# Konfigurieren von SNMPv3 auf Cisco ONS15454-/NCS2000-Geräten

## Inhalt



## Einführung

Dieses Dokument beschreibt Schritt-für-Schritt-Anweisungen zur Konfiguration des Simple Network Management Protocol Version 3 (SNMPv3) auf ONS15454/NCS2000-Geräten. Alle Themen enthalten Beispiele.

> **Hinweis:** Die Liste der in diesem Dokument enthaltenen Attribute ist weder vollständig noch autoritär und kann jederzeit ohne Aktualisierung dieses Dokuments geändert werden.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Benutzeroberfläche des Cisco Transport Controller (CTC)
- Grundlegendes Serverwissen
- Grundlegende Linux-/Unix-Befehle

## Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

# Konfiguration

## Auf einem Standalone/Multishelf-Knoten

### Konfigurieren des authPriv-Modus auf ONS15454-/NCS2000-Geräten

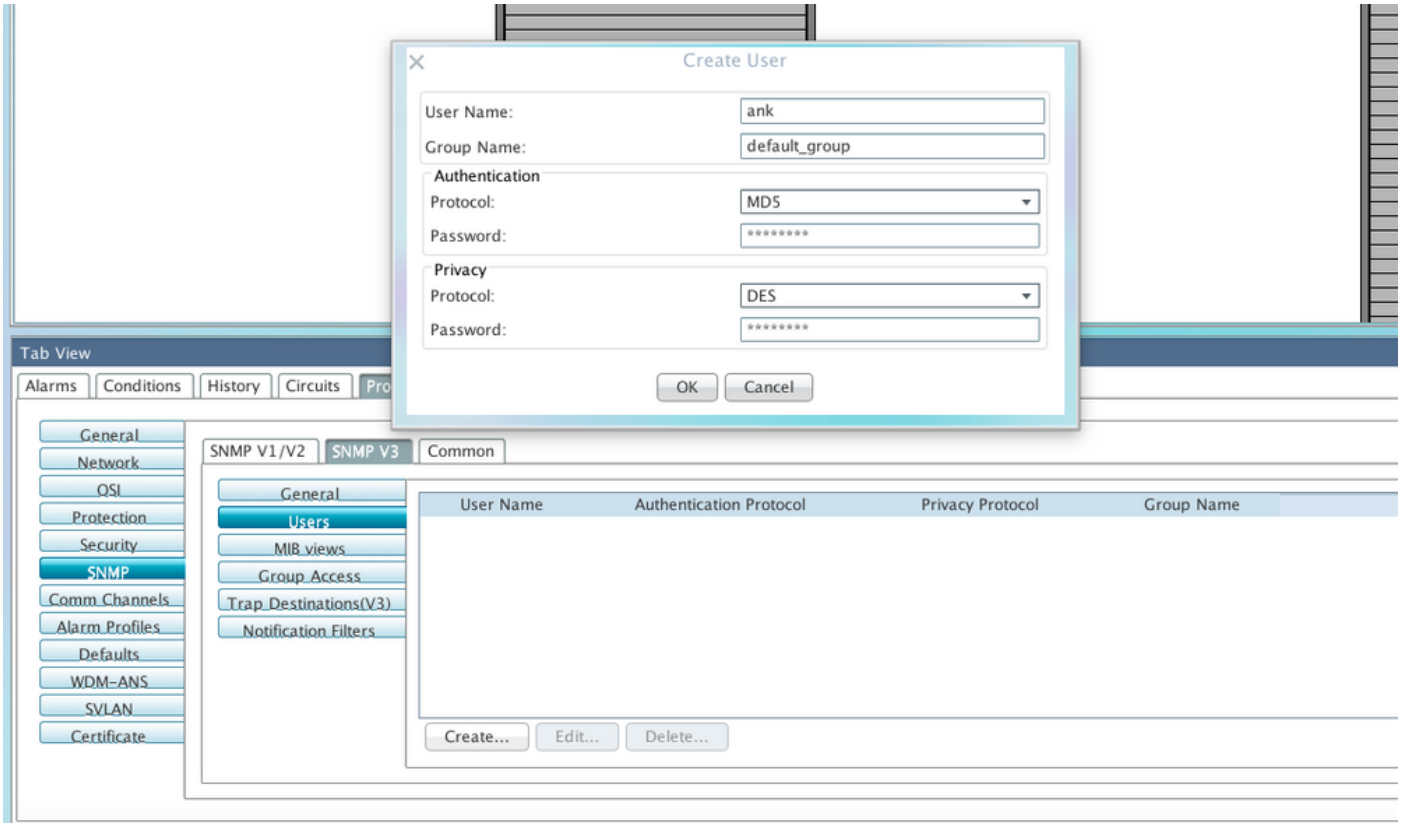
Schritt 1: Melden Sie sich mit den Super User-Anmeldeinformationen über CTC beim Knoten an.

Schritt 2: Navigieren Sie zu **Node View > Provisioning > SNMP > SNMP V3**.

Schritt 3: Navigieren Sie zur Registerkarte **Benutzer**. Erstellen Sie Benutzer.

```
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>
```

Schritt 4: Klicken Sie auf **OK**, wie im Bild gezeigt.




Spezifikationen:

Benutzername: Geben Sie den Namen des Benutzers auf dem Host an, der mit dem Agenten verbunden ist. Der Benutzername muss mindestens 6 und höchstens 40 Zeichen enthalten (maximal 39 Zeichen für die TACACS- und RADIUS-Authentifizierung). Es enthält alphanumerische Zeichen (a-z, A-Z, 0-9), und die zulässigen Sonderzeichen sind @, "-" (Bindestrich) und "". (Punkt). Der Benutzername muss aus Gründen der TL1-Kompatibilität 6 bis 10 Zeichen lang sein.

Gruppenname: Geben Sie die Gruppe an, der der Benutzer angehört.

Authentifizierung:

Protokoll - Wählen Sie den Authentifizierungsalgorithmus aus, den Sie verwenden möchten. Die Optionen sind KEINE, MD5 und SHA.

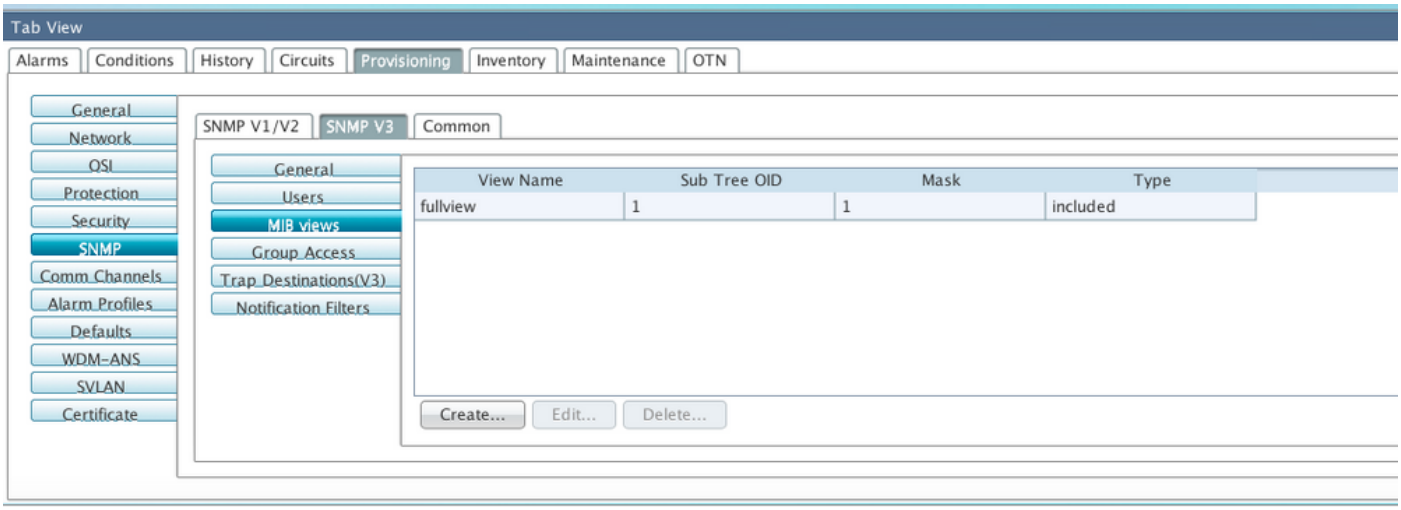
Passwort: Geben Sie ein Passwort ein, wenn Sie MD5 oder SHA auswählen. Standardmäßig ist die Kennwortlänge auf mindestens acht Zeichen festgelegt.

Datenschutz - Initiiert eine Sitzung zum Festlegen der Datenschutzstufe, die es dem Host ermöglicht, den Inhalt der Nachricht zu verschlüsseln, die an den Agenten gesendet wird.

Protokoll - Wählen Sie den Algorithmus zur Datenschutzauthentifizierung aus. Die verfügbaren Optionen sind None (Keine), DES und AES-256-CFB.

Kennwort: Geben Sie ein Kennwort ein, wenn Sie ein anderes Protokoll als "Keine" auswählen.

Schritt 5: Stellen Sie sicher, dass MIB-Ansichten gemäß diesem Image konfiguriert sind.




Spezifikationen:

Name - Name der Ansicht.

Subtree OID - Die MIB-Unterstruktur, die in Kombination mit der Maske die Familie der Unterbäume definiert.

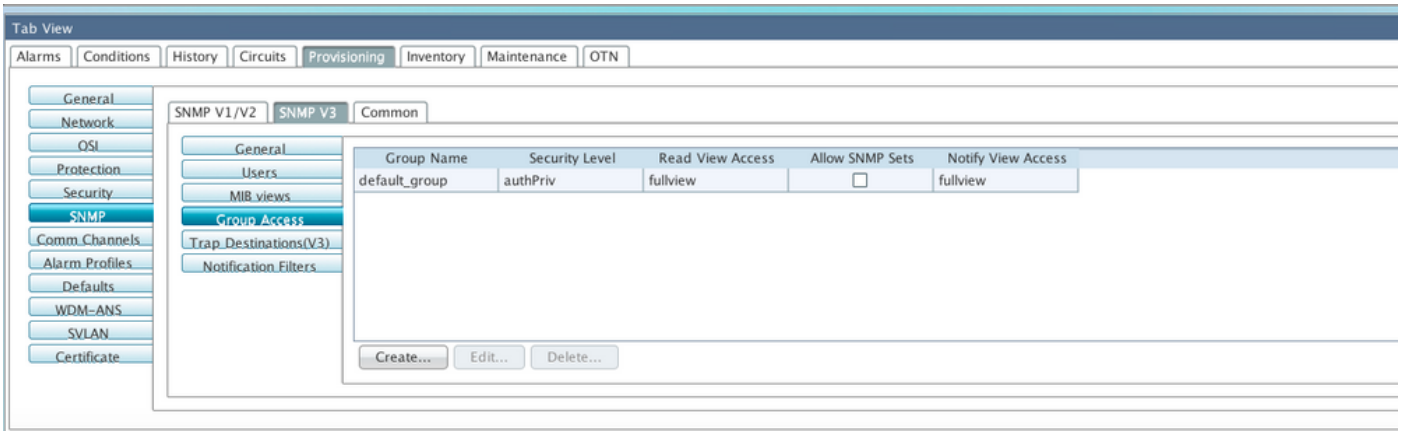
Bitmaske - Eine Familie von View-Unterbäumen. Jedes Bit in der Bitmaske entspricht einer Unterkennung der Substruktur-OID.

