ENGLISH

Anybus® Wireless Bolt II™

USER MANUAL

SCM-1202-209
Version 1.0
Publication date 2023-03-21

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.

Contact Information
Postal address:
Box 4126
300 04 Halmstad, Sweden

E-Mail: info@hms.se

Table of Contents

1. Preface 1
1.1. About This Document 1
1.2. Document Conventions 1
1.3. Trademarks 2

2. Safety 3
2.1. General Safety 3
2.2. Intended Use 3

3. Preparation 4
3.1. Cabling 4
3.2. Network Environment 4
3.3. Placement Considerations 4
3.4. System Requirements 4
3.4.1. Supported Operating Systems 4
3.5. Support and Resources 5
3.6. HMS Software Applications 5
3.7. Third-Party Software Applications 5

4. Installation 6
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

5. Configuration 14
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 18
5.3. Bolt II Built-In Web Interface Overview 19
5.4. Wireless Bolt II Operation Modes 20
5.5. Cable Replacement Mode Setup 21
5.6. Access Point Mode Setup 25
5.7. Wireless Settings 28
5.7.1. Cable Replacement Device A Settings 28
5.7.2. Cable Replacement Device B Settings 30
5.7.3. Access Point Settings 32
5.7.4. WLAN Channels and World Mode 33
5.8. Ethernet Settings 34
5.8.1. To Configure IP Settings Manually 34
5.8.2. To Use DHCP Client 35
5.9. Apply Configuration 36

6. Verify Operation 37
6.1. Bolt II Status Monitor 37
6.2. Ethernet LED Indication 39

7. Use Cases 40
7.1. Cable Replacement Between a PLC and a Network Switch 40
7.2. Access PLC from Handheld Device via Wi-Fi 44

8. Maintenance 48
8.1. Time & Date Settings 48
8.1.1. Set Time 48
8.1.2. Network Time Protocol (NTP) Synchronization 49
8.1.3. Use Timezone Settings 50
8.2. Configuration File Handling 51
8.2.1. Export Configuration 51
8.2.2. Import Configuration 52
8.3. Revert Configuration 53
8.4. Firmware Management 54
8.4.1. View the Firmware Version 54
8.4.2. Firmware and Configuration Compatibility 54
8.4.3. Firmware File Validation 54
8.4.4. Update Firmware 55
8.5. Web Server Certificate Settings 56
8.6. Change the Bolt II Password 58

9. Troubleshooting 59
9.1. Diagnostics 59
9.1.1. Event Log 59
9.1.2. Remotely Monitor the Bolt II Status 60
9.2. Find the Bolt II IP Address 60
9.3. Reboot Using the Reset Button 61
9.4. Reboot Using the Built-In Web Interface 62
9.5. Factory Reset Using the Reset Button 64
9.6. Reset Using the Built-In Web Interface 65
9.7. Support 67
9.7.1. Support Package 67

10. Technical Data 68
10.1. Technical Specifications 68

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.anybus.com/support.

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.anybus.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.

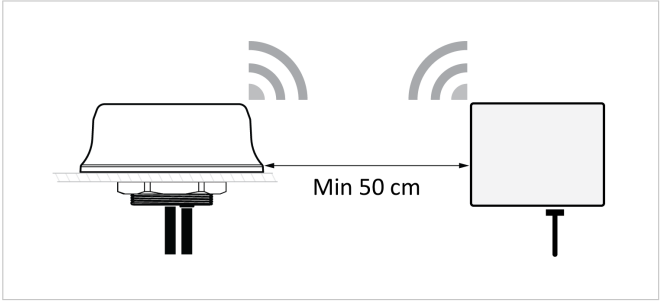


Figure 1. Required minimum distance between wireless devices

3.4. System Requirements

3.4.1. 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

3.5. Support and Resources

For additional documentation and software downloads, FAQs, troubleshooting guides and technical support, please visit www.anybus.com/support.

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.

3.6. HMS Software Applications

Download the software installation files and user documentation from www.anybus.com/support.

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.

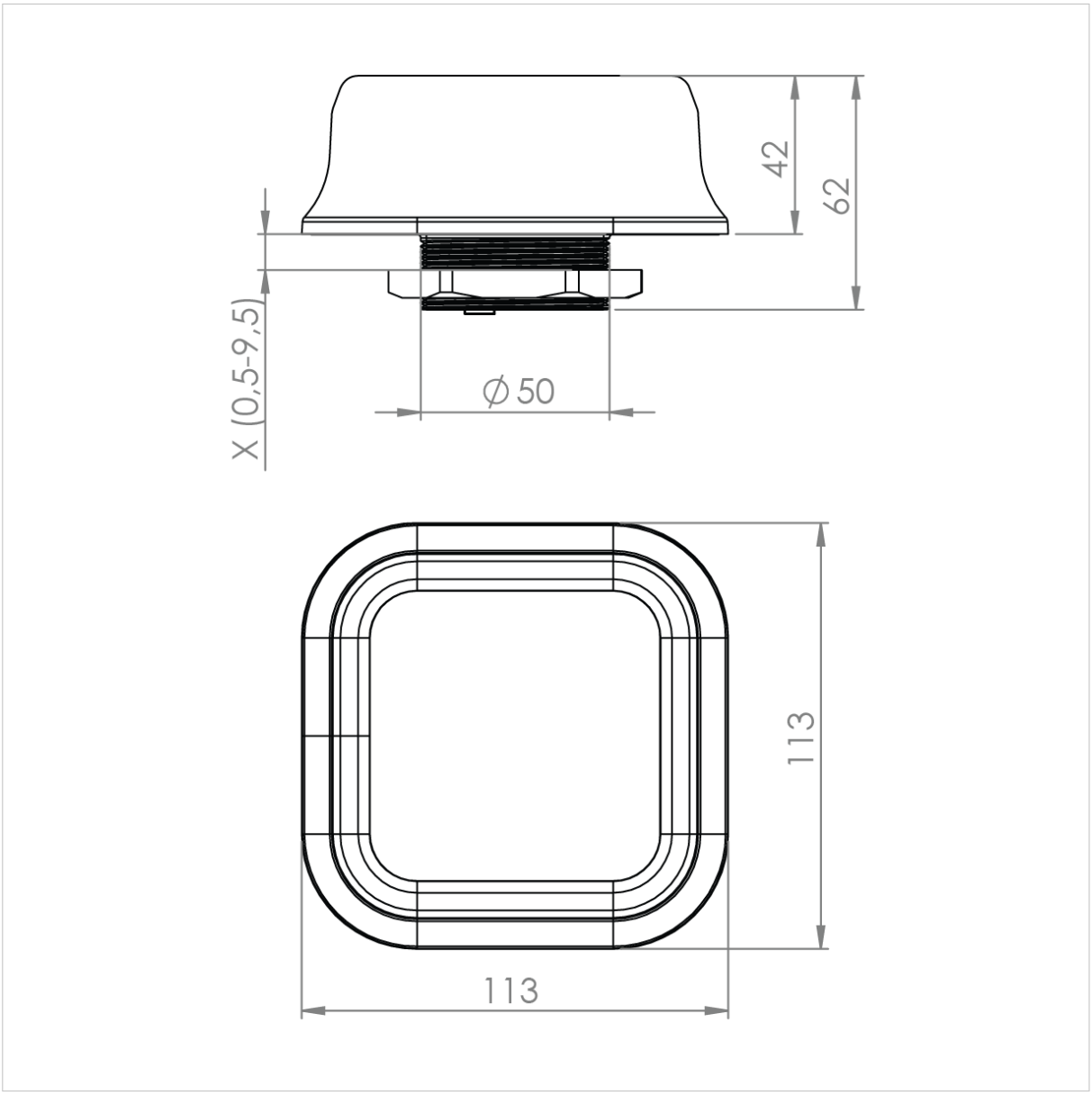
3.7. Third-Party Software Applications

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

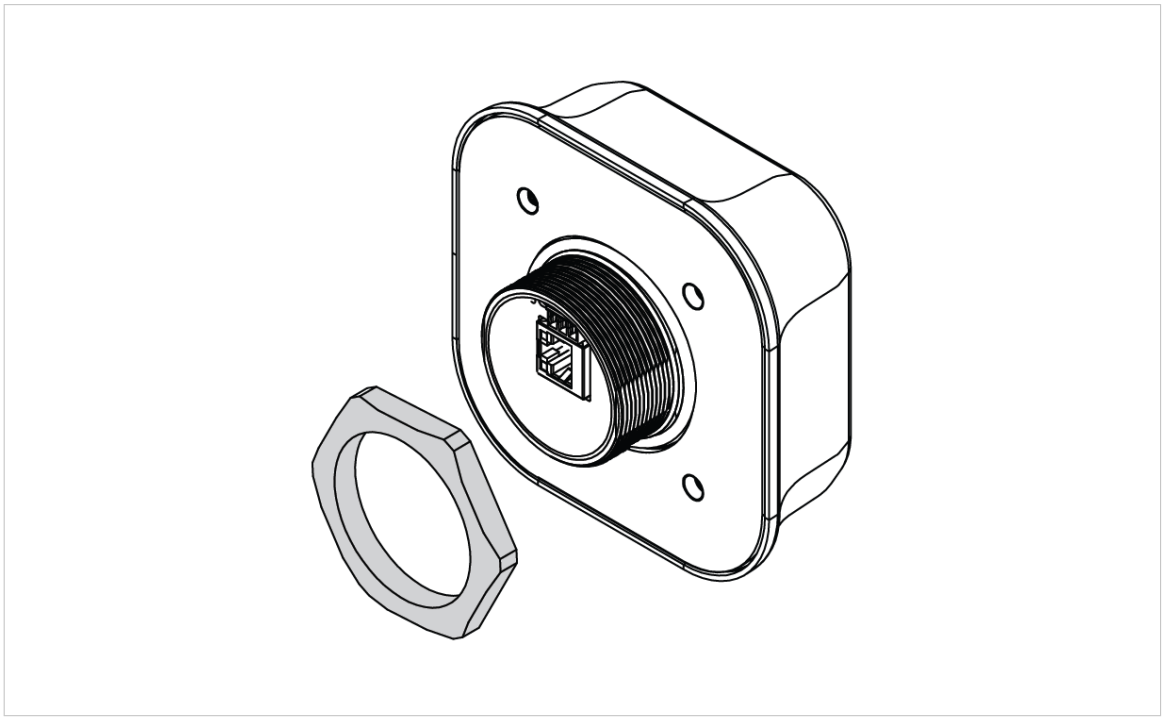
For information about placement for optional reception, see Placement Considerations (page 4).

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 ±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.

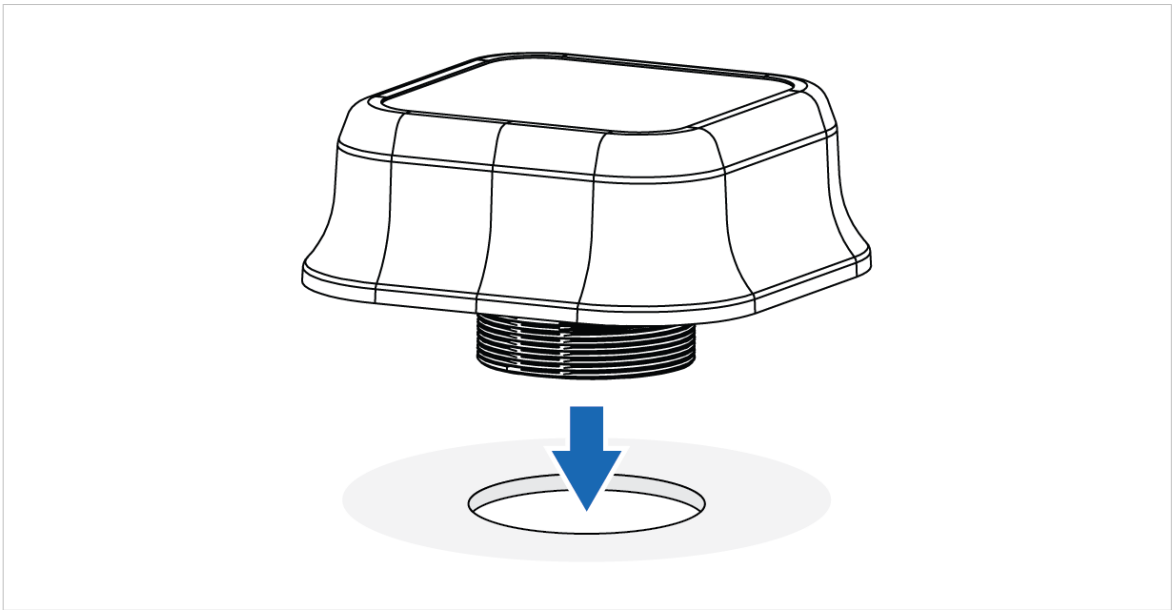
Mounting Procedure

1. Unscrew and remove the Bolt II lock nut.



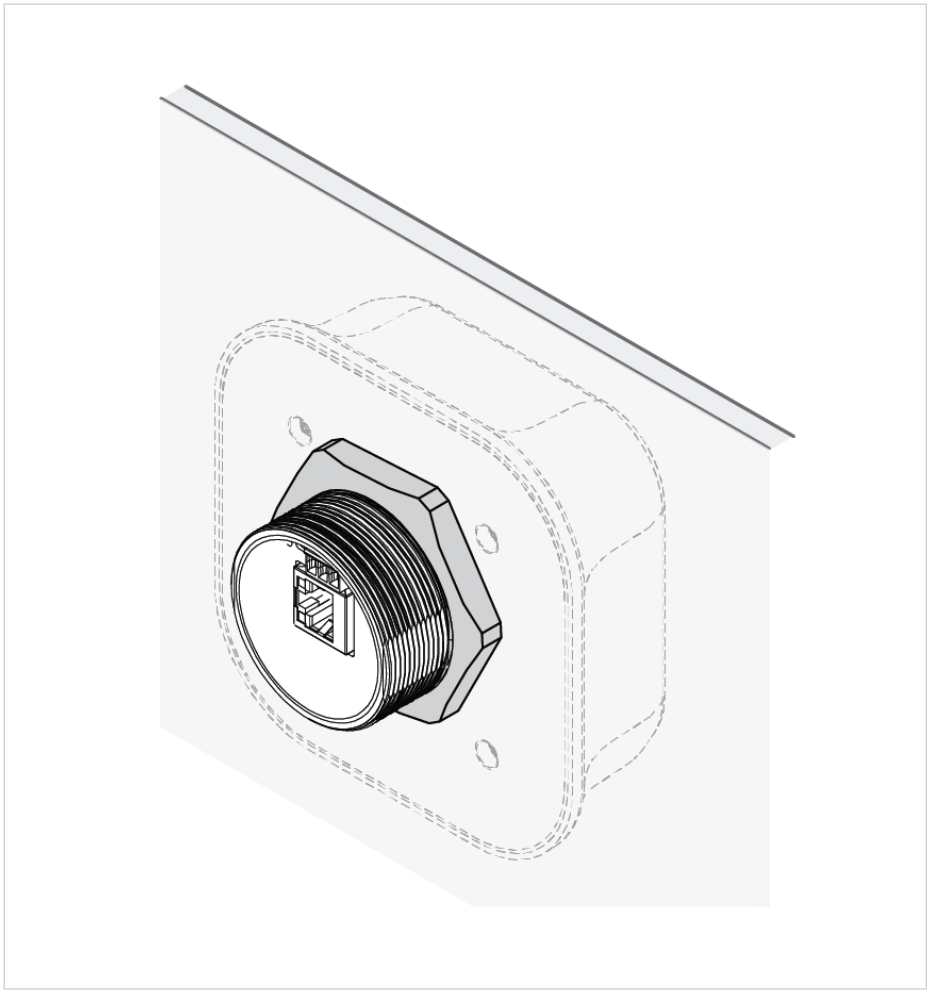
2. Place the Bolt II housing sealing ring in its groove.

3. In the mounting surface, drill a mounting hole with the size Ø 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 ±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

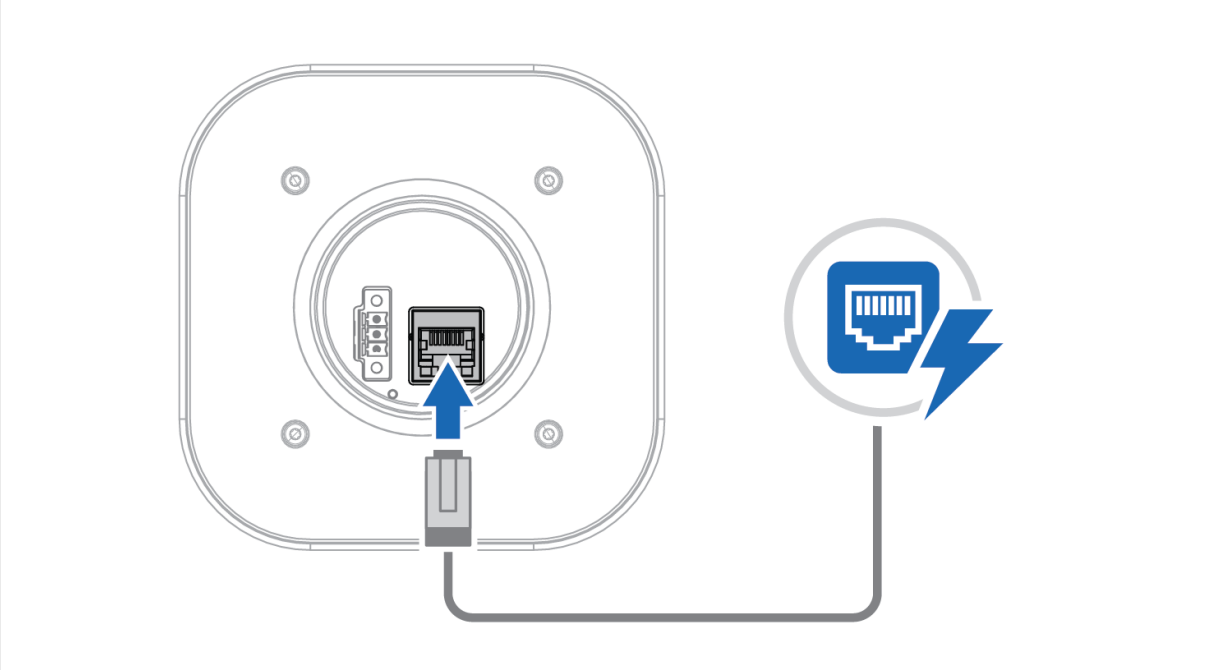


Figure 3. Connect to Power Over Ethernet (PoE)

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

RJ45 Ethernet PoE Connector

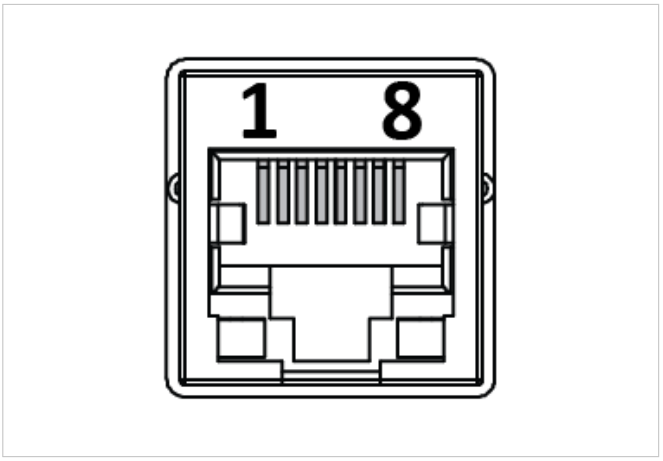


Table 1. RJ45 Ethernet PoE Connector pinning

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^2 (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.

