Management des Switches Nexans - Haut degré de Sécurité - Recommandations de configuration

Version Firmware V7.04 ou plus

KD975F13

SOMMAIRE

1. Recommandations de configuration

1.1. Comparaison du Mode Secure et du Mode par défaut

Trois méthodes permettent de configurer le Switch de telle sorte qu'un haut niveau de sécurité soit garanti :
• Configurer manuellement point par point les paramètres liés à la sécurité
• Activer via software le mode « Access Policy »
• Activer via cavalier le mode « Access Policy »

Le tableau ci-dessous compare les paramètres liés à la sécurité du mode par défaut (Default) et du mode Secure :

Fonction	**Mode Default**	**Mode Secure Access Policy**
Telnet	Activé	Désactivé
SSH	Activé	Activé et les clients doivent utiliser une méthode d'échange de clés par courbe elliptique.
HTTP	Activé	Désactivé
HTTPS	Activé	Activé
Accès SNMP	SNMPv1	SNMPv3-SHA1-AES128
Accès Manager	Secure Copy - SCP	Secure Copy - SCP
Password strength checker	Désactivé	Activé
Password Encryption Mode	Standard	SHA256 Hash

1.2. Configurer manuellement les paramètres liés à la sécurité

Lors d'une configuration manuelle des paramètres de sécurité, il faut désactiver un à un les protocoles et fonctionnalités à risque.

Nous recommandons par exemple de paramétrer comme suit :

a) Eteindre TELNET
Commande CLI :
```
config telnet-auth-mode disable
```

b) Eteindre HTTP
Commande CLI :
```
config web-auth-mode disable
```

c) Accès SNMP uniquement via SNMPv3-SHA1-AES128
Commande CLI:
```
config snmp-protocol-version v3-aes-auth-sha
```

Remarque: Sortie usine (Factory Default), aucun SNMPv3 Account n'est défini: ni Read/Only, ni Read/Write sont possibles via SNMPv3.

d) Authentification du Manager et transfert de données uniquement via Secure Copy Protcol (SCP)
Ceci désactive l'authentification UDP et le serveur TFTP du Switch.
En alternative au serveur TFTP désactivé, on peut réaliser par commande CLI un transfert TFTP (via le TFTP-Client intégré). Ceci est bien sûr possible uniquement si le User s'est authentifié correctement à la console CLI.

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

e) Activer le vérificateur de qualité de mot de passe
En activant "Password Strength Checker", on est obligé, pour ensuite administrer le Switch, de remplacer le mot de passe sortie usine (Factory-Default Password) par un mot de passe sûr.
Un mot de passe „sûr“ doit répondre aux critères suivants :
8…14 caractères dont minimum:
une minuscule : (a-z)
une majuscule : (A-Z)
un chiffre : (0-9)
un caractère spécial : . , ; ! " ' % # $ & ^ ~ @ * : + - = _ / \ | ( ) [ ] { } < >
Commande CLI:
```
set password-strength enabled
```

f) Paramétrer “Password Encrytion Mode” sur SHA256 Hash
Grâce à cette configuration, les mots de passe des 2 comptes locaux sont enregistrés uniquement comme SHA256 Hash. Si ceux-ci sont suffisamment complexes (min. 8 caractères, voire jusqu‘à 12), il est pratiquement impossible de les déchiffrer en cas de compromission des valeurs Hash.
Commande CLI:
```
set password-encryption sha256-hash
```

1.3. Activer via software le mode « Access Policy »

Tous les paramètres exposés dans le § 1.2 peuvent être configurés en un seul clic dans « Access Policy » sur "Allow secure protocols and passwords only".

Commande CLI:
```
config global-security mode enabled
```

Tant que ce mode de Acces Policy est activé, il n’est plus possible de modifier individuellement un des paramètres exposés dans le § 1.2.

