Catalyst SD-WAN에서 SNMPv3 구성

목차

[소개](#)

[배경](#)

[사전 요구 사항](#)

- [요구 사항](#)
- [사용되는 구성 요소](#)

[구성](#)

[다음을 확인합니다.](#)

[참조](#)

소개

이 문서에서는 SNMPv3 컨피그레이션에 대해 설명하고 보안(인증), 암호화(프라이버시) 및 제한(보기)에 대해 설명합니다.

배경

SNMPv3 컨피그레이션은 수행해야 할 작업이 파악될 때까지 구성이 복잡하고 어려운 것으로 간주되는 경우가 많습니다. SNMPv3의 존재 이유는 HTTPS와 유사합니다. 보안, 암호화 및 제한 사항.

사전 요구 사항

SD-WAN 기능 템플릿 및 디바이스 템플릿에 대한 지식

SNMP MIB, SNMP Poll 및 SNMP Walk에 대한 일반적인 이해

요구 사항

SD-WAN 컨트롤러

Cisco 에지 라우터

사용되는 구성 요소

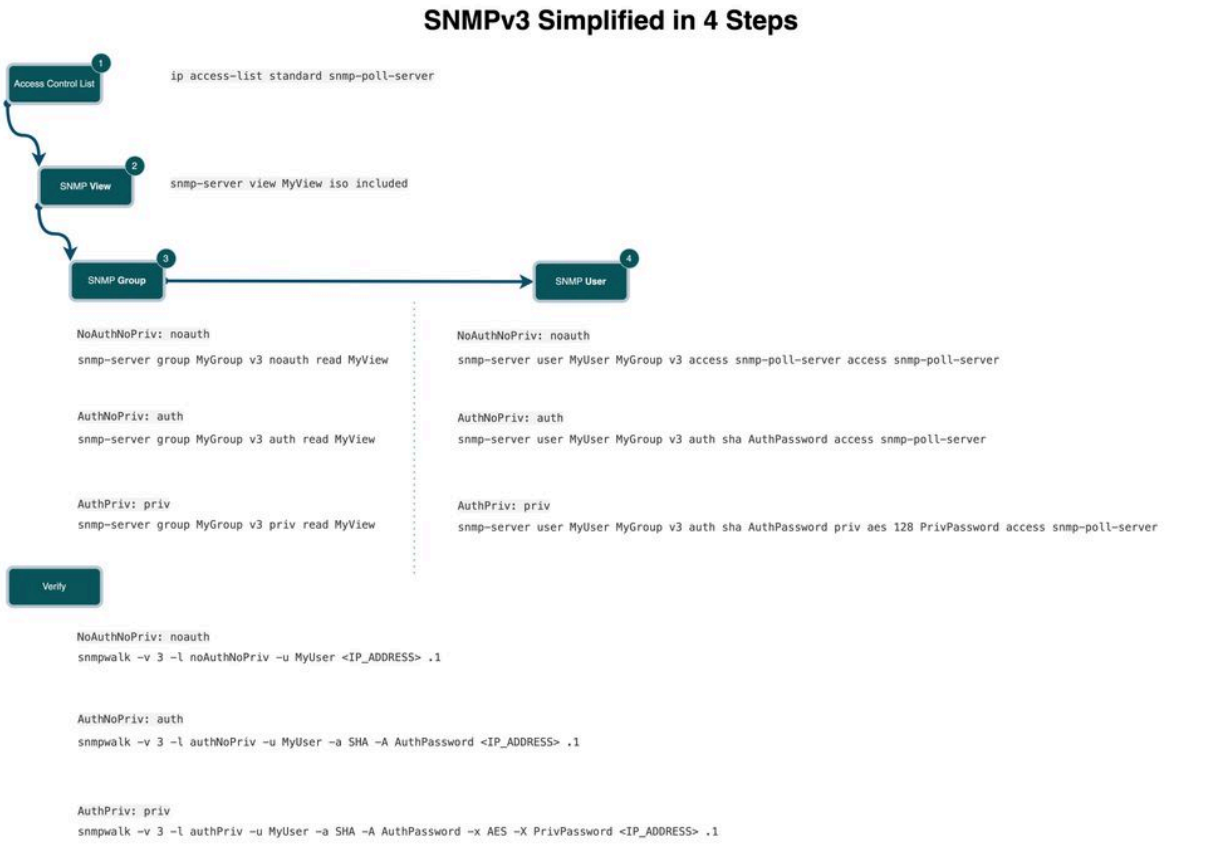
20.9의 SD-WAN 컨트롤러

Cisco Edge Router on 17.9

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이 다이어그램은 CLI 스탠드포인트에서 SNMPv3를 구성하는 데 필요한 모든 사항을 이해하는 데 도움이 됩니다.



- 4단계로 간소화된 SNMPv3

개념을 CLI 또는 기능 템플릿에 쉽게 추가할 수 있습니다. 한번 들어봅시다.

1단계:

누가 시스템(이 경우에는 라우터)을 폴링할 수 있도록 ACL을 구성합니다.

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

2단계:

용어 는 poller가 액세스할 수 있는 mib를 의미하므로 snmp 보기를 정의합니다. 이는 제한입니다.

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

3단계:

snmp 그룹을 정의합니다. snmp 그룹에는 주로 두 개의 part a가 있습니다. 보안 수준 b. 제한(보기).

