Configurazione di SNMPv3 sui dispositivi Cisco ONS15454/NCS2000

Sommario

Introduzione

Questo documento descrive le istruzioni dettagliate su come configurare il protocollo SNMPv3 (Simple Network Management Protocol versione 3) sui dispositivi ONS15454/NCS2000. Tutti gli argomenti includono esempi.

> **Nota:** L'elenco degli attributi fornito in questo documento non è esaustivo né autorevole e può essere modificato in qualsiasi momento senza un aggiornamento del documento.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- GUI Cisco Transport Controller (CTC)
- Conoscenze base dei server
- Comandi Linux/Unix di base

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Su un nodo autonomo/multipiattaforma

Configurazione della modalità authPriv sul dispositivo ONS15454/NCS2000

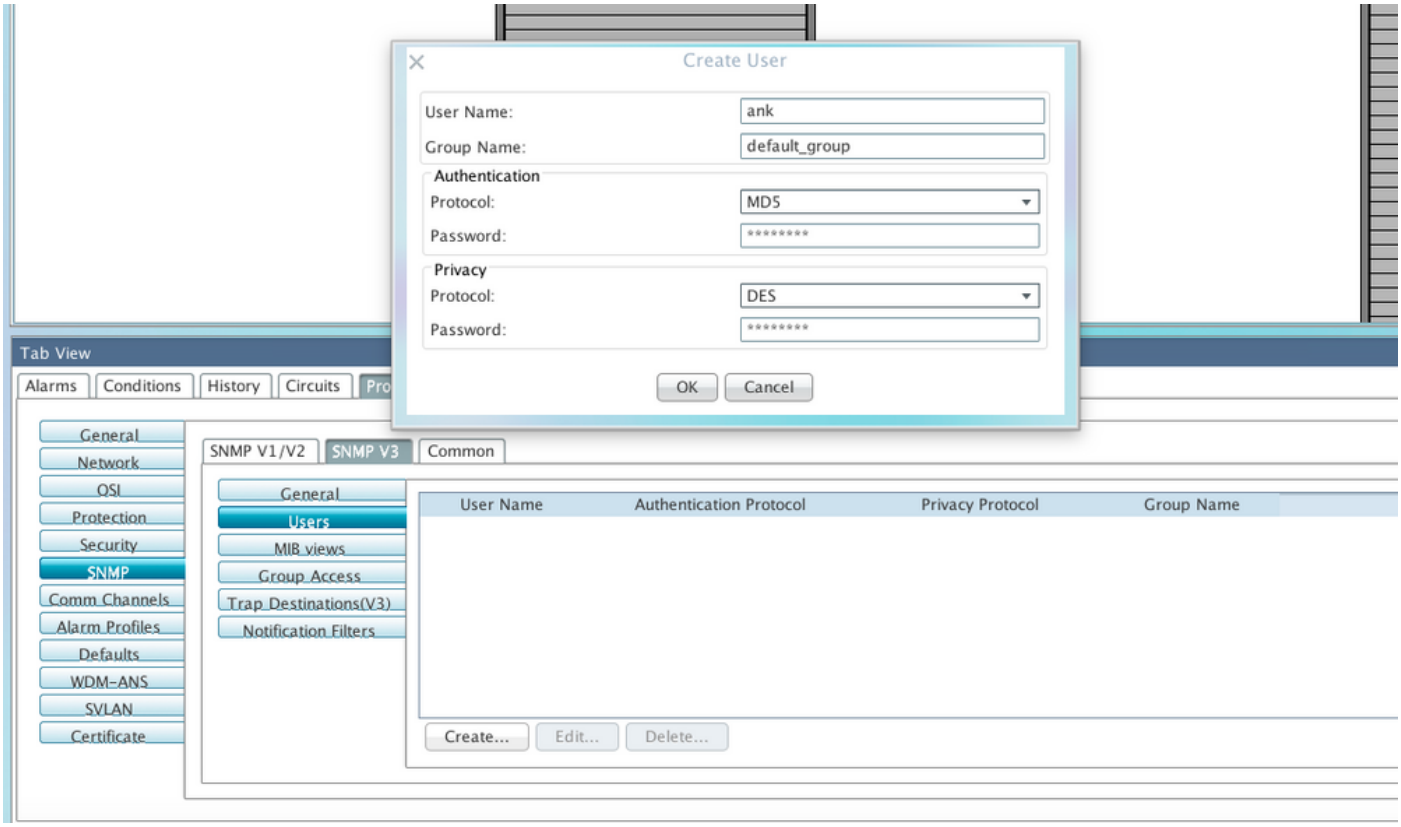
Passaggio 1. Accedere al nodo tramite CTC con le credenziali di Utente avanzato.

Passaggio 2. Passare a **Vista nodo > Provisioning > SNMP > SNMP V3**.

Passaggio 3. Passare alla scheda **Utenti**. Creare utenti.

```
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>
```

Passaggio 4. Fare clic su **OK** come mostrato nell'immagine.



Specifiche:

Nome utente: specificare il nome dell'utente sull'host che si connette all'agente. Il nome utente deve contenere da un minimo di 6 a un massimo di 40 caratteri (fino a un massimo di 39 caratteri per l'autenticazione TACACS e RADIUS). Include caratteri alfanumerici (a-z, A-Z, 0-9) e i caratteri speciali consentiti sono @, "-" (trattino) e "." (punto). Per la compatibilità con TL1, il nome utente deve contenere da 6 a 10 caratteri.

Nome gruppo: specificare il gruppo a cui appartiene l'utente.

Autenticazione:

Protocollo: selezionare l'algoritmo di autenticazione che si desidera utilizzare. Le opzioni sono NONE, MD5 e SHA.

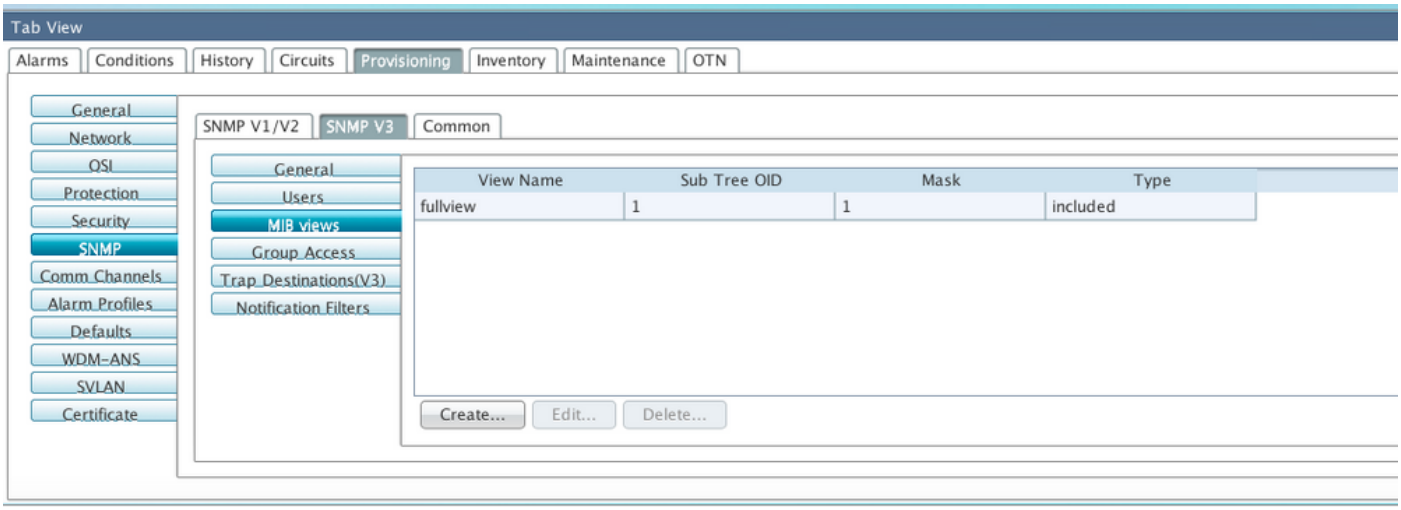
Password: immettere una password se si seleziona MD5 o SHA. Per impostazione predefinita, la lunghezza della password è impostata su un minimo di otto caratteri.

Privacy - Avvia una sessione di impostazione del livello di autenticazione della privacy che consente all'host di crittografare il contenuto del messaggio inviato all'agente.

Protocollo: selezionare l'algoritmo di autenticazione della privacy. Le opzioni disponibili sono None, DES e AES-256-CFB.

Password: immettere una password se si seleziona un protocollo diverso da Nessuno.

Passaggio 5. Verificare che le visualizzazioni MIB siano configurate in base a questa immagine.



Specifiche:

Nome: nome della vista.

OID sottoalbero (Subtree OID) - Sottoalbero MIB che, se combinato con la maschera, definisce la famiglia di sottoalberi.

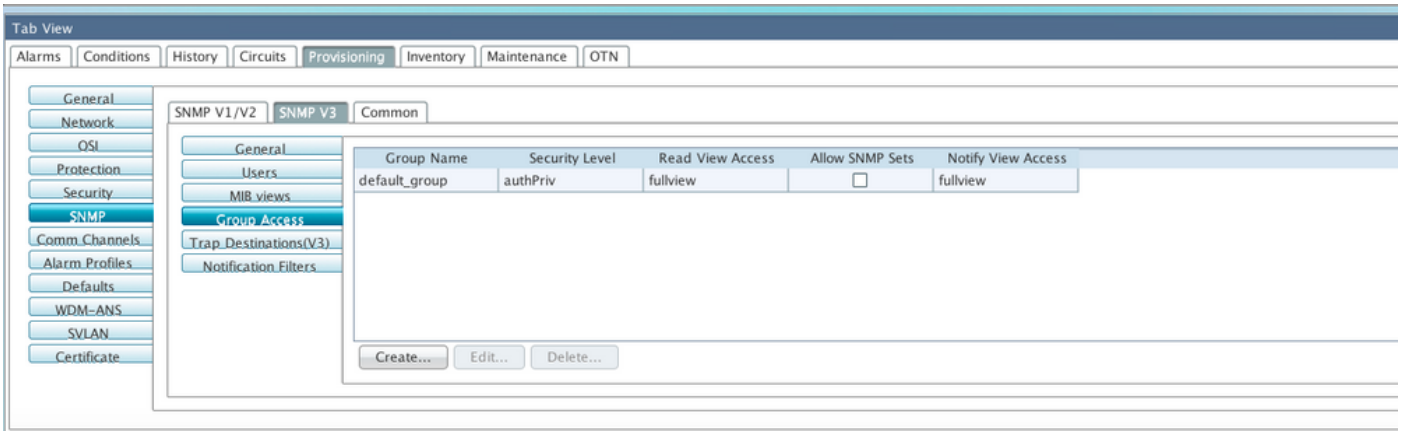
Maschera di bit - Famiglia di sottoalberi di visualizzazione. Ogni bit nella maschera di bit corrisponde a un identificatore secondario dell'OID della sottostruttura.

