# SNMP configureren op RV160- en RV260-routers

## Doel

Het doel van dit artikel is om u te tonen hoe u de instellingen Simple Network Management Protocol (SNMP) kunt configureren op de RV160- en RV260-routers.

## Inleiding

SNMP is een Internet-standaard protocol voor het verzamelen en organiseren van gegevens over beheerde apparaten op de IP netwerken. Hiermee kunnen netwerkbeheerders belangrijke gebeurtenissen beheren, controleren, ontvangen zoals ze op het netwerk optreden, en probleemoplossing.

Het SNMP-kader bestaat uit drie elementen; een SNMP-beheerder, een SNMP-agent en een Management Information Base (MIB). De functie van SNMP Manager is om de activiteiten van de netwerkhosts te controleren en te controleren die gebruik maken van SNMP. De SNMP-agent bevindt zich in de software van het apparaat en ondersteunt het bij het onderhoud van gegevens om het systeem te kunnen beheren. Tot slot is MIB een virtueel opslaggebied voor netwerkbeheerinformatie. Deze drie combineren om de apparaten in een netwerk te controleren en te beheren.

RV160/260-apparaten ondersteunen SNMP-versie v1, v2c en v3. Ze fungeren als SNMP-agents die SNMP-opdrachten van SNMP-netwerkbeheersystemen beantwoorden. De ondersteunde opdrachten zijn de standaard SNMP-opdrachten krijgen/volgende/ingesteld. De apparaten genereren ook valberichten om de SNMP manager op de hoogte te stellen als de alarmcondities zich voordoen. Tot de voorbeelden behoren herstart, stroomcycli en WAN-linkgebeurtenissen.

## Toepasselijke apparaten

- RV160
- RV260

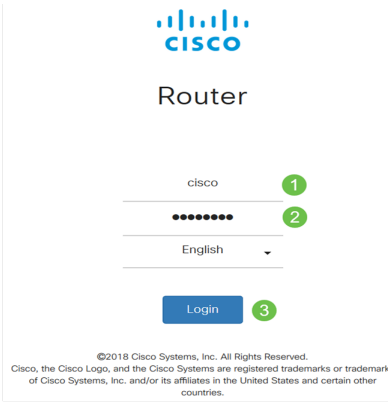
## Softwareversie

- 1.0.00.13

## SNMP configureren

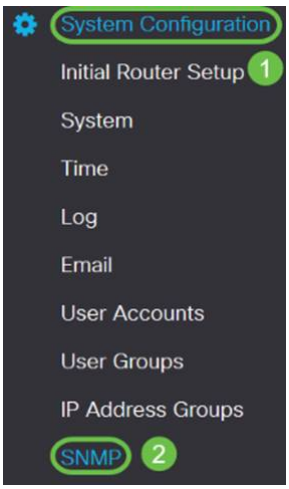
Om SNMP van de router te configureren voert u de volgende stappen uit.

Stap 1. Meld u aan bij de webconfiguratie van uw router.



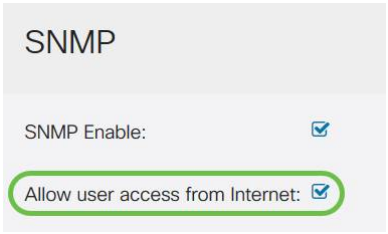

Opmerking: In dit artikel gebruiken we de RV260W om SNMP te configureren. De configuratie kan variëren afhankelijk van het model dat u gebruikt.

Stap 2. Navigeer naar **systeemconfiguratie > SNMP**.




Stap 3. Controleer het aanvinkvakje **SNMP inschakelen** om SNMP in te schakelen.


Stap 4. (Optioneel) Controleer het aanvinkvakje **Toegang voor gebruiker via internet** zodat geautoriseerde gebruikers toegang hebben tot het netwerk via beheertoepassingen zoals Cisco FindIT Network Management.

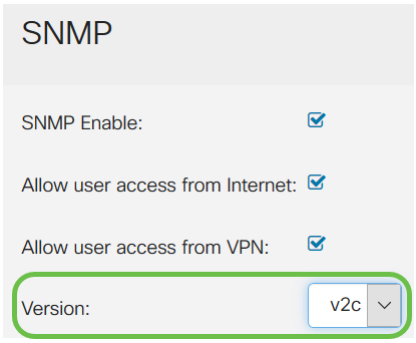



Stap 5. (Optioneel) Controleer het aanvinkvakje **Toegang voor gebruiker via VPN** om geautoriseerde toegang van een Virtual Private Network (VPN) mogelijk te maken.


Stap 6. Kies in het vervolgkeuzemenu *Versie*, een SNMP-versie die u op het netwerk wilt gebruiken. De opties zijn:

- v1 - minst beveiligde optie. Gebruikt kladtekst voor community strings.
- v2c - De verbeterde ondersteuning voor foutenbehandeling van SNMPv2c omvat uitgebreide foutcodes die verschillende soorten fouten onderscheiden; alle soorten fouten worden door één foutcode in SNMPv1 gerapporteerd.
- v3 - SNMPv3 biedt veilige toegang tot apparaten door gegevenspakketten via het netwerk te authentiseren en te versleutelen. Verificatiealgoritmen omvatten berichtdigest-algoritme (MD5) en veilig hash-algoritme (SHA). Encryptiemethoden zijn onder meer Data Encryption Standard (DES) en Advanced Encryption Standard (AES).

