Cisco CTR(Threat Response) 및 ESA 통합

목차

소개

이 문서에서는 Cisco CTR(Threat Response)을 ESA(Email Security Appliance)와 통합하는 프로세스와 CTR 조사를 수행하기 위해 이를 확인하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco 위협 대응
- Email Security Appliance

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CTR 계정

- Cisco Security Services Exchange
- 소프트웨어 버전 13.0.0-392의 ESA C100V

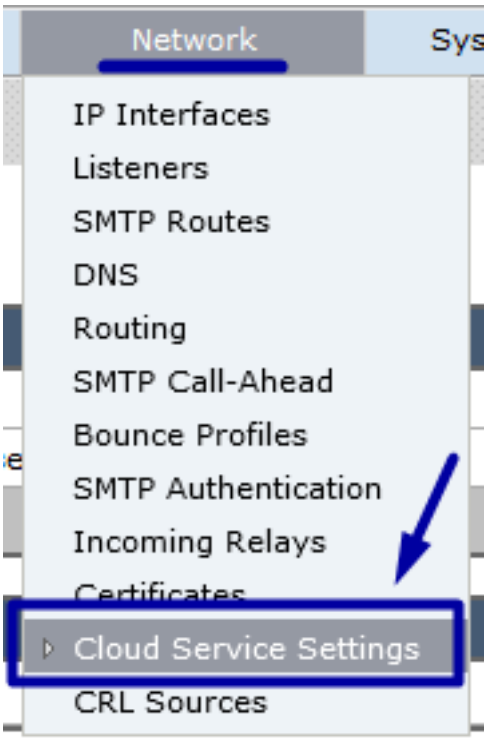
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

Integration CTR 및 ESA를 구성하려면 Email Security Virtual Appliance에 로그인하고 다음 빠른 단계를 수행하십시오.

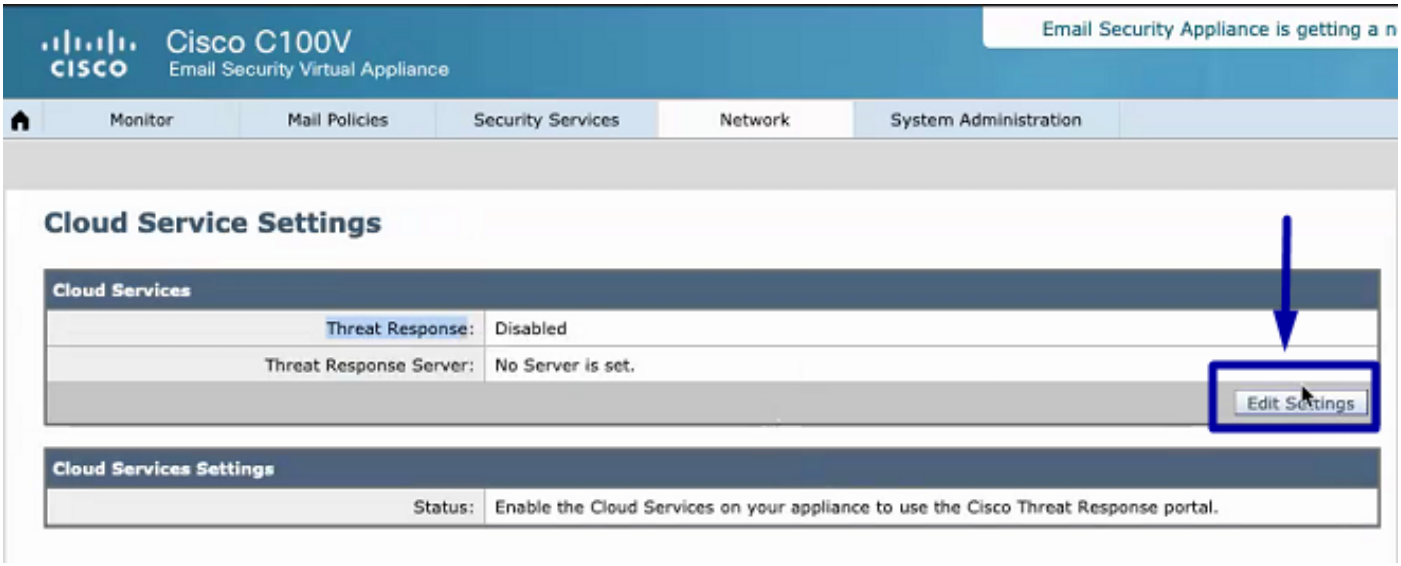
1단계. Network(네트워크) > Cloud Service Settings(클라우드 서비스 설정)로 이동합니다.

ESA에서 이미지에 표시된 대로 현재 Threat Response Status(Disabled/Enabled)를 보려면 컨텍스트 메뉴 Network(네트워크) > Cloud Service Settings(클라우드 서비스 설정)로 이동합니다.



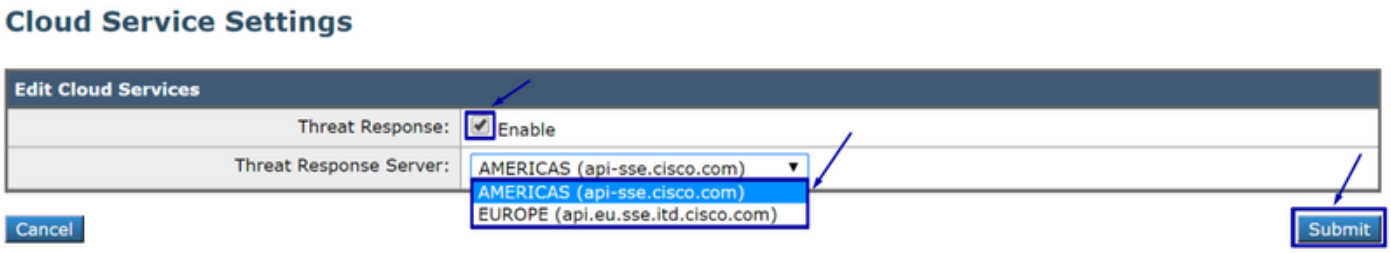
2단계. Edit Settings(설정 수정)를 클릭합니다.