Tipo (Type) - Consente di selezionare il tipo di vista. Le opzioni sono Incluso ed Escluso.

Il tipo definisce se la famiglia di sottostrutture definite dalla combinazione di OID sottostruttura e Maschera di bit vengono incluse o escluse dal filtro di notifica.

Passaggio 6. Configurare l'accesso al gruppo come mostrato nell'immagine. Per impostazione predefinita, il nome del gruppo sarà default_group e il livello di protezione authPriv.

Nota: Il nome del gruppo deve essere uguale a quello utilizzato quando si crea l'utente nel passaggio 3.



Specifiche:

Nome gruppo: il nome del gruppo SNMP o della raccolta di utenti che condividono un criterio di accesso comune.

Livello di protezione: il livello di protezione per il quale vengono definiti i parametri di accesso.

Selezionare una delle seguenti opzioni:

noAuthNoPriv - Utilizza un nome utente corrispondente per l'autenticazione.

AuthNoPriv: fornisce l'autenticazione basata sugli algoritmi HMAC-MD5 o HMAC-SHA.

AuthPriv: fornisce l'autenticazione basata sugli algoritmi HMAC-MD5 o HMAC-SHA. Crittografia DES a 56 bit basata sullo standard CBC-DES (DES-56), oltre all'autenticazione.

Se si seleziona authNoPriv o authPriv per un gruppo, l'utente corrispondente deve essere configurato con un protocollo di autenticazione e una password, con protocollo di privacy e password o entrambi.

Visualizzazioni

Read View Name: nome della visualizzazione di lettura per il gruppo.

Notifica nome vista - Notifica il nome della vista per il gruppo.

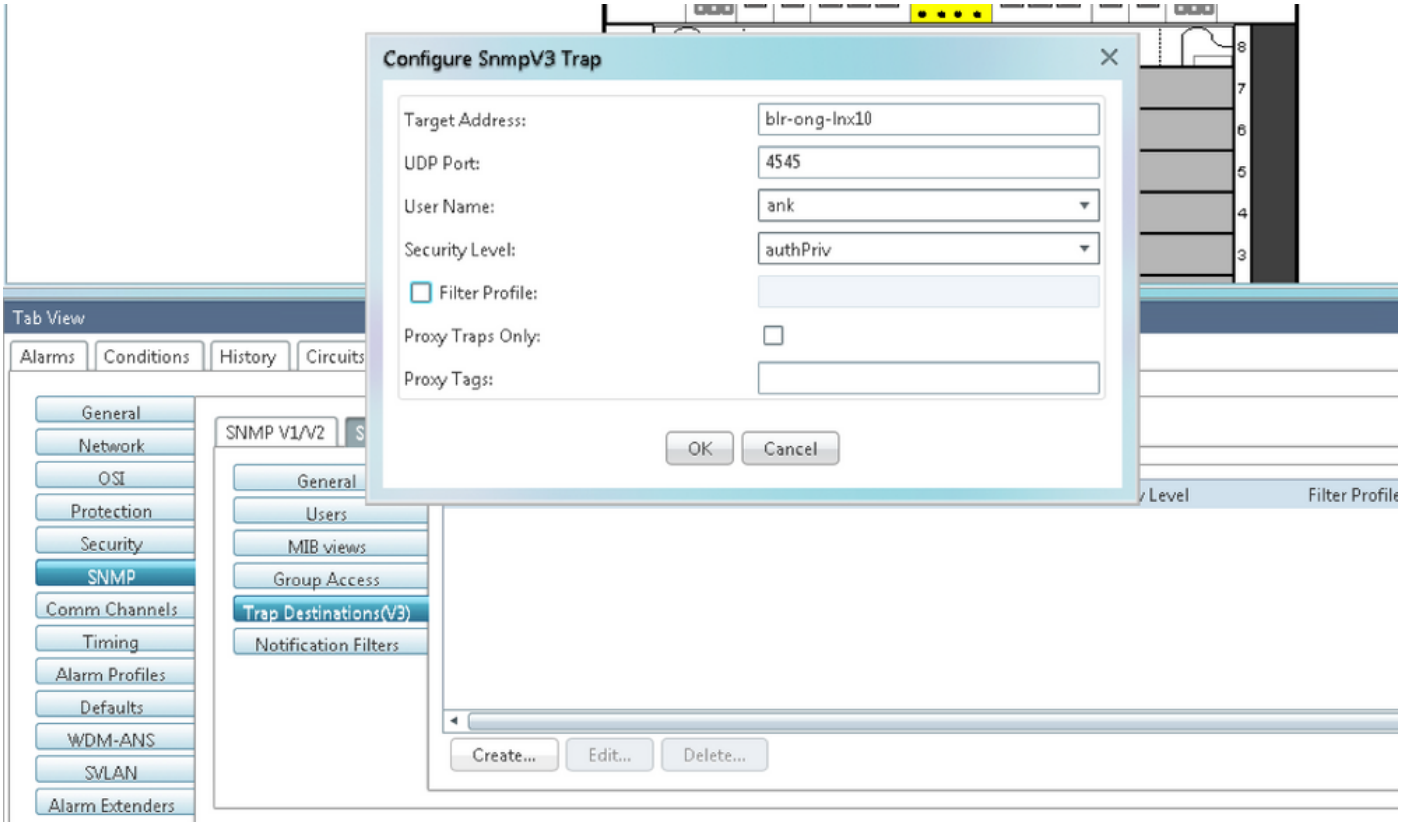
Consenti set SNMP: selezionare questa casella di controllo se si desidera che l'agente SNMP accetti le richieste SET SNMP. Se questa casella di controllo non è selezionata, le richieste SET vengono rifiutate.

Nota: L'accesso alle richieste SET SNMP è implementato per un numero limitato di oggetti.

Passaggio 7. Passare a **Vista nodo > Provisioning > SNMP > SNMP V3 > Destinazione trap (V3)**. Fare clic su **Create** and **Configure** (Crea e configura).

```
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
```

Passaggio 8. Fare clic su **OK** come mostrato nell'immagine.



Nota: blr-ong-lnx10 è il server NMS.

Specifiche:

Target Address: destinazione alla quale devono essere inviate le trap. Utilizzare un indirizzo IPv4 o IPv6.

Porta UDP: numero di porta UDP utilizzato dall'host. Il valore predefinito è 162.

Nome utente: specificare il nome dell'utente sull'host che si connette all'agente.

Livello di protezione: selezionare una delle seguenti opzioni:

noAuthNoPriv - Utilizza un nome utente corrispondente per l'autenticazione.

AuthNoPriv: fornisce l'autenticazione basata sugli algoritmi HMAC-MD5 o HMAC-SHA.

AuthPriv: fornisce l'autenticazione basata sugli algoritmi HMAC-MD5 o HMAC-SHA. Crittografia DES a 56 bit basata sullo standard CBC-DES (DES-56), oltre all'autenticazione.

Profilo filtro: selezionare questa casella di controllo e immettere il nome del profilo di filtro. I trap vengono inviati solo se si specifica un nome di profilo di filtro e si crea un filtro di notifica.

Solo trap proxy: se questa opzione è selezionata, inoltra solo le trap proxy dalla rete ENP. I trap da questo nodo non vengono inviati alla destinazione di trap identificata da questa voce.

Tag proxy: specificare un elenco di tag. L'elenco di tag è necessario su un GNE solo se l'ENE deve inviare trap alla destinazione identificata da questa voce e desidera utilizzare il GNE come proxy.

Configurazione del server NMS (blr-ong-lnx10)

Passaggio 1. Nella home directory del server, creare una directory con il nome **snmp**.

Passaggio 2. In questa directory, creare un file **snmptrapd.conf**.

Passaggio 3. Modificare il file **snmptrapd.conf** in:

```
vi snmptrapd.conf

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

Ad esempio:

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

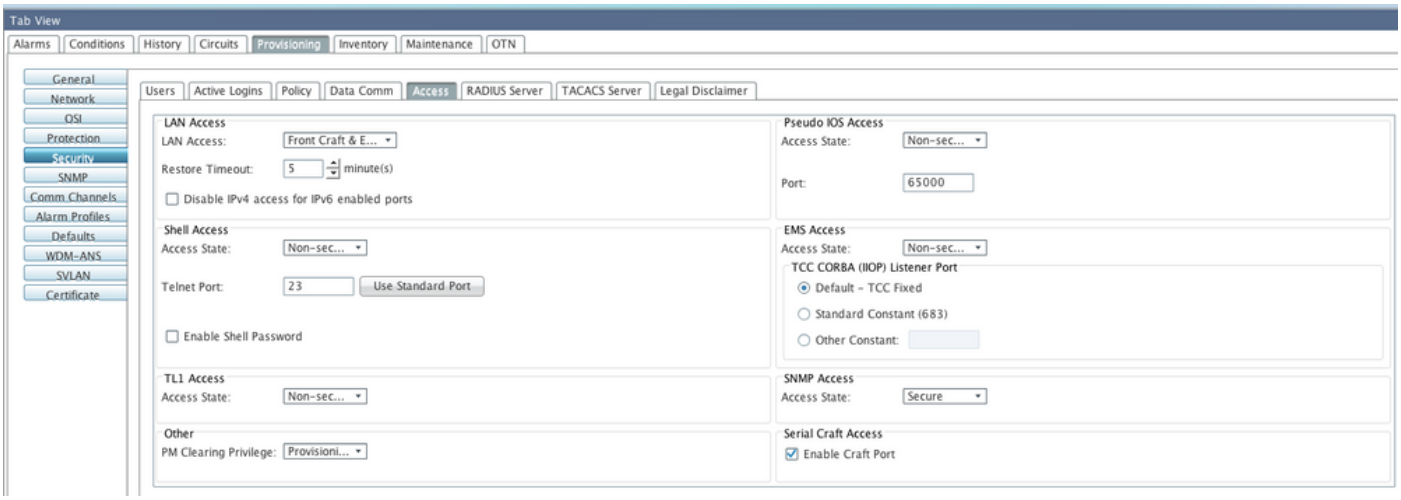
In questo esempio:

```
user_name=ank

MD5 password = cisco123

DES password  = cisco123

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

Node view > Provisioning > SNMP > SNMP V3 > General

Verifica modalità authPriv

Passaggio 1. In CTC, selezionare **Node View > Provisioning > Security > Access > change snmp access state to Secure (Vista nodi > Provisioning > Sicurezza > Accesso > cambia lo stato di accesso snmp su Secure (Protetto)), come mostrato nell'immagine.**



Passaggio 2. Passare al server NMS ed eseguire lo snmpwalk.

