Cisco Secure Firewall Threat Defense 호환성 가이드

초판: 2022년 5월 5일

최종 변경: 2022년 6월 6일

Cisco Secure Firewall Threat Defense 호환성 가이드

이 가이드에서는 Cisco Secure Firewall Threat Defense의 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, 23 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 Management Center 호환성 가이드 Cisco Firepower 4100/9300 FXOS 호환성
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 Cisco Firepower 4100/9300 FXOS 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 Cisco Secure Firewall Device Manager 릴리스별 새로운 기능
문서 로드맵은 현재 사용 가능한 레거시 문서에 대한 링크를 제공합니다. 찾고 있는 것이 위에 나열 되지 않은 경우 로드맵을 시도 합니다.	Cisco Firepower 문서 탐색 Cisco FXOS 문서 탐색

Threat Defense 관리

이 표에는 위협 대응에 대해 지원되는 디바이스 및 관리 방법이 버전별로 나열되어 있습니다.

관리 방법

관리 센터를 사용하여 여러 디바이스를 원격으로 관리합니다. 관리 센터는 하드웨어, 가상 또는 클라우드 플랫폼으로 제공됩니다. 하드웨어 관리 센터 또는 관리 센터 가상는 관리되는 디바이스와 동일하거나 최신 버전을 실행해야 합니다.

단일 위협 대응 디바이스를 로컬로 관리하는 데 디바이스 관리자을 사용합니다.

관리 센터 대신 여러 위협 대응 디바이스를 원격으로 관리하려면 Cisco Defense Orchestrator(CDO)를 디바이스 관리자과 함께 사용합니다. 일부 구성에서는 여전히 필요하지만 디바이스 관리자를 사용하면 위협 대응 구축 전체에서 일관된 보안 정책을 설정하고 유지할 수 있습니다.

Threat Defense 하드웨어

표 *2: Threat Defense* 관리자 및 버전별 하드웨어

디바이스 플랫폼	디바이스 버전: **Management Center**		디바이스 버전: **Device Manager**	
	하드웨어 또는 가상 **Management Center**	클라우드 제공 **Management Center**	**Device Manager** 전용	**Device Manager + CDO**
Firepower 1010, 1120, 1140	6.4+	7.2+	6.4+	6.4+
Firepower 1150	6.5+	7.2+	6.5+	6.5+
Firepower 2110, 2120, 2130, 2140	6.2.1+	7.2+	6.2.1+	6.4+
Secure Firewall 3110, 3120, 3130, 3140	7.1+	7.2+	7.1+	7.1+

디바이스 플랫폼	디바이스 버전: **Management Center**		디바이스 버전: **Device Manager**	
	하드웨어 또는 가상 **Management Center**	클라우드 제공 **Management Center**	**Device Manager** 전용	**Device Manager + CDO**
Firepower 4110, 4120, 4140	6.0.1+	7.2+	6.5+	6.5+
Firepower 4150	6.1	7.2+	6.5+	6.5+
Firepower 4115, 4125, 4145	6.4+	7.2+	6.5+	6.5+
Firepower 4112	6.6+	7.2+	6.6+	6.6+
Firepower 9300: SM-24, SM-36, SM-44	6.0.1+	7.2+	6.5+	6.5+
Firepower 9300: SM-40, SM-48, SM-56	6.4+	7.2+	6.5+	6.5+
ISA 3000	6.2.3 이상	7.2+	6.2.3 이상	6.4+
ASA 5506-X, 5506H-X, 5506W-X	6.0.1~6.2.3	—	6.1~6.2.3	—
ASA 5508-X, 5516-X	6.0.1~7.0	—	6.1~7.0	6.4~7.0
ASA 5512-X	6.0.1~6.2.3	—	6.1~6.2.3	—
ASA 5515-X	6.0.1~6.4	—	6.1~6.4	6.4
ASA 5525-X, 5545-X, 5555-X	6.0.1~6.6	—	6.1~6.6	6.4 ~ 6.6

Threat Defense Virtual

표 ***3: Threat Defense Virtual*** 관리자 및 버전별

디바이스 플랫폼	디바이스 버전: **Management Center**		디바이스 버전: **Device Manager**	
	하드웨어/가상 **Management Center**	클라우드 제공 **Management Center**	**Device Manager** 전용	**Device Manager + CDO**
Alibaba	7.2+	7.2%	—	—
AWS	6.0.1+	7.2+	6.6+	6.6+
Azure	6.2+	7.2+	6.5+	6.5+
GCP	6.7+	7.2+	7.2+	7.2%

