

Com'X 210 Energy Server

User manual

DOCA0036EN-15
09/2020

Legal Information

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this guide are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owners.

This guide and its content are protected under applicable copyright laws and furnished for informational use only. No part of this guide may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the guide or its content, except for a non-exclusive and personal license to consult it on an "as is" basis. Schneider Electric products and equipment should be installed, operated, serviced, and maintained only by qualified personnel.

As standards, specifications, and designs change from time to time, information contained in this guide may be subject to change without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this material or consequences arising out of or resulting from the use of the information contained herein.

Safety information

Important information

Read these instructions carefully and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this manual or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.



The addition of either symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.



This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that accompany this symbol to avoid possible injury or death.

DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in death or serious injury**.

Failure to follow these instructions will result in death or serious injury.

WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in death or serious injury**.

CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result in minor or moderate injury**.

NOTICE

NOTICE is used to address practices not related to physical injury.

Please note

Electrical equipment should be installed, operated, serviced and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material. A qualified person is one who has skills and knowledge related to the construction, installation, and operation of electrical equipment and has received safety training to recognize and avoid the hazards involved.

Notice

FCC

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that the interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The user is cautioned that any changes or modifications not expressly approved by Schneider Electric could void the user's authority to operate the equipment.

This digital apparatus complies with CAN ICES-3 (B) /NMB-3(B).

Table of Contents

Safety precautions	9
Com'X 210 Introduction	11
Product Overview	11
Architecture	11
Main Features	11
Com'X 210 Quickstart	14
Quickstart Overview.....	14
Quickstart: Setting up and Starting Data Logging	14
Quickstart: Viewing On-board Data	14
Quickstart: Setting Up Publication	14
Com'X 210 Access the User Interface	16
Supported Web Browsers.....	16
Start Up Your Com'X.....	16
Accessing Through the Ethernet Port With Windows	16
Accessing Through the Ethernet Port With Other Operating Systems	17
Accessing Through Wi-Fi Access Point Mode With Windows	18
Accessing Through Wi-Fi Access Point Mode	19
Logging In.....	20
Logging In for the First Time	20
Changing the Password	21
User Interface Overview.....	21
User Interface Features	22
Com'X 210 Security	24
Security overview	24
Security features on your device	24
Password Requirements	24
Security Configuration Recommendations	27
Com'X 210 Settings	29
Settings Overview.....	29
Date and Time Settings.....	29
Configuring Date and Time	29
Network Settings	29
Network Configuration Options	30
Selecting a Network Configuration	30
Ethernet Port Settings	31
GPRS/3G Settings	33
Wi-Fi Settings	37
Proxy Settings	39
Contact Management.....	40
Email Settings	41
Publication	43
Publication Identification Settings	46
File Format of CSV Export	46
Digital Service Platform Connection	47
Enabling Schneider Electric Services	47
Disabling Schneider Electric Services.....	48

Wi-Fi Access Point Settings.....	48
Activating the Wi-Fi Access Point.....	48
Deactivating the Wi-Fi.....	48
Site Information.....	49
Configuring Site Information.....	49
Data Logging.....	49
Defining the Logging Intervals.....	49
Security.....	49
Firewall Management.....	49
Port Settings.....	50
Upstream Network Access.....	50
Configuring Firewall Settings.....	50
Disabling DPWS and SSH services.....	51
Disabling the Password Reset Button.....	51
Account Lockout Policy.....	51
Configuring Account Lockout Policy.....	52
Disabling Account Lockout Policy.....	52
Warning Banner Overview.....	52
Certificates.....	53
Uploading a New Certificate.....	53
HTTPS Redirection.....	53
Event Settings.....	53
Predefined Events.....	54
Custom Events.....	54
Creating a Custom Event.....	54
Editing or Deleting a Custom Event.....	56
Copying an Event.....	56
Com'X 210 Communications.....	57
IPv4 Address Settings.....	57
Modbus TCP Access.....	59
Configuring Modbus TCP/IP Filtering.....	61
Modbus Serial Port.....	62
Modbus Serial Port Settings.....	62
Advanced Ethernet Settings.....	63
ZigBee Network Settings.....	64
Com'X 210 Device Settings.....	67
Device Settings Overview.....	67
Common Properties.....	68
Adding a Downstream Device.....	70
Modifying a Device.....	71
Disconnecting a Device.....	71
Reconnecting a Device.....	71
Replacing a Device.....	72
Deleting a Device.....	72
Measurement and Metadata Exported Per Hosted Platform.....	73
Selecting Measurements to Log or Publish.....	73
Factory Settings of the Device Measurement Table.....	73
Measurement Table Notification Icons.....	74
Built-In Pulse Meters.....	74
Custom Pulse Meter.....	75
Resistance Temperature Detectors.....	75

Custom Analog Devices	75
Discovering Connected Devices	75
Discovered Modbus Device Status	76
Adding a Modbus Device Manually	76
Modbus Meter Measurements	77
Connecting Devices to WT4200 Modbus Receiver	77
Connecting Devices to Smartlink	78
Built-in Ethernet Devices	79
Ethernet Device Configuration Parameters	79
Custom Ethernet Devices	79
Discovering Zigbee Devices	79
Com'X 210 Measurements	81
Viewing the Measurements Table	81
Com'X 210 Commissioning	82
Commissioning Overview	82
Starting the Data Logging	82
Starting the Publication	83
Com'X 210 Custom Library	84
Custom Models	84
Custom Modbus Devices	86
Custom Pulse Meter Model	90
Custom KYZ Pulse Meter Model	91
Custom Main Meter Model	92
Custom Contactor or Impulse Relay	94
Status Custom Model	95
Creating a Status Custom Model	95
Custom Analog Sensor Model	96
Com'X 210 Diagnostics	98
Diagnostics Overview	98
Statistics	98
Viewing Statistics	98
Resetting Statistics	98
Read Device Registers	100
Communications Check	101
Com'X 210 Maintenance	102
Logs	102
System Settings	102
Configuration Management	103
Save the Configuration	103
Restore a configuration	104
Upgrade Firmware	106
Enabling Remote Access	107
Disabling Remote Access from Cloud Services	108
Restarting the Com'X from the Web Interface	108
Product Replacement	108
Resetting the Password Locally	108
Resetting to Factory Settings	109
Checklist Before Leaving Customer Site	111
Com'X 210 Troubleshooting	112
Metering Device Troubleshooting	112

Modbus Device Troubleshooting.....	113
Network Troubleshooting	113
Com'X Troubleshooting.....	114
Certificate Authorities	117
Modbus Register Mapping.....	120

Safety precautions

Installation, wiring, testing and service must be performed in accordance with all local and national electrical codes.

⚠️⚠️ DANGER
<p>HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH</p> <ul style="list-style-type: none"> • Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices. See NFPA 70E in the USA, CSA Z462 or applicable local standards. • Turn off all power supplying this device and the equipment in which it is installed before working on the device or equipment. • Always use a properly rated voltage sensing device to confirm that all power is off. • Treat communications and I/O wiring connected to multiple devices as hazardous live until determined otherwise. • Do not exceed the device's ratings for maximum limits. • Replace all devices, doors and covers before turning on power to this equipment. <p>Failure to follow these instructions will result in death or serious injury.</p>

⚠️ WARNING
<p>UNINTENDED OPERATION</p> <ul style="list-style-type: none"> • Do not use the software for critical control or protection applications where human or equipment safety relies on the operation of the control action. • Do not use the software to control time-critical functions because communication delays can occur between the time a control is initiated and when that action is applied. • Do not use the software to control remote equipment without securing it with an authorized access level, and without including a status object to provide feedback about the status of the control operation. <p>Failure to follow these instructions can result in death, serious injury, or equipment damage.</p>

⚠️ WARNING
<p>INACCURATE DATA RESULTS</p> <ul style="list-style-type: none"> • Do not incorrectly configure the software, as this can lead to inaccurate reports and/or data results. • Do not base your maintenance or service actions solely on messages and information displayed by the software. • Do not rely solely on data displayed in the software reports to determine if the system is functioning correctly or meeting all applicable standards and requirements. • Do not use data displayed in the software as a substitute for proper workplace practices or equipment maintenance. <p>Failure to follow these instructions can result in death, serious injury, equipment damage, or permanent loss of data.</p>

⚠ WARNING**POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY**

- Change default passwords to help prevent unauthorized access to device settings and information.
- Disable unused ports/services and default accounts, where possible, to minimize pathways for malicious attacks.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Use cybersecurity best practices (for example: least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, interruption of services, or unintended operation.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Com'X 210 Introduction

Product Overview

The Com'X 210 energy server is a compact plug and play data logger.

The Com'X 210 collects and stores consumption of WAGES (Water, Air, Gas, Electricity, and Steam) and environmental parameters such as temperature, humidity, and CO² levels in a building. Data can be securely transmitted as a report to an Internet database server.

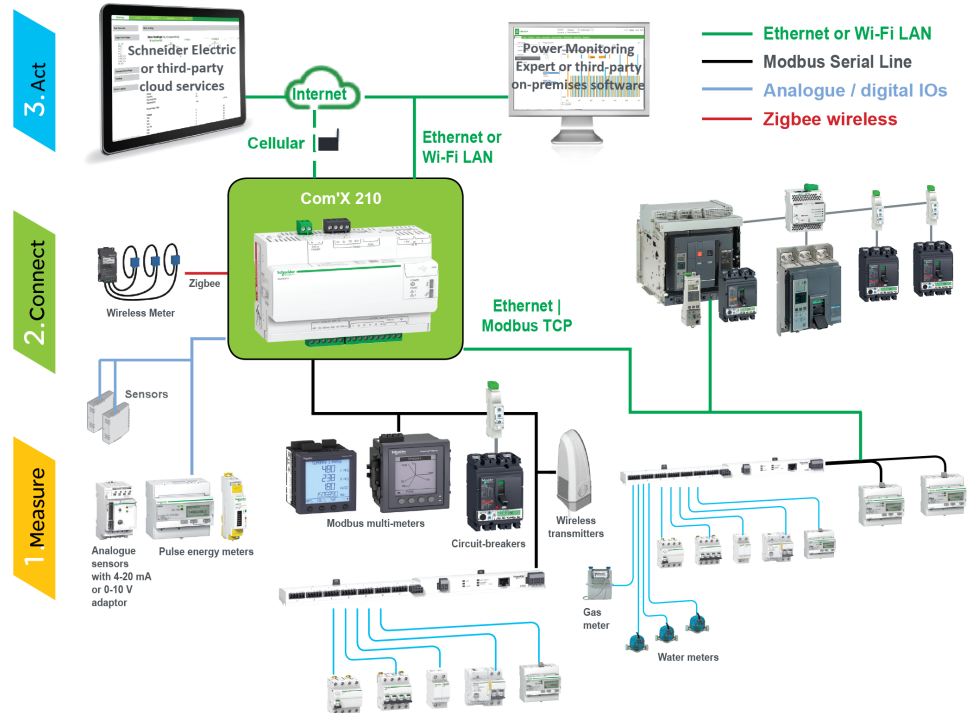
Data is ready to be processed once received by the server. Data is displayed as web pages through energy management services provided by Schneider Electric, such as EcoStruxure™ Energy Operation and EcoStruxure™ Facility Expert, to support optimization of energy performance and cost management.

The Com'X 210 also provides a transparent interface between Ethernet-based networks and field devices. This gateway function supports the use of monitoring software to access information from devices for data collection, trending, event management, analysis, and other functions.

Architecture

From a simple metering installation with one device to large metering systems, the Com'X 210 collects data from any Modbus TCP/Modbus serial line gateway, pulse meter, actuator, and analog sensor.

This graphic shows possible architectures of the Com'X 210:



Main Features

The Com'X 210 has several main features.

- Automatic discovery of connected Modbus devices
- Connectivity to the cloud through three media: Cellular, wired Ethernet, or Wi-Fi Ethernet

- Two Ethernet ports to separate upstream cloud connection from field device network
- Four supported transfer protocols: HTTP, HTTPS, FTP, and SMTP with proxy management
- Data storage in case of upstream communication interruption
- Data export with native connection to Schneider Electric service platforms (such as Energy Operation) and with .csv file for other database servers
- Gateway functionality Modbus TCP to Modbus RTU
- Setup through on-board web pages
- Compliant with electrical switchboard environment (temperature, electromagnetic compatibility)
- Local backup of configuration parameters
- ZigBee Pro with EM4300 sensors

Schneider Electric Digital Service Platform

The energy server can be associated with Schneider Electric Digital Service Platform.

This platform allows you to:

- Remotely manage firmware upgrade, troubleshooting, and parameter settings.
- Provide a SIM card with worldwide coverage, by using the EBXA-GPRS-SIM option.
- Publish collected data to Schneider Electric energy management services.

NOTE: It is recommended to use external cellular router instead of EBXA-GPRS-SIM option.

EcoStruxure™ Facility Expert

EcoStruxure™ Facility Expert allows you to outsource energy management and maintenance, reducing your energy costs and increasing operating efficiency in buildings.

EcoStruxure™ Facility Expert is a cloud-based software application from Schneider Electric to improve energy efficiency, and manage assets and maintenance. EcoStruxure™ Facility Expert is used for small and medium buildings in industry, retail, public, and healthcare markets.

EcoStruxure™ Facility Expert provides the following features:

- Support for data acquisition hardware: meters, gateways, and sensors.
- Cloud platform for data displays.
- Consulting service from Schneider Electric expert teams.
- A network of local partners to implement solutions.

Power Monitoring Expert

The Com'X can send data in comma-separated value (CSV) files to supervision software such as Power Monitoring Expert (PME) or third-party supervision software.

PME is a complete, interoperable, and scalable software package for power management applications. The software collects and organizes data gathered from the electrical network and presents it as meaningful, actionable information through an intuitive Web interface. Share information with key stakeholders or

across your entire operation to influence behavioral changes that can save you money.

Additional Resources

To find these and other resources, go to www.se.com and search for "Com'X."

Document	Reference Number(s)
Com'X Instruction Sheet	5406AD002 5406AD005 5406AD006
EBXA-GPRS/EBXA-GPRS-SIM Instruction Sheet	253537613
EBXA-WIFI Instruction Sheet	253537634
Zigbee Instruction Sheet	NHA2243500

Com'X 210 Quickstart

Quickstart Overview

This chapter describes how to perform common tasks with the Com'X 210. See the referenced chapters for a further details.

NOTE: Ensure your Com'X is running the latest firmware. Go to www.schneider-electric.com/en/download/ to download the latest version of the firmware.

Quickstart: Setting up and Starting Data Logging

Below are the general tasks related to starting data logging. There may be additional steps for publishing to a specific platform.

1. Add the downstream devices as in [Adding a Downstream Device](#), page 70. There are additional configuration tasks for each type of device:
 - Devices that can connect to digital inputs
 - Devices that can connect to analog inputs
 - Modbus devices
 - [Ethernet Device Configuration Parameters](#), page 79
2. Select the measurements to log as in [Selecting Measurements to Log or Publish](#), page 73
3. Define the logging interval as in [Defining the Logging Intervals](#), page 49
4. Start the data logging as in [Starting the Data Logging](#), page 82

Quickstart: Viewing On-board Data

You can view real time and logged data on the Com'X 210 without having to connect to a hosted platform. Below are the steps for viewing on-board data.

1. Add the downstream devices as in [Adding a Downstream Device](#), page 70. There are additional configuration tasks for each type of device:
 - Modbus Devices
 - [Ethernet Device Configuration Parameters](#), page 79
2. Complete the following steps to view an Energy dashboard. Skip to step 3 to view real time data.
 - [Selecting the Measurements to Log or Publish](#), page 73
 - [Defining the Logging Intervals](#), page 49
 - [Starting the Data Logging](#), page 82
3. View real time data that has been selected for logging: [Viewing the Measurements Table](#), page 81

Quickstart: Setting Up Publication

The steps below are a summary of publishing options. Refer to the appropriate sections for a full description of publishing per platform.

1. Choose the platform and publication frequency as in [Selecting Platform and Publication Frequency](#), page 43. For each platform, see these related tasks:
 - For a connection to a Schneider Electric subscribed service via Digital Service Platform (for example, EcoStruxure Facility Expert), see [Connection](#), page 47.
 - For .csv export options, you may want to refer to [File Format of CSV Export](#), page 46.
2. Define the transfer protocol as in [Define the Transfer Protocol](#), page 43.
3. Start the publication as in [Starting the Publication](#), page 83.

Com'X 210 Access the User Interface

Supported Web Browsers

You can access the energy server using a variety of web browsers.

Browser	Browser Version
Microsoft Edge	42.0 and above
Internet Explorer	IE9 and above
Firefox	20.0 and above
Chrome	24.0 and above

Recommended Web Browsers

It is recommended to use Chrome for PC.

The following browsers are recommended for tablets:

Operating System	Browser
Windows 10	<ul style="list-style-type: none"> Microsoft Edge
Windows 8	<ul style="list-style-type: none"> Internet Explorer Firefox
iOS	<ul style="list-style-type: none"> Chrome Safari
Android	<ul style="list-style-type: none"> Chrome Android browser

Start Up Your Com'X

The Com'X takes time to start up. Wait for the power LED to turn green before performing any actions.

Once the Com'X is started, most configuration modifications are taken in account without a reboot.

Reboot Cases

The Com'X requires a reboot in the following cases:

- Upgrading the firmware.
- Restoring a configuration.
- Changing the Ethernet network settings between 2 switched ports and 2 separate ports.
- Inserting a GPRS or 3G modem.
- Installing a Zigbee key.

Accessing Through the Ethernet Port With Windows

Access the Com'X user interface for initial setup using Windows 10.

The default configuration for Com'X Ethernet port 2 is DHCP server.

⚠ DANGER**HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH**

- This equipment must only be installed and serviced by qualified personnel.
- Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices. See NFPA 70E in the USA, CSA Z462 or applicable local standards.

Failure to follow these instructions will result in death or serious injury.

NOTICE**IP ADDRESS CONFLICT**

Do not connect a Com'X Ethernet port to a local area network if it is configured to DHCP server.

Failure to follow these instructions can result in impaired communications.

1. Disconnect your local computer from all networks.
2. Connect an Ethernet cable from your local computer to the Ethernet port 2 of the Com'X.
3. Open Windows Explorer on your local computer and click **Network**.
The Com'X appears in the list of devices.
4. Double-click the Com'X. The login page is opened automatically on your default web browser.

NOTE: HTTPS is enabled by default on the Com'X configuration. The Com'X has an autosigned security certificate. Therefore, connecting to the energy server interface displays a security message. Before accepting, confirm that communication with the energy server has been established.

5. Type the username (default: **admin**) and the password (default: **admin**).

NOTE: The username and password are case-sensitive.

6. Click **OK**.

Related Topics

- Com'X 210 Troubleshooting
- Uploading a New Certificate

Accessing Through the Ethernet Port With Other Operating Systems

Access the Com'X user interface for initial setup using an operating system other than Windows.

The default configuration for Com'X Ethernet port 2 is DHCP server.

⚠ DANGER**HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH**

- This equipment must only be installed and serviced by qualified personnel.
- Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices. See NFPA 70E in the USA, CSA Z462 or applicable local standards.

Failure to follow these instructions will result in death or serious injury.

NOTICE

IP ADDRESS CONFLICT

Do not connect a Com'X Ethernet port to a local area network if it is configured to DHCP server.

Failure to follow these instructions can result in impaired communications.

1. Disconnect your local computer from all networks.
2. Connect an Ethernet cable from your local computer to the Ethernet port 2 of the Com'X.
3. Open your web browser.
4. Type **[10.25.1.1]** in the address field and press **Enter**.

NOTE: HTTPS is enabled by default on the Com'X configuration. The Com'X has an autosigned security certificate. Therefore, connecting to the Com'X interface displays a security message. Before accepting, confirm that communication with the Com'X has been established.

5. Type the username (default: **admin**) and the password (default: **admin**).

NOTE: The username and password are case-sensitive.

6. Click **OK**.

Related Topics

- [Uploading a New Certificate](#)

Accessing Through Wi-Fi Access Point Mode With Windows

You can access the energy server user interface through Wi-Fi Access Point Mode using Windows.

⚠ DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- This equipment must only be installed and serviced by qualified personnel.
- Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices. See NFPA 70E in the USA, CSA Z462 or applicable local standards.

Failure to follow these instructions will result in death or serious injury.

NOTICE

UNINTENDED EQUIPMENT OPERATION

Do not close the door of a metallic enclosure while using the Wi-Fi USB key.

Failure to follow these instructions can result in equipment damage.

1. Connect the Wi-Fi USB key to a USB port on the energy server.
2. Press the **Wi-Fi** button on the energy server.
The Wi-Fi button LED flashes green.
3. On your local computer, connect to the energy server wireless network using the **Windows Wireless Network configuration** window.
4. Open Windows Explorer on your local computer and click **Network**. The energy server appears in the list of devices.

- Double-click the energy server and the login page opens automatically in your default browser.

HTTPS is enabled by default on the energy server configuration. The energy server has an autosigned security certificate. Therefore, connecting to the energy server interface displays a security message. Before accepting, confirm that communication with the energy server has been established.

- Type the username (default: **admin**) and the password (default: **admin**).
The username and password are case-sensitive.
- Click **Ok**.

Related Topics

- Com'X 210 Troubleshooting
- Uploading a New Certificate

Accessing Through Wi-Fi Access Point Mode

You can access the energy server user interface using Wi-Fi Access Point Mode on operating systems other than Windows 7/Vista.

⚠ DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- This equipment must only be installed and serviced by qualified personnel.
- Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices. See NFPA 70E in the USA, CSA Z462 or applicable local standards.

Failure to follow these instructions will result in death or serious injury.

NOTICE

UNINTENDED EQUIPMENT OPERATION

Do not close the door of a metallic enclosure while using the Wi-Fi USB key.

Failure to follow these instructions can result in equipment damage.

- Connect the Wi-Fi USB key to a USB port on the energy server.
- Press the Wi-Fi button on the energy server.
The Wi-Fi button LED flashes green.
- On your local computer, connect to the energy server wireless network using the **Windows Wireless Network configuration** window.
- Open your browser.
- Type **[10.25.2.1]** in the address field and press **Enter**.
HTTPS is enabled by default on the energy server configuration. The energy server has an autosigned security certificate. Therefore, connecting to the energy server interface displays a security message. Before accepting, confirm that communication with the energy server has been established.
- Type the username (default: **admin**) and the password (default: **admin**).
The username and password are case-sensitive.

7. Click **Ok**.

Related Topics

- Uploading a New Certificate

Logging In

You need to log in to access the energy server's user interface.

If multiple sessions are opened, only the first session can be used to edit parameters. Sessions opened after the first session are read-only.

1. Select your language.
2. Type the username and the password.

NOTE: The username and password are case-sensitive.

3. Click **Connect** to be logged in to the configuration web page.

NOTE: HTTPS is enabled by default on the Com'X configuration. The Com'X has an autosigned security certificate. Therefore, connecting to the Com'X interface displays a security message. Before accepting, confirm that communication with the Com'X has been established.

Related Topics

- Uploading a New Certificate

Logging In for the First Time

There are special instructions when you log in to the user interface for the first time.

The web server is a tool for reading and writing data. It controls the state of the system, with full access to all data in your application. You will be prompted to change your password the first time you log in to prevent unauthorized access to the application.

NOTICE

UNAUTHORIZED DATA ACCESS

- Immediately change the default password to a new, secure password.
- Do not distribute the password to unauthorized or otherwise unqualified personnel.

Failure to follow these instructions can result in equipment damage.

A secure password should not be shared or distributed to unauthorized personnel. The password should not contain any personal or obvious information.

1. Log in as the default administrator.
Username and password: **admin**
2. Read the License Agreement completely.


NOTE: The **Accept** button will remain grayed until you scroll to the bottom of the User License Agreement.

3. Accept the License Agreement.

4. Enter a new password.
It must contain:
 - 8 characters
 - 1 uppercase letter
 - 1 numeric digit
 - 1 special character

Changing the Password

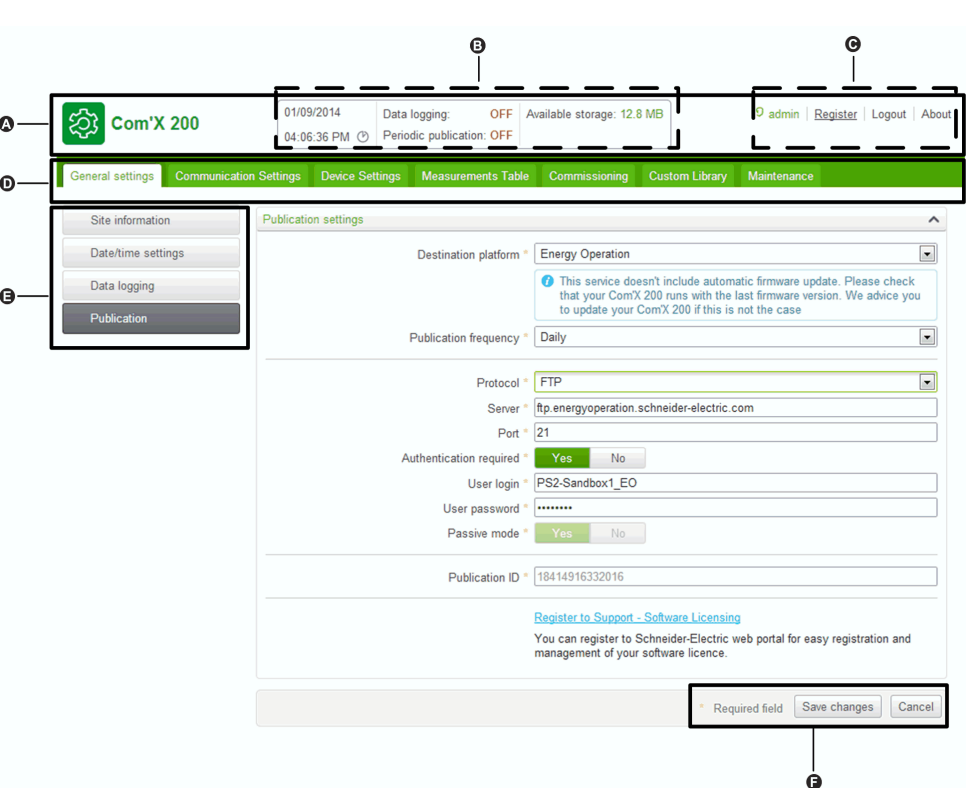
You will need to change the password after the first login and will be directed automatically to the username/password page.

1. Click the username/admin link  in the banner.
2. Enter the current password.
3. Enter a new password.
4. Confirm the new password.
5. Click **OK**.

User Interface Overview

The web user interface allows you to commission your Com'X 210.

