Cisco Secure Firewall Device Manager의 릴리스별 새로운 기능

초판: 2021년 1월 19일

최종 변경: 2024년 1월 17일

릴리스별 새로운 기능

이 문서에서는 업그레이드 영향을 포함하여 각 릴리스의 새로운 기능과 사용되지 않는 기능에 대해 설명합니다.

업그레이드 및 구축으로 인해 사용자가 다른 조치를 취하지 않아도 시스템이 트래픽을 처리하거나 다른 방식으로 작동하는 경우 기능에 업그레이드 영향이 있습니다. 이러한 현상은 새로운 위협 탐지 및 애플리케이션 식별 기능에서 특히 흔히 볼 수 있습니다. 또는 업그레이드 프로세스에 특별한 요구 사항이 있는 경우도 있습니다. 예를 들어, 경우에 따라 업그레이드 전후에 비표준 작업을 수행해야 합니다(특정 구성 편집 또는 삭제, 상태 정책 적용, 웹 인터페이스에서 FlexConfig 명령 다시 실행 등).

버전별 Snort 개선 사항에 대한 자세한 내용은 Management Center가 device manager보다 더 구성 가능한 옵션을 제공할 수 있다는 점을 참고하십시오. Cisco Secure Firewall Management Center의 릴리스별 새로운 기능을 참조하십시오. Snort는 device manager 또는 Management Center를 사용하는지 여부에 관계없이 threat defense에 대한 기본 검사 엔진입니다.

영어 이외의 언어로 된 웹 인터페이스를 사용하는 경우에는 다음 주요 릴리스까지 유지 보수 릴리스 및 패치에 도입된 기능이 번역되지 않을 수 있습니다.

제안된 릴리스

제안된 릴리스: 버전 **7.2.5.x**

새로운 기능과 해결된 문제를 사용하려면 적격한 모든 어플라이언스를 최신 패치를 포함하여 제안된 릴리스 이상으로 업그레이드하는 것이 좋습니다. Cisco 지원 및 다운로드 사이트에서 제안된 릴리스에는 금색 별표가 표시되어 있습니다. 버전 /7.4.1 이상의 경우, 새로운 제안된 릴리스를 사용할 수 있으면 Management Center가 알림을 보내고 제품 업그레이드 페이지에 제안된 릴리스가 표시됩니다.

기존 어플라이언스의 제안된 릴리스

어플라이언스가 너무 오래되어 제안된 릴리스를 실행할 수 없는데 지금 당장 하드웨어를 새로 고칠 계획이 없는 경우 주요 버전을 선택한 다음 가능하다면 패치를 적용합니다. 일부 주요 버전은 장기 또는 초장기로 지정되므로, 이 중 하나를 고려하십시오. 자세한 용어 설명은 Cisco NGFW 제품 라인 소프트웨어 출시 및 유지보수 게시판의 내용을 참조하십시오.

하드웨어를 갱신하고 싶다면 Cisco 담당자 또는 파트너 담당자에게 문의하십시오.

Device Manager 버전 7.4의 새로운 기능

참고 버전 7.4 기능에 대한 Device Manager 지원은 버전 7.4.1부터 지원됩니다. 이는 Device Manager를 지원하는 플랫폼에서 버전 7.4.0을 사용할 수 없기 때문입니다.

표 *1: Device Manager* 버전 *7.4.1*의 새로운 기능 및 사용 중지된 기능

기능	설명
플랫폼 기능	
Firepower 1010E 지원 반환.	버전 7.2.3에서 도입되었으며 버전 7.3에서 일시적으로 사용이 중단된 Firepower 1010E에 대한 지원이 재개됩니다. 참조: Firepower 1010 케이블 연결
Secure Firewall 3130 및 3140용 네트워크 모듈	이러한 네트워크 모듈을 Secure Firewall 3130 및 3140에 도입했습니다. • 2포트 100G QSFP+ 네트워크 모듈(FPR3K-XNM-2X100G) 참조: Cisco Secure Firewall 3110, 3120, 3130 및 3140 하드웨어 설치 설명서
VPN 기능	
Secure Firewall 3100에 대한 VTI 루프백 인터페이스의 IPsec 플로우 오프로드	업그레이드 영향. 적격 연결이 오프로드되기 시작합니다. Secure Firewall 3100에서는 VTI 루프백 인터페이스를 통한 IPsec 연결이 기본적으로 오프로드됩니다. 이전에는 이 기능이 물리적 인터페이스에서만 지원되었습니다. 이 기능은 업그레이드를 통해 자동으로 활성화됩니다. FlexConfig 및 **flow-offload-ipsec** 명령을 사용하여 구성을 변경할 수 있습니다.
인터페이스 기능	

기능	설명
관리 및 진단 인터페이스 병합.	업그레이드 영향. 업그레이드 후 인터페이스를 병합합니다. 7.4 이상 버전을 사용하는 새 디바이스의 경우 레거시 진단 인터페이스를 사용할 수 없습니다. 병합된 관리 인터페이스만 사용할 수 있습니다. 7.4 이상으로 업그레이드했고 진단 인터페이스에 대한 설정이 없는 경우 인터페이스가 자동으로 병합됩니다. 7.4 이상으로 업그레이드했고 진단 인터페이스에 대한 설정이 있는 경우 인터페이스를 수동으로 병합하거나 별도의 진단 인터페이스를 계속 사용할 수 있습니다. 진단 인터페이스에 대한 지원은 이후 릴리스에서 제거되므로 가능한 빨리 인터페이스를 병합해야 합니다. 병합 모드는 기본적으로 데이터 라우팅 테이블을 사용하도록 AAA 트래픽의 동작을 변경합니다. 관리 전용 라우팅 테이블은 설정에서 관리 전용 인터페이스(관리 포함)를 지정한 경우에만 사용할 수 있습니다. 신규/수정된 화면: • **Devices(**디바이스**)** > **Interfaces(**인터페이스**)** > **Management(**관리**)** 인터페이스 • (인터페이스로 이동) **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)** • **Devices(**디바이스**)** > **Interfaces(**인터페이스**)** > **Merge Interface action needed(**병합 인터페이스 작업 필요**)** > **Management Interface Merge(**관리 인터페이스 병합**)** 신규/수정된 명령: **show management-interface convergence**
Azure 및 GCP에 대해 Threat Defense Virtual에서 진단 인터페이스 없이 구축.	이제 Azure 및 GCP에 대해 Threat Defense Virtual에서 진단 인터페이스 없이 구축할 수 있습니다. Azure 구축에는 여전히 두 개 이상의 데이터 인터페이스가 필요하지만, GCP에서는 진단 인터페이스를 데이터 인터페이스로 교체해야 하며 최소 3개 이상의 새 인터페이스가 필요합니다. (이전에는 Threat Defense Virtual 구축에 하나의 관리 인터페이스, 하나의 진단 인터페이스 및 최소 2개의 데이터 인터페이스가 필요했습니다.) 제한: 이 기능은 새 구축에만 지원됩니다. 업그레이드된 디바이스에서는 지원되지 않습니다. 참조: Cisco Secure Firewall Threat Defense Virtual 시작 가이드
Firepower 1000 Series, Firepower 2100, Secure Firewall 3100에 대한 인라인 집합.	Firepower 1000 Series, Firepower 2100, Secure Firewall 3100 디바이스에 대한 인라인 집합을 구성할 수 있습니다. Interface(인터페이스) 페이지에 인라인 집합 탭이 추가되었습니다.

기능	설명
라이선싱 기능	
라이선스 이름 변경 및 캐리어 라이선스 지원.	라이선스 이름이 변경되었습니다. • 위협은 이제 IPS입니다. • 악성코드는 이제 악성코드 방어입니다 • 기본은 이제 필수입니다 • AnyConnect Apex는 이제 Secure Client Premier입니다 • AnyConnect Plus는 이제 Secure Client Advantage입니다 • AnyConnect VPN Only는 이제 Secure Client VPN Only입니다 또한 이제 캐리어 라이선스를 적용하여 GTP/GPRS, Diameter, SCTP 및 M3UA 검사를 구성할 수 있습니다. FlexConfig를 사용하여 이러한 기능을 구성합니다. 참조: 시스템 라이선싱
관리 및 트러블슈팅 기능	
기본 NTP 서버 업데이트.	업그레이드 영향. 시스템이 새 리소스에 연결됩니다. 기본 NTP 서버가 sourcefire.pool.ntp.org에서 time.cisco.com으로 변경되었습니다. 다른 NTP 서버를 사용하려면 **Device**(디바이스)를 선택하고 **System Settings**(시스템 설정) 패널에서 **Time Services**(시간 서비스)를 클릭합니다.
HTTPS 관리 사용자 액세스를 위한 SAML 서버.	HTTPS 관리 액세스를 위해 외부 인증을 제공하도록 SAML 서버를 구성할 수 있습니다. 관리자, 감사 관리자, 암호화 관리자, 읽기-쓰기 사용자, 읽기 전용 사용자 유형의 권한 부여 액세스 유형을 가진 외부 사용자를 구성할 수 있습니다. SAML 서버를 사용하는 경우 로그인에 CAC(Common Access Card)를 사용할 수 있습니다. SAML ID 소스 개체 구성 및 **System Settings**(시스템 설정) > **Management Access**(관리 액세스) 페이지에서 이를 수락하도록 업데이트되었습니다.
Threat Defense 고가용성 쌍에서 구성 불일치 탐지.	이제 CLI를 사용하여 Threat Defense 고가용성 쌍에서 구성 불일치를 탐지할 수 있습니다. 신규/수정된 CLI 명령: **show failover config-sync error**, **show failover config-sync stats** 참조: Cisco Secure Firewall Threat Defense 명령 참조

기능	설명
Secure Firewall 3100으로 삭제된 패킷 캡처.	MAC 주소 테이블 불일치로 인한 패킷 손실은 디버깅 기능에 영향을 줄 수 있습니다. Secure Firewall 3100에서 이제 삭제된 패킷을 캡처할 수 있습니다. 신규/수정된 CLI 명령: **capture** 명령의 [**drop** { **disable** | **mac-filter** }]. 참조: Cisco Secure Firewall Threat Defense 명령 참조
FXOS 업그레이드에 포함되는 펌웨어 업그레이드.	섀시/**FXOS** 업그레이드 영향**.** 펌웨어 업그레이드로 인해 추가 재부팅이 발생합니다**.** Firepower 4100/9300의 경우, 이제 버전 2.14.1로의 FXOS 업그레이드에는 펌웨어 업그레이드가 포함됩니다. 디바이스의 펌웨어 구성 요소가 FXOS 번들에 포함된 것보다 오래된 경우, FXOS 업그레이드 시 펌웨어도 업데이트됩니다. 펌웨어가 업그레이드되면 디바이스가 두 번(FXOS용으로 한 번, 펌웨어용으로 한 번) 재부팅됩니다. 소프트웨어 및 운영 체제를 업그레이드할 때와 마찬가지로 펌웨어 업그레이드 중에는 구성을 변경하거나 구축하지 마십시오. 시스템이 비활성 상태로 나타나더라도 펌웨어 업그레이드 중에 수동으로 재부팅하거나 종료하지 마십시오. 참조: Cisco Firepower 4100/9300 업그레이드 가이드
Firepower 1000/2100 및 Firepower 4100/9300의 데이터 플레인 장애 후 빠른 복구.	Firepower 1000/2100 또는 Firepower 4100/9300의 데이터 플레인 프로세스가 충돌하면 시스템이 디바이스를 재부팅하는 대신 프로세스를 다시 로드합니다. 데이터 플레인을 다시 로드하면 Snort를 비롯한 다른 프로세스도 재시작됩니다. 부팅 중에 데이터 플레인이 충돌하면 디바이스는 일반 다시 로드/재부팅 시퀀스를 따릅니다. 이렇게 하면 다시 로드 루프를 방지할 수 있습니다. 이 기능은 새 디바이스 및 업그레이드된 디바이스 모두에서 기본적으로 활성화됩니다. 비활성화하려면 FlexConfig를 사용하십시오. 신규/수정된 ASA CLI 명령: **data-plane quick-reload**, **show data-plane quick-reload status** 신규/수정된 Threat Defense CLI 명령: **show data-plane quick-reload status** 지원되는 플랫폼: Firepower 1000/2100, Firepower 4100/9300 참조: Cisco Secure Firewall Threat Defense 명령 참조 및 Cisco Secure Firewall ASA Series 명령 참조.

Device Manager 버전 7.3의 새로운 기능

버전별 Snort 개선 사항에 대한 자세한 내용은 Management Center가 device manager보다 더 구성 가능한 옵션을 제공할 수 있다는 점을 참고하십시오. Cisco Secure Firewall Management Center의 릴리스별 새로운 기능을 참조하십시오. Snort는 device manager 또는 Management Center를 사용하는지 여부에 관계없이 threat defense에 대한 기본 검사 엔진입니다.

표 *2: Device Manager* 버전 *7.3*의 새로운 기능 및 사용 중지된 기능

기능	설명
플랫폼 기능	
Secure Firewall 3105.	Secure Firewall 3105를 도입했습니다. 최소 위협 방어: 버전 7.3.1
Secure Firewall 4100용 네트워크 모듈	Firepower 4100용으로 다음 네트워크 모듈을 도입했습니다. • 2포트 100G 네트워크 모듈(FPR4K-NM-2X100G) 지원되는 플랫폼: Firepower 4112, 4115, 4125, 4145
종료를 위한 ISA 3000 시스템 LED 지원	이 기능에 대한 지원 반환 ISA 3000을 종료하면 시스템 LED가 꺼집니다. 그런 다음 디바이스에서 전원을 제거하기 전에 10초 이상 기다립니다. 이 기능은 버전 7.0.5에서 도입되었지만 버전 7.1–7.2에서 일시적으로 사용이 중단되었습니다.
위협 방어 가상 및 OCI용의 새로운 컴퓨팅 환경.	OCI용 위협 방어 가상은 다음 컴퓨팅 환경에 대한 지원을 추가합니다. • Intel VM.DenseIO2.8 • Intel VM.StandardB1.4 • Intel VM.StandardB1.8 • Intel VM.Standard 1.4 • Intel VM.Standard1.8 • Intel VM.Standard3.Flex • Intel VM.Optimized3.Flex • AMD VM.Standard.E4.Flex VM.Standard2.4 및 VM.Standard2.8 컴퓨팅 환경은 2022년 2월에 주문 가능 여부가 종료되었습니다. 버전 7.3 이상을 배포하는 경우 다른 컴퓨팅 구성을 권장합니다. 참조: Cisco Secure Firewall Threat Defense Virtual 시작 가이드

기능	설명
지원 종료: Firepower 4110, 4120, 4140, 4150	Firepower 4110, 4120, 4140 또는 4150에서는 버전 7.3 이상을 실행할 수 없습니다.
지원 종료: Firepower 9300: SM-24, SM-36, SM-44 모듈	SM-24, SM-36 또는 SM-44 모듈이 있는 Firepower 9300에서는 버전 7.3 이상을 실행할 수 없습니다.
Firepower 1010E는 지원되지 않음(임시).	버전 7.2.3에서 도입된 Firepower 1010E는 버전 7.3을 지원하지 않습니다. 버전 7.4에서는 지원이 반환됩니다. 버전 7.2.x Firepower 1010E를 버전 7.3으로 업그레이드할 수 없으며, 버전 7.3에서도 리이미징해서는 안 됩니다. 버전 7.3을 실행하는 Firepower 1010E 디바이스가 있는 경우 지원되는 릴리스로 이미지 재설치합니다.
방화벽 및 **IPS** 기능	
SSL 암호 해독 정책의 TLS 1.3 지원 및 암호 해독 불가 연결에 대한 구성 가능한 동작.	업그레이드 영향**.** TLS 1.3 트래픽에 대한 SSL 암호 해독 규칙을 구성합니다. TLS 1.3 지원은 Snort 3을 사용하는 경우에만 사용할 수 있습니다. 해독 불가 연결에 대해 기본이 아닌 동작을 구성할 수도 있습니다. Snort 3을 사용하는 경우 업그레이드 시 모든 SSL/TLS 버전이 선택된 규칙에 대해 TLS 1.3이 자동으로 선택됩니다. 그렇지 않으면 TLS 1.3이 선택되지 않습니다. Snort 2에서 Snort 3으로 전환하는 경우에도 동일한 동작이 발생합니다. 규칙 추가/수정 대화 상자의 고급 탭에서 TLS 1.3을 옵션으로 추가했습니다. 또한 TLS 1.3 암호 해독을 활성화하고 암호 해독할 수 없는 연결 작업을 구성하는 기능을 포함하도록 SSL 암호 해독 정책 설정을 재설계했습니다. 참조: SSL 암호 해독 규칙에 대한 고급 기준 및 고급 및 암호 해독 불가 트래픽 구성
구체화된 URL 필터링 조회.	이제 URL 필터링 조회가 발생하는 방식을 명시적으로 설정할 수 있습니다. 로컬 URL 데이터베이스만 사용하거나, 로컬 데이터베이스와 클라우드 조회를 모두 사용하거나, 클라우드 조회만 사용하도록 선택할 수 있습니다. URL 필터링 시스템 설정 옵션을 보강했습니다. 참조: URL 필터링 기본 설정 구성
인터페이스 기능	

기능	설명
가상 어플라이언스에 대한 IPv6 지원.	위협 방어 가상은 이제 다음 환경에서 IPv6를 지원합니다. • AWS • Azure • KVM • VMWare 참조: Cisco Secure Firewall Threat Defense Virtual 시작 가이드
DHCPv6 클라이언트.	이제 DHCPv6에서 IPv6 주소를 가져올 수 있습니다. 신규/수정된 화면: **Device(**디바이스**)** > **Interfaces(**인터페이스**)** > **Edit Interface(**인터페이스 편집**)** > **Advanced(**고급**)** 참조: 고급 인터페이스 옵션 구성
관리 및 트러블슈팅 기능	
CA 번들을 자동으로 업데이트.	업그레이드 영향**.** 시스템은 새로운 것을 위해 **Cisco**에 연결합니다**.** 로컬 CA 번들에는 여러 Cisco 서비스에 액세스하기 위한 인증서가 포함되어 있습니다. 이제 시스템은 매일 시스템 정의 시간에 새 CA 인증서를 자동으로 쿼리합니다. 이전에는 CA 인증서를 업데이트하려면 소프트웨어를 업그레이드해야 했습니다. CLI를 사용하여 이 기능을 비활성화할 수 있습니다. 신규/수정된 CLI 명령: **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** 버전 제한: 이 기능은 버전 7.0.5 이상, 7.1.0.3 이상 및 7.2.4 이상에 포함되어 있습니다. 7.0, 7.1 또는 7.2 이전 릴리스에서는 지원되지 않습니다. 지원되는 버전에서 지원되지 않는 버전으로 업그레이드하면 해당 기능이 일시적으로 비활성화되고 시스템에서 Cisco와의 연결이 중지됩니다. 참조: Cisco Secure Firewall Threat Defense 명령 참조
신뢰할 수 있는 인증서에 대한 인증 기관 확인을 건너뜀.	로컬 CA 인증서를 신뢰할 수 있는 CA 인증서로 설치해야 하는 경우 확인을 건너뛸 수 있습니다. 신뢰할 수 있는 CA 인증서를 업로드할 때 **Skip CA Certificate Check(CA** 인증서 확인 건너뛰기**)** 옵션을 추가했습니다.

기능	설명
Secure Firewall 3100용 통합 업그레이드 및 설치 패키지.	