1.4. Activer via cavalier le mode « Access Policy »

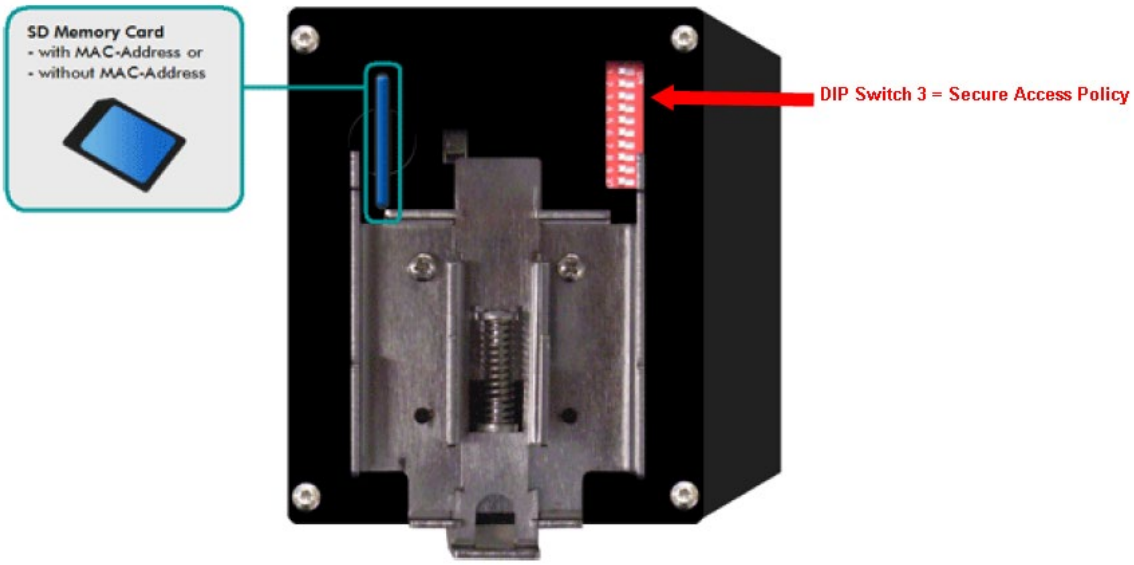
Le mode "Allow secure protocols and passwords only" peut, pour les iGigaSwitches, être activé via cavalier DIP.

Tant que ce mode de Acces Policy est activé, il n’est plus possible de modifier individuellement par software un des paramètres exposés dans le § 1.2.

Ces cavaliers existent uniquement sur les Switches Industriels et se trouvent au dos ou en façade du boîtier.

Position des cavaliers sur 54X, 74X et sur les 104X:

Positionnement des cavaliers sur les switches industriels 54X, 74X et 104X:



Positionnement des cavaliers sur les switches industriels 16XX :

1.5. Autres paramètres envisageables

Les recommandations suivantes ne sont pas absolument nécessaires pour un haut degré de sécurité mais peuvent, au besoin, y contribuer :

a) Configurer l'interface WEB HTTPS sur Read/Only

L'interface WEB est en premier lieu un outil de diagnostic et ne devrait être utilisée qu'exceptionnellement pour la configuration des Switches. En configurant le mode "WEB Authentication Mode" sur Read/Only, on peut empêcher que la configuration soit modifiée via WEB, même si la personne accède bien au compte Admin (pas de droit d'écriture).
Commande CLI:

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

b) Configurer l'interface WEB HTTS pour TLS 1.2

L'interface HTTPS supporte par Factory Default les protocoles TLS 1.0, 1.1 et 1.2. Selon BSI (Ministère Allemand pour la Sécurité Informatique), il est toutefois recommandé d'employer uniquement TLS 1.2. Le serveur HTTPS intégré peut donc être configuré tel qu'il n'autorise que TLS 1.2.

Commande CLI :

```
config tls 1.2
```

c) Créer des listes d'accès

Ceci permet d'autoriser l'accès au Switch seulement à partir de quelques postes de management définis et autorisés.

Commande CLI (dans cet exemple, les adresses IP de 11.222.3.4 à 11.222.3.6):

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

d) Eteindre l'envoi de paquets Life et Autodiscovery

Ainsi, l'envoi régulier de paquets Life n'a pas lieu et le Switch ne répond pas aux requêtes Autodiscovery de niveau 2 (Layer 2) du Manager. Seule l'Autodiscovery de niveau 3 (Layer-3) est possible.

Commande CLI:

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

e) Bloquer la lecture des Switches via le Basic Configurator

Ceci évite que le Switch réponde à des requêtes de niveau 2 du Basic Configurator et que celui-ci lise les configurations de base telles Nom, Lieu (Location), Contact, Adresse IP, Masque sous-réseau et Passerelle.

