보안 인증 컴플라이언스

다음 주제에서는 보안 인증 표준을 준수하도록 시스템을 구성하는 방법에 대해 설명합니다.

보안 인증 컴플라이언스 모드

조직에서는 미국국방부 및 글로벌 인증 기관이 마련한 보안 표준을 준수하는 장비 및 소프트웨어만 사용해야 할 수 있습니다. Firepower에서는 다음 보안 인증 표준에 대한 컴플라이언스를 지원합니다.

- CC(Common Criteria): 국제상호인정협정(Common Criteria Recognition Arrangement)에서 마련한 글로벌 표준으로, 보안 제품의 속성이 정의되어 있음
- UCAPL(Unified Capabilities Approved Products List): 미국국방부 정보시스템 계획국(U.S. Defense Information Systems Agency, DISA)이 마련한 보안 요구 사항을 충족하는 제품의 목록

참고 미국 정부에서 UCAPL(Unified Capabilities Approved Products List)의 이름을 DODIN APL(국방부 정보 네트워크 승인 제품 목록)로 변경했습니다. Firepower Management Center 웹 인터페이스 및 이 문서의 UCAPL에 대한 참조를 DODIN APL에 대한 참조로 해석할 수 있습니다.

- FIPS(Federal Information Processing Standard) 140: 암호화 모듈에 대한 요구 사항 사양

CC 모드 또는 UCAPL 모드에서 보안 인증서 컴플라이언스를 활성화할 수 있습니다. 보안 인증 컴플라이언스를 활성화한다고 해서 선택한 보안 모드의 모든 요구 사항이 반드시 엄격하게 준수되는 것은 아닙니다. 강화 절차에 대한 자세한 내용은 엔티티 인증을 통해 제공된 이 제품에 대한 지침을 참조하십시오.

주의 이 설정을 활성화한 후에는 비활성화할 수 없습니다. 어플라이언스를 CC 또는 UCAPL 모드에서 해제해야 한다면, 이미지로 다시 설치해야 합니다.

보안 인증서 컴플라이언스 특성

다음 표에서는 CC 또는 UCAPL 모드를 활성화하는 경우 동작 변경에 대해 설명합니다. (로그인 계정에 대한 제한은 웹 인터페이스 액세스가 아닌 명령줄 액세스를 의미합니다.)

시스템 변경	**CC** 모드	**UCAPL** 모드
FIPS 컴플라이언스 활성화됨	예	예
시스템에서 백업 또는 보고서를 위한 원격 스토리지를 허용하지 않습니다.	예	예
시스템이 추가 시스템 감사 데몬을 시작합니다.	아니요	예
시스템 부트 로더가 보호됩니다.	아니요	예
시스템은 로그인 계정에 추가 보안을 적용합니다.	아니요	예
시스템은 재부팅 키 시퀀스 Ctrl-Alt-Del을 비활성화합니다.	아니요	예
시스템은 최대 10개의 동시 로그인 세션을 시행합니다.	아니요	예
시스템이 eStreamer를 사용하여 이벤트 데이터 내보내기를 지원하지 않습니다.	예	예
시스템은 로그인 계정에 대해 더 엄격한 보호 장치를 적용합니다. • 비밀번호는 대/소문자가 혼합된 영숫자 15자 이상이고 숫자를 하나 이상 포함해야 합니다. • 비밀번호는 사전에 나와 있는 단어를 사용할 수 없고 연속적으로 반복되는 문자를 포함할 수 없습니다. • 세 번 연속으로 로그인 시도에 실패한 후 시스템이 사용자를 잠금 처리합니다. 이 경우 관리자가 비밀번호를 재설정해야 합니다. • 시스템은 비밀번호 기록을 저장합니다.	아니요	예

