XDR 및 Secure Email Appliance(이전의 ESA) 통합 문제 해결

목차

소개

이 문서에서는 기본 분석을 수행하는 단계와 XDR 및 Insights와 Secure Email Appliance 통합 모듈의 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- XDR
- Security Services Exchange
- 보안 이메일

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Security Services Exchange
- XDR
- 소프트웨어 버전 13.0.0-392의 Secure Email C100V

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

배경 정보

Cisco Secure Email Appliance(이전의 Email Security Appliance)는 지능형 위협 차단 기능을 제공하여 위협을 더 신속하게 탐지, 차단, 치료하고 데이터 손실을 방지하며 엔드 투 엔드 암호화를 통해

전송 중인 중요한 정보를 보호합니다. 일단 구성되면 Secure Email Appliance 모듈은 관찰 대상과 관련된 세부사항을 제공합니다. 다음과 같은 작업을 수행할 수 있습니다.

- 조직의 여러 어플라이언스에서 이메일 보고서 및 메시지 추적 데이터 보기
- 이메일 보고서 및 메시지 트랙에서 관찰된 위협 식별, 조사 및 치료
- 식별된 위협을 신속하게 해결하고 식별된 위협에 대해 취할 수 있는 권장 조치를 제공합니다.
- 위협을 문서화하여 조사 내용을 저장하고 다른 장치 간에 정보 협업 지원

Secure Email Appliance 모듈을 통합하려면 SSE(Security Services Exchange)를 사용해야 합니다. SSE를 사용하면 Secure Email Appliance가 Exchange에 등록할 수 있으며 사용자는 등록된 디바이스에 액세스할 수 있는 명시적 권한을 제공합니다.

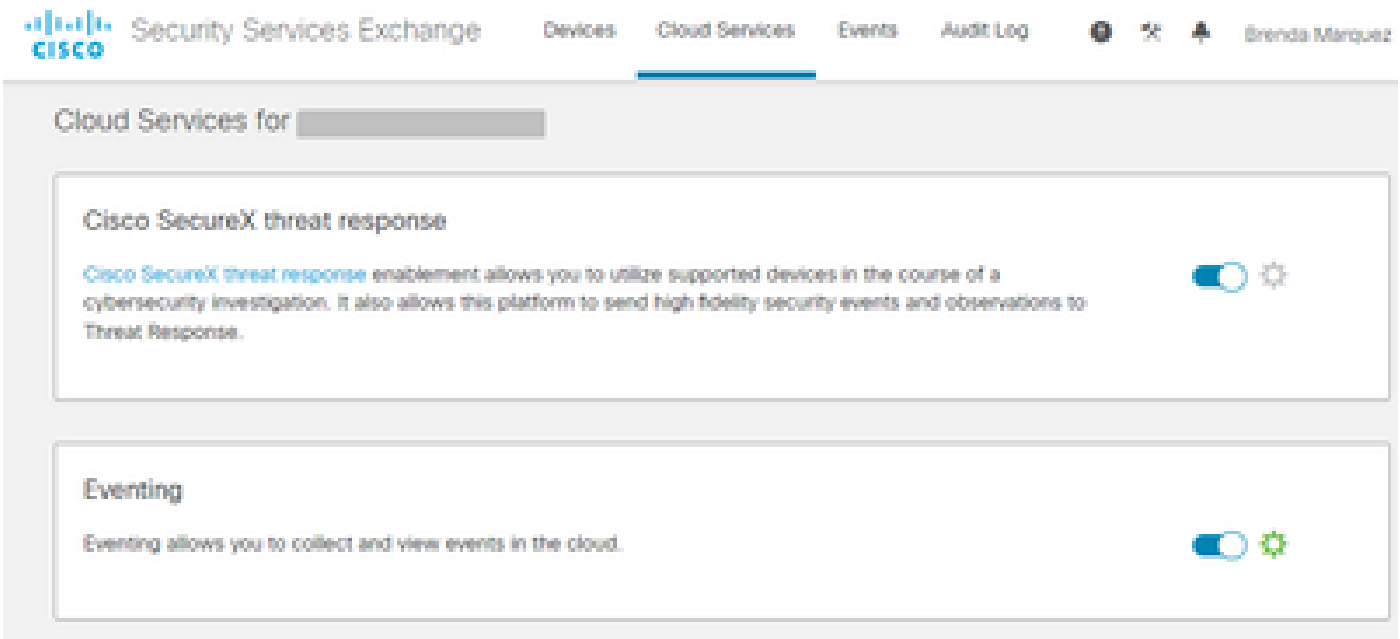
컨피그레이션에 대해 자세히 알아보려면 통합 모듈 세부사항의 이 문서를 검토하십시오.

