

CSM 3.x - 인벤토리에 IDS 센서 및 모듈 추가

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[Security Manager 인벤토리에 디바이스 추가](#)

[IDS 센서 및 모듈 추가 단계](#)

[디바이스 정보 제공—새 디바이스](#)

[문제 해결](#)

[오류 메시지](#)

[관련 정보](#)

소개

이 문서에서는 CSM(Cisco Security Manager)에서 IDS(Intrusion Detection System) 센서 및 모듈 (Catalyst 6500 스위치의 IDSM, 라우터의 NM-CIDS 및 ASA의 AIP-SSM 포함)을 추가하는 방법에 대해 설명합니다.

참고: CSM 3.2는 IPS 6.2를 지원하지 않습니다. CSM 3.3에서 지원됩니다.

사전 요구 사항

요구 사항

이 문서에서는 CSM 및 IDS 디바이스가 설치되고 제대로 작동한다고 가정합니다.

사용되는 구성 요소

이 문서의 정보는 CSM 3.0.1을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오](#).

Security Manager 인벤토리에 디바이스 추가

Security Manager에 디바이스를 추가할 때 디바이스의 DNS 이름 및 IP 주소와 같은 식별 정보 범위를 가져옵니다. 디바이스를 추가하면 Security Manager 디바이스 인벤토리에 표시됩니다. 인벤토리에 디바이스를 추가한 후에만 Security Manager에서 디바이스를 관리할 수 있습니다.

다음 방법으로 Security Manager 인벤토리에 디바이스를 추가할 수 있습니다.

- 네트워크에서 디바이스를 추가합니다.
- 아직 네트워크에 없는 새 장치 추가
- DCR(Device and Credentials Repository)에서 하나 이상의 디바이스를 추가합니다.
- 구성 파일에서 하나 이상의 디바이스를 추가합니다.

참고: 이 문서에서는 다음 방법에 중점을 둡니다. 아직 네트워크에 없는 새 디바이스를 추가합니다.

IDS 센서 및 모듈 추가 단계

Security Manager 인벤토리에 단일 디바이스를 추가하려면 Add New Device 옵션을 사용합니다. 사전 프로비저닝에 이 옵션을 사용할 수 있습니다. 시스템에서 디바이스를 생성하고, 디바이스에 정책을 할당하고, 디바이스 하드웨어를 받기 전에 컨피그레이션 파일을 생성할 수 있습니다.

디바이스 하드웨어를 수신할 때 Security Manager에서 관리할 디바이스를 준비해야 합니다. 자세한 내용은 [Security Manager를 위한 디바이스 준비](#)를 참조하십시오.

다음 절차는 새 IDS 센서 및 모듈을 추가하는 방법을 보여줍니다.

