Configurazione di SNMPv3 su Catalyst SD-WAN

Sommario

Introduzione

Questo documento descrive la configurazione di SNMPv3 e spiega la sicurezza (autenticazione), la crittografia (privacy) e le restrizioni (visualizzazione).

Introduzione

Spesso la configurazione di SNMPv3 è considerata complessa e difficile da configurare, fino a quando non si sa quali operazioni è necessario eseguire. Il motivo per cui SNMPv3 esiste è simile a HTTPS: per la protezione, la crittografia e la restrizione.

Prerequisiti

Conoscenza dei modelli di funzionalità SD-WAN e dei modelli di dispositivo.

Informazioni generali su SNMP MIB, SNMP Poll e SNMP Walk

Requisiti

Controller SD-WAN

Cisco Edge Router

Componenti usati

Controller SD-WAN su 20.9

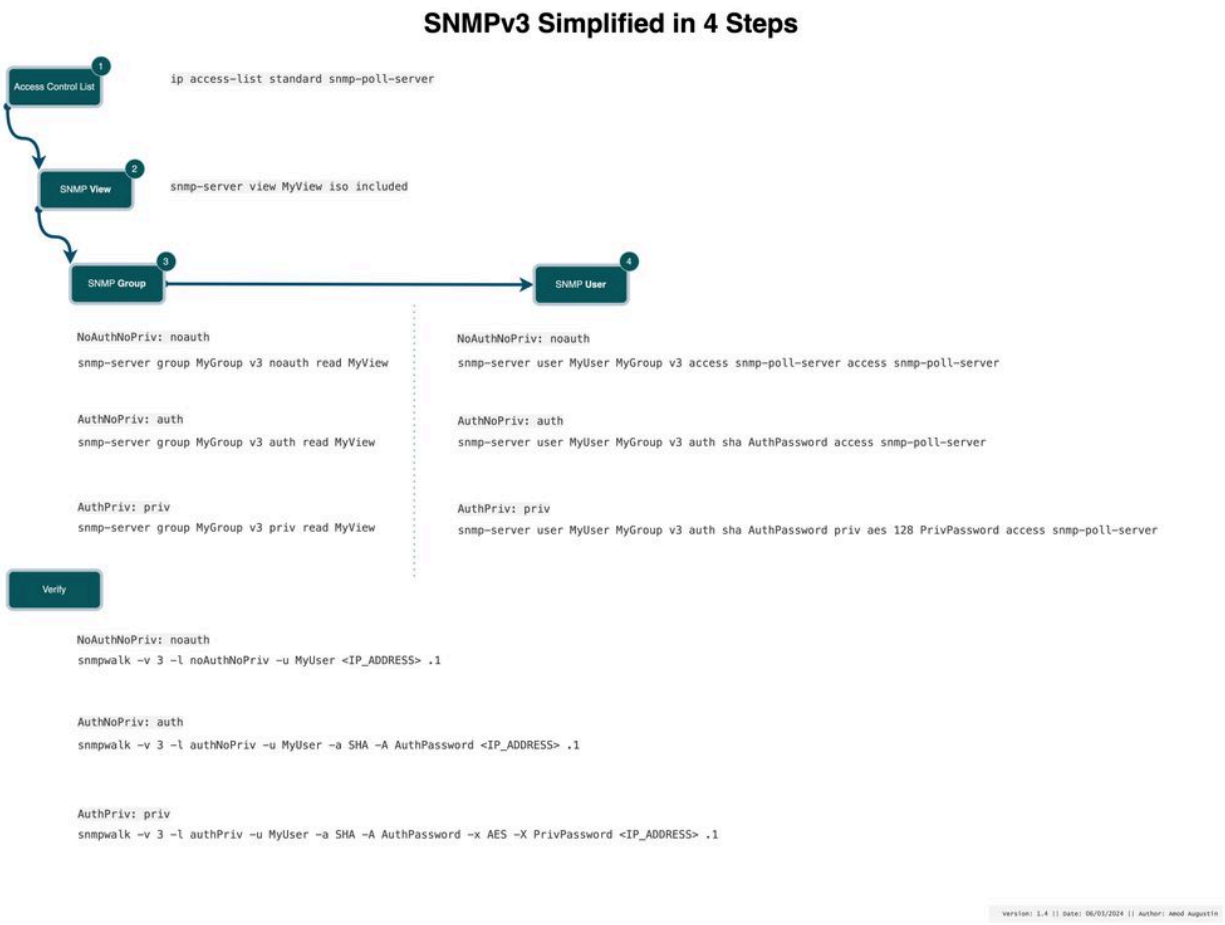
Cisco Edge Router su 17.9

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

Il diagramma consente di comprendere tutto ciò che è necessario per configurare SNMPv3 da un punto di supporto CLI.



- SNMPv3 semplificato in 4 passaggi

Una volta compreso il concetto, è facile inserirlo nella CLI o in un modello di funzionalità. Ci immergiamo.

Passaggio 1:

Configurare un ACL per consentire agli utenti di eseguire il polling del sistema (nel nostro caso, un router).

```
ip access-list standard snmp-poll-server
```

Passaggio 2:

Definire una visualizzazione snmp, poiché il termine indica a quali mibs ha accesso il poller, questa è la nostra restrizione.

```
snmp-server view MyView iso included
```

Passaggio 3:

Definire il gruppo snmp. Il gruppo snmp è composto principalmente da due parti a. Livello di protezione b. Restrizione (visualizzazione).