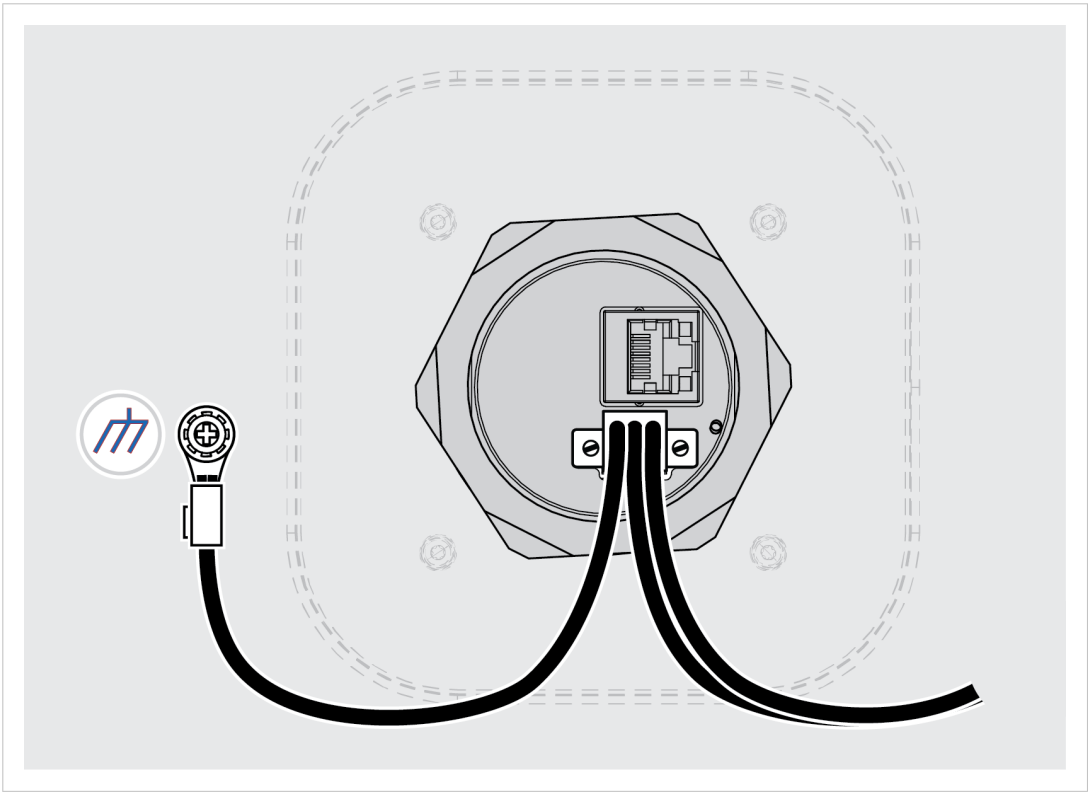


Figure 4. Functional earth wire screw placement, view from below

Procedure

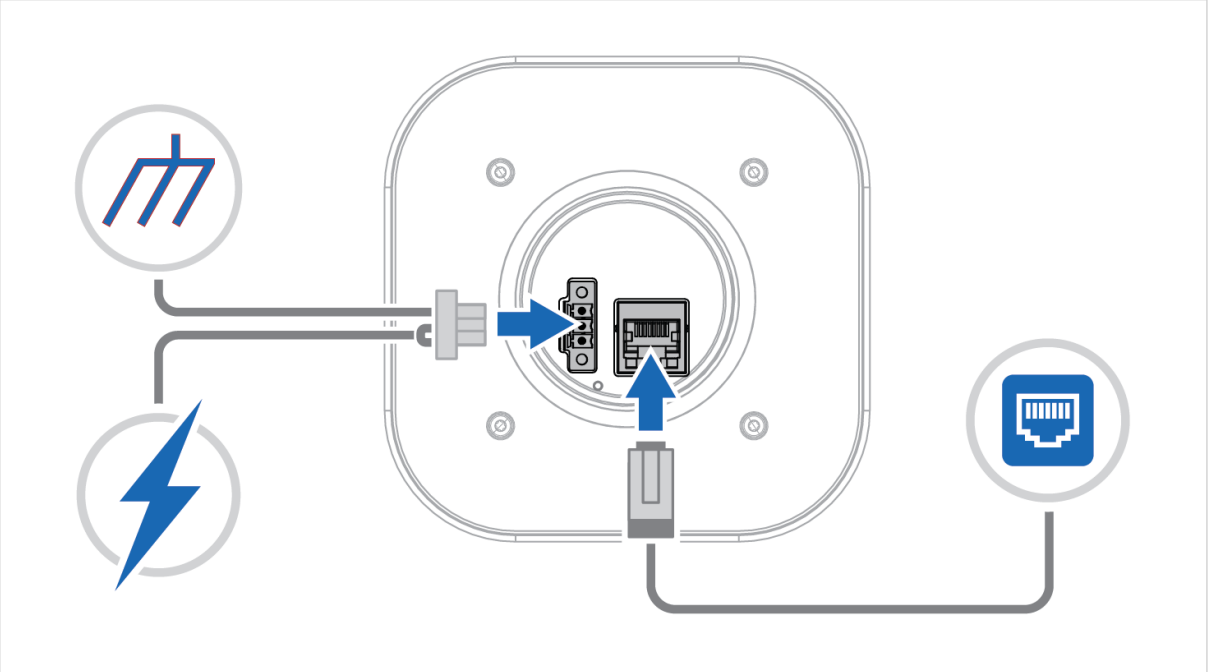


Figure 5. Connect Power, Functional Earth (FE) and Ethernet

Power Connector 3-Pin

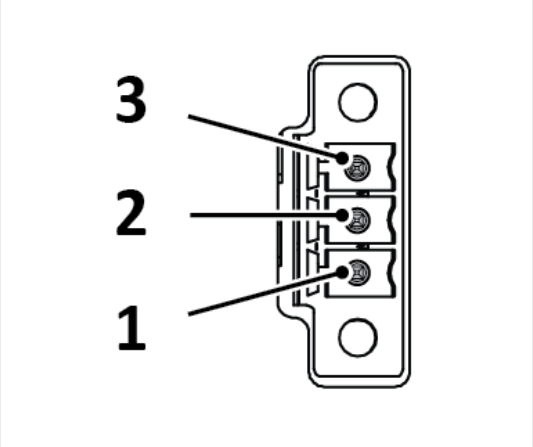


Table 2. Power connector, 3-pin terminal block

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.

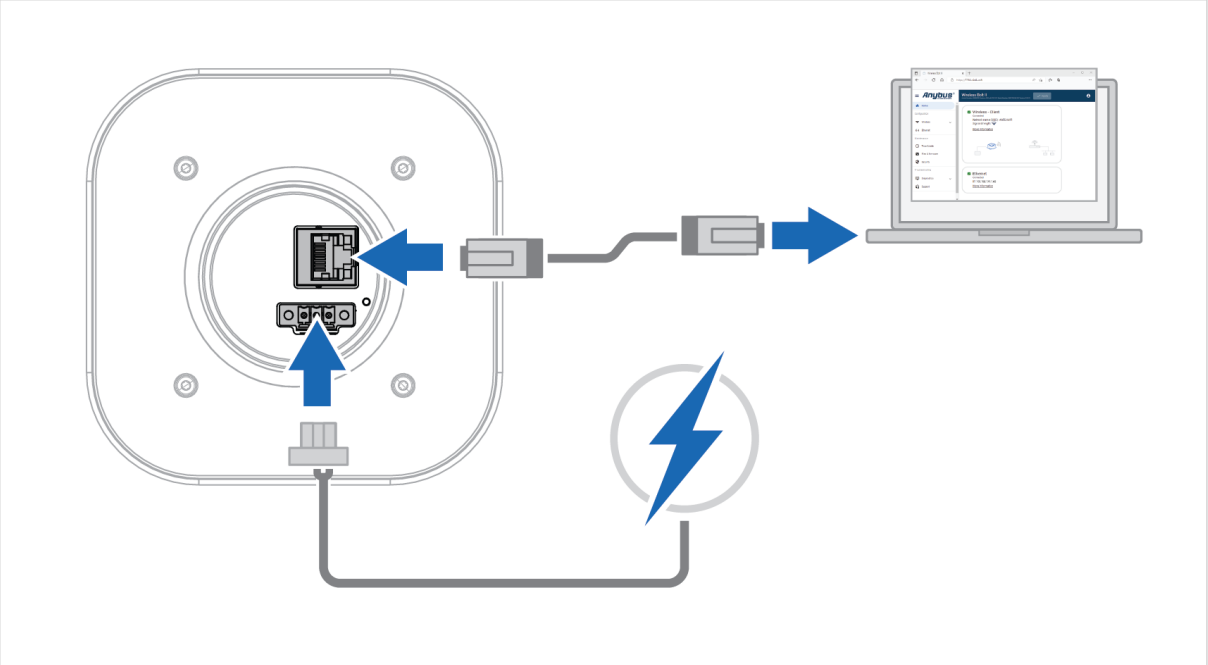


Figure 6. Configure the Bolt II using a PC

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

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

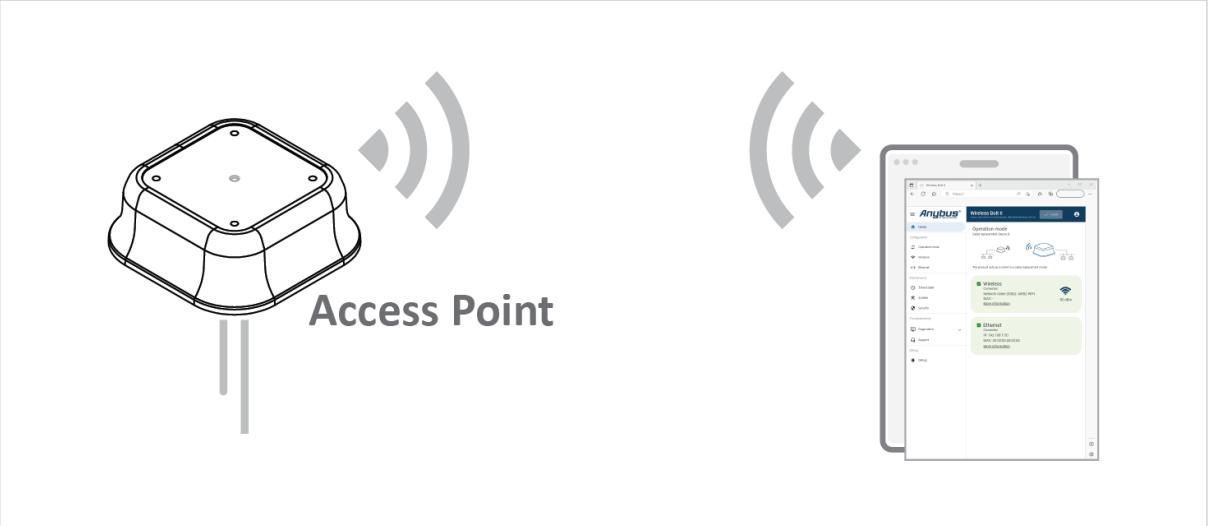


Figure 7. Configure the Bolt II using a wireless device

On the wireless device:

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

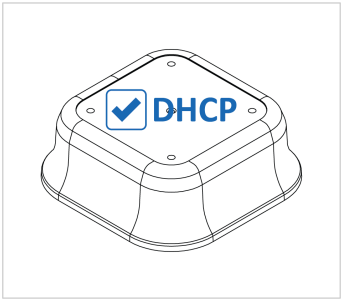
5.2. Access the Built-In Web Interface

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 Client



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

If the **DHCP client** 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

NOTE
When you change to a static IP address on your PC, internet access is lost.

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 and search 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 cyber security 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 58).

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 and the Bolt II IP address.

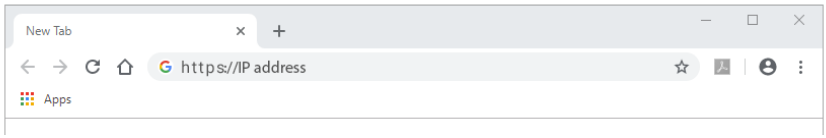


Figure 8. Enter IP address in web browser

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 Settings (page 56).

4.

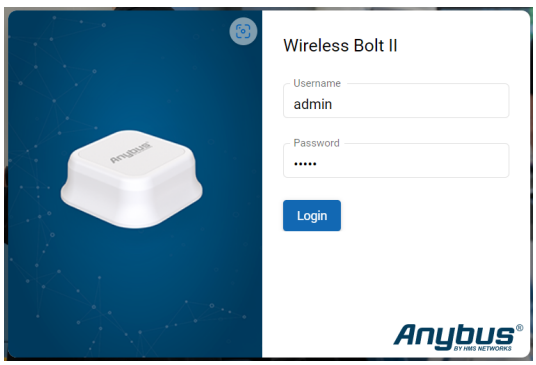


Figure 9. Built-in web interface login screen

Result

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

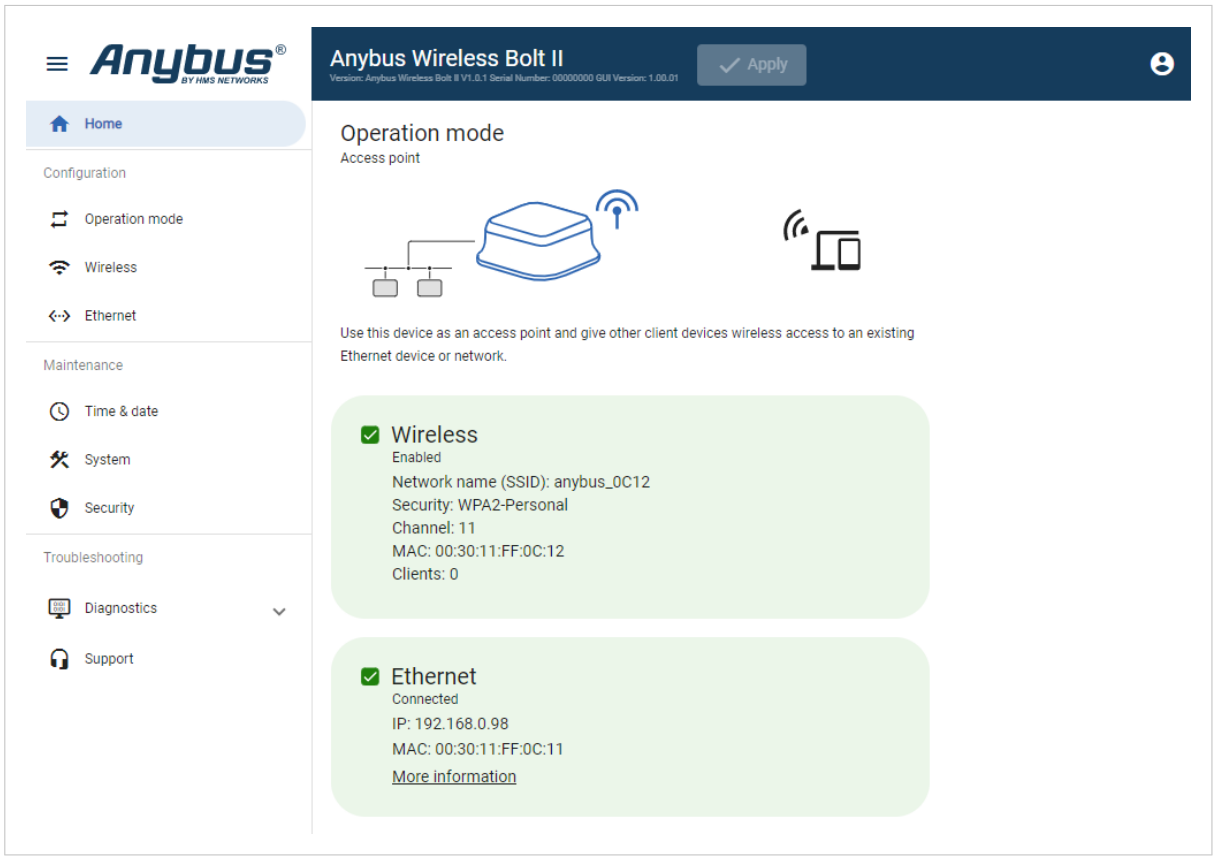


Figure 10. **System Overview** page

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

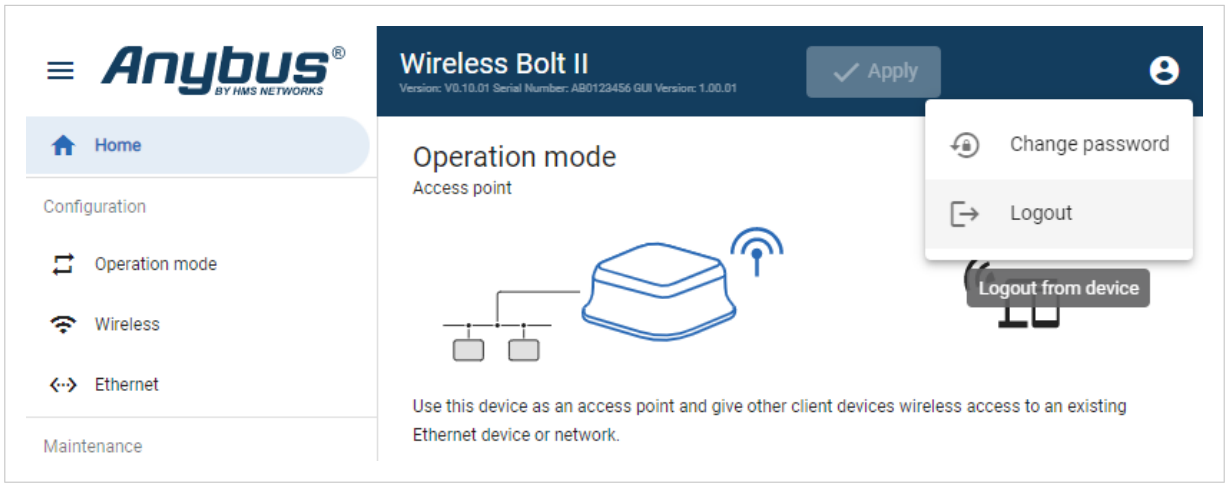


Figure 11. Account menu, Logout

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.

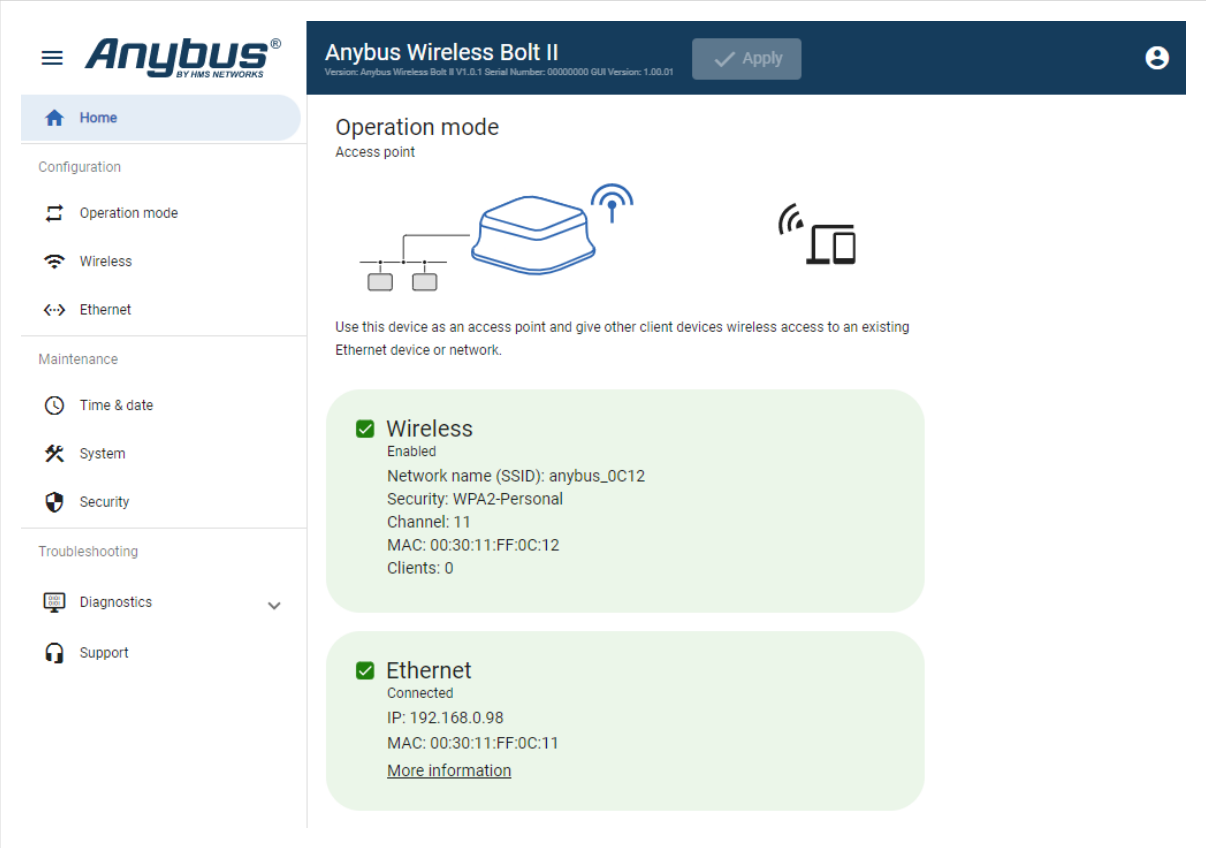


Figure 12. The Bolt II built-in web interface Home page

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 **Operation mode**: • **Cable replacement**: **Cable replacement Device A** or **Cable replacement Device B** • **Access point**
Wireless	Configure the **Wireless** settings for the selected **Operation mode**.
Ethernet	Configure the **Ethernet** network **IP Settings**.
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 **Apply** to make the settings take effect.

5.4. Wireless Bolt II Operation Modes

Bolt II comes with two Wireless Mode types: Cable replacement and Access Point.

