in-service causes service disruption and loss of network connectivity.

NOTICE – Loss of data. A restart with factory defaults deletes all data and previous configurations. Current startup and running configurations are lost. Network communication parameters are overwritten with factory defaults as well. Perform the procedures in section 8.1 Preserve data and configuration before restoring factory defaults. We do not recommend triggering the restart remotely on a network connection because the device might lose connectivity. Physical access to the device is required to reconfigure.

To restore factory configuration:

1. Launch PCCU.
2. Click the **32-Bit Loader** icon in the toolbar. A message to confirm PCCU launch displays.
3. Click **Yes**.
4. Verify the connection setup information and click **Connect**. The loader screen displays.
5. Click **Services>Restart** in the menu bar and select **Factory restart using the device loader** from the drop-down list (Figure 8-35).

Figure 8-35: Factory restart using the device loader



8.6 Remove and restore power

NOTICE – Equipment damage. Remove the external power connections before removing all other cables, boards, and field connections. Connection or disconnection of cables and wires on the electronic board while power is connected can damage the electronic components.

8.6.1 Remove power from the device

It might be necessary to remove power from a device for maintenance. This procedure describes the removal of the power port terminal connectors from the XIO. You do not need to remove individual wires.

DANGER – Serious damage to health / risk to life. Explosion Hazard: Do not connect or disconnect connectors or their terminations while energized unless the area is known to be non-hazardous.

IMPORTANT NOTE: Remove the power connector by inserting a small, slotted screwdriver between the connector and the housing.

1. Remove the power source.
2. Remove the terminal connector

8.6.2 Reconnect power to the device

Follow this procedure to reconnect the power port terminal connectors or the power cables back into the XIO. You do not need to rewire if the connectors are not removed from the cables. This procedure assumes wiring was left intact before terminal connector removal.

NOTICE – Equipment damage. Do not reconnect the external power until all service procedures are complete. This includes reconnecting all wires, plugs, terminations, and peripheral equipment. Otherwise, property damage can result. Do not perform this procedure until you receive instructions to do so.

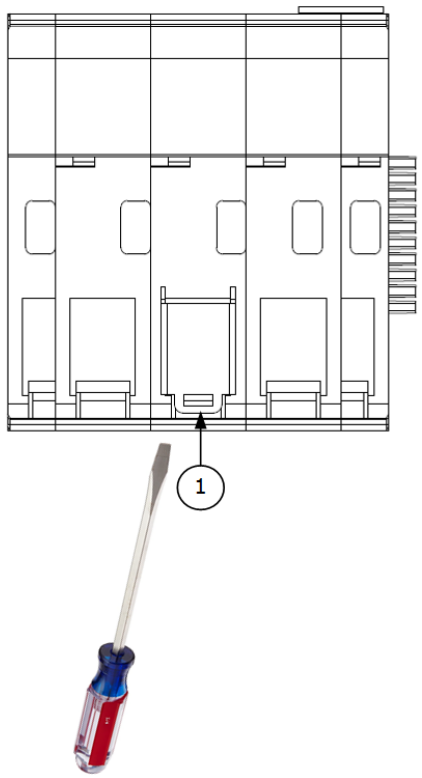
1. Reconnect the external power source cable to the board.
2. Observe the power-on sequence information on the System LEDs to confirm that the device is receiving power (see details in section 3.5.1 Power-on sequence). When all LEDs are solid, the sequence is complete.

8.6.3 Remove the XIO from the DIN rail

To remove the XIO from the DIN rail:

1. Remove terminal connectors from power ports according to section 8.6.1, Remove power from the device.
2. Remove cables from communication ports (USB and/or Ethernet).
3. Remove TFIO modules from the TFIO interface (if used).
4. Insert a slotted screwdriver into the bottom slot (Figure 8-36) of the DIN rail release clip.
5. Pull the screwdriver handle up gently to release the clip.
6. Tilt the XIO up gently and hold it to prevent it from snapping back onto the DIN rail.

Figure 8-36: Remove XIO from DIN rail



Legend: Remove XIO from DIN rail

ID	Description
1	DIN rail clip

8.6.4 Return device for repair

Securely wrap the XIO in protective anti-static packaging before returning it for repair. Call the ABB main office number on the last page of this manual and ask for a Return Authorization number (RA). Affix the number to the outside of the return package. The customer prepays for shipment.

ABB ships any device not covered by the original system warranty to the customer FOB.

8.7 Maintain cleanliness of the XIO

Devices installed as standalone should be kept free of dust and other contaminants.

NOTICE – Equipment damage. Potential electrostatic charging hazard: Clean only with a damp cloth.

When the device is installed in an enclosure, keep the enclosure door closed and secured, except during maintenance or service procedures that require access to the XIO and other components in the enclosure. Inspect the enclosure, door, and access holes regularly to ensure that all seals and gaskets are clean and intact, and that environmental elements have not reached inside of the enclosure.

Regularly inspect connected cabling to ensure that protective coverings are in place and intact. If the installation includes a solar panel, clean the cell surface of the panel regularly to ensure that dust and debris are not on the cell surface. Dust and debris inhibit the charging ability of the solar panel. Inspect all other peripheral equipment to ensure that it is properly maintained.

9 Ethernet connectivity scenarios

ABB Totalflow equipment with onboard Ethernet ports supports TCP/IP-based communications. Some devices have multiple Ethernet ports, which provide additional possibilities for Ethernet connections. This section describes several Ethernet connection types or scenarios that are helpful when planning field installations, local configuration and monitoring, remote management over a network, and connection of additional equipment.

Additional Ethernet ports in multi-port devices eliminate the need for additional network equipment in some cases. Plan the connections carefully to ensure connectivity for each device.

NOTICE – Cybersecurity risk. Plan Ethernet connections carefully to protect your device and peripherals from unauthorized or malicious access. The device should only connect to a firewall-protected private network, never directly to the Internet. For security guidelines and recommendations, see section 7 Configure security (recommended). Follow your company policies and guidelines for cybersecurity.

IMPORTANT NOTE: Never use an external port for permanent connections, such as to peripherals or additional equipment. The external ports on enclosures are reserved for local communication (configuration or maintenance only). Connect additional equipment to the device's Ethernet ports internally, following required guidelines for cable length and cable routing/management.

The illustrations in this section show the XIO as a standalone device. Adapt instructions for connections when enclosures and other network equipment are involved. XIO standalone enclosures offer an external-weather proof USB port by default. An external Ethernet port is optional. When the enclosure has an external Ethernet port, it may come internally connected to one of the XIO Ethernet ports. This connection reserves the port for local access. Use the other 3 ports for additional connections based on topology and Ethernet mode.

IMPORTANT NOTE: For additional information on Ethernet configuration parameters or connection procedures, refer to the Networking Communication Guide listed in Additional information.

9.1 Connection types supported by the XIO

The XIO Ethernet interfaces support several connection topologies in the field. This section introduces the connections and configuration modes supported by the XIO. Additional sections, later in this chapter, provide more detailed descriptions of common topologies.

IMPORTANT NOTE: For additional information on Ethernet configuration parameters or connection procedures, click **Help** from PCCU to view networking or Ethernet topics. See also Additional information for the link to the Network Communication Guide which has several connection scenarios and detailed procedures for configuration.

9.1.1 Connection types

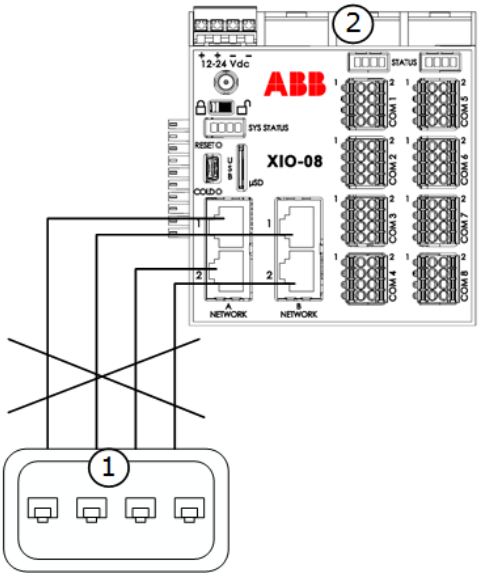
The XIO supports standard-compliant Ethernet interfaces. Its Ethernet ports support connections between the XIO and the following:

- Hosts systems (PC or laptop): for access by user interfaces and other host software for local or remote communication to configure, monitor, or collect data.
- Network equipment (Ethernet hubs/switches): to support network communications locally (onsite) or remotely (over the customer network).
- Other XIOs, remote controllers, and flow computers with Ethernet ports: to connect additional equipment without additional external Ethernet switches or network equipment. The XIO can switch traffic for attached devices when connected in daisy chain fashion.
- Other ABB or third-party control or peripheral equipment with Ethernet ports: for a variety of field peripheral equipment such as measurement devices. Peripherals must have an Ethernet port for direct connection.

IMPORTANT NOTE: If the XIO is inside an *X*CORE enclosure or in its own enclosure, connection to an XIO Ethernet port may require internal access to the XIO. An external Ethernet port may not be available on an XIO enclosure as it is optional at the time of purchase. Illustrations in the following sections show local access as direct connections to XIO ports.

IMPORTANT NOTE: When the XIO is in 4-port switch mode, never connect the Ethernet ports to an external Ethernet switch at the same time (Figure 9-1). Connecting to the same switch in this mode causes loss of connections to the device.

Figure 9-1: Incorrect Ethernet connections for an XIO in 4-port switch mode



Legend: Incorrect use of Ethernet connections

ID	Description
1	Third party Ethernet switch or hub
2	XIO

9.1.2 Ethernet modes

The connections supported by the XIO depend on the configuration of the Ethernet interfaces. The interfaces support several modes of operation, and these modes need to be taken into consideration when planning connections.

The supported modes on the XIO are:

- 4-port switch mode: factory default. All 4 Ethernet interfaces are logically combined into a single network. The 4 ports switch traffic between each other.
- 1 network mode: supported by the enterprise ports only. The two enterprise ports are logically combined into a single network (ports switch traffic between each other).
- 2 network mode: supported by both the enterprise and industrial ports. Each set of Ethernet interfaces are isolated into individual ports, each assigned to its own network. Traffic on each of the ports is isolated from the other ports. Communication in each is independent of the others.

9.2 IP parameter configuration

Ethernet connectivity requires the correct IP parameters for connecting systems. To configure a host system, controllers, flow computers or any other device supporting native Ethernet interfaces, each system must have a unique and valid IP address, the correct associated subnet mask, and a gateway (if remote or network communication is required).

IMPORTANT NOTE: IP addressing depends on the number of Ethernet interfaces or ports on the device and their configuration mode. Devices with multiple Ethernet interfaces may require more than one IP address. Consult the network administrator to determine the appropriate configuration for each specific scenario. See section 9.2.1 for additional details or see PCCU online help topics.

9.2.1 IP Addressing per Ethernet mode

IP parameter configuration depends on the way the Ethernet interfaces are configured (mode), and the number and type of connections required in the field. The table below shows several configurations and the number of IP addresses required per configuration. Ports can be assigned to the same network or to separate networks. Configure addresses only for those interfaces used. Factory default values are provided for your reference. IP addresses must be unique for communication with other devices on the same network. Factory default values are used for initial local access. They need to be replaced by valid and unique IP addresses once you determine connection topology.

Table 9-1: XIO IP addressing per Ethernet mode

Mode	Ethernet interface configuration	Ports	Number of required IP addresses	Default IP addresses (Port assigned)
4-port switch	Single interface, all ports assigned to a single network	A1+A2+B1+B2	1 address	169.254.0.13 (All ports)
Enterprise ports-1 Network, Industrial ports-2 Network	Three interfaces: 1: One for both Enterprise ports 2: One for each Industrial port	A1+A2 B1, B2	1 address for each interface used	169.254.0.13 (A1+A2) 169.254.0.15 (B1) 169.254.0.16 (B2)
Enterprise ports-2 Network, Industrial ports-2 Network	Four Interfaces: 2: One for each Enterprise port 2: One for each Industrial port	A1, A2 B1, B2	1 address for each interface used	169.254.0.13 (A1) 169.254.0.14 (A2) 169.254.0.15 (B1) 169.254.0.16 (B2)

Totalflow devices support automatic and static configuration of IP parameters. The following two sections discuss these two options.

9.2.2 Dynamic and static addressing

ABB Totalflow devices with Ethernet ports support both dynamic and static IP addressing standard methods of IP configuration. Select what is appropriate for the field conditions.

