Cisco Secure Firewall Management Center 호환성 가이드

초판: 2022년 5월 5일

최종 변경: 2022년 6월 6일

Cisco 보안 방화벽 관리 센터 호환성 가이드

이 가이드에서는 Cisco 보안 방화벽 관리 센터의 소프트웨어 및 하드웨어 호환성을 제공합니다. 관련 호환성 가이드는 추가 리소스, 1 페이지를 참조하십시오.

참고 모든 소프트웨어 버전, 특히 패치가 모든 플랫폼에 적용되는 것은 아닙니다. 버전이 지원되는지 확인하는 빠른 방법은 해당 업그레이드/설치 패키지가 Cisco 지원 및 다운로드 사이트에 게시되어 있는지를 확인하는 것입니다. 사이트에 업그레이드 또는 설치 패키지가 "누락된" 경우 해당 버전은 지원되지 않습니다. 릴리스 노트 및 End-of-Life 공지, 17 페이지도 확인할 수 있습니다 오류로 인해 버전이 누락되었다고 생각되면 Cisco TAC에 문의하십시오.

추가 리소스

표 *1:*

설명	리소스
유지보수 게시판은 관리 플랫폼 및 운영 체제를 비롯해 Cisco 차세대 방화벽 제품 라인에 대한 지원 일정을 제공합니다.	Cisco NGFW 제품 라인 소프트웨어 출시 및 유지보수 게시판
호환성 가이드는 번들 구성 요소 및 통합 제품을 포함하여 지원되는 하드웨어 모델 및 소프트웨어 버전에 대한 자세한 호환성 정보를 제공합니다.	Cisco Secure Firewall Threat Defense 호환성 가이드 Cisco Firepower Classic 디바이스 호환성 가이드
릴리스 노트는 업그레이드 경고 및 동작 변경 사항을 포함하여 중요하고 릴리스별 정보를 제공합니다. 릴리스 노트에는 업그레이드 및 설치 지침에 대한 빠른 링크도 포함되어 있습니다.	Cisco Secure Firewall Threat Defense 릴리스 노트

설명	리소스
새로운 기능 가이드는 릴리스별로 새로운 기능과 사용되지 않는 기능에 대한 정보를 제공합니다.	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/roadmap/management-center-new-features-by-release.html
문서 로드맵은 현재 사용 가능한 레거시 문서에 대한 링크를 제공합니다. 찾고 있는 것이 위에 나열되지 않은 경우 로드맵을 시도합니다.	Cisco Firepower 문서 탐색

Management Center

모든 Firepower 및 Secure Firewall Threat Defense 및 디바이스는 management center의 원격 관리를 지원합니다.

하드웨어/가상 관리 센터

하드웨어 management center 또는 management center virtual는 관리되는 디바이스와 동일하거나 최신 버전을 실행해야 합니다. 이것은 다음을 의미합니다:

- 일반적으로 몇 가지 주요 버전인 최신 management center로 이전 디바이스를 관리할 수 있습니다. 그러나 항상 전체 구축을 업데이트하는 것이 좋습니다. 새로운 기능을 사용하고 해결된 문제를 적용하려면 management center와 관리되는 디바이스 모두에서 최신 릴리스를 사용해야 하는 경우가 많습니다.
- management center 이상으로 디바이스를 업그레이드할 수 없습니다. 유지 보수(세자리 숫자) 릴리스의 경우에도 management center를 먼저 업그레이드해야 합니다.

표 ***2: Management Center*-디바이스 호환성**

Management Center 버전	관리 가능한 가장 오래된 디바이스 버전
7.2	6.6
7.1	6.5
7.0	6.4
6.7	6.3
6.6	6.2.3
6.5	6.2.3
6.4	6.1
6.3	6.1
6.2.3	6.1
6.2.2	6.1

Management Center 버전	관리 가능한 가장 오래된 디바이스 버전
6.2.1	6.1
6.2	6.1
6.1	5.4.0.2/5.4.1.1
6.0.1	5.4.0.2/5.4.1.1
6.0	5.4.0.2/5.4.1.1
5.4.1	ASA-5506-X 시리즈, ASA5508-X 및 ASA5516-X에서 ASA FirePOWER용 5.4.1. ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X, and ASA-5585-X 시리즈에서 ASA FirePOWER용 5.3.1. Firepower 7000/8000 시리즈 및 레거시 디바이스용 5.3.0

클라우드 제공 관리 센터

클라우드 제공 관리 센터는 여러 Cisco 보안 솔루션에서 관리를 통합하는 CDO(Cisco Defense Orchestrator) 플랫폼을 통해 제공됩니다. Cisco에서 관리자 업데이트를 처리합니다. 클라우드 제공 관리 센터는 버전 7.2 이상을 실행하는 위협 방어 디바이스를 관리할 수 있습니다.

