FireSIGHT 시스템의 초기 컨피그레이션 단계

목차

소개

FireSIGHT Management Center 또는 FirePOWER Device를 이미지로 재구성한 후 시스템이 정상적으로 작동하고 침입 이벤트에 대한 알림을 생성하려면 몇 가지 단계를 완료해야 합니다.라이센스 설치, 어플라이언스 등록, 상태 정책 적용, 시스템 정책, 액세스 제어 정책, 침입 정책 등이 문서는 FireSIGHT System Installation Guide의 보충 자료입니다.

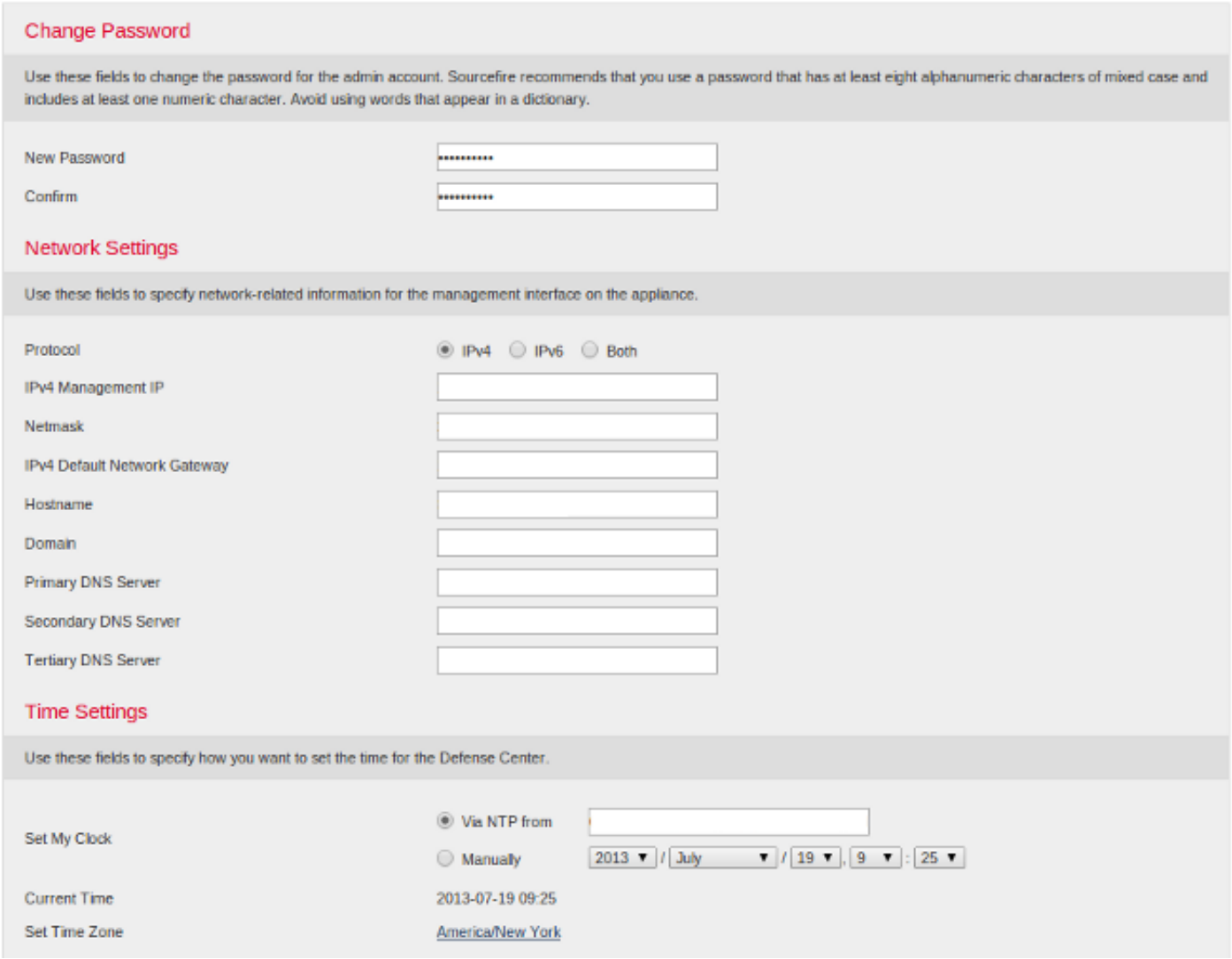
전제 조건

이 설명서에서는 FireSIGHT System 설치 가이드를 주의 깊게 읽었다고 가정합니다.