기능	설명
	이미지 재설치 영향. 버전 7.3에서는 다음과 같이 Secure Firewall 3100에 대한 위협 방어 설치 및 업그레이드 패키지를 통합했습니다. • 버전 7.1–7.2 설치 패키지: cisco-ftd-fp3k.*version*.SPA • 버전 7.1–7.2 업그레이드 패키지: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar • 버전 7.3 이상 통합 패키지: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar 문제 없이 위협 방어를 업그레이드할 수 있지만, 이전 위협 방어 및 ASA 버전에서 직접 위협 방어 버전 7.3 이상으로 이미지 재설치할 수는 없습니다. 이는 새 이미지 유형에 필요한 ROMMON 업데이트 때문입니다. 이러한 이전 버전에서 이미지를 재설치하려면 이전 ROMMON에서 지원되지만 새 ROMMON으로 업데이트되는 ASA 9.19 이상을 "처리"해야 합니다. 별도의 ROMMON 업데이터는 없습니다. 위협 방어 버전 7.3 이상을 사용하기 위한 옵션은 다음과 같습니다. • Threat Defense 버전 7.1 또는 7.2에서 업그레이드 - 일반 업그레이드 프로세스를 사용합니다. 해당 업그레이드 가이드를 참조하십시오. • Threat Defense 버전 7.1 또는 7.2에서 이미지 재설치 - 먼저 ASA 9.19 이상으로 이미지 재설치한 다음 Threat Defense 버전 7.3 이상으로 이미지 재설치. Cisco Secure Firewall ASA 및 Secure Firewall Threat Defense 이미지 재설치 가이드에서 *Threat Defense(*위협 방어*)→ASA: Firepower 1000, 2100; Secure Firewall 3100* 및 *ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode(Firepower 1000, 2100* 어플라이언스 모드*) Secure Firewall 3100*을 참조하십시오. • ASA 9.17 또는 9.18에서 이미지 재설치 - ASA 9.19 이상으로 먼저 업그레이드한 다음 Threat Defense 버전 7.3 이상으로 이미지 재설치. Cisco Secure Firewall ASA 업그레이드 가이드를 참조한 다음 Cisco Secure Firewall ASA 및 Secure Firewall Threat Defense 이미지 재설치 가이드에서 *ASA→*위협 방어*: Firepower 1000, 2100* 어플라이언스 모드*, Secure Firewall 3100*을 참조하십시오. • 위협 방어 버전 7.3 이상에서 이미지 재설치 - 일반 이미지 재

기능	설명
	설치 프로세스를 사용합니다. Firepower Threat Defense를 사용하는 Firepower 1000/2100 및 Secure Firewall 3100/4200용 Cisco FXOS 문제 해결 가이드에서 새 소프트웨어 버전으로 시스템 이미지 재설치를 참조하십시오.
Threat Defense REST API 버전 6.4(v6).	소프트웨어 버전 7.3의 위협 방어 REST API는 버전 6.4입니다. API URL의 v6를 사용하거나 /latest/를 사용하여 디바이스에서 지원되는 가장 최신 API 버전을 사용하고 있음을 나타내는 것이 좋습니다. 6.4의 URL 버전 경로 요소는 다른 6.x과 동일한 v6입니다. 사용 중인 리소스 모델에 변경 사항이 적용되었을 수 있으므로 모든 기존 호출을 다시 평가하십시오. 리소스를 확인할 수 있는 API Explorer를 열려면 device manager에 로그인한 다음, More options(추가 옵션) 버튼( )을 클릭하고 **API Explorer**를 선택합니다. 참조: Cisco Secure Firewall Threat Defense REST API 가이드

Device Manager 버전 7.2의 새로운 기능

표 *3: Device Manager* 버전 *7.2*의 새로운 기능 및 사용 중지된 기능

기능	설명
플랫폼 기능	
Firepower 1010E.	PoE(power over Ethernet)를 지원하지 않는 Firepower 1010E가 도입되었습니다. 최소 위협 방어: 7.2.3 참조: Firepower 1010 케이블 연결
Threat Defense Virtual for GCP.	이제 디바이스 관리자를 사용하여 GCP에 대한 위협 방어 가상을 구성할 수 있습니다. 참조: Cisco Secure Firewall Threat Defense Virtual 시작 가이드

기능	설명
Secure Firewall 3100용 네트워크 모듈.	Secure Firewall 3100에 대해 다음과 같은 네트워크 모듈을 도입했습니다. • 6포트 1G SFP 네트워크 모듈, SX(다중 모드)(FPR-X-NM-6X1SX-F) • 6포트 10G SFP 네트워크 모듈, SR(다중 모드)(FPR-X-NM-6X10SR-F) • 6포트 10G SFP 네트워크 모듈, LR(단일 모드)(FPR-X-NM-6X10LR-F) • 6포트 25G SFP 네트워크 모듈, SR(다중 모드)(FPR-X-NM-X25SR-F) • 6포트 25G 네트워크 모듈, LR(단일 모드)(FPR-X-NM-6X25LR-F) • 8포트 1G 구리 네트워크 모듈, RJ45(구리)(FPR-X-NM-8X1G-F) 최소 위협 방어: 7.2.1
KVM용 위협 방어 가상을 사용하는 Intel 이더넷 네트워크 어댑터 E810-CQDA2 드라이버.	이제 KVM용 위협 방어 가상을 사용하여 Intel 이더넷 네트워크 어댑터 E810-CQDA2 드라이버를 지원합니다. 최소 위협 방어: 7.2.1 참조: KVM에서 Threat Defense Virtual 구축
ISA 3000 종료 지원.	ISA 3000 종료에 대한 반환을 지원합니다. 이 기능은 버전 7.0.2에서 도입되었지만 버전 7.1에서 일시적으로 사용이 중단되었습니다.
방화벽 및 **IPS** 기능	
개체 그룹 검색은 액세스 제어에 대해 기본적으로 활성화되어 있음.	이제 새 구축에 대해 CLI 구성 명령 **object-group-search access-control**이 기본적으로 활성화됩니다. FlexConfig를 사용하여 명령을 구성하는 경우 해당 명령이 여전히 필요한지 여부를 평가해야 합니다. 기능을 비활성화해야 하는 경우 FlexConfig를 사용하여 **no object-group-search access-control** 명령을 구현합니다. 참조: Cisco Secure Firewall ASA Series 명령 참조

기능	설명
규칙 적중 횟수는 재부팅 후에도 유지됨.	디바이스를 재부팅해도 더 이상 액세스 제어 규칙 적중 횟수가 0으로 재설정되지 않습니다. 적중 횟수는 카운터를 직접 지우는 경우에만 재설정됩니다. 또한 개수는 HA 쌍 또는 클러스터의 각 유닛에서 개별적으로 유지 관리됩니다. **show rule hits** 명령을 사용하여 HA 쌍 또는 클러스터 전체에서 누적 카운터를 보거나 노드당 카운트를 확인할 수 있습니다. 다음 위협 방어 CLI 명령 **show rule hits**를 수정했습니다. 참조: 규칙 적중 횟수 검토
VPN 기능	
IPsec 플로우 오프로드.	Secure Firewall 3100에서 IPsec 플로우는 기본적으로 오프로드됩니다. IPsec 사이트 간 VPN 또는 원격 액세스 VPN 보안 연계(SA)의 초기 설정 후 IPsec 연결은 디바이스의 FTPA(field-programmable gate Array)로 오프로드되므로 디바이스 성능이 향상됩니다. FlexConfig 및 **flow-offload-ipsec** 명령을 사용하여 구성을 변경할 수 있습니다. 참조: IPsec 플로우 오프로드
인터페이스 기능	
Secure Firewall 3130 및 3140에 대한 브레이크아웃 포트 지원.	이제 Secure Firewall 3130 및 3140에서 각 40GB 인터페이스에 대해 10GB 브레이크아웃 포트 4개를 구성할 수 있습니다. 신규/수정 화면: **Device(**디바이스**)** > **Interfaces(**인터페이스**)** 참조: Secure Firewall 3100용 네트워크 모듈 관리
인터페이스에서 Cisco Trustsec 활성화 또는 비활성화.	물리적, 하위 인터페이스, EtherChannel, VLAN, 관리 또는 BVI 인터페이스(명명 여부에 관계없이)에서 Cisco Trustsec을 활성화하거나 비활성화할 수 있습니다. 기본적으로 Cisco Trustsec은 인터페이스의 이름을 지정할 때 자동으로 활성화됩니다. **Propagate Security Group Tag(**보안 그룹 태그 전파**)** 속성을 인터페이스 구성 대화 상자에 추가하고 **ctsEnabled** 속성을 다양한 인터페이스 API에 추가했습니다. 참조: 고급 옵션 구성
라이선싱 기능	
ISA 3000 영구 라이선스 예약 지원.	이제 ISA 3000은 승인된 고객에 대해 범용 영구 라이선스 예약을 지원합니다. 참조: 에어 갭(Air-Gapped) 네트워크에서 영구 라이선스 적용
관리 및 트러블슈팅 기능	

기능	설명
전체 구축을 강제 실행하는 기능 지원.	변경 사항을 구축할 때 시스템은 일반적으로 마지막 구축 이후의 변경 사항만 구축합니다. 그러나 문제가 발생하는 경우 전체 구축을 강제로 선택하여 디바이스의 구성을 완전히 새로 고칠 수 있습니다. 구축 대화 상자에 **Apply Full Deployment(**전체 구축 적용**)** 옵션을 추가했습니다. 참조: 변경 사항 구축
CA 번들을 자동으로 업데이트.	업그레이드 영향**.** 시스템은 새로운 것을 위해 **Cisco**에 연결합니다**.** 로컬 CA 번들에는 여러 Cisco 서비스에 액세스하기 위한 인증서가 포함되어 있습니다. 이제 시스템은 매일 시스템 정의 시간에 새 CA 인증서를 자동으로 쿼리합니다. 이전에는 CA 인증서를 업데이트하려면 소프트웨어를 업그레이드해야 했습니다. CLI를 사용하여 이 기능을 비활성화할 수 있습니다. 신규/수정된 CLI 명령: **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** 버전 제한: 이 기능은 버전 7.0.5 이상, 7.1.0.3 이상 및 7.2.4 이상에 포함되어 있습니다. 7.0, 7.1 또는 7.2 이전 릴리스에서는 지원되지 않습니다. 지원되는 버전에서 지원되지 않는 버전으로 업그레이드하면 해당 기능이 일시적으로 비활성화되고 시스템에서 Cisco와의 연결이 중지됩니다. 참조: Cisco Secure Firewall Threat Defense 명령 참조
Threat defense REST API 버전 6.3(v6).	소프트웨어 버전 7.2의 위협 방어 REST API는 버전 6.3입니다. API URL의 v6를 사용하거나 /latest/를 사용하여 디바이스에서 지원되는 가장 최신 API 버전을 사용하고 있음을 나타내는 것이 좋습니다. 6.3의 URL 버전 경로 요소는 6.0, 6.1, 6.2와 동일한 v6입니다. 사용 중인 리소스 모델에 변경 사항이 적용되었을 수 있으므로 모든 기존 호출을 다시 평가하십시오. 리소스를 확인할 수 있는 API Explorer를 열려면 device manager에 로그인한 다음, More options(추가 옵션) 버튼( )을 클릭하고 **API Explorer**를 선택합니다. 참조: Cisco Secure Firewall Threat Defense REST API 가이드

FDM 버전 7.1의 새로운 기능

표 *4: FDM* 버전 *7.1*의 새로운 기능 및 사용 중단된 기능

기능	설명
플랫폼 기능	

기능	설명
Secure Firewall 3100.	Secure Firewall 3110, 3120, 3130, 3140을 도입했습니다. 재부팅할 필요 없이 방화벽의 전원이 켜져 있는 동안 동일한 유형의 네트워크 모듈을 핫 스왑할 수 있습니다. 다른 모듈을 변경하려면 재부팅해야 합니다. 보안 방화벽 3100 25Gbps 인터페이스는 착신 전환 오류 수정 및 설치된 SFP를 기반으로 하는 속도 탐지를 지원합니다. SSD는 SED(자체 암호화 드라이브)이며, 2개의 SSD가 있는 경우 소프트웨어 RAID를 구성합니다. 버전 7.1 디바이스 관리자에는 이러한 디바이스에 대한 온라인 도움말이 포함되어 있지 않습니다. Cisco.com에 게시된 설명서를 참조하십시오. 신규/수정 화면: **Device(**디바이스**)** > **Interfaces(**인터페이스**)** 신규/수정된 위협 방어 명령: **configure network speed, configure raid, show raid, show ssd**

기능	설명
AWS 인스턴스용 FTDv.	AWS용 FTDv는 다음 인스턴스에 대한 지원을 추가합니다. • c5a.xlarge, c5a.2xlarge, c5a.4xlarge • c5ad.xlarge, c5ad.2xlarge, c5ad.4xlarge • c5d.xlarge, c5d.2xlarge, c5d.4xlarge • c5n.xlarge, c5n.2xlarge, c5n.4xlarge • i3en.xlarge, i3en.2xlarge, i3en.3xlarge • inf1.xlarge, inf1.2xlarge • m5.xlarge, m5.2xlarge, m5.4xlarge • m5a.xlarge, m5a.2xlarge, m5a.4xlarge • m5ad.xlarge, m5ad.2xlarge, m5ad.4xlarge • m5d.xlarge, m5d.2xlarge, m5d.4xlarge • m5dn.xlarge, m5dn.2xlarge, m5dn.4xlarge • m5n.xlarge, m5n.2xlarge, m5n.4xlarge • m5zn.xlarge, m5zn.2xlarge, m5zn.3xlarge • r5.xlarge, r5.2xlarge, r5.4xlarge • r5a.xlarge, r5a.2xlarge, r5a.4xlarge • r5ad.xlarge, r5ad.2xlarge, r5ad.4xlarge • r5b.xlarge, r5b.2xlarge, r5b.4xlarge • r5d.xlarge, r5d.2xlarge, r5d.4xlarge • r5dn.xlarge, r5dn.2xlarge, r5dn.4xlarge • r5n.xlarge, r5n.2xlarge, r5n.4xlarge • z1d.xlarge, z1d.2xlarge, z1d.3xlarge
Azure 인스턴스용 FTDv.	Azure용 FTDv는 다음 인스턴스에 대한 지원을 추가합니다. • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2

기능	설명
ASA 5508-X 및 5516-X에 대한 지원 종료. 마지막으로 지원되는 릴리스: 위협 방어 7.0.	ASA 5508-X 또는 5516-X에 위협 방어위협 방어 7.1을 설치할 수 없습니다. 이 모델에 대해 마지막으로 지원되는 릴리스는 위협 방어 7.0입니다.
방화벽 및 **IPS** 기능	
Snort 3에 대한 네트워크 분석 정책(NAP) 구성.	Snort 3을 실행할 때 device manager를 사용하여 네트워크 분석 정책(NAP)을 구성할 수 있습니다. 네트워크 분석 정책은 트래픽 전처리 검사를 제어합니다. 검사기는 트래픽을 정규화하고 프로토콜 이상 징후를 확인하여 트래픽의 추가 검사를 준비합니다. 모든 트래픽에 사용할 NAP를 선택하고, 네트워크의 트래픽에 가장 적합한 설정을 사용자 지정할 수 있습니다. Snort 2를 실행할 때는 NAP를 구성할 수 없습니다. 네트워크 분석 정책을 **Policies(**정책**)** > **Intrusion settings(**침입 설정**)** 대화 상자에 추가했습니다. 여기에는 직접 변경을 허용하는 JSON 편집기, 재정의를 업로드하거나 생성한 항목을 다운로드할 수 있는 기타 기능이 포함되어 있습니다.
변환된 대상으로 정규화된 도메인 이름(FQDN) 개체에 대한 수동 NAT 지원.	www.example.com을 지정하는 것과 같이 FQDN 네트워크 개체를 수동 NAT 규칙의 변환된 대상 주소로 사용할 수 있습니다. 시스템은 DNS 서버에서 반환된 IP 주소를 기반으로 규칙을 구성합니다.
활성 인증 ID 규칙 개선.	사용자의 연결이 디바이스에 입력되는 인터페이스의 IP 주소가 아닌 정규화된 도메인 이름(FQDN)으로 사용자 인증을 리디렉션하도록 활성 인증 ID 정책 규칙을 구성할 수 있습니다. FQDN은 디바이스에 있는 인터페이스 중 하나의 IP 주소로 확인되어야 합니다. FQDN을 사용하면 클라이언트가 인식할 활성 인증에 대한 인증서를 할당할 수 있으므로, IP 주소로 리디렉션될 때 신뢰할 수 없는 인증서 경고가 표시되지 않습니다. 인증서는 인증서의 SAN(Subject Alternate Name)에 FQDN, 와일드카드 FQDN 또는 여러 FQDN을 지정할 수 있습니다. ID 정책 설정에 **Redirect to Host Name(**호스트 이름으로 리디렉션**)** 옵션을 추가했습니다.
VPN 기능	
사이트 간 VPN을 위한 백업 원격 피어.	원격 백업 피어를 포함하도록 사이트 간 VPN 연결을 구성할 수 있습니다. 기본 원격 피어를 사용할 수 없는 경우 시스템은 백업 피어 중 하나를 사용하여 VPN 연결 재설정을 시도합니다. 각 백업 피어에 대해 별도의 사전 공유 키 또는 인증서를 구성할 수 있습니다. 백업 피어는 정책 기반 연결에 대해서만 지원되며, 경로 기반(가상 터널 인터페이스) 연결에는 사용할 수 없습니다. 백업 피어 구성을 포함하도록 사이트 간 VPN 마법사를 업데이트했습니다.

기능	설명
원격 액세스 VPN(MSCHAPv2)의 비밀번호 관리.	원격 액세스 VPN에 대한 비밀번호 관리를 활성화할 수 있습니다. 그러면 AnyConnect에서 사용자에게 만료된 비밀번호를 변경하라는 프롬프트를 표시할 수 있습니다. 비밀번호 관리가 없으면 사용자는 AAA 서버에서 만료된 비밀번호를 직접 변경해야 하며, AnyConnect는 비밀번호 변경 프롬프트를 표시하지 않습니다. LDAP 서버의 경우, 사용자에게 향후 비밀번호 만료를 알리는 경고 기간을 설정할 수도 있습니다. 원격 액세스 VPN 연결 프로파일의 인증 설정에 Enable Password Management(비밀번호 관리 활성화) 옵션을 추가했습니다.
AnyConnect VPN SAML 외부 브라우저.	원격 액세스 VPN 연결 프로파일의 기본 인증 방법으로 SAML을 사용하는 경우, AnyConnect 클라이언트가 AnyConnect 내장 브라우저 대신 클라이언트의 로컬 브라우저를 사용하여 웹 인증을 수행하도록 선택할 수 있습니다. 이 옵션은 VPN 인증과 기타 기업 로그인 간에 SSO(Single Sign-On)를 활성화합니다. 생체 인증과 같이 임베디드 브라우저에서 수행할 수 없는 웹 인증 방법을 지원하고자 하는 경우 이 옵션을 선택합니다. **SAML** 로그인 환경을 구성할 수 있도록 원격 액세스 VPN 연결 프로파일 마법사를 업데이트했습니다.
관리 및 트러블슈팅 기능	
시스템 인터페이스의 IP 주소 매핑에 FQDN(Fully Qualified Domain Name)을 업데이트하는 데 DDNS(Dynamic Domain Name System) 지원.	업그레이드 영향**.** 업그레이드 후 **FlexConfig**를 다시 실행합니다**.** DNS 서버에 동적 업데이트를 보내도록 시스템의 인터페이스에서 DDNS를 설정할 수 있습니다. 이렇게 하면 인터페이스에 대해 정의된 FQDN이 올바른 주소로 확인되므로 사용자가 IP 주소가 아닌 호스트 이름을 사용하여 시스템에 더욱 쉽게 액세스할 수 있습니다. 이는 DHCP를 사용하여 주소를 가져오는 인터페이스에 특히 유용하지만 정적으로 주소가 지정된 인터페이스에도 유용합니다. 업그레이드 후 FlexConfig를 사용하여 DDNS를 설정한 경우 device manager 또는 위협 방어 API를 사용하여 설정을 다시 실행하고, FlexConfig 정책에서 DDNS FlexConfig 개체를 제거해야 변경 사항을 다시 구축할 수 있습니다. device manager를 사용하여 DDNS를 설정한 다음 Management Center 관리로 전환하면 Management Center가 DNS 이름을 사용하여 시스템을 찾을 수 있도록 DDNS 설정이 유지됩니다. device manager에서 **System Settings(**시스템 설정**)** > **DDNS Service(DDNS** 서비스**)** 페이지를 추가했습니다. 위협 방어 API에서 DDNSService 및 DDNSInterfaceSettings 리소스를 추가했습니다.
dig 명령이 디바이스 CLI의 **nslookup** 명령 대체.	디바이스 CLI에서 정규화된 도메인 이름(FQDN)의 IP 주소를 조회하려면 **dig** 명령을 사용합니다. **nslookup** 명령이 제거되었습니다.

기능	설명
device manager를 사용하는 DHCP 릴레이 구성.	device manager를 사용하여 DHCP 릴레이를 구성할 수 있습니다. 인터페이스에서 DHCP 릴레이를 사용하면 다른 인터페이스를 통해 액세스할 수 있는 DHCP 서버로 DHCP 요청을 보낼 수 있습니다. 물리적 인터페이스, 하위 인터페이스, EtherChannel 및 VLAN 인터페이스에서 DHCP 릴레이를 설정할 수 있습니다. 임의의 인터페이스에서 DHCP 서버를 구성하는 경우 DHCP 릴레이를 구성할 수 없습니다. **System Settings(**시스템 설정**)** > **DHCP** > **DHCP Relay(DHCP** 릴레이**)** 페이지를 추가하고 DHCP Server(DHCP 서버)를 새 DHCP 제목 아래로 이동했습니다.
device manager의 자체 서명 인증서에 대한 키 유형 및 크기.	device manager에서 새로운 자체 서명 내부 및 내부 CA 인증서를 생성할 때 키 유형 및 크기를 지정할 수 있습니다. 키 유형에는 RSA, ECDSA, EDDSA가 있습니다. 허용되는 크기는 키 유형에 따라 다릅니다. 키 크기가 권장 최소 길이보다 작은 인증서를 업로드하면 경고 메시지가 표시됩니다. 또한 가능한 경우 교체해야 하는 약한 인증서를 찾는 데 도움이 되는 약한 키 사전 정의 검색 필터도 있습니다.
신뢰할 수 있는 CA 인증서에 대한 사용 검증 제한.	신뢰할 수 있는 CA 인증서를 사용하여 특정 연결 유형을 검증할 수 있는지 여부를 지정할 수 있습니다. SSL 서버(동적 DNS에서 사용), SSL 클라이언트(원격 액세스 VPN에서 사용), IPsec 클라이언트(사이트 간 VPN에서 사용) 또는 Snort 검사 엔진(예: LDAPS)에서 관리하지 않는 기타 기능에 대한 검증을 허용하거나 방지할 수 있습니다. 이러한 옵션의 기본 목적은 특정 인증서에 대해 검증될 수 있으므로 VPN 연결이 설정되지 않도록 하는 것입니다. **Validation Usage(**검증 사용**)**를 신뢰할 수 있는 CA 인증서의 속성으로 추가했습니다.
device manager에서 관리자 비밀번호 생성.	device manager에서 초기 시스템 구성을 수행하는 동안 또는 device manager를 통해 관리자 비밀번호를 변경할 때 임의의 16자 비밀번호를 생성하는 버튼을 클릭할 수 있습니다.
시작 시간 및 tmatch 컴파일 상태.	이제 **show version** 명령에는 시스템을 시작(부팅)하는 데 걸린 시간에 대한 정보가 포함됩니다. 구성이 클수록 시스템을 부팅하는 시간이 더 오래 걸립니다. 새로운 **show asp rule-engine** 명령은 tmatch 컴파일에 대한 상태를 표시합니다. tmatch 컴파일은 액세스 그룹, NAT 테이블 및 기타 항목으로 사용되는 액세스 목록에 사용됩니다. 매우 큰 ACL 및 NAT 테이블이 있는 경우 CPU 리소스를 사용하고 진행 중인 성능에 영향을 줄 수 있는 내부 프로세스입니다. 컴파일 시간은 액세스 목록, NAT 테이블 등의 크기에 따라 달라집니다.

