Configure SNMPv3 on Catalyst SD-WAN

Contents

Introduction

This document describes SNMPv3 configuration and explains about security (authentication), encryption (privacy), and restriction (view).

Background

Often, SNMPv3 configuration is seen as complex and hard to configure, until we know what needs to be done. The reason for SNMPv3's existence is similar to HTTPS: for security, encryption, and restriction.

Prerequisites

Knowledge of SD-WAN feature templates and device template.

General understanding on SNMP MIB, SNMP Poll, and SNMP Walk

Requirements

SD-WAN Controllers

Cisco Edge Router

Components Used

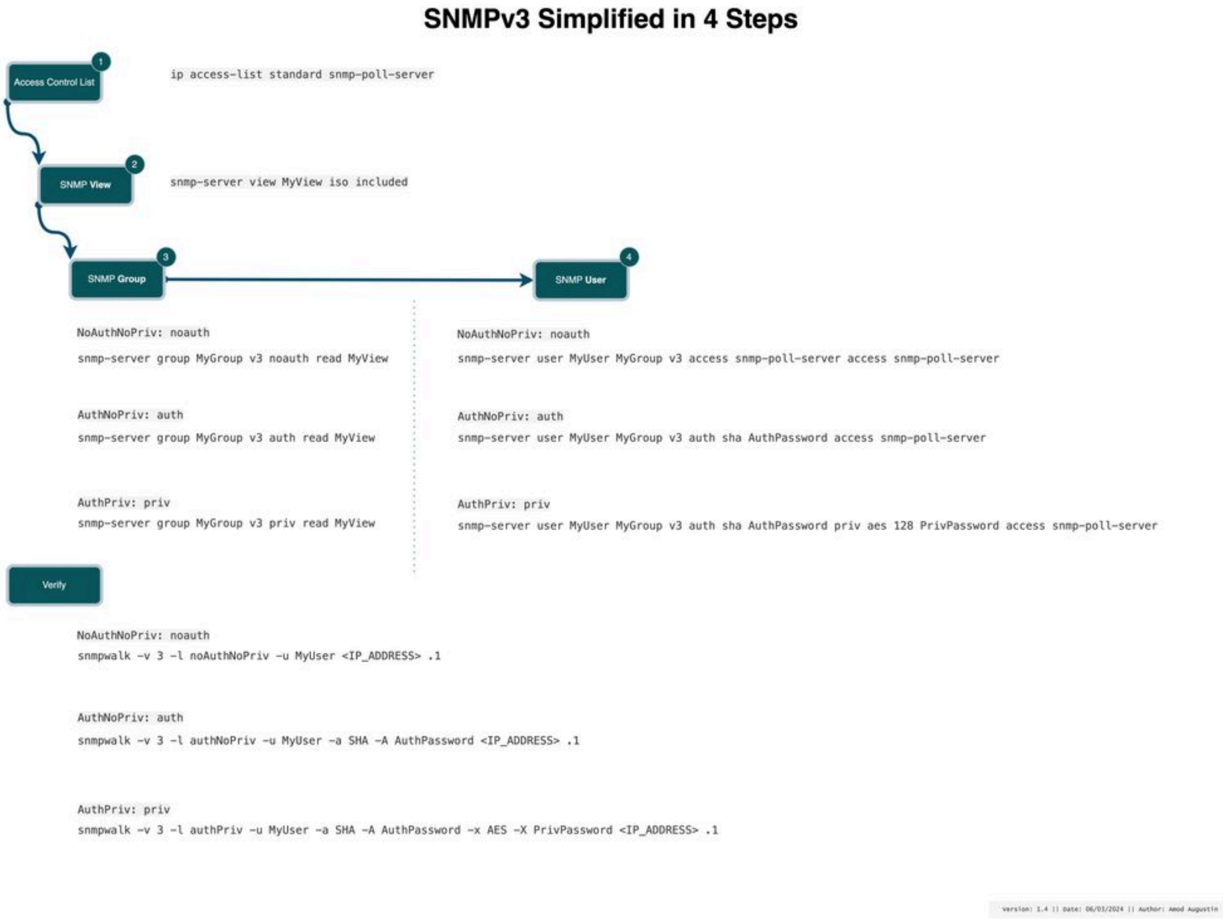
SD-WAN Controllers on 20.9

Cisco Edge Router on 17.9

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. If your network is live, ensure that you understand the potential impact of any command.

Configure

The diagram help you to understand what is all required to configure SNMPv3 from a CLI stand point.

