Configuración de SNMPv3 en dispositivos Cisco ONS15454/NCS2000

Contenido

Introducción

Este documento describe instrucciones paso a paso sobre cómo configurar el protocolo simple de administración de red versión 3 (SNMPv3) en dispositivos ONS15454/NCS2000. Todos los temas incluyen ejemplos.

> **Nota:** La lista de atributos proporcionada en este documento no es exhaustiva ni fidedigna y podría cambiar en cualquier momento sin actualizar este documento.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- GUI de Cisco Transport Controller (CTC)
- Conocimiento básico del servidor
- Comandos Linux/Unix básicos

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

En un nodo independiente/de varias estanterías

Configuración del modo authPriv en el dispositivo ONS15454/NCS2000

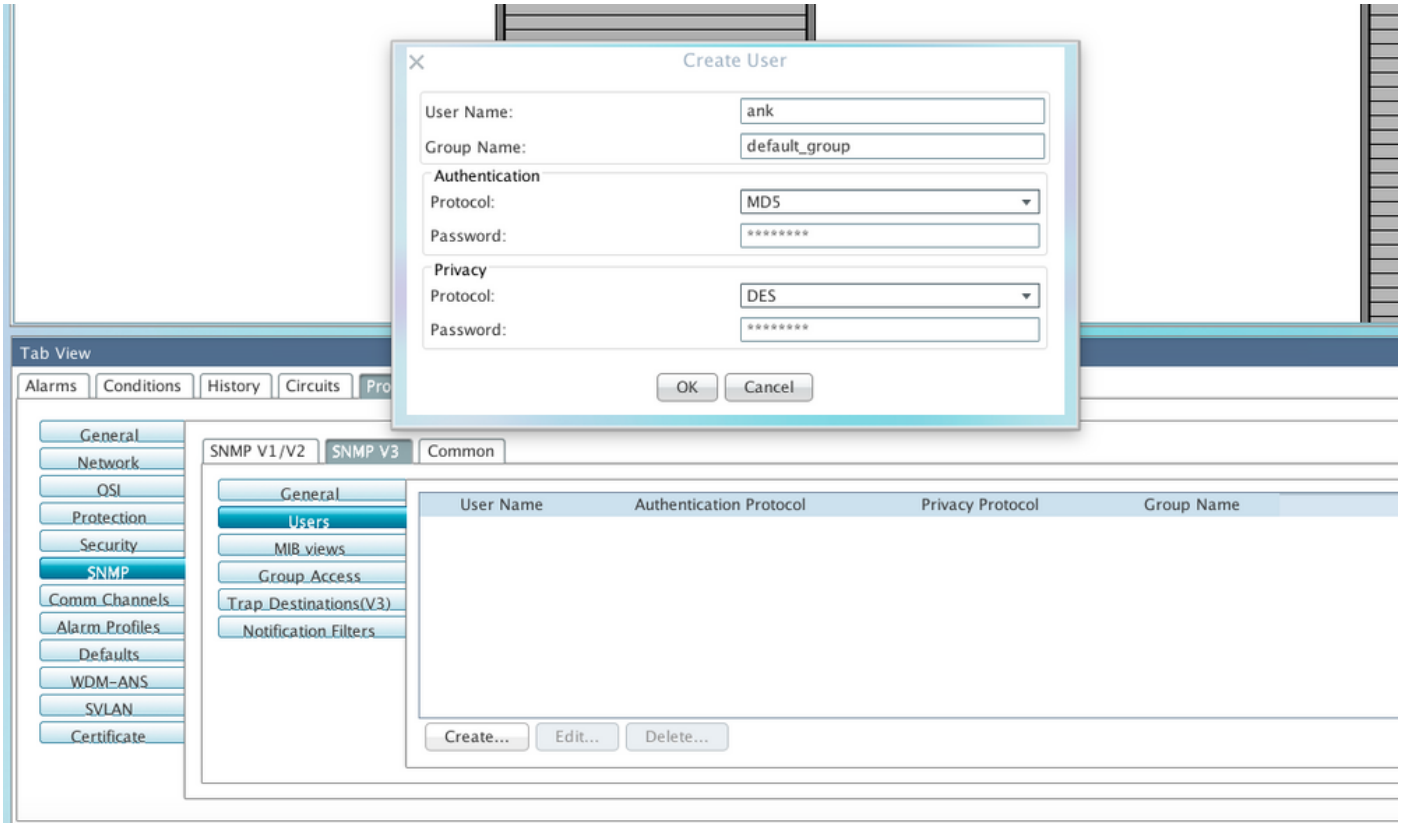
Paso 1. Inicie sesión en el nodo a través de CTC con las credenciales de superusuario.

Paso 2. Vaya a **Vista de nodos > Provisioning > SNMP > SNMP V3**.

Paso 3. Vaya a la pestaña **Usuarios**. Crear usuarios.

```
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>
```

Paso 4. Haga clic en **Aceptar** como se muestra en la imagen.



Especificaciones:

Nombre de usuario: especifique el nombre del usuario en el host que se conecta al agente. El nombre de usuario debe tener un mínimo de 6 y un máximo de 40 caracteres (hasta sólo 39 caracteres para la autenticación TACACS y RADIUS). Incluye caracteres alfanuméricos (a-z, A-Z, 0-9) y los caracteres especiales permitidos son @, "-" (guión) y "." (punto). Para la compatibilidad con TL1, el nombre de usuario debe tener entre 6 y 10 caracteres.

Group Name (Nombre de grupo): especifique el grupo al que pertenece el usuario.

Autenticación:

Protocol (Protocolo): Seleccione el algoritmo de autenticación que desea utilizar. Las opciones son NONE, MD5 y SHA.

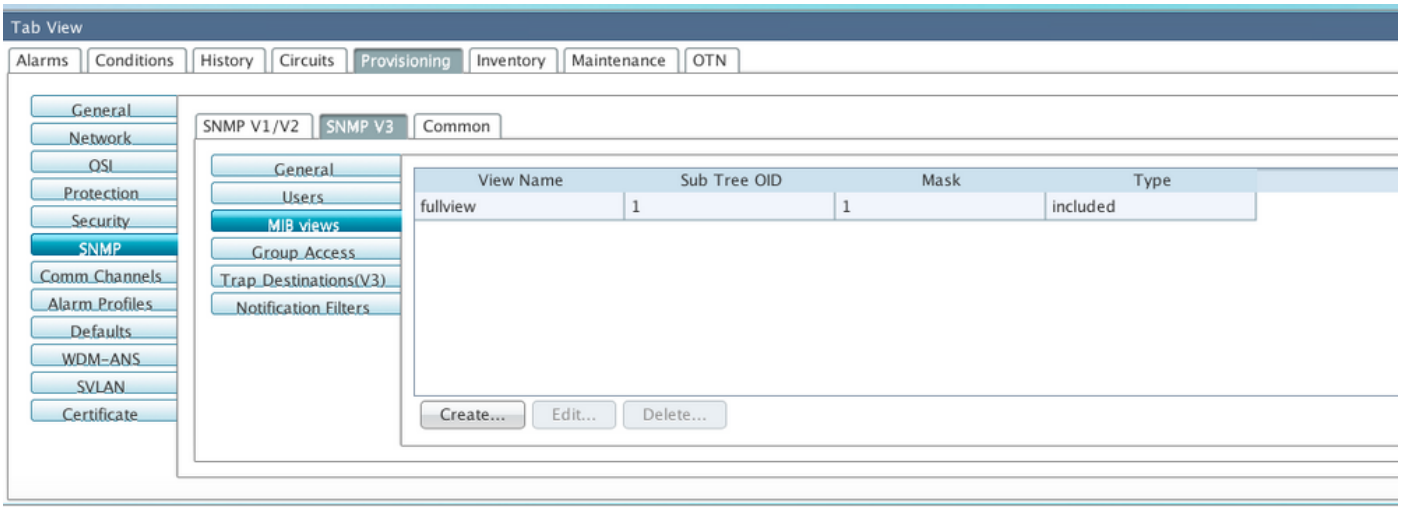
Password (Contraseña): Introduzca una contraseña si selecciona MD5 o SHA. De forma predeterminada, la longitud de la contraseña se establece en un mínimo de ocho caracteres.

Privacidad: inicia una sesión de configuración de nivel de autenticación de privacidad que permite al host cifrar el contenido del mensaje que se envía al agente.

Protocol (Protocolo): Seleccione el algoritmo de autenticación de privacidad. Las opciones disponibles son None, DES y AES-256-CFB.

Password (Contraseña): Introduzca una contraseña si selecciona un protocolo distinto de None (Ninguno).

Paso 5. Asegúrese de que las vistas MIB estén configuradas según esta imagen.



Especificaciones:

Nombre: nombre de la vista.

OID de subárbol - El subárbol MIB que, cuando se combina con la máscara, define la familia de subárboles.

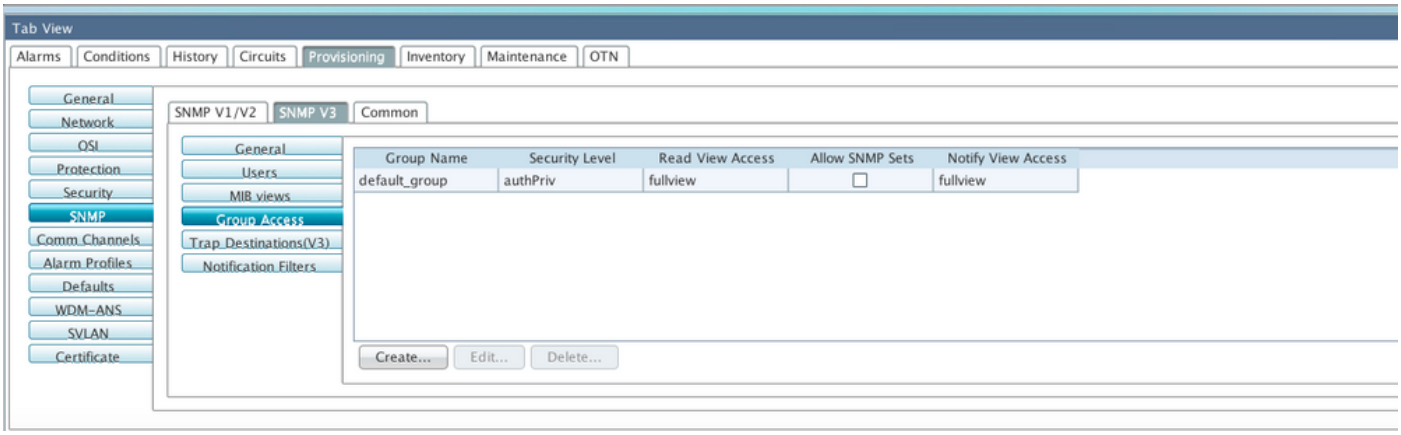
Máscara de bits: una familia de subárboles de vista. Cada bit de la Máscara de Bit corresponde a un sub-identificador del OID del subárbol.

