Konfigurieren von SNMP auf den Routern RV160 und RV260

Ziel

In diesem Artikel erfahren Sie, wie Sie die SNMP-Einstellungen (Simple Network Management Protocol) für die Router RV160 und RV260 konfigurieren.

Einführung

SNMP ist ein Internetstandardprotokoll zum Erfassen und Organisieren von Daten auf verwalteten Geräten in IP-Netzwerken. Sie ermöglicht Netzwerkadministratoren die Verwaltung, Überwachung und den Empfang von Benachrichtigungen über kritische Ereignisse im Netzwerk sowie die Fehlerbehebung.

Das SNMP-Framework besteht aus drei Elementen: einen SNMP-Manager, einen SNMP-Agent und eine Management Information Base (MIB). Der SNMP-Manager steuert und überwacht die Aktivitäten der Netzwerk-Hosts, die SNMP verwenden. Der SNMP-Agent ist in der Software des Geräts enthalten und unterstützt die Datenpflege zur Verwaltung des Systems. MIB ist ein virtueller Speicherbereich für Netzwerkmanagementinformationen. Diese drei Komponenten überwachen und verwalten die Geräte in einem Netzwerk.

RV160/260-Geräte unterstützen die SNMP-Versionen v1, v2c und v3. Sie fungieren als SNMP-Agenten, die auf SNMP-Befehle von SNMP-Netzwerkmanagementsystemen antworten. Die unterstützten Befehle sind die standardmäßigen SNMP-Befehle get/next/set. Die Geräte generieren auch Trap-Meldungen, um den SNMP-Manager zu benachrichtigen, wenn Alarmbedingungen auftreten. Beispiele sind Neustarts, Ein- und Ausschalten und WAN-Verknüpfungsereignisse.

Anwendbare Geräte

- RV160
- RV260

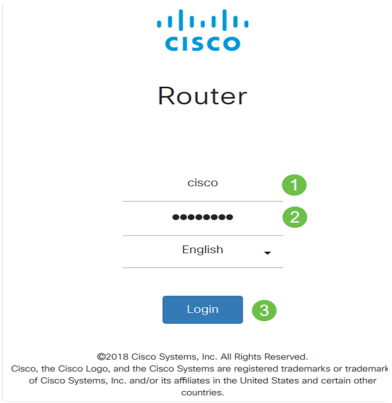
Softwareversion

- 1,0 00,13

SNMP konfigurieren

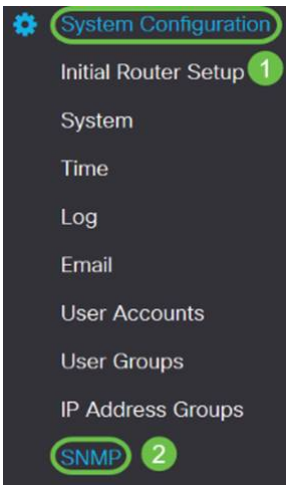
So konfigurieren Sie das SNMP des Routers:

Schritt 1: Melden Sie sich auf der Webkonfigurationsseite Ihres Routers an.



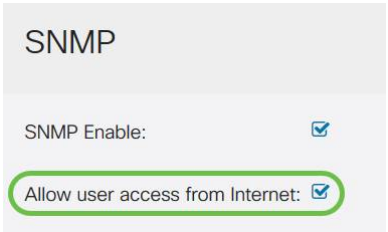
Hinweis: In diesem Artikel wird der RV260W zum Konfigurieren von SNMP verwendet. Die Konfiguration kann je nach verwendetem Modell variieren.

Schritt 2: Navigieren Sie zu **Systemkonfiguration > SNMP**.



Schritt 3: Aktivieren Sie das Kontrollkästchen **SNMP aktivieren**, um SNMP zu aktivieren.

Schritt 4: (Optional) Aktivieren Sie das Kontrollkästchen **Benutzerzugriff aus dem Internet zulassen**, um autorisierten Benutzerzugriff außerhalb des Netzwerks über Verwaltungsanwendungen wie Cisco FindIT Network Management zuzulassen.

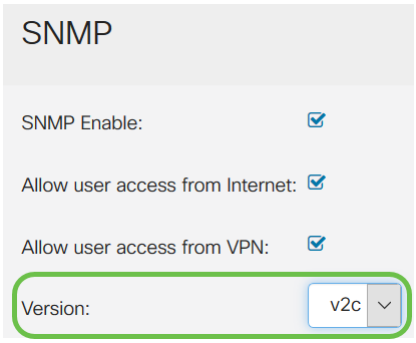


Schritt 5: (Optional) Aktivieren Sie das Kontrollkästchen **Benutzerzugriff von VPN zulassen**, um autorisierten Zugriff von einem Virtual Private Network (VPN) aus zuzulassen.

Schritt 6: Wählen Sie im Dropdown-Menü *Version* eine SNMP-Version aus, die im Netzwerk verwendet werden soll. Folgende Optionen stehen zur Verfügung:

- v1 - Option mit der geringsten Sicherheit. Verwendet Klartext für Community-Strings.
- v2c - Die verbesserte Fehlerbehandlungsunterstützung von SNMPv2c beinhaltet erweiterte Fehlercodes, die verschiedene Fehlertypen unterscheiden. Alle Fehlertypen werden in SNMPv1 über einen einzigen Fehlercode gemeldet.
- v3 - SNMPv3 bietet sicheren Zugriff auf Geräte, indem Datenpakete über das Netzwerk authentifiziert und verschlüsselt werden. Zu den Authentifizierungsalgorithmen gehören der Message Digest Algorithm (MD5) und der Secure Hash Algorithm (SHA). Zu den Verschlüsselungsmethoden zählen Data Encryption Standard (DES) und Advanced Encryption Standard (AES).