Livelli di protezione:

- noAuthNoPriv: Nessuna autenticazione e nessuna privacy (nessuna crittografia).
- authNoPriv: È necessaria l'autenticazione, ma non la privacy.
- authPriv: Sono richieste sia l'autenticazione che la privacy.

La restrizione è ciò che abbiamo definito al Passo 2, mettiamoli tutti insieme.

```
!NoAuthNoPriv: noauth
snmp-server group MyGroup v3 noauth read MyView

!AuthNoPriv: auth
snmp-server group MyGroup v3 auth read MyView

!AuthPriv: priv
snmp-server group MyGroup v3 priv read MyView
```

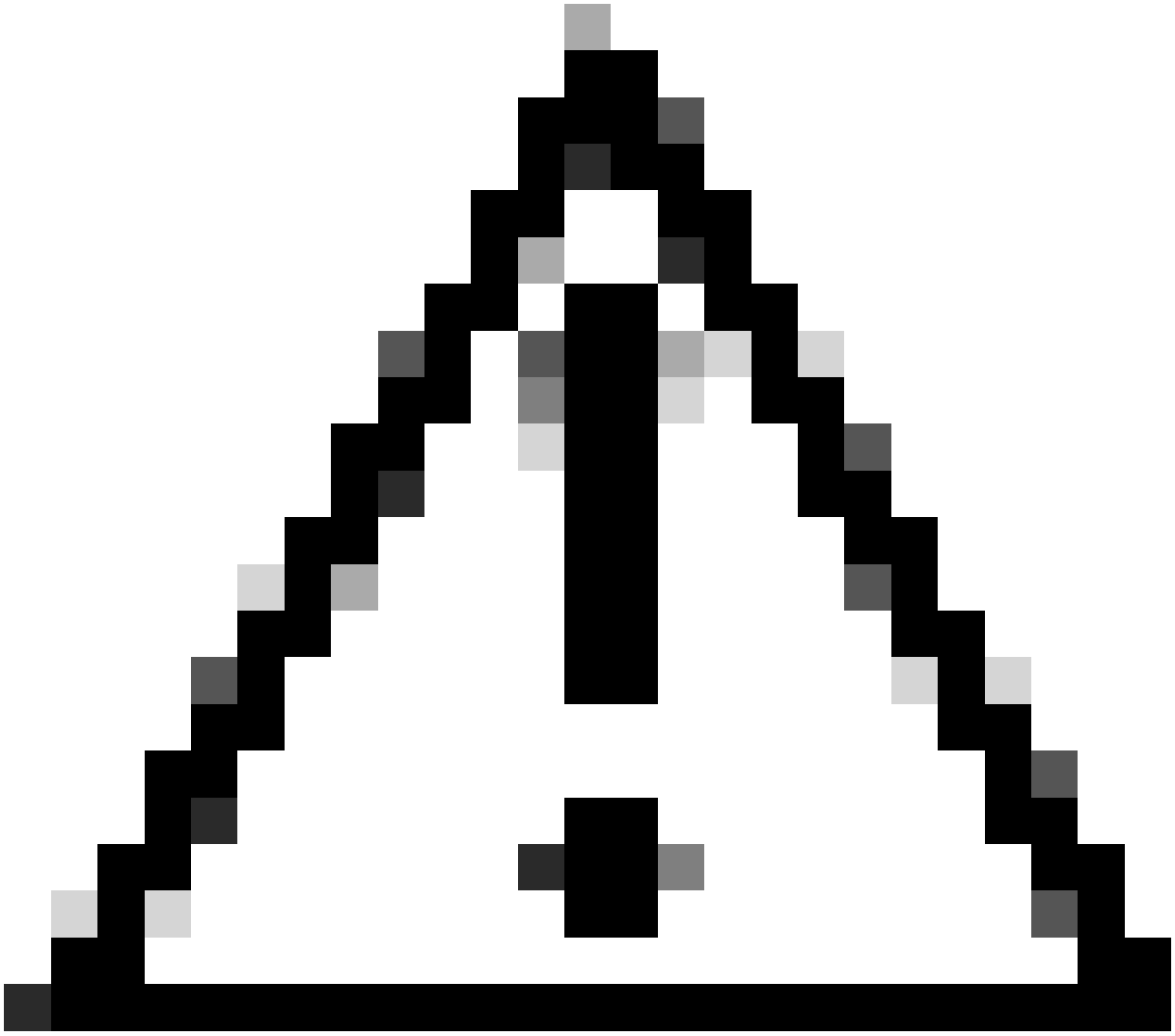
Passaggio 4:

In questo passaggio si associa il gruppo a un utente, si associa ciascun gruppo a utenti che definiscono la rispettiva autenticazione e privacy (crittografia) e si può ulteriormente proteggere utilizzando l'elenco di controllo di accesso.

```
!NoAuthNoPriv: noauth
snmp-server user MyUser MyGroup v3 access snmp-poll-server

!AuthNoPriv: auth
snmp-server user MyUser MyGroup v3 auth sha AuthPassword access snmp-poll-server

!AuthPriv: priv
snmp-server user MyUser MyGroup v3 auth sha AuthPassword priv aes 128 PrivPassword access snmp-poll-ser
```



