The Icomera A2-e Access Point

Installation and Maintenance Manual

Icomera AB, Odinsgatan 28, SE 411 03 Göteborg, Sweden
Phone: +46 (0)31 799 21 00 | Web: www.icomera.com

Document Information

Document Title	Icomera A2-e Access Point – Installation and Maintenance Manual
Document Classification	Commercial in Confidence
Document Number	REL-00832
Version	1.0
Approval Date	2025-02-10
Author	Hardware Development

Revision History

Date	Version	Comment
2025-02-10	1.0	Released

TABLE OF CONTENTS

List of Figures

List of Tables

1 Introduction

The A2-e is a high-performance mobile access point, supporting a high number of simultaneous users and is part of Icomera's industry-leading platform for connected vehicles. The A2-e is foremost intended for use in rail environments.

Supporting Wi-Fi 7, the A2-i allows high volumes of traffic to pass to and from the on-board router at high speed, while keeping latency low. It contains four Wi-Fi radios (1x 6 GHz, 1x 5 GHz-L, 1x 5 GHz-H, and 1x 2.4 GHz), each with 4x4 MU-MIMO. Beamforming provides extra bandwidth to the streams and makes them more reliable.

The A2-e has external antenna connectors and two Ethernet ports. It supports a wide input range via its 24-110 VDC (EN50155 compliant) DC power supply. The A2-e has an optional bypass relay that ensures that (in daisy-chained topologies) Ethernet traffic can still flow through the access point, even in cases of power failure. Alternatively, the access point can be powered with PoE++ via one of its two 10Gbps ports. If an PoE+ switch is used, the functionality of the access point will be limited.

The memory and processing power of the A2-e enables future needs.

The A2-e comes with the Icomera Wireless Platform (IWP) operating system. The configuration is made remotely through Icomera Network Insight and Control (ICONIC), Icomera's web-based portal that provides a user interface for different Icomera applications. ICONIC is also used for managing Icomera routers, providing one common Over the Air management tool for the Icomera on-board units. Applications included in ICONIC can provide information from the A2-e. For instance, in Discovery it is possible view status information, information about used channels, frequencies, connected users, and transferred data amount, etc. Discovery is further described in the document "REL-00468 X.X Icomera Discovery XXX – User Manual".

This manual provides instructions for installing the access point and includes important considerations to achieve optimal performance. It also offers basic operating instructions, as well as guidance on maintenance and troubleshooting for the unit.

The A2-e is referred to as "access point" in the remaining parts of the document.

The installation of other Icomera devices is described in their installation and maintenance manuals.

If referenced documents include information that contradicts recommendations provided in this manual, please follow the recommendations provided here. When mentioning clients or client devices, this refers to smartphones, laptops, tablets, as well as handheld ticket validators used by staff.

2 Product Overview

The following sections provide an overview of the access point features.

Each access point can work either as base station, or on-board client, depending on software configuration.

Figure 1. The A2-e access point.

2.1 Technical Data

Table 1. A2-e Technical Data

Features	Specification
Model name	A2-e
CPU	Quad-core Cortex-A73 ARM 2.2 GHz
Wi-Fi radios	— 1 x 2.4 GHz: Speed 1148 Mbps (802.11ax), 2401-2482 Mhz. — 1x 5 GHz-L: Speed 5760 Mbps (802.11be), 5150-5350 MHz. — 1x 5 GHz-H: Speed 5760 Mbps (802.11be), 5470-5850 MHz. — 1x 6 GHz: Speed 11520 Mbps (802.11be), 5925-7125 MHz. — 4x4 MU-MIMO per radio combined with OFDMA for more efficient multi-user communications. — Quadband with client load balancing between the bands. — Supports 20 /40 /80 /160/ 320 MHz channel spectrum width. — 4k QAM and 320 MHz channel width to maximize data throughput. — Up-to 600 simultaneous client users. — Supports IEEE 802.11be/ax/ac/n/a/b/g (Wi-Fi 7/6E/6/5/4). — Supports 802.11 k, v, r, ai.
System memory	3 GB DDR4

Features	Specification
Voltage Supply	24 to 110 VDC (nominal) as per EN 50155 Class S2 (10 ms interruption) For the A2-e PoE specification, see Table 2: PoE+/PoE++ Type 3 IEEE 802.3bt (limited performance with PoE+) PoE+/PoE++ is not compatible with the A2-e Bypass model, see below.
Power consumption	< 61 W
LAN	2 x 10GbE (backwards compatible 1Gbps and 100Mbps) Bypass relay included in the A2-e Bypass model, see Table 2
MTBF[1]	598,353 hours

2.1.1 Models

The available A2-e models are described in Table 2.

Table 2. A2-e models.

Model Name	Specification
A2-e PoE	Powered with either PoE++ in or DC in.
A2-e Bypass	Only powered with DC in. With a bypass relay to ensure Ethernet traffic continues to flow through the access point, even during a power failure. Foremost intended for daisy chain setup.

[1] MTBF estimation according to Telcordia SR-332, issue 4.

2.2 Housing and Environmental Features

The Icomera access point is specifically designed to withstand the harsh environment found on-board trains and trams.

The A2-e unit is rail certified, according to EN 50155.

2.2.1 Dimensions

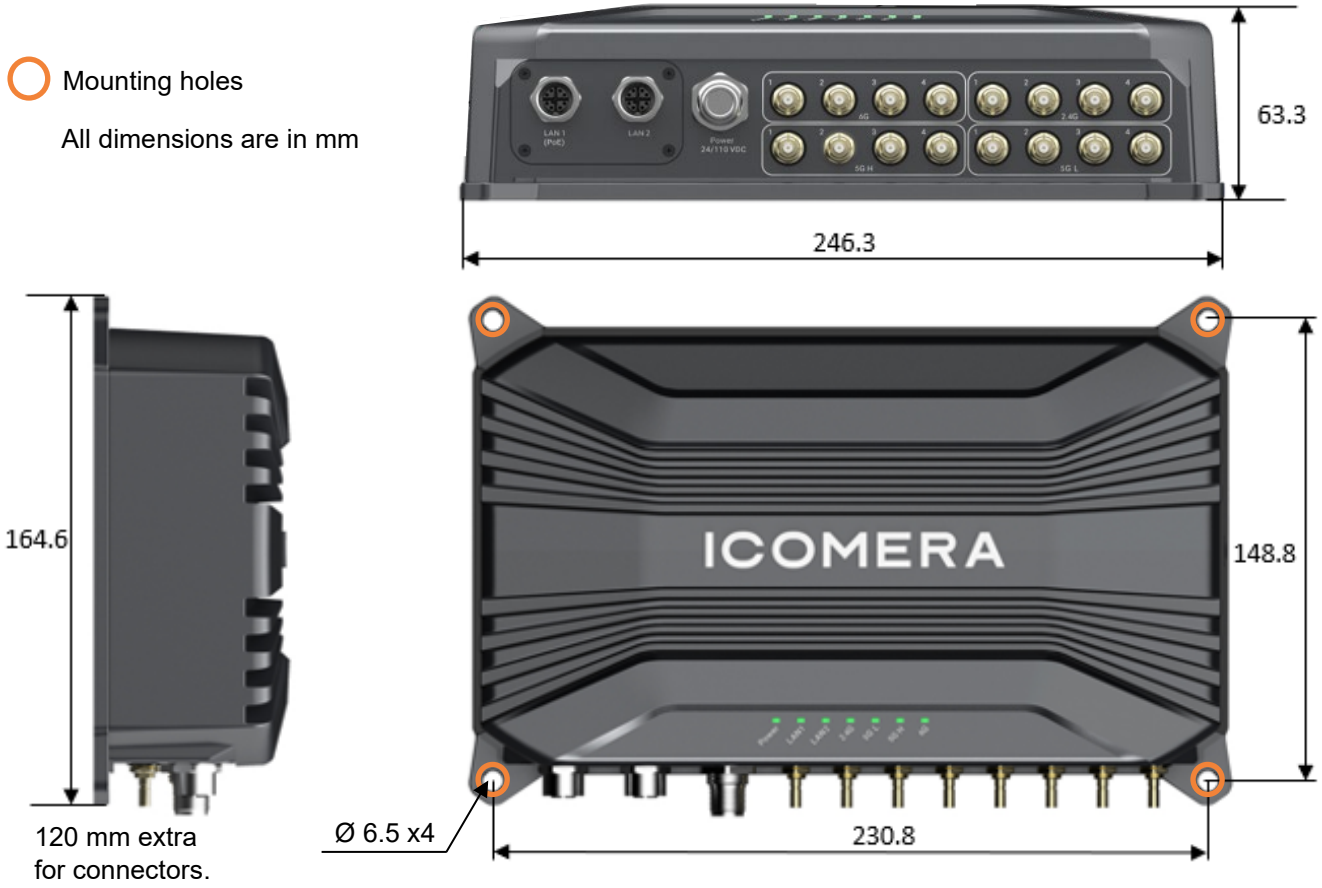


Figure 2. Dimensions of the access point.