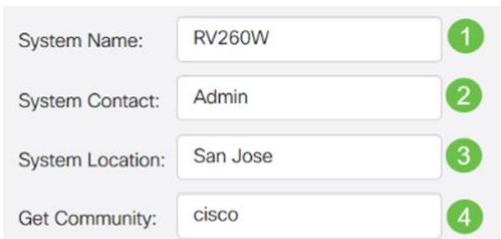
Klik hier voor meer informatie over SNMPv3.




In dit voorbeeld is **v2c** geselecteerd als de *Versie*.

Stap 7. Voer de volgende velden in

- **Systeemnaam** - Voer een naam in voor de router om gemakkelijker te kunnen worden herkend in netwerkbeheertoepassingen.
- **Systeemcontact** - Voer een naam in van een individu of beheerder om deze te identificeren met de router in geval van nood.
- **Systeemlocatie** - Voer een locatie van de router in. Dit maakt de lokalisatie van een probleem veel gemakkelijker voor een beheerder.
- **Community**-naam van de SNMP-community in het veld *Get Community*. Het creëert een alleen-lezen gemeenschap die wordt gebruikt om de informatie voor SNMP agent te benaderen en terug te krijgen.
- **Community**-naam instellen in het veld *Set Community*. Het creëert een read-Writcommunity die wordt gebruikt om de informatie voor SNMP-agents te benaderen en aan te passen. Alleen verzoeken van de hulpmiddelen die zich met deze gemeenschapsnaam identificeren worden aanvaard. Dit is een door de gebruiker gemaakte naam. Het standaard is privé.

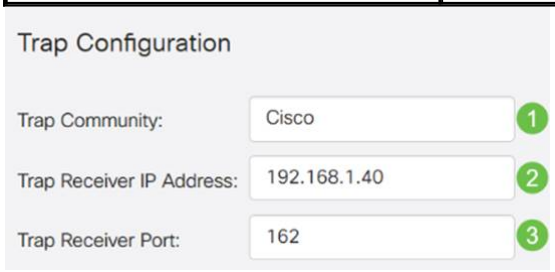


## Vlagconfiguratie

Met behulp van Trap configuraties kunt u het bronadres van elk SNMP-valpakket instellen dat door de router naar één adres wordt verzonden ongeacht de uitgaande interface.

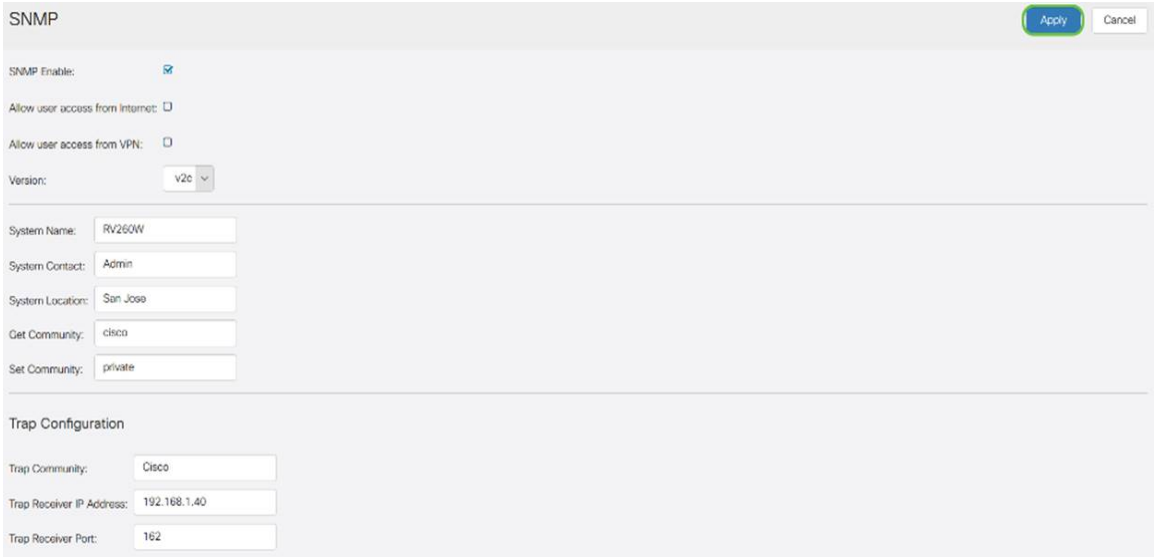
Stap 8. Om de SNMP-val te configureren voert u de volgende informatie in.

| | |
|---|---|
| **Trap Community** | Voer de naam van de valgemeenschap in |
| **IP-adres voor Trap ontvanger** | Voer het IP-adres in |
| **Trap-ontvangerpoort** | Voer het poortnummer in |




Opmerking: Meestal gebruikt SNMP User Datagram Protocol (UDP) als het transportprotocol en de standaard UDP-poorten voor SNMP-verkeer zijn 161 (SNMP) en 162 (SNMP-trap).

Stap 9. Klik op **Toepassen**.




U hebt nu SNMP ingeschakeld en ingesteld op uw RV160/RV260-router.