Anybus® Wireless Bolt IoT™

USER MANUAL

SCM-1202-139 1.12 en-US ENGLISH

Connecting Devices™

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.

Table of Contents

Page

1 Preface 3

1.1 About This Document 3
1.2 Document Conventions 4
1.3 Trademarks 4

2 Safety 5

2.1 General Safety Instructions 5
2.2 Intended Use 5

3 Preparation 6

3.1 Support and Downloads 6
3.2 Network Environment 6
3.3 SIM Card 6
3.4 Network Operator Certified Firmware 6
3.5 Placement 7
3.6 Firewall and Routing 7

4 Installation 8

4.1 Installing SIM Card 8
4.2 Mechanical Installation 9
4.3 Connecting to Power Over Ethernet (PoE) 10
4.4 Connecting to Power and Ethernet 11

5 Configuration 14

5.1 Connecting to PC and Power 14
5.2 PC IP Address Setting 15
5.3 Accessing Wireless Bolt IoT Web Interface 16
5.4 Web Interface Overview 17
5.5 Save and Reboot 18
5.6 Factory Default Settings 18
5.7 Ethernet Settings 19
5.8 Cellular Settings 21
5.9 NAT/Port Forward Settings 25
5.10 Positioning Settings 26
5.11 Setting Up with REST Commands 27

6 Configuration Examples 28

6.1 Setting Up Wireless Bolt IoT as an Internet Router 28
6.2 Setting Up Wireless Bolt IoT with ULPM REST Command 31

7 Verify Operation 32
7.1 System Settings and Network Connection 32
7.2 Ethernet LED Status Indication 33

8 Maintenance 34
8.1 Firmware Update 34
8.2 Set Administrator Password 36
8.3 Settings Backup 36
8.4 Reboot System 38

9 Troubleshooting 39
9.1 Logs 39
9.2 Diagnostics 40
9.3 Reset and Recovery 43

10 Technical Data 45
10.1 Technical Specifications 45

1 Preface

1.1 About This Document

This manual describes how to install and configure Anybus Wireless Bolt IoT.

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

1.2 Document Conventions

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

► An action

→ and a result

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

```
Program code and script examples
```

Cross-reference within this document: *Document Conventions, p. 4*

External link (URL): www.hms-networks.com

WARNING
Instruction that must be followed to avoid a risk of death or serious injury.

Caution
Instruction that must be followed to avoid a risk of personal injury.

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.

Additional information which may facilitate installation and/or operation.

1.3 Trademarks

Anybus® is a registered trademark and Wireless Bolt IoT™ is a trademark of HMS Networks AB. All other trademarks mentioned in this document are the property of their respective holders.

2 Safety

2.1 General Safety Instructions

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
Minimum temperature rating of the cable to be connected to the field wiring terminals, 90 °C.

Caution
Use copper wire only for field wiring terminals.

This equipment is recommended for use in both industrial and domestic environments. For industrial environments it is mandatory to use the functional earth connection to comply with immunity requirements. For domestic environments the functional earth must be used if a shielded Ethernet cable is used, in order to meet emission requirements.

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

2.2 Intended Use

The intended use of this equipment is as a communication interface and router. The equipment receives and transmits data over Ethernet and Cellular standard networks.

3 Preparation

3.1 Support and Downloads

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

Have the product article number available, to search for the specific product page.

You find the product article number on the Wireless Bolt IoT product housing.

3.2 Network Environment

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

Ensure that the network operator supports your intended network type(s), *LTE-M (Cat-M1)*, *LTE NB1 (NB-IoT)* or *GSM (2G)*, at the location where Wireless Bolt IoT is to be installed.

3.3 SIM Card

Network Type Considerations

Use a SIM card that supports at least one of the following cellular network type(s):
LTE-M (Cat-M1), *LTE NB1 (NB-IoT)* or *GSM (2G)*

Most SIM cards do not support Radio Access Technology (RAT).

Prepaid Data Plan

If a prepaid data plan is used, ensure that:

- the data amount is sufficient
- that any SMS notifications are sent to a monitored number

3.4 Network Operator Certified Firmware

You may need to install a firmware certified for the operator you are going to use, it is not possible to connect the Wireless Bolt IoT to the operator network otherwise.

Before you start to configure the Wireless Bolt IoT settings:

- Ensure that the current firmware installed on the Wireless Bolt IoT is valid for the network operator you are going to use.
- You find the firmware version number in the Wireless Bolt IoT built-in web interface Overview page. Refer to *Web Interface Overview, p. 17*.
- If you need to install a firmware version certified for your network operator:

  Download the firmware update file, specific for your network operator, from www.anybus.com/support.
- For information on how to update the firmware, refer to *Firmware Update, p. 34*.

3.5 Placement

For optimal reception, cellular devices should not be confined in buildings made of concrete or metal, without windows.

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

At least 20 cm separation distance between the device and the user's body must be maintained at all times.

3.6 Firewall and Routing

There are routing options set for the system.

By default, the firewall allow routing of:

- Outgoing traffic for TCP, UDP and ICMP (for ipv4 only).
- Ingoing traffic for already established connections only.

For other possible configurations, refer to *NAT/Port Forward Settings, p. 25*.

4 Installation

4.1 Installing SIM Card

Supported SIM card types are Nano SIM for IoT and M2M, for data communication, as well as standard mobile phone Nano SIM.

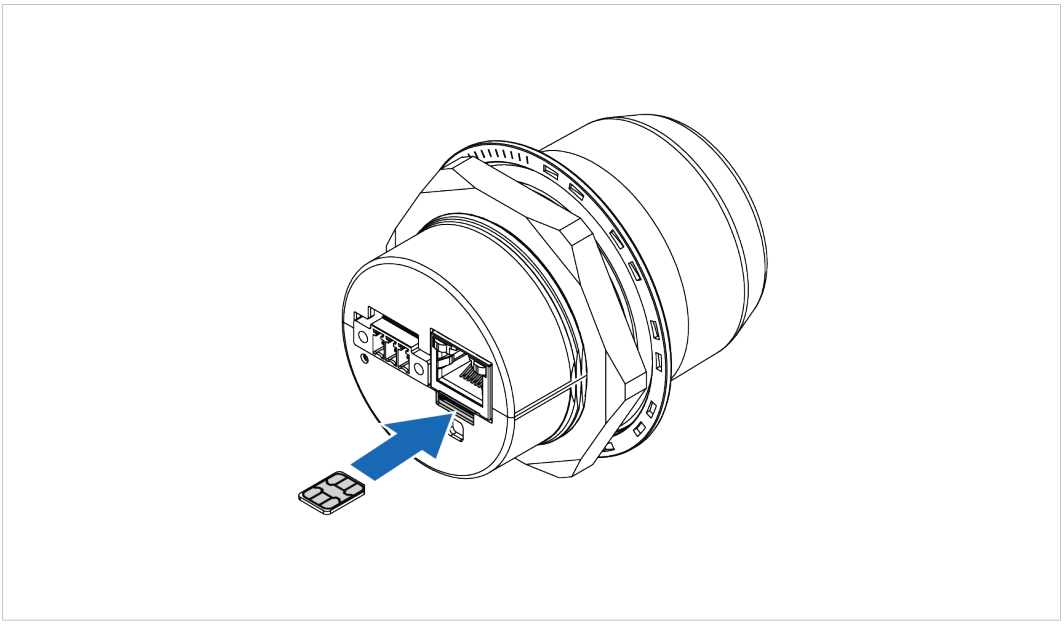


Fig. 1

To connect Wireless Bolt IoT to a cellular data network, install a cellular SIM card:

1. Insert a *SIM card* into the Wireless Bolt IoT *SIM card holder.*

Ensure that the SIM card contact surface is facing towards the Ethernet port.

4.2 Mechanical Installation

Placement

- The device is intended to be mounted on top of a machine or cabinet through an M50 (50.5 mm) hole using the included sealing ring and nut.
- The top mounting surface, in contact with the sealing, must be flat with a finish equivalent to Ra 3.2 or finer and cleaned and free from oils and greases.
- For optimal reception, cellular devices require a zone around them clear of objects that could obstruct or reflect the signal. To avoid interference, a minimum distance of 50 cm between Wireless Bolt IoT and other cellular devices should be observed.

> **!** Make sure that the sealing ring is correctly placed in the circular groove in the top part of the housing before tightening the nut.

> **!** Always hold the BOTTOM part of the unit when untightening the nut, not the top part (the cap).

Tightening torque: 5 Nm ±10 %

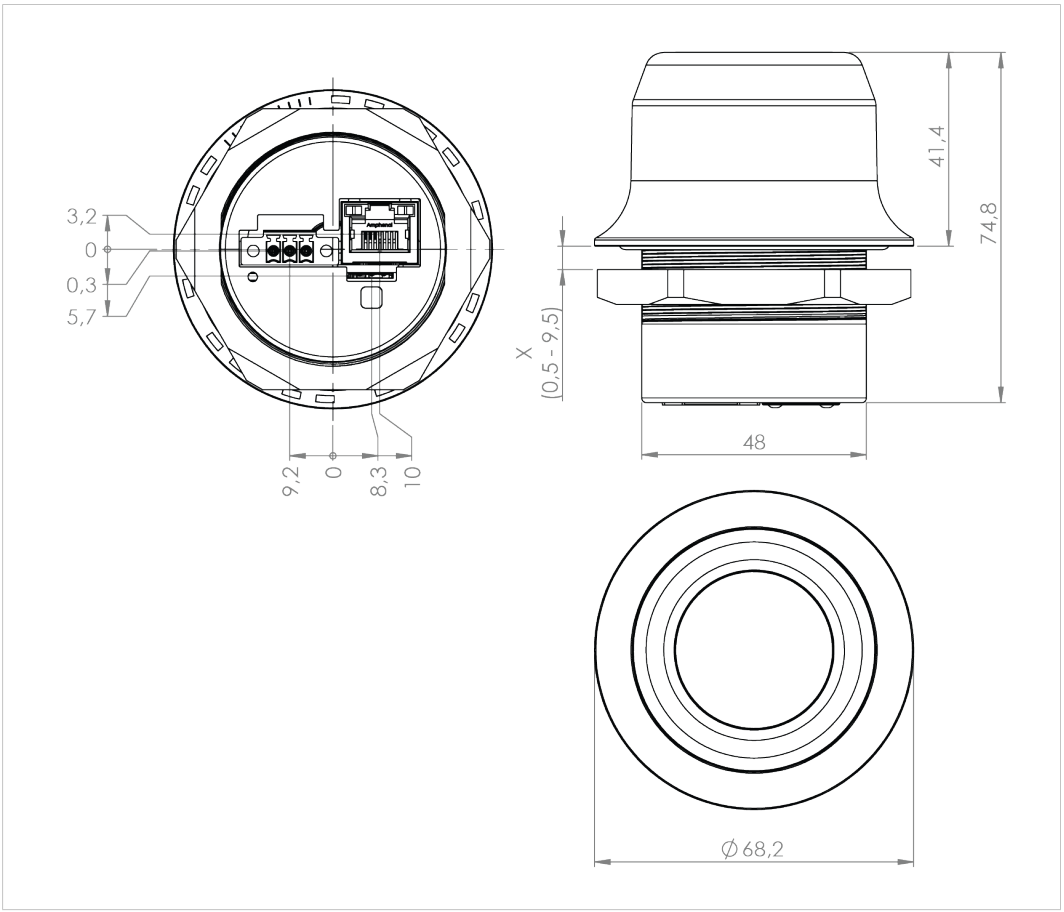


Fig. 2 Installation drawing

All measurements are in mm.

4.3 Connecting to Power Over Ethernet (PoE)

Before You Begin

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

Shielded or unshielded Ethernet cables may be used.

Wireless Bolt IoT is designed to comply with PoE class 0 (37-57 VDC, max 0.35 A), according to IEEE 802.3.

