

Konfigurieren der SNMP-Einstellungen (Simple Network Management Protocol) auf einem Router der Serie RV34x

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. Der Router der Serie RV34x unterstützt die SNMP-Versionen 1, 2 und 3.

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.

In diesem Artikel wird erläutert, wie SNMP-Einstellungen auf dem Router der Serie RV34x konfiguriert werden.

Anwendbare Geräte

- Serie RV34x

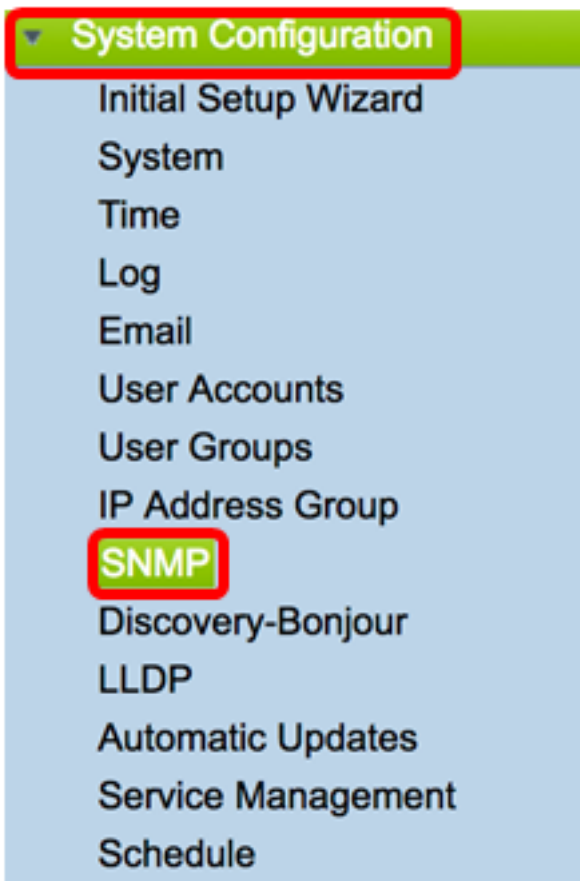
Softwareversion

- 1,0/1,16

Konfigurieren der SNMP-Einstellungen auf dem Router der Serie RV34x

SNMP-Einstellungen konfigurieren

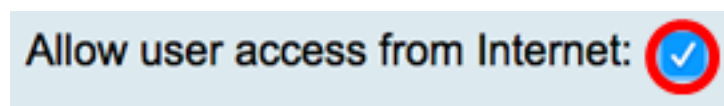
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Routers an, und wählen Sie **Systemkonfiguration > SNMP** aus.



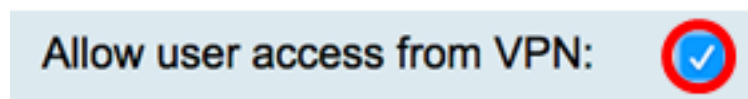
Schritt 2: Aktivieren Sie das Kontrollkästchen **SNMP aktivieren**, um SNMP zu aktivieren.



Schritt 3: (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 4: (Optional) Aktivieren Sie das Kontrollkästchen **Benutzerzugriff von VPN zulassen**, um autorisierten Zugriff von einem VPN aus zuzulassen.

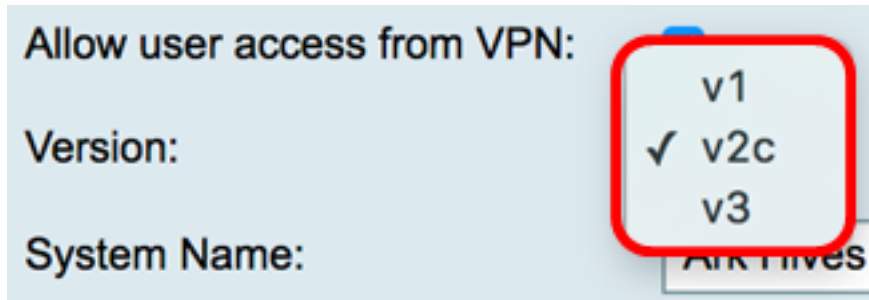


Schritt 5: Wählen Sie im Dropdown-Menü Version (Version) eine SNMP-Version aus, die im Netzwerk verwendet werden soll. Folgende Optionen stehen zur Verfügung:

- v1 - Option mit der niedrigsten Sicherheitsstufe. 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 ist ein Sicherheitsmodell, in dem eine Authentifizierungsstrategie für einen Benutzer und die Gruppe, in der sich der Benutzer befindet, eingerichtet wird. Die

Sicherheitsstufe ist der zulässige Sicherheitsgrad innerhalb eines Sicherheitsmodells. Eine Kombination aus Sicherheitsmodell und Sicherheitsstufe bestimmt, welcher Sicherheitsmechanismus bei der Verarbeitung eines SNMP-Pakets verwendet wird.