이벤트 로깅 및 분석 목적으로만 버전 7.2 이상의 하드웨어 또는 가상 관리 센터에 클라우드 매니지드 디바이스를 추가할 수 있습니다. 또는 Security Analytics and Logging(SaaS)을(를) 사용하여 Cisco Cloud에 보안 이벤트를 전송할 수 있습니다.

Management Center 하드웨어

표 ***3: Management Center*** 하드웨어 호환성

Management Center	FMC 1600 FMC 2600 FMC 4600	FMC 1000 FMC 2500 FMC 4500	FMC 2000 FMC 4000	FMC 750 FMC 1500 FMC 3500	DC 500 DC 1000 DC 3000
7.2	예	—	—	—	—
7.1	예	—	—	—	—
7.0	예	예	—	—	—
6.7	예	예	—	—	—
6.6	예	예	예	—	—
6.5	예	예	예	—	—
6.4	예	예	예	예	—

Management Center	FMC 1600 FMC 2600 FMC 4600	FMC 1000 FMC 2500 FMC 4500	FMC 2000 FMC 4000	FMC 750 FMC 1500 FMC 3500	DC 500 DC 1000 DC 3000
6.3	예	예	예	예	—
6.2.3	—	예	예	예	—
6.2.2	—	예	예	예	—
6.2.1	—	예	예	예	—
6.2.0	—	예	예	예	—
6.1	—	—	예	예	—
6.0.1	—	—	예	예	—
6.0.0	—	—	예	예	—
5.4 *	—	—	예	예	예

* 5.4.x 디바이스를 관리하려면 5.4.1.x Defense Center 사용

Management Center 하드웨어용 BIOS 및 펌웨어

management center 하드웨어에서 BIOS 및 RAID 컨트롤러 펌웨어에 대한 업데이트를 제공합니다. management center이(가) 요구 사항을 충족하지 않으면 적절한 핫픽스를 적용합니다. 사용 중인 management center 모델 및 버전이 목록에 없고 업데이트가 필요하다고 생각되면 Cisco TAC에 문의하십시오.

표 *4: BIOS* 및 펌웨어 최소 요구 사항

플랫폼	버전	BIOS	RAID 컨트롤러 펌웨어	CIMC 펌웨어	Hotfix
FMC 1600, 2600, 4600	6.3.0~7.0	C220M5.4.1.3i.0	51.10.0-3612	4.1(3d)	BIOS 업데이트 핫픽스 EL
FMC 1000, 2500, 4500	6.2.3~7.0	C220M4.4.1.2c.0	24.12.1-0456	4.1(2g)	BIOS 업데이트 핫픽스 EL
FMC 2000, 4000	6.2.3~6.6	C220M3.3.0.4e.0	23.33.1-0060	3.0(4s)	BIOS 업데이트 핫픽스 EI
MC750, 1500, 3500	6.2.3~6.4	C220M3.3.0.4e.0	23.33.1-0060	3.0(4s)	BIOS 업데이트 핫픽스 EI

핫픽스는 BIOS 및 RAID 컨트롤러 펌웨어를 업데이트할 수 있는 유일한 방법입니다. 소프트웨어를 업그레이드해도 이 작업을 수행할 수 없으며, 이후 버전으로 이미지를 재설치할 수도 없습니다. management center가 이미 최신 상태라면 핫픽스가 적용되지 않습니다.

팁 이러한 핫픽스는 CIMC 펌웨어도 업데이트합니다. 해결된 문제는 Cisco UCS 랙 서버 소프트웨어에 대한 릴리스 노트를 참조하십시오. 일반적으로 CIMC를 사용하는 management center에서는 컨피그레이션 변경을 지원하지 않습니다. 그러나 유효하지 않은 CIMC 사용자 이름의 로깅을 활성화하려면 최신 핫픽스를 적용한 다음 Cisco UCS C-Series 서버 통합 관리 컨트롤러 CLI 구성 가이드 버전 4.0 이상에서 오류 및 로그 보기 장에 있는 지침을 따르십시오.

