在Cisco ONS15454/NCS2000设备上配置SNMPv3

目录

简介

本文档介绍如何在ONS15454/NCS2000设备上配置简单网络管理协议第3版(SNMPv3)的分步说明。所有主题都包括示例。

> **注意**：本文档中提供的属性列表并非详尽或权威，在不更新本文档的情况下随时可能更改。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科传输控制器(CTC)GUI
- 基本服务器知识
- 基本Linux/Unix命令

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

在独立/多机架节点上

在ONS15454/NCS2000设备上配置authPriv模式

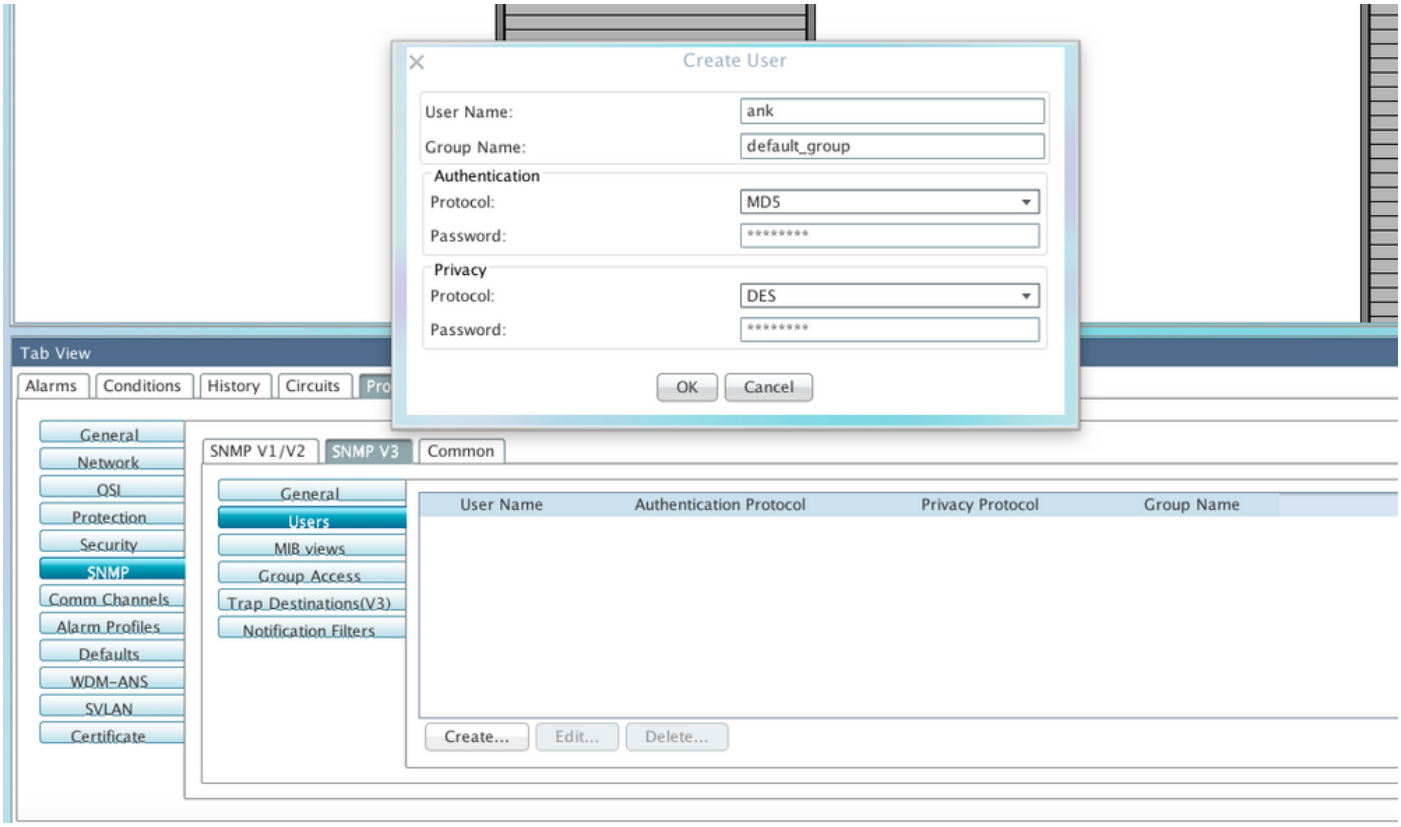
步骤1.使用超级用户凭证通过CTC登录节点。

步骤2.导航至“节**点”视图>“调配”>“SNMP”>“SNMP V3**”。

步骤3.导航至“用户”**选项**卡。创建用户。

```
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>
```

步骤4.单击“**确定”**，如图所示。



规格：

用户名 — 指定连接到代理的主机上的用户名。用户名必须至少为6个字符，最多为40个字符（TACACS和RADIUS身份验证最多只有39个字符）。 它包含字母数字(a-z、A-Z、0-9)字符，允许的特殊字符为@、"-"（连字符）和""。 （点）。 为了与TL1兼容，用户名必须为6到10个字符。

组名 — 指定用户所属的组。

身份验证:

协议 — 选择要使用的身份验证算法。选项为NONE、MD5和SHA。

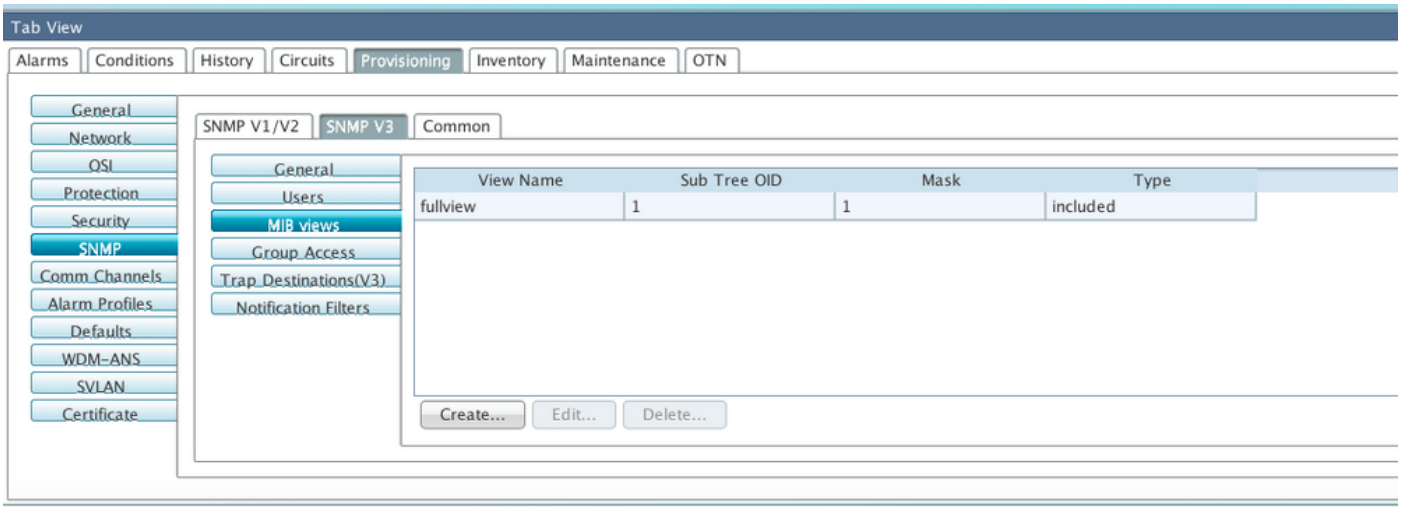
密码 — 如果选择MD5或SHA，请输入密码。默认情况下，密码长度设置为至少八个字符。