Hinweis: In diesem Beispiel wird v2c ausgewählt.



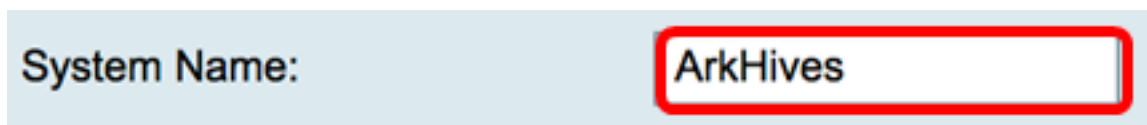
Allow user access from VPN:

Version: v1
✓ v2c
v3

System Name: ArkHives

Schritt 6: Geben Sie im Feld *Systemname* einen Namen für den Router ein, um die Identifizierung in Netzwerkverwaltungsanwendungen zu vereinfachen.

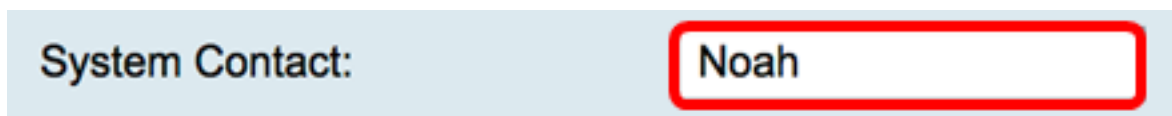
Hinweis: In diesem Beispiel wird ArkHives als Systemname verwendet.



System Name: ArkHives

Schritt 7: Geben Sie im Feld *Systemkontakt* einen Namen einer Person oder eines Administrators ein, der im Notfall mit dem Router identifiziert werden kann.

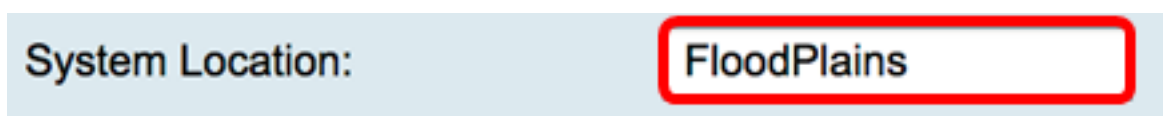
Hinweis: In diesem Beispiel wird Noah als Systemkontakt verwendet.



System Contact: Noah

Schritt 8: Geben Sie im Feld *Systemstandort* einen Speicherort des Routers ein. Dadurch wird das Auffinden eines Problems für einen Administrator viel einfacher.

Hinweis: In diesem Beispiel wird FloodPlains als Systemspeicherort verwendet.



System Location: FloodPlains

Um mit der Konfiguration fortzufahren, klicken Sie auf die in Schritt 5 ausgewählte SNMP-Version.

- [Konfigurieren von SNMP 1 oder v2c](#)
- [Konfigurieren von SNMP v3](#)

[Konfigurieren von SNMP 1 oder v2c](#)

Schritt 1: Wenn SNMP v2c in Schritt 5 ausgewählt wurde, geben Sie den SNMP-Community-Namen in das Feld *Get 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: Das schreibgeschützte Kennwort gibt die Berechtigung, nur Informationen abzurufen. In diesem Beispiel wird pblick verwendet.

Get Community:	<input type="text" value="pblick"/>
----------------	-------------------------------------

Schritt 2: Geben Sie im Feld *Community festlegen* 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: Es ist ratsam, beide Kennwörter in etwas individueller zu ändern, um Sicherheitsangriffe von Außenstehenden zu vermeiden. In diesem Beispiel wird pribado verwendet.

