

Anybus<sup>®</sup> Wireless Bolt II<sup>™</sup>  
**USER MANUAL**

SCM-1202-209  
Version 1.3  
Publication date 2024-09-25



## Important User Information

### **Disclaimer**

The information in this document is for informational purposes only. Please inform HMS Networks of any inaccuracies or omissions found in this document. HMS Networks disclaims any responsibility or liability for any errors that may appear in this document.

HMS Networks reserves the right to modify its products in line with its policy of continuous product development. The information in this document shall therefore not be construed as a commitment on the part of HMS Networks and is subject to change without notice. HMS Networks makes no commitment to update or keep current the information in this document.

The data, examples and illustrations found in this document are included for illustrative purposes and are only intended to help improve understanding of the functionality and handling of the product. In view of the wide range of possible applications of the product, and because of the many variables and requirements associated with any particular implementation, HMS Networks cannot assume responsibility or liability for actual use based on the data, examples or illustrations included in this document nor for any damages incurred during installation of the product. Those responsible for the use of the product must acquire sufficient knowledge in order to ensure that the product is used correctly in their specific application and that the application meets all performance and safety requirements including any applicable laws, regulations, codes and standards. Further, HMS Networks will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features or functional side effects found outside the documented scope of the product. The effects caused by any direct or indirect use of such aspects of the product are undefined and may include e.g. compatibility issues and stability issues.

Copyright © 2023 HMS Networks

### **Contact Information**

Postal address:

Box 4126

300 04 Halmstad, Sweden

E-Mail: [info@hms.se](mailto:info@hms.se)

# Table of Contents

<b>1. Preface</b>	<b>1</b>
1.1. About This Document	1
1.2. Document Conventions	1
1.3. Trademarks	2
<b>2. Safety</b>	<b>3</b>
2.1. General Safety	3
2.2. Intended Use	3
<b>3. Preparation</b>	<b>4</b>
3.1. Cabling	4
3.2. Network Environment	4
3.3. Placement Considerations	4
3.4. Support and Resources	4
3.5. HMS Software Applications	5
3.6. Third-Party Software Applications	5
<b>4. Installation</b>	<b>6</b>
4.1. Installation Drawing	6
4.2. Surface Mounting	7
4.3. Connect to Power Over Ethernet (PoE)	10
4.4. Connect to Power and Ethernet	12
<b>5. Configuration</b>	<b>14</b>
5.1. Connect to Configure	14
5.2. Access the Built-In Web Interface	16
5.2.1. Required IP Address Settings	16
5.2.2. Login to the Built-In Web Interface	17
5.2.3. Logout From the Bolt II Built-In Web Interface	19
5.3. Bolt II Built-In Web Interface Overview	20
5.4. Wireless Bolt II Operation Modes	21
5.5. Cable Replacement Mode Setup	22
5.6. Access Point Mode Setup	26
5.7. Client Mode Setup	29
5.8. Wireless Settings	32
5.8.1. I/O-Data Cycle Time Considerations	32
5.8.2. Cable Replacement Access Point Settings	32
5.8.3. Cable Replacement Client Settings	34
5.8.4. Access Point Settings	36
5.8.5. Client Forwarding Modes	38
5.8.6. Client Security Settings	43
5.8.7. Client MAC Clone (MAC Address Cloning) Settings	44
5.8.8. Client NAT (Network Address Translation) Settings	47
5.9. Ethernet Settings	49
5.9.1. To Configure IP Settings Manually	49
5.9.2. To Use DHCP Client	50
5.10. Apply Configuration	51
<b>6. Verify Operation</b>	<b>52</b>
6.1. Bolt II Status Monitor	52
6.2. Ethernet LED Indication	54
<b>7. Use Cases</b>	<b>55</b>

7.1. Cable Replacement Between a PLC and a Network Switch .....	55
7.2. Access PLC from Handheld Device via Wi-Fi .....	59
7.3. Connect Device to Wi-Fi Network via Bolt II Client .....	63
7.4. Connect Bolt II Clients on Enterprise Wireless Network .....	66
<b>8. Maintenance .....</b>	<b>68</b>
8.1. Time & Date Settings .....	68
8.1.1. Set Time .....	68
8.1.2. Network Time Protocol (NTP) Synchronization .....	69
8.1.3. Use Timezone Settings .....	70
8.2. Configuration File Handling .....	71
8.2.1. Export Configuration .....	71
8.2.2. Import Configuration .....	72
8.3. Revert Configuration .....	73
8.4. Firmware Management .....	74
8.4.1. View the Firmware Version .....	74
8.4.2. Firmware and Configuration Compatibility .....	74
8.4.3. Firmware File Validation .....	74
8.4.4. Update Firmware .....	75
8.5. Security .....	76
8.5.1. Web Server Certificate .....	76
8.5.2. WPA2/WPA3 Enterprise Certificates .....	77
8.6. Change the Bolt II Password .....	80
<b>9. Troubleshooting .....</b>	<b>81</b>
9.1. Diagnostics .....	81
9.1.1. Event Log .....	81
9.1.2. Remotely Monitor the Bolt II Status .....	82
9.2. Find the Bolt II IP Address .....	82
9.3. Reboot Using the Reset Button .....	83
9.4. Reboot Using the Built-In Web Interface .....	84
9.5. Factory Reset Using the Reset Button .....	86
9.6. Reset Using the Built-In Web Interface .....	87
9.7. Support .....	89
9.7.1. Support Package .....	89
<b>10. Technical Data .....</b>	<b>90</b>
10.1. Technical Specifications .....	90

# 1. Preface

## 1.1. About This Document

This document describes how to install and configure Anybus® Wireless Bolt II™.

For additional documentation and software downloads, FAQs, troubleshooting guides and technical support, please visit [www.hms-networks.com](http://www.hms-networks.com).

## 1.2. Document Conventions

### Lists

Numbered lists indicate tasks that should be carried out in sequence:

1. First do this
2. Then do this

Bulleted lists are used for:

- Tasks that can be carried out in any order
- Itemized information

### User Interaction Elements

User interaction elements (buttons etc.) are indicated with bold text.

### Program Code and Scripts

```
Program code and script examples
```

### Cross-References and Links

Cross-reference within this document: [Document Conventions \(page 1\)](#)

External link (URL): [www.hms-networks.com](http://www.hms-networks.com)

### Safety Symbols



#### DANGER

Instructions that must be followed to avoid an imminently hazardous situation which, if not avoided, will result in death or serious injury.



#### WARNING

Instructions that must be followed to avoid a potential hazardous situation that, if not avoided, could result in death or serious injury.



#### CAUTION

Instruction that must be followed to avoid a potential hazardous situation that, if not avoided, could result in minor or moderate injury.



#### IMPORTANT

Instruction that must be followed to avoid a risk of reduced functionality and/or damage to the equipment, or to avoid a network security risk.

## Information Symbols

**NOTE**

Additional information which may facilitate installation and/or operation.

**TIP**

Helpful advice and suggestions.

## 1.3. Trademarks

Anybus® is a registered trademark and Wireless Bolt II™ is a trademark of HMS Networks AB.

All other trademarks are the property of their respective holders.

## 2. Safety

### 2.1. General Safety

**CAUTION**

This equipment emits RF energy in the ISM (Industrial, Scientific, Medical) band. Make sure that all medical devices used in proximity to this equipment meet appropriate susceptibility specifications for this type of RF energy.

**CAUTION**

This equipment contains parts that can be damaged by electrostatic discharge (ESD). Use ESD prevention measures to avoid damage.

**CAUTION**

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

**CAUTION**

Connecting power with reverse polarity or using the wrong type of power supply may damage the equipment. Make sure that the power supply is connected correctly and of the recommended type.

**CAUTION**

This equipment is not intended for use in an environment where children are present. Keep out of reach of children.

### 2.2. Intended Use

The intended use of this equipment is as a communication interface and gateway. The equipment receives and transmits data on various physical and wireless levels and connection types.

## 3. Preparation

### 3.1. Cabling

Have the following cables available:

- Ethernet cable for configuration
- Ethernet cable for connecting to network



#### NOTE

Both shielded and unshielded Ethernet cables may be used.

- Power cable or Power over Ethernet (PoE) power source.

### 3.2. Network Environment

Ensure that you have all the necessary information about the capabilities and restrictions of your local network environment before installation.

### 3.3. Placement Considerations

For optimal reception, wireless devices require a zone between them clear of objects that could otherwise obstruct or reflect the signal.

To avoid signal interference, a minimum distance of 50 cm between the wireless devices should be observed.

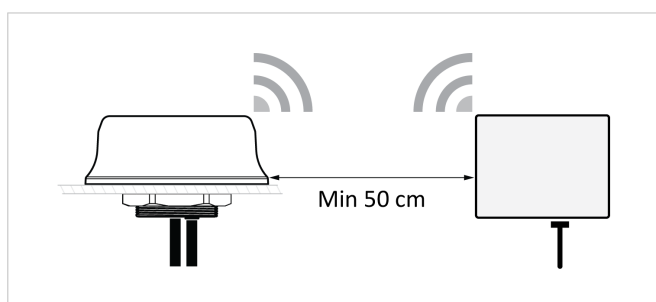


Figure 1. Required minimum distance between wireless devices

### 3.4. Support and Resources

For additional documentation and software downloads, FAQs, troubleshooting guides and technical support, please visit [www.hms-networks.com](http://www.hms-networks.com).



#### TIP

Have the product article number available, to search for the product specific support web page. You find the product article number on the product cover.



## 3.5. HMS Software Applications

Download the software installation files and user documentation from [www.hms-networks.com](http://www.hms-networks.com).

### Supported Operating Systems

Operating System	Description
Windows 7 SP1, 32-bit	Windows 7 32-bit with Service Pack 1
Windows 7 SP1, 64-bit	Windows 7 64-bit with Service Pack 1
Windows 10 64-bit	Windows 10 64-bit
Windows 11 64-bit	Windows 11 64-bit

### HMS IPconfig

Use the software application HMS IPconfig and scan your network to discover the Bolt II IP address and to access the Bolt II built-in web interface.

**NOTE**

HMS IPconfig is only available for Windows.

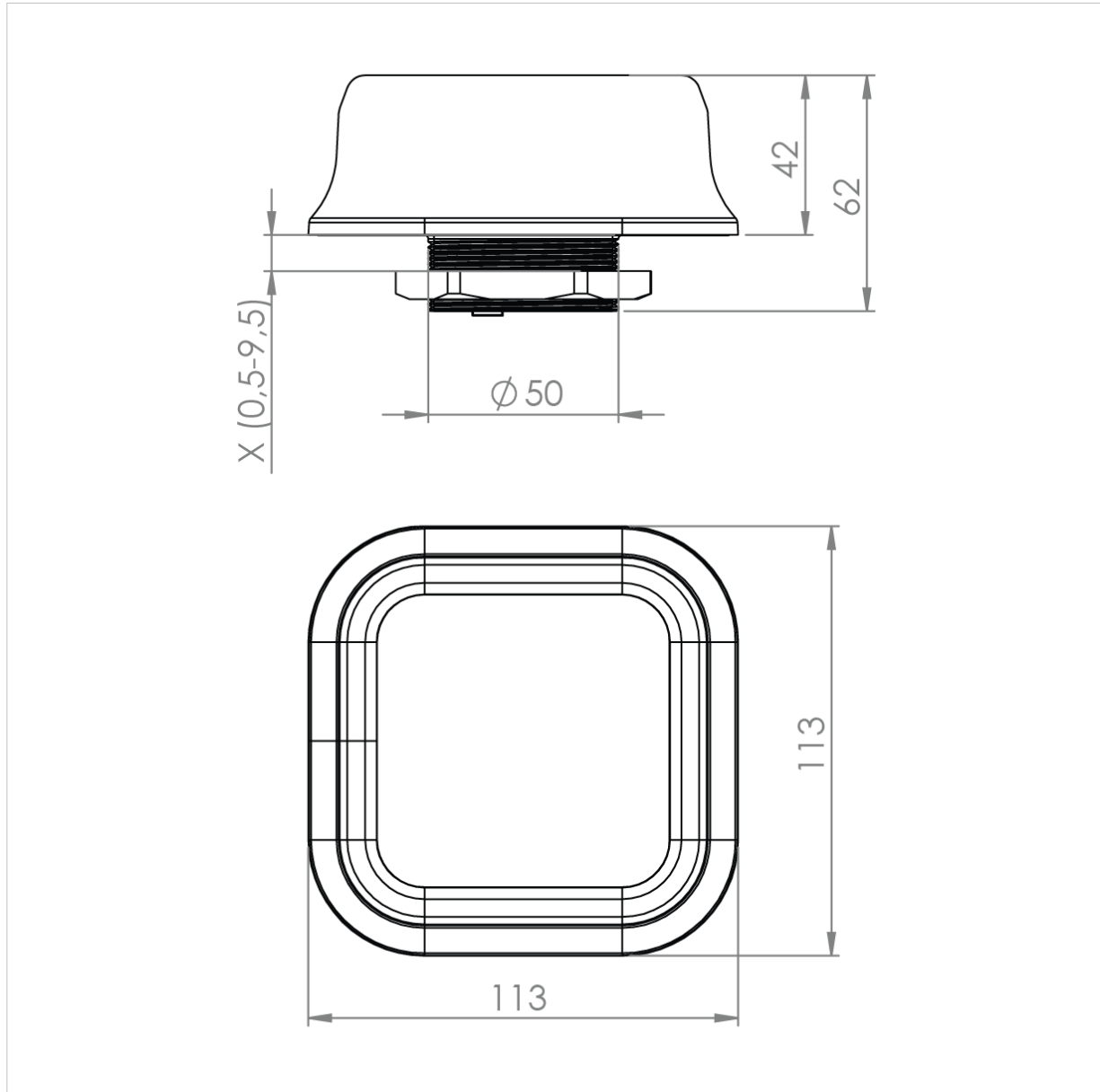
## 3.6. Third-Party Software Applications

### Microsoft Excel

Microsoft Excel, or equivalent software application that supports the Office Open XML Workbook (xlsx) file format. Needed to open and read the **Event log** file.

## 4. Installation

### 4.1. Installation Drawing



All measurements are in mm.

Figure 2. Bolt II installation drawing

## 4.2. Surface Mounting

### Before You Begin

#### Placement Considerations

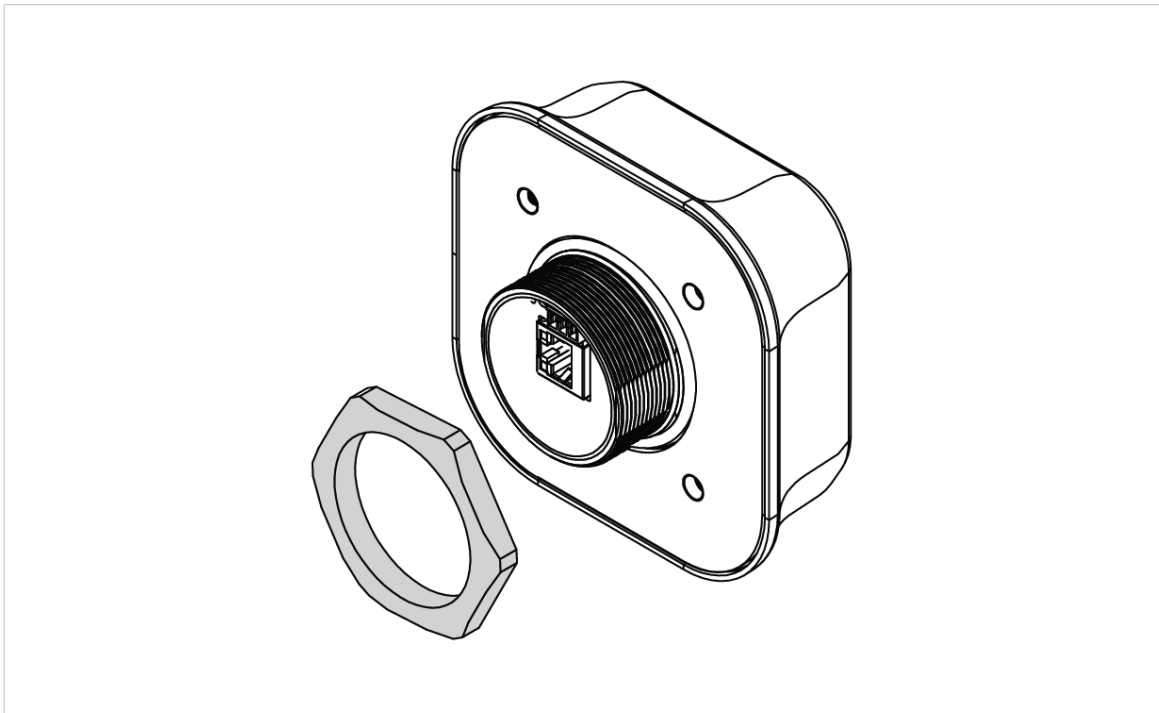
For information about placement for optional reception, see [Placement Considerations \(page 4\)](#).

#### Mounting Considerations

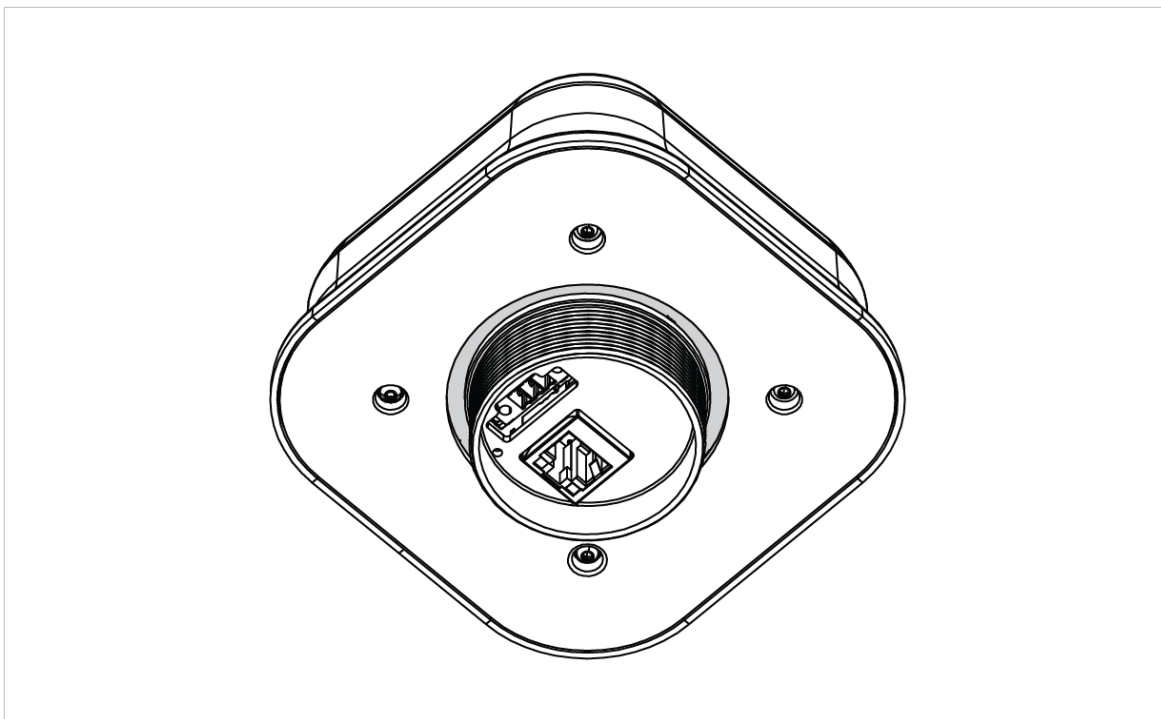
- Mount the Bolt II on a machine or cabinet.
- Mounting hole diameter: M50 (50,5 mm).
- Bolt II lock nut tightening torque: 5 Nm  $\pm$ 10 %.
- Ensure to use the included housing sealing ring and lock nut.
- The top mounting surface, in contact with the sealing, must be:
  - flat with a finish equivalent to Ra 3.2 or finer.
  - cleaned and free from oils and greases.

### Mounting Procedure

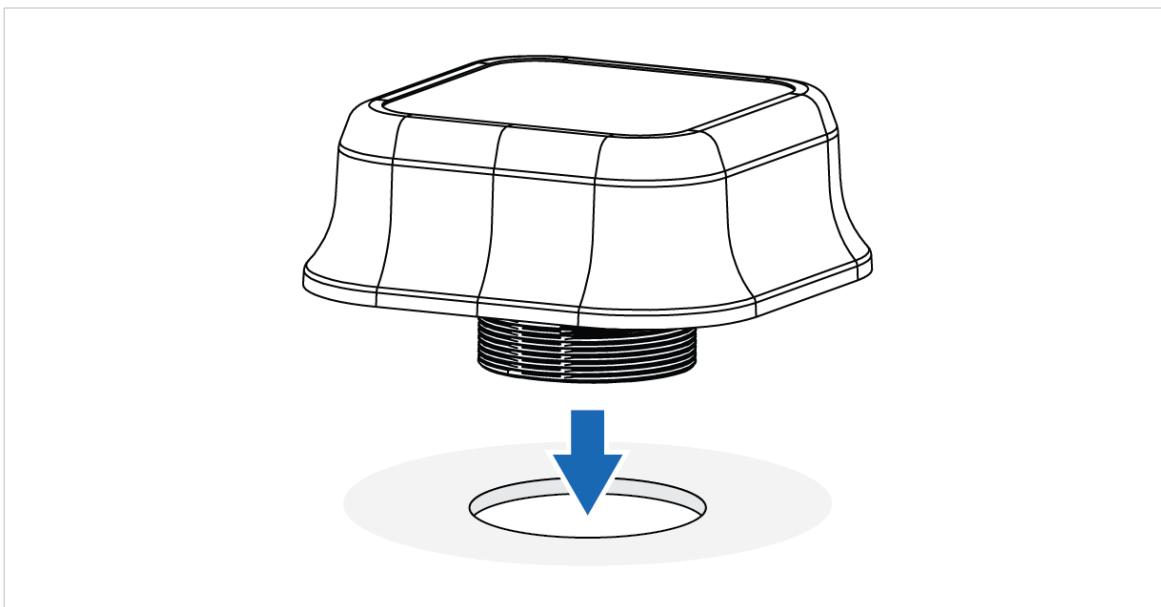
1. Unscrew and remove the Bolt II lock nut.



2. Place the Bolt II housing sealing ring in its groove.



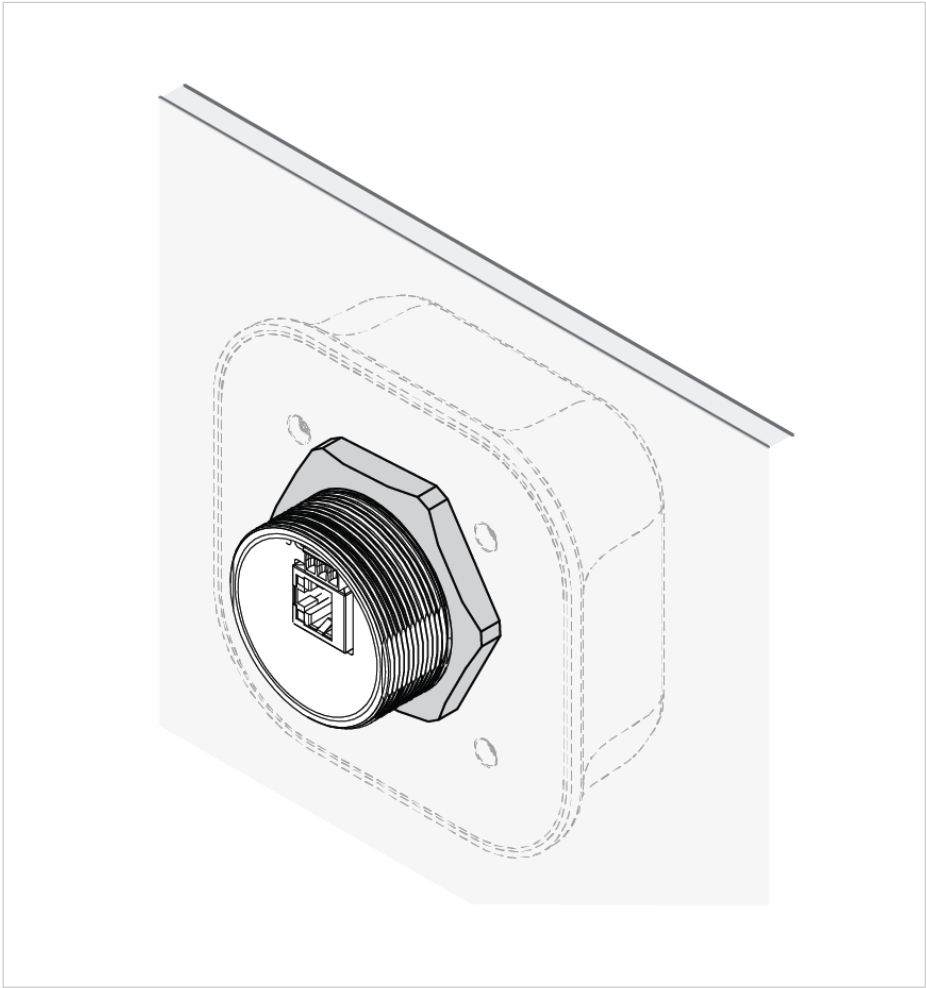
3. In the mounting surface, drill a mounting hole with the size  $\varnothing$  M50 (50,5 mm).
4. Place the Bolt II in its mounting hole.



5. Screw the Bolt II lock nut into place and tighten it.  
Tightening torque: 5 Nm  $\pm$ 10 %

**IMPORTANT**

To keep the Bolt II sealed against dirt and moisture, make sure the housing sealing ring is properly seated in its groove before tightening the lock nut.



## 4.3. Connect to Power Over Ethernet (PoE)

### Before You Begin

**IMPORTANT**

Connecting the Bolt II to PoE and DC power simultaneously may result in a current loop that could damage both the power sources and the Bolt II. Ensure to use only one of the power connections at a time.

**NOTE**

Both shielded and unshielded Ethernet cables may be used.

### Procedure

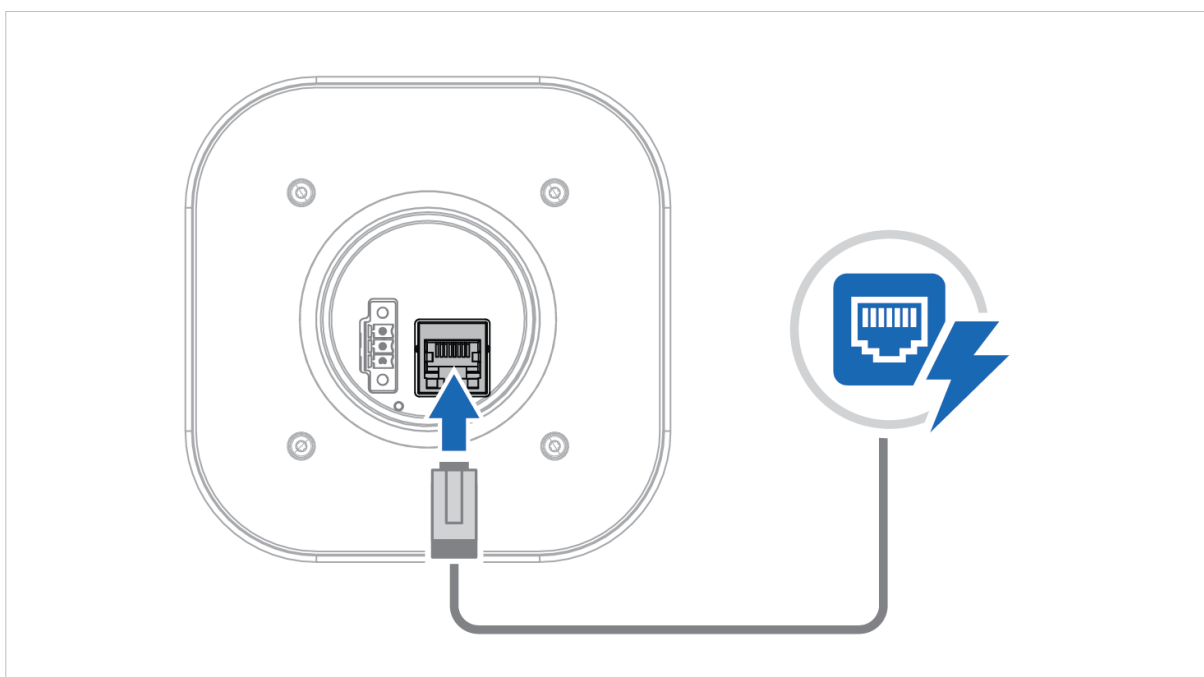


Figure 3. Connect to Power Over Ethernet (PoE)

Connect the Bolt II Ethernet port to Power Over Ethernet (PoE).

RJ45 Ethernet PoE Connector Pinout

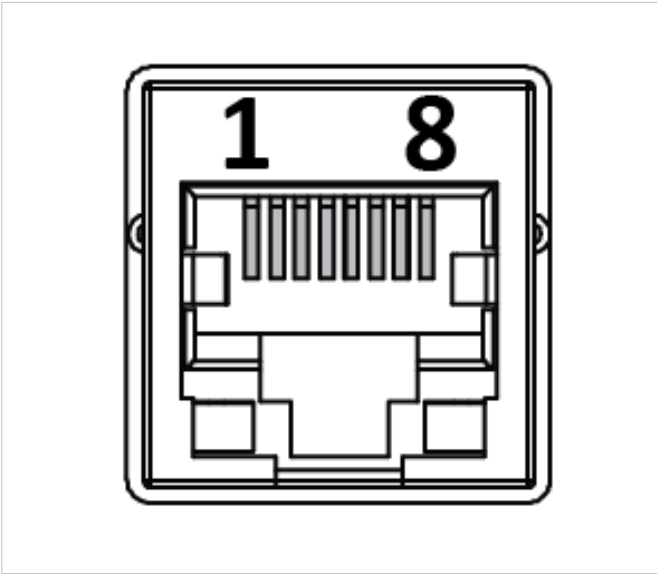


Table 1. RJ45 Ethernet PoE Connector pinning

Pin	Data	PoE	
1	TD+	A+	Positive power from alt. A PSE
2	TD-		
3	RD+	A-	Negative power from alt. A PSE (with pin 6)
4	N/A	B+	Positive power from alt. B PSE
5			
6	RD-	A-	Negative power from alt. A PSE (with pin 3)
7	N/A	B-	Negative power from alt. B PSE
8			
Housing	Shield	Functional Earth (FE), via 1 nF capacitor and 1 MΩ bleeder resistor	

## 4.4. Connect to Power and Ethernet

### Before You Begin

**CAUTION**

Connecting power with reverse polarity or using the wrong type of power supply may damage the equipment. Make sure that the power supply is connected correctly and of the recommended type.

**IMPORTANT**

Connecting the Bolt II to PoE and DC power simultaneously may result in a current loop that could damage both the power sources and the Bolt II. Ensure to use only one of the power connections at a time.

**IMPORTANT**

When Bolt II is powered via the power connector, Functional Earth (FE) must be connected.

### Power Supply Requirements

- Use insulated power supply 10-33 VDC, minimum 2 W.
- Use 0.25 - 1.5 mm<sup>2</sup> (24-16 AWG) cable for supply wiring.
- Use minimum 90 °C copper (Cu) wire only.

