

RV215W上的簡單網路管理協定(SNMP)配置

目標

簡單網路管理協定(SNMP)是用於管理和監控網路的應用層協定。SNMP由網路系統管理員用來管理網路效能、偵測和修正網路問題，以及收集網路統計資料。SNMP託管網路由託管裝置、代理和網路管理器組成。受管裝置是具備SNMP功能的裝置。代理是受管裝置上的SNMP軟體。網路管理器是從SNMP代理接收資料的實體。使用者必須安裝SNMP v3管理器程式才能檢視SNMP通知。

本文說明如何在RV215W上配置SNMP。

適用裝置

- RV215W

軟體版本

- 1.1.0.5

SNMP組態

步驟1.登入到Web配置實用程式並選擇Administration > SNMP。SNMP頁面隨即開啟：

SNMP

SNMP System Information

SNMP: Enable

Engine ID: 80000009033CCE738E0126

SysContact:

SysLocation:

SysName:

SNMPv3 User Configuration

UserName: guest admin

Access Privilege: Read Write User

Security level:

Authentication Algorithm Server: MD5 SHA

Authentication Password:

Privacy Algorithm: DES AES

Privacy Password:

Trap Configuration

IP Address: (Hint: 192.168.1.100 or fec0::64)

Port: (Range: 162 or 1025 - 65535, Default: 162)

Community:

SNMP Version:

Save

Cancel

SNMP系統資訊

SNMP System Information

SNMP: Enable

Engine ID: 80000009033CCE738E0126

SysContact:

SysLocation:

SysName:

步驟1.在SNMP欄位中選中**Enable**，以允許RV215W上的SNMP配置。

附註：RV215W代理的引擎ID顯示在「引擎ID」(Engine ID)欄位中。引擎ID用於唯一標識受管裝置上的代理。

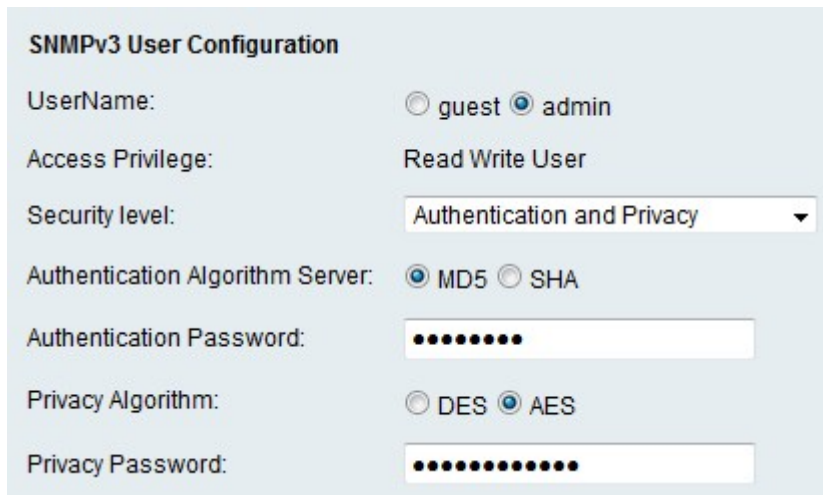
步驟2.在SysContact欄位中輸入系統聯絡人的名稱。通常做法是包括系統聯絡人的聯絡資訊。

步驟3.在SysLocation欄位中輸入RV215W的物理位置。

步驟4.在SysName欄位中輸入用於標識RV215W的名稱。

步驟5.按一下Save。

SNMPv3使用者配置



SNMPv3 User Configuration

UserName: guest admin

Access Privilege: Read Write User

Security level: Authentication and Privacy

Authentication Algorithm Server: MD5 SHA

Authentication Password:

Privacy Algorithm: DES AES

Privacy Password:

步驟1.在UserName欄位中點選與要配置的所需帳戶對應的單選按鈕。使用者的訪問許可權顯示在「訪問許可權」欄位中。

- 訪客 — 訪客使用者僅具有讀取許可權。
- 管理員 — 管理員使用者具有讀寫許可權。

步驟2.從Security level下拉選單中選擇所需的安全。驗證是用來進行驗證並允許使用者檢視或管理SNMP功能。隱私是可用於提高SNMP功能安全性的另一個金鑰。