Sintassi:

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

Esempio:

```
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
```

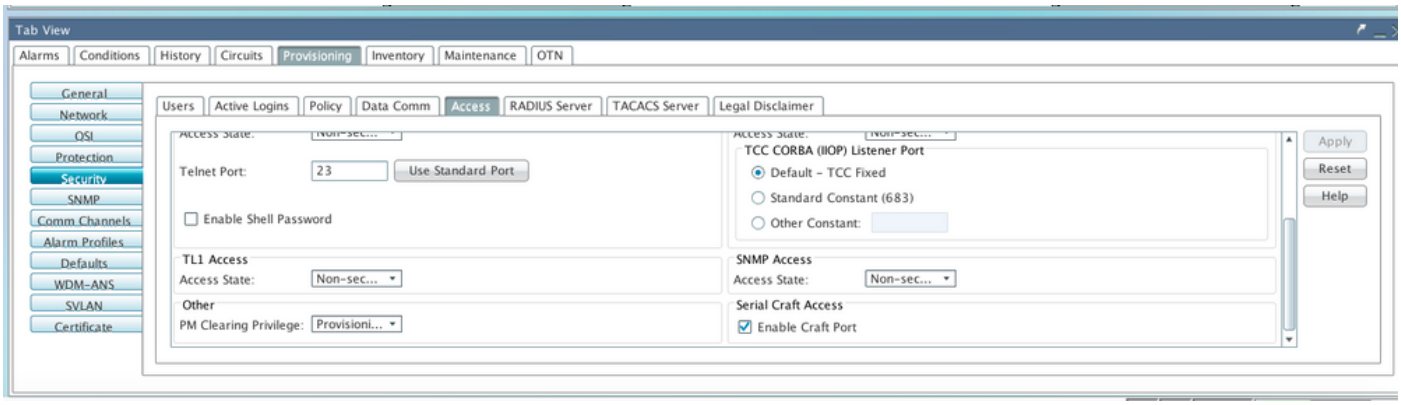
Trap SNMP:

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

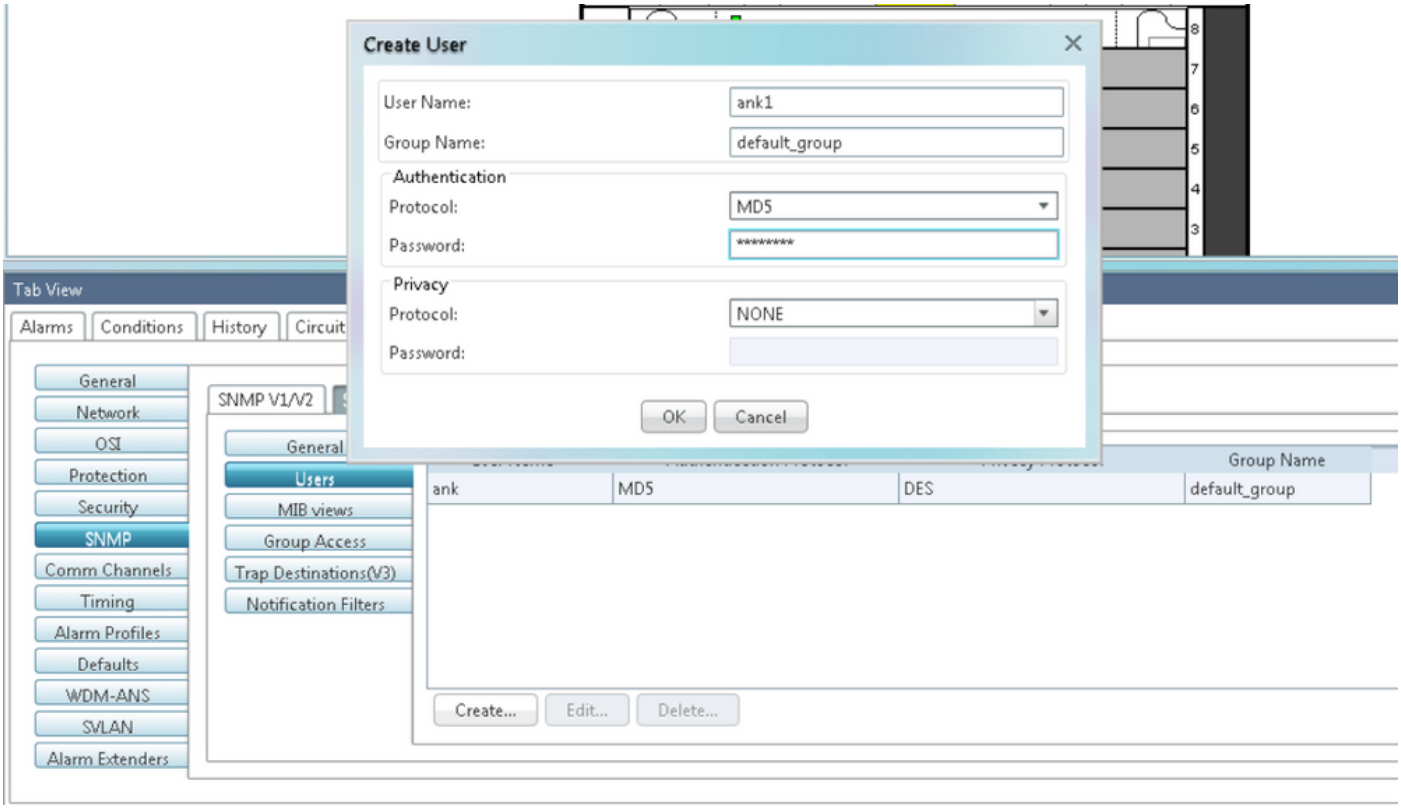
Il comando Trap è lo stesso per tutte le versioni.

Configurazione della modalità authNoPriv sul dispositivo ONS15454/NCS2000

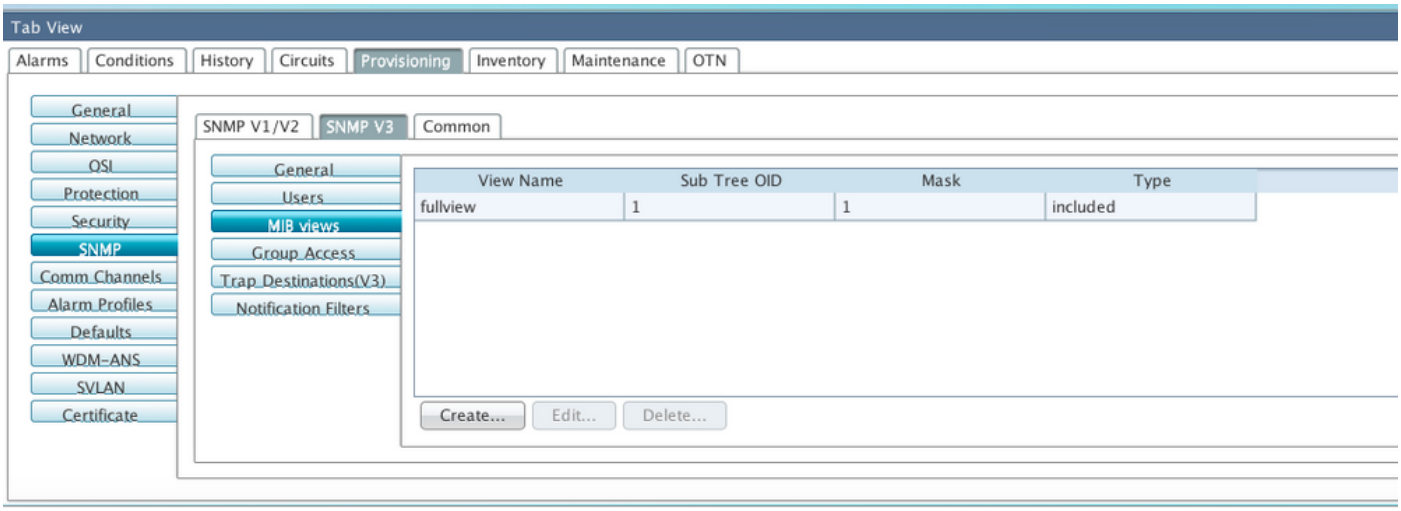
Passaggio 1. In CTC, selezionare **Node View > Provisioning > Security > Access > change snmp access state to Non-secure mode** (Visualizzazione nodo > Provisioning > Sicurezza > Accesso > Modifica stato accesso snmp in modalità non protetta), come mostrato nell'immagine.



