

在RV34x系列路由器上配置簡單網路管理協定(SNMP)設定

目標

簡易網路管理通訊協定(SNMP)用於網路管理、疑難排解和維護。SNMP在兩款重要軟體的幫助下記錄、儲存和共用資訊：在管理器裝置上運行的網路管理系統(NMS)和在受管裝置上運行的代理。RV34x系列路由器支援SNMP版本1、2和3。

SNMP v1是SNMP的原始版本，它缺少某些功能，只能在TCP/IP網路上運行，而SNMP v2是v1的改進版本。SNMP v1和v2c只應選擇用於使用SNMPv1或SNMPv2c的網路。SNMP v3是SNMP的最新標準，解決了SNMP v1和v2c的許多問題。特別是，它解決了v1和v2c中的許多安全漏洞。SNMP v3還允許管理員移動到一種常見的SNMP標準。

本文說明如何在RV34x系列路由器上配置SNMP設定。

適用裝置

- RV34x系列

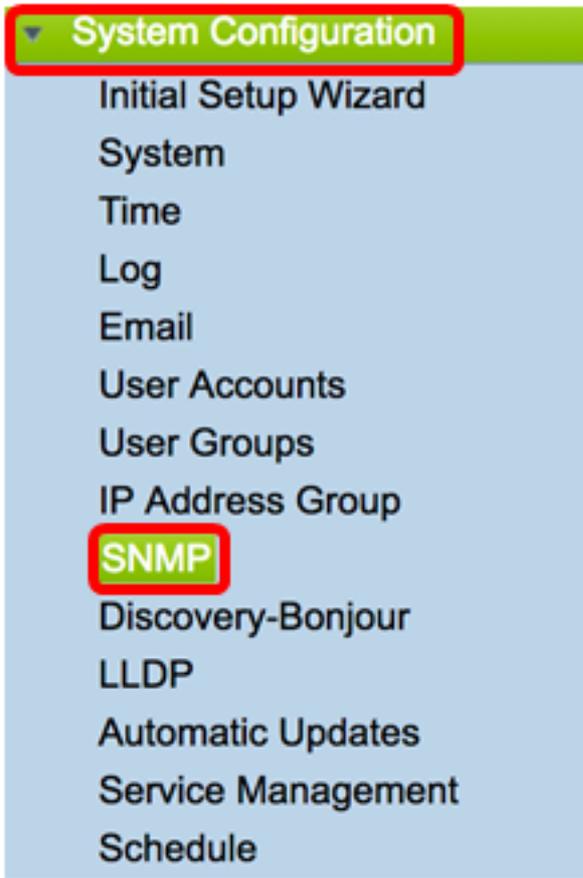
軟體版本

- 1.0.1.16

在RV34x系列路由器上配置SNMP設定

配置SNMP設定

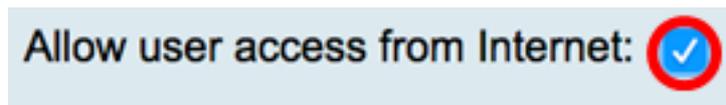
步驟1.登入到路由器的基於Web的實用程式，然後選擇System Configuration > SNMP。



步驟2. 勾選「SNMP Enable」覈取方塊以啟用SNMP。



步驟3. (可選) 選中Enable Allow user access from Internet覈取方塊，允許授權使用者通過管理應用程式 (如Cisco FindIT Network Management) 訪問網路外部。



步驟4. (可選) 選中Allow user access from VPN覈取方塊以允許從VPN進行授權訪問。



步驟5. 從「版本」下拉選單中，選擇要在網路上使用的SNMP版本。選項包括：

- v1 — 最不安全的選項。使用明文作為社群字串。
- v2c — SNMPv2c提供的改進型錯誤處理支援包括區分不同錯誤型別的擴展錯誤代碼；所有型別的錯誤都通過SNMPv1中的單個錯誤代碼報告。
- v3 — SNMPv3是一種安全模型，其中為使用者和使用者所在的組設定了身份驗證策略。安全級別是安全模型中允許的安全級別。安全模型和安全級別的組合確定了在處理SNMP資料包時使用的安全機制。

附註：在此示例中，選擇了v2c。

Allow user access from VPN:

Version:

System Name:



v1
✓ v2c
v3
ArkHives

步驟6.在 *System Name* 欄位中，輸入路由器的名稱，以便在網路管理應用程式中更容易識別。

附註：在本示例中，ArkHives 用作系統名稱。

System Name:

ArkHives

步驟7.在 *系統聯絡人* 欄位中，輸入個人或管理員的姓名，以便在緊急情況下識別路由器。

附註：在本示例中，Noah 用作系統聯絡人。

System Contact:

Noah

步驟8.在 *System Location* 欄位中輸入路由器的位置。這樣管理員可以更輕鬆地查詢問題。

附註：在本示例中，FloodPlains 用作系統位置。

System Location:

FloodPlains

要繼續配置，請按一下步驟5中選擇的SNMP版本。

- [配置SNMP 1或v2c](#)
- [配置SNMP v3](#)

[配置SNMP 1或v2c](#)

步驟1. 如果在步驟5中選擇了SNMP v2c，請在 *Get Community* 欄位中輸入SNMP社群名稱。它建立用於訪問SNMP代理資訊的只讀社群。傳送方傳送的請求資料包中傳送的社群字串必須與代理裝置上的社群字串匹配。只讀的預設字串是公共字串。