Type (Tipo): Seleccione el tipo de vista. Las opciones se incluyen y excluyen.

El tipo define si la familia de subárboles definidos por el OID del subárbol y la combinación de Máscara de bits se incluyen o se excluyen del filtro de notificación.

Paso 6. Configure el acceso de grupo como se muestra en la imagen. De forma predeterminada, el nombre de grupo será default_group y el nivel de seguridad como authPriv.

Nota: El nombre de grupo debe ser el mismo que el utilizado al crear el usuario en el paso 3.



Especificaciones:

Group Name (Nombre de grupo): nombre del grupo SNMP o colección de usuarios que comparten una política de acceso común.

Nivel de seguridad: nivel de seguridad para el que se definen los parámetros de acceso. Seleccione entre estas opciones:

noAuthNoPriv: utiliza una coincidencia de nombre de usuario para la autenticación.

AuthNoPriv - Proporciona autenticación basada en los algoritmos HMAC-MD5 o HMAC-SHA.

AuthPriv - Proporciona autenticación basada en los algoritmos HMAC-MD5 o HMAC-SHA. Proporciona cifrado DES de 56 bits basado en el estándar CBC-DES (DES-56), además de autenticación.

Si selecciona authNoPriv o authPriv para un grupo, el usuario correspondiente debe configurarse con un protocolo de autenticación y una contraseña, con protocolo de privacidad y contraseña, o ambos.

Vistas

Leer el nombre de la vista: leer el nombre de la vista del grupo.

Notificar nombre de vista: notifica el nombre de vista del grupo.

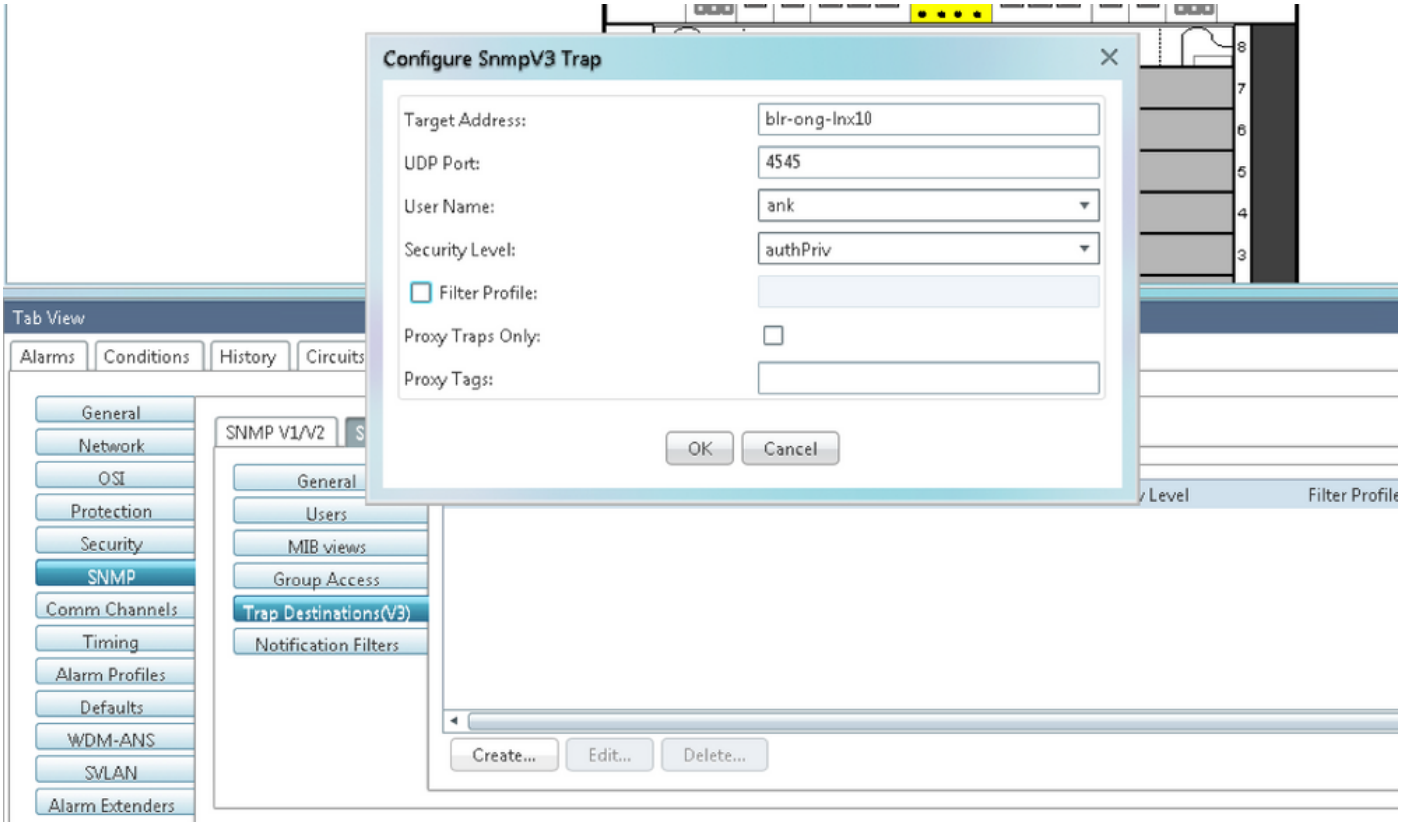
Allow SNMP sets (Permitir conjuntos SNMP): Active esta casilla de verificación si desea que el agente SNMP acepte solicitudes SNMP SET. Si esta casilla de verificación no está activada, se rechazarán las solicitudes SET.

Nota: El acceso de solicitud SNMP SET se implementa para muy pocos objetos.

Paso 7. Vaya a **Node View > Provisioning > SNMP > SNMP V3 > Trap Destination (V3)**. Haga clic en **Crear** y **Configurar**.

```
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
```

Paso 8. Haga clic en **Aceptar** como se muestra en la imagen.



Nota: blr-ong-lnx10 es el servidor NMS.

Especificaciones:

Dirección de destino: Destino al que se deben enviar las trampas. Utilice una dirección IPv4 o IPv6.

Puerto UDP: número de puerto UDP que utiliza el host. El valor predeterminado es 162.

Nombre de usuario: especifique el nombre del usuario en el host que se conecta al agente.

Nivel de seguridad: seleccione una de estas opciones:

noAuthNoPriv: utiliza una coincidencia de nombre de usuario para la autenticación.

AuthNoPriv - Proporciona autenticación basada en los algoritmos HMAC-MD5 o HMAC-SHA.

AuthPriv - Proporciona autenticación basada en los algoritmos HMAC-MD5 o HMAC-SHA. Proporciona cifrado DES de 56 bits basado en el estándar CBC-DES (DES-56), además de autenticación.

Filter Profile (Perfil de filtro): active esta casilla de verificación e introduzca el nombre del perfil de filtro. Las trampas se envían sólo si se proporciona un nombre de perfil de filtro y se crea un filtro de notificación.

Proxy Traps Only (Sólo capturas de proxy): si se selecciona, sólo reenvía las trampas de proxy del ENE. Las trampas de este nodo no se envían al destino de trampa identificado por esta entrada.

Etiquetas de proxy: especifique una lista de etiquetas. La lista de etiquetas es necesaria en un GNE sólo si un ENE necesita enviar trampas al destino de trampa identificado por esta entrada y

desea utilizar el GNE como proxy.

Configuración del servidor NMS (blr-ong-lnx10)

Paso 1. En el directorio de inicio del servidor, cree un directorio con el nombre **snmp**.

Paso 2. Bajo este directorio, cree un archivo **snmptrapd.conf**.

Paso 3. Cambie el archivo **snmptrapd.conf** a:

```
vi snmptrapd.conf

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

Por ejemplo:

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

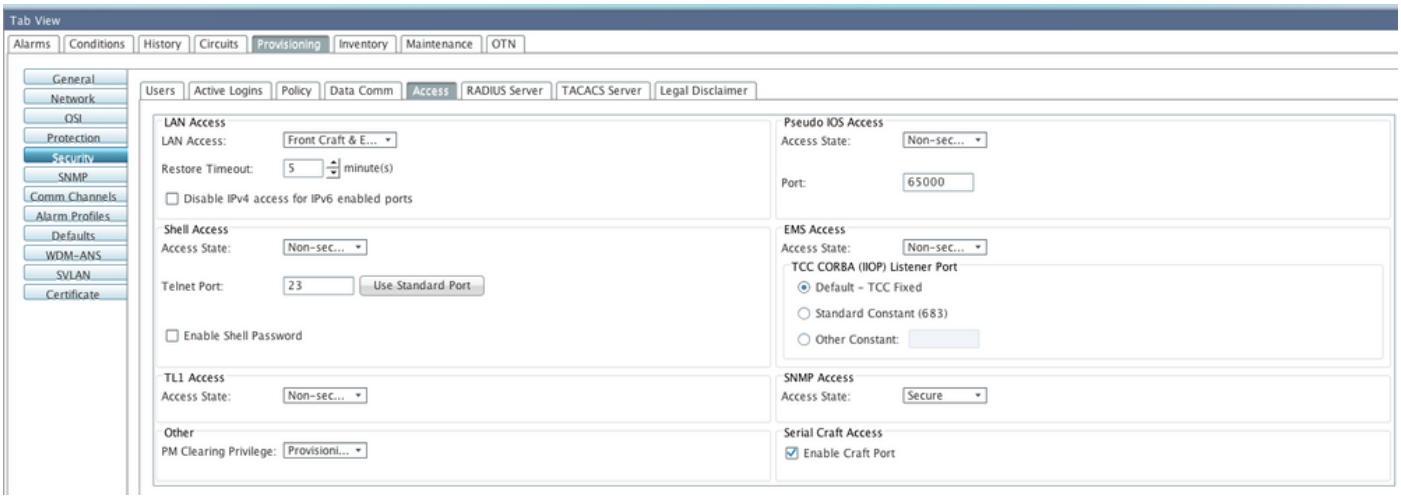
En este ejemplo:

```
user_name=ank

MD5 password = cisco123

DES password  = cisco123

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

Node view > Provisioning > SNMP > SNMP V3 > General

Verificar el modo authPriv

Paso 1. En CTC, navegue hasta **Node View > Provisioning > Security > Access > change snmp access state to Secure** como se muestra en la imagen.