### Ethernet Cable Requirement

If the Ethernet cables are to be exposed in an outdoor environment, transient protection must be provided.

### Functional Earth (FE) Wire Screw Placement

When Bolt II is mounted on a sheet metal plate, connect Functional Earth (FE) to the plate near Bolt II.

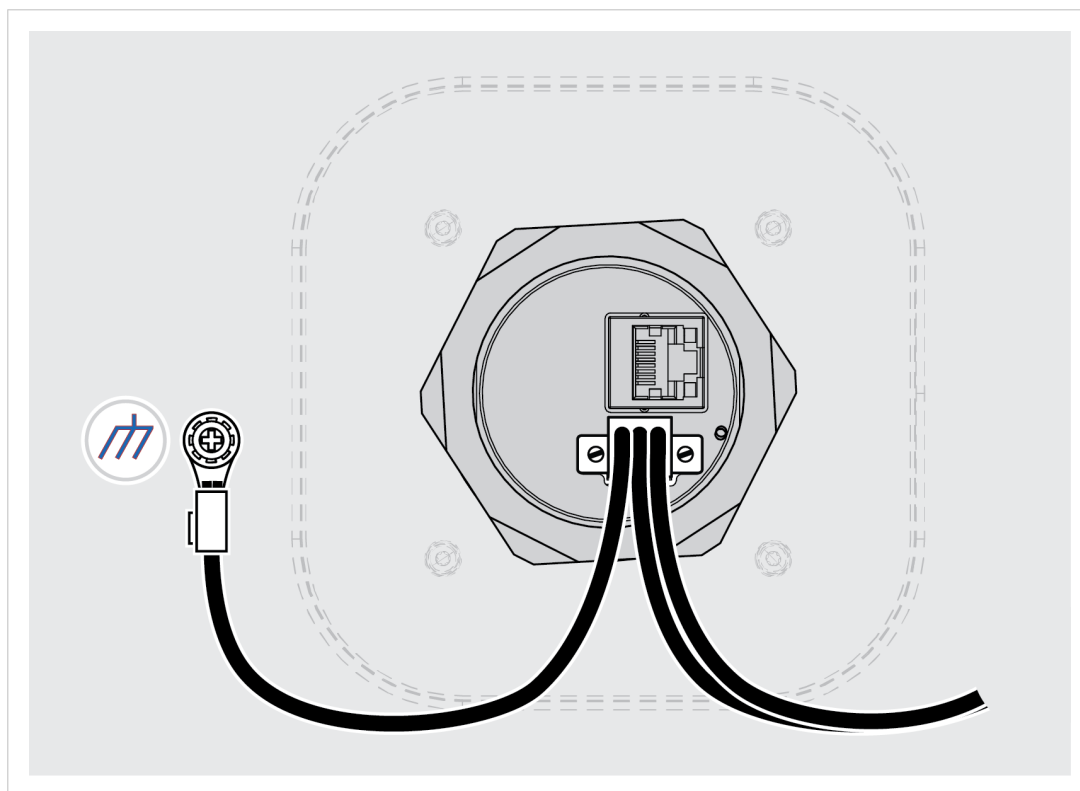


Figure 4. Functional earth wire screw placement, view from below



Procedure

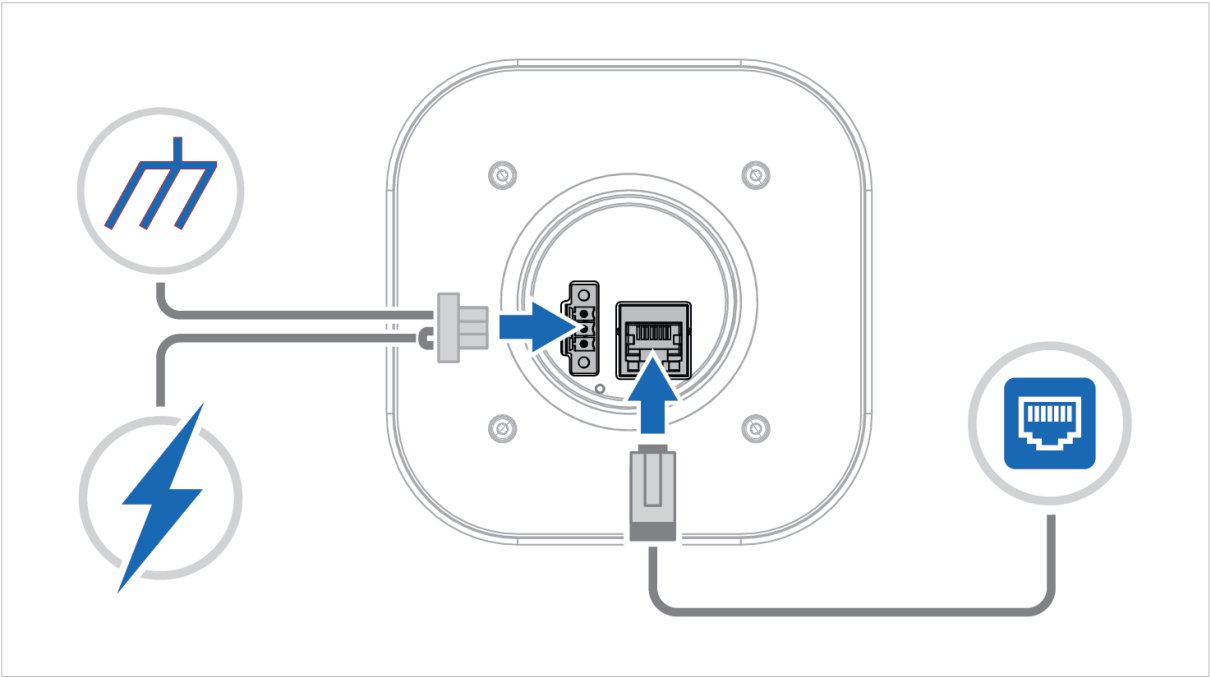


Figure 5. Connect Power, Functional Earth (FE) and Ethernet

Power Connector 3-Pin

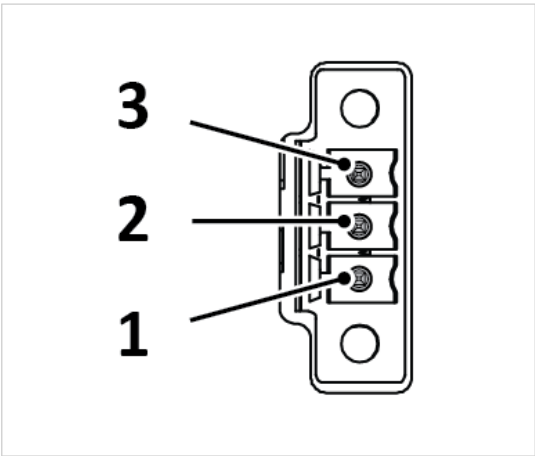


Table 2. Power connector, 3-pin terminal block

Pin	Function	
1	+	Recommended: 12–24 VDC Reverse voltage protection Min: 10 VDC Max: 33 VDC
2	-	
3	Functional Earth (FE)	

Connect Power, Functional Earth (FE) and Ethernet

1. Connect the Bolt II to Functional Earth (FE).
2. Connect the Bolt II to a power supply.
3. Connect the Bolt II to Ethernet network.

## 5. Configuration

### 5.1. Connect to Configure

#### Configure Using a Wired PC

The first time you configure the Bolt II or after a factory reset, connect it to a PC via an Ethernet cable.

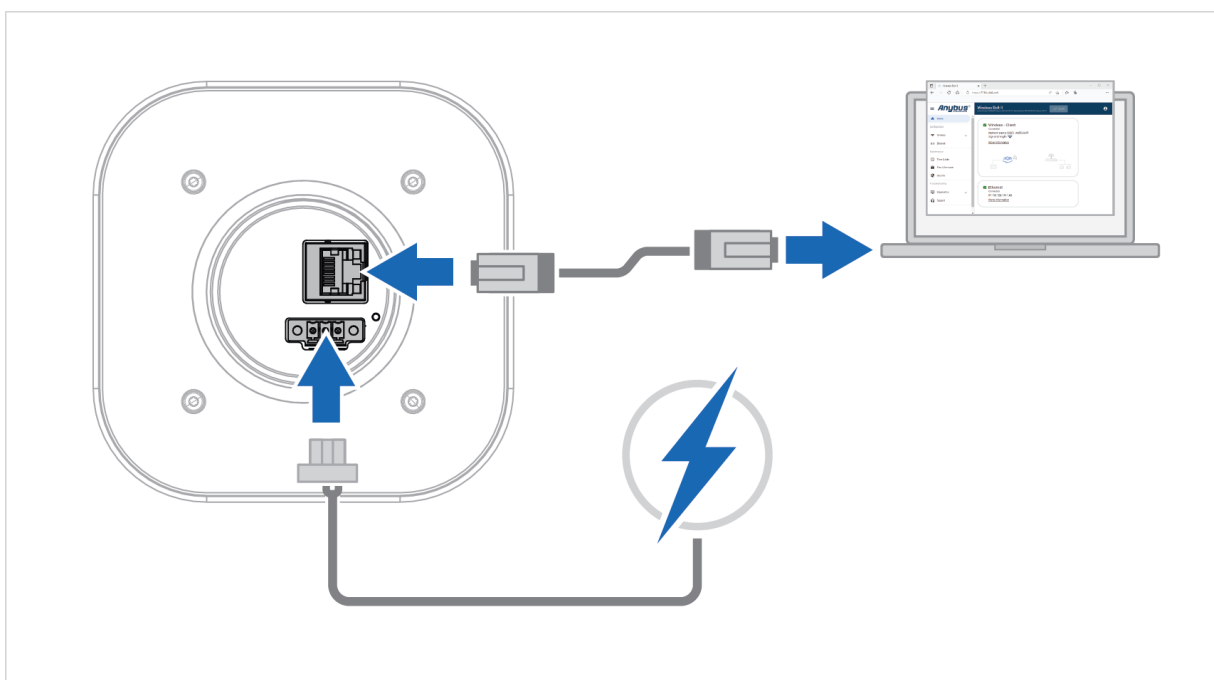


Figure 6. Configure the Bolt II using a PC

1. Connect the Bolt II Ethernet port to your PC.
2. Connect the Bolt II Power connector to a power supply.

## Configure Bolt II Using a Wireless Device



### IMPORTANT

To access the Bolt II Client built-in web interface via a Wi-Fi connection when the **MAC clone** setting is enabled, ensure that the capture port setting is also enabled.

To access the Bolt II Client built-in web interface from a PC connected to it with an Ethernet cable always works.

When the Bolt II is set up as an **Access point** or **Cable replacement Access point** unit, you can configure it using a wireless device.

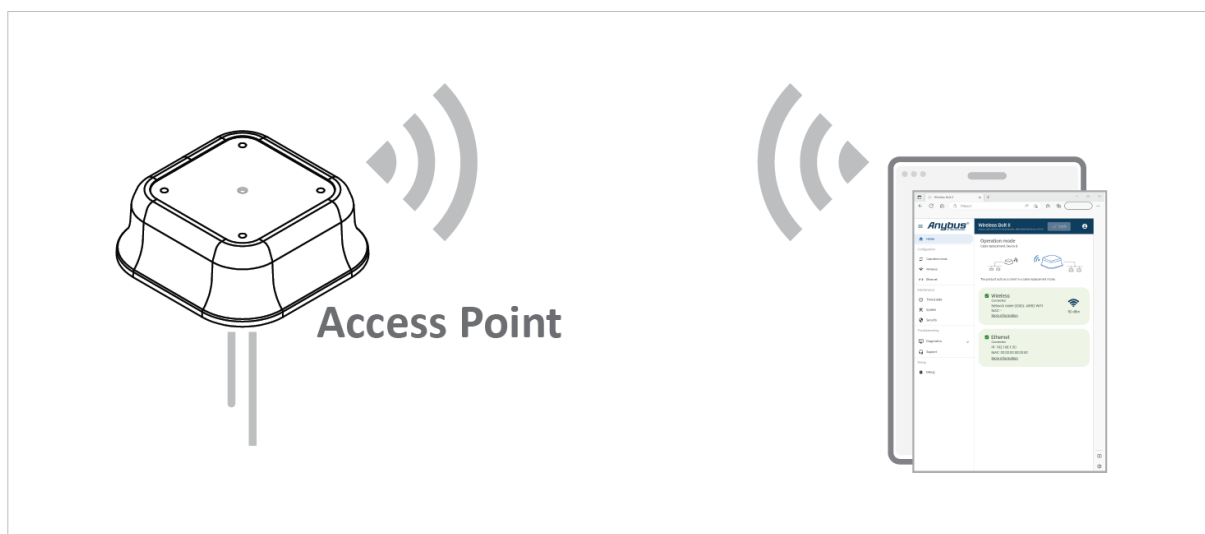


Figure 7. Configure the Bolt II using a wireless device

On the wireless device:

1. Connect to the Bolt II SSID (Network name).



### TIP

You find the default SSID (Network name) and PSK (Pre-Shared Key) on the product cover.

2. To access the Bolt II built-in web interface, enter the Bolt II IP address in a browser.

## 5.2. Access the Built-In Web Interface

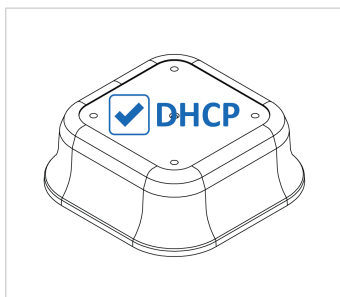
### 5.2.1. Required IP Address Settings

To be able to access the Bolt II built-in web interface you may need to adjust the IP settings, choose one of the following methods.

**NOTE**

The Bolt II default IP address is 192.168.0.97 and the subnet mask is 255.255.255.0.

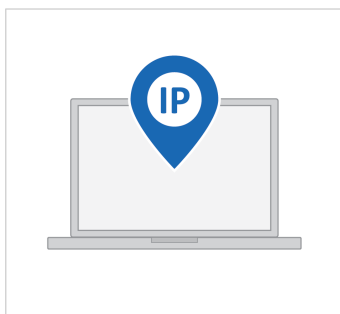
#### Option 1- To use DHCP Server



By default, **DHCP server** is enabled on the Bolt II. Bolt II assigns an IP address to the PC used to configure it.

If the **DHCP server** is disabled, you need to set a static IP address manually on the PC used to configure the Bolt II.

#### Option 2 - Set a Static IP Address on Your PC



On the PC accessing the Bolt II built-in web interface, set a static IP address within the same IP address range as the Bolt II IP address.

**Result**

Now you can enter the Bolt II IP address in your web browser to access the built-in web interface login page.

See [Login to the Built-In Web Interface \(page 17\)](#).

## 5.2.2. Login to the Built-In Web Interface

The Bolt II built-in web interface can be accessed from a standard web browser.

### Before You Begin



#### IMPORTANT

For cybersecurity reasons, you are prompted to change the password at first login using the Bolt II factory default password. You are redirected to the **Change password** page, see [Change the Bolt II Password \(page 80\)](#).



#### NOTE

The Bolt II comes with the default username: admin and password: admin. The default username/password is written in lowercase letters.



#### NOTE

The Bolt II default IP address is 192.168.0.97 and the subnet mask is 255.255.255.0.

### Procedure

Login to the Bolt II built-in web interface:

1. Open a web browser.
2. Click to select the **Address bar** and enter **https://** and the Bolt II IP address.



Figure 8. Enter IP address in web browser

3. Press **Enter**.  
The Bolt II built-in web interface login screen appears.



#### IMPORTANT

By default, a self-signed certificate is installed in the Bolt II.

When you try to access the Bolt II built-in web interface, most browsers issue a security warning. To continue, you need to accept the security warning.

To secure the connection, you need to install a web server certificate in the Bolt II, see [Web Server Certificate \(page 76\)](#).

4. Enter **Username** and **Password** and click **Login**.

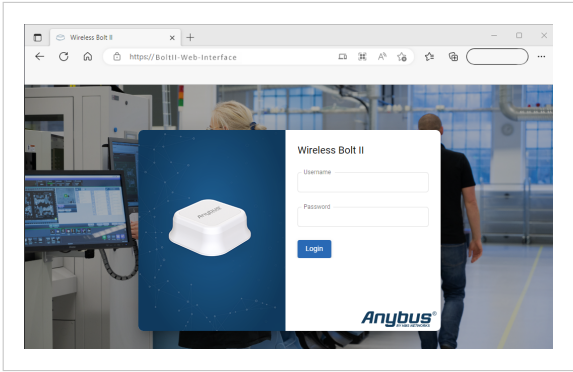


Figure 9. Built-in web interface login screen

Result

You are logged in to the Bolt II built-in web interface **Home** page.

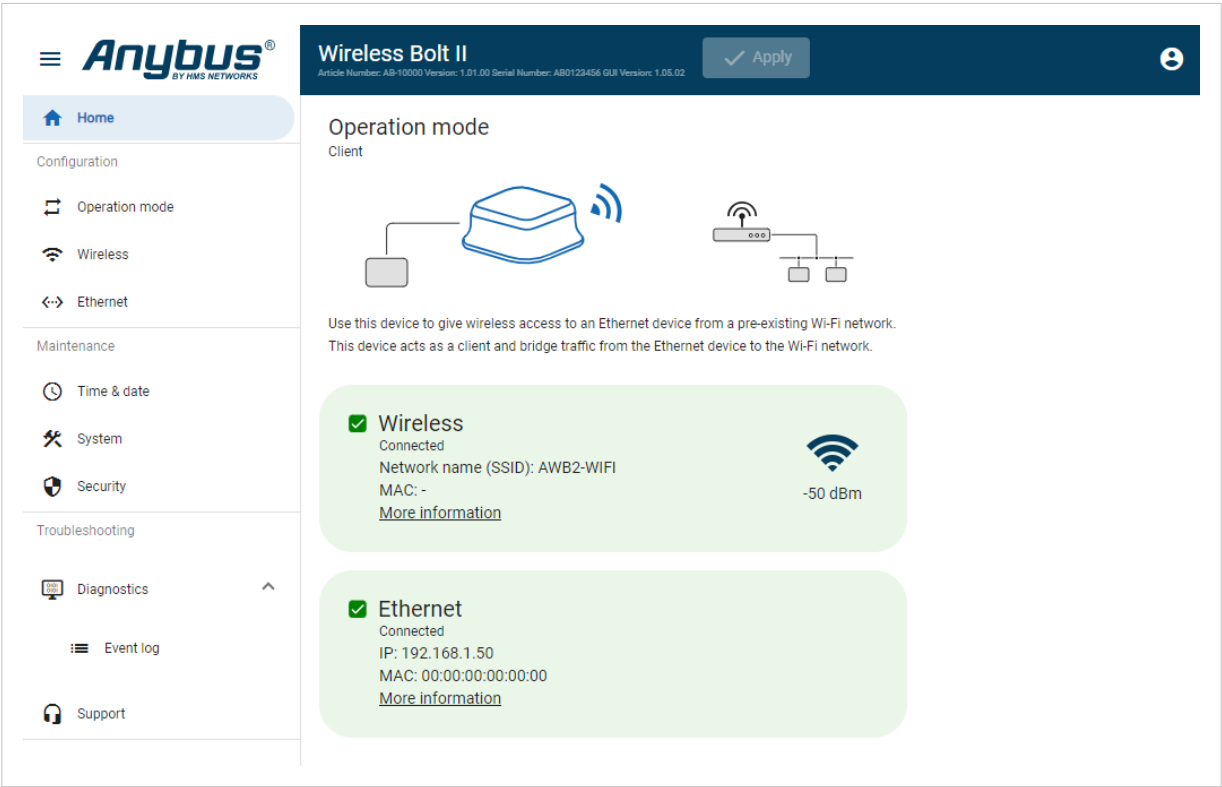


Figure 10. Home page

5.2.3. Logout From the Bolt II Built-In Web Interface



Figure 11. Account menu, Logout

To logout, click on the **Account** icon in the built-in web interface header > **Logout**.

## 5.3. Bolt II Built-In Web Interface Overview

Use the Bolt II built-in web interface to configure, maintain and troubleshoot the Bolt II.

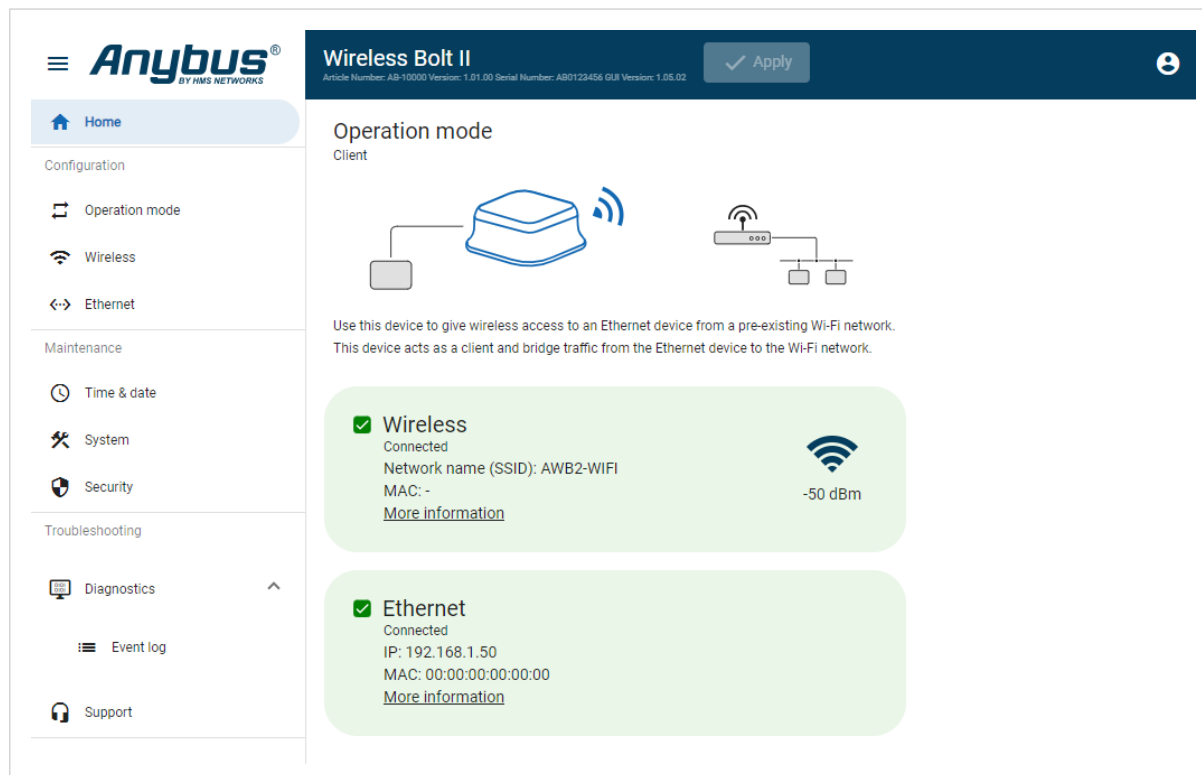


Figure 12. The Bolt II built-in web interface Home page

Table 3. The Bolt II built-in web interface menu

Menu item	Description
Home	View the current Bolt II settings and network status.
Operation mode	Select an <b>Operation mode</b> : <ul style="list-style-type: none"> <li>• <b>Cable replacement</b>: Cable replacement Access point or Cable replacement Client</li> <li>• <b>Client</b></li> <li>• <b>Access point</b></li> </ul>
Wireless	Configure the <b>Wireless</b> settings for the selected <b>Operation mode</b> .
Ethernet	Configure the <b>Ethernet</b> network <b>IP Settings</b> .
Time & date	Set device time and date. Enable/Disable NTP synchronization. Enable/Disable Timezone.
System	Save settings in a configuration files, upload configuration files and upgrade firmware. Revert, reboot, or reset the Bolt II.
Security	Upload a web server certificate to the Bolt II.
Diagnostics	Monitor and troubleshoot the Bolt II.
Support	Contains Bolt II product information, Anybus contact information, link to Anybus support website, and product file for download. Here you can generate a support package with product information, to send to your Anybus support technician.
Apply	After configuration changes are made and verified, press <b>Apply</b> to make the settings take effect.



## 5.4. Wireless Bolt II Operation Modes

Bolt II comes with three wireless **Operation mode** types: Cable replacement, Client and Access Point.

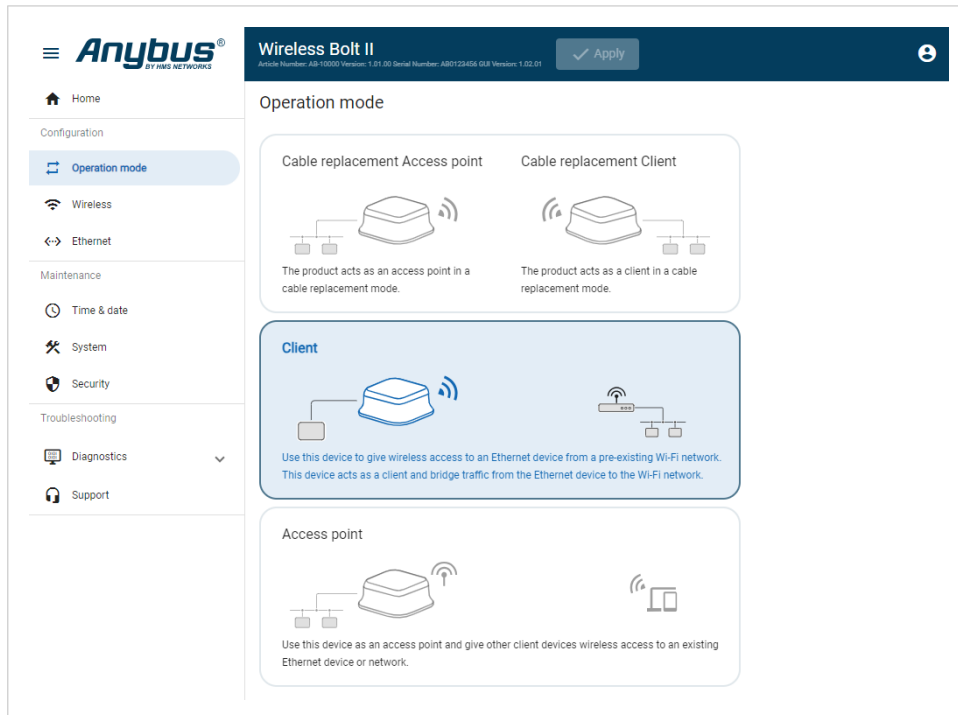


Figure 13. Bolt II Mode page

### Cable Replacement

In a cable replacement installation, two pair of Bolt II units are used to create a wireless bridge between two physical locations.

- **Cable replacement Access point**  
Set up one of the Bolt II as an access point in the cable replacement installation.
- **Cable replacement Client**  
Set up one of the Bolt II as a client in the cable replacement installation.

See also [Cable Replacement Mode Setup \(page 22\)](#).

### Client

Set up the Bolt II as a Client to give Ethernet devices connected to it access to an existing Wi-Fi network.

The Bolt II bridge traffic from the wired Ethernet device to other devices located on the Wi-Fi network.

See also [Client Mode Setup \(page 29\)](#).

### Access Point

Access Point mode is selected by default.

Set up the Bolt II as an access point to give other client devices wireless access to an existing Ethernet device or network.

See also [Access Point Mode Setup \(page 26\)](#).

## 5.5. Cable Replacement Mode Setup

### Before You Begin

In a cable replacement installation, two Bolt II units are used.

One Bolt II acts as an access point and the other Bolt II acts as a client.

### Procedure

#### Configure the Bolt II Cable Replacement Access Point

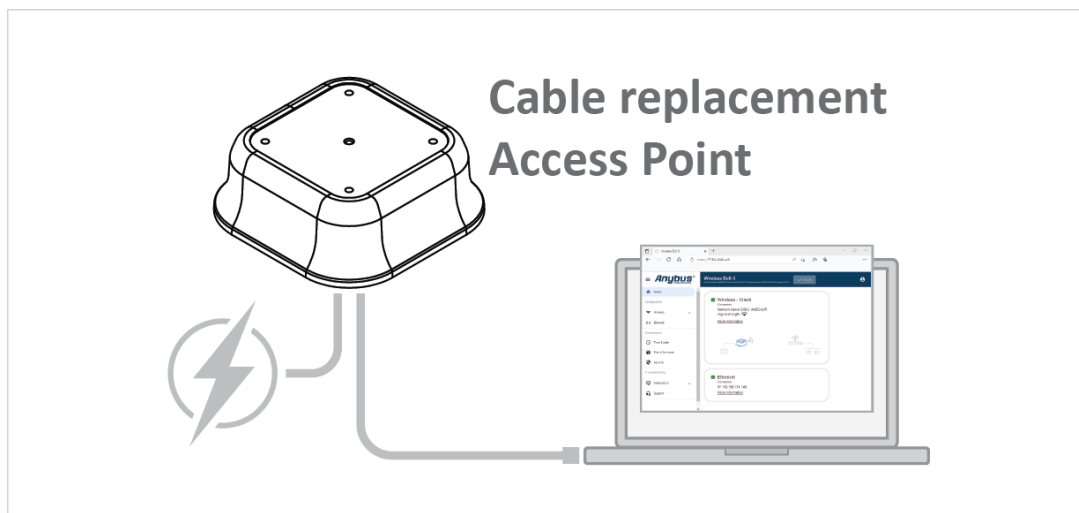


Figure 14. Configure the Bolt II Cable replacement access point

1. Connect the Bolt II access point to power.
2. Connect the Bolt II access point to your PC.
3. Login to the Bolt II access point built-in web interface.
4. Navigate to the **Operation mode** page.
5. Select the **Cable replacement Access point** Mode.

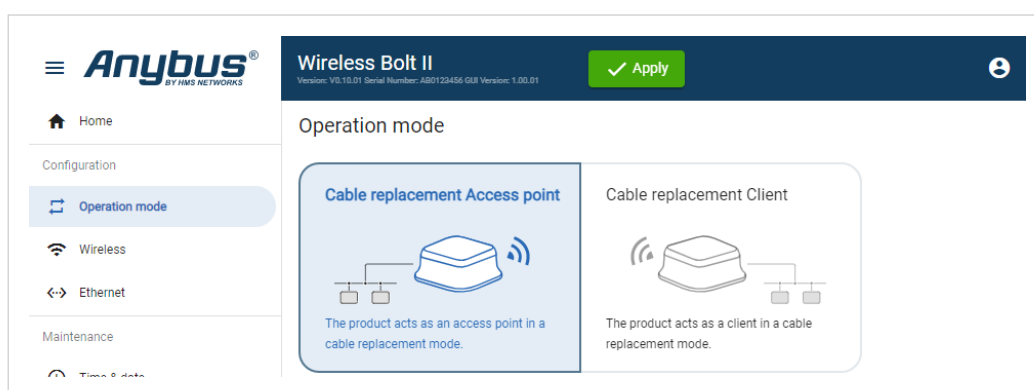


Figure 15. Select Cable replacement Access point

6. Navigate to the **Wireless** settings page.

7. Configure the **Cable replacement Access point** settings.  
See also [Cable Replacement Access Point Settings \(page 32\)](#).

Figure 16. **Cable replacement Access point** settings page

8. Optional step: To use the same settings when configuring the Bolt II Cable replacement Client unit, click **Cable replacement Client** and follow the instructions.  
See also [Export Cable Replacement Access Point Settings \(page 33\)](#).

