Recommended Security Settings for SEH deviceserver

Optimal Configuration for Maximum Security and Compliance

Modern corporate networks place high demands on security—especially when it comes to embedded devices such as USB device servers. The SEH device server family (utnserver Pro, utnserver ProMAX, dongleserver Pro, dongleserver ProMAX, INU-100, and INU-50) offers comprehensive security features. By configuring them appropriately, these devices can be reliably integrated into existing security policies and pass security and vulnerability scans without false alarms.

1. Secure the Web Interface

The web interface is the device's central management point and must be properly secured.

- **Use strong passwords:** Each user account (Admin, USB Manager, Read-only user) should have a unique, secure password.
- **Allow HTTPS only:** Disable HTTP access and enforce HTTPS as the default.
- **Use valid certificates:** Replace self-signed certificates with trusted ones (e.g., via corporate CA) to ensure authenticity and trust.
- **Restrict access:** Allow access to the web interface only from trusted management networks or disable it entirely if not needed.

2. Encrypt USB Communication

Communication between the device server and SEH UTN Manager should always be encrypted.

- **Enable TLS encryption:** Activate this feature to protect all USB data transfers.

3. Secure or Disable SNMP

SNMP is often used for monitoring but can pose a security risk in outdated versions.

- **Disable SNMPv1:** It transmits data unencrypted and is unsuitable for modern environments.
- **Use SNMPv3:** If SNMP is required, use SNMPv3 with authentication and encryption.
- **Disable SNMP entirely** if it's not used for monitoring.

4. Disable Bonjour (mDNS)

Bonjour (mDNS) enables automatic device discovery but also exposes device information.

- **Disable** if not strictly necessary—especially in security-sensitive networks.

5. Optimize TLS Configuration

Ensure encryption for both management and device data adheres to current standards.

- **Prefer TLS 1.3:** Enable to use state-of-the-art encryption and performance.
- **Allow TLS 1.2 only as fallback** for legacy clients.

6. Network Access and Segmentation

Network access control adds an extra layer of security.

- **Use 802.1X authentication:** Prevents unauthorized devices from accessing the network (e.g., via RADIUS).
- **Implement VLANs:** Segment devices logically and securely from other parts of the network.

7. USB Port and Device Management (Optional, but Recommended)

- **Disable unused USB ports.**
- **Device binding:** Assign USB devices to specific ports based on PID/VID.
- **Access control and scheduling:** Define who can use ports and when.
- **Device type filtering:** Block specific device types, e.g., HID (keyboards/mice).

8. Enable Monitoring, Logging, and Notifications

Active monitoring helps to detect unwanted activities at an early stage.

- **Use integrated monitoring features** to detect critical events such as unauthorized access or configuration changes.
- **Enable logging** to record relevant system and access events.
- **Configure notification features** such as email or SNMP traps to be alerted immediately of security-related events.

9. Minimize Attack Surface

Following the principle of "less is more":

- **Disable all unused protocols and services** (e.g., SNMP, Bonjour, unused USB ports).
- **Only enable features that are actively in use—**this reduces the potential attack surface.

Summary – Recommendations at a Glance

Measure	Recommendation
Web Interface	Use strong passwords, enable HTTPS, restrict access
SNMP	Disable SNMPv1, use SNMPv3 if needed, or disable SNMP entirely
Bonjour (mDNS)	Disable (enable only if strictly required)
USB Communication	Enable TLS encryption for USB communication
General Encryption	Use TLS 1.3 as the standard
Authentication	Use 802.1X (optional, recommended)
Network Segmentation	Use VLANs to assign USB devices to isolated subnetworks
USB Port Management	Disable unused ports
Monitoring	Enable logging and notifications
Protocol/Service Control	Only keep necessary services active

Conclusion

SEH device servers offer a wide range of security functions that can be flexibly tailored to meet the requirements of modern IT environments. Through consistent configuration—as described in this article—devices can be effectively secured, attack surfaces minimized and security checks passed. These recommendations ensure that your devices can be operated reliably and securely in both traditional enterprise networks and sensitive environments.