

ads-tec Industrial IT GmbH

IRF1000 Firmware Release Documentation

SW-IM-00001243 01/DB | 2.3.1 rev-a | 186119

Generated

2026-07-17 05:30

1 Current Changelog for version 2.3.1

1.1 Major New Features

Ticket	Description
#59898	Extensive Security Hardening according to ADS-TEC IIT's certified IEC62443 4-1 process
#58830	The Web Interface was refactored to improve Usability. Most notable his includes a new Startpage, Firmware Update Section and IPsec config page and many small details.
#58575	The WWAN connection monitor has been extended: - A second monitoring IP address can be configured. When both are set, the modem is only reset once both targets have been unreachable for the configured offline time. - The offline time until the modem is reset is now configurable in seconds (default: 60s). - Optionally, the Big-LinX WWH heartbeat can be used as an alternative criterion: the modem is reset if the heartbeat is unavailable for the configured offline time.

1.2 New Features

Ticket	Description
#59252	Added GCM cipher (AES-256-GCM) and EC Diffie-Hellman groups (ecp256, ecp384, ecp521, curve25519) to the IPsec configuration options for BSI TR-02102 compliance.
#58539	Improved IPsec configuration page: connection table is now directly editable and the page has been redesigned with an updated layout.
#58279	For Big-LinX VPN, enable WWHv3 as default protocol version in case of factory defaults. New primary server address is: ww2-we.aw-cp.de. Please update border firewalls which use whitelists to allow connections to the new service. WWHv3 can be enabled or disabled under Configuration -> VPN -> Big-LinX -> Additional settings. A migration to the new version is recommended. Software Updates will >not< change this setting automatically.
#58117	Added DHCP server support for PXE boot (UEFI x86_64) and NTP server distribution to DHCP clients.

1.3 Major Bug Fixes

Ticket	Description
#60038	Fixed Layout issues in the Paket Filter Web Wizard which got introduced with version 2.3.0

1.4 Bug Fixes

Ticket	Description
#60060	Fixed the SMS Service page layout (trap checkbox alignment and setting groups).
#59072	Fixed: LTE/WWAN connection passwords containing '?' and other special characters were rejected since firmware 2.2.7, preventing connections that worked in earlier firmware versions.
#58033	The Web Access page (Configuration → Access control → Web access) now warns you when you disable web access on the interface your current session is using. To apply such a change, you must explicitly confirm with a checkbox — preventing accidental lockouts.

1.5 Security Issues

Ticket	Description	Cert@VDE ID	CVE
#59809	A low privileged remote attacker can perform privileged configuration changes reserved for the administrator level including permission management due to incorrect authorization.	VDE-2026-076	CVE-2026-14167
#59782	Due to incorrect behavior order a low privileged remote attacker could trigger account inconsistent state via crafted input and overwrites existing user passwords which could result in complete administrative unavailability of the device.	VDE-2026-076	CVE-2026-14169
#59379	A low privileged remote attacker can gain administrator privileges due to missing authorization at the insert path of the configuration table resulting in gaining full system access.	VDE-2026-076	CVE-2026-14168
#59377	An unauthenticated remote attacker can abuse the improper validation of the post-login redirect of the web-UI to trick users to a malicious website. This can result in a loss of confidentiality and availability.	VDE-2026-076	CVE-2026-14171
#59276	CVE-2026-2291: dnsmasqs extract_name() function can be abused to cause a heap buffer overflow, allowing an attacker to inject false DNS cache entries, which could result in DNS lookups to redirect to an attacker-controlled IP address, or to cause a DoS. CVE-2026-4893: An information disclosure vulnerability in dnsmasq allows remote attackers to bypass source checks via a crafted DNS packet with RFC 7871 client subnet information. CVE-2026-5172: A buffer overflow in dnsmasq's extract_addresses() function allows an attacker to trigger a heap out-of-bounds read and crash by exploiting a malformed DNS response, enabling extract_name() to advance the pointer past the record's end.	VDE-2026-076	CVE-2026-2291 CVE-2026-4893 CVE-2026-5172
#58709	OpenSC before 0.27.0-rc1, fixed in commit 3f24f0b, contains a stack buffer overflow vulnerability in piv_process_history() in src/libopensc/card-piv.c that allows physically present attackers to trigger memory corruption by presenting a crafted PIV smart card or USB device returning a URL field longer than 118 bytes in the Key History Object ASN.1 response.	VDE-2026-076	CVE-2026-40510