시스템 변경	**Firepower Management Center**		클래식 관리 디바이스		**Firepower Threat Defense**	
	CC 모드	**UCAPL** 모드	**CC** 모드	**UCAPL** 모드	**CC** 모드	**UCAPL** 모드
FIPS 컴플라이언스 활성화됨	예	예	예	예	예	예
시스템에서 백업 또는 보고서를 위한 원격 스토리지를 허용하지 않습니다.	예	예	—	—	—	—
시스템은 버전 6.2.2.1 및 이후 6.2.2.x 패치에 대해서만 eStreamer를 사용하여 이벤트 데이터 내보내기를 지원합니다.	예	예	예	예	—	—
시스템이 추가 시스템 감사 데몬을 시작합니다.	아니요	예	아니요	예	아니요	아니요
시스템 부트 로더가 보호됩니다.	아니요	예	아니요	예	아니요	아니요
시스템은 로그인 계정에 추가 보안을 적용합니다.	아니요	예	아니요	예	아니요	아니요
시스템은 재부팅 키 시퀀스 Ctrl+Alt+Del을 비활성화합니다.	아니요	예	아니요	예	아니요	아니요
시스템은 최대 10개의 동시 로그인 세션을 시행합니다.	아니요	예	아니요	예	아니요	아니요
비밀번호는 대/소문자가 혼합된 영숫자 15자 이상이고 숫자를 하나 이상 포함해야 합니다.	아니요	예	아니요	예	아니요	아니요
로컬 관리자 CLI의 최소 필수 암호 길이는 로컬 장치 CLI를 사용하여 구성할 수 있습니다.	아니요	아니요	아니요	아니요	예	예
비밀번호는 사전에 나와 있는 단어를 사용할 수 없고 연속적으로 반복되는 문자를 포함할 수 없습니다.	아니요	예	아니요	예	아니요	아니요
세 번 연속으로 로그인 시도에 실패한 후 시스템이 관리자가 아닌 사용자를 잠금 처리합니다. 이 경우 관리자가 비밀번호를 재설정해야 합니다.	아니요	예	아니요	예	아니요	아니요
시스템은 기본적으로 비밀번호 기록을 저장합니다.	아니요	예	아니요	예	아니요	아니요
관리자는 웹 인터페이스를 통해 구성할 수 있는 최대 로그인 시도 실패 횟수가 초과된 후에 잠금 처리될 수 있습니다.	예	예	예	예	—	—

시스템 변경	**Firepower Management Center**		클래식 관리 디바이스		**Firepower Threat Defense**	
	CC 모드	**UCAPL** 모드	**CC** 모드	**UCAPL** 모드	**CC** 모드	**UCAPL** 모드
관리자는 로컬 어플라이언스 CLI를 통해 구성할 수 있는 최대 로그인 시도 실패 횟수가 초과된 후에 잠금 처리될 수 있습니다.	아니요	아니요	예, 보안 인증서 컴플라이언스 활성화 여부와 관계없습니다.	예, 보안 인증서 컴플라이언스 활성화 여부와 관계없습니다.	예	예
다음의 경우 시스템이 어플라이언스와 함께 SSH 세션을 자동으로 재설정합니다. • 세션 활동 1시간 동안 키가 사용된 후 • 연결을 통해 1GB의 데이터를 전송하는 데 키가 사용된 후	예	예	예	예	예	예
시스템은 부팅 시 FSIC(파일 시스템 무결성 검사)를 수행합니다. FSIC가 실패하면 Firepower 소프트웨어가 시작되지 않고 원격 SSH 액세스가 비활성화되며 로컬 콘솔을 통해서만 어플라이언스에 액세스할 수 있습니다. 이러한 현상이 발생하는 경우 Cisco TAC에 문의하십시오.	예	예	예	예	예	예

보안 인증서 컴플라이언스 추천

보안 인증서 컴플라이언스가 설정된 시스템을 사용하는 경우 다음 모범 사례를 준수하는 것이 좋습니다.

- 구축에서 보안 인증서 컴플라이언스를 활성화하려면 먼저 Firepower Management Center에서 보안 인증을 활성화한 다음 모든 매니지드 디바이스에서 동일한 모드로 활성화합니다.

  ⚠ 주의 Firepower Management Center는 둘 다 동일한 보안 인증서 컴플라이언스 모드에서 작동하지 않는 한 매니지드 디바이스에서 이벤트 데이터를 수신하지 않습니다.