Typ - Wählen Sie den Ansichtstyp aus. Optionen sind inklusive und ausgeschlossen.

Der Typ legt fest, ob die durch die Unterstruktur-OID und die Bit-Maske-Kombination definierte Unterbaufamilie in den Benachrichtigungsfilter eingeschlossen oder ausgeschlossen wird.

Schritt 6: Konfigurieren Sie den Gruppenzugriff, wie im Bild gezeigt. Standardmäßig ist der Gruppenname default_group und die Sicherheitsstufe authPriv.

**Hinweis:** Der Gruppenname muss mit dem beim Erstellen des Benutzers in Schritt 3 übereinstimmen.




Spezifikationen:

Gruppenname: Der Name der SNMP-Gruppe oder eine Auflistung von Benutzern, die eine gemeinsame Zugriffsrichtlinie verwenden.

Sicherheitsstufe - Die Sicherheitsstufe, für die die Zugriffsparameter definiert sind. Wählen Sie

eine der folgenden Optionen aus:

noAuthNoPriv: Verwendet eine Übereinstimmung mit dem Benutzernamen für die Authentifizierung.

AuthNoPriv - Stellt Authentifizierung auf Basis der HMAC-MD5- oder HMAC-SHA-Algorithmen bereit.

AuthPriv - Bietet Authentifizierung auf Basis der HMAC-MD5- oder HMAC-SHA-Algorithmen. DES 56-Bit-Verschlüsselung, die neben der Authentifizierung auf dem CBC-DES-Standard (DES-56) basiert.

Wenn Sie authNoPriv oder authPriv für eine Gruppe auswählen, muss der entsprechende Benutzer mit einem Authentifizierungsprotokoll und einem Kennwort, mit Datenschutzprotokoll und Kennwort oder beidem konfiguriert werden.

Ansichten

Read View Name (Name anzeigen) - Name der Leseansicht für die Gruppe.

Benachrichtigungsansichtname - Benachrichtigungsansichtsname für die Gruppe.

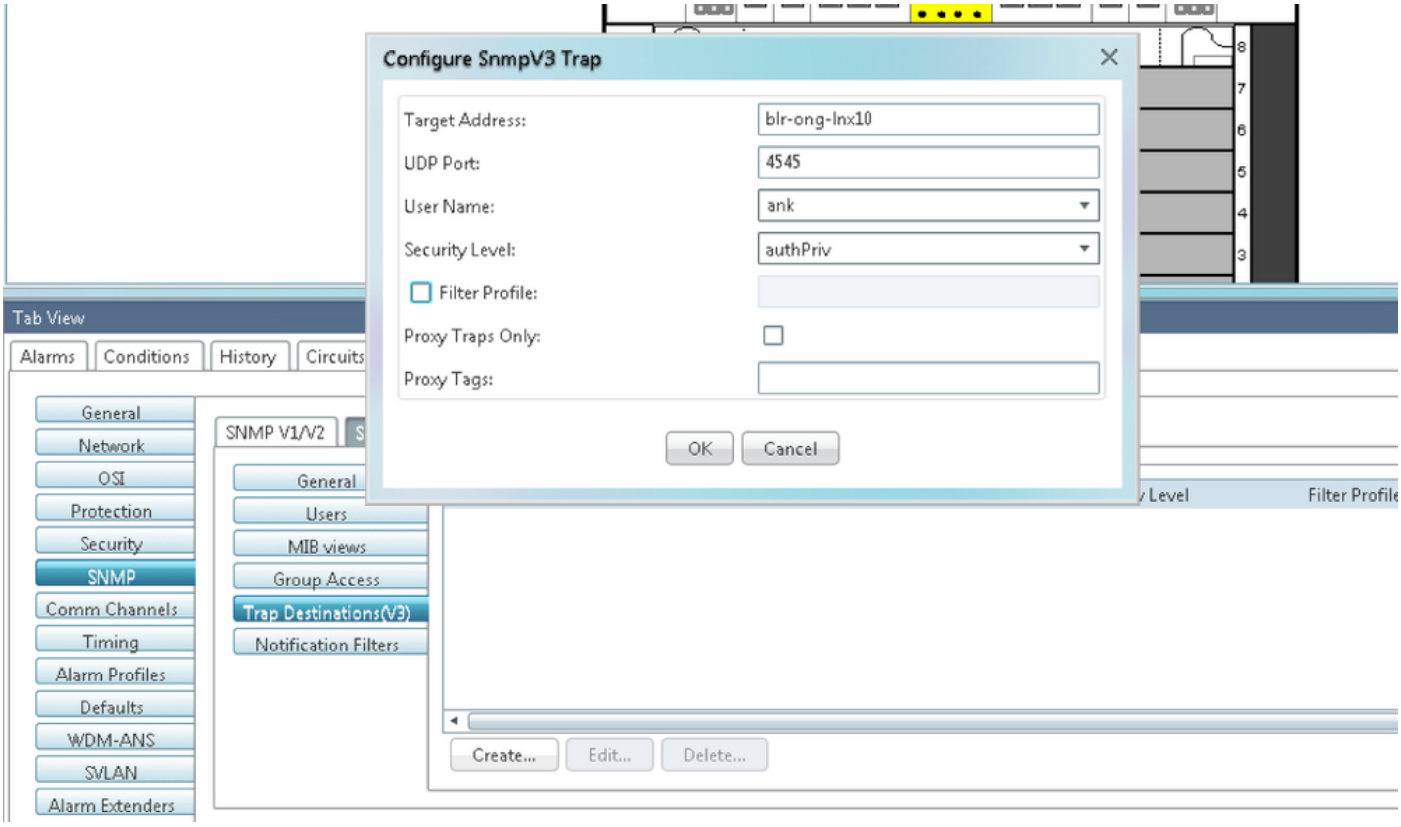
SNMP-Sets zulassen - Aktivieren Sie dieses Kontrollkästchen, wenn der SNMP-Agent SNMP-SET-Anforderungen akzeptieren soll. Wenn dieses Kontrollkästchen nicht aktiviert ist, werden SET-Anforderungen abgelehnt.

**Hinweis:** Der SNMP SET-Anforderungszugriff wird für sehr wenige Objekte implementiert.

Schritt 7: Navigieren Sie zu **Knotenansicht > Provisioning > SNMP > SNMP V3 > Trap Destination (V3)**. Klicken Sie auf **Erstellen** und **Konfigurieren**.

```
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
```

Schritt 8: Klicken Sie auf **OK**, wie im Bild gezeigt.




**Hinweis:** blr-ong-lnx10 ist der NMS-Server.

Spezifikationen:

Zieladresse: Ziel, an das die Traps gesendet werden sollen. Verwenden Sie eine IPv4- oder eine IPv6-Adresse.

UDP-Port - UDP-Portnummer, die der Host verwendet. Der Standardwert ist 162.

Benutzername: Geben Sie den Namen des Benutzers auf dem Host an, der mit dem Agenten verbunden ist.

Sicherheitsstufe - Wählen Sie eine der folgenden Optionen aus:

noAuthNoPriv: Verwendet eine Übereinstimmung mit dem Benutzernamen für die Authentifizierung.

AuthNoPriv - Stellt Authentifizierung auf Basis der HMAC-MD5- oder HMAC-SHA-Algorithmen bereit.

AuthPriv - Bietet Authentifizierung auf Basis der HMAC-MD5- oder HMAC-SHA-Algorithmen. DES 56-Bit-Verschlüsselung, die neben der Authentifizierung auf dem CBC-DES-Standard (DES-56) basiert.

Filterprofil: Aktivieren Sie dieses Kontrollkästchen, und geben Sie den Namen des Filterprofils ein. Traps werden nur gesendet, wenn Sie einen Filterprofilnamen angeben und einen Benachrichtigungsfilter erstellen.

Nur Proxy-Traps: Bei Auswahl dieser Option werden nur Proxy-Traps aus der ENE weitergeleitet. Traps von diesem Knoten werden nicht an das Trap-Ziel gesendet, das durch diesen Eintrag identifiziert wird.

Proxytags: Geben Sie eine Liste von Tags an. Die Tag-Liste ist nur dann auf einem GNE erforderlich, wenn ein ENE Traps an das Trap-Ziel senden muss, das durch diesen Eintrag identifiziert wird, und das GNE als Proxy verwenden möchte.

### NMS-Server konfigurieren (blr-ong-lnx10)

Schritt 1: Erstellen Sie im Stammverzeichnis des Servers ein Verzeichnis mit dem Namen **snmp**.

Schritt 2: Erstellen Sie unter diesem Verzeichnis eine Datei **snmptrapd.conf**.

