WSA와 CTR 통합

목차

소개

이 문서에서는 WSA(Web Security Appliance)를 CTR(Cisco Threat Response) 포털과 통합하는 단계에 대해 설명합니다.

기고자: Shikha Grover, Yeraldin Sanchez Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- WSA 액세스
- CTR 포털 액세스
- Cisco 보안 계정

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 비동기 운영 체제 버전 12.x 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

> **주의:**아시아 태평양, 일본 및 중국 URL(https://visibility.apjc.amp.cisco.com/)을 사용하여 CTR에 액세스하는 경우 어플라이언스와의 통합이 현재 지원되지 않습니다.

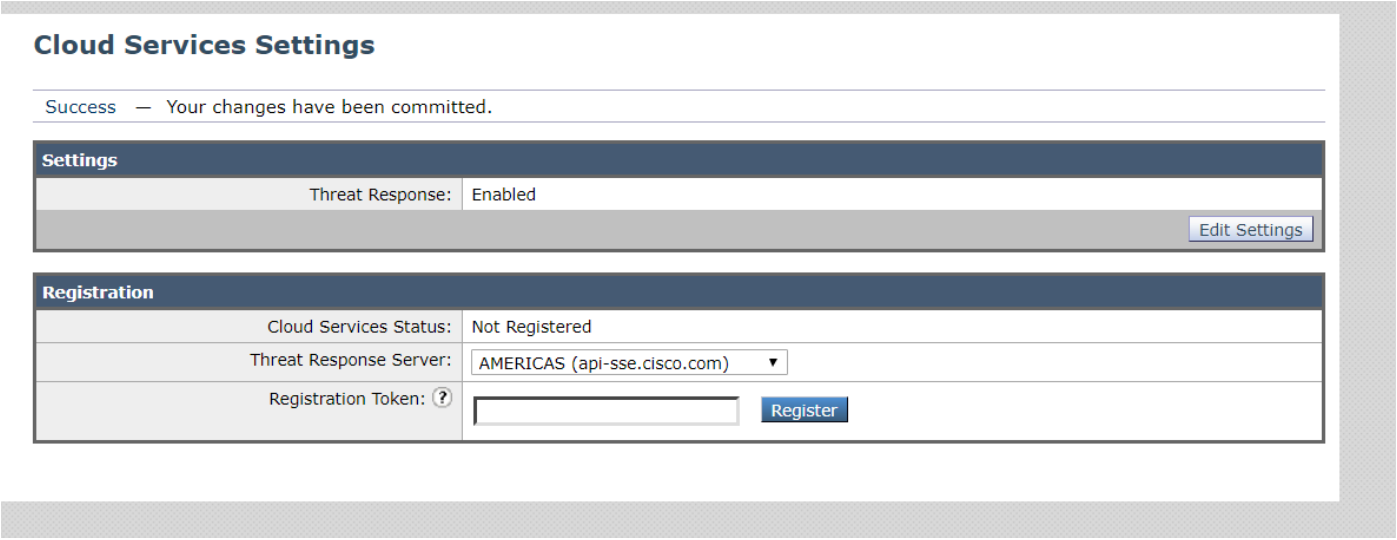
1단계. CLI의 REPORTINGCONFIG 아래에서 TROBSERVABLE을 활성화하고 이미지에 표시된 대

로 변경 사항을 커밋합니다.

```
WSA-12-0-1-173.COM> reportingconfig


hoose the operation you want to perform:
 COUNTERS - Limit counters recorded by the reporting system.
 WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
 AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings
alculation.
 WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
 CTROBSERVABLE - Enable or Disable CTR observable based indexing.
 CENTRALIZED - Enable/Disable Centralized Reporting for this WSA appliance.
]> ctrobservable

TR observable indexing currently Enabled.
re you sure you want to change the setting? [N]> y


hoose the operation you want to perform:
 COUNTERS - Limit counters recorded by the reporting system.
 WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
 AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
 WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
 CTROBSERVABLE - Enable or Disable CTR observable based indexing.
 CENTRALIZED - Enable/Disable Centralized Reporting for this WSA appliance.
```

2단계. SSE(Security Service Exchange) 클라우드 포털을 구성하고 **Network(네트워크) > Cloud Services Settings(클라우드 서비스 설정) > Edit settings(설정 수정)로** 이동하고 이미지에 표시된 대로 **Enable** and **Submit(**활성화 및 **제출)**을 클릭합니다.