See Figure 2 for the access point dimensions.

2.2.3 Environmental Features

Table 3. Environmental Data

Features	Specification
Weight	2.72 kg
Chassis material	Aluminium
Chassis colour	Black, RAL 7016
IP classification	65
Temperature range, as per EN50155	-40 °C to +70 °C (85 °C for 10 min), as per EN 50155 OT4 ST1 (operation) -40 °C to 85 °C (storage)

2.2.4 Antenna, LAN, and Power Supply Connectors

Figure 3. The A2-e connectors.

All connectors on the access point, see Figure 3, are selected to ensure IP 65. They also have locking devices to prevent the cables from coming loose, due to vibrations. The connectors have dust covers, that should be used if nothing is connected.

No.	Label	Specification
1	LAN 1	M12 X-coded, 10 GbE PoE++ in [1]
2	LAN 2	M12 X-coded, 10 GbE
3	Power 24/110 VDC	M12 K-coded, 4 pin Power in, 24 to 110 VDC nominal
4	6 GHz 5 GHz L 5 GHz H 2.4 GHz	16x QMA, Wi-Fi antennas

[1] PoE++ or PoE+ is not compatible with A2-e bypass.

2.2.4.1 Power Supply

The access point's power supply is galvanically isolated from the rest of the device, which is protected against reverse polarity and includes a built-in fuse.

M12 K-coded (male) connector, 4 pin, for power input, 24 to 110 VDC.

Mating supply connector: M12 K-coded (female) connector, 4 pin, see Figure 4.

Pin No.	Signal
1	VIN+
2	VIN+
3	VIN-
4	VIN-
PE	NC

Figure 4. Mating M12 K-coded (female) connector, pinning seen from the connector side.

2.2.4.2 LAN (PoE and Ethernet)

2x M12 X-coded connectors:

- LAN 1 port for PoE++ in [1] and LAN, as per IEEE 802.3bt, type 3 and 10GBase-T.
- LAN 2 as per 10GBase-T

Mating LAN connector: M12 X-coded (male), see Figure 5.

Pin No.	Signal
1	DA+
2	DA-
3	DB+
4	DB-
5	DD+
6	DD-
7	DC-
8	DC+

Figure 5. Mating M12 X-coded (male) connector, pinning seen from the connector side.

2.2.4.3 Wi-Fi Antennas

16 x QMA connectors, for connecting Wi-Fi antennas to the Wi-Fi radios (4x4 MIMO (Multiple-Input Multiple-Output)).

Mating connector: QMA plug (male), see Figure 6.

Figure 6. Mating connector: plug QMA (male) with a quick lock snap-on connector.

[1] PoE++ or PoE+ is not compatible with A2-e bypass.

2.2.5 Status Indication by Light Emitting Diodes

The LEDs can be disabled in the access point configuration. Ensure they are enabled before relying on them to check the access point status.

Figure 7. The status LEDs of the access point.

The status Light Emitting Diodes (LEDs), on the access point provide some basic feedback about the access point's status.

LED	Description
Power	Power Green (with a delay of 5 s) Is continuously on: The power to the access point is OK. Either from DC in or PoE.
LAN1 LAN2	Ethernet status Green: 2.5/5/10 Gbps Blue: 1 Gbps Red: 10/100 Mbps Is on: - something is connected. Is blinking: - there is traffic over the Ethernet link, with the speed indicated by the LED colour. Is off: - nothing is connected, or - there is no communication activity, or - the cable is broken, or - the access point and the connected unit cannot agree on the link speed.
2.4G 5G L 5G H 6G	Wi-Fi radio status Green Is on: - the radio is active but there is no data transfer. Is blinking: - there is data transferred over the radio. Is off: - the radio is inactive, either due to that the radio is disabled by the software or broken.

2.3 Wi-Fi Radios

The access point has four Wi-Fi radios with each radio supporting 4x4 MU-MIMO.

- Wi-Fi radio 1 supports the 2.4 GHz band.
- Wi-Fi radio 2 supports the lower range, 5.150 to 5.350 GHz, of the 5 GHz band.
- Wi-Fi radio 3 supports the 6 GHz band.
- Wi-Fi radio 4 supports the higher range, 5.470 to 5.850 GHz, of the 5 GHz band.

Refer to section 2.4 for regulatory compliance.

The Wi-Fi radios support

- 2.4 GHz (2.401 ~ 2.482 GHz)
  Channel 14 is not used in EU.
  Channels 12, 13, and 14 are not used in the USA.
- 5 GHz (5.150 ~ 5.850 GHz)
  UNII-1 5.150 ~ 5.250 GHz for EU, UK, USA and Canada[1].
  UNII-2a 5.250 ~ 5.350 GHz for EU, UK, AUS, USA and Canada.
  UNII-2c 5.470 ~ 5.725 GHz for EU, UK, AUS, USA and Canada.
  UNII-3 5.725 ~ 5.850 GHz for EU, UK, AUS, USA and Canada.

  When the access point is used in Australia the Band 5600 ~ 5650 MHz is disabled to protect weather radars.
  The access point is subject to restrictions on putting into service under “Indoor use only” conditions in the frequency range 5150 to 5350 MHz, as provided for in Article 10(10) of Directive 2014/53/EU. Thus, the product packaging has the pictogram as indicated below:

BE	DE	LT	AT	IT	FI	PT
BG	EL	LU	EE	CY	RO	SE
CZ	ES	HU	IE	LV	UK(NI)	SI
DK	FR	MT	NL	HR	PL	SK

  Indoor only for UNII-1 in EU/UK means acceptable EIRP for use inside train carriages is 40 mW (16 dBm). If the attenuation loss of the train carriage is on average greater than 12 dB then 200 mW (23 dBm) is applicable[2].

  When the unit is used in EU and the frequency range 5725-5850 MHz the output power is limited to 25 mW (14 dBm) EIRP.

  UNII-2A 5250 ~ 5350 MHz and UNII-2C 5470 MHz are only to be used for ‘In-building’ or ‘Indoor’ use cases and not in vehicles. 200 mW EIRP is allowed for UNII Band 2a and 1 W for UNII Band 2c. Transmitter Power Control (TPC) and Dynamic Frequency Selection (DFS) are required.
- 6 GHz (5.925 ~ 7.125 GHz)
  UNII-5 5.925 ~ 6.425 GHz for EU, UK, USA, Canada, AUS and NZ.
  UNII-7 6.525 ~ 6.865 GHz for USA, Canada.

[1] HPOD (Higher Power RLAN Devices) licensing requirements need to be followed.
[2] For detailed information relating to specific restrictions on use and allowed EIRP, please read:
COMMISSION IMPLEMENTING DECISION (EU) 2022/179 of 8 February 2022 on the harmonised use of radio spectrum in the 5 GHz frequency band for the implementation of wireless access systems including radio local area networks and repealing Decision 2005/513/EC.

2.4 Regulatory Compliance

Icomera has implemented processes to ensure compliance to directives, regulations, and laws applicable on Icomera products and services. Table 4 below lists some requirements met by the access point. The full text of the EU declaration of conformity can be found in, Appendix C. See Appendix B for FCC/ISED regulatory notices.

Table 4. Requirements met by the A2-e

Regulatory Certifications	Market
— **CE conformity - RED (2014/53/EU)** Article 3.1a, Health & Safety ○ EN 50385 ○ EN IEC 62311 ○ EN IEC 62368-1 Article 3.1b, EMC ○ EN 301489-1, -3, -17 ○ EN 55032 ○ EN 55035 Article 3.2, Radio ○ EN 300 328 ○ EN 301 893 ○ EN 300 440 ○ EN 303 687 — RoHS (2011/65/EU) & (2015/863) ○ EN IEC 63000	EU
— **FCC** ○ 47 CFR FCC Part 15b and Part 2.1091 — **ISED** ○ ICES-003, Issue 7 ○ RSS-102, Issue 5 — **CP65**	North America
Rail Industry Requirements	
— EN 45545 Fire Assessment — EN 50155 Rail Standard (Rolling stock) ○ EMC, EN 50121-3-2 ○ Environmental, IEC 60068-2, IEC 61373, EN 50125-1 ○ Protective Provisions EN 50153-1	All
Additional Requirements	
— IP65 rating to EN 60529 — REACH (EC) 1907/2006	All

3 System Design

The two access point configurations support both star topology and daisy chain setups. Regardless of the network design, Internet connectivity is provided by an Icomera router connected to the network. The system is designed according to the principle of least privilege and secure by default. This means that there is no need for additional firewalls, or equivalent security measurements.

