Cisco ONS15454/NCS2000デバイスでのSNMPv3の設定

内容

概要

このドキュメントでは、ONS15454/NCS2000デバイスで簡易ネットワーク管理プロトコルバージョン3(SNMPv3)を設定する手順について説明します。これらにはすべて例が示されます。

> **注**：このドキュメントで提供されている属性のリストは、すべてを網羅しているわけでも、信頼できるものでもなく、このドキュメントを更新しなければ随時変更される可能性があります。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Transport Controller(CTC)GUI
- サーバに関する基本的な知識
- 基本的なLinux/Unixコマンド

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

スタンドアロン/マルチシェルフノードの場合

ONS15454/NCS2000デバイスでのauthPrivモードの設定

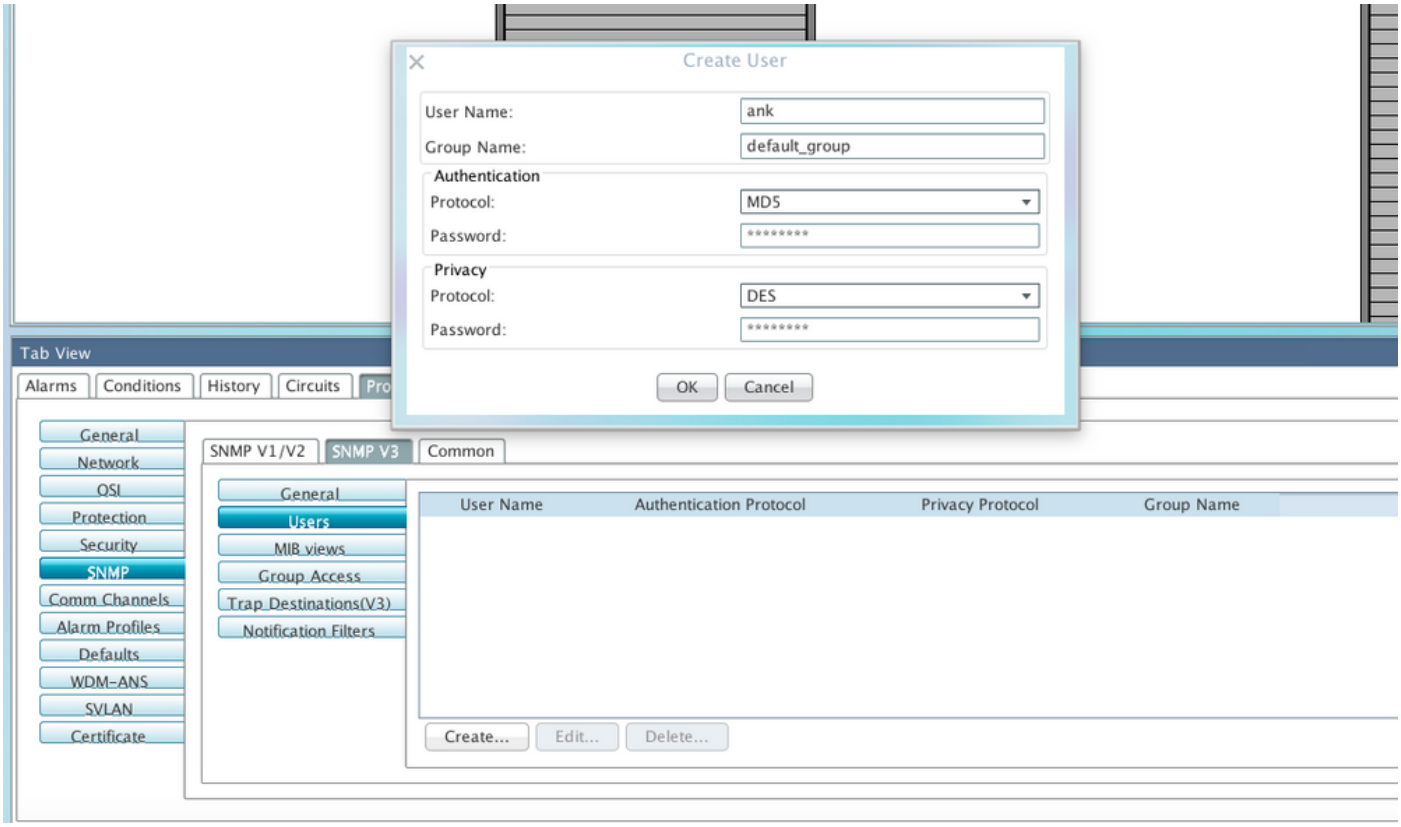
ステップ1：スーパーユーザクレデンシャルを使用してCTC経由でノードにログインします。

ステップ2:[Node view] > [Provisioning] > [SNMP] > [SNMP V3]に移動します。

ステップ3:[Users]タブに移動します。ユーザを作成します。

```
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>
```

ステップ4：図に示すように[OK]をクリックします。



仕様：アナログ FXS インターフェイス

[User Name]：エージェントに接続するホスト上のユーザの名前を指定します。ユーザ名は、6文字以上40文字以下にする必要があります（TACACSおよびRADIUS認証では39文字以下）。 英数字(a ~ z、A ~ Z、0 ~ 9)を含み、特殊文字として@、"-"（ハイフン）、および"を使用できます。 （ドット）を表します。 TL1互換の場合、ユーザ名は6 ~ 10文字である必要があります。

[Group Name]：ユーザが属するグループを指定します。

認証：

[Protocol]：使用する認証アルゴリズムを選択します。オプションは、NONE、MD5、およびSHAです。

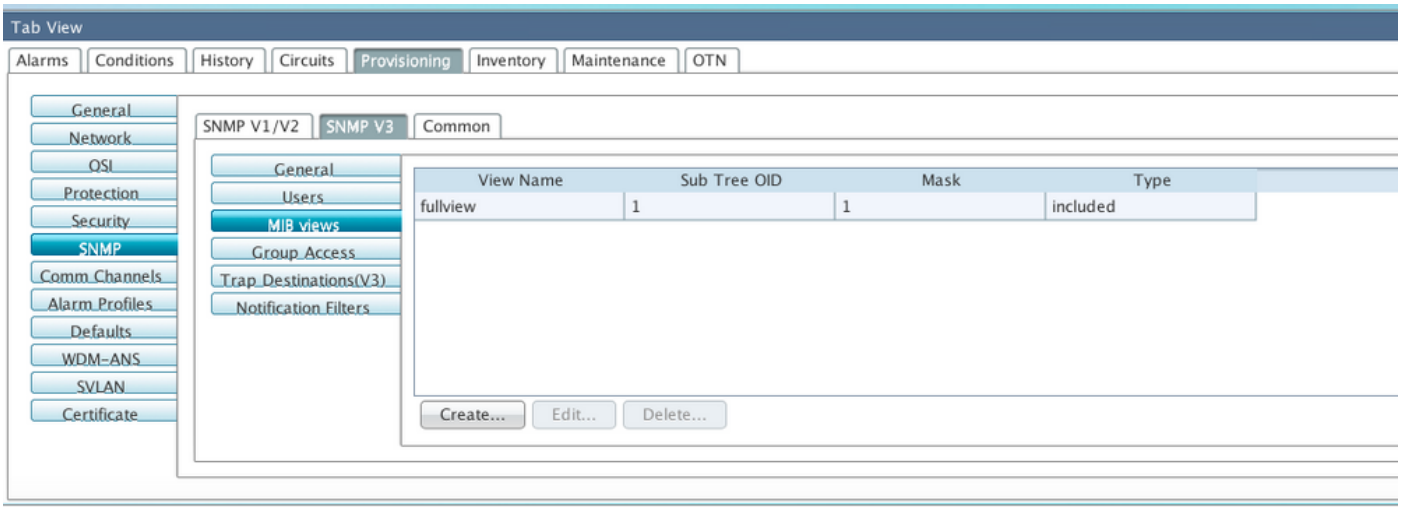
[パスワード(Password)]:MD5またはSHAを選択する場合は、パスワードを入力します。デフォルトでは、パスワードの長さは8文字以上に設定されています。

[Privacy]：ホストがエージェントに送信されるメッセージの内容を暗号化できるようにするプライバシー認証レベル設定セッションを開始します。

[Protocol]：プライバシー認証アルゴリズムを選択します。使用できるオプションは、[なし(None)]、[DES]、および[AES-256-CFB]です。

[パスワード(Password)]:[なし(None)]以外のプロトコルを選択した場合は、パスワードを入力します。

ステップ5:MIBビューがこのイメージに従って設定されていることを確認します。



仕様：アナログ FXS インターフェイス

[名前]：ビューの名前。

サブツリーOID：マスクと組み合わせると、サブツリーのファミリを定義するMIBサブツリー。

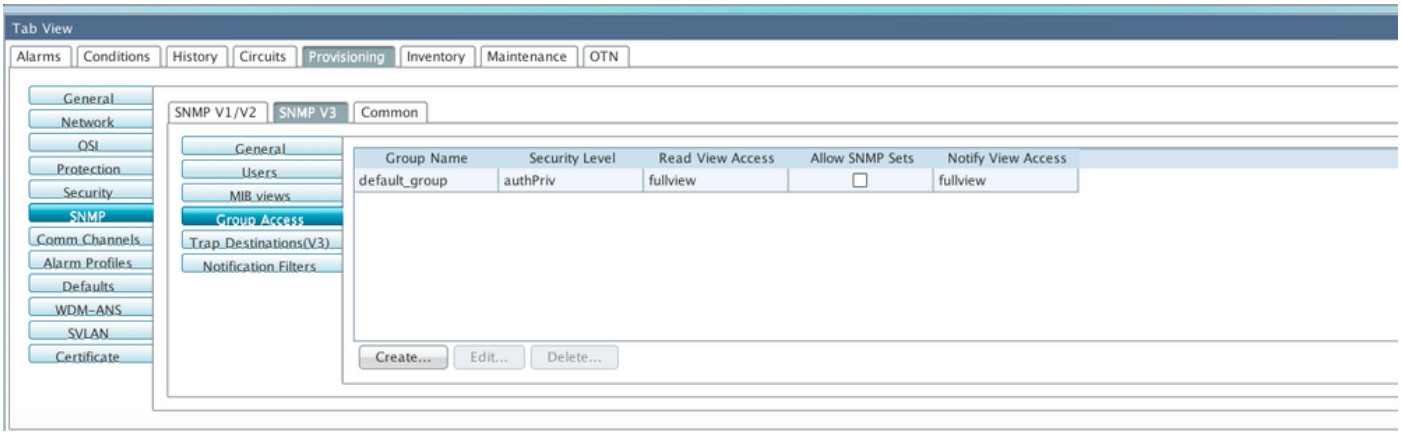
ビットマスク：ビューサブツリーのファミリ。ビットマスクの各ビットは、サブツリーOIDのサブ識別子に対応します。