Paso 2. Navegue hasta el servidor NMS y haga snmpwalk.

Sintaxis:

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

```
<MIB>
```

Ejemplo:

```
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
```

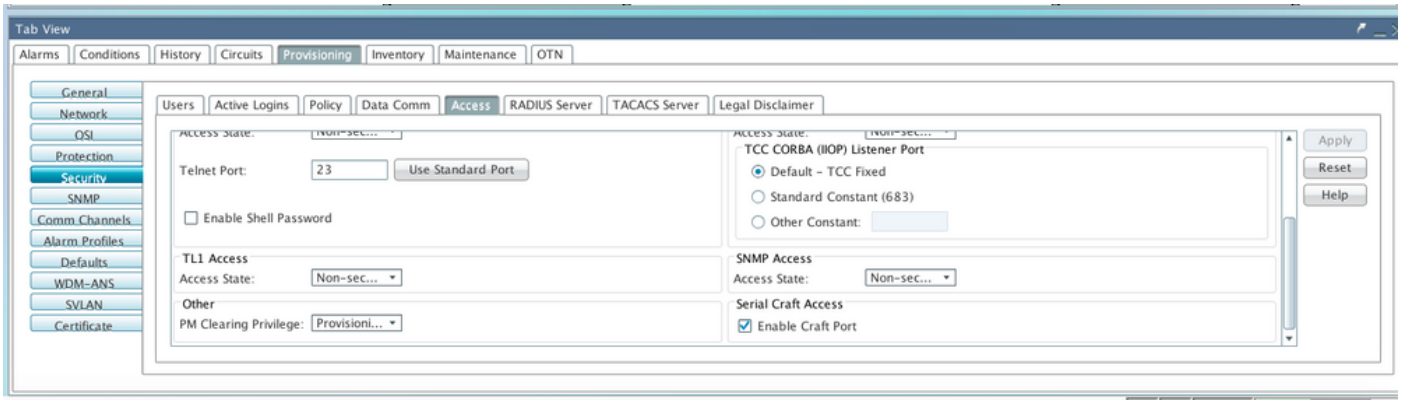
Trampa SNMP:

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

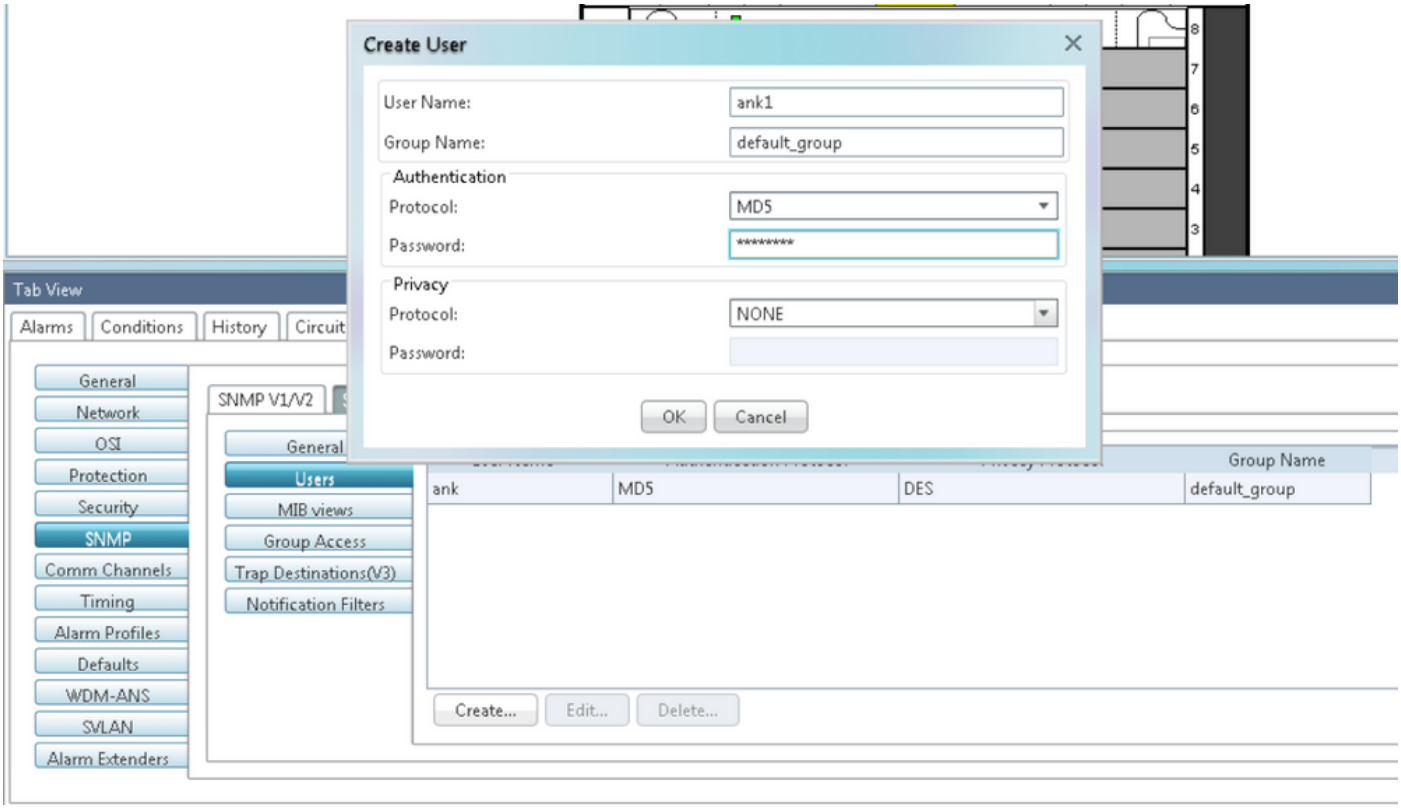
Trap cmd es el mismo para todas las versiones.

Configuración del modo authNoPriv en el dispositivo ONS15454/NCS2000

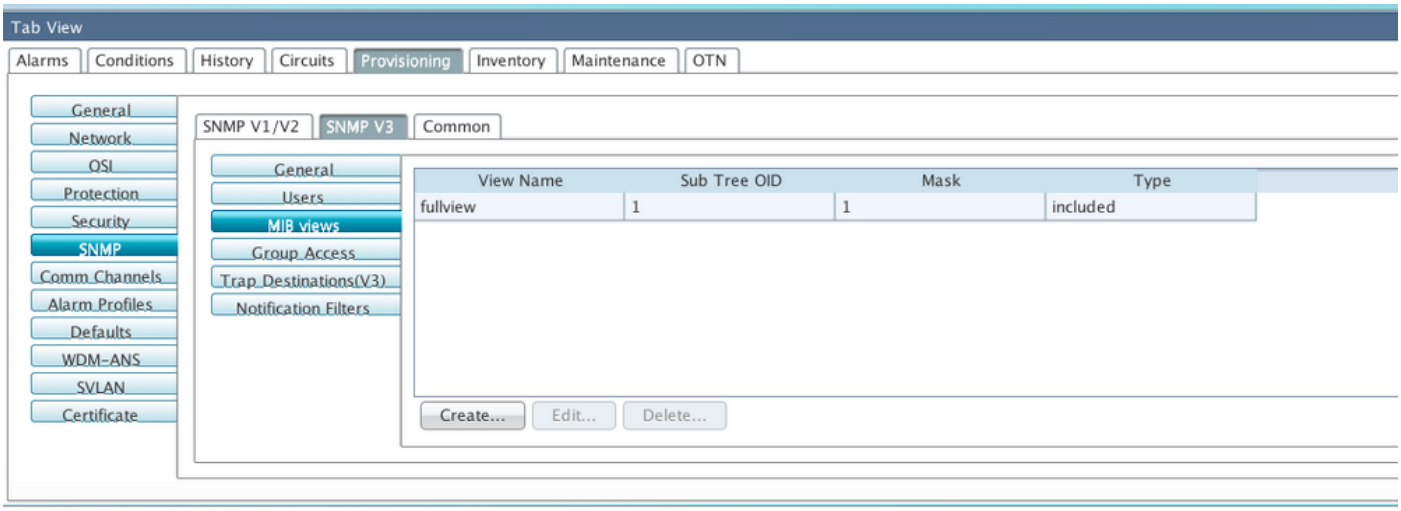
Paso 1. En CTC, navegue hasta **Node View > Provisioning > Security > Access > change snmp access state to Non-secure mode** como se muestra en la imagen.