3.1 Star Topology

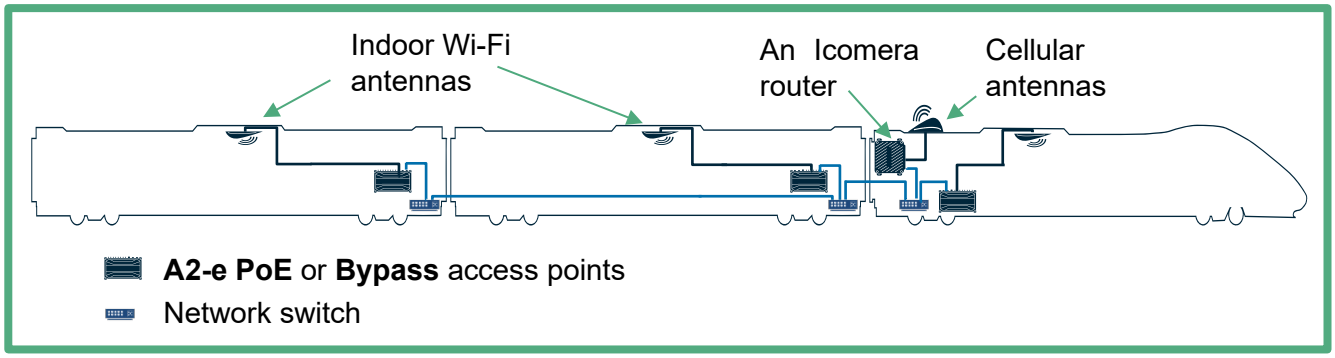


Figure 8. Example of system design overview with star topology access points.

In a star topology, as illustrated in Figure 8, the access point is connected to a network switch, either with or without PoE++. This network design can also be combined with daisy-chained access points, refer to section 3.2.

3.2 Daisy Chain Network

Implementing a daisy chain network requires the A2-e Bypass model of the access point.

In a daisy-chained network, devices are connected sequentially, one to the next, forming a single pathway for data. Each device relays data to the next until it reaches its destination. The bypass relay ensures that Ethernet traffic can still flow through the access point, even in case of power failure.

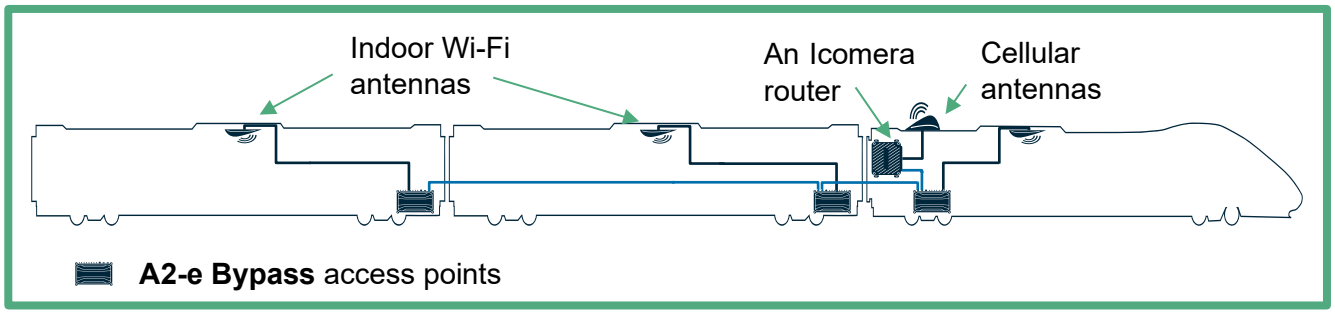


Figure 9. Example of system design overview with daisy-chained access points.

Figure 9 illustrates a possible system design, where the access points are daisy-chained, removing the need for network switches in each train car. This system design requires an external DC source.

4 Pre-installation Preparations

Before the actual on-site installation, some preparations are needed. The following sections describe considerations made to select suitable installation locations and cable routing, as well as some software configuration to regard.

Installation and configuration of other Icomera devices and peripherals should be made as described in respective manual.

4.1 Selecting the Optimal Access Point Location

Before starting the actual on-board installation of the access point(s), consider the following to ensure proper cable lengths and optimal system performance:

- The access point must be installed at a secure location, accessible only to authorized and trained personnel.
- There should be convenient connector access. The access point has all connectors on one side. The power and Ethernet connectors require the most space, 120 mm with straight connectors.
- Preferably install the access point so it is easy to see the status indication LEDs.
- The access point should be installed at a ventilated location, with air circulation, out of direct sunlight and away from other sources of heat.
- The unit should be located at a place, where it cannot be exposed to water ingress.
- The access point is designed with cooling fins. Vertical placement of the access point is preferred, to create best possible airflow. When installing the access point horizontally, ensure there is good air flow around the fins. A larger distance between the access point and the mounting surface (5 mm as minimum) provides a better air flow.

4.2 Centrally Made Configuration

Upon production, the access point is assigned a default configuration in which the Wi-Fi functionality is disabled. This configuration may be modified by Icomera personnel using the cloud-based application Organiser, a component of the Icomera Network Insight and Control (ICONIC) platform.

Prior to the physical installation, the access point status should be set to **Commissioned** in ICONIC, and ideally, the desired customer configuration should be defined for the access points. This allows the devices to retrieve their assigned configurations as soon as an Internet connection is established, facilitating a smoother installation process on-site. Additionally, access point reports will become available in ICONIC as soon as the access points have downloaded and applied their configurations. Refer to section 5.3 for Wi-Fi related configuration. By default, the access points will check for configuration updates every five minutes.

Safety features that can be enabled via the configuration are described in the document REL-00928 X.X The Icomera Wireless Platform 5 - Supported Features.

4.3 Wi-Fi

Follow the guidelines provided in the following sections to ensure regulatory compliance.

It is highly recommended to use all Wi-Fi radios to support a wide range of connecting devices, enabling the 2.4, 5, and 6 GHz bands.

The Wi-Fi radios can be configured either as access point or client. When used as a client, the Wi-Fi radio will search for an access point to connect to, enabling the Ship-to -Shore feature, refer to section 4.3.5.

The allowed transmit power at maximum data rate (Equivalent Isotropic Radiated Power, EIRP) vary, depending on 802.11 protocol, see Table 6 to Table 13. The maximum transmit power in access point mode is configurable via the software.

4.3.1 Selecting the Optimal Antenna Location for Passenger Wi-Fi Coverage

- Since the 5 GHz and 6 GHz band is less able to penetrate objects, those antennas need to be centrally located in the train car, see Appendix A.
- More than one antenna may be needed if the coverage is insufficient.
- Locate the Wi-Fi antennas as far away as possible from radiating or jamming signals.
- Avoid any metallic material in front of, or beside the Wi-Fi antennas.
- The antenna(s) should preferably be mounted above head height, underneath the ceiling.
- To maintain regulatory compliance, at least 20 cm in EU/Australia/UK and 30 cm in USA/Canada separation distance between the antenna and the user’s body must always be maintained.
- Note that passenger bodies attenuate the Wi-Fi signal, and this should be considered.
- The routing of cable between the antenna(s) and the access point should be easy.
- Longer antenna cables and patches along the way cause some attenuation of the signal.
- If long cables are needed to achieve good Wi-Fi coverage, low loss cables (1 dB/m at 5 GHz) can be used to minimize signal attenuation.
- Carefully follow the instructions from the antenna manufacturer, regarding ground plane, distance to other objects, etc.

4.3.2 Wi-Fi Antenna Gain and Path Loss

Tests conducted to ensure regulatory compliance were performed using antennas with the gain specified in Table 5. The access point was connected to the antenna's cables which have a loss of 0.1 dB. The default configuration of the access point radios assumes that the combination of antennas and cables used in the installation maintains the same Effective Isotropic Radiated Power (EIRP[1]). This configuration ensures that the access point does not exceed permissible EIRP limits across different countries.

If a different combination of antennas and cables is used, please ensure that the resulting EIRP matches that of the configuration used during the regulatory compliance test, see Table 5. For instance, if a higher gain antenna is used, the cable length must be increased or the transmit power needs to be reduced accordingly.

- The antenna should have a nominal impedance of 50 Ω.
- The selected antenna should be a dipole type antenna.

Additionally, the maximum transmit power in access point mode can be further reduced via software configuration, if necessary, see section 4.3.3.

Table 5. Configuration details and needed combination of cable loss and antenna gain for regulatory compliance.

	Wi-Fi 2.4G	Wi-Fi 5GL	Wi-Fi 6G	Wi-Fi 5GH
Radio interface name	**wlan0**	**wlan1**	**wlan2**	**wlan3**
Frequency range (MHz)	2401-2482	5150-5350	5925-7125	5470-5850
Radio frequency range (included in the interface setting "Wi-Fi channel settings")	**2.4G**	**5GL**	**6G**	**5GH**
Peak antenna gain (dBi)	4			
Cable/path loss (dB)	0.1			
Resulting gain (dBi)	3.9			

The logics for combination of channel and channel bandwidth follows the standard defined by IEEE 802.11. Refer to https://en.wikipedia.org/wiki/List_of_WLAN_channels for example.

