

# Algemene SNMP-instellingen configureren op WAP361 en WAP150

## Doel

Simple Network Management Protocol (SNMP) is een protocol dat wordt gebruikt voor netwerkbeheer, probleemoplossing en onderhoud. SNMP registreert, slaat en deelt informatie met de hulp van twee-sleutel software: een Network Management System (NMS) dat op beheerapparaten en een agent die op beheerde apparaten draait. WAP361 en WAP150 ondersteunen SNMPv2c en SNMPv3.

SNMPv2c is vergelijkbaar met de oorspronkelijke SNMP door verbeterde ondersteuning voor beveiliging en foutenbehandeling. Deze verbetering omvat uitgebreide foutcodes die verschillende soorten fouten onderscheiden; alle soorten fouten worden door één foutcode in SNMPv1 gerapporteerd.

SNMPv3 verbeterde de tweede vrijgegeven versie door nieuwe beveiligingsfuncties te bieden zoals verificatie, privacy, autorisatie en toegangscontrole.

Dit artikel legt uit hoe u de algemene SNMP-instellingen op WAP361 en WAP150 kunt configureren.

## Toepasselijke apparaten

- WAP300 Series — WAP361
- WAP100 Series — WAP150

## Softwareversie

- 1.0.0.16

## SNMP-algemene instellingen

Stap 1. Meld u aan bij het op internet gebaseerde hulpprogramma en kies **SNMP > General**.



Stap 2. In het gebied Global Settings controleert u het selectieteken **Enable** om SNMP in te schakelen.

The screenshot shows the 'General' settings page. Under 'Global Settings', the 'SNMP' checkbox is checked and circled in red. Below it, the 'UDP Port' is set to '161' in a text box, which is also circled in red. A note next to the text box indicates '(Range:1025-65535, Default: 161)'.

Stap 3. Voer het UDP-poortnummer in in het veld *UDP-poort*. De SNMP agent controleert deze poort voor toegangsverzoeken. De standaardpoort is 161.

This screenshot is identical to the previous one, but the 'UDP Port' text box containing '161' is highlighted with a red rectangle.

**Timesaver:** Als u geen SNMPv2-configuratie nodig hebt, sla deze stap over en stap over naar [Stap 11](#).

Stap 4. Voer een alleen-lezen gemeenschapsnaam in het veld *alleen-lezen* in met alfanumerieke tekens tussen 1 en 256. De gemeenschapsnaam is een door de gebruiker gedefinieerde naam die fungeert als een eenvoudig authenticatiemechanisme of wachtwoord om de apparaten in het netwerk te beperken die gegevens van de SNMP-agent kunnen vragen. De community string die door de zender in het request pakje wordt verstuurd moet de community string op het agent device aanpassen. De standaard string voor alleen-lezen is `cisco_public`.

Opmerking: Het alleen-lezen wachtwoord geeft alleen autoriteit om informatie op te halen.

The screenshot shows the 'SNMPv2c Settings' page. The 'Read-only Community' field contains 'public' and is circled in red. The 'Read-write Community' field contains 'private'.

Stap 5. Voer een gelezen-schrijfnaam in het veld van de *Lezen-schrijfgemeenschap* met alfanumerieke tekens uit 1 tot 256 voor toegestane SNMP-bewerkingen. Alleen verzoeken van de hulpmiddelen die zich met deze gemeenschapsnaam identificeren worden aanvaard. De standaardinstelling is `cisco_private`. Dit is een wachtwoord waarmee zowel informatie uit de agent kan worden opgehaald als instellingen op het betreffende Agent-apparaat kunnen worden gewijzigd.

Opmerking: Het wordt aanbevolen om beide wachtwoorden in een door de gebruiker ingesteld wachtwoord te wijzigen om beveiligingsbedreigingen te voorkomen.

This screenshot is identical to the previous one, but the 'Read-write Community' text box containing 'private' is highlighted with a red rectangle.

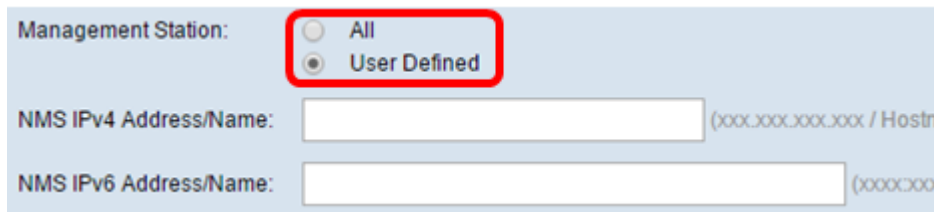
Stap 6. Kies tussen Alle instellingen of gebruikers die in het radioknop van het beheerstation gedefinieerd zijn, om een voorkeur voor een beheerstation te kiezen. Het beheerstation

controleert en werkt de waarden in de Management Information Base (MIB) bij.

Opmerking: De optie die als voorbeeld in de onderstaande afbeelding is geselecteerd, is door de gebruiker gedefinieerd.

Alle — Hiermee kunnen alle stations in het netwerk toegang krijgen tot het draadloze access point (WAP) via SNMP als beheerstation. Als u dit kiest, gaat u naar [Stap 8](#).

Gebruikershandleiding: beperkt de toegang tot een bepaald station of groep stations.