- 

SNMPv3 Simplified in 4 Steps

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

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

```
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
```

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

```
NoAuthNoPriv: noauth
snmpwalk -v 3 -l noAuthNoPriv -u MyUser <IP_ADDRESS> .1

AuthNoPriv: auth
snmpwalk -v 3 -l authNoPriv -u MyUser -a SHA -A AuthPassword <IP_ADDRESS> .1

AuthPriv: priv
snmpwalk -v 3 -l authPriv -u MyUser -a SHA -A AuthPassword -x AES -X PrivPassword <IP_ADDRESS> .1
```

Version: 1.4 || Date: 06/03/2024 || Author: Amod Augustin

SNMPv3 Simplified in 4 Steps

Once you understand its easy to put the concept to CLI or a feature template. Lets dive in.

Step 1:

Configure an ACL to allow who can poll the system (router in our case).

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

Step 2:

Define a snmp view, as the term implies what mibs does the poller have access to, this is our **restriction**.

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

Step 3:

Define snmp group, snmp group has mainly two parts a. Security Level b. Restriction (view).

Security Levels:

- **noAuthNoPriv:** No authentication and no privacy (no encryption).
- **authNoPriv**: Authentication is required, but no privacy.
- **authPriv**: Both authentication and privacy are required.

Restriction is what we defined in Step 2, lets put them all together.

```
!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
```

Step 4:

In this step we associate the group to a user, associate each groups with users defining respective authentication and privacy (encryption) and can be further secured using access control list.

```
!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-serv
```

⚠

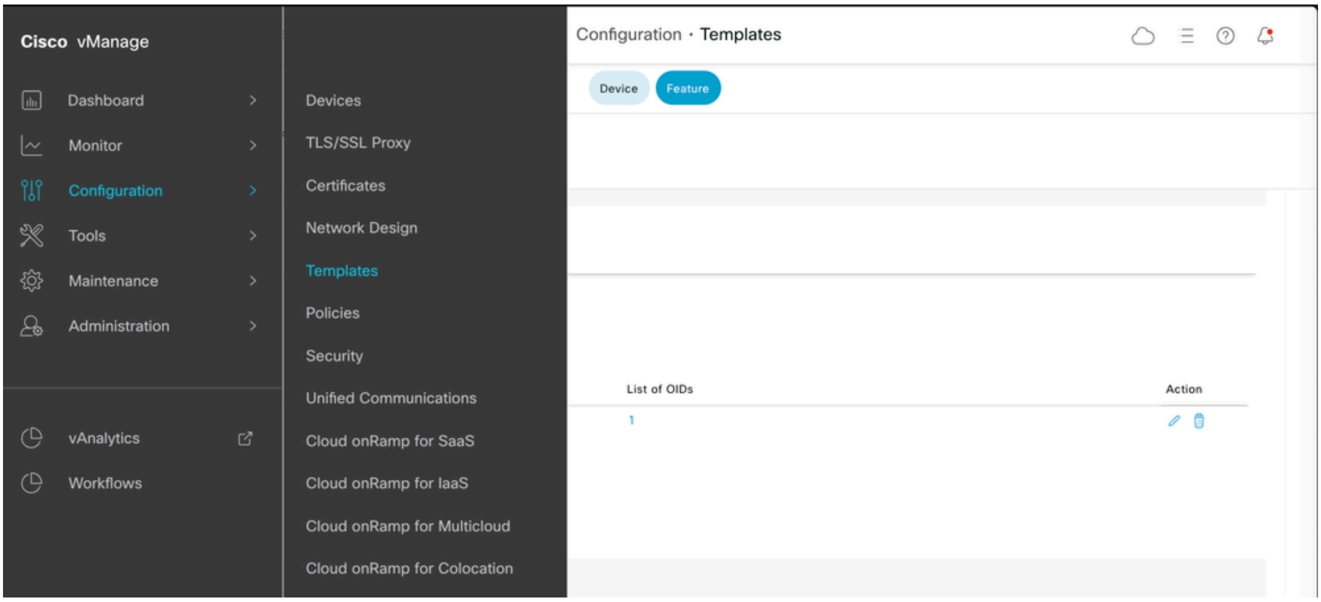
Caution: You can notice when trying to configure **snmp-server user** the context help is not available and also not shown in running configuration this is to comply with RFC 3414. Type in the full command and the parser accepts the configuration

