Cisco IOS IPS 컨피그레이션의 CiscoWorks IPS MC 예

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[표기 규칙](#)
[구성](#)
[구성 작업에 대한 기본 이해](#)
[Cisco IOS IPS 라우터의 초기 컨피그레이션](#)
[Cisco IOS IPS 라우터를 IPS MC로 가져오기](#)
[사전 조정된 서명 파일을 사용하도록 Cisco IOS IPS 라우터 구성](#)
[사전 조정된 SDF 서명 수정](#)
[사용자 지정 서명 선택](#)
[인터페이스에 적용할 규칙 만들기](#)
[구성 구축](#)
[서명 업데이트 자동 다운로드](#)
[새 SDF 파일로 Cisco IOS IPS 라우터 업데이트](#)
[관련 정보](#)

소개

CiscoWorks Management Center for IPS Sensors(IPS MC)는 Cisco IPS 장치의 관리 콘솔입니다. IPS MC 버전 2.2는 Cisco IOS® 소프트웨어 라우터에서 IPS(Intrusion Prevention System) 기능 프로비저닝을 지원합니다. 이 문서에서는 IPS MC 2.2를 사용하여 Cisco IOS IPS를 구성하는 방법에 대해 설명합니다.

IPS MC 사용 방법(Cisco IOS 소프트웨어를 기반으로 하지 않는 장치를 구성하는 데 사용하는 방법 포함)에 대한 자세한 내용은 다음 URL에서 CiscoWorks Management Center for IPS Sensors 설명서를 참조하십시오.

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/index.html

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 CiscoWorks Management Center for IPS Sensor(IPS MC) 버전 2.2를 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.

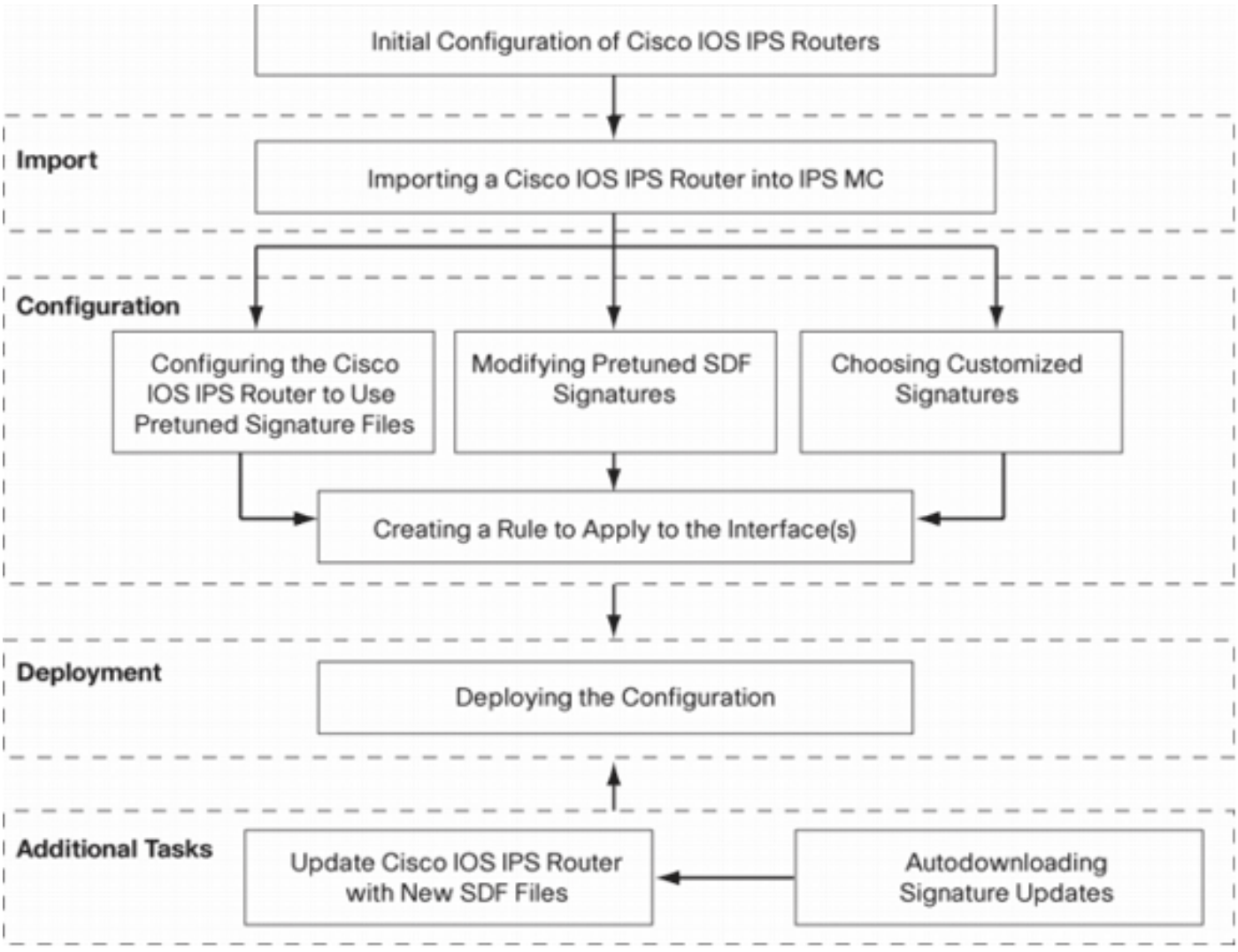
표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

구성

구성 작업에 대한 기본 이해

IPS MC는 Cisco IOS IPS 라우터 그룹의 컨피그레이션을 관리하는 데 사용됩니다. IPS MC는 IPS를 실행하는 라우터의 알림을 관리하지 않습니다. Cisco는 IPS 모니터링을 위해 Cisco Security Monitoring, Analysis and Response System(Cisco Security MARS)을 권장합니다. 구성 관리는 이 문서에 설명된 일련의 작업으로 구성됩니다. 이러한 작업은 다음 세 단계로 나눌 수 있습니다. 이 이미지에 표시된 대로 가져오기, 구성 및 구축



각 단계에는 고유한 책임 및 기능 집합이 있습니다.

- *Import(*가져오기) - 라우터를 IPS MC로 가져옵니다. IPS MC를 사용하여 구성하려면 먼저 라우터를 IPS MC로 가져와야 합니다. 라우터에 초기 IPS 컨피그레이션이 있지 않으면 라우터를 가져올 수 없습니다(자세한 내용은 이 문서의 뒷부분에 나와 있음).
- *Configuration*(컨피그레이션) - 디바이스를 구성합니다. 예를 들어 Cisco 권장 사전 조정 서명 파일 중 하나를 사용하도록 Cisco IOS IPS 라우터를 구성할 수 있습니다. 컨피그레이션 변경 사항은 IPS MC에 저장되지만 이 단계에서는 라우터로 전송되지 않습니다.
- *Deployment*(구축) - 실제 디바이스에 컨피그레이션 변경 사항을 전달합니다. 이 단계에서는 구성 작업의 변경 사항을 라우터에 커밋합니다.
- *추가 작업*—IPS MC는 Cisco.com에서 서명 업데이트를 자동으로 다운로드하는 자동 다운로드 기능을 제공합니다.

IPS MC를 효과적으로 사용하려면 이러한 단계별 접근 방식을 이해해야 합니다. Cisco 라우터 및 SDM(Security Device Manager)과 같은 디바이스 기반 관리 GUI와는 다릅니다. 디바이스 기반 GUI는 단일 라우터에서 직접 작동하는 반면 IPS MC는 네트워크 전반에 걸쳐 라우터 그룹(및 Cisco IPS 4200 Series Sensors와 같은 기타 IPS 장치에서 작동하도록 설계되었습니다.

이 문서에서는 IPS MC를 사용하여 Cisco IOS IPS 라우터를 관리하는 데 도움이 되는 다이어그램의 각 작업에 대한 정보를 제공합니다.

Cisco IOS IPS 라우터의 초기 컨피그레이션

Cisco IOS IPS 라우터를 IPS MC에 성공적으로 가져오거나 추가하려면 Cisco IOS IPS 라우터에서 특정 초기 컨피그레이션 단계를 수행해야 합니다. 이 섹션에서는 이러한 단계를 설명합니다.

Cisco IPS MC를 통한 구성, 가져오기 및 구축을 위해 Cisco IOS IPS 라우터에서 SSH(Secure Shell) 프로토콜을 활성화해야 합니다. 또한 이벤트 보고를 위해 SDEE(Security Device Event Exchange) 프로토콜을 활성화해야 합니다(IPS MC는 프로비저닝에만 사용되므로 IPS MC로 전송되지는 않지만 보고에는 사용되지 않음). 마지막으로, IPS 라우터의 클럭 설정이 IPS MC와 동기화되었는지 확인해야 합니다.

IOS IPS 라우터를 구성하려면 다음 단계를 완료하십시오.

1. 라우터의 로컬 사용자 이름과 비밀번호를 생성합니다.
   ```
   Router#config terminal
   Router(config)#username <username> password <password>
   ```

2. vty 라인 인터페이스에서 로컬 로그인을 활성화합니다.
   ```
   Router#config terminal
   Router(config)#line vty 0 15
   Router(config-line)#login local
   Router(config-line)#exit
   ```

   전송 입력 또는 전송 출력 CLI(Command-Line Interface)가 vty 라인 컨피그레이션에서 구성된 경우 SSH가 활성화되어 있는지 확인합니다. 예를 들면 다음과 같습니다.
   ```
   Router#conf terminal
   Router(config)#line vty 0 15
   Router(config-line)#transport input ssh telnet
   Router(config-line)#exit
   ```

3. 1024비트 RSA 키를 생성합니다(키가 없는 경우).SSH는 암호화 키 생성 후 자동으로 활성화됩니다.

```
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#crypto key generate rsa
The name for the keys will be: Router.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys.
    Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Router(config)#
*Jan 23 00:44:40.952: %SSH-5-ENABLED: SSH 1.99 has been enabled
Router config)#
```

4. 라우터에서 SDEE를 활성화합니다.

```
Router(config)#ip ips notify sdee
```

5. HTTPS를 활성화합니다.IPS MC가 이벤트 정보를 수집하기 위해 SDEE와 라우터와 통신하려면 HTTP 또는 HTTPS가 필요합니다.

```
Router(config)#ip http authentication local
Router(config)#ip http secure-server
```

6. IPS 라우터에서 클럭 설정을 구성하려면 외부 NTP(Network Time Protocol) 서버 또는 clock 명령을 사용합니다.

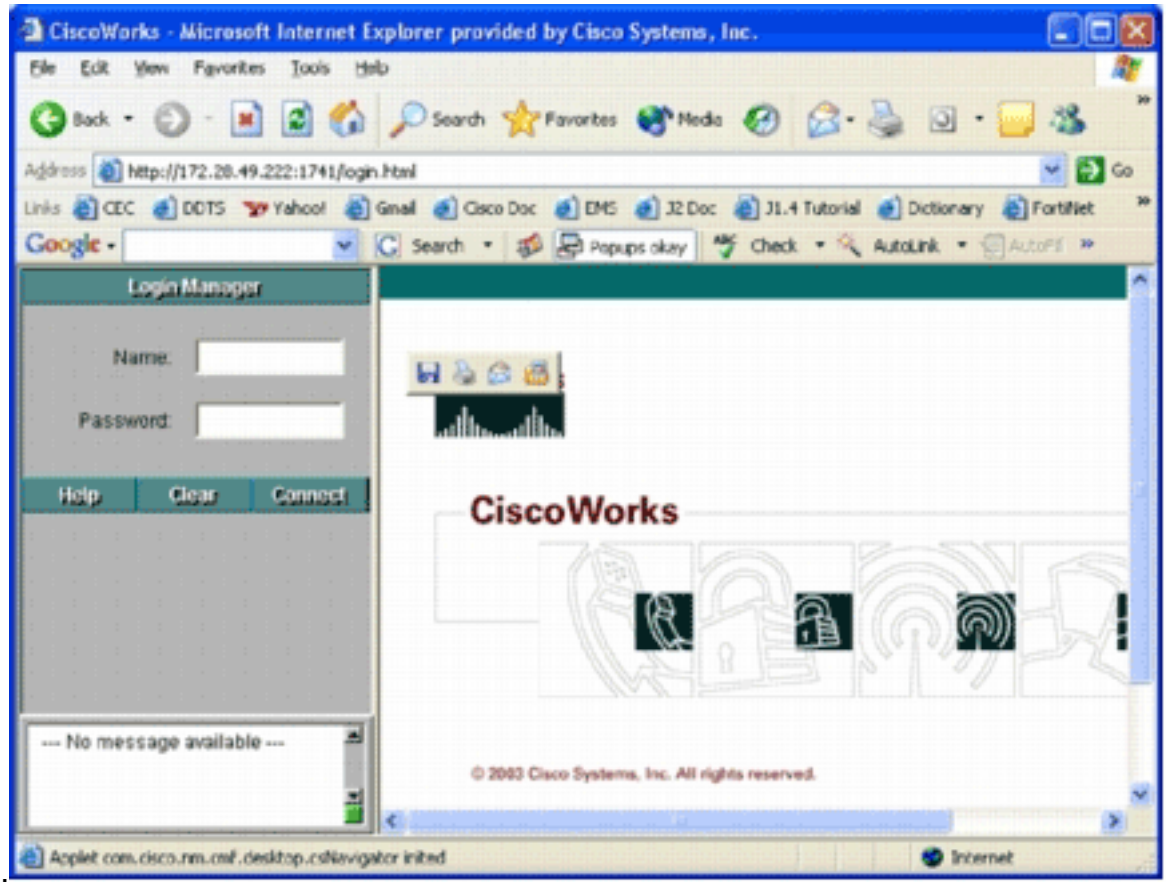
```
Router(config)#clock set hh:mm:ss day month year
```

이제 Cisco IOS IPS 라우터가 준비되었으며 추가 구성 및 관리를 위해 IPS MC로 가져올 수 있습니다.

Cisco IOS IPS 라우터를 IPS MC로 가져오기

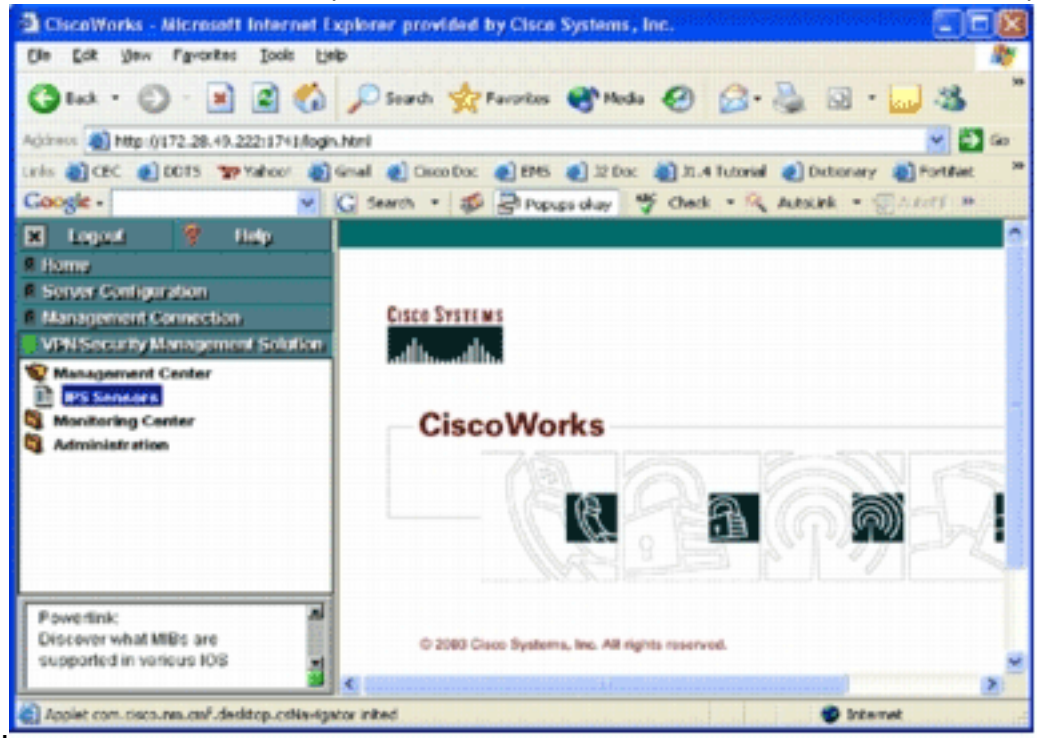
라우터에서 초기 컨피그레이션을 완료하면 IPS MC에 추가하거나 가져올 수 있습니다.

