Configureer de instellingen van Simple Network Management Protocol (SNMP) op SPA100 Series

Doel

Simple Network Management Protocol (SNMP) is een tool dat wordt gebruikt om apparaten op een netwerk te bewaken en te reguleren en configuraties te onderhouden. Met de verzameling, prestaties en beveiliging van statistieken kunt u netwerkproblemen snel oplossen. 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. U moet een SNMP v3 Manager-programma installeren om SNMP-meldingen te bekijken. Op het apparaat kan een gebruiker de instellingen voor de valconfiguratie aanpassen. Trappen zijn foutmeldingen die naar een specifiek IP-adres worden verzonden wanneer er een fout in het netwerk optreedt.

Het doel van dit document is om u te tonen hoe u de instellingen van SNMP op de SPA100 Series Analog Telephone Adapter (ATA) kunt configureren.

Toepasselijke apparaten

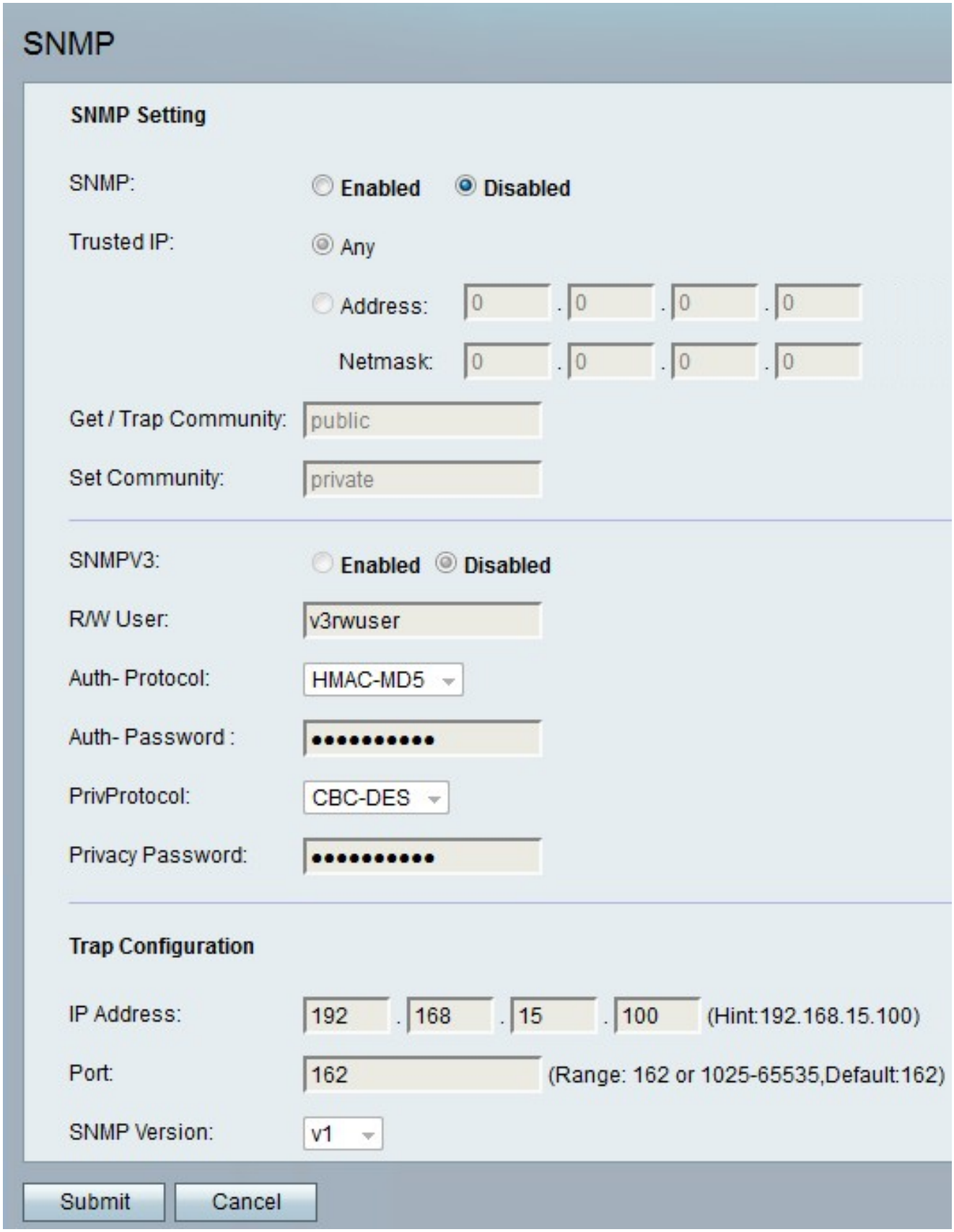
- SPA100 Series analoge telefoonadapter

Softwareversie

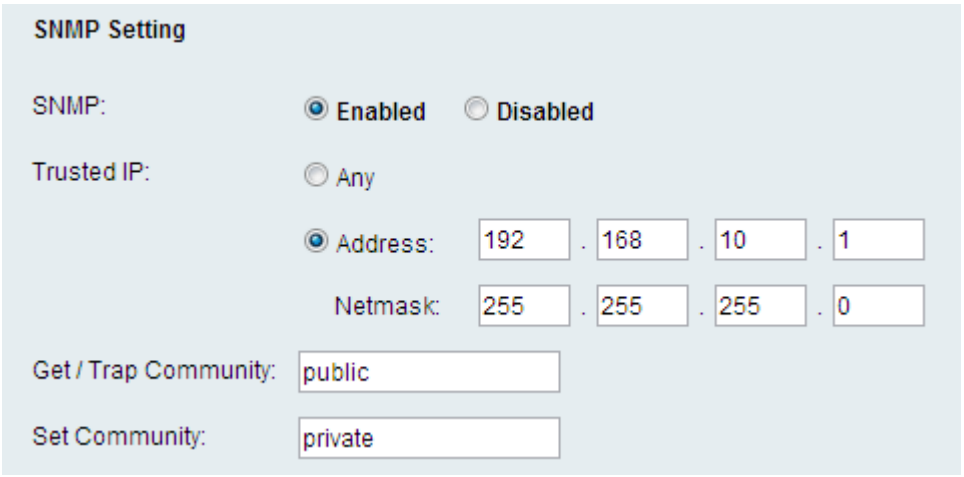
- v1.1.0

SNMP-configuratie

Stap 1. Meld u aan bij het programma voor webconfiguratie en kies **Administratie > Beheer > SNMP**. De *SNMP*-pagina wordt geopend:



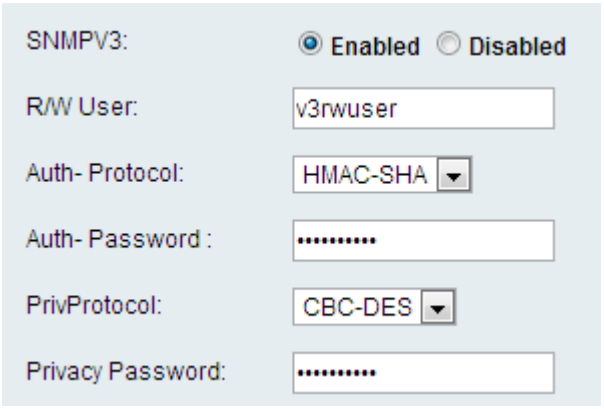
Stap 2. Rechts van het *SNMP*-veld klikt u op de knop **Ingeschakeld** om SNMP in te schakelen, of klikt u op de knop **Uitgeschakeld** om SNMP op het apparaat uit te schakelen.



Stap 3. In het veld *Trusted IP* klikt u op **Any** om toegang tot de ATA via SNMP toe te staan, of op **Adres** om een bereik van IP-adressen toe te staan om de ATA via SNMP te bereiken.

Stap 4. *Voer* in het veld *Get Community* een zin in die fungeert als een wachtwoord voor het ophalen van opdrachten in de SNMP-gemeenschap.