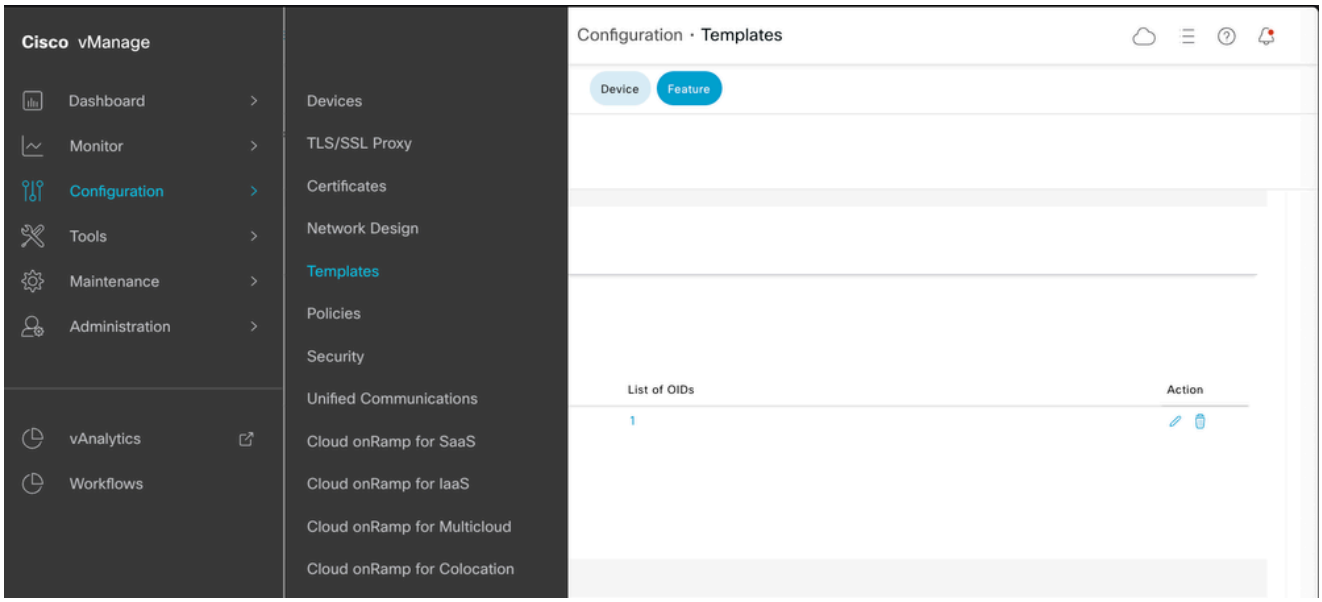
Attenzione: Si noti che quando si cerca di configurare un utente snmp-server, la guida contestuale non è disponibile e non viene mostrata nella configurazione corrente. Questa condizione è conforme alla RFC 3414. Digitare il comando full e il parser accetta la configurazione

```
cEdge-RT01(config)# snmp-server user ? ^ % Invalid input detected at '^' marker.
```

ID bug Cisco CSCvn71472

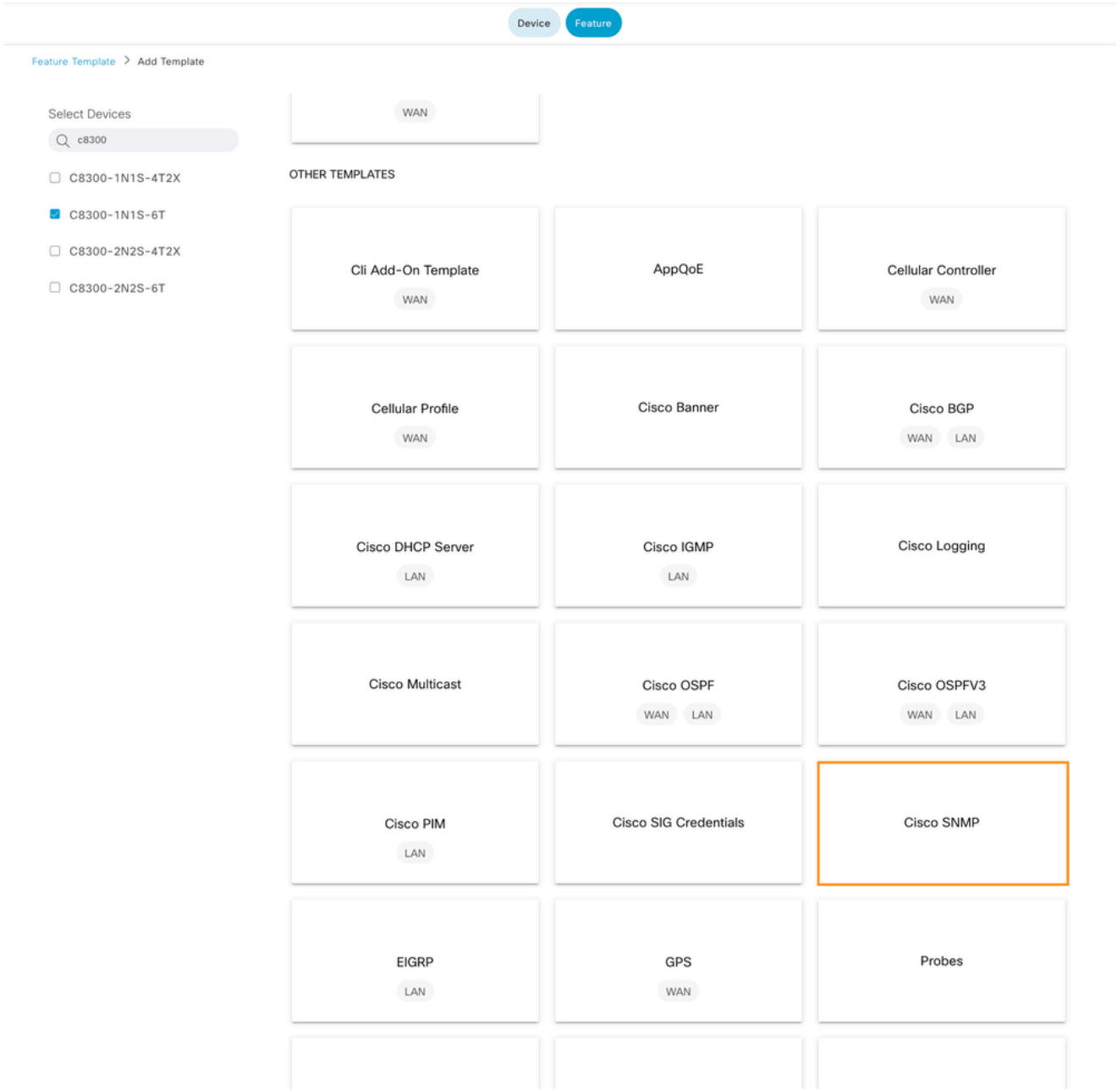
Congratulazioni, questo è tutto ciò che serve. Ora che si conosce la cli e il concetto, è possibile vedere come configurare utilizzando il modello di funzionalità SNMP su un Catalyst SD-WAN Manager

