



UNIVERSAL ROBOTS

User Manual

Connectivity Kit



Contents

1. Introduction	1
1.1. About This Manual	1
2. Safety	2
2.1. Safety Message Types	2
2.2. General Safety Precautions	3
2.3. Product Safety Precautions	4
3. Intended Use	5
4. Cybersecurity Threat Assessment	8
4.1. General Cybersecurity	8
4.2. Cybersecurity Requirements	8
4.3. Cybersecurity Hardening Guidelines	10
5. Product Description	11
5.1. UR Connectivity Kit	11
5.2. Router Restrictions	12
5.3. Router Reset	13
6. Hardware Installation: Components	14
6.1. Component Connection	14
7. Hardware Installation: Router	18
7.1. Cellular Connectivity Setup	18
8. Software Installation	20
8.1. Software Configuration	20
8.2. Wired Connection Setup	21
9. Troubleshooting	22
9.1. Checking for Failing Networks	22
10. Maintenance	23
10.1. Maintaining the Router	23



1. Introduction

1.1. About This Manual

Description The purpose of this manual is to provide the essential information to start using the UR Connectivity Kit. Universal Robots offers users of the UR Connectivity Kit a range of online services to maintain and support applications.

Abbreviations In this document the following abbreviations are used.

CLI	Command-line Interface
CSF	Cybersecurity Framework
HTTP(S)	HyperText Transfer Protocol (Secure)
ICMP	Internet Control Message Protocol
MQTT	Telemetry Transport
RMS	Remote Management System
SMS	Short Messaging Service
SSH	Secure Shell
SSL	Secure Socket Layer
SYN (flood)	Half-open Attack
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

What's in the box

- Teltonika router and accessories (packaged)
- Cable gland
- This manual

Business contact details Universal Robots A/S (hereinafter Universal Robots or UR)
 Energivej 51, 5260 Odense S, Denmark
 +45 89 93 89 89
<https://www.universal-robots.com>

2. Safety

2.1. Safety Message Types

Description

Safety messages are used to emphasize important information. Read all the messages to help ensure safety and to prevent injury to personnel and product damage. The safety message types are defined below.



WARNING

Indicates a hazardous situation that, if not avoided, can result in death or serious injury.



WARNING: ELECTRICITY

Indicates a hazardous electrical situation that, if not avoided, can result in death or serious injury.



WARNING: HOT SURFACE

Indicates a hazardous hot surface where injury can result from contact and non-contact proximity.



CAUTION

Indicates a hazardous situation that, if not avoided, can result in injury.



GROUND

Indicates grounding.



PROTECTIVE GROUND

Indicates protective grounding.



NOTICE

Indicates the risk of damage to equipment and/or information to be noted.



READ MANUAL

Indicates more detailed information that should be consulted in the manual.

2.2. General Safety Precautions

Description



WARNING

Failure to adhere to the test protocols listed below can result in hazardous situations.

- Test the robot protective stop, to verify the Servo also stops.
- Test the Servo fault, to verify the robot stops.
- Test the brakes when the Servo is deactivated.



WARNING

Combining different machines can increase hazards, or create new hazards.

- Always make an overall risk assessment for the complete installation.
- Depending on the assessed risk, different levels of safety can apply; as when different safety and emergency stop performance levels are needed.



ELECTROSTATIC DISCHARGE

Failure to take Electrostatic Discharge (ESD) precautions, when handling or replacing ESD sensitive parts, can lead to damage to property.

- To prevent property damage, use an ESD wristband when handling or replacing ESD sensitive parts.



NOTICE

Disregard for the robot workspace and operating space can result in the damage to property.

Ensure there is adequate space for the robot to move.



READ MANUAL

Failure to read and understand information about the equipment used in the installation can increase the likelihood of safety risks.

Always read and understand the manuals for all equipment used in the installation.