This graphic shows the interface layout:



A. Banner

B. Gateway status

C. Generic information

D. Main tabs

E. Subtabs

F. Action buttons

Banner

The banner displays the following information at the top of all pages:

Status	Data Logging: Displays status of data logging, which can be activated in the Commissioning tab.
--------	---

	Periodic Publication: Displays publication status, which can be activated in the Commissioning tab.
	Available Storage: Shows available storage for data logging.
Generic Information	Username/admin link: Displays the connected user.
	About: Click to access information on your Com'X 210 and GPRS or 3G modem (serial number and MAC address), IPv4 Ethernet ports, IPv6 address, and software versions.
	Logout: To log out of the session, click Logout or close your browser. It is recommended to log out of the Com'X 210 when not in use.
	Time: Displays the time as set in the Date/Time Settings .

Main Tabs and Subtabs

Subtabs display the submenus under the selected main tab. You can use your web browser to bookmark each subtab of the Com'X 210 web interface.





The main tabs and subtabs are detailed in the section on device features.

Action Buttons

The action buttons correspond to the selected tab and vary. This table describes the interface buttons:

Button	Action
Save changes	Validates the modifications. Disabled when: <ul style="list-style-type: none"> there is no change in the web page. a mandatory field is left blank. The field is highlighted in red. inappropriate characters are entered in a field. The field is highlighted in red.
Cancel	Cancels the modifications to return to the last saved settings.

Icons

Icon	Description
	Indicates that the information necessary to complete the energy server configuration and activation of data logging and publication is unavailable for the tab.
	Fields marked with a red star are required fields.
	Indicates the user that is logged in for the current session.
	Contains information about configuration in the open menu.

Related Topics

- Configuring Date and Time

User Interface Features

The user interface organizes the features in main tabs and subtabs.

Main Tab	Subtab	Description
Settings	General Settings	Configures the date and time, network settings, proxy settings, publication parameters, and Wi-Fi access point settings.
	Site Settings	<ul style="list-style-type: none"> Contains the name of the site. This field is used by Energy Operation. Configures the logging interval for each commodity and for environmental parameters.
	Communication	Configures the Modbus serial port, Modbus gateway, TCP/IP filtering, and advanced Ethernet settings. Setup and create a ZigBee network.
	Security	Update SSL certificate and firewall settings.
Device Settings	–	Configures the metering architecture and the data to log and publish.
Measurements Table	–	Displays meters with metadata and data to be logged.
Commissioning	–	<ul style="list-style-type: none"> Checks the system configuration. Starts or stops data logging. Starts, stops, or tests data publication.
Diagnostics	Network	Displays diagnostic data used to troubleshoot network problems.
	Modbus	Allows users to read register data from local and remote Modbus devices connected to the Com'X 210.
	Read Device Registers	Allows users to read register data from local and remote Modbus devices connected to the Com'X.
	Communications Check	Tests the communications health of Modbus devices configured on the Com'X.
Custom Library	–	<ul style="list-style-type: none"> Create a custom device model, new device model or based on an existing custom device model in the library. Modify and delete custom models Import and export custom models.
Maintenance	Logs	Shows the date, time, and description of: <ul style="list-style-type: none"> changes in the configuration errors detected during logging publication steps and status communication interruption with metering devices unsuccessful login attempts
	System Settings	<ul style="list-style-type: none"> Allows you to back up and restore a Com'X 210 configuration. Activates the remote access for Schneider Electric technical support. Upgrades the Com'X 210 firmware. Allows you to manually restart the Com'X 210.
	Events	<ul style="list-style-type: none"> Provides log of all generated pre-defined events. Provides log of all pre-defined events to be published.

Related Topics

- Com'X 210 Settings
- Com'X 210 Communications
- Com'X 210 Device Settings
- Com'X 210 Commissioning
- Com'X 210 Custom Library
- Com'X 210 Diagnostics
- Com'X 210 Maintenance

Com'X 210 Security

Security overview

Your Schneider Electric product is equipped with security-enabling features.

These features arrive in a default state and can be configured for your installation needs. Please note that disabling or modifying settings within the scope of these individual features can impact the overall security robustness of the device and ultimately the security posture of your network in either positive or negative ways. Review the security intent and recommendations for the optimal use of your device's security features.

Products are hardened to increase security robustness. This is an ongoing process consisting of secure development practices, inclusion of security features and testing at our security test facilities. Following system hardening best practices is also necessary to help ensure your overall system security.

See the [Cybersecurity Hardening Best Practices](#) white paper for suggested best practices.

Security features on your device

Your device comes with security features that you can configure to help protect against unauthorized configuration and access to your device's data through its user interfaces or communications.

Password Requirements

The Com'X incorporates complex password requirements.

Each user is prompted to change their password the first time they log in to prevent unauthorized access to the application. It is recommended to schedule regular changes to your password.

Related Topics

- [Logging In for the First Time](#)

HTTPS Connection

Your connection to the Com'X web server is HTTPS by default.

The Com'X has a self-signed security certificate. Therefore, connecting to the Com'X interface displays a security message. Before accepting, confirm that communication with the Com'X has been established.

HTTPS Redirection is enabled by default. It is recommended to leave this setting enabled to secure communications between PC and the Com'X.

HTTPS Proxy is supported in **Settings > General Settings**. The proxy address and port number are provided by your network administrator, or you can retrieve these values in the Internet Options of a PC connected to the LAN.

Related Topics

- Proxy Settings
- Uploading a New Certificate

Secure Data Export

Using a secure protocol when publishing data logs can help prevent interception and corruption of data logs.

Secure publication options include:

- HTTPS when publishing data as a .csv file or publishing to Energy Operation.
- SMTP with connection security mode to TLS/SSL or STARTTLS when publishing a .csv file over SMTP. The default mode is None.
- DSP (a Schneider Electric hosted platform)

Destination platform is not configured by default. If you are publishing to a location other than DSP, you must configure the protocol in **Settings > General Settings > Publication**, then **Email Settings** if using SMTP.

Related Topics

- Define the Transfer Protocol
- Configuring the SMTP Server

Firewall Management

Firewall management allows you to configure network access.

You can configure items such as:

- Enable or disable ports.
- Configure port numbers per interface (Eth1, Eth2, WiFi, GPRS/3G), except where noted in *Port Settings*.
- Enable upstream network access.
- Enable Account Lockout policy.

Disabling unused ports (determined by your network selection in **Settings > General Settings > Network Settings**) can help prevent unauthorized access.

Upstream Network Access

This feature allows downstream devices to access servers (such as DNS, SNTP, and SMTP) on the upstream network.

Upstream Network Access is disabled by default. It is recommended to leave this setting disabled unless it is required to publish data or send event messages from downstream clients.

Account Lockout Policy

Account lockout feature disables a user account when the number of failed login attempts exceeds the set limit within a predetermined time interval. You can configure the following:

- Enable account lockout Account lockout policy is enabled by default. Select **No** to disable this feature. It is recommended to keep the Account Lockout feature enabled to secure the device from unauthorized access.
- Reset account lockout counter (number of attempts) determines the number of invalid login attempts allowed before user account gets disabled. The default is set to 10 attempts.
- Account lockout duration (minutes) determines amount of time user account remains disabled. The default is set to 15 minutes.

Disabling Account Lockout Policy

NOTE: It is recommended to keep the Account Lockout enabled to better secure the device from unauthorized access.

Related Topics

- Port Settings

Communications

Ethernet Security

The Com'X supports two separate Ethernet networks for isolated device network, for two separate infrastructure backbones, or for a switched network.

Wireless Security

Your Com'X wireless network can be secured with WPA2 (recommended), WPA, or WEP.

Modbus TCP/IP Filtering

The Modbus TCP/IP filtering feature controls which IP addresses are allowed to communicate with the Com'X and its downstream devices using Modbus TCP/IP.

Minimizing the number of IP address that can access the device reduces the likelihood of unauthorized intrusions.

This feature is disabled by default. When enabled, the default access level is **Read** for any Modbus TCP/IP client not in the filtered list. Setting the **Default Access field** to **None** blocks all Modbus TCP/IP clients not in the filtered list.

It is recommended that you enable this feature, if your system architecture permits.

Related Topics

- Configuring Modbus TCP/IP Filtering

Maintenance

Real-time access to maintenance logs allow you to check for excessive denied accesses, unexpected firmware upgrades or unplanned backup restoration.

Configuration Backup

Configuration backup allows recovery of Com'X and device settings.

Firmware

Users can only install firmware signed by Schneider Electric.

Remote Access from Cloud Services

By default, a Com'X device connected to DSP can be accessed through remote assistance. The **Enable remote access from cloud** option is enabled (ON) by default. For security reasons it is recommended to disable this feature and enable it only when remote access is required for technical support from Schneider Electric.

Refer to [Disabling Remote Access from Cloud Services](#), page 108 for additional information.

Related Topics

- Logs
- Save the Configuration
- Restore a configuration
- Upgrade Firmware

Security Configuration Recommendations

There are some general security configuration recommendations for your device.

- Do not add more users than those who need access, and evaluate your system needs before granting users access to critical pages, for example, **Firewall Management** or **Device Settings**.
- Limit the number of IP addresses that have access to the Com'X.
- Do not use SHA1 certificates.

Recommended best practices for unsecure protocols

⚠ WARNING
<p>POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY</p> <ul style="list-style-type: none"> • Change default passwords to help prevent unauthorized access to device settings and information. • Disable unused ports/services and default accounts, where possible, to minimize pathways for malicious attacks. • Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection). • Use cybersecurity best practices (for example: least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, interruption of services, or unintended operation. <p>Failure to follow these instructions can result in death, serious injury, or equipment damage.</p>

NOTE: Table below lists risks and best practices associated with unsecure protocols. It is highly recommended to follow these best practices.

Unsecure protocols	Risks	Best Practices
SMTP	<ul style="list-style-type: none"> • Threat of malware. • Unauthorized access to data. • Threat of data leakage. • Email contents transferred in plain-text. 	For publication: <ul style="list-style-type: none"> • Select SMTP with either SSL/TLS or SMART TLS configured for publication.
HTTP	<ul style="list-style-type: none"> • Cross site scripting. • Broken authentication and session management. • Cross-site request forgery. • Eavesdropping and tampering. 	For network configuration: <ul style="list-style-type: none"> • Disable HTTP. • Select HTTPS for network connections. For publication: <ul style="list-style-type: none"> • Do not select HTTP. • Select HTTPS with authentication.

FTP	<ul style="list-style-type: none"> • FTP brute force attack. • Packet sniffing. • Spoof attack. • User credentials can be compromised since all authentication is done in clear-text. 	<p>For publication:</p> <ul style="list-style-type: none"> • Do not use FTP. • Select either HTTPS with authentication, or SMTP with either SSL/TLS or SMART TLS configured for publication.
Modbus TCP/IP	<ul style="list-style-type: none"> • Message interception. • Information capture. • Arbitrary command issuance. • Unauthorized users can gather and /or tamper device configurations. 	<p>For Modbus device communications:</p> <ul style="list-style-type: none"> • Limit access to Modbus Communications by use of Modbus TCP/IP Filtering. • Disable the Modbus port for each network interface when not in use.

Com'X 210 Settings

Settings Overview

This section describes how to configure the general settings of the Com'X.

⚠ WARNING

INACCURATE DATA RESULTS

Do not incorrectly configure the software, as this can lead to inaccurate reports and/or data results.

Failure to follow these instructions can result in death, serious injury, equipment damage, or permanent loss of data.

Date and Time Settings

The **Date/Time Settings** subtab allows you to set the date and time by time zone through SNTP or manually.

Configuring Date and Time

The time and date settings must be set to the current date and time before enabling Schneider Electric Services on your Com'X.

Any manual changes on the date and time are overwritten by Digital Service Platform. You can only edit the **Timezone**.

It is recommended that DST time zone is selected when using Energy Operation to ensure consistent time stamping with the Com'X.

To set the date and time:

1. Click **Settings > General Settings > Date/Time Settings**.
2. Select the appropriate **Timezone** in the drop-down list. If a DST time zone is selected, the clock will automatically adjust for Daylight Saving Time.
3. Choose one of the following:
 - a. Click the **Today** button to set the date and time automatically with the date and time of your computer.
 - b. Manually enter the date and time in the date and time fields.
 - c. Select Yes for **SNTP support**, then enter an SNTP server address. (Default: pool.ntp.org)
4. Click **Save changes**.

Network Settings

The Com'X offers several connection interfaces.

- Ethernet with two ports
- Wi-Fi
- GPRS or 3G for isolated sites or sites where the IT administrator does not allow access to the network infrastructure.

The available interfaces are determined by the accessories connected to the Com'X: GPRS or 3G modem or Wi-Fi USB key.

Network Configuration Options

The Com'X features two Ethernet ports as well as a bay for a GPRS module or a USB port for 3G modem.

This table presents the network configuration options of the Com'X:

Options	Port			
	Ethernet Port 1	Ethernet Port 2	Wi-Fi	GPRS/3G
GPRS/3G only	Configuration and data collection ⁽¹⁾	Configuration ⁽¹⁾ and data collection	Configuration ⁽²⁾	Data publishing
GPRS/3G and switched network	Configuration and data collection		Configuration ⁽²⁾	Data publishing
Wi-Fi only	Configuration and data collection ⁽¹⁾	Configuration ⁽¹⁾ and data collection	Configuration, data collection, and publishing	–
Wi-Fi and switched network	Configuration and data collection		Configuration, data collection, and publishing	–
2 Switched Ports (1 IP address for both)	Configuration, data collection and publishing		Configuration ⁽²⁾	–
2 Separate Ports (1 IP address for each)	Configuration and data publishing	Configuration and data collection	Configuration ⁽²⁾	–
⁽¹⁾ Preferred usage for this port.				
⁽²⁾ Available only in Wi-Fi Access Point mode.				

NOTE: It is recommended to use an external cellular router instead of the above configurations.

With a GPRS or 3G Modem

The GPRS or 3G modem is used to publish data.

If you want to use Ethernet for data collection, configure the Com'X in **GPRS/3G and Switched network**. Otherwise the Com'X must be configured as **GPRS/3G only**.

When the Com'X is configured in **GPRS/3G only**, the Ethernet port 2 acts as a DHCP server. This mode allows you to connect a PC for configuration.

NOTE: It is recommended to use an external cellular router instead of the above configurations.

If a Wi-Fi module is installed, it can be used to establish a connection with a PC, a tablet, or a smartphone to configure the system.

With a Wi-Fi Key

A Wi-Fi key can be used to publish data. If you want to use Ethernet for data collection, configure the Com'X in Wi-Fi and switched network. Otherwise the Com'X must be configured as Wi-Fi only.

Wired Ethernet

If the Com'X does not use a GPRS/3G modem or a Wi-Fi module for data publishing, the two Ethernet ports can be configured separately.

Selecting a Network Configuration

Select the appropriate network configuration for your system.

1. Click **Settings > General Settings > Network Settings**.
2. Select the network configuration in the **Choose your network configuration** drop-down list.
3. If necessary, enter the parameters for each connection interface displayed. Refer to the corresponding sections.
4. Click **Save changes**.
5. Wait for the Com'X to reboot.
The power LED turns green when the reboot is complete.

Related Topics

- GPRS/3G Settings
- Configuring Advanced Ethernet Settings
- Configuring a Wi-Fi Network

Reboot Cases

Changing some Com'X settings can cause an automatic reboot.

Initial Network Configuration	New Network Configuration
2 separate ports	<ul style="list-style-type: none"> • 2 switched ports • GPRS/3G and 2 switched ports • Wi-Fi and 2 switched ports
GPRS/3G only	<ul style="list-style-type: none"> • 2 switched ports • GPRS/3G and 2 switched ports • Wi-Fi and 2 switched ports
Wi-Fi only	<ul style="list-style-type: none"> • 2 switched ports • GPRS/3G and 2 switched ports • Wi-Fi and 2 switched ports
2 switched ports	<ul style="list-style-type: none"> • 2 separate ports • GPRS/3G only • Wi-Fi only
GPRS/3G and 2 switched ports	<ul style="list-style-type: none"> • 2 separate ports • GPRS/3G only • Wi-Fi only
Wi-Fi and 2 switched ports	<ul style="list-style-type: none"> • 2 separate ports • GPRS/3G only • Wi-Fi only

NOTE: It is recommended to use an external cellular router instead of the GPRS/3G configurations. Please refer to [GPRS/3G Settings](#), page 33 to see a list of recommended external 3G modems.

Ethernet Port Settings

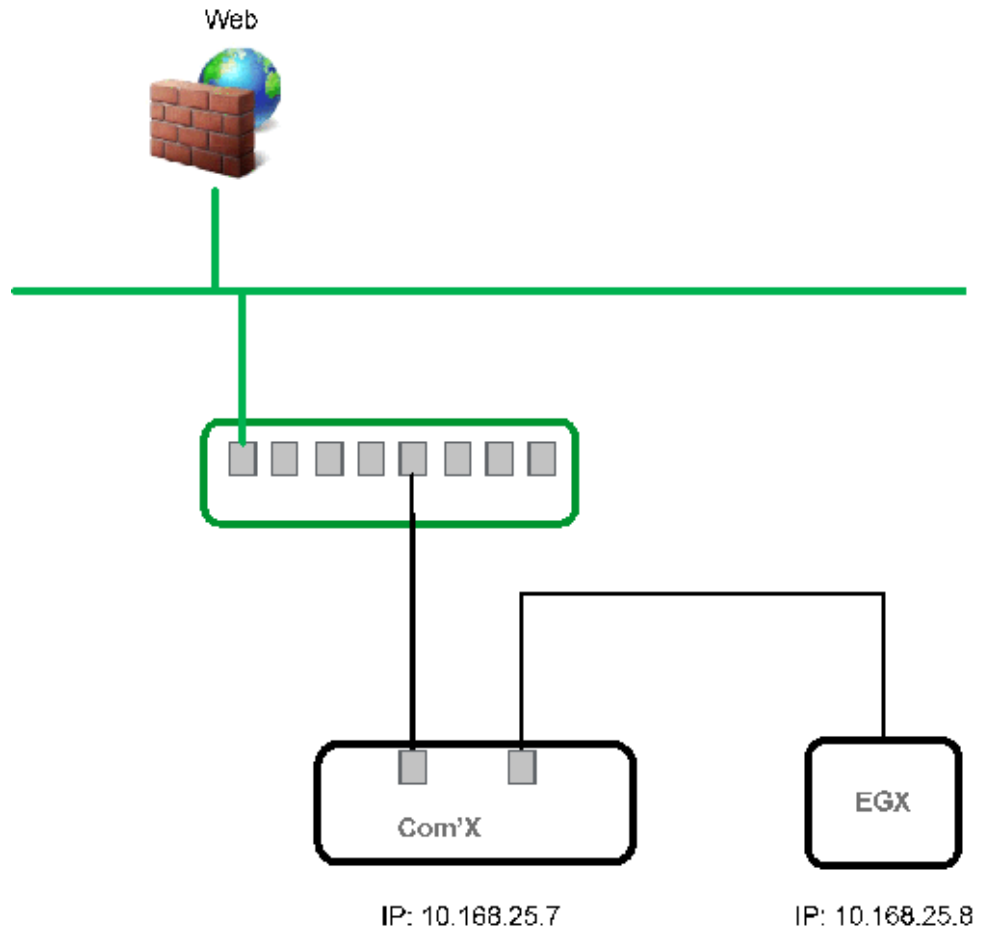
Your Com'X has two Ethernet ports.

The Ethernet ports can be configured in two modes:

- Switch mode: two Ethernet ports share the same configuration.
- Upstream/downstream mode: two Ethernet ports are configured separately.

Switch Mode Configuration

This graphic illustrates the Ethernet port configuration in switch mode:

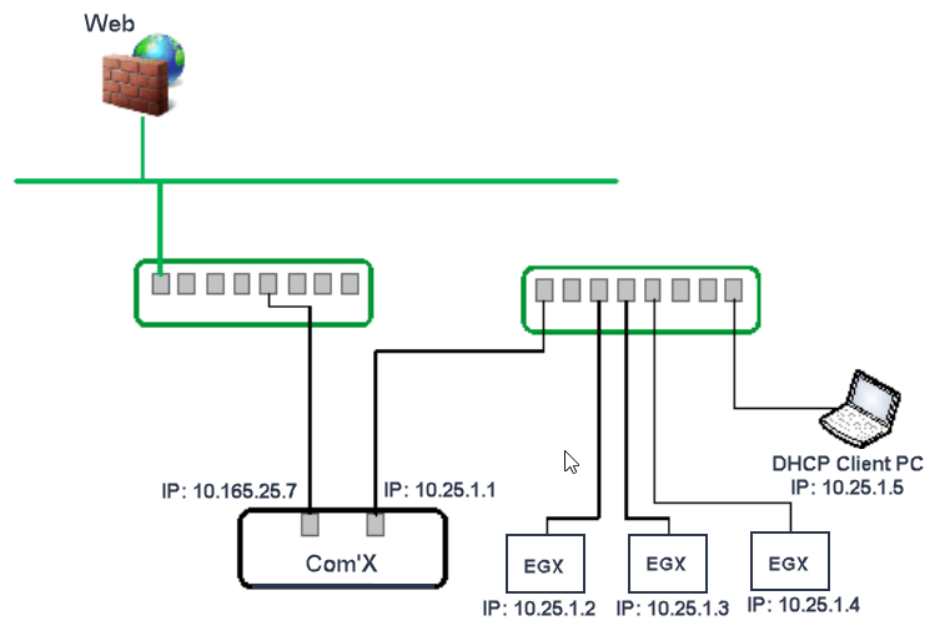


In switch mode, both Ethernet ports have the same settings. Using two ports simplifies wiring:

- one port can be connected to a switch in the local network.
- one port can be used to connect a PC for configuration operations or to connect a data collection device locally with an Ethernet port.

Upstream/Downstream Mode Configuration

This graphic illustrates the Ethernet port configuration in upstream/downstream mode:



In upstream/downstream mode, the two Ethernet ports have different settings and function independently:

- one port must be used for data publishing.
- one port must be used for data collection.

The port used for data publishing (eth1) can be configured in DHCP client mode or static IPv4 address mode. The port used for data collection (eth2) can be configured in DHCP client, static IPv4 address, or DHCP server.

Ethernet Configuration Settings

DHCP client: The IP address is automatically assigned to the Com'X. It is recommended to have a fixed IP address, obtained by a DSL modem or by a network administrator.

Static IPv4 address: Type the IP, subnetwork mask, and default gateway addresses. Addresses are assigned to the Com'X by the IT administrator.

Related Topics

- IPv4 Address Settings

Configuring the Ethernet Ports

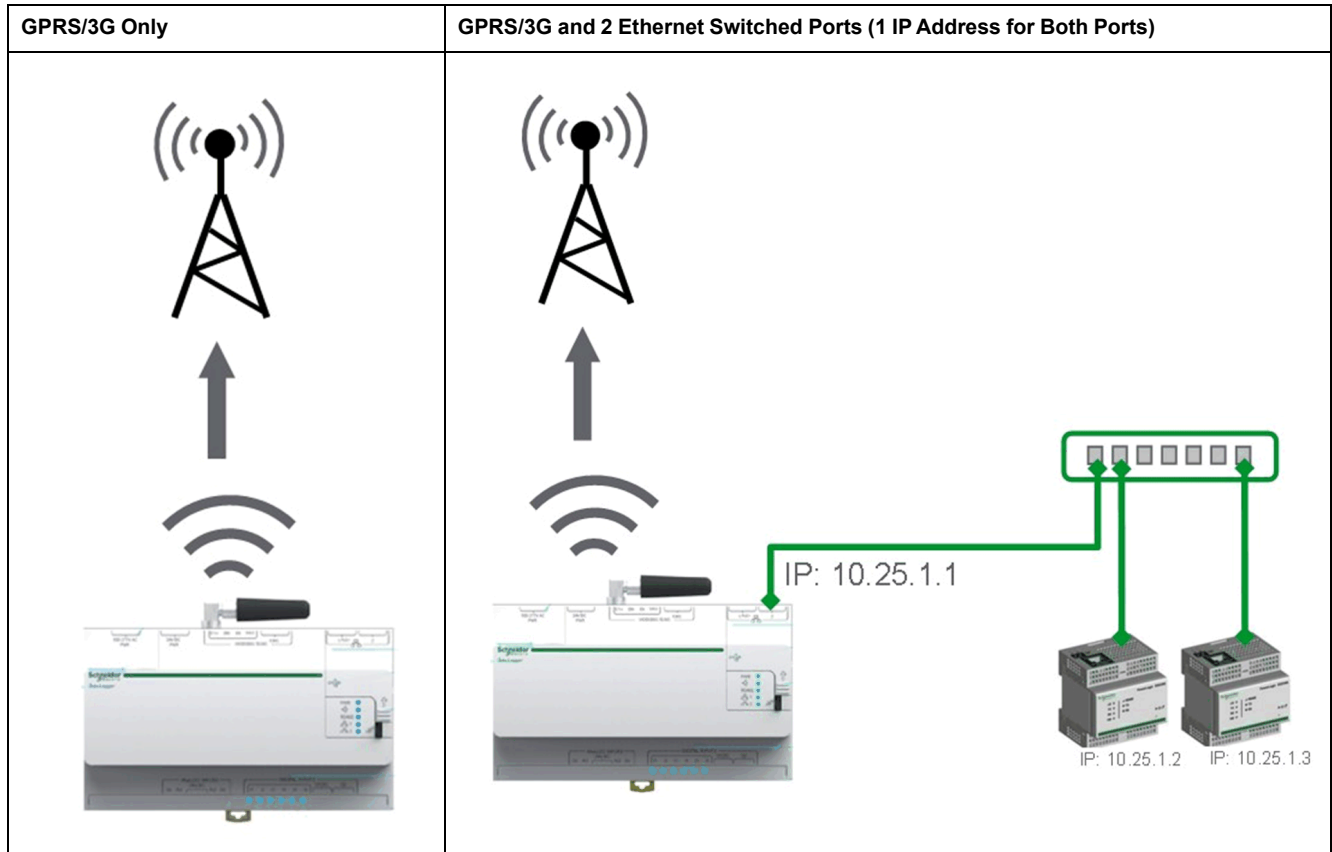
You can configure the Ethernet ports to as two separate ports.

1. Click **Settings > General Settings > Network Settings**.
2. Select the **Choose your network configuration** field.
NOTE: If you change the configuration of the Ethernet port you are configuring through, you will be disconnected through the browser. Begin a new browsing session to continue configuration.
3. Select **2 Separate Ports (1 IP address for each)** in the drop-down list.
4. Select **DHCP client** and **Static IPv4 address** in the **Configuration mode** drop-down list.
5. In the **Ethernet configuration** collapsible menu, enter the parameters in the **WAN network configuration (eth1)** and **LAN network configuration (eth2)** fields.
The **Interface Status** field changes to **ACTIVE** (if correctly wired).
6. In **General network settings** collapsible menu, type the addresses in the **Default gateway**, **Primary DNS server**, and, if necessary, **Secondary DNS server** fields.
Addresses are assigned to the Com'X by the IT administrator.
7. To enable ping replies, select **Yes** in **General network settings > Reply to ping**.
Reply to ping is disabled by default.
8. Click **Save changes**.

