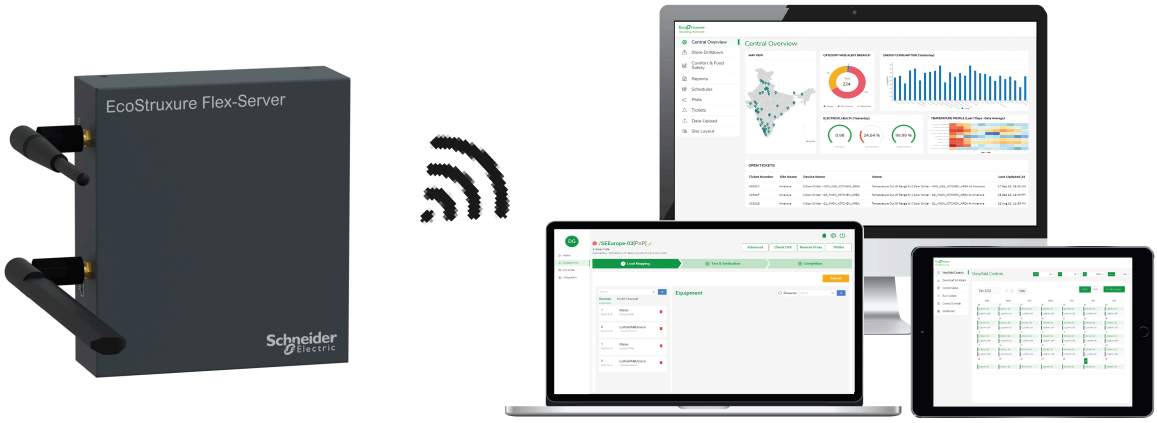
EcoStruxure™ Building Activate

User Guide

For Solution Deployment

DOCA0343EN-02

07/2025



www.se.com

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

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

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time 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 document, as well as any non-intended use or misuse of the content thereof.

Table of Contents

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 documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this 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 follow 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.

⚠ 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 and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

About the Document

Document Scope

This guide provides complete information to assist in installation and deployment of the EcoStruxure™ Building Activate.

This guide describes the following key points:

- EcoStruxure™ Flex-Server installation.
- Field troubleshooting

This guide is intended for:

- Technicians
- Maintenance Engineer
- Partners

Validity Note

This guide is valid for the IoT-enabled, plug-and-play, open, interoperable architecture, platform, and buildings.

The characteristics of the products described in this document are intended to match the characteristics that are available on www.se.com. As part of our corporate strategy for constant improvement, we may revise the content over time to enhance clarity and accuracy. If you see a difference between the characteristics in this document and the characteristics on www.se.com, consider www.se.com to contain the latest information.

General Cybersecurity Information

In recent years, the growing number of networked machines and production plants has seen a corresponding increase in the potential for cyber threats, such as unauthorized access, data breaches, and operational disruptions. You must, therefore, consider all possible cybersecurity measures to help protect assets and systems against such threats.

To help keep your Schneider Electric products secure and protected, it is in your best interest to implement the cybersecurity best practices as described in the Cybersecurity Best Practices document.

Schneider Electric provides additional information and assistance:

- Subscribe to the Schneider Electric security newsletter.
- Visit the Cybersecurity Support Portal web page to:
  - Find Security Notifications.
  - Report vulnerabilities and incidents.
- Visit the Schneider Electric Cybersecurity and Data Protection Posture web page to:
  - Access the cybersecurity posture.
  - Learn more about cybersecurity in the cybersecurity academy.
  - Explore the cybersecurity services from Schneider Electric.

Environmental Data

For product compliance and environmental information, refer to the Schneider Electric Environmental Data Program.

Available Languages of the Document

The document is available in these languages:

- English
- French

Related Documents

Title of documentation	Reference number
Cybersecurity Best Practices	General Cybersecurity Information, page 6
EcoStruxure™ Flex-Server Technical Datasheet	EXBED324401EN EXBED324401FR
EcoStruxure™ Flex-Server Installation Sheet	ZEN0000102
EcoStruxure™ Building Activate Cybersecurity Hardening Guide	DOCA0396EN-00

To find documents online, visit the Schneider Electric download center (www.se.com/ww/en/download/).

Information on Non-Inclusive or Insensitive Terminology

As a responsible, inclusive company, Schneider Electric is constantly updating its communications and products that contain non-inclusive or insensitive terminology. However, despite these efforts, our content may still contain terms that are deemed inappropriate by some customers.

Precautions

General Precautions

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, damage, or improper operating results.

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION OR ARC FLASH

- Turn off all power supplying this equipment before working on or inside equipment.
- Always use a properly rated voltage sensing device to confirm power is off.

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

⚠WARNING

UNINTENDED OPERATION

- 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.

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

⚠WARNING

INACCURATE DATA RESULTS

- Do not incorrectly configure the software, as this can lead to inaccurate reports and data results.
- Do not plan 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, or equipment damage.

Environmental Precautions

To take the measures to conserve the environment, it is recommended to follow the steps for the disposal of packages, products, or batteries:

Package Disposal

The following package disposal rules must follow:

- The exceptions detailed in the First Additional Provision of Law 11/1997 on commercial or industrial packaging states that the final holder of the waste of used containers and packaging must deliver the waste to an authorized recuperator, recycler, or revalue in proper conditions for reuse.
- The subsets of the system are recyclable products and cannot be treated as household or municipal waste at the end of its useful life.
- To preserve the environment, manage the waste in accordance with the current environmental regulations and requirements in each country or community. For any assistance, consult the manufacturer.

Product Disposal

The following product disposal rules must follow:

- The electrical-electronic device (AEE) is marked with the symbol of compliance with the European Directive 2012/19 / EU (WEEE) regarding used electrical and electronic equipment (waste electrical and electronic equipment WEEE, RD 110/2015).
- The directive provides the general framework valid throughout the European Union for the removal and reuse of waste from EEE.
- To dispose off the product and to ensure its proper management, follow the current local environmental legislation and regulations. In this way, it will contribute to environmental conservation.
- The wheeled bin crossed out on the product, in the documentation or on its packaging, means that the electrical-electronic devices and batteries must be collected separately at the end of their life cycle.
- According to the current local legislation and environmental regulations, before the deposit of the RAEE (waste generated from appliances, instruments and devices powered by electricity or batteries) in their collection facilities, the batteries must be removed and deposited separately from the rest of the RAEE for proper management.
- Never dispose the product or its associated equipment with household waste.
- The symbols marked on the product are valid in the European Union and in those places where separate collection systems are available.

Cybersecurity Safety Notice

⚠WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default passwords at first use to help prevent unauthorized access to device settings, controls, and information.
- Disable unused ports/services and default accounts to help minimize pathways for malicious attackers.
- 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, or interruption of services.

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

EcoStruxure™ Building Activate

What's in This Part

Introduction

EcoStruxure™ Master Range

EcoStruxure™ is Schneider Electric's IoT-enabled, plug-and-play, open, interoperable architecture, platform, and buildings. Innovation at every level from connected products to edge control, and applications, analytics, and services.

Overview

EcoStruxure™ Flex-Server is a multi-protocol IoT gateway that has been designed specifically for commercial applications. It enables businesses to perform bi-directional data or control communication between a range of sensors and devices on-premises and cloud. Exposed physical interfaces include RS485, USB ports, power connector, LEDs, and Ethernet.

System Features and Benefits

The features and benefits of Industrial or Commercial grade Flex-Server are:

- Running standard Linux operating system.
- Fanless operation.
- Remote bidirectional connectivity between cloud and Flex-Server over a VPN.
- Remotely manage all gateways from a single portal.
- Role-based access control for Flex-Server management for different users.
- Remotely configure connected devices on the Flex-Server over the supported protocols.
- Pre-supported library of hundreds of devices.
- Remote health monitoring and management.

Supported Gateways

The supported gateways are listed below:

- LoRa connector - RAK Wireless 7371 - D10005

Box Contents

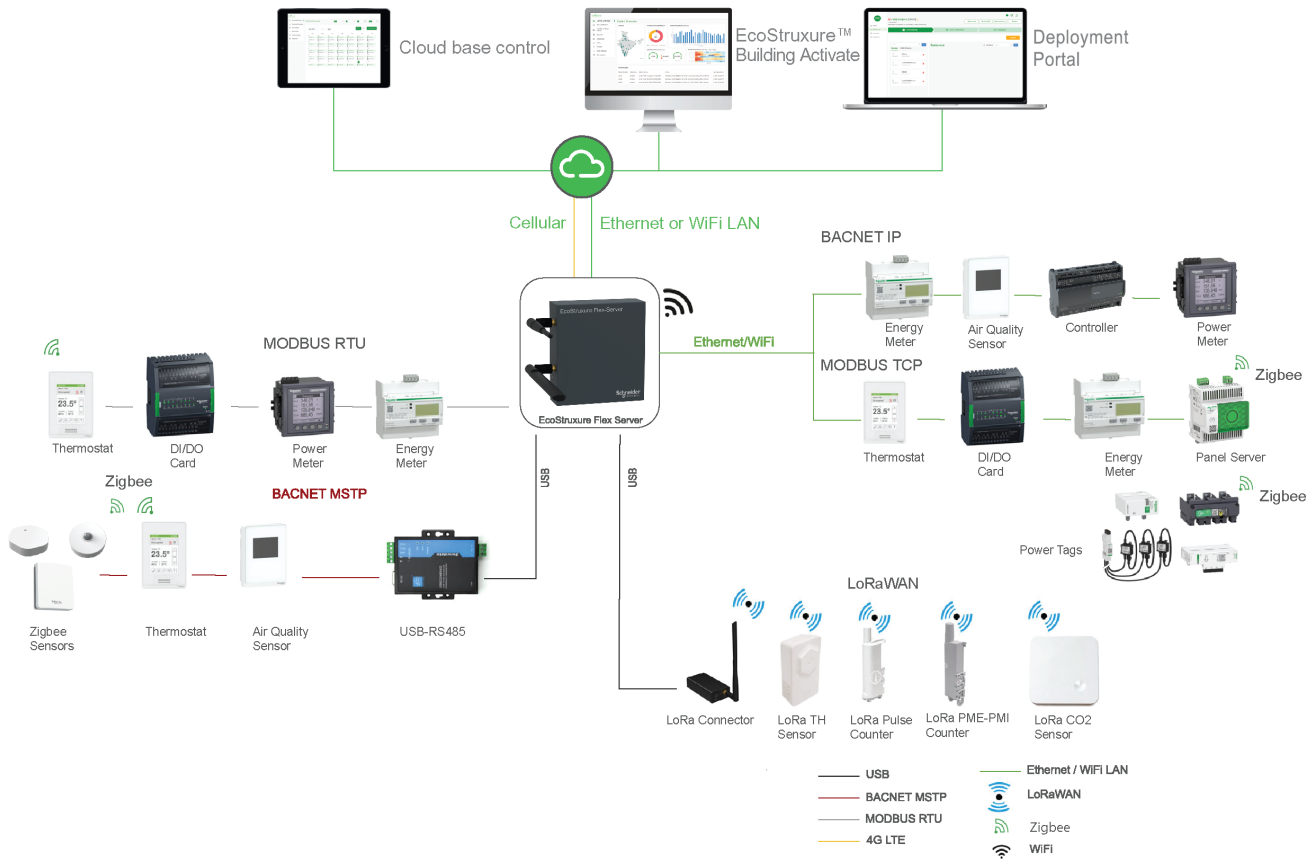
The box contains the listed parts:

- EcoStruxure™ Flex-Server IoT gateway
- Power supply
- 4G antenna
- Wi-Fi antenna
- Four M3 x 6 mm screws flat head
- Four M4 x 25 mm self-tapping screws
- Installation guide
- Mounting Bracket for Flex-Server

- Mounting bracket for LoRa and RS485

Architecture

The sample architecture of the EcoStruxure™ Flex-Server is shown in the following diagram:



Technical Specifications

Technical Characteristics

Characteristics	Values
Physical Characteristics	
Enclosure	Steel enclosure with powder coating with two external SMA connectors for antenna
Mechanical	
Dimensions	Ethernet: 137 x 124 x 41 mm Ethernet+Cellular: 137 x 194 x 41 mm Ethernet+Cellular+Wi-Fi: 137 x 194 x 41 mm
Weight	Ethernet: 503 g Ethernet+Cellular: 528 g Ethernet+Cellular+Wi-Fi: 558 g
RAM	1GB LPDDR4-3200 SDRAM
Storage	8GB eMMC
Processor	Quad core Cortex-A72 (ARM v8) 64-bit SoC @ 1.5 GHz
Connectors	1x RS485, 2x USB2.0 Type A, 1x 10/100 Ethernet
Electrical Characteristics	
Power Supply	11...24 V DC (12 V DC, 25 W (included in the box))
Communication Characteristics	
Wi-Fi	Dual Band Wi-Fi with external Omnidirectional antenna
LTE	1 X LTE/3G/2G with external Omnidirectional antenna
Environmental Characteristics	
Environmental Conditions	Indoor Use Only
Ambient Air Temperature	0...45 °C
Storage Temperature	-20...65 °C
Humidity	0...95%
Installation	
Mounting	Wall-Mounted
Installation Equipment Included	Installation instructions, mounting brackets, and screws
Certifications and Compliances	CE, UKCA, RoHS, and REACH

NOTE: Battery is not being installed/recommended in the below Commercial References used for UL Certifications: ESXBFXSVRBCW008, , ESXBFXSVR0BC008, and ESXBFXSVR00B008.

Optional Accessories

Reference Number	Description
D10005	LoRA Connector RAK7371 EU868
D16011	LoRA Connector RAK7371 US915

Flex-Server Guidelines

Parameters	Maximum Number
Flex-Server	
Maximum number of total devices (all protocols combined)	50
Maximum number of controlled points (all devices combined)	500
BACnet	
Maximum number of BACnet MS/TP devices per network	32*
Maximum number of BACnet MS/TP networks per server	2**
Maximum number of BACnet IP devices	50
Point Types	
Analog values	500
Digital values	500
Multi-state values	500
Analog input	500
Digital input	500
Multi-state input	500
Analog output	500
Digital output	500
Multi-state output	500
Modbus	
Maximum number of Modbus RTU devices per RS485 port	32*
Maximum number of RS485 ports	2**
Maximum number of Modbus TCP devices	50
LoRa* **	
Maximum number of LoRa sensors per server (100 messages per day)	50
Maximum number of points	50
SNMP Client (V1 & V3) **Function**	
Maximum number of SNMP devices (1024 Read/Write per device)	10

NOTE: *Maximum number of devices according to protocol specifications and guidelines.

NOTE: ***LoRa distances - LoRa is noted for its long range and deep penetration. LoRa transmissions can penetrate glass, metal, and concrete found in most buildings. Radio's antenna and installation can affect the range of LoRa sensors. You must test the transmission and signal strength when you install wireless devices.

Cable Specifications

Parameter	Details
Type	Shielded twisted pair low capacitance
Twisted wire size	22 AWG to 24 AWG (0.33 mm^2 to 0.20 mm^2)
Characteristic impedance	120 ohms
Capacitance (wire to shield)	< 82 pF/m (< 25 pF/ft)
Capacitance (wire to wire)	< 46 pF/m (< 14 pF/ft)
Distributed capacitance	Less than 100 pF per meter (30 pF per foot)
Maximum length per segment	1200 m (4000 ft) Note: depending on termination and bias restrictions
Polarity	Polarity sensitive
Multi-drop	Daisy-chain (no T-connections)
Terminations	1. Devices are installed at both ends of RS485 network: 120 Ohms resistors should be installed at each end. 2. A device is installed at one end of RS485 network and a their-party devices is installed at the other end. Install an End-Of-Line resistor value that matches the third-party device instructions on the End-Of-Line resistors. 3. Third-party devices are installed at both ends of RS485 network. Follow the third-party device instructions on the End-Of-Line resistors.
Network bias resistors	510 ohms per wire (maximum two sets per segment)
Maximum number of nodes per segment	32
Baud rates supported	9600, 19200, 38400, 57600, 76800, 115200 (Auto detect is not supported)

Commercial Reference Number

Commercial Reference Number	Description
ESXBFXSVR00B008	ESXB Flex-Server, Ethernet, RS485, 8GB storage
ESXBFXSVR0BC008	ESXB Flex-Server, Ethernet, RS485, cellular, 8GB storage
ESXBFXSVRBCW008	ESXB Flex-Server, Ethernet, RS485, cellular, Wi-Fi, 8GB storage

Regulatory Compliance

FCC Compliance Statement (USA)

ESXBFXSVRBCW008: ESXB Flex-Server, Ethernet, RS485, cellular, Wi-Fi, 8GB storage

FCC ID: 2BATG- ESXBFXSVRBCW

ESXBFXSVR0BC008: ESXB Flex-Server, Ethernet, RS485, cellular, 8GB storage

FCC ID: 2BATG- ESXBFXSVR0BC

Compliance Statements: This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including, an interference that may cause undesired operation.

Caution Statements:

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This equipment should be installed and operated with a minimum distance of 200 mm between the radiator and your body.

Industry Canada (IC) Compliance Statement

ESXBFXSVRBCW008: ESXB Flex-Server, Ethernet, RS485, cellular, Wi-Fi, 8GB storage

IC: 30486-FXSVRBCW

ESXBFXSVR0BC008: ESXB Flex-Server, Ethernet, RS485, cellular, 8GB storage

IC: 30486-FXSVR0BC

Compliance Statements: This device complies with Industry Canada license exempt RSS standard(s). Operation is subject to the following two conditions:

- This device may not cause interference.
- This device must accept any interference, including interference that may cause undesired operation of the device.

Déclarations de conformité: Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

- l'appareil ne doit pas produire de brouillage, et.
- l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement

Caution Statements:

- This equipment complies with radio frequency exposure limits set forth by Industry Canada for an uncontrolled environment.
- This equipment should be installed and operated with a minimum distance of 200 mm between the device and the user or bystanders.

Déclarations de mise en garde:

- Cet équipement est conforme aux limites d'exposition aux radiofréquences défines par Indstrie Canada pourun environment non contrôlé.
- Cet équipement doit être installé et utilisé aven un minimum de 20 cm de distance dispositif et l'utilisateur ou des tiers.

INFORMATION TO THE USER

For Class A and Class B digital devices, information to the user is required to include the following statements (Section 15.105):

1. For a Class A digital device or peripheral, the instructions furnished to the user shall include the following or similar statement, placed in a prominent location in the text of the manual:

   NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

2. For a Class B digital device or peripheral, the instructions furnished to the user shall include the following or similar statement, placed in a prominent location in the text of the manual:

   NOTE: 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 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 into 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.

Unboxing the Flex-Server

To unbox the Flex-Server, perform the following steps:

1. Unbox the Flex-Server after you receive it.

   NOTE: The Flex-Server is received in two layers of packaging, the shipping box and the product packaging.

2. Remove the outside packaging and arrange the Flex-Server in an organized manner.

Cord and Plug Connections

NOTICE

WIRE INSULATION DAMAGE

- Ensure that all pathways and raceways used for routing and storing conductors are free of rough, sharp, or moving parts to prevent damage to conductor insulation.
- Ensure that the connectors are inserted properly to avoid any loose connections.
- Ensure that the striped wire length is as per the specifications given in the manual. The screws are fastened to ensure the reliability of connections.

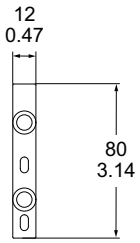
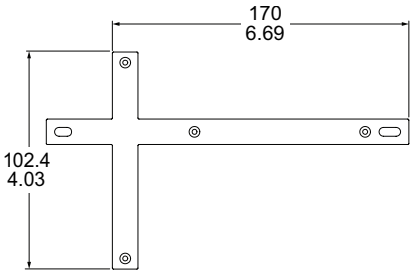
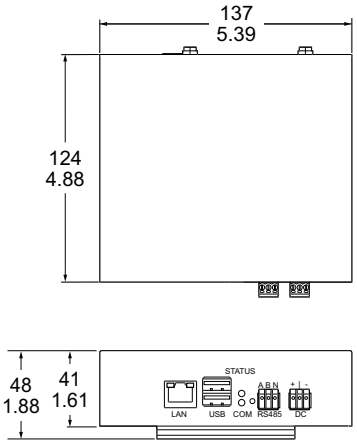
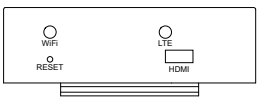
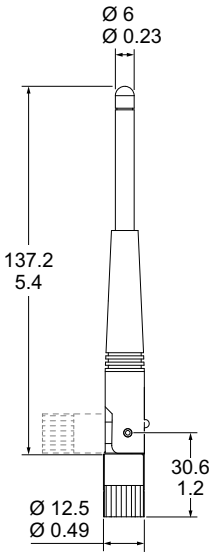
Failure to follow these instructions can result in equipment damage.

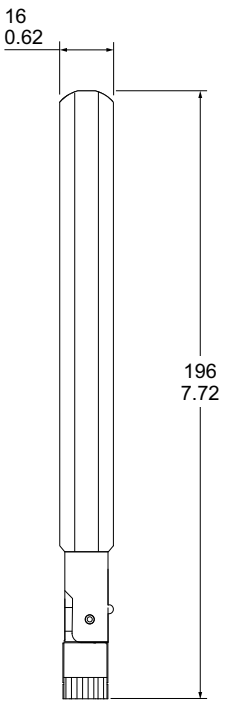
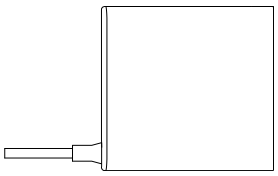
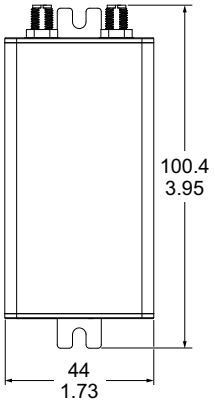
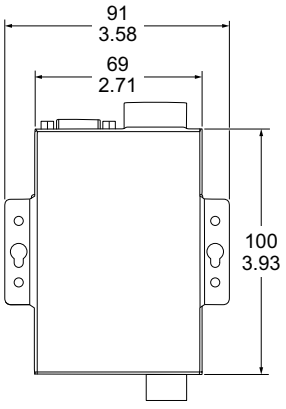
NOTE:

- Use a Class 2 external power supply in case the supplied power supply is not being used.
- Follow the install instructions of the power supply used.
- For the DC connections of the Flex-Server. refer to the instruction sheet.
- Use a heat shrink tube to secure the loose insulated conductors.