Procedure

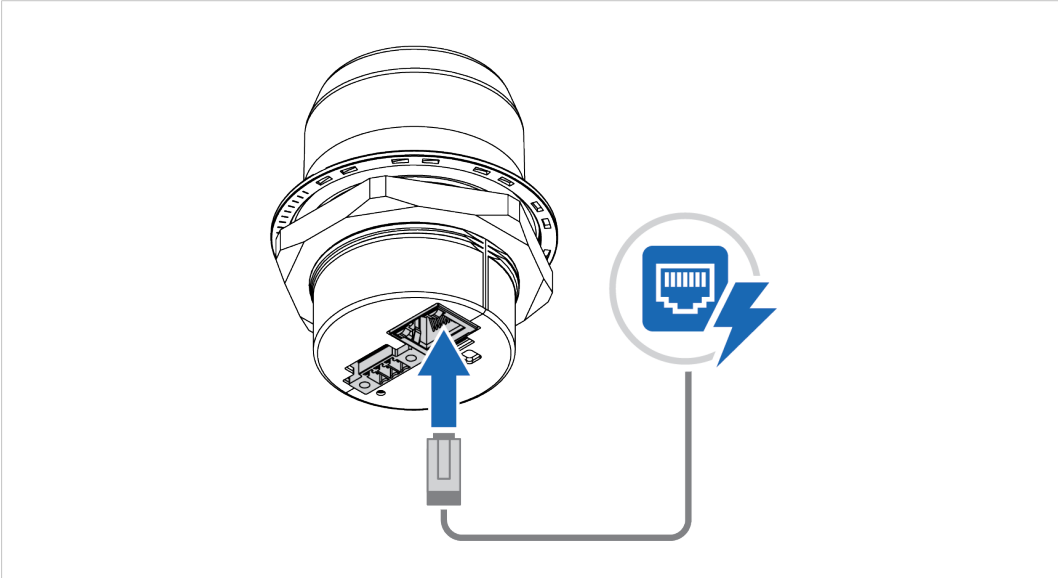
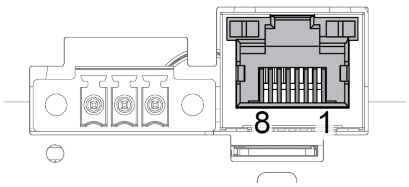


Fig. 3

1. Connect the Wireless Bolt IoT *Ethernet port* to Ethernet/PoE.

Ethernet Connector, RJ45 PoE



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

4.4 Connecting to Power and Ethernet

Before You Begin

> **!** 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.

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

> **!** When Wireless Bolt IoT is powered via the power connector, Functional Earth (FE) must be connected.

> *When Wireless Bolt IoT is installed in an environment with a high level of electrical noise, use a power/ Functional Earth (FE) cable with a maximum length of 3 meters.*

See also *Technical Data, p. 45* regarding power supply requirements.

Functional earth wire screw placement

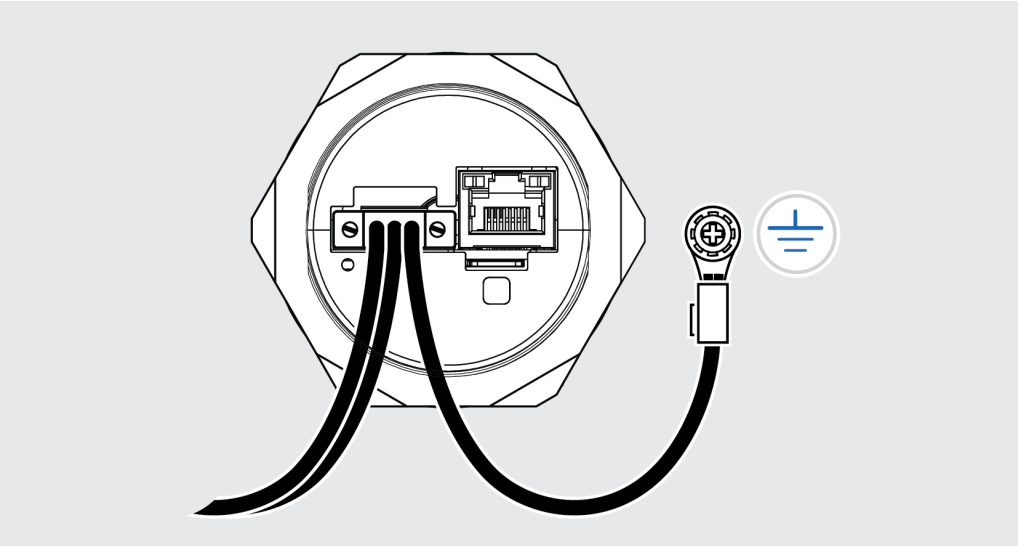


Fig. 4

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

Procedure

Connecting to power

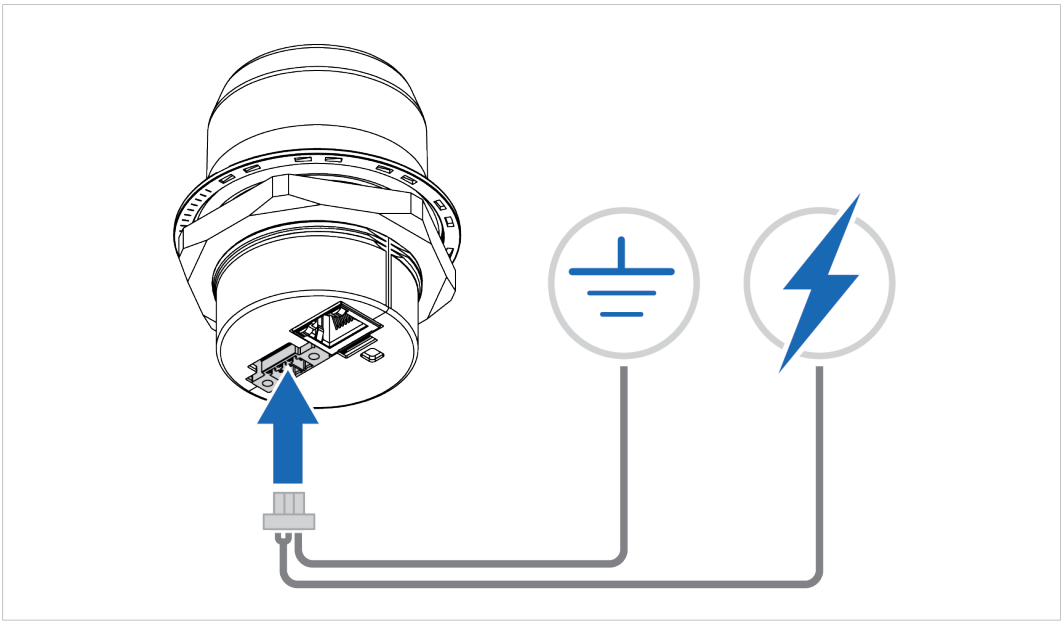
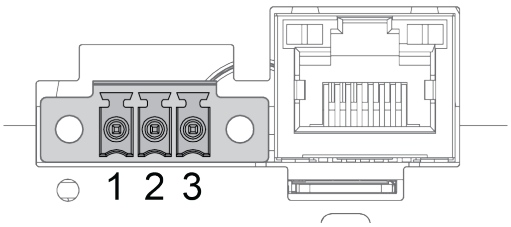


Fig. 5

1. Connect Wireless Bolt IoT *Power connector* to a power supply.
2. Connect Wireless Bolt IoT *Power connector* to Functional Earth (FE).

Power connector, 3-pin terminal block



Pin	Function	
1	+	11–33 VDC
2	-	
3	Functional Earth (FE)	

Connecting to Ethernet

3. Connect the Wireless Bolt IoT to Ethernet.

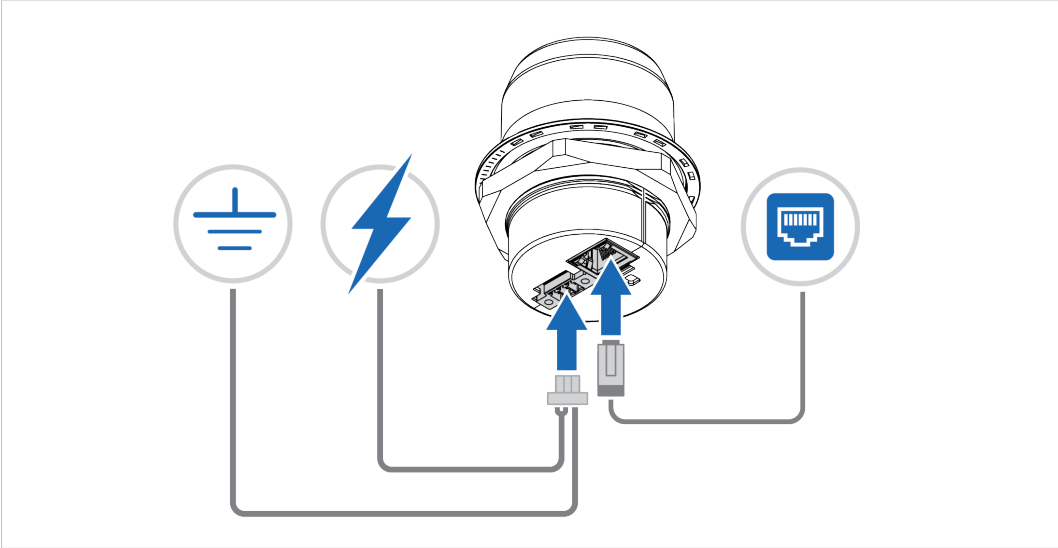


Fig. 6

5 Configuration

5.1 Connecting to PC and Power

When configuring Wireless Bolt IoT it must be connected to a PC.

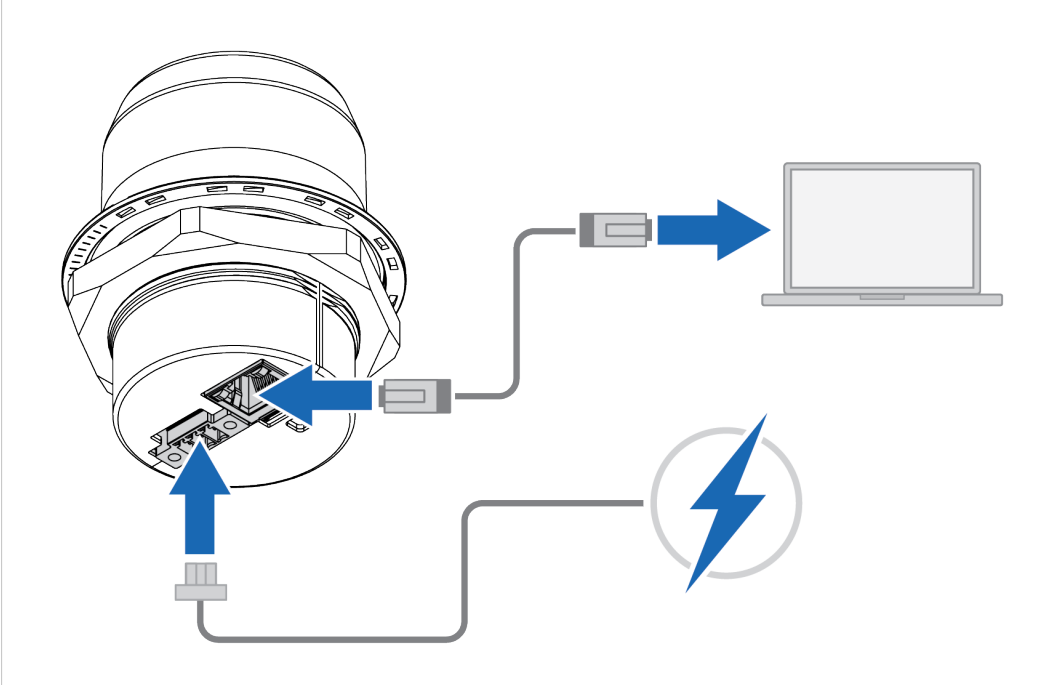


Fig. 7

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

5.2 PC IP Address Setting

> **!** By default, the Wireless Bolt IoT internal DHCP server is enabled.
> To avoid interference, keep only one DHCP server enabled on the network.