GPRS/3G Settings

Cellular access can be added to the Com'X by installing a modem under the cover.

This table illustrates GPRS/3G settings:



Cellular network options depend on the modem that is connected.

GPRS/3G/4G and wireless transmissions are sensitive to local environmental conditions, such as weather, network availability, and other GPRS/3G/4G devices. You could incur increased communication costs in the event of low connectivity.

3G Modems

The following 3G modems have been tested and are compatible with the Com'X. For each modem, refer to the manufacturer's documentation for technical specifications and detailed installation instructions.

Manufacturer/Model	Antenna	Notes
MultiTech (rCell)	External	<ul style="list-style-type: none"> Recommended Connected via an Ethernet cable. This modem must be mounted to the enclosure. Refer to the manufacturer's installation instructions.
Digi Routers	External	<ul style="list-style-type: none"> Recommended Connected via an Ethernet cable. This modem must be mounted to the enclosure. Refer to the manufacturer's installation instructions.
MOXA (OnCell)	External	<ul style="list-style-type: none"> Recommended Connected via an Ethernet cable. This modem must be mounted to the enclosure. Refer to the manufacturer's installation instructions.
eTIC	External	<ul style="list-style-type: none"> Recommended Connected via an Ethernet cable. This modem must be mounted to the enclosure. Refer to the manufacturer's installation instructions.

Related Topics

- Configuring Access Settings with EBXA-GPRS or a 3G Modem
- Configuring Access Settings with EBXA-GPRS-SIM Card

Installing a 3G Modem on the Com'X

You can install a 3G modem on the Com'X.

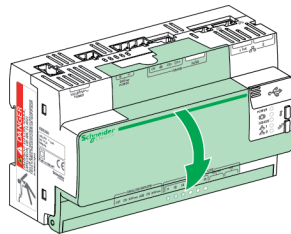
⚠ DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- This equipment must only be installed and serviced by qualified personnel.
- Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices. See NFPA 70E in the USA, CSA Z462 or applicable local standards.

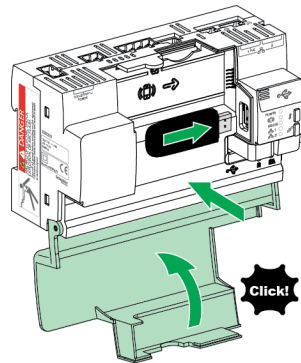
Failure to follow these instructions will result in death or serious injury.

1. Power off the Com'X.
2. Open the Com'X front door.

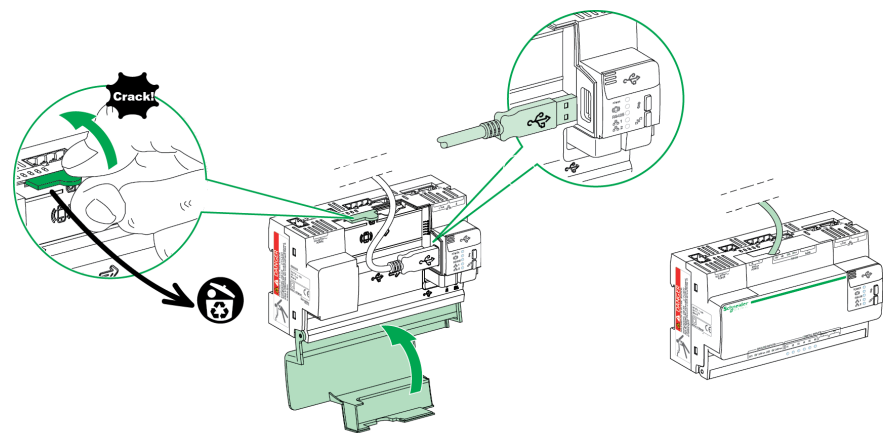


3. Connect the 3G modem.

- For modems that mount inside the Com'X, connect the modem to the internal USB port.

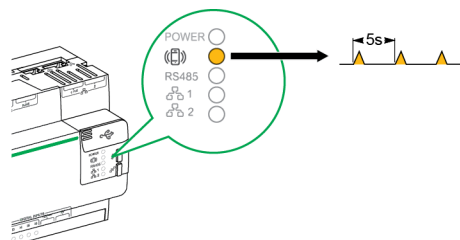


- For 3G modems that do not mount inside the Com'X front cover, break off the tab to create an opening for the cable, then connect the modem cable to the internal USB port.



4. Close the Com'X door as shown above.

5. Power on the Com'X. The Radio Modem LED flashes to show the modem has been detected.



Configuring Access Settings with EBXA-GPRS-SIM Card

You can only use the EBXA GPRS SIM to publish data if you are exporting data to Digital Service Platform.

The SIM card is embedded in the GPRS modem. The access settings of this GPRS modem are set by the Com'X.

The reference **EBXA-GPRS-SIM** must be selected for this GPRS modem.

NOTE: It is recommended to use an external cellular router instead of the EBXA-GPRS-SIM. Please refer to GPRS/3G Settings, page 33 to see a list of recommended external 3G modems.

Configuring Access Settings with EBXA-GPRS or a 3G Modem

You need to configure access settings when using an EBXA-GPRS or 3G modem.

Install the SIM card into the GPRS modem as described in the EBXA-GPRS/EBXA-GPRS-SIM Instruction Sheet, reference 253537613. For 3G, install the SIM card into the 3G modem as described in the manufacturer's installation instructions.

The EBXA-GPR/3G modem requires:

- a mini SIM 2FF type card.
- a minimum 1 MB/month data export on the telecom contract.

A robust M2M SIM card is recommended rather than a standard SIM card.

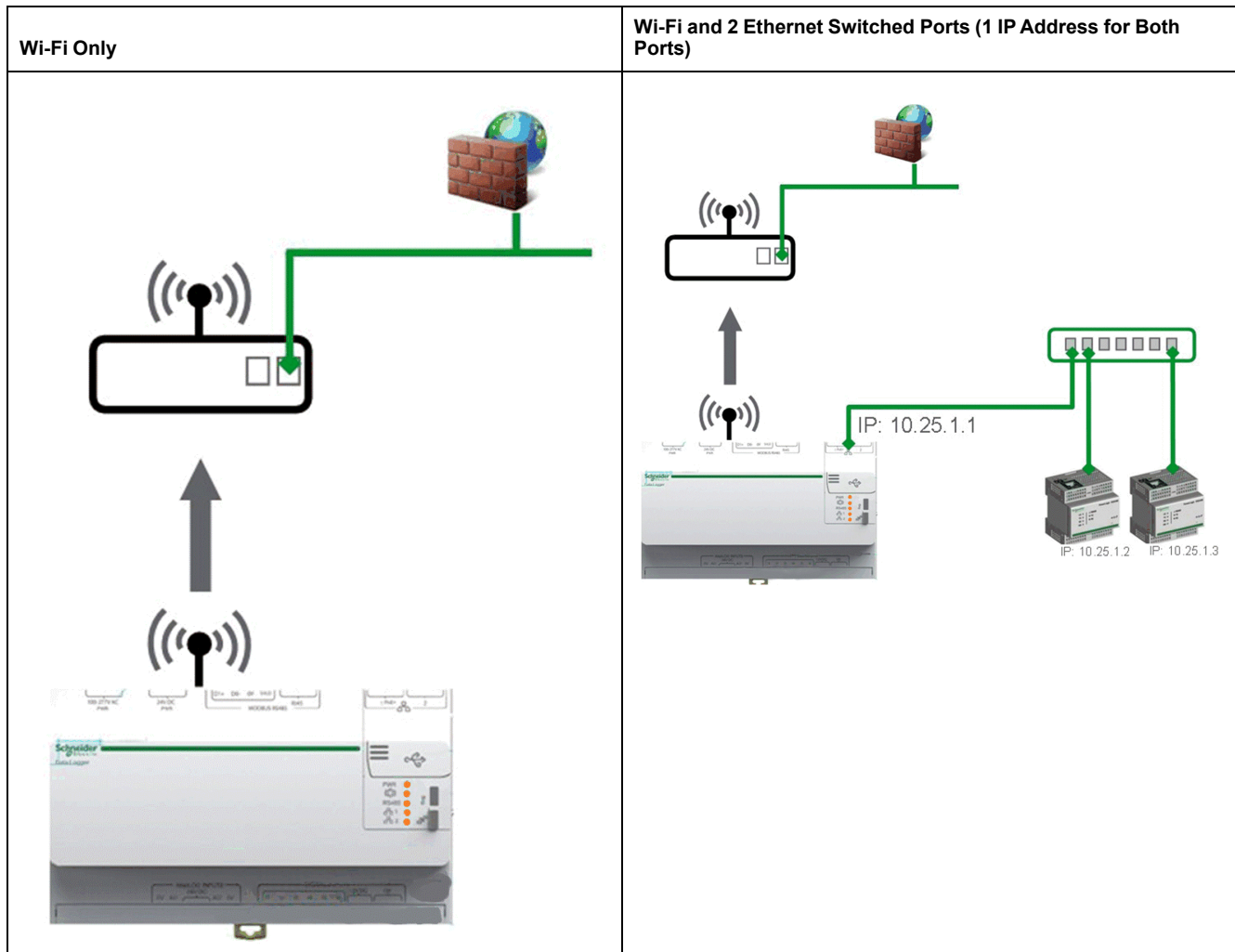
NOTE: It is recommended to use an external cellular router instead of the EBXA-GPRS. Please refer to GPRS/3G Settings, page 33 to see a list of recommended external 3G modems.

1. Click **Settings > General Settings > Network Settings**.
2. Select **EBXA-GPRS/3G**.
3. Type the **APN, Username, Password, and PIN Code** provided by the access provider.
4. Click **Save changes**.

NOTE: The PIN code and the password of the SIM card cannot be changed by the energy server.

Wi-Fi Settings

This table illustrates Wi-Fi settings:



Use any USB port for temporary access, for example, to configure the Com'X.

For permanent use, the Wi-Fi USB key must be installed outside the enclosure for EMC reasons. Schneider Electric provides accessories to mount the Wi-Fi key outside the enclosure.

NOTICE

UNINTENDED EQUIPMENT OPERATION

Do not install the Wi-Fi key inside a metallic enclosure.

Failure to follow these instructions can result in equipment damage.

The Com'X does not enable Point-to-Point connections with other Wi-Fi field devices. Wi-Fi traffic is controlled by the Wi-Fi infrastructure of the site.

Related Topics

- [Wi-Fi Access Point Settings](#)

Configuring a Wi-Fi Network

You can configure your Com'X wireless network.

1. Click **Settings > General Settings > Network Settings**.
2. Select **WiFi only** or **WiFi and 2 Switched Ports (1 IP address network)** in the **Choose your network configuration** dropdown list.

NOTE: Schneider Electric recommends using WPA2.

3. Click Select a Wi-Fi network in the Wi-Fi settings collapsible menu.

4. Click **Refresh network list** to scan all the Wi-Fi networks available.
5. Select the Wi-Fi network required. Type the key in the **Secure key** field if the key does not appear automatically.
6. Select **Other** if the required Wi-Fi network does not automatically appear in the list of Wi-Fi networks. Type the SSID and the key in the **Secure key** field.
7. Click **Save changes**.

Running Network Diagnostics

You can run diagnostic tests for the network and server connections.

1. Navigate to **Settings > General Settings > Network Settings**.
2. Click **Launch diagnostic** in the **Diagnostic network** menu.
A new **Diagnostic Network** window opens which shows the progress and status of the diagnostic tests.
3. Click **Start** to restart the network diagnostics or click **Close** to exit the **Diagnostic Network** window.

Proxy Settings

It is necessary to configure Internet proxy settings in the Com'X in a couple of scenarios.

- if you use the HTTP or HTTPS protocols, and
- if the network administrator has implemented an Internet proxy on your local network

Configuring Proxy Settings

You can configure the Internet proxy settings, if required.

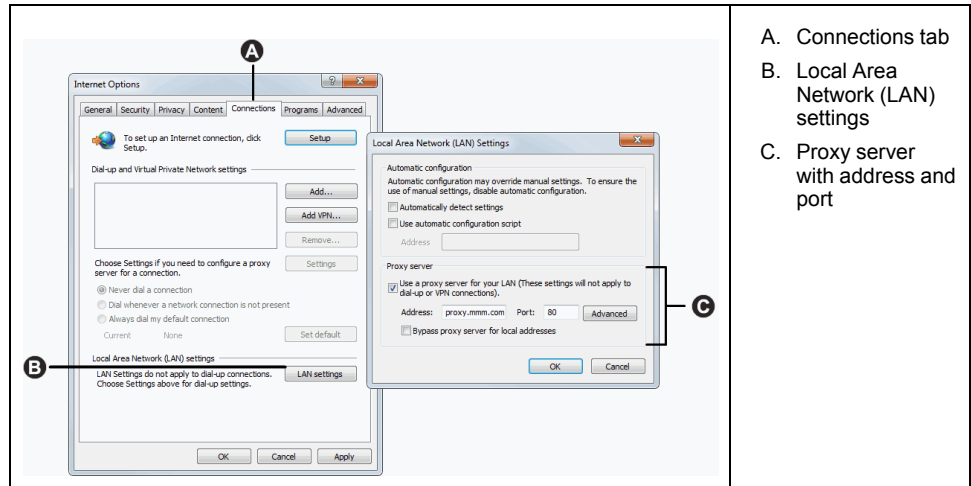
The proxy address and port number are provided by your network administrator, or you can retrieve these values in the **Internet Options** of a PC connected to the LAN.

1. Click **Settings > General Settings > Proxy Settings**.
2. Select the **HTTP Proxy settings** or **HTTPS Proxy settings** field.
3. Select the **Enable HTTP proxy support** check box.
4. Type the address and port of the proxy in the **Proxy address** and **Proxy port** fields.
5. If proxy authentication is required, select **Yes** for **Proxy requires authentication**, and enter the login and password to the proxy.
6. Click **Save changes**.

Retrieving Proxy Values

You can retrieve your network proxy values in Internet Explorer.

This graphic shows the interface to retrieve proxy values from Internet Explorer:



- A. Connections tab
- B. Local Area Network (LAN) settings
- C. Proxy server with address and port

1. Click the **Tools** menu.
2. Select **Internet Options** in the drop-down list.
3. Select the **Connections** tab.
4. Click the **LAN settings** button.
5. Read the values of the proxy in the **Local Area Network (LAN) Settings** window.
6. Copy the same values into the Com'X proxy settings.

Contact Management

Contact Management allows you to create an address list for publishing data over SMTP or when sending emails on event in **Custom Events**.

You must create at least one contact before setting up email on event.

NOTICE

DATA PRIVACY INFRINGEMENT

Comply with regional data privacy regulations and laws when using individual email addresses and personal information.

Failure to follow these instructions can result in complaints, liability, or penalties for non-compliance with applicable data protection regulations.

Creating a Contact

You can create a contact.

1. Click **Settings > General Settings > Contact Management**.
2. Type the **Name** and **Email address**, then press Enter or click +.
The Contact is added to list.
3. Click **Save Recipient List**.

The contacts are now available in:

- **Publication settings** for publishing over SMTP.
- **Custom Events** for setting up email on events.

To delete a contact, click the X beside the contact name, then **Save Recipient List**.

Related Topics

- Event Settings
- Configuring SMTP Transfer Protocol

Email Settings

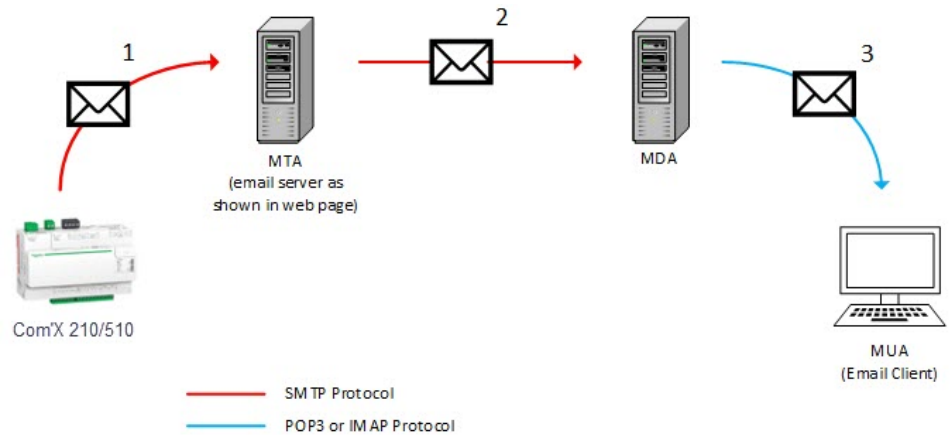
Email Settings allows you to configure the connection to an SMTP server to publish a .csv file over SMTP.

NOTICE
DATA PRIVACY INFRINGEMENT
Comply with regional data privacy regulations and laws when using individual email addresses and personal information.
Failure to follow these instructions can result in complaints, liability, or penalties for non-compliance with applicable data protection regulations.

Email Service

Configure the Com'X to send emails to deliver periodic data publications and custom event notifications.

NOTE: Contact your network administrator to determine the correct IT connection for port, LAN connection to Internet, and email server to use.



- Com'X sends an email to the configured email server/MTA (Mail Transfer Agent) using SMTP protocol.
- MTA forwards the message to the email client MDA (Mail Delivery Agent).
- MDA delivers email to the client/MUA (Mail User Agent) using POP3 or IMAP protocol.

Recommendation

- To ensure the secure delivery of email to the MTA, the Com'X must be updated with the latest available firmware to use current secure email transfer mechanisms. However, this will not guarantee full compatibility with the latest version of the internet email service provider.
- Schneider Electric recommends using an on-premise email server (instead of internet email service provider) with a stable and clear security policy defined by the client IT department.
- Schneider Electric strongly recommends the use of "TLS/SSL" or "STARTTLS" for the connection security mode between the Com'X and the Email SMTP server. The "None" option is provided only for compatibility with older Email SMTP servers.

NOTE: Avoid using the “None” security mode option. The “None” security mode option is not recommended as it does not support secure communications.

- Each internet email service provider has its own security policy and data protection mechanisms to check the sender's reputation, detect a spam message, etc.

Configuring the SMTP Server

You can configure the Com'X SMTP server.

NOTE: SMTP is not a secure protocol, as login IDs and passwords are communicated in plain text. Schneider Electric strongly recommends using SMTP with TLS/SSL or STARTTLS connection security mode. Refer to [Security Configuration Recommendations](#), page 27 for additional information regarding risks associated with unsecure protocols and recommended best practices.

NOTICE

UNAUTHORIZED ACCESS

Use SMTP only with TLS/SSL or STARTTLS connection security mode.

Failure to follow these instructions can result in equipment damage.

To configure the SMTP server:

1. Click **Settings > General Settings > Email Settings**, then click **Yes** to enable the connection to SMTP server.

NOTE: Disabling the connection blocks SMTP publication or event emails from being sent.
2. Type the server address (Fully qualified domain name, IP address, or host name).
3. Select the **Connection security mode**: None, TLS/SSL or STARTTLS.

NOTE: Schneider Electric strongly recommends using SMTP with TLS/SSL or STARTTLS connection security mode.
4. Type the outgoing delivery port in the **Server port** field. The port for the selected security mode is provided by default.
5. Select **Yes** in the Authentication required field if the SMTP server requires authentication. Type the username and the password.
6. Type the address of the email sender in the **From** address field. The factory setting is in the format: `Com'X[model]_SiteName_[last three digits of the mac address]@schneider-electric.com`.

NOTE: The **From** address must reference a valid email account. Otherwise, emails may not be delivered.
7. Select the **Email Language**
8. Click **Save changes**.
9. Enter a valid email address in **Recipient address for test**, then click **Send Test Email**.

Ensure the test email was received. The email is sent in the language of the current login session, not the language selected above.

Continue configuring .csv publication over SMTP on the **Publication** subtab, if necessary. To set up email on event, see **Events**.

Refer to the firmware release notes for a list of servers validated at the time of the release.

Related Topics

- Event Settings

Publication

Use the **Publication** subtab to select the platform to which the logged data is sent.

The Com'X can publish data to three different Schneider Electric platforms (database servers):

- Energy Operation
- Digital Service Platform (DSP)
- CSV Export

The Com'X exports the data in the correct file format according to the selected platform. Then the data can be analyzed in the service to which you have subscribed.

The subscription to Energy Operation or DSP must be set up with a Schneider Electric representative before setting up the Com'X **Destination platform**.

To publish to DSP, you must enable Schneider Electric Services in **Settings > General Settings > Schneider Electric Services**.

With **CSV Export**, the Com'X exports data to your own database server in a .csv file.

Selecting Platform and Publication Frequency

Use the Publication subtab to select the platform to which the logged data is sent and at what frequency.

1. Click **Settings > General Settings > Publication**.
2. Select the **Destination platform** in the drop-down list.
3. Select how often the data is sent in the **Publication frequency** drop-down list:
 - Weekly: select the day of the week.
 - Daily: the data is sent at 1:00 a.m. local time.
 - For higher frequencies, publication times are calculated starting at 0:00 a.m. For example, if **Every 2 hours** is selected, data is sent at 0:00 a.m., 2:00 a.m., 4:00 a.m., and so on. If **Every 3 hours** is selected, data is sent at 0:00 a.m., 3:00 a.m., 6:00 a.m., and so on.
4. Click **Save changes**.

The first publication occurs on the first hour that matches the selected frequency after the **Start publication** task. For example, if **Every 2 hours** is selected and the publication starts at 9:45 a.m., the first publication is at 10:00 a.m.

NOTE: DSP will be available as a drop-down option under **Destination platform** only after you enable Schneider Electric services.

Related Topics

- Com'X 210 Commissioning

Define the Transfer Protocol

There are different protocols that you can use to export data.

The protocols in the **Protocol** drop-down list vary depending on the selected platform, as shown in this table:

Platforms	Supported Transfer Protocols	File Format
Energy Operation	<ul style="list-style-type: none"> FTP HTTP and HTTPS 	XML
Digital Service Platform	Automatically defined by the Com'X	EWS
CSV export	<ul style="list-style-type: none"> FTP HTTP and HTTPS SMTP 	CSV

Configuring FTP Transfer Protocol

You can configure FTP as the file transfer protocol for publications.

NOTE: FTP is not a secure protocol, as login IDs and passwords are communicated in plain text. Schneider Electric strongly recommends using only HTTPS protocol for security purposes. Refer to [Security Configuration Recommendations, page 27](#) for additional information regarding risks associated with unsecure protocols and recommended best practices.

1. Click **Settings > General Settings > Publication**.
2. Select the **Destination platform** in the drop-down list.
3. Select FTP in the **Protocol** drop-down list.
4. Type the address of the server transporting the data in the **Server** field.
Server address for Energy Operation is automatically filled. Do not modify the server address.
5. Type the outgoing delivery port in the **Port** field.
The factory setting is 21.
6. Select **Yes** in the **Authentication required** field for any platform requiring authentication, for example Energy Operation.
7. Type the username and the password.
For Schneider Electric platforms, this information is given with the subscription contract. Contact the Schneider Electric representative to provide you with this information.
8. For CSV, type the directory information for the remote server in the **Directory** field.
9. Click **Save changes**.

Configuring HTTP and HTTPS Transfer Protocols

You can configure HTTP or HTTPS as the file transfer protocol for publications.

NOTE: HTTP is not a secure protocol as login IDs and passwords are communicated in plain text. Schneider Electric strongly recommends using only HTTPS protocol. Disable HTTP on each interface for security purposes. Refer to [Security Configuration Recommendations, page 27](#) for additional information regarding risks associated with unsecure protocols and recommended best practices.

Certificate considerations for HTTPS:

- You can secure the HTTP connection to your server with TLS/SSL technology.
- As with a web browser, the box is preloaded with all the major certificate authorities as of the time of the firmware release. Schneider Electric offers an update of the list of certificate authorities with the firmware updates.
This means that your HTTPS server certificates must have been issued by one of the box's trusted certificate authorities. Check with your IT department

to know if your HTTPS server certificate complies with this rule. If not, you can select HTTP.

1. Click **Settings > General Settings > Publication**.
2. Select the **Destination platform** in the drop-down list.
3. Select HTTP or HTTPS in the **Protocol** drop-down list.
4. Type the address of the server transporting the data in the **Server** field.
The server address is automatically filled for Energy Operation. Do not modify the server address for this platform.
5. Type the outgoing delivery port in the **Port** field.
The factory setting is 80 for HTTP and 443 for HTTPS.
6. Select **Yes** in the **Authentication required** field for any platform requiring authentication, for example Energy Operation.
7. Type the username and the password.
For Schneider Electric platforms, this information is given with the subscription contract. Contact the Schneider Electric representative to provide you with this information.

The username and password are case-sensitive.
8. In the **Path** field, type the path to the server script executed by the web server when the Com'X sends data to the web server.
This field is already filled with a /. Do not modify this value when Energy Operation is selected as a platform.
9. According to your network administrator either:
 - type the file name that the web server expects in the **Field Name** field (only for CSV), or
 - use the **datafile1** factory setting.
10. Click **Save changes**.

Related Topics

- Certificate Authorities

Configuring SMTP Transfer Protocol

The SMTP protocol is available only with a CSV export. SMTP is not a secure protocol. Refer to *Security Configuration Recommendations*, page 27 for additional information regarding risks associated with unsecure protocols and recommended best practices.

NOTICE

DATA PRIVACY INFRINGEMENT

Comply with regional data privacy regulations and laws when using individual email addresses and personal information.

Failure to follow these instructions can result in complaints, liability, or penalties for non-compliance with applicable data protection regulations.

To send the data file by email with the SMTP protocol:

1. Click **Settings > General Settings > Publication**.
2. Select CSV export in the **Destination platform** drop-down list.
3. Select SMTP in the **Protocol** drop-down list.
4. Enter the address of the server transporting data in the **Server** field.

5. Enter the outgoing delivery port in the **Port** field.
6. Select **Yes** for **Authentication required**.
7. Enter the user login information and the password.
This information is given with the subscription contract. contact the local IT representative to get this information.
NOTE: The username and password are case-sensitive.
8. Enter the email address in the **From address** field.
The factory setting for email is ComX[model]_SiteName_[last three digits of the mac address]@schneider-electric.com.
9. Enter the email addresses of recipients in the **To address** field.
Separate the addresses with a semicolon (;).
10. Click **Save changes**.

Exported files are zipped to reduce the size of attached documents in the email.

Related Topics

- [Creating a Contact](#)
- [Configuring the SMTP Server](#)

Publication Identification Settings

There are publication identification settings for Energy Operation.