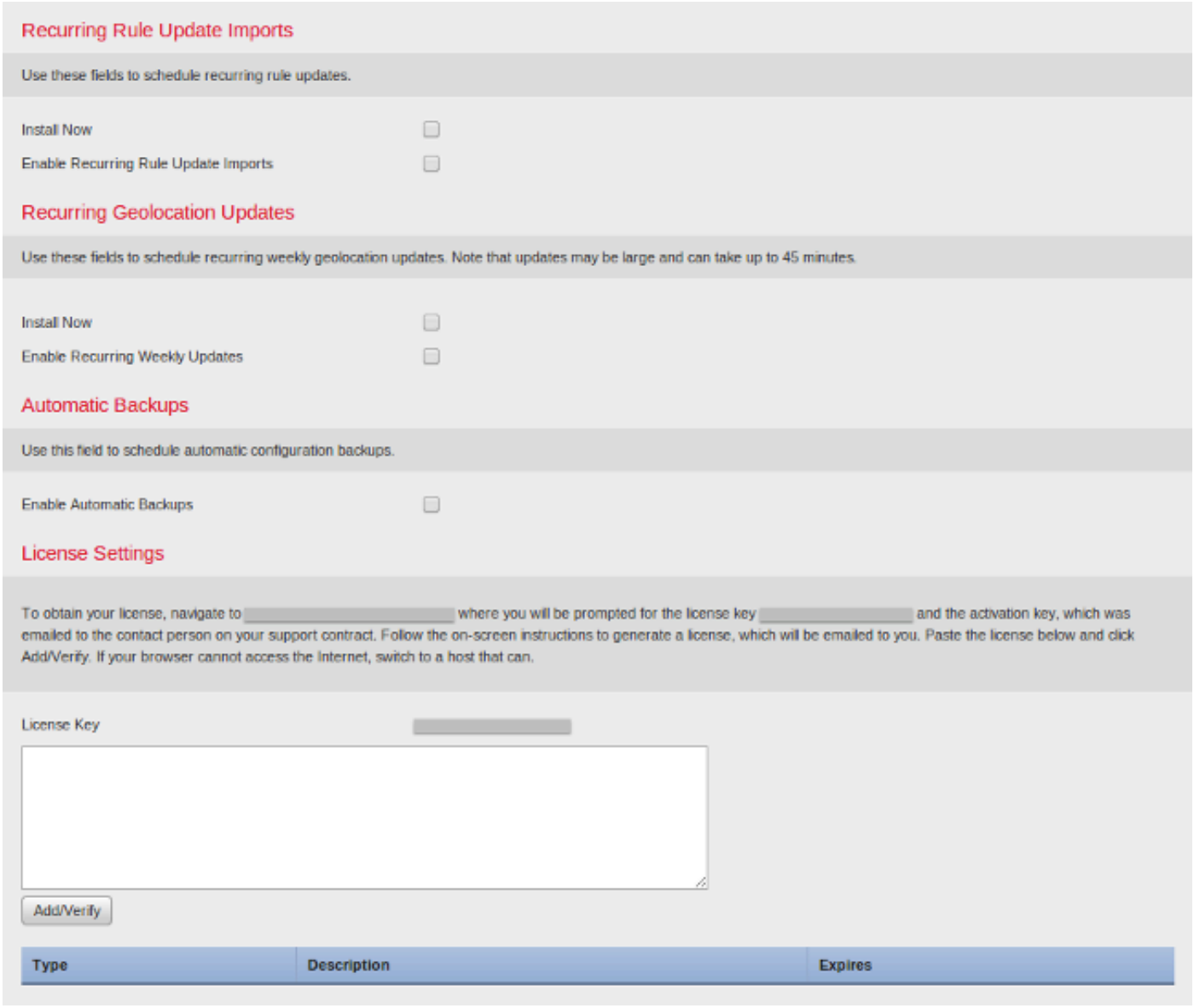
구성

1단계:초기 설정

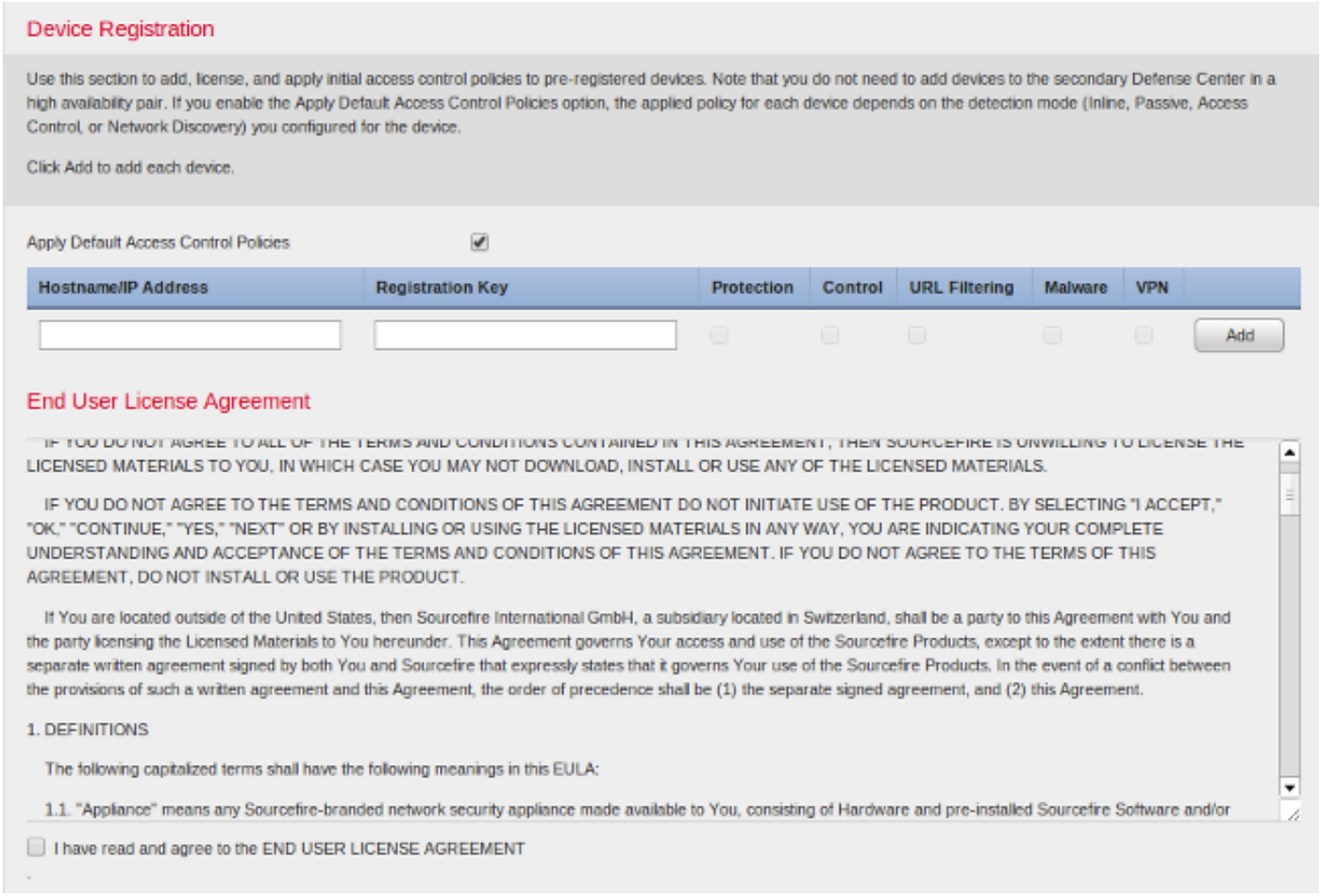
FireSIGHT Management Center에서 아래 그림과 같이 웹 인터페이스에 로그인하고 설정 페이지에서 초기 구성 옵션을 지정하여 설정 프로세스를 완료해야 합니다.이 페이지에서 관리자 비밀번호를 변경해야 하며 도메인 및 DNS 서버, 시간 컨피그레이션과 같은 네트워크 설정을 지정할 수도 있습니다.