Figure 17. **Cable replacement Access point** page, export settings

9. To apply the settings, click **Apply** in the built-in web interface header and follow the instructions.  
10. Disconnect the Bolt II from power and your PC.

## Configure the Bolt II Cable Replacement Client

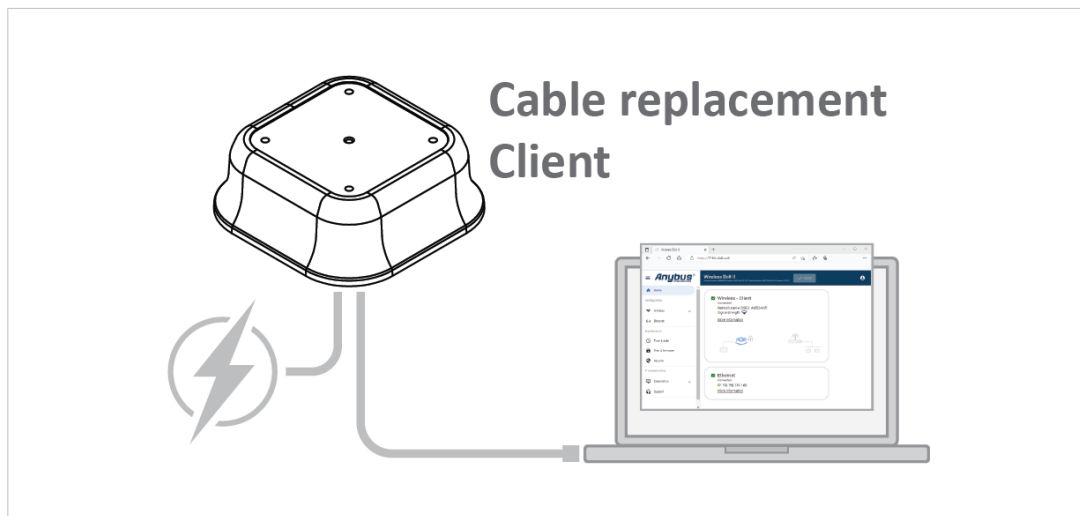


Figure 18. Configure the Bolt II Cable replacement client

1. Connect the Bolt II client to power.
2. Connect the Bolt II client to your PC.
3. Login to the Bolt II client built-in web interface.
4. Navigate to the **Operation mode** page.
5. Select the **Cable replacement Client Mode**.

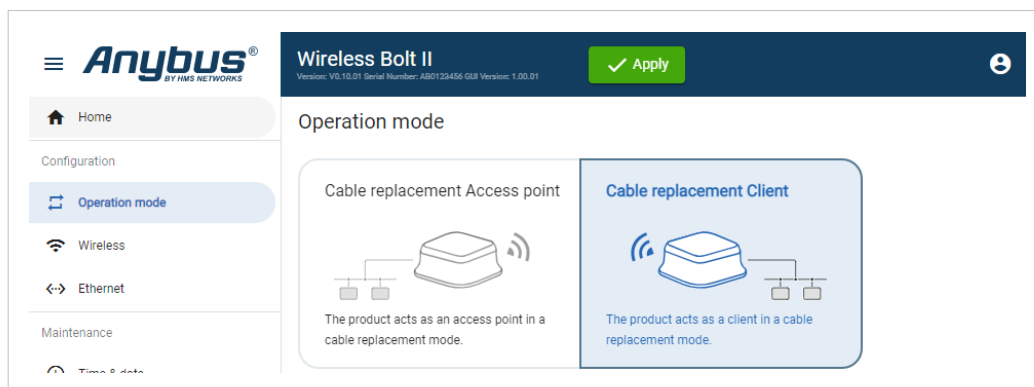


Figure 19. Select Cable replacement Client

6. Navigate to the **Wireless** settings page.

7. Configure the **Cable replacement Client** settings.

- To configure the settings manually, see [Cable Replacement Client Settings \(page 34\)](#).
- Option when you want import the settings used for the Bolt II Cable replacement access point, see [Import Cable Replacement Access Point Settings to Configure Cable Replacement Client \(page 34\)](#).

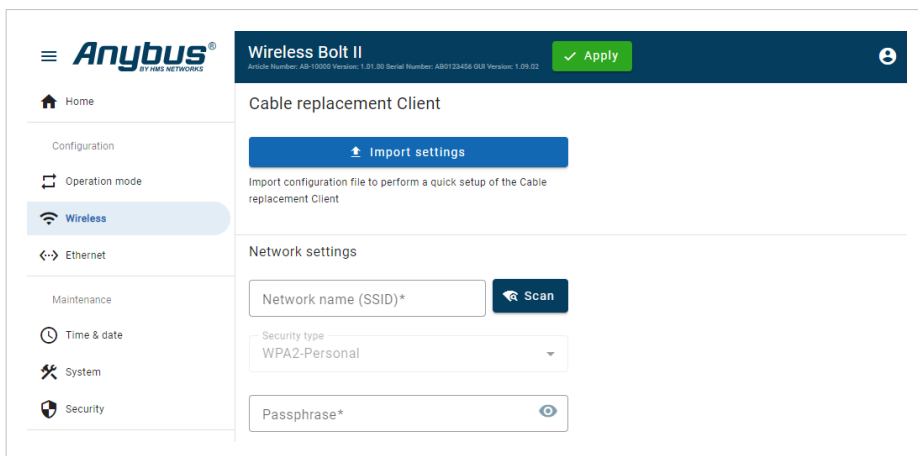


Figure 20. Cable replacement Client page

8. To apply the settings, click **Apply** in the built-in web interface header and follow the instructions.
9. Disconnect the Bolt II from power and your PC.

## Installation

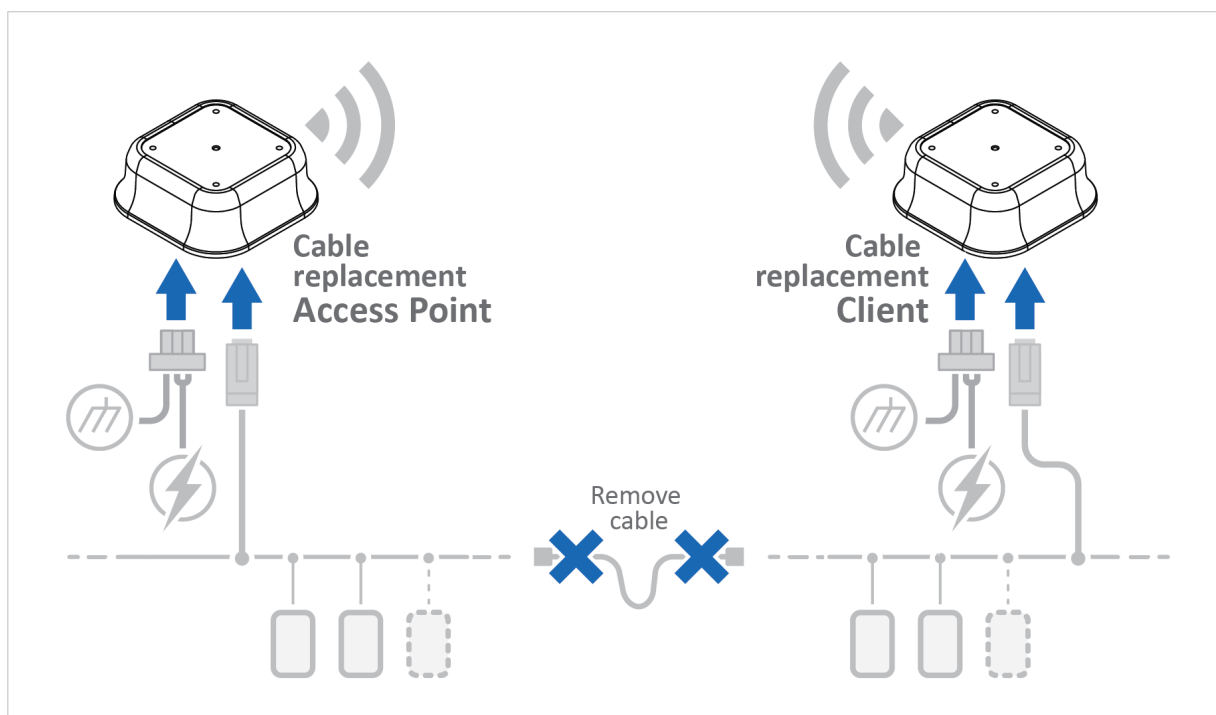


Figure 21. Install the Cable replacement Bolt II Access point and Bolt II client

1. Mount the Bolt II Cable replacement Access point and Bolt II Cable replacement Client.
2. Connect Bolt II Cable replacement Access point and Bolt II Cable replacement Client to power, Functional Earth (FE) and to network.

See [Installation \(page 6\)](#).

## 5.6. Access Point Mode Setup

### Before You Begin

Use the Bolt II as an access point and give other client devices wireless access to an Ethernet device or network.

### Access Point Configuration

#### Procedure

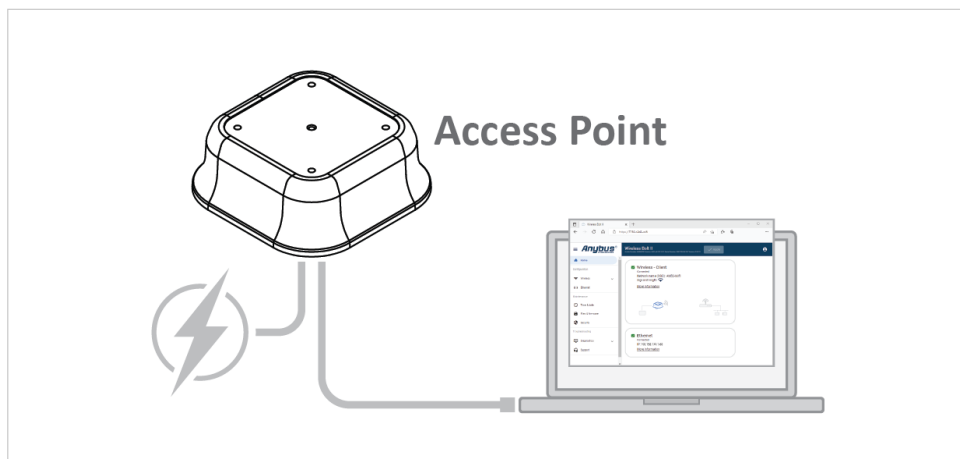


Figure 22. Connect the Bolt II access point to your PC and to power

1. Connect the Bolt II to power.
2. Connect the Bolt II to your PC.
3. Log in to the Bolt II built-in web interface.
4. Navigate to the **Operation mode** page.
5. Select the **Access point** Operation mode.

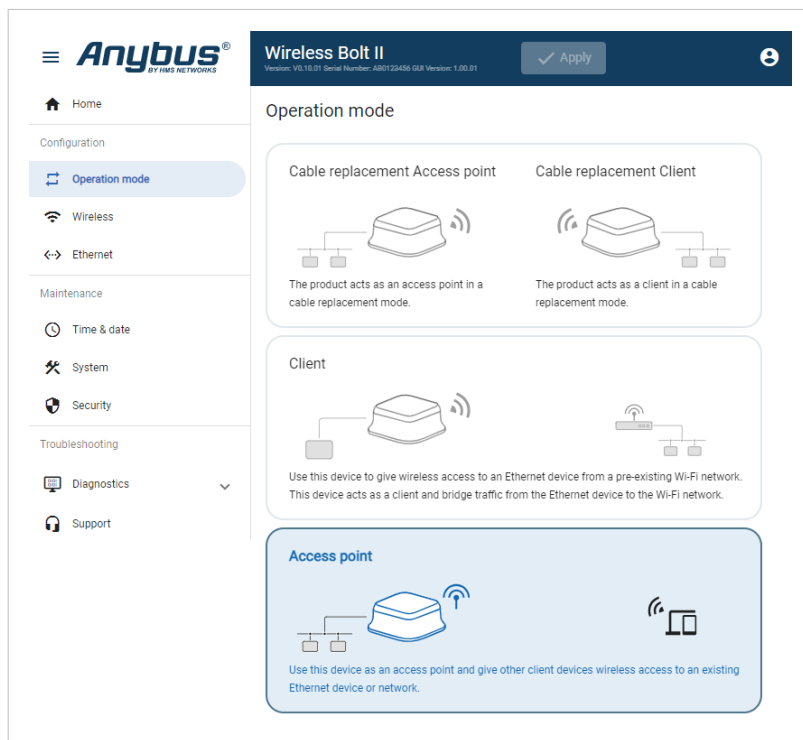


Figure 23. Access point Operation mode

6. Navigate to the **Wireless** settings page.
7. Configure the **Access point** settings.



### IMPORTANT

By default, the Bolt II internal DHCP server is enabled. To avoid interference, keep only one DHCP server enabled on the network.

See [Access Point Settings \(page 36\)](#).

The screenshot shows the 'Wireless Bolt II' web interface. The left sidebar contains navigation links: Home, Configuration, Operation mode, **Wireless** (selected), Ethernet, Maintenance (Time & date, System, Security), Troubleshooting (Diagnostics, Support). The main content area is titled 'Access point' and includes the following fields:

- Network name (SSID): WIFI\_003056500C86
- ☐ Broadcast the network name (SSID)
- Frequency: 2.4 Ghz (selected), 5 Ghz
- Channel: 1
- Security type: WPA2-Personal
- Passphrase: (masked with dots)
- ☐ DHCP server enabled
- Start IP address, End IP address, Subnet mask, Gateway address, Primary DNS, Secondary DNS (all empty)
- Lease time: 0 seconds, Lease interval: 0 seconds

An 'Apply' button is located in the top right corner of the configuration area.

Figure 24. Wireless, **Access point** page

8. To apply the settings, click **Apply** in the built-in web interface header and follow the instructions.
9. Disconnect the Bolt II from power and your PC.

## Installation

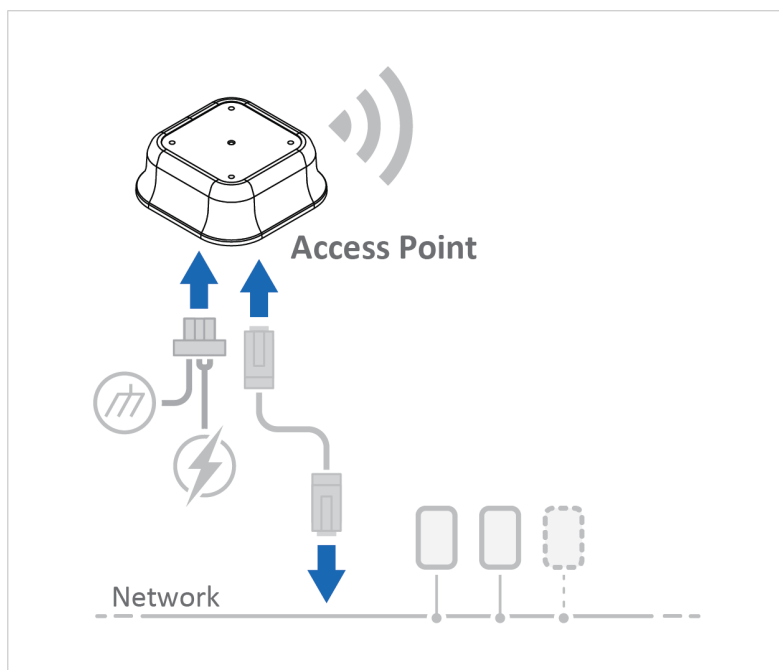


Figure 25. Install the Bolt II access point

1. Mount the Bolt II access point.
2. Connect the Bolt II access point to network, power, and Functional Earth (FE).

See [Installation \(page 6\)](#).

## Connect Wireless Devices

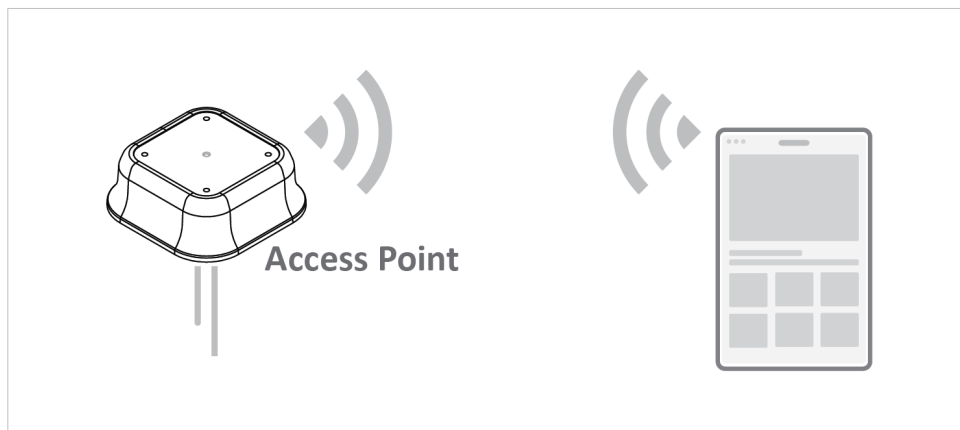


Figure 26. Connect wireless device(s) to Bolt II access point

On each wireless device to be connected to the Bolt II access point:

1. Navigate to the Wi-Fi settings.
2. Enter the Bolt II access point Network name (SSID) and Passphrase.  
If the Network name (SSID) is hidden, enter Security type and Network name (SSID) manually.
3. Option if the wireless device has a built-in web interface: Enter the wireless device IP address in a browser.



## 5.7. Client Mode Setup

### Before You Begin

Use the Bolt II to give Ethernet devices connected to it access to an existing Wi-Fi network.

The Bolt II acts as a client to an access point and bridges traffic from the Ethernet device to the Wi-Fi network.

### Procedure

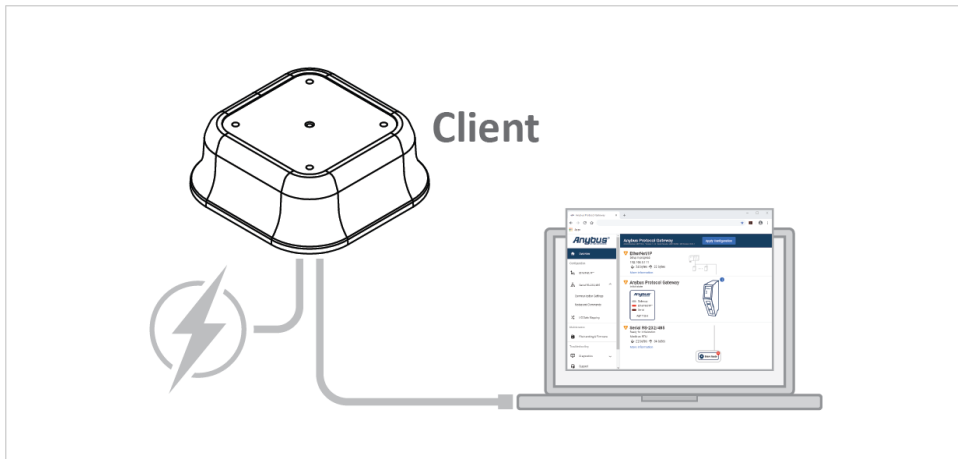


Figure 27. Connect the Bolt II Client to your PC and to power

1. Connect the Bolt II to power.
2. Connect the Bolt II to your PC.
3. Log in to the Bolt II built-in web interface.
4. Navigate to the **Operation mode** page.

5. Select the **Client** Operation mode.

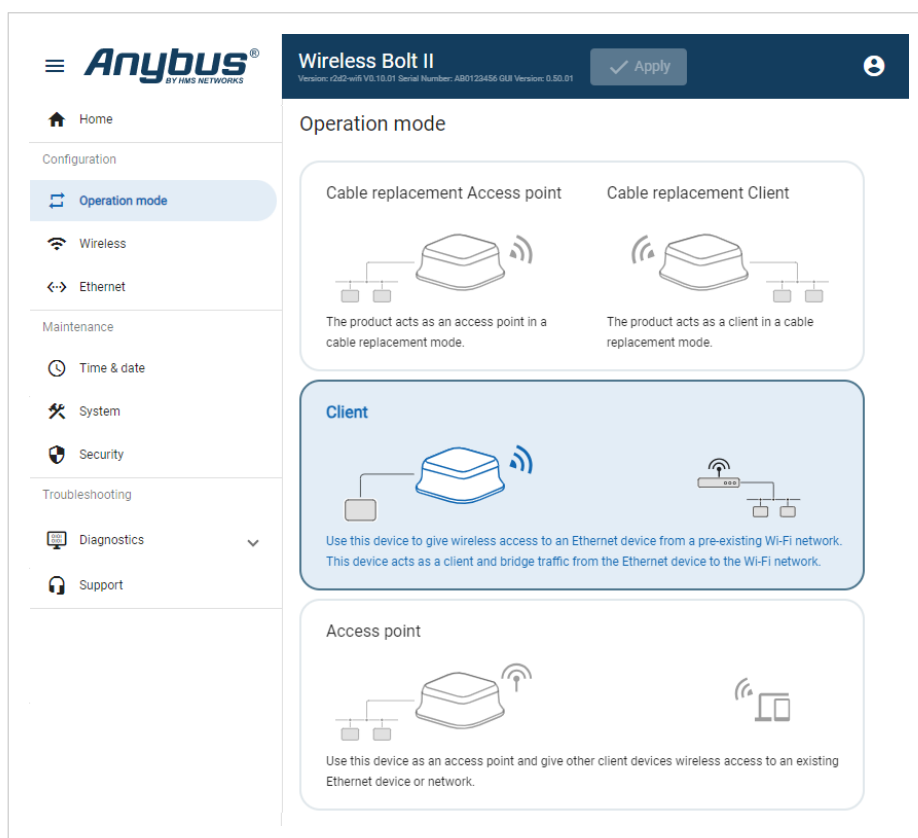


Figure 28. Client Operation mode

- Navigate to the **Wireless** settings page and configure the **Client** settings for network security and roaming and choose what **Forwarding mode** to use, **MAC clone (MAC Address Cloning)** or **NAT (Network Address Translation)**.  
See [Client Security Settings \(page 43\)](#) and [Client Forwarding Modes \(page 38\)](#).
- When NAT (Network Address Translation) is used: Navigate to the **Ethernet** settings page and configure the IP settings required by the wired network.  
See [Ethernet Settings \(page 49\)](#).

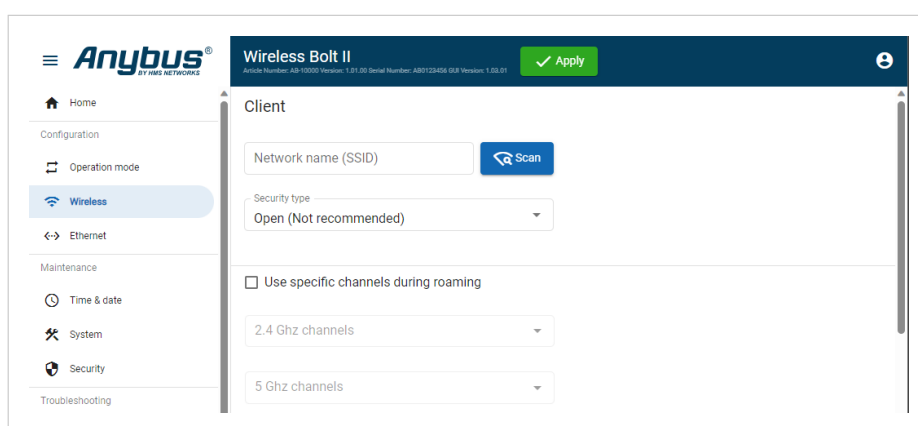


Figure 29. Client page

- To apply the settings, click **Apply** in the built-in web interface header and follow the instructions.
- Disconnect the Bolt II from power and your PC.

## Installation

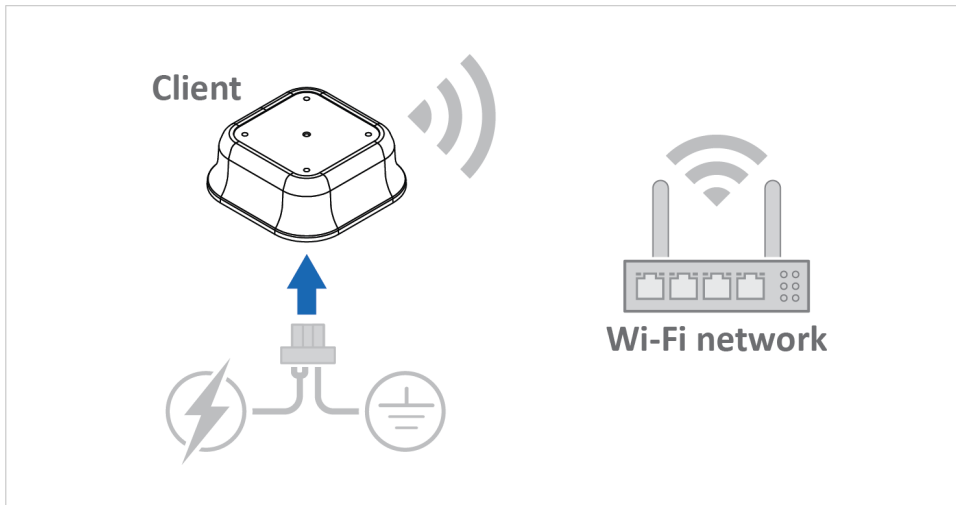


Figure 30. Install the Bolt II Client

1. Mount the Bolt II Client.
2. Connect the Bolt II Client to power and Functional Earth (FE).

See [Installation \(page 6\)](#).

## Connect Ethernet Device

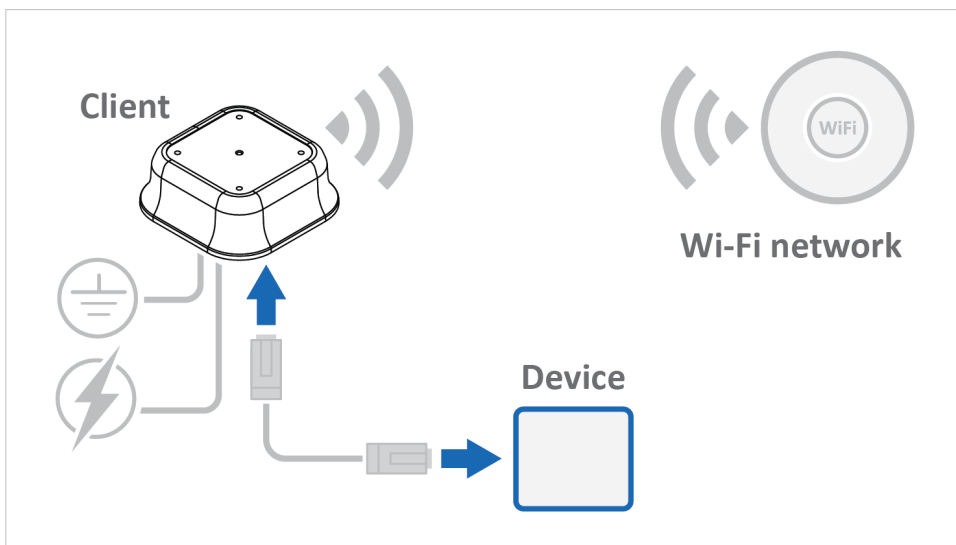


Figure 31. Connect the Ethernet Device to the Bolt II Client

1. Connect an Ethernet cable between the Bolt II client and the Ethernet device to be connected to the Wi-Fi network.
2. Verify that the wired device is connected to the Wi-Fi network.

## 5.8. Wireless Settings

### 5.8.1. I/O-Data Cycle Time Considerations

I/O data cycle time is valid for the Bolt II Cable replacement mode.

For PROFINET and EtherNet/IP networks, use a minimum I/O data cycle time of 64 ms and 3 retries.

### 5.8.2. Cable Replacement Access Point Settings

Ensure that **Cable replacement Access point** is selected on the **Operation mode** page.

On the **Wireless** settings page, configure the settings for the Bolt II **Cable replacement Access point**.

The screenshot shows the 'Wireless Bolt II' configuration interface. The left sidebar contains navigation links: Home, Configuration, Operation mode, Wireless (selected), Ethernet, Maintenance, Time & date, System, Security, Troubleshooting, Diagnostics, and Support. The main content area is titled 'Cable replacement Access point' and includes an 'Apply' button. The settings are as follows:

- Network name (SSID) \***: WIFI\_003056500C86
- Broadcast the network name (SSID)**: ☐
- Radio frequency band**: 2.4 Ghz (selected), 5 Ghz
- Channel**: 11
- Security type**: WPA2-Personal
- Passphrase \***: [masked]
- Export settings for Cable replacement Client**: [button]

Figure 32. Cable replacement Access point page


### Access Point Security Settings

Setting	Value	Description
Network name (SSID)	Default, Anybus_<dynamic> <dynamic> is the last four digits of the Bolt II MAC address. Example: Anybus_a053	Name the Bolt II access point with a unique SSID (Service Set Identifier).
Radio frequency band	2.4 Ghz, Default 5 Ghz	Select the radio frequency band to be used, <b>2.4 Ghz</b> or <b>5 Ghz</b> . See also <a href="#">WLAN Channels and World Mode</a> .
Broadcast the network name (SSID)	Broadcast the network name (SSID) is enabled by default.	By default, SSID broadcast is enabled. When users try to connect their wireless devices, the name of the Bolt II access point appears in the list of available networks. To disable SSID broadcast, deselect the <b>Broadcast the network name (SSID)</b> checkbox.
Channel	Auto, Default 2.4 GHz channels: 1 to 11 5 GHz channels: 36, 40, 44, 48, 149, 153, 157, 161 and 165	Select a <b>Channel</b> for the radio frequency band. See also <a href="#">WLAN Channels and World Mode</a> .
Security type	Open (Not recommended) WPA2-Personal, Default WPA3-Personal	Select a <b>Security type</b> for the wireless connection.



#### NOTE

For **Cable Replacement Access point** the Security type is locked to WPA2-Personal.