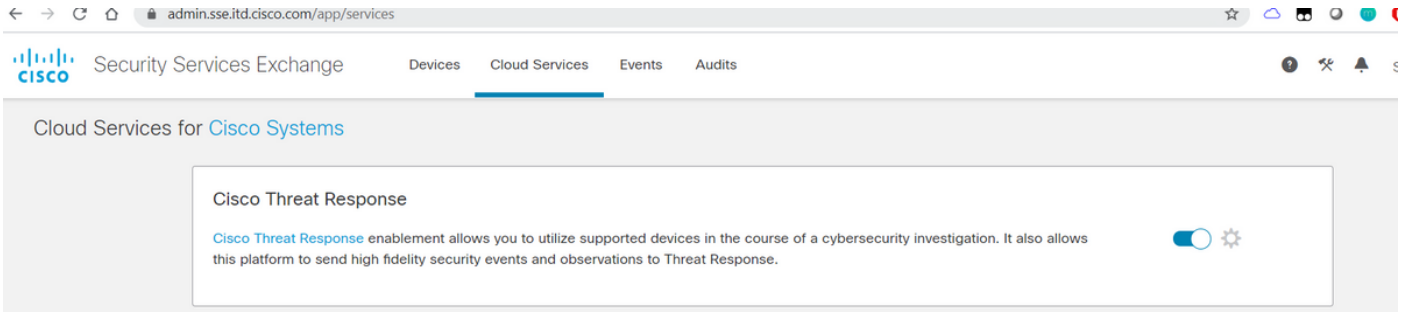
이미지에 표시된 대로 위치에 따라 클라우드를 선택합니다.



3단계. Cisco Security 계정이 없는 경우 Cisco Threat Response 포털에서 관리자 액세스 권한을 가진 사용자 계정을 생성할 수 있습니다.

새 사용자 계정을 생성하려면 Cisco Threat Response 포털 로그인 페이지로 이동합니다.

4단계. 이미지에 표시된 대로 SSE 포털의 클라우드 서비스 아래에서 Cisco Threat Response를 활성화합니다.



5단계. WSA가 포트 443에서 SSE 포털에 연결할 수 있는지 확인합니다.

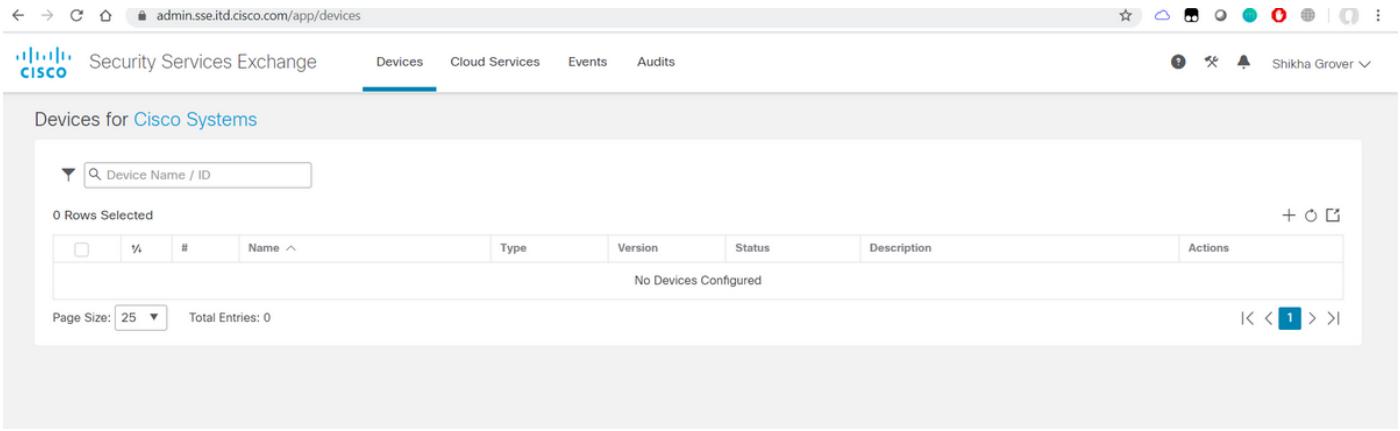
- api.eu.sse.itd.cisco.com(유럽)
- api-sse.cisco.com(미국)