[1] EIRP=P_{out} (dBm) + Antenna gain (dBi) – Cable loss (dB).

4.3.3 Radio Considerations

The default configuration of the access point radios is designed to prevent them from exceeding the permitted Equivalent Isotropic Radiated Power (EIRP[1]) across different countries. To ensure regulatory compliance, the following considerations are essential:

- The operating country of the unit, as only channels permitted in that specific country may be used. When travelling across multiple countries, select the country with the strictest regulations. Refer to Table 6 to Table 13 for information on allowed channels and EIRP limits.
- The maximum allowed EIRP must not be exceeded for the country in which the device is operating.
- Ensure that the combination of antennas and cables used, see section 5.3.1, Table 5, matches that of the tested configuration.

— The 5 GHz channels should be selected to be as far apart as possible for the two 5 GHz radios.

— When several access points are installed select the channels in each access point to get an optimal channel spacing between neighbouring access points, see Appendix C for an example.

To create an optimal radio environment inside the train, it is important to consider the Signal-to-Noise Ratio (SNR) level within the coach, as this directly affects the user experience. The SNR should be kept as high as possible to maximise the distance between the signal and the noise floor. However, high transmission power can increase the noise level, which may, in turn, degrade the strength and performance of the wireless signal, ultimately reducing throughput.

To ensure compliance with regulations in the operating area, the default access point configuration follows the values stated in Table 6 to Table 13.

Setting:

Country
Should always be set.
This will allow the access point to automatically adapt to local regulations. When the access point will be used in several countries, select the country with the strictest regulations.

Interface settings (should be defined for each radio):

Wi-Fi channel settings
This includes the **radio frequency** range, **channel** and optionally the **channel bandwidth**. The **radio frequency** range should be the same as stated in Table 5.

The radio will not work if:
- the wrong frequency range is set for the radio in question.
- a disabled channel is set by mistake (such as channel 12 and 13 in US).

Wi-Fi transmission power
This is only used to limit the power. When transmission power needs to be reduced, for example, to minimise interference between neighbouring access points, or if the combination of selected antenna and antenna cable exceed 3.9 dBi resulting gain, the **Maximum conducted TX power** specified in the tables, along with the **Measured EIRP** can be used to determine the appropriate **Wi-Fi transmission power** setting.

Example:
An antenna with gain 6 dBi and a 3 m cable with 0.5 dB/m attenuation has been used to connect the 2.4 GHz radio in Europe.
Resulting gain = 6 – (3 x 0.5) = 4.5 dBi which is higher than 3.9 dBi.
The default transmission power needs to be reduced by 0.6 dB (4.5 – 3.9).
The channel bandwidth is set to **HT40**.
Wi-Fi transmission power = Default transmission power of 15.76 – 0.6 ≈ **15**.

Refer to Table 8 and section 6.4.4 to avoid too high power transmission if the attenuation loss of the train carriage is on average below 12 dB, in EU for 5 GHz-L radios, UNII-1. For all other cases, the access point software will ensure that the allowed EIRP is not exceeded, provided that the correct country has been set, see **Country** above.

For the 5 GHz radios, only Wi-Fi channels belonging to the 20 MHz channel bandwidth can be used, even if the Wi-Fi channel width is set to 40 or 80. Allowed channels to use are:
- 5GL 36, 40, 44, 48,
- 5GH 149, 153, 157, 161, and 165.

Table 6. The maximum conducted transmission power for the 2.4 GHz radio, for various channels and protocols when used in Europe (RED).

Wi-Fi channel bandwidth	Wi-Fi channel setting	Maximum conducted TX power (dBm)	Measured EIRP (dBm)	EIRP limit (dBm)
802.11b	1-13	13.59	17.28	<=20
802.11g	1-13	15.48	19.17	<=20
HT20/HEW20	1-13	15.75	19.44	<=20
HT40/HEW40	1-13	15.76	19.45	<=20

Table 7. The maximum conducted transmission power for the 2.4 GHz radio, for various channels and protocols when used in USA and Canada (FCC/ISED).

Wi-Fi channel bandwidth	Wi-Fi channel setting	Maximum conducted TX power (dBm)	Measured EIRP (dBm)	EIRP limit (dBm)
802.11b	1-11	29.34	32.88	<=36.02
802.11g	1-11	29.03	32.58	<=36.02
HT20/HEW20	1-11	29.14	32.69	<=36.02
HT40/HEW40	1-6	26.55	30.09	<=36.02

Table 8. The maximum allowed transmission power for the 5 GHz-L radios, UNII-1, for various channels and protocols when used in Europe (RED)

Wi-Fi channel bandwidth	Wi-Fi channel setting	Maximum conducted TX power (dBm)	Wi-Fi transmission power setting[1]	Measured EIRP (dBm)	EIRP limit (dBm)
802.11a	36, 40, 44, 48	17.44	11	21.77	<=23
HT20/VHT20/HEW20/EHT20	36, 40, 44, 48	17.97	11	22.26	<=23
HT40/VHT40/HEW40/EHT40	36, 44	18.02	11	22.31	<=23
VHT80/HEW80/EHT80	36	18.14	11	22.43	<=23

Table 9. The maximum conducted transmission power for the 5 GHz-L radios, UNII-1, for various channels and protocols when used in USA and Canada[2] (FCC/ISED).

Wi-Fi channel bandwidth	Wi-Fi channel setting	Maximum conducted TX power (dBm)	Measured EIRP (dBm)	EIRP limit (dBm)
802.11a	36, 40, 44, 48	16.92	21.25	<=23
HT20/VHT20/HEW20/EHT20	36, 40, 44, 48	17.33	21.66	<=23
HT40/VHT40/HEW40/EHT40	36, 44	17.88	22.21	<=23
VHT80/HEW80/EHT80	36	17.04	21.36	<=23

[1] If the attenuation loss of the train carriage is on average less than 12 dB, the transmission power of the radio must be reduced.

[2] UNII-1 may only be used in Canada under ISED HPOD licencing laws.

Table 10. The maximum conducted transmission power for the 5 GHz-H radios, UNII-3, for various channels and protocols when used in Europe (RED)

Wi-Fi channel bandwidth	Wi-Fi channel setting	Maximum conducted TX power (dBm)	Measured EIRP (dBm)	EIRP limit (dBm)
802.11a	149, 153, 157, 161, 165	10	13.53	13.98
HT20/VHT20/HEW20/EHT20	149, 153, 157, 161, 165	10	13.71	13.98
HT40/VHT40/HEW40/EHT40	149, 157	10	13.56	13.98
VHT80/HEW80/EHT80	149	10	13.65	13.98

Table 11. The maximum conducted transmission power for the 5 GHz-H radios, UNII-3, for various channels and protocols when used in USA and Canada (FCC/ISED).

Wi-Fi channel bandwidth	Wi-Fi channel setting	Maximum conducted TX power (dBm)	Measured EIRP (dBm)	EIRP limit (dBm)
802.11a	149, 153, 157, 161, 165	29.93	34,0	<=36
HT20/VHT20/HEW20/EHT20	149, 153, 157, 161, 165	29.37	33.46	<=36
HT40/VHT40/HEW40/EHT40	149, 157	29.74	33.82	<=36
VHT80/HEW80/EHT80	149	29.3	33.38	<=36

Table 12. The maximum conducted transmission power for the 6 GHz radios, UNII-5, for various channels and protocols when used in Europe (RED)

Wi-Fi channel bandwidth	Wi-Fi channel setting	Maximum conducted TX power (dBm)	Measured EIRP (dBm)	EIRP limit (dBm)
HEW20/EHT20	1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 69, 73, 77, 81, 85, 89, 93	17.87	22.57	<=23
HEW40/EHT40	1, 9, 17, 25, 33, 41, 49, 57, 65, 73, 81, 89	17.57	22.41	<=23
HEW80/EHT80	1, 17, 33, 49, 65, 81	17.84	22.54	<=23
HEW160/ETH160	1, 33, 65	17.35	22.05	<=23
ETH320	1	16.88	21.58	<=23

Table 13. The maximum allowed transmission power for the 6 GHz radios, for various channels and protocols when used in USA and Canada (FCC/ISED).

