EcoStruxure Building-IoT

IoT Solution

Operating Guide

04-10050-03-en
February, 2026

Life Is On | Schneider Electric

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.

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.

Purpose of This Guide

This guide provides information about EcoStruxure™ Building-IoT Sensor Solution and how it is used to give System Integrators, Integrated Workplace Management System (IWMS) Players, Facility Managers, and Commercial Real Estate (CRE) Owner/Managers the ability to capture, move and manage IoT data seamlessly, reliably and securely across the globe. It is an integrated solution that provides access to real-time building management data in terms of Occupancy, Indoor Air Quality (IAQ), and Space Utilization.

This IoT Sensor Solution provides customers with an ecosystem of state-of-the-art sensors and device management capabilities for easy deployment and management of IoT sensors at scale.

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

Cybersecurity Safety Notice

The IoT Sensor Solution Cloud Portal is powered using Enterprise Grade Security. Each sensor has embedded security in the hardware and network.

NOTICE

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Disable unused ports/services 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 loss of data or unauthorized system access.

For more information, see section 8 “Hardening Specifics for Cybersecurity” on page 60.

How to Report a Cybersecurity Vulnerability

In the event that a security vulnerability is discovered or suspected, the portal found at www.se.com/ww/en/work/support/cybersecurity/report-a-vulnerability.jsp is to be used for reporting and to establish communication around suspected issues.

Table of Contents

1 Terms and Hierarchy

There are various terms used in the portal to define customers and their real estate properties. The Hierarchy can be split into two parts: Clients and Real Estate.

What's in This Chapter?

1.1 Clients

Clients can be further split into two segments: Partners and Customers.

1.1.1 Partner

A Partner is an entity that procures the devices from Schneider Electric and integrates them with its product to provide services to its own or end-customer’s real estate assets.

1.1.2 Customer

A Customer is an entity that avails services from a partner to manage its real estate assets.

1.2 Real Estate

The hierarchy of real estate is as follows: Site -> Building -> Floor -> Space

1.2.1 Site

A Site is the largest form of real estate and can have one or more buildings. A site could be anything such as university campus, commercial malls, or a special economy zone. Partners and Customers can have multiple sites at multiple locations.

1.2.2 Building

A Building refers to a single real estate building inside a site. For example, if we consider a university campus as a site, then Library, Auditorium or indoor stadium can be considered as individual buildings.

1.2.3 Floors

A Building might have multiple floors and floors will have multiple spaces.

1.2.4 Spaces

Spaces are the smallest form of real estate, and they are used to point out the location of a device. They could be anything, such as a desk, meeting room, or even a washroom.

1.3 Devices

Devices could either be a gateway or a sensor. Gateway is a device that collects data from all the sensors and pushes it to the cloud portal through the internet connectivity. It can also receive commands from the portal. Sensor is a device that measures some parameter and pushes the data to the gateway.

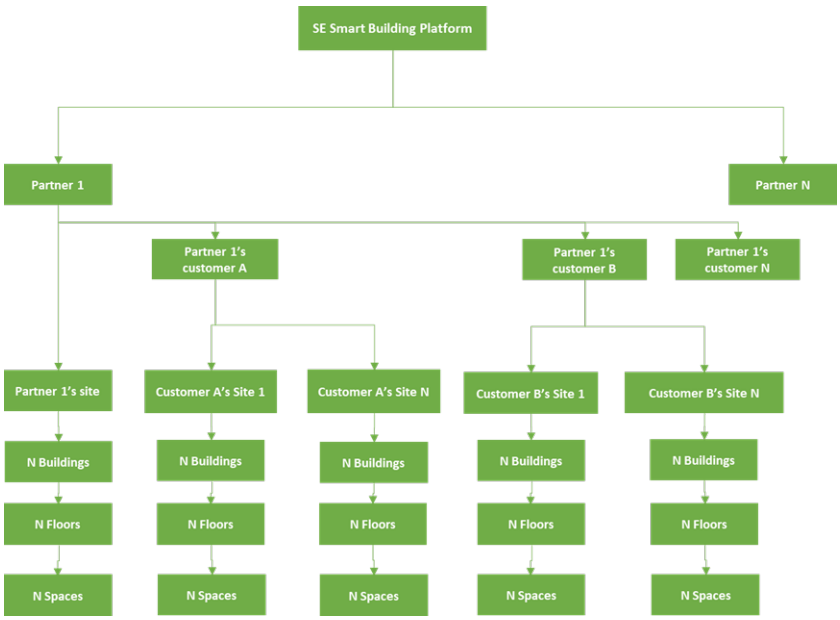

Figure – Hierarchy

2 User Account Handling

What's in This Chapter?

2.1 User Account Handling

The IoT Sensor Solution Cloud Portal authenticates users via username and password.

There are four different types of users in the portal:

- Partner Administrator
- Customer Administrator
- Site Administrator
- Installer

Table – IoT Sensor Solution Users

Modules	Partner Admin	Customer Admin	Site Admin	Installer
Manage Users	x	x	x	
Manage Customers	x			
Manage Sites	x	x		
Manage Buildings/Floors/ Spaces	x	x	x	x
Manage Devices	x	x	x	x
FW Updates	x			
Subscription	View + Assign	View + Assign	View + Assign	View

2.2 Commissioning Process

To complete the commissioning process, the Installer must visit the site and select the partner, customer, and sites in the Schneider Electric Smart Building portal, which is already created by the Line of Business (LoB) Solution Architect in the pre-commissioning phase. The Installer will then select the building, floor, and space, before installing devices following the customer's requirements.

3 IoT Sensor Solution Cloud Portal

The IoT Sensor Solution Cloud Portal allows you to:

- Update or delete user profiles
- Change passwords
- Install gateways and sensors
- Allow sensors to join a network
- Delete devices
- And more

What's in This Chapter?

3.1 Logging on to the IoT Sensor Solution Cloud Portal

You log on to IoT Sensor Solution Cloud Portal to display and interact with the connected gateway and sensors.

The Cloud Portal provides functionality for managing devices—such as gateways and sensors—on the floor plan and for viewing sensor measurements on dashboards. However, it does not allow modification of any gateway parameters. This functionality is distinct from that of the Gateway Configuration Portal. User management and overall functionality of the Cloud Portal are supported exclusively by Schneider Electric.

> **NOTE:** Please get in touch with your Sales Representative for initial account creation. The Line of Business (LoB) Solution Architect is responsible for creating user accounts. When an account is created, the user will receive a registration message at the email address defined in the profile.

For more information, see section 2 “User Account Handling” on page 10.

To log on to the IoT Sensor Solution Cloud Portal

1. In a web browser, visit the Schneider Electric Building Portal at https://ecostruxure-building-iot-sensor-solution.se.app/.
2. On the **Login** page, in the **Email** box, type the email address for this profile.

   NOTE: If you are entering the portal for the first time, you must complete the registration process by entering the activation code sent to you by email.
3. Click **Continue**.
4. In the **Password** box, type the password for this user profile.
5. Click **Login**.

3.2 Logging on to IoT Sensor Solution Cloud Portal for Schneider Electric Employees

You log on to IoT Sensor Solution Cloud Portal to display and interact with the connected gateway and sensors. As a Schneider Electric employee, the procedure is slightly different.

For more information, see section 2 “User Account Handling” on page 10.

To log on to IoT Sensor Solution Cloud Portal

1. In a web browser, visit the Schneider Electric Building Portal at https://ecostruxure-building-iot-sensor-solution.se.app/.
2. On the **Welcome** page, click on the Single Sign-On button .
3. Authenticate using **PingID**.
4. Complete the PingID authentication process on your registered device to securely access the Cloud Portal.

3.3 Updating Profile

You update a profile to change the information related to a user account.

For more information, see section 2 “User Account Handling” on page 10.

To update a profile

1. In the IoT Sensor Solution Cloud Portal, tap the user profile menu button .
2. On the menu, click **Update Profile**.
3. On the **Profile** screen, on the **My Profile** tab, change the Name, Language Preference, Email and Mobile Number, as needed.
4. On the **My address** tab, change the information as needed.
5. Click **Update**.

3.4 Changing Password

You change a password to update your access to the IoT Sensor Solution Cloud Portal.

For more information, see section 2 “User Account Handling” on page 10.

To change a password

1. In the IoT Sensor Solution Cloud Portal, tap the user profile menu button .
2. On the menu, click **Change Password**.
3. On the **Change password** screen, in the **Existing password** box, type your current password.
4. In the **New password** box, type your new password.

   NOTE: The following special characters can be used:

   !*#$%'()*+-/:;<=>?@[\]^_'{|}~
5. Click **Change Password**.

3.5 Deleting an Account

You delete an account to remove a specific profile from the platform.

For more information, see section 2 “User Account Handling” on page 10.

To delete an account

1. In the IoT Sensor Solution Cloud Portal, tap the user profile menu button .
2. On the menu, click **Update Profile**.
3. On the **Profile** screen, under the **Security and Preferences** tab, click on the **Delete my account** button.
4. On the **Account Deletion Request** screen, click **Next** to confirm the operation.
5. On the **Account Deletion Request Confirmation** screen, click **Delete My Account**.

3.6 Installing a Gateway

You install a gateway to onboard a new device on a floor plan.

For more information, see section 2 “User Account Handling” on page 10.

To install a gateway

1. In the IoT Sensor Solution Cloud Portal, on the **Device Management** screen, click **Install Device**.

Continued on next page

2. On the **Site Selection** screen, click:
   - **My Partner's Site**: To install a device on a partner's site.
   - **My Partner's Customer's Site**: To install a device on a partner's customer's site.
3. Select the **Partner**, **Customer**, **Site**, **Building**, and **Floor**. The floor plan will be displayed on the screen.
4. Click the radio button to select **Install Gateway**.

   TIP: Always install a gateway before installing sensors.
5. On the **Floor Plan View**, click anywhere to add the gateway.
6. On the **Map Device** popup screen, select a **Space ID** from the drop-down list.

   NOTE: The Space ID is normally pre-populated based on your selection, but you can still make a selection from the drop-down list.
7. In the **Gateway UID** box, type the serial number of the gateway.
8. Click **Map**.
9. Repeat steps 4 to 8 to install other gateways.
10. Click **Save Mapping** once you are done adding devices.
11. Click **Proceed to Network Lock**.

You have successfully onboarded a gateway. On the floor plan, you can see a blue triangle for a gateway ▲ in the selected space. The color of the triangle indicates the connection status of the device:

- Blue: The device is in unknown status and has not established a connection with the cloud yet.
- Green: A connection to the Cloud is established.
- Red: The established connection is lost.

To complete the onboarding of devices to the portal, you must allow sensors to join the network. For more information, see section 3.9 “Allowing Sensors to Join a Network” on page 16.

3.7 Adding Another Gateway

You can add another Gateway to the Sensor network to create redundancy and improve robustness.

For more information, see section 3.6 “Installing a Gateway” on page 13.

To add another gateway

1. Log into the IoT Gateway Configuration Portal of the additional gateway.

Continued on next page

2. On the **Wireless** screen, configure the parameters below using the same values as for the already installed gateway:
   - **Network**
   - **Channel**
   - **Auth Key**
   - **Cipher Key**
3. In the **Address** box, enter the unique address that identifies the gateway on the wireless network. For more information, see section 4.11 “Configuring the Wireless Connection” on page 24. This is the only value that needs to be distinct between Gateways that share the same network.
4. Click **Submit** to save the settings.

You have successfully added another gateway.

When you configure the gateways with the same values for the parameters mentioned in step 2, and assign each a unique address, they will share the network load.

If some sensors are unable to stay connected to the initial gateway, they will automatically connect to the redundant gateway—provided it is reachable. This behavior is part of the network’s self-healing capability, helping to prevent sensors from going offline even if one of the gateways becomes unavailable.

3.8 Installing a Sensor

You install a sensor to onboard a new device on a floor plan.

For more information, see section 3.6 “Installing a Gateway” on page 13.

To install a sensor

1. In the IoT Sensor Solution Cloud Portal, on the **Device Management** screen, click **Install Device**.
2. On the **Site Selection** screen, click:
   - **My Partner's Site**: To install a device on a partner's site.
   - **My Partner's Customer's Site**: To install a device on a partner's customer's site.
3. Select the **Partner**, **Customer**, **Site**, **Building**, and **Floor**. The floor plan will be displayed on the screen.
4. Click the radio button to select **Install Sensor**.

   TIP: Always install a gateway before installing sensors.
5. On the **Floor Plan View**, click anywhere to add the sensor.

6. On the **Map Device** popup screen, select a **Space ID** from the drop-down list.

   NOTE: The Space ID is normally pre-populated based on your selection, but you can still make a selection from the drop-down list.

7. In the **Gateway UID** box, type a unique identifying name.
8. Click **Map**.
9. Repeat steps 4 to 8 to install other devices.
10. Click **Save Mapping** once you are done adding devices.
11. Click **Proceed to Network Lock**.

You have successfully onboarded a sensor. On the floor plan, you can see a blue circle for a sensor in the selected space. The color of the circle indicates the connection status of the device:

- Blue: The device is in unknown status and has not joined the network yet.
- Green: The device has joined the network.
- Red: The device has left the network.

To complete the onboarding of devices to the portal, you must allow sensors to join the network. For more information, see section 3.9 “Allowing Sensors to Join a Network” on page 16.

3.9 Allowing Sensors to Join a Network

You allow sensors to join a network to complete the onboarding of devices to the portal.

NOTE: You must first install new devices. For more information, see section 3.8 “Installing a Sensor” on page 15.

For more information, see section 3.6 “Installing a Gateway” on page 13.

To allow sensors to join a network

1. On the **Device Management** page, once you have installed new devices on the **Floor Plan View**, click the radio button to select **Gateway List View**. You can see a list of the gateways that were added to the floor plan.
2. On the **Gateway List View**, click the toggle switch to **Unlock** a network . This will allow sensors to join the network.
3. On the **Network Lock** confirmation popup, click **Yes** to unlock the network.
4. On the **Gateway List View**, once all the sensors go online ., click the toggle switch to **Lock** the network .
5. On the **Gateway List View**, in the **Sensors** column, you can click on the hyperlinked number to see the list of sensors.

Continued on next page

6. In the **Sensor UID** column, click the hyperlinked name to see the details of a sensor.

You have now successfully onboarded devices to the portal.

3.10 Deleting a Device

You delete a device to remove a device from the network and floor plan.

For more information, see section 3.8 “Installing a Sensor” on page 15.

To delete a device

1. On the **Device Management** page, click the radio button to select **Sensor List** or **Gateway List View**. You can see a list of the gateways and sensors that were added to the floor plan.
2. In the selected **List View**, click the delete button 🗑 next to the gateway or sensor you wish to remove from the platform.
3. On the **Delete Gateway/Sensor** confirmation popup, enter the **UID** of the device to confirm its deletion, then click **Yes**.
4. Press and hold the **Reset** button on the sensor for more than 10 seconds to perform a Settings Reset. This will remove the sensor from the wireless network.