Commande CLI:

```
config basic-configurator disable
```

f) Désactiver la sauvegarde des configurations du Switch dans la Database du Manager

Ceci évite de sauvegarder les configurations binaires et CLI dans la base de données et répond tout particulièrement aux applications spécifiques où, pour des raisons de sécurité, la configuration des Switches ne doit pas être enregistrée sur support de données.

Manager Device-List Menu:

Preferences > Global > Don't save Config to Database

g) Configurer le mode Memory Card sur AES-256 encryption

Active la sauvegarde chiffrée AES-256 de la configuration du switch sur la carte mémoire. Il est ainsi impossible de lire la configuration du switch avec un quelconque lecteur de carte SD.

Commande CLI:

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

2. Liste des ports utilisés en Secure Mode

2.1. Port 22 TCP (SSH - Secure Shell)

Le Switch est accessible via n'importe quel Client SSHv2 standard. Tous les paramètres du Switch sont configurables via SSHv2.

Pour des raisons de sécurité, il n'est pas possible d'ouvrir simultanément plusieurs sessions SSH, Telnet ou Console V.24.

Si l'on saisit 3 fois de suite le mauvais nom ou mot de passe, toutes les interfaces console (SSH, TELNET et V.24) sont bloquées pour 60 secondes.

Seule la version 2 de SSH est supportée. Sortie d'usine, une clé serveur RSA et une ECC sont déjà pré-installées ; elles sont générées individuellements par switch.
IMPORTANT : Il est fortement recommendé aux clients d'utiliser la méthode d'échange de clés elliptique ci-dessous (ecdh-sha2-nistp256) et l'algorithme (ecdsa-sha2-nistp256), qui garantissent un accès encrypté à l'épreuve du temps, et qui permettent également une configuration bien plus rapide des connexions SSH et SCP. La méthode RSA est à utiliser uniquement pour la rétrocompatibilité avec les anciens clients SSH.

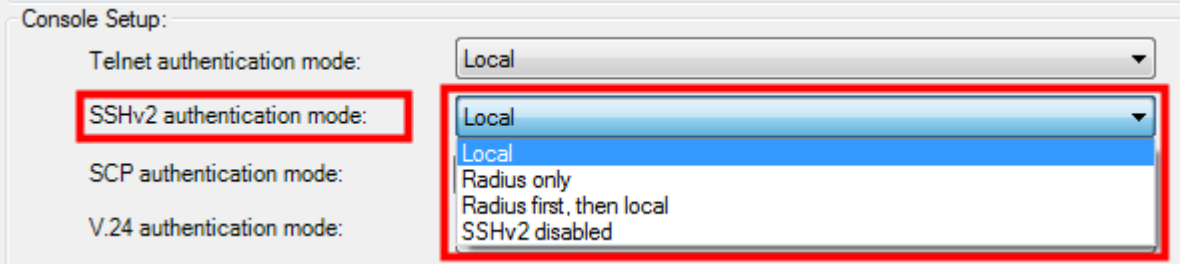
Méthodes d'échange de clé supportées :
- ecdh-sha2-nistp256
- diffie-hellman-group14-sha1
- diffie-hellman-group1-sha1

Algorithmes de clé serveur supportés :
- ecdsa-sha2-nistp256 (256 Bit ECC Key)
- ssh-rsa (1024 Bit RSA-Key)

Méthodes de chiffrage (Encryption) supportées :
- aes128-ctr
- aes128-cbc
- aes256-cbc
- aes256-ctr

Méthodes Hash supportées :
- hmac-sha2-256
- hmac-sha2-512

Via "SSH Authentication Mode", il est possible d'éteindre SSH et le port correspondant.
On a aussi les modes suivants au choix :
- Local: Authentification via noms et mots de passe locaux
- Disabled: Interface SSH désactivée
- Radius only: Authentification uniquement via Serveur RADIUS
- Radius first, then local: Authentification via RADIUS, si aucun serveur ne répond: Authentification locale



En complément, il est possible de créer une „IP Access-List" pour n'autoriser l'accès au serveur SSH qu'à certaines adresses IP ou domaines d'adresses IP.

2.2. Port 50271 TCP (SCP - Secure Copy)

Le Switch peut être consulté via tout Client SCP standard.