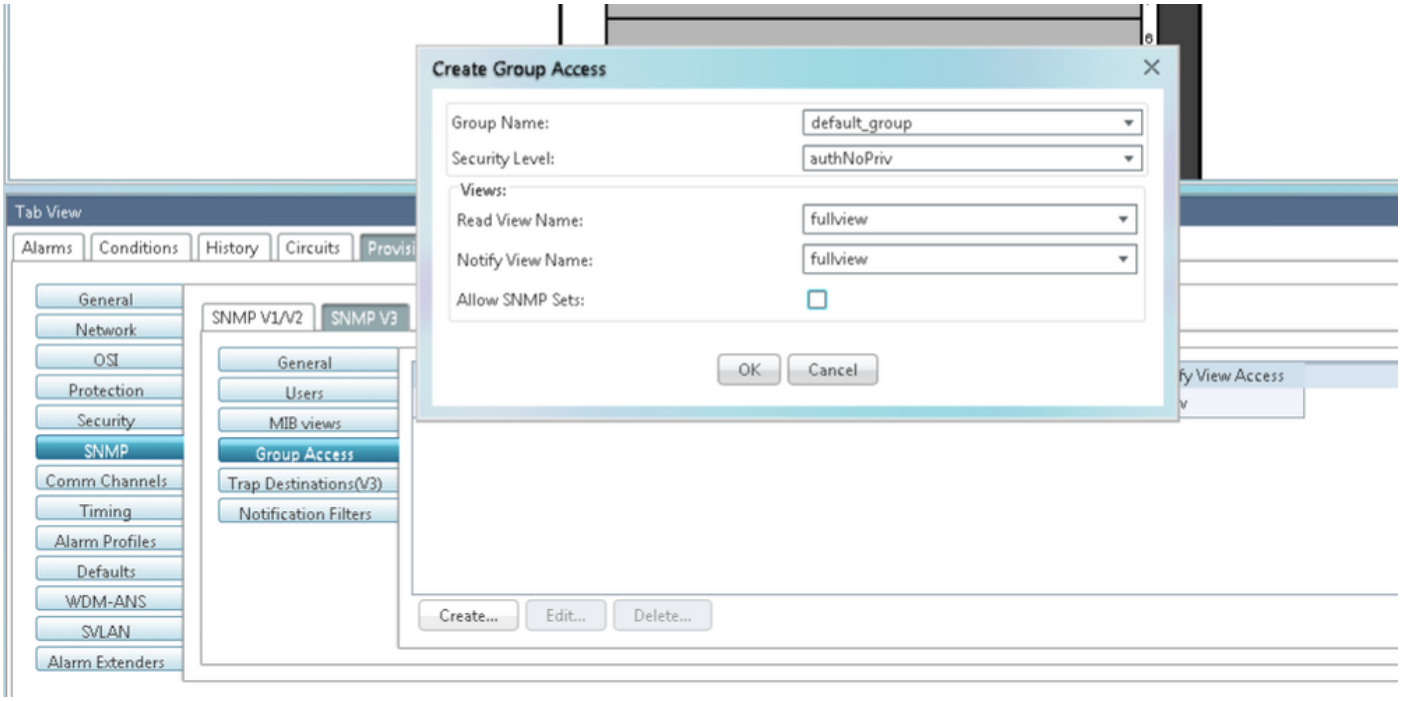
Passaggio 2. Passare a **Vista nodo > Provisioning > SNMP > SNMP V3 > Utenti > Crea utente** e configurare come mostrato nell'immagine.



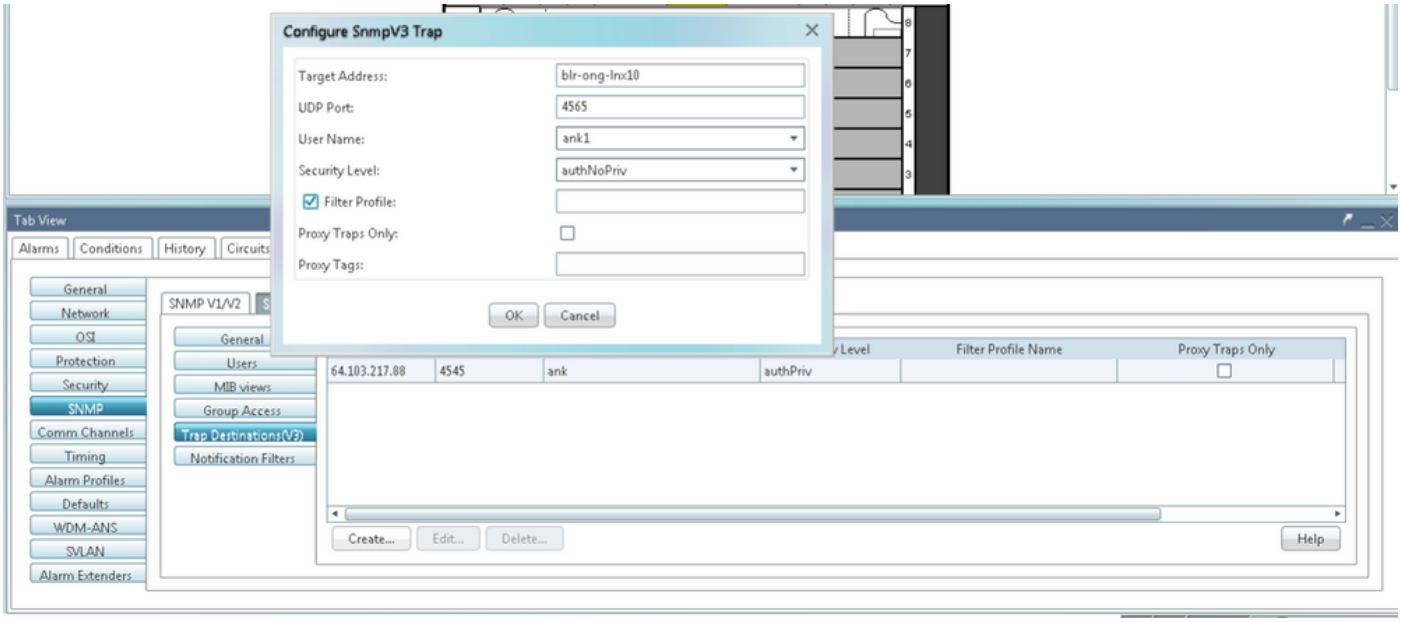
Passaggio 3. Verificare che le viste MIB siano configurate come mostrato nell'immagine.



Passaggio 4. Configurare l'accesso al gruppo come mostrato nell'immagine per la modalità authnopriv.



Passaggio 5. Passare a **Vista nodo > Provisioning > SNMP > SNMP V3 > Destinazione trap (V3)**. Fare clic su **Create** and **Configure** (Crea e configura) come mostrato nell'immagine.



Verifica modalità authNoPriv

Passaggio 1. Passare al server NMS ed eseguire lo snmpwalk.

Sintassi:

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

Esempio:

```
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
```

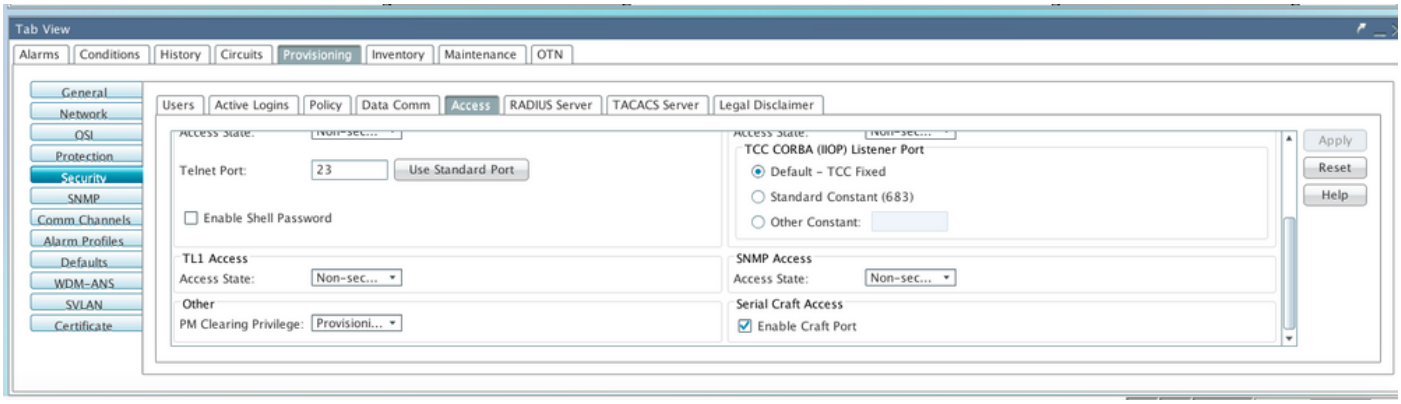
Trap SNMP:

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

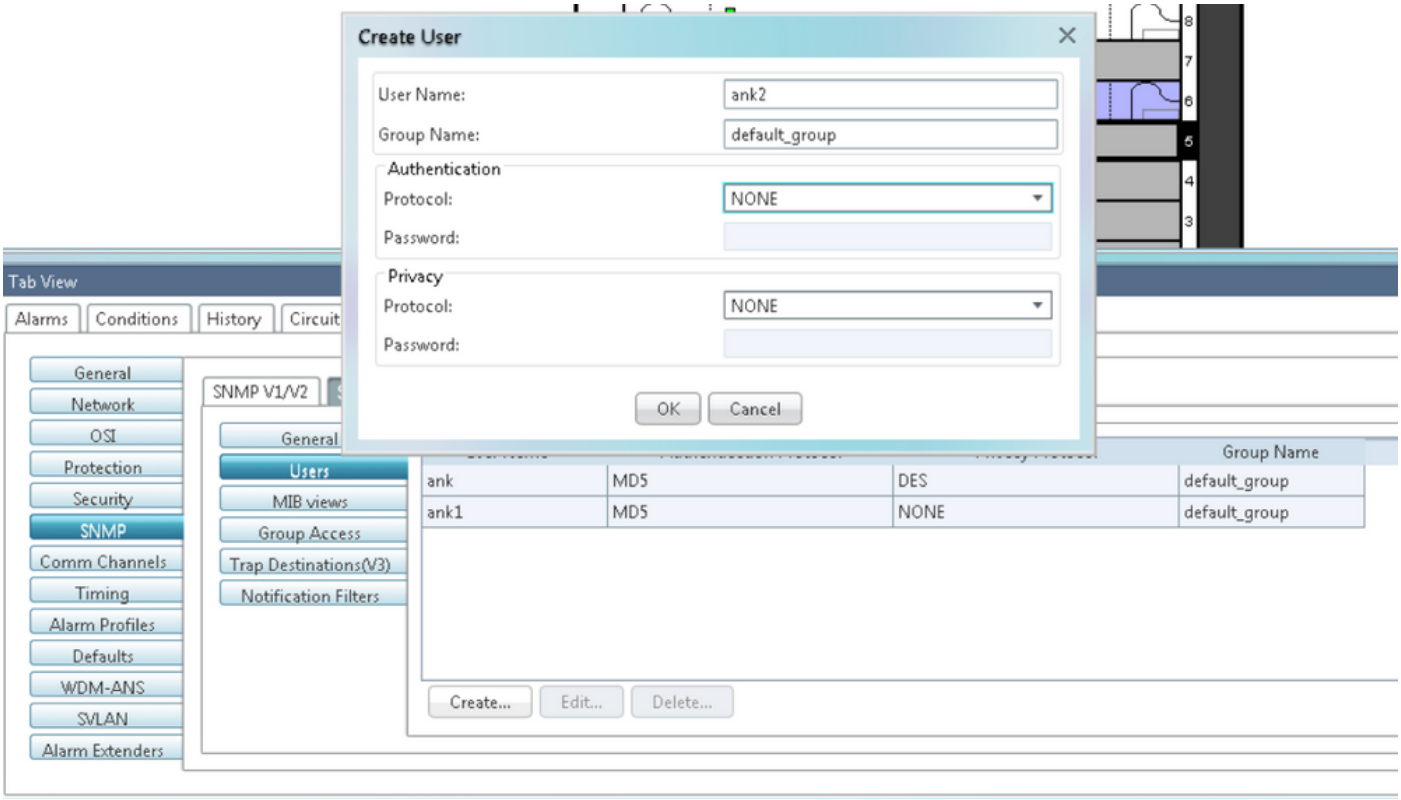
Il comando Trap è lo stesso per tutte le versioni.

