Firepower 릴리스 노트, 버전 6.2.1

초판: 2017년 05월 15일

최종 변경: 년 월 일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

목 차

1 장

소개

이 문서에서는 어플라이언스를 버전 6.2.1(으)로 업데이트하거나 이미지를 재설치하는 방법을 설명합니다.

이 릴리스 노트의 내용을 잘 알고 있더라도 빠짐없이 읽고 숙지하십시오.

주의

Firepower Threat Defense 디바이스 또는 Firepower Threat Defense 디바이스를 관리하는 Firepower Management Center는에서 이미지를 재설치하기 전에 관리하는 어플라이언스를 Cisco Smart Software Manager에서 등록 취소해야 합니다. 관리하는 어플라이언스를 등록 취소하지 않으면 Smart Software Manager에서 전체 엔타이틀먼트에 대해 고아 엔타이틀먼트가 생깁니다. 어플라이언스 이미지 재설치를 시작하기 전에 Smart Software Manager에서 고아 엔타이틀먼트를 제거해야 합니다. 자세한 내용은 Cisco Smart Software Manager에서 Firepower Management Center는 등록 취소, 39 페이지 및 Cisco Smart Software Manager에서 Firepower Threat Defense 디바이스 등록 취소에 Firepower Device Manager 사용, 39 페이지를 참조하십시오.

2 장

버전 6.2.1의 지원되는 플랫폼 및 환경

참고

버전 6.2.1에서는 7000 및 8000 Series 디바이스, NGIPSv(가상 매니지드 디바이스), ASA(FirePOWER 모듈), Cisco ASA with Firepower Threat Defense, Firepower Threat Defense 디바이스(Firepower 4110, Firepower 4120, Firepower 4140, Firepower 4150, Firepower 9300 Appliance) 또는 Firepower Threat Defense virtual과 같은 어플라이언스를 지원하지 않습니다.

다음 플랫폼에서 버전 6.2.1을(를) 설치할 수 있습니다.

표 *1:* 지원되는 플랫폼 및 환경

지원되는 플랫폼	지원되는 환경
Firepower Management Center는: MC750, MC1000, MC1500, MC2000, MC2500, MC3500, MC4000, MC4500	–
64비트 Firepower Management Center Virtual	• VMware vSphere/VMware ESXi 5.5 • VMware vSphere/VMware ESXi 6.0 • AWS(Amazon Web Services) VPC/EC2 • KVM(Kernel-based virtual machine)
Firepower 2100 Series 디바이스(Firepower Threat Defense): Firepower 2110, Firepower 2120, Firepower 2130, Firepower 2140	• Firepower Management Center는 • Firepower Management Center Virtual • Firepower Device Manager

3 장

버전 6.2.1의 관리 기능

버전 6.2.1의 관리 옵션에 대한 자세한 내용은 다음 섹션을 참조하십시오.

관리 기능: Firepower Management Center는

Firepower Management Center는 웹 인터페이스를 사용하여 Firepower Management Center는 및 그 매니지드 디바이스를 구성하고 관리할 수 있습니다.

Firepower Management Center는에서 버전 6.2.1을(를) 실행하고 있다면 아래의 표에 지정된 버전을 실행하는 디바이스를 관리할 수 있습니다.

참고 Firepower Management Center는는 적어도 버전 6.2.1을(를) 실행하고 있어야 Firepower Threat Defense에서 버전 6.2.1을(를) 실행 중인 Firepower 2100 Series를 관리할 수 있습니다.

표 *2:* 버전 ***6.2.1****을(를)* 실행 중인 ***Firepower Management Center****는에서 관리하기 위한 디바이스 버전 요구 사항*

디바이스	디바이스의 최소 필수 버전
7000 및 8000 Series 매니지드 디바이스	버전 6.1.0 이상 또는 버전 6.2.0 이상
NGIPSv 가상 매니지드 디바이스	버전 6.1.0 이상 또는 버전 6.2.0 이상
ASA with FirePOWER Services: ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5512-X, ASA5515-X, ASA5516-X, ASA5525-X, ASA5545-X, ASA5555-X, ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, ASA5585-X-SSP-60	버전 6.1.0 이상 또는 버전 6.2.0 이상

디바이스	디바이스의 최소 필수 버전
ASA with Firepower Threat Defense: ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5512-X, ASA5515-X, ASA5516-X, ASA5525-X, ASA5545-X, ASA5555-X	버전 6.1.0 이상 또는 버전 6.2.0 이상
Firepower 2100 Series with Firepower Threat Defense: 2110, Firepower 2120, Firepower 2130, Firepower 2140	버전 6.2.1
Firepower 4100 Series with Firepower Threat Defense: Firepower 4110, Firepower 4120, Firepower 4140, Firepower 4150	버전 6.1.0 이상 또는 버전 6.2.0 이상
Firepower 9300 Appliance with Firepower Threat Defense	버전 6.1.0 이상 또는 버전 6.2.0 이상
Firepower Threat Defense Virtual	VMWare: Version 6.1.0 이상 또는 버전 6.2.0 이상 AWS(Amazon Web Services): 버전 6.1.0 이상 또는 버전 6.2.0 이상 KVM(Kernel-based virtual machine): 버전 6.1.0 이상 또는 버전 6.2.0 이상 Azure: 버전 6.2.0 이상

로컬 관리 기능**: Firepower Device Manager**

Firepower Device Manager에서 관리하는 **Firepower Threat Defense** 디바이스

지원되는 플랫폼**:** 하드웨어: Firepower 2110, Firepower 2120, Firepower 2130, Firepower 2140.

Firepower Device Manager에서 버전 6.2.1을(를) 실행 중인 Firepower Threat Defense 디바이스를 구성하고 관리할 수 있습니다. 컨피그레이션 및 관리에 대해서는 *Firepower Device Manager*용 *Cisco Firepower Threat Defense* 컨피그레이션 가이드의 내용을 참조하십시오.

4 장

새로운 기능

이 섹션에서는 버전 6.2.1의 새로운 기능 및 업데이트된 기능을 설명합니다. Firepower 2100 Series 디바이스만 버전 6.2.1을(를) 지원하므로 디바이스에 구축된 새 기능은 Firepower 2100 Series에서만 지원됩니다.

