Simple Network Management Protocol (SNMP)-configuratie voor RV215W

Doel

Simple Network Management Protocol (SNMP) is een protocol op de toepassingslaag dat wordt gebruikt om een netwerk te beheren en te bewaken. SNMP wordt door netwerkbeheerders gebruikt om netwerkprestaties te beheren, netwerkproblemen te detecteren en te corrigeren en netwerkstatistieken te verzamelen. Een SNMP beheerd netwerk bestaat uit beheerde apparaten, agenten, en een netwerkmanager. Beheerde apparaten zijn apparaten die geschikt zijn voor de SNMP optie. Een agent is SNMP-software op een beheerd apparaat. Een netwerkbeheerder is een entiteit die gegevens van de SNMP agenten ontvangt. De gebruiker moet een SNMP v3 Manager-programma installeren om SNMP-meldingen te bekijken.

Dit artikel legt uit hoe je SNMP op de RV215W moet configureren.

Toepasselijke apparaten

- RV215W

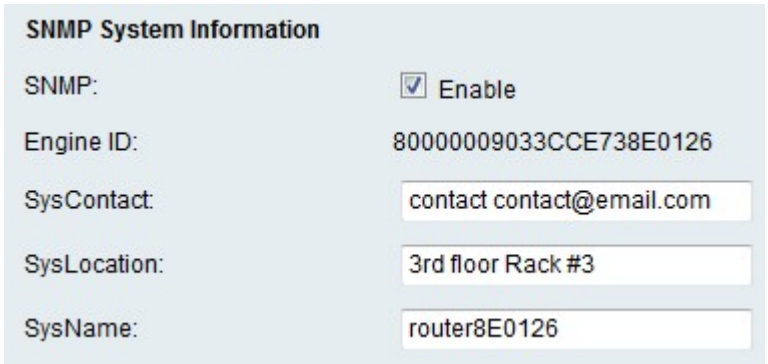
Softwareversie

•1.1.0.5

SNMP-configuratie

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

SNMP-systeeminformatie



Stap 1. Controleer het veld SNMP in om SNMP-configuratie op de RV215W toe te staan.

Opmerking: De motor-ID voor de agent van de RV215W wordt weergegeven in het veld ID van de motor. De motor-ID's worden gebruikt om op een unieke wijze de agenten op de beheerde apparatuur te identificeren.

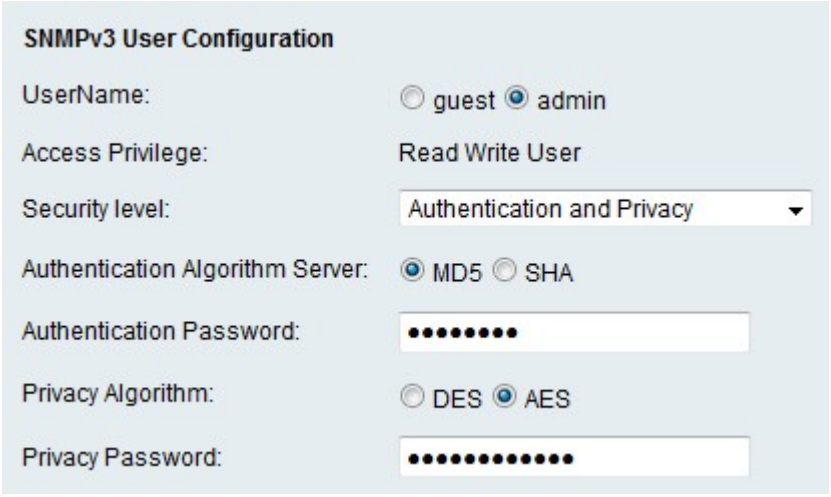
Stap 2. Voer een naam in voor het systeemcontact in het veld SysContact. Het is gebruikelijk om contactgegevens voor het systeemcontact op te nemen.

Stap 3. Voer de fysieke locatie van RV215W in het veld SysLocation.

Stap 4. Voer een naam in voor identificatie van de RV215W in het veld Naam.

Stap 5. Klik op **Opslaan**.

SNMPv3-gebruikersconfiguratie



Stap 1. Klik op de radioknop die overeenkomt met de gewenste account die u in het veld UserName wilt configureren. Het toegangsvoorrecht van de gebruiker wordt weergegeven in het veld Toegangsrecht.

- Guest — Een gastgebruiker heeft alleen rechten gelezen.
- Admin — Een beheerder heeft rechten gelezen en geschreven.

Stap 2. Kies in de vervolgkeuzelijst Beveiligingsniveau de gewenste beveiliging. Verificatie wordt gebruikt om de SNMP-functies te controleren en door gebruikers te laten bekijken of beheren. Privacy is een andere sleutel die gebruikt kan worden om de beveiliging van de SNMP-functie te verhogen.

