

# ISE를 사용하여 Firepower 6.1 pxGrid 교정 구성

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[firepower 구성](#)

[ISE 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

---

## 소개

이 문서에서는 ISE(Identity Services Engine)를 사용하여 Firepower 6.1 pxGrid 교정을 구성하는 방법에 대해 설명합니다. Firepower 6.1+ ISE 교정 모듈을 ISE EPS(Endpoint Protection Service)와 함께 사용하여 네트워크 액세스 레이어에서 공격자의 격리/블랙리스트 작성을 자동화할 수 있습니다.

## 사전 요구 사항

### 요구 사항

Cisco에서는 다음 항목에 대한 기본 지식을 갖춘 것을 권장합니다.

- Cisco ISE
- Cisco Firepower

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE 버전 2.0 패치 4
- Cisco Firepower 6.1.0
- vWLC(Virtual Wireless LAN Controller) 8.3.102.0

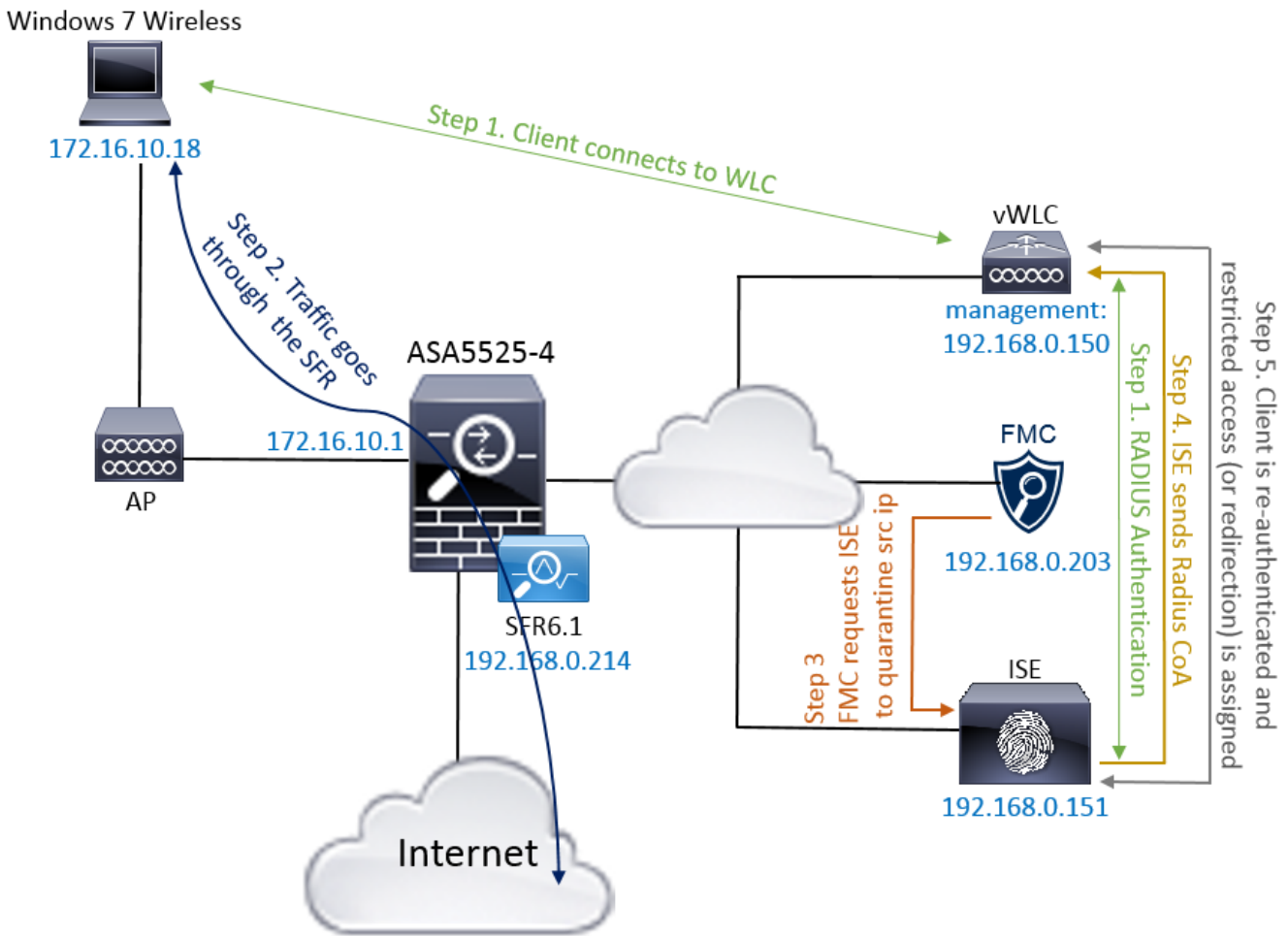
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