표 ***3:*** 버전 ***6.2.1***의 새 기능*:* 코어 방화벽

기능	설명	지원되는 플랫폼
원격 액세스 VPN		• Firepower Management Center는

기능	설명	지원되는 플랫폼
	Firepower RA(Remote Access) VPN은 개별 사용자가 인터넷에 연결된 랩톱 또는 데스크톱, Android, Apple iOS 모바일 디바이스를 사용하여 전용 비즈니스 네트워크에 연결할 수 있게 합니다. 원격 사용자는 공유 미디어 및 인터넷을 통해 전송되는 데이터에 중요한 암호화 기술을 사용하여 안전하게, 자신 있게 데이터를 전송합니다. RA VPN의 주요 기능: • 보안 액세스 - Cisco AnyConnect VPN 클라이언트에서 제공하며 SSL 또는 IPsec 터널링/암호화 프로토콜을 사용합니다. 원격 액세스 연결이 지원되는 유일한 클라이언트입니다. • 인증 및 권한 부여 액세스 – 인증(LDAP/AD/RADIUS 및 클라이언트 인증서 기반), 권한 부여(RADIUS 권한 부여 속성-DACL, 그룹 속성, 주소 지정 등), 어카운팅(RADIUS)을 위한 AAA 지원. • VPN 연결 - 연결 프로파일 및 그룹 정책을 통해 주소 지정, 스플릿 터널링, DNS 서버, 시간 초과, 액세스 시간, 클라이언트 방화벽 ACL, AnyConnect 클라이언트 프로파일을 정의할 수 있습니다. • 모니터링 및 트러블슈팅 – 여러 분석 보기를 제공하므로 장기적으로 VPN 사용자 활동을 추적하고 분석할 수 있습니다. 또한 원격 액세스 VPN 트러블슈팅 로그를 볼 수 있습니다. RA VPN 정책 생성 또는 구축에 문제가 있거나 RA VPN 연결 또는 트래픽이 정상적이지 않거나 이벤트 및 통계가 제대로 입력되지 않을 경우 트러블슈팅을 사용할 수 있습니다. 이 기능은 현재 로그인한 VPN 사용자를 한꺼번에 로그아웃할 수도 있습니다. 이러한 기능은 Firepower Management Center는 또는 Firepower Device Manager에서 사용할 수 있습니다. • 가용성 - Firepower Threat Defense 고가용성, 멀티 인터페이스(듀얼 ISP), 다중 AAA 서버가 지원됩니다. • 라이선싱 - Apex, Plus, VPN 전용 라이선스는 AnyConnect 4.x 모델 기준 스마트 라이선싱. • 관리 - Firepower Management Center는 및 Firepower Device Manager의 간단한 RA VPN 마법사에서 빠르고 손쉽게 다음 항목을 설정할 수 있습니다. ◦ RA VPN 정책 컨피그레이션 엔티티: 연결 프로파일, 그룹 정책, 주소 풀 등 포함.	

기능	설명	지원되는 플랫폼
	◦ 원격 사용자가 Firepower Threat Defense 디바이스에 연결하는 데 쓰이는 보안 게이트웨이. ◦ 사용자가 VPN 연결 설정을 위해 액세스할 매니지드 Firepower Threat Defense의 인터페이스. ◦ 데스크톱 또는 랩톱 플랫폼에서 연결을 시작할 때 다운로드되는 AnyConnect 클라이언트 이미지. 모바일 디바이스는 앱스토어에서 AnyConnect를 얻습니다. • ID 통합 및 모니터링 - 7가지의 새로운 대시보드 위젯에서 사용자 VPN 활동을 모니터링할 수 있습니다. 여기에는 로그온 및 로그오프 이벤트, 활성 세션 상태, 특정 VPN 세션 모니터링/종료 기능이 포함됩니다.	
QoS/속도 제한의 개선 사항	속도 제한은 애플리케이션, 파일 다운로드 등 트래픽 속성을 기준으로 하여 네트워크 인터페이스를 오가는 트래픽의 속도를 관리하는 메커니즘입니다. 소스 영역, 대상 영역, 소스 네트워크, 대상 네트워크, 소스 포트, 대상 포트, 애플리케이션, 사용자, URL, ISE 속성과 같은 트래픽 속성을 기준으로 하여 대역폭을 제어하는 기능과 연계하면 큰 효과를 거둘 수 있습니다. 네트워크 관리자는 Firepower Device Manager에서 QoS(Quality of Service) 정책을 구성하고 Firepower Threat Defense 디바이스에 이 정책을 구축하는 방법으로 네트워크 인터페이스별로 속도 제한을 실현할 수 있습니다. 관리자는 버전 6.2.1에서 다음 작업을 수행할 수 있습니다. • 최대 100,000Mbps로 트래픽 속도를 제한합니다(이전에는 1,000Mbps). • QoS 규칙에서 고객 SGT(Security Group Tag)를 사용합니다. • QoS 규칙에서 원본 클라이언트 네트워크 조건(XFF, True-Client-IP 또는 맞춤 설정 정의 HTTP 헤더)을 사용합니다.	• Firepower Management Center는

기능	설명	지원되는 플랫폼
충돌 시점의 패킷 캡처	이전에는 어플라이언스에 문제가 생기면 Firepower 활성 캡처의 내용이 저장되지 않았습니다. 이제는 어플라이언스에 충돌이 일어나면 활성 캡처의 내용을 플래시/디스크에 저장하여 트러블슈팅에 활용할 수 있습니다. 트래픽 관련 충돌의 트러블슈팅에서 Cisco TAC가 충돌의 원인이 된 트래픽에 대한 정확한 정보를 필요로 할 때가 많습니다. Cisco TAC는 코어 덤프에서 이 정보를 얻을 수 있으나, 다음 이유 때문에 이 정보가 제한될 수 있습니다. • 패킷이 손상되어 코어 덤프에 유용한 정보가 전혀 없을 수도 있습니다. • 일련의 패킷에서 비롯된 여러 조건의 조합이 충돌의 원인인데, 코어 덤프는 마지막 패킷의 정보만 제공합니다. 버전 6.2.1에서는 (캡처에 순환 옵션이 지정된 경우) 시스템 충돌 시점까지 Firepower 어플라이언스를 드나든 캡처된 패킷을 저장합니다.	• Firepower Management Center는 • Firepower Device Manager
액세스 규칙 벌크 삽입	버전 6.2.1에서는 REST API를 사용하여 벌크 액세스 제어 규칙 생성을 지원합니다. 이전에는 1,000개의 액세스 규칙을 생성해야 한다면 액세스 규칙마다 5초 ~ 10초 가량 걸리는 사후 프로세스를 거쳐야 했습니다. 이 API 개선 사항 덕분에 단일 사후 프로세스에서 모든 규칙을 제출할 수 있어 이 작업에 소요되는 시간이 크게 단축됩니다.	• Firepower Management Center는
Firepower Management Center는 API 개선 사항	Firepower Management Center는 API는 벌크 액세스 제어 규칙 생성을 지원합니다. 이전에는 1,000개의 액세스 규칙을 생성해야 한다면 액세스 규칙마다 5초 ~ 10초 가량 걸리는 사후 프로세스를 거쳐야 했습니다. 이 API 개선 사항 덕분에 단일 사후 프로세스에서 모든 규칙을 제출할 수 있어 이 작업에 소요되는 시간이 크게 단축됩니다.	• Firepower Management Center는

