



Empfehlung für die sichere Einstellung von Nexans Switches mit Firmware V7.04 oder höher

KD975D13

INHALT

1. Empfehlung für die sichere Einstellung.....	2
1.1. Gegenüberstellung des Default- und Secure-Betriebsmodus.....	2
1.2. Einzelkonfiguration der sicherheitsrelevanten Parameter.....	2
1.3. Aktivierung einer sicheren Access Policy per Konfiguration	3
1.4. Aktivierung einer sicheren Access Policy per DIP Schalter	3
1.5. Weitere sicherheitsrelevante Einstellungen	4
2. Liste der verwendeten Ports beim Secure Mode	6
2.1. Port 22 TCP (SSH - Secure Shell)	6
2.2. Port 50271 TCP (SCP - Secure Copy).....	7
2.3. Port 443 TCP (HTTPS)	8
2.4. Port 123 UDP (SNTP)	10
2.5. Port 161 UDP (SNMPv3).....	11
2.6. Port 514 UDP (Remote SYSLOG) und Local Logging.....	13
2.7. Port 50266/50268 UDP (Switch Manager NexManV3).....	14

1. Empfehlung für die sichere Einstellung

1.1. Gegenüberstellung des Default- und Secure-Betriebsmodus

Der Secure-Betriebsmodus des Switches kann über folgende Methoden aktiviert werden:

- Einzelkonfiguration der sicherheitsrelevanten Parameter
- Aktivierung des Secure-Betriebsmodus per Konfigurationseinstellung „Access Policy“
- Aktivierung des Secure-Betriebsmodus per DIP Schalter

Diese Methoden werden in den folgenden Kapiteln detailliert beschrieben.

Die folgende Tabelle zeigt eine Gegenüberstellung der sicherheitsrelevanten Parameter beim Default- bzw. Secure Betriebsmodus:

Funktion	Default-Betriebsmodus	Secure-Betriebsmodus
Telnet	Aktiviert	Deaktiviert
SSH	Aktiviert	Aktiviert und Clients sollten die Elliptic Curve Key Exchange Methode verwenden.
HTTP	Aktiviert	Deaktiviert
HTTPS	Aktiviert	Aktiviert
SNMP Access	SNMPv1	SNMPv3-SHA1-AES128
Manager Access	Secure Copy - SCP	Secure Copy - SCP
Password strength checker	Deaktiviert	Aktiviert
Password Encryption Mode	Standard	SHA256 Hash

1.2. Einzelkonfiguration der sicherheitsrelevanten Parameter

Bei der Einzelkonfiguration der sicherheitsrelevanten Parameter müssen unsichere Protokolle und Konfigurationsschnittstellen separat deaktiviert werden.

Abweichend von dem Default-Betriebsmodus sollten folgende Einstellungen vorgenommen werden:

a) TELNET abschalten

CLI Kommando:
`config telnet-auth-mode disable`

b) HTTP abschalten

CLI Kommando:
`config web-auth-mode disable`

c) SNMP Zugriff ausschließlich via SNMPv3-SHA1-AES128

CLI Kommando:
`config snmp-protocol-version v3-aes-auth-sha`

Hinweis: Per Factory Default sind keine SNMPv3 Accounts konfiguriert, d.h., dass weder Read/Only not Read/Write Zugriffe per SNMPv3 möglich sind.

d) Manager Authentifizierung und Dateitransfer ausschließlich via Secure Copy Protocol (SCP)

Dadurch werden die UDP-Authentifizierung und der TFTP-Server im Switch deaktiviert.

Bei deaktiviertem TFTP-Server kann alternativ per CLI Kommando ein TFTP-Transfer ausgeführt werden (über den integrierten TFTP-Client). Dies ist allerdings erst möglich, nachdem sich der User erfolgreich an der CLI Console authentifiziert hat.

CLI Kommando:
`config manager-auth-mode scp`

e) Password Strength Checker aktivieren

Durch Aktivierung des "Password Strength Checker" kann der Switch erst dann administriert werden, wenn das Factory-Default Passwort in ein sicheres Passwort geändert wurde.