기능	설명
show access-list element-count 출력 향상.	**show access-list element-count** 명령의 출력이 향상되었습니다. 개체 그룹 검색을 활성화하여 사용하면 출력에 요소 수의 개체 그룹 수에 대한 세부 정보가 포함됩니다. 또한 **show tech-support** 출력에 **show access-list element-count** 및 **show asp rule-engine**의 출력이 포함됩니다.
Management Center를 통한 위협 방어 관리 구성을 위해 device manager 사용.	device manager를 사용하여 초기 설정을 수행할 때 관리 및 Management Center 액세스 설정 외에 관리를 위해 Management Center로 전환하면 device manager에서 완료된 모든 인터페이스 구성이 유지됩니다. 액세스 제어 정책 또는 보안 영역과 같은 기타 기본 구성 설정은 유지되지 않습니다. 위협 방어 CLI를 사용하는 경우 관리 및 Management Center 액세스 설정만 유지됩니다(예: 기본 내부 인터페이스 구성은 유지되지 않음). Management Center로 전환한 후에는 더 이상 device manager를 사용하여 위협 방어를 관리할 수 없습니다. 신규/수정 화면: **System Settings(**시스템 설정**)** > **Management Center(**관리 센터**)**
CA 번들을 자동으로 업데이트.	업그레이드 영향**.** 시스템은 새로운 것을 위해 **Cisco**에 연결합니다**.** 로컬 CA 번들에는 여러 Cisco 서비스에 액세스하기 위한 인증서가 포함되어 있습니다. 이제 시스템은 매일 시스템 정의 시간에 새 CA 인증서를 자동으로 쿼리합니다. 이전에는 CA 인증서를 업데이트하려면 소프트웨어를 업그레이드해야 했습니다. CLI를 사용하여 이 기능을 비활성화할 수 있습니다. 신규/수정된 CLI 명령: **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** 버전 제한: 이 기능은 버전 7.0.5 이상, 7.1.0.3 이상 및 7.2.4 이상에 포함되어 있습니다. 7.0, 7.1 또는 7.2 이전 릴리스에서는 지원되지 않습니다. 지원되는 버전에서 지원되지 않는 버전으로 업그레이드하면 해당 기능이 일시적으로 비활성화되고 시스템에서 Cisco와의 연결이 중지됩니다. 참조: Cisco Secure Firewall Threat Defense 명령 참조

기능	설명
FTD REST API 버전 6.2(v6).	소프트웨어 버전 7.1의 위협 방어 REST API는 버전 6.2입니다. API URL의 v6를 사용하거나 /latest/를 사용하여 디바이스에서 지원되는 가장 최신 API 버전을 사용하고 있음을 나타내는 것이 좋습니다. 6.2의 URL 버전 경로 요소는 6.0/1과 동일한 v6입니다. 사용 중인 리소스 모델에 변경 사항이 적용되었을 수 있으므로 모든 기존 호출을 다시 평가하십시오. 리소스를 확인할 수 있는 API Explorer를 열려면 device manager에 로그인한 다음, More options(추가 옵션) 버튼( )을 클릭하고 **API Explorer**를 선택합니다.

FDM 버전 7.0의 새로운 기능

표 *5: FDM* 버전 *7.0*의 새로운 기능 및 사용 중단된 기능

기능	설명
플랫폼 기능	
HyperFlex 및 Nutanix용 FTDv.	Cisco HyperFlex 및 Nutanix Enterprise Cloud용 FTDv를 도입했습니다.
VMware vSphere/VMware ESXi 7.0용 FTDv.	이제 VMware vSphere/VMware ESXi 7.0에 FTDv를 구축할 수 있습니다. 버전 7.0에서는 VMware 6.0에 대한 지원도 중단됩니다. FTD를 업그레이드하기 전에 호스트 환경을 지원되는 버전으로 업그레이드합니다.
AWS의 threat defense virtual에 대한 새 기본 비밀번호.	AWS에서 구축 중에 사용자 데이터(**Advanced Details(**고급 세부정보**)** > **User Data(**사용자 데이터**)**)로 기본 비밀번호를 정의하지 않은 경우 threat defense virtual에 대한 기본 관리자 비밀번호는 AWS 인스턴스 ID입니다.
ISA 3000 종료 지원.	버전 7.0.2 이상에서는 ISA 3000을 종료할 수 있습니다. 이전에는 디바이스를 리부팅만 할 수 있었습니다. 버전 7.0.5 이상에서는 ISA 3000을 종료하면 시스템 LED가 꺼집니다. 그런 다음 디바이스에서 전원을 제거하기 전에 10초 이상 기다립니다. 버전 제한: 버전 7.1에서는 이 기능에 대한 지원을 일시적으로 중단합니다. 버전 7.2에서는 지원이 반환됩니다.
방화벽 및 **IPS** 기능	

기능	설명
시스템 정의 NAT 규칙에 대한 새 섹션 0.	새 섹션 0이 NAT 규칙 테이블에 추가되었습니다. 이 섹션은 시스템에서만 사용할 수 있습니다. 시스템이 정상적으로 작동하는 데 필요한 모든 NAT 규칙이 이 섹션에 추가되며, 이러한 규칙은 사용자가 생성하는 규칙보다 우선 적용됩니다. 이전에는 시스템 정의 규칙이 섹션 1에 추가되었으며, 사용자 정의 규칙이 적절한 시스템 기능을 방해할 수 있었습니다. 섹션 0 규칙을 추가, 편집 또는 삭제할 수는 없지만 **show nat detail** 명령 출력에서 이를 볼 수 있습니다.
Snort 3용 맞춤형 침입 규칙.	오프라인 툴을 사용하여 Snort 3에 사용할 맞춤형 침입 규칙을 생성하고 이를 침입 정책에 업로드할 수 있습니다. 필요에 따라 쉽게 업데이트할 수 있도록 고유한 맞춤형 규칙 그룹에서 맞춤형 규칙을 구성할 수 있습니다. device manager에서 직접 규칙을 생성할 수도 있지만 규칙의 형식은 업로드된 규칙과 동일합니다. Device Manager는 규칙 생성을 안내하지 않습니다. 시스템 정의 규칙을 포함하여 기존 규칙을 새 침입 규칙의 기반으로 복제할 수 있습니다. 침입 정책을 편집할 때 **Policies(**정책**)** > **Intrusion(**침입**)** 페이지에 맞춤형 그룹 및 규칙에 대한 지원이 추가되었습니다.
device manager 관리 시스템용 Snort 3의 새로운 기능.	이제 device manager 관리 시스템에서 Snort 3을 검사 엔진으로 사용할 때 다음과 같은 추가 기능을 설정할 수 있습니다. • 시간 기반 액세스 제어 규칙. (Threat Defense API 전용.) • 여러 가상 라우터. • SSL 암호 해독 정책을 사용하는 TLS 1.1 이하 연결의 암호 해독. • SSL 암호 해독 정책을 사용하여 다음 프로토콜의 암호 해독: FTPS, SMTPS, IMAPS, POP3S.
URL 범주 및 평판을 기반으로 하는 DNS 요청 필터링.	URL 필터링 범주 및 평판 규칙을 DNS 조회 요청에 적용할 수 있습니다. 조회 요청의 FQDN(Fully Qualified Domain Name)에 차단 중인 범주 및 평판이 있는 경우 시스템은 DNS 응답을 차단합니다. 사용자는 DNS 확인을 받지 않으므로 연결을 완료할 수 없습니다. 웹 이외의 트래픽에 URL 범주 및 평판 필터링을 적용하려면 이 옵션을 사용합니다. 이 기능을 사용하려면 URL 필터링 라이선스가 있어야 합니다. 액세스 제어 정책 설정에 **Reputation Enforcement on DNS Traffic(DNS** 트래픽에 평판 시행**)** 옵션을 추가했습니다.

기능	설명
Snort 2를 사용하는 메모리가 적은 디바이스의 경우 VDB가 작아짐.	업그레이드 영향. 메모리가 낮은 디바이스의 애플리케이션 식별이 영향을 받습니다. Snort 2를 사용하는 버전 7.0.6 이상 디바이스와 VDB 363 이상의 경우 시스템은 이제 Snort 2를 실행하는 메모리가 적은 디바이스에 더 작은 VDB(*VDB lite*라고도 함)를 설치합니다. 더 작은 VDB에는 동일한 애플리케이션이 포함되어 있지만, 탐지 패턴이 더 적습니다. 더 작은 VDB를 사용하는 디바이스는 전체 VDB를 사용하는 디바이스에 비해 일부 애플리케이션 식별을 누락할 수 있습니다. 더 낮은 메모리 디바이스: ASA-5508-X, ASA-5516-X 버전 제한: 더 작은 VDB는 모든 버전에서 지원되지 않습니다. 지원되는 버전에서 지원되지 않는 버전으로 업그레이드할 경우 Snort 2를 실행하는 메모리가 적은 디바이스에 363 이상 VDB를 설치할 수 없습니다. 영향을 받는 릴리스의 목록은 CSCwd88641을 참조하십시오.
VPN 기능	
원격 액세스 VPN에 대한 Device Manager SSL 암호 설정.	device manager에서 원격 액세스 VPN 연결에 사용할 TLS 버전 및 암호화 암호를 정의할 수 있습니다. 이전에는 위협 방어 API를 사용하여 SSL 설정을 지정해야 했습니다. 다음 페이지를 추가했습니다. **Objects(**개체**)** > **SSL Ciphers(SSL** 암호**)**, **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **SSL Settings(SSL** 설정**)**.
Diffie-Hellman 그룹 31 지원.	이제 IKEv2 제안 및 정책에서 DH(Diffie-Hellman) 그룹 31을 사용할 수 있습니다.
디바이스의 최대 Virtual Tunnel Interface의 수는 1024.	생성할 수 있는 최대 VTI(Virtual Tunnel Interface)의 수는 1024입니다. 이전 버전에서는 소스 인터페이스당 최대 100이었습니다.
사이트 간 VPN 보안 연결을 위한 IPsec 수명 설정.	재협상해야 하기 전에 보안 연결이 유지되는 기간에 대한 기본 설정을 변경할 수 있습니다. 사이트 간 VPN 마법사에 **Lifetime Duration(**수명 기간**)** 및 **Lifetime Size(**수명 크기**)** 옵션을 추가했습니다.
라우팅 기능	
ISA 3000에 대한 가상 라우터 지원.	ISA 3000 디바이스에서 최대 10개의 가상 라우터를 설정할 수 있습니다.

기능	설명
ECMP(Equal-Cost Multi-Path) 라우팅.	기존 연결의 트래픽이 영역 내 모든 인터페이스에서 위협 방어 디바이스로 들어가거나 나갈 수 있도록 ECMP 트래픽 영역을 구성하여 여러 인터페이스를 포함합니다. 이 기능을 통해 위협 방어 디바이스에서 ECMP(Equal-Cost Multi-Path) 라우팅이 가능하며, 여러 인터페이스에 걸쳐 위협 방어 디바이스로의 트래픽에 외부 로드 밸런싱이 가능합니다. ECMP 트래픽 영역은 라우팅에만 사용됩니다. 이들은 보안 영역과 동일하지 않습니다. Routing(라우팅) 페이지에 **ECMP Traffic Zones(ECMP** 트래픽 영역**)** 탭을 추가했습니다. 위협 방어 API에 ECMPZones 리소스를 추가했습니다.
인터페이스 기능	
새 기본 내부 IP 주소.	내부 인터페이스에 대한 기본 IP 주소는 192.168.1.1에서 **192.168.95.1**로 변경됩니다. 192.168.1.0/24의 주소가 DHCP를 사용하여 외부 인터페이스에 할당될 때 IP 주소 충돌을 방지하기 위해서입니다.
이제 기본 외부 IP 주소에서 IPv6 자동 설정이 활성화됨. 관리를 위한 새로운 기본 IPv6 DNS 서버.	이제 외부 인터페이스의 기본 설정에 IPv4 DHCP 클라이언트 외에도 IPv6 자동 설정이 포함됩니다. 이제 기본 관리 DNS 서버에 IPv6 서버 2620:119:35::35도 포함됩니다.
ISA 3000용 EtherChannel 지원.	이제 device manager를 사용하여 ISA 3000에서 EtherChannel을 설정할 수 있습니다. 신규/수정 화면: **Devices(**디바이스**)** > **Interfaces(**인터페이스**)** > **EtherChannels**
라이선싱 기능	
threat defense virtual용 성능 계층 라이선싱.	threat defense virtual은 이제 처리량 요구 사항 및 RA VPN 세션 제한을 기반으로 성능 계층 스마트 라이선싱을 지원합니다. threat defense virtual에 사용 가능한 성능 라이선스 중 하나를 통해 라이선싱되면 두 가지 작업이 이루어집니다. 먼저, 디바이스 처리량을 지정된 레벨로 제한하는 속도 제한기가 설치됩니다. 그리고 VPN 세션 수는 라이선스에서 지정된 수로 제한됩니다.
관리 및 트러블슈팅 기능	

기능	설명
위협 방어 API를 사용하는 DHCP 릴레이 설정.	업그레이드 영향. 업그레이드 후 구축을 방지할 수 있습니다. 위협 방어 API를 사용하여 DHCP 릴레이를 설정할 수 있습니다. 인터페이스에서 DHCP 릴레이를 사용하면 다른 인터페이스를 통해 액세스할 수 있는 DHCP 서버로 DHCP 요청을 보낼 수 있습니다. 물리적 인터페이스, 하위 인터페이스, EtherChannel 및 VLAN 인터페이스에서 DHCP 릴레이를 설정할 수 있습니다. 임의의 인터페이스에서 DHCP 서버를 구성하는 경우 DHCP 릴레이를 구성할 수 없습니다. 이전 릴리스에서 FlexConfig를 사용하여 DHCP 릴레이를 설정한 경우(**dhcprelay** 명령), 업그레이드 후 API를 사용하여 설정을 다시 실행하고 FlexConfig 개체를 삭제해야 합니다. 위협 방어 API에 dhcprelayservices 모델을 추가했습니다.
더 빠른 부트스트랩 처리 및 device manager 조기 로그인.	초기에 device manager 관리 시스템을 부트스트랩하는 프로세스가 개선되어 더욱 빨라졌습니다. 따라서 디바이스를 시작한 후 device manager에 로그인할 때까지 기다릴 필요가 없습니다. 또한 부트스트랩이 진행되는 동안에도 로그인할 수 있습니다. 부트스트랩이 완료되지 않은 경우 프로세스에서 상태 정보를 확인하여 디바이스에서 발생하는 상황을 확인할 수 있습니다.
다대일 및 일대다 연결의 CPU 사용 및 성능 개선.	동적 NAT/PAT와 스캐닝 위협 탐지 및 호스트 통계를 포함하는 연결을 제외하고, 시스템은 연결을 생성할 때 더 이상 로컬 호스트 개체를 생성하고 잠그지 않습니다. 이렇게 하면 많은 연결이 동일한 서버(예: 로드 밸런서 또는 웹 서버)에 연결되거나 하나의 엔드포인트가 여러 원격 호스트에 연결되는 상황에서 성능과 CPU 사용량이 향상됩니다. 다음 명령이 변경되었습니다. **clear local-host**(더 이상 사용되지 않음), **show local-host**
device manager 관리 디바이스에 대한 업그레이드 준비도 확인.	설치를 시도하기 전에 업로드된 위협 방어 업그레이드 패키지에서 업그레이드 준비도 확인을 실행할 수 있습니다. 준비도 확인은 업그레이드가 시스템에 유효한지, 그리고 시스템이 패키지 설치에 필요한 기타 요건을 충족하는지 확인합니다. 업그레이드 준비도 확인을 실행하면 설치 실패를 방지할 수 있습니다. 업그레이드 준비도 확인 실행 링크가 **Device(**디바이스**)** > **Updates(**업데이트**)** 페이지의 **System Upgrade(**시스템 업그레이드**)** 섹션에 추가되었습니다.

기능	설명
CA 번들을 자동으로 업데이트.	업그레이드 영향. 시스템은 새로운 것을 위해 **Cisco**에 연결합니다. 로컬 CA 번들에는 여러 Cisco 서비스에 액세스하기 위한 인증서가 포함되어 있습니다. 이제 시스템은 매일 시스템 정의 시간에 새 CA 인증서를 자동으로 쿼리합니다. 이전에는 CA 인증서를 업데이트하려면 소프트웨어를 업그레이드해야 했습니다. CLI를 사용하여 이 기능을 비활성화할 수 있습니다. 신규/수정된 CLI 명령: **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** 버전 제한: 이 기능은 버전 7.0.5 이상, 7.1.0.3 이상 및 7.2.4 이상에 포함되어 있습니다. 7.0, 7.1 또는 7.2 이전 릴리스에서는 지원되지 않습니다. 지원되는 버전에서 지원되지 않는 버전으로 업그레이드하면 해당 기능이 일시적으로 비활성화되고 시스템에서 Cisco와의 연결이 중지됩니다. 참조: Cisco Secure Firewall Threat Defense 명령 참조
FTD REST API 버전 6.1(v6).	소프트웨어 버전 7.0에 대한 위협 방어 REST API는 6.1 버전입니다. API URL의 v6를 사용하거나 /latest/를 사용하여 디바이스에서 지원되는 가장 최신 API 버전을 사용하고 있음을 나타내는 것이 좋습니다. 6.1의 URL 버전 경로 요소는 6.0과 동일한 v6입니다. 사용 중인 리소스 모델에 변경 사항이 적용되었을 수 있으므로 모든 기존 호출을 다시 평가하십시오. 리소스를 확인할 수 있는 API Explorer를 열려면 device manager에 로그인한 다음, More options(추가 옵션) 버튼( )을 클릭하고 **API Explorer**를 선택합니다.

FDM 버전 6.7의 새로운 기능

표 *6: FDM* 버전 *6.7*의 새로운 기능 및 사용 중단된 기능

기능	설명
플랫폼 기능	
ASA 5525-X, 5545-X 및 5555-X에 대해 지원 종료. 마지막으로 지원되는 릴리스: 위협 방어 6.6.	ASA 5525-X, 5545-X 또는 5555-X에는 위협 방어6.7을 설치할 수 없습니다. 이러한 모델에 대해 마지막으로 지원되는 릴리스는 위협 방어 6.6입니다.
방화벽 및 **IPS** 기능	

기능	설명
액세스 제어 규칙 일치를 위한 TLS 서버 ID 검색	TLS 1.3 인증서가 암호화됩니다. 애플리케이션 또는 URL 필터링을 사용하는 액세스 규칙과 일치하도록 TLS 1.3으로 암호화된 트래픽의 경우 시스템은 TLS 1.3 인증서를 암호 해독해야 합니다. 암호화된 연결이 올바른 액세스 제어 규칙과 일치하는지 확인하려면 **TLS** 서버 **ID** 검색을 활성화하는 것이 좋습니다. 설정은 인증서만 암호 해독합니다. 연결은 암호화된 상태로 유지됩니다. 액세스 컨트롤 설정(⚙) 버튼 및 대화 상자를 정책 > 액세스 컨트롤 페이지에 추가했습니다.
외부의 신뢰할 수 있는 CA 인증서 그룹.	이제 SSL 암호 해독 정책에서 사용하는 신뢰할 수 있는 CA 인증서 목록을 맞춤화할 수 있습니다. 기본적으로 정책은 모든 시스템 정의의 신뢰할 수 있는 CA 인증서를 사용하지만, 인증서를 추가하기 위해 맞춤형 그룹을 만들거나 기본 그룹을 더 제한적인 고유 그룹으로 대체할 수 있습니다. 인증서 그룹을 **Objects(**개체**)** > **Certificates(**인증서**)** 페이지에 추가하고 SSL 암호 해독 정책 설정을 수정하여 인증서 그룹을 선택할 수 있도록 했습니다.
패시브 ID 규칙에 대한 Active Directory 영역 시퀀스.	AD(Active Directory) 서버 및 해당 도메인의 순서가 지정된 목록으로 영역 시퀀스를 생성하고 이를 패시브 인증 ID 규칙에서 사용할 수 있습니다. 영역 시퀀스는 두 개 이상의 AD 도메인을 지원하고 사용자 기반 액세스 컨트롤을 수행하려는 경우 유용합니다. 각 AD 도메인에 대해 별도의 규칙을 작성하는 대신 모든 도메인을 포괄하는 단일 규칙을 작성할 수 있습니다. 시퀀스 내의 AD 영역 순서 지정은 ID 충돌이 발생하는 경우 이를 해결하는 데 사용됩니다. **Objects(**개체**)** > **Identity Sources(ID** 소스**)** 페이지에서 AD 영역 시퀀스 개체를 추가하고 패시브 인증 ID 규칙에서 개체를 영역으로 선택하는 기능을 추가했습니다. 위협 방어 API에서는 영역 시퀀스 리소스를 추가했으며, **ID** 규칙 리소스에서는 작업으로 수동 인증을 사용하는 규칙의 영역으로 영역 시퀀스 개체를 선택하는 기능을 추가했습니다.
트러스트섹(Trustsec) SGT(Security Group Tag) 그룹 개체에 대한 FDM 지원 및 액세스 제어 규칙에서의 사용.	위협 방어 6.5에서는 SGT 그룹 개체를 구성하고 이러한 개체를 액세스 제어 규칙에서 일치 기준으로 사용할 수 있도록 위협 방어 API에 대한 지원이 추가되었습니다. 또한 ISE에서 게시한 SXP 주제를 수신하도록 ISE ID 개체를 수정할 수 있습니다. 이제 이러한 기능을 FDM에서 직접 구성할 수 있습니다. 새 개체, SGT 그룹을 추가하고 선택 및 표시를 허용하도록 액세스 제어 정책을 업데이트했습니다. 또한 구독할 주제를 명시적으로 선택할 수 있도록 ISE 개체를 수정했습니다.

기능	설명
Snort 3.0 지원	새 시스템의 경우 Snort 3.0이 기본 검사 엔진입니다. 이전 릴리스에서 6.7로 업그레이드하는 경우 Snort 2.0이 액티브 검사 엔진으로 유지되지만 Snort 3.0으로 전환할 수 있습니다. 이 릴리스에서는 Snort 3.0이 가상 라우터, 시간 기반 액세스 제어 규칙 또는 TLS 1.1 이하 연결의 암호 해독을 지원하지 않습니다. 이러한 기능이 필요하지 않은 경우에만 Snort 3.0을 활성화하십시오. Snort 2.0과 3.0 간에 자유롭게 전환할 수 있으므로 필요한 경우 변경 사항을 되돌릴 수 있습니다. 트래픽은 버전을 전환할 때마다 중단됩니다. **Intrusion Rules(**침입 규칙**)** 그룹에서 **Device(**디바이스**)** > **Updates(**업데이트**)** 페이지로 Snort 버전을 전환하는 기능을 추가했습니다. 위협 방어 API에서 IntrusionPolicy resource action/toggleinspectionengine이 추가되었습니다. 또한 Snort 3 규칙 패키지 업데이트에서 추가, 삭제 또는 변경된 침입 규칙을 보여주는 새로운 감사 이벤트인 규칙 업데이트 이벤트도 있습니다.
Snort 3용 맞춤형 침입 정책.	Snort 3을 검사 엔진으로 사용하는 경우 맞춤형 침입 정책을 생성할 수 있습니다. 반면 Snort 2를 사용하는 경우에만 사전 정의된 정책을 사용할 수 있습니다. 맞춤형 침입 정책을 사용하면 규칙 그룹을 추가 또는 제거하고 그룹 레벨의 보안 레벨을 변경하여 그룹에 있는 규칙의 기본 작업(비활성, 알림 또는 삭제)을 효율적으로 변경할 수 있습니다. Snort 3 침입 정책을 사용하면 기본 Cisco Talos에서 제공하는 정책을 수정할 필요 없이 IPS/IDS 시스템의 동작을 보다 효율적으로 제어할 수 있습니다. 침입 정책이 나열되도록 **Policies(**정책**)** > **Intrusion(**침입**)** 페이지를 변경했습니다. 새 정책을 생성하고 그룹 추가/제거, 보안 레벨 할당, 규칙에 대한 작업 변경을 비롯한 기존 정책을 확인하거나 수정할 수 있습니다. 여러 규칙을 선택하고 작업을 변경할 수도 있습니다. 또한 액세스 제어 규칙에서 맞춤형 침입 정책을 선택할 수 있습니다.
침입 이벤트에 대한 여러 시스템 로그 서버	침입 정책에 대해 여러 시스템 로그 서버를 구성할 수 있습니다. 침입 이벤트는 각 시스템 로그 서버로 전송됩니다. 여러 시스템 로그 서버 개체를 선택하는 기능을 침입 정책 설정 대화 상자에 추가했습니다.
URL 평판 일치에는 평판을 알 수 없는 사이트가 포함될 수 있음.	URL 범주 트래픽 일치 기준을 구성하고 평판 범위를 선택할 때 평판 일치에 평판을 알 수 없는 URL을 포함할 수 있습니다. **Include Sites with Unknown Reputation(**평판을 알 수 없는 사이트 포함**)** 체크 박스를 액세스 제어 및 SSL 암호 해독 규칙의 URL 평판 기준에 추가했습니다.