Field/Button	Description
Publication ID	This number is a unique identifier of the site for the Energy Operation database. It is used to create a site in Energy Operation. This ID is automatically generated by the Com'X.
Generate new publication ID	This button generates a new publication ID number. Use this button whenever you reuse: <ul style="list-style-type: none"> • the Com'X for a new site. • the current Com'X configuration on a different site.

File Format of CSV Export

There is one file exported for each device.

Exported files are in the following naming format: `Device Name_Date&time.csv` where `Device Name` is the name given to the slave device. The date and time are appended to the file name in the following format: `_yyyymmddhhmmss`.

For example:

- **Device name:** `Building 1 Utility Entrance`
- **Date/time:** `20130218115216`

The exported file is named `Building 1 Utility Entrance_20130218115216.csv` and was exported on February 18, 2013 at 11:52:16 a.m.

The following table provides the details of each line of a CSV file, with sample data:

Row	Data in CSV Format	Description
1	[Gateway Name,Gateway SN,Gateway IP Address,Gateway MAC Address,Device Name,Device Local ID,Device Type ID,Device Type Name,Logging Interval,Historical Intervals]	This row contains the column headings for the information in row 2.
2	[ComX210_F930B8, DN13045SBX10091,10.195.23.45,00:80:67:F9:30:B8,	This row contains the information about the Com'X 210 and the logged device.

Row	Data in CSV Format	Description
	COMX_008067F930B8_1,Resource-1,PM810,PM810,30,6,23227,157.198.184.116,Building 1 Utility Entrance,3,CM4000,15]	
3	This row is left blank.	–
4	[...Topic ID 1, Topic ID 2, Topic ID 3]	This row contains the column headings for the topic IDs ⁽¹⁾ in row 5. The first 3 commas are used for layout purposes in a spreadsheet application.
5	[...1617,1621,1625]	This row contains the topic IDs of the values logged.
6	This row is left blank.	–
7	[Error,UTC Offset (Minutes),Local Time Stamp,Apparent Energy (kVAh),Real Energy (kWh),Reactive Energy (kVARh)]	This row contains the column headings for the data logged in rows 8 and higher.
8 and higher	[0,-300,2008-10-09 14:15:00,1400738,219,1201962.707,647069.906,15] [0,-300,2008-10-09 14:20:00,1400758,260,1201980.725,647078.602,15] [0,-300,2008-10-09 14:25:00,1400778,198,1201998.661,647087.233,15]	These rows contain the logged data.
<p>⁽¹⁾ A topic ID is a numerical reference to the quantity being logged. The name given to a quantity may slightly differ between devices and languages. Topic IDs are used to identify the quantity regardless of the device or language.</p>		

Digital Service Platform Connection

To publish to DSP, you must enable Schneider Electric Services in **Settings > General Settings > Schneider Electric Services**.

Each state of connection to Digital Service Platform is confirmed with a green check mark when enabled or grayed out when disabled. A red check mark indicates an issue with the specific connection state. The three connection states are:

Initialize – DSP agent initialized.

Authenticate – DSP connection authenticated.

Connect – DSP connection complete, and device has been identified on the remote platform.

NOTE: Maintenance logs record Schneider Electric Services state changes.

When using the DSP connection, firmware upgrades are automatically launched. It is recommended that you update the firmware if you want to use the DSP platform through a slower GPRS connection.

Related Topics

- Upgrading Firmware via DSP

Enabling Schneider Electric Services

To enable Schneider Electric Services:

1. Configure **Proxy Settings**, if required.
2. Click **Settings > General Settings > Schneider Electric Services**.
3. Click **Yes** in the Configuration section.
4. Click **Save Changes**.

All three states display in green and a confirmation message displays when DSP connection is enabled.

NOTE: The configured date and time are synchronized periodically and display after DSP sync time command runs automatically.

Disabling Schneider Electric Services

To disable Schneider Electric Services:

1. Click **Settings > General Settings > Schneider Electric Services**.
2. Click **No** in the Configuration section.
3. Click **Save Changes**.

All three states are grayed out and a confirmation message displays when DSP connection is disabled.

Wi-Fi Access Point Settings

The USB Wi-Fi key can be used as a temporary communication medium during the commissioning phase.

This allows you to use a laptop or a tablet to configure the Com'X.

In this case, communication is direct between the Com'X and the laptop or tablet. The Com'X functions as a Wi-Fi access point.

Wi-Fi access can be added to the Com'X using a Wi-Fi USB key inserted under the cover or on the front face. It is recommended to use the front face USB, as you can easily remove the USB key after configuration is done.


Installing the Wi-Fi USB key directly on a Com'X port is allowed only for temporary access point connection for configuration.

Activating the Wi-Fi Access Point

You can configure the USB Wi-Fi key to be used as a temporary communication medium during the commissioning phase.

1. Click **Settings > General Settings > Wi-Fi Access Point Settings**.
2. Click **Yes** to **Enable Wi-Fi access point**.
3. Select the duration in the **Session duration** drop-down list (Default: 1 hour).
4. Click **Save changes**.

If **Session duration** is modified during a Wi-Fi access point session, the modification is taken into account at the next session.

This setting only enables access point mode. To start the Wi-Fi access point mode session, push the Wi-Fi button  located near the USB port on the front face. The Wi-Fi button LED flashes green.

Related Topics

- Accessing Through Wi-Fi Access Point Mode With Windows
- Accessing Through Wi-Fi Access Point Mode

Deactivating the Wi-Fi

You can end the Wi-Fi access point session.

1. Press the Wi-Fi button on the front of the Com'X.

The Wi-Fi button LED flashes orange, and the Wi-Fi access point session ends.

Site Information

The **Site name** field that appears in the **Site Information** collapsible menu is used as a site name by different platforms.

All measurements are assigned to this site location.

In Energy Operation, the **Site name** parameter is used to create the site location name that appears in Energy Operation platform environment.

Configuring Site Information

You can change the site name.

1. Click **Settings > Site Settings > Site Information**.
2. Enter the site location name.

NOTE: The site name must not include any of these characters: “/:*?<>|. A space is not allowed in front of or after the site name.

3. Click **Save changes**.

Data Logging

The Com'X can log data at pre-defined intervals.

The logging interval can be set for each type of commodity, for example, electricity, water, or gas. Each device can report only one type of commodity.

Defining the Logging Intervals

It is important to consider how much data is being logged across all devices when selecting the logging interval and number of topics to log.

Logging too many topics per interval may affect Com'X performance, including degraded web page response and missed logging intervals.

For example, for a logging interval of less than five minutes, it is recommended that you log no more than 8 devices with 50 total topics.

1. Click **Settings > Site Settings > Data Logging**.
2. Select your country.

NOTE: This will automatically set the logging intervals of data for different commodities in the country. You can also edit these intervals individually.

3. Click **Save changes**.

Security

You can configure the firewall, upload a certificate provided by your network administrator, and control HTTPS redirection.

Security displays the Com'X firewall settings as well as the HTTPS security certificate currently in use.

Firewall Management

Firewall Management allows you to enable or disable the ports and configure port numbers per interface, except where noted.

Related Topics

- Modbus Register Mapping
- Selecting Measurements to Log or Publish

Port Settings

There are default **Firewall Management** settings for each protocol per interface.

	Ethernet 1	Ethernet 2	Wi-Fi	GPRS/3G
HTTP	80, Enabled	80, Enabled	80, Enabled	80, Disabled
HTTPS	443, Enabled ⁽¹⁾	443, Enabled ⁽¹⁾	443, Enabled	443, Disabled
Modbus TCP	502, Disable	502, Enabled	502, Enabled	502, Disabled
⁽¹⁾ Cannot be updated.				

NOTE: Refer to [Security Configuration Recommendations](#), page 27 for additional information regarding risks associated with unsecure protocols and recommended best practices.

Upstream Network Access

In **Firewall Management**, you can enable upstream network access.

This allows downstream devices to access servers (such as DNS, SNTP, and SMTP) on the upstream network.

The table below describes the downstream interface (where the message originated) and the upstream interface on which the message will be forwarded, based on your network selection.

Network Option	Downstream (from)	Upstream (to)
GPRS/3G only	Ethernet Port 2	GPRS/3G
GPRS/3G and switched network	---	---
Wi-Fi only	Ethernet Port 2	Wi-Fi
Wi-Fi and switched network	---	---
2 Switched Ports (1 IP address for both)	Upstream network access not available	
2 Separate Ports (1 IP address for each)	Ethernet Port 2	Ethernet Port 1

For example, with the Com'X configured to use two separate Ethernet ports, an IFE connected downstream on Com'X Ethernet Port 2 can send emails to EcoStruxure™ Facility Expert through Ethernet Port 1.

Upstream network access is disabled by default. When enabled, access adapts to the network configuration in **Network Settings**.

Configuring Firewall Settings

You can configure firewall settings.

NOTE: HTTP and Modbus are not a secure protocols. Schneider Electric strongly recommends using only HTTPS protocol. Disable the HTTP and Modbus ports for each interface for security purposes. If Modbus access is required, Schneider Electric strongly recommends using Modbus IP filtering feature for added security.

1. Click **Settings > Security > Firewall Management**. Configure each interface by protocol according to the available options above.

NOTE: Editable port numbers can be set to the default value or any port number above 1023.

2. Alternatively, click **Defaults** to reset to defaults.
3. Click **Save changes**.

Disabling DPWS and SSH services

DPWS and SSH services are enabled by default. DPWS uses a specific port for Com'X discovery and SSH uses a specific port for remote access by Schneider Electric technical support. For security reasons it is recommended to disable these services by setting the options to **No** and enabling them only when required.


NOTE: Com'X cannot be discovered by other devices after DPWS service is disabled. It is recommended to record the Com'X IP address before disabling DPWS service.

To disable DPWS and SSH services:

1. Select **Settings>Firewall Management>Services**.
2. Select **No** to disable DPWS service.
3. Select **No** to disable SSH service.
4. Select **Save changes** to save settings.

Disabling the Password Reset Button

For a Com'X installed in a publicly accessible location, you can disable the password reset function for the Backup button.

The Backup button () is located on the front face.

If you lose the default admin password, you must perform a factory reset on the Com'X to reset the password to default. This destroys all logged data, user accounts, and configuration.

NOTICE

IRRECOVERABLE PASSWORD

Record your device's user and password information in a secure location.

Failure to follow these instructions can result in data loss.

It is recommended to save a backup configuration before disabling the password reset button.

1. Click **Settings > Security > Firewall Management**.
2. Click **Enable default admin reset**.
3. Click **No** to disable the password reset button.
4. Click **Save changes**.

Account Lockout Policy

Account lockout feature disables a user account when the number of failed login attempts exceeds the set limit within a predetermined time interval. This feature is enabled by default.

You can configure the following:

- Enable account lockout Account lockout policy is enabled by default. Select **No** to disable this feature. It is recommended to keep the Account Lockout feature enabled to secure the device from unauthorized access.
- Reset account lockout counter (number of attempts) determines the number of invalid login attempts allowed before user account gets disabled. The default is set to 10 attempts.
- Account lockout duration (minutes) determines amount of time user account remains disabled. The default is set to 15 minutes.

Configuring Account Lockout Policy

To configure account lockout policy:

1. Navigate to **Firewall Management**.
2. Click **Account lockout Policy**.
3. Enter **Reset account lockout counter**.
4. Click **Save changes**.

Disabling Account Lockout Policy

NOTE:It is recommended to keep the Account Lockout enabled to better secure the device from unauthorized access.

1. Navigate to **Firewall Management**.
2. Click **Account lockout Policy**.
3. Enter **No** to disable the account lockout policy.
4. Click **Save changes**.

Warning Banner Overview

The Warning Banner allows you to display a message to warn against unauthorized use and advice authorized users of their obligations relating to acceptable use of the Com'X. This feature is disabled by default. Once enabled, a user can access Com'X login page only after agreeing to the terms and conditions displayed in the Warning Banner.

You can configure the following:

- Enable warning banner – allows you to enable the warning banner to be displayed for users prior to login. This is disabled by default. Once enabled, the warning banner text field displays.
- Warning banner text –You can enter desired text to warn against unauthorized use and notify authorized users of their obligations relating to acceptable use of Com'X. A maximum of 4000 characters is allowed. If you enter more than 4000 characters, the text displays in red and the **Save changes** button is disabled.
- Defaults – allows you revert to default settings. The Warning Banner gets disabled and the Warning banner text field is hidden.

Configuring Warning Banner Settings

To configure Warning Banner settings:

1. Navigate to **Settings >Firewall Management**.
2. Click **Warning Banner Settings**.
3. Click **Yes** to enable warning banner.
4. Enter text to be displayed in the warning banner.

5. Click **Save changes**.

Disabling Warning Banner Settings

To disable Warning Banner settings:

1. Navigate to **Settings > Firewall Management**.
2. Click **Warning Banner Settings**.
3. Click **Defaults** to disable the warning banner.
4. Click **Save changes**.

Certificates

You can view the current HTTPS security certificate, upload a certificate provided by your network administrator to the Com'X, and reset to factory default from this page.

Uploading a New Certificate

You can install a new HTTPS certificate on your device.

It is recommended to create a backup of your configuration before installing a new certificate. To update the HTTPS certificate:

1. Click **Settings > Security > Certificates**.
2. Click inside the text box **Install a new certificate**.
3. In the browser, select your *.pem file, then click **Open**.
4. Click **Install**. The **Installed certificate details** update to display the new certificate.

To remove the current certificate and set the Com'X back to the factory default certificate, click **Reset**.

HTTPS Redirection

HTTPS Redirection allows you to secure the communication between PC and Com'X and is enabled by default.

NOTICE

UNAUTHORIZED ACCESS

Do not disable HTTPS redirection if there is sensitive or private information on your local network.

Failure to follow these instructions can result in equipment damage.

Schneider Electric recommends using **HTTPS Redirection**. Disabling the HTTPS redirection disables your browser security check and compromises the security of your local network.

Event Settings

Events includes predefined and custom events that can be sent to EcoStruxure™ Facility Expert.

Custom events can also be sent to an email recipient.

Before configuring events for EcoStruxure™ Facility Expert, contact EcoStruxure™ Facility Expert support to confirm availability of events. To send events to EcoStruxure™ Facility Expert through DSP, you must enable Schneider ElectricServices in **Settings > General Settings > Schneider Electric Services**.

To enable/disable predefined or custom events, click **Settings > Events > Event Settings**.

Predefined Events

Predefined Events are defined in the Com'X for protection devices. Enabling **Predefined Events** allows Facility Expert users to send event information from Com'X to Facility Expert.

Your Schneider Electric Partner can help you understand how to use these events to signal pre-trip conditions, analyze trips, and schedule periodic maintenance.

Predefined Events cannot be edited or acknowledged from the Com'X.

To enable/disable predefined events, click **Settings > Events > Event Settings**.

Custom Events

Custom Events allows you to define event conditions for any device using the drag and drop event builder.

An event consists of the following block elements, found in the event builder menu.

Block Element	Description
Event	Container block for event conditions, actions, and severity level field.
Event Conditions	<ul style="list-style-type: none"> • Threshold: Set one threshold value at which an event occurs. • Pickup/Dropout: Set the value at which an event occurs (pickup) and the value at which the event is no longer active (dropout). Use this type to avoid nuisance events. • Boolean: Create an event when a Boolean topic value changes, is True, or is False, for example, when breaker open status is True. • And: Allows you to combine up to three conditions for an event.
Devices	<p>Select the device and topic that trigger an event. For example, receive a notification when the Temperature on a Temperature Probe Pt100 exceeds 26°C.</p> <p>The device must be connected to the Com'X in Device Settings.</p>
Value	<ul style="list-style-type: none"> • Threshold value for the selected topic. • Contact for sending email on event.
Actions	<ul style="list-style-type: none"> • Send Email: The Com'X routes an email to the specified recipient when the event conditions are met. • Send to EcoStruxure™ Facility Expert: You can enter text in the Action block, for example, the event description. It is recommended to use the same or similar text as the Event Name field in the Com'X.

Creating a Custom Event

Use the drag and drop event builder to define event conditions for any device.

Before You Begin:

- You should be familiar with the device register lists and values.
- Enable custom events in **Settings > Events > Event Settings**.

- For email on event, you must enable Email Service in **Email Settings** and create at least one contact in **Contact Management**.

⚠ WARNING

INACCURATE DATA RESULTS

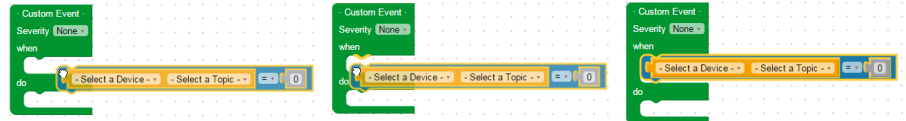
- Do not incorrectly configure the software, as this can lead to inaccurate reports and/or data results.
- Do not base your maintenance or service actions solely on messages and information displayed by the software.
- Do not rely solely on data displayed in the software reports to determine if the system is functioning correctly or meeting all applicable standards and requirements.
- Do not use data displayed in the software as a substitute for proper workplace practices or equipment maintenance.

Failure to follow these instructions can result in death, serious injury, equipment damage, or permanent loss of data.

1. Click **Settings > Events > Custom Events**, then click **New Custom Event**.
The event builder displays.
2. Click **Event Types** in the event builder menu, then drag a green event block onto the workspace.
3. Select the event's **Severity**: None, Low (alert), or High (Error).

NOTE: For EcoStruxure™ Facility Expert users, this field corresponds to the severity level in EcoStruxure™ Facility Expert.

4. Click **Event Conditions** in the event builder menu, and drag a conditions block into the "when" space, until it snaps into place.



5. Define the **Event Conditions**.
 - a. Select the device and topic.
 - b. For a Boolean event, select a Boolean value: Has changed, True, or False.
 - c. For a threshold or pickup/dropout event, select an operator (=, <, or >) and enter a pickup value. Enter a dropout value if applicable.
6. If the event has more than one condition, add up to two more conditions as described above. Join more than one condition with the "and" logic block.

NOTE: You must choose the same device for each condition in an event.
7. Click **Actions** in the event builder menu, and drag an action block into the "do" space.
8. Drag any unused blocks to the trash can in the bottom right corner.
9. Enter a name, then click **Save changes**.

NOTE: You should refer to the EcoStruxure Facility Expert commissioning guide for best practices when creating or editing custom events which will be sent to Facility Expert.

Editing or Deleting a Custom Event

You can modify or remove events from the **Custom Event Library**.

1. Click **Settings > Events > Custom Events**.
2. Click the event name.
3. Either edit the event block and click **Save changes**, or click **Delete** to remove the event from the **Custom Event Library**.

Related Topics

- Com'X 210 Troubleshooting

Copying an Event

You can create a new event from an existing event.

1. Click **Settings > Events > Custom Events**.
2. Click the existing event name.
3. Click on the green event block in the workspace, then press CTRL+C.
4. Click **Cancel** to return to the **Custom Event Library**.
5. Click **New Custom Event**.
6. Click inside the workspace, then press CTRL+V.
The event block is pasted into the workspace.
7. Edit the device, topic, or values, then click **Save changes**.

Com'X 210 Communications

IPv4 Address Settings

The Com'X supports three different operating modes for assigning the IP address.

These modes are:

- Static IPv4
- DHCP client
- DHCP server

Static IP Settings

In the Com'X, you can define the IPv4 addresses of the Ethernet interface, subnet mask, and default gateway.

These settings must be consistent with the network policy of the site. The IT administrator of the site should be contacted to provide this information.

Setting up a fixed address as a DHCP Client

You can configure the Com'X to have a fixed DHCP address when it is a DHCP client.

You can configure the Com'X so that the IPv4 address is automatically set by the facility DHCP server. The IT administrator of the site can be asked to configure the DHCP server to systematically assign the same IPv4 address to the Com'X.

1. Provide the local IT manager with the MAC address of the Com'X Ethernet port 1.

The address can be found on the label on the front face of the device or in the **About** page.

2. Ask the IT manager to provide a fixed IPv4 address so that the same IP address is always assigned to the Com'X.

The IP address is to be given by the IT manager.

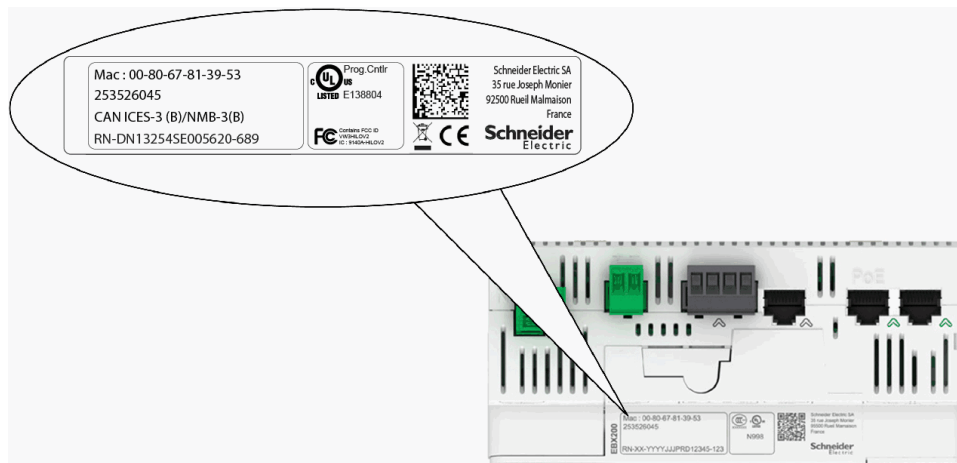
3. Write down the IPv4 address:

- on the label sheet provided with the Com'X. This sheet can be adhered inside the cover.

4. Check that the IT manager has added the Com'X to the DHCP server.

It is also possible to log in by entering the IP address provided by the IT manager in the address bar of the browser.

This graphic shows the MAC address on the label of the Com'X:



Related Topics

- Selecting a Network Configuration

DHCP Server Over Ethernet Port

You can configure the Com'X so that it assigns IP addresses to the network.

In that case, the Com'X configures its Ethernet interface Eth2 with the IP address 10.25.1.1.

The Com'X also starts an internal DHCP server. It enables you to assign automatically an IP address, consistent with its own address, to any devices connected to the same network and configured to operate as DHCP clients.

IP addresses assigned by the Com'X are in the subnetwork 10.25.1.0/24 (starting from 10.25.1.65, 10.25.1.66, and so on). The Com'X has no routing capabilities. As a result, no Default Gateway nor Domain Name Server are sent by this DHCP server.

The IT administrator of the site should be contacted to confirm that the network where the Eth2 interface of the Com'X is connected:

- is separated from the rest of the site network installation.
- does not disturb another DHCP server.

DHCP Server Over Wi-Fi

When a Wi-Fi key is connected to the Com'X, you can configure the Com'X so that it creates a Wi-Fi access point.

In that case, the Com'X creates a Wi-Fi network with an SSID using the same name as the Com'X but without any access restriction (no WEP nor WPA authentication) in this mode. The Com'X configures its Wi-Fi interface with the IP address 10.25.2.1.

The Com'X also starts an internal DHCP server on this Wi-Fi interface. It enables you to assign automatically an IP address, consistent with its own address, to any Wi-Fi devices that are configured to operate as DHCP clients.

IP addresses assigned by the Com'X are in the subnetwork 10.25.2.0/24 (starting from 10.25.2.65, 10.25.2.66, and so on). The Com'X has no routing capabilities. As a result, no Default Gateway nor Domain Name Server are sent by this DHCP server.

Remote Access with Windows Operating Systems

You can remotely access the Com'X by using an IP address under Windows XP.

The IT administrator should be requested to provide a fixed IP address to assign systematically the same IP address to the Com'X.

With Windows, the Com'X is accessible under Windows Explorer when connecting the PC to the same LAN. It is not necessary to know the IP address.

Related Topics

- Accessing Through the Ethernet Port With Windows

Modbus TCP Access

The Com'X acts as both a Modbus TCP gateway and a Modbus device by using the internal Modbus TCP server.

Modbus TCP Gateway

NOTE: Modbus is not a secure protocol. Disable the Modbus ports for security purposes. If Modbus access is required, Schneider Electric strongly recommends using Modbus IP filtering feature for added security.

The Com'X acts as a Modbus gateway for wired or wireless Ethernet communications from an upstream PC to Ethernet devices and field instruments on the downstream network. This capability allows the user of local or cloud-based monitoring software to access information from devices for data collection, historical trending, analysis, and other functions.

Accessing the Internal Modbus Slave Device

The internal Modbus TCP server allows reading the digital input and analog input values of the Com'X via various Modbus registers. These registers can be read using Modbus slave ID 255.

After you configure the Com'X inputs in **Device Settings**, values are accessible through the gateway. The register values can also be viewed in the **Measurements Table** tab for measurements selected for logging.

The internal Modbus TCP server is active when Modbus TCP/IP communications is enabled in **Firewall Management**.

Companion Software Modbus TCP/IP Server Function

Downstream Modbus devices can be accessed from an upstream PC running a software application. Recommended software applications offered by Schneider Electric include:

- Remote Setting Utility software for Masterpact and Compact NSX
- EcoStruxure™ Power Monitoring Expert software.

Related Topics

- Firewall Management
- Modbus Register Mapping
- Selecting Measurements to Log or Publish

Modbus Gateway Settings

Modbus Gateway Settings allows you to customize network settings for your specific environment.

The defined parameters apply to both Ethernet ports.

Serial port

Setting	Description	Options
Transmission Mode	Used to select how data is transmitted over a serial connection.	RTU, ASCII Default: RTU
Silent Interval Extension (ms)	Allows the silent interval used to signify the end of a Modbus RTU packet to be extended beyond the 3.5 characters defined by the standard.	0–10 ms Default: 5 ms
Delay Between Frames (ms)	Defines the minimum silent time between the end of a received response and the beginning of a new request on the serial line.	0, 10, 20, 30, 40, 50, 60, 70, 80, 90, 100 Default: 50 ms

TCP/IP Server

Setting	Description	Options
Enable Server Connection Idle Time	Enables a timer that closes the Modbus TCP/IP connection after a specified amount of idle time.	Yes, No Default: No
Server Connection Idle Time	Length of time after which a TCP/IP connection is closed.	1–65535 seconds
Enable Modbus TCP/IP Proxy	Setting that determines if Modbus TCP/IP messages from remote clients will be routed to remote Modbus TCP/IP devices that are defined in the Com'X.	Yes, No Default: Yes
Enable Serial Modbus Broadcasts	Forwards received Modbus broadcast messages to the slave devices connected to the local serial port.	Yes, No Default: No

TCP/IP Client

Setting	Description	Options
Client Connection Timeout (seconds)	Amount of time the Com'X will wait for a remote Modbus TCP/IP device to respond to a Modbus TCP/IP connection request initiated by the Com'X.	.1–10 seconds Default: 2
Client Message Timeout (seconds)	Amount of time the Com'X will wait for a remote Modbus TCP/IP device to respond to a Modbus TCP/IP request initiated by the Com'X.	1–20 seconds Default: 3

Configuring the Modbus Gateway

You can configure the Com'X Modbus gateway settings.

