

Konfigurieren allgemeiner SNMP-Einstellungen auf dem WAP361 und WAP150

Ziel

Simple Network Management Protocol (SNMP) ist ein Protokoll, das für die Netzwerkverwaltung, Fehlerbehebung und Wartung verwendet wird. SNMP-Datensätze, -Speicher und -Informationsaustausch mithilfe einer Zwei-Schlüssel-Software: ein Network Management System (NMS), das auf Manager-Geräten ausgeführt wird, und ein Agent, der auf verwalteten Geräten ausgeführt wird. WAP361 und WAP150 unterstützen SNMPv2c und SNMPv3.

SNMPv2c ähnelt dem ursprünglichen SNMP durch verbesserte Sicherheits- und Fehlerbehandlungsunterstützung. Diese Verbesserung umfasst erweiterte Fehlercodes, die unterschiedliche Fehlertypen unterscheiden. Alle Fehlertypen werden in SNMPv1 über einen einzigen Fehlercode gemeldet.

SNMPv3 verbesserte die zweite Version durch neue Sicherheitsfunktionen wie Authentifizierung, Datenschutz, Autorisierung und Zugriffskontrolle.

In diesem Artikel wird erläutert, wie die allgemeinen SNMP-Einstellungen auf dem WAP361 und WAP150 konfiguriert werden.

Anwendbare Geräte

- WAP300-Serie - WAP361
- WAP100-Serie - WAP150

Softwareversion

- 1,0 0,16

Allgemeine SNMP-Einstellungen

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Access Points an, und wählen Sie **SNMP > General** aus.



Schritt 2: Aktivieren Sie im Bereich "Globale Einstellungen" das Kontrollkästchen **Aktivieren**, um SNMP zu aktivieren.

General

Global Settings

SNMP: Enable

UDP Port: (Range:1025-65535, Default: 161)

Schritt 3: Geben Sie die UDP-Portnummer im Feld *UDP-Port* ein. Der SNMP-Agent überprüft diesen Port auf Zugriffsanfragen. Der Standard-Port ist 161.

General

Global Settings

SNMP: Enable

UDP Port: (Range:1025-65535, Default: 161)

Timesaver: Wenn Sie keine SNMPv2-Konfiguration benötigen, überspringen Sie diesen Schritt und fahren Sie mit [Schritt 11](#) fort.

Schritt 4: Geben Sie im Feld *schreibgeschützte Community* einen schreibgeschützten Community-Namen mit alphanumerischen Zeichen zwischen 1 und 256 ein. Der Communityname ist ein benutzerdefinierter Name, der als einfacher Authentifizierungsmechanismus oder Kennwort fungiert, um die Geräte im Netzwerk einzuschränken, die Daten vom SNMP-Agent anfordern können. Der vom Absender im Anforderungspaket gesendete Community-String muss mit dem Community-String auf dem Agent-Gerät übereinstimmen. Die Standardzeichenfolge für schreibgeschützt ist `cisco_public`.

Hinweis: Das schreibgeschützte Kennwort gibt die Berechtigung, nur Informationen abzurufen.

SNMPv2c Settings

Read-only Community:

Read-write Community:

Schritt 5: Geben Sie im Feld *Read-Write Community* (Lese- und SchreibCommunity) einen Community-Namen mit alphanumerischen Zeichen zwischen 1 und 256 für zulässige SNMP-Set-Operationen ein. Nur Anfragen von Geräten, die sich mit diesem Community-Namen identifizieren, werden akzeptiert. Der Standardwert ist "`cisco_private`". Mit diesem Kennwort können Sie sowohl Informationen vom Agenten abrufen als auch die Einstellungen für dieses Agent-Gerät ändern.

Hinweis: Es wird empfohlen, beide Kennwörter in ein benutzerdefiniertes Kennwort zu ändern, um Sicherheitsbedrohungen zu vermeiden.

SNMPv2c Settings

Read-only Community:

Read-write Community:

Schritt 6: Wählen Sie im Optionsfeld der Verwaltungs-Workstation entweder All (Alle) oder User Defined (Benutzerdefiniert) aus, um eine bevorzugte Verwaltungs-Workstation auszuwählen. Die Managementstation überwacht und aktualisiert die Werte in der Management Information Base (MIB).

