Konfigurieren von SNMPv3 auf Catalyst SD-WAN

Inhalt

Einleitung

Dieses Dokument beschreibt die SNMPv3-Konfiguration und erläutert die Sicherheit (Authentifizierung), Verschlüsselung (Datenschutz) und Einschränkung (Ansicht).

Hintergrund

Häufig wird die SNMPv3-Konfiguration als komplex und schwierig zu konfigurieren angesehen, bis wir wissen, was zu tun ist. Der Grund für die Existenz von SNMPv3 ist ähnlich wie HTTPS: für Sicherheit, Verschlüsselung und Einschränkungen.

Voraussetzungen

Kenntnis der SD-WAN-Funktionsvorlagen und der Gerätevorlage

Grundlegendes zu SNMP MIB, SNMP Poll und SNMP Walk

Anforderungen

SD-WAN-Controller

Cisco Edge-Router

Verwendete Komponenten

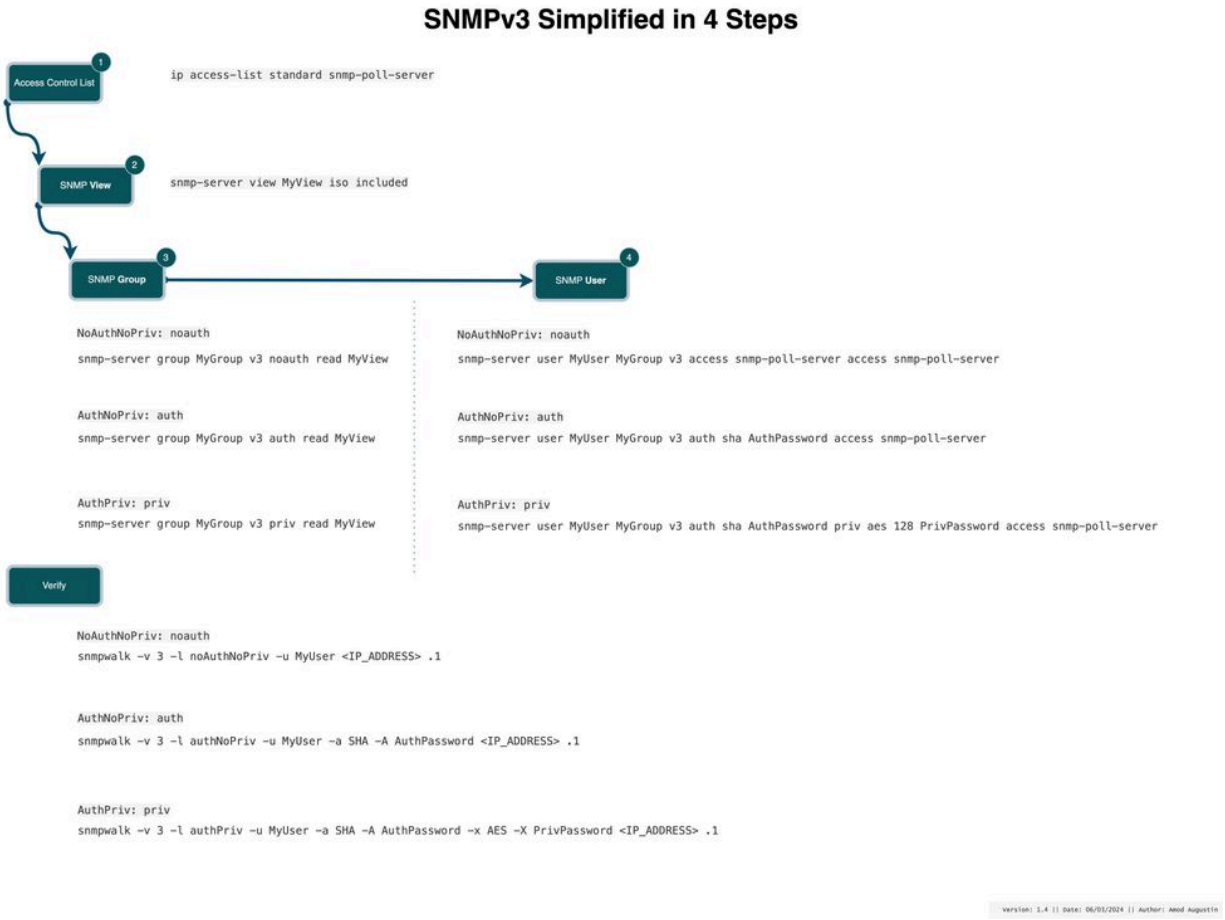
SD-WAN-Controller auf 20.9

Cisco Edge-Router mit 17,9

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Das Diagramm hilft Ihnen zu verstehen, was alles erforderlich ist, um SNMPv3 aus einer CLI-Perspektive zu konfigurieren.



- SNMPv3 in 4 Schritten vereinfacht

Sobald Sie verstanden haben, ist es einfach, das Konzept in der Kommandozeile oder einer Funktionsvorlage zu platzieren. Lassen Sie uns eintauchen.

Schritt 1:

Konfigurieren Sie eine ACL, um zu ermöglichen, wer das System abfragen kann (in unserem Fall der Router).