Assembling the Flex-Server

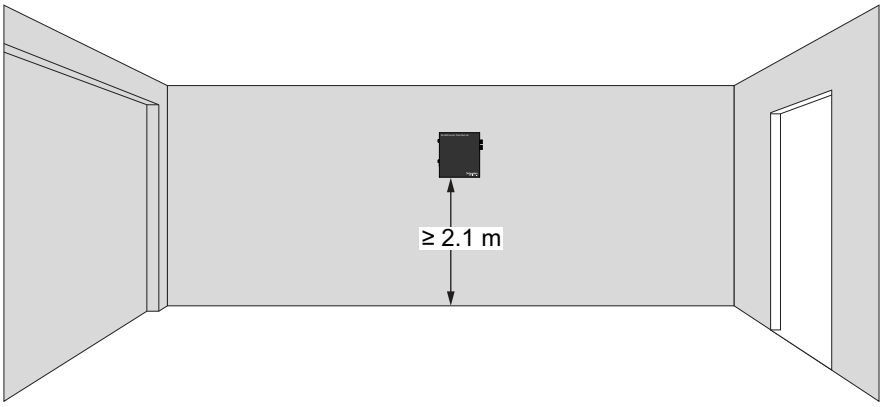
Refer to the below table for physical description and dimensions:

Description	Image
Mounting bracket for Flex-Server	
Mounting bracket for LoRa and RS485	
Flex-Server dimensions	
Flex-Server	
Wi-Fi antenna	

4G antenna	
Power supply	
LoRa Connector	
RS485 Converter	

Perform the following steps to install the Flex-Server on mounting bracket with power supply:

NOTE: The Flex-Server must be installed ≥ 2.1 m (6.889 ft) above the ground level:



1. Mark the positions of two drilling holes on the surface to install the mounting bracket.
2. Drill two holes using a drill bit of 6 mm diameter.
3. Install the mounting bracket on the surface with two M4 x 25 mm self-tapping screws.
4. Tighten the screws using PH1 screwdriver.
5. Slide the Flex-Server on the mounting bracket.

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION OR ARC FLASH

- Turn off all power supplying this equipment before working on or inside equipment.

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

6. Do the necessary wiring. Refer to the *EcoStruxure™ Flex-Server Installation Sheet - ZEN0000102*.

   NOTE: Use 0.2 A fuse with appropriate line to main voltage between AC power supply and mains.

Perform the following steps to install the LoRa connector and RS485I on mounting bracket:

1. Mark the positions of two drilling holes on the surface to install the mounting bracket.
2. Drill two holes using a drill bit of 6 mm diameter.
3. Install the mounting bracket on the surface with two M4 x 25 mm self-tapping screws.
4. Tighten the screws using PH1 screwdriver.
5. Install two M3 x 6 mm flat head screws on the dedicated screw slot present on mounting bracket.
6. Hang the RS485 converter on the two M3 x 6 mm flat head screws installed on the mounting bracket.
7. Install the LoRa connector on the mounting bracket with two M4 x 25 mm self tapping screws.
8. Tighten the screws using PH1 screwdriver.

Cellular Configuration:

NOTICE
REDUCED DEVICE PERFORMANCE • This device is for indoor use only and is not suitable for wet locations. • Do not install the device close to an exterior window. • When replacing a device, install the new device in the same position and direction as the replaced device. **Failure to follow these instructions can result in equipment damage.**

1. In case of a cellular configuration, open the four screws on the sides of the Flex-Server and carefully open the box, without removing the antenna cables. Insert a micro-SIM card and close the Flex-Server.
2. Attach the Wi-Fi antenna to the Wi-Fi antenna connector on Flex-Server.
3. Attach the 4G antenna to the 4G antenna connector on Flex-Server.
4. Slide the Flex-Server on the mounting bracket.
5. The new power supply has + and -ve to be connected to the Flex-Server's +ve and -ve.
6. Connect the Modbus or the BACnet to the RS485 port on the Flex-Server.
7. Connect Modbus or the BACnet to the RS485 converter using the manual provided with the RS485 converter.
8. Connect the LoRa module using the USB cable provided in the box.
9. Connect the RS485 converter with the USB cable provided in the box.
10. Plug the Power Supply Adaptor.
11. Switch on the AC mains power supply.

Support New SIM Cards in the Field

Objective

This procedure details how to support new SIM cards on field-deployed servers and ensure their details are added to the central database. This automated process eliminates the need for manual configuration of validated SIM operators on individual servers.

Prerequisites

Share the following SIM details at least one week in advance to allow for timely coordination and setup:

- SIM Operator Name
- SIM APN (Access Point Name)
- Country

Important Notes

- **The SIM card must not have a Username, Password, or PIN. These features are not supported**.
- Ensure that the SIM provider does not apply a firewall. A firewall may block connectivity. We recommend using SIMs without any firewall restrictions.
- While inserting the SIM card into the Flex-Server, ensure that you do not disturb the antenna cable. It must remain securely connected. If the cable comes out, gently click it back onto the connector labelled Main on the Cellular module.
- Check the Wi-Fi cable for ESBFXSVRBCW008, refer to Inserting SIM card.
- Ensure the SIM card's data plan is not less than 2 GB per month for approximately 100-200 streams.

Server-Side APN Handling

The server automatically handles APN settings using a script:

1. **If the APN is already configured in the database**:
   - The script automatically sets the correct APN.
   - It checks SIM connectivity.
   - If connectivity fails, manual intervention is required (see post-setup section).
2. **If the APN is not found**:
   - The script sets an empty APN.
   - In most cases, the SIM still comes online with an empty APN.

   IMPORTANT:

   - For long-term stability, we recommend correctly mapping the operator and APN in our database. If you are using a SIM for a new operator that we have never used before, please contact us so we can confirm the correct information is mapped in our system.
   - We support wherever SIM cards globally, but only with the **wsim** APN. We do not support other APNs for Wherever SIM cards.

Add a New SIM Card

1. Bring the Server Online.

   NOTE: Connect the server to the internet using Ethernet or Wi-Fi so it is remotely accessible.

2. Gently insert the new SIM card into the Flex-Server.

   NOTE: No manual configuration is required.

3. Automatic APN Detection.

   NOTE: The server will execute the automatic script as explained above.

Post-Setup (For the SIM Card with a new operator)

Once the SIM is online and verified:

- The backend team will add its details to the database.
- This enables automatic support for this operator on other servers going forward.

  NOTE: We support wherever SIM cards globally, but only with the **wsim** APN. Other APNs are not supported.

  NOTE: SIM cards listed below are supported in the database and if the SIM card is not mentioned in the list consider the SIM as new configuration and map it in our database.

Mcc code (Country Code)	Operator	APN
260	play	{"generic": "internet"}
260	plus	{"generic": "mbb.mobi-data.com"}
732	claro	{"generic": "internet.comcel.com.co"}
454	smc hk	{"generic": "Smartone"}
520	ais	{"generic": "internet"}
240	tele2 se	{"generic": "mbb.mobi-data.com"}
260	t-mobile	{"generic": "internet"}
262	t-mobile	{"generic": "internet.v6.telekom"}
505	telstra	{"generic": "telstra.internet"}
204	nl kpn	{"generic": "matooma.m2m"}
208	208 28	{"generic": "datapro"}
234	voda uk	{"generic": "wap.vodafone.co.uk"}
901	901 40	{"generic": "internet.m2mportal.de"}
208	free	{"generic": "free"}
208	bouygues telecom	{"generic": "mmsbouygtel.com"}
208	sfr	{"generic": "sl2sfr"}
208	orange	{"generic": "orange"}
268	vodafone	{"generic": "internet.vodafone.pt"}
268	nos	{"generic": "umts"}

Mcc code (Country Code)	Operator	APN
405	vi india	{"iot": "IOT.ZENATIX.COM"}
404	vi india	{"iot": "IOT.ZENATIX.COM"}
405	ind airtel	{"iot": "iot.com"}
404	ind airtel	{"iot": "iot.com"}
724	tim internet	{"generic": "timbrasil.br"}
724	vivo	{"iot": "smart.m2m.vivo.com.br", "generic": "zap.vivo.com.br"}
724	claro	{"generic": "claro.com.br"}
310	at&t	{"iot": "armstrongdynm.com.attz", "generic": "NXTGENPHONE"}
440	fl1	{"generic": "soracom.io"}
302	bell	{"generic": "mnet.bell.ca.ioe"}
302	rogers	{"generic": "M2Minternet.apn"}
302	at&t	{"iot": "armstrongdynm.com.attz", "generic": "NXTGENPHONE"}
404	idea	{"generic": "Internet"}
431	etisalat	{"generic": "mnet"}
430	etisalat	{"generic": "mnet"}
424	etisalat	{"generic": "mnet"}
424	du	{"generic": "du"}
405	404 11	{"iot": "IOT.ZENATIX.COM"}
405	vodafone	{"iot": "IOT.ZENATIX.COM"}
405	airtel	{"iot": "iot.com"}
404	airtel	{"iot": "iot.com"}
404	vodafone	{"iot": "IOT.ZENATIX.COM"}
404	404 11	{"iot": "IOT.ZENATIX.COM"}
404	jio	{"generic": "jionet"}
405	jio	{"generic": "jionet"}

User Management on Deployment Portal

Users cannot be created or managed directly from the Deployment Dashboard interface.

NOTE: User accounts for the Deployment Portal are created through by the system administrator or support team.

Potential Risks and Compensation Controls

Area	Issue	Risk	Compensating Controls
Unsecure protocols	Modbus RTU, Modbus TCP/IP, BACnet MSTP, BACnet IP and some IT protocols (DHCP, DNS, and DPWS) are unsecure. The device does not have the capability to transmit data encrypted using these protocols.	These protocols do not support encrypted data transmission. If a malicious user gains access to the network, they could intercept and manipulate communications.	• For internal networks: Physically or logically segment the network to limit access. • For external networks: Use encryption (For example: VPN) to secure data transmission.

Network Priority Configuration (Flex-Server)

The Flex-Server follows a predefined interface priority for internet connectivity. This priority determines which network interface the server uses when multiple options are available. Currently, USB takes the highest precedence, followed by the order: GSM > Ethernet > Wi-Fi.

NOTE: If the server has internet via Wi-Fi and you connect an Ethernet cable, the server will switch to Ethernet and may go offline temporarily if Ethernet does not have internet, as it will now look for internet via Ethernet.

Priority Order

The current interface priority order is:

1. USB (highest priority)
2. GSM
3. Ethernet
4. Wi-Fi

NOTE: This priority cannot be changed from the dashboard. To modify the priority order, please contact the support team.

Common Field Use Cases

Use Case	GSM	Ethernet	Wi-Fi
1	✓	✓	–
2	–	✓	–
3	✓	–	✓
4	–	✓	✓

Configuration Notes

Review the following configuration details.

- **GSM**

  The server automatically handles GSM configuration; no dashboard configuration is necessary.

  For more information, refer to Support New SIM Cards in the Field, page 25 section.

- **Ethernet and Wi-Fi**

  If you are using only Ethernet or Wi-Fi to bring the server online, DHCP configuration is sufficient.

  If you are using these interfaces to communicate with devices, we recommend static IP configuration.

  Static IP configuration is a prerequisite for proper equipment and device communication setup.

Future Scope

The ability to view and change interface priority directly from the dashboard will be introduced in future releases.

Ensuring the Flex-Server is Online

Make sure that the Flex-Server is online, and then proceed with the deployment process.

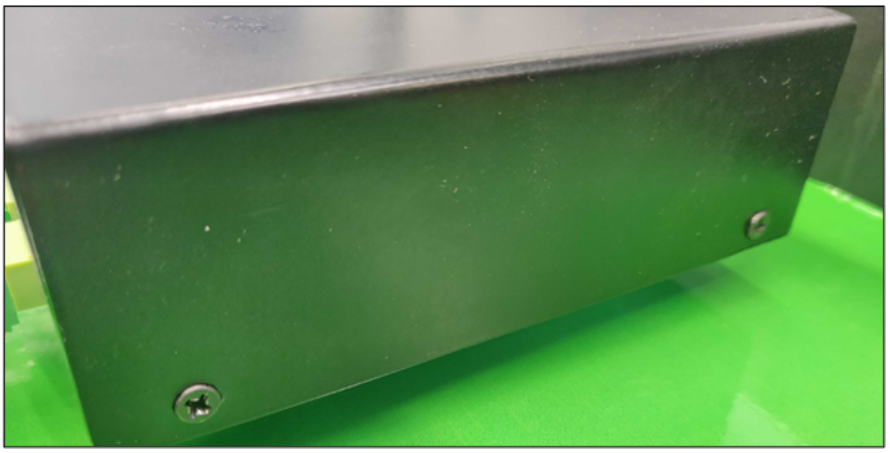
To get the kit online, you need to make sure that the Flex-Server can be connected through the internet once the Flex-Server is powered up.

NOTICE
LOSS OF COMMUNICATION • Carefully open the cover to ensure that antenna cables are not damaged. • Make sure to connect antenna cables to the correct antenna port if they are disconnected. • Take necessary precautions to avoid component damage from tools and electrostatic discharge. • When handling the product or any conductive cable/ESD-sensitive component connected to the product, wear a conductive wrist strap connected to ground through a minimum of 1 MΩ resistance. • Avoid touching exposed conductors and component leads with skin or clothing. **Failure to follow these instructions can result in equipment damage.**

There are two ways to get the Flex-Server online, through GSM and through Wi-Fi:

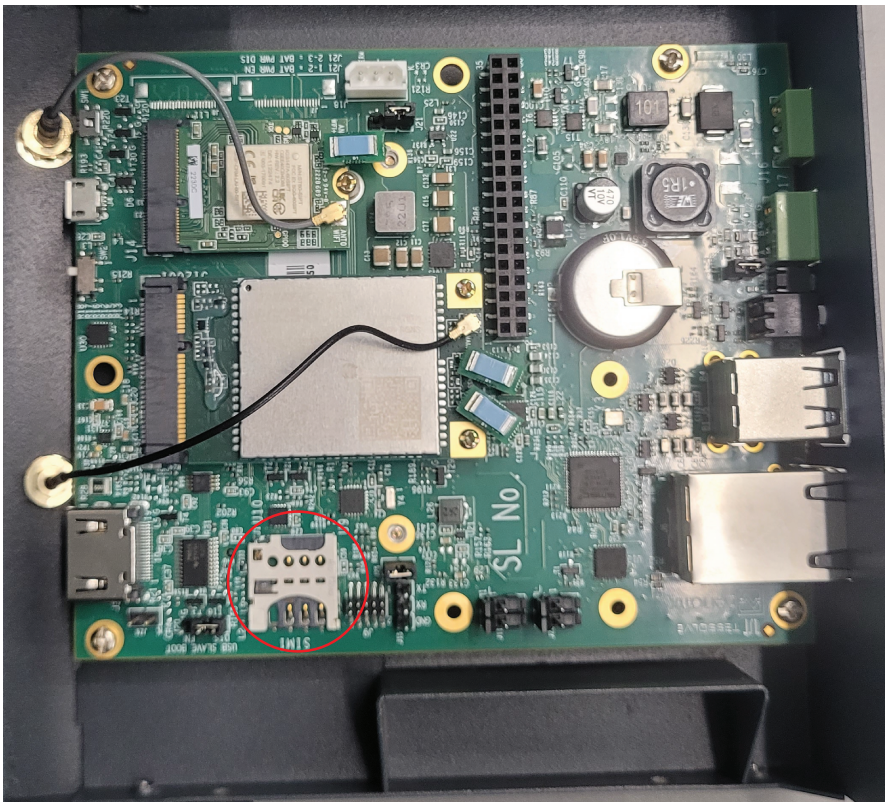
1. **Getting the Flex-Server online through GSM**:
   a. Open the Flex-Server screws and delicately remove the top cover.

      IMPORTANT: Take extra care during this step, as the top cover is connected to the antenna cable via a thin wire.



b. After opening the top cover, you will be able to see the top view of the board. Insert the active SIM card in the designated slot as shown in the image.

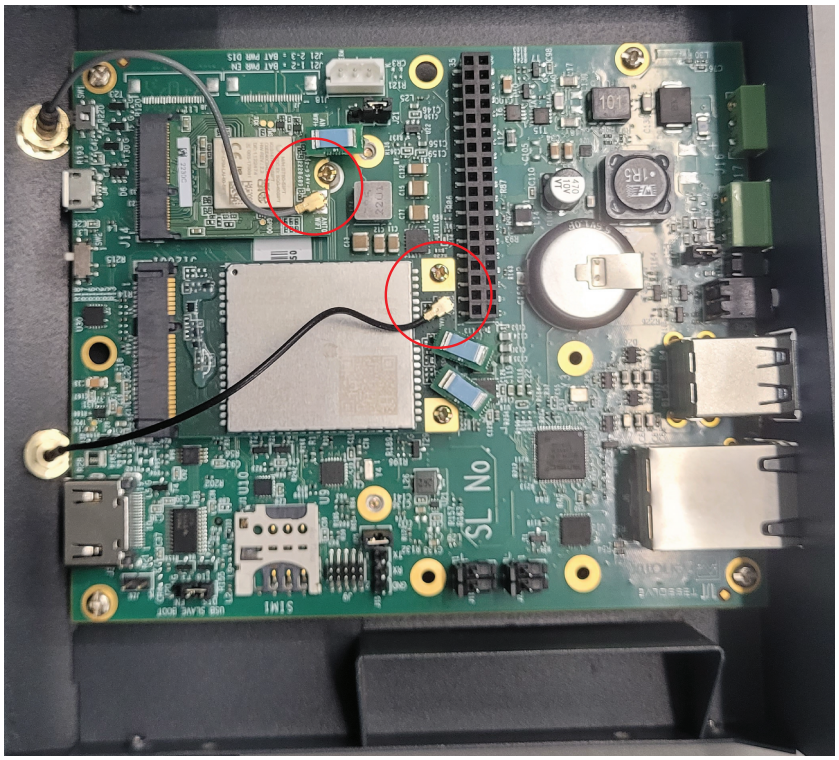
NOTE: If SIM is PIN enabled, contact www.se.com/buildings.



c. While removing the top cover of the box, if the antenna wire becomes detached from the board, you can attach it again by following these steps:

(1) After opening the top cover, carefully inspect the top view of the board.

(2) Locate the connection point labelled **MAIN** as shown in the image below.



(3) Attach the antenna wire again to the **MAIN** connection point.

d. Once the SIM card is properly placed, fix the screws back and make sure that the antenna is still attached to the Flex-Server.

NOTE: If the antenna gets removed then the GSM will not work.

e. After powering up the kit, allow the Flex-Server to boot up. This process may take up to five minutes. Once completed, the device should come online and be visible on the Deployment Portal page.

NOTE: The connectivity depends on the network of the network provider being available in the location where the Flex-Server is currently in.

2. **Getting the Flex-Server online through Wi-Fi**:

a. To get the Flex-Server online, provide a hotspot to the device with the following credentials:

- **SSID**: xxxxx
- **Password**: xxxxxxxx

NOTE: It may take up to five minutes to get online.

b. Once the Flex-Server is online, share the compute module and carrier board serial number with the commissioning engineer, so that he can initiate the provisioning process.

3. **Getting the Flex-Server Online through Ethernet**:

To get the Flex-Server online through an Ethernet network:

a. If the network uses a static IP configuration, enter the network's IP address, subnet, and gateway.

b. If the network uses DHCP, connect the cable. The Flex-Server will come online.

NOTE: It may take up to five minutes to get online.

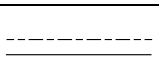
c. Share the compute module and carrier board serial number with the commissioning engineer to initiate the provisioning process.

NOTE: Fallback IP (169.254.x.x) should not be accepted (If the IP starts with this it means the DHCP server is not reachable).

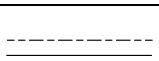
LED Indicators

LED indicators are used to check the status of the internet connection, server connection, SD card health, Flex-Server firmware health, device connection, and data transfer. Refer to the below tables for more details about top LED indicators and bottom LED indicators.

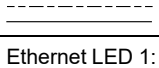
Flex-Server Status LED

Sl. No.	Indicator	Description
1		Server not functioning as expected.
2		Firmware is not healthy; internet is not connected
3		Firmware is healthy, internet is not working.
4		Connected to server, firmware is not healthy.
5		All okay.

Network Status LED

Sl. No.	Indicator	Description
1		No power.
2		Wi-Fi is ON.
3		Wi-Fi is OFF, device is searching for the network.
4		Wi-Fi is OFF, device is registered on network, but it is in an idle state.
5		Wi-Fi is OFF, internet connection is available, and data transfer is taking place successfully.
6		Wi-Fi is OFF, phone calling is taking place.
7		Wi-Fi is ON, device is not connected to the cellular network, and it is searching for the network.
8		Wi-Fi is ON, device is registered on cellular network, but it is in an idle state.
9		Wi-Fi is ON, internet connection is available, and data transfer is taking place successfully.
10		Wi-Fi is ON, phone calling is taking place.

Ethernet Status LED

Sl. No.	Indicator	Description
1		Ethernet communication is not connected.
2	Ethernet LED 1: 	Ethernet communication active.
3	Ethernet LED 2: 	Ethernet communication active.

Power LED

Sl. No.	Indicator	Description
1		No Power.
2		Flex-Server is powered.

NOTE: Press the reset button using a pin for 1-2 seconds and release for a reboot/reset.

Users

The system has three types of users, each with different permissions:

- Basic User
  - Can view all functionalities in the dashboard.
  - Cannot create, update, or delete configurations.
- Intermediate User
  - Can view and update existing configurations and functionalities.
  - Cannot create new configurations.
- Advanced User
  - Can view, update, and manage configurations.
  - Can create new configurations.

  NOTE: You cannot sign in unless at least one of the above permissions is assigned.

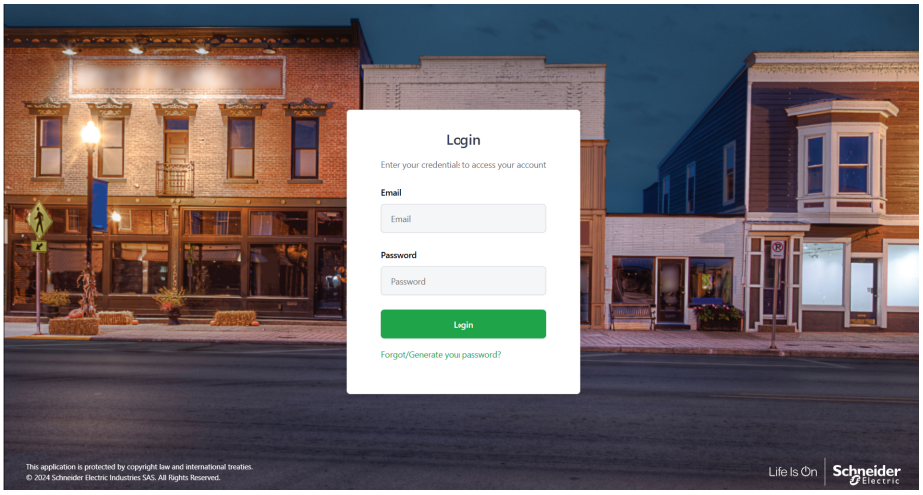
Provisioning the Flex-Server

What's in This Chapter

Perform the following steps to provision the Flex-Server.