디바이스 플랫폼	디바이스 버전: **Management Center**		디바이스 버전: **Device Manager**	
	하드웨어/가상 **Management Center**	클라우드 제공 **Management Center**	**Device Manager** 전용	**Device Manager + CDO**
HyperFlex	7.0+	7.2+	7.0+	7.0+
KVM	6.1+	7.2+	6.2.3 이상	6.4+
Nutanix	7.0+	7.2+	7.0+	7.0+
OCI	6.7+	7.2+	—	—
OpenStack	7.0+	7.2+	—	—
VMWare	6.0.1+	7.2+	6.2.2 이상	6.4+

Threat Defense 하드웨어

Firepower 1000/2100 및 Secure Firewall 3100 Series

Firepower 1000/2100 및 Secure Firewall 3100 시리즈 디바이스는 FXOS 운영 체제를 사용합니다. 위협 대응을 업그레이드하면 FXOS도 자동으로 업그레이드됩니다. 각 Firepower 버전과 함께 번들로 제공되는 FXOS 버전에 대한 자세한 내용은 번들 구성 요소, 10 페이지을(를) 참조하십시오.

이러한 디바이스는 Cisco Secure Firewall ASA 호환성 대신 ASA를 실행할 수도 있습니다.

표 *4: Firepower 1000/2100* 및 *Secure Firewall 3100 Series* 호환성

Threat Defense	**Secure Firewall 3110** **Secure Firewall 3120** **Secure Firewall 3130** **Secure Firewall 3140**	**Firepower 1150**	**Firepower 1010** **Firepower 1120** **Firepower 1140**	**Firepower 2110** **Firepower 2120** **Firepower 2130** **Firepower 2140**
7.2	예	예	예	예
7.1	예	예	예	예
7.0		예	예	예
6.7		예	예	예
6.6		예	예	예
6.5		예	예	예

Threat Defense	Secure Firewall 3110 Secure Firewall 3120 Secure Firewall 3130 Secure Firewall 3140	Firepower 1150	Firepower 1010 Firepower 1120 Firepower 1140	Firepower 2110 Firepower 2120 Firepower 2130 Firepower 2140
6.4		—	예	예
6.3		—	—	예
6.2.3		—	—	예
6.2.2		—	—	예
6.2.1		—	—	예

Firepower 4100/9300

Firepower 4100/9300의 경우, 아래에 굵게 표시된 주요 위협 대응 버전에 대해 특별히 검증되고 권장되는 컴패니언 FXOS 버전이 있습니다. 이런 조합에 대해서는 향상된 테스트를 수행하므로 가능한 경우라면 언제든지 사용하십시오.

이러한 디바이스는 위협 대응 대신 ASA를 실행할 수도 있습니다. ASA 9.12 이상 및 위협 대응 6.4.0 이상을 사용하면 동일한 Firepower 9300 섀시의 별도 모듈에서 ASA와 위협 대응를 모두 실행할 수 있습니다. 자세한 내용은 Cisco Firepower 4100/9300 FXOS 호환성 를 참고하십시오.

문제를 해결하려면 FXOS를 최신 빌드로 업그레이드해야 할 수 있습니다. 결정에 도움이 필요하면 Cisco Firepower 4100/9300 FXOS 릴리스 노트를 참조하십시오.

참고 다음 주요 버전 시퀀스에서 흐름 오프로드를 수행하려면 위협 대응 및 FXOS의 특정 조합을 실행해야 합니다.

