Ads-tec-Industrial IT GmbH

IRF1421, IRF3421 and IRF3821

Application Note – RED (EN18031-1)
Product Changes Beginning with Version 2.2.x

© *Copyright* 2025

Contents

1 Introduction 3
1.1 RED Overview 3
2 Software Related Changes 3
2.2 New Features starting with version 2.2.x 3
2.2 Removed Features as of version 2.2.x 4
2.4 Downgrading of Firmware 2.2.x 4
3 Hardware Related Changes 5
3.5 Packaging 5
3.6 User Manual 5
4 Current Security Advisories 5
5 History 5

© *Copyright* 2025

1 Introduction

1.1 RED Overview

As of August 1, 2025, compliance with the new Radio Equipment Directive (RED), specifically "BS EN 18031-1_2024", will be mandatory for the ADS-TEC IRF1000 and IRF3000 product series. This directive enhances cybersecurity for wireless devices and directly impacts ADS-TEC firewall products equipped with LTE modules. It imposes strict requirements to mitigate cybersecurity threats, including the prohibition of insecure access methods to ensure secure network operation and data protection.

ADS-TEC will introduce all security improvements for the non-LTE version of the products series as well!

2 Software Related Changes

2.2 New Features starting with version 2.2.x

Commissioning Mode

Commissioning Mode Commissioning Mode is a special operational state intended for devices in their factory default configuration.

In this mode, the device's Status LED blinks, signaling that mandatory initial security settings are pending. To proceed with regular operation, the user must:

- Replace the factory default password with a secure, custom password.
- Configure the default packet filter behavior (either Drop or Allow).

While the device is in commissioning mode, IP routing is disabled. These two conditions must be met to exit commissioning mode and transition the device into normal operation. Once fulfilled, the Status LED stops blinking, indicating that commissioning is complete.

Additionally, the ADS-TEC Detection Tool can be used during this mode to modify the device's default IP address. However, any password-protected actions using the ADS-TEC Detection Tool or its underlying API (adsdp) are permanently blocked once commissioning mode is exited.

Login Ban

Within the factory default settings of the device, the login ban function is enabled. This can be individually configured under User Accounts → Security.

By default, after 10 incorrect password attempts, logins from the originating IP address will be blocked for 60 seconds.

© *Copyright* 2025

2.2 Removed Features as of version 2.2.x

The following functions have been removed for RED compliance:

- SNMPv2, only SNMPv3 remains (all devices)
- The ADS-TEC HTTP classic API based on MD5 Passwords can no longer be enabled (only removed for devices with LTE modules)

2.3 Restricted Features Starting from Version 2.2.x

Beginning with firmware version 2.2.x, several interfaces and services are now restricted to operation under secure conditions. New Interface Filters have been introduced to allow our users to enforce these limitations. For detailed configuration instructions, please refer to the updated product manual.

These features are disabled by default. If you're upgrading existing installations or using preconfigured configuration files, make sure they are adapted accordingly and make sure you have them disabled on interfaces which are exposed to public Internet or untrusted networks.

These following services must now only be used within secure intranets or over protected VPN channels:

- Modbus/TCP Interface – for example, when used to control VPN services.
- NTP Server – restricted to trusted internal networks.
- Dynamic Routing Protocols – including RIPv2 (UDP 520) and OSPF (IP Protocol 89).
- Remote Packet Capture
- USBIP Device Server – typically accessed via TCP port 3240.
- GPS Daemon (gpsd) – accessed via TCP port 2947.
- DNS Proxy – UDP port 53.
- Virtual COM Port Services – including TCP ports 3001 and 20000.
- SMS Communication Interface – if used, ensure it is secured via private APN services that prevent exposure to public telephone networks.

2.4 Downgrading of Firmware 2.2.x

Compliance Firmware version 2.2.x is the first RED-compliant release for the IRF1421, IRF3421 and IRF3821 series. All LTE devices shipped on or after August 1, 2025, must be delivered with firmware version 2.2.x or later. Devices delivered before this date are not affected by this requirement.

Due to technical constraints all devices with LTE option shipped before August 1, 2025 and which might get updated to versions > 2.2.x cannot be downgraded to older versions as well! Non-LTE variants can still be downgraded to earlier versions.

© *Copyright* 2025

3 Hardware Related Changes

3.5 Packaging

All delivered devices will include a tamper detection seal on the packaging starting from August 1, 2025.

3.6 User Manual

Feel free to visit our website to download the latest full user manual which contains all relevant information.

4 Current Security Advisories

We place the highest quality standards on our products and services. Our Product Security Incident Response Team (PSIRT) continuously monitors product security. Through our partner CERT@VDE, we inform you about any potential security-related vulnerabilities.

All Security Related Updates will be publicly published at:

https://certvde.com/de/advisories/vendor/ads-tec-iit/

5 Document History

Version	Date	Content	Author
V 1.0	31.07.2025	First document version	SiSm
V1.1	31.07.2025	Review	SnPr

© *Copyright* 2025