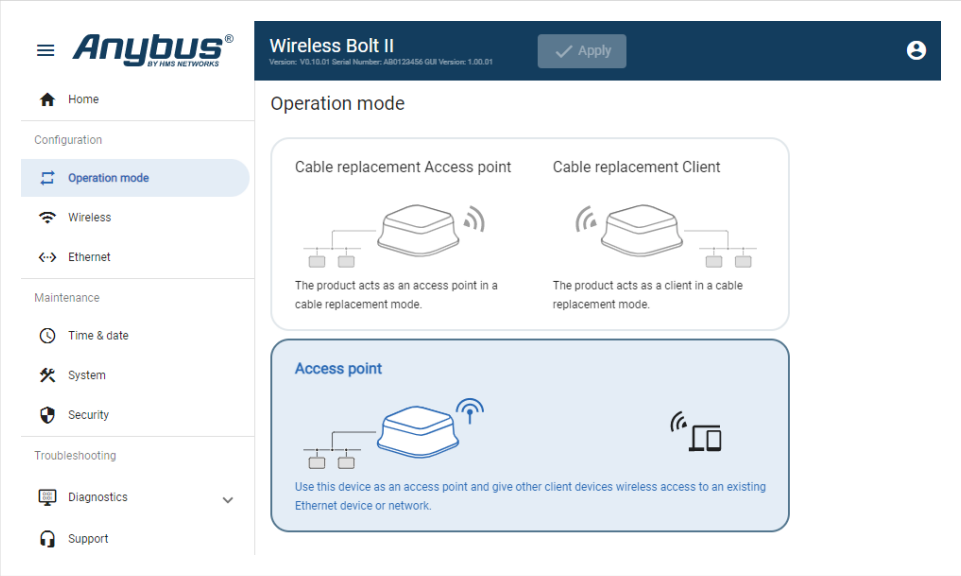


Figure 13. Bolt II Mode page

Cable Replacement

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

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

See also Cable Replacement Mode Setup (page 21).

Access Point

This 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 25).

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

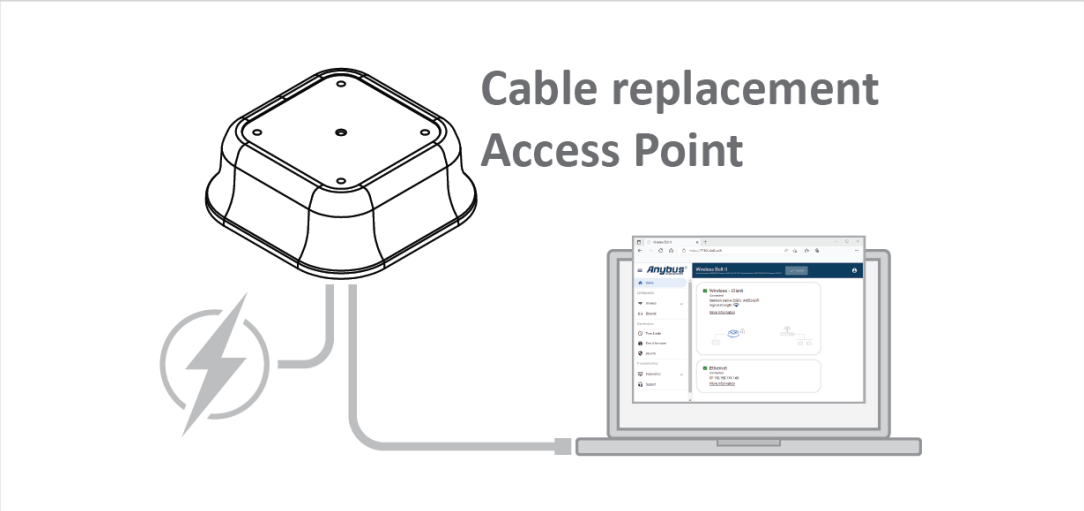


Figure 14. Configure the Bolt II Cable replacement access point

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 Device A** Mode.

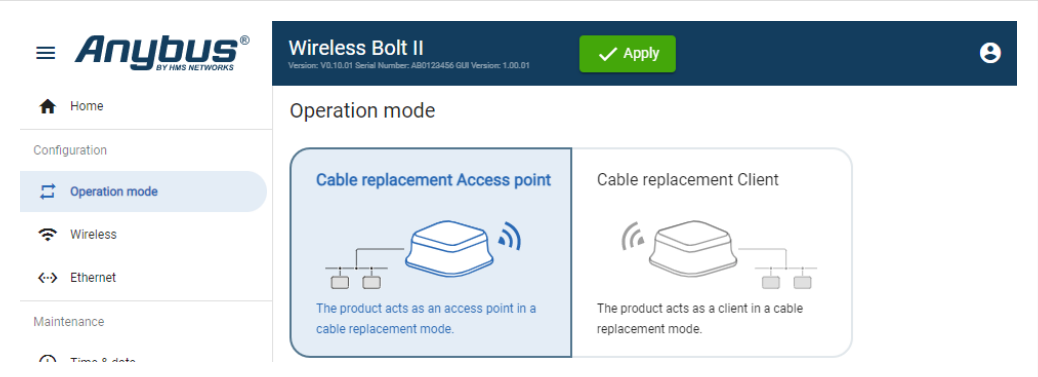


Figure 15. Select Cable replacement Device A

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

7. Configure the **Cable replacement Device A** settings.
   See also Cable Replacement Device A Settings (page 28).

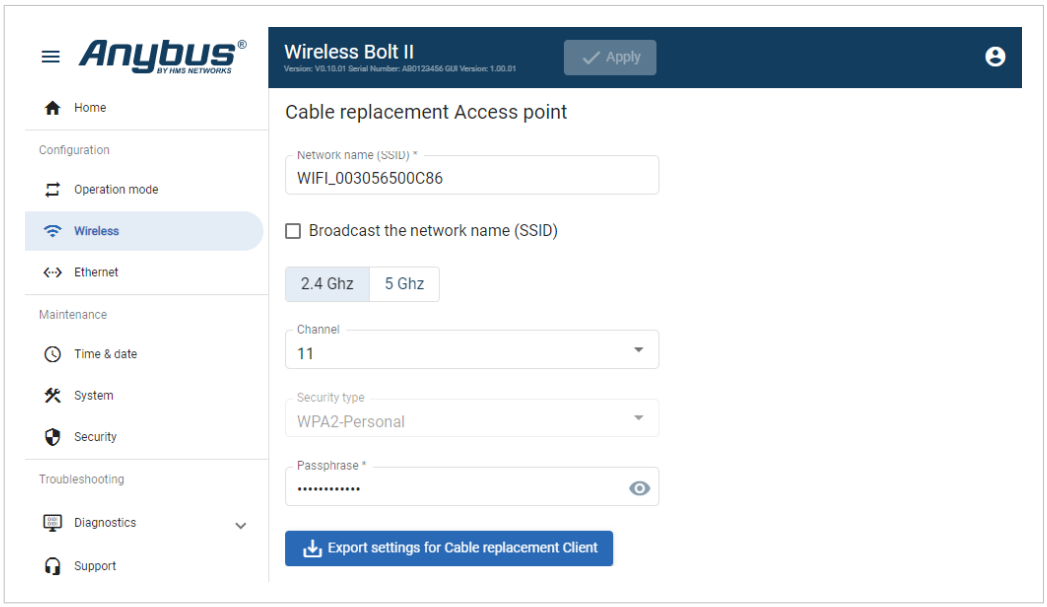


Figure 16. **Cable replacement Device A** settings page

8. Optional step: To use the same settings when configuring the Bolt II client unit B, click **Cable replacement Device B** and follow the instructions.
   See also Export Cable Replacement Device A Settings (page 29).

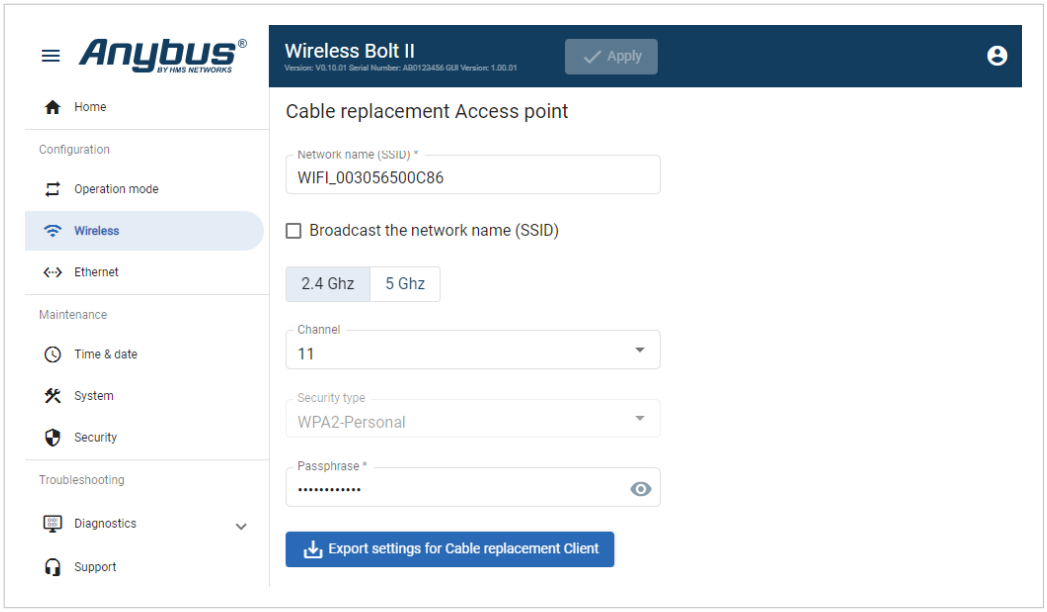


Figure 17. **Cable replacement Device A** page, export settings

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

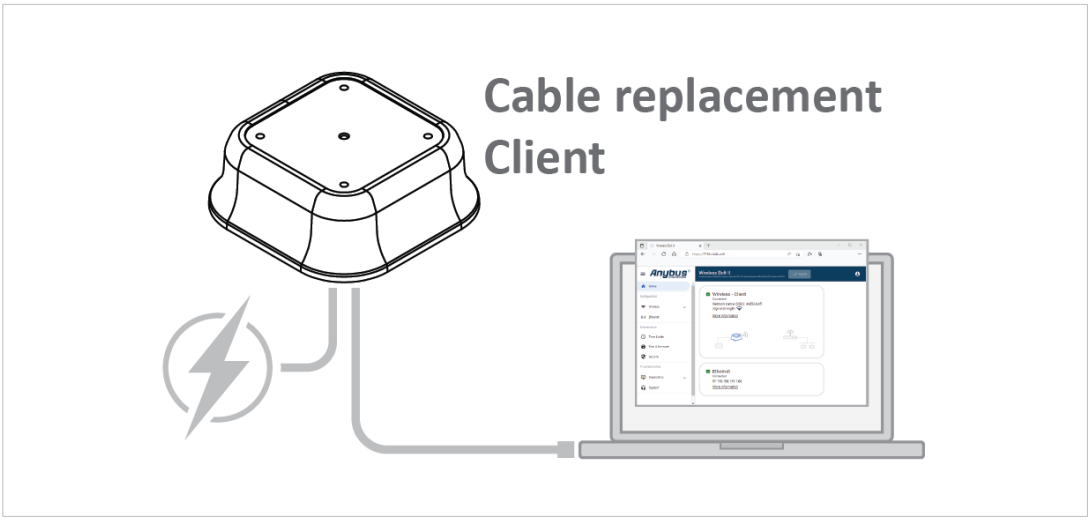


Figure 18. Configure the Bolt II Cable replacement client

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 Device B** Mode.

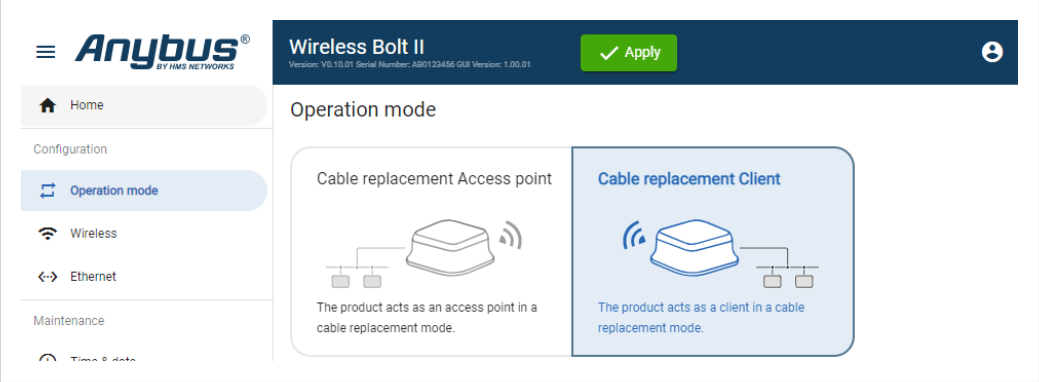


Figure 19. Select Cable replacement Device B

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

7. Configure the **Cable replacement Device B** settings.
   - To configure the settings manually, see Cable Replacement Device B Settings (page 30).
   - Option when you want import the settings used for the Bolt II Cable replacement access point, see Import Cable Replacement Device A Settings to Configure Cable Replacement Device B (page 31).

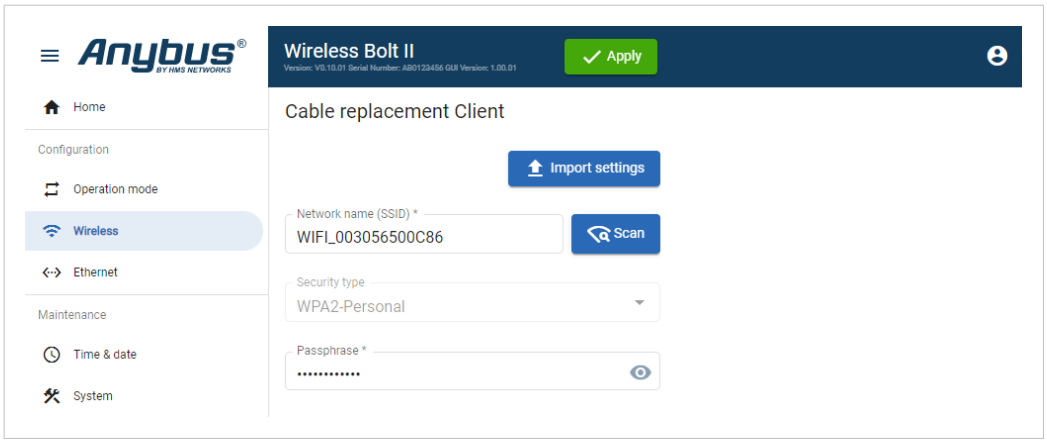


Figure 20. **Cable replacement Device B** page

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

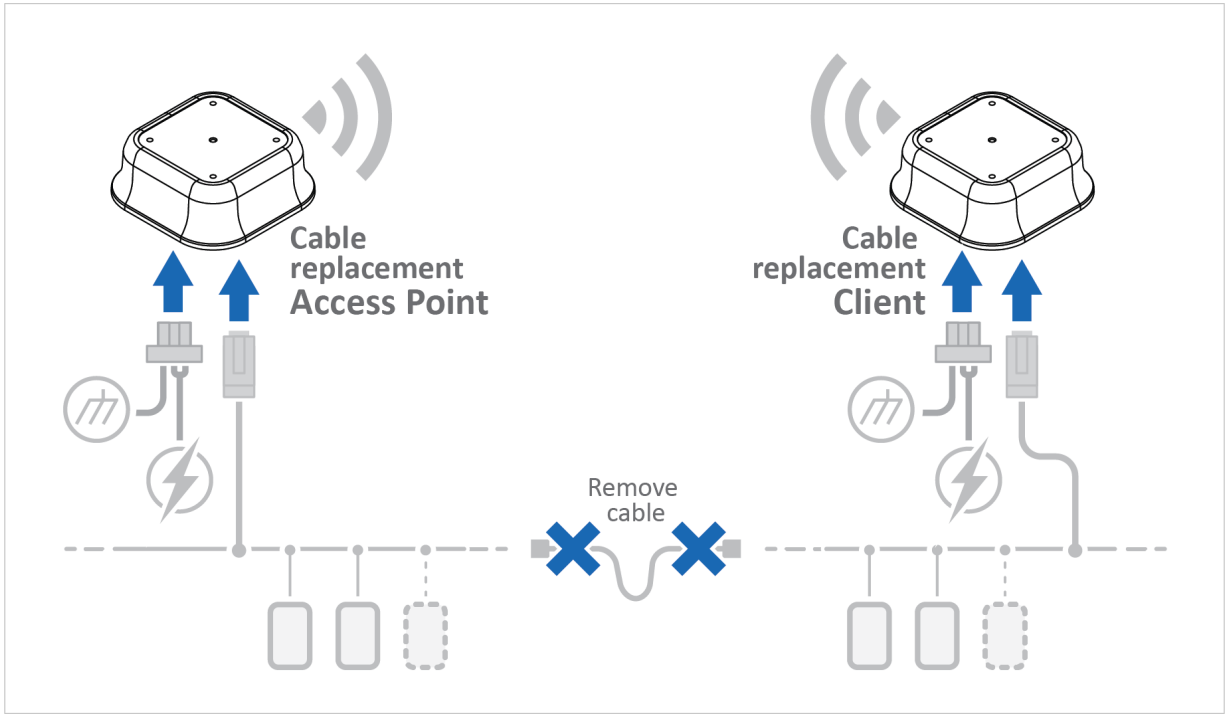


Figure 21. Install the Cable replacement Bolt II access point and Bolt II client

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

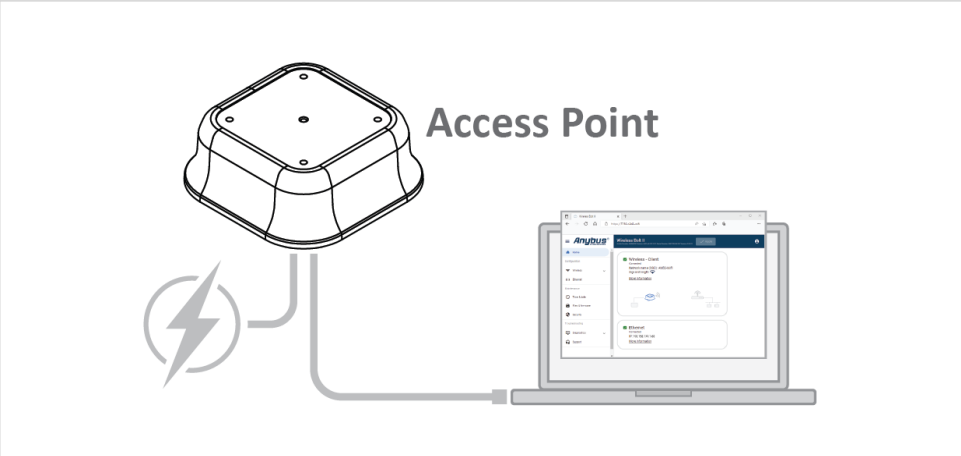


Figure 22. Connect the Bolt II access point to your PC and to power

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.

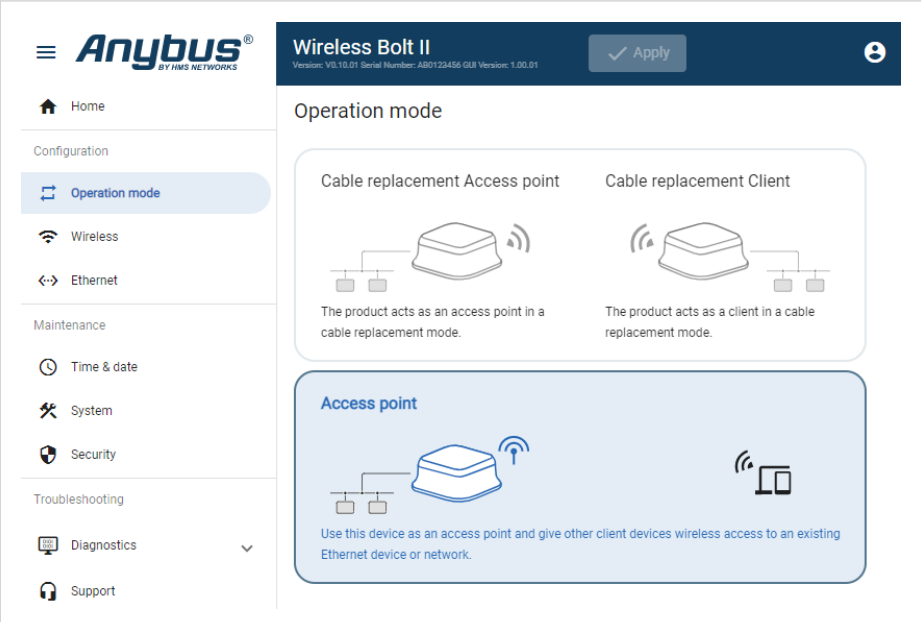


Figure 23. Access point Operation mode

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 32).

