SNMPv3 configureren op Cisco ONS 15454/NCS 2000 apparaten

Inhoud

Inleiding

Dit document beschrijft stap-voor-stap instructies hoe u de Simple Network Management Protocol, versie 3 (SNMPv3), kunt configureren op ONS 15454/NCS 2000-apparaten. Alle onderwerpen omvatten voorbeelden.

> **Opmerking:** De lijst van eigenschappen in dit document is niet volledig of gezaghebbend en kan te allen tijde zonder bijwerking van dit document worden gewijzigd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Transport Controller (CTC) GUI
- Basisserverkennis
- Basis Linux/Unix-opdrachten

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Op een standalone/meervoudig knooppunt

Instellen van de automatische modus priv op ONS 15454/NCS 2000 apparaat

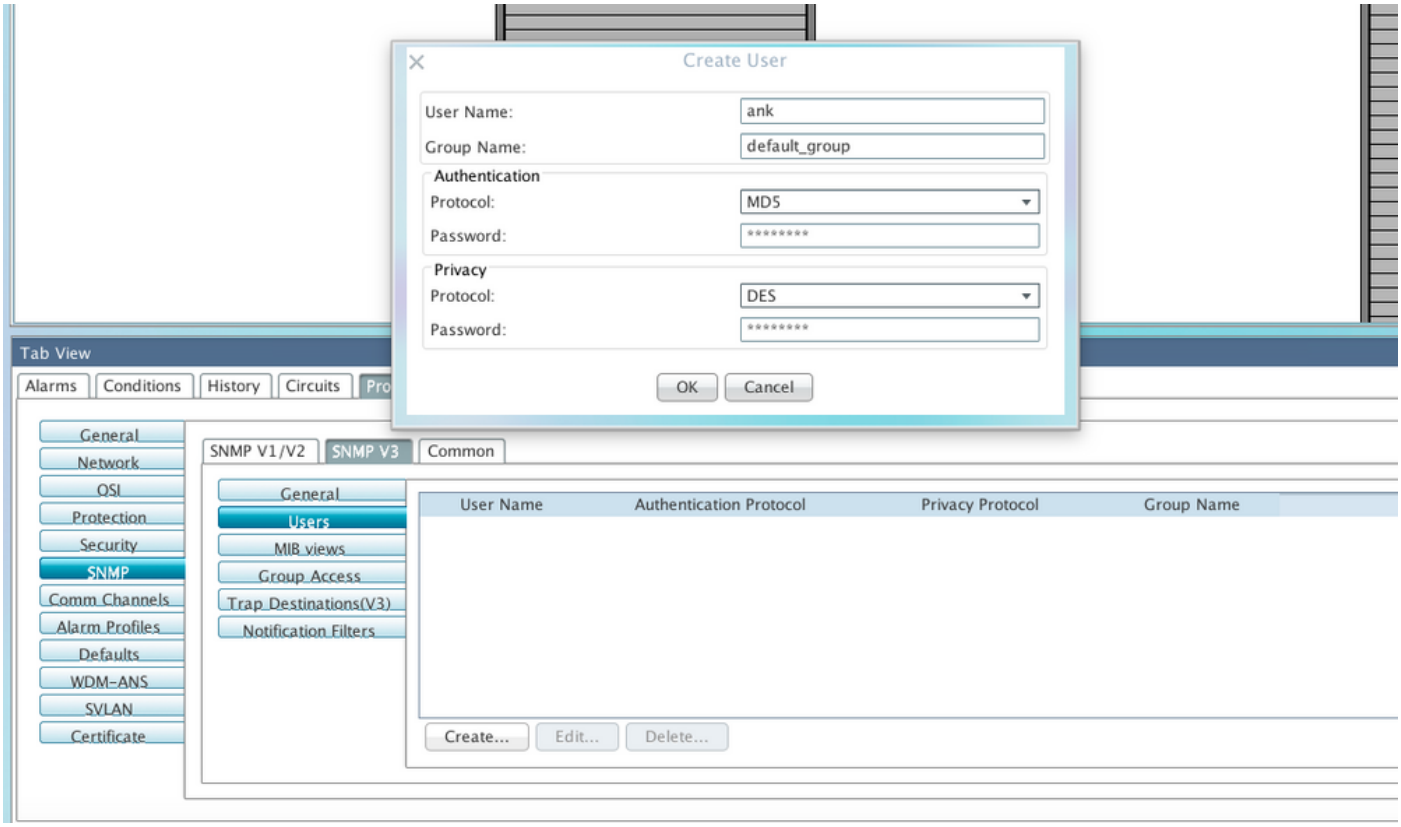
Stap 1. Meld u aan bij het knooppunt via CTC met de Super User-referenties.

Stap 2. Navigeer naar **Node view > Provisioning > SNMP > SNMP V3**.

Stap 3. Navigeer naar het tabblad **Gebruikers**. Gebruikers maken

```
User Name:<anything based on specifications>

Group name:default_group

Authentication

      Protocol:MD5

      Password:<anything based on specifications>

   Privacy

         Protocol:DES

         Password:<anythingbased on specifications>
```

Stap 4. Klik op **OK** zoals in de afbeelding.



Specificaties:

Gebruikersnaam - Specificeer de naam van de gebruiker op de host die met de agent verbonden is. De gebruikersnaam moet minimaal 6 en maximaal 40 tekens zijn (maximaal 39 tekens voor de TACACS- en RADIUS-verificatie). Het bevat alfanumerieke (a-z, A-Z, 0-9) tekens en de toegestane speciale tekens zijn @, "-" (koppelteken) en "." (punt). Voor TL1-compatibiliteit moet de gebruikersnaam uit 6 tot 10 tekens bestaan.

Naam groep - Specificeer de groep waartoe de gebruiker behoort.

Verificatie:

Protocol - Selecteer het verificatiealgoritme dat u wilt gebruiken. De opties zijn ONE, MD5 en SHA.

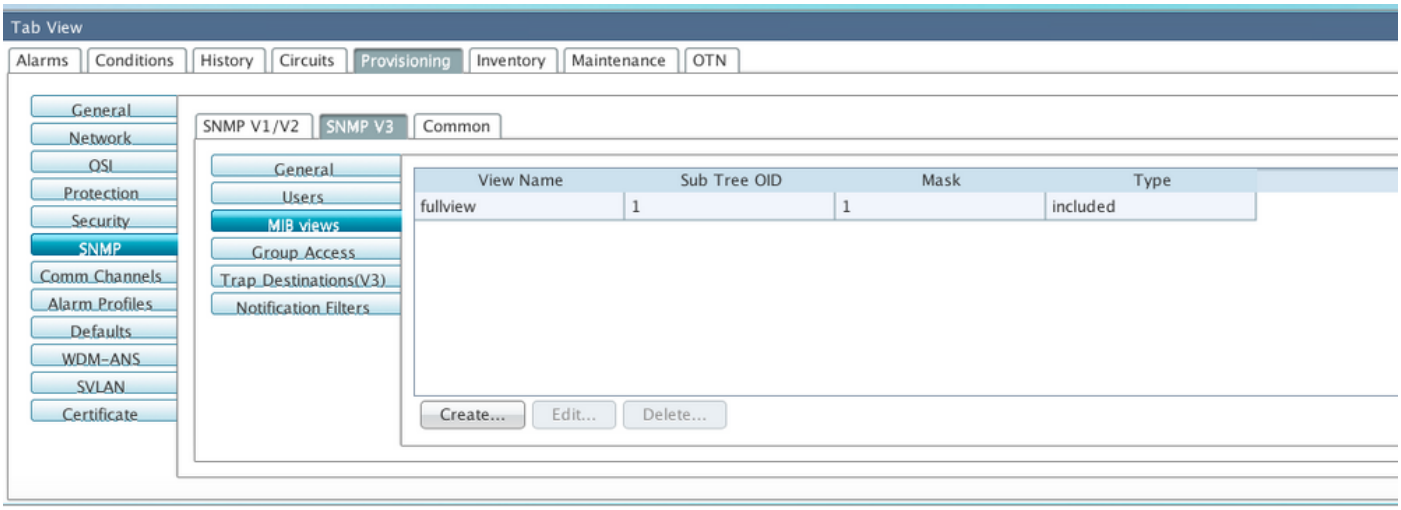
Wachtwoord - Voer een wachtwoord in als u MD5 of SHA selecteert. Standaard is de wachtwoordlengte ingesteld op minimaal acht tekens.

Privacy - initieert een instellingssessie voor de privacy-verificatie die de host in staat stelt de inhoud van het bericht te versleutelen dat naar de agent wordt verzonden.

Protocol - Selecteer het algoritme voor de verificatie van de privacy. De beschikbare opties zijn geen, DES en AES-256-CFB.

Wachtwoord - Voer een wachtwoord in als u een ander protocol selecteert dan geen.

Stap 5. Zorg ervoor dat de MIB-weergave in deze afbeelding is ingesteld.



Specificaties:

Naam - Naam van de weergave.

Subtree OID - De MIB-subboom die, wanneer gecombineerd met het masker, de reeks subbomen definieert.

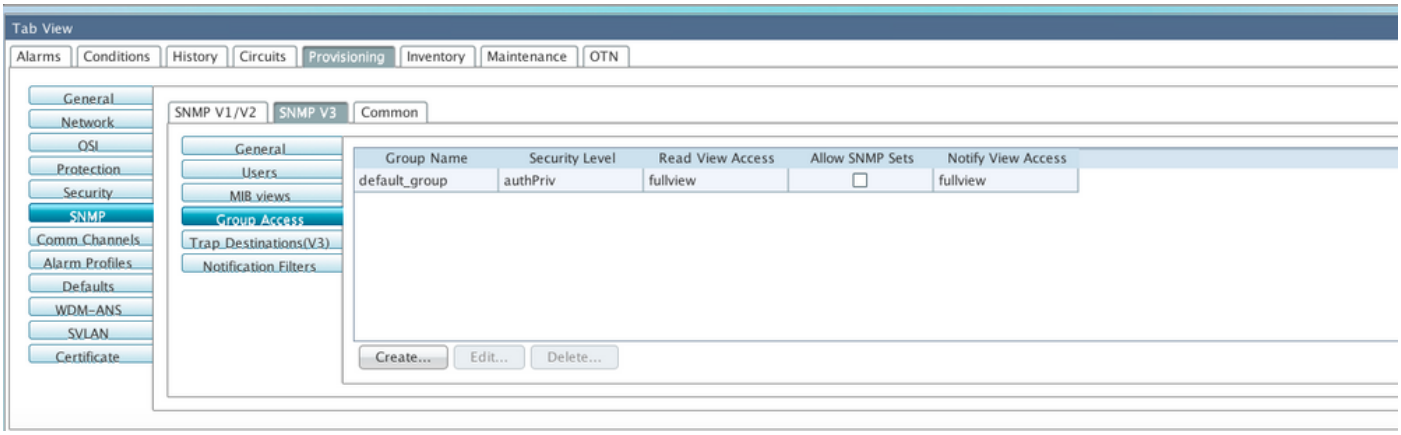
Beetje masker - Een familie van uitzicht subbomen. Elke bit in het bit Mask correspondeert met een sub-identifier van de subtree OID.

