

Configurazione delle impostazioni SNMP (Simple Network Management Protocol) su un router serie RV34x

Obiettivo

Il protocollo SNMP (Simple Network Management Protocol) viene utilizzato per la gestione, la risoluzione dei problemi e la manutenzione della rete. SNMP registra, memorizza e condivide le informazioni con l'aiuto di due software chiave: un sistema di gestione della rete (NMS, Network Management System) in esecuzione sui dispositivi di gestione e un agente in esecuzione sui dispositivi gestiti. I router della serie RV34x supportano il protocollo SNMP versioni 1, 2 e 3.

SNMP v1 è la versione originale di SNMP che non dispone di determinate funzionalità e funziona solo sulle reti TCP/IP, mentre SNMP v2 è un'iterazione migliorata di v1. SNMP v1 e v2c devono essere scelti solo per le reti che utilizzano SNMPv1 o SNMPv2c. SNMP v3 è lo standard più recente di SNMP e risolve molti dei problemi di SNMP v1 e v2c. In particolare, vengono affrontate molte delle vulnerabilità di protezione di v1 e v2c. L'SNMP v3 consente inoltre agli amministratori di passare a uno standard SNMP comune.

In questo documento viene spiegato come configurare le impostazioni SNMP sui router serie RV34x.

Dispositivi interessati

- Serie RV34x

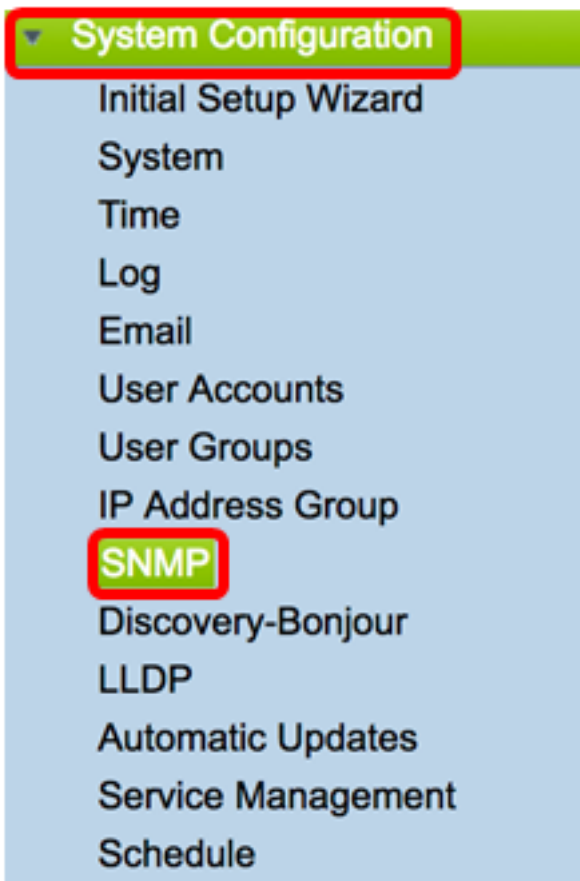
Versione del software

- 1.0.1.16

Configurazione delle impostazioni SNMP sui router serie RV34x

Configurazione delle impostazioni SNMP

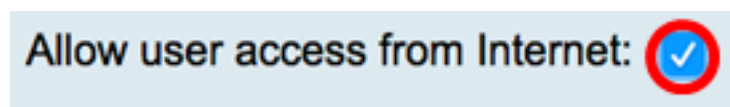
Passaggio 1. Accedere all'utility basata sul Web del router e scegliere **Configurazione di sistema > SNMP**.



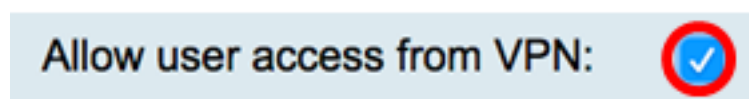
Passaggio 2. Selezionare la casella di controllo **SNMP Enable** per abilitare il protocollo SNMP.



Passaggio 3. (Facoltativo) Selezionare la casella di controllo **Consenti accesso utente da Internet** per consentire l'accesso degli utenti autorizzati all'esterno della rete tramite applicazioni di gestione come Cisco FindIT Network Management.



Passaggio 4. (Facoltativo) Selezionare la casella di controllo **Consenti accesso utente da VPN** per consentire l'accesso autorizzato da una VPN.