隐私 — 启动隐私身份验证级别设置会话，使主机能够加密发送到代理的消息的内容。

协议 — 选择隐私身份验证算法。可用选项为None、DES和AES-256-CFB。

密码 — 如果选择协议(None)以外的协议，请输入密码。

步骤5.确保根据此映像配置MIB视图。



规格：

名称 — 视图的名称。

子树OID - MIB子树，与掩码结合时定义子树系列。

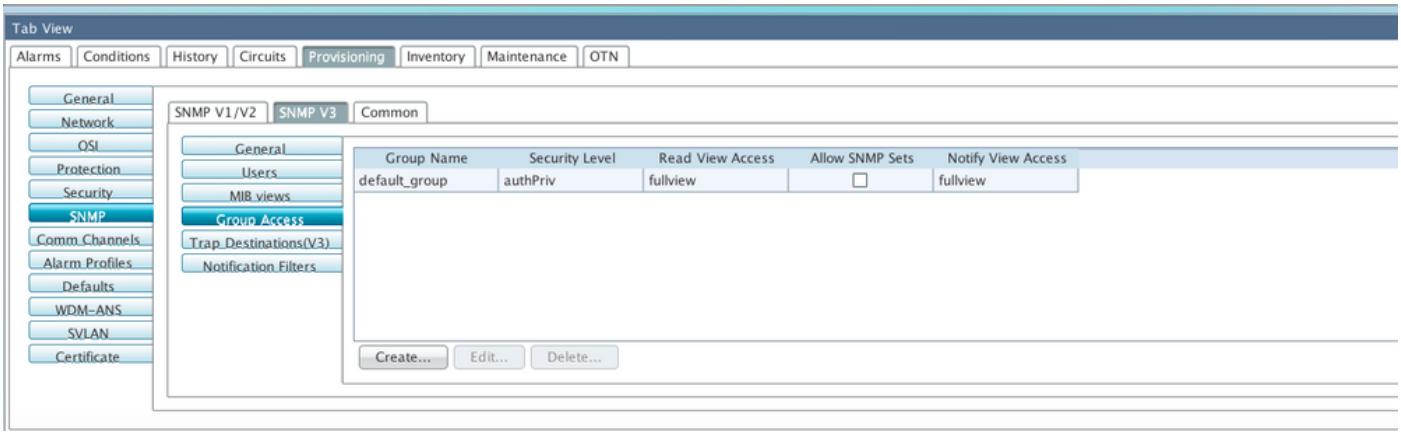
位掩码 — 一系列视图子树。位掩码中的每个位对应于子树OID的子标识符。

类型 — 选择视图类型。选项包括和排除。

该类型定义子树OID和位掩码组合定义的子树系列是否包含在通知过滤器中或从通知过滤器中排除。

步骤6.配置组访问，如图所示。默认情况下，组名称将默认组和安全级别为authPriv。

注意：组名应与在步骤3中创建用户时使用的组名相同。



规格：

组名 — SNMP组的名称或共享通用访问策略的用户集合。

安全级别 — 为其定义访问参数的安全级别。从以下选项中选择：

noAuthNoPriv — 使用用户名匹配进行身份验证。

AuthNoPriv — 根据HMAC-MD5或HMAC-SHA算法提供身份验证。

AuthPriv — 根据HMAC-MD5或HMAC-SHA算法提供身份验证。除身份验证外，还根据CBC-DES(DES-56)标准提供DES 56位加密。

如果为组选择authNoPriv或authPriv，则必须为相应用户配置身份验证协议和密码、隐私协议和密码或两者。

视图

读取视图名称 — 读取组的视图名称。

通知视图名称 — 通知组的视图名称。

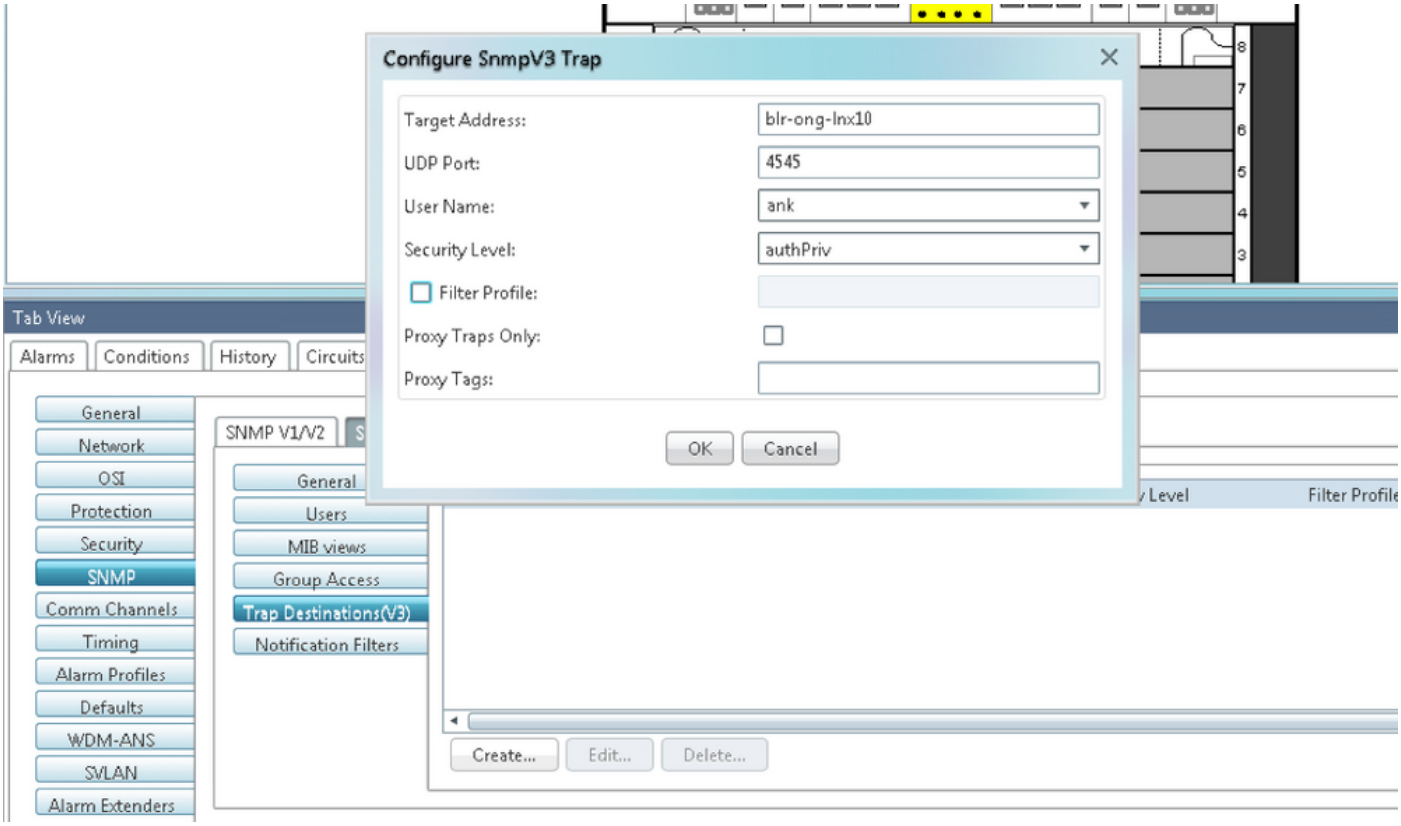
允许SNMP集 — 如果希望SNMP代理接受SNMP SET请求，请选中此复选框。如果未选中此复选框，则SET请求将被拒绝。

注意： SNMP SET请求访问针对极少数对象实施。

步骤7.导航至**Node View > Provisioning > SNMP > SNMP V3 > Trap Destination(V3)**。 单击“**创建并配置**”。

```
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
```

步骤8.单击“**确定**”，如图所示。



注意：blr-ong-lnx10是NMS服务器。

规格：

目标地址 — 陷阱应发送到的目标。使用IPv4或IPv6地址。

UDP端口 — 主机使用的UDP端口号。默认值为 162。

用户名 — 指定连接到代理的主机上的用户名。

安全级别 — 选择以下选项之一：

noAuthNoPriv — 使用用户名匹配进行身份验证。

AuthNoPriv — 根据HMAC-MD5或HMAC-SHA算法提供身份验证。

AuthPriv — 根据HMAC-MD5或HMAC-SHA算法提供身份验证。除身份验证外，还根据CBC-DES(DES-56)标准提供DES 56位加密。

过滤器配置文件 — 选中此复选框并输入过滤器配置文件名称。仅当您提供过滤器配置文件名称并创建通知过滤器时，才会发送陷阱。

仅代理陷阱(Proxy Traps Only) — 如果选中，则仅从ENE转发代理陷阱。来自此节点的陷阱不会发送到此条目标识的陷阱目标。

代理标记 — 指定标记列表。仅当ENE需要将陷阱发送到此条目标识的陷阱目标并希望将GNE用作代理时，才需要在GNE上使用标记列表。

配置NMS服务器(blr-ong-lnx10)

步骤1.在服务器的主目录中，创建名为snmp的**目录**。

第二步： 在此目录下，创建文**件snmptrapd.conf**。

步骤3.将snmptrapd.conf**文件更**改为：

```
vi snmptrapd.conf

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

例如：

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

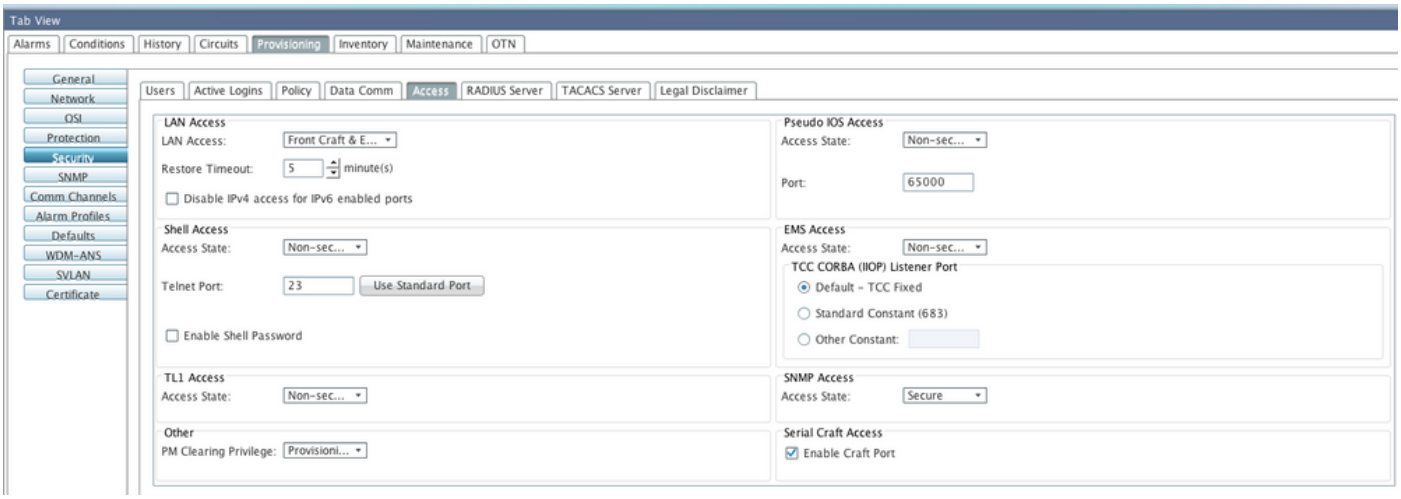
在本例中：

```
user_name=ank

MD5 password = cisco123

DES password  = cisco123

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

Node view > Provisioning > SNMP > SNMP V3 > General

验证authPriv模式

步骤1.在CTC中，导航至**Node View > Provisioning > Security > Access > Change snmp access state to Secure**，如图所示。



步骤2.导航到NMS服务器并执行snmpwalk。

语法:

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

示例：

```
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
```

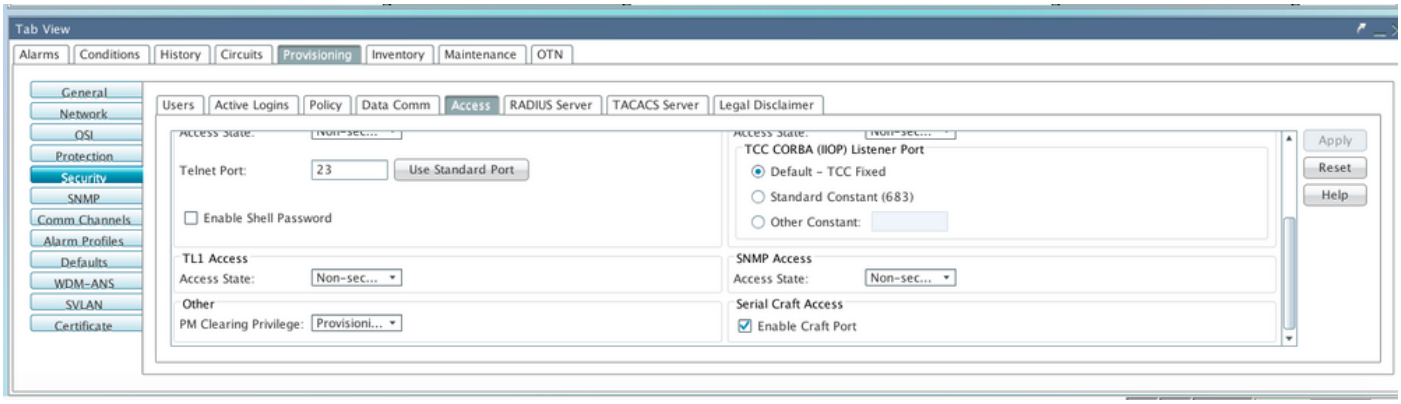
SNMP 陷阱:

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

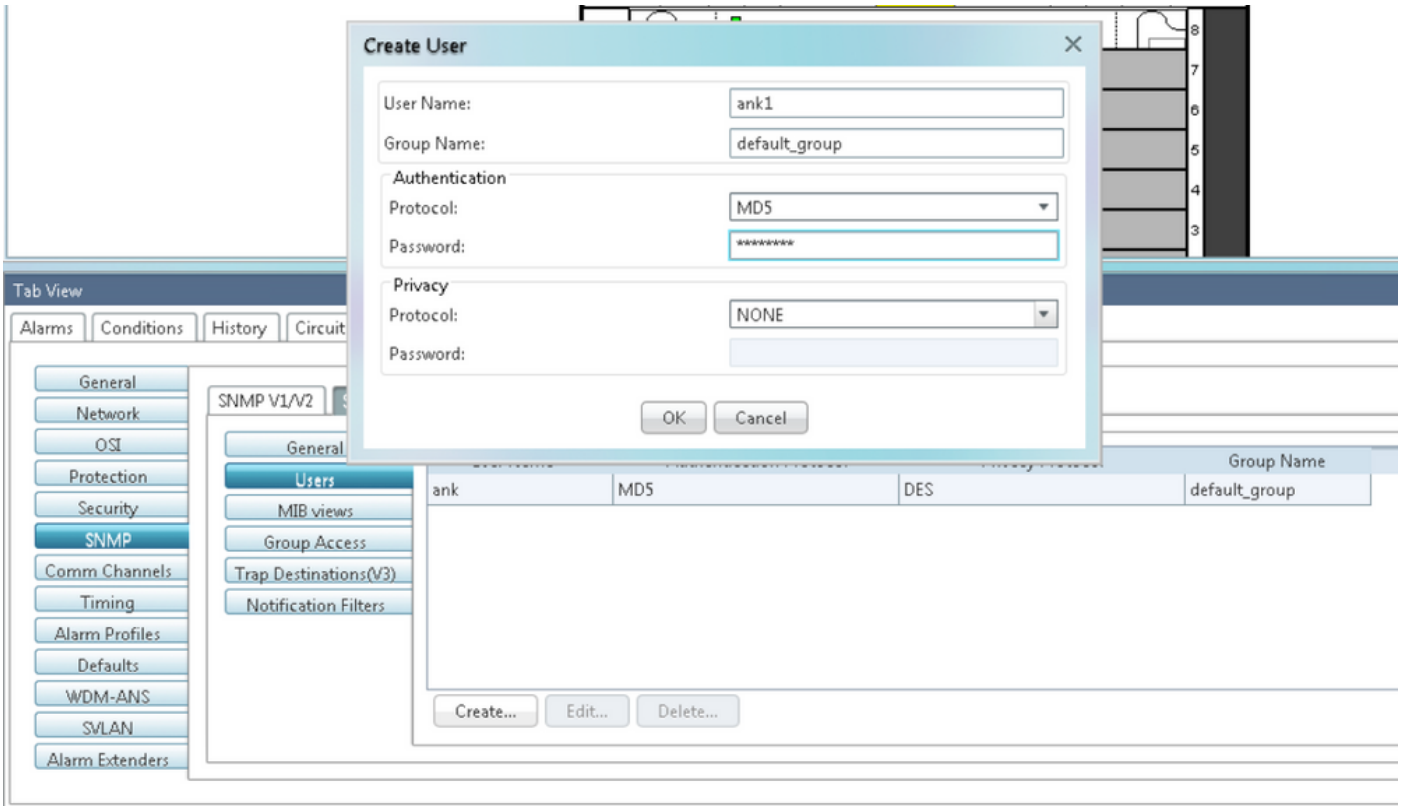
陷阱cmd对所有版本都相同。

在ONS15454/NCS2000设备上配置authNoPriv模式

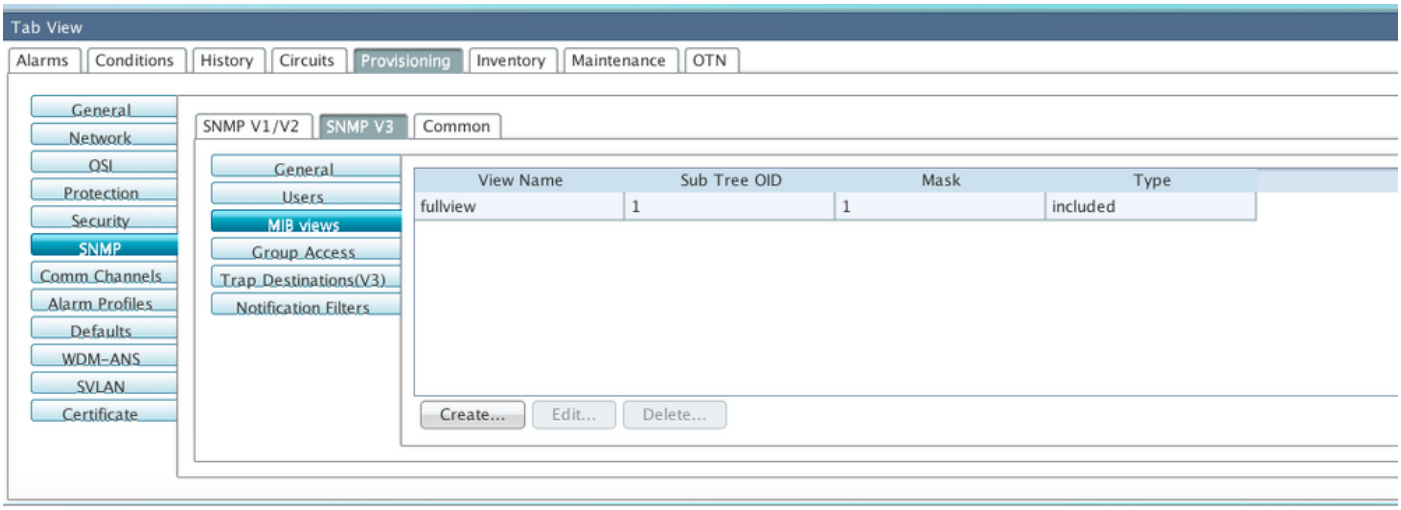
步骤1.在CTC中，导航至**Node View > Provisioning > Security > Access > Change snmp access state to Non-secure mode**，如图所示。



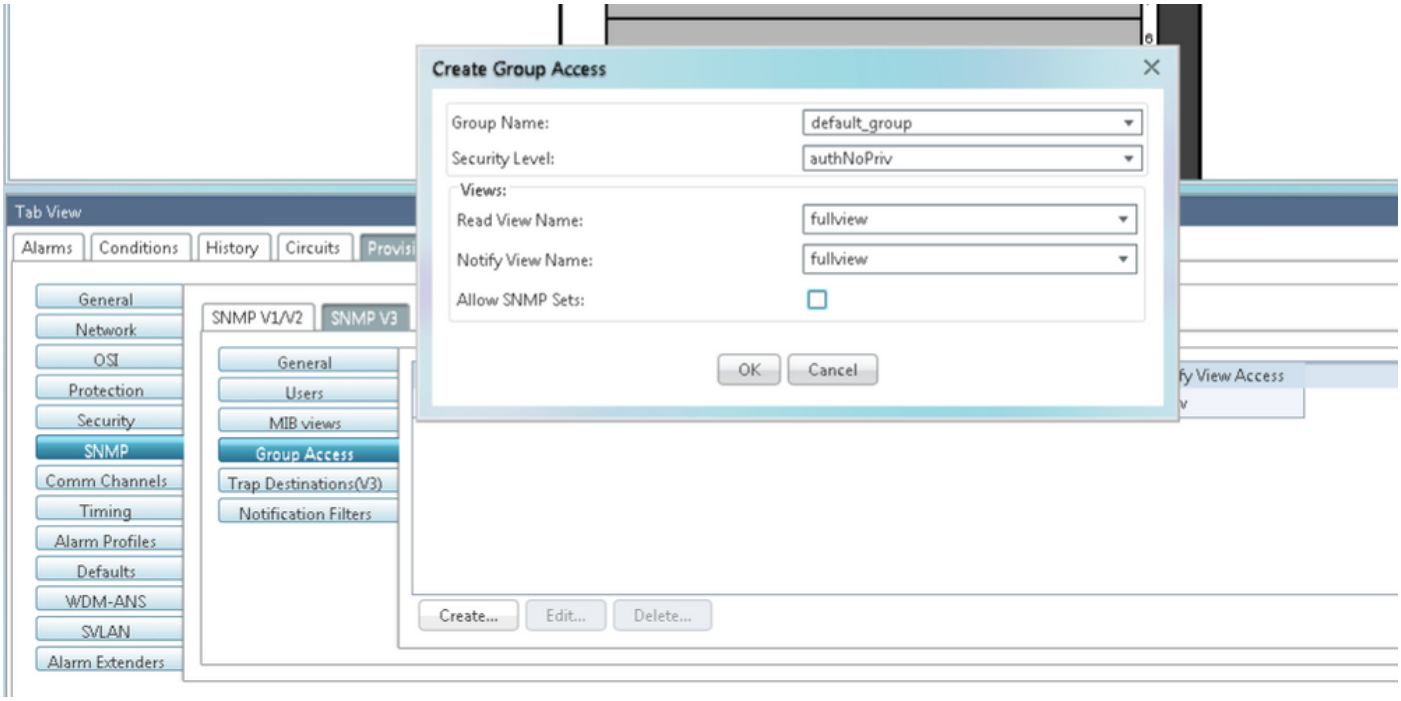
步骤2.导航至**Node View > Provisioning > SNMP > SNMP V3 > Users > Create User**，并按照图中所示进行配置。