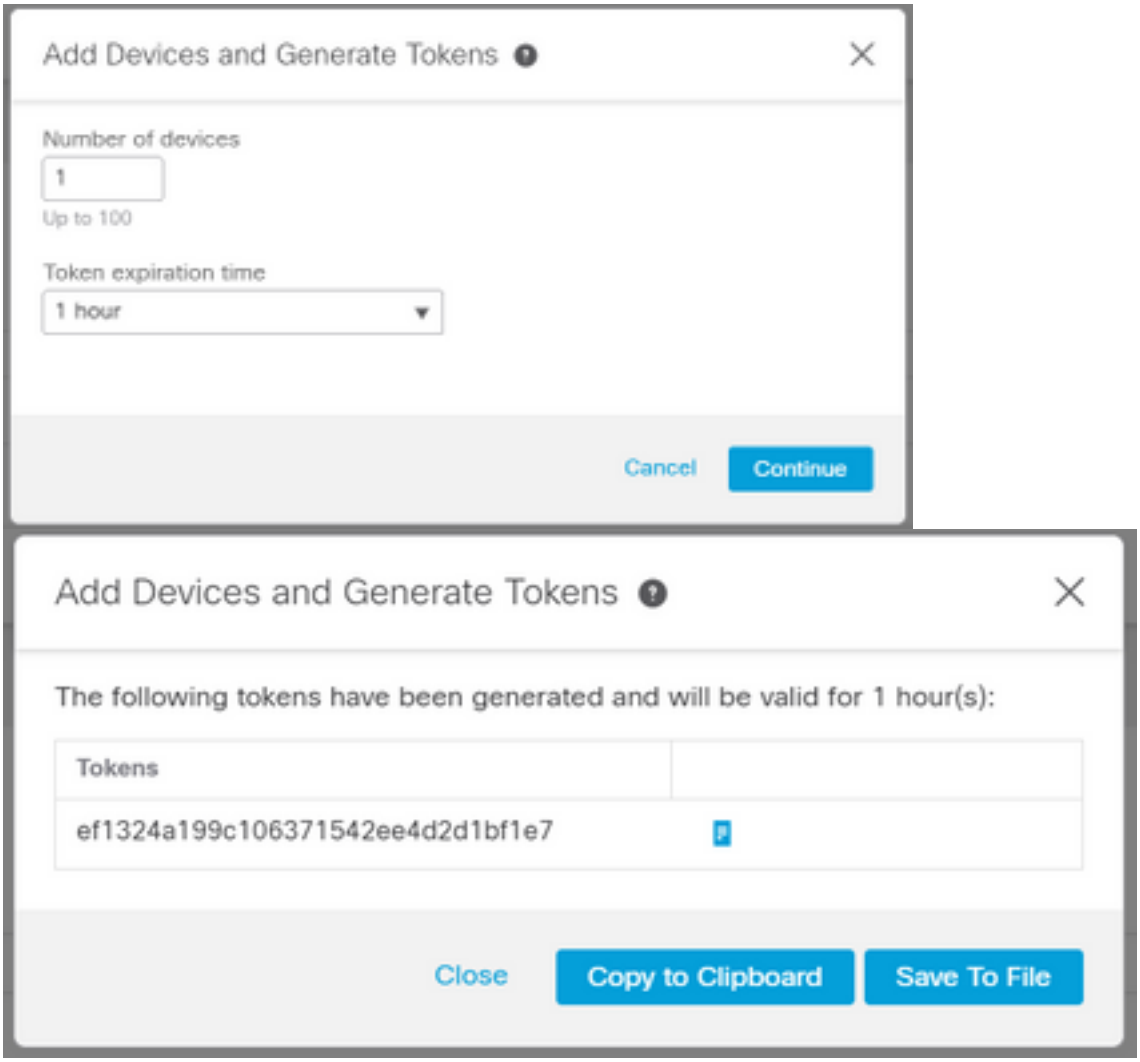
어플라이언스 등록

1단계. SSE(Security Services Exchange) 포털에서 등록 토큰을 가져와 Security Services Exchange 포털에 어플라이언스를 등록합니다.