기능	설명	지원되는 플랫폼
AAB(Automatic Application Bypass)	AAB(Automatic Application Bypass)는 인터페이스를 통해 단일 패킷을 처리하는 데 드는 시간을 제한할 수 있습니다. 시간이 초과되면 이 패킷에서 탐지를 건너뛸 수 있습니다. 이 기능은 어떤 구축에서도 작동하지만, IPS 인라인 구축에서 패킷 처리 지연과 네트워크의 패킷 레이턴시 허용도를 균형적으로 조정하는 데 가장 효과적입니다. Snort 내 오작동 또는 디바이스 컨피그레이션 오류 때문에 트래픽 처리 시간이 지정된 임계값을 초과하면 AAB는 Snort가 다시 시작되게 하고, 과도한 처리 시간의 원인 규명을 위해 분석할 수 있는 트러블슈팅 데이터를 생성합니다. 이 옵션을 선택한 경우 우회 임계값을 변경할 수 있습니다. 기본 설정은 3000밀리초입니다. 유효한 범위는 250밀리초 ~ 60,000밀리초입니다.	• Firepower Management Center는

기능	설명	지원되는 플랫폼
FlexConfig 업데이트	FlexConfig에서는 Firepower Management Center는의 CLI 템플릿 기반 기능을 사용하여 Firepower Management Center는 사용자 인터페이스에서 아직 지원되지 않는 ASA 기능을 활성화합니다. 정부 인증 요구 사항에 따라 시스템 제공 또는 사용자 정의 FlexConfig 개체에 있는 모든 중요 정보(비밀번호, 공유 키 등)는 비밀 키 변수를 사용하여 마스킹해야 합니다. Firepower Management Center는를 버전 6.2.1(으)로 업데이트하면 FlexConfigObject의 모든 중요 정보가 비밀 키 변수 형식으로 변환됩니다. 또한 다음 새 FlexConfig 템플릿이 버전 6.2.1의 일부로 추가됩니다. • **TCP** 초기 연결 제한 및 시간 초과 컨피그레이션 템플릿을 사용하면 SYN Flood DoSAttack을 차단하기 위한 초기 연결 제한/시간 초과 CLI를 구성할 수 있습니다. • 위협 탐지 구성 및 해제 활성화 템플릿을 사용하면 TCP 인터셉트가 적용되는 공격의 위협 탐지 통계를 구성할 수 있습니다. • **IPV6** 라우터 헤더 검사 템플릿을 사용하면 다양한 유형의 특정 헤더를 선택적으로 허용/차단하도록 IPV6 검사 헤더를 구성할 수 있습니다(예: RH Type 2,mobile 허용). • **DHCPv6** 접두사 위임 템플릿을 사용하면 IPv6 접두사 위임을 위해 외부 인터페이스(PD 클라이언트) 및 내부 인터페이스(위임된 접두사의 수신자)를 하나씩 구성할 수 있습니다.	• Firepower Management Center는

기능	설명	지원되는 플랫폼
정책 구축 개선 사항	다음 항목의 컨피그레이션 구축 과정에서 Elimination of Snort가 재시작합니다. • SMTP, POP, IMAP 프리프로세서 복호화 깊이 • HTTP 프리프로세서 압축 깊이 • 영향을 받는 적응형 프로파일, 성능 모니터, 고급 액세스 제어 정책 파일 및 악성코드 설정 다음 상황에서 Warnings of Snort가 재시작합니다. • Firepower Threat Defense 고가용성 시작 또는 중지 • 애플리케이션 탐지 기능 활성화, 비활성화, 수정	• Firepower Management Center는
TCP 시퀀스 무작위화를 제어하는 CLI 명령	각 TCP 패킷은 2개의 시퀀스 번호를 전달합니다. 기본적으로 Firepower Threat Defense 디바이스는 인바운드 및 아웃바운드 방향 모두에서 시퀀스 번호를 무작위화합니다. 이 기능을 사용하면 명령줄에서 이 무작위화를 활성화하고 비활성화할 수 있습니다. 필요하다면 TCP 무작위화가 비활성화되었음을 확인하기 위해 내부 및 외부 인터페이스에서 TCP 패킷을 수집합니다. 내부 및 외부 인터페이스에서 동일한 패킷의 시퀀스 번호는 동일하게 유지됩니다.	• Firepower Management Center는 • Firepower Device Manager

표 *4:* 버전 ***6.2.1***의 새 기능*:* 정부 인증 지원

기능	설명	지원되는 플랫폼
사이트 대 사이트 VPN에 대한 정부 인증서 지원	사이트 대 사이트 VPN에 추가된 다음 기능은 버전 6.2.0에서는 지원되지 않았습니다. • 전송 모드 - 정부 인증서 요구 사항 FCS_IPSEC_EXT.1.3 Refinement를 지원하기 위한 전송 모드(호스트 대 호스트 VPN이라고도 함). • IKEv2 사전 공유 수동 키에 대한 16진수 지원 - 정부 인증서 요구 사항 FIA_PSK_EXT.1.4를 지원하기 위해 16진수 기반 사전 공유 키 지원을 추가했습니다. • 인증서 맵 지원 - 정부 인증서 요구 사항 FIA_X509_EXT.4.1을 지원하기 위해 인증서 콘텐츠로부터 사용할 터널을 결정하는 데 쓰일 인증서 맵을 구현했습니다. • SA 강도 적용 - 정부 인증서 요구 사항 FCS_IPSEC_EXT.1.12를 지원하기 위해 하위 IPsec SA에서 사용하는 암호화 알고리즘이 상위 IKE보다 높지 않게 하는 옵션을 Firepower Management Center는에 추가했습니다. 참고 지원되는 기능은 IKEv2만 대상으로 합니다.	• Firepower Management Center는 • Firepower Device Manager
플랫폼 설정 개선 사항(컴플라이언스 모드 지원)	다음 요구 사항은 Firepower Management Center는 버전 6.2.1 릴리스부터 지원되었습니다. • 사용자가 매니지드 Firepower Threat Defense 디바이스에 대해 콘솔 유휴 시간 초과를 구성할 수 있어야 합니다. • 사용자는 보안 syslog를 구성할 수 있습니다. 또한 Firepower Threat Defense syslog-NGTLS에 대한 인증서를 업로드할 수 있어야 합니다.	• Firepower Management Center는
Firepower Threat Defense에 대한 전문가 모드 비활성화 기능	보안을 강화하기 위해 Firepower Threat Defense 환경에서 전문가 모드를 비활성화할 수 있습니다.	• Firepower Management Center는 • Firepower Device Manager