9.2.2.1 Dynamic addressing

A device with an enabled DHCP function automatically configures IP parameters. DHCP requests and obtains the IP parameters for the unit without manual intervention. This is a good option when the device can connect to a network that has a DHCP server supplying the IP configuration. Network connections must be reliable because disconnection or network outages cause the controller to lose its IP configuration. DHCP-obtained IP addresses are public IP addresses valid for connection to the customer network.

A public address is an address that is valid for the corporate IP address range assigned to a private customer network. This does not mean it is accessible from outside the customer network. Well-designed customer networks protect devices from unauthorized users with the use of firewalls and other methods implemented throughout the network.

IMPORTANT NOTE: The DHCP capability for dynamic Ethernet parameter configuration is that of a DHCP client, not a DHCP server. If no DHCP server is available on the corporate network, a local switch/router that supports DHCP can support dynamic addressing. The switch/router in this case must support the DHCP server function to provide the IP parameters when the Totalflow device requests them. To support this scenario, enable the DHCP server function in the router/network equipment before connecting. DHCP adds options to automate configuration, but carefully consider the reliability of network connections and the specific scenarios. ABB recommends static IP addressing to ensure IP configuration is not affected by failure on the network connection or local router.

9.2.2.2 Static addressing

Manually configured IP parameters do not depend on a connection to a network and DHCP server. IP parameters remain intact when they are saved in the device. Static IP addresses can be public or private. Obtain valid IP addresses from the network administrator.

9.2.3 Private and public addressing

Totalflow devices can be configured with private or public IP addresses. Select what is appropriate for the field conditions.

9.2.3.1 Private addressing

Private addressing is the default for local connection with hosts (PC or laptop) for device setup, maintenance or monitoring over Ethernet.

Equipment with Ethernet ports has default private IP addresses configured at the factory. Configure the PC or laptop with a compatible private IP address to communicate with a device in the field.

IMPORTANT NOTE: All ABB Totalflow devices have the same default address. If a field location requires network communication, and more than one device is installed at that location, the default address in each device must be changed to a unique and valid IP address.

Table 9-2 displays common examples of address blocks reserved for private addressing. Consult with the network administrator for approved configuration and parameters. General IP addressing and information about other reserved address blocks is available on publicly available Internet sites.

Table 9-2: Reserved private address blocks

Address block type	Address range	Subnet mask	Notes
APIPA (Automatic Private IP Addressing, IPv4)	169.254.0.1 to 169.254.255.254	255.255.0.0	The factory-default IP addresses on Totalflow devices are from this block: 169.254.0.11. APIPA automates the address configuration on hosts used to locally connect to the Totalflow devices. Hosts must be running Windows® 98 operating systems or later. Hosts running older operating systems require manual configuration of the IP parameters. If manual configuration is required, choose any address in this block except the one used for the device.
IETF RCF 1918 (for IPv4), 16-bit block	192.168.0.0 to 192.168.255.255	255.255.0.0	Factory-default IP addresses on third-party devices can be from this block.

IMPORTANT NOTE: ABB Totalflow devices do not support automatic configuration of private IP addresses. If the default IP address is changed or deleted, it requires manual reconfiguration. Restore the factory configuration to restore IP parameter factory defaults.

9.2.3.2 Public addressing

Use public addresses when the Totalflow device requires connectivity from the customer network and a valid IP address is available for the device. The DHCP server on the customer network usually assigns public addresses. Request a valid IP address from the network administrator and configure manually if you do not use DHCP.

ABB recommends public addresses when multiple devices on the site require Ethernet connectivity. Each device must have a unique valid IP address assignment. Public addressing replaces default IP addresses on the devices, which are then no longer in effect. Configure the PC or laptop that connects to a device in the field with a compatible public IP address for communication.

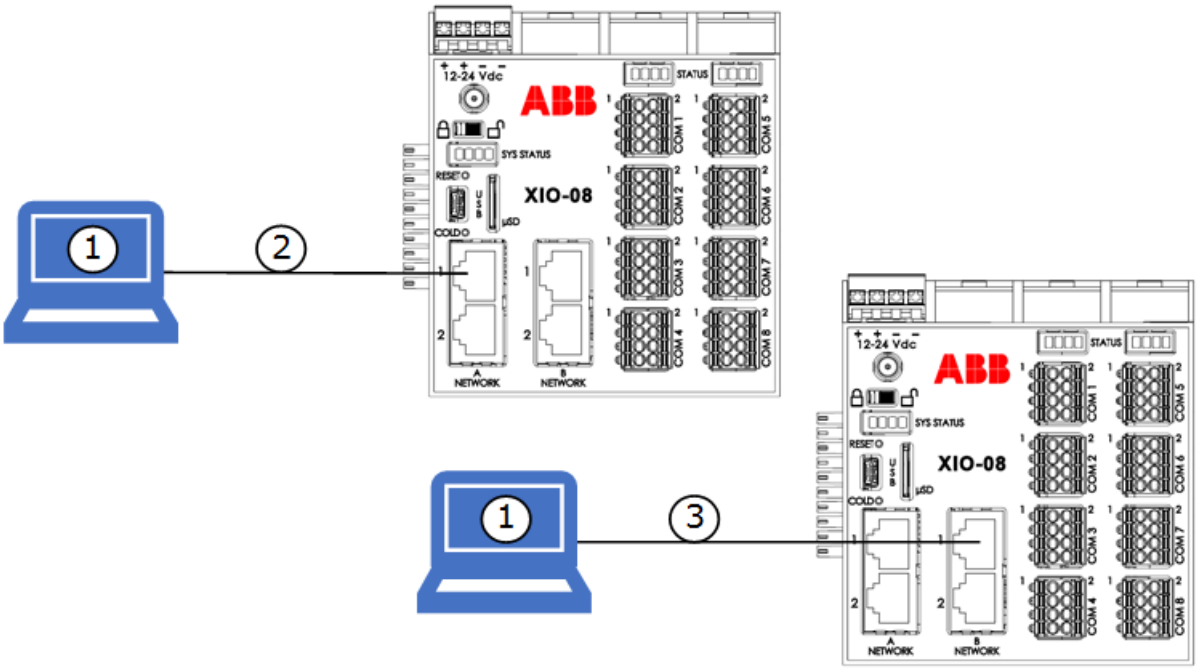
9.3 First-time local communication (4-port switch mode)

The startup configuration of the Totalflow devices requires first-time local communication. Establish a connection between a PC or laptop and the XIO after installation and power-on sequence is complete. The XIO factory default Ethernet configuration is a 4-port switch: all Ethernet ports are logically combined into a single network. Connect the laptop and the XIO directly via Ethernet on any of the Ethernet ports. Figure 9-2 shows the laptop connecting directly to the XIO on either port A1 or B1.

The default IP configuration on the XIO is available to support initial local access by an operator during installation and first-time configuration. If the XIO is configured for networking communication, a valid IP configuration for the field network must replace the factory default.

IMPORTANT NOTE: If the XIO is inside an enclosure, and the enclosure has an external Ethernet connector, use this connector for initial local communication for convenience. Connecting to the other ports requires opening the enclosure door and connecting directly on the XIO ports. External ports are meant for local access only, never for permanent field connections.

Figure 9-2: Local connection to XIO on 4-port switch mode



Legend: Local connection to XIO on 4-port switch mode

Number	Description
1	Local connection device
2	Connection to network A (either port is usable)
3	Connection to network B (either port is usable)

9.3.1 Configuration

First-time configuration of local communication using Ethernet requires that:

- The device's IP parameter and Ethernet network ports configuration are the factory-defaults.
- The PC or laptop that communicates with the controller is running a Windows® 7 or later operating system.

Enable DHCP on the laptop for automatic addressing. First-time direct connection between the XIO and the laptop does not require any configuration of IP parameters in either system, (if DHCP is enabled on the laptop.)

Table 9-3: Configuration for first-time local communication

Item	Laptop	XIO	PCCU connection setup
Ethernet interfaces	Verify the Ethernet interface is enabled. Verify the Local Area Connection is enabled.	In PCCU Entry mode, go to Communications> Networking: 4 port switch option must be selected (Enabled). Ethernet interface: Port: A1+A2+B1+B2 State: Enable	On the Setup tab: For communications, select TCP/IP For connection parameters, type the default XIO IP address: 169.254.0.13
Network (IP) Parameters	For operating systems older than Windows® 98, manually configure a private address from the APIPA block, for example 169.254.0.12. For Windows® 98 operating system or newer, the laptop auto-configures its IP address if set for DHCP. The TCP/IP properties must be set to: General: Obtain an IP address automatically (DHCP). Alternate Configuration: Automatic Private IP address	Leave defaults: IP address: 169.254.0.13 Subnet mask: 255.255.0.0	

9.4 Network communication on 4-port switch mode

The XIO controller must be configured for network communication as its core functionality depends on TCP/IP-based connections with remote controllers.

Successful network communication depends on correct configuration of valid IP parameters for all devices on a field network. Configuration depends on desired network topologies. The XIO supports several scenarios with its different modes of operation as described in section 9.1.2 Ethernet modes.

Factory default IP configuration is meant for initial local access only. Valid IP configuration for the chosen topology must replace factory defaults. Each XIO on the field must have unique IP addresses.

Local access to the XIO and other devices on the network is still supported after the default configuration is replaced, but the operator laptop must have an IP configuration compatible with the non-default addresses assigned to the XIOs. Local access is also available using Wi-Fi® as described in 10 Wi-Fi® connectivity scenarios.

Network communication supports:

- Host system-to-device access (local and remote): PCCU clients can connect to XIOs for configuration or management purposes from the corporate network or on the field.
- Device-to-device communication (local): Remote controller-XIO communication is supported when devices connect to a field network switch on independent connections (star topology) or when devices connect to each other in daisy-chain fashion.

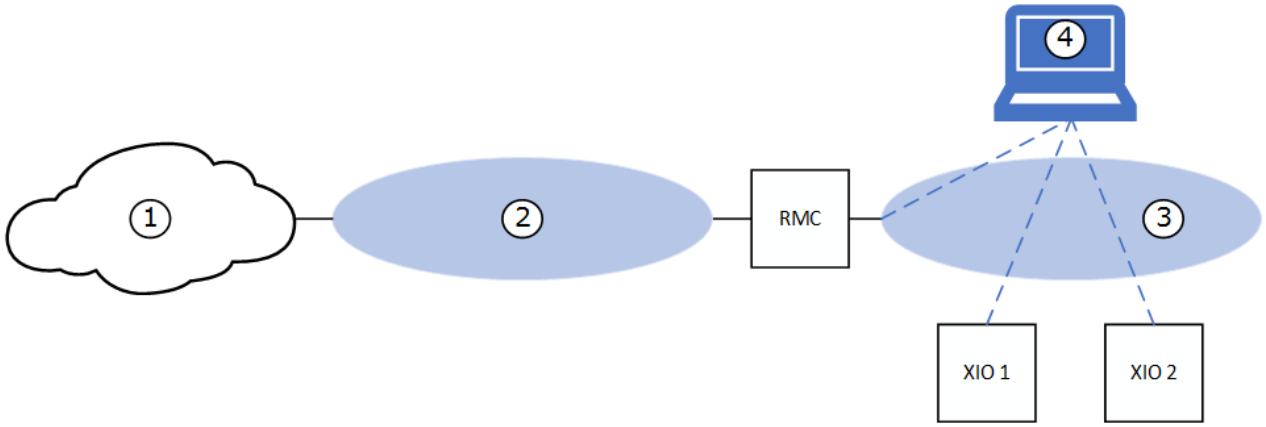
9.4.1 Daisy-chain connection support by the RMC

When the XIOs are deployed for connection to an RMC-100 in the field, they can connect to a field network switch or an RMC for the uplink connection to the corporate customer network (WAN). The RMC-100 supports this connection with its two Ethernet ports. These ports can be configured as: Switched

ports (the RMC behaves as a 2-port switch, 1 network), or as separate ports (2 networks). When connecting XIOs to RMCs, consider the following:

- An RMC in 1-Network mode forwards traffic between the network and daisy chained XIOs transparently.
- An RMC in 2-Network mode isolates daisy-chained XIOs in the field, as traffic received on the RMC's network uplink port will not be automatically switched (forwarded) to the port with the daisy-chained XIOs. Plan connections carefully to ensure that access to devices is available as required. For remote access to the XIOs, a router is required. Figure 9-3 shows local access on one of the networks associated with one of the RMC Ethernet ports (for example E2).