Selezionare Cisco vManage > Configuration > Templates > Feature

- 

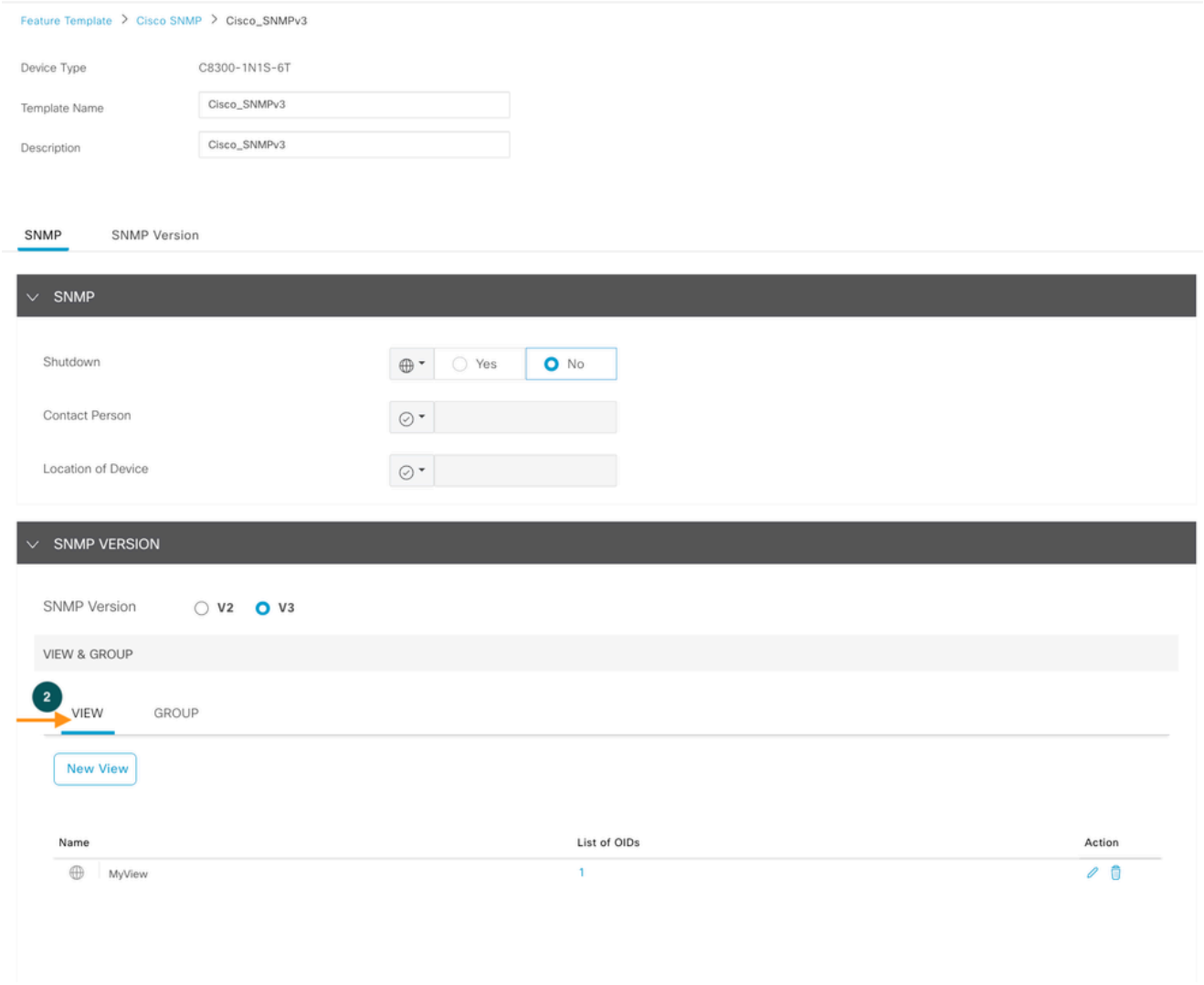
  Modello funzionalità

Passare a Cisco SNMP, disponibile nella sezione Altri modelli

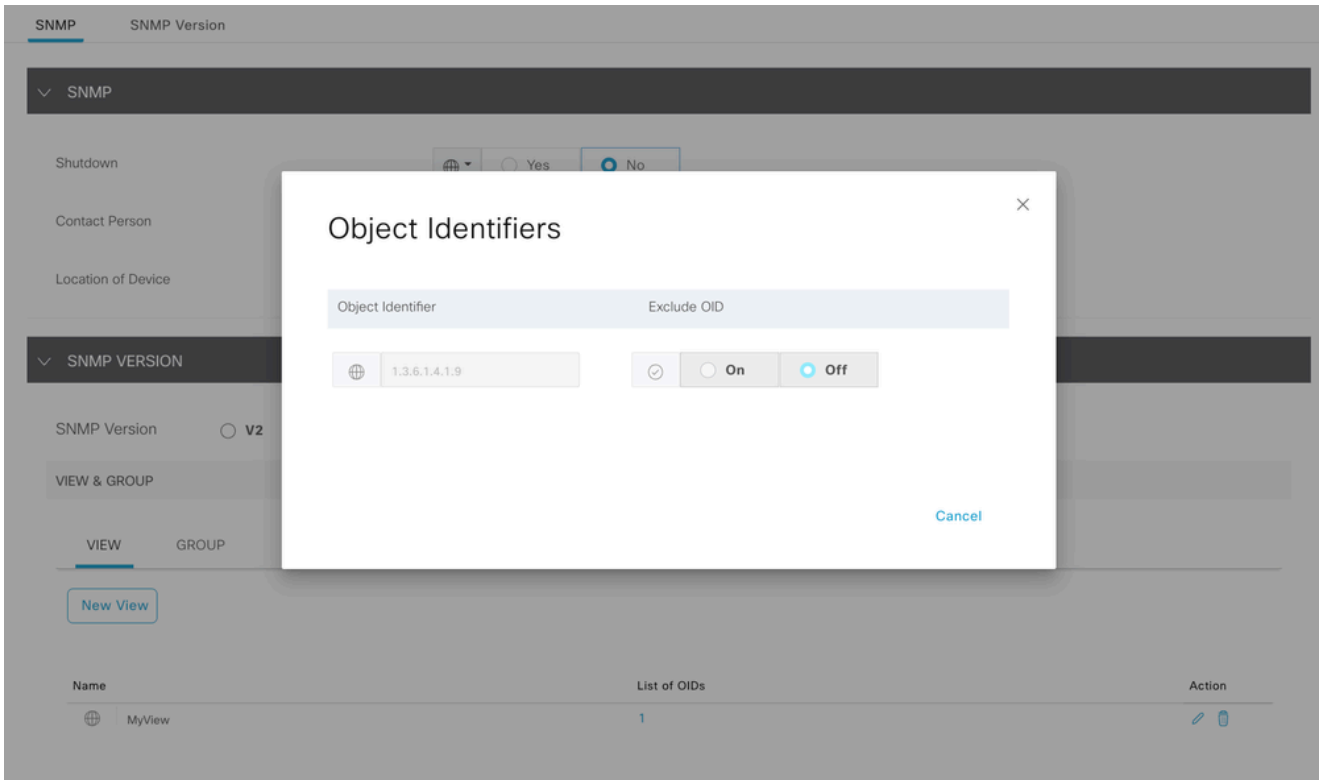


- Funzione SNMP