기능	설명	지원되는 플랫폼
USGv6 FlexConfig: Firepower Management Center는 라우팅 헤더	FlexConfig에서는 Firepower Management Center는의 CLI 템플릿 기반 기능을 사용하여 Firepower Management Center는 사용자 인터페이스에서 아직 지원되지 않는 ASA 기능을 활성화합니다. USGv6 NPD:FW 인증에서는 USGv6GCT TME가 다양한 유형의 IPv6 헤더(예: EH, 라우팅 등)를 선택적으로 허용/차단해야 합니다. ASA FirePOWER 모듈에서는 사용자가 정책 맵을 사용하여 이를 허용할 수 있었지만 Firepower Management Center는에서는 구성하지 못했습니다. 이제는 정책 개체 및 정책 그룹을 개발하여 특정 IPv6 헤더를 차단, 허용, 로깅하는 정책을 구성할 수 있습니다. 다음 헤더 유형을 차단, 허용, 로깅할 수 있습니다. • 인증 확장 헤더 • 대상-옵션 확장 헤더 • ESP 확장 헤더 • 프래그먼트 확장 헤더 • 홉 바이 홉 확장 헤더 • 라우팅 헤더 유형 2-225	• Firepower Management Center는

• 기능 변경 사항, 16 페이지

기능 변경 사항

다음은 버전 6.2.1에서 변경된 사항입니다.

- 버전 6.2.0.1 또는 후속 버전인 6.2.0.x 패치를 버전 6.2.1(으)로 업데이트하면 사용자 인터페이스에서 IAB(Intelligent Application Bypass) **All applications including unidentified application(**식별되지 않은 애플리케이션을 포함한 모든 애플리케이션**)** 옵션이 사라집니다.

  버전 6.2.1(으)로 업데이트할 때 이 옵션이 활성화될 경우, 액세스 제어 정책에 바이패스 가능한 애플리케이션 및 필터 컨피그레이션이 없다면 사용자 인터페이스는 다음과 같이 예기치 않은 동작을 수행합니다.

  - IAB가 활성화되지만 **All applications including unidentified applications(**식별되지 않은 애플리케이션을 포함한 모든 애플리케이션**)** 옵션이 더 이상 나타나지 않습니다.
  - IAB 컨피그레이션 페이지의 **1 Applications/Filters(**애플리케이션/필터**)**에서 하나의 애플리케이션 또는 필터를 구성했다고 잘못 표시됩니다.

- 애플리케이션 및 필터 편집기의 Selected Applications and Filters(선택된 애플리케이션 및 필터) 창이 삭제된 애플리케이션(Firepower Management Center는, ASA with FirePOWER Services) 또는 임의의 애플리케이션(ASDM에서 관리하는 ASA FirePOWER 모듈)을 표시합니다.

5 장

버전 6.2.1의 제품 호환성

버전 6.2.1 웹 인터페이스와의 제품 호환성에 대한 자세한 내용은 다음 섹션을 참조하십시오.

통합 제품 호환성

다음 통합 제품에 필요한 버전은 FirePOWER 버전별로 다릅니다.

- Cisco ISE(Identity Services Engine)
- Cisco AMP Threat Grid
- Cisco Firepower System User Agent

필요한 버전에 대한 자세한 내용은 *Firepower System* 호환성 가이드를 참조하십시오.

버전 6.2.1의 웹 브라우저 호환성

버전 6.2.1의 Firepower 웹 인터페이스는 아래의 표에 나와 있는 브라우저에서 테스트받았습니다.

주의 Chrome 브라우저는 시스템에서 제공하는 자체 서명 인증서를 사용하여 이미지, CSS, Javascript와 같은 고정 콘텐츠를 캐시에 저장하지 않습니다. 따라서 새로고침할 때 고정 콘텐츠를 다시 다운로드할 수도 있습니다. 이를 방지하려면 브라우저/OS의 인증 저장소에 자체 서명 인증서를 추가하거나 다른 웹 브라우저를 사용하십시오.

표 *5:* 지원되는 웹 브라우저

브라우저	필수 활성화 옵션 및 설정
Google Chrome 57	JavaScript, 쿠키
Mozilla Firefox 52	JavaScript, 쿠키, TLS(Transport Layer Security) v1.1 또는 v1.2 참고 Firepower Management Center는에서 자체 서명 인증서를 사용하는 경우 로그인 화면을 로드하는 데 시간이 오래 걸리면 Firefox 웹 브라우저 검색 창에 **about:support**를 입력하고 **Refresh Firefox(Firefox** 새로고침**)**를 클릭합니다. Firefox를 새로고침하면 기존 Firefox 설정을 잃을 수도 있습니다. 자세한 내용은 https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings를 참조하십시오. Firepower Management Center는에서는 기본적으로 자체 서명 인증서를 사용합니다. 이 인증서를 신뢰받는 인증 기관에서 서명한 인증서로 대체하는 것이 좋습니다. 서버 인증서 교체에 대한 자세한 내용은 해당 버전의 *Firepower Management Center* 구성 가이드에서 시스템 컨피그레이션 섹션을 참조하십시오.
Microsoft Internet Explorer 10 및 11	JavaScript, 쿠키, TLS(Transport Layer Security) v1.1 또는 v1.2, 128비트 암호화, 액티브 스크립팅 보안 설정, 호환성 보기, **Check for newer versions of stored pages(**저장된 페이지의 새 버전 확인**)**를 **Automatically(**자동**)**로 설정 참고 Microsoft Internet Explorer 11 브라우저를 사용하는 경우 **Tools(**도구**) > Internet Options(**인터넷 옵션**) > Security(**보안**) > Custom level(**사용자 지정 수준**) ...**에서 **Include local directory path when uploading files to server(**파일을 서버에 업로드할 때 로컬 디렉터리 경로 포함**)** 옵션을 사용 안 함으로 설정해야 합니다.
Apple Safari 8 및 9	지원되지 않음
Microsoft Edge	지원되지 않음

화면 해상도 호환성

Firepower 관리를 위해 UI에 액세스할 때 아래 표의 화면 해상도를 선택하는 것이 좋습니다. 사용자 인터페이스는 낮은 해상도에서도 호환되지만, 높은 해상도에서 디스플레이가 최적화됩니다.