Figure 9-3: RMC on 2-Network mode supports local access only

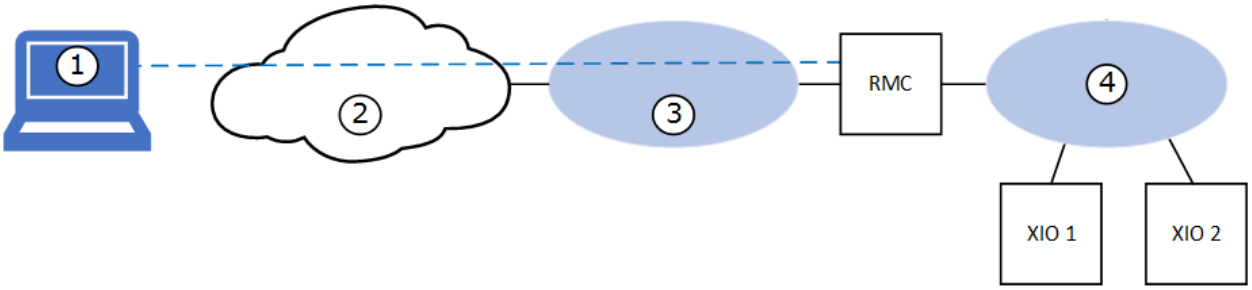


Legend: RMC on 2-Network mode supports local access only

ID	Name	ID	Name
1	Customer (TCP/IP) network	**3**	RMC: E2-LAN
2	RMC: E1-LAN	**4**	Local host system with PCCU

Figure 9-4 shows that remote access is only available to the RMC. Access to the XIOs is not possible in this scenario as the RMC does not route between E1 and E2. Traffic from the network is not forwarded to the XIOs.

Figure 9-4: RMC on 2-Nework mode isolates XIOs on local field network



Legend: RMC on 2-Network mode isolates XIOs on local field network

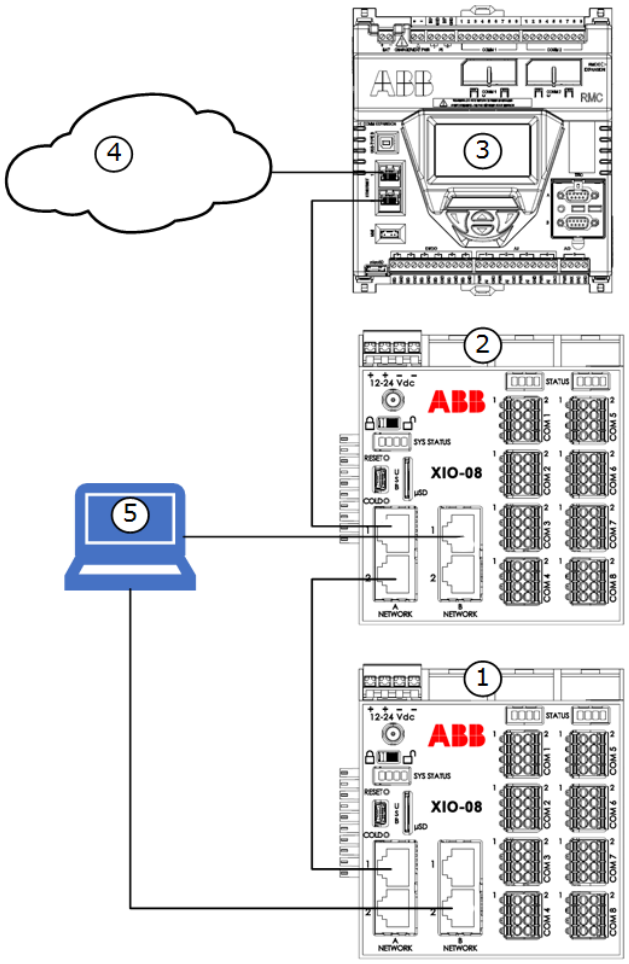
ID	Name	ID	Name
1	Local host system with PCCU	**3**	RMC: E1-LAN
2	Customer (TCP/IP) network	**4**	RMC: E2-LAN

9.4.2 Local access by host

Figure 9-5 shows the connections for local access by a host for devices daisy-chained in the field. In this example, the RMC (3) is configured as a 2-port switch (Ethernet interfaces E1 and E2 are set to 1-Network Mode). The XIOs (1, 2) are configured as 4-port switches (Ethernet interfaces A1, A2, B1, and B2 set to 4-port switch mode). The first XIO (2) connects to the RMC with A1, and to the second XIO (1) with A2.

To establish communication with the devices, the operator can connect the host system (5) to any of the available ports without permanent connections. The figure shows two connections from the host as examples, but only one physical connection is needed. When the host connects to either interface, it is connecting to the common network the switched-mode interfaces provide. See the logical equivalent of this configuration in Figure 9-6.

Figure 9-5: Local access by host – supported physical connections (daisy-chain topology)



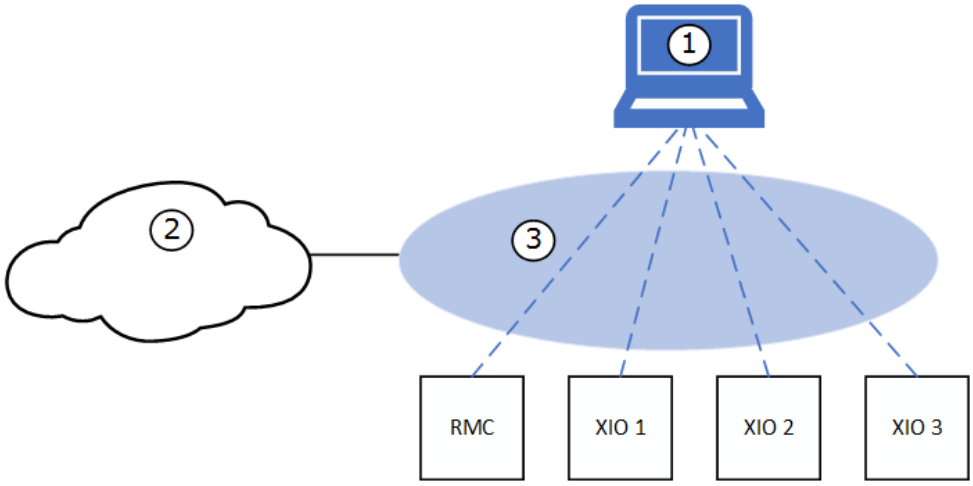
Legend: Local access by host – supported physical connections (daisy chain topology)

ID	Name	ID	Name	ID	Name
1	XIO-2 in the daisy chain	**3**	RMC-100	**5**	Host system with PCCU: local access through XIO-1(B1) or XIO-2(B2).
2	XIO-1 in the daisy chain	**4**	Customer (TCP/IP) network		

Figure 9-6 shows the logical network equivalent to the connections shown in Figure 9-5 above. A local system with PCCU (1) can establish connections to each daisy-chained device on the same network (3). Each device must have an IP address with the same subnet assigned to the network. The host must also have that same subnet in its IP address. Note that connections lines on diagrams are independent logical

TCP/IP based connections to each device (from a PCCU instance for each). The host connects to any available Ethernet port on any of the XIOs (physical connection not shown).

Figure 9-6: Local access by host – Logical connections to all daisy-chained devices



Legend: Local access by host – Logical connections to all daisy-chained devices

ID	Name	ID	Name
1	Host system with PCCU	**3**	Field Network (all devices, same subnet)
2	Customer (TCP/IP) network		

9.4.3 Remote access by host

Network communication is necessary for remote management of the device over a TCP/IP network (customer private network). Hosts can have remote access to the XIO when both the host and the XIO are configured with valid IP parameters to connect to the customer network.

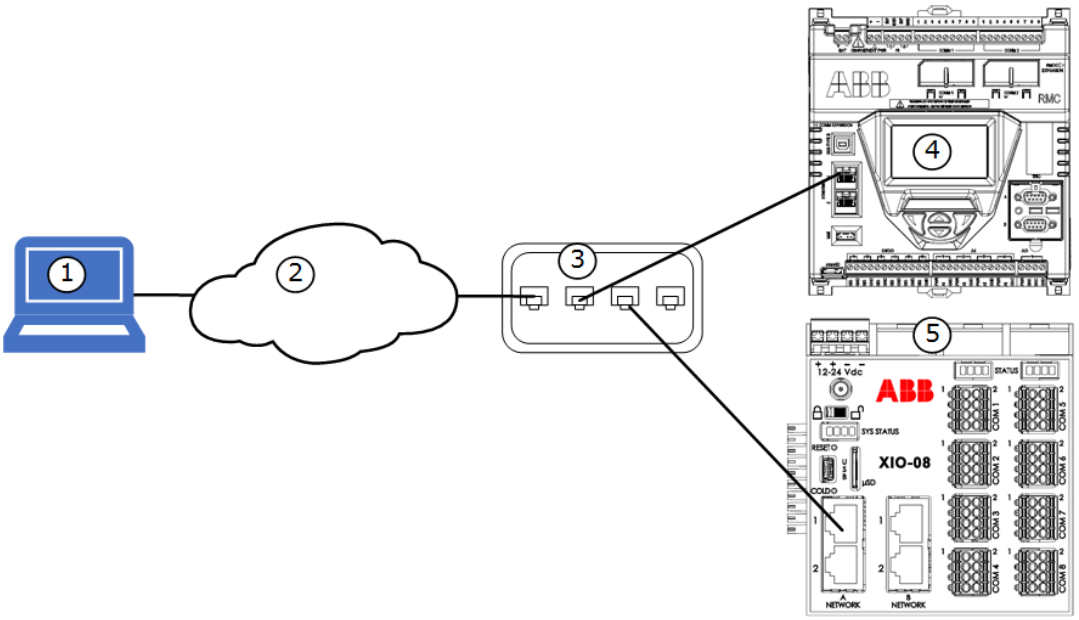
In 4-port switch mode, the XIO requires only a single valid IP address which the host can use to establish connection over the network.

9.4.3.1 Host connects to XIO on field network switch (star topology)

XIO connects to the network in star topology. Figure 9-7 shows the network connection for the XIO on a field switch (3) in a star topology implementation. This connection requires that a network switch is available in the field and that there are enough ports available for additional equipment or XIOs.

IMPORTANT NOTE: When the XIO is in 4-port switch mode, you can use any of the Ethernet ports (A1, A2, B1 or B2) to connect to the network switch. You can move the connection to any of the ports without the need to reconfigure the IP address of the XIO. Keep consistency in selecting the ports for network connection when installing multiple XIOs, for example use A1 port.

Figure 9-7: Remote access by host - supported physical connections (star topology)



Legend: Remote access by host – supported physical connections (star topology)

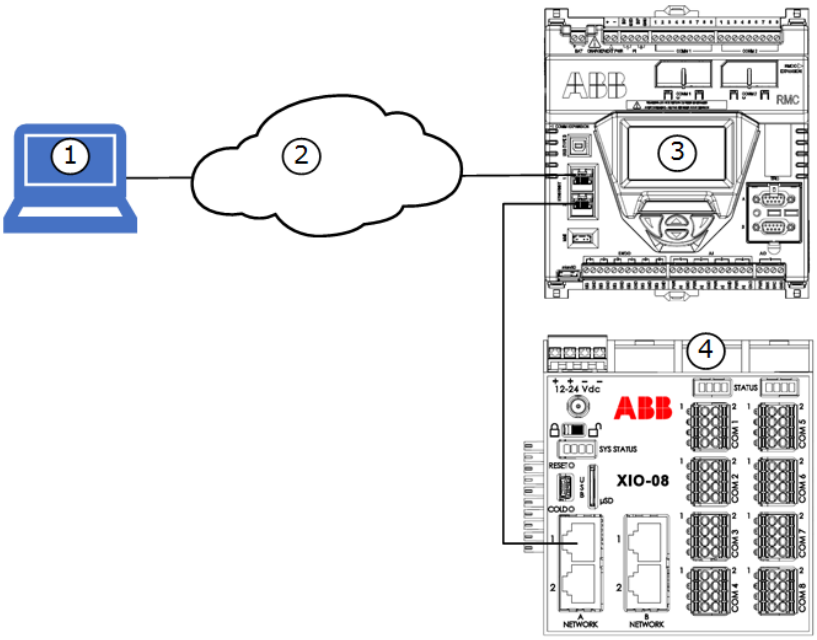
ID	Name	ID	Name	ID	Name
1	Host System with PCCU	**3**	Field Ethernet switch	**5**	XIO (Network connection on A1)
2	Customer (TCP/IP) network	**4**	RMC-100		

9.4.3.2 Host connects to XIO daisy-chained to RMC

Figure 9-8 shows the network connection for the XIO through an RMC-100 in a daisy-chain topology. This connection requires that the RMC-100 Ethernet interfaces are configured in 1 Network mode. This mode allows the RMC-100 to behave as a 2-port switch to switch traffic between the network and the XIO. This scenario may be necessary when there are not additional ports available on a field network switch.