2.3. Product Safety Precautions

Description

Universal Robots does not assume any responsibility or liability for any actions, products, and services of third-party manufacturers or suppliers. Users are advised to read and follow all safety precautions and instructions provided by the third-party product manufacturers. Universal Robots makes no representations or warranties regarding the quality, safety, or suitability of any third-party products and expressly disclaims any implied warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose.



WARNING

The UR Connectivity Kit does not provide protection for cybersecurity threats where the attacker has physical access to the robot or any of its interfaces or ports, such as the USB port.

- The user/integrator shall ensure that only authorized people have access to the robot.



WARNING

The user/integrator is at all times responsible for keeping the Software up to date and applying any relevant Software patches from both Universal Robots and Teltonika.



READ MANUAL

Failure to read the Teltonika documentation can be a risk to safe use.

- Read the safety information for the router RUT951 available in the Teltonika online documentation.

See wiki.teltonika-networks.com



NOTICE

Changing the configuration of the UR Connectivity Kit can increase risks to the safe use of your robot.

- Only professionals, who understand the cybersecurity implications, shall be authorized to change the UR Connectivity Kit configuration.

3. Intended Use

Description

The UR Connectivity Kit provides connectivity of UR robots to online services. The UR Connectivity Kit is intended for industrial use, to provide an internet connection to your Universal Robots robot.



WARNING

The UR Connectivity Kit shall not be used with CB3 robots or PolyScope versions prior to 5.17.

- Only use UR Connectivity Kit with UR e-Series robots as well as UR20 and UR30 running PolyScope 5.17 or later.

Connecting your Universal Robots robot to the internet requires the integrator and the user to address cybersecurity threats and risks due to physical access to the robot. The mandatory risk assessment of any robot application is required to include a cybersecurity threat assessment, then implementation of the needed cybersecurity measures.


WARNING

Using UR robots or UR products outside of the intended uses can result in injuries, death and/or property damage. Do not use the UR robot or products for any of the below unintended uses and applications:

- Medical use, i.e. uses relating to disease, injury or disability in humans including the following purposes:
 - Rehabilitation
 - Assessment
 - Compensation or alleviation
 - Diagnostic
 - Treatment
 - Surgical
 - Healthcare
 - Prosthetics and other aids for the physically impaired
 - Any use in proximity to patient/s
- Handling, lifting, or transporting people
- Any application requiring compliance with specific hygienic and/or sanitation standards, such as proximity or direct contact with food, beverage, pharmaceutical, and /or cosmetic products.
 - UR joint grease can be released into the air (vapor), or drip.
- Any use, or any application, deviating from the intended use, specifications, and certifications of UR robots or UR products.
- Misuse is prohibited as the result could be death, personal injury, and /or property damage

UNIVERSAL ROBOTS EXPRESSLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR ANY PARTICULAR USE.

**WARNING**

- UR Connectivity Kit is not designed or intended for use in any application requiring compliance with specific hygienic and/or sanitation standards, such as direct contact with food, beverage and/or pharmaceutical products.
- Any use or application deviating from the intended use, specifications, and certifications is prohibited as the result could be death, personal injury and/or property damage.
- The UR Connectivity Kit is designed for use in standard industrial environments and is sold “AS-IS”. Universal Robots makes no declaration of conformity, claim of functionality, or fitness for particular purpose to the extent the UR Connectivity Kit is used beyond the prescribed intended use.
- The user shall ensure that the UR Connectivity Kit is at all times used in full compliance with all applicable regulatory and legal requirements. If the user utilizes the UR Connectivity Kit for applications outside the intended use, the user shall bear sole and exclusive liability.

**READ MANUAL**

Failure to use the UR Connectivity Kit in accordance with the intended use can result in unsafe situations.

- Read and follow the recommendations for intended use provided in this manual.

**READ MANUAL**

Failure to use the Teltonika component in accordance with the Teltonika instructions can result in unsafe situations.