버전 6.2.1에서 지원되지 않는 플랫폼에 대한 권장 화면 해상도는 *Firepower* 릴리스 노트, 버전 6.2.0을 참조하십시오.

표 ***6:*** 웹 인터페이스별 권장 화면 해상도

웹 인터페이스	최소 권장 화면 해상도
Firepower Management Center는	가로 1280픽셀 이상
Firepower Device Manager(Firepower Threat Defense 관리)	가로 1024픽셀, 세로 768픽셀

6 장

버전 6.2.1의 용어

버전 6.2.1에 쓰이는 용어 및 브랜드가 이전 릴리스에 쓰인 것과 다를 수 있습니다. 다음 표에서 이를 간추려 정리했습니다. 용어 및 브랜드 변경에 대한 자세한 내용은 *Firepower System* 호환성 가이드를 참조하십시오.

표 ***7:*** 버전 ***6.2.1*** 제품 용어 및 브랜딩

이름	설명
Firepower Firepower System	제품 라인을 가리킵니다.
Firepower Management Center Management Center	물리적 또는 가상 FirePOWER 플랫폼에서 실행되는 FirePOWER 관리 소프트웨어를 가리킵니다.
Cisco ASA with FirePOWER Services ASA FirePOWER 모듈을 실행 중인 ASA 디바이스 ASA FirePOWER 모듈	ASA 플랫폼에 설치된 ASA 운영 체제에서 실행되는 FirePOWER 소프트웨어를 가리킵니다.
ASDM을 통해 매니지드 ASA FirePOWER 모듈	ASDM을 통해 액세스 가능한 ASA FirePOWER 모듈 로컬 컨피그레이션 인터페이스를 가리킵니다.
Firepower Threat Defense	ASA, Firepower 2100 Series, Firepower 4100 Series, Firepower 9300 Appliance 또는 가상 플랫폼의 Firepower 운영 체제에서 실행 중인 Firepower Threat Defense 소프트웨어를 가리킵니다.
Firepower Device Manager	특정 Firepower Threat Defense 플랫폼을 통해 액세스 가능한 Firepower Threat Defense 로컬 컨피그레이션 인터페이스를 가리킵니다.

7 장

버전 6.2.1 설명서

버전 6.2.1에서는 새로운 기능과 변경된 기능을 반영하고 보고된 설명서의 문제점을 해결하기 위해 다음 문서가 업데이트되었습니다.

- *Cisco Firepower Management Center* 컨피그레이션 가이드 및 온라인 도움말
- *Cisco Firepower Threat Defense Firepower Device Manager* 컨피그레이션 가이드 및 *Firepower Device Manager* 온라인 도움말
- *Firepower Threat Defense*용 명령 참조
- *Cisco ASA-Firepower Threat Defense* 마이그레이션 가이드
- *Cisco Firepower 2100 Series* 하드웨어 설치 가이드
- 규정 준수 및 안전 정보 - *Cisco Firepower 2100 Series*
- *Firepower Management Center*를 사용하는 *Firepower 2100 Series*용 *Cisco Firepower Threat Defense* 빠른 시작 가이드
- *Firepower Device Manager*를 사용하는 *Firepower 2100 Series*용 *Cisco Firepower Threat Defense* 빠른 시작 가이드
- *Cisco Firepower 2100 Series* 장애 및 오류 메시지
- *Firepower 2100 Series*용 *Cisco FXOS* 트러블슈팅 가이드
- *Firepower System Event Streamer* 통합 가이드
- *Cisco Firepower REST API* 참조 가이드
- *Cisco FirePOWER* 호환성 가이드
- *Firepower System Version 6.2.1*에 사용되는 오픈소스
- *Cisco Firepower System* 기능 라이선스

시스템 업데이트 및 컨피그레이션에 대한 자세한 내용은 *Cisco Firepower System* 설명서 로드맵(http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html)을 참조하십시오.

병렬 ASA 버전에 대한 ASA 설명서 로드맵 및 릴리스 노트(알려진 문제 포함)는 http://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html을 참조하십시오.

병렬 FXOS 버전에 대한 FXOS 설명서 로드맵 및 릴리스 노트(알려진 문제 포함)는 http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/roadmap/fxos-roadmap.html을 참조하십시오.

다음 항목도 참고하십시오.

- 버전 6.2.1에서 알려진 설명서 문제, 26 페이지

버전 6.2.1에서 알려진 설명서 문제

- *Firepower Management Center* 컨피그레이션 가이드에는 액세스 제어 규칙, SSL 규칙 또는 ID 규칙을 지리위치 네트워크 조건과 함께 구축할 경우 다른 국가로 이동하는 것처럼 보이는 IP 주소가 탐지될 때 시스템에서 해당 대륙 규칙을 알 수 없는 국가로 잘못 보고한다는 내용이 없습니다.

8 장

중요 업데이트 메모

이 릴리스로 업데이트하는 프로세스를 시작하기 전에 업데이트 과정의 시스템 동작, 호환성 문제 또는 업데이트 전후에 필요한 컨피그레이션 변경 사항을 숙지해야 합니다.

주의

업데이트 과정에서 로그인 프롬프트가 표시될 때까지는 어플라이언스를 리부팅하거나 종료하지 마십시오. 사전 확인 과정에서 시스템이 비활성 상태로 보일 수 있습니다. 이것은 정상적인 동작이므로 어플라이언스를 리부팅하거나 종료할 필요가 없습니다.

자세한 내용은 다음 섹션을 참고하십시오.

버전 6.2.1 경로 업데이트

어플라이언스는 Firepower 버전 6.2.0을 실행하고 있어야 버전 6.2.1(으)로 업데이트할 수 있습니다.

어플라이언스가 더 오래된 버전을 실행하고 있다면 버전 6.2.1(으)로 업데이트하기 전에 아래의 표에서 설명하는 업데이트를 수행해야 합니다.

참고 버전 6.2.1 업그레이드 경로에서 Firepower Management Center MC 750 또는 MC1500을 버전 5.4.x에서 버전 6.0으로 업데이트할 경우 어플라이언스 메모리 추가가 필요할 수 있습니다. 버전 6.0은 이전 Firepower 버전보다 많은 메모리가 필요합니다. Cisco 제품 요구 사항에 따라 메모리가 증가하는 것이므로 Cisco는 이 모델의 고객을 위해 메모리 업그레이드 키트를 무료로 제공하고 있습니다. 자세한 내용은 *Firepower System* 릴리스 노트 버전 *6.0*을 참조하십시오.