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

Cisco bug ID CSCvn71472

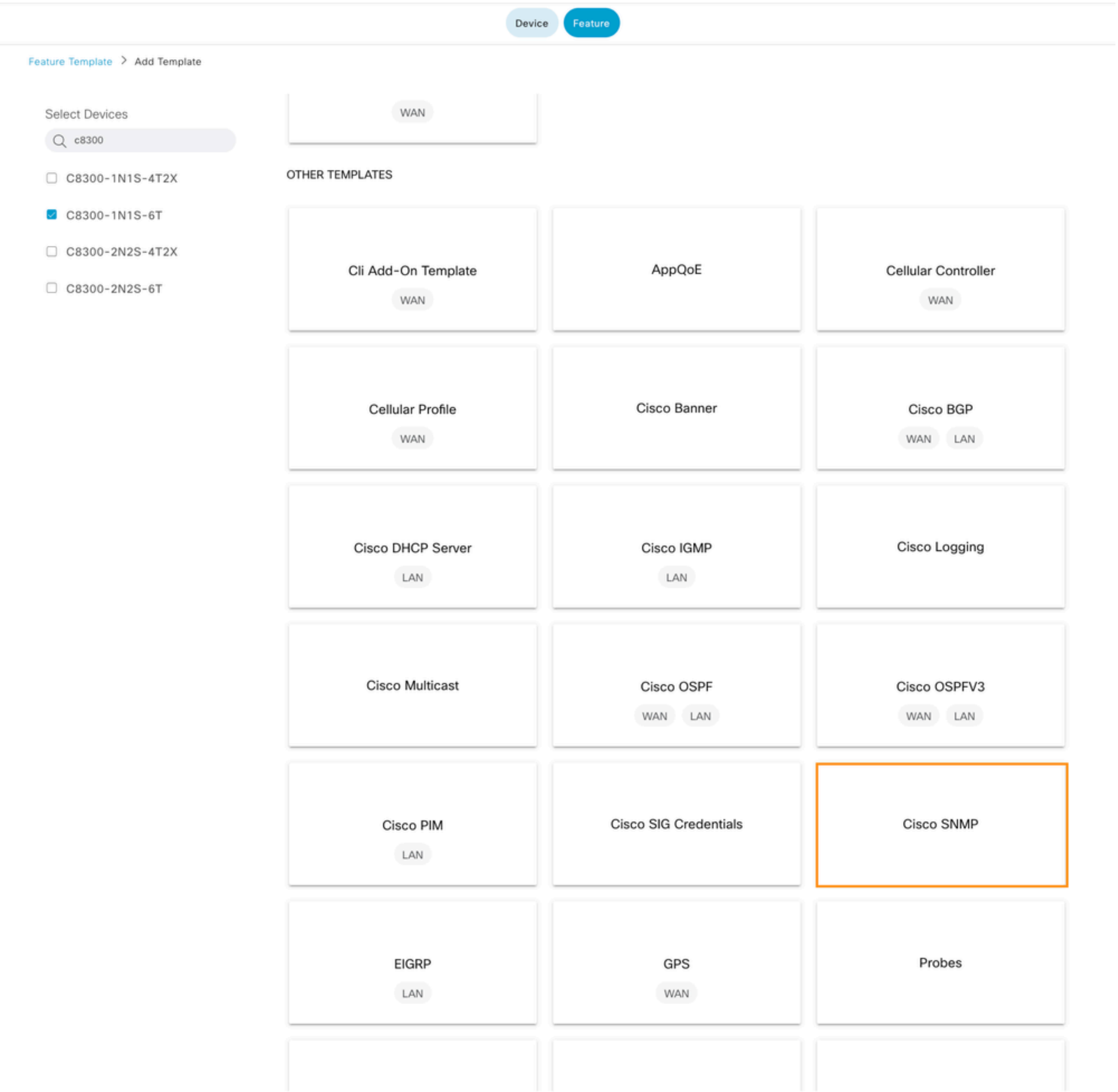
Congratulations, that is all what is needed. Now that you know the cli and the concept lets see how to configure using SNMP feature template on a Catalyst SD-WAN Manager