Set Community:	<input type="text" value="pribado"/>
----------------	--------------------------------------

Sie sollten jetzt die SNMP v1- oder v2-Einstellungen erfolgreich konfiguriert haben. Fahren Sie mit dem Bereich [Trap Configuration](#) fort.

[Konfigurieren von SNMP v3](#)

Schritt 1: Wenn SNMP v3 ausgewählt wurde, klicken Sie auf ein Optionsfeld im Bereich Benutzername, um eine Zugriffsberechtigung auszuwählen. Folgende Optionen stehen zur Verfügung:

- guest — schreibgeschützte Berechtigungen
- admin - Lese- und Schreibberechtigungen

Hinweis: In diesem Beispiel wird guest ausgewählt.

Der Bereich "Zugriffsberechtigung" zeigt den Berechtigungstyp an, je nachdem, auf welches Optionsfeld geklickt wurde.

Username:	<input checked="" type="radio"/> guest <input type="radio"/> admin
Access Privilege:	Read

Schritt 2: Klicken Sie im Bereich Authentifizierungsalgorithmus auf ein Optionsfeld, um eine Methode auszuwählen, die der SNMP-Agent für die Authentifizierung verwenden soll. Folgende Optionen stehen zur Verfügung:

- Keine - Es wird keine Benutzerauthentifizierung verwendet.
- MD5 - Message-Digest Algorithm 5 verwendet einen 128-Bit-Hash-Wert für die Authentifizierung. Benötigt Benutzername und Kennwort.
- SHA1 - Secure Hash Algorithm (SHA-1) ist ein unidirektionaler Hashing-Algorithmus, der ein

160-Bit-Digest erzeugt. SHA-1 berechnet langsamer als MD5, ist aber sicherer als MD5.

Hinweis: Für dieses Beispiel wird MD5 gewählt.

Authentication Algorithm: None MD5 SHA1

Authentication Password:

Hinweis: Wenn Sie None (Keine) ausgewählt haben, wechseln Sie zum Bereich [Trap Configuration \(Trap-Konfiguration\)](#).

Schritt 3: Geben Sie im Feld *Authentifizierungskennwort* ein Kennwort ein.

Authentication Algorithm: None MD5 SHA1

Authentication Password:

Schritt 4: (Optional) Klicken Sie im Bereich Encryption Algorithm (Verschlüsselungsalgorithmus) auf ein Optionsfeld, um festzulegen, wie SNMP-Informationen verschlüsselt werden sollen. Folgende Optionen stehen zur Verfügung:

- Keine - Es wird keine Verschlüsselung verwendet. Wenn dieser Schritt ausgewählt ist, fahren Sie mit dem Bereich [Trap Configuration](#) (Trap-Konfiguration) fort.
- DES - Data Encryption Standard (DES) ist eine 56-Bit-Verschlüsselungsmethode, die nicht sehr sicher ist, aber möglicherweise für die Abwärtskompatibilität erforderlich ist.
- AES - Advanced Encryption Standard (AES) Wenn diese Option ausgewählt ist, ist ein Verschlüsselungskennwort erforderlich.

Hinweis: Für dieses Beispiel wird DES gewählt.

Encryption Algorithm: None DES AES

Encryption Password:

Schritt 5: (Optional) Wenn DES oder AES ausgewählt wurde, geben Sie ein Verschlüsselungskennwort in das Feld *Verschlüsselungskennwort ein*.

Encryption Algorithm: None DES AES

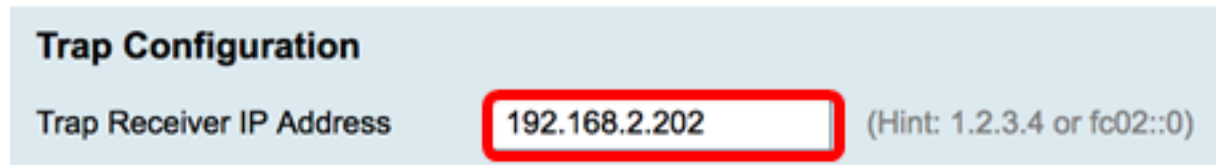
Encryption Password:

Sie sollten jetzt die SNMP v3-Einstellungen erfolgreich konfigurieren. Fahren Sie jetzt mit dem Bereich ["Trap Configuration"](#) fort.

