在Cisco ONS15454/NCS2000裝置上配置SNMPv3

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[設定](#)
[在獨立/多機架節點上](#)
[在ONS15454/NCS2000裝置上配置authPriv模式](#)
[配置NMS伺服器(blr-long-lnx10)](#)
[驗證authPriv模式](#)
[在ONS15454/NCS2000裝置上配置authNoPriv模式](#)
[驗證authNoPriv模式](#)
[在ONS15454/NCS2000裝置上配置noAuthNoPriv模式](#)
[驗證noAuthNoPriv模式](#)
[適用於GNE/ENE設定的SNMP V3陷阱](#)
[在GNE節點上](#)
[在ENE節點上](#)
[驗證GNE/ENE設定](#)
[疑難排解](#)

簡介

本文描述如何在ONS15454/NCS2000裝置上配置簡單網路管理協定版本3(SNMPv3)的逐步說明。所有主題均包含示例。

> **附註**：本檔案提供的屬性清單並不詳盡，也不具權威性，可能會隨時變更，無需更新本檔案即可。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Transport Controller(CTC)GUI
- 基本伺服器知識
- 基本Linux/Unix命令

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

在獨立/多機架節點上

在ONS15454/NCS2000裝置上配置authPriv模式

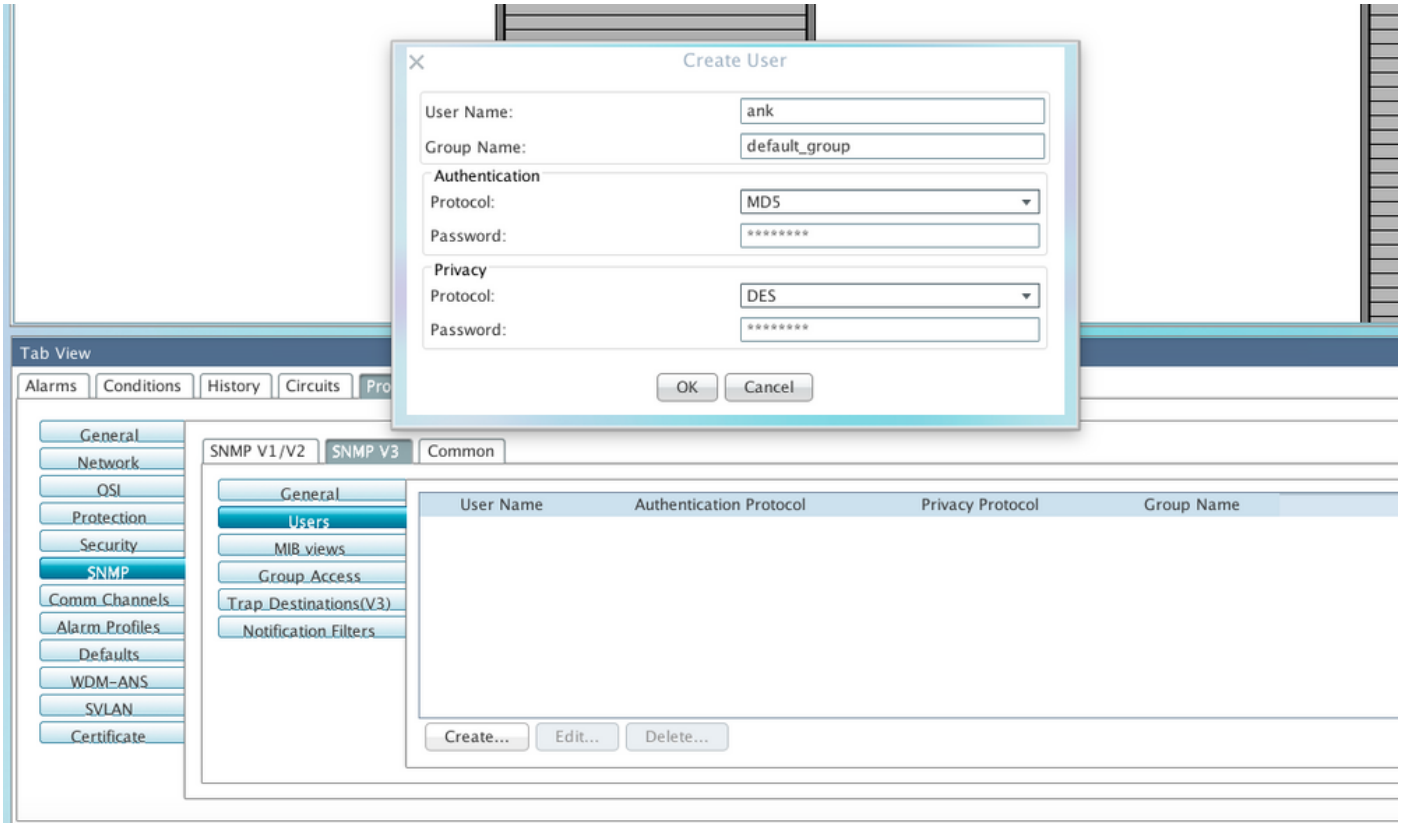
步驟1.使用超級使用者憑據通過CTC登入到節點。

步驟2.導覽至**節點檢視>布建> SNMP > SNMP V3**。

步驟3.導航到**Users**頁籤。建立使用者。

```
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>
```

步驟4.按一下**OK**，如下圖所示。



規格：

使用者名稱 — 指定連線到代理的主機上的使用者名稱稱。使用者名稱必須至少為6個字元，最多為40個字元（對於TACACS和RADIUS身份驗證，最多只能為39個字元）。 它包括字母數字(a-z、A-Z、0-9)字元，允許的特殊字元為@、"-"（連字元）和"。 （點）。 為了與TL1相容，使用者名稱必須包含6到10個字元。

組名 — 指定使用者所屬的組。

驗證:

Protocol — 選擇要使用的身份驗證演算法。選項包括NONE、MD5和SHA。

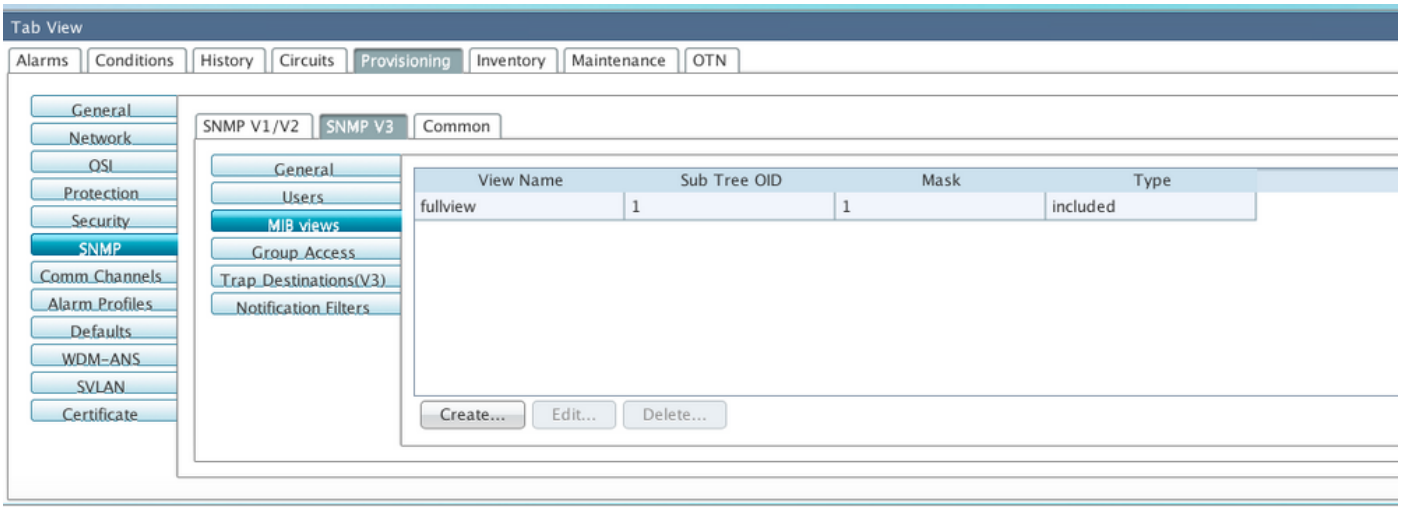
密碼 — 如果您選擇MD5或SHA，請輸入密碼。預設情況下，密碼長度設定為至少八個字元。