Als sicher eingestuft werden Passwörter, die die folgenden Kriterien erfüllen:

8...14 Zeichen mit mindestens:

einem Kleinbuchstaben: a-z

einem Großbuchstaben: A-Z

einer Zahl: 0-9

einem Sonderzeichen: .,;!'"%#\$%^~@*:+-=_/\|`()[]{}<>

CLI Kommando:

```
set password-strength enabled
```

f) Password Encryption Mode auf SHA256 Hash einstellen

Bei dieser Einstellung werden die Passwörter der beiden Local Accounts ausschließlich als SHA256 Hash gespeichert. Sofern die Komplexität der Passwörter ausreichend hoch ist (mindestens 8 Zeichen, empfohlen werden 12 Zeichen), ist bei einer Kompromittierung des Hash Wertes ein Rückschluss auf das Passwort praktisch unmöglich.

CLI Kommando:

```
set password-encryption sha256-hash
```

1.3. Aktivierung einer sicheren Access Policy per Konfiguration

Alle im Kapitel 1.2. aufgeführten Einzelkonfigurationen können alternativ durch die Aktivierung der Access Policy "Allow secure protocols and passwords only" erzwungen werden.

Das CLI Kommando lautet:

```
config global-security mode enabled
```

Eine Umkonfiguration der in Kapitel 1.2.aufgeführten Einzelparameter ist nicht möglich solange die Access Policy aktiviert ist.

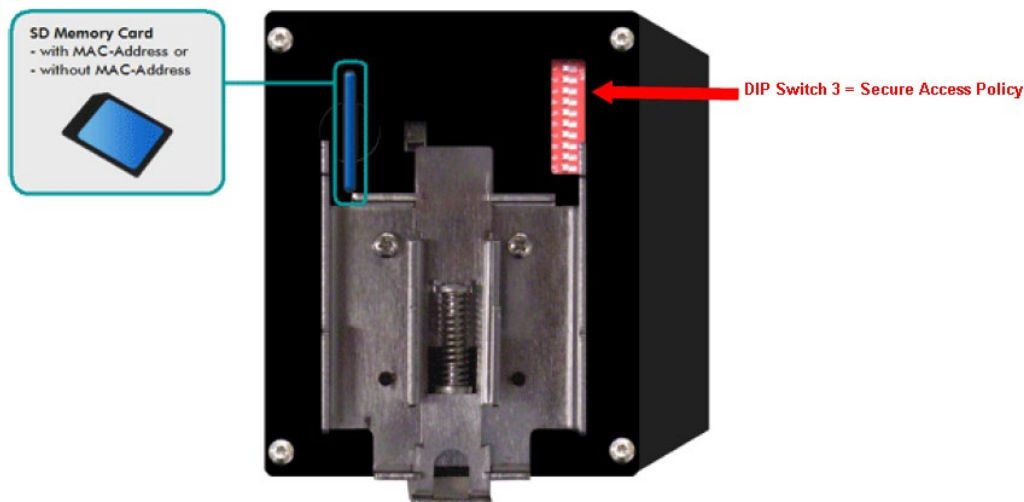
1.4. Aktivierung einer sicheren Access Policy per DIP Schalter

Die Access Policy "Allow secure protocols and passwords only" kann alternative per DIP Schalter erzwungen werden.

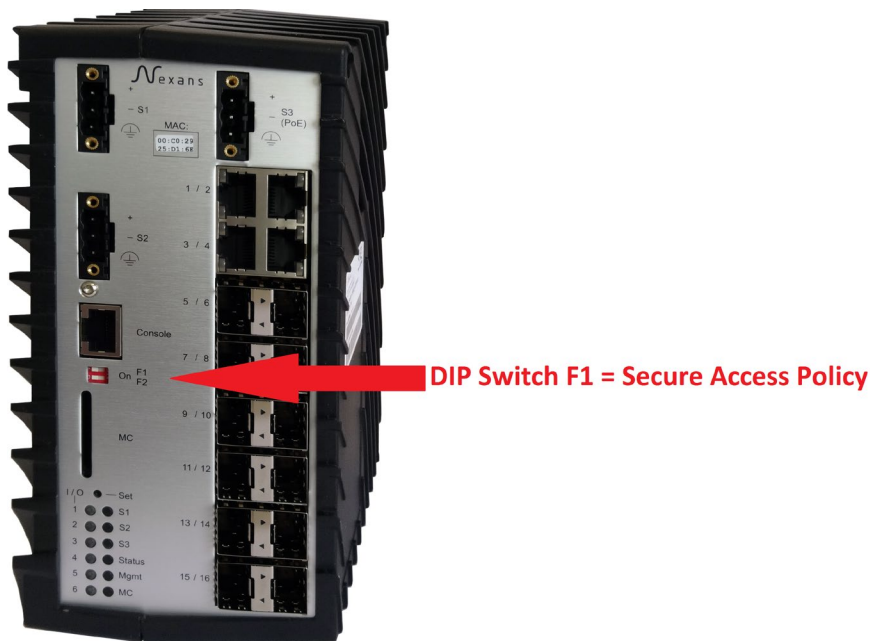
Bei Aktivierung durch den DIP-Schalter, kann die Access Policy (und somit auch alle Einzelparameter) per Software nicht umkonfiguriert werden.