중요 아래의 경로에 있는 버전으로 업데이트할 경우 큰 변경이 일어나거나 필요할 수 있습니다. 또는 중요한 고려 사항이 생길 수도 있습니다. 예를 들어 버전 6.2.0으로 업데이트할 경우 중첩된 상관 관계 규칙이 제거됩니다. 따라서 이 변경과 관련하여 조치가 필요할 수도 있습니다. 업데이트 경로의 각 대상 버전에 대한 *Firepower System* 릴리스 노트(http://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html)를 참조하십시오.

버전 6.2.0이 되면 버전 6.2.1 업데이트, 33 페이지의 설명대로 버전 6.2.1(으)로 업데이트할 수 있습니다.

표 ***8:*** 어플라이언스별 업그레이드 경로

어플라이언스	지원되는 업데이트 경로
Firepower Management Center는: MC750, MC1000, MC1500, MC2000, MC 2500, MC3500, MC4000, MC 4500	버전 5.4.1.1 > 버전 6.0 설치 준비 패키지 > 버전 6.0 > 버전 6.0.1 설치 준비 > 버전 6.0.1. > 버전 6.1 설치 준비 패키지 > 버전 6.1 > 버전 6.2.0 > 버전 6.2.1
Firepower Management Center Virtual	

업데이트 순서 지침

고가용성 다음 업데이트 순서 요구 사항을 참고하십시오.

고가용성 **Firepower Management Center**는를 위한 업데이트 시퀀스

작업의 연속성을 보장하기 위해 고가용성 쌍의 Firepower Management Center는를 동시에 업데이트하지 마십시오. 다음 단계에 따라 안전하게 쌍을 업데이트할 수 있습니다.

단계 **1** Integtation(통합) 페이지의 High Availability(고가용성) 탭(**System(**시스템**) > Integration(**통합**)**)을 통해 고가용성 쌍의 액티브 Firepower Management Center는에서 동기화를 일시 중지합니다.*Firepower Management Center* 컨피그레이션 가이드의 쌍을 구성하는 Firepower Management Center 간 통신 일시 중지 항목을 참조하십시오.

단계 **2** 고가용성 쌍의 스탠바이 Firepower Management Center는를 업데이트합니다.

Firepower Management Center는가 스탠바이에서 액티브로 전환하므로 고가용성 쌍의 두 Firepower Management Center는 모두 액티브 상태가 됩니다.

업데이트가 성공적으로 완료됩니다.

단계 **3** 쌍의 나머지 Firepower Management Center는를 업데이트합니다.
업데이트가 완료됩니다.

단계 **4** Firepower Management Center는 웹 인터페이스 중 하나에서 High Availability(고가용성) 탭의 **Make-Me-Active**를 클릭합니다.
사용자가 액티브로 전환하지 않은 Firepower Management Center는는 자동으로 스탠바이 모드가 됩니다.

주의 업그레이드 프로세스에서 일어난 정책 변경사항은 고가용성을 재설정할 때 사라질 수 있습니다. 이는 업그레이드 후 어떤 어플라이언스를 액티브로 선택하느냐에 따라 달라집니다.

매니지드 디바이스를 등록하고 고가용성 스플릿 브레인 시나리오(두 어플라이언스 모두 액티브)에서 Firepower Management Center는에 정책을 구축할 경우 이 구축은 지원되지 않습니다. 스플릿 브레인을 해결하기 전에 반드시 스탠바이 Firepower Management Center는에서 모든 정책을 내보내고 모든 매니지드 디바이스를 등록 취소해야 합니다. 그런 다음 액티브 Firepower Management Center는에서 매니지드 디바이스를 등록하고 정책을 가져올 수 있습니다.

단계 **5** *Firepower Management Center* 컨피그레이션 가이드의 쌍을 구성하는 Firepower Management Center 간 통신 재시작 항목의 설명대로 통신을 다시 시작합니다.

업데이트 사전 컨피그레이션 및 이벤트 백업

업데이트를 시작하기 전에 현재 이벤트 및 컨피그레이션 데이터를 외부 위치에 백업하는 것이 강력히 권장됩니다. 외부 위치에 백업할 경우 외부 백업이 성공했음을 확인한 다음 시스템을 업데이트합니다.

Firepower Management Center는를 사용하여 이 시스템 및 여기에서 관리하는 디바이스에 대한 이벤트 및 컨피그레이션 데이터를 백업합니다. 백업 및 복원 기능에 대해서는 *Firepower Management Center* 구성 가이드의 내용을 참조하십시오.

Firepower Management Center는에서는 이전 업데이트에서 로컬에 저장된 백업을 제거합니다. 보관된 백업을 보존하려면 외부 장치에 백업을 저장하십시오.

버전 6.2.1로 업데이트하면 IAB 옵션이 바뀔 수 있습니다. IAB 옵션이 컨피그레이션에 미칠 영향에 대해서는 기능 변경 사항, 16 페이지의 내용을 참조하십시오.

업데이트 도중 트래픽 흐름 및 검사

업데이트 프로세스는 트래픽 검사, 트래픽 흐름, 링크 상태에 영향을 미칠 수 있으므로 유지 보수 기간에 또는 가동 중단이 구축에 미치는 영향이 최소화되는 시점에 업데이트를 수행하는 것을 강력히 권장합니다.

업데이트 프로세스는 모든 어플라이언스를 리부팅합니다. 디바이스가 어떻게 구성되고 구축되었는지에 따라 다음 기능이 영향을 받을 수 있습니다.

- 애플리케이션 인식 및 제어, URL 필터링, 보안 인텔리전스, 침입, 파일, 악성코드 검사/제어, 연결 로깅을 포함한 트래픽 검사
- 스위칭, 라우팅, NAT, VPN 및 관련 기능을 포함한 트래픽 흐름
- 링크 상태

인라인 구축의 경우, 컨피그레이션 구축 시 매니지드 디바이스가 (모델 및 트래픽 처리 방식에 따라) 트래픽에 영향을 미칠 수 있습니다.

업데이트 과정에서 디바이스가 트래픽 검사를 처리하는 방식에 대한 자세한 내용은 *Firepower* 릴리스 노트, 버전 6.2.0을 참조하십시오.

버전 **6.2.1** 업데이트를 위한 시간 및 디스크 공간 요구 사항

아래의 표에서는 업데이트를 위한 디스크 공간 및 시간 지침이 제공됩니다.

