Translation of the original
operating instructions
Version 1.1
Updated: 2025-08-11

Operating instructions

Industrial Router & Firewall

IRF3000 with DNV approval

TYPE APPROVED PRODUCT
DNV
DNV.COM/AF

ads tec
Industrial IT

Table of Contents

1 Comments

1.1 General

These operating instructions are intended to ensure the safe and efficient use of the *Industrial Router and Firewall* type **IRF34x1 with DNV approval**, hereinafter referred to as the "device".

The operating instructions must be read carefully by personnel before starting any work.

All safety instructions and operating instructions are prerequisites for safe working and must be observed.

When using the device, the laws and regulations applicable in the respective country at national, federal and European or international level must be observed.

The generally accepted rules of technology apply, which are usually formulated in the form of standards, guidelines, regulations, provisions and technical rules by national and federal organisations, as well as professional associations and committees for the relevant field.

Illustrations in this manual are for basic understanding and may differ from the actual design.

The operator is solely responsible for compliance with and observance of subsequent technical or legal changes as well as the operator's obligations.

The original version of these operating instructions was written in German. Any non-German version of these operating instructions is a translation of the German operating instructions.

1.2 Manufacturer

The manufacturer of the product is ads-tec Industrial IT GmbH. Hereinafter referred to as ADS-TEC.

1.3 Limitation of liability

ADS-TEC accepts no liability for personal injury, property damage, damage to the device or consequential damage resulting from failure to observe these operating instructions, improper use of the device, repairs and any other actions carried out on the device by unqualified electricians who are not certified by ADS-TEC, or the use of unauthorised spare parts. Failure to observe maintenance intervals also leads to exclusion of liability. Furthermore, it is strictly prohibited to make unauthorised modifications or technical changes to the device.

1.4 Relevant documentation for the device

The following documentation is authoritative for the setup and operation of the device:

- These operating instructions: Contain information on the installation, commissioning and operation of the device as well as the technical data of the device hardware.
- Technical data sheet (in English, see download area)
- Website: Drivers, software, user manuals, brochures and flyers can be downloaded from www.ads-tec-iit.com in the **download** area.

2 Safety

2.1 Structure of the safety instructions

The signal word classifies the hazard.

The type/sequence and source of the hazard are indicated below the signal word.

Instructions for avoiding the hazard are marked with an arrow (➡).

⚠ ⚠ **SIGNAL WORD**

Type/consequences of the hazard!

- Source of the hazard

➡ Measures to avoid the hazard

2.2 Grading of the degree of danger

The signal word classifies the hazard.

Instructions for avoiding the hazard are indicated by an arrow (➡).

2.3 Explanation of the symbols used

⚠ ⚠ **DANGER**

Indicates an imminent danger. If not avoided, death or serious injury will result.

⚠ ⚠ **WARN**

Indicates a potentially imminent danger. If not avoided, death or serious injury may result.

⚠ ⚠ **CAUTION**

Indicates a potentially imminent danger. If not avoided, minor or moderate injury may result.

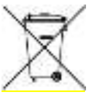
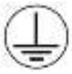
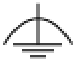
CAUTION

Indicates a potentially harmful situation. If not avoided, the equipment or something in its vicinity may be damaged.

Recommendation for use:

The symbol "Recommendation for use" indicates conditions that must be observed to ensure fault-free operation. It also provides tips and advice on how to use the device efficiently and optimise the software.

2.4 Symbols

Symbol	Meaning
	Marking for batteries and electronic devices. These must not be disposed of with household waste, but must be collected separately. Used batteries and electronic devices must be returned to the point of sale or to a disposal system.
	Symbol for the protective earth connection (PE)
	Symbol for the functional earth connection (FE)

2.5 Data, illustrations, changes

All data, texts and illustrations have been compiled to the best of our knowledge and belief. They do not constitute a guarantee of properties. Despite the greatest possible care, no liability can be accepted for accuracy, completeness and timeliness. We reserve the right to make changes.

2.6 Trademarks

Please note that the software and hardware designations and brand names of the respective companies used in this documentation are subject to general trademark protection.
Big-LinX® and X-Remote® are registered trademarks of ADS-TEC.
All other trademarks used are hereby acknowledged.
ADS-TEC reserves the right to assert all rights in the event of a violation of trademark rights.

2.7 Copyright

This operating manual is protected by copyright. The authorised user has a simple right of use within the scope of the purpose of the contract. Any modified use or exploitation of the content provided, in particular the reproduction, modification or publication of any kind, is only permitted with the prior consent of ADS-TEC.
ADS-TEC reserves the right to assert all rights in the event of a violation of copyright.

2.8 Conformity

The manufacturer hereby declares that, in accordance with the essential requirements and other relevant provisions of the following European Directives, the CE mark has been affixed to this device:

- 2011/65/EU RoHS Directive
- 2014/30/EU EMC Directive (only devices without radio)
- 2014/53/EU RED Directive (only devices with radio)
- 2014/35/EU Low Voltage Directive
- EC 1907/2006 REACH Regulation

The following applies with regard to electromagnetic compatibility: The device is a **Class A** device (industrial sector).

The EU Declaration of Conformity is available for download at https://www.ads-tec-iit.com/support/eu-konformitaetserklaerung.

Recommendation for use:
To comply with the legal EMC requirements, the connected components and cable connections must also meet these requirements. Shielded bus and LAN cables with shielded connectors must therefore be used and installed in accordance with the instructions in the operating manual.

Devices with a **DNV** logo on the type plate
meet the following requirements:

- DNV rules for classification – Ships
- IEC 60945 Ed. 4 (2002-08) Maritime navigation and radiocommunication equipment and systems – General requirements – Methods of testing and required test results
- E10

Areas of application:
Temperature: B; Humidity: B; Vibration: A; EMC: B; Housing/control cabinet: The device must be protected in accordance with DNV rules when installed on board.

ATTENTION

High-frequency fields can interfere with the functioning of compasses!