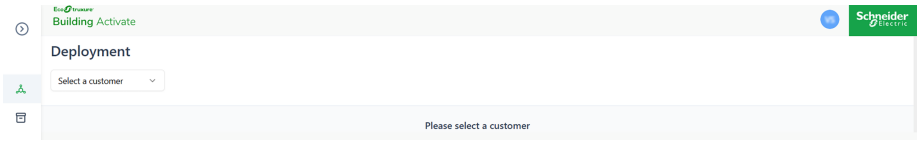
1. Power on the Flex-Server by connecting it to the power source using the power cable provided inside the box.
2. Wait for the top LED on the Flex-Server to start blinking green, this process may take up to 5 minutes.

   NOTE: The inserted SIM automatically connects the Flex-Server online and if the Flex-Server does not come online then manual intervention is needed. The option to choose between Wi-Fi or Ethernet is available in the later stages.
3. Visit the partner portal dashboard.
4. Sign in to the Deployment Portal.



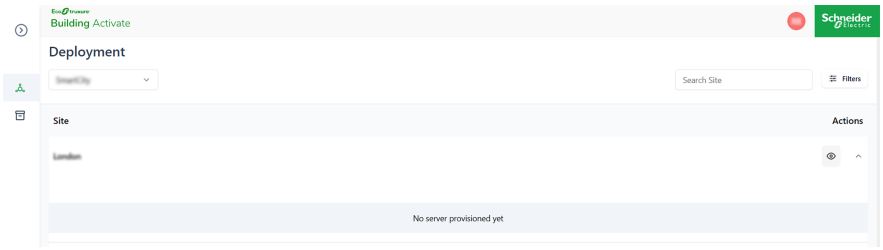
5. Click **Deployment** tab.

6. Select customer from **Select a customer** menu.

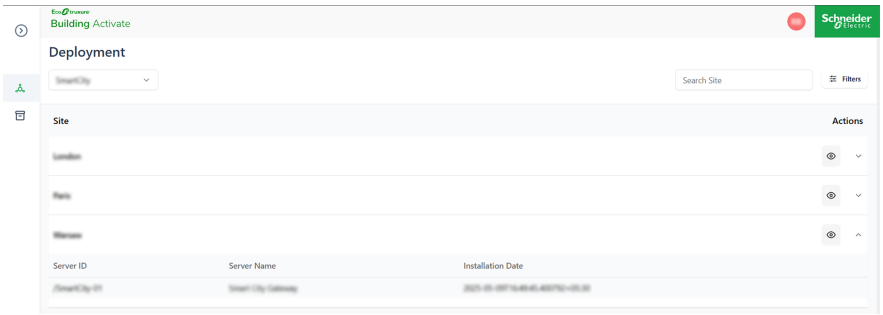


The list of associated sites appears.

- If no server is associated with a site, the system displays: *No server provisioned yet*



- A list of Flex-Server's associated with the site appears.



7. Configure a Flex-Server. For more information, refer to Configure Flex Server, page 43.

Login to Dashboard

The login flow on the deployment portal is integrated with EIAM, which uses OAuth2 to enable secure authentication on our platform.

The integration has two options to login:

- Login via SE SSO (for SE user)
- Self-register (for non-SE user)

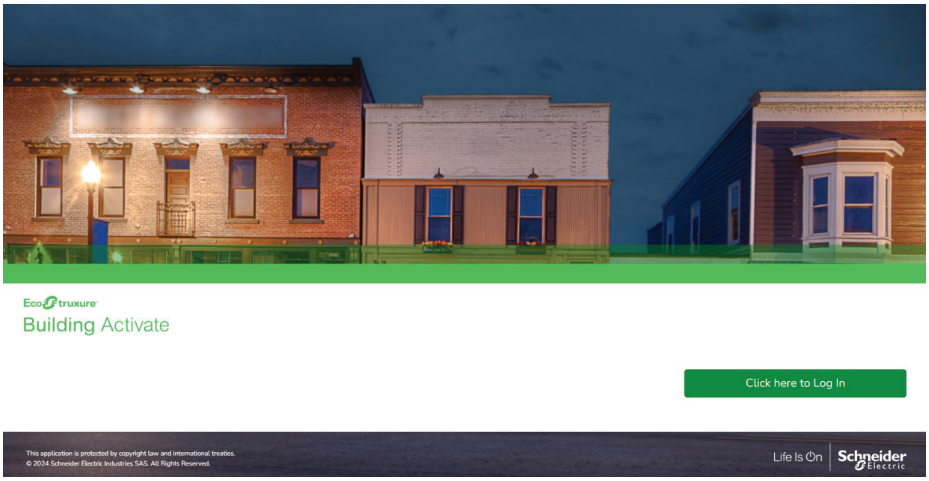
Non-SE users can login using the existing user creation process, SE users can login using SESA and password. Follow below password rules:

1. Password length should be a minimum of 10 characters
2. At least one special character (#$%^&*)
3. At least lowercase letter (a-z)
4. At least uppercase letter (A-Z)
5. At least one number (0-9)
6. Space not allowed

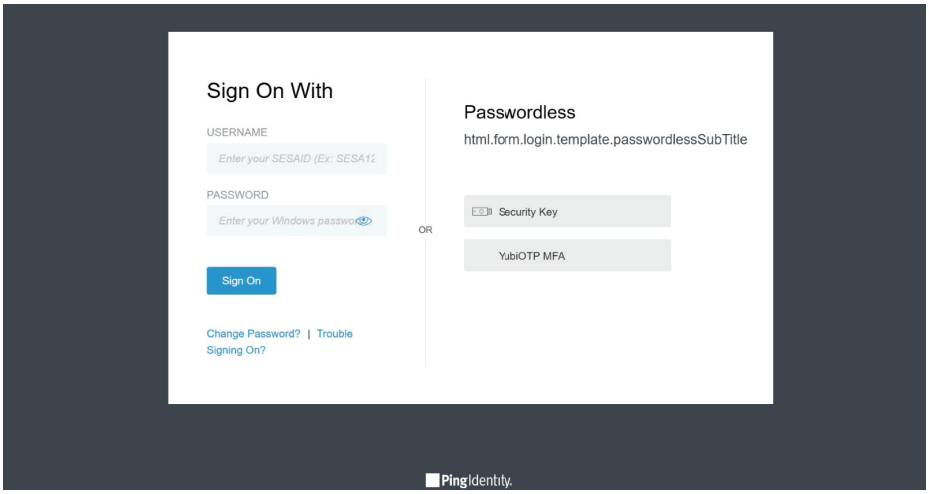
For both SE and non-SE user's login process refer to Login with SSO for SE users, page 39 Self-register for non-SE users, page 40:

Login with SSO for SE users

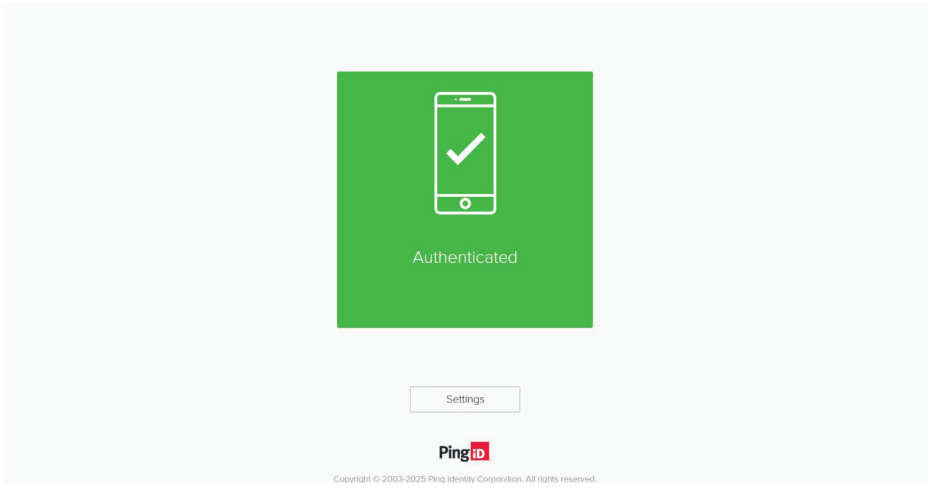
1. After accessing the deployment portal, the user will be directed to this Login page.
2. Click **Click here to Log In**.



3. Click SE **SSO** icon .
4. Enter **SESA ID** and **Password**.
5. Click **Sign On**.



6. The user needs to follow the authentication process as directed on the screen and complete the authentication through mobile.



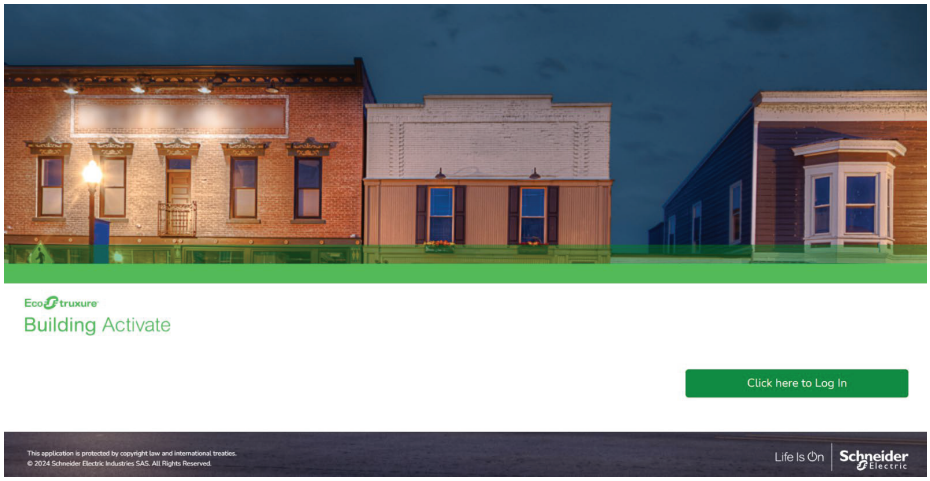
7. Once registered, users are redirected to the dashboard page.

At this stage, the user can get their account created through their account manager, allowing them to log in to the dashboard.

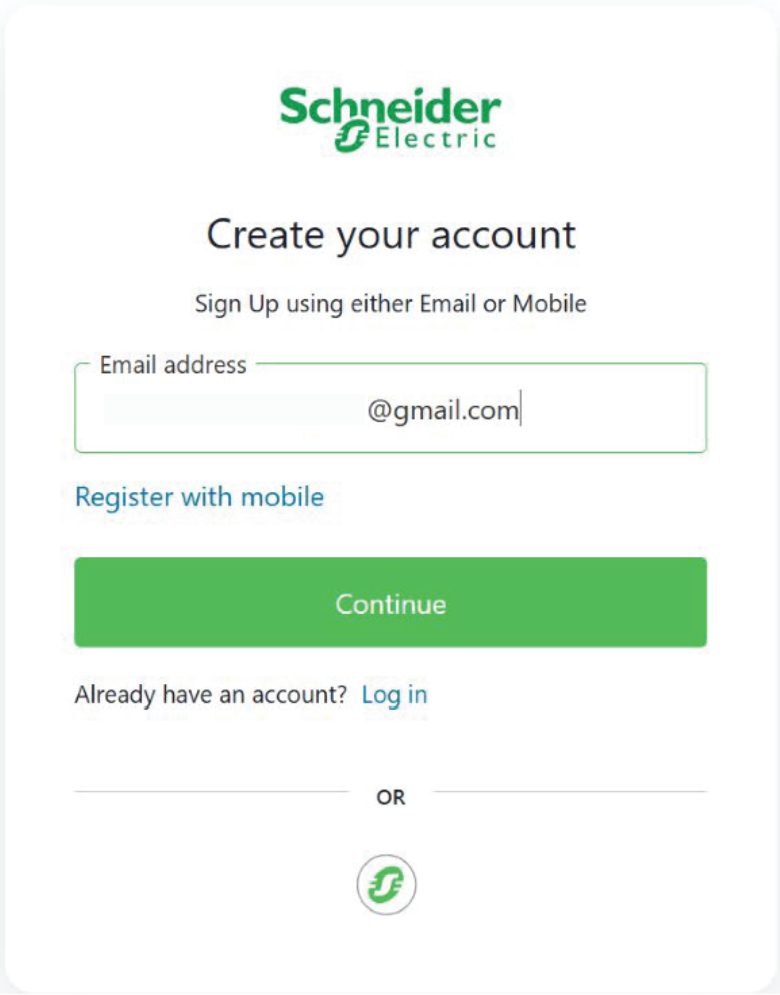
After receiving confirmation from the account manager, the user can proceed to log in to the dashboard successfully.

Self-register for non-SE users

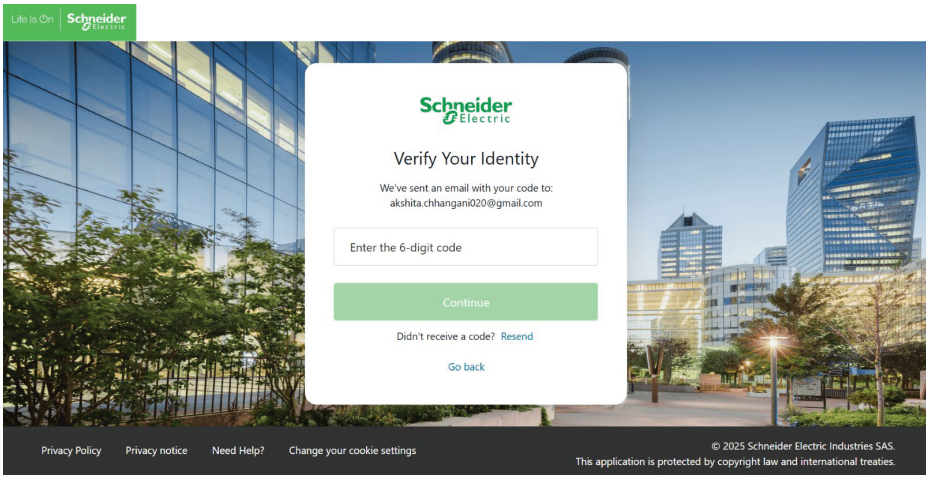
1. After accessing the deployment portal, the user will be directed to this Login page.
2. Click **Click here to Log In**.



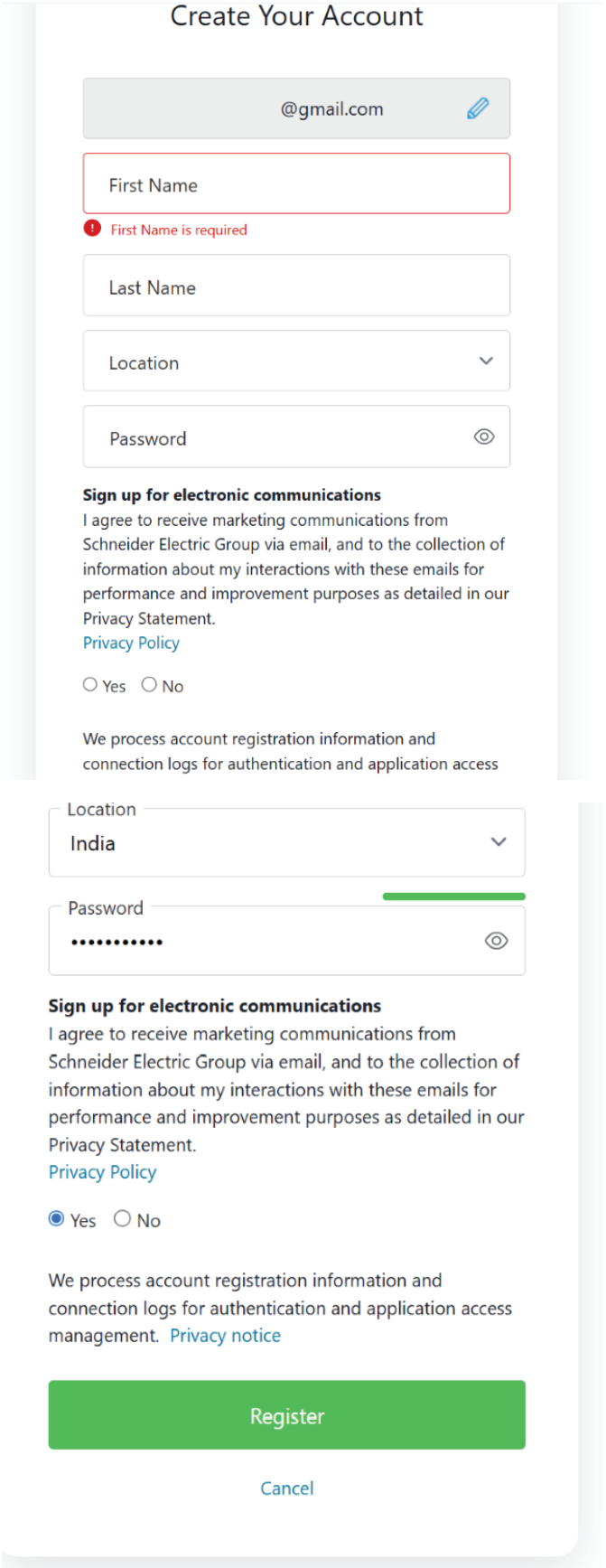
3. Enter the **Email address** and then click **Continue**.



4. You will receive a verification code on the email. Enter 6-digit verification code and then click **Continue**.



5. Enter the required details, set your **password**, and then click **Register** to complete the process.



6. Select **Yes** for privacy policy statement.
7. Once registered, users are redirected to the dashboard page.

At this stage, the user can get their account created through their account manager, allowing them to log in to the dashboard.

After receiving confirmation from the account manager, the user can proceed to log in to the dashboard successfully.

Configure Flex-Server

To configure a Flex-Server, follow the below steps:

1. Click **view** on the right of the selected site.

   The system displays two sections:

   - Site Information: This section shows the **Site name**, **Site Location**, **Latitude**, and **Longitude**.

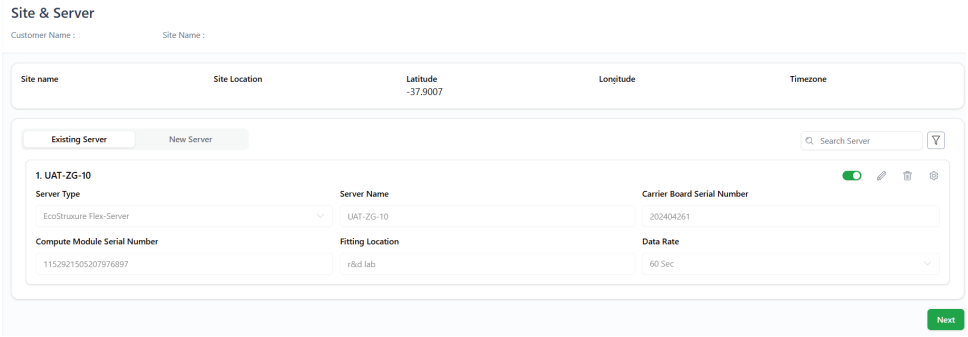
     NOTE: These parameters are pre-configured through backend and not by the user.

   - Server Information: This section contains two options:
     - **Existing Server**: Displays all configured servers if a server is already configured.
     - **New Server**: User must fill all the data. For more information, refer to Add a New Server, page 44.

Existing Server

Enable server: Server and associated devices will be visible on deployment portal and other like Customer Portal.

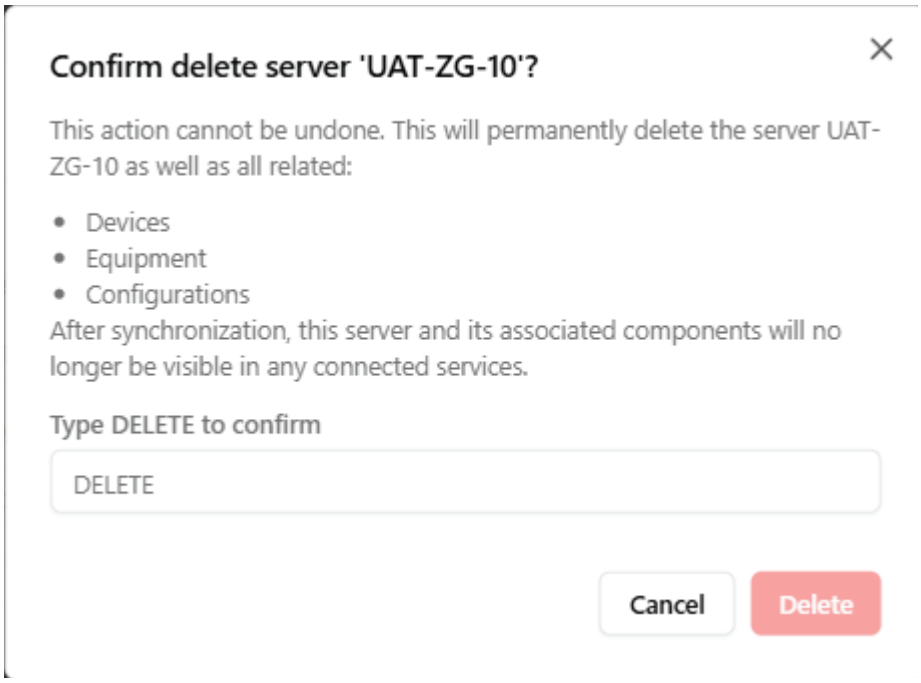
Disable server: Server will shift into the disabled list and user cannot access the associated devices and equipment in troubleshooting section on deployment portal and it will be also removed from Customer Portal.



1. To disable/enable the server, click toggle right side on top of the server card.
2. To delete the server from the site, click and type DELETE in uppercase letters.