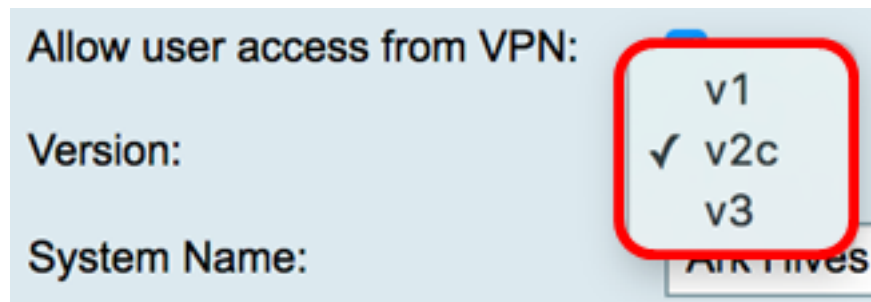


Passaggio 5. Dal menu a discesa Versione, scegliere una versione SNMP da utilizzare sulla rete. Le opzioni sono:

- v1 — Opzione meno sicura. Utilizza testo normale per le stringhe della community.
- v2c: il supporto migliorato per la gestione degli errori fornito da SNMPv2c include codici di errore estesi che distinguono i diversi tipi di errore; tutti i tipi di errori vengono segnalati tramite un singolo codice di errore in SNMPv1.
- v3 — SNMPv3 è un modello di protezione in cui viene impostata una strategia di

autenticazione per un utente e il gruppo in cui risiede l'utente. Il livello di protezione è il livello di protezione consentito in un modello di protezione. La combinazione di un modello di sicurezza e di un livello di sicurezza determina il meccanismo di sicurezza da utilizzare quando si gestisce un pacchetto SNMP.

Nota: In questo esempio viene scelto v2c.



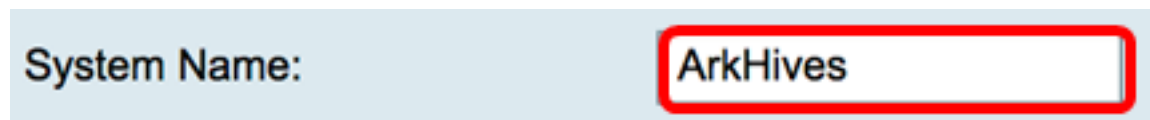
Allow user access from VPN:

Version: v1
✓ v2c
v3

System Name: ArkHives

Passaggio 6. Nel campo *System Name* (Nome di sistema), immettere un nome per il router per facilitarne l'identificazione nelle applicazioni di gestione della rete.

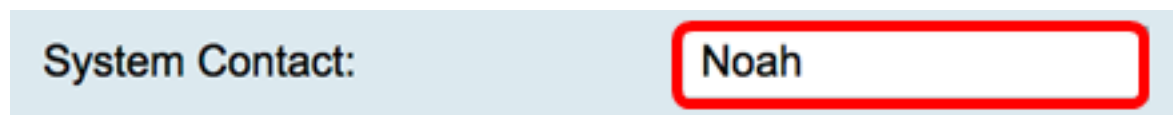
Nota: In questo esempio, ArkHives viene utilizzato come nome del sistema.



System Name: ArkHives

Passaggio 7. Nel campo *Contatto di sistema*, immettere il nome di un utente o di un amministratore da identificare con il router in caso di emergenza.

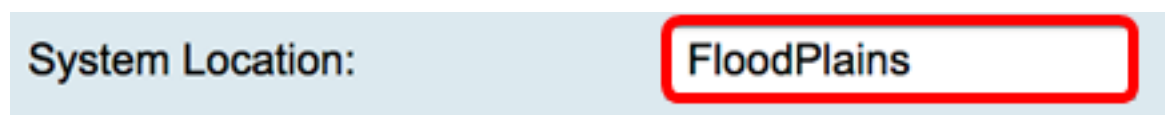
Nota: Nell'esempio, Noah viene utilizzato come contatto di sistema.



System Contact: Noah

Passaggio 8. Nel campo *System Location* (Posizione del sistema), immettere la posizione del router. In questo modo l'individuazione di un problema risulta molto più semplice per l'amministratore.

Nota: In questo esempio, FloodPlains viene utilizzato come posizione del sistema.



System Location: FloodPlains

Per continuare con la configurazione, fare clic sulla versione SNMP scelta nel passaggio 5.

- [Configurazione di SNMP 1 o v2c](#)
- [Configurazione di SNMP v3](#)

[Configurazione di SNMP 1 o v2c](#)

Passaggio 1. Se SNMP v2c è stato scelto nel Passaggio 5, immettere il nome della community SNMP nel campo *Otteni community*. Crea una community di sola lettura che viene utilizzata per accedere alle informazioni per l'agente SNMP. La stringa della community inviata nel pacchetto di richiesta inviato dal mittente deve corrispondere alla

stringa della community sul dispositivo agente. La stringa predefinita per la sola lettura è public.

