

Security Recommendations for Using EIBPORT Systems

Why IT Security Matters

In the increasingly connected world of building automation, IT security is not optional – it's essential. Not only are private smart homes at risk, but commercial and industrial building automation systems are also becoming frequent targets of cyberattacks. Systems like the EIBPORT control critical functions such as lighting, climate, access, or energy distribution – potentially qualifying as critical infrastructure.

Security doesn't start with the device itself – it starts with infrastructure planning and day-to-day operations:

- How is your network structured?
- Who has access – internally and externally?
- What measures do you take when making configuration changes or firmware updates?

The following recommendations will help you operate the EIBPORT securely. However, they also apply in principle to any IP-enabled automation solution and provide a solid foundation for a well-thought-out security concept – regardless of the manufacturer.



These security recommendations serve as general best-practice guidelines. They do not replace an individual risk assessment or qualified IT consulting.

1. Network Security

- Use static IP addresses
- Segment your network using VLANs (e.g., visualization, control, internet access)
- Disable KNXnet/IP routing and/or tunneling if not actively in use
- Use a firewall that only opens necessary ports:
 - HTTP/HTTPS: 80 / 443
 - SSH: 36
 - VPN SSL: 1724 (recommended)
 - KNXnet/IP: 3671
 - Enable HTTPS: Completely avoid unencrypted connections

2. Remote Access and VPN Usage

Why VPN instead of port forwarding?

Port forwarding exposes your network to external access and is frequently scanned automatically by attackers. VPN connections are encrypted, authenticated, and controllable – making them the more secure method for remote access to your building automation system. **Direct port forwarding from the internet to the EIBPORT web interface or KNX services (e.g., ports 80, 443, 3671) represents a significant security risk.**

Use a VPN connection as a secure tunnel for remote access:

- SSL VPN (OpenVPN) with BAB SECURELINK – robust and secure
- HOOC Gateway – easy to integrate, cloud-based
- PPTP VPN – avoid if possible; only use if absolutely necessary for iOS
(PPTP uses outdated encryption methods like MS-CHAPv2, which have been considered insecure for years. Several vulnerabilities allow attackers to crack passwords or decrypt data with relatively little effort.)

3. User Management

- Clearly separate system access (configuration, editor) from visualization access
- Use different usernames and passwords for administrators and end users
- Use complex passwords
- Use PIN protection for visualization elements that should be visible but not operable by unauthorized users
- Optionally hide users with extended rights from lists visible to others

4. Maintenance & Monitoring

- Perform firmware updates regularly
- Create regular project backups and store them securely
- Use time servers (NTP) to ensure correct system time

Legal Notice

These security recommendations represent general best-practice guidelines. They do not replace individual analysis or professional IT consultation. BAB TECHNOLOGIE accepts no liability for any damage resulting from implementing or failing to implement these recommendations. Responsibility for secure operation lies with the user or system integrator. **If you are uncertain about planning or implementing security measures, we strongly recommend consulting a qualified IT security expert or system integrator. Professional guidance can help minimize risks and ensure a security architecture tailored to your environment.**