- Observe the required **minimum distance** between the device and compasses:
  - Safety distance from magnetic control compass: 0.40 m
  - Protective distance from magnetic steering compass: 0.30 m
  - Reduced protective distance from magnetic control compass: 0.30 m
  - Reduced protective distance from magnetic steering compass: 0.30 m

3 Operating/safety instructions

The device contains electrical voltages and highly sensitive components. The user is only permitted to connect the connection cables. If further changes are to be made, the manufacturer or a service centre authorised by the manufacturer must be consulted. The device must be disconnected from the power supply during work. Suitable measures must be taken to prevent electrostatic discharge to components. If the device is opened by an unauthorised person, this may result in danger to the user and the warranty claim will be void.

General information

Installation, commissioning and operation must only be carried out by trained and qualified personnel.

The safety instructions and operating instructions must be observed by all persons working with the device.

The applicable rules and regulations for accident prevention must be observed at the place of use of the device

The operating instructions contain the most important information for operating the device safely.

To ensure safe and proper operation of the device, proper storage, transport, installation and commissioning as well as careful operation are required

3.1 Safety instructions

ATTENTION

Cables (power supply, interface cables) must only be connected when the device is switched off to prevent damage to the device.

CAUTION

Installation work on the device is only permitted when it is secured and disconnected from the power supply.

→ **Recommendation for use**:
When handling components that are susceptible to electrostatic discharge, observe the relevant safety measures (DIN EN 61340-5-1 / DIN EN 61340-5-2).

3.2 Operating location

The device is designed for maritime use. Ensure that the specified environmental conditions are observed. Use in non-specified environments, e.g. in potentially explosive areas or at extreme altitudes, is prohibited.

CAUTION

Damage caused by condensation
To avoid short circuits and malfunctions due to condensation, the device must only be switched on after it has adjusted to the specified ambient temperature. The same applies if the device has been exposed to extreme temperature fluctuations.

Damage caused by heat
→ Do not expose the device to direct sunlight or other sources of light or heat.

3.3 Damage caused by improper use

If the operating system shows obvious damage caused by incorrect operating/storage conditions or improper handling, the device must be shut down immediately and secured against accidental start-up.

3.4 Warranty / Repair

During the warranty period, repairs may only be carried out by the manufacturer or by persons authorised by the manufacturer.

3.5 Intended use

The device was specially developed for IT security in machines and systems and for secure remote maintenance via the Internet.

The Industrial Firewall is designed for the following areas of application:

- Remote maintenance, NAT router, mobile phone router, machine firewall, Gigabit router.

The device must only be assembled, installed and operated within the permissible specifications. Use in unspecified environments is prohibited.

3.6 Improper use

Any use of the device other than that described or beyond the scope of the intended use is considered improper use.

The device must not be used to control vehicles or for applications for which further approvals beyond the manufacturer's declaration are required, e.g. Ex areas or medical technology. Use for payment services is excluded. Use by private individuals is considered improper.

The device must not be put into operation if it has been damaged during transport or if the specifications have not been complied with, and must be taken out of operation if the conditions change.

In the event of improper use, ADS-TEC accepts no responsibility or liability for personal injury or property damage resulting directly or indirectly from the use of the device. If the device shows obvious damage caused by, for example, incorrect operating/storage conditions or improper handling, it must be shut down immediately and protected against unintentional start-up.

3.7 Network environment and services

ATTENTION

Security risks arising from the use of certain services in unsecure networks

- Please observe the following notes.

This device supports a variety of optional network services and special functions that are disabled by default. Some of these functions are not secure against attacks from the public Internet in their default configuration. These include, among others:

- USBIP Device Server (TCP 3240)
- gpsd service (TCP 2947)
- RIP v2 (UDP 520) and OSPF (IP Proto 89)
- Modbus/TCP server
- DNS Proxy (UDP 53)
- SMS communication interfaces
- Virtual COM port services (TCP 3001/20000)
- Debug and diagnostic services such as rpcap and SSH (port 22)

Purpose of these services

These services are intended for use in controlled, trusted networks only. This usually means that they should be used:

- behind an active and fully configured firewall,
- via a secure VPN (e.g. IPsec, OpenVPN, Big-LinX),
- or in completely isolated networks (e.g. workshop networks, commissioning environments).

No use on the public Internet

Activating these functions in unsecured or publicly accessible networks poses a significant security risk. This can result in unauthorised access, data leaks or remote control by attackers. This contradicts the requirements of EN 18031-1:2024.

Recommendations for safe use

If you still require these functions, please observe the following security measures:

1. Secure via VPN or tunnel: Use IPsec or OpenVPN.
2. Access protection: Use strong authentication methods.
3. Network segmentation: Isolate services with potentially weak security.
4. Firewall restrictions: Restrict IP ranges and ports.
5. Logging: Enable audit and log functions for monitoring.
6. Access restriction: Restrict access to authorised network participants.

Configuration notes

These features are activated and configured via the configuration web interface or APIs.

3.8 Protection of hardware interfaces

The device has several physical interfaces that do not have integrated authentication or access control mechanisms. These interfaces represent potential access points for unauthorised physical attacks and must be protected against tampering.

Risk assessment per hardware interface

Interface	Risk	Impact
USB ports	Connection of unauthorised devices (e.g. keyloggers, malware sticks)	Introduction of malware, data exfiltration
Reset button (factory default)	Reset to insecure factory settings	Loss of secure configuration, removal of access controls
Serial and digital I/O interfaces	Direct access to internal control signals	Control manipulation, unintentional triggering of functions
Smart card slot	Access to cryptographic keys or identities	Identity theft, misuse of authentication

These interfaces must be secured during installation and commissioning, e.g. as follows:

- Place the device in a secure control cabinet or server cabinet that is only accessible to authorised persons
- Physical protection of connections with mechanical locks ("port blockers")

3.9 Overview of available network interfaces

In addition to the physical interfaces mentioned above, the device has several network interfaces. The configuration described below corresponds to the factory default settings and is relevant for safe operation and network integration.