Type - Selecteer het type weergave. Opties zijn opgenomen en uitgesloten.

Het type definieert of de reeks subbomen die wordt gedefinieerd door de subboom OID en de combinatie bitmasker zijn opgenomen of uitgesloten van het aanmeldingsfilter.

Stap 6. Het configureren van groepstoegang zoals in de afbeelding. Standaard zal de naam van de groep default_group en security niveau als authPriv zijn.

Opmerking: De naam van de groep moet hetzelfde zijn als de naam die wordt gebruikt wanneer u in Stap 3 de gebruiker maakt.



Specificaties:

Naam van de groep - de naam van de SNMP groep, of de verzameling gebruikers, die een gemeenschappelijk toegangsbeleid delen.

Beveiligingsniveau - het beveiligingsniveau waarvoor de toegangsparameters worden

gedefinieerd. Selecteer uit deze opties:

NoAuthNoPriv - Gebruikt een gebruikersnaammatch voor authenticatie.

AuthNoPriv - biedt verificatie op basis van de HMAC-MD5 of HMAC-SHA-algoritmen.

AuthPriv - levert verificatie op basis van de HMAC-MD5 of HMAC-SHA-algoritmen. Biedt DES 56-bits codering op basis van de CBC-DES (DES-56)-standaard, naast verificatie.

Als u authNoPriv of authPriv voor een groep selecteert, moet de betreffende gebruiker worden geconfigureerd met een verificatieprotocol en een wachtwoord, met een privacy-protocol en een wachtwoord, of beide.

Bekijk

Lees View Name - Lees de naam van de weergave voor de groep.

Melden van View Name - Melden de naam van de weergave voor de groep.

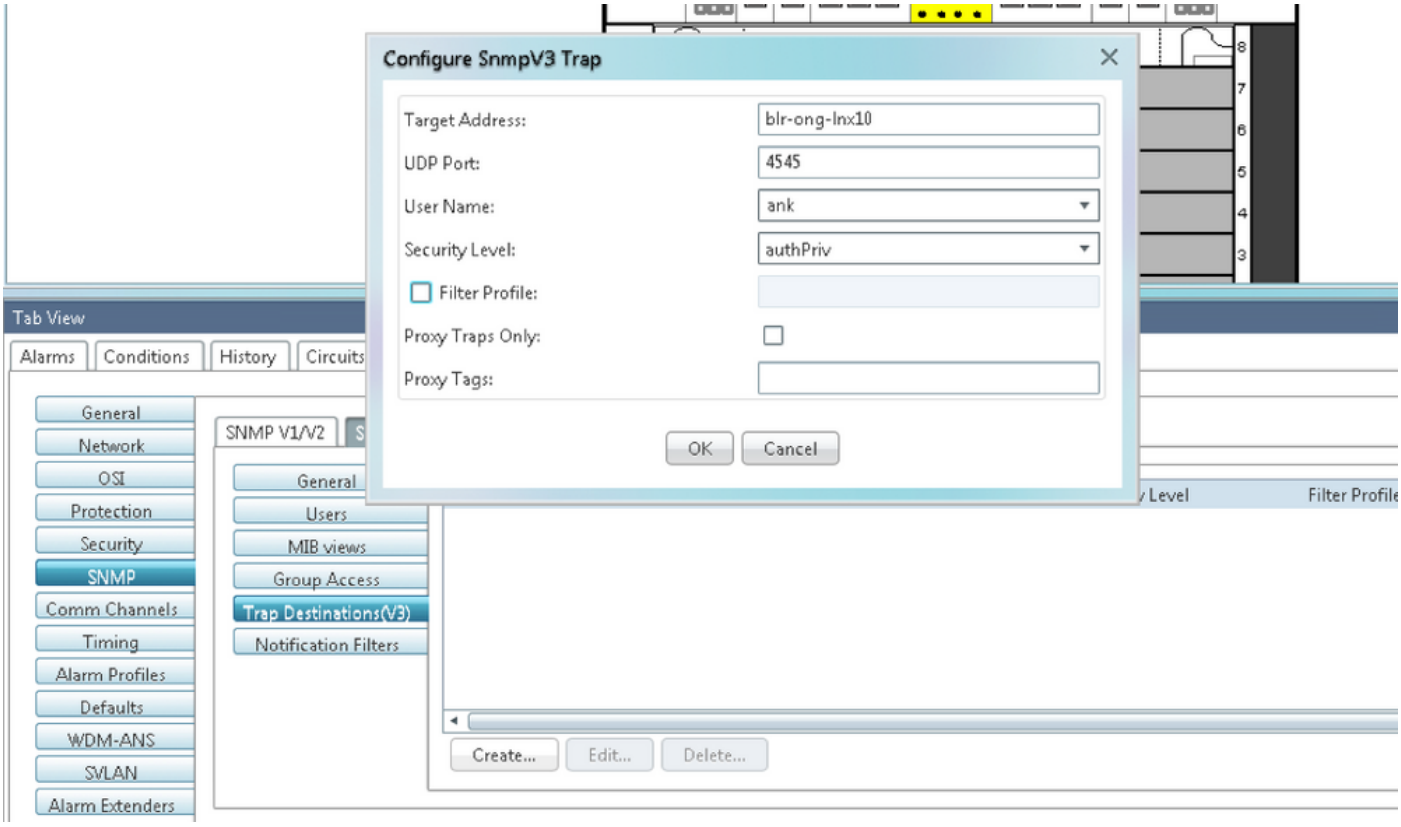
Geef SNMP-bestanden toe - Selecteer dit aankruisvakje als u wilt dat de SNMP-agent SNMP-verzoeken accepteert. Als dit selectieteken niet is geselecteerd, worden de SET-aanvragen afgewezen.

Opmerking: SNMP SET-aanvraagtoegang wordt voor heel weinig objecten geïmplementeerd.

Stap 7. Navigeer naar **Node View > Provisioning > SNMP > SNMP V3 > Trap Destination (V3)**. Klik op **Maken** en **Configureren**.

```
Target address:<any build server> (eg: blr-ong-lnx10)

UDP port: <anything between 1024 to 65535>

User name:<same as we created in step 3>

Security Level:AuthPriv
```

Stap 8. Klik op **OK** zoals in de afbeelding.



Opmerking: blr-ong-lnx10 is de NMS-server.

Specificaties:

Doel - Doel waarvoor de vallen dienen te worden verzonden. Gebruik een IPv4- of IPv6-adres.

UDP Port - UDP-poortnummer dat de host gebruikt. De standaardwaarde is 162.

Gebruikersnaam - Specificeer de naam van de gebruiker op de host die met de agent verbonden is.

Beveiligingsniveau - Selecteer een van deze opties:

NoAuthNoPriv - Gebruikt een gebruikersnaammatch voor authenticatie.

AuthNoPriv - biedt verificatie op basis van de HMAC-MD5 of HMAC-SHA-algoritmen.

AuthPriv - levert verificatie op basis van de HMAC-MD5 of HMAC-SHA-algoritmen. Biedt DES 56-bits codering op basis van de CBC-DES (DES-56)-standaard, naast verificatie.

Filterprofiel - Selecteer dit aankruisvakje en voer de naam van het filterprofiel in. Splitsen worden alleen verzonden als u een naam van het filterprofiel geeft en een waarschuwing van het filter maakt.

Alleen proxy-trappen - indien geselecteerd, alleen proxy-traps van de ENE doorsturen. Vraps van dit knooppunt worden niet naar de valbestemming verzonden die door deze ingang wordt geïdentificeerd.

Proxy-tags - geeft een lijst met tags aan. De labellijst is alleen nodig op een BNE als een ENE vallen naar de doelmap moet sturen die door deze vermelding geïdentificeerd is, en de GNE als de proxy wil gebruiken.

NMS Server configureren (blr-ong-lnx10)

Stap 1. Maak in uw adresmap van de server een directory met de naam **snmp**.

Stap 2. Maak onder deze folder een bestand **snmptrapd.conf**.

Stap 3. Verander het bestand **SNMP.conf** in:

```
vi snmptrapd.conf

createUser -e 0xEngine ID <user_name>< MD5> <password > DES <password>
```

Bijvoorbeeld:

```
createUser -e 0x0000059B1B00F0005523A71C ank MD5 cisco123 DES cisco123
```

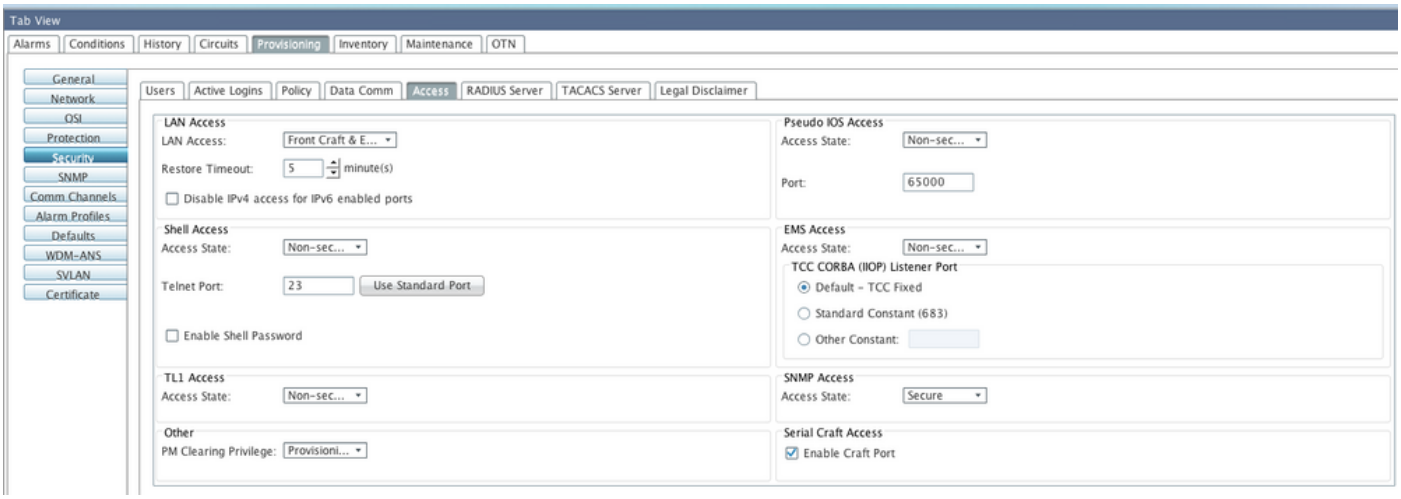
In dit voorbeeld:

```
user_name=ank

MD5 password = cisco123

DES password  = cisco123

Engine ID = can be available from CTC.
```

Node view > Provisioning > SNMP > SNMP V3 > General

Controleer de modus AutoPriv

Stap 1. In CTC, navigeer naar **Node Beeld > Provisioning > Beveiliging > Access > Verander de status van SNMP om beveiligde** zoals in de afbeelding te **bevestigen**.