1. 웹 브라우저를 시작하고 CiscoWorks 서버를 가리킵니다.CiscoWorks 로그인 관리자가 나타납



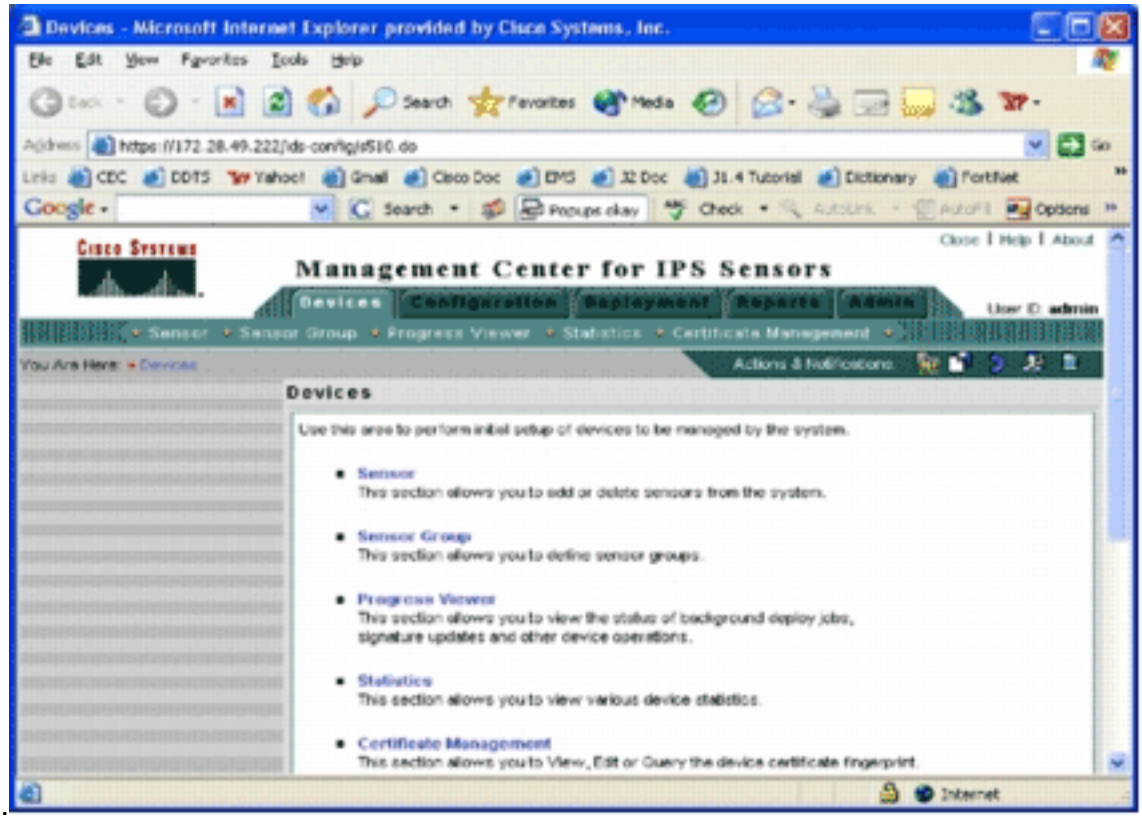
니다. **참고:** 웹 서버의 기본 포트 번호는 1741입니다. 따라서 http://<*server ip address*>:1741/와 유사한 URL을 사용해야 합니다.

2. 로그인하려면 사용자 이름과 암호를 입력하십시오.CiscoWorks 기본 페이지가 나타납니다



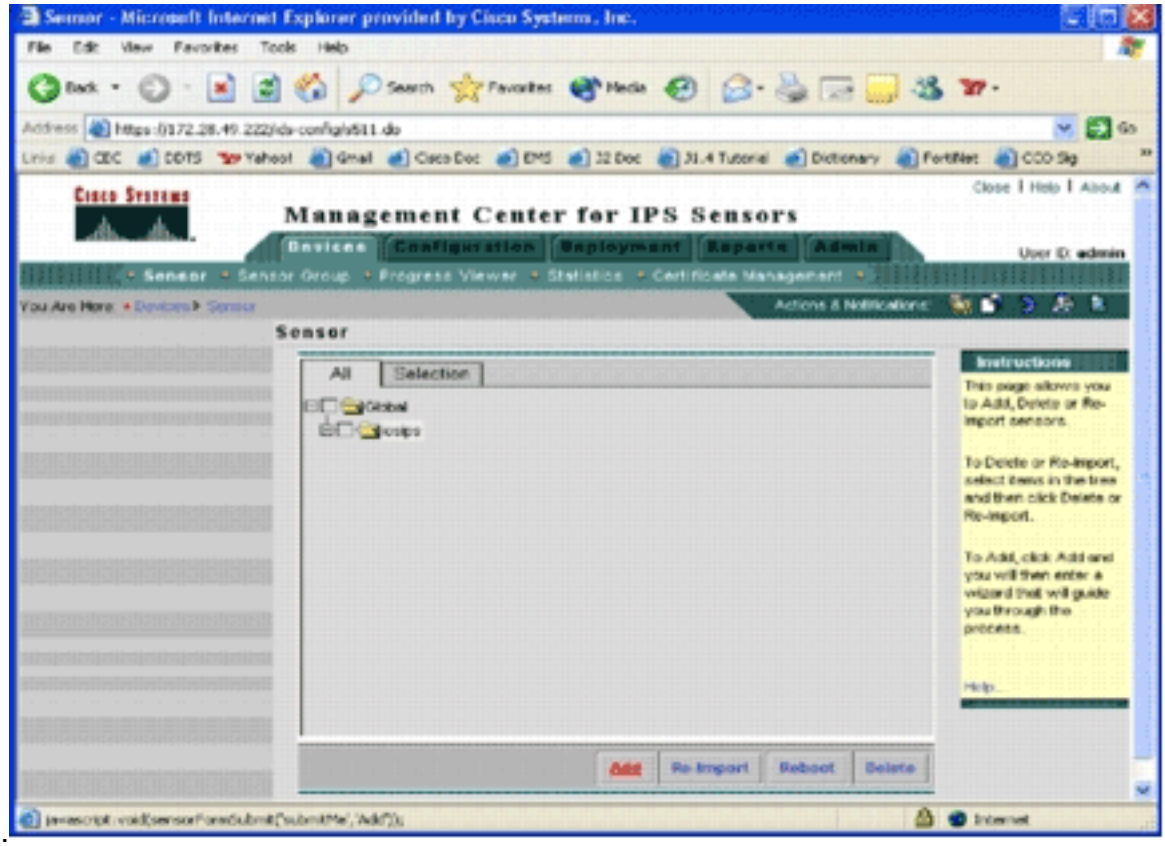
.

3. 왼쪽 탐색 창에서 **VPN/Security Management Solution(VPN/보안 관리 솔루션)**을 선택한 다음 **Management Center(관리 센터)**를 선택합니다.Management Center for IPS Sensors 페이지가 나타납니다

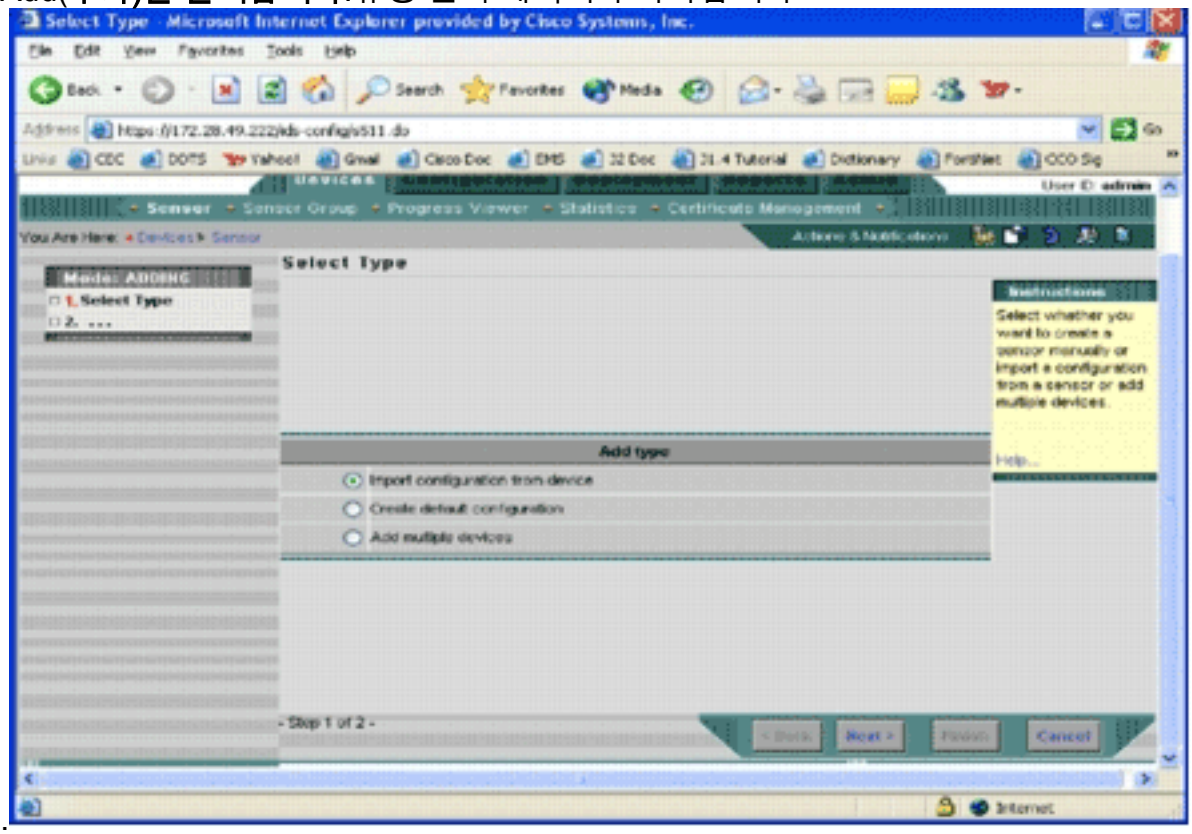


이 페이지에는 다음 5개의 탭이 표시됩니다.*Devices*(디바이스) - Devices(디바이스) 탭에서 시스템의 모든 디바이스를 초기 설정하고 관리할 수 있습니다.*구성* - 구성 탭에서 프로비저닝 기능을 수행할 수 있습니다. 개별 디바이스 레벨 또는 그룹 레벨에서 디바이스를 구성할 수 있습니다. 하나의 장치 그룹은 여러 장치를 포함할 수 있습니다. 구성 작업을 통해 변경한 모든 내용을 저장해야 합니다. 컨피그레이션 기능은 즉시 디바이스를 변경하지 않습니다. 변경 사항을 배포하려면 배포 기능을 사용해야 합니다.*Deployment*(구축) - Deployment(구축) 탭에서 디바이스에 컨피그레이션 변경 사항을 구축할 수 있습니다. 일정 기능을 통해 구성 변경 사항을 적용할 시기를 유연하게 제어할 수 있습니다.*보고서* - 보고서 탭에서 다양한 시스템 작업 보고서를 생성할 수 있습니다.*Admin*(관리) - Admin(관리) 탭에서 데이터베이스 관리, 시스템 구성 및 라이센스 관리와 같은 시스템 관리 작업을 수행할 수 있습니다.

4. 새 디바이스를 추가하려면 **Devices** 탭을 클릭합니다.Sensor 페이지가 나타납니다

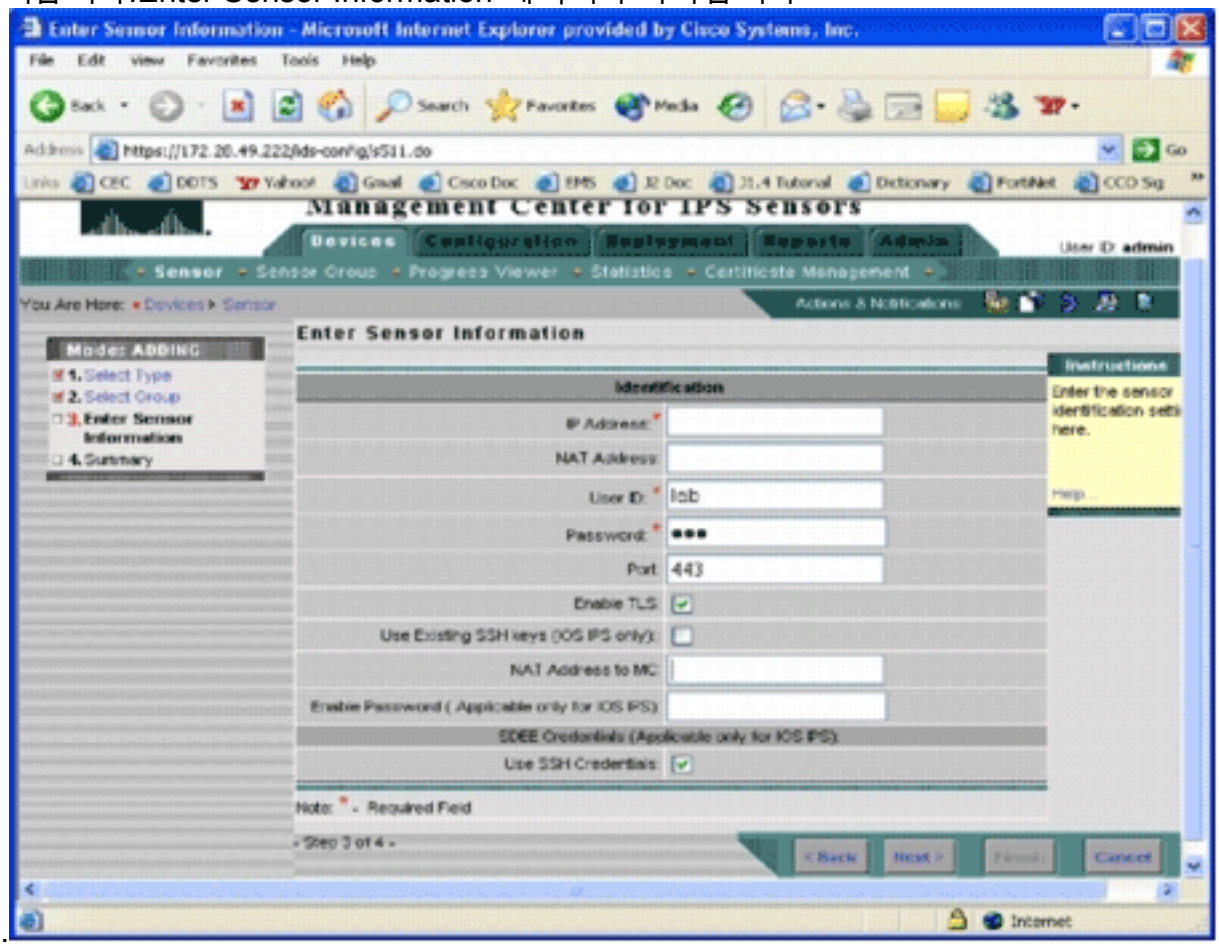


5. Add(**추가)를 클릭합니다**.유형 선택 페이지가 나타납니다



수행할 추가 기능 유형을 IPS MC에 알려야 합니다. 이 목록에서는 각 옵션에 대해 설명합니다.*디바이스에서 컨피그레이션 가져오기* - 이 옵션을 사용하여 네트워크에서 현재 실행 중인 IPS MC 디바이스에 추가합니다.*Create default configuration(기본 컨피그레이션 생성)* - 이 옵션을 사용하여 현재 네트워크에서 실행되지 않는 디바이스를 추가합니다.*여러 디바이스 추가* - 이 옵션을 사용하여 여러 디바이스를 추가합니다. 모든 디바이스 정보가 포함된 .csv 또는 .xml 파일을 생성한 다음 IPS MC로 가져와 한 번에 디바이스를 추가할 수 있습니다.**팁:** 샘플 .csv 형식 및 .xml 형식 파일은 다음 위치에 있습니다. InstallDirectory\MDC\etc\ids\ and are named MultipleAddDevices-format.csv 및 MultipleAddDevices-format.xml을 각각 사용합니다.