문제 해결

XDR 및 Secure Email Appliance 통합과 관련된 일반적인 문제를 해결하려면 다음 단계를 확인할 수 있습니다.

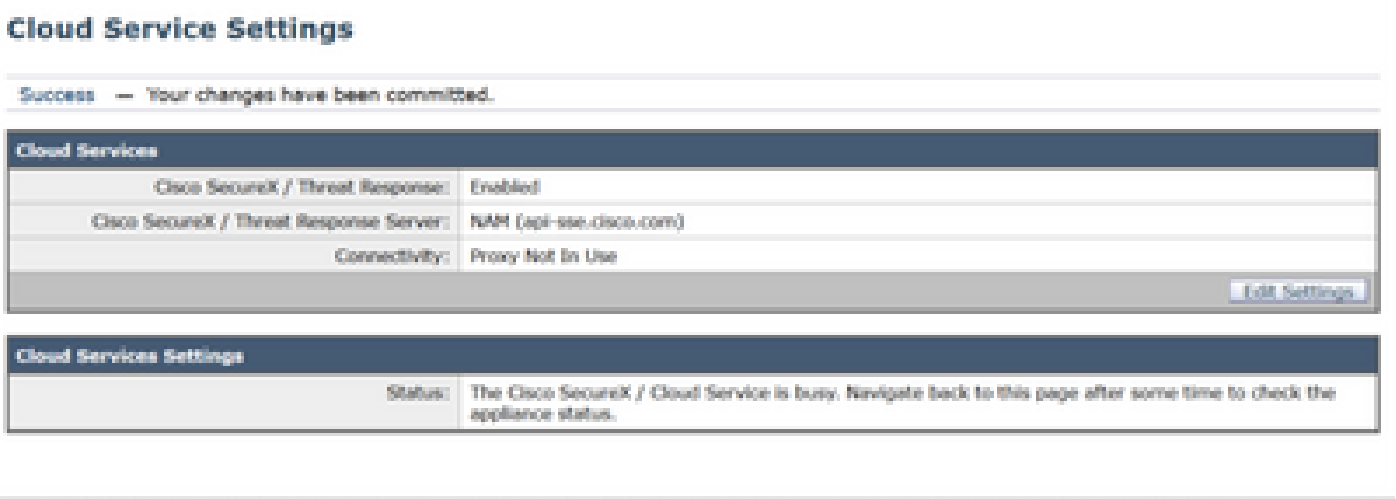
보안 이메일 장치는 XDR 또는 보안 서비스 교환 포털에 표시되지 않습니다

디바이스가 SSE 포털에 표시되지 않으면 아래 이미지와 같이 SSE 포털에서 XDR 위협 대응 및 이벤트 서비스를 활성화했는지 확인하고 클라우드 서비스로 이동하여 서비스를 활성화하십시오.