# 구성

이 문서에서는 ISE와 Firepower의 통합, ISE와 AD(Active Directory)의 통합, Firepower과 AD의 통합의 초기 컨피그레이션을 다루지 않습니다. 이 정보를 보려면 참조 섹션으로 이동합니다. Firepower 6.1 리미디에이션 모듈을 사용하면 상관관계 규칙이 일치할 때 Firepower 시스템에서 ISE EPS 기능(격리, 격리 해제, 포트 종료)을 리미디에이션으로 사용할 수 있습니다.

 참고: 무선 구축에는 포트 종료를 사용할 수 없습니다.


## 네트워크 다이어그램



### 플로우 설명:

1. 클라이언트는 네트워크에 연결하고 ISE를 통해 인증하며 네트워크에 무제한 액세스를 부여하는 권한 부여 프로파일과 함께 권한 부여 규칙에 도달합니다.
2. 그런 다음 클라이언트의 트래픽은 Firepower 디바이스를 통해 이동합니다.
3. 사용자가 악의적인 활동을 수행하기 시작하고 상관관계 규칙에 도달하여 FMC(Firepower 관리 센터)가 pxGrid를 통해 ISE 교정을 수행하도록 트리거합니다.
4. ISE는 엔드포인트에 EPSStatus Quarantine을 할당하고 네트워크 액세스 디바이스(WLC 또는 스위치)에 RADIUS Change of Authorization을 트리거합니다.

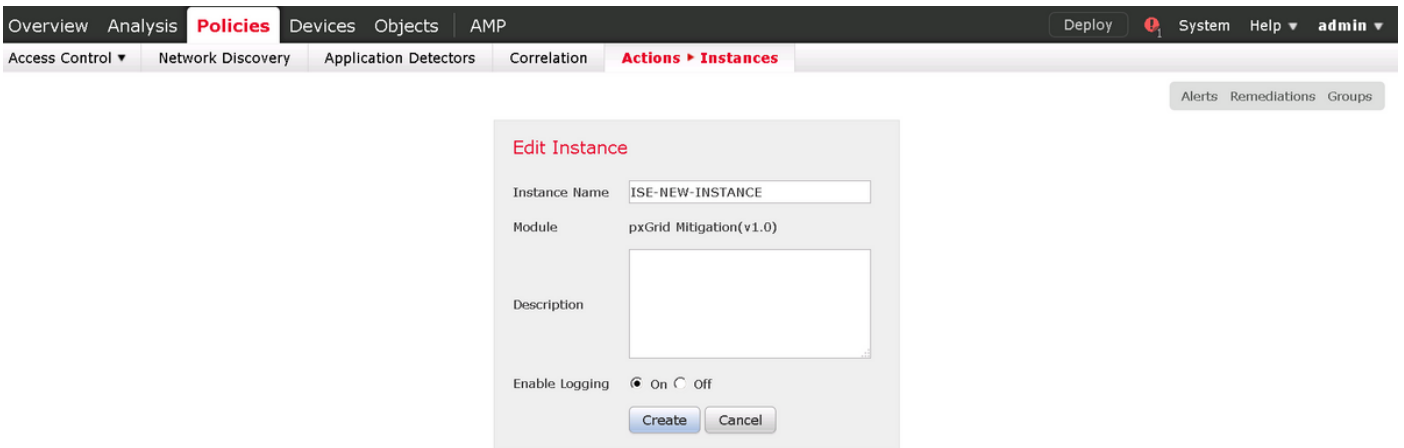
5. 클라이언트는 제한된 액세스를 할당하는 또 다른 권한 부여 정책에 도달합니다(SGT를 변경하거나 포털로 리디렉션하거나 액세스를 거부함).