Schritt 3: Ändern Sie die Datei **snmptrapd.conf in**:

```
vi snmptrapd.conf

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

Beispiele:

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

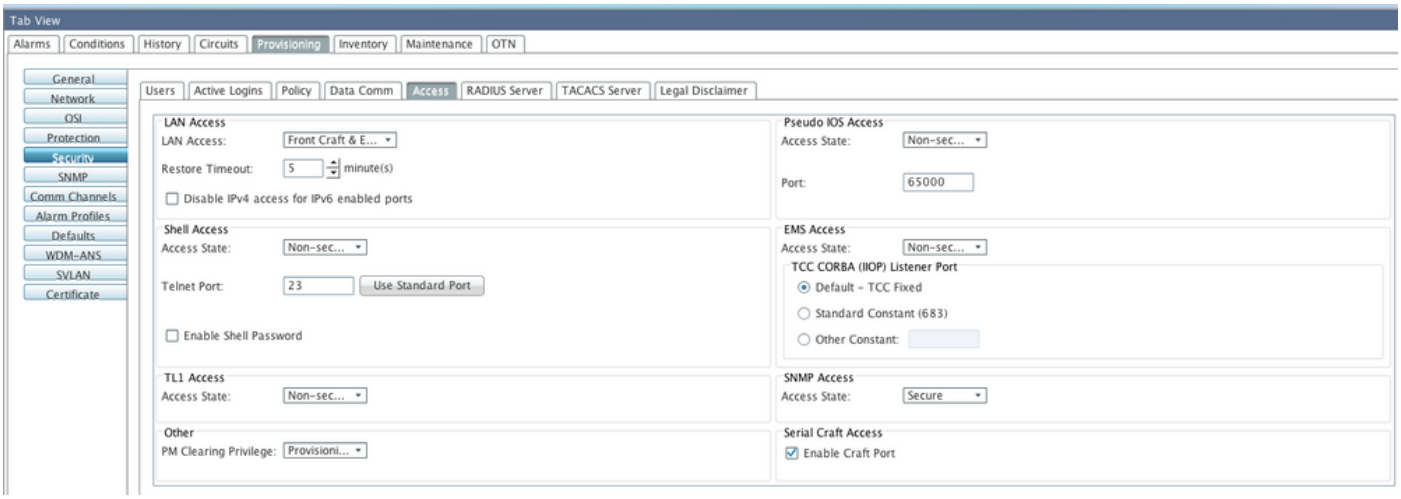
In diesem Beispiel:

```
user_name=ank

MD5 password = cisco123

DES password  = cisco123

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

**Node view > Provisioning > SNMP > SNMP V3 > General**

### Authentifizierungsmodus überprüfen

Schritt 1: Navigieren Sie im CTC zu **Node View > Provisioning > Security > Access > Change snmp access state to Secure (Knotenansicht > Bereitstellung > Sicherheit > Zugriff > SNMP-Zugriffsstatus ändern** wie im Bild gezeigt.




Schritt 2: Navigieren Sie zum NMS-Server, und führen Sie einen Snapshot aus.

Syntax:

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

Beispiel:

```
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
```

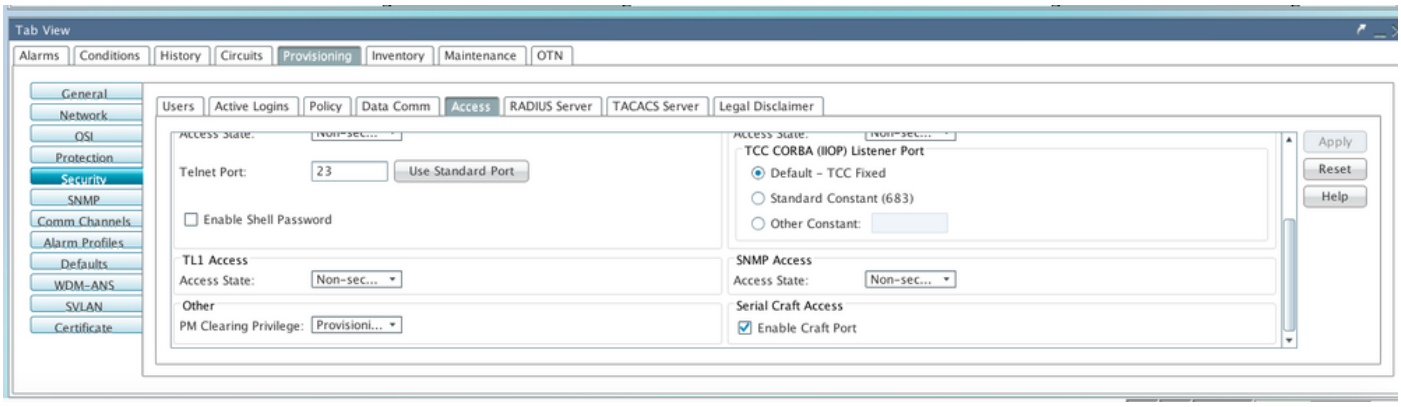
SNMP-Trap:

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

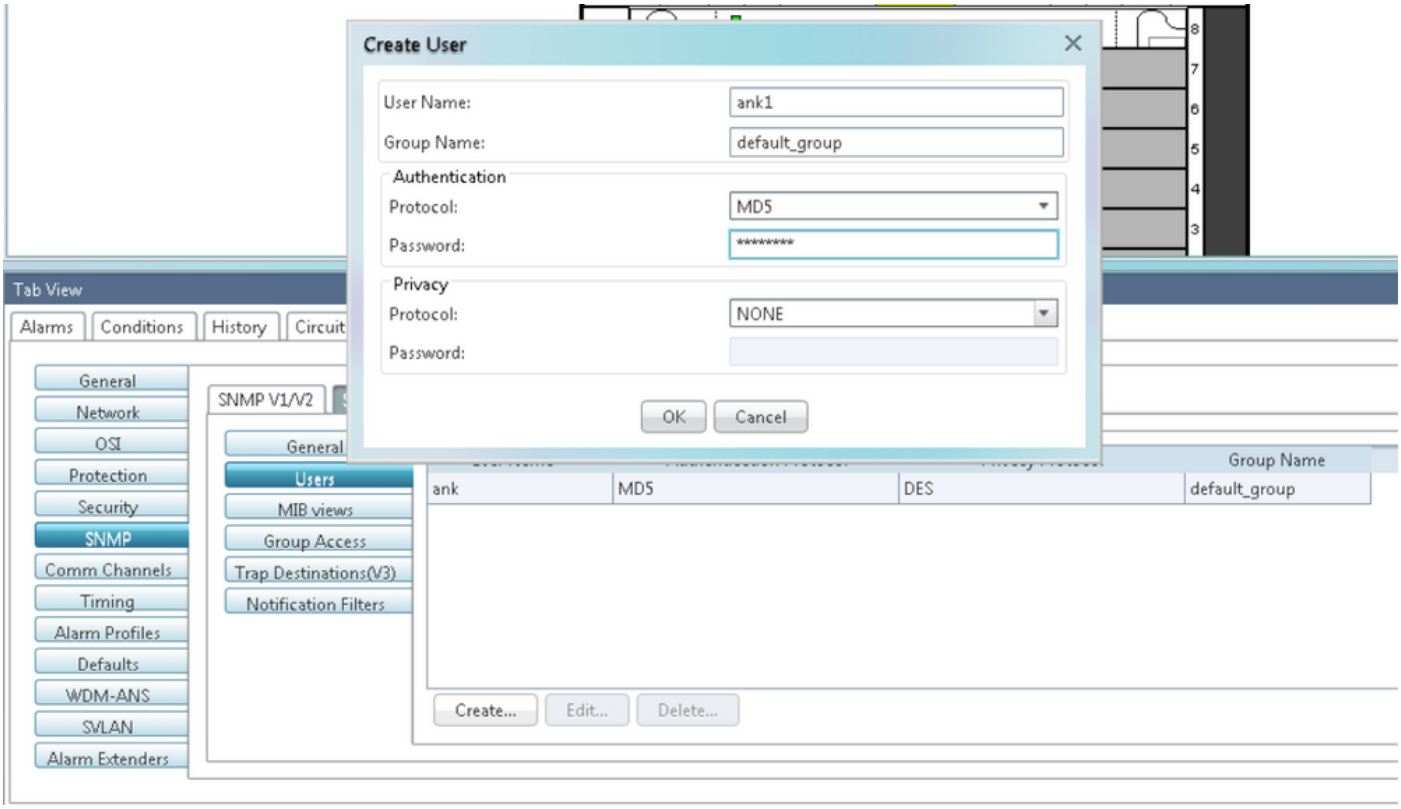
Trap cmd ist für alle Versionen identisch.

## Konfigurieren des authNoPriv-Modus auf ONS15454/NCS2000-Geräten

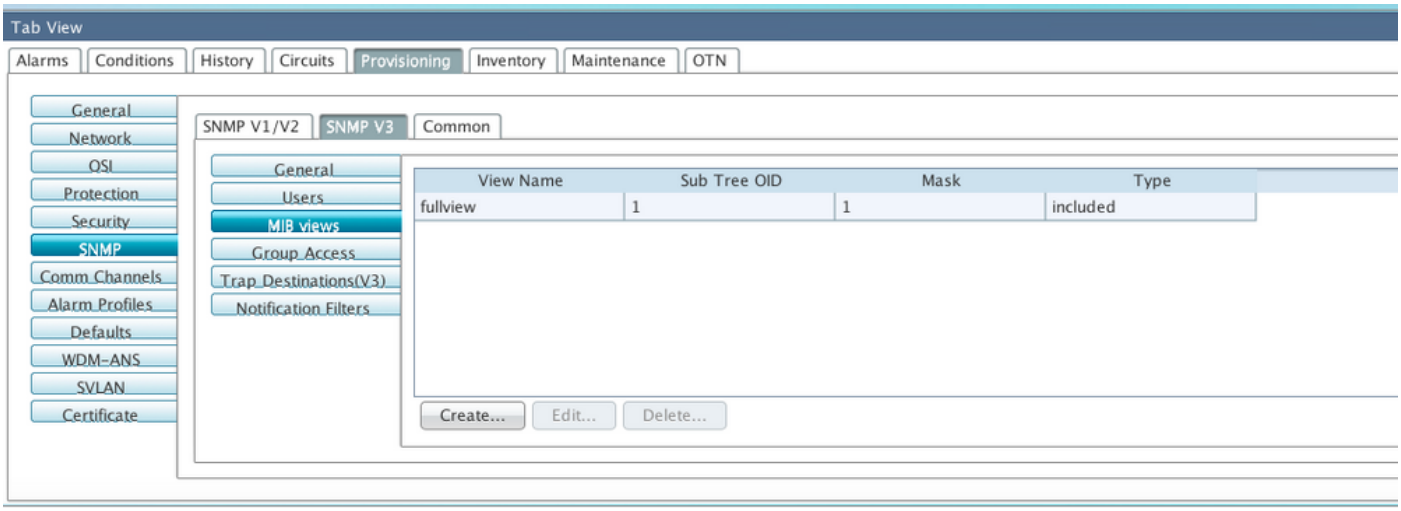
Schritt 1: Navigieren Sie im CTC zu **Node View > Provisioning > Security > Access > Change snmp access state to Non secure mode** as in the image.