Configurazione della modalità noAuthNoPriv su un dispositivo ONS15454/NCS2000

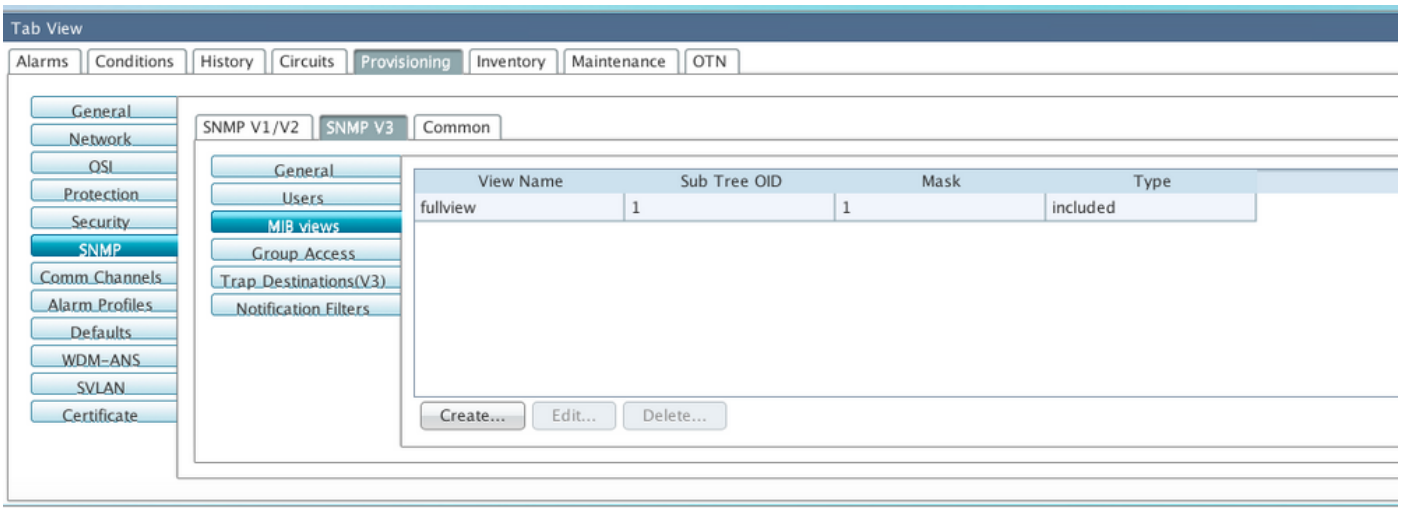
Passaggio 1. In CTC, selezionare **Node View > Provisioning > Security > Access > change snmp access state to Non-secure mode** (Visualizzazione nodo > Provisioning > Sicurezza > Accesso > Modifica stato accesso snmp in modalità non protetta), come mostrato nell'immagine.



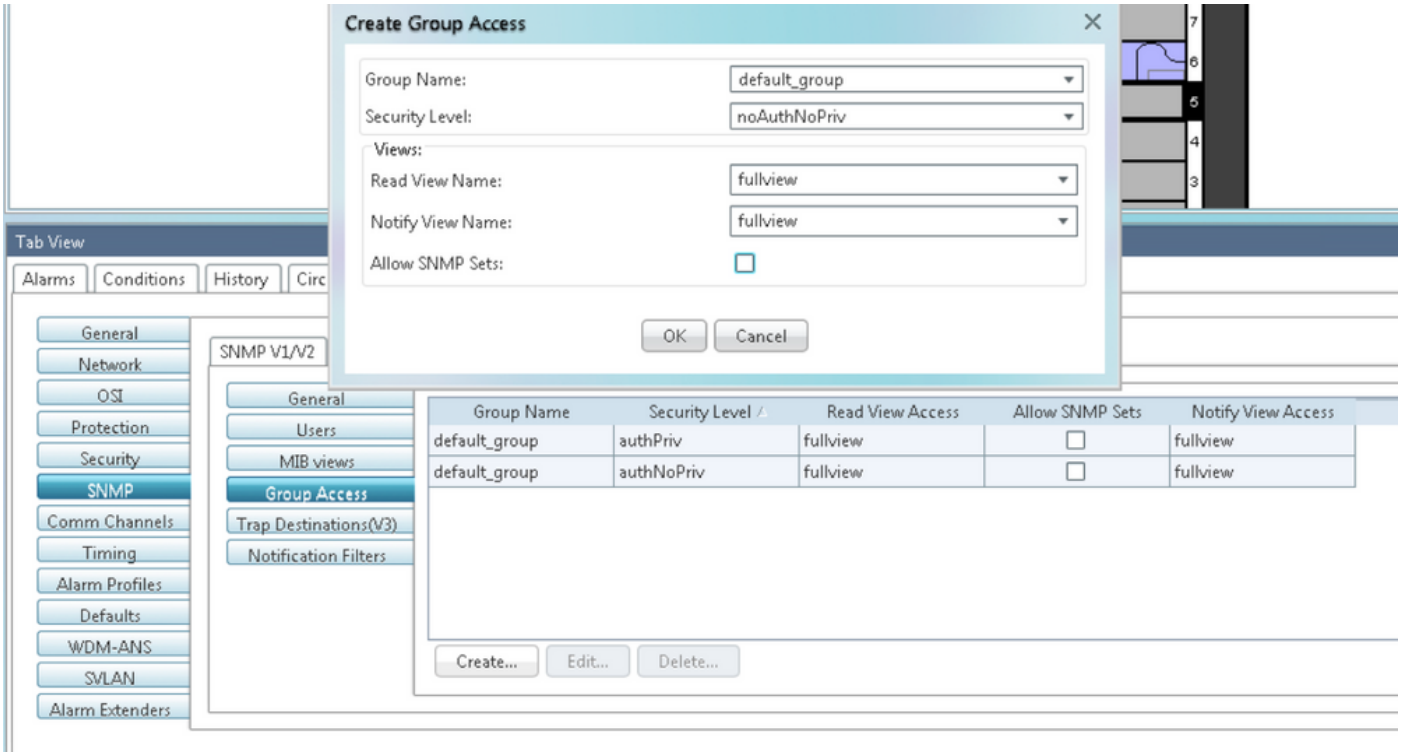
Passaggio 2. Passare a **Vista nodo > Provisioning > SNMP > SNMP V3 > Utenti > Crea utente e Configura** come mostrato nell'immagine.



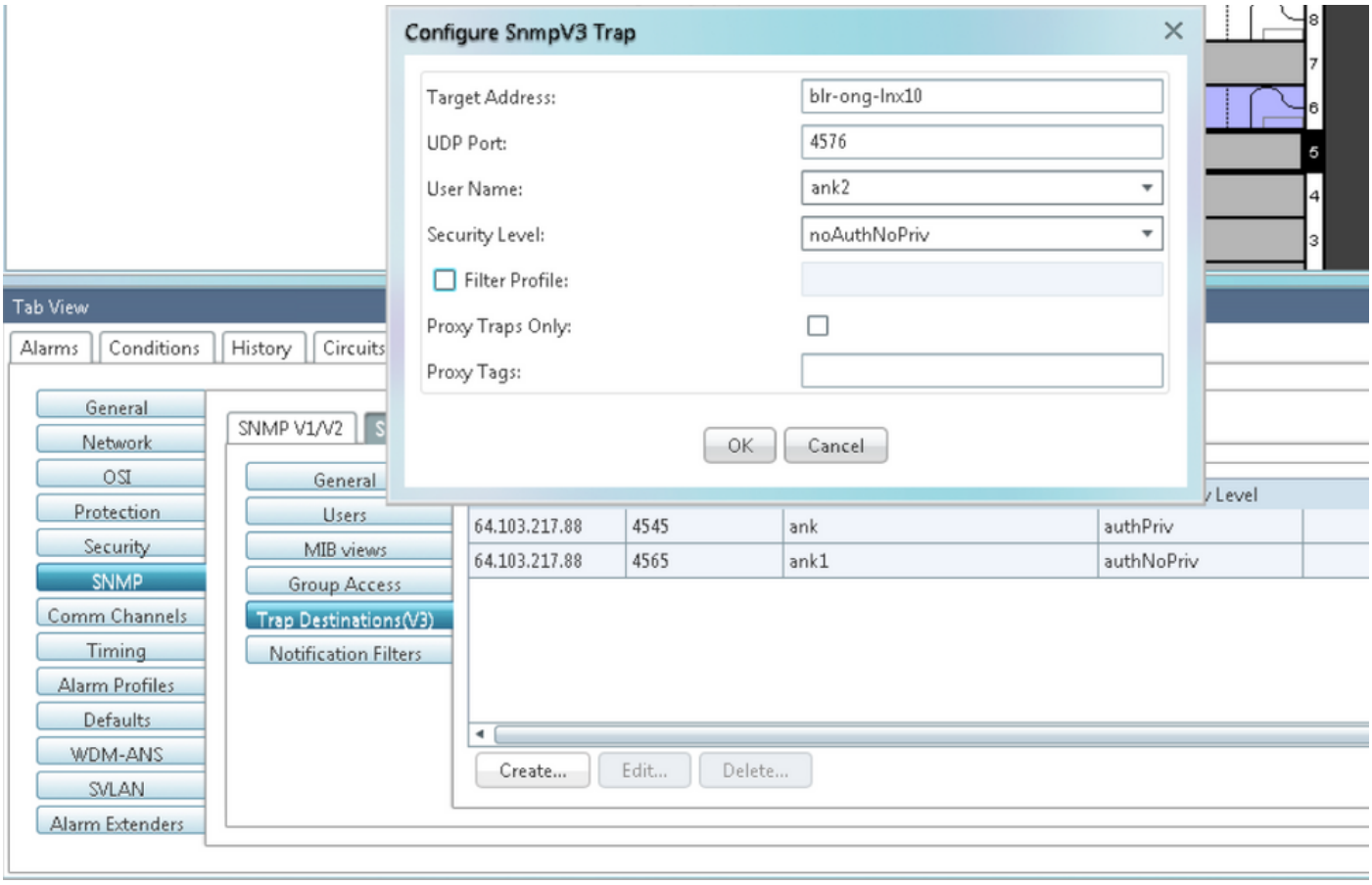
Passaggio 3. Verificare che **le viste MIB** siano configurate come mostrato nell'immagine.