- Read the safety information provided in the Teltonika Wiki accessible by QR code (included with the Teltonika router package).

4. Cybersecurity Threat Assessment

4.1. General Cybersecurity

Description

Connecting a Universal Robots robot to a network can introduce cybersecurity risks. These risks can be mitigated by using qualified personnel and implementing specific measures for protecting the robot's cybersecurity. Implementing cybersecurity measures requires conducting a cybersecurity threat assessment.

The purpose is to:

- Identify threats
- Define trust zones and conduits
- Specify the requirements of each component in the application



WARNING

Failure to conduct a cybersecurity risk assessment can place the robot at risk.

- The integrator or competent, qualified personnel shall conduct a cybersecurity risk assessment.



NOTICE

Only competent, qualified personnel shall be responsible for determining the need for specific cybersecurity measures and for providing the required cybersecurity measures.

4.2. Cybersecurity Requirements

Description

Configuring your network and securing your robot requires you to implement the threat measures for cybersecurity.

Follow all the requirements before you start configure your network, then verify the robot setup is secure.

Cybersecurity

- Operating personnel must have a thorough understanding of general cybersecurity principles and advanced technologies as used in the UR robot.
- Physical security measures must be implemented to allow only authorized personnel physical access to the robot.
- There must be adequate control of all access points. For example: locks on doors, badge systems, physical access control in general.

**WARNING**

Connecting the robot to a network that is not properly secured, can introduce security and safety risks.

- Only connect your robot to a trusted and properly secured network.

Network configuration requirements

- Only trusted devices are to be connected to the local network.
- There must be no inbound connections from adjacent networks to the robot.
- Outgoing connections from the robot are to be restricted to allow the smallest relevant set of specific ports, protocols and addresses.
- Only URCaps and magic scripts from trusted partners can be used, and only after verifying their authenticity and integrity

Robot setup security requirements

- Change the default password to a new, strong password.
- Disable the "Magic Files" when not actively used (PolyScope 5).
- Disable SSH access when not needed. Prefer key-based authentication over password-based authentication
- Set the robot firewall to the most restrictive usable settings and disable all unused interfaces and services, close ports and restrict IP addresses

4.3. Cybersecurity Hardening Guidelines

Description Although PolyScope includes many features for keeping the network connection secure, you can harden security by observing to following guidelines:

- Before connecting your robot to any network, always change the default password to a strong password.



NOTICE

You cannot retrieve or reset a forgotten or lost password.

- Store all passwords securely.

- Use the built-in settings to restrict the network access to the robot as much as possible.
- Some communication interfaces have no method of authenticating and encrypting communication. This is a security risk. Consider appropriate mitigating measures, based on your cybersecurity threat assessment.
- SSH tunneling (Local port forwarding) must be used to access robot interfaces from other devices if the connection crosses the trust zone boundary.
- Remove sensitive data from the robot before it is decommissioned. Pay particular attention to the URCaps and data in the program folder.
 - To ensure secure removal of highly sensitive data, securely wipe or destroy the SD card.

5. Product Description

5.1. UR Connectivity Kit

Description The UR Connectivity Kit provides internet connection to your Universal Robots robot. It also provides an isolated VLAN (ports LAN2 and LAN3) where up-to two additional units can communicate with each other and with the robot without accessing the internet.

Hardware components The Connectivity Kit hardware components consist the following:

- A cable gland
- The Teltonika packaged items:
 - Teltonika RUT951 router
 - Power supply cable to connect the router to a power outlet
 - Ethernet cable to connect the robot to the router
 - Antennas to facilitate 4G & Wifi connection
 - A Teltonika Quick Start Guide to access router safety information

Software requirements Robots with PolyScope 5.17 as the factory default software will have the full set of cybersecurity features and security settings set by default to restrictive level.



READ MANUAL

Updating your robot to PolyScope 5.17 introduces new cybersecurity features, but does not change the security settings to restrictive. This requires manual action described in Secure Setup of UR Cobots article.