주의 업데이트 과정에서 로그인 프롬프트가 표시될 때까지는 어플라이언스를 리부팅하거나 종료하지 마십시오. 사전 확인 과정에서 시스템이 비활성 상태로 보일 수 있습니다. 이것은 정상적인 동작이므로 어플라이언스를 리부팅하거나 종료할 필요가 없습니다.

업데이트 진행에 문제가 있을 경우 Cisco TAC에 문의하십시오.

표 ***9:*** 시간 및 디스크 공간 요구 사항

어플라이언스	**/**에 필요한 공간	**/Volume**에 필요한 공간	**Manager /Volume**에 필요한 공간	시간
Firepower Management Center는	22 MB	11222 MB	–	42분
Firepower Management Center Virtual	23 MB	10436 MB	–	하드웨어에 따라 다름

업그레이드 사후 작업

Firepower Management Center는에서 업데이트를 수행한 다음 컨피그레이션 변경 사항을 구축해야 합니다.

컨피그레이션 변경 사항 구축 시 리소스 수요로 인해 일부 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그레이션을 구축하려면 Snort 프로세스를 재시작해야 하므로 트래픽 검사가 잠시 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 또는 추가 검사 없이 통과되는지 여부는 매니지드 디바이스의 모델 및 트래픽 처리 방법에 따라 달라집니다. 자세한 내용은 *Firepower Management Center* 구성 가이드, 버전 6.2.1을 참조하십시오.

구축한 기능이 제대로 작동하는지 확인하려면 업데이트 후 몇 가지 추가 단계를 수행해야 합니다. 예를 들면 다음과 같습니다.

- 업데이트가 성공했는지 확인
- 구축의 모든 어플라이언스가 성공적으로 통신하는지 확인
- (선택 사항) 침입 규칙 및 VDB(Vulnerability Database) 업데이트, 컨피그레이션 변경 사항 구축
- 새로운 기능에 따라 컨피그레이션 변경

9 장

버전 6.2.1 업데이트

업데이트를 시작하기 전에 이 릴리스 노트, 특히 중요 업데이트 메모, 27 페이지를 빠짐없이 읽고 숙지해야 합니다.

Firepower Management Center는 및 Firepower Management Center는 Virtual 업데이트

Firepower Management Center는 및 Firepower Management Center는 Virtual을 업데이트하려면 이 섹션의 절차를 사용합니다.

주의 업데이트 과정에서 로그인 프롬프트가 표시될 때까지는 어플라이언스를 리부팅하거나 종료하지 마십시오. 사전 확인 과정에서 시스템이 비활성 상태로 보일 수 있습니다. 이것은 정상적인 동작이므로 어플라이언스를 리부팅하거나 종료할 필요가 없습니다.

Firepower Management Center는를 업데이트하려면:

단계 **1** 고가용성 쌍의 Firepower Management Center는를 업데이트하려면 고가용성 Firepower Management Center는를 위한 업데이트 시퀀스, 28 페이지의 내용을 참조하십시오.

단계 **2** 버전 6.2.1 경로 업데이트, 27 페이지의 설명대로 최소 버전으로 업데이트합니다.

단계 **3** 릴리스 노트를 읽고 필요한 모든 업데이트 사전 작업을 완료합니다. 자세한 내용은 다음 링크를 참고하십시오.

- 버전 6.2.1의 제품 호환성, 19 페이지
- 중요 업데이트 메모, 27 페이지

단계 **4** 지원 사이트에서 업데이트 다운로드:
Sourcefire_3D_Defense_Center_S3_Upgrade-6.2.1-xxx.sh

참고 지원 사이트에서 직접 업데이트 패키지를 다운로드합니다. 업데이트 파일을 이메일로 전송하는 경우, 손상될 수 있습니다.

단계 **5** **System(**시스템**)** > **Updates(**업데이트_를 선택하고 **Product Updates(**제품 업데이트**)** 탭에서 **Upload Update(**업데이트 업로드**)**를 선택하여 Firepower Management Center는에 업데이트를 업로드합니다. 업데이트를 찾은 다음 **Upload(**업료드**)**를 클릭합니다.
업데이트는 Firepower Management Center는에 업로드됩니다. 웹 인터페이스에 방금 업로드한 업데이트의 유형, 버전 번호 및 생성된 날짜와 시간이 표시됩니다.

단계 **6** 모든 매니지드 디바이스에 컨피그레이션 변경사항을 재구축합니다. 그렇지 않으면 매니지드 디바이스의 최종 업데이트가 실패할 수 있습니다.

단계 **7** 구축의 어플라이언스가 성공적으로 통신하는지, 상태 모니터에서 보고하는 문제가 없는지 확인합니다.

단계 **8** 시스템 상태 아이콘을 클릭하고 Message Center의 **Tasks(**작업**)** 탭에서 진행 중인 작업이 없음을 확인합니다. 업데이트를 시작하기 전에 오랫동안 실행되는 작업이 모두 완료될 때까지 기다려야 합니다. 업데이트를 시작할 때 실행되고 있는 작업은 중단되고 실패한 작업이 되며 다시 시작할 수 없습니다. 업데이트가 완료된 후 작업 대기열에서 수동으로 삭제해야 합니다. 작업 대기열은 10초마다 자동으로 새로 고침됩니다.

단계 **9** **System(**시스템**)** > **Updates(**업데이트**)** 페이지에서 설치 중인 업데이트의 옆에 있는 설치 아이콘을 클릭합니다.

단계 **10** Firepower Management Center는를 선택하고 **Install(**설치**)**을 클릭합니다.

단계 **11** 업데이트 설치를 확인하고 Firepower Management Center는를 재부팅합니다.
업데이트 프로세스가 시작됩니다. Message Center의 **Tasks(**작업**)** 탭에서 업데이트 진행 상황 모니터링을 시작할 수 있습니다. 그러나 Firepower Management Center는가 필요한 사전 업데이트 점검을 완료하면 사용자는 로그아웃됩니다. 다시 로그인하면 Upgrade Status 페이지가 나타납니다. Upgrade Status(업그레이드 상태) 페이지에 진행률 표시줄이 표시되고, 현재 실행 중인 스크립트에 대한 정보가 나타납니다.

어떤 이유로든 업데이트가 실패하면 실패 시간 및 날짜, 업데이트가 실패했을 때 실행 중이었던 스크립트, Cisco TAC에 문의하는 방법을 알리는 오류 메시지가 페이지에 표시됩니다. 업데이트를 다시 시작하지 마십시오.

