SNMP-configuratie op de RV315W VPN-router

Doel

Simple Network Management Protocol (SNMP) is een TCP/IP-protocol voor netwerkbeheer. SNMP stelt beheerders in staat om netwerkprestaties, foutensnelheden te controleren. SNMP kan ook netwerkbeschikbaarheid in kaart brengen. Het SNMP-kader bestaat uit drie elementen; een SNMP-manager, een SNMP-agent en een 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. Ten slotte is de Management Information Base (MIB) een virtueel opslaggebied voor netwerkbeheerinformatie. Deze drie combineren om de apparaten in een netwerk te controleren en te beheren.

Dit artikel helpt uit te leggen hoe u SNMP op de RV315W VPN-router kunt configureren.

Toepassbaar apparaat

- RV315W

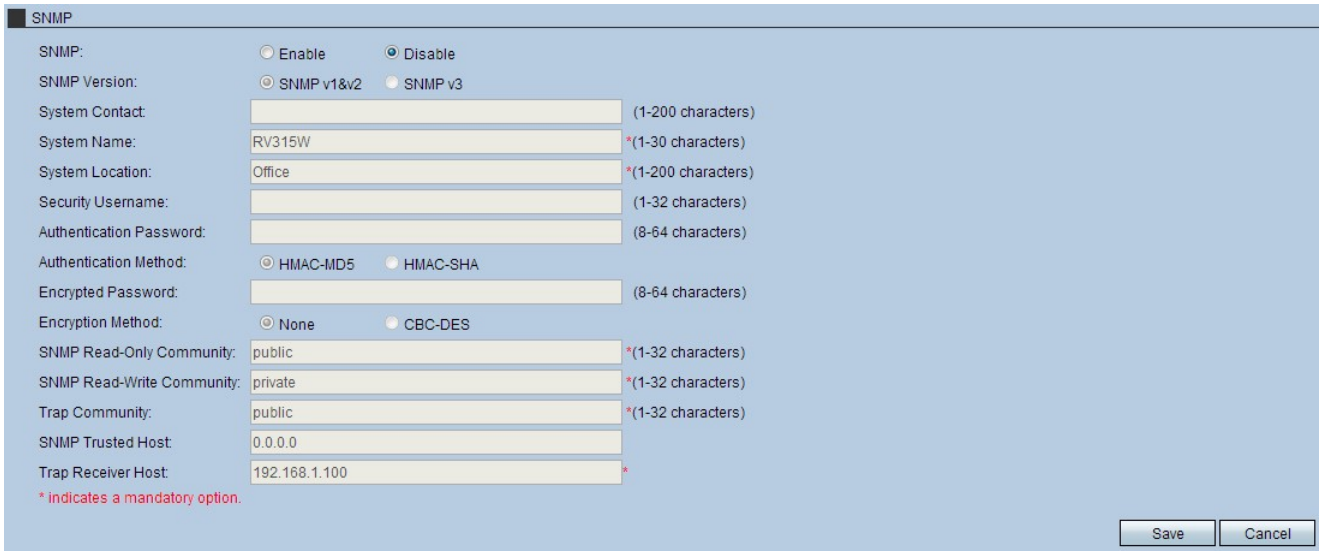
Softwareversie

•1.01.03

SNMP configureren

SNMP v1 is de oorspronkelijke versie van SNMP, die bepaalde functionaliteit ontbeert en alleen werkt op TCP/IP-netwerken, SNMP v2 is een verbeterde iteratie van v1. SNMP v1&v2 dient alleen te worden geselecteerd voor netwerken die SNMPv1 of SNMPv2 gebruiken. SNMP v3 is de nieuwste standaard van SNMP en behandelt veel problemen van SNMP v1 en v2. In het bijzonder: veel van de veiligheidskwetsbaarheden van v1 en v2. SNMP v3 staat ook beheerders toe om naar één gemeenschappelijke SNMP standaard te bewegen.