 참고: 엔드포인트에 ip 주소를 매핑하는 데 사용되는 ip 주소 정보를 ISE에 제공하려면 RADIUS 어카운팅을 전송하도록 NAD(Network Access Device)를 구성해야 합니다.

## firepower 구성

1단계. pxGrid Mitigation 인스턴스를 구성합니다.

Policies(정책) > Actions(작업) > Instances(인스턴스)로 이동하고 이미지에 표시된 대로 pxGrid Mitigation Instance(pxGrid 완화 인스턴스)를 추가합니다.



Overview Analysis **Policies** Devices Objects AMP Deploy System Help admin

Access Control Network Discovery Application Detectors Correlation **Actions > Instances** Alerts Remediations Groups

**Edit Instance**

Instance Name: ISE-NEW-INSTANCE

Module: pxGrid Mitigation(v1.0)

Description:

Enable Logging:  On  Off

Create Cancel

2단계. 교정을 구성합니다.

사용 가능한 유형에는 대상 완화와 소스 완화의 두 가지가 있습니다. 이 예에서는 소스 완화가 사용 됩니다. 이미지에 표시된 대로 교정 유형을 선택하고 Add(추가)를 클릭합니다.



**Configured Remediations**

Remediation Name	Remediation Type	Description
No configured remediations available		

Add a new remediation of type: Mitigate Destination Mitigate Destination **Mitigate Source** Add

이미지에 표시된 대로 교정에 완화 조치를 할당합니다.

## Edit Remediation

Remediation Name

QUARANTINE-SOURCE

Remediation Type

Mitigate Source

Description

Mitigation Action

quarantine

Whitelist

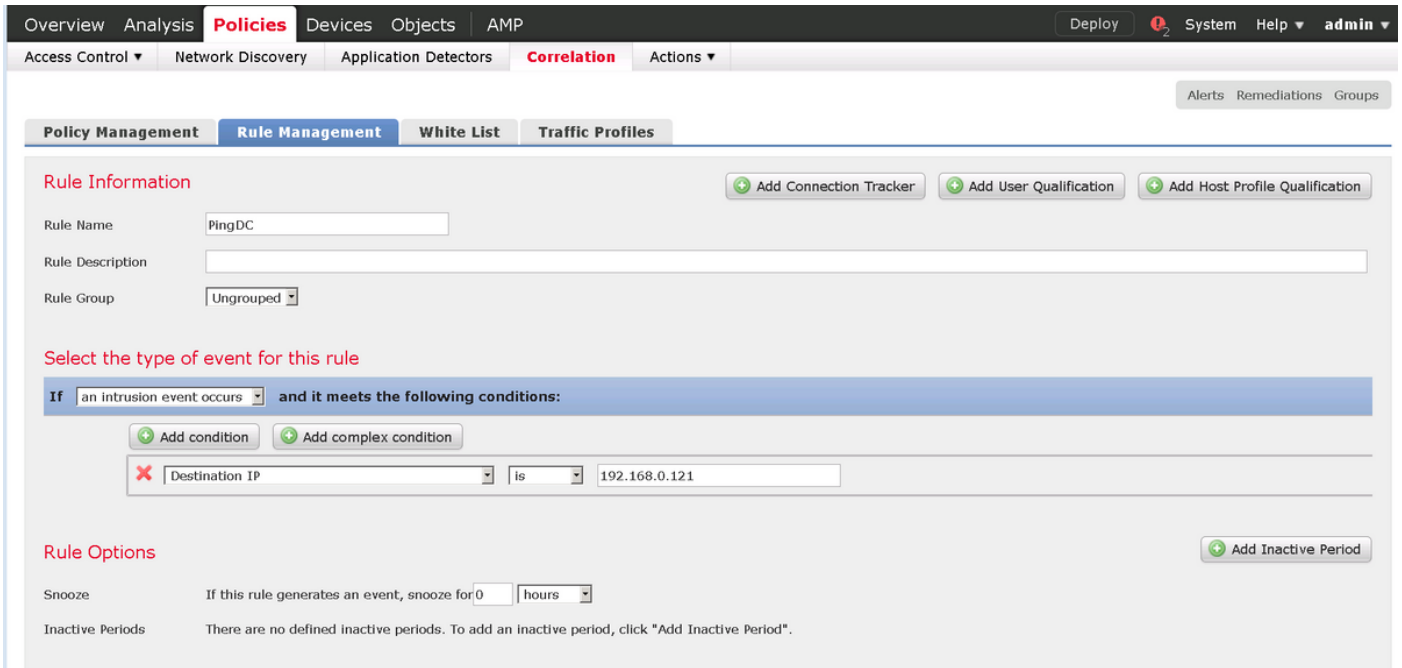
(an *optionallist* of networks )

