Advanced Threat Solutions 트러블슈팅 참조 설명서

목차

소개

이 문서에서는 Cisco Secure Endpoint, Cisco Secure Malware Analytics, Cisco Threat Response (CTR), Cisco SecureX와 같은 제품의 ATS(Advanced Threat Solutions) 설명서 링크에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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

다음 문서는 Advanced Threat Solutions 제품의 컨피그레이션/트러블슈팅에 대한 참조 가이드입니다. 이 문서는 Cisco TAC에 참여하기 전에 참조할 수 있습니다.

Cisco Secure Endpoint 설명서 링크

제품 포털	관련 문서	태그
퍼블릭 클라우드 미국 클라우드 EU 클라우드 APJC 클라우드	일반 문서	Documentation
	적절한 보안 엔드포인트 및 보안 악성코드 분석 작업에 필요한 서버 주소	Configuration
	보안 엔드포인트 커넥터 지원 정책	Documentation
	Cisco Security Account 사용 설명서	Documentation
	보안 엔드포인트에서 2단계 인증 구성	Configuration
	보안 엔드포인트 구축 방법론 및 모범 사례	Configuration
	보안 엔드포인트 자격	Configuration

	Cisco Security Accounts에 대한 Secure Sign-On 활성화		Configuration
	보안 엔드포인트 알림 이메일		Configuration
	보안 엔드포인트에서 제외 구성 및 관리	비디오	Configuration
	Secure Endpoint Console에 대한 Cisco 유지 관리 제외 목록 변경 사항		Configuration
	Secure Endpoint 제외에 대한 모범 사례		Configuration
	보안 엔드포인트 포털에서 Simple Custom Detection(단순 맞춤형 탐지) 목록 구성		Configuration
	보안 엔드포인트 콘솔 및 마지막으로 확인한 필터		Troubleshooting
	API를 사용하여 보안 엔드포인트 포털에서 애플리케이션 차단 목록 내보내기		Configuration
	보안 엔드포인트 API를 사용하여 이벤트 스트림을 생성하는 방법		Configuration
	Secure Endpoint Portal에서 Secure Malware Analytics의 파일을 제출하는 방법		Troubleshooting
	보안 엔드포인트 구축에서 Orbital 고급 검색 옵트인 및 활성화		Documentation
	TETRA 정의 업데이트 실패 문제 해결		Troubleshooting
	Splunk와 안전한 엔드포인트 통합		Configuration
	보안 엔드포인트에서 팝업 알림 구성		Configuration
Android 커넥터	보안 엔드포인트용 Android 디바이스에서 문제 해결 데이터 가져오기		Troubleshooting
iOS 선명도	Cisco Security Connector Apple iOS 호환성		Documentation
	보안 엔드포인트 Cisco Security Connector에서 보고서 문제/진단 데이터 생성		Troubleshooting
	CSC(Cisco Security Connector)에서 사용할 iOS 디바이스를 감독하는 방법		Troubleshooting

Windows 커넥터	Windows에서 실행 중인 보안 끝점 커넥터에서 진단 데이터 수집	Troubleshooting
	보안 엔드포인트 Windows 커넥터 OS 호환성	Documentation
	보안 엔드포인트 Windows 커넥터 업데이트 재부팅 요구 사항	Documentation
	Secure Endpoint Connector 버전에 대한 지원 종료 발표	Documentation
	Secure Endpoint Connector용 Windows XP, Windows Vista 및 Windows 2003의 지원 종료 공지	Documentation
	새로운 보안 엔드포인트 패키지와 관련하여 2020년 1월 8일 기준 기존 고객을 위한 FAQ	Documentation
	보안 엔드포인트에서 Windows 정책 구성 / 비디오	Configuration
	[외부] - Secure Endpoint Connector Installer용 명령줄 스위치	Configuration
	보안 엔드포인트 명령줄 스위치	Configuration
	TETRA 정의 수동 업데이트 - 보안 엔드포인트 / 비디오	Troubleshooting
	보안 엔드포인트 업데이트 서버 컨피그레이션 단계	Configuration
	시작 시 보안 엔드포인트 문제를 해결하기 위해 ProcMon 로그를 수집하는 방법	Troubleshooting
	Cisco Secure Endpoint에서 고급 맞춤형 탐지 목록 생성	Troubleshooting
	높은 CPU를 위한 보안 엔드포인트 진단 번들 분석	Troubleshooting
	안전 모드로 보안 엔드포인트 Windows 커넥터를 제거하는 방법	Troubleshooting