지금까지 ESA의 Threat Response(위협 응답) 기능이 비활성화되었습니다. 이 기능을 활성화하려면 이미지에 표시된 대로 Edit Settings(설정 수정)를 클릭합니다.



3단계. Enable(활성화) 및 Threat Response Server(위협 응답 서버) 확인란을 선택합니다.

Enable(활성화) 확인란을 선택한 다음 Threat Response Server(위협 응답 서버)를 선택합니다. 아래 이미지를 참조하십시오.

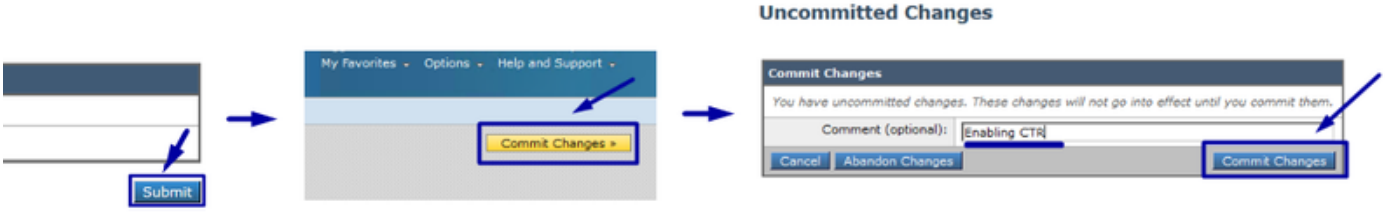


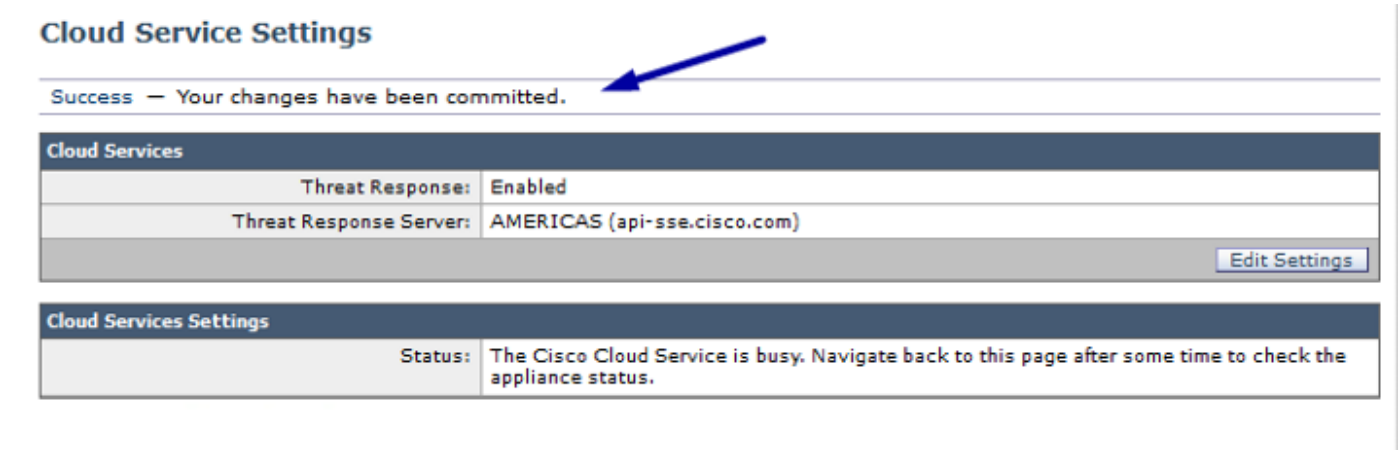
참고: Threat Response Server URL의 기본 선택은 AMERICAS(api-sse.cisco.com)입니다. EUROPE business의 경우 드롭다운 메뉴를 클릭하고 EUROPE(api.eu.sse.itd.cisco.com)을 선택합니다.

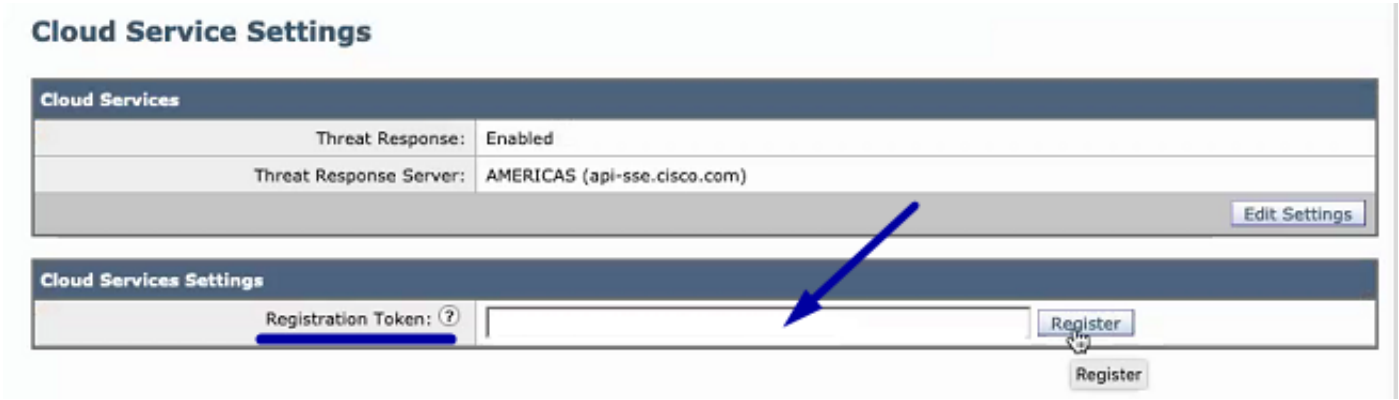
4단계. 변경 사항 제출 및 커밋

변경 사항을 저장하고 적용하려면 변경 사항을 제출하고 커밋해야 합니다.이제 ESA 인터페이스를 새로 고치면 아래 이미지와 같이 통합을 등록하기 위해 등록 토큰이 요청됩니다.

참고:성공 메시지가 표시됩니다.변경 내용이 커밋되었습니다.

