Cisco FireSIGHT 및 ISE Rapid Threat Containment Solution

목차

이 문서 정보

이 문서는 FireSIGHT Management Center 5.4를 Cisco ISE(Identity Service Engine) 1.3 이상과 함께 구축하는 데 관심이 있는 Cisco 엔지니어 및 고객을 대상으로 하며, pxGrid(platform exchange Grid)의 ANC(Adaptive Network Control) 완화 조치를 사용하여 엔드포인트에서 조치를 수행합니다. 이 문서는 FireSIGHT Management Center 5.4에만 해당되며 FireSIGHT Management Center 6.0에는 해당되지 않습니다.

이 문서는 셀프 서명된 인증서와 함께 pxGrid가 활성화된 CA(Certificate Authority) 서명 인증서도 사용하는 독립형 환경에서 ISE를 사용한 FireSIGHT Management Center의 컨피그레이션에 대한 세부 정보를 제공합니다. pxGrid 교정 모듈, pxGrid 에이전트 설치 및 컨피그레이션 세부 정보를 다룹니다. pxGrid 교정 모듈은 격리(quarantine), 포트 바운스(portbounce), 포트 종료(portshut), 재인증(reauthenticate), 종료(terminate), 격리 해제(unquarantine)와 같은 pxGrid ANC 완화 기능을 제공합니다. pxGrid 에이전트는 FireSIGHT Management Center와 ISE pxGrid 노드 간의 ISE pxGrid 노드 연결 정보 및 인증서 정보를 제공합니다. 각 ANC 완화 조치 유형에 대한 상관관계 정책, 규칙, 교정 유형이 정의됩니다.

독자는 FireSIGHT Management Center 및 ISE(Identity Service Engine) 액세스 컨트롤 시스템에 어느 정도 익숙해야 합니다. FireSIGHT Management Center 5.4 및 독립형 ISE 1.3 또는 ISE 1.4 환경이 설치된 것을 전제로 합니다. 또한 FireSIGHT Management Center 5.4는 ISE 2.0에서 테스트되었습니다.

다음 소프트웨어 버전이 이 문서의 테스트에 사용되었습니다.

- FireSIGHT Management Center 5.4
- FireSIGHT Appliance Virtual Sensor 5.4
- Cisco ISE(Identity Services Engine) 1.3 및 ISE 1.4
- FireSIGHT pxGrid 교정 모듈 1.0
- FireSIGHT pxGrid Agent 1.0
- Microsoft CA 2008 R2 Enterprise

분산 ISE 환경에서 ISE pxGrid를 구성하는 경우 참조 섹션의 링크를 참조하십시오. 또한 MAC를 pxGrid 클라이언트로 사용하는 셀프 서명된 인증서 및 CA 서명 인증서를 통한 구축 방법 가이드에 대한 링크가 참조로 포함되어 있습니다.

기술 개요

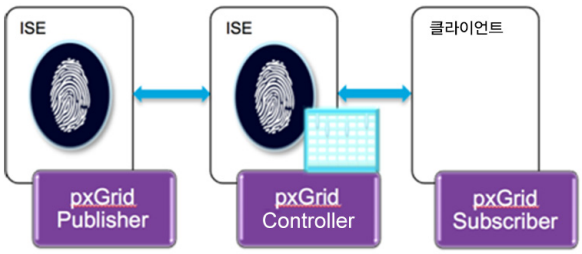
Cisco pxGrid(Platform Exchange Grid)를 사용하면 IT 인프라 간의 멀티벤더 및 교차 플랫폼 네트워크 시스템 협업을 구현할 수 있습니다. 보안 모니터링 및 탐지 시스템, 네트워크 정책 플랫폼, 자산 및 컨피그레이션 관리, ID 및 액세스 관리 플랫폼, 거의 모든 기타 IT 운영 플랫폼을 허용합니다. pxGrid는 ISE(Identity Service Engine) 정책 서버를 사용하여 인증, 권한 부여 및 액세스 컨트롤(AAA)을 제공합니다.

pxGrid 프레임워크는 다음으로 구성됩니다.

pxGrid Publisher - 관심 있는 주제 또는 기능을 게시합니다.

pxGrid Controller - 모든 pxGrid 클라이언트 인증, 권한 부여, 기능 및 서브스크립션 목록을 관리합니다.

pxGrid Subscriber(pxGrid 클라이언트라고도 함) - 게시된 pxGrid 주제를 서브스크립션합니다.



FireSIGHT ISE 교정 모듈은 pxGrid 클라이언트이며 ISE 게시/서브스크립션 방법을 통해 완화 조치를 제공합니다.

ISE는 세션 디렉토리 및 엔드포인트 보호 서비스를 게시합니다. 세션 디렉토리는 pxGrid 세션 개체에 대한 기존 특성을 ISE 세션 디렉토리에 표시합니다. 예를 들면 다음과 같습니다.

세션 상태

IP 주소

Username

사용자 AD 도메인

MAC

NAS.IP.ADDRESS

TrustSec 보안 그룹 이름

엔드포인트 프로파일 이름

프로파일링 정책 이름

상태

감사 세션 ID

계정 세션 IP(RADIUS AV 쌍으로, 마지막 업데이트 시간)

엔드포인트 보호 서비스는 다음과 같은 pxGrid ANC 완화 개체를 제공합니다.

격리

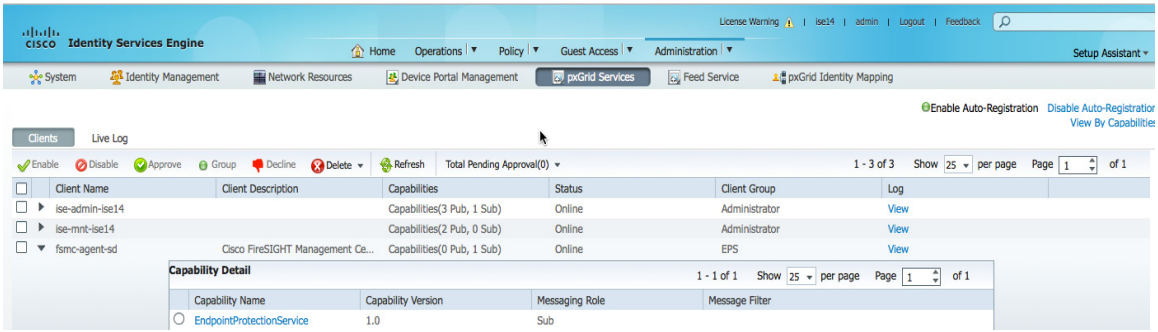
격리 해제

종료

바운스 포트

종료

FireSIGHT 에이전트가 ISE pxGrid 노드에 pxGrid 클라이언트로 등록되고 pxGrid ANC 완화 조치를 수행하기 위해 엔드포인트 보호 서비스 주제 및 EPS 세션 그룹을 서브스크립션합니다.



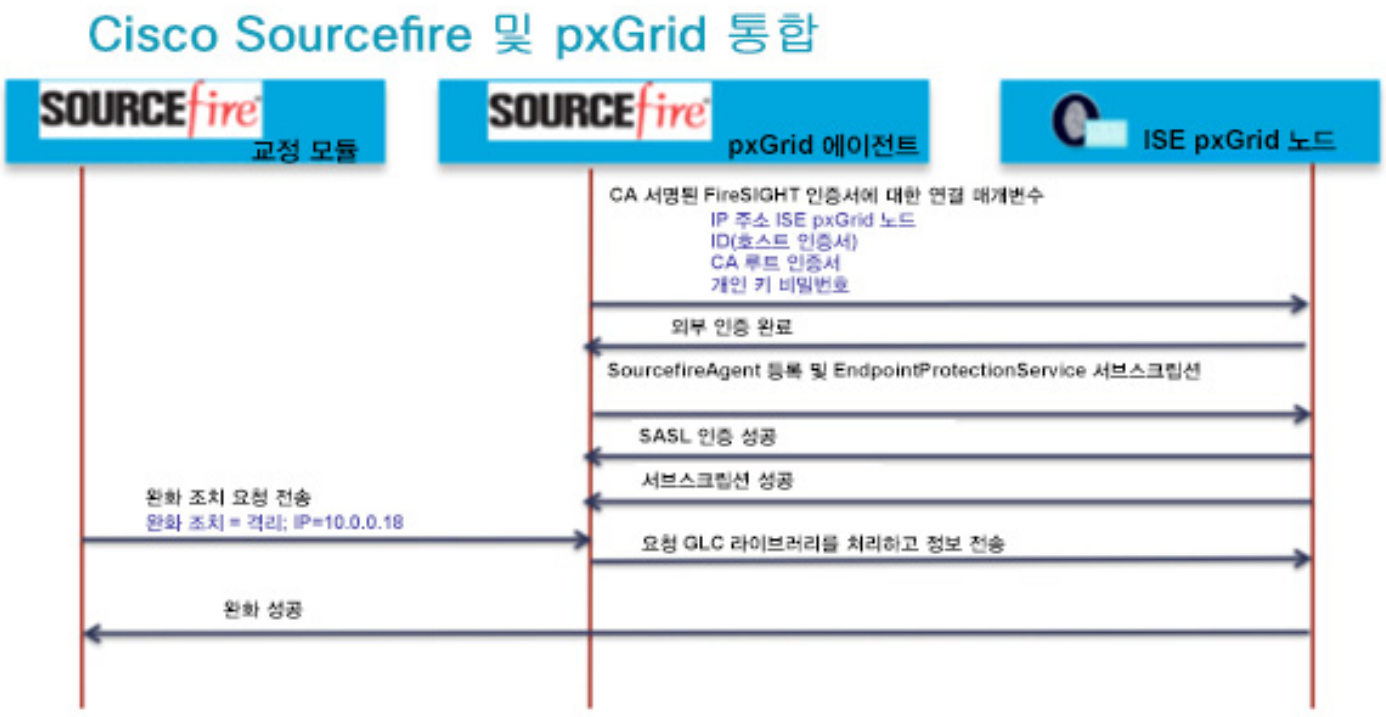
실제 FireSIGHT pxGrid 통합은 pxGrid 에이전트 및 pxGrid 교정 모듈을 FireSIGHT Management Center에 업로드하여 발생합니다.

pxGrid 에이전트 설치는 세 가지 기능을 제공합니다.

pxGrid 서비스 설치 및 라이브러리 지원

- pxGrid 연결 매개변수 컨피그레이션 - pxGrid 노드 IP 주소, 호스트/ID 인증서, 호스트 개인 키 인증서 및 신뢰할 수 있는 CA 루트
- pxGrid 서비스를 시작하고 pxGrid 교정 모듈의 완화 조치 요청을 처리하여 ISE pxGrid 노드에 정보를 전송합니다.
- pxGrid 교정 모듈은 모든 pxGrid 상호 작용을 pxGrid 서비스에 전달하고 ISE pxGrid 노드로부터 알림 결과를 수신합니다.

FireSIGHT pxGrid 교정 모듈은 pxGrid ANC 완화 조치 요청을 FireSIGHT pxGrid 서비스에 전송합니다. FireSIGHT pxGrid 서비스는 pxGrid GCL 라이브러리를 기반으로 이러한 요청을 처리한 후 이 정보를 ISE pxGrid 노드에 전송합니다. FireSIGHT Management Center에서 엔드포인트의 운영 체제 세부 정보와 사용자 로그온/로그오프 정보를 얻기 위해 호스트 및 사용자에 대한 네트워크 검색이 설정된 상태로 Microsoft AD 영역이 구성됩니다.

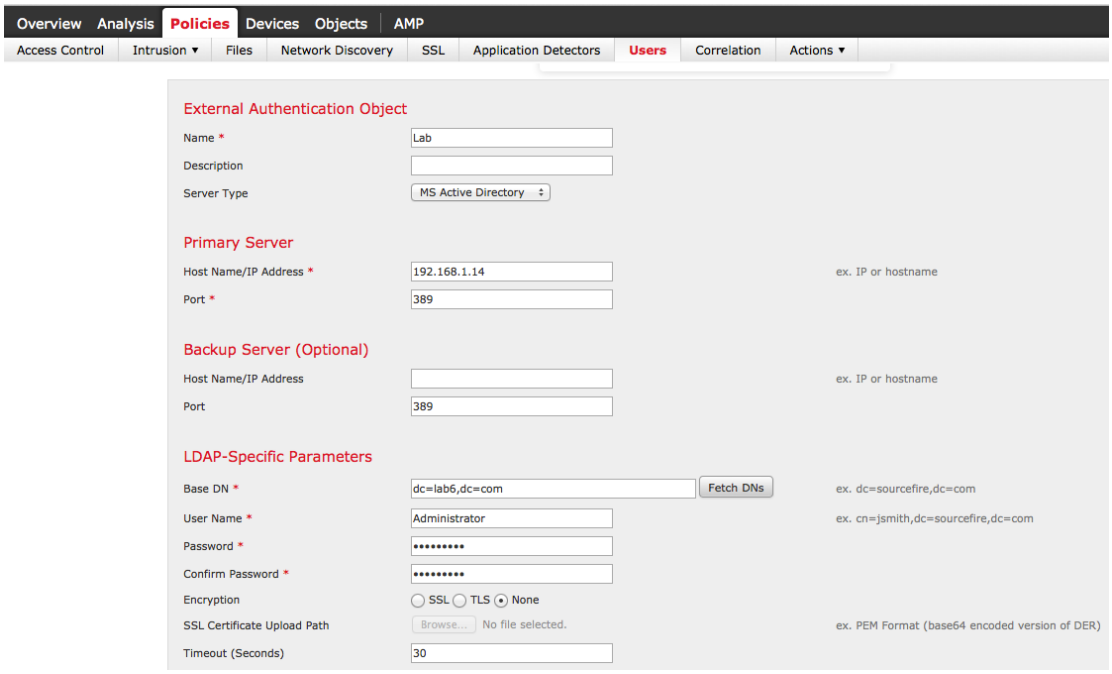


FireSIGHT 영역 컨피그레이션

LDAP 사용자 정보를 제공하는 인증 서버가 정의됩니다. 또한 사용자 로그온/로그오프 세부 정보와 호스트 정보 및 운영 체제 세부 정보를 제공하기 위해 사용자 인식이 활성화되고 네트워크 검색이 설정됩니다.

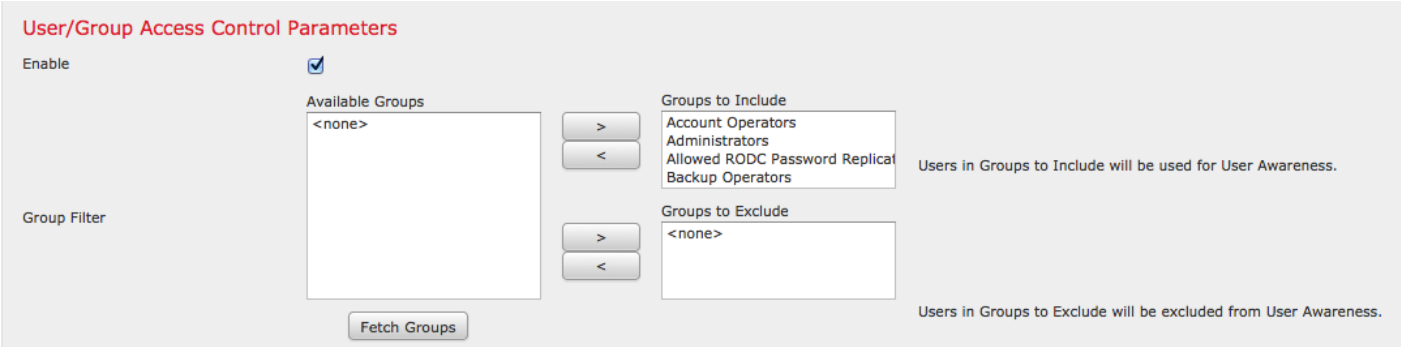
LDAP 연결 구성

1단계 **Policies(정책)->Users(사용자)->Add LDAP Connection(LDAP 연결 추가)**를 선택한 후 다음을 입력합니다.



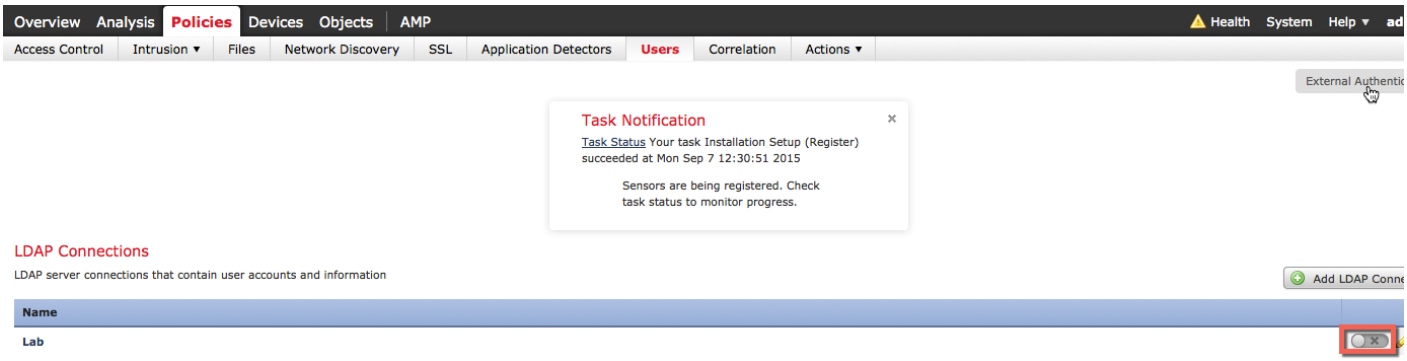
2단계 **Enable(활성화)->User/Group Access Control Parameters(사용자/그룹 액세스 컨트롤 매개변수)->Fetch Groups(그룹 가져오기)**

참고: 사용자 인식을 위해 모든 그룹을 포함합니다.

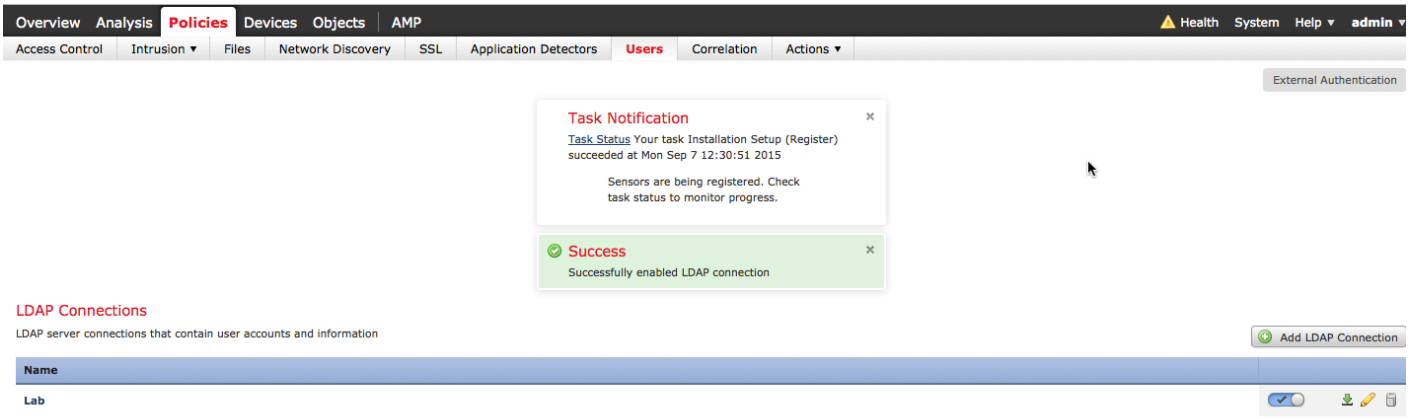


3단계 **테스트 및 저장**

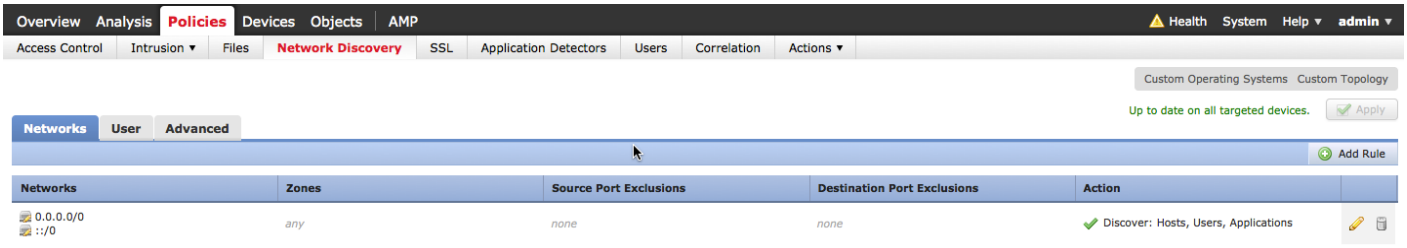
4단계 LDAP 연결을 활성화하고**->버튼을 클릭합니다**.



5단계 다음과 같이 표시되어야 합니다.

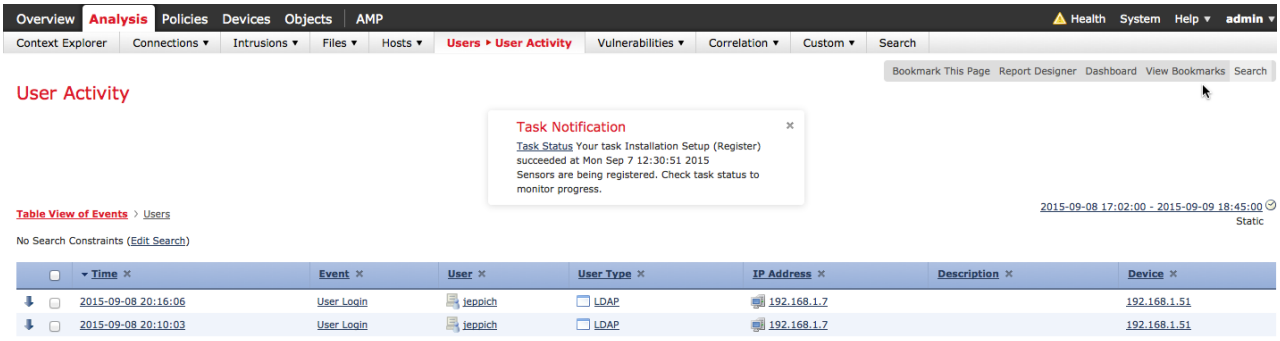


6단계 호스트, 사용자 및 애플리케이션에 대한 네트워크 검색을 활성화합니다.
Policies(정책)->Network Discovery(네트워크 검색)를 선택한 후 연필을 클릭하고 Hosts(호스트), Users(사용자) 및 Applications(애플리케이션)를 선택한 다음 Save(저장)를 클릭합니다.

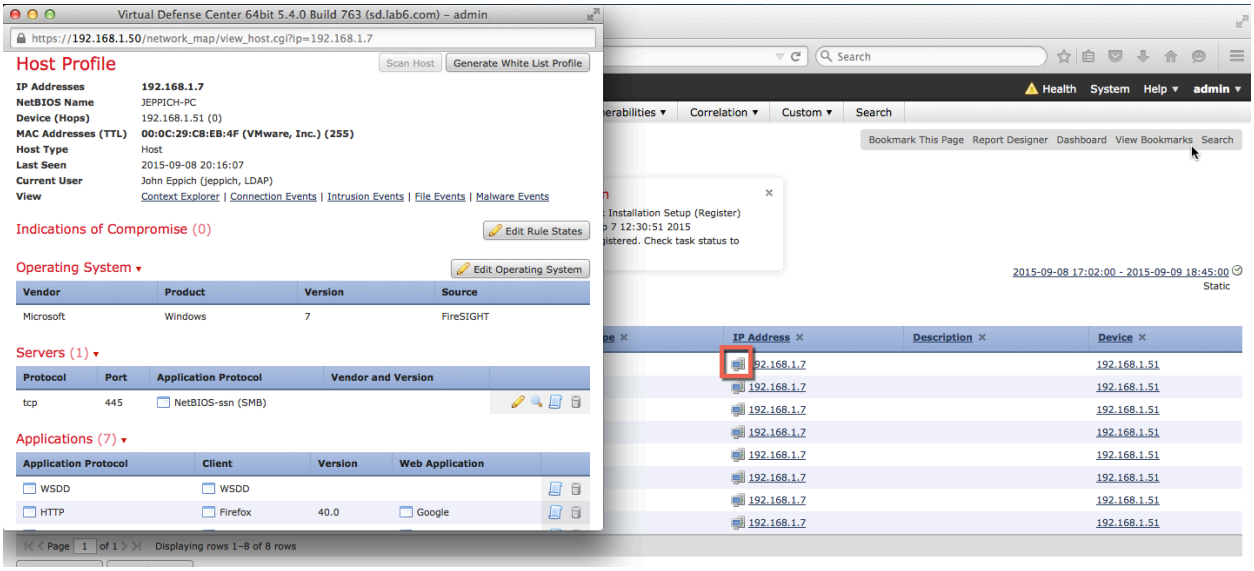


샘플 사용자 LDAP 정보

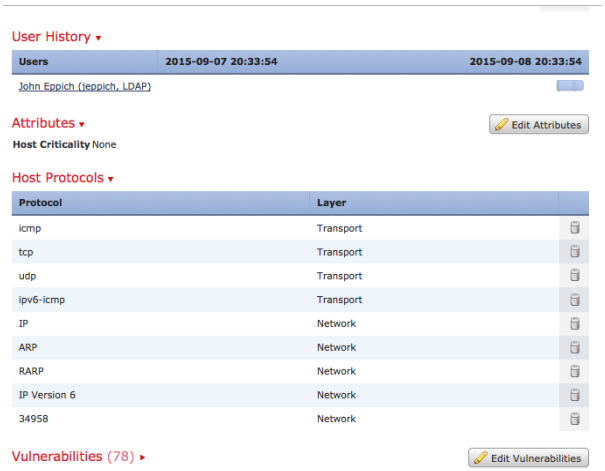
User Activity(사용자 활동) 화면에는 최종 사용자 정보가 표시됩니다.



또한 아래의 PC 아이콘을 클릭하면 아래의 IP 주소에 대한 "호스트 프로파일"이 수신됩니다.



이 호스트 프로파일에는 사용자 기록 정보, 호스트 프로토콜 및 취약성 정보가 포함됩니다.



pxGrid를 사용하는 독립형 환경에서 셀프 서명된 인증서에 대한 ISE 구성

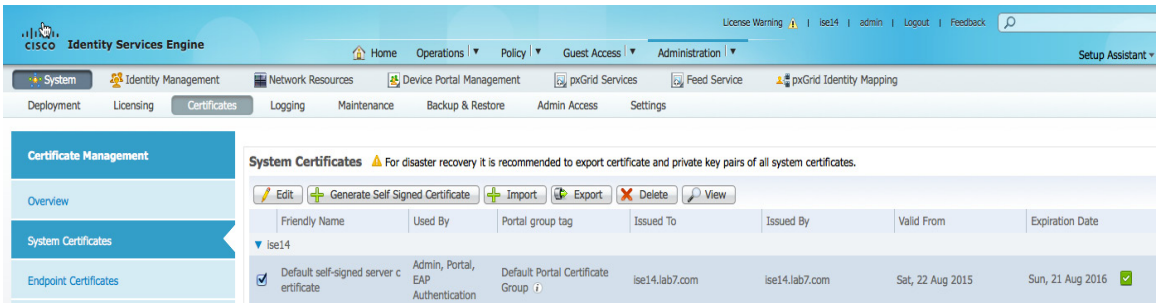
이 섹션에서는 pxGrid를 사용하는 독립형 환경에서 셀프 서명된 인증서를 사용하여 ISE를 구성하는 프로세스 단계를 설명합니다.

ISE ID 셀프 서명된 인증서를 ISE의 신뢰할 수 있는 인증서 저장소로 내보내기

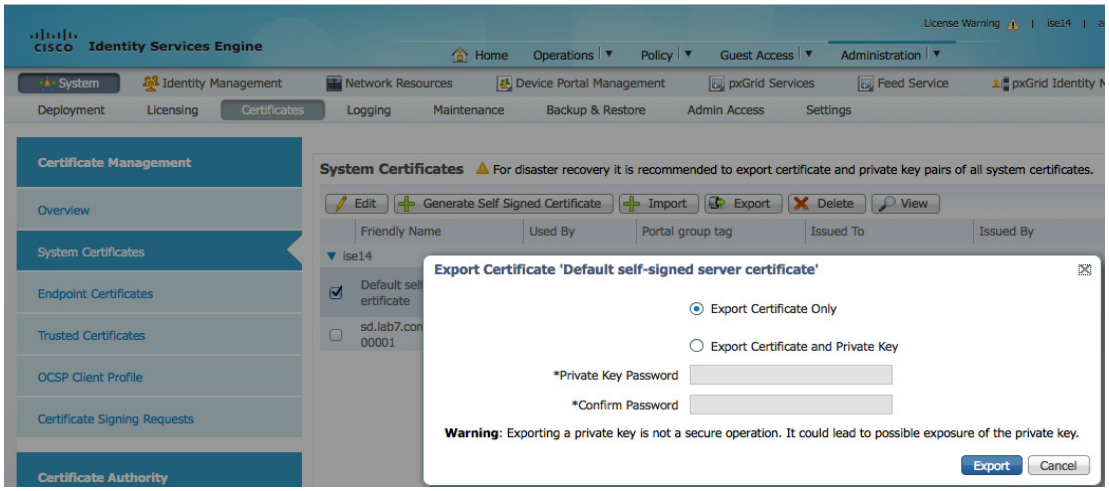
이를 수행하려면 ISE가 셀프 서명된 인증서를 신뢰해야 합니다.

참고: ISE 2.0에서는 이 과정이 필요하지 않습니다. 기본적으로, pxGrid가 ISE에서 활성화되면 게시된 노드가 표시되고 ISE pxGrid 노드에 대한 연결이 설정됩니다. 이 ISE ID 셀프 서명된 인증서가 신뢰됩니다.

1단계 **Administration(관리)->System(시스템)->Certificates(인증서)->System Certificates(시스템 인증서)를 선택하고 ISE 셀프 서명된 ID 인증서를 선택합니다.**

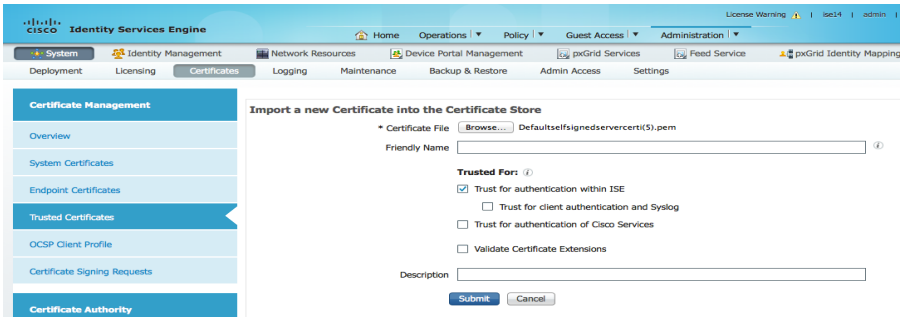


2단계 인증서만 내보내도록 선택한 후 **Export(내보내기)를 클릭합니다**.



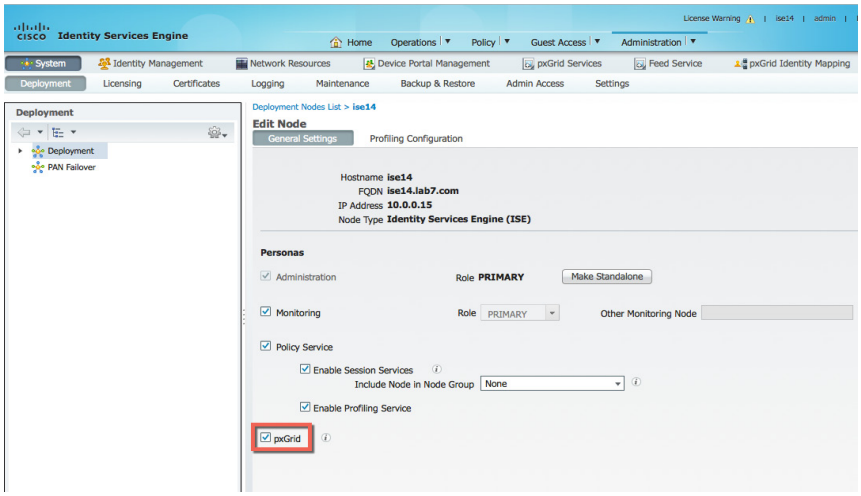
3단계 ISE ID 셀프 서명된 인증서를 ISE의 신뢰할 수 있는 저장소로 가져옵니다.

Administration(관리)->System(시스템)->Certificates(인증서)->Trusted Certificates(신뢰할 수 있는 인증서)->Import(가져오기)->ISE ID 셀프 서명된 인증서(PEM)를 선택하고 Trust for authentication within ISE(ISE 내의 인증 신뢰)를 활성화한 후 Submit(제출)를 클릭합니다.



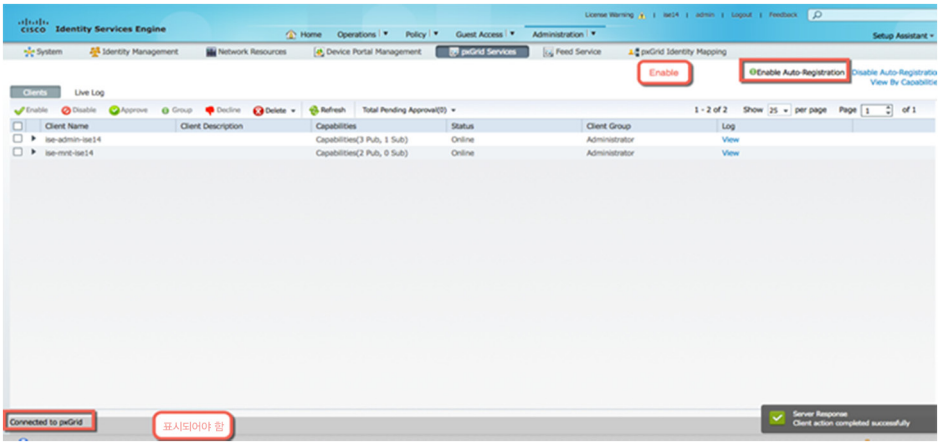
4단계 ISE 노드에서 pxGrid를 활성화합니다.

