ACKSYS
COMMUNICATIONS & SYSTEMS

APPLICATION NOTE

Secure Setup and Network Interface Management

May 2025

Content

1. Introduction

1.1 Purpose

This guide supports you during the first-time setup of your ACKSYS device. It helps you secure your installation from the initial steps and understand which services are enabled by default, in accordance with the EN 18031 security requirements. It is intended to complement the WaveOS user manual and the quick start guide, where you can find detailed instructions for configuring and deploying your ACKSYS product.

1.2 Target Audience

This document is intended for any user or installer of ACKSYS products—especially access points, routers, or Wi-Fi gateways—used in industrial, railway, or embedded environments. It is also designed to meet the expectations of IT/OT security auditors or managers.

2. Secure installation: First steps

The device must be installed in a secure environment, inaccessible to the public or unauthorized individuals. This measure is intended to ensure the physical protection of the equipment and prevent any unauthorized access to the network interfaces.

2.1 Initial Connection

1) Connect an Ethernet cable to eth0 or eth1 (device LAN port).
2) Configure your PC with a static IP address in the 192.168.1.0/24 range.
3) Open your browser and go to: http://192.168.1.253
4) You will be prompted to set a **strong administrator password**. You cannot proceed without completing this step.

2.2 Password Security

The administrator password protects all critical services. We recommend:

- At least 8 characters
- A mix of uppercase, lowercase, digits, and special characters
- Avoid using previously used passwords

A temporary lockout is triggered after multiple failed login attempts.

2.3 Services available after setup

Once connected, the following services can be enabled:

- **Wi-Fi** (wlan0/wlan1): SSID, WPA2/WPA3, AP/client mode
- **VLAN, Bridge, Routing**
- **VPN**
- **SSH**: remote CLI, public key recommended
- **SNMPv3**: secure network monitoring via user accounts
- **Cellular**: wwan0 interface (APN, PIN, etc.)

For the complete list, please refer to the WaveOs user guide.

3. Factory Default Configuration

3.1 Enabled by Default

- **HTTP Interface**: enabled for initial setup (HTTPS available with self-signed certificate)
- **Static IP Address**: 192.168.1.253/24
- **No Default Password**
- **Cellular Interface**: enabled by default, auto APN detection, no PIN required, enables secure connection to ACKSYS cloud via embedded certificate. Used only for product registration. Configured in NAT mode, no port forwarding allowed from incoming WAN.
- **SNMPv2**: enabled for initial on-premise NMS monitoring. Must be disabled afterward for security.

3.2 Disabled by Default

- All other services: Wi-Fi, SSH, mDNS, LLDP, VPN, etc.
- No external service access without administrator action
- Reset button restores full factory defaults

4. Network Interface Configuration and Control

4.1 Available interfaces and user Control

Interface	Enabled by Default	Can Be Disabled	Port(s)/Protocol(s)	Authentication	Typical Use
Ethernet LAN	Yes	No, but unusable if not configured	Ethernet	Local physical access only	Access to Web UI
Wi-Fi	No	Yes	WLAN / WPA2-WPA3	WPA2/WPA3 shared key	Client or AP mode
Cellular	Yes	Yes	PPP/IP / Cellular	SIM	WAN/ACKSYS Cloud access
Web (HTTP)	Yes	Yes	TCP 80 / HTTP	Password	Initial setup
Web (HTTPS)	Yes	Yes	TCP 443 / HTTPS	Password / TLS certificate	Secure web access
SSH	No	Yes	TCP 22 / SSH	Password or public key	Remote CLI
SNMPv2	Yes	Yes	UDP 161 / SNMPv2c	Community string	Initial monitoring (disable after use)
UDAP	Yes	Yes	TCP 17784	–	Local device discovery
SNMPv3	Yes	Yes	UDP 161 / SNMPv3	User + password/encryption	Secure remote monitoring
MQTT	Yes	Yes	TCP 443 / TLS/HTTPS	Embedded ACKSYS certificate	ACKSYS cloud / On-premise NMS

4.2 Connection acceptance (Router Mode)

The device allows configuration of **acceptance policies** that restrict access to administrative services (Web, SSH, SNMP, etc.) based on interface (LAN, WAN, Cellular, VLAN). This helps limit exposure to trusted networks.

4.3 User control

All disabled interfaces can be explicitly and selectively activated via the Web interface. No service is enabled without administrator confirmation.

4.4 Monitoring and Audit

- All access (Web, SSH) is logged
- Network configuration changes are timestamped
- System logs are stored locally and exportable

4.5 Security Checklist and Best Practices

1) Set a strong root password upon first login
2) Enable HTTPS, upload a valid certificate (replace self-signed), and disable HTTP
3) Disable or restrict SSH to trusted IPs
4) Disable SNMPv2 after initial use; if required, create SNMPv3 users
5) Enable system logs and review them regularly (access/config changes)
6) Block any unused ports or protocols
7) Configure firewall and restrict remote access to trusted segments
8) Isolate administrative services on VLANs or internal subnets
9) Limit Web/SSH access to trusted interfaces (e.g. LAN or admin VLAN)
10) Enable only strictly necessary services
11) Apply firmware/security updates provided by ACKSYS regularly

Support : https://support.acksys.fr