선택적으로 반복 규칙 및 지오로케이션 업데이트와 자동 백업을 구성할 수 있습니다.모든 기능 라이센스를 이 시점에 설치할 수도 있습니다.



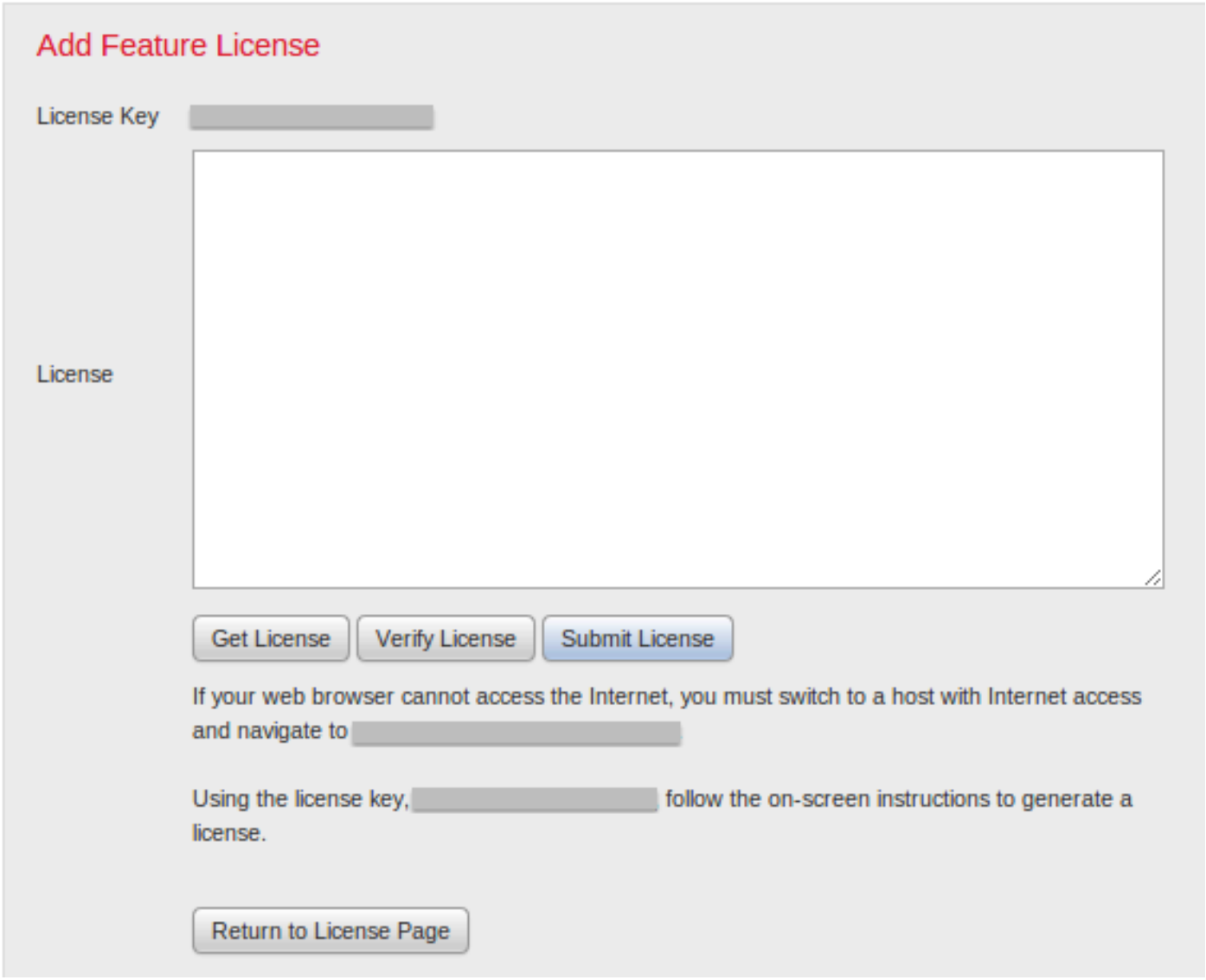
이 페이지에서 FireSIGHT Management Center에 디바이스를 등록하고 탐지 모드를 지정할 수도 있습니다.등록 중에 선택하는 탐지 모드 및 기타 옵션은 시스템에서 생성하는 기본 인터페이스, 인라인 집합, 영역 및 관리되는 디바이스에 처음 적용되는 정책을 결정합니다.



2단계:라이센스 설치

초기 설정 페이지 중에 라이센스를 설치하지 않은 경우 다음 단계를 수행하여 작업을 완료할 수 있습니다.

- 다음 페이지로 이동합니다.**System(시스템) > Licenses(라이센스)**.
- Add New **License를 클릭합니다**.



라이센스를 받지 못한 경우 어카운트의 세일즈 담당자에게 문의하십시오.

3단계:시스템 정책 적용

시스템 정책은 FireSIGHT Management Center와 관리되는 디바이스 간의 인증 프로파일 및 시간 동기화에 대한 컨피그레이션을 지정합니다. 시스템 정책을 구성하거나 적용하려면 System(시스템) **> Local(로컬) > System Policy(시스템 정책)로 이동합니다**. 기본 시스템 정책이 제공되지만 관리되는 디바이스에 적용해야 합니다.

4단계:상태 정책 적용

상태 정책은 관리되는 디바이스가 FireSIGHT Management Center에 상태를 보고하는 방법을 구성하는 데 사용됩니다. Health Policy를 구성하거나 적용하려면 Health **> Health Policy로 이동합니다**. 기본 상태 정책이 제공되지만 관리되는 디바이스에 적용해야 합니다.