隱私 — 啟動隱私身份驗證級別設定會話，使主機能夠加密傳送到代理的郵件的內容。

協定 — 選擇隱私身份驗證演算法。可用的選項包括None、DES和AES-256-CFB。

Password — 如果選擇None以外的協定，請輸入密碼。

步驟5.確保根據此映像配置MIB檢視。



規格：

Name — 檢視的名稱。

子樹OID - MIB子樹，在與掩碼結合使用時定義子樹系列。

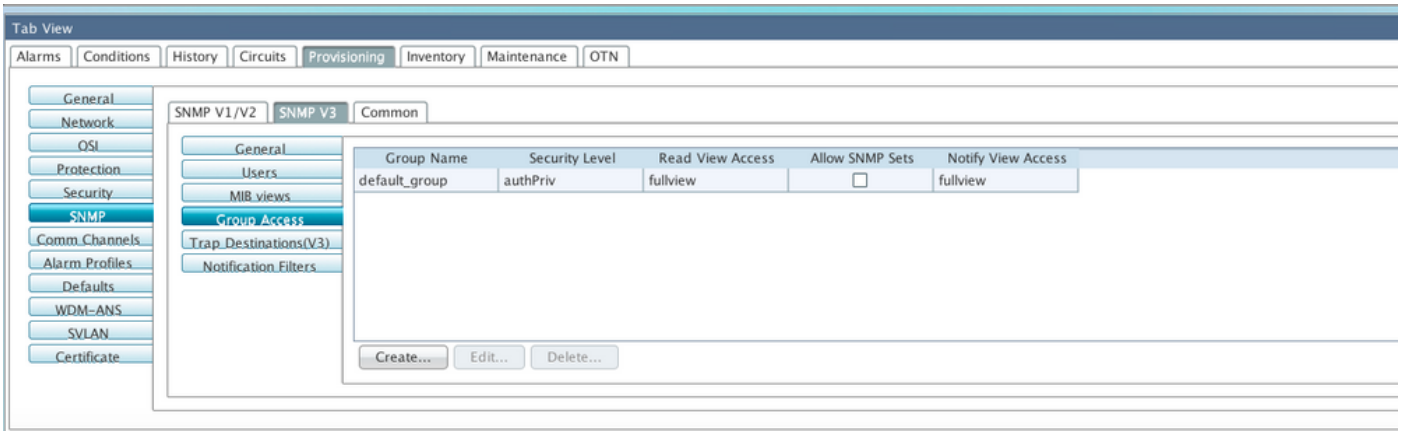
位掩碼 — 檢視子樹族。位掩碼中的每個位對應於子樹OID的子識別符號。

型別 — 選擇檢視型別。選項包括和排除。

型別定義子樹OID和位掩碼組合所定義的子樹族是否包含在通知過濾器中，或是否排除在通知過濾器之外。

步驟6.設定群組存取，如下圖所示。預設情況下，組名稱將為default_group，安全級別為authPriv。

附註：組名應與您在步驟3中建立使用者時使用的組名相同。



規格：

Group Name - SNMP組的名稱，或共用通用訪問策略的使用者集合。

Security Level — 為其定義訪問引數的安全級別。從以下選項中選擇：

noAuthNoPriv — 使用匹配的使用者名稱進行身份驗證。

AuthNoPriv — 提供基於HMAC-MD5或HMAC-SHA演算法的身份驗證。

AuthPriv — 提供基於HMAC-MD5或HMAC-SHA演算法的身份驗證。除了身份驗證之外，還提供基於CBC-DES(DES-56)標準的DES 56位加密。

如果為組選擇authNoPriv或authPriv，則必須為相應的使用者配置身份驗證協定和密碼、隱私協定和密碼，或兩者都配置。

檢視

Read View Name — 組的讀取檢視名稱。

Notify View Name — 通知組的檢視名稱。

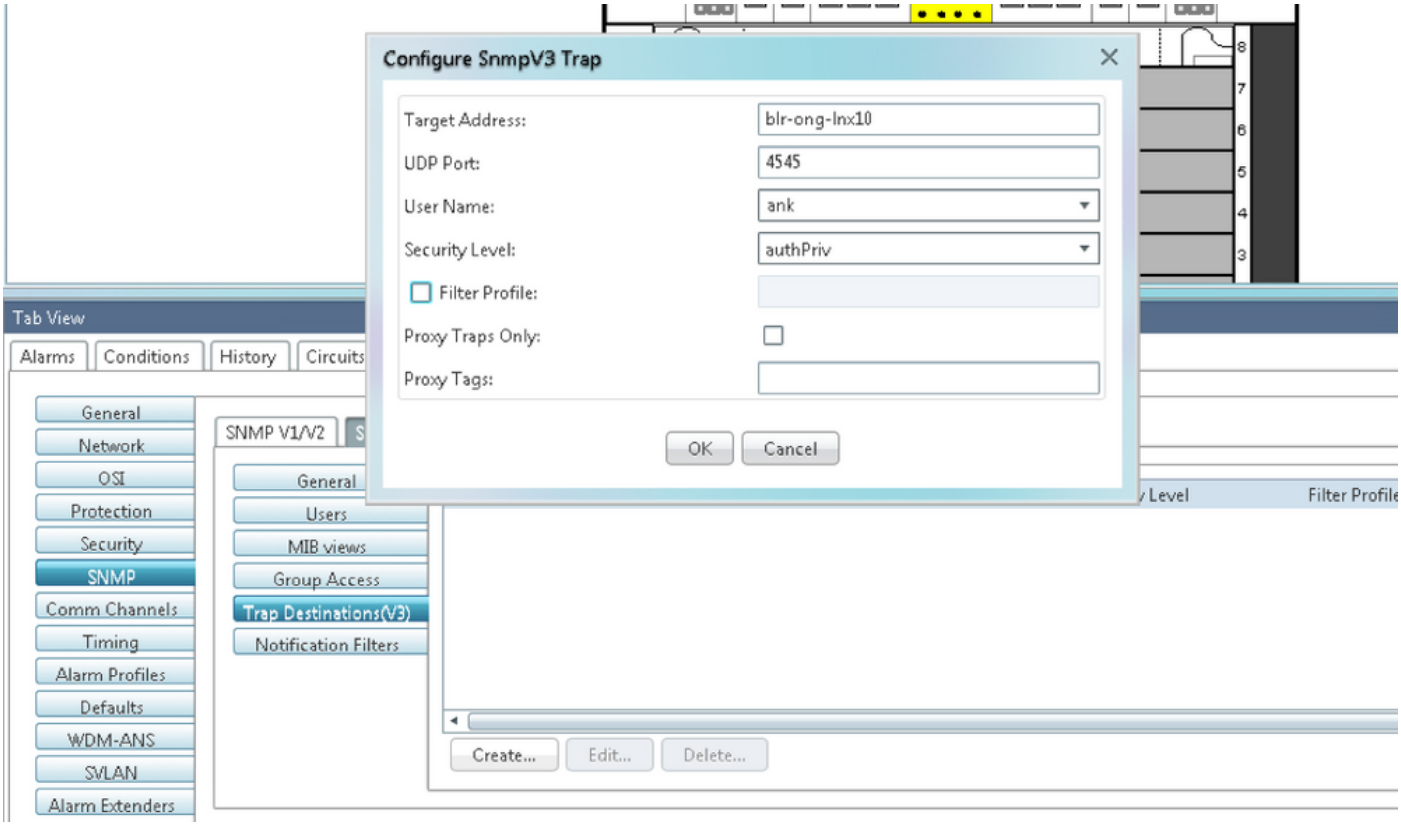
允許SNMP集 — 如果希望SNMP代理接受SNMP SET請求，請選中此覈取方塊。如果未選中此覈取方塊，則會拒絕SET請求。

附註： SNMP SET請求訪問是為極少數對象實現的。

步驟7.導覽至**Node View > Provisioning > SNMP > SNMP V3 > Trap Destination(V3)**。 按一下「**Create**」和「**Configure**」。

```
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
```

步驟8.按一下**OK**，如下圖所示。



註：blr-ong-lnx10是NMS伺服器。

規格：

Target Address — 應將陷阱傳送到的目標。使用IPv4或IPv6地址。

UDP埠 — 主機使用的UDP埠號。預設值為 162。

使用者名稱 — 指定連線到代理的主機上的使用者名稱稱。

安全級別 — 選擇以下選項之一：

noAuthNoPriv — 使用匹配的使用者名稱進行身份驗證。

AuthNoPriv — 提供基於HMAC-MD5或HMAC-SHA演算法的身份驗證。

AuthPriv — 提供基於HMAC-MD5或HMAC-SHA演算法的身份驗證。除了身份驗證之外，還提供基於CBC-DES(DES-56)標準的DES 56位加密。

Filter Profile — 選中此覈取方塊並輸入過濾器配置檔名稱。只有當您提供過濾器配置檔名稱並建立通知過濾器時，才會傳送陷阱。

僅代理陷阱 — 如果選擇此選項，則僅從ENE轉發代理陷阱。來自此節點的陷阱不會傳送到由此條目標識的陷阱目標。

代理標籤 — 指定標籤清單。只有在ENE需要將陷阱傳送到此條目所識別的陷阱目的地並且想要使用GNE作為代理時，GNE上才需要標籤清單。

配置NMS伺服器(blr-long-lnx10)

步驟1.在伺服器的主目錄中，建立名為snmp的**目錄**。

步驟2. 在此目錄下，建立檔案**snmptrapd.conf**。

步驟3.將**snmptrapd.conf**檔案變更為：

```
vi snmptrapd.conf

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

例如：

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

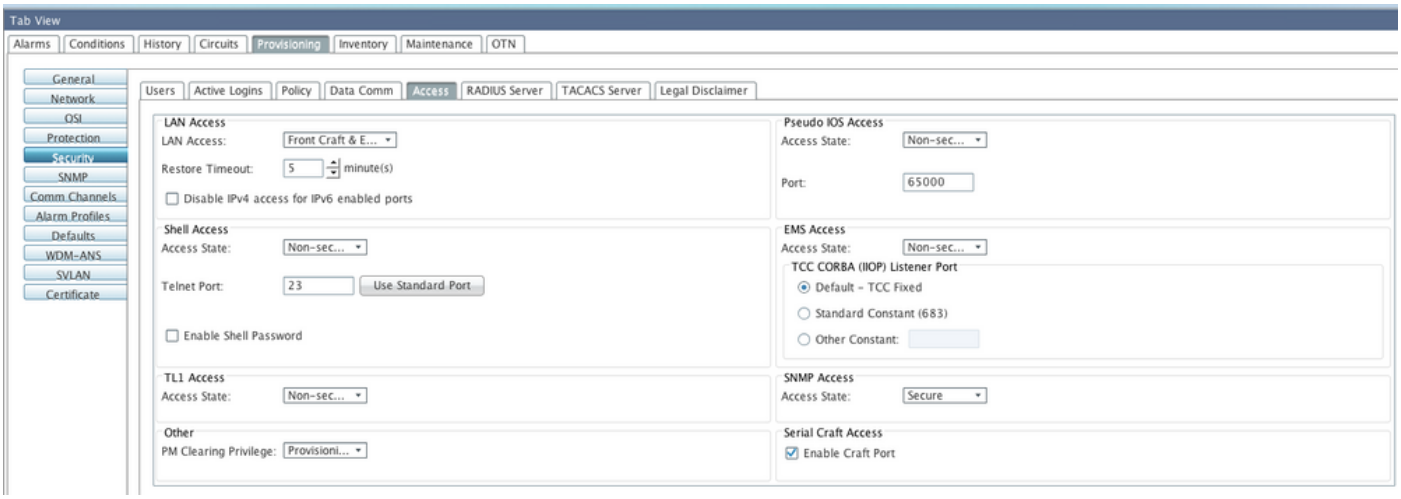
在此範例中：