보안 수준:

- noAuthNoPriv: 인증 및 개인 정보 보호 없음(암호화 없음)
- 인증 번호: 인증이 필요하지만 개인 정보는 없습니다.
- 인증 권한: 인증과 개인 정보 보호 모두 필요합니다.

제한은 우리가 2단계에서 정의한 것이며, 모든 것을 종합해 보자.

```
!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
```

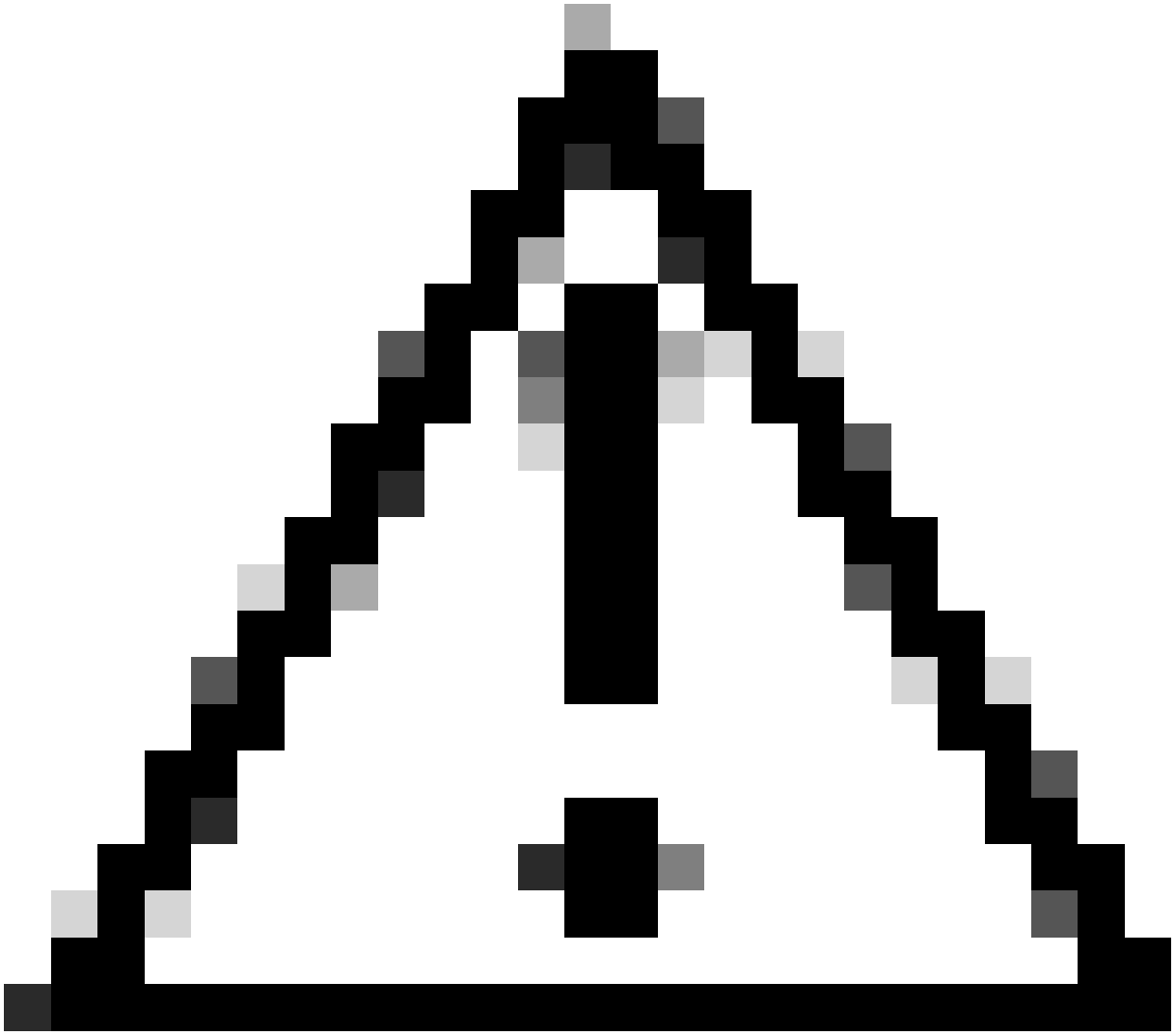
4단계:

이 단계에서는 그룹을 사용자와 연결하고, 각 그룹을 각 인증 및 개인 정보(암호화)를 정의하는 사용자와 연결하며, 액세스 제어 목록을 사용하여 더 안전하게 보호할 수 있습니다.

```
!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
```



