Management of Nexans Switches
High Security Configuration Recommendations

Firmware version V7.04 or higher KD975E13

SUMMARY

1. Configuration recommendations

1.1. Comparison of the Secure Mode and the Default Mode

The secure operation mode of the switch can be activated by the following methods:
• Individual configuration of the security-related parameters
• Activation of the secure operating mode via the configuration setting "Access Policy"
• Activation of the secure operating mode via DIP switch

These methods are described in detail in the following chapters.

The table below compares the security-related parameters of the default mode and the secure operation mode:

Function	Default Mode	Secure Operation Mode
Telnet	Activ	Disabled
SSH	Activ	Activ and clients should use elliptic curve key exchange method
HTTP	Activ	Disabled
HTTPS	Activ	Activ
Acces SNMP	SNMPv1	SNMPv3-SHA1-AES128
Acces Manager	Secure Copy - SCP	Secure Copy - SCP
Password strength checker	Disabled	Activ
Password Encryption Mode	Standard	SHA256 Hash

1.2. Configure security-related parameters manually

In case of a manual configuration of the security parameters, it is necessary to deactivate insecure protocols and configuration interfaces one by one.

We recommend that you configure as follows:

a) Deactivate TELNET
CLI Command:
```
config telnet-auth-mode disable
```

b) Deactivate HTTP
CLI Command:
```
config web-auth-mode disable
```

c) Access SNMP only via SNMPv3-SHA1-AES128
CLI Command:
```
config snmp-protocol-version v3-aes-auth-sha
```

Note: For Factory Default configuration, there is no SNMPv3 Account configured: neither Read/Only nor Read/Write is possible via SNMPv3.

d) Manager Authentication and file transfer only via Secure Copy Protcol (SCP)
This disables the UDP authentication and the TFTP server of the switch.
Even the TFTP server is disabled, it is possible to enter a CLI command to do a TFTP transfer (via integrated TFTP-Client). Of course, only if the user has successfully authenticated at the CLI console.
CLI Command:
```
config manager-auth-mode scp
```

e) Activate Password Strenth Checker

By activating "Password Strength Checker", it is necessary to replace Factory-Default password with a secured password before doing any work on the switch.
A secured password must meet the following criteria:
8…14 characters with at least:

one lowercase letter	a-z
one uppercase letter	A-Z
one number	0-9
non-alphanumberic characters	. , ; ! " ' % # $ & ^ ~ @ * : + - = _ / \ | ( ) [ ] { } < >

CLI Command:

```
set password-strength enabled
```

f) Configure Password Encrytion Mode on SHA256 Hash

Thanks to this configuration, the passwords of all local accounts are recorded as SHA256 Hash. If these are complex enough (min. 8 and max.12 characters), it is practically impossible to recover them.
CLI Command:

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

1.3. Activate « Access Policy » mode via software

All the parameters explained in chapter 1.2 can be configured by clicking the "Access Policy" then "Allow secure protocols and passwords only".

CLI Command:

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

As long as this Acces Policy mode is activated, it is no longer available to modify individual parameters that are explained in chapter 1.2.