Create

Cancel

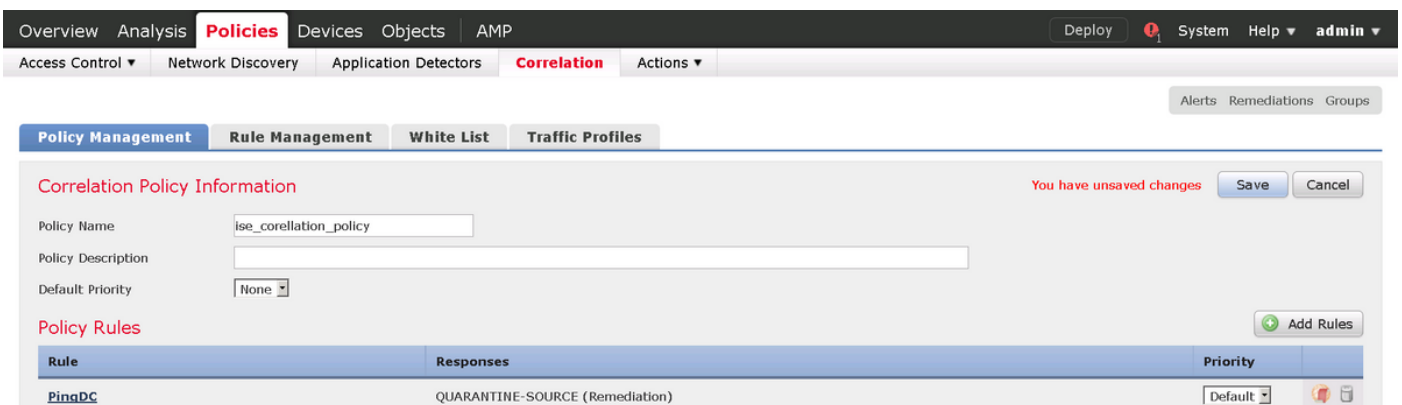
3단계. 상관관계 규칙을 구성합니다.

Policies(정책) > Correlation(상관관계) > Rule Management(규칙 관리)로 이동하고 Create Rule Correlation rule(규칙 상관관계 규칙 생성)을 클릭하면 교정이 실행됩니다. 상관관계 규칙에는 여러 조건이 포함될 수 있습니다. 이 예에서 침입 이벤트가 발생하고 목적지 ip 주소가 192.168.0.121인 경우 상관관계 규칙 PingDC가 적용됩니다. ICMP 에코 응답과 일치하는 사용자 지정 침입 규칙은 이미지에 표시된 대로 테스트용으로 구성됩니다.

