RV215W의 SNMP(Simple Network Management Protocol) 구성

목표

SNMP(Simple Network Management Protocol)는 네트워크를 관리하고 모니터링하는 데 사용되는 애플리케이션 레이어 프로토콜입니다.SNMP는 네트워크 관리자가 네트워크 성능을 관리하고 네트워크 문제를 탐지 및 수정하고 네트워크 통계를 수집하는 데 사용합니다.SNMP 관리 네트워크는 관리되는 디바이스, 에이전트 및 네트워크 관리자로 구성됩니다.관리되는 디바이스는 SNMP 기능을 지원하는 디바이스입니다.에이전트는 관리되는 디바이스의 SNMP 소프트웨어입니다.네트워크 관리자는 SNMP 에이전트로부터 데이터를 수신하는 엔티티입니다.사용자는 SNMP 알림을 보려면 SNMP v3 관리자 프로그램을 설치해야 합니다.

이 문서에서는 RV215W에서 SNMP를 구성하는 방법에 대해 설명합니다.

적용 가능한 디바이스

·RV215W

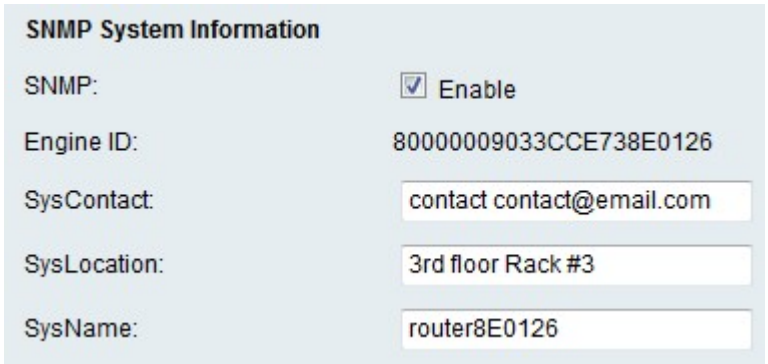
소프트웨어 버전

•1.1.0.5

SNMP 컨피그레이션

1단계. 웹 구성 유틸리티에 로그인하고 관리 **> SNMP를** 선택합니다.SNMP 페이지가 열립니다.

SNMP 시스템 정보



1단계. RV**215**W에서 SNMP 컨피그레이션을 허용하려면 SNMP 필드에서 Enable(활성화)을 선택합니다.

참고:RV215W 에이전트의 엔진 ID가 Engine ID 필드에 표시됩니다.엔진 ID는 관리되는 디바이스에서 에이전트를 고유하게 식별하는 데 사용됩니다.

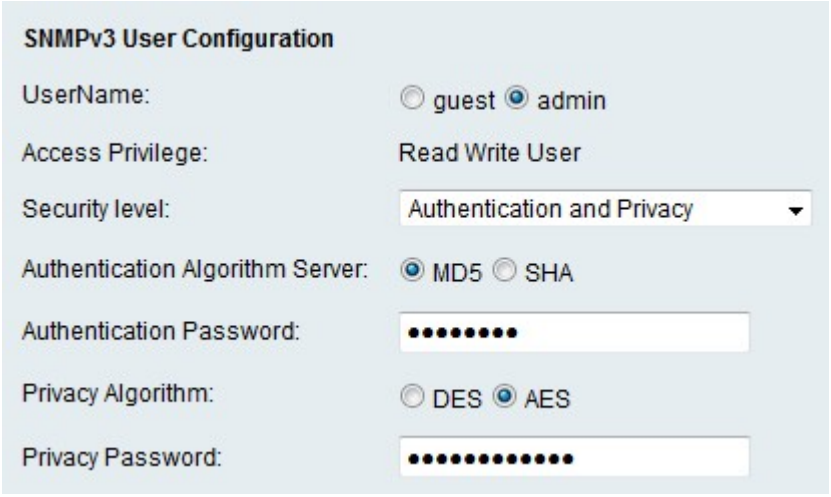
2단계. SysContact 필드에 시스템 연락처의 이름을 입력합니다.일반적으로 시스템 연락처에 대한 연락처 정보를 포함하는 것이 좋습니다.

3단계. SysLocation 필드에 RV215W의 물리적 위치를 입력합니다.

4단계. SysName 필드에 RV215W의 식별 이름을 입력합니다.

9단계. **저장**을 클릭합니다.

SNMPv3 사용자 구성



1단계. UserName 필드에서 구성할 원하는 계정에 해당하는 라디오 버튼을 클릭합니다.사용자의 액세스 권한이 액세스 권한 필드에 표시됩니다.

·게스트 — 게스트 사용자는 읽기 권한만 갖습니다.

·관리자 — 관리자 사용자에게 읽기 및 쓰기 권한이 있습니다.

2단계. Security level(보안 레벨) 드롭다운 목록에서 원하는 보안을 선택합니다.인증은 사용자가 SNMP 기능을 보거나 관리할 수 있도록 인증하고 허용하는 데 사용됩니다.프라이버시는 SNMP 기능의 보안을 강화하는 데 사용할 수 있는 또 다른 키입니다.