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

Phase 2:

Definieren Sie eine SNMP-Ansicht, da der Begriff impliziert, auf welche MIBs der Abfrageprozess zugreifen kann. Dies ist unsere Einschränkung.

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

Schritt 3:

SNMP-Gruppe definieren, SNMP-Gruppe besteht hauptsächlich aus zwei Teilen a. Sicherheitsstufe b. Einschränkung (Ansicht).

Sicherheitsstufen:

- NeinAuthNeinPriv: Keine Authentifizierung und kein Datenschutz (keine Verschlüsselung).
- authNoPriv: Authentifizierung ist erforderlich, aber kein Datenschutz.
- authPriv: Sowohl Authentifizierung als auch Datenschutz sind erforderlich.

Einschränkung ist das, was wir in Schritt 2 definiert haben, setzen wir sie alle zusammen.

```
!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
```

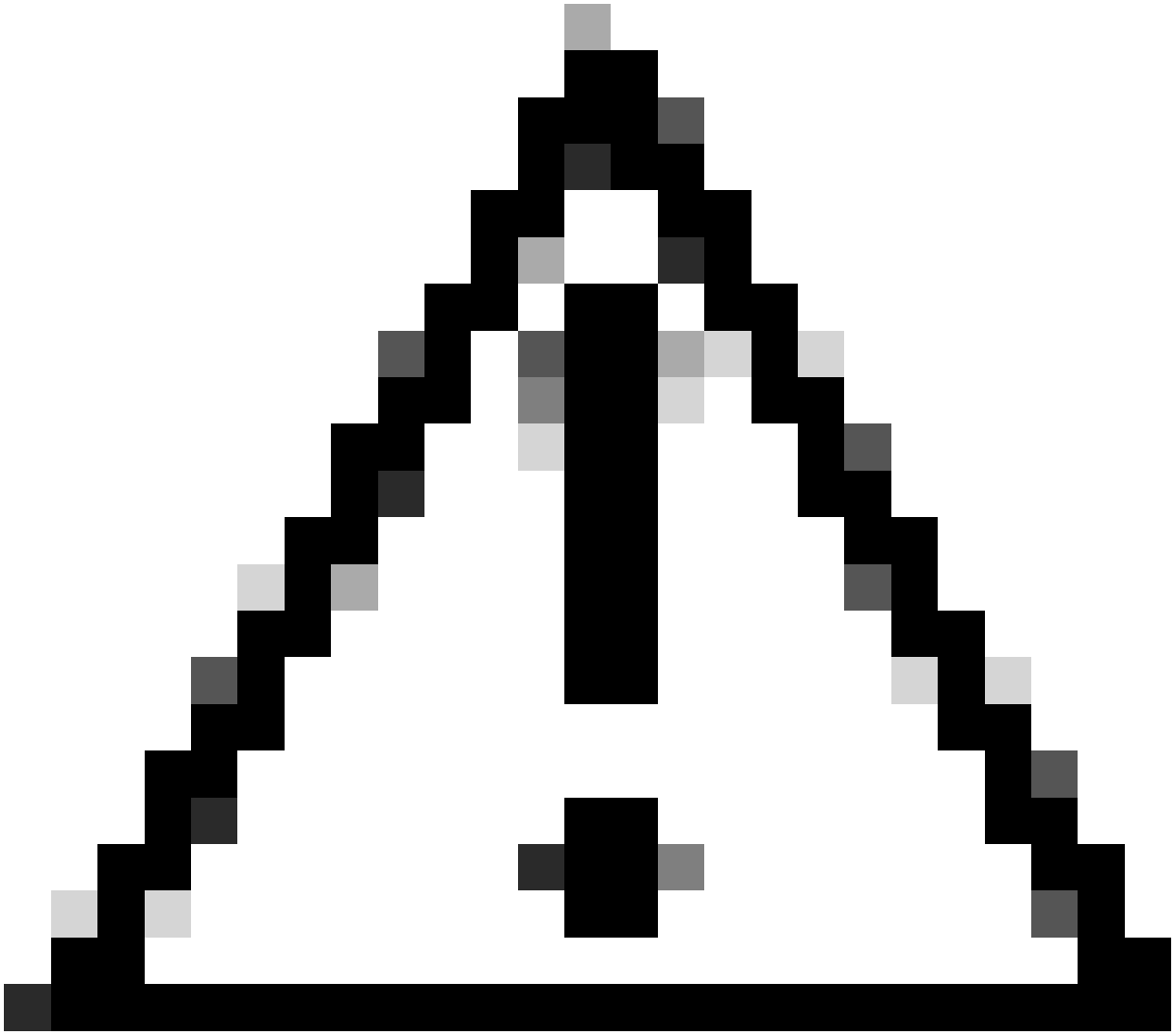
Schritt 4:

In diesem Schritt ordnen wir die Gruppe einem Benutzer zu, ordnen jede Gruppe einem Benutzer zu, der die jeweilige Authentifizierung und den Datenschutz (Verschlüsselung) definiert, und können mithilfe der Zugriffskontrollliste weiter gesichert werden.

```
!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
```