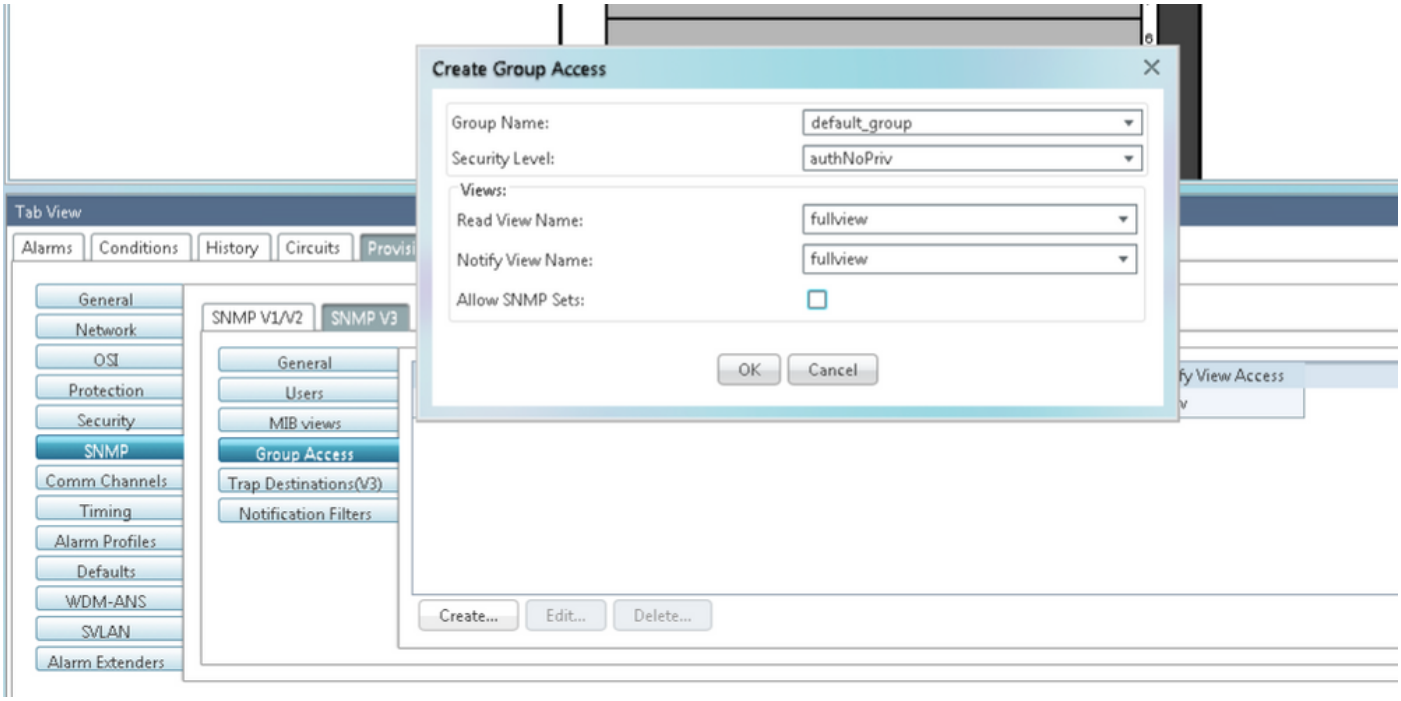

Schritt 2: Navigieren Sie zu **Knotenansicht > Provisioning > SNMP > SNMP V3 > Users > Create User** und konfigurieren Sie wie im Bild gezeigt.



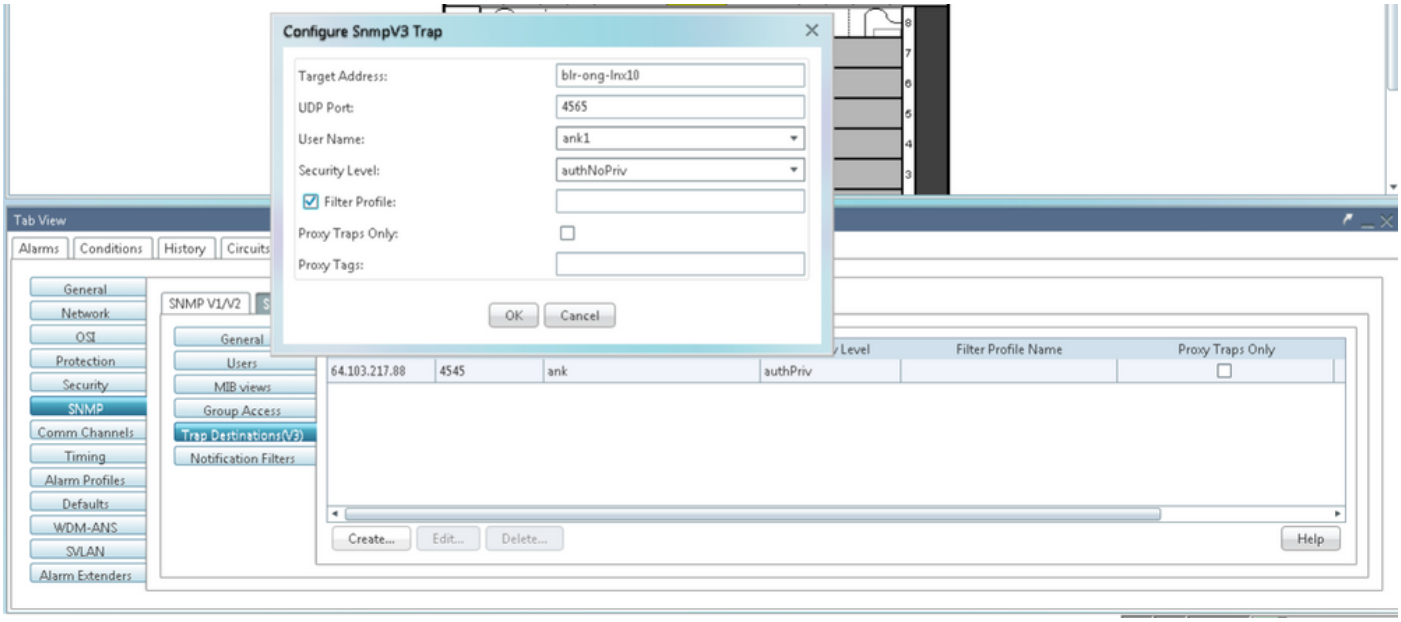

Schritt 3: Stellen Sie sicher, dass die MIB-Ansichten wie im Bild gezeigt konfiguriert sind.




Schritt 4: Konfigurieren Sie den Gruppenzugriff, wie im Bild für den Authentifizierungsmodus dargestellt.




Schritt 5: Navigieren Sie zu **Knotenansicht > Provisioning > SNMP > SNMP V3 > Trap Destination (V3)**. Klicken Sie auf **Erstellen** und **Konfigurieren**, wie im Bild gezeigt.




## Überprüfen des Authentifizierungsmodus "NoPriv"

Schritt 1: Navigieren Sie zum NMS-Server, und führen Sie einen Snapshot aus.

Syntax:

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

Beispiel:

```
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
```

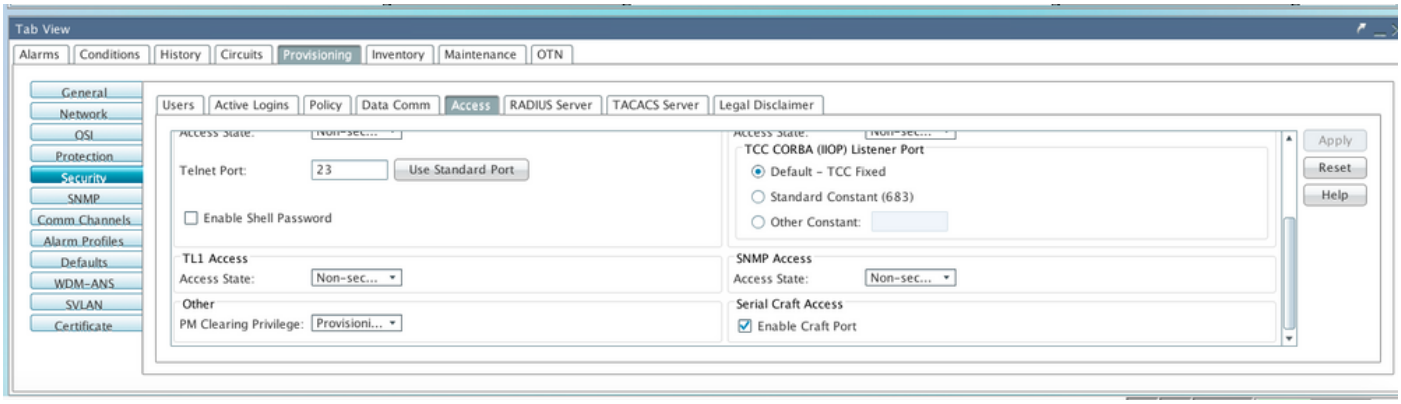
SNMP-Trap:

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

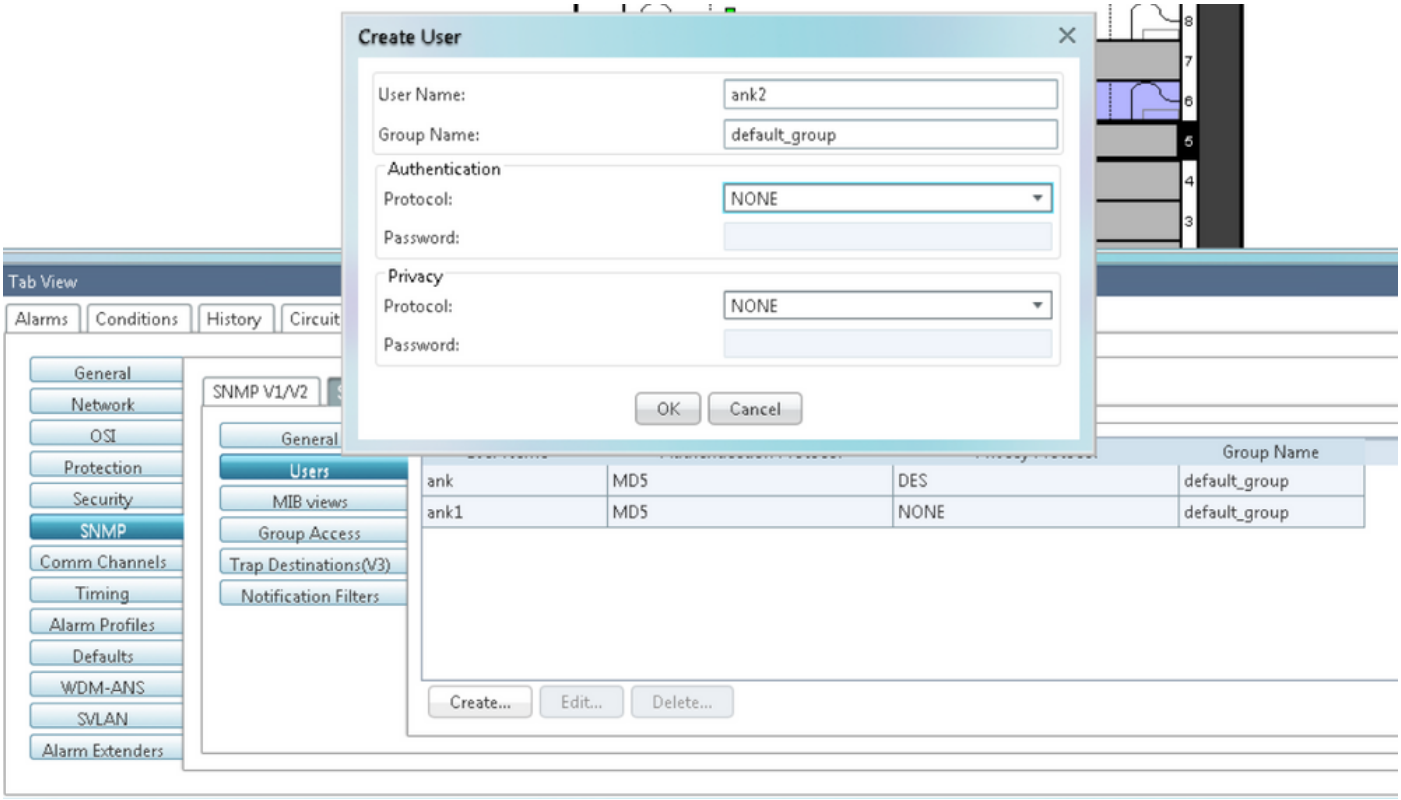
Trap cmd ist für alle Versionen identisch.