[タイプ]：ビュータイプを選択します。オプションは[含める(Included)]と[除外(Excluded)]です。

このタイプは、サブツリーのOIDとビットマスクの組み合わせで定義されるサブツリーのファミリを、通知フィルタに含めるか除外するかを定義します。

ステップ6：図に示すように、グループアクセスを設定します。デフォルトでは、グループ名はdefault_groupで、セキュリティレベルはauthPrivです。

注：グループ名は、ステップ3でユーザを作成するときに使用したものと同じである必要があります。



仕様：アナログ FXS インターフェイス

[Group Name]：共通のアクセスポリシーを共有するSNMPグループまたはユーザのコレクションの名前。

[セキュリティレベル(Security Level)]：アクセスパラメータが定義されるセキュリティレベル。次のオプションから選択します。

noAuthNoPriv：認証にユーザ名の一致を使用します。

AuthNoPriv:HMAC-MD5またはHMAC-SHAアルゴリズムに基づく認証を提供します。

AuthPriv:HMAC-MD5またはHMAC-SHAアルゴリズムに基づく認証を提供します。認証に加えて、CBC-DES(DES-56)標準に基づくDES 56ビット暗号化を提供します。

グループに対してauthNoPrivまたはauthPrivを選択する場合、対応するユーザに認証プロトコルとパスワード、プライバシープロトコルとパスワード、またはその両方を設定する必要があります。

[Views]

Read View Name – グループのビュー名を読み取ります。

[Notify View Name]：グループのビュー名を通知します。

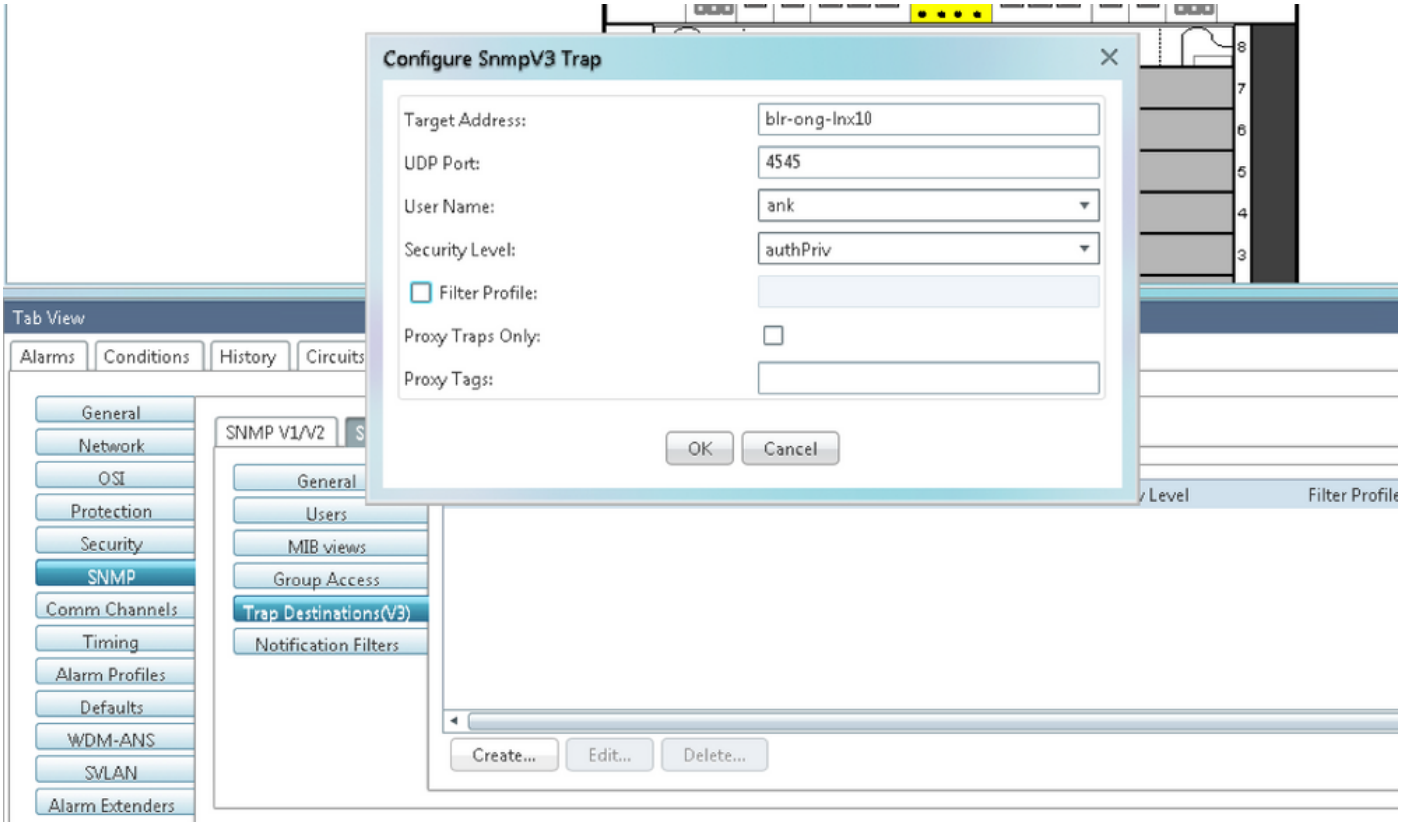
[Allow SNMP Sets]:SNMPエージェントがSNMP SET要求を受け入れるようにするには、このチェックボックスをオンにします。このチェックボックスをオフにすると、SET要求は拒否されます。

注： SNMP SET要求アクセスは、ごく少数のオブジェクトに対して実装されます。

ステップ7:[Node View] > [**Provisioning] > [SNMP] > [SNMP V3] > [Trap Destination (V3)]に移動します。** [**Create** and **Configure**]をクリックしてください。

```
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
```

ステップ8：図に示すように**[OK]**をクリックします。



注： blr-ong-lnx10はNMSサーバです。

仕様：アナログ FXS インターフェイス

Target Address（ターゲットアドレス）：トラップの送信先のターゲット。IPv4またはIPv6アドレスを使用します。

UDPポート：ホストが使用するUDPポート番号。デフォルト値は 162 です。

[User Name]：エージェントに接続するホスト上のユーザの名前を指定します。

[Security Level]：次のいずれかのオプションを選択します。

noAuthNoPriv：認証にユーザ名の一致を使用します。

AuthNoPriv:HMAC-MD5またはHMAC-SHAアルゴリズムに基づく認証を提供します。

AuthPriv:HMAC-MD5またはHMAC-SHAアルゴリズムに基づく認証を提供します。認証に加えて、CBC-DES(DES-56)標準に基づくDES 56ビット暗号化を提供します。

[Filter Profile]：このチェックボックスをオンにして、フィルタプロファイル名を入力します。トラップは、フィルタプロファイル名を指定し、通知フィルタを作成した場合にのみ送信されます。

[Proxy Traps Only]：オンにすると、ENEからプロキシトラップのみを転送します。このノードからのトラップは、このエントリによって識別されるトラップ宛先には送信されません。

プロキシタグ：タグのリストを指定します。タグリストは、ENEがこのエントリによって識別されるトラップ宛先にトラップを送信する必要があり、GNEをプロキシとして使用する場合にのみ、GNEで必要になります。

NMSサーバの設定(blr-ong-lnx10)

ステップ1：サーバのホームディレクトリで、snmpという名前のディレクトリを作成します。

ステップ 2： このディレクトリの下に、snmptrapd.confファイルを作成します。

ステップ3: snmptrapd.confファイルを次のように変更します。

```
vi snmptrapd.conf

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

以下に、いくつかの例を示します。

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

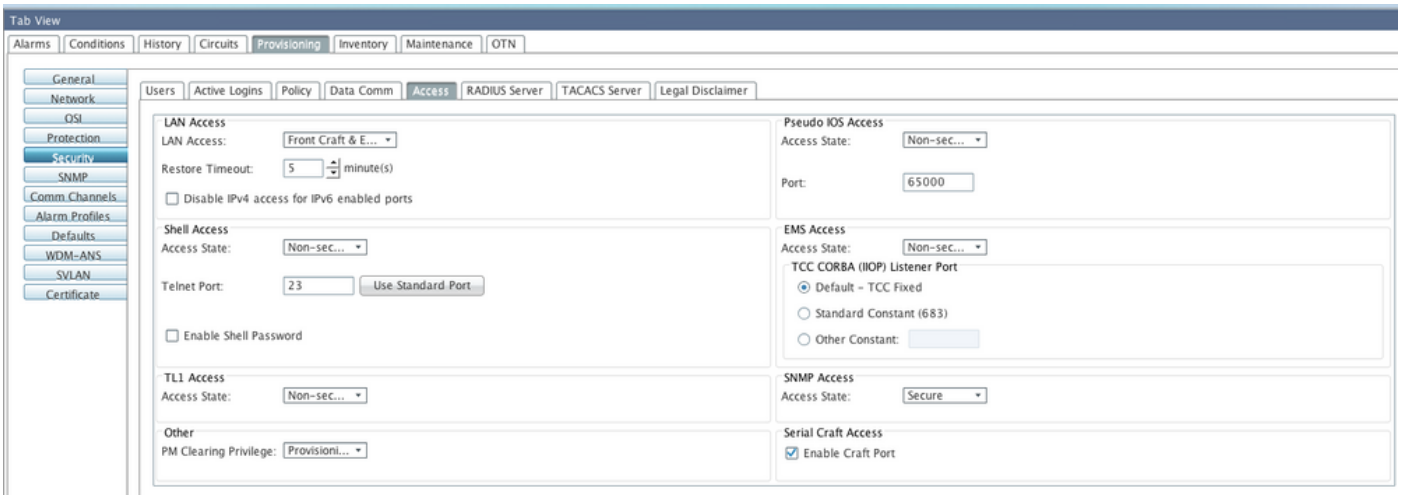
この例では、