Ticket	Description	Cert@VDE ID	CVE
#57630	OpenSSL 1.1.1w: multiple low-severity denial-of-service / memory-corruption issues reachable only by locally parsing crafted PKCS#12, PKCS#7 or RFC 3161 timestamp input.	VDE-2026-076	CVE-2025-68160 CVE-2025-69418 CVE-2025-69419 CVE-2025-69420 CVE-2025-69421 CVE-2026-22795 CVE-2026-22796

2 Up-/Downgrade Information

- Downgrades to versions below 2.3.0 will loose all settings on WWAN connection monitor, IPsec GCM cipher, DHCP server PXE boot and NTP settings.
- When a Docker container is run on version 2.2.8 and then downgraded to an earlier version, the older Linux kernel does not support overlay2fs. As a result, the Docker service fails to start.
- Downgrades to versions below 2.2.1 will loose all settings on Remote Capture and NTP Interface Filter
- Downgrades to versions below 2.2.0 will loose all settings on SNMP.
- Downgrades to versions below 2.2.0 will loose all settings on network interface access filter for Docker.
- Downgrades to versions below 2.2.0 will loose all settings regarding WWH3.
- Products with WWAN modem can no longer be downgraded below version 2.2.0 due to EN18031-1 restrictions.
- Downgrades to versions below 2.1.1 will loose all settings on user specific display of menu entries in the web interface.
- Downgrades to versions below 2.1.0 will loose all settings on password lifetime and password reuse policies.
- Downgrades to versions below 2.0.9 will loose all settings on Docker USB and RS485 device access.
- Downgrades to versions below 2.0.0 need a run of the password migration wizard to convert all passwords to htdigest before an downgrade is accepted.
- Downgrades to versions below 1.6.0 will loose all DNS based entries in the network groups lists
- Downgrades to versions below 1.6.0 will loose several NTP related settings
- Downgrades to versions below 1.5.0 will loose all static routes above the 20 count.
- Downgrades to versions below 1.5.0 will loose the PPPoE settings
- Downgrades to versions below 1.4.0 will loose all Docker containers and Docker related settings.
- Downgrades to versions below 1.3.0 will loose IPsec connections with wildcards in the identities.
- Downgrades to versions below 1.2.11 will loose settings regarding the Scheduler.
- Upgrade to version 2.x is only possible from version $\geq 1.6.8$
- IRF1000 with alternative Ethernet switch chip are supported starting with firmware versions than 1.2.3. Downgrades below 1.2.3 are blocked on the corresponding devices.
- Downgrades from 1.1.x or later to 1.0.x or earlier will loose settings regarding Forwarding, OpenVPN and IOT.
- Support for first generation Big-LinX smartcards is deprecated for hardware revision BA or higher. These old smartcards use 3.3V and the latest hardware revision from BA and higher uses an 1.8V only smartcard reader.

3 License and Version Information

The following file distributed by ADS-TEC Industrial IT GmbH:

Ads-tec-IRF1xxx-2.3.1-SVN-R66702.B-186119.bin

SHA256 checksum:

af9831be881195433b0cadcd67a9e1d1fa94c82746a6a118f72294debe595a34

contains software based on the following listed open source software given by name version and license. You can order a CD-ROM free of charge containing all used open source code and its modifications by us as far as required by each of the dedicated licenses at ads-tec under the following address:

ADS-TEC Industrial IT GmbH
Heinrich-Hertz-Straße 1
72662 Nürtingen

order number: DZ-PCKO-13077-0 [2.3.1]

Please take into regard the following table with the different components and licenses. Each software component might have multiple licenses. All referenced licenses are distributed in general form together with this file under the corresponding subfolder and in dedicated original form as distributed by the original author(s) together with the source code on the above given CD-ROM.

