Wolf IoT Gateway

Product Security Information

Manufacturer: FoxIoT OÜ | **Address:** Pärnu mnt 148, 11317 Tallinn, Estonia | **Website:** www.foxiot.eu | **Email:** info@foxiot.eu

Document: CRA-UI-001 | **Version:** 0.2 | **Date:** 2026-05-07

About This Document

This document provides security information for the Wolf IoT Gateway, as required by the EU Cyber Resilience Act (Regulation 2024/2847).

Reporting Security Vulnerabilities

If you discover a security vulnerability in a Wolf IoT Gateway product:

Email: security@foxiot.eu
Policy: www.foxiot.eu/security

Product Identification

Field	Value
Product	Wolf IoT Gateway
Model	Printed on the device label (backside)
Serial number	MAC address, printed on the device label
Firmware version	Visible in the web UI (System > Versions)

Intended Purpose

The Wolf IoT Gateway is a programmable industrial IoT controller for field deployment. It serves as a communication gateway and edge controller, bridging field devices (sensors, actuators, Modbus devices) with upstream systems (cloud platforms, SCADA, management systems).

Typical use cases:

- Monitoring and controlling distributed energy assets via Modbus RTU/TCP
- Building automation — interfacing with HVAC systems and controllers
- IoT sensor data collection and forwarding to cloud platforms via MQTT

- Protocol conversion — Modbus RTU to Modbus TCP
- Connectivity — LTE modem provides internet access for the gateway and connected field devices

Security Features

Feature	Description
Firewall	Default-deny firewall. Only SSH (port 22) and HTTP (port 5080) open by default on Ethernet.
WireGuard VPN	Available for encrypted remote access. User configures via web UI.
Password policy	Minimum 10 characters (uppercase, lowercase, number, special character). Forced on first login.
Two-factor authentication	TOTP (Time-based One-Time Password) available.
Port management	SSH and HTTP ports can be closed via the web UI after VPN is configured.
MQTT encryption	TLS/SSL for MQTT connections to upstream systems.
Firmware signing	Ed25519 digital signature — device rejects tampered firmware.
Dual firmware failsafe	Two firmware areas. If primary fails, device boots from backup.
Hardware watchdog	Automatic restart if services stop responding.
Read-only filesystem	System files cannot be modified.
Factory reset	Physical button with multi-step sequence (prevents accidental reset).
Audit log	Records configuration changes, firmware updates, and login events.
Data minimisation	No telemetry sent to manufacturer. Device does not contact external servers unless configured by user.

Security Limitations

Limitation	Description
No secure boot	Hardware limitation of the NUC980 processor. Mitigated by firmware signing.
No HTTPS	Web UI and REST API use HTTP only. Mitigated by WireGuard VPN + TOTP 2FA. See "Network Security Requirements" below.
No disk encryption	Flash storage is not encrypted. Passwords are securely hashed (bcrypt). Sensitive keys protected by physical access (metal enclosure, locked cabinet).
Modbus has no encryption	Modbus RTU/TCP is an industry standard protocol without built-in encryption. Physical security of cabling is the primary control.

Network Security Requirements

The Wolf IoT Gateway web UI uses unencrypted HTTP. There are two recommended deployment approaches:

Option A — Trusted internal network only:
Install the device on a dedicated, trusted industrial network segment. The device must not be reachable from the internet or untrusted networks. No VPN required.

Option B — WireGuard VPN with closed ports:

1. Configure a WireGuard VPN tunnel via the web UI
2. Verify VPN connectivity
3. Close HTTP (port 5080) and SSH (port 22) on the Ethernet interface via the web UI firewall
4. After this, the device is only reachable through the VPN

In both cases:

- Enable TOTP two-factor authentication for all user accounts
- Do not expose HTTP directly to the internet
- Keep firmware up to date

Getting Started

The web UI ships with a single administrator account:

- **Username:** `foxiot`
- **Password:** `foxiot`

The factory default password is shared across all devices — change it immediately, before connecting the device to any network from which it should not be administered.