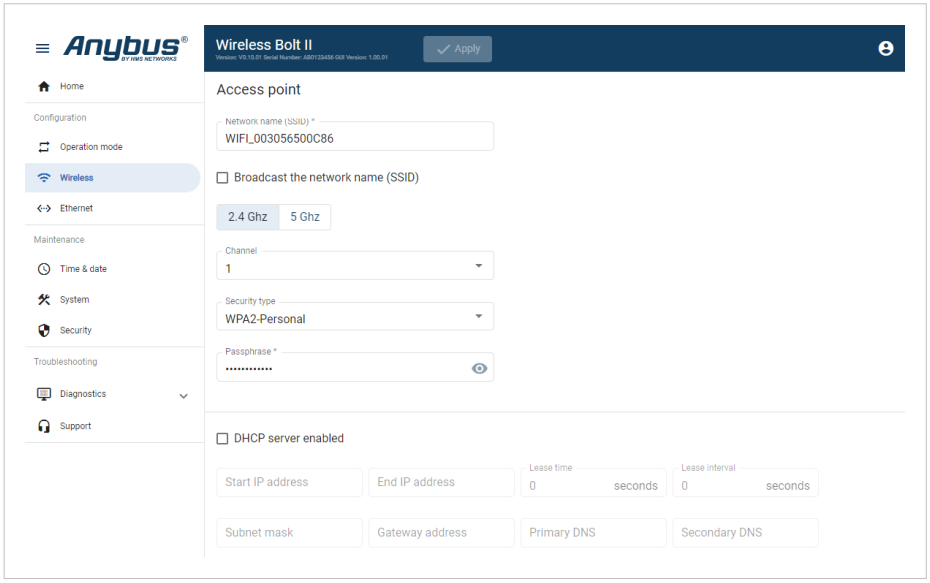


Figure 24. Wireless, **Access point** page

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

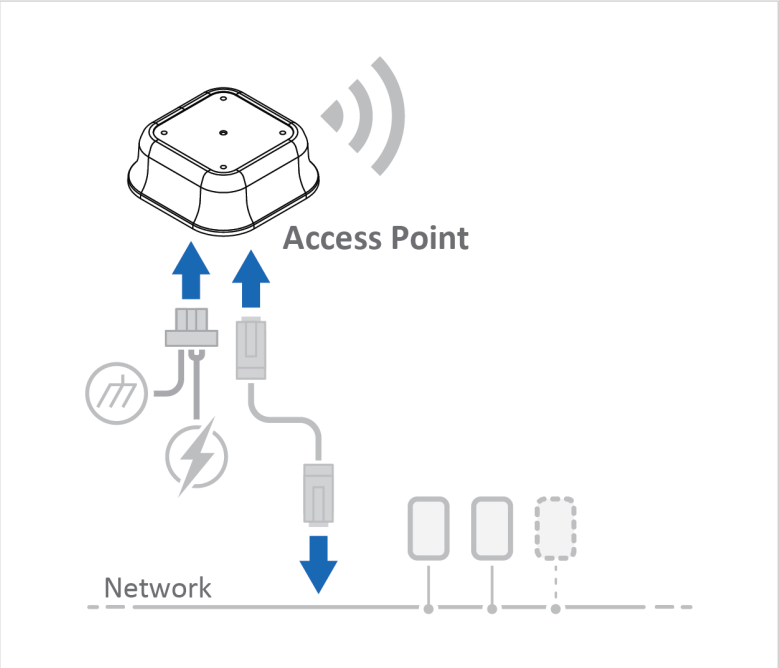


Figure 25. Install the Bolt II access point

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

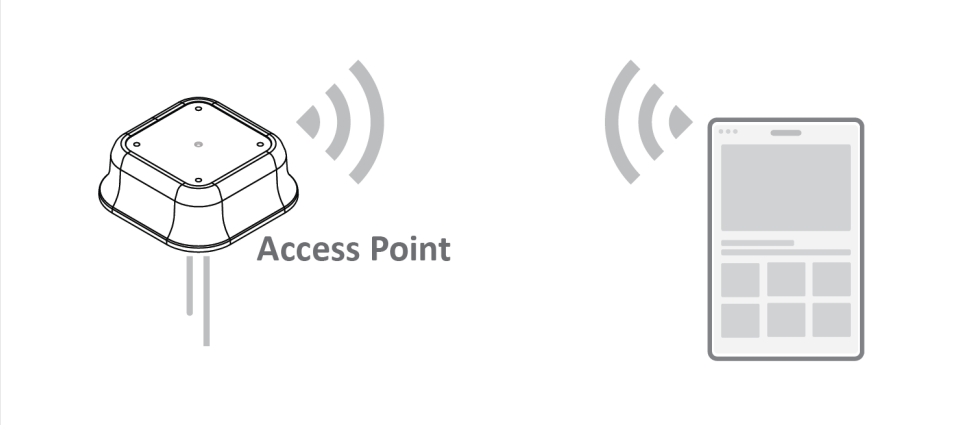


Figure 26. Connect wireless device(s) to Bolt II access point

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. Wireless Settings

5.7.1. Cable Replacement Device A Settings

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

On the **Wireless** settings page, configure the **Cable replacement Device A** settings for the Bolt II access point.

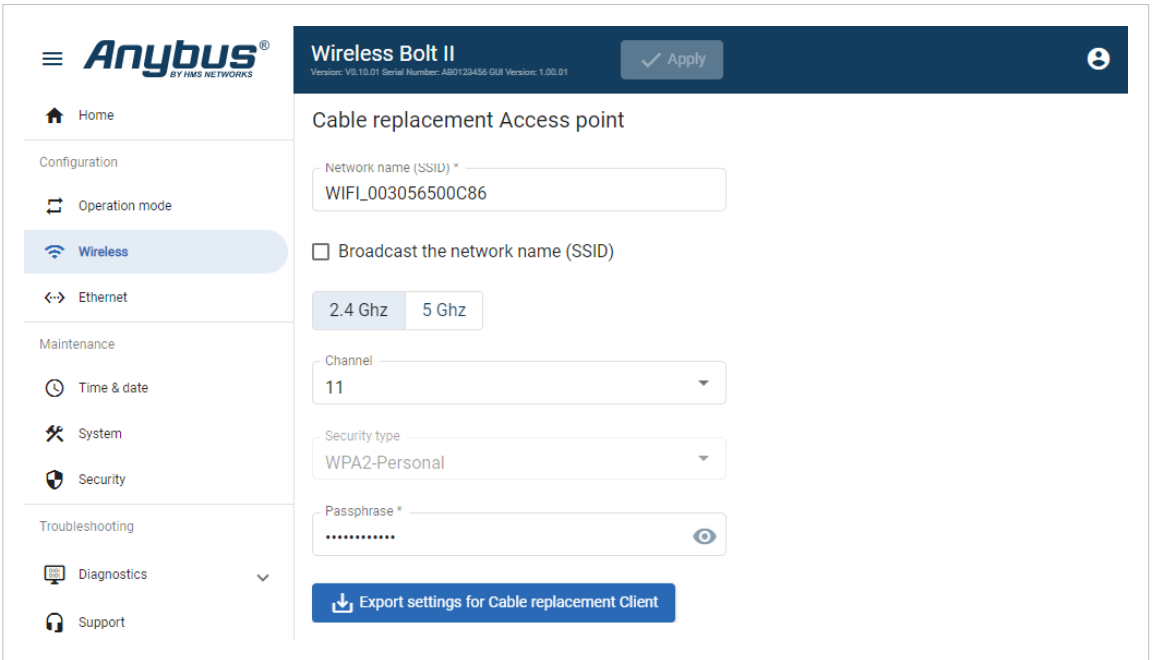


Figure 27. **Cable replacement Device A** page

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, **2.4 Ghz** or **5 Ghz**. See also WLAN Channels and World Mode (page 33).
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 **Broadcast the network name (SSID)** 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 **Channel** for the radio frequency band. See also WLAN Channels and World Mode (page 33).
Security type	Open (Not recommended) WPA2-Personal, Default WPA3-Personal	Select a **Security type** for the wireless connection. **NOTE** For **Cable Replacement Device A** the Security type is locked to WPA2-Personal.
Passphrase	No default Passphrase is used.	Enter the **Passphrase**, password, for the selected **Security type**. **NOTE** The **Passphrase** must be a minimum of eight characters in length.

Export Cable Replacement Device A Settings

Before You Begin

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

The settings saved in the configuration file are compatible with the available **Cable replacement Device B** client settings.

Procedure

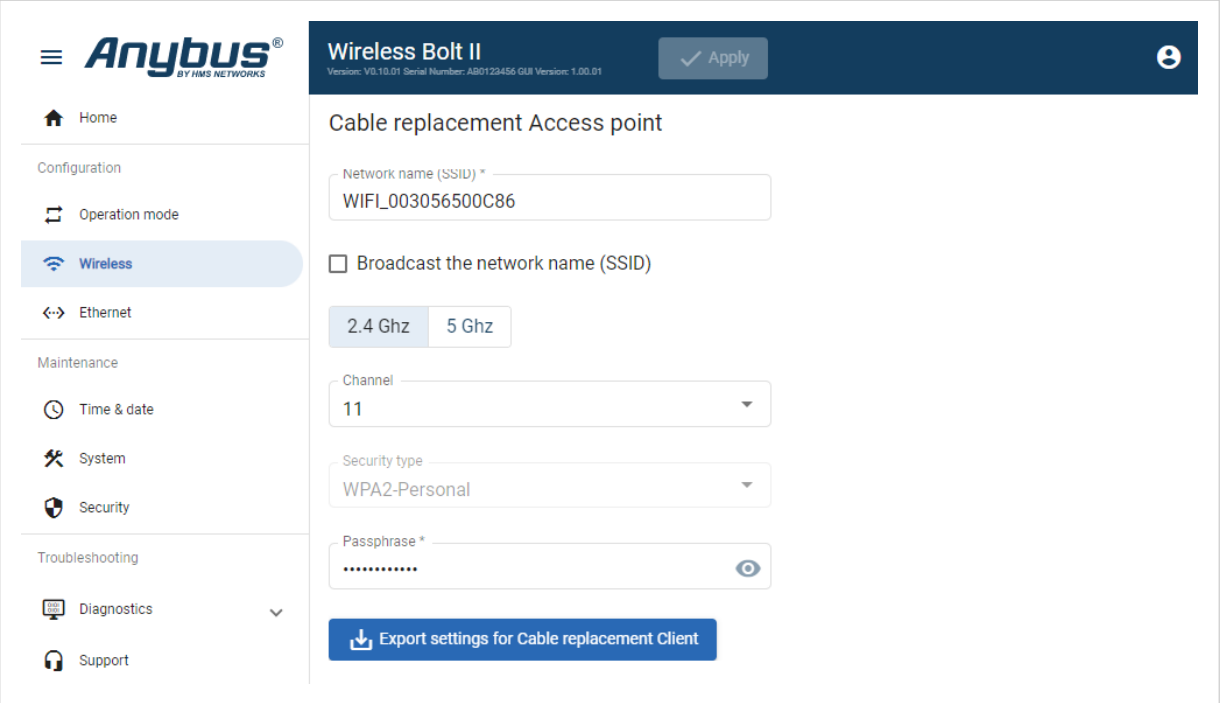


Figure 28. **Cable replacement Device A** page, export settings

1. To export a configuration file, click **Export settings for Cable replacement Device B**.
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 Device B** settings.

See Cable Replacement Device B Settings (page 30).

5.7.2. Cable Replacement Device B Settings

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

On the **Wireless** settings page, configure the **Cable replacement Device B** settings for the Bolt II client.

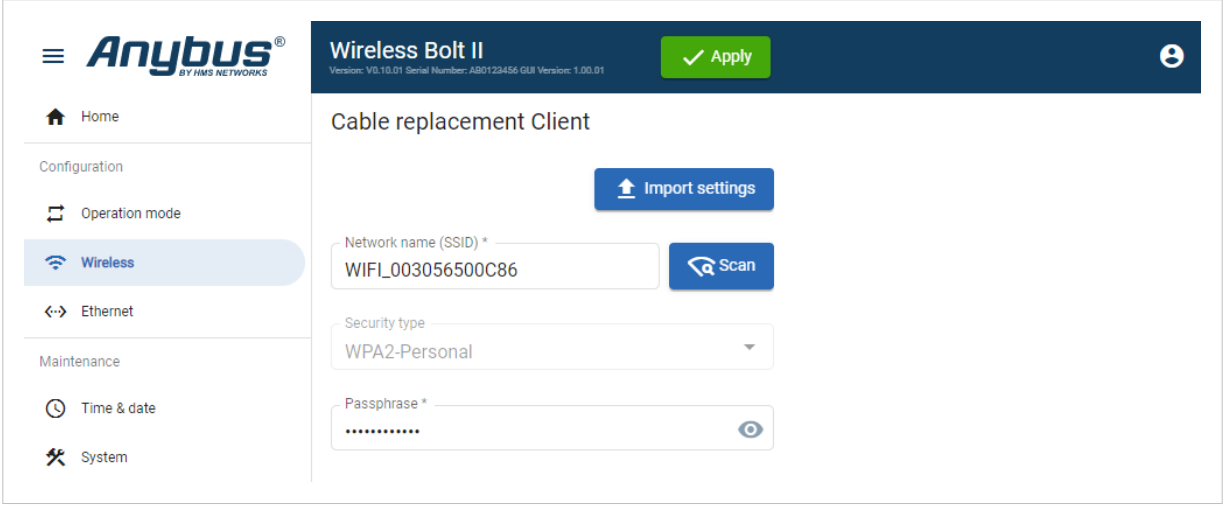


Figure 29. **Cable replacement Device B** page

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	Select a security type for the wireless connection is locked to WPA2-Personal.
Passphrase	No default Passphrase is used.	Enter the **Passphrase**, password, for the selected security type. **NOTE** The **Passphrase** must be a minimum of eight characters in length.

Import Cable Replacement Device A Settings to Configure Cable Replacement Device B

Before You Begin

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

Procedure

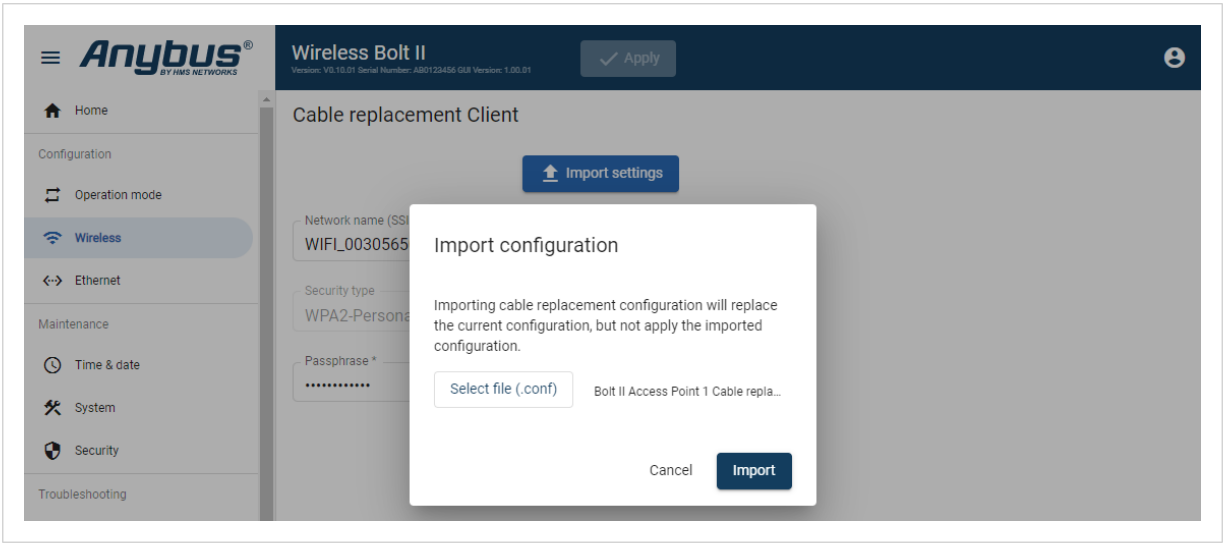


Figure 30. **Cable replacement Device B**, Import settings

1. Ensure that you have exported the **Cable replacement Device A** settings in a configuration file, (.devb). See Export Cable Replacement Device A Settings (page 29).
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 Device A** settings are imported.
4. To apply the settings, click **Apply** in the built-in web interface header and follow the instructions.

5.7.3. 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.

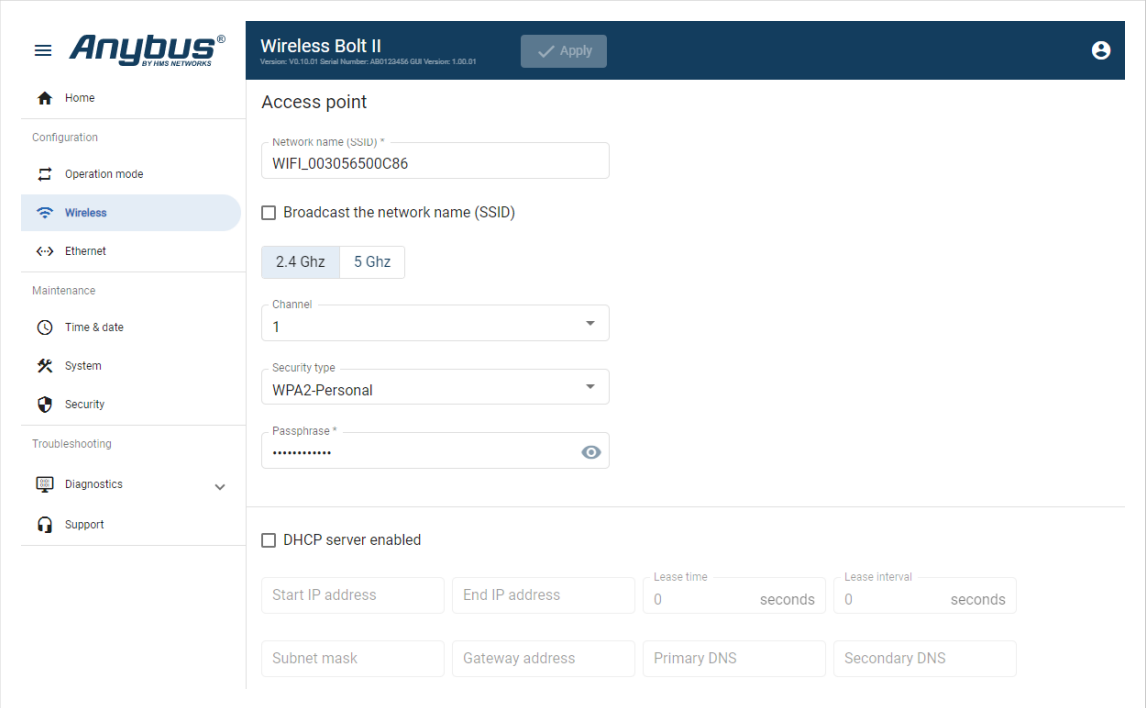


Figure 31. **Access point** page

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, **2.4 Ghz** or **5 Ghz**. See also WLAN Channels and World Mode (page 33).
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 **Broadcast the network name (SSID)** 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 **Channel** for the radio frequency band. See also WLAN Channels and World Mode (page 33).
Security type	Open (Not recommended) WPA2-Personal, Default WPA3-Personal	Select a **Security type** for the wireless connection. **NOTE** For **Cable Replacement Device A** the Security type is locked to WPA2-Personal.
Passphrase	No default Passphrase is used.	Enter the **Passphrase**, password, for the selected **Security type**. **NOTE** The **Passphrase** must be a minimum of eight characters in length.

Access Point IP 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: 2 hours, 7200 seconds Default: 12 hours, 43200 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.

5.7.4. WLAN Channels and World Mode

WLAN Channels and World Mode is only used for Client Mode.

NOTE

The maximum output power will be reduced on some channels depending on regulatory requirements.

Which channels are available for WLAN communication is restricted by the regulatory domain where the unit is operating.

Bolt II supports regulatory domain detection and channel settings for FCC and ETSI according to the IEEE 802.11d specification.

Table 4. Regulatory domains and WLAN channels

Domain	2.4 GHz	5 GHz
ETSI (European Telecommunications Standards Institute)	1-11	36, 40, 44, 48, 149, 153, 157, 161, 165
FCC (Federal Communications Commission)		

5.8. Ethernet Settings

5.8.1. To Configure IP Settings Manually

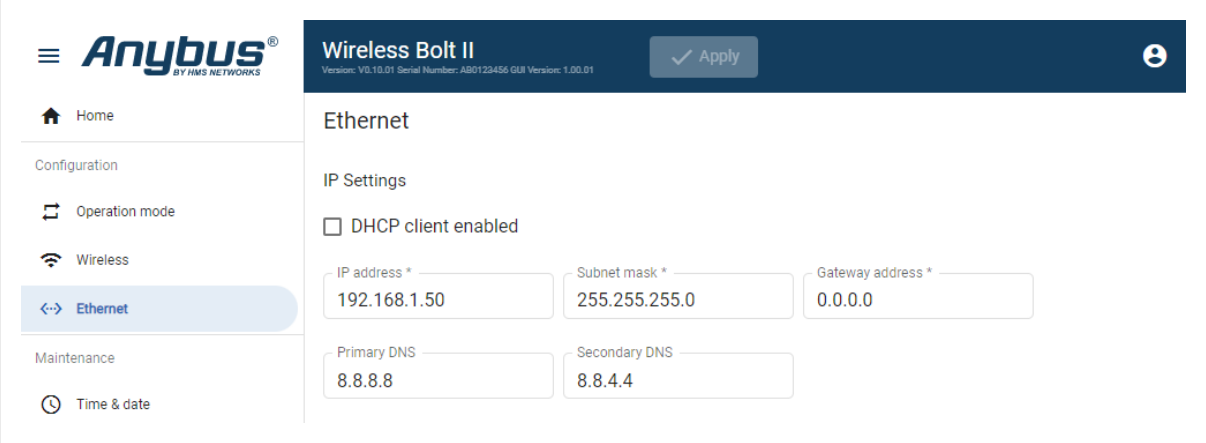


Figure 32. Ethernet IP Settings, DCHP client disabled

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
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	The Bolt II network Primary DNS in IPv4 dot-decimal notation.
Secondary DNS	The Bolt II network Secondary DNS in IPv4 dot-decimal notation.