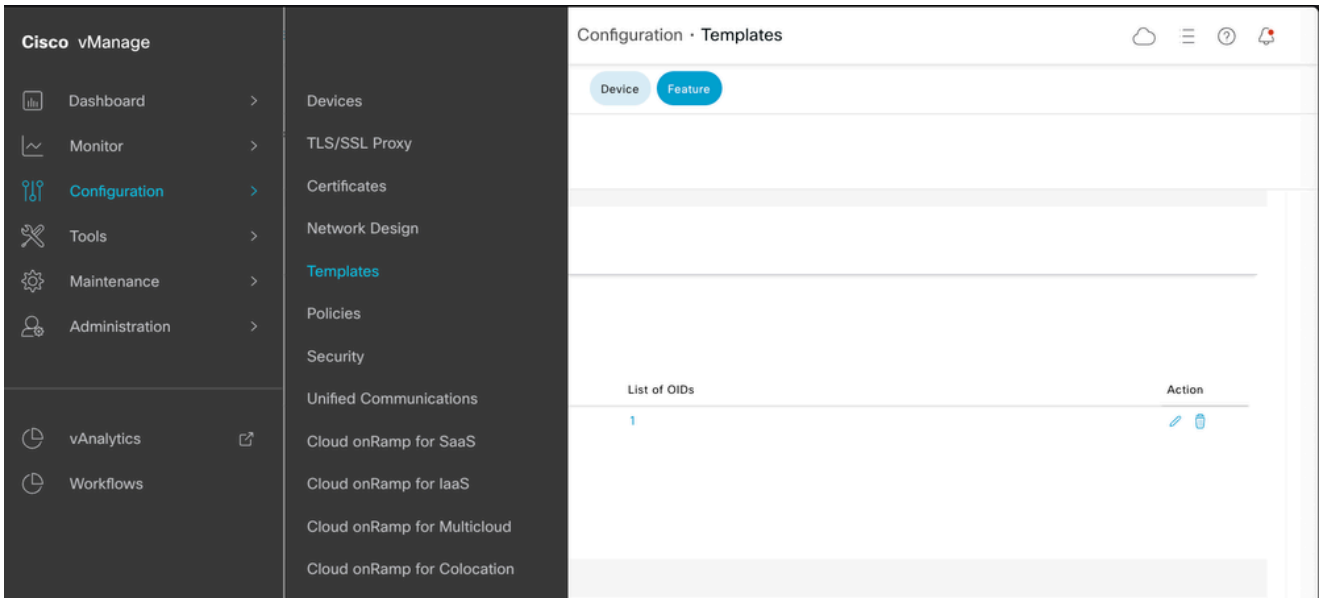
Vorsicht: Wenn Sie versuchen, den SNMP-Serverbenutzer zu konfigurieren, ist die Kontexthilfe nicht verfügbar und wird in der aktuellen Konfiguration auch nicht angezeigt. Dies entspricht RFC 3414. Geben Sie den vollständigen Befehl ein, und der Parser akzeptiert die Konfiguration.

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

Cisco Bug-ID CSCvn71472

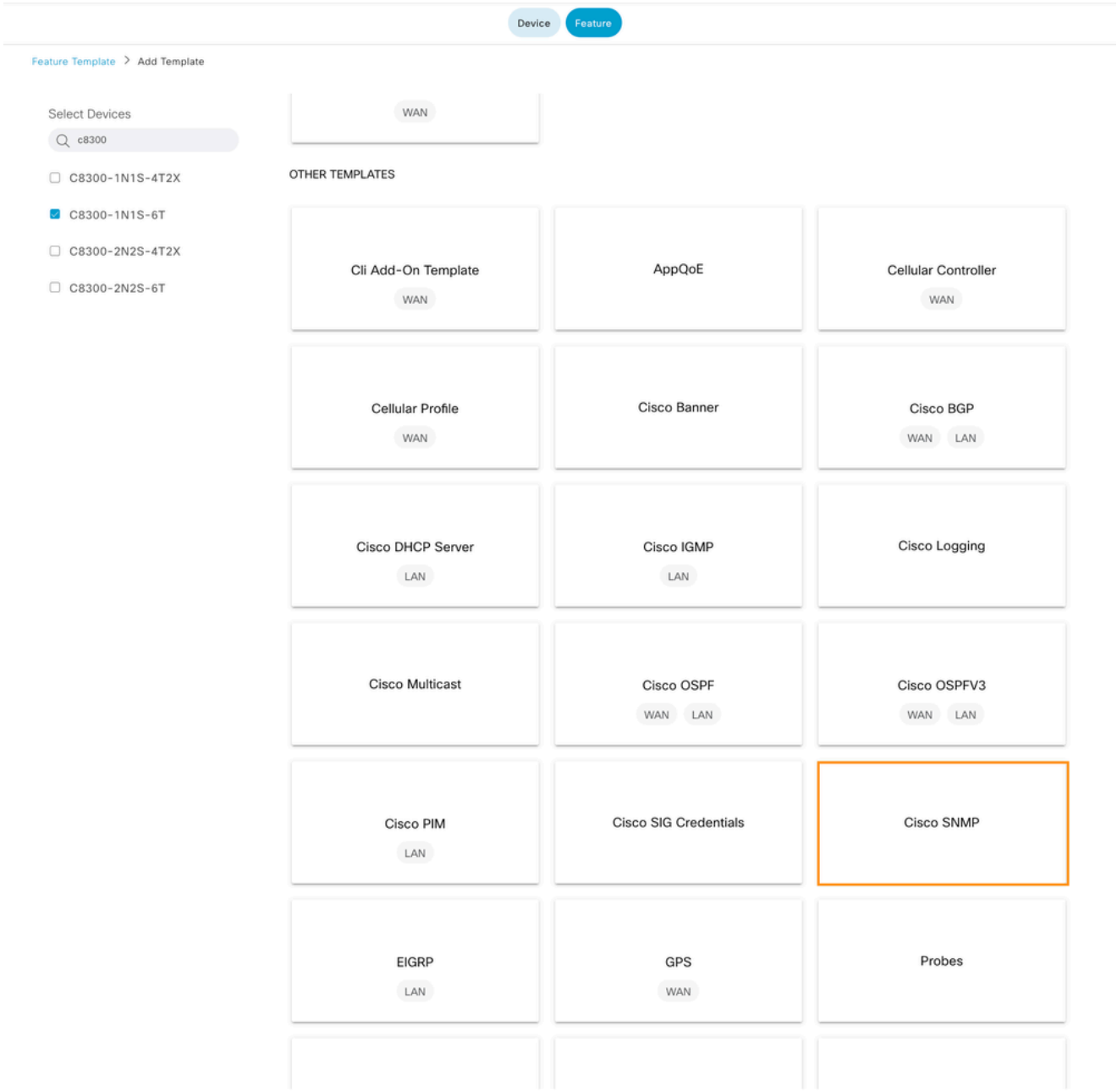
Herzlichen Glückwunsch! Das ist alles, was wir brauchen. Nachdem Sie die CLI und das Konzept kennen, erfahren Sie, wie Sie die SNMP-Funktionsvorlage auf einem Catalyst SD-WAN Manager konfigurieren.