Via SCP, on peut lire les fichiers suivants du Switch :
- Configuration CLI (avec seulement les paramètres divergents du Factory Default)
- Configuration CLI (avec tous les paramètres)
- Configuration binaire (utilisée en premier lieu par le Manager)
- Journal local

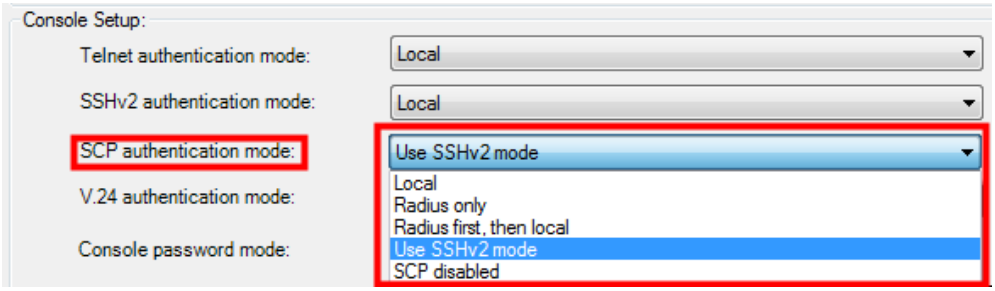
Via SCP, on peut écrire les fichiers suivants dans le Switch :
- Configuration CLI avec Reset sur Factory Default
- Configuration CLI sans Reset sur Factory Default
- Configuration binaire (utilisée en premier lieu par le Manager)
- Firmware Image avec lancement immédiat de la mise à jour
- Firmware Image avec lancement programmé via Time Client de la mise à jour

Si l'on saisit 3 fois à suivre le mauvais nom ou mot de passe, toutes les interfaces console (SSH, TELNET et V.24) sont bloquées pour 60 secondes.

SCP supporte uniquement la Version 2 de SSH et utilise les mêmes algorithmes que SSH. Cf chapitre „Port 22 TCP (SSH - Secure Shell)".

Via "SCP Authentication Mode", il est possible d'éteindre SCP et le port correspondant.
On a aussi les modes suivants au choix :

- Local : Authentification via noms et mots de passe locaux
- Radius only : Authentification uniquement via Serveur RADIUS
- Radius first, then local: Authentification via RADIUS, si aucun serveur ne répond: Authentification locale
- Use SSHv2 Mode : SCP utilise les mêmes configurations que « SSHv2 Authentication Mode »
- Disabled : Interface SCP désactivée



En complément, il est possible de créer une „IP Access-List" pour n'autoriser l'accès au serveur SCP qu'à certaines adresses IP ou domaines d'adresses IP.

2.3. Port 443 TCP (HTTPS)

L'accès HTTPS au Switch est possible via tout browser web standard. Seul le langage HTML est employé (d'autres langages tels JavaScript ne sont pas employés).

Via le Code HTML "autocomplete='off'", on évite que le browser web n'enregistre les mots de passe.

La session entre le Switch et le browser web est sécurisée via l'adresse IP du browser et, en complément, via un numéro à 32 hexadécimales généré lors du Login et randomisé.

Lors du Login, le nom et le mot de passe sont transmis par la méthode POST, de telle sorte qu'ils ne puissent être lus, du fait du chiffrage SSL, dans le browser ou par Sniffer.

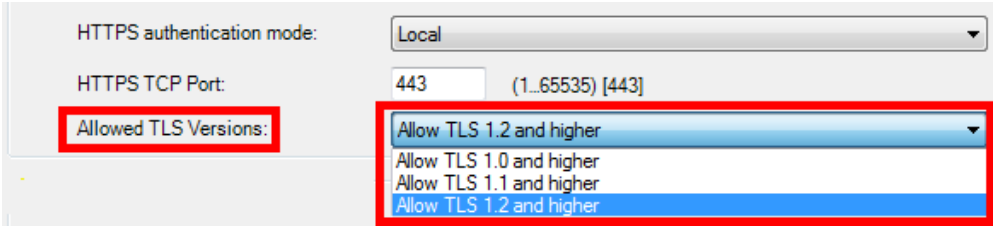
Un Certificat électronique signié Nexans Advanced Networking Solutions CA (Nexans-ANS CA) est installé sur les Switches (RSA, 1024 Bit Key pour switches HW3 ou 3072 Bit Key pour switches HW5, SHA-256).