6. 적절한 Add type(유형 추가) 옵션을 선택하고 Next(**다음**)를 클릭합니다.
7. Cisco IOS IPS 라우터를 추가할 그룹을 선택하거나 기본 전역 그룹을 사용한 다음 **Next**를 클릭합니다.Enter Sensor Information 페이지가 나타납니다



8. Identification(식별) 페이지에서 디바이스의 식별 정보를 입력합니다.**참고:** 사용자에게 권한 레벨 15 액세스 권한이 없는 경우 enable 비밀번호를 제공해야 합니다. Identification 페이지의 마지막 행에서 Use SSH **Credentials(SSH 자격 증명 사용**) 확인란을 선택합니다.
9. Next(**다음)를 클릭합니다**.Add Sensor Summary(센서 요약 추가)가 나타납니다.
10. **마침**을 **클릭합니다**.디바이스가 IPS MC에 성공적으로 추가되었습니다.**참고:** 임포트 프로세스 중에 오류가 발생한 경우 다음 항목을 확인해야 합니다.*전제 조건 컨피그레이션* - IPS MC가 Cisco IOS IPS 라우터와 통신하려면 이러한 컨피그레이션이 필요합니다 .*Connectivity*(연결) - IPS MC가 Cisco IOS IPS 라우터에 도달할 수 있는지 확인합니다 .*Clock*(시계) - IPS MC 및 Cisco IOS IPS 라우터의 시간을 확인합니다. 시간은 인증에 사용되는 https 인증서의 중요한 구성 요소입니다. 시간은 서로 12시간 이내여야 합니다. (모범 사례는 최대 몇 시간 정도입니다.)*Cisco IOS IPS Certificate(Cisco IOS IPS 인증서*) - 저장된 Cisco IOS IPS 인증서가 잘못된 경우가 있습니다. Cisco IOS IPS에서 인증서를 삭제하려면 Cisco IOS IPS 라우터에서 신뢰 지점을 제거해야 합니다.*Additional Configuration*(추가 컨피그레이션) - **ip http** timeout-**policy**가 **낮은 수의 최대 요청**(예: **ip http timeout-policy idle 600 life 86400 요청 1)으로 구성된** 경우 최대 요청 수를 늘려야 합니다. 예를 들면 다음과 같습니다. **ip http timeout-policy idle 600 life 86400 요청 8400**

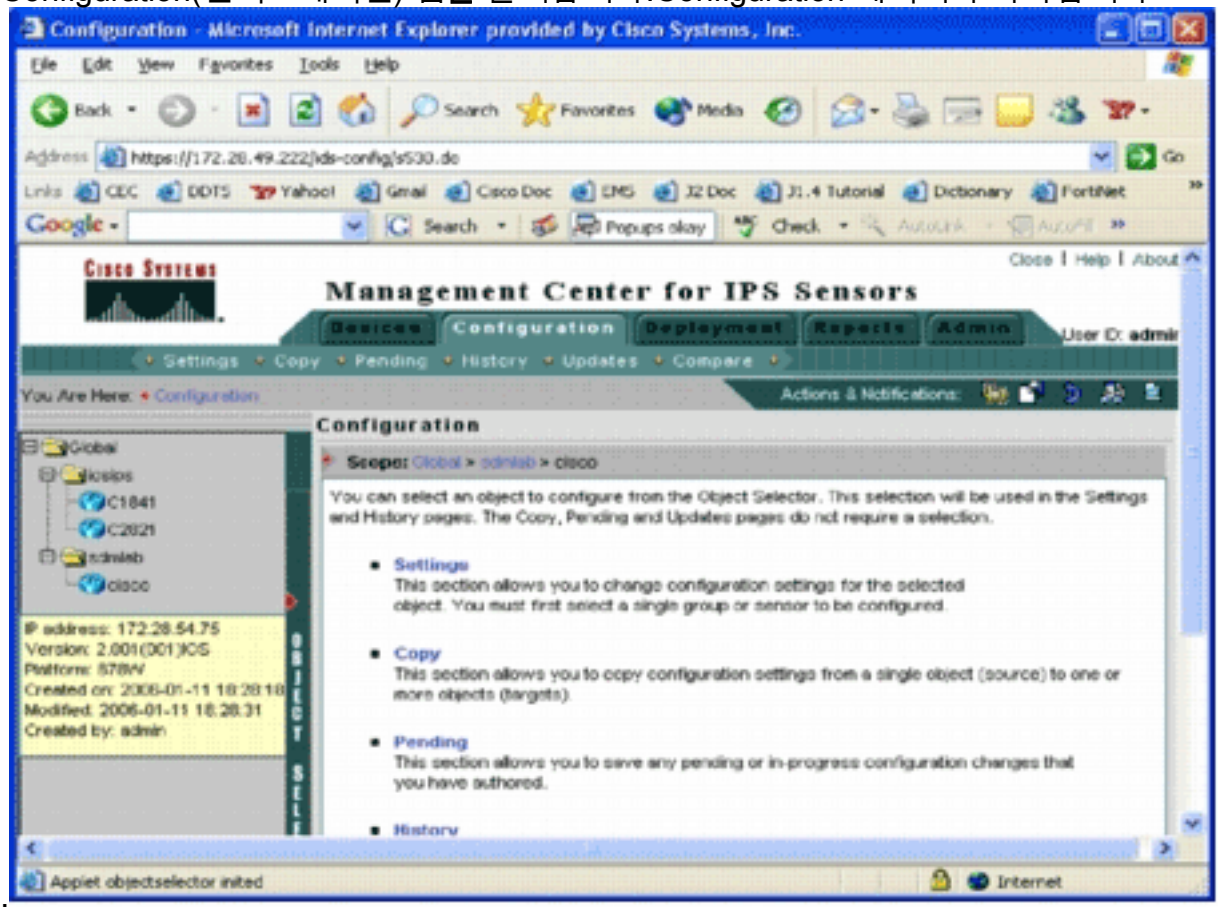
사전 조정된 서명 파일을 사용하도록 Cisco IOS IPS 라우터 구성

라우터를 IPS MC로 가져온 후 SDF(Signature Definition File)(IPS 라우터에서 사용할 위협 시그니처를 포함하는 텍스트 기반 파일) 및 각 서명이 트리거될 때 수행할 작업(예: 삭제, TCP 재설정, 경보)을 선택해야 합니다.

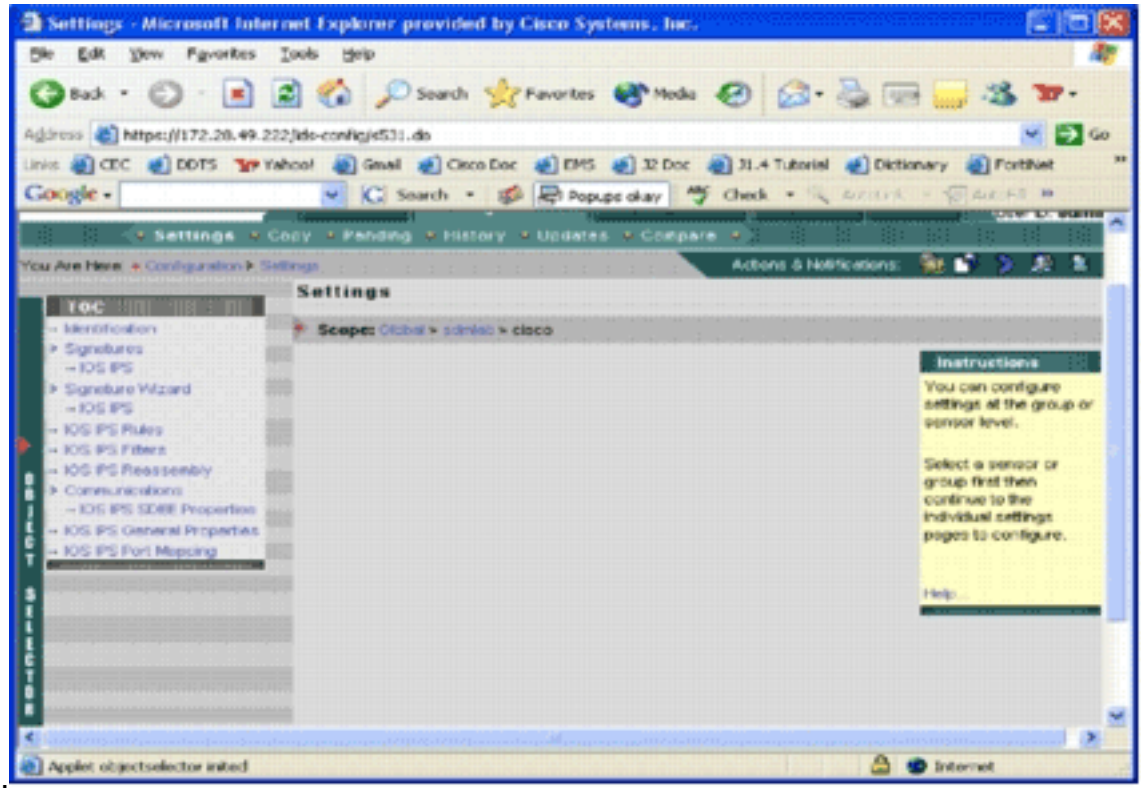
Cisco Systems®는 Cisco 사전 조정된 SDF 파일을 사용할 것을 권장합니다. 현재 세 개의 파일이 있습니다. attack-drop.sdf, 128MB.sdf 및 256MB.sdf IPS MC는 Cisco.com에서 이러한 파일을 자동으로 다운로드할 수 있습니다. 자세한 내용은 서명 업데이트 자동 다운로드를 참조하십시오.

이 절차에서는 단일 디바이스를 예로 사용하며 IPS 컨피그레이션이 없는 라우터로 시작합니다. 그룹 레벨의 여러 디바이스에 대해서도 이 절차를 사용할 수 있습니다.

1. Configuration(컨피그레이션) 탭을 클릭합니다.Configuration 페이지가 나타납니다

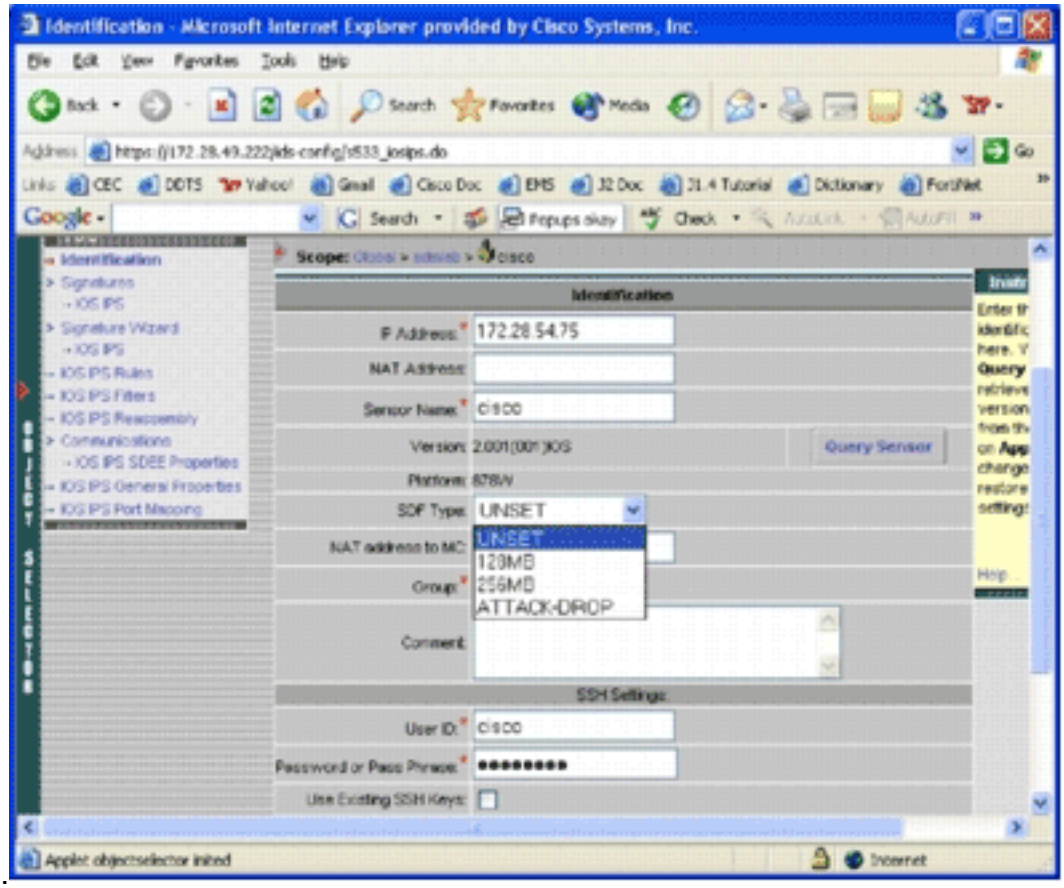


2. 페이지 왼쪽에 있는 Object Selector에서 구성할 Cisco IOS IPS 라우터를 선택합니다.**참고:** IPS MC 2.2의 대부분의 컨피그레이션 설정은 그룹 레벨과 개별 디바이스 레벨에서 구성할 수 있습니다. 예를 들어 전역, ipops 및 sdmlab 그룹은 모두 구성 가능한 객체 그룹입니다. 이 예에서는 sdmlab 그룹의 개별 device-cisco를 사용합니다.구성할 라우터를 선택하면 Configuration(컨피그레이션) 페이지 상단에 있는 경로 표시줄에 현재 컨피그레이션 범위가 표시됩니다. 예를 들어 이 예제의 범위는 *Global > sdmlab > cisco입니다*. *cisco*는 현재 구성 객체(즉, 객체 선택기에서 선택된 라우터)입니다.
3. 구성 메뉴 모음에서 **설정**을 클릭합니다.Settings 페이지가 나타납니다



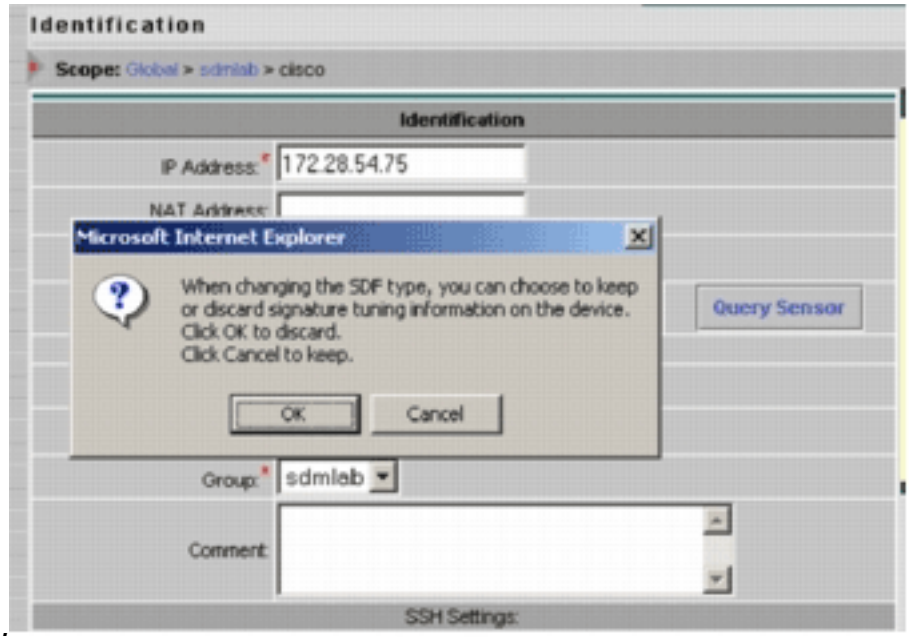
설정 페이지에서 선택한 객체의 구성 설정을 변경할 수 있습니다. Cisco IOS IPS 라우터별 컨피그레이션 설정은 페이지 왼쪽에 있는 TOC 섹션에 있습니다. 목차 섹션에서 사용할 수 있는 작업 목록은 다음과 같습니다. *식별* - Cisco IOS IPS 라우터 기본 정보 여기에 미리 조정된 SDF 파일을 지정할 수 있습니다.*Signature(시그니처)* - Cisco IOS IPS 라우터 서명*Signature Wizard*(시그니처 마법사) - 사용자 지정 서명을 추가하기 위한 서명 마법사*Cisco IOS IPS Rules* - 인터페이스에 적용하는 데 사용되는 Cisco IOS IPS 규칙을 구성합니다.*Cisco IOS IPS Filters*—Cisco IOS IPS 필터*Cisco IOS IPS Reassembly*—인터페이스 IP 가상 리어셈블리 컨피그레이션 *Cisco IOS IPS SDEE 속성* - SDEE 설정을 구성합니다.*Cisco IOS IPS 일반 속성*—추가 Cisco IOS IPS 관련 구성