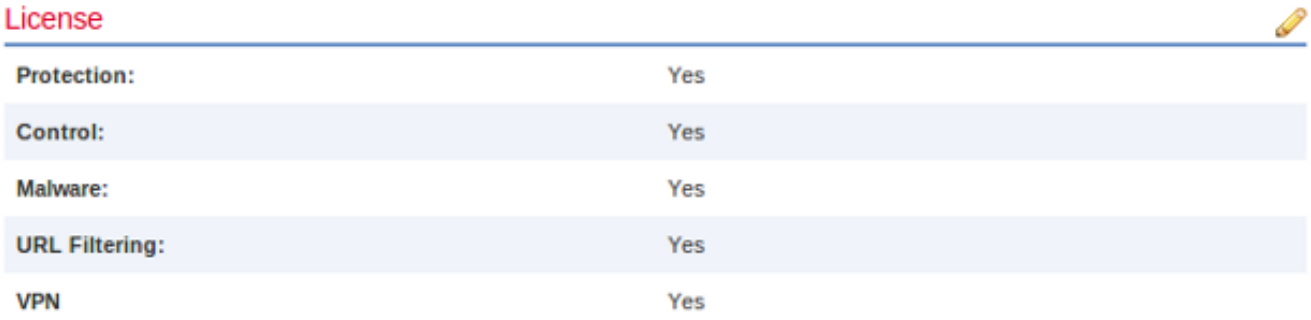
5단계:관리되는 디바이스 등록

초기 설정 페이지에서 디바이스를 등록하지 않은 경우 이 문서에서 FireSIGHT Management Center에 디바이스를 등록하는 방법에 대한 지침을 읽습니다.

6단계:설치된 라이센스 활성화

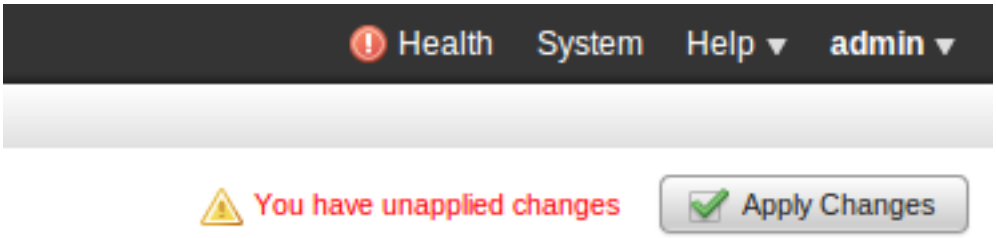
어플라이언스에서 기능 라이센스를 사용하려면 먼저 관리되는 각 디바이스에 대해 활성화해야 합니다.

1. 다음 페이지로 이동합니다.**디바이스 > 디바이스 관리**.
2. 라이센스를 활성화할 디바이스를 클릭하고 Device 탭을 입력합니다.
3. License(라이센스) 옆에 있는 Edit(*연필* 아이콘)를 클릭합니다.



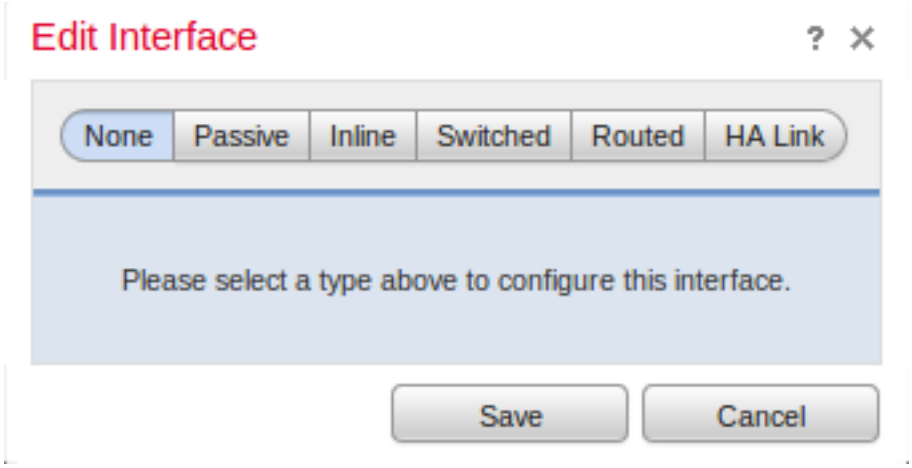
이 디바이스에 필요한 라이센스를 활성화하고 Save(저장)를 **클릭합니다**.

오른쪽 상단에 "*You have unapplied changes*"라는 메시지가 표시됩니다.이 경고는 디바이스 관리 페이지에서 벗어나 **Apply Changes(변경 사항 적용)** 버튼을 클릭할 때까지 이동하더라도 활성 상태로 유지됩니다.