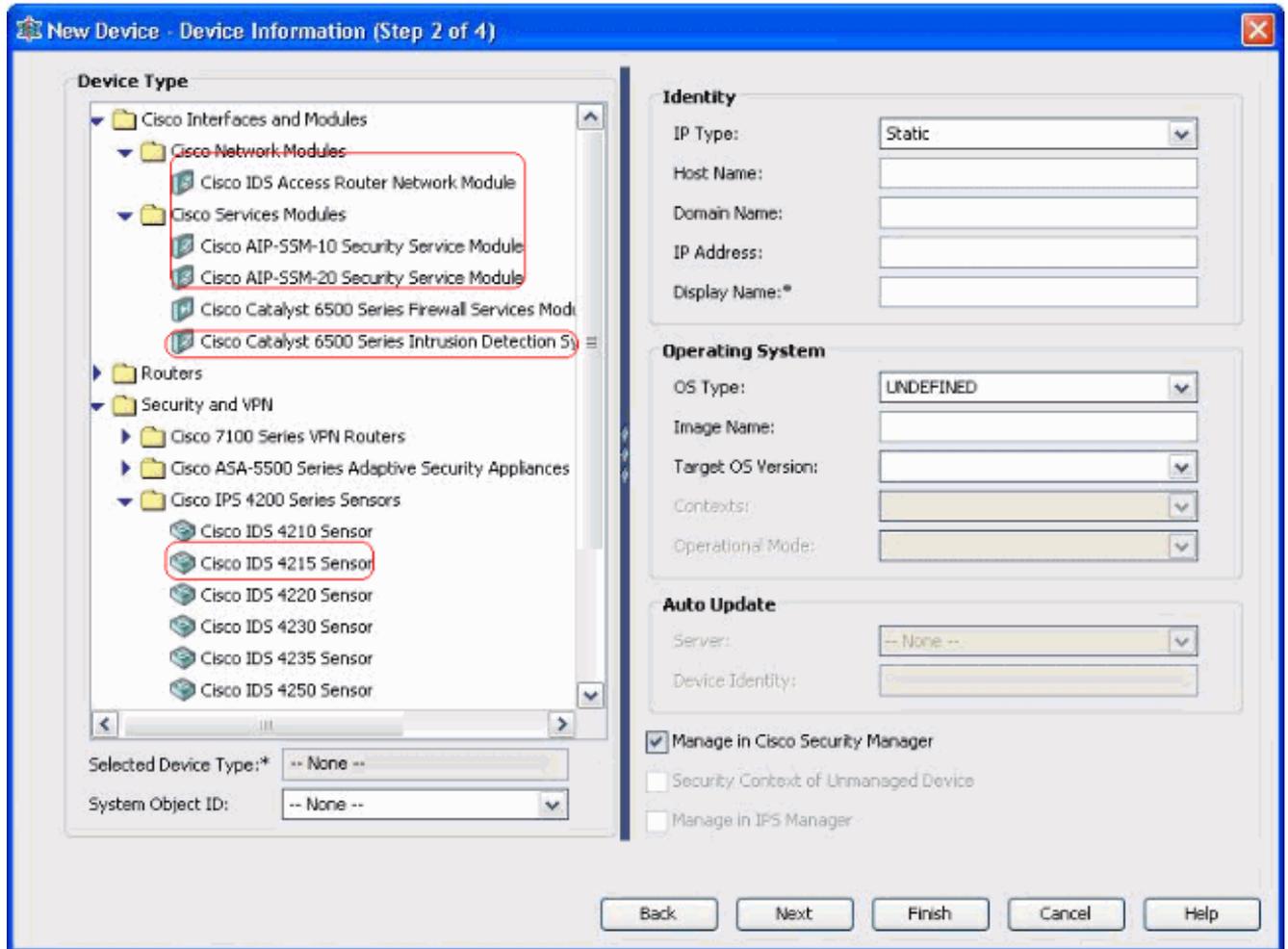
1. 도구 모음에서 **Device View** 버튼을 클릭합니다.Devices 페이지가 나타납니다.
2. Device **Selector**에서 Add 버튼을 클릭합니다.New Device - Choose Method 페이지가 4개의 옵션과 함께 나타납니다.
3. Add **New Device(새 디바이스 추가)**를 선택한 다음 **Next(다음)**를 클릭합니다.New Device - Device Information 페이지가 나타납니다.
4. 해당 필드에 디바이스 정보를 입력합니다.자세한 내용은 [Providing Device Information—New Device](#) 섹션을 참조하십시오.
5. **마침을 클릭합니다.**시스템은 디바이스 검증 작업을 수행합니다.데이터가 올바르지 않으면 오류 메시지가 생성되고 오류가 발생하는 페이지가 표시됩니다. 이 페이지에 해당하는 빨간색 오류 아이콘이 표시됩니다.데이터가 올바르면 디바이스가 인벤토리에 추가되고 디바이스 선택기에 표시됩니다.

디바이스 정보 제공—새 디바이스

다음 단계를 완료하십시오.