## Konfigurieren des AutoNoPriv-Modus auf ONS15454/NCS2000-Geräten

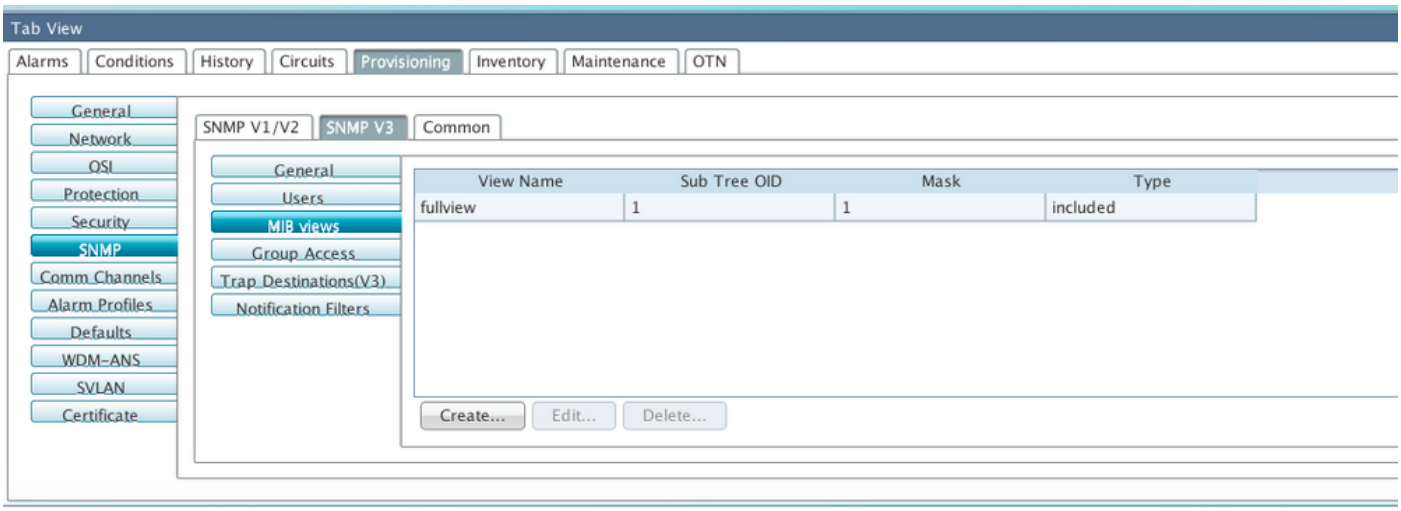
Schritt 1: Navigieren Sie im CTC zu **Node View > Provisioning > Security > Access > Change snmp access state to Non secure mode** as in the image.



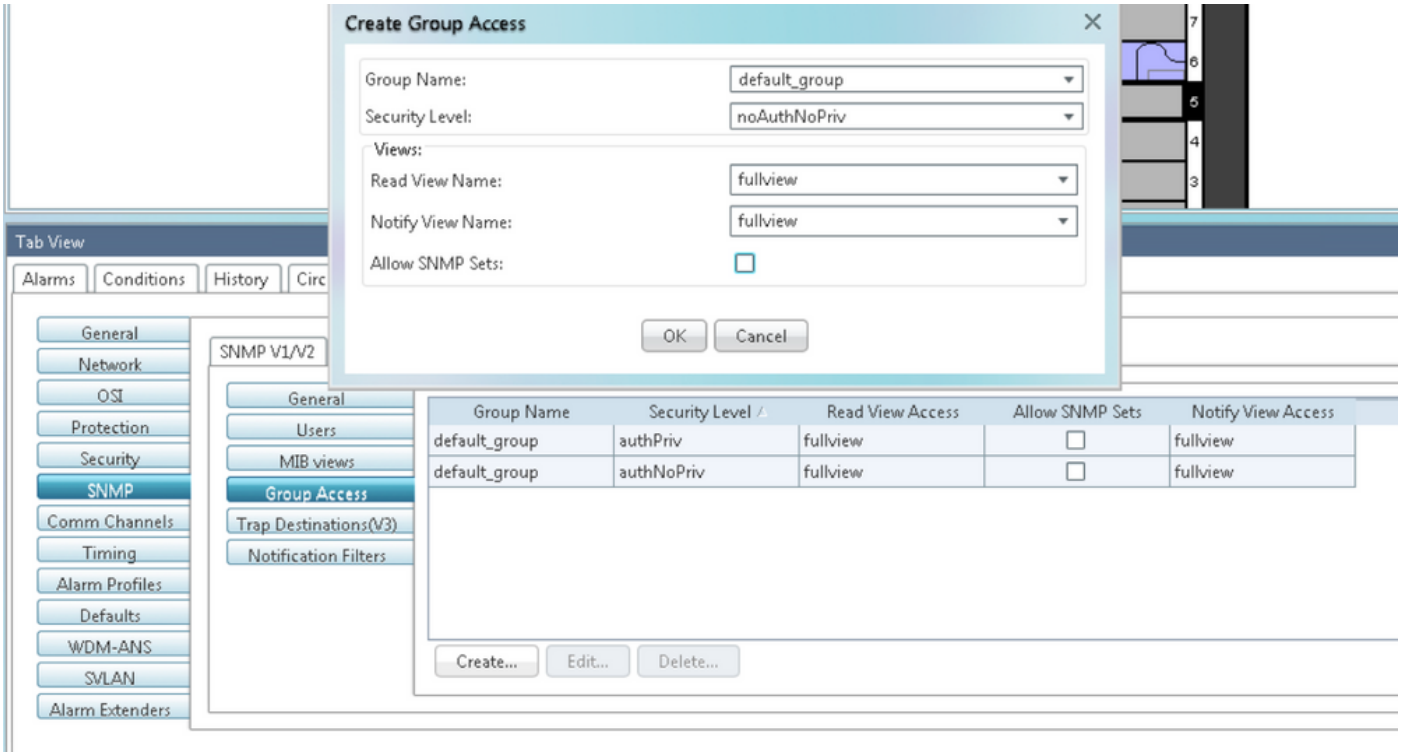

Schritt 2: Navigieren Sie zu **Node View > Provisioning > SNMP > SNMP V3 > Users > Create User and Configure (Knotenansicht > Bereitstellung > SNMP > SNMP V3 > Benutzer > Benutzer erstellen und Konfigurieren**, wie im Bild gezeigt.



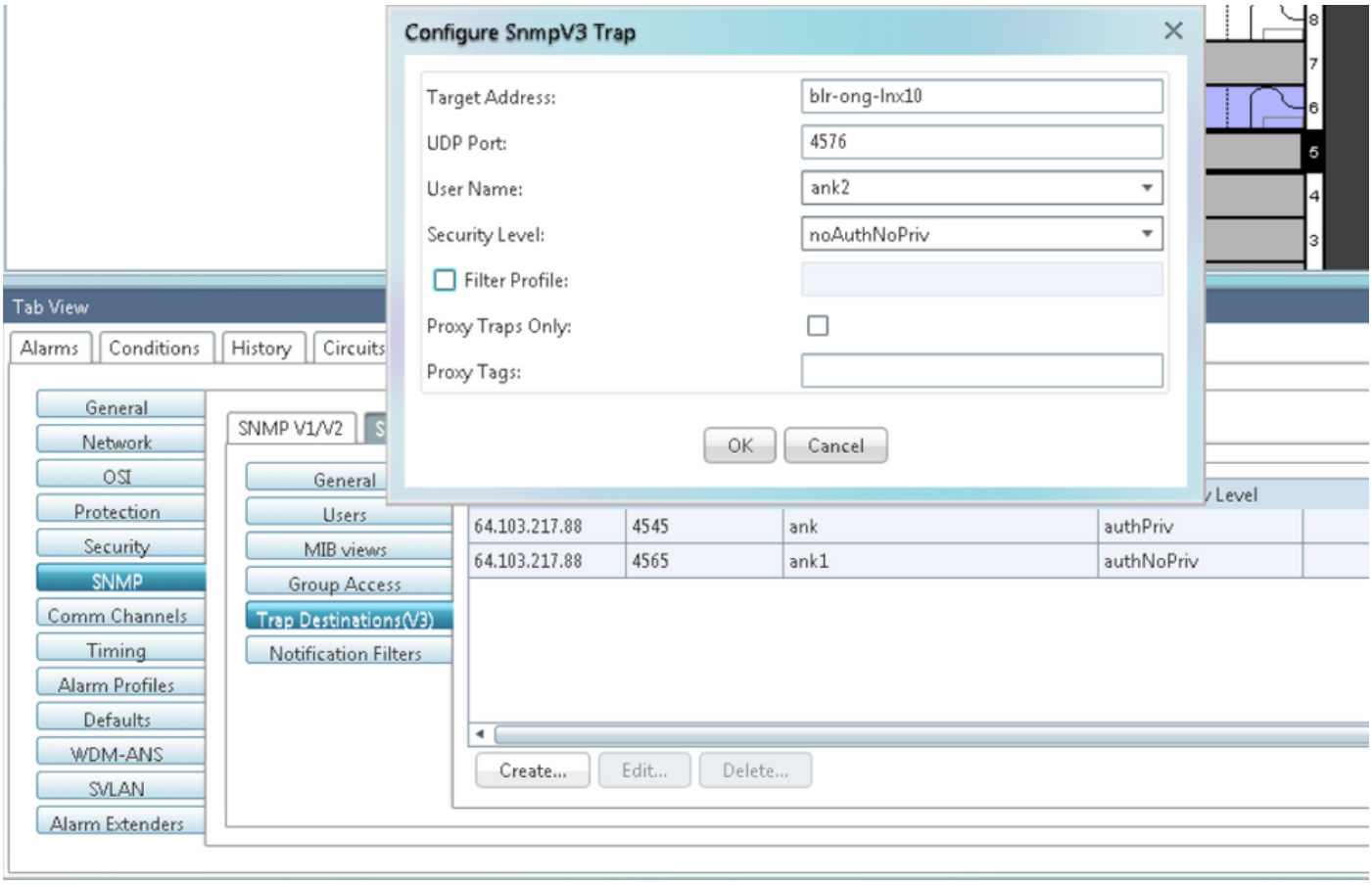

Schritt 3: Stellen Sie sicher, dass **MIB-Ansichten** wie im Bild gezeigt konfiguriert sind.