7단계:센싱 인터페이스 구성

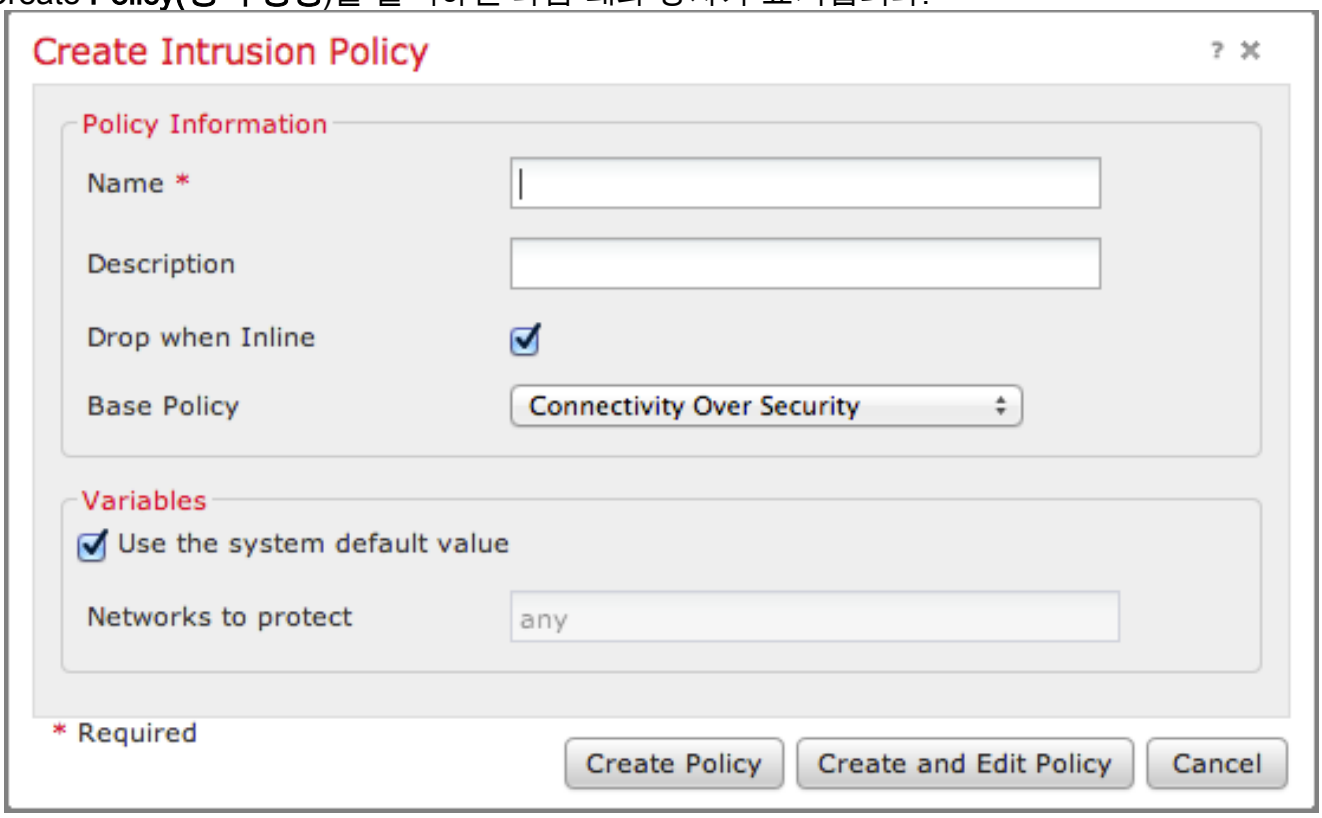
1. 다음 페이지 Devices **> Device Management로 이동합니다**.
2. 선택한 센서의 **편집**(연필) 아이콘을 클릭합니다.
3. Interfaces(**인터페이스**) 탭에서 선택한 인터페이스의 Edit(수정) 아이콘을 클릭합니다.



Passive 또는 Inline 인터페이스 컨피그레이션을 선택합니다.스위치드 및 라우티드 인터페이스는 이 문서의 범위를 벗어납니다.

8단계:침입 정책 구성

- 다음 페이지로 이동합니다. Policies(정책) **> Intrusion(침입) > Intrusion Policy(침입 정책)**
- Create **Policy(정책 생성)**를 클릭하면 다음 대화 상자가 표시됩니다.



이름을 지정하고 사용할 기본 정책을 정의해야 합니다.구축에 따라 Drop when Inline enabled(인라인 활성화 시 삭제) 옵션**을** 선택할 수 있습니다.오탐을 줄이고 시스템 성능을 개선하기 위해 보호할 네트워크를 정의합니다.

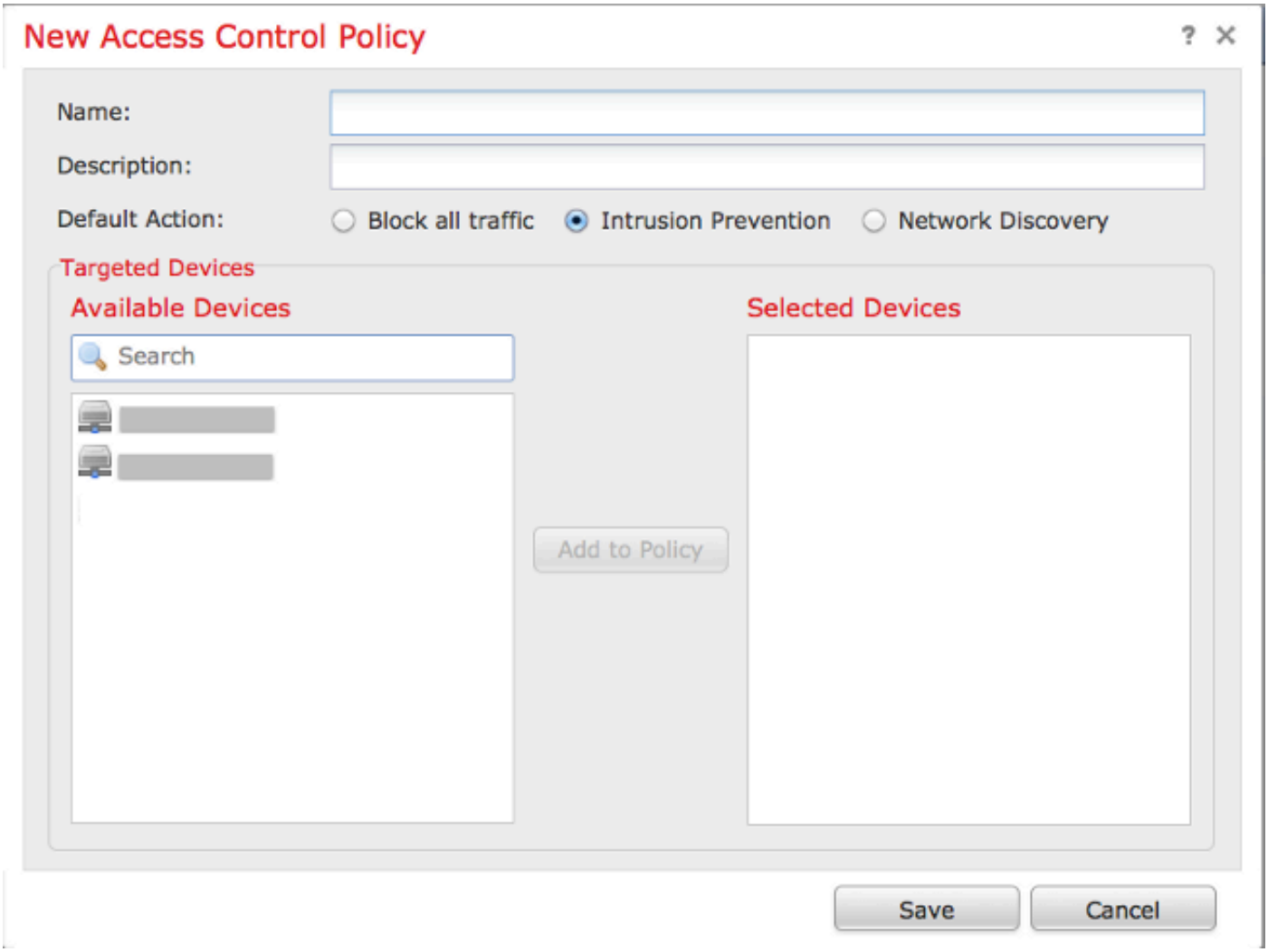
Create Policy(정책 생성)를 클릭하면 설정이 저장되고 IPS 정책이 생성됩니다. 침입 정책을 수정하려는 경우 대신 Create and Edit Policy(정책 **생성 및 수정)를** 선택할 수 있습니다.