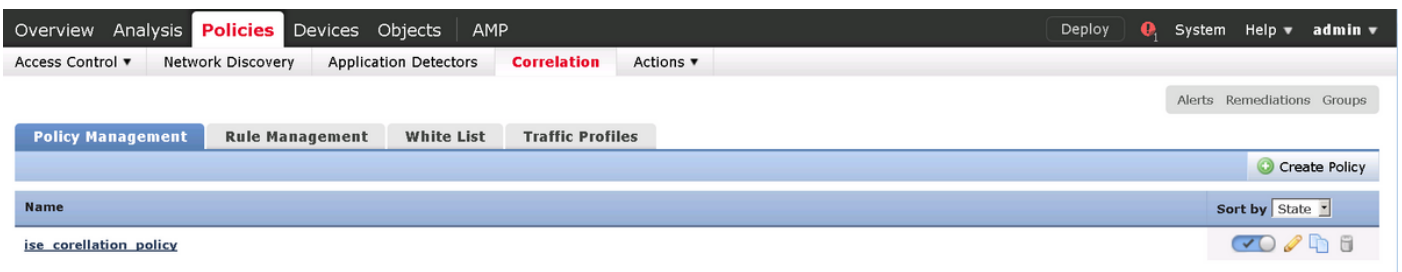


4단계. 상관관계 정책을 구성합니다.

Policies(정책) > Correlation(상관관계) > Policy Management(정책 관리)로 이동하고 Create Policy(정책 생성)를 클릭하고, 정책에 규칙을 추가하고, 이미지에 표시된 대로 응답을 할당합니다.



이미지에 표시된 대로 상관관계 정책을 활성화합니다.



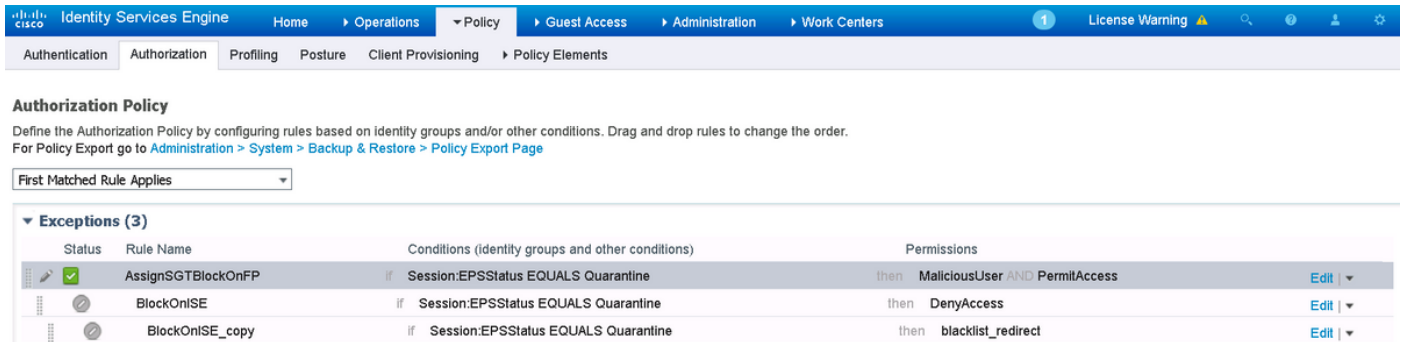
## ISE 구성

1단계. 권한 부여 정책을 구성합니다.

Policy(정책) > Authorization(권한 부여)으로 이동하여 새 권한 부여 정책을 추가합니다. 그러면 교정이 수행된 후에 이 정책이 적용됩니다. 조건으로 세션: EPSStatus EQUALS Quarantine을 사용합

니다. 다음과 같은 몇 가지 옵션을 사용할 수 있습니다.

- 액세스 허용 및 다른 SGT 할당(네트워크 디바이스에 대한 액세스 제어 제한 적용)
- Deny Access(액세스 거부)(사용자가 네트워크에서 쫓겨나 다시 연결할 수 없어야 함)
- 블랙리스트 포털로 리디렉션(이 시나리오에서는 맞춤형 핫스팟 포털이 이 용도로 구성됨)