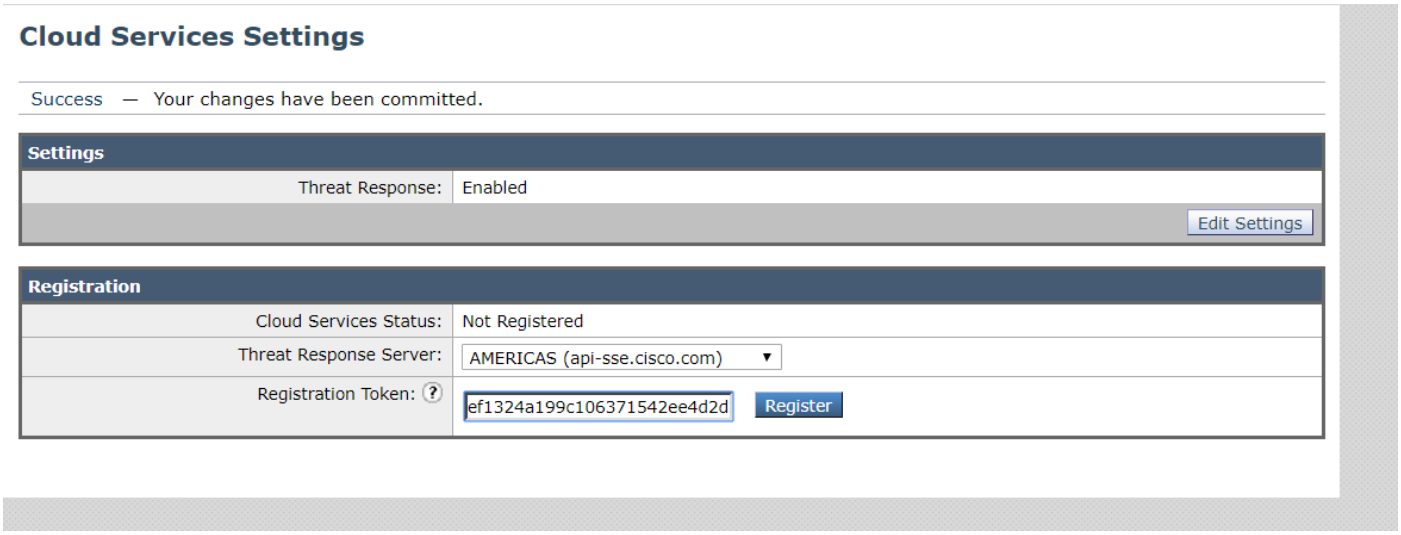
SSE 포털 링크는 https://admin.sse.itd.cisco.com/app/devices입니다.

> **참고:**CTR 계정 자격 증명을 사용하여 SSE 포털에 로그인합니다.