*Wireless Bolt IoT default IP address is **192.168.0.98**.*

To find Wireless Bolt IoT on your network, choose one of the following methods:

To find Wireless Bolt IoT on your network:

Set a Static IP Address on Your PC

On the PC accessing the Wireless Bolt IoT built-in web interface:

1. Set a static IP address within the same IP address range as the Wireless Bolt IoT IP address.

Finding Wireless Bolt IoT with IPconfig

1. Download the HMS software application IPconfig installation files and user documentation from www.anybus.com/support.
2. Install IPconfig on your PC.
3. In IPconfig, start a network scan to find the Wireless Bolt IoT IP address on your network.
4. Set an IP address on the *Wireless Bolt IoT Ethernet port* within the same IP address range as your PC IP address.

Result

→ Now you can enter the Wireless Bolt IoT IP address in your web browser and search to access the built-in web interface login page.

Refer to *Accessing Wireless Bolt IoT Web Interface, p. 16*

5.3 Accessing Wireless Bolt IoT Web Interface

The Wireless Bolt IoT built-in web interface can be accessed from standard web browsers.

> **!** Before installing the Wireless Bolt IoT on a network, change the Wireless Bolt IoT default password.

> *The Wireless Bolt IoT comes with a default username and password.*
> *The default username is **admin**. Written in lowercase letters.*
> *You find the default password on the Wireless Bolt IoT product housing.*

> *Wireless Bolt IoT default IP address is **192.168.0.98**.*

Login to the Wireless Bolt IoT built-in web interface:

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

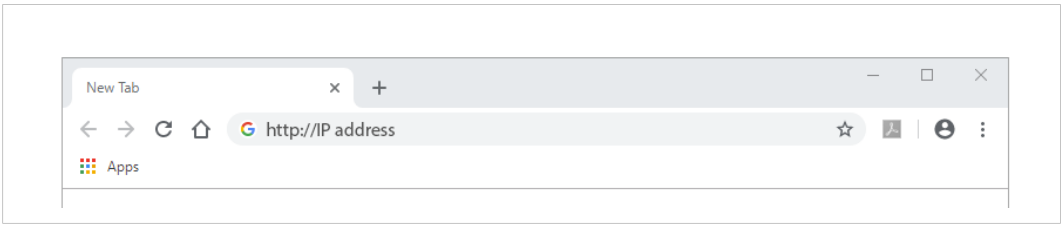


Fig. 8

3. Press **Enter**.
   → The built-in web interface login screen appears.
4. Enter *Username* and *Password* and click **Sign in**.

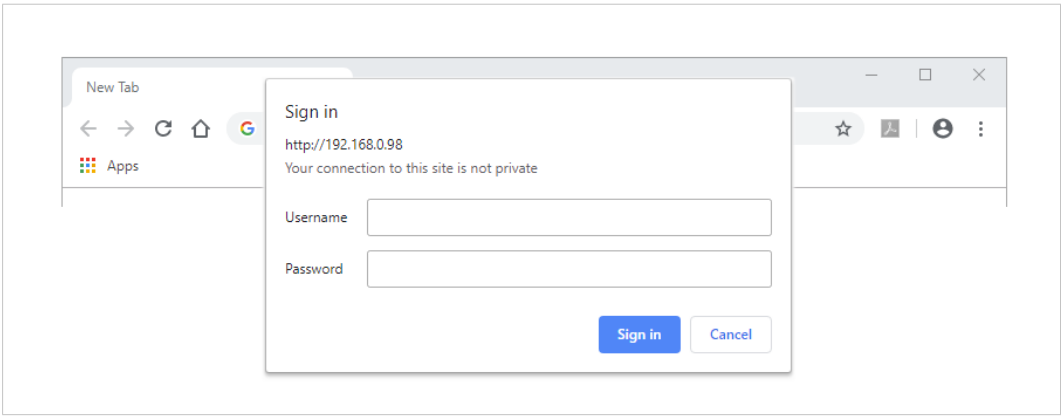


Fig. 9

5.4 Web Interface Overview

The Wireless Bolt IoT built-in web interface is used to configure the Wireless Bolt IoT system settings as well as for diagnostics and maintenance.

The *System Overview* page shows the current settings and network connection status.

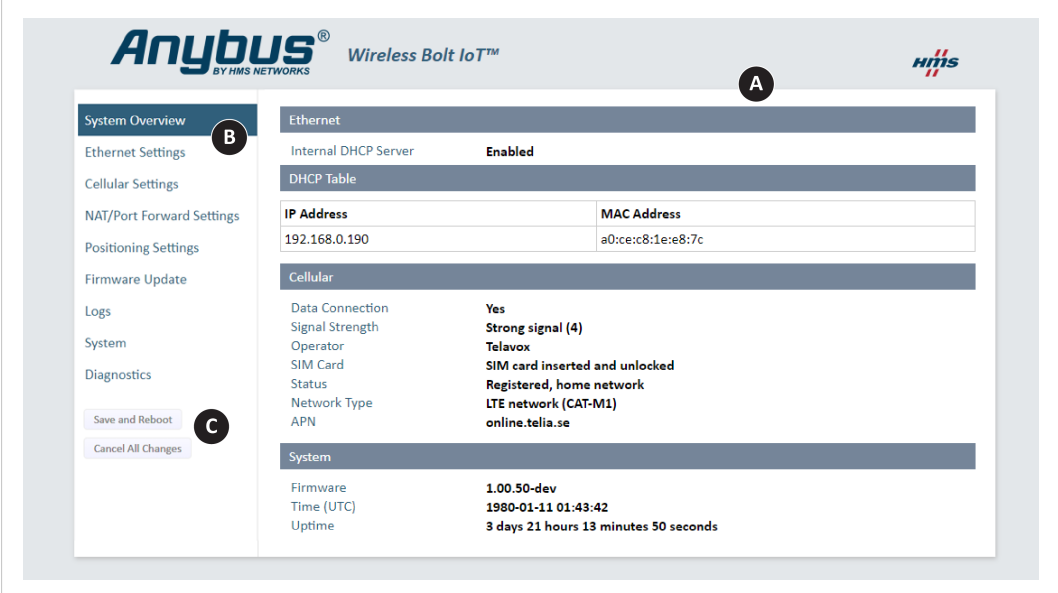


Fig. 10 Wireless Bolt IoT built-in web interface, example

A. **System Overview**
Shows the current settings and network connection status

B. **Left sidebar menu**

- System Overview
- Ethernet Settings
- Cellular Settings
- NAT/Port Forward Settings
- Positioning Settings
- Firmware Update
- Logs
- System
- Diagnostics

C. **Save and Reboot** button and **Cancel All Changes** button

5.5 Save and Reboot

Cancel Changes

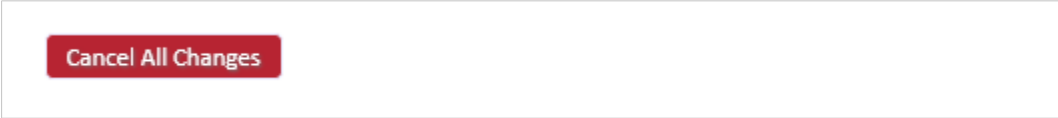


Fig. 11

If you need to cancel the changes you have made to the settings:

1. In the left sidebar menu, click **Cancel All Changes**.

To restore settings, refer to *Restore Settings, p. 37*.

Apply Changes

Fig. 12

To apply changes:

1. In the left sidebar menu, click **Save and Reboot**.
   → Wireless Bolt IoT restarts for the changes to take effect.

5.6 Factory Default Settings

Wireless Bolt IoT comes with the following factory default settings.

Wireless Bolt IoT default settings	
IP Assignment	Static
IP Address	192.168.0.98
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.98
Internal DHCP Server	Enabled
Network Type	Modem Preset List Connects automatically to an available network according to priority order LTE-M (Cat-M1), LTE NB1 (NB-IoT) and GSM (2G) mobile network.
Incoming Traffic	NAT/Port Forward incoming traffic is Disabled.

You can restore factory default settings by making a *Factory Reset*. Refer to *Factory Reset, p. 43*

5.7 Ethernet Settings

On the **Ethernet Settings** page:

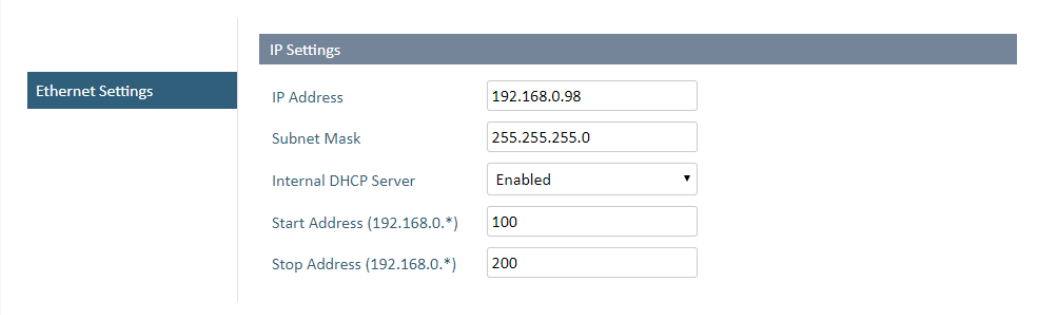


Fig. 13 Default, IP Settings with Internal DHCP Server Enabled

IP Settings

IP Address

*The default Wireless Bolt IoT static IP address is **192.168.0.98**.*

When you change the IP address:

1. Click **Save and Reboot** to reboot Wireless Bolt IoT.
   → Wireless Bolt IoT reboots for the setting to take effect.
2. In your web browser, enter the new IP address and press **Enter**.
   → The built-in web interface login screen appears.
3. Enter *Username* and *Password* and click **Sign in**.

Subnet Mask

*The default subnet mask is **255.255.255.0**.*
The subnet mask identifies the subnetwork to which the static IP address belongs.

Internal DHCP Server

> **!** By default, the Wireless Bolt IoT internal DHCP server is enabled.
>
> To avoid interference, keep only one DHCP server enabled on the network.

The DHCP server is only enabled on the LAN interface.

By default, **Internal DHCP Server** is set to **Enabled**.

→ This means that the IP address settings are set automatically by the Wireless Bolt IoT internal DHCP server.

IP Address Range

When the Wireless Bolt IoT is enabled, you can still use static IP addresses within the remaining IP address range. The devices assigned to these IP addresses can set Wireless Bolt IoT as the default gateway and DNS server.

The *internal DHCP server address* host ID range is by default set to start at 100 and stop at 200.

You can set a preferred host ID range.

5.8 Cellular Settings

When you are going to connect Wireless Bolt IoT to a cellular network, make sure that you have installed a SIM card in *Wireless Bolt IoT SIM card holder.*

Refer to *Installing SIM Card, p. 8*.

5.8.1 Network Settings

Before You Begin

- When using the *LTE-M* technology, it can take several hours for a device to get connected to the cellular network.
- It can take up to one hour to connect to a *LTE NB1* network.
- If the SIM card does not support *LTE-M* or *LTE-NB1* set the Preferred Network Type to GSM.

About Preferred Network Type

By default, the **Preferred Network Type** is set to **Modem Preset List**.

The most recently registered network type takes precedence.

When a specific Preferred Network Type is selected and available, the Wireless Bolt IoT modem might remain locked to that network type, even if you switch to Modem Preset List.

Solution: If the Wireless Bolt IoT modem is locked to a network type you do not want to use, ensure that the network type is no longer available to the Wireless Bolt IoT. The Wireless Bolt IoT modem then selects the next available network type.