Administration(관리)->System(시스템)->Deployment(구축)를 클릭한 후 노드를 선택하고 pxGrid를 활성화한 다음 Save(저장)를 클릭합니다.



5단계 pxGrid 서비스가 실행 중인지 확인합니다.
Administration(관리)->pxGrid services(pxGrid 서비스)를 선택하고"Enable Auto Registration(자동 등록 활성화)"을 활성화합니다.

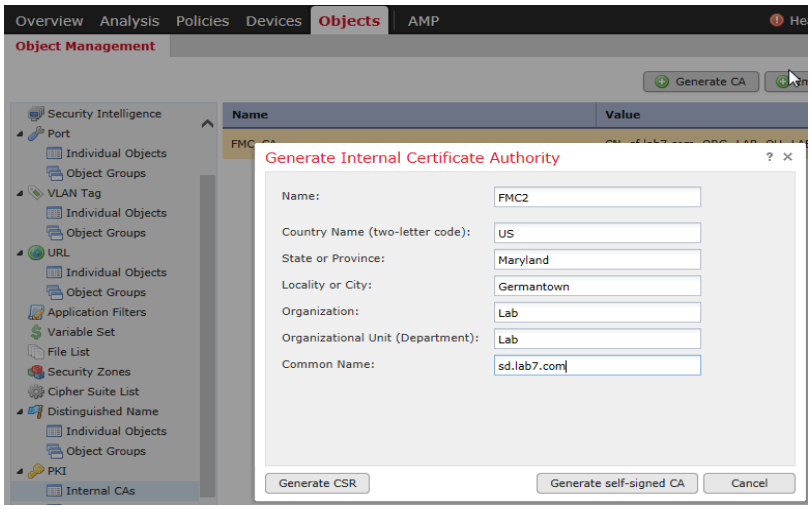
참고: 연결을 확인하기 전에 이 작업을 수행하는 데 몇 분이 소요될 수 있습니다.



셀프 서명된 인증서에 대한 FireSIGHT Management Center 구성

이 섹션에서는 ISE pxGrid 노드 작업을 위해 셀프 서명된 인증서를 사용하도록 FMC(FireSIGHT Management Center)를 구성합니다. 내부 FMC 인증 기관이 FireSIGHT Management Center에 생성되며 공개/개인 키 쌍을 ISE 인증서 시스템 저장소로 내보내고 가져옵니다. 내부 FMC 공용 인증서를 ISE 인증서의 신뢰할 수 있는 시스템 저장소로 내보냅니다. ISE ID 셀프 서명된 공용 인증서를 FireSIGHT Management Center의 신뢰할 수 있는 CA 저장소로 가져옵니다.

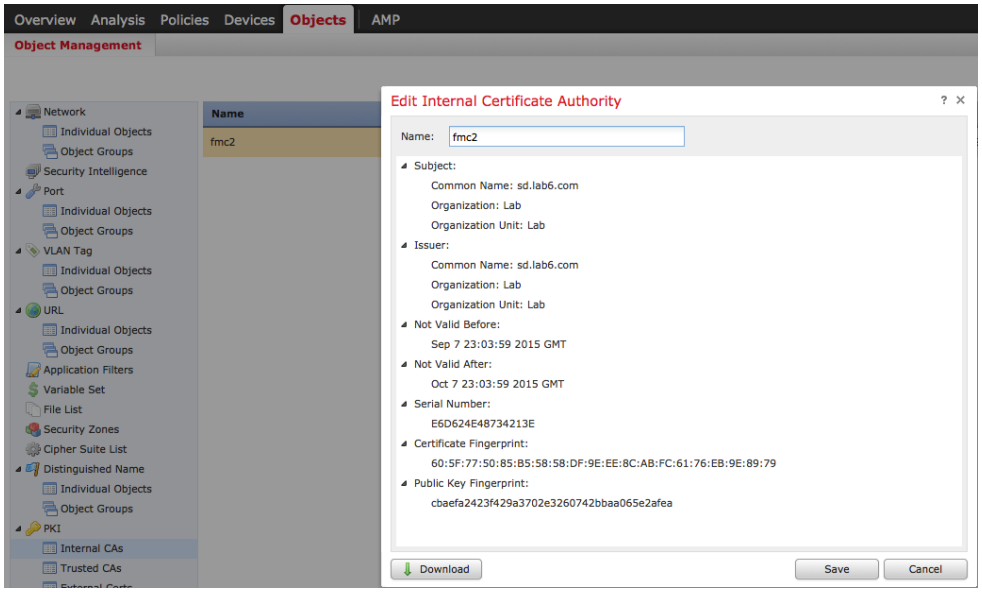
1단계 **Objects(개체)->Object Management(개체 관리)->PKI->Internal CAs(내부 CA)->Generate CA(CA 생성)**를 선택한 후 아래의 인증서 정보를 제공합니다.
이 예에서는 내부 CA에 지정된 이름이 FMC2입니다.



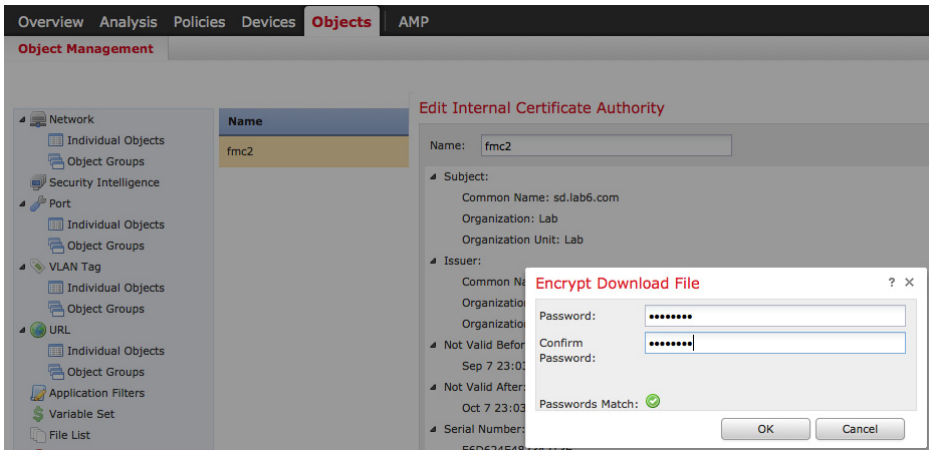
2단계 **Generate self-signed CA(셀프 서명된 CA 생성)를 클릭합니다.**

3단계 CA 인증서 파일을 다운로드하고 아래의 **연필을 클릭합니다.**

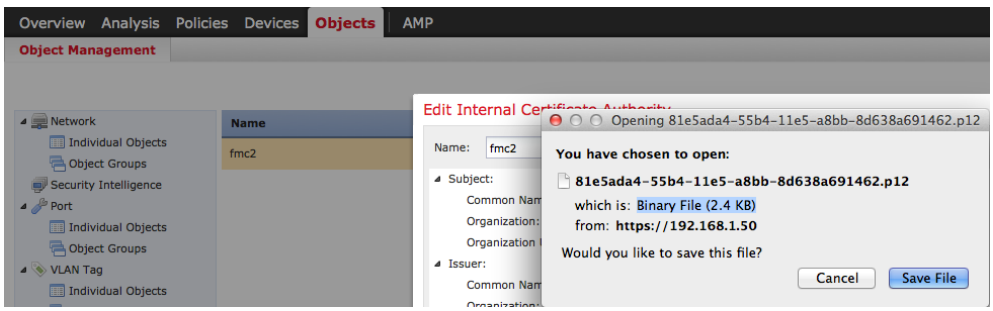
4단계 **Download(다운로드)**를 선택합니다.



5단계 암호화 비밀번호를 입력한 후 **OK(확인)**를 클릭합니다. 이 예에서는 cisco123이 사용되었습니다.

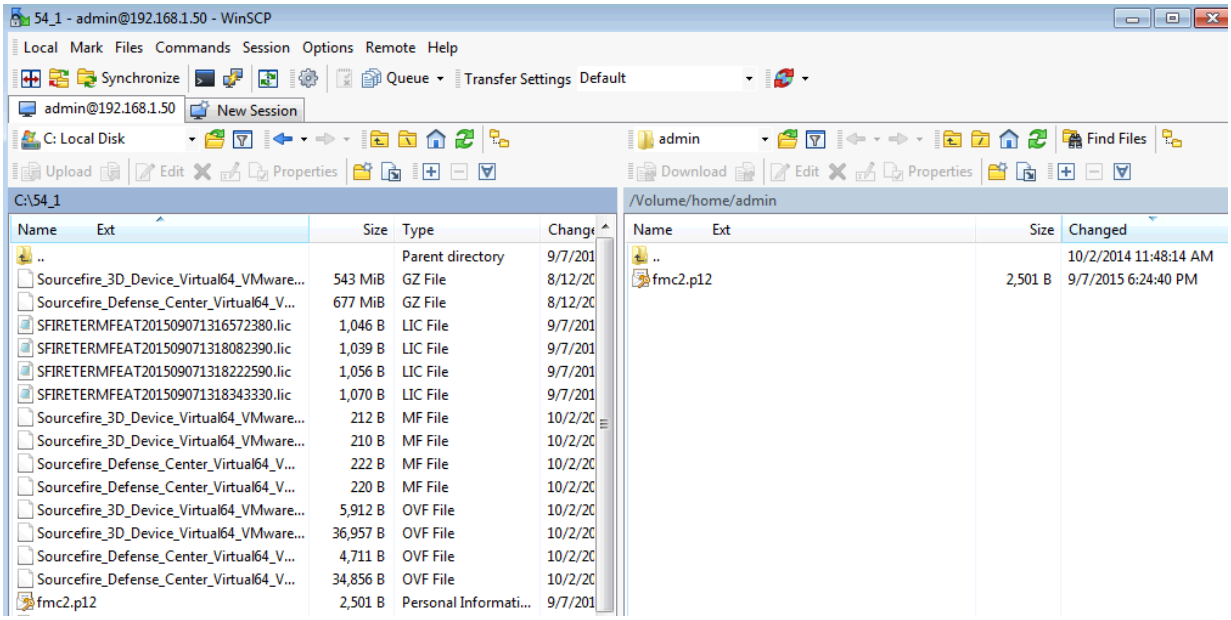


6단계 p12 파일을 로컬에 저장합니다.



7단계 보다 쉽게 작업할 수 있도록 .p12 파일 이름을 변경합니다. 이 예에서는 파일 이름을 fmc2.p12로 변경했습니다.

8단계 winSCP 또는 다른 방법을 사용하여 파일을 FireSIGHT Management Console로 업로드합니다.



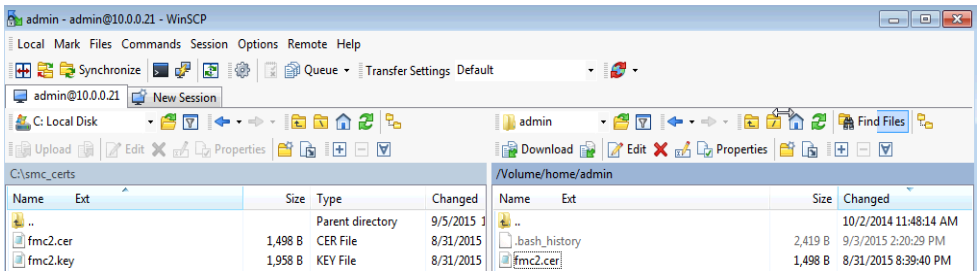
9단계 FireSIGHT Management Console에 SSH로 접속합니다.

10단계 다음 명령을 입력하여 .p12 파일을 CER 및 KEY 파일로 변환합니다.

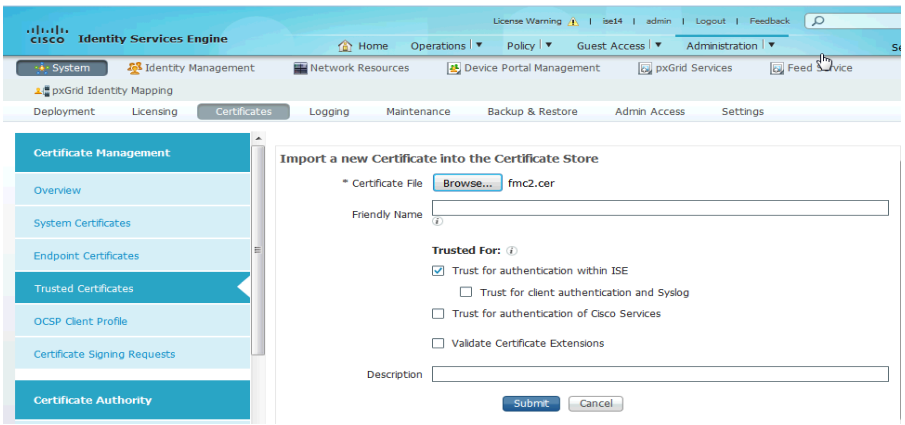
참고: CER 및 KEY 파일 이름은 임의로 지정됩니다. original.p12 파일의 이름이 fmc2.p12로 변경되었습니다.

```
sudo openssl pkcs12 -nokeys -clcerts -in fmc2.p12 -out fmc2.cer
Enter Import Password:
MAC verified OK
admin@sd:~$



sudo openssl pkcs12 -nocerts -in fmc2.p12 -out fmc2.key
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
admin@sd:~$
```

11단계 winSCP를 사용하여 fmc2.cer 및 fmc2.key 파일을 FireSIGHT Management Center에서 로컬 PC로 복사했습니다.



12단계 FireSIGHT Management 내부 CA 공용 인증서를 ISE 인증서 신뢰 저장소로 내보냈습니다. **Administration(관리)->System(시스템)->Certificates(인증서)->Trusted Certificates(신뢰할 수 있는 인증서)->Browse(찾아보기)**를 선택하고 **fmc2.cer**을 업로드합니다.

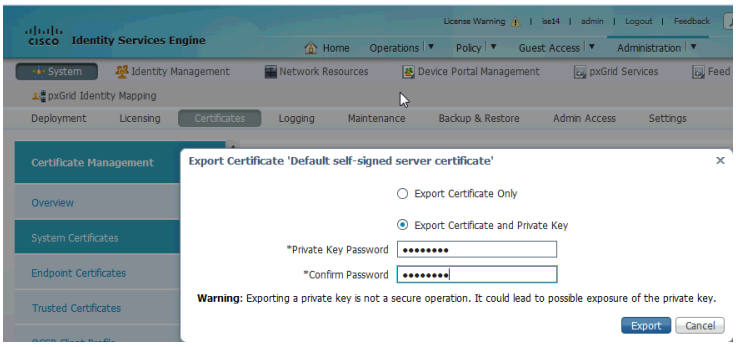


13단계 **"Trust for authentication within ISE(ISE 내의 인증 신뢰)"를 활성화한 후 Submit(제출)를 클릭합니다.**

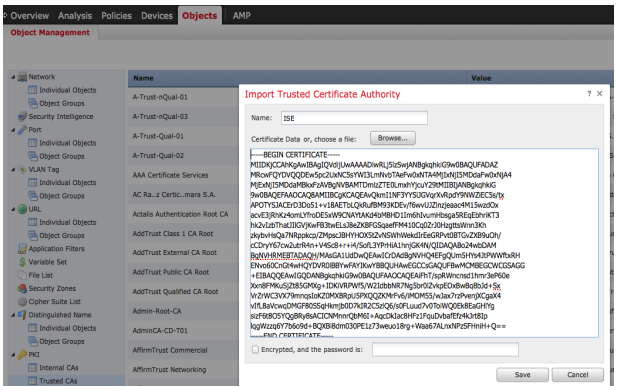
14단계 ISE ID 셀프 서명된 공용 인증서 및 개인 키를 모두 ISE의 신뢰할 수 있는 인증서 저장소에서 내보냅니다. ISE ID 셀프 서명된 공용 인증서를 FireSIGHT Management의 신뢰할 수 있는 CA 저장소로 내보내기만 하면 됩니다. FireSIGHT Management Console이 이 인증서를 신뢰할 수 있는 인증서로 인식합니다.

Administration(관리)->System(시스템)->Certificates(인증서)->Certificate Management(인증서 관리)->Trusted Certificates(신뢰할 수 있는 인증서)를 클릭하고 ISE 인증서를 선택한 후 공개 및 개인 키를 모두 내보내고 비밀번호를 제공합니다.

참고: 이 절차는 ISE 2.0에서도 동일합니다.

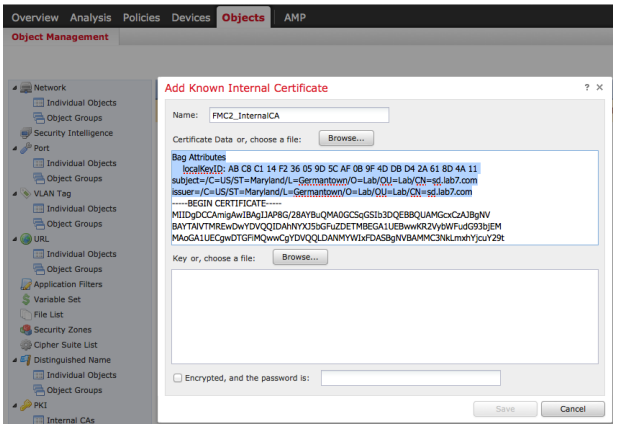


15단계 ISE 셀프 서명된 ID 인증서를 FireSIGHT Management의 신뢰할 수 있는 CA 저장소로 가져옵니다. **Objects(개체)->Object Management(개체 관리)->PKI ->Trusted CAs(신뢰할 수 있는 CA)->Add Trusted CA(신뢰할 수 있는 CA 추가)를 선택한 후 이름을 입력하고 Save(저장)를 클릭합니다.**

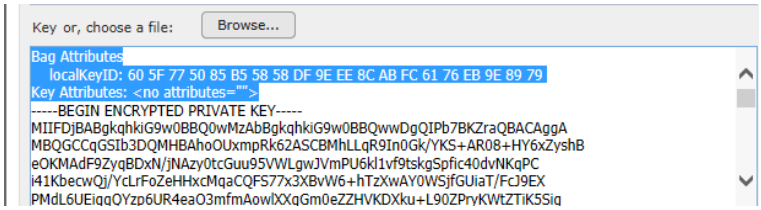


16단계 FireSIGHT Management 내부 CA 공개/개인 키 쌍을 FireSIGHT Management Center의 내부 인증서 저장소로 가져옵니다.
Objects(개체)->Object Management(개체 관리)->PKI->Internal Certs(내부 인증서)->Add Internal Cert(내부 인증서 추가)를 선택합니다.
개인 키에 대해서도 동일한 절차를 수행합니다.

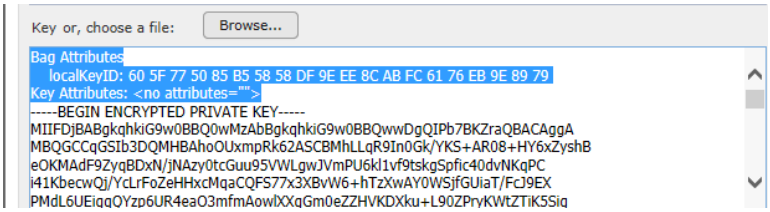
참고: ----Begin Certificates가 표시될 때까지 Bag 특성을 삭제하십시오.



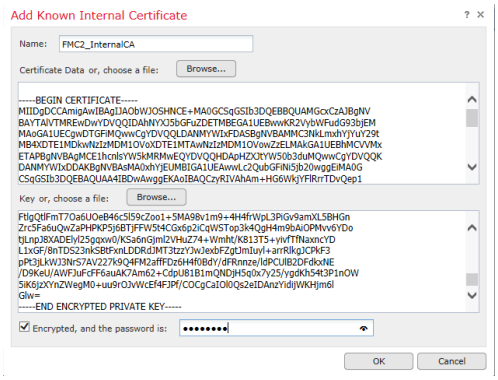
17단계 "---Begin..." 직전까지 키 파일의 Bag 특성을 삭제합니다.



18단계 또한 </no>를 삭제하고 암호화된 비밀번호를 입력합니다.



19단계 다음과 같이 표시되어야 합니다. OK(확인)를 클릭하여 완료합니다.



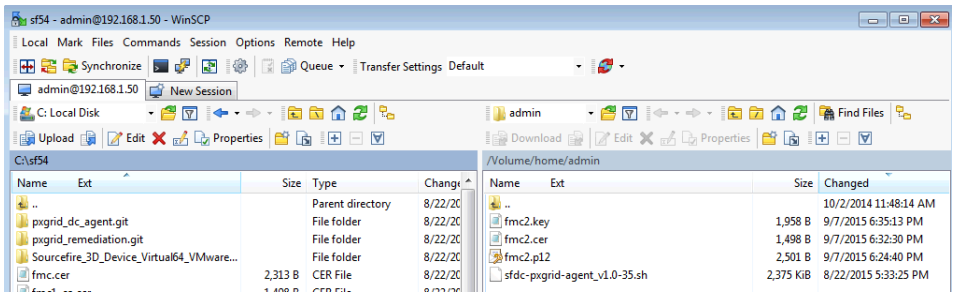
셀프 서명된 인증서를 사용하여 pxGrid 에이전트 구성

pxGrid 에이전트는 인증서 컨피그레이션 및 FireSIGHT Management Center와 ISE pxGrid 노드 간의 통신을 담당합니다. ISE pxGrid 노드의 IP 주소가 필요합니다. 다음 단계를 위해 FireSIGHT Management Center의 공용 인증서 및 키 파일이 필요합니다.

FireSIGHT Management Center의 공용 인증서가 호스트 인증서로 사용됩니다. ISE ID 셀프 서명된 인증서가 CA 인증서로 사용됩니다.

FireSIGHT Management Center의 개인 키 파일이 호스트 키입니다. 키 비밀번호도 필요합니다.

1단계 winSCP 또는 선택한 다른 SCP/SFTP 클라이언트를 사용하여 pxGrid 에이전트를 FireSIGHT Management Console에 업로드합니다.

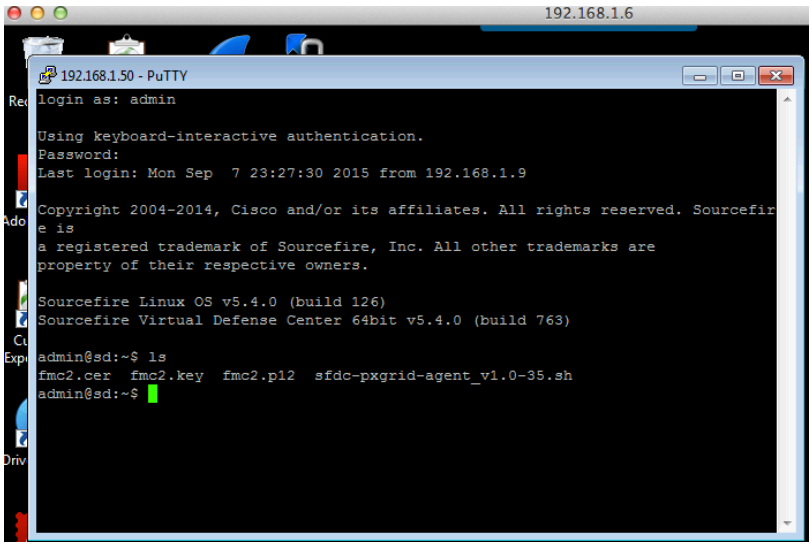


2단계 winSCP 또는 다른 방법을 사용하여 FireSIGHT 내부 CA 공용 인증서, 내부 CA 키를 FireSIGHT MC/Volume/home/admin에 업로드합니다.

참고: 대문자/소문자 구문이 유지됩니다.

3단계 FireSIGHT Management Center에 SSH로 접속하여 다음을 입력합니다.

```
sudo bash sfdc-pxgrid_agent_v1.0.35.sh
```

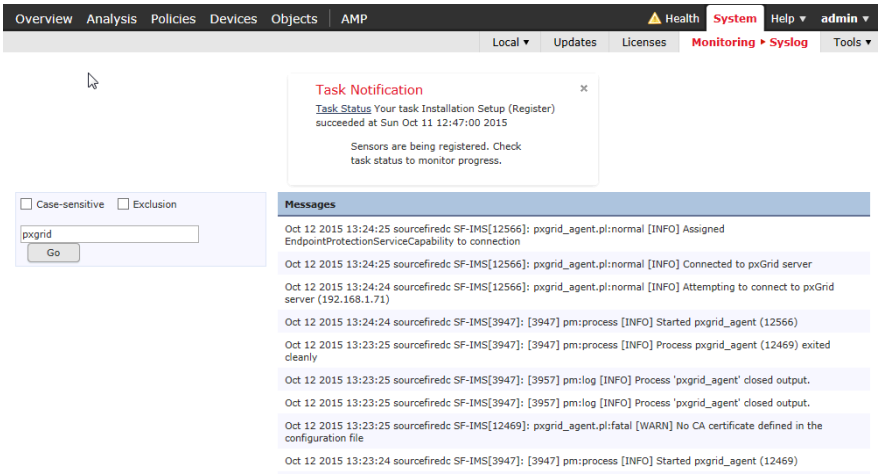


샘플 스크립트는 아래를 참조하십시오.

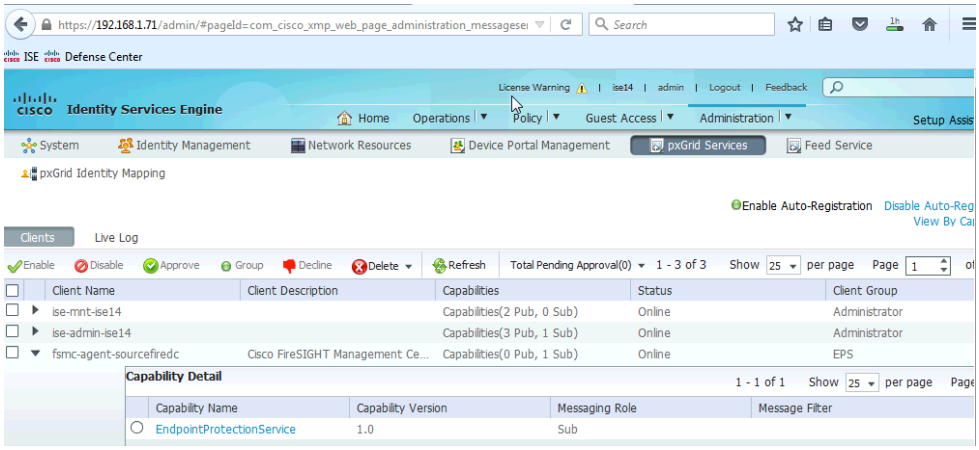
```
Verifying archive integrity... All good.
Uncompressing Cisco pxGrid Agent Installer......
Installing the agent...
Installing the pxGrid libraries and Perl module...
Setting up the agent to be managed by PM...
Installation done!

Configuring pxGrid...

Below you will be asked a series of questions relating to your pxGrid install
and the files supporting it. Health alerts WILL be generated by PM until the
configuration is completed, however. The answers to these questions will
populate the /etc/sf/pxgrid/pxgrid.conf configuration file, which can be
manually modified later at any time. A configuration example is provided in the
same directory with the filename pxgrid.conf.example.


To get this all to work, the agent will need to connect to a pxGrid server.
This is typically your Cisco Identity Services Engine instance, which must also
have the pxGrid service enabled.

What is the IP address of your pxGrid server
> 192.168.1.71

Every agent connecting to pxGrid must have a unique host certificate which will
be used to identify the agent host. Associated key and CA certs must also be
provided.

What is the full path and filename to the host certificate?
```

```
> /Volume/home/admin/fmc2.cer
What is the full path and filename to the host key?
> /Volume/home/admin/fmc2.key
What is the host key password?
> cisco123
What is the full path and filename to the CA certificate?
> /Volume/home/admin/ise14lab.pem

Configuration witten to /etc/sf/pxgrid/pxgrid.conf
```

4단계 **System(시스템)->Monitoring(모니터링)->Syslog**를 선택하여 FireSIGHT Management Center가 성공적으로 ISE pxGrid 노드에 클라이언트로 등록되었고 EPS 주제를 서브스크립션했는지 확인합니다.



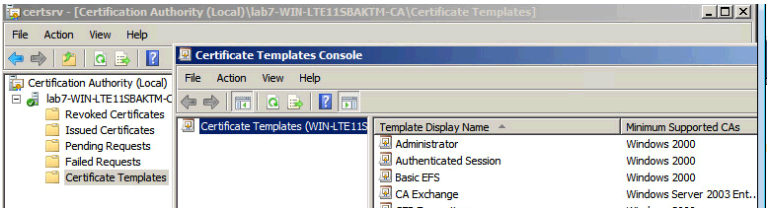
5단계 ISE에서 보려면 **Administration(관리)->pxGrid Services(pxGrids 서비스)**를 선택합니다. FireSIGHT Management Console이 ISE pxGrid 노드 EndpointProtectionService 기능에 등록되었습니다.



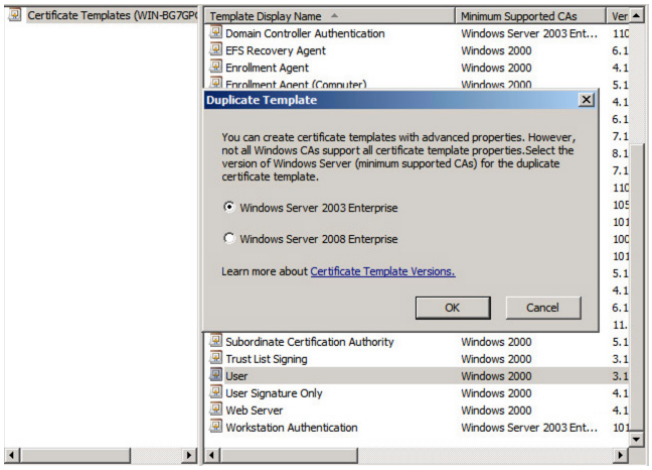
CA 서명 작업에 대한 사용자 지정된 pxGrid 템플릿

pxGrid 클라이언트, FireSIGHT Management Center 및 ISE pxGrid 노드 간의 pxGrid 작업에는 클라이언트 인증 및 서버 인증 모두의 EKU(Enhanced Key Usage)가 있는 사용자 지정된 pxGrid 템플릿이 필요합니다. 이 템플릿은 FireSIGHT Management Center 및 ISE pxGrid 노드가 동일한 CA에서 서명된 CA(Certificate Authority) 서명 환경에 필요합니다.

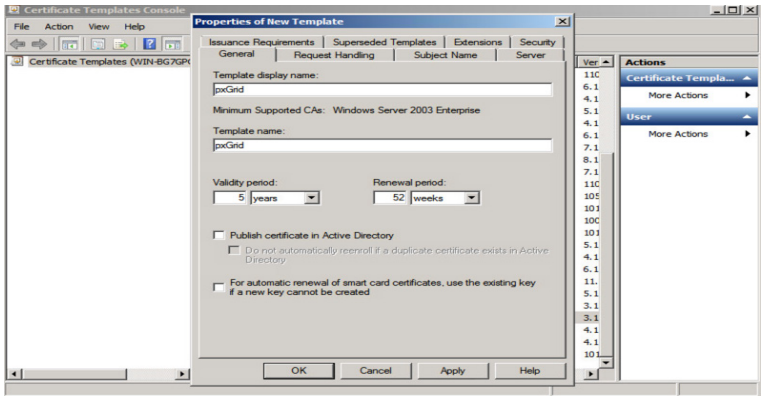
1단계 **Administrative Tools(관리 툴)->Certificate Authority(인증 기관)-> CA 서버 옆의"+" 드롭다운을 선택하고 Certificate Templates(인증서 템플릿)를 마우스 오른쪽 버튼으로 클릭한 후 Manage(관리)를 클릭합니다.**



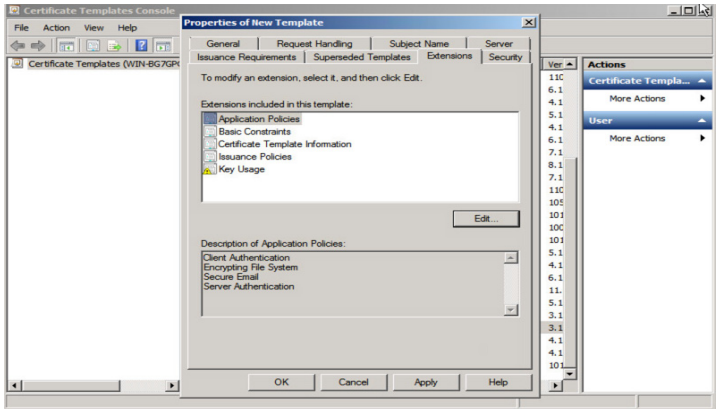
2단계 **마우스 오른쪽 버튼으로 Duplicate User template 클릭->Windows 2003 Enterprise->OK 클릭**



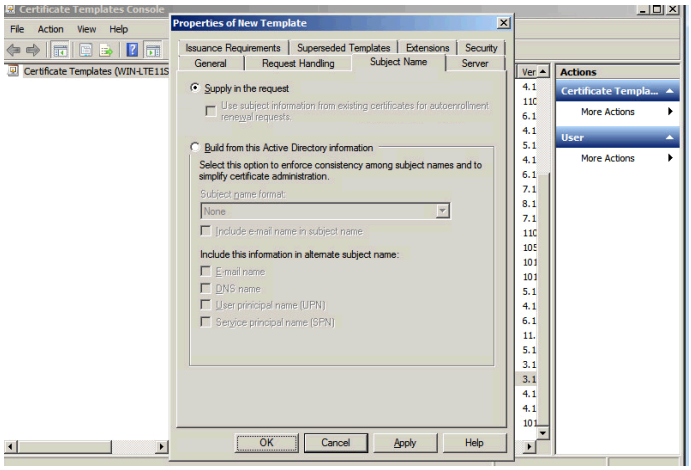
3단계 인증서 템플릿의 이름을 입력하고"Publish certificate in Active Directory(Active Directory에 인증서 게시" 선택을 취소한 후 유효 기간 및 갱신 기간을 제공합니다.