- 無身份驗證和無隱私 — 使用者不需要身份驗證或隱私密碼。
- 身份驗證和無隱私 — 使用者只需要身份驗證。
- 身份驗證和隱私 — 使用者需要身份驗證和隱私密碼。

步驟3.如果安全級別包括身份驗證，請在Authentication Algorithm Server欄位中點選與所需伺服器對應的單選按鈕。此演算法是一個雜湊函式。雜湊函式用於將金鑰轉換為指定的位消息。

- MD5 - Message-Digest 5(MD5)是一種接受輸入並產生128位輸入消息摘要的演算法。
- SHA — 安全雜湊演算法(SHA)是一種接受輸入並產生160位元輸入訊息摘要的演算法。

步驟4.在Authentication Password欄位中輸入使用者的密碼。

步驟5.如果安全級別包括隱私，請點選與Privacy Algorithm欄位中所需演算法對應的單選按鈕。

- DES — 資料加密標準(DES)是一種加密演算法，使用相同的方法加密和解密消息。DES演算法的處理速度比AES快。
- AES — 高級加密標準(AES)是一種加密演算法，它使用不同的方法來加密和解密消息。這

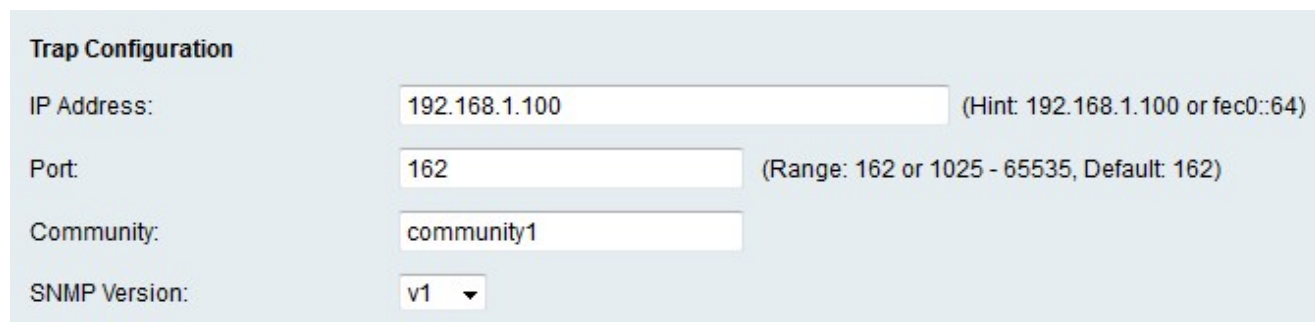
使得AES比DES更安全的加密演算法。

步驟6.在「隱私密碼」欄位中輸入使用者的隱私密碼。

步驟7.按一下「Save」。

陷阱配置

陷阱是生成的SNMP消息，用於報告系統事件。陷阱將強制受管裝置向網路管理器傳送SNMP消息，該消息將系統事件通知網路管理器。



The image shows a 'Trap Configuration' form with the following fields and values:

Field	Value	Hint/Range
IP Address:	192.168.1.100	(Hint: 192.168.1.100 or fec0::64)
Port:	162	(Range: 162 or 1025 - 65535, Default: 162)
Community:	community1	
SNMP Version:	v1	

步驟1.在IP地址欄位中輸入陷阱通知將傳送到的IP地址。

步驟2.在「埠」欄位中輸入陷阱通知將傳送到的IP地址的埠號。

步驟3.在Community欄位中輸入陷阱管理器所屬的社群字串。社群字串是充當密碼的文本字串。SNMP用它來驗證代理和網路管理器之間傳送的消息。

附註：此欄位僅在SNMP陷阱版本不是版本3時適用。

步驟4.從SNMP版本下拉選單中，為SNMP陷阱消息選擇SNMP管理器版本。

- v1 — 使用社群字串對陷阱消息進行身份驗證。
- v2c — 使用社群字串對陷阱消息進行身份驗證。
- v3 — 使用加密密碼驗證陷阱消息。

步驟5.按一下Save。