Navigieren Sie zu Cisco vManage > Configuration > Templates > Feature.

- 

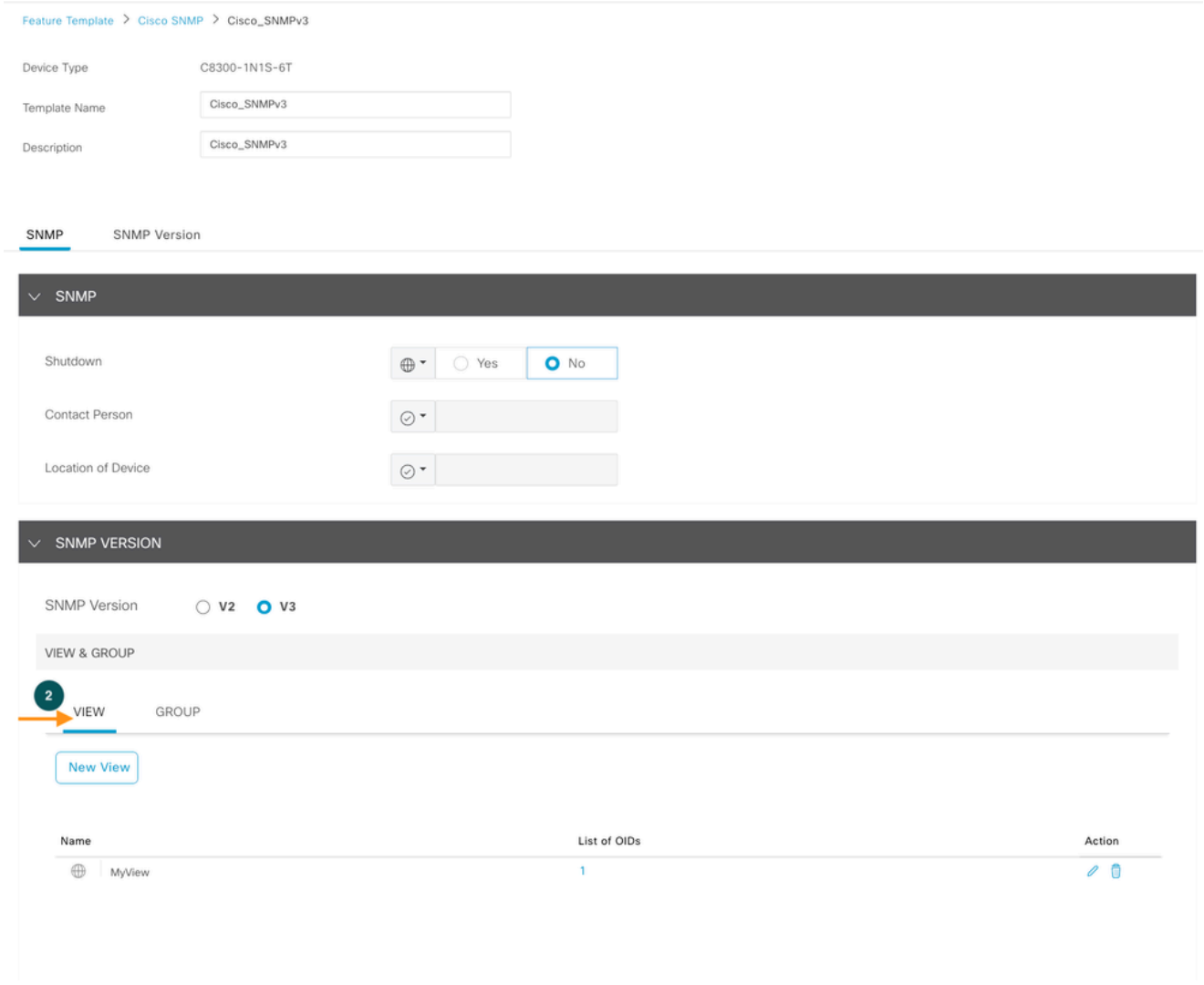
  Funktionsvorlage

Navigieren Sie zu Cisco SNMP, das Sie im Abschnitt "Other Template" (Andere Vorlagen) finden.