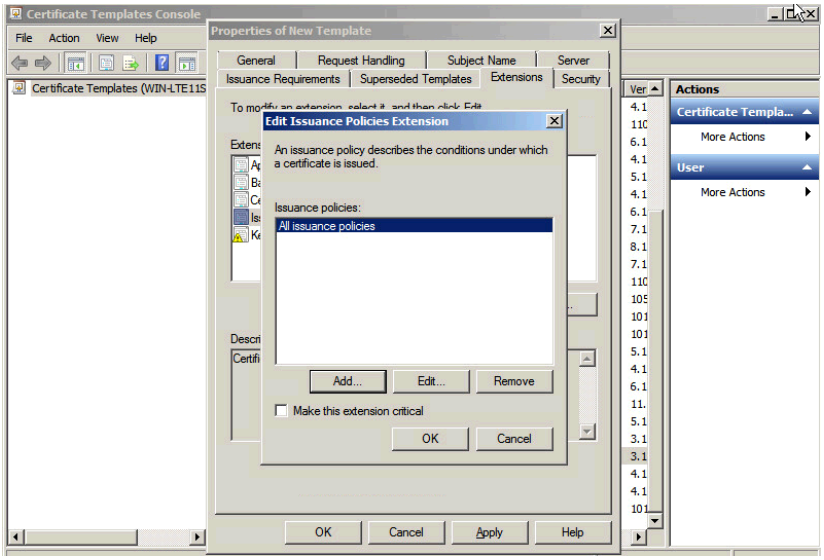
4단계 Extensions(확장)->Add(추가)->Server Authentication(서버 인증)->OK(확인)->Apply(적용)를 클릭합니다.



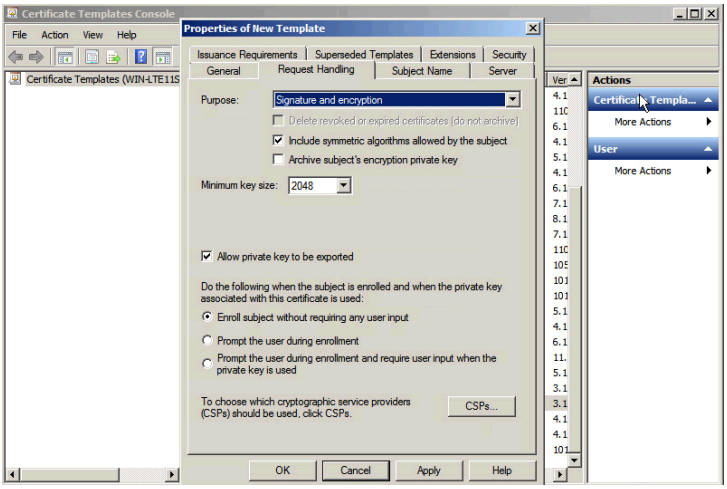
5단계 Subject Name(제목 이름)을 클릭하고 Supply in request(요청 시 공급)를 활성화합니다.



6단계 **Extensions(확장)->Issuance Policies(발급 정책)->Edit(편집)->All Issuance Policies(모든 발급 정책)를 클릭합니다.**

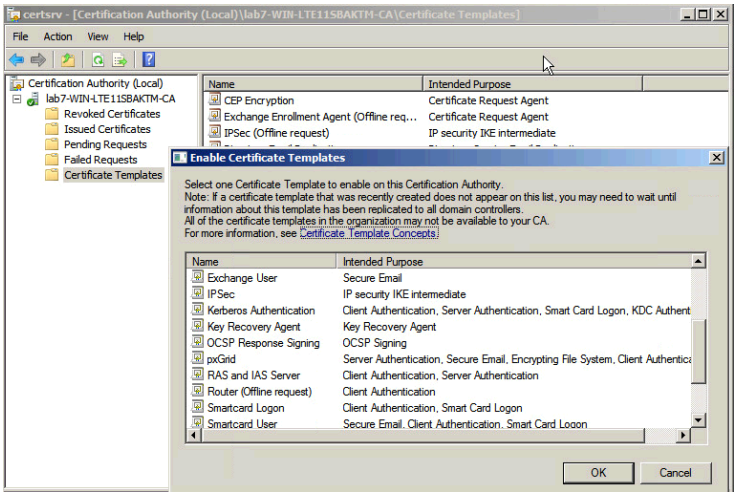


7단계 **Request Handling(요청 처리)에 대한 기본값을 그대로 둡니다.**

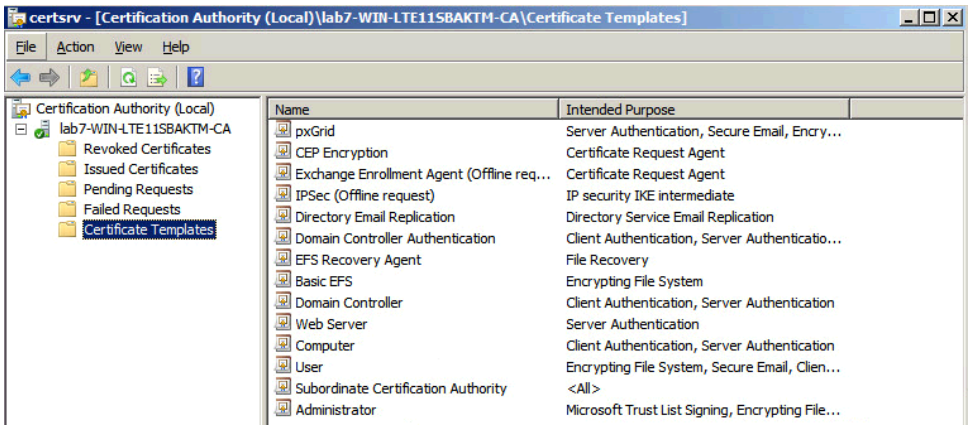


8단계 **Certificate templates(인증서 템플릿)를 마우스 오른쪽 버튼으로 클릭합니다.**

9단계 **New Template to issue(발급할 새 템플릿)를 선택한 후 pxGrid를 선택합니다.**



10단계 pxGrid 템플릿이 표시되어야 합니다.



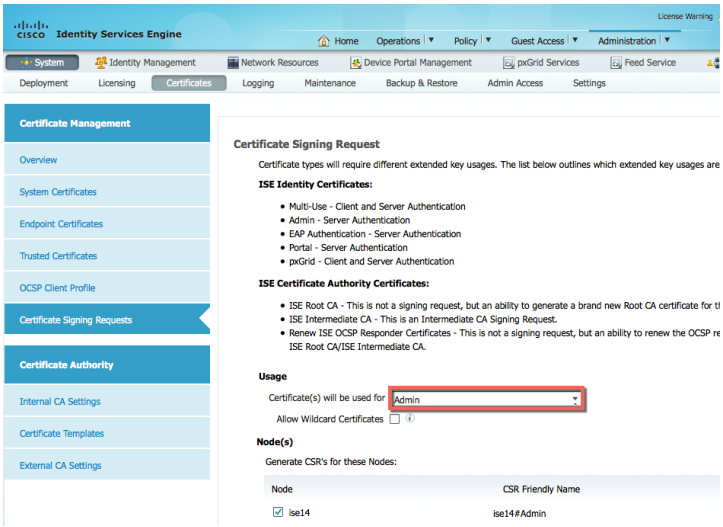
pxGrid를 사용하는 독립형 환경에서 CA 서명 인증서에 대한 ISE 구성

이 섹션에서는 CA(Certificate Authority) 서명 환경에 대한 ISE pxGrid 노드를 구성합니다. 먼저, "pxGrid" CSR 요청이 ISE 노드에서 생성되고 pxGrid 사용자 지정 템플릿을 사용하여 CA 서버에서 서명됩니다. 인증서는 초기 ISE CSR 요청에 바인딩됩니다.

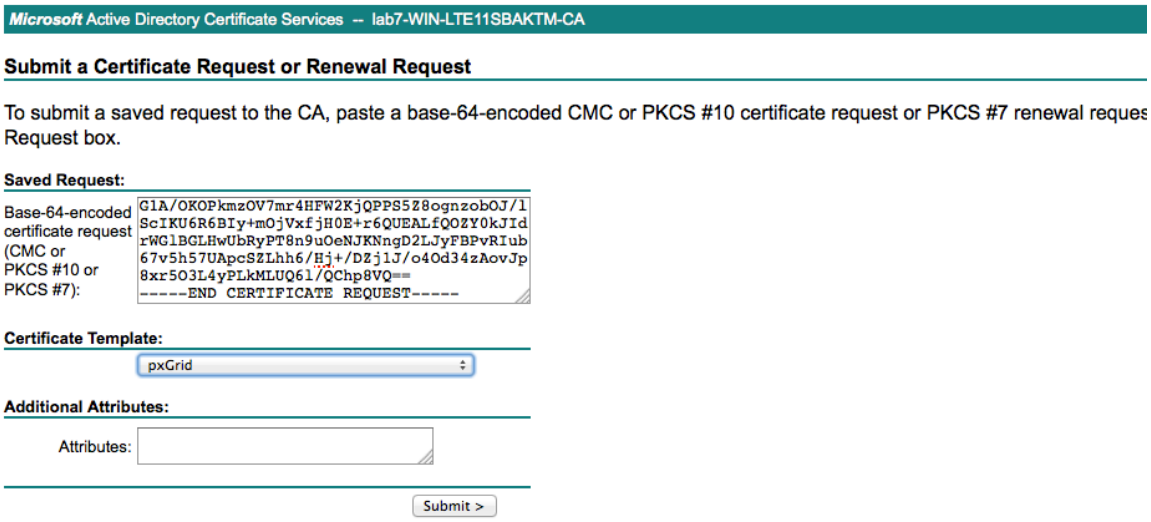
CA 루트 인증서를 ISE 인증서의 신뢰할 수 있는 저장소로 가져옵니다. ISE ID 인증서를 ISE 인증서 시스템 저장소로 내보냅니다. ISE 노드가 pxGrid 작업에 사용할 수 있도록 활성화됩니다.

1단계 ISE pxGrid 노드가 될 ISE 노드에 대한 CSR 요청을 생성합니다. **Administration(관리)->System(시스템)->Certificates(인증서)->Certificate Signing Request(인증서 서명 요청)->Generate(생성)**

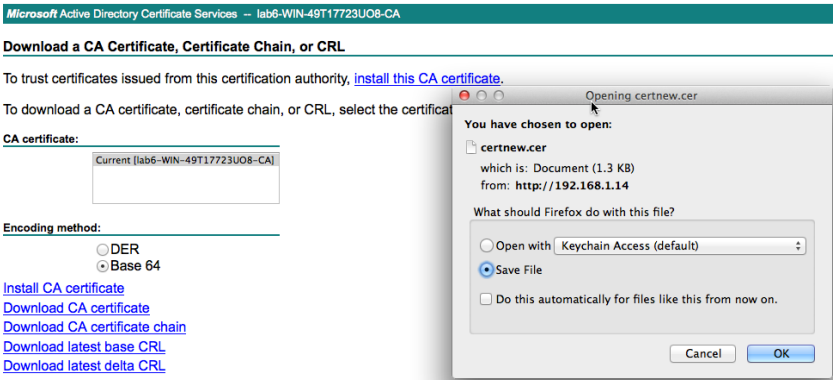
참고: 템플릿이 pxGrid 사용자 지정 템플릿인 경우에는 certificate usage(인증서 사용)가 admin(관리), multipurpose(다목적) 또는 pxGrid일 수 있습니다.



2단계 사용자 지정된 pxGrid 템플릿을 선택하여 CSR 정보를 복사한 후 **Request a certificate(인증서 요청)->Advanced Certificate request(고급 인증서 요청)**에 붙여넣고 **Submit(제출)**를 클릭합니다.

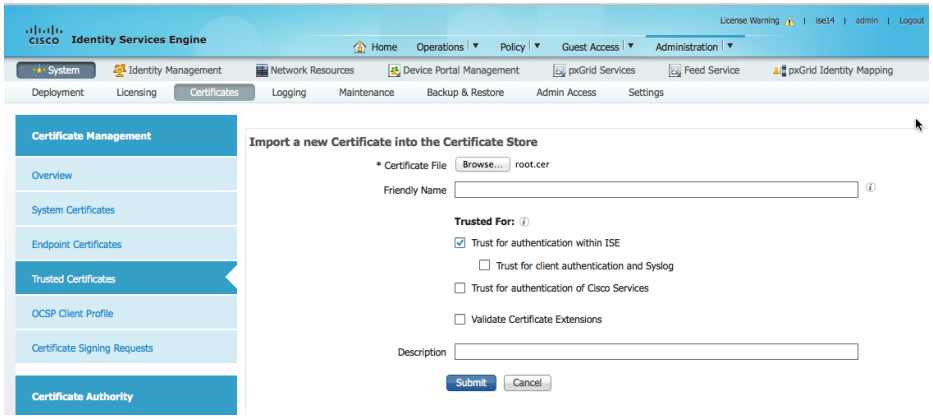


3단계 CA 루트를 기본 64 인코딩 형식으로 다운로드합니다.



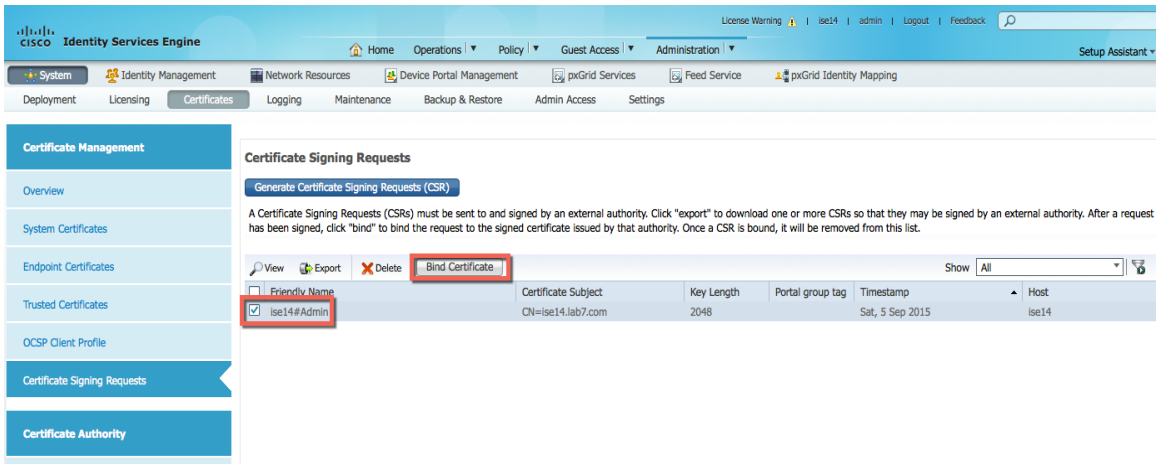
4단계 CA 루트를 ISE 인증서의 신뢰할 수 있는 시스템 저장소로 업로드합니다.

Administration(관리)->System(시스템)->Certificates(인증서)->Trusted Certificates(신뢰할 수 있는 인증서)를 선택하고 CA 루트 인증서를 업로드합니다.

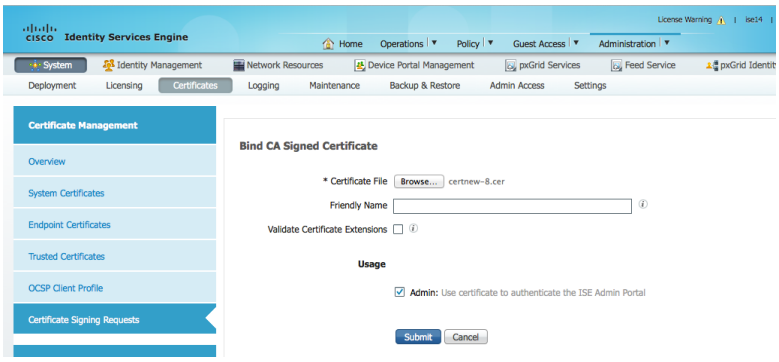


5단계 **"Trust for authentication within ISE(ISE 내의 인증 신뢰)"를 활성화한 후 Submit(제출)를 클릭합니다.**

6단계 ISE pxGrid 노드 인증서를 ISE 인증서 시스템 저장소로 업로드합니다. **Administration(관리)->System(시스템)->Certificate Signing Requests(인증서 서명 요청)를 선택하고 인증서를 CSR 요청에 바인딩합니다.**

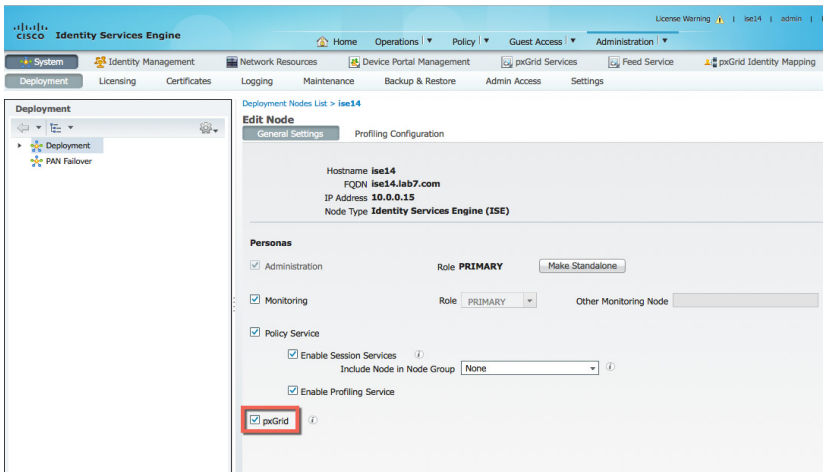


7단계 **ISE pxGrid 노드 인증서를 찾아서 업로드한 후 Submit(제출)를 클릭합니다.**



8단계 ISE 노드에서 pxGrid를 활성화합니다.

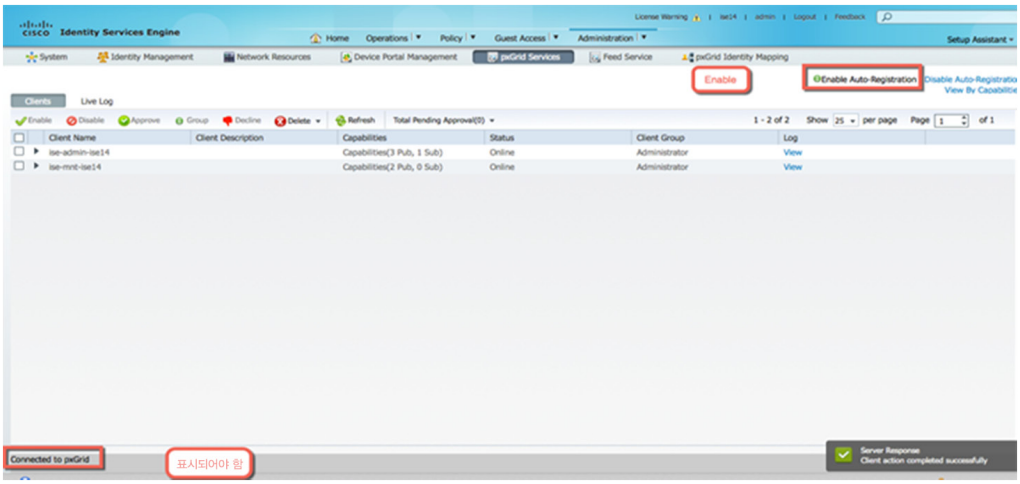
Administration(관리)->System(시스템)->Deployment(구축)를 선택하고 ISE 노드를 강조 표시한 후 pxGrid를 활성화합니다.



9단계 pxGrid 서비스가 실행 중인지 확인하고 "**Enable Auto Registration(자동 등록 활성화)**"을 활성화합니다.

Administration(관리)->pxGrid services(pxGrid 서비스)

참고: pxGrid 서비스가 표시되는 데 몇 초가 소요될 수 있습니다.



CA 서명 인증서에 대한 FireSIGHT Management Center 구성

이 섹션에서는 CA(Certificate Authority) 서명 작업을 위해 FMC(FireSIGHT Management Center)를 구성합니다. FMC(FireSIGHT Management Center) Console에서 FireSIGHT Management Center 개인 키 및 CSR 요청이 생성됩니다. CA 서버에서 CSR 요청을 서명하고 사용자 지정된 pxGrid 템플릿을 사용하는 FMC ID 인증서를 제공합니다.

FMC 인증서 및 FMC 키가 FMC 내부 인증서 저장소에 업로드됩니다. CA 루트 인증서가 FMC의 신뢰할 수 있는 CA 저장소에 업로드됩니다.

1단계 FireSIGHT 개인 키를 생성합니다.

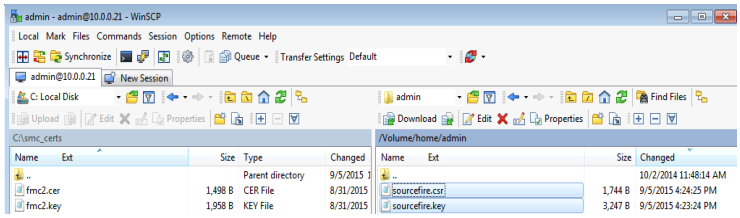
참고: 여기의 비밀번호가 pxGrid 에이전트 컨피그레이션에 정의됩니다.

```
openssl genrsa -des3 -out sourcefire.key 4096
```

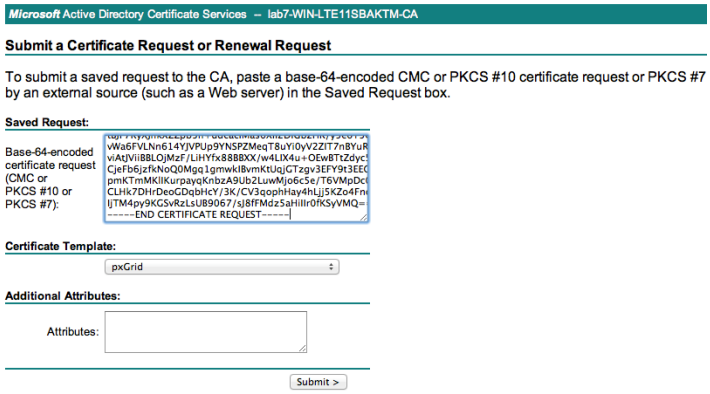
2단계 CSR 요청을 생성합니다.

```
openssl req -new -key sourcefire.key -out sourcefire.csr
```

3단계 winSCP를 사용하여 파일을 FMC(FireSIGHT Management Center)에서 PC에 로컬로 복사합니다.

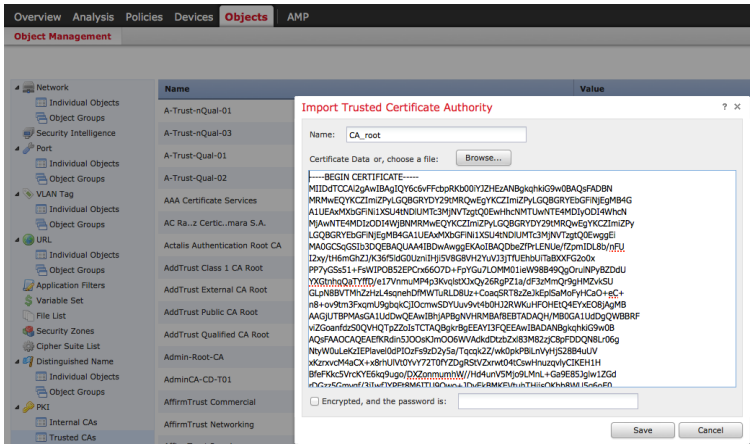


4단계 사용자 지정된 pxGrid 템플릿을 사용하여 FMC CSR 요청을 복사한 후 Request a certificate(인증서 요청)->Advanced User request(고급 사용자 요청)에 붙여넣은 다음 제출합니다. 인증서를 기본 64 인코딩 형식으로 다운로드합니다.

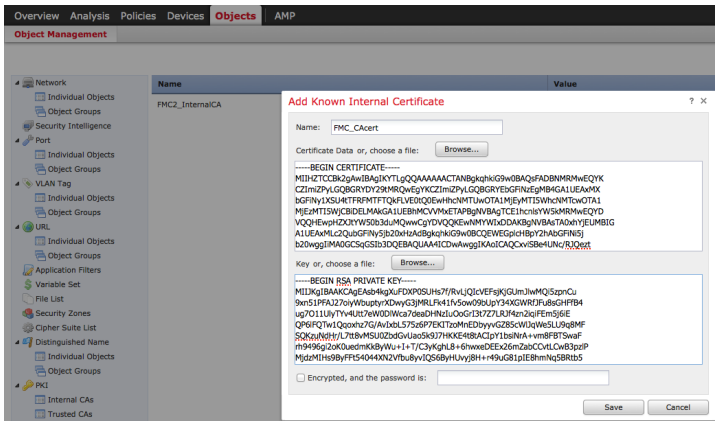


5단계 CA 루트 인증서를 기본 64 인코딩 형식으로 다운로드합니다.

6단계 CA 루트 인증서를 FireSIGHT Management의 신뢰할 수 있는 CA 저장소로 업로드합니다. **Objects(개체)->Object Management(개체 관리)->PKI->Trusted CAs(신뢰할 수 있는 CA)->Add Trusted CA(신뢰할 수 있는 CA 추가)를 선택하고 이름을 제공한 후 루트 CA 인증서를 업로드하고 Save(저장)를 클릭합니다.**



7단계 FireSIGHT Management Center 공용 인증서 및 개인 키를 FMC 내부 인증서 저장소에 업로드합니다. **Objects(개체)->Object Management(개체 관리)->PKI->Internal Certs(내부 인증서)를 선택하고 Sourcefire CER 파일 및 Sourcefire KEY 파일을 추가한 후 Save(저장)를 클릭합니다.**



CA 서명 인증서를 사용하여 pxGrid 에이전트 구성

pxGrid 에이전트는 인증서 컨피그레이션 및 FireSIGHT Management Center와 ISE pxGrid 노드 간의 통신을 담당합니다. ISE pxGrid 노드의 IP 주소가 필요합니다. FireSIGHT Management Center의 공용 인증서 및 키 파일이 필요합니다.

FireSIGHT Management Center의 공용 인증서가 호스트 인증서로 사용됩니다. CA 루트 인증서가 CA 인증서로 사용됩니다.

FireSIGHT 키 파일이 호스트 키입니다. 키 비밀번호도 필요합니다.

1단계 winSCP를 사용하여 pxGrid 에이전트를 FireSIGHT Management Console에 업로드합니다.

2단계 winSCP 또는 다른 방법을 사용하여 FireSIGHT 공용 인증서, FireSIGHT CA 키 및 CA 루트 인증서를 FireSIGHT MC /Volume/home/admin에 업로드합니다.

참고: 대문자/소문자 구문이 유지됩니다.

3단계 FireSIGHT Management Center에 SSH로 접속하여 다음을 입력합니다.

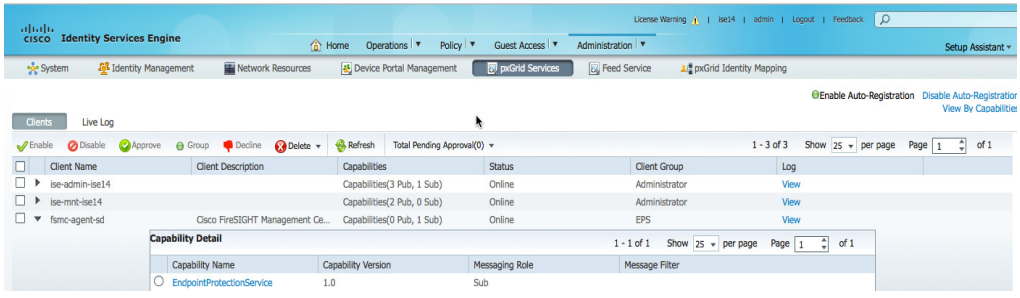
```
sudo bash sfdc-pxgrid_agent_v1.0.35.sh
```

샘플 스크립트는 아래를 참조하십시오.

```
Verifying archive integrity... All good.
Uncompressing Cisco pxGrid Agent Installer......
Installing the agent...
Installing the pxGrid libraries and Perl module...
Setting up the agent to be managed by PM...
Installation done!

Configuring pxGrid...

Below you will be asked a series of questions relating to your pxGrid install
and the files supporting it. Health alerts WILL be generated by PM until the
configuration is completed, however. The answers to these questions will
populate the /etc/sf/pxgrid/pxgrid.conf configuration file, which can be
manually modified later at any time. A configuration example is provided in the
same directory with the filename pxgrid.conf.example.


To get this all to work, the agent will need to connect to a pxGrid server.
This is typically your Cisco Identity Services Engine instance, which must also
have the pxGrid service enabled.

What is the IP address of your pxGrid server
> 10.0.0.0.15

Every agent connecting to pxGrid must have a unique host certificate which will
be used to identify the agent host. Associated key and CA certs must also be
provided.

What is the full path and filename to the host certificate?
> /Volume/home/admin/sourcefire.cer
What is the full path and filename to the host key?
> /Volume/home/admin/sourcefire.key
What is the host key password?
> cisco123
What is the full path and filename to the CA certificate?
> /Volume/home/admin/root.cer

Configuration witten to /etc/sf/pxgrid
```

4단계 FireSIGHT Management Center가 성공적으로 pxGrid 클라이언트로 등록되고 EPS 게시 주제에 서브스크립션되었어야 합니다.

Administration(관리)->pxGrid Services(pxGrid 서비스)를 선택합니다.



FireSIGHT pxGrid 교정 모듈

이 섹션에서는 pxGrid 완화 교정 모듈이 FireSIGHT Management Center에 업로드됩니다. pxGrid 인스턴스가 생성되고 교정 유형이 정의됩니다. 이러한 교정 유형은 각 상관관계 정책에 대한 응답으로 할당되는 경우 pxGrid ANC 기능을 제공합니다.

이러한 교정 유형은 다음으로 구성됩니다.

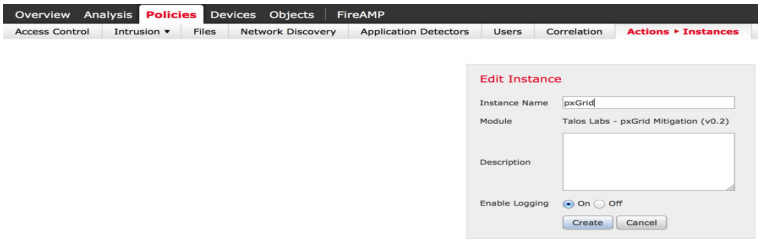
- **격리** - 소스 IP 주소를 기반으로 하여 엔드포인트를 격리합니다.
- **포트 바운스** - 엔드포인트 또는 호스트 포트를 일시적으로 바운스합니다.
- **종료(Terminate)** - 최종 사용자 세션을 종료합니다.
- **종료(Shutdown)** - 호스트 포트 종료를 시작합니다. 이 조치는 스위치 포트 컨피그레이션에 "shutdown" 명령을 삽입합니다.
- **재인증** - 최종 사용자를 재인증합니다.
- **격리 해제** - 엔드포인트의 격리를 해제합니다.

FireSIGHT pxGrid 교정 모듈 업로드

1단계 pxGrid 교정 모듈을 FireSIGHT Management Center에 업로드합니다. **Policies(정책)->Actions(조치)->Remediations(교정)->Modules(모듈)->Install a new module(새 모듈 설치)**을 선택하고 모듈, pxGrid_Mitigation_Remediation_v1.0.tgz 파일을 찾아서 업로드합니다.

새 인스턴스 생성

1단계 새 pxGrid 인스턴스를 생성합니다.
Policies(정책)->Actions(조치)->Remediations(교정)->Instances(인스턴스)->Add a new Instance(새 인스턴스 추가)->Module type(모듈 유형)->Talos Labs - pxGrid mitigation(pxGrid 완화)->Add(추가)->Instance Name(인스턴스 이름)->pxGrid->Create(생성)를 선택합니다.



FireSIGHT pxGrid 완화 유형 생성

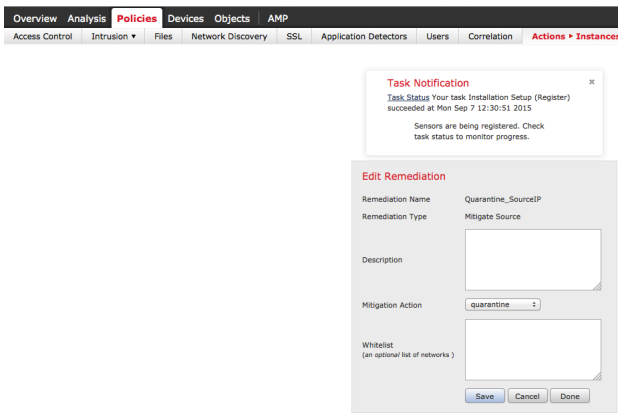
다음과 같은 교정 유형은 엔드포인트에서 교정 작업을 호출하는 상관관계 규칙에 대한 응답으로 할당되는 pxGrid ANC 완화 작업을 정의합니다.

참고: 돋보기를 클릭하여 선택합니다.

격리

소스 완화를 기반으로 하여 격리 완화 조치를 생성합니다.

1단계 **Policies(정책)->Actions(조치)->Remediations(교정)->Modules(모듈)->Talos Labs - pxGrid Mitigation(pxGrid 완화)->구성된 인스턴스 아래의 pxGrid**
2단계 **"돋보기"를 클릭한 후 소스 완화를 기반으로 하여 새 교정 유형을 추가합니다.**
3단계 교정 이름 **Quarantine_SourceIP**를 입력합니다.
4단계 드롭다운 메뉴 목록에서 **quarantine(격리)**을 완화 조치로 선택합니다.
5단계 **Save(저장)**를 클릭합니다.



포트 바운스

소스 완화를 기반으로 하여 포트 바운스 완화 조치를 생성합니다.

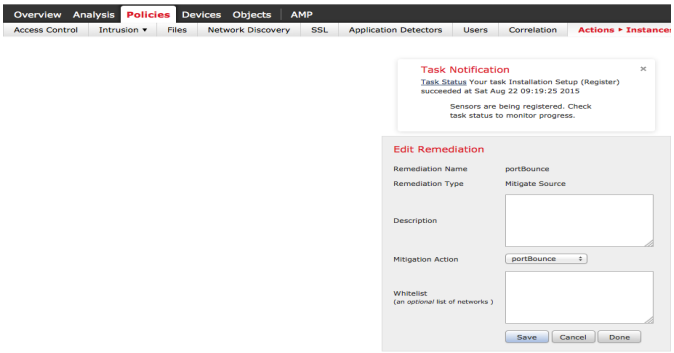
1단계 **Policies(정책)->Actions(조치)->Instances(인스턴스)를 선택하고 구성된 인스턴스 아래의 "pxGrid" 옆에 있는 돋보기를 클릭합니다.**

2단계 드롭다운 메뉴에서 **Mitigate Source(소스 완화)**를 선택하고 **Add(추가)**를 클릭합니다.