Le Certificat électronique Nexans CA utilisé pour la signature est disponible sur le portail Support de Nexans. Il peut être importé dans le browser comme certificat racine afin d'éviter les messages d'alerte lorsqu'on accède pour la 1ère fois à chacun des Switches. Remarque : dans ce cas, il n'est pas possible de contacter un Switch via son adresse IP mais via un nom symbolique (c'est une des limites intrinsèques du concept de certificat HTTPS). La résolution du nom correspondant à l'adresse IP se fait par un Serveur DNS ou par le fichier hosts. Le même certificat est installé sur tous les Switches Nexans et il a été signé pour le nom symbolique ***.switch.nexans***. L'étoile ***** peut être remplacée par n'importe quel nom de Switch (mais il ne doit pas contenir de point **.**) pour que le browser considère le certificat du Switch comme valable.

Protocoles de chiffrage (Encryption) supportés :
- TLS1.0, TLS1.1, TLS1.2

Il est possible de configurer la version de protocole TLS la plus petite autorisée pour l'accès par HTTPS.

Les modes suivants sont disponibles:
- Allow TLS 1.0 or higher: TLS 1.0, 1.1 et 1.2 sont autorisés
- Allow TLS 1.1 or higher: TLS 1.1 et 1.2 sont autorisés
- Allow TLS 1.2 or higher: Seul TLS 1.2 est autorisé

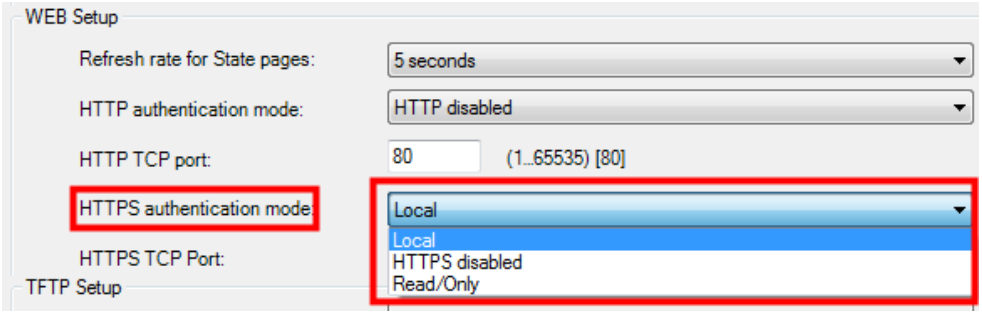


Cipher Suites supportées pour les Switche HW3:
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

Cipher Suites supportées pour les Switche HW5:
- TLS_ ECDHE_RSA_WITH_AES_256_CBC_SHA

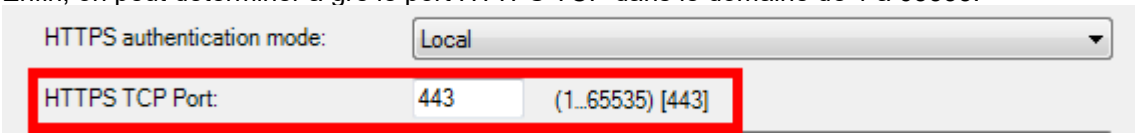
Via "HTTPS Authentication Mode", on peut éteindre HTTPS et le port correspondant. On peut aussi paramétrer le mode sur Read/Only afin de bloquer toute écriture même à quelqu'un qui parviendrait à accéder au compte Read/Write.