Schritt 4: Konfigurieren Sie den Gruppenzugriff, wie im Bild für den noauthnopriv-Modus gezeigt.




Schritt 5: Navigieren Sie zu **Knotenansicht > Provisioning > SNMP > SNMP V3 > Trap Destination (V3)**. Klicken Sie auf **Erstellen** und **Konfigurieren**, wie im Bild gezeigt.




## Überprüfen des AutoNoPriv-Modus

Schritt 1: Navigieren Sie zum NMS-Server, und führen Sie einen Snapshot aus.

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

Beispiel:

```
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:

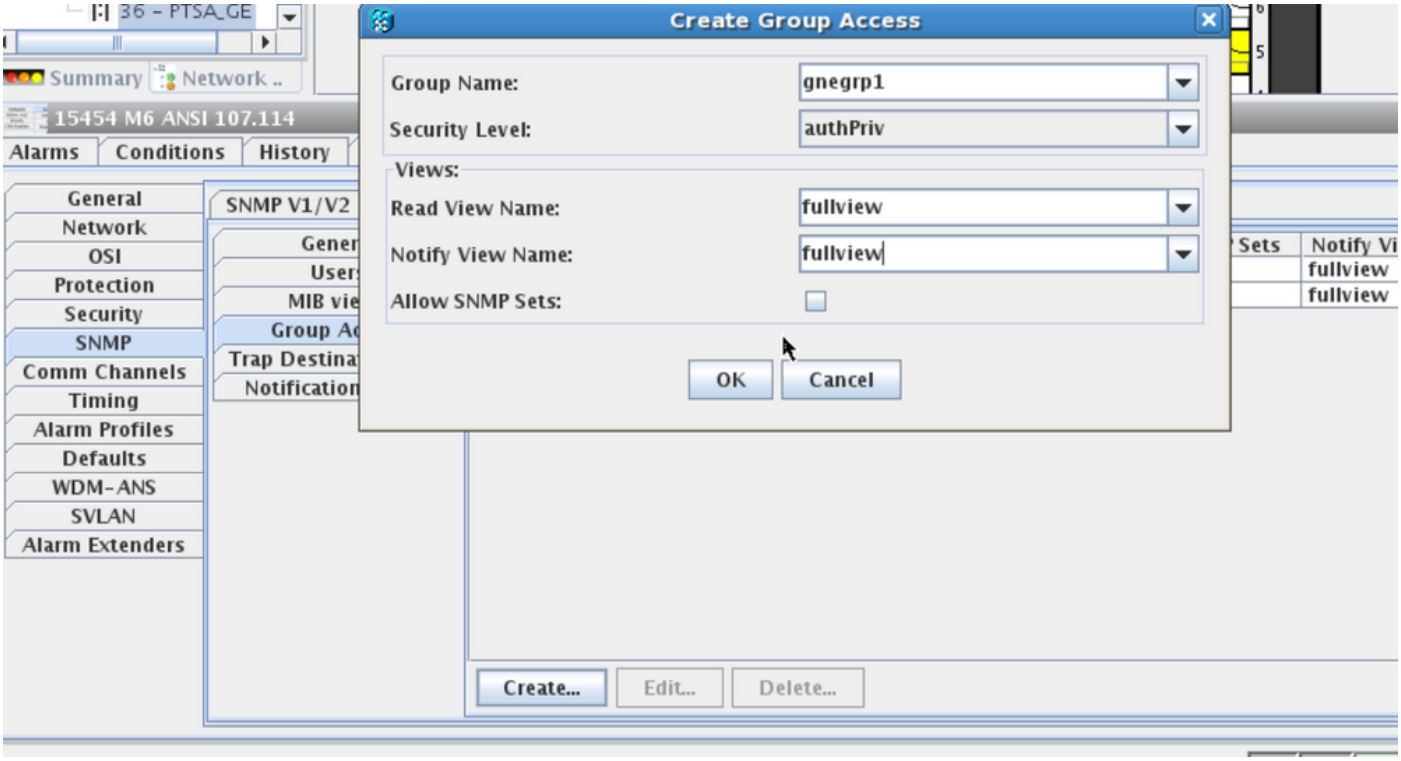
```
snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n" <port number>
```

Trap cmd ist für alle Versionen identisch.

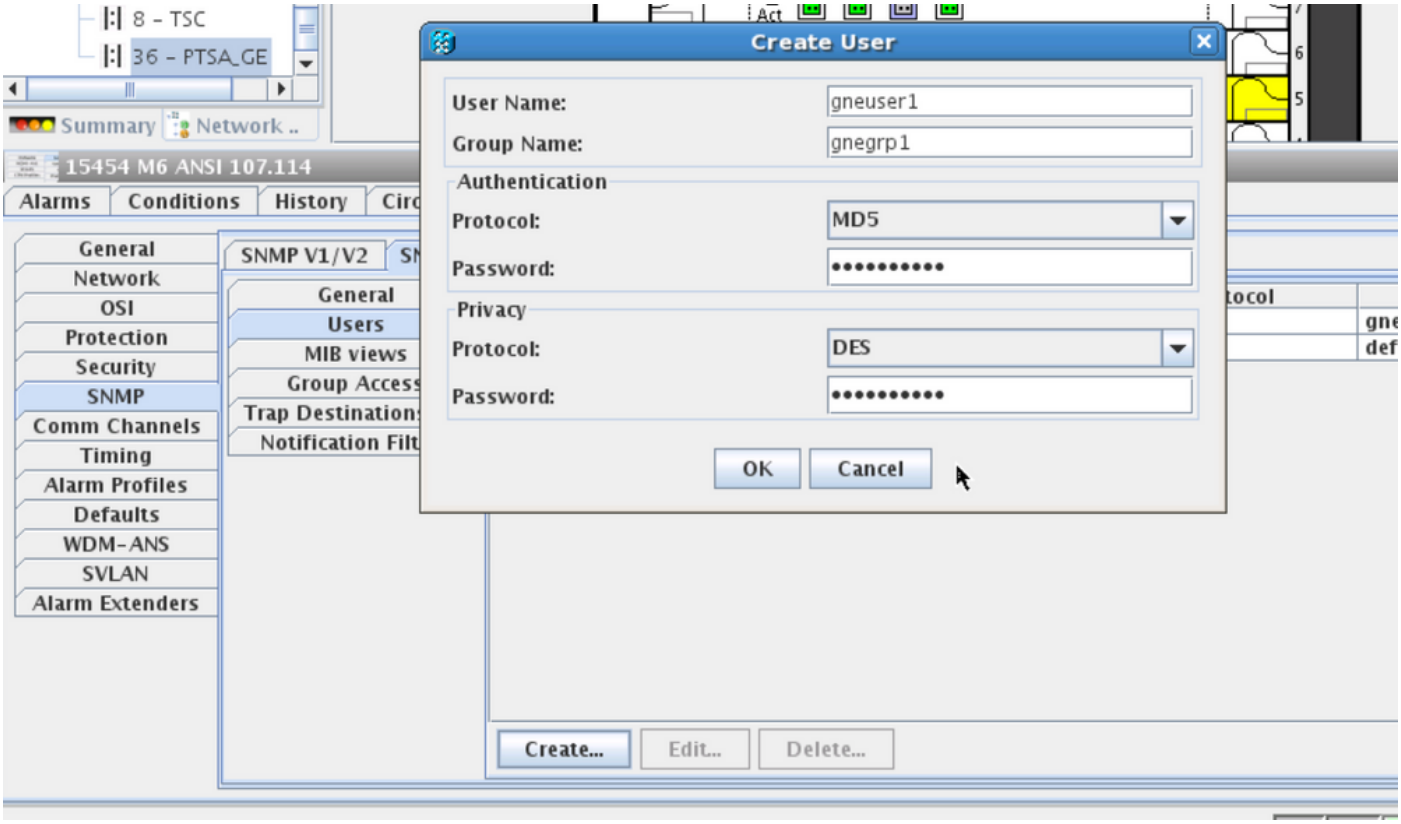
## SNMP V3-Trap für GNE/ENE-Einrichtung

### Auf GNE-Knoten

Schritt 1: Navigieren zu **Bereitstellung > SNMP > SNMP V3 und CGruppenzugriff erstellen (Registerkarte "Gruppenzugriff"): Geben Sie einen Gruppennamen mit Sicherheitsstufe (noAuthnoPriv|AuthnoPriv|authPriv) und eine vollständige Ansicht mit Lesen und Benachrichtigen an, wie im Bild gezeigt.**




Schritt 2: Benutzerzugriff erstellen (Registerkarte "Benutzer"): Erstellen Sie einen Benutzer mit dem Gruppennamen, der mit dem zuvor in der Registerkarte Gruppenzugriff erstellten Namen identisch ist. Stellen Sie außerdem die Authentifizierung basierend auf der Zugriffsebene bereit, wie im Bild gezeigt.




Schritt 3: Registerkarte Trap Destination (V3):