```
user_name=ank

MD5 password = cisco123

DES password  = cisco123

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

Node view > Provisioning > SNMP > SNMP V3 > General

驗證authPriv模式

步驟1。在CTC中，導覽至**Node View > Provisioning > Security > Access > change snmp access state to Secure**，如下圖所示。



步驟2.導航到NMS伺服器並執行snmpwalk。

語法：

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

範例：

```
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
```

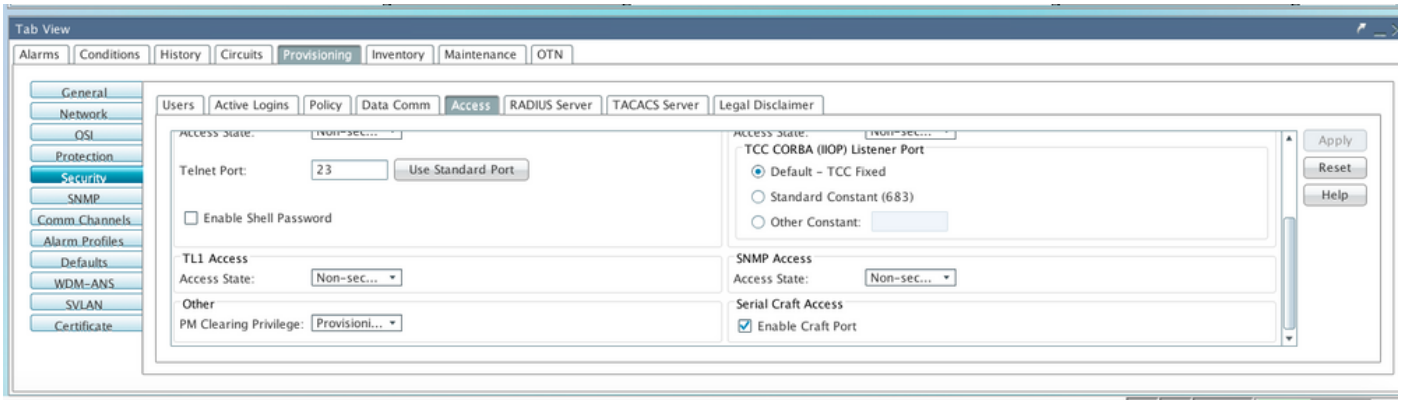
SNMP陷阱：

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

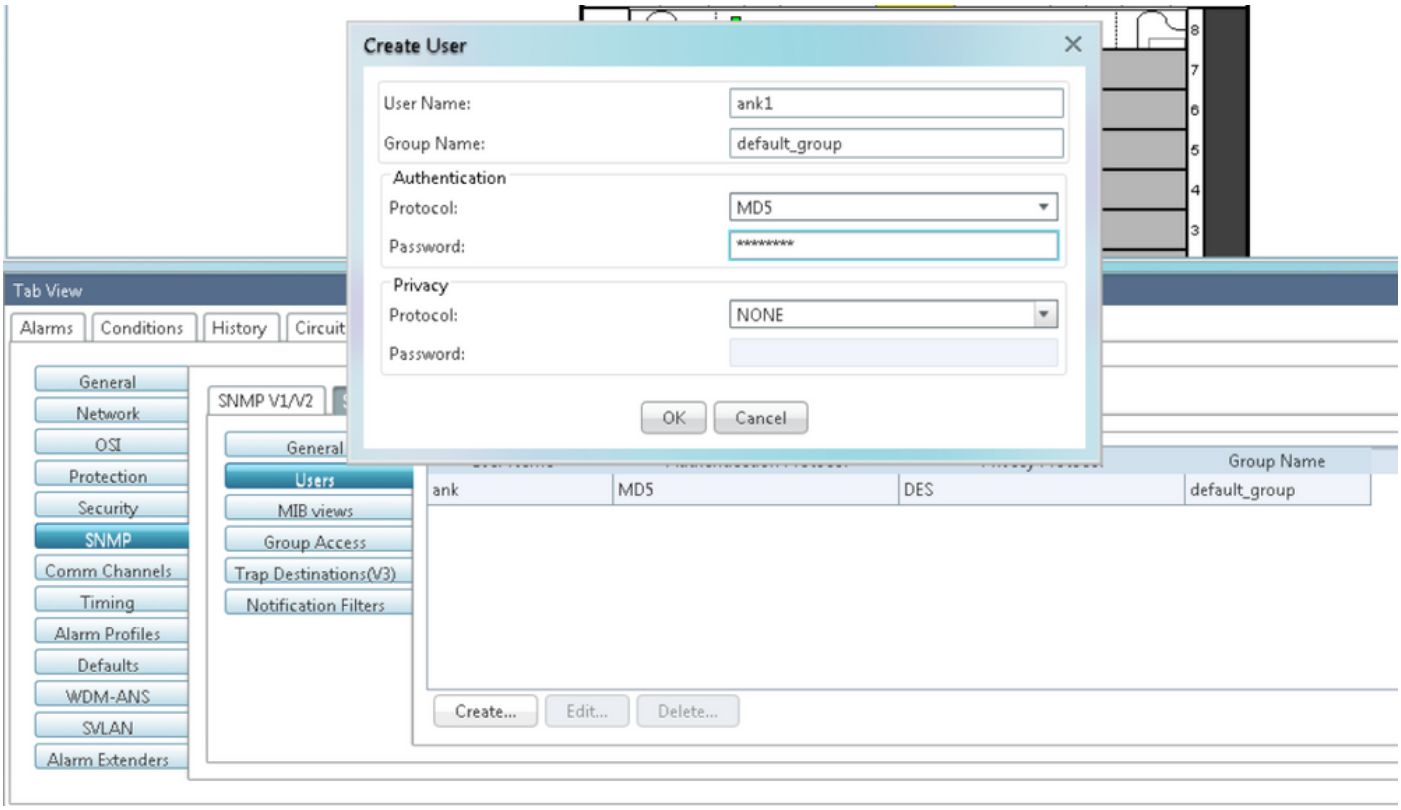
所有版本的陷阱命令都相同。

在ONS15454/NCS2000裝置上配置authNoPriv模式

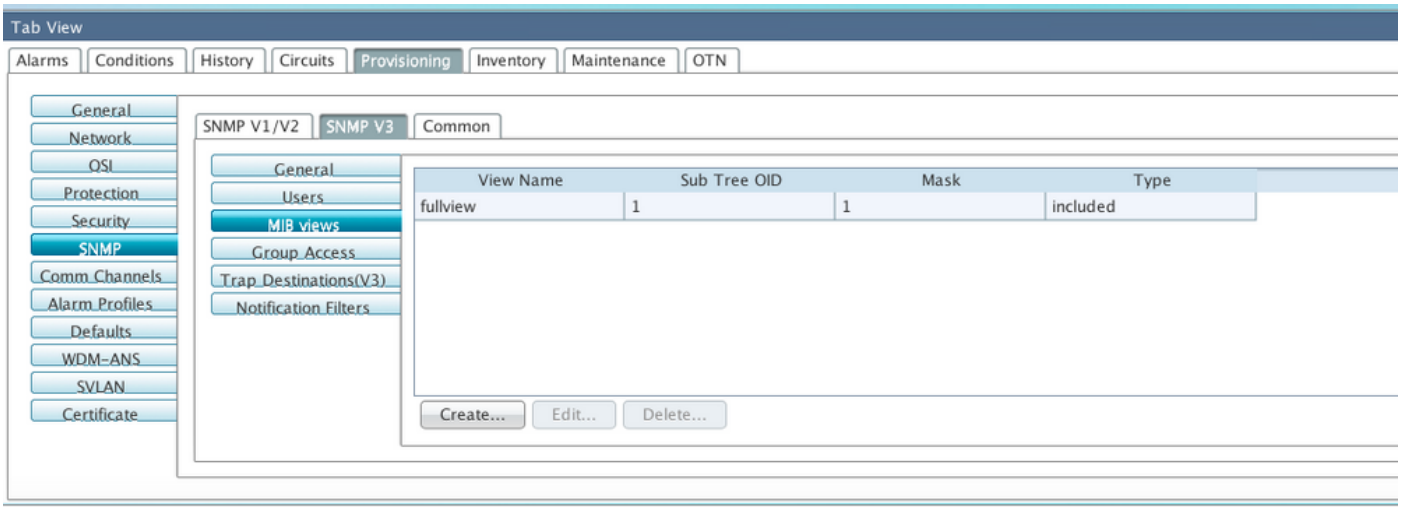
步驟1。在CTC中，導覽至**Node View > Provisioning > Security > Access > change snmp access state to Non-secure mode**，如下圖所示。