3단계 교정 이름 **portBounce**를 입력합니다.

4단계 드롭다운 메뉴 목록에서 **portBounce(포트 바운스)**를 완화 조치로 선택합니다.

5단계 **Save(저장)**를 클릭합니다.



재인증

소스 완화를 기반으로 하여 재인증 완화 조치를 생성합니다.

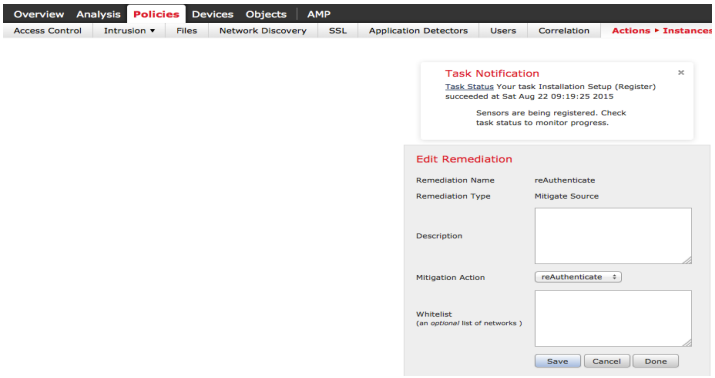
1단계 **Policies(정책)->Actions(조치)->Instances(인스턴스)를 선택하고 구성된 인스턴스 아래의"pxGrid" 옆에 있는 돋보기를 클릭합니다.**

2단계 드롭다운 메뉴에서 **Mitigate Source(소스 완화)**를 선택하고 **Add(추가)**를 클릭합니다.

3단계 교정 이름 **reAuthenticate**를 입력합니다.

4단계 드롭다운 메뉴 목록에서 **reAuthenticate(재인증)**를 완화 조치로 선택합니다.

5단계 **Save(저장)**를 클릭합니다.



종료(shutDown)

소스 완화를 기반으로 하여 종료(shutdown) 완화 조치를 생성합니다.

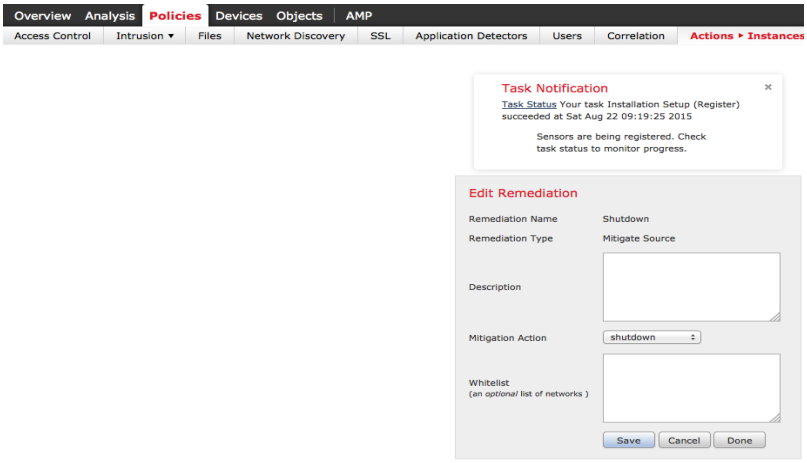
1단계 **Policies(정책)->Actions(조치)->Instances(인스턴스)를 선택하고 구성된 인스턴스 아래의 "pxGrid" 옆에 있는 돋보기를 클릭합니다.**

2단계 드롭다운 메뉴에서 **Mitigate Source(소스 완화)**를 선택하고 **Add(추가)**를 클릭합니다.

3단계 교정 이름 **Shutdown**을 입력합니다.

4단계 드롭다운 메뉴 목록에서 **shutdown(종료)**을 완화 조치로 선택합니다.

5단계 **Save(저장)**를 클릭합니다.



종료(terminate)

소스 완화를 기반으로 하여 종료(terminate) 완화 조치를 생성합니다.

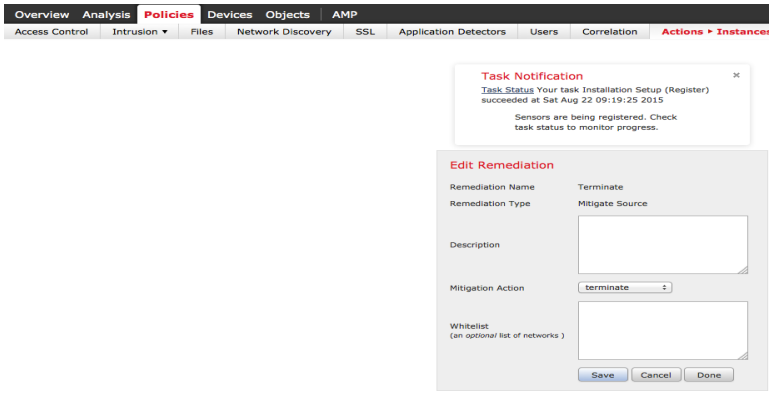
1단계 **Policies(정책)->Actions(조치)->Instances(인스턴스)를 선택하고 구성된 인스턴스 아래의 "pxGrid" 옆에 있는 돋보기를 클릭합니다.**

2단계 드롭다운 메뉴에서 **Mitigate Source(소스 완화)**를 선택하고 **Add(추가)**를 클릭합니다.

3단계 교정 이름 **Terminate**를 입력합니다.

4단계 드롭다운 메뉴 목록에서 **terminate(종료)**를 완화 조치로 선택합니다.

5단계 **Save(저장)**를 클릭합니다.



격리 해제

소스 완화를 기반으로 하여 격리 해제 완화 조치를 생성합니다.

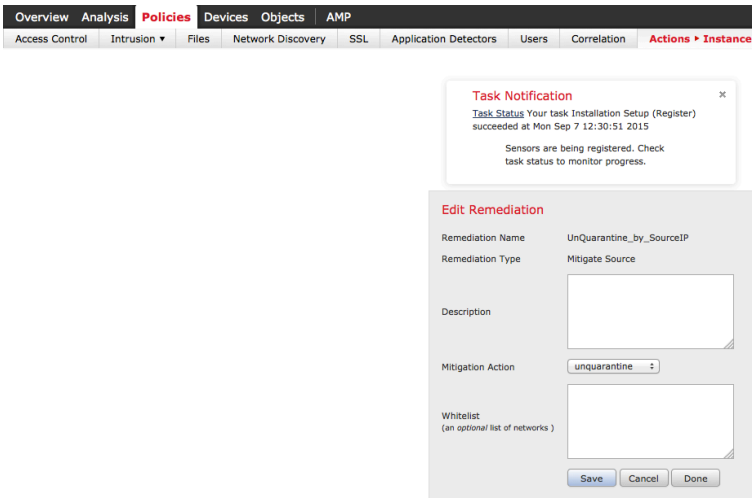
1단계 **Policies(정책)->Actions(조치)->Instances(인스턴스)를 선택하고 구성된 인스턴스 아래의 "pxGrid" 옆에 있는 돋보기를 클릭합니다.**

2단계 드롭다운 메뉴에서 **Mitigate Source(소스 완화)**를 선택하고 **Add(추가)**를 클릭합니다.

3단계 교정 이름 **UnQuarantine_SourceIP**를 입력합니다.

4단계 드롭다운 메뉴 목록에서 **unquarantine(격리 해제)**을 완화 조치로 선택합니다.

5단계 **Save(저장)**를 클릭합니다.



FireSIGHT pxGrid 침입 정책

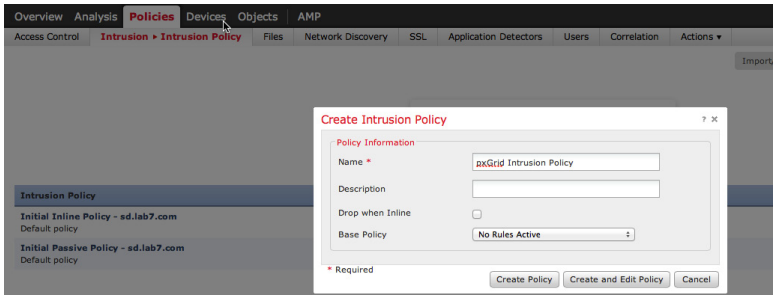
이 섹션에서는 pxGrid 침입 정책이 생성되고 FireSIGHT 센서에 구축됩니다. 이 정책에는 "SERVER IIS CMD.EXE 액세스" 규칙이 포함됩니다. 이 액세스 규칙은 최종 사용자가 브라우저에 www.yahoo.com/cmd.exe를 입력할 때 격리 해제 상관관계 정책을 제외한 상관관계 정책을 기반으로 하여 침입 이벤트를 생성합니다.

1단계 **Policies(정책)->Intrusion(침입)->Intrusion Policy(침입 정책)**로 이동합니다.

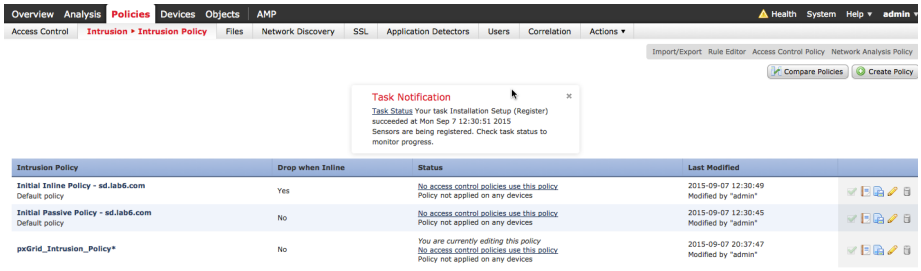
2단계 **Create Policy(정책 생성)**를 클릭합니다.

3단계 새 정책의 이름을 **pxGrid_Intrusion_Policy**로 지정합니다.

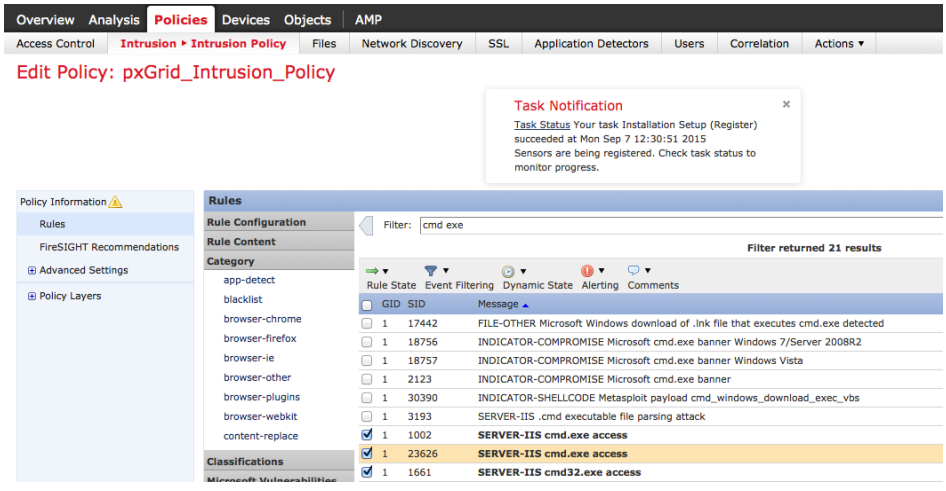
4단계 **Create Policy(정책 생성)**를 클릭합니다.



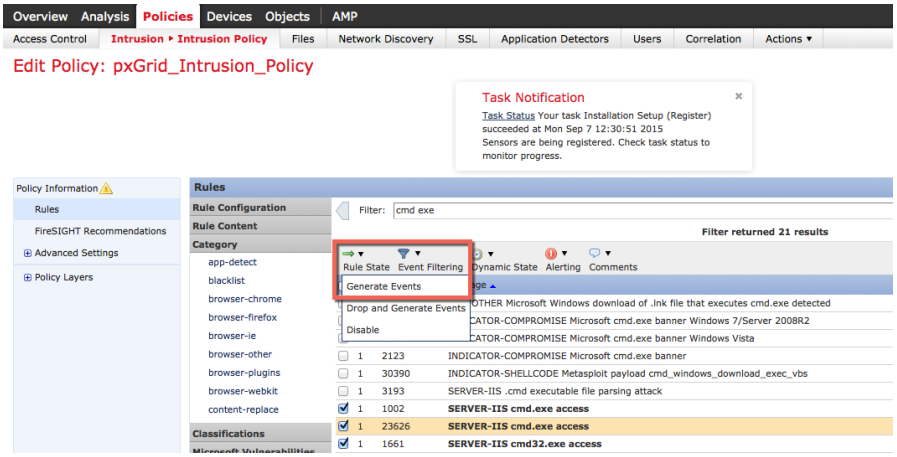
5단계 편집할 **pxGrid_Intrusion_Policy**를 클릭합니다.



6단계 **Rules(규칙)**을 클릭하고 **cmd.exe**로 필터링한 후 아래의 규칙을 선택합니다.

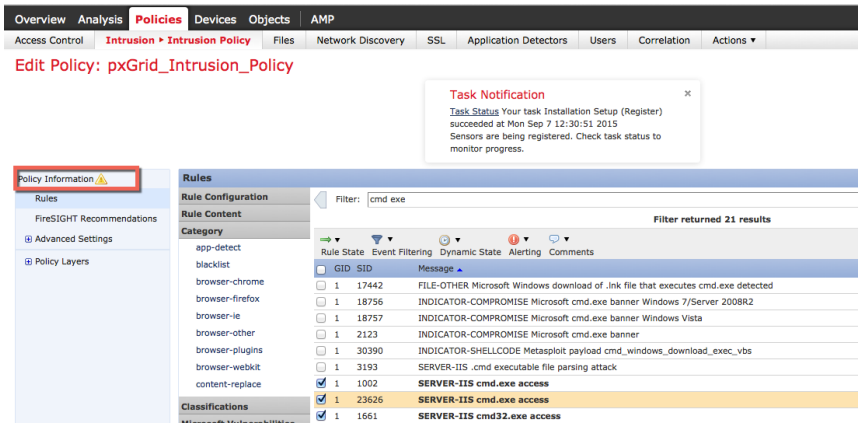


7단계 **Rule State(규칙 상태)->Generate Events(이벤트 생성)**를 클릭한 후 **OK(확인)**를 클릭합니다.

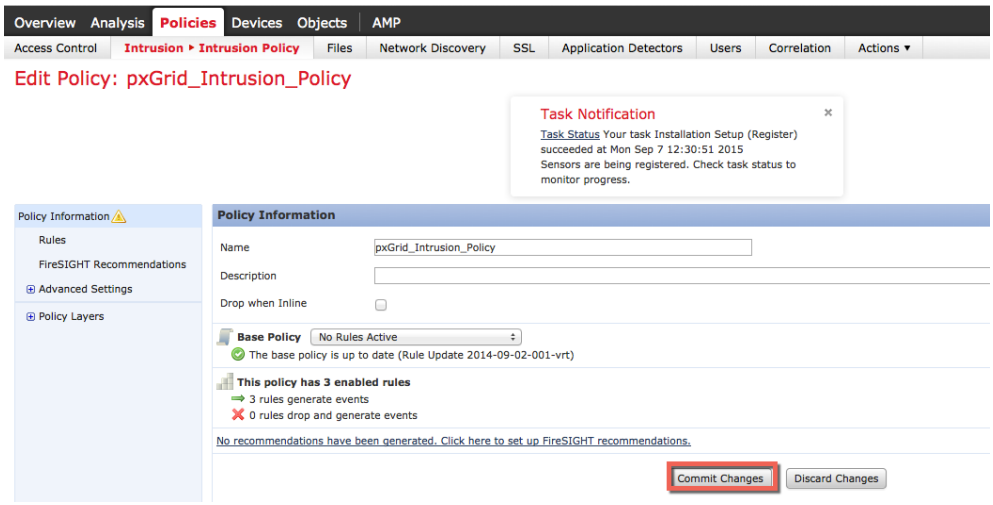


8단계 "successfully set the rule state for 3 rules(3개 규칙에 대한 규칙 상태가 성공적으로 설정됨)"라는 성공 메시지가 표시되어야 합니다.

9단계 **Policy Information(정책 정보)**를 클릭합니다.



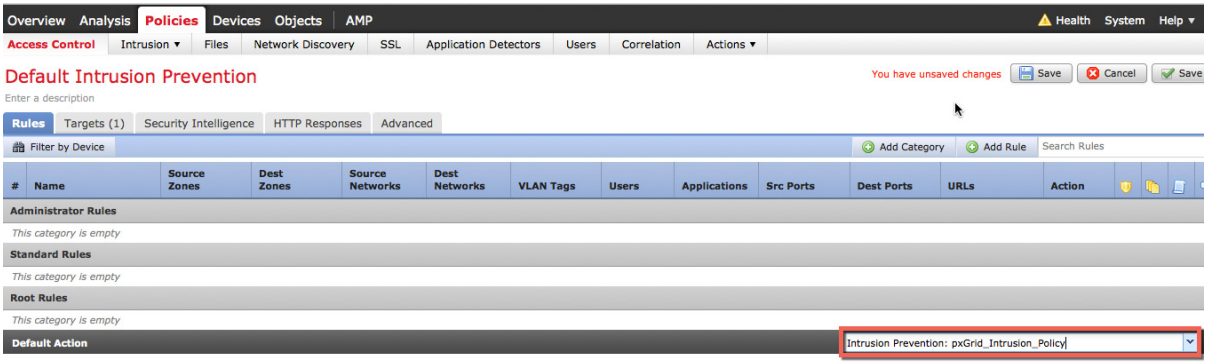
10단계 그런 다음 **"Commit Changes(변경 사항 커밋)"**를 클릭합니다.



11단계 **OK**(확인)를 클릭합니다.

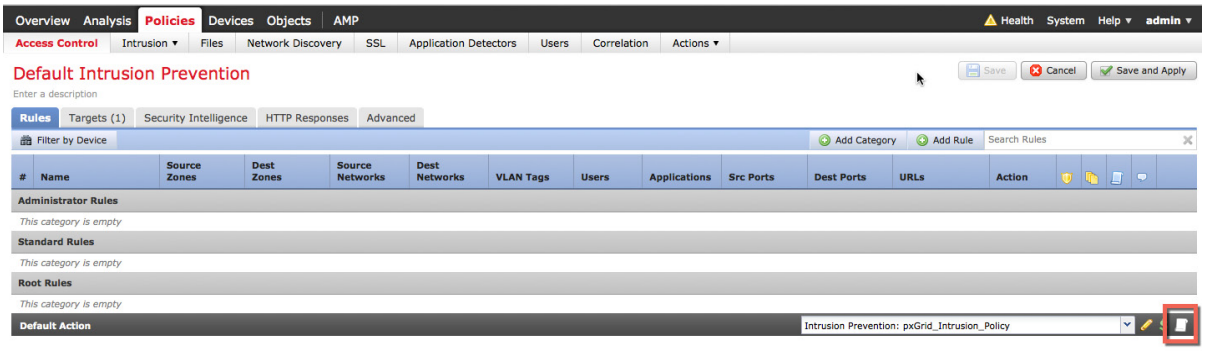
12단계 **Policies(정책)->Access Control Policies(액세스 컨트롤 정책)->Default Intrusion Prevention(기본 침입 방지)**을 선택하여 편집합니다.

13단계 기본 조치의 드롭다운에서 **pxGrid_Intrusion_Policy**를 선택합니다.



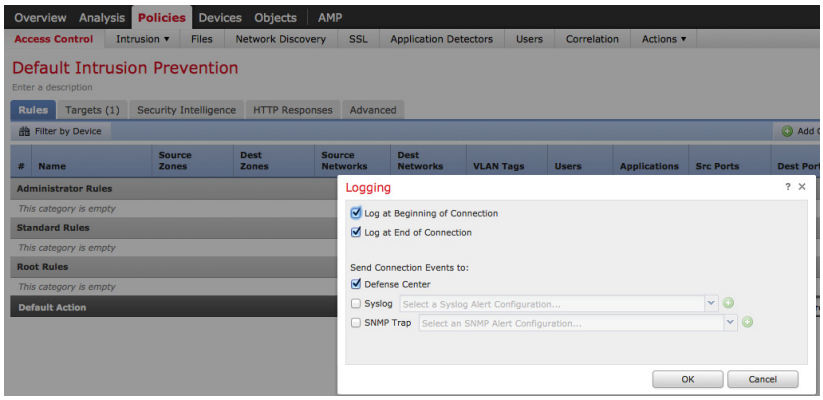
14단계 **Save(저장)**를 클릭합니다.

15단계 테이블의 오른쪽 하단에 있는 **로깅** 아이콘을 클릭합니다.



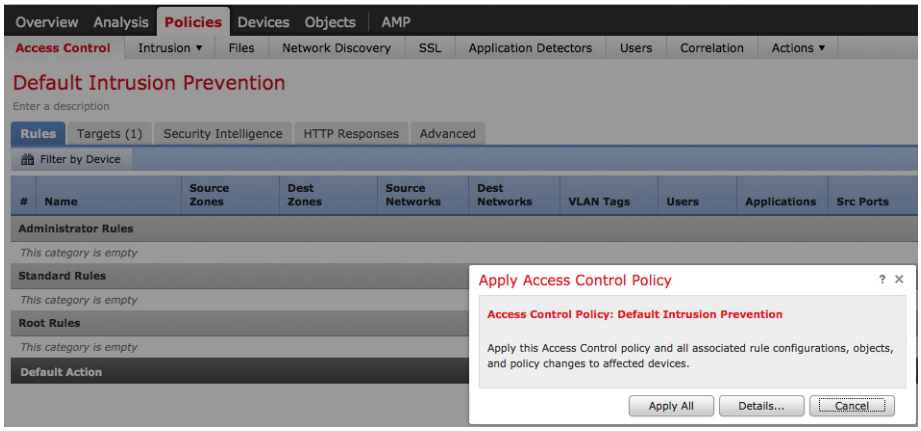
16단계 연결의 시작 및 끝에 로깅을 활성화합니다. Defense Center(방어 센터)를 대상으로 선택합니다.

17단계 **OK(확인)**를 클릭합니다.



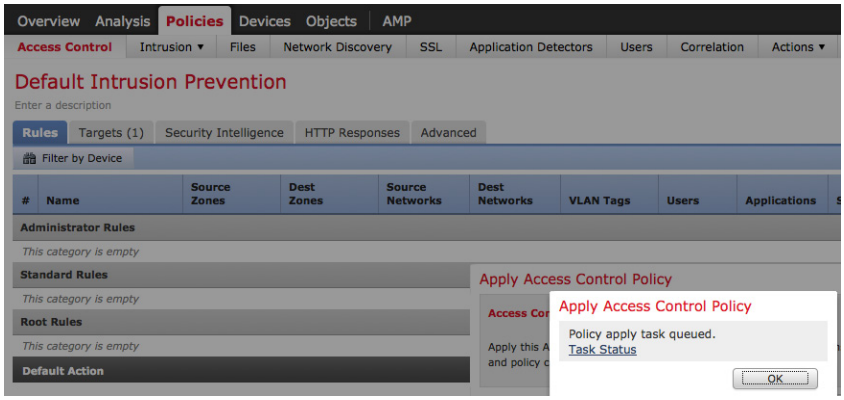
18단계 **Save and Apply(저장 및 적용)**를 클릭합니다.

19단계 다음과 같이 표시되어야 합니다.



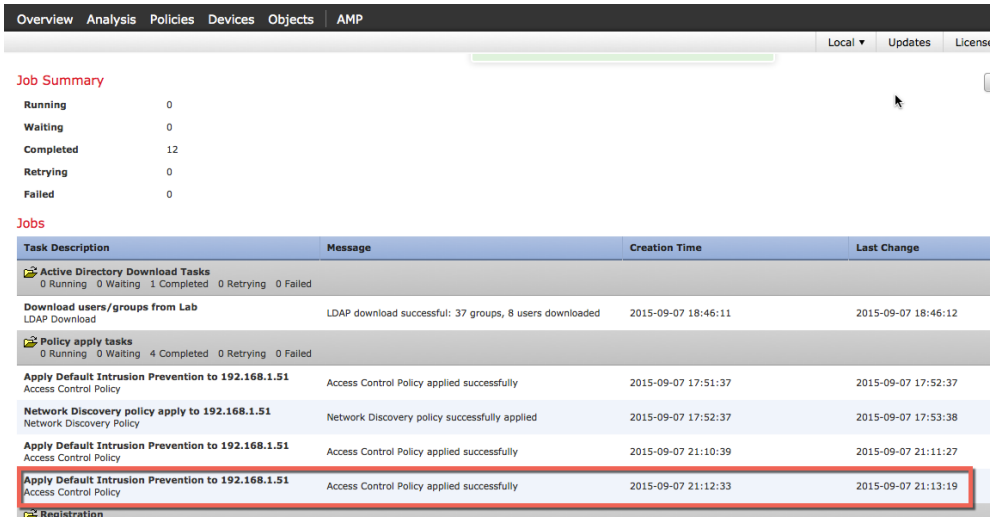
20단계 **Apply All(모두 적용)**을 클릭합니다.

21단계 작업이 큐에 대기되었다고 표시되어야 합니다.



22단계 **OK(확인)**를 클릭합니다.

23단계 **System(시스템)->Monitoring(모니터링)->Task Status(작업 상태)**를 선택하여 작업이 성공적으로 완료되었다는 결과를 확인합니다.



FireSIGHT 연결 규칙

이 섹션에서는 기본 액세스 정책에 추가할 연결 규칙을 정의합니다. 이 기본 액세스 정책에는 pxGrid 침입 정책도 포함됩니다. 이 연결 규칙은 HTTP/HTTPS를 통해 연결 이벤트를 모니터링하고 이러한 연결 세부 정보를 FireSIGHT Management Center에 기록합니다. 격리 해제 정책에서 이 연결 규칙을 사용하여 격리 해제 교정 유형을 트리거하는 연결 이벤트를 모니터링합니다.

1단계 **Policies(정책)->Access Control(액세스 컨트롤)**로 이동합니다.

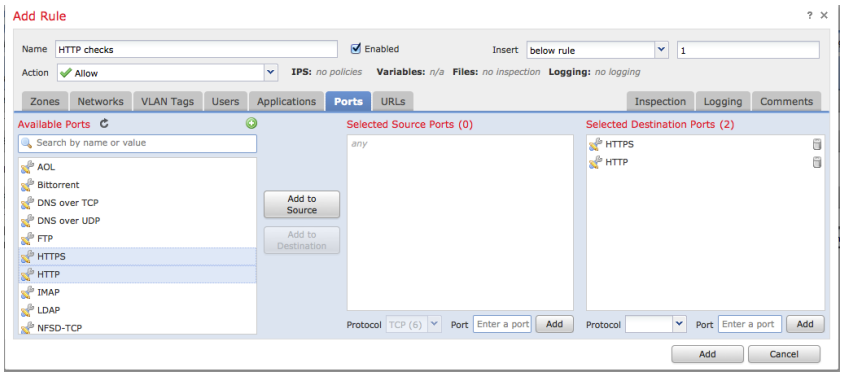
2단계 연필을 클릭하여 **Default Intrusion Prevention(기본 침입 방지)**을 편집합니다.

3단계 **Add Rule(규칙 추가)**을 클릭합니다.

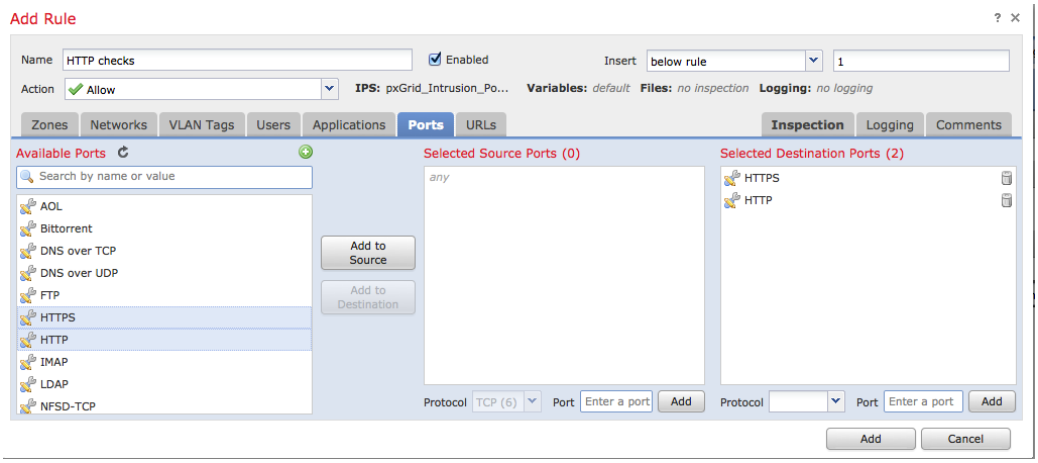
4단계 규칙 이름을 **"HTTP Checks"**로 지정합니다.

5단계 **Ports(포트)** 탭을 선택합니다.

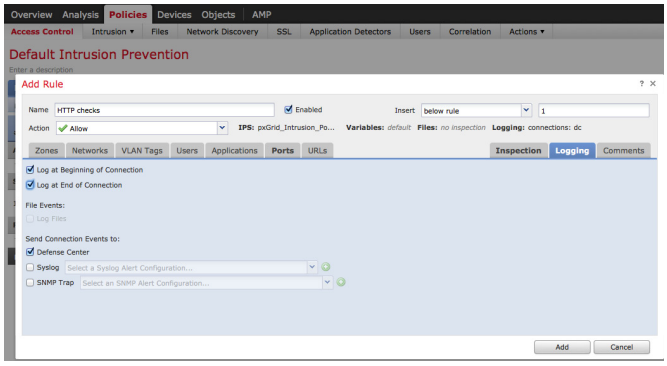
6단계 **HTTP** 및 **HTTPS**를 대상 포트로 선택합니다.



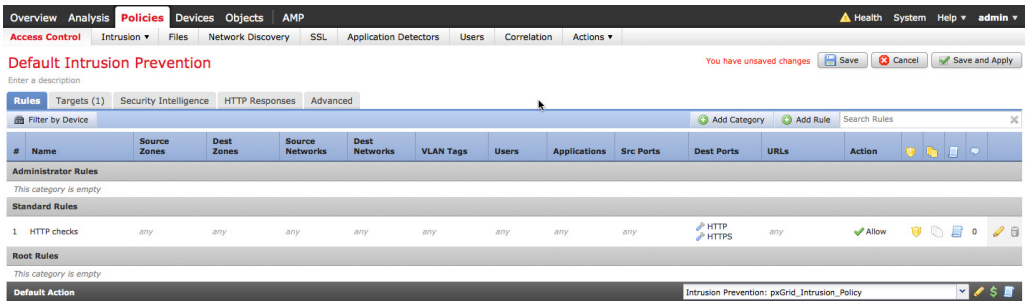
7단계 **IPS**를 클릭하고 **pxGrid_Intrusion_Policy**를 선택합니다.



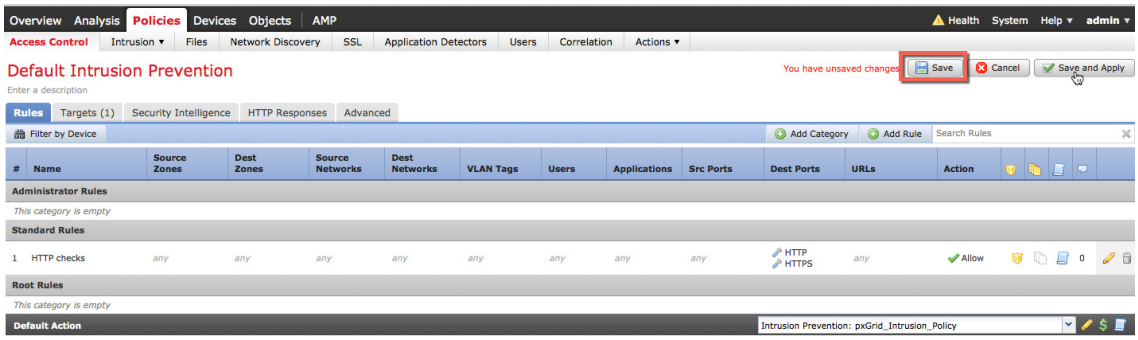
8단계 **Logging(로깅)**을 선택합니다.



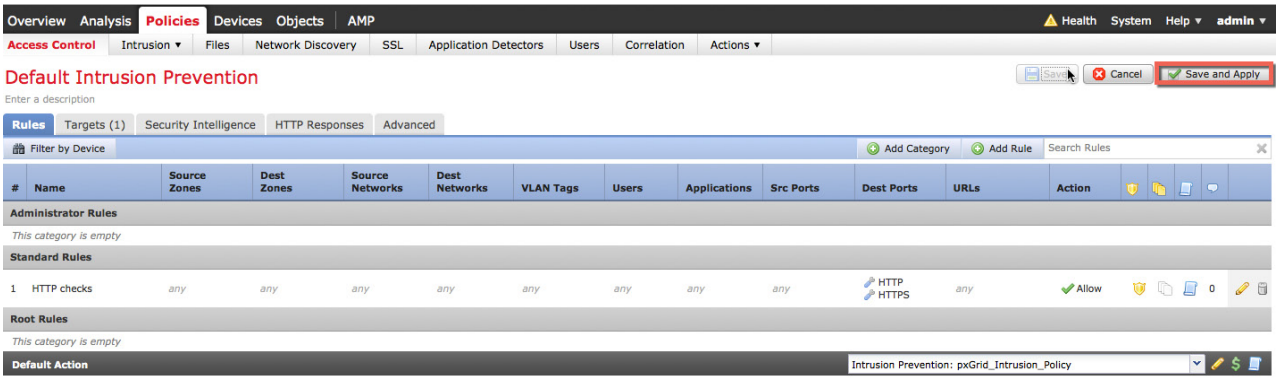
9단계 다음과 같이 표시되어야 합니다.



