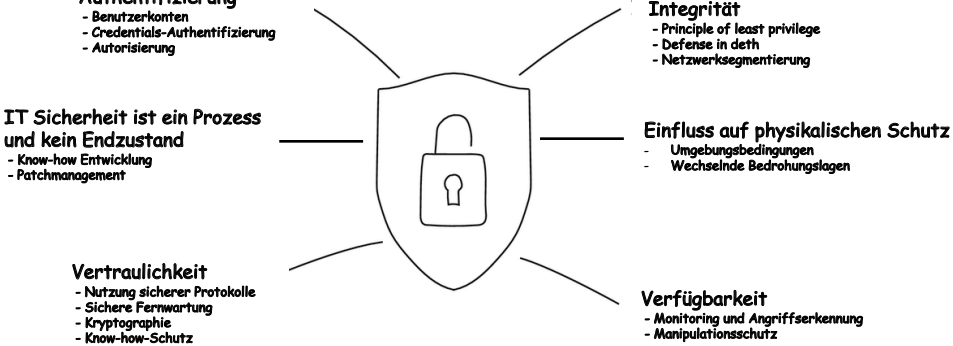
Secure configuration – 11 basic steps



Funktionsübersicht

Konfiguration

- Web-based management (HTTP/HTTPS)
- Smart mode-Button
- CLI (Telnet/SSH)
- SNMPv1/v2/v3
- SD-Karte

IP-Adressvergabe

- BootP
- DHCP Client
- Address Conflict detection

Datenübertragung

- Jumbo Frames (nur Gigabit-Varianten)**
- Flow control

Diagnose

- N:1-Port mirroring
- Event Table
- RMON
- SNMPv1/v2/v3

Redundanz

- RSTP (IEEE802.1w)
- MRP Client

PROFINET

- Quality of Service (IEEE 802.1p, 8 queues)
- LLDP
- MRP Client
- Hardware-basierte Priorisierung

Multicast-Filter / EtherNet/IP

- IGMP Snooping/Querier
- Multicast Source Detection
- Auto Query Port

Zeitsynchronisierung

- SNTP*

Security

- SSH/HTTPS

Priorisierung

- Quality of Service (IEEE 802.1p, 8 queues)
- Port-Priorisierung (IEEE 802.1D/p)

Segmentierung

- VLANs (IEEE 802.1Q)

* Ergänzt mit FW2.60
** Ergänzt mit FW2.70

Funktionsübersicht

Konfiguration

- Web-based management (HTTP/HTTPS)
- Smart mode-Button
- CLI (Telnet/SSH)
- SNMPv1/v2/v3
- SD-Karte

IP-Adressvergabe

- BootP
- DHCP Client/**Server/Relay Agent (option82)**
- **DCP***
- Address Conflict detection

Datenübertragung

- Jumbo Frames (nur Gigabit-Varianten)**
- Flow control

Diagnose

- N:1-Port mirroring
- Event Table
- RMON
- SNMPv1/v2/v3

Redundanz

- RSTP (IEEE802.1w)
- **Fast Ring Detection**
- **Large Tree Support**
- MRP Client/**Server** (IEC 62439)

PROFINET

- Quality of Service (IEEE 802.1p, 8 queues)
- **DCP***
- LLDP
- **PROFINET device***
- MRP Client/**Server** (IEC 62439)
- Hardware-basierte Priorisierung

Multicast-Filter / EtherNet/IP

- IGMP Snooping/Querier
- Multicast Source Detection
- Auto Query Port

Zeitsynchronisierung

- SNTP*

Security

- SSH/HTTPS
- **MAC-based port security****
- **RADIUS authentication****

Priorisierung

- Quality of Service (IEEE 802.1p, 8 queues)
- Port-Priorisierung (IEEE 802.1D/p)

Segmentierung

- VLANs (IEEE 802.1Q)

* Ergänzt mit FW2.60
** Ergänzt mit FW2.70

Security für industrielle Switche - Minimalkonfigurationen

Security is not a goal, it‘s a Livestyle.

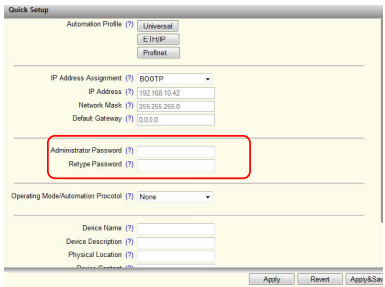
➢ **Daher gilt grundsätzlich:**

- ☑ Prüfen Sie alle Updates und Patches für das Betriebssystem und die Dienste.
- ☑ Deaktivieren Sie nicht verwendete Router/Switch-Schnittstellen.
- ☑ Deaktivieren Sie alle nicht genutzten Dienste.
- ☑ Deaktivieren Sie Verwaltungsprotokolle, die Sie nicht verwenden.
- ☑ Deaktivieren Sie Funktionen, die Techniken zur Umleitung Ihres Datenverkehrs sind.
- ☑ Prüfen Sie die Sicherheit der Terminalverbindungen.
- ☑ Kontrolle der Kennwortrichtlinien für alle zur Authentifizierung erforderlichen Dienste.
- ☑ Nutzen Sie SNMP v3.
- ☑ Verwendung von HTTPs anstelle von HTTP.
- ☑ Entfernen von unsicheren Diensten wie Telnet.