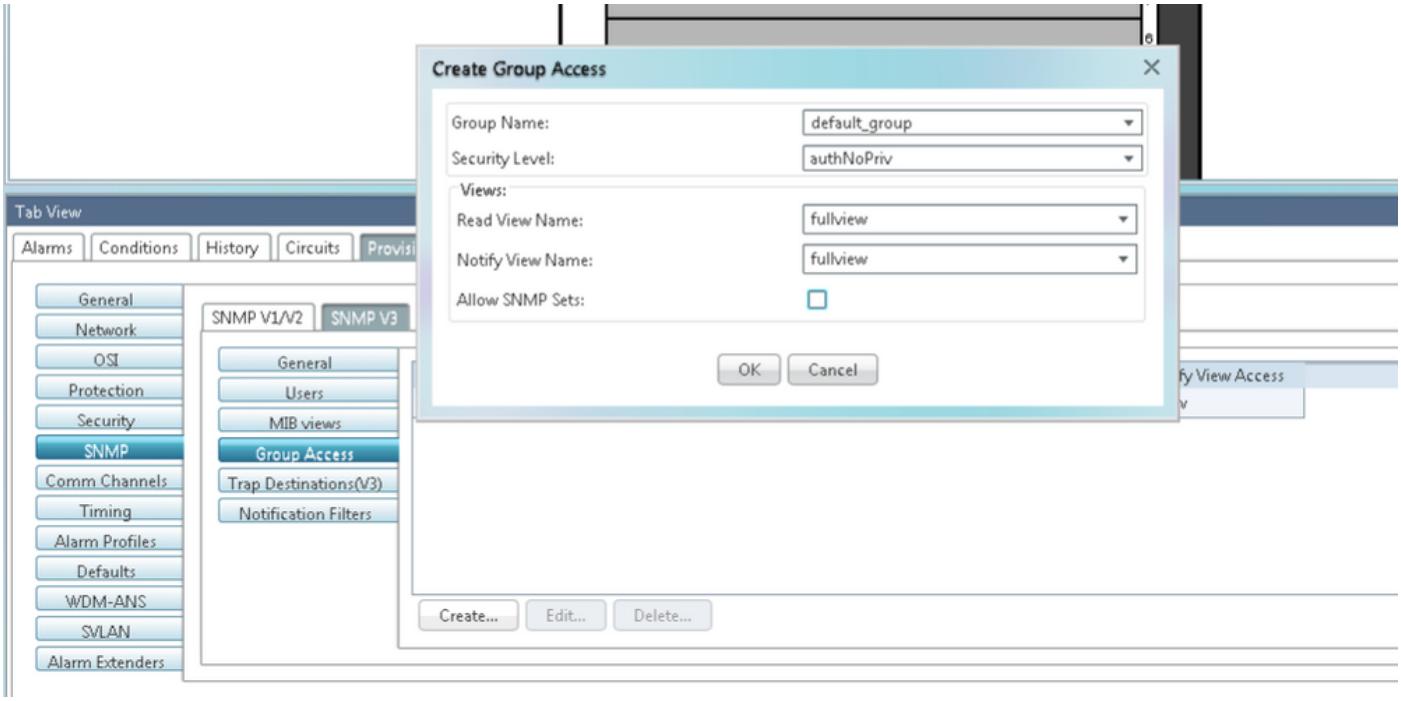
步驟2.導覽至Node View > Provisioning > SNMP > SNMP V3 > Users > Create User，並進行設定，如下圖所示。



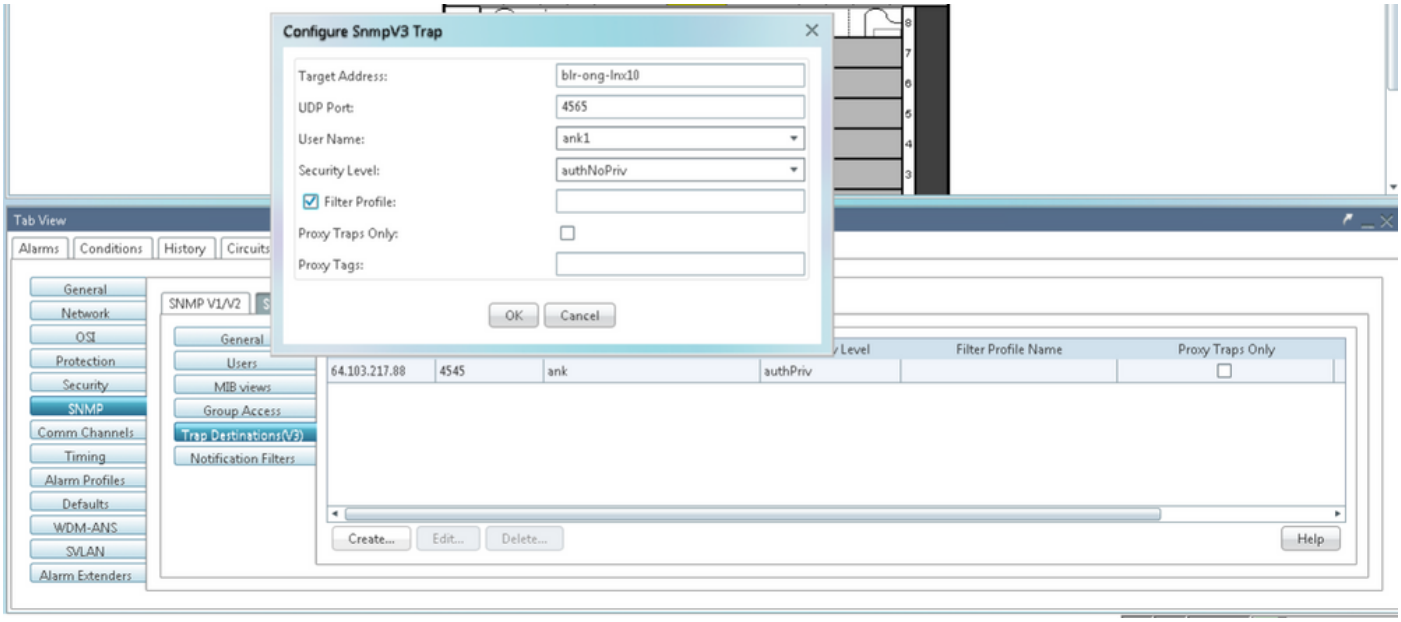
步驟3.確保MIB檢視的配置如圖所示。



步驟4.配置Group Access，如圖所示為authnopriv模式。



步驟5.導覽至**Node View > Provisioning > SNMP > SNMP V3 > Trap Destination(V3)**。 按一下「**Create**」和「**Configure**」，如下圖所示。