Procedure

On the **Cellular Settings** page:

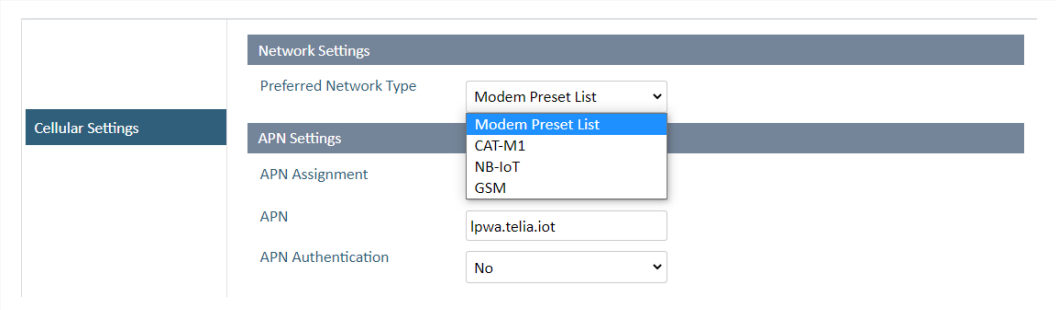


Fig. 14

1. Select a Preferred Network Type:

Setting	Description
Modem Preset List	Use the Modem Preset List search order for Radio Access Technology (RAT). Connects automatically to an available network according to following priority order LTE-M, LTE NB1 and GSM mobile network. The Wireless Bolt IoT modem scans for all available Public Land Mobile Networks (PLMN) in each RAT.
LTE-M	Use LTE-M (Cat-M1) network.
LTE NB1	Use LTE NB1 (NB-IoT) network.
GSM	Use GSM (2G) mobile network.

5.8.2 APN Settings

On the **Cellular Settings** page:

Automatic APN Assignment

> **!** An APN automatically derived from SIM card identification may not give full access to the cellular network. Follow your network operator's guidelines.

> **!** By default, Wireless Bolt IoT is set to automatically search for the SIM card APN setting.
>
> If a general APN string is available for the network operator, it will be set as the APN Assignment.
>
> Ensure that the general APN string is recommended by the network operator and in accordance with the SIM card IoT data plan.

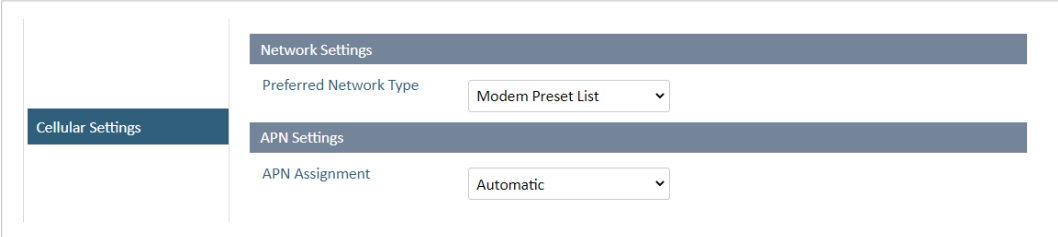


Fig. 15

The **APN Assignment** is by default set to **Automatic**.

→ The *APN* (Access Point Name) is assigned automatically.

Manual APN Assignment

You can set the APN Assignment manually.

Ensure that you have the APN supplied by your carrier available.

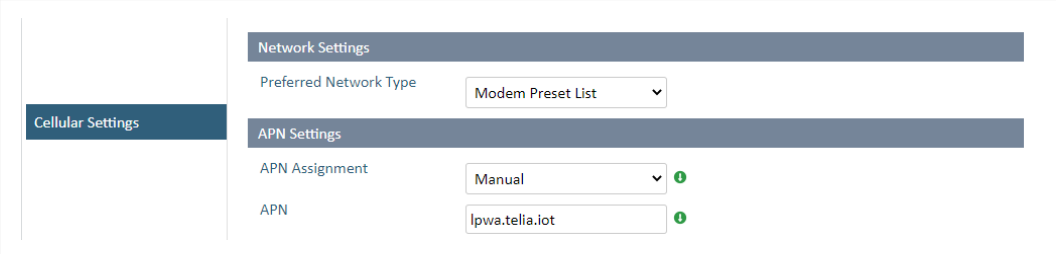


Fig. 16 APN example

1. Enter the *APN* in the **APN** field.

APN Authentication

By default, **APN Authentication** is set to **No**. When enabled, PAP method is used.

APN Authentication *is to be configured only if your carrier has setup APN (Access Point Name) with username and password.*

Ensure that you have the APN username and password supplied by your carrier available.

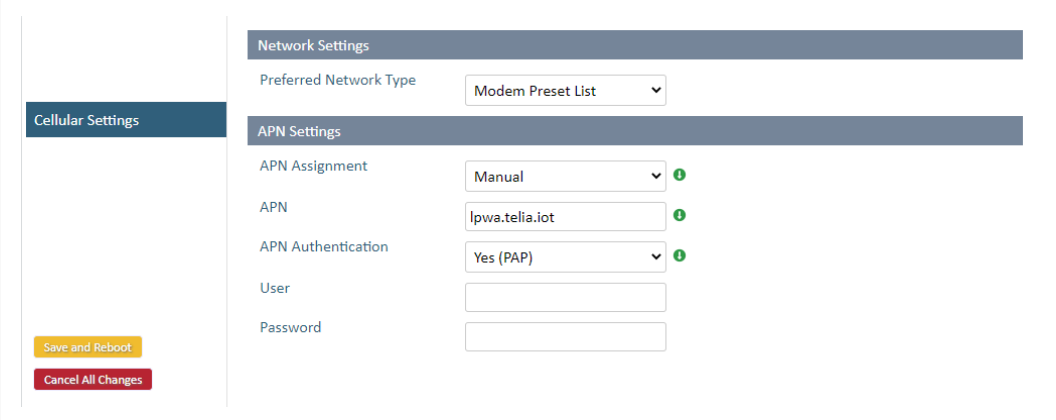


Fig. 17

To activate APN Authentication:

1. Set the **APN Authentication** setting to **Yes (PAP)**.
2. In the **User** field, enter a username.
3. In the **Password** field, enter a password.
4. In the left sidebar menu, click **Save and Reboot**.
   → Wireless Bolt IoT automatically reboots for the settings to take effect.

5.8.3 Lock Configuration

When configuration is locked, you can still access and use the Wireless Bolt IoT built-in web interface but the settings can not be configured.

On the **System** page:

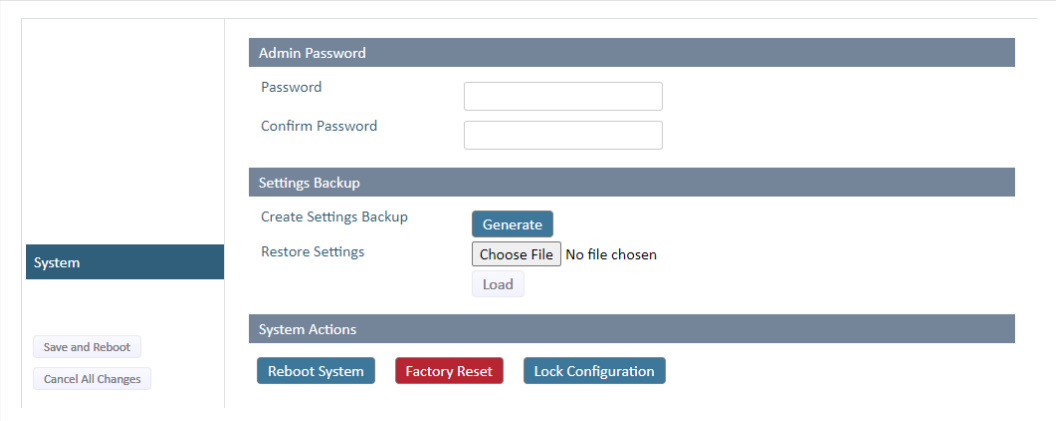


Fig. 18 Restore Settings from a backup file

To lock the configuration:

1. Click **Config Lock**.
2. To confirm lock configuration, click **OK**.

5.8.4 Unlock Configuration

To unlock configuration, do a factory reset using the Wireless Bolt IoT **Reset** button.

Refer to *Reset and Recovery, p. 43*.

5.9 NAT/Port Forward Settings

NAT/Port forward is used to allow incoming traffic from an external (cellular mobile-radio) network access to a device IP address on the internal (Ethernet) network.

The Source Filter setting is used to prevent unauthorized traffic on the local network.

By default, Incoming Traffic **NAT 1:1** is set to **Disabled**. All incoming traffic from the external network is rejected.

Procedure

On the **NAT/Port Forward Settings** page:

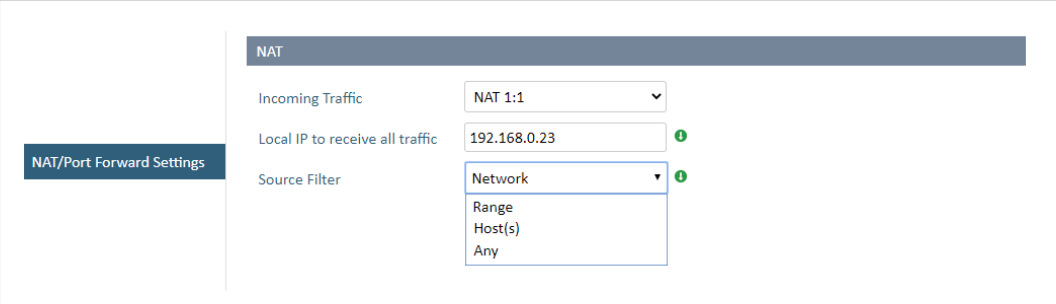


Fig. 19

To configure the NAT 1:1 settings:

1. In the **Incoming Traffic** drop down menu, select **NAT 1:1**.
2. In the **Local IP to receive all traffic** field, enter the IP address to receive all incoming traffic from the external network.
3. In the **Source Filter** drop down menu, select the desired source filter.

Source Filter adds a layer of security on the internal network. The source filter controls which IP addresses on the external network that have access to the Local IP address.	
Source Filter	**Description**
Network	Default setting Allow any IP address on a specific network to access the Local IP address. Enter **Source base IP** and **Source IP netmask**.
Range	Allow a specific IP address range to access the Local IP address. Enter the **Source IP range start** and **Source IP range stop** addresses.
Host(s)	Allow a specific host(s) to access the Local IP address. Enter **Source IP(s)**. You can add up to five Source IP(s).
Any	Allow any external IP address to access the Local IP address.

Result

→ The communication is redirected to one specific device IP address on the local network, that will receive all incoming traffic from the external network.

5.10 Positioning Settings

Use the positioning function to locate the position of the Wireless Bolt IoT.

For example, to send the Wireless Bolt IoT position to an application via the REST API.

By default, Positioning Service is **Disabled**.

Procedure

To activate Positioning Service:

1. On the Positioning Settings page, select **Enable** from the Positioning Service drop down menu.

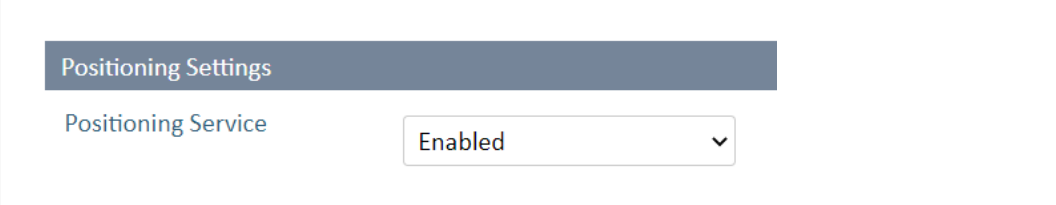


Fig. 20

2. In the left sidebar menu, click **Save and Reboot**.

   → Wireless Bolt IoT automatically reboots for the setting to take effect.

Result

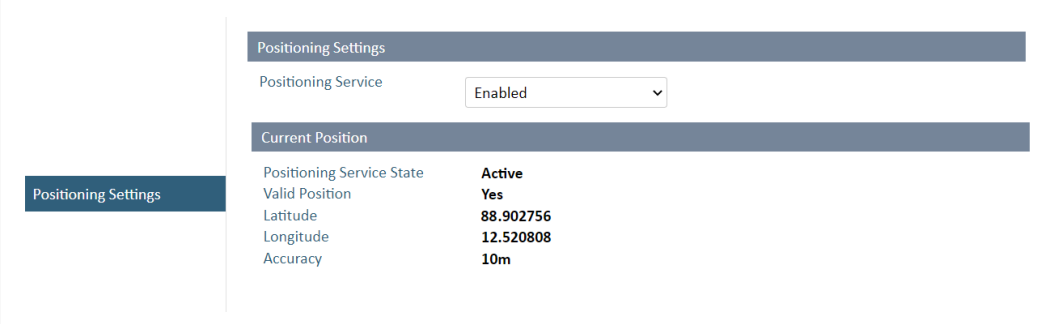


Fig. 21 Example, Current Position information

In Current Position you can view the following information.