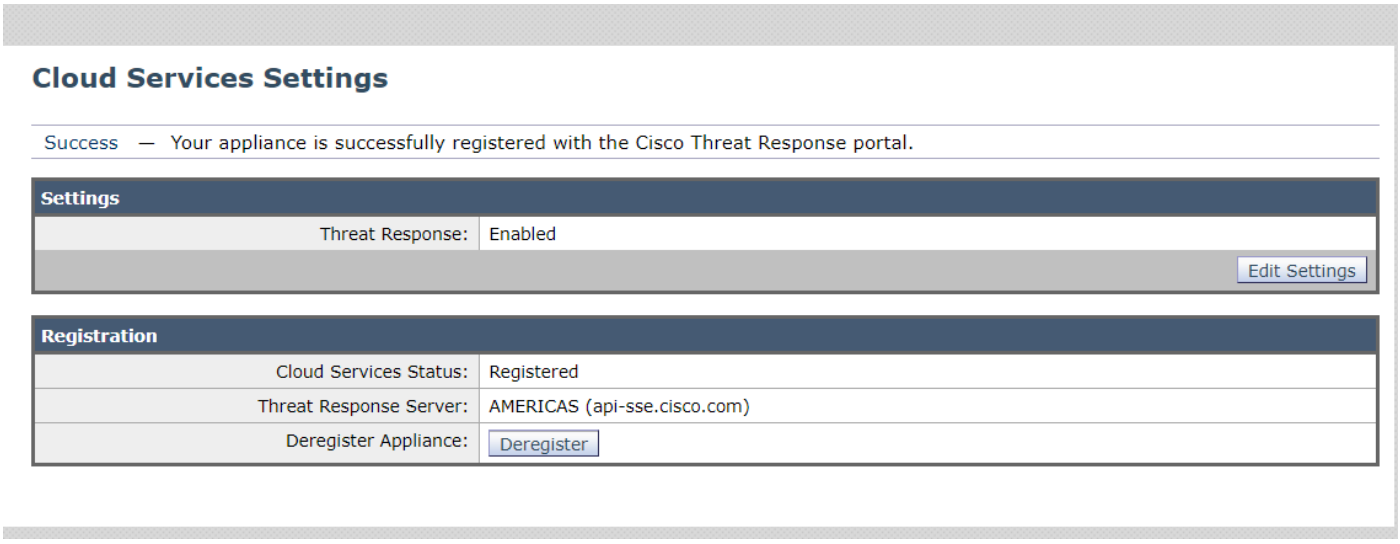


2단계. WSA의 Security Services Exchange 포털에서 가져온 등록 토큰을 입력하고 이미지에 표시된 대로 **Register**(등록)를 클릭합니다.

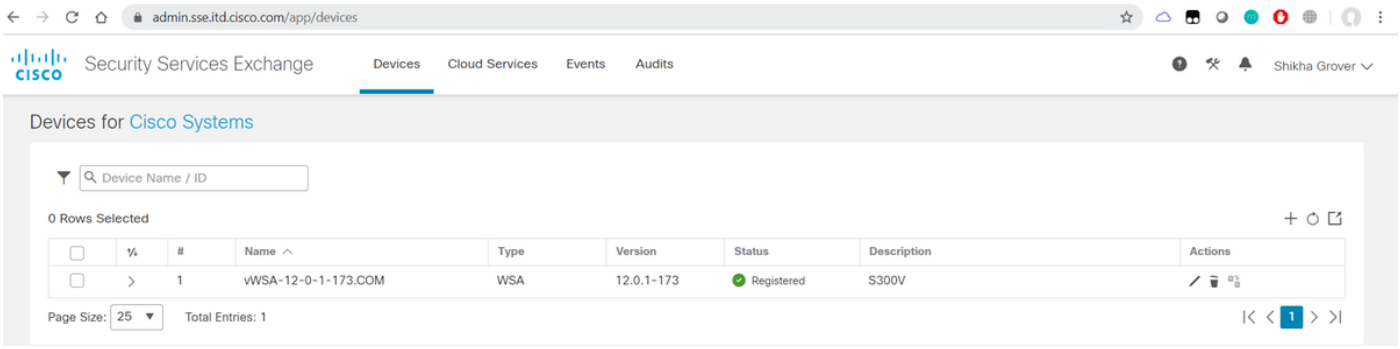


3단계. 몇 초 후에 등록이 성공적으로 완료되었음을 확인할 수 있습니다.

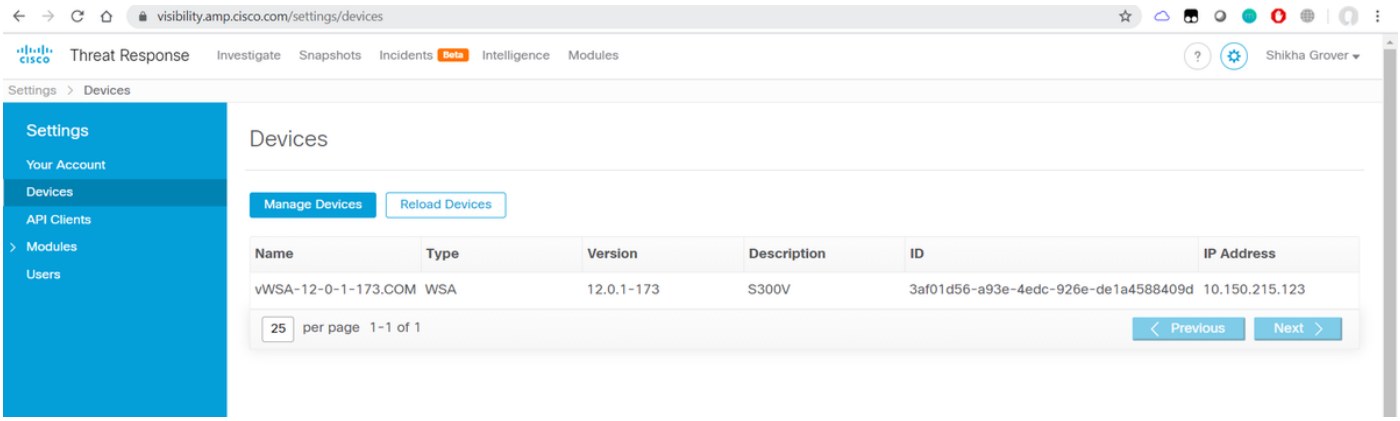
주의:생성된 토큰이 만료되기 전에 사용되는지 확인합니다.



