

SMART BOLT SYSTEM

User Manual (EN)

Table of Contents

SAFETY INFORMATION	1
PRODUCT DESCRIPTION	3
Product overview.....	4
INSTALLATION AND CONFIGURATION	5
Enter gateway web interface.....	6
Set up internet connection of gateway.....	7
Wi-Fi configuration	7
Cellular configuration	8
LAN configuration.....	10
Prioritize connections.....	11
Change gateway admin password	11
Bolt installation.....	12
Real-time mode.....	12
Bolt tightening.....	13
TECHNICAL DATA	14
Compliance information.....	15



support@strainlabs.com



www.strainlabs.com

SAFETY INFORMATION



- This product is not intended for children. Keep away from children and pets, as to avoid hazards such as suffocation from accidental ingestion.
- This product must be disposed of appropriately. For disposal, please return the product to your local Strainlabs representative. Alternatively, you may dispose the product in accordance with local requirements for the disposal of Waste Electrical and Electronic Equipment (WEEE).
- Do not subject the plastic parts of the bolt to excessive force, as this may damage the internal electronics.
- Do not install the product if it is damaged.
- Do not exceeded the product's rated operating conditions. See [Technical Data](#).
- This product may only be installed in countries where the CE mark is applicable. See [Compliance information](#).
- This product is intended for professional use within industrial and light-industrial environments.
- Do not pull the cables of the product. When disconnecting, only pull the connector of the cables.
- Do not exceed the proof load of the bolt. If the proof load is exceeded, the warranty no longer applies, and the bolt is permanently destroyed. In this case, the bolt must be replaced.
- *Strainlabs* takes no responsibility for setting or determining warning and/or critical preload limit levels in *Analytics*. It is the responsibility of the user to determine and configure these levels, as well as take necessary action in the event that the levels are exceeded.



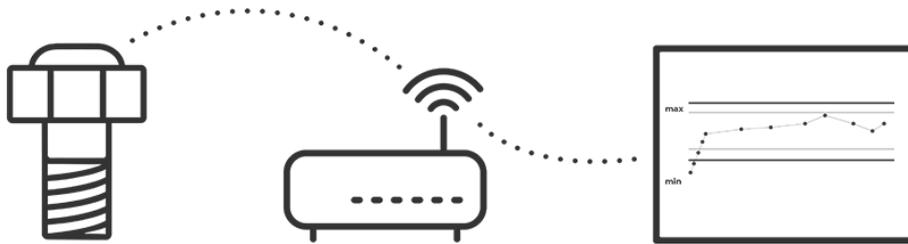
- *Strainlabs* takes no responsibility or action for error messages (“warning”, “critical”, “information”, ...) or other notifications generated by the *Analytics* software due to bolt data, such as tension warnings. It is the responsibility of the user to monitor and take action on bolt data and notifications.
- Personnel must have sufficient training and use adequate safety equipment when installing and removing bolted joints.
- During the manufacturing process, modifications are made to standardized bolts to facilitate the installation of electronics and turning them into Strainlabs Bolts. The modifications may therefore result in changes to the mechanical properties of the bolt. It is the responsibility of the user to ensure the safety of the final installation (e.g. test for fatigue strength).

PRODUCT DESCRIPTION

The *Strainlabs Smart Bolt System* is a system used to monitor bolted joints.

The system consists of:

- one or more *Strainlabs Bolt(s)*
- one or more *gateway(s)* collecting bolt data and transmitting it to the web
- *Analytics* – a web-based data analysis software



The *Strainlabs Bolt* measures preload (in kilonewtons, *kN*) and temperature (in Celsius, °C).

By studying the gathered data, the user can monitor the performance of bolted joints remotely and gain valuable insights into the operation of a certain application. Thus, potentially hazardous situations as well as costly downtime and damage to property can be avoided due to bolt failure.

Several bolt types are available, such as:

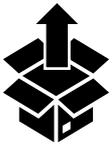
- M10 – M27 of different lengths
- Several bolt and thread standards
 - ISO 4014
 - ISO 4017
 - ...
- Several materials and grades
 - Carbon steel (8.8, 10.9, ...)
 - Stainless steel (Bumax 88, Bumax 109, ...)
 - ...