NOTICE
<p>IMPAIRED NETWORK PERFORMANCE</p> <p>Only qualified workers should modify the Modbus gateway settings. Such modifications should be performed only after reading about and understanding the Modbus gateway settings.</p> <p>Failure to follow these instructions can impair network performance.</p>

1. Click **Settings > Communication > Modbus Gateway**.

2. Select the required **Transmission Mode**, **Silent Interval Extension**, and **Delay Between Frames** for the serial port.
3. Select **Yes** or **No** to **Enable Server Connection Idle Time**, **Enable Modbus TCP/IP Proxy**, and **Enable Serial Modbus Broadcast** for the TCP/IP server.
4. Enter a **Server Connection Idle Time** in seconds, if enabled.
5. Select the required TCP/IP client values for **Client Connection Timeout** and **Client Message Timeout**.
6. Click **Save changes**.

Local ID Settings and Device IDs

In order for an external Modbus TCP/IP client to access a device connected to the Com'X, each device must have a unique ID, or **Local ID**. The **Local ID** is automatically assigned whenever a device is created and is associated with a device's **Slave ID**.

The **Slave ID** is either

- the configured Modbus ID of any device connected to the RS485 serial port,
- the configured Modbus ID of a connected Modbus TCP/IP device, or
- the ID used by a Modbus TCP/IP gateway that connects a device to an Ethernet network.

You can change the **Local ID** in **Settings > Communication > Modbus Gateway > Device IDs**. The **Local ID** must be unique and can only be changed if data logging is disabled for the device being updated.

The **Devices** page also provides the following information for each device:

- **Slave ID**
- **Connection**: "Serial Port," IP address for remote devices, or Zigbee ID
- **Device Type** as defined in **Device Settings**

Related Topics

- Starting the Data Logging

Configuring Modbus TCP/IP Filtering

This function allows the administrator to create a whitelist and assign the level of access IP addresses have to the Com'X and its downstream devices.

When enabled, the default access level is **Read** for any Modbus TCP/IP client not in the filtered list. Setting the **Default Access** field to **None** blocks all Modbus TCP/IP clients not in the filtered list.

1. Click **Settings > Communication > Modbus TCP/IP Filtering**.
2. Click **Yes** to enable filtering.
3. In the Whitelist column, enter the IP address you want to filter on.

NOTE: An empty octet field is treated as a wildcard. Empty fields must begin with the least significant octet and be contiguous. The most restrictive filter is applied in cases of contradiction.

4. Select the access level: **None**, **Read**, or **Full**.
5. Optionally, you can edit the **Default Access**: **Read** or **None**.
6. Click **Save changes**.

Modbus Serial Port

The RS-485 serial line standard is an industrial standard.

If configured correctly, it can potentially reduce transmission errors even in an environment with electrical disturbances. This section describes the serial line properties of the local Modbus/RS-485 network controlled by the Com'X.

Modbus Serial Port Settings

The Com'X is the master of the Modbus serial line. All the other devices connected to this serial line must be configured as Modbus slaves.

The slave device settings such as **Baud rate**, **Parity**, and **Number of stop bits** must match the Com'X. These settings are set by using the front display of each device.

This table describes the Modbus serial port settings:

Field	Description	Options
Baud rate	Defines the speed of the serial line.	1200, 4800, 9600, 19200, 38400, 57600, and 115200 Bauds. ⁽¹⁾ The factory setting is 19200 to match the values of Schneider Electric equipment. Most third-party Modbus equipment supports this Baud rate.
Parity	Defines the parity bit of the transmitted bytes.	<ul style="list-style-type: none"> • odd ⁽²⁾ • even • none The factory setting is even to match the values of Schneider Electric equipment. Most third-party Modbus equipment supports this parity setting.
Number of stop bits	Defines the number of stop bits transmitted between 2 bytes.	1 or 2 The factory setting is 1 to match the values of Schneider Electric equipment. Most third-party Modbus equipment supports this number of stop bits.
Timeout	Defines the time the Com'X has to wait before generating an error for an unanswered Modbus request.	100 to 10000 ms The factory setting is 1000 ms to match the values of Schneider Electric equipment.
Terminator resistance	Has a value of 120 Ω.	Yes or No Terminator resistance must be activated if the Com'X is located at the end of the Modbus bus. Not following this rule can result in communication interruption.
Serial line polarization	Has a value of 510 Ω.	Yes or No It is recommended that the master polarizes the line. No other slave device has to support line polarization resistances or to activate serial line polarization resistances.
<p>⁽¹⁾ A high Baud rate value reduces response time but may be more sensitive to disturbance. In case of disturbance, check the impedance on the serial line before reducing the Baud rate.</p> <p>⁽²⁾ Even or odd settings enable a byte integrity check that may detect a transmission error at byte level. At this level, there is no advantage to use this check: Modbus protocol provides a CRC check that keeps the integrity of the whole Modbus frame.</p>		

Configuring Modbus Serial Port Settings

You can configure Modbus serial port settings on your Com'X.

NOTICE

IMPAIRED NETWORK PERFORMANCE

Only qualified workers should modify the Modbus gateway settings. Such modifications should be performed only after reading about and understanding the Modbus gateway settings.

Failure to follow these instructions can impair network performance.

1. Click **Settings > Communication > Modbus Serial**.
2. Select the required value in the **Baud rate** drop-down list.
3. Select the required value in the **Parity** drop-down list.
4. Select the required value in the **Number of stop bits** drop-down list.
5. Select the required value in the **Timeout** drop-down list.
6. Select **Yes** in the **Terminator resistance** field if the bus is terminated at its end
7. Select **Yes** in the **Serial line polarization** field if no other device in the line is providing polarization.
8. Click **Save changes**.

Advanced Ethernet Settings

Advanced Ethernet Settings allow you to customize network settings for your specific environment.

The defined parameters apply to both Ethernet ports.

Setting	Description	Options
Time to Live	Identifies the number of routers a TCP packet can pass before it is discarded.	1-255 hops Default: 60 hops
Enable TCP Keep Alive	A keepalive is a message sent to check that the link between the Com'X and its connected host is operating, or to prevent this link from being broken.	Yes or No Default: Yes
Time	Elapsed time between two successive keepalive retransmissions, if acknowledgment to the previous transmission is not received.	1-7200 seconds Default: 30 seconds

Configuring Advanced Ethernet Settings

You to customize network settings for your specific environment by configuring the advanced Ethernet settings.

NOTICE

IMPAIRED NETWORK PERFORMANCE

Only qualified workers should modify the advanced Ethernet settings. Such modifications should be performed only after reading about and understanding the advanced Ethernet settings.

Failure to follow these instructions can impair network performance.

1. Click **Settings > Communication > Advanced Ethernet Settings**.
2. Enter the **Time to Live**.
3. **TCP Keep Alive** is enabled by default.
 - enter the keep alive time, or
 - click **No** to disable **TCP Keep Alive**.
4. Click **Save changes**.
To return to default values, click **Defaults**.

ZigBee Network Settings

You can add up to 20 ZigBee devices to the Com'X (Zigbee dongle EBXA-USB-Zigbee defines the number of ZigBee devices allowed).

ZigBee is a wireless networking standard for remote control and sensor applications.

Related Topics

- Discovering Zigbee Devices

Creating a ZigBee Network for the First Time

Schneider Electric provides accessories to mount the ZigBee key outside the cabinet. **NOTE:** Power to the Com'X must be removed before the Zigbee dongle is inserted or removed from the Com'X.

For information, see the ZigBee Instruction Sheet. Use this procedure when a ZigBee network has never previously been created for the Com'X.

NOTICE

UNINTENDED EQUIPMENT OPERATION

Do not mount the ZigBee key inside the cabinet or switchboard when using the High power transmission setting.

Failure to follow these instructions can result in equipment damage.

1. Power off the Com'X.
2. Plug the ZigBee key into one of the USB ports in the Com'X, or connect it to the Com'X through a USB extension cable.
3. Power on the Com'X and wait for its power LED to turn green.
 - NOTE:** The ZigBee key firmware is deployed with the Com'X firmware. The Com'X automatically updates the firmware if a newer version is available.
4. Log in to the Com'X, and then select **Settings > Communication > ZigBee Settings**.
The ZigBee Settings screen is displayed.
5. In the **Activate ZigBee** field, select **Yes**.
6. (Optional) In the **Channel** field, select a ZigBee channel. If you leave the setting as –, the Com'X scans all available channels and automatically selects a channel for the ZigBee network. The channel with strongest signal is usually selected.

7. In the **Transmission power** field, select one of the following options:
 - **Standard power**: Select this option when the ZigBee key and all ZigBee devices are in the same switchboard or cabinet.
 - **High power**: Select this option when the ZigBee key is connected to the Com'X through a USB extension cable. You are asked to confirm that the ZigBee key is outside the switchboard or cabinet. Click **OK** to confirm.
8. Click **Save changes**.

The setup takes about 60 seconds. When the network starts, the **ZigBee status** shows that the network is ready to be used, and the ZigBee key LED flashes green.

You can now use the ZigBee discovery function to connect devices to the network.

Related Topics

- Discovering Zigbee Devices

Stopping and Restarting a ZigBee Network

Use this procedure to stop and restart a ZigBee network so that you can change the network settings or perform maintenance.

1. Log in to the Com'X, and then select **Settings > Communication > ZigBee Settings**.
The **ZigBee Settings** screen is displayed.
2. In the **Activate ZigBee** field select **No**, and then click **Save changes**.
The ZigBee status shows that no network is defined. You can now perform maintenance or change the network settings.
3. In the **Activate ZigBee** field, select **Yes**.
4. In the **Create New ZigBee Network** field, leave the value as **No**.
5. In the **Transmission power** field, select one of the following options:
 - **Standard power**: Select this option when the ZigBee key and all ZigBee devices are in the same switchboard or cabinet.
 - **High power**: Select this option when the ZigBee key is connected to the Com'X through a USB extension cable. You are asked to confirm that the ZigBee key is outside the switchboard or cabinet. Click **OK** to confirm.
6. Click **Save changes**.

The setup takes a few seconds. When the network starts, the ZigBee status shows that the network is ready to be used, and the ZigBee key LED flashes green.

Recreating a ZigBee Network

Use this procedure to change the channels on a ZigBee network that has already been created for the Com'X.

When you perform this procedure, all equipment that is connected to the ZigBee network is disconnected. You must use the ZigBee discovery function to reconnect devices to the network.

1. Log in to the Com'X, and then select **Settings > Communication > ZigBee Settings**.
The **ZigBee Settings** screen is displayed.
2. In the **Activate ZigBee** field select **No**, and then click **Save changes**.
The ZigBee status shows that no network is defined. You can now perform maintenance or change the network settings.

3. In the **Activate ZigBee** field, select **Yes**.
4. In the **Create New ZigBee network** field, select **Yes**.
5. Follow step 6 through to the end of *ZigBee Network Settings* to complete the setup.

Related Topics

- [ZigBee Network Settings](#)
- [Discovering Zigbee Devices](#)

Com'X 210 Device Settings

Device Settings Overview

The **Device Settings** interface defines the devices connected to the energy server, for example, Ethernet gateways, Modbus meters, pulse meters, or analog sensors.

⚠ WARNING

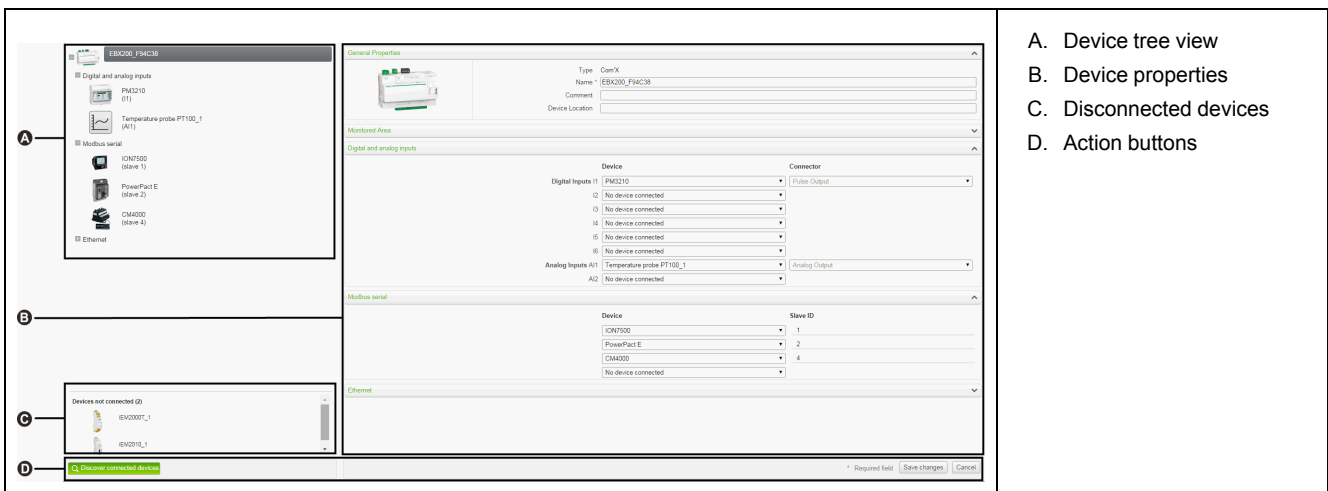
INACCURATE DATA RESULTS

Do not incorrectly configure the software, as this can lead to inaccurate reports and/or data results.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

The Com'X supports up to 64 devices. Devices supported by the Com'X are described in the firmware release package. You can also create custom models that are based on custom model types, which have been added to the **Custom Library**.

This graphic shows the **Device Settings** interface:



- A. Device tree view
- B. Device properties
- C. Disconnected devices
- D. Action buttons

Device Tree View

The device tree view represents the communication architecture of the installation. The Com'X is always at the top of the tree. Devices are grouped by their connection interfaces: Ethernet ports, Modbus port, digital inputs, and analog inputs.

For digital and analog inputs, each device appears with its **Name** and the input number to which it is connected.

The multiple outputs of a main meter (for example, kWh, kVARh pulses) can be connected to several digital inputs.

For Modbus TCP/Modbus serial line gateway, each device appears with its **Name** and its **Slave ID**.

Click a device to display its properties in **General Properties**.

Disconnected Devices

This area displays the devices that are not connected to the installation. Measurements from these devices are not logged.

Device Properties

For a selected device, this zone allows you to:

- define some metadata such as the name, the physical location and, for a meter, the commodity, the energy usage, and the area in the building that is being monitored.
- set up or modify settings such as: the pulse weight for a pulse meter, the slave ID for a Modbus meter, the IP address for a gateway, and the measurements to be logged and published to the selected hosted platform.
- connect and disconnect downstream devices in the drop-down lists when the selected device allows it. Each connection type has its own area. Only devices that can be connected to this type are listed.

Action Buttons

This table describes the interface buttons:

Button	Action	Availability
Discover connected devices	Launches a Modbus device discovery and automatically retrieves devices that are connected downstream.	Enabled when the Com'X or an Ethernet gateway is selected.
Delete	Removes the selected device. Deletes or moves the devices connected downstream to the Disconnected devices area.	Enabled when a device is selected.
Save changes	Validates the modifications.	Disabled when: <ul style="list-style-type: none"> • there is no change in the web page. • mandatory fields are left blank. Those fields are highlighted in red. • inappropriate characters are entered in a field. This field is highlighted in red.
Cancel	Cancels the modifications to return to the last saved settings.	–
Replace	Allows you to swap out a device for a different device.	–

Common Properties

All devices have **General Properties** and **Monitored Area**.

General Properties

All devices have a set of general properties that includes **Type**, **Name**, **Comment**, **Commodity**, and **Device Location**.

This table presents the general properties of the Com'X:

Field	Description	Comments
Type	Corresponds to the device type that is selected.	This field is automatically assigned by the Com'X and cannot be modified.
Name	Corresponds to the name of the device.	This field must not include the following characters: /:*?< > or space.

Field	Description	Comments
Comment	Allows you to type additional information.	-
Commodity	Corresponds to the type of measurements.	This field is available only for meters or sensors. The logging interval of measurements is set according to the value defined in Data Logging.
Device location	Defines where the device is physically installed.	For example: <ul style="list-style-type: none"> main low voltage switchboard for an electric meter boiler room for a gas meter outdoor north front for a temperature probe

The device name is associated with a measurement to create the meter in Energy Operation. For example, the active energy measurement for a PM3250 named Ventilation Q01 creates a meter Ventilation Q01_Active Energy.

NOTE: Energy Operation retrieves this information from the Com'X to create the metering site architecture.

Monitored Area

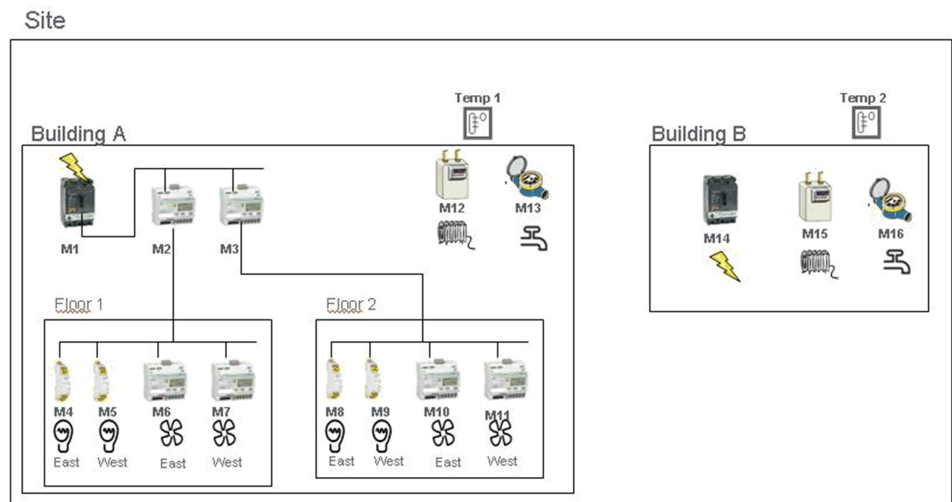
The monitored area enables you to define the building area measured by the meter or sensor. A site can be made up of several buildings. Each building can have several floors. Each floor can be made up of several zones. The site topology is defined by entering values in the **Building**, **Floor**, and **Zone** fields.

The **Usage** field helps identify the device in the **Measurement Table**. You can either use a predefined name or customize your own.

To type a floor name, you must enter a building name first. To type a zone name, you must enter a floor name first.

Example: Monitored Area

This example describes how to define the name of the buildings, floors, zones, and usage for the meters or sensors of a site made up of 2 buildings:



This table shows naming examples for the different fields of the **Monitored Area** collapsible menu:

Meter/ Sensor	Device Location	Monitored Area			Usage
		Building	Floor	Zone	
M1	Main switchboard	Building A	–	–	Main meter
M2	Main switchboard	Building A	1st	–	Submeter
M3	Main switchboard	Building A	2nd	–	Submeter
M4	Distribution board 1	Building A	1st	East	Lighting
M5	Distribution board 1	Building A	1st	West	Lighting
M6	Distribution board 1	Building A	1st	East	Ventilation
M7	Distribution board 1	Building A	1st	West	Ventilation
M8	Distribution board 2	Building A	2nd	East	Lighting
M9	Distribution board 2	Building A	2nd	West	Lighting
M10	Distribution board 2	Building A	2nd	East	Ventilation
M11	Distribution board 2	Building A	2nd	West	Ventilation
M12	Boiler room	Building A	–	–	Heating
M13	Outdoor	Building A	–	–	Main meter
Temp1	Outdoor north front	Building A	Outdoor	–	Other
M14	Main switchboard	Building B	–	–	Main meter
M15	Boiler room	Building B	–	–	Heating
M16	Outdoor	Building B	–	–	Main meter
Temp2	Outdoor north front	Building B	Outdoor	–	Other

Related Topics

- Data Logging

Adding a Downstream Device

Add downstream devices to your Com'X.

1. Click the **Device Settings** main tab.
2. In the device tree view, click the upstream device to which the downstream device is connected.

For example, select the Com'X to connect a device to the Com'X.

3. Click the collapsible menu that corresponds to the type of device to be connected:
 - **Digital and analog inputs** collapsible menu for devices connected to the Com'X digital and analog inputs, for example, pulse meters or analog sensors.
 - **Modbus Serial** collapsible menu for a Modbus device. Modbus can also be automatically discovered with the **Discover connected devices** button.
 - **Ethernet** collapsible menu for a Modbus TCP/Modbus serial line gateway or IP-enabled device.
4. Select **Create a new device** in the **Device** drop-down list.
5. Select the type of device to be created in the **Device Type** drop-down list.

NOTE: Only the devices that can be connected to this interface are listed. You cannot modify the device type after the device has been created.
6. Configure the device. Refer to the sections that correspond to the device category.
7. Click **Create** and the device appears in the device tree view.

Related Topics

- [Discovering Connected Devices](#)

Modifying a Device

You can modify device settings.

1. Click the **Device Settings** main tab.
2. Click the device in the device tree view.
3. Modify the settings in the required collapsible menu.
4. Click **Save changes**.

NOTE: The device type cannot be modified. If a device is incorrectly configured, delete the device and create a new one.

Disconnecting a Device

There is a procedure to disconnect a device from an upstream device. When disconnected, the device does not appear in the **Measurements Table**. No measurement from this device is sent to the hosted platform. The device is still available in Real Time Data.

1. Click the **Device Settings** main tab.
2. Click the parent device in the device tree view.
3. Select **No device connected** in the **Connected to** drop-down list.

The device appears in the **Devices not connected** collapsible menu under the device tree view.
4. Click **Save changes**.

Reconnecting a Device

You can reconnect a device from an upstream device.

1. Click the **Device Settings** main tab.

2. In the device tree view, click the upstream device to which the downstream device must be connected.
For example, select your Com'X to reconnect a downstream device to the Com'X.
3. In the **Digital and analog input** collapsible menu, select the device to be reconnected on the required digital input.
4. Click **Save changes**.

Replacing a Device

You can replace an existing device with another device of a similar type.

This procedure can be used to replace a standard device with a custom device without losing the properties of the original device.

1. Click the **Device Settings** main tab
2. In the device tree view, click the upstream device to which the device to be replaced is connected.
For example, select the Com'X to replace a device connected to the Com'X.
3. Click the collapsible menu that corresponds to the type of device to be replaced:
 - **Digital and analog inputs** collapsible menu for devices connected to the Com'X digital and analog inputs (for example, pulse meters or analog sensors).
 - **Modbus Serial** collapsible menu for a Modbus device. Modbus can also be automatically discovered with the **Discover connected devices** button.
 - **Ethernet** collapsible menu for a Modbus TCP/Modbus device.
 - **ZigBee**: Replacing a ZigBee device launches the ZigBee Devices discovery function. The discovery is stopped when the first ZigBee device is found. If several ZigBee devices are near to each other, the first ZigBee device found might not be the one you want. In this case, repeat the procedure.
4. Select the device you want to replace. Select a replacement device that is of the same (or similar) type and that supports the same published measurement data as the original device.
5. Click **Replace** at the bottom of the **Device Settings** main tab.
The **Replace device** dialog opens.
6. In the **Replace device** dialog, select the replacement device type and click **Replace**.
When you replace an existing device, the replacement device will display the previous device **Name** unless you edit the name.
7. If necessary, edit the **Name** and other settings for the replacement device, then click **Save changes** at the bottom of the **Device Settings** main tab.

Related Topics

- [Discovering Zigbee Devices](#)

Deleting a Device

You can delete devices from the Com'X.

1. Click the **Device Settings** main tab.

- Click the device to be deleted in the device tree view.

NOTE: Do not deactivate the ZigBee network when removing ZigBee devices. Do not restart the Com'X until the Zigbee device has left the network. This can be confirmed by information in the maintenance log.

- Click **Delete** to confirm the deletion of the device.

Measurement and Metadata Exported Per Hosted Platform

The exported data varies per hosted platform.

Measurement/ Metadata	Energy Operation	CSV Export	Digital Service Platform
Customer ID	–	–	–
Site name	X	X	X
Device name	X	X	X
Selected measurement	X	X	X
Commodity	X	–	X
Monitored area parameters			
Building	X	–	X
Floor	X	–	X
Zone	X	–	X
Usage	X	–	X

Selecting Measurements to Log or Publish

It is important to consider how much data is being logged across all devices when selecting the logging interval and number of topics to log.

Logging too many topics per interval may affect your Com'X performance, including degraded web page response and missed logging intervals. For example, for a logging interval of less than five minutes, it is recommended that you log no more than 8 devices with 50 total topics.

- Click the **Device Settings** main tab.
- Click the meter or sensor in the device tree view.
- Click the **Measurements Table** main tab.
- Select the **Log** check box of the measurement to be logged.
- Select the **Publish** check box to send the data to the selected publishing platform (optional).
- Click **Save changes**.

Related Topics

- Firewall Management
- Modbus Register Mapping


Factory Settings of the Device Measurement Table

Some measurements are selected by default in the device measurement table.

Device Type	Measurement
Pulse meter	<ul style="list-style-type: none"> • Index
Contactor/Impulse relay	<ul style="list-style-type: none"> • Status • Run hours
Electric utility meter	<ul style="list-style-type: none"> • Active energy • Reactive energy
Power meter	<ul style="list-style-type: none"> • Active energy • Reactive energy
Resistance Temperature Detector (RTD)	Temperature
0–10 V/4–20 mA analog sensors	Analog value

Measurement Table Notification Icons

The Com'X displays a notification icon when no measurement can be retrieved from a device.

Icon	Description
	This icon indicates that no measurement can be retrieved from this device.

Built-In Pulse Meters

Built-in pulse meters have specific measurement properties.

Measurement Properties

This table describes the measurement properties of a built-in Schneider Electric pulse meter:

Field	Description	Comment
Connected To	Displays the upstream device and the digital input number to which the device is connected. The digital input number can be modified. Only the available digital inputs of the upstream device are listed.	The device can be disconnected by selecting No device connected in the list of upstream device. From this list, it is not possible to change from 1 upstream device to another.
Pulse weight	The active energy counter increases by this value each time a pulse is received. The list is restricted to the values that correspond to the selected meter type.	The value cannot be modified if there is only 1 possible pulse weight, for example with the iEM2000T meter. ⁽¹⁾
Offset	Sets an offset for the active energy. The value can be positive or negative.	Enables you to start the counter with the value that can be read on the meter display.
Upper Range	Defines when the active energy counter rolls back to zero.	The counter sets back to zero when it reaches the entered value.

⁽¹⁾ Refer to the specific pulse meter documentation for further information.

Measurement Table

The active power is calculated according to the frequency of received pulses.

Custom Pulse Meter

You can add a pulse meter that is based on a custom pulse meter model.