1. 새 디바이스의 디바이스 유형을 선택합니다.지원되는 디바이스 제품군을 표시하려면 최상위 디바이스 유형 폴더를 선택합니다.지원되는 디바이스 유형을 표시하려면 디바이스 패밀리 폴더를 선택합니다.**Cisco IDS Access Router Network Module**을 추가하려면 **Cisco Interfaces and Modules(Cisco Interfaces and Modules) > Cisco Network Modules(Cisco IDS Access Router 네트워크 모듈)**를 선택합니다. 마찬가지로 표시된 AIP-SSM 및 IDSM 모듈을 추가하려면 **Cisco Interfaces and Modules(Cisco Interfaces and Modules) > Cisco Services Modules(시스코 서비스 모듈)**를 선택합니다.CSM 인벤토리에 Cisco IDS 4210 센서를 추가하

려면 Security and VPN > Cisco IPS 4200 Series Sensor를 선택합니다



디바이스 유형을 선택합니다.참고: 디바이스를 추가한 후에는 디바이스 유형을 변경할 수 없습니다. 해당 디바이스 유형에 대한 시스템 객체 ID가 SysObjectId 필드에 표시됩니다. 첫 번째 시스템 개체 ID는 기본적으로 선택됩니다. 필요한 경우 다른 항목을 선택할 수 있습니다.

2. IP 유형(정적 또는 동적), 호스트 이름, 도메인 이름, IP 주소, 표시 이름과 같은 디바이스 ID 정보를 입력합니다.
3. OS 유형, 이미지 이름, 대상 OS 버전, 컨텍스트 및 운영 모드와 같은 디바이스 운영 체제 정보를 입력합니다.
4. 선택한 디바이스 유형에 따라 Auto Update 또는 CNS-Configuration Engine 필드가 나타납니다. Auto Update(자동 업데이트) - PIX 방화벽 및 ASA 디바이스에 대해 표시됩니다. CNS-Configuration Engine - Cisco IOS® 라우터에 대해 표시됩니다.참고: 이 필드는 Catalyst 6500/7600 및 FWSM 디바이스에 대해 활성화되지 않습니다.
5. 다음 단계를 완료하십시오. Auto Update(자동 업데이트) - 화살표를 클릭하여 서버 목록을 표시합니다. 디바이스를 관리하는 서버를 선택합니다. 서버가 목록에 나타나지 않으면 다음 단계를 완료합니다. 화살표를 클릭한 다음 + Add Server...를 선택합니다. Server Properties 대화 상자가 나타납니다. 필수 필드에 정보를 입력합니다. 확인을 클릭합니다. 새 서버가 사용 가능한 서버 목록에 추가됩니다. CNS-Configuration Engine(CNS-컨피그레이션 엔진) - 고정 또는 동적 IP 유형을 선택하느냐에 따라 다른 정보가 표시됩니다. Static(고정) - 구성 엔진 목록을 표시하려면 화살표를 클릭합니다. 디바이스를 관리하는 컨피그레이션 엔진을 선택합니다. 구성 엔진이 목록에 나타나지 않으면 다음 단계를 완료합니다. 화살표를 클릭한 다음 + Add Configuration Engine...(컨피그레이션 엔진 추가...)을 선택합니다. 구성 엔진 속성 대화 상자가 나타납니다. 필수 필드에 정보를 입력합니다. 확인을 클릭합니다. 사용 가능한 구성 엔진 목록에 새 구성 엔진이 추가됩니다. Dynamic(동적) - 화살표를 클릭하여 서버 목록을 표시합니다.

디바이스를 관리하는 서버를 선택합니다. 서버가 목록에 나타나지 않으면 다음 단계를 완료합니다. 화살표를 클릭한 다음 + **Add Server...**를 선택합니다. Server Properties 대화 상자가 나타납니다. 필수 필드에 정보를 입력합니다. **확인**을 클릭합니다. 새 서버가 사용 가능한 서버 목록에 추가됩니다.