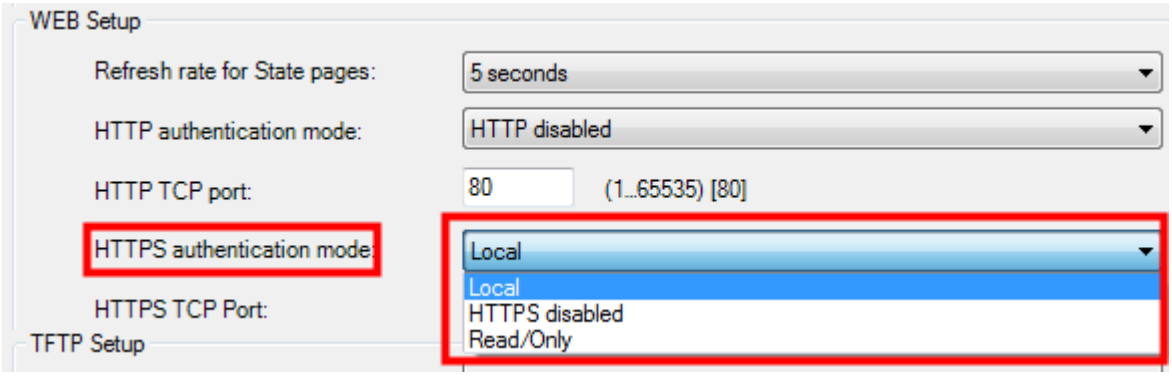
Les modes suivants sont au choix :
- Local : Authentification via noms et mots de passe locaux
- Read/Only Authentification locale ; seul accès Read/Only autorisé
- Disabled : Interface HTTPS éteinte



Si l'on saisit 3 fois à suivre le mauvais nom ou mot de passe, toutes les interfaces web (HTTP und HTTPS) sont bloquées pour 60 secondes.

Enfin, on peut déterminer à gré le port HTTPS TCP dans le domaine de 1 à 65535.

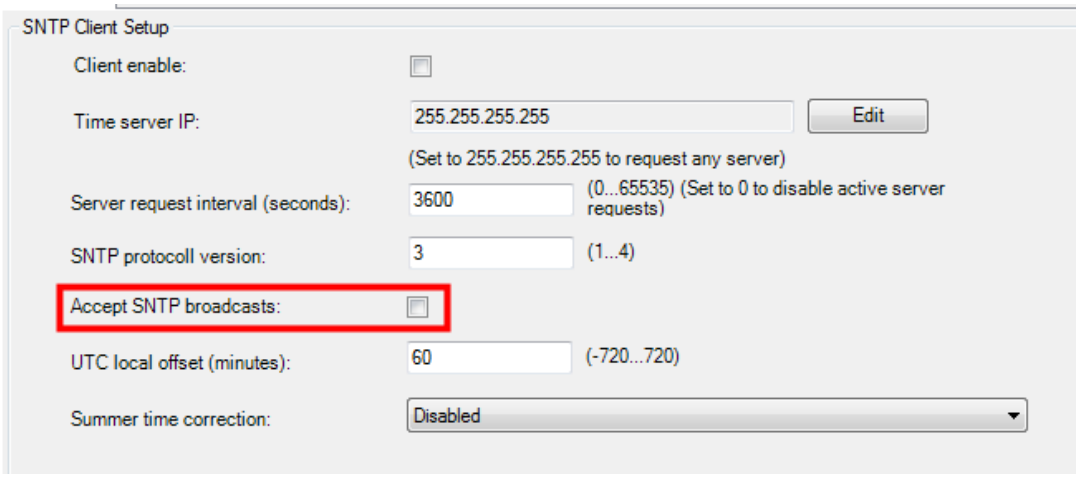




En complément, il est possible de créer une „IP Access-List" pour n'autoriser l'accès au serveur HTTPS qu'à certaines adresses IP ou domaines d'adresses IP.

2.4. Port 123 UDP (SNTP)

Sortie usine, le port SNTP est bloqué. Il s'ouvre si la réception de Broadcasts SNTP est autorisée dans la configuration SNTP :