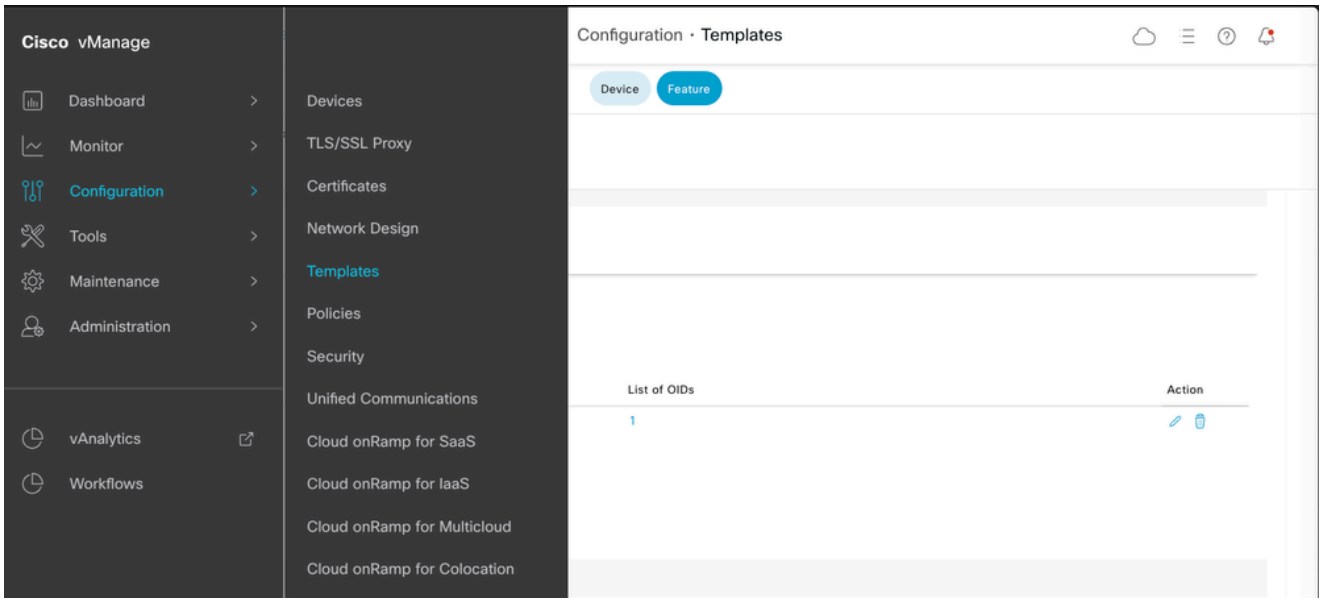
주의: snmp 서버 사용자를 구성하려고 할 때 컨텍스트 도움말이 제공되지 않으며 실행 중인 컨피그레이션에도 표시되지 않음을 알 수 있습니다. 이는 RFC 3414를 준수하기 위한 것입니다. full 명령을 입력하면 파서가 컨피그레이션을 수락합니다

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

Cisco 버그 ID CSCvn71472

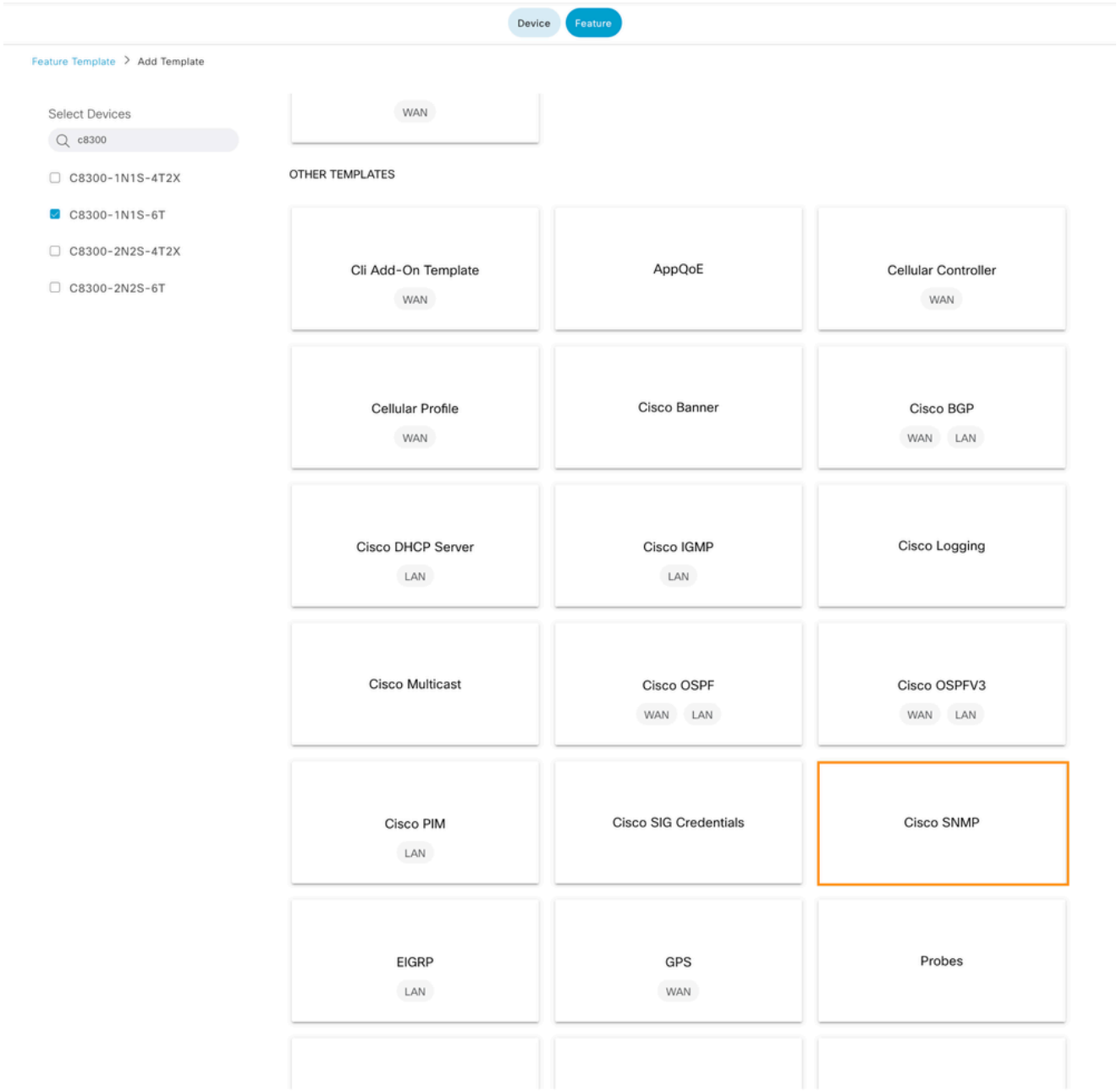
축하드립니다, 그것이 필요한 전부입니다. 이제 cli 및 개념을 통해 Catalyst SD-WAN Manager에서 SNMP 기능 템플릿을 사용하여 구성하는 방법을 확인할 수 있습니다