기능	설명
VPN 기능	
VTI(Virtual Tunnel Interface) 및 경로 기반 사이트 간 VPN.	이제 Virtual Tunnel Interface를 VPN 연결 프로파일에 대한 로컬 인터페이스로 사용하여 경로 기반 사이트 간 VPN을 생성할 수 있습니다. 경로 기반 사이트 간 VPN을 통해 VPN 연결 프로파일을 전혀 변경하지 않고 단순히 라우팅 테이블을 변경하여 지정된 VPN 연결에서 보호된 네트워크를 관리합니다. 이 변경 사항을 고려하여 원격 네트워크를 추적하고 VPN 연결 프로파일을 업데이트할 필요가 없습니다. 이는 클라우드 서비스 제공자 및 대기업에 대한 VPN 관리를 간소화합니다. **Virtual Tunnel Interfaces** 탭을 인터페이스 목록 페이지에 추가하고 사이트 간 VPN 마법사를 업데이트하여 로컬 인터페이스로 VTI를 사용할 수 있도록 했습니다.
Threat Defense 원격 액세스 VPN 연결을 위한 Hostscan 및 DAP(Dynamic Access Policy)에 대한 API 지원	Hostscan 패키지 및 DAP(Dynamic Access Policy) 규칙 XML 파일을 업로드하고, DAP 규칙을 구성하여 XML 파일을 생성하고, 연결 엔드포인트의 상태와 관련된 특성을 기반으로 하여 원격 사용자에게 그룹 정책을 할당하는 방법을 제어할 수 있습니다. Cisco ISE(Identity Services Engine)가 없는 경우 이러한 기능을 사용하여 COA(Change of Authorization)를 수행할 수 있습니다. 위협 방어 API를 사용하는 경우에만 Hostscan을 업로드하고 DAP를 구성할 수 있으며, FDM을 사용하는 경우에는 이를 구성할 수 없습니다. Hostscan 및 DAP 사용량에 대한 자세한 내용은 AnyConnect 설명서를 참조하십시오. 추가 또는 수정된 위협 방어 API 개체 모델: dapxml, hostscanpackagefiles, hostscanxmlconfigs, ravpns
외부 CA 인증서에 대한 인증서 해지 확인 활성화.	위협 방어 API를 사용하여 특정 외부 CA 인증서에서 인증서 해지 확인을 활성화할 수 있습니다. 해지 확인은 원격 액세스 VPN에서 사용되는 인증서에 특히 유용합니다. FDM을 사용하여 인증서에서 해지 확인을 구성할 수 없습니다. 위협 방어 API를 사용해야 합니다. 다음 특성을 ExternalCACertificate 리소스(revocationCheck, crlCacheTime, oscpDisableNonce)에 추가했습니다.

기능	설명
보안성이 낮은 Diffie-Hellman 그룹, 암호화 및 해시 알고리즘에 대한 지원 제거.	업그레이드 영향. 업그레이드 후 구축을 방지할 수 있습니다. 다음 기능은 6.6에서 사용되지 않으며 이제 제거되었습니다. IKE 제안 또는 IPsec 정책에서 이러한 정책을 계속 사용하는 경우에는 업그레이드 후에 이를 변경해야 컨피그레이션 변경 사항을 구축할 수 있습니다. VPN이 올바르게 작동하도록 지원되는 DH 및 암호화 알고리즘으로 업그레이드하기 전에 VPN 컨피그레이션을 변경하는 것이 좋습니다. • Diffie-Hellman 그룹: 2, 5 및 24. • 강력한 암호화를 위한 내보내기 제어를 충족하는 사용자를 위한 암호화 알고리즘: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. 내보내기 제어를 충족하지 않는 사용자의 경우 DES는 계속 지원됩니다(유일한 옵션임). • 해시 알고리즘: MD5.
원격 액세스 VPN용 맞춤형 포트.	원격 액세스 VPN(RA VPN) 연결에 사용되는 포트를 구성할 수 있습니다. RA VPN에 사용된 것과 동일한 인터페이스에서 FDM에 연결해야 하는 경우 RA VPN 연결의 포트 번호를 변경할 수 있습니다. FDM은 기본 RA VPN 포트이기도 한 포트 443을 사용합니다. 포트 컨피그레이션을 포함하도록 RA VPN 마법사의 전역 설정 단계를 업데이트했습니다.
원격 액세스 VPN 인증을 위한 SAML 서버 지원.	원격 액세스 VPN에 대한 인증 소스로 SAML 2.0 서버를 구성할 수 있습니다. 지원되는 SAML 서버: Duo **Objects(**개체**)** > **Identity Sources(ID** 소스**)** 페이지에서 SAML 서버를 ID 소스로 추가하고 원격 액세스 VPN 연결 프로파일을 사용할 수 있도록 있도록 업데이트했습니다.
AnyConnect 모듈 프로파일에 대한 Threat Defense API 지원.	위협 방어 API를 사용하여 AMP Enabler, ISE Posture 또는 Umbrella와 같은 AnyConnect와 함께 사용되는 모듈 프로파일을 업로드할 수 있습니다. AnyConnect 프로파일 편집기 패키지에서 설치할 수 있는 오프라인 프로파일 편집기를 사용하여 이러한 프로파일을 생성해야 합니다. AnyConnectModuleType 특성을 AnyConnectClientProfile 모델에 추가했습니다. 처음에는 모듈 프로파일을 사용하는 AnyConnect 클라이언트 프로파일 개체를 생성할 수 있지만, API를 사용하여 FDM에서 생성된 개체를 수정하여 올바른 모듈 유형을 지정해야 합니다.
라우팅 기능	

기능	설명
스마트 CLI를 사용한 EIGRP 지원.	업그레이드 영향. 업그레이드 후 구축을 방지할 수 있습니다. 이전 릴리스에서는 Advanced Configuration(고급 컨피그레이션) 페이지에서 FlexConfig를 사용하여 EIGRP를 구성했습니다. 이제 Routing(라우팅) 페이지에서 직접 스마트 CLI를 사용하여 EIGRP를 구성합니다. FlexConfig를 사용하여 EIGRP를 구성한 경우 릴리스 6.7로 업그레이드할 때 FlexConfig 정책에서 FlexConfig 개체를 제거한 다음, 스마트 CLI 개체에서 컨피그레이션을 다시 생성해야 합니다. 스마트 CLI 업데이트를 완료할 때까지 참조를 위해 EIGRP FlexConfig 개체를 유지할 수 있습니다. 컨피그레이션이 자동으로 변환되지는 않습니다. Routing(라우팅) 페이지에 EIGRP 스마트 CLI 개체를 추가했습니다.
인터페이스 기능	
ISA 3000 하드웨어 우회 지속성.	이제 지속성 옵션을 사용하여 ISA 3000 인터페이스 쌍에 대해 하드웨어 우회를 활성화할 수 있습니다. 전원이 복구된 후에는 수동으로 비활성화할 때까지 하드웨어 우회가 활성화된 상태로 유지됩니다. 지속성 없이 하드웨어 우회를 활성화하면 전원이 복구된 후 하드웨어 우회가 자동으로 비활성화됩니다. 하드웨어 우회가 비활성화되면 트래픽이 잠시 중단될 수 있습니다. 지속성 옵션을 통해 트래픽이 일시 중단되는 시점을 제어할 수 있습니다. 신규/수정된 화면: **Device(**디바이스**)** > **Interfaces(**인터페이스**)** > **Hardware Bypass(**하드웨어 우회**)** > **Hardware Bypass Configuration(**하드웨어 우회 컨피그레이션**)**

기능	설명
위협 방어 작동 링크 상태와 Firepower 4100/9300 물리적 링크 상태 간 동기화.	이제 Firepower 4100/9300 섀시가 위협 방어 작동 링크 상태를 데이터 인터페이스의 물리적 링크 상태와 동기화할 수 있습니다. 현재로서는, FXOS 관리 상태가 작동 중이고 물리적 링크 상태가 작동 중이면 인터페이스는 작동 상태가 됩니다. 위협 방어 애플리케이션 인터페이스 관리 상태는 고려되지 않습니다. 예를 들어 위협 방어에서 동기화하지 않으면 위협 방어 애플리케이션이 완전히 온라인 상태가 되기 전에 데이터 인터페이스가 물리적으로 작동 상태가 되거나 위협 방어 종료를 시작한 후 일정 기간 동안 작동 상태를 유지할 수 있습니다. 이 기능은 기본적으로 비활성화되어 있으며 FXOS에서 논리적 디바이스별로 활성화할 수 있습니다. 참고 이 기능은 Radware vDP 데코레이터를 포함한 위협 방어에서 지원되지 않습니다. 신규/수정된 섀시 관리자 화면: **Logical Devices(**논리적 디바이스**) > Enable Link State(**링크 상태 활성화**)** 신규/수정된 FXOS 명령: **set link-state-sync enabled**, **show interface expand detail** 지원되는 플랫폼: Firepower 4100/9300
Firepower 1100 및 2100 SFP 인터페이스에서 자동 협상 비활성화 지원.	이제 Firepower 1100 및 2100 SFP 인터페이스에서 자동 협상 비활성화를 설정할 수 있습니다. 10GB 인터페이스의 경우 자동 협상 없이 속도를 1GB로 설정할 수 있습니다. 속도가 10GB로 설정된 인터페이스에 대해서는 자동 협상을 비활성화할 수 없습니다. 신규/수정된 화면: **Device(**디바이스**) > Interfaces(**인터페이스**) > Edit Interface(**인터페이스 편집**) > Advanced Options(**고급 옵션**) > Speed(**속도**)** 지원되는 플랫폼: Firepower 1100 및 2100
관리 및 트러블슈팅 기능	

기능	설명
실패한 위협 방어 소프트웨어 업그레이드를 취소하고 이전 릴리스로 되돌릴 수 있음.	위협 방어 주요 소프트웨어 업그레이드가 실패하거나 제대로 작동하지 않는 경우 업그레이드를 설치할 때의 상태로 디바이스를 되돌릴 수 있습니다. FDM의 System Upgrade(시스템 업그레이드) 패널로 업그레이드를 되돌릴 수 있는 기능을 추가했습니다. 업그레이드 중에 FDM 로그인 화면에 업그레이드 상태가 표시되며 업그레이드 실패 시 취소하거나 되돌릴 수 있는 옵션이 제공됩니다. 위협 방어 API에서 CancelUpgrade, RevertUpgrade, RetryUpgrade 및 UpgradeRevertInfo 리소스를 추가했습니다. 위협 방어 CLI에서 **show last-upgrade status**, **show upgrade status**, **show upgrade revert-info**, **upgrade cancel**, **upgrade revert**, **upgrade cleanup-revert**, **upgrade retry** 명령을 추가했습니다.
데이터 인터페이스에서 FDM/위협 방어 API 액세스를 위한 맞춤형 HTTPS 포트.	데이터 인터페이스에서 FDM 또는 위협 방어 API 액세스에 사용되는 HTTPS 포트를 변경할 수 있습니다. 포트를 기본값 443에서 변경하면 동일한 데이터 인터페이스에 구성된 원격 액세스 VPN과 같은 다른 기능과 관리 액세스 간의 충돌을 방지할 수 있습니다. 관리 인터페이스의 관리 액세스 HTTPS 포트를 변경할 수 없습니다. **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Access(**관리 액세스**)** > **Data Interfaces(**데이터 인터페이스**)** 페이지에 포트를 변경하는 기능을 추가했습니다.
Firepower 1000 및 2100 시리즈 디바이스의 Cisco Defense Orchestrator에 대한 로우 터치(low-touch) 프로비저닝.	Cisco Defense Orchestrator(CDO)를 사용하여 새 위협 방어 디바이스를 관리하려는 경우 이제 디바이스 설정 마법사를 완료하거나 FDM에 로그인하지 않고도 디바이스를 추가할 수 있습니다. 새로운 Firepower 1000 및 2100 시리즈 디바이스는 처음에 Cisco 클라우드에 등록되며, 이를 통해 CDO에서 쉽게 디바이스를 클레임할 수 있습니다. 일단 CDO에 등록되면 CDO에서 즉시 디바이스를 관리할 수 있습니다. 이러한 로우 터치(low-touch) 프로비저닝은 물리적 디바이스와 직접 상호 작용할 필요성을 최소화하므로, 원격 사무실이나 네트워킹 디바이스 작업 경험이 적은 근로자가 있는 기타 장소에 적합합니다. Firepower 1000 및 2100 시리즈 디바이스의 초기 프로비저닝 방식을 변경했습니다. 또한 **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)** 페이지에 자동 등록을 추가하여 업그레이드된 디바이스 또는 이전에 FDM을 사용하여 관리했던 다른 디바이스에 대한 프로세스를 수동으로 시작할 수 있습니다.

기능	설명
SNMP 구성에 대한 Threat Defense API 지원.	업그레이드 영향. 업그레이드 후 구축을 방지할 수 있습니다. 위협 방어 API를 사용하여 FDM 또는 CDO 관리 위협 방어 디바이스에서 SNMP 버전 2c 또는 3을 구성할 수 있습니다. API 리소스(SNMPAuthentication, SNMPHost, SNMPSecurityConfiguration, SNMPServer, SNMPUser, SNMPUserGroup, SNMPv2cSecurityConfiguration, SNMPv3SecurityConfiguration)를 추가했습니다. 참고 FlexConfig를 사용하여 SNMP를 구성한 경우 위협 방어 API SNMP 리소스를 사용하여 컨피그레이션을 다시 실행해야 합니다. SNMP 구성 명령은 FlexConfig에서 더 이상 허용되지 않습니다. FlexConfig 정책에서 SNMP FlexConfig 개체를 제거하기만 하면 변경 사항을 구축할 수 있습니다. 그러면 API를 사용하여 기능을 재구성하는 동안 개체를 참조로 사용할 수 있습니다.
시스템에 유지되는 최대 백업 파일이 10개에서 3개로 감소.	시스템은 10개가 아닌 최대 3개의 백업 파일을 시스템에 보관합니다. 새 백업이 생성되면 가장 오래된 백업 파일은 삭제됩니다. 필요한 경우 시스템을 복구하는 데 필요한 버전을 사용할 수 있도록 백업 파일을 다른 시스템에 다운로드하십시오.
Microsoft Internet Explorer에 대한 지원 종료.	이제 Microsoft Internet Explorer를 사용하여 Firepower 웹 인터페이스를 테스트하지 않습니다. Google Chrome, Mozilla Firefox 또는 Microsoft Edge로 전환하는 것이 좋습니다.
Threat Defense API 버전 이전 버전과의 호환성.	위협 방어 버전 6.7부터는 기능에 대한 API 리소스 모델이 릴리스 간에 변경되지 않는 경우 위협 방어 API는 이전 API 버전을 기반으로 하는 통화를 수락할 수 있습니다. 기능 모델이 변경된 경우에도 이전 모델을 새 모델로 변환하는 논리적 방법이 있는 경우 이전 콜을 사용할 수 있습니다. 예를 들어, v4 통화는 v5 시스템에서 허용될 수 있습니다. "최신"을 통화의 버전 번호로 사용하는 경우 이러한 "이전" 통화는 이 시나리오에서 v5 통화로 해석되므로 이전 버전과의 호환성을 활용하고 있는지 여부는 API 호출을 어떻게 구성할지에 따라 달라집니다.

기능	설명
Threat Defense REST API 버전 6(v6).	소프트웨어 버전 6.7의 위협 방어 REST API는 버전 6입니다. API URL의 v6를 사용하거나 /latest/를 사용하여 디바이스에서 지원되는 가장 최신 API 버전을 사용하고 있음을 나타내는 것이 좋습니다. 사용 중인 리소스 모델에 변경 사항이 적용되었을 수 있으므로 모든 기존 호출을 다시 평가하십시오. 리소스를 확인할 수 있는 API Explorer를 열려면 FDM에 로그인한 다음, More options(추가 옵션) 버튼( )을 클릭하고 **API Explorer**를 선택합니다.

FDM 버전 6.6의 새로운 기능

표 *7: FDM* 버전 *6.6*의 새로운 기능 및 사용 중단된 기능

기능	설명
플랫폼 기능	
AWS(Amazon Web Services) Cloud용 threat defense virtual에 대한 Device Manager 지원.	device manager를 사용하여 AWS Cloud에 대한 threat defense virtual의 위협 방어를 구성할 수 있습니다.
Firepower 4112용 Device Manager.	Firepower 4112용 위협 방어가 도입되었습니다. 참고 FXOS 2.8.1이 필요합니다.
FTDv for VMware의 e1000 인터페이스.	업그레이드를 방지합니다. 버전 6.6에서는 FTDv for VMware의 e1000 인터페이스에 대한 지원을 종료합니다. vmxnet3 또는 ixgbe 인터페이스로 전환하지 않으면 업그레이드할 수 없습니다. 또는 새 장치를 구축할 수 있습니다. 자세한 내용은 Cisco Secure Firewall Threat Defense Virtual 시작 가이드를 참조하십시오.
방화벽 및 **IPS** 기능	
기본적으로 비활성화된 침입 규칙을 활성화하는 기능	각 시스템 정의 침입 정책에는 기본적으로 비활성화되는 규칙이 많이 있습니다. 이전에는 이러한 규칙에 대한 동작을 알림 또는 삭제로 변경할 수 없었습니다. 이제 기본적으로 비활성화되는 규칙에 대한 동작을 변경할 수 있습니다. 이렇게 기본적으로 비활성화되는 규칙을 비롯하여 모든 규칙을 표시하도록, 그리고 이러한 규칙에 대한 동작을 수정할 수 있도록 침입 정책 페이지가 변경되었습니다.

기능	설명
침입 정책에 대한 IDS(침입 탐지 시스템) 모드	이제 IDS(침입 탐지 시스템) 모드에서 작동하도록 침입 정책을 구성할 수 있습니다. IDS 모드에서 활성 침입 규칙은 규칙 동작이 삭제인 경우에도 알림만 발행합니다. 따라서 네트워크에서 침입 정책을 활성 예방 정책으로 설정하기 전에 침입 정책이 작동하는 방식을 모니터링하거나 테스트할 수 있습니다. device manager에서는 **Policies(**정책**)** > **Intrusion(**침입**)** 페이지의 각 침입 정책에 검사 모드의 표시가 추가되었으며 모드를 변경할 수 있도록 **Edit(**수정**)** 링크가 추가되었습니다. 위협 방어 API에서 IntrusionPolicy 리소스에 inspectionMode 속성이 추가되었습니다.
취약점 데이터베이스(VDB), 지리위치 데이터베이스, 침입 규칙 업데이트 패키지의 수동 업로드 지원	이제 VDB, 지리위치 데이터베이스, 침입 규칙에 대한 업데이트 패키지를 수동으로 검색한 후 device manager를 사용하여 이를 워크스테이션에서 위협 방어 디바이스로 업로드할 수 있습니다. 예를 들어 에어 갭(air-gapped) 네트워크에서 device manager가 Cisco Cloud로부터 업데이트를 검색할 수 없는 경우, 이제는 필요한 업데이트 패키지를 가져올 수 있습니다. 워크스테이션에서 파일을 선택하고 업로드할 수 있도록 **Device(**디바이스**)** > **Updates(**업데이트**)** 페이지가 업데이트되었습니다.
위협 방어 시간에 따라 제한되는 액세스 제어 규칙에 대한 API 지원	위협 방어 API를 사용하면 일회성 또는 반복적인 시간 범위를 지정하는 시간 범위 개체를 생성하고, 이러한 개체를 액세스 제어 규칙에 적용할 수 있습니다. 시간 범위를 사용하면 특정 시간 동안 또는 특정 기간 동안 트래픽에 액세스 제어 규칙을 적용하여 네트워크 사용량을 유연하게 제공할 수 있습니다. device manager를 사용하여 시간 범위를 생성하거나 적용할 수 없으며, 액세스 제어 규칙에 시간 범위가 적용된 경우에도 device manager가 표시되지 않습니다. TimeRangeObject, Recurrence, TimeZoneObject, DayLightSavingDateRange, DayLightSavingDayRecurrence 리소스가 위협 방어 API에 추가되었습니다. 시간 범위를 액세스 제어 규칙에 적용할 수 있도록 TimeRangeObjects 속성이 accessrules 리소스에 추가되었습니다. 이 외에도, GlobalTimeZone 및 TimeZone 리소스가 변경되었습니다.