Wi-Fi channel bandwidth	Band	Wi-Fi channel setting	Maximum conducted TX power (dBm)	Measured EIRP (dBm)	EIRP limit (dBm)
HEW20/EHT20	UNII-5	1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 69, 73, 77, 81, 85, 89, 93	2.01	6.49	<=14
HEW20/EHT20	UNII-7	117, 121, 125, 129, 133, 137, 141, 145, 149, 153, 157, 161, 165, 169, 173, 177, 181	1.76	6.42	<=14
HEW40/EHT40	UNII-5	1, 9, 17, 25, 33, 41, 49, 57, 65, 73, 81, 89	4.5	8.98	<=14
HEW40/EHT40	UNII-7	121, 129, 137, 145, 153, 161, 169, 177	4.3	8.97	<=14
HEW80/EHT80	UNII-5	1, 17, 33, 49, 65, 81	7.18	11.66	<=14
HEW80/EHT80	UNII-7	129, 145, 161	7.38	12.04	<=14
VHT160	UNII-5	1, 33, 65	9.34	13.83	<=14
VHT160	UNII-7	129	8.25	12.91	<=14
VHT320	UNII-5	1	8.88	13.37	<=14

4.3.4 On-board Network Considerations

There are several network configuration options that can be enabled for the access point. Some of the features are listed below:

- The device can be configured with either static IP address or to receive its IP address dynamically (DHCP).
- The passenger traffic can be separated from other traffic in the Wi-Fi network, for instance by using VLANs.
- It is necessary to have separate virtual networks on different interfaces to support client isolation.
- The access points always have SNMP traps enabled through Ethernet.
- Up to twelve SSIDs can be used for each Wi-Fi radio.
- Unique MAC addresses can be set by the access point for each SSID.
- SSIDs can be visible or hidden.
- SSIDs can be password protected.
- Password protected traffic can be encrypted.

When configuring the access point for use in a daisy chain setup, the Ethernet ports must be assigned to the same VLAN.

Safety features that can be enabled via the configuration are described in the document REL-00928 X.X The Icomera Wireless Platform 5 - Supported Features.

4.3.5 Ship-to-Shore Wi-Fi

If a system should include Ship-to-Shore Wi-Fi[1], where data is transferred between the train and a stationary access point, one of the access point Wi-Fi radios can be configured to act as a client. Select the radio that follows the same frequency range as the stationary access point. The radio should use the SSID, passphrase and encryption method as defined in the stationary Wi-Fi access point[2].

In Europe, the 5150 – 5350 MHz bands are only allowed to be used indoors.

The resulting gain from the antenna is not allowed to exceed the value stated in Table 5, to maintain regulatory compliance, when the access point is used for Ship-to-Shore Wi-Fi.

Preferably, use an access point installed close to a router for Ship-to-Shore Wi-Fi. This allows a diplexer filter to connect one of the cellular antennas to both the access point's Wi-Fi antenna connector and the router's cellular antenna connector. As a result, the number of required antennas is reduced, eliminating the need for a dedicated Ship-to-Shore Wi-Fi antenna. For further details, refer to the installation and maintenance manual of the router included in the on-board system.

[1] See separate license component.
[2] Consider the regulations applicable in the present country when configuring the stationary access point.

5 Safety and General Handling

- Installation and service staff should have appropriate skills.
- Keep away from catenary and high voltage lines.
- Be careful when working at height.
- Always secure ladders.
- When drilling holes, ensure suitable eye protection is worn and there is enough clearance behind drilled components.
- When drilling and cutting holes, ensure sharp edges are de-burred.
- Icomera does not take responsibility for damage caused to ESD-sensitive devices due to improper handling during unpacking, or installation. Therefore, always take precaution to protection against electrostatic discharge, by grounding yourself.
- Do NEVER attempt to open the unit, as non-expert handling of the interior may damage the device. Internal parts may have dangerous voltage levels and high temperatures.
- When working, the surface of the unit can get hot. This might cause pain or discomfort. The time to human touch is less than 1s.
- Follow any applicable regulations, or rules. For example, do not place an operational unit near unshielded medical equipment.
- Do not drop the unit. Excessive mechanical shocks can reduce product lifetime. Therefore, always carry the unit with both hands and handle it with care.
- Use the correct external power source.
- Only use Icomera-approved antennas and accessories.

The resulting current can reach dangerous levels to humans.

- Ensure the unit’s power source is disconnected before any maintenance activities.
- Do not modify cables or connectors. Consult a licensed electrician for site modifications. Always follow local or national wiring rules.
- The unit meets international guidelines for exposure to radio waves. However, this equipment generates, uses, and radiates radio frequency energy, and if NOT installed and used in accordance with this manual, may cause harmful interference.

All Icomera wireless products are evaluated to ensure they conform to the RF emissions safety limits and regulations valid around most of the world, in accordance with the various regulations and guidelines adopted, or recommended by the Federal Communications Commission (FCC), the European Commission and other worldwide agencies, see section 2.4.

6 On-Site Installation

All installation material provided via Icomera is PVC and halogen free.

During the installation, consider the following:

- To prevent damage of equipment, all screws and connectors should be fastened and unfastened by using hand tools, e.g., by using a torque wrench. Using power tools, or otherwise excessive power to fasten, or loosen screws and connectors may damage the equipment, or cause reduced product lifetime. Tighten all screws with appropriate torque.
- Label all cables thoroughly before routing them.
- Cables should be routed in a way that prevents tensile stress and sharp bends.
- Use cable ties, or tape to secure the cable at 30-45 cm (12”-18”) intervals.
- Do not wrap the cables.

6.1 Physical Installation

Icomera recommends to initially perform field tests, in each train model, to find optimal antenna locations, before choosing a permanent spot and committing to cable routing.

1 When the best location has been decided for each unit, see section 5.1, 5.3.1 and 5.3.5, label and route all cables. Use cable ties, or straps to secure the cables.

2 Mount each antenna, using supplied washers and nut. Follow the instructions provided with respective antenna. Ensure all antenna mounting/antenna cable holes are drilled to correct size and location. The torque is provided in the antenna mounting instructions, for the mounting screws.
Make sure to mount each antenna firmly so it cannot come loose which could result in personal injury.

3 Connect the antenna cables to the antennas. Use 1 Nm torque for N connectors. Refer to the antenna mounting instructions as well.

4 Always connect the unit to protective earth, as described in section 7.2.

Connect the unit to protective earth, before it is mounted, since protective earth always must be the first element to be connected and this might be difficult to do afterwards.

The access point is designed with cooling fins. Vertical placement of the unit is preferred, to create best possible airflow.

When installing the access point horizontally, ensure there is good air flow around the fins.

5 Mount the unit into place by only using four screws, such as M6, in the mounting holes, indicated in Figure 2. Make sure the screws and mounting area can handle the weight of the unit. Apply appropriate torque, based on selected screws, the material and thickness of the mounting area.

6 Connect all cables to the access point, in in the order described in section 7.3.

7 Check that the Power LED turns solid green. Verify the installation as described in section 7.4. The access point automatically connects to ICONIC and downloads its configuration.

See the router's installation manual and other units connected to the on-board network to test other parts of the on-board installation.

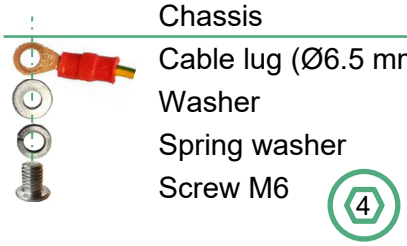
6.2 Grounding of the Access Point

The access point must be grounded. Never operate the equipment in the absence of a suitably installed connection to protective earth since this could result in personal injury and might damage the unit. Therefore, protective earth must always be the first element to be connected and the last element to be disconnected from the unit. Contact the appropriate electrical inspection authority, or an electrician, if it is uncertain that protective earth is available.

Consider the following:

- All earthing connections shall comply with EN 50343.
- The minimum cross-section of the protective earth conductor shall be 2.5 mm^2.
- The length of the ground cable should be as short as possible and not exceed one meter.
- Contact surfaces shall be protected against corrosion.
- Earthing connections shall ensure a permanent electrical connection with good conductivity and shall be vibration-proof.
- The system shall not contain several earthing connections in series, where the removal of one component would interrupt the earthing connection.

Connect the protective earth directly to the access point's ground poit (indicated with the symbol as in Figure 11), by using the M6 screw and washers included with the unit, see Figure 10. Apply 1.5 Nm torque.



Do not rotate or adjust the cable lug after the nut has been tightened.

Figure 10. The ground bolt of the access point.

Figure 11. Protective earth symbol

Connect the other end of the ground cable to protective earth. On-board the trains this should be indicated with the symbol in Figure 11. For the screw mounting of cable lug, use a cable lug that fits the nominal diameter of the screw.

6.3 Connecting Cables

6.3.1 Antenna Cables

All antenna connectors compatible with the access point have an outer ring, designed to be grasped and pulled directly away from the access point to disconnect, see Figure 6

All antenna cables provided by Icomera are designed so that the shield will be connected to ground when the cable is attached to the access point connector. When connecting, check that the connector is completely inserted with a “click”. Refer to section 3.2.4 and Figure 3 for the Wi-Fi ports.

6.3.2 LAN

Always use CAT7 network cables.

