

Konfigurieren der SNMPv2c-Einstellungen auf dem WAP125 und WAP581

Ziel

Simple Network Management Protocol (SNMP) wird für die Netzwerkverwaltung, Fehlerbehebung und Wartung verwendet. SNMP-Datensätze, -Speicher und -Informationsaustausch mithilfe von zwei Schlüsselsoftware: ein Netzwerkmanagementsystem (NMS), das auf Manager-Geräten ausgeführt wird, und ein Agent, der auf verwalteten Geräten ausgeführt wird.

SNMP v1 ist die ursprüngliche Version von SNMP, die nicht über bestimmte Funktionen verfügt und nur in TCP/IP-Netzwerken funktioniert, während SNMP v2 eine verbesserte Version von v1 ist. SNMP v1 und v2c sollten nur für Netzwerke ausgewählt werden, die entweder SNMPv1 oder SNMPv2c verwenden. SNMP v3 ist der neueste Standard für SNMP und behandelt viele Probleme mit SNMP v1 und v2c. Insbesondere werden viele der Sicherheitsschwachstellen von v1 und v2c behoben. SNMP v3 ermöglicht es Administratoren außerdem, auf einen gemeinsamen SNMP-Standard zu wechseln.

Traps sind Meldungen, die den SNMP-Manager auf einen Zustand im Netzwerk hinweisen. Informationsanfragen (Informationen) sind Traps, die eine Anfrage zur Bestätigung des Empfangs durch den SNMP-Manager enthalten. Benachrichtigungen können auf eine unsachgemäße Benutzerauthentifizierung, Neustarts, das Schließen einer Verbindung, den Verlust der Verbindung zu einem Nachbarrouter, einen Wireless Access Point oder andere wichtige Ereignisse hinweisen.

In diesem Artikel wird erläutert, wie SNMPv2c-Einstellungen auf dem WAP125 konfiguriert werden.

Hinweis: Um zu erfahren, wie die SNMPv3-Einstellungen konfiguriert werden, klicken Sie [hier](#).

Anwendbare Geräte

- WAP125
- WAP581

Softwareversion

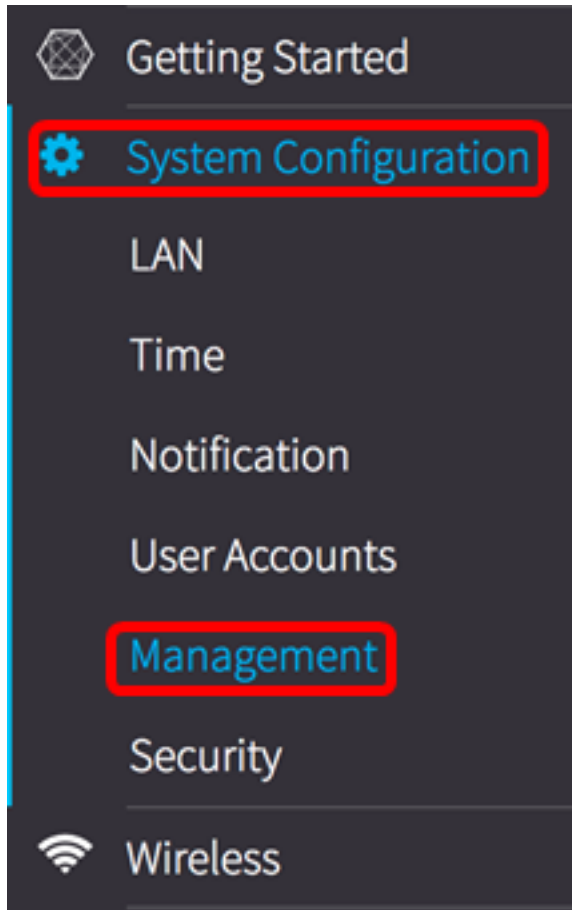
- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

Konfigurieren der SNMPv2c-Einstellungen

SNMP-Einstellungen konfigurieren

Hinweis: Die Menüoptionen können je nach dem verwendeten WAP-Modell variieren. Die folgenden Bilder stammen aus dem WAP125.

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Wireless Access Point an, und wählen Sie **Systemkonfiguration > Verwaltung** aus.



Schritt 2: Aktivieren Sie unter SNMP Settings (SNMP-Einstellungen) das Kontrollkästchen **Enable (Aktivieren)**.