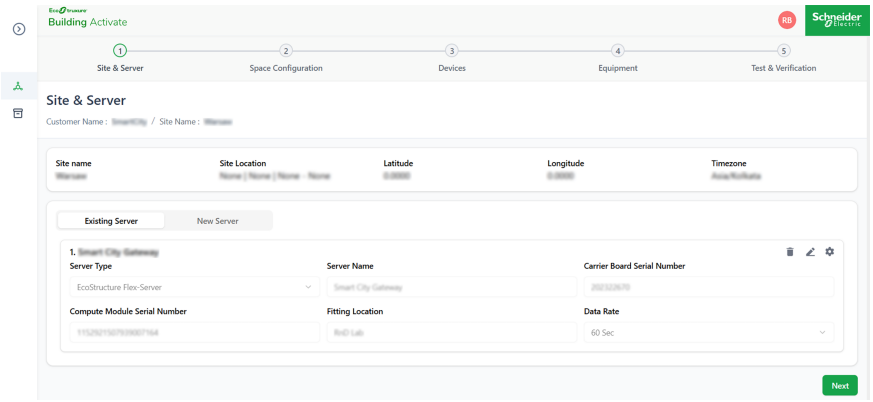
   NOTE: Enabling or disabling the server will automatically submit to the backend within 5 minutes. No manual submission is required.

3. Click **Delete**.



Add a New Flex-Server

1. Click **New Server** and fill in the following details:
   a. **Server Type**: Select Flex-Server (currently the only option available).
   b. **Server Name**: Enter a display name for the Flex-Server.
   c. **Carrier Board Serial Number**: Enter the serial number from the sticker on the Flex-Server.
   d. **Compute Module Serial Number**: Enter the compute module serial number from the sticker.
   e. **Fitting Location**: Indicate the physical location where the Flex-Server is installed.
   f. **Data Rate**: Select 60 from the drop - down menu.

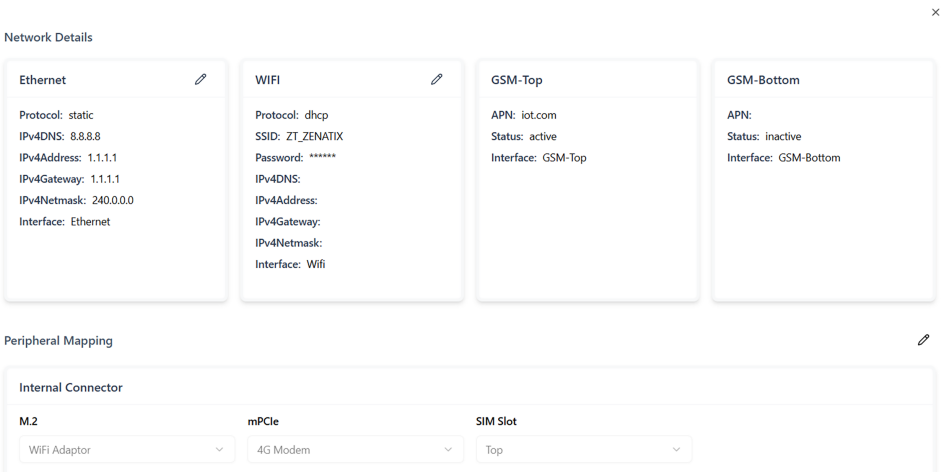


Note: Currently set to a default publishing rate of 60 seconds (not configurable).

2. Proceed to Network and Peripheral Configuration.
   After entering the required details, you will be automatically redirected to the Network and Peripheral Configuration section to continue the setup.
   a. If the server is unreachable, you will not be redirected to the Network and Peripheral Configuration page.
   b. In this case, if you navigate away from the screen, you will find the server card in the existing tab with a button labelled **Check Status**.
   c. Clicking **Check Status** will attempt to restart the provisioning process.
   d. If the server is online, you will be redirected to the Network Configuration screen to proceed with the setup

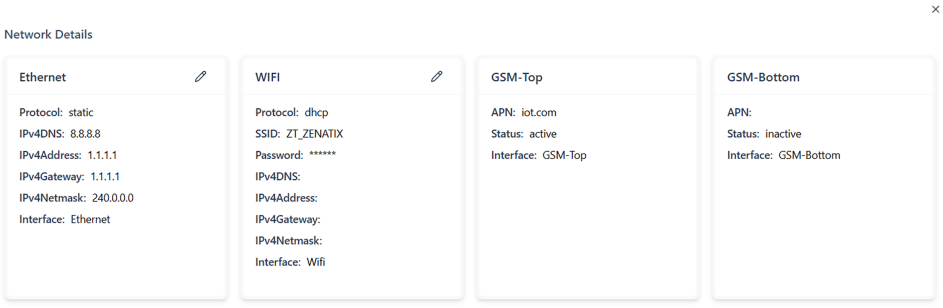
Configure Network Configurations

The Network Configuration page is divided into two sections:



- Network Details, page 45.
- Peripheral Mapping, page 46.

Network Details



This section displays the network configuration that the Flex-Server directly fetches for **Ethernet**, **Wi-Fi**, **GSM-Top**, and **GSM-Bottom**.

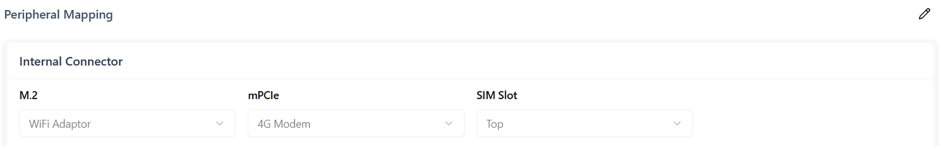
- You can view or update the **Ethernet** and **Wi-Fi** settings as needed.
- GSM settings cannot be modified since the Flex-Server runs an auto APN configuration script. If a SIM card is detected, the APN settings will be applied automatically.

- If the Flex-Server fails to come online after inserting the SIM, verify the following:
  - Check the antenna connection.
  - Check that the SIM card is correctly inserted and does not have a PIN or username/password enabled, as the Deployment Portal does not support these security features.

    NOTE: If the Flex-Server is offline, network details will not be available for configuration. The server must be online to view and modify settings.

    NOTE: If you're using a new SIM card provider, contact the admin to add the operator's APN to the database. This will allow the system to automatically fetch the configuration once the Flex-Server comes online.
- IP Address configuration guidelines:
  - The Wi-Fi (wlan0) and Ethernet (eth0) IP ranges must be different to avoid conflicts.
  - Incorrect example:
    - wlan0: 192.168.1.100-255
    - eth0: 192.168.1.100-255
  - Recommended example:
    - wlan0: 192.168.1.100-255
    - eth0: 192.168.0.100-255

Peripheral Mapping



The Peripheral Mapping section consists of four configuration cards:

- Internal Connector - Displays devices connected to the Flex-Server.
  - M.2 Slot - If set to Wi-Fi Adapter, the Flex-Server supports Wi-Fi connectivity. If set to **None**, Wi-Fi is not available.
  - mPCIe Slot - If configured with a 4G modem, the Flex-Server can connect to a SIM network; otherwise, it cannot.
  - SIM Slot - Selecting the incorrect SIM slot may prevent the Flex-Server from coming online.
- On-Board (RS485) - Serial Port Configuration.

  The RS485 port supports either Modbus RTU or BACnet MSTP connections.
  - If using Modbus RTU:
    - Priority (Set priority for communication)
    - Baud Rate (Speed of data transmission)
    - Stop Bit (Defines stop bit configuration)
  - If using BACnet MSTP:
    - Gateway Address
    - Baud Rate
- USB Ports Configuration (Top and Bottom).
  - USB (Top): Functions similarly to the On-Board RS485 port.
  - USB (Bottom): Functions similarly to the On-Board RS485 port.

- Using LoRaWAN (Top and Bottom).
  - Select **Protocol** as LoRaWAN.
  - Select **Region** from the dropdown as per the country.

Future Scope

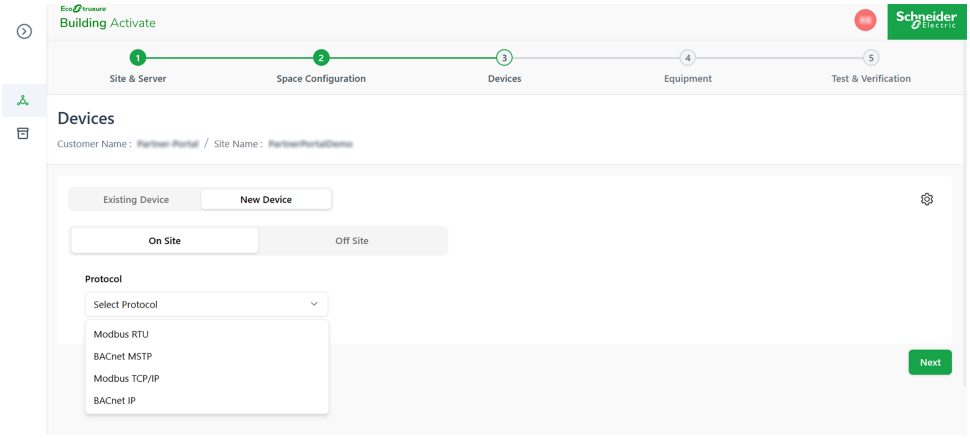
- Allows you to enter PIN, username, and password for SIM authentication.
- Enable you to set default network priority from the dashboard.
- Expand USB port support for additional protocols.

Devices

What's in This Chapter

This interface allows you to manage devices, showing existing devices and providing options to add new ones

Interface Overview



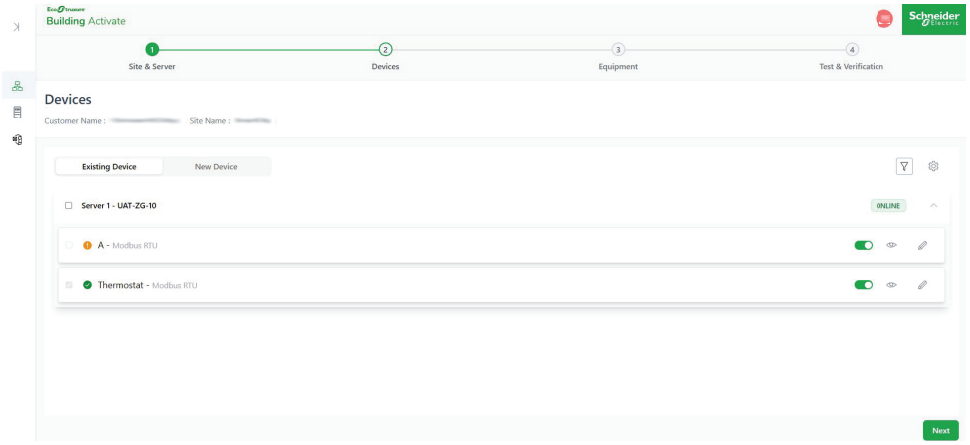
The **Devices** interface is divided into two main sections:

- **Existing Device**: Displays all configured devices, grouped by the server. For more information, refer to Existing Device, page 48.
- **New Device**: Allows you to add new devices using the following supported protocols:
  - **Modbus TCP/IP**: Devices can only be added through templates. For more information, refer to Add a Modbus TCP/IP Device, page 54.
  - **Modbus RTU**: Devices can only be added through templates. For more information, refer to Add a Modbus RTU Device, page 52.
  - **BACnet IP**: Devices can be added through templates or using the scan flow. For more information, refer to Add a BACnet IP device, page 58.
  - **BACnet MSTP**: Devices can only be added through templates. For more information, refer to Add a BACnet MSTP device, page 56.
  - **LoRaWAN**: Devices can only be added through templates. For more information, refer to Add a LoRaWAN Device, page 63.
  - **Multichannel Modbus RTU**: Devices can only be added through templates. For more information, refer to Add a Multichannel on Modbus RTU , page 65.

Existing Devices

You can view a list of all servers. Clicking a server card reveals all associated devices, providing context for the server and its connected devices.

Device Status Indicators



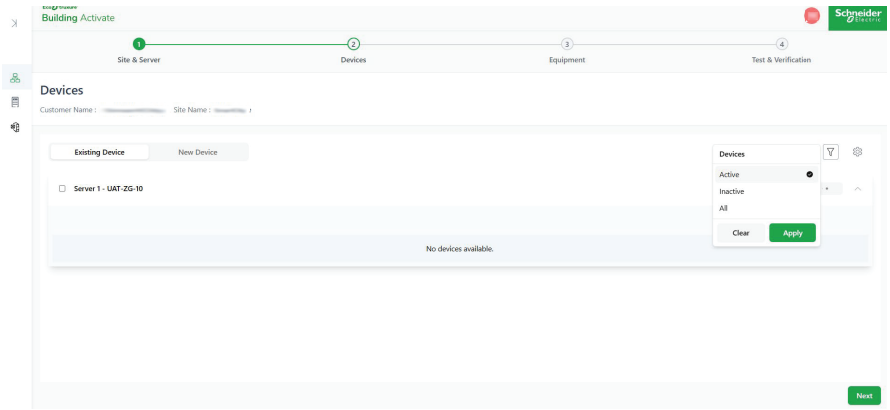
- ✅ indicates that the device is successfully configured on the Deployment Portal, sent to the Flex-Server, and data is populating if the connections are also done at the site. Hovering over the icon displays. Device successfully configured and data is being received.
- ⚠ indicates that the device configuration is incomplete or was unchecked when submitting devices to the Flex-Server. Hovering over this icon displays. Device configuration incomplete or not submitted to the Flex-Server.

  NOTE: You can see the device display name and protocol in the list.

Device Configuration

After configuring all devices, you need to:

1. Select the box beside the server's name to select all modified or newly added devices.
2. Clear the box to cancel the selection of the device if device configuration is not complete or is not required to be set up in the system yet.
3. Click 👁 icon to view the configuration.
4. Click ✎ icon to modify the configuration.
5. Click **Next** at the bottom right, to submit the configuration.
6. Click toggle to disable and remove the device from the list.
7. To recover the device.
   - Click ▼ and select the **Inactive** device.
   - Click toggle to remove the device from the inactive list to active list.
   - To submit the configuration, Click **Submit**.



NOTE:

- Disabled device will not be visible in Troubleshooting screen.
- After disabling the device, it will sync to the backend in next 5 minute and it will not require a specific submit.
- After enable, the device submission is required.

Troubleshoot Server Selection

If selecting the server check box does not select all devices, it means:

- You did not click **Mark as Complete** while configuring a device.
- Some required configurations, like templates, are missing.

  NOTE: The system displays the server's status (Online/Offline) to the right of the server's name.

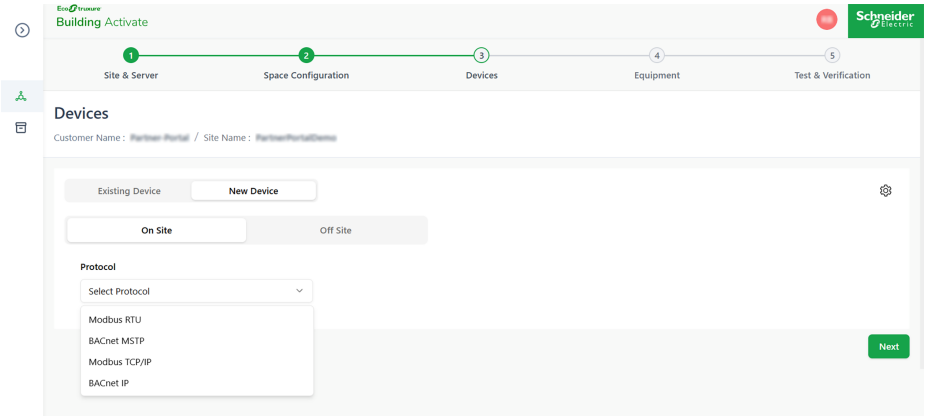
New Device

The **New Device** screen is used for configuring new devices.

Add New Device

To add a device, follow the steps below:

1. Select a protocol from the menu.



2. After you select a protocol, proceed to add devices.

You can add multiple devices of the same protocol at once. The system displays all newly added devices in a list below, allowing you to review and submit them together.

NOTE: To remove a device before creating it, click **Delete** to remove it from the list before submission.

This process reduces the need to repeatedly enter the same information and minimizes configuration effort.

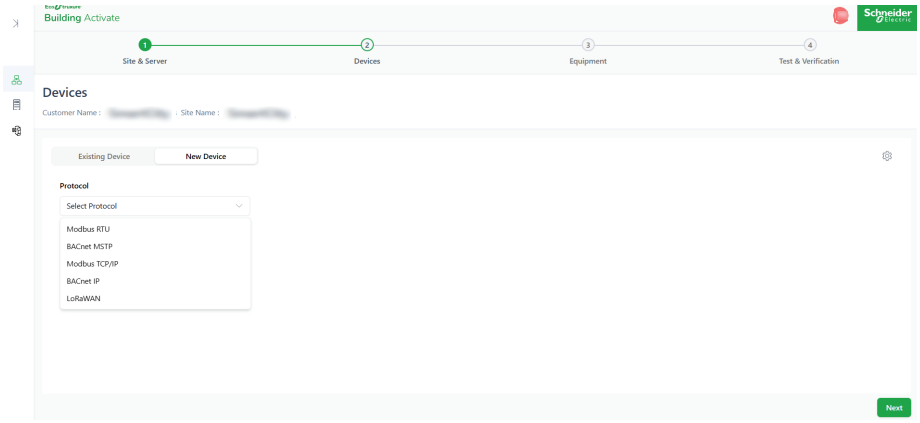
Future Scope

- Expand device list with additional details.
- Allows you to add more ports for **BACnet IP** and **Modbus TCP/IP**.
- Enable device unit configuration in the template or scan flow.
- Provide functionality to edit templates by removing or adding parameters.

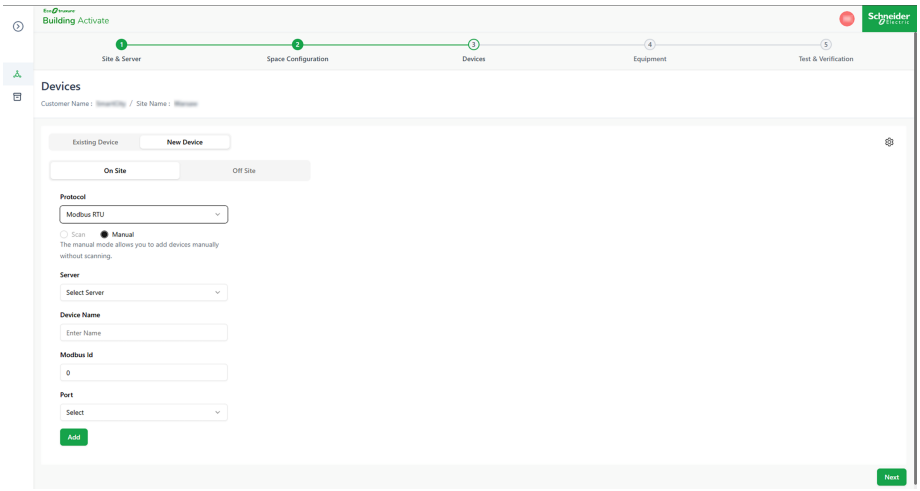
- Introduce an Upload Points feature.
- Enable **BACnet MSTP** scanning.

Add a Modbus RTU Device

1. On the **Devices** page, click **New Device > On Site**.
2. Select **Protocol** as **Modbus RTU**.



3. Select the desired **Server**.
4. Enter a unique **Device Name** for display on the dashboard.
5. Enter the **Modbus ID** of the device.
6. Select the configured **Port** provisioned during server setup.

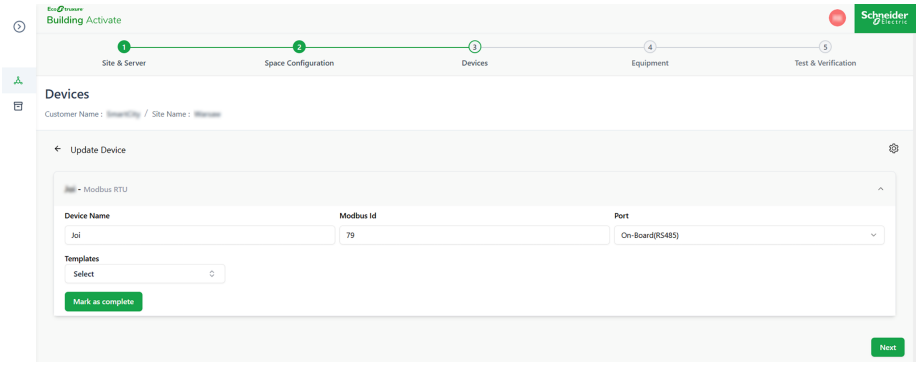


IMPORTANT: If the port list is empty, click the gear icon on the right to view and configure port settings.

7. Click **Add**.

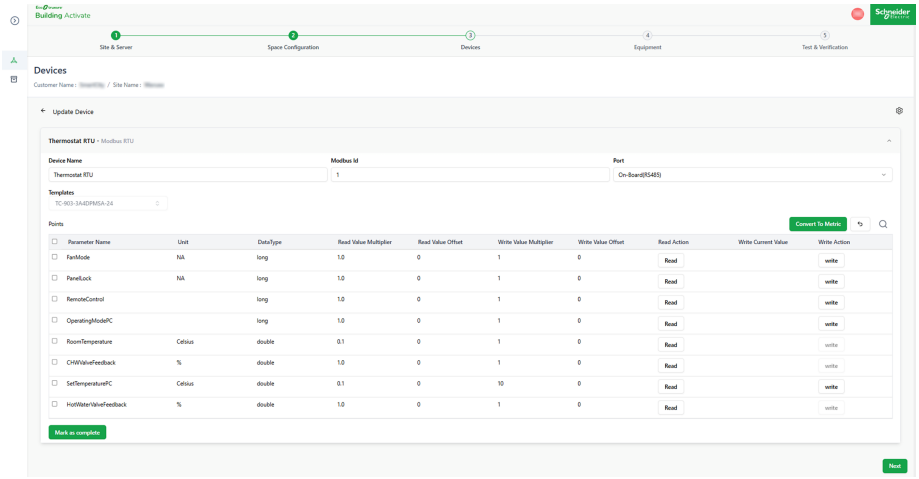
   The review table displays the added device.
8. To add another device, enter a unique **Device Name**, **Modbus ID**, **Port** and then click **Add**.
9. Once you have added all devices, click **Next**.
10. In the **Template** search for the device model.

11. Select the appropriate template.



Review the selected template displayed below to ensure it is correct.

12. (Optional) Check if the device uses SI Units or Imperial Units.



The dashboard stores the data in SI Units by default. Convert values if needed:

a. Select the parameters in the table.

b. Click **Convert to Metric** to switch to SI Units.