Interface	Affiliation	Behaviour in factory setting	Default IP address	DHCP	Packet forwarding
ETH1	Single port	Separate, not connected to ETH2–ETH4. DHCP enabled. No IP forwarding in commissioning mode	None (DHCP client)	Yes	No
ETH2 – ETH4	Internal switch network	Connected as **an** internal **Ethernet switch. Passes all data traffic**, even in factory settings. Optionally configurable with packet filters	**192.168.0.254** (fixed)	No	Yes (switch)

Notes

- ETH2 to ETH4 behave like a Layer 2 switch without routing function. There is no isolation between the ports.
- ETH1 is physically and logically isolated from ETH2–ETH4, which enables a secure initial configuration in commissioning mode.
- The behaviour can be modified by activating routing or firewall functions. These functions are not active in the factory settings.
- All Ethernet ports are **physically accessible** and must be secured or documented accordingly as part of a risk analysis.

3.10 Packet filter rules

The device has an integrated packet filter engine with support for Layer 2 (Ethernet/MAC-based) and Layer 3 (IP-based) **packet filter rules**. These filters are a central component of network access control and enable granular control over incoming and outgoing data streams.

Supported filter mechanisms:

- Layer 2 filters (Ethernet):
  - MAC address-based filtering (e.g., discard all frames except those from specific sources)
- Layer 3 filters (IP):
  - IP addresses, subnets, protocols and ports (TCP/UDP)
  - Policies for incoming and outgoing packets

Operating modes:
The packet filters can be operated in two basic modes:

- **Whitelist mode ("Block All"):** Only explicitly permitted packets are allowed through. Everything else is discarded.
- **Blacklist mode ("Allow All"):** By default, all data traffic is allowed; specific rules can block individual packets.

Factory settings

Filter type	Mode (default)	Description
Layer 2 filter	**Allow All**	No restrictions at MAC level active
Layer 3 filter	-	In start-up mode, no packets are forwarded (drop all). An operating mode must be selected.

3.11 Protection of sensitive data

Data stored on the device, such as

- cryptographic keys
- passwords, certificates
- configuration parameters with security functions

are currently not protected against modification or theft, as no secure storage methods in accordance with EN 18031-1 Section 6.4 have been implemented.

This requires the following measures:

1. **Physical environment security**: Sensitive data may only be generated, stored and used on the device if it is located in a physically protected environment (e.g. locked control cabinet, access control, video surveillance).
2. **Measures in the event of theft**: If the device is lost, it must be assumed that all passwords, certificates, keys, etc. have been compromised. They must therefore be blocked or withdrawn immediately (e.g. revoke certificates, assign new keys).
3. **Device parameterisation only at the place of use**: Configuration data may only be transferred to the device at its final place of use. Pre-loading during storage or transport is not permitted. For downstream remote communication, especially via HTTPS, it is strongly recommended to use an organisation-specific certificate. The factory-set device certificate should be replaced with your own trusted certificate to ensure the integrity and authenticity of the communication.
4. **Security seal check**: Each device is provided with a security seal by the manufacturer. This seal serves as proof of tampering and must be visually checked by the customer for integrity during initial commissioning and at regular intervals.

3.12 Mobile communications and cyber security

ATTENTION

Security risks in unsecure networks

The mobile connection of the device via the optionally integrated modem is a publicly accessible network connection and is therefore not considered trustworthy within the meaning of EN 18031-1:2024.

- Please observe the following notes.

Mandatory requirement

For secure operation via mobile communications or other wide area connections (e.g. also for Internet uplink via Ethernet), the use of an additional secure communication mechanism is mandatory.
Permissible measures are:

- VPN connections, e.g. via the ADS-TEC Big-LinX© service
- OpenVPN or IPsec-based tunnels through the device
- Use of mutual TLS/HTTPS for direct communication between the end devices, independent of the ADS-TEC device

Special note for customer data

The device provides its own web interfaces (e.g. the configuration interface) exclusively via HTTPS with a valid certificate. However, it is the responsibility of the operator to ensure the confidentiality and integrity of the data traffic transmitted (e.g. from connected machines or sensors).
Further recommended measures:

- Use of a private APN (Access Point Name) to disconnect the device from the public Internet
- Provision of traffic filtering and IP whitelisting via the private APN by the mobile network provider to effectively prevent unauthorised access and denial-of-service attacks.
- If using the SMS service, it is recommended to also protect this service with a private APN

3.13 Safety information on mobile communications

⚠ **WARNING**

Radio interference could have unpredictable effects in certain environments!

- The wireless card must NOT be operated in the following environments:
  – near medical and life-saving equipment,
  – in explosive atmospheres (e.g. near fuel depots or chemical plants),
  – near blasting operations.
- Switch the device OFF in these environments and secure it against accidental start-up.

⚠ **WARNING**

Communication via radio connections cannot be guaranteed.

- The device must not be used for applications in which people or objects could be harmed due to a malfunction of the radio connection.

⚠ **WARNING**

Danger from lightning strikes when installing antennas in exposed locations!

- Check whether lightning protection is required at the installation site (protection against direct lightning strikes and protection against induced voltages from distant lightning strikes).

⚠ **WARNING**

Electromagnetic radiation may be hazardous to health.

- In accordance with the requirements of the American Federal Communications Commission (FCC) and ISED (Industry Canada), maintain a minimum distance of 20 cm between the transmitting antennas and people.

⚠ WARNING

Radio interference and possible health hazards due to exceeding the permissible transmission power!

When using directional antennas with high antenna gain, the maximum permissible field strength may be exceeded.