You have successfully removed a device from the network and floor plan.

3.11 Moving a Device

You can reposition a device to a different location within the floor plan after installation, if needed.

For more information, see section 3.8 “Installing a Sensor” on page 15.

To move a device

1. In the **Floor Plan** view, click **Move Device**.
2. Select the device you want to move.
3. Drag the device icon to the desired location on the floor plan.
4. In the **Move Device** dialog box, select the target **Space ID**.
5. Click **Move** and wait for the confirmation message.

You have successfully moved a device to a new location.

4 IoT Gateway Configuration Portal

A Building-IoT multi-protocol gateway:

- Supports simultaneous communication with multiple protocols
- Connects up to 200 devices in a robust mesh network
- Supports Power Over Ethernet (PoE)
- Includes a GSM-LTE slot

Each gateway is managed using the Gateway Configuration Portal.

What's in This Chapter?

4.1 Logging on to IoT Gateway Configuration Portal

You log on to IoT Gateway Configuration Portal to configure the Internet connection, the system time and other parameters required to have the gateway connect to the IoT Sensor Solution Cloud.

To log on to IoT Gateway Configuration Portal

1. Configure the IP address of your computer to 10.110.210.1, with the subnet mask as 255.255.255.0.
2. Connect an Ethernet cable to the Gateway.

Continued on next page

3. In a web browser, visit the IoT Gateway Configuration Portal at https://10.110.210.2.
4. Tap to Continue to https://10.110.210.2 despite the security warning.
5. On the login page, in the **Username** box, type the name of this profile. The default—and only—username allowed to access the portal is **admin**.
6. In the **Password** box, type the password for this user profile. The default value is **P@ssword**.

   NOTE: On the first login, the Configuration Portal will require that the default password be changed. It is recommended to keep the new password confidential and safe. Once the new password is entered correctly, the Configuration Portal will return to the login page. Enter the new credentials.
7. Click **Login**.

   NOTE: The Configuration Portal will lock out the user if there are five failed login attempts. Click on **Forgot Password** from the login page to start the process of resetting the password. Enter the username (**admin**). A unique sequence of characters will be generated. Contact Technical Support with this sequence of characters to complete the password reset.

4.1.1 Password Policy

Password Requirements

Passwords must meet the following criteria:

- At least one lowercase letter
- At least one uppercase letter
- At least one digit
- At least one special character
- A minimum length of 12 characters
- A maximum length of 1,500 characters
- Commonly used passwords are prohibited

Password Expiration Policy

Passwords will expire every 180 days for security purposes. After expiration, users will be required to reset their password.

NOTE: A password reset may also be required after the first login or following a firmware upgrade if there is a change in time synchronization.

4.2 Configuration of the Internet Connection to Access the Cloud Portal

The IoT Gateway provides three ways to allow it to connect to the Internet for accessing the Cloud Portal.

- Ethernet
- WiFi
- Cellular

NOTE: For effective and reliable communication, ensure that only one of the three connectivity modes listed above is configured.

NOTE: It is crucial to perform a Network Reset before switching between different connectivity modes. For more information, see section 4.16 “Gateway Reset Options” on page 26.

NOTICE
CONNECTION REQUIREMENTS • Ports 443 and 123 must be opened (outbound) for the IoT Gateway to communicate with the Cloud. **Failure to follow these instructions can result in connection issues between the IoT gateway and the Cloud.**

NOTE: A gateway does not serve as an access point for any external devices.

4.3 Configuration of the Ethernet Connection

The IoT Gateway supports DHCP and static IP address configurations. Note that if the current connection to the configuration portal is via Ethernet when a new IP address is configured, the configuration portal will disconnect because the IP address will change. If DHCP was selected, please contact the local network administrator to find the assigned IP address. It is recommended to use a static IP address.

NOTE: Accessing the Configuration Portal via Ethernet is not recommended. For secure and reliable access, customers should create a dedicated VLAN for the IoT Gateway.

4.4 Assigning a Static IP Address to the IoT Gateway

You assign a Static IP address to the IoT Gateway to complete the network configuration.

For more information, see section 4.6 “Configuration of the WiFi Connection” on page 22.

To assign a Static IP address to the IoT Gateway

1. In the IoT Gateway Configuration Portal, on the **Network** screen, in the **Ethernet** or **WiFi** tab, click to open the **Mode** drop-down list.
2. Select **Static.**
3. In the **IP Address** box, type the static IP address in the format "aaa.bbb.ccc.ddd".
4. In the **Network Mask** box, type the network mask in the format "aaa.bbb.ccc.ddd".
5. In the **Gateway** box, type the network gateway IP address in the format "aaa.bbb.ccc.ddd".
6. In the **DNS** box, type one or more domain name servers in the format "aaa.bbb.ccc.ddd", with each entry separated by a comma (e.g., 8.8.8.8, 8.8.4.4).
7. Click **Submit** to save the settings. The Configuration Portal will be disconnected if currently connected via Ethernet or WiFi, because the gateway IP address will change.

   NOTE: Do not lose the new IP address as it will be needed for subsequent connections to the Configuration Portal.

4.5 Connecting the IoT Gateway to a Network with a DHCP Server

You connect the IoT Gateway via Ethernet cable or WiFi to a Network equipped with a DHCP Server as an alternative option to a Static IP address.

IMPORTANT: It is strongly recommended to use a Static IP address.

For more information, see section 4.6 “Configuration of the WiFi Connection” on page 22.

To connect the IoT Gateway to a network with a DHCP server

1. Connect the IoT Gateway via Ethernet cable or WiFi to a network that is equipped with a DHCP server.
2. In the IoT Gateway Configuration Portal, on the **Network** screen, in the **Ethernet** or **WiFi** tab, click to open the **Mode** drop-down list.
3. Select **DHCP.**
4. Click **Submit** to save the settings. The Configuration Portal will be disconnected if currently connected via Ethernet or WiFi, because the gateway IP address will change.

   NOTE: Do not lose the new IP address as it will be needed for subsequent connections to the configuration portal.

4.6 Configuration of the WiFi Connection

The IoT Gateway supports DHCP and static IP address configurations for WiFi connectivity. Note that if the current connection to the configuration portal is via WiFi when a new IP address is configured, the configuration portal will disconnect because the IP address will change. If DHCP was selected, please contact the local network administrator to find the assigned IP address. It is recommended to use a static IP address.

> **NOTE:** Accessing the Configuration Portal via WiFi is not recommended. For secure and reliable access, customers should create a dedicated VLAN for the IoT Gateway.

4.7 Selecting a WiFi Network

You select a WiFi network to complete the network configuration.

For more information, see section 4.6 “Configuration of the WiFi Connection” on page 22.

To select a WiFi network

1. In the IoT Gateway Configuration Portal, on the **Network** screen, in the **WiFi** tab, click to open the **SSID** drop-down list. A list of the available WiFi networks within range of the IoT Gateway is displayed.
2. Select the desired network to connect to**.**

   > **NOTE:** If it is not in the list, refresh the page or enter the SSID of the network in the **Hidden SSID** text box.
3. In the **Password** box, type the password for this specific network.
4. Click **Submit** to save the settings.

   > **NOTE:** The Gateway must connect to a WiFi network that does not require a login portal with a separate username and password.

4.8 Assigning a Static IP Address to the IoT Gateway

You assign a Static IP address to the IoT Gateway to complete the network configuration.

For more information, see section 4.6 “Configuration of the WiFi Connection” on page 22.

To assign a Static IP address to the IoT Gateway

1. In the IoT Gateway Configuration Portal, on the **Network** screen, in the **Ethernet** or **WiFi** tab, click to open the **Mode** drop-down list.
2. Select **Static.**

Continued on next page

3. In the **IP Address** box, type the static IP address in the format "aaa.bbb.ccc.ddd".
4. In the **Network Mask** box, type the network mask in the format "aaa.bbb.ccc.ddd".
5. In the **Gateway** box, type the network gateway IP address in the format "aaa.bbb.ccc.ddd".
6. In the **DNS** box, type one or more domain name servers in the format "aaa.bbb.ccc.ddd", with each entry separated by a comma (e.g., 8.8.8.8, 8.8.4.4).
7. Click **Submit** to save the settings. The Configuration Portal will be disconnected if currently connected via Ethernet or WiFi, because the gateway IP address will change.

   NOTE: Do not lose the new IP address as it will be needed for subsequent connections to the Configuration Portal.

4.9 Connecting the IoT Gateway to a Network with a DHCP Server

You connect the IoT Gateway via Ethernet cable or WiFi to a Network equipped with a DHCP Server as an alternative option to a Static IP address.

IMPORTANT: It is strongly recommended to use a Static IP address.

For more information, see section 4.6 “Configuration of the WiFi Connection” on page 22.

To connect the IoT Gateway to a network with a DHCP server

1. Connect the IoT Gateway via Ethernet cable or WiFi to a network that is equipped with a DHCP server.
2. In the IoT Gateway Configuration Portal, on the **Network** screen, in the **Ethernet** or **WiFi** tab, click to open the **Mode** drop-down list.
3. Select **DHCP.**
4. Click **Submit** to save the settings. The Configuration Portal will be disconnected if currently connected via Ethernet or WiFi, because the gateway IP address will change.

   NOTE: Do not lose the new IP address as it will be needed for subsequent connections to the configuration portal.

4.10 Configuring the Cellular Connection

You configure the Cellular connection of the IoT Gateway to complete the network configuration.

The gateway supports an LTE connection to the Cloud. The Cellular configuration menu displays the IMEI and Operator and Phone Number (if configured). A SIM card with a data plan is required to enable this feature. To enable the LTE connection for Internet connectivity please follow these steps. The SIM must be inserted in the gateway before powering it on.

For more information, see section 4.2 “Configuration of the Internet Connection to Access the Cloud Portal” on page 20.

To configure the Cellular connection

1. Power off the IoT Gateway.
2. Insert the SIM card into the corresponding slot on the front panel.
3. Power on the IoT Gateway.
4. Connect to the IoT Gateway Configuration Portal. For more information, see section 4.1 “Logging on to IoT Gateway Configuration Portal” on page 18.
5. In the Configuration Portal, on the **Network** screen, in the **Cellular** tab, enter the **Operator APN** in the corresponding box.
6. In the **Username**, **Password** and/or **SIM Card Pin** boxes, enter the Sim card credentials as needed.
7. Click **Submit** to save the settings.

NOTE: It may take a few minutes for the connection to be established.

4.11 Configuring the Wireless Connection

You configure the wireless settings to establish a secure wireless network for device communication.

To configure the Wireless connection

1. In the **Stack Version** box of the Configuration Portal, you will see the version of the firmware currently being used by the wireless radio.
2. In the **Address** box, enter a unique address (between 1 and 2147483647 OR between 2164260864 and 4292967294) used to identify the gateway on the wireless network.
3. In the **Network** box, enter the network ID (between 1 and 5570559 OR between 5636096 and 11141119 OR between 11206656 and 16777214) used to identify the wireless network in the wireless spectrum.
4. In the **Channel** box, enter the channel number (between 1 and 40) used during the commissioning/joining process only.

Continued on next page

5. In the **Auth Key** box, enter a string of 32 characters composed of numbers 0-9 and A-F. It is used for network security.
6. In the **Cipher Key** box, enter a string of 32 characters composed of numbers 0-9 and A-F. It is used for network security.

   IMPORTANT: The Cipher Key must be different from the Auth Key.
7. Click **Submit** to save the settings.

   NOTE: Remember to record the wireless credentials—including Network, Channel, Auth Key, and Cipher Key. These details will be required if you plan to: add additional gateways for redundancy or replace an existing gateway in the future.

4.12 Configuring the NTP Server

You configure an NTP Server to ensure that the Gateway's system time is correct to be allowed to connect to the IoT Cloud Portal.

NOTE: For gateways running firmware version 1.4.3 or later, configuring an NTP server or setting the date and time manually is optional, not mandatory. However, if the gateway is running a firmware version earlier than 1.4.3, the following steps are mandatory to ensure a successful connection to the Cloud.

To configure the NTP server

1. In the Configuration Portal, on the **System** screen, click on the **Enable** switch below **NTP Server** to make sure it is green (enabled).
2. In the **Server Address** box, enter a new NTP server address.

   NOTE: If DHCP is used to connect to the Internet, Server Address may already be configured.
3. Click **Submit** to save the settings.

   NOTE: It is strongly recommended to use an NTP server, however the date and time can be entered manually.

   NOTE: If there is a significant difference between the previous and the new system date and time, the user will need to log in to the Configuration Portal again.

4.13 Manually Entering the Date and Time

You can manually set the gateway’s system time to enable its connection to the IoT Cloud Portal.

To manually enter the date and time

1. In the Configuration Portal, on the **System** screen, click on the **Enable** switch below **NTP Server** to make sure it is gray (disabled). Time and Date boxes will appear on the screen.
2. In the **Time** box, enter the time in 12-hour format, as hh:mmAM or hh:mmPM.
3. In the **Date** box, enter the date as yyyy-mm-dd.
4. Click **Submit** to save the settings.

   NOTE: If there is a significant difference between the previous and the new system date and time, the user will need to log in to the Configuration Portal again.

4.14 Rebooting the Gateway

You reboot the IoT Gateway to refresh its connection to the network.

To reboot the Gateway

1. In the IoT Gateway Configuration Portal, on the **System** screen, click **Reboot Gateway**.
2. Click **Yes** reboot the Gateway or **No** to return to the **System** page

   NOTE: Rebooting the Gateway will result in a loss of connection to the Configuration Portal temporarily. Once the gateway has completely booted, the Configuration Portal will be accessible again.

4.15 Logging out of IoT Gateway Configuration Portal

You log out of IoT Gateway Configuration Portal to end a session and leave the platform.

To log out of IoT Gateway Configuration Portal

1. In the IoT Gateway Configuration Portal, tap the user profile menu button .
2. On the menu, click **Logout**.

4.16 Gateway Reset Options

In the Configuration Portal, on the Settings screen, you will find a section labeled "Reset Gateway", which includes a subsection titled "Reset Types". This section provides the following reset options.

NOTE: This feature is only available on gateways running firmware version 1.4.3 or later.

4.16.1 Reset Types

Log in to the Gateway Configuration Portal, navigate to the System page, and scroll down to locate the Reset Gateway section. This section provides five reset types described as follows:

- **Factory Reset**: Restores the Gateway to factory settings.
- **Network Settings**: Resets all current WiFi, Cellular, and Ethernet configurations. The Ethernet interface will revert to its default IP address: 10.110.210.2.
- **Sensor Settings**: Resets all wireless sensor settings to random values. This action affects existing sensor connections and should only be performed when no active sensors are connected to the Gateway.
- **System Settings**: Resets the log level, user password, and network time method.
- **Cloud Settings**: Refreshes the ETP connection string by retrieving a new one from the cloud.