- 버전 6.2.2.x: FXOS 2.3.1.130 이상에서 버전 6.2.2.2 이상
- 버전 6.2.0.x: FXOS 2.2.1.x 또는 FXOS 2.2.2 빌드 17-86에서 버전 6.2.0.3 이상

표 ***5: Firepower 4100/9300*** 호환성

Threat Defense	FXOS	Firepower 9300		Firepower 4100 Series			
		SM-26 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
7.2	**2.12.0.31** 이상	예	예	예	예	예	예
7.1	**2.11.1.154** 이상 2.12.0.31 이상	예	예	예	예	예	예
7.0	**2.10.1.159** 이상 2.11.1.154 이상 2.12.0.31 이상	예	예	예	예	예	예
6.7	**2.9.1.131** 이상 2.10.1.159 이상 2.11.1.154 이상 2.12.0.31 이상	예	예	예	예	예	예
6.6	**2.8.1.105** 이상 2.9.1.131 이상 2.10.1.159 이상 2.11.1.154 이상 2.12.0.31 이상	예	예	예	예	예	예
6.5	**2.7.1.92** 이상 2.8.1.105 이상 2.9.1.131 이상 2.10.1.159 이상 2.11.1.154 이상	예	예	예	예	—	예
6.4	**2.6.1.157** 이상 2.7.1.92 이상 2.8.1.105 이상 2.9.1.131 이상 2.10.1.159 이상	예	예	예	예	—	예

Threat Defense	FXOS	Firepower 9300		Firepower 4100 Series			
		SM-26 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
6.3	**2.4.1.214** 이상 2.6.1.157 이상 2.7.1.92 이상 2.8.1.105 이상 2.9.1.131 이상	예	—	예	예	—	—
6.2.3	**2.3.1.73** 이상 2.4.1.214 이상 2.6.1.157 이상 2.7.1.92 이상 2.8.1.105 이상 참고 Firepower 6.2.3.16 이상에는 FXOS 2.3.1.157 이상이 필요합니다.	예	—	예	예	—	—
6.2.2	**2.2.2.x** 2.3.1.73 이상 2.4.1.214 이상 2.6.1.157 이상 2.7.1.92 이상	예	—	예	예	—	—
6.2.1	—	—	—	—	—	—	—
6.2.0	**2.1.1.x**, **2.2.1.x**, **2.2.2.x** 2.3.1.73 이상 2.4.1.214 이상 2.6.1.157 이상	예	—	예	예	—	—

Threat Defense	FXOS	Firepower 9300		Firepower 4100 Series			
		SM-26 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
6.1	**2.0.1.x** 2.1.1.x 2.3.1.73 이상	예	—	예	예	—	—
6.0.1	**1.1.4.x** 2.0.1.x	예	—	예	—	—	—

ASA 5500-X Series 및 ISA 3000

ASA 5500-X Series 및 ISA 3000 디바이스는 ASA 운영 체제를 사용합니다. 위협 대응을 업그레이드하면 ASA도 자동으로 업그레이드됩니다. 각 Firepower 버전과 함께 번들로 제공되는 ASA 버전에 대한 자세한 내용은 번들 구성 요소, 10 페이지을(를) 참조하십시오.

버전 7.0은 ASA 5500-X Series 디바이스를 지원하는 마지막 주요 위협 대응 릴리스입니다.

표 ***6: ASA 5500-X Series*** 및 ***ISA 3000*** 호환성

Threat Defense	ISA 3000	ASA 5508-X ASA 5516-X	ASA 5525-X ASA 5545-X ASA 5555-X	ASA 5515-X	ASA 5506-X ASA 5506H-X ASA 5506W-X ASA 5512-X
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	—
6.3	예	예	예	예	—
6.2.3	예	예	예	예	예
6.2.2	—	예	예	예	예

Threat Defense	ISA 3000	ASA 5508-X ASA 5516-X	ASA 5525-X ASA 5545-X ASA 5555-X	ASA 5515-X	ASA 5506-X ASA 5506H-X ASA 5506W-X ASA 5512-X
6.2.1	—	—	—	—	—
6.2.0	—	예	예	예	예
6.1	—	예	예	예	예
6.0.1	—	예	예	예	예

Threat Defense Virtual

버전 7.0 이상에서 위협 대응 가상는 처리량 요구 사항 및 원격 액세스 VPN 세션 제한에 따라 계층화된 성능의 Smart Software Licensing을 지원합니다. 지원되는 인스턴스, 처리량 및 기타 호스팅 요구 사항 구축에 대한 자세한 내용은 해당 시작 가이드를 참조하십시오.