Positioning Service State	When the Positioning Service is: • Enabled the status is Active. • Disabled the status is Disabled.
Valid Position	Yes: The satellite coverage is sufficient to provide a position. No: The satellite coverage is insufficient to provide a position. This can occur: • at startup, before the Wireless Bolt IoT has found enough satellites to provide a position. • if the Wireless Bolt IoT is installed in a location where the satellite coverage is poor.
Latitude	The latitude of the Wireless Bolt IoT current location
Longitude	The longitude of the Wireless Bolt IoT current location
Accuracy	The closeness of the measured location to the actual location of the Wireless Bolt IoT.

5.11 Setting Up with REST Commands

5.11.1 How To Use REST Commands

For information about the supported REST commands and how to use them, refer to the REST Commands Reference Guide at www.anybus.com/support.

5.11.2 Use/Test REST Commands From a Web Browser

For information about the supported REST commands, refer to the REST Commands Reference Guide at www.anybus.com/support.

Procedure

1. Setup the Wireless Bolt IoT as an internet router. Refer to *Setting Up Wireless Bolt IoT as an Internet Router, p. 28*

To send the REST command to the Wireless Bolt IoT:

2. Connect the Wireless Bolt IoT to your PC and log in to the Wireless Bolt IoT built-in web interface.
3. Open a new tab in your web browser.
4. Enter the desired command string in the **Address bar**.
5. To send the string, press **Enter**.

Result

→ The command is sent to the *TCP port 80* on the Wireless Bolt IoT Ethernet interface.

→ The Wireless Bolt IoT enters the state requested by the REST command.

Example 1: URL

```
http://192.168.0.99/cgi-bin/info.cgi
```

Example 2: Response


```
{"uptime":"338053","time":"1980-01-11 02:24:04",
"radio_power":"1","sim":"2","signal_strength":"4",
"signal_strength_raw":"22","signal_quality":"-10",
"cell_id":"26650646",""operator":"Telavox","status":"1",
"amplifier_temp":"31","controller_temp":"31","connection_state":"2",
"voltage":"3868","iotbolt_version":"1.00.50-dev",
"modem_version":"SWI9X06Y_02.16.06.00","pri":"GENERIC_001.028_004",
"apn":"online.telia.se","rat_specific":"7","imsi":"240017431192642",
"imei":"352653090225053","cellular_gateway":"10.209.230.108",
"cellular_ip":"10.209.230.107","iccid":"89460100174311926424"}
```

6 Configuration Examples

6.1 Setting Up Wireless Bolt IoT as an Internet Router

Use Wireless Bolt IoT as an internet router to connect machines, controllers or other devices to internet.

Before You Begin

Wireless Bolt IoT comes with a default username and password.

*The default username is **admin**. Written in lowercase letters.*

You find the default password on the Wireless Bolt IoT product housing.

*Wireless Bolt IoT default IP address is **192.168.0.98**.*

To access the Wireless Bolt IoT built-in web interface, ensure that the Wireless Bolt IoT IP address and your PC IP address are within the same IP address range.

Procedure

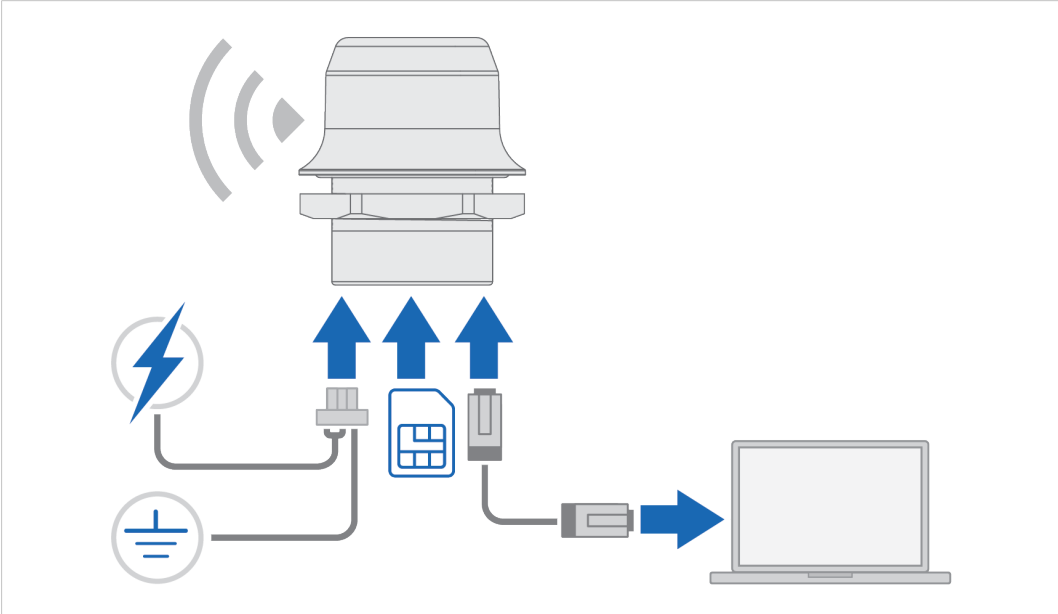


Fig. 22

Connecting Wireless Bolt IoT to internet:

1. Insert a *cellular SIM card* in the Wireless Bolt IoT *SIM card holder.*

Ensure that the SIM card contact surface is facing towards the Ethernet port.

2. Connect the Wireless Bolt IoT *Ethernet port* to your PC.
3. Connect the Wireless Bolt IoT *Power connector* to a power supply.
4. To access the built-in web interface, enter the Wireless Bolt IoT IP address in your web browser and click Enter.
5. Login to the Wireless Bolt IoT built-in web interface.

6. Configure the **Ethernet Settings**, IP address and internal DHCP server settings.
7. Verify that the **APN Settings** are correct. You can adjust the settings manually.
8. In the left sidebar menu, click **Save and Reboot**.
   → Wireless Bolt IoT automatically reboots for the settings to take effect
9. On the **System Overview** page, verify that the cellular **Data Connection** has status **Yes**.

Result

Wireless Bolt IoT should now be connected to internet.

Depending on the mobile network operator and network type, it can take up to 10 minutes the first time Wireless Bolt IoT is connecting to internet.

Verify that Wireless Bolt IoT is connected to internet, by sending a ping to *Google Public DNS*.

1. On the **Diagnostics** page, select the **Ping** method.
2. In the **Target** field, enter the IP address *8.8.8.8*.
3. To **Perform Action**, click **Start**.
   → The ping request is sent.
   → When the ping response return, a message appears.

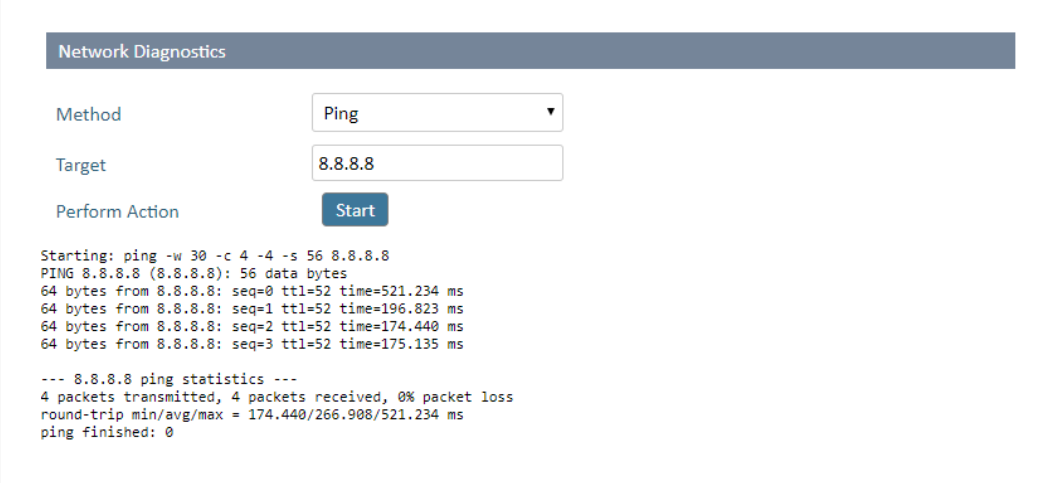


Fig. 23 **Example, Ping response message from Target 8.8.8.8**

Connecting Devices

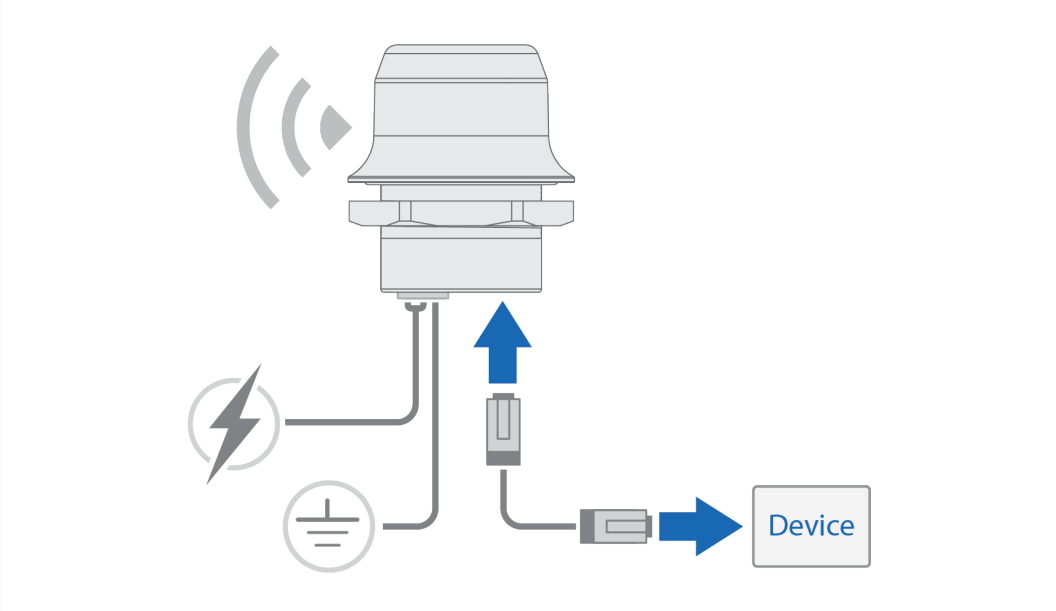


Fig. 24

Connecting a device to internet:

1. Connect an Ethernet cable between Wireless Bolt IoT and the device.
2. Verify that the device is connected to internet.

6.2 Setting Up Wireless Bolt IoT with ULPM REST Command

The Wireless Bolt IoT variant for the US market does not support the ULPM REST Command.

You can use Wireless Bolt IoT as an internet router with Ultra Low Power Mode (ULPM) to save electrical energy.

Devices using other power sources than grid connected power, such as devices powered by batteries and/or solar panels, benefit from using ULPM.

Before You Begin

Setup Wireless Bolt IoT as an internet router, refer to *Setting Up Wireless Bolt IoT as an Internet Router, p. 28*.

Procedure

To put the Wireless Bolt IoT in ULPM for a specified duration:

1. Connect the Wireless Bolt IoT to your PC.
2. Open a web browser.
3. Enter the *ULPM command* together with the desired *ULPM sleep time* string in the **Address bar**.
4. To send the string, press **Enter**.

Result

→ The command is sent to the *TCP port 80* on the Wireless Bolt IoT Ethernet interface.

→ The Wireless Bolt IoT enters ULPM and wakes up after the specified time has elapsed.