핫픽스를 적용하려면 일반 업그레이드 프로세스를 사용하십시오. Cisco 지원 및 다운로드 사이트에 대한 빠른 링크가 포함된 핫픽스 릴리스 노트는 Cisco Firepower 핫픽스 릴리스 노트를 참조하십시오.

참고 management center 웹 인터페이스는 현재 소프트웨어 버전과 다른(일반적으로 이후) 버전으로 이러한 핫픽스를 표시할 수 있습니다. 이는 정상적인 동작이므로, 핫픽스를 적용해도 문제가 없습니다.

BIOS 및 펌웨어 버전 확인

management center에서 현재 버전을 확인하려면 Linux 쉘/전문가 모드에서 다음 명령을 실행합니다.

- BIOS: **sudo dmidecode -t bios -q**
- RAID 컨트롤러 펌웨어(FMC 4500): **sudo MegaCLI -AdpAllInfo -aALL | grep "FW Package"**
- RAID 컨트롤러 펌웨어(기타 모든 모델): **sudo storcli /c0 show | grep "FW Package"**

Management Center Virtual

management center virtual을(를) 사용하면 2개, 10개, 25개 또는 300개의 디바이스를 관리할 수 있는 라이선스를 구매할 수 있습니다. 일부 플랫폼만 FMCv300을 지원합니다. 지원되는 인스턴스에 대한 자세한 내용은 Cisco Secure Firewall Management Center Virtual 시작 가이드의 내용을 참조하십시오.

Management Center Virtual: VMware

표 *5: Management Center Virtual for VMware* 호환성: 버전 *6.2.3+*

Management Center	VMware vSphere/VMware ESXi				
	7.0	6.7	6.5	6.0	5.5
7.2	예	예	예	—	—
7.1	예	예	예	—	—
7.0	예	예	예	—	—

Management Center	VMware vSphere/VMware ESXi				
	7.0	6.7	6.5	6.0	5.5
6.7	—	예	예	예	—
6.6	—	예	예	예	—
6.5 FMCv300에 대한 첫 번째 지원	—	예	예	예	—
6.4	—	—	예	예	—
6.3	—	—	예	예	—
6.2.3	—	—	예	예	예

표 ***6: Management Center Virtual for VMware*** 호환성*:* 버전 ***5.4***부터 ***6.2.2***

Management Center	VMware vSphere/VMware ESXi				VMware vCloud Director
	6.0	5.5	5.1	5.0	
6.2.2	예	예	—	—	—
6.2.1	예	예	—	—	—
6.2.0	예	예	—	—	—
6.1	예	예	—	—	—
6.0.1	—	예	예	—	—
6.0.0	—	예	예	—	—
5.4	—	예	예	예	예

* 5.4.x 디바이스를 관리하려면 5.4.1.x Defense Center 사용

Management Center Virtual: 온프레미스/프라이빗 클라우드

표 ***7: Management Center Virtual*** 호환성*:* 온프레미스/프라이빗 클라우드

Management Center	Cisco HyperFlex(HyperFlex)	KVM(Kernel-Based Virtual Machine)	Nutanix Enterprise Cloud(Nutanix)	OpenStack
7.2	예	예	예	예
7.1	예	예	예	예

Management Center	Cisco HyperFlex(HyperFlex)	KVM(Kernel-Based Virtual Machine)	Nutanix Enterprise Cloud(Nutanix)	OpenStack
7.0	예	예	예	예
6.7	—	예	—	—
6.6	—	예	—	—
6.6	—	예	—	—
6.5	—	예	—	—
6.4	—	예	—	—
6.3	—	예	—	—
6.2.3	—	예	—	—
6.2.2	—	예	—	—
6.2.1	—	예	—	—
6.2.0	—	예	—	—
6.1	—	예	—	—

Management Center Virtual: 퍼블릭 클라우드

표 *8: Management Center Virtual* 호환성: 퍼블릭 클라우드

Management Center	Alibaba	AWS(Amazon Web Services)	Microsoft Azure(Azure)	GCP(Google Cloud Platform)	OCI(Oracle Cloud Infrastructure)
7.2	예	예	예	예	예
7.1	—	예 FMCv300에 대한 첫 번째 지원	예	예	예 FMCv300에 대한 첫 번째 지원
7.0	—	예	예	예	예
6.7	—	예	예	예	예
6.6	—	예	예	—	—
6.6	—	예	예	—	—
6.5	—	예	예		—