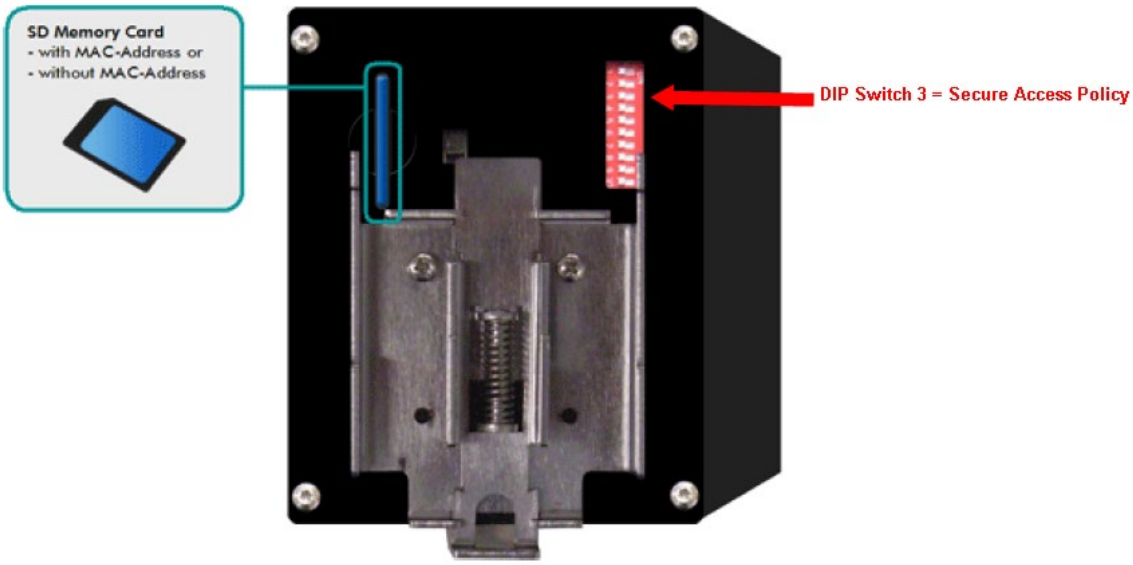
1.4. Activate « Access Policy » mode via DIP-Switch

The "Allow secure protocols and passwords only" mode can also be forced via a DIP-Switch.

When it is activated by the DIP switch, the access policy (also all individual parameters) cannot be reconfigured by the software.

This DIP switch is currently only available for industrial switches and is located on the back of the front side of housing.

Position of the DIP switch on 54X, 74X and 104X Industrial switches:



Position of the DIP switch on 16XX Industrial switches:

1.5. Other security-related parameters

The following parameters are not mandatory for a high degree of security, but can be applicable on a case-by-case basis:

a) Configure the WEB HTTPS interface on Read/Only

The WEB interface is mainly used as a diagnostic interface. In exceptional cases, it can also be used as an alternative tool for the switch configuration. By configuring the mode "WEB Authentication Mode" to Read/Only, we can prevent the configuration changes via WEB interface, even if you are logged in with an Admin account.

CLI Command:

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

b) Configure the WEB HTTPS interface for TLS1.2

The HTTPS interface supports the TLS 1.0, 1.1 and 1.2 protocols by default. According to the BSI, however, it is recommended to only use TLS 1.2. The integrated HTTPS server can therefore be configured so that it only allows TLS 1.2.

CLI Kommando:

```
config tls 1.2
```

c) Create Access lists

You can define in an Access List which IP addresses are allowed to access the management of the switch.

CLI Command (in this example, the IP addresses range of from 11.222.3.4 to 11.222.3.6):

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

d) Disable sending of Life and Autodiscovery packets

If the „Disable Life and Autodiscover Packets" setting is used, neither Life nor Autodiscover packets are sent. The result is that the switch cannot be found via Layer 2, but only via Layer 3 Autodiscover.

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

e) Disable Basic Configurator

This avoids switches answering to Layer 2 requests from the Basic Configurator as well as reading and writing the basic configurations like name, location, contact, IP address, subnet mask and gateway.

By disabling the basic configurator function on the switch the reading as well as the writing via basic configurator will be disabled.

CLI Command:

```
config basic-configurator disable
```

f) Enable "Don't save Config to Database"

If this setting is enabled, binary and CLI configurations are prevented from being saved in the database. This makes particular sense, if for reasons of security the switch configuration must not be saved to a data storage medium. Manager Device-List Menu:

Preferences > Global > Don't save Config to Database

g) Configure Memory Card Mode to AES-256 encryption

When it is configured, the entire switch configuration will be stored with an AES-256 encryption on the memory card. This prevents any readout of the switch configuration by SD card readers.

CLI Command:

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

2. List of used ports in Secure Mode

2.1. Port 22 TCP (SSH - Secure Shell)

The switch can be accessed via all standard SSHv2 Client. All the parameters are configurable via SSHv2.

For security reasons, several SSH orTelnet or V.24 Console sessions cannot be opened simultaneously.