```
user_name=ank

MD5 password = cisco123

DES password  = cisco123

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

Node view > Provisioning > SNMP > SNMP V3 > General

authPrivモードの確認

ステップ1:CTCで、図に示すように、[Node View] > [Provisioning] > [Security] > [Access] > [snmp access state]を[Secure]に変更します。



ステップ2:NMSサーバに移動し、snmpwalkを実行します。

構文：

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

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
```

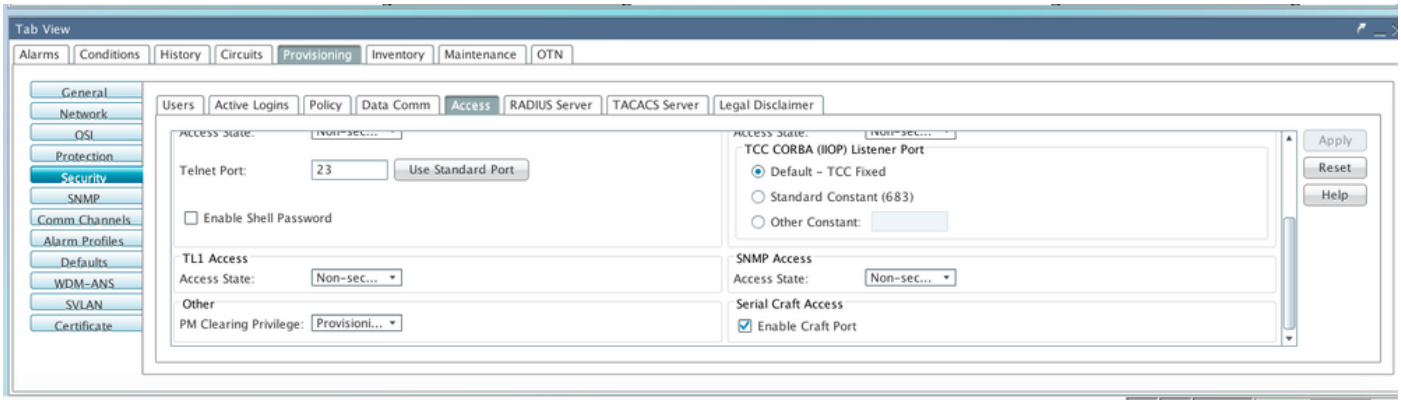
SNMP trap：

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

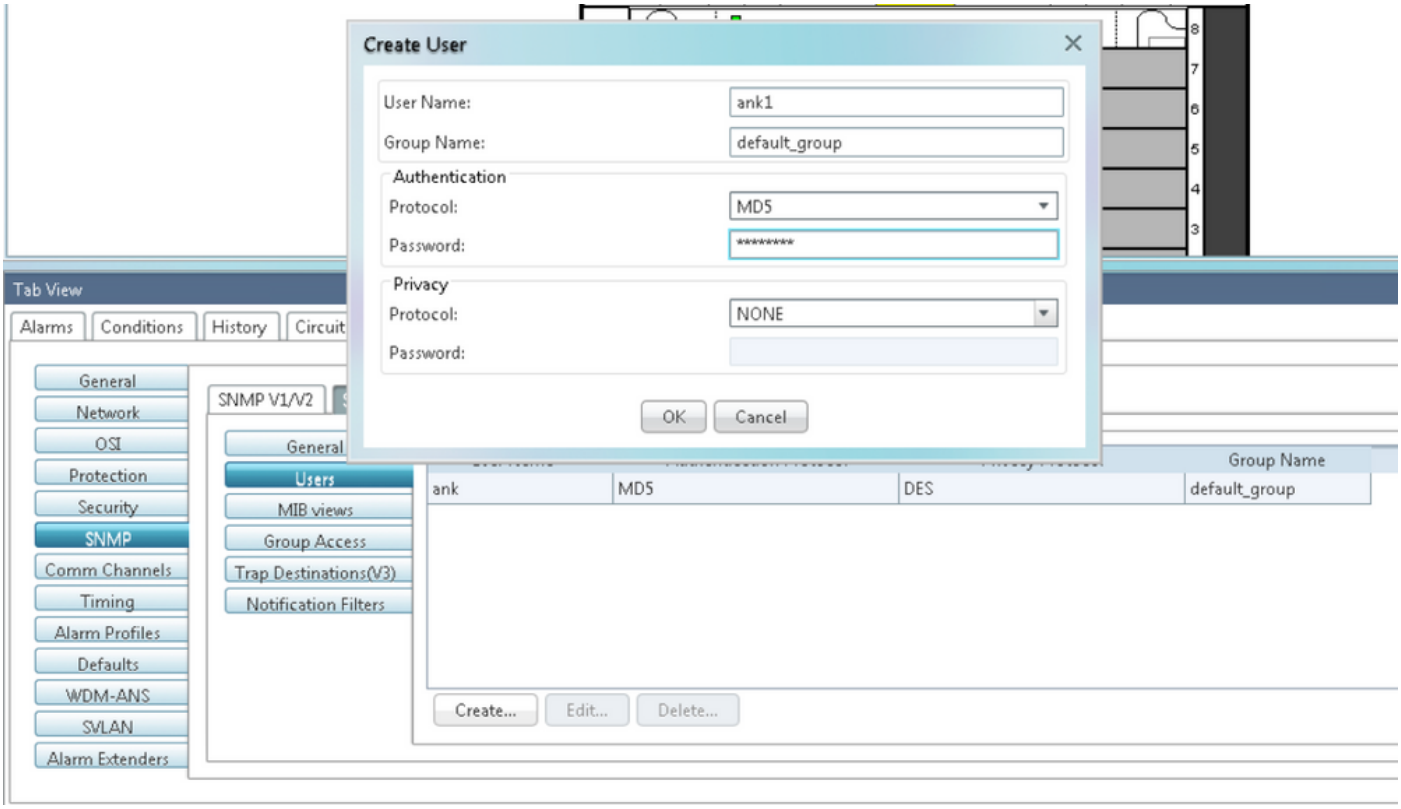
Trap cmdはすべてのバージョンで同じです。

ONS15454/NCS2000デバイスでのauthNoPrivモードの設定

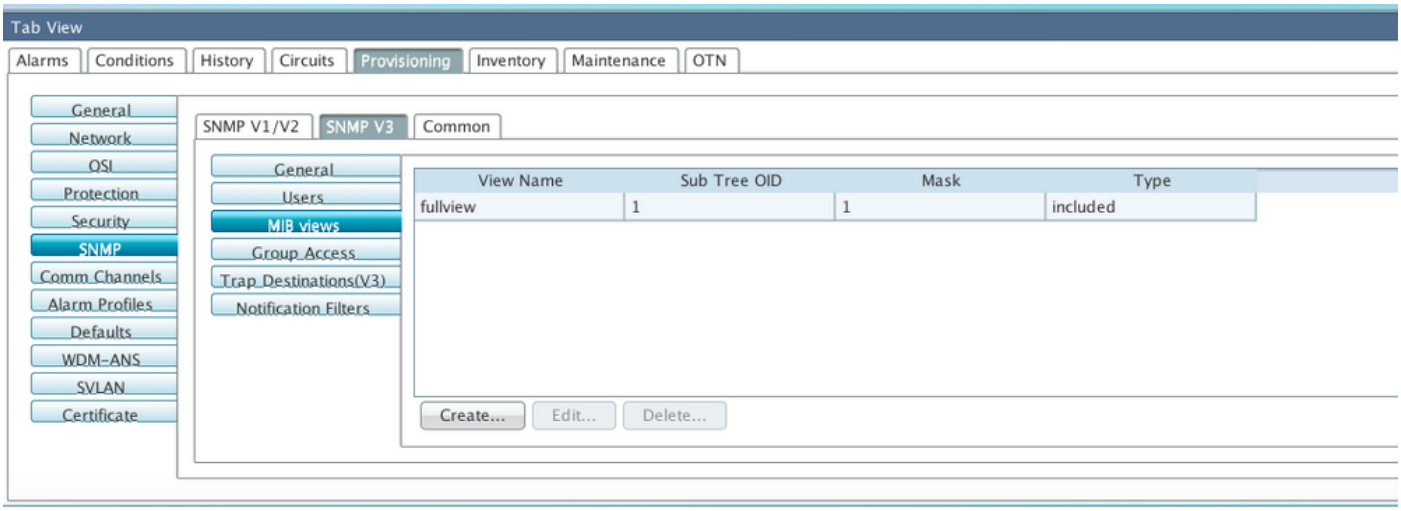
ステップ1:CTCで、[Node View] > [Provisioning] > [Security] > [Access] > [snmp access state]を[Non-secure mode]に移動します（図を参照）。



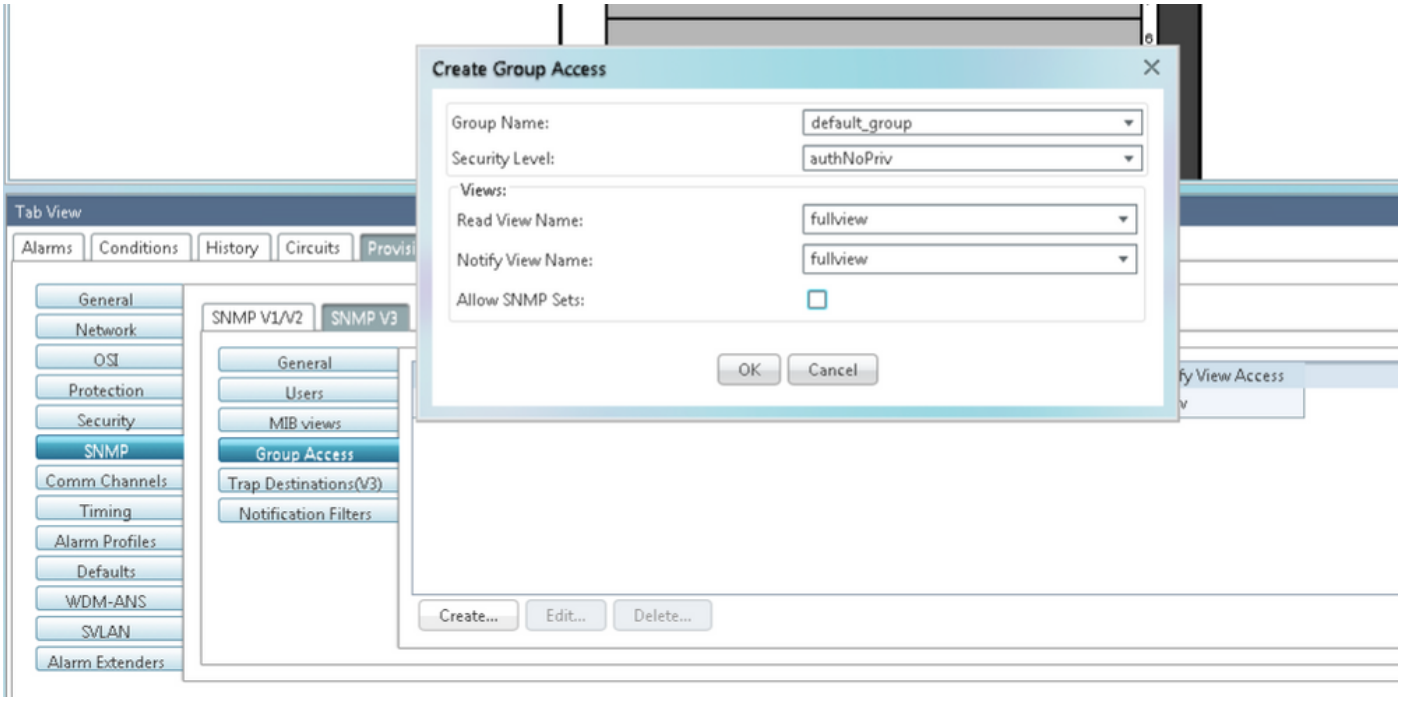
ステップ2:[Node View] > [Provisioning] > [SNMP] > [SNMP V3] > [Users] > [Create User]に移動し、図に示すように設定します。



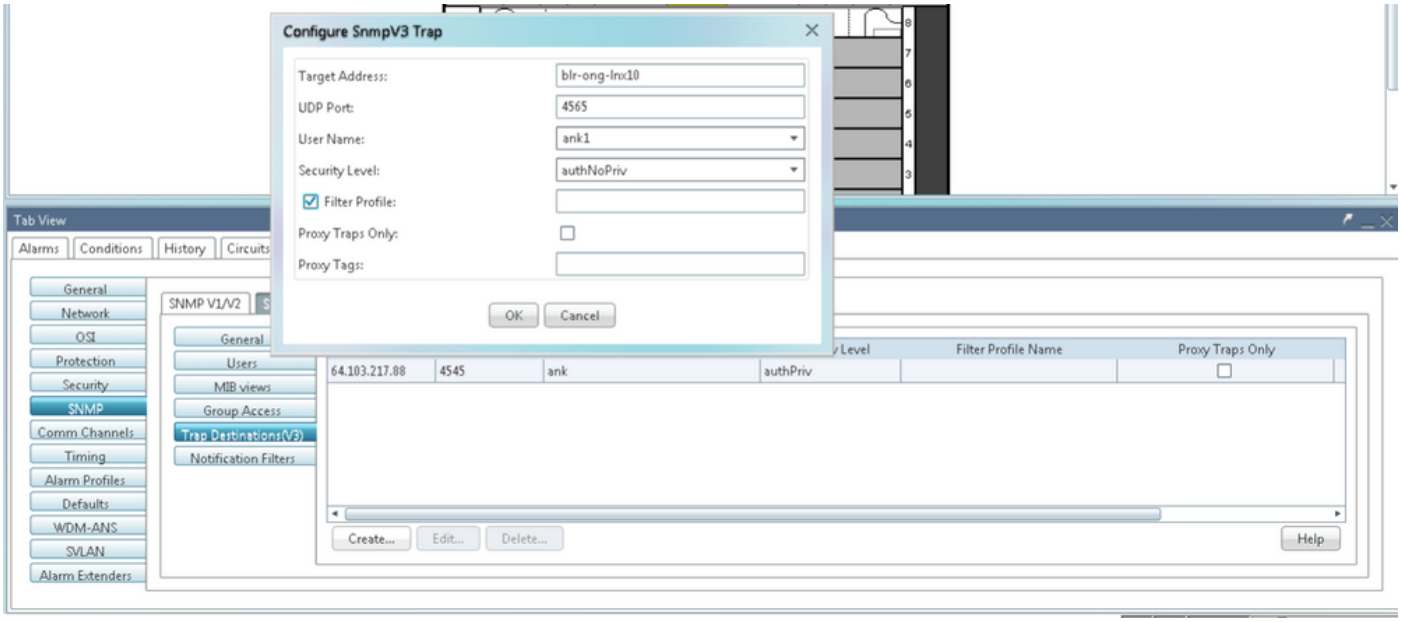
ステップ3：図に示すようにMIBビューが設定されていることを確認します。



ステップ4: authnoprivモードの図に示すように、グループアクセスを設定します。



ステップ5:[Node View] > [**Provisioning] > [SNMP] > [SNMP V3] > [Trap Destination (V3)]に移動します。** 図に示すように、[**Create** and **Configure**]をクリックします。



authNoPrivモードの確認

ステップ1:NMSサーバに移動し、snmpwalkを実行します。

構文：

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

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
```