Name	Version	License
arptables	0.0.5	GPL-2.0
audit	3.1.5	GPL-2.0-or-later
base-files	-	GPL-2.0
util-linux	2.38	GPL-2.0-only
bridge-utils	1.7	GPL-2.0-or-later
btrfs-progs	5.7	GPL-2.0-only
busybox	1.33.0	GPL-2.0
ca-certificates-adstec	20260223	GPL-2.0-or-later,MPL-2.0
ccid	1.6.2	LGPL-2.1-or-later
ppp	2.4.9	BSD-4-Clause
chrony	4.8	GPL-2.0
cjson	1.7.18	MIT
containerd	1.7.28	Apache-2.0
cryptsetup	2.5.0	GPL-2.0-or-later,LGPL-2.1-or-later
curl	8.17.0	MIT
dnsmasq	2.92rel2	GPL-2.0
docker	27.5.1	Apache-2.0
docker-rootless-extras	27.5.1	Apache-2.0
dockerd	27.5.1	Apache-2.0
e2fsprogs	1.47.0	GPL-2.0

Name	Version	License
ebtables	2018-06-27	GPL-2.0
ethtool	6.15	GPL-2.0
ubox	24.10.4	GPL-2.0
glib2	2.82.5	LGPL-2.1-or-later
gpsd	3.27.5	BSD-2-Clause
hostapd	2024-09-15	GPL-2.0-only
htop	3.0.5	GPL-2.0-or-later
hub-ctrl	1.0.0	PUBLICDOMAIN
ifplugd	0.28	GPL-2.0+
iproute2	5.11.0	GPL-2.0
iptables	1.8.7	GPL-2.0
ipset	7.6	GPL-2.0
isc-dhcp	4.4.3-P1	MPL-2.0
iw	6.9	GPL-2.0
jq	1.8.2	MIT
libubox	24.10.4	ISC
jsonfilter	2018-02-04	ISC
libaio	0.3.112	LGPL-2.1-only
libalpar	1.0.1	LGPL-2.0
bzip2	1.0.8	bzip2-1.0.8
libcap	2.69	GPL-2.0-only
libcprops	0.1.12	LGPL-2.1
lvm2	2.03.16	GPL-2.0, LGPL-2.1
libedit	20210419-3.1	BSD-3-Clause
libevdev	1.10.1	MIT
libevent2	2.1.12	BSD-3-Clause
libfaketime	0.9.10	GPL-2.0-or-later
libffi	3.3	MIT
gmp	6.3.0	GPL-2.0-or-later
gnutls	3.8.10	LGPL-2.1-or-later
libgpg-error	1.55	LGPL-2.1-or-later
libiconv-full	1.16	LGPL-2.1-or-later
libjson-c	0.15	MIT
libtool	2.4.6	GPL-2.0+
lxc	4.0.5	LGPL-2.1-or-later, BSD-2-Clause, GPL-2.0
lzo	2.10	GPL-2.0-or-later
libmnl	1.0.4	LGPL-2.1+
libmodbus	3.1.8	LGPL-2.1-or-later
mosquitto	2.0.19	EPL-2.0