After entering invalid username or password 3 times, all the interfaces (SSH, TELNET and V.24 console) are blocked for 60 seconds.

Only SSH version 2 is supported and an individually generated RSA and ECC server keys are already preinstalled in the delivery state.
IMPORTANT: It is strongly recommended that clients use the below elliptic curve key exchange method (ecdh-sha2-nistp256) and algorithm (ecdsa-sha2-nistp256) which garantees future proof encrypted access and also allows a much faster SSH and SCP connection setup. The RSA method is implemented only for backward compatibility with old SSH clients

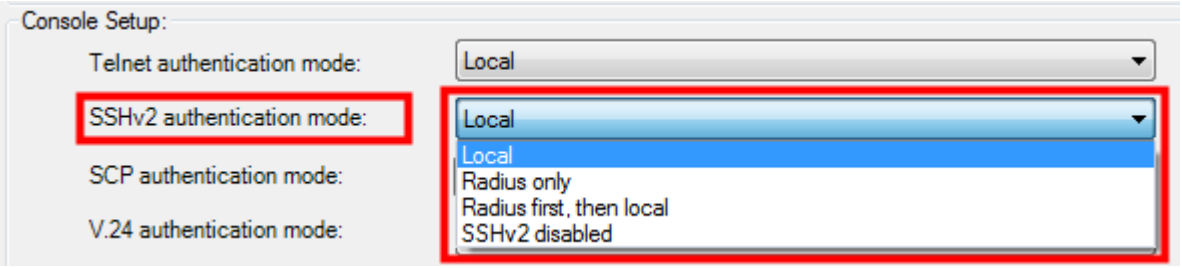
The following key exchange methods are supported:
- ecdh-sha2-nistp256
- diffie-hellman-group14-sha1
- diffie-hellman-group1-sha1

The following server key algorithms are supported:
- ecdsa-sha2-nistp256 (256 Bit ECC key)
- ssh-rsa (1024 Bit RSA-Key)

The following encryption methods are supported:
- aes256-ctr
- aes128-ctr
- aes256-cbc
- aes128-cbc

The following hash methods are supported:
- hmac-sha2-256
- hmac-sha2-512

Via "SSH Authentication Mode", it is possible to disable SSH and the corresponding port.
Following modes are available:
- Local: Authentication via local names and passwords
- Disabled: SSH Interface disabled
- Radius only: Authentication only via RADIUS Server
- Radius first, then local: Authentication via RADIUS, if any server answers: local Authentication



In addition, it is feasible to create an "IP Access-List" to authorize only certain IP addresses or a range of IP addresses which are allowed to access to the SSH server.

2.2. Port 50271 TCP (SCP - Secure Copy)

The switch can be accessed via all standard SCP Clients.

Via SCP, the following switch files can be read:
- CLI Configuration (with only with parameters changed from the Factory-Default)
- CLI Configuration (with all parameters)
- Binary Configuration (primarely used by the Manager)
- Local Logging

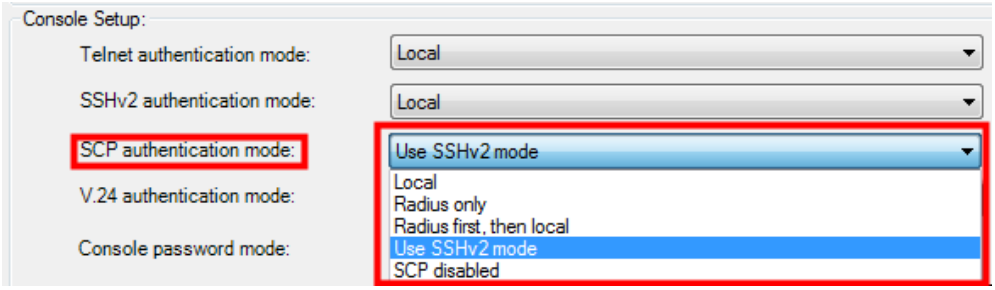
Via SCP, the following files can be written on the Switch:
- CLI Configuration with Reset to Factory Default
- CLI Configuration without Reset to Factory Default
- Binary Configuration (primarely used by the Manager)
- Firmware Image update with immediate start
- Firmware Image update with scheduled start (via Time Client)
- Customer Default Konfiguration
- Customer Reboot Konfiguration

After entering invalid username or password 3 times, all the interfaces (SCP, SSH, TELNET and V.24 console) are blocked for 60 seconds.