附註：只讀密碼授予僅檢索資訊的許可權。在此示例中，使用pblick。

Get Community:

pblick

步驟2.在 *Set Community* 欄位中，輸入SNMP社群名稱。它建立用於訪問SNMP代理資訊的讀寫社群。僅接受來自使用此社群名稱標識自己的裝置的請求。這是使用者建立的名稱。預設值為private。

附註：建議將兩個密碼更改為更自定義的密碼，以避免外部人員的安全攻擊。在本示例中，使

用pribado。

Set Community:

pribado

您現在應該已經成功配置了SNMP v1或v2設定。進入[Trap Configuration](#)區域。

配置SNMP v3

步驟1。如果已選擇SNMP v3，則按一下使用者名稱區域中的單選按鈕以選擇訪問許可權。選項包括：

- guest — 只讀許可權
- admin — 讀寫許可權

附註：在本例中，選擇了guest。

Access Privilege區域根據按一下的單選按鈕顯示許可權型別。

Username:

guest admin

Access Privilege:

Read

步驟2.按一下Authentication Algorithm區域中的單選按鈕以選擇SNMP代理將用於進行身份驗證的方法。選項包括：

- 無 — 不使用使用者身份驗證。
- MD5 — 消息摘要演算法5使用128位雜湊值進行身份驗證。需要使用者名稱和密碼。
- SHA1 — 安全雜湊演算法(SHA-1)是一種產生160位摘要的單向雜湊演算法。SHA-1的計算速度比MD5慢，但比MD5更安全。

附註：在本例中，選擇了MD5。

Authentication Algorithm:

None MD5 SHA1

Authentication Password:

附註：如果選擇無，請跳至[陷阱配置](#)區域。

步驟3.在Authentication Password欄位中輸入密碼。

Authentication Algorithm:

None MD5 SHA1

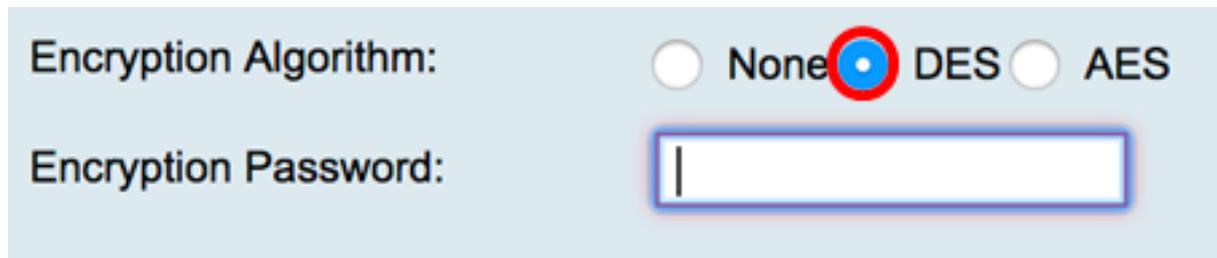
Authentication Password:

步驟4. (可選) 在Encryption Algorithm區域中，按一下單選按鈕以選擇如何加密SNMP資訊。選項包括：

- 無 — 不使用加密。如果選擇此步驟，請跳至[陷阱配置](#)區域。

- DES — 資料加密標準(DES)是一種56位加密方法，不太安全，但為了向後相容，可能需要這種加密方法。
- AES — 進階加密標準(AES)。如果選擇此項，則需要加密密碼。

附註：在本示例中，選擇了DES。



步驟5. (可選) 如果選擇DES或AES，請在*Encryption Password*欄位中輸入加密密碼。

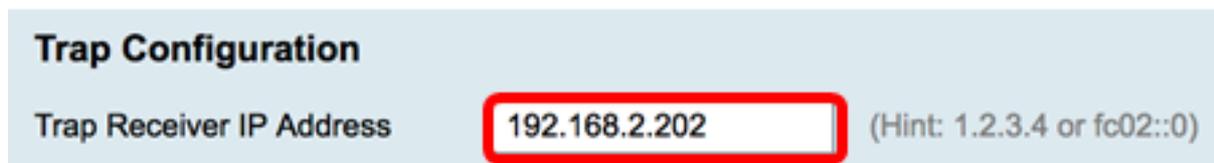


您現在應該已經成功配置SNMP v3設定。現在進入[Trap Configuration](#)區域。

陷阱配置

步驟1. 在*陷阱接收器IP地址*欄位中，輸入將接收SNMP陷阱的IPv4或IPv6 IP地址。

附註：在本示例中，使用了192.168.2.202。



步驟2. 在*Trap Receiver Port*欄位中輸入使用者資料包協定(UDP)端口號。SNMP代理檢查此埠是否有訪問請求。

附註：在本示例中，使用161。



步驟3. 按一下Apply。

Trap Configuration

Trap Receiver IP Address

192.168.2.100

Trap Receiver Port

161

Apply

Cancel

SNMP



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

SNMP Enable:



Allow user access from Internet:



Allow user access from VPN:



Version:

v3

System Name:

Ark Hives

System Contact:

Noah

System Location:

FloodPlains

Username:

guest admin

Access Privilege:

Read

Authentication Algorithm:

None MD5 SHA1

Authentication Password:

.....

Encryption Algorithm:

None DES 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

步驟4. (可選) 若要永久儲存組態，請前往「複製/儲存組態」頁面，或按一下頁面上部的圖



標。

現在，您應該已經在RV34x系列路由器上成功配置了SNMP設定。