표 *7: Threat Defense Virtual* 호환성*: VMware*

Threat Defense Virtual	VMware vSphere/VMware ESXi					
	7.0	6.7	6.5	6.0	5.5	5.1
7.2	예	예	예	—	—	—
7.1	예	예	예	—	—	—
7.0	예	예	예	—	—	—
6.7	—	예	예	예	—	—
6.6	—	예	예	예	—	—
6.5	—	예	예	예	—	—
6.4	—	—	예	예	—	—
6.3	—	—	예	예	—	—
6.2.3	—	—	예	예	예	—
6.2.2	—	—	—	예	예	—
6.2.1	—	—	—	—	—	—
6.2.0	—	—	—	예	예	—
6.1	—	—	—	예	예	—

Threat Defense Virtual	VMware vSphere/VMware ESXi					
	7.0	6.7	6.5	6.0	5.5	5.1
6.0.1	—	—	—	—	예	예

표 *8: Threat Defense Virtual* 호환성: 기타 *Hypervisors*

Threat Defense Virtual	Alibaba	AWS(Amazon Web Services)	Microsoft Azure(Azure)	GCP(Google Cloud Platform)	Cisco HyperFlex(HyperFlex)	KVM(kernel-based Virtual Machine)	Nutanix Enterprise Cloud(Nutanix)	OpenStack	OCI(Oracle Cloud Infrastructure)
7.2	예	예	예	예	예	예	예	예	예
7.1	—	예	예	예	예	예	예	예	예
7.0	—	예	예	예	예	예	예	예	예
6.7	—	예	예	예	—	예	—	—	예
6.6	—	예	예	—	—	예	—	—	—
6.5	—	예	예	—	—	예	—	—	—
6.4	—	예	예	—	—	예	—	—	—
6.3	—	예	예	—	—	예	—	—	—
6.2.3	—	예	예	—	—	예	—	—	—
6.2.2	—	예	예	—	—	예	—	—	—
6.2.1	—	—	—	—	—	—	—	—	—
6.2.0	—	예	예	—	—	예	—	—	—
6.1	—	예	—	—	—	예	—	—	—
6.0.1	—	예	—	—	—	—	—	—	—

번들 구성 요소

이 표에는 위협 대응 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.

Operating Systems(운영 체제)

ASA 5500-X Series 및 ISA 3000 디바이스는 ASA 운영 체제를 사용합니다. Firepower 1000/2100 및 Secure Firewall 3100 시리즈 디바이스는 FXOS 운영 체제를 사용합니다. 이러한 디바이스에서 위협 대응을 업그레이드하면 운영 체제가 자동으로 업그레이드됩니다.

표 *9:*

위협 방어	**ASA**	**FXOS**
7.2.0	9.18(1)	2.12.0.31
7.1.0.1	9.17(1.150)	2.11.1.154
7.1.0	9.17(1.0)	2.11.1.154
7.0.1.1	9.16(2.5)	2.10.1.175
7.0.2	9.16(3.11)	2.10.1.192
7.0.1	9.16(2.5)	2.10.1.175
7.0.0.1	9.16(1.25)	2.10.1.159
7.0.0	9.16(1)	2.10.1.159
6.7.0.3	9.15(1.19)	2.9.1.138
6.7.0.2	9.15(1.15)	2.9.1.138
6.7.0.1	9.15(1.8)	2.9.1.135
6.7.0	9.15(1)	2.9.1.131
6.6.5.2	9.14(3.22)	2.8.1.172
6.6.5.1	9.14(3.15)	2.8.1.172
6.6.5	9.14(3.6)	2.8.1.165
6.6.4	9.14(2.155)	2.8.1.1148
6.6.3	9.14(2.151)	2.8.1.1146
6.6.1	9.14(1.150)	2.8.1.129
6.6.0.1	9.14(1.216)	2.8.1.105
6.6.0	9.14(1.1)	2.8.1.105
6.5.0.5	9.13(1.18)	2.7.1.129
6.5.0.4	9.13(1.5)	2.7.1.117
6.5.0.3	9.13(1.4)	2.7.1.117