Trap-Konfiguration

Schritt 1: Geben Sie im Feld *IP-Adresse des Trap Receivers* eine IPv4- oder eine IPv6-IP-Adresse ein, die die SNMP-Traps empfangen soll.

Hinweis: In diesem Beispiel wird 192.168.2.202 verwendet.

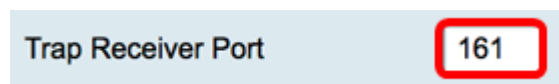


Trap Configuration

Trap Receiver IP Address (Hint: 1.2.3.4 or fc02::0)

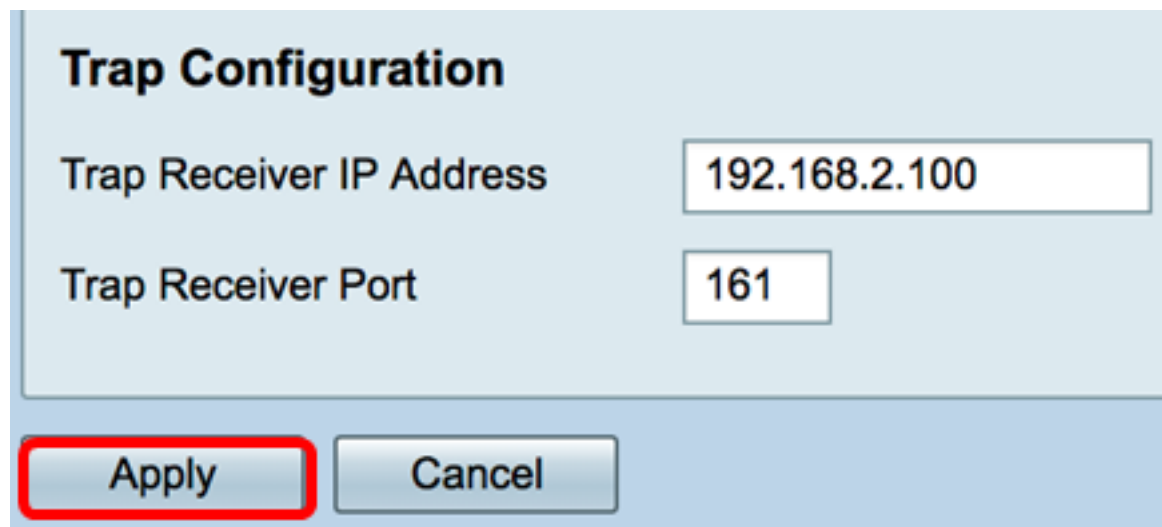
Schritt 2: Geben Sie eine UDP-Portnummer (User Datagram Protocol) im Feld *Trap Receiver Port* ein. Der SNMP-Agent überprüft diesen Port auf Zugriffsanfragen.

Hinweis: In diesem Beispiel wird 161 verwendet.



Trap Receiver Port

Schritt 3: Klicken Sie auf **Übernehmen**.



Trap Configuration

Trap Receiver IP Address

Trap Receiver Port

SNMP



Success. To permanently save the configuration. Go to [Configuration Management](#) page or click Save icon.

SNMP Enable:	<input checked="" type="checkbox"/>
Allow user access from Internet:	<input checked="" type="checkbox"/>
Allow user access from VPN:	<input checked="" type="checkbox"/>
Version:	v3
System Name:	Ark Hives
System Contact:	Noah
System Location:	FloodPlains
Username:	<input checked="" type="radio"/> guest <input type="radio"/> admin
Access Privilege:	Read
Authentication Algorithm:	<input type="radio"/> None <input checked="" type="radio"/> MD5 <input type="radio"/> SHA1
Authentication Password:
Encryption Algorithm:	<input type="radio"/> None <input checked="" type="radio"/> DES <input type="radio"/> AES
Encryption Password:

Trap Configuration

Trap Receiver IP Address	192.168.2.100	(Hint: 1.2.3.4 or fc02::0)
Trap Receiver Port	161	

Apply

Cancel

Schritt 4: (Optional) Um die Konfiguration dauerhaft zu speichern, öffnen Sie die Seite "Copy/Save Configuration" (Konfiguration kopieren/speichern), oder klicken Sie auf das



Symbol oben auf der Seite.

Sie sollten jetzt die SNMP-Einstellungen auf einem Router der Serie RV34x erfolgreich konfiguriert haben.