Dieser DIP-Schalter ist z.Z. ausschließlich bei Industrie Switchen verfügbar und befindet sich auf der Rück- bzw. Frontseite des Gehäuses.

Position des DIP Schalters bei 54X, 74X und 104X Industrie Switchen:



Position des DIP Schalters bei 16XX Industrie Switchen:



1.5. Weitere sicherheitsrelevante Einstellungen

Die folgenden Parameter gehören nicht zu den zwingend erforderlichen Sicherheitseinstellungen. Eine Konfiguration dieser Parameter erhöht jedoch zusätzlich die Sicherheit:

a) Das WEB HTTPS Interface auf Read/Only konfigurieren

Das WEB Interface ist primär als Diagnose Interface konzipiert und sollte nur in Ausnahmefällen zur Konfiguration des Switches verwendet werden. Durch konfigurieren des „WEB Authentication Mode“ auf Read/Only kann verhindert werden, dass Konfigurationsänderung per WEB vorgenommen werden. Selbst beim Einloggen mit dem Admin Account ist dann kein Schreibzugriff möglich.

CLI Kommando:

```
config web-auth-mode read-only
```

b) Das WEB HTTPS Interface für TLS 1.2 konfigurieren

Das HTTPS Interface unterstützt per Factory Default die Protokolle TLS 1.0, 1.1 und 1.2. Gemäß BSI wird jedoch empfohlen, ausschließlich TLS 1.2 zu verwenden. Der integrierte HTTPS Server kann daher so konfiguriert werden, dass er ausschließlich TLS 1.2 zulässt.

CLI Kommando:

```
config tls 1.2
```

c) Accessliste anlegen

Mit dieser Einstellung können nur zugelassene Management Stationen auf den Switch zugreifen.

CLI Kommando (hier im Beispiel die IP Adressen von 11.222.3.4 bis 11.222.3.6):

```
accesslist 1 11.222.3.4 11.222.3.6 read-write
config accesslist-mode all
```

d) Das Senden von Life- und Autodiscovery Paketen abschalten

Dadurch werden weder periodische Life Pakete gesendet, noch antwortet der Switch auf Layer-2 Autodiscovery Anfragen des Managers. Somit ist ein Autodiscovery nur noch auf Layer-3 möglich.

CLI Kommando:

```
config lifepacket-rate all-disabled
```

e) Das Lesen des Switches durch den Basic Configurator unterbinden

Dies unterbindet, dass der Switch auf Layer-2 Anfragen des Basic Configurators antwortet und dieser die Basis Konfiguration (Name, Location, Contact, IP Adresse, Netzmaske und Gateway) auslesen kann.

CLI Kommando:

```
config basic-configurator disable
```

f) Das Speichern der Switch Konfigurationen in der Database des Managers deaktivieren

Dadurch wird verhindert, dass binäre und CLI Konfigurationen in der Database gespeichert werden. Dies ist insbesondere dann sinnvoll, wenn aus Sicherheitsgründen die Konfiguration des Switches nicht auf einem Datenträger gespeichert werden darf.

Manager Device-List Menü:

Preferences > Global > Don't save Config to Database

g) Den Memory Card Mode auf AES-256 encryption konfigurieren

Bei Aktivierung wird die komplette Switchkonfiguration mit einer AES-256 Verschlüsselung auf die Memory Card abgespeichert. Dies verhindert somit jegliches Auslesen der Switchkonfiguration durch beliebige SD-Card Lesegeräte.

CLI Kommando:

```
config memory-card-mode aes-256-enabled
```

2. Liste der verwendeten Ports beim Secure Mode

2.1. Port 22 TCP (SSH - Secure Shell)

Der Switch kann über jeden Standard SSHv2 Client angesprochen werden. Dabei können alle Parameter des Switches ausnahmslos per SSHv2 konfiguriert werden.