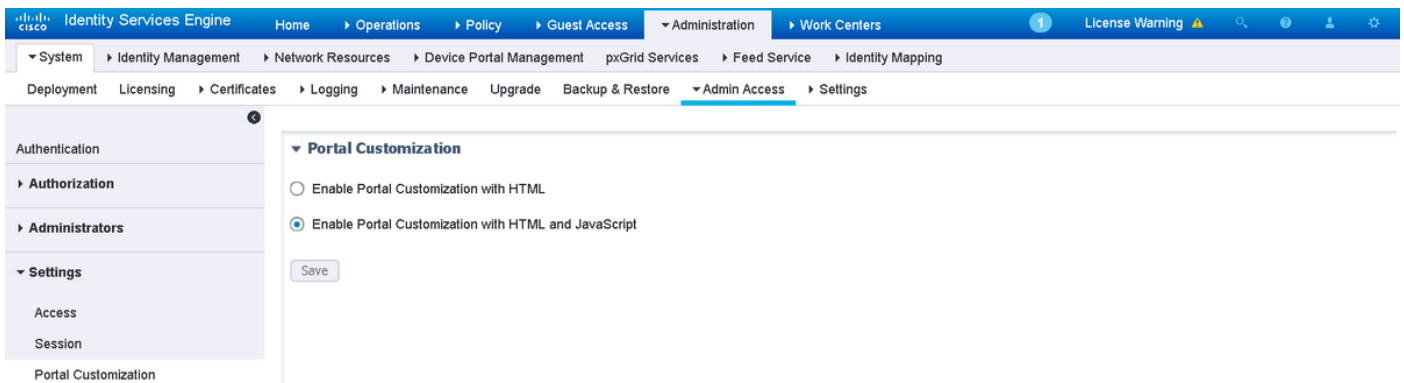


### 맞춤형 포털 컨피그레이션

이 예에서는 핫스팟 포털이 블랙리스트로 구성됩니다. 사용자 지정 텍스트가 있는 AUP(Acceptable Use Policy) 페이지만 있으며 AUP를 수락할 가능성은 없습니다(JavaScript로 수행). 이를 위해서는 먼저 JavaScript를 활성화한 다음 포털 사용자 지정 컨피그레이션에서 AUP 버튼 및 컨트롤을 숨기는 코드를 붙여넣어야 합니다.

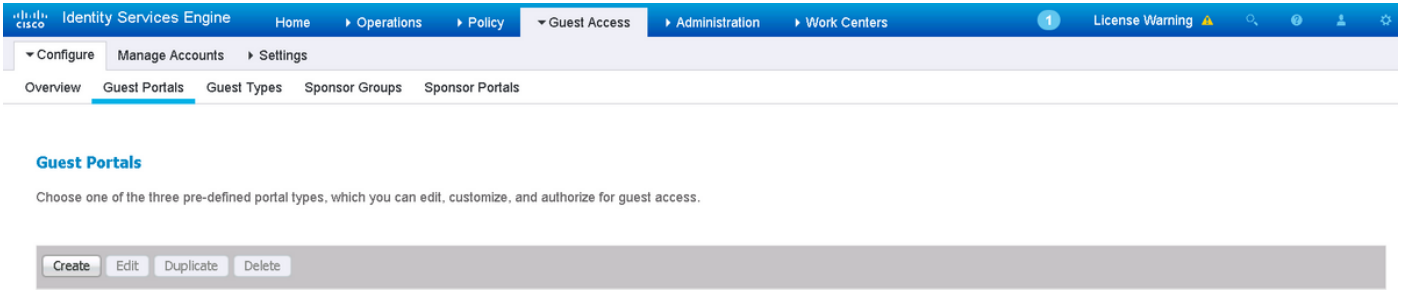
1단계. JavaScript를 활성화합니다.

Administration(관리) > System(시스템) > Admin Access(관리 액세스) > Settings(설정) > Portal Customization(포털 사용자 지정)으로 이동합니다. Enable Portal Customization with HTML and JavaScript(HTML 및 JavaScript로 포털 사용자 지정 활성화)를 선택하고 Save(저장)를 클릭합니다.