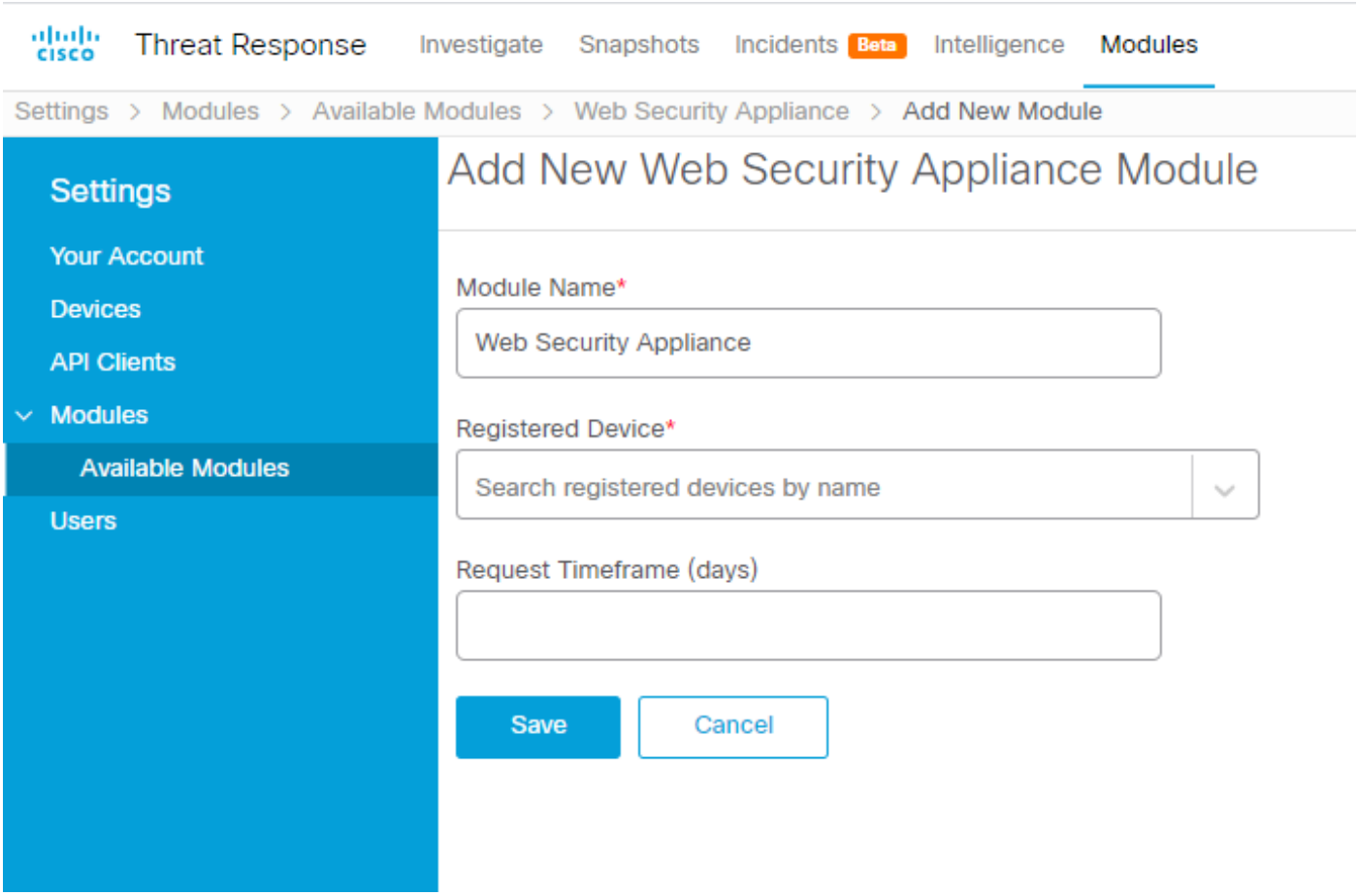
4단계.SSE 포털에서 디바이스 상태를 볼 수 있습니다.