Setting	Value	Description
Passphrase	Default Passphrase: hms-anybus	Enter the <b>Passphrase</b> , password, for the selected <b>Security type</b> .  <div>  <b>NOTE</b>            For Security type WPA2 (Wi-Fi Protected Access 2), the <b>Passphrase</b> must be a minimum of eight characters in length.         </div>

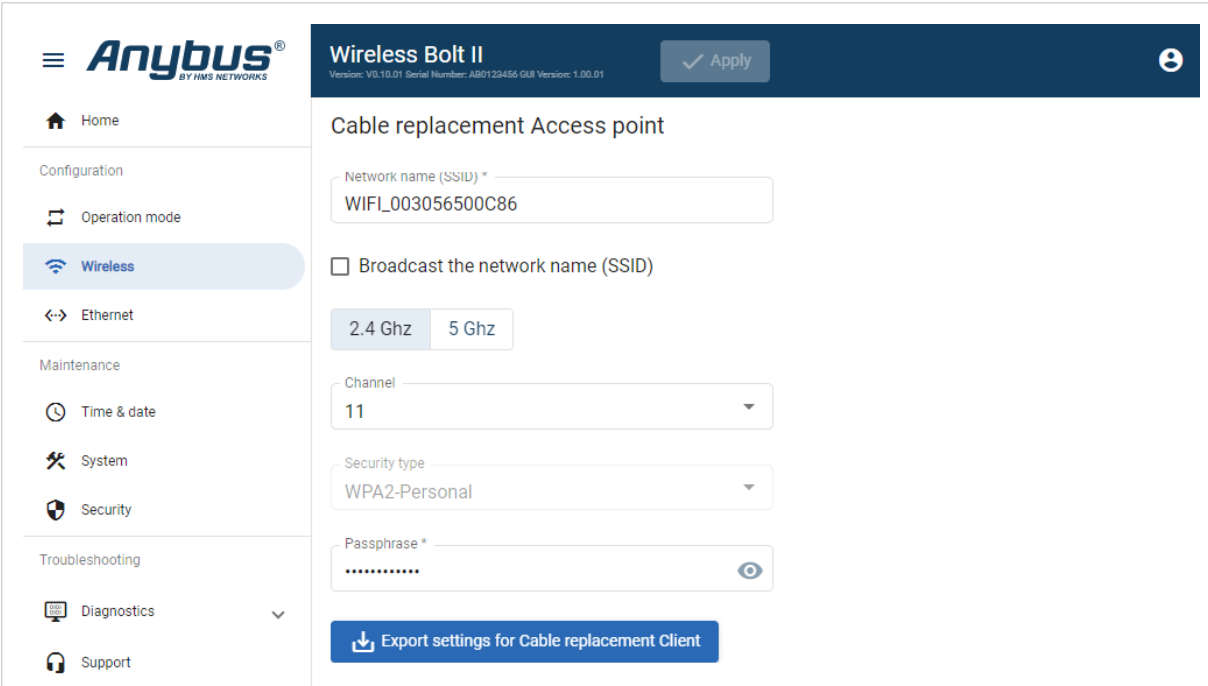
## Export Cable Replacement Access Point Settings

### Before You Begin

You can export the current **Cable replacement Access point** access point settings, in order to use when configuring the **Cable replacement Client** client.

The settings saved in the configuration file are compatible with the available **Cable replacement Client** settings.

### Procedure



The screenshot displays the 'Wireless Bolt II' web interface. The left sidebar contains navigation links: Home, Configuration, Operation mode, **Wireless**, Ethernet, Maintenance, and Troubleshooting. The main panel is titled 'Cable replacement Access point'. It features several configuration fields: 'Network name (SSID) \*' with the value 'WIFI\_003056500C86', a checkbox for 'Broadcast the network name (SSID)', frequency selection buttons for '2.4 Ghz' and '5 Ghz', a 'Channel' dropdown set to '11', a 'Security type' dropdown set to 'WPA2-Personal', and a 'Passphrase \*' field masked with dots. An 'Apply' button is in the top right. At the bottom, there is a blue button labeled 'Export settings for Cable replacement Client'.

Figure 33. **Cable replacement Access point** page, export settings

1. To export a configuration file, click **Export settings for Cable replacement Client**.
2. The configuration settings are stored in a .devb file and downloaded to your PC.

### To Do Next

Import the .devb file to configure the **Cable replacement Client** settings.

See [Cable Replacement Client Settings \(page 34\)](#).


### 5.8.3. Cable Replacement Client Settings

Ensure that **Cable replacement Client** is selected on the **Operation mode** page.

On the **Wireless** settings page, configure the settings for the Bolt II **Cable replacement Client**.

Figure 34. **Cable replacement Client** page

#### Client Security Type Settings

Setting	Value	Description
Network name (SSID)	No default Network name (SSID) is used.	Name the Bolt II with a unique Network name (SSID) (Service Set Identifier).
Security type	WPA2-Personal	The Security type for the wireless connection is locked to WPA2-Personal.
Passphrase	No default Passphrase is used.	Enter the <b>Passphrase</b> , password, for the selected security type.
<div>  <b>NOTE</b>            For Security type WPA2 (Wi-Fi Protected Access 2), the <b>Passphrase</b> must be a minimum of eight characters in length.         </div>		

#### Import Cable Replacement Access Point Settings to Configure Cable Replacement Client

##### Before You Begin

You can import the current settings used for the **Cable Replacement Access point** access point and use the same settings for the **Cable replacement Client** Bolt II client.

## Procedure

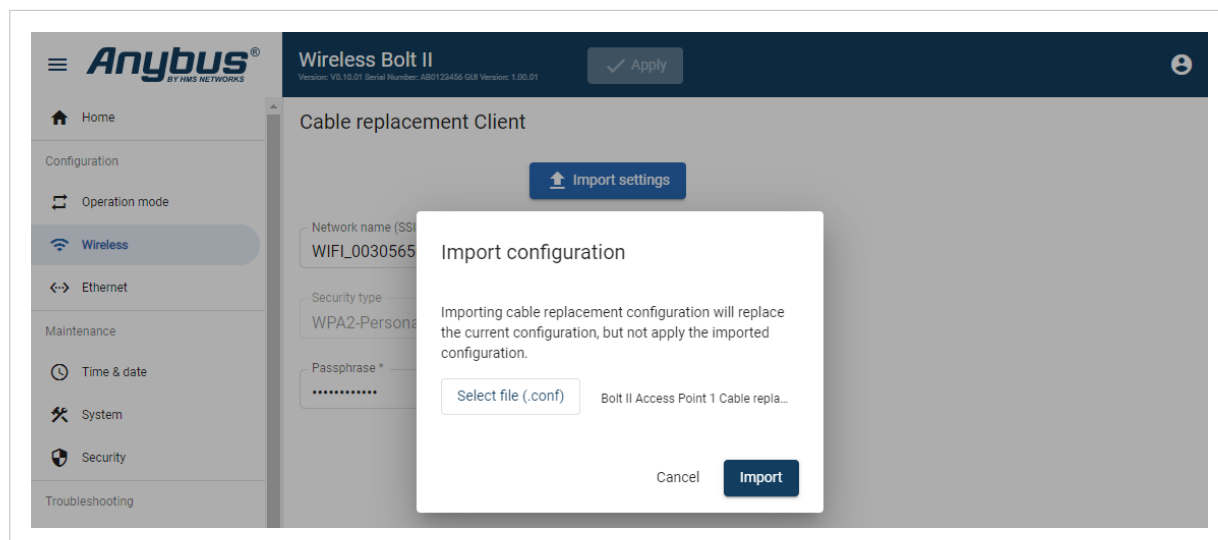


Figure 35. **Cable replacement Client**, Import settings

1. Ensure that you have exported the **Cable replacement Access point** settings in a configuration file, (.devb). See [Export Cable Replacement Access Point Settings \(page 33\)](#).
2. To import the configuration file, click **Import settings** > **Select file (.devb)**.
3. In the **Open** dialog box, browse to and select the configuration file (.devb) and click **Open** > **Import**. The **Cable replacement Access point** settings are imported.
4. To apply the settings, click **Apply** in the built-in web interface header and follow the instructions.

### 5.8.4. Access Point Settings



Ensure that **Access point** is selected on the **Operation mode** page.

On the **Wireless** page, configure the **Access point** settings for the Bolt II access point.

The screenshot shows the 'Wireless Bolt II' configuration interface. On the left is a navigation menu with options: Home, Configuration, Operation mode, Wireless (selected), Ethernet, Maintenance, Time & date, System, Security, Troubleshooting, Diagnostics, and Support. The main content area is titled 'Access point'. It includes a text field for 'Network name (SSID) \*' with the value 'WIFI\_003056500C86'. Below it is a checkbox for 'Broadcast the network name (SSID)'. There are two buttons for '2.4 Ghz' and '5 Ghz' radio frequency bands. A 'Channel' dropdown menu is set to '1'. The 'Security type' dropdown menu is set to 'WPA2-Personal'. A 'Passphrase \*' field is masked with dots. At the bottom, there is a checkbox for 'DHCP server enabled'. Below this checkbox are several input fields: 'Start IP address', 'End IP address', 'Lease time' (0 seconds), 'Lease interval' (0 seconds), 'Subnet mask', 'Gateway address', 'Primary DNS', and 'Secondary DNS'. An 'Apply' button is located at the top right of the configuration area.

Figure 36. Access point page

#### Access Point Security Settings

Setting	Value	Description
Network name (SSID)	Default, Anybus_<dynamic> <dynamic> is the last four digits of the Bolt II MAC address. Example: Anybus_a053	Name the Bolt II access point with a unique SSID (Service Set Identifier).
Radio frequency band	2.4 Ghz, Default 5 Ghz	Select the radio frequency band to be used, <b>2.4 Ghz</b> or <b>5 Ghz</b> . See also <a href="#">WLAN Channels and World Mode</a> .
Broadcast the network name (SSID)	Broadcast the network name (SSID) is enabled by default.	By default, SSID broadcast is enabled. When users try to connect their wireless devices, the name of the Bolt II access point appears in the list of available networks. To disable SSID broadcast, deselect the <b>Broadcast the network name (SSID)</b> checkbox.
Channel	Auto, Default 2.4 GHz channels: 1 to 11 5 GHz channels: 36, 40, 44, 48, 149, 153, 157, 161 and 165	Select a <b>Channel</b> for the radio frequency band. See also <a href="#">WLAN Channels and World Mode</a> .
Security type	Open (Not recommended) WPA2-Personal, Default WPA3-Personal	Select a <b>Security type</b> for the wireless connection.   <b>NOTE</b> For <b>Cable Replacement Access point</b> the Security type is locked to WPA2-Personal.
Passphrase	Default Passphrase: hms-anybus	Enter the <b>Passphrase</b> , password, for the selected <b>Security type</b> .   <b>NOTE</b> For Security type WPA2 (Wi-Fi Protected Access 2), the <b>Passphrase</b> must be a minimum of eight characters in length.



### Access Point DHCP Settings

By default, DHCP server is enabled. The Bolt II acts as a DHCP server and provides the IP settings to the client devices connected to it.



#### IMPORTANT

By default, the Bolt II internal DHCP server is enabled. To avoid interference, keep only one DHCP server enabled on the network.

To disable DHCP server, deselect the **DHCP server enabled** checkbox.

Setting	Description
Start IP address	Enter the first IP address of the DHCP address pool. Write in IPv4 dot-decimal notation.
End IP address	Enter the last IP address of the DHCP address pool. Write in IPv4 dot-decimal notation.
Lease time	Set the length of time the clients can use an IP address assigned by the DHCP server. Minimum: 5 minutes, 300 seconds Maximum: 14 days, 1209600 seconds Default: 24 hours, 86400 seconds
Lease interval	Set the length of time the DHCP server writes the lease information to the dhcp.leases file. Minimum: 1 minutes, 60 seconds Maximum: 12 hours, 43200 seconds Default: 2 hours, 7200 seconds
Subnet mask	The Bolt II network Subnet mask in IPv4 dot-decimal notation.
Gateway address	The Bolt II network Gateway address in IPv4 dot-decimal notation. If there is no gateway available, set the Gateway address to: 0.0.0.0
Primary DNS	Enter the network Primary DNS for the DHCP address pool. Write in IPv4 dot-decimal notation.
Secondary DNS	Enter the network Secondary DNS for the DHCP address pool. Write in IPv4 dot-decimal notation.

### 5.8.5. Client Forwarding Modes

When the Bolt II Client mode is enabled, there are two **Forwarding mode** types available: **MAC clone (MAC Address Cloning)** and **NAT (Network Address Translation)**.

The screenshot displays the 'Wireless Bolt II' configuration page. The left sidebar contains navigation links: Home, Configuration (Operation mode, **Wireless**, Ethernet), Maintenance (Time & date, System, Security), and Troubleshooting (Diagnostics, Support). The main content area is titled 'Client' and includes a green 'Apply' button. The 'Network name (SSID)' field has a 'Scan' button. The 'Security type' is set to 'Open (Not recommended)'. Under 'Channels used when roaming', the '2.4 Ghz channels' are set to '1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11' and the '5 Ghz channels' are set to '36, 40, 44, 48, 149, 153, 157, 161, 165'. The 'Forwarding mode' section shows two options: 'NAT (Network Address Translation)' and 'MAC clone (MAC Address Cloning)'. The 'MAC clone' option is highlighted with a blue border and contains the text: 'Enables the Wireless Bolt II to mimic the MAC address of another device on the network.' Below this, a message states: 'There are currently no settings for Network Address Translation (NAT).'

Figure 37. Wireless, Forwarding mode

By default, **MAC clone (MAC Address Cloning)** is enabled.

See also [About Client MAC Clone \(MAC Address Cloning\) \(page 39\)](#) and [Client MAC Clone \(MAC Address Cloning\) Settings \(page 44\)](#).

To enable NAT, click **NAT (Network Address Translation)**.

See also [About NAT \(Network Address Translation\) \(page 42\)](#) and [Client NAT \(Network Address Translation\) Settings \(page 47\)](#).

### About Client MAC Clone (MAC Address Cloning)

The **MAC clone (MAC Address Cloning)** feature allows a single Layer 2 dependent device to be connected to a Wi-Fi network with little to no reconfiguration of the underlying system.

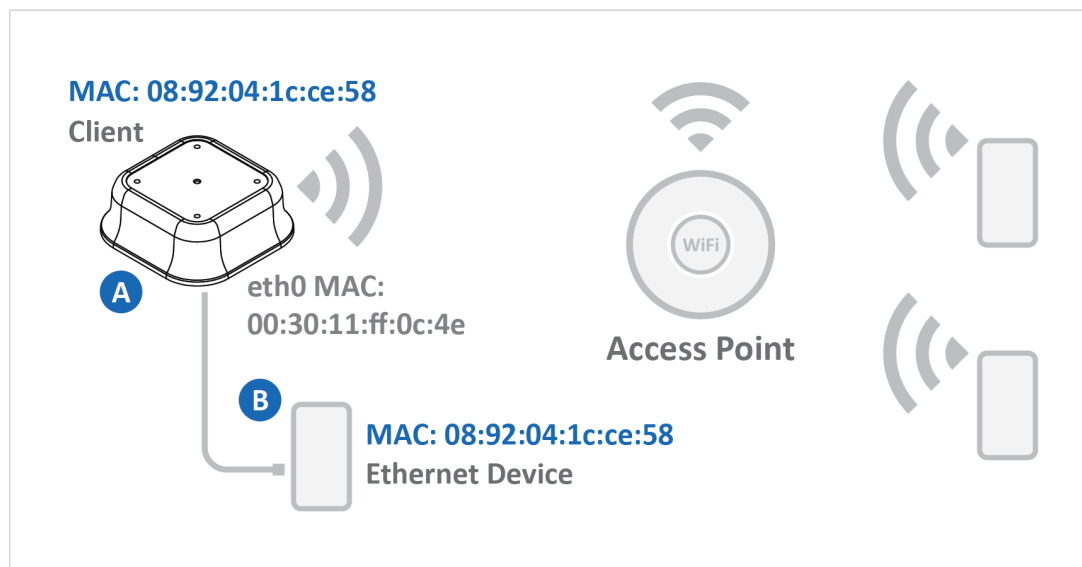
The MAC clone feature is compatible with any brand of access points.

#### Example 1. Cloned MAC address of an Ethernet device connected to a Bolt II Client

To bridge traffic between an Ethernet device, without Wi-Fi access, and other devices connected to the Wi-Fi access point, the Ethernet device is connected to the Bolt II with an Ethernet cable.

When **MAC clone (MAC Address Cloning)** is enabled, the Bolt II clones the MAC address of the connected Ethernet device and assigns it to its own Wi-Fi interface.

The Wi-Fi access point perceives the Bolt II and the Ethernet device to be one single device.



This example shows a Bolt II Client (A) with the cloned MAC address 08:92:04:1c:ce:58 of the connected Ethernet device (B).

The eth0 MAC address 00:30:11:ff:0c:4e is the MAC address of the Bolt II Client Ethernet interface.

Figure 38. Ethernet device connected to a Bolt II Client

### MAC Address Filtering

The Bolt II forwards incoming packets between its Ethernet interface and its Wi-Fi interface.

Traffic to/from the cloned MAC address is forwarded, while traffic from other connected devices is ignored.

Packets destined for the Bolt II Ethernet interface are not forwarded.

The Bolt II built-in web interface remains accessible from the Ethernet side.

### IP Clone Address

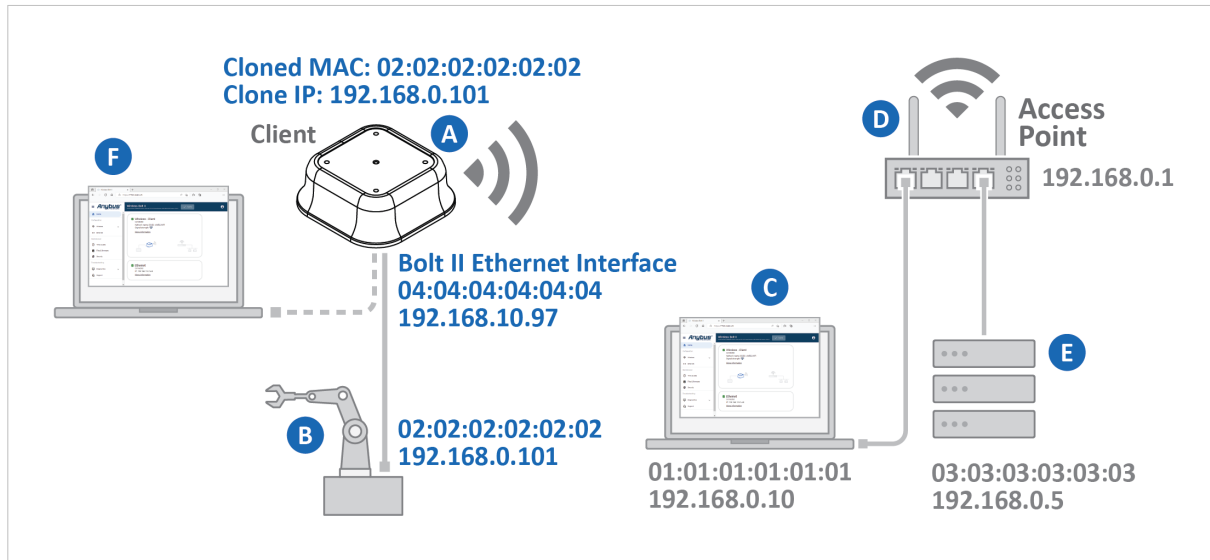
- The IP address is needed to inform the devices on the network where to route the packets after they have roamed and switched access point.
- The technique used is Gratuitous Address Resolution Protocol (GARP).

- The GARP communication protocol detects the IP address associated with the MAC address of a device. It is used to detect duplicate IP addresses.

### About MAC Clone Capture Port

When MAC clone (MAC Address Cloning) is used, the Capture port feature is used to access to the Bolt II Client built-in web interface via Wi-Fi connection.

#### Example 2. Bolt II Client capture port and subnetwork setup



For the Capture port feature and the routing to work, the cloned IP address and the main IP address of the Bolt II must have different subnetwork. This way, the Bolt II built-in web interface can still be accessed via the Ethernet port in case the Wi-Fi connection becomes unavailable.

In this example:

A robot (B) is connected to a Bolt II Client (A) with an Ethernet cable.

The Bolt II Client (A) have the cloned MAC address 02:02:02:02:02:02 and IP address 192.168.0.101 of the connected robot (B).

The Bolt II Client Ethernet interface have the MAC address 04:04:04:04:04:04 and IP address 192.168.10.97.

A laptop (C) and the Bolt II Client is connected to a Wi-Fi access point (D).

When the MAC clone capture port feature is enabled, the laptop (C) can still access the Bolt II Client (A) Ethernet interface and the built-in web interface via the Wi-Fi connection.

A laptop (F) can be connected to the Bolt II via the Ethernet port to access the Bolt II built-in web interface if the Wi-Fi connection is not available.

Figure 39. A Bolt II Client (A) connected to a robot (B), Ethernet device

## About NAT (Network Address Translation)



### NOTE

NAT (Network Address Translation) does not forward Layer 2 traffic. When using network protocols that depend on layer 2, use the MAC clone mode. See [Client Forwarding Modes \(page 38\)](#).

NAT (Network Address Translation) mode is available when the Bolt II Client mode is enabled.

NAT must be used when there is more than one device connected to the Bolt II Ethernet port, via a switch or hub.

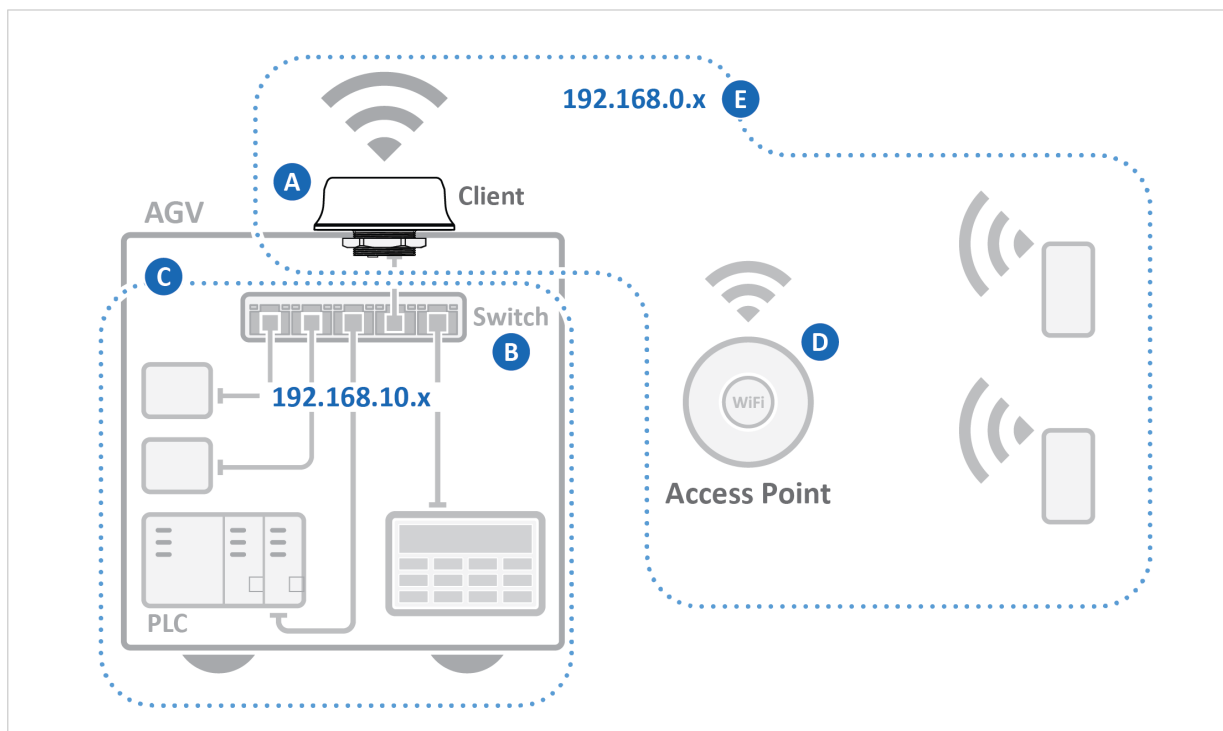
When NAT is enabled the Bolt II act as a DHCP client on the wireless network interface.

The IP address for each device connected to the Bolt II Ethernet port is mapped to the Bolt II IP address.

The Bolt II IP address represent the entire group of devices on the industrial network.

The devices can be accessed via the Wi-Fi network by forwarding specific ports on the Bolt II to selected IP addresses on the wired subnet.

Example 3. Bolt II Client with multiple devices connected to it




This example shows a Bolt II Client (A) mounted on an AGV (Automated guided vehicle). There are multiple devices connected to the Bolt II via a switch (B). The Bolt II with its connected devices forms a subnetwork (C) and the Access Point (D) with its connected devices forms another subnetwork (E) within the industrial network.

## 5.8.6. Client Security Settings

The screenshot shows the 'Client' configuration page for the Anybus Wireless Bolt II. The sidebar on the left contains navigation links: Home, Configuration, Operation mode, Wireless (highlighted), Ethernet, Maintenance, Time & date, System, Security, and Troubleshooting. The main content area has a title bar with 'Wireless Bolt II' and an 'Apply' button. Below the title bar, the 'Client' section includes a 'Network name (SSID)' input field with a 'Scan' button, a 'Security type' dropdown menu set to 'Open (Not recommended)', and a checkbox for 'Use specific channels during roaming'. Below this are two dropdown menus for '2.4 Ghz channels' and '5 Ghz channels'.

Figure 40. Client page, network security settings

Setting	Value	Description
Security type	Open (Not recommended) WPA2-Personal WPA2-Enterprise WPA2-Enterprise TLS WPA3-Personal WPA3-Enterprise WPA3-Enterprise TLS	Select a <b>Security type</b> for the wireless connection.
Identity	No default Identity is used.	Option for Security type WPA2 Enterprise and WPA3 Enterprise. Enter the <b>Identity</b> , for the selected <b>Security type</b> .
Passphrase	No default Passphrase is used.	Enter the <b>Passphrase</b> , password, for the selected <b>Security type</b> .
Use specific channels during roaming	By default, all channels are used during roaming.	To enable the use of specific channels, select the <b>Use specific channels during roaming</b> checkbox. Select the preferred channels to use during roaming. You can choose to scan only the 2.4 GHz or 5 GHz channel band, or both.  <div>  <b>TIP</b>            To optimize the scanning time, select only the channels to be used by your access point.         </div> <ul style="list-style-type: none"> <li>2.4 Ghz channels: 1 to 11</li> <li>5 Ghz channels: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165</li> </ul>

### 5.8.7. Client MAC Clone (MAC Address Cloning) Settings

For information about MAC clone (MAC Address Cloning), see [About Client MAC Clone \(MAC Address Cloning\) \(page 39\)](#).

#### Option 1 - Automatic MAC Address Configuration

Automatic MAC address detection is performed once at each boot as the Bolt II listens for incoming packets on the Bolt II Ethernet interface.

#### Procedure

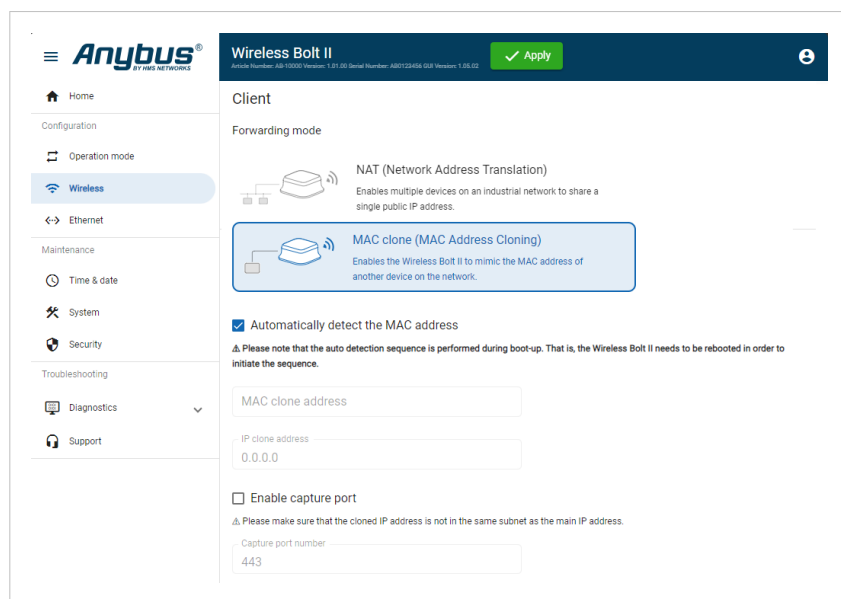


Figure 41. Wireless, Client page, **Automatically detect the MAC address** enabled

1. Ensure that the Bolt II Client operation mode is enabled.
2. To enable MAC cloning, click **MAC clone (MAC Address Cloning)**.
3. To enable automatic MAC address detection, select the **Automatically detect the MAC address** checkbox.
4. In the Bolt II built-in web-interface header, click **Apply**.
5. If the Bolt II is configured via a PC device connected to it via the Bolt II Ethernet port:  
Disconnect the PC device from the Bolt II Ethernet port.

#### To Do Next



#### IMPORTANT

At the next power up, ensure that the device with the MAC address to be cloned is the only device connected to the Bolt II Ethernet port.

Install the Bolt II. See [Installation \(page 6\)](#).

#### Result

The auto detection sequence is performed during boot-up.

The MAC address of the device connected to the Bolt II via an Ethernet cable is automatically detected and cloned by the Bolt II.

The IP address associated with the MAC clone address is automatically detected and cloned by the Bolt II.



## Option 2 - Static MAC Address Configuration Procedure

The screenshot shows the Anybus Wireless Bolt II web interface. The left sidebar has a menu with 'Home', 'Configuration', 'Maintenance', and 'Troubleshooting'. Under 'Configuration', 'Wireless' is selected. Under 'Maintenance', 'Time & date', 'System', and 'Security' are listed. Under 'Troubleshooting', 'Diagnostics' and 'Support' are listed. The main content area is titled 'Wireless Bolt II' and 'Client'. It shows 'Forwarding mode' with two options: 'NAT (Network Address Translation)' and 'MAC clone (MAC Address Cloning)'. The 'MAC clone (MAC Address Cloning)' option is highlighted with a blue border. Below it, the 'Automatically detect the MAC address' checkbox is unchecked. The 'MAC clone address' field is empty. The 'IP clone address' field contains '0.0.0.0'. The 'Enable capture port' checkbox is unchecked. The 'Capture port number' field contains '443'.

Figure 42. Wireless, Client page, **Automatically detect the MAC address** disabled

1. Ensure that the Bolt II Client operation mode is enabled.
2. To enable MAC cloning, click **MAC clone (MAC Address Cloning)**.
3. Deselect the **Automatically detect the MAC address** checkbox.
4. In the **MAC clone address** field, enter the MAC (Media Access Control) address of the device connected to the Bolt II via an Ethernet cable.



### NOTE

Write the MAC (Media Access Control) address with 12 hexadecimal digits, grouped in pairs and separated by colons.

Example: 00:1e:62:84:45:e7

5. In the **IP clone address** field, enter the IP address associated with the **MAC clone address**.
6. In the Bolt II built-in web-interface header, click **Apply**.

## Capture Port

When MAC clone is used, the Capture port feature is used to access the Bolt II Client built-in web via Wi-Fi connection.



### IMPORTANT

To access the Bolt II Client built-in web interface via a Wi-Fi connection when the **MAC clone** setting is enabled, ensure that the capture port setting is also enabled.

To access the Bolt II Client built-in web interface from a PC connected to it with an Ethernet cable always works.



### IMPORTANT

For the Capture port feature and the routing to work, the cloned IP address and the main IP address of the Bolt II must have different subnetwork. This way, the Bolt II built-in web interface can still be accessed via the Ethernet port in case the Wi-Fi connection becomes unavailable.

Make sure that the Bolt II Client and the device connected to it, with an Ethernet cable, have separate subnetworks.

See also [About MAC Clone Capture Port \(page 41\)](#).