Management Center	Alibaba	AWS(Amazon Web Services)	Microsoft Azure(Azure)	GCP(Google Cloud Platform)	OCI(Oracle Cloud Infrastructure)
6.4	—	예	예	—	—
6.3	—	예	—	—	—
6.2.3	—	예	—	—	—
6.2.2	—	예	—	—	—
6.2.1	—	예	—	—	—
6.2.0	—	예	—	—	—
6.1	—	예	—	—	—
6.0.1	—	예	—	—	—

번들 구성 요소

이 표에는 management center 릴리스와 함께 번들로 제공되는 다양한 구성 요소의 버전이 나열되어 있습니다. 이 정보를 사용하여 구축에 영향을 줄 수 있는 번들 구성 요소에서 발생하거나 해결된 버그를 파악할 수 있습니다.

일부 릴리스에 대해 업데이트된 빌드를 릴리스하는 경우도 있습니다. 번들 구성 요소가 빌드에서 빌드로 변경되는 경우 최신 빌드에 구성 요소가 포함됩니다. (대부분의 경우 최신 빌드만 다운로드할 수 있습니다.) 새 빌드 및 새 빌드로 해결된 문제에 대한 자세한 내용은 사용 중인 릴리스 노트 내용을 참조하십시오.

Snort

Snort는 기본 검사 엔진입니다. Snort 3이 필요합니다.threat defense

표 ***9:***

Management Center	Snort 2	Snort 3
7.2.0	2.9.20-107	3.1.21.1-126
7.1.0.1	2.9.19-1013	3.1.7.2-200
7.1.0	2.9.19-92	3.1.7.1-108
7.0.2	2.9.18-2022	3.1.0.200-16
7.0.1.1	2.9.18-1026	3.1.0.100-11
7.0.1	2.9.18-1026	3.1.0.100-11
7.0.0.1	2.9.18-1001	3.1.0.1-174

Management Center	Snort 2	Snort 3
7.0.0	2.9.18-174	3.1.0.1-174
6.7.0.3	2.9.17-3014	—
6.7.0.2	2.9.17-2003	—
6.7.0.1	2.9.17-1006	—
6.7.0	2.9.17-200	—
6.6.5.2	2.9.16-5204	—
6.6.5.1	2.9.16-5107	—
6.6.5	2.9.16-5034	—
6.6.4	2.9.16-4022	—
6.6.3	2.9.16-3033	—
6.6.1	2.9.16-1025	—
6.6.0.1	2.9.16-140	—
6.6.0	2.9.16-140	—
6.5.0.5	2.9.15-15510	—
6.5.0.4	2.9.15-15201	—
6.5.0.3	2.9.15-15201	—
6.5.0.2	2.9.15-15101	—
6.5.0.1	2.9.15-15101	—
6.5.0	2.9.15-7	—
6.4.0.14	2.9.14-24000	—
6.4.0.13	2.9.14-19008	—
6.4.0.12	2.9.14-18011	—
6.4.0.11	2.9.14-17005	—
6.4.0.10	2.9.14-16023	—
6.4.0.9	2.9.14-15906	—
6.4.0.8	2.9.14-15707	—

Management Center	Snort 2	Snort 3
6.4.0.7	2.9.14-15605	—
6.4.0.6	2.9.14-15605	—
6.4.0.5	2.9.14-15507	—
6.4.0.4	2.9.12-15301	—
6.4.0.3	2.9.14-15301	—
6.4.0.2	2.9.14-15209	—
6.4.0.1	2.9.14-15100	—
6.4.0	2.9.14-15003	—
6.3.0.5	2.9.13-15503	—
6.3.0.4	2.9.13-15409	—
6.3.0.3	2.9.13-15307	—
6.3.0.2	2.9.13-15211	—
6.3.0.1	2.9.13-15101	—
6.3.0	2.9.13-15013	—
6.2.3.18	2.9.12-1813	—
6.2.3.17	2.9.12-1605	—
6.2.3.16	2.9.12-1605	—
6.2.3.15	2.9.12-1513	—
6.2.3.14	2.9.12-1401	—
6.2.3.13	2.9.12-1306	—
6.2.3.12	2.9.12-1207	—
6.2.3.11	2.9.12-1102	—
6.2.3.10	2.9.12-902	—
6.2.3.9	2.9.12-806	—
6.2.3.8	2.9.12-804	—
6.2.3.7	2.9.12-704	—