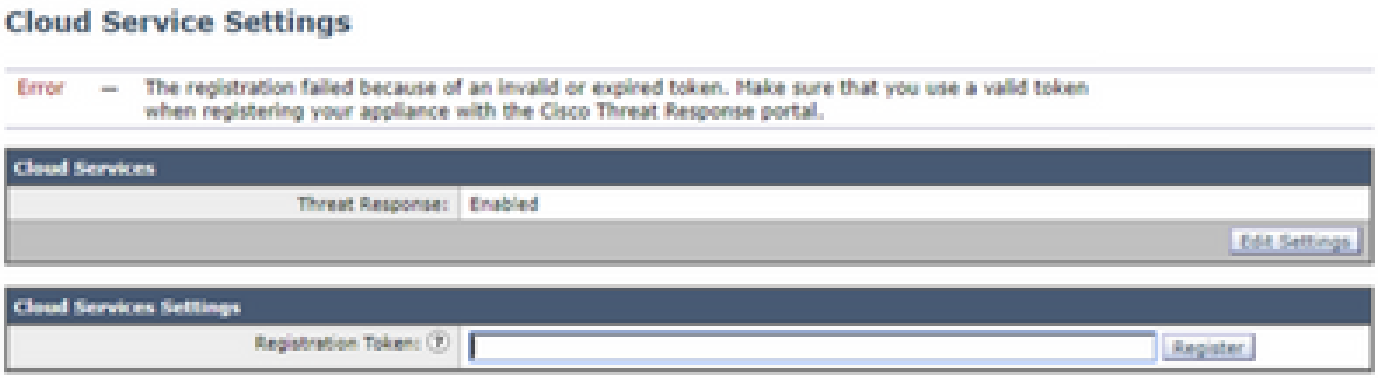
보안 이메일이 등록 토큰을 요청하지 않음

Cisco XDR/Threat Response 서비스가 활성화된 후에는 변경 사항을 커밋하십시오. 그렇지 않으면 보안 이메일의 클라우드 서비스 섹션에 변경 사항이 적용되지 않습니다. 아래 이미지를 참조하십시오.



유효하지 않거나 만료된 토큰으로 인해 등록하지 못했습니다.