- Geen verificatie en geen privacy — De gebruiker heeft geen echtheidscontrole of een privacy-wachtwoord nodig.
- Verificatie en geen privacy — Alleen verificatie is vereist door de gebruiker.
- Verificatie en privacy - Zowel verificatie als een privacy-wachtwoord zijn vereist door de gebruiker.

Stap 3. Als het beveiligingsniveau verificatie bevat, klikt u op de radioknop die overeenkomt met de gewenste server in het veld Algorithm Server. Dit algoritme is een hashfunctie. De wasfuncties worden gebruikt om toetsen om te zetten in een toegewezen bits bericht.

- MD5 — Message-Digest 5 (MD5) is een algoritme dat een ingangssignaal bevat en een 128-bits berichtoverzicht van de invoer oplevert.
- SHA - Secure Hash Algorithm (SHA) is een algoritme dat een input neemt en een 160 bit bericht-berichtoverzicht van de invoer produceert.

Stap 4. Voer een wachtwoord in voor de gebruikers in het veld Wachtwoord voor verificatie.

Stap 5. Als het beveiligingsniveau privacy bevat, klikt u op de radioknop die overeenkomt met het gewenste algoritme in het veld Privacy Algorithm.

- DES - Data Encryption Standard (DES) is een encryptie-algoritme dat dezelfde methode gebruikt om een bericht te versleutelen en decrypteren. Het DES-algoritme verwerkt sneller dan AES.

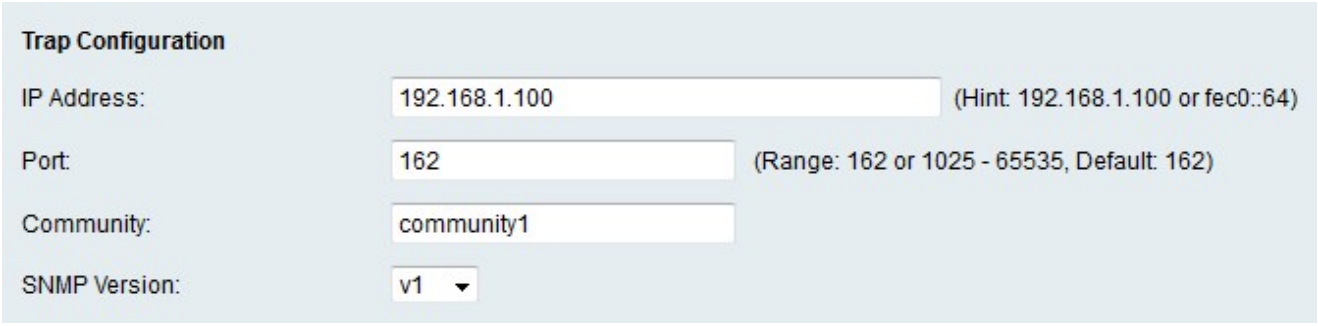
- AES — Advanced Encryption Standard (AES) is een encryptie-algoritme dat verschillende methoden gebruikt om een bericht te versleutelen en te decrypteren. Dit maakt AES een veiliger encryptie algoritme dan DES.

Stap 6. Voer een privacywachtwoord in voor de gebruikers in het veld Privacywachtwoord.

Stap 7. Klik op **Opslaan**.

Vlagconfiguratie

Trappen worden gegenereerd door SNMP-berichten die worden gebruikt om systeemgebeurtenissen te melden. Een val zal een beheerd apparaat dwingen om een SNMP bericht naar de netwerkmanager te verzenden die de netwerkmanager van een systeemgebeurtenis op de hoogte brengt.



Stap 1. Voer het IP-adres in waarop de valmeldingen in het IP-adresveld worden verzonden.

Stap 2. Voer het poortnummer in van het IP-adres waarop de valmeldingen in het veld Port worden verzonden.

Stap 3. Voer de communautaire reeks in waartoe de valmanager in het veld Gemeenschap behoort. Een community-string is een tekststring die werkt als een wachtwoord. Het wordt gebruikt door SNMP om berichten die tussen een agent en een netwerkmanager worden verzonden voor de authenticatie te verklaren.

Opmerking: Dit veld is alleen van toepassing als de SNMP-trap versie 3 niet is.

Stap 4. Kies in de vervolgkeuzelijst SNMP-versie de SNMP-beheerversie voor de SNMP-trap-berichten.

- v1 — Gebruikt een lokale string om valmeldingen echt te maken.

- v2c — Gebruikt een lokale string om valmeldingen echt te maken.

- v3 — Gebruikt gecodeerde wachtwoorden om valmeldingen te authenticeren.

Stap 5. Klik op **Opslaan**.