Stap 2. Navigeer naar de NMS server en wandel de computer.

Syntaxis:

```
snmpwalk -v 3 -l authpriv -u <user name> -a MD5 -A <password> -x DES -X <password> <node IP>
<MIB>
```

Voorbeeld:

```
blr-ong-lnx10:151> snmpwalk -v 3 -l authpriv -u ank -a MD5 -A cisco123 -x DES -X cisco123
10.64.106.40 system

RFC1213-MIB::sysDescr.0 = STRING: "Cisco ONS 15454 M6 10.50-015E-05.18-SPA Factory Defaults
PLATFORM=15454-M6"

RFC1213-MIB::sysObjectID.0 = OID: CERENT-GLOBAL-REGISTRY::cerent454M6Node

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (214312) 0:35:43.12

RFC1213-MIB::sysContact.0 = ""

RFC1213-MIB::sysName.0 = STRING: "Ankit_40"

RFC1213-MIB::sysLocation.0 = ""

RFC1213-MIB::sysServices.0 = INTEGER: 79
```

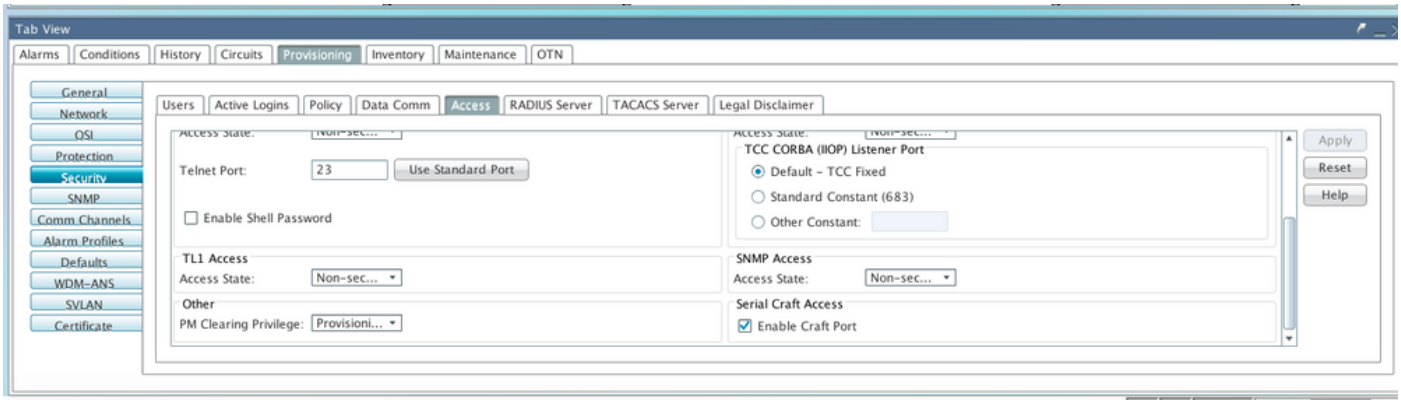
SNMP-trap:

```
snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n" <port number>
```

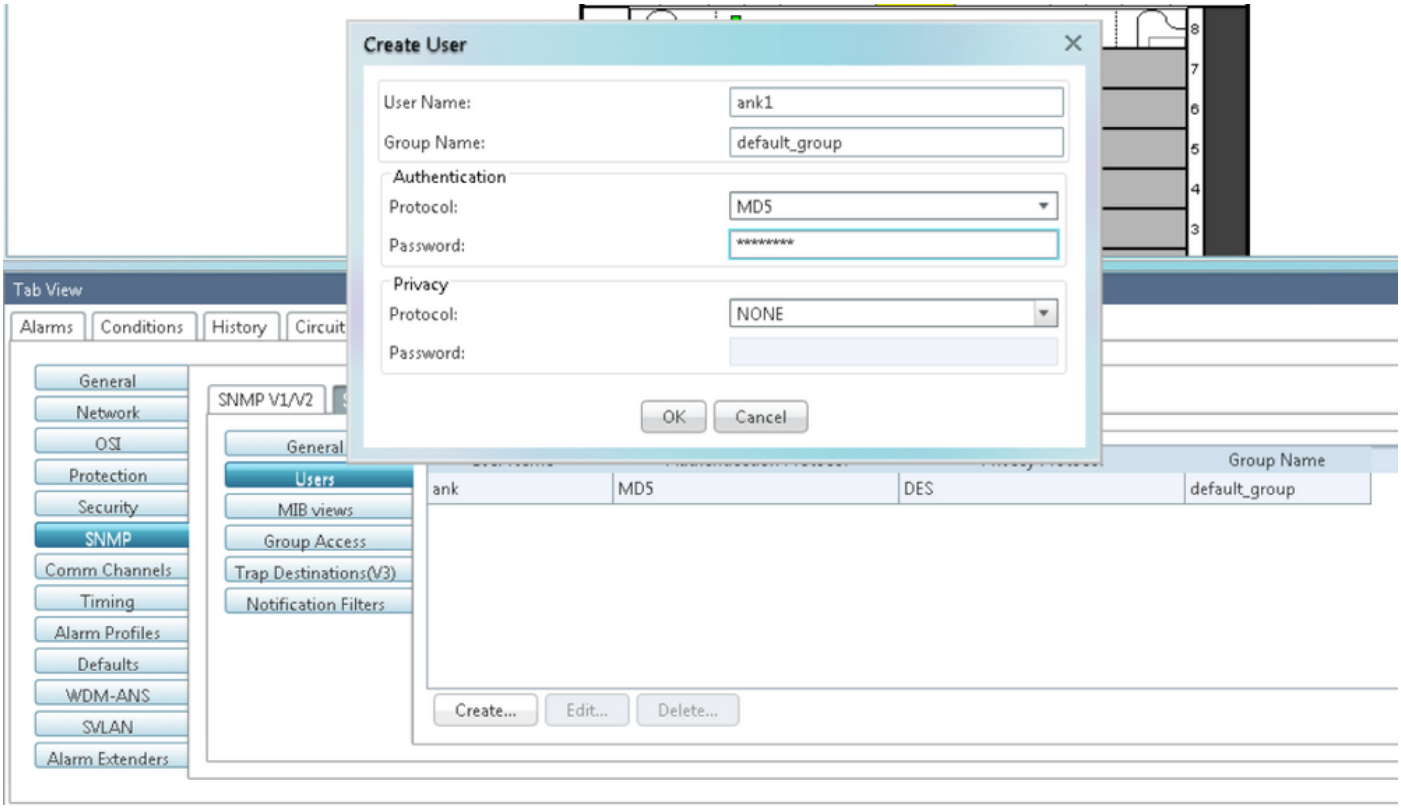
Trap cmd is voor alle versies hetzelfde.

Instellen van de toegangsmodus voor NoPriv op ONS 15454/NCS 2000 apparaat

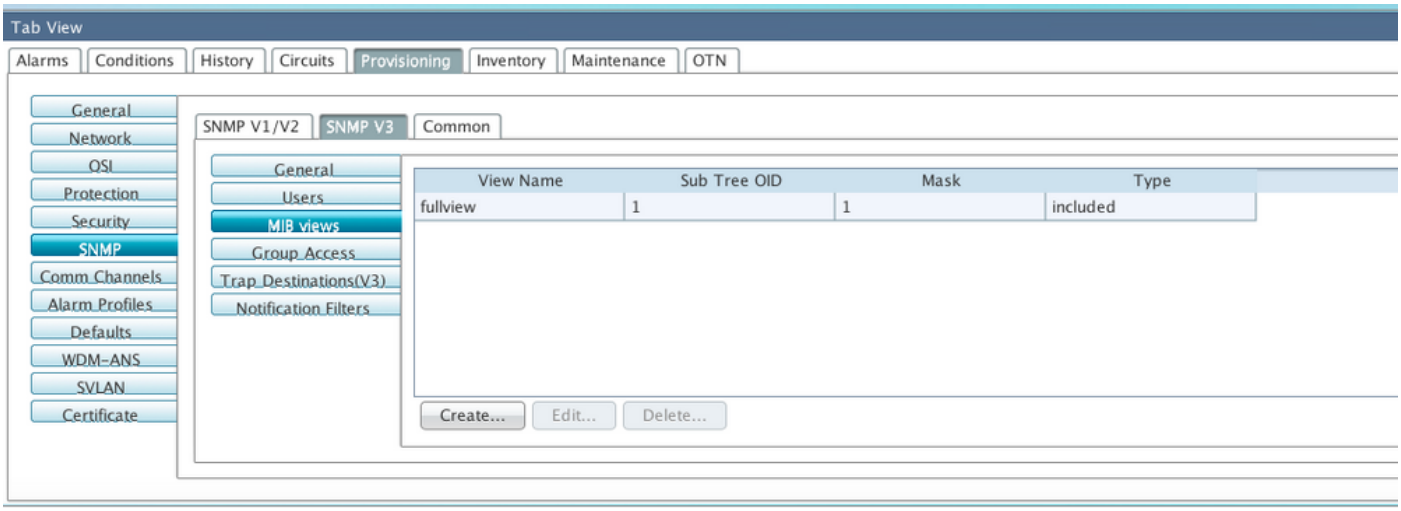
Stap 1. In CTC, navigeer naar **Node View > Provisioning > Beveiliging > Access > Verander de status van toegang tot niet-beveiligde modus** zoals in de afbeelding.