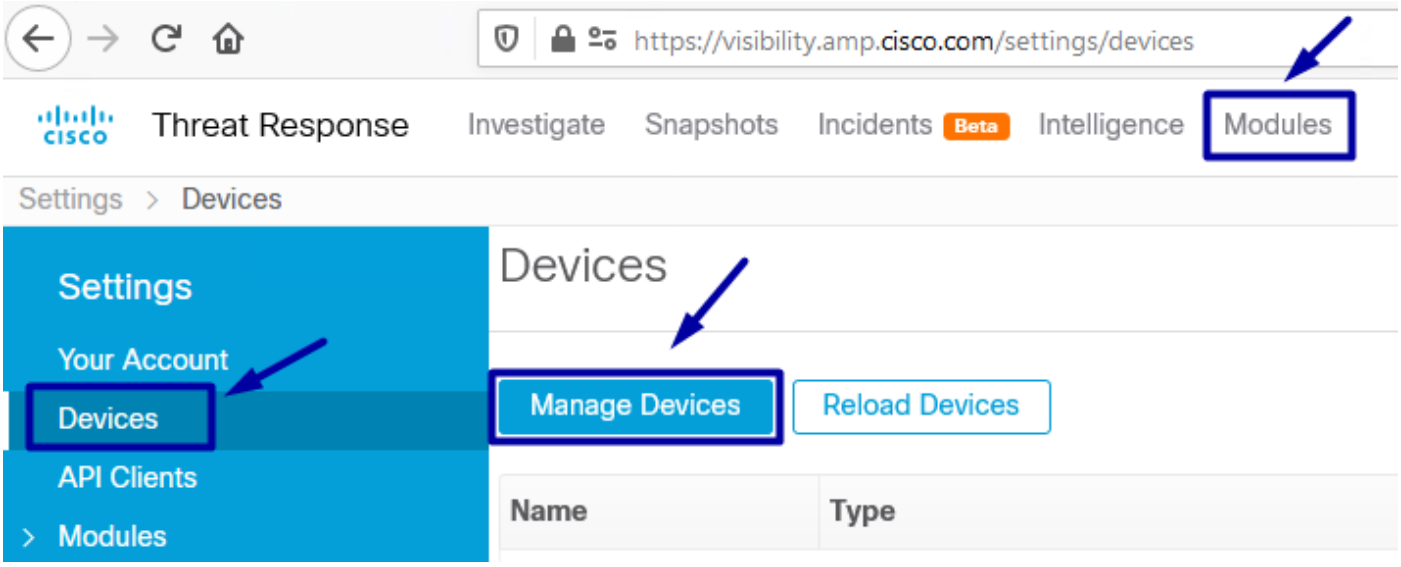




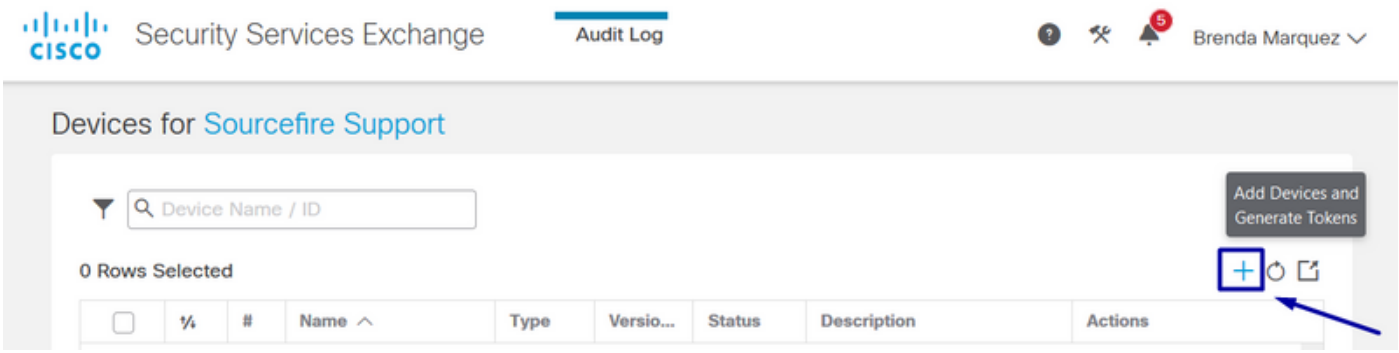


5단계. CTR 포털에 로그인하고 ESA에서 요청된 등록 토큰을 생성합니다.

1.- CTR 포털에서 Modules(모듈) > Devices(디바이스) > Manage Devices(디바이스 관리)로 이동한 후 다음 이미지를 확인하십시오.

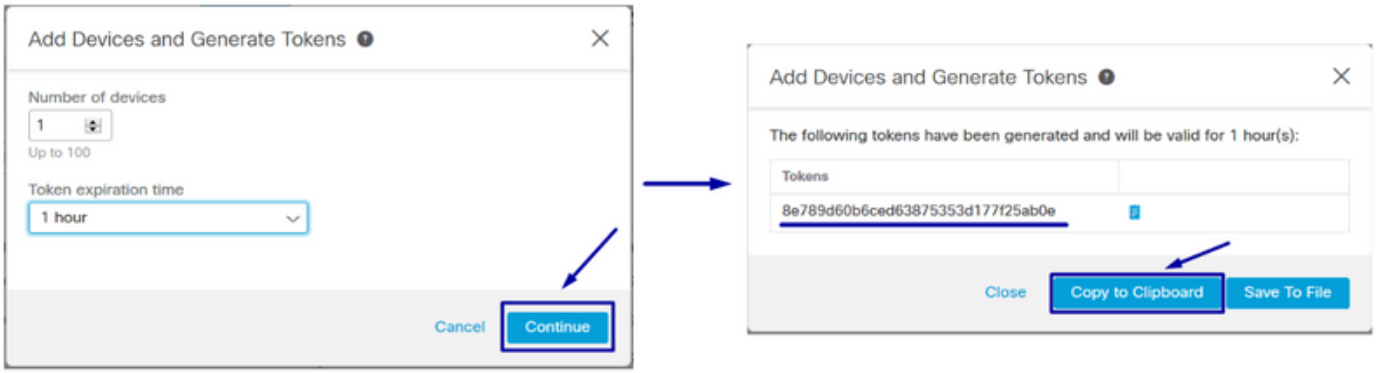


2.- Manage Devices(디바이스 관리) 링크를 클릭하면 SSE(Security Services Exchange)로 리디렉션되고, Add Devices(디바이스 추가) 및 Generate Tokens(토큰 생성) 아이콘을 클릭합니다(이미지에 표시됨).