5.8.2. To Use DHCP Client

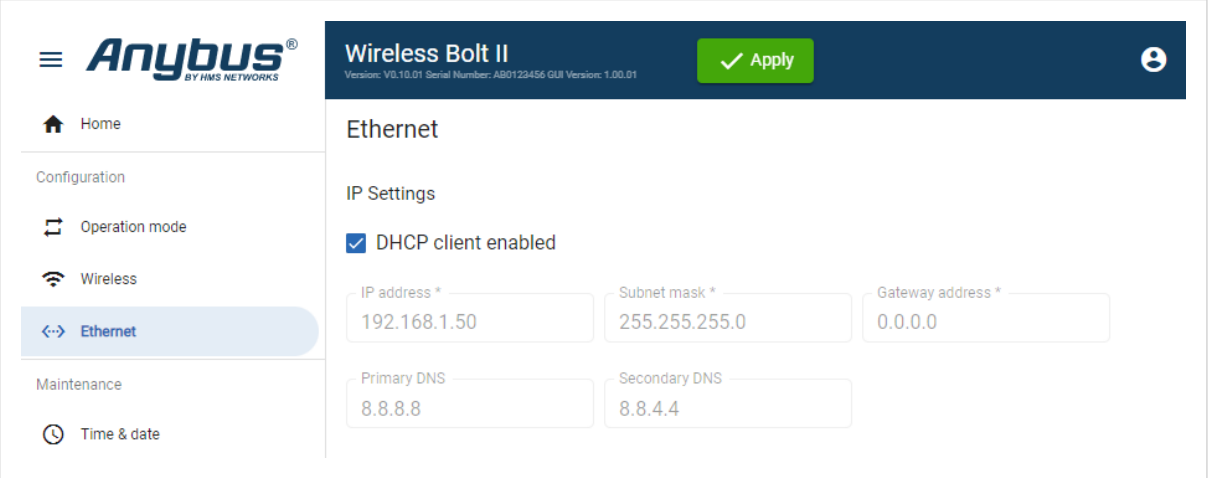


Figure 33. Ethernet IP Settings, DHCP client enabled

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 5. 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.

5.9. Apply Configuration

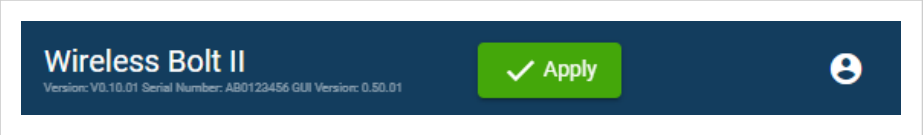
Before You Begin

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

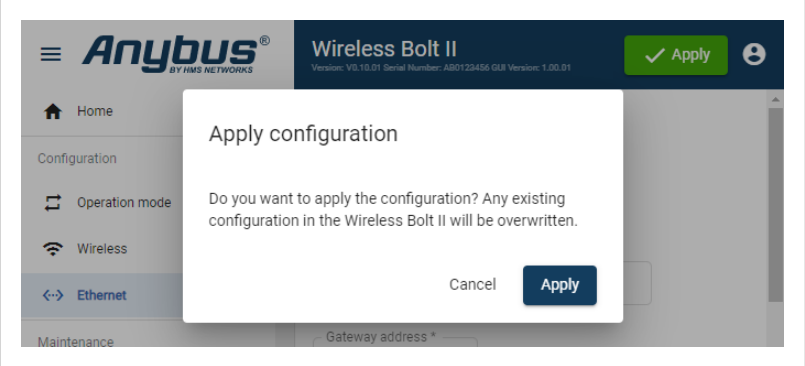
Procedure

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

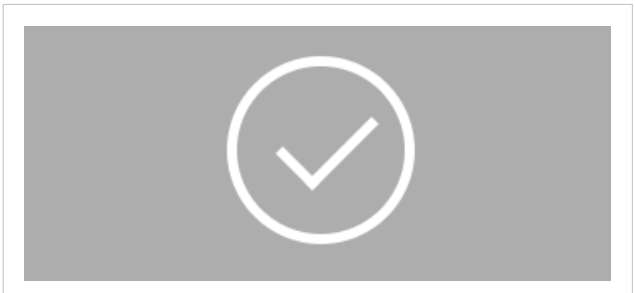
1. In the Bolt II web-interface header, click **Apply**.



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.

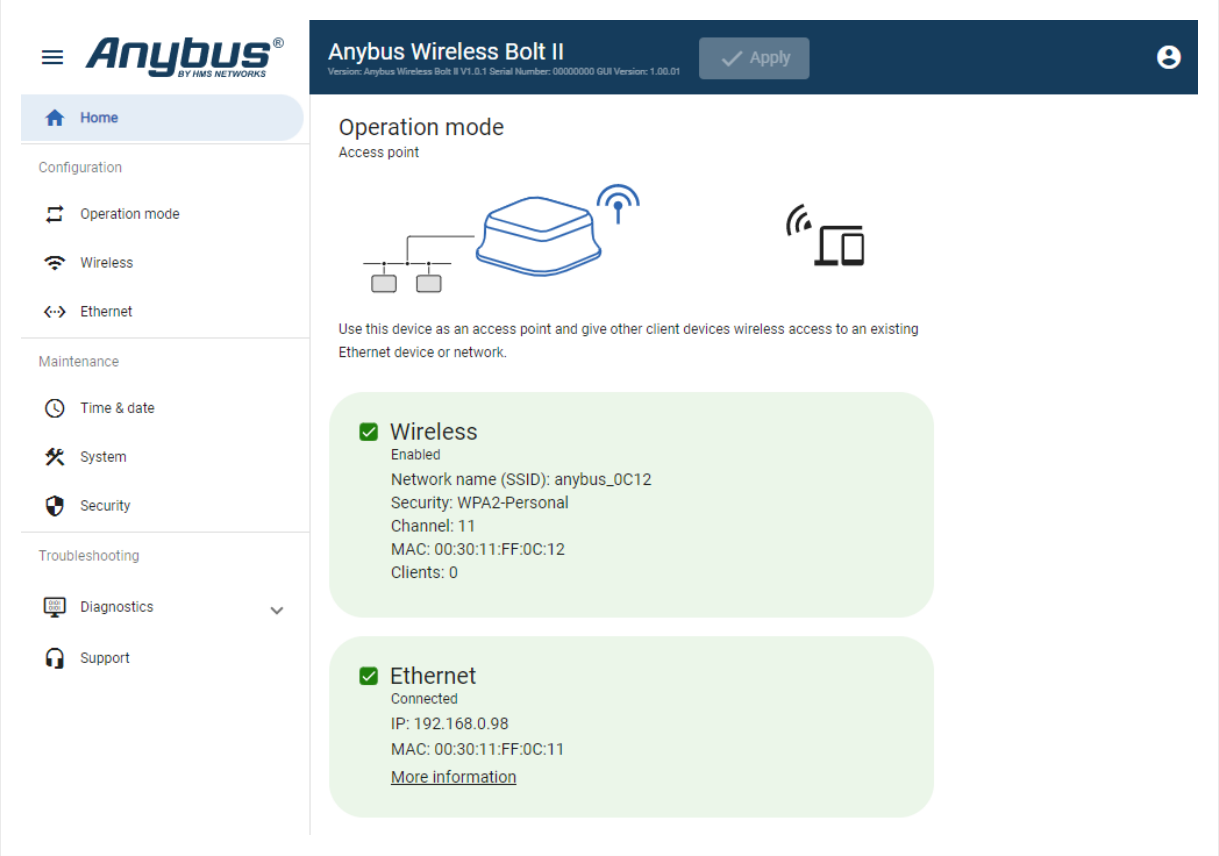


Figure 34. Home page

Operation Mode

View the current selected Operation mode, see Wireless Bolt II Operation Modes (page 20).

Wireless Status

Overview communication status, signal strength and current networks settings.

Ethernet Status

Overview the Bolt II RJ45 connector LED indications remotely.

Refer to Ethernet LED Indication (page 39).

Status Symbols

Symbol	Description
	Internal error has occurred, and operation cannot be guaranteed. Examples for Run Time System: • Could not initialize WLAN device management control: Could not add device management data point wlan-station/rssi: Endpoint receive operation timed out (-32603). • Could not initialize SystemInfo Managment Control: SystemInfo: Error (-32603) adding data point system : os, Endpoint receive operation timed out. • Could not initialise Device Manager Control: Update DevMgmCtrl: Error (-32603) adding data point update : counter, Endpoint receive operation timed out.
	Out of Specification.
	• Power fail handling not supported. • Could not load and start program. Alerts for Cable replacement, Client: • The unit is in idle state, waiting for an event. • The unit is inactive. • The unit is disconnected. • The unit is restarting. • Incorrect password is detected. Alerts for Access point and Cable replacement, Access point: • The unit is disabled.
	Normal operation. Cable replacement, Client: • The unit is connected. • The unit is scanning. Access point and Cable replacement, Access point: • The unit is enabled. • The unit is connected to Ethernet network.

6.2. Ethernet LED Indication

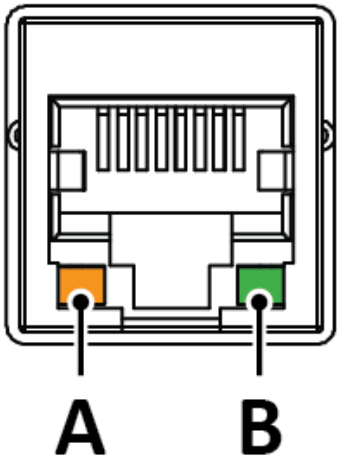


Figure 35. RJ45 LED indicators

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

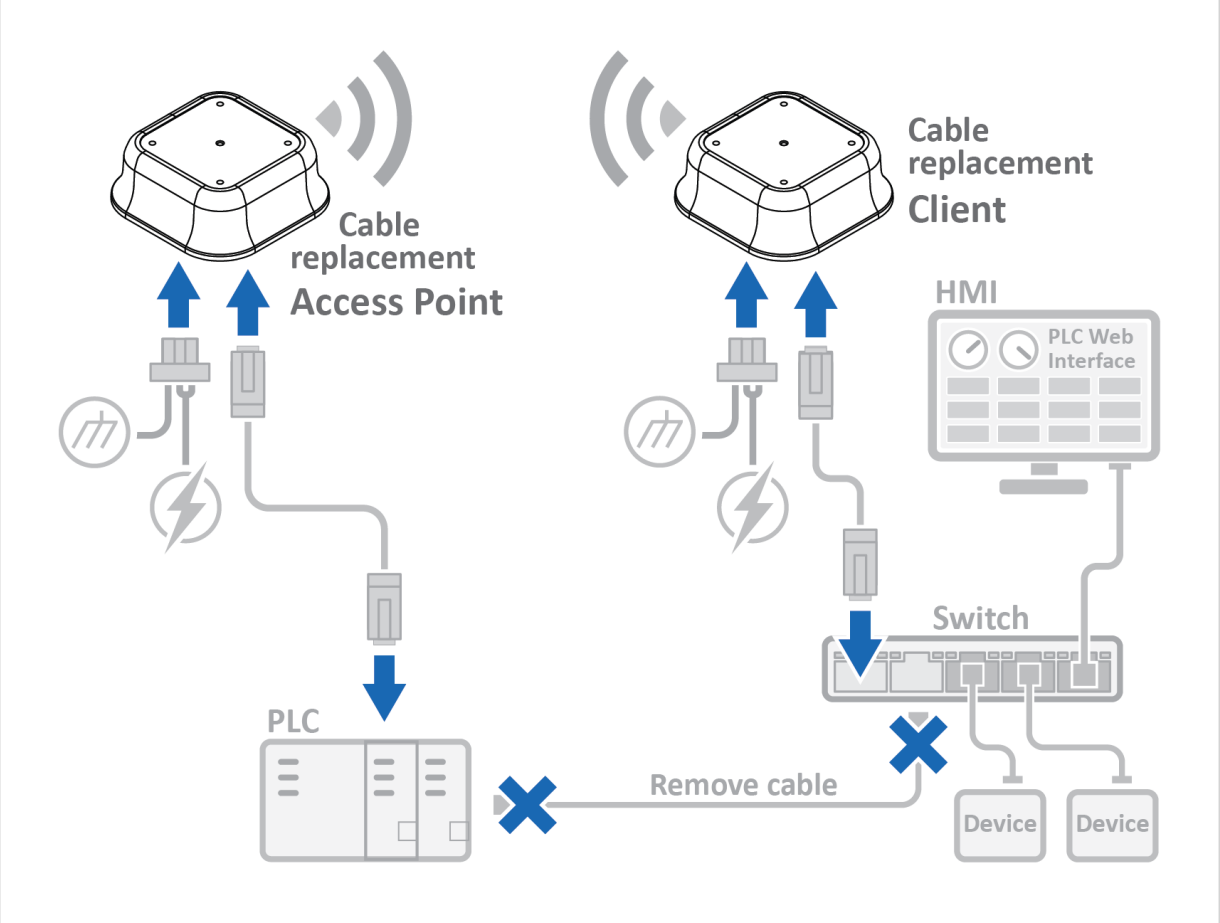


Figure 36. Cable replacement between a PLC and a Network Switch

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 access Point unit and one Bolt II Client unit.

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

The HMI is connected to the Bolt II access point to access the PLC built-in web interface.

Bolt II Cable replacement Access Point Configuration

Procedure

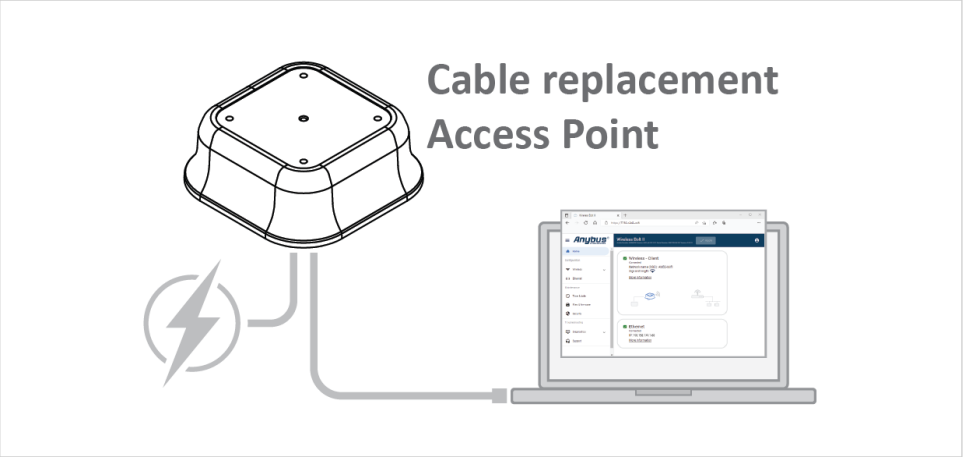


Figure 37. Configure the Bolt II Cable replacement access point

Configure one Bolt II as a Cable replacement access point.

See Configure the Bolt II Cable Replacement Access Point (page 21).

Bolt II Cable replacement Client Configuration

Procedure

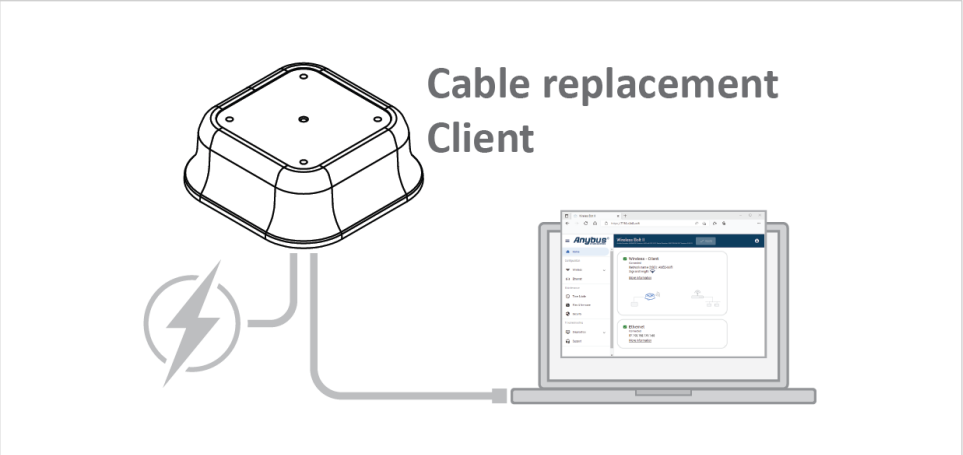


Figure 38. Configure the Bolt II Cable replacement client

Configure one Bolt II as a Cable replacement client.

See Configure the Bolt II Cable Replacement Client (page 23).

Cable Replacement Installation

Procedure

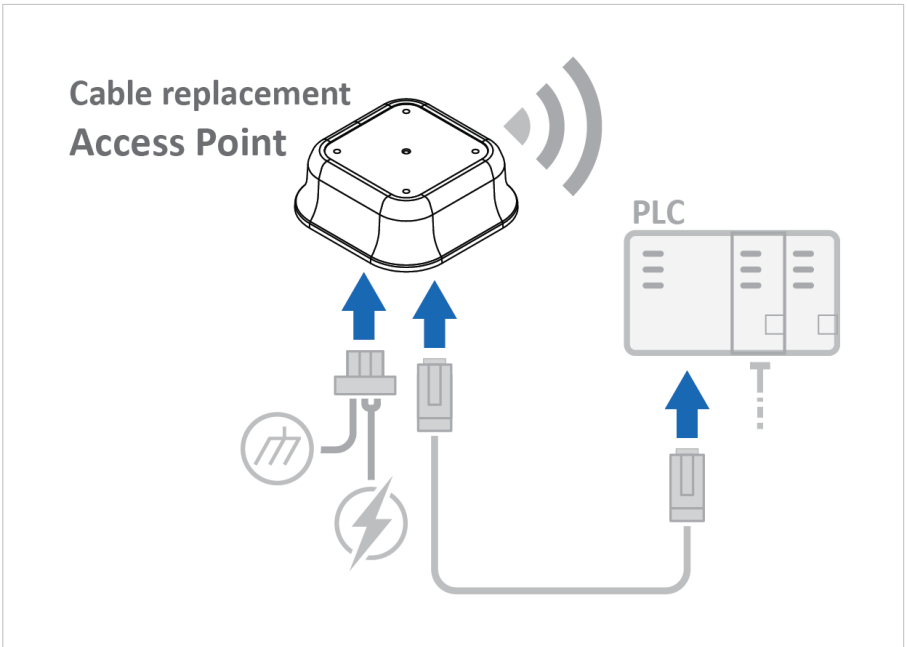


Figure 39. Install the Bolt II Cable replacement access point

1. Connect the Bolt II Cable replacement access point to power and Functional Earth (FE).
2. Connect an Ethernet cable between Bolt II Cable replacement access point and the PLC.

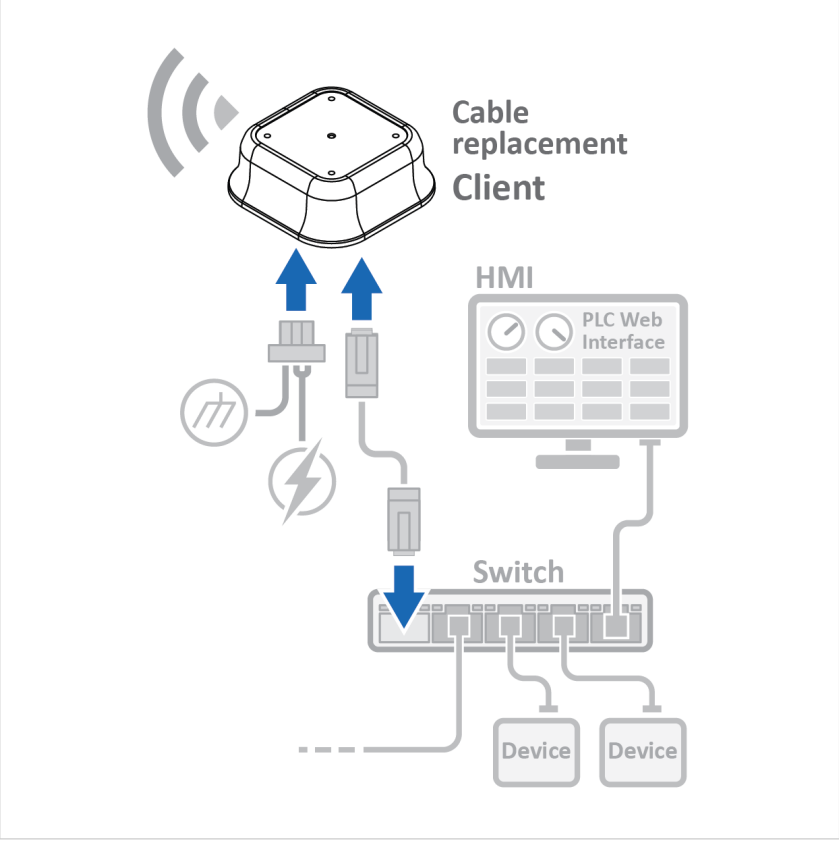


Figure 40. Install the Bolt II Cable replacement client

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

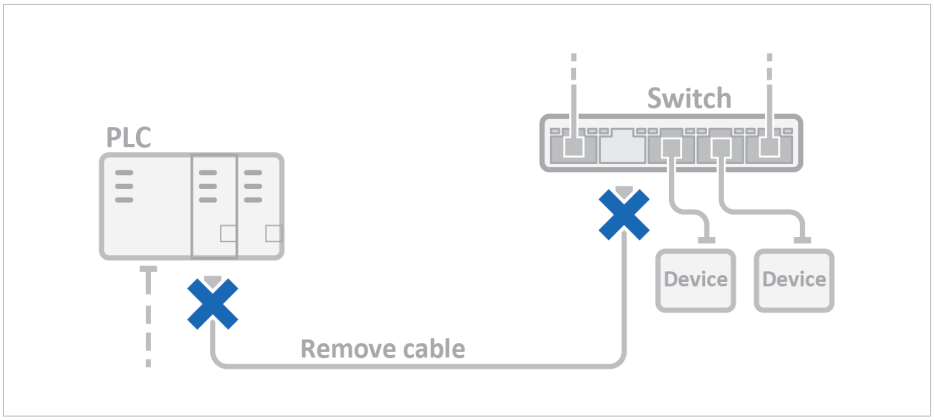


Figure 41. Remove the cable

Result

Wireless connection is now established between the Bolt II Cable replacement access point and the e Bolt II Cable replacement client.