참고:침입 정책은 액세스 제어 정책의 일부로 적용됩니다. 침입 정책을 적용한 후에는 Reapply(다시 적용) 버튼을 클릭하여 전체 액세스 제어 정책을 다시 적용하지 않고도 수정 사항을 적용할 수 **있습니다**.

9단계:액세스 제어 정책 구성 및 적용

1. **정책 > 액세스 제어로 이동합니다**.

2. **새 정책**을 클릭합니다.

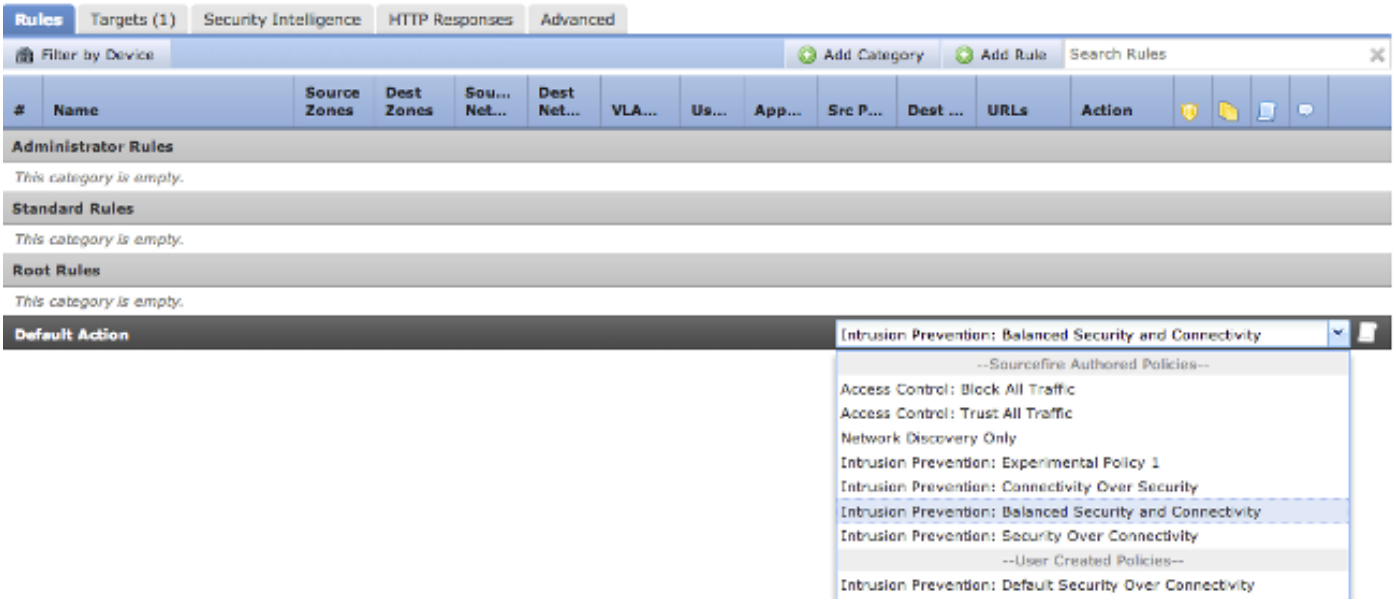


3. 정책 **이름**과 **설명**을 입력합니다.

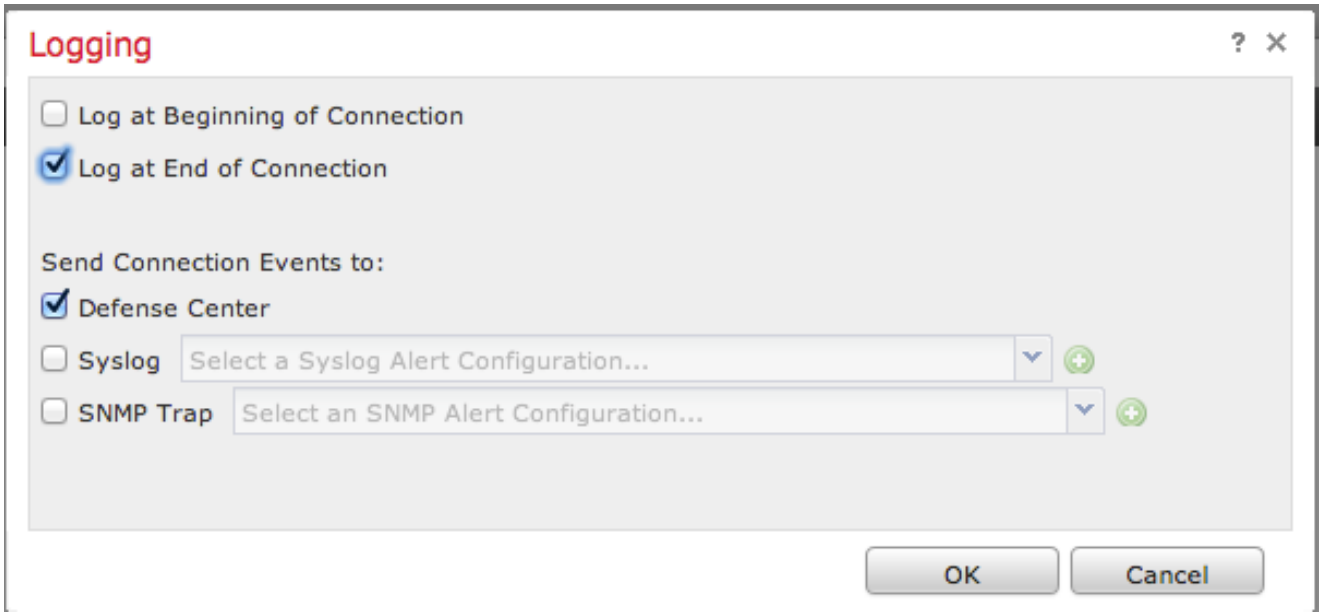
4. Access **Control** 정책의 **Default Action**으로 Intrusion Prevention을 선택합니다.