"유효하지 않거나 만료된 토큰으로 인해 등록이 실패했습니다. 아래 이미지와 같이 Secure Email GUI의 "Cisco XDR Threat Response portal"에서 어플라이언스에 유효한 토큰을 사용해야 합니다.



올바른 클라우드에서 토큰이 생성되었는지 확인하십시오.

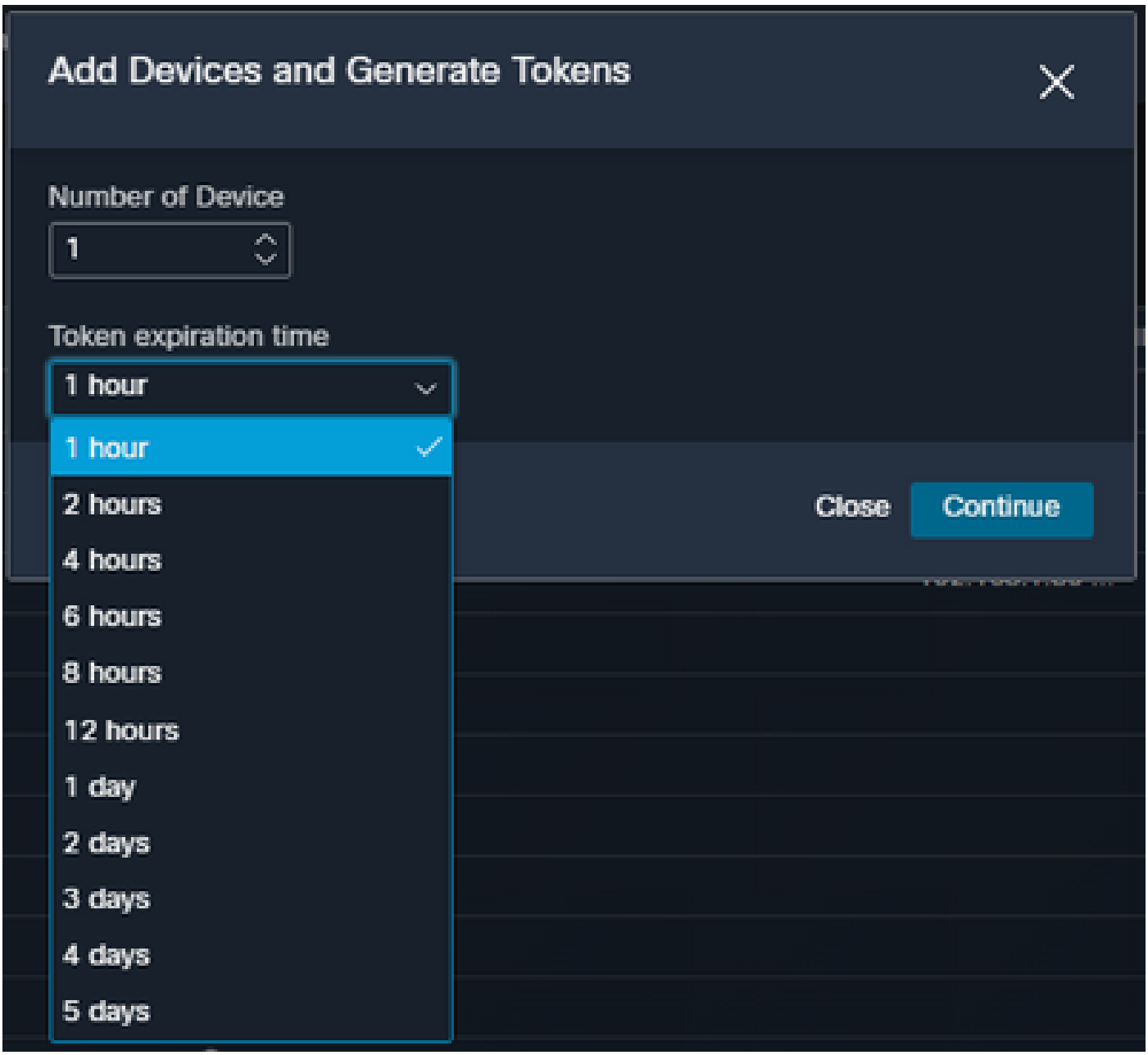
Secure Email에 유럽(EU) 클라우드를 사용하는 경우 https://admin.eu.sse.itd.cisco.com/에서 토큰을 생성합니다.