- 다음 단계를 완료하십시오. Security Manager에서 디바이스를 관리하려면 **Cisco Security Manager에서 관리** 확인란을 선택합니다. 이것이 기본값입니다. 추가하는 디바이스의 유일한 기능이 VPN 엔드포인트 역할을 하는 경우 **Cisco Security Manager에서 관리** 확인란의 선택을 취소합니다. Security Manager는 이 장치의 구성을 관리하거나 구성을 업로드 또는 다운로드하지 않습니다.
- Security Manager에서 상위 디바이스(PIX Firewall, ASA 또는 FWSM)를 관리하지 않는 보안 컨텍스트를 관리하려면 Security Context of Unmanaged Device 확인란을 선택합니다. PIX 방화벽, ASA 또는 FWSM을 보안 컨텍스트라고도 하는 여러 보안 방화벽으로 분할할 수 있습니다. 각 컨텍스트는 고유한 컨피그레이션 및 정책을 포함하는 독립적인 시스템입니다. 상위 (PIX Firewall, ASA 또는 FWSM)가 Security Manager에서 관리되지 않는 경우에도 Security Manager에서 이러한 독립형 컨텍스트를 관리할 수 있습니다. **참고:** 이 필드는 Device 선택기에서 선택한 디바이스가 보안 컨텍스트를 지원하는 PIX Firewall, ASA 또는 FWSM과 같은 방화벽 디바이스인 경우에만 활성화됩니다.
- IPS Manager에서** Cisco IOS 라우터를 관리하려면 Manage in IPS Manager 확인란을 선택합니다. 이 필드는 Device(디바이스) 선택기에서 Cisco IOS 라우터를 선택한 경우에만 활성화됩니다. **참고:** IPS Manager는 IPS 기능이 있는 Cisco IOS 라우터에서만 IPS 기능을 관리할 수 있습니다. 자세한 내용은 IPS 설명서를 참조하십시오. Manage in IPS Manager(IPS Manager에서 관리) 확인란을 선택한 경우 Manage in Cisco Security Manager(Cisco Security Manager에서 관리) 확인란도 선택해야 합니다. 선택한 디바이스가 IDS인 경우 이 필드는 활성 상태가 아닙니다. 그러나 IPS Manager가 IDS 센서를 관리하기 때문에 확인란이 선택됩니다. 선택한 디바이스가 PIX Firewall, ASA 또는 FWSM인 경우 IPS Manager에서 이러한 디바이스 유형을 관리하지 않으므로 이 필드가 활성화되지 않습니다.
- 마침**을 클릭합니다. 시스템은 디바이스 검증 작업을 수행합니다. 입력한 데이터가 올바르지 않으면 오류 메시지가 생성되고 오류가 발생한 페이지가 표시됩니다. 입력한 데이터가 올바르면 디바이스가 인벤토리에 추가되고 디바이스 선택기에 표시됩니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결할 수 있습니다.

오류 메시지

CSM에 IPS를 추가하면 Invalid device(): 오류 메시지 SysObjId .

솔루션

이 오류 메시지를 해결하려면 다음 단계를 완료하십시오.

- Windows에서 CSM 데몬 서비스를 중지한 다음 **Program Files(프로그램 파일) > CSCOPx > MDC > athena > config > Directory**(여기서 VMS-SysObjID.xml을 찾을 수 있음)를 선택합니다.
- CSM 시스템에서 기본적으로 C:\Program Files\CSCOPx\MDC\athena\config\directory에 있는 원래 VMS-SysObjID.xml 파일을 최신 VMS-SysObjID.xml 파일로 바꿉니다.
- CSM 데몬 관리자 서비스(CRMDmgtd)를 다시 시작하고 영향받는 디바이스를 다시 추가하거나 검색합니다.

관련 정보

- [Cisco Security Manager 지원 페이지](#)
- [Cisco Intrusion Detection System 지원 페이지](#)
- [기술 지원 및 문서 - Cisco Systems](#)