Before adding a custom device, you first need to create the custom model in the **Custom Library**.

Related Topics

- Custom Models

Resistance Temperature Detectors

The Com'X supports resistance temperature detectors connected to its analog inputs.

Measurement Properties

The Pt100/Pt1000 Resistance Temperature Detectors (RTD) are sensors used to measure temperature by correlating the resistance of the RTD element with temperature.

The RTD can only be connected to the analog inputs of the Com'X.

The temperature range is from -50 °C (-58 °F) to +104 °C (219 °F).

When connecting an RTD probe to the Com'X, there are no specific parameters to configure.

Measurement Table

By default, the temperature is logged and published to the selected platform.

Custom Analog Devices

You can add an analog device that is based on a custom analog device model.

Before adding a custom device you first need to create the custom model in the **Custom Library**.

Related Topics

- Custom Models

Discovering Connected Devices

With the Modbus discovery function, the Com'X can discover the devices that are locally connected to their Modbus serial port and downstream Modbus TCP/Modbus serial line gateways.

1. Click the **Device Settings** main tab.
2. Click the Com'X in the device tree view. Or, click the gateway in the device tree view to discover only the downstream devices connected to a gateway such as an EGX.
3. Click **Discover connected devices** to open the **Discovery** window.
4. Enter a **Slave ID min** and **Slave ID max**.

The default range is 1 to 10, and the allowable range is 1 to 247.

- Click **Start** to discover the devices.

Discovered devices are listed in the **Modbus Discovery** window. Click **Stop** if you want to stop the **Discovery** process.

- Deselect any devices you do not want to add, then click **Create**.

The **Modbus Discovery** window closes and all the discovered devices appear in the device tree view as follows:

- If a device was created using a built-in model, the application automatically associates the device with the appropriate model.
- If a device was created from a custom model that was added to the Custom Library, the application associates the device with the first model in the custom device list. In this case, you need to select the appropriate custom model for the device in the device type list.

Related Topics

- Replacing a Device
- Discovering Zigbee Devices
- Modifying a Device

Discovered Modbus Device Status

Discovered devices can have different status.

Message	Description
OK	The device is discovered and supported by the Com'X..
This device is already connected	The device has been discovered from a previous Modbus discovery or by manual entry. It is supported by the Com'X.
Unknown device	The device has been discovered but it is not supported by the Com'X. This occurs if the device is a custom device, and no custom models have been created in the Custom Library .
No device discovered	No device is connected to this Modbus address (slave ID).

Adding a Modbus Device Manually

Modbus devices that are not connected cannot be discovered, but they can be added manually using the following procedure.

You can add either a built-in Modbus device or a custom Modbus device that you have previously created in the **Custom Library**.

- Click the **Device Settings** main tab.
- Select the upstream device with a Modbus serial port in the device tree view. For example, the Com'X must be selected to connect a Modbus device to the Com'X.
- Select the **Modbus Serial** collapsible menu. Click the header to expand the **Modbus Serial** collapsible menu.
- Click **Create a new device** in the **Device** drop-down list.
- Select a **Device Type** in the drop-down list.

NOTE: Only the devices that can be connected to a Modbus serial port are listed.

- Type the **Slave ID** in the **Configuration** collapsible menu.
- Click **Create** and the device appears in the device tree view.

Related Topics

- Common Properties

Modbus Meter Measurements

The Com'X retrieves available measurements from Schneider Electric Modbus meters.

Available measurements include:

- total active energy
- active energy per phase
- total reactive energy
- reactive energy per phase
- total apparent energy
- active power
- reactive power
- apparent power
- phase-neutral voltages
- phase-phase voltages
- phase and neutral currents
- frequency
- power factor
- total harmonic distortion

Additional Measurements for Built-in Devices

For additional measurements, you must create a new model of the device based on an existing built-in device, and then customize it to your needs. Refer to the data sheet of the specific meter to identify which Modbus registers correspond to the measurement required.

Related Topics

- Creating a Custom Model
- Replacing a Device

Connecting Devices to WT4200 Modbus Receiver

The WT4200 Modbus Receiver is a Modbus interface between the Com'X and the WT4200 radio transmitters.

Each transmitter is seen as a different channel for the WT4200 Modbus Receiver.

You must configure the WT4200 Modbus Receiver before adding it to the Com'X device list and connecting transmitters. WT4200 configuration determines to which channel the transmitter can be added. Refer to the *PowerLogic WT4100 series / WT4200 series long-range RF wireless devices user manual* for wireless receiver programming instructions.

⚠ WARNING

INACCURATE DATA RESULTS

The configuration in the Com'X must be consistent with the configuration in the WT4200 Modbus receiver.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

1. Click the **Device Settings** main tab.
2. Click the WT4200 in the device tree view.
3. In the **Channel** collapsible menu, select the channel (C1, C2, and so on) to which the device is connected. Click the header to expand the channel area.
4. Select **Create a new device** in the appropriate digital input dropdown list.
5. Select the type of device to be created from the dropdown list.
Only the devices that can be connected to this interface are listed. You may need to create your own custom device.
6. Configure the device. Refer to the sections that correspond to the specific device category.
7. Click **Create** and the device appears in the device tree view downstream from the WT4200.

Related Topics

- Com'X 210 Custom Library

Connecting Devices to Smartlink

The Smartlink Modbus and Smartlink SI-B are communication system modular interfaces that are used to remotely meter, monitor, and control the essential functions of one or more distribution panels. The Smartlink interfaces provide multiple digital channels supporting two digital inputs and one digital output. The Smartlink Modbus supports eleven digital channels. The Smartlink SI-B supports seven digital channels.

Prior to creating the Smartlink device on the Com'X it is recommended to configure the Smartlink device inputs through the web interface or the **EcoStruxure Power Commission** tool.

1. Click the **Device Settings** main tab.
2. Click the Smartlink device created earlier in the device tree view.
3. Click the **Channel** Accordion which the device is connected.
4. Click input 1 or input 2 drop-down under **Devices** .

NOTE: Input 1 drop-down is labeled **CX_I1**, and input 2 drop-down is labeled **CX_I2** where 'X' is the channel number.

5. Select **Create a new device** in the selected input drop-down list.
6. Select the type of device to be created from the drop-down list.

NOTE: Only the devices that can be connected to this interface are listed: Schneider Electric pulse meters, utility meters, contactors, impulse relays, and Acti 9 auxiliary devices. You may create your own custom device if it is not listed.

The following Acti 9 Auxiliary devices utilize both channel inputs and must be created on input 1: Acti9 OFSD24, Acti9 OF24, Acti9 SD24, Acti9 Reflex iC60, Acti9 RCA iC60, Acti9 iACT24, and Acti 9 iATL24.

7. Configure the device.
8. Click **Create** and the device appears in the device tree view downstream from the Smartlink.

NOTE: To ensure values get reported and displayed correctly, match the configuration on both physical Smartlink device and the device created on Com'X. Values displayed as '- -' in the **Measurements Table** page indicate a configuration mismatch or a communication error. This applies to the Acti 9 pulse meters and wired auxiliary devices.

Built-in Ethernet Devices

You can add built-in Ethernet devices to your system.

In the system, you can add these devices:

- Modbus TCP/IP to Modbus serial line gateways. These gateways are used to collect data from serial devices.
- Modbus TCP/IP meters.
- Custom Modbus TCP/IP to serial gateway used to collect data from serial devices.

NOTE: To collect data from a PM800 series meter with an Ethernet card and use this PM800 as a gateway, you must define 2 devices: the meter (for example, PM850ECC) and the gateway (PM8ECC Modbus gateway).

Ethernet Device Configuration Parameters

There are a set of parameters for an Ethernet device connected to the Com'X.

This table shows how to configure Ethernet devices:

Field	Description
Host	Defines the IP address of the device.
Port	Defines the port number. 502 is used for Modbus.
Slave ID	Gives the address only for Modbus TCP meters or devices.
Local ID	The address to use when accessing data from a device by an external client. The Local ID must be unique. This configuration parameter can only be changed if data logging is disabled for the device being updated.

Related Topics

- Starting the Data Logging

Custom Ethernet Devices

You can add an Ethernet device that is based on a custom Ethernet model.

Before adding a custom device, you first need to create the custom model in the **Custom Library**.

Discovering Zigbee Devices

With the ZigBee discovery function, the Com'X can discover ZigBee devices that are within range.

Do not launch the ZigBee discovery mode of several Com'X devices simultaneously. If you have two or more ZigBee networks in discovery mode, the ZigBee devices are installed randomly on these networks.

1. Click the Com'X in the device tree view.
2. Click **Discover devices** to open the **Discovery** window.
3. Select the communication protocol ZigBee.
4. Enter the Timeout time (in minutes).
5. Click **Start** to discover the devices.

In order to detect the ZigBee devices, you also need to activate the discovery mode on the different devices.

Discovered devices are listed in the **ZigBee Discovery** window. Click **Stop** if you want to stop the ZigBee Discovery process.

6. Close the ZigBee Discovery window.

All the discovered devices appear in the device tree view. A Local ID is automatically assigned whenever a device is created. You can change the Local ID in **Settings > Communication > Modbus Gateway > Device IDs**.

Related Topics

- ZigBee Network Settings
- Replacing a Device

Com'X 210 Measurements

Viewing the Measurements Table

The **Measurements Table** allows you to view all the meters and sensors of the system that log data. Only the data that has been selected for logging is present in the **Measurements Table**.

1. Click the **Measurements Table** main tab.
2. Select the required meters in the **Filter by commodity** field:
 - Click **All** to visualize all the commodities at the same time.
 - Click **None** to hide all the commodities at the same time.
 - Check the corresponding check box to view all the measurements of a commodity.
 - Uncheck the corresponding box to hide all the measurements of a commodity.

Com'X 210 Commissioning

Commissioning Overview

The **Commissioning** tab allows you to view configuration notifications and commission other features.

Commissioning allows you to:

- check that configuration is completed.
- start/stop data logging.
- send the metering architecture to Energy Operation. This option is available only if Energy Operation is selected as the publication platform.
- export the logged data manually to the selected hosted platform.
- start the periodic publication of data to the selected hosted platform.

Commissioning Interface

Use the commissioning interface to start data logging and publication.

This table shows commissioning fields:

Field	Description
Notifications	Displays the status of the configuration process. If any requested field or parameters are missing, a link to the corresponding tab is displayed. Click the link to be redirected to the tab.
Data logging	Displays a button to start data logging. The button is disabled if: <ul style="list-style-type: none"> • the configuration is not complete. • there is no selected data to be logged.
Topology ⁽¹⁾	Sends the metering architecture to Energy Operation. This creates the metering hierarchy in Energy Operation. This option is available only if Energy Operation is selected as the publication platform. If you do not send the topology to Energy Operation, all measurements will appear under the site named <i>Site Newmeters</i> .
Publication	Allows you to export the logged data manually to the hosted platform.
Status console	Displays the successive steps with the corresponding status when the publication is launched, from the construction of the data file to the delivery of the file on the database server. Refer to the maintenance logs if an error occurs during publication.
⁽¹⁾ If you change the topology of the Com'X or modify the Com'X configuration by adding some measurement values or meters after the first publication, do not use the Send Topology button. Contact local Schneider Electric technical support.	

Related Topics

- Logs

Starting the Data Logging

You need to start data logging on your energy server for it to log data.

Before you can log data, you must:

- complete configuration of the Com'X.
- configure the devices that you want to log data .
- select the data to be logged.

1. Click **Commissioning > Data Logging**.
2. Click **Start data logging**.

The date and time that logging is initiated are displayed.

To disable data logging, click **Commissioning > Data Logging > Stop data logging**.

Starting the Publication

Publication allows you to send data to the hosted platform at a specified frequency.

If you are publishing data to Energy Operation, you must send the topology to Energy Operation.

After you have configured devices for publishing:

1. Click the **Manual publication** button to send data to the hosted platform.
2. Click the **Start periodic publication** button to send data to the hosted platform according to the frequency set in **Publication settings**.

Com'X 210 Custom Library

Custom Models

The Com'X supports the use of custom models.

A custom model is any model other than a Built-in model from Schneider Electric. To use a custom model, you must first create a new custom model. A custom model can be:

- based on a pre-existing Schneider Electric model
- based on a previously created custom model
- an entirely new model

If you base a custom model on a pre-existing Schneider Electric model or a previously created custom model, the new model inherits the properties of the underlying model on which it is based. Inheritance simplifies the task of creating a new custom model, because you need only add or edit properties unique to the new custom model in order to create it.

Creating a Custom Model

To use a custom model, you must first create a new custom model.

1. Click the **Custom Library** main tab.
2. Click **+Create** on the lower left part of the page.
The **Create a custom model** dialog opens.
3. Enter the following settings:

Field	Setting
Select model type	Select a model type from the list. This selection determines the properties structure of the new custom model.
Create model	Select the basis for the new custom model: <ul style="list-style-type: none"> • New • Based on a Schneider Electric model • Based on a custom model
<base model type>	If you are basing the new custom model on an existing Schneider Electric model or a custom model, select the existing model on which the new model is based.
Model name	Enter the name of the new custom model, or accept the default name.
Default value of commodity	Select a default commodity the new model measures.
Default value of usage	Select a default value for how the new model is used

4. Click **Create**.

The dialog closes, and the newly created custom model properties page opens for initial configuration.

Modifying a Custom Model


You can modify the settings of an existing custom model.

1. Click the **Custom Library** main tab.

2. Display a list of existing models. Either:
 - Click **Models** in the navigation tree to display a list of all models, or
 - Click **Models**, then **<Model Type>** (for the model type you wish to modify) to display a list of models of the selected type.
3. Click the model in the list you want to modify.
4. Make your edits of the configurable properties for the selected model.
5. Click **Save changes**.

Deleting a Custom Model


You can only delete a model if no devices have been created from the model.

1. Click the **Custom Library** main tab.
2. Display a list of existing models. Either:
 - Click **Models** in the navigation tree to display a list of all models, or
 - Click **Models**, then **<Model Type>** (for the model type you wish to delete) to display a list of models of the selected type.
3. Do one of the following. Either:
 - To delete a single model, click the delete icon () in the row for the model you want to delete, or
 - To delete multiple models, place a check mark next to the models you want to delete, then click **Delete**.

A model is deleted when you issue the delete command. No message box appears and asks you to confirm the delete command.

Exporting One or More Custom Models

You can export custom models.

1. Click the **Custom Library** main tab.
2. Navigate to the model you want to export. Either:
 - Click **Models** in the navigation tree to display a list of all models, or
 - Click **Models**, then **<Model Type>** (for the model type you wish to export).
3. Do one of the following. Either:
 - To export a single model, click the **Export** icon () in the row for the model you want to export, or
 - To export multiple models, place a check mark next to the models you want to export, then click **Export**.

The exported model is wrapped in a .zip file and sent to the default download location of your browser.

Importing One or More Custom Models

You can import custom models.

1. Click the **Custom Library** main tab.
2. Click **Import**.
The **Import models** dialog opens.
3. Click **Browse**. The **Open** dialog appears.
4. In the **Open** dialog, navigate to and select the custom model or models to import, then click **Open**.

5. In the **Import models** dialog, click **Import**.
6. After the import process is complete, click **Close**.
The imported model or models appear in the **Custom Library** beneath the appropriate device type.

Custom Modbus Devices

The Com'X can also communicate with any third-party Modbus device. This type of Modbus device is called Modbus serial line custom slave.

The Com'X is able to communicate with a Modbus serial line custom slave in two ways:

- directly by using its own serial port
- through a ModbusTCP/Modbus serial line gateway

Creating a Modbus Custom Slave

You can configure the energy server to communicate with a Modbus serial line custom slave.

1. Click the **Custom Library** main tab.
2. Click **+Create** on the lower left part of the page.
The **Create a custom model** dialog opens.
3. Enter the following settings:

Field	Setting
Select model type	Select Modbus RTU or Modbus TCP.
Create model	Select the basis for the new custom model: <ul style="list-style-type: none"> • New • Based on a Schneider Electric model • Based on a custom model
<base model type>	If you are basing the new custom model on an existing Schneider Electric model or a custom model, select the existing model on which the new model is based.
Model name	Enter the name of the new custom model, or accept the default name <code>Modbus RTU Slave_Custom</code> or <code>Modbus TCP Slave_Custom</code> .
Default value of commodity	Select a default commodity the new model measures.
Default value of usage	Select a default value for how the new model is used

4. Click **Create**.
The dialog closes, and the newly created custom model properties page opens for initial configuration.

Defining a Modbus Custom Slave

After you have created the new Modbus custom slave model, you can complete its definition in the **Custom Library**.

This procedure requires that you have created a custom model.

1. Select the new model in the model tree view, then click the **Slave** collapsible menu.

2. Select the reading order in the **Endianness** drop-down list.

This setting describes the register order to be used when a variable is formatted with more than one register.

NOTE: The endianness depends on the device and must be selected in the Com'X settings. For example, PM700 is big endian and PM800 is little endian. The endianness setting is not used if variables are formatted with 16-bit registers.

3. Click **New frame**.

Modbus Custom Slave Register Examples

Register	Register Number	Read/write	Scale	Unit	Format	Interval	Description
1037	1	R	x1	kW	INT	+/-0...32767	Total active power
1041	1	R	x1	kVAR	INT	+/-0...32767	Total reactive power
1049	1	R	x1000	None	INT	-1000...1000	Total power factor
1054	1	R	x10	Hz	INT	0...4000	System frequency

When reading the device documentation, it appears that all variables can be read with 1 frame of registers (Function code 03) starting from register 1037 and ending with register 1054 (count = 18).

Post-requisite: Continue to Creating a Modbus Frame to define a new frame.

Creating a Modbus Frame

To enhance performance, you can map several variables to the same frame.

In the Modbus protocol, the data exchange is described by frames. A frame is a request to read an array of consecutive variables. Several frames can be necessary to access all the variables of a device. To enhance performance, reduce the number of frames by mapping several variables to the same frame.

1. Click **New** frame, a new line with default settings appears.

Item	Name	Description	Options
A	Function code	Specifies the types of read requests that the energy server can perform.	<ul style="list-style-type: none"> FC01: coils (array of output or internal bits) FC02: discrete input (array of input bit) FC03: holding registers (array of output or 16-bit internal registers) FC04: input registers (array of 16-bit input registers)
B	Starting address	Specifies the address.	0–65535 ⁽¹⁾
C	Item count	Specifies the number of items that the frame contains.	<ul style="list-style-type: none"> 1–1000 for function code FC01 or FC02 1–125 for function code FC03 or FC04
D	Number	Specifies the type of information that is mapped on this frame.	<ul style="list-style-type: none"> Boolean for FC01 or FC02 function code Boolean or number for FC03 or FC04 function code
E	Edit frame	Describes the variables of this frame.	–

⁽¹⁾There is an offset between register number and address. Register numbers can be found in the device documentation.

2. When you finish adding and configuring frame settings, click **Save changes**.

Creating Modbus Variables

As part of defining a Modbus Custom Slave, you need to set up the Modbus variables read by a Modbus frame.

1. Click **Edit frame**.

A dialog box appears and allows you to set up each variable.

2. Click **New item** to create a new variable, and fill in these different fields:

Field	Description	Comment
Name and Unit	Enables you to select a variable name from the Name list. This variable name determines the Unit options.	You can select Customized in the drop-down list and type a new text string for the name field and the unit field.
Format	Specifies the format of this number.	Several formats are available as described in the table below.
First register address	Specifies the first register number.	The register number must belong to the range of the frame. If the format contains more than 1 register, the setting checks that the last register used by this measurement is inside the frame content.
Factor	The displayed measure = (transmitted value x factor) + offset.	The displayed measure is the value displayed in the measurement tables. Transmitted value is the measure done by the meter.
Offset		
Invalid value	Indicates the transmitted value is invalid.	–

3. When you finish adding and configuring frame settings, click **OK** to close the dialog, then click **Save changes**.

The table describes the available formats:

Format	Description	Minimum Value	Maximum Value	Use "Endian" Setting
INT16	1 register with signed integer value	–32768	32767	No
UINT16	1 register with positive integer value	0	65535	No
INT32	2 registers with signed integer value	–2147483648	2147483647	Yes
UINT32	2 registers with positive integer value	0	4294967295	Yes
FLOAT32	2 registers with signed floating point value coded according to IEEE754 standard	–1E–10	+1E–10	Yes
UINT32_MOD10K	2 registers with positive integer value from 0 to 9999	0	99999999	Yes
INT64	4 registers with signed integer value	–2 (^63)	–2 (^63)–1	Yes
UINT64	4 registers with positive integer value	0	–2 (^63)–1	Yes
UINT64_MOD10K	4 registers with positive integer value from 0 to 9999	0	9 999 999 999 999 999	Yes

Custom Modbus Device

After you create a custom Modbus device in the **Custom Library**, you can add it to your network in the same way you add any Modbus device.

You can add a custom Modbus device either by discovering connected devices or by adding a Modbus device manually.

Related Topics

- Discovering Connected Devices
- Adding a Modbus Device Manually

Custom Pulse Meter Model

You can create a customized pulse meter.

To create a customized pulse meter input customized settings for the following measure properties:

- Count element
- Count unit
- Flow element
- Flow unit

Creating a Custom Pulse Meter

You can create a customized pulse meter by inputting customized settings.

1. Click the **Custom Library** main tab.
2. Click **+Create** on the lower left part of the page.
The **Create a custom model** dialog opens.
3. Enter the following settings:

Field	Setting
Select model type	Select Pulse Meter .
Create model	Select the basis for the new custom model: <ul style="list-style-type: none"> • New • Based on a Schneider Electric model • Based on a custom model
<base model type>	If you are basing the new custom model on an existing Schneider Electric model or a custom model, select the existing model on which the new model is based.
Model name	Enter the name of the new custom model, or accept the default name <code>Pulse Meter_Custom</code> .
Default value of commodity	Select a default commodity the new model measures.
Default value of usage	Select a default value for how the new model is used

4. Click **Create**.

The dialog closes, and the newly created custom model properties page opens for initial configuration.

- Configure the measure properties for a newly created custom pulse meter model.

The measure properties include the following:

Field	Description
Count element	Select a measure element from the list, or select Custom and type a personalized name into the Custom count element field.
Count unit	Select a measure unit from the list, or select Custom and type a personalized unit into the Custom count unit field.
Pulse weight	The pulse counter increases by this value each time a pulse is received. The list is restricted to the values that correspond to the selected meter type.
Upper Range	Defines when the active energy counter rolls back to zero.
Flow element	Select a flow element from the list, or select Custom and type a personalized name into the Custom flow element field.
Flow unit	Select a flow unit from the list, or select Custom and type a personalized unit into the Custom flow unit field.

Measurements table

The measure property selections you make, including customized properties, are reflected in the measurementstable.

Custom KYZ Pulse Meter Model

The custom KYZ pulse meter model has a dry contact closure that changes state each time the counter advances.

The Com'X detects the change of state, and the counter increases by the pulse weight value.

Each instance of a custom KYZ pulse meter needs to be directly connected to the digital inputs of the Com'X.

Measurement Properties

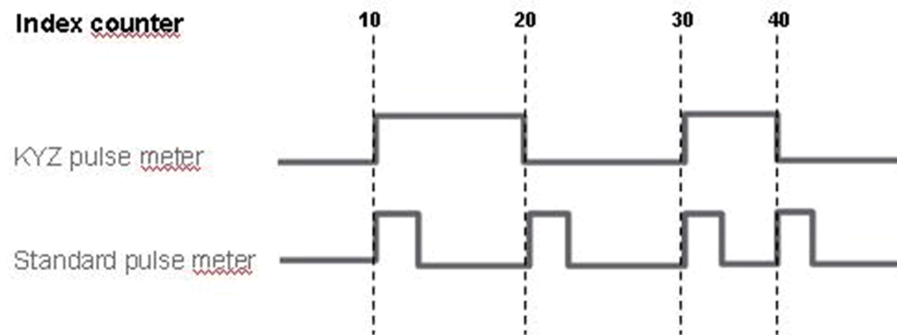
The custom KYZ pulse meter model presents the same **Measure Properties** and **Measurements table** items as a Custom Pulse Meter.

The measure properties include the following:

Field	Description
Count element	Select a measure element from the list, or select Custom and type a personalized name into the Custom count element field.
Count unit	Select a measure unit from the list, or select Custom and type a personalized unit into the Custom count unit field.
Pulse weight	The pulse counter increases by this value each time a pulse is received. The list is restricted to the values that correspond to the selected meter type.
Upper Range	Defines when the active energy counter rolls back to zero.
Flow element	Select a flow element from the list, or select Custom and type a personalized name into the Custom flow element field.
Flow unit	Select a flow unit from the list, or select Custom and type a personalized unit into the Custom flow unit field.

Index Counter

This graphic shows the difference between a KYZ pulse meter and a standard pulse meter (pulse weight = 10):



Custom Main Meter Model

The custom main meter model is made up of two pulse outputs and four contact outputs.

You can create a customized main meter by entering customized settings for the following measure properties of each of the two pulse outputs:

- Count element
- Count unit
- Flow element
- Flow unit

The signal properties of the four contact outputs present the same configuration choices as the Schneider Electric standard main meter.

Creating a Custom Main Meter

You can create a customized main meter by entering customized settings for selected measure properties of each of the two pulse outputs.

1. Click the **Custom Library** main tab.
2. Click **+Create** on the lower left part of the page.

The **Create a custom model** dialog opens.

3. Enter the following settings:

Field	Setting
Select model type	Select Main Meter .
Create model	Select the basis for the new custom model: <ul style="list-style-type: none"> • New • Based on a Schneider Electric model • Based on a custom model
<base model type>	If you are basing the new custom model on an existing Schneider Electric model or a custom model, select the existing model on which the new model is based.
Model name	Enter the name of the new custom model, or accept the default name <code>Main Meter_Custom</code>
Default value of commodity	Select a default commodity the new model measures.
Default value of usage	Select a default value for how the new model is used

4. Click **Create**.

The dialog closes, and the newly created custom model properties page opens for initial configuration.

Main Meter Measure and Signal Properties

The customized main meter has customized settings for the measure properties of each of the two pulse outputs, and the same signal properties as the standard main meter.

Each pulse output presents the following measure properties:

Field	Description
Count element	Select a measure element from the list, or select Custom and enter a personalized name into the Custom count element field.
Count unit	Select a measure unit from the list, or select Custom and enter a personalized unit into the Custom count unit field.
Pulse weight	The pulse counter increases by this value each time a pulse is received. The list is restricted to the values that correspond to the selected meter type.
Upper Range	Defines when the active energy counter rolls back to zero.
Flow Element	Select a flow element from the list, or select Custom and enter a personalized name into the Custom flow element field.
Flow unit	Select a flow unit from the list, or select Custom and enter a personalized unit into the Custom flow unit field.