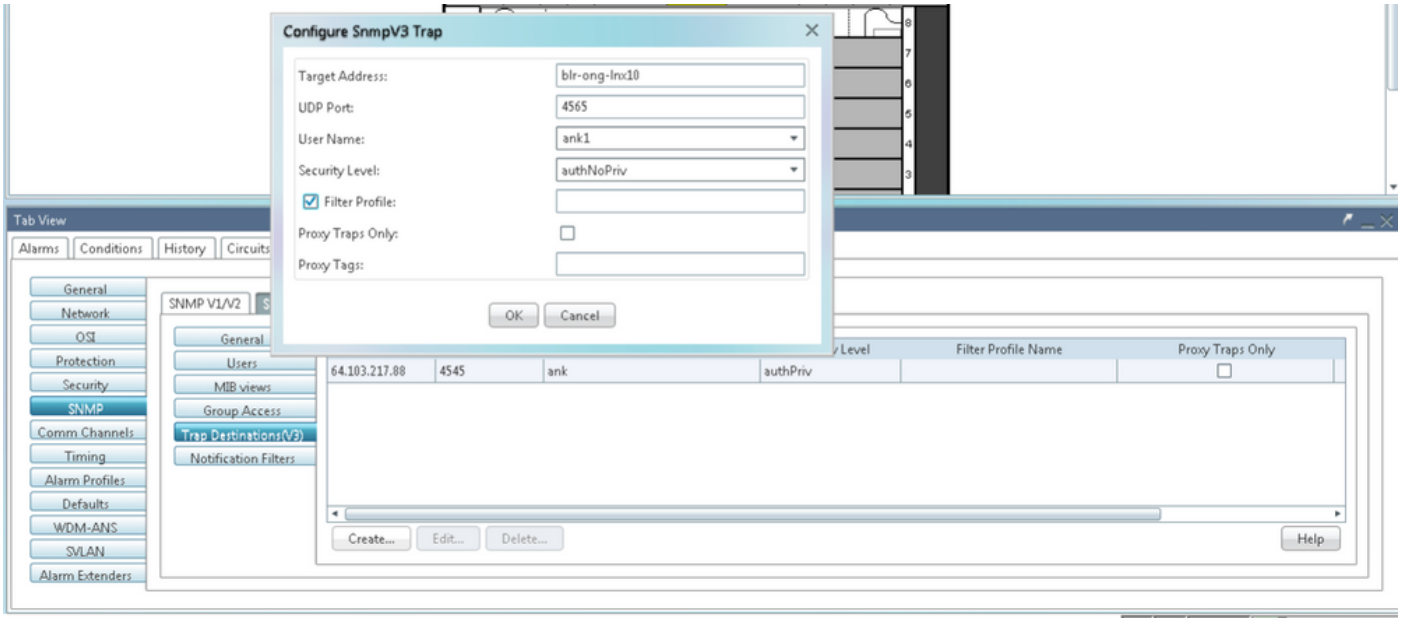
步骤3.确保MIB视图的配置如图所示。



步骤4.配置组访问（如图所示）以进行authnopriv模式。



步骤5.导航至**Node View > Provisioning > SNMP > SNMP V3 > Trap Destination(V3)。** 单击“**创建并配置**”，如图所示。



验证authNoPriv模式

步骤1.导航到NMS服务器并执行snmpwalk。

语法:

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

示例：

```
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
```

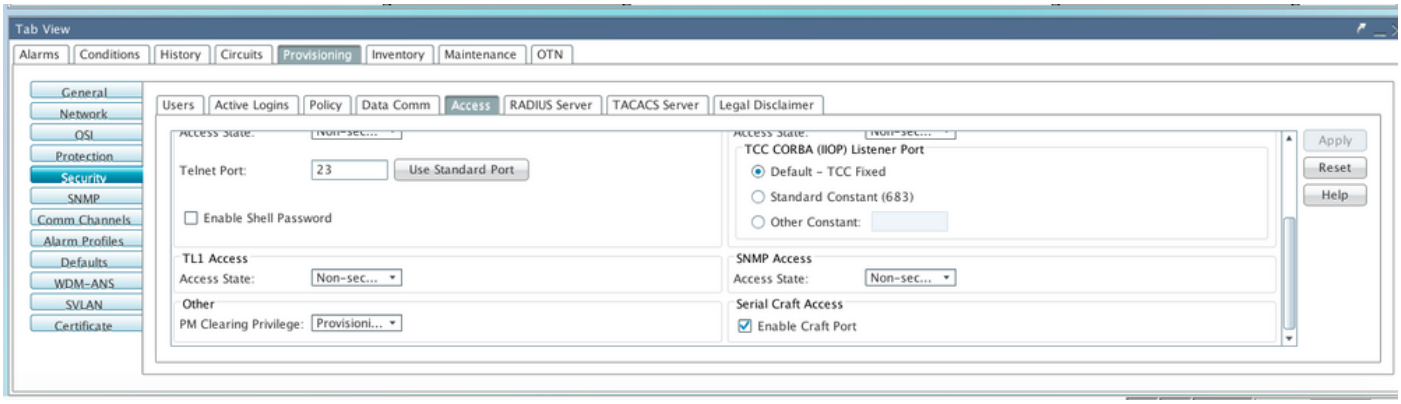
SNMP 陷阱:

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

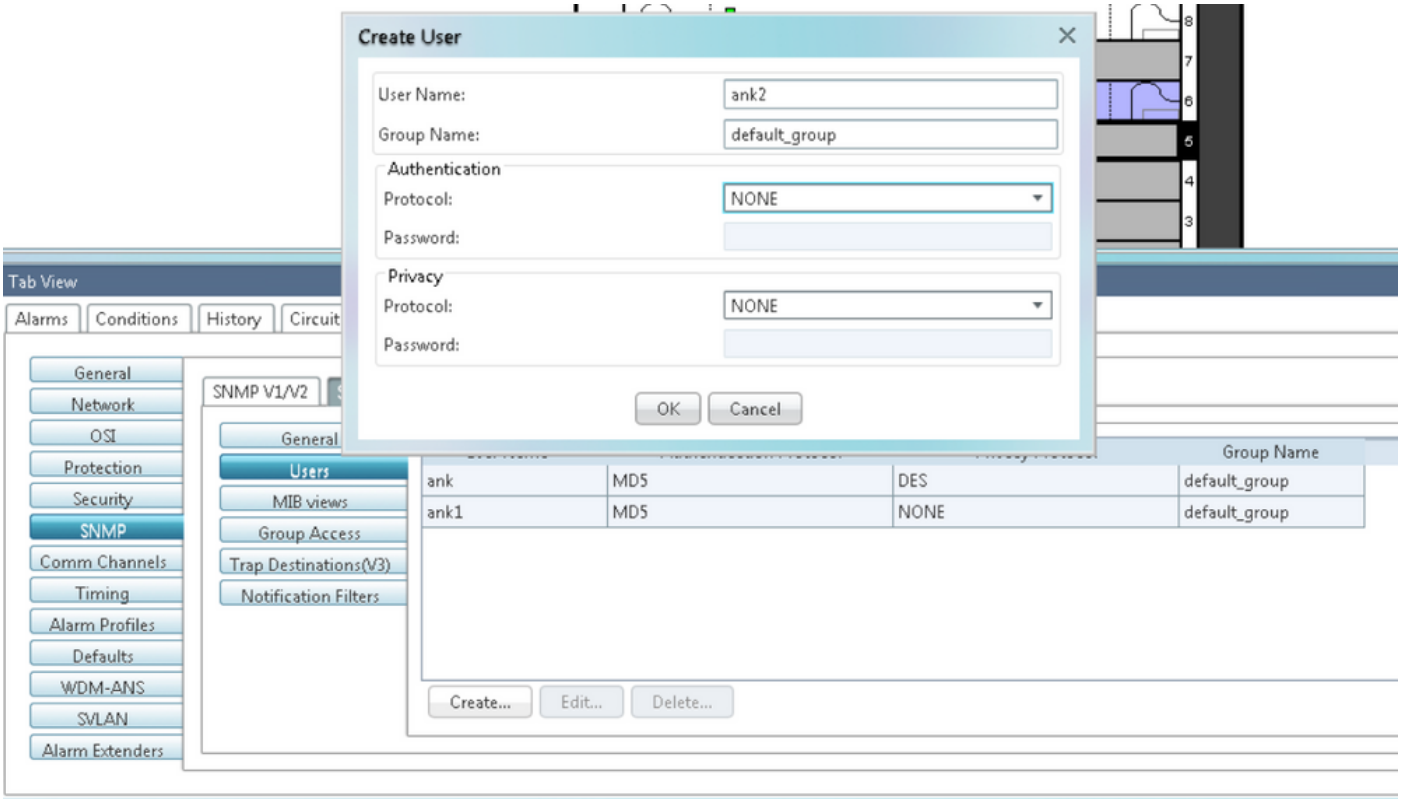
陷阱cmd对所有版本都相同。

在ONS15454/NCS2000设备上配置noAuthNoPriv模式

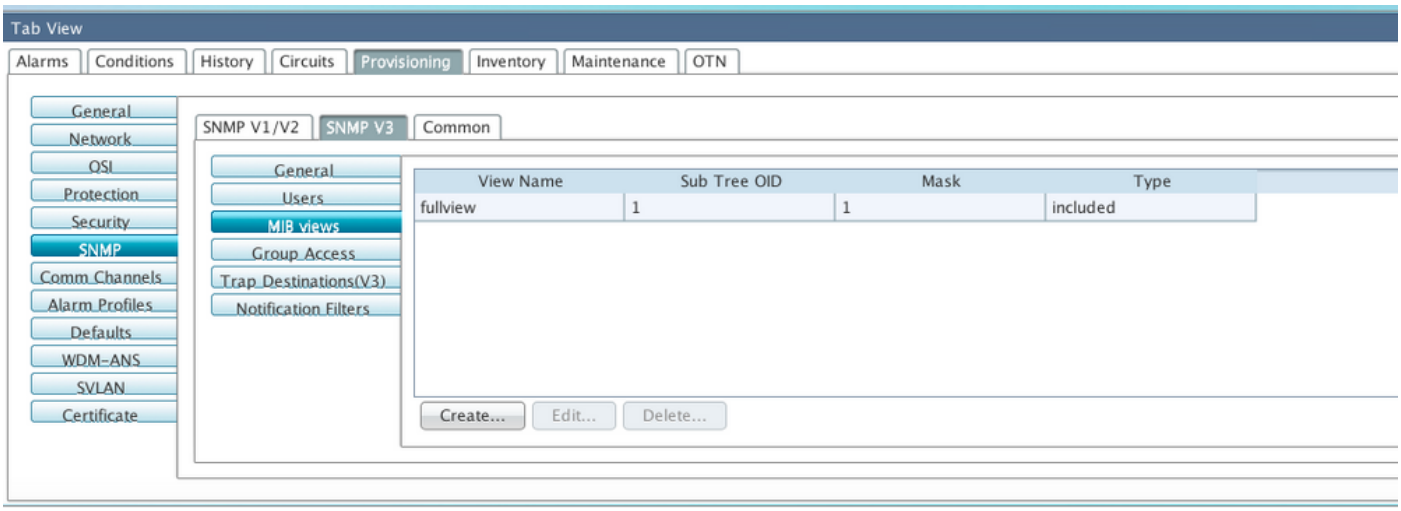
步骤1.在CTC中，导航至**Node View > Provisioning > Security > Access > Change snmp access state to Non-secure mode**，如图所示。



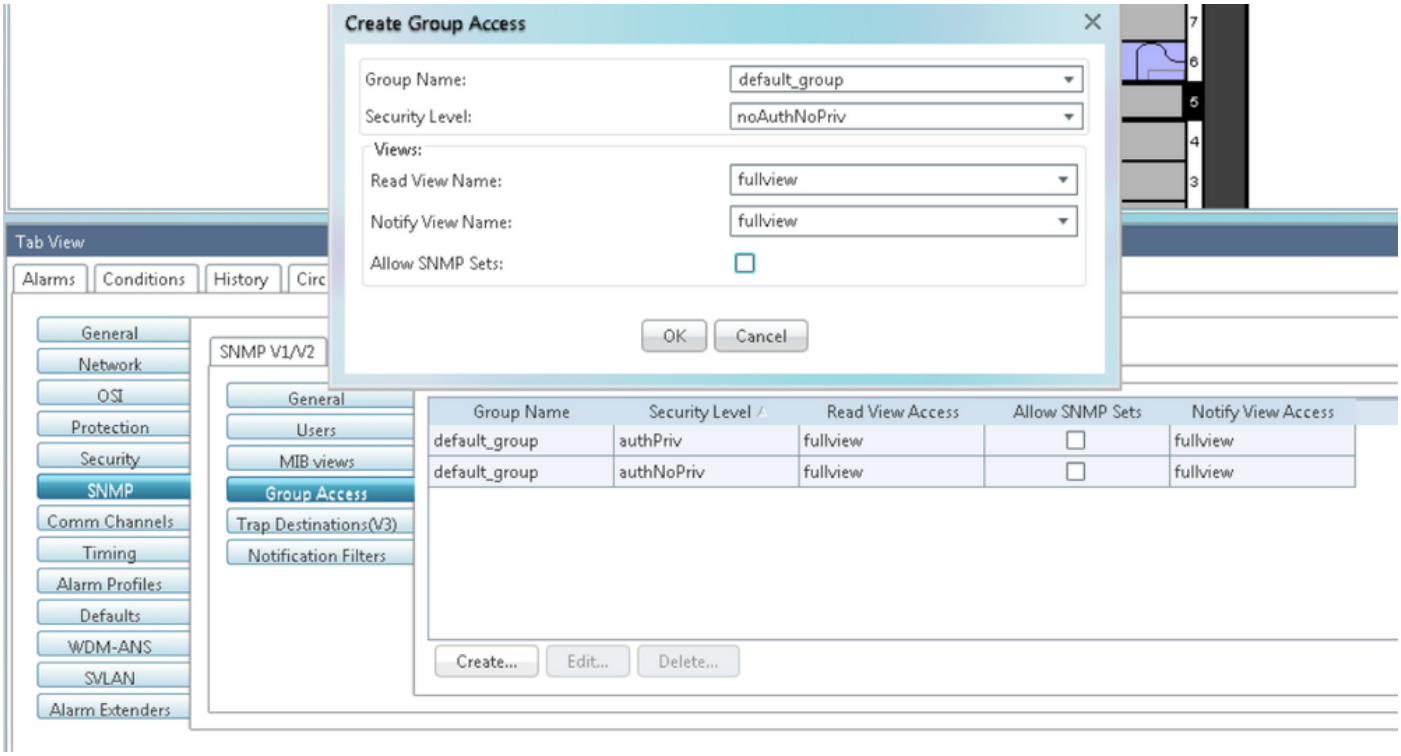
步骤2.导航至**Node View > Provisioning > SNMP > SNMP V3 > Users > Create User and Configure**，如图所示。



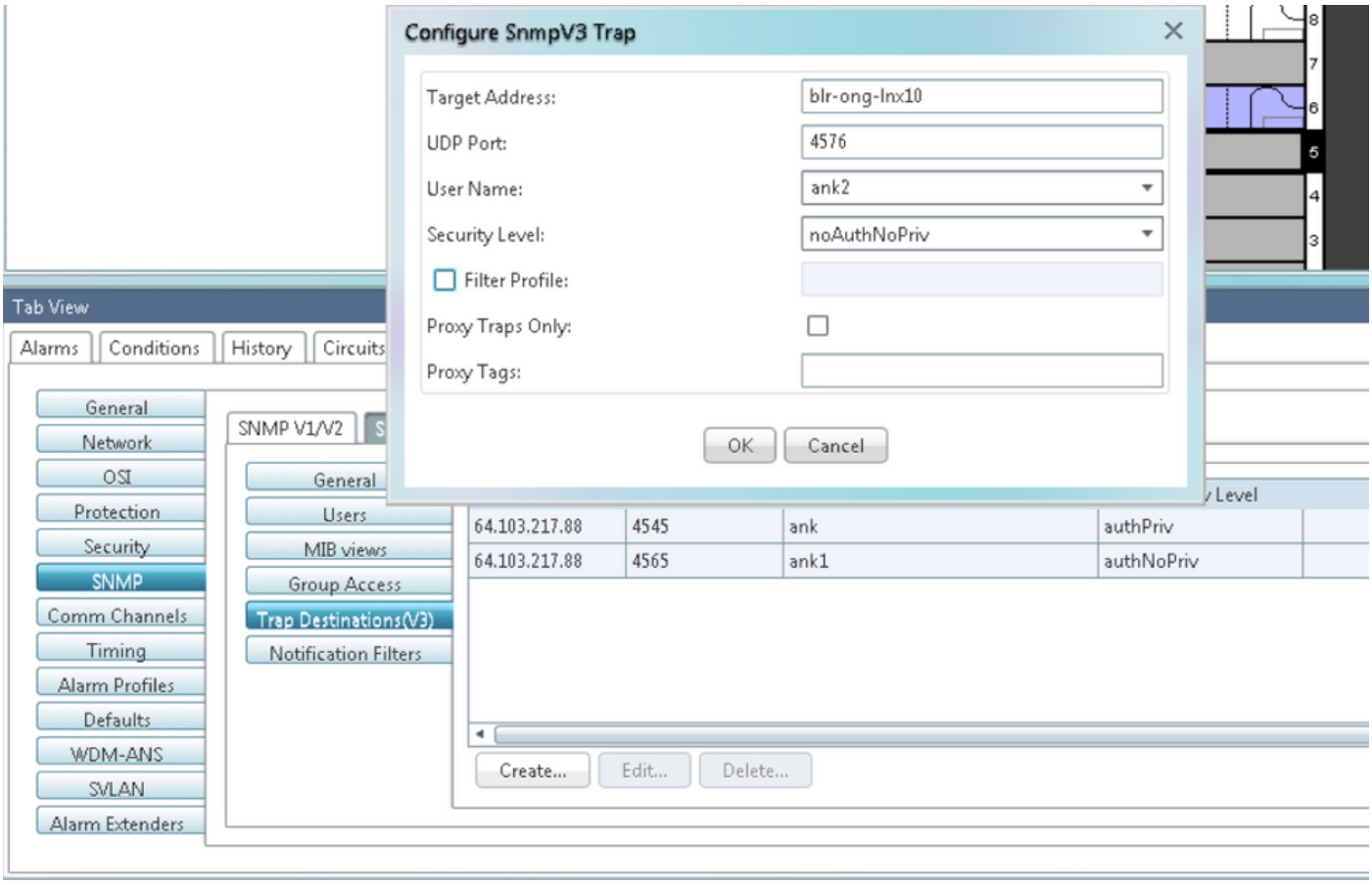
步骤3.确保MIB视图配置如图所示。



步骤4.配置组访问（如图所示），使其处于noauthnopriv模式。



步骤5.导航至**Node View > Provisioning > SNMP > SNMP V3 > Trap Destination(V3)**。 单击“**创建并配置**”，如图所示。