## Procedure

The screenshot shows the 'Wireless Bolt II' web interface. The left sidebar contains navigation links: Home, Configuration, Operation mode, Wireless (selected), Ethernet, Maintenance, Time & date, System, Security, Troubleshooting, Diagnostics, and Support. The main content area is titled 'Client' and shows 'Forwarding mode' with two options: 'NAT (Network Address Translation)' and 'MAC clone (MAC Address Cloning)'. The 'MAC clone' option is selected and highlighted with a blue box. Below this, there is a checkbox for 'Automatically detect the MAC address' which is unchecked. A note states: 'Please note that the auto detection sequence is performed during boot-up. That is, the Wireless Bolt II needs to be rebooted in order to initiate the sequence.' Below this are input fields for 'MAC clone address \*', 'IP clone address \*' (with the value '0.0.0.0'), and 'Capture port number \*' (with the value '443'). The 'Enable capture port' checkbox is checked. A final note states: 'Please make sure that the cloned IP address is not in the same subnet as the main IP address.' An 'Apply' button is visible in the top right corner of the main content area.

Figure 43. Wireless, Client page, Capture port enabled

1. To enable capture port, select the **Enable capture port** checkbox.
2. In the **Capture port number** field, enter the number of the port that you want to use to access the Bolt II Client built-in web interface.

### 5.8.8. Client NAT (Network Address Translation) Settings

For information about NAT (Network Address Translation), see [About NAT \(Network Address Translation\)](#) (page 42).

**NOTE**

NAT (Network Address Translation) does not forward Layer 2 traffic. When using network protocols that depend on layer 2, use the MAC clone mode. See [Client Forwarding Modes](#) (page 38).

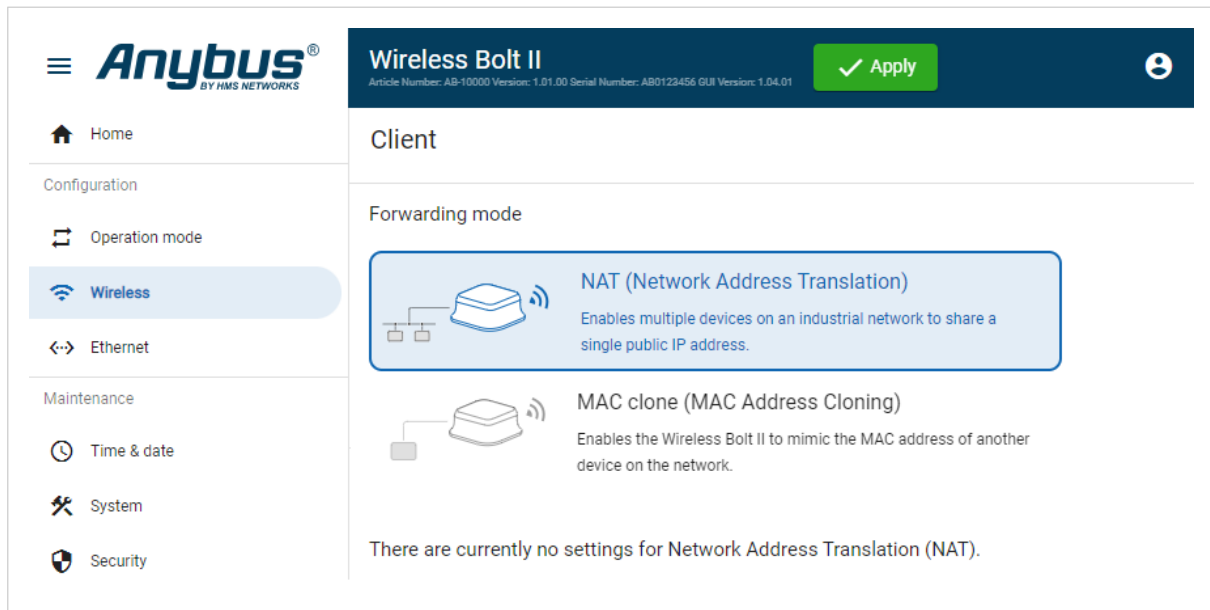
**Procedure**

Figure 44. Wireless, Client page, **NAT (Network Address Translation)** enabled

1. Ensure that the Bolt II Client operation mode is enabled.
2. To enable NAT, click **NAT (Network Address Translation)**.

**Result**

When NAT (Network Address Translation) is enabled the Bolt II act as a DHCP client on the wireless network interface.

Devices connected to the Bolt II can access the Wi-Fi network through the Bolt II IP address.

## Client Port Forwarding

Option for NAT (Network Address Translation).

Client **Port forwarding** allows the radio interface (WAN side) to access L3 devices connected to the Bolt II Ethernet interface (LAN side).

## Procedure

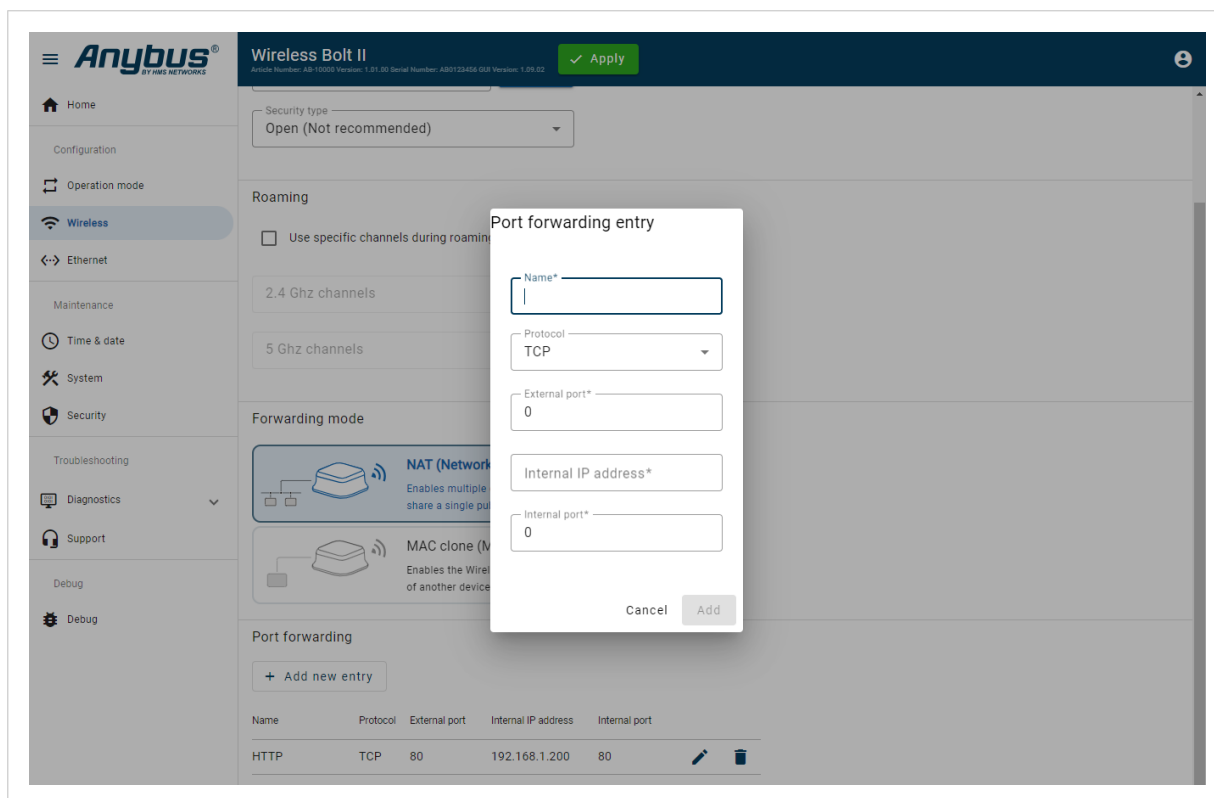


Figure 45. Port forwarding entry

1. Click **NAT (Network Address Translation)**.
2. To add a new port forwarding rule, click **Add new entry**.
3. Enter a rule **Name**.
4. Select a **Protocol**, **TCP** or **UDP**.
5. Enter the **External port**, ranging from 1 to 65535, through which incoming traffic should reach the internal network.
6. Enter the **Internal IP address** to to which incoming traffic should be forwarded.
7. Enter the **Internal port**, ranging from 1 to 65535, on the device receiving incoming traffic.

## 5.9. Ethernet Settings

### 5.9.1. To Configure IP Settings Manually

The screenshot shows the 'Wireless Bolt II' web interface. The left sidebar contains navigation links: Home, Configuration, Operation mode, Wireless, Ethernet (selected), Maintenance, and Time & date. The main content area is titled 'Ethernet' and shows 'IP Settings'. A checkbox for 'DHCP client enabled' is unchecked. Below this, five input fields are shown: 'IP address \*' (192.168.1.50), 'Subnet mask \*' (255.255.255.0), 'Gateway address \*' (0.0.0.0), 'Primary DNS' (8.8.8.8), and 'Secondary DNS' (8.8.4.4). An 'Apply' button is visible in the top right corner of the settings area.

Figure 46. Ethernet IP Settings, DHCP client disabled

By default, DHCP client is disabled.

1. On the **Ethernet** page, ensure that the **DHCP client enabled** checkbox is deselected.
2. Configure the IP settings.

Setting	Description
IP address	The Bolt II network IP address in IPv4 dot-decimal notation Default: 192.168.0.97
Subnet mask	The Bolt II network Subnet mask in IPv4 dot-decimal notation. Default: 255.255.255.0
Gateway address	The Bolt II network Gateway address in IPv4 dot-decimal notation. If there is no gateway available, set the Gateway address to: 0.0.0.0
Primary DNS	The Bolt II network Primary DNS in IPv4 dot-decimal notation. There is no default Primary DNS.
Secondary DNS	The Bolt II network Secondary DNS in IPv4 dot-decimal notation. There is no default Secondary DNS.

5.9.2. To Use DHCP Client

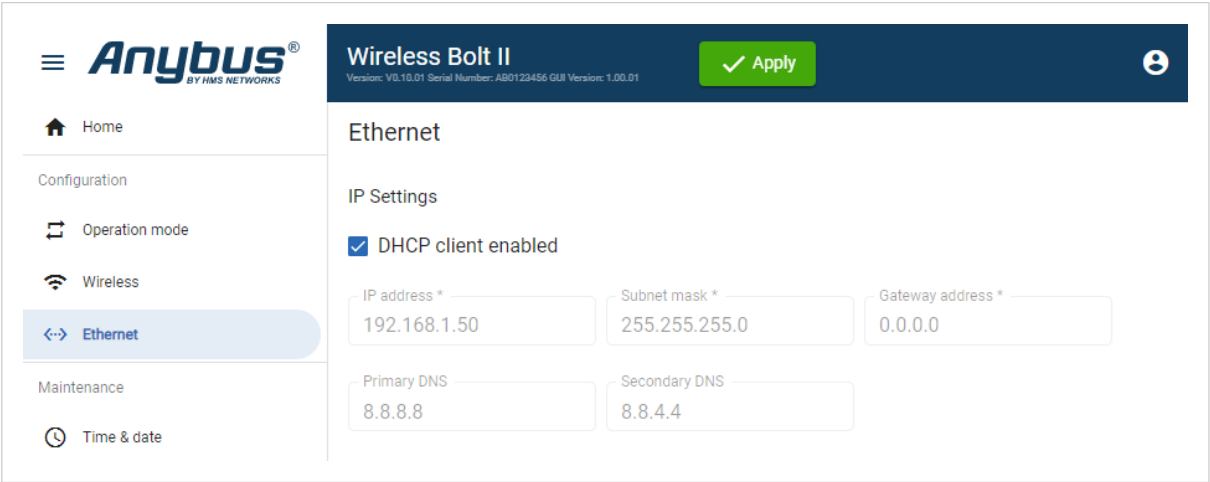


Figure 47. Ethernet IP Settings, DHCP client enabled

By default, DHCP client is disabled.

To enable DHCP client, select the **DHCP client enabled** checkbox. The IP settings will be provided by the network DHCP server.

Table 4. Bolt II default Ethernet IP Settings

Settings	Default value
IP address	192.168.0.97
Subnet mask	255.255.255.0
Gateway address	0.0.0.0
Primary DNS	There is no default Primary DNS.
Secondary DNS	There is no default Secondary DNS.

## 5.10. Apply Configuration

### Before You Begin

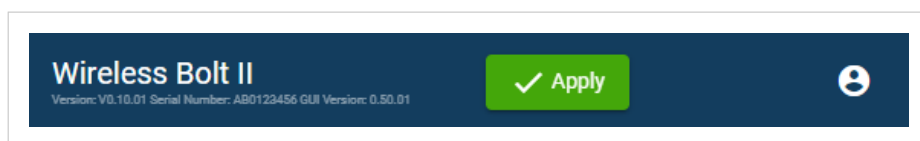
**NOTE**

When you apply the configuration, any existing configuration is overwritten.

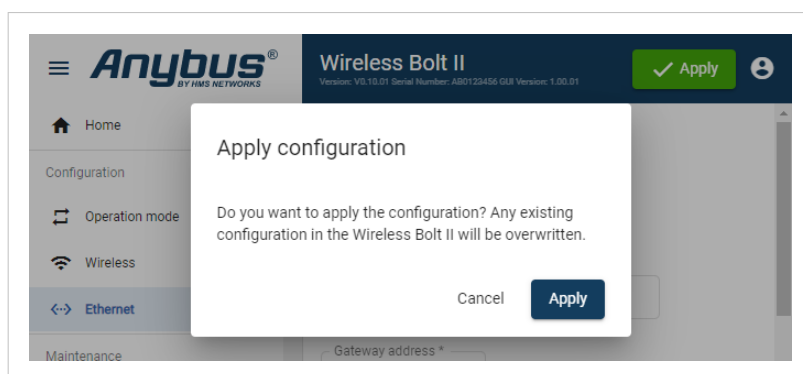
### Procedure

To make the settings take effect, upload the configuration to the Bolt II:

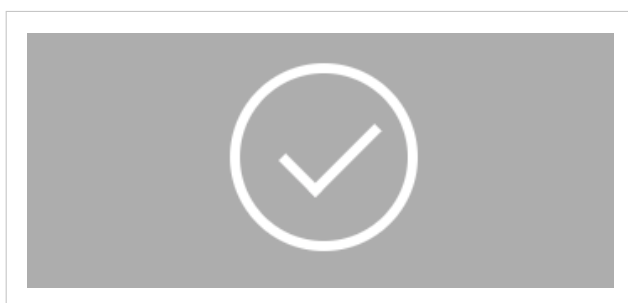
1. In the Bolt II web-interface header, click **Apply**.



2. To confirm the upload, click **Apply**.



3. The configured settings are uploaded and applied to the Bolt II.



## 6. Verify Operation

### 6.1. Bolt II Status Monitor

On the **Home** page, you can get a quick overview of the network and the Bolt II operating status.

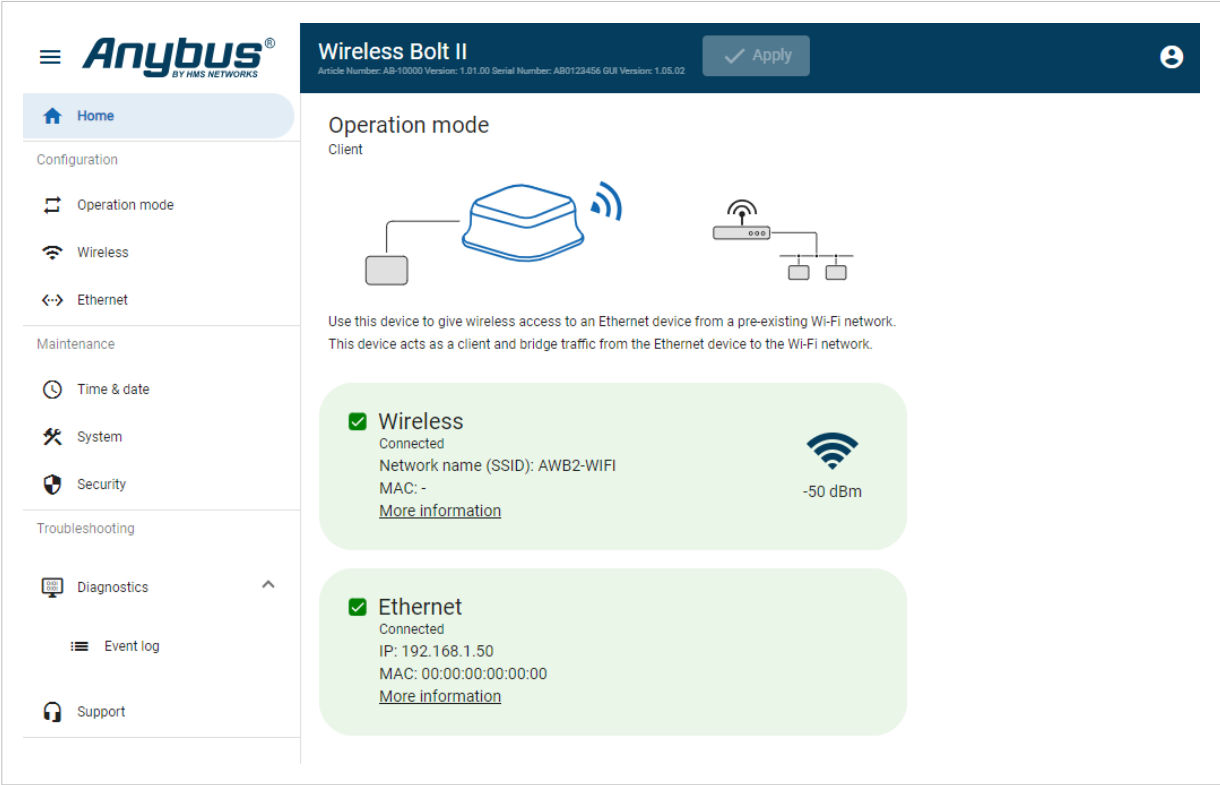


Figure 48. Home page

### Operation Mode

View the current selected Operation mode, see [Wireless Bolt II Operation Modes \(page 21\)](#).

### Wireless Status





Overview of communication status, signal strength and current networks settings.

### Ethernet Status

Overview of connection status, MAC and IP address.



## Status Symbols

Symbol	Description
	<p>Internal error has occurred, and operation cannot be guaranteed.</p> <p>Examples for Run Time System:</p> <ul style="list-style-type: none"> <li>• Could not initialize WLAN device management control: Could not add device management data point wlan-station/rssi: Endpoint receive operation timed out (-32603).</li> <li>• Could not initialize SystemInfo Management Control: SystemInfo: Error (-32603) adding data point system : os, Endpoint receive operation timed out.</li> <li>• Could not initialise Device Manager Control: Update DevMgmCtrl: Error (-32603) adding data point update : counter, Endpoint receive operation timed out.</li> </ul>
	<p>Out of Specification.</p>
	<ul style="list-style-type: none"> <li>• Power fail handling not supported.</li> <li>• Could not load and start program.</li> </ul> <p>Alerts for Cable replacement, Client:</p> <ul style="list-style-type: none"> <li>• The unit is in idle state, waiting for an event.</li> <li>• The unit is inactive.</li> <li>• The unit is disconnected.</li> <li>• The unit is restarting.</li> <li>• Incorrect password is detected.</li> </ul> <p>Alerts for Access point and Cable replacement, Access point:</p> <ul style="list-style-type: none"> <li>• The unit is disabled.</li> </ul>
	<p>Normal operation.</p> <p>Cable replacement, Client:</p> <ul style="list-style-type: none"> <li>• The unit is connected.</li> <li>• The unit is scanning.</li> </ul> <p>Access point and Cable replacement, Access point:</p> <ul style="list-style-type: none"> <li>• The unit is enabled.</li> <li>• The unit is connected to Ethernet network.</li> </ul>

6.2. Ethernet LED Indication

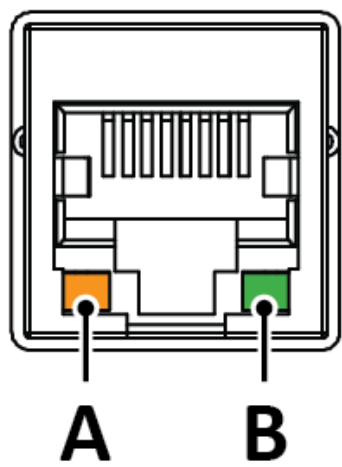


Figure 49. RJ45 LED indicators

LED A – LINK	Function
Off	No Ethernet link or no power
Yellow	Ethernet link established
Yellow, flashing	Ethernet traffic

LED B – ACTIVITY	Function
Off	No power
Green	Power on

## 7. Use Cases

### 7.1. Cable Replacement Between a PLC and a Network Switch

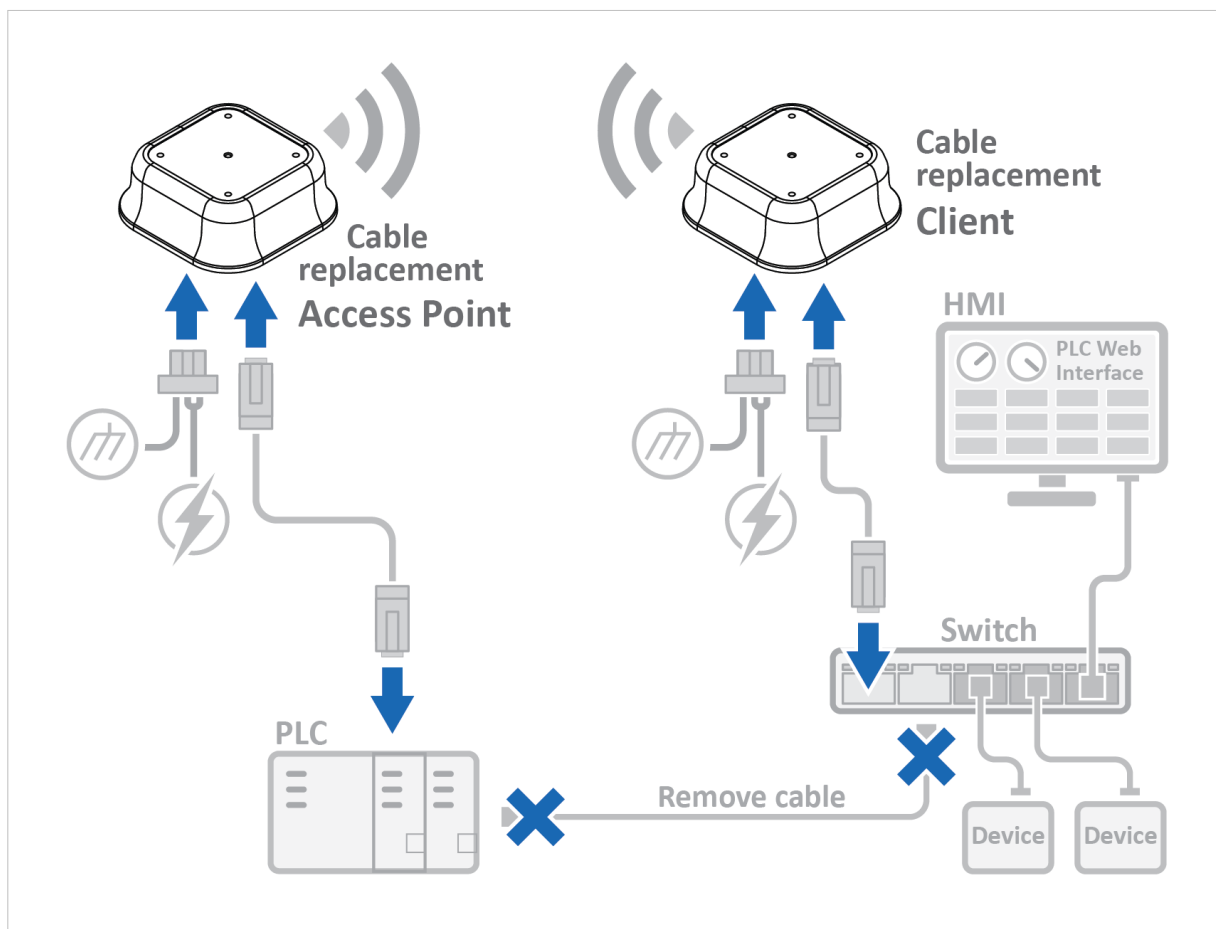


Figure 50. Cable replacement between a PLC and a Network Switch

#### About the Use Case

This use case describes how to set up cable replacement between a Network Switch and a PLC using one Bolt II Cable replacement Access point unit and one Bolt II Cable replacement Client unit.

An HMI and multiple I/O devices are connected to the Network Switch.

The HMI is used to access the PLC built-in web interface over the wireless link.

## Bolt II Cable replacement Access Point Configuration Procedure

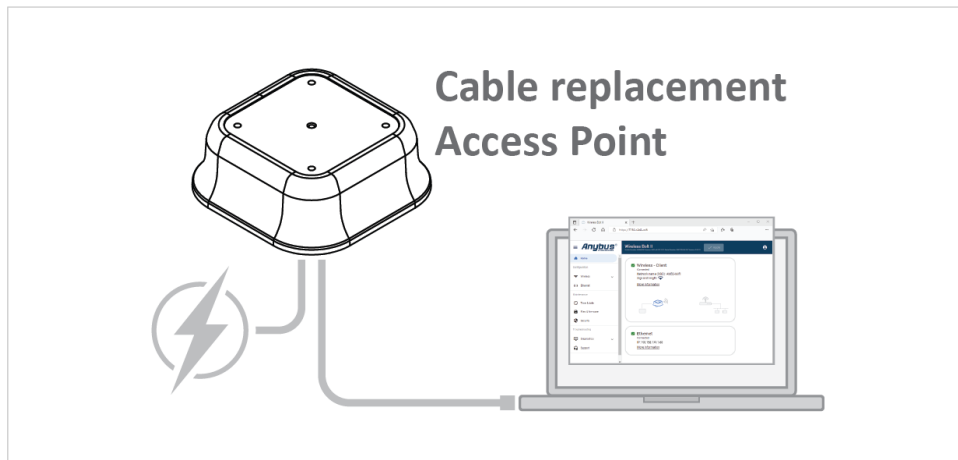


Figure 51. Configure the Bolt II Cable replacement Access point

Configure one Bolt II as a Cable replacement Access point.

See [Configure the Bolt II Cable Replacement Access Point \(page 22\)](#).

## Bolt II Cable replacement Client Configuration Procedure

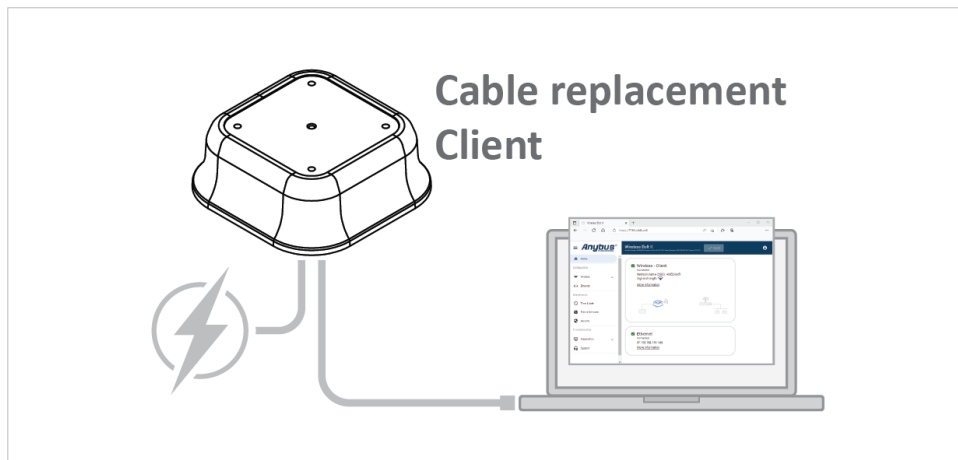


Figure 52. Configure the Bolt II Cable replacement Client

Configure one Bolt II as a Cable replacement Client.

See [Configure the Bolt II Cable Replacement Client \(page 24\)](#).

## Cable Replacement Installation

### Procedure

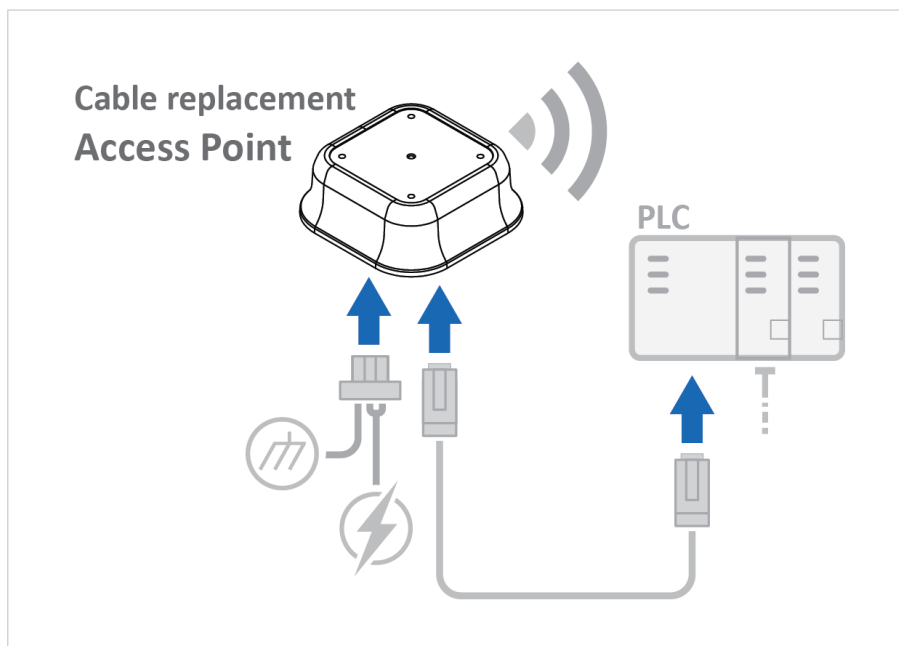


Figure 53. Install the Bolt II Cable replacement Access point

1. Connect the Bolt II Cable replacement Access point to power and Functional Earth (FE).
2. Remove the Ethernet cable between the PLC and the Network Switch.