- Observe the **maximum permissible signal strength (EIRP)** in accordance with national or local regulations (see calculation example for EIRP).
- Observe the regulations and standards applicable at the installation site (e.g. the standards for antenna installation VDE 0855 and for lightning protection VDE 0185-305).
- Have antenna systems planned, installed and approved exclusively by qualified electrical engineers.
- When operating in North America, the **antenna gain** (including line losses) must not exceed the following values in accordance with the specifications of the US Federal Communications Commission (FCC) and the Canadian ISED (Industry Canada):

LTE	
Band 2 (1850–1910 MHz)	6 dBi
Band 4 (1710–1755 MHz)	6 dBi
Band 5 (824–849 MHz)	6 dBi
Band 7 (2500–2570 MHz)	9 dBi
Band 12 (699–716 MHz)	6 dBi
Band 13 (777–787 MHz)	6 dBi
Band 25 (1850–1915 MHz)	6 dBi
Band 26 (814–849 MHz)	6 dBi
Band 30 (2305–2315 MHz)	1 dBi (external vehicle antennas not permitted!)
Band 41 (2496–2690 MHz)	9 dBi
UMTS	
Band 2 (1850–1910 MHz)	6 dBi
Band 4 (1710–1755 MHz)	6 dBi
Band 5 (824–849 MHz)	6 dBi

3.14 Calculation example for transmission power (EIRP)

$$\mathrm{EIRP} = P_{out} - C_{loss} + \mathrm{Ant}_{gain} = 22\ \mathrm{dBm} - 8\ \mathrm{dB} + 9\ \mathrm{dBi} = 23\ \mathrm{dBm}\ (\triangleq 200\ \mathrm{mW})$$

EIRP = Equivalent Isotropically Radiated Power

$P_{(out)}$ = transmission power of the radio card

$C_{(loss)}$ = Losses due to attenuation in coaxial cable and connectors

$\mathrm{Ant}_{(gain)}$ = Antenna gain

3.15 Protection against electrostatic discharge

ATTENTION

Damage caused by electrostatic discharge

Electrostatic discharge can cause damage to the device.

- When handling components that are susceptible to electrostatic discharge, observe the relevant safety measures (e.g. DIN EN 61340-5-1 / DIN EN 61340-5-2).
- Installation/service work on the device is only permitted when it is secured and de-energised.

4 Introduction

The Industrial Firewall is the link between the IT world and automation and meets the requirements of both IT security and maintenance personnel in production. It can be used to control the network and access to it. An essential protective mechanism is situation-dependent and physical network separation. It also offers secure access for service purposes, among other things.

4.1 Equipment variants / nomenclature

Example:

DVG -	**IRF3421**	**050 -**	**AA /**	**AF01**
A	**B**	**C**	**D**	**E**

A: Device with software

B: Model: IRF3 = Industrial Router and Firewall, third generation

IRF34xx: Device with 4 x LAN

IRF3401: Device without wireless card (LTE)

IRF3421: Device with wireless card (LTE)

C: Configuration

Numbers 001 … 099: Standard variants from the manufacturer

Example: 050 = variant with DNV certification for shipping

Numbers 100 … 899: Customer and application-specific variants

Numbers 900 … 999: Sample devices (e.g. for testing purposes)

D: Operating system: Letters AA … ZZ

E: Exact specification of the parts list version and software configuration

4.2 Event log

If the firewall is not disconnected from the power supply, an event log stores all events. The event log can be read both locally and via a central syslog server.

4.3 Mobile modem (optional)

The integrated LTE modem enables mobile connections.

4.4 Scope

Check the contents of the package for completeness and damage:

> **Scope of delivery**
>
> 1 x Industrial Router & Firewall Type IRF34x1
>
> 1 x 4-pin plug for power supply
>
> 1 x 3-pin plug for Modbus RTU
>
> 1 x 4-pin plug (grey) for digital I/Os No. 2
>
> 1 x 8-pin plug for digital I/Os No. 3…5
>
> 1 x quick start guide
>
> Optional: 2 x mobile phone antenna
>
> Optional accessories: 1 x VESA adapter plate

4.5 Environmental conditions

The device can be operated under the following conditions. Failure to comply with these specifications will void the warranty. See section "8 " in the technical data.

ADS-TEC is not liable for damage caused by incorrect operating conditions.

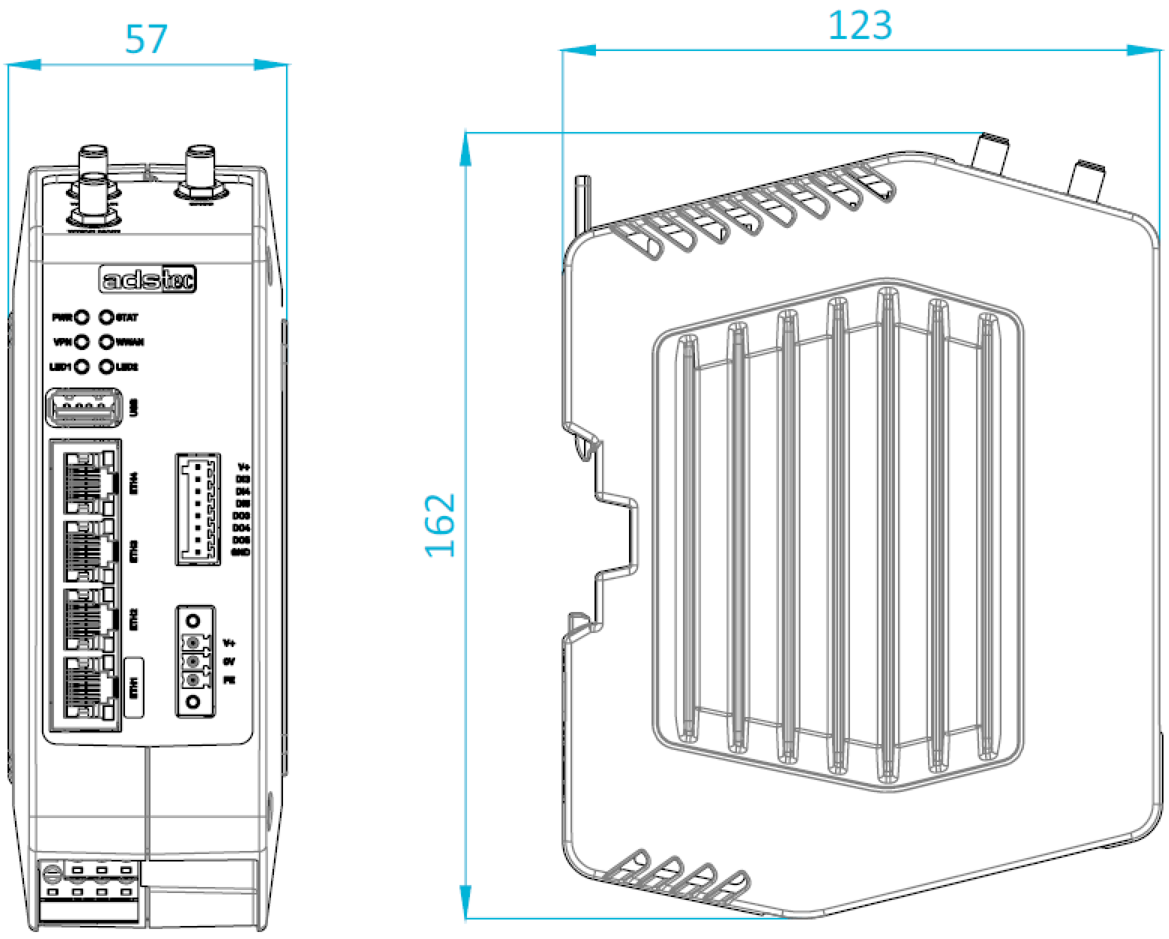
The following temperature specifications apply to an operating altitude of max. 2000 m:

Ambient temperature	
during operation	-30 ... +70 °C
during storage	-40 ... +85 °C
Humidity	
During operation	5 … 90 % without condensation
During storage	5 … 90 % without condensation

5 Installation

5.1 External dimensions

The images show the version with connections for radio antennas.



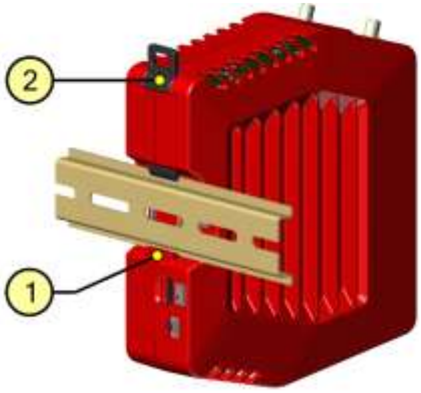
5.2 Top-hat rail mounting

1. Place the IRF at an angle on the top-hat rail from below (1).

2. Pull the DIN rail lock (2) upwards with a screwdriver, press the device against the top of the DIN rail and remove the screwdriver.

3. The top-hat rail lock springs back to its original position.

4. Check that the IRF is securely seated on the top-hat rail.

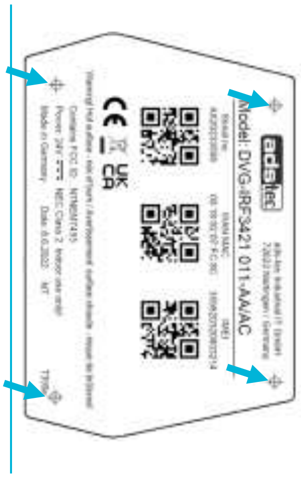


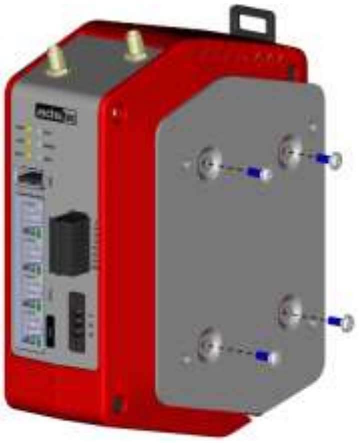
To remove the device from the DIN rail, proceed in reverse order.

When removing, take care not to damage the device's top-hat rail adapter.

5.3 Screw on the VESA adapter plate

The VESA adapter plate, available as an accessory, can be screwed directly onto the device label using the screws supplied. The positions of the screw holes are marked with target crosses (⌖) on the label.





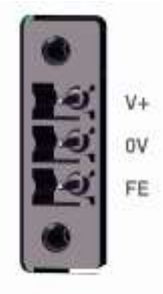
5.4 Optional: Connecting antennas

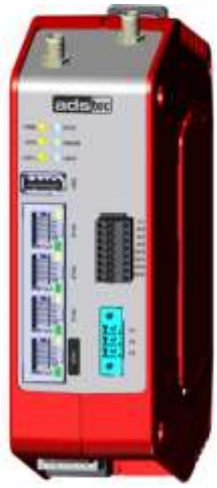
- Screw the mobile antennas directly or via SMA extension cables to the antenna connections (WWAN AUX/MAIN).

6 Electrical interfaces

6.1 Power supply

Pin	Signal
FE	⏚ Functional earth (required for EMC)
0	Reference potential 0 V
V	Supply voltage +24 VDC ± 20%



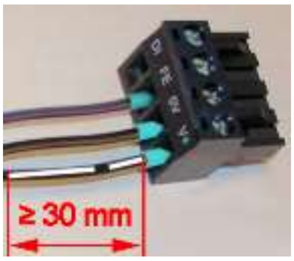


Requirements for the power supply

The following requirements also apply to the operation of the digital inputs and outputs:

- Power supply compliance:
  - Class PS2 according to IEC 62368-1 *or*
  - Limited Power Source (LPS) according to IEC 60950-1 *or*
  - NEC Class 2
- Voltage: 24 VDC ± 20%
- Short-circuit current:< 8 A

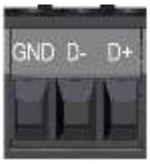
Recommended application:
Use flexible cables with a wire cross-section of 0.5 mm² / AWG20 and appropriate ferrules. To keep the mechanical stress on the individual wires and the connector to a minimum, the distance between the sheathing and the connector should be at least 30 mm.



6.2 Modbus RTU (RS-485)

The fieldbus node is galvanically isolated from the IRF electronics. Its electrical bus load is 1/8 unit (unit load = 1/8; impedance: 96 kΩ).