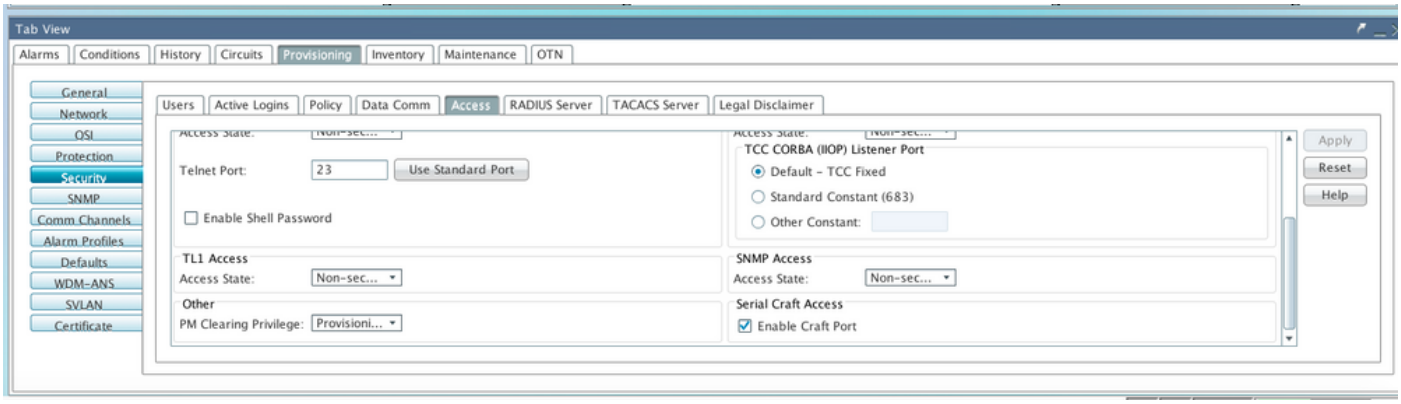
SNMP trap：

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

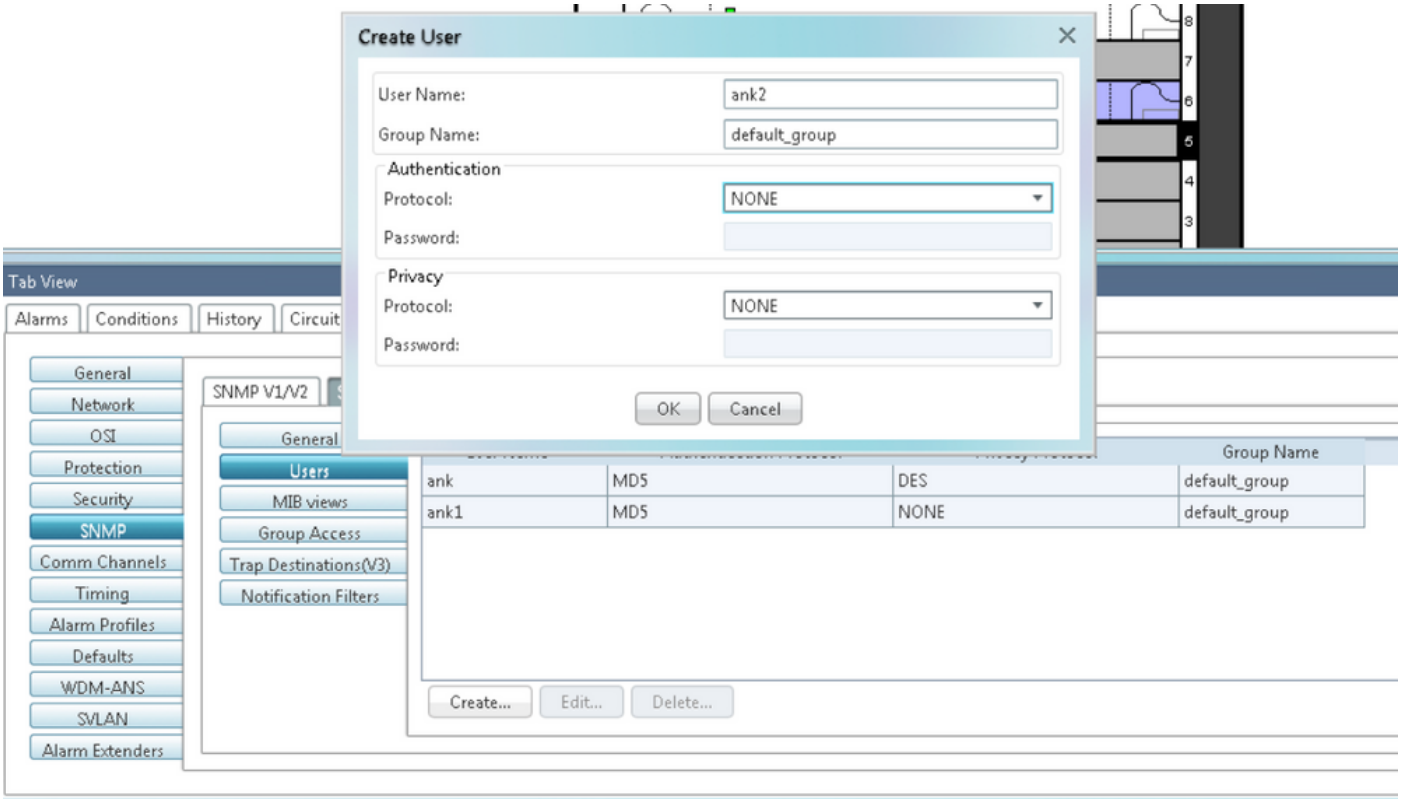
Trap cmdはすべてのバージョンで同じです。

ONS15454/NCS2000デバイスでのnoAuthNoPrivモードの設定

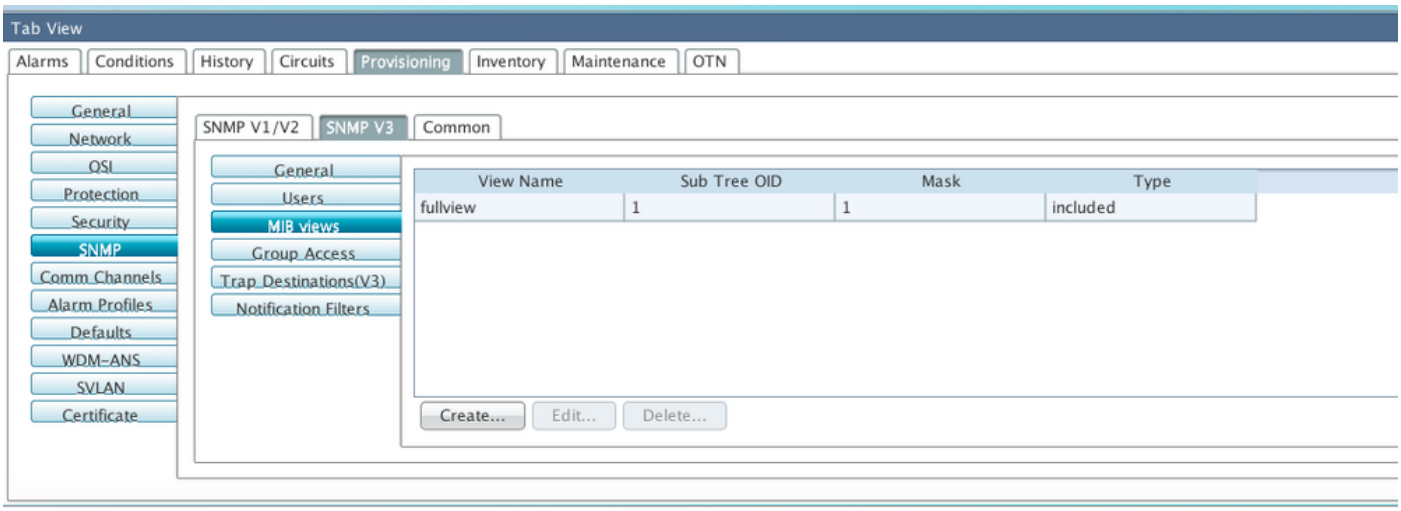
ステップ1:CTCで、[Node View] > [Provisioning] > [Security] > [Access] > [snmp