Cisco vManage > Configuration > Templates > Feature로 이동합니다.



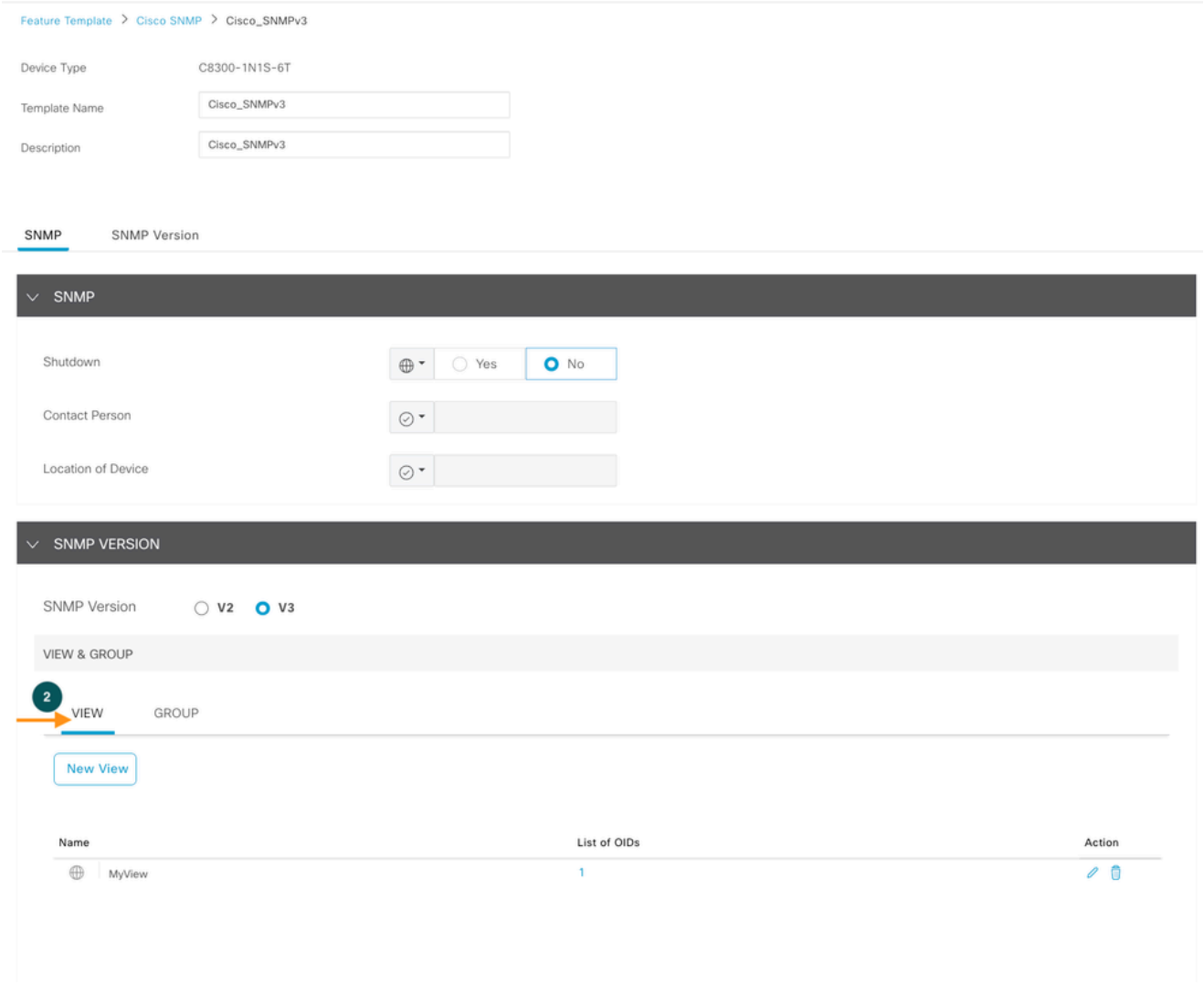
- 기능 템플릿

Other Template(기타 템플릿) 섹션에 있는 Cisco SNMP로 이동합니다.