Secure Email에 Americas(NAM) Cloud를 사용하는 경우 https://admin.sse.itd.cisco.com/에서 토큰을 생성합니다

SSE(Security Services Exchange) 포털:	NAM: https://admin.sse.itd.cisco.com/ EU: https://admin.eu.sse.itd.cisco.com/
Cisco XDR 포털	NAM: https://XDR.us.security.cisco.com/ EU: https://XDR.eu.security.cisco.com/
보안 이메일 Cisco XDR/Threat Response Server:	NAM: api-sse.cisco.com

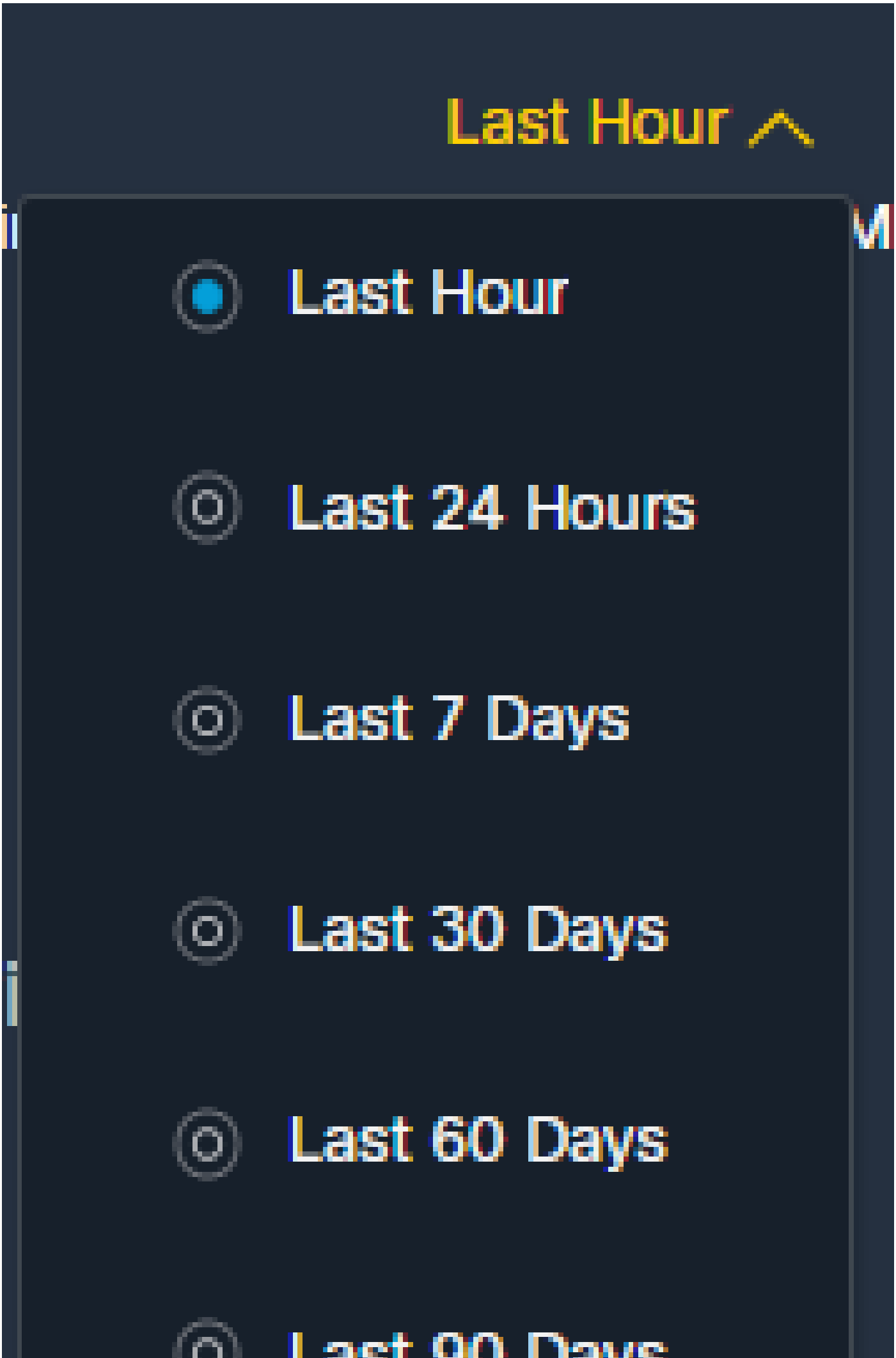
	EU: api.eu.sse.itd.cisco.com

또한 등록 토큰에는 이미지에 표시된 대로 만료 시간이 있습니다(적시에 통합을 완료하는 데 가장 편리한 시간 선택).