4.17 Reset via Physical Button

NOTE: This feature is only available on gateways running firmware version 1.4.3 or later.

4.17.1 Button Press Definition

To perform a reset using the physical button:

Press the ON/OFF button 5 times within 10 seconds.

NOTE: The button is located on the back of the unit.

This action will:

- Reset all network configurations.
- Set the Ethernet IP address back to the default: 10.110.210.2.
- Reboot the gateway.

5 Energy Management Profiles

This section outlines the procedure for configuring Energy Management Profiles, which allow users to efficiently manage data traffic from sensors. By optimizing data transmission, these profiles help extend the battery life of the sensors.

What's in This Chapter?

5.1 Energy Management Profiles

Energy Management Profiles enable you to optimize the battery life of your IAQ and IAQ+ sensors by customizing their sampling rates based on your requirements. This includes increasing sampling rates during peak traffic hours and decreasing them during low-traffic periods and holidays. Moreover, you can selectively deactivate specific IAQ parameters, such as noise or VOC, when they are not in use.

Additionally, Energy Management Profiles provide control over the LED on your IAQ and IAQ+ sensors. You can activate or deactivate the LED and set CO2 thresholds to trigger the LED to turn red.

5.2 Configuring an Energy Profile

You configure an energy profile to create a new gateway configuration to monitor, manage, and control building operations from a single, mobile-enabled control center.

To configure an energy profile

1. In the **IoT Sensor Solution Cloud Portal**, click on **Energy Management**.
2. In the **Site Selection** section, click to select **My Partner's Site** or **My Partner's Customer's Site**.
3. Select the **Partner** and/or **Customer** from the drop-down list(s).
4. Click on the green **Configure** button under the **Actions** column.
5. In the **Configure Energy Profile** section, use the various options to configure the profile for the **Occupied Hours** section of the **Workweek** tab.
6. Click **Next**.
7. In the **Unoccupied Hours** section, use the various options to configure the profile.
8. Click **Save & Next**.
9. In the **Weekend** tab, use the various options to configure the profile.
10. Click **Save & Next**.
11. In the **Holidays** tab, use the various options to configure the profile.

    NOTE: You can use the **Upload Holidays** button to upload a holiday bulk file. You will have the possibility of downloading a template for this bulk file. Click **Save** when the upload is complete.

12. Click **Save & Continue**.
13. In the **Configure Sensor Profile** section, use the various options to configure the profile.
14. Click **Save**.

    NOTE: The message "Sensor profile created successfully" will appear in a green box at the bottom of the screen once the operation has been completed.

6 EcoStruxure Building Operation Integration

EcoStruxure Building Operation is Schneider Electric's uniquely open, integrated building management platform that lets you monitor, manage, and control building operations from a single, mobile-enabled control center. The software turns data from connected devices, sensors, and systems into actionable intelligence. What's more, the flexible platform scales easily to meet the evolving needs of any enterprise and is designed with security top-of-mind to help protect building information and assets.

This section describes the integration of the IoT Sensor Solution Cloud Portal to EcoStruxure Building Operation.

What's in This Chapter?

6.1 Creating a New Gateway Configuration for EcoStruxure Building Operation

You create a new gateway configuration for EcoStruxure Building Operation to monitor, manage, and control building operations from a single, mobile-enabled control center.

NOTICE

POTENTIAL COMPROMISE OF ECOSTRUXURE BUILDING OPERATION CONFIGURATION

- Gateways must be connected to the Cloud (status = ONLINE) in the Portal before configuring a new EcoStruxure Building Operation setup.
- Any changes to the EcoStruxure Building Operation configuration should be made at intervals of at least 20 minutes to ensure proper propagation across all components.

Failure to follow these instructions can result in loss of data.

To create a new gateway configuration for EcoStruxure Building Operation

1. In the **IoT Sensor Solution Cloud Portal**, click on **Site Management**, then click on **EBO**.
2. In the **Site Selection** section, click **Add New**.
3. In the **Add Gateway Configuration** box, select the **Server Gateway ID** from the drop-down list.

   NOTE: Once a site is chosen correctly, all the gateways of that site will be available in the **Server Gateway ID** drop-down list.

4. Type in the **Server IP** address and **Port**.

   NOTE: A commonly used port for the EcoStruxure Building Operation is 8883, but a different port can be used.

5. Create a **Username** and **Password**, which will be important later in the configuration.

6. Select the **Client ID** from the drop-down list.

   NOTE: A Server can host a maximum of two Clients simultaneously.

7. Click **Save**.

8. In the **EBO Details** section, a new line is added for the new gateway. You can edit, download or delete the configuration.

   NOTE: It may take up to 30 minutes for the Gateways to confirm the creation of their new EcoStruxure Building Operation configurations as Server and Clients.

9. Click on the download icon to save the XML file, which will be used to import the configuration into EcoStruxure Building Operation.

10. Log in to the **IoT Gateway Configuration Portal**, navigate to the **Integration tab**, and refresh the page (if necessary) to ensure the **Integration Certificates** are available for download.

11. Click **Download** then **Extract** all the files from the Zip.

12. Go in **EcoStruxure Building Operation**, to import XML file and complete the configuration. For more information, see section 6.2 “Importing a New Gateway Configuration into EcoStruxure Building Operation ” on page 31.

6.2 Importing a New Gateway Configuration into EcoStruxure Building Operation

You import a new gateway configuration into EcoStruxure Building Operation to monitor, manage, and control building operations from a single, mobile-enabled control center.

To import a new gateway configuration into EcoStruxure Building Operation

1. In **EcoStruxure Building Operation**, right-click on the Server's name and click on **Import**.

2. In the **Open** box, find the downloaded XML file and click on **Open** then on **Import**. This will create an MQTT interface with a Client and all the sensors beneath it.

3. Click on the MQTT Client name, then click on **MQTT client**.

4. Click on the **Properties** tab.

5. In the **Authorization** section, type in the **Username** and **Password** that was created for this gateway configuration. Confirm the password.

Continued on next page

6. In the **Communication** section:
   - Enabled: Click **Yes**.
   - Host: Type in the IP address.
7. In the **TLS settings** section, click the **...** buttons to point to the downloaded certificates for **Client certificate filename**, **Private key filename**, and **Certificate authority filename**.
8. Click the save button.

   NOTE: A notification will appear in the **Alarms** window if there is an issue with the configuration.
9. Refresh the page and scroll down to confirm that the **Status** field indicates **Online**.

   NOTE: For more information, see EcoStruxure Building Operation - WorkStation Operating Guide.

This completes the setup required to configure EcoStruxure Building Operation for the IoT Gateways. We can now select any sensor, add a measurement or even Tamper Alert to Watchdog. This value will update dynamically whenever a new value is obtained.

For example: If Tamper Alert is added to the EcoStruxure Building Operation Watchdog window, remove the lid of the sensors and the tamperDetection value will go from False to True. This confirms that the EcoStruxure Building Operation setup is verified as well.

7 User Interface

What's in This Chapter?

7.1 IoT Sensor Solution Cloud Portal Screens

The IoT Sensor Solution Cloud Portal allows you to:

- Update or delete user profiles
- Change passwords
- Install gateways and sensors
- Allow sensors to join a network
- Delete devices
- And more

7.1.1 Login Screen

Use this **Login** screen to log on to IoT Sensor Solution Cloud Portal.

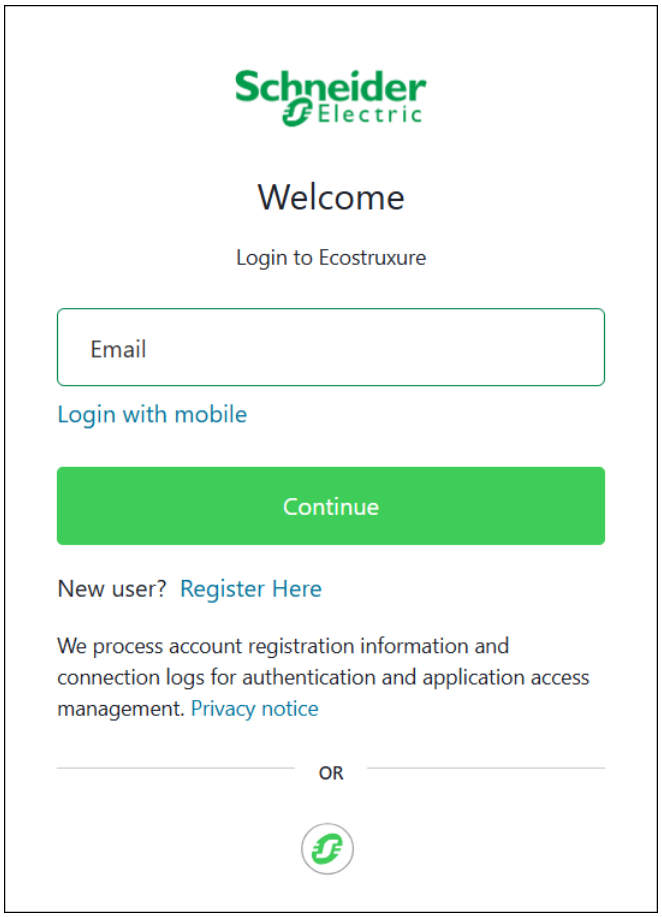

Figure – Login screen

Table – Login Screen

Component	Description
Email	Type a valid email address.
Continue	Click to log on to Iot Sensor Solution and open the Site Matnagement screen. For more information, see the *Site Management Screen* topic on WebHelp.
	Click to use the Schneider Electric Employee Login.

7.1.2 Toolbar

Use the toolbar at the top of the screen to access the main features available for this profile.

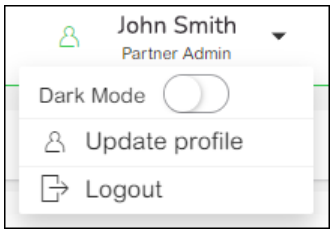

Figure – Toolbar

Table – Toolbar

Button	Description
	Click to display the user profile menu options.
Dark Mode	Click to enable/disable the dark screen mode.
Update Profile	Click to open the Profile screen where you can update the information. For more information, see section 3.3 “Updating Profile” on page 12.
Logout	Click to log out of the platform.

7.1.3 Menu

Use the menu to access the different features of the IoT Sensor Solution Cloud Portal.

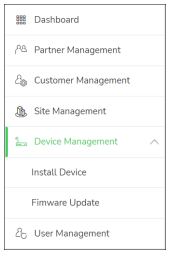

Figure – Menu

Table – Menu

Component	Description
Dashboard	Click to open the IoT Sensor Solution Cloud Portal dashboard.
Partner Management	Click to open the platform Partner Management page.
Customer Management	Click to open the platform Customer Management page.
Site Management	Click to open the platform Site Management page.
Device Management	Click to open the platform Device Management page.
Install Device	Click to open the page where you can install gateways and sensors.
Firmware Update	Click to open the page where you can proceed to a firmware update.
User Management	Click to open the platform User Management page.

7.1.4 Profile Screen for Schneider Electric Users

Use the user profile screen to display and edit the information of the current user profile on this IoT Sensor Solution Cloud Portal.

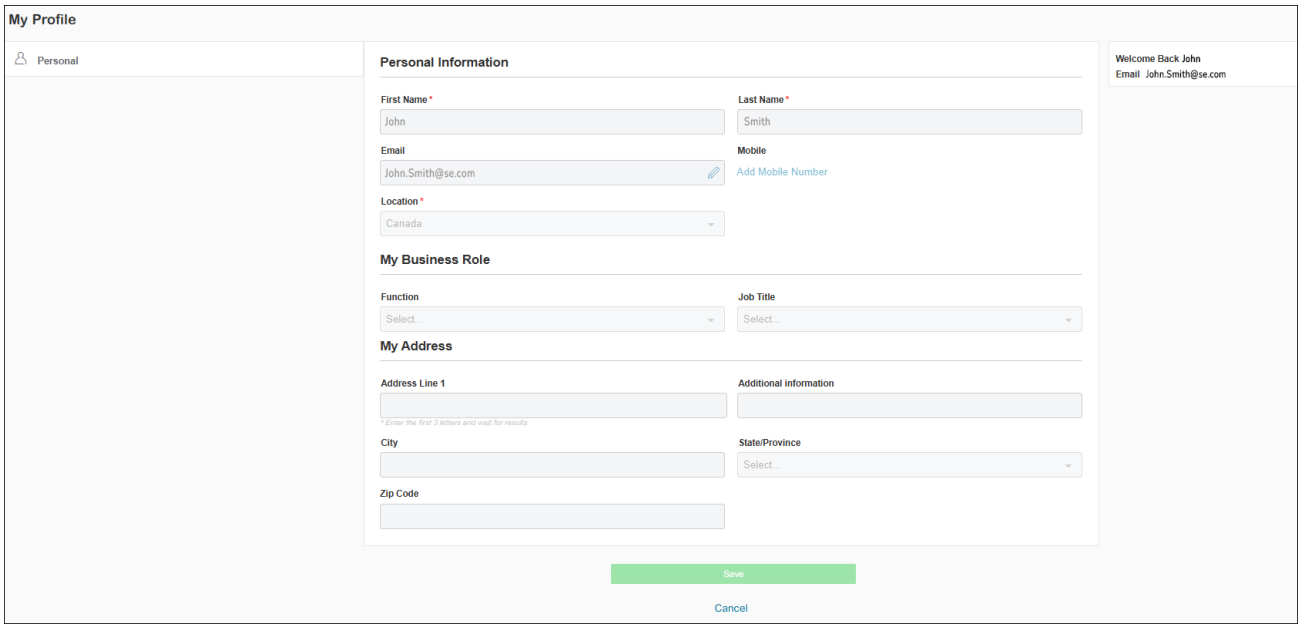

Figure – Profile screen for Schneider Electric users

Table – Profile Screen for Schneider Electric Users

Component	Description
Name (First and Last)	Displays the first and last names.
Email	Displays the email address. Click to edit the information in this field.
Add Mobile Number	Click to add a mobile phone number.
Location	Displays the country.
Function	Displays the role function.
Job Title	Displays the role job title.
Address Line 1 / Additional Information / City / State/Province / Zip Code	Displays the complete address.

7.1.5 Profile Screen for Non-Schneider Electric Users - Personal

Use the user profile screen to display and edit the information of the current user profile on this IoT Sensor Solution Cloud Portal.