SCP only supports SSH version 2 and uses the same algorithms as SSH, see chapter "Port 22 TCP (SSH - Secure Shell)".

Via "SCP Authentication Mode", it is feasible to disable SCP and the corresponding port.
Following modes are available:

- Local: Authentication via local names and passwords
- Disabled: SCP Interface disabled
- Radius only: Authentication only via RADIUS Server
- Radius first, then local: Authentication via RADIUS, if any server answers: local Authentication
- Use SSHv2 Mode: SCP uses the same configurations as « SSHv2 Authentication Mode »



In addition, it is possible to create an "IP Access-List" to authorize only certain IP addresses or a range of IP addresses which are allowed to access to the SCP server.

2.3. Port 443 TCP (HTTPS)

The HTTPS access to the switch can occur via all standard web browsers. Only HTML language is used (other languages like JavaScript are not used).

Via the HTML Code "autocomplete='off'", it can prevent web browser from storing passwords.

The session between the switch and the web browser is secured via the IP address of the browser. In addition, a random 32-hexadecimal-digits-session-key is generated for a single login session.

During Loging in, the name and the password are transmited via the POST method, so that they cannot be read in the browser or by sniffers because of SSL encryption.

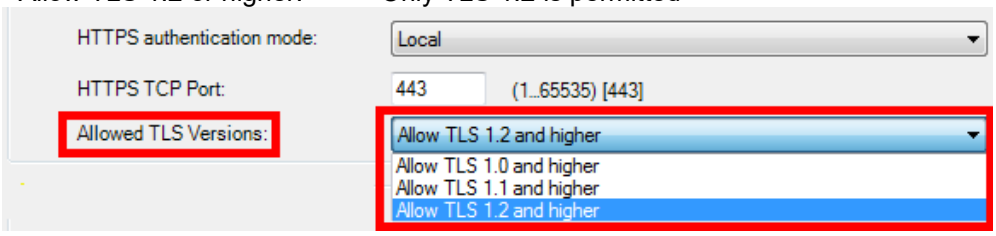
A certificate signed by Nexans Advanced Networking Solutions CA (Nexans-ANS CA) is installed on the switches (RSA, 1024 Bit Key for HW3 switches or 3072 Bit Key for HW5 switches, SHA-256).

The Nexans CA Certificate used for the signature is available on the Nexans Support portal. It can be imported in the browser as a root certificate in order to avoid alarm messages while acceding for the first time each Switch.

Note : in this case, it is not possible to access a switch via its IP address but only via a symbolic name (this is one of the basic limits of the HTTPS certificates concept). The name will be resolved to the corresponding IP address by the DNS Server or by the hosts file. The same certificate is installed on all Nexans switches and named: ***.switch.nexans***. The star sign * can be replaced by any switch name (but cannot contain any dots) and the browser will treat the switch certificate as a valid one.

Supported encryption protocols:
- TLS1.0, TLS1.1, TLS1.2

The minimum allowed TLS protocol version for access via HTTPS can be configured.
The following modes are available here:
- Allow TLS 1.0 or higher: TLS 1.0, 1.1 and 1.2 are permitted
- Allow TLS 1.1 or higher: TLS 1.1 and 1.2 are permitted
- Allow TLS 1.2 or higher: Only TLS 1.2 is permitted



The following cipher suits are supported for switches with management hardware HW3:
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