5단계. CTR 포털에 등록된 디바이스가 나타납니다.



이 장치를 모듈에 연결하고 이미지에 표시된 대로 **Modules > Add New Module > Web Security Appliance**로 이동할 수 있습니다.



이제 디바이스가 통합되었습니다.WSA에서 트래픽을 전달하고 CTR 포털에서 위협을 조사할 수 있습니다.

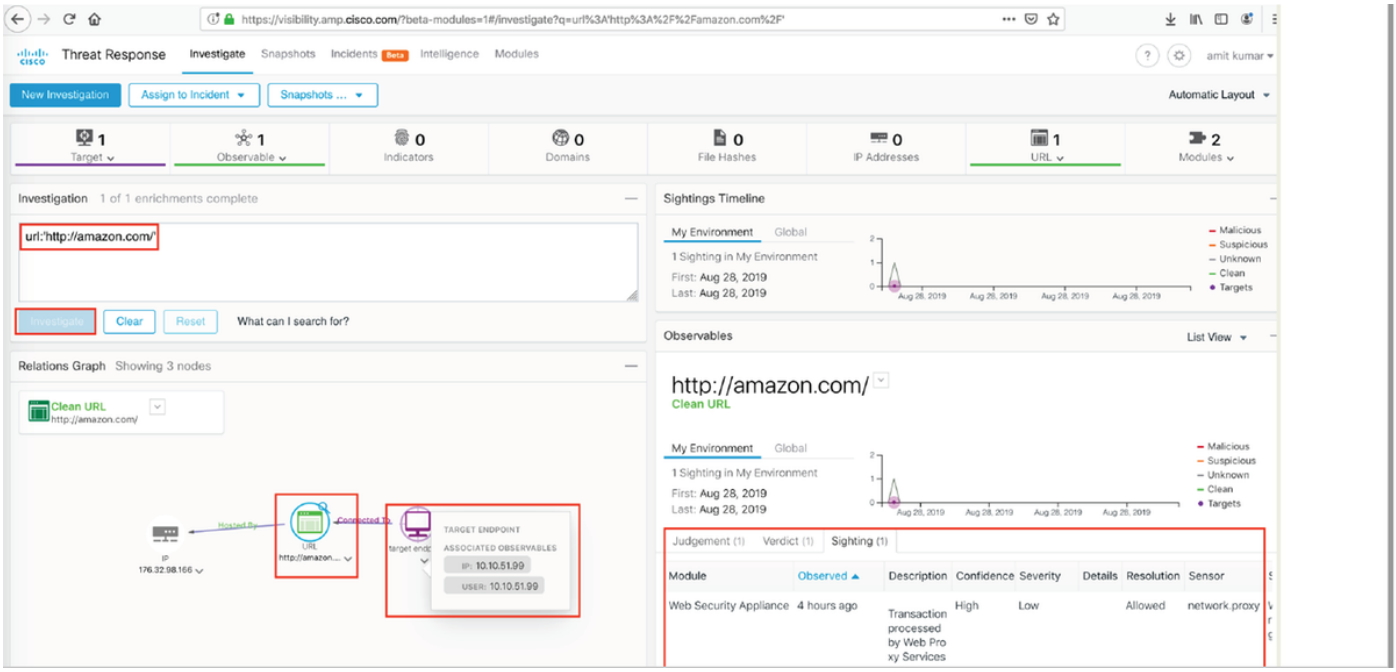
다음을 확인합니다.

