# uGo and uSuite – Technical Summary and Notes for IT

Customer document · uLog series · Version 1.1 · from uGo 1.0.8, network guard 1.1.9, Kiosk 1.0.3 (as at 15 September 2026) · United Robotics Group GmbH · Product Management

**Changes from version 1.0 (10 September 2026):** 1.1: clarification on the site computer, data protection note on location, remote access, network segmentation. All other details – destinations, protocols, ports, periods – are unchanged.

## Part A – What has changed (short version)

As of this release, the uLog series runs on **uGo**, the new United Robotics Group operating software on the robot, together with **uSuite**, the matching cloud platform with data held in Europe (Frankfurt data centre). The chassis manufacturer's software is now used internally only, for drive, navigation and safety sensors; it can no longer be reached from outside and no longer reports to any manufacturer platform.

| AREA | BEFORE | NOW WITH UGO / USUITE |
|---|---|---|
| Operation at the robot | Manufacturer app on the tablet, robot registered on the manufacturer platform | **uGo user interface** (kiosk mode): start a run, stations, maps, rules, fault dialogue with step-by-step guidance for the user, restart/shutdown at the push of a button |
| Data path to the outside | Robot reported to the chassis manufacturer's cloud (outside Europe) | **uSuite only** (Frankfurt), encrypted, individual device identity per robot; **no connection to any manufacturer platform** |
| Network protection | Chassis freely addressable on the customer network | **uGo network guard** (Netzschranke) on the robot: the chassis can only be reached by URG software, outbound traffic only to the approved destinations (see Part B), everything else is refused and logged |
| Remote maintenance | Manufacturer tool permanently active | Remote maintenance tool active **only during a service window** (opened by the technician at the device, closes by itself after 60 minutes); no open channel in between |
| Fleet and charging | Each robot on its own | Charging supervisor across the fleet (no approaching occupied charging stations), map archive and map backup, trip log with daily summary |
| Building | Manufacturer's door module | **u-IoT**: call button, signal light/tone, **uGate** door opener – URG's own modules, controlled through uGo |
| Updates | Manually at the device | Releases are approved in uSuite per site; the device fetches the package, verifies the signature and can roll back |
| Service | Email/telephone | Cases in uSuite: fault report or service request from the robot or from the console, handled by URG, time zone per customer |

Principles that apply throughout: there is **no drive command from the cloud**, no map recording and no remote setting of the position – the robot only moves when instructed on site. The cloud sees status, trip log, faults and releases; it does not control.

**Location information in uSuite (coarse location):** uSuite knows the location of a robot only as building, floor and area from the operator's map – no tracking, no personal data. The operator can switch this information off for each individual device.

# Part B – Notes for IT (firewall, addresses, remote maintenance)

## B.1 What the robot is on the network

The robot joins the wireless network with **one** device: the control unit (tablet running uGo). It obtains its address by DHCP; a fixed reservation per robot (by MAC address, which we provide at commissioning) is recommended so that the call button and the site computer find the robot reliably. The chassis sits on an internal network **behind** the control unit and has no connection to your network. Wireless: 2.4 GHz or 5 GHz, WPA2-Personal pre-configured; other authentication methods by arrangement.

**Site computer – when it is needed:** A call button (u-IoT) at a uServe or uLog needs **no** site computer; the call button talks directly to the robot over u-IoT. A site computer is only required **with uGo+** (lift control, doors/uGate, changing levels). Without uGo+ it is not needed at all.