IMPORTANT NOTE: When the XIO is in 4-port switch mode, any of the Ethernet ports (A1, A2, B1 or B2) are usable to connect to the RMC-100. Move the connection to any of the ports without reconfiguration of the IP address of the XIO.

Figure 9-8: Remote access by host – supported physical connections (daisy chain topology)

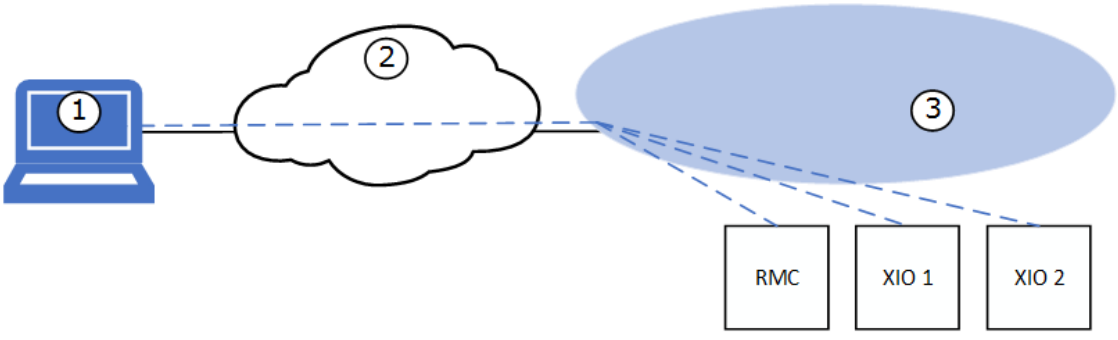


Legend: Remote access by host – supported physical connections (daisy chain topology)

ID	Name	ID	Name
1	Host system with PCCU	**3**	RMC (Ethernet ports configured in 1-Network Mode)
2	Customer (TCP/IP) network	**4**	XIO

Figure 9-9 shows the logical network equivalent to the connections shown in Figure 9-7 and Figure 9-8 above. A remote system with PCCU (1) can establish connections to each device (connected to local switch or daisy-chained) on the same network (3). Each device must have an IP address with the same subnet assigned to the network. Note that connections lines on the diagram are independent logical TCP/IP based connections to each device (from a PCCU instance for each). The host connects to the corporate network (2).

Figure 9-9: Remote access by host – logical connections



Legend: Remote access by host – logical connections

ID	Name	ID	Name
1	Host system with PCCU	**3**	Field network
2	Customer (TCP/IP) network		

9.4.3.3 Configuration

Remote communication over a TCP/IP network requires that:

- Valid IP addresses are available for both the laptop and the XIO.
- Network equipment is available (with links that are active and reliable), or additional equipment supports daisy-chain connections.
- A DCHP server is available on the network or on the local switch/router equipment if you configure the XIO for dynamic addressing.

Table 9-4 describes the configuration for the remote host, the XIO, and PCCU for communication over a network.

IMPORTANT NOTE: When configured as one network (1-Network mode), Enterprise or Industrial Ethernet port 1 and port 2, are physically separate but do not have separate identification or IP addresses in the user interface. When you enable, disable, or configure Ethernet, it enables, disables, or configures both ports. Both port sets are assigned a single IP address regardless of the Ethernet port (1 or 2) used for the network connection.

Table 9-4: Configuration for remote communication with networked XIO (ports A1 or A2)

Item	Remote host	XIO	PCCU connection
Ethernet interfaces	Verify that the Ethernet interface is enabled: Verify the Local Area Connection is enabled. Verify the Ethernet link is active.	In PCCU Entry mode, go to **Communications**>**Networking**: 4 port switch option must be selected (Enabled). Ethernet interface: Port: A1+A2+B1+B2 State: Enable	On the Setup tab: For communications, select **TCP/IP**. For connection parameters, type the IP address assigned to the XIO. If the IP address is assigned by DHCP, obtain the address from the Networking tab after the XIO is restarted.
Network (IP) parameters	Valid public IP address either through DHCP or manually configured	Change factory default IP parameters for valid public IP parameters and restart the XIO. In PCCU Entry mode, go to **Communications**>**Networking**: For dynamic addressing: Set DHCP to **Yes** (Enable DHCP). For static addressing: Obtain valid public IP parameters from network administrator and configure manually.	

9.4.4 Device-to-device communication

Device-to-device communication includes the communication flow between Totalflow applications running on the different devices installed in the field and connected through a network.

Using client-server-based communication, client applications on one device can request and establish a TCP/IP connection to a server application on another device.

In the case of the XIO, its core functionality depends on secure and stable TCP/IP based connections with a remote controller. These connections must have their end points correctly configured for communication to establish and succeed.

Table 9-5 shows the connections required for successful implementation of XIOs. These connections require that the end points (responsible for establishing and maintaining the connection), be on devices connected to the same network. Each application end point must be configured with a unique IP address valid for that network.

When configuring IP parameters consider the following:

- When both the RMC and XIOs are in switched mode, the RMC and the XIOs need unique IP addresses with the same subnet as the single network segment resulting from this mode.
- When the RMC is not in 2-port switch mode, the RMC requires two IP addresses for each of its Ethernet Interfaces. One for the connection upstream to the local network switch or to the corporate network. The other for the connection to the XIOs. In this case, the RMC IP address must have the same subnet as the network it connects to for communication with the XIO.
- When XIOs are not in 4-port switch mode, the XIO IP address configuration depends on how the interfaces are configured and what network segment is used to connect both the RMC and the XIO.

Unless routers are installed in the field network, traffic between different subnets is not possible. Plan your field network topology carefully.

Table 9-5: Required connections for XIO – RMC communication

Client app (RMC)	Server app (XIO)	Connection end points	Network Config
XIO Interface	XIO [Read] Server	RMC IP to XIO IP/Read TCP port	Both end points MUST be on same network.
XIO Interface	XIO Write Server	RMC IP to XIO IP/Write TCP port	Both end points MUST be on same network.
Communication Application Instance	Ethernet-Serial Passthrough instance	RMC IP to XIO IP/E-S Instance TCP port	Both end points MUST be on same network.

9.5 Enterprise and industrial (3-network) support

The 4 Ethernet interfaces on the XIO can support separate networks in two sets: The Enterprise Network ports (port A1 and port A2) and Industrial Network ports (port B1 and port B2). Each of these sets can be configured independently of the other to provide additional connection and topology options in the field.

IMPORTANT NOTE: Separate configuration options for these ports become available only when the XIO 4-port switch mode is disabled. Configuring an XIO for 3 Network support requires 3 separate subnets. The IP address for each supported interface must have the correct subnet.

The Enterprise port set (A-Networks) supports both 1-Network and 2-Network modes. The Industrial port set (B-Networks) supports only 2-Network mode. For this scenario, the Enterprise Network set is left on 1-Network mode.

Table 9-6 summarizes the configuration options for this scenario. The Enterprise Network ports can be used for device management connections (connections supporting remote or local host access) and the industrial ports can be used for application and measurement data traffic (supporting device-to-device communication flows). This scenario supports complex applications with several XIOs and where there is need to isolate XIOs in separate subnets or domains within in the field. Consult with ABB Technical Support for more details.

Table 9-6: Enterprise and industrial networks - configuration

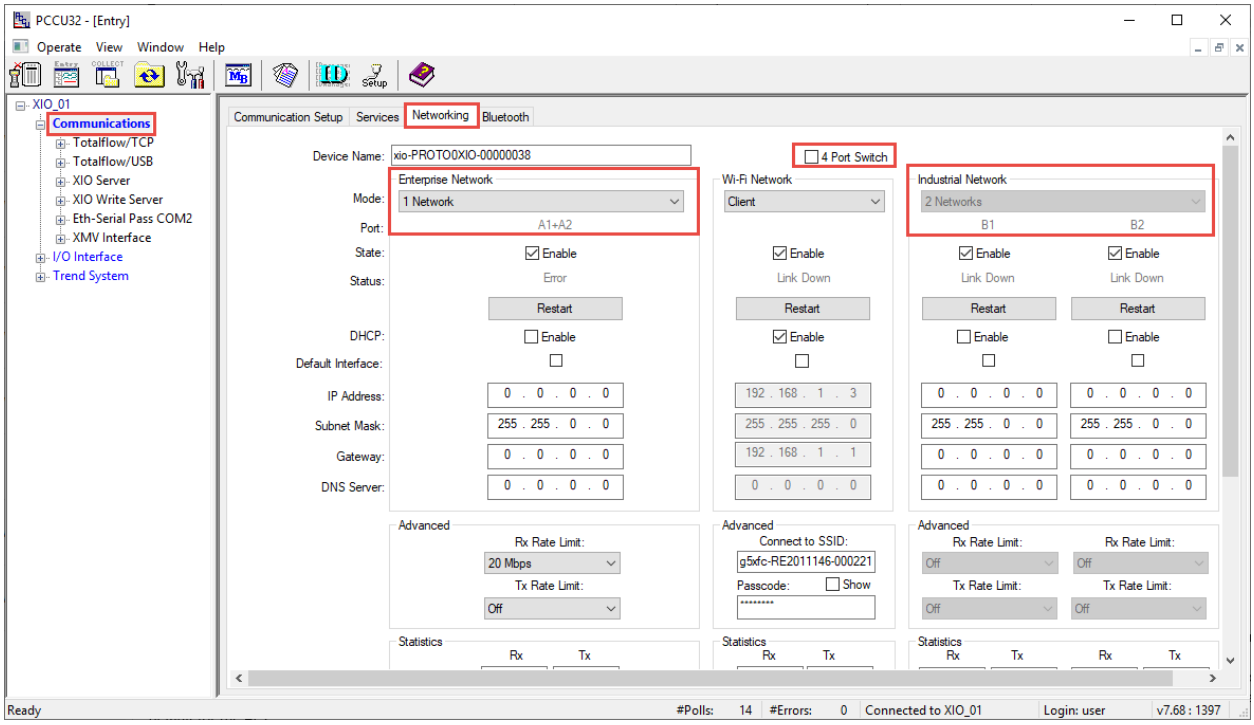
Ports: Mode	Ethernet interface configuration	Interface	Number of Networks	Number of required IP addresses
Enterprise ports: 1 Network	1: One for both Enterprise ports	A1+A2	1	One per interface: (A1+A2)
Industrial ports: 2 Networks	2: One for each Industrial port	B1, B2	2	One per port: (B1 IP, B2 IP)

9.5.1 Configuration

To configure for 3-network support:

1. Connect to the XIO on PCCU entry mode.
2. On the navigation tree, select **Communications**. The Communication Setup screen displays.
3. Select the **Networking** tab.
4. Clear the **4-Port switch** mode checkbox to display options.
5. Click **Send**. The Enterprise (A-Network) and Industrial (B-Network) interfaces activate for individual configuration (Figure 9-10). In new systems, default or factory IP addresses may display for each of the interfaces.

Figure 9-10: XIO 3 network support (1 Enterprise and 2 Industrial networks)



6. On the Enterprise Network section, in the **Mode** drop-down list, leave the default: 1-Network.
7. Select **Enable** for the State of the A1+A2 interface. The IP parameter fields activate for configuration.
8. Change the default IP parameters to the required IP parameters for LAN connection.
9. Click **Send**.
10. Click **Restart**.
11. Verify that the link status for the interface shows: Ready

IMPORTANT NOTE: After completing the configuration of the Enterprise interface, a single (A1+A2) interface should display as an option in the Enterprise Interface drop-down list in the XIO's Port Forwarding tab. If the XIO will be used in port forwarding mode, see section 9.7.7 Define port forwarding rules.

12. On the Industrial Network section, select **Enable** for the State of the preferred port (B1 or B2). The IP parameter fields activate for update. If you are enabling both interfaces, enable the state for each and configure each interface.
13. Configure IP parameters as required.
14. Click **Send**.
15. Click **Restart**.
16. Verify that the link status for the configured interface shows: Ready.

IMPORTANT NOTE: After completing the configuration of the Industrial interfaces, the enabled interface (B1 or B2) should display as an option in the Enterprise Interface drop-down list in the Port Forwarding tab. If both interfaces have been configured, each will display in that list. If the XIO will be used in port forwarding mode, define port forwarding rules. See section 9.7.7 Define port forwarding rules.

9.6 Enterprise and industrial (4 Network) support

The 4 Ethernet interfaces on the XIO can support separate 4 separate networks: 2 networks by the Enterprise Network ports (port A1 and port A2) and 2 networks by the Industrial Network ports (port B1 and port B2). Each of these ports can be configured independently of the other to provide additional connection and topology options in the field.