5. 마지막으로 액세스 제어 정책을 적용할 대상 **장치**를 선택하고 **저장**을 클릭합니다.

6. 기본 작업에 대한 침입 정책을 선택합니다.



7. 연결 이벤트를 생성하려면 연결 로깅을 활성화해야 합니다.기본 작업 오른쪽에 있는 드롭다운 메뉴를 **클릭합니다**.



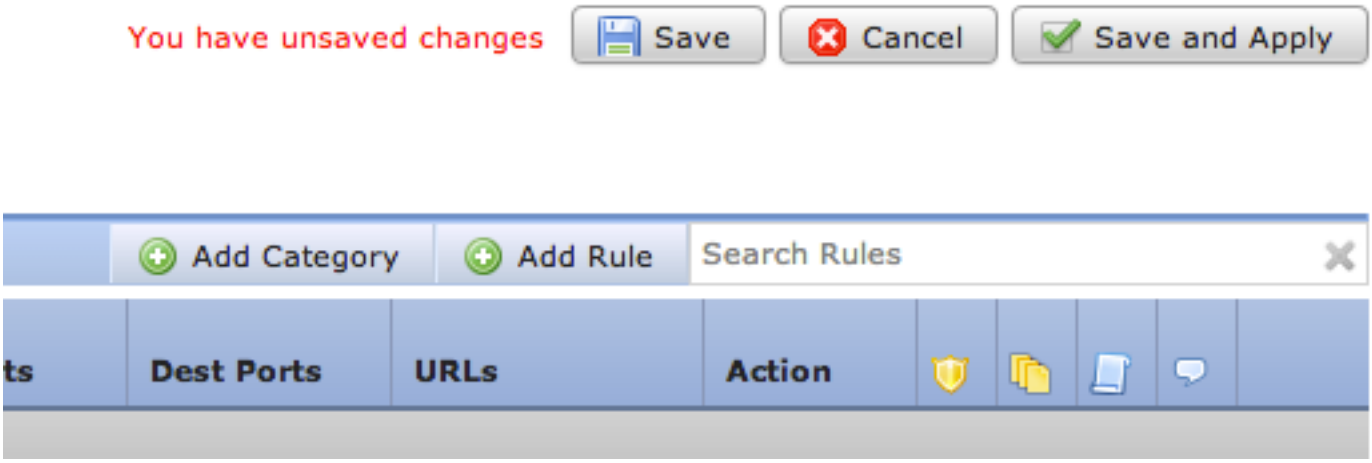
8. 연결의 시작 또는 끝에 연결을 로깅하도록 선택합니다.이벤트는 FireSIGHT Management Center, syslog 위치 또는 SNMP를 통해 로깅할 수 있습니다.

> **참고:**모든 연결(차단된 연결 제외)이 두 번 로깅되므로 연결의 양쪽 끝에서 로깅하지 않는 것이 좋습니다.시작 시 로깅은 차단될 연결에 유용하며, 끝 부분에 로깅하는 것은 다른 모든 연결에 유용합니다.

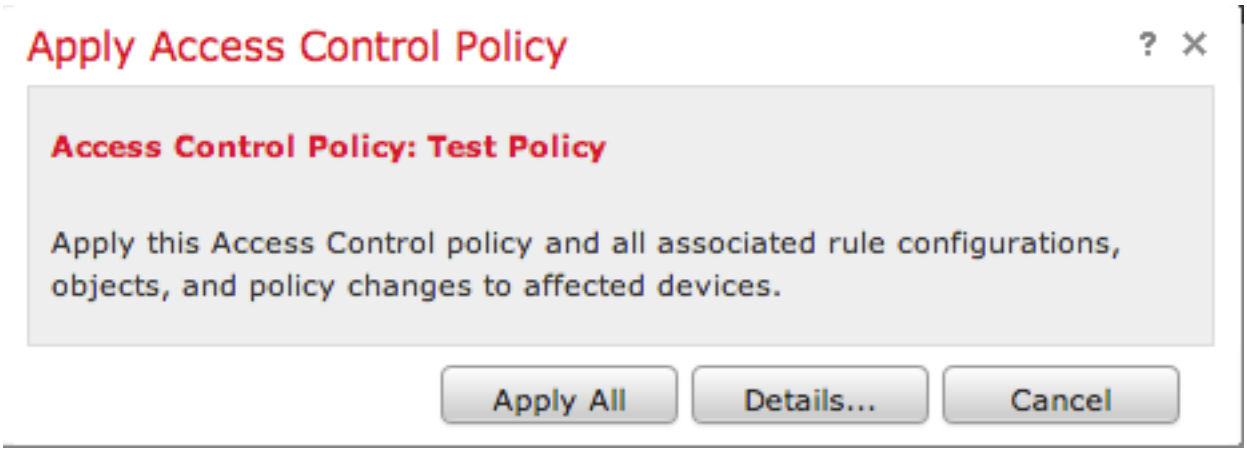
9. **확인**을 클릭합니다.로깅 아이콘의 색상이 변경되었습니다.

