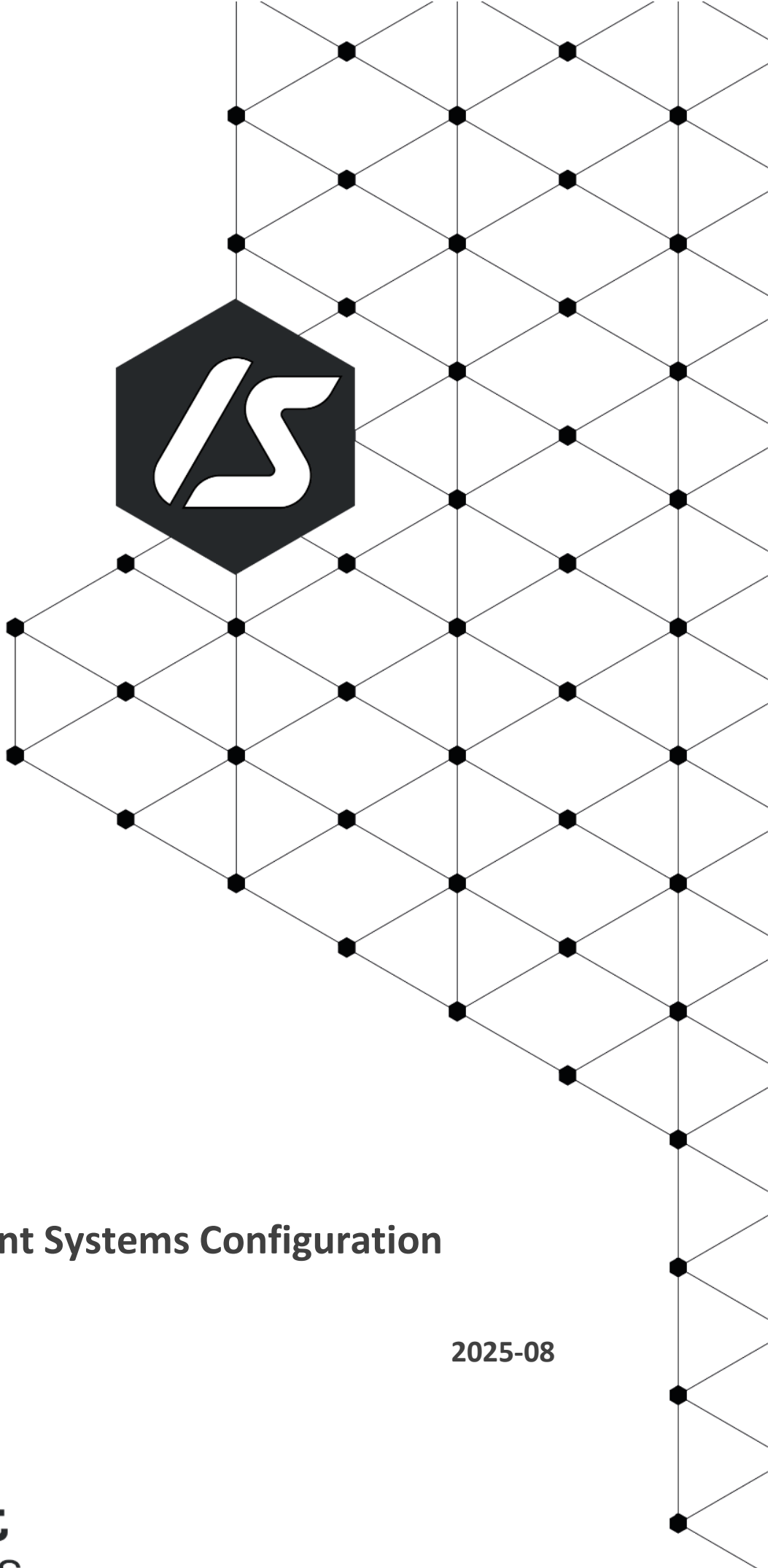


Teltonika – Instant Systems Configuration Standards

2025-08

instant systems

Teltonika – Instant Systems Configuration Standards

(Applies to all router-based systems delivered by Instant Systems Sweden AB)

As part of our work to meet the requirements of **EN 18031-1** (common security requirements for internet-connected radio equipment), we have **updated the standardized configurations** for the Teltonika routers used in our systems. These configurations are designed to strengthen security, minimize vulnerabilities, and provide a robust foundation for network communication. This document outlines the key security measures and their purpose.