Nota: La password di sola lettura consente di recuperare solo le informazioni. Nell'esempio viene utilizzato pblick.

Get Community:

Passaggio 2. Nel campo *Set Community*, immettere un nome di community SNMP. Crea una community di lettura/scrittura che viene utilizzata per accedere alle informazioni per l'agente SNMP. Vengono accettate solo le richieste dei dispositivi che si identificano con questo nome community. Nome creato dall'utente. Il valore predefinito è private.

Nota: Si consiglia di cambiare entrambe le password con qualcosa di più personalizzato al fine di evitare attacchi di sicurezza da parte di estranei. Nell'esempio viene utilizzato il pribado.

Set Community:

A questo punto, è necessario aver configurato correttamente le impostazioni SNMP v1 o v2. Passare all'area [Configurazione trap](#).

[Configurazione di SNMP v3](#)

Passaggio 1. Se è stato scelto SNMP v3, fare clic su un pulsante di opzione nell'area Nome utente per scegliere un privilegio di accesso. Le opzioni sono:

- guest: privilegi di sola lettura
- admin: privilegi di lettura e scrittura

Nota: Per questo esempio, viene scelto guest.

Nell'area Privilegio di accesso viene visualizzato il tipo di privilegio, a seconda del pulsante di opzione selezionato.

Username: guest admin
Access Privilege: Read

Passaggio 2. Fare clic su un pulsante di scelta nell'area Algoritmo di autenticazione per scegliere un metodo che l'agente SNMP utilizzerà per l'autenticazione. Le opzioni sono:

- Nessuno — non viene utilizzata l'autenticazione utente.
- MD5 — Message-Digest Algorithm 5 utilizza un valore hash a 128 bit per l'autenticazione. Richiede nome utente e password.
- SHA1 — Secure Hash Algorithm (SHA-1) è un algoritmo hash unidirezionale che produce un digest a 160 bit. SHA-1 è più lento di MD5, ma più sicuro di MD5.

Nota: Per questo esempio, viene scelto MD5.

Authentication Algorithm: None MD5 SHA1

Authentication Password:

Nota: Se si sceglie Nessuno, passare all'area [Configurazione trap](#).

Passaggio 3. Nel campo *Password di autenticazione*, immettere una password.

Authentication Algorithm: None MD5 SHA1

Authentication Password:

Passaggio 4. (Facoltativo) Nell'area Algoritmo di crittografia, fare clic su un pulsante di opzione per scegliere la modalità di crittografia delle informazioni SNMP. Le opzioni sono:

- Nessuno — non viene utilizzata alcuna crittografia. Se si sceglie questo passaggio, andare all'area [Configurazione trap](#).
- DES — Data Encryption Standard (DES) è un metodo di crittografia a 56 bit che non è molto sicuro, ma può essere necessario per garantire la compatibilità con le versioni precedenti.
- AES — Advanced Encryption Standard (AES). Se si sceglie questa opzione, è necessaria una password di crittografia.

Nota: Per questo esempio, viene scelto DES.

Encryption Algorithm: None DES AES

Encryption Password:

Passaggio 5. (Facoltativo) Se è stato scelto DES o AES, immettere una password di crittografia nel campo *Password crittografia*.

Encryption Algorithm: None DES AES

Encryption Password:

A questo punto è necessario configurare correttamente le impostazioni SNMP v3. Procedere ora all'area [Configurazione trap](#).

[Configurazione trap](#)

Passaggio 1. Nel campo *Trap Receiver IP Address* (Indirizzo IP ricevitore trap), immettere un indirizzo IPv4 o IPv6 che riceverà le trap SNMP.

Nota: Nell'esempio, viene usato 192.168.2.202.

Trap Configuration

Trap Receiver IP Address

(Hint: 1.2.3.4 or fc02::0)

Passaggio 2. Immettere un numero di porta UDP (User Datagram Protocol) nel campo *Porta ricevitore trap*. L'agente SNMP controlla questa porta per individuare eventuali richieste di accesso.

Nota: Nell'esempio viene utilizzato 161.

Trap Receiver Port

Passaggio 3. Fare clic su **Applica**.

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

Passaggio 4. (Facoltativo) Per salvare la configurazione in modo permanente, andare alla pagina Copia/Salva configurazione o fare clic sull'  icona nella parte superiore della pagina.

A questo punto, le impostazioni SNMP su un router serie RV34x devono essere configurate correttamente.