SNMP Settings

SNMP: Enable

UDP Port:

SNMPv2c Settings

Read-only Community:

Read-write Community:

SNMP Settings ▾

Schritt 3: Geben Sie eine UDP-Portnummer (User Datagram Protocol) im Feld *UDP Port ein* . Der SNMP-Agent überprüft diesen Port auf Zugriffsanfragen. Der Standardwert ist 161. Der gültige Bereich liegt zwischen 1025 und 65535.

Hinweis: In diesem Beispiel wird 161 verwendet.

SNMP Settings

SNMP: Enable

UDP Port:

SNMPv2c Settings

Read-only Community:

Read-write Community:

SNMP Settings ▾

Schritt 4: Geben Sie den SNMP-Community-Namen in das Feld *schreibgeschützte Community* ein. Es wird eine schreibgeschützte Community erstellt, die für den Zugriff auf die Informationen für den SNMP-Agenten verwendet wird. Der Community-String, der im Anforderungspaket gesendet wird, muss mit dem Community-String auf dem Agent-Gerät übereinstimmen. Die Standardzeichenfolge für schreibgeschützt ist public.

Hinweis: In diesem Beispiel wird der Standardwert verwendet. Der schreibgeschützte Community-Name dient als Kennwort, wodurch nur der Abruf von Informationen möglich ist.

SNMP Settings

SNMP: Enable

UDP Port:

SNMPv2c Settings

Read-only Community:

Read-write Community:

SNMP Settings ▾

Schritt 5: Geben Sie im Feld *Read-Write Community (Read-Write-Community)* einen SNMP-Community-Namen ein. Es wird eine Lese- und Schreibgemeinschaft erstellt, die für den Zugriff auf die Informationen für den SNMP-Agenten verwendet wird. Nur Anfragen von Geräten, die sich mit diesem Community-Namen identifizieren, werden akzeptiert. Dies ist ein vom Benutzer erstellter Name. Der Standardwert ist "Privat".

Hinweis: In diesem Beispiel wird private verwendet. Der Community-Name für Lese- und Schreibberechtigungen dient als Kennwort, das das Abrufen und Ändern von Informationen ermöglicht. Es ist ratsam, den Community-Namen in etwas individueller zu ändern, um Sicherheitsangriffe von Außenstehenden zu vermeiden.

SNMP Settings

SNMP: Enable

UDP Port:

SNMPv2c Settings

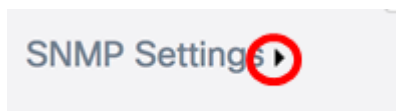
Read-only Community:

Read-write Community:

SNMP Settings ▾

Konfigurieren der SNMPv2c-Einstellungen

Schritt 6: Klicken Sie auf die rechte Schaltfläche SNMP Settings.



Schritt 7: Klicken Sie auf die Registerkarte **SNMPv2c**, um die SNMPv2c-Einstellungen weiter zu konfigurieren.

SNMPv2c | SNMPv3

SNMPv2c Settings

Management Station: All User Defined

NMS IPv4 Address/Name:

NMS IPv6 Address/Name:

Schritt 8: Wählen Sie im Bereich Management Station (Managementstation) eine Methode aus, mit der Stationen über SNMP auf den WAP zugreifen können. Folgende Optionen stehen zur Verfügung:

- Alle - Alle Stationen haben über SNMP Zugriff auf den WAP. Wenn Sie diese Option auswählen, fahren Sie mit [Schritt 11 fort](#).
- User Defined (Benutzerdefiniert) - Ein Satz definierter SNMP-Anforderungen, die Zugriff erhalten. Wenn diese Option ausgewählt ist, fahren Sie mit dem nächsten Schritt fort.

Hinweis: In diesem Beispiel wird User Defined verwendet.

The image shows a configuration interface for SNMPv2c. At the top, there are two tabs: 'SNMPv2c' (active) and 'SNMPv3'. Below the tabs, the title 'SNMPv2c Settings' is displayed. Underneath, there are three settings: 'Management Station' with radio buttons for 'All' and 'User Defined' (selected), 'NMS IPv4 Address/Name' with an empty text input field, and 'NMS IPv6 Address/Name' with an empty text input field. Each input field has a small question mark icon to its left.

Schritt 9: Geben Sie im Feld *NMS IPv4-Adresse/Name* eine NMS-Adresse (Network Management System) oder eine DNS-Serveradresse (Domain Name System) im IPv4-Format ein (xxx.xxx.xxxx.xxx). Dies ist die Adresse, an die Anforderungen an die verwalteten Geräte ausgeführt, abgerufen und festgelegt werden.