## B.2 Outbound connections (from the robot to the internet)

The robot needs **only** the outbound rules listed below. Everything else is blocked by the network guard on the device itself; your firewall can block it as well.

| DESTINATION | PROTOCOL / PORT | PURPOSE | DURATION |
|---|---|---|---|
| `a2r3pnkk0q34p6-ats.iot.eu-central-1.amazonaws.com` | TCP 8883 (MQTT over TLS) and TCP 443 | Permanent connection to uSuite: status, faults, trip log, releases | permanent |
| `ipvjbplrpa.execute-api.eu-central-1.amazonaws.com` | TCP 443 (HTTPS) | Device registration with uSuite (once, then again when keys are rotated) | at commissioning |
| `*.s3.eu-central-1.amazonaws.com` | TCP 443 (HTTPS) | Fetching update packages, storing map backups | for updates/backups |
| Your DNS server (assigned by DHCP) | UDP/TCP 53 | Name resolution for the destinations above | permanent |
| Your NTP server or a time server you have approved | UDP 123 | Time of day (logs, certificate validation) | permanent |

All destinations are located in the Frankfurt region (eu-central-1). There is no connection to any manufacturer platform, to app stores or to advertising or telemetry services. If you use TLS inspection or a mandatory proxy, please let us know the proxy address; the connections can be routed through it, but this then requires a setting on the device.

## B.3 Remote maintenance and remote access

For work carried out by URG, the device uses a remote maintenance tool. It is active **only during a service window**: the technician opens it at the device (service access, 60 minutes at most), after which the access closes by itself; between two visits the application is hidden and has no network permission. Access is limited to the control unit; a remote drive command is not provided for, and the rest of your network cannot be reached. Every access is logged on the device (30 days) and is available for you to inspect.

uSuite itself needs **only outbound TCP 443** to the cloud; inbound access is not required. A maintenance session started directly from the uSuite console is prepared and will be enabled with a later version; until then, remote access is provided through the remote maintenance tool at the site.

| DESTINATION | PROTOCOL / PORT | DIRECTION | DURATION |
|---|---|---|---|
| Servers of the remote maintenance provider (we will pass the domain list to your IT separately) | TCP 5938, alternatively TCP 443 | outbound | only during the service window |

Inbound rules from the internet are **not** required – neither for remote maintenance nor for uSuite. If you do not want remote maintenance at all, service access stays closed permanently; visits then take place on site.

## B.4 Within your network (laboratory segment)

| ON THE ROBOT | PORT | WHO MAY ACCESS | WHAT FOR |
|---|---|---|---|
| uGo user interface and API | TCP 5301 (HTTP) | Call button (u-IoT), technician on site, site computer only with uGo+ (lift, doors, changing levels) | Operation in the browser, call button actions, technician page; write access only with the service password/service key |
| Maintenance access (device interface) | TCP 5555 | Only during the service window, only from the local network | Software installation by the technician |
| Chassis | TCP 8090 | Only the registered site computer – only with uGo+ (lift, doors, changing levels) – nobody else | Diagnostics by URG |
| Network guard, status query | TCP 5302 | Only on the device itself (loopback) | – |

Recommendation: place the robot, the u-IoT modules and – only with uGo+ – the site computer in a dedicated laboratory VLAN; from other segments allow port 5301 only, in case the user interface is to be used from office workstations. u-IoT modules communicate exclusively with uGo (port 5301) and never with the chassis.

**Network segmentation:** We recommend a single common robot segment (a dedicated VLAN), separated from the hospital network. From this segment, outbound port 443 to the cloud has to be opened, together with the destinations listed in B.2. The u-IoT interfaces stay exclusively inside the protected segment and never belong on the open hospital network. A laboratory robot (uLab) without a connection to the laboratory information system can sit in the same segment.

## B.5 What you can check

On the robot's technician page, the network guard shows its status (`aktiv`), the destinations most recently refused and the connection log for each day. This lets you cross-check against your firewall log that nothing leaves the device apart from the destinations in B.2 (and B.3 during the service window).

## B.6 Contact

Technical enquiries: Product Management, United Robotics Group GmbH, An der Riede 2, 28816 Stuhr · Sales: health@unitedrobotics.group



United Robotics Group GmbH · An der Riede 2, 28816 Stuhr, Germany · uGo and uSuite · Customer document · Version 1.1 · 15 September 2026