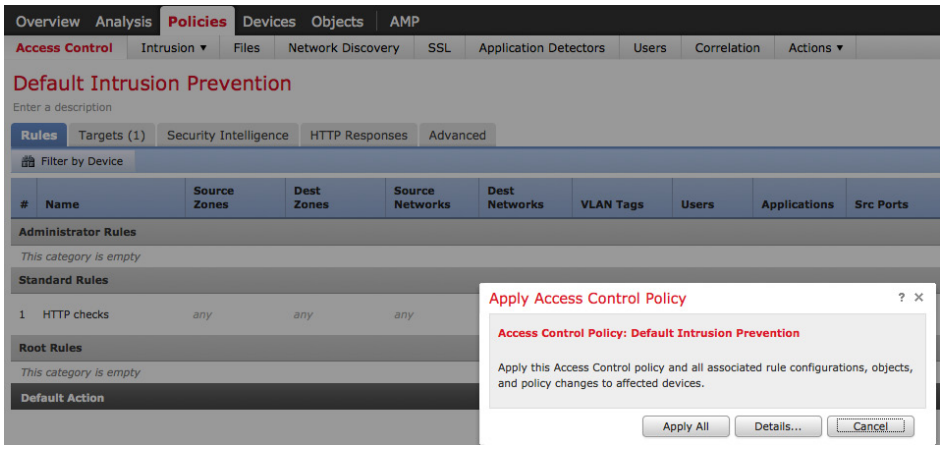
10단계 **Save(저장)**를 선택합니다.



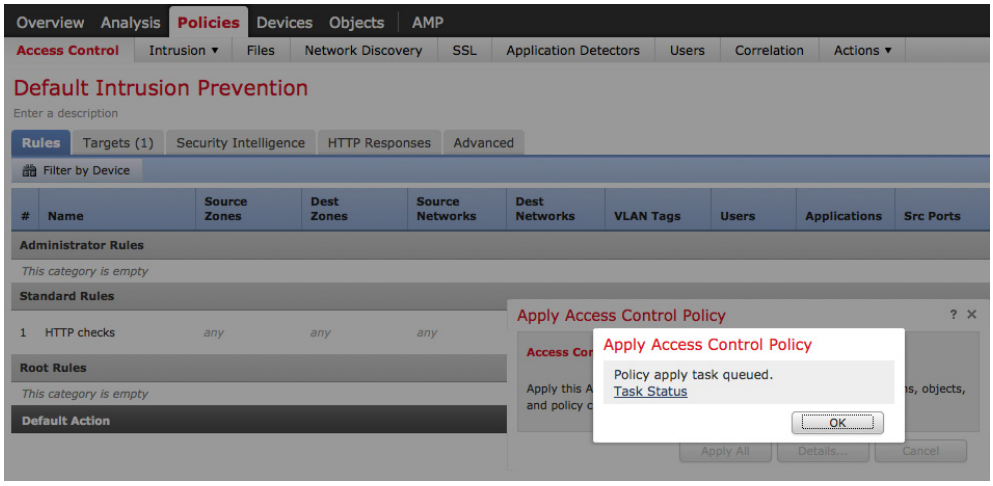
11단계 **Save and Apply(저장 및 적용)**를 선택합니다.



12단계 **Apply All(모두 적용)**을 클릭합니다.



13단계 정책 적용 작업이 큐에 대기되었다고 표시되어야 합니다. **OK(확인)**를 클릭합니다.



ISE EPS 서비스 및 격리 권한 부여 정책 구성

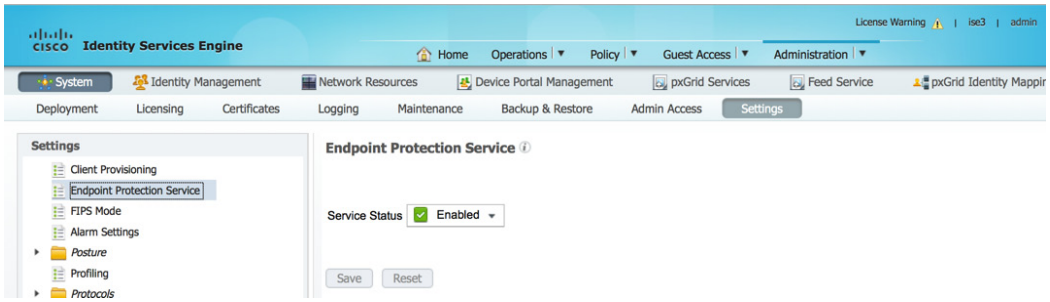
이 섹션에서는 ISE에서 EPS를 활성화하고 ISE에 격리 권한 부여 정책을 생성하는 단계를 설명합니다. ISE 1.4에서는 EPS(Endpoint Protection Service)가 Adaptive Network Control로 이름이 변경되었습니다. ISE 2.0에서는 이 서비스가 기본적으로 활성화되기 때문에 Administration(관리) 아래에 Adaptive Network Control 서비스 설정이 없습니다.

참고: ISE 2.0의 Adaptive Network Control 정책은 AdaptiveNetworkControl 기능에 등록하는 pxGrid 클라이언트에 종속됩니다. FireSIGHT Management Center의 경우는 다릅니다. FireSIGHT Management Center는 EndpointProtectionService 기능에 등록하고 ISE 권한 부여 정책에 의존합니다. ISE 2.0에서는 pxGrid GCL EPS_unquarantine 스크립트를 사용하여 엔드포인트 격리 해제를 수행해야 합니다. 이는 FireSIGHT Management Center에서 격리 해제 상관관계 정책 및 상관관계 규칙을 생성하고 격리 해제 상관관계 정책에 격리 해제 완화 응답을 할당하여 수행됩니다.

1단계 ISE 엔드포인트 보호 서비스를 활성화합니다.

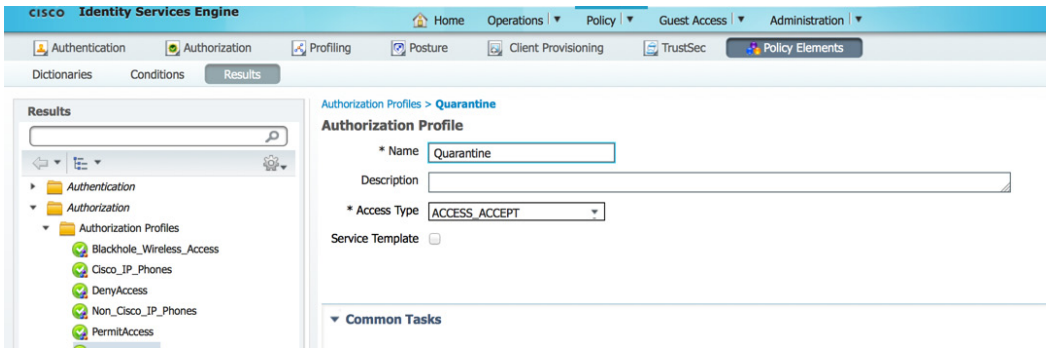
Administration(관리)->System(시스템)->Settings(설정)->Endpoint Protection Service(엔드포인트 보호 서비스)를 선택하고 엔드포인트 보호 서비스를 활성화한 후 Save(저장)를 클릭합니다.

참고: ISE 2.0에서는 엔드포인트 보호 서비스를 적용할 수 없습니다. 기본적으로 설정되어 있습니다.



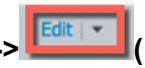
2단계 격리 권한 부여 프로파일을 생성합니다.

Policy(정책)->Policy Elements(정책 요소)->Results(결과)->Authorization(권한 부여)-> Authorization Profiles(권한 부여 프로파일)->Add(추가)->Name(이름): Quarantine->Save(저장)



참고: 이 예에서는 Access Type(액세스 유형)이 ACCESS_ACCEPT로 설정되어 권한 부여 조건 프로파일을 보여줍니다.

3단계 격리 권한 부여 정책을 생성합니다.

Policy(정책)->Authorization(권한 부여)->Exceptions(예외)-> 

(편집)-> 

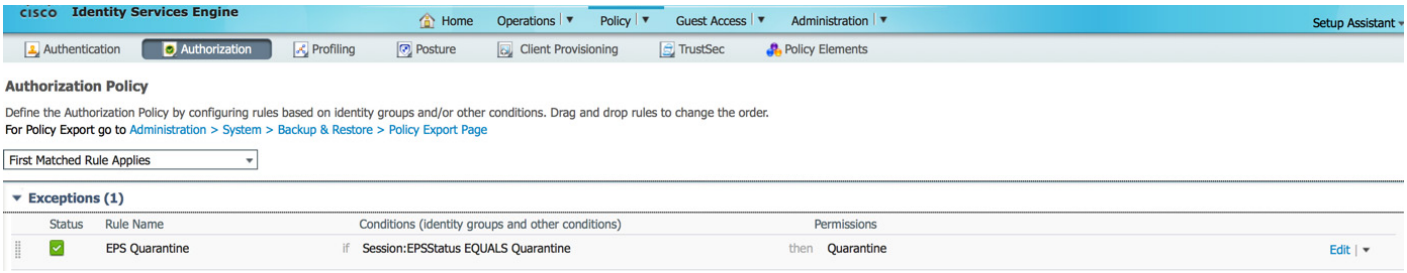
(위에 새 규칙 삽입)를 클릭한 후 다음을 입력합니다.

규칙 이름: EPS Quarantine

새 조건 규칙 생성: Session:EPSStatus:EQUALS:Quarantine

표준 프로파일:Quarantine

Done(완료)을 클릭합니다.



4단계 **Save(저장)를 클릭합니다.**

FireSIGHT Management Center 상관관계 정책

이 섹션에서는 격리, 포트 바운스, 재인증, 포트 종료, 종료 및 격리 해제에 대한 FireSIGHT 상관관계 정책 및 규칙이 생성됩니다. 이러한 정책에 각각의 교정 응답이 할당되고 엔드포인트에 pxGrid ANC 완화 교정 조치가 제공됩니다.

상관관계 정책이 생성된 후 규칙 모듈이 생성됩니다. 상관관계 정책이 각 규칙 모듈을 추가합니다. 규칙 모듈에 각 응답이 할당됩니다.

예를 들어, 격리 상관관계 정책이 생성됩니다. 침입 이벤트 발생 시 엔드포인트의 소스 IP 주소가 격리되는 격리 규칙 모듈이 생성됩니다. 격리 규칙 모듈에 격리 교정 유형 응답이 할당됩니다. 최종 사용자가 pxGrid 침입 정책을 위반하면 침입 이벤트가 트리거되고 격리 교정 유형 응답에 따라 격리 완화 조치를 시작하는 상관관계 이벤트도 트리거됩니다.

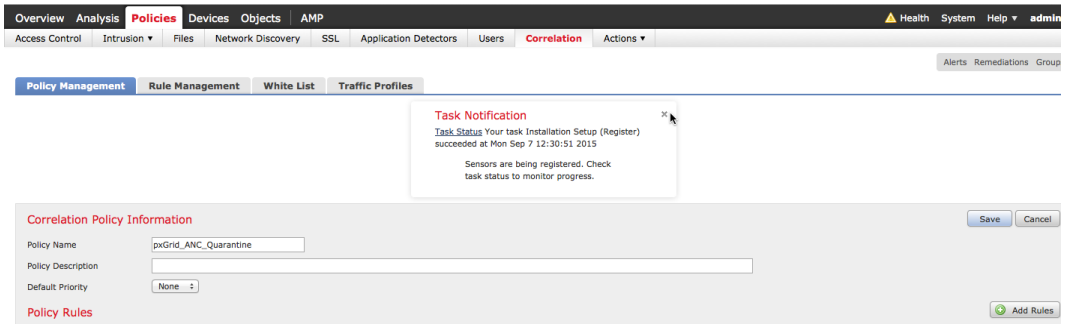
포트 바운스, 재인증, 포트 종료, 종료 정책도 동일한 플로우를 따릅니다.

격리 해제 정책에는 연결 이벤트를 트리거하는 격리 해제 규칙 모듈이 있습니다. 격리 해제 규칙 모듈은 엔드포인트가 특정 URL 사이트에 액세스할 때 엔드포인트의 소스 IP 주소를 기반으로 하여 격리 해제됩니다.

격리

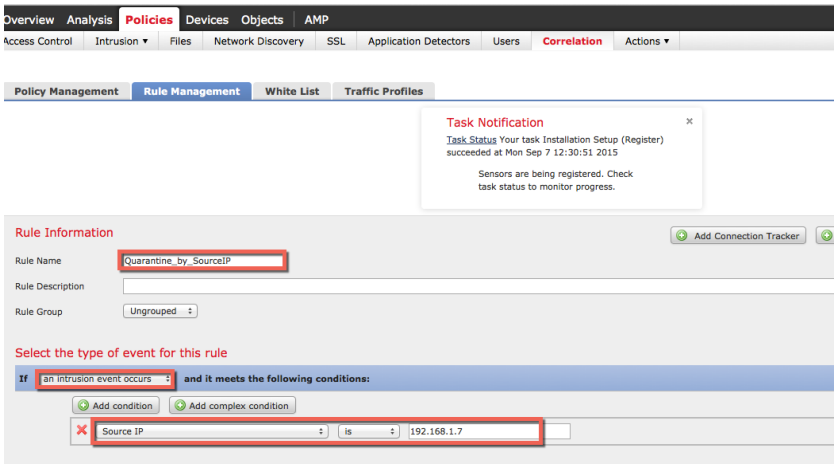
격리 상관관계 정책이 생성됩니다.

1단계 **Policies(정책)->Correlation(상관관계)->Policy Management(정책 관리)->Create Policy(정책 생성)->pxGrid_ANC_Quarantine->Save(저장)**

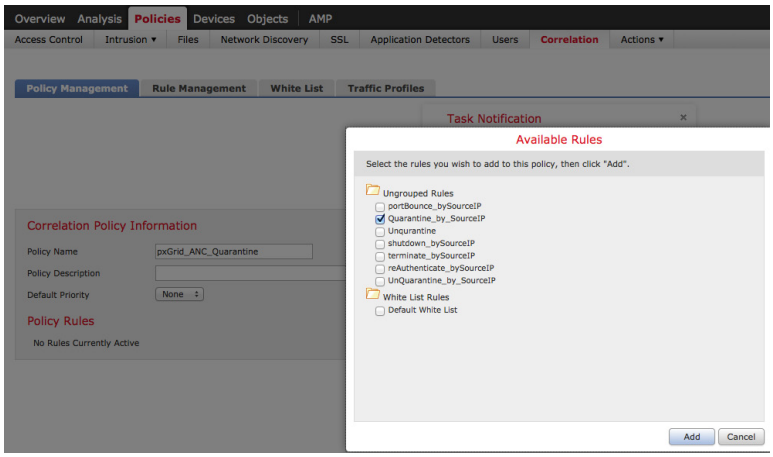


2단계 **Policies(정책)->Correlation(상관관계)->Rule Management(규칙 관리)->Create Rule(규칙 생성)**을 선택한 후 규칙 이름 **Quarantine_by_SourceIP**를 추가하고 다음을 입력한 후 **Save(저장)**를 클릭합니다.

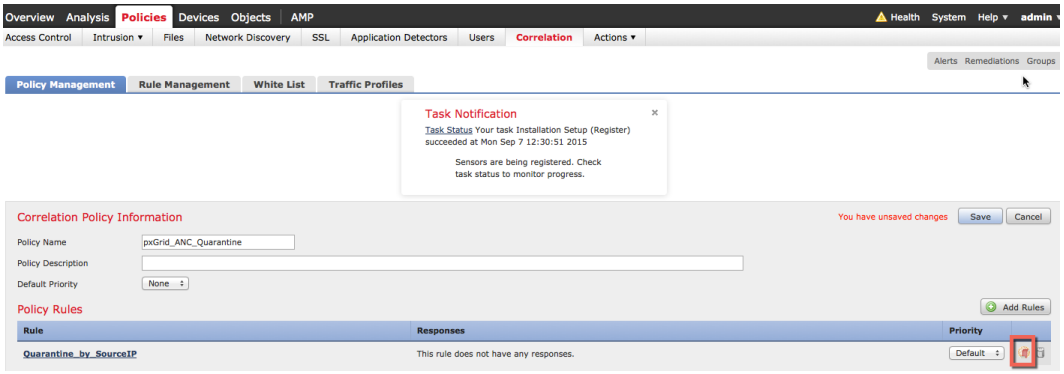
참고: 이 규칙은 소스 IP 주소가 격리되는 개념 증명을 제공합니다.



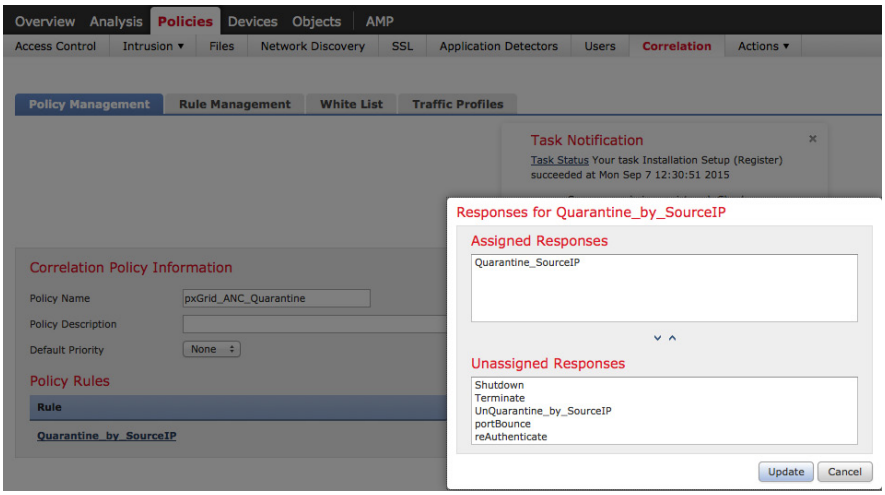
3단계 **Policies(정책)->Correlation(상관관계)->Policy Management(정책 관리)->pxGrid ANC Quarantine>Add rules(규칙 추가)->pxGrid ANC Quarantine->Add(추가)**



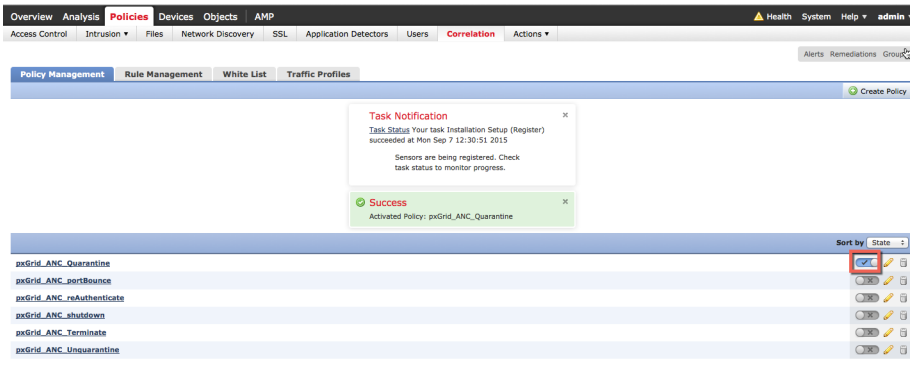
4단계 다음으로 응답을 추가합니다. **Responses(응답)** 탭을 클릭합니다.



5단계 **Quarantine_SourceIP**를 **Assigned Responses(할당된 응답)**로 이동하고 **Update(업데이트)-> Save(저장)**를 클릭합니다.



6단계 **버튼**을 클릭하여 격리 상관관계 정책을 활성화합니다.

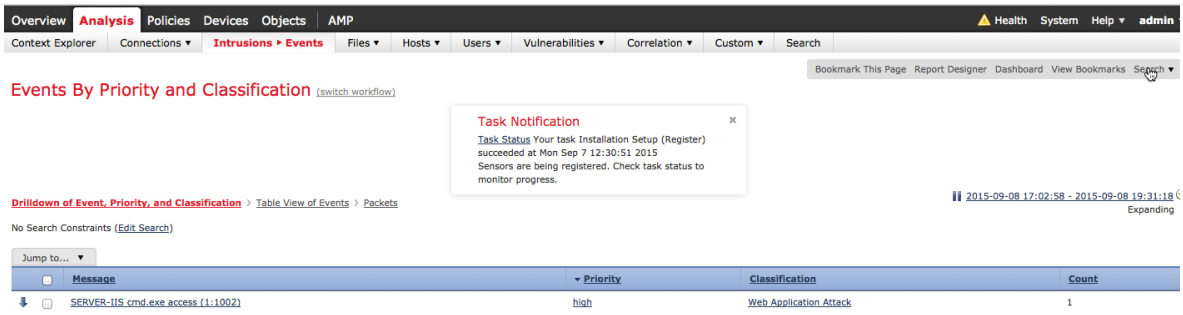


테스트

최종 사용자가 브라우저 창에 www.yahoo.com/cmd.exe를 입력합니다. 이렇게 하면 FireSIGHT의 pxGrid 침입 정책에서 "SERVER-IIS.cmd.exe 액세스" 규칙 위반 시 침입 이벤트가 트리거됩니다. 상관관계 정책에 정의된 대로 격리 규칙에 할당된 격리 완화 응답을 기반으로 하여 엔드포인트가 격리됩니다.

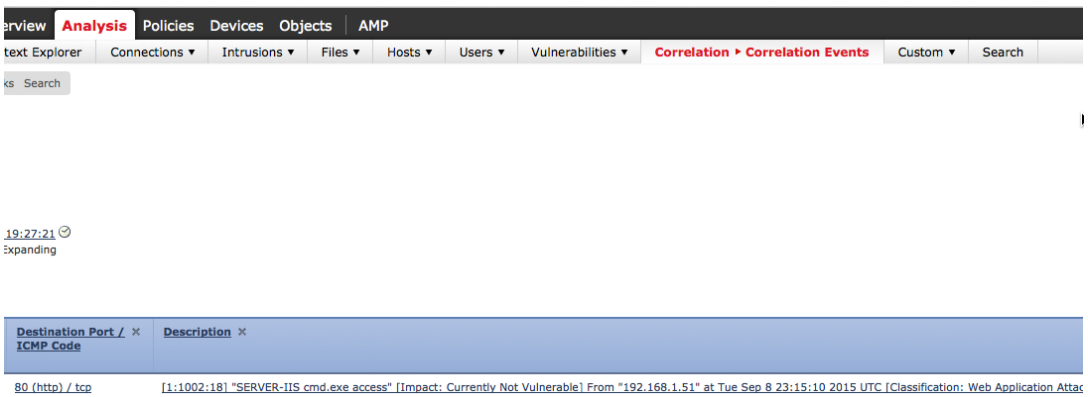
1단계 최종 사용자가 브라우저에 www.yahoo.com/cmd.exe를 입력합니다.

2단계 이렇게 하면 "웹 애플리케이션 공격" 침입 이벤트가 트리거됩니다.

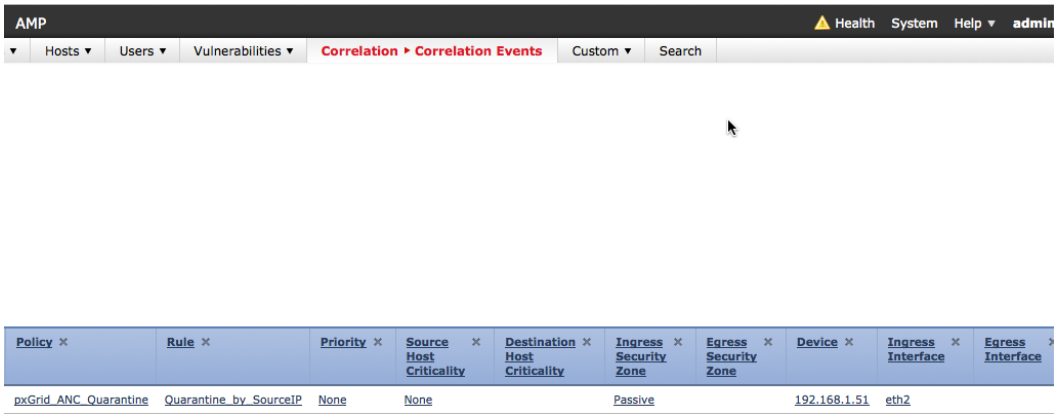


3단계 또한 "상관관계 이벤트"가 트리거됩니다.
격리되는 소스 IP 주소와 FireSIGHT LDAP/사용자 인식 컨피그레이션에 따른 사용자 정보에 주의하십시오.

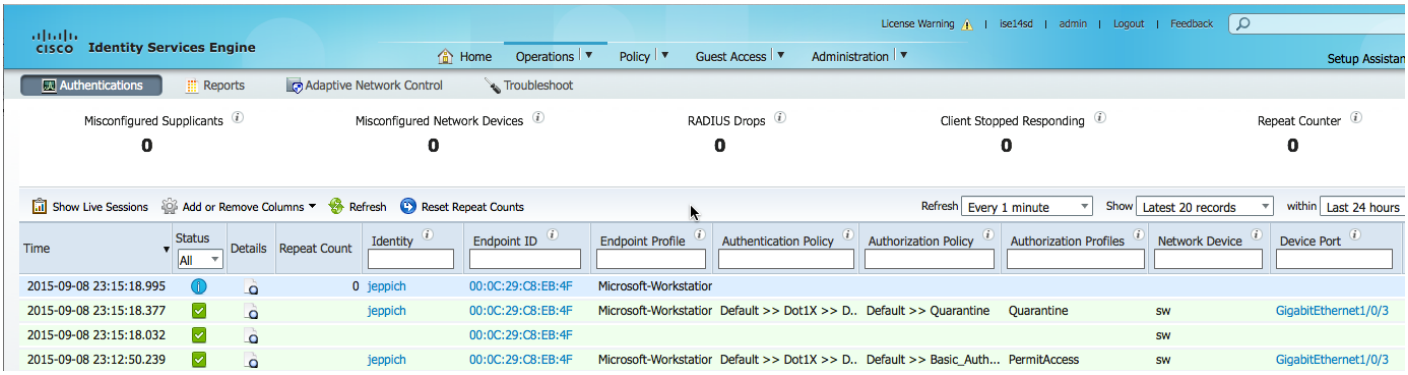
4단계 동일한 이벤트를 계속하는 경우
pxGrid_Intrusion_Policy 규칙에 포함된 규칙 위반 및 대상 포트에 주의하십시오.



5단계 동일한 이벤트를 계속 진행하는 경우
할당된 격리 완화 응답을 트리거한 상관관계 정책 및 상관관계 규칙에 주의하십시오.



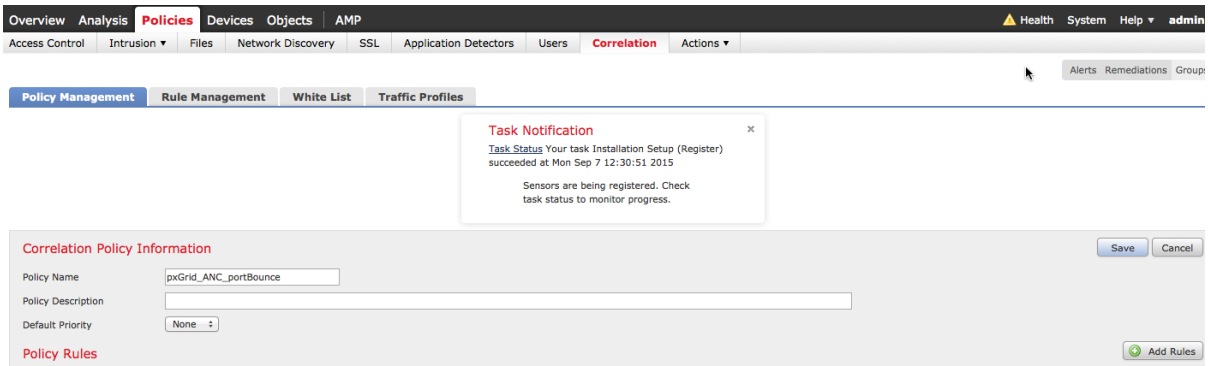
6단계 ISE에서 응답을 보려면 Operations(작업)->Authentications(인증)를 선택합니다.



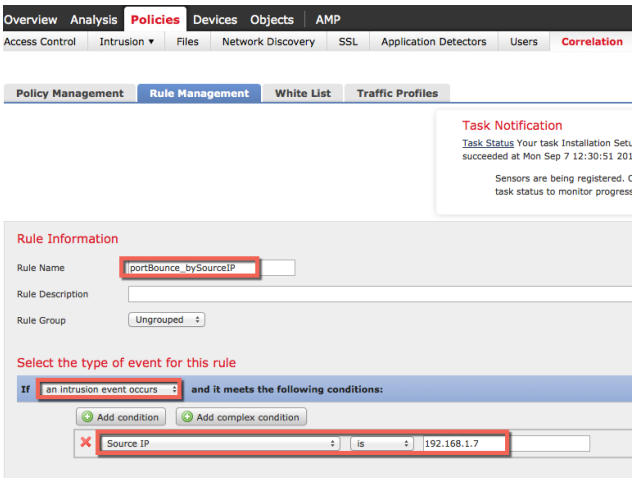
포트 바운스

포트 바운스 상관관계 정책이 생성됩니다.

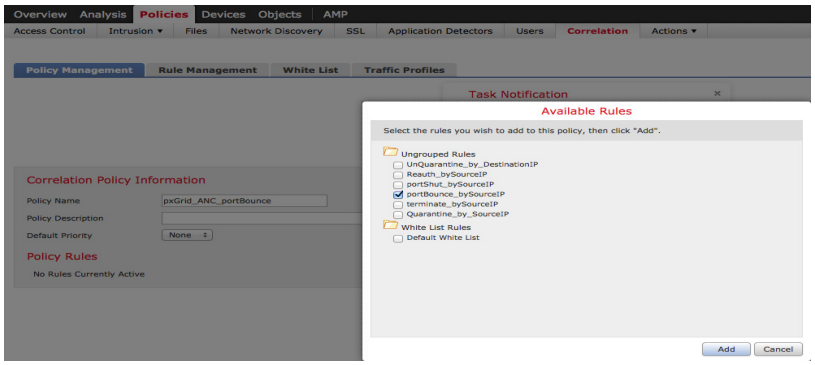
1단계 **Policies(정책)->Correlation(상관관계)->Policy Management(정책 관리)->Create Policy(정책 생성)->pxGrid ANC portBounce->Save(저장)**



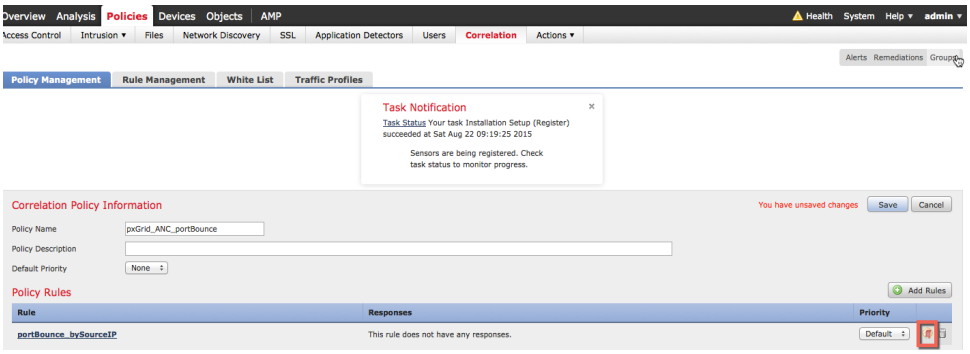
2단계 **Policies(정책)->Correlation(상관관계)->Rule Management(규칙 관리)->Create Rule(규칙 생성)을 선택한 후 규칙 이름 portBounce_by_SourceIP를 추가하고 다음을 입력한 다음 Save(저장)를 클릭합니다.**



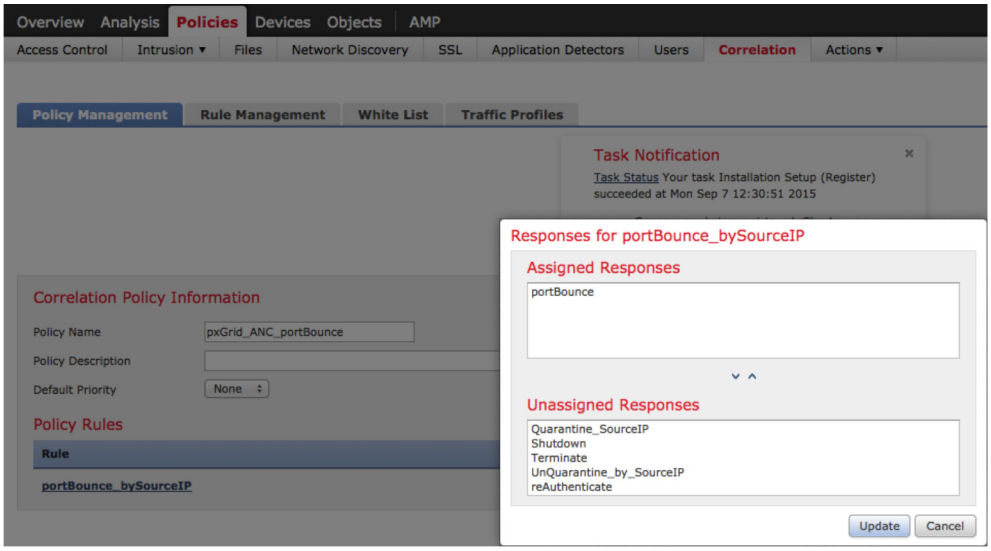
3단계 **Policies(정책)->Correlation(상관관계)->Policy Management(정책 관리)->xGrid ANC portBounce->Add rule(규칙 추가)을 선택하고 portBounce_by_SourceIP를 선택하여 규칙을 추가합니다.**



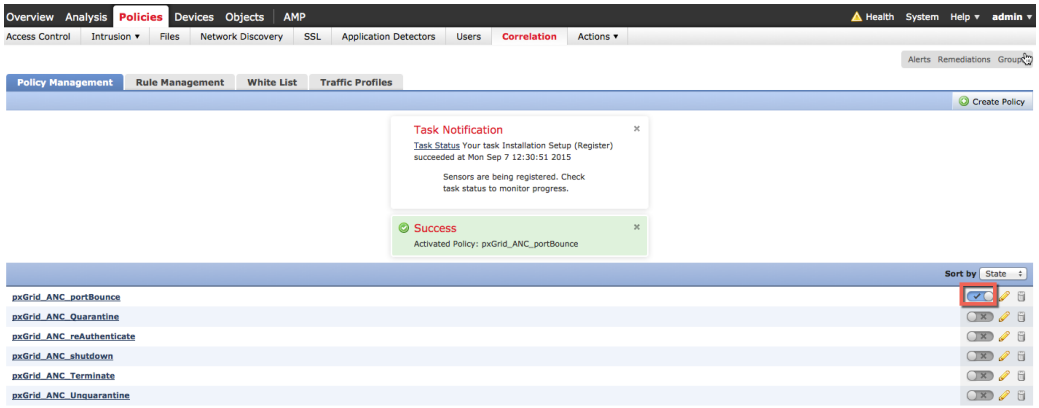
4단계 다음으로 응답을 추가합니다. **Responses(응답)** 탭을 **클릭합니다.**



5단계 **Policies(정책)->Correlation(상관관계)->portBounce_by_SourceIP**를 선택하고 **portBounce**를 **Assigned Responses(할당된 응답)**로 이동한 후 **Update(업데이트)->Save(저장)**를 클릭합니다.