Each contact output presents the following signal properties:

Field	Description
Signal element	Enter the name of this signal, or accept the default name Status Output n , where n represents the signal number (1 to 4).
Value for 0	Enter the status associated with a value of 0. Default is OFF .
Value for 1	Enter the status associated with a value of 1. Default is ON .

Measurements Table

The measure and signal property selections you make, including customized properties for pulse outputs, are reflected in the measurements table.

Custom Main Meter

After you create a custom main meter model in the **Custom Library**, you can add instances of that custom main meter in the **Device Settings**.

When you add a custom main meter, the two pulse outputs are automatically connected to the upstream device. You can connect the four contact outputs as in [Connecting a Standard Main Meter](#).

Connecting a Standard Main Meter (Main Meter)

You can connect the contact outputs from the properties collapsible menu of the standard main meter.

1. Click the **Device Settings** main tab.
2. Select the main meter in the device tree view.
3. Select **Pulse Output 1** in the **Properties** collapsible menu.
4. Select the number of digital outputs in the drop-down list.
5. Repeat steps 3 and 4 for the Pulse Output 2 properties.
6. Click **Save changes**.

Connecting a Standard Main Meter (Upstream Device)

You can connect the contact outputs from the properties area of the upstream device.

1. Click the **Device Settings** main tab.
2. Select the upstream device in the device tree view.
3. Click the Digital and analog inputs collapsible menu.
4. Select the name of the main meter in the **Device** drop-down list.
5. Select the contact output that has to be connected in the **Connector** drop-down list.
6. Click **Save changes**.

The device tree view shows that the standard main meter is connected to an additional digital input.

Custom Contactor or Impulse Relay

Connecting a contactor or impulse relay to a digital input allows you to monitor status output. The counter runs when the contact is closed.

Creating a Custom Contactor or Impulse Relay

You can create a new custom generic pulse meter model.

1. Click the **Custom Library** main tab.
2. Click **+Create** on the lower left part of the page.
The **Create a custom model** dialog opens.

3. Enter the following settings:

Field	Setting
Select model type	Select either Contactor or Impulse Relay .
Create model	Select the basis for the new custom model: <ul style="list-style-type: none"> • New • Based on a custom model
<base model type>	If you are basing the new custom model on an existing custom model, select the existing model on which the new model is based.
Model name	Enter the name of the new custom model, or accept the default name <code>Contactor Custom Or Impulse Relay Custom</code> .
Default value of commodity	Select a default commodity the new model measures.
Default value of usage	Select a default value for how the new model is used

4. Click **Create**.

The dialog closes, and the newly created custom model properties page opens for initial configuration.

5. Configure the measurement properties of a contactor or impulse relay.

Measurement Properties

Field	Description
Signal element	Enter the element being monitored, or accept the default <code>Status Output</code> .
Value for 0	Enter the state represented by a value of 0, or accept the default <code>OFF</code> .
Value for 1	Enter the state represented by a value of 1, or accept the default <code>ON</code> .

By default, measurements are logged and published to the hosted platform.

Status Custom Model

Creating a custom status model allows you to create and monitor the output status for common devices based on predefined Boolean signal elements selected from a list.

Creating a Status Custom Model

You can create a new status custom model.

1. Click the **Custom Library** main tab.
2. Click **+Create** on the lower left part of the page.

The **Create a custom model** dialog opens.

3. Enter the following settings:

Field	Setting
Select model type	Select Status from drop down menu.
Create model	Select the basis for the new custom model: <ul style="list-style-type: none"> • New • Based on a custom model
<base model type>	If you are basing the new custom model on an existing custom model, select the existing model on which the new model is based.
Model name	Enter the name of the new custom model, or accept the default name <code>Status_Custom</code> .
Default value of commodity	Select a default commodity that the new model measures.
Default value of usage	Select a default value for how the new model is used.

4. Click **Create**.

The dialog closes, and the newly created custom model properties page opens for initial configuration.

5. Configure the signal properties of Status custom model.

Signal Properties

Field	Description
Signal element	Select the required signal element from the drop down menu.
Value for 0	Select the signal element state represented by the value 0 or accept the default value given.
Value for 1	Select the signal element state represented by the value 1 or accept the default value given.

6. Click **Save changes** to save the configured Status custom model.

The custom signal element is selected for logging and publishing by default.

Custom Analog Sensor Model

Each custom analog sensor model monitors a single point.

The Com'X offers two analog sensor templates:

- 4...20 mA
- 0...10 V

You can create a customized analog sensor model by entering customized settings for the following properties:

- Count element
- Count unit

Creating a Custom Analog Sensor

You can create a customized analog sensor model by entering customized settings.

1. Click the **Custom Library** main tab.
2. Click **+Create** on the lower left part of the page.

The **Create a custom model** dialog opens.

3. Enter the custom model settings:

Field	Setting
Select model type	Select either 4-20 mA Sensor or 0-10 V Sensor .
Create model	Select the basis for the new custom model: <ul style="list-style-type: none"> • New
Type	Enter the name of the new custom model, or accept the default name, either Sensor 4-20mA_Custom or Sensor 0-10V_Custom , depending on the selected model type.
Default value of commodity	Select a default commodity the new model measures.
Default value of usage	Select a default value for how the new model is used

4. Click **Create**.

The dialog closes, and the newly created custom model properties page opens for initial configuration.

5. Configure the sensor properties.

Each pulse output presents the following measure properties:

Field	Description
Element	Select a monitoring element from the list, or select Custom and enter a personalized name into the Custom element field.
Unit	Select a monitoring unit from the list, or select Custom and enter a personalized unit into the Custom unit field.
LowerBound	The value mapped as the minimum monitored value.
UpperBound	The value mapped as the maximum monitored value.

Measurements Table

The monitoring property selections you make, including customized properties, are reflected in the measurements table.

Com'X 210 Diagnostics

Diagnostics Overview

Diagnostics provides statistical data about the Com'X and connected devices. It also allows you to perform manual register reads and check communications status of connected devices.

Statistics

Statistics shows accumulated readings since the Com'X was last reset.

If power to the Com'X is lost or the device is reset due to a configuration change or other event, all cumulative values reset to zero.

Viewing Statistics

You can view network or Modbus statistics.

1. Click **Diagnostics**.
2. Click one of the following categories: **Network** or **Modbus**.
3. Click the expandable menu for the group of statistics you want to view.
4. Click **Refresh** if you want to update the data.

NOTE: Network statistics update approximately every 10 seconds.

Resetting Statistics

You can reset a category of statistics.

1. Click **Diagnostics**.
2. Click one of the following categories: **Network** or **Modbus**.
3. Click **Reset**, then click **Yes** to confirm the reset.

Parameters in all expandable menus are reset.

Modbus Statistics

Modbus statistics are available for your device.

Parameter	Description
RS485	
Messages Received	A counter that increments each time a message is received.
Messages Transmitted	A counter that increments each time a message is sent.
Message Timeouts	A counter that increments each time a request message is sent without receiving a corresponding response message within the allowed time. Timeouts are typically the result of configuration errors or a non-responsive device.
CRC Errors	A counter that increments each time a frame is received that has a checksum/CRC that does not match what is calculated.
Protocol Errors	A counter that increments each time an ill-formed message is received.
Exceptions Received	A counter that increments each time an exception is received.
Device Details	A detailed table providing statistics per device. Click the link to open the table in a new window.

Parameter	Description
TCP/IP Server	
Messages Received	A counter that increments each time a message is received.
Messages Transmitted	A counter that increments each time a message is sent.
Protocol Errors	A counter that increments each time an ill-formed message is received.
Active Connections	A status value that represents the number of connections (internal and external) that are active at the moment the diagnostics page is refreshed. Click the link to open a dialog box with a list of all of the active external client connections.
Accumulated Connections	A counter that increments each time a connection (internal or external) is made to the Com'X.
Maximum Connections	A status value that represents the maximum number of connections that have been made since power up.
TCP/IP Client	
Messages Received	A counter that increments each time a message is received.
Messages Transmitted	A counter that increments each time a message is sent.
Message Timeouts	A counter that increments each time a request message is sent without receiving a corresponding response message within the allowed time. Timeouts are typically the result of configuration errors or a non-responsive device.
Connection Timeouts	A counter that increments each time the device times out on a connection request.
Protocol Errors	A counter that increments each time an ill-formed message is received.
Exceptions Received	A counter that increments each time an exception is received.
Device Details	A detailed table providing statistics per device. Click the link to open the table in a new window.

Network Statistics

Your device provides network statistics.

Parameter	Description
Ethernet	
Speed	A status string that represents the speed setting being used to communicate with the linking partner. Options: <i>10 Mbps</i> or <i>100 Mbps</i>
Duplex	A status string that represents the duplex setting. Options: <i>Full-Duplex</i> or <i>Half-Duplex</i>
Collisions	A counter that increments each time a frame is retransmitted due to collision detection.
CRC Errors	A counter that increments each time a frame is received that has a checksum/CRC that does not match what is calculated.
Frame Errors	A counter that increments each time a receive frame error is detected.
Packets Received OK	A counter that increments each time a packet is successfully received.
Receive Packets Dropped	A counter that increments each time a receive packet is dropped.
Receive Errors	A counter that increments each time a packet is received with a receive error.
Packets Transmitted OK	A counter that increments each time a packet is successfully transmitted.

Parameter	Description
Transmit Packets Dropped	A counter that increments each time a transmit packet is dropped.
Transmit Errors	A counter that increments each time a transmit packet experiences a transmission error.

Read Device Registers

Read Device Registers allows the Com'X to read Modbus registers from its local and remote devices.

Below are **Read Device Registers** settings.

Setting	Description	Options
Device Name	Selects a device to read from the list of previously added devices. A device not defined in the device list can be read by entering its Local ID.	—
Local ID	The address (Local ID) of the device that is to be read.	1-255 Default: 1
Starting Register	The first register to read.	Default: 1000
Number of Registers	The number of registers to read.	1-125 Default: 10
Register	A column displaying the register numbers.	—
Value	A column displaying the data stored for each register. Values retrieved depend on the device connected to the Com'X. Refer to the documentation for the connected device for more information about stored register values.	—
Data Type	Menu for selecting the type of data the registers hold and the format (Decimal, Hexadecimal, Binary, or ASCII) you want returned.	Holding Registers, Input Registers, Output Coils, Input Coils, or Device ID Default: Holding Registers.

Reading Device Registers

You can read Modbus registers from local and remote devices using **Read Device Registers**.

1. Click **Diagnostics > Read Device Registers**
2. Select a device from the **Device Name** drop-down list, or choose **Select by Device ID** for devices that aren't in the device list.
3. If you chose **Select by Device ID**, enter the **Local ID**.

If you selected a device name in the previous step, this field is populated automatically and cannot be changed.

NOTE: The **Slave ID** is the identifier on the serial port to which it is connected. The **Local ID** is the identifier used by the Com'X.

4. Enter a starting register and the number of registers to read.
5. Select a data type.

6. If you selected **Holding** or **Input registers**, choose a format for the returned data.
7. Click **Read**.

Communications Check

The communication status of a device is evaluated with each communication initiated by the Com'X, for example when using Real Time Data.

When the **Out of Service Time** is enabled, the Com'X discontinues communications to a device after two consecutive message time-outs. The Com'X treats the device as out of service and does not attempt to communicate with it again until the **Out of Service Time** period has expired.

This reduces unnecessary network traffic by removing messages going to a device that is known to be out of service. You can circumvent the timer by manually initiating a communications check.

If you do not enable **Out of Service Time**, the Com'X continues to attempt communications with the device, and time-outs from unresponsive devices will affect bandwidth of external clients.

In the **Communications Check** subtab, you can execute a manual communications check as well as configure the Out of Service timer for re-establishing communication.

Executing a Manual Communications Check

In certain cases, you may not want to wait for the automated communications check interval and need to force the check to run manually.

1. Click **Diagnostics > Communications Check**.
2. Click **Check Device Status** to begin the check.
3. Optionally, you can click **Stop Status Check** to stop the check.

The Status column displays **In Service** or **Out of Service**.

Defining the Out of Service Time

You can define the **Out of Service Time**.

1. Click **Diagnostics > Communications Check**.
2. Select **Yes** for **Enable Out of Service Time**.
3. Select the **Out of Service Time**. Options are 1, 2, 3, 4, 5, 10, 15, 30 and 60 minutes (default: 15).
4. Click **Save changes**.

Com'X 210 Maintenance

Logs

The Logs subtab displays the list of events that have been logged with the recorded date and time and a short description of the event.

The Com'X displays logs for at least 10 minutes before power outage or shutdown.

Schneider Electric recommends checking the logs periodically for excessive denied accesses, unexpected firmware upgrades or unplanned backup restoration. These can be signs of fraudulent attacks. If this happens, contact your local Schneider Electric technical support.

Downloading Logs

Get diagnostics info allows you to download the Com'X logs.

The downloaded file cannot be read with common software. This file is useful only to Schneider Electric technical support.

Logged Events

Your device logs events.

The events that are logged are:

Topic	Event
Resource	Change in the configuration of: <ul style="list-style-type: none"> • devices • publication
Delivery	Publication steps and status (unsuccessful or successful)
	Activation/deactivation of the periodic publication
Logging	Activation/deactivation of the data logging
Security	Unsuccessful login
Alarm	Low level of GPRS/3G signal
	Error detected during the login
	Device not communicating
	CPU and RAM overuse
	Communication interruptions with metering devices
System	Time setting modification
	Firmware update and status
	Boot time

System Settings

System Settings allows you to save and restore a device configuration, apply a common configuration to other devices, upgrade Com'X firmware, enable remote access for support, and restart Com'X device.

Configuration Management

The Configuration Management menu has the following options:

- Save the configuration: use this option to create a configuration file to be used to save and apply the configuration on the **same** device.
- Backup for duplication: use this option to create a backup file which can be used to configure one or more Com'X devices. The backup file can reduce configuration time when a common system configuration is used for several Com'X devices being installed.
- Apply the configuration: use this option to apply a configuration file saved using the above options. Depending on which option is used, some parameters will be set to a default during the restore process as detailed below. You can apply the configuration from:

Saved configuration file generated from the same device: The DSP parameters saved within the configuration file will only be applied if the backup and restore device is the same.

Saved duplicate backup configuration file generated from a different device: This will default the Device and Site names. The device name field is set to Com'X 210/510_xxyyzz, where xxyyzz represents the last three hexadecimal octets of the device MAC address, and the site name field is left blank.

NOTE: When Com'X is connected to DSP:

- Do not restore a backup configuration file from a Com'X device which is not connected to DSP to a device connected to DSP.
- The DSP parameters saved within the configuration file will only be applied if the backup and restore device is the same.
- If configuration is restored on a different Com'X device, then the DSP configuration on the restored device does not change.
- Restoring the configuration file from another Com'X is not possible remotely through DSP.

Save the Configuration

The configuration of a Com'X can be saved to a file and used to restore the configuration on the same Com'X.

You should save a backup configuration before and after each firmware upgrade.

Backup files contain sensitive information such as network passwords. Safeguard the media after the backup in a protected location to prevent unauthorized access.

NOTICE
HAZARD OF UNAUTHORIZED ACCESS
Do not communicate a backup file to unauthorized persons.
Failure to follow these instructions can result in equipment damage.

The file name is in the format Com'X name_Firmware version_YYYYMMDD-HHMM.zip. For example, MyComXEnergyServer_V6.0_20190110_1020.zip indicates that the file is generated from:

- a Com'X named MyComXEnergyServer
- running on the firmware version 6.0
- on January 10th, 2019 at 10:20 a.m.

The configuration should be saved only after completing the initial update or configuration.

Related Topics

- Upgrade Firmware

Saving the Configuration Locally

You can save the configuration locally.

1. Click **Maintenance > System Settings**.
2. Click **Save Configuration** OR **Backup for Duplication** in the **Configuration Management** collapsible menu.
According to the web browser used, a dialog box appears to open, save, or cancel the configuration file.
3. Select the option to save the file in the dialog box.
The date and time of the last configuration backup are displayed under the **Save Configuration** button.
4. In the **Choose File** field, select the location on the computer to save the file and save the configuration.

To save configuration to USB device


You can save the Com'X configuration to a file on a USB drive.

⚠ DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- This equipment must only be installed and serviced by qualified personnel.
- Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices. See NFPA 70E in the USA, CSA Z462 or applicable local standards.

Failure to follow these instructions will result in death or serious injury.

1. Insert a USB key into the USB port on the Com'X front panel.
2. Press and hold the **Backup** button  for at least three seconds.
During backup the USB LED behaves as follows:
 - If no error is detected during backup, the USB LED blinks green for 500 ms, then off for 500 ms.
 - If an error is detected, the USB LED blinks green for 250 ms, then off for 250 ms for a total of three seconds.
3. If no error is detected during backup, the backup is complete when the blinking stops.
You can remove the USB key from the Com'X front panel.

Restore a configuration

You can restore configuration by using a local file or configuration file in a USB key.

Restoring the Configuration with a Local File

To restore configuration from a local file:

1. Navigate to **Maintenance > System Settings > Configuration Management**.
2. Click **Browse** in the **Configuration Management** collapsible menu to select the locally saved configuration file and click **Open**.

3. Click **Apply the configuration** and wait for Com'X to reboot.
The power LED turns green when the reboot is complete.
4. Reconnect to the Com'X.
5. If configuration files was saved using **Backup for Duplication**the following steps are required:
 - a. Click **Settings > Site Settings > Site Information**.
 - b. Type the new site location name, then click **Save changes** to save the modification.
NOTE: The site location name may not include any of the following: '/' :*?<>| or space.
 - c. Click the **Device Settings** tab and select Com'X in the Device tree view and type the name in the **General Properties**collapsible menu.
 - d. Click **Save changes** to save your modification.
6. Click the **Measurement table** tab to check the correct connection, setting, and functioning on the new site.
7. Select **Commissioning** tab to activate logging and publication according to destination platform.

Related Topics

- Save the Configuration

Restoring the Configuration with a USB Key

You can save configuration on a USB key and use it to restore configuration.

DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- This equipment must only be installed and serviced by qualified personnel.
- Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices. See NFPA 70E in the USA, CSA Z462 or applicable local standards.

Failure to follow these instructions will result in death or serious injury.

1. Copy the saved configuration file to a folder named "Restore" at the root of the USB key.
2. Power off Com'X, then plug the USB key into the USB port on the Com'X front panel.
3. Power on the Com'X and wait for it to reboot.
When the power LED turns green, the reboot is complete.
4. Log in to the Com'X.

5. If configuration files was saved using **Backup for Duplication** the following steps are required:
 - a. Click **Settings > Site Settings > Site Information**.
 - b. Type the new site location name, then click **Save changes** to save the modification.

NOTE: The site location name may not include any of the following: / : * ? < > | or space.
 - c. Click the **Device Settings** tab and select Com'X in the Device tree view and type the name in the **General Properties** collapsible menu.
 - d. Click **Save changes** to save your modification.
6. Click the **Measurement table** tab to check the correct connection, setting, and functioning on the new site.
7. Select **Commissioning** tab to activate logging and publication according to destination platform.

Related Topics

- Save the Configuration

Upgrade Firmware

The Com'X can be updated using secured firmware through the web page or the USB port on the Com'X front face.

For the latest firmware update, check www.se.com on the Com'X page, or contact your local sales representative.

Firmware upgrades can only be successful if the date and time of the Com'X is correctly configured.

Before You Begin

- You should save a backup configuration before and after each firmware upgrade.
- Manually push any logged data in **Commissioning > Publication > Manual publication**.

NOTE: Depending on the number of devices connected to the Com'X, it can take 10 to 35 minutes to upgrade the firmware and reboot the Com'X.

Related Topics

- Save the Configuration
- Configuring Date and Time

Upgrading Firmware via the Web Page

You can upgrade the firmware through the web interface.

1. Save the firmware file on your laptop.
2. Click **Maintenance > System settings**.
3. Click **File** in the **Firmware upgrade** collapsible menu, and select the firmware file.
4. Click **Open**.

The selected file appears in the field next to the **Browse** button.

5. Click **Upgrade Firmware**.

The message "Application not reachable" is displayed during the upgrade.

6. Wait up to 20 minutes for the Com'X to reboot.

The power LED turns green when the reboot is complete.

7. Log in to the Com'X.

8. Check that the new firmware has been installed in the **About** page.

9. Clear browser cache after upgrade.

Upgrading Firmware via the USB Port

You can upgrade the firmware using the USB port.

DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- This equipment must only be installed and serviced by qualified personnel.
- Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices. See NFPA 70E in the USA, CSA Z462 or applicable local standards.

Failure to follow these instructions will result in death or serious injury.

1. Save the firmware file at the root of the USB memory key.

2. Rename the file to upgrade.sp1.

3. Make sure there is no file located at the root of the USB memory key with a name that is the same as the serial number of the Com'X.

4. Power down the Com'X.

5. Insert the USB memory key in the USB port located on the front face.

6. Power up the Com'X.

7. Wait up to 20 minutes for the Com'X to reboot.

The power LED turns green when the reboot is complete.

8. Connect to the Com'X through a PC and click the **About** link to check that the new firmware is installed.

9. Clear browser cache after upgrade.

Upgrading Firmware via DSP

Firmware upgrade through DSP is managed by Schneider Electric technical support.

At the end of the firmware upgrade process, the Com'X reboots. Logging and publication restart automatically.

NOTE: It is not recommended to make the first firmware upgrade of the Com'X using the DSP through GPRS connection. Because the GPRS connection has a speed of only 20 kb/s, the firmware update could take several hours.

Enabling Remote Access

Remote Access allows Schneider Electric support to connect remotely to a Com'X to check settings and to troubleshoot without having to go to the customer site.

Schneider Electric does not attempt connections unless required to do so. If a proxy is necessary, it must be configured.

When activated, **Remote Access** is used to create a connection between the Com'X and Schneider Electric remote services.

To activate Remote Access:

1. Click **Maintenance > System Settings**.
2. Under **Applications**, click the **Remote access for support** button to ON only if Schneider Electric support team is asking for it. Otherwise, leave the remote access button OFF (default).

The **Remote Access** button is deactivated three hours after you turn it on. Alternatively, you can deactivate **Remote Access** as in the steps above.

Disabling Remote Access from Cloud Services

By default, a Com'X device connected to DSP can be accessed through remote assistance. The **Enable remote access from cloud** option is enabled (ON) by default. For security reasons it is recommended to disable this feature and enable it only when remote access is required for technical support from Schneider Electric.

To disable remote access from the cloud:

1. Select **Maintenance > System Settings > Applications**.
2. Click **OFF** to disable **Enable remote access from the cloud** option.

The Com'X cannot be remotely accessed from cloud services. **Enable remote access from cloud** can be switched on when remote connection is required for technical support.

Restarting the Com'X from the Web Interface

Use the **Restart Com'X** feature to manually restart the Com'X.

1. Click **Maintenance > System Settings**.
2. Under **Restart Com'X**, click **Restart**, then **Yes** to confirm.
The reboot begins.

Product Replacement

To restore the Com'X configuration via a local file, replace the old Com'X with the new one and use one of the methods for restoring the configuration.

Related Topics

- Restore a configuration

Resetting the Password Locally

If you lose the password, you can reset the default administrator password to factory values.

Resetting the password does not affect the other configuration settings and data.


The web server is a tool for reading and writing data. It controls the state of the system, with full access to all data in your application. You will be prompted to change your password the first time you log in to prevent unauthorized access to the application.

A secure password should not be shared or distributed to unauthorized personnel. The password should not contain any personal or obvious information.

The new password must contain:

- 8 characters
- 1 uppercase letter
- 1 numeric digit
- 1 special character

NOTE: The password reset function must be enabled. See **Settings > Security > Firewall Management > Enable default admin reset** to check the status of the password reset function.

1. Press the Backup button  on the Com'X front face and hold it for at least 10 s until the power LED flashes green three times.
2. Release the button.
3. To access to the Com'X configuration web pages, use these settings:
 - Username: admin
 - Password: admin

Related Topics

- Disabling the Password Reset Button

Resetting to Factory Settings

When following the procedure below, all data and logs that have been stored are erased.

NOTICE



HAZARD OF IP ADDRESS CONFLICT

Disconnect the Com'X from any Ethernet networks before resetting the IP settings to factory values.

Failure to follow these instructions can result in impaired communications.

If you are using a Schneider Electric Service through DSP, contact Schneider Electric support before performing a factory reset. Otherwise, you must contact DSP support to reconnect to your subscribed service: dsp-support@schneider-electric.com.

To reset the energy server completely, follow this procedure to set all configuration settings to factory values:

1. Power down the Com'X and wait until the power LED is off.
2. Press simultaneously the Backup button  and the Wi-Fi button  on the Com'X front face and power up the Com'X.
Hold the buttons until the power LED flashes three times.

3. Release the buttons.

It can take up to 20 minutes for the Com'X to reboot.

4. Wait for the Com'X to restart completely.

The power LED is:

- orange when the Com'X is starting.
- green when the Com'X has been reset to factory settings and is ready to be configured.

5. Follow the instructions described in *Access the User Interface* to access the Com'X web pages.

Related Topics

- [Com'X 210 Access the User Interface](#)

Checklist Before Leaving Customer Site

Schneider Electric recommends using this checklist before leaving customer site.

This list is not exhaustive.

Checkpoint	Done	Comments
Logging is ON in the banner.		
Publication is ON in the banner (if applicable).		
Each meter returns relevant values in the Measurements Table and Real Time Data tabs.		
Each analog sensor returns relevant values in the Measurements Table.		
No notification icon is in the Measurements Table.		
For Ethernet connections, the LED eth1 and/or eth2 is blinking.		
For GPRS or 3G connections, the wireless connection has a reception level at least equal to 2/4.		
For GPRS or 3G connections, check the LED and the general status.		
For Wi-Fi connections, the wireless connection has a good reception level.		
For Wi-Fi connections, check the LED and the general status.		
The last publication to the platform has to be successful (if applicable).		

Com'X 210 Troubleshooting

Metering Device Troubleshooting

There are tips for troubleshooting your metering devices.

⚠ DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- This equipment must only be installed and serviced by qualified personnel.
- Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices. See NFPA 70E in the USA, CSA Z462 or applicable local standards.

Failure to follow these instructions will result in death or serious injury.

Digital Input Troubleshooting

This table describes how to solve issues with digital inputs.

Issue	Possible Solution
No pulse is received. The digital input LED is not flashing.	Bridge the input terminals between the terminal and the 12 V power supply with a short piece of wire to confirm that the LED is working. If the input LED lights up when you bridge the input terminals, the issue is likely with the meter and/or the wiring to the meter.
	Check that the pulse output meter is connected to a digital input terminal and the 12 V power supply.
	Refer to the <i>Installation Guide</i> for wiring diagrams.
	Check that the pulse output device is operating.
No pulse is received. The digital input LED is flashing.	Check the digital input number to which the pulse meter is connected.

Analog Input Troubleshooting

This table describes how to solve issues with analog inputs.