驗證authNoPriv模式

步驟1.導航到NMS伺服器並執行snmpwalk。

語法：

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

範例：

```
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
```

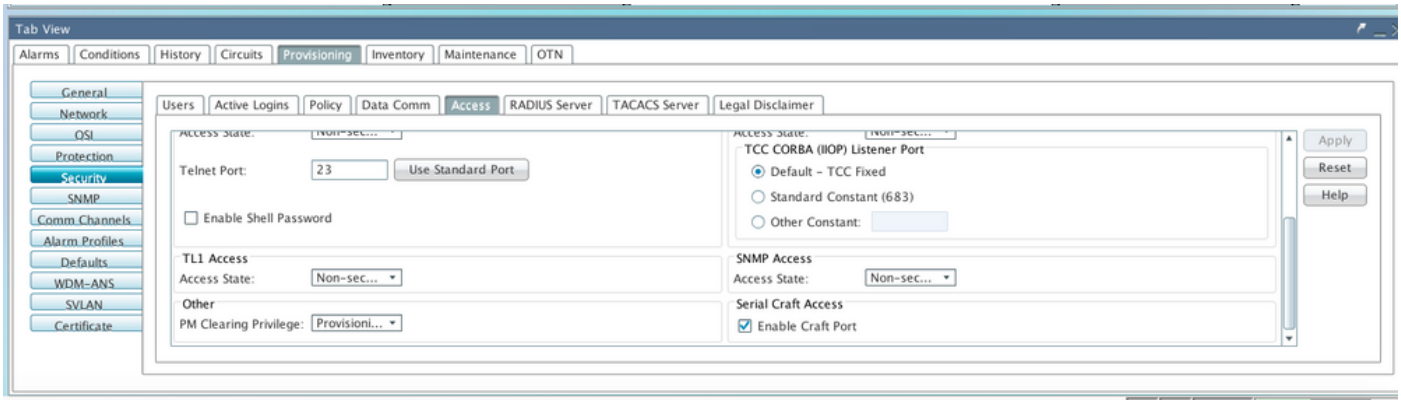
SNMP陷阱：

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

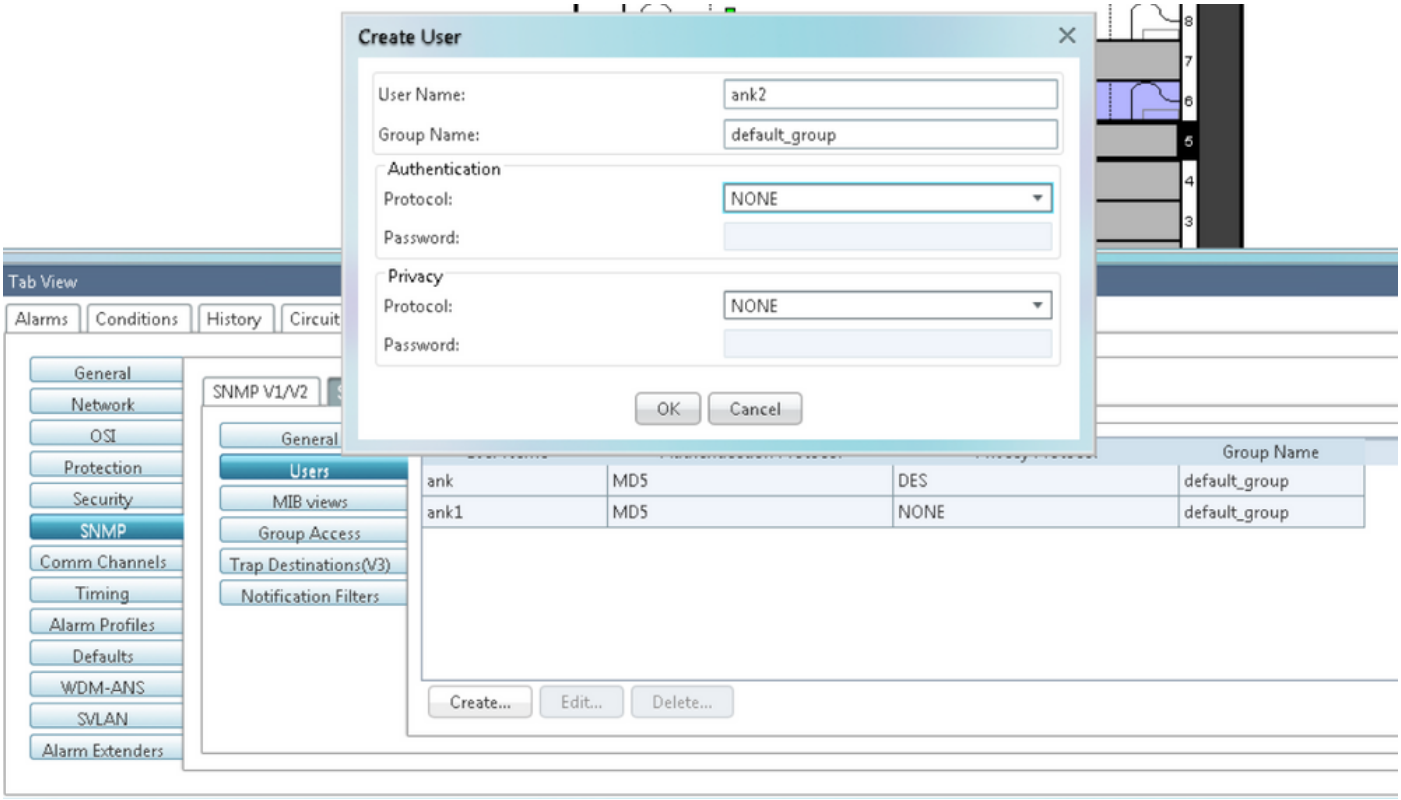
所有版本的陷阱命令都相同。

在ONS15454/NCS2000裝置上配置noAuthNoPriv模式

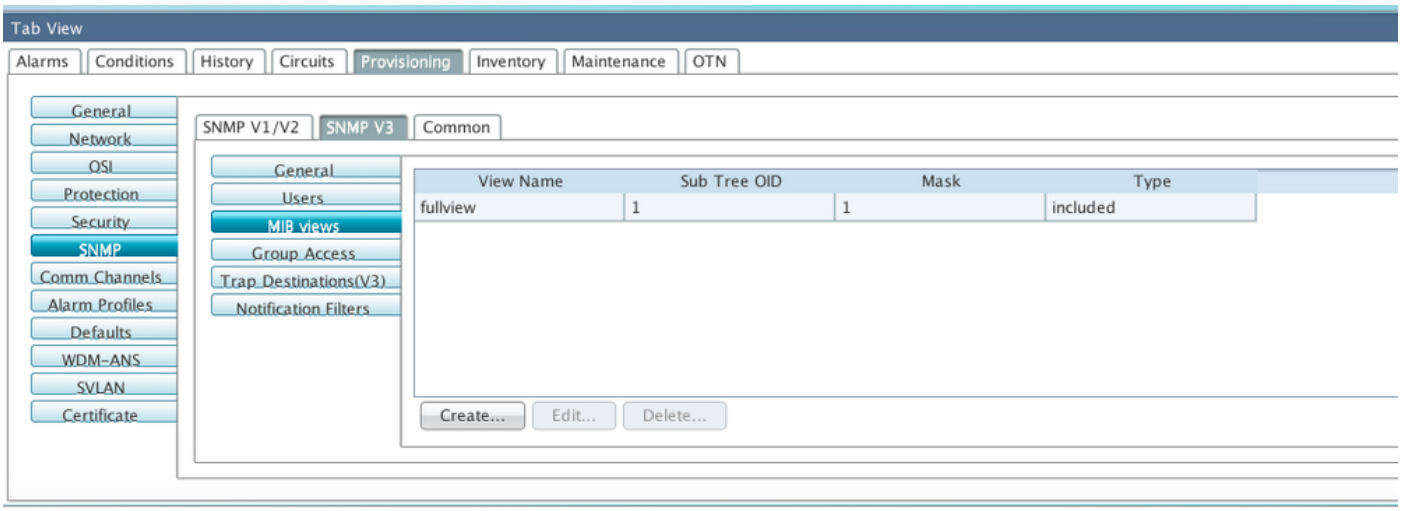
步驟1。在CTC中，導覽至**Node View > Provisioning > Security > Access > change snmp access state to Non-secure mode**，如下圖所示。



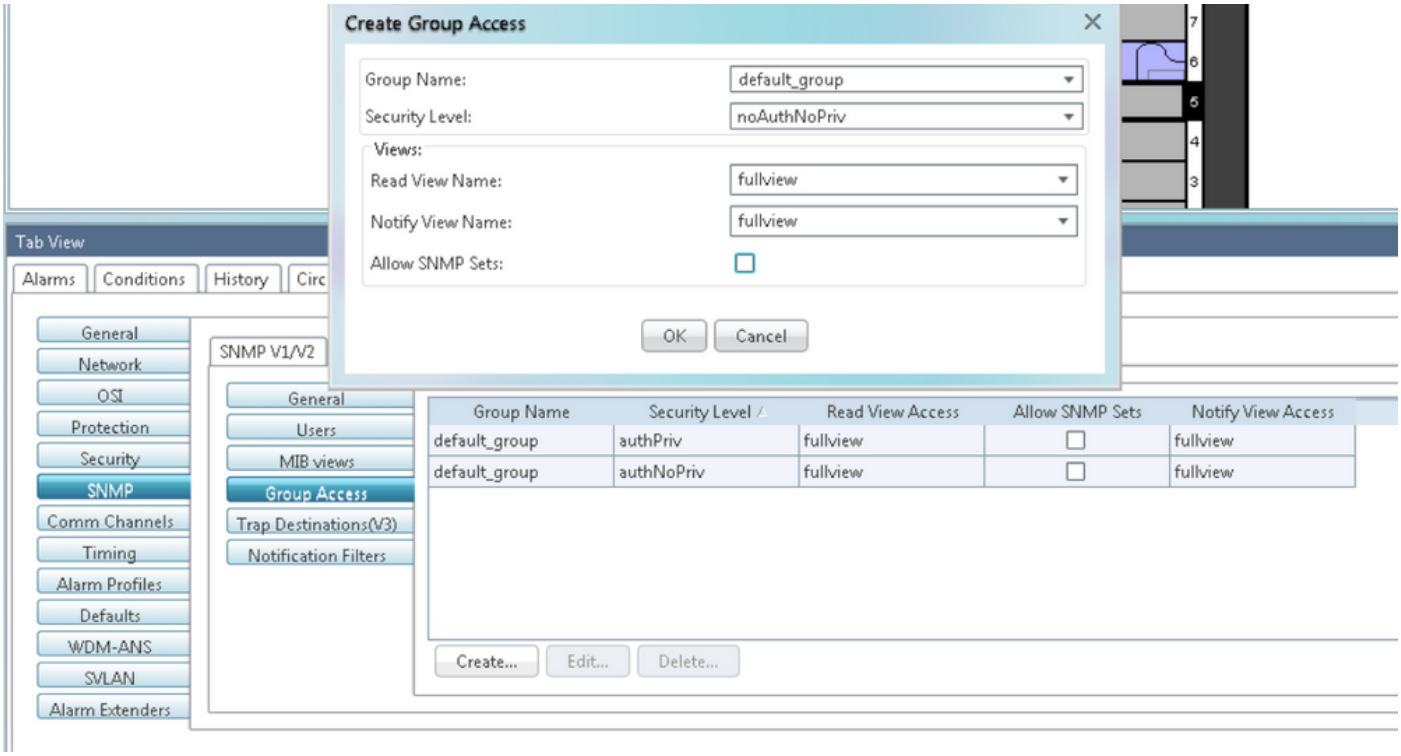
步驟2.導覽至**Node View > Provisioning > SNMP > SNMP V3 > Users > Create User** and Configure，如下圖所示。



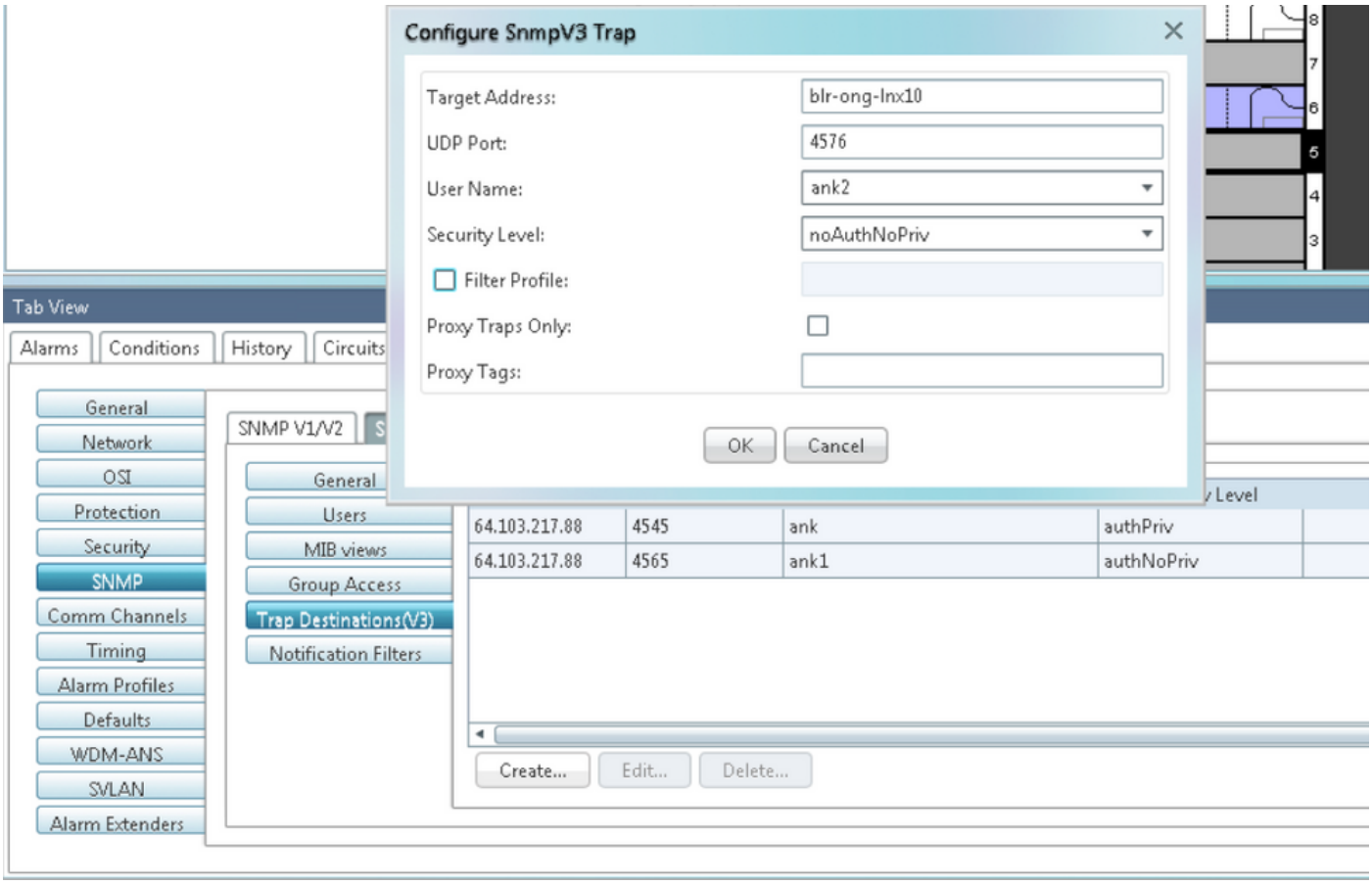
步驟3.確保**MIB視**圖配置如圖所示。



步驟4.配置Group Access（如圖所示）為noauthnopriv模式。



步驟5.導覽至Node View > Provisioning > SNMP > SNMP V3 > Trap Destination(V3)。 按一下「Create」和「Configure」，如下圖所示。