Pin	Signal
GND	Reference potential (common) for the data signals
D	Inverted data signal
D	Non-inverted data signal

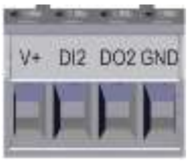


Recommendation:
If the device is located at a bus end, a 120 Ω terminating resistor must be attached to the plug between D- and D+ (e.g. a wire resistor covered with heat-shrink tubing).

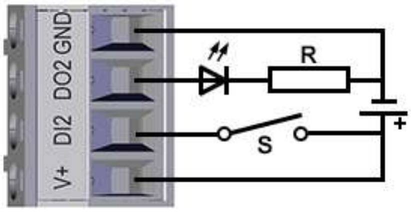
6.3 Digital I/O No. 2

When operating the digital I/O, the requirements for the voltage supply specified in section "6.1 " must be observed.

Pin	Signal
V	Power supply +24 VDC ±20%
DI2	Digital input no. 2
DO2	Digital output no. 2
GND	Reference potential



Principle circuit diagram:

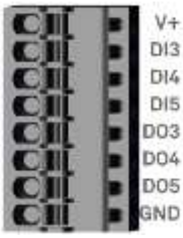


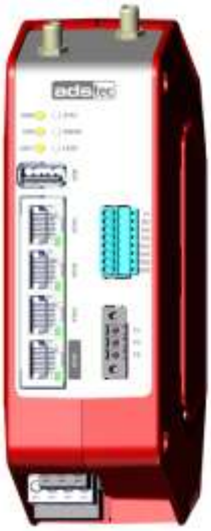
6.4 Digital I/O No. 3…5

When operating the digital I/O, the requirements for the voltage supply must be observed in accordance with section "6.1 ".

Schematic diagram: see section 6.3

Pin	Signal
V+	Voltage supply +24 VDC ±20%
DIx	Digital input no. 3…5
DOx	Digital output no. 3…5
GND	Reference potential



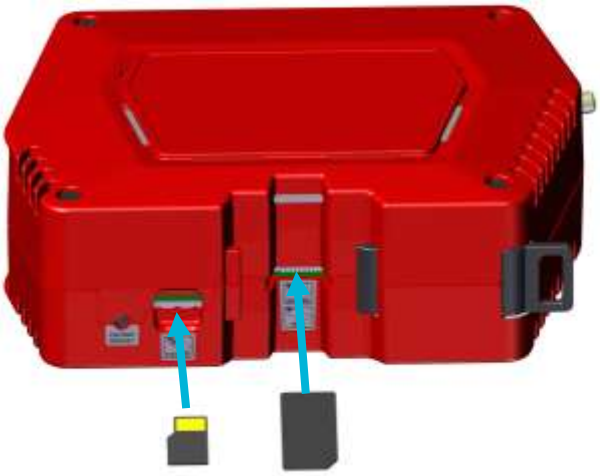


6.5 Smartcard reader and slot for SIM card

SIM cards and smart cards (SC) in ID-000 format according to ISO 7816 (25x15 mm) can be used.

- The **SIM card** for mobile communications must be inserted **in the lower slot** (SIM1).
- The **smart card** is intended for **backing up configuration data** or for connecting to **Big-LinX**® and must be inserted in the upper slot (SC/SIM2).
- You can insert a **microSD card** with up to 2048 GB as **memory expansion** into the left slot.

Insert the cards in the orientation shown:



→ The **configuration data** of a device can be stored on the smart card. In the event of a service call, the stored configuration can be transferred to the new device. No new setup is required.

→ Complex IT infrastructures with a large number of devices can be conveniently managed, monitored and controlled via **Big-LinX**® . Further information about Big-LinX is available here: https://www.ads-tec-iit.com/sicherer-fernzugriff-iiot-loesungen/biglinx

7 Commissioning

7.1 Connect device to a PC

Supply power to the device: see section 6.1 Power supply.

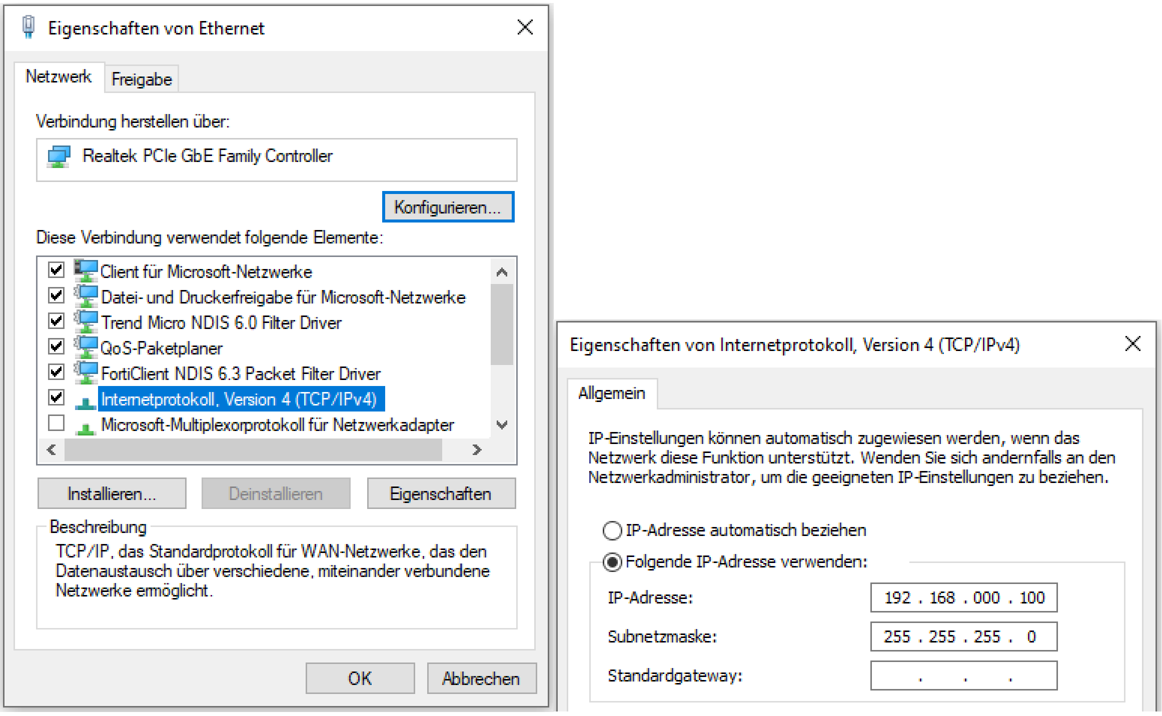
Connect the **ETH2** port to a PC using a **patch cable**.
(Note: A DHCP client runs on ETH1 by default.)