A power cycle will cancel ULPM. When power is restored, the ULPM command must be re-sent for the Wireless Bolt IoT to re-enter ULPM.

Example 3: Enter ULPM and sleep for 300 seconds (5 minutes)

```
Query:  http://192.168.0.98/cgi-bin/ulpm.cgi?duration=300
 Response: {"success":true,"message":"sleeping for 300 s"}
```

For more information about the REST commands, refer to *Use/Test REST Commands From a Web Browser, p. 27*.

7 Verify Operation

7.1 System Settings and Network Connection

On the **System Overview** page, verify the settings and network connection status.

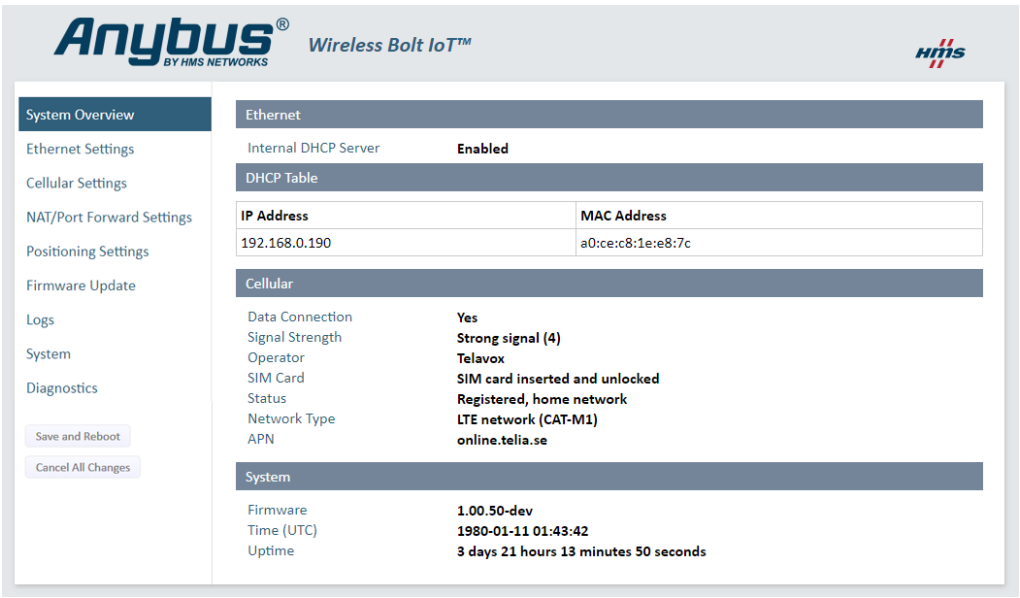


Fig. 25 Example, Verify Settings and Network Connection

Data Connection

Data Connection status *Yes* is picked up from the underlying system and is not tested for data transfer.

The Wireless Bolt IoT modem may get a control connection, but once data is sent the connection is terminated immediately.

This can be caused by discrepancy between the selected network technology, the SIM card and the operator setting.

To troubleshoot the cause of the termination, analyze the **System Log**, refer to *Logs, p. 39*.

If the problem recurs, contact your network operator.

7.2 Ethernet LED Status Indication

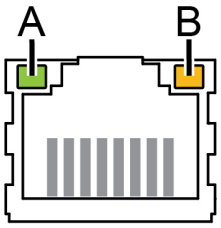


Fig. 26 RJ45 LED indicators

LED A – LINK/ACTIVITY	Function
Off	No Ethernet link
Yellow	10 Mb/s Ethernet link established
Yellow, flashing	10 Mb/s Ethernet activity
Green	100 Mb/s Ethernet link established
Green, flashing	100 Mb/s Ethernet activity

LED B – STATUS	Function
Off	No power
Blue	Connected on LTE-M
Purple	Connected on LTE NB1
Blue, slow blink	Connected on GSM.
Alternating blue/purple	Trying to connect
Red, slow blink	No configured cellular interface/no SIM card/no valid configuration
Red	Recoverable/unrecoverable fault
Yellow	Booting or sleep

8 Maintenance

8.1 Firmware Update

Update Wireless Bolt IoT firmware.

The configuration settings are not affected when updating firmware.

- Download the *firmware update file* from www.anybus.com/support.
- Connect Wireless Bolt IoT to your computer, refer to *Connecting to PC and Power, p. 14*.

On the **Firmware Update** page:

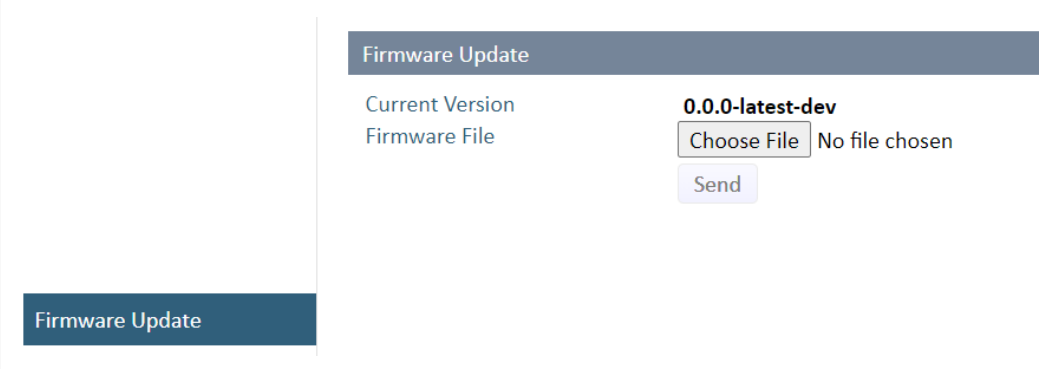


Fig. 27 Firmware Update

1. Click **Choose File**.
2. In the **Open** dialog box, browse to and select the *firmware update file* and click **Open**.
3. To start the file transfer, click **Send**.

Do not refresh or leave the Firmware Update page until the process has finished.

Firmware update:

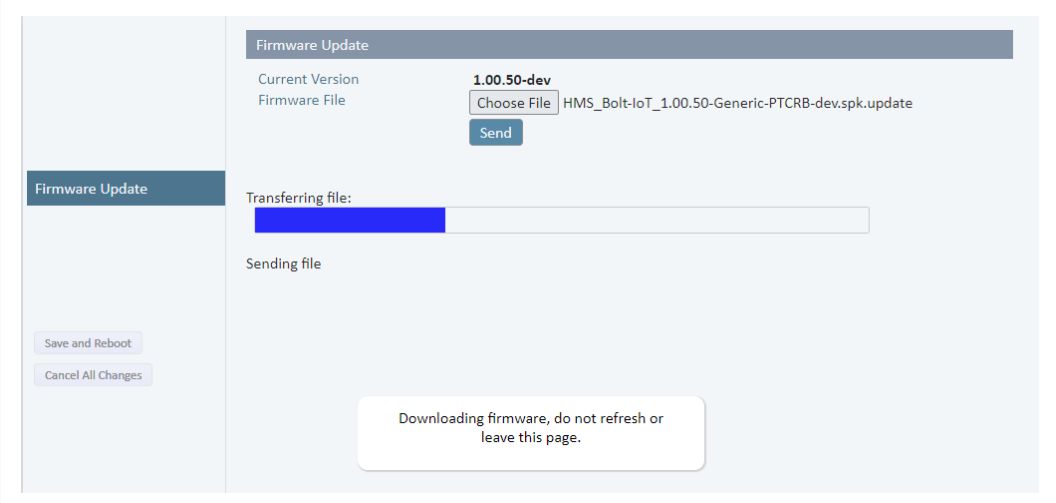


Fig. 28 Firmware Update

→ The progress bar, Transferring file, indicates the progress of the file transfer.

Status messages show the progress of the firmware update stages.

→ When the file transfer is finished, the progress bar turns green.

Reboot:

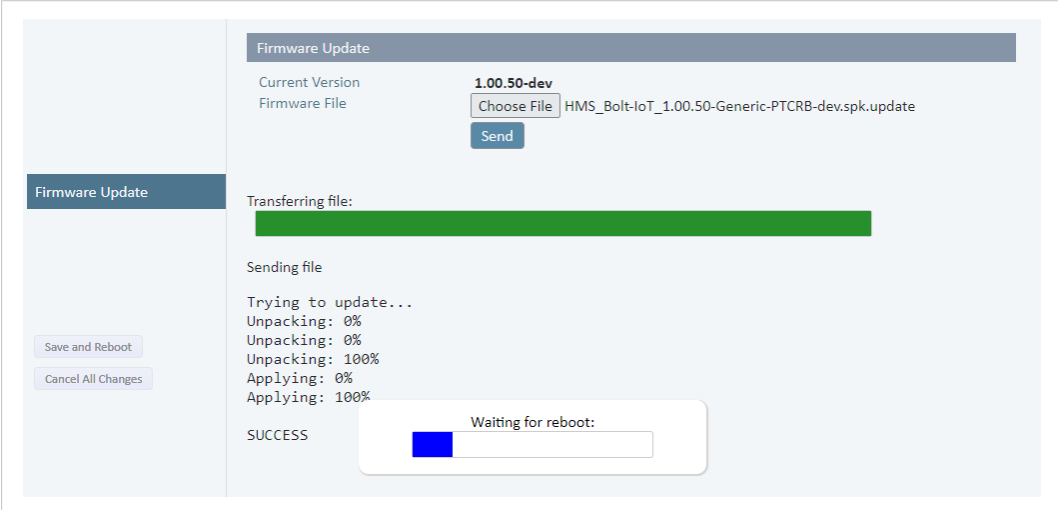


Fig. 29 Firmware Update

→ When the firmware update is finished, Wireless Bolt IoT automatically reboots for the updates to take effect.

The progress bar, Waiting for reboot, indicates the progress.

→ When the reboot is complete, the web browser automatically redirects to the **System Overview** page.

8.2 Set Administrator Password

> **!** Before installing Wireless Bolt IoT on a network, change the default administrator password.

> *Wireless Bolt IoT comes with a default username and password.*
> *The default username is **admin**. Written in lowercase letters.*
> *You find the default password on the Wireless Bolt IoT product housing.*

On the **System Settings** page, **Admin Password** pane:

Fig. 30 Set Admin Password

1. In the **Password** field, enter your preferred admin password.
2. To confirm the admin password, enter it in the **Confirm Password** field.
3. In the left sidebar menu, click **Save and Reboot**.
   → Wireless Bolt IoT restarts and you will be prompted to log in to the web interface with the new admin password.

8.3 Settings Backup

8.3.1 Create Settings Backup

On the **System** page:

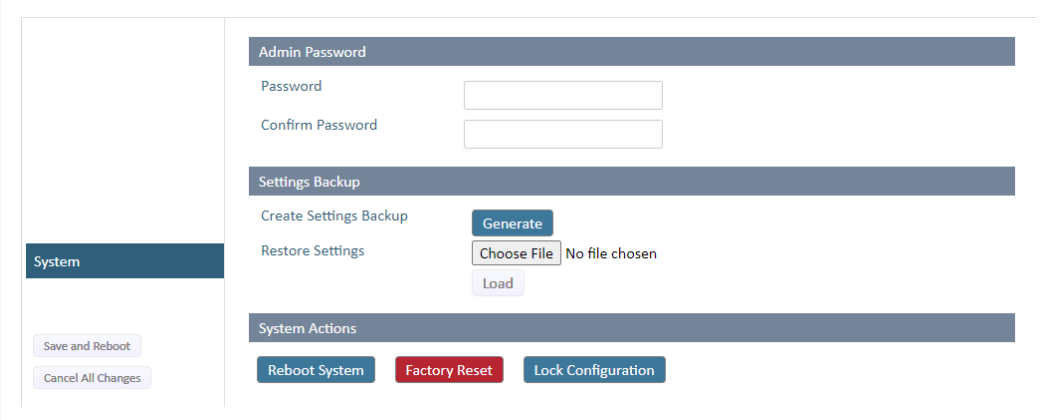


Fig. 31 Generate backup file

Create a Settings Backup:

1. To save the current configuration in a *backup file*, click **Generate**.
   → A *backup file* is automatically downloaded and saved in the **Downloads** folder on your PC.