6단계 정책을 설정하는 아래의 **버튼**을 클릭하여 종료 정책을 활성화합니다.

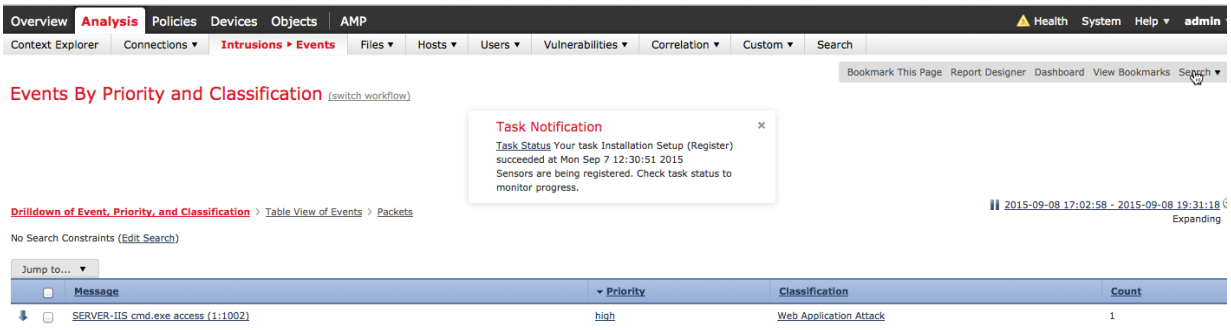


테스트

최종 사용자가 브라우저 창에 www.yahoo.com/cmd.exe를 입력합니다. 이렇게 하면 FireSIGHT의 pxGrid 침입 정책에서 "SERVER-IIS.cmd.exe 액세스" 규칙 위반 시 침입 이벤트가 트리거됩니다. 상관관계 정책에 정의된 대로 규칙에 할당된 포트 바운스 완화 응답을 기반으로 하여 엔드포인트를 포함하는 포트가 바운스됩니다.

1단계 최종 사용자가 브라우저에 www.yahoo.com/cmd.exe를 입력합니다.

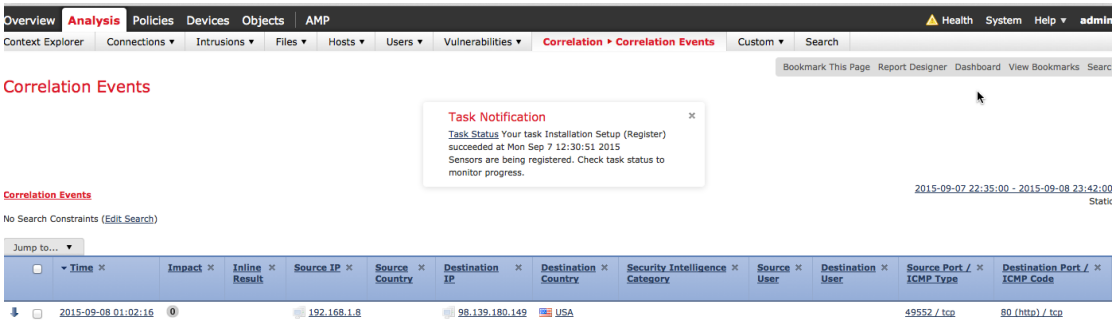
2단계 이렇게 하면 "웹 애플리케이션 공격" 침입 이벤트가 트리거됩니다.



3단계 또한 "상관관계 이벤트"가 트리거됩니다.

소스 IP 주소에 속하는 호스트에 대한 포트가 바운스됩니다.

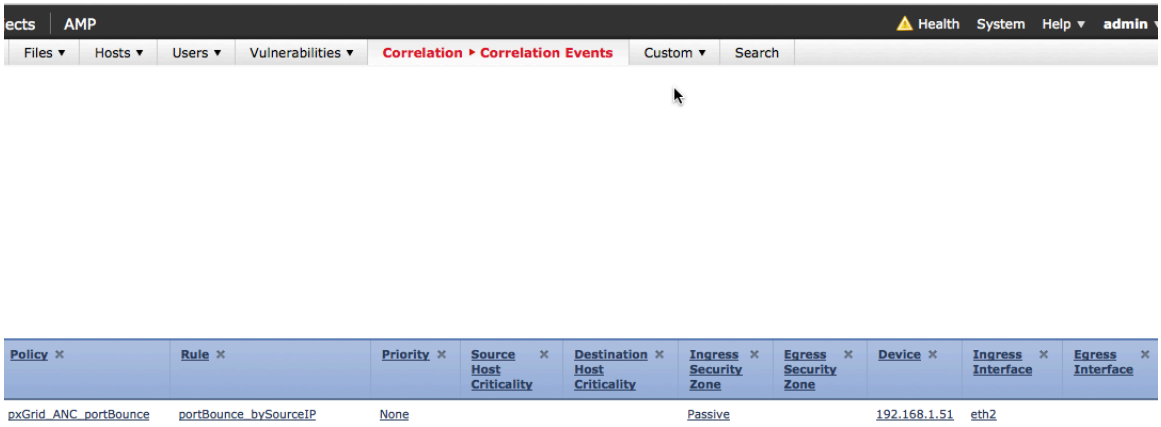
참고: 네트워크 검색 호스트 및 사용자가 설정되어 있지 않으므로 사용자 정보가 없습니다.



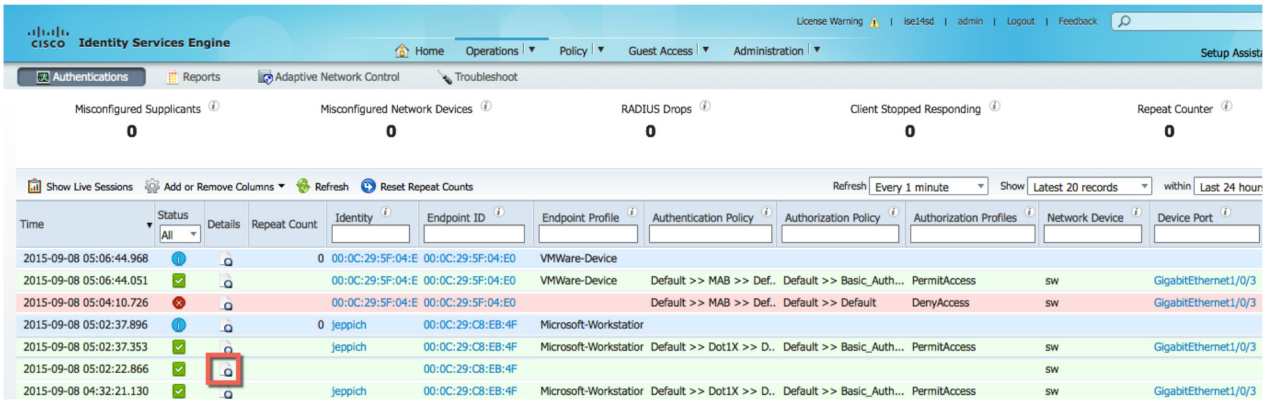
4단계 동일한 이벤트를 계속하는 경우

pxGrid_Intrusion_Policy 규칙에 포함된 규칙 위반에 주의하십시오.

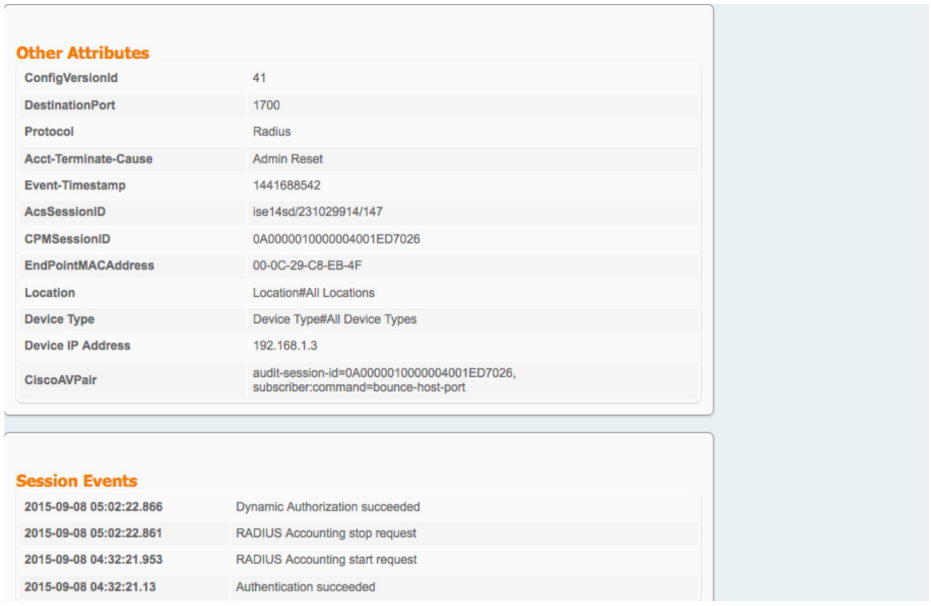
5단계 동일한 이벤트를 계속 진행하는 경우
할당된 포트 바운스 완화 응답을 트리거한 상관관계 정책 및 상관관계 규칙에 주의하십시오.



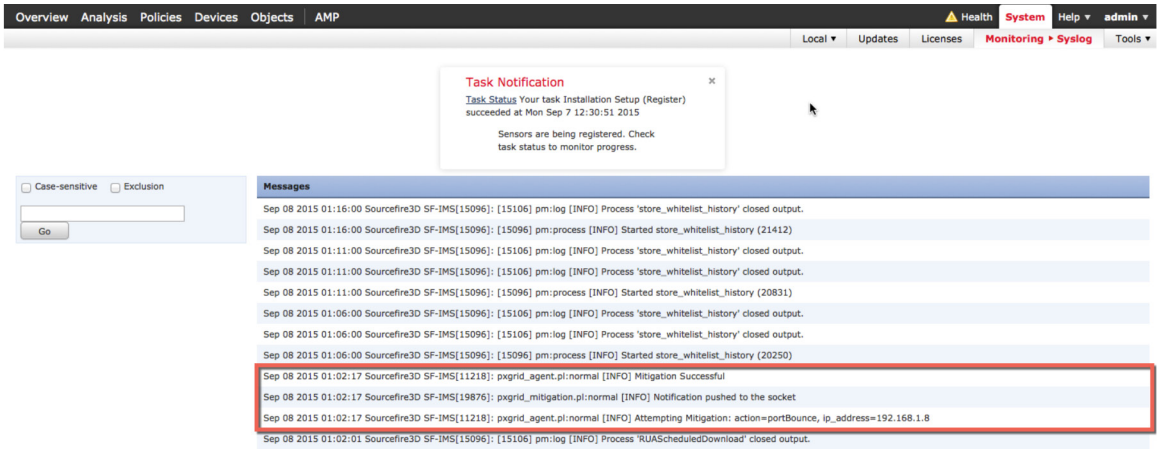
6단계 ISE에서 응답을 보려면 **Operations(작업)->Authentications(인증)**를 선택합니다.



7단계 세부 정보 버튼을 선택하면 포트가 CiscoAVpair 특성에 따라 바운스되었음을 알 수 있습니다.



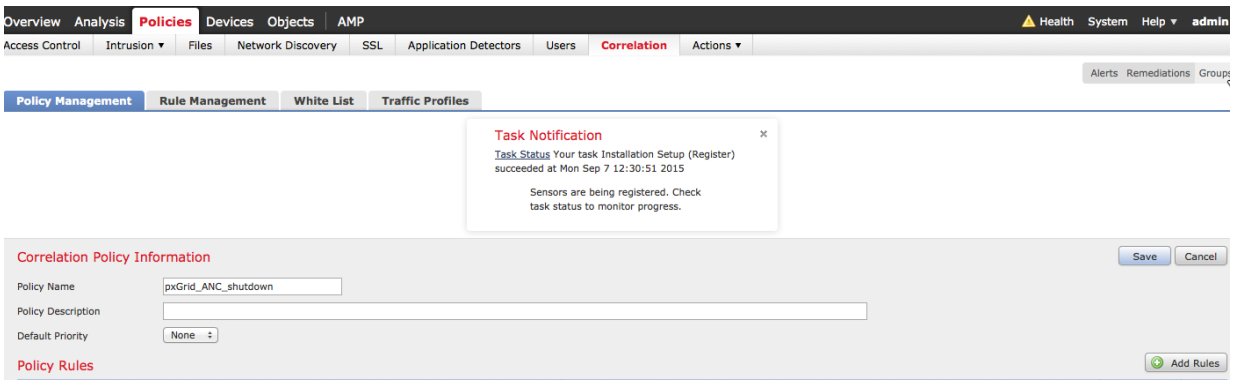
8단계 또한 FireSIGHT Management Center syslog 이벤트를 보고 포트 바운스 완화 조치에 성공했는지 확인할 수 있습니다.



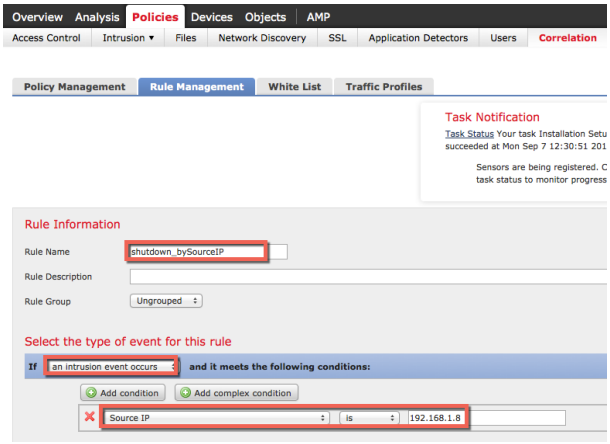
포트 종료

포트 종료 상관관계 정책이 생성됩니다.

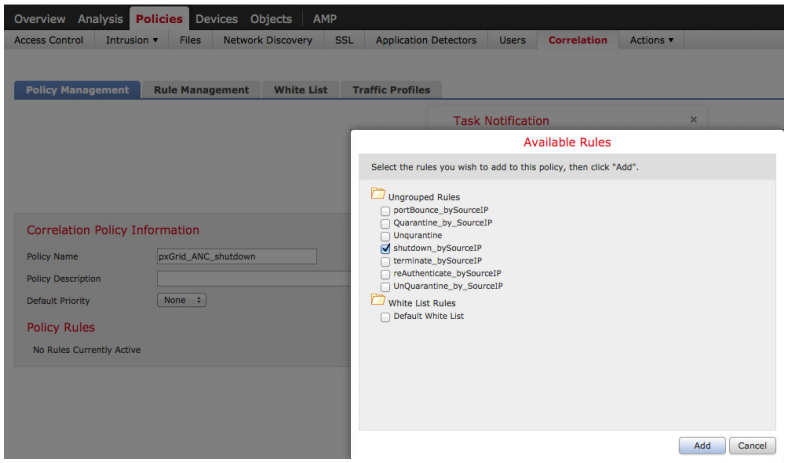
1단계 **Policies(정책)->Correlation(상관관계)->Policy Management(정책 관리)->Create Policy(정책 생성)->pxGrid_ANC_shutdown->Save(저장)**



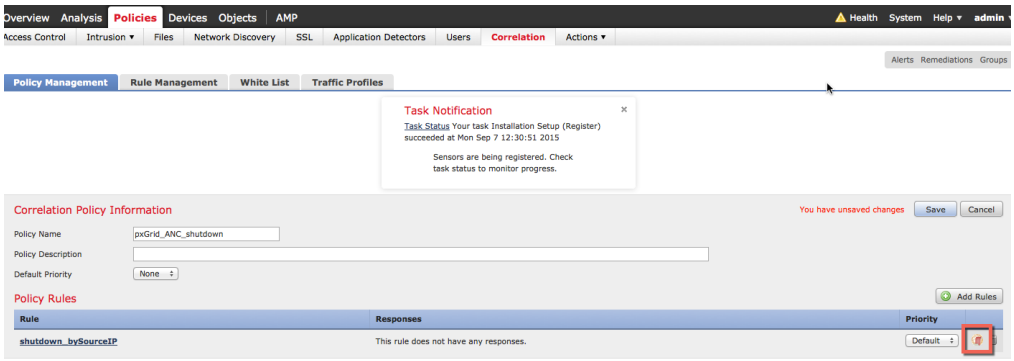
2단계 **Policies(정책)->Correlation(상관관계)->Rule Management(규칙 관리)->Create Rule(규칙 생성)을 선택한 후 규칙 이름 shutdown_by_SourceIP를 추가하고 다음을 입력한 다음 Save(저장)를 클릭합니다.**



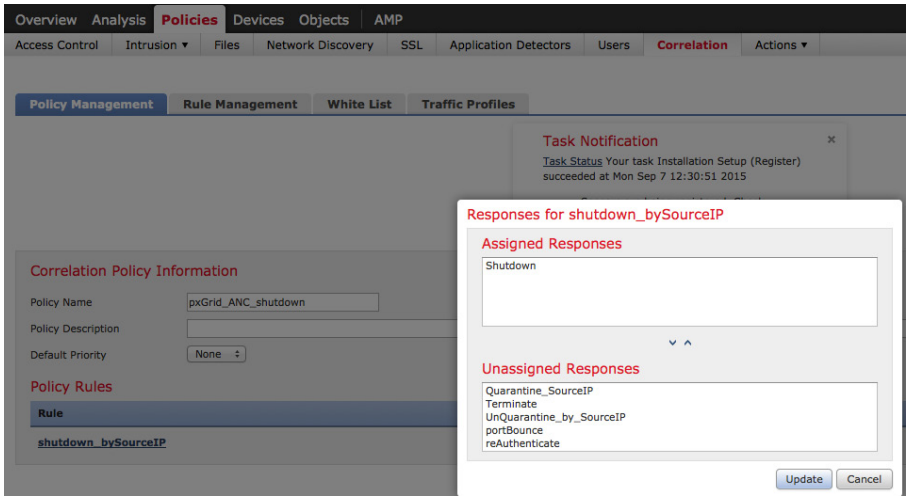
3단계 **Policies(정책)->Correlation(상관관계)->Policy Management(정책 관리)-> pxGrid_ANC_shutdown>Add rules(규칙 추가)를 클릭하고 "shutdown_bySourceIP를 선택한 후 규칙을 추가합니다.**



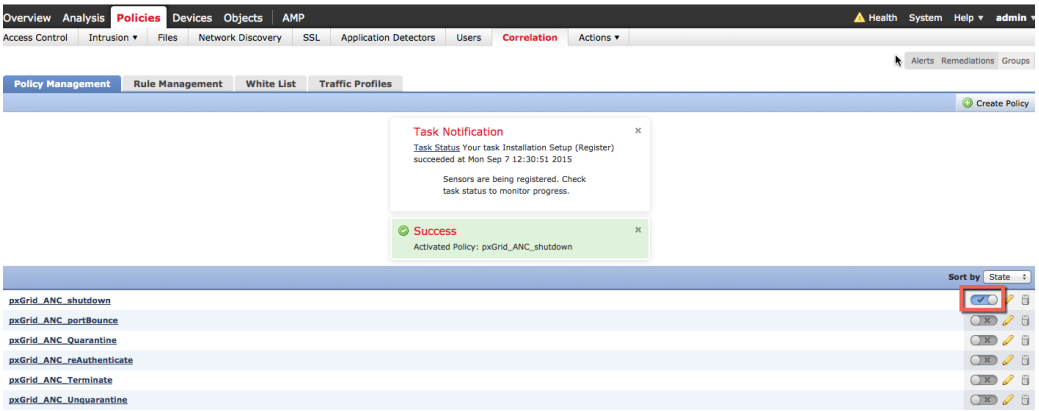
4단계 다음으로 응답을 추가합니다. **Responses(응답)** 탭을 클릭합니다.



5단계 **Policies(정책)->Correlation(상관관계)->pxGrid_ANC_shutdown**을 선택하고 **Shutdown을 Assigned Responses(할당된 응답)로 이동한 후 Update(업데이트)->Save(저장)**를 클릭합니다.



6단계 정책을 설정하는 아래의 **버튼**을 클릭하여 종료 정책을 활성화합니다.

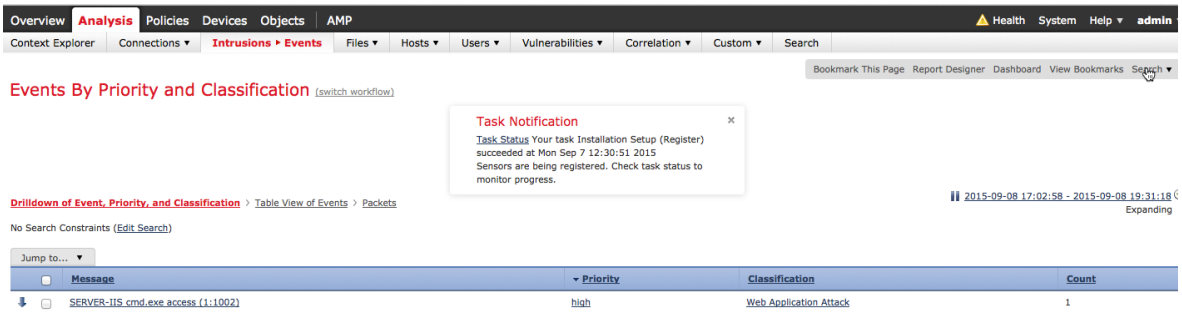


테스트

최종 사용자가 브라우저 창에 www.yahoo.com/cmd.exe를 입력합니다. 이렇게 하면 FireSIGHT의 pxGrid 침입 정책에서 "SERVER-IIS.cmd.exe 액세스" 규칙 위반 시 침입 이벤트가 트리거됩니다. 상관관계 정책에 정의된 규칙에 할당된 종료 완화 응답에 따라 엔드포인트의 포트가 종료됩니다.

1단계 최종 사용자가 브라우저에 www.yahoo.com/cmd.exe를 입력합니다.

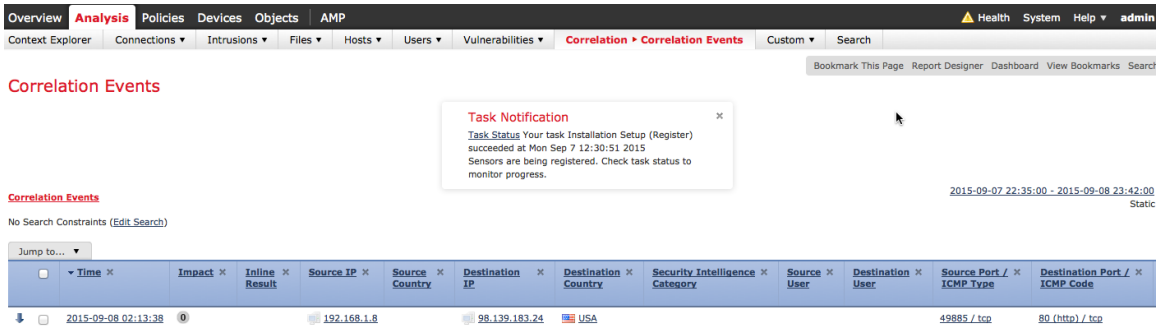
2단계 이렇게 하면 "웹 애플리케이션 공격" 침입 이벤트가 트리거됩니다.



3단계 또한 "상관관계 이벤트"가 트리거됩니다.

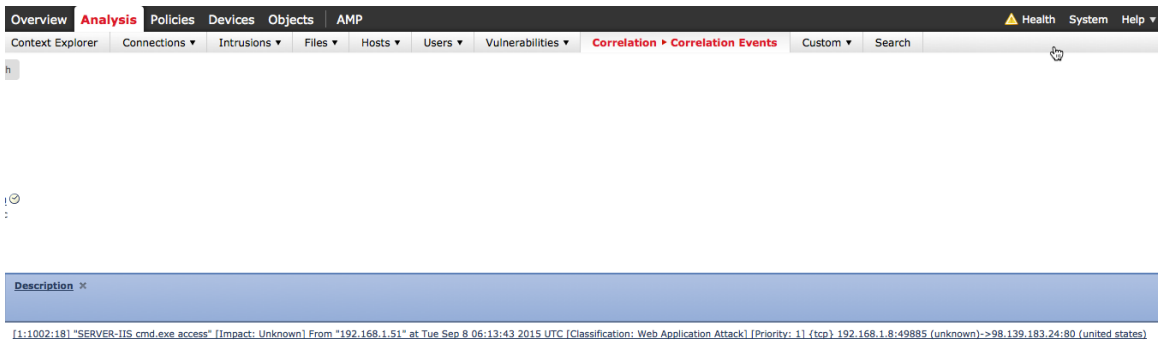
소스 IP 주소에 속하는 호스트의 포트가 종료됩니다.

참고: 네트워크 검색 호스트 및 사용자가 설정되어 있지 않으므로 사용자 정보가 없습니다.

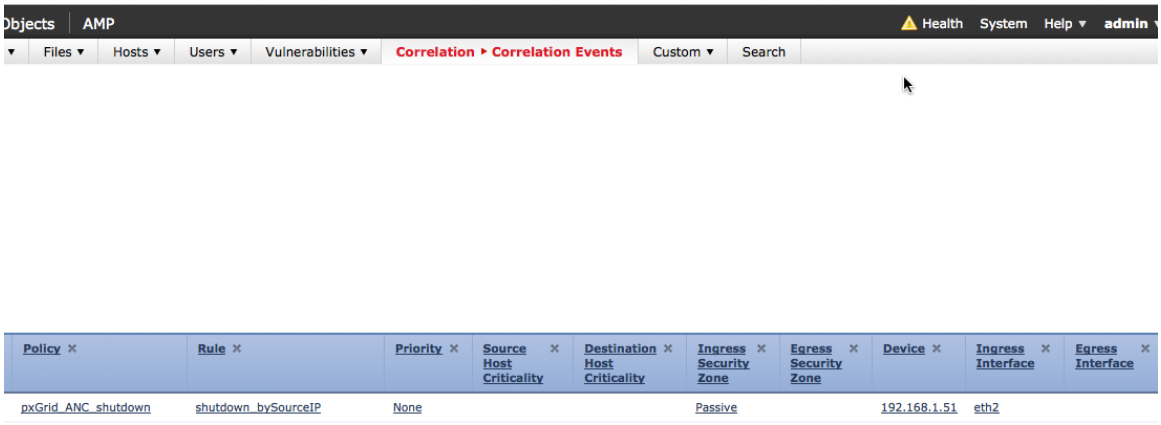


4단계 동일한 이벤트를 계속하는 경우

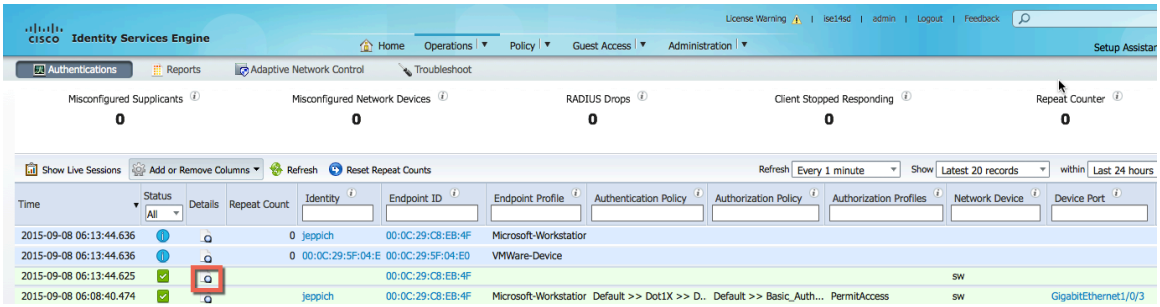
pxGrid_Intrusion_Policy 규칙에 포함된 규칙 위반에 주의하십시오.



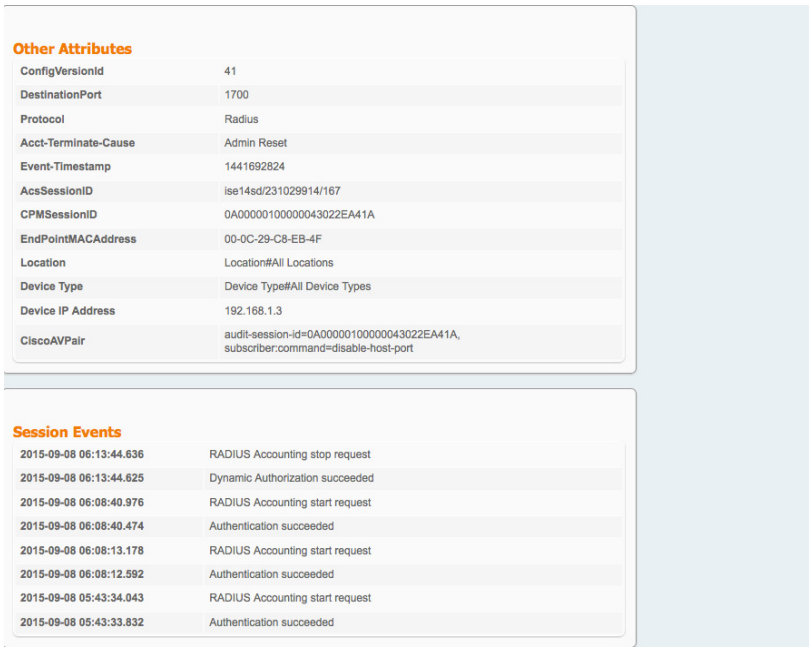
5단계 동일한 이벤트를 계속 진행하는 경우
할당된 포트 종료 완화 응답을 트리거한 상관관계 정책 및 상관관계 규칙에 주의하십시오.



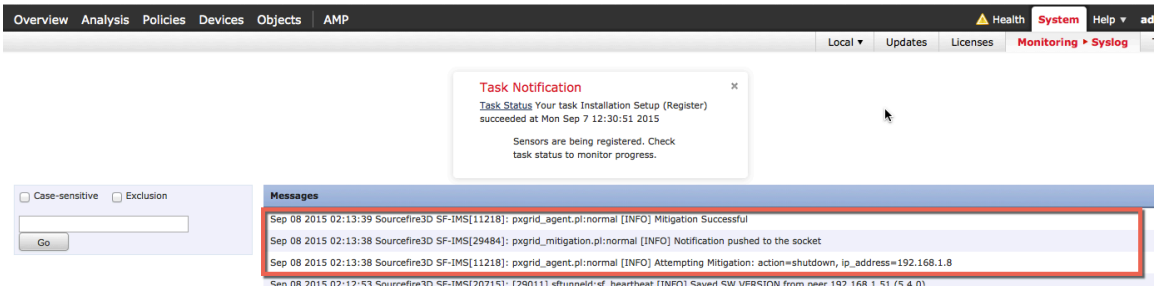
6단계 ISE에서 응답을 보려면 **Operations(작업)->Authentications(인증)**를 선택합니다.



7단계 세부 정보 버튼을 선택하면 포트가 CiscoAVpair 특성에 따라 비활성화되었음을 알 수 있습니다.



8단계 또한 FireSIGHT Management Center syslog 이벤트를 보고 포트 종료 완화 조치에 성공했는지 확인할 수 있습니다.



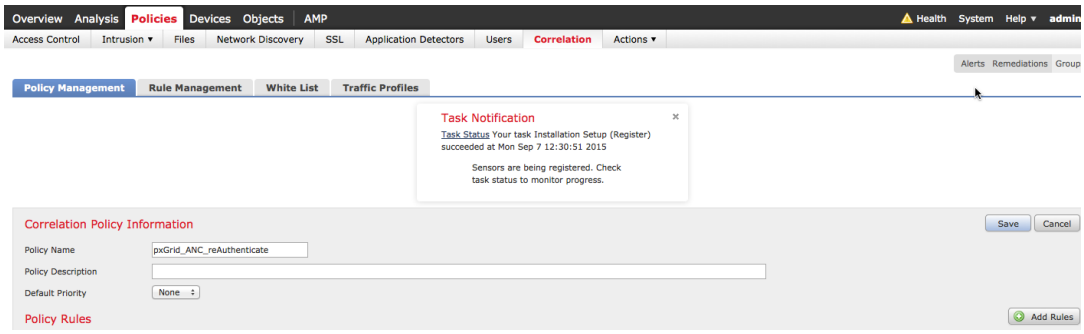
9단계 또한 포트에 "shutdown"이 표시됩니다.

```
interface GigabitEthernet1/0/3
 description internal LAN
 switchport mode access
 shutdown
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication fallback mab
 mab
```

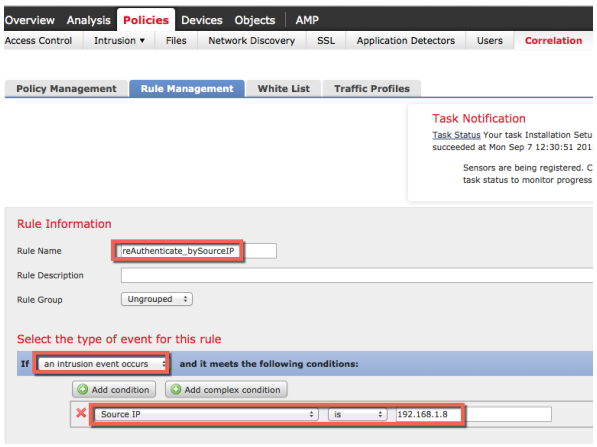
재인증

재인증 정책이 생성됩니다.