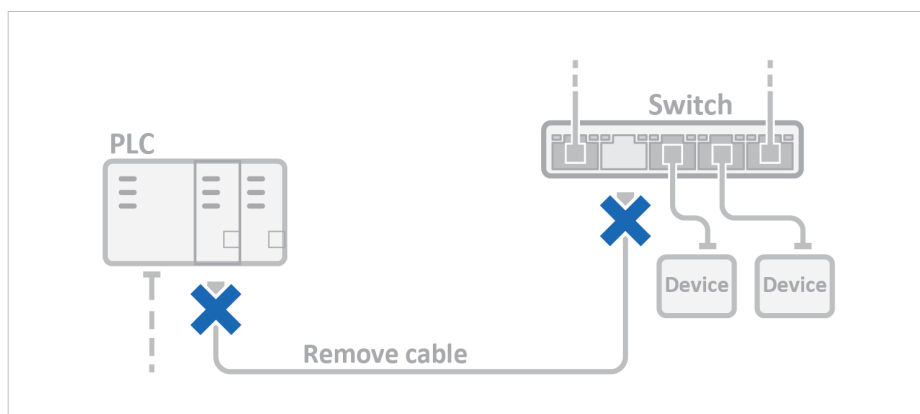


Figure 54. Remove the cable

3. Connect an Ethernet cable between Bolt II Cable replacement Access point and the PLC.

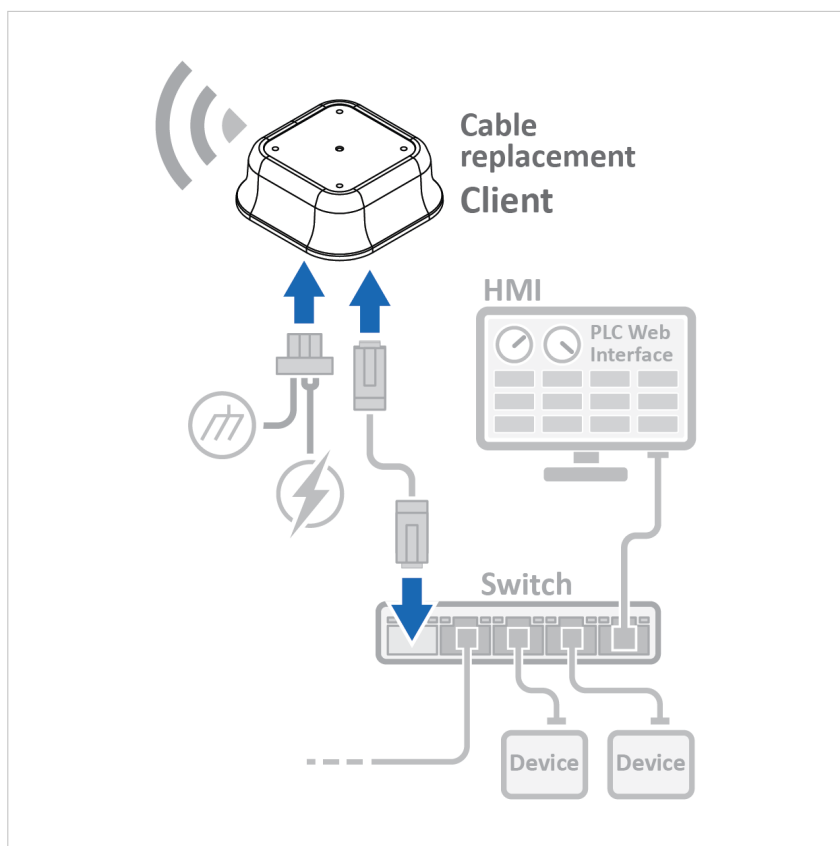


Figure 55. Install the Bolt II Cable replacement Client

4. Connect the Bolt II Cable replacement Client to power and Functional Earth (FE).
5. Connect an Ethernet cable between the Bolt II Cable replacement Client and the Network Switch.

## Result

Wireless connection is now established between the Bolt II Cable replacement Access point and the Bolt II Cable replacement Client.

## Access the PLC Built-In Web Interface on the HMI

### Procedure

On the HMI: To access the PLC built-in web interface, enter the PLC IP address in a browser.

## 7.2. Access PLC from Handheld Device via Wi-Fi

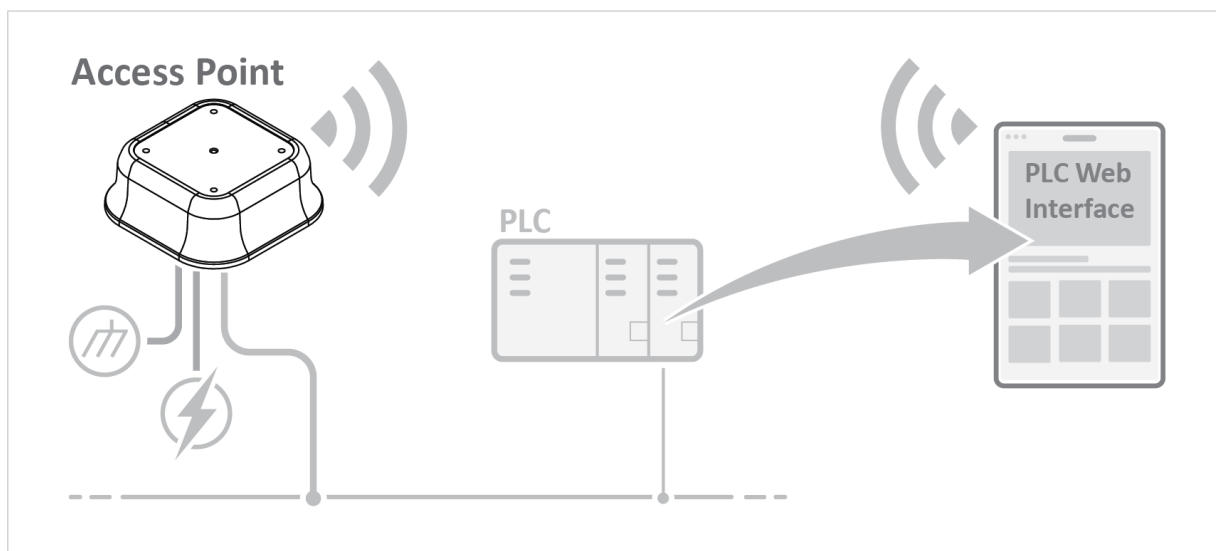


Figure 56. Access a PLC from a handheld device using WLAN

### About the Use Case

This use case describes how to configure a Bolt II as a Wi-Fi access point.

A handheld device and a PLC connected to a wired network are connected to the Bolt II Wi-Fi access point.

The PLC built-in web interface can then be accessed via the handheld device.

### Before You Begin

For information on how to configure the network settings, please refer to the documentation for the handheld device and PLC.

### Bolt II Configuration

#### Procedure

1. Log in to the Bolt II built-in web interface.

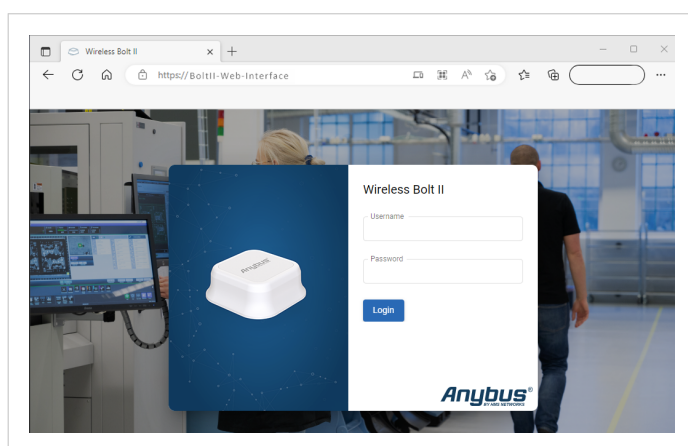


Figure 57. Bolt II Login

2. On the **Operation mode** page, select the **Access point** mode.

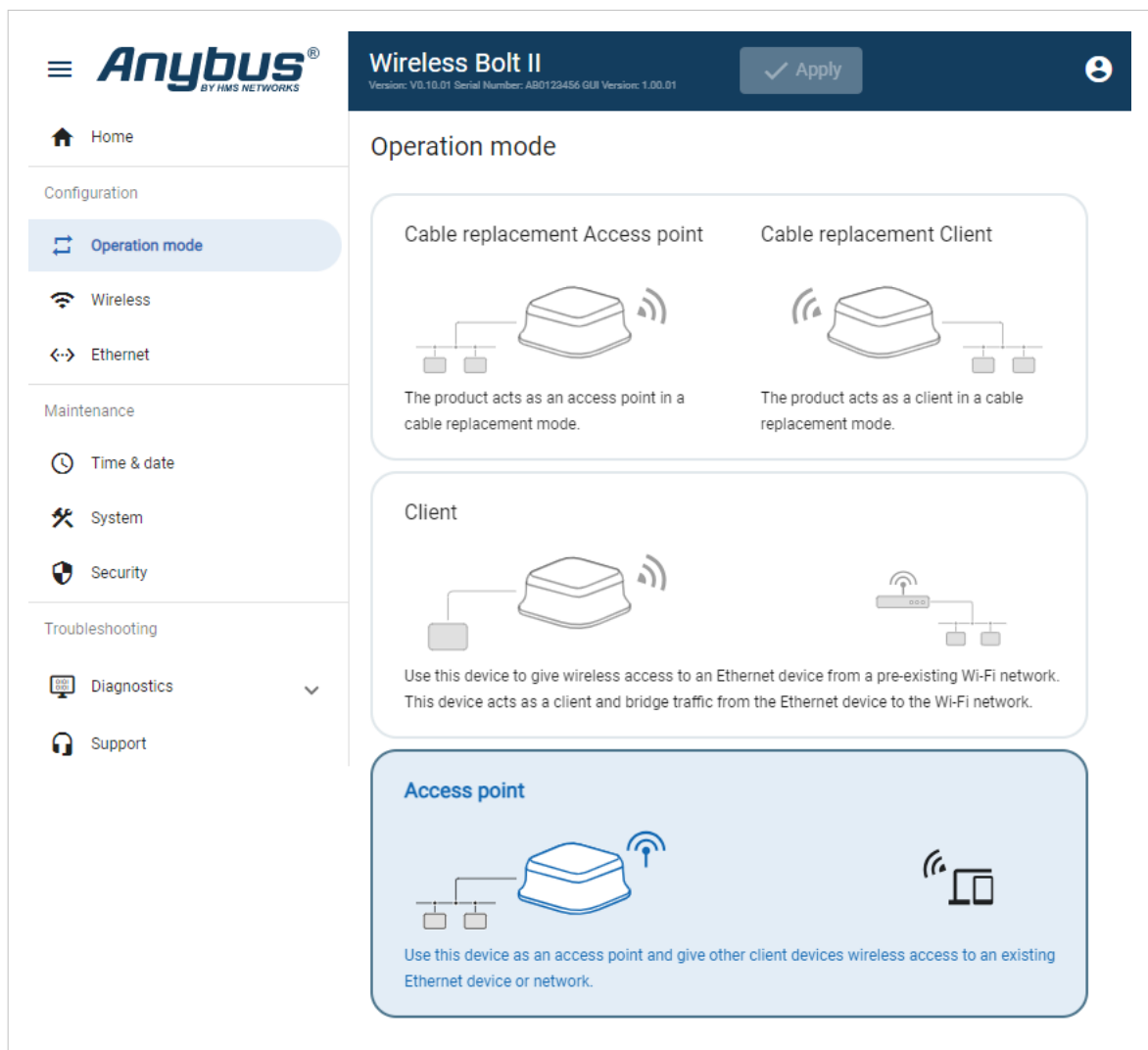


Figure 58. Operation mode page, Access point



3. On the **Wireless** settings page, configure the **Access point** settings.

The screenshot shows the 'Wireless Bolt II' settings page. On the left is a navigation menu with options: Home, Configuration (Operation mode, **Wireless**, Ethernet), Maintenance (Time & date, System, Security), and Troubleshooting (Diagnostics, Support). The main content area is titled 'Access point' and includes an 'Apply' button. The settings are as follows:
 

- Network name (SSID) \***: WIFL\_003056500C86
- Broadcast the network name (SSID)**: ☐
- Radio frequency band**: 2.4 Ghz (selected) and 5 Ghz
- Channel**: 1
- Security type**: WPA2-Personal
- Passphrase \***: [masked]
- DHCP server enabled**: ☐
  - Start IP address**: [empty]
  - End IP address**: [empty]
  - Lease time**: 0 seconds
  - Lease interval**: 0 seconds
  - Subnet mask**: [empty]
  - Gateway address**: [empty]
  - Primary DNS**: [empty]
  - Secondary DNS**: [empty]

Figure 59. Settings page, Access point

- Select radio frequency band **2.4 GHz** or **5 GHz**.
    - 2.4 GHz band (Default): Long range but lower speeds.
    - 5 GHz band: Shorter range but higher speeds.
  - In the **Network name (SSID)** field, enter a unique network name for the Bolt II Wi-Fi access point.
  - In the **Channel** menu, select a band channel.
  - In the **Security type** menu, select **WPA2-Personal** (default) or **WPA3-Personal**.
  - In the **Passphrase** field, enter the desired passphrase for the selected security type.
4. On the **Wireless** settings page, configure the **DHCP server** settings.



#### IMPORTANT

By default, the Bolt II internal DHCP server is enabled. To avoid interference, keep only one DHCP server enabled on the network.

#### Option if you want to use the Bolt II as a DHCP server:

- Select the **DHCP server enabled** checkbox.
- Configure the **DHCP server** settings. See [Access Point DHCP Settings \(page 37\)](#).



#### NOTE

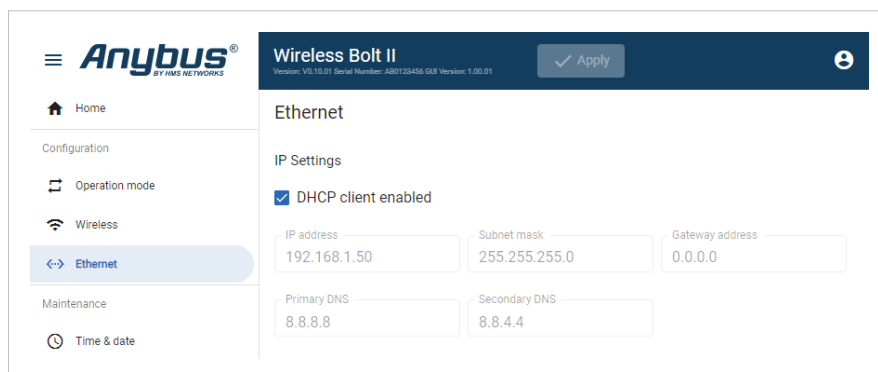
Ensure that the IP address range does not contain any existing addresses on the network.

#### Option if there is an existing DHCP server on the wired network:

- Deselect the **DHCP client enabled** checkbox.

5. On the **Ethernet** page.**Option if the wired network uses DHCP:**

- a. Select the **DHCP client enabled** checkbox.

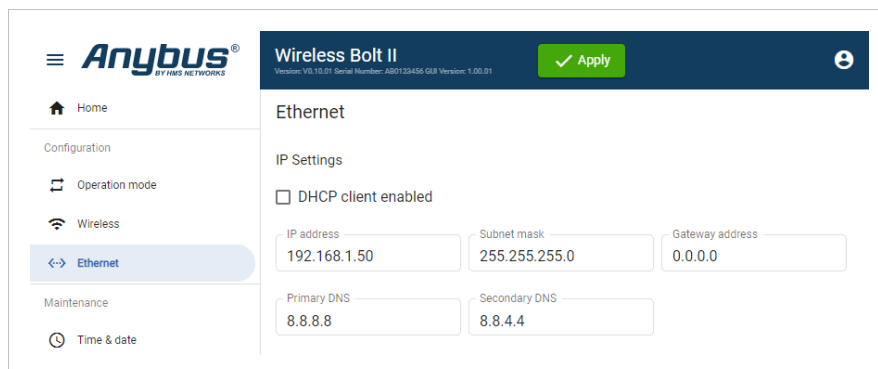


The screenshot shows the 'Anybus' web interface for 'Wireless Bolt II'. The left sidebar contains a menu with 'Home', 'Configuration', 'Operation mode', 'Wireless', 'Ethernet' (highlighted), 'Maintenance', and 'Time & date'. The main content area is titled 'Ethernet' and 'IP Settings'. The 'DHCP client enabled' checkbox is checked. Below it, there are input fields for 'IP address' (192.168.1.50), 'Subnet mask' (255.255.255.0), 'Gateway address' (0.0.0.0), 'Primary DNS' (8.8.8.8), and 'Secondary DNS' (8.8.4.4). An 'Apply' button is visible in the top right corner of the main content area.

Figure 60. DHCP enabled

**Option if the wired network uses Static IP:**

- a. Deselect the **DHCP client enabled** checkbox.
- b. Enter a static **IP address** for the Bolt II.



The screenshot shows the 'Anybus' web interface for 'Wireless Bolt II'. The left sidebar is identical to Figure 60. The main content area is titled 'Ethernet' and 'IP Settings'. The 'DHCP client enabled' checkbox is now unchecked. The input fields for 'IP address', 'Subnet mask', 'Gateway address', 'Primary DNS', and 'Secondary DNS' remain the same as in Figure 60. The 'Apply' button is now green and located in the top right corner of the main content area.

Figure 61. DHCP disabled

6. To apply the settings, click **Apply** in the built-in web interface header and follow the instructions.

**To Access the PLC Built-In Web Interface****Procedure**

On the handheld device:

1. Connect to the Bolt II SSID (Network name).
2. To access the PLC built-in web interface, enter the PLC IP address in a browser.

### 7.3. Connect Device to Wi-Fi Network via Bolt II Client

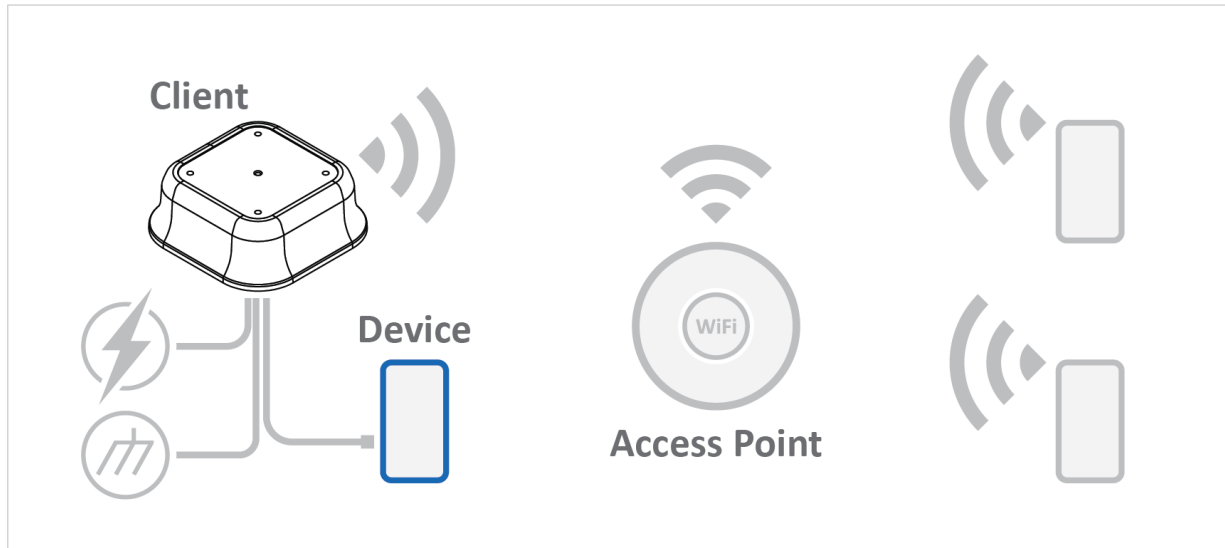


Figure 62. Device connected to Wi-Fi network via Bolt II Client

#### About the Use Case

This use case describes how to configure Bolt II as an client to give a Ethernet device access to a Wi-Fi network.

#### Before You Begin

For information on how to configure the network settings, please refer to the documentation for the wired device.

#### Bolt II Configuration

##### Procedure

1. Log in to the Bolt II built-in web interface.
2. Ensure that the Bolt II is reset to the factory default settings.

3. On the **Operation mode** page, select the **Client** mode.

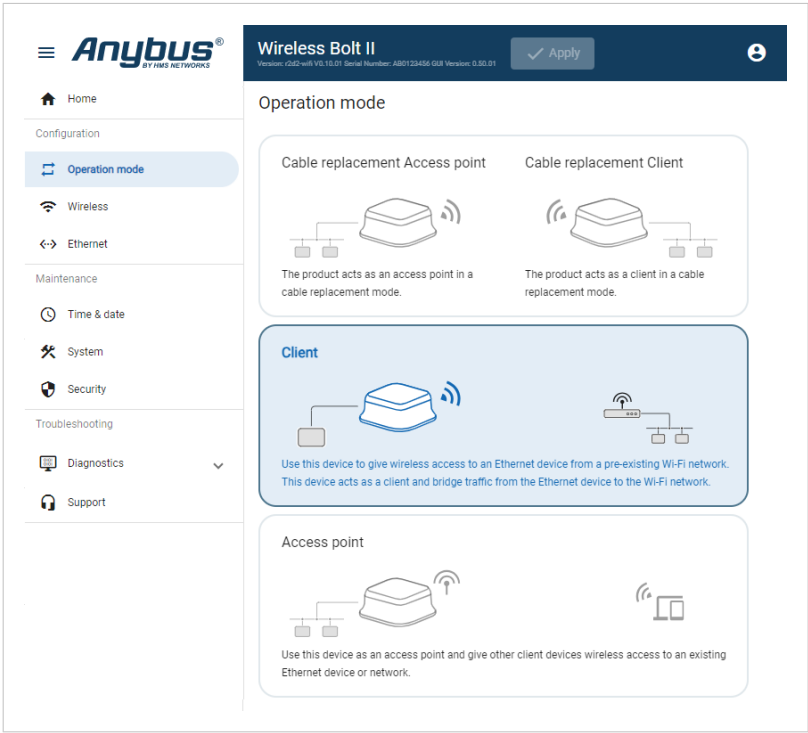


Figure 63. Operation mode page, Client

4. On the **Wireless** page, configure the **Client** settings.

Figure 64. Wireless page, Client

- a. In the **Network name (SSID)** field, enter the name of the Wi-Fi network you want to connect to.
- b. In the **Security type** menu, select a security type for the Wi-Fi network connection.
- c. In the **Passphrase** field, enter the password for the selected Security type.
- d. In the **Forwarding mode** panel, select **MAC clone (MAC Address Cloning)** (default) or **NAT (Network Address Translation)**.  
See [Client MAC Clone \(MAC Address Cloning\) Settings \(page 44\)](#) and [Client NAT \(Network Address Translation\) Settings \(page 47\)](#).
5. When NAT (Network Address Translation) is used: Navigate to the **Ethernet** settings page and configure the IP settings required by the wired network.
6. To apply the settings, click **Apply** in the built-in web interface header and follow the instructions.

## Connect Ethernet Device

### Procedure

1. Connect the Bolt II to a power supply and to Functional Earth (FE).  
See [Installation \(page 6\)](#).
2. Connect an Ethernet cable between the Bolt II client and the Ethernet device to be connected to the Wi-Fi network.
3. Verify that the wired device is connected to the Wi-Fi network.

### 7.4. Connect Bolt II Clients on Enterprise Wireless Network

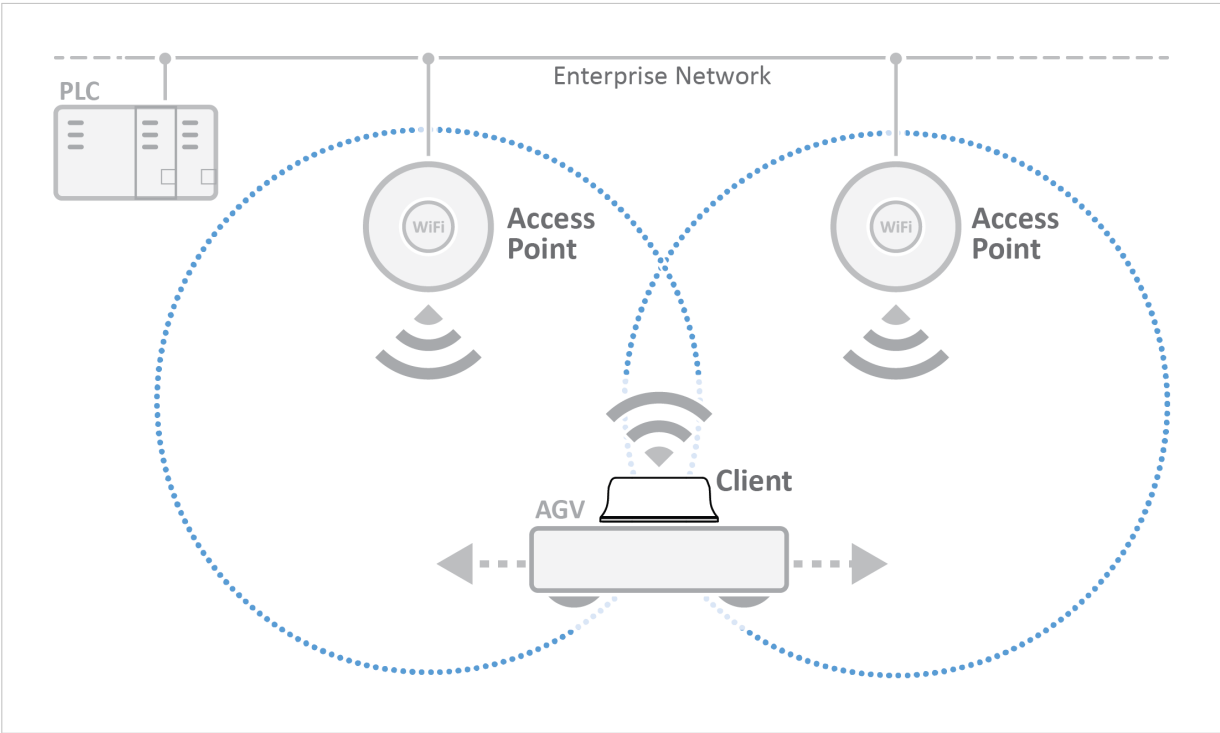


Figure 65. Bolt II Client, installed on an AGV, roaming between two Wi-Fi Access Points located on an enterprise wireless network

#### About the Use Case

This use case describes how to use Bolt II(s) as a Client(s) to give AGV(s) (Automated guided vehicle) Wi-Fi access to access points located on an enterprise wireless network.

#### Before You Begin

For information on how to configure the AGV and PLC (Programmable Logic Controller), please refer to the documentation for the AGV and PLC.

#### Bolt II Client Configuration

##### Procedure

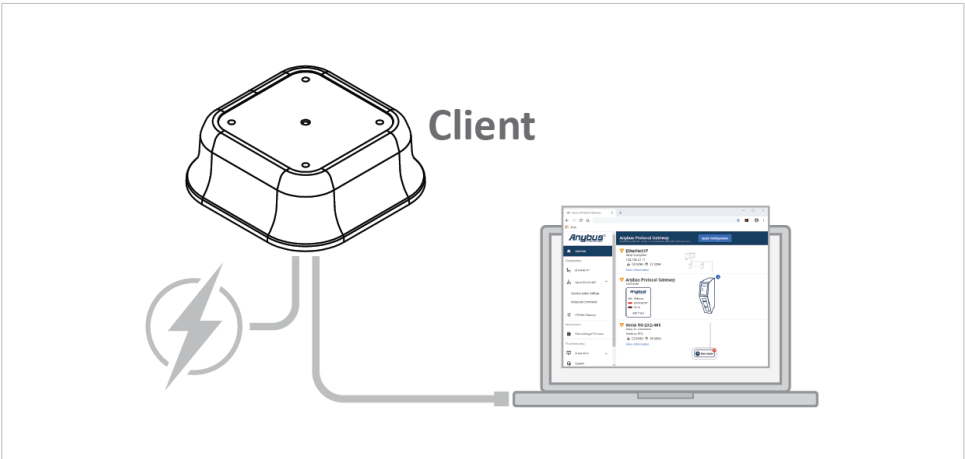


Figure 66. Configure the Bolt II Client(s)

Configure the Bolt II as a Client unit.

Forwarding mode:

- Use **NAT (Network Address Translation)** to connect multiple devices on Layer 3, IP based protocols.
- Use **MAC clone (MAC Address Cloning)** (Default mode) to connect a single device, providing Layer 2 transparency.

See [Client Mode Setup \(page 29\)](#).

Repeat the configuration procedure for each Bolt II Client to be connected to the enterprise wireless network.

## Install the Bolt II Clients

### Procedure

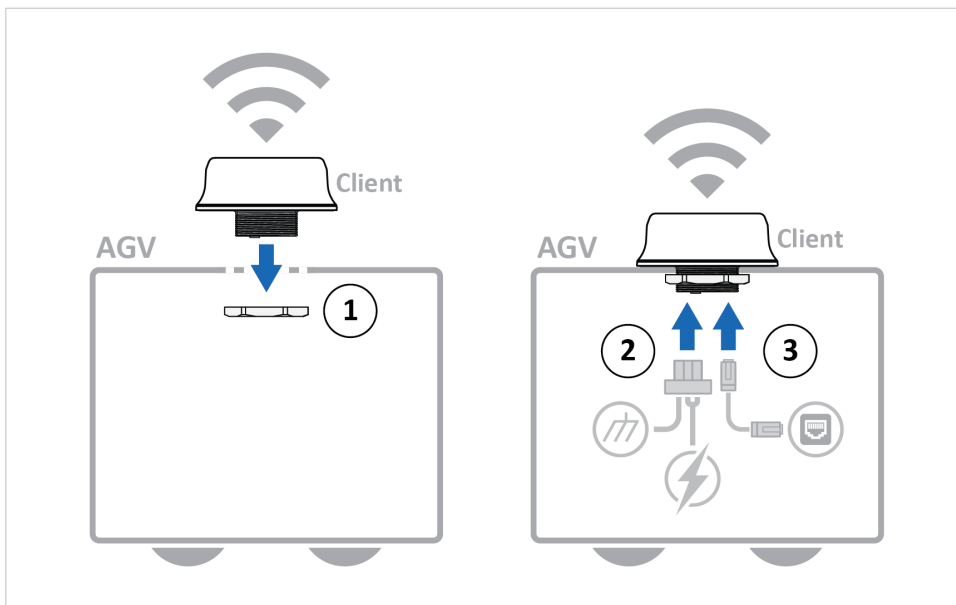


Figure 67. Install Bolt II Client on AGV

1. Mount the Bolt II Client on the AGV.
2. Connect the Bolt II Client to power and Functional Earth (FE).
3. Connect an Ethernet cable between the Bolt II Client and the AGV.

See also [Installation \(page 6\)](#).

Repeat the installation procedure for each Bolt II to be installed on an AGV.

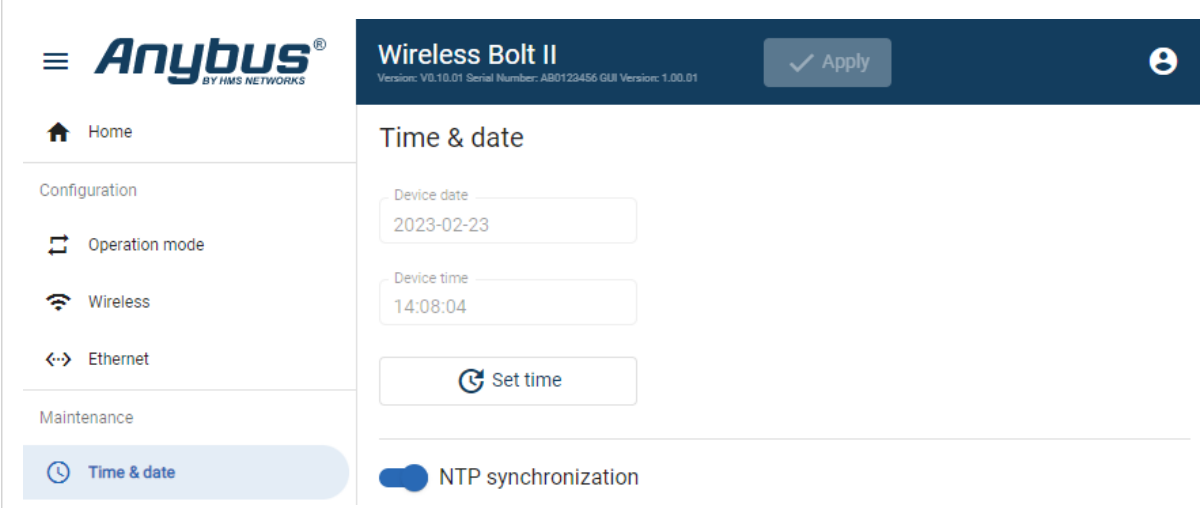
## Result

Wireless connection is now established between the Bolt II Client and the enterprise wireless network.