8.3.2 Restore Settings

> **!** When you restore settings from a *backup file*, all the current settings are overwritten by the settings loaded from the *backup file*.

On the **System** page:

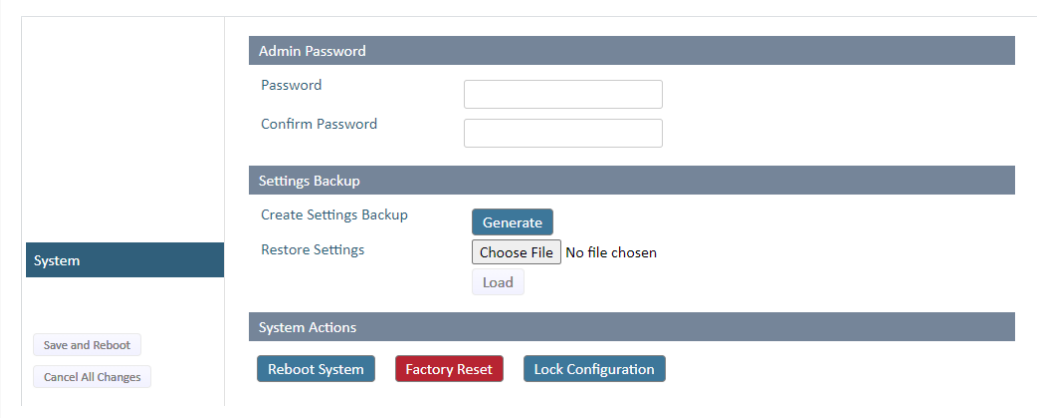


Fig. 32 Restore Settings from a backup file

Restore settings from a *backup file*:

1. Click **Choose file**.
2. Browse to and select your *backup file*
3. Click **Load**.

→ Wireless Bolt IoT reboot automatically, for the settings loaded from the *backup file* to take effect.

8.4 Reboot System

On the **System** page:

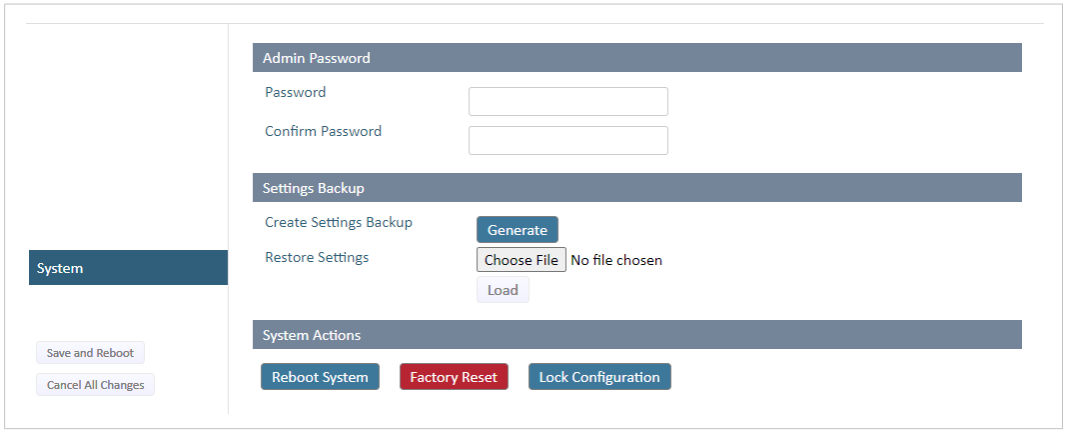


Fig. 33 Reboot System

1. If you have made any changes to the settings, you are prompted to click:
   - **Save**, to save the settings.
   - **Cancel**, to reboot the system without applying changes.
2. To reboot the system, press **Reboot System**.

9 Troubleshooting

9.1 Logs

The System Log contain useful information for troubleshooting issues that may occur in the system.

The Log file contains additional information, such as messages from the kernel, drivers, init scripts, services and applications (not originating from HMS).

Before contacting support for assistance, it is suggested that you save the System Log file and then add it as an attachment when you create the support ticket.

On the **Logs** page:

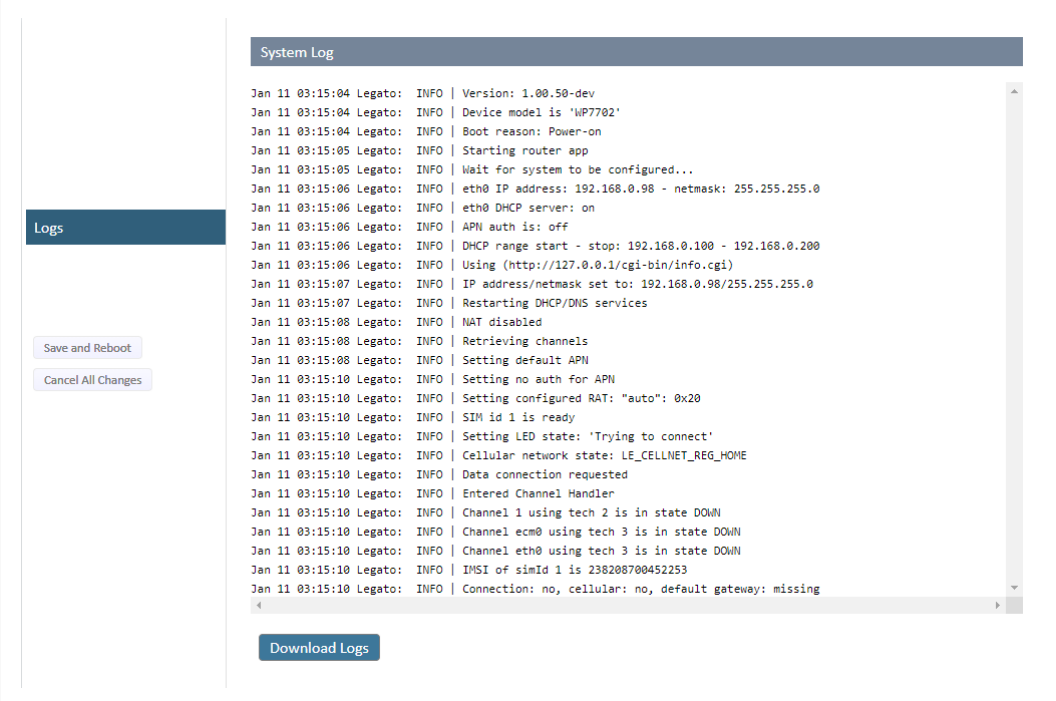


Fig. 34 Logs

1. To download current full system log and, if present, two previous boots logs, click **Download Logs**.

   → A *GNU zip (.gz) file* is automatically downloaded and saved in the **Downloads** folder on your PC.

9.2 Diagnostics

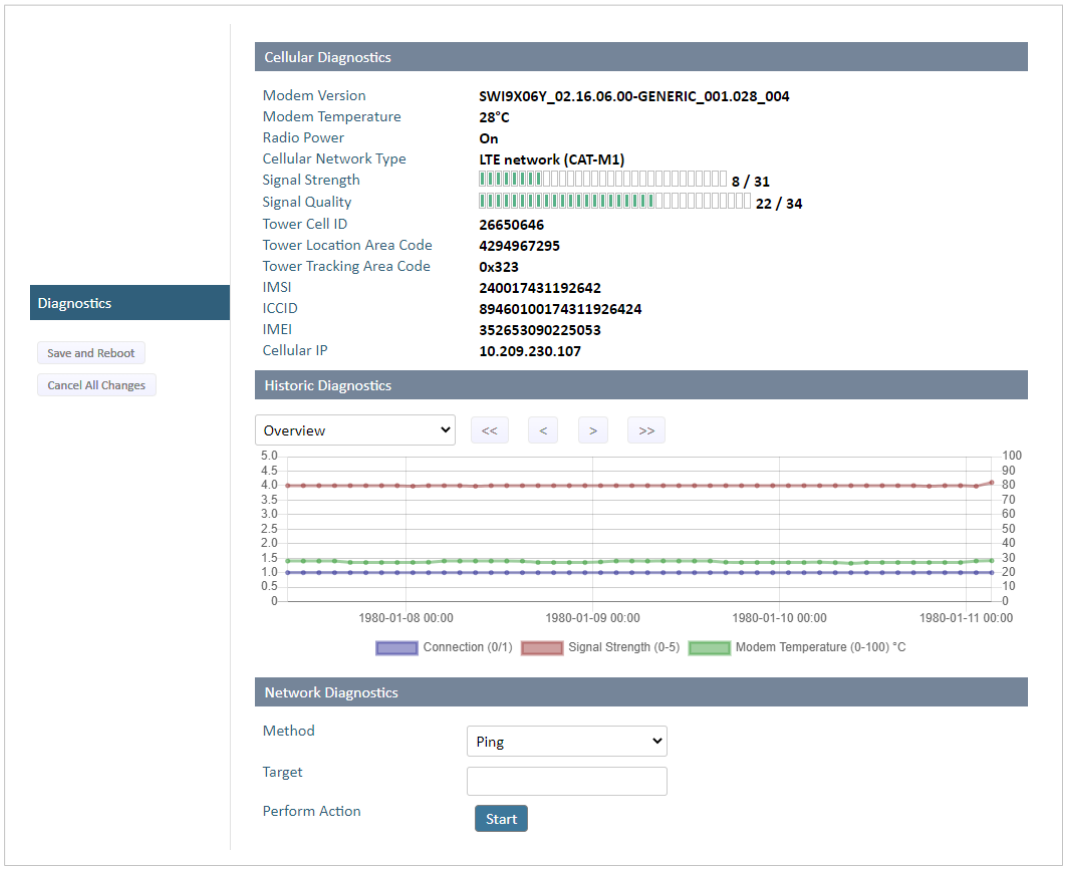


Fig. 35 Diagnostics

9.2.1 Cellular Diagnostics

Monitor Signal Strength and Quality

You can use the diagnostics information when planning the installation of Wireless Bolt IoT.

If Wireless Bolt IoT are going to be placed in a fixed installation and there are several possible locations to choose between, it is viable to monitor the signal strength and quality in the intended locations.

View Mobile Network Information

Cellular diagnostic information, such as Tower Cell ID, IMEI (International Mobile Equipment Identity) and ICCID (Integrated Circuit Card ID), is useful when you are in contact with your mobile network operator.

9.2.2 Historic Diagnostics

In the Historic Diagnostics you can overview the connection and signal strength over time in a diagram.

Select **Overview** or **Detailed** view.

9.2.3 Network Diagnostics

If Anybus Wireless Bolt IoT is installed on a private cellular network, the methods are limited according to the restrictions of the private network.

The methods are useful when evaluating the connection on the cellular network. Complete the evaluation by performing tests from the connected device on the LAN network.

To get reliable network diagnostics results, large amounts of data may be used.

Before running the Wget method, check the SIM card data rate.

The network diagnostics methods work for both modem devices and for LAN interface devices.

Perform a network diagnosis:

1. Select the **Method**.

Method	Description
Ping	Ping sends a packet to the specified address and then waits for the response. Some devices do not expect longer round trip time, introduced by some supported network types, such as *NB-IoT*. Use ping to measure the *round trip time*. Ideally, measure towards the host that your device connects to, or another host at a similar distance. The host must be configured to respond to these types of requests. If errors exist, ping reports the errors. Ping can also show packet loss. If the host's IP address is known, start by pinging the host's IP address and then the host's DNS name. The DNS name is dependent on *name server lookup*. To verify that Wireless Bolt IoT is connected to internet, you can send a ping to *Google Public DNS*. In the **Target** field, enter the IP address (IPv4) *8.8.8.8* or *8.8.4.4*.
Nslookup	Nslookup is used to query *internet domain name servers*. When Nslookup is run, the IP address of the DNS server and the targeted host IP address are shown. The DNS server is usually specified by the network operator.
Wget	Retrieve files using HTTP. The retrieval can help you evaluate the real download capacity of the connection. The retrieved file is not saved to the Wireless Bolt IoT.