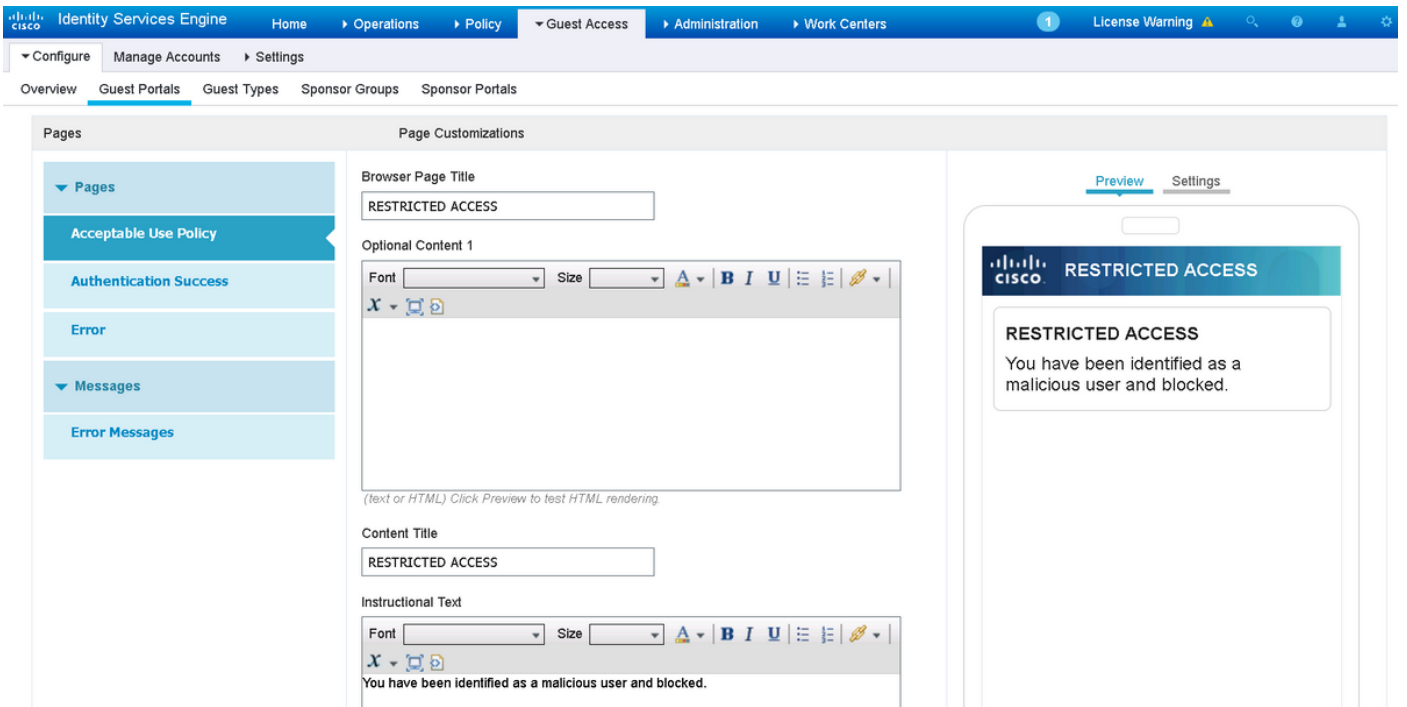
2단계. 핫스팟 포털을 생성합니다.

Guest Access(게스트 액세스) > Configure(구성) > Guest Portals(게스트 포털)로 이동하고 Create(생성)를 클릭한 다음 Hotspot type(핫스팟 유형)을 선택합니다.



3단계. 포털 사용자 지정을 구성합니다.

Portal Page Customization(포털 페이지 사용자 맞춤화)으로 이동하여 제목 및 콘텐츠를 변경하여 사용자에게 적절한 경고를 제공합니다.



옵션 내용 2로 스크롤하고 HTML 소스 토글을 클릭한 다음 스크립트 내부를 붙여넣습니다.

Untoggle HTML Source(HTML 소스 전환 취소)를 클릭합니다.

## Optional Content 2

```
Font [ ] Size [ ] A | B I U | [ ] [ ] [ ]
X - [ ] [ ]
<script>
(function(){
  jQuery('.cisco-ise-aup-text').hide();
  jQuery('.cisco-ise-aup-controls').hide();
  setTimeout(function(){ jQuery('#portal-session-timeout-popup-screen, #portal-session-
timeout-popup-popup, #portal-session-timeout-popup').remove(); }, 100);
})();
</script>
<br _moz_editor_bogus_node="TRUE" />
```

(text or HTML) Click Preview to test HTML rendering.