- Update the software to PolyScope 5.17.
- Review the security settings after updating to PolyScope 5.17.
- Make any necessary adjustments.

See PolyScope in Online Manuals on myur.universal-robots.com

You can also read Secure Setup on www.universal-robots.com/articles

As an advanced user, you can reset previously provisioned robots to secure settings by re-imaging the robot SD-card. See How to Replace Flashcards on www.universal-robots.com/articles

5.2. Router Restrictions

Description The UR Connectivity Kit uses the Teltonika 4G router, preconfigured with restrictive settings, to allow the minimum needed functionality.

Router configuration restrictions

- Disabled WiFi
 - Disabled RMS (Remote Management System)
 - Disabled VPN
 - Enabled attack prevention
 - SYN flood
 - ICMP limit
 - SSH limit
 - HTTP limit
 - HTTPS limit
 - Port scan
 - Disabled SSH and CLI
 - Only allowing connecting to UR-controlled addresses
 - Not allowing incoming connections
 - Only allowing outgoing connections using port 443
 - Disabled SMS utilities
 - Configured VLANs to only allow direct outgoing connections from port 1. Communication is still allowed between all ports
-

5.3. Router Reset

Description Resetting the router to factory settings restores the restrictive settings as it is running custom firmware preconfigured by UR. Only Teltonika RUT951 routers bought as part of the UR Connectivity Kit, have the default settings of the custom firmware. Failure to analyze the security impact of any configuration changes can increase cybersecurity risks.



WARNING

- If there is a need to return to default, restrictive configuration, reset the router. The default, restrictive settings are applied again.
- Changes to the router settings shall be done by authorized and qualified personnel (IT security professionals), upon thorough analysis of security impact of the changes.

To reset router

1. Press the reset button on the back of the router.
See the Teltonika Manual.
-

Password protection

The default admin password is engraved on the back of the router. Change the default password to your own, strong password. When the router is reset the default password located on the back of the router becomes valid again.



WARNING

The admin password allows access to the router configuration, which if reconfigured by unauthorized persons can introduce cybersecurity risks.

- Store the admin password securely.
 - Limit access to the admin password to authorized personnel.
 - Limit physical access to the router to authorized personnel.
-

6. Hardware Installation: Components

6.1. Component Connection

Description

The UR Connectivity Kit components are to be connected such that the Teltonika router is installed on the outside of the Universal Robots Control Box and connected to the Ethernet port, using the included Ethernet cable.



READ MANUAL

See the installation instructions of the Teltonika router for instructions and environmental requirements.

The following sections illustrate how to connect the router and the Control Box.

To attach the cable gland to the LAN cable

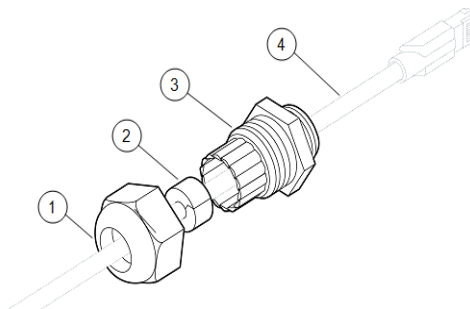
Criteria for success: The cable gland is correctly attached and sealed to your LAN cable and Control Box.

1. Separate the cable gland and identify the parts you are going to use.

Cable gland parts to use:

- Sealing nut
- Seal
- Body (cone and entry thread)

2. Insert your LAN cable into the sealing nut.
3. Clip the seal onto your LAN cable to the right of the sealing nut, as shown.
4. Insert your LAN cable and the seal into the body and adjust the LAN cable length accordingly.
 - Insert the seal completely into the cone side of the body.
 - Make sure the inserted seal appears flush with the cone.
 - Tighten the sealing nut securely onto the body.