Management Center	Snort 2	Snort 3
6.2.3.6	2.9.12-607	—
6.2.3.5	2.9.12-506	—
6.2.3.4	2.9.12-383	—
6.2.3.3	2.9.12-325	—
6.2.3.2	2.9.12-270	—
6.2.3.1	2.9.12-204	—
6.2.3	2.9.12-136	—
6.2.2.5	2.9.11-430	—
6.2.2.4	2.9.11-371	—
6.2.2.3	2.9.11-303	—
6.2.2.2	2.9.11-273	—
6.2.2.1	2.9.11-207	—
6.2.2	2.9.11-125	—
6.2.1	2.9.11-101	—
6.2.0.6	2.9.10-301	—
6.2.0.5	2.9.10-255	—
6.2.0.4	2.9.10-205	—
6.2.0.3	2.9.10-160	—
6.2.0.2	2.9.10-126	—
6.2.0.1	2.9.10-98	—
6.2.0	2.9.10-42	—
6.1.0.7	2.9.9-312	—
6.1.0.6	2.9.9-258	—
6.1.0.5	2.9.9-225	—
6.1.0.4	2.9.9-191	—
6.1.0.3	2.9.9-159	—

Management Center	Snort 2	Snort 3
6.1.0.2	2.9.9-125	—
6.1.0.1	2.9.9-92	—
6.1.0	2.9.9-330	—
6.0.1.4	2.9.8-490	—
6.0.1.3	2.9.8-461	—
6.0.1.2	2.9.8-426	—
6.0.1.1	2.9.8-383	—
6.0.1	2.9.8-224	—
6.0.0.1	2.9.8-235	—
6.0.0	2.9.8-229	—

시스템 데이터베이스

취약성 데이터베이스(VDB)는 호스트가 영향을 받기 쉬운 잘 알려진 취약성의 데이터베이스일 뿐만 아니라 운영 체제, 클라이언트 및 애플리케이션의 지문입니다. 시스템이 VDB를 사용하여 특정 호스트가 침해 위험을 높이는지 여부를 결정합니다.

GeoDB(지리위치 데이터베이스)는 지리적 위치를 기준으로 트래픽을 보고 필터링하는 데 사용할 수 있는 데이터베이스입니다.

표 ***10:***

Management Center	VDB	GeoDB
7.2.0	4.5.0-353	2022-05-11-103
7.1.0	4.5.0-346	2020-04-28-002
7.0.2	4.5.0-338	2020-04-28-002
7.0.1	4.5.0-338	2020-04-28-002
7.0.0	4.5.0-338	2020-04-28-002
6.7.0	4.5.0-338	2020-04-28-002
6.6.5	4.5.0-336	2019-06-03-002
6.6.4	4.5.0-336	2019-06-03-002
6.6.3	4.5.0-336	2019-06-03-002

Management Center	VDB	GeoDB
6.6.1	4.5.0-336	2019-06-03-002
6.6.0	4.5.0-328	2019-06-03-002
6.5.0	4.5.0-309	2019-06-03-002
6.4.0	4.5.0-309	2018-07-09-002
6.3.0	4.5.0-299	2018-07-09-002
6.2.3	4.5.0-290	2017-12-12-002
6.2.2	4.5.0-271	2017-01-17-002
6.2.1	4.5.0-271	2017-01-17-002
6.2.0	4.5.0-271	2015-10-12-001
6.0.1	4.5.0-271	2015-10-12-001
6.0.0	4.5.0-271	2015-10-12-001

통합 제품

아래에 나열된 Cisco 제품에는 다른 호환성 요구 사항이 있을 수 있습니다. 예를 들어 특정 하드웨어 또는 특정 운영 체제에서 실행해야 할 수 있습니다. 자세한 내용은 해당 제품의 설명서를 참조하십시오.

참고 가능하면 각 통합 제품의 최신 호환 버전을 사용하는 것이 좋습니다. 이렇게 하면 최신 기능, 버그 수정 및 보안 패치를 사용할 수 있습니다.

ID 서비스 및 사용자 제어

다음을 참고하십시오.

- Cisco ISE 및 ISE-PIC: 다른 조합도 가능하지만 향상된 호환성 테스트를 제공하는 ISE 및 ISE-PIC 버전이 나열됩니다.
- Cisco Firepower 사용자 에이전트: 버전 6.6은 사용자 에이전트 소프트웨어를 ID 소스로 지원하는 마지막 management center 릴리스입니다. 이렇게 하면 버전 6.7 이상으로의 업그레이드가 차단됩니다.
- Cisco TS Agent: 버전 1.0 및 1.1은 더 이상 사용할 수 없습니다.