	비밀번호를 잊은 경우 Secure Endpoint 커넥터를 제거하는 절차	Troubleshooting
	Windows Process가 보안 엔드포인트 커넥터 전에 시작됨 해결 방법 - 보안 엔드포인트	Configuration
	Secure Endpoint Exploit Prevention Engine과 EMET 호환성	Configuration
	익스플로잇 차단	Documentation
	ID 지속성 Cisco Secure Endpoint 가이드	Configuration
	Windows에서 보안 엔드포인트 설치에 필요한 루트 인증서 목록	Troubleshooting
	보안 엔드포인트 Windows 커넥터 설치 프로그램 종료 코드	Documentation
	보안 엔드포인트에서 스크립트 보호 문제 해결	Troubleshooting
Linux 커넥터	보안 엔드포인트 Linux 커넥터에서 진단 데이터 수집	Troubleshooting
	보안 엔드포인트 Linux 커넥터 OS 호환성	Documentation
	보안 엔드포인트 Linux 커넥터 업데이트 재부팅 요구 사항	Documentation
	보안 엔드포인트 Linux 커넥터 설치 — 비디오	Configuration
	Linux의 보안 엔드포인트 ClamAV 바이러스 정의 옵션	Configuration
	Cisco Secure Endpoint Mac/Linux CLI	Configuration
	보안 엔드포인트 Linux 커넥터 결합	Troubleshooting
	Secure Endpoint Linux Connector 기본 문제 해결 설명서	Troubleshooting
	보안 엔드포인트 Linux 입문서	Documentation
	Ubuntu의 보안 엔드포인트 Linux 커넥터	Configuration
	Ubuntu 20.04.0 LTS 및 Ubuntu 20.04.1 LTS의	Documentation

	Secure Endpoint Linux Connector 1.15.0 권고	
	Linux 커널 레벨 결함	Troubleshooting
Mac 커넥터	Mac 진단 데이터 수집을 위한 보안 엔드포인트 커넥터	Troubleshooting
	보안 엔드포인트 Mac 커넥터 OS 호환성	Documentation
	높은 CPU를 위한 macOS 보안 엔드포인트 진단 번들 분석	Troubleshooting
	MacOS 및 Linux에서 안전한 엔드포인트 프로세스 제외	Configuration
	Secure Endpoint Mac Connector 성능 조정 가이드	Troubleshooting
	콘솔의 MAC 커널 및 전체 디스크 액세스 - 보안 엔드포인트	Troubleshooting
	보안 엔드포인트 Mac Connector의 수동 제거 절차	Configuration
	MacOS 11(Big Sur), macOS 10.15(Catalina) 및 macOS 10.14(Mojave)의 Secure Endpoint Mac Connector 1.14 권고	Configuration
	보안 엔드포인트 Mac 커넥터 결함	Troubleshooting
프라이빗 클라우드	일반 문서	Documentation
	보안 엔드포인트 프라이빗 클라우드 지원 정책	Documentation
	Secure Endpoint Virtual Private Cloud 설치 및 구성	Documentation
	Secure Endpoint Private Cloud PC3000 이미지 재구축 및 백업 복원	Configuration
	Secure Endpoint Private Cloud 3.x 이후 설치에 필요한 인증서 생성 및 추가	Configuration
	AirGapped Secure Endpoint Private Cloud(가상 및 어플라이언스) 업그레이드 절차	Configuration

	보안 엔드포인트 프라이빗 클라우드 지원 스냅샷 생성 및 라이브 지원 세션 활성화	Troubleshooting
	SSH를 통해 Secure Endpoint Private Cloud의 CLI에 액세스하고 SCP를 통해 파일 전송	Configuration
	Secure Endpoint Private Cloud 3.0.1 업그레이드 절차	Documentation
	Secure Endpoint Private Cloud 3.1.1로 업그레이드 - 디스크 공간 및 메모리 추가	Documentation
효율성/위협 요소 제거/규정 준수	신종 바이러스/감염(사고 대응)	Documentation