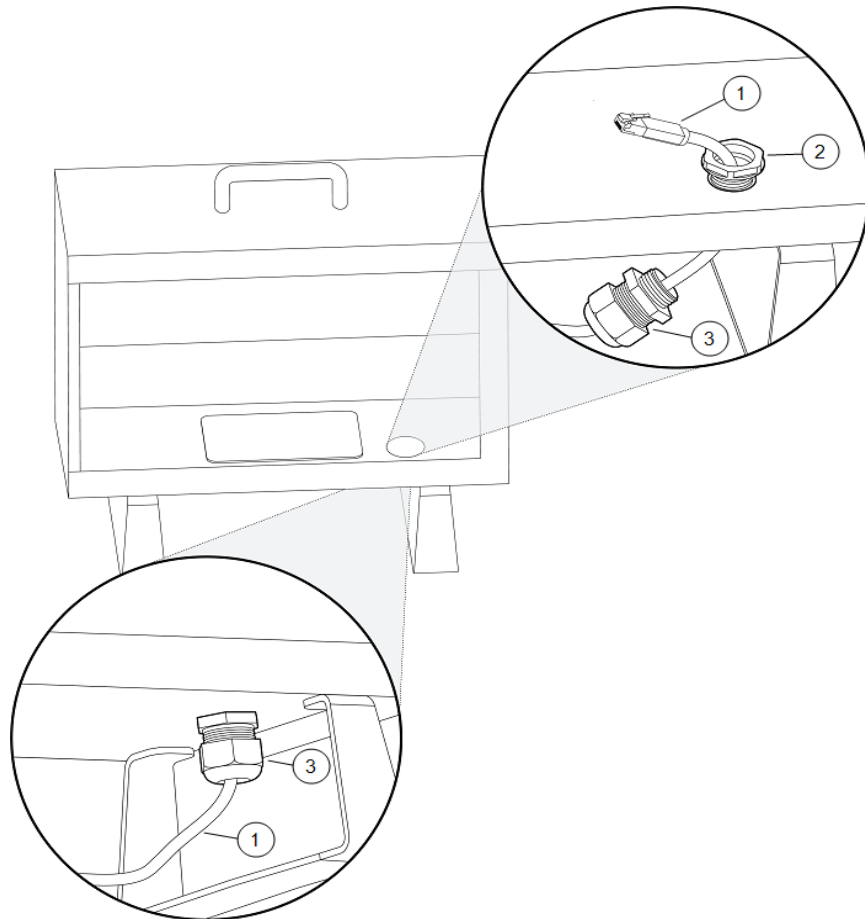
1	Sealing nut	2	Seal
3	Body (cone and entry thread)	4	LAN cable

**To connect
the cable
gland to the
Control Box**

Criteria for success: Your LAN cable is locked in place inside the Control Box.
Before you install the cable gland: Remove one of the caps at the base of the Control Box.

**To connect
the ethernet
cable to the
Control Box**

1. Insert the entry thread side of the body into the hole in the Control Box base.
2. Tighten the locknut securely onto the entry thread and adjust the LAN cable length as needed.

