

# snmpwalk 명령 컨피그레이션 예와 함께 ESA, SMA 및 WSA 쿼리

## 목차

[소개](#)

[사전 요구 사항](#)

[구성](#)

[ESA 컨피그레이션](#)

[SMA 컨피그레이션](#)

[WSA 컨피그레이션](#)

[다음을 확인합니다.](#)

[문제 해결](#)

## 소개

이 문서에서는 snmpwalk 명령을 사용하여 Cisco ESA(Email Security Appliance), Cisco SMA(Content Security Management Appliance) 또는 Cisco WSA(Web Security Appliance)를 쿼리하거나 폴링합니다.

## 사전 요구 사항

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ESA with AsyncOS 5.x 이상
- AsyncOS 5.x 이상의 SMA
- AsyncOS 5.x 이상의 WSA
- 배포 net-snmp 패키지가 설치된 별도의 Linux 또는 Unix 호스트 시스템이 필요합니다.

**참고:** 이 문서는 Cisco에서 유지 관리하거나 지원하지 않는 소프트웨어를 참조합니다. 이 정보는 귀하의 편의를 위해 제공됩니다. 자세한 내용은 소프트웨어 공급업체에 문의하십시오.

## 구성

이 섹션에서는 ESA, SMA 및 WSA의 컨피그레이션에 대해 설명합니다.

### ESA 컨피그레이션

1. 다음을 입력합니다. snmpconfig SNMP(Simple Network Management Protocol)가 활성화되도록 하기 위한 CLI 명령
2. 관련 툴의 [Cisco Email Security Appliance](#)에서 모든 관련 AsyncOS MIB 파일을 다운로드합니다.  
AsyncOS SMI MIB for ESA(txt) AsyncOS Mail MIB for ESA(txt)

3. 이러한 파일을 로컬 시스템 SNMP 디렉토리에 배치합니다. 이 디렉토리는 일반적으로 다음과 유사합니다. `/usr/net-snmp/share/mibs/`.

4. SNMP 호스트를 사용하여 `snmpwalk` 명령:

```
snmpwalk -O a -v 2c -c ironport -M /usr/net-snmp/share/mibs/ -m "ALL" host.example.com iso.3.6.1.2.1.1
```

이전 명령에서 다음을 지정합니다.

- '-O'가 있는 모든 출력 필드입니다.
- SNMP 프로토콜 버전 2c('-v 2c' 포함).
- 읽기 전용 또는 공용 커뮤니티 문자열(어플라이언스의 `snmpconfig` 설정) 또는 '-c cisco'가 있는 'cisco'.
- '-M /the/path/to/snmp/mibs/'를 사용하는 MIB 파일의 절대 경로 또는 위치(선택 사항).
- 로드할 MIB 파일(모두 로드됨)을 '-m "ALL"'로 로드합니다.
- 'hostname' 또는 'x.x.x.x'로 폴링할 어플라이언스의 대상 호스트 주소.
- 어플라이언스의 OID(Object Identifier) 트리의 시작점으로, 'iso.3.6.1.2.1.1'으로 이동을 시작합니다.

이전에 나열된 샘플 명령은 어플라이언스에서 가져온 모든 진단 정보 목록을 반환합니다.

```
~$ snmpwalk -O a -v 2c -c ironport -M "/usr/net-snmp/share/mibs/" -m "ALL" host.example.com iso.3.6.1.2.1.1 iso.3.6.1.2.1.1.1.0 = STRING: "IronPort Model C10, AsyncOS Version: 7.0.0-702, Build Date: 2009-11-10, Serial #: 00C09F3AED0E-#####" iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.15497.1.1
```

## SNMPv3 예

```
snmpwalk -v3 -l authPriv -u v3get -a SHA -A "cisco" -x AES -X "cisco" x.x.x.x iso.3.6.1.2.1.1
```

이전 명령에서 다음을 지정합니다.

- SNMP 프로토콜 버전 3('-v 3' 포함).
- -l 옵션은 사용할 인증 및 암호화 기능을 구성합니다.
- -u 옵션은 SNMP 사용자 이름을 User Security Module 하위 시스템으로 설정합니다. 1~32자의 문자열입니다. 통신을 시도하는 두 SNMP 엔티티에서 동일한 방식으로 구성해야 합니다.
- -a 옵션은 인증을 설정하는 것입니다.
- -A는 비밀 암호화 키입니다.
- -x 옵션은 암호화 유형을 설정하는 것입니다.

- -X는 SNMPv3 프라이버시 패스프레이즈를 설정하는 것입니다.
- 'hostname' 또는 'x.x.x.x'로 폴링할 어플라이언스의 대상 호스트 주소.
- 어플라이언스의 OID(Object Identifier) 트리의 시작점으로, 'iso.3.6.1.2.1.1'으로 이동을 시작합니다.

또한 Net-[SNMP 자습서](#) 또는 `snmpwalk --help` 자세한 내용은 `snmpwalk` 명령 및 기타 SNMP 관련 유틸리티.

## SMA 컨피그레이션

1. 다음을 입력합니다. `snmpconfig` SNMP가 활성화되었는지 확인하기 위한 CLI 명령
2. 관련 톨의 [Cisco Content Security Management Appliance](#)에서 모든 관련 AsyncOS MIB 파일을 다운로드합니다.  
AsyncOS SMI MIB for SMA(txt) AsyncOS Mail MIB for SMA(txt)
3. 이러한 파일을 로컬 시스템 SNMP 디렉토리에 배치합니다. 이 디렉토리는 일반적으로 다음과 유사합니다. `/usr/net-snmp/share/mibs/`.
4. SNMP 호스트를 사용하여 `snmpwalk` 명령:

```
snmpwalk -O a -v 2c -c ironport -M /usr/net-snmp/share/mibs/ -m "ALL" host.example.com iso.3.6.1.2.1.1
```

이전 명령에서 다음을 지정합니다.