Navigate to Cisco vManage > Configuration > Templates > Feature

- 

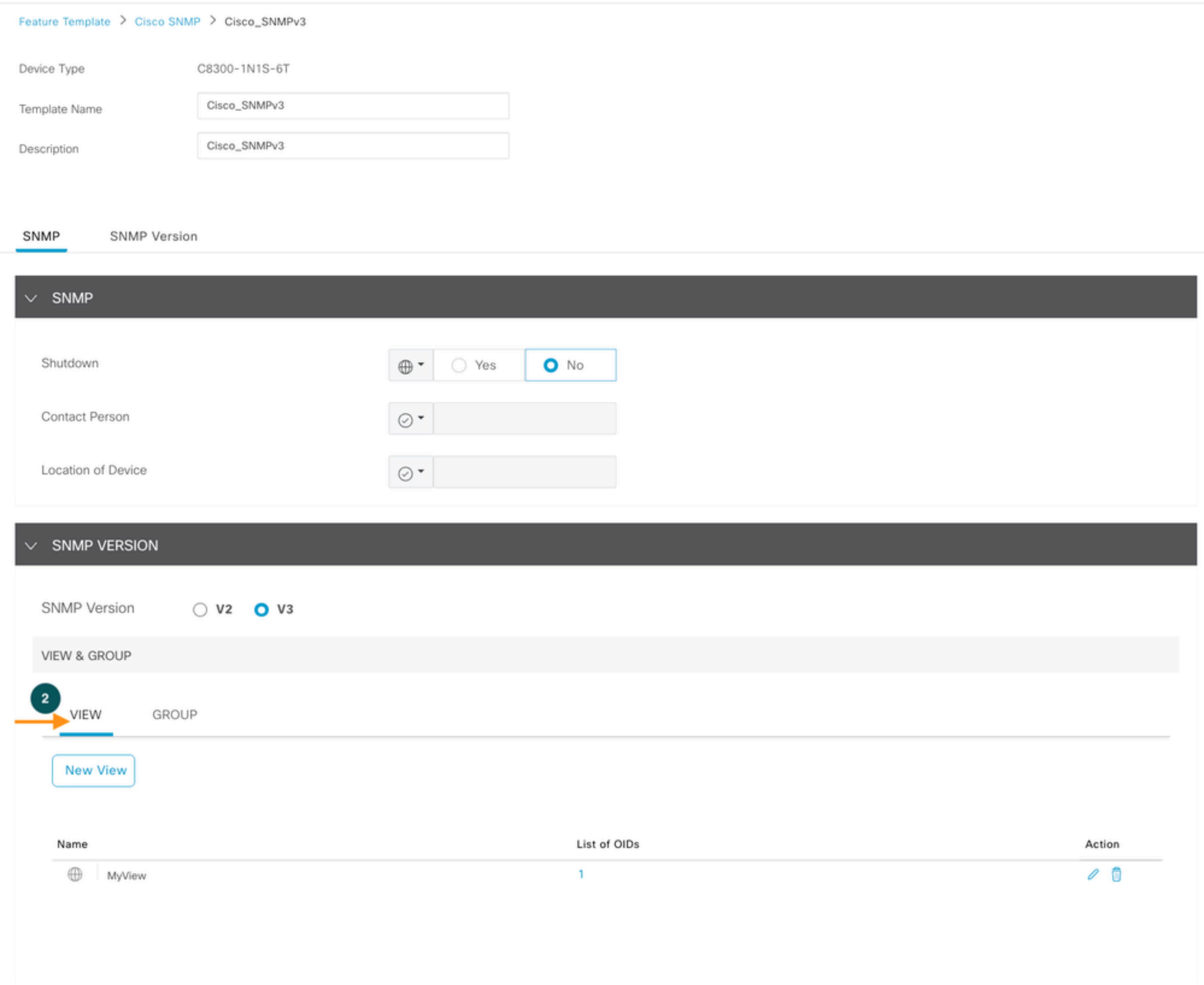
  Feature Template

Navigate to Cisco SNMP which can be found in Other Template Section

- 

SNMP Feature

Define SNMP View (restriction), this is our Step 2



Feature Template > Cisco SNMP > Cisco_SNMPv3

Device Type: C8300-1N1S-6T

Template Name: Cisco_SNMPv3

Description: Cisco_SNMPv3

SNMP

Shutdown: ○ Yes ● No

Contact Person:

Location of Device:

SNMP VERSION

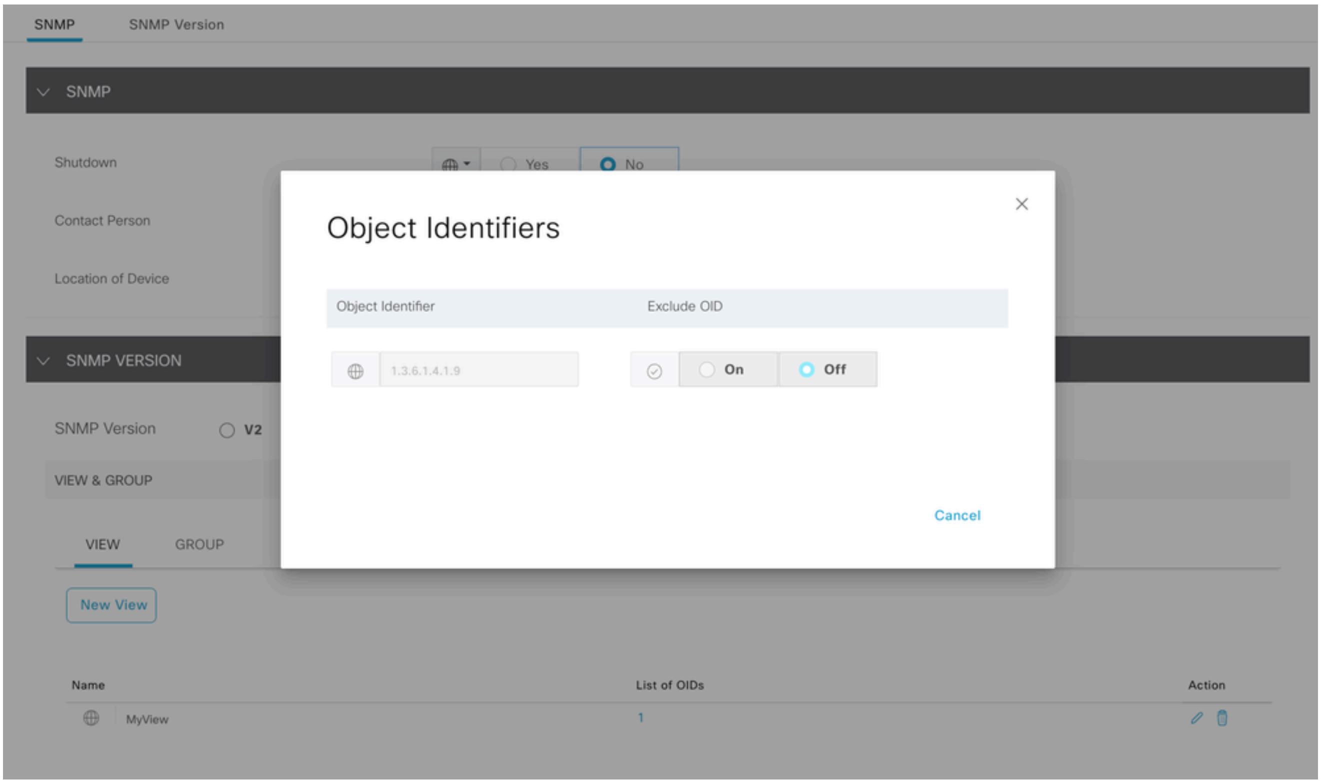
SNMP Version: ○ V2 ● V3

VIEW & GROUP

Name	List of OIDs	Action
MyView	1	

-

SNMP View

- 

  Shutdown ○ Yes ● No

  Contact Person

  Location of Device

  SNMP Version ○ V2

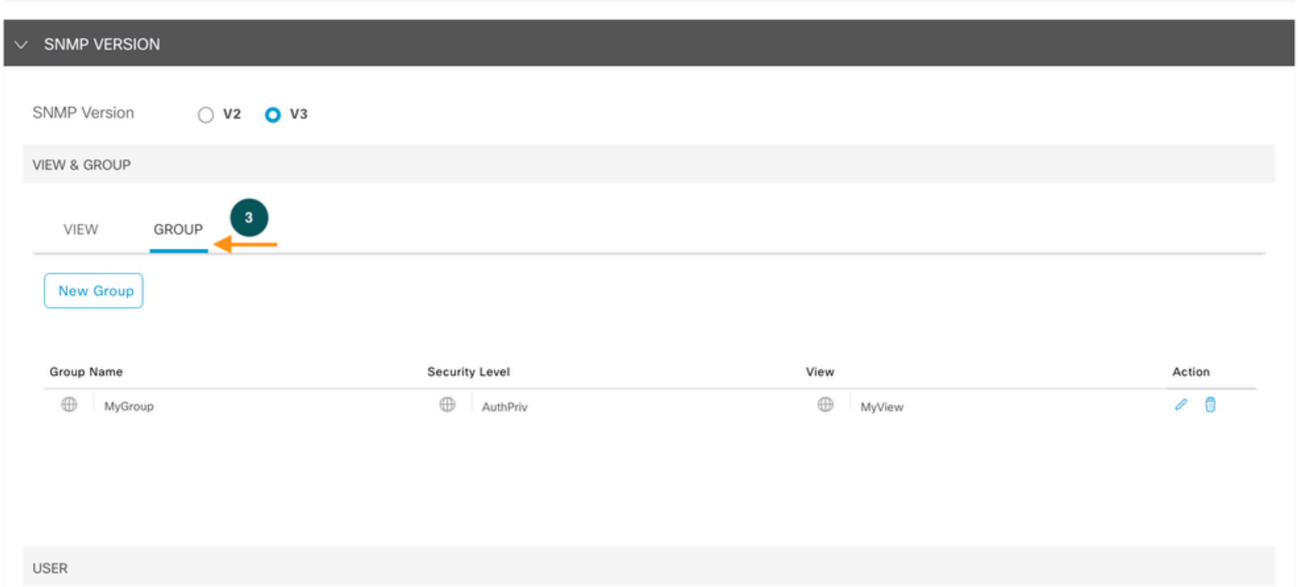
  Object Identifiers

Object Identifier	Exclude OID
1.3.6.1.4.1.9	○ On ● Off

Name	List of OIDs	Action