Passaggio 4. Configurare l'accesso al gruppo come mostrato nell'immagine per la modalità noauthnopriv.



Passaggio 5. Passare a **Vista nodo > Provisioning > SNMP > SNMP V3 > Destinazione trap (V3)**. Fare clic su **Create** and **Configure** (Crea e configura) come mostrato nell'immagine.



Verifica modalità noAuthNoPriv

Passaggio 1. Passare al server NMS ed eseguire lo snmpwalk.

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

Esempio:

```
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>
```

Trap SNMP:

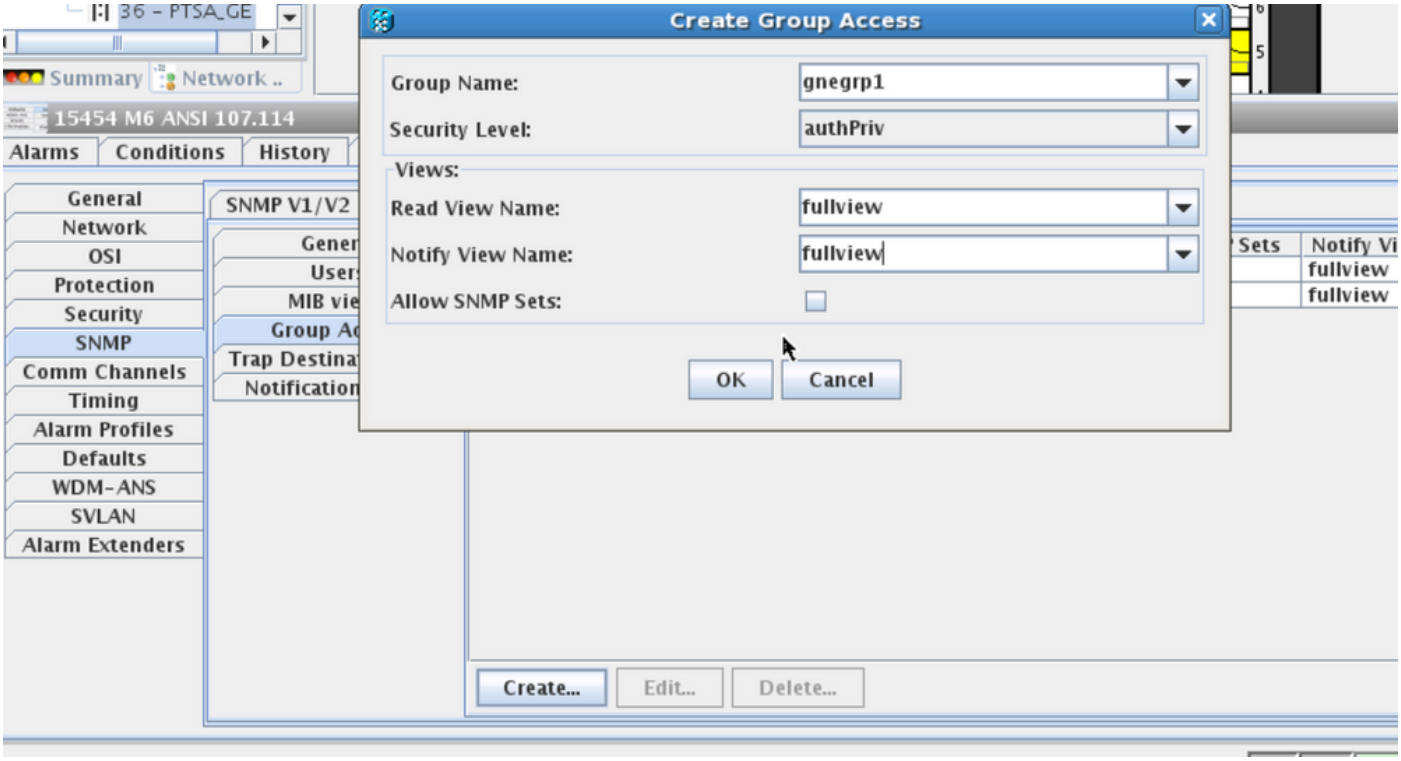
```
snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n" <port number>
```

Il comando Trap è lo stesso per tutte le versioni.

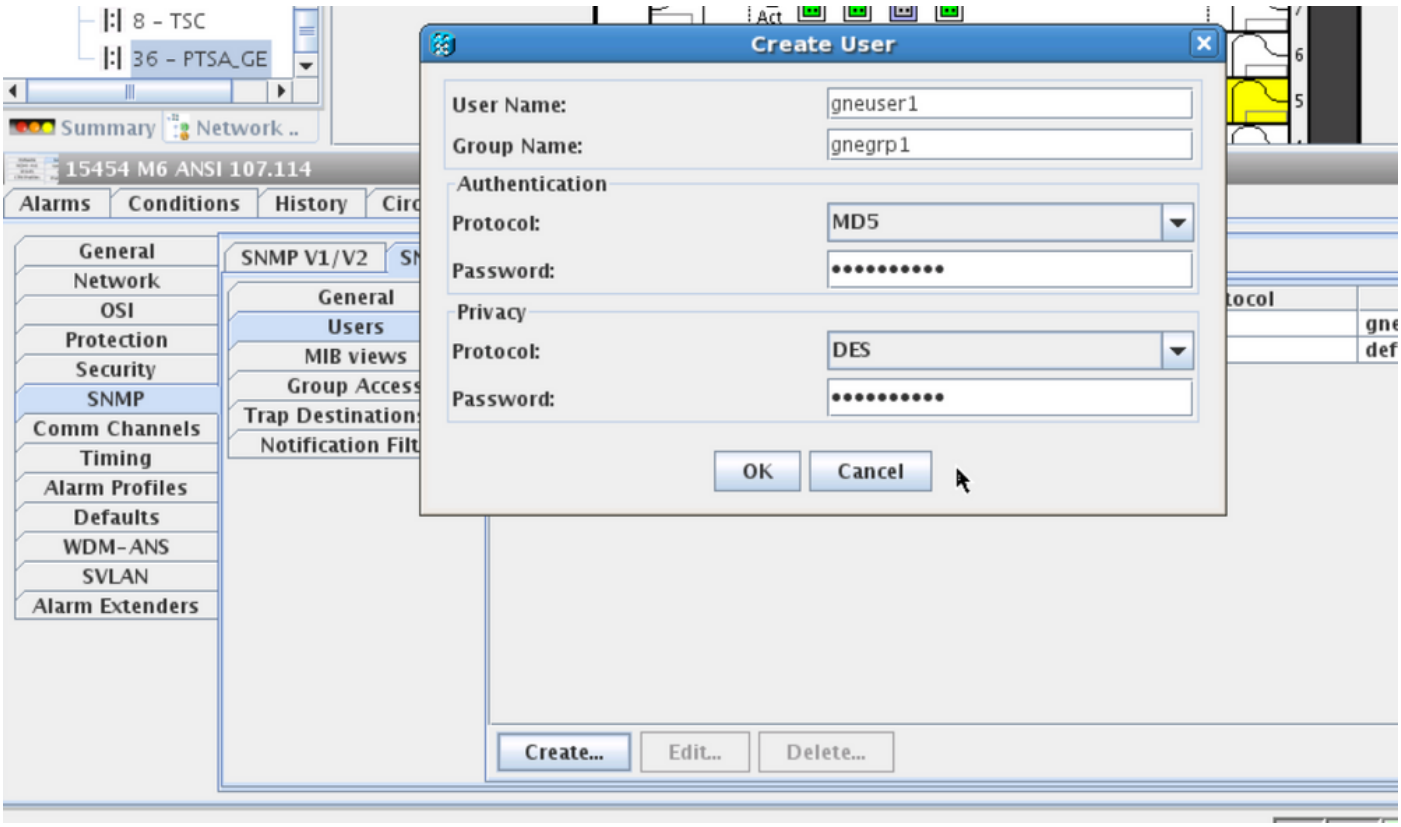
Trap SNMP V3 per configurazione GNE/ENE

Su nodo GNE

Passaggio 1. Passare a **Provisioning > SNMP > SNMP V3 e CCrea accesso gruppo (scheda Accesso gruppo): fornire un nome di gruppo con il livello di protezione (noAuthnoPriv|AuthnoPriv|authPriv) e l'accesso in lettura e notifica della visualizzazione completa, come mostrato nell'immagine.**



Passaggio 2. Creazione dell'accesso utente (scheda Utenti): creare un utente con lo stesso nome di gruppo creato in precedenza nella scheda Accesso gruppo. Fornire inoltre l'autenticazione basata sul livello di accesso, come mostrato nell'immagine.