Product overview



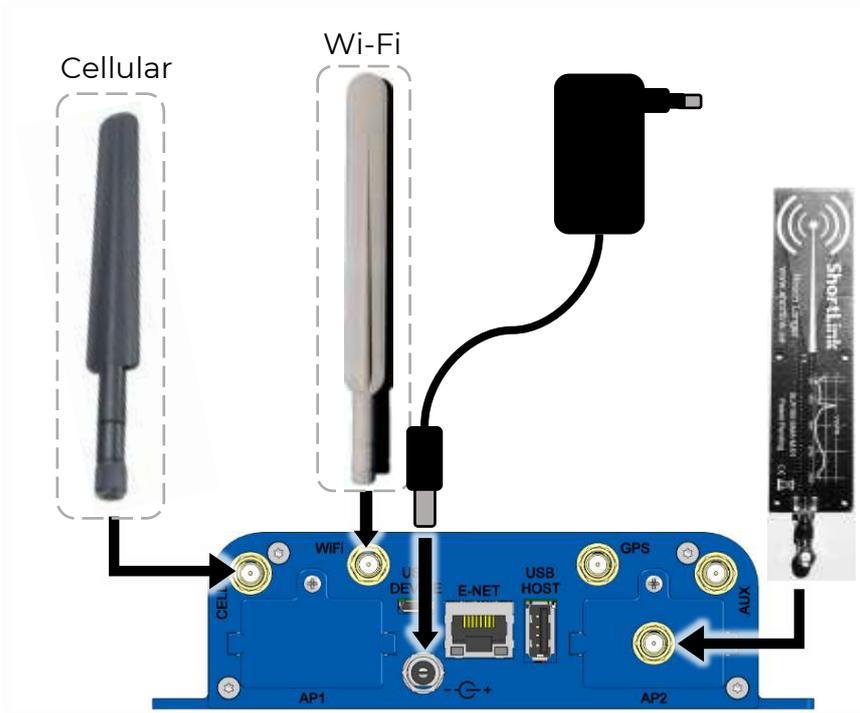
- | | | | |
|----------|---------------------------------|-----------|--------------------------------|
| 1 | LED Indicators | 10 | Power supply connector |
| 2 | Reset button | 11 | USB Host connector (not used) |
| 3 | Front plate (SIM card slot) | 12 | Bolt antenna connector |
| 4 | Cellular connector | 13 | Bolt, magnetic switch location |
| 5 | Wi-Fi connector | 14 | Power supply |
| 6 | USB Device connector (not used) | 15 | Wi-Fi antenna |
| 7 | Ethernet port | 16 | Cellular antenna |
| 8 | GPS connector (not used) | 17 | Bolt antenna |
| 9 | Auxiliary connector (not used) | | |

INSTALLATION AND CONFIGURATION

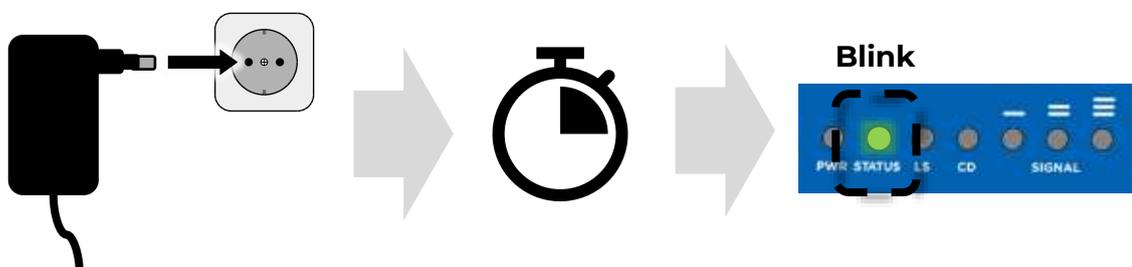
- 

Unpack of the box and inspect the contents.
If any pieces of equipment were damaged during shipping, please report to the shipping company and Strainlabs.

- Connect the power supply **14** to the power connector **10** of the gateway.
Carefully mount antennas **15**, **16** and **17** to their respective connectors.