7.2 Configuring the PC's network adapter

Recommended use:
The procedure described below was created using Microsoft Windows as an example. If you are using a different operating system, the paths and properties described here may vary.

On your PC: Open the properties card for the network adapter you are using and enter the following:

- **IP address: 192.168.0.100** (The last number of the IP address must be a number between 1 and 253, e.g. "100".)
- **Subnet mask: 255.255.255.0** (Some input masks require the short notation **/24** instead).



Eigenschaften von Ethernet

Netzwerk | Freigabe

Verbindung herstellen über:
Realtek PCIe GbE Family Controller

Diese Verbindung verwendet folgende Elemente:
☑ Client für Microsoft-Netzwerke
☑ Datei- und Druckerfreigabe für Microsoft-Netzwerke
☑ Trend Micro NDIS 6.0 Filter Driver
☑ QoS-Paketplaner
☑ FortiClient NDIS 6.3 Packet Filter Driver
☑ Internetprotokoll, Version 4 (TCP/IPv4)
□ Microsoft-Multiplexorprotokoll für Netzwerkadapter

Beschreibung
TCP/IP, das Standardprotokoll für WAN-Netzwerke, das den Datenaustausch über verschiedene, miteinander verbundene Netzwerke ermöglicht.

Eigenschaften von Internetprotokoll, Version 4 (TCP/IPv4)

Allgemein

IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.

○ IP-Adresse automatisch beziehen
● Folgende IP-Adresse verwenden:
IP-Adresse: 192 . 168 . 000 . 100
Subnetzmaske: 255 . 255 . 255 . 0
Standardgateway: . . .

Confirm your entries with **OK.**

7.3 Calling up the device web interface

Application recommendation:

The device's web interface has been optimised for **Mozilla Firefox**.

Functional restrictions may apply when using other browsers.

Start your web browser and enter the following in the address bar of the browser:

http://192.168.0.254

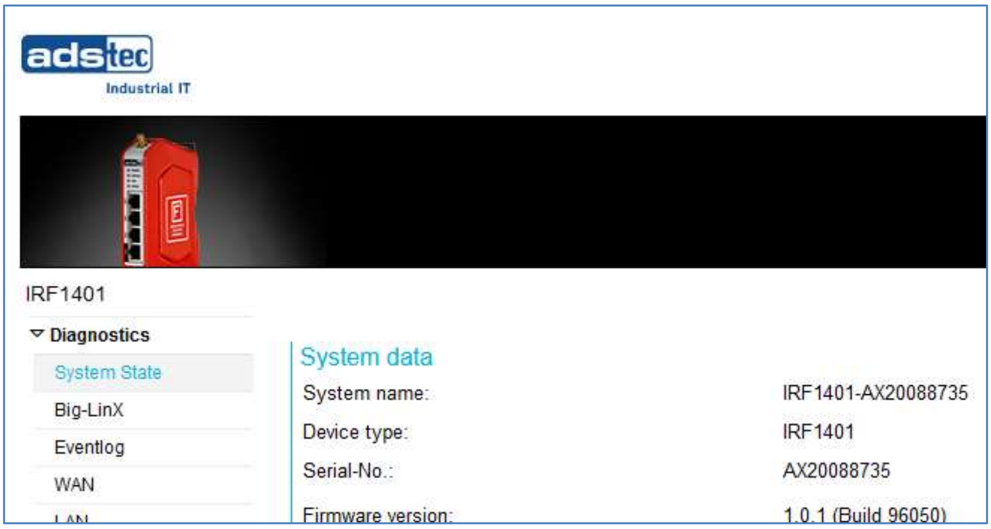
Confirm with **Enter.**

The login prompt will then appear. The default login details are:

Username:	**admin**
Password:	**admin**

Confirm your entries with **OK**.

The device's web interface will open:



System data

System name: IRF1401-AX20088735

Device type: IRF1401

Serial-No.: AX20088735

Firmware version: 1.0.1 (Build 96050)

Tip:

If you cannot establish a connection, check your proxy and firewall settings. Local subnet addresses (e.g. 192.168.x.x) are often redirected to a proxy server.

In this case, select the option "Bypass proxy server for local addresses" and enter the affected address spaces.

Follow the instructions in the start-up wizard.

Startup mode

During this initial configuration, the device is in a special commissioning mode. Certain functions and interfaces of the device are specifically restricted or specially configured to ensure that security-critical configuration steps are implemented and to prevent unauthorised access.

- In commissioning mode, **the device does not route network packets** between network interfaces. This prevents unintended communication between, for example, WAN and LAN.
- The **ads-tec Discovery Tool** is only fully functional in commissioning mode. It allows you to **set the IP address** and detect devices in the network.

After completion of commissioning mode, i.e. in normal operation, the firmware prevents

- prevents the setting of IP addresses
- and API calls that require authentication (e.g. password changes).

ADS-TEC Discovery Tools

The ADS-TEC Discovery Tool uses a special Ethernet protocol with the EtherType number 0x890E. This software interface is activated by the system and **cannot be deactivated**.

Access options

The functionality of this interface is divided as follows:

Commissioning mode

In commissioning mode, device settings and system parameters can be **read** and **changed** via this interface. Access requires the entry of a **valid user name and password**.