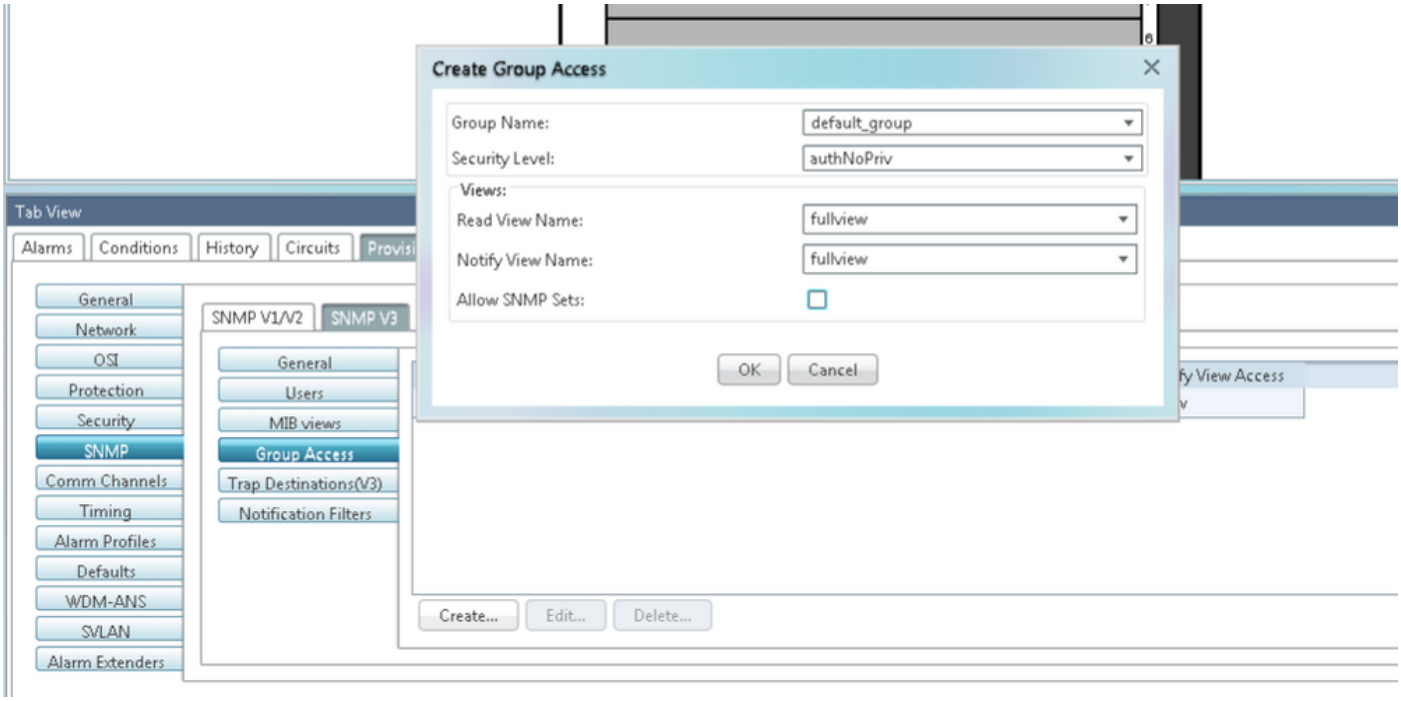
Paso 2. Vaya a **Node View > Provisioning > SNMP > SNMP V3 > Users > Create User** y configure como se muestra en la imagen.



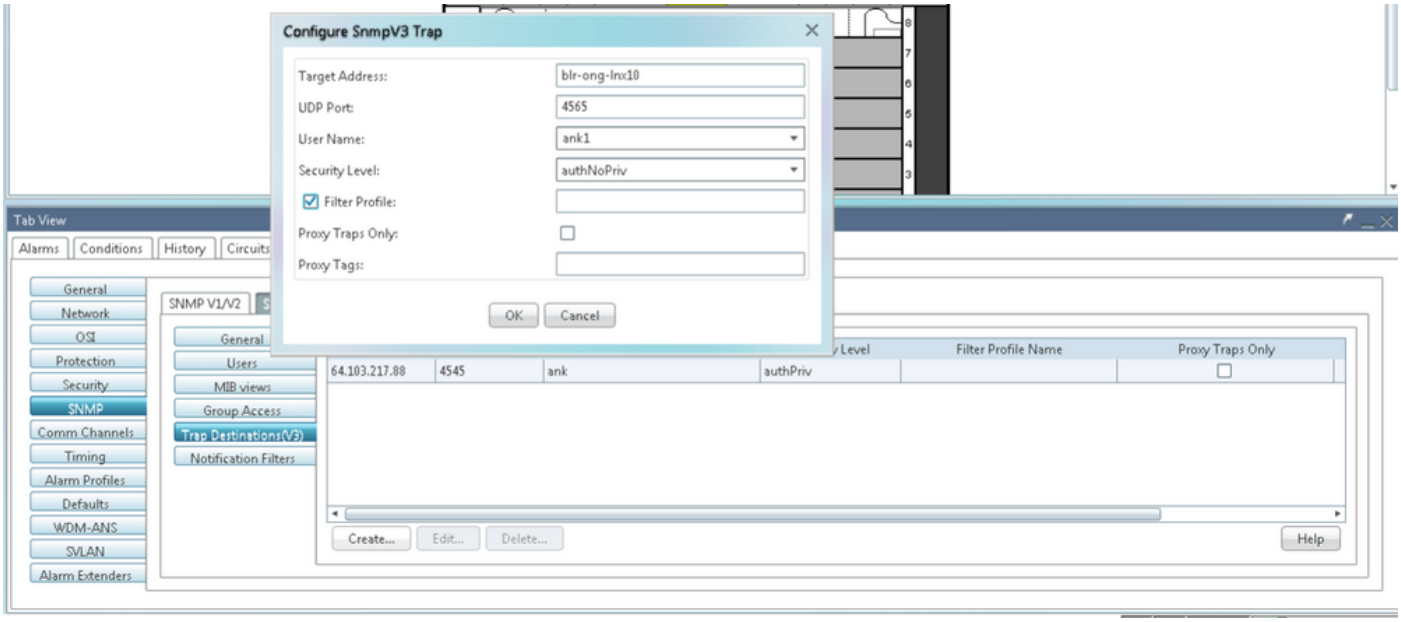
Paso 3. Asegúrese de que las vistas MIB estén configuradas como se muestra en la imagen.



Paso 4. Configure Group Access como se muestra en la imagen para el modo authnopriv.



Paso 5. Vaya a **Node View > Provisioning > SNMP > SNMP V3 > Trap Destination (V3)**. Haga clic en **Crear** y **Configurar** como se muestra en la imagen.



Verificar el modo authNoPriv

Paso 1. Navegue hasta el servidor NMS y haga snmpwalk.

Sintaxis:

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

Ejemplo:

```
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
```

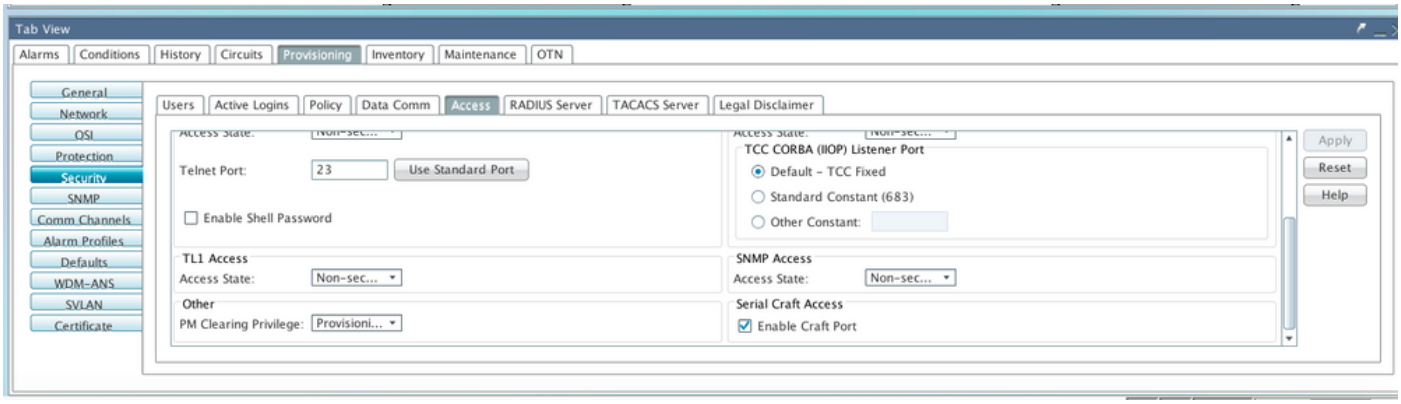
Trampa SNMP:

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

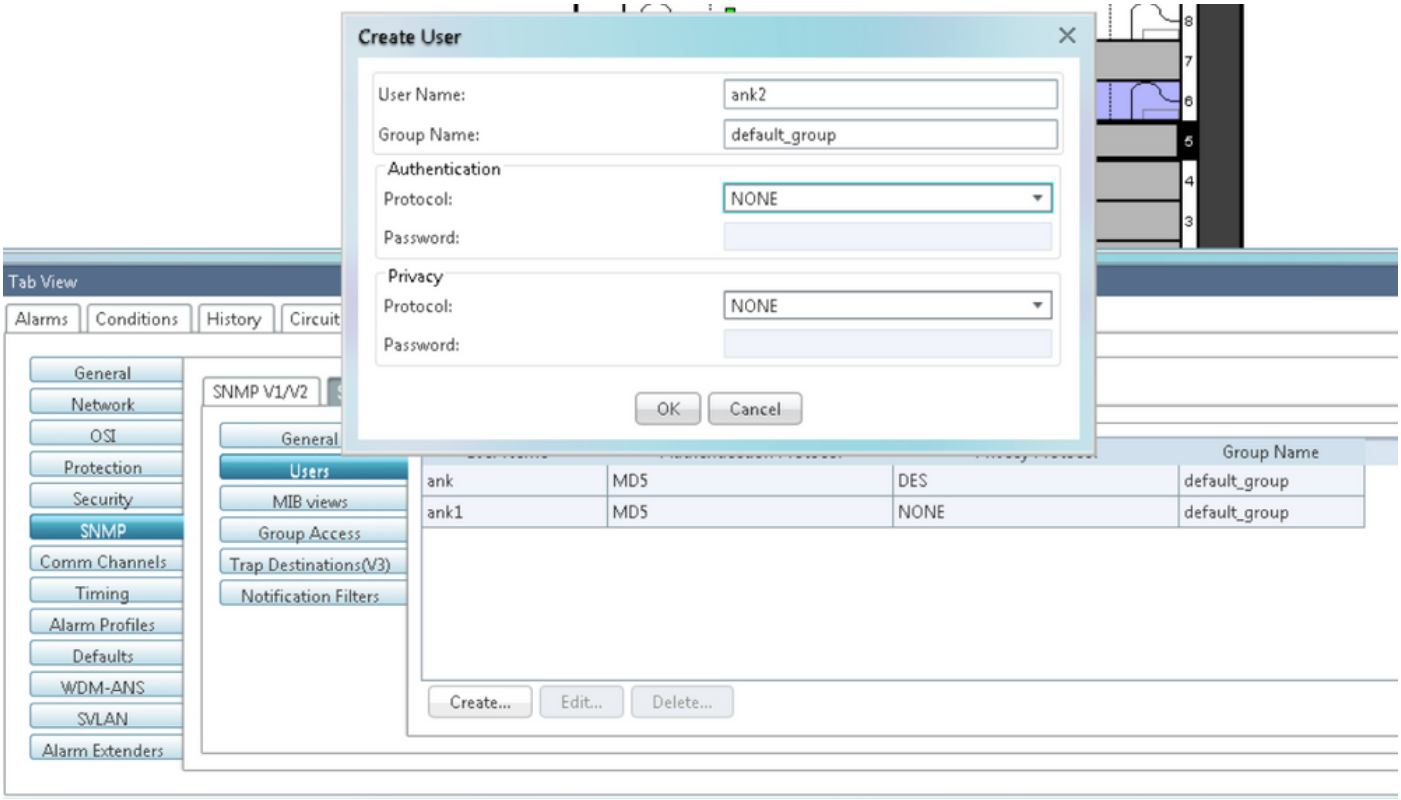
Trap cmd es el mismo para todas las versiones.