## 8. Maintenance

### 8.1. Time & Date Settings

#### 8.1.1. Set Time



The screenshot displays the web interface for the Anybus Wireless Bolt II. The top navigation bar includes the Anybus logo, the device name 'Wireless Bolt II', version information (V0.10.01, Serial Number: A80123456, GUI Version: 1.00.01), an 'Apply' button, and a user profile icon. The left sidebar contains a menu with 'Home', 'Configuration' (sub-menu: 'Operation mode'), 'Wireless', 'Ethernet', and 'Maintenance' (sub-menu: 'Time & date', which is currently selected). The main content area is titled 'Time & date' and features two input fields: 'Device date' with the value '2023-02-23' and 'Device time' with the value '14:08:04'. Below these fields is a 'Set time' button with a circular arrow icon. At the bottom of the page, there is a toggle switch for 'NTP synchronization', which is currently turned on.

Figure 68. Time & date page, Set time

You can set the current browser time and date in the Bolt II.

On the **Time & date** page, click **Set time**.



### 8.1.2. Network Time Protocol (NTP) Synchronization

You can use the **Network Time Protocol (NTP)** to synchronize with computer clock time sources on a network.

The screenshot shows the 'Time & date' configuration page for the 'Wireless Bolt II' device. The interface includes a sidebar with navigation options: Home, Configuration (Operation mode, Wireless, Ethernet), Maintenance (Time & date, System, Security), and Troubleshooting. The 'Time & date' section is active, showing a toggle for 'NTP synchronization' which is turned on. Below this, there are four input fields for 'NTP server' with the values '1.se.pool.ntp.org', '2.se.pool.ntp.org', '3.se.pool.ntp.org', and '4.se.pool.ntp.org'. An 'Interval' field is set to '20 minutes'. A green 'Apply' button is visible in the top right corner of the configuration area.

Figure 69. Time & date page, NTP synchronization enabled

By default, **NTP synchronization** is disabled.

To use **NTP synchronization**:

1. On the **Time & date** page, enable **NTP synchronization**.
2. In the **NTP server** fields, enter the Server name or IP number of the NTP server.  
You can enter up to four different NTP servers.
3. In the **Interval** field, enter the number of minutes between the time synchronization attempts (1-65535).

### 8.1.3. Use Timezone Settings

You can set the time zone for where the Bolt II is installed.

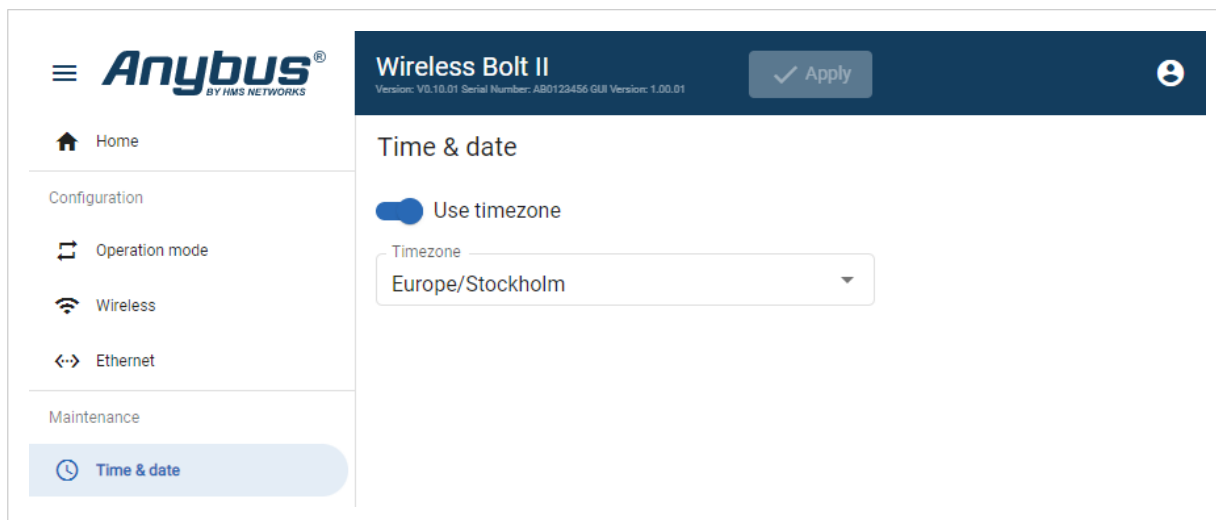


Figure 70. Time & date page, Use timezone

To set the **Use timezone**:

1. On the **Time & date** page, enable **Use timezone**.
2. In the **Timezone** menu, select the timezone where the product is installed.

## 8.2. Configuration File Handling

### 8.2.1. Export Configuration

You can export the current configuration, in order to store the configuration file as a backup or to import and use the same settings to configure additional Bolt II units.

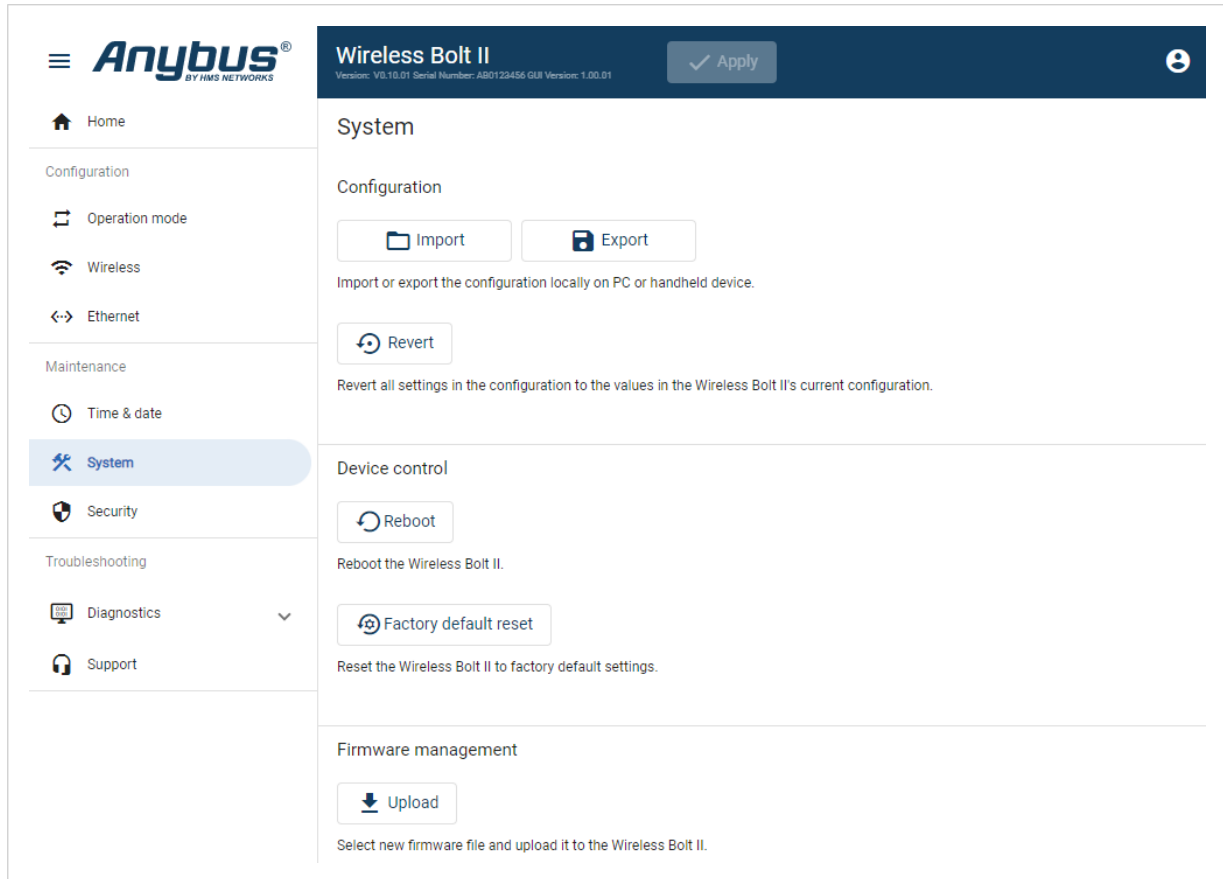


Figure 71. System page

To export a configuration file:

In **System**, click **Export**.

The configuration settings are stored in a .conf file and downloaded to your PC.

## 8.2.2. Import Configuration

To configure multiple Bolt II units with the same settings, you can import a configuration file.

### Before You Begin



#### NOTE

Importing a configuration replaces the current applied configuration.

The supported file format is .conf.

### Procedure

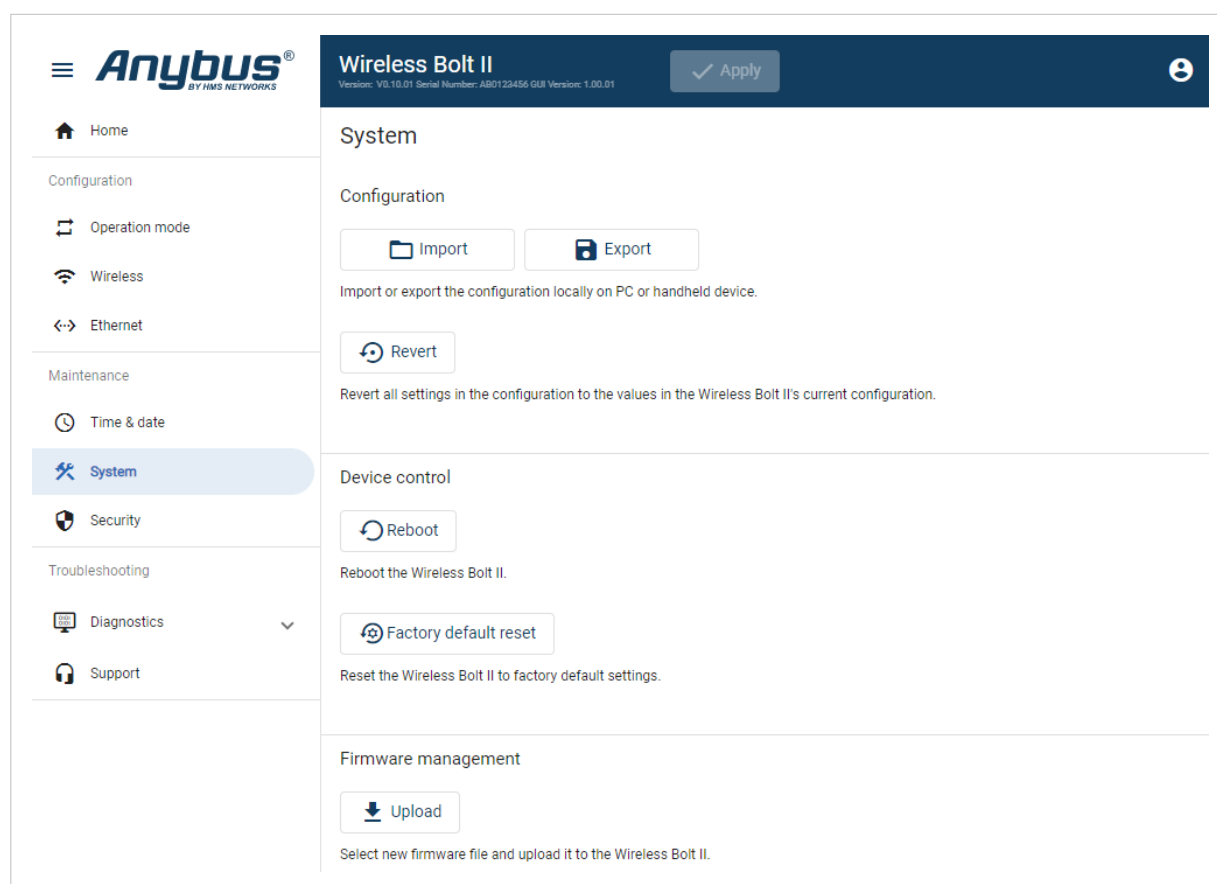


Figure 72. System page

Import configuration file:

1. On the **System** page, click **Import**.
2. In the Import configuration window, click **Select file (.conf)**.
3. In the Open dialog box, browse to and select the configuration file and click **Open**.
4. In the Import configuration window, click **Import**.
5. The configuration file is parsed.
  - If the configuration is compatible, the settings are imported.
  - If any compatibility mismatches occur, a message about the mismatch appears.
6. To apply the settings, click **Apply** in the web-interface header, and follow the instructions.

## 8.3. Revert Configuration

You can restore all settings in a configuration to the default settings.

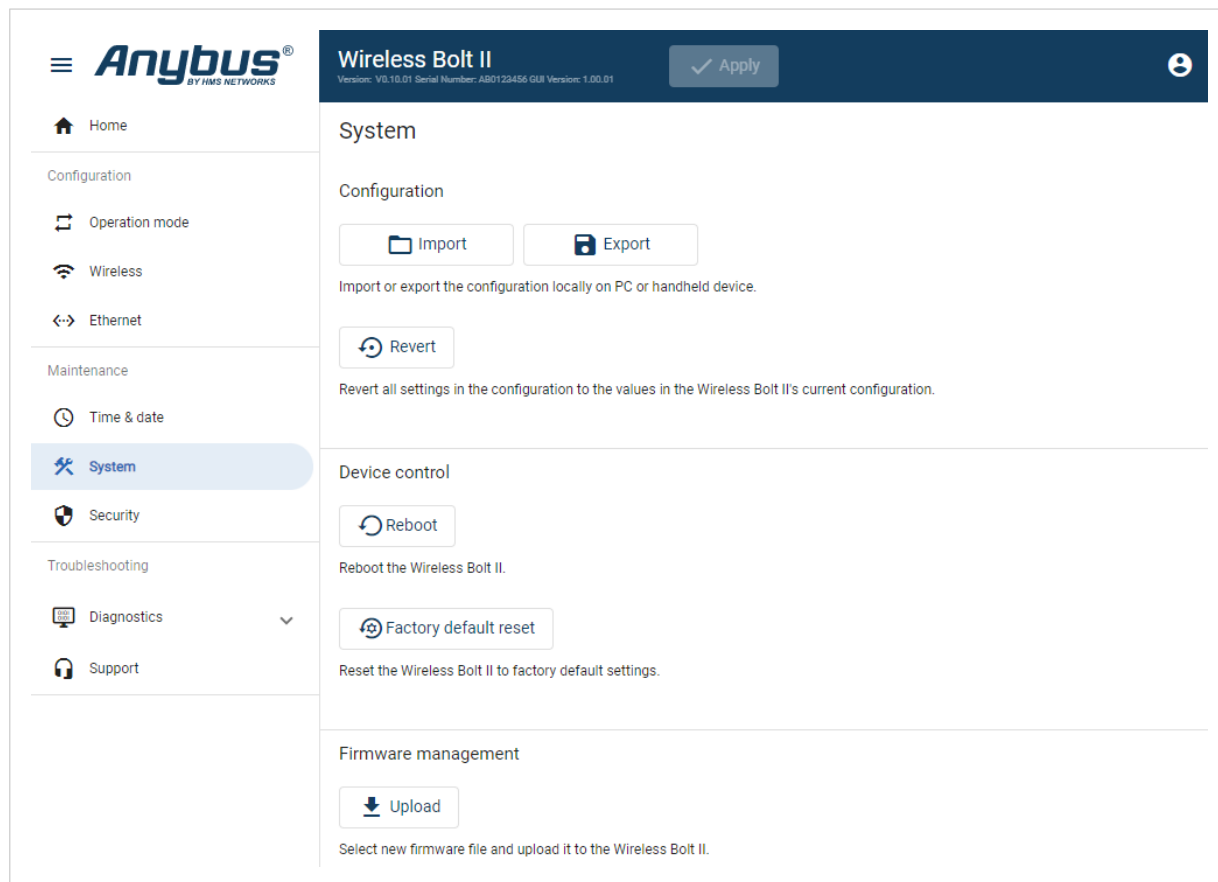


Figure 73. System page

When you want to remove any configuration made in a current session and re-load the configuration from the Bolt II.

1. On the **System** page, click **Revert**.
2. In the Confirm revert window, click **Revert**.

## 8.4. Firmware Management

### 8.4.1. View the Firmware Version

On the **Support** page, you can view the current applied firmware version.

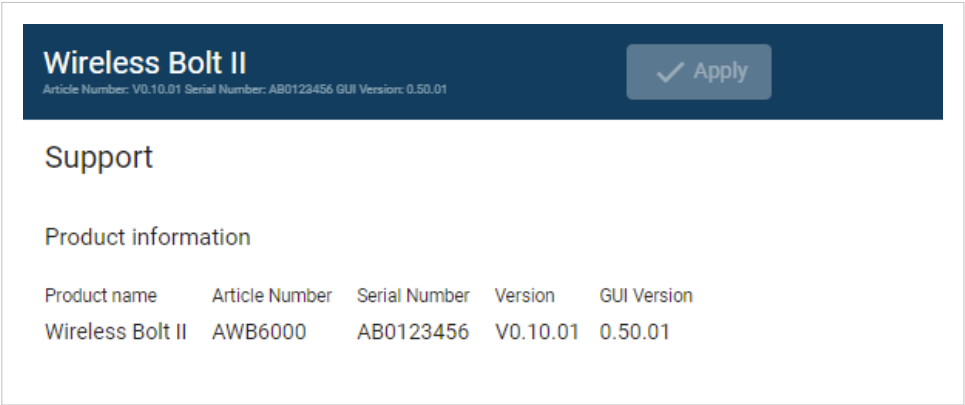



Figure 74. Support page, Product information example

### 8.4.2. Firmware and Configuration Compatibility

#### Compatibility after Firmware Upgrade

Current configuration is still compatible after upgrading the firmware.

#### Compatibility after Firmware Downgrade

**IMPORTANT**  
Compatibility after a firmware downgrade cannot be guaranteed.  
  
The current configuration may use features not available in the older firmware version.

### 8.4.3. Firmware File Validation

Before the firmware file is imported into the system, the firmware upgrade function performs a validation of the file, to ensure compatibility and validity of the firmware file.

If the firmware file does not pass the validation, the firmware file is rejected, and an error message appear.

## 8.4.4. Update Firmware

### Before You Begin



#### NOTE

If the firmware update process is interrupted or if the power is lost during the update process, the update process will resume as soon as the Bolt II is powered on again.

### Download Firmware Package

To download the firmware update package zip file, please visit [www.hms-networks.com](http://www.hms-networks.com) and enter the product article number to search for the Bolt II support web page. You find the product article number on the product cover.

### Procedure

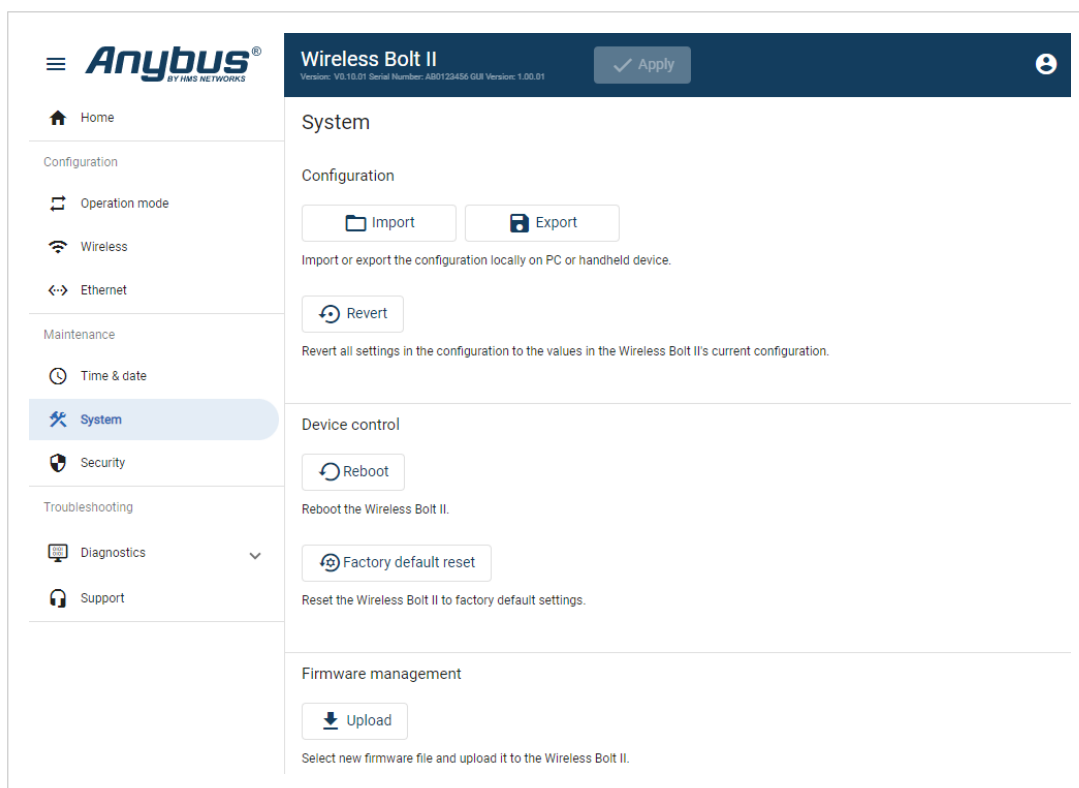


Figure 75. System page

To update the firmware:

1. On the **System** page > **Firmware management**, click **Upload**.
2. In the Upload Firmware window, click **Select firmware (.cup)**.
3. In the Open dialog box, browse to and select the firmware file and click **Open**.
4. To start the firmware upgrade, click **Update firmware**.  
The firmware file is validated and transferred.

### Result

- If the firmware file passes the validation: The firmware is upgraded and then the Bolt II automatically reboots, for the upgrade to take effect.
- If the firmware file is rejected: An error message appears.

## 8.5. Security

### 8.5.1. Web Server Certificate

Install a web server certificate in the Bolt II.

#### Before You Begin

**NOTE**

The Web Server Certificate file must contain both Certificate and Private key.

**NOTE**

The device certificate must be a Base64 encoded DER certificate. Use the PEM (Privacy Enhanced Mail) file format.

**NOTE**

If the certificate is to be used by HTTPS, the subject name “CN” parameter must be set to the device address (IP number or DNS name).

#### Procedure

1. Login to the Bolt II built-in web interface.
2. Navigate to the **Security** page.

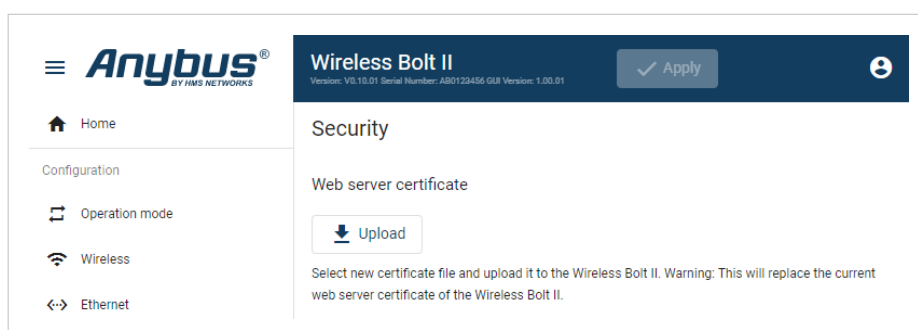


Figure 76. Security page

3. To upload the web server certificate, click **Upload**.
4. In the **Upload web server certificate** window, click **Select certificate file (.pem)**.
5. In the **Open** dialog box, browse to and select the web server certificate file and click **Open > Upload certificate**.



## Result

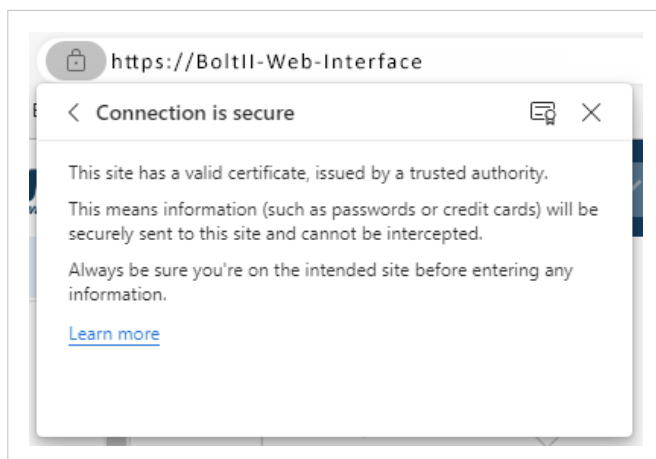


Figure 77. Example View site information > Connection is secure

The web server certificate is uploaded in the web browser.

In the web browser **View site information**, check that the **Connection is secure**.

### 8.5.2. WPA2/WPA3 Enterprise Certificates

#### Before You Begin



#### IMPORTANT

The certificates remain on the Bolt II until new files are uploaded or a factory reset is performed.

To avoid exposure of sensitive data, always perform a factory reset before decommissioning the equipment.



#### NOTE

Uploading a CA certificate is not mandatory. The Bolt II still connects to the network, but no server validation is performed.

#### Procedure

5. On the **Operation mode** page, ensure **Client** is selected.

6. On the **Wireless** page, ensure that **Security type** is set to **WPA2-Enterprise**, **WPA2-Enterprise TLS**, **WPA3-Enterprise**, or **WPA3-Enterprise TLS**.  
See also [Client Security Settings](#) (page 43).

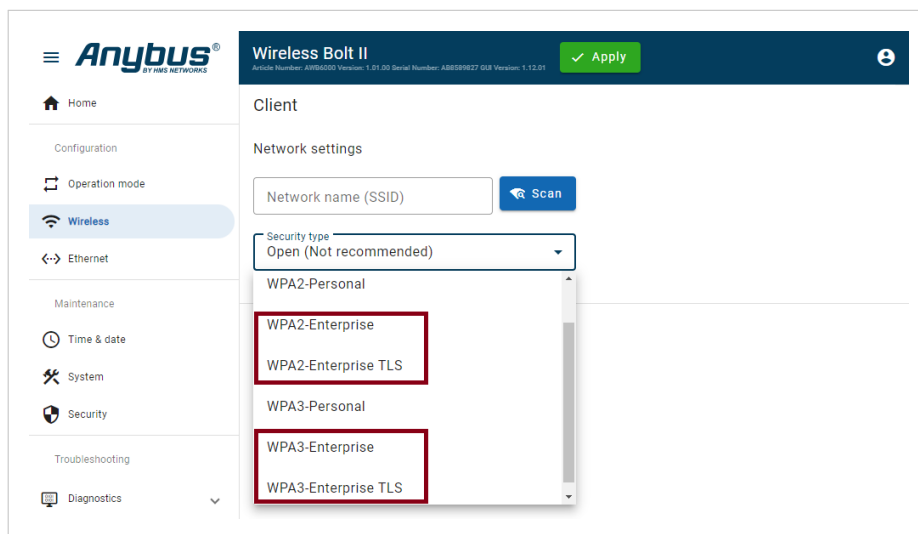


Figure 78. Wireless page, Security type

7. Click on **Click here to upload certificates**.  
You are redirected to the **Security** page.

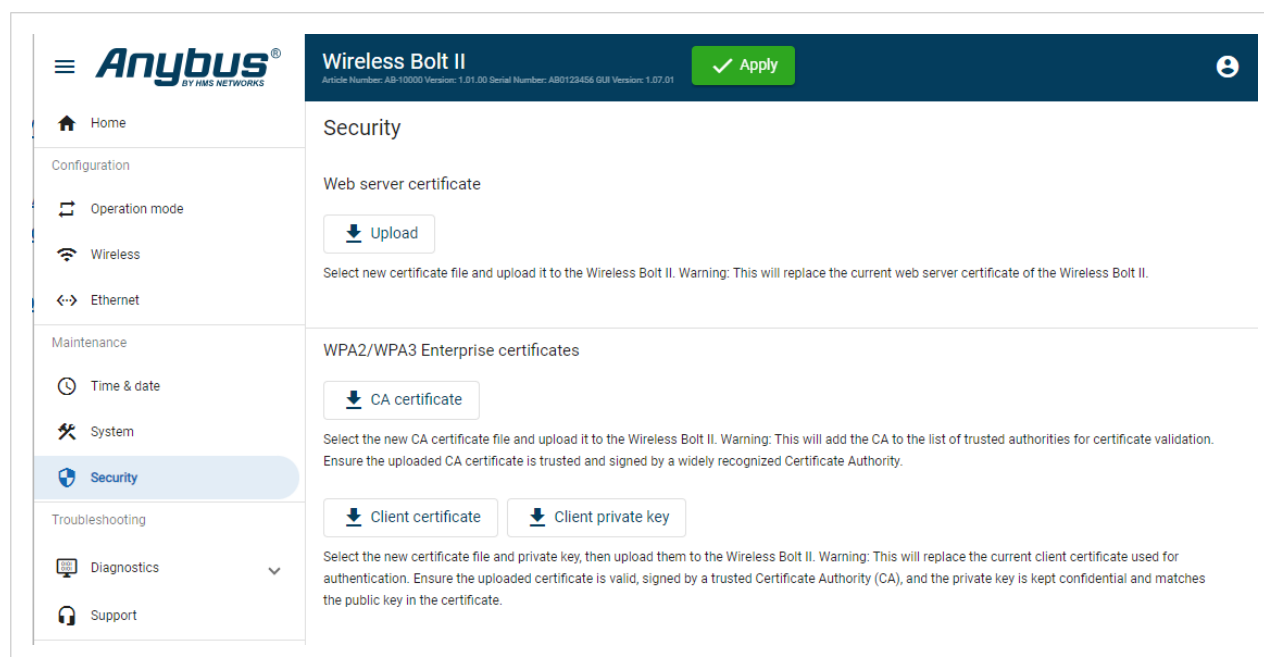


Figure 79. Security page

### Upload CA certificate

8. To upload the CA certificate, click **CA certificate**.
9. In the **Upload CA certificate** window, click **Select certificate file (.pem)**.
10. In the **Open** dialog box, browse to and select the CA certificate file and click **Open > Upload certificate**.

### Upload Client certificate and Client private key

Mandatory when Transport Layer Security (TLS) is used.

11. To upload the client certificate, click **Client certificate**.
12. In the **Upload client certificate** window, click **Select certificate file (.crt)**.
13. In the **Open** dialog box, browse to and select the client certificate file and click **Open > Upload certificate**.
14. To upload the client private key, click **Client private key**.

**NOTE**

Before uploading the client private key file, ensure that it corresponds to the client certificate.

15. In the **Upload client private key** window, click **Select private key file (.key)**.
16. In the **Open** dialog box, browse to and select the client private key file and click **Open > Upload key**.

**Result**

The certificates and client key are uploaded to the Bolt II.

The uploaded certificates and key are used for connecting to the wireless network.

The certificates remain on the Bolt II until new files are uploaded or a factory reset is performed.

## 8.6. Change the Bolt II Password



### IMPORTANT

For cybersecurity reasons, you are prompted to change the password at first login using the Bolt II factory default password. You are redirected to the **Change password** page, see [Change the Bolt II Password \(page 80\)](#).