驗證noAuthNoPriv模式

步驟1.導航到NMS伺服器並執行snmpwalk。

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

範例：

```
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陷阱：

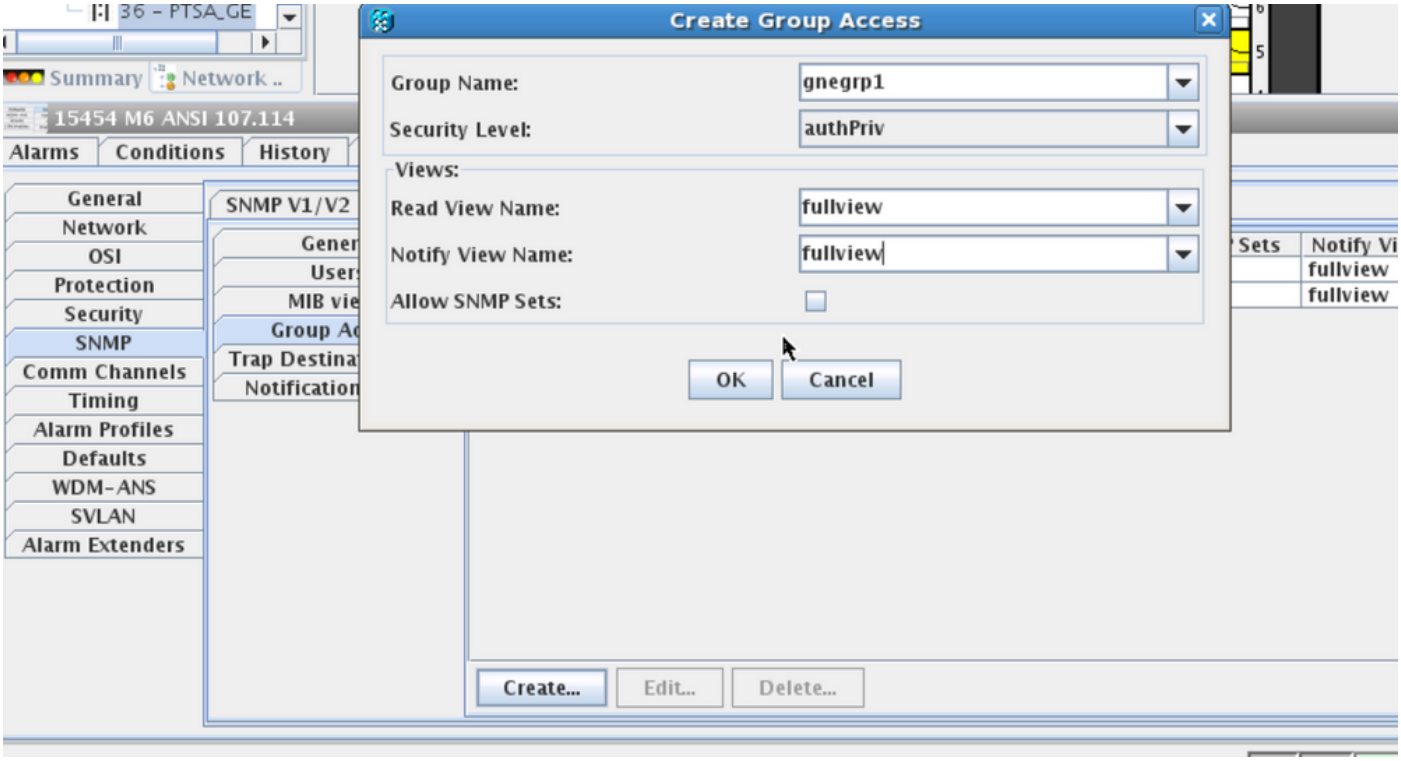
```
snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n" <port number>
```

所有版本的陷阱命令都相同。

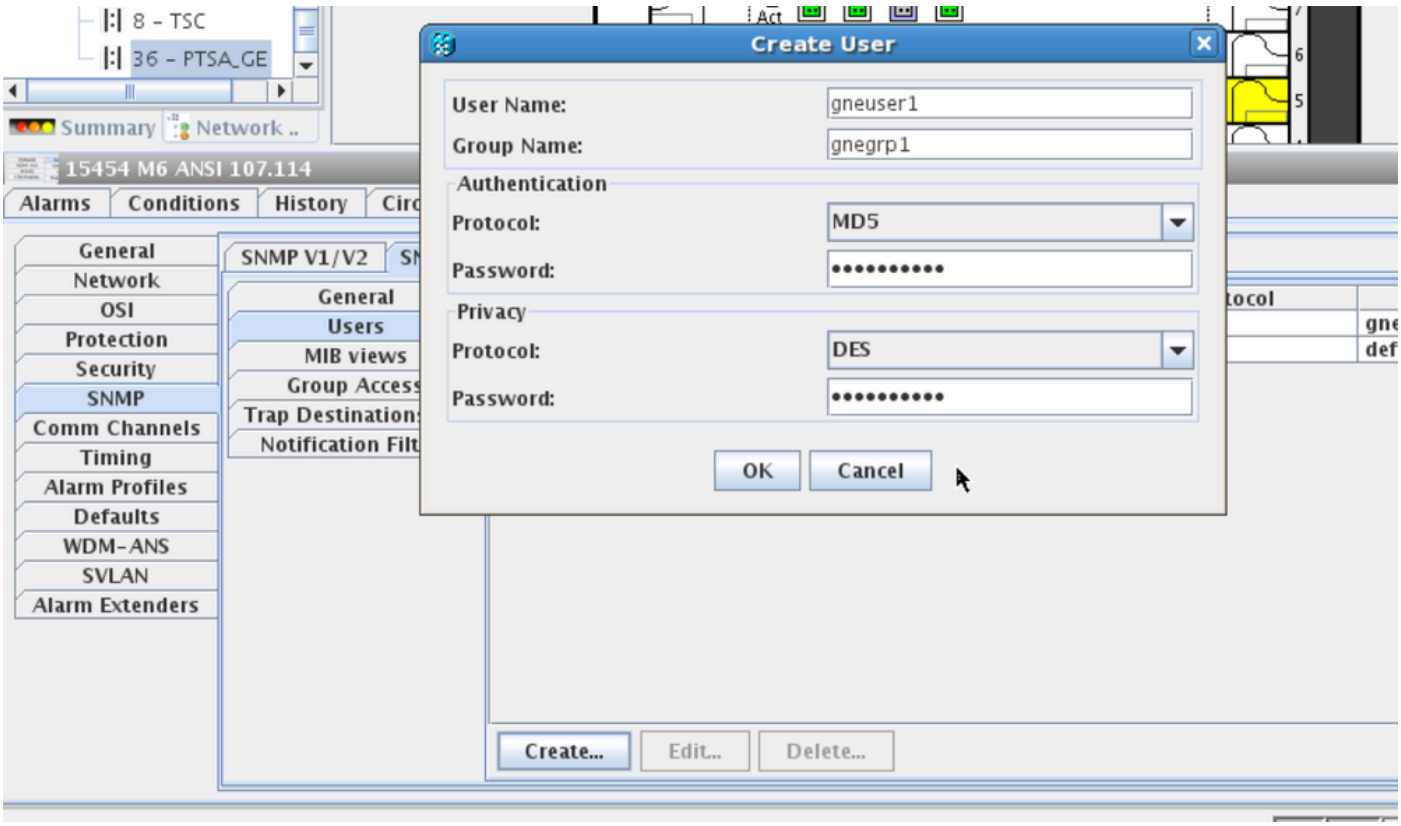
適用於GNE/ENE設定的SNMP V3陷阱

在GNE節點上

步驟1.導航至 Provisioning > SNMP > SNMP V3和C建立組訪問（「組訪問」頁籤）：提供具有安全級別(noAuthnoPriv|AuthnoPriv|authPriv)的組名稱以及完整檢視「讀取」和「通知」訪問許可權，如下圖所示。



步驟2. 建立使用者訪問許可權（「使用者」頁籤）：建立組名與先前在「組訪問」(Group Access)頁籤中建立的組名相同的使用者。此外，還提供基於訪問級別的身份驗證，如下圖所示。



步驟3.陷阱目標(V3)頁籤：

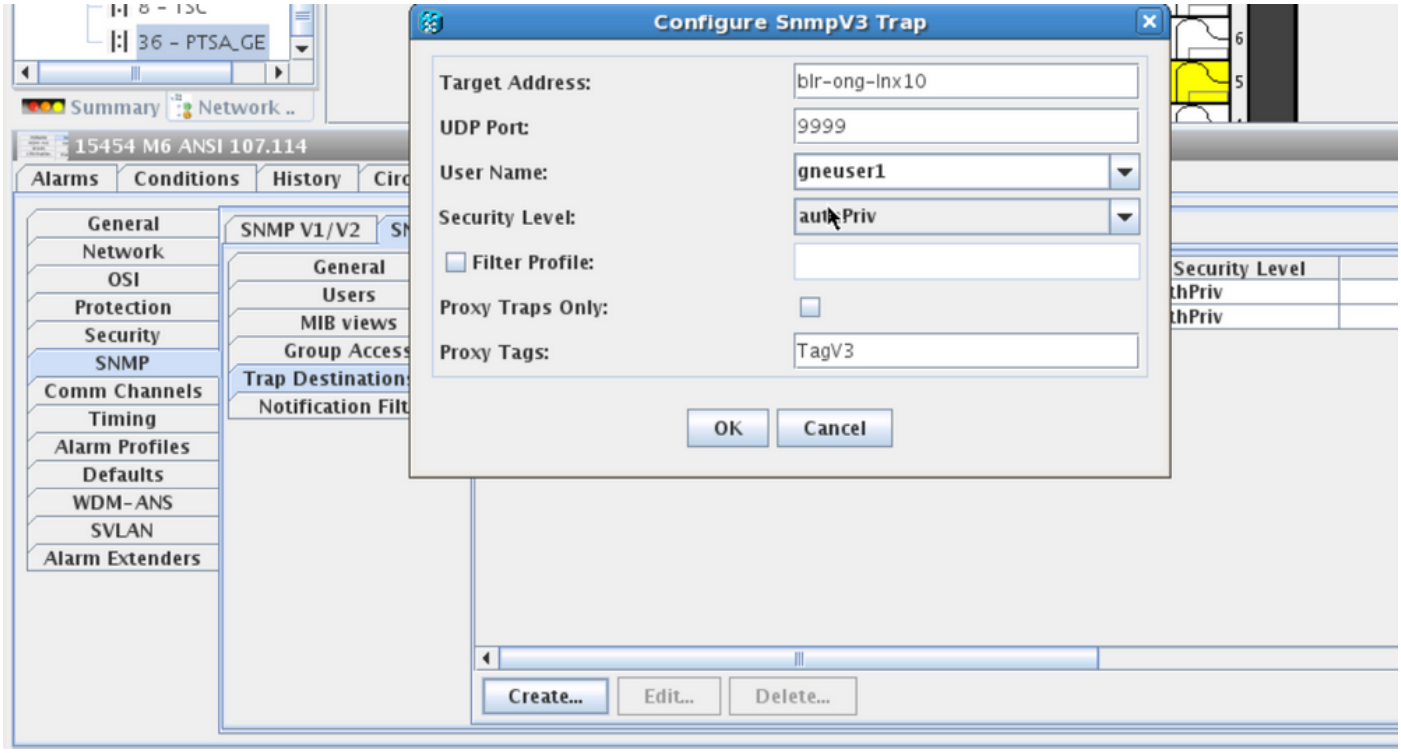
目標地址：運行陷阱的NMS伺服器的地址(例如Blr-ong-lnx10)。

UDP埠：將偵聽陷阱的任何埠號（例如9977）。

使用者名稱：使用者頁籤中的使用者名稱稱。