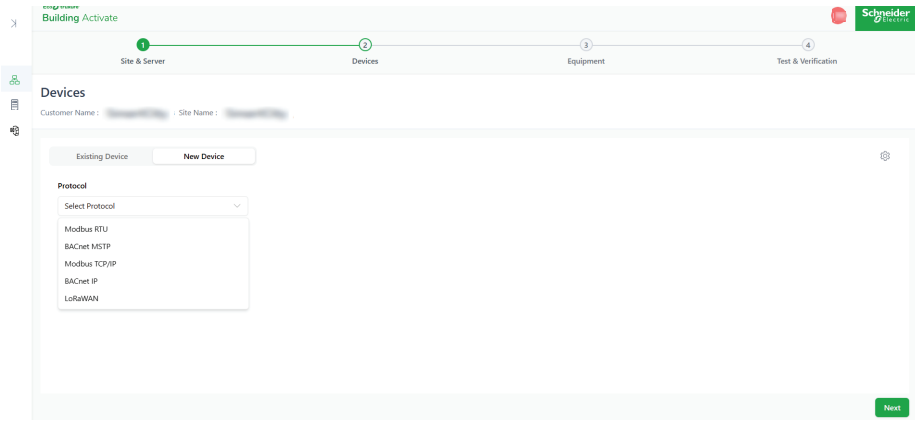
c. If necessary, click **Undo** to revert the changes.

13. Use the search bar to find specific parameters.
14. Click **Mark as Completed** to save the configuration.
15. Click **Next** to go to the Existing Devices list.
16. Select the box next to the server's name to include all modified or newly added devices.
17. Clear the box for any device you do not want to send to the Flex-Server.
18. Click **Next** at the bottom right to submit the configuration.

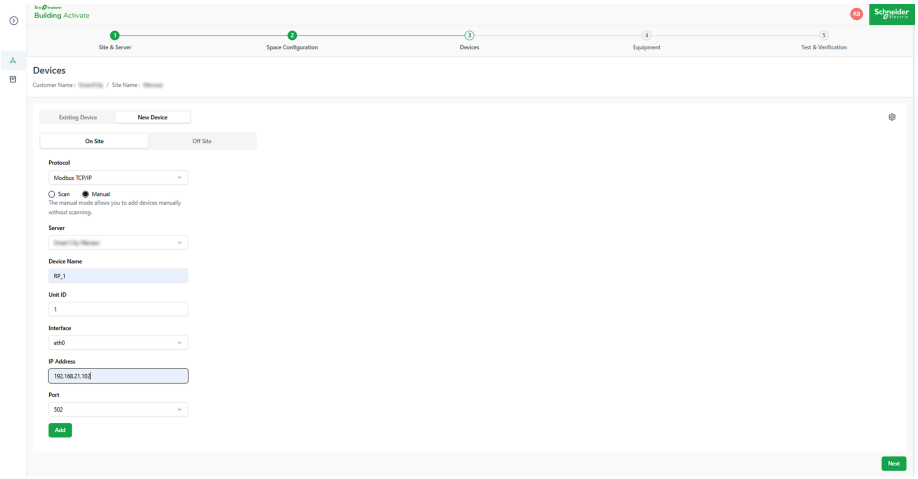
    For more details on submitting configurations, refer to the Existing Device, page 48 section.

Add a Modbus TCP/IP Device

1. On the **Devices** page, click **New Device > On Site**.
2. Select **Protocol** as **Modbus TCP/IP**.



3. Select the desired **Server**.
4. Enter a unique **Device Name** for display on the dashboard.
5. Enter the **Unit ID** of the device.
6. Select the **Interface** provisioned during server setup.
7. Enter the **IP address** of the device for communication.
8. Select the **Port**.



NOTE: By default, port is set to 502.

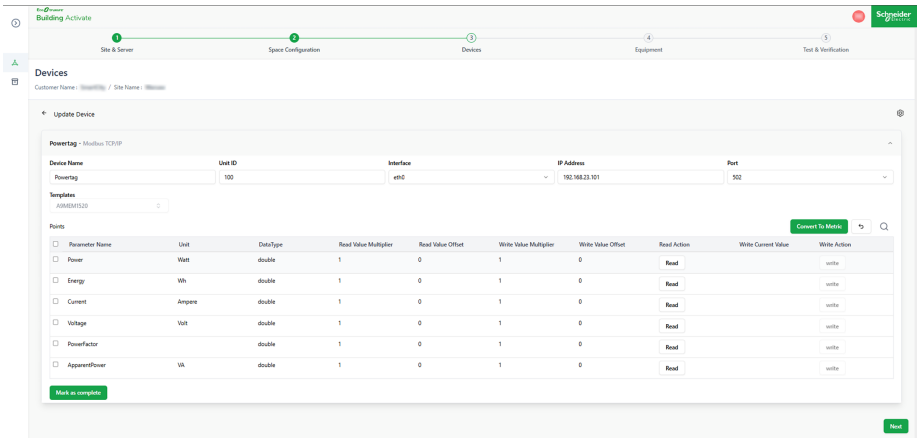
9. Click **Add**.

   The review table displays the added device.
10. To add another device, enter a unique **Unit ID**, **Device Name**, and then click **Add**.
11. Once you have added all devices, click **Next**.
12. In the **Template** search for the device model.
13. Select the appropriate template.

    Review the selected template displayed below to ensure it is correct.

    NOTE: Make sure the panel server should be configured with static IP.

14. (Optional) Check if the device uses SI Units or Imperial Units.



The dashboard stores the data in SI Units by default. Convert values if needed:

a. Select the parameters in the table.

b. Click **Convert to Metric** to switch to SI Units.

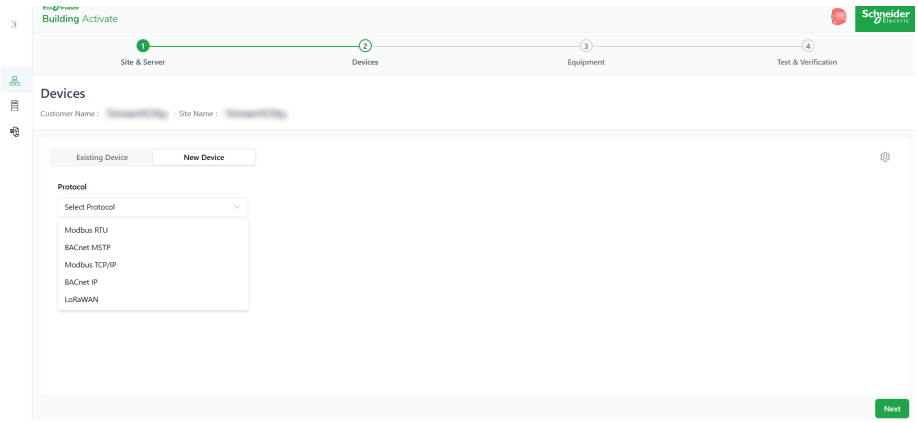
c. If necessary, click **Undo** to revert the changes.

15. Use the search bar to find specific parameters.
16. Click **Mark as Completed** to save the configuration.
17. Click **Next** to go to the Existing Devices list.
18. Select the box next to the server's name to include all modified or newly added devices.
19. Clear the box for any device you do not want to send to the Flex-Server.
20. Click **Next** at the bottom right to submit the configuration.

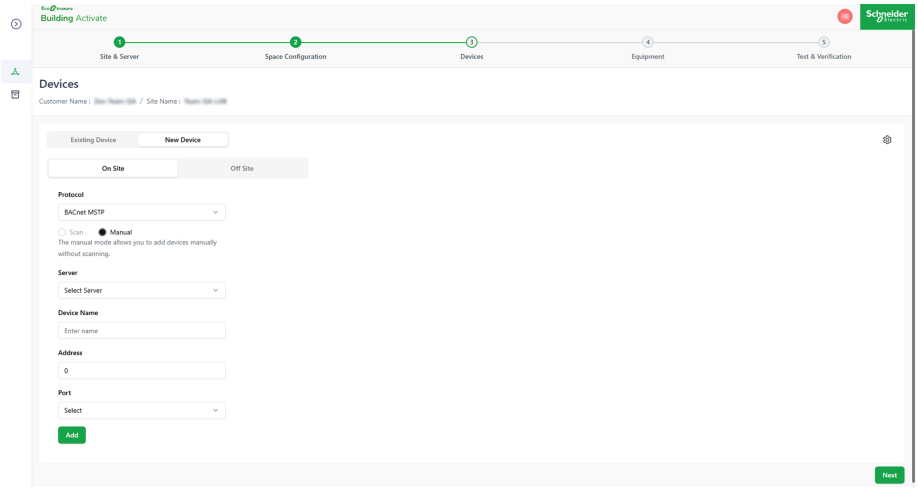
    For more details on submitting configurations, refer to the Existing Device, page 48 section.

Add a BACnet MSTP Device

1. On the **Devices** page, click **New Device > On Site**.
2. Select **Protocol** as **BACnet MSTP**.



3. Select the desired **Server**.
4. Enter a unique **Device Name** for display on the dashboard.
5. Enter the **Address** in the range of 0-127.
6. Select the **Port**.



NOTE: By default, port is set to 502.

7. Click **Add**.

   The review table displays the added device.
8. To add another device, enter a unique **Address**, **Device Name** and then click **Add**.
9. Once you have added all devices, click **Next**.
10. In the **Template** search for the device model.
11. Select the appropriate template.

    Review the selected template displayed below to ensure it is correct.
12. (Optional) Check if the device uses SI Units or Imperial Units.

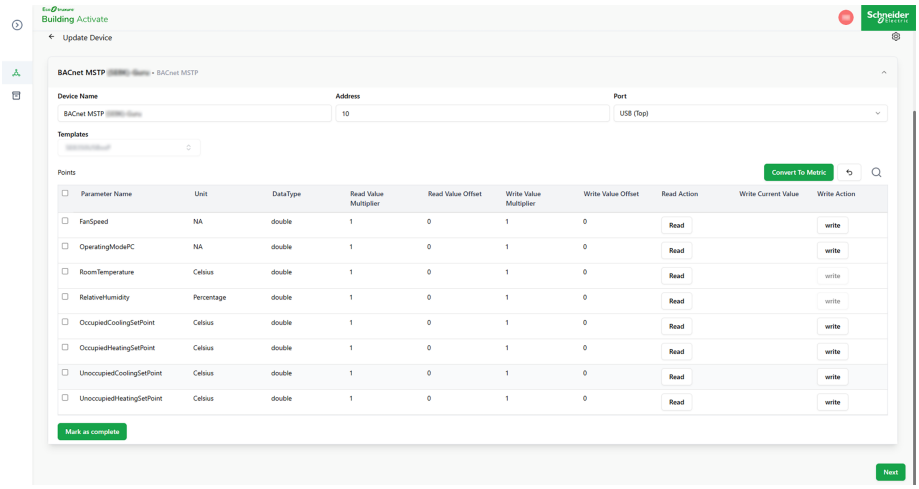
    The dashboard stores the data in SI Units by default. Convert values if needed:

    a. Select the parameters in the table.

    b. Click **Convert to Metric** to switch to SI Units.

    c. If necessary, click **Undo** to revert the changes.
13. Use the search bar to find specific parameters.
14. Click **Mark as Completed** to save the configuration.

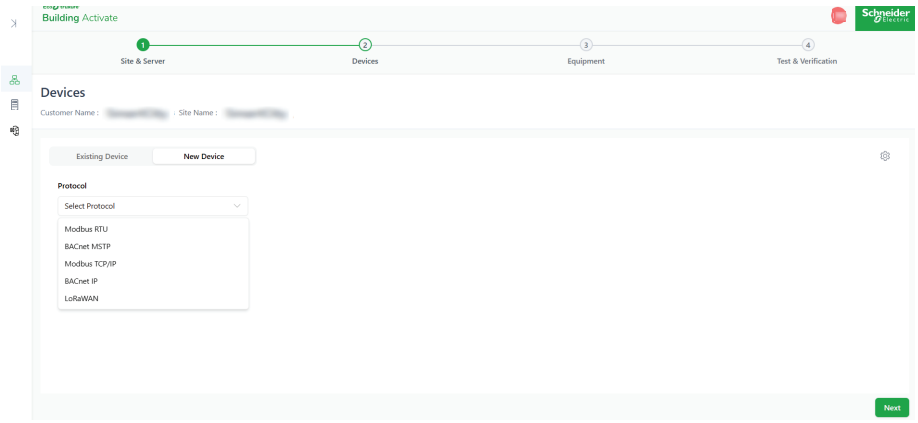
15. Click **Next** to go to the Existing Devices list.
16. Select the box next to the server's name to include all modified or newly added devices.
17. Clear the box for any device you do not want to send to the Flex-Server.
18. Click **Next** at the bottom right to submit the configuration.



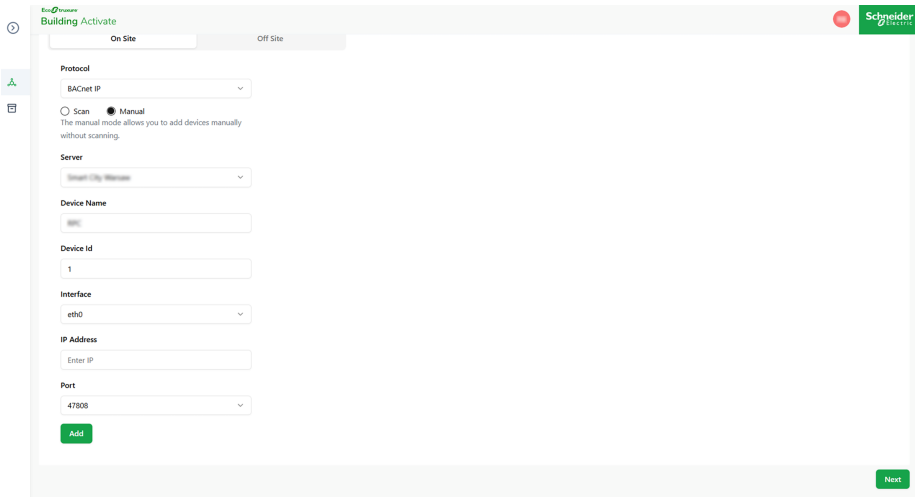
For more details on submitting configurations, refer to the Existing Device, page 48 section.

Add a BACnet IP Device (Manual Entry)

1. On the **Devices** page, click **New Device > On Site**.
2. Select **Protocol** as **BACnet IP**.



3. Select the desired **Server**.
4. Enter a unique **Device Name** for display on the dashboard.
5. Enter the **Device ID**.
6. Select the **Interface** provisioned during server setup.
7. Enter the **IP Address** of the device for communication.
8. Select the **Port** as **47808** or **47809**.
9. Click **Add**.

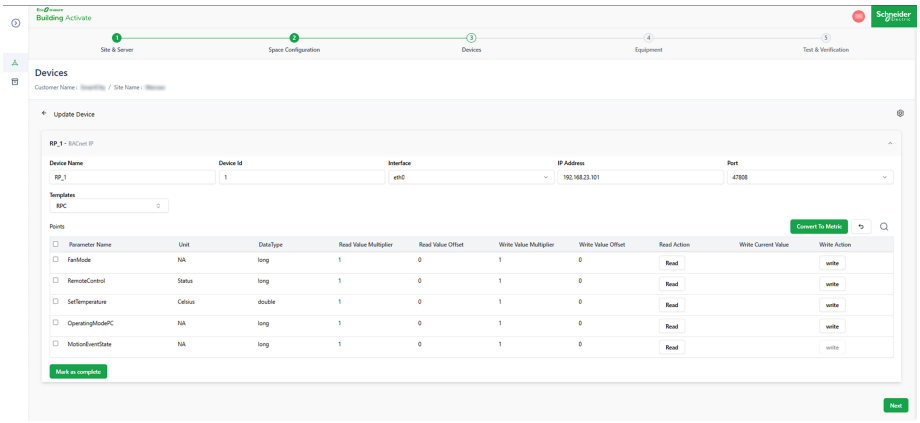


   The review table displays the added device.

10. To add another device, enter a unique **Address**, **Device Name** and then click **Add**.
11. Once you have added all devices, click **Next**.
12. In the **Template** search for the device model.
13. Select the appropriate template.

    Review the selected template displayed below to ensure it is correct.

14. (Optional) The dashboard stores the data in SI Units by default. Convert values if needed:



    a. Select the parameters in the table.

    b. Click **Convert to Metric** to switch to SI Units.

    c. If necessary, click **Undo** to revert the changes.

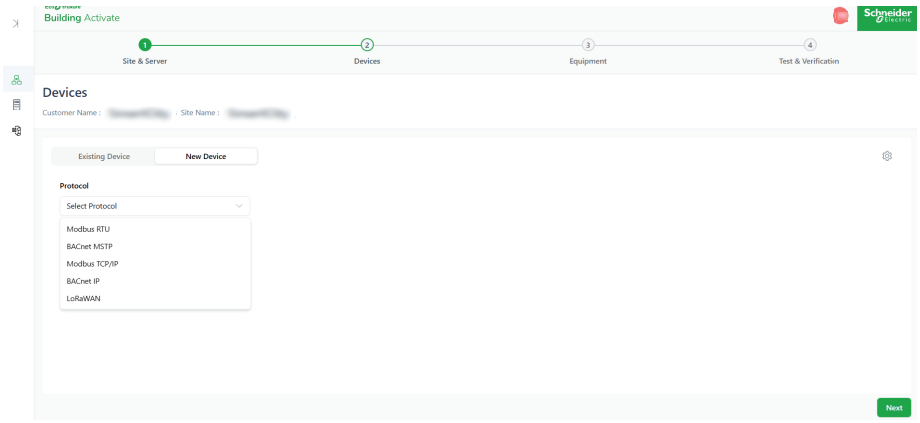
15. Use the search bar to find specific parameters.
16. Click **Mark as Completed** to save the configuration.
17. Click **Next** to go to the Existing Devices list.
18. Select the box next to the server's name to include all modified or newly added devices.
19. Clear the box for any device you do not want to send to the Flex-Server.
20. Click **Next** at the bottom right to submit the configuration.

    For more details on submitting configurations, refer to the Existing Device, page 48 section.

    NOTE: Make sure the panel server is configured with static IP.

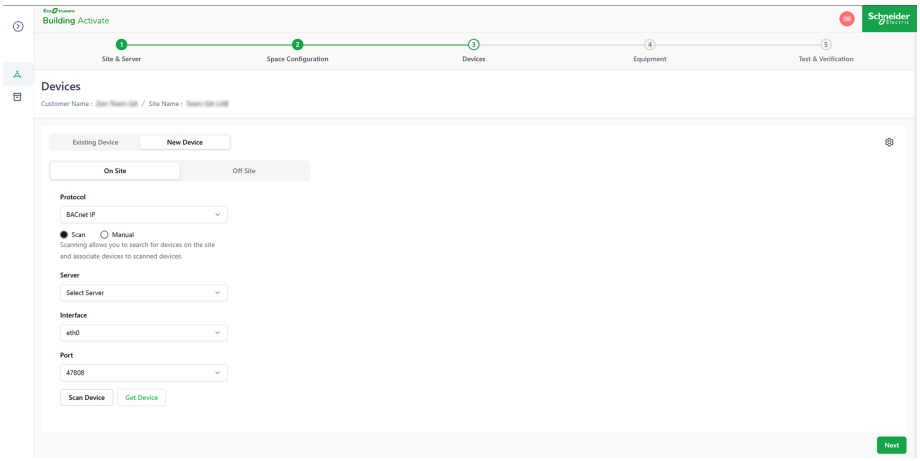
Add a BACnet IP Device through BACnet Scan

1. On the **Devices** page, click **New Device > On Site**.
2. Select **Protocol** as **BACnet IP**.



3. Select the desired **Server**.
4. Select the **Interface** provisioned during server setup.
5. Select the **Port** as **47808** or **47809**.

   NOTE: Before starting the scan make sure you have configured static IP configuration on (eth0, wlan0) interface.
6. Click **Scan Device** to perform a new scan.
7. Click **Get Device** to retrieve a previously saved scan from the backend.



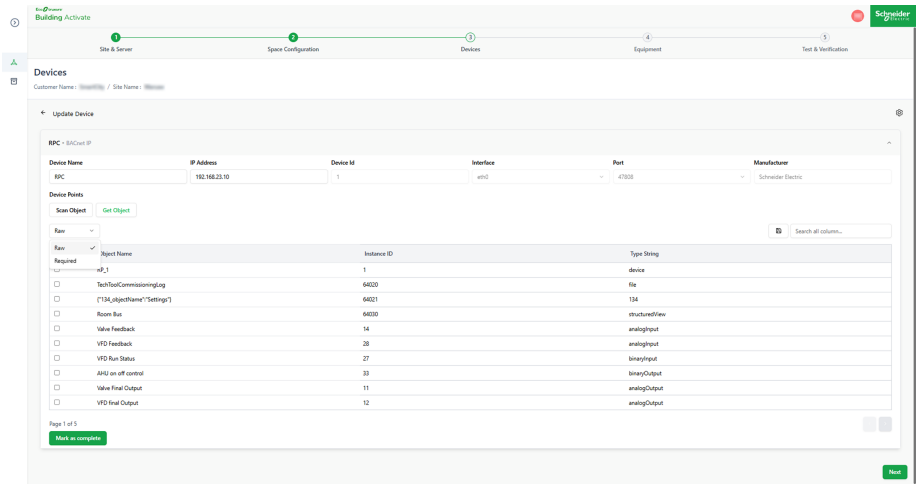
   The review table displays the list of detected devices.
8. Click the checkbox next to each device to select device.
9. Make sure reference details like **Device ID**, **IP Address**, and **Manufacturer** are correctly selected.

   If a device is already selected, it means it exists in the system.
10. After selecting the device, click **Next** to proceed with object scanning.

11. Click **Scan** for a fresh scan OR click **Get Point** to fetch pre-scanned results.

    The scanned Object List will show:

    - Object Name
    - Object Instance ID
    - Type String (to verify correct details)



12. Select objects and click Move to Required.
13. Switch views between **Raw** and **Required** to manage objects.

    Use the search bar to locate specific objects.
14. To configure object, fill in the parameters listed below:
    a. **Parameter Name**: Name associated with the stream.
    b. **Unit**: Measurement unit (e.g., Volt, Amperes, kW).
    c. **Data Type**: Integer, Decimal.
    d. **Actuation**: Indicates if actuation is enabled.
    e. **Actuation Class**: Digital, Analog, On/Off.
    f. **Default State**: Initial value when scanned.
    g. **Priority**: you can select priority from 7-16.

    NOTE: By default, it is 7, higher priorities 1-6 are reserved and cannot be selected.
    h. **Valid State Mapping**: Example: ON = 1, OFF = 0.
    i. **Mapping Status**: Indicates Mapped/Not Mapped objects.
15. Click **Read** to view real-time object data.
16. (Optional) Check if the device uses SI Units or Imperial Units.
    a. Click **Convert to Metric** to switch to SI Units.
    b. If necessary, click **Undo** to revert the changes.
17. Click **Mark as Completed** to save the configuration.
18. Click **Next** to go to the Existing Devices list.
19. Select the check box next to the server's name to include all modified or newly added devices.
20. Clear the box for any device you do not want to send to the Flex-Server.