验证noAuthNoPriv模式

步骤1.导航至NMS服务器并执行snmpwalk。

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

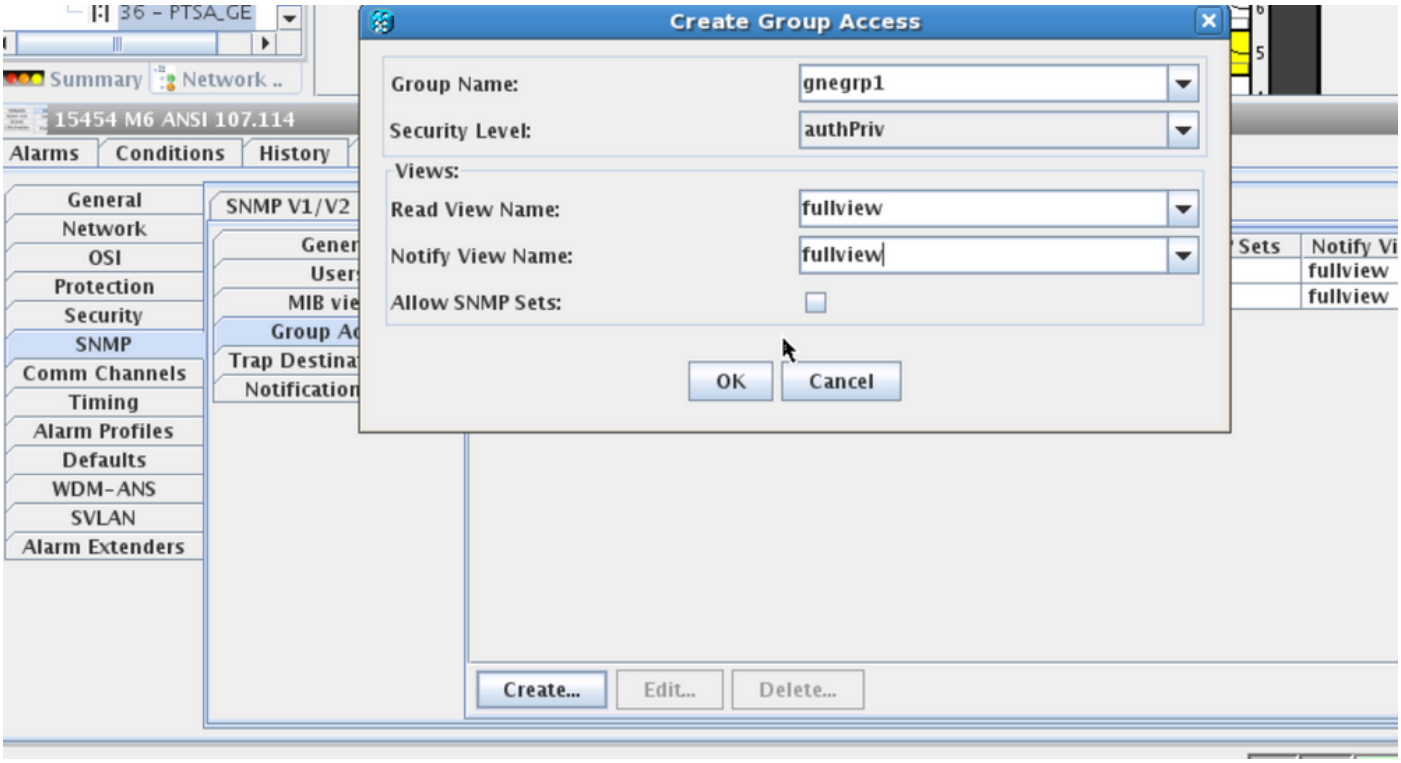
```
blr-ong-lnx10:155> snmpwalk -v 3 -l noauthnopriv -u ank2 10.64.106.40 system

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>
```
陷阱cmd对所有版本都相同。

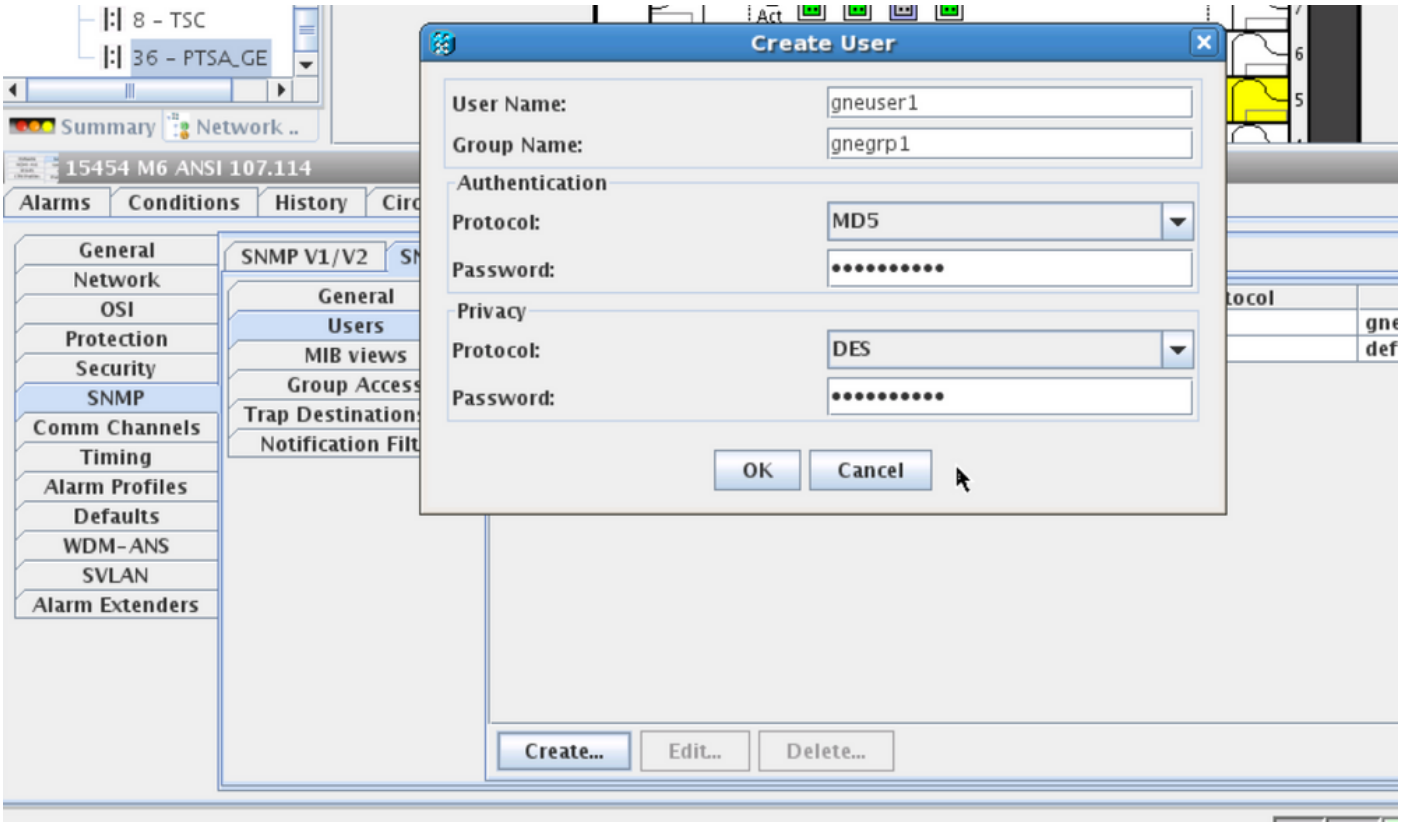
用于GNE/ENE设置的SNMP V3陷阱

在GNE节点上

步骤1.导航至 调配> SNMP > SNMP V3和C创建组访问（“组访问”选项卡）：提供具有安全级别(noAuthnoPriv|AuthnoPriv|authPriv)和全视图读取和通知访问权限的组名，如图所示。