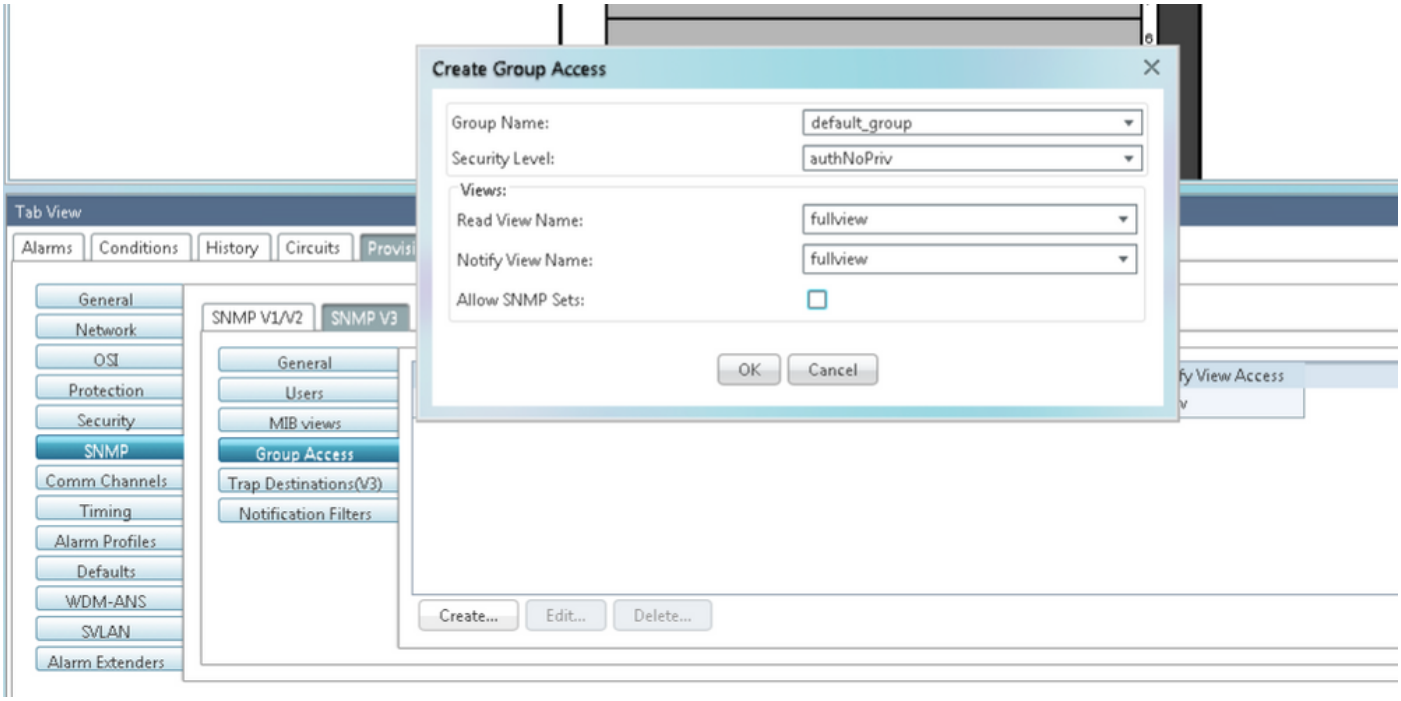
Stap 2. Navigeer naar **Node View > Provisioning > SNMP > SNMP V3 > Gebruikers > Gebruikers maken** en configureren zoals in de afbeelding.



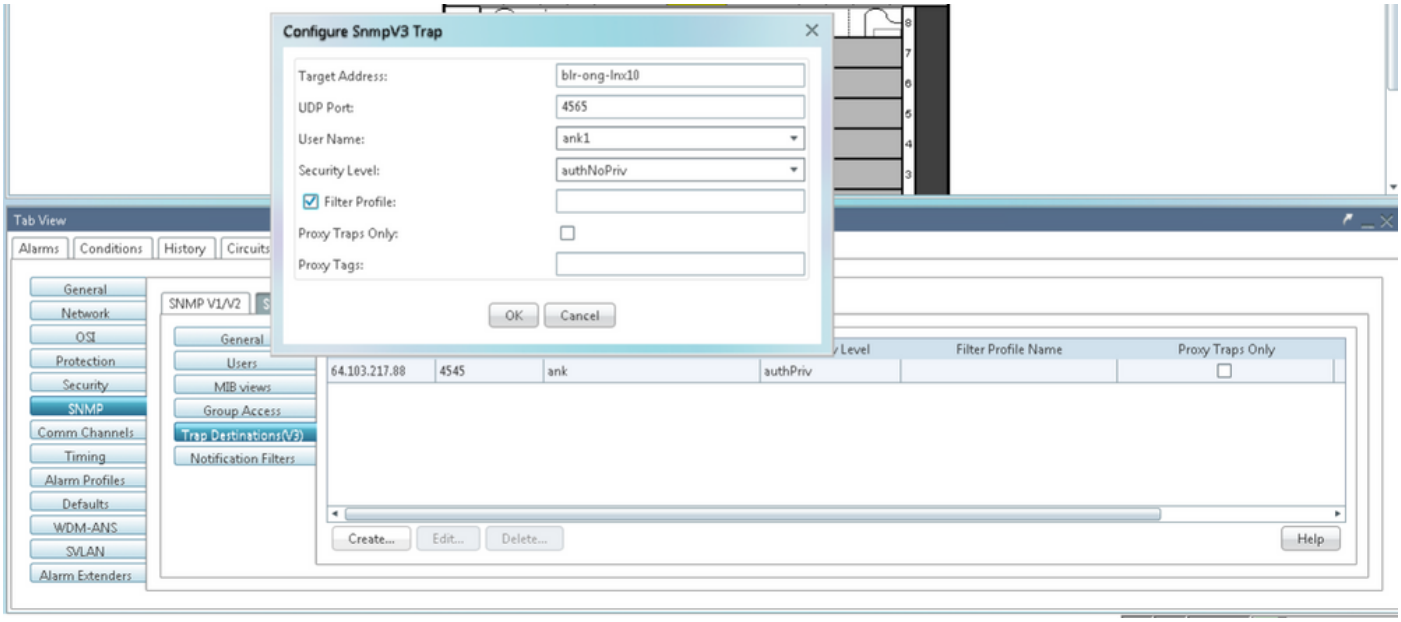
Stap 3. Zorg ervoor dat de MIB-weergave is ingesteld zoals in de afbeelding.



Stap 4. Het configureren van groepstoegang zoals in de afbeelding voor autorisatie-modus.



Stap 5. Navigeer naar **Node View > Provisioning > SNMP > SNMP V3 > Trap Destination (V3)**. Klik op **Maken** en **Configureren** zoals in de afbeelding wordt weergegeven.



Controleer de modus AutoNoPriv

Stap 1. Navigeer naar de NMS server en wandel.

Syntaxis:

```
snmpwalk -v 3 -l authnopriv -u <user name> -a MD5 -A <password> <node IP> <MIB>
```

Voorbeeld:

```
blr-ong-lnx10:154> snmpwalk -v 3 -l authnopriv -u ank1 -a MD5 -A cisco123  10.64.106.40 system

RFC1213-MIB::sysDescr.0 = STRING: "Cisco ONS 15454 M6 10.50-015E-05.18-SPA Factory Defaults
```

```
PLATFORM=15454-M6"

RFC1213-MIB::sysObjectID.0 = OID: CERENT-GLOBAL-REGISTRY::cerent454M6Node

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (430323) 1:11:43.23

RFC1213-MIB::sysContact.0 = ""

RFC1213-MIB::sysName.0 = STRING: "Ankit_40"

RFC1213-MIB::sysLocation.0 = ""

RFC1213-MIB::sysServices.0 = INTEGER: 79
```

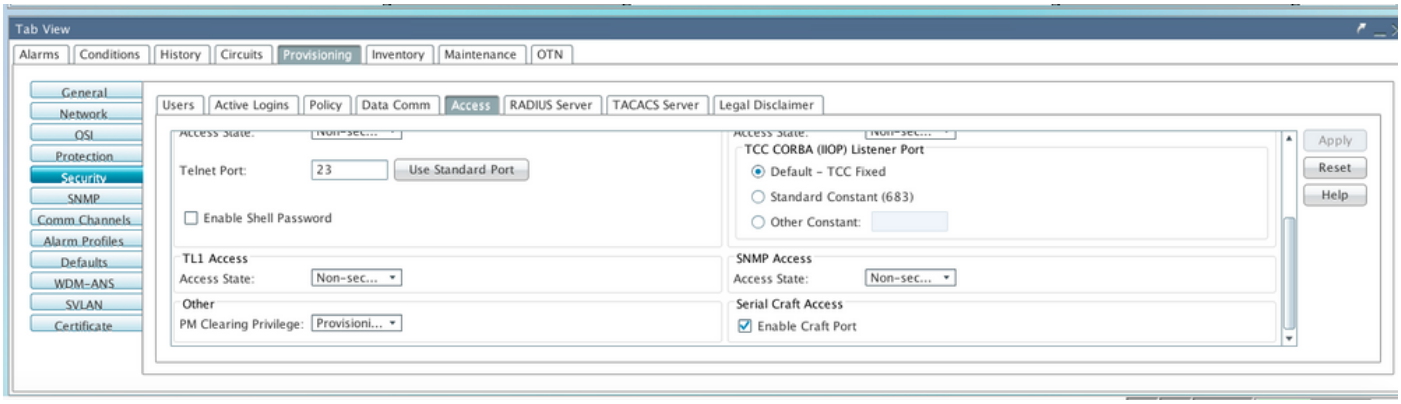
SNMP-trap:

```
snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n" <port number>
```

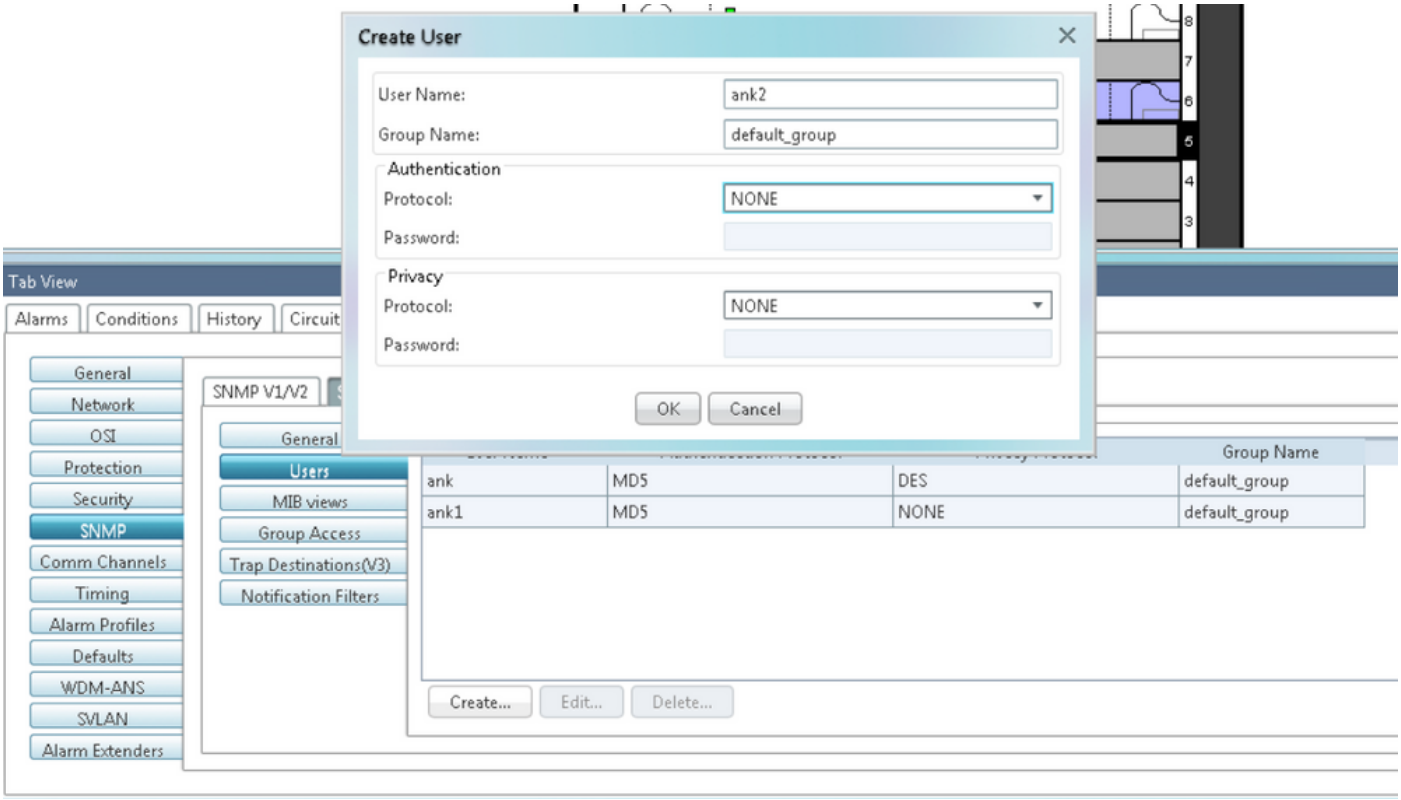
Trap cmd is voor alle versies hetzelfde.