Ein DNS ist eine verteilte Datenbank, in der Sie Hostnamen über das DNS-Protokoll eines DNS-Servers IP-Adressen zuordnen können. Jede eindeutige IP-Adresse kann einen zugewiesenen Hostnamen haben. Ein DNS-Hostname kann aus mehreren Bezeichnungen bestehen, und jede Bezeichnung wird durch einen Punkt getrennt.

Ein NMS ist ein Tool oder Programm, das bzw. das von einem Administrator zum Empfangen von SNMP-Meldungen verwendet wird.

Hinweis: In diesem Beispiel wird ein NMS 192.168.2.126 verwendet.

This image shows the same 'SNMPv2c Settings' form as above, but now the 'NMS IPv4 Address/Name' field contains the IP address '192.168.2.126'. The 'Management Station' remains 'User Defined'. The 'NMS IPv6 Address/Name' field is still empty. The IP address '192.168.2.126' is highlighted with a red rectangular box.

Schritt 10: Geben Sie im Feld *NMS IPv6 Address/Name (NMS-IPv6-Adresse/Name)* eine NMS-Adresse oder eine DNS-Serveradresse im IPv6-Format ein (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx). Dies ist die Adresse, an die Anforderungen an die verwalteten Geräte ausgeführt, abgerufen und festgelegt werden.

Hinweis: In diesem Beispiel wird fdce:223e:c00d:d00d:afaf:0000:0000:0000 verwendet.

This image shows the 'SNMPv2c Settings' form with both fields filled. The 'NMS IPv4 Address/Name' field contains '192.168.2.126' and the 'NMS IPv6 Address/Name' field contains 'fdce:223e:c00d:d00d:afaf:0000:0000:0000'. Both fields are highlighted with red rectangular boxes. The 'Management Station' remains 'User Defined'.

Schritt 11: Geben Sie im Feld *Trap Community* unter SNMPv2c Trap Settings den Community-Namen für das Trap ein.

Hinweis: In diesem Beispiel wird snmptraps.foo.com als Trap-Community-Name verwendet.

SNMPv2c Settings

Management Station: All User Defined

NMS IPv4 Address/Name:

NMS IPv6 Address/Name:

SNMPv2c Trap Settings

Trap Community:

Schritt 12: Aktivieren Sie das Kontrollkästchen eines Hostnameneintrags in der Trap-Zieltabelle, um die Bearbeitung zu aktivieren.

Hinweis: Sie können bis zu drei Hostnamen/IP-Adressen konfigurieren.

Trap Destination Table

	Host IP Address Type	Hostname/IP Address
<input checked="" type="checkbox"/>	IPv4	<input type="text"/>
<input type="checkbox"/>	IPv4	<input type="text"/>
<input type="checkbox"/>	IPv4	<input type="text"/>

Schritt 13: Wählen Sie in der Dropdown-Liste Host IP Address Type (Hostadresse-Typ) eine IP-Version aus. Folgende Optionen stehen zur Verfügung:

- IPv4 - vierte Generation oder Version des IP-Adressierungsschemas (Internet Protocol) im Format xxx.xxx.xxx.xxx.
- IPv6 - sechste Generation oder Version des IP-Adressierungsschemas im Format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.




Trap Destination Table

	Host IP Address Type	Hostname/IP Address
<input checked="" type="checkbox"/>	IPv4 IPv6	<input type="text"/>
<input type="checkbox"/>	IPv4	<input type="text"/>
<input type="checkbox"/>	IPv4	<input type="text"/>

Schritt 14: Geben Sie im Feld *Hostname/IP-Adresse* eine IPv4- oder eine IPv6-IP-Adresse ein, die die SNMP-Traps empfangen soll.

Hinweis: In diesem Beispiel wird 192.168.2.202 verwendet.

Trap Destination Table

	Host IP Address Type	Hostname/IP Address
<input checked="" type="checkbox"/>	IPv4 	192.168.2.202
<input type="checkbox"/>	IPv4 	
<input type="checkbox"/>	IPv4 	

Schritt 15: Klicken Sie [Save](#).

Sie sollten jetzt die SNMPv2c-Einstellungen auf dem WAP125 und dem WAP581 erfolgreich konfiguriert haben.