access state]を[Non-secure mode]に移動します（図を参照）。



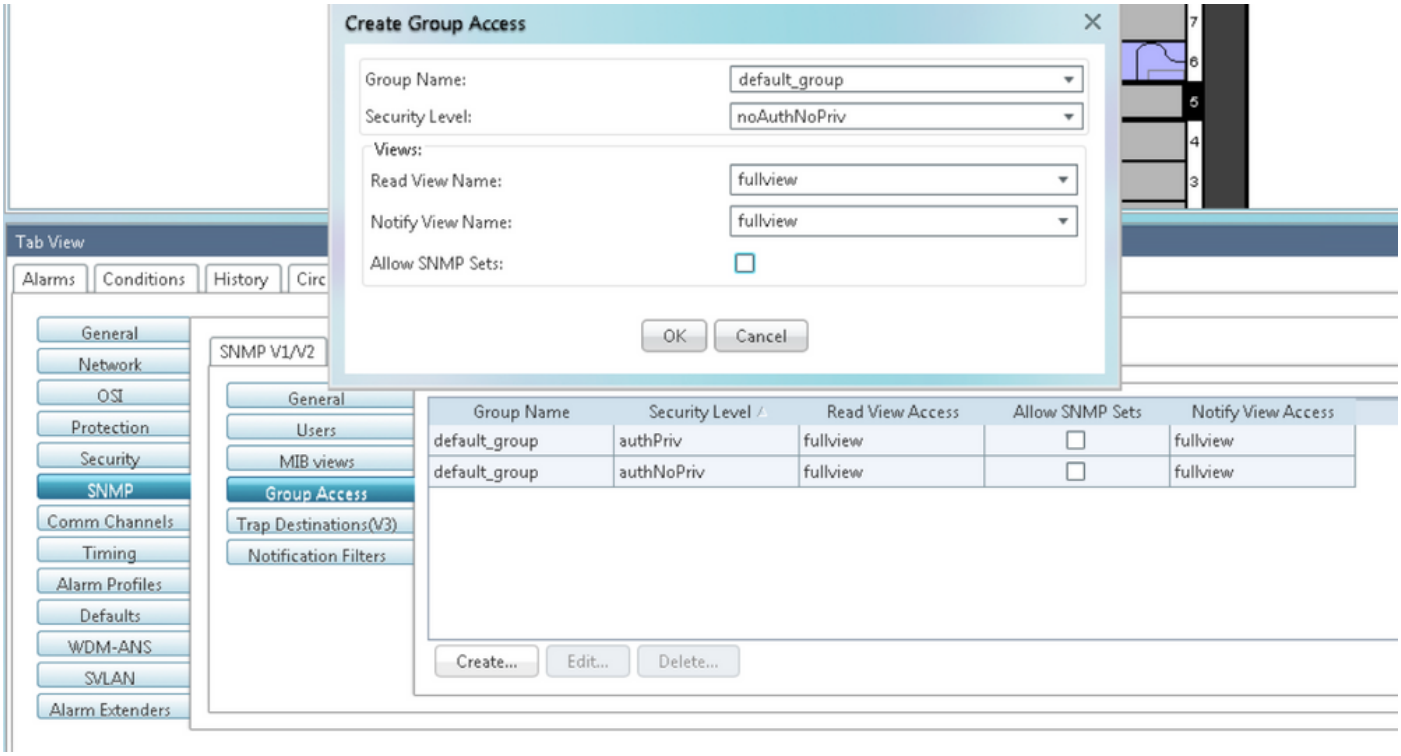
ステップ2：図に示すように、[Node View] > [Provisioning] > [SNMP] > [SNMP V3] > [Users] > [Create User and Configure]に移動します。



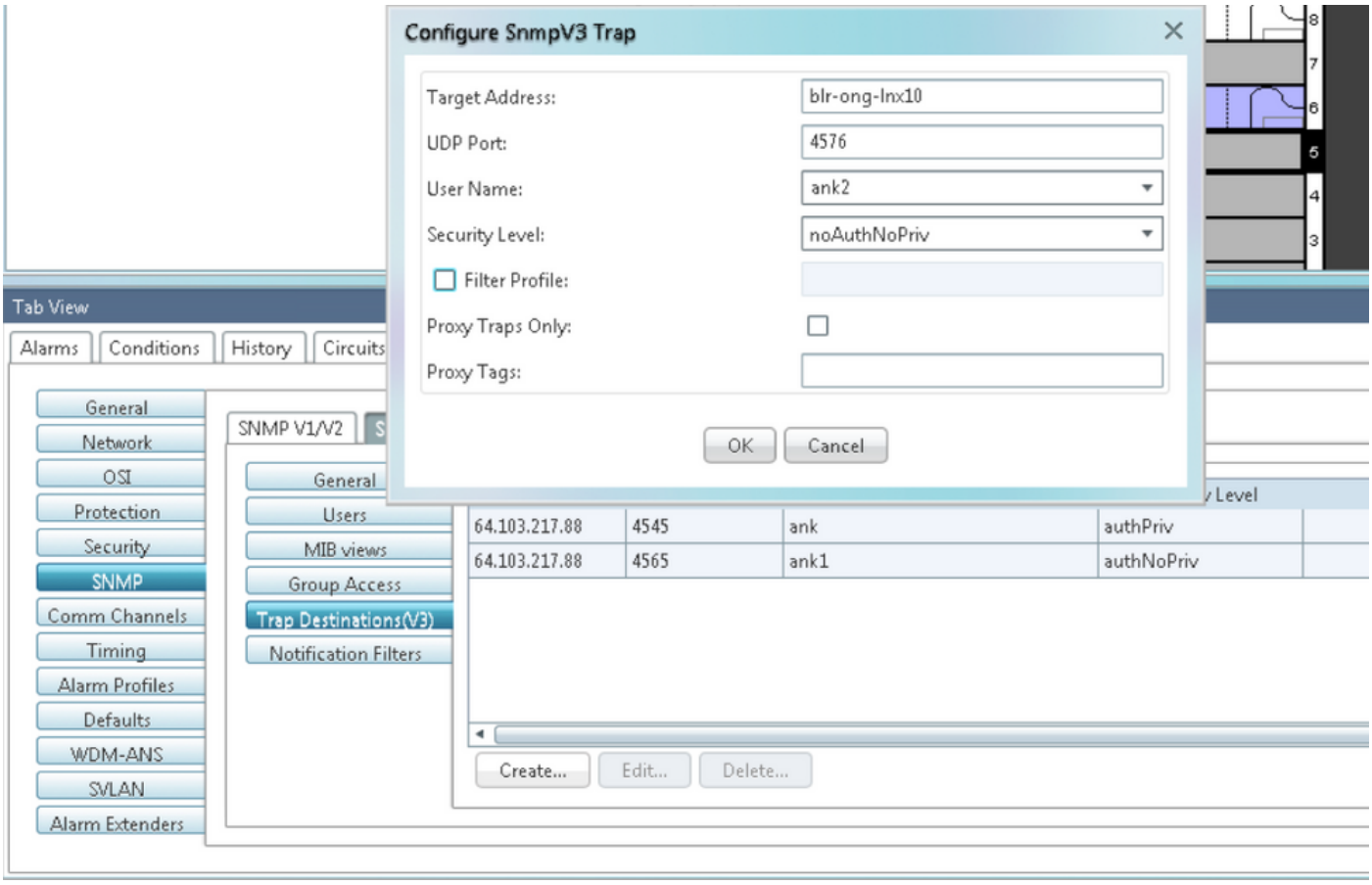
ステップ3：図に示すように**MIBビュー**が設定されていることを確認します。