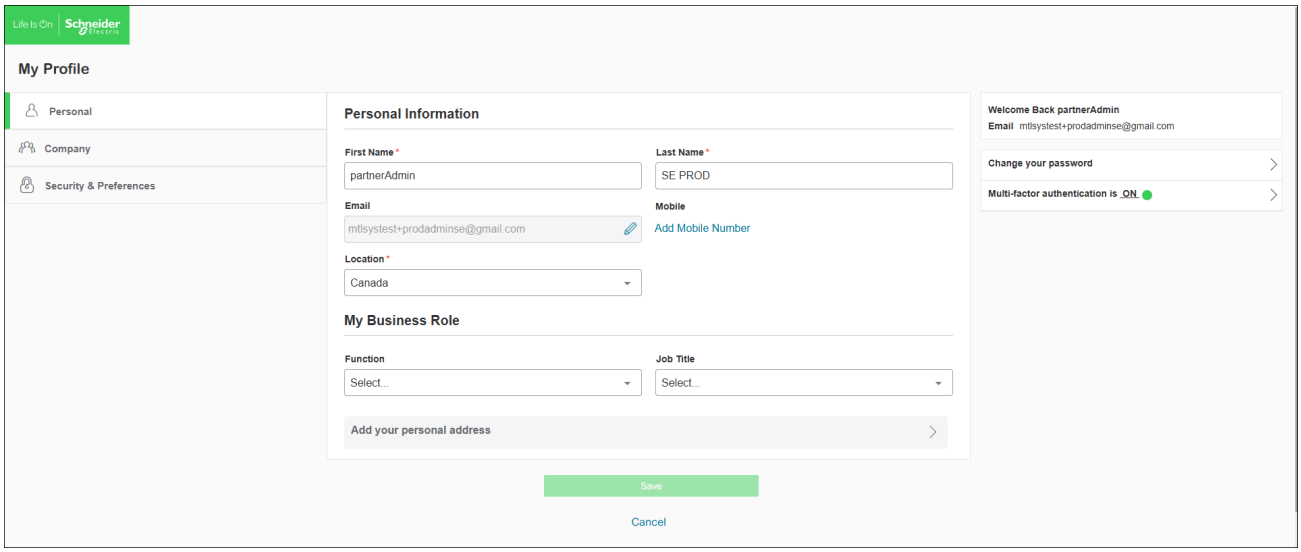

Figure – Profile screen for non-Schneider Electric users - Personal

Table – Profile Screen for Non-Schneider Electric Users - Personal

Component	Description
Name (First and Last)	Type to change the first and/or last name.
Email	Displays the email address. Click or Change Email to edit the information in this field.
Add Mobile Number	Click to add a mobile phone number.
Location	Click to select a country from the drop-down list.
Function	Click to select a function from the drop-down list.
Job Title	Click to select a job title from the drop-down list.
Change your password	Click to change the password.
Multi-Factor Authentication is	Displays ON or OFF to indicate the status of multi-factor authentication.

7.1.6 Profile Screen for Non-Schneider Electric Users - Company

Use the user profile screen to display and edit the information of the current user profile on this IoT Sensor Solution Cloud Portal.

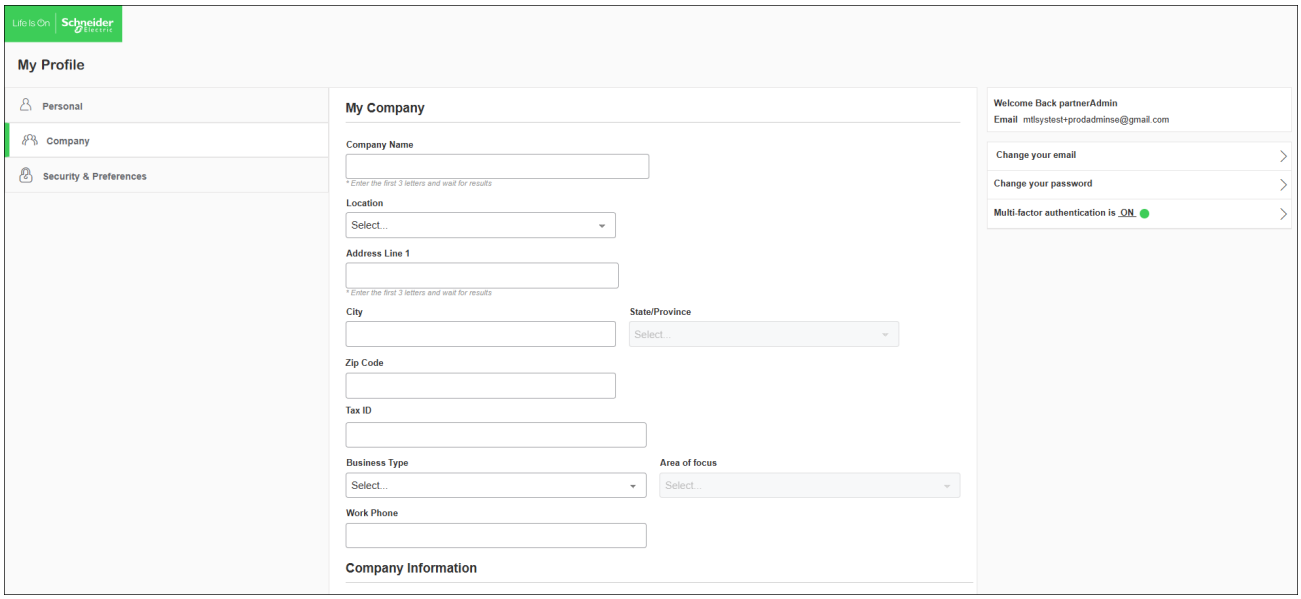

Figure – Profile screen for non-Schneider Electric users - Company

Table – Profile Screen for Non-Schneider Electric Users - Company

Component	Description
Company Name	Type to add the company name.
Location	Click to select a country from the drop-down list.
Address Line 1	Start typing the company address, then click to select the correct address from the drop-down list.
City / Province / Zip Code	Displays the correct information as soon as an address is selected from the drop-down list in Address Line 1.
Tax ID	Type to add a tax identification number.
Business Type	Click to select a business type from the drop-down list.
Area of Focus	Click to select a area of focus from the drop-down list.
Work Phone	Type to add a work phone number.
Change your email	Click to change the recorded email.
Change your password	Click to change the recorded password.
Multi-Factor Authentication is	Displays ON (green light) or OFF (red light) to indicate the status of multi-factor authentication.

7.1.7 Profile Screen for Non-Schneider Electric Users - Security & Preferences

Use the user profile screen to display and edit the information of the current user profile on this IoT Sensor Solution Cloud Portal.

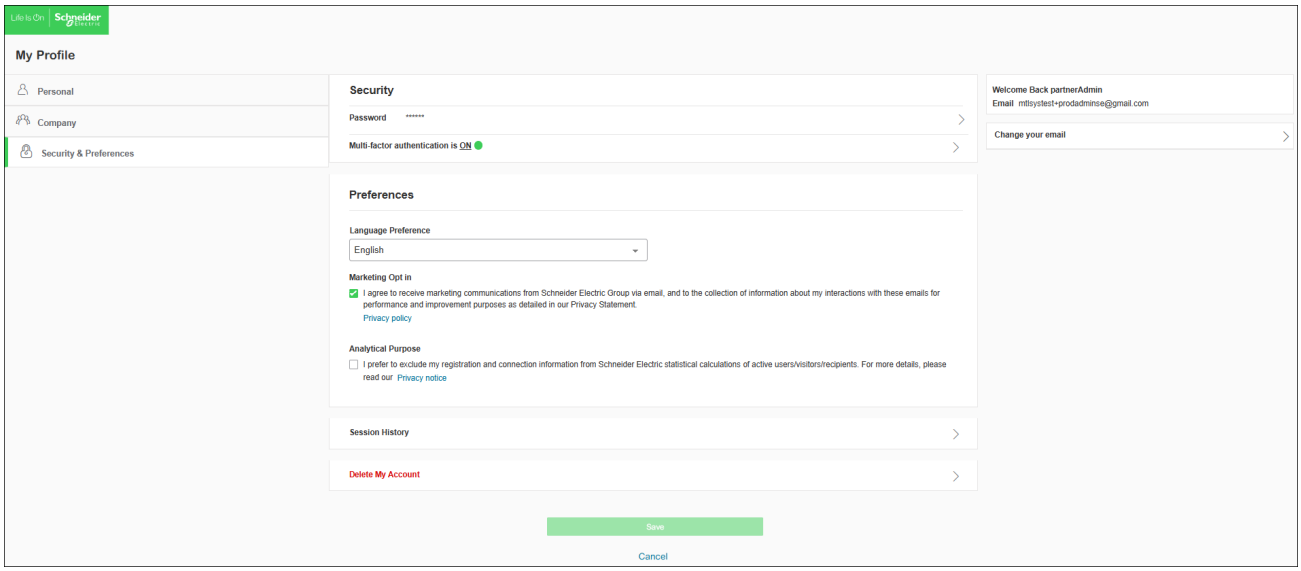

Figure – Profile screen for non-Schneider Electric users - Security & Preferences

Table – Profile Screen for Non-Schneider Electric Users - Security & Preferences

Component	Description
Password	Display a hidden version of your password.
Multi-Factor Authentication is	Displays ON (green light) or OFF (red light) to indicate the status of multi-factor authentication.
Language	Click to select a language from the drop-down list.
Marketing Opt in	Click to select or clear the check box to indicate whether you choose to opt in to marketing communications by email and to the collection of information.
Analytical Purpose	Click to select or clear the check box to indicate whether you prefer to keep your registration and connection information private.
Session History	Click the arrow to display this session history.
Delete My Account	Click the arrow to delete this account.
Change your email	Click to change the recorded email.

7.1.8 Change Password Screen

Use the **Change password** screen to assign a new unique password to this user.

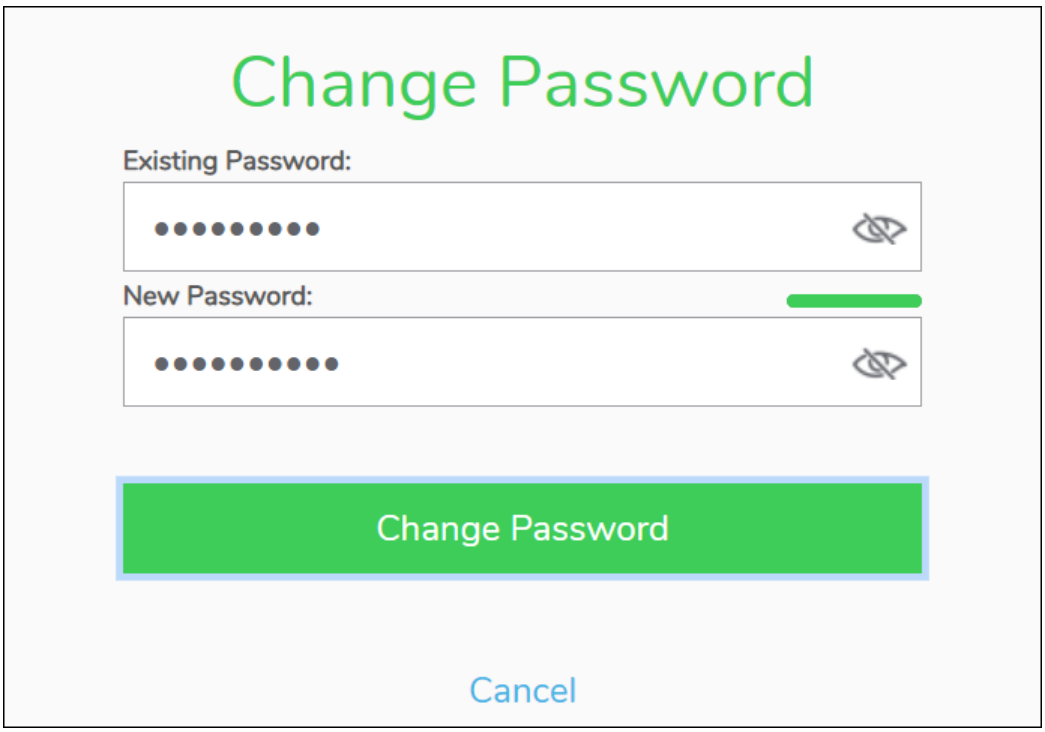

Figure – Change password screen

Table – Change Password Screen

Component	Description
Existing Password	Type the current password for this user. For more information, see section 2 “User Account Handling” on page 10.
New Password	Type a unique password. For more information, see section 2 “User Account Handling” on page 10.

7.1.9 Site Management Screen

Use the Site Management screen to access the list and details of Partner and Customer Sites.

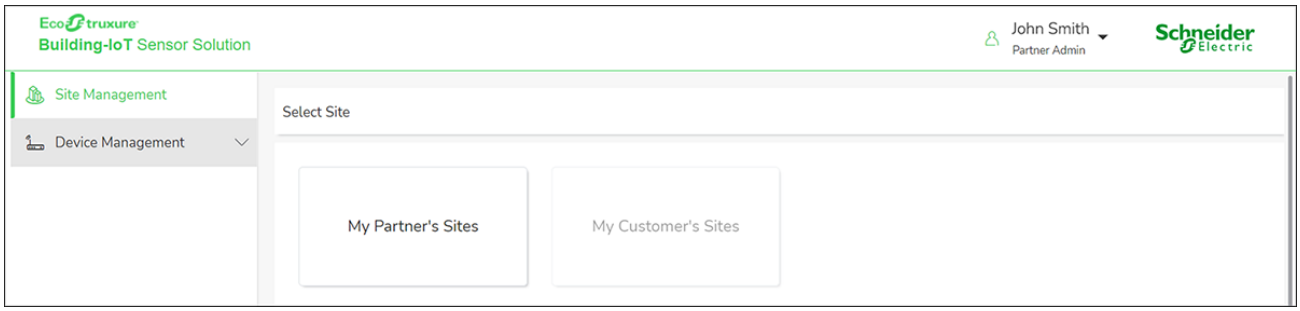

Figure – Sensor list screen

Table – Sensor List Screen

Component	Description
My Partner's Sites	Click to see the list of available Partner Sites.
My Customer's Sites	Click to see the list of available Customer Sites.

7.1.10 Install Device Screen

Use the Install Device screen to access the list and details of Partner and Customer Sites.