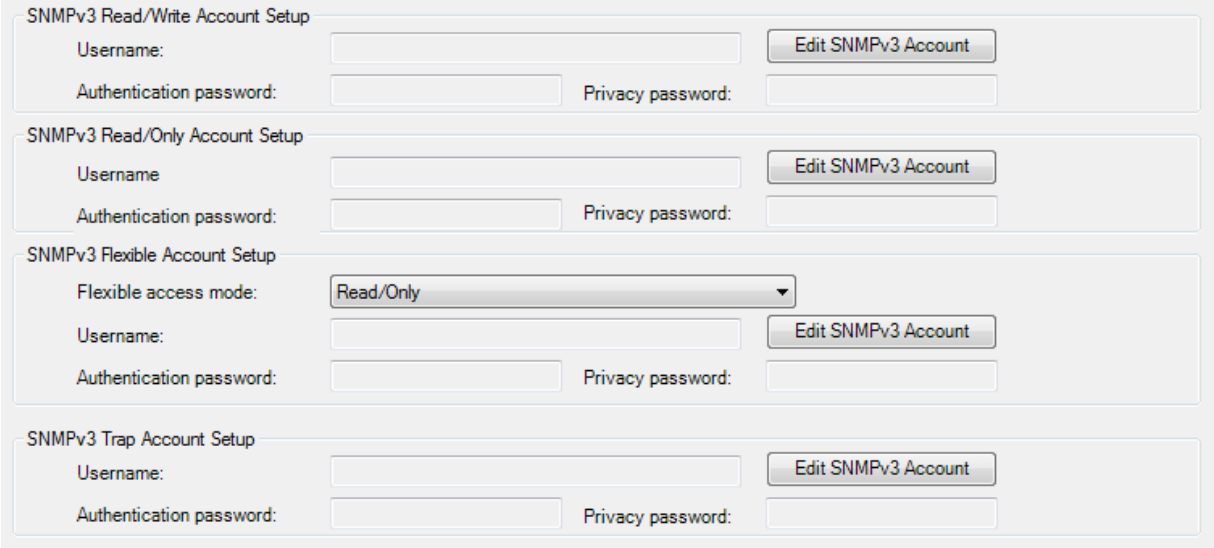
2.5. Port 161 UDP (SNMPv3)

En „Secure Mode“, seul le protocole SNMP suivant est supporté :
• SNMPv3 Auth.-SHA Priv.-AES-128

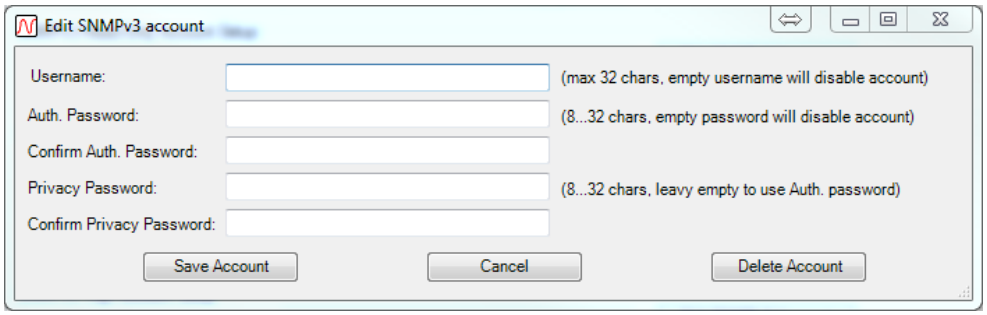
Méthode de chiffrage (Encryption) supportée :
• aes-128-cfb

Méthode Hash supportée:
• hmac-sha1-96

Pour l’accès via SNMPv3, on peut configurer pour chacun des types d’accès (Read/Write, Read/Only et accès flexible) un nom et un mot de passe distincts :

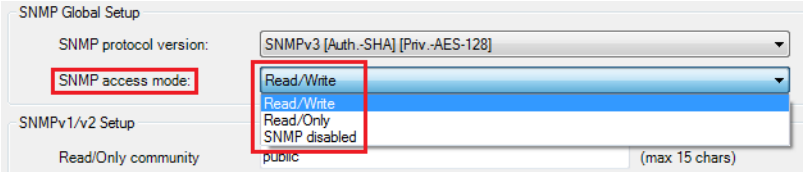


Le nom et mot de passe servent autant pour l’authentification que pour le chiffrage (Encryption).



Via "SNMP Access Mode", on peut éteindre SNMP et le port correspondant. On peut aussi paramétrer le mode sur Read/Only afin de bloquer toute écriture même à quelqu’un qui parviendrait à accéder au compte SNMPv3 Read/Write Username/Password.

Les modes suivants sont au choix :
• Read/Write: Accès Read/Write autorisé
• Read/Only Seul accès Read/Only autorisé
• SNMP disabled: Interface SNMP désactivée



En complément, il est possible de créer une „IP Access-List“ pour n’autoriser l’accès à l’agent SNMPv3 qu’à certaines adresses IP ou domaines d’adresses IP.

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

Sortie usine, l’envoi de messages Remote SYSLOG via le port UDP 514 est désactivé et le Local Logging est activé.