기능	설명
액세스 제어 정책에 대한 개체 그룹 검색	작동하는 동안 위협 방어 디바이스는 액세스 규칙에 사용되는 모든 네트워크 개체의 콘텐츠에 따라 액세스 제어 규칙을 여러 액세스 제어 목록 항목으로 확장합니다. 개체 그룹 검색을 활성화하여 액세스 컨트롤 규칙을 검색하는 데 필요한 메모리를 줄일 수 있습니다. 개체 그룹 검색을 사용하면 시스템이 네트워크 개체로 확장되지 않습니다. 대신 해당 그룹 정의를 기반으로 일치하는 액세스 규칙을 검색합니다. 개체 그룹 검색은 액세스 규칙이 정의된 방식 또는 device manager에 표시되는 방식에 영향을 주지 않습니다. 이는 액세스 컨트롤 규칙과의 연결을 일치시키는 동안 디바이스가 이를 해석 및 처리하는 방법에만 영향을 미칩니다. 개체 그룹 검색은 기본적으로 비활성화되어 있습니다. device manager에서 FlexConfig를 사용하여 **object-group-search access-control** 명령을 활성화해야 합니다.
VPN 기능	
사이트 대 사이트 VPN을 위한 백업 피어 (위협 방어 API 전용.)	위협 방어 API를 사용하여 사이트 대 사이트 VPN 연결에 백업 피어를 추가할 수 있습니다. 예를 들어 ISP가 2개 있을 경우, 첫 번째 ISP에 대한 연결을 사용할 수 없게 되면 VPN 연결을 백업 ISP로 페일오버하도록 구성할 수 있습니다. 백업 피어의 또 다른 주요 용도는 기본 허브 및 백업 허브처럼 터널의 다른 쪽 끝에 두 개의 다른 디바이스가 있는 경우입니다. 일반적으로 시스템은 기본 허브에 대한 터널을 설정합니다. VPN 연결이 실패하면 시스템에서 자동으로 백업 허브와의 연결을 재설정할 수 있습니다. SToSConnectionProfile 리소스의 outsideInterface에 대해 둘 이상의 인터페이스를 지정할 수 있도록 위협 방어 API가 업데이트되었습니다. BackupPeer 리소스 및 remoteBackupPeers 속성도 SToSConnectionProfile 리소스에 추가되었습니다. device manager를 사용하여 백업 피어를 구성할 수 없으며, 백업 피어의 존재가 device manager에 표시되지 않습니다.
원격 액세스 VPN에서 DTLS(Datagram Transport Layer Security) 1.2 지원	이제 원격 액세스 VPN에서 DTLS 1.2를 사용할 수 있습니다. 이는 위협 방어 API를 사용해서만 구성할 수 있으며 device manager를 사용해서는 구성할 수 없습니다. 하지만 이제 DTLS 1.2는 기본 SSL 암호 그룹의 일부이며, 그룹 정책의 AnyConnect 속성에서 device manager를 사용하여 DTLS의 일반적인 사용을 활성화할 수 있습니다. DTLS 1.2는 ASA 5508-X 또는 5516-X 모델에서 지원되지 않습니다. DTLSV1_2를 열거형 값으로 수락하도록 sslcipher 리소스의 protocolVersion 속성이 업데이트되었습니다.

기능	설명
보안성이 낮은 Diffie-Hellman 그룹, 암호화 및 해시 알고리즘에 대한 지원이 중단됨.	다음 기능은 더 이상 사용되지 않으며 향후 릴리스에서 제거될 예정입니다. 이러한 기능은 VPN에서 사용할 수 있도록 IKE 제안 또는 IPSec 정책에서 구성하지 마십시오. 이러한 기능의 사용을 중단하고 가급적 빨리 더 강력한 옵션을 사용하십시오. • Diffie-Hellman 그룹: 2, 5 및 24. • 강력한 암호화를 위한 내보내기 제어를 충족하는 사용자를 위한 암호화 알고리즘: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. 내보내기 제어를 충족하지 않는 사용자의 경우 DES는 계속 지원됩니다(유일한 옵션임). • 해시 알고리즘: MD5.
라우팅 기능	
가상 라우터 및 VRF(가상 라우팅 및 포워딩)-Lite	여러 가상 라우터를 생성하여 인터페이스 그룹에 대해 별도의 라우팅 테이블을 유지 관리할 수 있습니다. 각 가상 라우터에는 자체 라우팅 테이블이 있으므로 디바이스를 통과하는 트래픽에서 명확하게 분리하는 기능을 제공할 수 있습니다. 가상 라우터에서는 가상 라우팅 및 포워딩의 "light" 버전, 즉 VRF-Lite를 구현합니다. 이는 BGP용 멀티프로토콜 확장(MBGP)을 지원하지 않습니다. 가상 라우터를 활성화할 수 있도록 **Routing(**라우팅**)** 페이지가 변경되었습니다. 활성화된 경우, **Routing(**라우팅**)** 페이지에 가상 라우터 목록이 표시됩니다. 각 가상 라우터에 대해 별도의 고정 경로 및 라우팅 프로세스를 구성할 수 있습니다. 또한 **clear ospf**, **clear route**, **ping**, **show asp table routing**, **show bgp**, **show ipv6 route**, **show ospf**, **show route**, **show snort counters** CLI 명령에 [**vrf** *name* | **all**] 키워드 집합이 추가되었으며, 해당하는 경우 가상 라우터 정보를 나타내도록 출력이 변경되었습니다. 추가된 명령: **show vrf**
OSPF 및 BGP 구성이 Routing(라우팅) 페이지로 이동됨.	이전 릴리스에서는 Advanced Configuration(고급 구성) 페이지에서 스마트 CLI를 사용하여 OSPF 및 BGP를 구성했습니다. 여전히 스마트 CLI를 사용하여 이러한 라우팅 프로세스를 구성하기는 하지만 이제 Routing(라우팅) 페이지에서 개체를 직접 사용할 수 있습니다. 이렇게 하면 가상 라우터별로 프로세스를 더 쉽게 구성할 수 있습니다. OSPF 및 BGP Smart CLI 개체는 Advanced Configuration(고급 구성) 페이지에서 더 이상 사용할 수 없습니다. 6.6으로 업그레이드하기 전에 이러한 개체를 구성한 경우에는 업그레이드 후 Routing(라우팅) 페이지에서 해당 개체를 찾을 수 있습니다.

기능	설명
고가용성 기능	
HA(고가용성) 쌍의 스탠바이 유닛에 로그인하는 외부 인증 사용자에 대한 제한이 제거됨.	이전에는 외부에서 인증된 사용자가 HA 쌍의 스탠바이 유닛에 바로 로그인할 수 없었습니다. 사용자는 스탠바이 유닛에 로그인하려면 먼저 액티브 유닛에 로그인한 다음, 구성을 구축해야 했습니다. 이 제한은 제거되었습니다. 유효한 사용자 이름/비밀번호를 제공하는 한, 외부에서 인증된 사용자는 액티브 유닛에 로그인하지 않았어도 스탠바이 유닛에 로그인할 수 있습니다.
위협 방어 API의 BreakHAStatus 리소스에서 인터페이스를 처리하는 방식에 대한 변경 사항.	이전에는 HA(고가용성) 구성을 해제하는 디바이스에서 인터페이스의 작동 상태를 제어하기 위해 **clearIntfs** 쿼리 파라미터를 포함할 수 있었습니다. 버전 6.6부터는 clearIntfs 쿼리 파라미터 대신, 새 속성인 **interfaceOption**을 사용해야 합니다. 이 속성은 액티브 노드에서 사용되는 경우에는 선택 사항이지만, 액티브 노드가 아닌 노드에서 사용되는 경우에는 필수 사항입니다. 다음 두 가지 옵션 중 하나를 선택할 수 있습니다. • DISABLE_INTERFACES(기본값) - 스탠바이 디바이스(또는 이 디바이스)의 모든 데이터 인터페이스가 비활성화됩니다. • ENABLE_WITH_STANDBY_IP - 인터페이스에 대한 스탠바이 IP 주소를 구성한 경우, 스탠바이 디바이스(또는 이 디바이스)의 인터페이스는 스탠바이 주소를 사용하도록 재구성됩니다. 스탠바이 주소가 없는 인터페이스는 비활성화됩니다. 디바이스가 정상적인 액티브/스탠바이 상태일 때 액티브 노드에서 HA 해제를 사용하는 경우, 이 속성은 스탠바이 노드의 인터페이스에 적용됩니다. 액티브/액티브 또는 일시 중단과 같은 기타 상태일 때는 해당 속성이 해제를 시작하는 노드에 적용됩니다. clearIntfs 쿼리 파라미터를 사용하는 경우 clearIntfs=true는 interfaceOption = DISABLE_INTERFACES와 같이 작동합니다. 즉, 액티브/스탠바이 쌍을 clearIntfs=true로 해제하면 더 이상 두 디바이스가 비활성화되지 않고 스탠바이 디바이스만 비활성화됩니다. device manager를 사용하여 HA를 해제하는 경우 인터페이스 옵션은 항상 DISABLE_INTERFACES로 설정됩니다. 스탠바이 IP 주소가 있는 인터페이스는 활성화할 수 없습니다. 다른 결과를 원하는 경우 API Explorer에서 API 호출을 사용합니다.

기능	설명
고가용성 문제의 마지막 실패 사유가 이제 High Availability(고가용성) 페이지에 표시됨.	액티브 디바이스를 사용할 수 없게 되고 스탠바이 디바이스에 페일오버를 수행하는 등의 이유로 고가용성(HA)이 실패하는 경우, 이제 기본 및 보조 디바이스의 상태 정보 아래에 마지막 실패 사유가 표시됩니다. 이 정보에는 이벤트의 UTC 시간이 포함됩니다.
인터페이스 기능	
PPPoE 지원.	이제 라우팅 인터페이스에 대해 PPPoE를 구성할 수 있습니다. 고가용성 디바이스에서는 PPPoE가 지원되지 않습니다. 신규/수정된 화면: **Device(**디바이스**)** > **Interfaces(**인터페이스**)** > **Edit(**수정**)** > **IPv4 Address(IPv4** 주소**)** > **Type(**유형**)** > **PPPoE** 신규/수정된 명령: **show vpdn group, show vpdn username, show vpdn session pppoe state**
관리 인터페이스는 기본적으로 DHCP 클라이언트 역할을 함.	이제 관리 인터페이스에서는 기본적으로 192.168.45.45 IP 주소를 사용하는 대신 DHCP에서 IP 주소를 가져옵니다. 이렇게 변경하면 기존 네트워크에서 위협 방어를 더욱 쉽게 구축할 수 있습니다. 이 기능은 Firepower 4100/9300(논리적 디바이스를 구축할 때 IP 주소를 설정하는 위치)과 threat defense virtual 및 ISA 3000(여전히 192.168.45.45 IP 주소를 사용함)을 제외한 모든 플랫폼에 적용됩니다. 관리 인터페이스에서 DHCP 서버는 또한 더 이상 활성화되지 않습니다. 기본적으로 IP 주소 내부의 기본값에 계속 연결할 수 있습니다(192.168.1.1).
device manager 관리 연결을 위한 HTTP 프록시 지원.	이제 device manager 연결과 함께 사용하기 위해 관리 인터페이스에 대한 HTTP 프록시를 구성할 수 있습니다. 수동 및 예약된 데이터베이스 업데이트를 비롯한 모든 관리 연결은 프록시를 통해 진행됩니다. 설정을 구성하기 위해 **System Settings(**시스템 설정**)** > **HTTP Proxy(HTTP** 프록시**)** 페이지가 추가되었습니다. 또한 위협 방어 API에 HTTPProxy 리소스가 추가되었습니다.
관리 인터페이스에 대한 MTU 설정.	이제 관리 인터페이스의 MTU를 최대 1500바이트로 설정할 수 있습니다. 기본값은 1500바이트입니다. 신규/수정된 명령: **configure network mtu, configure network management-interface mtu-management-channel** 수정된 화면이 없습니다.
라이선싱 기능	

기능	설명
스마트 라이선싱 및 클라우드 서비스 등록은 이제 분리되어 있으므로 등록을 별도로 관리할 수 있음.	이제 스마트 라이선싱 어카운트 대신 보안 어카운트를 사용하여 클라우드 서비스에 등록할 수 있습니다. Cisco Defense Orchestrator를 사용하여 디바이스를 관리하려는 경우 보안 어카운트를 사용하여 등록하는 것이 좋습니다. 스마트 라이선싱에서 등록을 취소하지 않고 클라우드 서비스에서 등록을 취소할 수도 있습니다. **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)** 페이지가 작동하는 방식이 변경되었으며, 클라우드 서비스에서 등록을 취소하는 기능이 추가되었습니다. 또한 웹 분석 기능이 페이지에서 제거되었습니다. 이제 이 기능은 **System Settings(**시스템 설정**)** > **Web Analytics(**웹 분석**)**에서 찾을 수 있습니다. 위협 방어 API에서는 새 동작이 반영되도록 CloudServices 리소스가 수정되었습니다.
영구 라이선스 예약 지원	인터넷에 대한 경로가 없는 에어 갭(air-gapped) 네트워크를 사용할 경우, 스마트 라이선싱을 위해 CSSM(Cisco Smart Software Manager)에 직접 등록할 수 없습니다. 이러한 경우, 이제 범용 영구 라이선스 예약(PLR) 모드를 사용하여 인증을 받을 수 있습니다. 이 모드에서는 CSSM과의 직접 통신이 필요하지 않은 라이선스를 적용할 수 있습니다. 에어 갭(air-gapped) 네트워크를 사용할 경우, 어카운트 담당자에게 문의하여 CSSM 어카운트에서 범용 PLR 모드를 사용할 수 있는 권한을 요청한 후 필요한 라이선스를 확보하십시오. ISA 3000은 범용 PLR을 지원하지 않습니다. PLR 모드로 전환하고, 범용 PLR 라이선스를 취소 및 등록 해제할 수 있는 기능이**Device(**디바이스**)** > **Smart License(**스마트 라이선스**)** 페이지에 추가되었습니다. 위협 방어 API에는 PLRAuthorizationCode, PLRCode, PLRReleaseCode, PLRRequestCode를 위한 새로운 리소스, 그리고 PLRRequestCode, InstallPLRCode, CancelReservation에 대한 작업이 있습니다.
관리 및 트러블슈팅 기능	
ISA 3000 디바이스의 PTP(Precision Time Protocol) 구성에 대한 Device Manager의 직접 지원.	device manager를 사용하여 ISA 3000 디바이스에서 PTP(Precision Time Protocol)를 구성할 수 있습니다. PTP는 패킷 기반 네트워크에서 다양한 디바이스의 클록을 동기화하기 위해 개발된 시간 동기화 프로토콜입니다. 이 프로토콜은 산업용, 네트워크 측정 및 제어 시스템용으로 특별히 설계되었습니다. 이전 릴리스에서는 FlexConfig를 사용하여 PTP를 구성해야 했습니다. 동일한 System Settings(시스템 설정) 페이지에서 NTP로 PTP가 그룹화되고 **System Settings(**시스템 설정**)** > **NTP** 페이지의 이름이 **Time Services(**시간 서비스**)**로 변경되었습니다. 또한 PTP 리소스가 위협 방어 API에 추가되었습니다.

기능	설명
device manager 관리 웹 서버 인증서에 대한 신뢰 체인 검증.	device manager 웹 서버에 대해 자체 서명되지 않은 인증서를 구성하는 경우, 이제 신뢰 체인에 모든 중간 인증서와 루트 인증서를 포함해야 합니다. 시스템에서는 전체 체인을 검증합니다. **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Access(**관리 액세스**)** 페이지의 **Management Web Server(**관리 웹 서버**)** 탭에 있는 체인의 인증서를 선택하는 기능이 추가되었습니다.
백업 파일 암호화에 대한 지원	이제 비밀번호를 사용하여 백업 파일을 암호화할 수 있습니다. 암호화된 백업을 복원하려면 올바른 비밀번호를 제공해야 합니다. 반복, 예약 및 수동 작업에 대한 백업 파일의 암호화 여부를 선택하는 기능과 복구 시 비밀번호를 제공하는 기능이 **Device(**디바이스**)** > **Backup and Restore(**백업 및 복구**)** 페이지에 추가되었습니다. 또한 encryptArchive 및 encryptionKey 속성이 BackupImmediate 및 BackupSchedule 리소스에 추가되고, encryptionKey가 위협 방어 API의 RestoreImmediate 리소스에 추가되었습니다.
클라우드 서비스에서 사용할 수 있도록 Cisco Cloud에 전송할 이벤트를 선택하는 기능에 대한 지원	Cisco Cloud에 이벤트를 전송하도록 디바이스를 구성하는 경우, 이제 전송할 이벤트 유형(침입, 파일/악성코드, 연결)을 선택할 수 있습니다. 연결 이벤트의 경우 침입, 파일 또는 악성코드 이벤트를 트리거하는 연결과 관련이 있거나 보안 인텔리전스 차단 정책과 일치하는 모든 이벤트를 전송하거나 그중 우선순위가 높은 이벤트만 전송할 수 있습니다. Send Events to the Cisco Cloud Enable(Cisco Cloud로 이벤트 전송 활성화) 버튼이 작동하는 방식이 변경되었습니다. 이 기능은 **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)** 페이지에 있습니다.
위협 방어 REST API 버전 5(v5).	소프트웨어 버전 6.6용 위협 방어 REST API가 버전 5로 올라갔습니다. API URL의 v1/v2/v3/v4를 v5로 교체해야 합니다. 또는 /latest/를 사용하여 디바이스에서 지원되는 가장 최신 API 버전을 사용하고 있음을 나타내는 것이 좋습니다. v5 API에는 소프트웨어 버전 6.6에 추가된 모든 기능을 아우르는 새로운 리소스가 다수 포함되어 있습니다. 사용 중인 리소스 모델에 변경 사항이 적용되었을 수 있으므로 모든 기존 호출을 다시 평가하십시오. 리소스를 확인할 수 있는 API Explorer를 열려면 device manager에 로그인한 다음, More options(추가 옵션) 버튼(⋮)을 클릭하고 **API Explorer**를 선택합니다.

FDM 버전 6.4의 새로운 기능

표 *8: FDM* 버전 *6.4*의 새로운 기능 및 사용 중단된 기능

기능	설명
Firepower 1000 Series 디바이스 컨피그레이션	device manager를 사용하여 Firepower 1000 Series 디바이스에서 위협 방어를 구성할 수 있습니다. PoE(Power over Ethernet) 포트를 일반 이더넷 포트로 컨피그레이션 및 사용할 수 있지만 어떤 PoE 관련 속성도 활성화 또는 컨피그레이션할 수 없다는 점에 유의하십시오.
ISA 3000에 대한 하드웨어 우회	이제 **Device(**디바이스**)** > **Interfaces(**인터페이스**)** 페이지에서 ISA 3000에 대해 하드웨어 우회를 설정할 수 있습니다. 6.3 릴리스에서는 FlexConfig를 사용하여 하드웨어 우회를 컨피그레이션해야 했습니다. FlexConfig를 사용 중인 경우, 인터페이스 페이지에서 컨피그레이션을 다시 수행하고 FlexConfig에서 하드웨어 우회 명령을 제거하십시오. 그러나 FlexConfig 중에서 TCP 시퀀스 번호 임의 설정 비활성화를 전담하는 부분을 사용하실 것을 권장합니다.
device manager CLI 콘솔에서 시스템을 리부팅하고 종료하는 기능.	이제 device manager에서 CLI 콘솔을 통해 **reboot** 및 **shutdown** 명령을 실행할 수 있습니다. 이전에는 시스템을 리부팅하거나 종료하기 위해 디바이스에 대한 별도의 SSH 세션을 열어야 했습니다. 이러한 명령을 사용하려면 관리자 권한이 있어야 합니다.
위협 방어 CLI 사용자에 대해 RADIUS를 사용한 외부 인증 및 권한 부여	위협 방어 CLI에 로그인하는 사용자를 외부 RADIUS 서버를 사용해 인증하고 권한을 부여할 수 있습니다. 외부 사용자에게는 컨피그레이션(관리자) 또는 기본(읽기 전용) 액세스 권한을 부여할 수 있습니다. **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Access(**관리 액세스**)** 페이지에 있는 **AAA Configuration(AAA** 설정**)** 탭에 SSH 설정을 추가했습니다.
네트워크 범위 개체 및 중첩 네트워크 그룹 개체에 대한 지원	이제 IPv4 또는 IPv6 주소의 범위를 지정하는 네트워크 개체와 다른 네트워크 그룹(즉 중첩된 그룹)을 포함하는 네트워크 그룹 개체를 만들 수 있습니다. 이러한 기능을 포함하도록 네트워크 개체 및 네트워크 그룹 개체 추가/수정 대화 상자를 수정하였고, 이 개체를 해당 유형의 주소 사양이 정책의 컨텍스트 내에서 의미가 통하는지 여부에 따라 사용할 수 있도록 여러 가지 보안 정책을 수정했습니다.

기능	설명
개체 및 규칙에 대한 전체 텍스트 검색 옵션	개체 및 규칙과 관련해 전체 텍스트 검색을 수행할 수 있습니다. 다수의 항목이 있는 정책 또는 개체 목록을 검색하여 규칙 또는 개체 내 어디서든지 검색 문자열을 포함하는 항목을 모두 찾을 수 있습니다. 규칙이 있는 모든 정책과 **Objects(**개체**)** 목록의 모든 페이지에 검색 상자를 추가했습니다. 뿐만 아니라 API에서 지원되는 개체에 대해 GET 호출의 **filter=fts~***search-string(*검색 문자열*)* 옵션을 사용하여 전체 텍스트 검색으로 항목을 조회할 수 있습니다.
device manager 관리형 위협 방어 디바이스용으로 지원되는 API 버전 목록 조회.	GET/api/버전(ApiVersions) 메서드를 사용해 디바이스에서 지원되는 API 버전의 목록을 얻을 수 있습니다. API 클라이언트를 사용하면 지원되는 모든 버전에 유효한 명령 및 구문을 통해 디바이스와 통신하고 디바이스를 컨피그레이션할 수 있습니다.
액세스 제어 규칙에 대한 적중 횟수	이제 액세스 제어 규칙에 대한 적중 횟수를 볼 수 있습니다. 적중 횟수는 연결이 규칙과 얼마나 자주 일치했는지 나타냅니다. 적중 횟수 정보를 포함하도록 액세스 제어 정책을 업데이트했습니다. 위협 방어 API에서 GET 액세스 정책 규칙 리소스에 HitCounts 리소스와 **includeHitCounts** 및 **filter=fetchZeroHitCounts** 옵션을 추가했습니다.
동적 주소 지정 및 인증서 인증을 위한 Site-to-Site VPN 개선 사항	이제는 사전 공유 키 대신 인증서를 사용하도록 Site-to-Site VPN 연결을 컨피그레이션하여 피어를 인증할 수 있습니다. 또한 원격 피어에 알 수 없는(동적) IP 주소가 있는 연결을 컨피그레이션할 수 있습니다. Site-to-Site VPN 마법사 및 IKEv1 정책 개체에 옵션을 추가했습니다.
원격 액세스 VPN의 RADIUS 서버 및 권한 부여 변경에 대한 지원	이제 원격 액세스 VPN(RA VPN) 사용자에 대한 인증, 권한 부여 및 과금을 위해 RADIUS 서버를 사용할 수 있습니다. Cisco ISE RADIUS 서버를 사용하는 경우, '동적 권한 부여'라고도 하는 CoA(Change of Authentication)를 컨피그레이션하여 인증 후에 사용자의 권한을 변경할 수도 있습니다. RADIUS 서버 및 서버 그룹 개체에 속성을 추가했으며, RA VPN 연결 프로파일 내에서 RADIUS 서버 그룹을 선택할 수 있게 했습니다.
원격 액세스 VPN에 대한 다중 연결 프로파일 및 그룹 정책	하나 이상의 연결 프로파일을 컨피그레이션할 수 있고, 프로파일에 사용할 그룹 정책을 생성할 수 있습니다. 연결 프로파일 및 그룹 정책에 대한 별도 페이지를 갖도록 **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)** 페이지를 변경하고 그룹 정책을 선택할 수 있도록 RA VPN 연결 마법사를 업데이트했습니다. 이전에는 마법사에서 컨피그레이션하던 일부 항목을 이제는 그룹 정책에서 컨피그레이션합니다.