Access the PLC Built-In Web Interface on the HMI

Procedure

On the HMI:

1. Connect to the Bolt II Cable replacement access point SSID (Network name).
2. 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

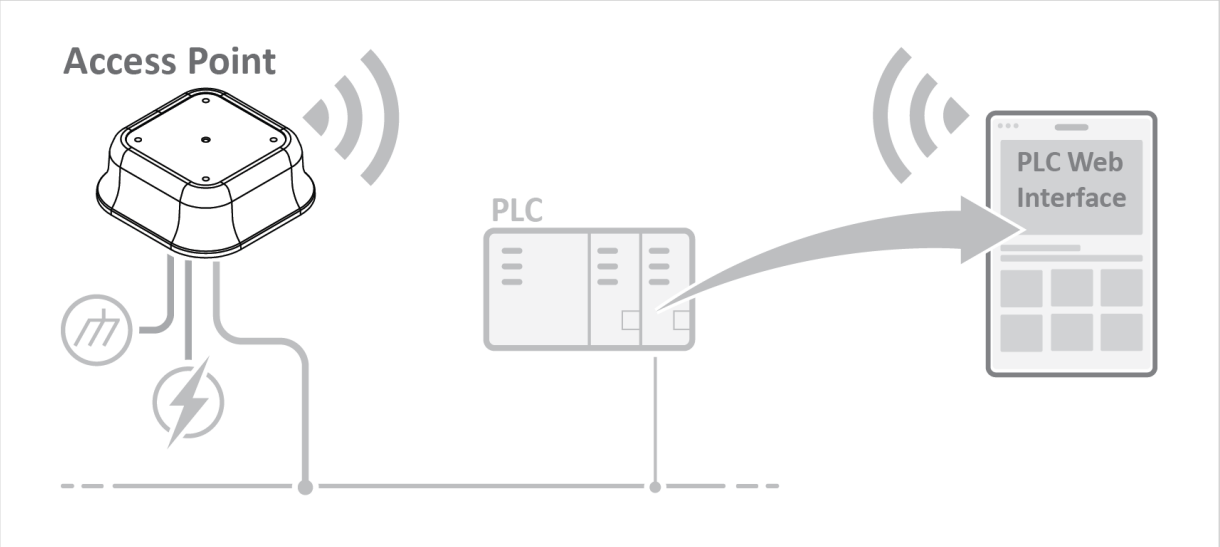


Figure 42. Access a PLC from a handheld device using WLAN

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.

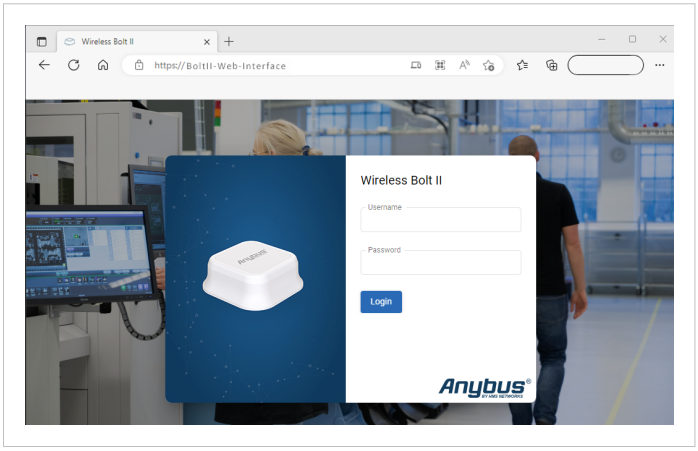


Figure 43. Bolt II Login

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

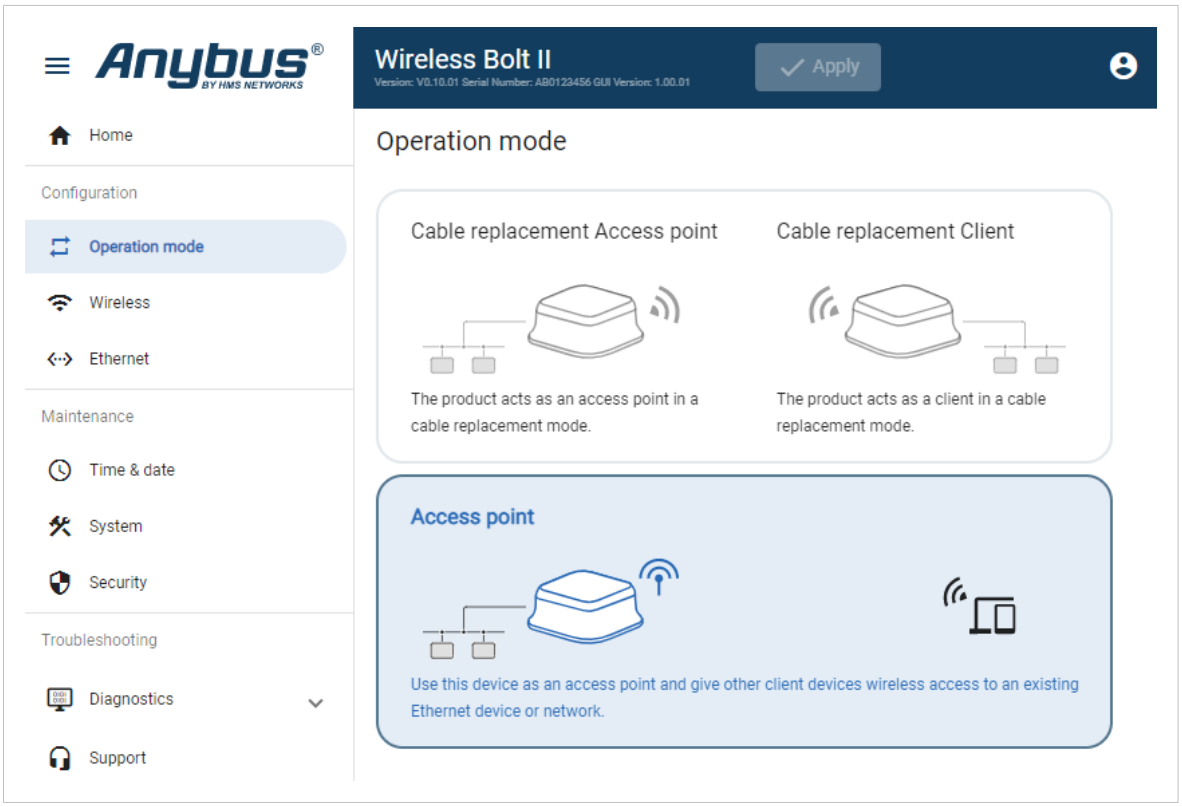


Figure 44. Operation mode page, Access point

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

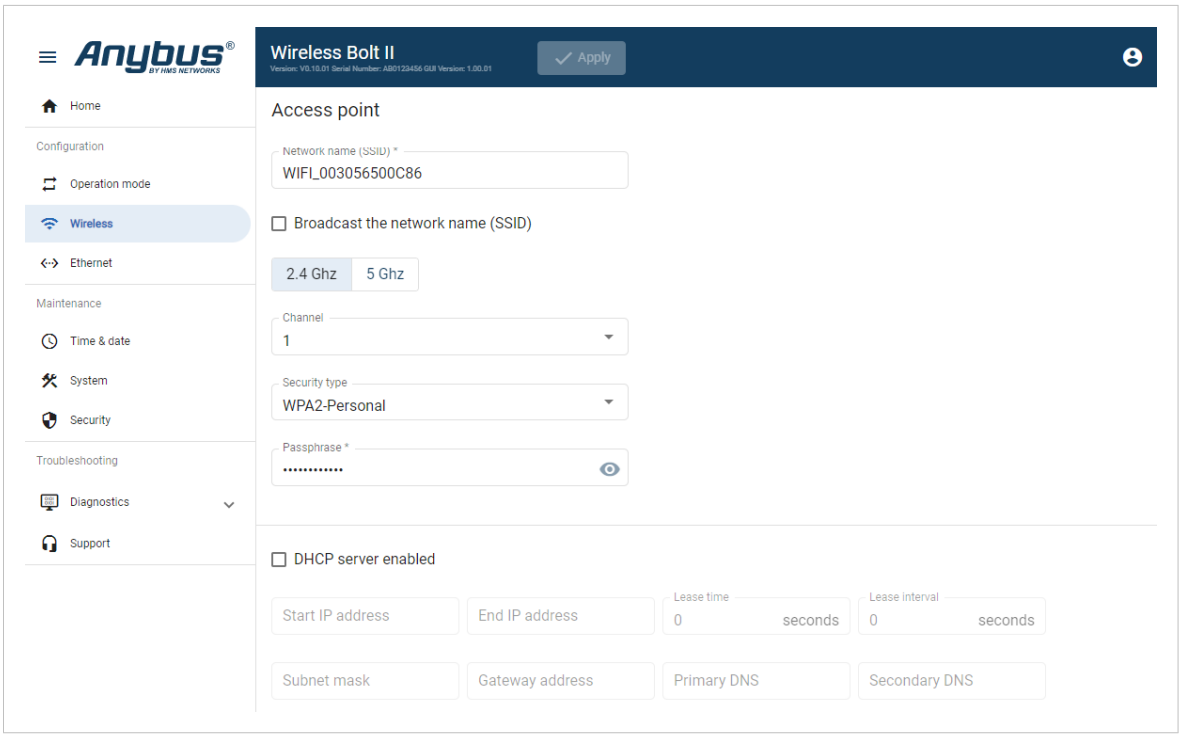


Figure 45. Settings page, Access point

a. 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.

b. In the **Network name (SSID)** field, enter a unique network name for the Bolt II Wi-Fi access point.

c. In the **Channel** menu, select a band channel.

d. In the **Security type** menu, select **WPA2-Personal** (default) or **WPA3-Personal**.

e. In the **Passphrase** field, enter the 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:

a. Select the **DHCP server enabled** checkbox.

b. Configure the **DHCP server** settings. See Access Point IP Settings (page 33).

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

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

a. 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.

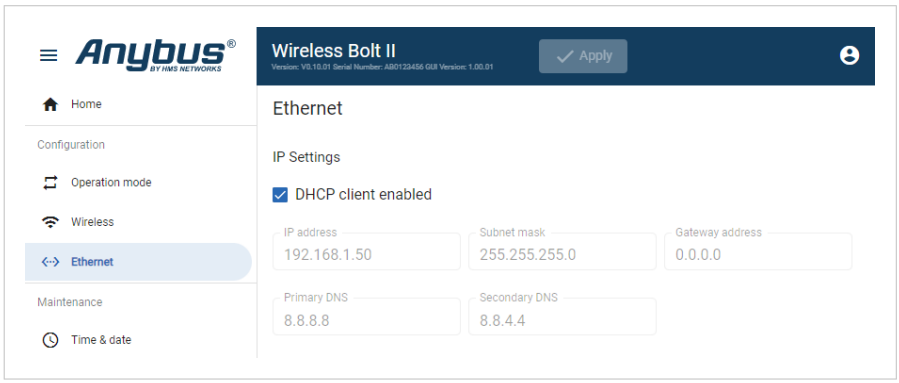


Figure 46. DHCP enabled

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.

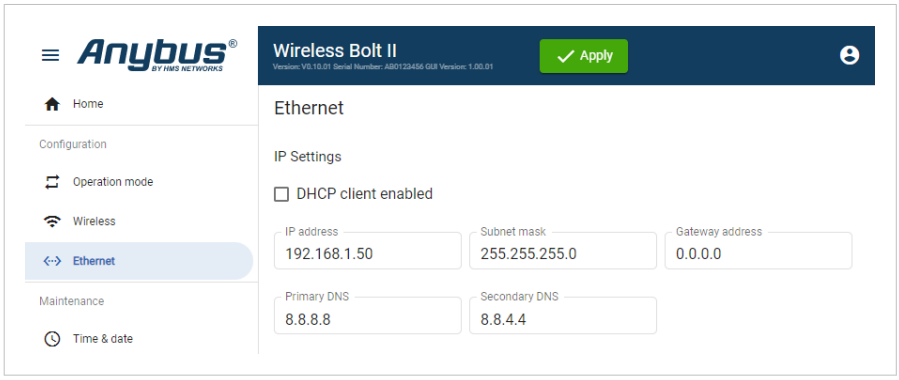


Figure 47. DHCP disabled

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.

8. Maintenance

8.1. Time & Date Settings

8.1.1. Set Time

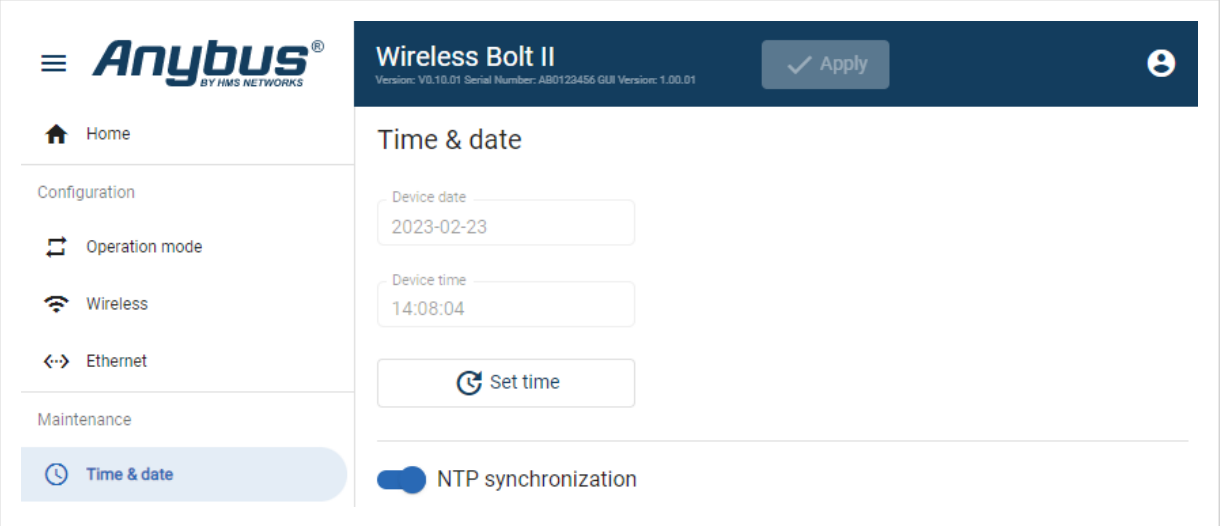


Figure 48. Time & date page, Set time

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.

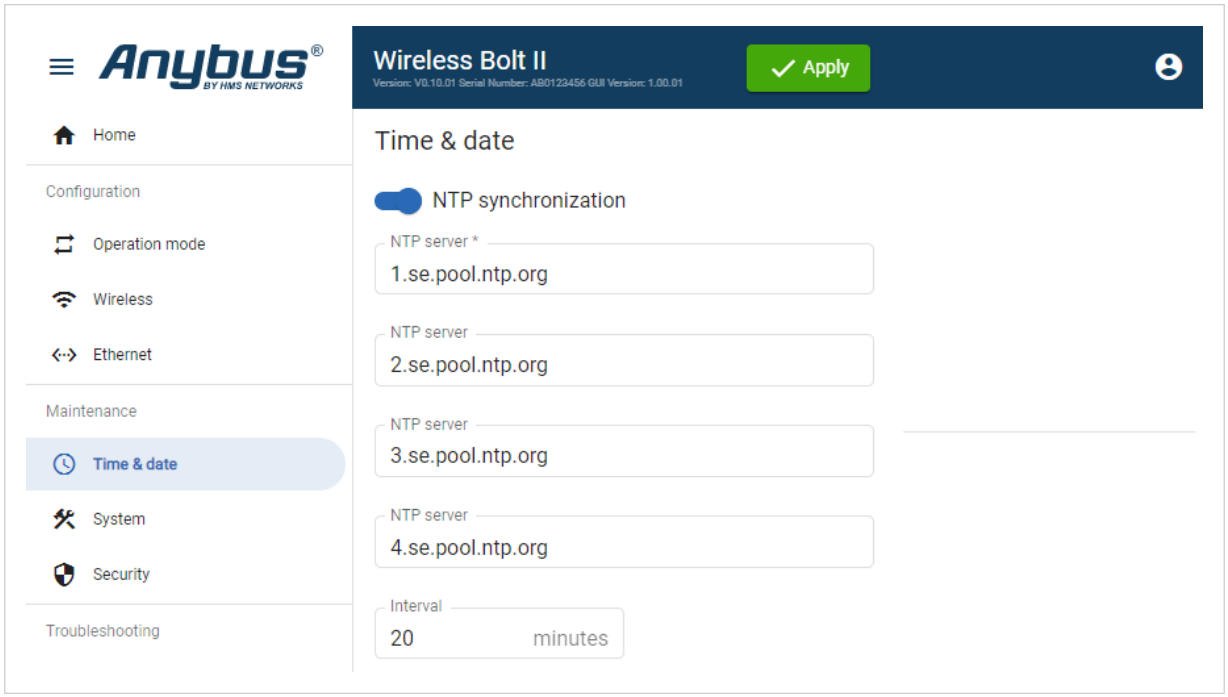


Figure 49. Time & date page, NTP synchronization enabled

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.

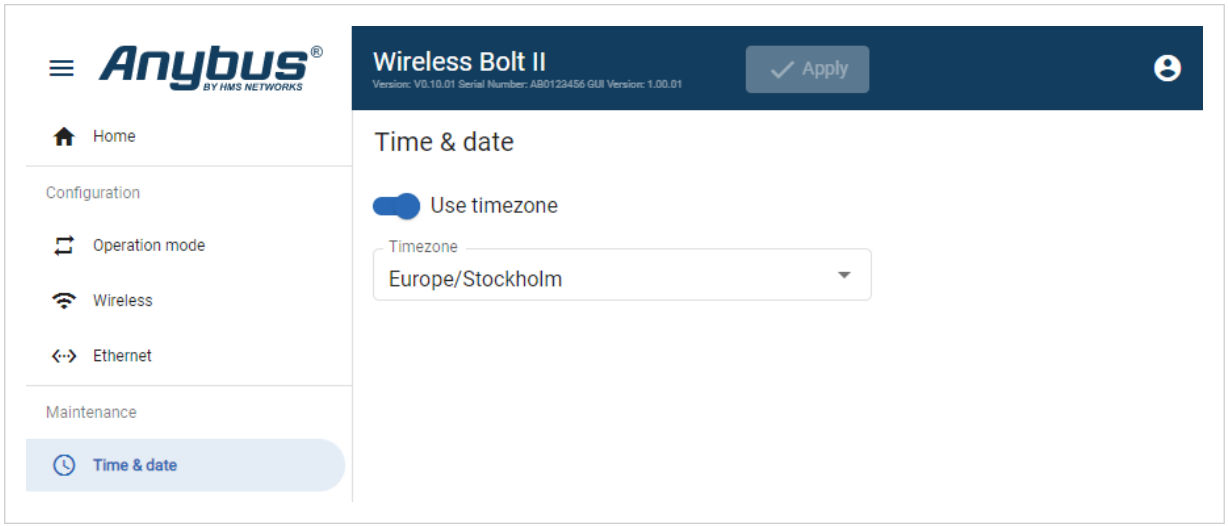


Figure 50. Time & date page, Use timezone

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.