·No Authentication and No Privacy(인증 없음 및 프라이버시 없음) - 사용자가 인증 또는 개인 정보 암호를 요구하지 않습니다.

·인증 및 프라이버시 없음 — 사용자가 인증만 필요로 합니다.

·인증 및 프라이버시 - 사용자가 인증 및 개인 정보 암호를 모두 필요로 합니다.

3단계. 보안 레벨에 인증이 포함된 경우 Authentication Algorithm Server(인증 알고리즘 서버) 필드에서 원하는 서버에 해당하는 라디오 버튼을 클릭합니다.이 알고리즘은 해시 함수입니다.해시 함수는 키를 지정된 비트 메시지로 변환하는 데 사용됩니다.

·MD5 — MD5(Message-Digest 5)는 입력을 받아 입력의 128비트 메시지 다이제스트를 생성하는 알고리즘입니다.

·SHA — SHA(Secure Hash Algorithm)는 입력을 받아 입력의 160비트 메시지 다이제스트를 생성하는 알고리즘입니다.

4단계. Authentication Password(인증 비밀번호) 필드에 사용자의 비밀번호를 입력합니다.

5단계. 보안 레벨에 개인 정보가 포함된 경우 프라이버시 알고리즘 필드에서 원하는 알고리즘

에 해당하는 라디오 버튼을 클릭합니다.

·DES — DES(Data Encryption Standard)는 동일한 방법을 사용하여 메시지를 암호화하고 해독하는 암호화 알고리즘입니다.DES 알고리즘은 AES보다 빠르게 처리됩니다.

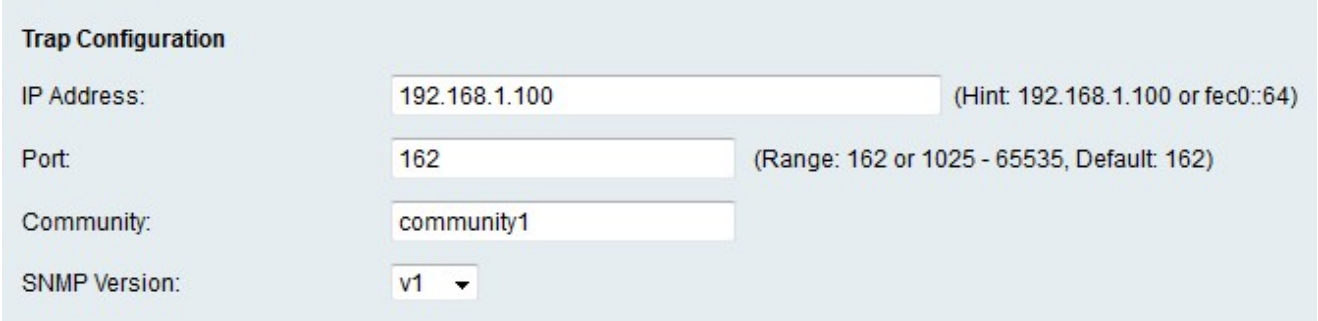
·AES — AES(Advanced Encryption Standard)는 메시지 암호화 및 해독에 다른 방법을 사용하는 암호화 알고리즘입니다.따라서 AES는 DES보다 더 안전한 암호화 알고리즘입니다.

6단계. Privacy Password(프라이버시 비밀번호) 필드에 사용자의 프라이버시 비밀번호를 입력합니다.

7단계. **저장**을 클릭합니다.

트랩 구성

트랩은 시스템 이벤트를 보고하는 데 사용되는 SNMP 메시지를 생성합니다.트랩은 관리 대상 장치가 네트워크 관리자에게 시스템 이벤트를 알리는 SNMP 메시지를 전송하도록 강제합니다.



1단계. IP 주소 필드에 트랩 알림을 전송할 IP 주소를 입력합니다.

2단계. Port(포트) 필드에 트랩 알림을 전송할 IP 주소의 포트 번호를 입력합니다.

3단계. Community(커뮤니티) 필드에 트랩 관리자가 속한 커뮤니티 문자열을 입력합니다.커뮤니티 문자열은 비밀번호로 작동하는 텍스트 문자열입니다.SNMP에서 에이전트와 네트워크 관리자 간에 전송되는 메시지를 인증하는 데 사용됩니다.

참고:이 필드는 SNMP 트랩 버전이 버전 3이 아닌 경우에만 적용됩니다.

4단계. SNMP Version(SNMP 버전) 드롭다운 목록에서 SNMP 트랩 메시지에 대한 SNMP 관리자 버전을 선택합니다.

·v1 — 커뮤니티 문자열을 사용하여 트랩 메시지를 인증합니다.

·v2c — 커뮤니티 문자열을 사용하여 트랩 메시지를 인증합니다.

·v3 — 암호화된 비밀번호를 사용하여 트랩 메시지를 인증합니다.

9단계. **저장**을 클릭합니다.