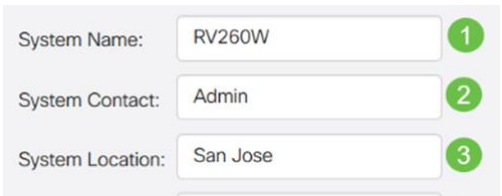
Weitere Informationen zu SNMPv3 erhalten Sie hier.



In diesem Beispiel wurde **v2c** als *Version* ausgewählt.

Schritt 7: Geben Sie die folgenden Felder ein

- **Systemname**: Geben Sie einen Namen für den Router ein, um die Identifizierung in Netzwerkverwaltungsanwendungen zu vereinfachen.
- **Systemkontakt** - Geben Sie einen Namen einer Person oder eines Administrators ein, der im Notfall mit dem Router identifiziert werden kann.
- **Systemstandort** - Geben Sie einen Speicherort des Routers ein. Dadurch wird das Auffinden eines Problems für einen Administrator viel einfacher.
- **Get Community** - Geben Sie im Feld *Get Community* den SNMP-Community-Namen ein. Es wird eine schreibgeschützte Community erstellt, die für den Zugriff auf und das Abrufen der Informationen für den SNMP-Agenten verwendet wird.
- **Community festlegen**: Geben Sie im Feld *Community festlegen* einen SNMP-Community-Namen ein. Es wird eine Lese- und Schreibcommunity erstellt, die für den Zugriff und die Änderung der 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".

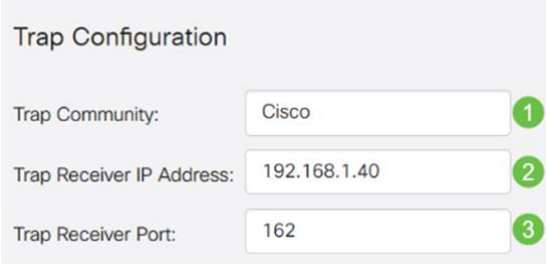


Trap-Konfiguration

Mit Trap-Konfigurationen können Sie die Quelladresse jedes vom Router gesendeten SNMP-Trap-Pakets auf eine einzige Adresse festlegen, unabhängig von der ausgehenden Schnittstelle.

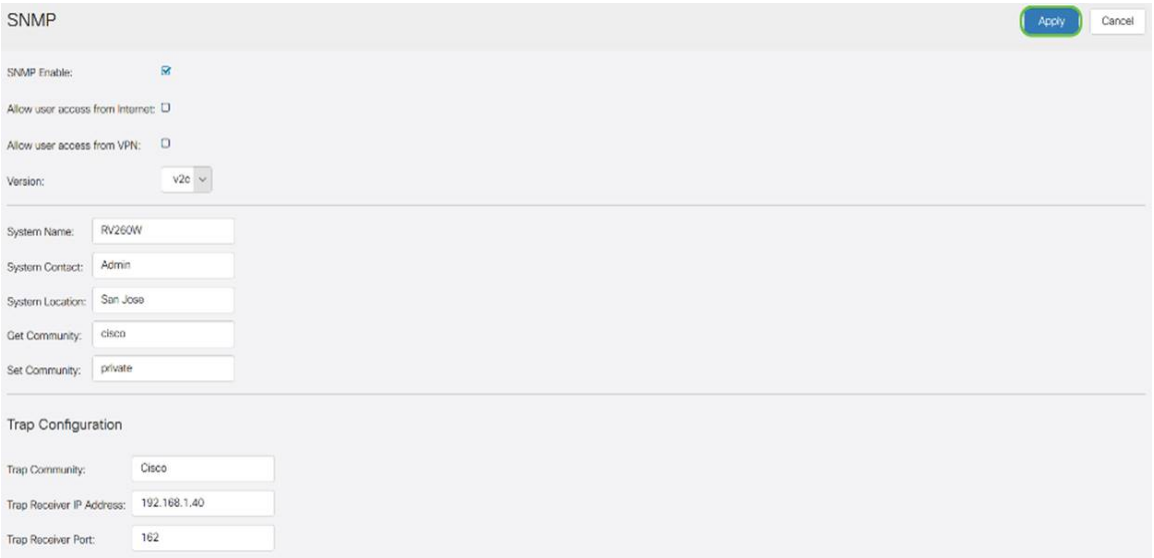
Schritt 8: Um das SNMP-Trap zu konfigurieren, geben Sie die folgenden Informationen ein.

Trap-Community	Geben Sie den Namen der Trap-Community ein.
IP-Adresse des Trap Receivers	Geben Sie die IP-Adresse ein
Trap Receiver-Port	Geben Sie die Portnummer ein



Hinweis: In der Regel verwendet SNMP User Datagram Protocol (UDP) als Transportprotokoll, und die UDP-Standardports für SNMP-Verkehr sind 161 (SNMP) und 162 (SNMP-Trap).

Schritt 9: Klicken Sie auf **Übernehmen**.



Sie sollten jetzt SNMP auf Ihrem RV160/RV260-Router erfolgreich aktiviert und konfiguriert haben.