3. - 토큰을 생성하려면 계속을 클릭하고, 토큰이 생성되면 이미지에 표시된 대로 클립보드에 복사를 클릭합니다.

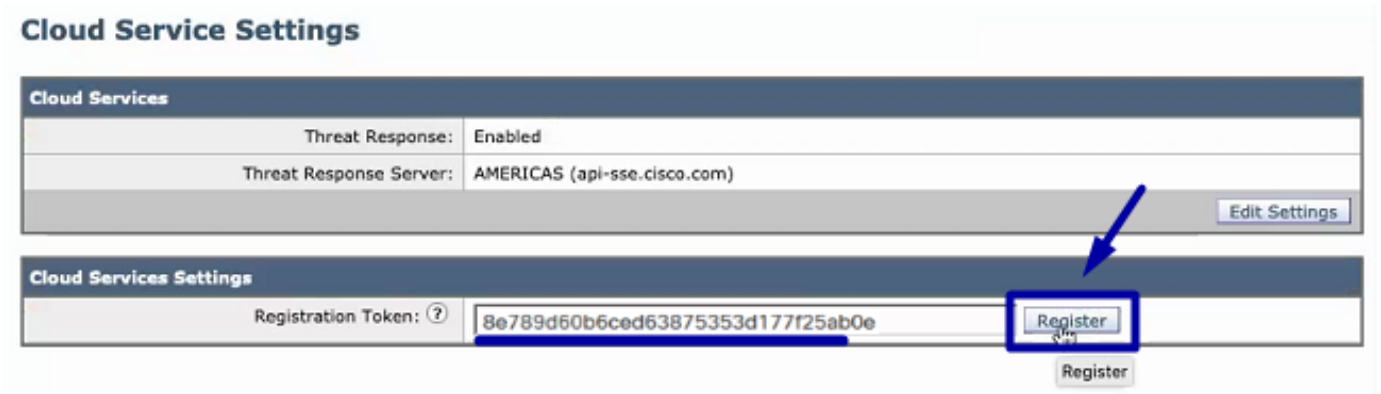
팁:추가할 디바이스 수(1부터 100까지)를 선택하고 토큰 만료 시간(1시간, 2시간, 4시간, 6시간, 6시간, 8시간, 12시간, 12시간, 01일, 02일, 03일, 04일 및 05일)을 선택할 수 있습니다.

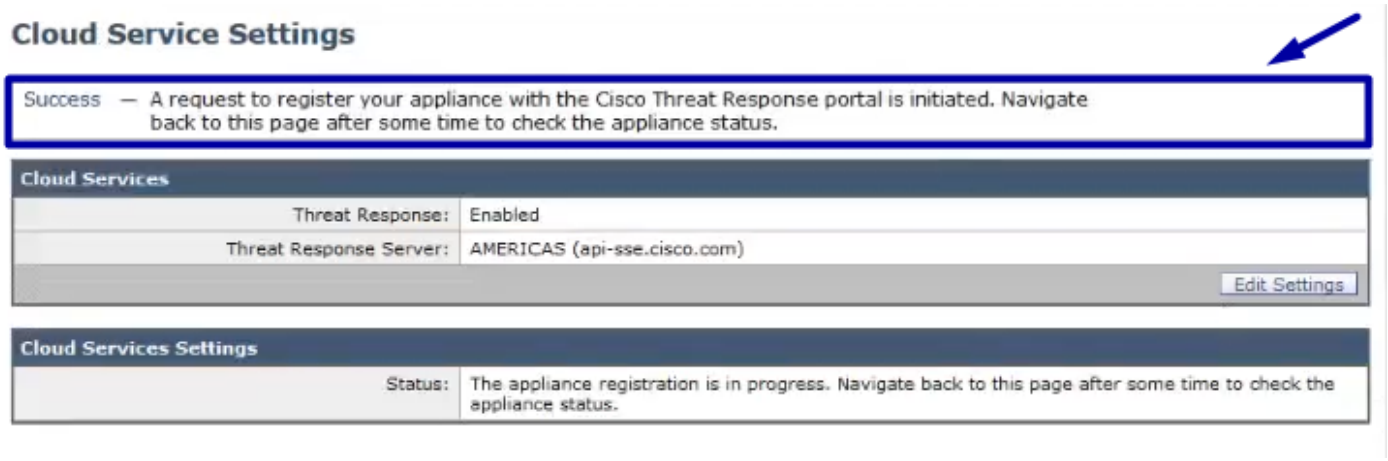


6단계. CTR 포털에서 생성된 등록 토큰을 ESA에 붙여넣기

등록 토큰이 생성되면 ESA의 Cloud Services Settings(클라우드 서비스 설정) 섹션에 아래 이미지와 같이 붙여넣습니다.