Stap 1. Meld u aan bij het web configuratie hulpprogramma en kies **systeembeheer > SNMP** . De *SNMP*-pagina wordt geopend:



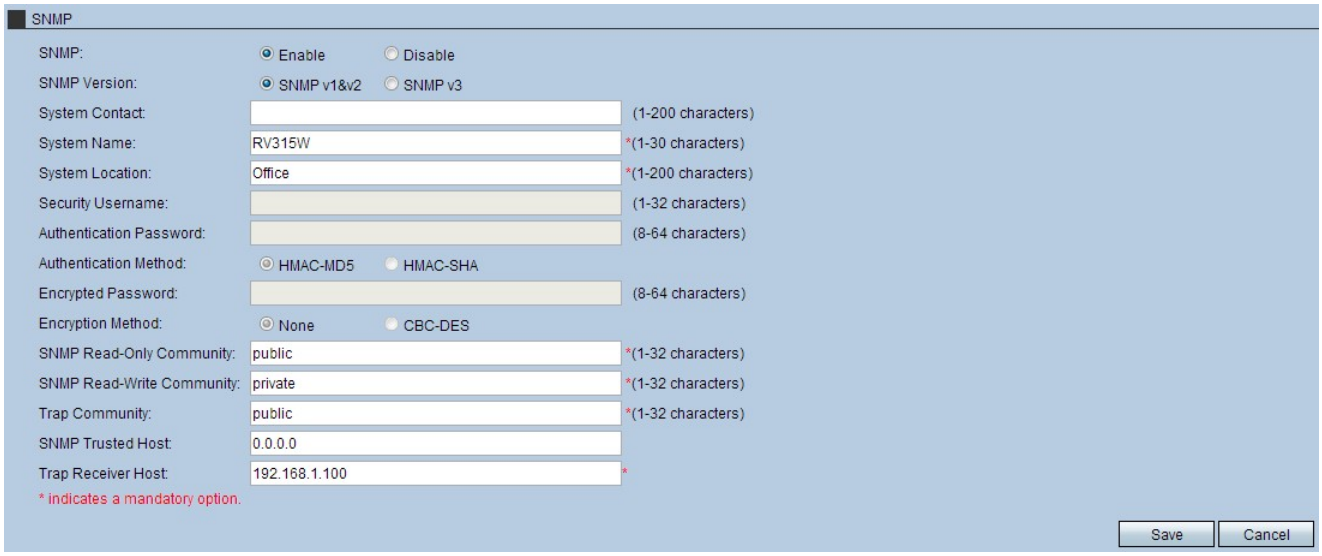
Stap 2. Klik op de radioknop **Enable** om SNMP in te schakelen.

Stap 3. Klik op de gewenste SNMP-versie.

- SNMP v1&v2 — SNMP v1 is de oorspronkelijke iteratie van SNMP en heeft geen bepaalde functionaliteit. SNMP v2 is de nieuwere versie die de functionaliteit verbetert, maar deze optie dient alleen te worden gekozen voor netwerken die SNMP v1 of SNMP v2 uitvoeren.

- SNMP v3 — SNMP 3 is de nieuwste versie, waarmee beheerders één standaard kunnen gebruiken. Deze optie dient te worden gekozen omdat deze veel beveiligingsfouten lapt binnen v1 en v2.

SNMP configureren voor SNMP v1&v2



Stap 4. (Optioneel) Voer de contactinformatie in het veld Systeemcontactgegevens in. Dit is het individu dat contact moet opnemen voor netwerkassistentie.

Stap 5. Voer een naam in het veld Systeemnaam in. Dit is de naam die aan SNMP-instellingen is toegewezen.

Stap 6. Voer een locatie in het veld Systeemlocatie in. Dit is waar het systeem zich bevindt.

Stap 7. Voer een gemeenschap in het veld Alleen-lezen van SNMP in. Dit is de client

parameter voor alleen-lezen toegang van de SNMP-instellingen.

Stap 8. Voer een community in het veld SNMP Read-Write Community-veld in. Dit is de client parameter voor lees- en schrijftoegang van de SNMP-instellingen.

Stap 9. Voer een gemeenschap in het veld Vak. Dit is de gemeenschap met de mogelijkheid om SNMP-vallen te gebruiken. Trappen zijn gerichte meldingen die naar de beheerder worden gestuurd. Trappen staan de beheerder toe om elk apparaat te beheren door hun gebruiker toe te staan om hen door het gebruiken van een val te informeren.

Stap 10. Voer een host in het veld SNMP Trusted Host in. Dit is het IP-adres van de trust host voor de SNMP-installatie.