XDR 대시보드에는 보안 이메일 모듈에 대한 정보가 표시되지 않습니다

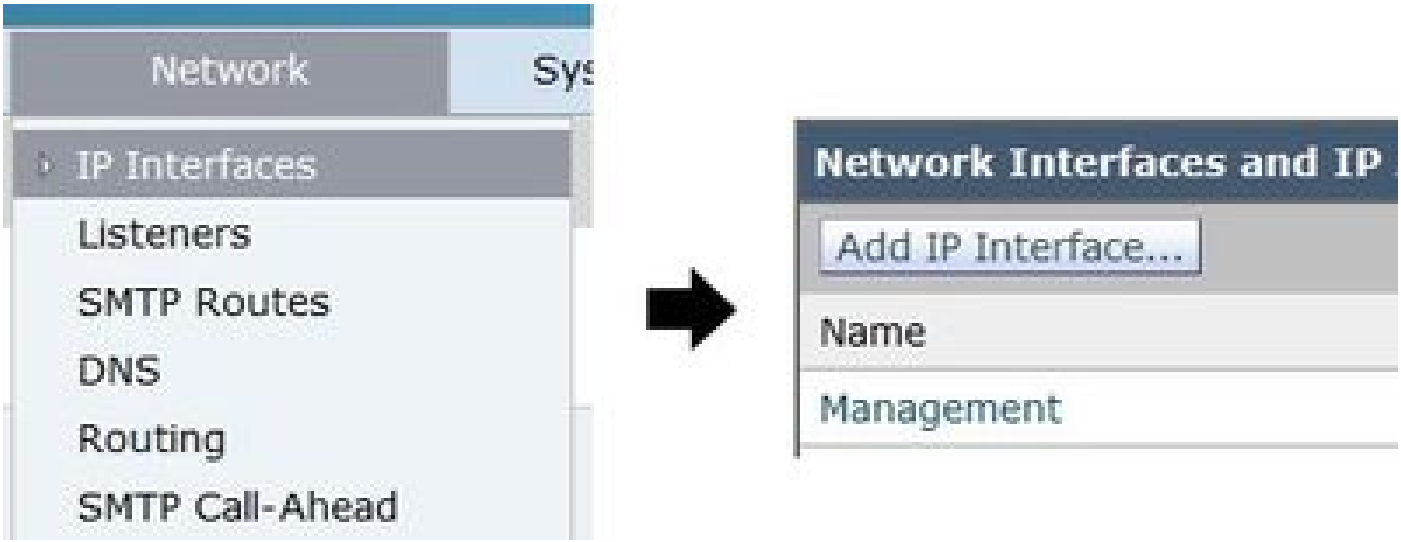
아래 그림과 같이 사용 가능한 타일에서 지난 1시간에서 지난 90일까지 더 넓은 시간 범위를 선택할 수 있습니다.

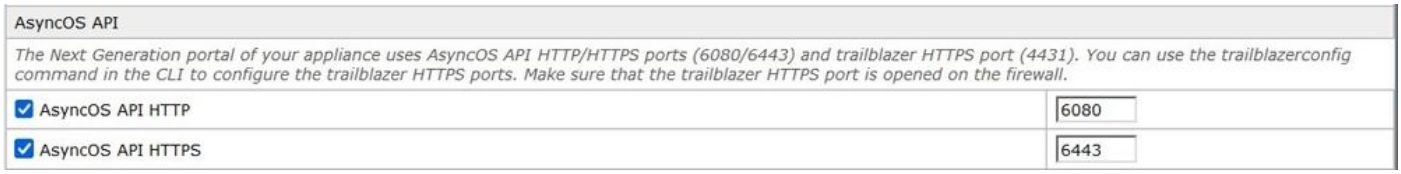

Last Hour
Last Hour
Last 24 Hours
Last 7 Days
Last 30 Days
Last 60 Days

포털을 통해 등록된 것으로 계속 표시되는지, 디바이스가 등록 취소되어 더 이상 표시되지 않는지 확인합니다. XDR 포털에 새 모듈을 추가해 보십시오.

XDR 보안 이메일 타일 모듈에 "보안 이메일 모듈에 예기치 않은 오류가 있습니다." 오류가 표시됩니다.

Secure Email을 사용하려면 관리 인터페이스를 통해 활성화된 AsyncOS API HTTP 및 HTTPS 컨피그레이션이 XDR/CTR 포털과 통신해야 합니다. 온프레미스 Secure Email의 경우 Secure Email 포털 GUI에서 이 기능을 구성합니다. 이미지에 표시된 대로 Network(네트워크) > IP Interfaces(IP 인터페이스) > Management interface(관리 인터페이스) > AsyncOS API로 이동하여 HTTP 및 HTTPS를 활성화합니다.