4. 사전 **조정된** SDF 파일을 구성하려면 Identification(식별)을 선택합니다.Identification 페이지가

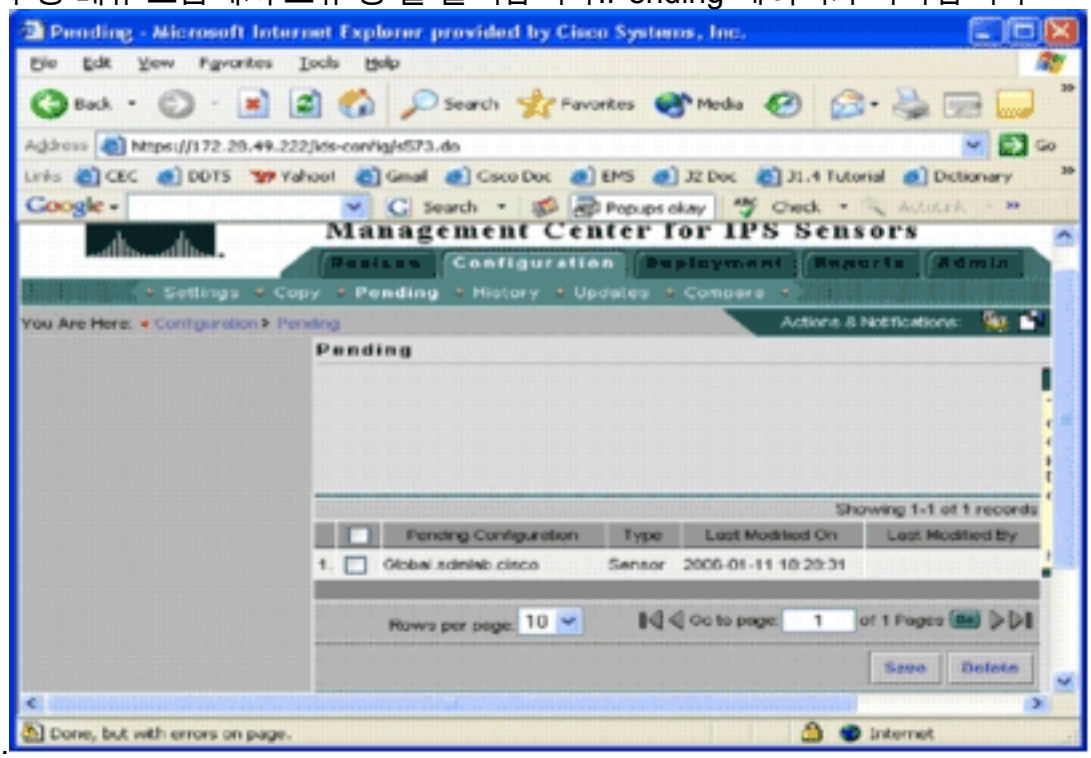


나타납니다.

5. SDF Type(SDF 유형) 드롭다운 목록에서 적절한 사전 조정된 SDF를 선택한 다음 **Apply(적용)**를 클릭하여 변경 사항을 적용합니다.Cisco IOS IPS는 1,600개 이상의 서명을 지원하며, 이는 라우터에서 수용할 수 있는 메모리 용량을 초과합니다. SDF는 가장 중요한 시그니처를 선택하고 로드하는 편리한 방법으로 개발되었습니다. 현재 3개의 SDF 중에서 선택할 수 있습니다. 라우터의 DRAM 용량에 따라 SDF 파일을 선택할 수 있도록 크기 차이가 있습니다. 사용 가능한 선택 사항은 다음과 같습니다.UNSET - SDF 유형이 설정되지 않았습니다.ATTACK-DROP—이 SDF는 64MB의 DRAM을 사용하는 라우터용입니다.256MB—이 SDF는 256MB의 DRAM이 있는 라우터용입니다.128MB—이 SDF는 128MB의 DRAM이 있는 라우터용입니다.**참고:** 128 및 256MB SDF에는 2.001 이상의 엔진이 필요합니다. 이 정보는 Settings(설정) > **Identification UI(식별 UI) > Version(버전)** 필드**에서** 사용할 수 있습니다.**경고:** IPS MC에는 Cisco IOS IPS 라우터의 메모리 관리 기능이 포함되지 않습니다. Cisco IOS IPS 라우터에 대해 SDF 파일을 선택할 때는 주의해야 합니다. Cisco IOS IPS 라우터에 선택한 SDF 파일을 실행할 수 있는 충분한 메모리가 있는지 확인합니다.**참고:** SDF 유형을 변경하면 다음 메시지가 표시될 수 있습니다. *SDF 유형을 변경할 때 디바이스에서 서명 조정 정보를 유지하거나 삭제하도록 선택할 수 있습니다. OK를 클릭하여 취소합니다. 계속하려면 취소를 클릭합니다*



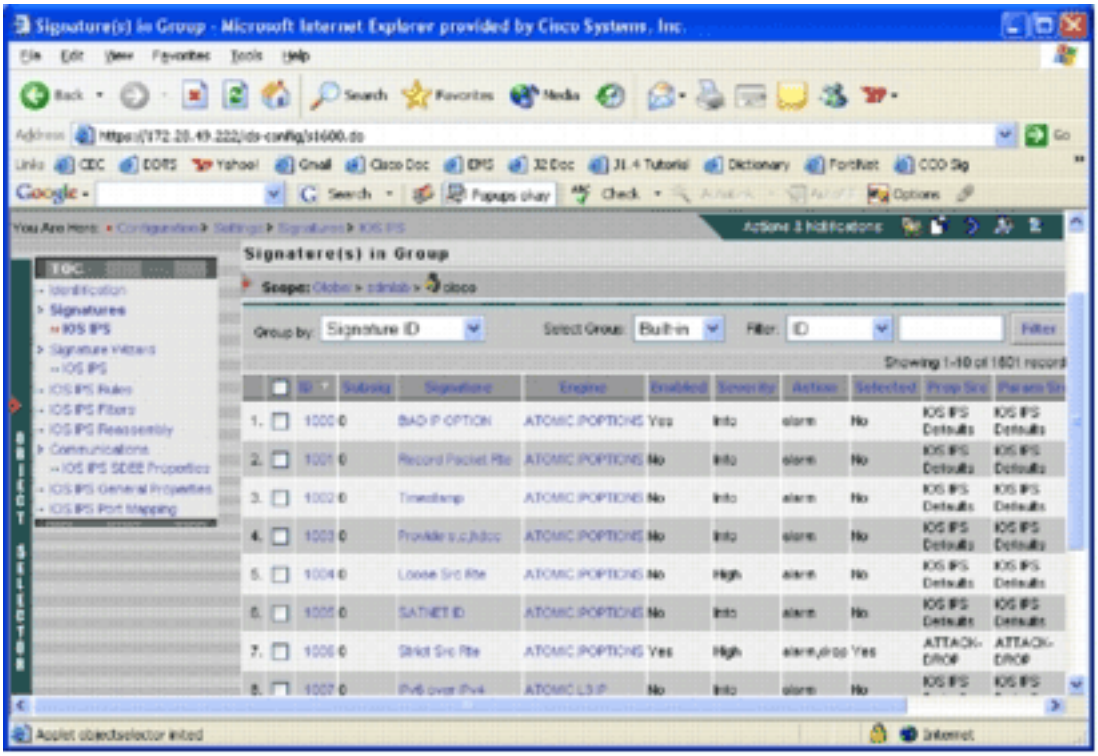
6. 서명 조정 정보를 유지하려면 **취소**를 클릭합니다.라우터-cisco에 대해 사전 조정된 SDF를 성공적으로 선택했으므로 추가 또는 편집과 같은 추가 서명 튜닝을 수행하거나 자체 서명을 생성할 수도 있습니다. 또는 서명 조정 작업을 건너뛰고 직접 인터페이스에 적용할 규칙 생성으로 이동할 수도 있습니다.
7. 구성 메뉴 모음에서 보류 중 을 클릭합니다.Pending 페이지가 나타납니다



이 시점에서 구성 작업이 완료됩니다. 그러나 대상 장치에 변경 사항을 배포하려면 배포 작업을 완료해야 합니다.

사전 조정된 SDF 서명 수정

라우터에 대해 미리 조정된 SDF 파일을 선택한 후 추가 서명 조정 작업을 수행할 수 있습니다. 필요에 맞게 시그니처를 추가, 편집, 삭제 및 수정할 수도 있고, 필요한 경우 자체 서명을 생성할 수도 있습니다. 이 예에서는 IPS MC를 사용하여 시그니처를 추가하고 작업을 수정합니다. 이 그림에서는 시그니처 컨피그레이션 인터페이스를 보여 줍니다.



서명 컨피그레이션을 사용하여 서명 활성화 또는 비활성화, 선택 또는 선택 취소, 서명 추가, 서명 삭제, 서명 작업 변경, 서명 매개변수 수정 등을 수행할 수 있습니다. 왼쪽에 있는 서명 마법사를 사용하여 사용자 지정 서명을 생성합니다.

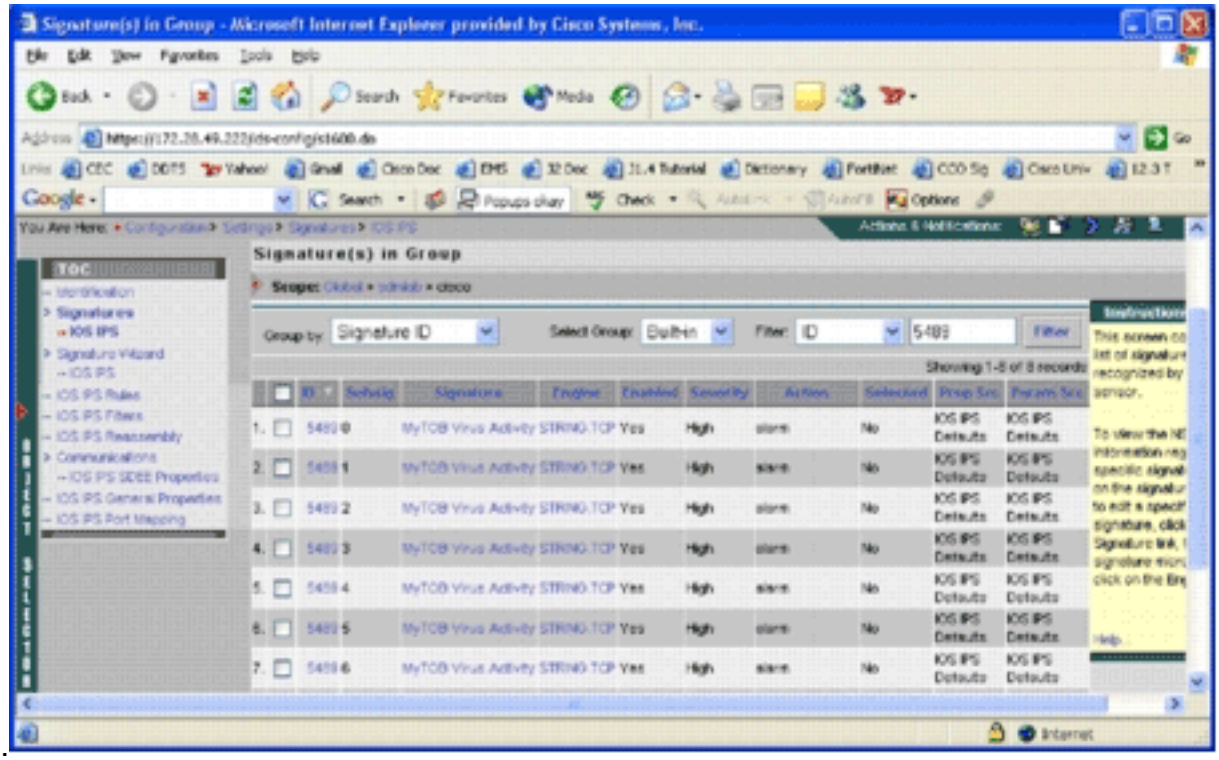
시그니처 컨피그레이션 사용자 인터페이스에서는 기본적으로 일부 정보가 표시됩니다. Selected(선택)는 라우터로 전송되는 SDF 파일에 서명이 포함되는지 여부를 나타냅니다. 서명을 선택하지 않으면 추가되지 않습니다. Enabled(활성화됨)는 서명이 선택된 경우에만 적용됩니다. 서명이 비활성화되면 IPS 엔진은 특정 서명에 대한 이벤트를 보내지 않습니다. 서명을 선택하지 않으면 자동으로 비활성화됩니다.

마지막 두 열(Prop Src 및 Param Src)은 시그니처와 해당 매개 변수가 어디에서 오는지 알려줍니다. 이 서명은 사전 조정된 SDF 파일 또는 공장 기본값에서 가져온 것이며 IOS-Sxxx.zip 파일 업데이트에서 찾을 수 있습니다(IOS IPS 기본값으로 표시됨). 이러한 값은 매개변수 열에도 적용됩니다.

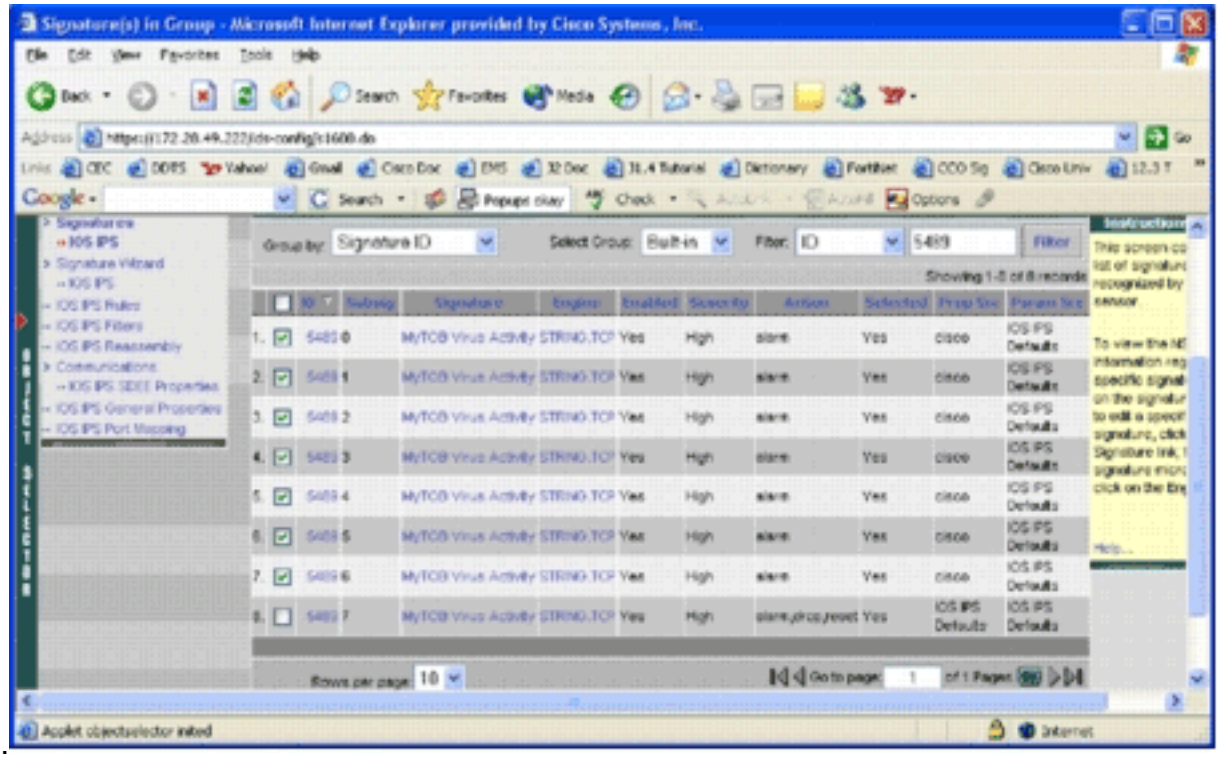
Cisco IOS IPS 라우터에 서명을 추가하는 동안 메모리 고려 사항을 고려해야 합니다. Cisco IOS IPS 라우터가 처리할 수 있는 것보다 더 많은 서명을 추가하면 IPS MC가 디바이스에 컨피그레이션 변경 사항을 구축하지 못합니다.