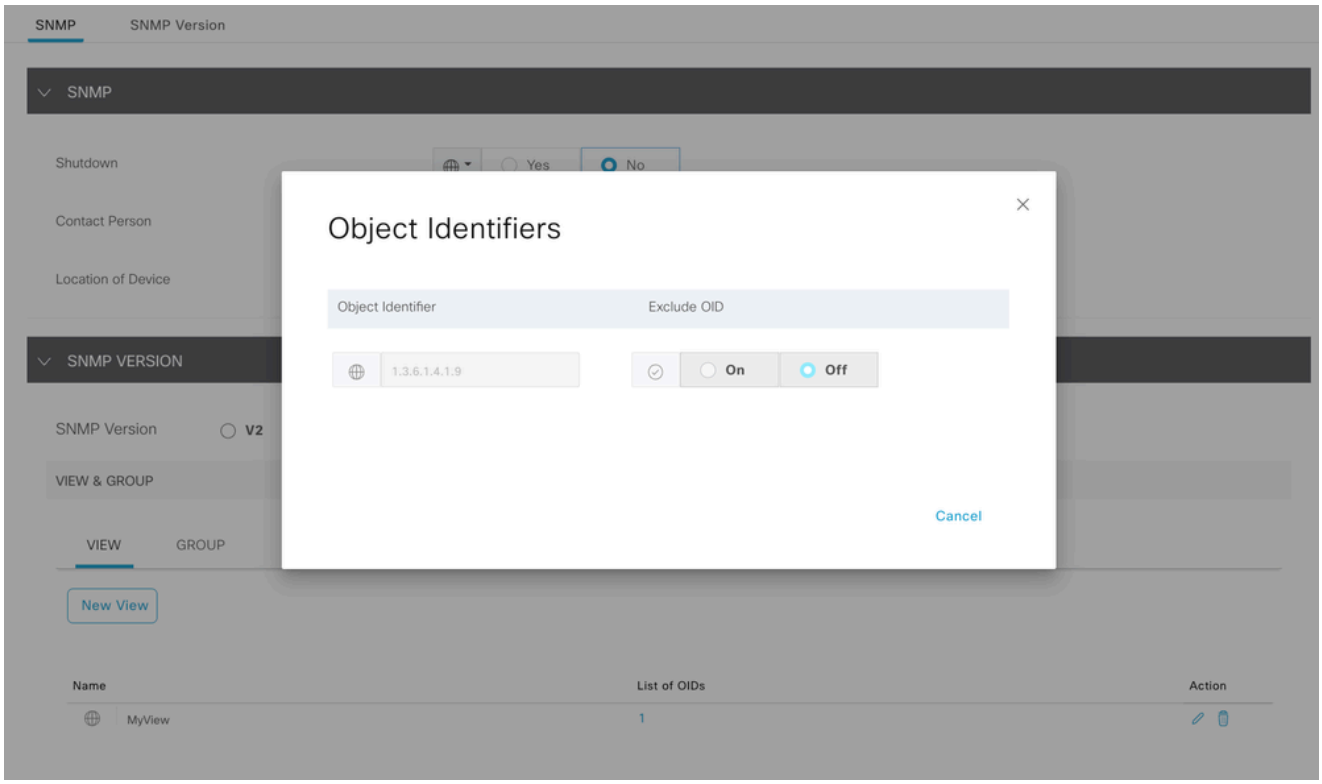


- SNMP 기능

SNMP 보기(제한)를 정의합니다. 2단계입니다.