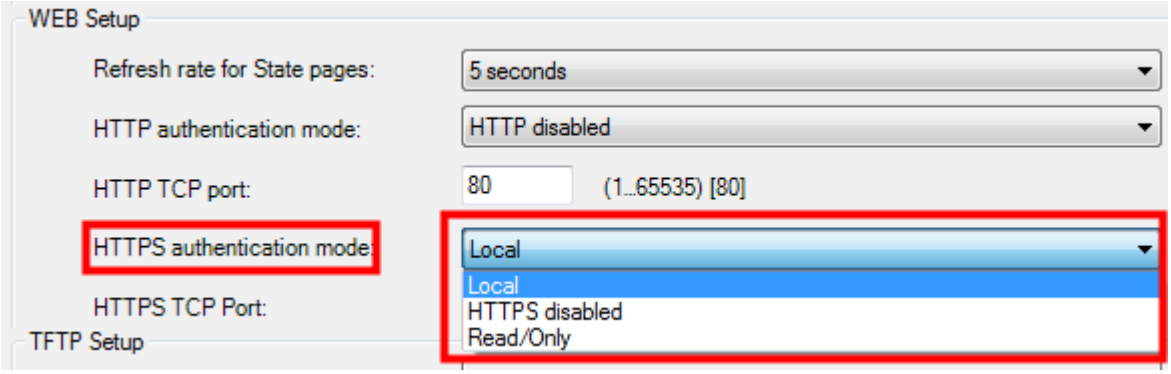
The following cipher suite is supported for switches with management hardware HW5:
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

Via "HTTPS Authentication Mode", it is feasible to disable HTTPS and the corresponding port. You can also configure the mode on Read/Only in order to prevent anybody from writing on switches even if they access to the Read/Write account.

Following modes are available:
- Local: Authentication via local names and passwords
- Read/Only local Authentication; only Read/Only access
- Disabled: HTTPS Interface disabled

After entering invalid name or password 3 times, all the web interfaces (HTTP and HTTPS) are blocked for 60 seconds.

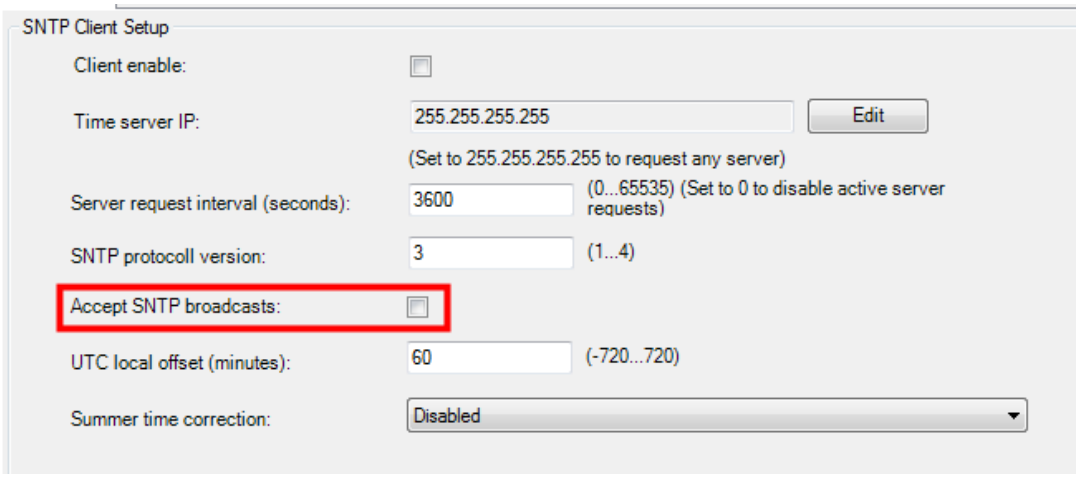
Finally, the HTTPS TCP port can be defined in the range from 1 to 65535.



In addition, it is possible to create an "IP Access-List" to authorize only certain IP addresses or a range of IP addresses which are allowed to access to the SCP server.