Instellen van geen AutoNoPriv-modus op ONS 15454/NCS 2000 apparaat

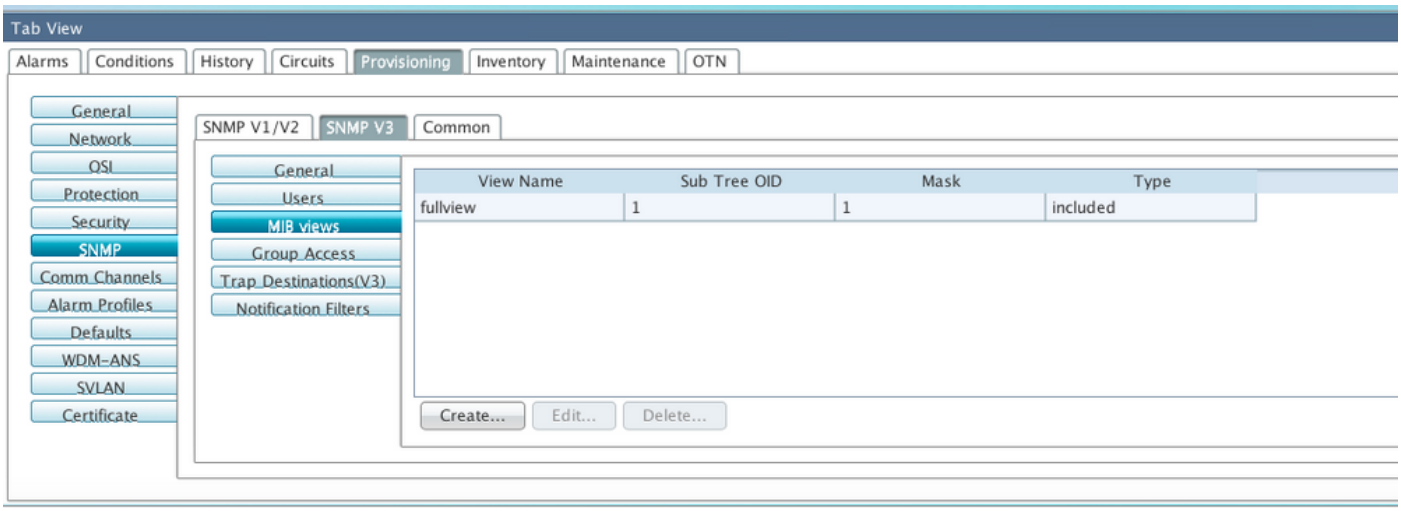
Stap 1. In CTC, navigeer naar **Node View > Provisioning > Beveiliging > Access > Verander de status van toegang tot niet-beveiligde modus** zoals in de afbeelding.



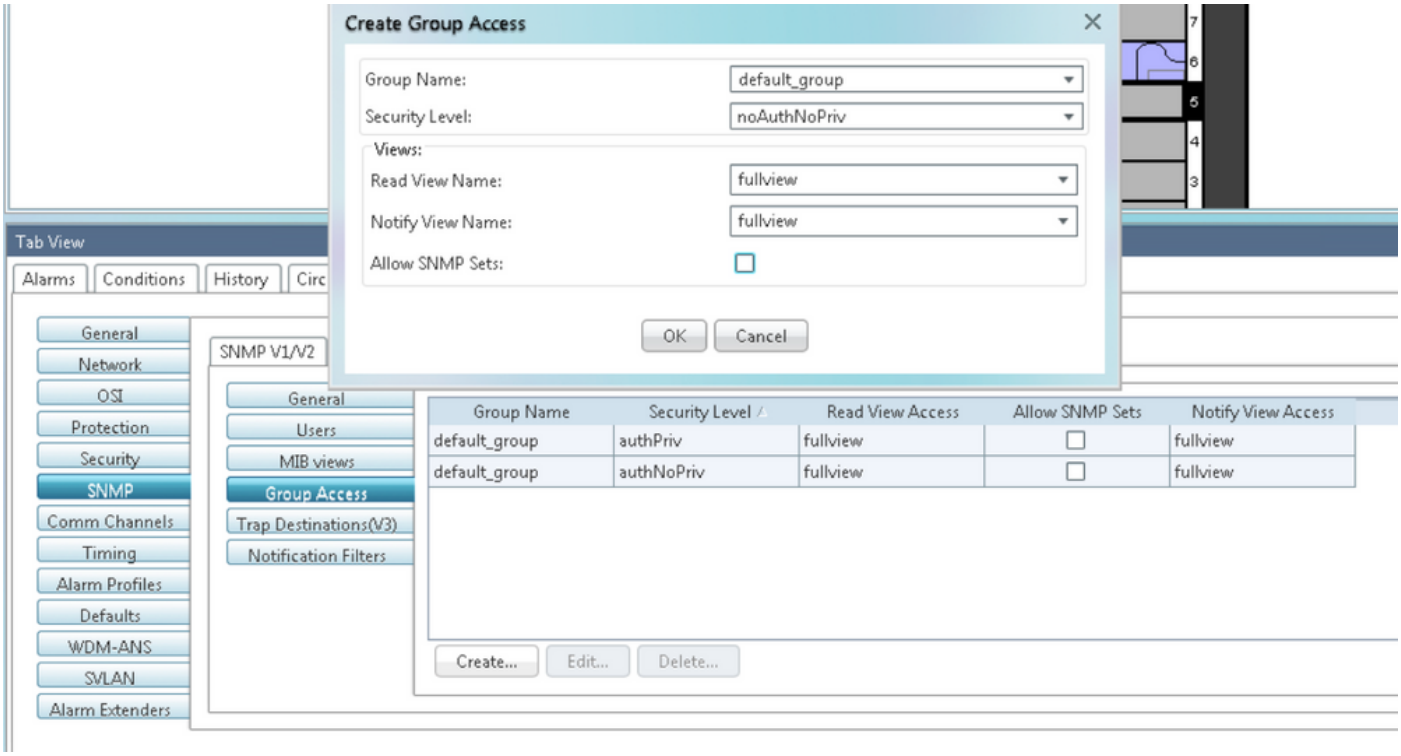
Stap 2. Navigeer naar **Node View > Provisioning > SNMP > SNMP V3 > Gebruikers > Gebruikers maken en configureren** zoals in de afbeelding.



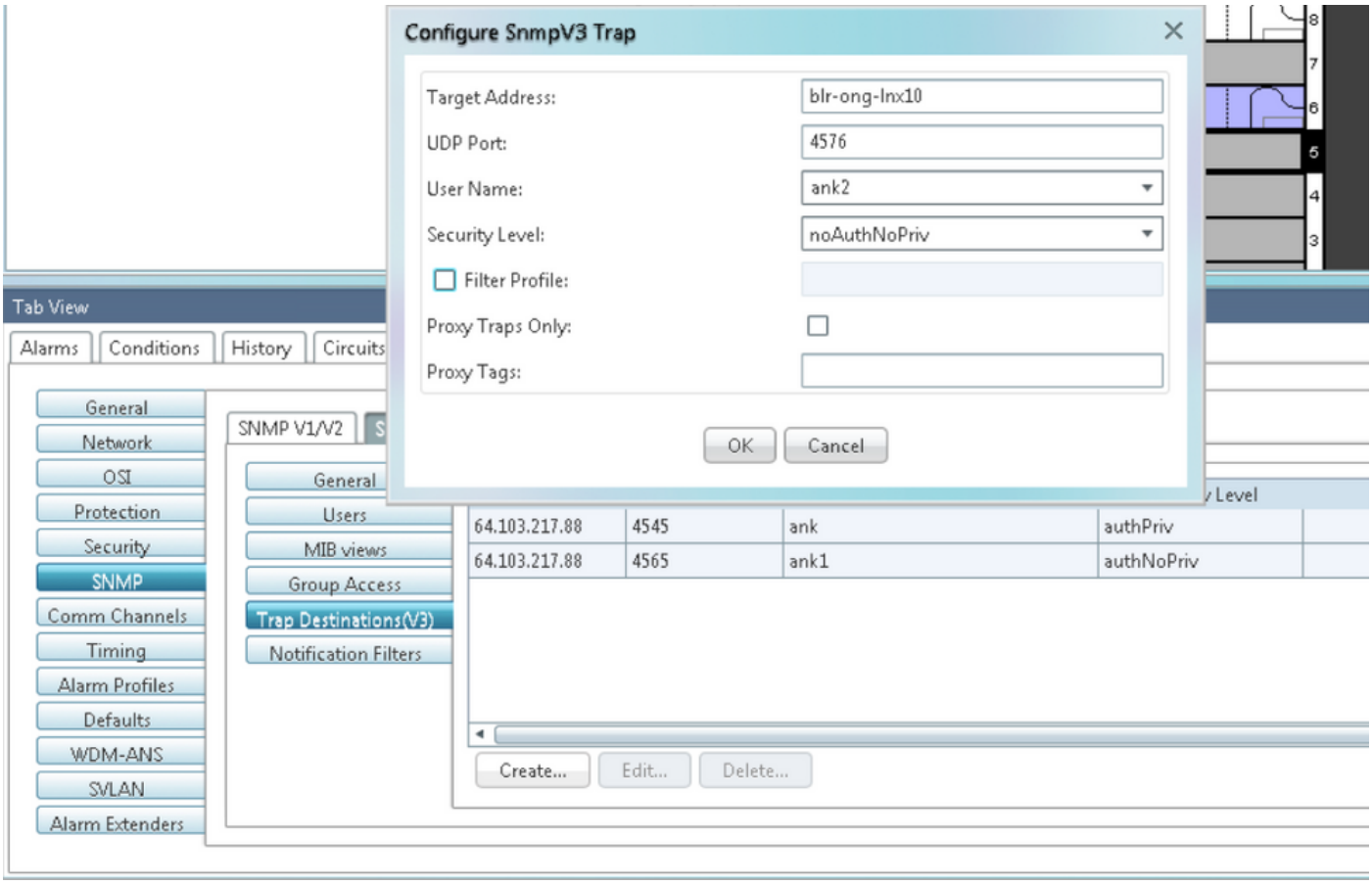
Stap 3. Zorg ervoor dat de **MIB-beelden** zijn geconfigureerd zoals in de afbeelding.