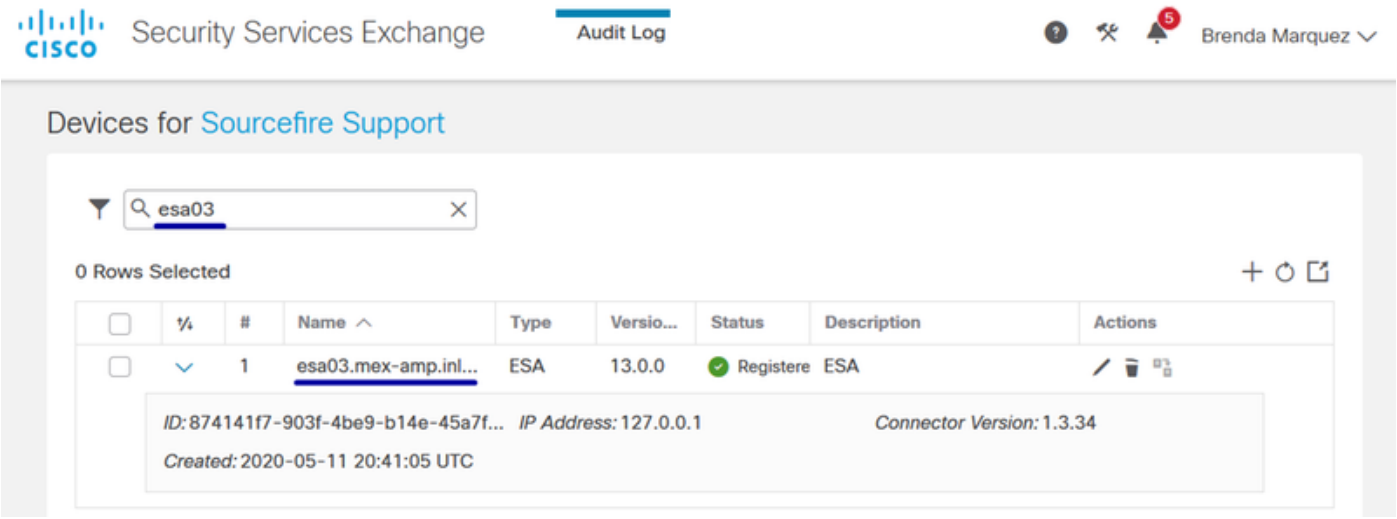
참고:성공 메시지가 표시됩니다.Cisco Threat Response 포털에 어플라이언스를 등록하라는 요청이 시작됩니다.잠시 후에 이 페이지로 이동하여 어플라이언스 상태를 확인합니다.





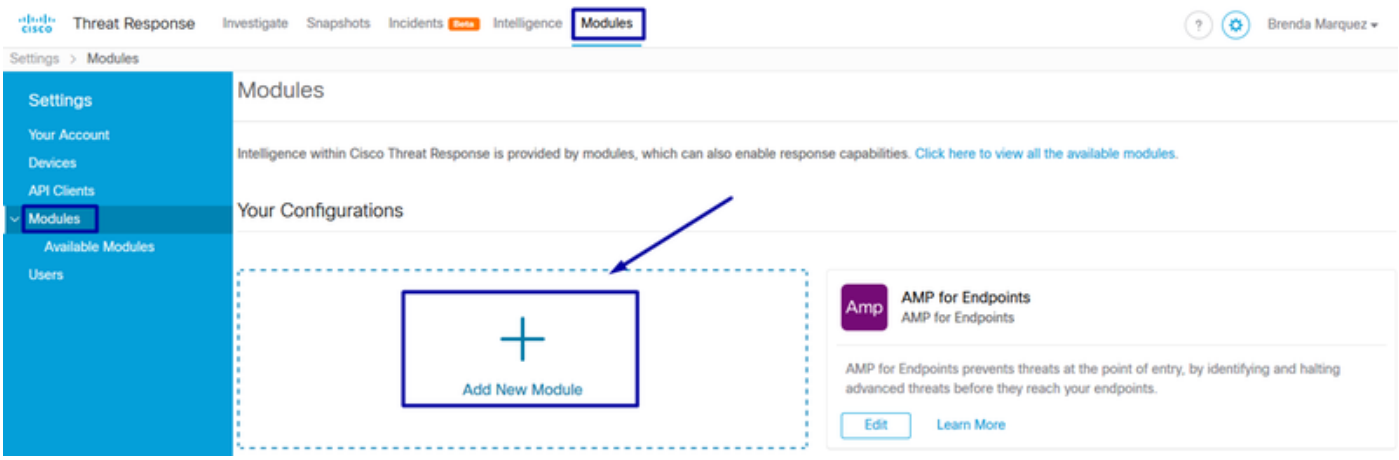
7단계. ESA 디바이스가 SSE 포털에 있는지 확인합니다.

SSE 포털(CTR > Modules > Devices > Manage Devices)으로 이동하고, Search 탭에서 이미지에 표시된 대로 ESA 디바이스를 볼 수 있습니다.