## 다음을 확인합니다.

컨피그레이션이 제대로 작동하는지 확인하려면 이 섹션에 제공된 정보를 사용합니다.

### Firepower

교정이 일어나도록 하는 트리거는 상관관계 정책/규칙의 적중입니다. Analysis(분석) > Correlation(상관관계) > Correlation Events(상관관계 이벤트)로 이동하여 상관관계 이벤트가 발생했는지 확인합니다.



### ISE

그런 다음 ISE가 Radius: CoA를 트리거하고 사용자를 다시 인증해야 합니다. 이러한 이벤트는 Operation(작업) > RADIUS Livelog(RADIUS 라이브 로그)에서 확인할 수 있습니다.

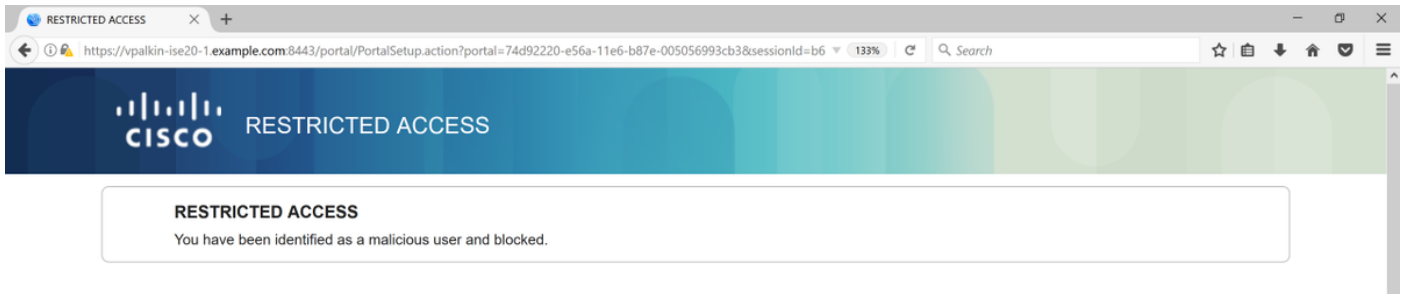
Time	Impact	Inline Result	Source IP	Source Country	Destination IP	Destination Country	Security Intelligence Category	Source User	Destination User	Source Port / ICMP Type	Destination Port / ICMP Code
2017-02-16 13:26:22.894	Success	Success	alice		E4:B3:18:69:EB:8C		Windows10-Workst...	Default >> Dot1X >> D..	Default >> AssignSGT...	MaliciousUser,PermitAcc...	vWLC
2017-02-16 13:26:21.040	Success	Success			E4:B3:18:69:EB:8C						vWLC
2017-02-16 13:25:29.036	Success	Success	alice		E4:B3:18:69:EB:8C		Windows10-Workst...	Default >> Dot1X >> D..	Default >> Standard R...	PermitAccess,Administra...	vWLC

이 예에서 ISE는 엔드포인트에 다른 SGT MaliciousUser를 할당했습니다. Deny Access 권한 부여



프로파일의 경우 사용자가 무선 연결이 끊어져 다시 연결할 수 없습니다.

블랙리스트 포털을 사용한 교정. 리미디어이션 권한 부여 규칙이 포털로 리디렉션되도록 구성된 경우 공격자의 관점에서 다음과 같이 표시되어야 합니다.



## 문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

이 이미지에 표시된 대로 Analysis > Correlation > Status로 이동합니다.



결과 메시지는 교정의 성공 완료 또는 특정 오류 메시지를 반환해야 합니다. syslog 확인: System > Monitoring > Syslog 및 filter output with pxgrid입니다. 동일한 로그를 /var/log/messages에서 확인할 수 있습니다.

## 관련 정보

- <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200319-Troubleshoot-ISE-and-FirePOWER-Integrati.html>
- <https://communities.cisco.com/docs/DOC-68284>
- <https://communities.cisco.com/docs/DOC-68285>
- <https://communities.cisco.com/thread/64870?start=0&tstart=0>
- [http://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin\\_guide/b\\_ise\\_admin\\_guide\\_20.html](http://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20.html)
- <http://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61.html>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.