위협 방어	**ASA**	**FXOS**
6.5.0.2	9.13(1.151)	2.7.1.115
6.5.0.1	9.13(1.2)	2.7.1.115
6.5.0	9.13(1)	2.7.1.107
6.4.0.15	9.12(4.41)	2.6.1.254
6.4.0.14	9.12(4.37)	2.6.1.239
6.4.0.13	9.12(4.37)	2.6.1.239
6.4.0.12	9.12(4.152)	2.6.1.230
6.4.0.11	9.12(2.40)	2.6.1.214
6.4.0.10	9.12(2.38)	2.6.1.214
6.4.0.9	9.12(2.33)	2.6.1.201
6.4.0.8	9.12(2.18)	2.6.1.166
6.4.0.7	9.12(2.151)	2.6.1.156
6.4.0.6	9.12(2.12)	2.6.1.156
6.4.0.5	9.12(2.4)	2.6.1.144
6.4.0.4	9.12(2.4)	2.6.1.144
6.4.0.3	9.12(1.12)	2.6.1.133
6.4.0.2	9.12(1.10)	2.6.1.133
6.4.0.1	9.12(1.7)	2.6.1.133
6.4.0	9.12(1.6)	2.6.1.133
6.3.0.5	9.10(1.31)	2.4.1.255
6.3.0.4	9.10(1.28)	2.4.1.248
6.3.0.3	9.10(1.18)	2.4.1.237
6.3.0.2	9.10(1.12)	2.4.1.237
6.3.0.1	9.10(1.8)	2.4.1.222
6.3.0	9.10(1.3)	2.4.1.216
6.2.3.18	9.9(2.91)	2.3.1.219
6.2.3.17	9.9(2.88)	2.3.1.217
6.2.3.16	9.9(2.74)	2.3.1.180

위협 방어	**ASA**	**FXOS**
6.2.3.15	9.9(2.60)	2.3.1.167
6.2.3.14	9.9(2.55)	2.3.1.151
6.2.3.13	9.9(2.51)	2.3.1.144
6.2.3.12	9.9(2.48)	2.3.1.144
6.2.3.11	9.9(2.43)	2.3.1.132
6.2.3.10	9.9(2.41)	2.3.1.131
6.2.3.9	9.9(2.37)	2.3.1.122
6.2.3.8	9.9(2.37)	2.3.1.122
6.2.3.7	9.9(2.32)	2.3.1.118
6.2.3.6	9.9(2.26)	2.3.1.115
6.2.3.5	9.9(2.245)	2.3.1.108
6.2.3.4	9.9(2.15)	2.3.1.108
6.2.3.3	9.9(2.13)	2.3.1.104
6.2.3.2	9.9(2.8)	2.3.1.85
6.2.3.1	9.9(2.4)	2.3.1.84
6.2.3	9.9(2)	2.3.1.84
6.2.2.5	9.8(2.44)	2.2.2.107
6.2.2.4	9.8(2.36)	2.2.2.86
6.2.2.3	9.8(2.30)	2.2.2.79
6.2.2.2	9.8(2.22)	2.2.2.75
6.2.2.1	9.8(2.10)	2.2.2.63
6.2.2	9.8(2.3)	2.2.2.52
6.2.1	9.8(1)	2.2.1.49
6.2.0.6	9.7(1.25)	—
6.2.0.5	9.7(1.23)	—
6.2.0.4	9.7(1.19)	—
6.2.0.3	9.7(1.15)	—

위협 방어	**ASA**	**FXOS**
6.2.0.2	9.7(1.10)	—
6.2.0.1	9.7(1.7)	—
6.2.0	9.7(1.4)	—
6.1.0.7	9.6(4.12)	—
6.1.0.6	9.6(3.23)	—
6.1.0.5	9.6(2.21)	—
6.1.0.4	9.6(2.16)	—
6.1.0.3	9.6(2.16)	—
6.1.0.2	9.6(2.4)	—
6.1.0.1	9.6(2.4)	—
6.1.0	9.6(2)	—
6.0.1.4	9.6(1.19)	—
6.0.1.3	9.6(1.12)	—
6.0.1.2	9.6(1.11)	—
6.0.1.1	9.6(1)	—
6.0.1	9.6(1)	—
6.0.0.1	9.6(1)	—
6.0.0	9.6(1)	—

Snort

Snort는 기본 검사 엔진입니다. Snort 3은 디바이스 관리자 버전 6.7 이상 및 관리 센터 버전 7.0 이상에서 사용할 수 있습니다.