2.4. Port 123 UDP (SNTP)

The SNTP port is blocked for Factory Default setting. It opens if the receipt of SNTP broadcasts is allowed in the SNTP configuration:



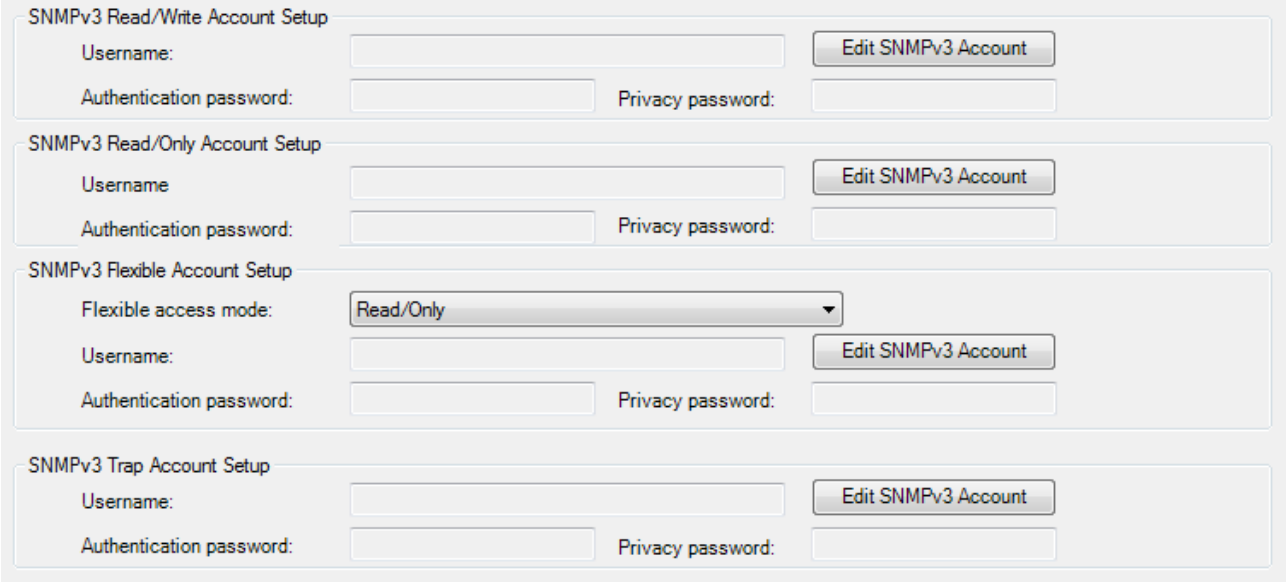
2.5. Port 161 UDP (SNMPv3)

In „Secure Mode“, only SNMP protocol is supported:
• SNMPv3 Auth.-SHA Priv.-AES-128

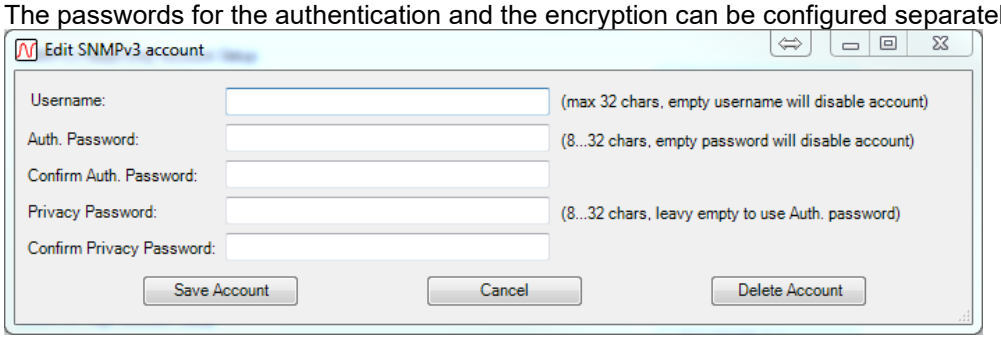
Supported Encryption Method:
• aes-128-cfb

Supported Hash Method:
• hmac-sha1-96

In the SNMPv3 access framwork, it is availble to configure a the user credentials for each type/level of access (Read/Write, Read/Only and flexible access):

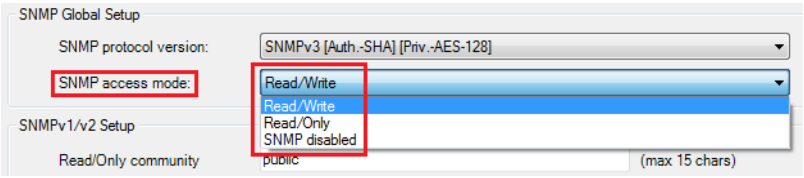


The passwords for the authentication and the encryption can be configured separately.