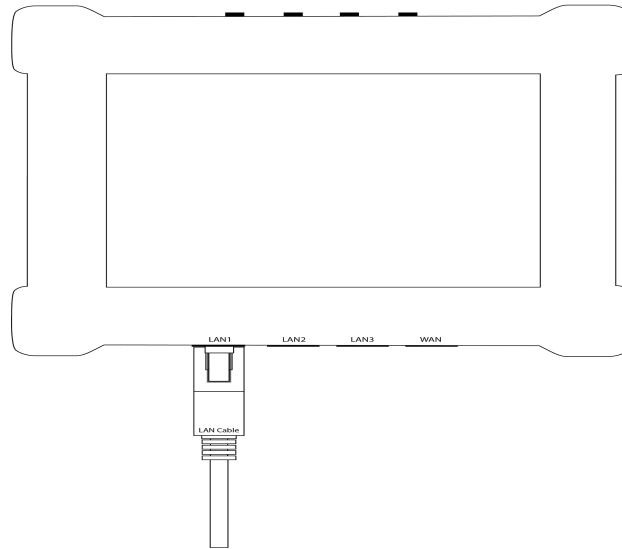


1	LAN cable	2	Locknut
3	Body with sealing nut attached		

To connect the ethernet cable to the router

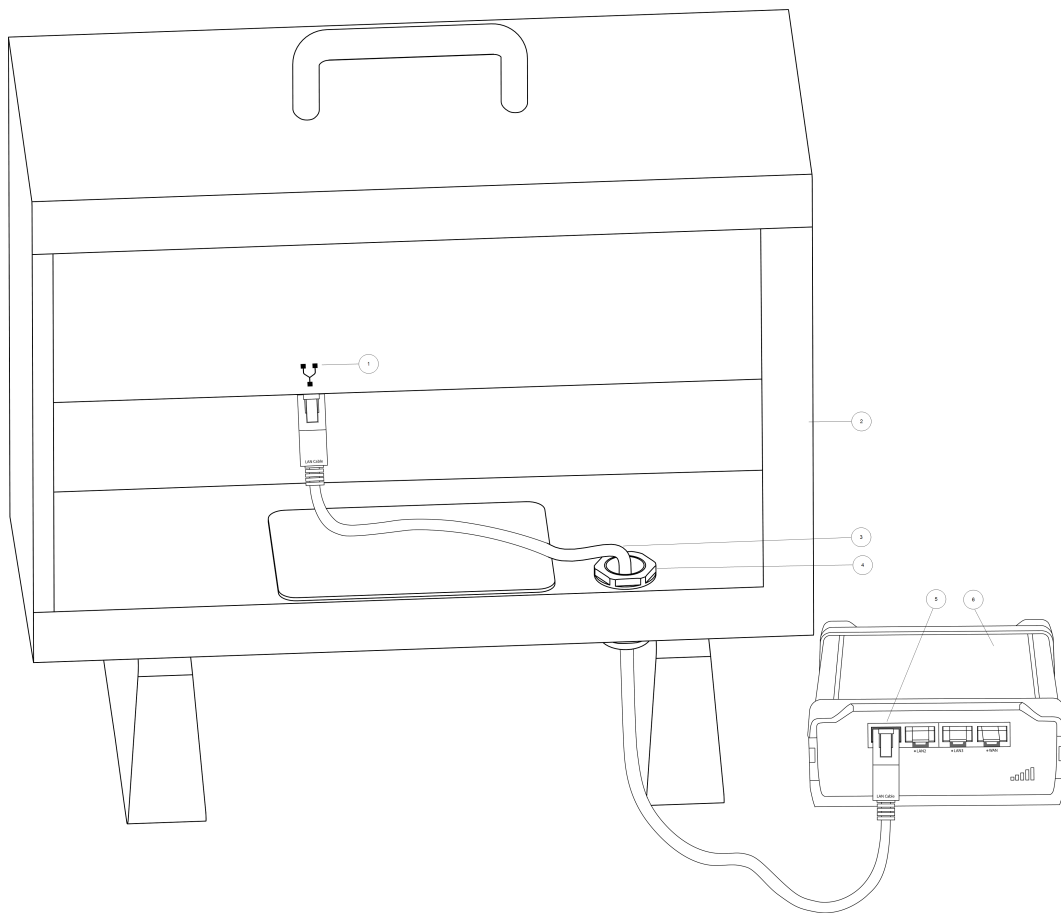
1. Insert the LAN cable into a LAN port in the Teltonika router.