1. Schritt – Default Passwort

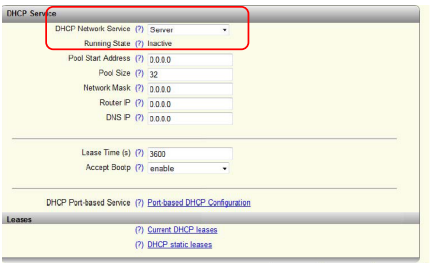
- Veränderung des Default Passwortes
  - Im Auslieferungszustand* ist der Benutzername „admin“ und das Passwort „private“.
  - Angreifer versuchen einen Zugriff über bekannte Default Passwörter oder unsichere Passwörter (*z.B. PW01; PW02 etc.*)
  - ➢ Sofortiger Änderung bei der Installation.
  - ➢ Die minimale Passwortlänge beträgt 8 Zeichen.

** Das Default Passwort ist im Handbuch aufgeführt und somit für jeden zugänglich!*



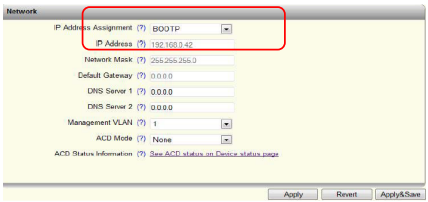
2. Schritt – DHCP

- DHCP deaktivieren
  - DHCP ist ein aktiver Dienst und dient dem Empfang dynamischer IP Informationen.
  - Dynamische Informationen erfordern Kommunikation.
  - Angreifer können diesen Dienst missbrauchen.
  - ➢ Arbeit mit statischen IP Adressen
  - DHCP Network Service: Wählen Sie hier den DHCP-Service, den Sie nutzen möchten.
    - None: Es wird kein DHCP Service auf dem Switch verwendet.
    - Relay Agent: Der DHCP Relay Agent (DHCP Option 82) wird eingeschaltet.
    - Server: Der Switch wird als DHCP-Server eingesetzt.



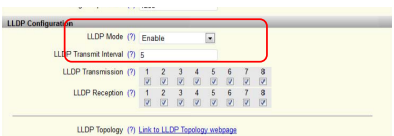
3. Schritt – BOOTP

- BOOTP deaktivieren
  - BOOTP ist ein aktiver Dienst und dient dem Empfang dynamischer IP Informationen.
  - Dynamische Informationen erfordern Kommunikation.
  - Angreifer können diesen Dienst missbrauchen.
  - ➢ Arbeit mit statischen IP Adressen
  - Bei Einstellung „STATIC“ folgende Einstellungen:
  - IP Adresse: Stellen Sie die gewünschte IP-Adresse ein.
  - Network Mask: Stellen Sie hier die gewünschte Subnetzmaske ein.
  - Default Gateway: Stellen Sie hier das Default Gateway ein.



4. Schritt – LLDP

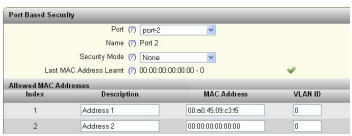
- LLDP deaktivieren
  - Die FL SWITCH 2200/2300 sind für den Einsatz auch in der PROFINET oder Ethernet/IP designt.
  - Das Link Layer Discovery Protokoll dient der Nachbarschaftserkennung.
  - Der Switch sendet regelmässig Informationen über sich.
  - Angreifer können Hinweise erhalten.
  - ➢ Nur aktivieren bei Profinet oder Ethernet/IP Modus oder bei der Verwendung von Netzwerkmonitoring Tools wie den FL Network Manager.



5. Schritt - Port-based Security

- MAC Adress Binding
  - Pro Port können bis zu 50 MAC-Adressen erlaubt werden.
  - Jede MAC-Adresse kann nur auf einem Port erlaubt werden.
  - ➢ MAC-Adressen, welche auf einem Port erlaubt werden, können auch nicht dynamisch an anderen Ports gelernt werden.
  - ➢ Somit ist ein Zugriff auf das web-based Management oder das Netzwerk über eine, an einem anderen Port erlaubte MAC-Adresse, nicht möglich*.

** ab FW 2.90*

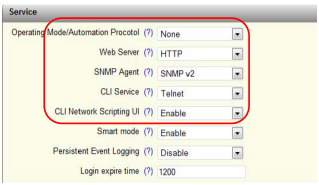


6. Schritt - Remote Access Protocol

- Telnet Protokoll deaktivieren/ SSH Aktivieren*
  - Im Auslieferungszustand ist CLI (Telnet) aktiviert.
  - ➢ Telnet hat keine Sicherheitsfeatures.
  - ➢ Passwörter werden im Klartext übertragen.