Passaggio 3. Scheda Destinazione trap (V3):

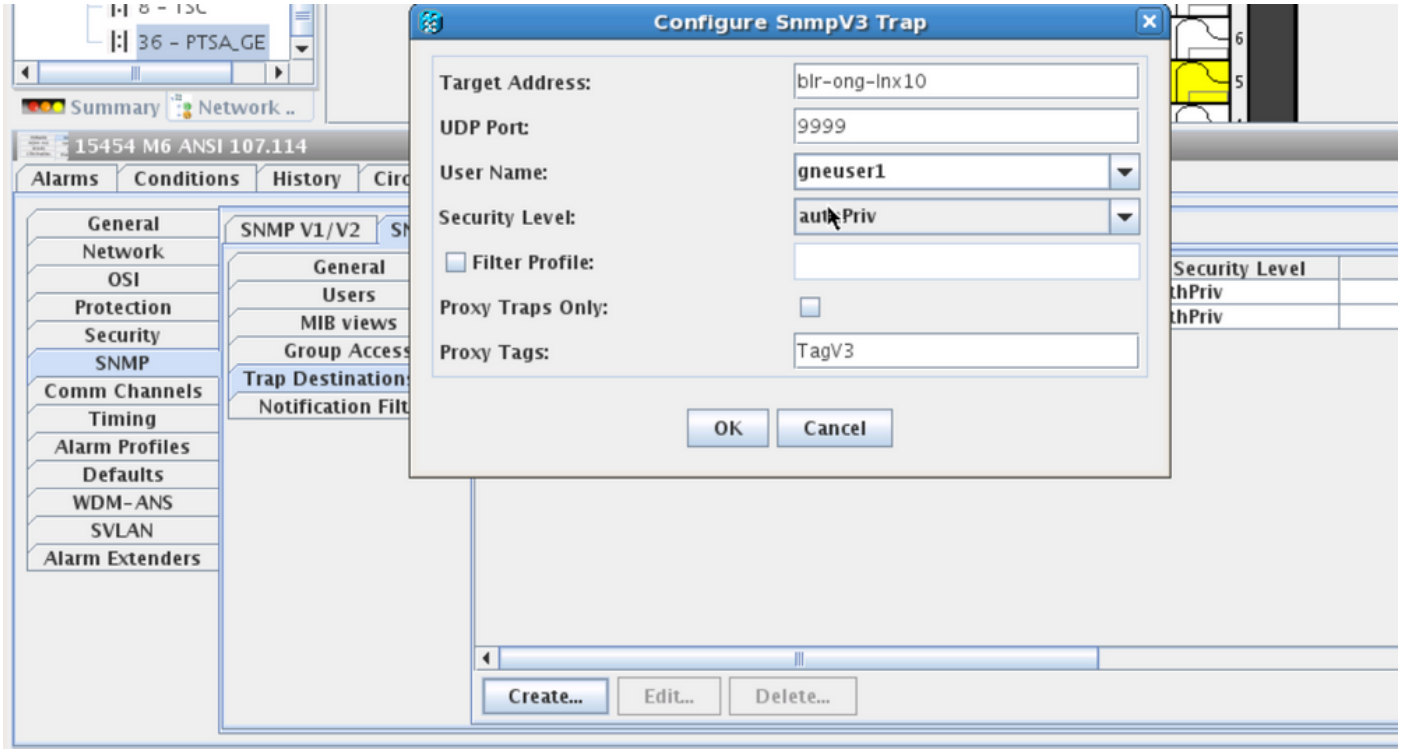
Target Address: Indirizzo del server NMS da cui verrà eseguita la trap, ad esempio Blr-ong-lnx10).

Porta UDP: Qualsiasi numero di porta in cui verrà ascoltata la trap (ad esempio, 9977).

Nome utente: Nome dell'utente nella scheda Utente.

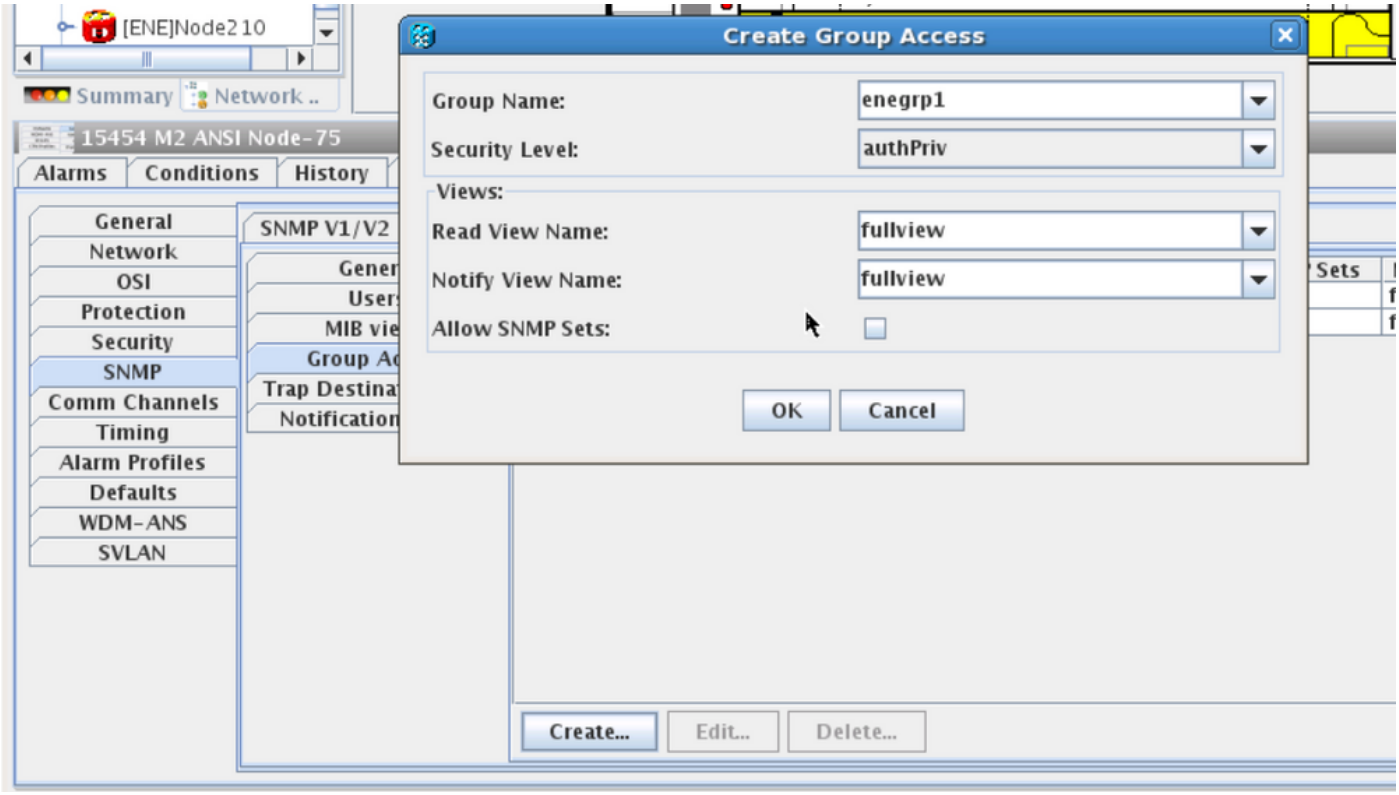
Livello di protezione: Come configurato in precedenza nella scheda Utente.

Tag proxy: Fornire un tag proxy (es. Tag75).

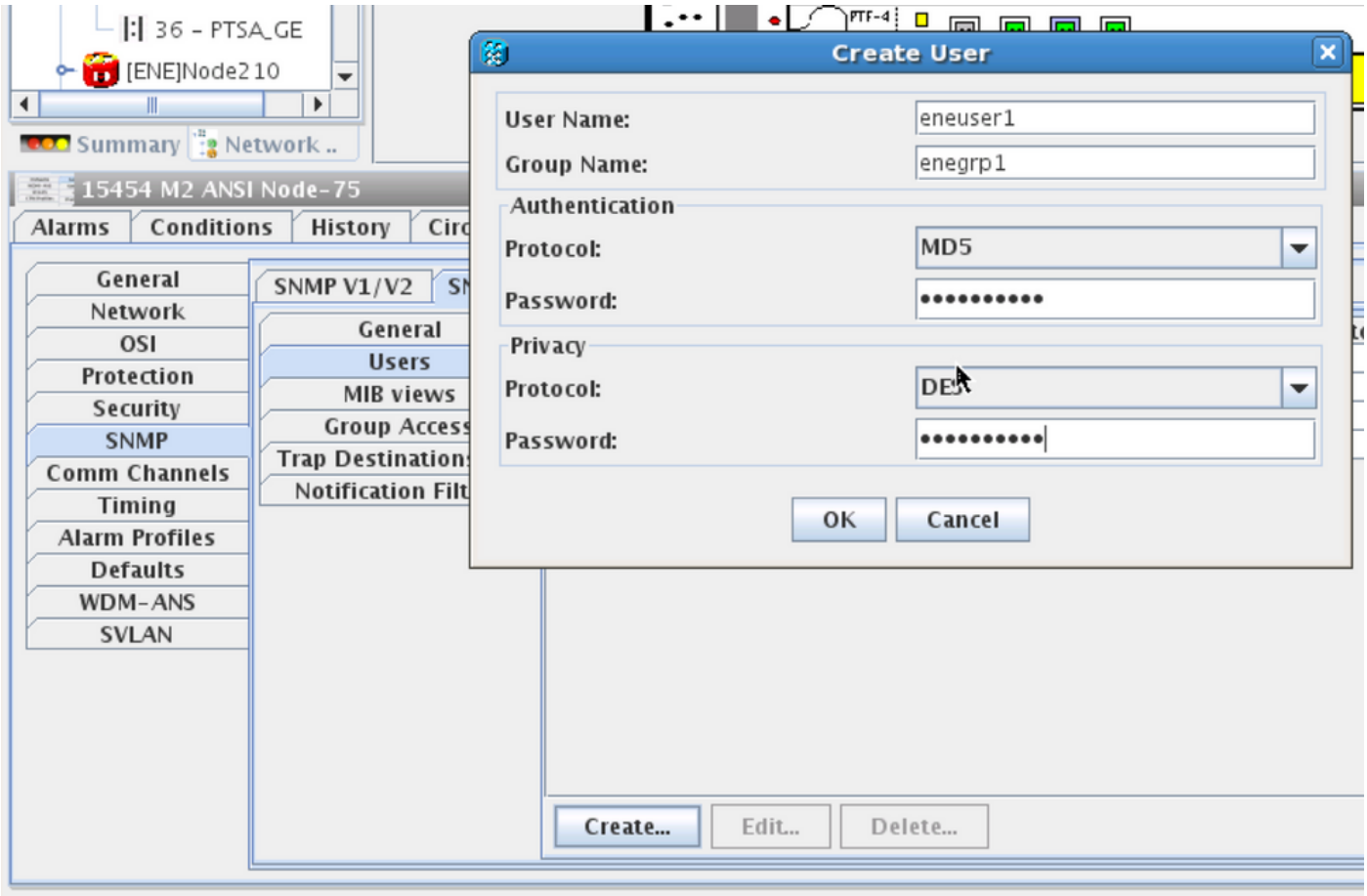


Su nodo ENE

Passaggio 1. Passare a **Provisioning > SNMP > SNMP V3 e Crea accesso gruppo (scheda Accesso gruppo):** fornire un nome di gruppo con livello di accesso (noAuthnoPriv|AuthnoPriv|authPriv) e accesso in lettura e notifica della visualizzazione completa, come mostrato nell'immagine.