- Connect the power supply **14** to power, then wait for the gateway to start. This may take up to 10 mins.
When the **STATUS** indicator on **1** starts blinking, the gateway is ready.



- Connect the Ethernet port **7** and the LAN port on your PC using the included Ethernet cable, then enter the gateway's web interface.

Enter gateway web interface

1.



On your PC, open a web browser.

Go to IP address **192.168.2.1**

This is the local IP address of the gateway.

Entering its local IP address in a web browser will bring you to its web interface.

Log in using the default credentials provided by Strainlabs.

Depending on which network interface(s) you intend to use with your gateway (Wi-Fi, Cellular, LAN, ...), additional setup is required.

Please follow the steps in the corresponding sections further on.



The gateway hosts a DHCP server on IP address **192.168.2.1**

The DHCP server will try to provide your PC with an IP address in the range **192.168.2.100 - 192.168.2.254**.

If the LAN interface of your PC is not configured to connect to IP addresses in this range, it will not be able to connect to the gateway.

Make sure the LAN interface of your PC is either configured to automatically be assigned an IP address from a DHCP server, e.g. **IP assignment: Automatic (DHCP)** or is configured to have a static IP address within the DHCP server IP address range of the gateway.



If your PC is connected to a Wi-Fi network, you may have trouble reaching your gateway, since your PC may try to access **192.168.2.1** on your Wi-Fi network and not the Ethernet network your gateway is connected to.

If you're experiencing this issue, disconnect your PC from Wi-Fi and try again.



It is **strongly recommended** to change the gateway admin password after initial setup to ensure network security.

Set up internet connection of gateway

The gateway needs access to the Internet to be able to transmit bolt data to *Analytics*.

The gateway can access the Internet via Wi-Fi, cellular and/or LAN. You may use any combination of these, as you prefer, as long as at least one is configured and active.

You may also prioritize which connection to use according to your preference.

Wi-Fi configuration

1. Ensure the Wi-Fi antenna **15** is connected to the Wi-Fi antenna port **5**

2. Enter the gateway's web interface.
From there, go to **Wireless** → **Wi-Fi as WAN**

3. Under **Available Wi-Fi Networks**, click **Scan**, then press **+** on the SSID you would like your gateway to connect to.

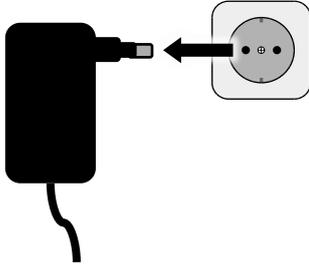
4. In **Shared Key**, enter the password of the network and press **Finish**.

5. The SSID of the added Wi-Fi network is now saved under **Saved Wi-Fi Networks**.

6. Your gateway will access your saved Wi-Fi network when in range. You can monitor the Wi-Fi connection status on the **Home** page.

Cellular configuration

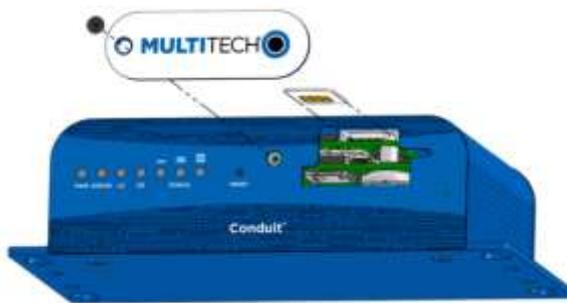
1. Disconnect power from the gateway.



-
2. Remove the front plate **3** from the gateway using a Phillips screwdriver.

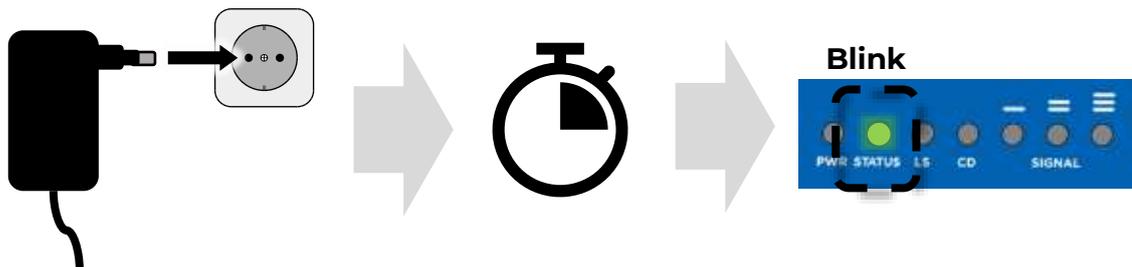
Gently insert the SIM card into the SIM card slot with the cut corner to the right and the SIM contacts facing down, as shown in the picture below.