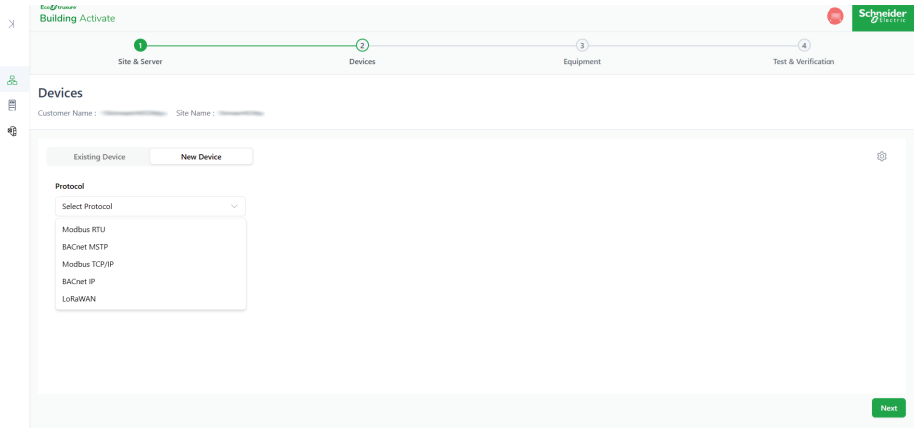
21. Click **Next** at the bottom right to submit the configuration.

    Future Scope:

    - Copy Device Mapping Across Sites: Provide functionality to copy the device mapping from another site.
    - Bulk Upload Support: Enable bulk uploading of device configuration and mapping information.
    - Point Upload and Download: Allows you to upload or download device points for easier configuration management.
    - Enhanced Table Validation: Implement additional validations in the table to ensure data accuracy.

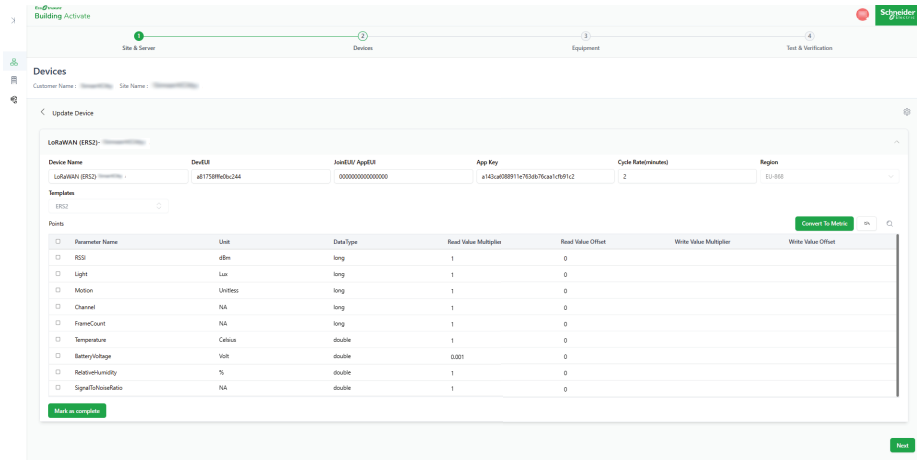
Add a LoRaWAN Device

1. On the **Devices** page, click **New Device > On Site**.
2. Select **Protocol** as **LoRaWAN**.



3. Select the desired **Server**.
4. Enter a unique **Device Name** to be displayed on the dashboard.
5. Enter **DevEUI** and **JoinEUI/AppEUI**. Both **DevEUI** and **JoinEUI/AppEUI** should be case-sensitive, hexadecimal, must be exactly 16 characters.
6. Enter **App Key**. The **App Key** should be case-sensitive, hexadecimal, must be exactly 32 characters.
7. Enter the **Data Rate** (in minutes).
8. The region configured in the peripheral mapping will be displayed here. To modify the region information, click the **Settings** icon located at the top-right corner of the screen and update the peripheral mapping.
9. Click **Add**.
10. To add another **Device**, enter a unique **Address**, **Device Name**, **DevEUI**, **App Key** and then click **Add**.
11. Once you have added all devices, click **Next**.
12. In the Template, search for the device model.
13. Select the relevant **Template**. Verify the chosen Template shown below to ensure it is correct.
14. Check if the **Device** uses SI Units or Imperial Units. The dashboard stores the data in SI Units by default. Convert values if needed:
    a. Select the parameters in the table.
    b. Click **Convert to Metric** to switch to SI Units.
    c. If necessary, click **Undo** to revert the changes.
15. Click **Mark as Completed** to save the configuration.
16. Click **Next** to go to the Existing Devices list.
17. Select the check box next to the server's name to include all modified or newly added devices.
18. Clear the box which is not necessary to send to the Flex-Server.

19. Click **Next** at the bottom right to submit the configuration.



For more details on submitting configurations, refer to the Existing Device, page 44 section, page 48.

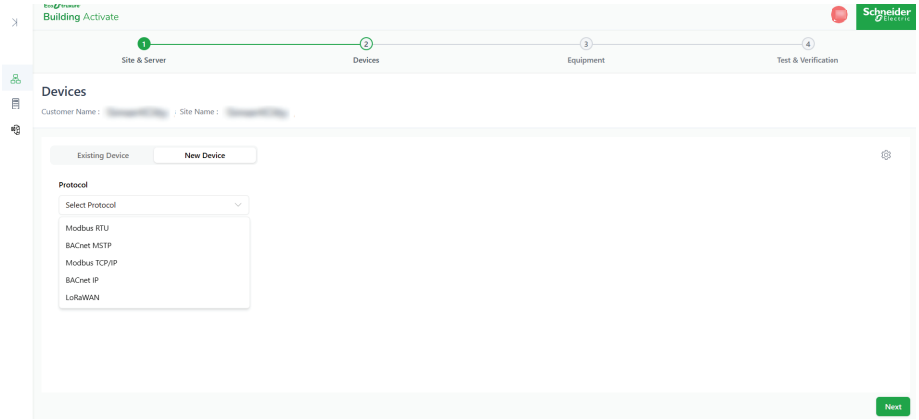
NOTE: Read and Write action functionality is not applicable for LoRaWAN protocol.

Add a Multi-channel on Modbus RTU

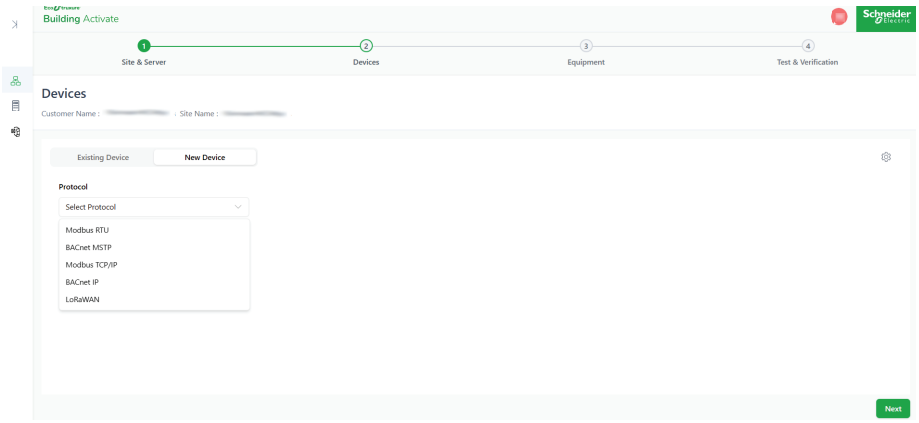
Modbus RTU support multi-channel devices such as DTA116A51, HGR42EW.

The device addition flow remains the same, however the view changes based on the selected template, as the template determines whether to open the single channel or multi-channel flow.

1. On Devices page, click **New Device**.
2. Select **Protocol** as **Modbus RTU**.



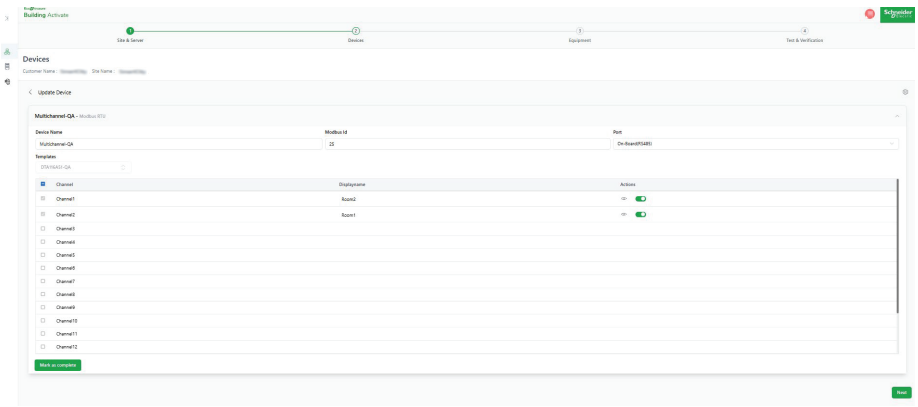
3. Select the desired **Server**.
4. Enter **Device name** to display on the dashboard.
5. Enter **Modbus ID** of the device.
6. Select the configured **Port** provisioned during server setup.



IMPORTANT: If the port list is empty, click icon on the right to view and configure port settings.

7. Click **Add**.
8. To add another **Device**, enter a unique **Device name**, **Modbus ID**, **Port** and then click **Add**.
9. Once you have added all devices, click **Next**.
10. In the **Template** tab, search for the device model.

11. Select the multi-channel template (like DTA116A51, HGR42EW).



12. Select the channel (Indoor) and enter a unique **Device name**.
13. Click **Mark as complete** to save the information.
14. Click on view icon to review the parameters table.
15. (Optional) Check whether the device uses SI units or Imperial units. The dashboard stores data in SI units by default. Convert values if needed:
    a. Select the parameters in the table.
    b. Click **Convert to Metric** to switch to SI Units.
    c. If necessary, click **Undo** to revert the changes.
16. Click **Next** to go to Existing Devices list.
17. Select the box next to the server's name to include all modified or newly added devices.
18. Clear the box which is not necessary to send to the Flex-Server.
19. Click **Next** at the bottom right to submit the configuration.

    For more details on submitting configurations, refer to the Existing Device, page 48, page 44 section.
20. To disable/enable the channel (Indoor), click on toggle button.

    NOTE:

    1. Disabled channels will remain visible in the list.
    2. Channel information will not appear in the main device list; only parent devices will be shown.
    3. If the user disables or enables a parent device, all associated channels will be automatically disabled or enabled.

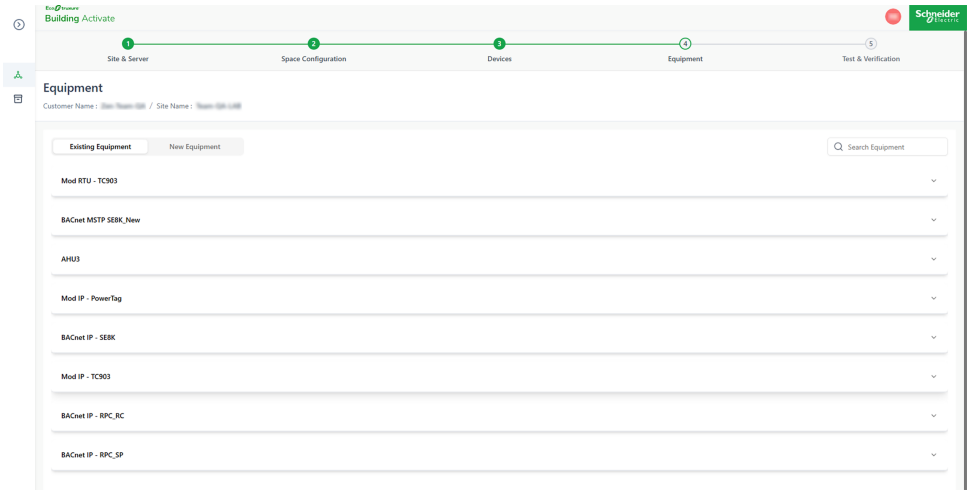
Equipment

What's in This Chapter

Equipment is a collection of device points that are mapped to an Equipment Point Name, making it understandable for the customer on the dashboard. The Equipment tab has two sections:

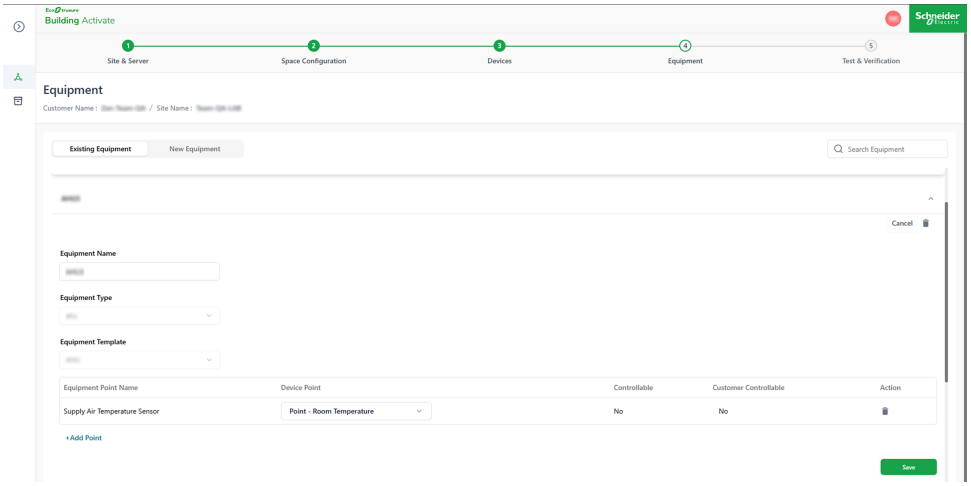
- **Existing Equipment**: Shows all configured equipment.
- **New Equipment**: Allows you to add and configure new equipment.

Existing Equipment



The **Existing Equipment** section displays all configured equipment. The Equipment table has these columns:

- **Equipment Point Name**: A display name that customers easily understand.
- **Device Point**: The device object/parameter as the device provides it and as configured in the system.
- **Controllable**: Indicates whether the equipment point is controllable (Yes/No).
- **Customer Controllable**: Specifies if the customer can control the equipment (Yes/No).
- **Action**: Provides an option to delete an Equipment Point Name.



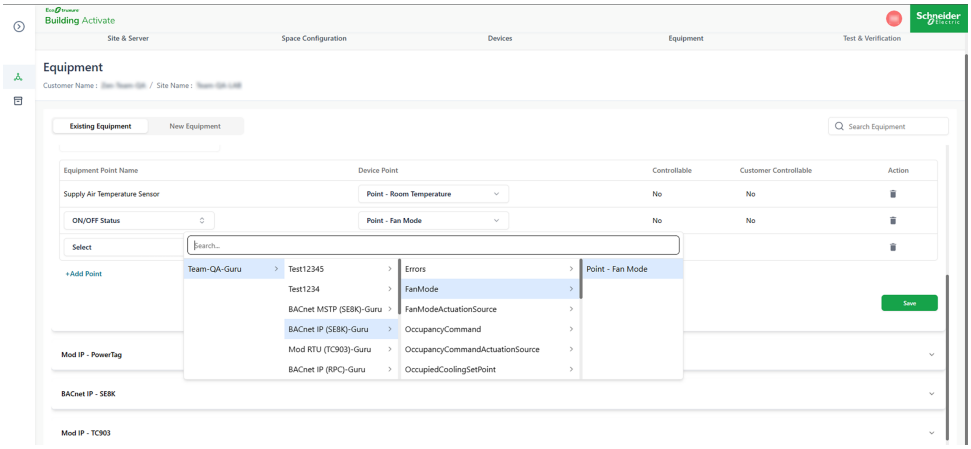
Viewing and Editing Equipment

You can view a list of all equipment by display name.

- Click equipment item to opens a detailed view of its configured device points.
- Click **Edit** to add more points.
- If an incorrect **Equipment Type** or **Equipment Template** was selected, you can delete and reconfigure the equipment.

  NOTE: Once created, the **Equipment Type** and **Equipment Template** fields cannot be edited.

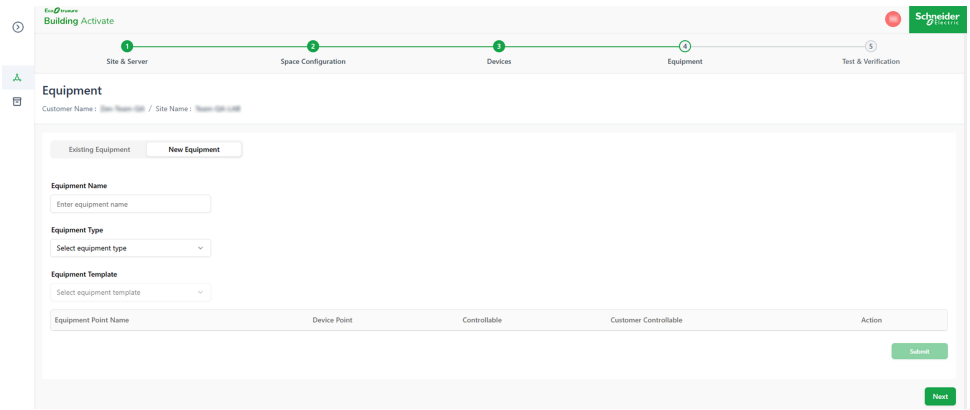
Adding Device Points to Equipment



1. Click **Add Point** to search for an **Equipment Point Name**.
2. Use the search box to search all the available **Equipment Point Name** in the system.

   NOTE: If an **Equipment Point Name** is missing, raise a request with the administrator.
3. To select a **Device Point**, follow the below steps:
   a. Search for the required point and view its full path, including device and server details.
   b. Select the Server, then the Device, and finally choose the desired point, if you are not sure about the exact point name.
4. Click **Save** to confirm the configuration.

New Equipment



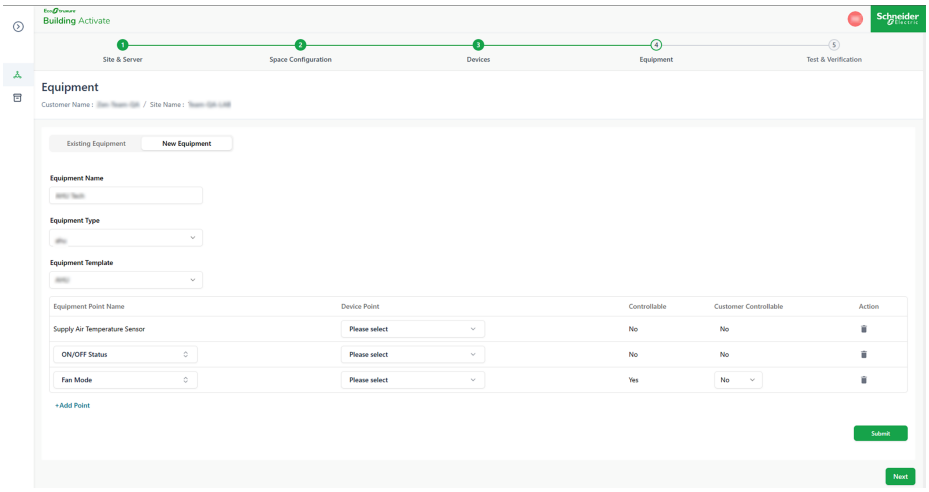
You can create new equipment for newly added devices.

Configure New Equipment

To configure **New Equipment**, follow the below steps:

1. On the **Equipment** page, click **New Equipment**.
2. Enter Equipment Details:
   a. **Equipment Name**: The display name of the equipment.
   b. **Equipment Type**: Select the appropriate type from the list.
   c. **Equipment Template**: Select a template based on the selected type.

   The system generates a table based on the provided information.
3. Map the **Equipment Point Name** with corresponding **Device Point**.
4. The table displays the following information:



   - **Equipment Point Name**: Display name for customer reference.
   - **Device Point**: Corresponding parameter from the device.
   - **Controllable**: Indicates if the system allows control (Yes/No).
   - **Customer Controllable**: Defines if customer control is allowed (Yes/No).
   - **Action**: Option to delete a mapped point.
5. (Optional) To add additional **Equipment Point**:
   a. Search and select a Device Point.

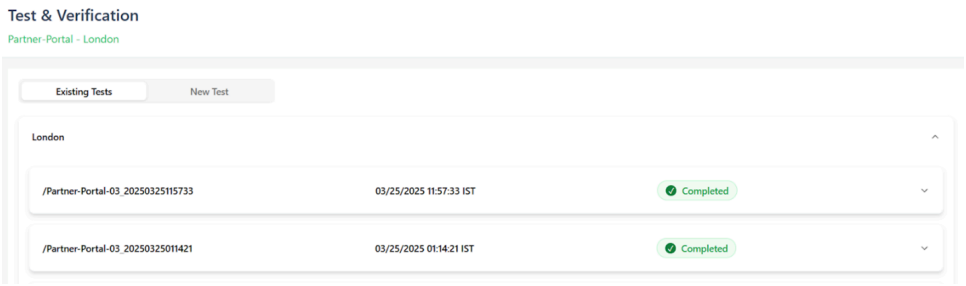
      If unsure, follow the Server → Device → Point selection path.
   b. Click **Submit** to save the configuration.

Future Scope

- Put prevent Equipment Deletion with Controls: Implement validation to restrict the deletion of equipment if it has associated controls.
- Direct Equipment Creation from Device: Allows you to create equipment directly from a device without manually mapping points.
- Automated Mapping and Suggestions: Enable automatic mapping or provide suggestions for equipment and device points based on the required Equipment Point Name and Device Points.
- Enhanced UI for Adding Device Points: Improve the user experience for selecting and adding device points.