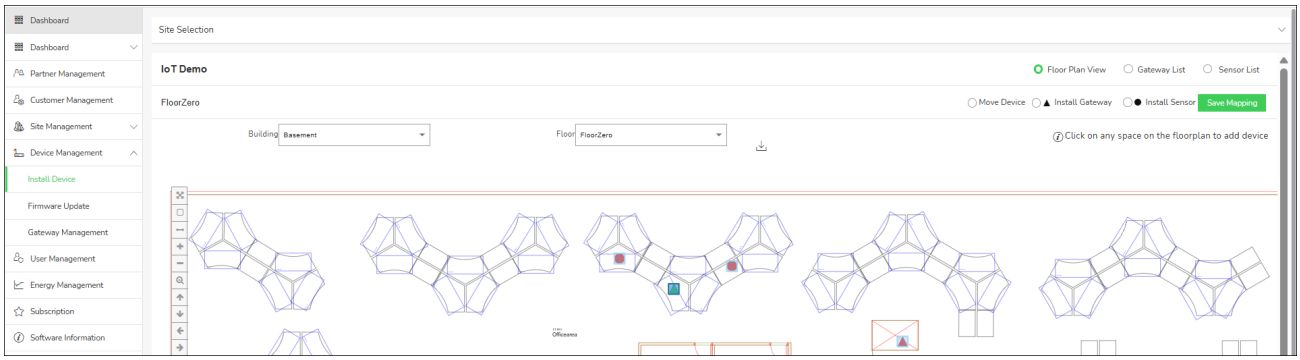

Figure – Sensor list screen

Table – Sensor List Screen

Component	Description
Site Selection	Click to choose between My Partner's Site and My Partner's Customer's Site.
Partner	Click to select a partner from the drop-down list.
Customer	Click to select a customer from the drop-down list.
Site	Click to select a site from the drop-down list.
Building	Click to select a building from the drop-down list.
Floor	Click to select a floor from the drop-down list.
Move Device	Click the radio button to move a gateway or sensor to a new location on the floor plan.
Install Gateway	Click the radio button to add a new gateway to the platform.
Install Sensor	Click the radio button to add a new sensor to the network.
▲	Displays an installed gateway on the floor plan. • Blue: The device is in unknown status and has not established a connection with the cloud yet. • Green: A connection to the Cloud is established. • Red: The established connection is lost

Continued

Component	Description
	Displays an installed sensor on the floor plan. • Blue: The device is in unknown status and has not joined the network yet. • Green: The device has joined the network. • Red: The device has left the network.

7.1.11 Gateway List View Screen

Use the gateway list view screen to see which gateways are currently available on the platform and their associated sensors.

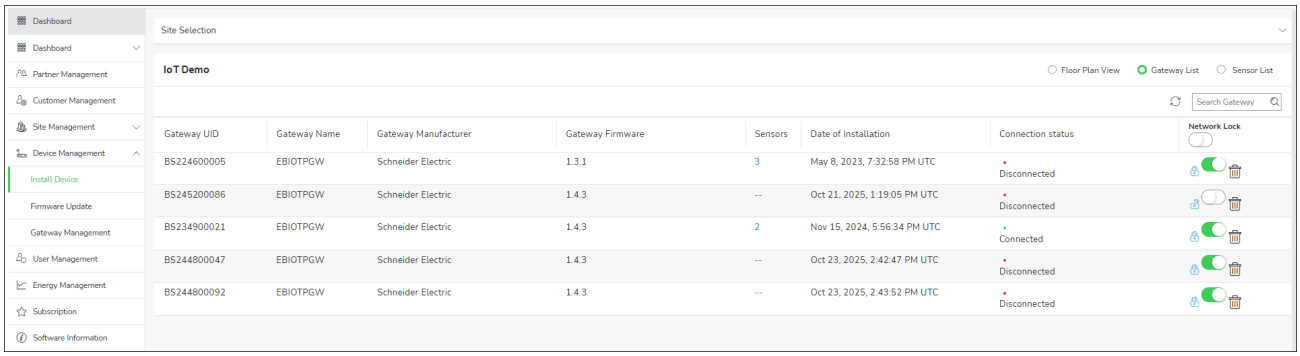

Figure – Gateway list view screen

Table – Gateway List View Screen

Component	Description
Gateway UID	Displays the unique identifying name for a gateway.
Gateway Name	Displays the gateway's model name.
Gateway Manufacturer	Displays the name of the gateway manufacturer.
Gateway Firmware	Displays the gateway's firmware version number.
Sensors	Displays the number of sensors associated to this gateway. Click the hyperlink to see the list of sensors and their details.
Date of Installation	Displays the date and time when the gateway was installed.
Connection Status	Display the current status of the gateway. It can be Online, Offline, or Unknown.
Network Lock	Click the toggle switch to lock/unlock the network.
🗑	Click to delete the gateway from the platform.

7.1.12 Sensor List View Screen

Use the sensor list view screen to see which sensors are assigned to a gateway, see their details, and delete them if necessary.

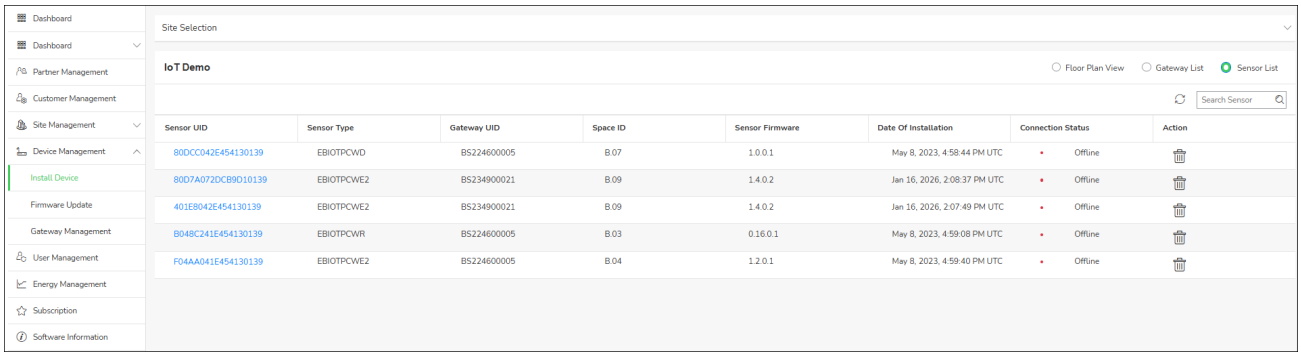

Figure – Sensor list view screen

Table – Sensor List View Screen

Component	Description
Sensor UID	Displays the unique identifying name for a sensor.
Sensor Type	Displays the type of the sensor. It can be Desk Occupancy, Room Occupancy, Well-Being, or Advanced Well-Being.
Gateway UID	Displays the unique identifying name for gateway linked to this sensor.
Space ID	Displays the space where the sensor is installed.
Sensor Firmware	Displays the sensor's firmware version number.
Date of Installation	Displays the date and time when the sensor was installed.
Connection Status	Display the current status of the sensor. It can be Online, Offline, or Unknown.
🗑	Click to delete the sensor from the gateway and platform.

7.1.13 View Sensor Details Screen

Use the View Sensor Details screen to see the information related to a specific sensor.

Figure – View sensor details view screen

Table – View Sensor Details Screen

Component	Description
Space Name	Displays the name of the space where the sensor is installed.
Space ID	Displays the space where the sensor is installed.
Gateway UID	Displays the unique identifying name for gateway linked to this sensor.
Sensor UID	Displays the unique identifying name for the sensor.
Sensor Manufacturer	Displays the manufacturer of the sensor.
Sensor Type	Displays the type of the sensor. It can be Desk Occupancy, Room Occupancy, Well-Being, or Advanced Well-Being.
Firmware Version	Displays the sensor's firmware version number.
Connection Status	Display the current status of the sensor. It can be Online, Offline, or Unknown.
Date of Installation	Displays the date and time when the sensor was installed.

7.2 IoT Gateway Configuration Portal Screens

A Building-IoT multi-protocol gateway:

- Supports simultaneous communication with multiple protocols
- Connects up to 200 devices in a robust mesh network
- Supports Power Over Ethernet (PoE)
- Includes a GSM-LTE slot

Each gateway is managed using the Gateway Configuration Portal.

7.2.1 Login Screen

Use this **Login** screen to log on to IoT Gateway Configuration Portal

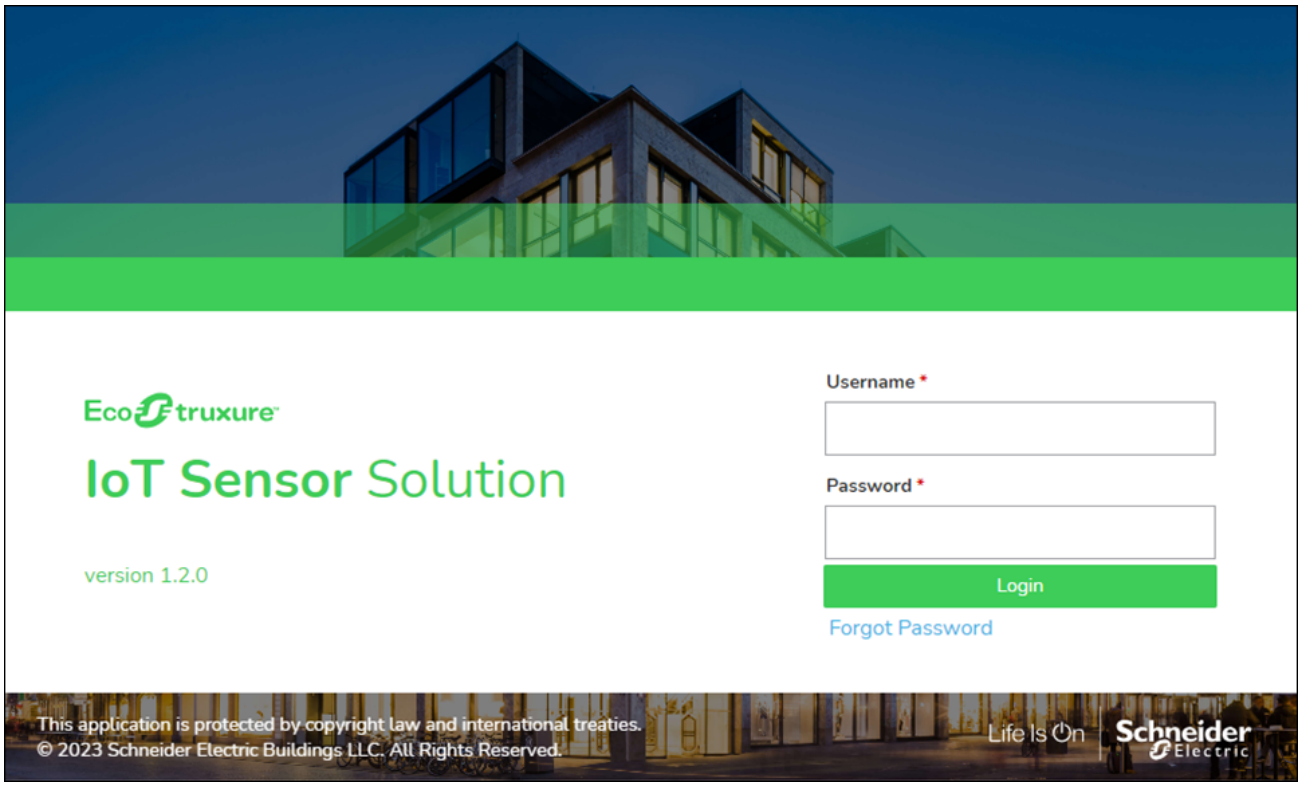

Figure – Login screen

Table – Login Screen

Component	Description
Username	Type **admin** as the username.
Password	Type the password for this user profile. The default value is P@ssword.
Forgot Password	Click on Forgot Password to start the process of resetting the password. Enter the username (admin). A unique sequence of characters will be generated. Contact Technical Support with this sequence of characters to complete the password reset.

7.2.2 Toolbar

Use the toolbar at the top of the screen to access the main features available for this profile.

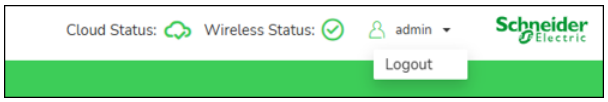

Figure – Toolbar

Table – Toolbar

Button	Description
Cloud Status	Displays the operational status of the Cloud network. Displays a green cloud icon when Cloud connectivity is established.
Wireless Status	Displays the operational status of the Wireless network. Displays a green icon when a wireless network is configured.
	Click to display the user profile menu options.
Logout	Click to log out of the platform. For more information, see section 4.15 “Logging out of IoT Gateway Configuration Portal” on page 26.

NOTE: The gateway will successfully communicate with the Cloud once an Internet connection is established, valid Wireless settings are configured, and a valid UTC date and time are configured.

7.2.3 Menu

Use the menu to access the different features of the IoT Gateway Configuration Portal.

Figure – Menu

Table – Menu

Component	Description
DASHBOARD	Click to open the portal Dashboard page. This is also the default home page when the Configuration Portal is launched. For more information, see section 7.2.4 “Dashboard Screen” on page 51.
NETWORK	Click to open the portal Network management page. For more information, see section 7.2.5 “Network Screen” on page 52.
WIRELESS	Click to open the portal Wireless management page. For more information, see section 7.2.9 “Wireless Screen” on page 56.
INTEGRATION	Click to download the certificates required for EBO workstation configuration. For more information, see section 7.2.10 “Integration Screen” on page 57.
SYSTEM	Click to open the portal System management page. For more information, see section 7.2.11 “System Screen” on page 58.

7.2.4 Dashboard Screen

Use the Dashboard screen to access a visualization of the current state of the gateway. This is also the default home page when the Configuration Portal is launched.

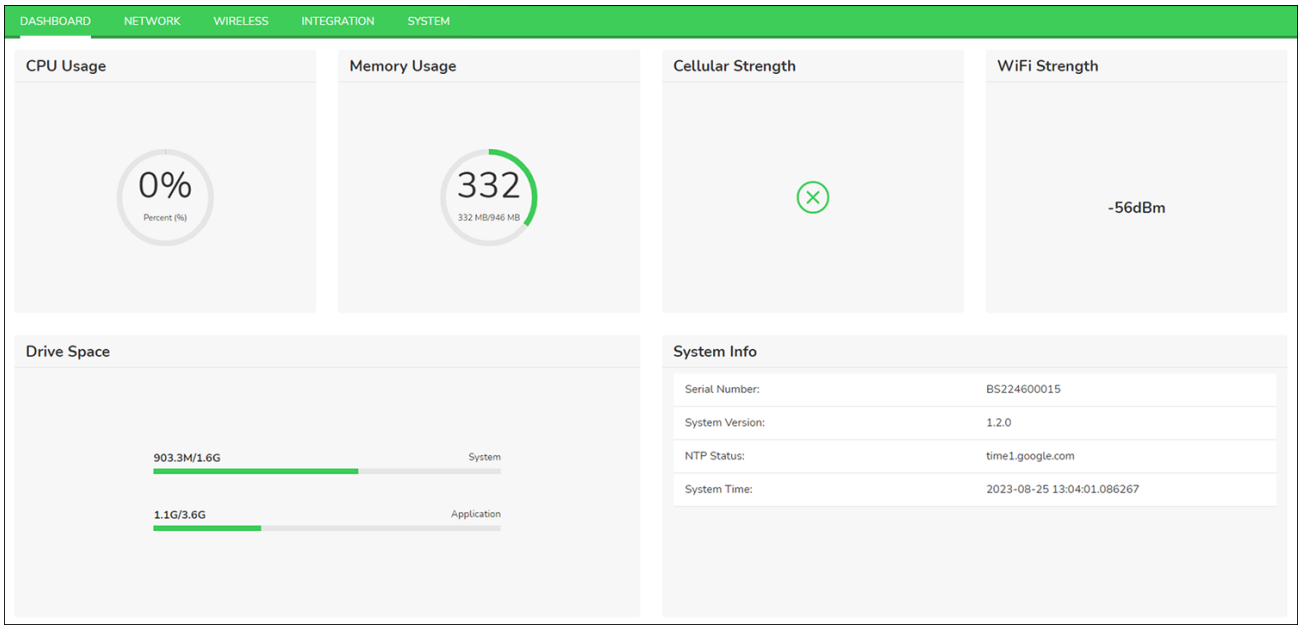

Figure – Dashboard screen

Table – Dashboard Screen

Button	Description
CPU Usage	Displays the percentage of processor usage since the last measurement.
Memory Usage	Displays the amount of RAM currently in use.
Cellular Strength	Displays the current cellular signal strength (if configured).
WiFi Strength	Displays the current wireless signal strength (if configured).
Drive Space	Displays the available space used by the system and application on the internal storage.
System Info	Displays the serial number, system version, NTP status (if connected), and system time. It is important to ensure that the System Time is correctly configured to UTC date and time for Cloud connectivity.