- In a daisy chain setup[1], use both the LAN 1 and LAN 2 ports.
- When using a star topology with PoE++, connect the Ethernet cable to the LAN 1 port (refer to section 7.3.3.1).
- When using a star topology with an external DC source, it is recommended to connect the Ethernet cable to the LAN 2 port. Never connect the LAN 1 port to a network switch providing PoE when the access point is powered by an external DC source.

Refer to section 2.2.4 and Figure 3 for the LAN ports.

Secure the LAN connector on the access point by screwing it clockwise by hand. The recommended tightening torque is 0.6 Nm.

6.3.3 Power Supply

Never power the A2-e PoE access point from both a PoE power source and through the DC power.

6.3.3.1 Star Topology

When the access point is connected to the network via a single network cable, the power source may be either PoE++ or an external DC source. For the latter, refer to section 6.3.3.2.

When using PoE++, connect a CAT7 Ethernet cable to the LAN 1 port on the access point, and the other end to a network switch port or PoE injector compliant with IEEE 802.3bt (PoE++) Type 3. Refer to section 7.3.2 for instructions on securing the connector to the access point.

[1] Requires the A2-e Bypass model.

6.3.3.2 Daisy Chain Network

Daisy-chained access points require the A2-e Bypass model.

The A2-e Bypass model must be powered by a nominal 24 to 110 V (DC) source.

Connect the access point to the external power source using a shielded cable, with a conductor area of at least 4 x 1.0 mm^2. The shield minimises electromagnetic interference affecting other equipment.

The cable shield must be connected to ground, isolated from the negative supply.

A circuit breaker or slow-blow fuse with an appropriate current rating MUST be used to protect the product and the cable.

The recommended ratings are:

- 24 V DC: 6 A slow-blow fuse
- 110 V DC: 1.5 A slow-blow fuse

Icomera can provide a 1.5 m power cable (608154) with the cable wires labelled according to their positions in the connector, refer to section 2.2.4.1.

Note: The pin configuration of the Icomera M12 K connector may differ from that of other manufacturers. Therefore, ensure to follow the pinout specified by Icomera.

6.4 On-Site Test of the Installation

A laptop, tablet, smartphone, or other mobile device with Wi-Fi capability is needed to test the installation.

Preferably perform the test in the order as described below.

6.4.1 The Ground Bolt

Check that the ground wire is properly attached. Use a multi-meter, to ensure there is less than 10 mΩ (0.01 Ω) of resistance point to point.

6.4.2 Power On

The access point automatically starts when power is supplied. This should be indicated on the Power LED, see section 2.2.5. The access point will be operational within approximately two minutes of first receiving power.

6.4.3 Verification of Internet Access

By default, the access point SSID will not become visible until the access point has connected to the Internet and fetched its centrally defined configuration. When the access point has Internet access it will automatically download its centrally made configuration. Do the following to ensure that the configuration has been downloaded:

1. Check that the SSID(s) defined in the access point configuration becomes visible in the list of available Wi-Fi networks when looking in the Wi-Fi settings on a mobile device, for instance. If the SSID does not appear, see section 8.2.

2. When an access point has been up and running for approximately 5 minutes, its **Online** status in the **Discovery**, **Browse**, **Devices** list should be updated and indicated as green.

6.4.4 Signal Strength

Preferably, use a proper measuring device to check the Wi-Fi coverage. If this is not available, a mobile device can be used instead.

The Wi-Fi signal strength should be around -55 dBm. The closer to zero, the better. However, excessively high signal strength can interfere with other access points, leading to reduced overall network performance. If the signal strength is around -75 dBm or worse, this indicates a potential issue with the setup, and further investigations should be carried out.

To create an optimal radio environment inside the train, it is important to consider the Signal-to-Noise Ratio (SNR) level within the coach, as this directly affects the user experience. The SNR should be kept as high as possible to maximise the difference between the signal and the noise floor. However, high

transmission power can increase the noise level, which may, in turn, degrade the performance of the wireless signal, ultimately reducing throughput.

Do the following to check the Wi-Fi coverage with a mobile device:

1 The visible SSID(s) should appear in the mobile device settings, under the Wi-Fi network list.

2 Select the access point SSID from the list. If the SSID does not appear, see section 8.2.

3 Check the coverage throughout the entire train by moving around and study the Wi-Fi strength symbol or use some app (for instance Wi-Fi Analyzer for Android, or AirPort Utility for iPhone.

Ensure the 2.4, 5, and 6 GHz frequency bands are functioning properly. The Wi-Fi signal strength should be approximately -55 dBm. If it measures around -75 dBm or worse, there is likely an issue that requires further investigation. The signal strength should remain as even as possible throughout the train. Additionally, ensure all neighbouring access points operate on different channels to avoid interference.

If the coverage is poor in certain areas, consider the following:

a) Verify that the channel spacing between neighbouring access points is optimised.
b) Adjust the transmission power settings in the access point configuration to reduce interference with adjacent access points. Refer to Table 6 to Table 13 for guidance.
c) Evaluate the physical placement of the antennas and relocate them if necessary to improve coverage and minimise interference.

For access points installed in the EU/UK countries, when using the 5 GHz-L radio:

4 Measure the signal strength on both sides of the outer wall of the train carriage.
If the attenuation loss of the train carriage is on average greater than 12 dB, then the power transmission strength can be handled as stated in section 4.3.3. If not, **Wi-Fi power transmission** needs to be reduced, until the resulting EIRP reaches 16 dBm, see Table 8. The set value depends on the selected channel bandwidth.

6.4.5 Ship-to-Shore Wi-Fi

Turn on the stationary access point. Check that the router can download/upload files via the Ship-to-Shore Wi-Fi by using SSH commands (only available for Icomera employees), or as described in the Discovery manual, see REL-00468 X.X Icomera Discovery XXX – User Manual. For instance, the SureWAN Connectivity graph can indicate whether the Wi-Fi radio has been used when expected.

7 Preventive Maintenance

No preventive maintenance is needed for the access point. However, preferably perform annual checks to ensure a significant amount of dust and dirt is not present on the chassis and external connectors. This ensures efficient, continuous heat dissipation and reliable electrical connections. Do also check that no parts are loose. If needed tighten screws and cable connectors.

8 Maintenance and Troubleshooting

Icomera provides service agreements in different levels. The Icomera solution is designed to be supported remotely, with the ability to both monitor and fault trace and rectify. Because of this, the only onsite access point maintenance required is checking cable connections and the replacement of failing devices.

All maintenance and fault tracing shall be performed by service staff with relevant skills.

To prevent damage of equipment, all screws and connectors should be fastened and unfastened by hand, e.g., by using a torque wrench. Using power tools, or otherwise excessive power to fasten, or loosen screws and connectors may damage the equipment, or cause reduced product lifetime.

If possible, do all troubleshooting when power to the Icomera router and good mobile coverage are available.

It is NOT allowed to open the unit for any reasons.

Incorrectly performed maintenance, or repair inside the access point voids any warranty.

Access point errors that cannot be eliminated remotely, or on site, require the unit to be replaced and sent to an Icomera service partner for further diagnosis, since there might be an internal error. Replacing the faulty unit (see section 9.3), is the most reliable way to get the system back into service, as fast as possible.

Before replacing a unit, perform the troubleshooting, as described in section 9.2, and contact Icomera, see section 9.3, if the problem persists.

8.1 Updating the Firmware

The IWP firmware is updated by using ICONIC. By default, the access point checks every 5 minutes for firmware updates. This ensures that all devices remain up-to-date with the latest security patches, added functionality, and other firmware improvements.

8.2 Troubleshooting to Identify Cause of Failure

The following troubleshooting procedures to identify cause of failure shall be performed in case the unit does not operate properly.

Disconnecting the power supply sometimes resolves a problem with the equipment. If this is called for, disconnect power to the equipment for 5 seconds, and then re-connect power and wait for at least two minutes.

Some parts of the troubleshooting procedures are made by using Icomera's web-based application Discovery, included in ICONIC. This can be used anywhere, by using an ordinary browser installed on a laptop, or tablet, with Internet connection.

The following sections describe some use cases, together with solutions.

The LEDs may be disabled within the access point configuration. Please verify that they are enabled prior to drawing any conclusions.

8.2.1 The Power LED Is on, but no Other LEDs Are Alive

If no other LED is on, besides the Power LED, see section 2.2.5, Figure 7, try to reboot the unit. If this does not help, the unit is probably defective. Contact the Icomera support organization, see section 8.6.

8.2.2 No Access Point SSID is Visible

There can be several reasons why no SSID is visible in the list of available Wi-Fi networks when looking in the Wi-Fi settings on a mobile device.