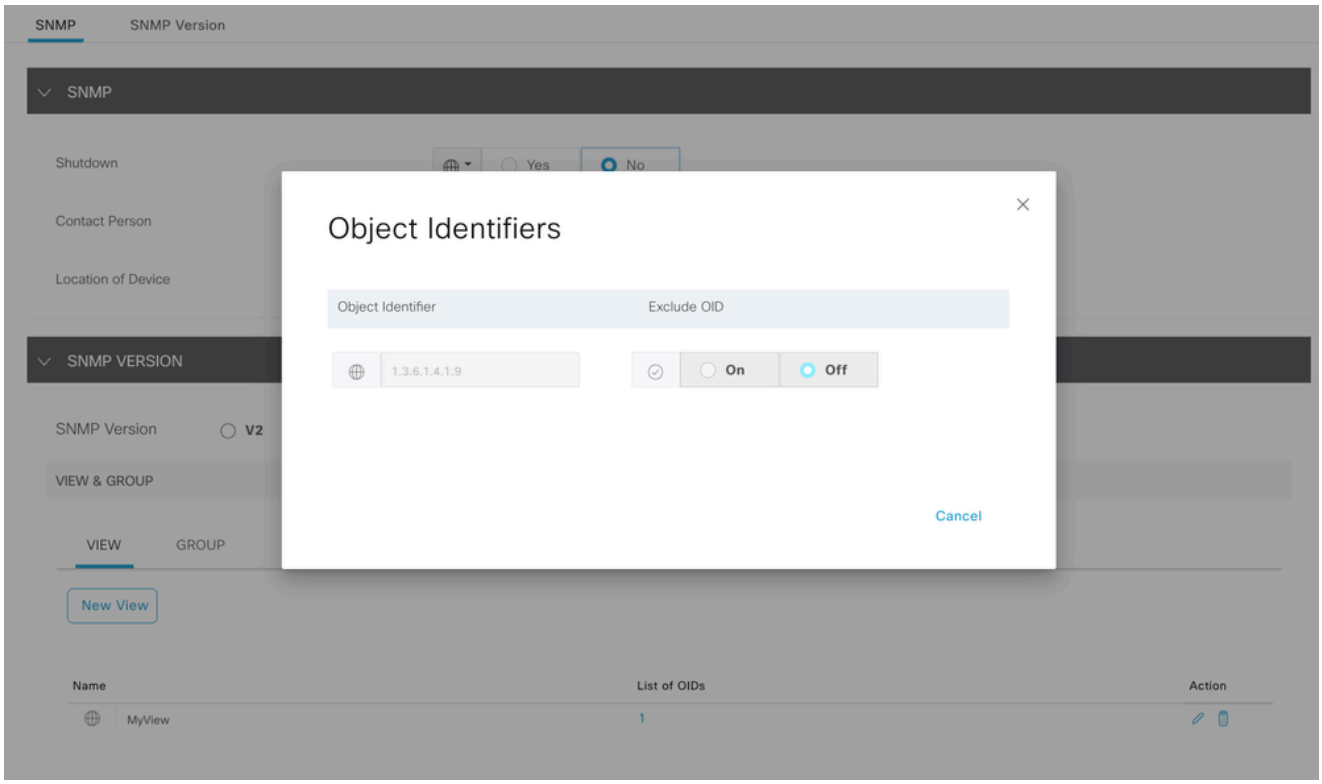


- SNMP-Funktion

SNMP-Ansicht definieren (Einschränkung), unser Schritt 2

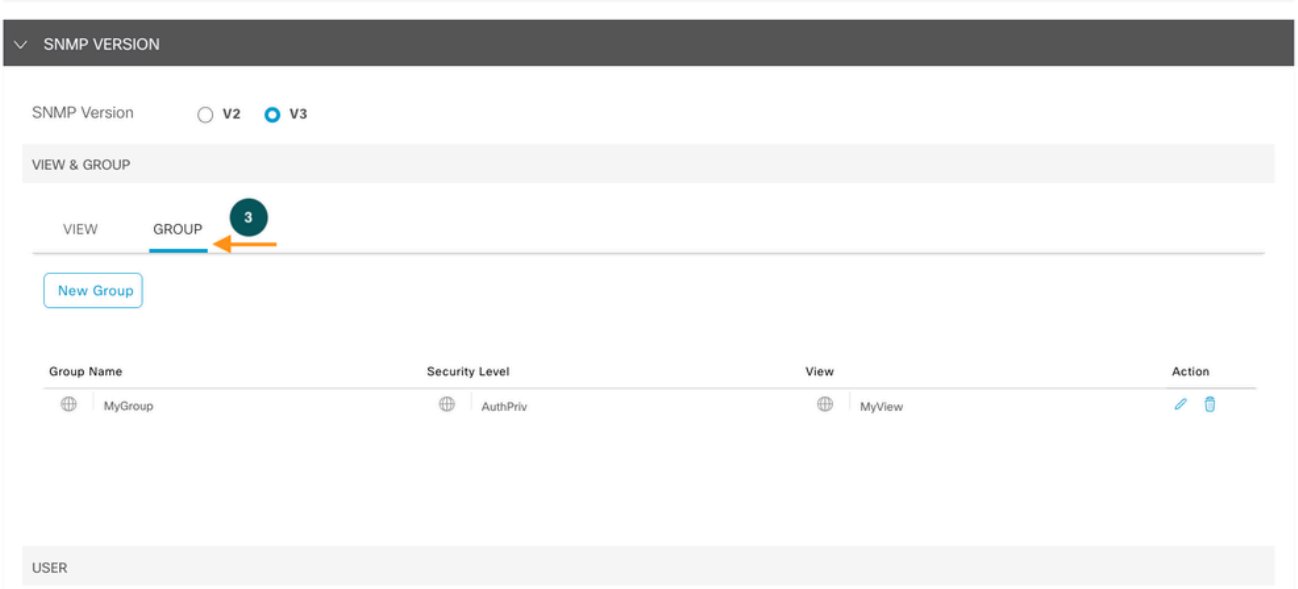