7.2.5 Network Screen

Use the Network screen to configure the various Internet connectivity options to connect the gateway to the Cloud portal.

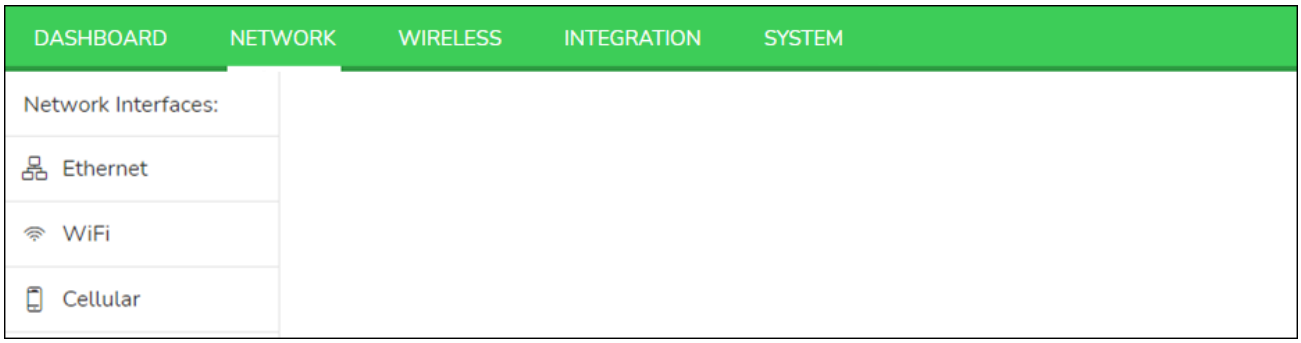

Figure – Network screen

Table – Network Screen

Button	Description
Ethernet	Displays the Ethernet configuration page. For more information, see section 7.2.6 “Ethernet Screen” on page 53.
WiFi	Displays the WiFi configuration page. For more information, see section 7.2.7 “WiFi Screen” on page 54.
Cellular	Displays the Cellular configuration page. For more information, see section 7.2.8 “Cellular Screen” on page 55.

7.2.6 Ethernet Screen

Use the Network Ethernet screen to complete the Ethernet configuration.

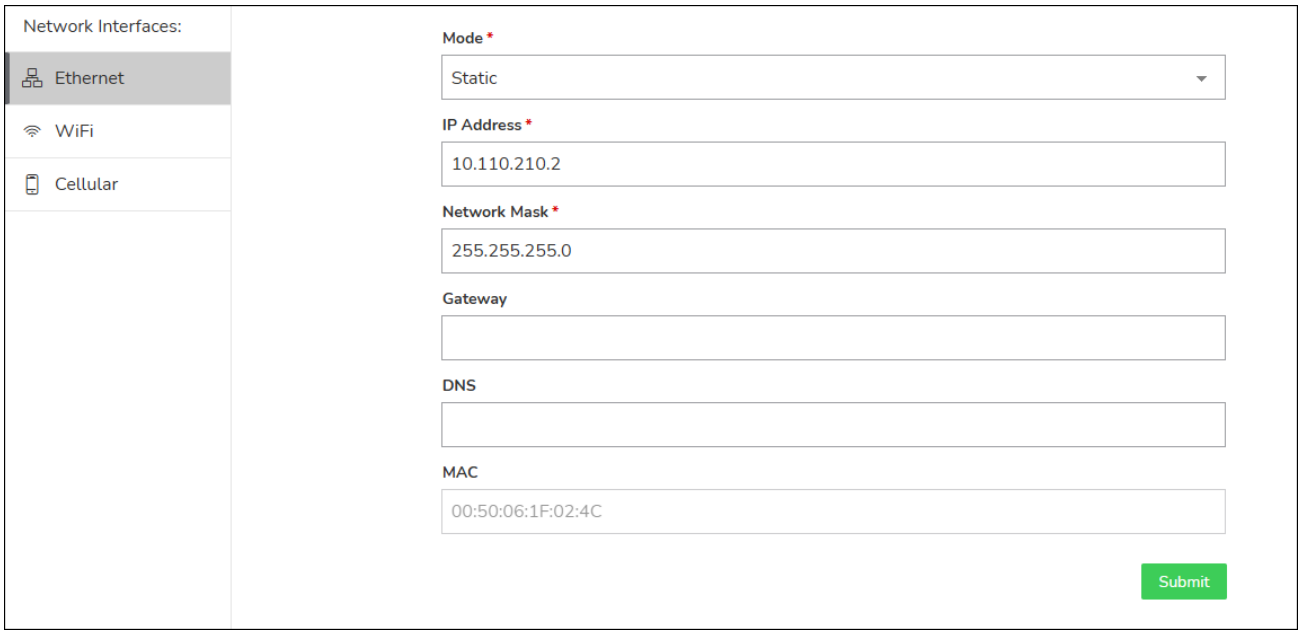

Figure – Ethernet screen

Table – Ethernet Screen

Button	Description
Mode	Click to select between Static and DHCP.
IP Address	Click to enter a unique IP address used to identify the gateway on the local network.
Network Mask	Click to enter a number that distinguishes the network address and the host address within an IP address.
Gateway	Click to enter the network gateway IP address.
DNS	Click to enter one or more domain name servers.
MAC	Displays the MAC address.

7.2.7 WiFi Screen

Use the Network WiFi screen to complete the WiFi configuration.

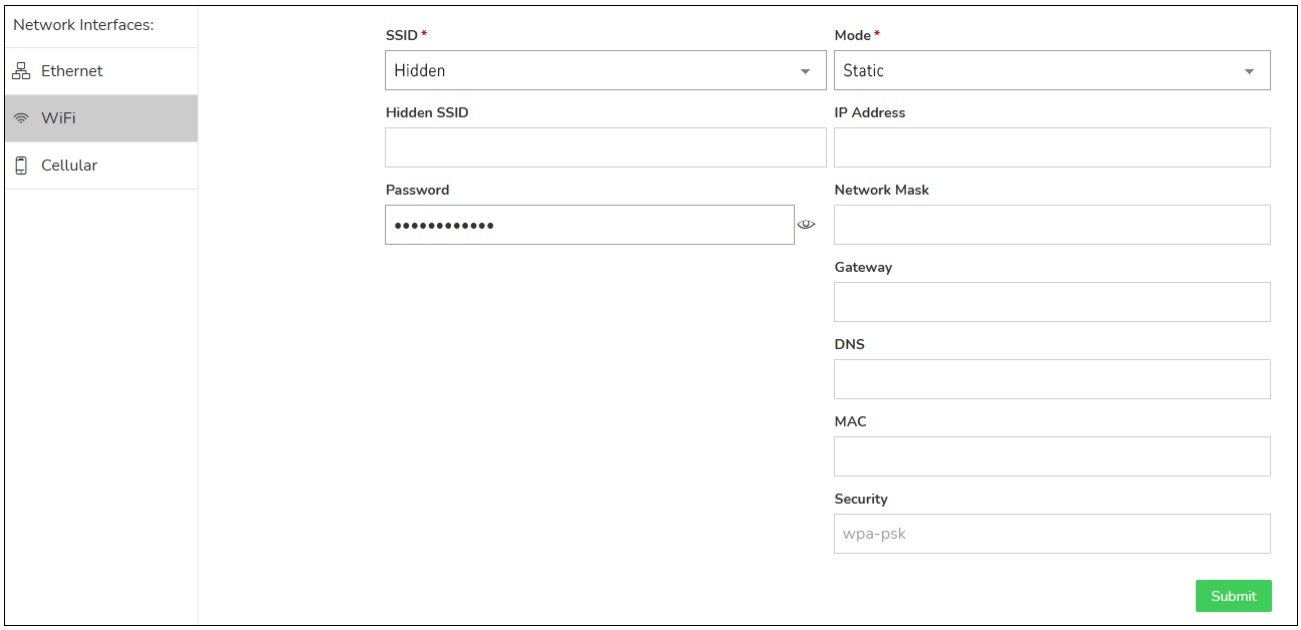

Figure – WiFi screen

Table – WiFi Screen

Button	Description
SSID	Click to select which WiFi network to connect to from the list of available networks.
Hidden SSID	Click to enter the SSID of the network to connect to if the desired one is not available in the SSID drop-down menu list.
Password	Click to enter the password to the network.
Mode	Click to select between Static and DHCP.
IP Address	Displays the unique IP address used to identify the gateway on the wireless network.
Network Mask	Displays the number that distinguishes the network address and the host address within an IP address.
Gateway	Displays the network gateway IP address.
DNS	Displays one or more domain name servers.
MAC	Displays the MAC address.
Security	Displays the WiFi security protocol.

7.2.8 Cellular Screen

Use the Network Cellular screen to configure the Cellular information.

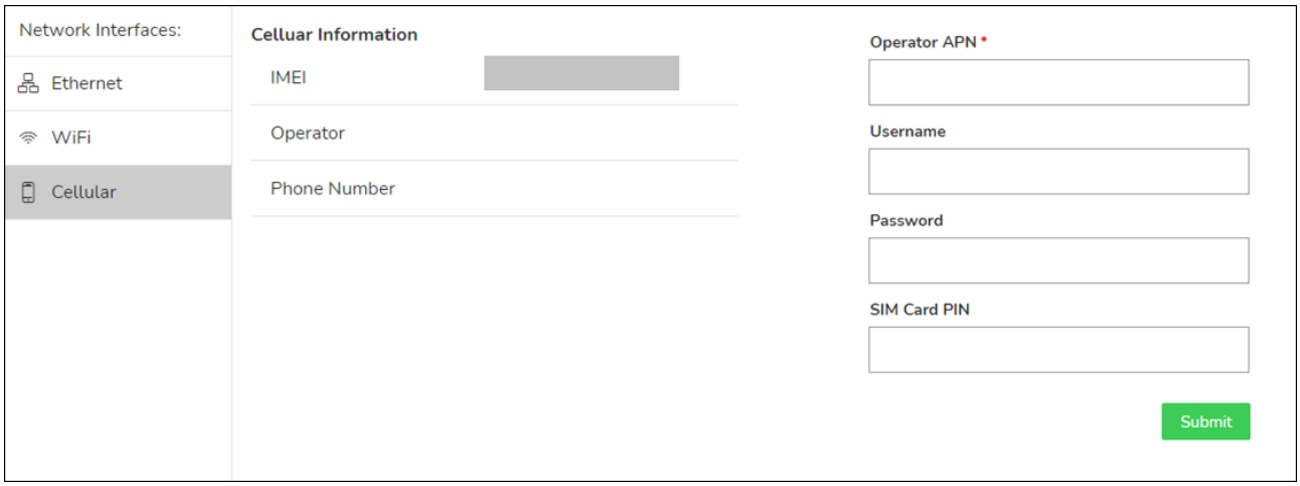

Figure – Cellular screen

Table – Cellular Screen

Button	Description
IMEI	Displays the device International Mobile Equipment Identity (IMEI) number, a unique identification or serial number that all mobile phones and devices have.
Operator	Displays the device operator.
Phone Number	Displays the device phone number.
Operator APN	Click to enter the operator Access Point Name (APN), which provides all the details the device needs to connect to mobile data.
Username	Click to enter the username of the SIM card, if required.
Password	Click to enter the password of the SIM card, if required.
SIM Card PIN	Click to enter the PIN code of the SIM card, if required.

7.2.9 Wireless Screen

Use the Wireless screen to configure the wireless network. The configuration can be unique for each gateway at a site (allowing independent networks) or have the same network credentials to allow one large redundant wireless network on the same floor.

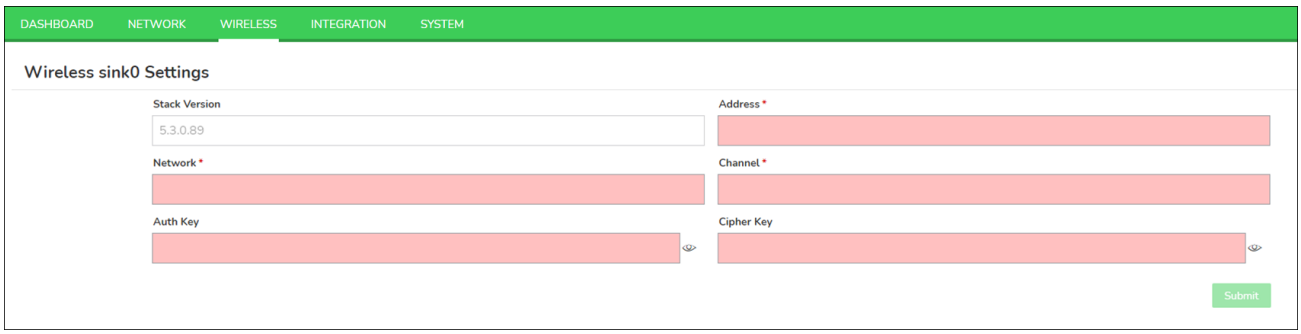

Figure – Wireless screen

Table – Wireless Screen

Button	Description
Stack Version	Displays the version of the firmware being used by the wireless radio.
Address	Click to enter the unique ID used to identify the gateway on the wireless network. This must always be different than other gateways on the same wireless network. Valid range of values between 1 and 2147483647 OR between 2164260864 and 4292967294.
Network	Click to enter the network ID is used to identify the wireless network in the wireless spectrum. The network ID uniqueness between all gateways in a site is dependent on the scenario desired above. Valid range of values between 1 and 5570559 OR between 5636096 and 11141119 OR between 11206656 and 16777214.
Channel	Click to enter the channel that is used during the commissioning/joining process only. The Channel uniqueness between all gateways in a site is dependent on the scenario desired above. Valid range of values between 1 and 40.
Auth Key	Click to enter the authentication key, which is used for network security. It is a string of 32 characters composed of numbers 0-9 and A-F.
Cipher Key	Click to enter the cipher key, which is used for network security. It is a string of 32 characters composed of numbers 0-9 and A-F.

