보안 인증서 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. Secure Firewall 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	**Secure Firewall Management Center**		클래식 관리 디바이스		**Secure Firewall 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	—	—	—	—
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

시스템 변경	**Secure Firewall Management Center**		클래식 관리 디바이스		**Secure Firewall Threat Defense**	
	CC 모드	**UCAPL** 모드	**CC** 모드	**UCAPL** 모드	**CC** 모드	**UCAPL** 모드
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	—	—
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 Secure Firewall Management Center에서 보안 인증을 활성화한 다음 모든 매니지드 디바이스에서 동일한 모드로 활성화합니다.

주의 Secure Firewall 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 Secure Firewall Management Center를 사용하는 경우 동일한 보안 인증서 컴플라이언스 모드를 사용하도록 구성합니다.
- Firepower 4100/9300에서 Secure Firewall Threat Defense가 CC 또는 UCAPL 모드에서 작동하도록 구성하는 경우 CC 모드에서 작동하도록 Firepower 4100/9300도 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
- 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 Secure Firewall 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 Secure Firewall Threat Defense 디바이스를 구성하지 마십시오.

참고 Firepower System은 다음에 대해 CC 또는 UCAPL 모드를 지원하지 않습니다.

- Secure Firewall Threat Defense 클러스터의 디바이스
- Secure Firewall Threat Defense 컨테이너 인스턴스: Firepower 4100/9300

어플라이언스 강화

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

- 라이선스
- Management Center의
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *Threat Defense*를 위한 *NTP* 시간 동기화 구성
- 이메일 알림 응답 생성
- 침입 이벤트에 대한 이메일 알림 설정
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *SMTP* 구성
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *Firepower 1000/2100* 시리즈용 *SNMP* 정보
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *SNMP* 구성
- SNMP 알림 응답 생성
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 동적 *DNS* 구성
- 보안 인증서 컴플라이언스, 1 페이지
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 시스템 로그 구성 관련 정보
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 사이트 간 *VPNThreat Defense*
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 원격 액세스 *VPN*
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *FlexConfig* 정책

네트워크 보호

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

- 액세스 제어 정책
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 보안 인텔리전스
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 침입 정책 시작하기
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 규칙을 사용하여 침입 정책 조정
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 맞춤형 침입 규칙
- 침입 규칙 업데이트

- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 침입 이벤트 로깅에 대한 글로벌 제한
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 전송 및 네트워크 레이어 전처리기
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 특정 위협 탐지
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 애플리케이션 레이어 프리프로세서
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 디바이스 관리
- 업데이트