🔐 User & Access Security

To protect against unauthorized access, we have implemented a strict password policy and disabled insecure remote access methods:

- **Password Policy:**
  - Minimum length: 12 characters
  - Must include digits, upper- and lowercase letters, and special characters
  - Each device is delivered with a unique password (no shared default credentials), physically printed on the router.
    → Reduces the risk of weak or guessable passwords and protects against brute-force attacks. Ensures compliance with the latest requirements under the EU Radio Equipment Directive (RED).

- **Remote Monitoring (RMS)**
  Remote Monitoring is enabled by default on all EU-based installations to support operational requirements of major customers. On non-EU markets, Remote Monitoring is disabled.
  → The feature itself does not introduce security risks when unused, but it is made available in the EU to align with customer requirements.

- **CLI (Command Line Interface) and Telnet access disabled**
  → Removes insecure management interfaces. Telnet does not use encryption, and disabling both prevents attackers from exploiting text-based administration channels.

- **Remote access disabled**
  → Unnecessary remote administration paths are closed, reducing the potential attack surface.

🌐 Network & Firewall

We have hardened network and firewall settings to prevent intrusion attempts and malicious traffic:

- **Forced HTTP → HTTPS redirection**
  → Ensures that all web traffic to the router is encrypted, protecting against

interception of sensitive information.

- **Firewall attack prevention enabled:**
  - SSH flood
  - HTTP/HTTPS flood
  - Ping flood
  - Port scan
  - SYN flood

  → Provides active protection against common network-based denial-of-service (DoS/DDoS) and scanning attacks.

- **Hardened traffic rules:**
  - ICMP ping, IGMP, IPSec-ESP, ISAKMP, mDNS blocked

  → Only necessary traffic is allowed, minimizing exposure to unnecessary or vulnerable network protocols.

- **Default network configuration changed**

  → Prevents the use of factory-default IP ranges that are widely known and often targeted by attackers.

- **Failover WAN → Mobile configured**

  → Ensures redundancy: if the primary WAN fails, the system automatically switches to mobile connectivity to maintain service availability.

🔒 **Access Control**

To mitigate repeated intrusion attempts, IP blocking is enforced:

- **Login attempt blocking:**
  - Threshold: 15 failed attempts
  - Blocking type: Timed, with automatic cleanup at reboot

  → Limits brute-force login attempts by automatically blocking repeated failures, while ensuring that legitimate users regain access after a system restart.

⚙️ **System Maintenance**

To ensure stable operation and controlled update management, the following routines are applied:

- **Automatic reboot enabled**
  - Ping check from both SIM cards against 8.8.8.8

  → Device reboots automatically if connectivity is lost, preventing the system from becoming unresponsive.