Cisco IOS IPS 라우터에 서명 5489/x를 추가하려면 다음 단계를 완료하십시오.

1. Configuration(**컨피그레이션**)을 선택한 다음 Object Selector(개체 선택기)를 사용하여 IPS 서명을 구성할 Cisco IOS IPS 라우터를 선택합니다.
2. Configuration **> Settings > Signatures > IOS IPS를 선택합니다**.Signature in Group 페이지가 나타납니다

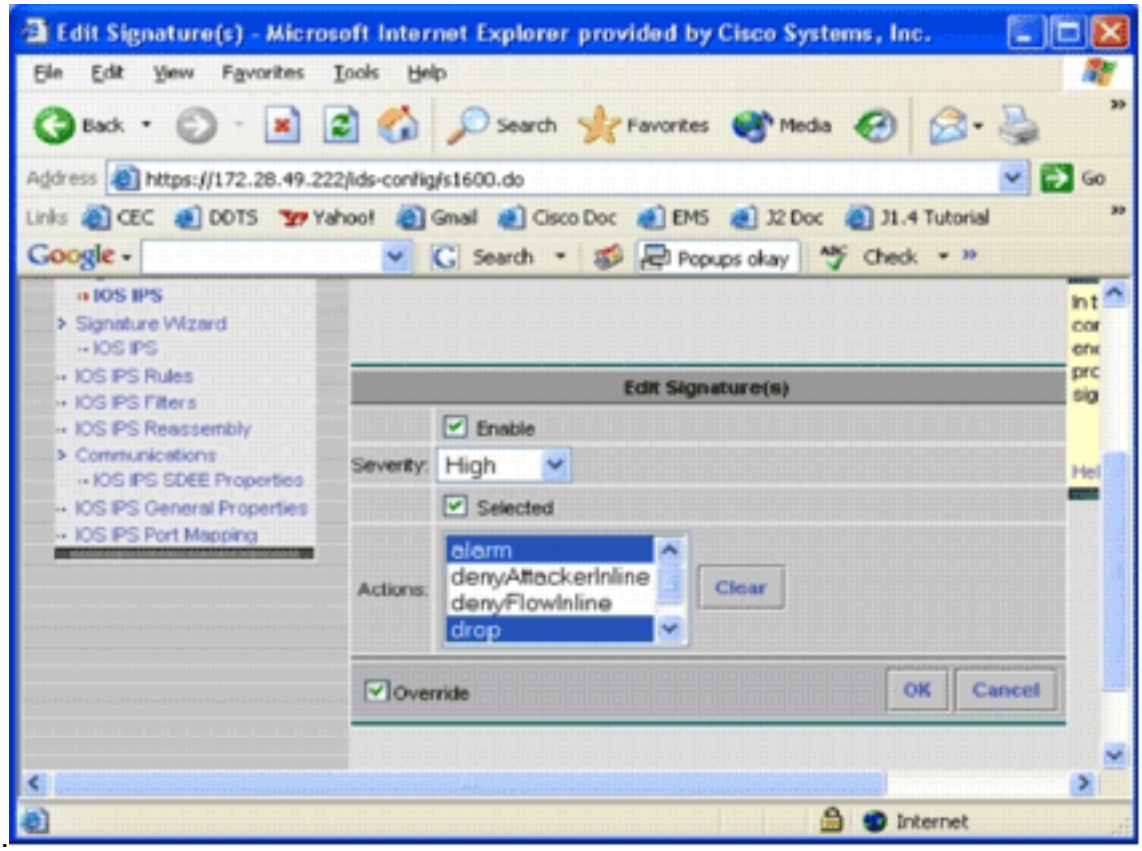


3. 결과를 나타내는 서명 목록에서 Filter by ID(ID로 필터링)를 선택하고 서명 ID 5489를 입력합니다.
4. **Filter**를 클릭하여 시그니처를 검색합니다.검색 결과가 나타납니다

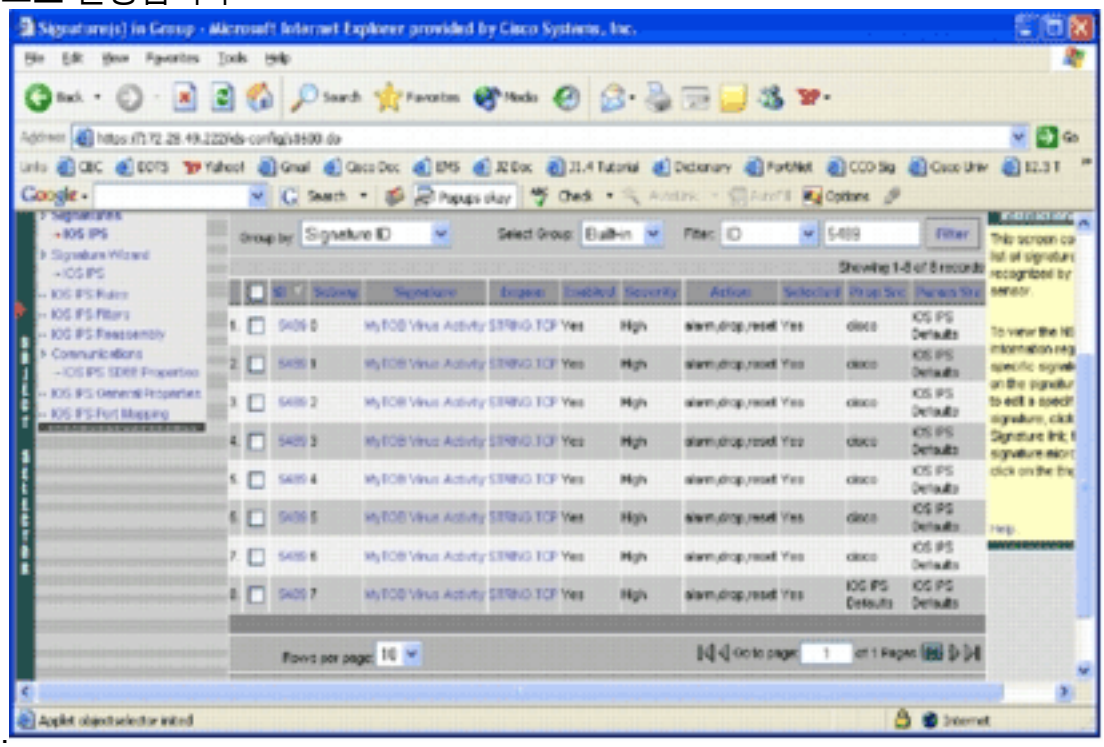


참고: IPS MC는 Cisco SDM에서 사용할 수 있는 새로운 분류를 지원하지 않습니다.

5. 선택되지 않은 서명 옆의 확인란을 선택하고 아래쪽 도구 모음에서 **선택**을 클릭합니다.
6. 서명 작업을 변경하려면 Edit를 클릭합니다.Edit Signature(s) 페이지가 나타납니다



7. Selected(**선택됨**) 확인란을 선택하고 Actions(작업**)** 목록**에서 경보**, **삭제** 및 **재설정**을 선택합니다.
8. Override(재정의**)** 확인란을 선택한 다음 **OK**(확인)를 클릭합니다.모든 시그니처가 원하는 작업으로 변경됩니다



9. Pending(보류 중) 작업으로 이동하여 모든 변경 사항을 저장합니다. 이렇게 하면 구성 작업이 완료됩니다.**팁:** Prop Src 열에 주의하십시오. 수정 후 소스가 *cisco*라는 디바이스로 변경되었으며, 이는 모든 튜닝 정보가 기본 사전 조정된 SDF 파일과 별도로 저장됨을 의미합니다. 이 메커니즘을 통해 IPS MC는 사용자 지정 서명 변경 사항을 유지할 수 있습니다.

이전 섹션에서 SDF 파일 유형을 변경할 때 IPS MC에서 서명 조정 정보를 유지할 것인지 묻습니다. 참조되는 서명 조정 정보입니다.

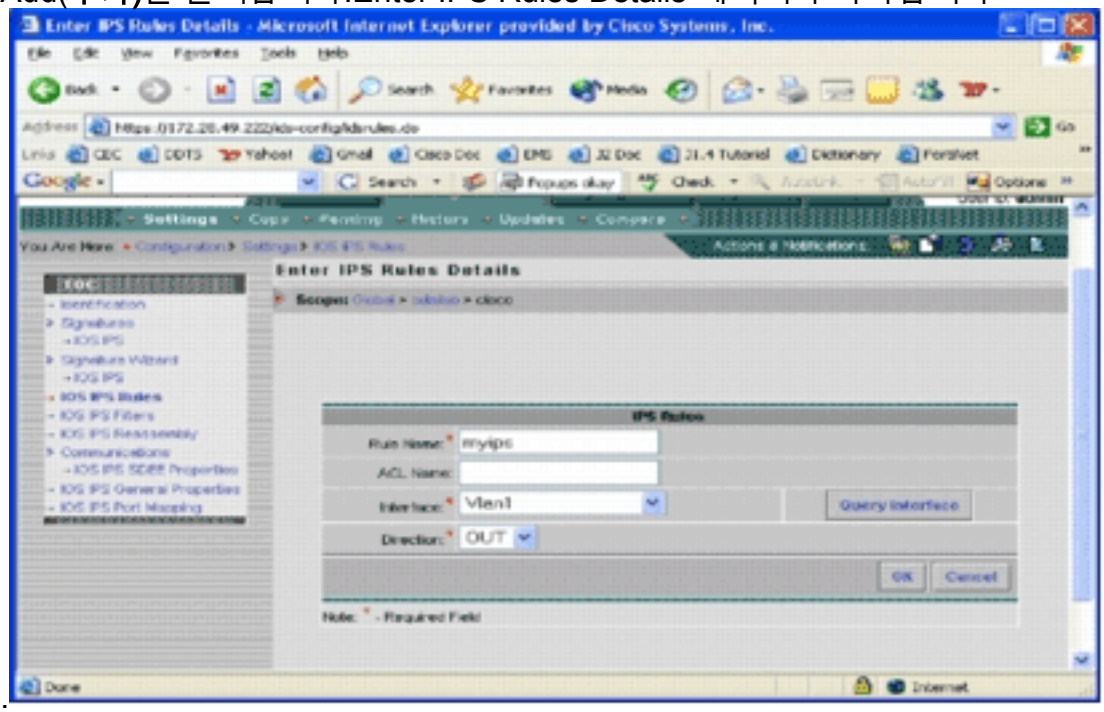
사용자 지정 서명 선택

기본 사전 조정된 SDF 파일을 사용하지 않으려면 디바이스에 대한 튜닝 시그니처를 선택하기 위해 Modify Pretended SDF Signatures 섹션에 지정된 단계를 사용할 수 있습니다. 식별 페이지에서 SDF 유형이 UNSET인지 확인해야 합니다. Configure the Cisco IOS IPS Router to use Pretuned Signature Files(사전 조정된 서명 파일을 사용하도록 Cisco IOS IPS 라우터 구성)의 3단계를 참조하십시오.

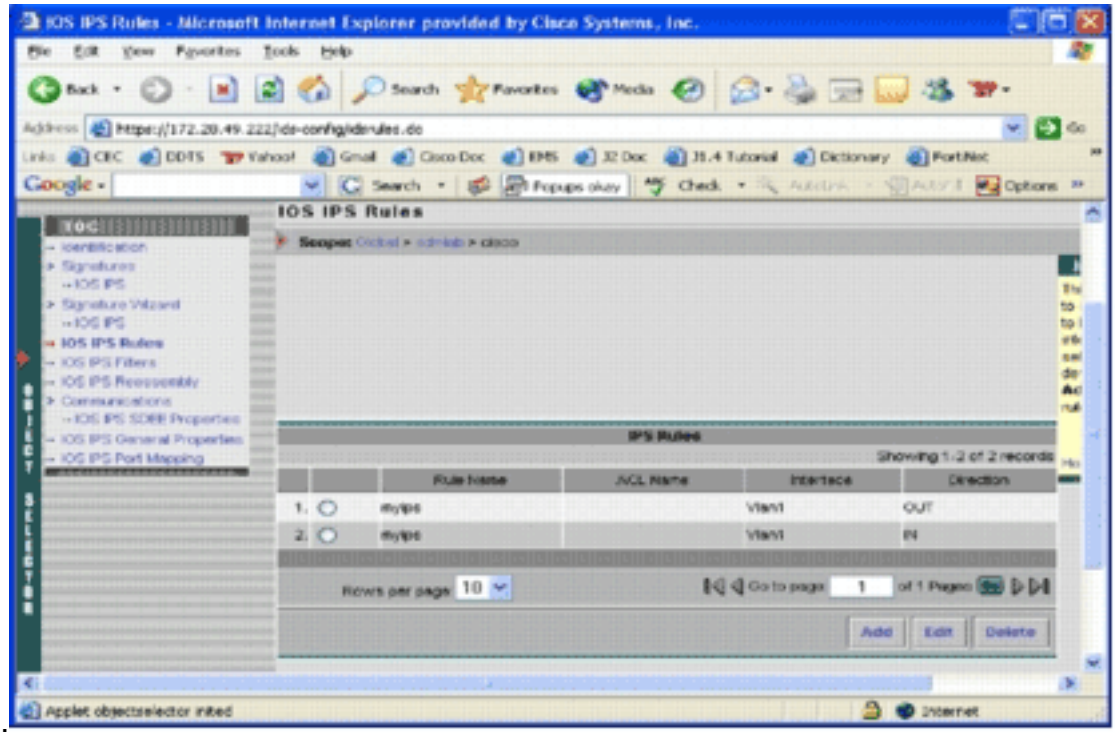
인터페이스에 적용할 규칙 만들기

서명을 튜닝한 후 Cisco IOS 라우터에서 IPS를 활성화해야 합니다. 라우터에서 IPS를 활성화하려면 IPS 규칙을 생성하여 하나 이상의 인터페이스에 적용해야 합니다.

1. Configuration을 선택한 다음 Object Selector를 사용하여 구성할 Cisco IOS IPS 라우터를 선택합니다. 경로 표시줄에서 범위가 그룹 수준이 아니라 장치 수준에 있는지 확인합니다.
2. Configuration(**컨피그레이션**) > **Settings(설정)** > **IOS IPS Rules(IOS IPS 규칙)**를 선택한 다음 Add(**추가**)를 클릭합니다.Enter IPS Rules Details 페이지가 나타납니다



3. 규칙 및 방향을 적용할 규칙 이름 및 인터페이스에 대한 정보를 입력합니다.
4. **확인**을 **클릭합니다**.IOS IPS Rules 페이지가 나타납니다



마찬가지로 인터페이스에 대한 양방향의 규칙을 생성할 수 있습니다.

