ACHT:WERK GmbH & Co. KG · Am Mohrenshof 11a · D-28277 Bremen

Adressed to:
Customer, System-Partner, Support

Bremen, March 10, 2025

Dear Customers, Partners, and Support Colleagues

this document describes the additional functions of the IRMA® system in the release mentioned.
Legal notice:

All contents, in particular texts, photographs and graphics of this document are protected by copyright and may only be copied or disclosed in accordance with the licenses concluded with Achtwerk GmbH & Co. KG and may only be copied or disclosed in accordance with the licences concluded with Achtwerk GmbH & Co. If you wish to use parts of this document, please contact the sales department of the IRMA® system. For the use of a network monitoring system and the recording of communication data, country- and company-specific legal conditions must be observed.

Important notes: This document, accompanying texts and marketing documents have been prepared with the greatest care. However, errors cannot be excluded. The information contained in this manual is subject to change without notice and should not be construed as a commitment or obligation on the part of Achtwerk GmbH & Co. KG. Therefore, no guarantee or legal liability can be assumed.
Users of the IRMA® system are subject to a separate contract which regulates further matters.

We reserve the right to change user manuals and other documents as well as the specification of the IRMA® system at any time and without prior notice. Changes may be reflected in future user manuals; however, there is no obligation to revise and provide further user documents in a timely manner.

V25.02 is a major release.

Notes on the upgrade:

Create a backup of the data from the IRMA® system beforehand.

During the upgrade, it is recommended to disconnect or deactivate the monitoring network connections.

Upgrading the software of the IRMA® devices requires a continuous power supply, a continuous availability of the network infrastructure and continuous connection of the client TAPs to the central IRMA device.

THE OFFLINE UPGRADE PROCEDURE (MANUAL: CHAPTER “SYSTEM UPDATE”) MUST BE PERFORMED TWICE.

1st step:
Start with the Achtwerk upgrade page https://office.acht-werk.de/upgrade-stable21 as shown in the user interface. The existing operating system and the existing software modules are updated and prepared for the upgrade.

Then perform a warm start and check the version of the IRMA® central unit. It must display [stable25]:

IRMA version v24.06 [stable25]
Release time 27.09.2024, xx:xx:xx
Device version: 24.06~250xxxxxxx

2nd step:
Now use this Achtwerk upgrade page: https://office.acht-werk.de/upgrade-stable25
(NOT .../upgrade-stable21 as displayed in the user interface!)

The upgrade will provide approx. 600-700 MB (package reply file) for download. The update will take 30-60 minutes. The existing operating system and the existing software modules will be updated.
This upgrade includes a cold start of the devices.

Then check in the Configuration / Info menu and the system overview:

IRMA Version v25.02 [stable25]
Release time 05.03.2025, xx:xx:xx
The device version of the IRMA® devices must be at least 25.02~250xxxxxxx.

New functions:

- SYSLOG forwarding: Syslog messages and anomaly detection events of the IRMA® system can be (automatically) forwarded by syslog:
    - Forwarding of received and analysed syslog messages from the Syslog Event Manager
    - Anomaly detection events of the IRMA® system
    - Audit log event of the IRMA® system
      All syslog messages of the IRMA® system are sent with Facility: User and Severity: Info.

- OPC UA DA server for exchanging the detection metrics
    - Threat level of the IRMA® system
    - Number of events with type "Alarm" and "Info“
    - Number of assets with status Warning
    - Server security mode is "SignAndEncrypt" with certificates and standard port TCP/4880

- RULESET:
    - Extension of the mail template for the Send email action
    - Creation of individual mail body
    - Variables: %(count) - number of hits, %(rule) - name of the rule, %(time) - timestamp, %(table) - table of the asset with detailed data.

- OT-ASSETMANAGEMENT:
    - Extension of the property fields / attributes of an asset, e.g. product, housing, serial number, firmware, status, lifecycle, startup, and free text fields)

- Pre-import of assets
    - Assets can be imported in advance from project planning or CMDB.
    - Comparison with the existing assets is primarily based on the MAC address, alternatively by IPv4 address.
    - If the asset is recognized in monitoring, the “Last access” field is updated accordingly. Initially, the field is empty.

- IM- and EXPORT of the networks
    - Simple import and export of the IPv4 networks that the IRMA® system monitors and generates assets accordingly
      NOTE: Network areas in the public IPv4 range can also be added with the import.

- NOTES:
    - Notes field for commenting on alarms
    - Creation of individual text notes in the PCAP files in the downloads

- RISK MANAGEMENT:
  - Multiple selection of assets (groups) for assignment to threats
  - Dedicated selection of protection targets per identified threat

- Extension of detection and analysis of layer 3 protocols
  - IPv4 (non-tcp, non-udp, non-icmp)
  - IPSEC (AH/EPS)
    NOTE: This upgrade may detect and display new assets or connections. The threat level will change!

- Improved heuristics and confirmation of connection direction
  - Additional column Port(2) in case of missing handshake
  - Manual change of direction without detected handshake

- Syslog permissions
  - Authorization for the Syslog menu (Syslog Event Manager)

- LDAP / ADS user authentication
  - Query search base in AD improved
  - By default via User Principal Name (UPN). If a domain is missing in the user name, the default domain is automatically used (e.g. Username@domain.com).
  - For multiple domains, enter the NetBIOS domain name in NTLM format (DOMAIN\Username)

Update and enhancement of security parameters and functions:

IEC 62443

- TLS 1.3 is default, migration of HTTPS certificate with 3072 length
- SFTP with PPKey
- OPC UA SecurityMode “SignAndEncrypt” with certificates
- De-/activation of support access (SSH)
- Identification of functions and configurations for secure operation and secure system according to IEC62443-4-x (manual)
- Update of open source software components and operating system

Bug Fixing:

- (Alarms) TTL analysis error, False Positive on Traceroute / Firewalking Alarm [5690]
- (System) Performance - Debian10 CryptSetup Fix (internal) [5721]
- (System) Control of the processes for the connections of the client TAPs [1016]
- (System) Performance for 10Gb monitoring network connections [1016]
- (Assets) Handling ICMP Type 3 reply changed - No asset is created [5641]
- (Rules) Error during Synchronization of rules and updating of endpoints Alarm of RestAPI fixed [5721]
- (System) PCAP export filter behavior [6295]
- (System) Wrong representation connection of same SRC / DST port [5862]
- (System) Connection directions / heuristics [3943] [3944] [5465] [5466] [5417]
- (Alarms) CONN::SWAP on rotation of a connection (formerly also CONN::DEL)
- (System) Search base queries/LDAP not working [5055]