Das gleichzeitige öffnen mehrerer SSH, Telnet bzw. V.24 Konsole Sessions ist aus Sicherheitsgründen nicht möglich.

Ferner werden nach dreimaliger falscher Eingabe von Name oder Passwort, alle Konsole Interfaces (SSH, TELNET und V.24) für 60 Sekunden gesperrt.

Es wird ausschließlich SSH Version 2 unterstützt und im Auslieferungszustand ist bereits ein individuell generierter RSA und ECC Server Key vorinstalliert.

WICHTIG: Es wird dringend empfohlen, dass Clients die untenstehende Methode zum Austausch von Schlüsseln mit elliptischen Kurven (ecdh-sha2-nistp256) und den Algorithmus (ecdsa-sha2-nistp256) verwenden, die einen zukunftssicheren verschlüsselten Zugriff gewährleisten und einen deutlich schnelleren SSH- und SCP-Verbindungsaufbau ermöglichen. Die RSA-Methode ist nur aus Gründen der Abwärtskompatibilität mit alten SSH-Clients implementiert.

Folgende Schlüssel Austausch Methoden werden unterstützt:

- ecdh-sha2-nistp256
- diffie-hellman-group14-sha1
- diffie-hellman-group1-sha1

Folgende Server Key Algorithmen werden unterstützt:

- ecdsa-sha2-nistp256 (256 Bit ECC key)
- ssh-rsa (1024 Bit RSA Key)

Folgende Encryption Methoden werden unterstützt:

- aes256-ctr
- aes128-ctr
- aes256-cbc
- aes128-cbc

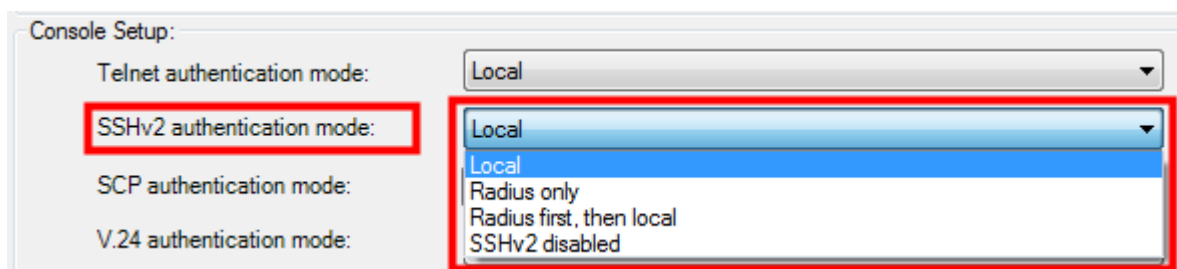
Folgende Hash Methoden werden unterstützt:

- hmac-sha2-256
- hmac-sha2-512

Über den "SSH Authentication Mode" ist es möglich, SSH und den betreffenden Port abzuschalten.

Hier stehen folgende Modi zur Verfügung:

- Local: Authentifizierung über lokale Benutzernamen und Passwörter
- Radius only: Authentifizierung ausschließlich durch den RADIUS Server
- Radius first, then local: Authentifizierung durch RADIUS, nur falls kein Server antwortet: lokale Authentifizierung
- SSHv2 disabled: SSH Interface abgeschaltet



Zusätzlich kann über eine IP Access-List der Zugriff auf den SSH-Server auf bestimmte IP-Adressen oder IP-Ranges eingeschränkt werden.

2.2. Port 50271 TCP (SCP - Secure Copy)

Der Switch kann über jeden Standard SCP Client angesprochen werden.

Mittels SCP könnten folgende Daten aus dem Switch gelesen werden:

- CLI Konfiguration (nur mit Parametern die von Factory Default abweichen)
- CLI Konfiguration (mit allen Parametern)
- Binäre Konfiguration (wird primär vom Manager verwendet)
- Lokales Logbuch

Folgende Daten können per SCP in den Switch geschrieben werden:

- CLI Konfiguration mit Reset auf Factory Default
- CLI Konfiguration ohne Reset auf Factory Default
- Binäre Konfiguration (wird primär vom Manager verwendet)
- Firmware Image mit sofortigem Start des Updates
- Firmware Image mit zeitverzögertem Update via Time Client
- Customer Default Konfiguration
- Customer Reboot Konfiguration

Ferner werden nach dreimaliger falscher Angabe von Name oder Passwort, alle Konsole Interfaces (SCP, SSH, TELNET und V.24) für 60 Sekunden gesperrt.