IMPORTANT NOTE: Separate configuration options for these ports become available only when the XIO 4-port switch mode is disabled. Configuring an XIO for 4 Network support requires 4 separate subnets. The IP address for each supported interface must have the correct subnet.

Table 9-7 summarizes the configuration options for this scenario. In this scenario all 4 interfaces support separate networks. Traffic in each network is isolated to that network. The XIO does not route traffic between interfaces. This scenario supports complex applications with several XIOs and where there is need to isolate XIOs in separate subnets or domains within in the field. Consult with ABB Technical Support for more details.

Table 9-7: Separate 4-network support

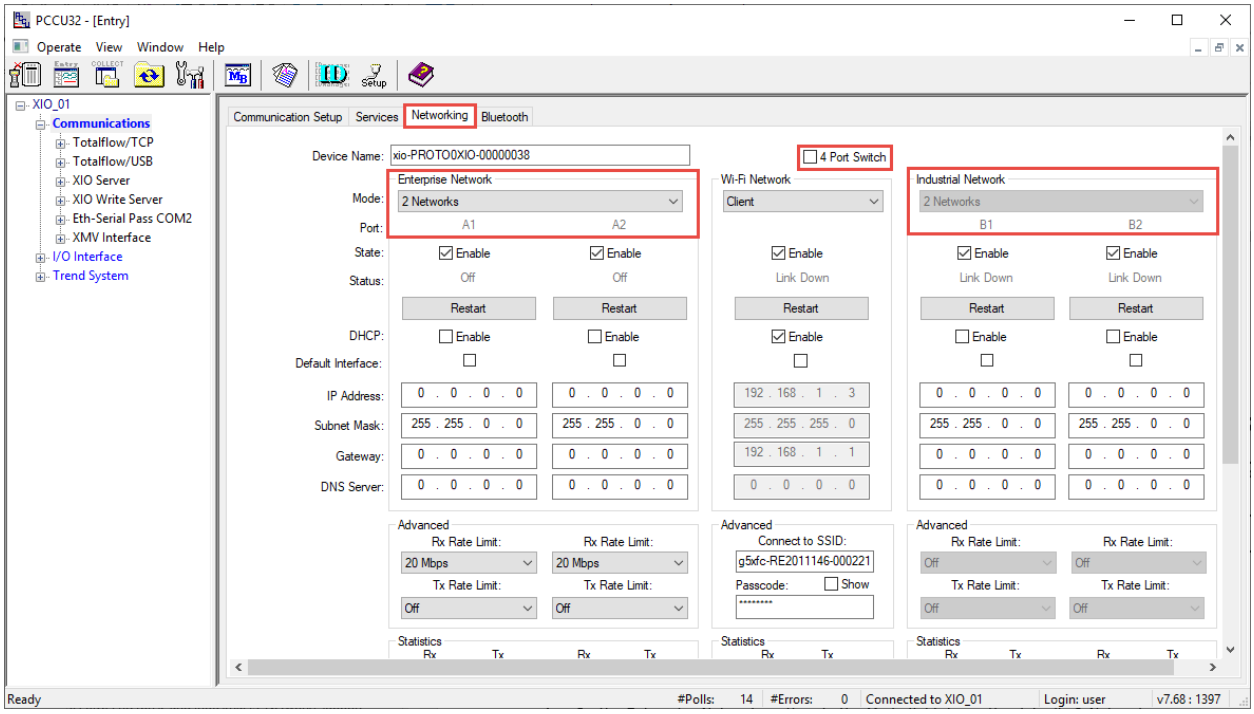
Ports: Mode	Ethernet interface configuration	Interfaces	Number of networks	Number of required IP addresses
Enterprise ports: 2 Networks	Two interfaces: One for each Enterprise port	A1, A2	2	One per port: (A1 IP, and A2 IP)
Industrial ports: 2 Networks	Two interfaces: One for each Industrial port	B1, B2	2	One per port: (B1 IP, B2 IP)

9.6.1 Configuration

To configure for 4-network support:

1. Connect to the XIO on PCCU entry mode.
2. On the navigation tree, select **Communications**. The Communication Setup screen displays.
3. Select the **Networking** tab.
4. Clear the **4-Port switch** mode checkbox.
5. Click **Send**. The Enterprise (A-Network) and Industrial (B-Network) interfaces activate for individual configuration. In new systems, default or factory IP addresses display for each of the interfaces.

Figure 9-11: XIO 4 Network support (2 Enterprise and 2 Industrial Networks)



6. On the Enterprise Network section, in the **Mode** drop-down list, select: 2 Networks.
7. Click **Send**. Two separate interfaces display: A1 and A2, each may have its own factory default address (new systems).
8. Click **Restart**.
9. Select **Enable** for the State of each interface. The IP parameter fields activate for configuration.
10. Configure or update all IP parameters for each interface as required.
11. Click **Send**.
12. Click **Restart** for each interface.
13. Verify that the link status for each interface shows: Ready.

IMPORTANT NOTE: After completing the configuration of each Enterprise interface, both A1 and A2 should display as options in the Enterprise Interface drop-down list in the XIO's Port Forwarding tab. If the XIO will be used in port forwarding mode, define port forwarding rules. See section 9.7.7 Define port forwarding rules.

14. On the Industrial Network section, select **Enable** for each preferred interface (B1 and B2). The IP parameter fields activate for update.
15. Configure IP parameters as required.
16. Click **Send**.
17. Click **Restart** for each interface.
18. Verify the link status shows for the configured interface shows: Ready.

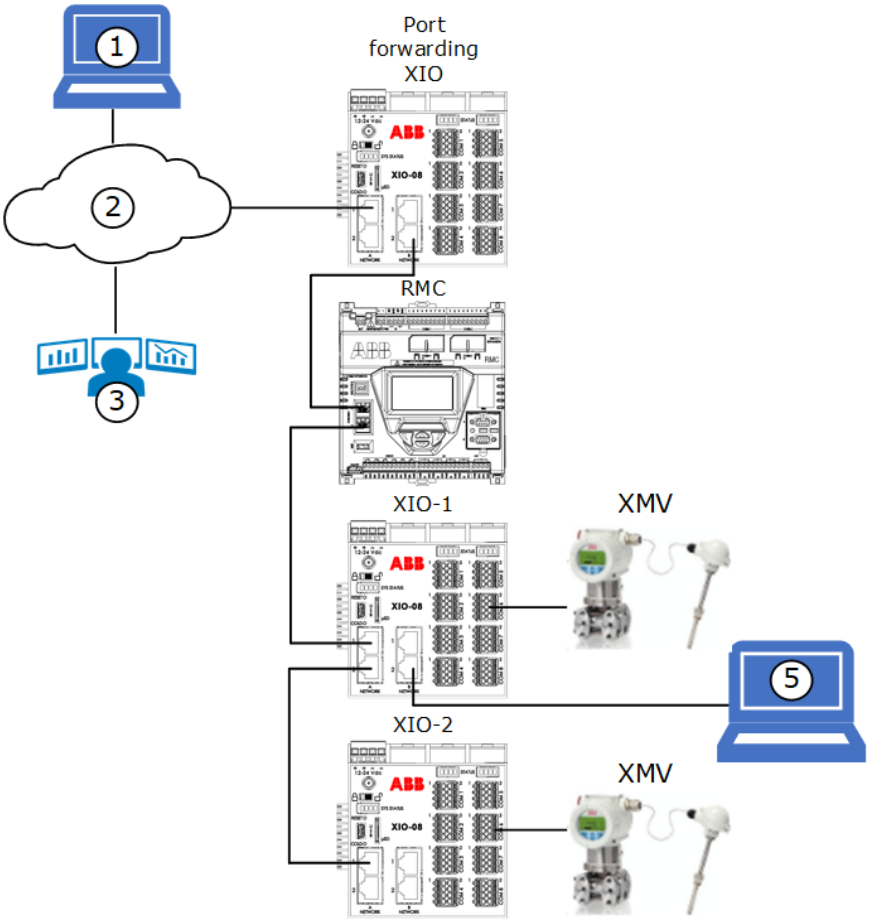
IMPORTANT NOTE: After completing the configuration of the Industrial interfaces, the enabled interfaces (B1 and B2) should display as options in the Enterprise Interface drop-down list in the Port Forwarding tab. If the XIO will be used in port forwarding mode, define port forwarding rules. See section 9.7.7 Define port forwarding rules.

9.7 Port forwarding

The XIO 3- or 4-network support provides options to separate connected Totalflow devices into different logical networks. In addition to this capability, the XIO also supports port forwarding. When an XIO is in port forwarding mode, it can be used as a gateway with specific rules to control access to other field devices. For example, the XIO can be connected to the corporate network on one of its Ethernet interfaces

and connected to other field devices on any of the other available Ethernet interfaces. Figure 9-12 shows an example of this scenario.

Figure 9-12: Use of a port forwarding XIO to securely isolate field LAN from WAN



The XIO connection to the corporate network (2) is considered the uplink connection (also referred to as the enterprise connection in PCCU). The connections to field devices (on XIO port B2) are local connections. In the example in Figure 9-12, devices (RMC, XIO-1, XIO-2) are daisy-chained. For security, the port forwarding XIO can be configured to keep the uplink connection to the corporate network isolated from the connections to the field while still allowing access to specific devices and their enabled services. That is, the Enterprise (A-Network) is separated from the Industrial (B-Networks).

IMPORTANT NOTE: The term "uplink" in port forwarding refers to the interface used for the connection to the wide area network. The Port Forwarding tab uses the term "enterprise" for the interface for this connection. Note that any of the Ethernet interfaces that are active and enabled can be selected as the enterprise interface from the Enterprise Interface drop-down menu on the Port Forwarding tab. Therefore, any A-Network or B-Network interface can be selected, not just A interfaces (which are the ones referred to as Enterprise interfaces on the Networking tab). The choice depends on the customer requirements for field connections.

9.7.1 Configuration overview

Port forwarding requires careful selection and configuration of the Ethernet interfaces used for WAN and LAN connections. Review sections 9.7.2 Ethernet interface IP addressing guidelines and 9.7.3 Determine field connections to determine configuration requirements for your field conditions. Sections 9.7.4 Use A-Network ports for field LAN connections and 9.7.5 Use A-Network ports for WAN (uplink) connection provide two example scenarios.

Sections 9.7.6 Enable port forwarding and 9.7.7 Define port forwarding rules describe how to enable port forwarding and configure forwarding rules on the XIO. These procedures assume that the devices for

which the XIO executes port forwarding are correctly configured and that their Ethernet interfaces are correctly configured and enabled. The procedures also assume the port forwarding XIO interfaces are configured correctly, enabled, and ready.

IMPORTANT NOTE: The port forwarding function can be enabled and configured on the Port Forwarding tab in PCCU. On this tab, click **Help** for additional configuration details.

9.7.2 Ethernet interface IP addressing guidelines

Port forwarding protocols provide the ability to use private addressing to reduce the number of unique valid public IP addresses required. With port forwarding enabled on an XIO in the field, devices attached to the XIO may be configured with addresses from any of the reserved private address ranges defined by the Internet authorities.

There are several private addressing ranges. Customers must configure their IP parameters based on their IT requirements. The port forwarding procedures in this document show addressing from one of the private address ranges as an example. Consult with your IT administrator for the recommended parameters and conventions used in your company.

The factory default addresses for Totalflow Ethernet interfaces are from the 169.254.0.1 to 169.254.255.254 range. These addresses are typically used for local point-to-point connection with the device. It is expected that those default addresses will be changed to unique IP addresses on interfaces used to connect to the field LAN. You may use addresses from the other ranges available. For more information, see the **IP addressing/G5/RMC/XIO** topic in the PCCU Help files.

9.7.3 Determine field connections

The XIO has 4 Ethernet ports available for network connections. There are several ways to use these ports based on the Ethernet modes available. The default configuration is 4-port switch mode. Clear this mode before configuring XIO port forwarding. Table 9-8 shows the available XIO Ethernet interfaces when not in 4-port switch mode. Any interface can be selected as the enterprise or uplink connection. The choice depends on the desired topology. Note that the B-Network ports are always independent (they cannot be combined into a single network). The A-Network ports can be either combined (1-Network mode, 2-port switch behavior) or independent (2-Network mode).

Table 9-8: Supported mode by Ethernet ports

Ethernet Ports	Mode	Configurable uplink interface options
A-ports, B-ports	4-port switch	None
A-ports	1-Network	A1+A2*
B-ports	2-Network **	B1, B2
A-ports	2-Network	A1, A2
B-ports	2-Network **	B1, B2

* Use either port A1 or A2 for actual physical connection

** B-Network ports support only 2-Network mode. B ports are always two independent interfaces.

Sections 9.7.4 Use A-Network ports for field LAN connections and 9.7.5 Use A-Network ports for WAN (uplink) connection provide examples for selecting interfaces for field connections.