Stap 4. Configureer de groepstoegang zoals in de afbeelding voor de automatische modus.



Stap 5. Navigeer naar **Node View > Provisioning > SNMP > SNMP V3 > Trap Destination (V3)**. Klik op **Maken** en **Configureren** zoals in de afbeelding wordt weergegeven.



Controleer of AutoNoPriv Mode

Stap 1. Navigeer naar de NMS server en wandel.

```
snmpwalk -v 3 -l noauthnopriv -u <user name> <node IP> <MIB>
```

Voorbeeld:

```
blr-ong-lnx10:155> snmpwalk -v 3 -l noauthnopriv -u ank2 10.64.106.40 system

RFC1213-MIB::sysDescr.0 = STRING: "Cisco ONS 15454 M6 10.50-015E-05.18-SPA Factory Defaults
PLATFORM=15454-M6"

RFC1213-MIB::sysObjectID.0 = OID: CERENT-GLOBAL-REGISTRY::cerent454M6Node

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (486910) 1:21:09.10

RFC1213-MIB::sysContact.0 = ""

RFC1213-MIB::sysName.0 = STRING: "Ankit_40"

RFC1213-MIB::sysLocation.0 = ""

RFC1213-MIB::sysServices.0 = INTEGER: 79

blr-ong-lnx10:156>
```

SNMP-trap:

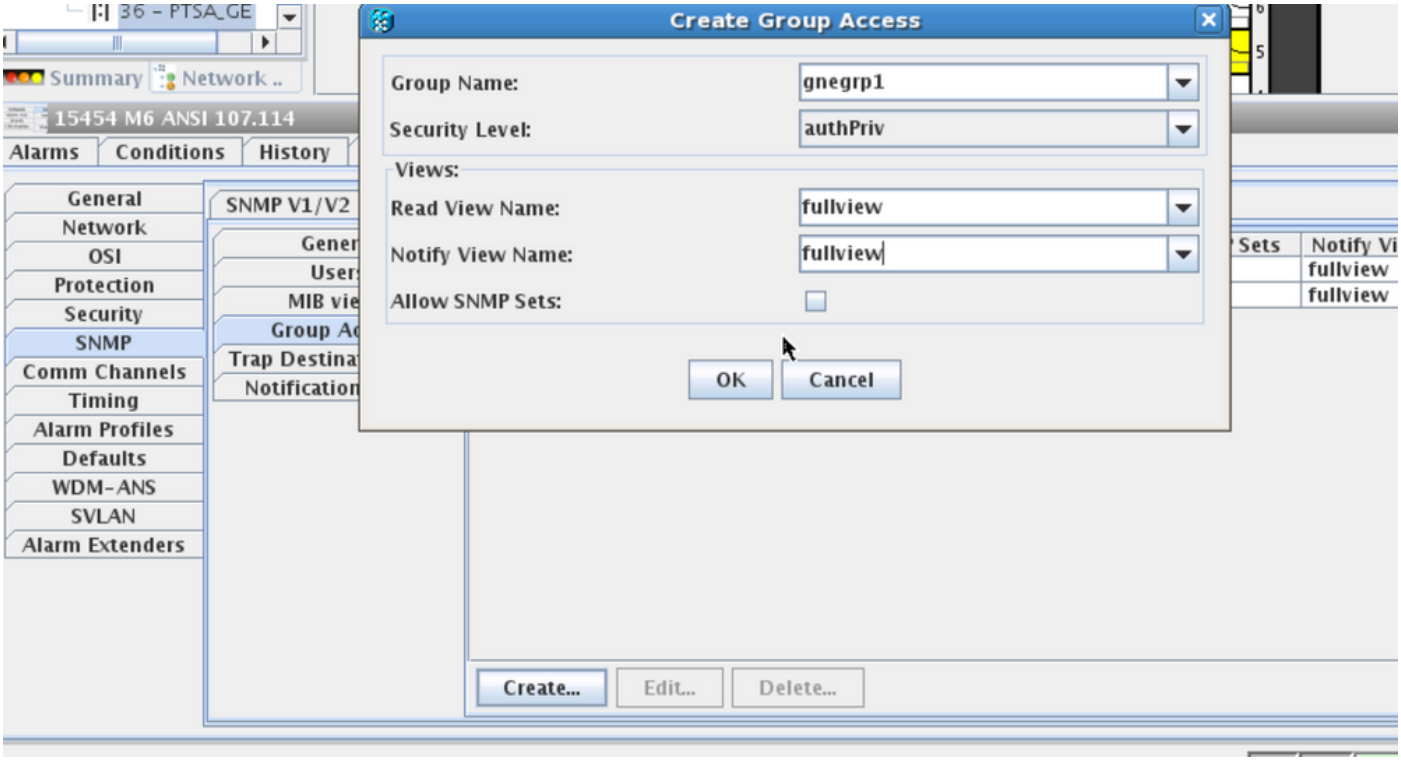
```
snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n" <port number>
```

Trap cmd is voor alle versies hetzelfde.

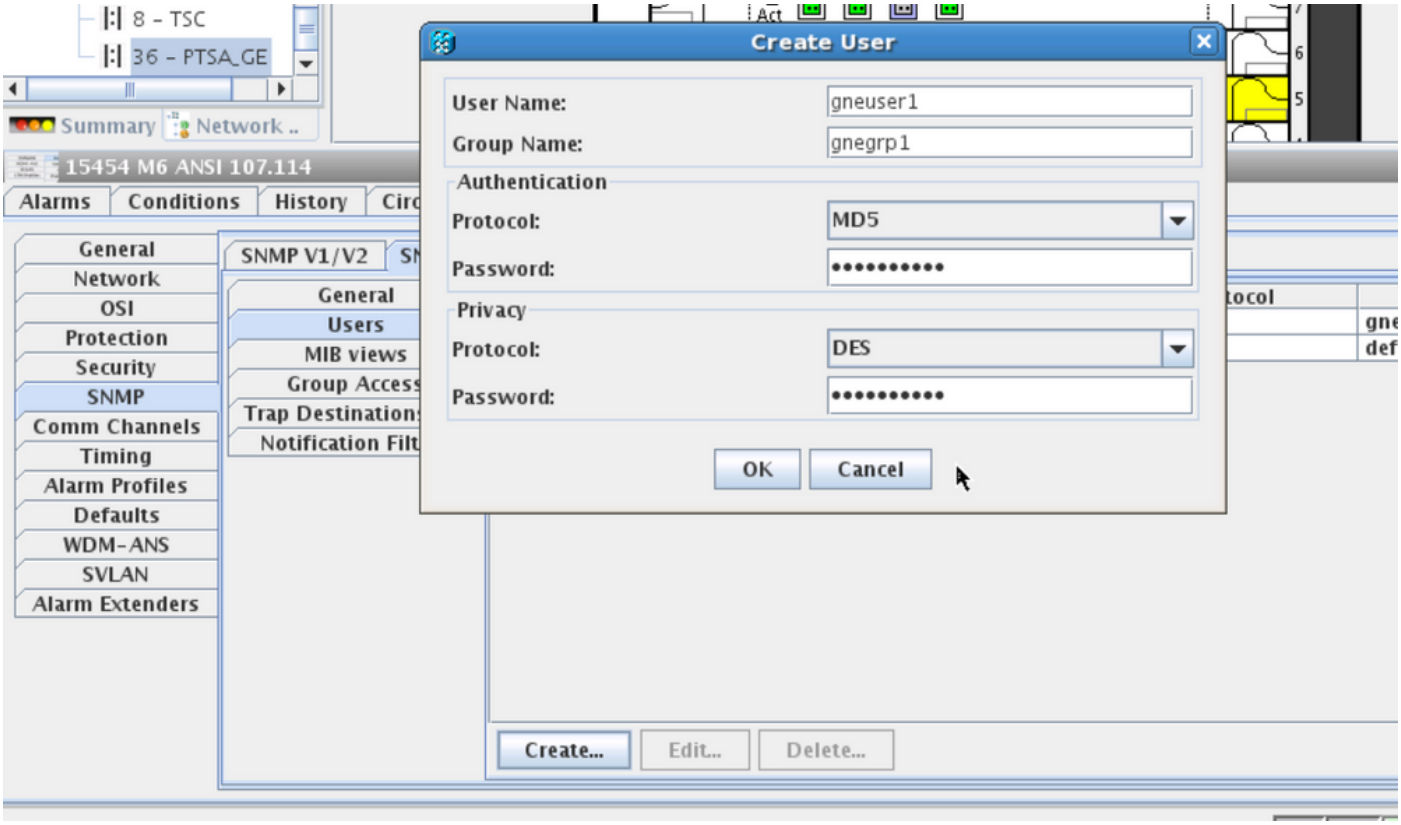
SNMP V3 Trap voor GNE/ENE Setup

Over BNE-knooppunt

Stap 1. navigeren naar **Provisioning > SNMP > SNMP V3 en CToegang tot groep maken (tabblad Toegang groep): Geef een groepsnaam op met Beveiligingsniveau (noAuthnoPriv|AuthnoPriv|authPriv) en volledige weergave Lezen en Melden van de toegang zoals in de afbeelding getoond.**



Stap 2. Maak gebruikerstoegang (tabblad Gebruikers): om een gebruiker met de groepsnaam te maken zoals eerder is gemaakt in het tabblad Toegang voor groep. Typ ook de verificatie op basis van het toegangsniveau zoals in de afbeelding.