7.2.10 Integration Screen

Use the Integration screen to access and download the MQTT Integration Certificates.

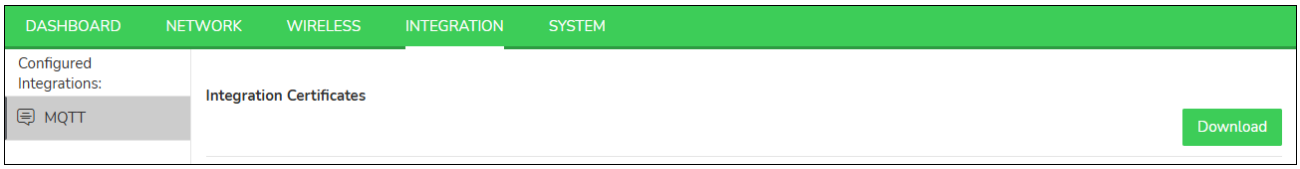

Figure – Integration screen

Table – Integration Screen

Button	Description
Integration Certificates	Click on **Download** to save the MQTT Integration Certificates.

7.2.11 System Screen

Use the System screen to access system functions such as configuring the Time Settings, downloading logs, and changing the login password.

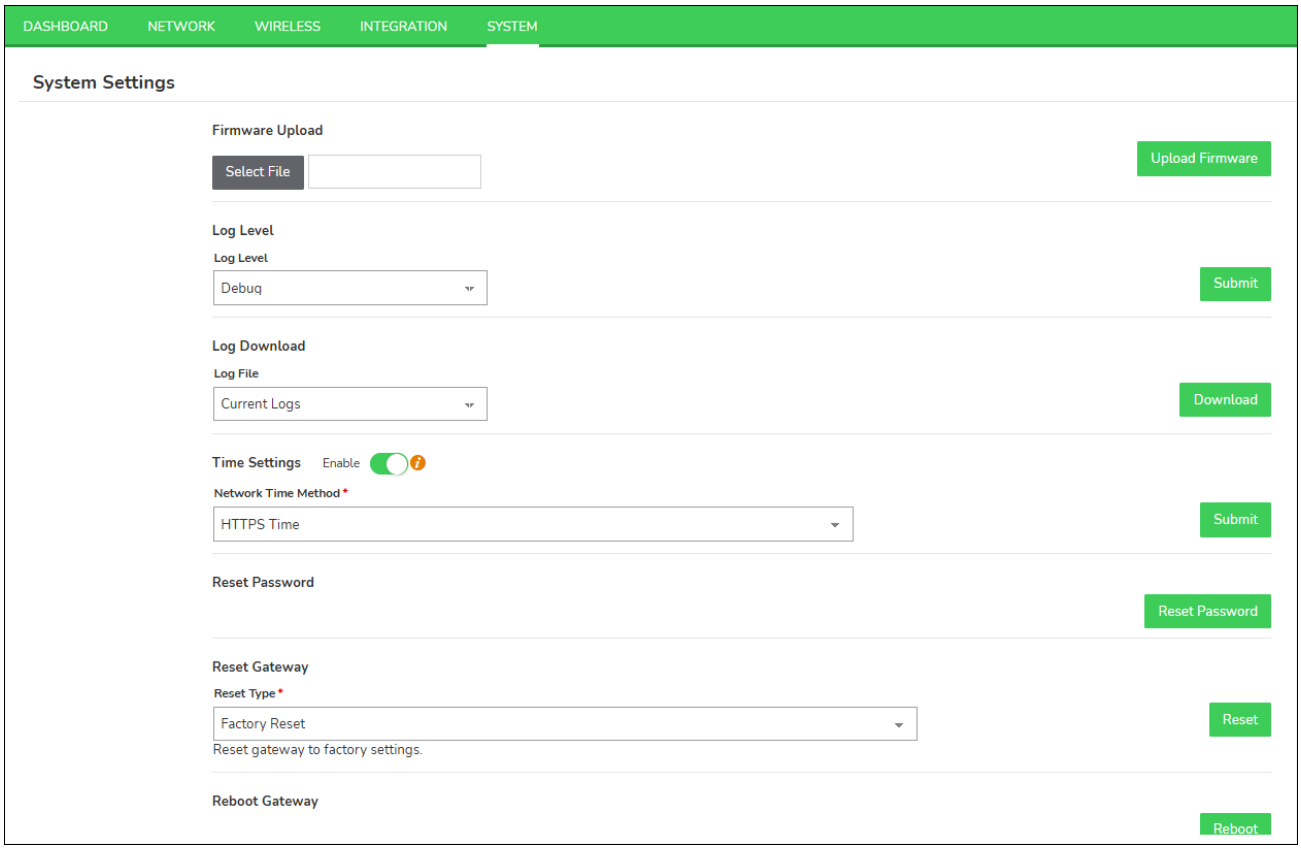

Figure – System screen

Table – System Screen

Button	Description
Firmware Upload	Click on **Select File** to select the firmware file to upload.
Log Level	Click to select how detailed the logs can be. This can impact available storage space on the gateway.
Log Download	Click to select the log corresponding to the desired day.
Time Settings	Click to either use the network time method or manually set the system time. • Enabled: Uses HTTPS Time (default). Optionally, you can enter a custom value for the NTP server. • Disabled: Allows manual entry of the system time.

Continued

Button	Description
Reset Password	Click on **Reset Password** to change the password used to log in the gateway's configuration portal. Enter the new password twice for confirmation.
Reset Gateway	Click on **Reset** to reset the gateway from the Configuration Portal.
Reboot Gateway	Click on **Reboot** to reboot the gateway from the Configuration Portal.

8 Hardening Specifics for Cybersecurity

This section provides information on cybersecurity aspects for EcoStruxure™ Building-IoT Sensor Solution to help system designers and operators promote a secure operating environment for the product.

This section does not address the more general topic of how to secure your operational technology network, or your company WiFi Ethernet network. For a general introduction to cybersecurity threats and how to address them: https://download.schneider-electric.com/files?p_Doc_Ref=STN+v2

What's in This Chapter?

8.1 Convention

In the Hardening Specifics for Cybersecurity section:

- The term security is used to refer to cybersecurity.
- EcoStruxure Building-IoT Gateway is hereafter referred to as Gateway.

8.2 Online Information

The information contained in this Hardening Specifics for Cybersecurity section may be updated at any time. Schneider Electric strongly recommends that you read the most recent and up-to date version available online: http://www.se.com/ww/en/download.

The technical characteristics of the devices described in this section also appear online. To access the information online, go to the Schneider Electric home page: http://www.se.com/.

8.3 An Introduction to Cybersecurity

8.3.1 EcoStruxure Master Range

EcoStruxure is Schneider Electric's IoT-enabled, plug-and-play, open, interoperable architecture and platform, in Homes, Buildings, Data Centers, Infrastructure and Industries. Innovation at Every Level from Connected Products to Edge Control, and Apps, Analytics and Services.

8.3.2 Introduction

Cybersecurity is intended to help protect your communication network and all equipment connected to it from attacks that could disrupt operations (availability), modify information (integrity), or give away confidential information (confidentiality). The objective of cybersecurity is to provide increased levels of protection for information and physical assets from theft, corruption, misuse, or accidents while maintaining access for their intended users. There are many aspects to cybersecurity including designing secure systems, restricting access using physical and digital methods, identifying users, as well as implementing security procedures and best practice policies.

8.3.3 Schneider Electric Guidelines

In addition to the recommendations provided in this guide that are specific to IoT Gateway, you should follow the defense-in-depth approach to cybersecurity on the Schneider Electric Website. Furthermore, you will find useful resources and up-to-date information on the Cybersecurity Support Portal on the Schneider Electric global website.

8.3.4 Schneider Electric Cybersecurity Policies and Rules

Schneider Electric use a Secure Development Lifecycle (SDL) process, a key product development-based framework that helps ensure products follow secure design processes across all lifecycle stages. The Schneider Electric SDL process complies with IEC 62443-4.1.

The SDL process includes the following:

- SDL practices applied to internal development actions, throughout the supply chain.
- Final security review required for project release.
- Security training for personnel involved in the product development.

8.4 Device Characteristics

8.4.1 Overview

The IoT Gateway is equipped with security-enabling features. These features come in a preset state and can be modified to meet your installation needs. The IoT Gateway must only be configured and set by qualified personnel because disabling or changing settings affect the overall security robustness of the IoT Gateway and your network security.

For more information, see section 4 “IoT Gateway Configuration Portal” on page 18.

8.4.2 IoT Gateway Interfaces

The IoT Gateway communicates through the following interface types:

- Wired communication through:
  - One Ethernet port

- Radio communication through:
  - WiFi infrastructure
  - 2.4GHz Wireless Sensors Protocol
  - Cellular LTE Connection

8.4.3 Supported Protocols

The IoT Gateway supports the following protocols:

- HTTPS and MQTTS (TLS v1.2)
- 2.4 GHz Wireless Protocol (AES Encryption)
- DHCP for network IP addressing
- DNS for network name resolution
- NTP for time synchronization
- WPA2 and WPA for WiFi communication
- LTE for cellular connection

NOTE: As a security best practice, the product uses TLS v1.2 and MQTTS protocols.

8.4.4 Security Features

The EcoStruxure Building IoT Gateway supports the following security features:

- Only firmware digitally signed by Schneider Electric can be installed on the IoT Gateway.
- At each boot, the firmware digital signature is validated before execution, to help ensure that it has not been tampered with.
- The device has an internal clock that needs to be synchronized with UTC time in order to connect to the Cloud.

8.5 Device Features

8.5.1 Firmware Update

Update the IoT Gateway to the latest firmware version to obtain the latest features and keep up-to-date with security patches. All firmware designed for the IoT Gateway is signed using the Schneider Electric Public Key Infrastructure (PKI) to help to provide integrity and authenticity of the firmware running on the IoT Gateway. For proper operation, keep the device date synchronized.

To be informed about security updates, register with the Security Notifications on the Schneider Electric Cybersecurity Support Portal.

Firmware Updates for Gateway Devices

To ensure system stability, performance, reliability, and security, and to support new features, periodic firmware updates are performed on the gateway.

Update Management

Firmware updates are managed and deployed by Schneider Electric and typically include the following features:

- **Automatic Updates**: Updates are applied remotely and automatically by Schneider Electric. No customer action is required for routine updates.
- **Customer Notification**: In rare cases where customer involvement is necessary (e.g., a reboot), Schneider Electric or the designated installer will coordinate with the customer in advance.
- **Release Notes**: Customers receive release notes detailing new features, bug fixes, and other changes included in the update.
- **Logging**: Firmware update activities and results are recorded in the gateway logs at the debug level.

8.5.2 Date and Time

Certificates and digital signatures are present in the IoT Gateway. To avoid errors, it is important to keep the date and time synchronized. For more information, see section 4.13 “Manually Entering the Date and Time ” on page 25.

8.5.3 TCP Ports

The following TCP ports are used in the EcoStruxure Building IoT Gateway:

Outbound:

- Port 443
- Port 8883
- Port 123

Disable any unnecessary or unused ports and services—except those explicitly specified here—to help minimize potential pathways for malicious attackers.

8.5.4 Audit Logs

The IoT Gateway generates audit logs that record events such as invalid login attempts, device management, configuration changes and firmware update.

The logs do not contain any personal information. The logs can be downloaded from the System Tab in the IoT Gateway configuration portal.

To detect unexpected behavior of IoT Gateway (for example, frequent rebooting, changes to network configuration), it is recommended to monitor IoT Gateway health streams regularly.

8.5.5 Device Disposal

The IoT Gateway contains confidential information, IoT Gateway source code, recent data values and logs. For example, this information can include wireless networks, and WiFi passwords.

You must factory reset the IoT Gateway prior to its disposal.

For more information, see section 4.16 “Gateway Reset Options” on page 26.

8.5.6 Secure Account Management

The Cloud Portal is responsible for creating a new user and assigning appropriate permissions in a system. The Line of Business Architect determines each user’s level of access to an application across the customer’s sites. This user can then use the password reset portal to verify their credentials and generate a password. Contact Schneider Electric’s Product Support to determine the Line of Business Architect for your region at ProductSupport.BMS@schneider-electric.com.

- Whenever creating a new user in the system, ensure that:
  - Email ID and phone number of the user are correct.
  - User language preference is set correctly.
  - Customer, site and access selection is done carefully to avoid any unwanted access.
- A user cannot be created unless a customer site is associated with that user.
- A Line of Business Architect at Schneider Electric is responsible for creating users.
- When logging in for the first time, it is mandatory for the user to:
  - To verify the email address and phone number
  - To set the password
- The password must meet the password policy requirements.
- Multi-Factor Authentication (MFA) has been implemented for the Cloud Portal Services, allowing users to verify their credentials using either email or phone number at each login.
- If at any point, the user wishes to withdraw from the privacy policy, there is an option to withdraw from the same in the profile section of the dashboard. However, in order to access the dashboard again, the user will have to accept the policy at the time of login.

NOTICE

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Do not log in the Cloud Portal where password entry may be monitored by humans or cameras.
- Line of Business Architects must only grant access to users (Partner Administrators, Installers etc.) that are authorized to use the Cloud Portal. Inactive accounts must be disabled.

Failure to follow these instructions can result in loss of data or unauthorized system access.

8.6 IoT Gateway Configuration Portal Account Management

The Gateway Configuration Portal is used to authenticate users via username and password. It provides the ability to configure internet connectivity, the wireless network, as well as access logs. The Gateway Configuration Portal can only be accessed locally by connecting to the gateway via Ethernet during the initial setup and configuration, using the default IP address (https://10.110.210.2). If WiFi is configured, or the default IP address has been changed, then it is possible to access the Configuration Portal using the new IP address. Please consult the IoT Gateway Configuration Portal section of the EcoStruxure Building IoT Sensor Solution - Operating Guide for detailed steps on configuring the gateway, and for accessing the Configuration Portal.

NOTICE

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Do not log in the Gateway configuration portal where password entry may be monitored by humans or cameras.
- Upon first log in, the Gateway configuration portal will require a password change. Ensure that the password meets company policy for password security.

Failure to follow these instructions can result in loss of data or unauthorized system access.

The Gateway Configuration Portal can only connect to the Cloud Portal if it has a valid date and time configured. The NTP server must be configured to connect to the Cloud Portal. The Gateway Configuration portal allows configuring the NTP time server in the "System" menu.

NOTICE
POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY • Ensure that all gateways have accurate configuration of NTP time synchronization. **Failure to follow these instructions can result in loss of data or unauthorized system access.**

8.7 Gateway Installation

It is important to install the gateway in a secure, protected location that is inaccessible to unauthorized personnel—for example, in ceilings or access-controlled rooms.

To avoid signal interference and ensure optimal performance, the gateway should be installed at least a few meters away from:

- WiFi routers
- Metal structures (e.g., bars, frames)
- RF-emitting equipment (e.g., radios, transmitters)

Proper placement helps maintain reliable communication with connected devices and ensures stable network performance.