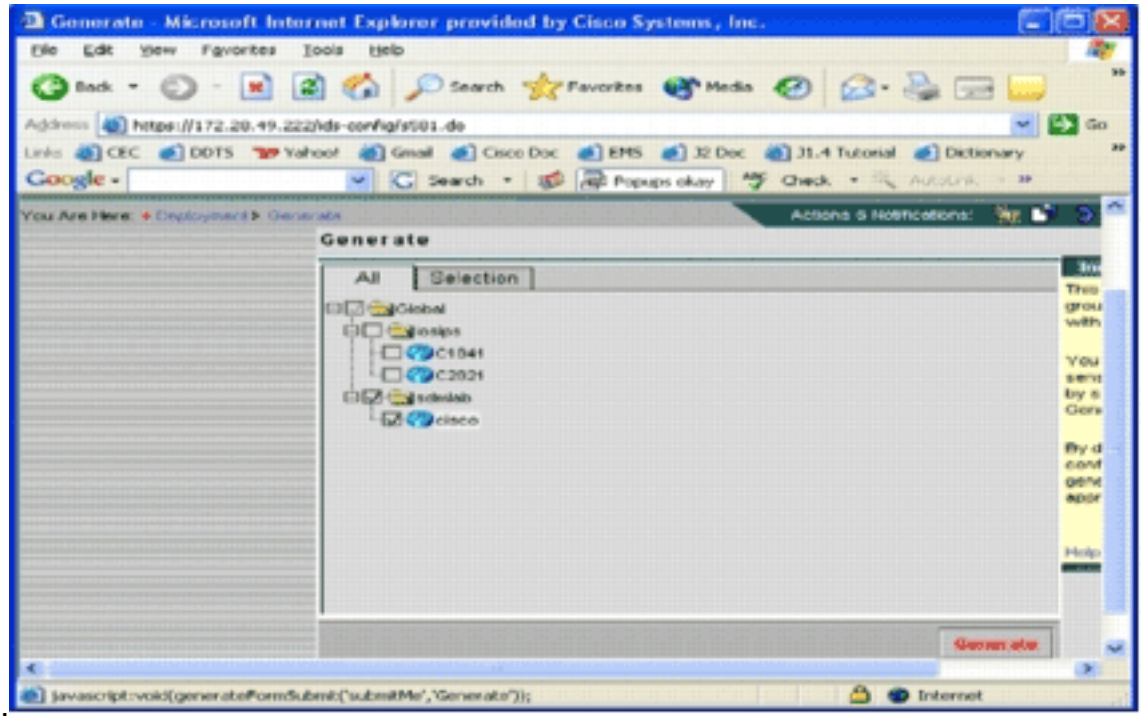
5. 컨피그레이션 변경 사항을 저장하고 구축 프로세스를 통해 영향을 받는 디바이스 또는 디바이스 그룹에 변경 사항을 전달해야 합니다.다른 IPS 관련 컨피그레이션도 수행할 수 있지만 다른 모든 작업은 선택 사항이며 필요하지 않습니다. 컨피그레이션 사용자 인터페이스 왼쪽에 있는 모든 옵션을 찾을 수 있습니다. 이 문서에서는 선택적 구성 옵션을 다루지 않습니다.

구성 구축

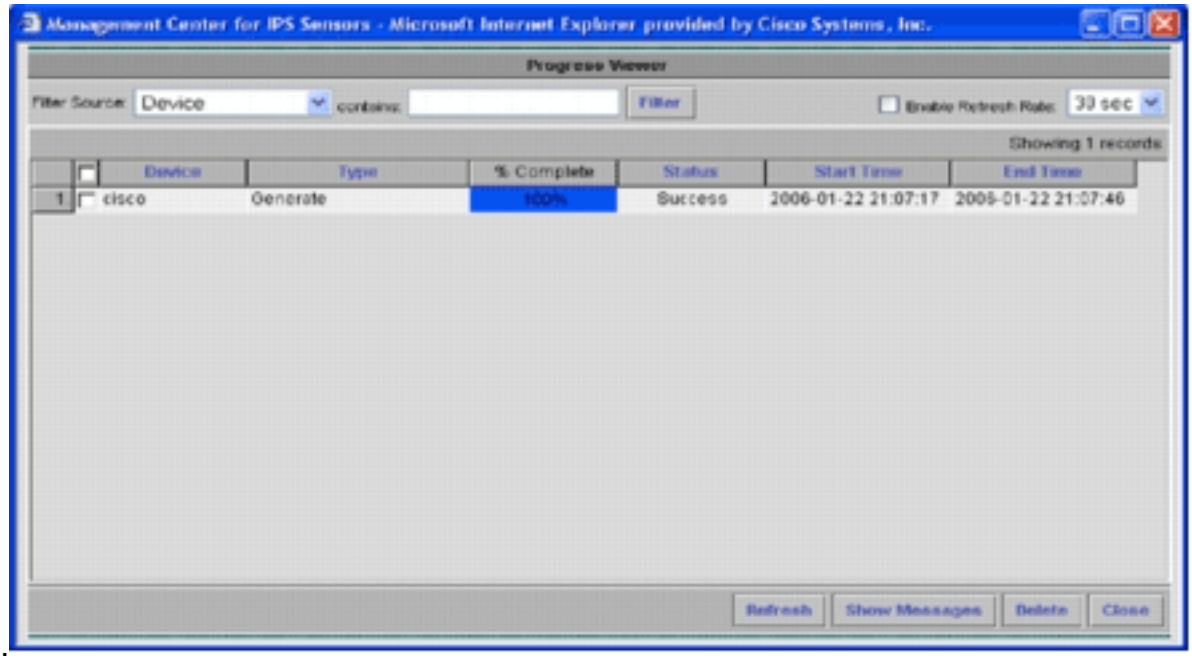
모든 컨피그레이션을 변경한 후 디바이스에 변경 사항을 커밋하려면 구축 작업을 사용해야 합니다. 지금까지 구성한 모든 컨피그레이션은 IPS MC 서버에 로컬로 저장됩니다.

컨피그레이션 변경 사항을 구축하려면 Deployment(구축) 페이지로 이동하여 다음 단계를 완료합니다.

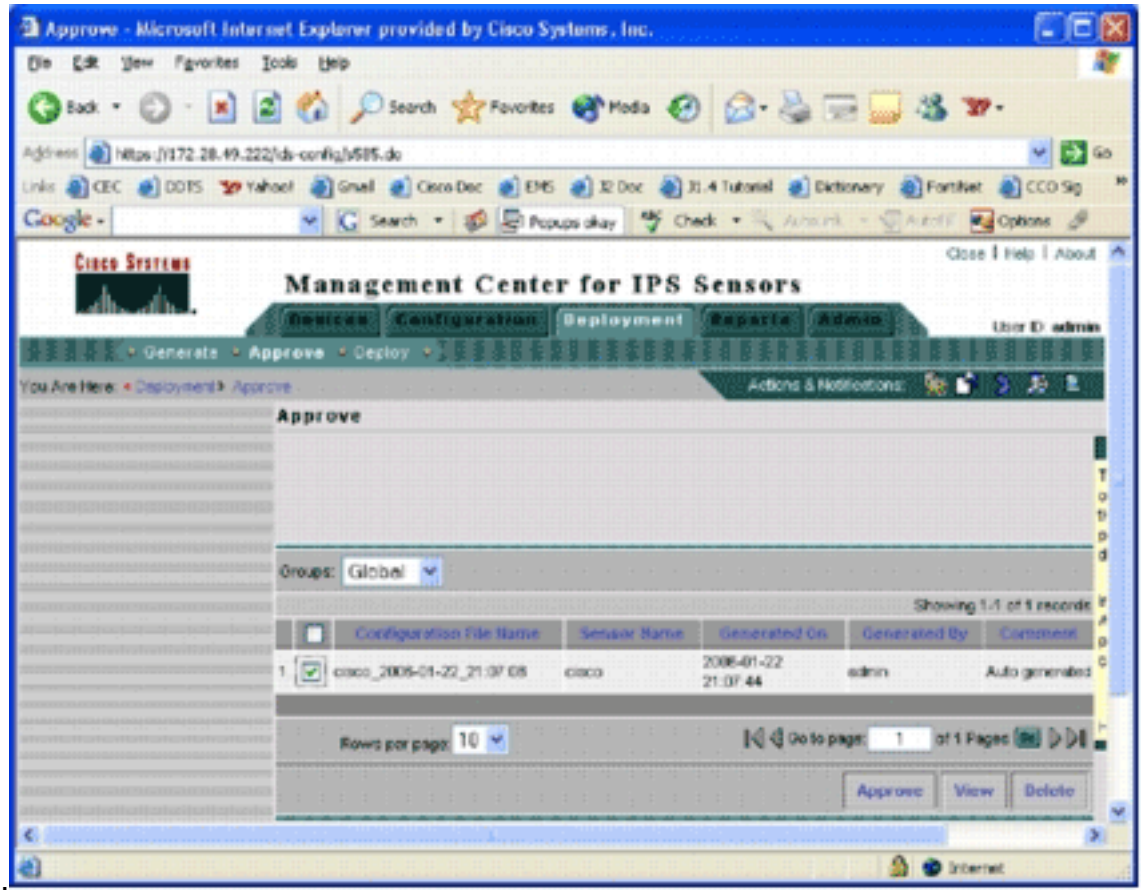
1. Deployment(구축) 탭을 클릭하고 **Generate(생성)를** 선택하여 컨피그레이션 변경 사항을 생성합니다.Generate 페이지가 나타납니다



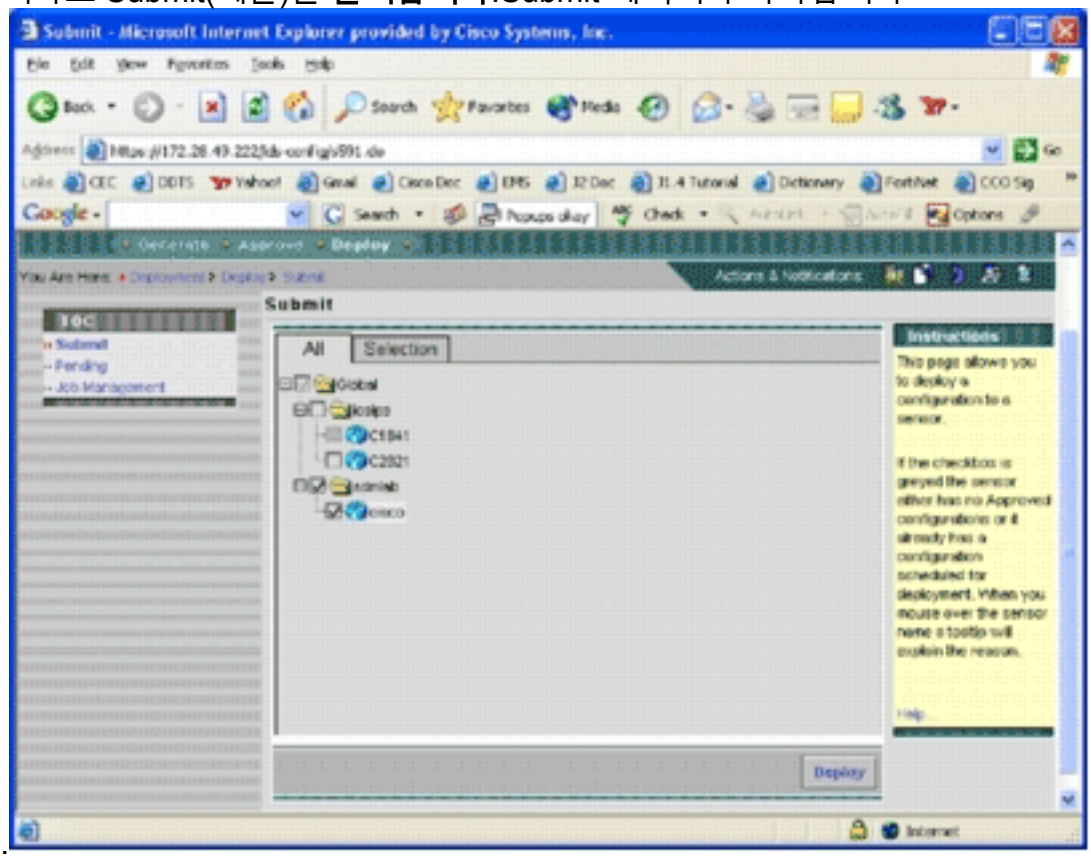
2. 방금 구성한 *cisco* 디바이스를 선택하고 Generate(생성)를 **클릭합니다**.
3. OK(**확인**)를 클릭하여 생성된 컨피그레이션을 적용한 다음 **OK**(확인)를 클릭합니다.상태 페이지가 나타납니다



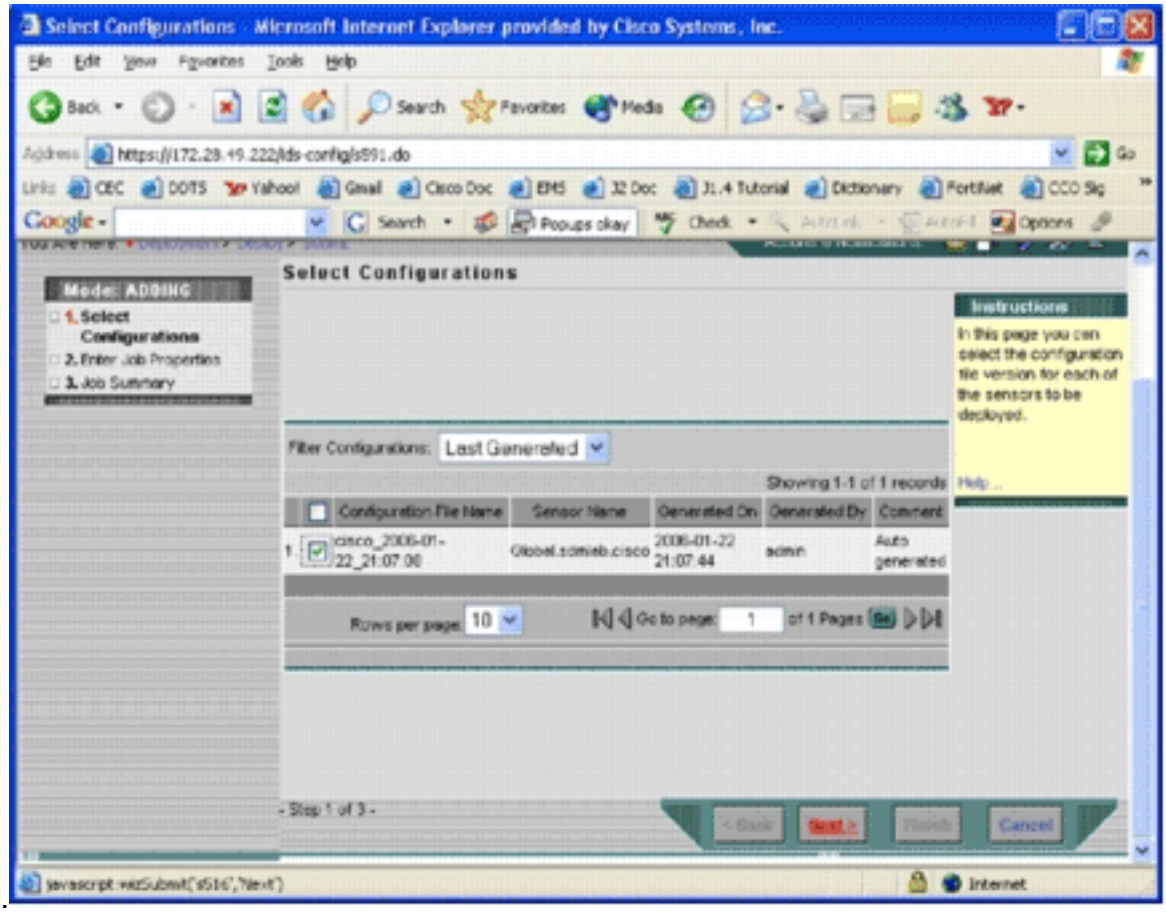
4. 생성 **작업**이 성공적으로 완료될 때까지 Refresh를 클릭합니다.
5. 승인이 필요한 구성 목록을 보려면 Deployment 메뉴 모음 및 sdmlab 그룹에 있는 Approve를 클릭합니다.승인 페이지가 나타납니다