IMPORTANT NOTE: Consider leaving ports available for local access when planning connections. It is assumed that local access to any device once it is in-service should be done without disconnecting the device from the field LAN.

9.7.4 Use A-Network ports for field LAN connections

The interface selected as the uplink (enterprise interface) depends on customer preference and access requirements in the field. As an example, Figure 9-13 shows a scenario where the A-Network is used for field connections. In this scenario, if A-Network ports are set to 1-Network mode (A1+A2), then they can

be used for field network connections. Connections on A1 and A2 are part of the same logical network. One port (A2 for example) can be used to connect other field devices in daisy-chained configuration.

The other port (A1) can be left available for local connection by an operator or field technician (see connection for laptop 4 in the figure). Connection to A1 gives access to all the devices, provided that the operator laptop is configured with a compatible IP address.

With this configuration, if the other devices are not collocated with the XIO, operators do not have to move to the location of the other devices to access them. Access is available from the A1 port. In this scenario, either interface B1 or B2 can be selected as the enterprise or uplink interface to the corporate WAN (2). Local access to all devices associated with the A1+A2 Network is also available on any unused port on those devices (See laptop 4 connecting to A1 on the port forwarding XIO and laptop 5 connecting to port B2 on the XIO-1).

Figure 9-13: Use A-Network ports for field LAN connections

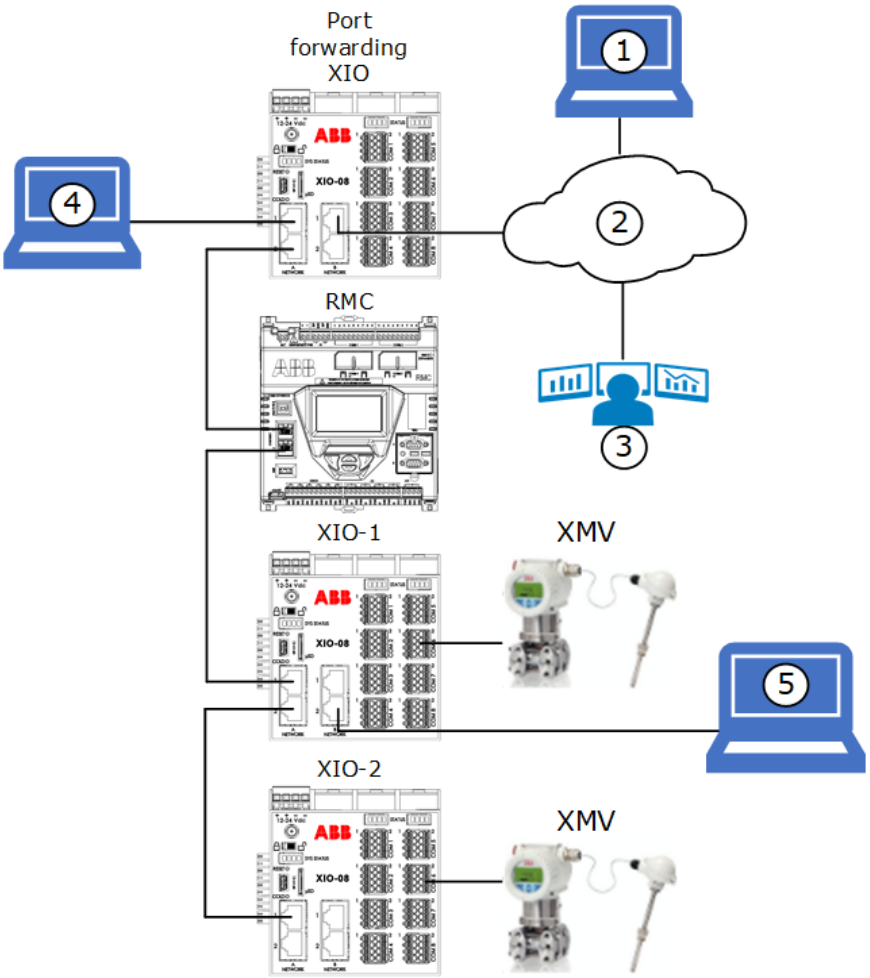
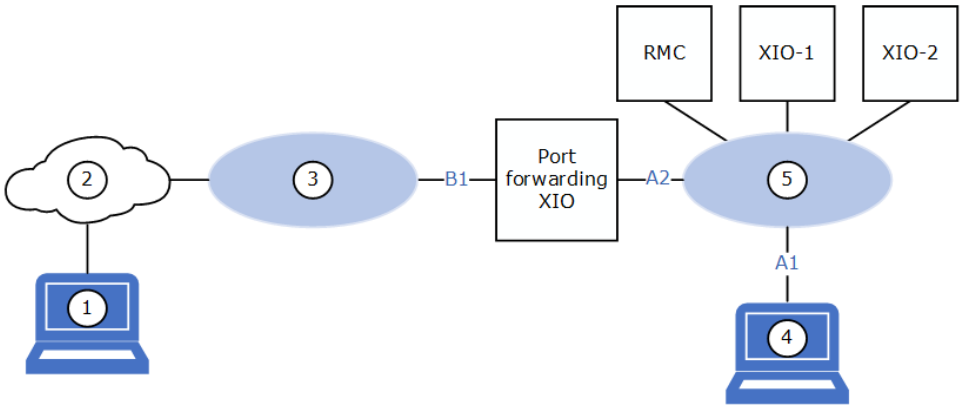


Figure 9-14 shows a logical diagram of the networks associated with the B1 interface (network 3) and the A1+A2 interface (network 5). The operator can connect to the port forwarding XIO on port A1 (see laptop 4) and be able access all field devices on that logical network (5). The RMC, XIO-1, and XIO-2 are configured in 2- and 4-port switch modes. All their Ethernet interfaces are associated with network 5.

Figure 9-14: Logical network diagram when A-Network ports are used for field LAN



9.7.5 Use A-Network ports for WAN (uplink) connection

A-Network interfaces can also be used as the enterprise interface whether in 1-Network or 2-Network mode. Either of the B-Network ports can be used to connect to other devices in daisy-chain configuration. The example in the figure below shows port A1 on the port forwarding XIO connected to the corporate WAN (2). The field devices connect to port B2. In this scenario, local access to the field devices attached to the port forwarding XIO will need a connection to an available port on any of these devices (see connection of laptop 5). Connecting to the port forwarding XIO directly (see connection of laptop 4) provides access only to that XIO, since the A-Network ports and B-Network ports are in separate logical networks.

Figure 9-15: Use A-Network ports for WAN (uplink) connection

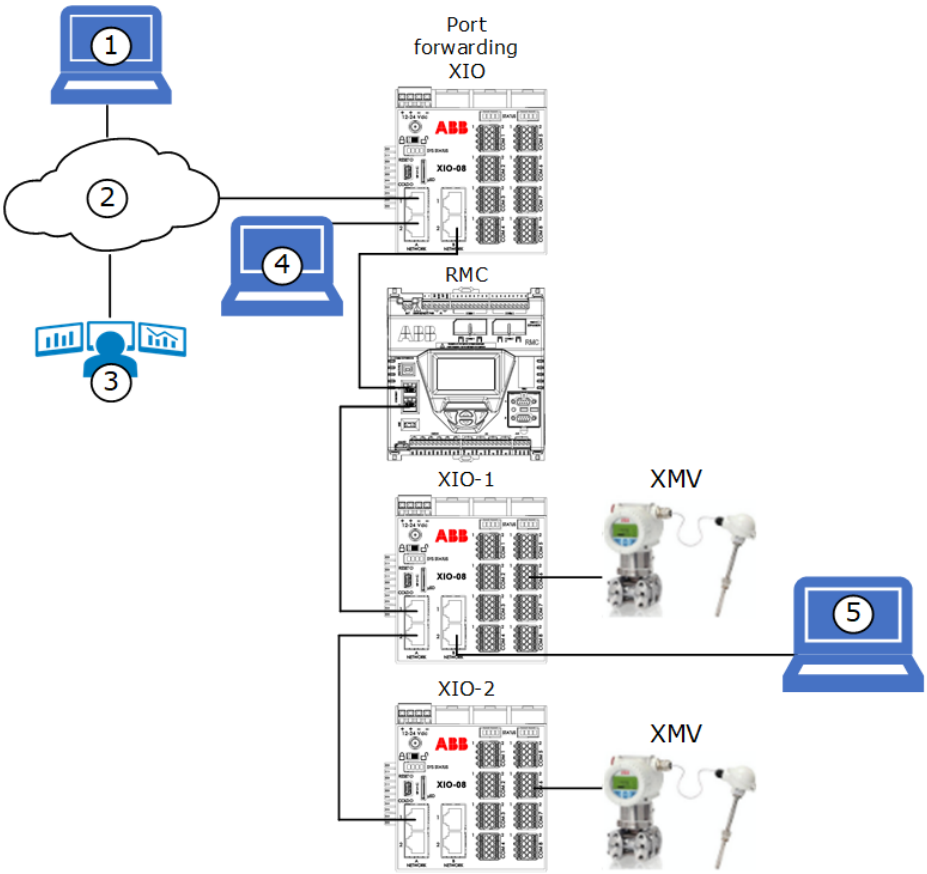
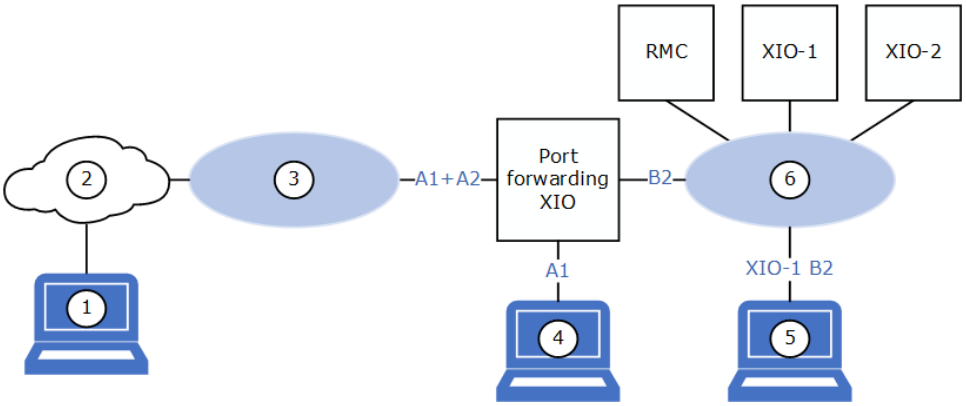


Figure 9-16 shows a logical diagram of the networks associated with the A1+A2 interface (network 3) and the B2 interface (network 6). The operator (see laptop 4) can connect to the port forwarding XIO on port A1 and access only that XIO. To access the other devices, the operator (see laptop 5) connects to an available port on one of the other XIOs (for example, XIO-1 port B2). The RMC, XIO-1, and XIO-2 are configured in 2- and 4- port switch modes. All of their Ethernet interfaces are associated with a single logical network (6).

Figure 9-16: Logical network diagram when A-Network ports are used for WAN connection



9.7.6 Enable port forwarding

This procedure assumes that the required XIO Ethernet interfaces are correctly configured and enabled on the Network tab. Port forwarding is available only when the default 4-port switch mode is disabled. See section 9.5 Enterprise and industrial (3-network) support and 9.6 Enterprise and industrial (4 Network) support for instructions to disable the XIO 4-port switch mode and configure the Ethernet interfaces.

To enable Port Forwarding:

1. Select **Communications** on the PCCU navigation tree.
2. Select the Port Forwarding tab.
3. Select the **Enable Port Forwarding** check box.
4. Click **Send**.
5. Verify that the Port Forwarding Status displays: Ready.
6. Click the **Enterprise Interface** drop-down list. Verify that the desired interface for the uplink connection displays.

IMPORTANT NOTE: Only enabled Ethernet interfaces display in the **Enterprise Interface** list. If the interface you plan to use as uplink does not display, go to the Networking tab, verify configuration, and set to enable.

Any of the XIO Ethernet interfaces, A1+A2 (if combined), A1, A2, B1 or B2, can be used as the Enterprise interface for connection to the customer network on the WAN. The selection depends on the customer configuration and field requirements.

7. Proceed to 9.7.7 Define port forwarding rules.

9.7.7 Define port forwarding rules

In the Port Forwarding tab's **Port Forwarding Rules** table, define rules for each device that the XIO will forward traffic for. There could be several rules or table entries for a single destination device. For example, if forwarding traffic to access several services on a single device, each service will need its own entry on the table. Add as many rules as needed to ensure access to those devices. Table 9-9 shows TCP ports assigned to PCCU, Device Loader and SSH/SFTP in each Totalflow device. PCCU and device loader access is normally required. SSH/SFTP access is normally reserved for advanced users and should not be enabled if not needed.