- 모든 사용자에 대해 비밀번호 강도 검사를 활성화하고 인증 기관에 요구하는 값으로 최소 비밀번호 길이를 설정합니다.
- 고가용성 구성에서 Firepower Management Center를 사용하는 경우 동일한 보안 인증서 컴플라이언스 모드를 사용하도록 구성합니다.

- Firepower 4100/9300 섀시에서 Firepower Threat Defense가 CC 또는 UCAPL 모드에서 작동하도록 구성하는 경우 CC 모드에서 작동하도록 Firepower 4100/9300 섀시도 구성해야 합니다. 자세한 내용은 *Cisco FXOS Firepower Chassis Manager* 환경 설정 가이드를 참조하십시오.
- 다음 기능 중 하나를 사용하도록 시스템을 구성하지 마십시오.
  - 이메일 보고서, 알림 또는 데이터 정리 알림.
  - Nmap 스캔, Cisco IOS Null Route, 속성 값 설정 또는 ISE EPS 재조정
  - 백업 또는 보고서를 위한 원격 스토리지
  - 시스템 데이터베이스에 대한 타사 클라이언트 액세스
  - 이메일(SMTP), SNMP 트랩 또는 시스템 로그를 통해 전송되는 외부 알림 또는 경고
  - 어플라이언스와 서버 사이의 채널을 보호하기 위해 SSL 인증서를 사용하지 않고 HTTP 서버 또는 시스템 로그 서버로 전송된 감사 로그 메시지
  - eStreamer를 사용하여 이벤트 데이터를 외부 클라이언트로 내보내기
- 버전 6.1.0.6 및 후속 6.1.0.x 패치에 대해서만 eStreamer를 사용하여 이벤트 데이터를 외부 클라이언트로 내보내도록 시스템을 구성할 수 있습니다.
- 버전 6.2.2.1 및 후속 6.2.2.x 패치에 대해서만 eStreamer를 사용하여 이벤트 데이터를 외부 클라이언트로 내보내도록 시스템을 구성할 수 있습니다.
- CC 모드를 이용하는 구축에서는 LDAP 또는 RADIUS를 사용하여 외부 인증을 활성화하지 마십시오.
- CC 모드를 사용하는 구축에서는 CAC를 활성화하지 마십시오.
- CC 또는 UCAPL 모드를 사용하는 구축에서는 Firepower REST API를 통해 Firepower Management Center 및 매니지드 디바이스에 대한 액세스를 비활성화합니다.
- UCAPL 모드를 사용하는 구축에서 CAC를 활성화합니다.
- CC 모드를 사용하는 구축에서는 SSO를 설정하지 마십시오.
- 디바이스가 모두 동일한 보안 인증서 컴플라이언스 모드를 사용하지 않는 한 고가용성 쌍으로 Firepower Threat Defense 디바이스를 구성하지 마십시오.

참고 Firepower System은 스택 또는 고가용성 쌍의

- 스택 및 고가용성 쌍의 클래식 디바이스
- Firepower Threat Defense 클러스터의 디바이스
- Firepower Threat Defense 컨테이너 인스턴스: Firepower 4100/9300

어플라이언스 강화

Firepower 시스템을 더욱 강화할 수 있는 기능 관련 정보는 최신 버전 *Cisco Firepower Mangement Center* 강화 가이드와 *Cisco Firepower Threat Defense* 강화 가이드 및 이 문서의 다음 주제에서 확인할 수 있습니다.

- Firepower System 라이선싱
- Firepower System 사용자 인증FMC의 사용자 계정
- Firepower System에 로그인
- 감사 로그
- 감사 로그 인증서
- 시간 및 시간 동기화
- Threat Defense를 위한 NTP 시간 동기화 구성
- 이메일 알림 응답 생성
- 침입 이벤트에 대한 이메일 알림 설정
- SMTP 설정
- Firepower 1000/2100 시리즈용 SNMP 정보
- Threat Defense에 대한 SNMP 설정
- SNMP 알림 응답 생성
- 동적 DNS 구성
- DNS 캐시
- 시스템 감사
- 액세스 목록
- 보안 인증 컴플라이언스, 1 페이지
- 원격 스토리지에 대한 SSH 설정
- 감사 로그 인증서
- HTTPS 인증서
- 사용자 역할웹 인터페이스의 사용자 역할 맞춤화
- 사용자 계정내부 사용자 추가
- 세션 시간 초과
- 시스템 로그 구성 관련 정보
- FMC 백업 예약