6. 작업을 선택하고 승인을 **클릭합니다**.Deployment(구축) 메뉴 모음에 있는 Deploy(구축)를 클릭하고 Submit(제출)을 **클릭합니다**.Submit 페이지가 나타납니다

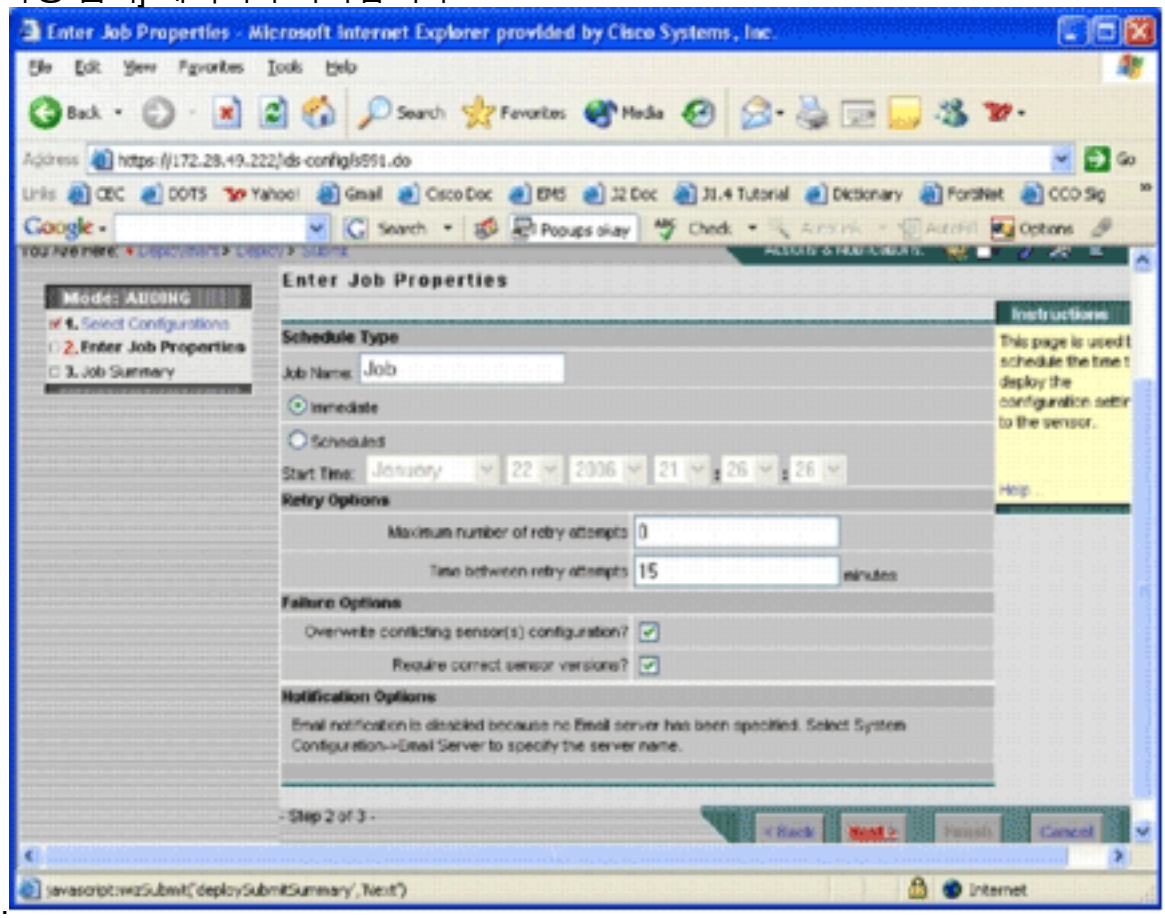


7. 배포 작업을 제출할 장치를 선택합니다.
8. *Cisco* 디바이스를 선택하고 Deploy(구축)를 **클릭합니다**.Select Configurations 페이지가 나타

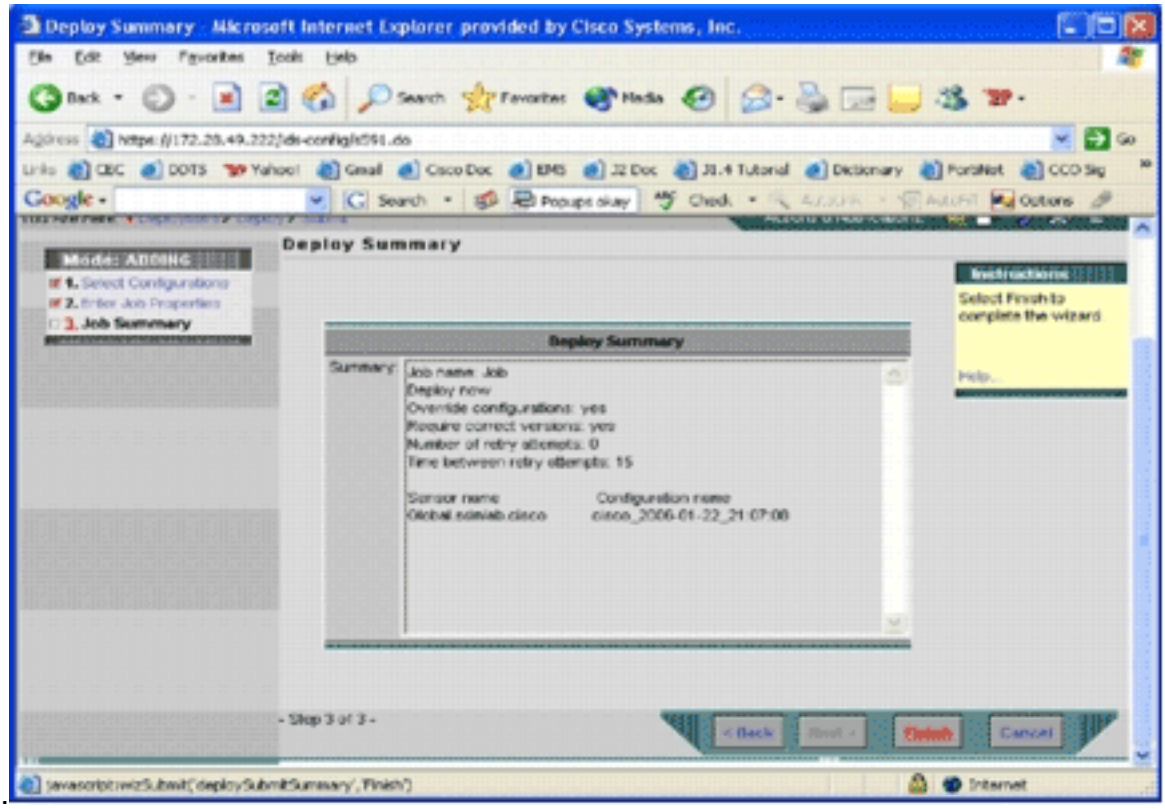


납니다.

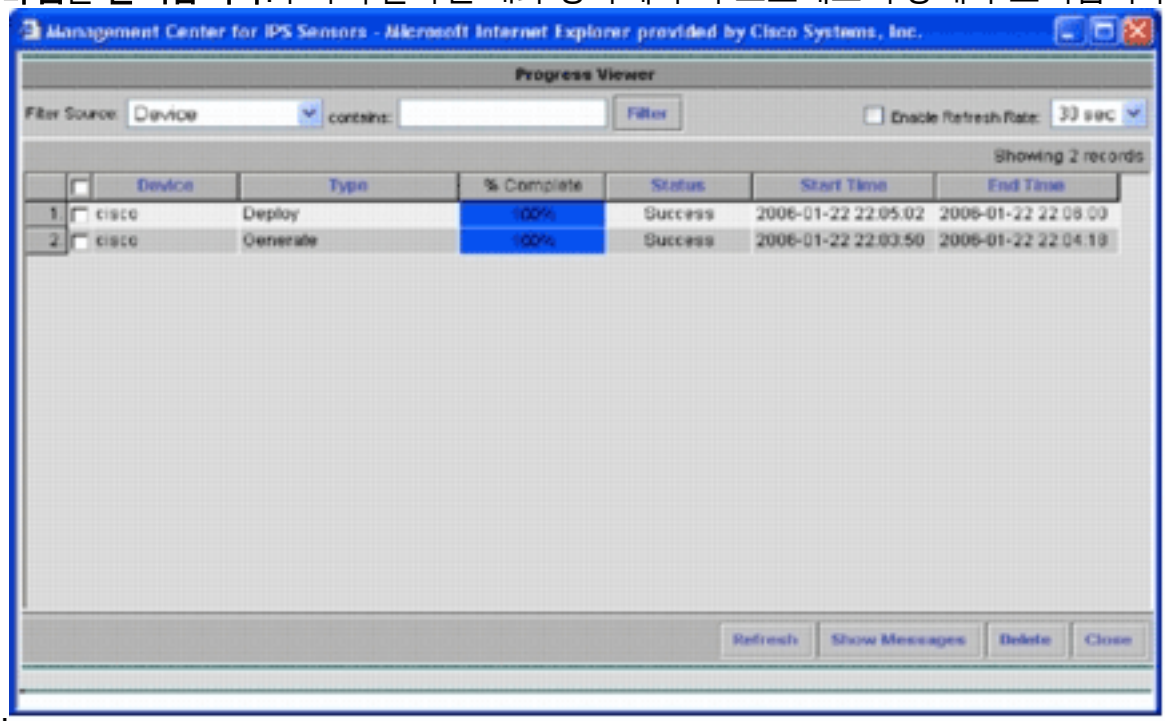
9. *cisco* 디바이스에 대해 방금 구성한 컨피그레이션을 선택하고 **Next**(다음)를 클릭합니다.[작업 속성 입력] 페이지가 나타납니다



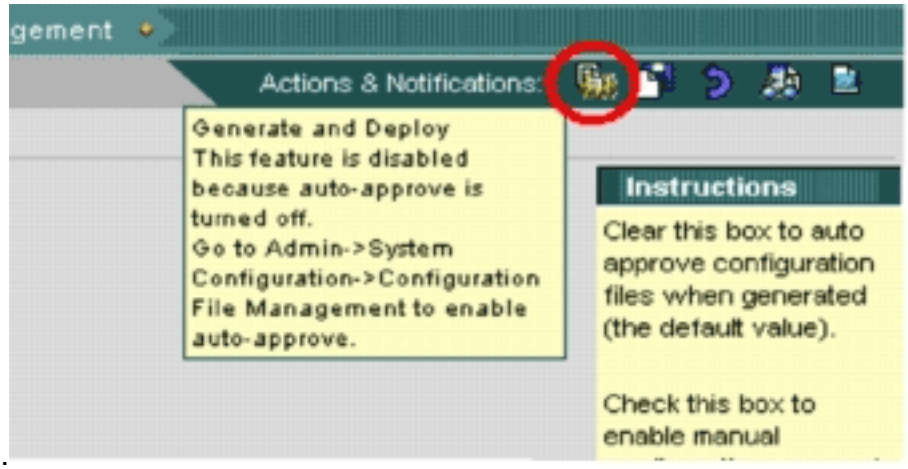
10. 변경 사항을 즉시 배포하거나 나중에 수행하도록 작업을 예약할 수 있습니다. 이 예에서 **Immediate** 옵션을 선택한 다음 **Next**를 클릭합니다.간단한 작업 요약이 표시되며 배포할 준비가 되었습니다



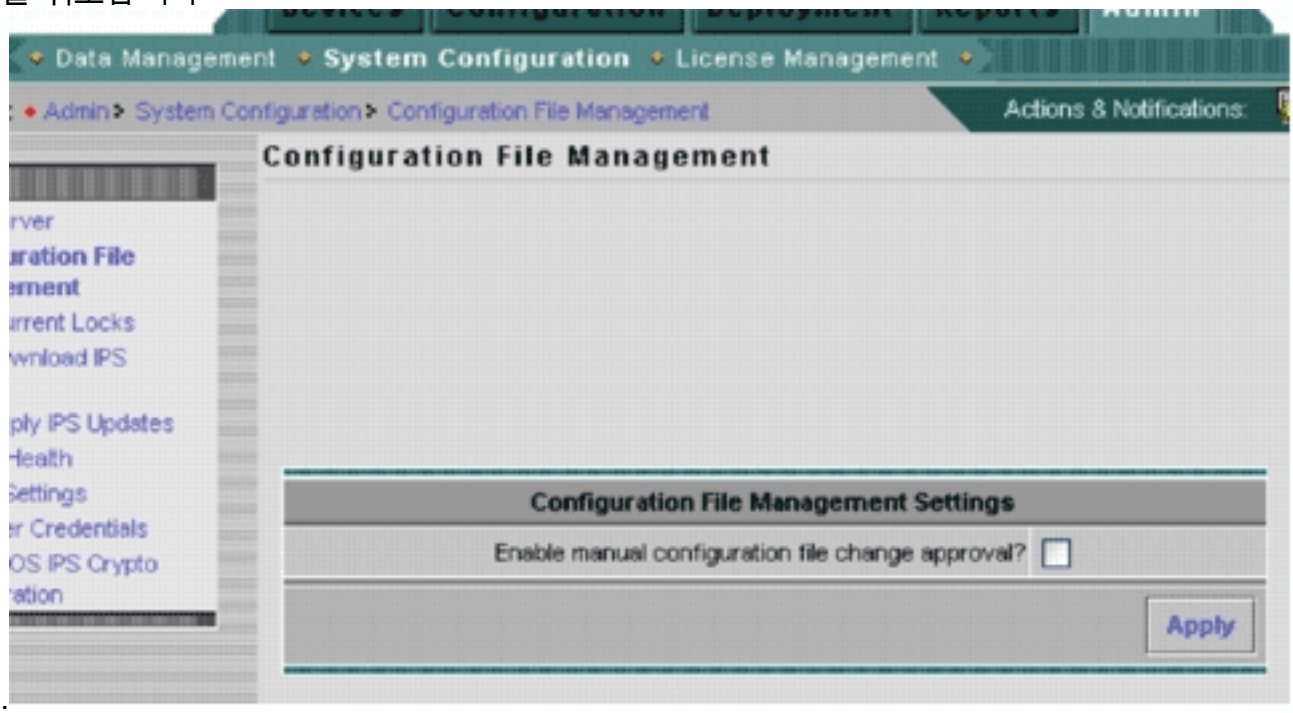
11. **마침**을 **클릭합니다**.구축이 끝나면 대화 상자에 구축 프로세스의 상태가 표시됩니다



디바이스에 Cisco IOS IPS 컨피그레이션을 성공적으로 구축했습니다. 여러 디바이스를 구성할 때 그룹 레벨에서 컨피그레이션을 변경한 다음 동일한 그룹에 속하는 모든 Cisco IOS IPS 라우터에 변경 사항을 적용할 수 있습니다.**팁:** 이 프로세스는 오래 걸리지만 빠른 제공 기능을 사용할 수 있습니다. 이 기능을 사용할 때 Generate(생성) **> Approve(승인) > Deploy(구축)** 프로세스**를** 거치지 않아도 됩니다. 이 기능을 사용하려면 다음 단계를 완료하십시오.사용자 인터페이스 상단에는 작은 아이콘 행이 있습니다. 마우스를 첫 번째 아이콘 위에 놓고 이 이미지에 표시된 도구 설명을 봅니다

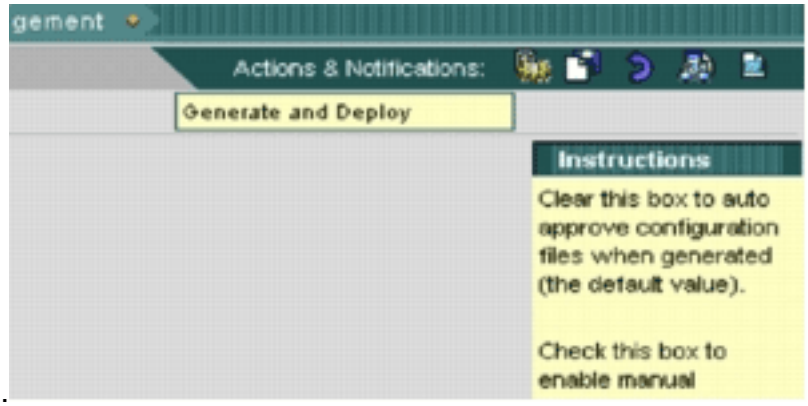


. Generate and Deploy(생성 및 구축) 작업을 활성화하려면 **Admin(관리) > System Configuration(시스템 컨피그레이션) > Configuration File Management(컨피그레이션 파일 관리)**로 이동하여 **Enable manual configuration file change approval(수동 컨피그레이션 파일 변경 승인 활성화)** 확인란의 선택을 취소합니다



.