Stap 3. Tabblad Bestemming van trap (V3):

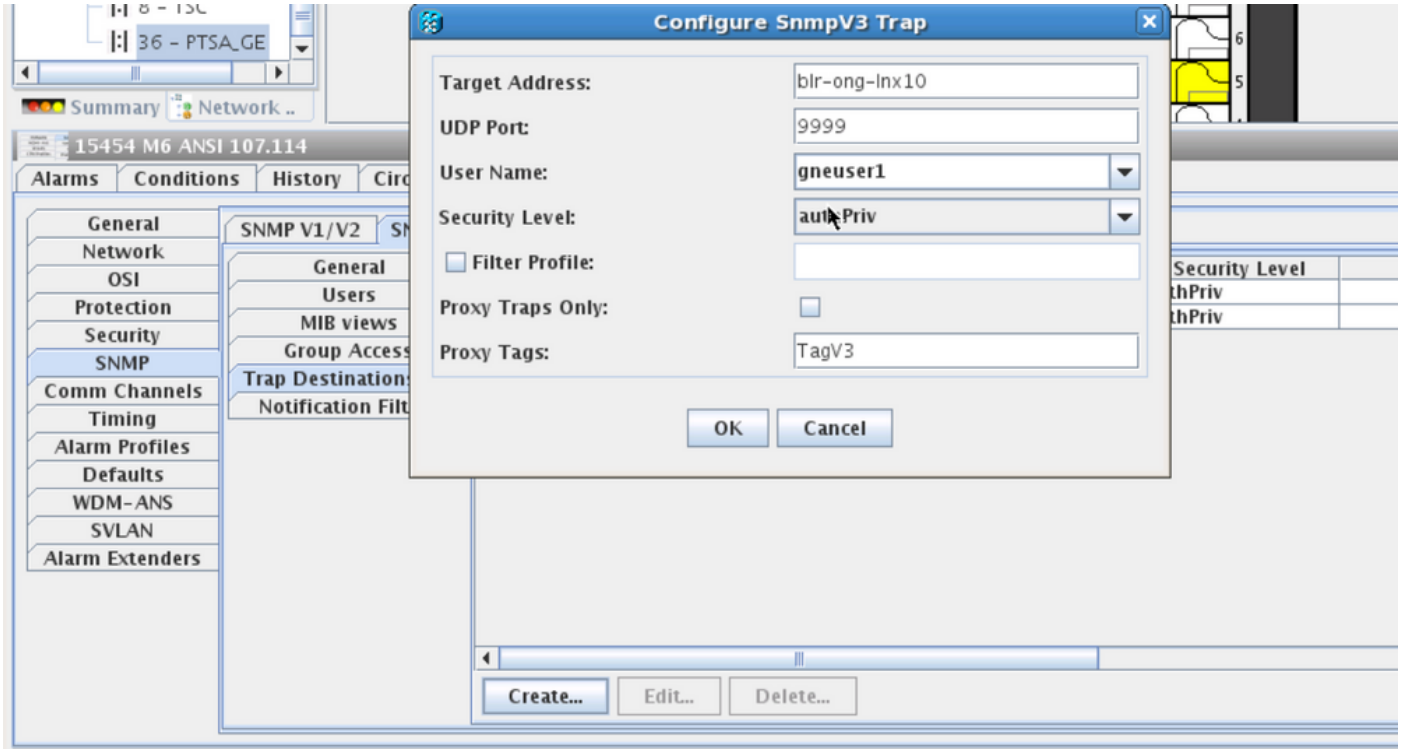
Doeladres: Adres van de NMS server van waar de val zal lopen (bijv. Blr-ong-lnx10).

UDP-poort: Elk havennummer waar de val wordt gehoord (ex 9977).

Gebruikersnaam: Naam van de gebruiker in het tabblad Gebruiker.

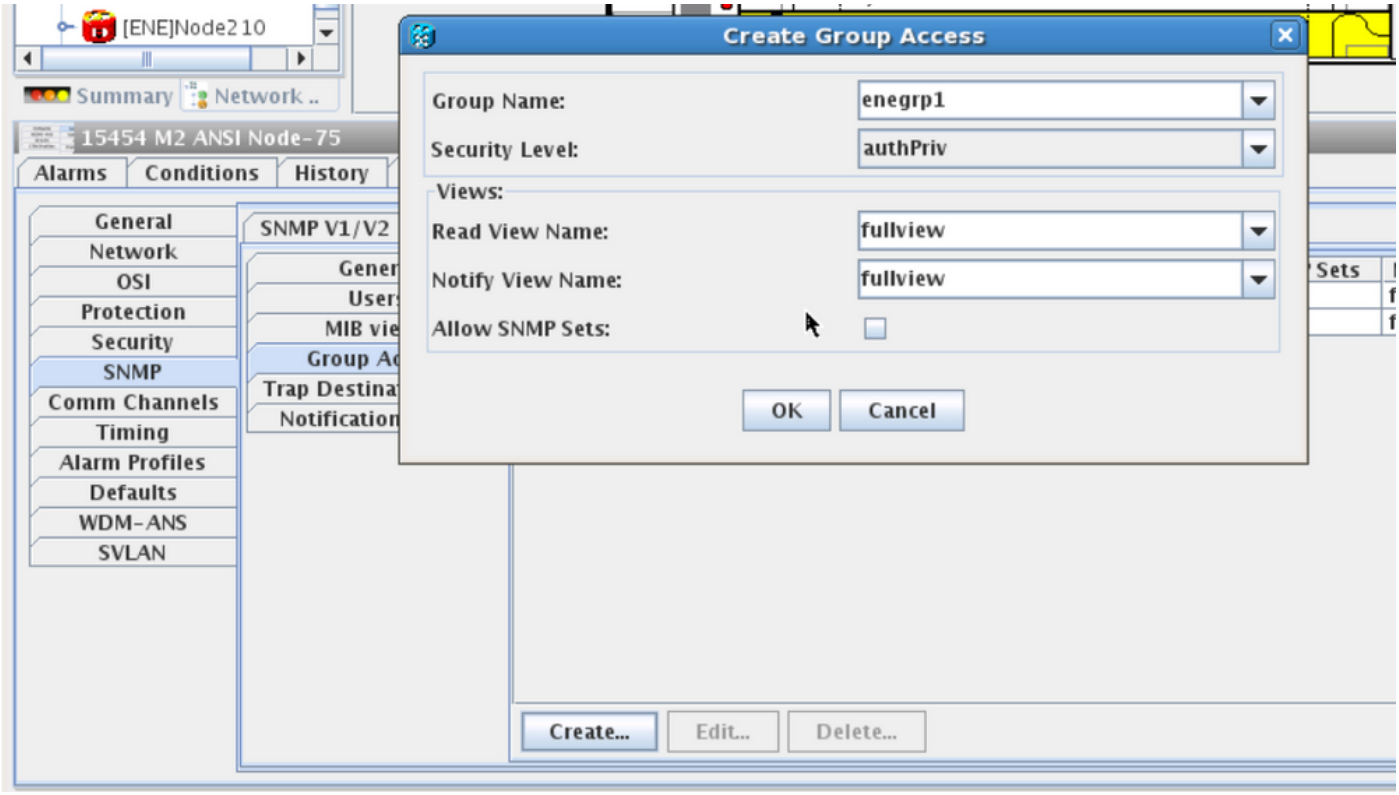
Beveiligingsniveau: Zoals eerder ingesteld in het tabblad Gebruiker.

Proxytags: Geef een proxy-tag op (Ex). Tag75).

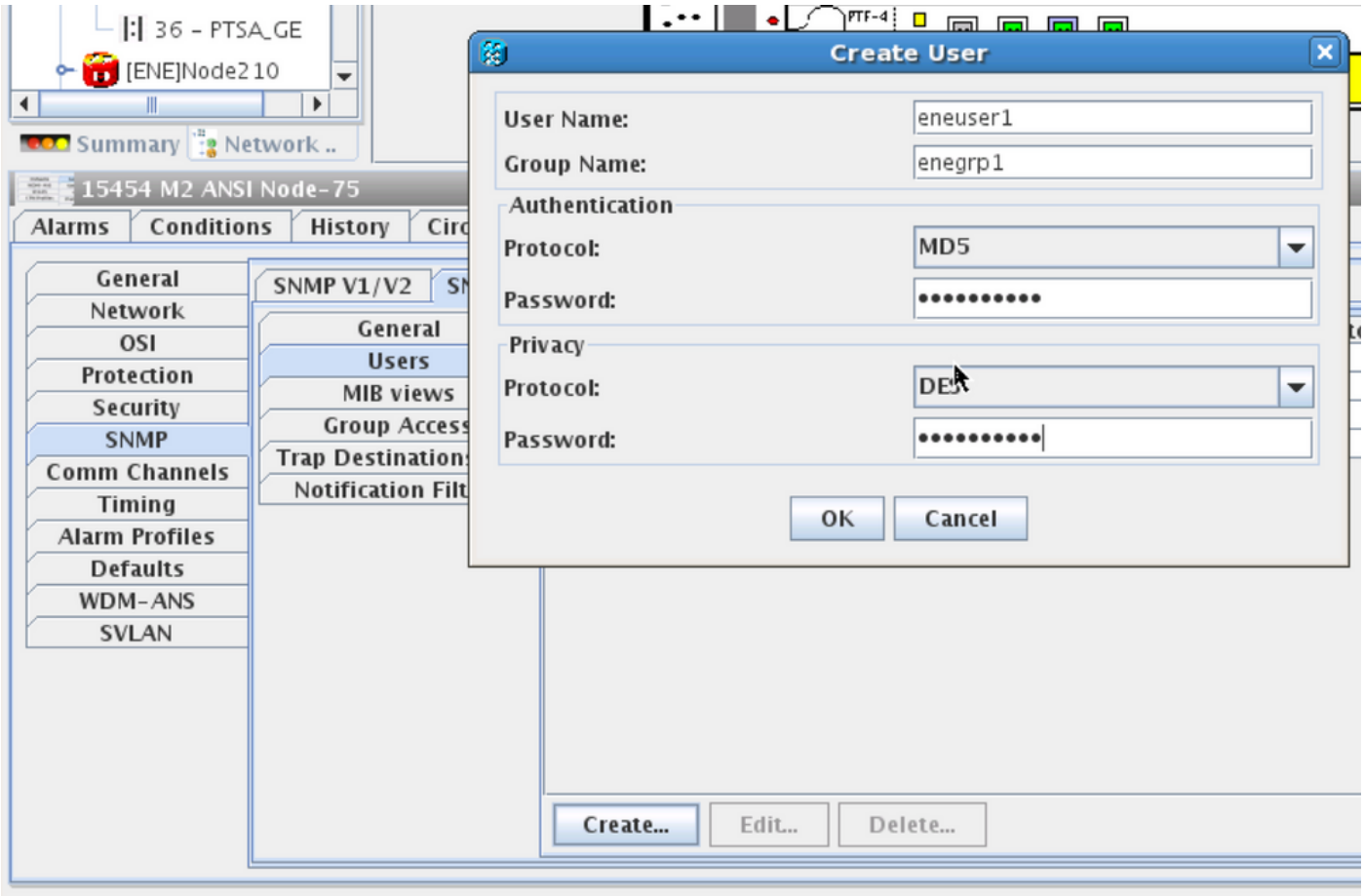


betreffende ENE-knooppunt

Stap 1. navigeren naar **Provisioning > SNMP > SNMP V3 en Groepstoegang (tabblad Groepstoegang):** Geef een groepsnaam een toegangsniveau op (noAuthnoPriv|AuthnoPriv|authPriv) en de volledige weergave Lezen en Melden van de toegang zoals in de afbeelding getoond.