  * *Sichere Verbindung für CLI: SSH*
- HTTPS (*Hypertext Transfer Protocol Secure* [*TCP Port 443*]) auswählen
  - ➢ HTTP (*TCP Port 80*) ist unverschlüsselt mit wenigen Sicherheitsfeatures.
  - ➢ Transportmechanismus für Angriffe und Würmer*.

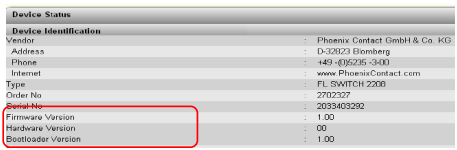
  * *z. B. Man-in-the-Middle Angriffe*



7. Schritt - Firmware

- Stand der Firmware prüfen
  - Veraltete Firmware ist ein offenes Tor für Angreifer.
  - ➢ Neue Firmware zeitnah installieren.

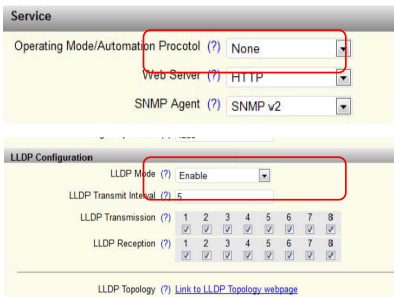
** Die neueste Firmware finden Sie im E-Shop von Phoenix Contact als Anhang an die entsprechenden Artikel.*



8. Schritt - PROFINET

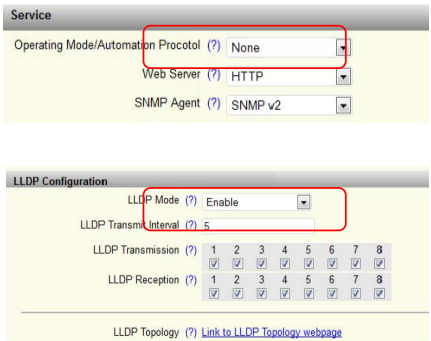
- Profinet deaktivieren
  - Die Seite „Profinet Configuration“ ist nur bei aktiviertem PROFINET-Mode sichtbar.
  - Via LLDP können Konfigurationseigenschaften des Switches ausgelesen werden.
  - ➢ Nach Rücksetzung in den Standardmodus* bleibt LLDP eingeschaltet.
  - ➢ LLDP deaktivieren und Switch neu starten.

** LLDP ist per Default auch im Standardmodus (Auslieferungszustand) aktiviert.*



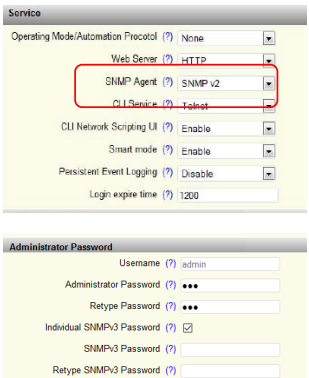
9. Schritt - Ethernet/IP

- Ethernet/IP deaktivieren
  - Die Seite „Ethernet/IP Configuration“ ist nur bei aktiviertem Ethernet/IP-Mode sichtbar.
  - Über Ethernet/IP können für Asset Management Systeme relevante Daten selbständig identifiziert und ausgelesen werden.
  - ➢ Nur aktivieren wenn benötigt.



10. Schritt - SNMP

- SNMP v3 aktivieren
  - SNMP bietet Netzwerkverwaltungsdienste zwischen einer zentralen Verwaltungskonsole (*Manager*) und Netzwerkgeräte wie Switche (*Agenten*).
  - ➢ SNMP v3 ist gesichertes Protokoll.
  - ➢ Schreib- und Leserechte sind via Passwort geschützt.
  - ➢ Passwort mind. 8 Zeichen.

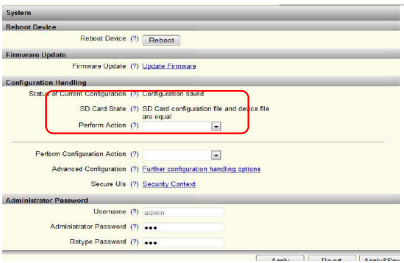


11. Schritt - SD-Karte

- Booten von SD-Karte deaktivieren
  - Die SD-Karte ermöglicht eine schnelle Konfiguration bei einem Gerätetausch.
  - ➢ Deaktivierung* beschleunigt Booten.

- Booten von SD-Karte aktiviert
  - ➢ Alarmtrap „Eventstatus fehlender Konfigurationsspeicher“ setzen.
  - ➢ Relaiskontakt schalten.
  - ➢ Alarm via Konfigurationstool „FL Manager Basic“.

  ** ab FW 2.90*



Phoenix Contact bietet 360° Security für den Rundum-Schutz

PHOENIX CONTACT AG
Zürcherstrasse 22
8317 Tagelswangen
Tel.: 052 354 55 55
Fax: 052 354 56 99
E-Mail: infoswiss@phoenixcontact.com
phoenixcontact.ch

INSPIRING INNOVATIONS