Test and Verification

What's in This Chapter

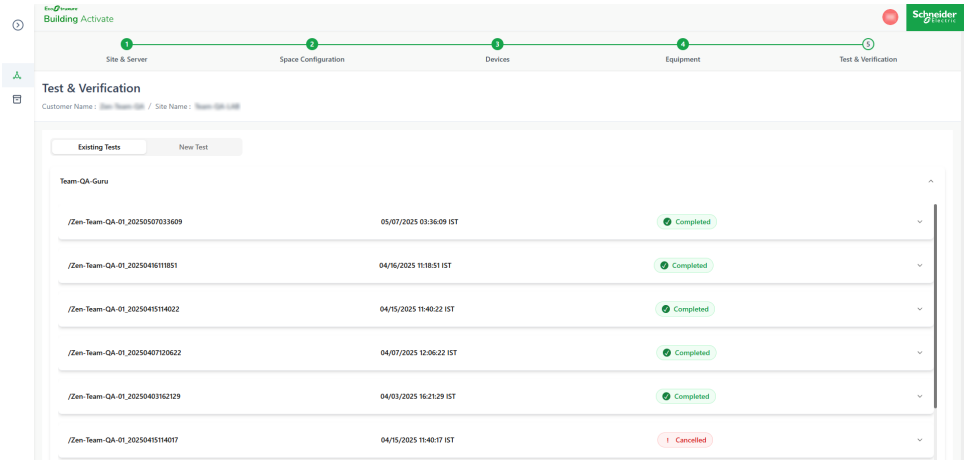


The **Test & Verification** feature allows you to run tests on all added devices at a site to check whether data is being received correctly. The Equipment tab is divided into two sections:

- **Existing Tests**: Displays all historical tests.
- **New Test**: Allows you to conduct a new test on the server.

Existing Tests

On the **Existing Tests** screen, you can view a list of servers. Click the server to display all historical tests. The following information is available:



- **Test ID**: System-generated unique ID for each test.
- **Date**: Date and time when the test was conducted.
- **Status**: Status of the test (Completed, Cancelled, In-Progress).

Click a test to see detailed results, including:

- **Devices**: List of all devices on the selected server.
- **Total Failed Tests**: Number of failed tests for each device.
- **Total Passed Tests**: Number of successful tests for each device.
- **Expand**: Option to view detailed test results for each device.

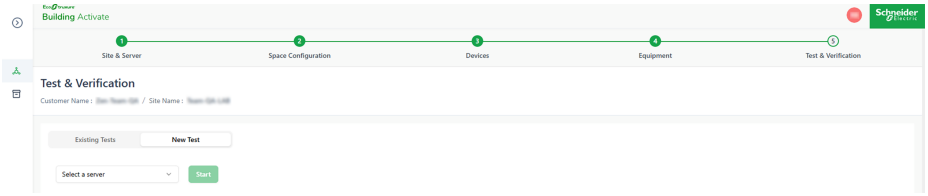
For each test, the following details are displayed:

- **Test Name**: Type of test conducted (configured in the backend).
- **Point/Parameter Name**: Device point on which the test was conducted.
- **Status**: Pass/Fail result of the test.

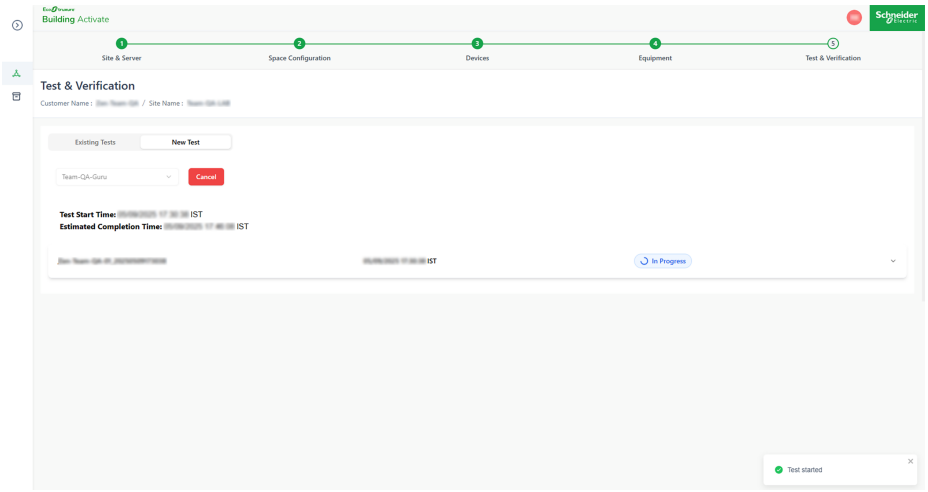
- **Remarks**: System-generated remarks explaining why the test passed or failed.
- **Recommendation**: Suggested action for failed test.

New Test

1. On the **Test & Verification** page, click **New Test**.



2. Select the server and click **Start** to initiate the test.



NOTE:

a. The test will take approximately 15 minutes to complete.

b. You can cancel the test midway if you need to make additional configurations before running it.

c. The system provides partial test results every three minutes, which allows you to monitor progress and take necessary action.

d. If you navigate away or refresh the screen, the test will continue to run, and its status will remain visible in this tab.

Future Scope

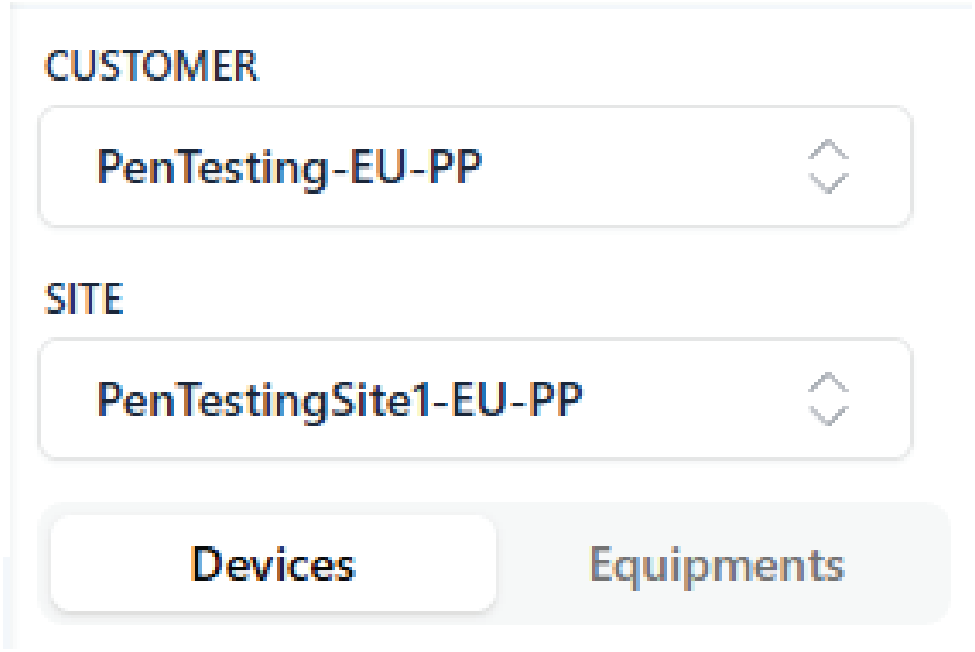
- Allows you to run tests for all servers simultaneously.
- Provide filtering options based on test status (Completed, In-Progress, Cancelled).
- Add more test types to the system.
- Expand the recommendation system with additional insights.

Device Plots

The Plotter feature helps visualize various data streams available on devices, equipment, and the Flex-Server. Follow the steps below to view and analyse data.

NOTE: Only Active devices will be visible here.

You can select **Customer** and **Site**.



After selecting the customer and site, two options will be displayed.

1. Device Tab (selected by default)
2. Equipment Tab

NOTE: By default, selected as Device tab.

Switch between the two tabs based on the data which you need to view.

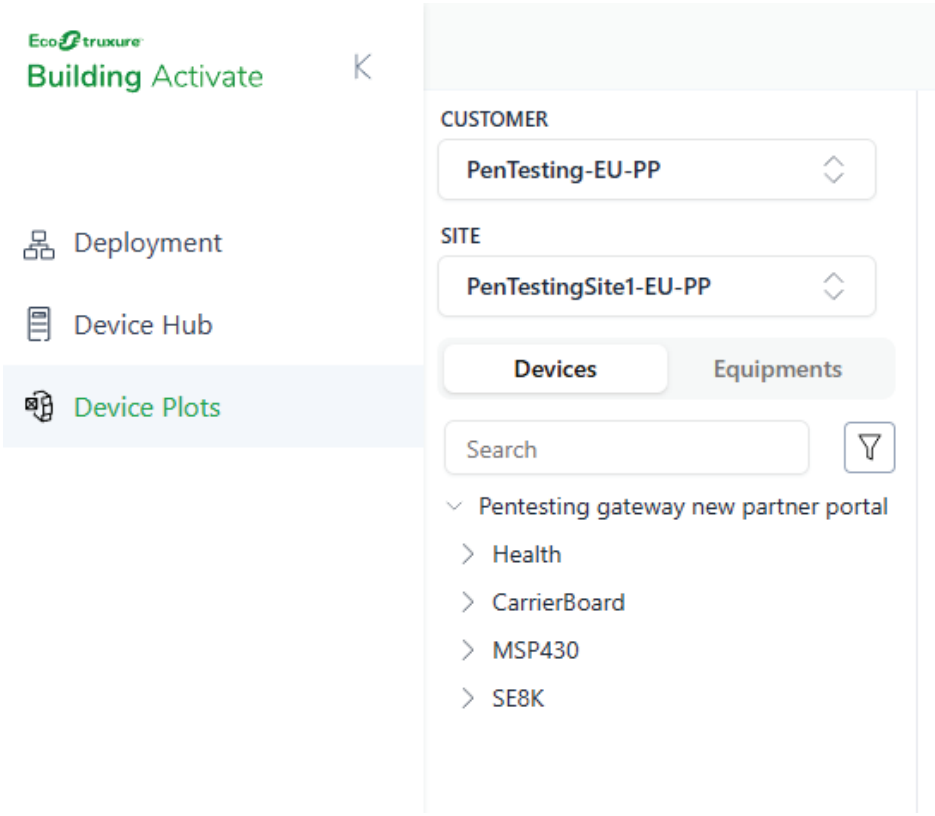
Follow the steps below to set the default plot for both the Device and Equipment tabs:

1. Date Range: Today, from 12:00 AM to current server local time
2. Aggregation: Operator Mean
3. Time Interval: 1 minute

Using Device Tab

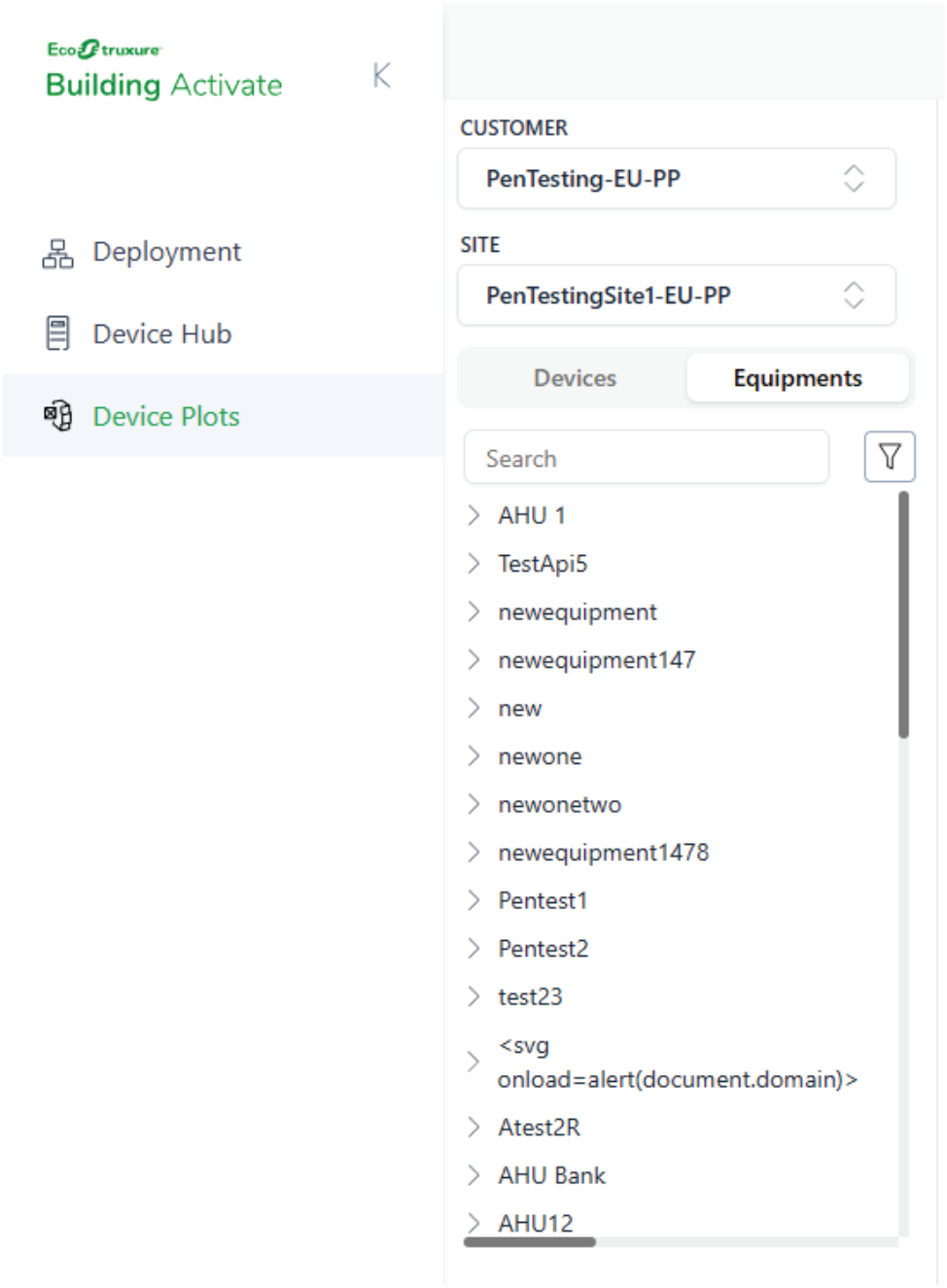
1. Click server's name to view all associated to devices.
2. Click device name to see its parameters.
3. Select the **point(s)** to view.

4. Click **Apply**.



Using Equipment Tab

1. Click equipment name to view parameters listed by display name.
2. Select the **point(s)** to view.
3. Click **Apply**.



NOTE: For both tabs, use the ▼ option to set and view parameters such as Gateways, Protocols, Equipment Type, and more.

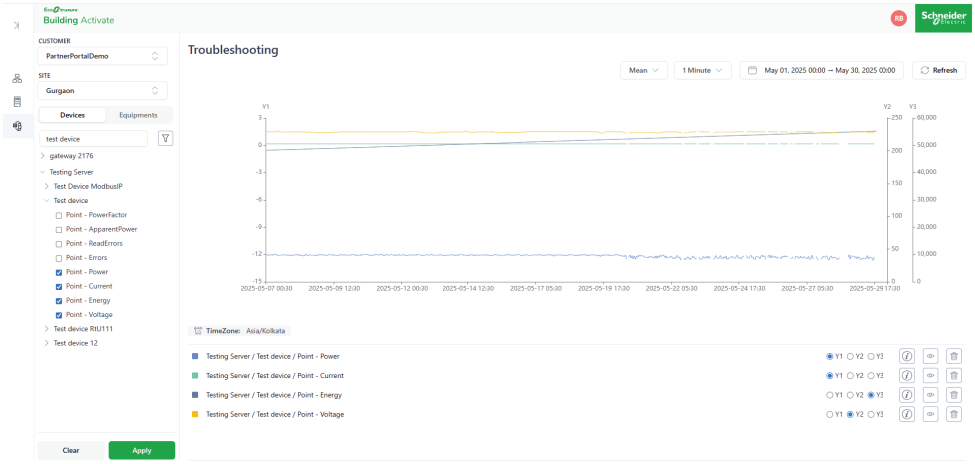
Search Functionality

Global search: Global Search refers to a unified search functionality that allows you to search across multiple data sources, modules, or sections within a system or application from a single search bar or interface. It provides a centralized way to retrieve relevant information - such as documents, records, users, settings, or content - regardless of where it is stored within the platform.

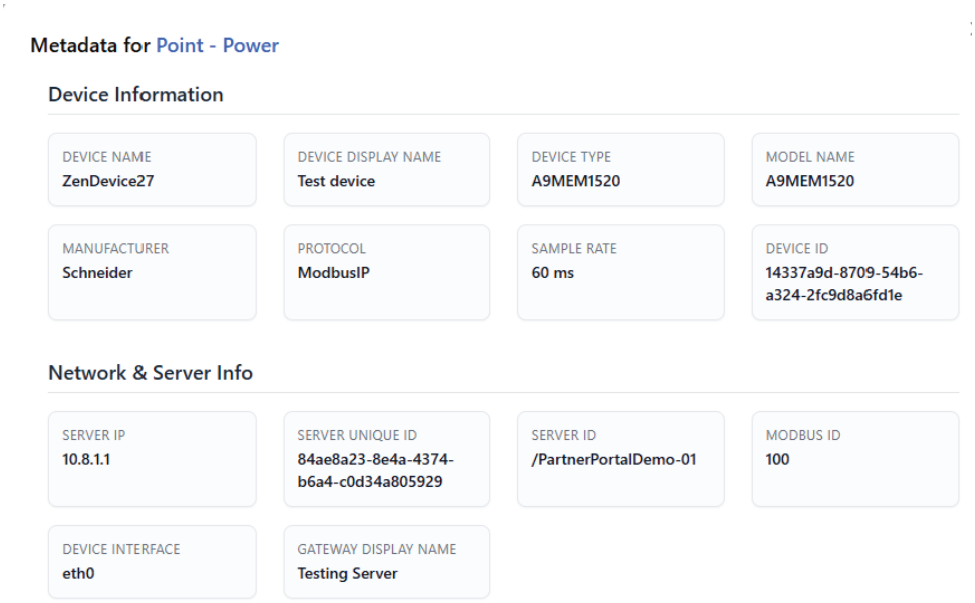
Use the Global Search to search by:

1. **Device Name**
2. **Parameter Name**
3. **Equipment Name**
4. **Equipment Type**

Post-Plot Features



Once the data is plotted, user can view the following list of parameters:

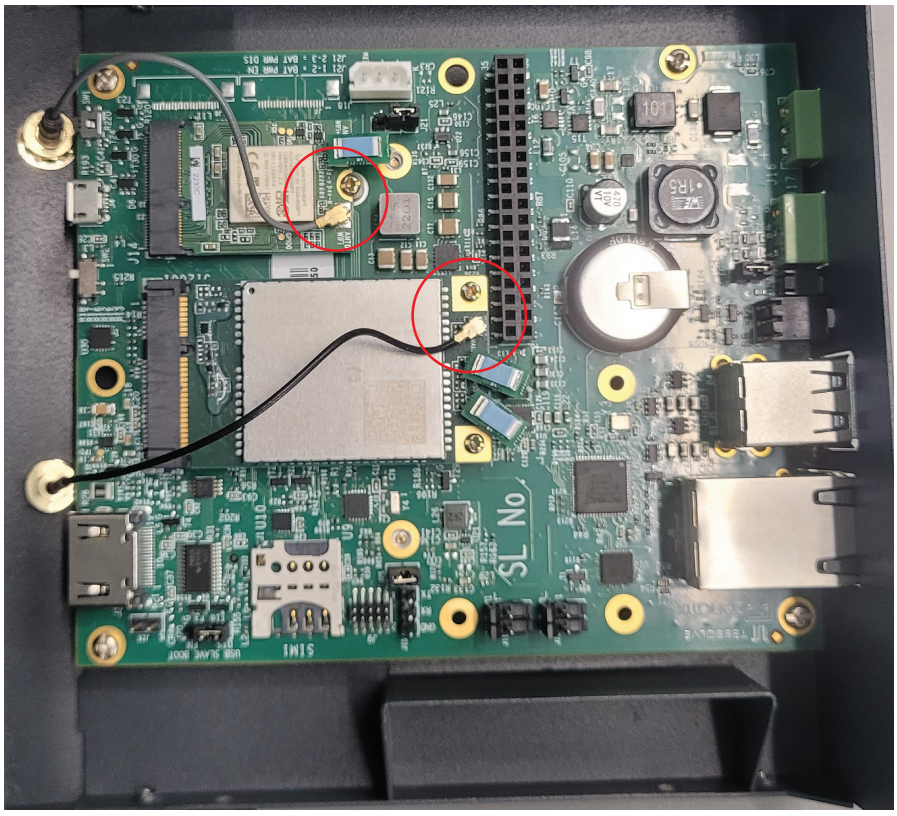


1. Click icon to view meta information.
2. Click icon to hide/unhide parameters.
3. Click icon to remove a parameters.
4. Plot a maximum of 10 parameters at once.
5. Select up to 3 axes for plotting based on the data type.

Troubleshooting

The troubleshooting steps for some known issues are listed below:

1. **Issue: If the hardware is missing in the box?**
   - If you find that essential hardware components are missing from the box, please contact your coordinator for assistance in resolving the hardware mismatch issue.
2. **Issue: Internet is not working even if an active SIM is installed inside the Flex-Server?**
   - If you are experiencing issues with the internet not working, even with an active SIM card installed in the Flex-Server, consider the following steps to resolve the problem:
     1. Antenna connection check:
        a. Make sure that the antenna is correctly connected, referring to the provided image.
        b. If the connection is loose or removed, secure it properly.
        c. After resolving the connection issue, wait for 5 minutes for the Flex-Server to come online.
   - Location or SIM operator change:
     1. If the antenna connection is secure and the issue persists, consider changing the location of the Flex-Server.
     2. Alternatively, try using a different SIM operator, as the network coverage at the current location may be insufficient.
     3. If the problem persists after trying these steps, please contact Schneider Electric for further assistance www.se.com/buildings.



3. **Issue: Flex-Server is on cellular network, however, not coming online.**
   - Follow the below steps to get the Flex-Server online:
     1. Check the antennas and antenna cables properly connected.
     2. Try removing the SIM card and inserting it again.

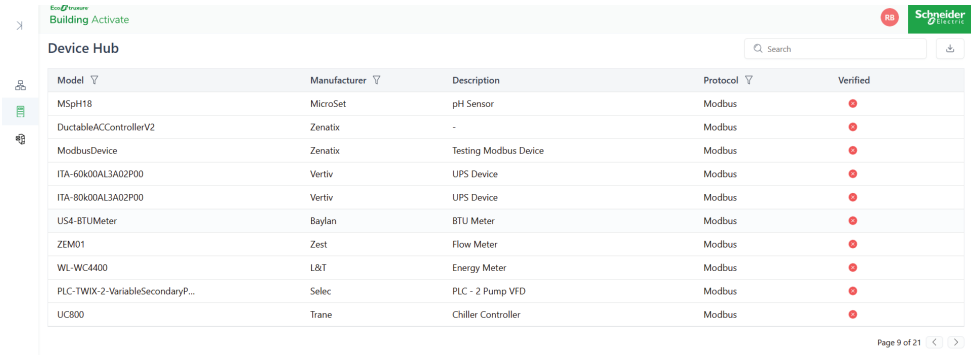
        NOTE: Pin enabled SIM card is not supported.