View from above



1	Teltonika router	2	LAN port
3	LAN cable		

**Control Box
and router
connection**



1	Ethernet port	2	UR Control Box
3	LAN cable	4	Cable gland
5	LAN port	6	Teltonika router

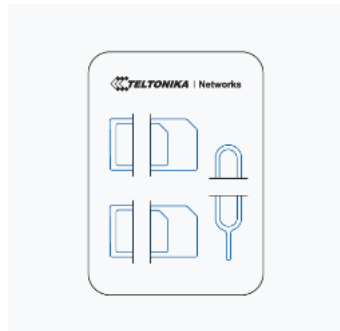
7. Hardware Installation: Router

7.1. Cellular Connectivity Setup

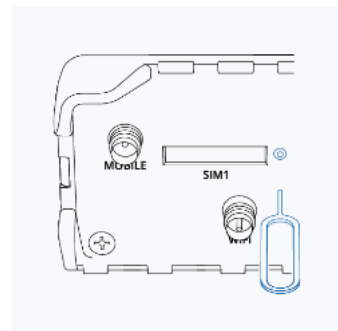
Description

The Teltonika router requires some set-up before you can use it.
The following steps show how to set up the router to connect to the internet.

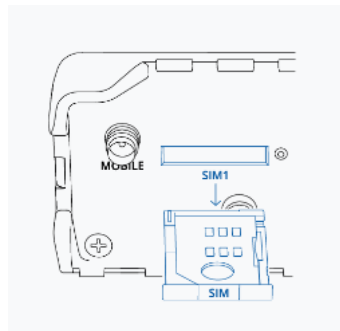
To set up the router



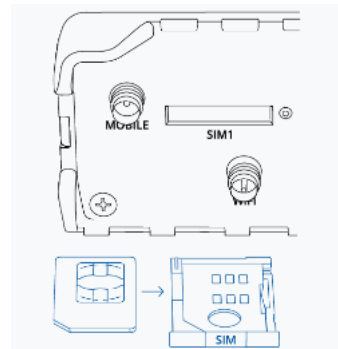
1. Locate the SIM Adapter kit.



2. Push the SIM holder button with the SIM needle.

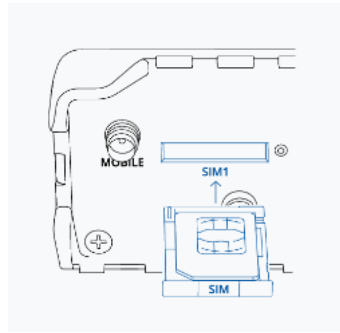


3. Pull out the SIM holder.

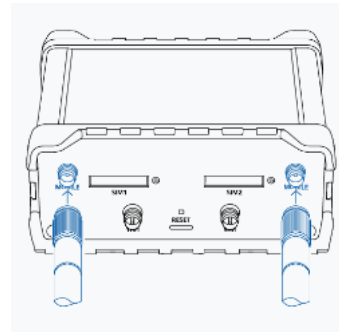


4. Insert your SIM card into the SIM holder.

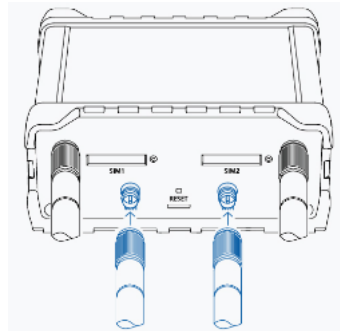
To set up the router



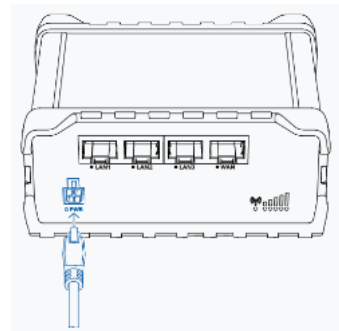
5. Slide the SIM back into the router.



6. Attach both MAIN and AUX Mobile antennas to connectors labeled Mobile.



7. Attach both Wi-Fi antennas to connectors labeled Wi-Fi.



8. Connect the 4-pin connector to the power socket on the front of the device. Then plug the power adapter into an electric outlet.