기능	설명
인증서 기반 2차 인증 소스와 원격 액세스 VPN의 이중 인증에 대한 지원	사용자 인증에 인증서를 사용할 수 있고, 2차 인증 소스를 컨피그레이션하여 사용자가 연결을 설정하기 전에 두 번 인증하게 할 수 있습니다. RSA 토큰 또는 이중 암호를 두 번째 요소로 사용하여 이중 인증을 컨피그레이션할 수도 있습니다. 이러한 추가 옵션의 컨피그레이션을 지원하기 위해 RA VPN 연결 마법사를 업데이트했습니다.
원격 액세스 VPN에 대해 주소 범위가 여러 개인 IP 주소 풀 및 DHCP 주소 풀 지원	이제 서브넷을 지정하는 여러 네트워크 개체를 선택하여 주소 범위가 하나 이상인 주소 풀을 컨피그레이션할 수 있습니다. 뿐만 아니라 DHCP 서버에서 주소 풀을 컨피그레이션하고, 이 서버를 사용하여 RA VPN 클라이언트에 주소를 제공할 수 있습니다. 권한 부여를 위해 RADIUS를 사용하는 경우에는 그 대신에 RADIUS 서버에서 주소 풀을 컨피그레이션할 수도 있습니다. 이러한 추가 옵션의 컨피그레이션을 지원하기 위해 RA VPN 연결 마법사를 업데이트했습니다. 선택 사항으로 연결 프로파일 대신에 그룹 정책에서 주소 풀을 컨피그레이션할 수 있습니다.
Active Directory 영역 개선 사항	이제 단일 영역에 최대 10개의 이중화 AD(Active Directory) 서버를 포함할 수 있습니다. 또한 여러 영역을 생성하고 더 이상 필요 없는 영역을 삭제할 수 있습니다. 뿐만 아니라 한 영역에서 다운로드할 수 있는 사용자 한도가 이전 릴리스의 2,000명에서 50,000명으로 증가했습니다. 여러 영역 및 서버를 지원하기 위해 **Objects(**개체**)** > **Identity Sources(ID** 소스**)** 페이지를 업데이트했습니다. 액세스 제어 및 SSL 암호 해독 규칙의 사용자 기준에서 영역을 선택하여 이 규칙을 영역 내 모든 사용자에게 적용할 수 있습니다. ID 규칙 및 RA VPN 연결 프로파일에서 영역을 선택할 수도 있습니다.
ISE 서버에 대한 이중화 지원	Cisco ISE(Identity Services Engine)를 수동 인증용 ID 소스로 컨피그레이션하면 ISE 고가용성 설정이 되어 있는 경우 보조 ISE 서버를 컨피그레이션할 수 있습니다. 보조 서버에 대한 속성을 ISE ID 개체에 추가했습니다.
외부 syslog 서버로 전송된 파일/악성코드 이벤트	이제 액세스 제어 규칙에 컨피그레이션된 파일 정책에서 생성되는 파일/악성코드 이벤트를 수신하도록 외부 syslog 서버를 컨피그레이션할 수 있습니다. 파일 이벤트에서 사용하는 메시지 ID는 430004이고, 악성코드 이벤트의 경우는 430005입니다. **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Logging Settings(**기록 설정**)** 페이지에 파일/악성코드 syslog 서버 옵션을 추가했습니다.

기능	설명
내부 버퍼에 대한 기록과 사용자 정의 이벤트 로그 필터에 대한 지원	이제 내부 버퍼를 시스템 기록의 대상으로 컨피그레이션할 수 있습니다. 뿐만 아니라 이벤트 로그 필터를 생성하여 syslog 서버 및 내부 버퍼 기록 대상에 대해 어떤 메시지를 생성할지 사용자 정의할 수 있습니다. **Objects(**개체**)** 페이지에 이벤트 로그 필터 개체를 추가하고 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Logging Settings(**기록 설정**)** 페이지에서 이 개체를 사용할 수 있는 기능을 추가했습니다. 내부 버퍼 옵션도 **Logging Settings(**기록 설정**)** 페이지에 추가했습니다.
device manager 웹 서버에 대한 인증서.	이제 device manager 컨피그레이션 인터페이스에 대한 HTTPS 연결에 사용되는 인증서를 구성할 수 있습니다. 웹 브라우저에서 이미 신뢰하는 인증서를 업로드하면 기본 내부 인증서를 사용할 때 신뢰할 수 없는 기관 메시지를 받지 않을 수 있습니다. **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Access(**관리 액세스**)** > **Management Web Server(**관리 웹 서버**)** 페이지를 추가했습니다.
Cisco Threat Response 지원	Cisco Threat Response 클라우드 기반 애플리케이션에 침입 이벤트를 전송하도록 시스템을 컨피그레이션할 수 있습니다. Cisco Threat Response를 사용해 침입을 분석할 수 있습니다. Cisco Threat Response를 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)** 페이지에 추가했습니다.
VDB, GeoDB, SRU 업데이트를 수동으로 업로드.	이제 VDB, 지리위치 데이터베이스, 침입 규칙에 대한 업데이트 패키지를 수동으로 검색한 후 FDM을 사용하여 이를 워크스테이션에서 FTD 디바이스로 업로드할 수 있습니다. 예를 들어 에어 갭(air-gapped) 네트워크에서 FDM이 Cisco Cloud로부터 업데이트를 검색할 수 없는 경우, 이제는 필요한 업데이트 패키지를 가져올 수 있습니다. 워크스테이션에서 파일을 선택하고 업로드할 수 있도록 **Device(**디바이스**)** > **Updates(**업데이트**)** 페이지가 업데이트되었습니다. 최소 FTD: 6.4.0.10 버전 제한: 이 기능은 6.5 버전에서 사용할 수 없습니다. 버전 6.6에서는 지원이 반환됩니다.

기능	설명
메모리가 적은 디바이스의 경우 VDB가 작아짐.	VDB 363 이상의 경우 시스템은 이제 메모리가 적은 디바이스에 더 작은 VDB(*VDB lite*라고도 함)를 설치합니다. 더 작은 VDB에는 동일한 애플리케이션이 포함되어 있지만, 탐지 패턴이 더 적습니다. 더 작은 VDB를 사용하는 디바이스는 전체 VDB를 사용하는 디바이스에 비해 일부 애플리케이션 식별을 누락할 수 있습니다. 최소 FTD: 6.4.0.17 더 낮은 메모리 디바이스: ASA-5508-X, ASA-5515-X, ASA-5516-X, ASA-5525-X, ASA-5545-X 버전 제한: 더 작은 VDB는 모든 버전에서 지원되지 않습니다. 지원되는 버전에서 지원되지 않는 버전으로 업그레이드할 경우 메모리가 적은 디바이스에 363 이상 VDB를 설치할 수 없습니다. 영향을 받는 릴리스의 목록은 CSCwd88641을 참조하십시오.
범용 영구 라이선스 예약(PLR) 모드.	인터넷에 대한 경로가 없는 에어 갭(air-gapped) 네트워크를 사용할 경우, 스마트 라이선싱을 위해 CSSM(Cisco Smart Software Manager)에 직접 등록할 수 없습니다. 이러한 경우, 이제 범용 영구 라이선스 예약(PLR) 모드를 사용하여 인증을 받을 수 있습니다. 이 모드에서는 CSSM과의 직접 통신이 필요하지 않은 라이선스를 적용할 수 있습니다. 에어 갭(air-gapped) 네트워크를 사용할 경우, 어카운트 담당자에게 문의하여 CSSM 어카운트에서 범용 PLR 모드를 사용할 수 있는 권한을 요청한 후 필요한 라이선스를 확보하십시오. PLR 모드로 전환하고, 범용 PLR 라이선스를 취소 및 등록 해제할 수 있는 기능이 **Device(**디바이스**) > Smart License(**스마트 라이선스**)** 페이지에 추가되었습니다. FTD API에는 PLRAuthorizationCode, PLRCode, PLRReleaseCode, PLRRequestCode를 위한 새로운 리소스, 그리고 PLRRequestCode, InstallPLRCode, CancelReservation에 대한 작업이 있습니다. 최소 FTD: 6.4.0.10. 이 기능은 버전 6.5에서 일시적으로 사용되지 않지만 버전 6.6에서 반환됩니다. 버전 6.4.0.10 이상 패치를 실행하는 경우, 버전 6.6 이상으로 직접 업그레이드하는 것이 좋습니다.

기능	설명
기본 HTTPS 서버 인증서.	업그레이드 영향. 패치를 적용하면 디바이스의 현재 기본 HTTPS 서버 인증서가 갱신될 수 있습니다. 인증서는 다음과 같이 생성된 시기에 따라 만료되도록 설정됩니다. • 6.5.0.5 이상: 800일 • 6.5.0~6.5.0.4: 3년 • 6.4.0.9 이상 패치: 800일 • 6.4.0~6.4.0.8: 3년 • 6.3.0 및 모든 패치: 3년 • 6.2.3: 20년
새로운 시스템 로그 필드.	이 새로운 시스템 로그 필드는 고유한 연결 이벤트를 종합적으로 식별합니다. • 센서 UUID • 첫 번째 패킷 시간 • 연결 인스턴스 ID • 연결 카운터 이 필드는 침입, 파일, 악성코드 이벤트에 대한 시스템 로그에도 나타나므로 연결 이벤트가 해당 이벤트와 연결될 수 있도록 합니다. 최소 FTD: 6.4.0.4
Threat Defense REST API 버전 3(v3)	소프트웨어 버전 6.4용 위협 방어 REST API가 버전 3으로 상승했습니다. 그러므로 API URL의 v1/v2를 v3으로 교체해야 합니다. v3 API에는 소프트웨어 버전 6.4에 추가된 모든 기능을 아우르는 새로운 리소스가 다수 포함되어 있습니다. 사용 중인 리소스 모델에 변경 사항이 적용되었을 수 있으므로 모든 기존 호출을 다시 평가하십시오. 리소스를 확인할 수 있는 API Explorer를 열려면 로그인한 후 device manager URL 끝부분을 **/#/api-explorer**로 변경하십시오.

FDM 버전 6.3의 새로운 기능

표 *9: FDM* 버전 *6.3*의 새로운 기능 및 사용 중단된 기능

기능	설명
고가용성 컨피그레이션.	두 디바이스를 액티브/스탠바이 고가용성 쌍으로 구성할 수 있습니다. 고가용성 또는 페일오버 설정에서는 두 디바이스가 조인하므로 기본 디바이스에 장애가 발생하면 보조 디바이스가 대신 작동할 수 있습니다. 그러면 디바이스 장애 시 네트워크를 계속 운영하는 데 도움이 됩니다. 두 디바이스는 모델, 번호, 인터페이스 유형이 같아야 하며 동일한 소프트웨어 버전을 사용해야 합니다. **Device(**디바이스**)** 페이지에서 고가용성을 구성할 수 있습니다.
패시브 사용자 ID 획득 지원.	패시브 인증을 사용하기 위해 ID 정책을 구성할 수 있습니다. 패시브 인증은 사용자에게 사용자 이름 및 비밀번호를 요구하지 않고 사용자 ID를 수집합니다. 시스템은 지정하는 ID 소스에서 매핑을 가져옵니다. 이는 Cisco ISE(Identity Services Engine)/Cisco ISE PIC(Identity Services Engine Passive Identity Connector) 또는 원격 액세스 VPN 사용자의 로그인일 수 있습니다. 변경 사항에는 **Policies(**정책**)** > **Identity(ID)**에서 지원하는 패시브 인증 규칙과 **Objects(**개체**)** > **Identity Sources(ID** 소스**)**의 ISE 설정이 포함됩니다.
원격 액세스 VPN 및 사용자 ID에 대한 로컬 사용자 지원.	이제 device manager를 통해 사용자를 직접 생성할 수 있습니다. 그런 다음 이러한 로컬 사용자 어카운트를 사용하여 원격 액세스 VPN으로의 연결을 인증할 수 있습니다. 로컬 사용자 데이터베이스는 기본 또는 대체 인증 소스로 사용할 수 있습니다. 또한 로컬 사용자 이름을 대시보드에 반영하고 정책에서 트래픽 일치에 사용할 수 있도록 ID 정책에서 패시브 인증 규칙을 구성할 수도 있습니다. **Objects(**개체**)** > **Users(**사용자**)** 페이지가 추가되었으며, 대체 옵션을 포함하도록 원격 액세스 VPN 마법사가 업데이트되었습니다.
액세스 제어 정책에서 VPN 트래픽 처리를 위한 기본 동작을 변경함(**sysopt connection permit-vpn**).	액세스 제어 정책에서 VPN 트래픽을 처리하는 방식의 기본 동작을 변경했습니다. 6.3부터는 모든 VPN 트래픽을 액세스 제어 정책에서 처리하도록 기본 설정됩니다. 이를 통해 URL 필터링, 침입 방지, 파일 정책 등 고급 검사를 VPN 트래픽에 적용할 수 있습니다. VPN 트래픽을 허용하도록 액세스 제어 규칙을 컨피그레이션하십시오. 또는 FlexConfig를 사용하여 VPN에서 종료한 트래픽에 대해 액세스 제어 정책 및 모든 고급 검사를 우회하도록 시스템에 지시하는 **sysopt connection permit-vpn** 명령을 컨피그레이션할 수 있습니다.

기능	설명
FQDN 기반 네트워크 개체 지원 및 DNS 조회에 대한 데이터 인터페이스 지원.	이제 고정 IP 주소가 아닌 FQDN(Fully Qualified Domain Name)으로 호스트를 지정하는 네트워크 개체와 그룹을 생성할 수 있습니다. 시스템은 FQDN-IP 주소 매핑에서 액세스 제어 규칙에 사용되는 FQDN 개체를 주기적으로 조회합니다. 이러한 개체는 액세스 제어 규칙에서만 사용할 수 있습니다. 개체 페이지에 DNS 그룹 개체가 추가되었고, 데이터 인터페이스에 대한 그룹 할당을 허용하도록 **System Settings(**시스템 설정**)** > **DNS Server(DNS** 서버**)** 페이지가 변경되었으며, FQDN 네트워크 개체 선택을 허용하도록 액세스 제어 규칙이 변경되었습니다. 또한 관리 인터페이스용 DNS 컨피그레이션은 이제 설정된 DNS 서버 주소 목록 대신 DNS 그룹을 사용합니다.
TCP syslog 및 관리 인터페이스를 통한 진단 syslog 메시지 전송 기능 지원.	이전 릴리스에서는 진단 syslog 메시지가 연결 및 침입 메시지와 달리 항상 데이터 인터페이스를 사용했습니다. 이제는 모든 메시지가 관리 인터페이스를 사용하도록 syslog를 구성할 수 있습니다. 최종 소스 IP 주소는 관리 인터페이스의 게이트웨이로 데이터 인터페이스를 사용하는지 여부에 따라 달라집니다. 데이터 인터페이스를 사용하는 경우 IP 주소는 데이터 인터페이스의 주소가 됩니다. 프로토콜로 UDP 대신 TCP를 사용하도록 syslog를 구성할 수도 있습니다. **Objects(**개체**)** > **Syslog Servers(Syslog** 서버**)**에서 syslog 서버의 Add/Edit(추가/편집) 대화 상자가 변경되었습니다.
device manager 사용자에 대해 RADIUS를 사용한 외부 인증 및 권한 부여.	device manager에 로그인하는 사용자를 외부 RADIUS 서버를 사용해 인증하고 권한을 부여할 수 있습니다. 외부 사용자에게 관리, 읽기-쓰기 또는 읽기 전용 액세스 권한을 부여할 수 있습니다. Device Manager는 5개의 동시 로그인을 지원할 수 있습니다. 6번째 세션은 가장 오래된 세션을 자동으로 로그오프합니다. 필요한 경우 device manager 사용자 세션을 강제로 종료할 수 있습니다. 개체를 설정할 수 있도록 **Objects(**개체**)** > **Identity Sources(ID** 소스**)** 페이지에 RADIUS 서버 및 RADIUS 서버 그룹 개체가 추가되었습니다. 서버 그룹 사용을 활성화할 수 있도록 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Access(**관리 액세스**)**에 **AAA Configuration(AAA** 설정**)** 탭이 추가되었습니다. 또한 **Monitoring(**모니터링**)** > **Sessions(**세션**)** 페이지에는 활성 사용자가 나열되며, 관리 사용자가 세션을 종료할 수 있습니다.
보류 중인 변경 사항 보기 및 구축 개선 사항.	구축되지 않을 보류 중인 변경 사항을 더욱 명확하게 확인할 수 있도록 구축 창이 변경되었습니다. 또한 이제는 변경 사항을 취소하고, 클립보드에 복사하고, YAML 형식 파일에 다운로드하는 옵션도 제공됩니다. 감사 로그에서 더 쉽게 찾을 수 있도록 구축 작업의 이름을 지정할 수도 있습니다.

기능	설명
감사 로그.	구축, 시스템 작업, 컨피그레이션 변경 사항, 관리 사용자 로그인 및 로그아웃 등의 이벤트를 기록하는 감사 로그를 확인할 수 있습니다. **Device(**디바이스**)** > **Device Administration(**디바이스 관리**)** > **Audit Log(**로그 감사**)** 페이지를 추가했습니다.
컨피그레이션을 내보내는 기능.	보관을 위해 디바이스 컨피그레이션의 복사본을 다운로드할 수 있습니다. 그러나 이 컨피그레이션을 디바이스로 가져올 수는 없습니다. 이 기능은 백업/복원 대신 제공되는 것이 아닙니다. **Device(**디바이스**)** > **Device Administration(**디바이스 관리**)** > **Download Configuration(**설정 다운로드**)** 페이지가 추가되었습니다.
알 수 없는 URL에 대한 URL 필터링 개선 사항.	액세스 제어 규칙에서 카테고리 기반 URL 필터링을 수행하는 경우 URL 데이터베이스에 카테고리와 평판이 정의되어 있지 않은 URL에 사용자가 액세스할 수 있습니다. 이전에는 Cisco CSI(Collective Security Intelligence)에서 이러한 URL에 대해 카테고리와 평판을 조회하는 옵션을 수동으로 활성화해야 했습니다. 이제는 이 옵션이 기본적으로 활성화됩니다. 또한 이제는 시스템이 알 수 없는 URL 각각에 대해 카테고리/평판을 새로 고칠 수 있도록 조회 결과에 대해 TTL(Time to Live)을 설정할 수 있습니다. **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **URL Filtering Preferences(URL** 필터링 환경 설정**)** 페이지가 업데이트되었습니다.
이제 보안 인텔리전스 기록이 기본적으로 활성화됨.	보안 인텔리전스 정책은 기본적으로 기록이 비활성화된 상태로 6.2.3에 도입되었습니다. 6.3.0부터는 기록이 기본적으로 활성화되어 있습니다. 6.2.3에서 업그레이드할 경우, 기록 설정은 활성화 또는 비활성화 상태가 보존됩니다. 정책 시행 결과를 확인하려면 기록을 활성화하십시오.
패시브 모드 인터페이스.	인터페이스를 패시브 모드로 구성할 수 있습니다. 인터페이스는 패시브 방식으로 작동할 때 스위치 자체(하드웨어 디바이스의 경우) 또는 프로미스큐어스 VLAN(threat defense virtual의 경우)에 구성된 모니터링 세션에서 소스 포트의 트래픽만 모니터링합니다. 패시브 모드를 사용하면 threat defense virtual 디바이스를 활성 방화벽으로 구축하는 경우 해당 디바이스가 동작하는 방식을 평가할 수 있습니다. 위협에 대해서는 알고 싶지만 디바이스가 위협을 능동적으로 차단하게 하지 않으려는 상태에서 IDS(Intrusion Detection System) 서비스가 필요한 경우, 프로덕션 네트워크에서도 패시브 인터페이스를 사용할 수 있습니다. 물리적 인터페이스를 수정할 때와 보안 영역을 생성할 때 패시브 모드를 선택할 수 있습니다.

기능	설명
OSPF용 스마트 CLI 개선 사항 및 BGP 지원.	스마트 CLI OSPF 컨피그레이션이 개선되었습니다. 개선된 사항으로는 표준/확장 ACL에 사용하는 새로운 스마트 CLI 개체 유형, 경로 맵, AS 경로 개체, IPv4 및 IPv6 접두사 목록, 정책 목록, 표준/확장 커뮤니티 목록 등이 포함됩니다. 또한 이제는 스마트 CLI를 사용하여 BGP 라우팅을 구성할 수 있습니다. 이러한 기능은 **Device(**디바이스**)** > **Advanced Configuration(**고급 설정**)** 페이지에서 확인할 수 있습니다.
지원 중단된 FlexConfig 명령.	다음 FlexConfig 명령의 지원이 중단되었습니다. • **access-list**: 이제 스마트 CLI 확장 액세스 목록 또는 표준 액세스 목록 개체를 사용하여 **extended** 및 **standard** 액세스 목록을 생성할 수 있습니다. 그런 다음, 서비스 정책 트래픽 클래스용 확장 ACL을 사용하는 **match access-list** 등의 개체 이름으로 ACL을 참조하는 FlexConfig 지원 명령에서 이러한 ACL을 사용할 수 있습니다. • **as-path**: 이제 스마트 CLI AS 경로 개체를 생성한 다음, 스마트 CLI BGP 개체에 이를 사용하여 자동 시스템 경로 필터를 구성할 수 있습니다. • **community-list**: 이제 스마트 CLI 확장 커뮤니티 목록 또는 표준 커뮤니티 목록 개체를 생성한 다음, 스마트 CLI BGP 개체에 이를 사용하여 커뮤니티 목록 필터를 구성할 수 있습니다. • **dns-group**: 이제 **Objects(**개체**)** > **DNS Groups(DNS** 그룹**)**를 사용하여 DNS 그룹을 구성한 다음, **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **DNS Server(DNS** 서버**)**를 사용하여 그룹을 할당할 수 있습니다. • **policy-list**: 이제 스마트 CLI 정책 목록 개체를 생성한 다음, 스마트 CLI BGP 개체에 이를 사용하여 정책 목록을 구성할 수 있습니다. • **prefix-list**: 이제 스마트 CLI IPv4 접두사 목록 개체를 생성한 다음, 스마트 CLI OSPF 또는 BGP 개체에 이를 사용하여 IPv4용 접두사 목록 필터링을 구성할 수 있습니다. • **route-map**: 이제 스마트 CLI 경로 맵 개체를 생성한 다음, 스마트 CLI OSPF 또는 BGP 개체에 이를 사용하여 경로 맵을 구성할 수 있습니다. • **router bgp**: 이제 BGP용 스마트 CLI 템플릿을 사용할 수 있습니다.