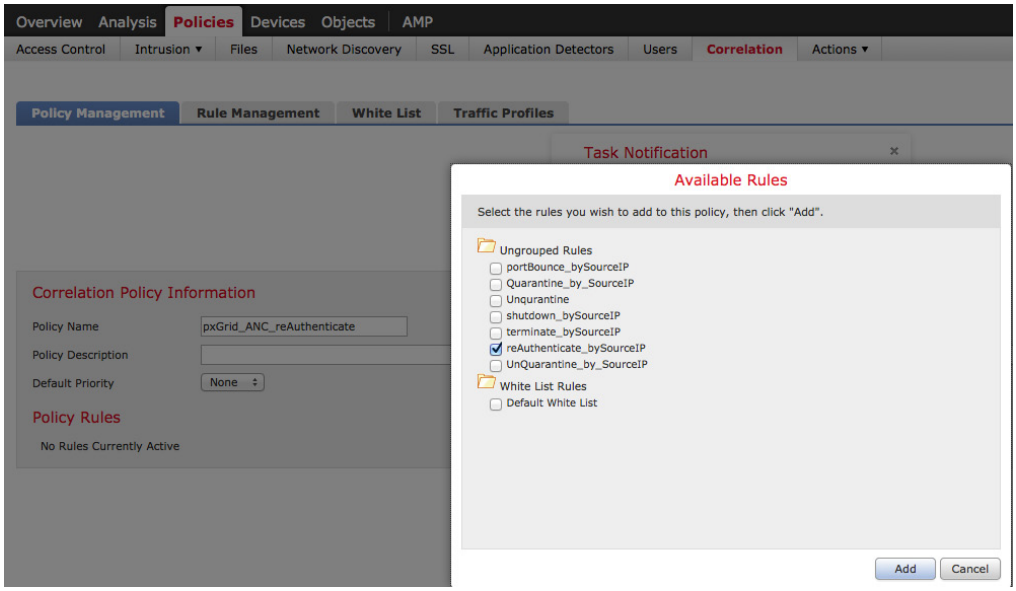
1단계 **Policies(정책)->Correlation(상관관계)->Policy Management(정책 관리)->Create Policy(정책 생성)->pxGrid ANC reAuthenticate->Save(저장)**



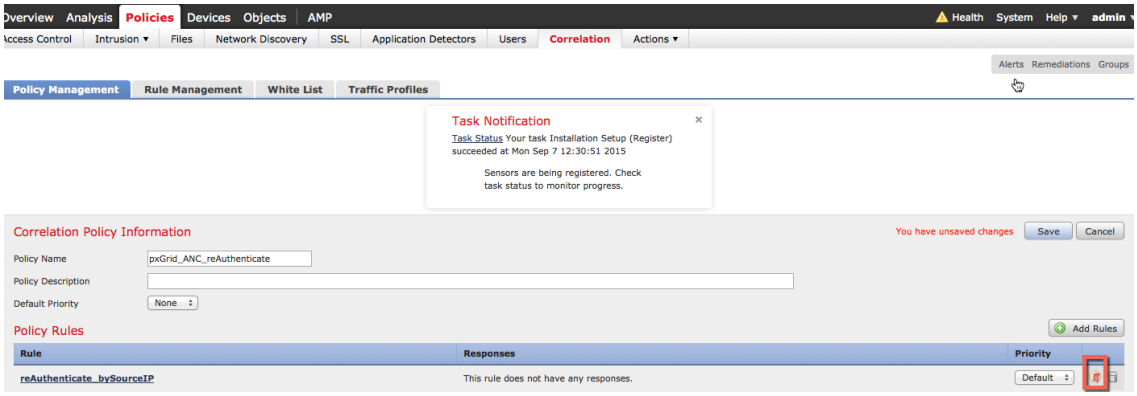
2단계 **Policies(정책)->Correlation(상관관계)->Rule Management(규칙 관리)->Create Rule(규칙 생성)**을 선택한 후 규칙 이름 **reAuthenticate_bySourceIP**를 추가하고 다음을 입력한 다음 **Save(저장)**를 클릭합니다.



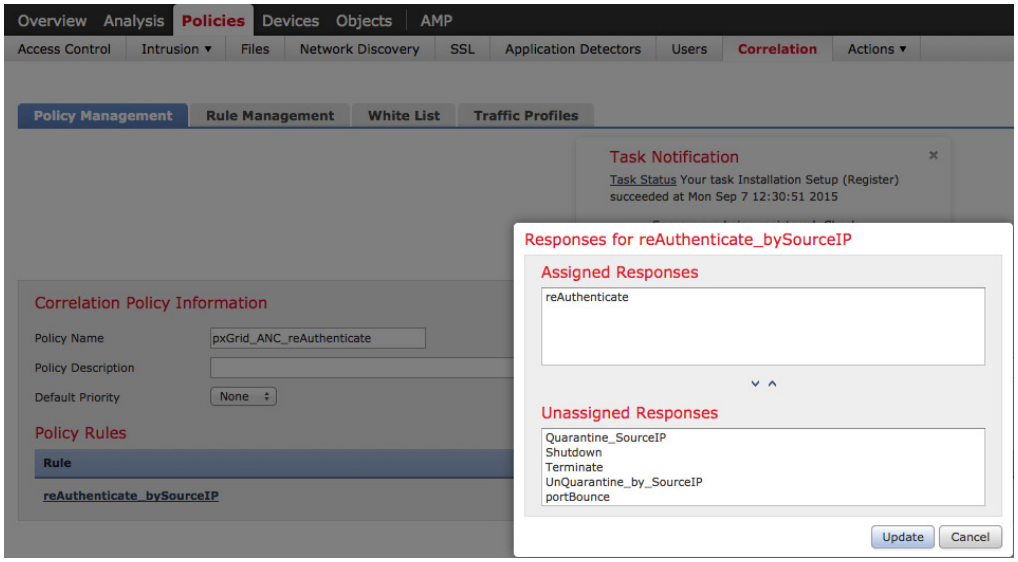
3단계 **Policies(정책)->Correlation(상관관계)->Policy Management(정책 관리)->pxGrid_ANC_reAuthenticate>Add rules(규칙 추가)**를 클릭하고 **"reAuthenticate_bySourceIP**를 선택한 후 규칙을 추가합니다.



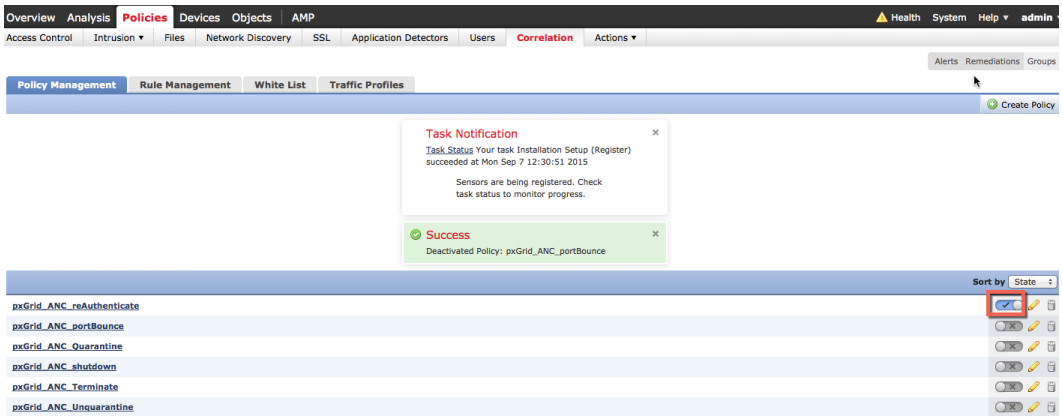
4단계 다음으로 응답을 추가합니다. **Responses(응답)** 탭을 클릭합니다.



5단계 **Policies(정책)->Correlation(상관관계)->pxGrid_ANC_reAuthenticate**를 선택하고 **reAuthenticate**를 **Assigned Responses(할당된 응답)**로 이동한 후 **Update(업데이트)->Save(저장)**를 클릭합니다.



6단계 정책을 설정하는 아래의 **버튼**을 클릭하여 종료 정책을 활성화합니다.

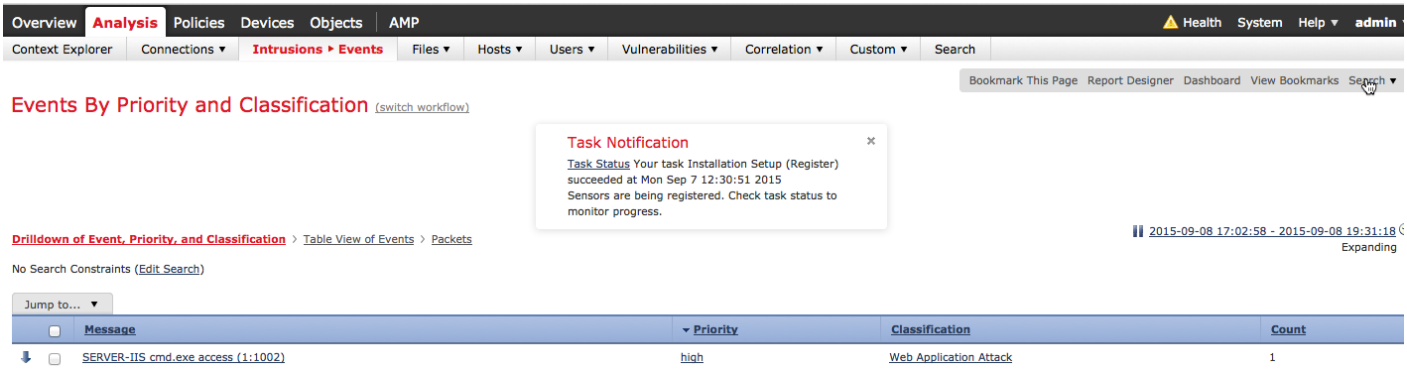


테스트

최종 사용자가 브라우저 창에 www.yahoo.com/cmd.exe를 입력합니다. 이렇게 하면 FireSIGHT의 pxGrid 침입 정책에서 "SERVER-IIS.cmd.exe 액세스" 규칙 위반 시 침입 이벤트가 트리거됩니다. 상관관계 정책에 정의된 대로 규칙에 할당된 재인증 완화 응답을 기반으로 하여 최종 사용자가 재인증됩니다.

1단계 최종 사용자가 브라우저에 www.yahoo.com/cmd.exe를 입력합니다.

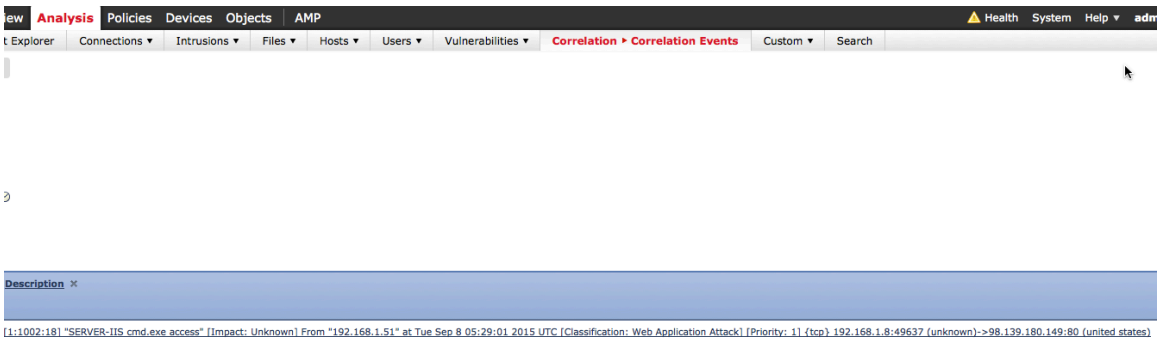
2단계 이렇게 하면 "웹 애플리케이션 공격" 침입 이벤트가 트리거됩니다.



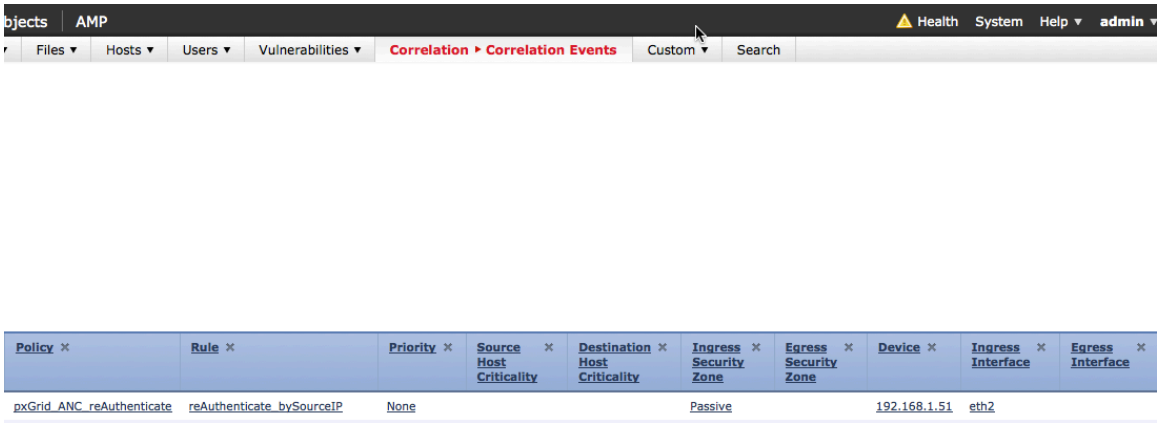
3단계 또한 "상관관계 이벤트"가 트리거됩니다.
소스 IP 주소에 속하는 최종 사용자가 재인증됩니다.

참고: 네트워크 검색 호스트 및 사용자가 설정되어 있지 않으므로 사용자 정보가 없습니다.

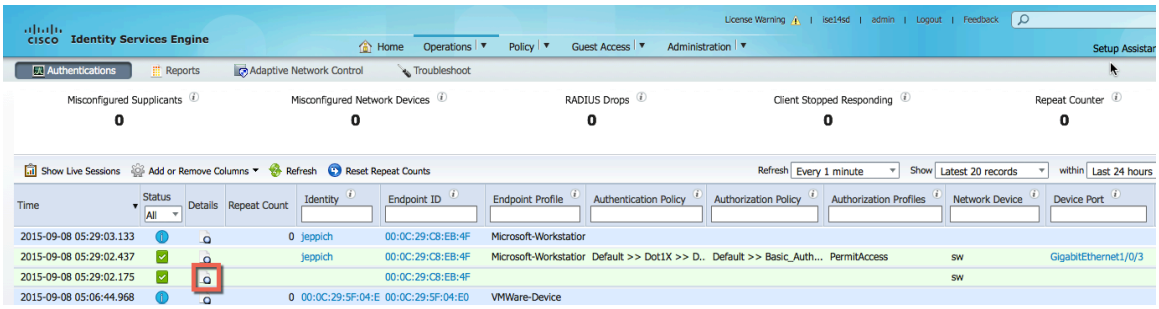
4단계 동일한 이벤트를 계속하는 경우
pxGrid_Intrusion_Policy 규칙에 포함된 규칙 위반에 주의하십시오.



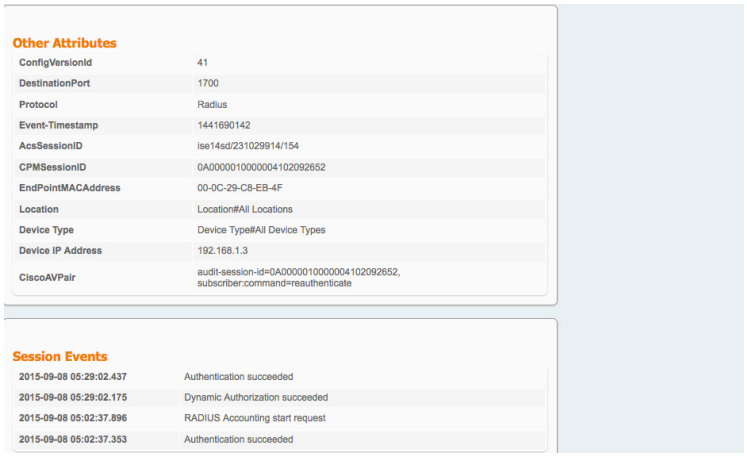
5단계 동일한 이벤트를 계속 진행하는 경우
할당된 재인증 완화 응답을 트리거한 상관관계 정책 및 상관관계 규칙에 주의하십시오.



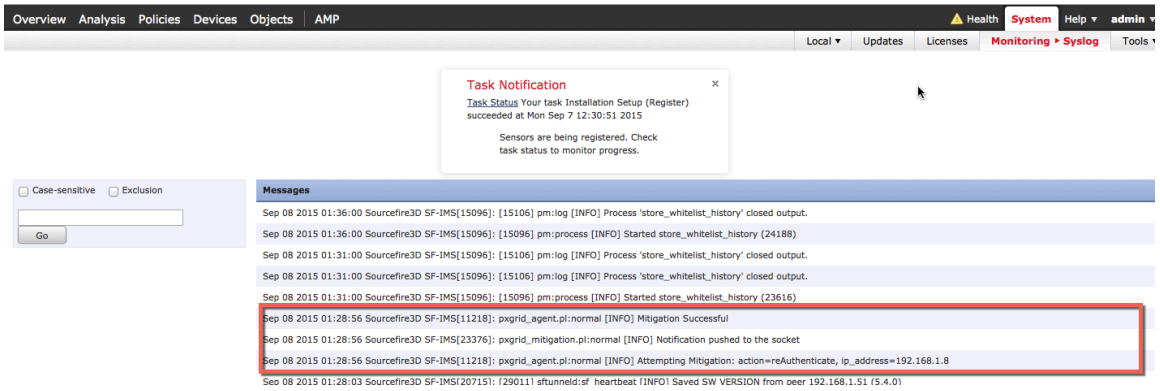
6단계 ISE에서 응답을 보려면 **Operations(작업)->Authentications(인증)**를 선택합니다.



7단계 세부 정보 버튼을 선택하면 포트가 CiscoAVpair 특성에 따라 비활성화되었음을 알 수 있습니다.



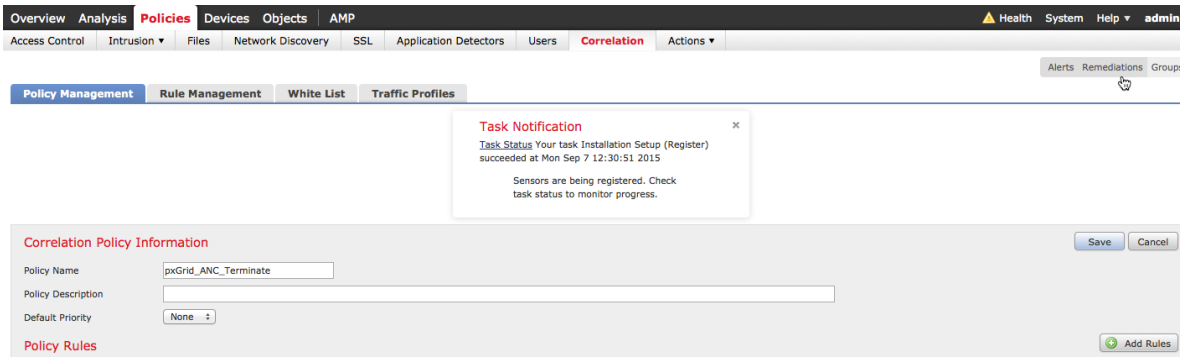
8단계 또한 FireSIGHT Management Center syslog 이벤트를 보고 재인증 완화 조치에 성공했는지 확인할 수 있습니다.



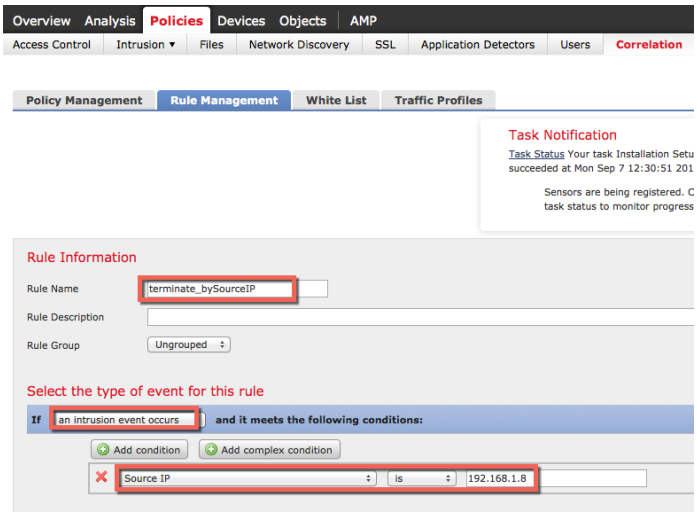
종료

종료 상관관계 정책이 생성됩니다.

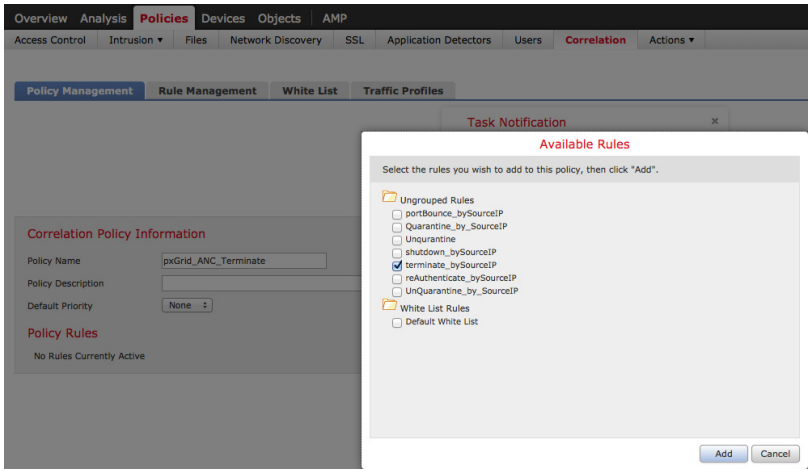
1단계 **Policies(정책)->Correlation(상관관계)->Policy Management(정책 관리)->Create Policy(정책 생성)->pxGrid ANC Terminate->Save(저장)**



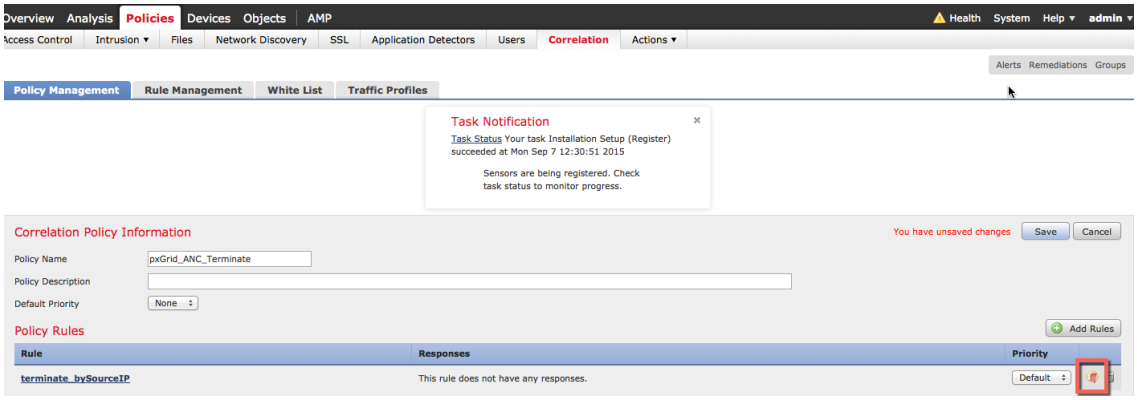
2단계 **Policies(정책)->Correlation(상관관계)->Rule Management(규칙 관리)->Create Rule(규칙 생성)**을 선택한 후 규칙 이름 **Terminate_by_SourceIP**를 추가하고 다음을 입력한 다음 **Save(저장)**를 클릭합니다.



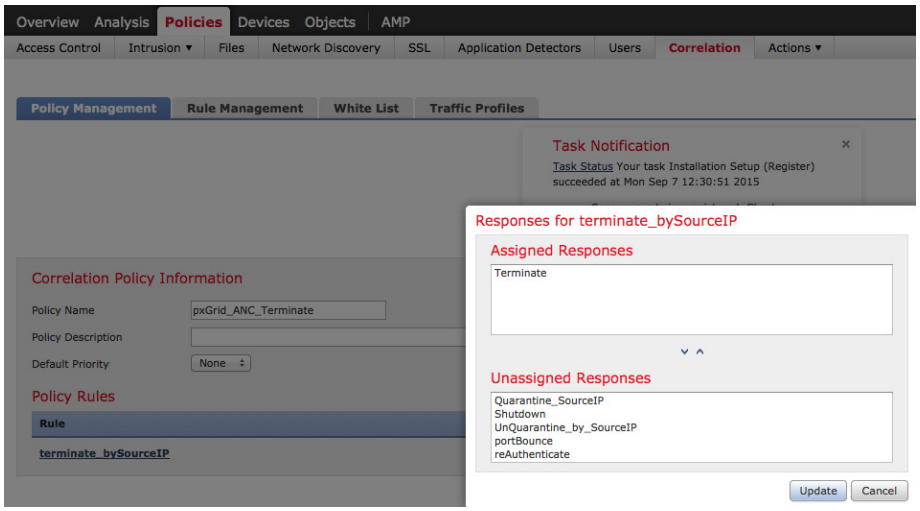
3단계 **Policies(정책)->Correlation(상관관계)->Policy Management(정책 관리)->pxGrid ANC Terminate>Add rule(규칙 추가)**을 선택하고 **Terminate_by_SourceIP**를 선택하여 규칙을 추가합니다.



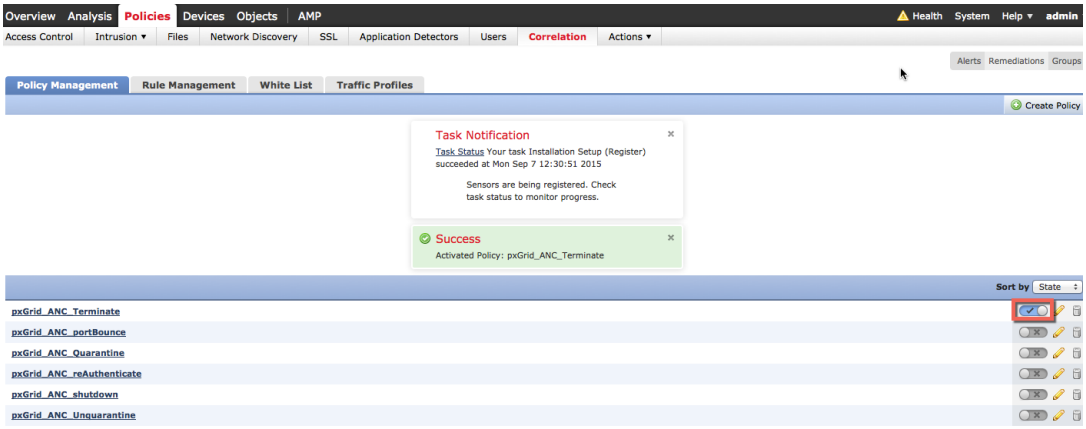
4단계 다음으로 응답을 추가합니다. **Responses(응답)** 탭을 클릭합니다.



5단계 **Policies(정책)->Correlation(상관관계)->pxGrid_ANC_Terminate**를 선택하고 **Terminate**를 **Assigned Responses(할당된 응답)**로 이동한 후 **Update(업데이트)->Save(저장)**를 클릭합니다.



6단계 정책을 설정하는 아래의 **버튼**을 클릭하여 종료 정책을 활성화합니다.

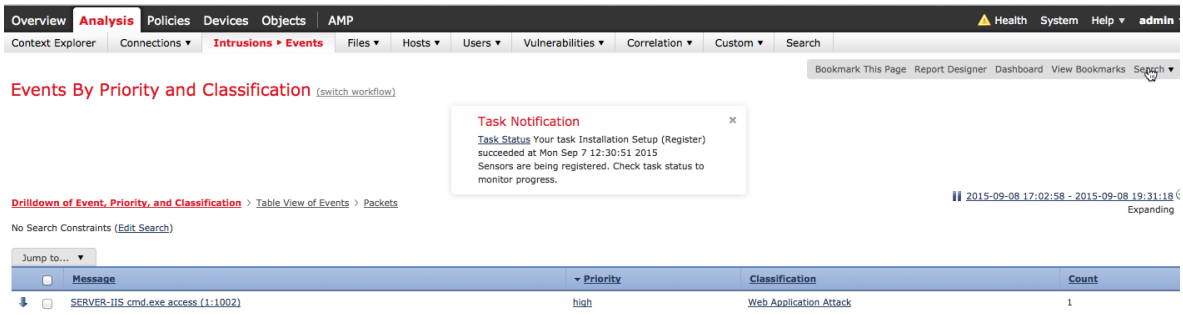


테스트

최종 사용자가 브라우저 창에 www.yahoo.com/cmd.exe를 입력합니다. 이렇게 하면 FireSIGHT의 pxGrid 침입 정책에서 "SERVER-IIS.cmd.exe 액세스" 규칙 위반 시 침입 이벤트가 트리거됩니다. 상관관계 정책에 정의된 대로 규칙에 할당된 종료 완화 응답을 기반으로 하여 최종 사용자의 세션이 종료됩니다.

1단계 최종 사용자가 브라우저에 www.yahoo.com/cmd.exe를 입력합니다.

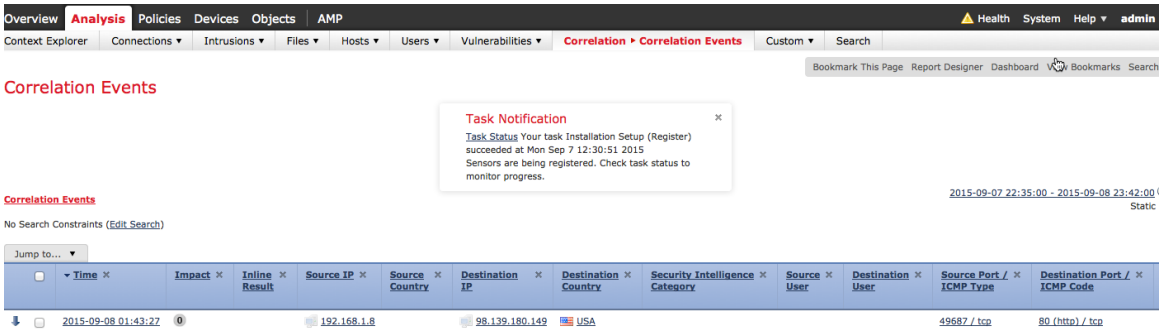
2단계 이렇게 하면 "웹 애플리케이션 공격" 침입 이벤트가 트리거됩니다.



3단계 또한 "상관관계 이벤트"가 트리거됩니다.

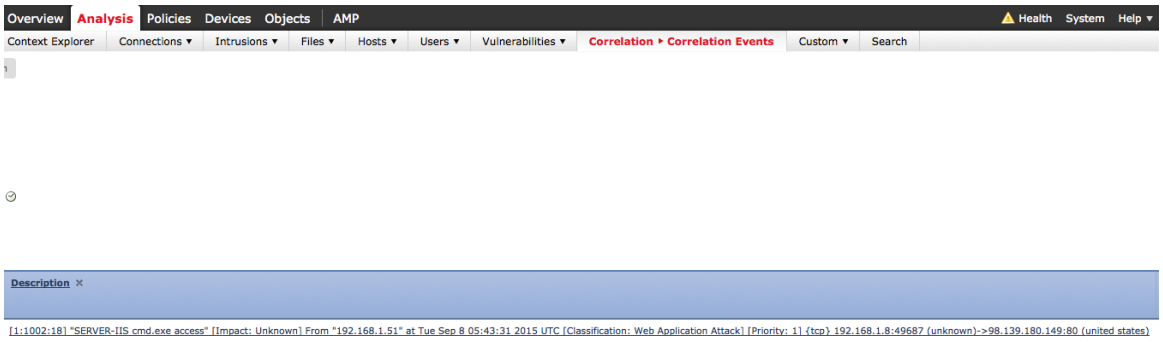
소스 IP 주소에 속하는 최종 사용자 세션이 종료됩니다.

참고: 네트워크 검색 호스트 및 사용자가 설정되어 있지 않으므로 사용자 정보가 없습니다.

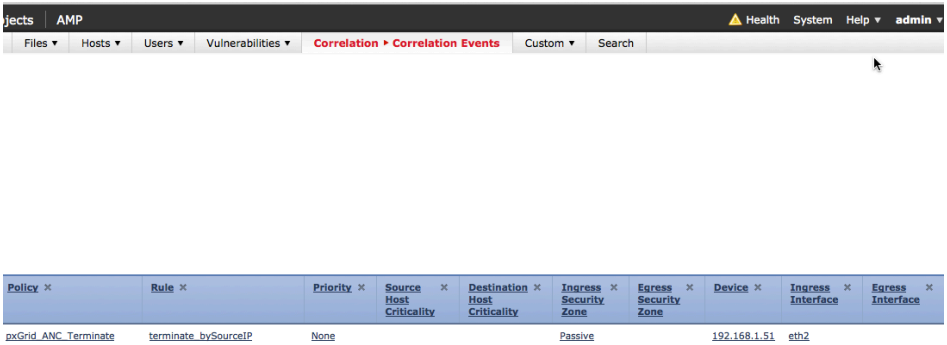


4단계 동일한 이벤트를 계속하는 경우

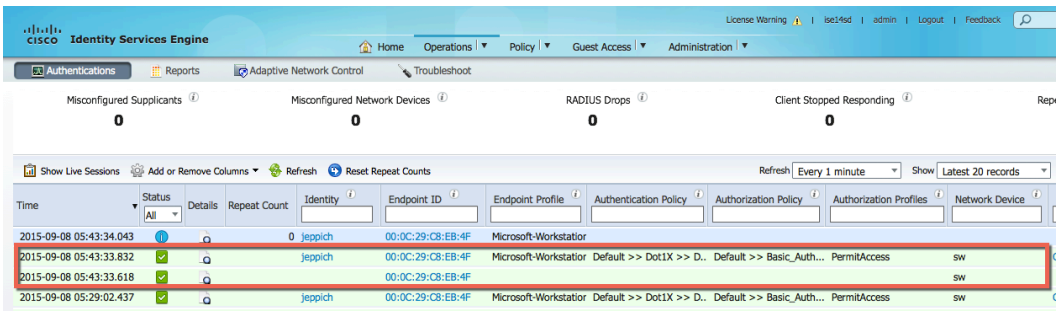
pxGrid_Intrusion_Policy 규칙에 포함된 규칙 위반에 주의하십시오.