If the access point LEDs are enabled in the software, these can be used to verify the status of the access point, see section 2.2.5. Besides, the following steps can be performed:

1. Check that the connected network switch is turned on.
2. Use a network tester capable of testing PoE, to check the network switch output power from the network switch port.
    a) If there is no output power, move the connector to anther PoE++ port and check if this solves the problem. If the problem remains, check the cables and connectors. If they all seem OK, continue with point 3.
    b) If the network switch output power seems OK, continue with point 3.
3. The access point has no Internet connection.
   Check the following:
    a) That the network switch is on and seems to work. If this is the case continue with b). If it is turned off, turn it on.
    b) Connect a laptop to the same port on the network switch and try to get Internet access. If the network switch seems to work, contact Icomera, see section 9.3. If this is not working continue with c).

c) The network switch configuration. If this is correct, continue with d).
d) That the network switch has Internet access.
If the network switch is connected to the Internet via an Icomera router,
- try to ping the router from the laptop connected to the network switch. Ensure that the laptop receives a DHCP lease if DHCP is used in the network. If this is working, check that the router has Internet access as described in its installation and maintenance manual (e.g. the section “The router Has Been Powered up but Does Not Connect to the Internet”).
- if it is impossible to ping the router, check the remaining network between the router and the network switch.
e) If the network switch has Internet connection, continue with point 4.

4 The access point configuration has no SSID defined in its configuration.

a) In ICONIC, check the configuration for the access point in question. Check that the SSID is defined for each Wi-Fi interface that should be used. Add the missing SSID(s) to the configuration. The changed configuration should be applied on the access point within 5 minutes.
b) If SSID(s) have been defined in the configuration, continue with point 5.

5 As soon as the access point starts reporting to ICONIC, its Online status in the Discovery, Browse, Devices list should be updated and indicated as green. If there still are no visible SSIDs, or the access point is indicated as red, or it says No information, contact the Icomera support organization, see section 9.3.

8.2.3 The SSIDs Are Visible, but There Is No Internet Access

If there are SSIDs visible but it is impossible to connect to the Internet, follow the steps described in section 9.2.1, point 3 for access points in a star topology.

If the access point is daisy-chained, there might be some network interruption between the access point and the router providing the Internet connectivity. If this is the case, other devices might be affected as well. Check all connections.

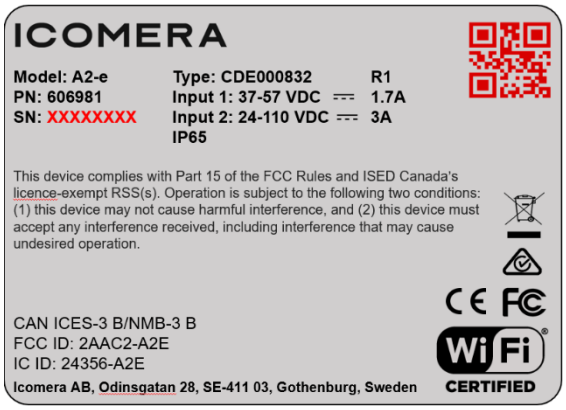
The bypass relay in the access point ensures that Ethernet traffic can still flow through the access point, even in cases of power failure.
To verify that the network switches work as intended follow the steps described in section 9.2.1, point 3.

8.3 When Troubleshooting Actions Do Not Solve the Problem

When troubleshooting has been performed as described in section 8.1, and no solution has been found, contact Icomera to be advised on further actions.

This is done by sending an email to online.support@icomera.com or the client specific email address specified in the service level agreement (SLA). Include the following information:

1. the customer return address, and contact details,
2. the serial number (visible on the product label and indicated by SN) of the faulty unit,
3. actions that have been performed when troubleshooting,
4. remaining problems and their consequences,



Only authorized service centres can handle maintenance of and/or repair the Icomera router. Improper handling can lead to loss of warranty.

Based on the information emailed to Icomera about the defective unit, Icomera will check if the warranty is still valid. Further remote troubleshooting can be performed, and some faults can be eliminated.

If Icomera classifies a unit as defective, a Return Material Authorization (RMA) issue will be raised and an email will be sent to the customer, together with an Icomera RMA form.

When a unit has been classified as defective, do the following:

1. Attach the RMA form to the defective unit.
2. Send the unit to the Return address stated on the RMA form.

If the warranty period has expired, all support actions will be charged for.

In case of damages occurred during transportation, when sent for repair, the repair will be treated as “Out of Warranty”.

Icomera takes no responsibility for shipping time, which might vary. When Icomera has the faulty unit, this will be repaired within the period as specified in the SLA. To avoid any inconvenience, it is recommended to have at least one spare unit in stock, that can be used instead of the faulty unit, see section 8.4.

8.4 Replacement of an Access Point

Sometimes an access point needs to be replaced when it is not working.

Usually, the replacement takes about 30 minutes, depending on the installation location.

When the unit needs to be replaced, prepare a spare unit before getting to the installation location:

Do the following on-location:

1. Locate the faulty unit.
2. Note the arrangement of the cable connecting directly to the unit, or those obstructing its removal.
3. Disconnect the PoE+ cable.
4. Loosen all screws holding the unit in place.
5. Disconnect the ground cable.

Protective earth must always be the first element to be connected and the last element to be disconnected from the router.

6. Remove the old unit.
7. Mount the spare unit as described in section 7.1.
8. Ensure the cables are routed in a proper way, see section 7, and replace any removed cable ties.

As soon as the unit has booted up and connected to the Internet, it automatically downloads its software and configuration from ICONIC.

Follow the procedures described in section 7.4 to check the installation.

9 Transport and Dispatch

Recyclable cardboard packaging is used for delivery of the unit.

No special precautions are necessary for transportation.

The product can be dispatched via customary parcel shipment.

10 Storage

The product should be stored in roofed buildings in an environment free of aggressive vapours, gases, and dust, in its undamaged package.

- Storage temperature range: -40 °C to +85 °C
- Relative humidity: max. 85 % at 40 °C

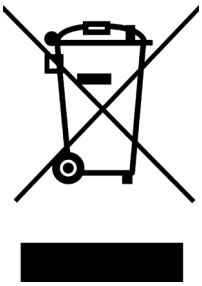
11 Disposal

Before any disposal of the unit, ensure that the configuration and other data has been deleted in a way that ensures data cannot be recovered.

Disposal of the device should follow the guidelines for electronic waste, never to be treated as household waste. It contains no dangerous agents as per UNIFE.

The owner is responsible for disposal of the device. Preferably leave the unit to an accredited WEEE recycler.

Return of the device to the producer is not intended but can be agreed upon in a separate contract.



12 Warranty

The warranty period is 12 months, starting from the date the unit is shipped from Icomera to the customer, unless no other agreement has been made. Extended warranty is available.

The warranty does not cover conditions, malfunctions, or damage caused by:

- poor installation,
- misuse,
- environment conditions which are deemed to be non-standard,
- water damage (due to poor storage and water ingress, for example),
- bad workmanship,
- damages occurred during transportation, when sent for RMA actions,
- failure brought about by a vehicle/connected unit fault.

13 Contact Information

For questions related to troubleshooting, see section 8, as well as common questions, send an email to online.support@icomera.com.

The global Support Desk team, including out of hours/on-call, is manned 24/7/365.

For customers with support agreement there are specific contact phone numbers.

14 Glossary

Acronym	Definition
BSSID	Basic Service Set Identifier A unique identifier, represented as a MAC address, assigned to each access point within a network. It distinguishes individual access points, even when they share the same SSID, and is critical for device-to-AP association and network management.
DHCP	Dynamic Host Configuration Protocol A client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.
EIRP	Equivalent Isotropic Radiated Power The maximum power (dBm) a perfectly isotropic antenna would need to radiate, to achieve the measured value in a fixed direction.
ESD	ElectroStatic Discharge A sudden flow of electricity between two electrically charged objects caused by contact. The discharge can be large enough to cause damage to sensitive electronic devices.
IMP	Icomera Mobility platform The operating system software, for instance used by the Icomera X6, X5, M4X, X^3 and X^3 (Rail).
ICONIC	Icomera Network Insight and Control The Icomera Internet portal providing a web-based user interface for applications used to configure, administer, monitor, and maintain the Icomera systems, both the hardware and software.
Internal error	An internal error is an error that is non-serviceable on site. All such errors require the unit to be replaced and shipped to an Icomera service partner. Due to the relatively dirty bus environment as well as the high risk of ESD damages, the functional demands of a unit cannot be met if the unit is not serviced by an Icomera Service partner.
IWP	Icomera Wireless Platform The operating system software used by the A2-e
LAN	Local Area Network A computer network that interconnects computers within a limited area such as a train, or a travel centre. Ethernet and Wi-Fi are the most commonly used transmission technologies.