步骤2.创建用户访问权限（用户选项卡）：创建组名与之前在“组访问”选项卡中创建的组名相同的用户。此外，根据访问级别提供身份验证，如图所示。



步骤3.陷阱目标(V3)选项卡：

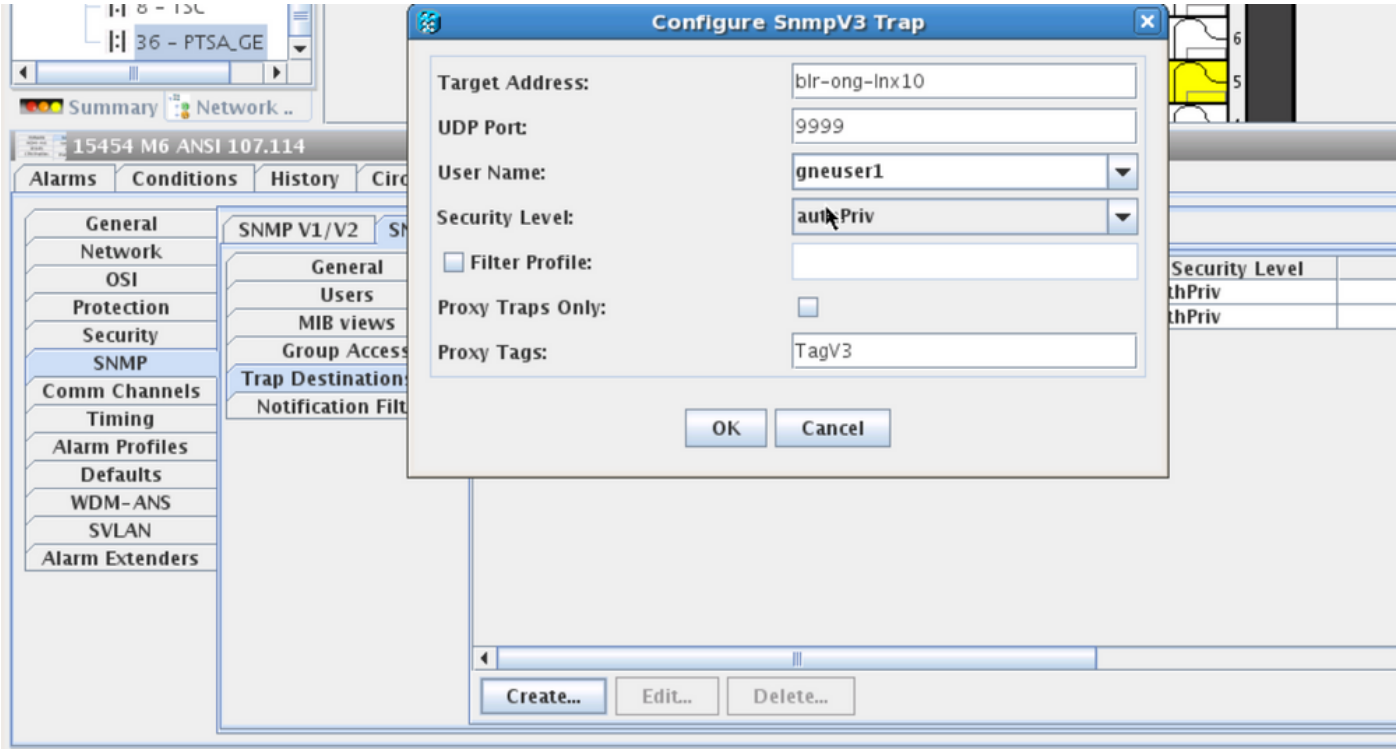
目标地址：将运行陷阱的NMS服务器的地址(例如Blr-ong-lnx10)。

UDP 端口:将侦听陷阱的任何端口号（例如9977）。

用户名：“用户”(User)选项卡中的用户名称。

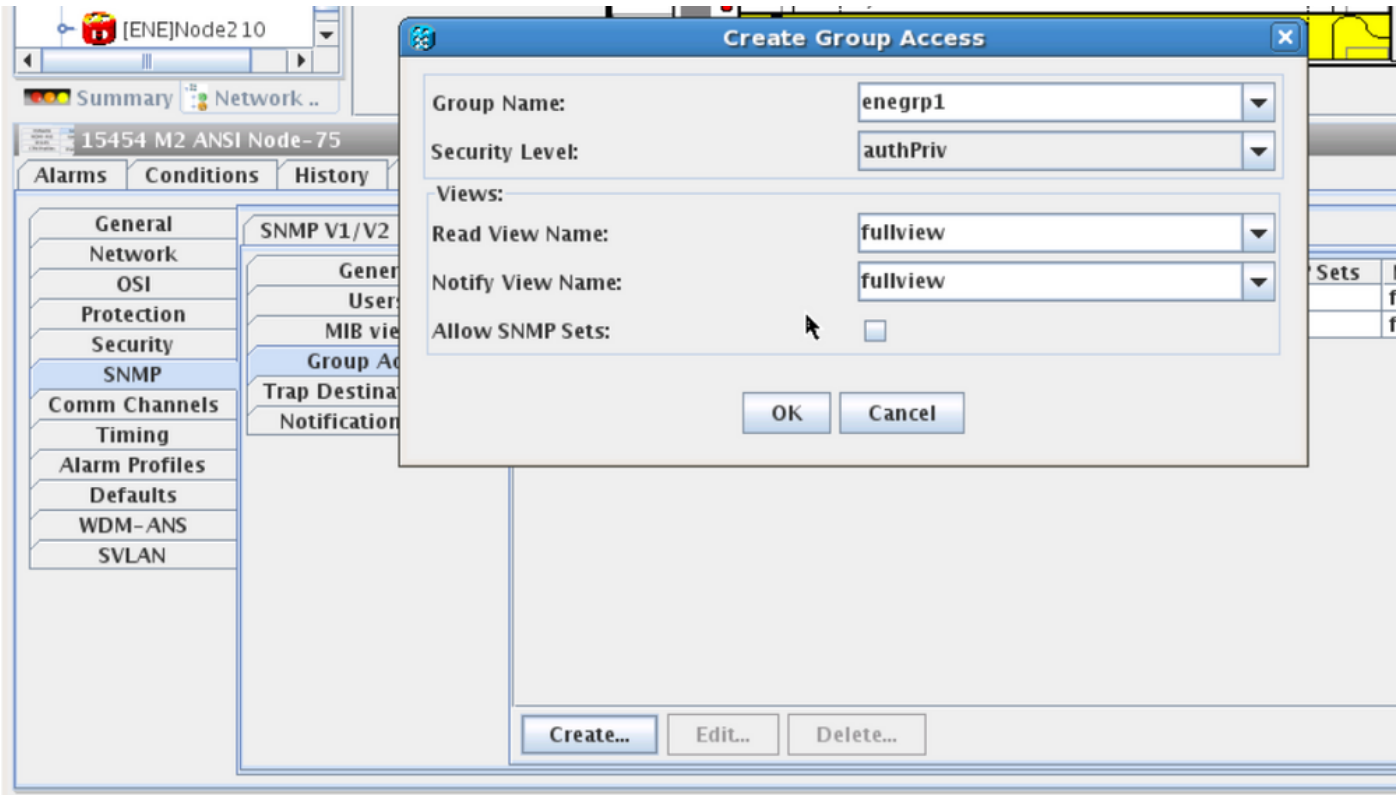
安全级别:如之前在“用户”选项卡中配置的。

代理标记：提供代理标记(例如Tag75)。

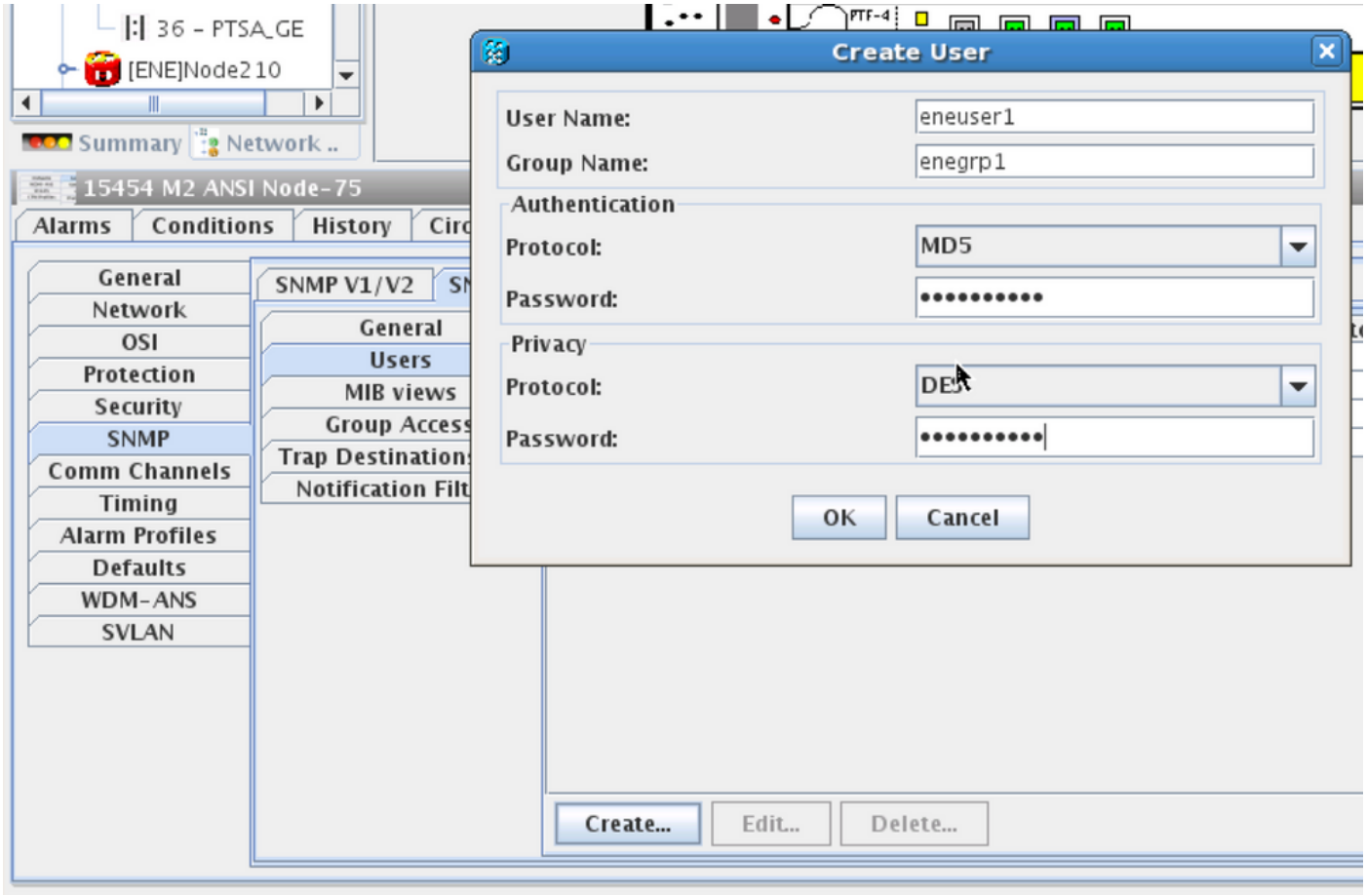


在ENE节点上

步骤1.导航至**Provisioning > SNMP > SNMP V3**和**Create Group Access（Group Access选项卡）**：提供具有访问级别(noAuthnoPriv|AuthnoPriv|authPriv)和全视图读取和通知访问权限的组名，如图所示。