Stap 2. Maak gebruikerstoegang (tabblad Gebruikers): om een gebruiker met de groepsnaam te maken zoals eerder is gemaakt in het tabblad Toegang voor groep. Typ ook de verificatie op basis van het toegangsniveau.



Verzeker een default_group als deze optie in het tabblad User is aangemaakt in het tabblad Group Access voor het geval dit ontbreekt in het tabblad Group Access.

Stap 3. Tabblad Bestemming van trap (V3):

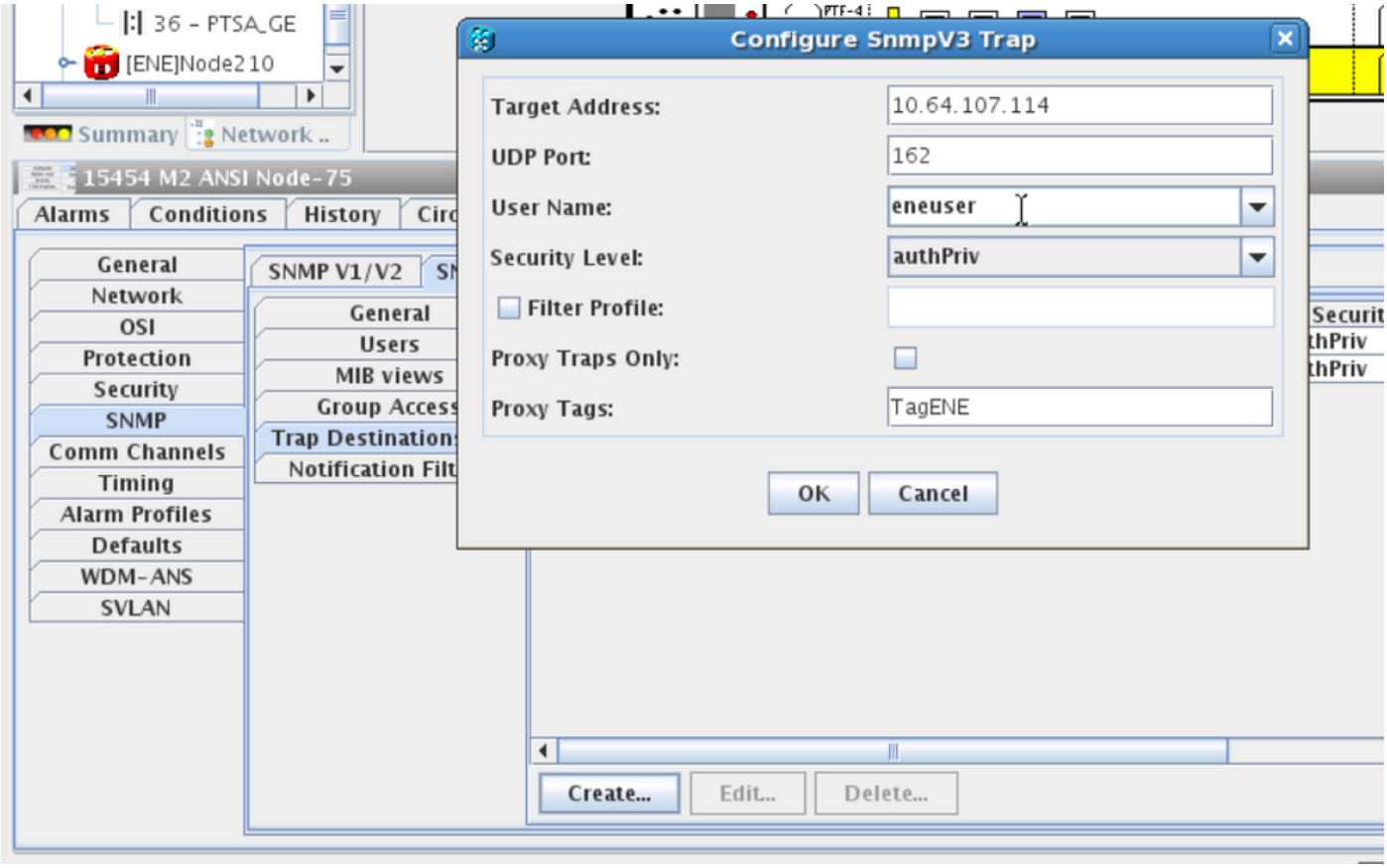
Doeladres: GNE-knooppunt IP.

UDP-poort: 162.

Gebruikersnaam: Naam van de gebruiker in het tabblad Gebruiker.

Beveiligingsniveau: Zoals eerder ingesteld in het tabblad Gebruiker.

Proxytags: Geef een proxy-tag op die gelijk is aan BNE (Ex). Tag75).



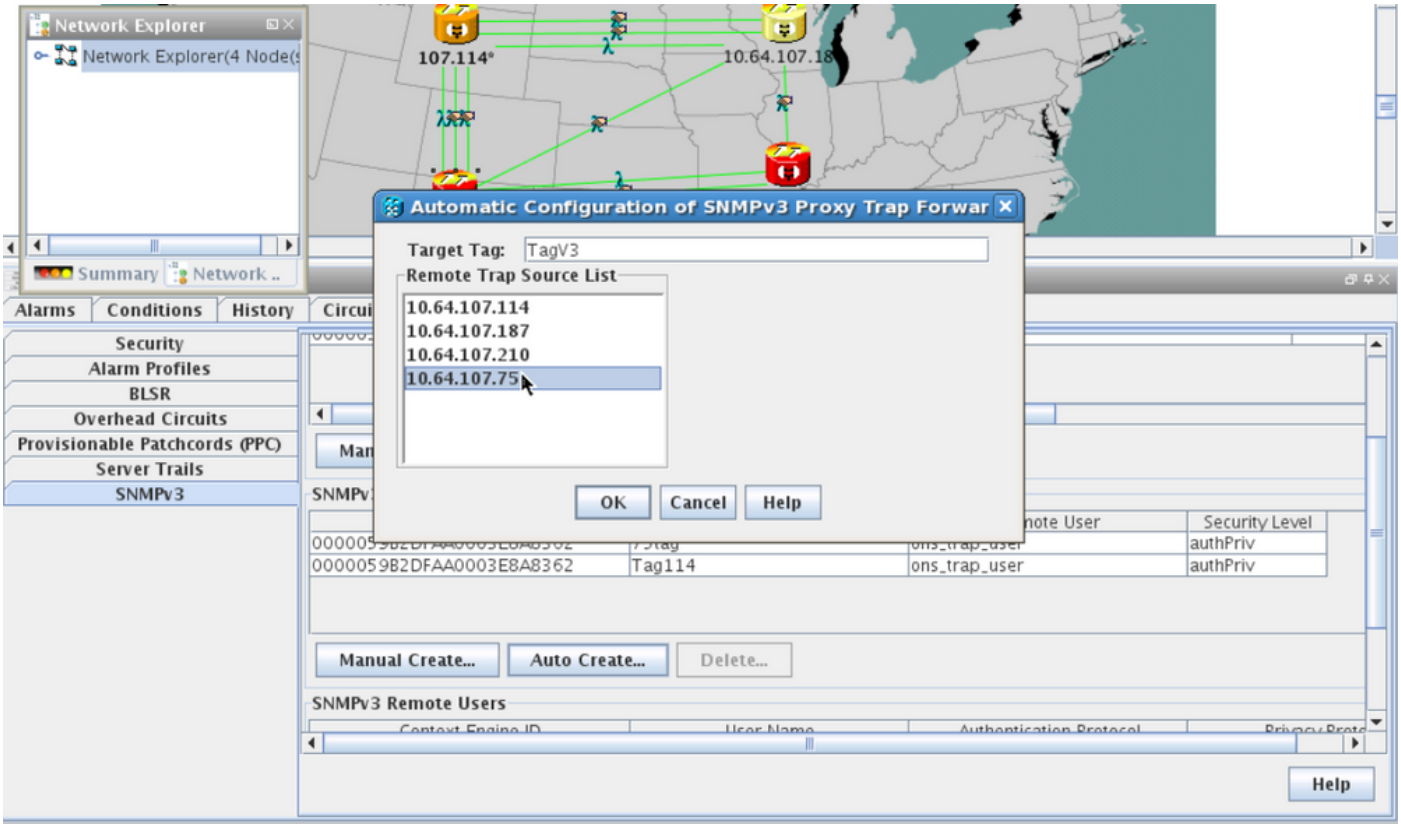
In CTC, navigeer naar netwerkweergave:

Stap 1. Navigeer naar het tabblad **SNMPv3**.

Stap 2. SNMPv3 Proxy-trap voor doorsturen van tabellen: U kunt **handmatig** of **automatisch maken** doen.

Selecteer **Automatisch maken**. In dat geval:

- Streepjesmarkering: Proxytag wordt ingesteld in BNE.
- Remote Trap-bronlijst: Selecteer het ENE-knooppunt van IP zoals in de afbeelding.



Controleer de installatie van BNE/ENE

NMS Server configureren (blr-ong-lnx10):

Stap 1. Voer in de adresmap van de server een directory aan en noem deze **snel**.

Stap 2. Maak onder deze folder een bestand **snmptrapd.conf**.

Stap 3. Creëer in **snmptrapd.conf** deze configuratie:

```
createUser -e 0x
```

```
                              Engine_NO = can be available from CTC. Open GNE node-->Node view-
>Provisioning->SNMP->SNMP V3-->General.
```

SNMP-trap:

```
snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n"
```

wegsmijten op ENE:

Voor aupriv-modus:

```
snmpwalk -v 3 -l authpriv -u <user_name> -a MD5 -A <auth_password>123 -x DES -X <des_password> -
E <ene_engine_id> <gne_ip_address> <OID>
```

Voor authentieke modus:

```
snmpwalk -v 3 -l authnopriv -u <user_name> -a MD5 -A <auth_password>  -E <ene_engine_id>
<gne_ip_address> <OID>
```

Voor de nieuwe modus:

```
snmpwalk -v 3 -l authpriv -u
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.