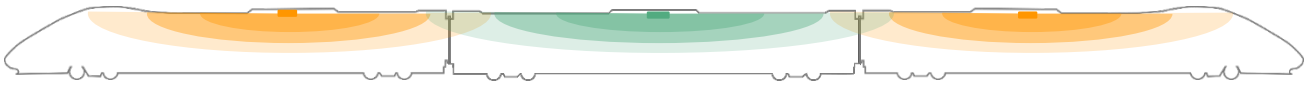
Acronym	Definition
MIMO	Multiple-Input Multiple-Output Multiple refers to multiple antennas used simultaneously for transmission and multiple antennas used simultaneously for reception, all over a radio channel. For instance, 4×4 MIMO refers to a configuration with four transmitter antennas and four receiver antennas.
MU-MIMO	Multi-user Multiple-Input Multiple-Output The technology allows a Wi-Fi access point to communicate with multiple devices simultaneously. This decreases the time each device must wait for a signal and dramatically speeds up your network.
RMA	Return Material Authorization When a unit has been classified as defective, an RMA should be issued by Icomera, before the faulty unit can be sent for repair.
SSID	Service Set Identifier Simplified, the human-readable name assigned to a Wi-Fi network as defined in the access point configuration. When connecting to a network, the SSID helps the device to know which Wi-Fi to join. The same SSID can be shared between several access points within the same network.
TCP	Transmission Control Protocol One of the main protocols of the Internet protocol suite.
WLAN	Wireless LAN See LAN.
WEEE	Waste Electrical and Electronic Equipment
Wi-Fi	A technology that lets electronic devices to connect to a wireless local area network (WLAN), using IEEE 802.11 standards, mainly using the 2.4 GHz and 5 GHz radio bands. A Wi-Fi radio is a self-contained system on a chip, with an integrated TCP/IP protocol stack, that can give any microcontroller access to a WLAN.

15 Referenced Documents

- The Icomera A2-e Access Point – Technical Product Description, document number SYS-00830
- Installation and Maintenance manuals for Icomera routers
- RF cables comparing the Huber+Suhner vs Rosenberger, document number 7060-P-CST-C.KA1.19589/HL-2
- Manuals for network switches, etc.
- Icomera Discovery– User Manual, document number REL-00468

Appendix A Indoor Antenna Location and Channel Selection

Figure 12 illustrates suitable locations for the access point indoor antennas for optimal carriage coverage. For each access point the Wi-Fi radio interface setting **Wi-Fi channel settings** is included, with reference to the radio interface, channel, and channel bandwidth. The channels have been selected to minimise interference both between the Wi-Fi radios within the access points and between neighbouring access points.



Antennas for access point 1
wlan0: 2.4G,1
wlan1: 5GL,36,HT40
wlan2: 6G,1,HT160
wlan4: 5GH,149,HT40

Antennas for access point 2
wlan0: 2.4G,11
wlan1: 5GL,44,HT40
wlan2: 6G,65,HT160
wlan4: 5GH,157,HT40

Figure 12. Example of antenna location and channel selection for the access points when the train will be used within the European Community, USA, and Canada.

Appendix B FCC/ISED Regulatory Notices

Modification statement

Icomera AB has not approved any changes or modifications to this device by the user. Any changes or modifications could void the user's authority to operate the equipment.

Icomera AB n'approuve aucune modification apportée à l'appareil par l'utilisateur, quelle qu'en soit la nature. Tout changement ou modification peuvent annuler le droit d'utilisation de l'appareil par l'utilisateur.

Interference statement

This device complies with Part 15 of the FCC Rules and Industry Canada's licence-exempt RSS standards. Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Wireless notice

This equipment complies with FCC and ISED radiation exposure limits set forth for an uncontrolled environment. The antenna should be installed and operated with minimum distance of 30 cm, between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter,

other than those covered by the device's human exposure report.

Cet appareil est conforme aux limites d'exposition aux rayonnements de l'ISDE pour un environnement non contrôlé. L'antenne doit être installée de façon à garder une distance minimale de 30 cm, entre la source de rayonnement et votre corps. L'émetteur ne doit pas être colocalisé ni fonctionner conjointement avec une autre antenne ou avec des émetteurs autres que ceux couverts par le rapport d'exposition humaine de cet équipement.

FCC Class B digital device notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television

reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CAN ICES-3 (B) / NMB-3 (B)

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de classe B est conforme à la norme canadienne ICES-003.

Very Low Power Device (6VL)

• The operation of this device is prohibited on oil platforms and aircraft, except that operation of this device in 5.925-6.425 GHz is permitted in large aircraft while flying above 10,000 feet.
• Installation on outdoor fixed infrastructure is prohibited.
• Controlling or communications with unmanned aircraft systems, including drones, is prohibited.

1. Devices shall not be used for control of or communications with unmanned aircraft systems.
2. Devices shall not be used on oil platforms.
3. Devices shall not be used on aircraft, except for the low-power indoor access points, indoor subordinate devices, low-power client devices, and very low-power devices operating in the 5925-6425 MHz band, that may be used on large aircraft as defined in the Canadian Aviation Regulations, while flying above 3,048 metres (10,000 feet).

devices shall prioritize operation on frequencies above 6105 MHz to 7125 MHz before operating on frequencies from 5925 MHz to 6105 MHz

1. Les dispositifs ne doivent pas être utilisés pour le contrôle ou les communications avec les systèmes d'aéronef sans pilote.
2. Les dispositifs ne doivent pas être utilisés sur les plates-formes pétrolières.
3. Les dispositifs ne doivent pas être utilisés à bord des aéronefs, sauf pour les points d'accès intérieurs à faible puissance, les dispositifs subalternes intérieurs, les dispositifs clients à faible puissance et les dispositifs à très faible puissance fonctionnant dans la bande de 5925 à 6425 MHz, qui peuvent être utilisés sur les gros aéronefs au sens du règlement de l'aviation canadien, alors qu'ils volent à plus de 3048 mètres (10 000 pieds).

the device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
le dispositif utilisé dans la bande 5150-5250 MHz est réservé à une utilisation en intérieur afin de réduire le risque de brouillage préjudiciable aux systèmes mobiles par satellite dans le même canal.
Les appareils doivent prioriser le fonctionnement sur des fréquences supérieures à 6105 MHz à 7125 MHz avant de fonctionner sur des fréquences de 5925 MHz à 6105 MHz

Appendix C Declaration of Conformity

ICOMERA
AN EQUANS COMPANY

Date: 2025-02-10

Declaration of Conformity

To whom it may concern

We,

Icomera AB
Odinsgatan 28, SE 411 03
Gothenburg, Sweden

Declare that the product:

Type of Equipment: Access Point
Brand: ICOMERA
Model Name: A2-e
HW version: R1
Type number: CDE000832
Intended use: Wireless Access Point, works as a mobile, high performance Wireless Access Point, foremost intended for rail

Conforms to:	2014/53/EU	Radio Equipment Directive, (RED)
	2011/65/EU	Restriction of Hazardous Substances Directive, (RoHS2)
	2015/863	Restriction of Hazardous Substances Directive, (RoHS3)

The conformity, to which this declaration refers, is demonstrated by the application of the following harmonized and non-harmonized standards:

Article 3.1 (a): Health and Safety of the User:	**EN 50385:2017** **EN IEC 62311:2020** **EN IEC 62368-1:2018**
Article 3.1 (b): Electromagnetic Compatibility:	**EN 55032:2015+A11:2020+A1:2020** **EN 55035:2017+A11:2020** **EN 61000-3-3:2013+A1:2019+A2:2021** **EN IEC 61000-3-2:2019+A1:2021** **EN 301 489-1:V2.2.3** **EN 301 489-3:V2.3.2** **EN 301 489-17:V3.2.4**

ICOMERA
AN EQUANS COMPANY

Article 3.2 : Effective and efficient use of RF spectrum:	**EN 300 328:V2.2.2** **EN 301 893:V2.1.1** **EN 300 440:V2.2.1** **EN 303 687:V1.1.1**

The conformity assessment procedure referred to in Directive 2014/53/EU (Module A in Annex II) has been followed thus CE is placed on the product. A2-e also complies with relevant parts of the following standards or regulations which may apply when used in certain environments or applications, (e.g. when used on railway rolling stock):

EN 45545-2:2020; EN 50155:2021; IEC 60068-2:2007, IEC 61373:2010, EN 50121-3-2:2016+A1:2019; REACH (EC 1907/2006); EN 50124-1:2017; EN 50125-1:2014; EN 50153:2014 +A1:2017+A2:2020, EMV06:2019

The Technical Documentation relevant to the product described above and which supports this Declaration of Conformity, is held at the manufacturer's address shown above.

Signed on behalf of **Icomera AB** by

By: Catherine Chardon
Title: Chief Executive Officer
Company: Icomera AB
Telephone: +46 317992103
e-mail: catherine.chardon@icomera.com

Icomera AB, Odinsgatan 28, SE 411 03 Göteborg, Sweden
Phone: +46 (0)31 799 21 00 | Web: www.icomera.com
VAT Registration Number: SE 556572286401 | Company Number: 556572-2864