10. 현재 **액세스 제어 규칙**을 추가할 수 있습니다.사용할 수 있는 옵션은 설치한 라이센스 유형에 따라 달라집니다.

11. 변경이 완료되면Save **and Apply** 버튼**을** 클릭합니다. 오른쪽 상단에서 버튼을 클릭할 때까지 정책에 저장되지 않은 변경 사항이 있음을 알리는 메시지가 표시됩니다.



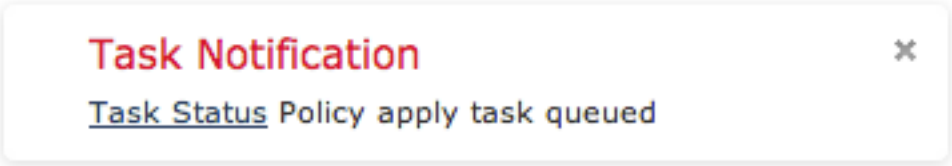
변경 내용만 **저장하도록** 선택하거나 **저장** 및 적용**을** 클릭할 수 있습니다. 후자를 선택할 경우 다음 창이 나타납니다.



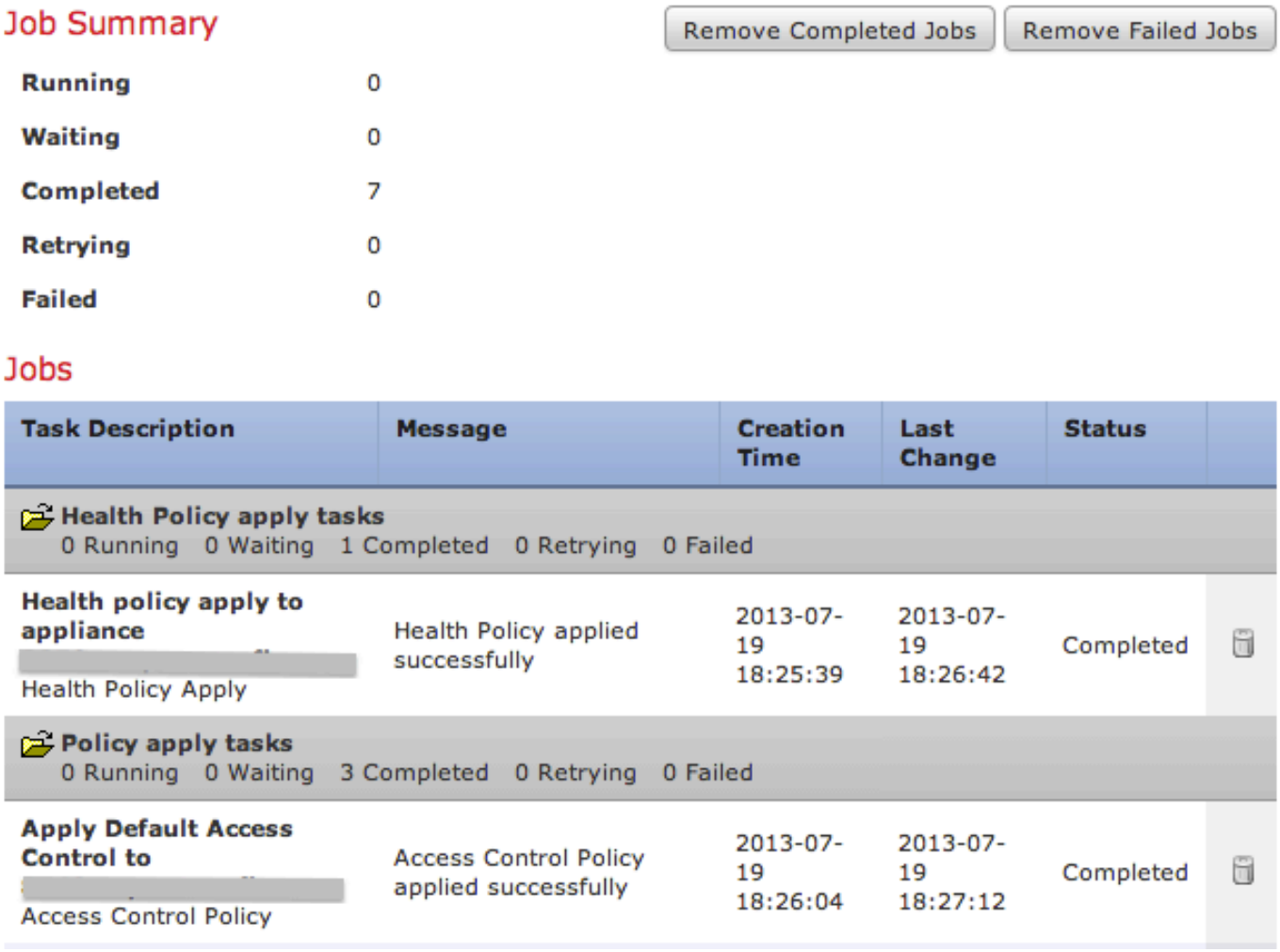
12. **Apply All(모두 적용)**은 액세스 제어 정책 및 관련 침입 정책을 대상 디바이스에 적용합니다.

참고:침입 정책이 처음으로 적용되는 경우 선택 취소할 수 없습니다.

13. 페이지 상단에 표시된 통지에서 **Task Status** 링크를 클릭하거나 다음으로 이동하여 태스크 상태를 모니터링할 수 있습니다.**시스템 > 모니터링 > 작업 상태**



14. Task Status(작업 상태) 링크를 클릭하여 Access Control(액세스 제어) 정책 적용의 진행 상황을 모니터링합니다.



10단계:FireSIGHT Management Center에서 이벤트를 수신하는지 확인

Access Control 정책 적용이 완료되면 연결 이벤트 및 트래픽 침입 이벤트에 따라 보기를 시작해야 합니다.

추가 권장 사항

시스템에서 다음 추가 기능을 구성할 수도 있습니다.구현 정보는 사용 설명서를 참조하십시오.

- 예약된 백업
- 자동 소프트웨어 업데이트, SRU, VDB 및 GeoLocation 다운로드/설치
- LDAP 또는 RADIUS를 통한 외부 인증