Configuración del modo noAuthNoPriv en el dispositivo ONS15454/NCS2000

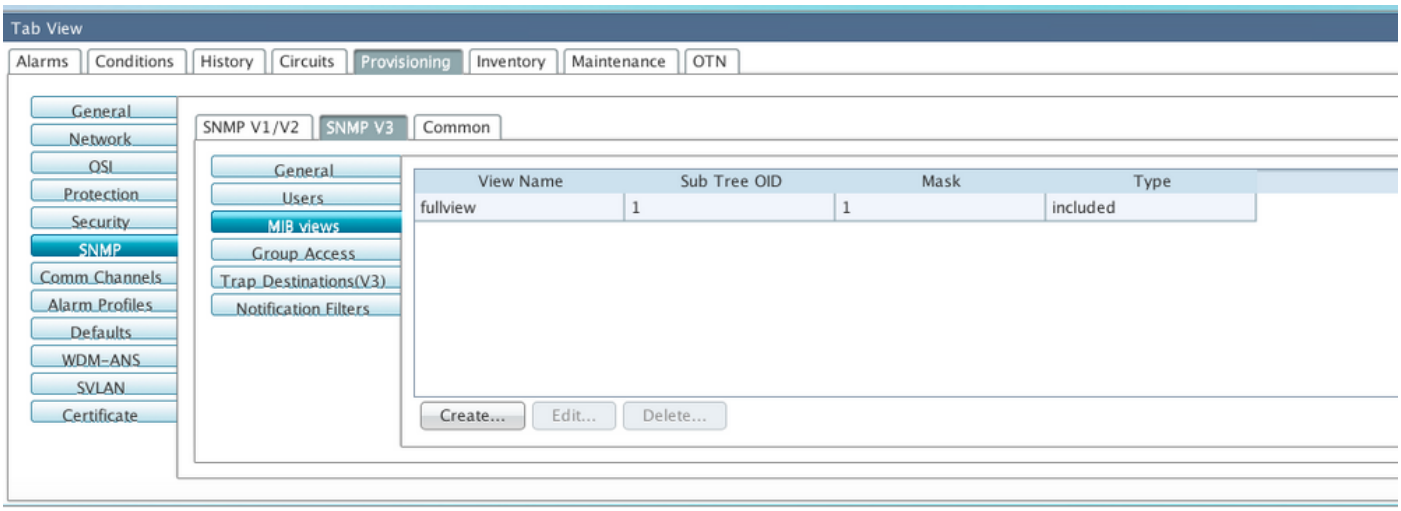
Paso 1. En CTC, navegue hasta **Node View > Provisioning > Security > Access > change snmp access state to Non-secure mode** como se muestra en la imagen.



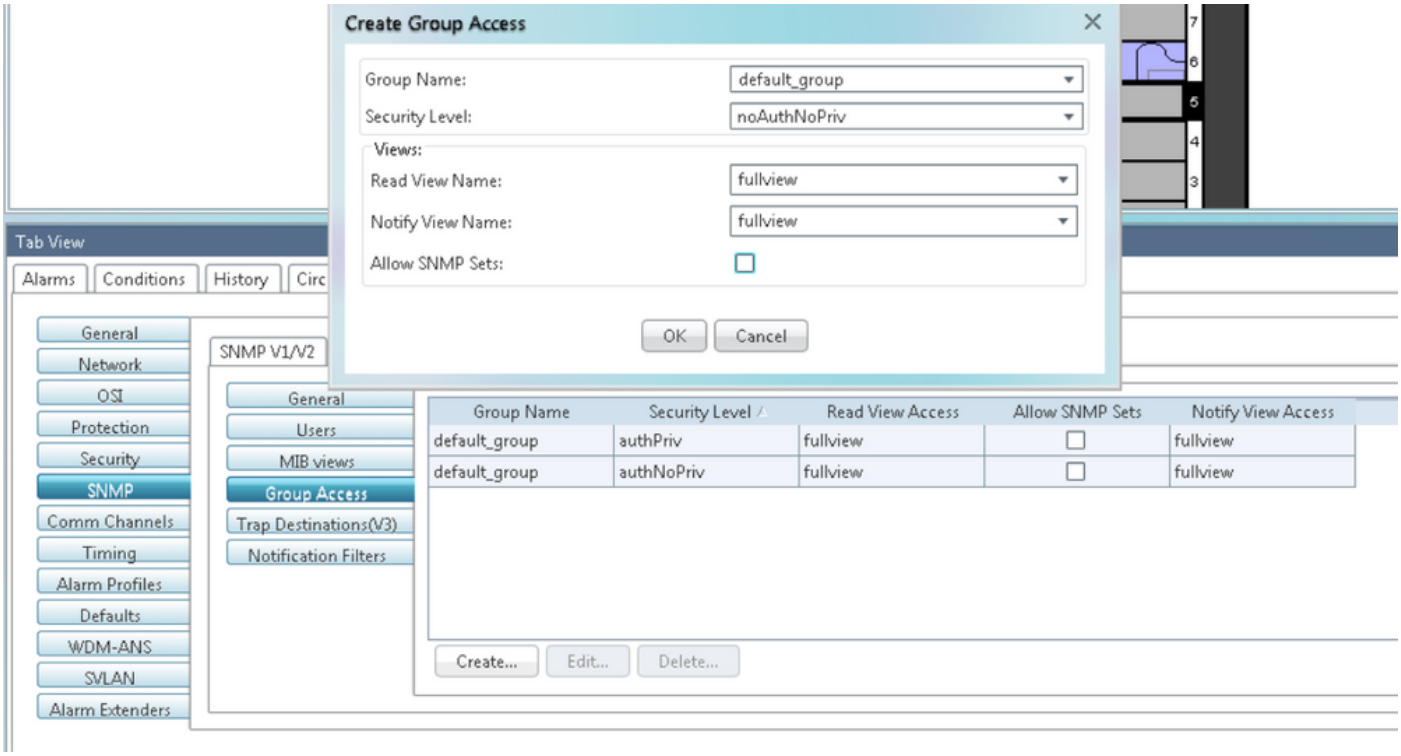
Paso 2. Vaya a **Node View > Provisioning > SNMP > SNMP V3 > Users > Create User and Configure** como se muestra en la imagen.



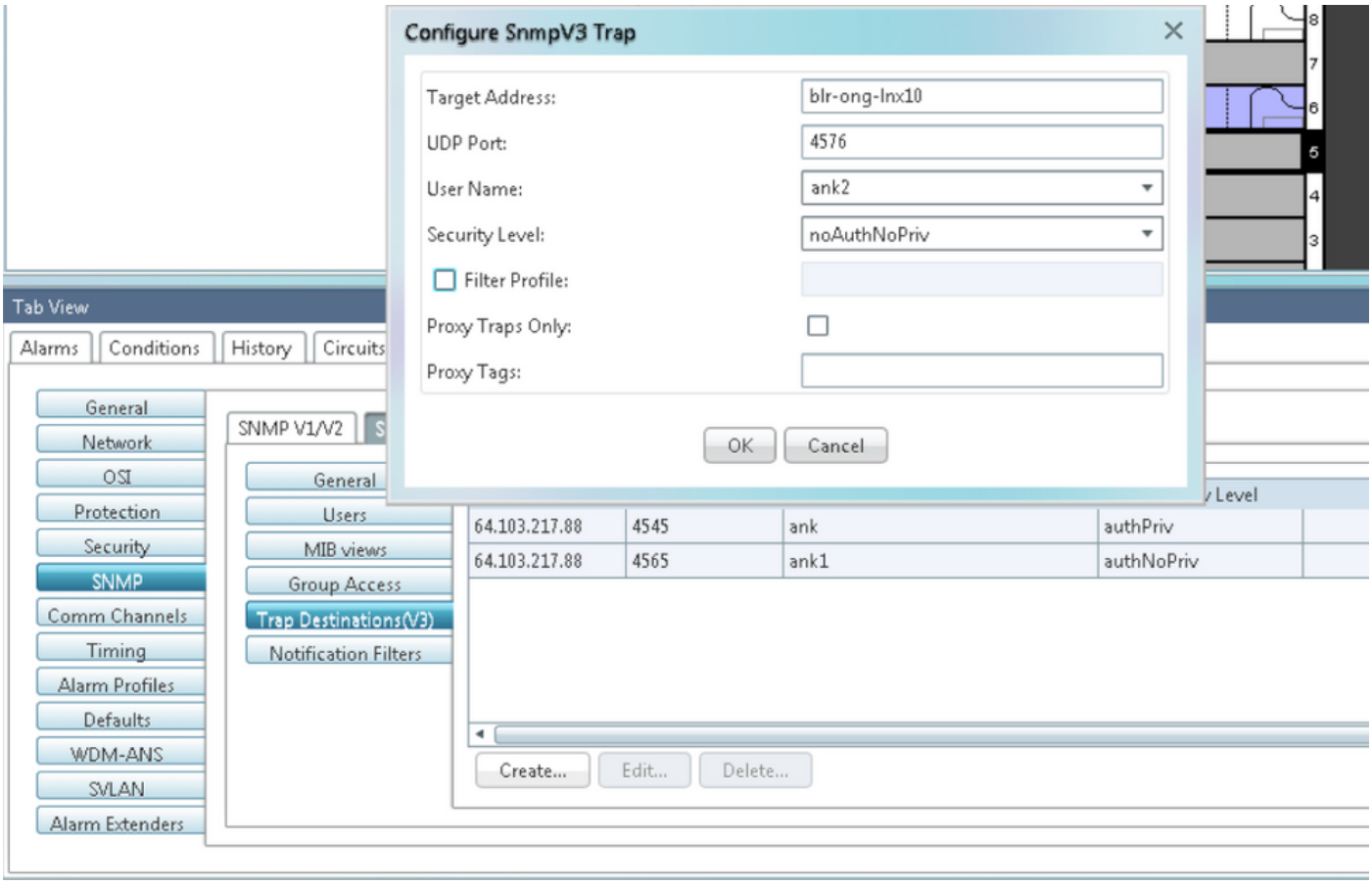
Paso 3. Asegúrese de que **las vistas MIB** se configuran como se muestra en la imagen.