Definizione della vista SNMP (restrizione), questo è il passo 2

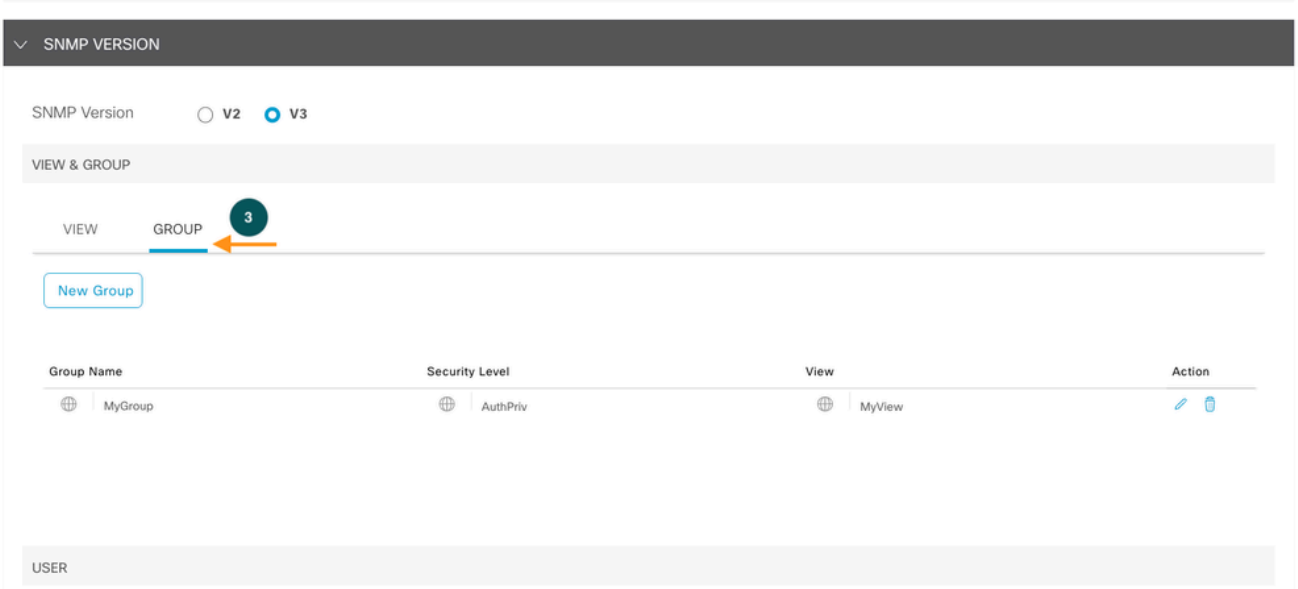

Feature Template > Cisco SNMP > Cisco_SNMPv3
Device Type
C8300-1N1S-6T
Template Name
Cisco_SNMPv3
Description
Cisco_SNMPv3
SNMP
SNMP Version
SNMP
Shutdown