기능	설명
ISA 3000 디바이스에 대한 개선 사항.	이제 ISA 3000에서 알람, 하드웨어 바이패스, SD 카드를 사용한 백업 및 복원 기능을 구성할 수 있습니다. FlexConfig를 사용하여 알람 및 하드웨어 바이패스를 구성할 수 있습니다. SD 카드의 경우 device manager의 백업/복원 페이지가 업데이트되었습니다.
ASA 5506-X, 5506W-X, 5506H-X 및 5512-X 지원 종료(위협 방어 6.3부터)	ASA 5506-X, 5506W-X, 5506H-X 및 5512-X에는 위협 방어 6.3 또는 후속 릴리스를 설치할 수 없습니다. 이러한 플랫폼에 대해 지원되는 최종 위협 방어 릴리스는 6.2.3입니다.
VMware vSphere/VMware ESXi 5.5에 대한 지원 제거.	버전 6.3에서는 VMware vSphere/VMware ESXi 6.0에서 FTDv의 지원을 중단합니다. FTD를 업그레이드하기 전에 호스트 환경을 지원되는 버전으로 업그레이드합니다.
Cisco에 제품 사용량 정보를 제공하는 웹 분석.	페이지 조회 수를 기반으로 익명 제품 사용량 정보를 Cisco에 제공하는 웹 분석을 활성화할 수 있습니다. Cisco는 이 정보를 활용해 기능 사용 패턴을 확인하고 제품을 개선할 수 있습니다. 모든 사용량 데이터는 익명으로 전송되며 민감한 데이터는 전송되지 않습니다. 웹 분석은 기본적으로 활성화됩니다. 웹 분석이 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)** 페이지에 추가되었습니다.
VDB(Vulnerability Database) 업데이트를 설치해도 더 이상 Snort가 재시작되지 않음.	VDB 업데이트를 설치할 때 설치 과정 자체에서는 더 이상 Snort가 재시작되지 않습니다. 그러나 다음 컨피그레이션 구축 중에는 Snort가 계속 재시작됩니다.
침입 규칙(SRU) 데이터베이스 업데이트를 구축해도 더 이상 Snort가 재시작되지 않음.	침입 규칙(SRU) 업데이트를 설치한 후에는 컨피그레이션을 구축하여 새 규칙을 활성화해야 합니다. SRU 업데이트를 구축해도 더 이상 Snort가 재시작되지 않습니다.
EMS 확장 지원.	업그레이드 영향**.** 버전 6.3.0에서는 버전 6.2.3.8/6.2.3.9에서 도입된 EMS 확장 지원을 일시적으로 중단합니다. 즉 **Decrypt-Resign(**암호 해독 - 다시 서명**)** 및 **Decrypt-Known Key(**암호 해독 - 알려진 키**)** SSL 정책 동작은 이제 통신 보안을 강화하던 ClientHello 협상 중 EMS 확장을 일시적으로 지원하지 않습니다. EMS 확장은 RFC 7627에 의해 정의됩니다. 버전 6.3.0.1에서는 지원이 반환됩니다.

기능	설명
위협 방어 REST API 버전 2(v2).	소프트웨어 버전 6.3용 위협 방어 REST API가 버전 2로 올라갔습니다. 그러므로 API URL의 v1을 v2로 교체해야 합니다. v2 API에는 소프트웨어 버전 6.3에 추가된 모든 기능을 아우르는 새로운 리소스가 다수 포함되어 있습니다. 사용 중인 리소스 모델에 변경 사항이 적용되었을 수 있으므로 모든 기존 호출을 다시 평가하십시오. 리소스를 확인할 수 있는 API Explorer를 열려면 로그인한 후 device manager URL 끝부분을 **/#/api-explorer**로 변경하십시오.

FDM 버전 6.2.3의 새로운 기능

표 ***10: FDM*** 버전 ***6.2.3***의 새로운 기능 및 사용 중단된 기능

기능	설명
SSL/TLS 암호 해독	연결의 콘텐츠를 검사할 수 있도록 SSL/TLS 연결을 암호 해독할 수 있습니다. 암호 해독을 사용하지 않으면 암호화된 연결을 효과적으로 검사하여 침입 및 악성코드 위협을 식별하거나 URL 및 애플리케이션 사용 정책을 준수할 수 없습니다. **Policies(**정책**)** > **SSL Decryption(SSL** 암호 해독**)** 페이지와 **Monitoring(**모니터링**)** > **SSL Decryption(SSL** 암호 해독**)** 대시보드가 추가되었습니다. 주의 활성 인증을 구현하는 ID 정책은 SSL 암호 해독 규칙을 자동으로 생성합니다. SSL 암호 해독을 지원하지 않는 릴리스에서 업그레이드하는 경우, 이 유형의 규칙을 사용하면 SSL 암호 해독 정책이 자동으로 활성화됩니다. 그러나 업그레이드를 완료하고 나면 재서명 암호 해독 규칙에 사용할 인증서를 지정해야 합니다. 업그레이드 후 즉시 SSL 암호 해독 설정을 수정하십시오.
보안 인텔리전스 차단.	새로운 **Policies(**정책**)** > **Security Intelligence(**보안 인텔리전스**)** 페이지에서는 보안 인텔리전스 정책을 설정할 수 있으며, 이 정책을 사용하여 소스/대상 IP 주소 또는 대상 URL을 기준으로 원치 않는 트래픽을 삭제할 수 있습니다. 모든 허용된 연결은 계속해서 액세스 제어 정책을 통해 평가되고 결과적으로 삭제될 수도 있습니다. 보안 인텔리전스를 사용하려면 Threat(위협) 라이선스를 활성화해야 합니다. 또한, **Policies(**정책**)** 대시보드의 이름이 **Access And SI Rules(**액세스 및 **SI** 규칙**)**로 변경되었으며 현재 해당 대시보드에는 액세스 규칙뿐만 아니라 보안 인텔리전스 규칙에 상응하는 규칙이 포함되어 있습니다.

기능	설명
침입 규칙 조정	액세스 제어 규칙과 함께 적용하는 사전 정의된 침입 정책 내에서 침입 규칙에 대한 작업을 변경할 수 있습니다. 이벤트(알림) 일치 트래픽을 삭제하거나 생성하기 위한 규칙을 각각 구성하거나 규칙을 비활성화할 수 있습니다. 활성화된 규칙(삭제하거나 알리도록 설정된 규칙)에 대한 작업만 변경할 수 있으며, 기본적으로 비활성화된 규칙은 활성화할 수 없습니다. 침입 규칙을 조정하려면 **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.
침입 정책을 기반으로 한 자동 NAP(네트워크 분석 정책) 할당	이전 릴리스에서는 항상 Balanced Security and Connectivity(보안과 연결의 균형 유지) 네트워크 분석 정책이 특정 소스/대상 보안 영역과 네트워크 개체 조합에 할당된 침입 정책과 관계없이 전처리기 설정에 사용되었습니다. 이제는 시스템에서 자동으로 NAP 규칙을 생성하여 이러한 기준을 기반으로 동일한 이름의 NAP 및 침입 정책을 트래픽에 할당합니다. 레이어 4 또는 7 기준을 사용하여 트래픽(다른 방법을 사용하면 동일한 소스/대상 보안 영역 및 네트워크 개체와 일치하는 트래픽)에 다른 침입 정책을 할당하는 경우, NAP 정책과 침입 정책이 완벽히 일치하지 않게 됩니다. 맞춤형 네트워크 분석 정책은 생성할 수 없습니다.
Threats(위협), Attackers(공격자), Targets(대상) 대시보드에 대한 드릴다운 보고서	이제 Threats(위협), Attackers(공격자) Targets(대상) 대시보드를 클릭하여 보고된 항목에 대한 자세한 정보를 확인할 수 있습니다. 이러한 대시보드는 Monitoring(모니터링) 페이지에서 사용할 수 있습니다. 이러한 새로운 보고서 때문에 6.2.3 이전 릴리스를 업그레이드할 때 이러한 대시보드에 대한 보고 데이터가 손실됩니다.
Web Applications(웹 애플리케이션) 대시보드	새로운 Web Applications(웹 애플리케이션) 대시보드에는 네트워크에서 가장 많이 사용되고 있는 웹 애플리케이션(예: Google)이 표시됩니다. 이 대시보드는 프로토콜 지향 정보(예: HTTP 사용량)를 제공하는 Applications(애플리케이션) 대시보드를 보완합니다.
새로운 Zones(영역) 대시보드가 Ingress Zone(인그레스 영역) 및 Egress Zone(이그레스 영역) 대시보드를 대체	새로운 Zones(영역) 대시보드에는 트래픽이 디바이스로 들어왔다가 나가는 데 가장 많이 사용되는 보안 영역 쌍이 표시됩니다. 이 대시보드는 인그레스 및 이그레스 영역에 대한 별도의 대시보드를 대체합니다.
새로운 Malware(악성코드) 대시보드	새로운 Malware(악성코드) 대시보드에는 가장 많이 사용되는 악성코드 작업 및 상태의 조합이 표시됩니다. 드릴다운하여 연결된 파일 유형에 대한 정보를 확인할 수 있습니다. 이 정보를 보려면 액세스 규칙에 대한 파일 정책을 구성해야 합니다.

기능	설명
자체 서명된 내부 인증서 및 내부 CA 인증서.	이제 자체 서명된 내부 ID 인증서를 생성할 수 있습니다. 또한, SSL 암호 해독 정책에 사용할 자체 서명된 내부 CA 인증서를 업로드하거나 생성할 수 있습니다. 이러한 기능은 **Objects(**개체**)** > **Certificates(**인증서**)** 페이지에서 설정합니다.
인터페이스 속성 편집 시 DHCP 서버 설정을 편집하는 기능	이제 인터페이스 속성을 수정하면서 동시에 인터페이스에 구성되어 있는 DHCP 서버의 설정을 수정할 수 있습니다. 이렇게 하면 인터페이스 IP 주소를 다른 서브넷으로 변경해야 하는 경우 DHCP 주소 풀을 재정의하기 쉽습니다.
Cisco Success Network에서 제품을 개선하고 효과적인 기술 지원을 제공하는 데 도움이 되도록 Cisco에 사용량 및 통계 데이터 전송.	Cisco Success Network에 연결하여 Cisco에 데이터를 보낼 수 있습니다. Cisco Success Network를 활성화하면 Cisco가 기술 지원을 제공하는 데 필수적인 사용량 정보 및 통계를 Cisco에 보내게 됩니다. 또한, 이 정보를 통해 Cisco는 제품을 개선할 수 있으며 사용 가능하지만 사용되지 않은 기능을 알려 네트워크의 제품 가치를 최대화하도록 할 수 있습니다. 연결은 디바이스를 Cisco Smart Software Manager에 등록하는 경우 활성화하거나 선택에 따라 나중에 활성화할 수 있으며, 언제든지 비활성화할 수 있습니다. Cisco Success Network는 클라우드 서비스입니다. **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Cloud Management(**클라우드 관리**)** 페이지 이름이 **Cloud Services(**클라우드 서비스**)**로 변경되었습니다. 같은 페이지에서 Cisco Defense Orchestrator를 구성할 수 있습니다.
Threat Defense Virtual KVM(Kernel-based Virtual Machine) 하이퍼바이저 디바이스 컨피그레이션용.	device manager를 사용하여 KVM 디바이스에 대한 threat defense virtual의 위협 방어를 구성할 수 있습니다. 이전에는 VMware만 지원되었습니다. 참고 device manager 지원을 받으려면 새 6.2.3 이미지를 설치해야 합니다. 이전 버전에서 기존 가상 머신을 업그레이드한 다음 device manager로 전환할 수는 없습니다.
VMware ESXi 6.5에 대한 지원.	이제 VMware vSphere/VMware ESXi 6.5에 FTDv를 구축할 수 있습니다.
ISA 3000(Cisco 3000 Series Industrial Security Appliances) 디바이스 컨피그레이션	device manager를 사용하여 ISA 3000 디바이스에서 위협 방어를 구성할 수 있습니다. ISA 3000은 위협 라이선스만 지원하며, URL 필터링 또는 악성코드 라이선스는 지원하지 않습니다. 따라서 ISA 3000에서는 URL 필터링 또는 악성코드 라이선스가 필요한 기능을 구성할 수 없습니다.

기능	설명
규칙 데이터베이스 또는 VDB 업데이트 시 선택 사항인 구축	침입 규칙 데이터베이스 또는 VDB를 업데이트하거나 업데이트 일정을 구성할 때 업데이트가 즉각적으로 구축되지 않도록 할 수 있습니다. 업데이트 시 검사 엔진이 재시작되므로 구축 중에 일시적으로 트래픽이 삭제됩니다. 자동으로 구축하지 않고 트래픽 삭제의 영향이 가장 적을 때 구축을 시작하도록 선택할 수 있습니다. 참고 VDB 다운로드 시에도 자체적으로 Snort가 재시작될 수 있으며 구축 시에도 다시 재시작이 수행됩니다. 다운로드 시 재시작을 중지할 수 없습니다.
구축 시 Snort가 재시작되는지 나타내는 개선된 메시지. 구축 시 Snort를 재시작해야 할 필요성 감소.	구축을 시작하기 전에 device manager는 컨피그레이션 업데이트 시 Snort를 재시작해야 하는지를 표시합니다. Snort가 재시작되면 일시적으로 트래픽이 삭제됩니다. 따라서 이제 구축이 트래픽에 영향을 주지 않으며 즉시 수행 가능한지 아니면 트래픽에 영향을 주는지를 알 수 있어 작업 중단 시간을 최소화하여 구축을 수행할 수 있습니다. 또한, 이전 릴리스에서는 Snort가 구축할 때마다 재시작되었습니다. 그러나 이제는 다음과 같은 이유로만 Snort가 재시작됩니다. • SSL 암호 해독 정책을 활성화하거나 비활성화하는 경우 • 규칙 데이터베이스가 업데이트되거나 VDB를 다운로드한 경우 • 하나 이상의 물리적 인터페이스(하위 인터페이스 제외)에서 MTU를 변경한 경우
device manager의 CLI 콘솔.	이제 device manager에서 CLI 콘솔을 열 수 있습니다. CLI 콘솔은 SSH 또는 콘솔 세션과 유사하지만, 명령의 하위 집합인 **show**, **ping**, **traceroute**, **packet-tracer**만 허용합니다. CLI 콘솔을 사용하여 트러블슈팅 및 디바이스 모니터링을 수행합니다.

기능	설명
관리 주소에 대한 액세스 차단 지원	이제 프로토콜에 대한 모든 관리 액세스 목록 항목을 제거하여 관리 IP 주소에 대한 액세스를 막을 수 있습니다. 이전에는 모든 항목을 제거하면 시스템의 기본값이 모든 클라이언트 IP 주소에서의 액세스를 허용하도록 설정되었습니다. 6.2.3으로 업그레이드할 때 이전에 프로토콜(HTTPS 또는 SSH)에 대한 관리 액세스 목록이 비어 있었던 경우, 시스템에서 모든 IP 주소에 대해 기본적 허용 규칙을 생성합니다. 이러한 규칙은 나중에 필요에 따라 삭제할 수 있습니다. 또한, device manager는 SSH 또는 HTTPS 액세스를 비활성화하는 경우를 비롯하여 CLI에서 관리 액세스 목록에 대해 수행하는 변경 사항을 인식합니다. 하나 이상의 인터페이스에 대해 HTTPS 액세스를 활성화해야 하며, 그렇지 않을 경우 디바이스를 구성 및 관리할 수 없습니다.
EMS 확장 지원.	**Decrypt-Resign(**암호 해독 - 다시 서명**)** 및 **Decrypt-Known Key(**암호 해독 - 알려진 키**)** SSL 정책 동작은 이제 ClientHello 협상 중 EMS 확장을 지원하므로 통신 보안을 강화할 수 있습니다. EMS 확장은 RFC 7627에 의해 정의됩니다. 참고 버전 6.2.3.8은 2019년 1월 7일에 Cisco 지원 및 다운로드 사이트에서 제거되었습니다. 버전 6.2.3.9로 업그레이드하면 EMS 확장 지원도 사용할 수 있습니다. 버전 6.3.0에서는 EMS 확장 지원이 중단됩니다. 버전 6.3.0.1에서 지원이 다시 도입됩니다. 최소 FTD: 버전 6.2.3.8
FTD에 대한 TLS v1.3 다운그레이드 CLI 명령.	새 CLI 명령을 사용하면 TLS v1.3 연결을 TLS v1.2로 다운그레이드하는 시기를 지정할 수 있습니다. 대부분의 브라우저는 기본적으로 TLS v1.3을 사용합니다. SSL 정책을 사용하여 암호화 트래픽을 처리하고 모니터링되는 네트워크의 사용자가 TLS v1.3이 활성화된 브라우저를 사용하는 경우, TLS v1.3을 지원하는 웹사이트가 로드되지 않습니다. 자세한 내용은 Cisco Secure Firewall Threat Defense 명령 참조의 **system support** 명령을 참조하십시오. 이러한 명령은 Cisco TAC와 상의한 후에 사용하는 것이 좋습니다. 최소 FTD: 버전 6.2.3.7

기능	설명
스마트 CLI 및 FlexConfig(디바이스 CLI를 사용하는 기능 구성)	스마트 CLI 및 FlexConfig를 사용하면 device manager 정책 및 설정을 통해 직접 지원되지 않는 기능을 구성할 수 있습니다. Threat Defense는 일부 기능 수행을 위해 ASA 구성 명령을 사용합니다. ASA 컨피그레이션 명령에 대해 잘 알고 있으며 전문성을 갖춘 경우, 다음과 같은 방법을 사용하여 디바이스에서 이러한 기능을 구성할 수 있습니다. • 스마트 CLI — (기본 방법) 스마트 CLI 템플릿은 특정 기능에 대해 사전 정의된 템플릿입니다. 이 기능에 필요한 모든 명령은 제공되므로 변수의 값을 선택하기만 하면 됩니다. 시스템에서 선택 항목을 검증해 주기 때문에 기능을 더욱 올바르게 구성할 수 있습니다. 원하는 기능에 해당하는 스마트 CLI 템플릿이 있는 경우, 해당 스마트 CLI를 사용해야 합니다. 이 릴리스에서는 스마트 CLI를 사용하여 OSPFv2를 구성할 수 있습니다. • FlexConfig — FlexConfig 정책은 FlexConfig 개체의 모음입니다. FlexConfig 개체는 스마트 CLI 템플릿보다 자유 형식으로 이용할 수 있으며, 시스템에서 CLI, 변수 또는 데이터 검증을 수행하지 않습니다. 유효한 명령 시퀀스를 생성하기 위해서는 ASA 컨피그레이션 명령을 알아야 하며 ASA 컨피그레이션 가이드를 준수해야 합니다. 주의 ASA에 대한 강력한 배경 지식을 보유하고 있으며 사용에 대한 전적인 책임을 질 수 있는 고급 사용자인 경우에만 스마트 CLI 및 FlexConfig를 사용하는 것이 좋습니다. 블랙리스트에 추가되지 않은 명령은 모두 구성할 수 있습니다. 스마트 CLI 또는 FlexConfig를 통해 기능을 활성화하는 경우, 구성되어 있는 다른 기능과 함께 의도하지 않은 결과를 초래할 수 있습니다.
Threat Defense REST API 및 API Explorer.	REST API를 사용하여 device manager를 통해 로컬로 관리 중인 위협 방어 디바이스와 프로그래밍 방식으로 상호 작용할 수 있습니다. 개체 모델을 확인하고 클라이언트 프로그램에서 만들 수 있는 다양한 호출을 테스트하는 데 사용할 수 있는 API Explorer가 있습니다. API Explorer를 열려면 device manager에 로그인한 다음 URL의 경로를 /#/api-explorer로 변경합니다(예: https://ftd.example.com/#/api-explorer).

FDM 버전 6.2.2의 새로운 기능

표 *11: FDM* 버전 *6.2.2*의 새로운 기능

기능	설명
ASA 5500-X Series 디바이스용 원격 액세스 VPN 컨피그레이션	ASA 5500-X Series 디바이스에서 AnyConnect 클라이언트용 원격 액세스 SSL VPN을 구성할 수 있습니다. RA VPN은 **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)** 그룹에서 설정합니다. RA VPN 라이선스는 **Device(**디바이스**)** > **Smart License(**스마트 라이선스**)** 그룹에서 설정합니다.
Threat Defense Virtual VMware 디바이스 컨피그레이션용	device manager를 사용하여 VMware 디바이스용으로 threat defense virtual에서 위협 방어를 구성할 수 있습니다. 다른 가상 플랫폼은 device manager에서 지원되지 않습니다. 참고 device manager 지원을 받으려면 새 6.2.2 이미지를 설치해야 합니다. 이전 버전에서 기존 가상 머신을 업그레이드한 다음 device manager로 전환할 수는 없습니다.

FDM 버전 6.2.1의 새로운 기능

이 릴리스는 Firepower 2100 Series에만 적용됩니다.

표 *12: FDM* 버전 *6.2.1*의 새로운 기능

기능	설명
원격 액세스 VPN 컨피그레이션	AnyConnect 클라이언트용 원격 액세스 SSL VPN을 구성할 수 있습니다. RA VPN은 **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)** 그룹에서 설정합니다. RA VPN 라이선스는 **Device(**디바이스**)** > **Smart License(**스마트 라이선스**)** 그룹에서 설정합니다.
Firepower 2100 Series 디바이스 컨피그레이션	device manager를 사용하여 Firepower 2100 Series 디바이스에서 위협 방어를 구성할 수 있습니다.