MyView	1	

  SNMP OID

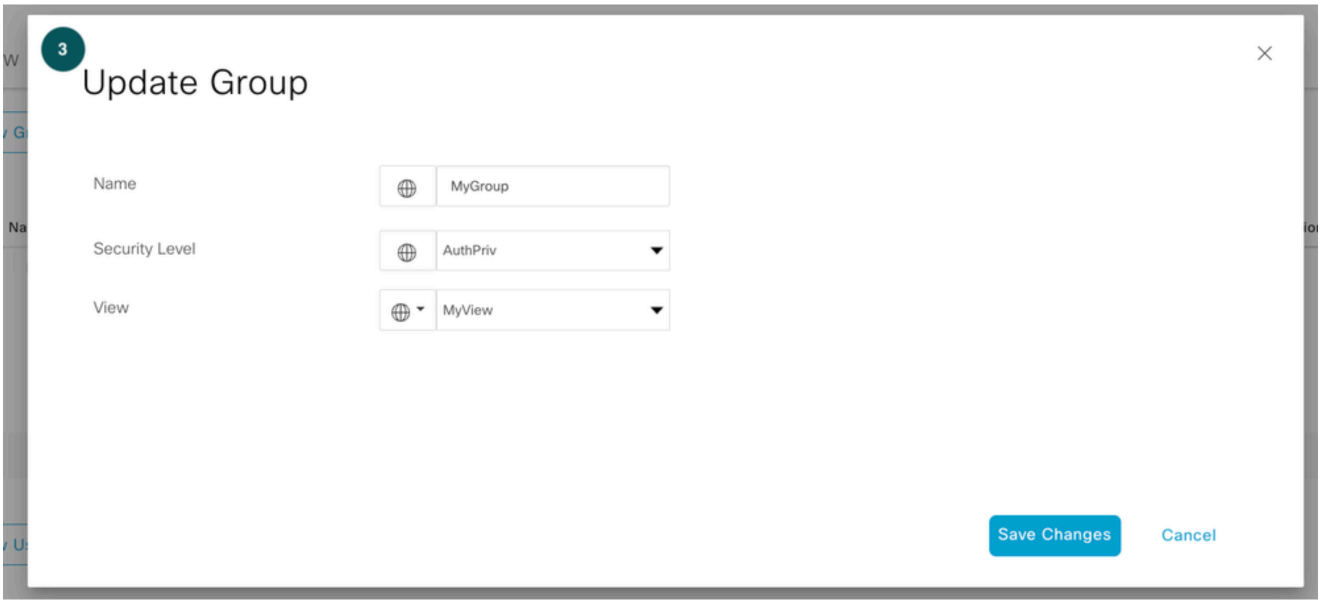
Define SNMP group this is our Step 3

- 

  SNMP Version ○ V2 ● V3

Group Name	Security Level	View	Action
MyGroup	AuthPriv	MyView	

  SNMP Group

- 

  3

  Update Group

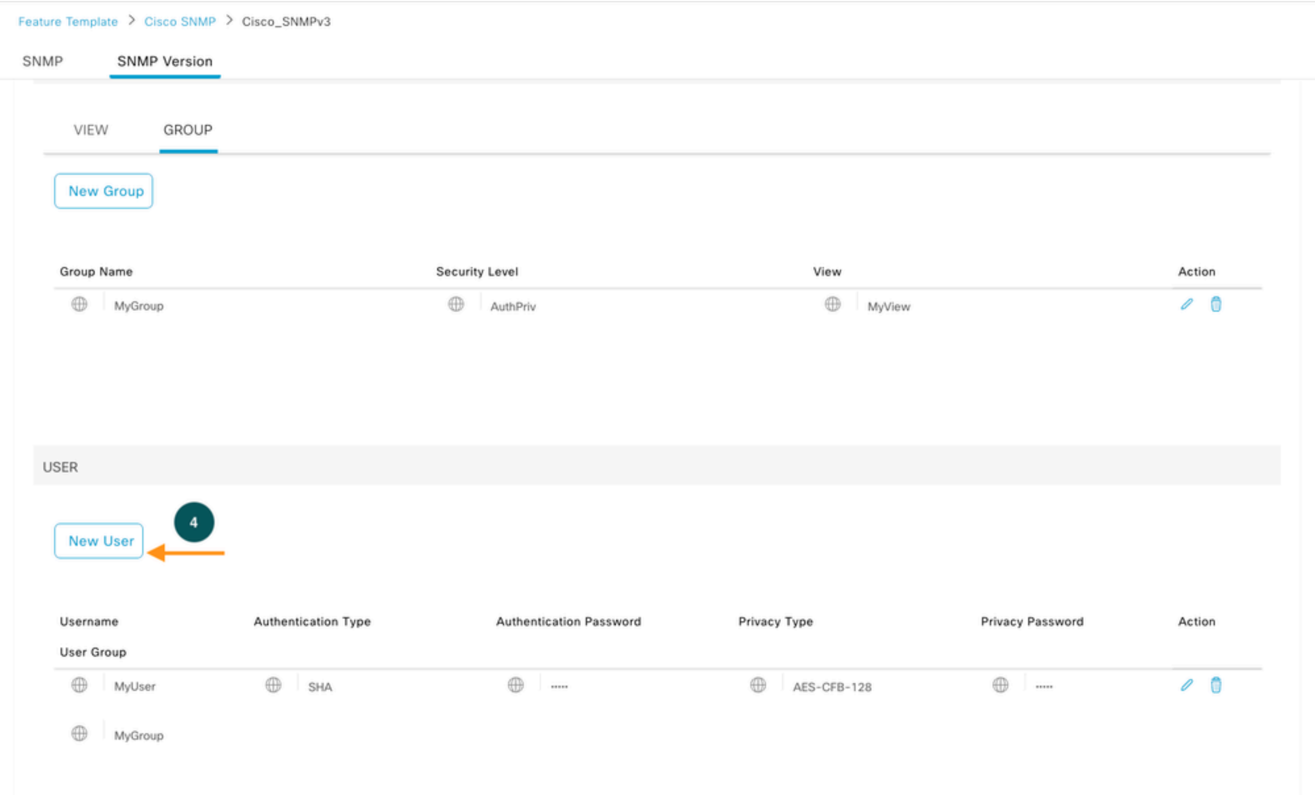
  Name: MyGroup

  Security Level: AuthPriv

  View: MyView

  SNMP Group