SCP unterstützt ausschließlich die SSH Version 2 und verwendet die selben Algorithmen wie SSH, siehe Kapitel „Port 22 TCP (SSH - Secure Shell)“.

Über den "SCP Authentication Mode" ist es möglich, SCP und den betreffenden Port abzuschalten. Hier stehen folgende Modi zur Verfügung:

- Local: Authentifizierung über lokale Benutzernamen und Passwörter
- Radius only: Authentifizierung ausschließlich durch den RADIUS Server
- Radius first, then local: Authentifizierung durch RADIUS, nur falls kein Server antwortet: lokale Authentifizierung
- Use SSHv2 mode: SCP verwendet dieselben Einstellung wie der „SSHv2 authentication mode“
- SCP disabled: SCP Interface abgeschaltet

Console Setup:

Telnet authentication mode:	Local
SSHv2 authentication mode:	Local
SCP authentication mode:	Use SSHv2 mode
V.24 authentication mode:	Local
Console password mode:	Use SSHv2 mode

The dropdown menu for SCP authentication mode is expanded, showing the following options: Local, Radius only, Radius first, then local, Use SSHv2 mode (highlighted), and SCP disabled.

Zusätzlich kann über eine IP Access-List der Zugriff auf den SCP-Server auf bestimmte IP-Adressen oder IP-Ranges eingeschränkt werden.

2.3. Port 443 TCP (HTTPS)

Der HTTPS Zugriff auf den Switch ist mit jedem Standard Web-Browser möglich. Dabei wird außer HTML, keine weitere Sprache verwendet (wie z.B. JavaScript).

Über den HTML Code "autocomplete='off'" wird verhindert, dass der WEB-Browser die Passwörter speichert.

Die Session zwischen Switch und WEB Browser wird über die IP Adresse des WEB Browsers und zusätzlich über eine, beim Login erzeugte, 32stellige hexadezimale Zufallszahl abgesichert.

Beim Login werden der Name und das Passwort per POST-Methode übermittelt, so dass diese, aufgrund der SSL Verschlüsselung, weder im Browser noch per Sniffer mitlesbar sind.

Auf den Switchen ist ein von Nexans Advanced Networking Solutions CA (Nexans-ANS CA) signiertes Zertifikat installiert (RSA, 1024 Bit Key (HW3) or 3072 Bit Key (HW5), SHA-256).

Das zur Signierung verwendete Nexans CA Zertifikat ist auf der Support Seite von Nexans verfügbar. Dieses CA Zertifikat kann in den verwendeten WEB-Browser als Stammzertifikat importiert werden um die Sicherheitswarnungen beim ersten Aufruf jedes Switches zu umgehen. Dabei ist jedoch zu beachten, dass der Aufruf des Switches nicht über die IP Adresse erfolgt (dies ist eine grundsätzliche Beschränkung des HTTPS Zertifikatkonzeptes), sondern über einen symbolischen Namen. Dieser Name muss entweder durch einen DNS-Server oder durch die hosts Datei in die entsprechende IP Adresse aufgelöst werden. Auf allen Nexans Switchen ist ein identisches Zertifikat installiert, das für den symbolischen Namen `*.switch.nexans` signiert wurde. Der * darf dabei durch einen beliebigen Switchnamen (der allerdings keinen „.“ enthalten darf) ersetzt werden damit der Browser das Switch-Zertifikat als gültig ansieht.

Die folgenden Verschlüsselungsprotokolle werden unterstützt:

- TLS1.0, TLS1.1, TLS1.2

Dabei kann die minimal erlaubte TLS Protokoll Version für den Zugriff per HTTPS kann konfiguriert werden.

Hier stehen folgende Modi zur Verfügung:

- Allow TLS 1.0 or higher: TLS 1.0, 1.1 und 1.2 sind zulässig
- Allow TLS 1.1 or higher: TLS 1.1 und 1.2 sind zulässig
- Allow TLS 1.2 or higher: Ausschließlich TLS 1.2 ist zulässig

HTTPS authentication mode: Local

HTTPS TCP Port: 443 (1..65535) [443]

Allowed TLS Versions: Allow TLS 1.2 and higher

Die folgenden Cipher Suites werden für Switches mit Management Hardware HW3 unterstützt:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Die folgende Cipher Suite wird für Switches mit Management Hardware HW5 unterstützt:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

Über den "HTTPS Authentication Mode" ist es möglich, HTTPS und den betreffenden Port abzuschalten.