NOTICE

Incorrect installation of the antennas can result in malfunction or damage to equipment.

- Verify the correct use of the cellular connectivity antennas (labeled MOBILE).

8. Software Installation

8.1. Software Configuration

Description The hardware components must be correctly installed before you can set up PolyScope for the Connectivity Kit connection.

- To establish connection**
1. Make sure the robot is set for **Local Control**, (otherwise configuration is disabled).
 2. In the top right of the screen, tap the Hamburger menu and select **Settings**.
 3. In the menu at the left side of the screen, tap **System**
 4. Select **Network**.
 5. Then select **DHCP** to enable networking.

When the robot is communicating with the router via your network connection, the PolyScope screen updates automatically to show the configuration.

- To disable automatic configuration**
- Disabling the automatic configuration allows you to set your own configuration.
1. In the top right of the screen, tap the Hamburger menu and select **Settings**.
 2. In the menu at the left side of the screen, tap **System**.
 3. Select **Network**.
 4. Then select the **Static Address** option.



NOTICE

Disabling the automatic configuration can lead to network conflicts, which can affect network performance and availability.

You can re-configure the router’s DHCP service which is set to use the entire IP range of the LAN1 subnet. See the Teltonika provided documentation of the router.

8.2. Wired Connection Setup

Description In situations where the a 4G connection is either impractical or impossible, you can establish a wired internet connection.

To establish a wired connection

1. Make sure no SIM card is in the router SIM holder.
2. Use an Ethernet cable to connect to the WAN port of the router.
3. Connect the router to your network.

When the robot is communicating with the router via your network connection, the PolyScope network screen updates automatically to show the configuration.

To verify the wired connection

1. Connect a PC to the LAN1 port of the router.
2. On your PC, open an internet browser and access the router's administration interface by going to address 192.168.1.1
3. Login using the name and password on the back of the router.
If you changed the password, according to previous recommendations, use the new password.
4. On the Teltonika router dashboard, access the Network->WAN menu, and make sure a WAN connection is active.

9. Troubleshooting

9.1. Checking for Failing Networks

Description Use the information below to identify possible reasons for network failure.

To diagnose network failures

	Must pass	Check or test
Prerequisites Installation	yes	Checks if the URCap is installed with all the software dependencies needed to connect.
TCP/IP Communication	yes	Test Socket Connection to ur-fleet-prod-hub.azure-devices.net via port 443.
IoT Hub Accessible	yes	Test DNS lookup for ur-fleet-prod-hub.azure-devices.net
Application Service Accessible	yes	Test DNS lookup for my-ur-fleet-prod-api.azurewebsites.net
Azure Blob Accessible	yes	Test DNS lookup for fleetblobprod.blob.core.windows.net

10. Maintenance

10.1. Maintaining the Router

Description To ensure cybersecurity protection, it is important to keep the router up to date with latest firmware from Teltonika.

To update firmware up-to-date You can access teltonika-networks.com/view/RUT951_Firmware for information and instructions for keeping the router firmware up-to-date.



WARNING

Updating the router with stock firmware from the Teltonika website will lead to an overwrite of the UR security settings, which can lead to an increased risk of cyber attacks.

- It is important to update the router by downloading the firmware directly from Teltonika firmware server in the router dashboard.
- Do not update with Teltonika stock firmware downloaded from the Teltonika website.

The router runs UR specific software, and if updating from server through dashboard, it will download the UR-specific version with default restrictive settings.

To reset the default configuration

1. Press and hold the button on the back of the router.
The LEDs at the front of the router turn on in sequence.
2. Continue to hold the reset button until all of the LEDs are lit.
The LEDs turn green.
3. When all the LEDs are lit, release the reset button.
The router resets.

Software Name: PolyScope 5/X
Software Version: 5.20
Document Version: 10.10.14