2. Enter a **Target**.

3. To Perform Action, click **Start**.

   → The request is sent to the target.

   → When the target response returns, a message appears.

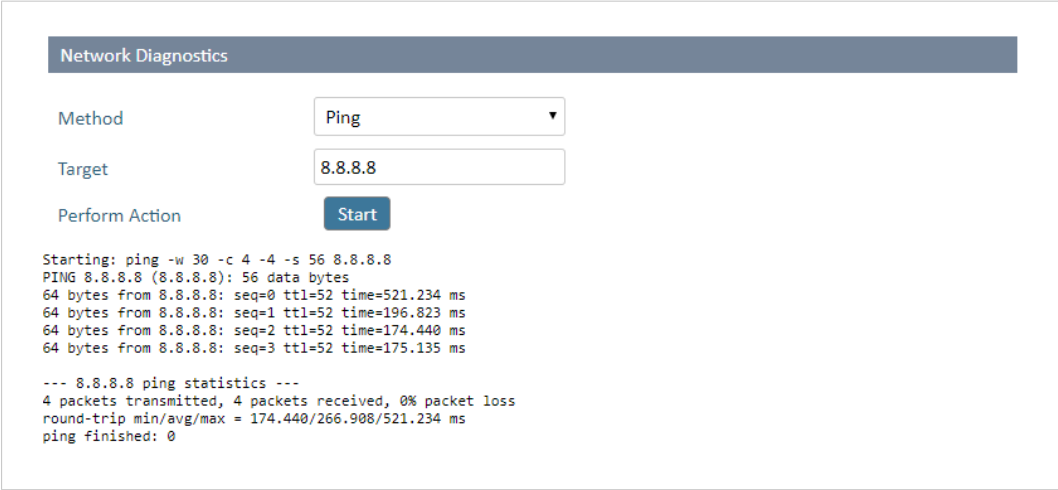


Fig. 36 Example, Ping response message from target 8.8.8.8

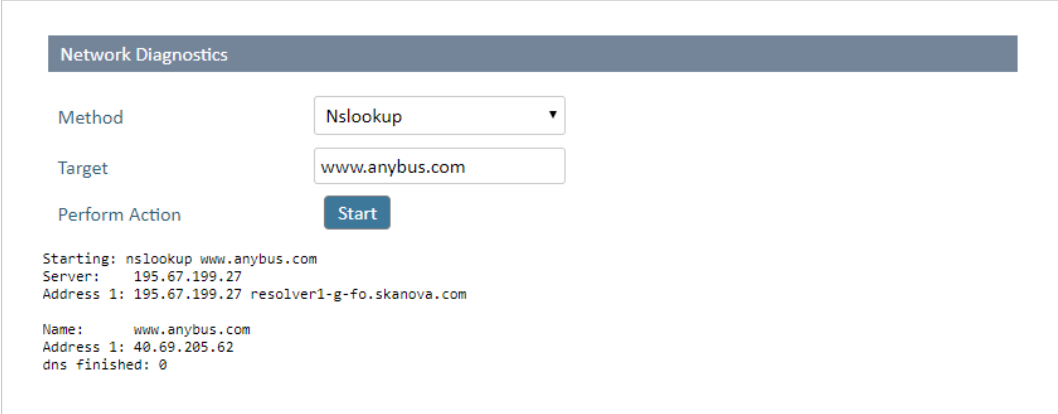


Fig. 37 Example, Nslookup response message from target www.anybus.com

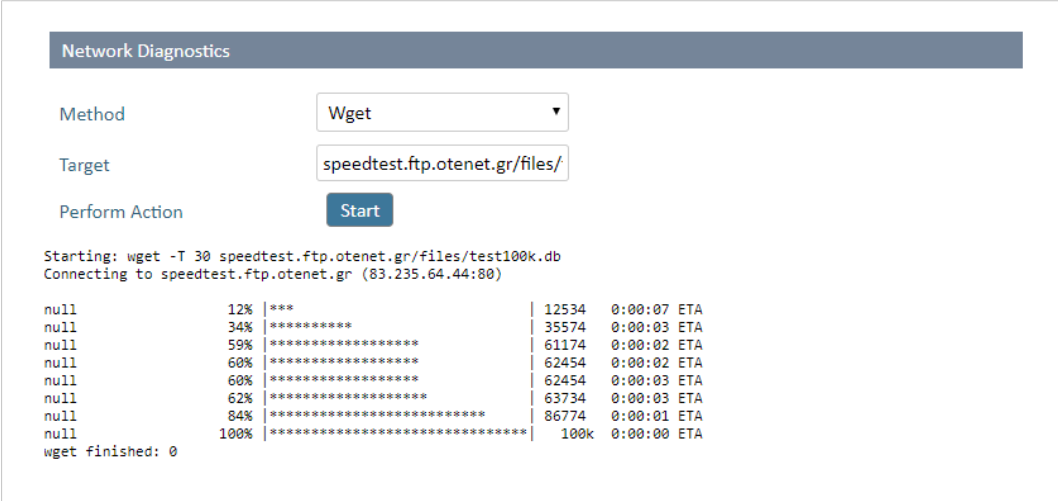


Fig. 38 Example, Wget response message from target Speedtest

9.3 Reset and Recovery

9.3.1 Reset Button

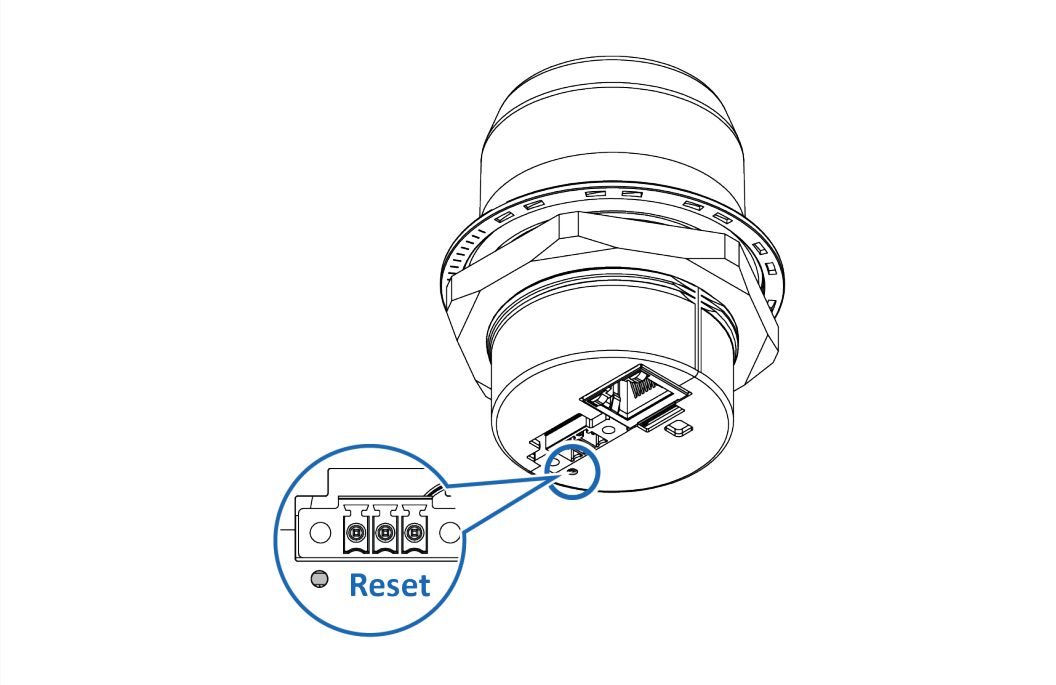


Fig. 39 Reset button

The **Reset** button is located on the bottom of the Wireless Bolt IoT.

9.3.2 Factory Reset

!	Factory Reset will result in the loss of all configuration settings and logs.

Factory Reset Using the Reset Button

1. Ensure that the Wireless Bolt IoT is powered on and running.
2. Use a pointed object (such as a ballpoint pen) to press and hold the **Reset** button for >10 seconds and then release it.

Result

→ Wireless Bolt IoT is reset to the factory default settings.

Factory Reset Using the Web Interface

On the **System** page:

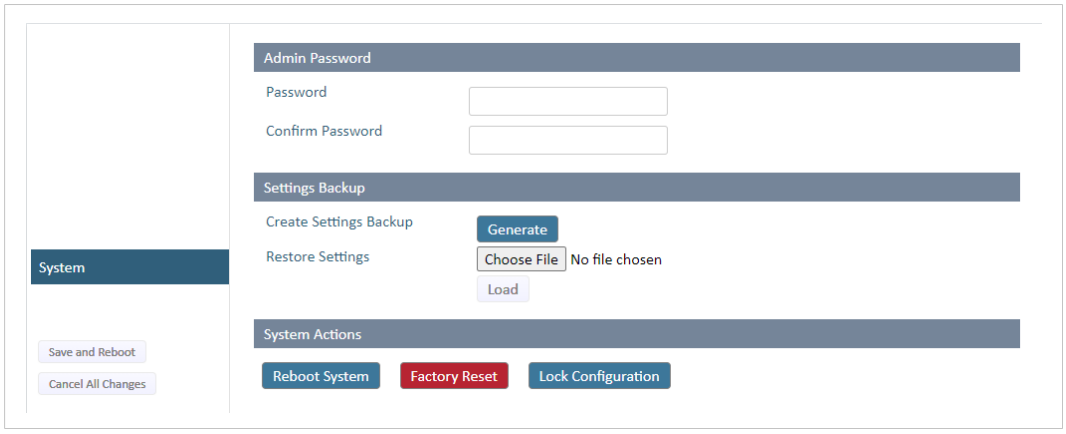


Fig. 40 Factory Reset

1. Click **Factory Reset**.
2. To confirm factory reset, click **OK**.

Result

→ Wireless Bolt IoT is reset to the factory default settings.

10 Technical Data

10.1 Technical Specifications

Order code	AWB1000	AWB1001
Color	Black	White top and black base
Operating temperature	Shadow: -40 to +65 °C Direct sunlight: -40 to +45 °C	Shadow: -40 to +65 °C Direct sunlight: -40 to +65 °C
Host interface	RJ45 Ethernet 10/100 Mbit/s, PoE	
Storage temperature	-40 to +85 °C	
Humidity compability	EN 600068-2-78: Damp heat, +40 °C, 90% (non-condensing).	
Vibration	Refer to datasheet at www.anybus.com/support.	
Dimensions	Diameter: 68 mm. Height: 75 mm without Power connector, 84 mm incl. Power connector. Height above mounting surface: 41 mm.	
Weight	95 g	
Housing material	Plastic (see datasheet for details)	
Protection class	Top (outside of host): IP66 and IP67 / UL Type 4X Base (inside of host): IP21	
Mounting	M50 screw and nut (50.5 mm hole needed)	
Power	3-pin screw connector and PoE (Power over Ethernet) 11-33 VDC through Power connector, PoE PD according to IEEE 802.3af through Eternet connector. Redundant or separate operation of PoE and DC connectors. Power Consumption: Sleep Mode: Power connector 0.1 W. PoE 0.3 W Idle Mode: Power connector 0.6 W. PoE 0.8 W Worst Case (GPRS/2G) average power: Power connector 3.2 W. PoE 3.6 W. Worst case (GPRS/2G) peak current: 1.2A@11VDC	
Cellular standards	4G LTE: Category Cat-M1 and NB-IoT. Frequency Bands: B1, B2, B3, B4, B5, B8, B12, B13, B17, B18, B19, B20, B26, B28 2G: EDGE, GPRS bands 850, 900, 1800, 1900	
Maximum Data speeds	Cat-M1: Download 300 kbps, Upload 375 kbps NB-IoT: Download 27 kbps, Upload 65 kbps GPRS/EDGE Download: 200 kbps, Upload: 200 kbps.	
Ethernet protocols	Transparent transfer of any TCP/UDP based protocol, Built-in firewall, NAT and DHCP server.	
Certifications	Refer to datasheet at www.anybus.com/support.	

© 2021 HMS Industrial Networks
Box 4126
300 04 Halmstad, Sweden

info@hms.se