Ferner kann der Mode auf Read/Only eingestellt werden, so dass auch bei Verwendung des Read/Write Accounts kein Schreibzugriff möglich ist.

Hier stehen folgende Modi zur Verfügung:

- Local: Authentifizierung über lokale Benutzernamen und Passwörter
- Read/Only: Lokale Authentifizierung, ausschließlich Read/Only Zugriff erlaubt
- Disabled: HTTPS Interface abgeschaltet

Refresh rate for State pages: 5 seconds

HTTP authentication mode: HTTP disabled

HTTP TCP port: 80 (1..65535) [80]

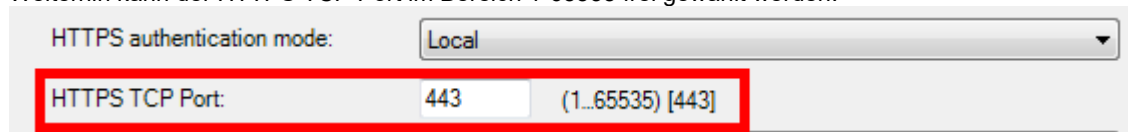
HTTPS authentication mode: Local

HTTPS TCP Port: []

TFTP Setup

Nach dreimaliger falscher Eingabe von Name oder Passwort, werden alle WEB Interfaces (HTTP und HTTPS) für 60 Sekunden gesperrt.

Weiterhin kann der HTTPS TCP Port im Bereich 1-65535 frei gewählt werden:

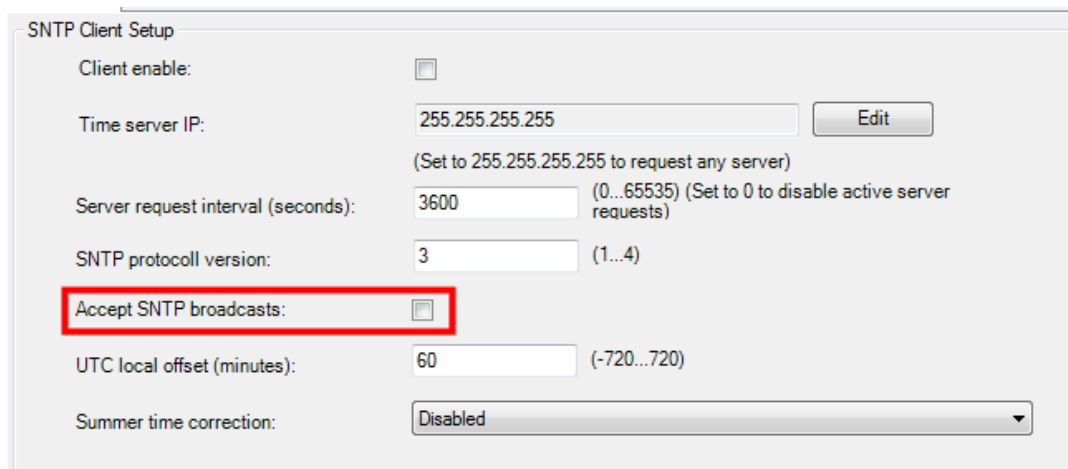


The screenshot shows a configuration panel with two main sections. The top section is labeled 'HTTPS authentication mode:' and contains a dropdown menu with 'Local' selected. The bottom section is labeled 'HTTPS TCP Port:' and contains a text input field with '443' and a range indicator '(1..65535) [443]'. A red rectangular box highlights the 'HTTPS TCP Port' section.

Zusätzlich kann über eine IP Access-List der Zugriff auf den HTTPS-Server auf bestimmte IP-Adressen oder IP-Ranges eingeschränkt werden.