Name	Version	License
ncurses	6.4	MIT
libnetfilter-contrack	1.0.8	GPL-2.0-or-later
libnetfilter-log	1.0.1	GPL-2.0+
net-snmp	5.9.5.2	MIT,BSD-3-Clause-Clear
nettle	3.9.1	GPL-2.0-or-later
libnetwork	2022-07-16	Apache-2.0
libnfnetlink	1.0.1	GPL-2.0+
libnftnl	1.1.8	GPL-2.0-or-later
libnl-tiny	2023-12-05	LGPL-2.1
libol	0.3.18	GPL-2.0
opensc	0.27.1	LGPL-2.1-or-later
openssl	1.1.1w	OpenSSL
libp11	0.4.11	LGPL-2.1-or-later
libpcap	1.10.5	BSD-3-Clause
pcre	8.44	BSD-3-Clause
pcre2	10.42	BSD-3-Clause
pcsc-lite	2.3.3	BSD-3-Clause
popt	1.16	MIT
readline	5.2	GPL-2.0
libseccomp	2.5.1	LGPL-2.1-or-later
libsodium	1.0.18	ISC
sqlite2	2.8.17	PUBLICDOMAIN
sqlite3	3.49.1	PUBLICDOMAIN
sysfsutils	2.1.0	LGPL-2.1
tee-suplicant	3.21.0	BSD-2-Clause
ubus	24.10.4	LGPL-2.1
uci	2020-10-06	LGPL-2.1
uclient	2020-12-10	ISC
udebug	24.10.4	GPL-2.0
libudev-zero	1.0.3	MIT
uqmi	2025-07-30	LGPL-2.1-or-later
libusb	1.0.24	LGPL-2.1-or-later
libusb-compat	0.1.7	LGPL-2.1-or-later
libwebsockets	3.1.0	LGPL-2.1+exception
lighttpd	1.4.65	BSD-3-Clause
memtester	4.3.0	GPL-2.0
mii-tool-ifw	1.50	GPL-2.0
minicom	2.7.1	GPL-2.0
mmc-utils	2019-10-10	GPL-2.0
netcat	0.7.1	GPL-2.0

Name	Version	License
netflash	4.1	GPL-2.0
nftables	0.9.6	GPL-2.0
openssh	9.9p2	BSD,ISC
openvpn-radiusplugin	v2.1a_beta1	GPL-2.0
openvpn	2.5.3	GPL-2.0
opkg	2021-03-15	GPL-2.0
paho-mqtt-c	3.10	Eclipse,Distribution,License,v 1.0
pcsc-tda8029	1.0.0	BSD-3c
php-jsonrpc	1.4.0	MIT
php8	8.3.31	PHP-3.01
php8-pecl-apcu	5.1.23	PHP
phytool	2	GPL-2.0+
pkcs11-helper	1.27.0	GPL-2.0
procd	24.10.4	GPL-2.0
quagga	1.2.4	GPL-2.0
rng-tools	6.10	GPL-2.0-or-later
rpcd	1.0	ISC
runc	1.3.3	Apache-2.0
gptfdisk	1.0.6	GPL-2.0-or-later
shadow	4.8.1	BSD-3-Clause
smtpclient	10911	GPL-2.0
spi-tools	0.8.6	GPL-2.0-only
sscep2	0.9.1	SSLEAY,OPENSSL,BSD-2c,VSL-1.0
stress	1.0.4	GPL-2.0
strongswan	6.0.7	GPL-2.0-or-later
syslog-ng	4.10.1	LGPL-2.1-or-later,GPL-2.0-or-later
tcpdump	4.99.4	BSD-3-Clause
tini	0.19.0	MIT
uboot-envtools	2015.10	GPL-2.0,GPL-2.0+
uchardet	v0.0.8	LGPLv2.1
uhttpd	2025-10-03	ISC
urandom-seed	-	GPL-2.0-only
urngd	2020-01-21	GPL-2.0,BSD-3-Clause
hwdata	0.387	GPL-2.0-or-later,,XFree86-1.0
usbutils	013	GPL-2.0-only
wwan	2019-04-29	GPL-2.0
zlib	1.3.1	Zlib

Name	Version	License
zoneinfo	2021a	Public,Domain
zxcvbn-c	2024-03-12	MIT
linux	6.1.177	GPL-2.0
golang	1.23.12	BSD-3-Clause
u-boot	2023.04	GPL-2.0+