Issue	Possible Solution
No analog value can be read.	Check that the analog output sensor is connected to the proper terminals.
	Refer to the <i>Installation Guide</i> for wiring diagrams.
	In the configuration web page, check that the analog input number is set to the correct type of sensor: RTD, 0–10 V, or 4–20 mA.

Possible Logging Errors

This table lists the possible logging errors for the Data log.

Error Code	Definition
0	No error detected
19	No valid values are recorded for the logging interval. This is most likely the result of failed communications with the device.

Modbus Device Troubleshooting

There are some tips for troubleshooting Modbus devices.

⚠ DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- This equipment must only be installed and serviced by qualified personnel.
- Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices. See NFPA 70E in the USA, CSA Z462 or applicable local standards.

Failure to follow these instructions will result in death or serious injury.

This table describes how to solve issues with Modbus devices.

Issue	Possible Solution
No Modbus device can be detected on the Com'X serial line.	<ol style="list-style-type: none"> 1. Open the Measurements Table main tab of the Com'X. 2. If the Rx communication LED does not flash on the device, check the wiring integrity. 3. If the Rx communication LED flashes on the device, but the Tx communication LED does not flash on the device: <ul style="list-style-type: none"> • check that the device settings match the Com'X Modbus serial settings (Baud rate, Parity, and Number of stop bits). • check that the Serial line polarization is set to Yes. • check that the Serial line polarization is not activated on another Modbus slave device on the same serial line.
Some Modbus devices are missing on the Com'X serial line.	Check the Modbus addresses of the missing devices.
	Check that two devices do not have the same slave ID.
	Check that the settings of the missing devices match the Com'X Modbus serial settings (Baud rate , Parity , and Number of stop bits).
	Check that the wiring connections of the missing devices are correct.
	Check that the discovery range is large enough. The factory settings range from 1 to 10.
No Modbus device can be detected downstream from a gateway.	Check that the wiring of the missing devices is correct.
	<p>Use the Diagnostic/Read Device Registers feature of the EGX to determine if the issue is between Modbus device and the EGX or between the Com'X and the EGX.</p> <p>If the issue is located between</p> <ul style="list-style-type: none"> • the Com'X and the EGX, check the IP address of the gateway. • the EGX and the Modbus device, check that the Modbus device settings match the EGX serial port setup (Baud rate, Parity, and Number of stop bits). <p>The combination (Parity = none and Number of stop bits = 1) of port settings is not supported by the EGX. Change to another combination.</p>

Network Troubleshooting

There are some tips for troubleshooting your network.

⚠ DANGER**HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH**

- This equipment must only be installed and serviced by qualified personnel.
- Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices. See NFPA 70E in the USA, CSA Z462 or applicable local standards.

Failure to follow these instructions will result in death or serious injury.

Ethernet Troubleshooting

This table describes how to solve issues with Ethernet.

Issue	Possible Solution
Ethernet LEDs are not blinking.	Check that the Ethernet LAN cables are not disconnected.
Cannot access to Modbus devices downstream from a Modbus TCP/Modbus serial line gateway.	Check the IP address of the gateway. If data export is via GPRS/3G, check that the gateway is on the same Ethernet subnetwork as the Com'X.

GPRS/3G Troubleshooting

This table describes how to solve issues with GPRS or 3G.

Issue	Possible Solution
Modem is not detected. The LED modem is not flashing.	Power down the Com'X. Reinsert the modem and power up the Com'X.
Modem cannot connect to the network.	Check that the settings such as the APN are correct.
GPRS LED on front panel turns ON and OFF periodically.	Check that protocol settings are correct in General Setting > Publication .

Wi-Fi Troubleshooting

This table describes how to solve issues with Wi-Fi.

Issue	Possible Solution
Wi-Fi USB key is not detected. The USB key LED is not flashing.	Power down the Com'X. Reinsert again the Wi-Fi USB key and power up the Com'X.
Wi-Fi USB key cannot connect to the network.	Check that the settings such as the SSID name and the WPA2 key are correct.

Com'X Troubleshooting

Com'X Access

Issue	Possible Solution
Cannot log in through customer LAN.	Log in to the Com'X. Check the IP address.
Lost password	Follow the procedure to reset the password.

Web Pages

Issue	Possible Solution
The web pages are not displayed correctly.	Check the screen resolution of your laptop. It must be set to at least 1280x1024.
	In Internet Explorer, check that the Display intranet sites in compatibility view box is disabled by selecting View settings compatibility in the Tools tab of Internet Explorer.
	Delete browsing history.

Digital Service Platform Selection

Issue	Questions to be asked	Possible Solution
Authentication Issue	Was the Com'X connected to DSP prior to the issue?	If yes, then restore configuration on the Com'X.
	Is this a duplicated Com'X or has the Com'X been factory reset?	If yes, then contact Schneider Electric Services.
Unable to connect to Digital Service Platform after configuring proxy.	N/A	Disable and enable Schneider Electric Services.
Unable to set date/time on the Com'X.	Is Com'X connected to Digital Service Platform ?	If yes, then wait for the date and time to get synchronized and display.

Data Publishing

Issue	Possible Solution
Publication to the platform was unsuccessful.	<ul style="list-style-type: none"> Check the platform user name and the password. Check the Com'X date and time.
Publication to the platform was unsuccessful with Ethernet or Wi-Fi.	Check if a proxy is implemented on the network.
The Com'X connects to the FTP server but does not succeed in delivering the data file.	Check that your FTP account has the right to rename a file on the FTP server.

Firmware Upgrade

Issue	Possible Solution
Firmware is not upgraded when managed through USB memory key plugged on front panel.	Delete the file DNxxxxxxxxxxxx-xxx (where xxxxxxxxxxxxxx-xxx is the serial number of the Com'X) registered at the root directory of the USB memory key.

Events

Issue	Possible Solution
EcoStruxure™ Facility Expert is not receiving events from the Com'X.	<ul style="list-style-type: none"> Check that Schneider Electric Services is enabled. Check that generated events are incrementing in Maintenance > Events. Check the Last delivery status in Maintenance > Events. Check the comms status of each device in Diagnostics > Communications Check.

Related Topics

- [Proxy Settings](#)
- [Logging In for the First Time](#)
- [Resetting the Password Locally](#)

Certificate Authorities

Certificate authorities supported on Com'X for HTTPS and SMTPS:

Certificate Name	Owner User	Owner
DigiCert Assured ID Root CA	www.digicert.com	DigiCert Inc
TC TrustCenter Class 2 CA II	TC TrustCenter Class 2	TC TrustCenterGmbH
Thawte Premium Server CA OID.1.2.840.113549.1.9.1= premiumserver@ thawte.com	Certification ServicesDivision	Thawte Consulting cc
SwissSign Platinum CA - G2	—	SwissSign AG
SwissSign Silver CA - G2	—	SwissSign AG
Thawte Server CA OID.1.2.840.113549.1.9.1=servercerts@ thawte.com	Certification Services Division	Thawte Consulting cc
Equifax Secure eBusiness CA-1	—	Equifax Secure Inc.
UTN-USERFirst-Client Authenticationand Email	http://www.usertrust.com	TheUSERTRUSTNetwork
Thawte Personal Freemail CA OID.1.2.840.113549.1.9.1= personalfreemail@ thawte.com	Certification ServicesDivision	ThawteConsulting
Entrust Root Certification Authority	www.entrust.net/CPSis incorporated byreference, (c) 2006Entrust, Inc.	Entrust, Inc.
UTN-USERFirst-Hardware	http://www.usertrust.com	TheUSERTRUSTNetwork
Certum CA	—	Unizeto Sp. zo.o.
AddTrust Class 1 CA Root	AddTrust TTP Network	AddTrust AB
Entrust Root Certification Authority - G2	Seewww.entrust.net/legalterms, (c) 2009 Entrust, Inc.™(1)	Entrust, Inc.
Equifax Secure Certificate Authority	—	Equifax
QuoVadis Root CA 3	—	QuoVadis Limited
QuoVadis Root CA 2	—	QuoVadis Limited
DigiCert High Assurance EV Root CA	www.digicert.com	DigiCert Inc
http://www.valicert. comOID.1.2.840.113549.1.9.1= info@valicert.com	ValiCert Class 1 Policy Validation Authority	ValiCert, Inc.
Equifax Secure Global eBusiness CA-1	—	Equifax Secure Inc.
GeoTrust Universal CA	—	GeoTrust Inc.
thawte Primary Root CA - G3	Certification Services Division, (c) 2008 thawte, Inc.(1)	thawte, Inc.
—	Class 3 Public Primary Certification Authority	VeriSign, Inc.

Certificate Name	Owner User	Owner
thawte Primary Root CA - G2	c) 2007 thawte, Inc.(1)	thawte, Inc.
Deutsche Telekom Root CA 2	T-TeleSec Trust Center	DeutscheTelekom AG
UTN-USERFirst-Object	http://www.usertrust.co	TheUSERTRUSTNetwork
GeoTrust Primary Certification Authority	—	GeoTrust Inc.
Baltimore CyberTrust Code Signing Root	CyberTrust	Baltimore
—	Class 1 Public Primary Certification Authority	VeriSign, Inc.
Baltimore CyberTrust Root	CyberTrust	Baltimore
—	Starfield Class 2 Certification Authority	StarfieldTechnologies, Inc.
Chambers of Commerce Root	http://www.chambersign.org	ACCamerfirmaSA CIFA82743287
T-TeleSec GlobalRoot Class 3	T-Systems Trust Center	T-SystemsEnterpriseServicesGmbH
VeriSign Class 3 Public Primary Certification Authority - G5	VeriSign Trust Network, (c) 2006 VeriSign, Inc. (1)	VeriSign, Inc.
T-TeleSec GlobalRoot Class 2	T-Systems Trust Center	T-SystemsEnterpriseServicesGmbH
TC TrustCenter Universal CA I	TC TrustCenter Universal CA	TCTrustCenterGmbH
VeriSign Class 3 Public Primary Certification Authority - G4	VeriSign Trust Network, (c) 2007 VeriSign, Inc. (1)	VeriSign, Inc.
VeriSign Class 3 Public Primary Certification Authority - G3	VeriSign Trust Network, (c) 1999 VeriSign, Inc. (1)	VeriSign, Inc.
Class 3P Primary CA	—	Certplus
Certum Trusted Network CA	Certum CertificationAuthority	UnizetoTechnologiesS.A.
Class 3 Public Primary Certification Authority - G2	VeriSign Trust Network, (c) 1998 VeriSign, Inc. (1)	VeriSign, Inc.
GlobalSign	GlobalSign Root CA —R3	GlobalSign
UTN - DATACorp SGC	http://www.usertrust.com	TheUSERTRUSTNetwork
—	SecurityCommunicationRootCA2	SECOM TrustSystems CO., LTD.
Certum CA	—	Unizeto Sp. z o.o.
GTE CyberTrust Global Root	GTE CyberTrustSolutions, Inc.	GTECorporation
—	SecurityCommunicationRootCA1	SECOM Trust. net
TC TrustCenter Class 4 CA II	TC TrustCenter Class 4	TCTrustCenterGmbH
VeriSign Universal Root CertificationAuthority	VeriSign Trust Network, (c) 2008 VeriSign, Inc. (1)	VeriSign, Inc.
GlobalSign	GlobalSign Root CA - R2	GlobalSign
Class 2 Primary CA	—	Certplus
DigiCert Global Root CA	www.digicert.com	DigiCert Inc
GlobalSign Root CA	Root CA	GlobalSign nvsa
thawte Primary Root CA	Certification Services	thawte, Inc.

Certificate Name	Owner User	Owner
	Division, (c) 2006 thawte, Inc.(1)	
GeoTrust Global CA	–	GeoTrust Inc.
Sonera Class2 CA	–	Sonera
Thawte Timestamping CA	Thawte Certification	Thawte
Sonera Class1 CA	–	Sonera
QuoVadis Root Certification Authority	Root CertificationAuthority	QuoVadisLimited
http://www.valicert.com OID.1.2.840.113549.1.9.1=info@valicert.com	ValiCert Class 2 PolicyValidation Authority	ValiCert, Inc.
AAA Certificate Services	—	Comodo CALimited
AddTrust Qualified CA Root	AddTrust TTP Network	AddTrust AB,C
KEYNECTIS ROOT CA	ROOT	KEYNECTIS
America Online Root CertificationAuthority 2	—	America OnlineInc.
VeriSign Class 2 Public Primary Certification Authority - G3	VeriSign Trust Network, (c) 1999 VeriSign, Inc. (1)	VeriSign, Inc.
AddTrust External CA Root	AddTrust External TTPNetwork	AddTrust AB,C
America Online Root CertificationAuthority 1	—	America OnlineInc.
Class 2 Public Primary CertificationAuthority - G2	VeriSign Trust Network, (c) 1998 VeriSign, Inc. (1)	VeriSign, Inc.
GeoTrust Primary Certification Authority - G3	(c) 2008 Geo Trust Inc.(1)	GeoTrust Inc.
GeoTrust Primary Certification Authority -G2	(c) 2007 Geo Trust Inc.(1)	GeoTrust Inc.
SwissSign Gold CA - G2	—	SwissSign AG
Entrust.net Certification Authority (2048)	www.entrust.net/CPS_ 2048 incorp. by ref. (limits liab.), (c) 1999 Entrust.net Limited	Entrust.net
GTE CyberTrust Root 5	GTE CyberTrustSolutions, Inc.	GTECorporation
Global Chambersign Root - 2008, OID.2.5.4.5=A82743287	–	ACCamerfirmaS.A.
Chambers of Commerce Root - 2008, OID.2.5.4.5=A82743287	—	ACCamerfirmaS.A.
-	Go Daddy Class 2Certification Authority	The Go DaddyGroup, Inc.
Entrust.net Secure Server Certification Authority	www.entrust.net/CPSincorp. by ref. (limitsliab.), (c) 1999Entrust.net Limited	Entrust, Inc.
VeriSign Class 1 Public Primary Certification Authority - G3	VeriSign Trust Network, (c) 1999 VeriSign, Inc. (1)	VeriSign, Inc.
—	SecurityCommunication EVRootCA1	SECOM TrustSystems CO., LTD.
(1) For authorized use only		
(2) See current address at www.camerfirma.com/address		

Modbus Register Mapping

The registers that can be read depend on the device you are communicating with.

Discovery Feature

The product responds to the Modbus function code FC43-14 with the following values:

- The `VendorName` = Schneider Electric
- The `ProductCode` = EBX210
- The `ProductName` = Com'X 210
- The `MajorMinorRevision` = the Com'X 210 version.

Com'X Register Mapping

Register values can be read only through Modbus function codes FC03-FC04.

Legacy registers from previous firmware versions are still supported.

Address	Register	Object	Size (Word)	Format	Unit	Comments
1199	1200	D1 Label	20	UTF-8	UTF-8	
1219	1220	D2 Label	20	UTF-8	UTF-8	
1239	1240	D3 Label	20	UTF-8	UTF-8	
1259	1260	D4 Label	20	UTF-8	UTF-8	
1279	1280	D5 Label	20	UTF-8	UTF-8	
1299	1300	D6 Label	20	UTF-8	UTF-8	
1319	1320	Reserved	12	–	–	
1331	1332	D1 Pulse Weight	2	FLOAT32	–	
1333	1334	D2 Pulse Weight	2	FLOAT32	–	
1335	1336	D3 Pulse Weight	2	FLOAT32	–	
1337	1338	D4 Pulse Weight	2	FLOAT32	–	
1339	1340	D5 Pulse Weight	2	FLOAT32	–	
1341	1342	D6 Pulse Weight	2	FLOAT32	–	
1343	1344	D1 On Time	2	INT32U	sec	See note 4.
1345	1346	D2 On Time	2	INT32U	sec	See note 4.
1347	1348	D3 On Time	2	INT32U	sec	See note 4.
1349	1350	D4 On Time	2	INT32U	sec	See note 4.
1351	1352	D5 On Time	2	INT32U	sec	See note 4.
1353	1354	D6 On Time	2	INT32U	sec	See note 4.
1355	1356	D1 Pulse Count	2	INT32U	–	See note 3.
1357	1358	D2 Pulse Count	2	INT32U	–	See note 3.
1359	1360	D3 Pulse Count	2	INT32U	–	See note 3.
1361	1362	D4 Pulse Count	2	INT32U	–	See note 3.
1363	1364	D5 Pulse Count	2	INT32U	–	See note 3.
1365	1366	D6 Pulse Count	2	INT32U	–	See note 3.
1367	1368	D1 Measured Value	4	INT64	–	See note 3.
1371	1372	D2 Measured Value	4	INT64	–	See note 3.

Address	Register	Object	Size (Word)	Format	Unit	Comments
1375	1376	D3 Measured Value	4	INT64	–	See note 3.
1379	1380	D4 Measured Value	4	INT64	–	See note 3.
1383	1384	D5 Measured Value	4	INT64	–	See note 3.
1387	1388	D6 Measured Value	4	INT64	–	See note 3.
1391	1392	D1 Measured Flow	2	FLOAT32	–	See note 3.
1393	1394	D2 Measured Flow	2	FLOAT32	–	See note 3.
1395	1396	D3 Measured Flow	2	FLOAT32	–	See note 3.
1397	1398	D4 Measured Flow	2	FLOAT32	–	See note 3.
1399	1400	D5 Measured Flow	2	FLOAT32	–	See note 3.
1401	1402	D6 Measured Flow	2	FLOAT32	–	See note 3.
1403	1404	Reserved	96	UINT16	–	
1499	1500	A1 Normalized Value	2	FLOAT32	–	See note 5.
1501	1502	A2 Normalized Value	2	FLOAT32	–	See note 5.
1503	1504	A1 Scaled Value	2	FLOAT32	–	
1505	1506	A2 Scaled Value	2	FLOAT32	–	
1507	1508	A1 Label	20	UTF-8	UTF-8	
1527	1528	A2 Label	20	UTF-8	UTF-8	
1547	1548	Reserved	852	INT16		
2399	2400	Digital Input Validity - Bit 0..5	1	Bitmap	–	See note 1. Can be read with Modbus code FC01 (coil 38400 - 38405).
2400	2401	Digital Input - Bit 0..5	1	Bitmap	–	See note 2. Can be read with Modbus code FC01 (coil 38416 - 38421).

1. One bit is set for each digital input (DI) used in the Com'X 210.
2. One bit is set for each digital input configured as a contactor or an impulse relay, if this device is closed.
3. This value is valid only if the digital input is configured as a pulse meter
4. This value is valid only if the digital input is configured as a contactor or an impulse relay
5. If the sensor connected to the analog input (AI)

- is a 0-10V sensor, the raw value is the voltage value [0–10V].
- is a 4-20mA sensor, the raw value is the current value [4–0.020A].

EM4300 Register Mapping

Register values can be read only through Modbus function codes FC03-FC04.

EM4300	EM4399	Address	Register	Description	Size	Data Type	Units	Update Frequency
X	X	1	2	Product Identifier 17150 — EM4300 17151 — EM4399	1	INT16U	–	<< 1 Minute
		2	3	Reserved	1998	–	–	–
X	X	2000	2001	Frequency	2	FLOAT32	Hz	1 Minute
X		2002	2003	Power Factor A	2	FLOAT32	–	1 Minute
X		2004	2005	Power Factor B	2	FLOAT32	–	1 Minute
X		2006	2007	Power Factor C	2	FLOAT32	–	1 Minute

EM4300	EM4399	Address	Register	Description	Size	Data Type	Units	Update Frequency
X	X	2008	2009	Apparent Power A	2	FLOAT32	VA	1 Minute
X	X	2010	2011	Apparent Power B	2	FLOAT32	VA	1 Minute
X	X	2012	2013	Apparent Power C	2	FLOAT32	VA	1 Minute
X	X	2014	2015	Apparent Power	2	FLOAT32	VA	1 Minute
X		2016	2017	Reactive Power A	2	FLOAT32	VAR	1 Minute
X		2018	2019	Reactive Power B	2	FLOAT32	VAR	1 Minute
X		2020	2021	Reactive Power C	2	FLOAT32	VAR	1 Minute
X		2022	2023	Reactive Power	2	FLOAT32	VAR	1 Minute
X	X	2024	2025	Active Power A	2	FLOAT32	W	1 Minute
X	X	2026	2027	Active Power B	2	FLOAT32	W	1 Minute
X	X	2028	2029	Active Power C	2	FLOAT32	W	1 Minute
X	X	2030	2031	Active Power	2	FLOAT32	W	1 Minute
X	X	2032	2033	Voltage A-N	2	FLOAT32	V	1 Minute
		2034	2035	Reserved	266	-	-	-
X	X	2100	2101	Max Current A over Dmd	2	FLOAT32	A	15 Minute
X	X	2102	2103	Max Current B over Dmd	2	FLOAT32	A	15 Minute
X	X	2104	2105	Max Current C over Dmd	2	FLOAT32	A	15 Minute
X	X	2106	2107	Min Voltage A-N over dmd	2	FLOAT32	V	15 Minute
X	X	2108	2109	Min Voltage B-N over dmd	2	FLOAT32	V	15 Minute
X	X	2110	2111	Min Voltage C-N over dmd	2	FLOAT32	V	15 Minute
		2113	2114	Reserved	187	-	-	-
X		2300	2301	Apparent energy delivered - received non-resettable	4	INT64	VAh	1 Minute
X		2304	2305	Apparent energy A delivered - received non-resettable	4	INT64	VAh	1 Minute
X		2308	2309	Apparent energy B delivered - received non-resettable	4	INT64	VAh	1 Minute
X		2312	2313	Apparent energy C delivered - received non-resettable	4	INT64	VAh	1 Minute
X		2316	2317	Reactive energy delivered - received non-resettable	4	INT64	VARh	1 Minute
X		2320	2321	Reactive energy A delivered - received non-resettable	4	INT64	VARh	1 Minute
X		2324	2325	Reactive energy B delivered - received non-resettable	4	INT64	VARh	1 Minute
X		2328	2329	Reactive energy C delivered - received non-resettable	4	INT64	VARh	1 Minute
X		2332	2333	Active energy delivered - received non-resettable	4	INT64	Wh	1 Minute
X		2336	2337	Active energy A delivered - received non-resettable	4	INT64	Wh	1 Minute

EM4300	EM4399	Address	Register	Description	Size	Data Type	Units	Update Frequency
X		2340	2341	Active energy B delivered - received non-resettable	4	INT64	Wh	1 Minute
X		2344	2345	Active energy C delivered - received non-resettable	4	INT64	Wh	1 Minute
X		2348	2349	Apparent energy delivered - received	4	INT64	VAh	1 Minute
X		2352	2353	Apparent energy A delivered - received	4	INT64	VAh	1 Minute
X		2356	2357	Apparent energy B delivered - received	4	INT64	VAh	1 Minute
X		2360	2361	Apparent energy C delivered - received	4	INT64	VAh	1 Minute
X		2364	2365	Reactive energy delivered - received	4	INT64	VARh	1 Minute
X		2368	2369	Reactive energy A delivered - received	4	INT64	VARh	1 Minute
X		2372	2373	Reactive energy B delivered - received	4	INT64	VARh	1 Minute
X		2376	2377	Reactive energy C delivered - received	4	INT64	VARh	1 Minute
X		2380	2381	Active energy delivered - received	4	INT64	Wh	1 Minute
X		2384	2385	Active energy A delivered - received	4	INT64	Wh	1 Minute
X		2388	2389	Active energy B delivered - received	4	INT64	Wh	1 Minute
X		2392	2393	Active energy C delivered - received	4	INT64	Wh	1 Minute
		2396	2397	Reserved	16	–	–	–
X	X	2412	2413	ZigBee link quality indicator (LQI)	1	INT16U	–	<< 1 Minute
X	X	2413	2414	ZigBee radio signal strength indicator (RSSI)	2	FLOAT32	dBm	<< 1 Minute
X	X	2415	2416	Zigbee packet error rate over last hour	2	FLOAT32	–	<< 1 Minute
X	X	2417	2418	ZigBee network extended network PAN ID 1	4	INT64U	–	<< 1 Minute
X	X	2421	2422	Zigbee radio output Power	2	FLOAT32	dBm	<< 1 Minute
		2423	2424	Reserved	77	–	–	–
	X	2500	2501	Apparent energy delivered + received non resettable	4	INT64	VAh	1 Minute
	X	2504	2505	Apparent Energy A Delivered + Received non resettable	4	INT64	VAh	1 Minute
	X	2508	2509	Apparent Energy B Delivered + Received non resettable	4	INT64	VAh	1 Minute
	X	2512	2513	Apparent Energy C Delivered + Received non resettable	4	INT64	VAh	1 Minute
		2514	18	Reserved	16	–	–	–
	X	2532	2533	Active energy delivered + received non resettable	4	INT64	Wh	1 Minute

EM4300	EM4399	Address	Register	Description	Size	Data Type	Units	Update Frequency
	X	2536	2537	Active Energy A Delivered + Received non resettable	4	INT64	Wh	1 Minute
	X	2540	2541	Active Energy B Delivered + Received non resettable	4	INT64	Wh	1 Minute
	X	2544	2545	Active Energy C Delivered + Received non resettable	4	INT64	Wh	1 Minute
	X	2548	2549	Apparent energy delivered + received	4	INT64	VAh	1 Minute
	X	2552	2553	Apparent Energy A Delivered + Received	4	INT64	VAh	1 Minute
	X	2556	2557	Apparent Energy B Delivered + Received	4	INT64	VAh	1 Minute
	X	2560	2561	Apparent Energy C Delivered + Received	4	INT64	VAh	1 Minute
		2562	18	Reserved	16	–	–	–
	X	2580	2581	Active energy delivered + received	4	INT64	Wh	1 Minute
	X	2584	2585	Active Energy A Delivered + Received	4	INT64	Wh	1 Minute
	X	2588	2588	Active Energy B Delivered + Received	4	INT64	Wh	1 Minute
	X	2592	2593	Active Energy C Delivered + Received	4	INT64	Wh	1 Minute

TH110 and CL110 Modbus Mapping

The following values can be read only through Modbus function codes FC03-FC04.

TH110	CL110	Address	Register	Description	Size	Data Type	Units
X	X	7937	31032	Product Code	1	INT16U	–
X	X	F9F	4001	Temperature	2	FLOAT32	°C
	X	FA5	4007	Relative Humidity	2	FLOAT32	–
	X	CF2	3316	Battery Voltage	2	FLOAT32	V
X	X	79B2	31156	ZigBee Link Quality Indicator (LQI) Gateway	1	INT16U	–
X	X	79B0	31154	ZigBee radio signal strength indicator (RSSI) Gateway	2	FLOAT32	dBm

Related Topics

- Firewall Management
- Selecting Measurements to Log or Publish

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.schneider-electric.com

As standards, specifications, and design change from time to time,
please ask for confirmation of the information given in this publication.

© 2020 – Schneider Electric. All rights reserved.

DOCA0036EN-15