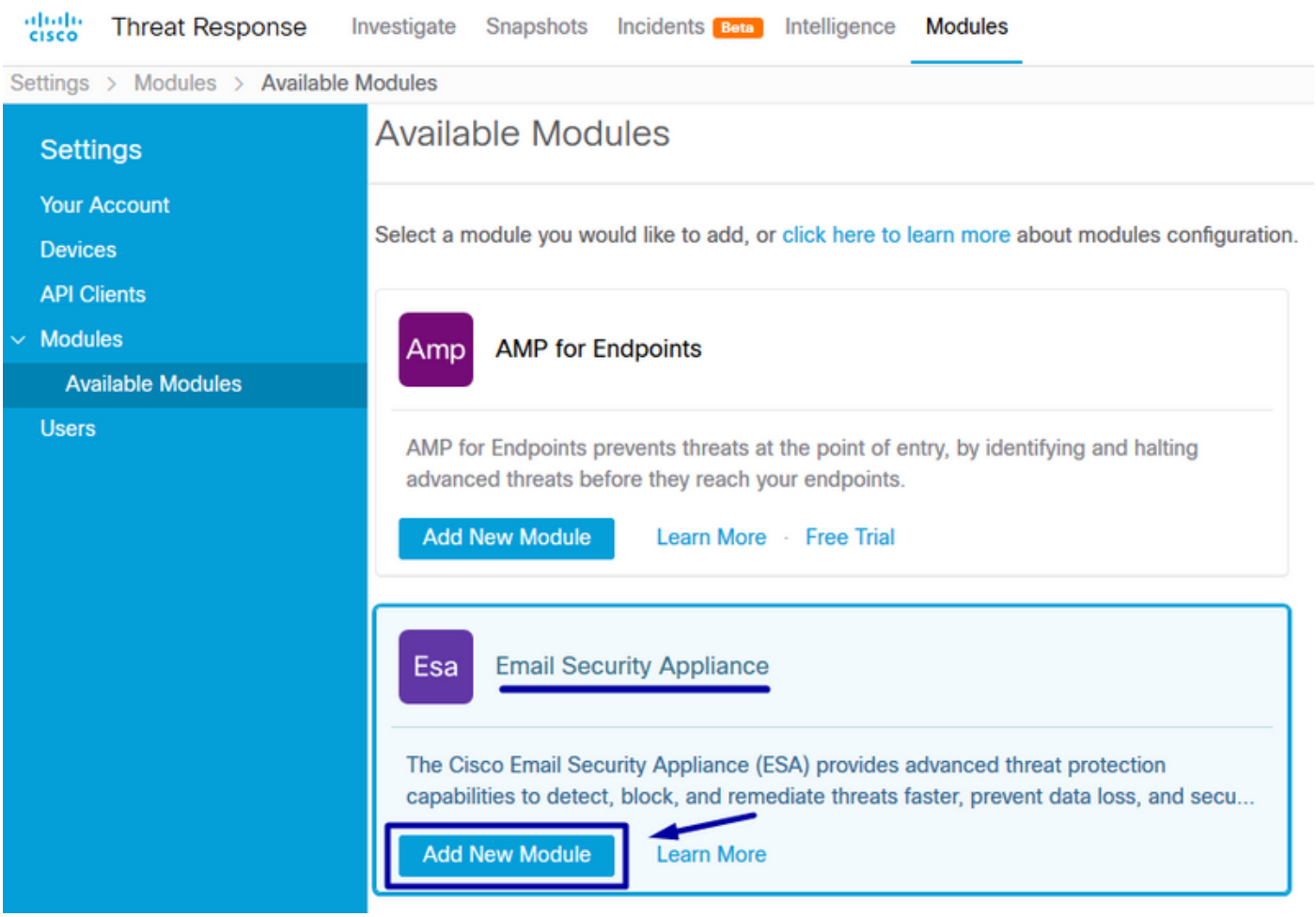


8단계. CTR 포털로 이동하여 새 ESA 모듈을 추가합니다.

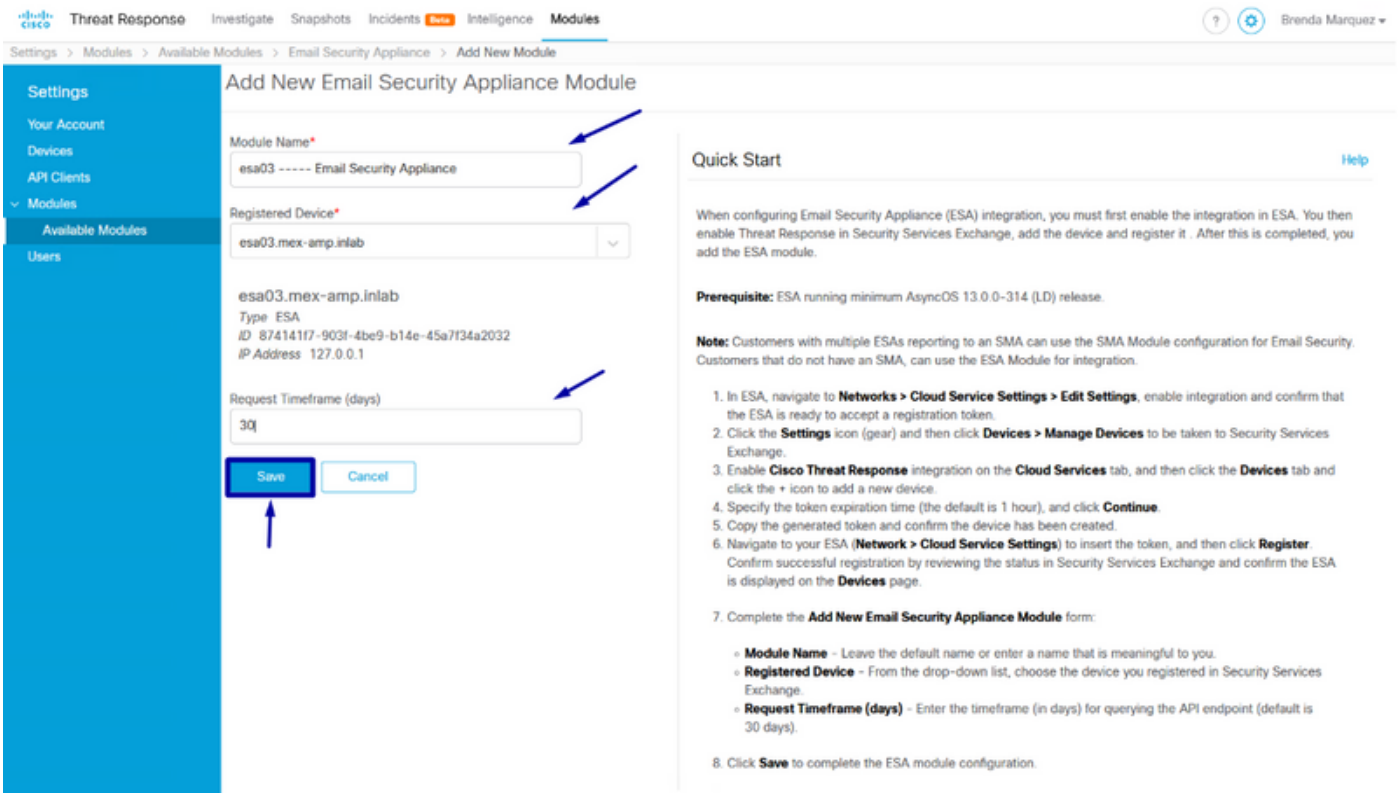
1.- CTR 포털에 있으면 이미지에 표시된 대로 Modules(모듈) > Add New Module(새 모듈 추가)으로 이동합니다.



2. - 모듈 유형을 선택합니다. 이 경우 모듈은 아래 이미지로 Email Security Appliance 모듈입니다.