Yes
No
Contact Person
Location of Device
SNMP VERSION
SNMP Version
V2
V3
VIEW & GROUP
2
VIEW
GROUP
New View
Name
List of OIDs
Action
MyView
1

- SNMP View



- OID SNMP

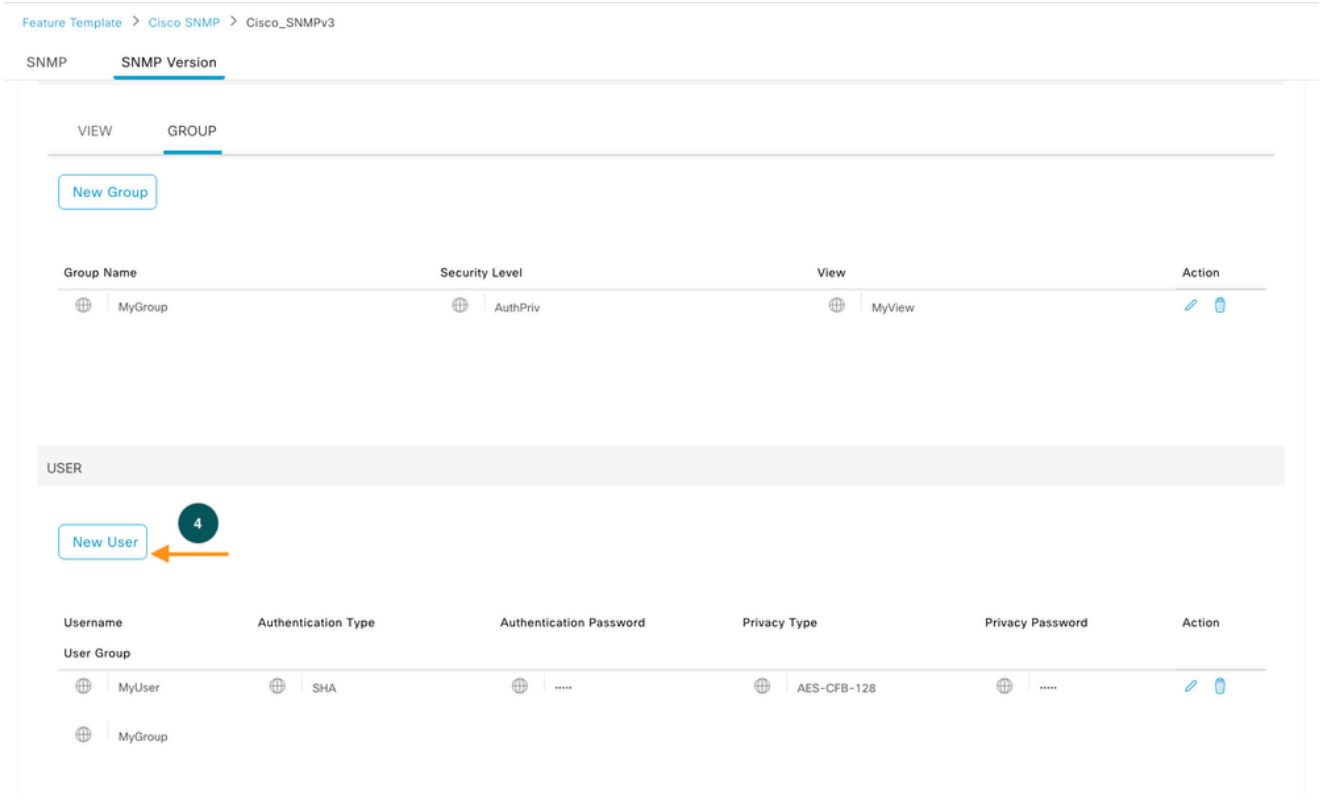
Definire il gruppo SNMP è il nostro passo 3