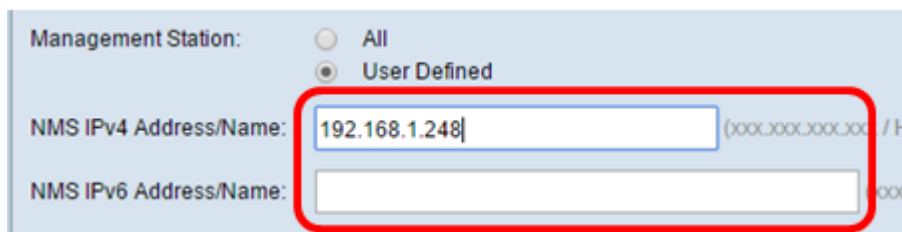
Management Station:  All  User Defined

NMS IPv4 Address/Name:  (xxx.xxx.xxx.xxx / Hostn

NMS IPv6 Address/Name:  (xxxx:xxx

Stap 7. Voer de IPv4- of IPv6-adressen, DNS-hostname of subtype van de NMS in die de verzoeken aan de beheerde apparaten kunnen uitvoeren, krijgen en instellen in respectievelijk de *NMSIPv4-adres/naam* en *NMS IPv6-adres/naam*. Een NMS verwijst naar de beheerstations die toepassingen uitvoeren die beheerde apparaten bewaken en besturen.

Opmerking: Het NMS IPv4-adres 192.168.1.241 wordt in de onderstaande afbeelding als voorbeeld gebruikt.



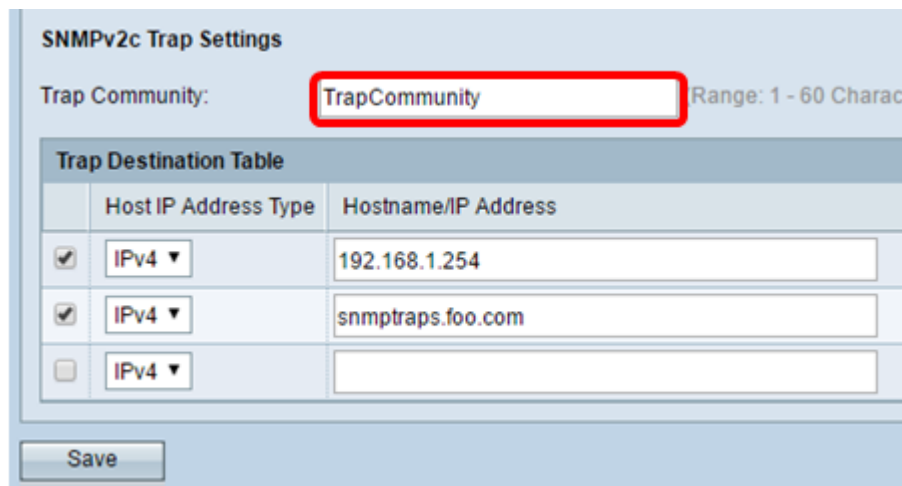
Management Station:  All  User Defined

NMS IPv4 Address/Name:  (xxx.xxx.xxx.xxx / H

NMS IPv6 Address/Name:  xxx

Stap 8. Voer de wereldwijde naam in van de gemeenschap die bij SNMP-trap is gekoppeld in het veld *Trap Community-trap*. Het geldige bereik is van 1 tot 60 alfanumerieke en speciale tekens. In onderstaande afbeelding wordt TrapCommunity als voorbeeld gebruikt.

Opmerking: Splitsen zijn mededelingen van een agent aan manager die agenteninformatie bevat. Vrap van het apparaat gebruiken de string die als gemeenschapsnaam is ingevoerd.



SNMPv2c Trap Settings

Trap Community:  Range: 1 - 60 Charact

Trap Destination Table	
Host IP Address Type	Hostname/IP Address
<input checked="" type="checkbox"/> IPv4	192.168.1.254
<input checked="" type="checkbox"/> IPv4	snmptraps.foo.com
<input type="checkbox"/> IPv4	

Save

Stap 9. In het gebied van de Tabel van de Bestemming van de Vaak, controleer het vakje en kies tussen IPv4 en IPv6 in de vervolgkeuzelijst Type host IP-adres.

Opmerking: In het onderstaande voorbeeld werden de eerste twee vakjes gecontroleerd met zowel IPv4 als het IP-hostadrestype ingesteld.

SNMPv2c Trap Settings

Trap Community:  (Range: 1 - 60 Charac

Trap Destination Table	
Host IP Address Type	Hostname/IP Address
<input checked="" type="checkbox"/> IPv4 ▾	192.168.1.254
<input checked="" type="checkbox"/> IPv4 ▾	snmptraps.foo.com
<input type="checkbox"/> IPv4 ▾	

Stap 10. In het veld *Hostname/IP-adres* voert u de hostnamen of IP-adressen in van maximaal drie hosts om SNMP-traps te ontvangen.

Opmerking: In de onderstaande afbeelding werden een IP-adres en een hostname ingevoerd als voorbeelden.

SNMPv2c Trap Settings

Trap Community:  (Range: 1 - 60 Charac

Trap Destination Table	
Host IP Address Type	Hostname/IP Address
<input checked="" type="checkbox"/> IPv4 ▾	192.168.1.254
<input checked="" type="checkbox"/> IPv4 ▾	snmptraps.foo.com
<input type="checkbox"/> IPv4 ▾	

Stap 1. Klik op **Opslaan**.

SNMPv2c Trap Settings

Trap Community:  (Range: 1 - 60 Charac

Trap Destination Table	
Host IP Address Type	Hostname/IP Address
<input checked="" type="checkbox"/> IPv4 ▾	192.168.1.254
<input checked="" type="checkbox"/> IPv4 ▾	snmptraps.foo.com
<input type="checkbox"/> IPv4 ▾	

U hebt met succes de SNMP General Settings in uw WAP ingesteld.

Klik op de volgende koppelingen voor meer informatie over het General Settings Simple Network Management Protocol:

- [Simple Network Management Protocol \(SNMP\) - algemene instellingen voor WAP121 en WAP321 access points](#)
- [Simple Network Management Protocol \(SNMP\) - algemene instellingen voor WAP551 en WAP561 access points](#)