Reattach the front plate using the screw previously removed.



-
3. Ensure the cellular antenna **16** is connected to the cellular antenna port **4**

-
4. Reconnect power to the gateway and wait for it to start up.



-
5. Enter the gateway's web interface.

6. In **Cellular** → **Cellular Configuration**, perform the following:

- Under **General Configuration**, toggle on **Enabled**.
 - If your SIM is locked with a PIN code, enter the code in the **SIM Pin** field.
 - In the **APN** field, enter your cellular provider's APN.
Contact your cellular provider for this info.
 - Click **Submit**.
 - Click **SAVE & APPLY**.
 - In the two following popup windows, click **OK**.
-

7.  Wait for the gateway to restart.
Once restarted, you may monitor the cellular connection status on the **Home** page.

LAN configuration



When configuring LAN as an internet connection method per the following instructions, the internal Ethernet bridge (which allows access to the gateway's web interface via LAN) will be disengaged. This means that access to the web interface via an Ethernet cable will be lost.

Before you continue, ensure that you have an alternative access method in **Setup** → **Access Configuration**.

1. Connect **7** to your local network (e.g., LAN switch, router or similar) using an Ethernet cable.
-
2. Enter the gateway's web interface.
-
3. In **Setup** → **Network Interface**, perform the following:
 - Under **Options**, press  for **eth0**.
 - Under **Bridge**, choose --
 - Under **IPv4 Settings**, enter the IP settings for your local network.
 - If you want the gateway to dynamically receive an IP configuration from a local DHCP server, set **Mode** to **DHCP Client**.
 - If you want to set the IP configuration of the gateway statically, set **Mode** to **Static** and enter the IP configuration fields appropriately.
 - Click **Submit**



In these settings you may also enable IPv6 support, should your network allow or enforce this protocol for connected devices.

Prioritize connections

1. [Enter the gateway's web interface.](#)
-
2. In **Setup** → **WAN Configuration**, perform the following:
 - Under **Options**, set the priority of each connection type using  
 - Click **SAVE & APPLY**
 - In the popup window, click **OK**.

Change gateway admin password

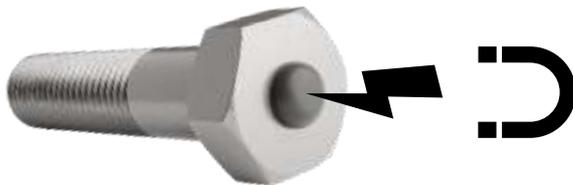
1. [Enter the gateway's web interface.](#)
-
2. In **Administration** → **User Accounts**, perform the following:
 - Under **Options**, press 
 - Click **Change Password**
 - Enter the current password (default: **Admin123**) and a new password.
 - Click **OK**.

Bolt installation

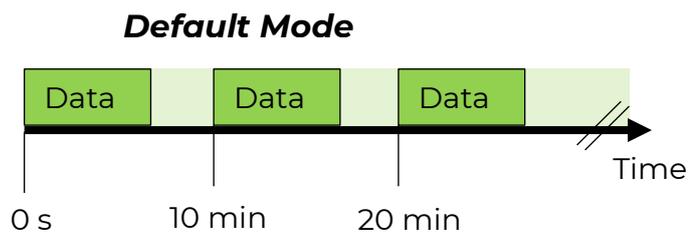
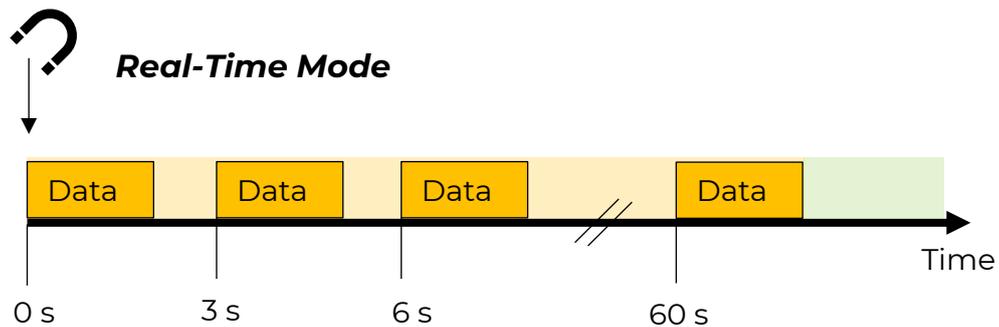
When installing a bolt, put the bolt in real-time mode and tighten it to the desired preload.