표 *11:* 통합 제품*: ID* 서비스/사용자 제어

Management Center/Threat Defense	**Cisco ISE(Identity Services Engine)**		**Cisco Firepower User Agent**	**Cisco Terminal Services(TS)** 에이전트
	ISE	**ISE-PIC**		
지원 대상	Management Center 디바이스 관리자	Management Center 디바이스 관리자	Management Center 전용	Management Center 전용
7.2	3.1 3.0 2.7 패치 2 이상	3.1 2.7 패치 2 이상	—	1.4 1.3
7.1	3.1 3.0 2.7 패치 2 이상	3.1 2.7 패치 2 이상	—	1.4 1.3
7.0	3.1 3.0 2.7 패치 2 이상 2.6 패치 6 이상	3.1 2.7 패치 2 이상 2.6 패치 6 이상	—	1.4 1.3
6.7.x	3.0 2.7 패치 2 이상 2.6 패치 6 이상	2.7 패치 2 이상 2.6 패치 6 이상	—	1.4 1.3
6.6	3.0 2.6, 모든 패치 2.4	2.6, 모든 패치 2.4	2.5 2.4	1.4 1.3 1.2
6.5	2.6 2.4	2.6 2.4	2.5 2.4	1.4 1.3 1.2 1.1
6.4	2.4 2.3 패치 2 2.3	2.4 2.2 패치 1	2.5 2.4 2.3, ASA FirePOWER 없음	1.4 1.3 1.2 1.1

Management Center/Threat Defense	Cisco ISE(Identity Services Engine)		Cisco Firepower User Agent	Cisco Terminal Services(TS) 에이전트
	ISE	ISE-PIC		
6.3	2.4 2.3 패치 2 2.3	2.4 2.2 패치 1 2.4	2.4 2.3, ASA FirePOWER 없음	1.2 1.1
6.2.3	2.3 패치 2 2.3 2.2 패치 5 2.2 패치 1 2.2	2.2 패치 1	2.4 2.3	1.2 1.1
6.2.2	2.3 2.2 패치 1 2.2 2.1	2.2 패치 1	2.3	1.2 1.1 1.0
6.2.1	2.1 2.0.1 2.0	2.2 패치 1	2.3	1.1 1.0
6.2.0	2.1 2.0.1 2.0 1.3	—	2.3	—
6.1	2.1 2.0.1 2.0 1.3	—	2.3	—
6.0.1	1.3	—	2.3	—
5.x	—	—	2.2	—

위협 탐지

Cisco Security Analytics and Logging(온프레미스)에는 SMC(Stealthwatch Management Console)용 Security Analytics and Logging On Prem 앱이 필요합니다. SMC의 SWE(Stealthwatch Enterprise) 요구 사항에 대

한 자세한 내용은 Cisco Security Analytics and Logging 온프레미스: Firepower 이벤트 통합 가이드를 참조하십시오.

표 *12:* 통합 제품*:* 위협 탐지

Management Center/Threat Defense	Cisco SecureX	Cisco Security Analytics and Logging(SaaS)	Cisco Security Analytics 및 Logging (온프레미스)	Cisco Secure Malware Analytics	Cisco Security Packet Analyzer
지원 대상	Management Center 디바이스 관리자	Management Center 디바이스 관리자	Management Center 전용	Management Center 전용	Management Center 전용
7.2	예	예	예	예	—
7.1	예	예	예	예	—
7.0	예	예	예	예	—
6.7	예	예	예	예	—
6.6	예	예	예	예	—
6.5	예	예	예	예	—
6.4	예	예	예	예	예
6.3	—	—	—	예	예
6.2.3	—	—	—	예	—
6.2.2	—	—	—	예	—
6.2.1	—	—	—	예	—
6.2.0	—	—	—	예	—
6.1	—	—	—	예	—

Cisco Secure Dynamic Attributes Connector

Cisco Secure Dynamic Attributes Connector는 클라우드/가상 워크로드 변경 사항을 기반으로 management center에서 방화벽 정책을 빠르고 원활하게 업데이트하는 경량 애플리케이션입니다. 자세한 내용은 Cisco Secure Dynamic Attributes Connector 구성 가이드를 참고하십시오.