Paso 4. Configure el acceso de grupo como se muestra en la imagen para el modo no authnopriv.



Paso 5. Vaya a **Node View > Provisioning > SNMP > SNMP V3 > Trap Destination (V3)**. Haga clic en **Crear** y **Configurar** como se muestra en la imagen.



Verificar el modo noAuthNoPriv

Paso 1. Navegue hasta el servidor NMS y haga snmpwalk.

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

Ejemplo:

```
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>
```

Trampa SNMP:

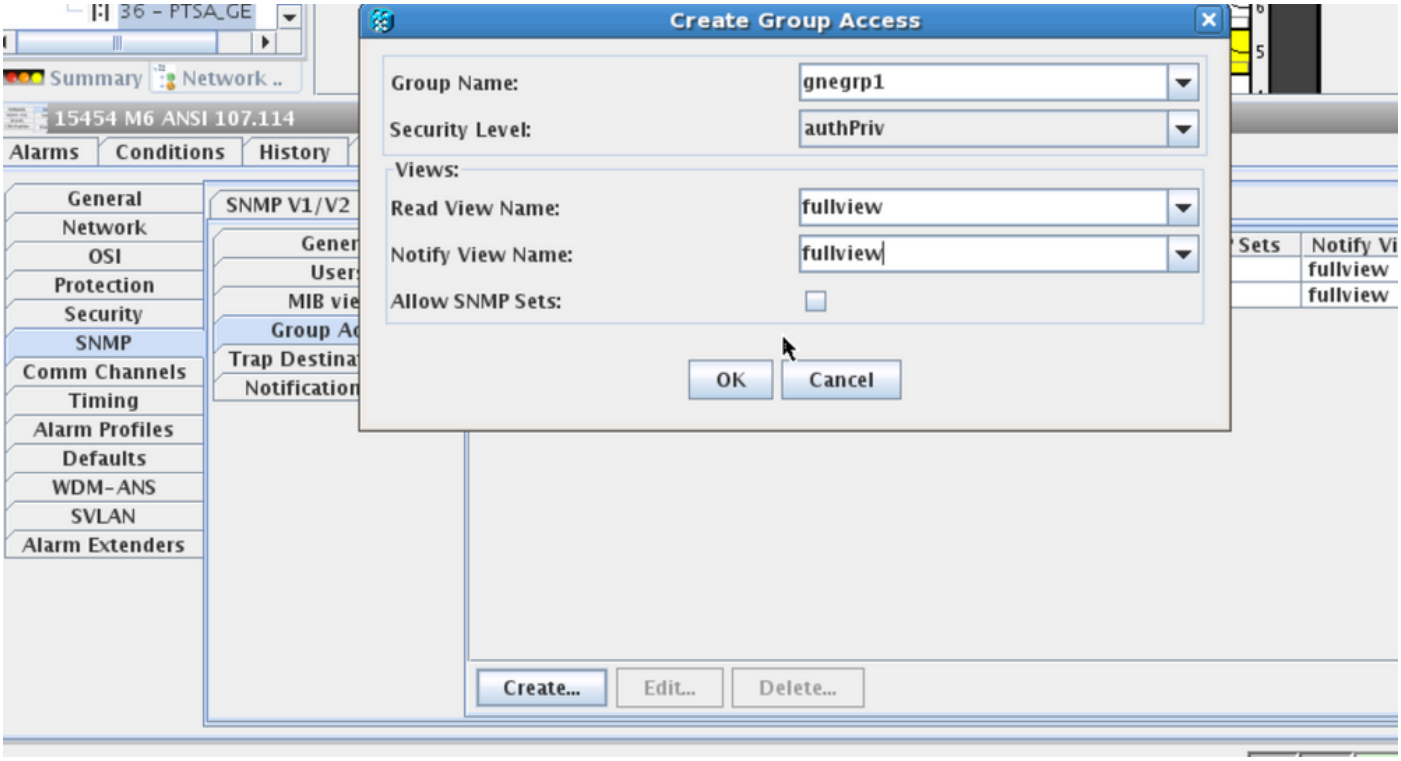
```
snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n" <port number>
```

Trap cmd es el mismo para todas las versiones.

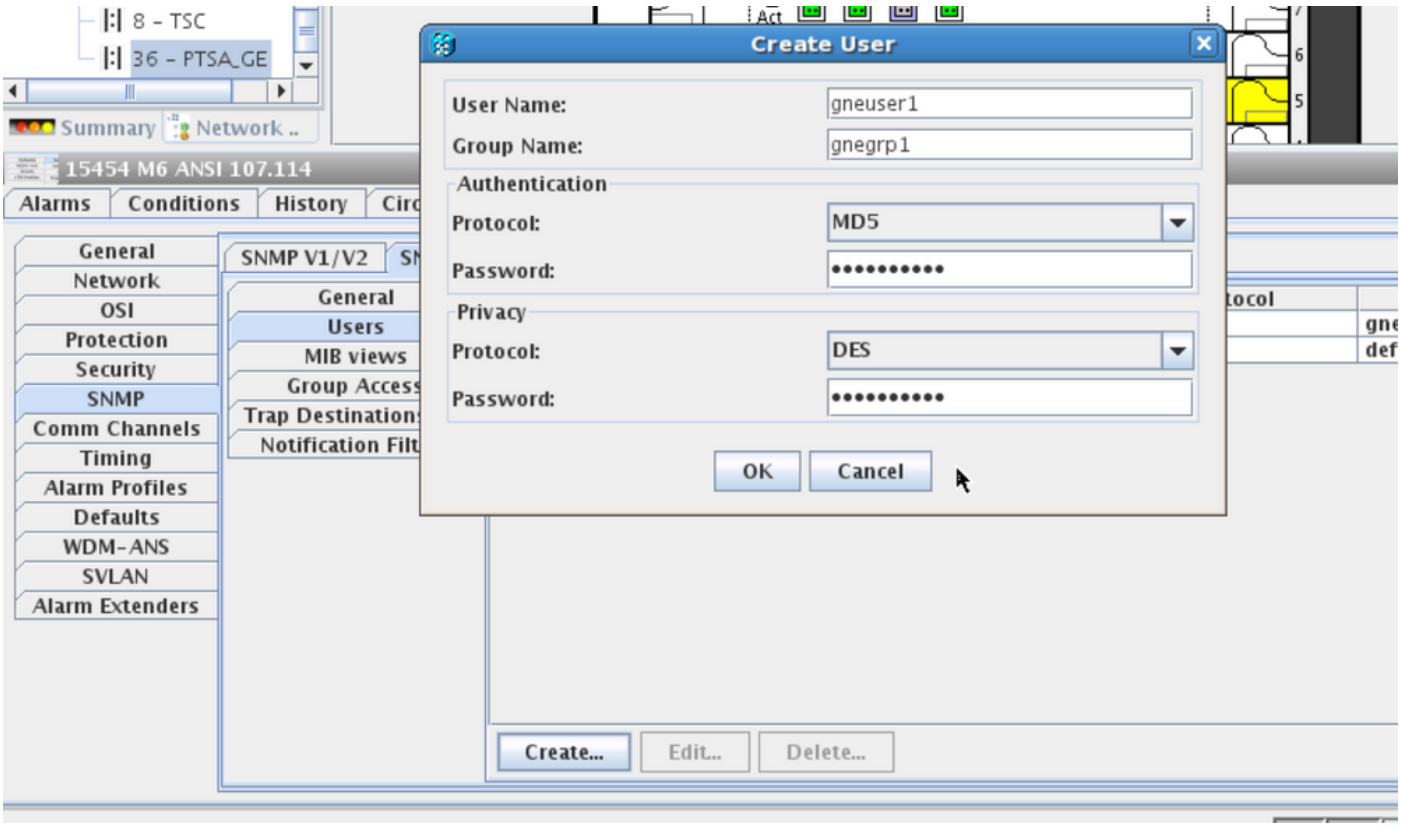
Trampa SNMP V3 para la configuración GNE/ENE

En el nodo GNE

Paso 1. Vaya a **Provisioning > SNMP > SNMP V3 y CCrear acceso de grupo (ficha Acceso de grupo): proporcione un nombre de grupo con el nivel de seguridad (noAuthnoPriv|AuthnoPriv|authPriv) y la vista completa Leer y notificar acceso, como se muestra en la imagen.**



Paso 2. Crear acceso de usuario (ficha Usuarios): cree un usuario con el mismo nombre de grupo que el creado anteriormente en la ficha Acceso de grupo. También, proporcione la autenticación basada en el nivel de acceso como se muestra en la imagen.