步骤2.创建用户访问权限（用户选项卡）：创建组名与之前在“组访问”选项卡中创建的组名相同的用户。此外，根据访问级别提供身份验证。



如果显示在“用户”选项卡中，则确保在“组访问”选项卡中创建default_group，以防“组访问”选项卡中缺少它。

步骤3.陷阱目标(V3)选项卡：

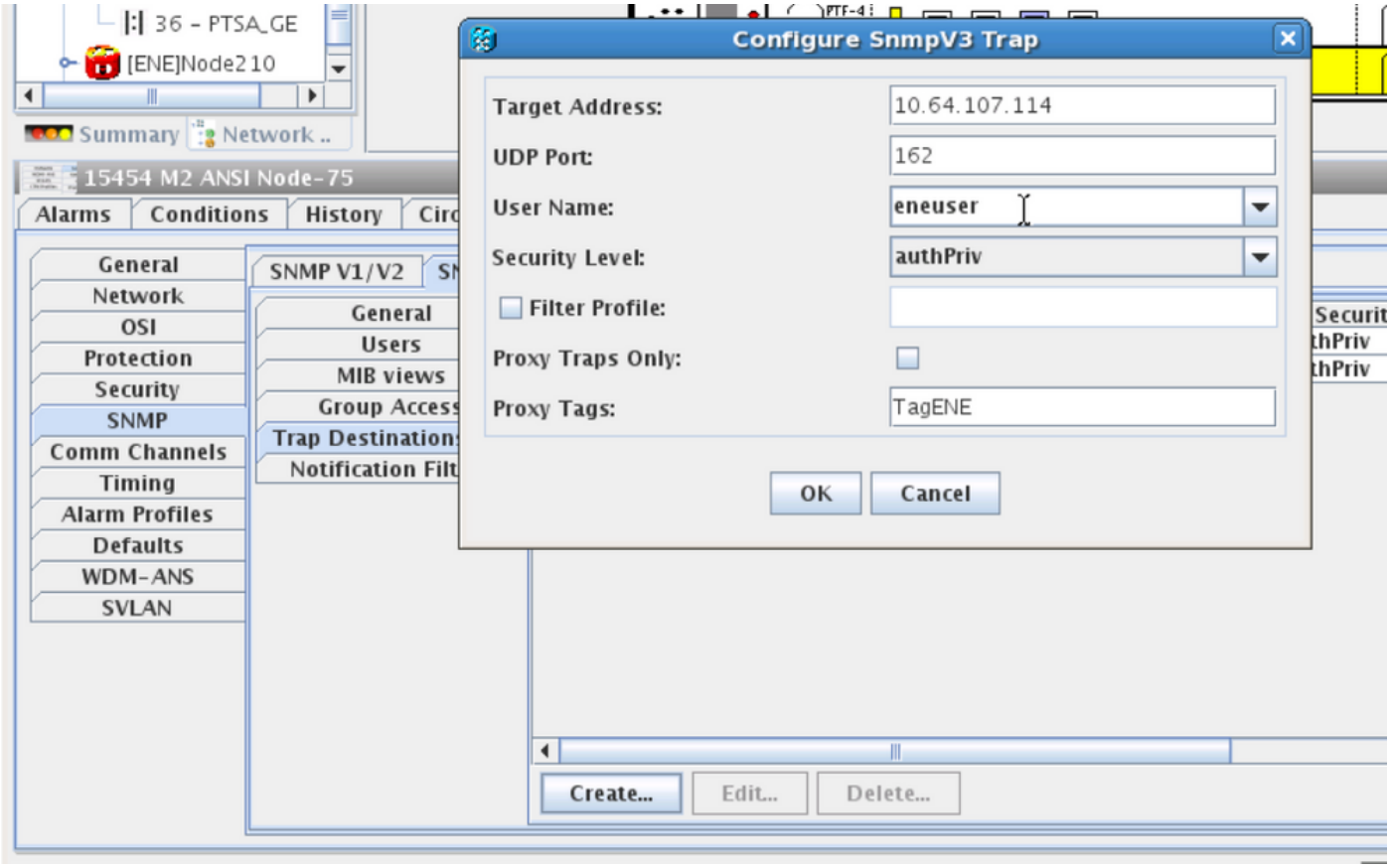
目标地址：GNE节点IP。

UDP 端口:162.

用户名：“用户”(User)选项卡中的用户名称。

安全级别:如之前在“用户”选项卡中配置的。

代理标记：提供与GNE相同的任何代理标记(例如Tag75)。



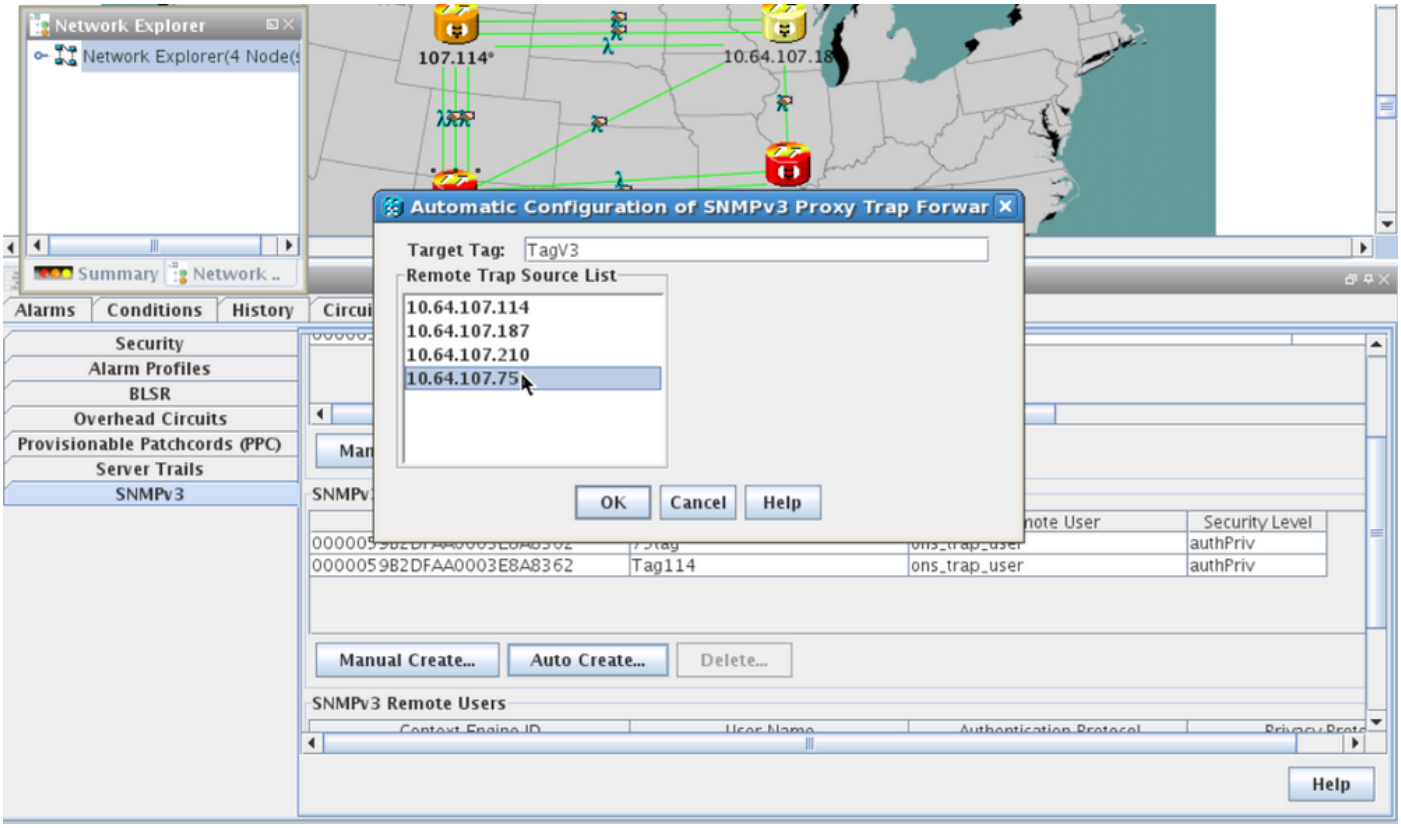
在CTC中，导航至网络视图：

步骤1.导航至**SNMPv3选**项卡。

第二步： SNMPv3代理陷阱转发器表：可以执行手**动或**自动**创建**。

选择“**自动创建**”。在这种情况下：

- 目标标记：在GNE中设置代理标记。
- 远程陷阱源列表：选择ENE节点IP，如图所示。



验证GNE/ENE设置

配置NMS服务器(blr-ong-lnx10):

步骤1.在服务器的主目录中，创建一个目录并将其命名为**snmp**。

第二步： 在此目录下，创建文**件snmptrapd.conf**。

第三步： 在**snmptrapd.conf**中，创建以下配置：

```
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:

对于身份验证模式：

```
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>
```

对于authnopriv模式：

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

对于noauthnopriv模式：

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

故障排除

目前没有针对此配置的故障排除信息。