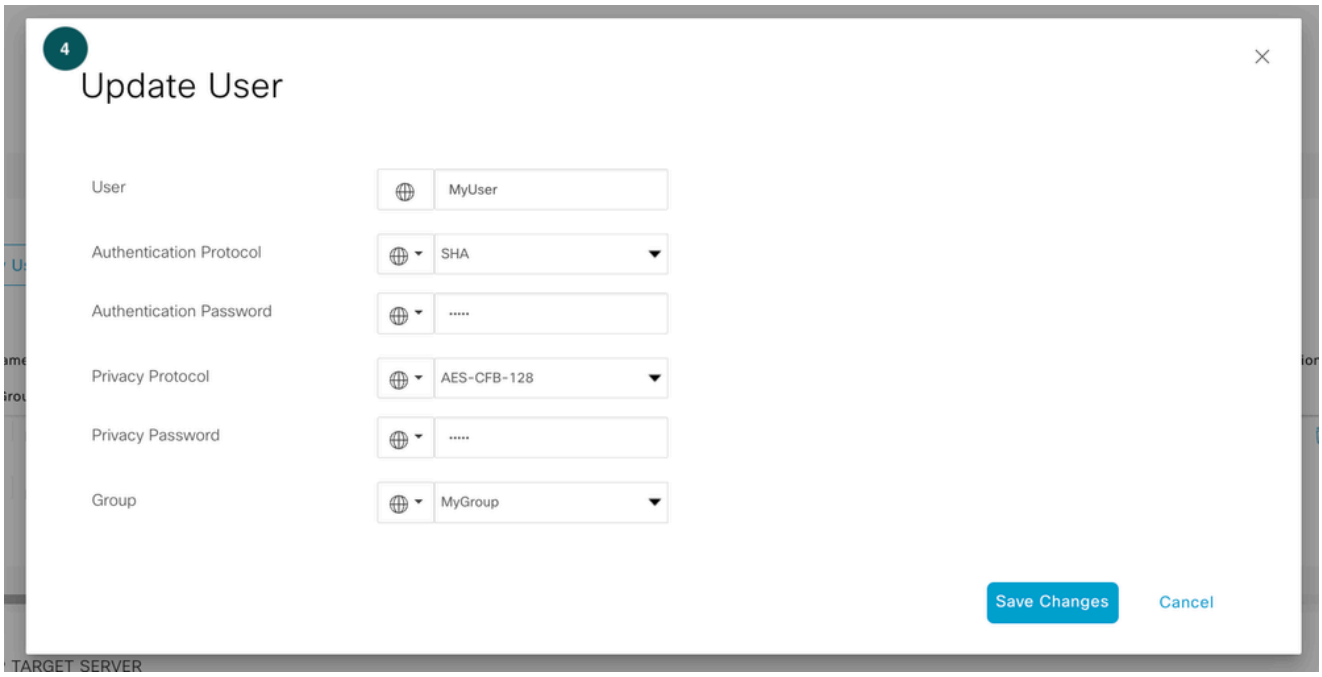
- Gruppo SNMP

- Gruppo SNMP

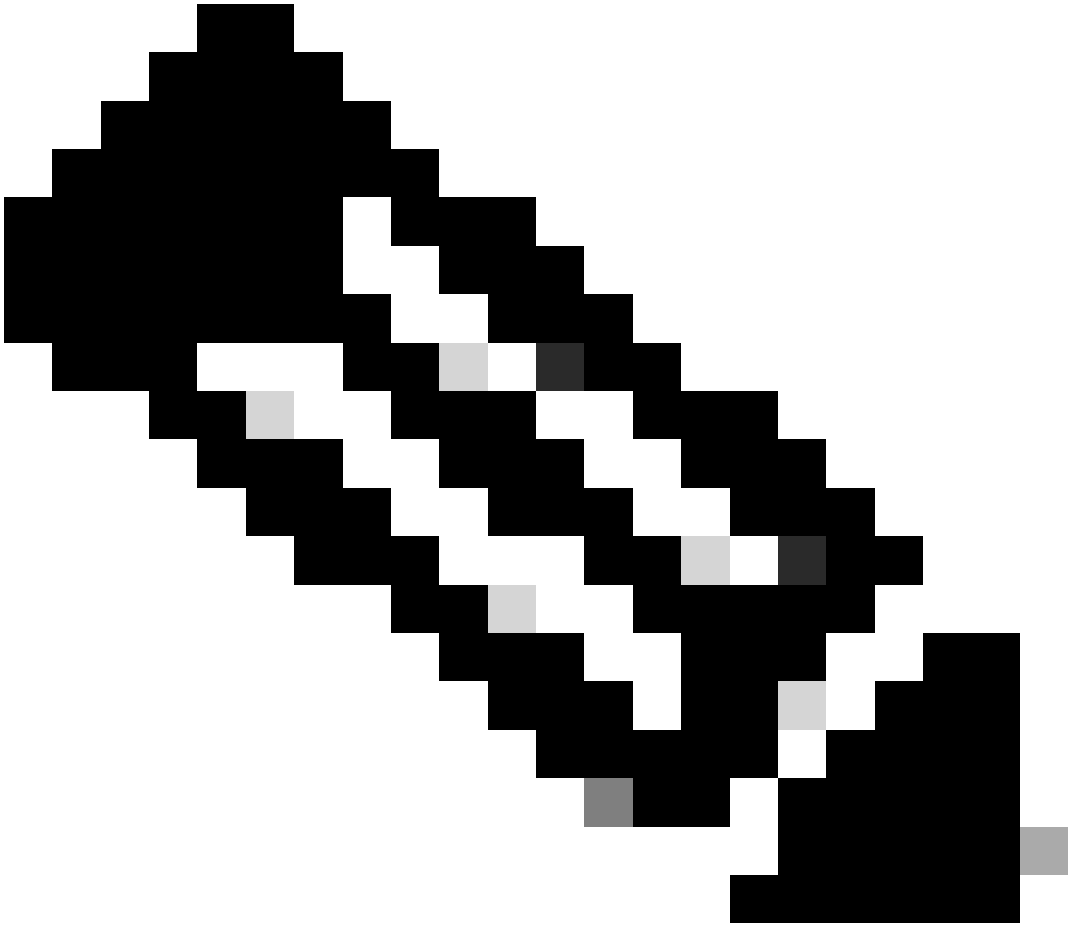
Definire il gruppo di utenti, questo è il nostro Passo 4 in cui definiamo l'autenticazione e la password di crittografia.