Stap 5. In het veld *Community*-instellingen *instellen*, geeft u een zin in die fungeert als een wachtwoord voor SET-opdrachten in de SNMP-gemeenschap.



Stap 6. SNMPV3 is een veiliger implementatie van SNMP. Het maakt het gebruik van geavanceerdere authenticatie- en encryptiesystemen mogelijk om ervoor te zorgen dat alleen geautoriseerde apparaten via SNMP kunnen lezen en schrijven naar uw netwerkapparaten. Klik op de radioknop **Enabled** om SNMPv3 te gebruiken of klik op de radioknop **Gehandicapten** om het uit te schakelen.

Stap 7. Voer in het veld *R/W-gebruiker* een gebruikersnaam in voor de SNMPv3-verificatie.

Stap 8. Kies in de vervolgkeuzelijst *Auth-Protocol* een verificatieprotocol voor SNMPv3. De beschikbare opties zijn als volgt gedefinieerd:

- 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.

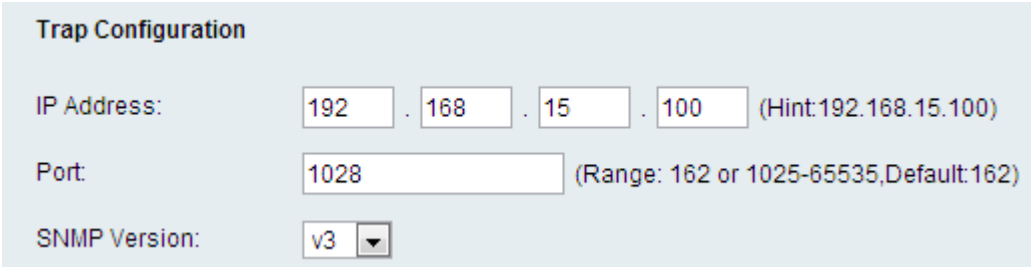
Opmerking: HMAC-SHA wordt veiliger geacht dan HMAC-MD5 en wordt aanbevolen.

Stap 9. Voer in het veld *Wachtwoord* in voor verificatie.

Stap 10. Kies in de vervolgkeuzelijst *PrivProtocol* een protocol voor de verificatie van de privacy. Aanbevolen wordt dat de gebruiker een privacy-functie heeft zodat de gegevens beveiligd zijn. De beschikbare opties zijn als volgt gedefinieerd:

- Geen — Er wordt geen privacy-algoritme gebruikt. De gegevens van een bericht worden niet versleuteld.
- CBC-DES - Met deze optie worden de gegevens van een bericht versleuteld met DES-encryptie.

Stap 1. Voer in het veld *Privacywachtwoord* een wachtwoord in voor het protocol voor de verificatie van de privacy.



Stap 12. Voer in het veld *IP-adres* een IP-adres in dat valberichten ontvangt.

Stap 13. Voer in het veld *Port* het poortnummer in dat valberichten ontvangt. De standaardpoort is 162.

Stap 14. Kies in de vervolgkeuzelijst *SNMP-versie* een versie van SNMP om valberichten te gebruiken. De beschikbare opties zijn:

- v1 — Gebruikt SNMPv1-vallen. SNMPv1-vallen gebruiken een gemeenschapsstring om valberichten te authenticeren en versleutelen geen gegevens.
- v2 — Gebruikt SNMPv2-vallen. SNMPv2-traps gebruikt een string om valberichten te authenticeren en versleutelt geen gegevens.
- v3 — Gebruikt SNMPv3-vallen. SNMPv3-traps kunnen worden ingesteld om een gebruikersnaam en wachtwoord te gebruiken om de bron van een val te controleren en om de gegevens van een val te versleutelen. SNMPv3 moet ingeschakeld en geconfigureerd zijn zoals in Stap 6 beschreven worden om deze optie te kunnen gebruiken.

Stap 15. Klik op **Inzenden** om wijzigingen toe te passen of **Annuleren** om ze te verwerpen.