ステップ4：図に示すように、noauthnoprivモードのグループアクセスを設定します。



ステップ5:[Node View] > [**Provisioning] > [SNMP] > [SNMP V3] > [Trap Destination (V3)]に移動します。** 図に示すように、[**Create** and **Configure**]をクリックします。



noAuthNoPrivモードの確認

ステップ1:NMSサーバに移動し、snmpwalkを実行します。

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

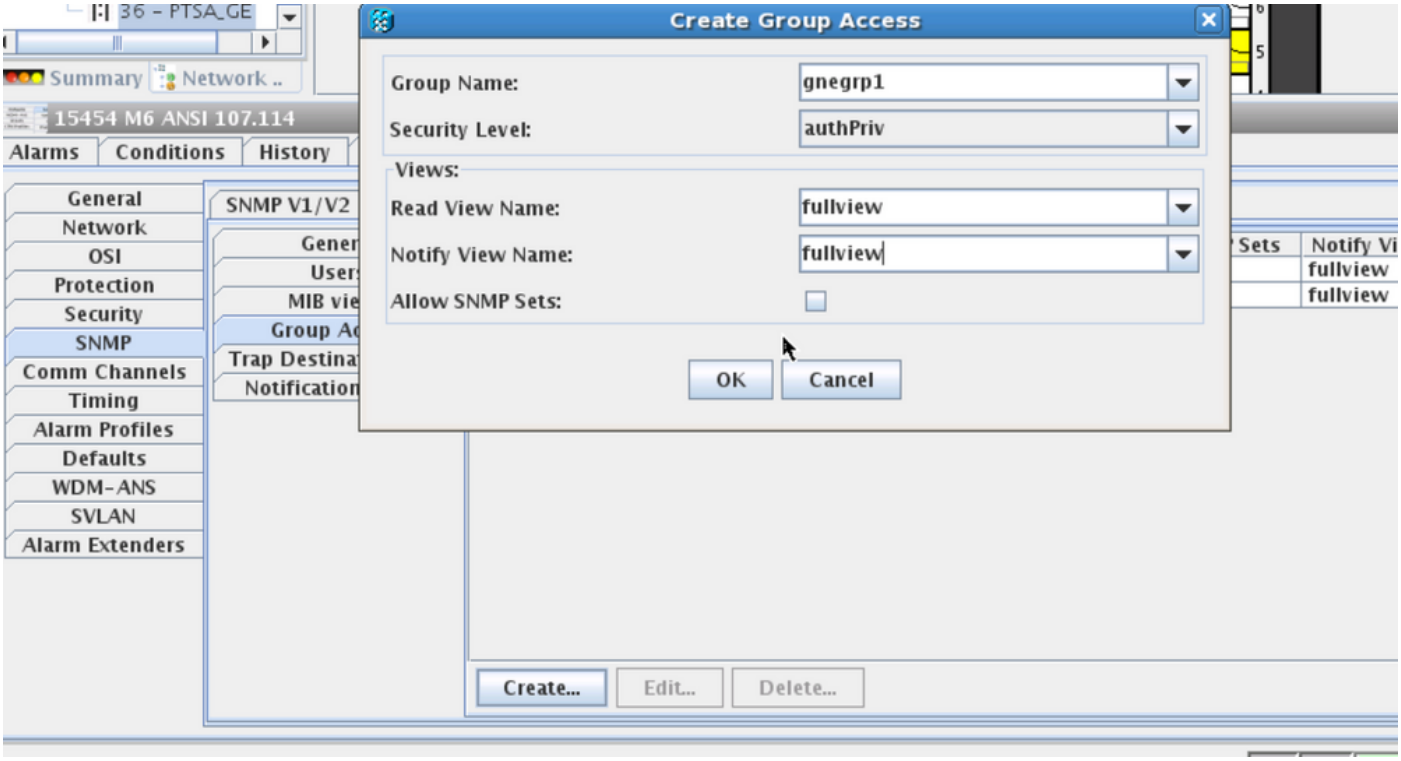
```
blr-ong-lnx10:155> snmpwalk -v 3 -l noauthnopriv -u ank2 10.64.106.40 system

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 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はすべてのバージョンで同じです。

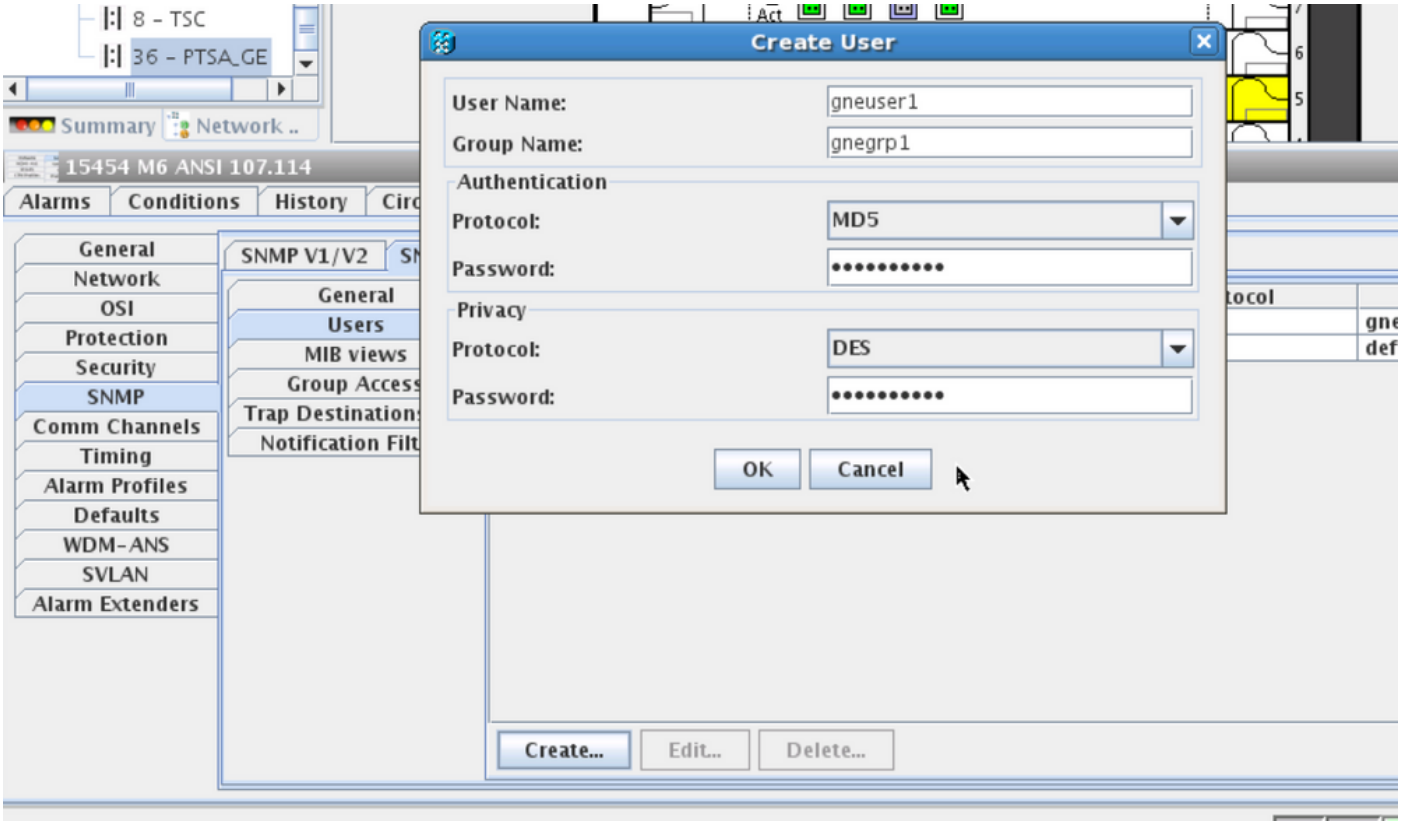
GNE/ENEセットアップのSNMP V3トラップ

GNEノード上

ステップ1: **[Provisioning] > [SNMP] > [SNMP V3 and C]グループアクセス権の作成（[Group Access]タブ）:図に示すように、セキュリティレベル(noAuthnoPriv|AuthnoPriv|authPriv)とフルビューの読み取りおよび通知アクセスを持つグループ名を指定します。**



ステップ2：ユーザアクセス権の作成（[Users]タブ）:[グループアクセス(Group Access)]タブで以前に作成したものと同じグループ名を持つユーザを作成します。また、図に示すように、アクセスレベルに基づいて認証を提供します。