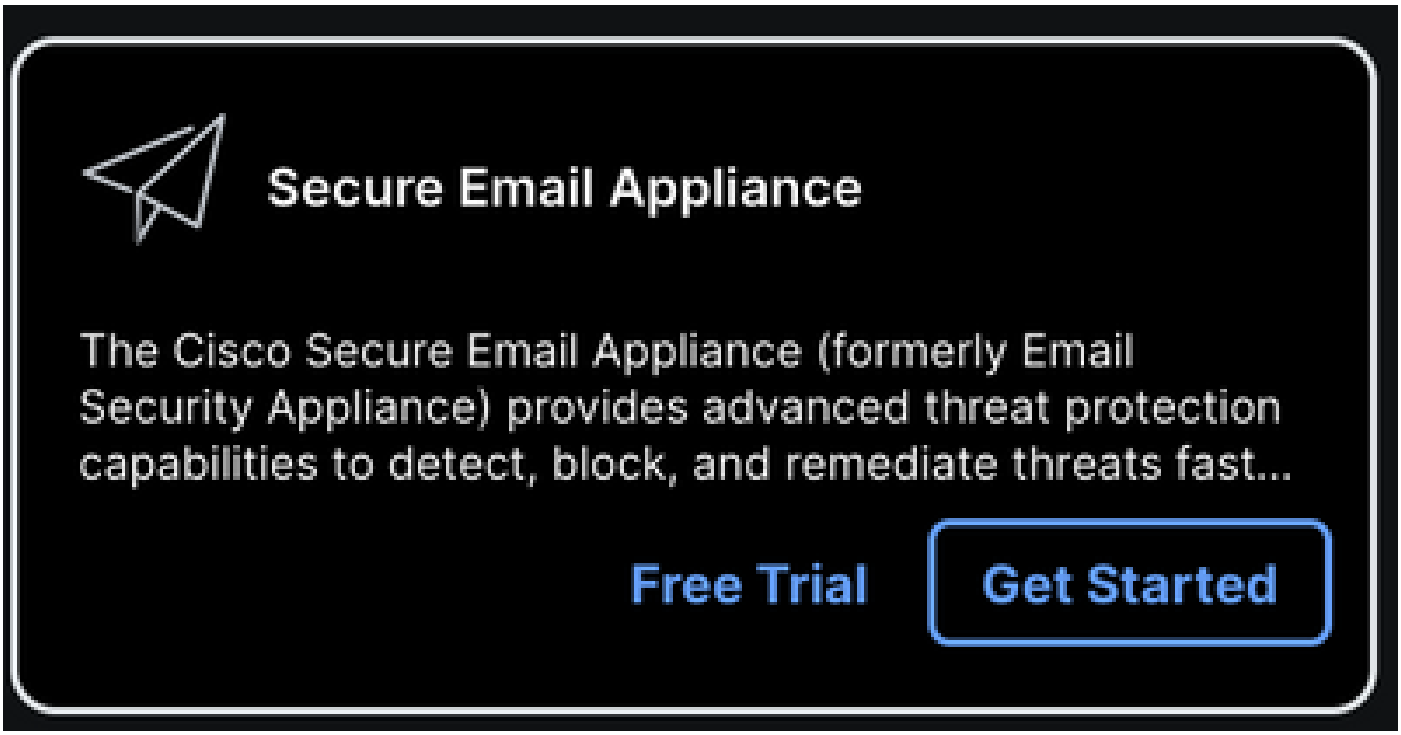


CES(Cloud-Based Secure Email)의 경우 Secure Email TAC 엔지니어가 백엔드에서 이 컨피그레이션을 수행해야 하며, 영향을 받는 CES의 지원 터널에 액세스해야 합니다.

다음을 확인합니다.

Secure Email이 Device Insights에 소스로 추가되면 성공적인 REST API 연결 상태를 확인할 수 있습니다.

- 녹색 상태의 REST API 연결을 볼 수 있습니다
- 이미지에 표시된 것처럼 초기 전체 동기화를 트리거하려면 SYNC NOW를 누릅니다



XDR 및 Secure Email Appliance 통합과 관련하여 문제가 지속되는 경우, 브라우저에서 HAR 로그를 수집하려면 이 문서를 참조하고 TAC 지원에 문의하여 자세한 분석을 수행하십시오.

관련 정보

- 이 문서의 정보는 이 XDR 및 보안 이메일 통합 비디오에서 확인할 수 있습니다.
- 여기서 제품 통합을 구성하는 방법에 대한 비디오를 찾을 수 있습니다
- 기술 지원 및 문서 – Cisco Systems

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.