Stap 1. Voer een host in het veld Trap ontvangerhost in. Dit is het IP-adres van de beheerder om de vallen te ontvangen.

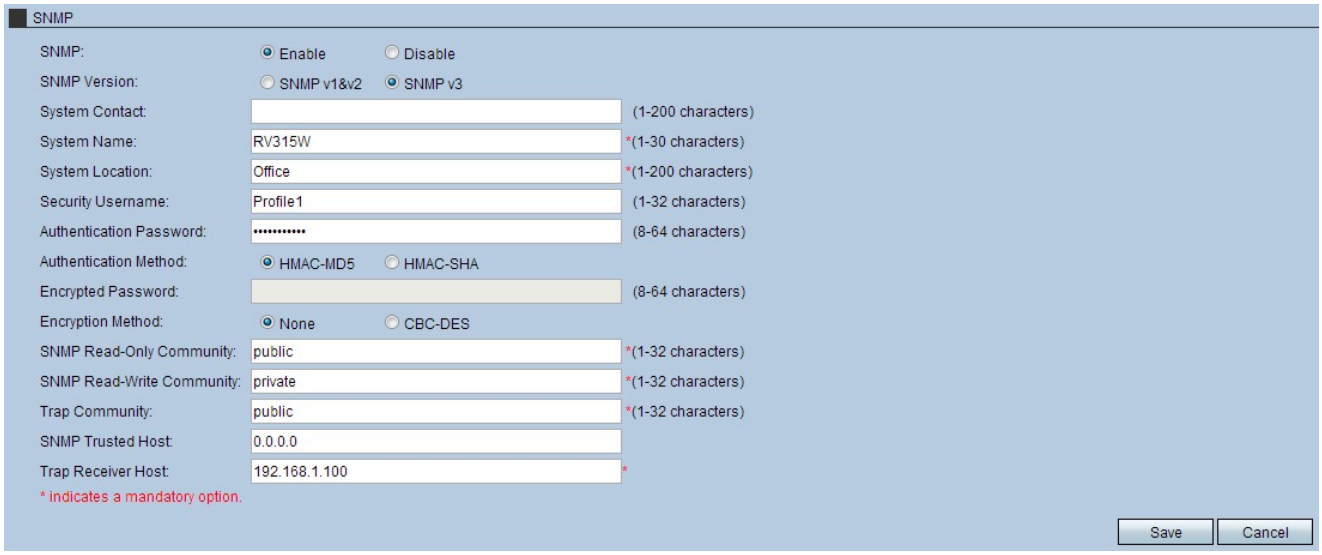
Stap 12. Klik op **Save** om de instellingen toe te passen.

SNMP configureren voor SNMP v3

Stap 4. (Optioneel) Voer de contactinformatie in het veld Systeemcontactgegevens in. Dit is het individu dat contact moet opnemen voor netwerkassistentie.

Stap 5. Voer een naam in het veld Systeemnaam in. Dit is de naam die aan SNMP-instellingen is toegewezen.

Stap 6. Voer een locatie in het veld Systeemlocatie in. Dit is waar het systeem zich bevindt.