- '-O'가 있는 모든 출력 필드입니다.
- SNMP 프로토콜 버전 2c('-v 2c' 포함).
- 읽기 전용 또는 공용 커뮤니티 문자열(어플라이언스의 `snmpconfig` 설정) 또는 '-c cisco'가 있는 'cisco'.
- '-M /the/path/to/snmp/mibs/'를 사용하는 MIB 파일의 절대 경로 또는 위치(선택 사항).
- 로드할 MIB 파일(모두 로드됨)을 '-m "ALL"'로 로드합니다.
- 'hostname' 또는 'x.x.x.x'로 폴링할 어플라이언스의 대상 호스트 주소.
- 어플라이언스의 OID(Object Identifier) 트리의 시작점으로, 'iso.3.6.1.2.1.1'으로 이동을 시작합니다.

이전에 나열된 샘플 명령은 어플라이언스에서 가져온 모든 진단 정보 목록을 반환합니다.

```
~$ snmpwalk -O a -v 2c -c ironport -M "/usr/net-snmp/share/mibs/" -m "ALL" host.example.com iso.3.6.1.2.1.1 iso.3.6.1.2.1.1.1.0 = STRING: "IronPort Model C10, AsyncOS Version: 7.0.0-702, Build Date: 2009-11-10, Serial #: 00C09F3AED0E-#####" iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.15497.1.1
```

## SNMPv3 예

snmpwalk -v3 -l authPriv -u v3get -a SHA -A "cisco" -x AES -X "cisco" x.x.x.x iso.3.6.1.2.1.1  
이전 명령에서 다음을 지정합니다.

- SNMP 프로토콜 버전 3('-v 3' 포함).
- - 옵션은 사용할 인증 및 암호화 기능을 구성합니다.
- -u 옵션은 SNMP 사용자 이름을 User Security Module 하위 시스템으로 설정합니다. 1~32자의 문자열입니다. 통신을 시도하는 두 SNMP 엔티티에서 동일한 방식으로 구성해야 합니다.
- -a 옵션은 인증을 설정하는 것입니다.
- -A는 비밀 암호화 키입니다.
- -x 옵션은 암호화 유형을 설정하는 것입니다.
- -X는 SNMPv3 프라이버시 패스프레이즈를 설정하는 것입니다.
- 'hostname' 또는 'x.x.x.x'로 폴링할 어플라이언스의 대상 호스트 주소.
- 어플라이언스의 OID(Object Identifier) 트리의 시작점으로, 'iso.3.6.1.2.1.1'으로 이동을 시작합니다.

또한 Net-[SNMP 자습서](#) 또는 `snmpwalk --help` 자세한 내용은 `snmpwalk` 명령 및 기타 SNMP 관련 유틸리티.

## WSA 컨피그레이션

1. 다음을 입력합니다. `snmpconfig` SNMP가 활성화되었는지 확인하기 위한 CLI 명령
2. 관련 툴의 [Cisco Web Security Appliance](#)에서 모든 관련 AsyncOS MIB 파일을 다운로드합니다.  
WSA용 AsyncOS SMI MIB(txt) AsyncOS Mail MIB for WSA(txt) AsyncOS 웹 MIB(txt)
3. 이러한 파일을 로컬 시스템 SNMP 디렉토리에 배치합니다. 이 디렉토리는 일반적으로 다음과 유사합니다. `/usr/net-snmp/share/mibs/`.
4. SNMP 호스트를 사용하여 `snmpwalk` 명령:

```
snmpwalk -O a -v 2c -c ironport -M /usr/net-snmp/share/mibs/ -m "ALL" host.example.com  
iso.3.6.1.2.1.1
```

이전 명령에서 다음을 지정합니다.

- '-O'가 있는 모든 출력 필드입니다.
- SNMP 프로토콜 버전 2c('-v 2c' 포함).
- 읽기 전용 또는 공용 커뮤니티 문자열(어플라이언스의 `snmpconfig` 설정) 또는 '-c cisco'가 있는 'cisco'.

- '-M /the/path/to/snmp/mibs/'를 사용하는 MIB 파일의 절대 경로 또는 위치(선택 사항).
- 로드할 MIB 파일(모두 로드됨)을 '-m "ALL"'로 로드합니다.
- 'hostname' 또는 'x.x.x.x'로 폴링할 어플라이언스의 대상 호스트 주소.
- 어플라이언스의 OID(Object Identifier) 트리의 시작점으로, 'iso.3.6.1.2.1.1'으로 이동을 시작합니다.

이전에 나열된 샘플 명령은 어플라이언스에서 가져온 모든 진단 정보 목록을 반환합니다.

```

:~$ snmpwalk -O a -v 2c -c ironport -M "/usr/net-snmp/share/mibs/" -m "ALL"
host.example.com iso.3.6.1.2.1.1
iso.3.6.1.2.1.1.1.0 = STRING: "IronPort Model C10, AsyncOS Version: 7.0.0-702,
Build Date: 2009-11-10, Serial #: 00C09F3AED0E-#####
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.15497.1.1

```

또한 [Net-SNMP 자습서](#) 또는 `snmpwalk --help` 자세한 내용은 `snmpwalk` 명령 및 기타 SNMP 관련 유틸리티.

## 다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

## 문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.