This procedure provides configuration steps for the example described in section 9.7.5 Use A-Network ports for WAN (uplink) connection. Adapt steps to your specific configuration requirements. Click **Help** on the Port Forwarding screen for additional details.

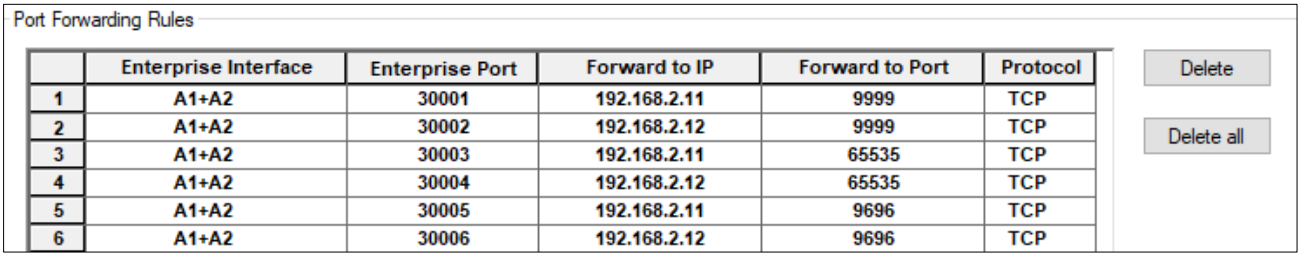
Table 9-9: Reserved TCP ports on Totalflow devices

Service	Access type	TCP port
PCCU	Ability to connect with destination device using the Totalflow user interface, PCCU, for device management or data collection	9999
Device Loader	Ability to connect with destination device using device loader (for software updates, configuration backup, etc.)	65535
SSH/SFTP service	Secure access to device using Secure Shell (SSH) or Secure File Transfer Protocol (SFTP).	9696

For each device, and for each service, under the **Add New Port Forward Rule** section in the **Port Forwarding** tab:

1. Select the **Enterprise Interface** drop-down list and choose the interface associated with the uplink port (that is, the port connecting the XIO to the corporate network). In the example in section 9.7.5, XIO ports A1 and A2 are configured in 1 Network mode (both ports are assigned a single interface: A1+A2). Port A1 is connected to the corporate network. Port A2 is left unused.
2. In the **Enterprise Port** field, type the XIO's TCP port assigned to handle traffic for the destination device or service. Be sure to use a unique port number for each entry (TCP port number range: 0-65532, except those already in use). The port should not be in use by other services or applications on the XIO.
3. In the **Forward to IP** field, type the IP address of the destination device the XIO will forward traffic to.
4. In the **Forward to Port** field, type the TCP port assigned to the service available on the destination device.
5. Click **Add**. This adds the rule values into the Port Forwarding Rules table.
6. Verify that the rule displays correctly in the table.
7. Click **Send**. The rule is permanently saved in the table.
8. Repeat steps for each rule as needed.
9. Verify that all required rules display on the table. Rules can be added as needed if additional devices are connected to the field network. Figure 9-17 shows an example of forwarding rules for several devices for access using PCCU (on port 9999), device loader (on port 65535), or SSH/SFTP (on port 9696). Note that there are several rule entries for each device to provide access to these 3 services.

Figure 9-17: Port Forwarding Rules table example

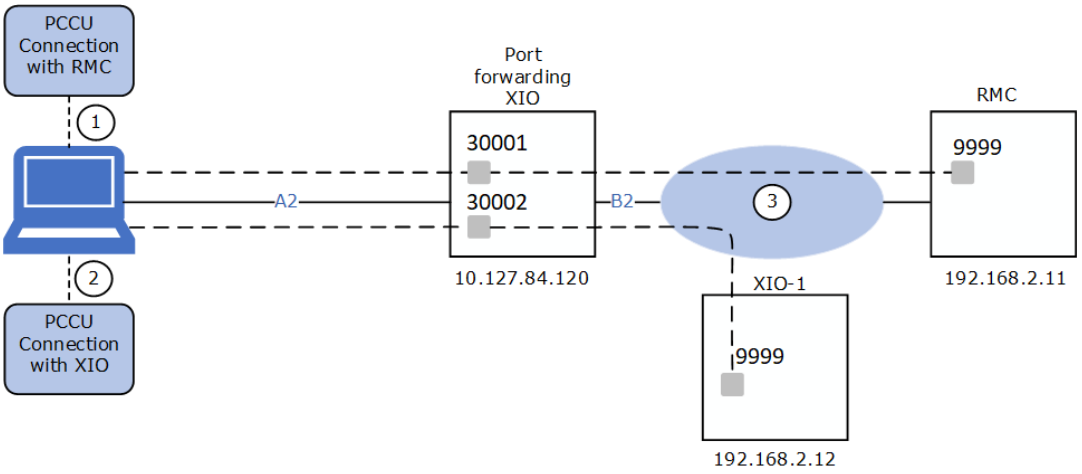


9.7.8 Verify access to field devices with PCCU

Verify access to each of the field devices that rules were defined for. This procedure uses PCCU to test access to those devices. If the forwarding rules are configured correctly, you should be able to establish PCCU connections with each of the devices attached to the port forwarding XIO. Test as follows:

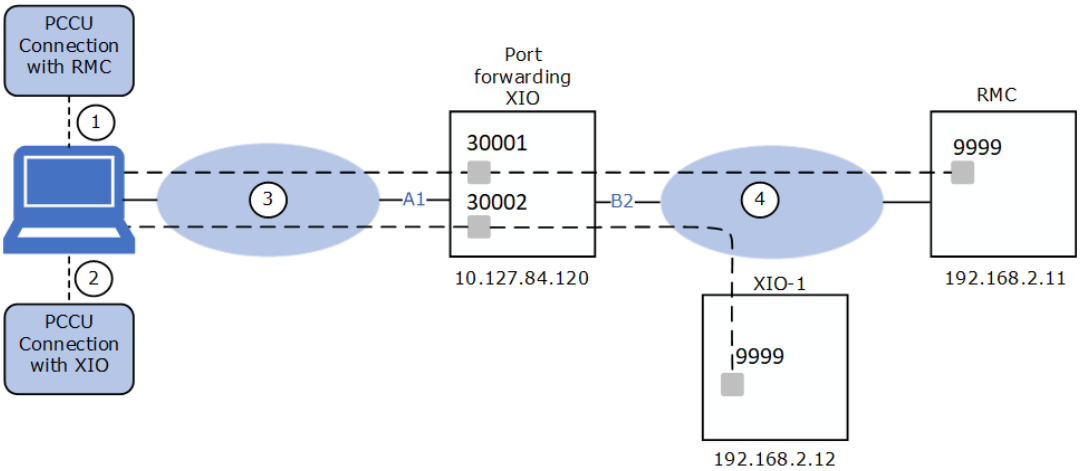
- Locally: If using A1+A2 as the uplink interface, you can connect your laptop to the available port (A1 or A2) and attempt PCCU connection to the devices from there. In the example in Figure 9-18, the laptop is directly connected to XIO port A2. (The uplink connection to port A1 is not shown). Two instances of PCCU are used to verify connections: The PCCU connection with the RMC (1) is handled at port XIO TCP port 30001. The PCCU connection with the XIO-1 (2) is handled at XIO TCP port 30002.

Figure 9-18: Verify local access



– Remotely: Verify connection from a remote host on the corporate network. In the example in Figure 9-19, the laptop with PCCU is connected to the corporate network (3) and establishes connection over that network (WAN). Two instances of PCCU are used to verify connections. The PCCU connection with the RMC (1) is handled at port XIO TCP port 30001. The PCCU connection with the XIO-1 (2) is handled at XIO TCP port 30002.

Figure 9-19: Verify remote access

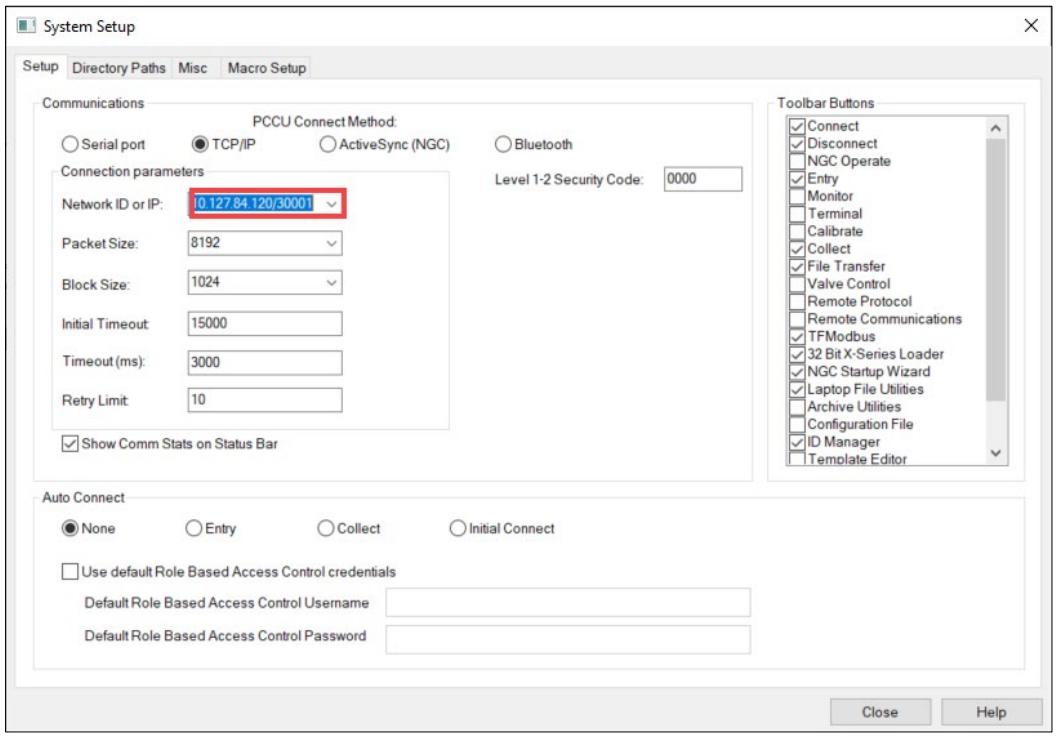


IMPORTANT NOTE: Obtain a screen capture of the forwarding rule table before testing for quick reference.

To verify access to the device using PCCU:

1. Start PCCU.
2. Click **Setup** on the top PCCU menu. The Setup tab displays.
3. Select the **TCP/IP** radio button under the Communications section (Figure 9-20).
4. In the Network ID or IP field, type the IP address of the port forwarding XIO and the XIO TCP port configured for the traffic to the destination device service. Use the following format: <XIO IP address>/<XIO TCP port number>. Refer to the forwarding rule table to configure the correct TCP port number. The image below shows an example of the PCCU connection setup when going through an XIO with IP address 10.27.84.120 and TCP port 30001. The XIO uses TCP port 30001 to handle PCCU connection traffic for the device with IP address 192.168.2.11.

Figure 9-20: Connection Setup for destination device connected to port forwarding XIO



5. Click **Close** to exit System Setup and return to the main PCCU screen.
6. Click the Entry icon on the top PCCU menu.
7. Verify that connection with the destination device is successfully established.

IMPORTANT NOTE: For details on other connection setups, see PCCU online help topics. For connection using the Device Loader, see the **Loader connection setup** topic. For connection using SSH or SFTP clients, see the **SSH and SFTP service** topic.

10 Wi-Fi® connectivity scenarios

The XIO supports Wi-Fi® wireless access by Wi-Fi clients. It can also connect to a Wi-Fi access point as a client. Wireless support depends on the Wi-Fi mode of operation configured on the XIO.

IMPORTANT NOTE: A wireless network made available by enabling Wi-Fi on Totalflow devices is for the purpose of local access by hosts only. The wireless network does not support device-to-device connections carrying critical real-time measurement data.

IMPORTANT NOTE: For additional information on Wi-Fi configuration parameters or connection procedures, refer to the Network Communication Application Guide listed in the Additional information.

IMPORTANT NOTE ON TERMINOLOGY: The term "network" in this section refers to a wireless network. In older Totalflow documentation, the term "network" has been used to describe an Ethernet network. With Wi-Fi support introduced in newer devices, the term applies to either an Ethernet or a Wi-Fi network. Either type of network will be clearly indicated in the text and diagrams.