Via "SNMP Access Mode", it is possible to disable SNMP and the corresponding port.
You can also configure the mode on Read/Only in order to prevent anybody from writing on the switch even if they have access to the SNMPv3 Read/Write account.

Following modes are available:
• Read/Write: Read/Write Access allowed
• Read/Only Only Read/Only access allowed
• SNMP disabled: SNMP Interface disabled



In addition, it is feasible to create an "IP Access-List" to authorize only certain IP addresses or a range of IP addresses which are allowed to access to the SNMPv3 agent.

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

Sending Remote SYSLOG messages via the UDP port 514 is disabled, and the Local Logging enabled by Factory Default configuration.

The following alarm messages can be sent:

- Cold Start
- Link Up
- Link Down
- Link Change
- Internal Voltage Failure
- Temperature Failure
- New MAC Adresse
- 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)

Port 50266 and 50268 are used by the Nexans Manager (NexMan) for the following functions:

- 50266 Polling of the Switch state
- 50268 Autodiscovery (can be disabled)
- 50266 Basic Configurator (can be disabled)

In addition, it is possible to create an "IP Access-List" to authorize only certain IP addresses or a range of IP addresses which are allowed to access to ports 50266 and 50268.

Following information is transmitted when polling the switch:

- MC MAC address
- Active MAC address
- Device MAC address
- Alarms
- Redundancy
- PoE
- IP address
- Name
- Location
- Description
- Type
- Management firmware version
- Management hardware version
- Voice VLAN
- Default VLAN
- Uptime
- Last seen
- Serial number
- TP-HEAD position
- Error counter
- Link status
- PoE voltage per port in Volt
- PoE power per port in milliWatt
- PoE input voltage in Volt
- PoE input power in milliWatt
- Current temperature oft he casing
- Forwarding State
- Speed-Duplex Mode
- Security Mode
- Trunking Mode
- Power Setup
- Power Limit
- Alarm M1 State
- Alarm M2 State
- Rapid Spanning Tree State
- Time from SNTP
- Flow Control State
- Too many MAC addresses
- Security Failure MAC Address
- Fix IP Address
- Numbre of entries in the local log
- PoE Power Class
- Time since last Link change
- State of the 1st Authentication Server
- State of the 2nd Authentication Server
- State of the 1st Accounting Server
- State of the 2nd Accounting Server
- Time since last request to the 1st Authentication Server
- Time since last request to the 2nd Authentication Server

- Time since last request to the 1st Accounting Server
- Time since last request to the 2nd Accounting Server
- MAC Addresses Status
- Temperature 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 BootsDevice
- State of Mgmt of the 1st Authentication Server
- State of Mgmt of the 2nd Authentication Server
- Time since last request to the Mgmt of the 1st Authentication Server
- Time since last request to the Mgmt of the 2nd Authentication Server

Following information is transmitted during the Autodiscovery:

- Active MAC address
- Name
- Location
- Description
- Type
- Management firmware
- Management hardware
- Uptime
- DHCP on or off
- Minimum and maximum temperatures measured
- Part N°
- Rolling N°
- Serial N°
- Current temperature
- Info if the MAC address is from the memory card or the switch

Following information is transmitted to the Basic Configurator:

- IP address
- Subnet mask
- Gateway
- DHCP enable
- Name
- Location
- Contact
- Firmware version
- Number of Ports
- Management VLAN ID
- Trunk port number

Nexans develops, produces and sells active LAN solutions
for Fiber to the Office (FTTO) and for harsh environments,
to a broad customer base including universities, hospitals
and public administration facilities
where our solutions have been proven to demonstrate
high reliability over many years.

With more than 25 years experience
in the development and production of optical solutions,
Nexans provides the reliability and the security
you expect for your network.

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**