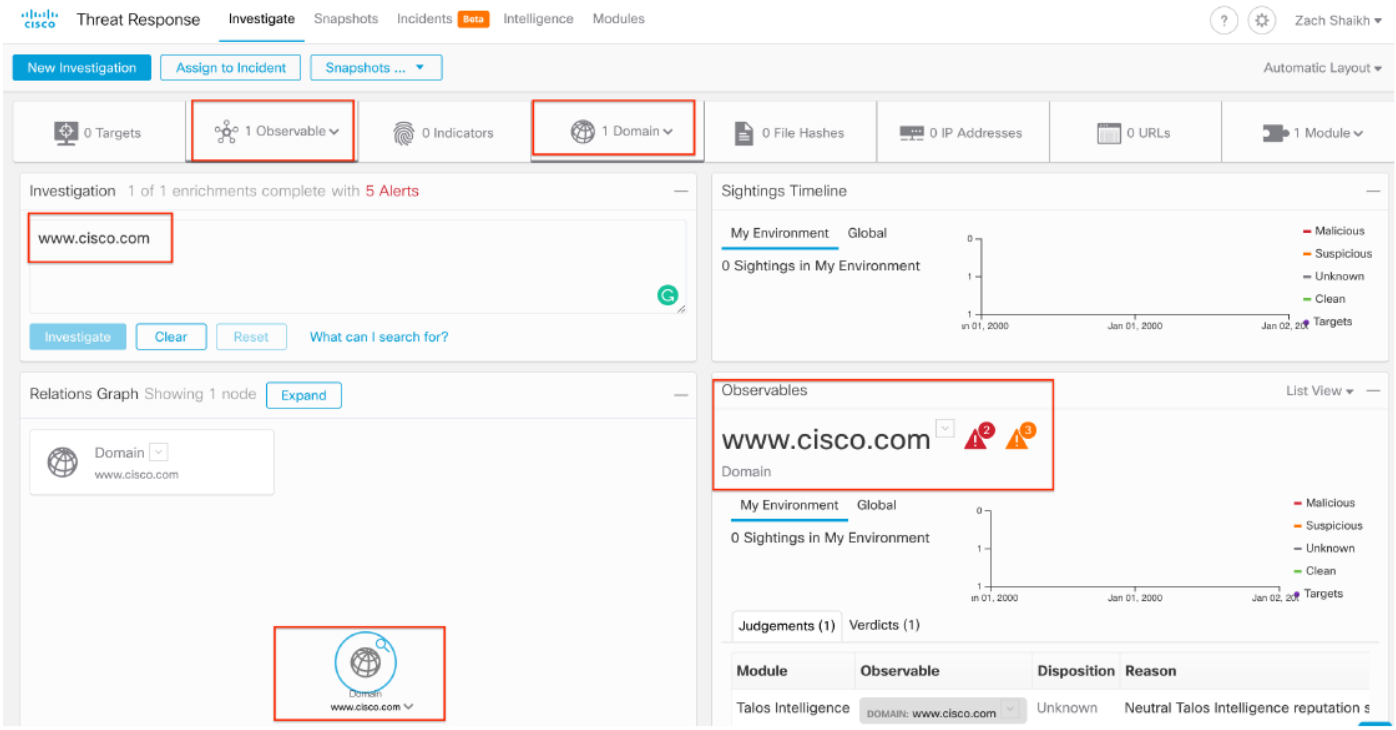
이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

CTR 포털에서 쿼리를 실행하기 위해 WSA 모듈에 사용 가능한 WSA 로그 쿼리 및 지원되는 형식:

- 도메인 - 도메인:"com"
- URL - url:"http://www.neverssl.com"
- SHA256 - sha256:"8d3aa8badf6e5a38e1b6d59a254969b1e0274f8fa120254ba1f7e02991872377999"
- IP - ip:"172.217.26.164"
- 파일 이름 - file_name:"test.txt"

그 예로,





포함해야 할 항목이 누락되었는지 언제든지 알려 주십시오. 포함해야 할 항목이 누락되었는지 언제든지 알려 주십시오. 포함해야 할 항목이 누락되었는지 언제든지 알려 주십시오. 포함해야 할 항목이 누락되었는지 언제든지 알려 주십시오.