8.8 Network Security

8.8.1 Expected Endpoints

Schneider Electric recommends only allowing access to the required domains as per your needs.

The following table lists the domain names and protocols used when the IoT Gateway connects to the Cloud.

Table – Domain Names and Protocols

Domain Name	Protocol	Description
cnm-ih-na.azure-devices.net	MQTT/WS (port 443)	Used at first connection of IoT Gateway to the cloud (or after a factory reset) and send data streams.
etp.prod.struxurewarecloud.com	HTTPS (TCP port 443)	Used for using IoT Sensor support functions.
cnmiothubappstna.blob.core.windows.net	HTTPS (TCP port 443)	Used for daily log upload to ETP from Gateway.

IMPORTANT:

- For **Gateways connected to the cloud via Ethernet**, we recommend enabling FQDN (Fully Qualified Domain Name) whitelisting for the domains listed above, using the device's MAC address as the source identifier. This approach helps prevent disconnections caused by unexpected IP address changes.
- For **Gateways connected to the cloud via WiFi**, be aware that MAC address randomization can occur depending on the SSID to which the device is connected. We recommend implementing appropriate measures to mitigate this impact.

8.8.2 Data Security in Motion

Schneider Electric's EcoStruxure cloud applications follow industry best practices, including:

- **Encrypted Communication**: All data exchanged between the EcoStruxure IoT Gateway and internal Schneider Electric systems or external third-party systems is encrypted using HTTPS, with a minimum requirement of TLS 1.2.
- **Secure Certificates**: Certificates used in these encrypted sessions employ the SHA-256 secure hash algorithm. This applies to all communications between the IoT Gateway and the cloud.

8.8.3 Data Security at Rest

Schneider Electric follows best practices to create secure solutions and to limit the risk of data being compromised in any meaningful manner while protecting the privacy, control, and autonomy of each customer's data independently from any other.

8.8.4 System Defense in Depth

All system components that may be used to integrate the IoT Gateway and/or the Cloud API must be secured. See the Notice below on ways to secure the system.

NOTICE

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Install routers, switches, or hubs that may be needed for interconnection of The IoT Gateway and Cloud Portal to be accessible by authorized personnel only.
- Ensure that the network only opens the ports required by the system.
- For network segmentation, ensure Gateway network design and Cloud API access is planned and implemented according to current guidelines and best practices. The IoT Gateway must be isolated from critical systems on the network. For more information, see Guidance on Implementing a Cybersecure BMS Architecture with EcoStruxure Building Operation on the Schneider Electric website (www.se.com).
- The EcoStruxure Buildings IoT Sensor Solution is a connected offer with devices installed at a customer site, and a Cloud portal to manage those devices. Various cybersecurity strategies need to be implemented to protect the system, including perimeter hardening, network hardening and more. For Cybersecurity best practices, follow current guidelines. For more information, see Recommended Cybersecurity Best Practices on the Schneider Electric website (www.se.com).
- The Gateway configuration portal must only be accessible on the local network. The Gateway configuration portal must not be accessible from the Internet (ex. outside the network firewall).

Failure to follow these instructions can result in loss of data or unauthorized system access.

NOTE: The Gateway and sensors support signed and authenticated firmware upgrades. Only firmware signed by the Schneider Electric public key infrastructure is supported by the system.

8.8.5 DNS Security Configuration

When deploying the Gateway, it is essential to use a secure DNS infrastructure:

- Ensure that DNS servers do not permit zone transfers unless explicitly required and tightly controlled.
- Unauthorized zone transfers can expose internal network structures and sensitive configuration details to attackers.
- Use DNS servers that support access control mechanisms, and configure them to reject AXFR requests from untrusted sources.

These measures help maintain the confidentiality and integrity of your network environment.

9 Troubleshooting

What's in This Chapter?

9.1 User Account Re-creation Issues

To re-create User accounts, Administrators cannot use the email IDs of Deleted Users/Revoked Users.

9.1.1 Solution

For new account creation, new email IDs for the members are needed. A Revoked User’s email ID is still in the system, and therefore cannot be re-used. This is a known Limitation with the Account Management tool.

9.2 Unknown Gateway Status

The gateway status is "Unknown" on the floor plan in the Cloud (gateway icon is blue).

9.2.1 Solution

Gateway Configuration Portal Shows a Red Cloud Icon

The Gateway has not successfully connected to the Cloud portal. This can occur if:

- The system clock is not correct. The Cloud will reject gateway connections when a system clock is not synchronized to UTC time. An NTP server is highly recommended to ensure the system clock is synchronized accurately. The system clock is visible on the Dashboard page. If it is not within a few minutes of UTC time, then the clock can be configured in the System page. Select "HTTPS Time Sync" or enter a valid NTP Server value on the System page of the Configuration Portal, while ensuring port 123 is opened on the network. If the NTP server is unavailable, you can manually set the date and time. However, this setting may be lost during a power outage.

- Wireless network settings are not correct. Although the gateway generates random Wireless network values in production, it is important to ensure that the wireless network icon is green. If not, go to the Wireless setting tab in the Configuration Portal and enter valid values. Note that these values should only be changed if there are no sensors on the network.
- Internet settings are incorrect in the Configuration Portal's Network page. Once the settings are entered correctly, the Cloud icon in the Configuration portal will become green.
    - Cellular Connection
        - If using a cellular connection, ensure that the LTE antenna is connected to the gateway.
        - Ensure that the SIM card is inserted in the gateway. The gateway needs to be powered off before inserting the SIM card. Once inserted, power on the gateway then enter the cellular connection settings. After saving the settings, it can take a few minutes before the LTE/Cellular connection is established. The Dashboard page of the gateway will show the signal strength quality.
    - WiFi
        - Ensure that the gateway is within range of an access point.
        - If the gateway is configured with a static IP address, ensure that the static IP address is in the proper range of the local network, and that the gateway and DNS entries are correct.
        - If DHCP is enabled, ensure that the gateway has obtained an IP address, Gateway IP address and DNS entries.
        - Ensure ports 443 and 123 are open.
        - Note that the gateway does not support connecting to a WiFi network that uses a guest portal for connectivity.
    - Ethernet
        - Ensure that an Ethernet cable is connected securely to the gateway.
        - If the gateway was configured with a static IP address, ensure that the static IP address is in the proper range of the local network, and that the gateway and DNS entries are correct.
        - If DHCP is enabled, ensure that the gateway has obtained an IP address, Gateway IP address and DNS entries.
        - Ensure ports 443 and 123 are open.
- Both the WiFi interface and Ethernet interfaces have a DNS and/or Gateway configured. In this case, Ethernet is given priority to connect to the Internet. If the Ethernet connection does not have access to the Internet, then the gateway will remain offline until the Ethernet cable is unplugged. Ensure that only the interface that has internet access will have its DNS and Gateway settings configured.

- Internet settings are correct in the Configuration Portal but there is a network issue or the connection is down.

Gateway Configuration Portal Shows a Green Cloud Icon

The Gateway is successfully connected to the Internet and the Cloud however the site is showing an "Unknown" status. In this scenario, the gateway has not identified itself to the specific customer's site. This can occur if:

- Wireless network settings are not correct. This issue is related to older gateways that were upgraded to version 1.2.3 or later before configuring the wireless settings to valid values. The wireless settings show "none" as shown in the image below as they were not generated correctly after the production process was completed. To correct this issue, go to the Wireless setting tab in the Configuration Portal and enter valid values then "Submit" the changes. Note that these values should only be changed if there are no sensors on the network.
- The gateway was powered on before adding the gateway to the floor plan. Gateway status announcements are sent every 20 minutes so it may be required to wait up to 20 minutes before the gateway's status becomes "online" in the Cloud. Refresh the floor plan or the gateway list in the Cloud portal to see if the status has changed to Online. Rebooting the gateway will result in the gateway sending its announcements after booting up completely. This can take five to seven minutes.
- The Gateway UID was entered incorrectly on the floor plan. Ensure that the Gateway UID entered on the floor plan is correct. The UID is case sensitive and can be found on the Gateway cover.

9.3 Offline Gateway Status

The gateway icon is red or the gateway status is "Offline" on the Cloud Portal floorplan.

9.3.1 Solution

The gateway status on the Cloud Portal's floor plan is showing a red icon and "offline" status. Gateways send a keepalive announcement every 20 minutes, and the Cloud monitors this to manage the gateway's connectivity status. An offline status can occur when:

- The gateway has not communicated with the Cloud in over 45 minutes.
- The internet connection is down at the gateway's site if connected via WiFi or Ethernet. Determine if the Internet provider is the issue. If not, check the Ethernet or WiFi settings to confirm that they are set correctly.
- The Gateway's WiFi signal strength is weak. The Configuration Portal's Dashboard displays the signal strength so it can be used to determine if the gateway needs to be moved to a new location.
- The cellular connection is down or the signal strength is weak. The Configuration Portal's Dashboard displays the signal strength so it can be used to determine if the gateway needs to be moved to a new location. Ensure that the cellular antenna is correctly attached to the gateway.

- The Gateway's system clock is no longer synchronized to UTC time. If using a NTP server, ensure that it is configured correctly and that port 123 is opened. If a date and time were entered manually (not recommended) but the gateway lost power for a long period of time, re-enter those values or configure an NTP server.

9.4 Sensor Is Not Joining the Network

The sensor is not joining the network.

9.4.1 Solution

If the sensor is not joining the network, follow these instructions and retry. Ensure that the gateway is "Online" in the Cloud by either checking the floor plan for the gateway icon to be green or verifying the status in the Gateway List. Also ensure that the Wireless settings on the gateway’s configuration portal are configured and saved with valid values (Address, Network, Channel, and encryption key).

- Delete the latest addition from the floor map and ensure the sensor is added again to the floor map. Hit Save Mapping and proceed to Network Lock.
- Ensure the gateway is unlocked again, then press the sensor button for more than three seconds to re-initiate the join process.

If this does not solve the issue, confirm that a single, quick press of the sensor button makes the LED blink red.

- If the LED blinks green, perform a factory reset on the sensor followed by a power cycle (as described below), then repeat the single-click test.
- A sensor that has not joined any network will blink red upon a single click.

Factory Reset: Insert a pin into the small hole on the sensor, press and hold for more than 10 seconds. Refer to the Device Specification Sheet for more details.

Power Cycle: Refer to the Device Specification Sheet for the power cycle procedure. After completing these steps, try adding the sensor again.

Checklist

Here is a checklist to go through when commissioning a sensor:

- Is the gateway connected to the Cloud? (i.e. green icon at the top of the page).
- Are the Wireless settings configured to valid values? (i.e. there are no "None" entries" anywhere, and the Auth and Cipher keys are not empty).
- Was the gateway added to the correct site's floor plan and showing "Connected" and a green icon?
- Was the floor plan map saved?
- Was the gateway network unlocked?
- Was the sensor join process started? (I.e. press and hold the sensor button for at least four seconds then release. The amber LED should be blinking)

- Once joined, the sensor will blink its green LED five times. A quick press of the button should confirm this by blinking the green LED again
- Does the sensor show "Online" status on the site's floor plan? The circle icon should also be green.

9.5 Sensors Are Offline

The sensors are offline.

9.5.1 Solution

Here are the possible reasons:

- If the gateway is online and connected, verify that the sensor batteries are correctly inserted and have sufficient charge.
- If the gateway is online, modify a sensor’s status—such as changing an Occupancy sensor from Unoccupied to Occupied—and check that it is now online.
- If the gateway is disconnected, it is normal that all sensors are Offline. Recheck the sensors status once Gateway is back to green or connected.

9.6 Installation Quality

This section offers information on troubleshooting the installation quality of the sensors.

9.6.1 Solution

There are two data points that are transmitted once per day by each sensor to help give an idea of the link quality between the sensor and its neighbor. These data points are:

- **RSSI**: This is the received signal strength indicator in dB and is a negative number. Values of -75 or higher generally good indications that the next message hop is close. Values of -85 to -95 generally mean the hop is much further away.
- **Output Power**: The sensors adjust how strong their transmission power is based on the proximity of its neighbor. 8dB is the highest so that means the sensor is transmitting messages at the maximum power. Anything lower than 8dB is good, particularly 0 or negative dB values. This means there is a neighbor sensor nearby.

9.7 Desk Sensor

This section offers information on troubleshooting the Desk Sensor.

9.7.1 Solution

False Unoccupied Status

Check if the Desk Sensor and the object of view (human) have any metal bar in between. It is a known limitation currently that Desk sensors installed behind a metal bar have a performance degradation where human detection is not consistent. One temporary workaround is to install a shim in between the sensor and the desk to have the sensor's field of view unobstructed by the metal bar.

If the desk sensor is installed near a heat source (such as a space heater), it may also report a false unoccupied status.

9.8 Room Occupancy Sensor

This section offers information on troubleshooting the Room Occupancy Sensor.

9.8.1 Solution

False Unoccupied Status

There are people in the field of view, however the room occupancy sometimes reports unoccupied status for short periods of time before reporting occupied again. This can occur if:

- It is possible that the PIR sensor cannot detect occupants if they remain fairly still or motionless for the occupied-to-unoccupied time (default is five minutes). The PIR detector used in the room occupancy sensor is very sensitive to motion in any direction.
- The sensor is installed too far from the occupants (or just at the limit of the range). Ensure that the room occupancy sensor is installed on the ceiling or wall closest to where the occupants will be. This distance must be within the sensor's detection range limits and field of view. See the data sheet for the specifications.

False Occupancy Detections

There is no one in the room where the room occupancy sensor is installed however it is sometimes reporting an occupied status. This can occur if the sensor's field of view overlaps with a hallway through glass windows/walls.

In either scenario it is recommended to move the sensor to a different location (wall or ceiling) that allows its field of view to capture room occupants while avoiding other sources of heat.

9.9 Well-Being Sensors

This section offers information on troubleshooting Well-Being Sensors.

9.9.1 Solution

Sensor Accuracy

The Well-Being Sensors need to be installed on a wall, and in a specific orientation (with the ventilation opening at the bottom). If the sensor is not installed in this way, then the airflow can potentially impact the sensor accuracy.

Battery Life

The Well-Being Sensors, and especially the Well-Being Sensor with the particulate matter sensor can have lower than expected battery life if the Energy Profiles are not managed correctly. Battery life measurements were estimated using standard working hours, with Profile 0 being used when the building is occupied, and Profile 5 or 6 used as the profile when the building is unoccupied and during the weekend. It is strongly

recommended to configure the correct working hours and weekends, and use the least aggressive energy profiles (in terms of measurement frequency) to extend the battery life as much as possible. Otherwise, if more measurements are required, for longer parts of the day, then it is strongly recommended to power the Well-Being Sensors via USB-C.

Schneider Electric
www.se.com/buildings

04-10050-03-en
February, 2026