표 *13:* 통합 제품*: Cisco Secure Dynamic Attributes Connector*

Management Center	Cisco Secure Dynamic Attributes Connector
7.0+	1.0+

Threat Defense 원격 액세스 VPN

원격 액세스 VPN(RA VPN, Remote Access Virtual Private Network)을 사용하면 개별 사용자가 인터넷에 연결된 컴퓨터 또는 지원되는 모바일 디바이스를 사용하여 원격 위치에서 네트워크에 연결할 수 있습니다. 자세한 내용은 Cisco AnyConnect Secure Mobility Client 구성 설명서를 참조하십시오.

표 *14:* 통합 제품*: Threat Defense RA VPN*

Threat Defense	Cisco AnyConnect Secure Mobility Client
6.2.2 이상	4.0 이상

End-of-Life 공지

다음 표에는 End-of-Life 세부사항이 나와 있습니다. 경과된 날짜는 굵게 표시됩니다.

소프트웨어

이러한 주요 소프트웨어 버전은 판매 및/또는 지원이 종료되었습니다.

표 *15:* 소프트웨어 *EOL* 알림

버전	판매 중단	지원 종료	공지사항
6.7	**2021-07-09**	2024-07-31	Cisco FTD(Firepower Threat Defense) 6.7, FMC(Firepower Management Center) 6.7 및 FXOS(Firepower eXtensible Operating System) 2.9(x)의 판매 중단 및 단종 알림
6.5	**2020-06-22**	2023-06-30	Cisco Firepower Threat Defense(FTD) 6.5(x), FMC(Firepower Management Center) 6.5(x) 및 Firepower eXtensible Operating System(FXOS) 2.7(x)의 판매 중단 및 단종 알림
6.3	**2020-04-30**	2023-04-30	Cisco Firepower Threat Defense(FTD) 6.2.2, 6.3(x), Firepower eXtensible Operating System(FXOS) 2.4.1 및 Firepower Management Center(FMC) 6.2.2 및 6.3(x)의 판매 중단 및 단종 알림
6.2.3	**2022-02-04**	2025-02-28	Cisco Firepower Threat Defense(FTD) 6.2.3, Firepower Management Center(FMC) 6.2.3 및 Firepower eXtensible Operating System(FXOS) 2.2(x)의 판매 중단 및 단종 알림

버전	판매 중단	지원 종료	공지사항
6.2.2	**2020-04-30**	2023-04-30	Cisco Firepower Threat Defense(FTD) 6.2.2, 6.3(x), Firepower eXtensible Operating System(FXOS) 2.4.1 및 Firepower Management Center(FMC) 6.2.2 및 6.3(x)의 판매 중단 및 단종 알림
6.2.1	**2019-03-05**	**2022-03-31**	Cisco Firepower Threat Defense 버전 6.2.0 및 6.2.1의 판매 중단 및 단종 알림
6.2	**2019-03-05**	**2022-03-31**	Cisco Firepower Threat Defense 버전 6.2.0 및 6.2.1의 판매 중단 및 단종 알림
6.1	**2019-11-22**	2023-05-31	Cisco Firepower Threat Defense 버전 6.1, NGIPSv 및 NGFWv 버전 6.1, Firepower Management Center 6.1 및 Firepower eXtensible Operating System(FXOS) 2.0(x)의 판매 중단 및 단종 알림
6.0.1	**2017-11-10**	**2020-11-30**	Cisco Firepower 소프트웨어 릴리스 5.4, 6.0, 6.0.1 및 Firepower Management Center 소프트웨어 릴리스 5.4, 6.0, 6.0.1의 판매 중단 및 단종 알림
6.0.0	**2017-11-10**	**2020-11-30**	Cisco Firepower 소프트웨어 릴리스 5.4, 6.0, 6.0.1 및 Firepower Management Center 소프트웨어 릴리스 5.4, 6.0, 6.0.1의 판매 중단 및 단종 알림
5.4	**2017-11-10**	**2020-11-30**	Cisco Firepower 소프트웨어 릴리스 5.4, 6.0, 6.0.1 및 Firepower Management Center 소프트웨어 릴리스 5.4, 6.0, 6.0.1의 판매 중단 및 단종 알림
5.3	**2016-01-29**	**2018-07-31**	Cisco FirePOWER Software v5.3 및 v5.3.1 및 FireSIGHT Management Center 소프트웨어 v5.3 및 v5.3.1의 판매 중단 및 단종 알림

이러한 소프트웨어 버전은 Cisco 지원 및 다운로드 사이트에서 제거되었습니다.