Les messages d‘alarme suivants peuvent être envoyés :

- 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)

Le port 50266 est utilisé par le Manager Nexans (NexMan) pour les fonctions suivantes :

- 50266 Polling de l'état du Switch
- 50268 Autodiscovery (peut être éteint)
- 50266 Basic Configurator (peut être éteint)

En complément, il est possible de créer une „IP Access-List“ pour n'autoriser l'accès aux ports 50266 et 50268 qu'à certaines adresses IP ou domaines d'adresses IP.

Les informations suivantes sont transmises lors du Polling de l'état du Switch :

- Adresse MAC de la Memory Card
- Adresse MAC Active
- Adresse MAC du Switch
- Alarmes
- Redondance
- PoE
- Adresse IP
- Nom-Location
- Description
- Type
- Version Fimrware Mgmt
- Version Hardware Mgmt
- Voice VLAN
- Default VLAN
- Uptime
- Vu pour la dernière fois
- Serie/no.
- Position du module TP
- Error Counter
- Link Status
- Tension PoE par port en Volt
- Puissance PoE par port en milliWatt
- Tension d'entrée PoE en Volt
- Puissance d'entrée PoE en milliWatt
- Température actuelle du boîtier
- Forwarding State
- Mode Speed-Duplex
- Mode Security
- Mode Trunking
- Power Setup
- Power Limit
- Etat Alarme M1
- Etat Alarme M2
- Etat Rapid Spanning Tree
- Heure fournie par SNTP
- Etat Flow Control
- Trop d'adresses MAC
- Security Failure MAC Adresse
- Adresse IP fixe ?
- Nombre des entrées dans le journal local
- PoE Power Class
- Temps écoulé depuis le dernier changement de Link
- Etat du 1er Serveur d'Authentification
- Etat du 2ème Serveur d'Authentification
- Etat du 1er Accounting Servers
- Etat du 2ème Accounting Servers
- Temps écoulé depuis la dernière requête au 1er Serveur d'Authentification
- Temps écoulé depuis la dernière requête au 2ème Serveur d'Authentification
- Temps écoulé depuis la dernière requête au 1er Serveur Accounting
- Temps écoulé depuis la dernière requête au 2ème Serveur Accounting

- Etat des Adresses MAC
- Etat Température
- Voltage 1 valeur en Millivolt
- Voltage 2 valeur en Millivolt
- Etat Voltage 1
- Etat Voltage 2
- Link Down Alarm
- Power Input S1
- Power Input S2
- Etat Contact d'entrée
- Etat Spanning Tree
- Alarme M1 Remote IP
- Alarme M2 Remote IP
- Alarme M1 Remote Time
- Alarme M2 Remote Time
- Total Bootsdu Switch
- Etat du Mgmt du 1er Serveur d'Authentification
- Etat du Mgmt du 2ème Serveur d'Authentification
- Temps écoulé depuis la dernière requête au Mgmt du 1er Serveur d'Authentification
- Temps écoulé depuis la dernière requête au Mgmt du 2ème Serveur d'Authentification

Les informations suivantes sont transmises lors du Autodiscovery :

- Adresse MAC active
- Nom
- Location
- Description
- Type
- Firmware Mgmt
- Hardware Mgmt
- Uptime
- DHCP on ou off
- Températures Minimale et Maximale constatées
- N° d'article
- N° dans la charge
- N° de série
- Température actuelle
- Info si l'adresse MAC vient de la Memory Card ou du Switch

Les informations suivantes sont transmises au Basic Configurator :

- Adresse IP
- Masque sous-réseau
- Passerelle
- DHCP Enable
- Nom
- Lieu (Location)
- Contact
- Version Firmware
- Nombre de ports
- Management VLAN ID
- N° du port Trunk

Nexans fabrique des solutions réseaux innovantes, fiables, flexibles et évolutives. Les multiples applications de nos clients (entreprises leaders mondiales, fournisseurs d'électricité, compagnies de chemin de fer, aéroports, industries, ports, administrations, centres hospitaliers, universités, banques et assurances, entités gouvernementales, territoriales et communales) en font la preuve au quotidien.

Fort de plus de 25 ans d'expérience
dans le développement et la fabrication
de solutions optiques,
Nexans est garant de la fiabilité et sécurité
que vous attendez de votre réseau.

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-fr@nexans.com • **www.nexans.fr/ans**