Real-time mode

1. To enter *real-time mode*, tap **13** with a magnet.



In *real-time mode*, the bolt will transmit one data packet **once every 3 seconds for 1 minute**, after which it returns to default mode (one data packet once every 10 minutes).



Bolt tightening

1. Put bolt into real-time mode.

2. While monitoring the real-time preload in *Analytics*, tighten the bolt to your desired preload.



Do not exceed the proof load of the bolt.

3. Monitor the preload of the bolt in *Analytics* over time and tighten / untighten the bolt as needed to achieve optimal joint performance.



The preload will change over time - this is normal.

Many factors (mechanical, environmental, ...) affect the preload.
Some factors include:

- Settlements and relaxation.
- Thermal contraction / expansion.
- Dynamic loads and vibration.
- Separation and yielding of parts

TECHNICAL DATA

This product is a system, consisting of one or more *Strainlabs Bolt(s)* and an IoT Gateway (*MultiTech Conduit MTCDT-L4E1* equipped with a *Strainlabs TESS Concentrator card*).

Strainlabs Bolt	
Power supply	Internal non-removable 3 V lithium coin cell battery.
Dimensions	M10 – M27, ISO 4014 / ISO 4017 (Steel grade of choice, typically carbon or stainless)
Operating conditions	-30 ... +70 °C
Storage conditions	-30 ... +70 °C
Ingress protection	IP67
Bolt RF range	Max. LoS < 90 m (1)
Battery life	Up to 5 years (2)
Compliance	See <i>Compliance information</i> .

- (1) The range is dependent on many factors (incl. obstacles, bolt mounting position, RF environment, material bolt is mounted in etc.) and will in reality be lower.
Monitor the RF link performance by observing the RSSI values in *Analytics*.
Higher RSSI values = higher RF link performance.
- (2) Battery life expectancy is simulated in room temperature conditions at a bolt sampling and transmission frequency of once every 10 minutes.
If a higher frequency is used, or the environment has a temperature higher or lower than room temperature, the battery life is reduced.

For technical and mechanical data regarding the IoT Gateway, consult the documentation provided by Multi-Tech Systems, Inc., such as its [Datasheet](#).

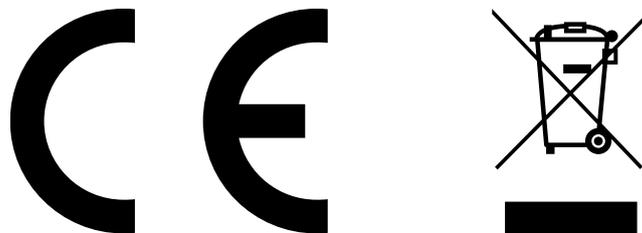
Compliance information

This product complies with the CE requirements, in accordance with the following directives:

2014/53/EU	Radio Equipment Directive (RED)
2011/65/EU with amendment 2015/863/EU	Restriction of Hazardous Substances in Electrical and Electronic Equipment (RoHS)
2012/19/EU	Waste from Electrical and Electronic Equipment (WEEE)

The product has been tested according to, and complies with, the following standards:

EN 300 328 V2.2.2
EN 62368-1:2014+A11
EN 301 489-1 V2.2.3
EN 301 489-17 V3.1.1
EN 61000-6-3:2007 + A1



Additional compliance information is available upon request.



www.strainlabs.com



2025-02-20_v08_OC