Hinweis: Die in der Abbildung unten als Beispiel ausgewählte Option ist User Defined (Benutzerdefiniert).

All (Alle) - Ermöglicht allen Stationen im Netzwerk, über SNMP als Managementstation auf den Wireless Access Point (WAP) zuzugreifen. Wenn Sie diese Option auswählen, fahren Sie mit [Schritt 8](#) fort.

User Defined (Benutzerdefiniert) - Schränkt den Zugriff auf eine bestimmte Station oder Gruppe von Stationen ein.



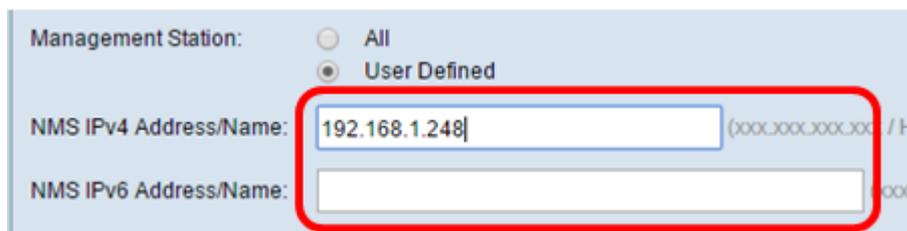
Management Station: All User Defined

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

NMS IPv6 Address/Name: (xxxx:xxx

Schritt 7: Geben Sie die IPv4- oder IPv6-Adressen, den DNS-Hostnamen oder das Subnetz des NMS ein, das die Anforderungen in den Feldern *NMSIPv4 Address/Name* und *NMS IPv6 Address/Name* ausführen, abrufen und auf die verwalteten Geräte festlegen kann. Ein NMS bezieht sich auf die Verwaltungsstationen, die Anwendungen ausführen, die verwaltete Geräte überwachen und steuern.

Hinweis: Die NMS IPv4-Adresse 192.168.1.248 wird im folgenden Bild als Beispiel verwendet.



Management Station: All User Defined

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

NMS IPv6 Address/Name: xxx

Schritt 8: Geben Sie im Feld *Trap Community* den globalen Community-Namen ein, der SNMP-Traps zugeordnet ist. Der gültige Bereich liegt zwischen 1 und 60 alphanumerischen und Sonderzeichen. In der Abbildung unten wird TrapCommunity als Beispiel verwendet.

Hinweis: Traps sind Benachrichtigungen von Agenten an Manager, die Agenteninformationen enthalten. Traps, die vom Gerät gesendet werden, verwenden die Zeichenfolge, die als Community-Name eingegeben wurde.

SNMPv2c Trap Settings

Trap Community: (Range: 1 - 60 Charact)

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

Schritt 9: Aktivieren Sie im Bereich Trap Destination Table (Trap-Zieltabelle) das Kontrollkästchen, und wählen Sie in der Dropdown-Liste Host IP Address Type (Host-IP-Adresstyp) zwischen IPv4 und IPv6 aus.

Hinweis: Im folgenden Beispiel wurden die ersten beiden Kontrollkästchen aktiviert, wobei beide IPv4 als Host-IP-Adresstyp festgelegt wurden.

SNMPv2c Trap Settings

Trap Community: (Range: 1 - 60 Charact)

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

Schritt 10: Geben Sie im Feld *Hostname/IP-Adresse* die Hostnamen oder IP-Adressen von bis zu drei Hosts ein, die SNMP-Traps empfangen sollen.

Hinweis: Im Bild unten wurden eine IP-Adresse und ein Hostname als Beispiele eingegeben.

SNMPv2c Trap Settings

Trap Community: (Range: 1 - 60 Charact)

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

Schritt 11: Klicken Sie auf **Speichern**.

SNMPv2c Trap Settings

Trap Community: (Range: 1 - 60 Characters)

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

Sie haben die allgemeinen SNMP-Einstellungen auf Ihrem WAP erfolgreich konfiguriert.

Weitere Informationen zu General Settings Simple Network Management Protocol finden Sie unter den folgenden Links:

- [Simple Network Management Protocol \(SNMP\) - Allgemeine Einstellungen für die WAP121- und WAP321-Access Points](#)
- [Simple Network Management Protocol \(SNMP\) - Konfiguration der allgemeinen Einstellungen auf den Access Points WAP551 und WAP561](#)