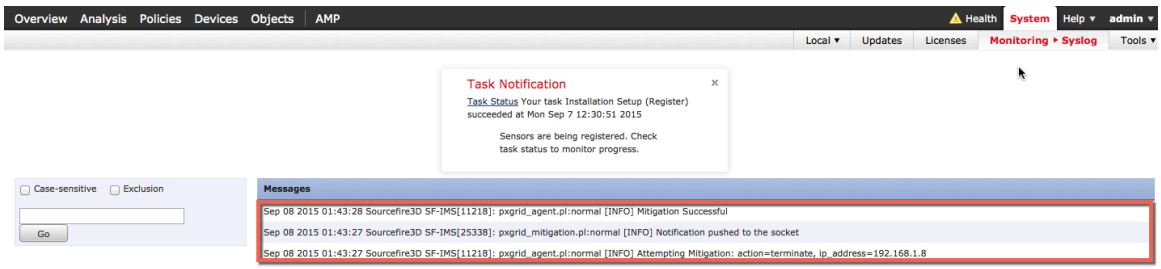
5단계 동일한 이벤트를 계속 진행하는 경우
할당된 종료 완화 응답을 트리거한 상관관계 정책 및 상관관계 규칙에 주의하십시오.



6단계 ISE에서 응답을 보려면 Operations(작업)->Authentications(인증)를 선택합니다.



7단계 또한 FireSIGHT Management Center syslog 이벤트를 보고 종료 완화 조치에 성공했는지 확인할 수 있습니다.

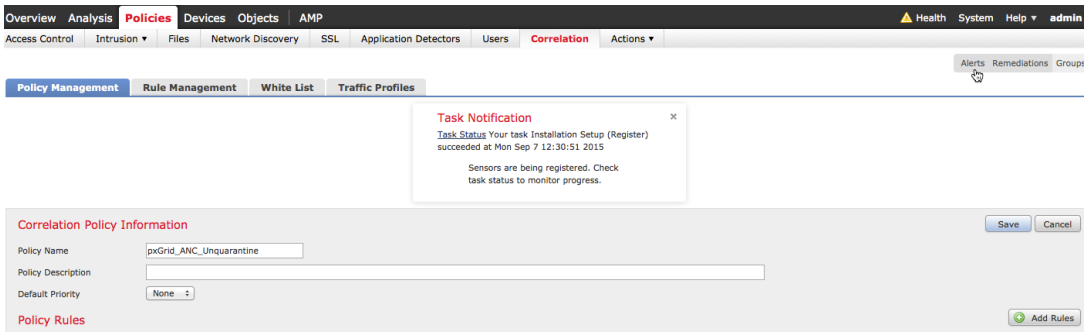


격리 해제 상관관계 정책

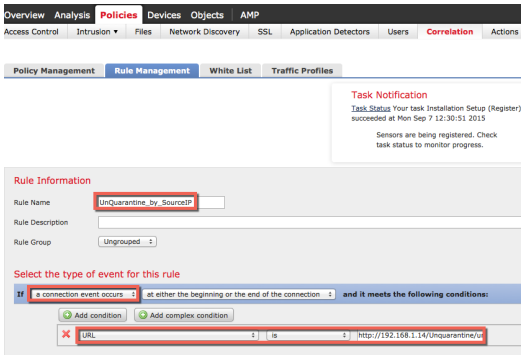
격리 해제 상관관계 정책 및 규칙이 나머지 상관관계 정책과 동일한 프로세스로 생성됩니다. 유일한 차이점은 상관관계 규칙이 "침입" 이벤트 대신 "연결 이벤트"에서 트리거된다는 것입니다. 최종 사용자가 격리 해제 규칙에 정의된 URL로 이동하면 격리 해제 완화 응답이 엔드포인트를 격리 해제합니다.

또한 모든 HTTP/HTTPS 트래픽이 모니터링되고 로깅되며 기본 액세스 정책에 할당될 수 있도록 "연결" 규칙을 생성해야 합니다. 기본 액세스 정책에는 pxGrid 침입 정책도 포함되어 있습니다.

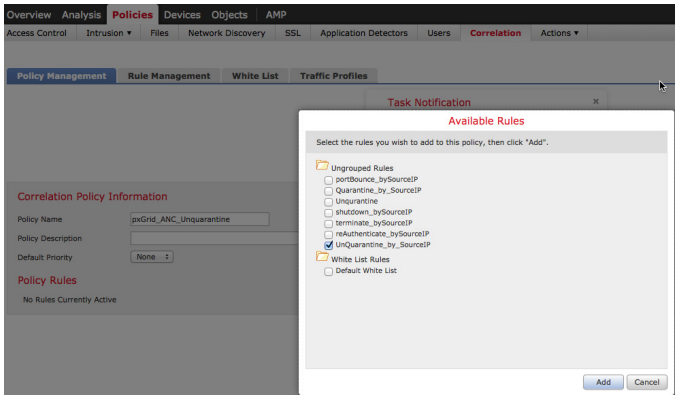
1단계 **Policies(정책)->Correlation(상관관계)->Policy Management(정책 관리)->Create Policy(정책 생성)->pxGrid_ANC_Unquarantine->Save(저장)**



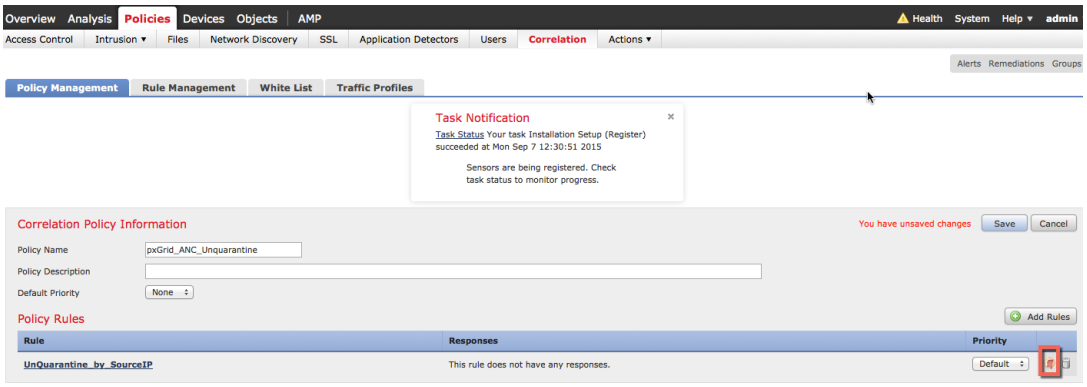
2단계 **Policies(정책)->Correlation(상관관계)->Rule Management(규칙 관리)->Create Rule(규칙 생성)**을 선택하고 규칙 이름 **UnQuarantine_by_DestinationIP**를 추가한 후 **Save(저장)**를 클릭합니다.



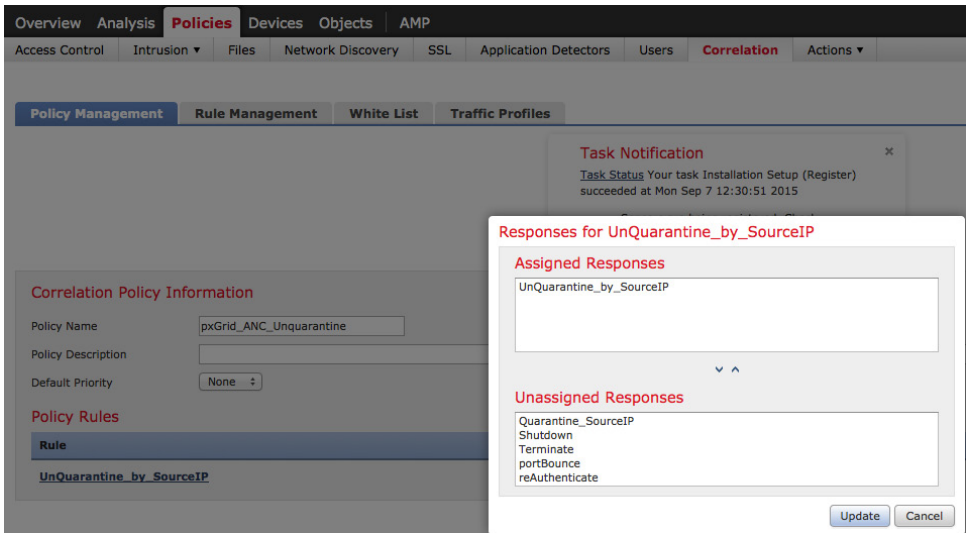
3단계 **Policies(정책)->Correlation(상관관계)->Policy Management(정책 관리)->pxGrid_ANC_Unquarantine->Add rules(규칙 추가)->UnQuarantine_by_DestinationIP**, 이후 변경 사항을 **저장**합니다.



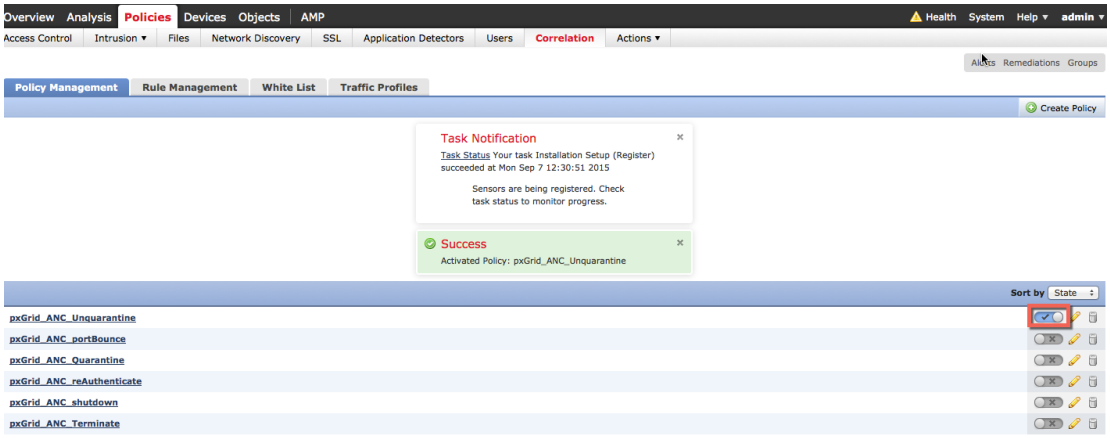
4단계 다음으로 응답을 추가합니다. **Responses(응답)** 탭을 클릭합니다.



5단계 **Policies(정책)->Correlation(상관관계)->UnQuarantine_by_DestinationIP**를 선택하고 **UnQuarantine_SourceIP**를 **Assigned Responses(할당된 응답)**로 이동한 후 **Update(업데이트)->Save(저장)**를 클릭합니다.



6단계 정책을 활성화합니다.

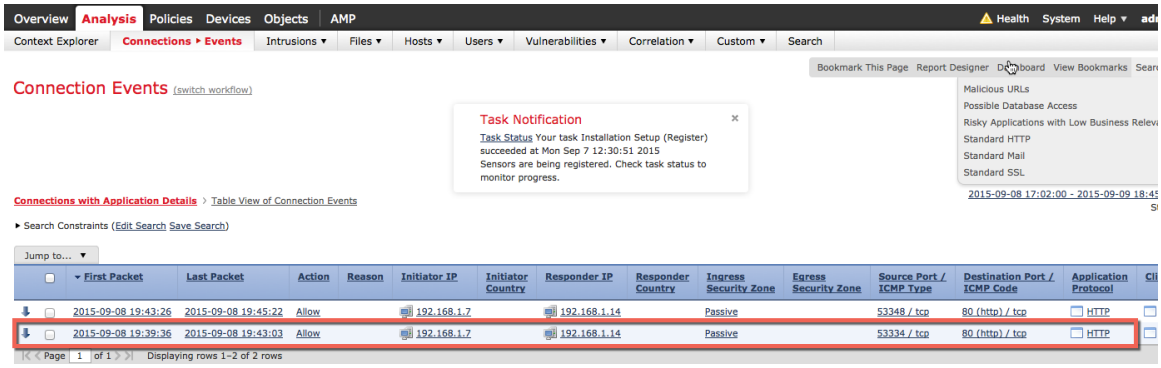


테스트

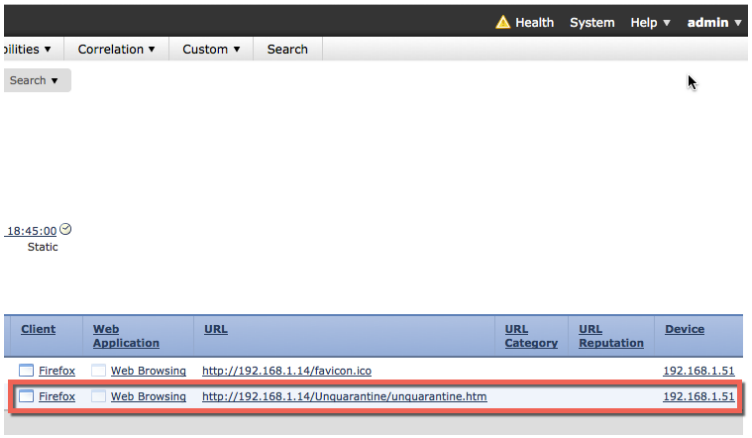
최종 사용자가 브라우저 창에 www.yahoo.com/cmd.exe를 입력합니다. 이렇게 하면 FireSIGHT의 pxGrid 침입 정책에서 "SERVER-IIS.cmd.exe 액세스" 규칙 위반 시 침입 이벤트가 트리거됩니다. 상관관계 정책에 정의된 대로 규칙에 할당된 격리 해제 완화 응답을 기반으로 하여 엔드포인트가 격리 해제됩니다.

1단계 최종 사용자가 브라우저에 http://192.168.1.14/Unquarantine/unquarantine.htm을 입력합니다.

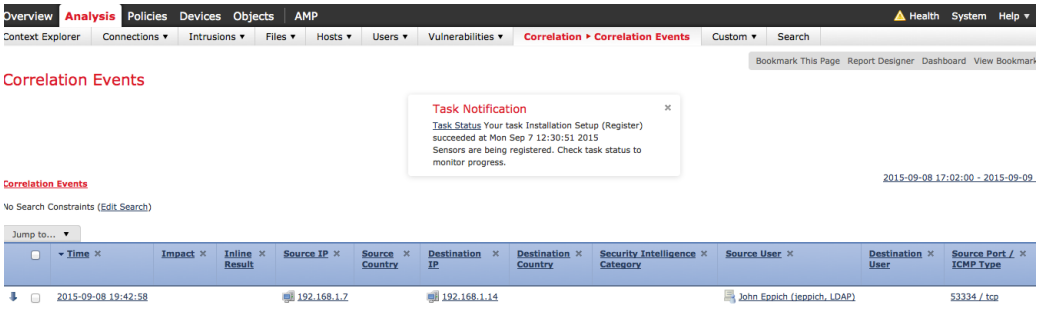
2단계 이렇게 하면 "연결" 이벤트가 트리거됩니다.



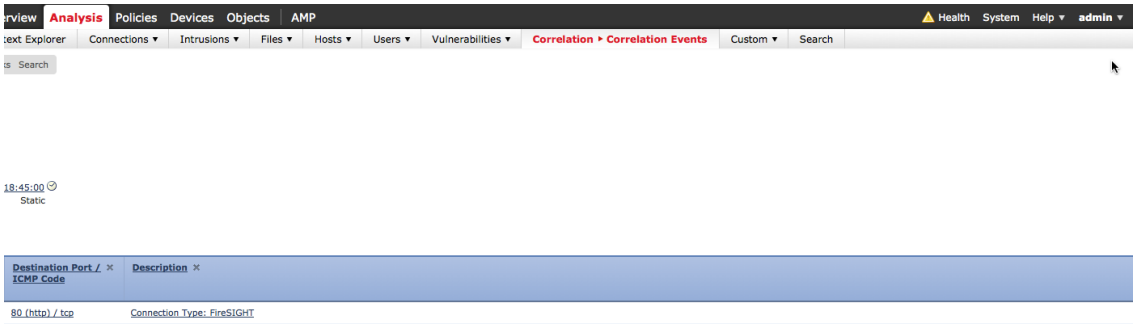
3단계 다음은 연결 이벤트의 다음 부분입니다.



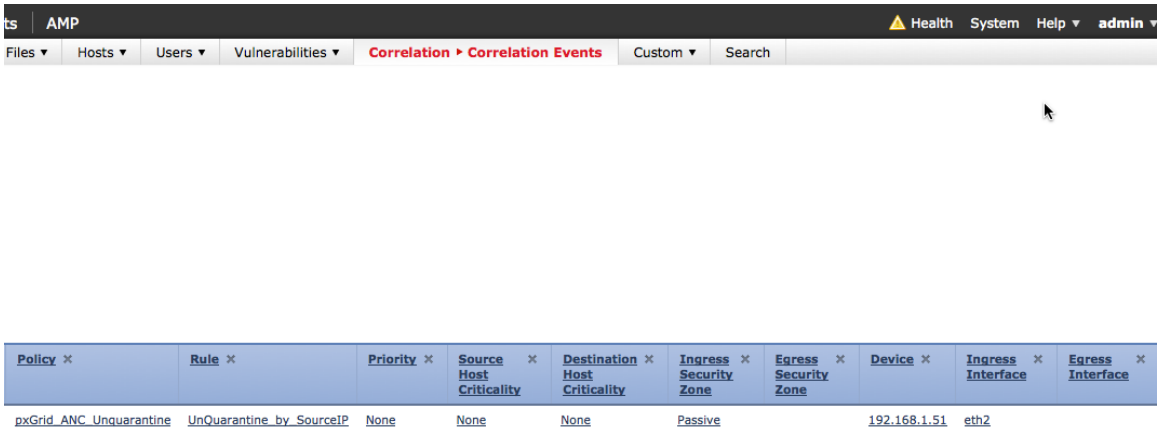
4단계 또한 "상관관계 이벤트"가 트리거됩니다.
소스 IP 주소가 격리 해제됩니다.



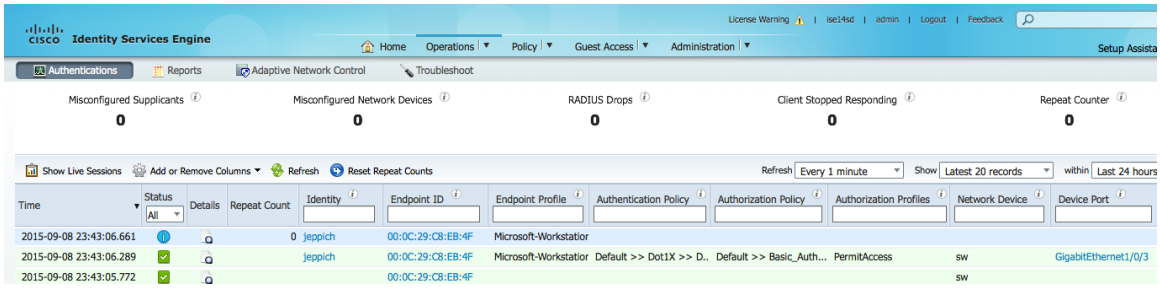
5단계 동일한 이벤트를 계속하는 경우
연결 이벤트에 주의하십시오.



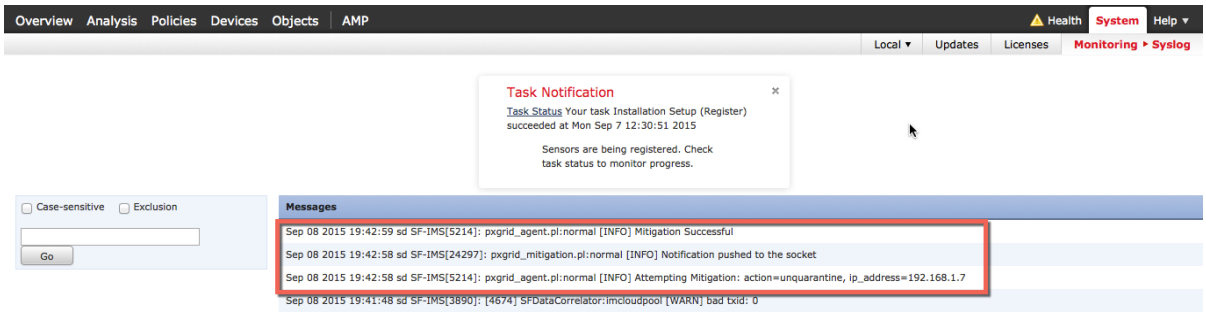
6단계 동일한 이벤트를 계속 진행하는 경우
할당된 격리 완화 응답을 트리거한 상관관계 정책 및 상관관계 규칙에 주의하십시오.



7단계 ISE에서 응답을 보려면 **Operations(작업)->Authentications(인증)**를 선택합니다.



8단계 또한 FireSIGHT Management Center syslog 이벤트를 보고 격리 완화 조치에 성공했는지 확인할 수 있습니다.



문제 해결

ISE pxGrid 서비스가 나타나지 않음

해결 방법: ISE pxGrid 노드에서 **"application stop ise"** 중단을 실행하십시오.

pxGrid 에이전트 인증서 오류 메시지

해결 방법: FireSIGHT Management Center Syslog 메시지에서 인증서 오류 메시지를 확인하십시오.

인증서의 전체 경로(**/Volume/home/admin/...**)가 올바른지 확인하십시오.

FireSIGHT Management Center 및 ISE pxGrid 노드 간에 시간이 동기화되었는지 확인하십시오.

FireSIGHT, ISE pxGrid 노드 및 엔드포인트가 모두 DNS를 분석할 수 있어야 합니다.

FireSiGHT Management Center가 ISE와 통신하지 않음

해결 방법: FireSIGHT, ISE pxGrid 노드 및 엔드포인트가 모두 DNS를 분석할 수 있어야 합니다.

FireSIGHT Management Center, 센서 및 ISE pxGrid 노드 간에 시간이 동기화되었는지 확인하십시오.

FireSIGHT Management Center를 재부팅하십시오.

FireSIGHT Management Center에 상관관계 이벤트가 표시되지 않음

해결 방법: FireSIGHT Management Center, 센서 및 ISE pxGrid 노드 간에 시간이 동기화되었는지 확인하십시오.

FireSIGHT 완화 시도 실패

해결 방법: FireSIGHT Management Center, 센서 및 ISE pxGrid 노드 간에 시간이 동기화되었는지 확인하십시오.

FireSIGHT Management Center를 재부팅하십시오.

완화 "조회 실패" 시도

해결 방법: 디바이스의 IP 주소가 ISE를 통해 인증되었는지 확인하십시오. 소스에 대한 교정 유형이 구성되었습니다.

FireSIGHT Management Console의 pxGrid 연결 실패 시도 syslog 오류 메시지

해결 방법: FireSIGHT Management Console CLI에서 다음을 실행하여 ISE pem 파일에 인증서가 포함되어 있는지 확인하십시오.

```
openssl x509 –noout –text –in ise14lab.pem
```

pem 파일에 인증서가 포함되어야 합니다.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            56:19:bf:90:00:00:00:00:ab:b7:4f:a0:57:21:a0:03
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=ise14.lab8.com
        Validity
            Not Before: Oct 11 01:46:56 2015 GMT
            Not After : Oct 10 01:46:56 2016 GMT
        Subject: CN=ise14.lab8.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a3:9e:b5:4e:68:e7:f9:db:4b:c6:3f:f4:f9:12:
                    e8:6f:ba:05:4d:b6:0b:13:fc:3c:35:61:ed:d6:d1:
                    0d:65:f4:e5:38:3d:5a:55:ac:94:e6:34:57:44:30:
                    64:75:9c:35:6f:f2:9c:0a:d6:f4:86:9d:94:10:2f:
                    b6:eb:ba:76:e2:33:84:77:70:20:71:a0:23:21:4b:
                    af:cc:6a:d9:c2:ba:9a:9c:eb:27:e6:b3:64:a7:e5:
                    29:31:65:03:23:06:d8:39:b9:74:48:32:75:de:6a:
                    5c:71:6a:27:8e:e6:d3:58:d0:44:e6:52:ec:3f:d8:
                    38:5b:d2:fc:c2:d6:90:02:e8:5a:9f:a7:a2:dc:44:
                    81:31:fc:5e:fd:60:41:40:e6:57:09:9b:d6:11:0e:
                    a6:93:1b:b0:c1:c5:9b:c4:98:45:af:78:1b:9c:55:
                    02:d3:e5:91:48:8b:1c:77:46:e6:49:d5:f0:5f:4c:
                    51:6c:d0:9b:82:25:b3:32:3b:ab:64:32:49:e5:b7:
                    45:db:9e:2c:c4:87:dc:d1:ff:9c:f8:99:d7:88:be:
                    c6:9d:7c:c6:ea:74:bd:b0:c5:a2:b5:a4:d4:fd:04:
                    64:61:db:c5:cb:07:69:d3:c7:72:8f:17:a7:2e:04:
                    11:d5:58:0d:00:aa:26:3a:5f:c3:08:2c:dc:a0:26:
                    e8:87
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE
            X509v3 Key Usage:
                Digital Signature, Key Encipherment, Key Agreement, Certificate Sign
            X509v3 Subject Key Identifier:
                8E:C0:5C:25:3A:5C:4E:9F:C4:6F:66:41:33:C3:6A:27:4C:00:A1:17
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            Netscape Cert Type:
                SSL Server
    Signature Algorithm: sha1WithRSAEncryption
         40:cc:1b:4d:94:94:d9:68:7b:95:6e:36:e4:3a:41:41:6c:f1:
         4e:f0:1a:fa:3e:42:7e:b0:73:80:ad:0f:4a:bb:d4:ce:cd:da:
         ef:32:f9:d0:58:f0:c4:90:0c:97:20:88:26:f5:9c:96:d7:61:
         fe:05:09:40:0a:f6:33:04:dc:30:ec:10:d2:82:f2:ec:5d:f9:
         b2:d1:69:5e:ed:ae:a5:b4:6d:b1:c4:16:bf:67:14:e9:ec:4f:
         9c:83:07:35:64:26:9d:e4:41:bb:65:5e:77:7b:e5:da:d1:98:
         9c:c0:50:fc:ba:a4:dc:51:c4:e5:49:28:55:9f:40:0c:61:20:
         1d:49:e3:ca:a5:a2:35:74:5c:57:71:17:32:71:2c:2b:51:2c:
         cf:49:30:9e:31:28:19:4a:62:1b:4a:86:21:0d:54:73:b8:86:
         92:df:8c:ae:3d:92:91:5f:70:d5:17:4c:14:07:d1:0c:59:0b:
         3d:6d:6a:16:ca:a9:3a:06:b8:37:f1:28:af:c5:03:32:30:82:
```

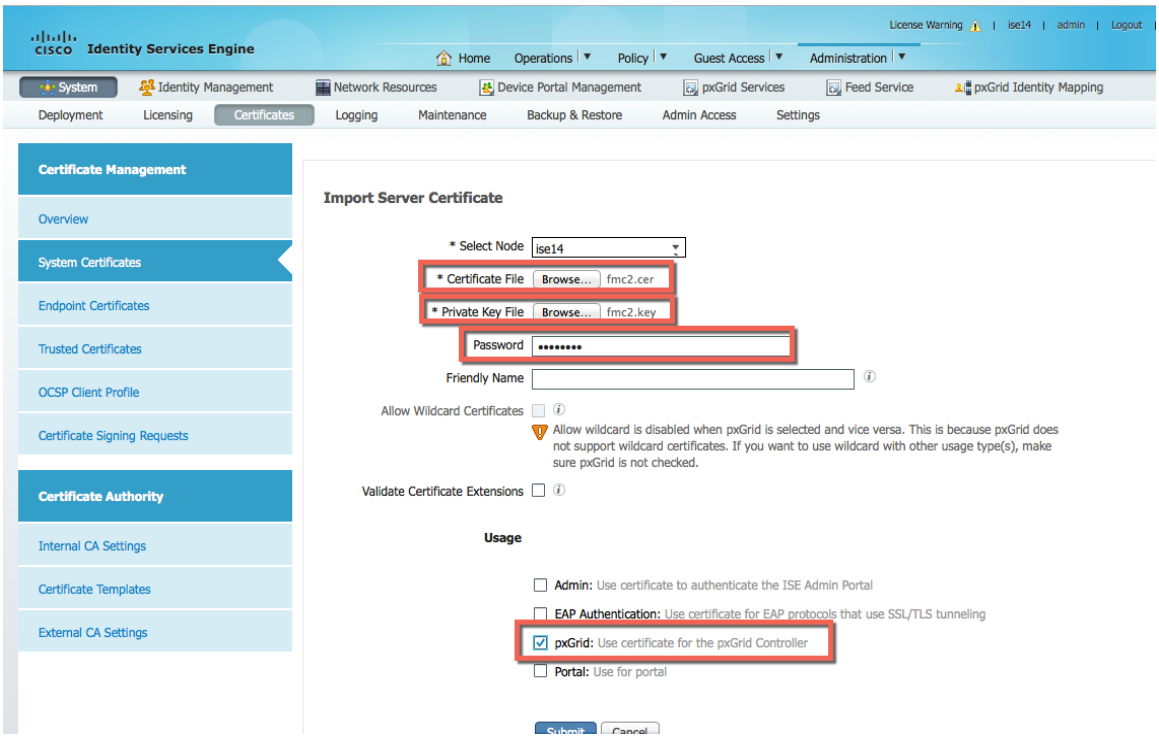
```
3d:53:8b:77:ed:e7:8a:5a:38:b6:3b:0e:c0:93:63:c1:f6:2e:
a3:ce:33:a4:0a:82:d4:f7:8f:0f:c2:99:9e:96:36:c5:89:a2:
9f:f3:66:01:12:da:13:53:d4:92:ef:17:9e:2b:26:4b:3c:7d:
1f:6f:a3:b4
```

이와 같이 표시되지 않는 경우 ISE ID 셀프 서명된 공개-개인 키 쌍을 내보내고 비밀번호를 제공한 후 ISE ID 셀프 서명된 인증서를 FMC의 신뢰할 수 있는 CA 저장소에 추가합니다.

ISE 시스템 저장소로 가져와서 셀프 서명된 인증서 확인

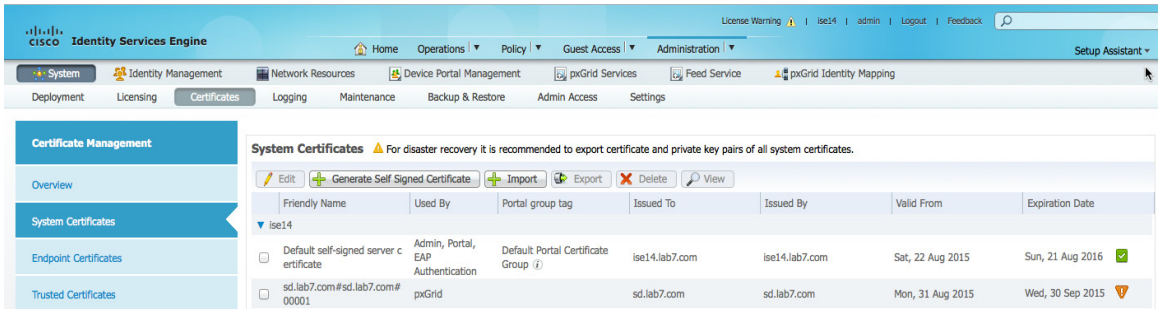
해결 방법: 이것이 반드시 문제는 아니지만 벤더의 공개/개인 키 쌍을 ISE의 신뢰할 수 있는 시스템 저장소로 가져올 수 있습니다. 이것은 pxGrid SDK의 ISE 샘플 인증서를 사용하기 때문이며, 테스트용으로만 사용해야 하고 프로덕션 환경에서는 사용하지 않는 것이 좋습니다. **셀프 서명된 인증서에 대한 FireSIGHT Management Center 구성**의 단계를 사용하여 셀프 서명된 인증서를 구성하십시오.

1단계 FireSIGHT 내부 CA 공개/개인 키 쌍을 ISE 인증서 시스템 저장소로 가져옵니다. 개인 키 비밀번호가 필요합니다.
Administration(관리)->System(시스템)->Certificates(인증서)->System Certificates(시스템 인증서)로 이동하여 FireSIGHT 내부 공개/개인 키 쌍을 가져옵니다. 개인 키 비밀번호를 입력합니다.



2단계 인증서 "Usage(사용)"를 pxGrid로 선택한 후 Submit(제출)를 클릭합니다.

3단계 다음과 같이 표시되어야 합니다.



솔루션 경고

pxGrid 및 ID 매핑 서비스 다시 시작

설명: 인증서를 ISE 구축의 신뢰 저장소에서 가져오거나 삭제할 때 ISE pxGrid 노드에서 pxGrid 및 ID 매핑 서비스가 다시 시작됩니다.

결함 제기: CSCuv43145

해결책: 서비스가 자동으로 다시 시작되므로 조치가 필요하지 않지만 서비스가 다시 시작되는 동안 새 격리 이벤트가 처리되지 않습니다.

해결 계획: ISE Carlsbad 릴리스 2016년 봄

활성 pxGrid 노드가 GUI에 반영되지 않고 CLI에 반영됨

설명: pxGrid HA 구축에서 두 개의 pxGrid 노드가 사용 가능한 경우 한 노드는 활성 상태이며 다른 노드는 대기 상태입니다. 활성 상태의 노드를 식별하려면 관리자가 CLI에서 pxGrid 상태를 검토해야 합니다. UI 구축 페이지에 상태가 표시되지 않습니다. 이 추가 사항은 Carlsbad에서 작성되었습니다.

해결책: CLI를 사용하여 활성/수동 상태를 판별하십시오.

해결 계획: ISE Carlsbad 릴리스 2016년 봄

참조

분산 ISE 환경에서 pxGrid 구성: http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-88-Configuring-pxGrid-in-an-ISE-Distributed-Environment.pdf

Cisco pxGrid를 사용하여 인증서를 배포하는 방법: CA 서명 ISE pxGrid 노드 및 CA 서명 pxGrid 클라이언트 구성: http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-89-CA_signed_pxGridISEnode_CAsigned_pxGridclient.pdf

Cisco pxGrid를 사용하여 인증서를 배포하는 방법: ISE pxGrid 노드 및 pxGrid 클라이언트를 통해 셀프 서명된 인증서: http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-90-Self_signed_pxGridClient_selfsigned_pxGrid.pdf