Cisco Secure Malware Analytics Appliance

제품 포털	관련 문서	태그
Cisco Secure Malware Analytics Appliance	컨피그레이션 가이드	Documentation
	설치 및 업그레이드 가이드	Documentation
	Secure Malware Analytics Appliance 시스템 버전	Documentation
	End-of-Sale 및 End-of-Life 공지	Documentation
	클러스터 작업을 위한 Secure Malware Analytics Appliance 구성	Configuration
	Secure Malware Analytics 지원 스냅샷 생성 및 실시간 지원 세션 활성화	Troubleshooting
	Cisco Secure Malware Analytics Appliance용 SSH 클라이언트 설정	Configuration
	Secure Malware Analytics Appliance Air-Gap 모드 업데이트	Configuration
	Secure Malware Analytics 지원 스냅샷 생성 및 실시간 지원 세션 활성화	Configuration
	Prometheus Monitoring Software로 Secure Malware Analytics Appliance 구성	Configuration

	EFI 셸을 사용하여 Secure Malware Analytics Appliance를 복구 모드로 부팅하고 복구 모드를 부팅 옵션에 추가하는 방법	Configuration
	Secure Malware Analytics Appliance Air-Gap 모드 업데이트	Configuration
	콘솔 및 OPadmin 포털에 대해 DTLS 인증을 통한 보안 악성코드 분석 RADIUS 구성	Configuration
	Secure Malware Analytics Appliance 서드파티 통합 구성	Configuration
	Secure Malware Analytics Appliance 대시보드에 없는 샘플 및 디바이스 트러블슈팅	Configuration
	FMC와의 Secure Malware Analytics Appliance 통합 문제 해결	Configuration
	Secure Malware Analytics 비디오 재생 목록	Video

Cisco SecureX

제품 포털	관련 문서	태그
Cisco SecureX 미국 클라우드 EU 클라우드 APJC 클라우드	컨피그레이션 가이드	Documentation
	SecureX 참조 설명서	Configuration
	SecureX 블로그	Documentation
	SecureX FAQ	Documentation
	Cisco Live On-Demand 라이브러리	Video
	Cisco SecureX 비디오 재생 목록	Video
	CTR 및 보안 악성코드 분석 통합	Configuration

SecureX 위협 대응 [이전 Cisco CTR(Threat Response)] 미국 클라우드 EU 클라우드 APJC 클라우드	Cisco 위협 대응 및 Firepower 통합		Configuration
	FMC 및 CTR 통합 문제 해결		Configuration
	Cisco CTR(Threat Response) 및 ESA 통합	비디오	Configuration
	ESA: 파일 평판 및 파일 분석		Configuration
	WSA와 CTR 통합		Configuration
	CTR FAQ		Configuration
	Cisco Threat Response 컨피그레이션 자습서		Configuration
	Cisco Threat Response 비디오 재생 목록		Video
SecureX Orchestrator 미국 클라우드 EU 클라우드 APJC 클라우드	SecureX 오케스트레이션 자습서		Documentation
	자동화 검토 - Cisco 커뮤니티		Configuration Troubleshooting
	ActionOrchestratorContent - Github		Documentation

통합 관련 문서

제품 포털	관련 문서	태그
Cisco Secure Endpoint 미국 클라우드 EU 클라우드	FMC와 보안 엔드포인트 통합	Configuration
	AnyConnect 4.x 및 AMP Enabler를 통한 AMP 모듈 설치 및 구성	Configuration
	ESA/CES - 클러스터링된 어플라이언스를 보안 엔드포인트에 등록하기 위한 절차	Configuration

APJC 클라우드	보안 엔드포인트 및 보안 악성코드 분석을 WSA와 통합	Configuration
Cisco Secure Malware Analytics 미국 클라우드 EU 클라우드	Umbrella 및 Secure Malware 분석 통합	Configuration
	Content Security Appliance(ESA, SMA, WSA) 및 DC/FMC의 파일 분석 클라이언트 ID	Troubleshooting
Cognitive 위협 분석 (CTA)	보안 엔드포인트를 사용한 CTA 데모	Configuration

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.