- Site-to-Site VPN Firepower Threat Defense
- Remote Access VPN Firepower Threat Defense
- Firepower Threat Defense에 대한 FlexConfig 정책

네트워크 보호

네트워크 보호를 위해 구성 할 수 있는 Firepower System 기능에 대한 자세한 내용은 다음 주제를 참조하십시오.

- 액세스 제어 정책
- 보안 인텔리전스 차단 목록
- 침입 정책 시작하기
- 규칙을 사용하여 침입 정책 조정
- 침입 규칙 편집기
- 침입 규칙 업데이트
- 침입 이벤트 로깅 글로벌 제한
- 전송 및 네트워크 계층 전처리기
- 특정 위협 탐지
- 애플리케이션 레이어 프리프로세서
- IPS 디바이스 구축 및 구성
- 시스템 감사
- 침입 이벤트 작업
- 이벤트 검색
- 워크플로
- 디바이스 관리 기본 사항
- 로그인 배너
- 시스템 업데이트

보안 인증서 컴플라이언스 활성화

이 구성은 Firepower Management Center 또는 매니지드 디바이스에 적용됩니다.

- Firepower Management Center의 경우 이 구성은 시스템 구성에 포함되어 있습니다.

• 매니지드 디바이스의 경우, FMC의 이 구성을 플랫폼 설정 정책의 일부로 적용합니다.

두 경우 모두, 시스템 구성 변경 사항을 저장하거나 공유 플랫폼 설정 정책을 구축할 때까지 구성이 적용되지 않습니다.

⚠

주의 이 설정을 활성화한 후에는 비활성화할 수 없습니다. 어플라이언스를 CC 또는 UCAPL 모드에서 해제해야 한다면, 이미지로 다시 설치해야 합니다.

시작하기 전에

- Cisco에서는 모든 어플라이언스에서 보안 인증서 컴플라이언스를 활성화하기 전에 구축에 포함할 모든 디바이스를 FMC에 등록하는 방법을 권장합니다.
- Firepower Threat Defense 디바이스는 평가 라이선스를 사용할 수 없습니다. Cisco Smart Software Manager 계정에서 내보내기 제어 기능을 활성화해야 합니다.
- Firepower Threat Defense 디바이스는 라우팅 모드에서 구축해야 합니다.
- 이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** FMC 또는 매니지드 디바이스 중 무엇을 구성하는지에 따라 다음 작업을 수행합니다.

- FMC: **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.
- 클래식 디바이스: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**을(를) 선택하고 Firepower 정책을 생성하거나 수정합니다.
- FTD 디바이스: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**을(를) 선택하고 Firepower Threat Defense 정책을 생성하거나 수정합니다.

단계 **2** **UCAPL/CC Compliance(UCAPL/CC** 규정준수**)**를 클릭합니다.

참고 UCAPL 또는 CC 컴플라이언스를 활성화하면 어플라이언스가 재부팅됩니다. 시스템 구성을 저장할 때 FMC가 재부팅됩니다. 매니지드 디바이스는 구성 변경 사항을 구축할 때 재부팅됩니다.

단계 **3** 어플라이언스에서 보안 인증서 컴플라이언스를 영구적으로 활성화하려면 다음 두 가지 중에서 선택할 수 있습니다.

- Common Criteria 모드에서 보안 인증서 컴플라이언스를 활성화하려면 드롭다운 목록에서 **CC**를 선택합니다.
- Unified Capabilities Approved Products List 모드에서 보안 인증서 컴플라이언스를 활성화하려면 드롭다운 목록에서 **UCAPL**을 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 아직 수행하지 않았다면 구축의 모든 클래식 디바이스에 제어 및 보호 라이선스를 적용합니다.
- 인증 엔티티가 제공한 이 제품의 지침에 설명된 대로 추가 구성 변경을 설정합니다.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.