- SNMP-Ansicht



- SNMP-OID

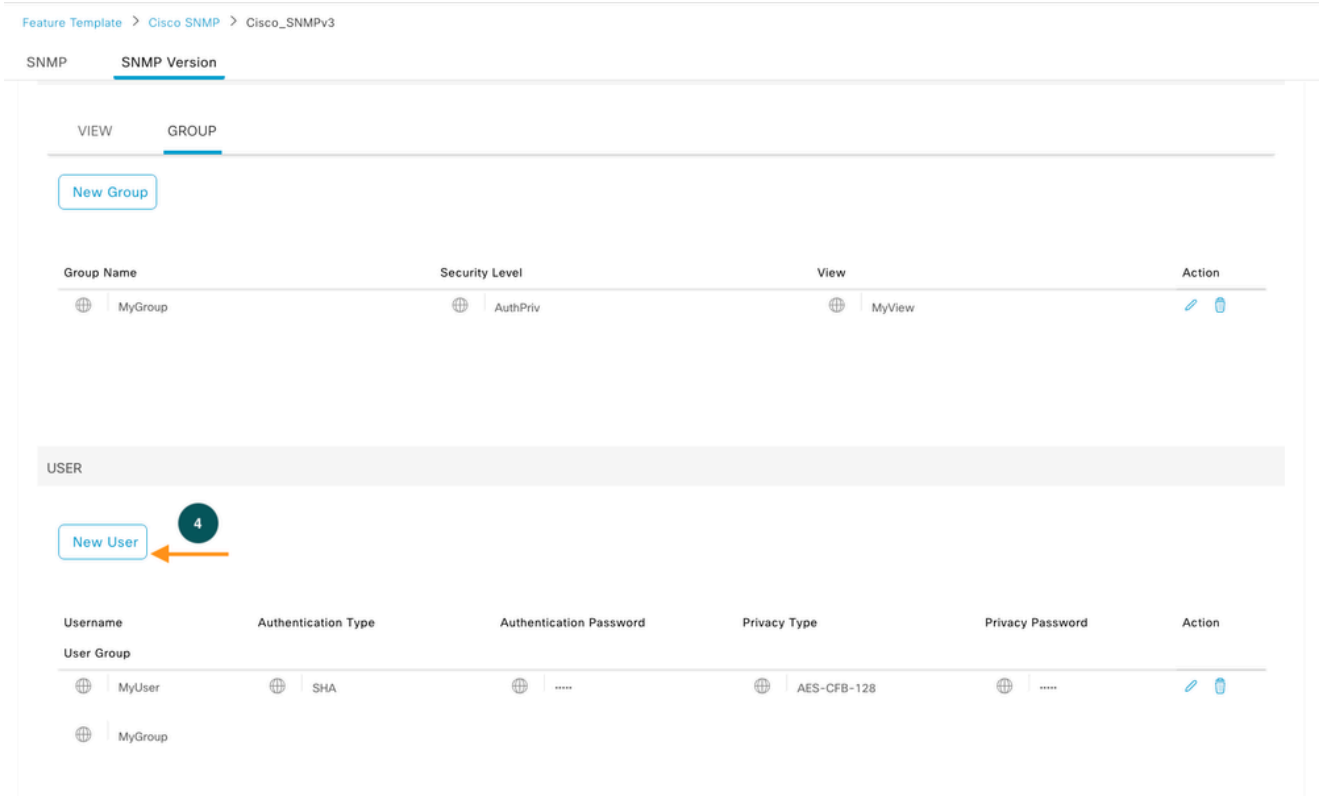
Definieren der SNMP-Gruppe - Dies ist unser Schritt 3



