

# RV160 및 RV260 라우터에서 SNMP 구성

## 목표

이 문서의 목적은 RV160 및 RV260 라우터에서 SNMP(Simple Network Management Protocol) 설정을 구성하는 방법을 보여 주는 것입니다.

## 소개

SNMP는 IP 네트워크에서 관리되는 디바이스에서 데이터를 수집 및 구성하기 위한 인터넷 표준 프로토콜입니다. 네트워크 관리자는 네트워크에서 발생하는 중요 이벤트에 대한 알림을 관리, 모니터링, 수신하고 문제를 해결할 수 있습니다.

SNMP 프레임워크는 세 가지 요소로 구성됩니다. SNMP 관리자, SNMP 에이전트 및 MIB(Management Information Base). SNMP 관리자의 기능은 SNMP를 사용하는 네트워크 호스트의 활동을 제어하고 모니터링하는 것입니다. SNMP 에이전트는 디바이스의 소프트웨어 내에 있으며 시스템을 관리하기 위해 데이터 유지 관리를 지원합니다. 마지막으로 MIB는 네트워크 관리 정보를 위한 가상 스토리지 영역입니다. 이 세 가지가 결합되어 네트워크의 디바이스를 모니터링하고 관리합니다.

RV160/260 디바이스는 SNMP 버전 v1, v2c 및 v3을 지원합니다. SNMP 네트워크 관리 시스템에서 SNMP 명령에 응답하는 SNMP 에이전트 역할을 합니다. 지원되는 명령은 표준 SNMP 명령 get/next/set입니다. 또한 이 디바이스는 경보 조건이 발생할 경우 SNMP 관리자에게 알리기 위해 트랩 메시지를 생성합니다. 예를 들면 재부팅, 전원 주기 및 WAN 링크 이벤트가 있습니다.

## 적용 가능한 디바이스

- RV160
- RV260

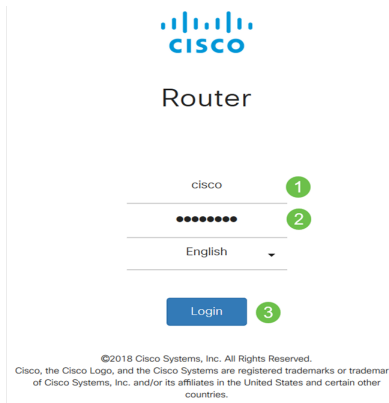
## 소프트웨어 버전

- 1.0.00.13

## SNMP 구성

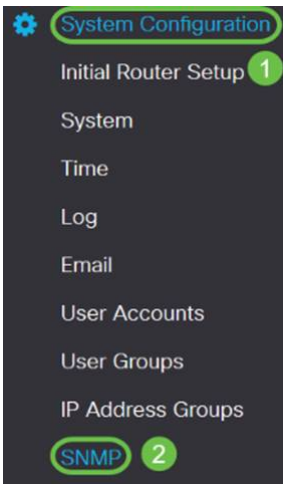
라우터의 SNMP를 구성하려면 다음 단계를 수행합니다.

1단계. 라우터의 웹 구성 페이지에 로그인합니다.

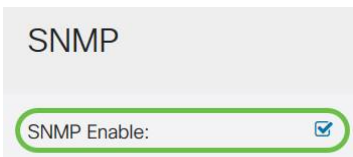


**참고:** 이 문서에서는 RV260W를 사용하여 SNMP를 구성합니다. 구성은 사용 중인 모델에 따라 달라질 수 있습니다.

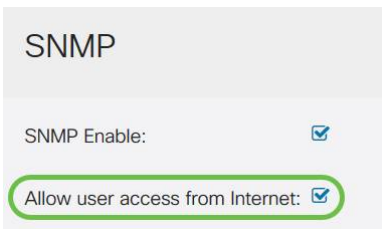
2단계. System Configuration(시스템 컨피그레이션) > SNMP로 이동합니다.



3단계. SNMP를 활성화하려면 **SNMP Enable** 확인란을 선택합니다.



4단계. (선택 사항) **Allow user access from Internet(인터넷에서 사용자 액세스 허용)** 확인란을 선택하여 Cisco FindIT Network Management와 같은 관리 애플리케이션을 통해 네트워크 외부에서 인증된 사용자 액세스를 허용합니다.