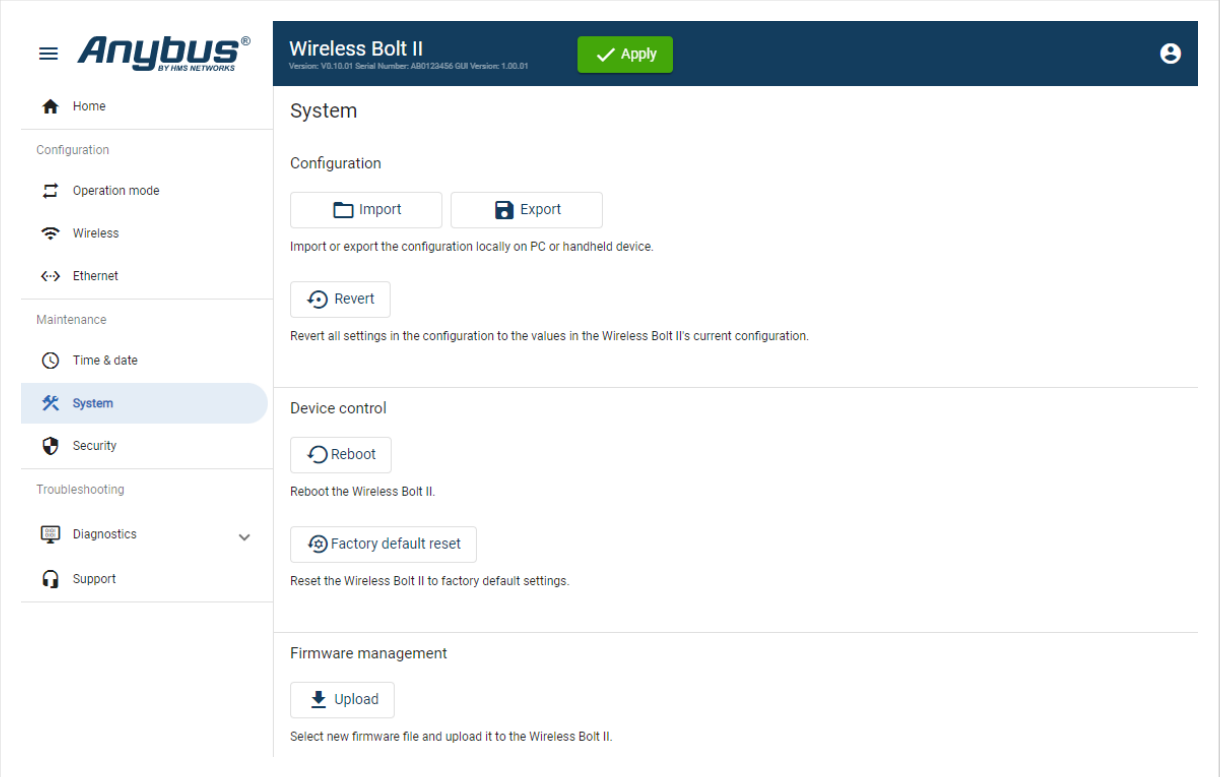


Figure 51. System page

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

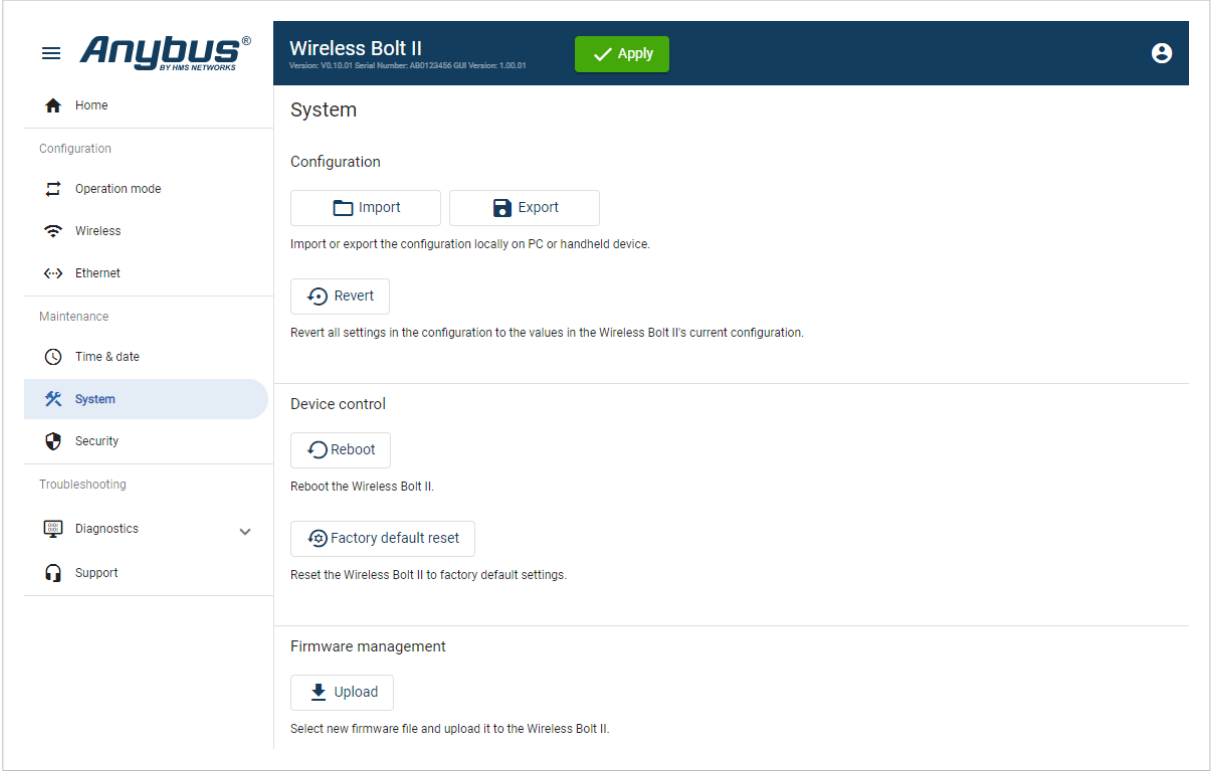


Figure 52. System page

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.

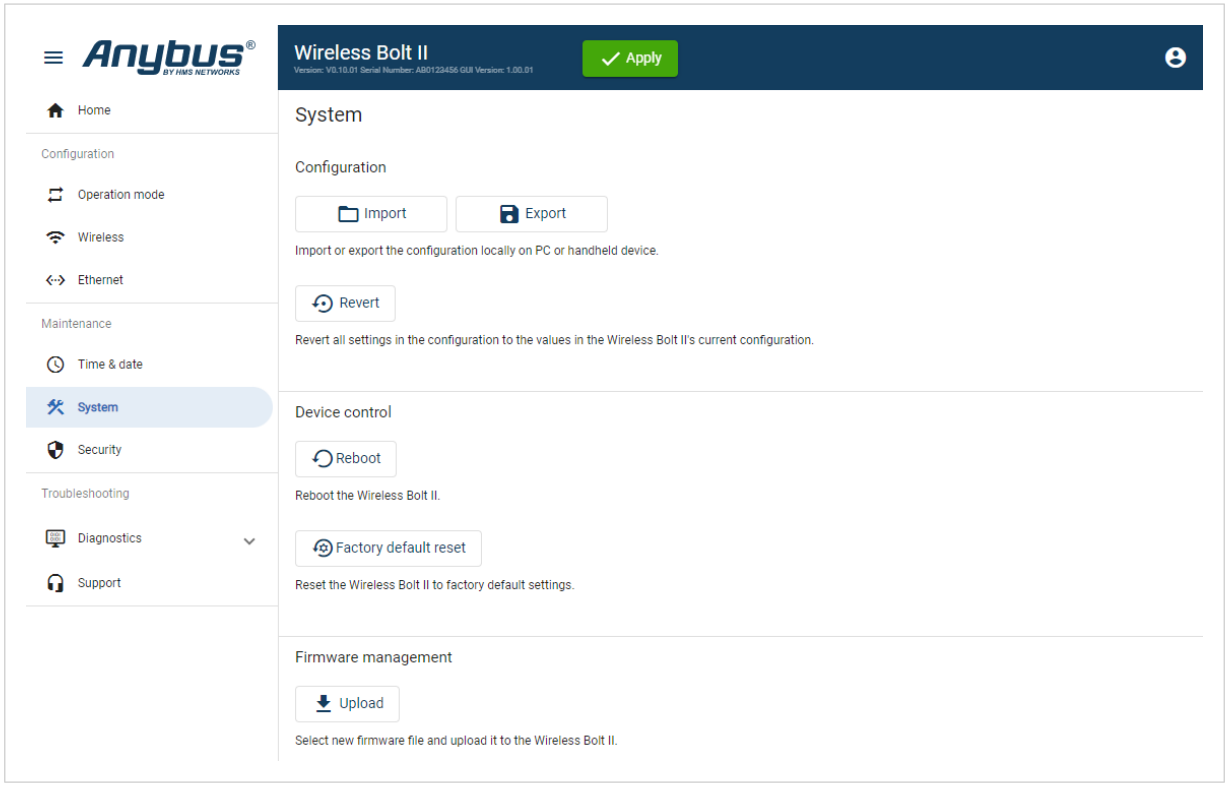


Figure 53. System page

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

1. On the **System** page, click **Revert**.
2. In the Confirm revert window, click **Revert**.
3. To apply the change, click **Apply** in the web-interface header, and follow the instructions.

8.4. Firmware Management

8.4.1. View the Firmware Version

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

Figure 54. 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 can not 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 compatibly 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.

Ensure that the Bolt II is disconnected from the OT networks.

To download the firmware update package zip file, please visit www.anybus.com/support 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

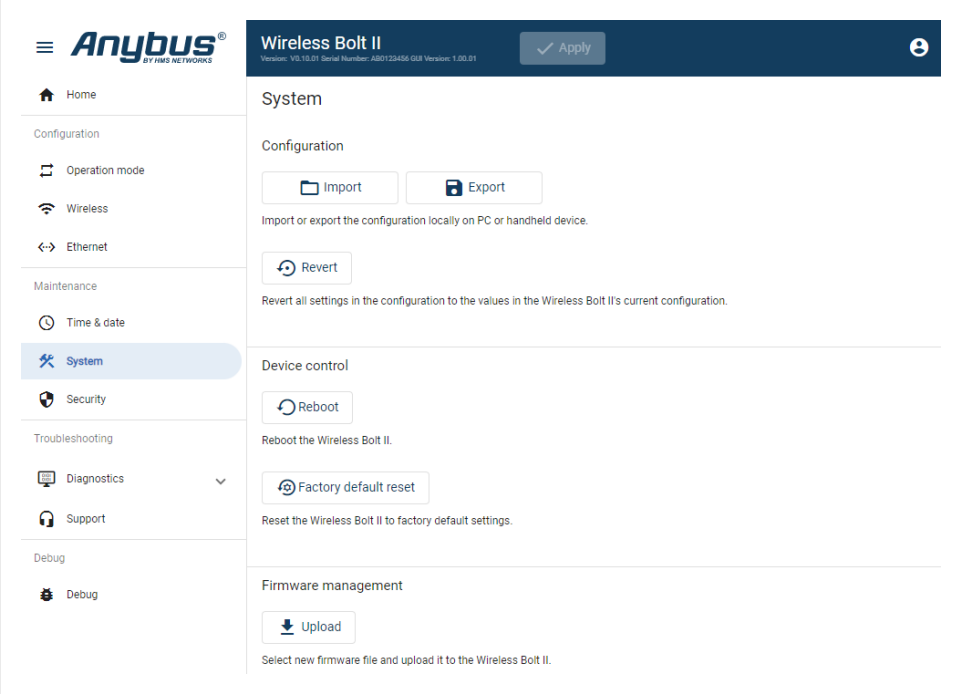


Figure 55. System page

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. Web Server Certificate Settings

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 56. 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**.
6. To install the web server certificate, click **Apply** in the web-interface header, and follow the instructions.

Result

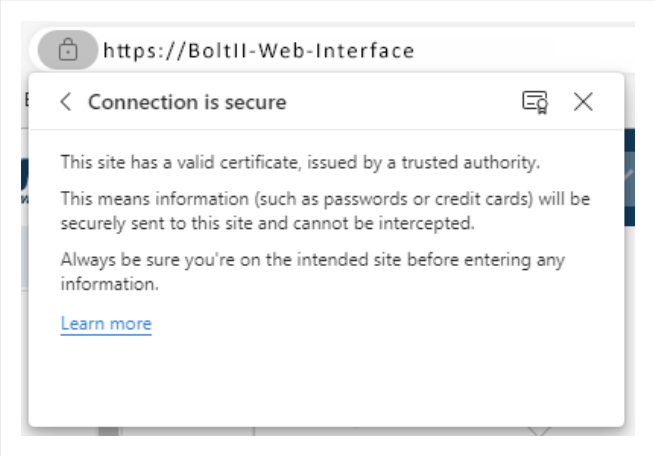


Figure 57. Example View site information > Connection is secure

The web server certificate is uploaded in the web browser.

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

8.6. Change the Bolt II Password

IMPORTANT
For cyber security 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 57).

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**.

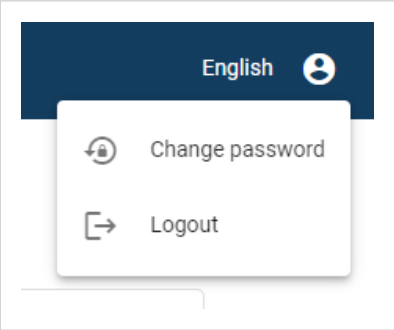


Figure 58. Account menu, Change password

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

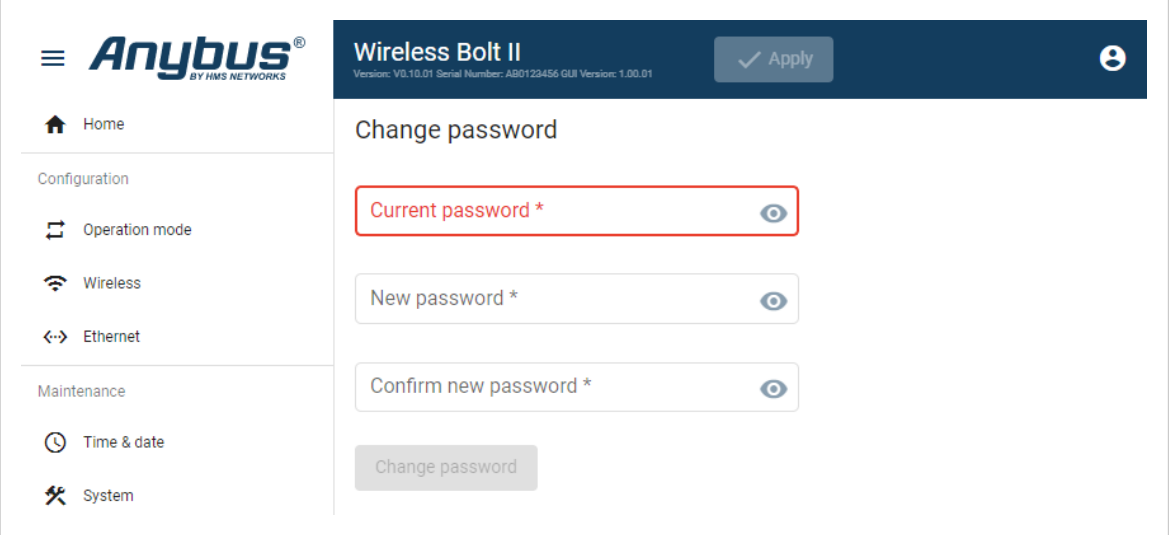


Figure 59. Change password page

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

9. Troubleshooting

9.1. Diagnostics

9.1.1. Event Log

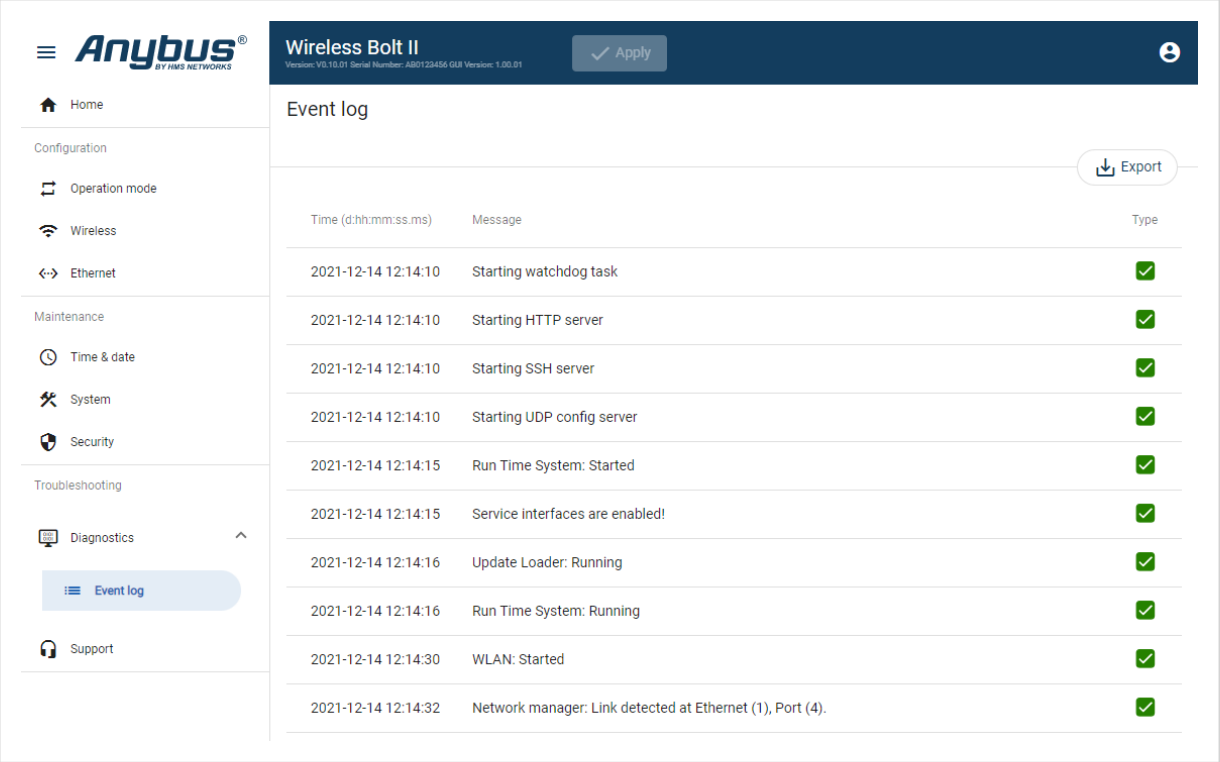


Figure 60. Event log page example

To export the log data, click **Export**. An Excel XLS 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 Status Symbols.

9.1.2. Remotely Monitor the Bolt II Status

On the **Home** page, you can remotely monitor the Bolt II Ethernet status, RJ45 connector LED indications.

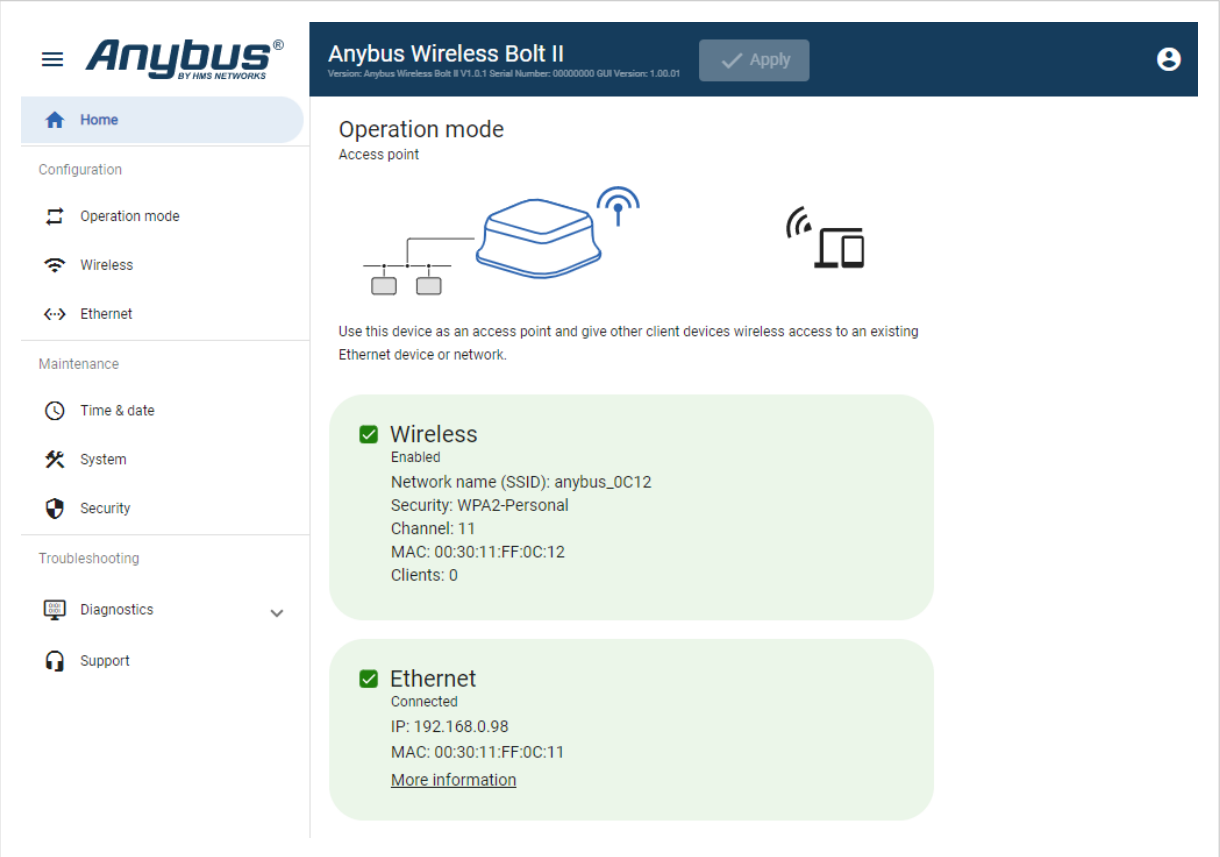


Figure 61. Home page

For information about the status symbols, see Status Symbols.