ステップ3:[Trap Destination(V3)]タブ：

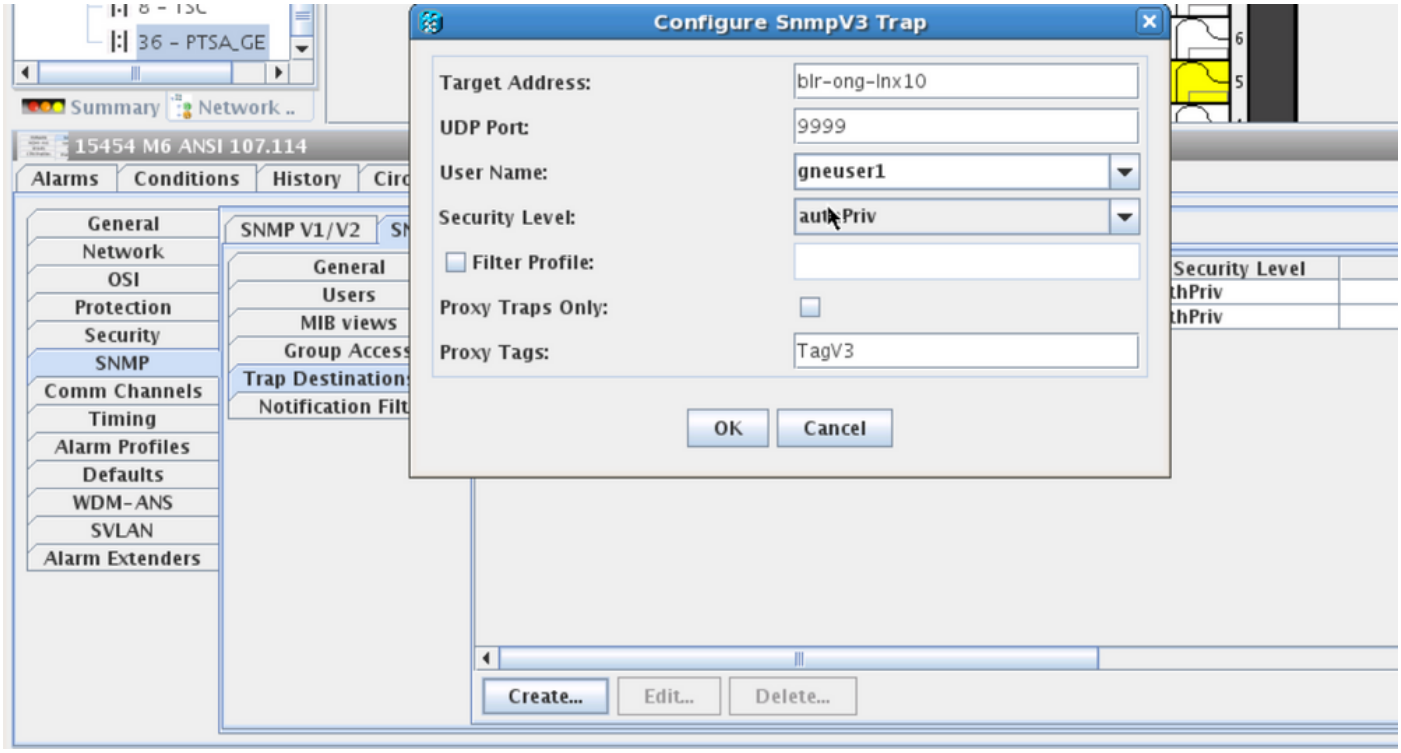
ターゲットアドレス：トラップの実行元となるNMSサーバのアドレス(例：Blr-ong-lnx10)。

UDPポート：トラップが受信されるポート番号（例：9977）。

ユーザ名：[ユーザ(User)]タブのユーザの名前。

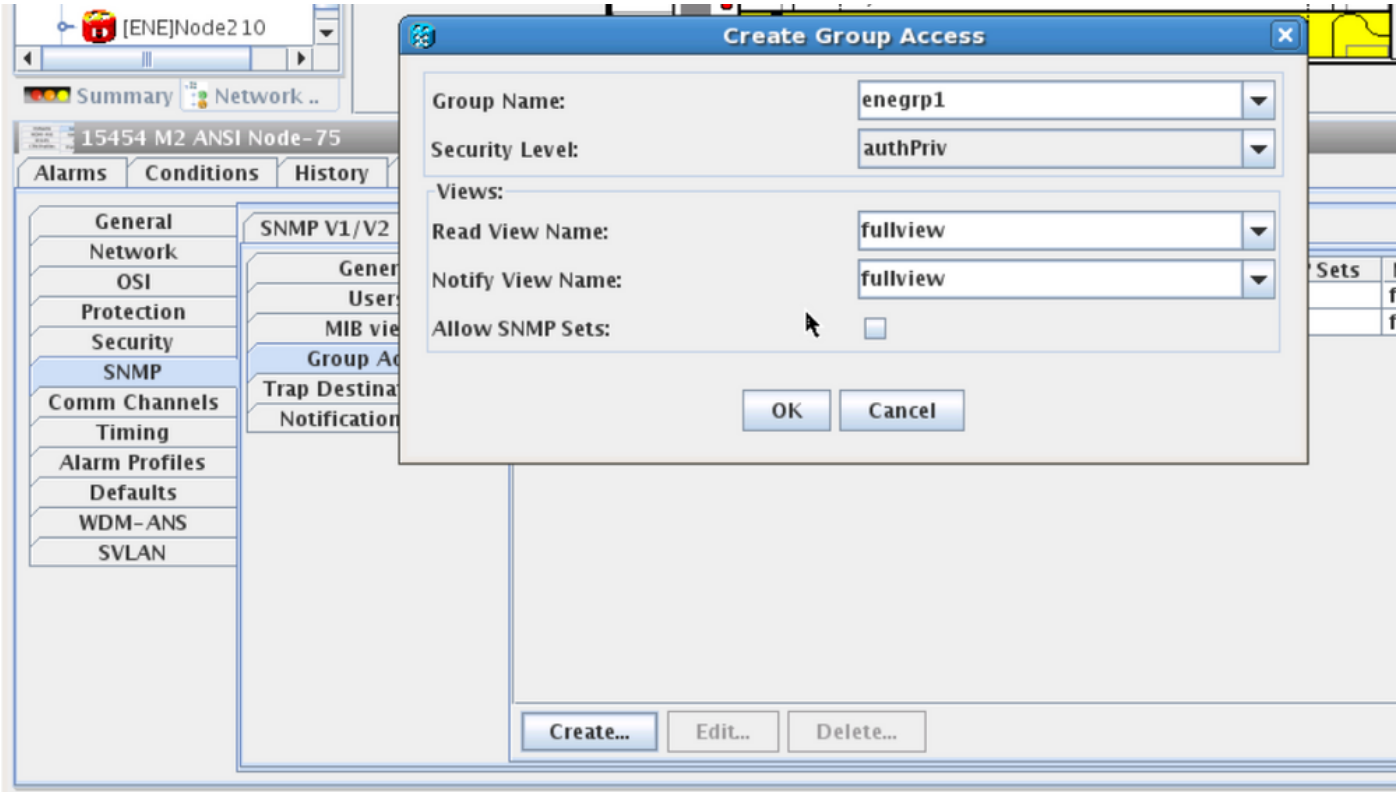
セキュリティレベル：[ユーザ(User)]タブで設定したとおり。

プロキシタグ：プロキシタグ(例：Tag75)。

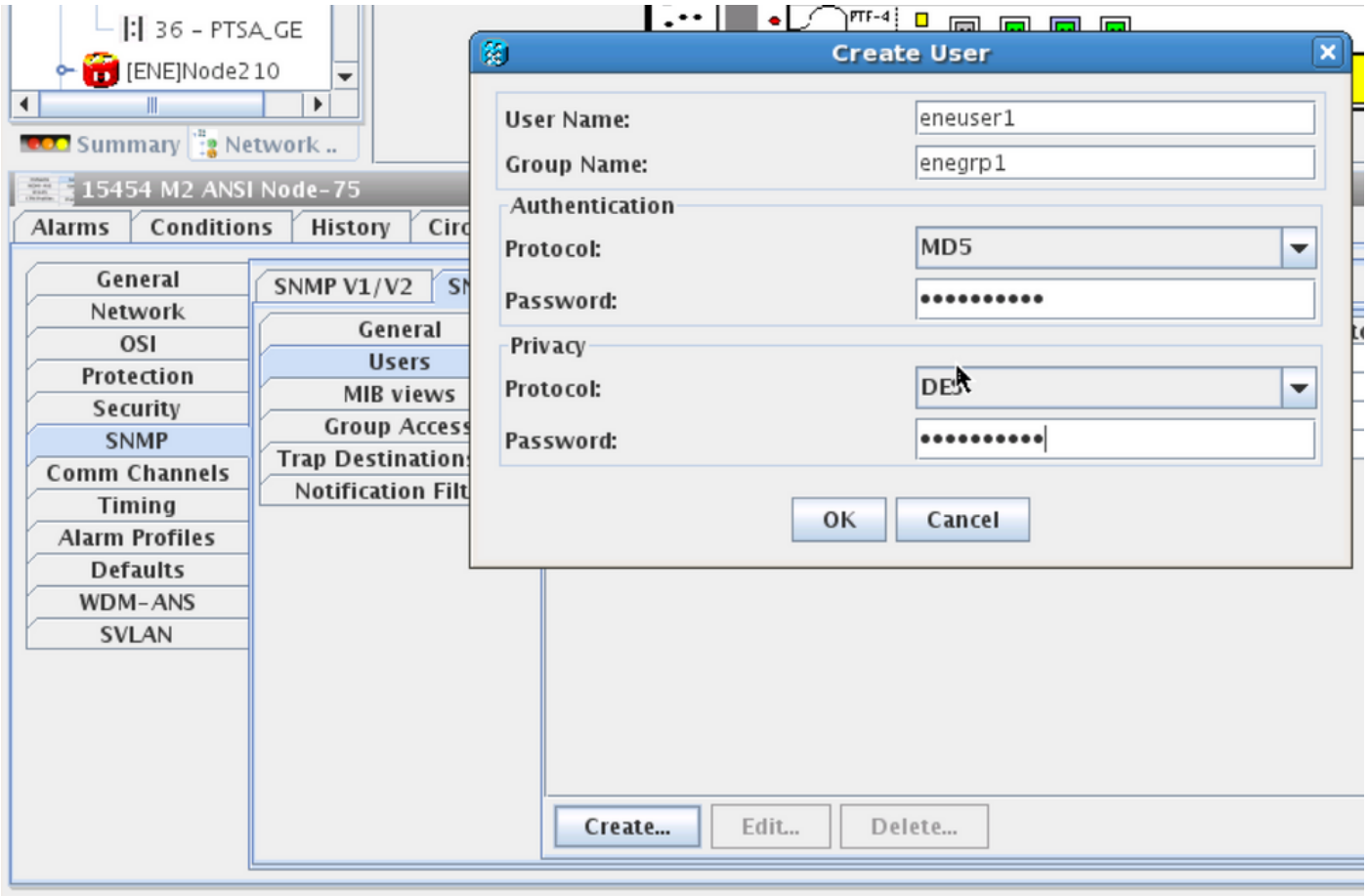


ENEノード上

ステップ1:[Provisioning] > [SNMP] > [SNMP V3]に移動し、[Create Group Access] ([Group Access]タブ) に移動します。図に示すように、アクセスレベル(noAuthnoPriv|AuthnoPriv|authPriv)とフルビューの読み取りおよび通知アクセスを持つグループ名を指定します。



ステップ2：ユーザアクセス権の作成（[Users]タブ）:[グループアクセス(Group Access)]タブで以前に作成したものと同じグループ名を持つユーザを作成します。また、アクセスレベルに基づいて認証を提供します。



[User]タブに示されているdefault_groupが[Group Access]タブにない場合は、[Group access]タブに作成されていることを確認します。

ステップ3:[Trap Destination(V3)]タブ：

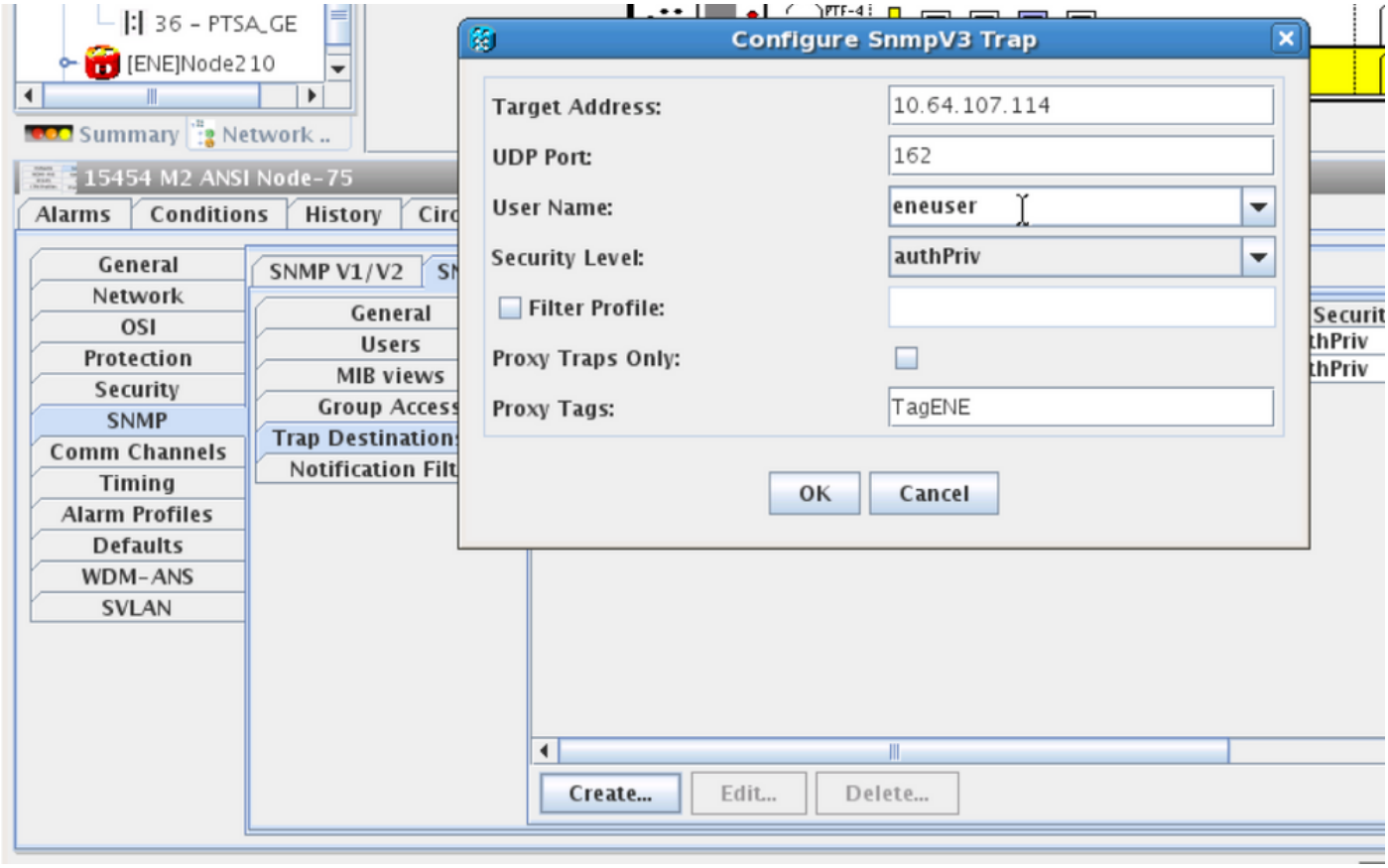
ターゲットアドレス：GNEノードIP。

UDPポート：162 .

ユーザ名：[ユーザ(User)]タブのユーザの名前。