On first login:

1. **Log in with `foxiot` / `foxiot`.** The system blocks all other UI actions with a "Change password required" dialog: you must set a new strong password (minimum 10 characters, including uppercase, lowercase, number, and special character) before any other action is possible. Until the new password is saved, only "Logout" or "Update password" are available.
2. Enable TOTP two-factor authentication (recommended) — open the Users page after the password change to set this up.
3. Configure WireGuard VPN if remote access is needed.
4. Close HTTP/SSH ports after VPN is configured (optional but recommended).
5. Verify the firmware version in System > Versions.

How Changes Affect Security

Some configuration changes affect the security of the device:

Change	Security Impact
Adding new user accounts	Each user can access the device — only grant to trusted personnel
Disabling TOTP for a user	Removes second factor; password alone is weaker
Opening additional firewall ports	Each open port increases the attack surface — only open ports that are required
Disabling SSH/HTTP ports	Reduces attack surface; ensure alternative access (e.g., VPN) is configured first
Installing firmware updates	May change security behaviour — read the changelog
Factory reset	Erases all user data, configuration, credentials, and keys — device returns to default state

Installing Security Updates

1. Download the firmware file from www.foxiot.eu/firmware/wolf-gateway/
2. Log in to the web UI
3. Navigate to **System**, find the **Firmware Upload** block
4. Upload the firmware file
5. Press the **Restart Controller** button
6. The device verifies the firmware signature during boot

Updates can also be installed via SSH or USB/SD card.

EU Declaration of Conformity

Hereby, FoxIoT OÜ declares that the Wolf IoT Gateway is in compliance with Regulation (EU) 2024/2847 (Cyber Resilience Act).

The full text of the EU Declaration of Conformity will be available at:
www.foxiot.eu/compliance/wolf-gateway-declaration-of-conformity.pdf

Automatic Security Updates

Not applicable — the Wolf IoT Gateway does not have an automatic security update mechanism. All security updates are installed manually (see "Installing Security Updates" above).

Security Updates and Support

- Security updates are provided **free of charge** during the support period
- Support period: **5 years** from the date the product is placed on the market
- Updates published at www.foxiot.eu/firmware/wolf-gateway/
- Security advisories announced at www.foxiot.eu/security

How to be notified about new updates: Email security@foxiot.eu to subscribe to our security advisory mailing list — every published advisory is emailed when it goes live. For critical or actively exploited vulnerabilities, FoxIoT also reaches out directly to known integrators. Updates are always installed manually by the operator, so timing remains under your control.

Per-device support end date: Each device has its own end-of-support date based on its date of manufacture. To request the end date for a specific device, email security@foxiot.eu and quote the MAC address printed on the device label. We reply within 5 working days.

After the support period: The device continues to operate normally. FoxIoT is no longer obligated to issue security updates, but in practice will normally continue to ship updates while the product remains in active production. Extended support beyond the formal period is available by separate commercial arrangement.

Decommissioning

To remove all data from the device before disposal or transfer, perform a factory reset using the physical button on the device. The factory reset erases all user credentials, configuration, application data, and cryptographic keys.

For high-security environments: NAND flash memory may retain residual data traces. If complete data destruction is required, physically destroy the device.

Known Risks

Risk	What to do
Device connected directly to internet without VPN	Use WireGuard VPN for remote access. Close SSH and HTTP ports when VPN is configured. Place device behind a network firewall.
TOTP not enabled	Enable TOTP two-factor authentication in the web UI.
HTTP web UI used on untrusted network	Use WireGuard VPN tunnel for web UI access.
Untrusted devices on RS-485 bus	Only connect trusted field devices. Modbus has no authentication.
Device in physically accessible location	Install in a locked cabinet or enclosure.
Outdated firmware	Always install the latest firmware version provided by FoxIoT.

Software Bill of Materials (SBOM)

The SBOM is maintained internally by FoxIoT in CycloneDX format. It is provided upon reasoned request to market surveillance authorities, customers, and security researchers. Contact security@foxiot.eu to request access.

Contact

Security issues	security@foxiot.eu
General support	info@foxiot.eu
Security policy	www.foxiot.eu/security

This document fulfils the requirements of EU Regulation 2024/2847 (Cyber Resilience Act), Annex II.
FoxIoT OÜ — www.foxiot.eu