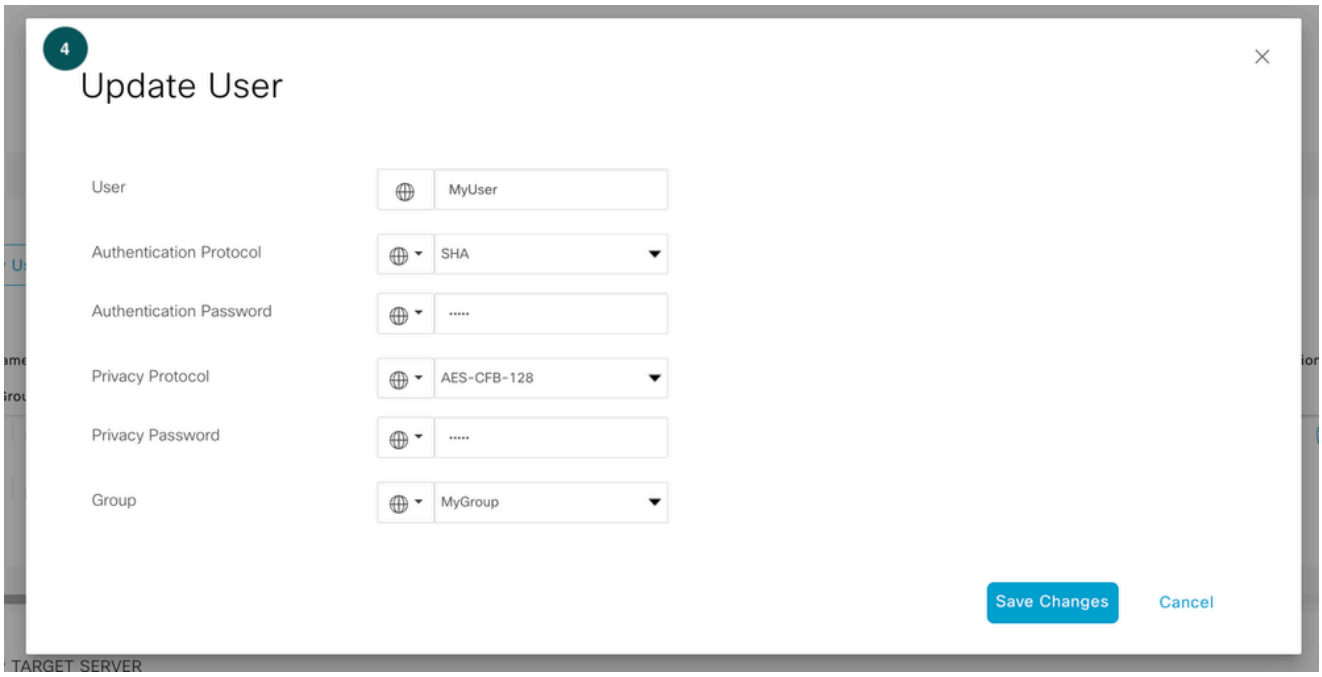
- SNMP-Gruppe

SNMP-Gruppe

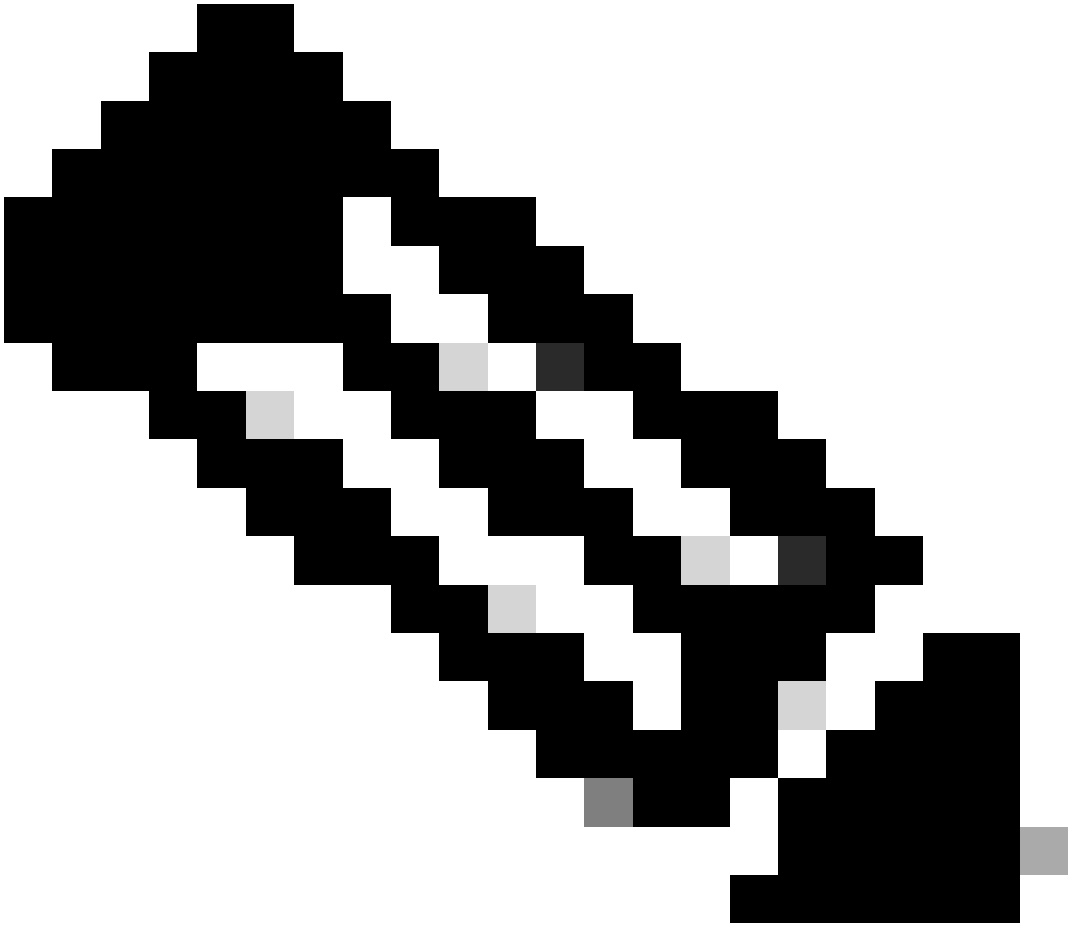
Definieren Sie die Benutzergruppe. Dies ist unser Schritt 4, in dem wir das Authentifizierungs- und Verschlüsselungskennwort definieren.