Passaggio 2. Creazione dell'accesso utente (scheda Utenti): creare un utente con lo stesso nome di gruppo creato in precedenza nella scheda Accesso gruppo. Fornire inoltre l'autenticazione basata sul livello di accesso.



Assicurarsi che venga creato un default_group se visualizzato nella scheda Utente nella scheda Accesso al gruppo nel caso in cui non sia presente nella scheda Accesso al gruppo.

Passaggio 3. Scheda Destinazione trap (V3):

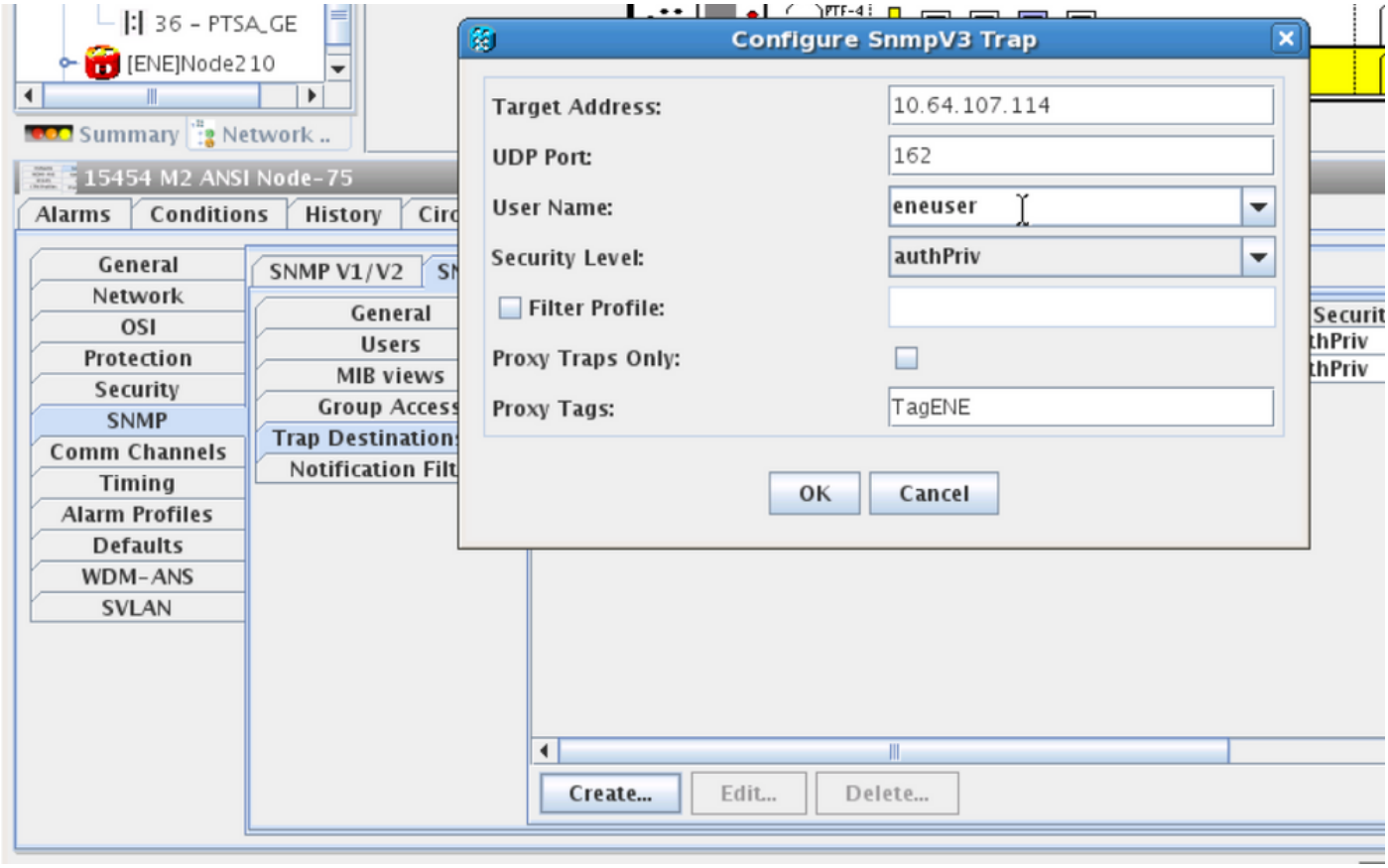
Target Address: IP nodo GNE.

Porta UDP: 162.

Nome utente: Nome dell'utente nella scheda Utente.

Livello di protezione: Come configurato in precedenza nella scheda Utente.

Tag proxy: Fornire un tag proxy uguale a quello di GNE (ad es. Tag75).



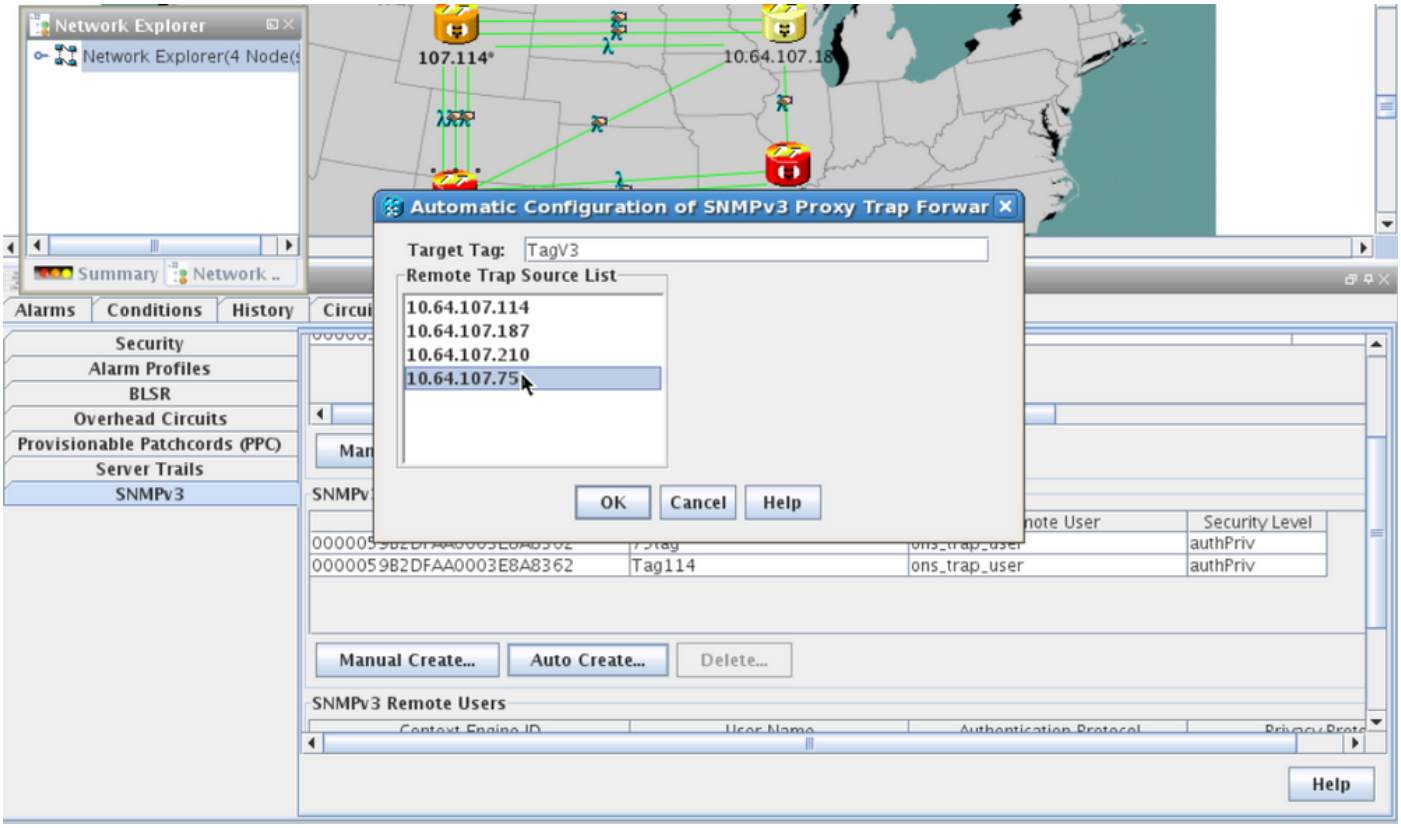
In CTC, passare alla visualizzazione rete:

Passaggio 1. Passare alla scheda **SNMPv3**.

Passaggio 2. Tabella del server di inoltro delle trap proxy SNMPv3: È possibile eseguire la **creazione manuale** o **automatica**.

Selezionare **Creazione automatica**. Ai sensi di tale articolo:

- Tag di destinazione: Tag proxy impostato in GNE.
- Elenco origini trap remote: selezionare il nodo ENE IP come mostrato nell'immagine.



Verifica configurazione GNE/ENE

Configurare il server NMS (blr-ong-lnx10):

Passaggio 1. Nella home directory del server, creare una directory e denominarla **snmp**.

Passaggio 2. In questa directory, creare un file **snmptrapd.conf**.

Passaggio 3. In **snmptrapd.conf**, creare la configurazione seguente:

```
createUser -e 0x
```

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

Trap SNMP:

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

snmpwalk su ENE:

Per la modalità di autenticazione:

```
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>
```

Per la modalità authnopriv:

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

Per la modalità noauthnopriv:

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

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.