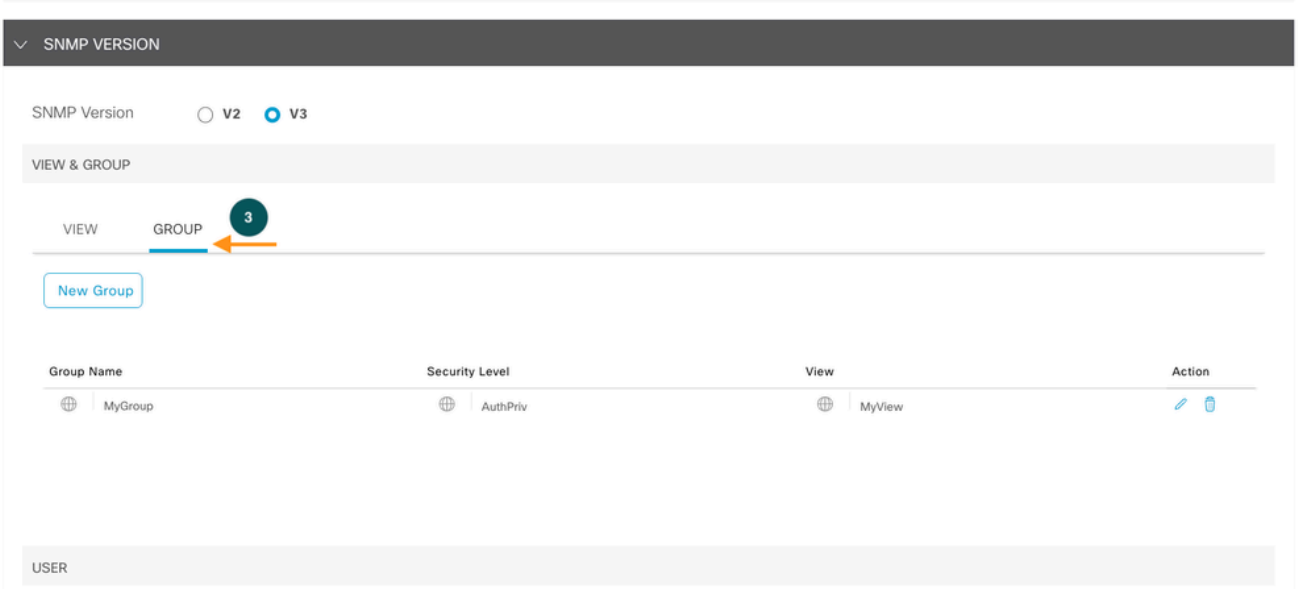

Feature Template > Cisco SNMP > Cisco_SNMPv3
Device Type
C8300-1N1S-6T
Template Name
Cisco_SNMPv3
Description
Cisco_SNMPv3
SNMP
SNMP Version
SNMP
Shutdown
Yes
No
Contact Person
Location of Device
SNMP VERSION
SNMP Version
V2
V3
VIEW & GROUP
2
VIEW
GROUP
New View
Name
List of OIDs
Action
MyView
1

- SNMP 보기



SNMP OID

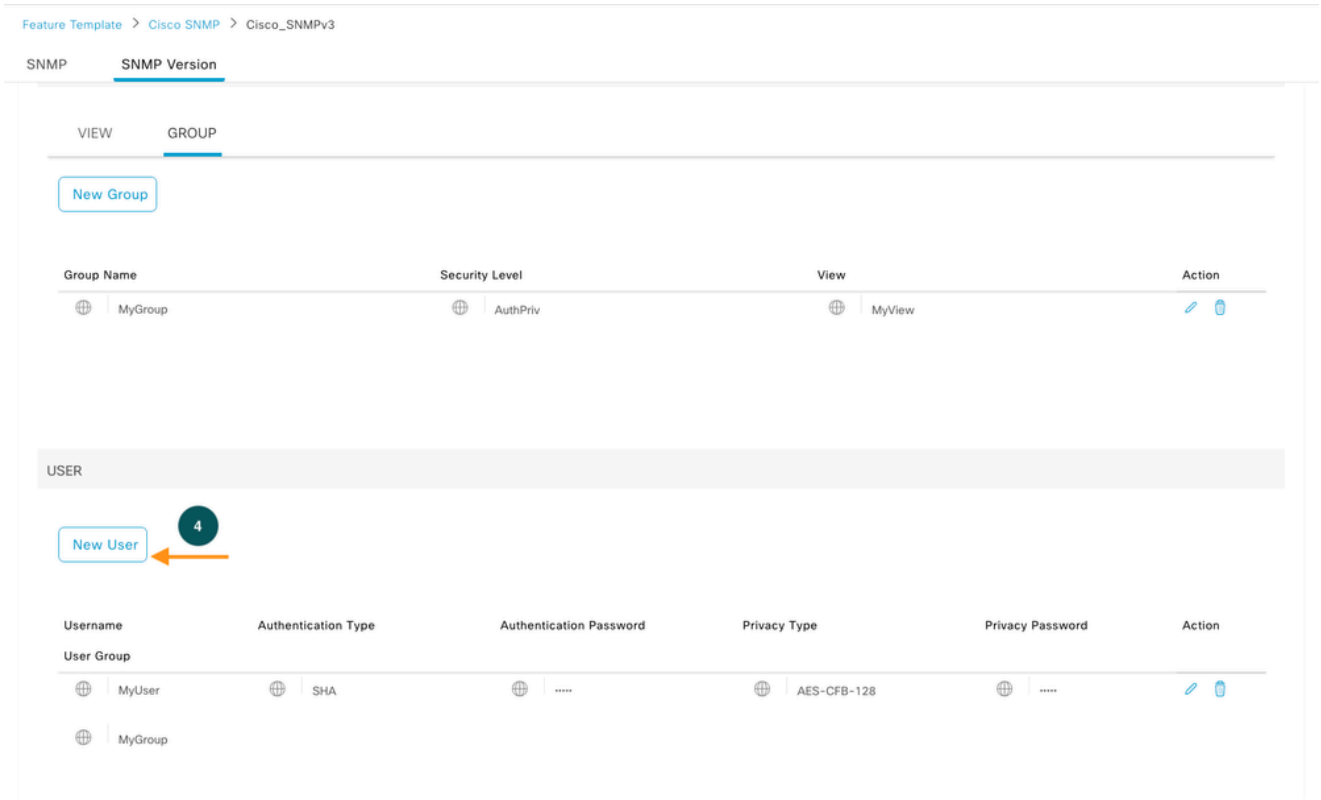
SNMP 그룹을 정의합니다. 3단계입니다.