セキュリティレベル：[ユーザ(User)]タブで設定したとおり。

プロキシタグ：GNE(例：Tag75)。



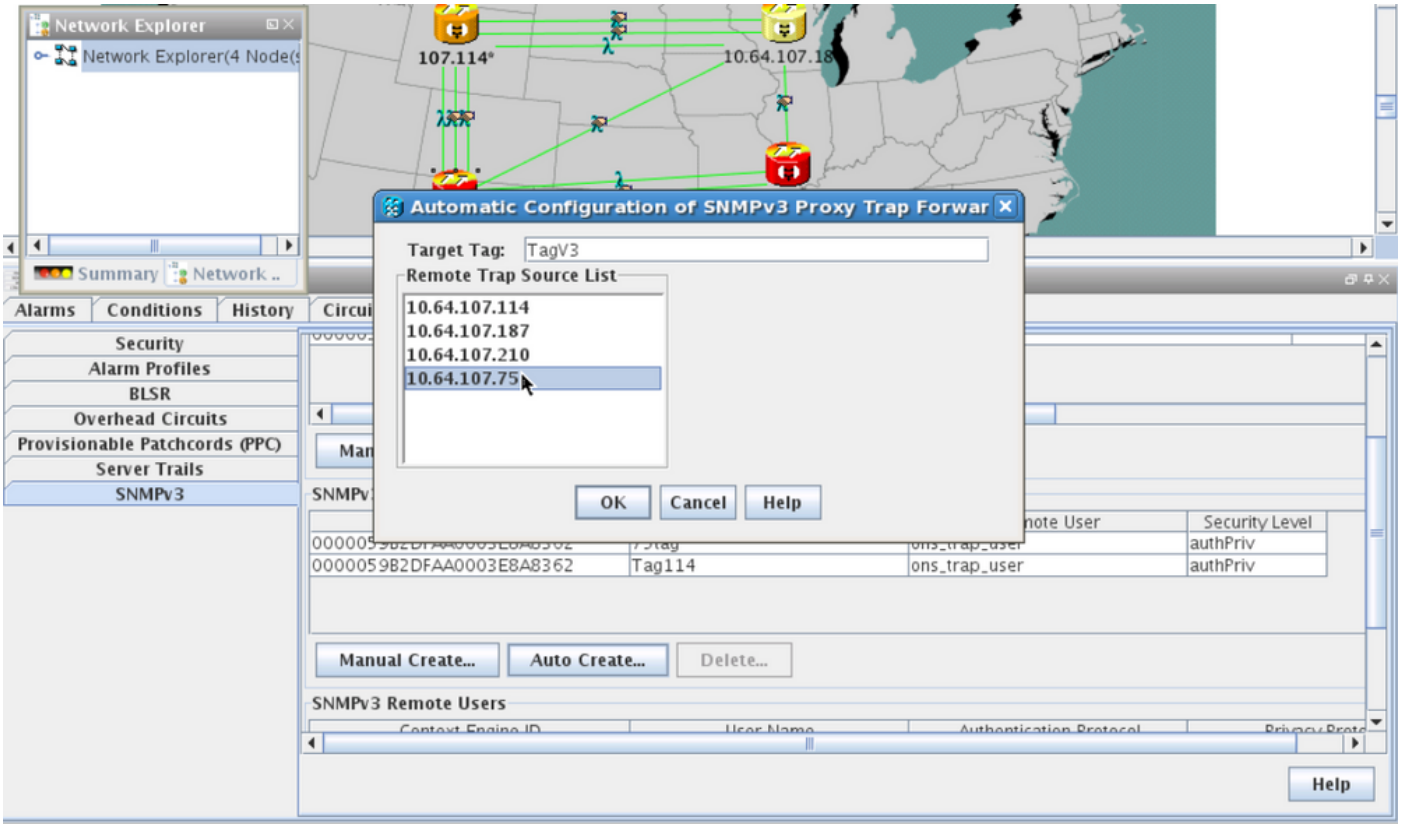
CTCで、ネットワークビューに移動します。

ステップ1:[SNMPv3]タブ**に移動**します。

ステップ 2： SNMPv3プロキシトラップフォワーダテーブル：手動または自動**作成を**実行**できます**。

[自動**作成]を選択します**。その下：

- ターゲットタグ：GNEで設定されたプロキシタグ。
- [Remote Trap Source List]:図に示すように、ENEノードIPを選択します。



GNE/ENE設定の確認

NMSサーバ(blr-ong-lnx10)を設定します。

ステップ1：サーバのホーム・ディレクトリで、ディレクトリを作成し、snmpという名前を付けます。

ステップ 2： このディレクトリの下に、snmptrapd.confファイルを作成します。

ステップ 3： snmptrapd.confで、次の構成を作成します。

```
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"
```

ENEでのsnmpwalk:

authprivモードの場合：

```
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>
```

authnoprivモードの場合：

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

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

noauthnoprivモードの場合：

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

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。