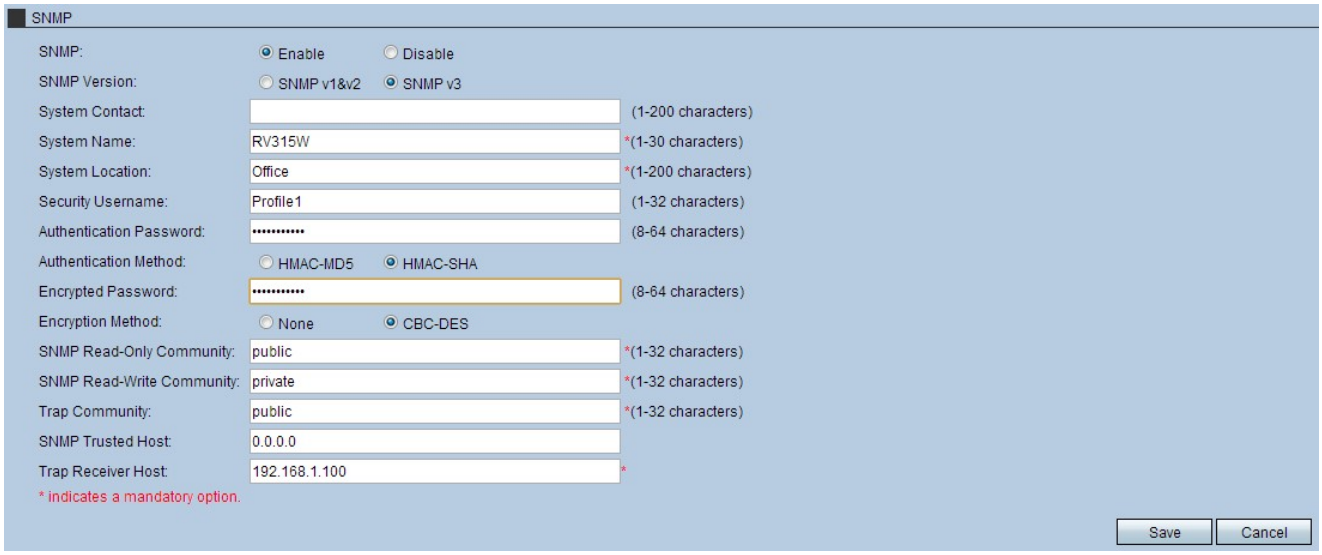
Stap 7. (Optioneel) Voer een gebruikersnaam in in het veld Security Gebruikersnaam. Dit is de gebruikersnaam die wordt gebruikt om toegang tot de SNMP-instellingen te verkrijgen.

Stap 8. (Optioneel) Voer een wachtwoord in het veld Wachtwoord voor verificatie in. Dit is het wachtwoord dat wordt gebruikt om toegang tot de SNMP-instellingen te verkrijgen.

Stap 9. Klik op de radioknop HMAC-MD5 of HMAC-SHA in het veld Verificatiemethode. De Hash-Based Message Verification Code (HMAC) is een gecodeerde code die een authenticatiecode en een geheime cryptografische sleutel combineert. Het primaire doel van HMAC is voor berichtbeveiliging. Een HMAC zal de gegevens op basis van geproduceerde geheime sleutels authenticeren.

- HMAC MD5 — Dit hashalgoritme heeft verschillende veiligheidsgebreken en gegevens kunnen worden gecompromitteerd. De HMAC MD5 is een mechanisme voor de verificatie van berichten met gebruikmaking van cryptografische hashfuncties. MD5 wordt gebruikt in situaties waarin een superieure prestatiesnelheid essentieel is voor een systeem, zij het minder veilig.

- HMAC SHA — Dit hashalgoritme is veel veiliger aangezien de encryptiemethode superieur is. Dit is een veiliger mechanisme voor berichtverificatie met gebruikmaking van cryptografische hashfuncties. HMAC SHA dient te worden gebruikt wanneer veiligheid van vitaal belang is.



Stap 10. Voer een wachtwoord in het veld Versleuteld wachtwoord in.

Stap 1. Klik op de radioknop CBC-DES in het veld Encryption Methode. CBC en DES zijn coderingsstandaarden die combineren met beveiligde gegevens die worden overgebracht.

Stap 12. Voer een community in het veld Alleen-lezen van SNMP in. Dit is de client parameter voor alleen-lezen toegang van de SNMP-instellingen.

Stap 13. Voer een community in het veld SNMP Read-Write Community-veld in. Dit is de client parameter voor lees- en schrijftoegang van de SNMP-instellingen.

Stap 14. Voer een gemeenschap in het veld Vak-community in. Dit is de gemeenschap met de mogelijkheid om SNMP-vallen te gebruiken. Vangen worden gericht aan de beheerder verzonden. Trappen staan de beheerder toe om elk apparaat te beheren door hun gebruiker toe te staan om hen door het gebruiken van een val te informeren.

Stap 15. Voer een host in het veld SNMP Trusted Host in. Dit is het IP-adres van de trust host voor de SNMP-installatie.

Stap 16. Voer een host in het veld Trap ontvangerhost in. Dit is het IP-adres van de beheerder om de vallen te ontvangen.

Stap 17. Klik op **Save** om de instellingen toe te passen.