Paso 3. Ficha Destino de trampa (V3):

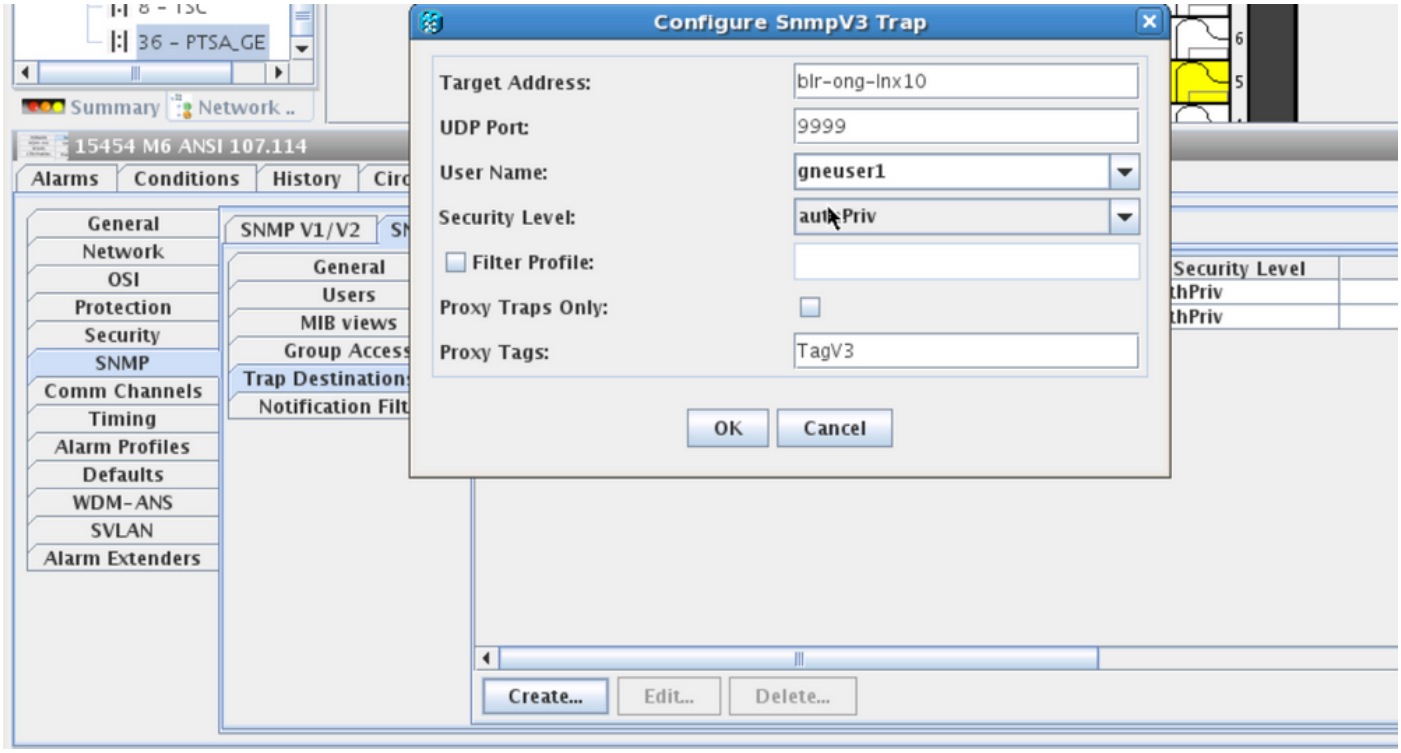
Dirección de destino: Dirección del servidor NMS desde el que se ejecutará la trampa(p. ej. Blr-ong-lnx10).

Puerto UDP: Cualquier número de puerto en el que se escuche la trampa(p. ej. 9977).

User Name: Nombre del usuario en la ficha Usuario.

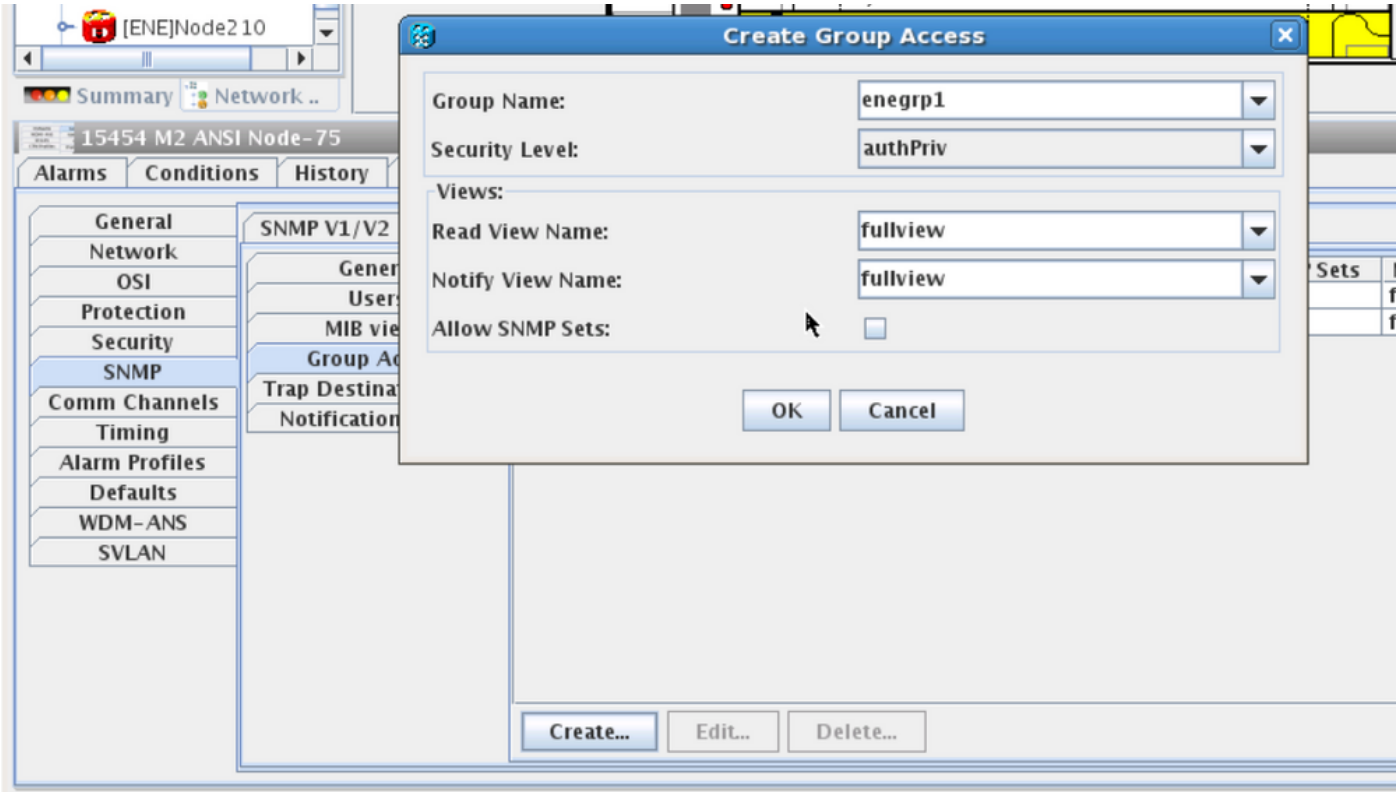
Nivel de seguridad: Tal y como se configuró anteriormente en la ficha Usuario.

Etiquetas de proxy: Proporcione una etiqueta de proxy (p. ej. Tag75).

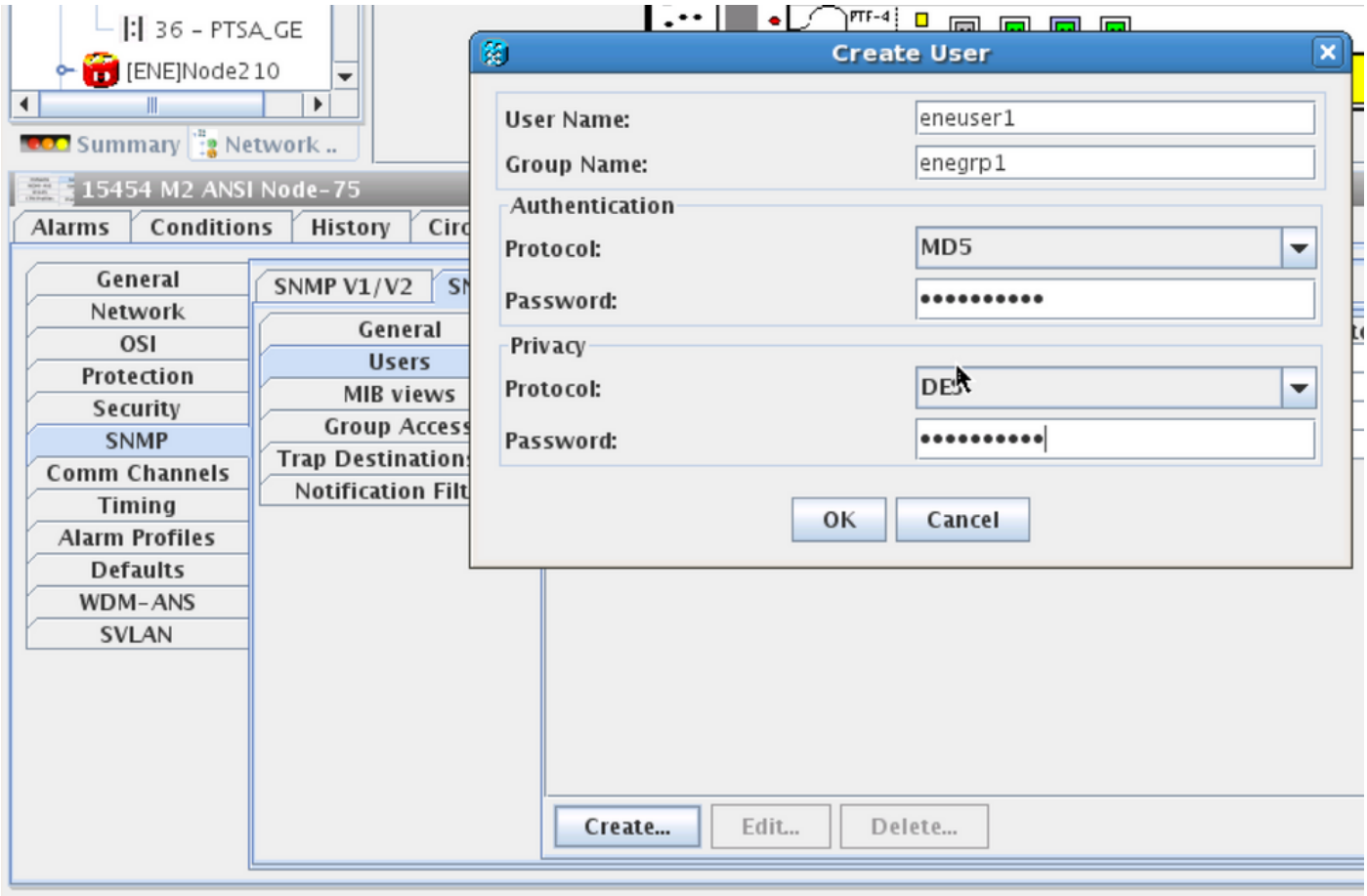


En el nodo ENE

Paso 1. Vaya a **Provisioning > SNMP > SNMP V3** y **Create Group Access** (Ficha Group Access): proporcione un nombre de grupo con acceso de nivel de acceso (noAuthnoPriv|AuthnoPriv|authPriv) y vista completa Leer y notificar, como se muestra en la imagen.