9.2. Find the Bolt II IP Address

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

Example 1. Device IP address detected in HMS IPconfig

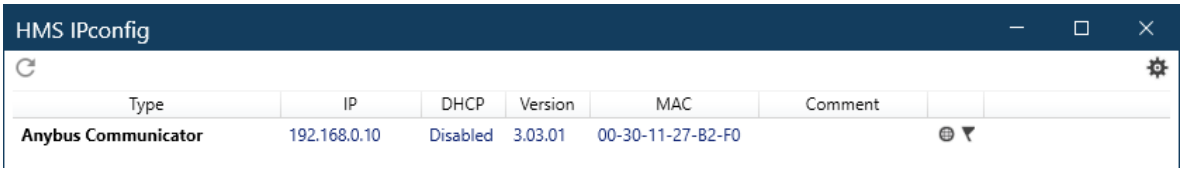


Figure 62. HMS IPconfig

To download the installation files, please visit www.anybus.com/support 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

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

Procedure

1. Ensure that the Bolt II is powered on.

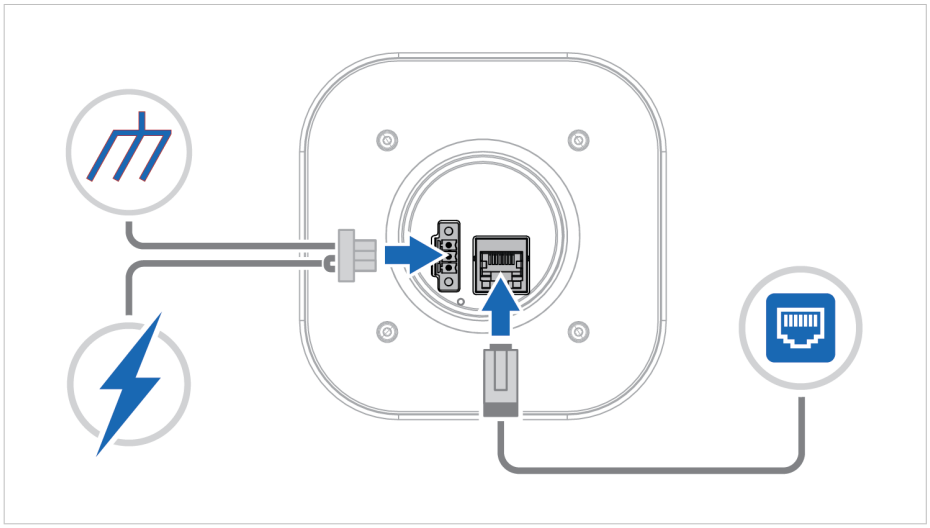


Figure 63. Power on the Bolt II

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

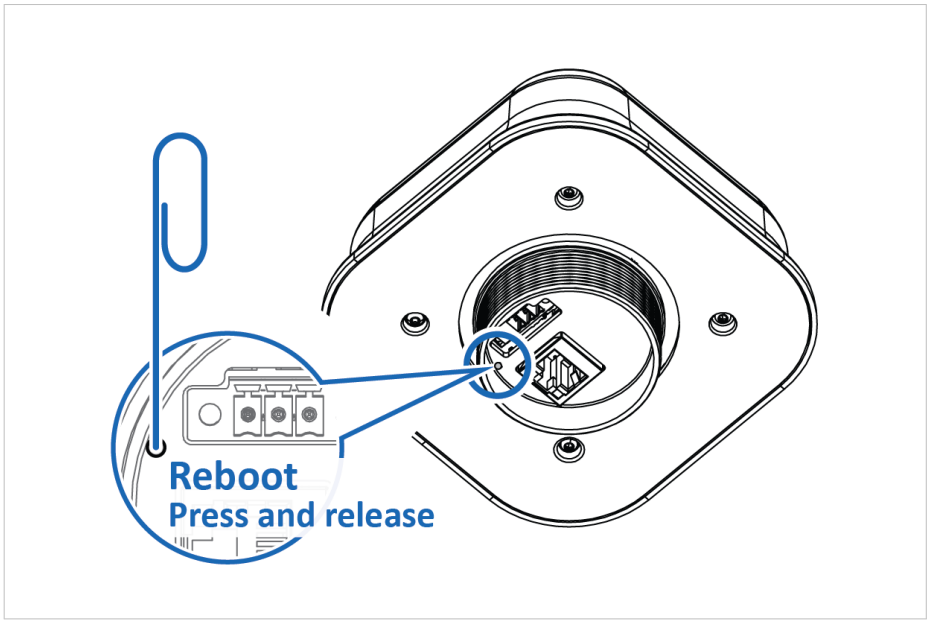


Figure 64. Quickly press and release the **Reset** button

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.

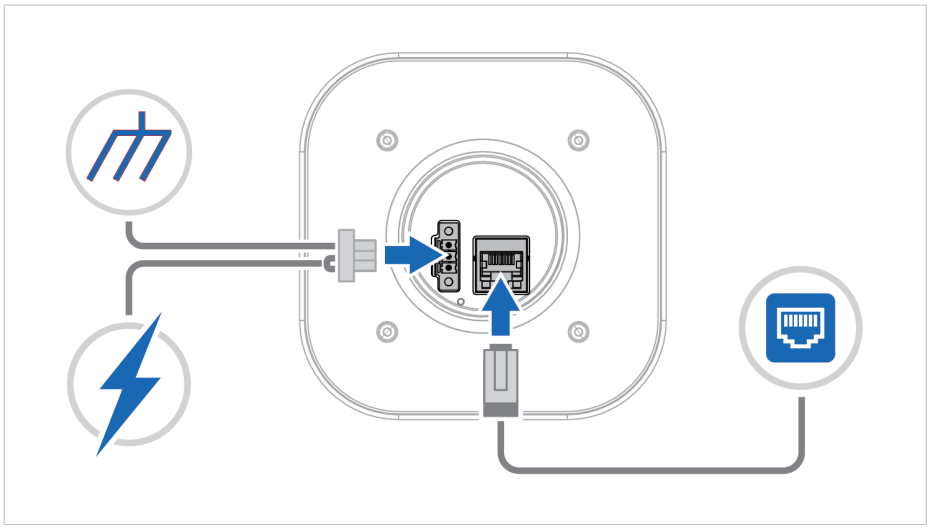


Figure 65. Power on the Bolt II

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

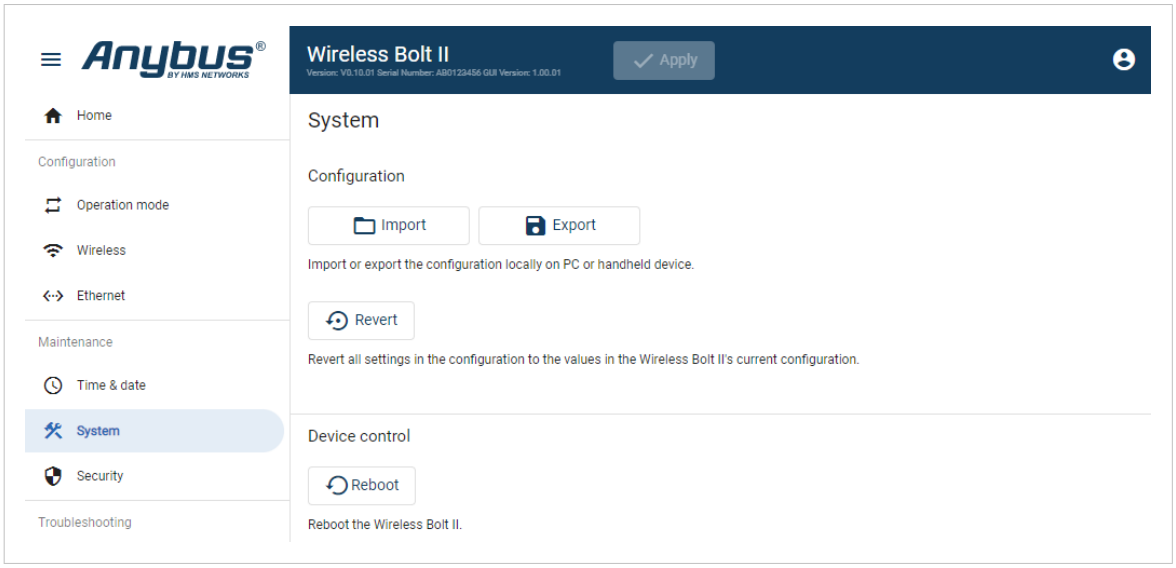


Figure 66. System page, Reboot

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

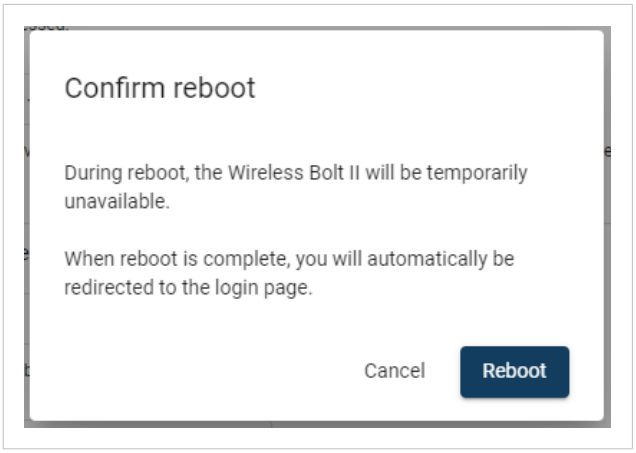


Figure 67. Confirm reboot

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 configuration to initial state after the update.

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

Procedure

1. Ensure that the Bolt II is powered on.

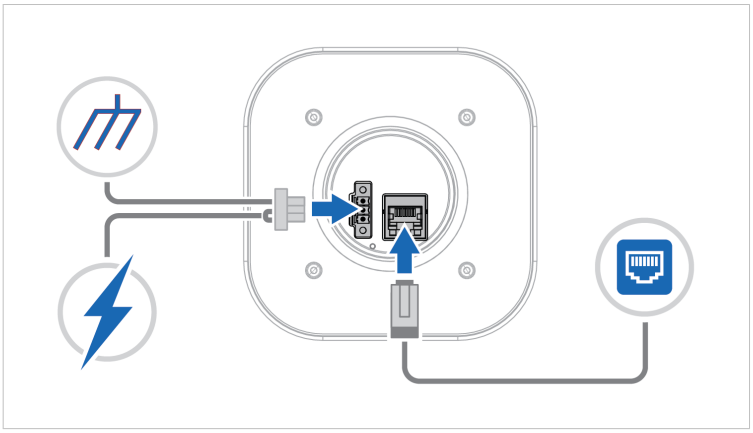


Figure 68. Power on the Bolt II

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

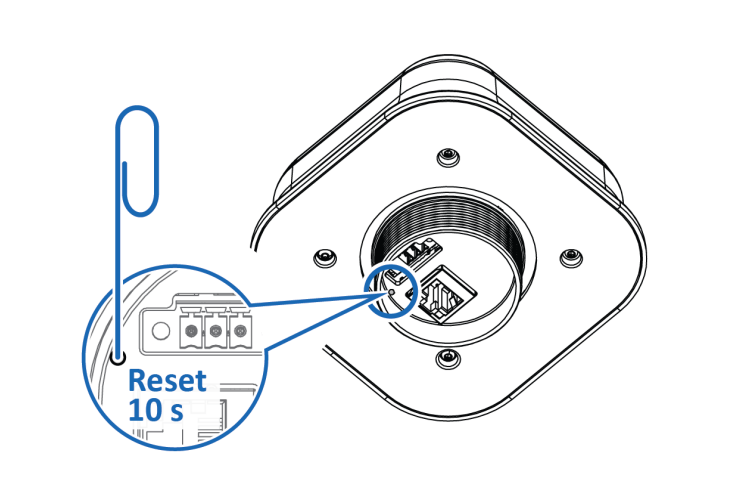


Figure 69. Press and hold **Reset** button

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 or the current configuration after firmware upgrade.

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 configuration to initial state after the update.

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

Procedure

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

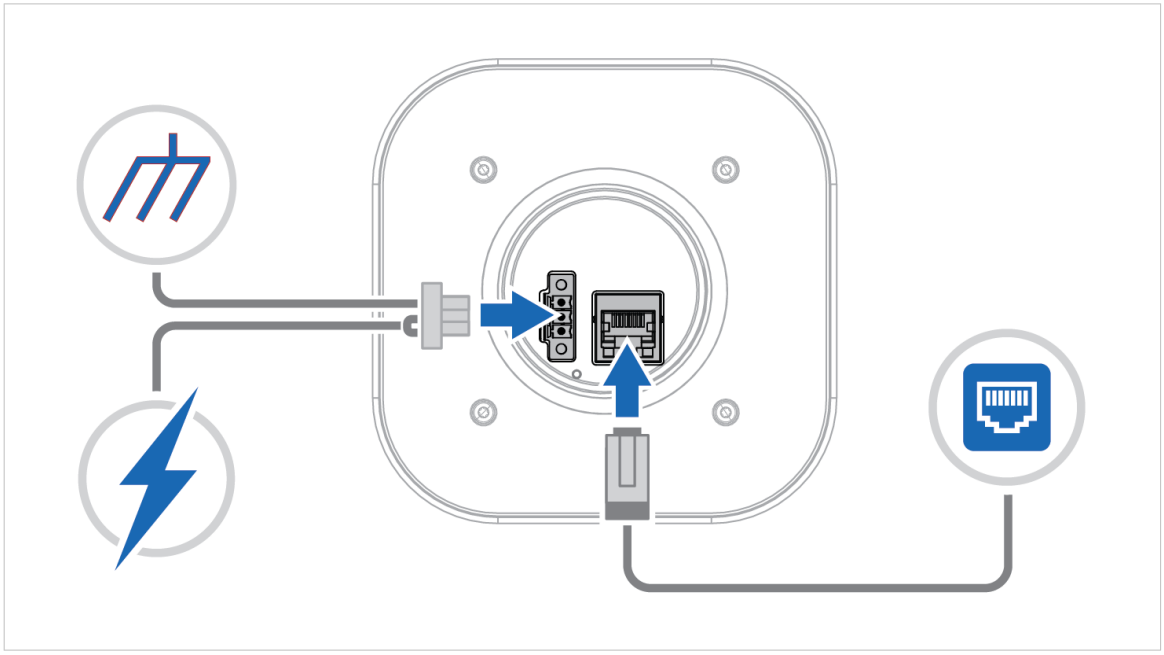


Figure 70. Power on the Bolt II

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

3. On the **System** page, click **Factory default reset**.

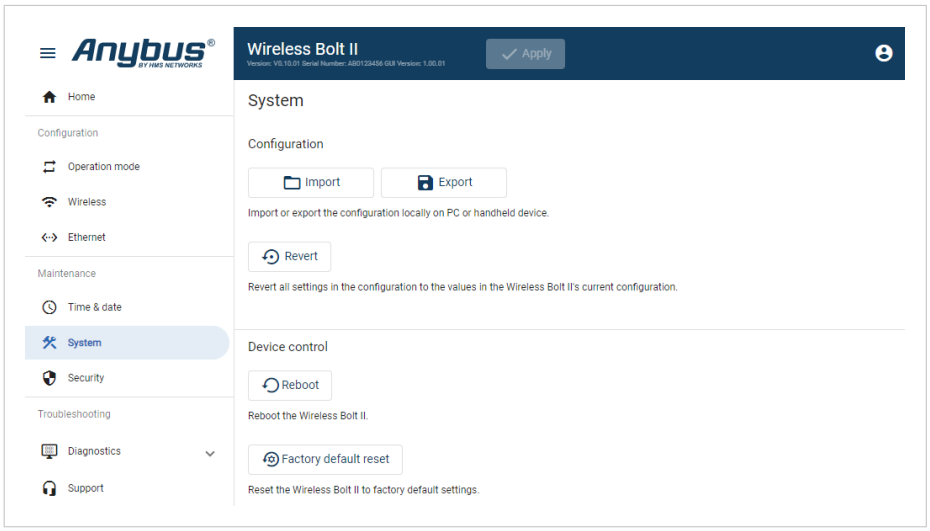


Figure 71. System page, Factory default reset

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

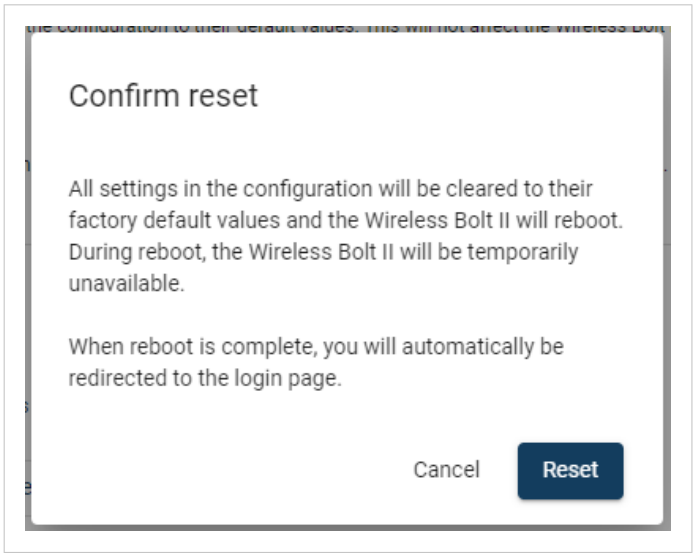


Figure 72. Confirm factory default reset

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 or the current configuration after firmware upgrade.

9.7. Support

9.7.1. Support Package

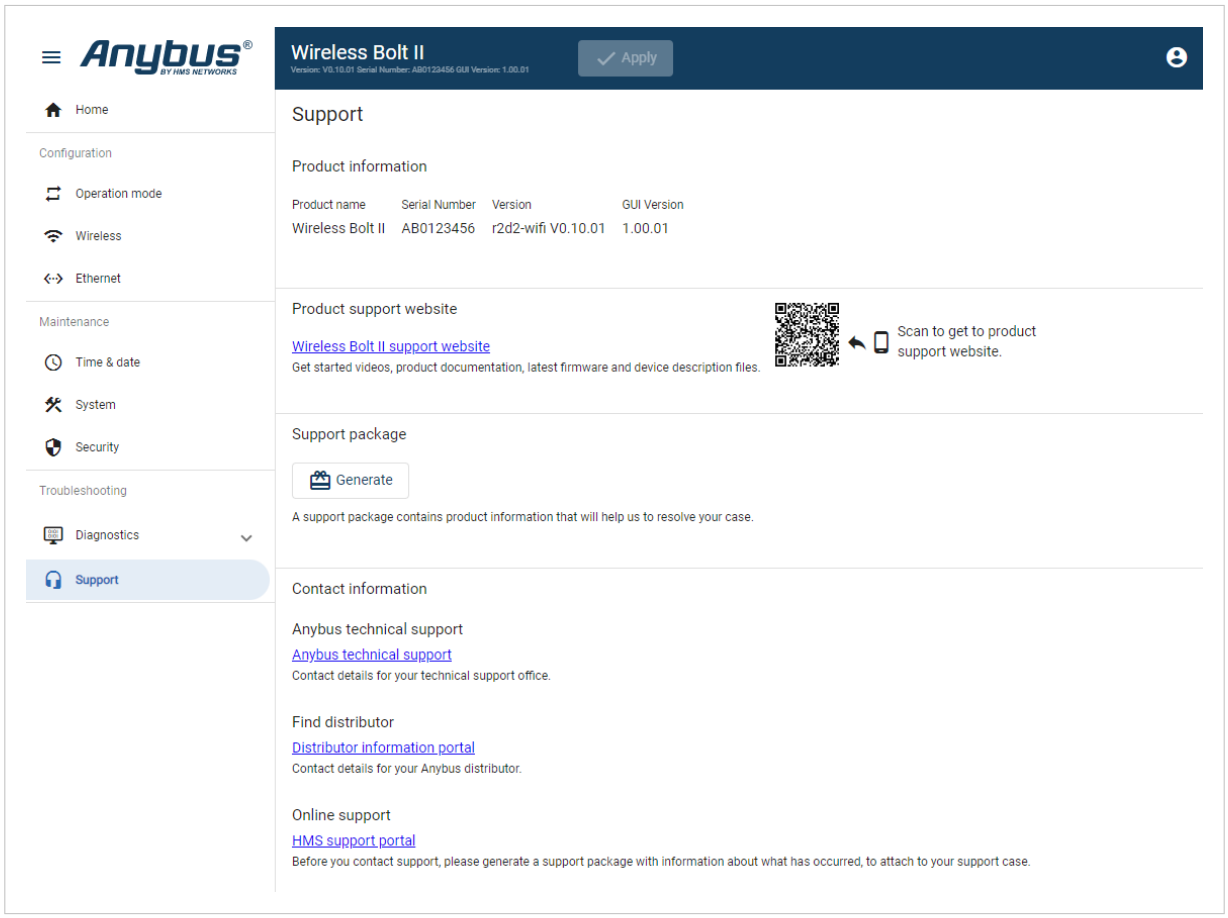


Figure 73. Support page example

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 **Anybus Technical Support** page, navigate to the **Support Center** page and click **HMS Support Portal**.
2. In the **HMS 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 + 12-13 depending on regulatory domain scan 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 600068-2-78: 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.anybus.com/support.