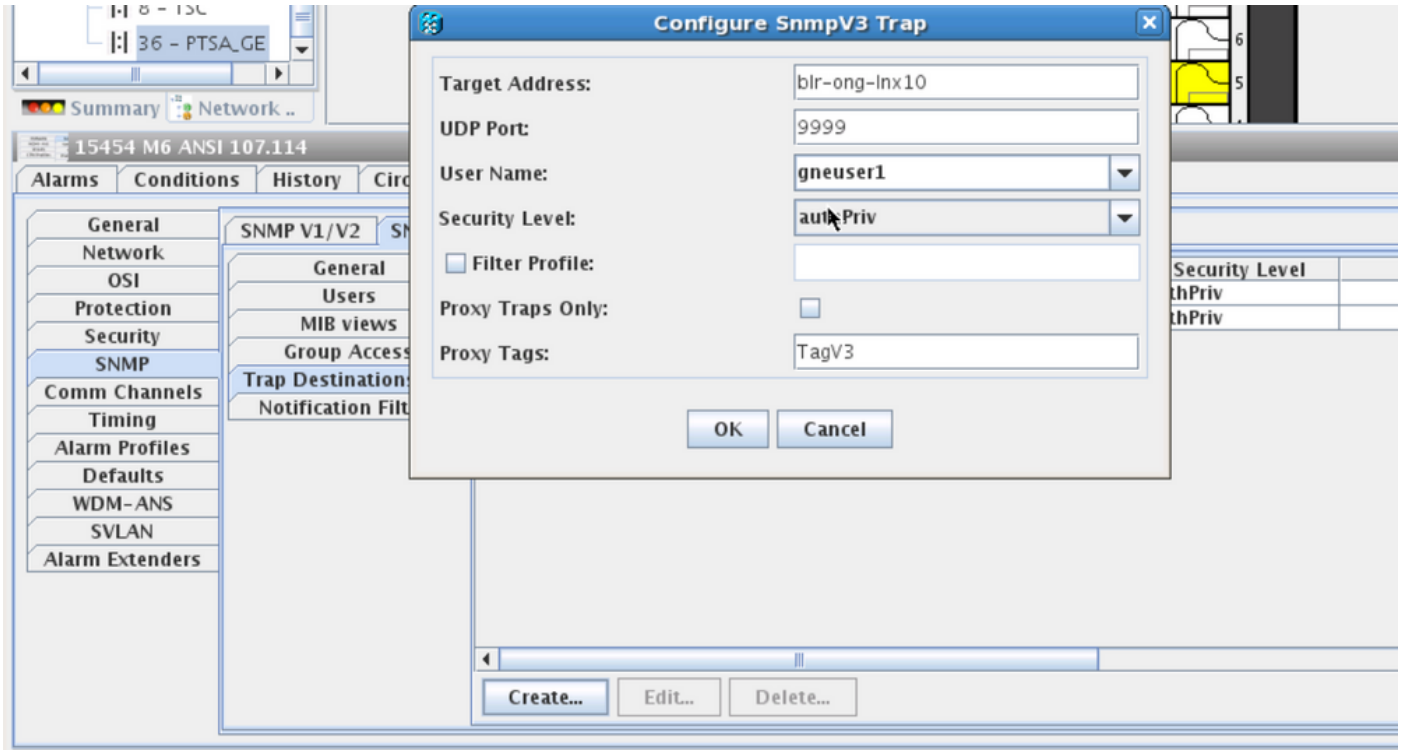
Zieladresse: Adresse des NMS-Servers, von dem aus das Trap ausgeführt wird (z. B. Blr-ong-lnx10).

UDP-Port: Alle Portnummern, unter denen das Trap überwacht wird (z. B. 9977).

Benutzername: Name des Benutzers auf der Registerkarte Benutzer.

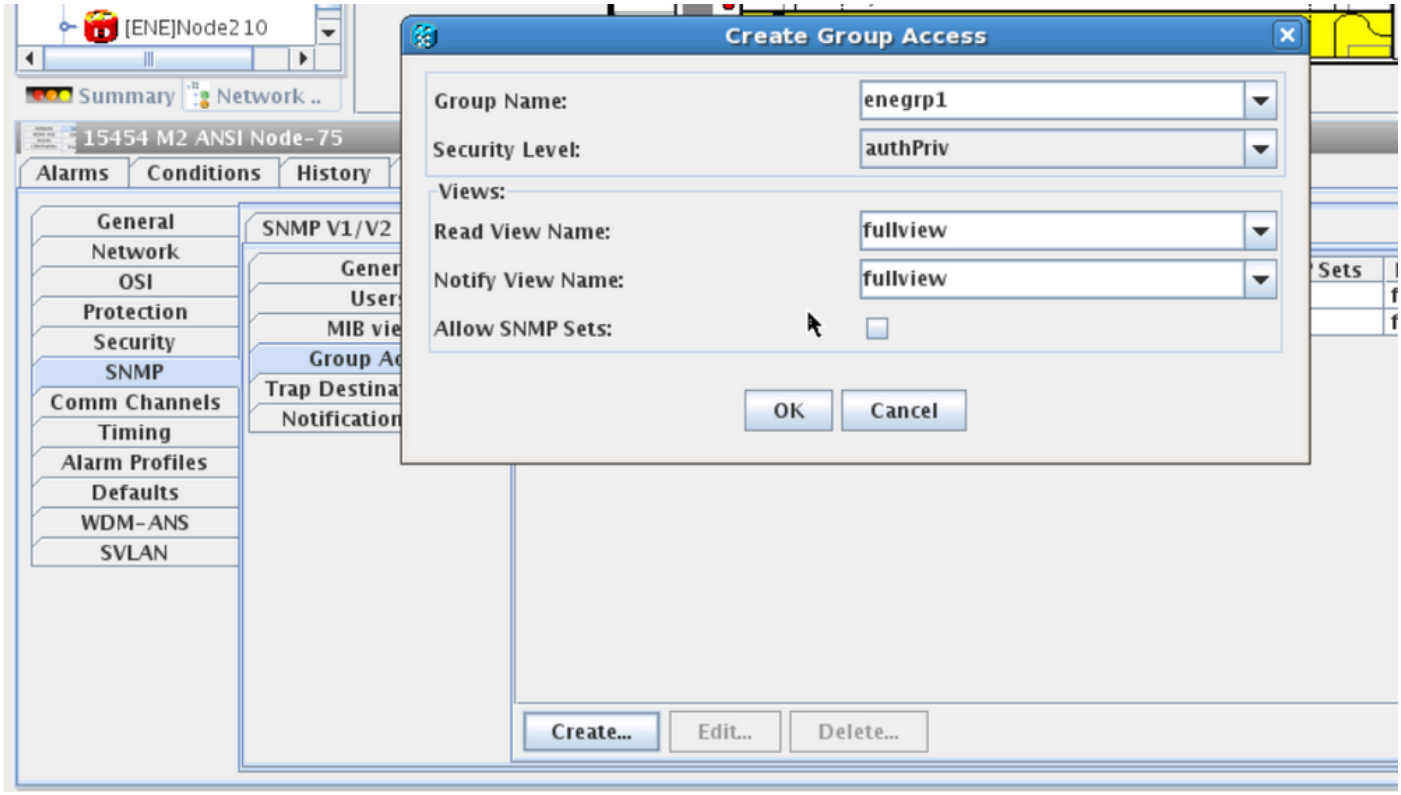
Sicherheitsstufe: Wie zuvor auf der Registerkarte "Benutzer" konfiguriert.

Proxy-Tags: Geben Sie ein Proxy-Tag (z. B. Tag75).

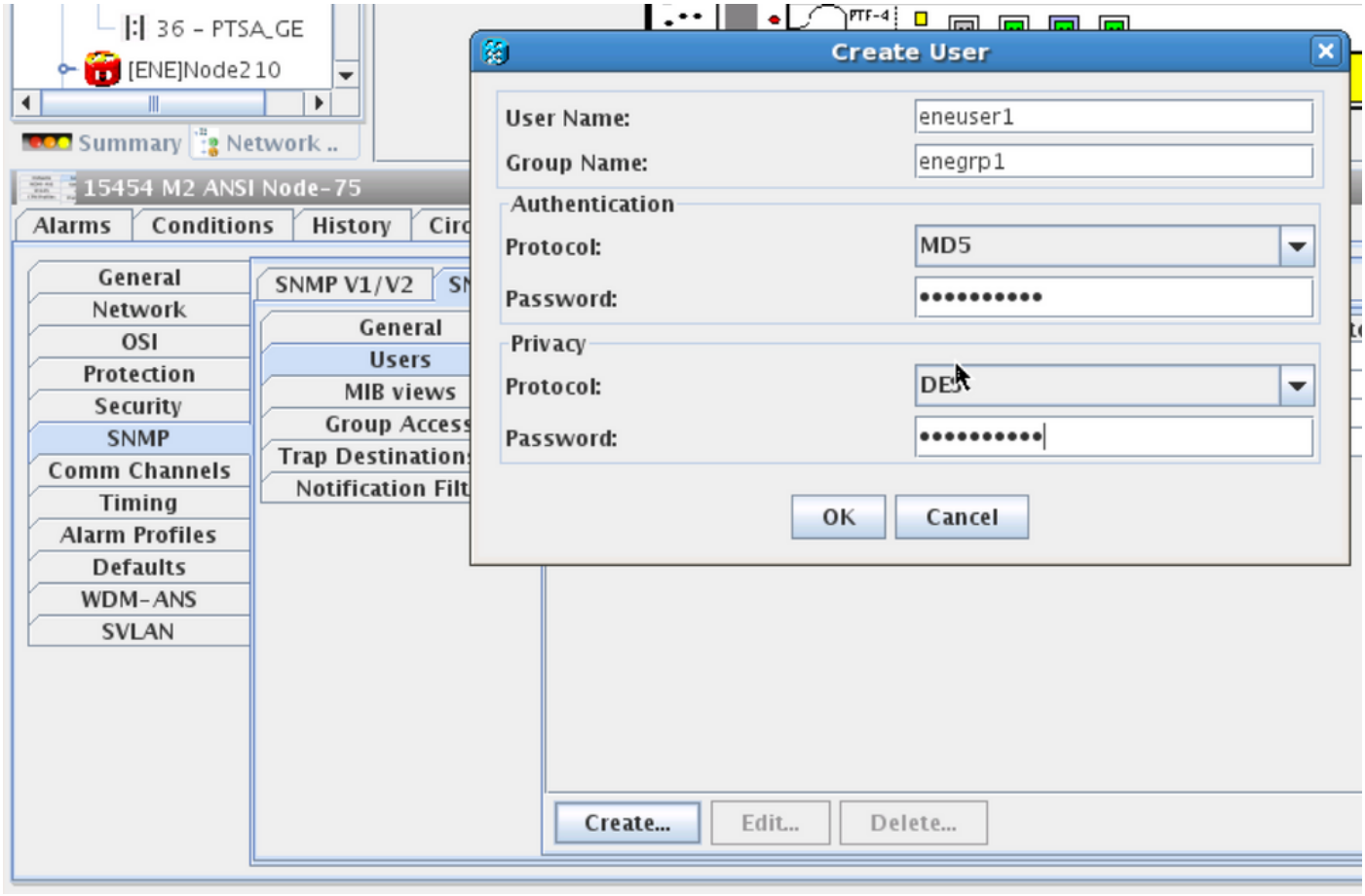



## Auf ENE-Knoten

Schritt 1: Navigieren Sie zu **Provisioning > SNMP > SNMP V3 und Create Group Access (Gruppenzugriff erstellen):** Geben Sie einen Gruppennamen mit Zugriffsebene (noAuthnoPriv|AuthnoPriv|authPriv) und eine vollständige Ansicht mit Lesen und Benachrichtigen an, wie im Bild gezeigt.




Schritt 2: Benutzerzugriff erstellen (Registerkarte "Benutzer"): Erstellen Sie einen Benutzer mit dem Gruppennamen, der mit dem zuvor in der Registerkarte Gruppenzugriff erstellten Namen identisch ist. Stellen Sie darüber hinaus die Authentifizierung basierend auf der Zugriffsebene bereit.




Stellen Sie sicher, dass auf der Registerkarte "Gruppenzugriff" eine default_group erstellt wird, falls diese in der Registerkarte "Gruppenzugriff" fehlt.

Schritt 3: Registerkarte Trap Destination (V3):

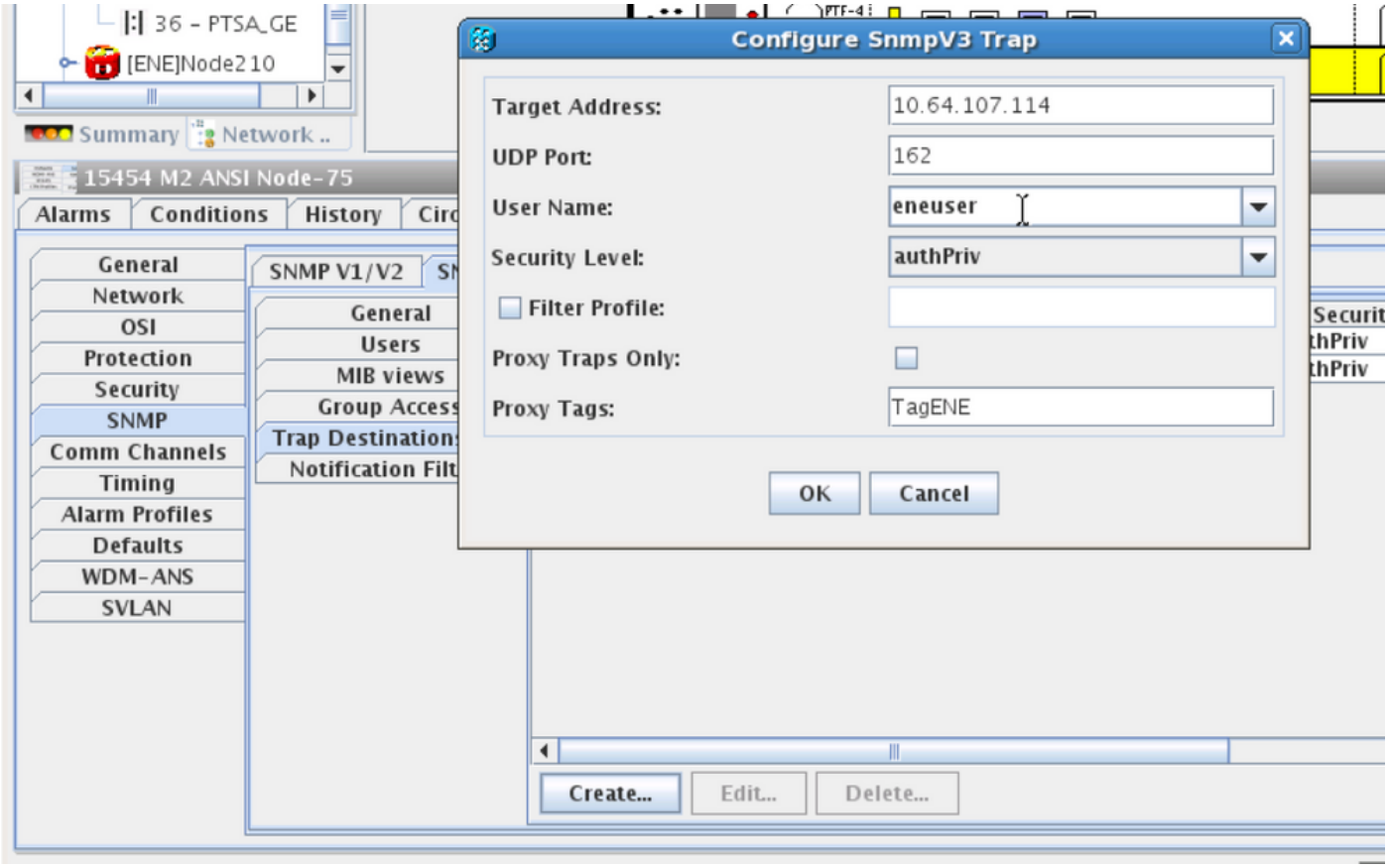
Zieladresse: GNE-Knoten-IP.

UDP-Port: 162.