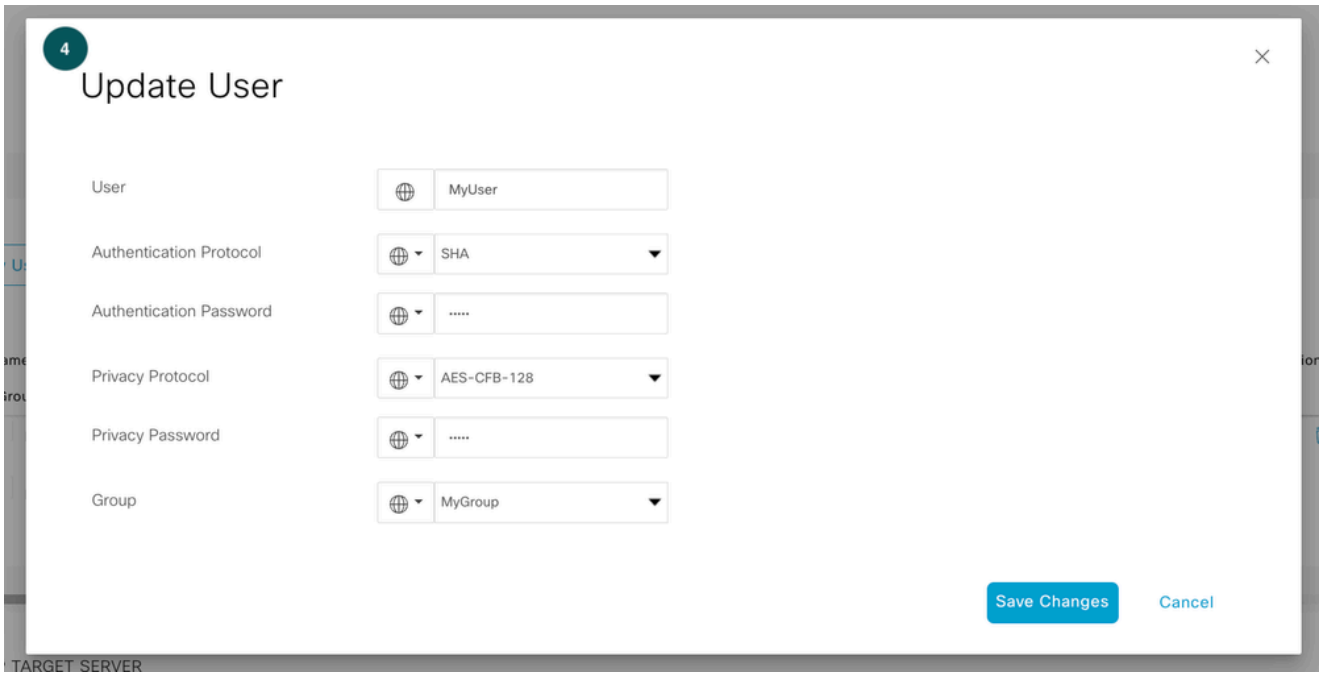
SNMP 그룹

SNMP 그룹

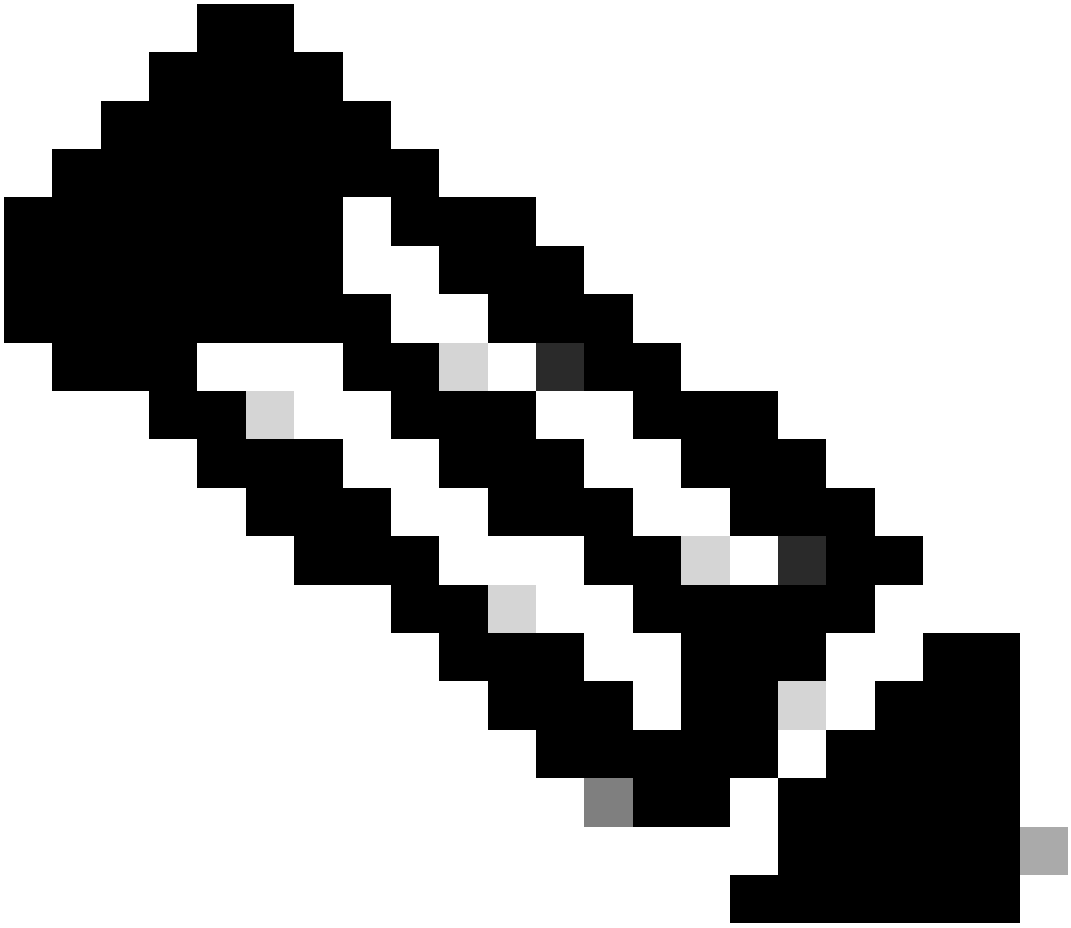
사용자 그룹을 정의합니다. 이 단계에서는 인증 및 암호화 비밀번호를 정의합니다.