5단계. (선택 사항) **Allow user access from VPN(VPN에서 사용자 액세스 허용)** 확인란을 선택하여 VPN(Virtual Private Network)에서 인증된 액세스를 허용합니다.

SNMP

SNMP Enable:

Allow user access from Internet:

Allow user access from VPN:

6단계. *Version* 드롭다운 메뉴에서 네트워크에서 사용할 SNMP 버전을 선택합니다. 옵션은 다음과 같습니다.

- v1 - 가장 안전하지 않은 옵션입니다. 커뮤니티 문자열에 일반 텍스트를 사용합니다.
- v2c - SNMPv2c에서 제공하는 향상된 오류 처리 지원에는 다양한 유형의 오류를 구별하는 확장된 오류 코드가 포함됩니다. 모든 유형의 오류는 SNMPv1의 단일 오류 코드를 통해 보고됩니다.
- v3 - SNMPv3는 네트워크를 통해 데이터 패킷을 인증하고 암호화하여 디바이스에 대한 보안 액세스를 제공합니다. 인증 알고리즘에는 MD5(Message Digest Algorithm) 및 SHA(Secure Hash Algorithm)가 포함됩니다. 암호화 방법에는 DES(Data Encryption Standard) 및 AES(Advanced Encryption Standard)가 포함됩니다.

SNMPv3에 대한 자세한 내용을 보려면 [여기](#)를 클릭하십시오.

SNMP

SNMP Enable:

Allow user access from Internet:

Allow user access from VPN:

Version:

이 예에서는 v2c가 버전으로 선택되었습니다.

7단계. 다음 필드를 입력합니다.

- **System Name**(시스템 이름) - 네트워크 관리 애플리케이션에서 더 쉽게 식별할 수 있도록 라우터 이름을 입력합니다.
- **시스템 연락처** - 긴급 상황에 라우터와 식별할 개인 또는 관리자의 이름을 입력합니다.
- **시스템 위치** - 라우터의 위치를 입력합니다. 따라서 관리자가 훨씬 쉽게 문제를 찾을 수 있습니다.
- **Get Community**(커뮤니티 가져오기) - Get Community(커뮤니티 가져오기) 필드에 SNMP 커뮤니티 이름을 입력합니다. SNMP 에이전트의 정보에 액세스하고 검색하는 데 사용되는 읽기 전용 커뮤니티를 생성합니다.
- **Set Community**(커뮤니티 설정) - Set Community(커뮤니티 설정) 필드에 SNMP 커뮤니티 이름을 입력합니다. SNMP 에이전트의 정보에 액세스하고 이를 수정하는 데 사용되는 읽기-쓰기 커뮤니티를 생성합니다. 이 커뮤니티 이름으로 자신을 식별하는 디바이스의 요청만 허용됩니다. 사용자가 만든 이름입니다. 기본값은 private입니다.

System Name:  1

System Contact:  2

System Location:  3

Get Community:  4

Set Community:  5

## 트랩 구성

Trap 컨피그레이션을 사용하면 나가는 인터페이스에 관계없이 라우터에서 전송하는 모든 SNMP 트랩 패킷의 소스 주소를 단일 주소로 설정할 수 있습니다.

8단계. SNMP 트랩을 구성하려면 다음 정보를 입력합니다.

	.
<b>IP</b>	IP

Trap Configuration

Trap Community:  1

Trap Receiver IP Address:  2

Trap Receiver Port:  3

**참고:**일반적으로 SNMP는 UDP(User Datagram Protocol)를 전송 프로토콜로 사용하고 SNMP 트래픽의 기본 UDP 포트는 SNMP(161) 및 162(SNMP 트랩)입니다.

9단계. **적용**을 클릭합니다.

SNMP Apply Cancel

SNMP Enable:

Allow user access from Internet:

Allow user access from VPN:

Version: v2c

---

System Name:

System Contact:

System Location:

Get Community:

Set Community:

---

Trap Configuration

Trap Community:

Trap Receiver IP Address:

Trap Receiver Port:

이제 RV160/RV260 라우터에서 SNMP를 성공적으로 활성화하고 구성해야 합니다.