2.4. Port 123 UDP (SNTP)

Der SNTP Port ist per Factory-Default gesperrt. Er wird nur dann geöffnet, wenn bei der SNTP Konfiguration der Empfang von SNTP Broadcasts erlaubt wird:



SNTP Client Setup

Client enable:

Time server IP:
(Set to 255.255.255.255 to request any server)

Server request interval (seconds): (0.. 65535) (Set to 0 to disable active server requests)

SNTP protocol version: (1...4)

Accept SNTP broadcasts:

UTC local offset (minutes): (-720...720)

Summer time correction:

2.5. Port 161 UDP (SNMPv3)

Folgendes SNMP Protokoll wird im Secure Mode unterstützt:

- SNMPv3 Auth.-SHA Priv.-AES-128

Folgende Encryption Methode wird hierbei unterstützt:

- aes-128-cfb

Folgende Hash Methoden wird hierbei unterstützt:

- hmac-sha1-96

Für den Zugriff per SNMPv3 können die User Credentials für den Read/Write, Read/Only und Flexible Zugriff konfiguriert werden:

The screenshot shows a configuration page with four distinct sections for setting up different types of SNMPv3 accounts:

- SNMPv3 Read/Write Account Setup:** Includes fields for Username, Authentication password, and Privacy password, with an 'Edit SNMPv3 Account' button.
- SNMPv3 Read/Only Account Setup:** Includes fields for Username, Authentication password, and Privacy password, with an 'Edit SNMPv3 Account' button.
- SNMPv3 Flexible Account Setup:** Includes a dropdown for 'Flexible access mode' (set to 'Read/Only'), and fields for Username, Authentication password, and Privacy password, with an 'Edit SNMPv3 Account' button.
- SNMPv3 Trap Account Setup:** Includes fields for Username, Authentication password, and Privacy password, with an 'Edit SNMPv3 Account' button.

Die Passwörter für die Authentifizierung und die Encryption können individuell vergeben werden.

The 'Edit SNMPv3 account' dialog box contains the following fields and constraints:

- Username:** (max 32 chars, empty username will disable account)
- Auth. Password:** (8...32 chars, empty password will disable account)
- Confirm Auth. Password:**
- Privacy Password:** (8...32 chars, leave empty to use Auth. password)
- Confirm Privacy Password:**

Buttons: Save Account, Cancel, Delete Account

Über den "SNMP Access Mode" ist es möglich, SNMP und den betreffenden Port abzuschalten.

Ferner kann der Mode auf Read/Only eingestellt werden, so dass auch bei Verwendung des SNMPv3 Read/Write Accounts kein Schreibzugriff möglich ist.

Hier stehen folgende Modi zur Verfügung:

- Read/Write: Read/Write Zugriff erlaubt
- Read/Only: Ausschließlich Read/Only Zugriff erlaubt
- SNMP disabled: SNMP Interface disabled

The 'SNMP Global Setup' page shows the following configuration:

- SNMP protocol version:** SNMPv3 [Auth.-SHA] [Priv.-AES-128]
- SNMP access mode:** Read/Write (highlighted with a red box, showing a dropdown menu with options: Read/Write, Read/Only, SNMP disabled)
- SNMPv1/v2 Setup:** Read/Only community: public (max 15 chars)

Zusätzlich kann über eine IP Access-List der Zugriff auf den SNMPv3 Agent auf bestimmte IP-Adressen oder IP-Ranges eingeschränkt werden.

2.6. Port 514 UDP (Remote SYSLOG) und Local Logging

Das Versenden von Remote SYSLOG Meldungen via UDP Port 514 ist per Factory-Default deaktiviert und das Local Logging aktiviert.

Folgenden Alarm Meldungen können versenden werden:

- Cold Start
- Link Up
- Link Down
- Link Change
- Internal Voltage Failure
- Temperature Failure
- New MAC Address
- Port Error Counter
- Port Bcast Failure
- Port Loop Detected
- Mgmt Auth. Reject
- Portsecurity Failure
- Radius Mgmt Auth. Reject
- Radius Portsecurity Reject
- Switch PoE Voltage Failure
- Switch PoE Overload
- Port PoE Overload
- Industrial Alarm M1
- Industrial Alarm M2
- RSTP New Root
- RSTP Topology Change
- TFTP Message
- SFP Event
- Client Remove Alarm
- Internal Management Warning

2.7. Port 50266/50268 UDP (Switch Manager NexManV3)

Der Port 50266 und 50268 werden vom Nexans Manager für folgende Funktionen verwendet:

- 50266 Polling des Switchstatus
- 50268 Autodiscovery (separat abschaltbar)
- 50266 Basic Configurator (separat abschaltbar)

Über eine IP Access-List kann der Zugriff auf den Port 50266 und 50268 auf bestimmte IP-Adressen oder IP-Ranges eingeschränkt werden.

