Contents

1. Introduction ................................................................................................................................... 2
2. Scope of the document ................................................................................................................ 2
3. Connecting the cabling ................................................................................................................ 2
4. Logging in and setting up the modem ....................................................................................... 5
5. Security hardening and connection testing .............................................................................. 9
6. Cybersecurity disclaimer ........................................................................................................... 14
1. **Introduction**

InRouter 615-S is a 4G to Ethernet (4 port) modem/router. This step-by-step guide instructs how to set up the modem securely for IoT gateway (NETA-21) connections. For technical data and the manufacturer’s documentation, refer to www.inhandnetworks.com.

2. **Scope of the document**

This document is intended for use at ABB internal factory line, where the modem and the NETA-21 gateway are commissioned. The instructions can also be used for commissioning at the customer’s site.

*Note:* To do the commissioning, the customer needs a SIM card with the mobile data service enabled and a data plan to avoid data charges from the teleoperator.

*Warning!*

Obey the safety instructions of the drive. If you ignore them, injury or death, or damage to the equipment can occur. If you are not a qualified electrical professional, do not do installation, commissioning, or maintenance work.

Repeat the Electrical safety precautions steps in the drive safety instructions before you start the work.

This document provides cybersecurity related deployment advice, but please note also the Cybersecurity disclaimer (Chapter 6).

3. **Connecting the cabling**

Connect the power, antenna and ethernet cabling to the modem.

1. Insert the SIM card into the modem.

   *Note:* If the SIM card’s PIN code is enabled, several startups may lock the SIM card. Use a SIM card with the PIN code disabled or insert the SIM card just before step 3 “Set up the SIM card” in Chapter 4.

2. Connect the antenna
Connect the SMA antenna connector and tighten the connector by hand.

3. Plug in the power connector.

Connect 24V DC power to the power plug according to the markings on the modem.

4. Connect the NETA-21 to the modem and power it up.
   a) Connect the NETA-21 ETH2 port to InRouter port 1.
   b) Power on the NETA-21 and wait 1 minute before connecting the PC.
Connect the PC Ethernet.

Connect the commissioning PC with an Ethernet cable to Ethernet port 4 (technically any available port 1, 2, 3, 4 works).

**Note:** Leave the “WAN” port of the modem disconnected.
4. Logging in and setting up the modem

The following steps describe the basic settings of the InRouter for remote connectivity. The settings allow the NETA-21 gateway to push data to the Internet. For advanced configuration options, see the manufacturer’s documentation at inhandgo.com.

1. First login
   a) When the PC is connected to the modem (step 5 on page 4), navigate to http://192.168.2.1.
   b) Login with the default credentials:
      - Username: adm
      - Password: 123456.

   **Note:** This password works only for the first login. You will change the password to the MAC address in chapter 5 Security hardening and connection testing. The end user should change the password to a secure one and keep it in a safe place.

   c) After a successful login, you should see the modem configuration front page:
2. Set the time and date.
   a) Click the **Sync time** button to synchronize the time from the PC to the modem.
   b) Verify that the **Router time field** shows the correct date and time.

![System Status](image)

3. Set up the SIM card.

   This step enables the Internet connectivity. Do step 5 immediately after this step, to block any unwanted external connections from the Internet.

   **Note:** This step is done quite early, just to avoid locking up the SIM card with too many reboots, if there is a PIN code enabled on the SIM card.

   On the production line where several modems are being set up using one SIM card, we recommend using a SIM card which has PIN code checking disabled. A customer SIM card may have a preferred PIN code.

   a) On the **Network** menu, select **Dialup**:

   ![Dialup Menu](image)
b) Set up the teleoperator specific settings. These depend on the SIM card. (It is possible that the username and password fields are empty, and that the APN is “internet” or something else specific to the network provider). The modem provides predefined settings for some teleoperators. Other settings can be left as default.

![Dialup settings](image)

4. Update the firmware

a) Check for any pending firmware updates.

   ![Note](image) Refer to the manufacturer’s website https://inhandgo.com/pages/download-center for the location of the latest modem firmware.


   ![Warning](image) Do the mandatory security update to all firmware versions prior to 2.3.0.r5484. The software patch was released in November 2021, but vulnerable software may also be included in modems delivered later.

c) Select System -> Upgrade to do the updates:
d) Click **Browse...**, select an upgrade file and click **Upgrade**.

5. **Security hardening and connection testing**

Security hardening protects the modem from external threats in case the customer’s SIM card provides access from the Internet towards the modem. SIM cards with public/static IP addresses are not needed or recommended.

1. In the **System** menu, select **Admin Access**:
2. **Configure the following:**

   a) **Old password**: enter the default password 123456
   
   b) **New password**: locate the type label of the router and use the “MAC” address as the new password, including capital letters and special characters, for example 00:18:05:11:01:B4-B5 in the figure below.
Note: The MAC address is set as a temporary password at the factory to increase the security of the modem. The end customer must create a secure password for the modem.

c) Uncheck (disable) HTTP
d) Check (enable) the HTTPS (preferably also only “Local access” not “Remote Access”)
e) Uncheck (disable) TELNET
f) Uncheck (disable) Console

See the example below.

3. Click Apply.

Applying the settings will take a moment:
You will be redirected to the login page. Make sure that the web address starts with https://.
You will see a web browser warning about a self-signed certificate.

4. Click **Advanced** (in Microsoft Edge browser).

5. **Continue to 192.168.2.1 (Unsafe)** because you are connecting point-to-point (not through Internet) to a modem which we know to have a valid identity.
6. Finally, you will be returned to the login page using HTTPS. Enter the changed password to make sure that it works.

![Router Login](image)

7. Test the Internet with the web browser of the PC.
   
a) When connected to the modem from a PC using wired Ethernet, disable the wireless network connection and try browsing the internet, for example https://www.abb.com.

   ![Windows 10 Airplane mode button](image)

   You can disable the wireless network using a keyboard shortcut (Fn + the Wi-Fi function key) or with the “Airplane mode” button on the Windows 10 toolbar:

8. Make sure that NETA-21 can connect to the cloud.

   Before this, make sure that the software and IPS packages have been preloaded to NETA-21 using an SD card, and that the Internet connection is working.
   
a) Login to the NETA-21 web UI and check the portal status for 4 green ticks:
6. **Cybersecurity disclaimer**

This product is designed to be connected to and to communicate information and data via a network interface. It is the customer’s sole responsibility to provide and continuously ensure a secure connection between the product and the customer’s network or any other network. The customer must establish and maintain any appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of anti-virus programs, etc.) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB and its affiliates are not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.