4. **Issue: Flex-Server is online; however, the data is lost, or delayed response is observed?**
    - In case of cellular network:
        1. Check the cellular network signal strength on the plotter.
        2. Check if the data plan is active on the SIM card.
    - In case of Wi-Fi network:
        - Check the Wi-Fi signal strength and speed on the Wi-Fi network using another device (which can be a mobile or a laptop).
5. **Issue: If RS485 port is not sending the data?**
    - Follow the below steps if the RS485 port is not sending the data:
        1. Check if the connections are done as per the installation instructions.
        2. Check if correct port is configured.
        3. Check again, if the connections are not reversed.
        4. Check for loose wires.
        5. Check the Modbus/BACnet ID is correct.
        6. Check the baud rate configured for the end device.
        7. Check if any loose strand is shorting on the bus or to the ground.
        8. Check if any Modbus device is connected to BACnet bus or vice-versa.
        9. Check if the number of devices in the loop are as per the specifications in installation instructions.
        10. Check if the loading of devices causes the resistance to drop or to increase significantly. You should not connect more than two resistors on a single bus.
        11. Check if wires are used as per the specifications in the installation instructions.
6. **Issue: Cannot Edit Compute Module and Carrier Board Number After Commissioning the Flex-Server**
    - The Compute Module and Carrier Board Number are unique identifiers. Once mapped to a server, they cannot be edited or reassigned to another server.
7. **Issue: Network Configuration is Not Visible**
    - The network configuration is retrieved directly from the Flex-Server.
    - If the information is missing, it indicates that the Flex-Server is offline, or the dashboard is unresponsive.
8. **Issue: Next button is always enabled**
    - The **Next** button is designed to navigate to the next page without validating whether changes were saved.
    - If you edit data but does not save it before clicking **Next** the changes will be lost.
9. **Issue: Unable to delete Space Configuration**
    - Currently, delete functionality is available for equipment only. **Space Configuration** cannot be deleted at this time.
10. **Issue: Unable to update Site Card Information**
    - The site name, location, and latitude/longitude are defined in the backend and cannot be changed through the dashboard.

Device Hub

What's in This Part

Overview



The Device Hub page provides a comprehensive list of templatized devices available in the Deployment Portal. It includes detailed information about each device, such as **Model**, **Manufacturer**, **Description**, **Protocol**, and **Verified** verification status. You can filter and search devices, and view mapping details for each device and download the list of devices.

Key Features

- **Comprehensive device listing**: Displays all registered devices with key details such as **Model**, **Manufacturer**, **Description**, **Protocol**, and **Verified** verification status.
- **Search and filter capabilities**: Easily search and apply filters to quickly locate specific devices.
- **Device Verification Status Indicators**:
  - ✅ indicates the device data has been evaluated and successfully integrated.
  - ❌ indicates the device is integrated, but its data has not been evaluated yet.
- **Parameter-Level Details**: Click a device entry to reveal parameters details and mapping templates.
- **Download**: Click icon located at the top right corner to download the list of all devices.

How to Use the Device Hub

Accessing the Device Hub

1. Go to the main menu on the left side of the Deployment Portal.
2. Click **Device Hub** to open the device listing page.

Viewing the Device List

1. The landing page displays a paginated list of devices with the following columns:
   - **Model**
   - **Manufacturer**
   - **Description**
   - **Protocol**
   - **Verified**
2. Use the pagination controls at the bottom to navigate through multiple pages.

Searching for a Device

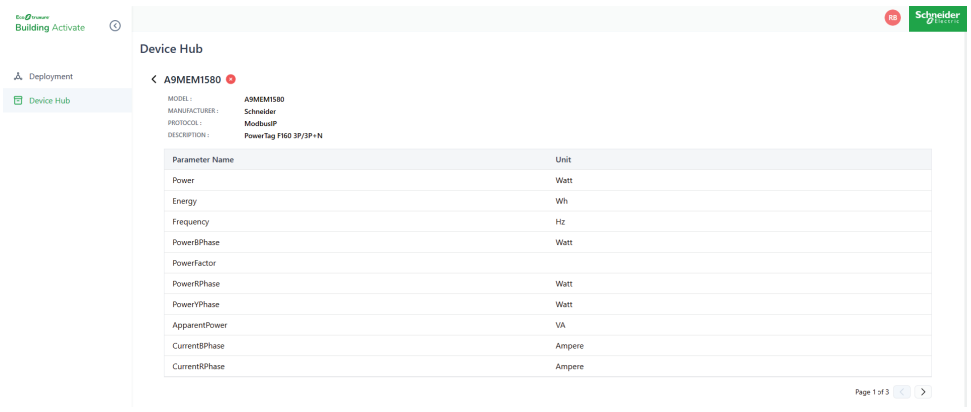
1. Use **Search** option at the top of the list.
2. Enter keywords such as **Model** name or **Protocol** to narrow the results.

Filtering Devices

1. Click ▼ icon next to any column header (for example, Protocol or Manufacturer).
2. Select your desired criteria to filter the list.

Viewing Detailed Device Parameters

1. Click any row in the device list to open the detailed view.
2. The detail page includes the device's parameter list and its mapping template.



How to use Local Web Dashboard (LWD)

What's in This Part

Introduction

The Local Web Dashboard (LWD) is a web-based interface that allows users to access and configure the Flex-Server over an Ethernet connection. It is compatible with major web browsers like Chrome, Firefox, Safari, and Edge.

Through the web dashboard, users can:

- Manage network settings
- View hardware information
- Override equipment settings (post-commissioning)

NOTE:

1. By default, LWD is not enabled on any Flex-Server.
2. To configure or use LWD, the user must request the support team to enable it for their Flex-Server.
3. Once enabled, it is strongly recommended that the user logs in to LWD and changes the default password immediately.
4. If a site has multiple Flex-Server’s (like 3 or 4 servers), the user must request LWD to be enabled on each server individually.

System Requirements

The System requirements section provides the necessary information about the Hardware, Software and Network .

Hardware

- A laptop with an Ethernet port or Ethernet-to-USB adapter
- A standard Ethernet cable
- A server with a pre-defined static IP address.
  (IP can found in the Network Configuration section of the dashboard)

  NOTE: If the server does not configure with static IP address, then you can assign one through the dashboard interface after initial access.

Software

- A modern web browser (Chrome, Firefox, Safari, or Edge).

Network

- Access to server’s IP address (available on deployment portal).

Dashboard Connection

What's in This Chapter

Laptop Network Settings Configuration

For Windows

1. Connect Ethernet cable to your laptop and the server.
2. Go to:
   Control Panel > Network and Internet > Network and Sharing Center change adapter settings.
3. Right-click on **Ethernet** → click on **Properties**.
4. Click on **Internet Protocol Version 4** (TCP/IPv4) → click on **Properties**.
5. Enter the following:
   - IP Address: 192.168.1.10 (same subnet as server)
   - Subnet Mask: 255.255.255.0
   - Default Gateway: 192.168.1.10
6. Click **OK** to apply settings.

For macOS

1. Connect the Ethernet cable.
2. Go to:
   Preferences > System > Network > Ethernet Set Configure IPv4 to Manually.
3. Enter the following:
   - IP Address: 192.168.1.10 (same subnet as server)
   - Subnet Mask: 255.255.255.0
   - Router: 192.168.1.10
4. Click **Apply**.

   NOTE: Ethernet Disconnection Handling:
   - If there is no communication between the Flex-Server and the laptop, the active session will expire after 5 minutes, and the user will need to log in again.
   - However, if the Ethernet cable is disconnected and reconnected within 5 minutes, the session will remain active, and re-login will not be required.

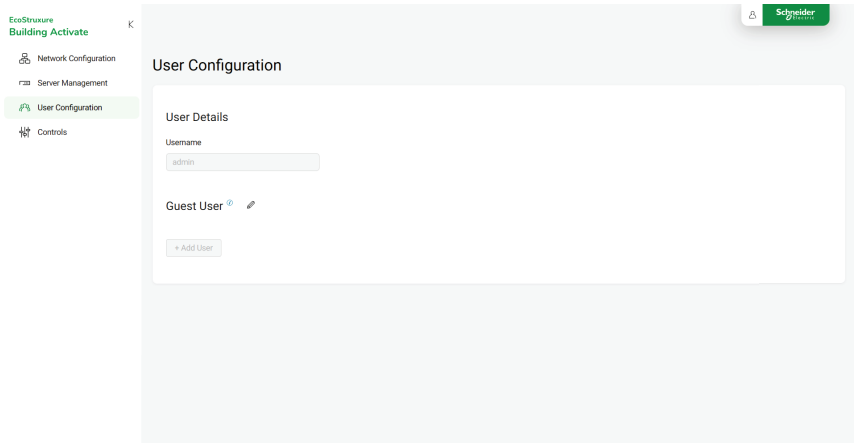
Connection Verification

1. Open your web browser.
2. Enter the server IP (for example https://192.168.1.100) in the address tab.

   NOTE:
   - Ensure that https:// is added in front of IP address.
   - Trust connection warning will appear on screen, connection should be trusted manually.

3. The LWD login screen will appear.

Logging In and Initial Setup



Default Login Credentials

Enter the default login credentials listed below.
Username: flexadmin@dashboard.local
Password: Admin@123

Password Change Guidelines

1. After initial login, the system enforces a mandatory password change.
2. New password rules:
   - At least one uppercase letter.
   - At least one lowercase letter.
   - At least one number.
   - At least one special character (#?!@$%^&*-).
   - Password length should be a minimum of 12 characters.
   - Maximum length 1500 characters.
   - Spaces are allowed.
   - Unicode characters are permitted.

User Roles and Management

The LWD has two types of users, each with different roles:

Admin User

- Can view and update all functionality of the dashboard.
- Can create or delete guest user's password.
- Cannot edit the **Hardware details**.

Guest User

- Can view all functionality of the dashboard.
- Can edit control points of equipment in the **Control** page.

Users Management

1. All user management must be done locally via LWD (not remotely).

2. Partner users can create and delete customer user credentials.
3. If a customer forgets their password, the partner must delete and recreate the user password by locally login in the system.
4. If a partner forgets their own credentials, they must contact the support team.

Session Time-out

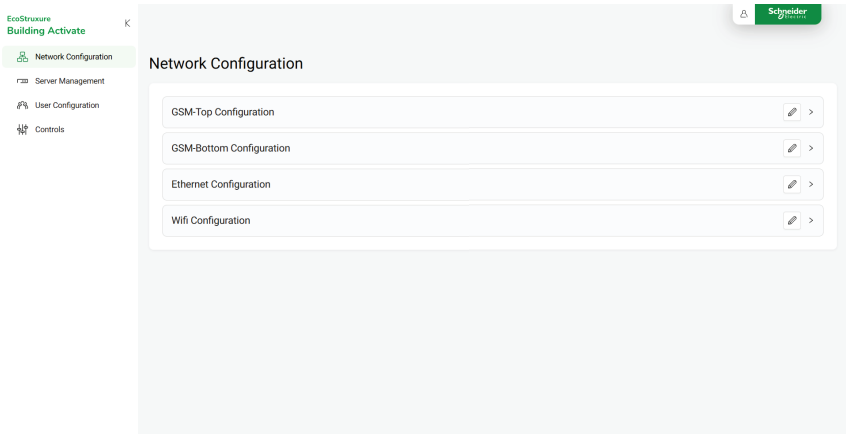
1. Inactivity session timeout: 10 minutes
2. Default session timeout: 1 hour
3. Session lock - 5 minutes (If frontend is disconnected for 5 minutes, the user will be logged out).

   NOTE:

   - Login Lockout Policy: If a user enters incorrect credentials five consecutive times, the account will be locked for 15 minutes.
   - Only one session is allowed at a time for LWD. Concurrent sessions are not supported.

Dashboard Navigation

Overview



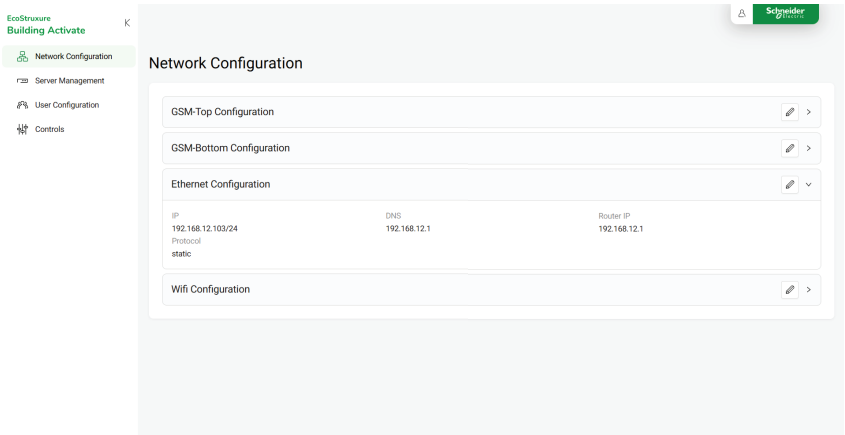
The **Home Page** of the Local Web Dashboard (LWD) provides a quick navigation panel to access key configuration and control options for your Flex Server. From **Home Page**, users can Access Network Configuration, Server Management, User Configuration, and Equipment Controls.

The home screen offers panels for:

- **Network Settings**: Ethernet, Wi-Fi, and SIM configuration
- **Hardware Info**: MAC Address, Serial Number, and SPIN Version
- **Control Screen**: Manage and sync equipment with cloud data

Network Configuration

Ethernet Configuration: Manage static IP, DNS, router IP, and protocol type.



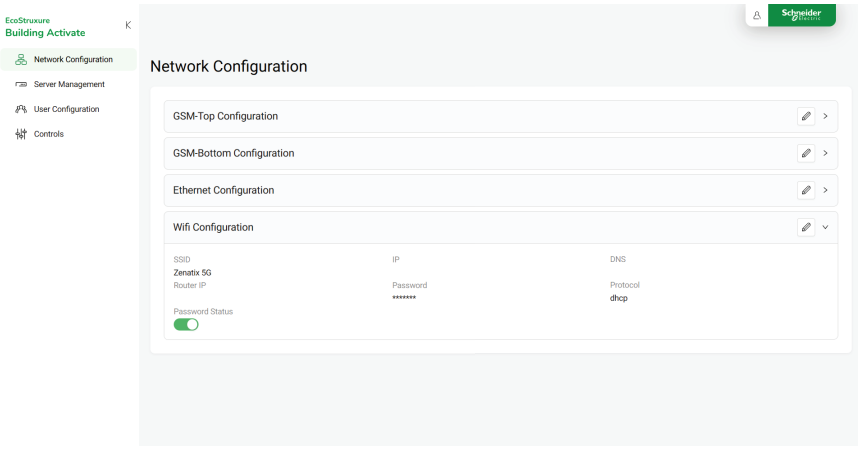
Static IP flow

Field	Description	Example
IP	Static IP address	192.168.0.150
DNS	DNS server address	8.8.8.8
Router IP	Default gateway/router address	192.168.0.1
Protocol	Set to Static for manual network settings	Static

DHCP flow

Field	Description	Example
Protocol	Set to DHCP for automatic IP configuration	DHCP

NOTE: In DHCP mode, no other fields are required. The IP, DNS, and Router IP will be auto assigned.



Wi-Fi Configuration: Configure SSID, password, router IP, DNS, and protocol (DHCP/static).

NOTE: Wi-Fi Access: Accessing LWD over Wi-Fi is not recommended. Customers should create a separate VLAN (Wi-Fi) dedicated to the IoT server to ensure secure and reliable access.

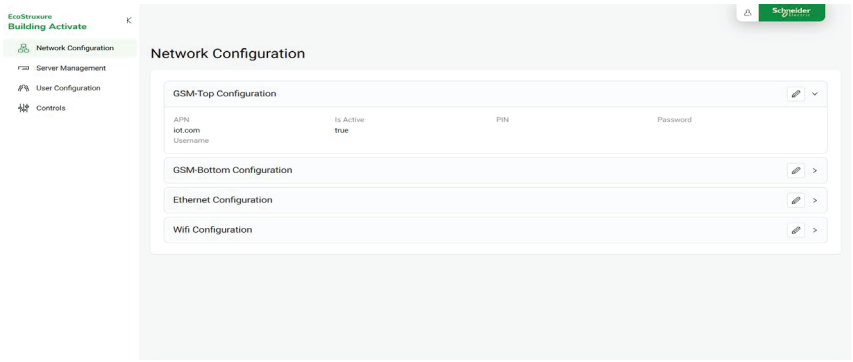
Static IP flow

Field	Description	Example
SSID	Wireless network name	Office_WiFi_01
Password	Wi-Fi Password	securewifi2024
Router IP	Default gateway for Wi-Fi network	192.168.43.1
DNS	DNS server address	8.8.4.4
Protocol	Set to Static for manual network settings	Static
Password Status	Toggle to enable/disable password authentication	True

DHCP flow

Field	Description	Example
SSID	Wireless network name	Guest_Network
Password	Wi-Fi password (if Password Status is True)	welcome123
Protocol	Set to DHCP for automatic IP settings	DHCP

GSM Top / GSM Bottom Configuration: Set APN, Username, Password, PIN, and View activation status for cellular connectivity.

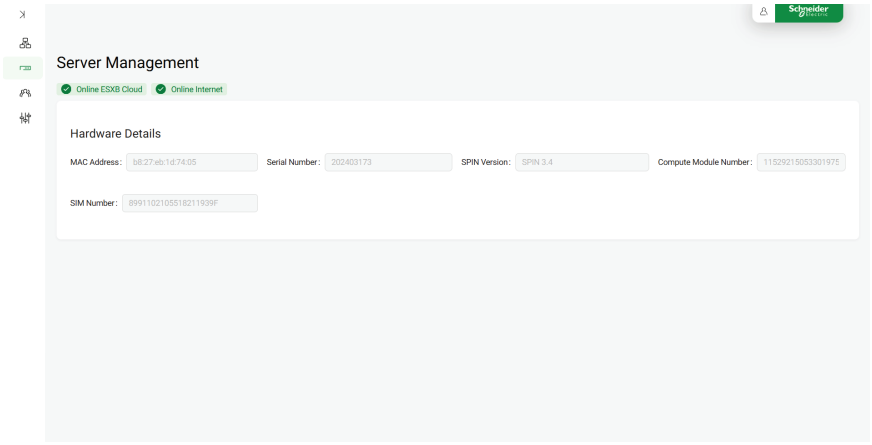


Field	Description
APN	Access Point Name for network connectivity
Username	SIM username (if provided by network)
Password	SIM password (if provided by network)
PIN	SIM PIN (if applicable)

Server Management/Hardware Details

The **Hardware Details** section provides essential information about the device's network interface, onboard compute module, and installed SIM card.

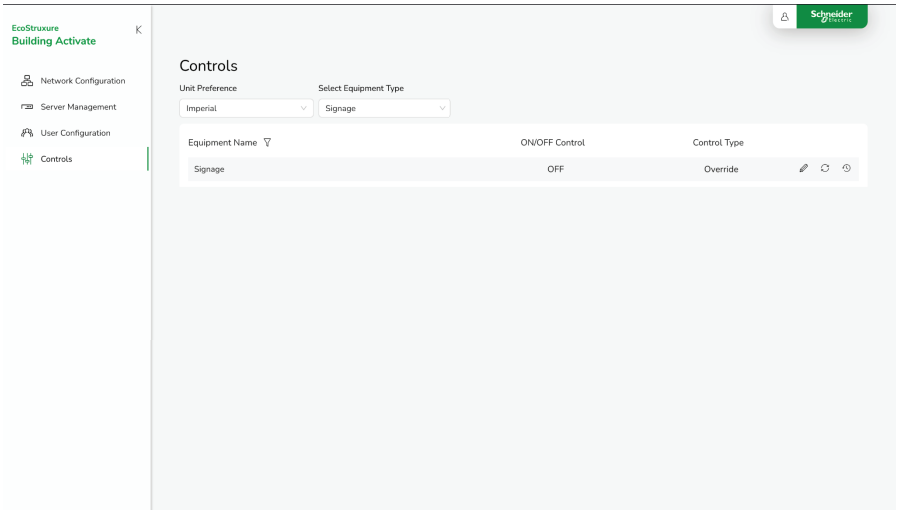
NOTE: The fields listed below are read-only and cannot be modified locally.



Field	Description
MAC Address	Displays unique hardware address of the device's network interface.
Serial Number	Displays unique identifier assigned to the hardware by the manufacturer.
SPIN Version	Displays version number of the SPIN software currently running on the device.
Compute Module Number	Displays identifier for the onboard compute module inside the device.
SIM Number	Displays unique number associated with the SIM card installed in the device.

NOTE: We do not recommend to use SIM with username, password and PIN, If SIM is not having these information, these can be skipped as information can be automatically configured via automatic APN script, take reference from the SIM configuration section., page 25

Control Screen



The Controls section of the Local Web Dashboard (LWD) allows users to view and manage operational controls for equipment connected to the current Flex-Server.

Field	Description
Unit Preference	Select the preferred measurement system (Imperial/Metric).
Select Equipment Type	Choose the equipment type available under the current Flex-Server.
Equipment Name	Displays the name of the connected equipment.
ON/OFF Control	Shows the current operational status (**ON/OFF Control**) of the equipment.
Control Type	Displays the control method – typically Override.

Click the Edit icon(✎) next to the Control Type to apply a temporary Override.

You can select one of the following durations for the override:

- 30 Minutes
- 1 Hour
- 2 Hours

The selected **ON/OFF Control** state will remain active for the chosen period, after which it will automatically return to its scheduled or default behaviour.

- User can view list of equipment synced from the cloud.
- User can verify equipment name, override duration and status.

  NOTE:

  - Equipment names are read-only on the local dashboard and can only be edited from the cloud.
  - All control actions on the Local Web Dashboard (LWD) are automated.
  - Any configuration changes on the LWD require a rollout from the cloud, as the dashboard operates on the edge.
  - Only parameters with Actuation Type: True and Visibility: True will be displayed for the selected equipment on the LWD.
  - Only equipment under the current Flex-Server will be visible – no cross-Flex-Server equipment will appear on this dashboard.

Troubleshooting Tips

If the dashboard's connectivity fails, follow the below steps and re-connect.

- **Check Cable Connection:** Make sure the cables are connected properly on both ends.
- **Disable Wi-Fi:** Turn off active wireless networks to avoid IP conflicts.
- **Verify IP Configuration:** Check that your laptop IP address is entered correctly.
- **Review Firewall Settings:** Allow access to your security software or firewall.
- **Restart Devices:** Restart both laptop and server.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

DOCA0343EN-02