SNMP 사용자

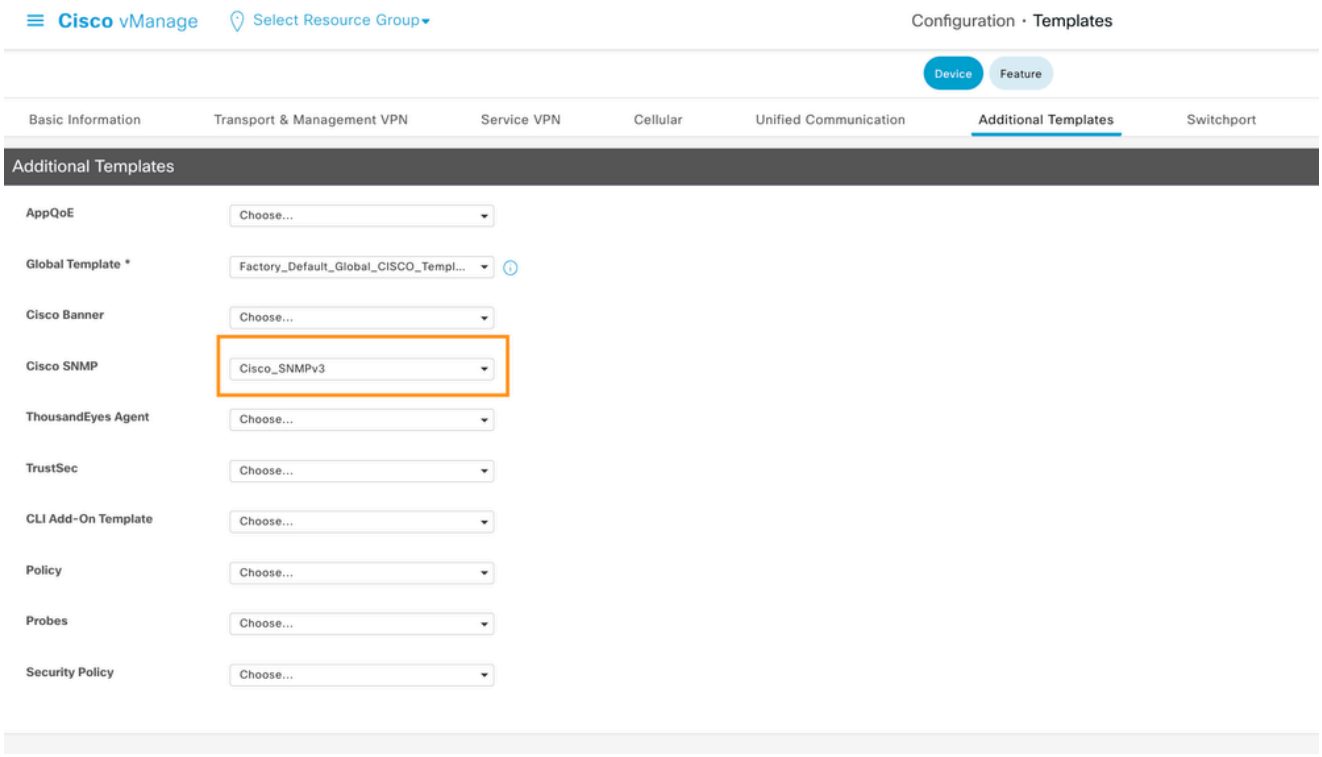
- 
4
Update User
User
MyUser
Authentication Protocol
SHA
Authentication Password
Privacy Protocol
AES-CFB-128
Privacy Password
Group
MyGroup
Save Changes
Cancel
TARGET SERVER

SNMP 사용자 암호화



참고: SNMP 그룹 보안 수준에 따라 사용자와 연결된 각 필드가 활성화됩니다.

이제 기능 템플릿을 디바이스 템플릿에 연결합니다.



-

SNMP 기능 템플릿

다음을 확인합니다.

```
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
```

snmpwalk가 설치된 시스템에서 명령을 실행하여 각 보안 레벨에 대한 SNMP 응답을 확인할 수 있습니다

```
!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: 버전 (3)

-l: 보안 수준

-A: 인증 프로토콜 암호

-X: 프라이버시 프로토콜 암호

참조

- Cisco Edge Router에서 SNMPv3 트랩 구성
- Tim Glen의 SNMPv3 컨피그레이션 템플릿

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.