Define user group, this is our Step 4 in which we define the authentication and encryption password.

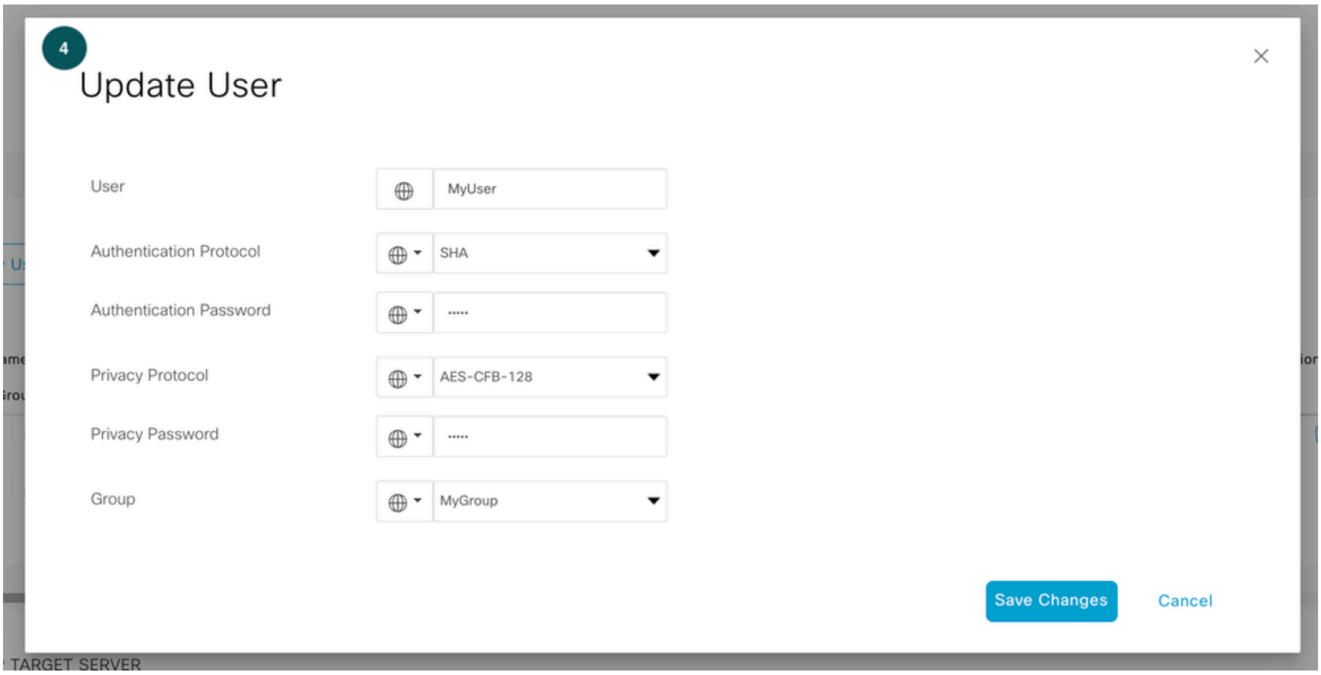
- 

Group Name	Security Level	View	Action
MyGroup	AuthPriv	MyView	

  USER

Username User Group	Authentication Type	Authentication Password	Privacy Type	Privacy Password	Action
MyUser MyGroup	SHA	•••••	AES-CFB-128	•••••	