Benutzername: Name des Benutzers auf der Registerkarte Benutzer.

Sicherheitsstufe: Wie zuvor auf der Registerkarte "Benutzer" konfiguriert.

Proxy-Tags: Geben Sie ein beliebiges Proxy-Tag wie GNE (z. B. Tag75).



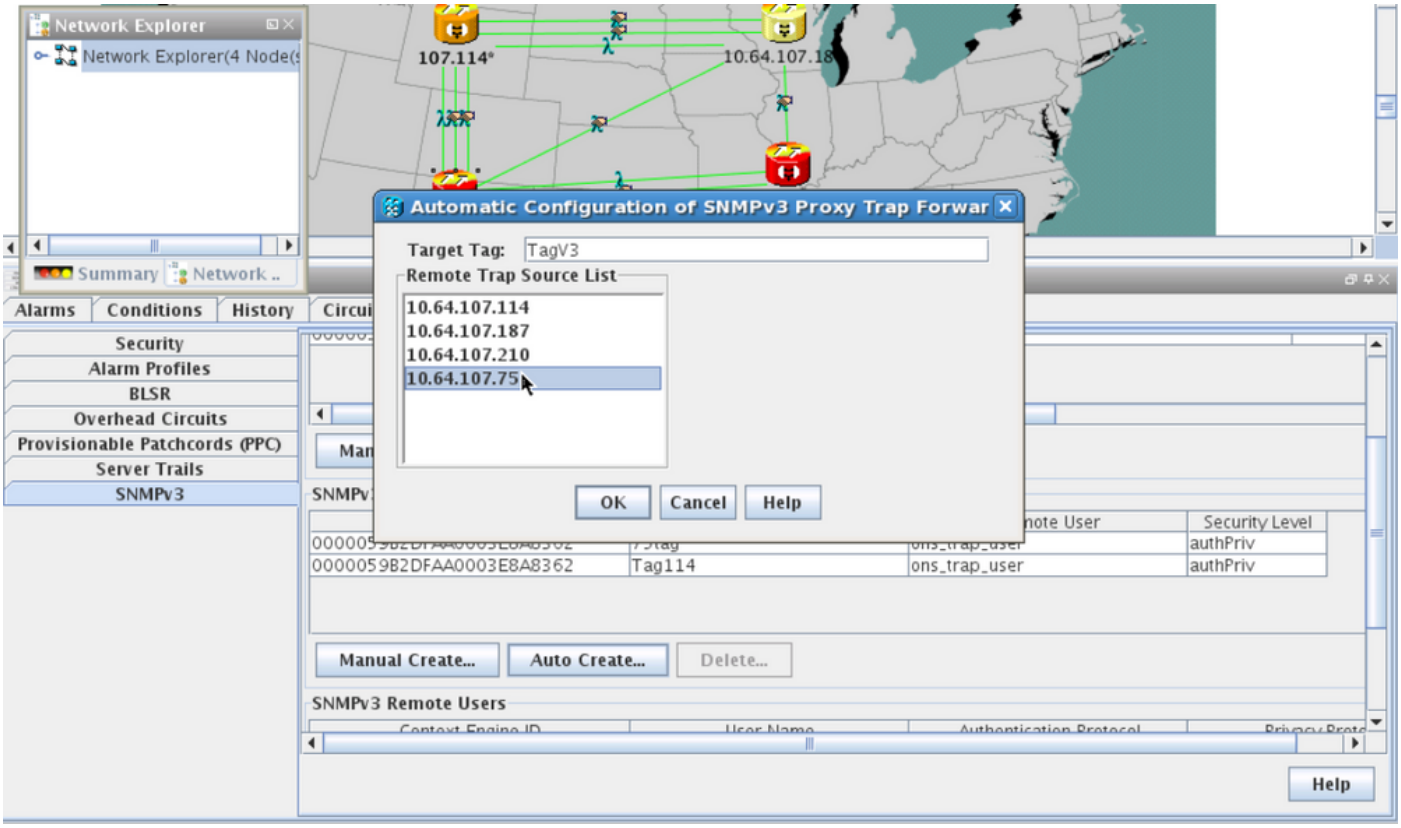

Navigieren Sie im CTC zur Netzwerkansicht:

Schritt 1: Navigieren Sie zur Registerkarte **SNMPv3**.

Schritt 2: SNMPv3-Proxy-Trap-Weiterleitungstabelle: Sie können entweder **manuell** oder **automatisch erstellen**.

Wählen Sie **Auto Create (Automatisch erstellen)**. Im Rahmen dieser Verordnung

- Ziel-Tag: Proxy-Tag in GNE festgelegt.
- Remote-Trap-Quellliste: Wählen Sie die ENE-Knoten-IP aus, wie im Bild gezeigt.




## GNE/ENE-Einrichtung überprüfen

NMS-Server konfigurieren (blr-ong-lnx10):

Schritt 1: Erstellen Sie im Stammverzeichnis des Servers ein Verzeichnis, und nennen Sie es **snmp**.

Schritt 2: Erstellen Sie unter diesem Verzeichnis eine Datei **snmptrapd.conf**.

Schritt 3: Erstellen Sie in **snmptrapd.conf** die folgende Konfiguration:

```
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"
```

snmpwalk auf ENE:

Für den Authentifizierungs-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>
```

Für den Authentifizierungsmodus:

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

```
<gne_ip_address> <OID>
```

Für den noauthnopriv-Modus:

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

# Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.