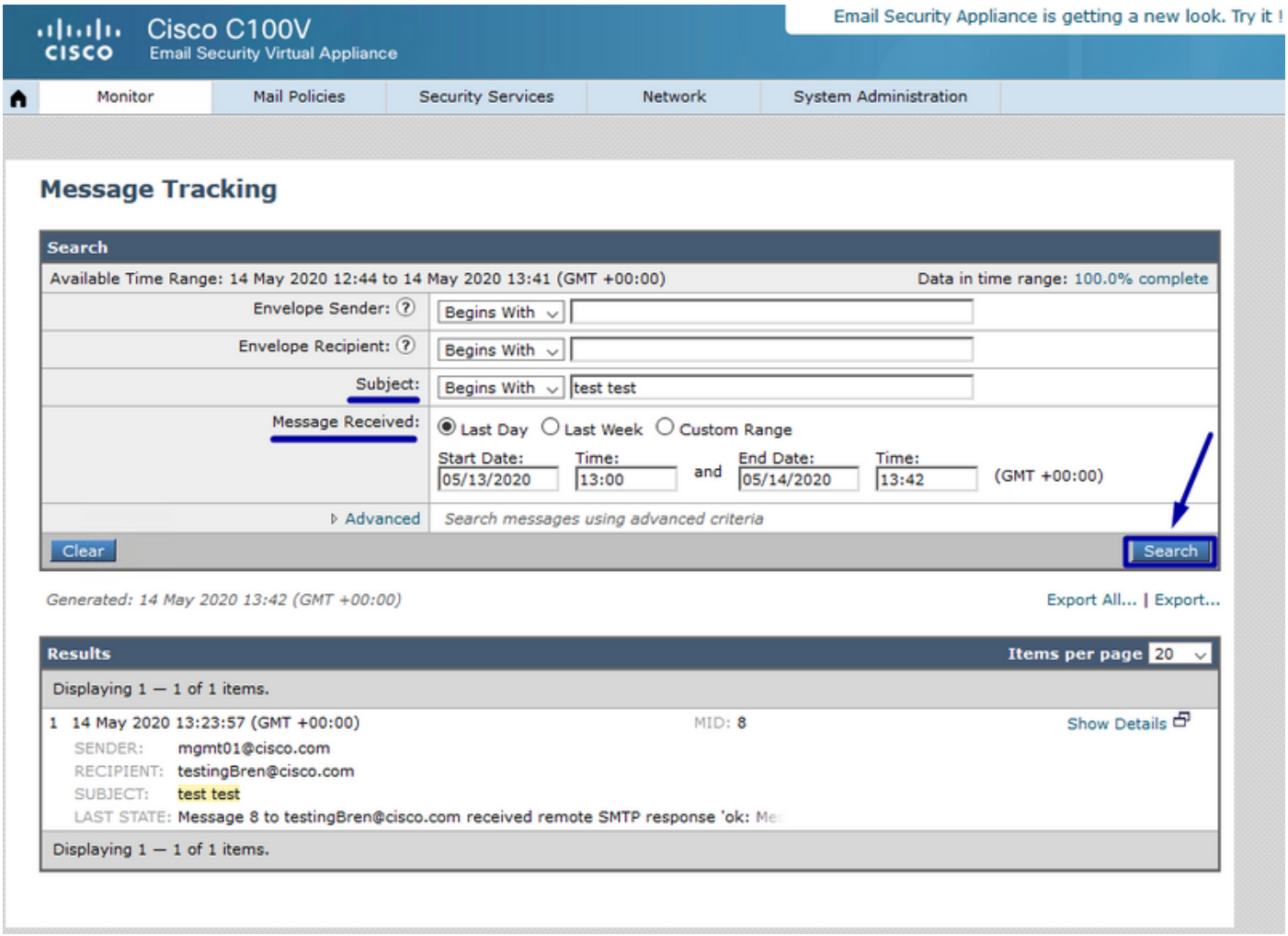


3.- 필드를 입력합니다.이미지에 표시된 대로 Module Name(모듈 이름), Registered Device(이전에 등록한 디바이스 선택) 및 Request Timeframe(기간(일)), Save(저장)가 있습니다.