  SNMP User

- 

Update User

User: MyUser

Authentication Protocol: SHA

Authentication Password: •••••

Privacy Protocol: AES-CFB-128

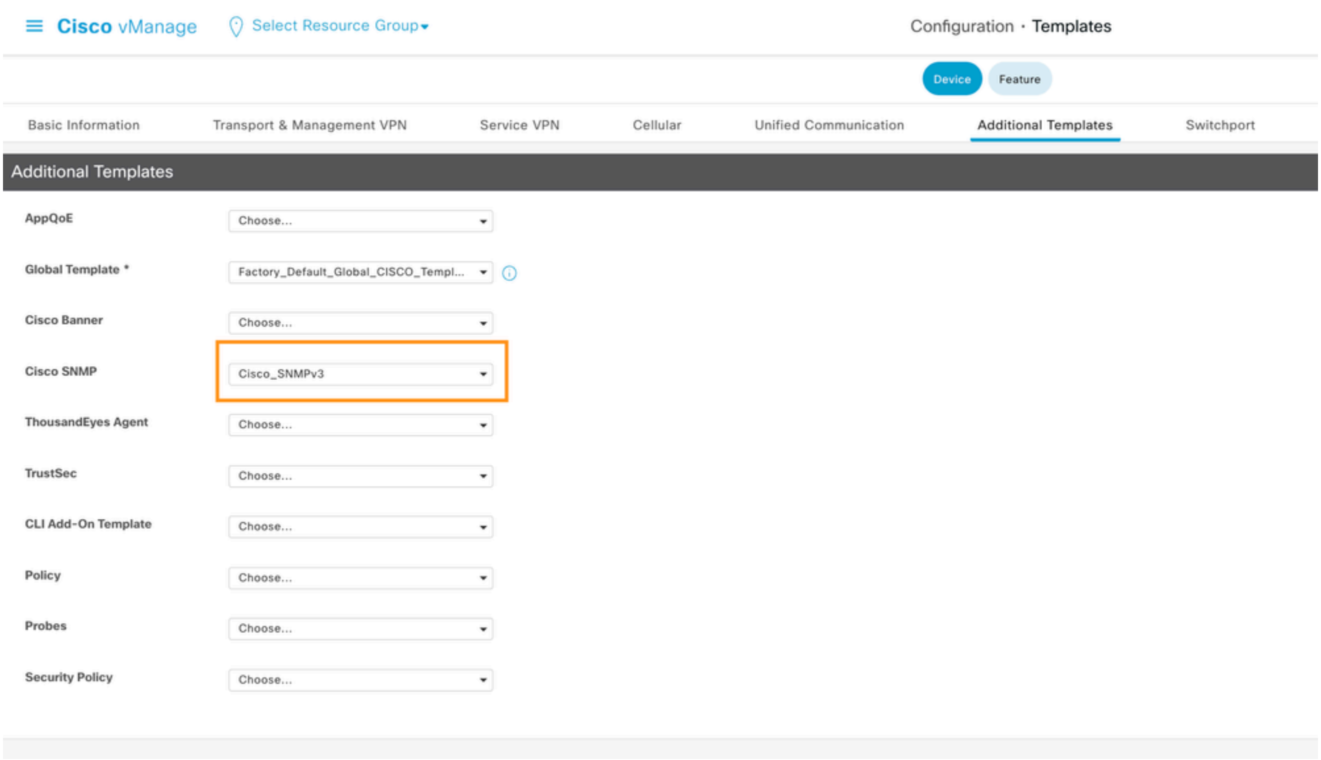
Privacy Password: •••••

Group: MyGroup

SNMP User Encryption

Note: Based on SNMP Group security level, respective field associated with user gets enabled.

Now Attach the feature template to device template.

- 

Additional Templates

AppQoE: Choose...

Global Template *: Factory_Default_Global_CISCO_Templ...

Cisco Banner: Choose...

Cisco SNMP: Cisco_SNMPv3

ThousandEyes Agent: Choose...

TrustSec: Choose...

CLI Add-On Template: Choose...

Policy: Choose...

Probes: Choose...

Security Policy: Choose...

SNMP Feature template

Verify

```
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
```

From a machine that has snmpwalk installed you can run the command to verify SNMP response for respective security level

```
!NoAuthNoPriv: noauth
snmpwalk -v 3 -l noAuthNoPriv -u MyUser <IP_ADDRESS> .1

!AuthNoPriv: auth
snmpwalk -v 3 -l authNoPriv -u MyUser -a SHA -A AuthPassword <IP_ADDRESS> .1

!AuthPriv: priv
snmpwalk -v 3 -l authPriv -u MyUser -a SHA -A AuthPassword -x AES -X PrivPassword <IP_ADDRESS> .1
```

-v: Version (3)

-l : Security Level

-A: Authentication protocol pass phrase

-X: Privacy protocol pass phrase

References

- Configure SNMPv3 Trap on Cisco Edge Router
- Configuration Template for SNMPv3 by Tim Glen