- **Firmware: Latest version installed**

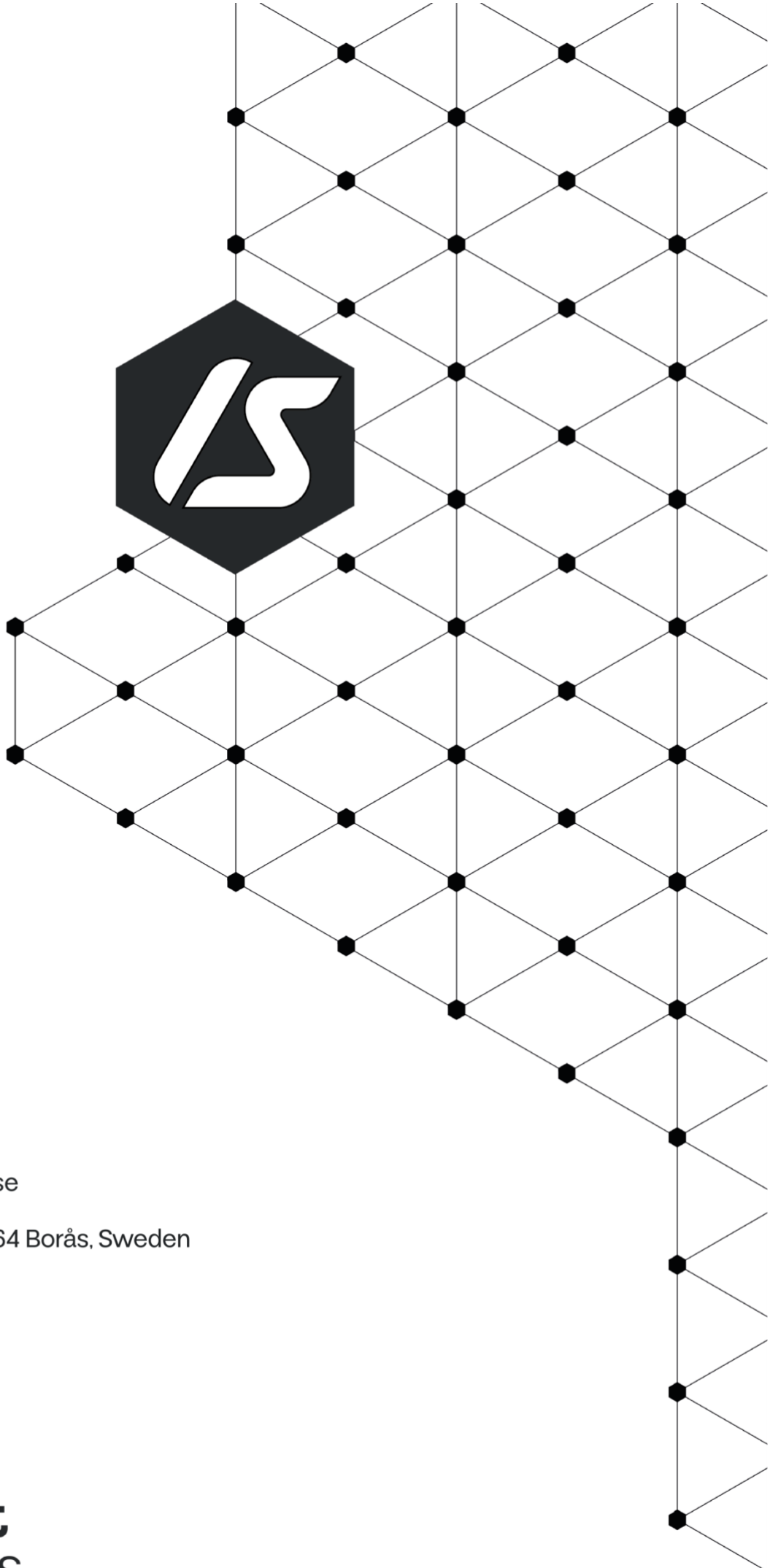
  → Ensures that the router benefits from the most recent security patches and

stability improvements.

- **FOTA (Firmware Over-The-Air) updates disabled**
  → Updates are performed only under Instant Systems' controlled process, avoiding untested or automatic changes that could affect reliability.

Summary
Through these configurations we deliver a router environment that is:

- **Hardened** against intrusions and attacks
- **Controlled** with clear routines for updates and maintenance
- **Redundant** for high availability
- **Compliant** with relevant aspects of EN 18031-1



instantsystems.se

info@instantsystems.se

Ryssnäsgatan 18, 504 64 Borås, Sweden

+46 33 750 1000

instant systems