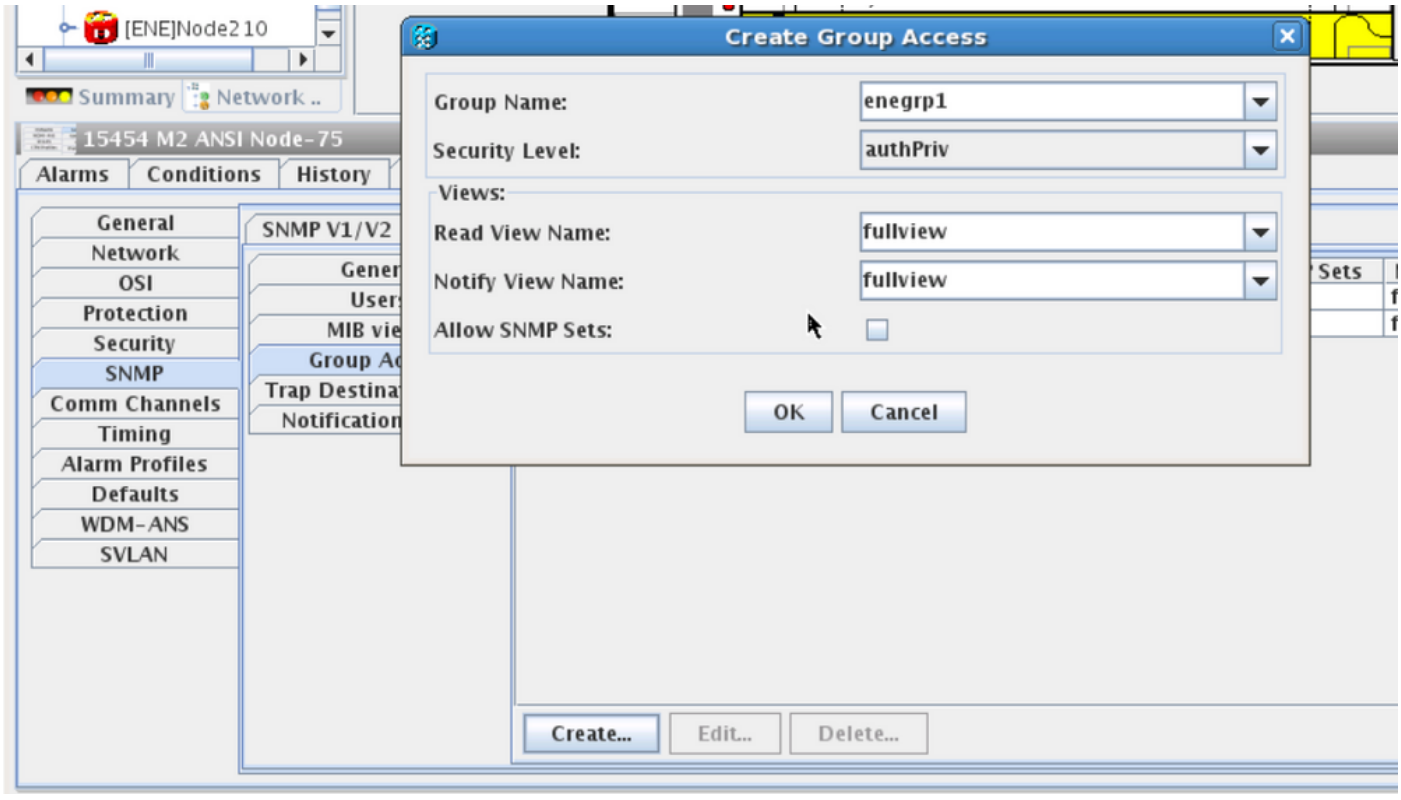
安全級別：如之前在「使用者」頁籤中配置。

代理標籤：提供代理標籤(例如標籤(75)。



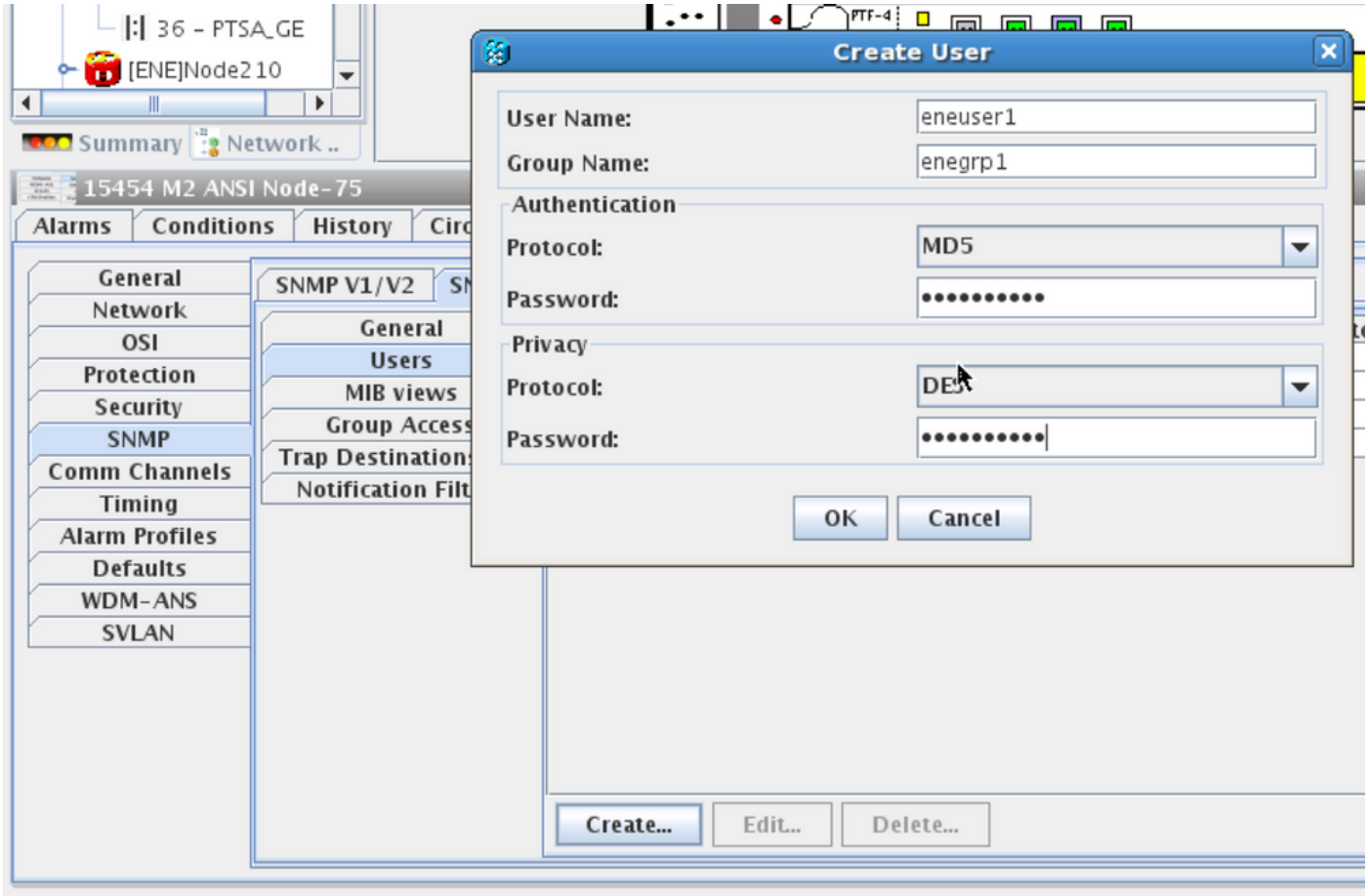
在ENE節點上

步驟1.導航到**Provisioning > SNMP > SNMP V3**和**Create Group Access**（Group Access頁籤）：提供具有訪問級別(noAuthnoPriv|AuthnoPriv|authPriv)的組名稱，並完整檢視「讀取」和「通知」訪問許可權，如下圖所示。



步驟2. 建立使用者訪問許可權（「使用者」頁籤）：建立組名與先前在「組訪問」(Group

Access)頁籤中建立的組名相同的使用者。此外，還提供基於訪問級別的身份驗證。



確保default_group（如果顯示在「使用者」頁籤中）在「組訪問」頁籤中建立，以防在「組訪問」頁籤中缺少它。

步驟3.陷阱目標(V3)頁籤：

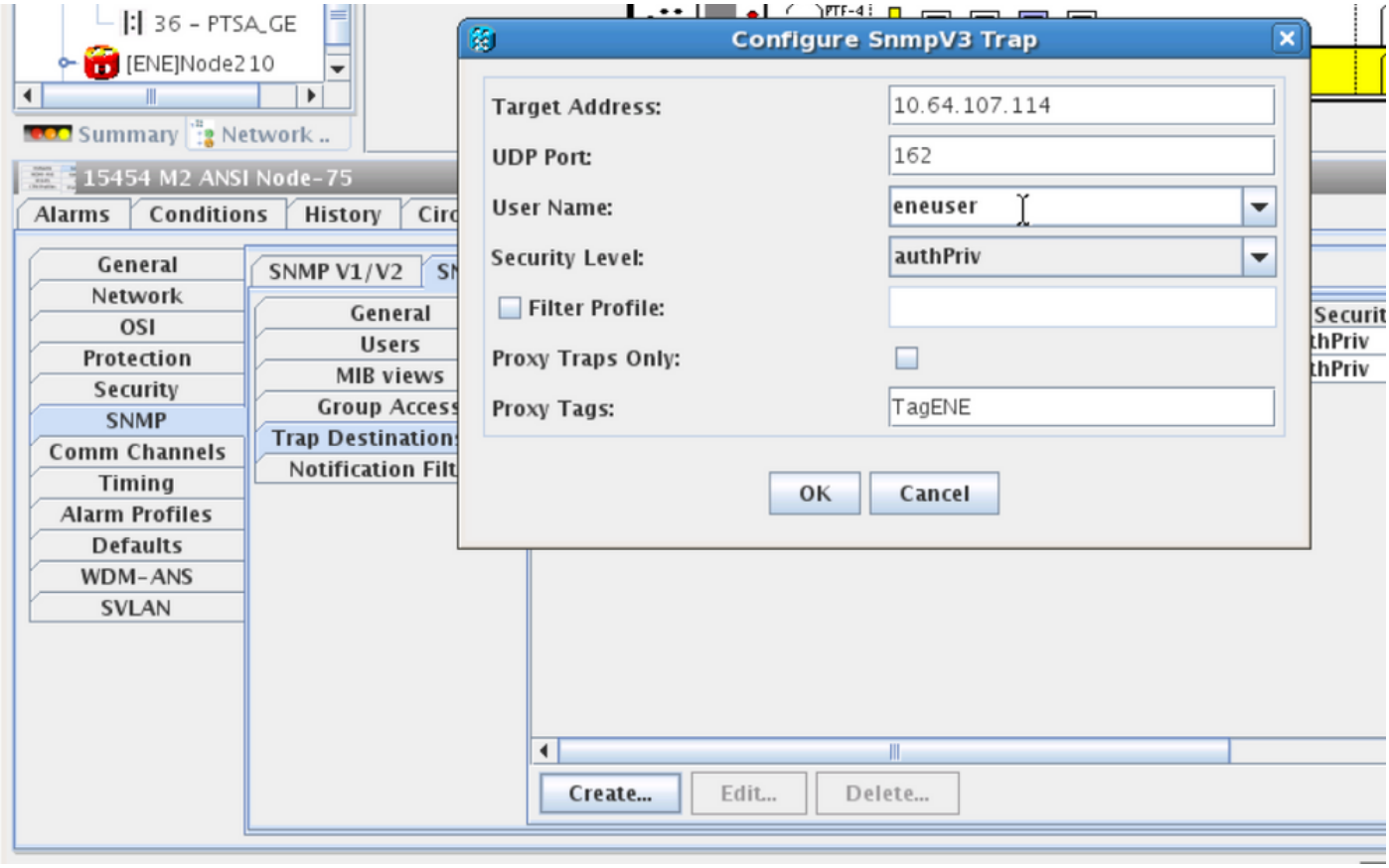
目標地址：GNE節點IP。

UDP埠：162.

使用者名稱：使用者頁籤中的使用者名稱稱。

安全級別：如之前在「使用者」頁籤中配置。

代理標籤：提供與GNE相同的代理標籤(例如標籤(75)。



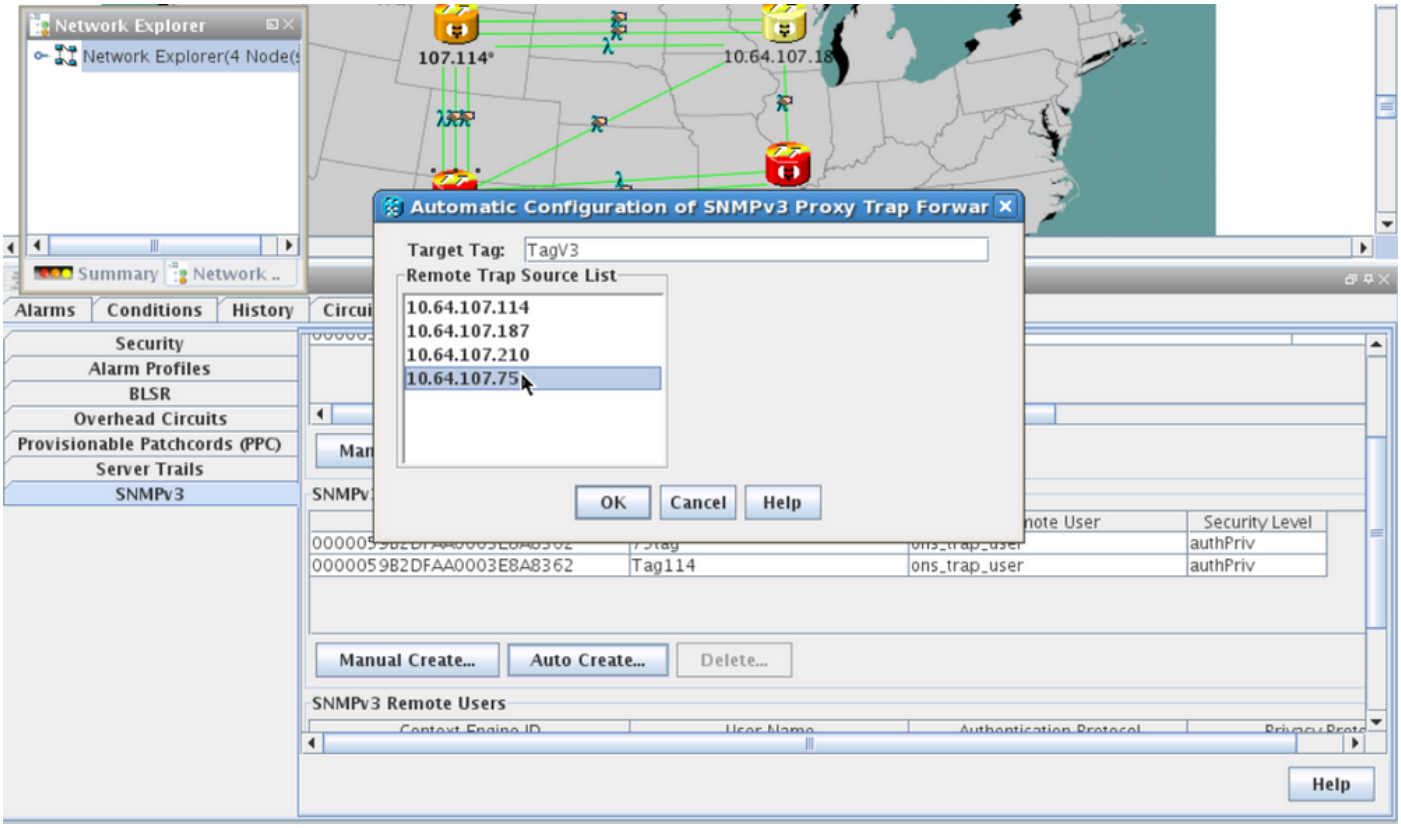
在CTC中，導航到網路檢視：

步驟1.導覽至**SNMPv3選**項卡。

步驟2. SNMPv3代理陷阱轉發器表：您可以執行**手動**或**自動建立**。

選擇**自動建立**。根據這一點：

- 目標標籤：在GNE中設定代理標籤。
- 遠端陷阱源清單：選擇ENE節點IP，如下圖所示。



驗證GNE/ENE設定

配置NMS伺服器(blr-long-lnx10):

步驟1.在伺服器的主目錄中，建立一個目錄並將其命**名為snmp**。

步驟2. 在此目錄下，建立檔案**snmptrapd.conf**。

步驟3. 在**snmptrapd.conf**中，建立以下設定：

```
createUser -e 0x
                                Engine_NO = can be available from CTC. Open GNE node-->Node view-
>Provisioning->SNMP->SNMP V3-->General.
```

SNMP陷阱：

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

ene上的snmpwalk:

對於authpriv模式：

```
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>
```

對於authnopriv模式：

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

對於noauthnopriv模式：

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

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。