- Utente SNMP

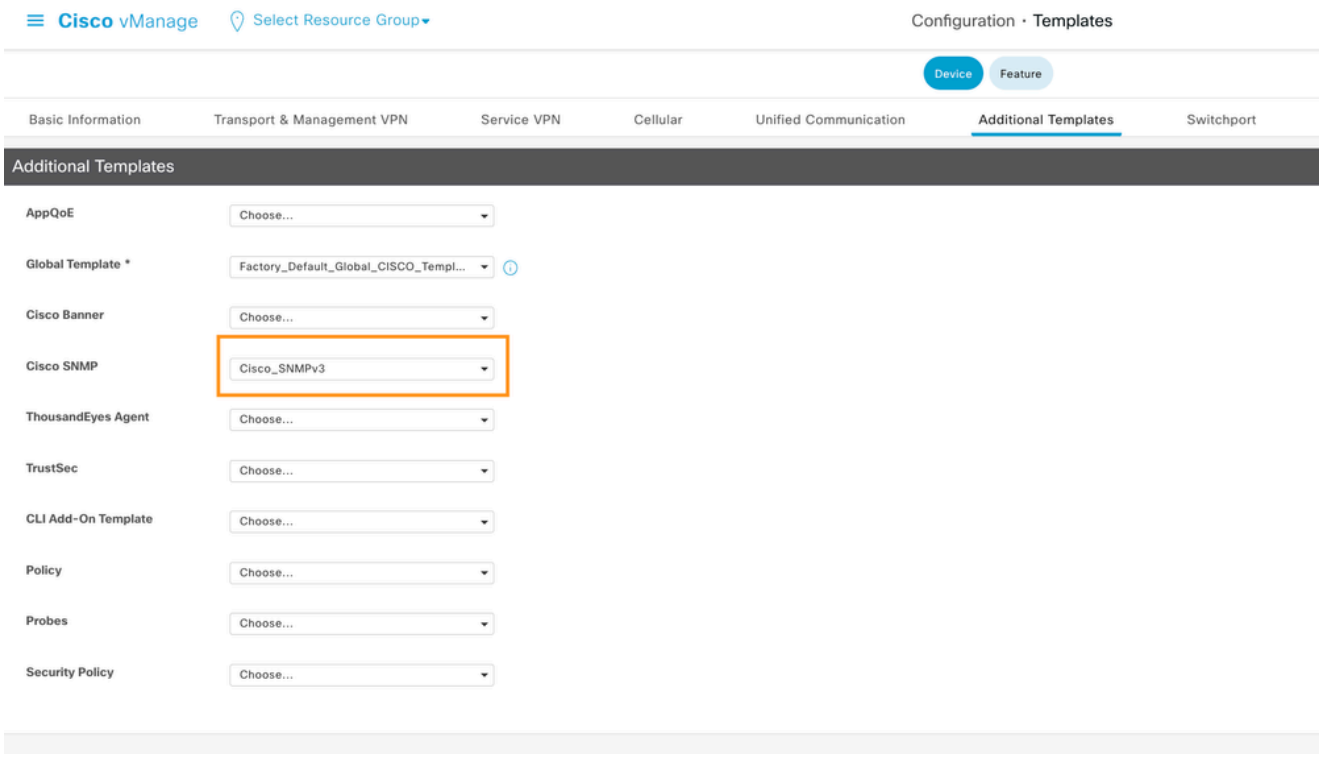


Crittografia utente SNMP



Nota: In base al livello di protezione del gruppo SNMP, il rispettivo campo associato all'utente viene abilitato.

Associare ora il modello di funzionalità al modello di dispositivo.



- SNMP Feature Template

Verifica

```
Router#show snmp user

User name: MyUser
Engine ID: 800000090300B8A3772FF870
storage-type: nonvolatile     active    access-list: snmp-poll-server
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: MyGroup
```

Da un computer in cui è installato snmpwalk è possibile eseguire il comando per verificare la risposta SNMP per il rispettivo livello di protezione

```
!NoAuthNoPriv: noauth
snmpwalk -v 3 -l noAuthNoPriv -u MyUser



        .1

!AuthNoPriv: auth
snmpwalk -v 3 -l authNoPriv -u MyUser -a SHA -A AuthPassword
```

```
         .1

!AuthPriv: priv
snmpwalk -v 3 -l authPriv -u MyUser -a SHA -A AuthPassword -x AES -X PrivPassword


          .1
```

-v: Versione (3)

-l : Livello di protezione

-A: passphrase protocollo di autenticazione

-X: passphrase protocollo privacy

Riferimenti

- Configurazione della trap SNMPv3 sul router perimetrale Cisco
- Modello di configurazione per SNMPv3 di Tim Glen

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).