FDM 버전 6.2의 새로운 기능

표 *13: FDM* 버전 *6.2*의 새로운 기능

기능	설명
Cisco Defense Orchestrator(CDO) 클라우드 관리.	Cisco Defense Orchestrator 클라우드 기반 포털을 사용하여 디바이스를 관리할 수 있습니다. 이렇게 하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Cloud Management(**클라우드 관리**)**를 선택합니다. Cisco Defense Orchestrator에 대한 자세한 내용은 http://www.cisco.com/go/cdo를 참조하십시오.
액세스 규칙 끌어 놓기(drag and drop).	액세스 규칙을 끌어다 놓아 규칙 테이블에서 액세스 규칙을 이동할 수 있습니다.
device manager를 통한 위협 방어 소프트웨어 업그레이드.	device manager를 통해 소프트웨어 업그레이드를 설치할 수 있습니다. 이렇게 하려면 **Device(**디바이스**)** > **Updates(**업데이트**)**를 선택합니다.

기능	설명
기본 구성 변경 사항.	새 디바이스 또는 재이미징된 디바이스의 경우 기본 컨피그레이션에는 다음과 같은 중요한 변경 사항이 포함되어 있습니다. • (ASA 5506-X, 5506W-X, 5506H-X) 첫 번째 데이터 인터페이스 및 ASA 5506W-X의 Wi-Fi 인터페이스를 제외하고 이러한 디바이스 모델의 다른 모든 데이터 인터페이스는 "내부" 브리지 그룹으로 구성되며 활성화됩니다. 내부 브리지 그룹에는 DHCP 서버가 있습니다. 브리지 인터페이스에 엔드포인트나 스위치를 연결할 수 있으며, 엔드포인트는 192.168.1.0/24 네트워크에서 주소를 가져옵니다. • 이제는 내부 인터페이스 IP 주소가 192.168.1.1이며, DHCP 서버는 주소 풀 192.168.1.5-192.168.1.254가 포함된 인터페이스에서 정의됩니다. • 내부 네트워크에서는 HTTPS 액세스가 활성화되므로 기본 주소 192.168.1.1에서 내부 인터페이스를 통해 device manager를 열 수 있습니다. ASA 5506-X 모델의 경우 임의의 내부 브리지 그룹 멤버 인터페이스를 통해 이 작업을 수행할 수 있습니다. • 관리 포트는 192.168.45.0/24 네트워크에 대해 DHCP 서버를 호스팅합니다. 워크스테이션을 관리 포트에 직접 연결하고 IP 주소를 가져온 다음 device manager를 열어 디바이스를 구성할 수 있습니다. • 이제는 OpenDNS 공용 DNS 서버가 관리 인터페이스의 기본 DNS 서버입니다. 이전에는 기본 DNS 서버가 없었습니다. 디바이스 설정 중에 다른 DNS 서버를 구성할 수 있습니다. • 관리 IP 주소의 기본 게이트웨이는 데이터 인터페이스를 사용하여 인터넷으로 라우팅됩니다. 따라서 관리 실제 인터페이스를 네트워크에 유선으로 연결하지 않아도 됩니다.

기능	설명
관리 인터페이스 및 액세스 변경 사항.	관리 주소 및 device manager에 대한 액세스가 작동하는 방식과 관련하여 여러 가지 사항이 변경되었습니다. • 이제는 HTTPS(device manager의 경우) 및 SSH(CLI의 경우) 연결에 대해 데이터 인터페이스를 열 수 있습니다. 따라서 디바이스를 관리하기 위해 별도의 관리 네트워크를 사용하거나 관리/진단 물리적 포트를 내부 네트워크에 연결할 필요가 없습니다. 데이터 인터페이스를 열려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Access List(**관리 액세스 목록**)**를 선택합니다. • 시스템은 외부 인터페이스에 대해 게이트웨이를 통해 시스템 데이터베이스 업데이트를 가져올 수 있습니다. 그러므로 관리 인터페이스 또는 네트워크에서 인터넷으로의 명시적 경로가 없어도 됩니다. 기본적으로는 데이터 인터페이스를 통해 내부 경로를 사용합니다. 그러나 별도의 관리 네트워크를 사용하려는 경우에는 특정 게이트웨이를 설정할 수 있습니다. 이렇게 하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**를 선택합니다. • device manager를 사용하여 DHCP를 통해 IP 주소를 가져오도록 관리 인터페이스를 구성할 수 있습니다. 이렇게 하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**를 선택합니다. • 고정 주소를 구성하는 경우 관리 주소에 대해 DHCP 서버를 구성할 수 있습니다. 이렇게 하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**를 선택합니다.

기능	설명
기타 사용자 인터페이스 변경 사항.	device manager 사용자 인터페이스의 주요 변경 사항은 다음과 같습니다. • 디바이스 주 메뉴 항목. 이전 릴리스에서 이 메뉴 항목은 디바이스의 호스트 이름이었습니다. 또한, 열리는 페이지의 이름은 디바이스 대시보드가 아닌 디바이스 요약입니다. • 초기 디바이스 설정 중에는 대체 외부 인터페이스를 선택할 수 없습니다. 첫 번째 데이터 인터페이스가 기본 외부 인터페이스입니다. • 이제는 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Cloud Preferences(**클라우드 기본 설정**)**의 이름이 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **URL Filtering Preferences(URL** 필터링 기본 설정**)**로 바뀌었습니다. • 이제는 **System Settings(**시스템 설정**)** > **DHCP Server(DHCP** 서버**)** 페이지가 2개 탭으로 구성되어 있으며 DHCP 서버 테이블이 글로벌 파라미터에서 분리되었습니다.
사이트 대 사이트 VPN 연결.	사전 공유 키를 사용하여 사이트 대 사이트 VPN(Virtual Private Network) 연결을 구성할 수 있습니다. IKEv1 및 IKEv2 연결을 구성할 수 있습니다.
통합 라우팅 및 브리징 지원	통합 라우팅 및 브리징은 브리지 그룹과 라우팅 인터페이스 간을 라우팅하는 기능을 제공합니다. 브리지 그룹은 위협 방어 디바이스에서 경로 대신 브리징하는 인터페이스 그룹입니다. 위협 방어 디바이스는 실제 브리지가 아닙니다. 위협 방어 디바이스는 계속해서 방화벽으로 작동하며, 이를 통해 인터페이스 간의 액세스 제어가 제어되고 모든 일반 방화벽 검사가 올바르게 수행됩니다. 이 기능을 사용하면 브리지 그룹을 구성하고 브리지 그룹 간, 그리고 브리지 그룹과 라우팅 인터페이스 간을 라우팅할 수 있습니다. 브리지 그룹은 BVI(브리지 가상 인터페이스)를 사용하여 라우팅에 참여함으로써 브리지 그룹의 게이트웨이로 작동합니다. 브리지 그룹에 할당할 추가 인터페이스가 위협 방어 디바이스에 있는 경우에는 외부 레이어 2 스위치를 사용하는 대신 통합형 라우팅 및 브리징을 사용할 수 있습니다. BVI는 이름이 지정된 인터페이스일 수 있으며 DHCP 서버 등의 일부 기능에는 멤버 인터페이스와 별도로 포함될 수 있습니다. 이 경우 브리지 그룹 멤버 인터페이스에서 NAT 및 액세스 제어 규칙과 같은 기타 기능을 구성합니다. 브리지 그룹을 설정하려면 **Device(**디바이스**)** > **Interfaces(**인터페이스**)**를 선택합니다.

FDM 버전 6.1의 새로운 기능

표 *14: FDM* 버전 *6.1.0*의 새로운 기능

기능	설명
지원되는 디바이스.	Firepower Device Manager를 사용하여 다음 디바이스 유형을 관리할 수 있습니다. • ASA 5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X • ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X
지원되는 방화벽 모드.	라우팅 모드에서만 실행되는 디바이스를 구성할 수 있습니다. 투명 모드는 지원되지 않습니다.
지원되는 인터페이스 유형 및 모드.	라우팅된 인터페이스만 구성할 수 있으며 인라인, 인라인 탭 또는 패시브 인터페이스는 구성할 수 없습니다. 또한 물리적 인터페이스와 하위 인터페이스만 구성할 수 있습니다. Etherchannel 또는 이중 인터페이스는 구성할 수 없습니다. PPPoE를 구성할 수도 없습니다.

보안 정책.	다음과 같은 유형의 보안 정책을 구성할 수 있습니다.
	• 액세스 제어 - 디바이스를 통과할 수 있는 연결을 결정합니다. 다음 유형의 액세스 제어를 수행할 수 있습니다.
	  • 보안 영역, IP 주소, 지리위치, 프로토콜 및 포트에 대한 필터링.
	  • 사용자 이름 및 사용자 그룹에 대한 필터링.
	  • 애플리케이션 필터링.
	  • URL 범주, 평판 및 개별 URL 필터링.
	  • 침입 정책, 위협 방지.
	  • 파일 정책, 악성코드 방지.
	• ID 정책 - IP 주소와 연결된 사용자를 결정합니다. 시스템은 패시브 인증이 아닌 활성 인증만 지원합니다.
	• 네트워크 주소 변환 - 내부 주소와 외부 주소 사이를 변환합니다. PAT 풀을 제외한 대부분의 NAT 기능이 지원됩니다.

라우팅.	정적 경로를 구성할 수 있습니다. 동적 라우팅 프로토콜은 지원되지 않습니다.

기능	설명
시스템 모니터링 및 시스템 로그.	Firepower Device Manager에는 이벤트 보기가 포함되어 있어 최근 연결 이벤트를 볼 수 있습니다. 장기적인 분석을 위해 이벤트를 수집하도록 외부 시스템 로그 서버를 구성할 수도 있습니다. 시스템 및 시스템을 통과하는 트래픽에 대한 통계 정보를 제공하는 대시보드도 많이 있습니다.
관리 인터페이스 구성.	관리 주소와 인터페이스는 Firepower Device Manager에서 구성할 수 있습니다. CLI를 사용할 필요가 없습니다. 시스템 호스트 이름, 관리 IP 주소 및 게이트웨이, DNS 서버, NTP 서버 및 액세스 규칙을 구성하여 CLI 또는 Firepower Device Manager에 액세스할 수 있는 IP 주소를 제한할 수 있습니다.
일정 업데이트.	시스템 데이터베이스가 업데이트되는 빈도를 제어할 수 있습니다. • 디바이스 주 메뉴 항목. 이전 릴리스에서 이 메뉴 항목은 디바이스의 호스트 이름이었습니다. 또한, 열리는 페이지의 이름은 디바이스 대시보드가 아닌 디바이스 요약입니다. • 초기 디바이스 설정 중에는 대체 외부 인터페이스를 선택할 수 없습니다. 첫 번째 데이터 인터페이스가 기본 외부 인터페이스입니다. • 이제는 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Cloud Preferences(**클라우드 기본 설정**)**의 이름이 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **URL Filtering Preferences(URL** 필터링 기본 설정**)**로 바뀌었습니다. • 이제는 **System Settings(**시스템 설정**)** > **DHCP Server(DHCP** 서버**)** 페이지가 2개 탭으로 구성되어 있으며 DHCP 서버 테이블이 글로벌 파라미터에서 분리되었습니다.
백업 및 복구.	시스템을 백업하고 Firepower Device Manager에서 복원할 수 있습니다.
문제 해결 파일.	Cisco Technical Support와 함께 작업할 때 Firepower Device Manager에서 문제 해결 파일을 생성할 수 있습니다.

릴리스 날짜

표 ***15:*** 버전 ***7.4*** 날짜

Version(버전**)**	구축	날짜	플랫폼
7.4.1	172	2023-12-13	모두

Version(버전)	구축	날짜	플랫폼
7.4.0	81	2023-09-07	Management Center Secure Firewall 4200 Series

표 ***16:*** 버전 ***7.3*** 날짜

Version(버전)	구축	날짜	플랫폼
7.3.1.1	83	2023-08-24	모두
7.3.1	19	2023-03-14	모두
7.3.0	69	2022-11-29	모두

표 ***17:*** 버전 ***7.2*** 날짜

Version(버전)	구축	날짜	플랫폼
7.2.5.1	29	2023-11-14	모두
7.2.5	208	2023-07-27	모두
7.2.4.1	43	2023-07-27	모두
7.2.4	169	2023-05-10	Management Center
	165	2023-05-03	디바이스
7.2.3.1	13	2023-04-18	Management Center
7.2.3	77	02-27-2023	모두
7.2.2	54	2022-11-29	모두
7.2.1	40	2022-10-03	모두
7.2.0.1	12	2022-08-10	모두
7.2.0	82	2022-06-06	모두

표 ***18:*** 버전 ***7.1*** 날짜

Version(버전)	구축	날짜	플랫폼
7.1.0.3	108	2022-03-15	모두
7.1.0.2	28	2022-08-03	FMC/FMCv Secure Firewall 3100 Series

Version(버전)	구축	날짜	플랫폼
7.1.0.1	28	2022-02-24	FMC/FMCv Secure Firewall 3100 Series를 제외한 모든 디바이스
7.1.0	90	2021-12-01	모두

표 ***19:*** 버전 ***7.0*** 날짜

Version(버전)	구축	날짜	플랫폼
7.0.6.1	36	2023-11-13	모두
7.0.6	236	2023-07-18	모두
7.0.5.1	5	2023-04-26	NGIPSv 보안 인증서 컴플라이언스가 활성화된 디바이스의 경우(CC/UCAPL 모드). 버전 7.0.5 FMC와 함께 사용합니다.
7.0.5	72	2022-11-17	모두
7.0.4	55	2022-08-10	모두
7.0.3	37	2022-06-30	모두
7.0.2.1	10	2022-06-27	모두
7.0.2	88	2022-05-05	모두
7.0.1.1	11	2022-02-17	모두
7.0.1	84	2021-10-07	모두
7.0.0.1	15	2021-07-15	모두
7.0.0	94	2021-05-26	모두

표 ***20:*** 버전 ***6.7*** 날짜

Version(버전)	구축	날짜	플랫폼
6.7.0.3	105	2022-02-17	모두
6.7.0.2	24	2021-05-11	모두
6.7.0.1	13	2021-03-24	모두
6.7.0	65	2020-11-02	모두

표 ***21:*** 버전 ***6.6*** 날짜

Version(버전)	구축	날짜	플랫폼
6.6.7.1	42	2023-01-26	모두
6.6.7	223	2022-07-14	모두
6.6.5.2	14	2022-03-24	모두
6.6.5.1	15	2021-12-06	모두
6.6.5	81	2021-08-03	모두
6.6.4	64	2021-04-29	Firepower 1000 Series
	59	2021-04-26	FMC/FMCv Firepower 1000 Series를 제외한 모든 디바이스
6.6.3	80	2020-03-11	모두
6.6.1	91	2020-09-20	모두
	90	2020-09-08	—
6.6.0.1	7	2020-07-22	모두
6.6.0	90	2020-05-08	Firepower 4112
		2020-04-06	FMC/FMCv Firepower 4112를 제외한 모든 디바이스

표 ***22:*** 버전 ***6.5*** 날짜

Version(버전)	구축	날짜	플랫폼: 업그레이드	플랫폼: 이미지 다시 설치
6.5.0.5	95	2021-02-09	All(모두)	—
6.5.0.4	57	2020-03-02	All(모두)	—
6.5.0.3	30	2020-02-03	더 이상 사용할 수 없습니다.	—
6.5.0.2	57	2019-12-19	All(모두)	—
6.5.0.1	35	2019-11-20	더 이상 사용할 수 없습니다.	—
6.5.0	123	2020-02-03	FMC/FMCv	FMC/FMCv
	120	2019-10-08	—	—
	115	2019-09-26	모든 디바이스	모든 디바이스

표 *23:* 버전 *6.4* 날짜

Version(버전)	구축	날짜	플랫폼
6.4.0.17	26	2023-09-28	모두
6.4.0.16	50	2022-11-21	모두
6.4.0.15	26	2022-05-31	모두
6.4.0.14	67	2022-02-18	모두
6.4.0.13	57	2021-12-02	모두
6.4.0.12	112	2021-05-12	모두
6.4.0.11	11	2021-01-11	모두
6.4.0.10	95	2020-10-21	모두
6.4.0.9	62	2020-05-26	모두
6.4.0.8	28	2020-01-29	모두
6.4.0.7	53	2019-12-19	모두
6.4.0.6	28	2019-10-16	더 이상 사용할 수 없습니다.
6.4.0.5	23	2019-09-18	모두
6.4.0.4	34	2019-08-21	모두
6.4.0.3	29	2019-07-17	모두
6.4.0.2	35	2019-07-03	FMC/FMCv Firepower 1000 series를 제외한 FTD/FTDv
	34	2019-06-27	—
		2019-06-26	Firepower 7000/8000 시리즈 ASA FirePOWER NGIPSv

Version(버전)	구축	날짜	플랫폼
6.4.0.1	17	2019-06-27	FMC 1600, 2600, 4600
		2019-06-20	Firepower 4115, 4125, 4145 SM-40, SM-48, SM-56 모듈을 지원하는 Firepower 9300
		2019-05-15	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv Firepower 2110, 2120, 2130, 2140 Firepower 4110, 4120, 4140, 4150 SM-24, SM-36, SM-44 모듈을 지원하는 Firepower 9300 ASA 5508-X, 5515-X, 5516-X, 5525-X, 5545-X, 5555-X ASA 5585-X-SSP-10, -20, -40, -60 ISA 3000 FTDv Firepower 7000/8000 시리즈 NGIPSv
6.4.0	113	2020-03-03	FMC/FMCv
	102	2019-06-20	Firepower 4115, 4125, 4145 SM-40, SM-48, SM-56 모듈을 지원하는 Firepower 9300
		2019-06-13	Firepower 1010, 1120, 1140
		2019-04-24	Firepower 2110, 2120, 2130, 2140 Firepower 4110, 4120, 4140, 4150 SM-24, SM-36, SM-44 모듈을 지원하는 Firepower 9300 ASA 5508-X, 5515-X, 5516-X, 5525-X, 5545-X, 5555-X ASA 5585-X-SSP-10, -20, -40, -60 ISA 3000 FTDv Firepower 7000/8000 시리즈 NGIPSv

표 *24:* 버전 *6.3* 날짜

Version(버전)	구축	날짜	플랫폼: 업그레이드	플랫폼: 이미지 다시 설치
6.3.0.5	35	2019-11-18	Firepower 7000/8000 시리즈 NGIPSv	—
	34	2019-11-18	FMC/FMCv 모든 FTD 디바이스 ASA FirePOWER	—
6.3.0.4	44	2019-08-14	All(모두)	—
6.3.0.3	77	2019-06-27	FMC 1600, 2600, 4600	—
		2019-05-01	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv 모든 디바이스	—
6.3.0.2	67	2019-06-27	FMC 1600, 2600, 4600	—
		2019-03-20	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv 모든 디바이스	—
6.3.0.1	85	2019-06-27	FMC 1600, 2600, 4600	—
		2019-02-18	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv 모든 디바이스	—
6.3.0	85	2019-01-22	Firepower 4100/9300	Firepower 4100/9300
	84	2018-12-18	FMC/FMCv ASA FirePOWER	—
	83	2019-06-27	—	FMC 1600, 2600, 4600
		2018-12-03	Firepower 4100/9300을 제외한 모든 FTD 디바이스 Firepower 7000/8000 NGIPSv	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv Firepower 4100/9300을 제외한 모든 디바이스

표 ***25:*** 버전 ***6.2.3*** 날짜

Version(버전)	구축	날짜	플랫폼: 업그레이드	플랫폼: 이미지 다시 설치
6.2.3.18	50	2022-02-16	All(모두)	—
6.2.3.17	30	2021-06-21	All(모두)	—
6.2.3.16	59	2020-07-13	All(모두)	—
6.2.3.15	39	2020-02-05	FTD/FTDv	—
	38	2019-09-18	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv	—
6.2.3.14	41	2019-07-03	All(모두)	—
	36	2019-06-12	All(모두)	—
6.2.3.13	53	2019-05-16	All(모두)	—
6.2.3.12	80	2019-04-17	All(모두)	—
6.2.3.11	55	2019-03-17	All(모두)	—
	53	2019-03-13	—	—
6.2.3.10	59	2019-02-07	All(모두)	—
6.2.3.9	54	2019-01-10	All(모두)	—
6.2.3.8	51	2019-01-02	더 이상 사용할 수 없습니다.	—
6.2.3.7	51	2018-11-15	All(모두)	—
6.2.3.6	37	2018-10-10	All(모두)	—
6.2.3.5	53	2018-11-06	FTD/FTDv	—
	52	2018-09-12	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv	—
6.2.3.4	42	2018-08-13	All(모두)	—
6.2.3.3	76	2018-07-11	All(모두)	—

Version(버전)	구축	날짜	플랫폼: 업그레이드	플랫폼: 이미지 다시 설치
6.2.3.2	46	2018-06-27	All(모두)	—
	42	2018-06-06	—	—
6.2.3.1	47	2018-06-28	All(모두)	—
	45	2018-06-21	—	—
	43	2018-05-02	—	—
6.2.3	113	2020-06-01	FMC/FMCv	FMC/FMCv
	111	2019-11-25	—	FTDv: AWS, Azure
	110	2019-06-14	—	—
	99	2018-09-07	—	—
	96	2018-07-26	—	—
	92	2018-07-05	—	—
	88	2018-06-11	—	—
	85	2018-04-09	—	—
	84	2018-04-09	Firepower 7000/8000 시리즈 NGIPSv	—
	83	2018-04-02	FTD/FTDv ASA FirePOWER	FTD: 물리적 플랫폼 FTDv: VMware, KVM Firepower 7000/8000 ASA FirePOWER NGIPSv
	79	2018-03-29	—	—

표 ***26:*** 버전 ***6.2.2*** 날짜

Version(버전)	구축	날짜	플랫폼
6.2.2.5	57	2018-11-27	모두

Version(버전)	구축	날짜	플랫폼
6.2.2.4	43	2018-09-21	FTD/FTDv
	34	2018-07-09	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv
	32	2018-06-15	—
6.2.2.3	69	2018-06-19	모두
	66	2018-04-24	—
6.2.2.2	109	2018-02-28	모두
6.2.2.1	80	2017-12-05	Firepower 2100 Series
	78	2017-11-20	—
	73	2017-11-06	FMC/FMCv Firepower 2100 Series를 제외한 모든 디바이스
6.2.2	81	2017-09-05	모두