SNMP-Benutzer

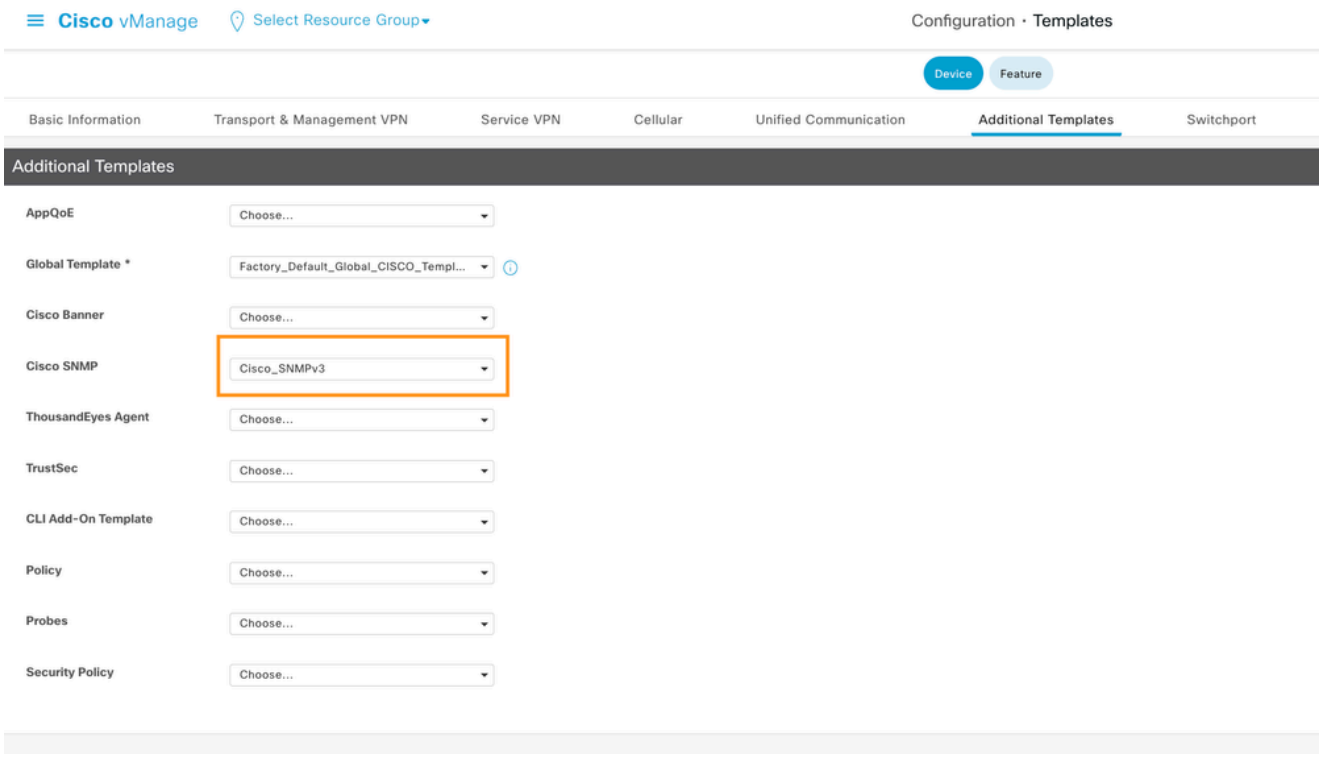
- 

SNMP-Benutzerverschlüsselung



Anmerkung: Basierend auf der Sicherheitsstufe der SNMP-Gruppe wird das entsprechende Feld für den Benutzer aktiviert.

Fügen Sie nun die Funktionsvorlage der Gerätevorlage hinzu.



- SNMP-Funktionsvorlage

Überprüfung

```
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
```

Auf einem Computer, auf dem snmpwalk installiert ist, können Sie den Befehl ausführen, um die SNMP-Antwort auf die entsprechende Sicherheitsstufe zu überprüfen.

```
!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: Version (3)

-l: Sicherheitsstufe

-A: Passphrase für das Authentifizierungsprotokoll

-X: Datenschutzprotokoll-Kennsatz

Referenzen

- SNMPv3-Trap auf dem Cisco Edge-Router konfigurieren
- Konfigurationsvorlage für SNMPv3 von Tim Glen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.