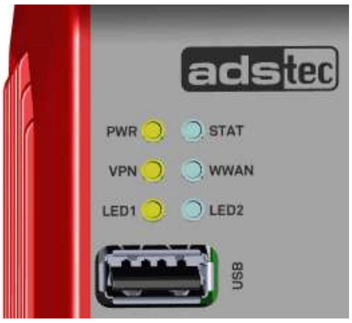
After commissioning (normal operation)

Access via this interface is also possible in normal operating mode. However, only **read access** to **the** following **information classified** as **public** is permitted **without a password**:

- Serial
- MAC address
- Hardware unique fingerprint
- Factory default configuration fingerprint

7.4 Front LEDs

	Signal	Action
PWR (Power)	□	The device is not powered.
	◧	Power has been switched on, device is booting. LED flashes slowly (1 Hz).
	◧	Firmware is being updated. LED flashes quickly (5 Hz).
	🟩	The device is ready for operation.
STAT (Status)	□	The device is not powered.
	◧	Device in commissioning mode
	🟥	Error during boot process / recovery image
VPN	□	No VPN tunnel is active.
	🟩	The tunnel activated via VPN key is active.
WWAN	□	No mobile connection is active.
	◩	Network search (1 Hz)
	◩	Registration rejected (2 Hz)
	◩	Firmware update of the radio module (5 Hz)
	🟧	Logged in, offline
	◧	Logged in, standby (dial on demand)
	🟩	Logged in, online



Legend:

LED status	Display
Off	□
Green	🟩
Flashing green	◧
Lights up red	🟥
Orange light	🟧
Flashing orange	◩

7.5 Operating mode-dependent LED indicators

7.5.1 Boot process

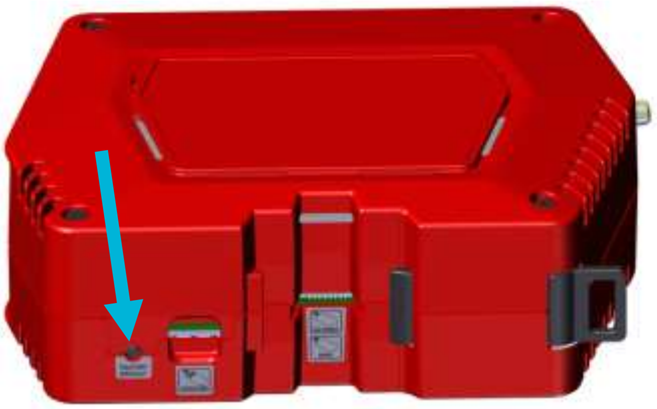
The boot process begins as soon as the device is supplied with power. The PWR LED flashes slowly.

7.5.2 Initial

During initial commissioning, the device is initially in a special commissioning mode until the required minimum configurations have been completed. During this time, the status LED flashes green (long – long – off).

7.5.3 Resetting to default settings

The firewall can be reset to the default settings at any time using the **Factory Default** button.



To do this, press the Factory Default button <u>before</u> the boot process and hold it down for approx. 10 seconds during the boot process. The PWR LED flashes rapidly when the device is reset to factory settings. As soon as the PWR LED lights up continuously, the web interface is accessible again.

7.5.4 Firmware update

A firmware update can be performed via the web interface.

- During a firmware update of **the firewall**, the **PWR LED** flashes rapidly. The actual update process takes a few minutes. After the update process has been completed successfully, initialisation begins. During this process, the PWR LED flashes slowly.
- During a firmware update of **the mobile radio module**, the WWAN LED flashes yellow at a frequency of 5 Hz.

8 Technical

Operating system	Embedded Linux
Hardware	ARM, 64 bit, 4 x 1.6 GHz; 4 GB RAM; 8 GB Flash
Interfaces	Ethernet: 4 x 1 Gbit/s 1 x USB 1 x ModbusRTU (RS485, half-duplex) 1 x slot for smart card 1 x slot for radio card (SIM) 1 x slot for microSD memory expansion (UHS II) With optional radio card: 2 x SMA antenna connection Digital inputs and outputs (I/O): 4E / 4A
VPN	Big-LinX, OpenVPN, IPSec
Firewall operating modes	IP router (two subnets); IP router extended (up to eight subnets); transparent bridge
Wireless (WWAN)	Optional: EMEA + US
External dimensions	See dimensional drawings in chapter 5
Weight	Approx. 0.8 kg
Protection	IP20 (tested by ADS-TEC, not verified by UL)
Overvoltage	Voltage resistant up to 800 V
Contamination	Degree of contamination 2 according to IEC 61010-1
Power supply	The supply voltage is galvanically isolated from the device's electronics via a DC-DC converter. Voltage: 24 VDC ± 20% Requirements for the power supply unit: • Class PS2 according to IEC 62368-1 *– or –* Limited Power Source (LPS) according to IEC 60950-1 • Short-circuit current: < 8 A • For devices with UL approval: NEC Class 2
Current consumption (in normal operation)	DVG-IRF3401: max. 1.3 A DVG-IRF3421: max. 1.5 A
Ambient temperatures	during operation -30 ... +70 °C Storage -40 ... +85 °C
Operating altitude	max. 2000 m

9 Service & Support

ADS-TEC and its partner companies offer their customers comprehensive service and support, providing fast and competent assistance with all questions relating to ADS-TEC products and assemblies.

As ADS-TEC devices are also used by partner companies, these devices may be configured to customer specifications. If you have any questions about these special configurations and software installations, please contact the company that supplied the device.

No support is provided for devices that were not purchased directly from ADS-TEC. In this case, support will be provided by our partner company.

9.1 ADS-TEC Support

The ADS-TEC support team is available to direct customers from Monday to Friday from

8:30 a.m. to 5:00 p.m. at the telephone number listed below:

Tel: +49 7022 2522-202

Email: support.iit@ads-tec.de

9.2 Company address

ads-tec Industrial IT GmbH

Heinrich-Hertz-Str.1

72622 Nürtingen

Germany

Tel +49 7022 2522

Email mailbox@ads-tec.de

Home: www.ads-tec-iit.com