참고 버전 6.2.3 이상에서 패치(네 번째 숫자 릴리스)를 제거하면 업그레이드한 원본 버전이 어플라이언스에서 실행됩니다. 즉, 최신 패치를 제거하기만 하면 더 이상 사용되지 않는 버전을 실행할 수 있습니다. 달리 명시되지 않는 한 더 이상 사용되지 않는 버전을 유지하지 마십시오. 대신 업그레이드하는 것이 좋습니다. 업그레이드가 불가능한 경우 사용되지 않는 패치를 제거합니다.

표 *16:* 소프트웨어 제거 버전

버전	제거된 날짜	관련된 버그 및 추가 디테일
6.5.0.3	**2020-03-02**: 디바이스 **2020-02-04**: FMC	CSCvs86257: 800_post/1025_vrf_policy_upgrade.pl에서 FMC 업그레이드가 실패합니다. 이는 업그레이드 버그입니다. 이 버전을 실행 중인 경우, 계속 사용해도 문제가 없습니다.
6.5.0.1	**2019-12-19**	CSCvr52109: 여러 디바이스에 구축한 후 FTD가 올바른 액세스 제어 규칙과 일치하지 않을 수 있음
6.4.0.6	**2019-12-19**	CSCvr52109: 여러 디바이스에 구축한 후 FTD가 올바른 액세스 제어 규칙과 일치하지 않을 수 있음
6.2.3.8	**2019-01-07**	CSCvn82378: FMC를 6.2.3.8-51로 업그레이드하면 ASA/FTD를 통과하는 트래픽이 전달을 중지할 수 있음
6.2.1	**2017-11-17**	해당 버전은 동일한 기능을 제공하고 Firepower 플랫폼 전체를 지원하는 버전 6.2.2로 대체되었습니다.
5.4.0.1	**2015**년	—
5.3.1.2	**2015**년	—

이러한 통합 제품은 더 이상 사용되지 않습니다.

표 *17:* 지원 중단된 통합 제품

제품	세부정보
Cisco Firepower 사용자 에이전트	버전 6.6은 Cisco Firepower 사용자 에이전트 소프트웨어를 ID 소스로 지원하는 마지막 릴리스입니다. 사용자 에이전트 구성이 포함된 FMC는 버전 6.7 이상으로 업그레이드할 수 없습니다. Cisco Identity Services Engine/Passive Identity Connector(ISE/ISE-PIC)로 지금 전환하는 것을 강력하게 권장합니다. 또한 현재 사용자 에이전트에서 사용할 수 없는 기능을 사용할 수도 있습니다. 라이선스를 변환하려면 영업팀에 문의하십시오. 자세한 내용은 Cisco Firepower 사용자 에이전트의 단종 및 지원 중단 발표 및 Firepower 사용자 ID: 사용자 에이전트에서 ID 서비스 엔진으로 마이그레이션 TechNote를 참조하십시오.
Cisco Terminal Services(TS) 에이전트	Cisco TS 에이전트 버전 1.0 및 1.1이 Cisco 지원 및 다운로드 사이트에서 제거되었습니다. 이 버전을 사용 중인 경우, 업그레이드하는 것이 좋습니다.
Cisco Security Packet Analyzer	Cisco Security 패킷 분석기는 버전 6.3 및 6.4와만 호환됩니다.

하드웨어

이러한 플랫폼은 판매 및/또는 지원이 종료되었습니다.

표 ***18: Management Center*** 하드웨어 ***EOL*** 알림

플랫폼	마지막 버전	판매 중단	지원 종료	공지사항
FMC 1000, 2500, 4500	7.0	**2019-07-12**	2024-07-31	Cisco Firepower Management Center 플랫폼 - FMC 1000, FMC 2500, FMC 4500 판매 중단 및 단종 발표
FMC 4000	6.6	**2017-03-31**	**2022-03-31**	Cisco Firepower Management Center 4000 판매 중단 및 단종 알림
FMC 2000	6.6	**2017-03-31**	**2022-03-31**	Cisco Firepower Management Center 2000 판매 중단 및 단종 알림
FMC 750	6.4	**2017-03-31**	**2022-03-31**	Cisco Firepower Management Center 750 판매 중단 및 단종 알림
FMC 1500	6.4	**2015-09-18**	**2020-09-30**	Cisco FireSIGHT Management Center 1500 제품의 판매 중단 및 단종 알림
FMC 3500	6.4.	**2015-08-31**	**2020-08-31**	Cisco FireSIGHT Management Center 3500 판매 중단 및 단종 알림
FMC 500, 1000, 3000	5.4	판매 종료	지원 종료됨	—