첫 번째 아이콘 위에 마우스 커서를 올려 놓으면 작업이 활성화되었음을 나타냅니다



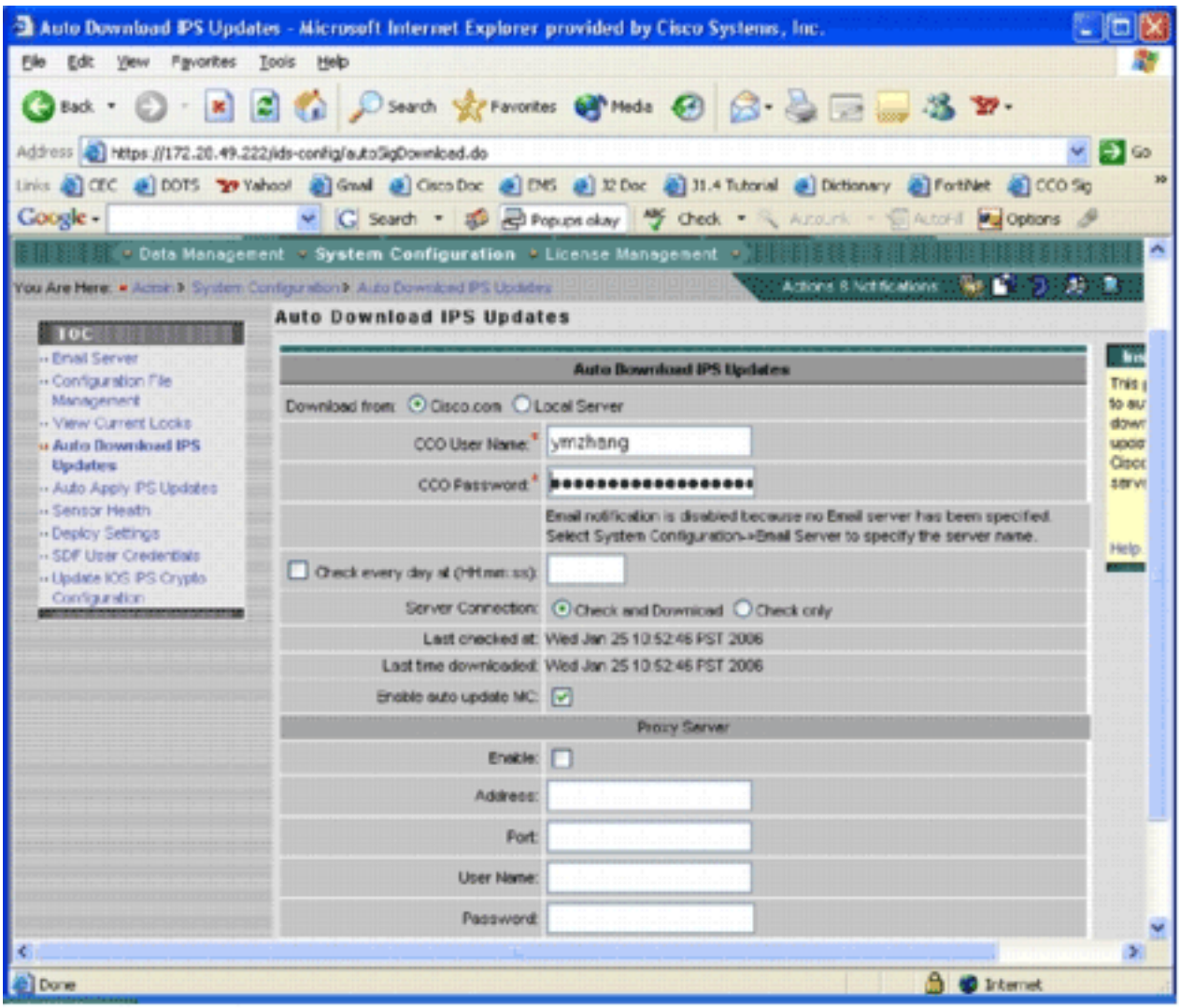
. 이 아이콘을 클릭합니다.IPS MC는 컨피그레이션 변경 사항을 자동으로 생성하여 디바이스에 구축합니다.

서명 업데이트 자동 다운로드

IPS MC는 Cisco.com에서 서명 자동 다운로드를 지원합니다. 센서 플랫폼과 Cisco IOS IPS 플랫폼의 시그니처 업데이트를 다운로드할 수 있습니다. 이 기능을 구성하려면 Admin(관리) **> System**

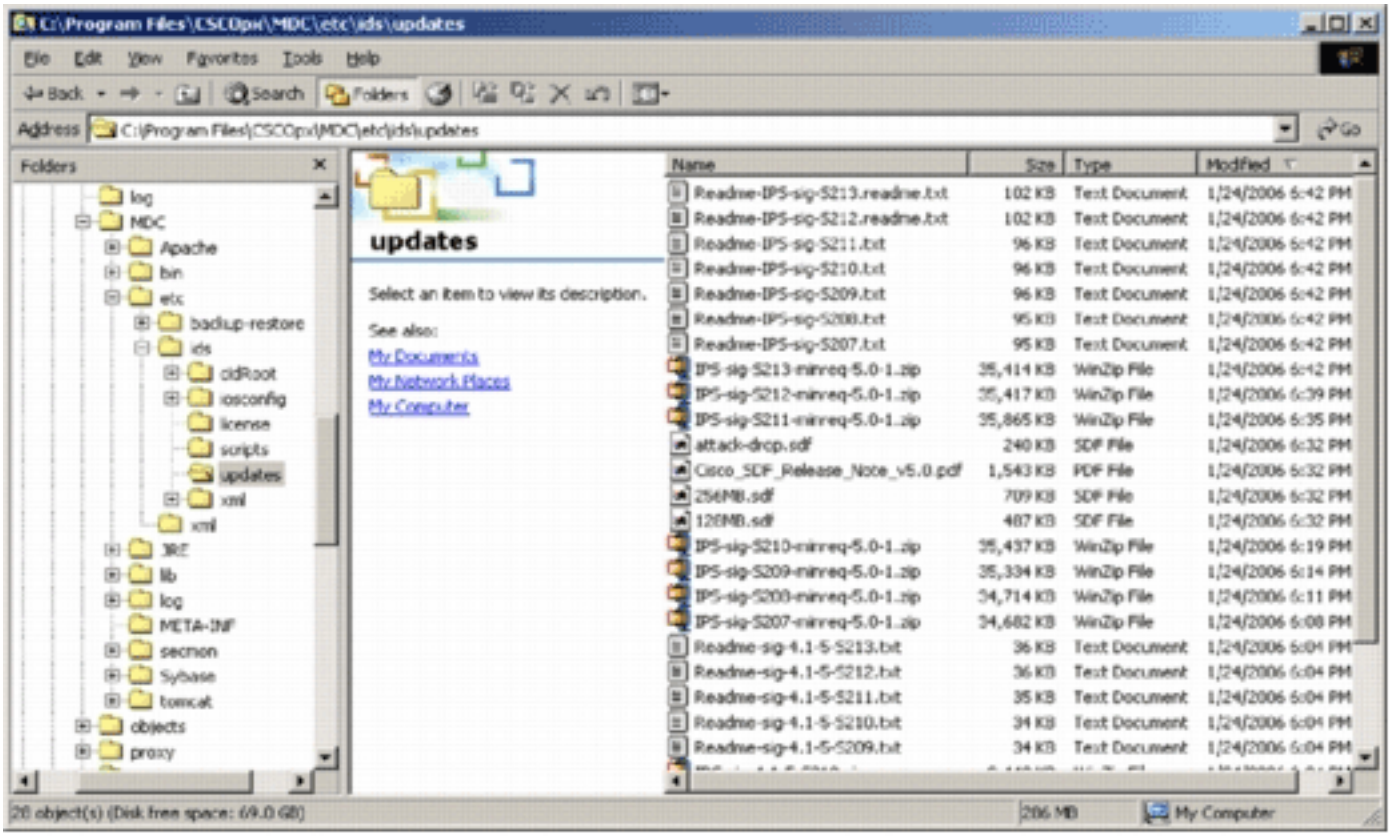
Configuration(시스템 컨피그레이션) > Auto Download IPS Updates(IPS 업데이트 자동 다운로드)로 이동합니다.

Auto Download IPS Update 페이지가 나타납니다.



이 서명 업데이트를 다운로드하려면 유효한 Cisco.com 계정이 있어야 합니다. 자동 다운로드된 파일을 확인하려면 IPS MC 설치 홈 디렉토리로 이동합니다. 기본적으로 \program files\CSCOpx\MDC\etc\ids\updates입니다.

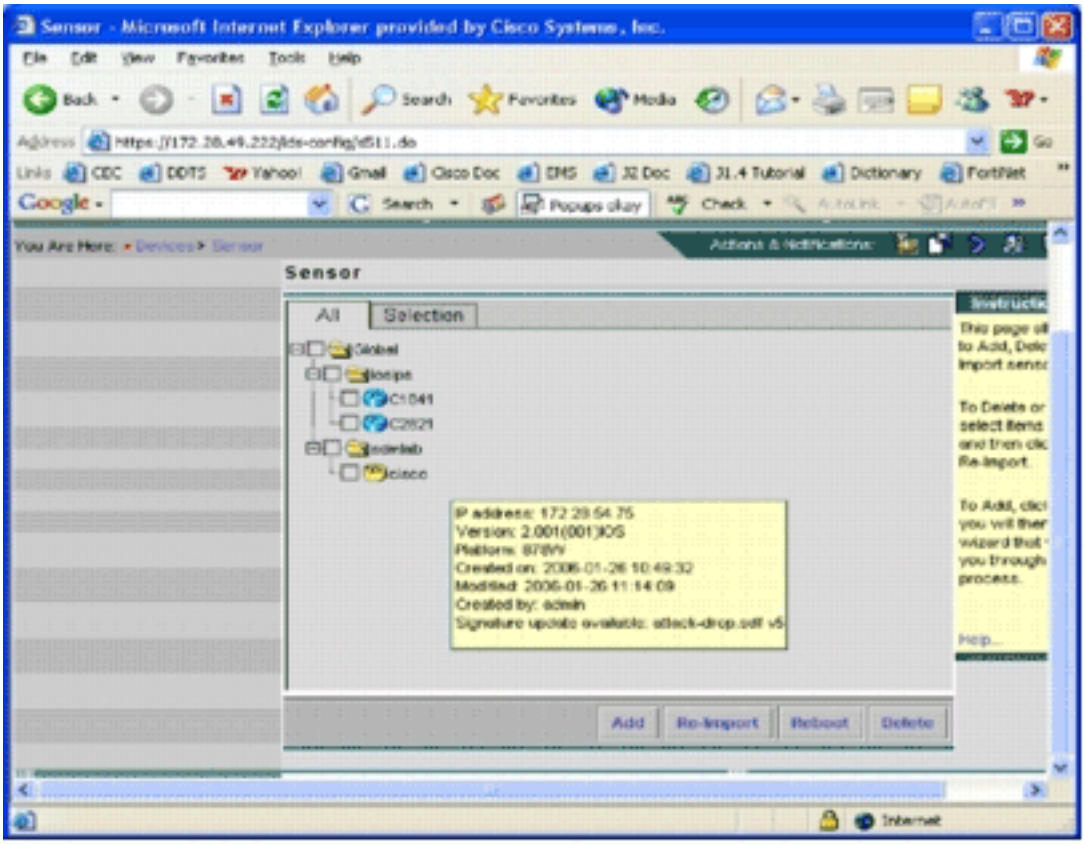
이 그림에서는 이 디렉토리에 다운로드된 파일의 이미지를 보여 줍니다.



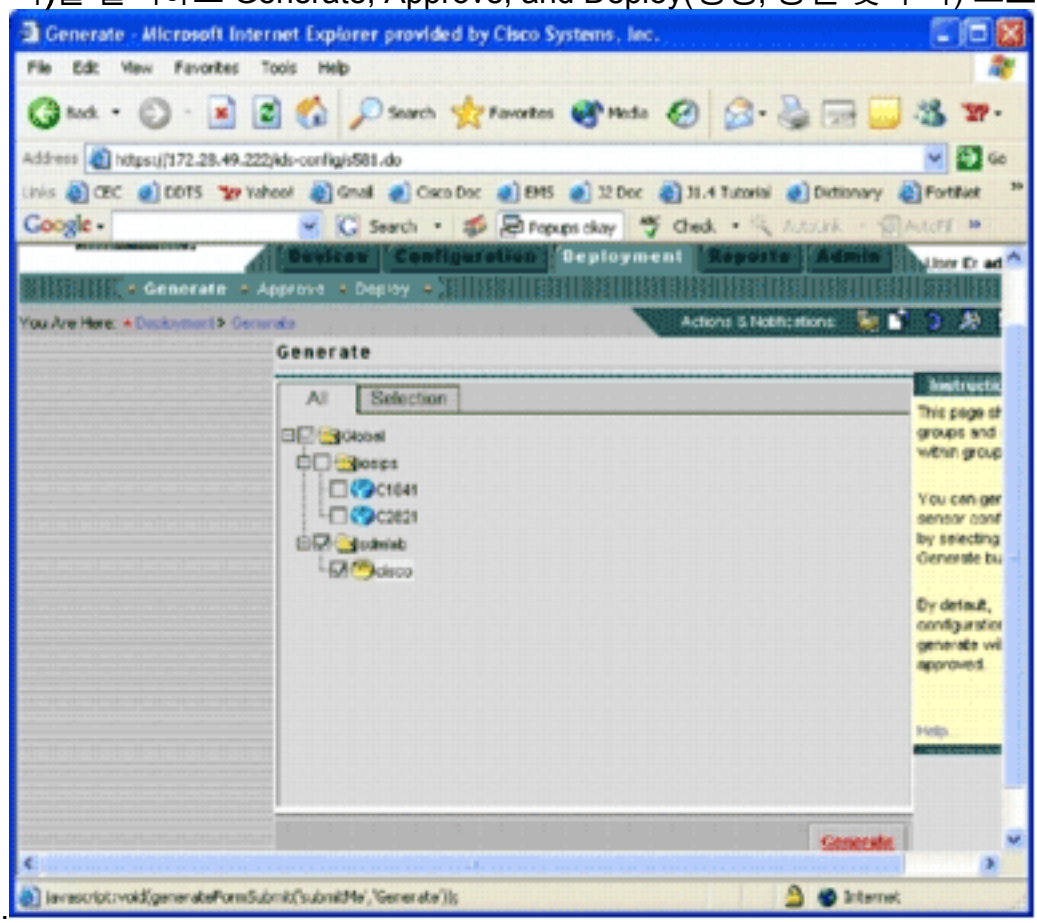
센서 업데이트 파일을 볼 수 있습니다. Cisco IOS Software 업데이트 파일 및 미리 조정된 SDF 파일이 다운로드됩니다.

새 SDF 파일로 Cisco IOS IPS 라우터 업데이트

사전 조정된 SDF 파일과 함께 구축된 Cisco IOS IPS 라우터의 경우, 자동 다운로드 또는 업데이트 디렉토리에 복사된 새로운 버전의 SDF 파일을 사용할 수 있게 되면 Cisco IPS MC는 새 버전을 인식합니다. 사용자 인터페이스를 새로 고치면 해당 디바이스의 디바이스 아이콘이 노란색으로 바뀝니다.



1. Deployment(구축)를 클릭하고 Generate, Approve, and Deploy(생성, 승인 및 구축) 프로세스



를 진행합니다.

2. 성공적으로 구축한 후 Cisco IOS IPS 라우터는 새로운 버전의 SDF 파일을 사용합니다.

관련 정보

- Cisco 침입 방지 시스템