### Procedure

To change the Bolt II built-in web interface login password:

1. In the Bolt II built-in web interface header, click on the **Account** icon > **Change password**.

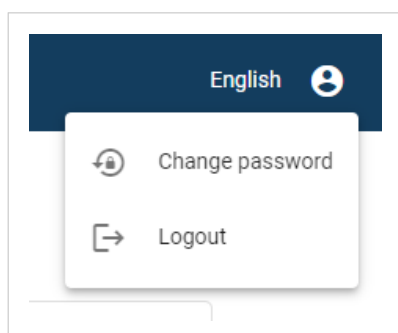


Figure 80. Account menu, Change password

2. Enter your current password, then enter a new password and confirm the new password.

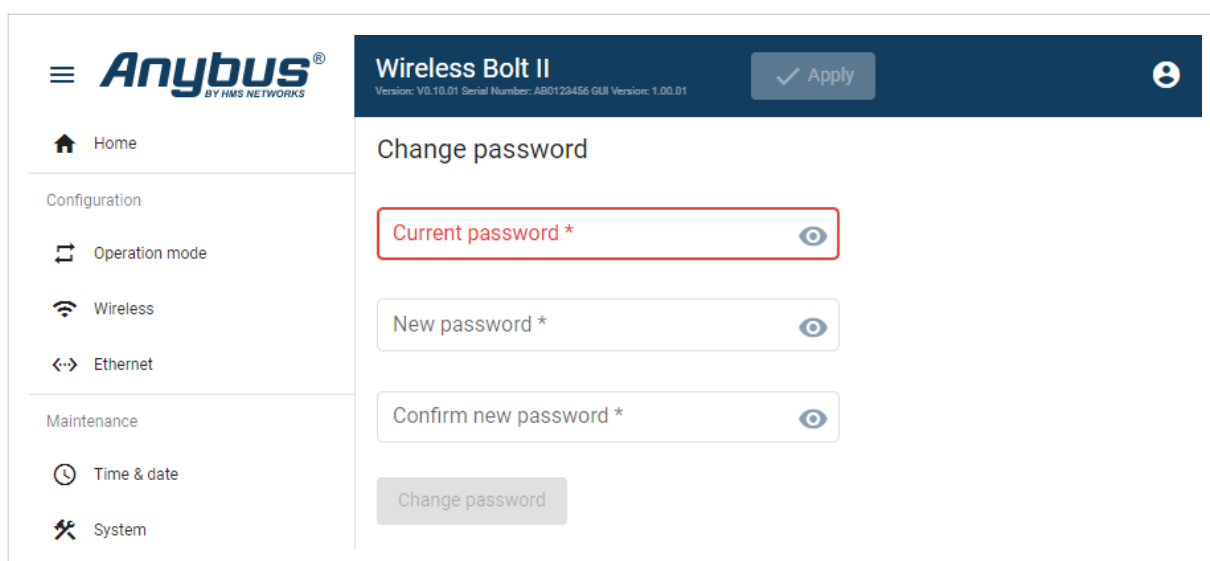


Figure 81. Change password page

3. To make the change take effect, click **Change password**.

## 9. Troubleshooting

### 9.1. Diagnostics

#### 9.1.1. Event Log

The screenshot shows the 'Event log' page for the 'Wireless Bolt II' device. The left sidebar contains navigation links: Home, Configuration (Operation mode, Wireless, Ethernet), Maintenance (Time & date, System, Security), Troubleshooting (Diagnostics, Event log), and Support. The main content area displays a table of events.

Time (d:hh:mm:ss.ms)	Message	Type
2021-12-14 12:14:10	Starting watchdog task	✓
2021-12-14 12:14:10	Starting HTTP server	✓
2021-12-14 12:14:10	Starting SSH server	✓
2021-12-14 12:14:10	Starting UDP config server	✓
2021-12-14 12:14:15	Run Time System: Started	✓
2021-12-14 12:14:15	Service interfaces are enabled!	✓
2021-12-14 12:14:16	Update Loader: Running	✓
2021-12-14 12:14:16	Run Time System: Running	✓
2021-12-14 12:14:30	WLAN: Started	✓
2021-12-14 12:14:32	Network manager: Link detected at Ethernet (1), Port (4).	✓

Figure 82. Event log page example

To export the log data, click **Export**. An Excel XLSX file with the data is downloaded to your PC.

#### How To Analyze the Information

The log follows the FIFO principle, first in and first out. The oldest (first) value is processed first.

Value	Description
Time (d:hh:mm:ss.ms)	The date and time when the event occurred.
Message	A brief description of the event.
Type	The severity of the event occurred. For description of the symbols, see <a href="#">Status Symbols (page 53)</a> .

9.1.2. Remotely Monitor the Bolt II Status

On the **Home** page, you can remotely monitor the Bolt II wireless and Ethernet status.

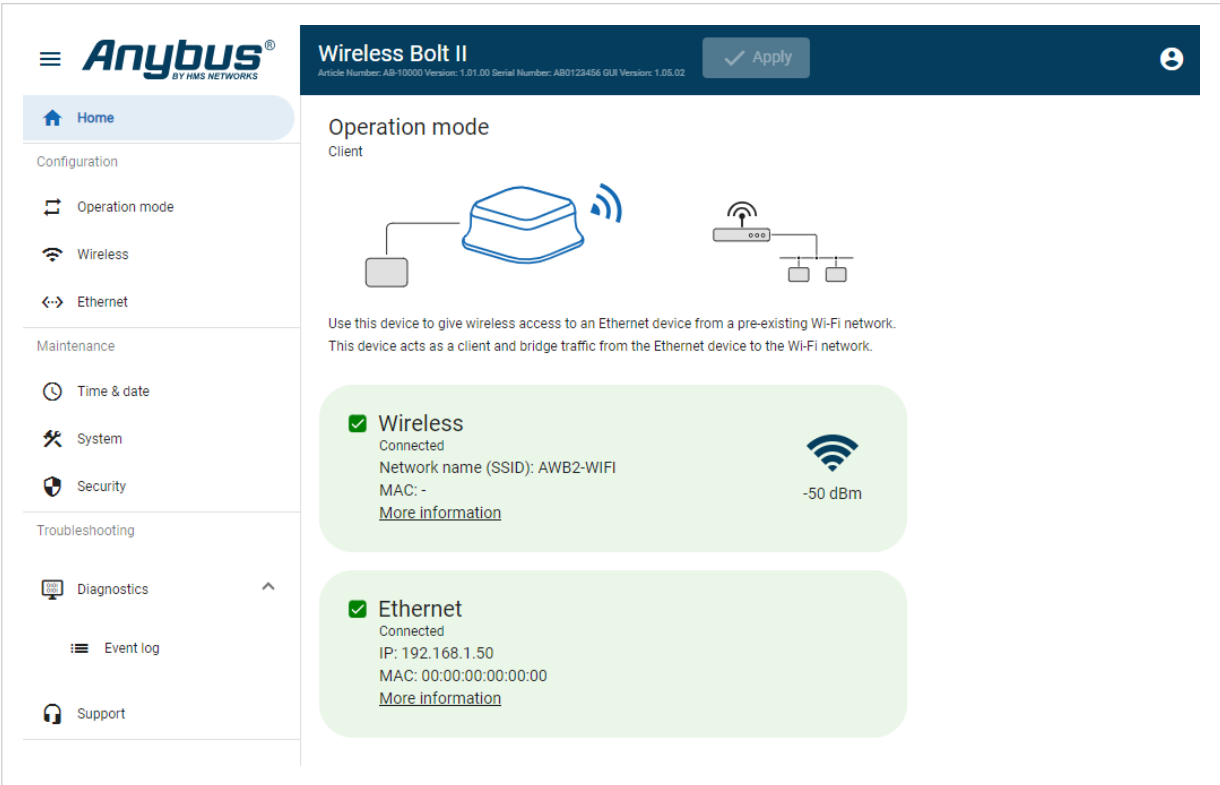


Figure 83. Home page

For information about the status symbols, see [Status Symbols \(page 53\)](#).

9.2. Find the Bolt II IP Address

You can use the software application HMS IPconfig to find the Bolt II IP address.

Example 4. Device IP address detected in HMS IPconfig

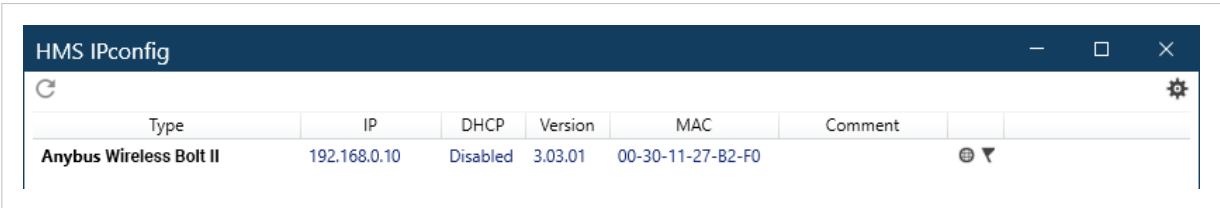


Figure 84. HMS IPconfig

To download the installation files, please visit [www.hms-networks.com](http://www.hms-networks.com) and enter the product article number to search for the Bolt II support web page. You find the product article number on the product cover.

## 9.3. Reboot Using the Reset Button

### Before You Begin

**NOTE**

Pressing and holding the reset button for more than 10 seconds will initiate a factory reset of the Bolt II.

During reboot, the Bolt II is temporarily unavailable for approximately two minutes.

### Procedure

1. Ensure that the Bolt II is powered on.

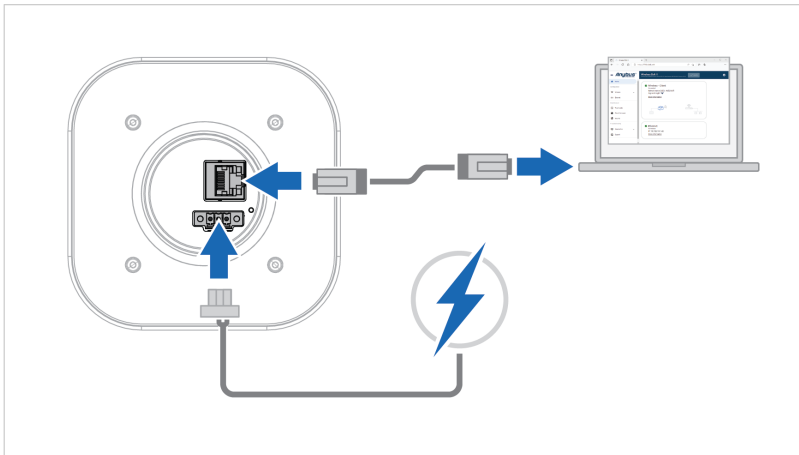


Figure 85. Power on the Bolt II

2. Use a pointed object, such as a paper clip to quickly press and release the **Reset** button.

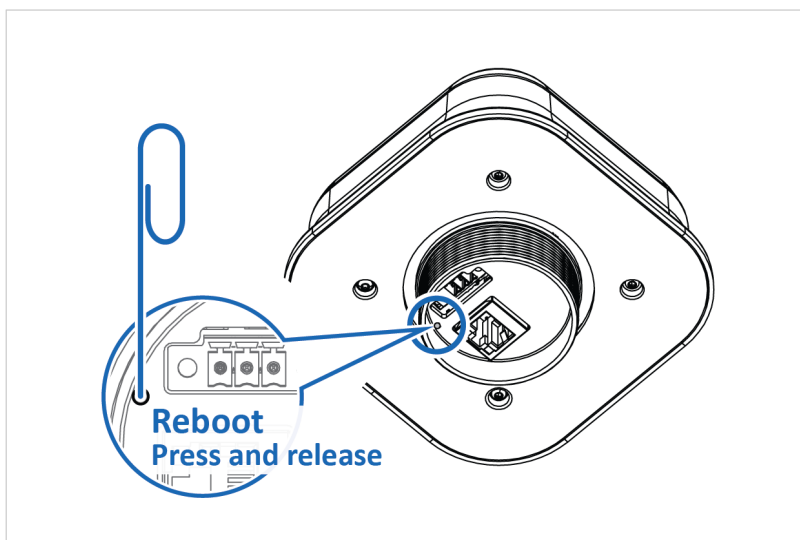


Figure 86. Quickly press and release the **Reset** button

3. Wait while the Bolt II reboots.

### Result

You are logged out of the Bolt II built-in web interface and redirected to the login page.

## 9.4. Reboot Using the Built-In Web Interface

### Before You Begin

During reboot, the Bolt II is temporarily unavailable for approximately two minutes.

### Procedure

1. Ensure that the Bolt II is powered on and running.

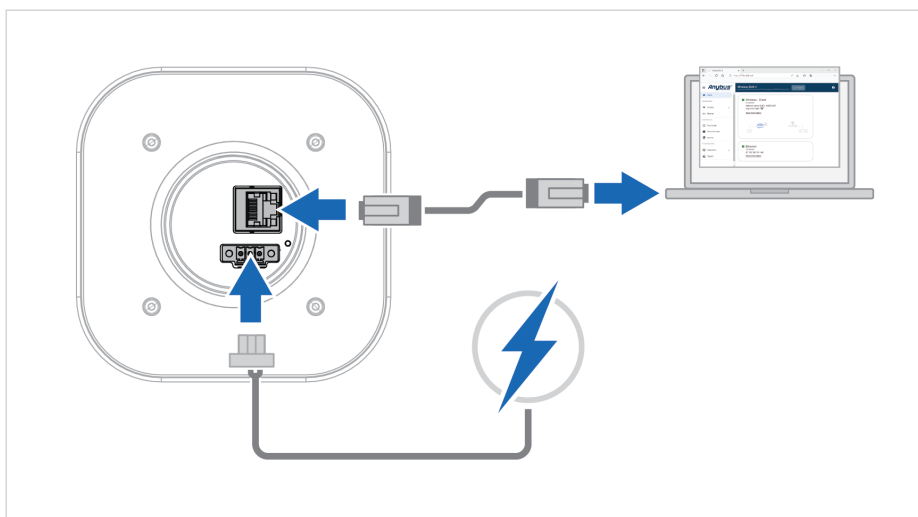


Figure 87. Power on the Bolt II

2. Login to the Bolt II built-in web interface.
3. On the **System** page, click **Reboot**.

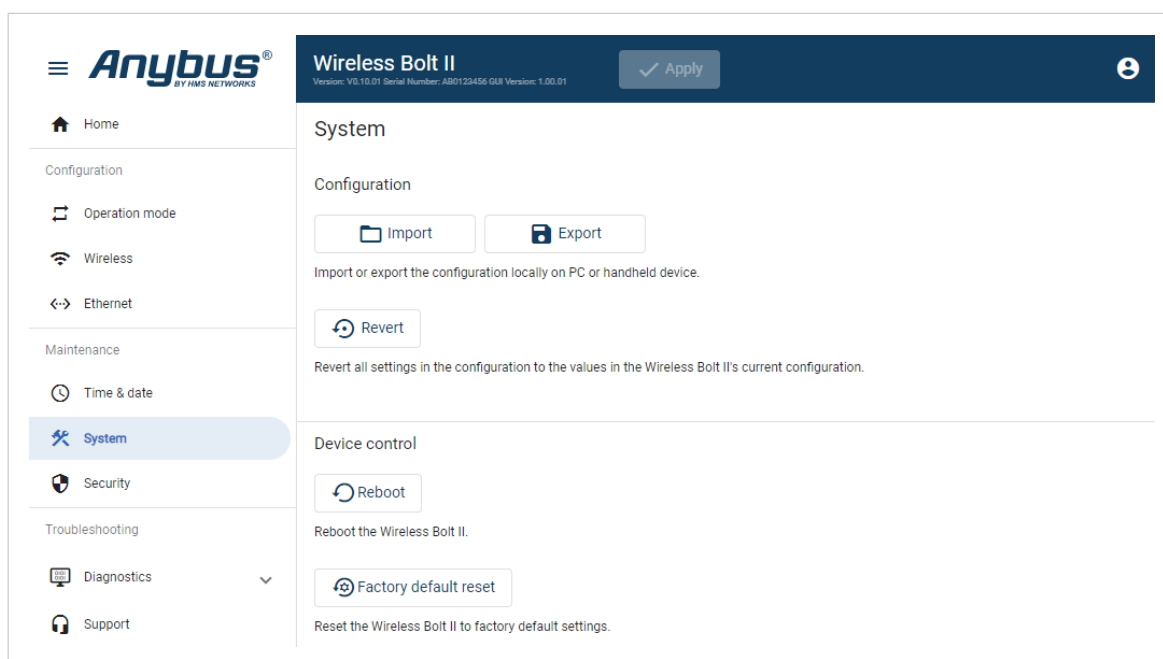


Figure 88. System page, Reboot



4. To confirm the reboot, click **Reboot**.

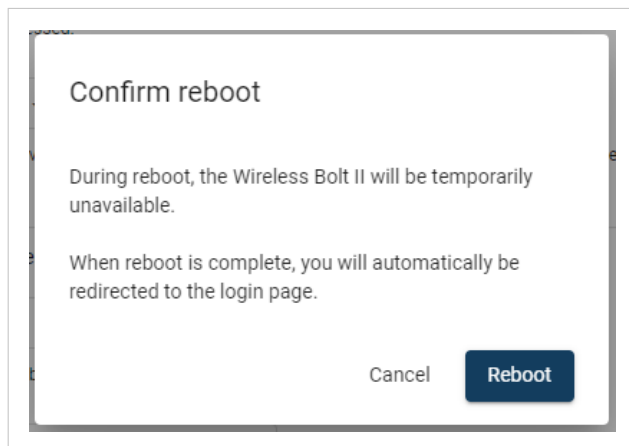


Figure 89. Confirm reboot

## Result

You are logged out of the Bolt II built-in web interface and redirected to the login page.

## 9.5. Factory Reset Using the Reset Button

### Before You Begin

Factory reset will reset any on site made configuration changes and set the Bolt II to the same state as leaving HMS production.

If the Firmware has been updated, factory reset will revert the Bolt II to the default configuration provided by the firmware.

During reset, the Bolt II is temporarily unavailable for approximately three minutes.

### Procedure

1. Ensure that the Bolt II is powered on.

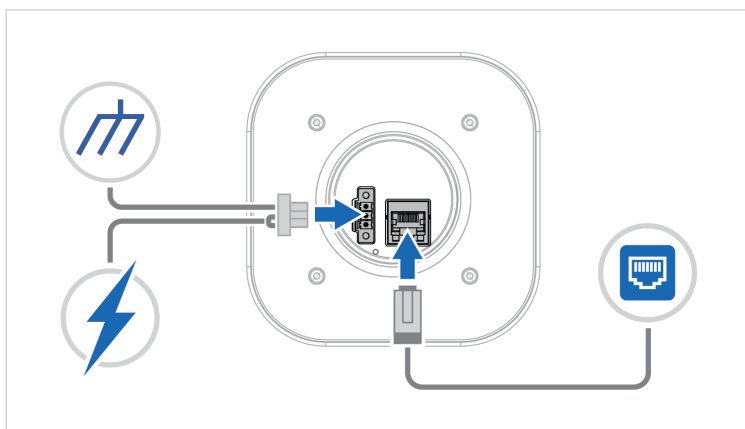


Figure 90. Power on the Bolt II

2. Use a pointed object, such as a paper clip to press and hold the **Reset** button for > 10 seconds.

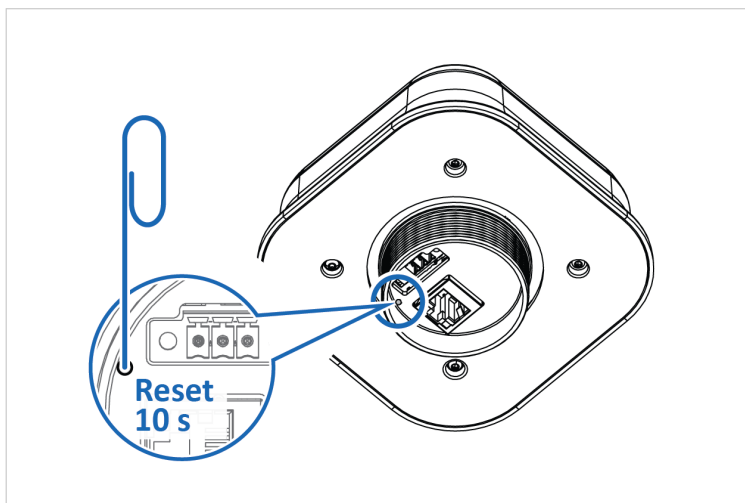


Figure 91. Press and hold **Reset** button

3. Release the **reset** button and wait while the Bolt II reboots.

### Result

When the Bolt II has successfully rebooted, the Bolt II configuration is reset to the factory default configuration.

## 9.6. Reset Using the Built-In Web Interface

### Before You Begin

Factory reset will reset any on site made configuration changes and set the Bolt II to the same state as leaving HMS production.

If the Firmware has been updated, factory reset will revert the Bolt II to the default configuration provided by the firmware.

During reset, the Bolt II is temporarily unavailable for approximately three minutes.

### Procedure

1. Ensure that the Bolt II is powered on and running.

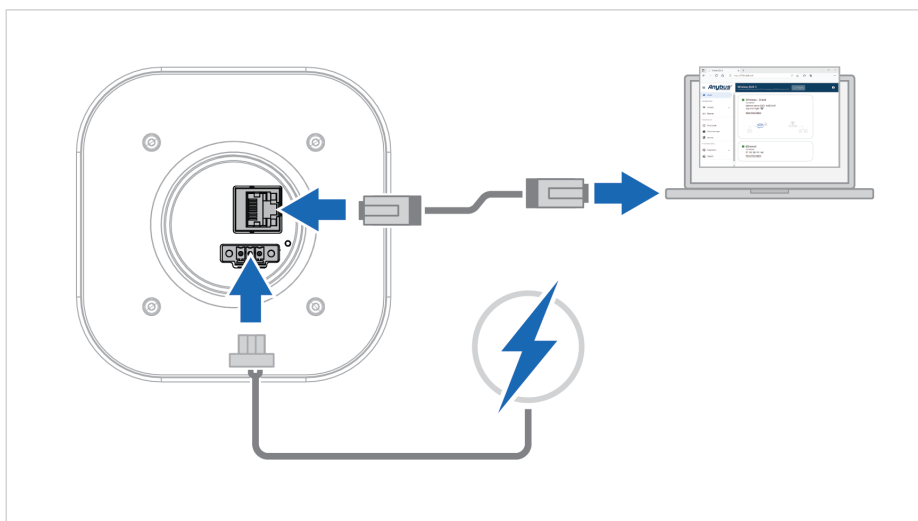


Figure 92. Power on the Bolt II

2. Log in to the Bolt II built-in web interface.
3. On the **System** page, click **Factory default reset**.

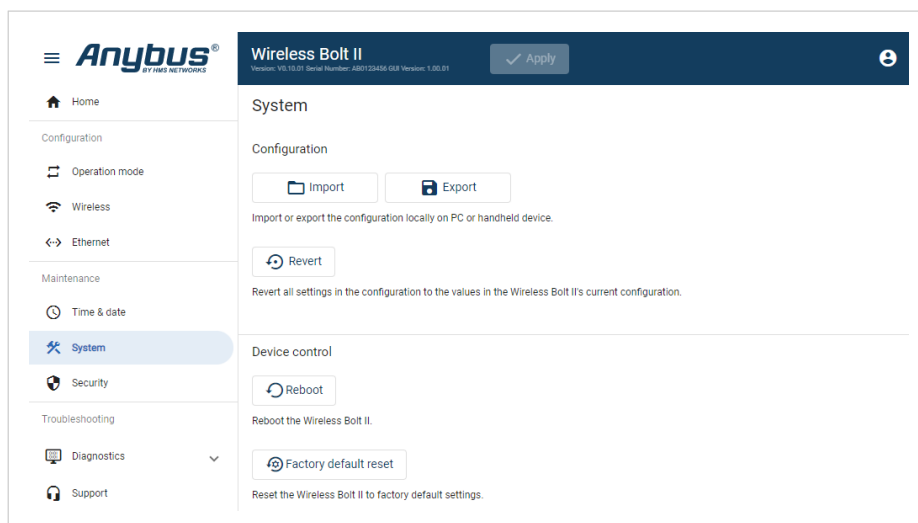


Figure 93. System page, Factory default reset

4. To confirm the factory default reset, click **Reset**.

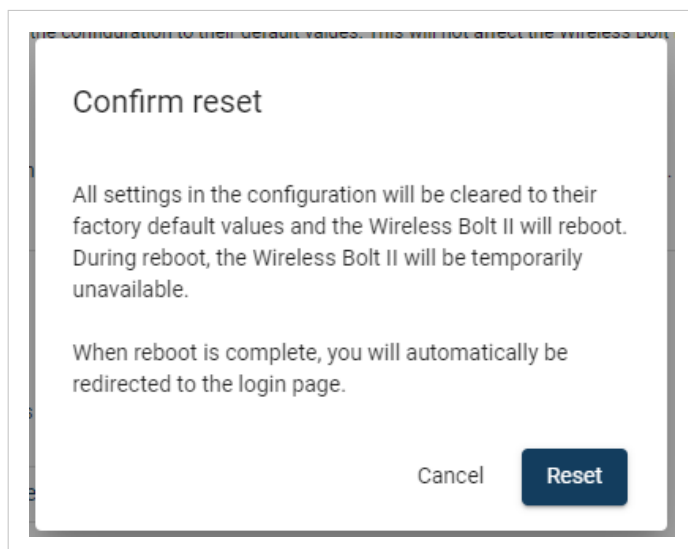


Figure 94. Confirm factory default reset

## Result

You are logged out of the Bolt II built-in web interface and redirected to the login page.

When the Bolt II has successfully rebooted, the Bolt II configuration is reset to the factory default configuration.

## 9.7. Support

### 9.7.1. Support Package

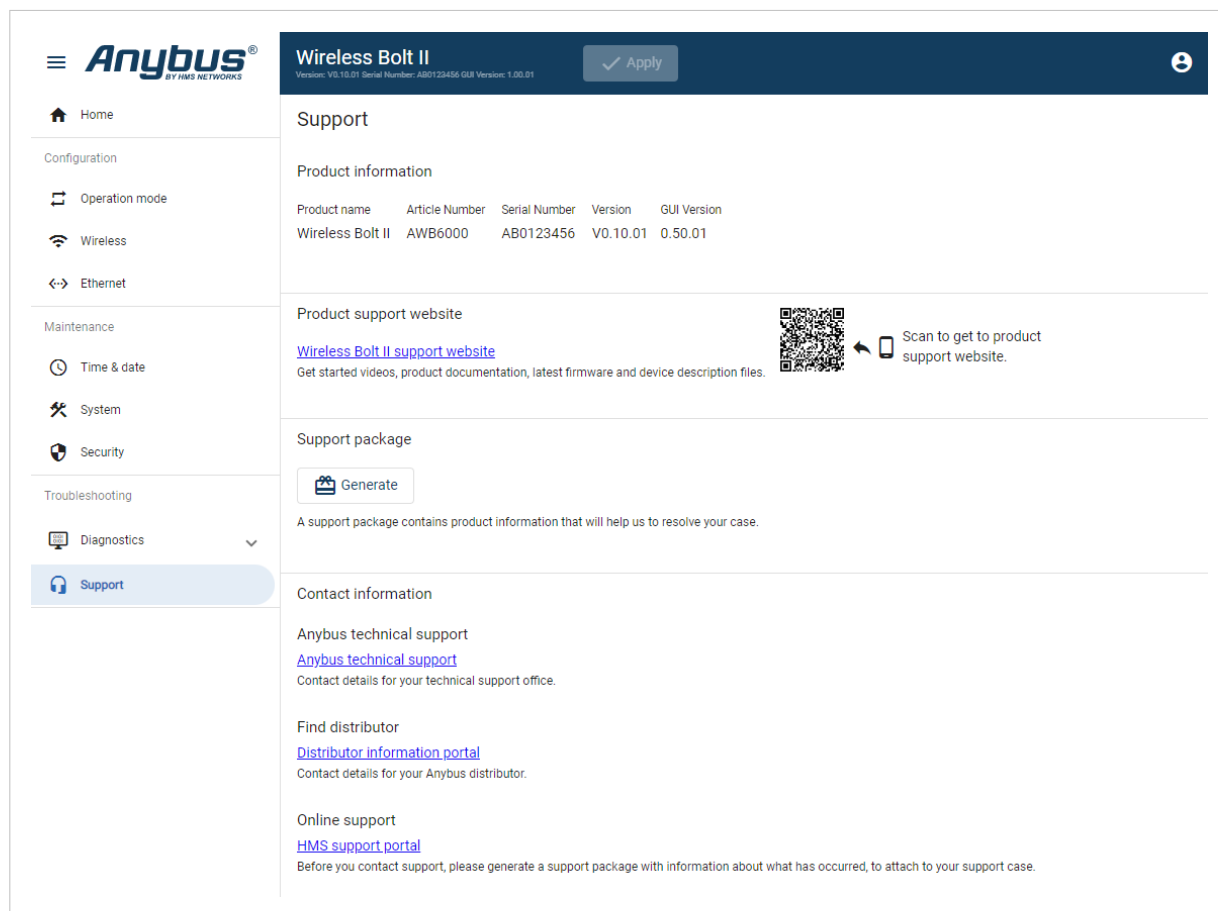


Figure 95. Support page example

Before you create a ticket for technical support, generate a support package.

The support package contains information about what has occurred and will help the Anybus technical support team resolve the support case as quickly and efficiently as possible.

#### Support Package Content

The information in the support package is available to open and read, the files are not locked or encrypted.

#### Generate Support Package

On the **Support** page, click **Generate**.

A zip file with the support files is downloaded to your PC.

#### Create a Support Ticket

1. On the **HMS Networks** home page, navigate to the **Support** main menu and click **Support portal**.
2. In the **Support portal**, create a support ticket and upload the support package.

## 10. Technical Data

### 10.1. Technical Specifications

Model identification	AWB6BA
Communication connector	RJ45
Power connector	3-pole push-in spring connection
Power supply	Recommended: 12–24 VDC Reverse voltage protection Min: 10 VDC Max: 33 VDC Max power: 2.5 W
Power over Ethernet (PoE)	IEEE 802.3af/802.3at Type 1 Class 3 Typical: 1.45 W Max: 2.7 W Voltage range: 37-57 V
Power consumption	Typical: 60 mA @ 24 V Max: 110 mA @ 24 V
Antenna	MIMO 802.11 a/b/g/n and 802.11ac
Wireless LAN	2.4 GHz, channel 1-11 5 GHz Access Point: 36-48 (U-NII-1) 5 GHz Client: 100-116 + 132-140 and 120-128 (U-NII-1, U-NII-2, U-NII-2e) depending on regulatory domain scan RF output power: 18 dBm
Storage temperature	-40 to +85 °C
Operating temperature	-25 to +65 °C
Humidity	EN 60068-2-78: Damp heat, +40°C, 93% humidity for 4 days.
Vibration	See datasheet
Housing material	Plastic (see data sheet for details) Aluminum (see data sheet for details)
Protection class	Top (outside of host): IP66 / UL Type 4X Base (inside of host): IP30
Product weight	284 g
Dimensions	113 x 59 x 113 mm (W x H x D)
Mounting	M50 screw and nut. 50.5 mm hole needed.

Additional technical data and information related to the installation and use of this product can be found at [www.hms-networks.com](http://www.hms-networks.com).