Paso 2. Crear acceso de usuario (ficha Usuarios): cree un usuario con el mismo nombre de grupo que el creado anteriormente en la ficha Acceso de grupo. También, proporcione la autenticación basada en el nivel de acceso.



Asegúrese de que se cree un grupo_predeterminado si se muestra en la ficha Usuario en la ficha Acceso de grupo en caso de que falte en la ficha Acceso de grupo.

Paso 3. Ficha Destino de trampa (V3):

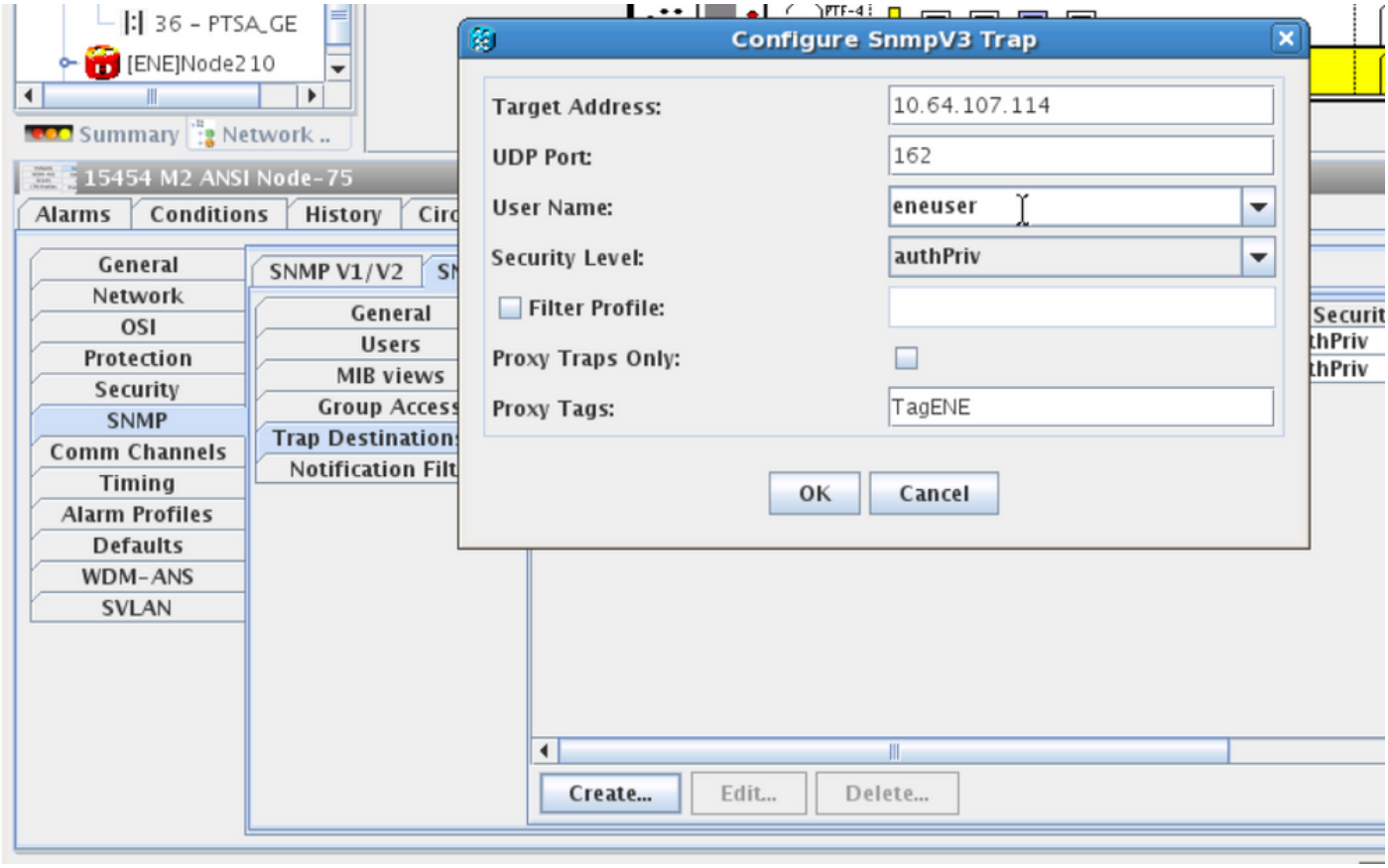
Dirección de destino: IP del nodo GNE.

Puerto UDP: 162.

User Name: Nombre del usuario en la ficha Usuario.

Nivel de seguridad: Tal y como se configuró anteriormente en la ficha Usuario.

Etiquetas de proxy: Proporcione cualquier etiqueta proxy igual que GNE (p. ej. Tag75).



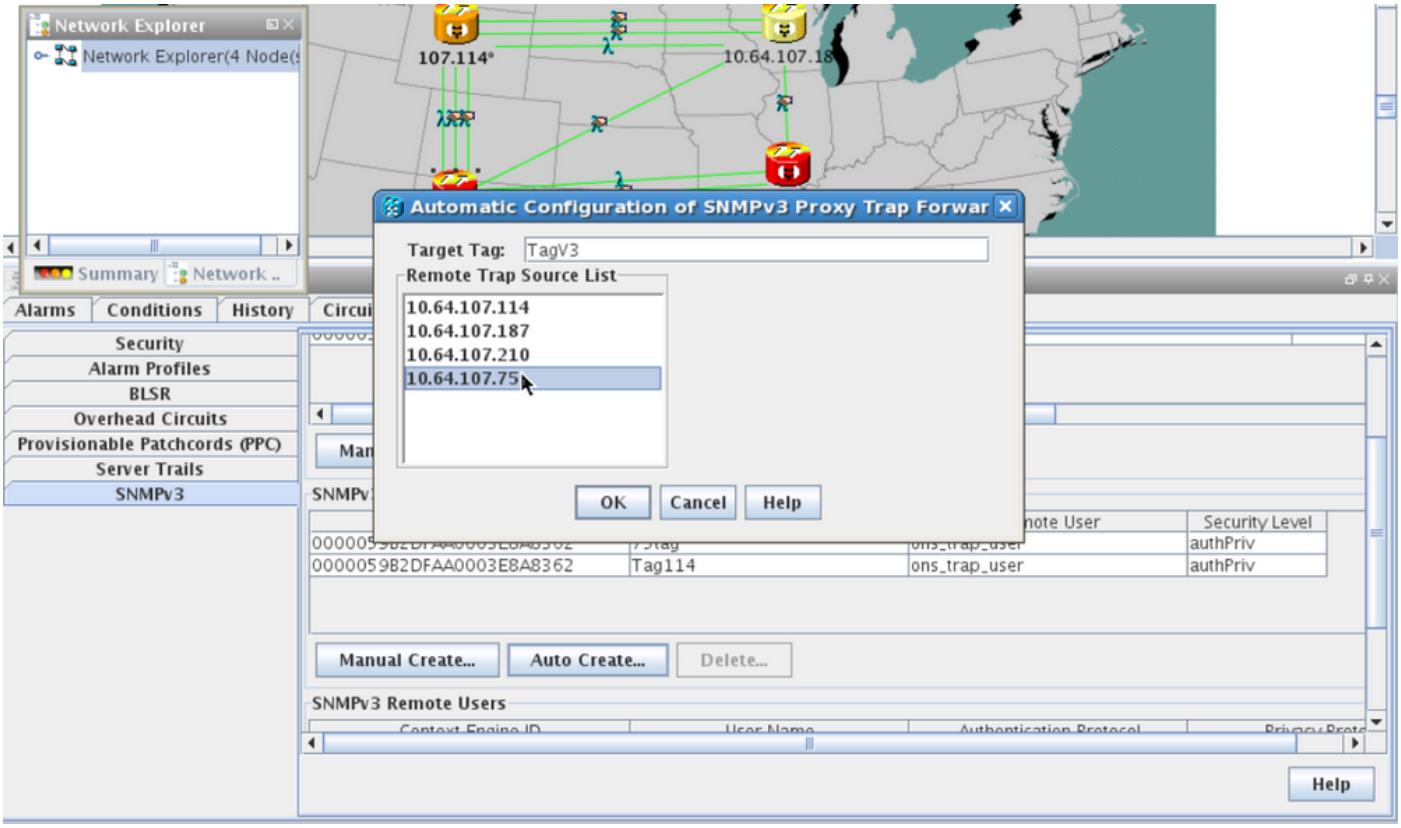
En CTC, vaya a la vista de red:

Paso 1. Vaya a la pestaña **SNMPv3**.

Paso 2. Tabla de Reenvío de Trampa de Proxy SNMPv3: Puede hacer **Manual** o **Auto Create**.

Seleccione **Auto Create**. En ese sentido:

- Etiqueta objetivo: Etiqueta proxy establecida en GNE.
- Lista de origen de trampa remota: seleccione la IP del nodo ENE como se muestra en la imagen.



Verificar la configuración de GNE/ENE

Configuración del servidor NMS (blr-ong-lnx10):

Paso 1. En el directorio de inicio del servidor, cree un directorio y asígnele el nombre **snmp**.

Paso 2. Bajo este directorio, cree un archivo **snmptrapd.conf**.

Paso 3. En **snmptrapd.conf**, cree esta configuración:

```
createUser -e 0x

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

Trampa SNMP:

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

snmpwalk en ENE:

Para el modo authpriv:

```
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>
```

Para el modo authnopriv:

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

Para el modo noauthnopriv:

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

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.