표 ***10:***

위협 방어	**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

위협 방어	**Snort 2**	**Snort 3**
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
7.0.0	2.9.18-174	3.1.0.1-174
6.7.0.3	2.9.17-3014	3.0.1-4.129
6.7.0.2	2.9.17-2003	3.0.1.4-129
6.7.0.1	2.9.17-1006	3.0.1.4-129
6.7.0	2.9.17-200	3.0.1.4-129
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	—

위협 방어	**Snort 2**	**Snort 3**
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	—
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	—

위협 방어	**Snort 2**	**Snort 3**
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	—
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	—

위협 방어	**Snort 2**	**Snort 3**
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	—
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	—

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 ***11:***

위협 방어	**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

위협 방어	**VDB**	**GeoDB**
6.6.4	4.5.0-336	2019-06-03-002
6.6.3	4.5.0-336	2019-06-03-002
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

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 관리 센터 릴리스입니다. 이렇게 하면 버전 6.7 이상으로의 업그레이드가 차단됩니다.
- Cisco TS Agent: 버전 1.0 및 1.1은 더 이상 사용할 수 없습니다.

표 *12:* 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
클라우드 제공 관리 센터(버전 없음)	3.1 3.0 2.7 패치 2 이상	3.1 2.7 패치 2 이상	—	1.4
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

Management Center/Threat Defense	Cisco ISE(Identity Services Engine)		Cisco Firepower User Agent	Cisco Terminal Services(TS) 에이전트
	ISE	ISE-PIC		
6.4	2.4 2.6 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
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	—

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

표 ***13:*** 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 FTD 6.4가 설치된 FMC가 필요합니다.	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 관리 센터에서 방화벽 정책을 빠르고 원활하게 업데이트하는 경량 애플리케이션입니다. 자세한 내용은 Cisco Secure Dynamic Attributes Connector 구성 가이드를 참고하십시오.

표 *14:* 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 *15:* 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 *16:* 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

버전	판매 중단	지원 종료	공지사항
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
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

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 ***17:*** 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 실패 합니다. 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

버전	제거된 날짜	관련된 버그 및 추가 디테일
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.

하드웨어

이러한 플랫폼은 판매 및/또는 지원이 종료되었습니다.

표 ***18: Threat Defense*** 하드웨어 ***EOL*** 알림

Platform(플랫폼)	마지막 버전	판매 중단	지원 종료	공지사항
Firepower 4110	—	**2022-01-31**	2027-01-31	Cisco Firepower 4110 Series 보안 어플라이언스 및 5년 구독 판매 중단 및 단종 발표
ASA 5508-X, 5516-X	7.0	**2021-08-02**	2026-08-31	Cisco ASA5508 및 ASA5516 Series Security Appliance 및 5년 구독 판매 중단 및 단종 발표
ASA 5525-X, 5545-X, 5555-X	6.6	**2020-09-04**	2025-09-30	Cisco ASA5525, ASA5545 및 ASA5555 Series 보안 어플라이언스 및 5년 구독 판매 중단 및 단종 발표
Firepower 4120, 4140, 4150 Firepower 9300: SM-24, SM-36, SM-44 모듈	—	**2020-08-31**	2025-08-31	Cisco Firepower 4120/40/50 및 FPR 9300 SM24/36/44 Series 보안 어플라이언스/모듈 및 5년 구독 판매 중단 및 단종 발표
ASA 5515-X	6.4	**2017-08-25**	2022-08-31	Cisco ASA 5512-X and ASA 5515-X 판매 중단 및 단종 발표

Platform(플랫폼)	마지막 버전	판매 중단	지원 종료	공지사항
ASA 5506-X, 5506H-X, 5506W-X	6.2.3	**2021-08-02**	2026-08-31	ASA 소프트웨어를 사용하는 Cisco ASA5506 Series Security Appliance의 판매 중단 및 단종 알림
		2021-07-31	2022-07-31	Cisco ASA5506 Series Security Appliance 1년 구독 판매 중단 및 단종 알림
		2020-05-05	2022-07-31	Cisco ASA5506 Series Security Appliance 3년 구독 판매 중단 및 단종 발표
		2018-09-30	2022-07-31	Cisco ASA5506 Series Security Appliance 5년 구독 판매 중단 및 단종 발표
ASA 5512-X	6.2.3	**2017-08-25**	2022-08-31	Cisco ASA 5512-X 및 ASA 5515-X 판매 중단 및 단종 발표