Folgende Informationen werden beim Polling des Switchstatus übertragen:

- MC MAC Address
- Active MAC Address
- Device MAC Address
- Alarms
- Redundancy
- PoE
- IP Address
- NameLocation
- Description
- Type
- Mgmt Firmware Version
- Mgmt Hardware Version
- Voice VLAN
- Default VLAN
- Uptime
- Last seen
- Serie/no.
- TP-HEAD Position
- Error Counter
- Link Status
- PoE Spannung pro Port in Volt
- PoE Leistung pro Port in milliWatt
- PoE Eingangsspannung in Volt
- PoE Eingangsleistung in milliWatt
- Die aktuelle Case-Temperatur
- Forwarding State
- Speed-Duplex Mode
- Security Mode
- Trunking Mode
- Power Setup
- Power Limit
- Alarm M1 State
- Alarm M2 State
- Rapid Spanning Tree State
- Systemzeit per SNTP bezogen
- Flow Control State
- Zu viele MAC Adressen
- Security Failure MAC Adresse
- Feste IP eingestellt?
- Anzahl der Events im lokalen Logbuch
- PoE Power Class
- Zeit seit der letzten Linkänderung
- Status des ersten Authenticatin Servers
- Status des zweiten Authenticatin Servers
- Status des ersten Accounting Servers
- Status des zweiten Accounting Servers
- Zeit seit dem letzten Request an den ersten Authenticatin Server
- Zeit seit dem letzten Request an den zweiten Authenticatin Server
- Zeit seit dem letzten Request an den ersten Accounting Server

-
- Zeit seit dem letzten Request an den zweiten Accounting Server
 - MAC Adressen Status
 - Temperatur Status
 - Voltage 1 Wert in Millivolt
 - Voltage 2 Wert in Millivolt
 - Voltage 1 Status
 - Voltage 2 Status
 - Link Down Alarm
 - Power Input S1
 - Power Input S2
 - Function Input State
 - Spanning Tree State
 - Alarm M1 Remote IP
 - Alarm M2 Remote IP
 - Alarm M1 Remote Time
 - Alarm M2 Remote Time
 - Total Boots Device
 - Status des ersten Mgmt Authenticatin Servers
 - Status des zweiten Mgmt Authenticatin Servers
 - Zeit seit dem letzten Request an den ersten Mgmt Authenticatin Server
 - Zeit seit dem letzten Request an den zweiten Mgmt Authenticatin Server

Folgende Informationen werden beim Autodiscovery übertragen:

- Active MAC Address
- Name
- Location
- Description
- Type
- Mgmt Firmware
- Mgmt Hardware
- Uptime
- DHCP an oder aus
- Minimale und Maximale Temperatur die festgestellt wurde
- Erzeugnis Nr.
- Laufende Nummer
- Seriennummer
- Aktuelle Temperatur
- Info ob MAC Adresse von Memory Card oder Switch stammt

Folgende Informationen werden zum Basic Configurator übertragen:

- IP Address
- Netzmaske
- Gateway
- DHCP Enable
- Name
- Location
- Contact
- Firmware Version
- Anzahl Ports
- Management VLAN ID
- Trunk Port Nummer



Nexans Netzwerklösungen befinden sich weltweit im Einsatz und haben Ihre Zuverlässigkeit vielfältig bewiesen. Unsere Referenzen schließen führende Firmen der Welt, Energieversorger, Bahngesellschaften, Flughäfen, industrielle Liegenschaften, Häfen und Wasserstraßen ein. Ein LAN System, das mit den Bedürfnissen seiner Benutzer wachsen kann, muss von Beginn an so flexibel konzipiert sein, dass insbesondere häufige Umzüge, Upgrades und Neugestaltungen unterstützt werden.

**Mit der Erfahrung von mehr als 25 Jahren in der
Entwicklung und Produktion von optischen Lösungen
bieten die Systeme von Nexans die Zuverlässigkeit
und die Sicherheit, die Sie von
Ihrem Netzwerk erwarten.**



Nexans Deutschland GmbH • Advanced Networking Solutions
Bonnenbroicher Str. 2-14 • 41238 Mönchengladbach • Tel (0) 2166 27-2985 • Fax (0) 2166 27-2499
E-Mail: sales.ans@nexans.com • www.nexans.de/ans