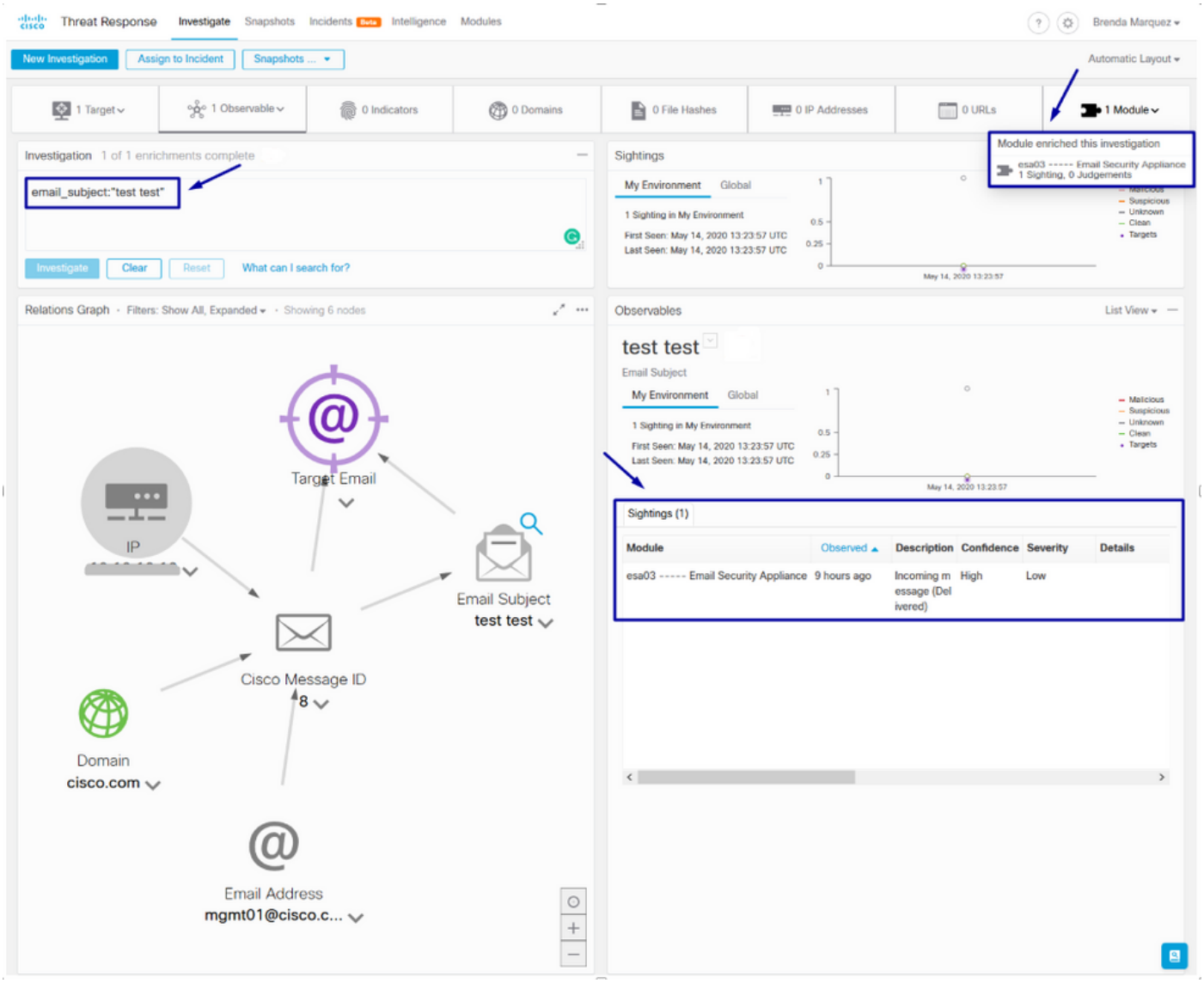


다음을 확인합니다.

CTR 및 ESA 통합을 확인하려면 ESA에서 볼 수 있는 테스트 이메일을 보내고 Monitor(모니터링) > Message Tracking(메시지 추적)으로 이동하여 테스트 이메일을 찾을 수 있습니다.이 경우 아래 이미지로 Email Subject(이메일 제목)로 필터링했습니다.



이제 CTR 포털에서 이미지에 표시된 대로 Investigate(조사)를 수행하고 Investigate(조사)로 이동하고 일부 이메일 관찰 가능 항목을 사용할 수 있습니다.



팁:이미지에 다음과 같은 다른 이메일 관찰 가능 요소에 동일한 구문을 사용할 수 있습니다.

IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file name	file_name:"invoice.pdf"

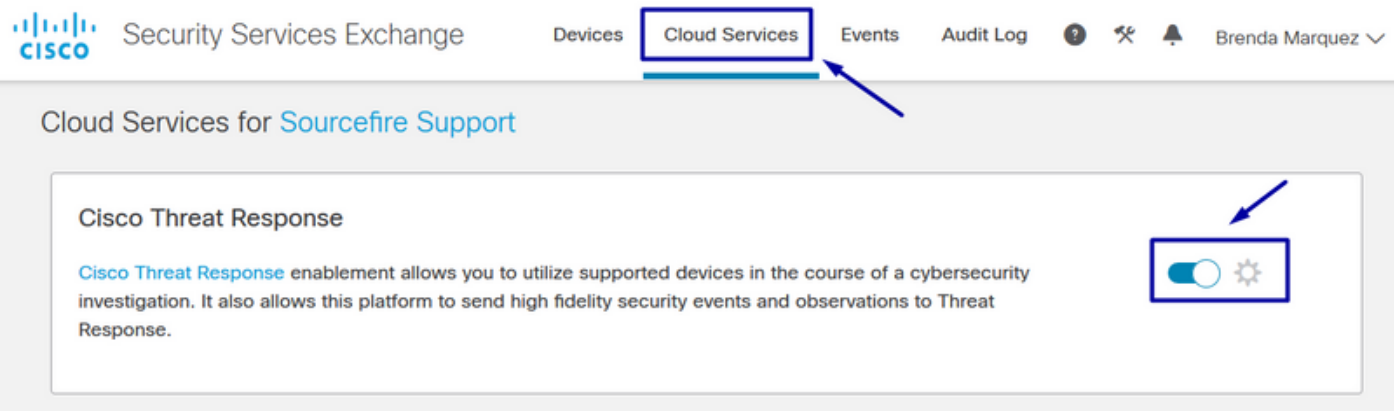
문제 해결

CES 고객이거나 SMA를 통해 ESA 디바이스를 관리하는 경우 SMA를 통해서만 위협 응답에 연결할 수 있습니다.SMA가 AsyncOS 12.5 이상을 실행하는지 확인하십시오.ESA를 SMA로 관리하지 않고 ESA를 직접 통합하는 경우 AsyncOS 버전 13.0 이상인지 확인합니다.

CTR 포털에 ESA 디바이스가 표시되지 않음

ESA 모듈이 CTR 포털에 추가되는 동안 ESA 디바이스가 드롭다운 Registered Device에 표시되지

않는 경우 SSE에서 CTR을 활성화했는지 확인하고, CTR에서 Modules(모듈) > Devices(디바이스) > Manage Devices(디바이스 관리)로 이동한 다음 SSE 포털에서 Cloud Services(클라우드 서비스)로 이동하여 CTR을 활성화합니다. 아래 이미지:



CTR 조사 결과 ESA의 데이터가 표시되지 않음

다음을 확인하십시오.

- 조사 구문은 올바르며, 이메일 관찰 가능 문구는 위에 Verify 섹션에 나와 있습니다.
- 적절한 Threat Response Server 또는 Cloud(Americas/Europe)를 선택했습니다.

ESA에서 등록 토큰을 요청하지 않습니다.

Threat Response가 활성화된 경우 변경 사항을 커밋해야 합니다. 그렇지 않으면 ESA의 Threat Response 섹션에 변경 사항이 적용되지 않습니다.

유효하지 않거나 만료된 토큰으로 인해 등록이 실패했습니다.

토큰이 올바른 클라우드에서 생성되었는지 확인하십시오.

ESA에 유럽(EU) 클라우드를 사용하는 경우 다음 위치에서 토큰을 생성합니다 .https://admin.eu.sse.itd.cisco.com/

ESA에 NAM(Americas) Cloud를 사용하는 경우 다음 위치에서 토큰을 생성합니다 .https://admin.sse.itd.cisco.com/

또한 등록 토큰에 만료 시간이 있습니다(Integration in time을 완료하는 데 가장 편리한 시간 선택).

관련 정보

- **Cisco Threat Response 및 ESA Integration 비디오에서 이 문서에 포함된 정보를 찾을 수 있습니다.**
- 기술 지원 및 문서 – Cisco Systems