The term "connection" in this section refers to the wireless link established between a wireless client and an advertised wireless network. The term is not used to refer to a physical connection as with Ethernet. Nodes on a wireless network can establish logical TCP connections with each other on the same wireless network. Diagrams depict wireless networks or links with dotted lines. Solid lines represent physical connections. Lines with arrows in different color represent communication or data flows.

10.1 Connections supported by Wi-Fi modes

Table 10-1 shows the XIO Wi-Fi modes and the connections they support. Preferred configuration depends on the number of XIOs, their location in the field, and the access requirements. Wi-Fi is a convenient way to access XIOs without having to be in proximity with the device. When there are several XIOs, the optimal configuration is to configure one as an access point and the rest as clients.

Table 10-1: Connections supported by Wi-Fi modes

Wi-Fi Mode	Connection	Description
Access Point (AP)	[Host Wi-Fi client]-to-XIO	Point-to-point connection from a wireless client to XIO. Wireless client joins the network advertised by the XIO. Use when there is only one XIO and there are no other Totalflow devices that can support Wi-Fi Access Point functionality.
Client	XIO-to-[XIO Wi-Fi Access Point]	XIO and other Wi-Fi clients join wireless network advertised by another XIO configured as an Access Point Wi-Fi clients can connect to the XIO over that network.
	XIO-to-[Totalflow Wi-Fi Access point]	XIO and other Wi-Fi clients join wireless network advertised by a Totalflow device configured as an Access Point. Wi-Fi clients can connect to the XIO over that network.
	XIO-to-[Third-party Wi-Fi Access Point]	XIO joins wireless network advertised by a third-party access point. Wi-Fi clients can connect to the XIO over that network.
Access Point (AP) Bridged	[Wi-Fi client]-to-XIO	Wireless client joins the network advertised by the XIO. Wi-Fi clients can connect to the XIO over that network.

10.2 IP parameter configuration

Connections over Wi-Fi networks are TCP/IP based. Each device connecting to a wireless network must have a unique and valid IP address. IP configuration depends on the Wi-Fi mode. Table 10-2 describes the IP configuration requirements.

When the XIO is configured as a Wi-Fi Access Point, it can automatically provide IP addresses for Wi-Fi clients with its DHCP server. Automatic addressing is the preferred option.

Table 10-2: IP parameter configuration

Wi-Fi Mode	Configuration	Description
Access Point (AP)	Default: 192.168.1.1	Wi-Fi clients (up to 10) can obtain their IP addresses from the XIO if DHCP server is enabled.
	DHCP Server available to clients	Wi-Fi clients can use default XIO address to connect to the XIO.

Wi-Fi Mode	Configuration	Description
Client	Default: none	XIO performs the Wi-Fi client role.
	Obtain IP address from Access Point	Manually configure Access Point SSID and passcode
		Ensure DHCP server in Access Point is supported and enabled.
Access Point (AP) Bridged	Default: 192.168.1.1	Wi-Fi clients (up to 10) can obtain their IP addresses from the XIO DHCP server.
	Default: DHCP Server always enabled	Wi-Fi Clients can use default XIO address to connect to the XIO.

10.3 Wireless network communication

The following sections depict scenarios for wireless access by hosts with Wi-Fi client support. They provide additional detail to some of the connection scenarios summarized in section 10.1 Connections supported by Wi-Fi modes.

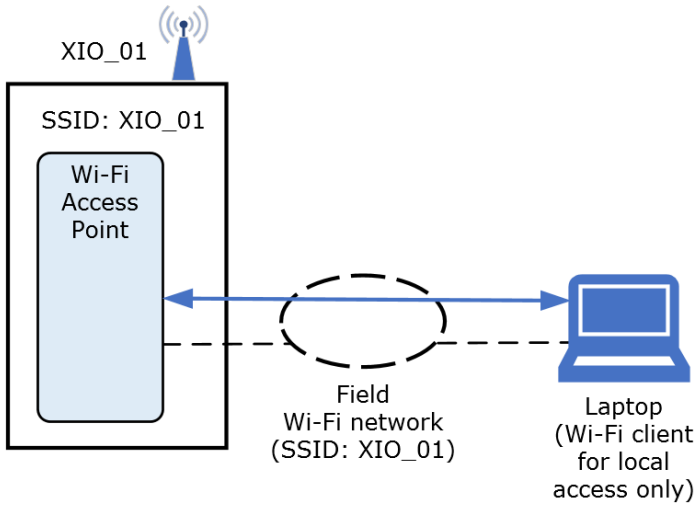
IMPORTANT NOTE: For details and configuration procedures see the Network Communication Application Guide (see link in Additional information).

10.3.1 Local point-to-point wireless access to XIO (Wi-Fi AP) by host

The XIO supports local wireless access by Wi-Fi clients. Wi-Fi clients can establish connections to the XIO in all Wi-Fi modes:

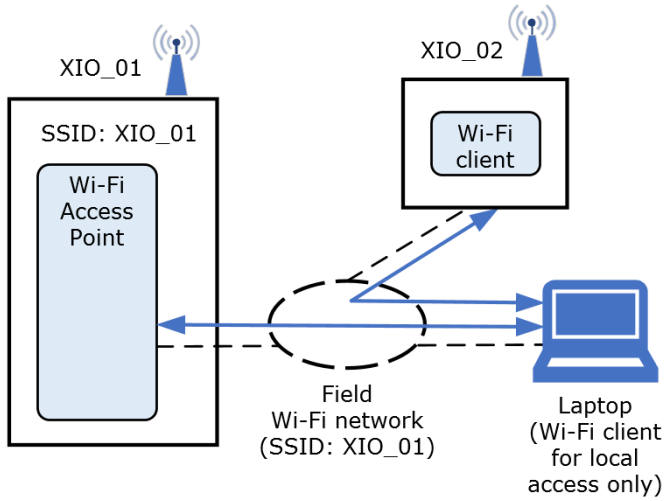
- When there is only a single XIO with no other Totalflow Wi-Fi access point available, the XIO needs to be configured as an access point for Wi-fi clients to connect. The Wi-Fi client detects and joins the network advertised by the XIO. The connection is basically a point-to-point connection since no other devices acts as clients to the XIO AP.

Figure 10-1: XIO Access Point: local access by operator



- When there are several XIOs, one may be configured as an access point and the others as clients. In this scenario, the Wi-Fi client only joins a single wireless network, but can establish connection to all XIOs on that network.

Figure 10-2: Local wireless access by operator to multiple XIOs

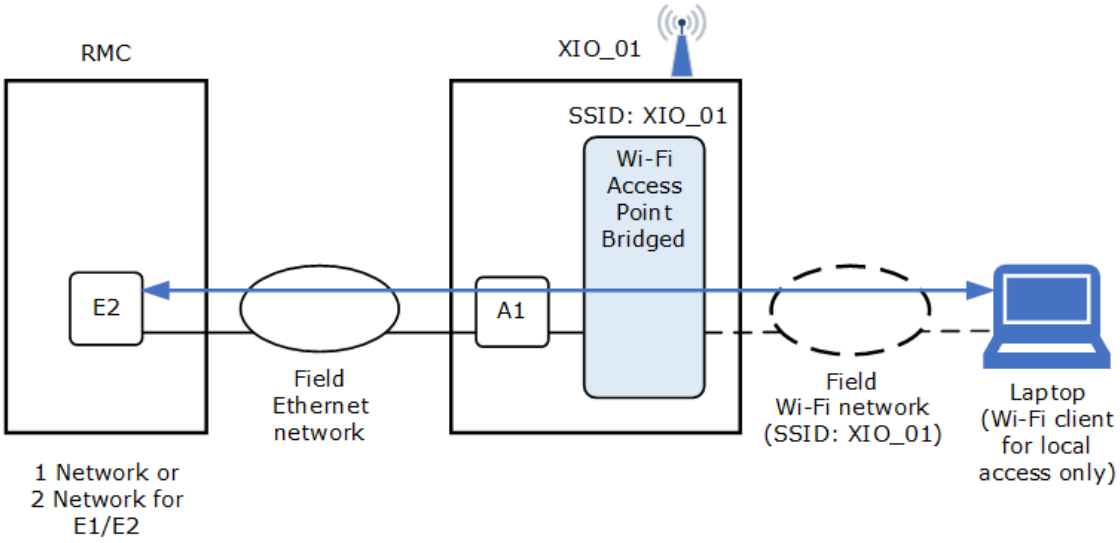


10.3.2 Local wireless access to RMC by host

The XIO AP bridge mode supports bridging of network traffic from a local wireless client to a wired device. Figure 10-3 depicts this scenario. The host with PCCU has Wi-Fi client capabilities and can establish a wireless link to the local wireless network advertised by the XIO. The XIO is configured in AP-Bridged mode. It connects to the wired network (using A1 port). When it receives traffic directed to the RMC IP address, on its wireless link, it forwards that traffic to the A1 port. The RMC receives traffic on its Ethernet port (E2). This network traffic flow is depicted by the blue line.

IMPORTANT NOTE: The XIO supports the Wi-Fi AP bridged mode only when in 4-port switch mode.

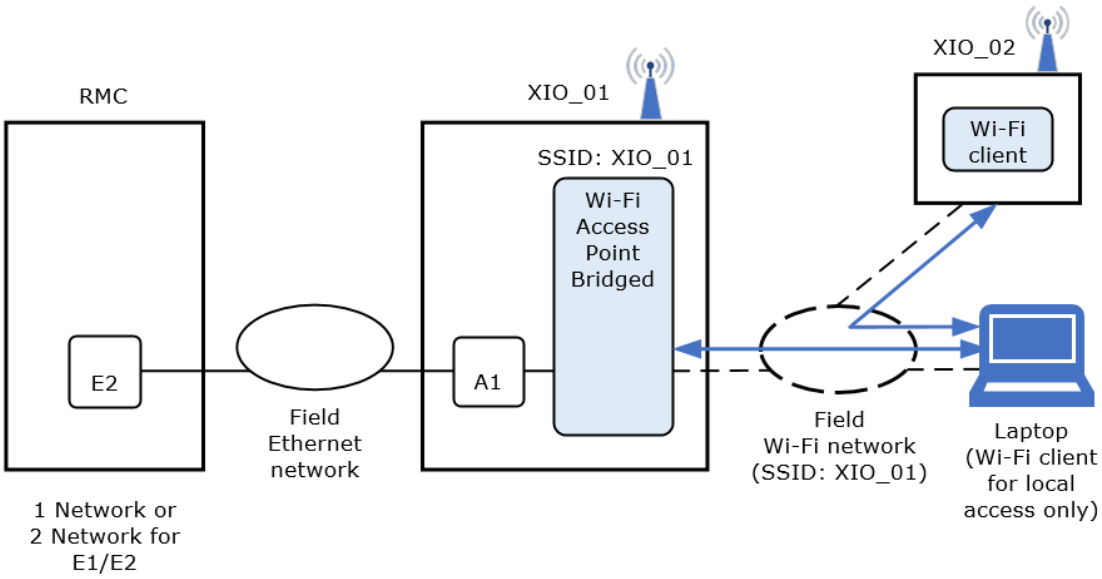
Figure 10-3: Local wireless access to an RMC (through an XIO)



10.3.3 Local wireless access to XIO (Wi-Fi client) by host

Figure 10-4 depicts local wireless access by a Wi-Fi client to an XIO in client mode (XIO_02) and to an XIO in access point bridge mode (XIO_01). See the blue flow lines from the laptop to XIO_01 and XIO_02. XIO_02 is configured as a Wi-Fi client and joins the network advertised by XIO_01. The laptop joins the same wireless network to connect to all devices.

Figure 10-4: Local wireless access to XIO (Wi-Fi client) by host



11 Product warranty

Before installation, store the equipment referred to in this manual in a clean, dry environment, per the Company's published specification. Make periodic checks on the equipment's condition. In the event of a failure under warranty, provide the following documentation to support your claim:

- A list providing evidence of process operation and alarm logs at the time of failure
- Copies of all storage, installation, operating and maintenance records relating to the alleged faulty XIO.

ABB Inc.

Measurement & Analytics

Quotes: US-IAMA.inquiry@us.abb.com

Orders: US-IAMA.order@us.abb.com

Training: US-IAMA.training@us.abb.com

Support: upstream.support@us.abb.com

+1 800 442 3097 (opt. 2)

Additional free publications are available for download at
www.abb.com/upstream

Main Office - Bartlesville
7051 Industrial Blvd
Bartlesville, OK 74006
Ph: +1 918 338 4888

Texas Office - Houston
3700 W. Sam Houston Parkway S., Suite 600
Houston, TX 77042
Ph: +1 713 587 8000

2106424MNAC