주의 업데이트에서 문제가 발생하면(예: Update Status(업데이트 상태) 페이지를 수동으로 새로 고친 후 몇 분이 흘러도 진행 상황이 표시되지 않음) 업데이트를 다시 시작하지 마십시오. 그 대신 Cisco TAC에 문의하십시오.

업데이트가 완료되면 Firepower Management Center는에서 성공 메시지를 표시한 후 재부팅됩니다.

단계 **12** 업데이트가 완료되면 브라우저 캐시를 지우고 브라우저를 다시 시작합니다. 이렇게 하지 않으면 사용자 인터페이스에서 예기치 않은 동작이 발생할 수 있습니다.

단계 **13** Firepower Management Center는에 로그인합니다.

단계 **14** **EULA(End User License Agreement)**가 나타나면 읽고 동의합니다. **EULA**에 동의하지 않으면 어플라이언스에서 로그아웃됩니다.

단계 **15** **Help(**도움말**)** > **About(**정보**)**을 선택하고 소프트웨어 버전이 정확하게 표시되는지 확인합니다. Firepower Management Center는에서 침입 규칙 업데이트 및 VDB의 버전도 확인하십시오. 이 정보는 나중에 필요합니다.

단계 **16** 구축의 어플라이언스가 성공적으로 통신하는지, 상태 모니터에서 보고하는 문제가 없는지 확인합니다.

단계 **17** 지원 사이트에서 제공하는 침입 규칙 업데이트가 Firepower Management Center는의 규칙보다 새 버전이면 이 새 규칙을 가져옵니다. 버전 6.2.1 작업 시 가져온 규칙을 자동 적용하지 마십시오.

침입 규칙 업데이트에 대해서는 *Firepower Management Center* 구성 가이드의 내용을 참조하십시오.

단계 **18** 지원 사이트에서 제공하는 VDB가 업데이트 과정에서 설치된 VDB보다 새 버전이면 이 최신 VDB를 설치합니다. 버전 6.2.1 작업 시 VDB 업데이트를 자동 적용하지 마십시오.
VDB 업데이트 설치 과정에서 컨피그레이션 변경사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 또는 추가 검사 없이 통과되는지 여부는 매니지드 디바이스의 모델 및 트래픽 처리 방법에 따라 달라집니다. 자세한 내용은 *Firepower Management Center* 구성 가이드을 참조하십시오.

단계 **19** 모든 매니지드 디바이스에 정책을 재구축합니다.
Deploy(구축**)** 버튼을 클릭하고 모든 사용 가능한 디바이스를 선택한 다음 **Deploy(**구축**)**를 클릭합니다.

단계 **20** 나중에 지원 사이트에서 패치가 제공될 경우 해당 버전의 *Firepower System* 릴리스 노트의 설명대로 최신 패치로 업데이트합니다. 최신 강화된 기능과 보안 수정 사항을 적용하려면 최신 패치로 업데이트해야 합니다.

단계 **21** 고가용성 쌍의 Firepower Management Center는를 업데이트한 경우 고가용성 Firepower Management Center는를 위한 업데이트 시퀀스, 28 페이지의 내용을 참조하여 통신을 다시 시작하십시오.

10 장

버전 6.2.1에 이미지 재설치 또는 구축

어플라이언스에 Firepower 이미지를 재설치하거나 가상 Firepower 환경을 구축하면 어플라이언스가 공장 기본 설정으로 돌아갑니다.

참고

버전 6.2.1에 디바이스 이미지를 재설치할 경우 리부팅 시퀀스 후 시스템 비밀번호가 기본값인 **Admin123**이 됩니다.

주의

Firepower Threat Defense 디바이스 또는 Firepower Threat Defense 디바이스를 관리하는 Firepower Management Center는에서 이미지를 재설치하기 전에 관리하는 어플라이언스를 Cisco Smart Software Manager에서 등록 취소해야 합니다. 관리하는 어플라이언스를 등록 취소하지 않으면 Smart Software Manager에서 전체 엔타이틀먼트에 대해 고아 엔타이틀먼트가 생깁니다. 어플라이언스 이미지 재설치를 시작하기 전에 Smart Software Manager에서 고아 엔타이틀먼트를 제거해야 합니다. 자세한 내용은 Cisco Smart Software Manager에서 Firepower Management Center는 등록 취소, 39 페이지 및 Cisco Smart Software Manager에서 Firepower Threat Defense 디바이스 등록 취소에 Firepower Device Manager 사용, 39 페이지를 참조하십시오.

자세한 내용은 다음 링크를 참고하십시오.

새로 지원되는 플랫폼의 이미지 재설치 또는 구축

버전 6.2.1에서 새로 지원하는 플랫폼에서 이미지를 재설치하고 구축하는 프로세스에 대한 자세한 내용은 다음을 참조하십시오.

- Firepower Management Center는에서 관리하는 형태로 Firepower 2100 Series를 구축하려면 *Firepower Management Center*는를 사용하는 *Firepower 2100 Series*용 *Cisco Firepower Threat Defense* 빠른 시작 가이드를 참조하십시오.
- Firepower Device Manager에서 관리하는 형태로 Firepower 2100 Series를 구축하려면 *Firepower Device Manager*를 사용하는 *Firepower 2100 Series*용 *Cisco Firepower Threat Defense* 빠른 시작 가이드를 참조하십시오.

기존 플랫폼 이미지 재설치 또는 구축

기존 플랫폼 이미지 재설치 또는 구축

기존 플랫폼의 이미지 재설치 및 구축 프로세스에 대한 자세한 내용은 아래 표의 설명대로 해당 플랫폼의 빠른 시작 가이드 또는 시작 가이드를 참조하십시오.

이 빠른 시작 가이드 및 시작 가이드를 찾으려면 *Cisco Firepower System* 가이드 로드맵(http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html) 및 *Cisco ASA Series* 가이드 탐색(http://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html)을 참조하십시오.

표 ***10:*** 플랫폼별 이미지 재설치 가이드

플랫폼	이미지 재설치 가이드
Firepower Management Center는: MC750, MC1000, MC1500, MC2000, MC2500, MC3500, MC4000, MC4500	모델 *750, 1500, 2000, 3500, 4000*용 *Cisco Firepower Management Center* 시작 가이드 또는 모델 *1000, 2500, 4500*용 *Cisco Firepower Management Center* 시작 가이드 참조
64비트 Firepower Management Center Virtual	*Cisco Firepower Management Center Virtual for VMware* 구축 빠른 시작 가이드 참조

Cisco Smart Software Manager에서 Firepower Management Center는 등록 취소

단계 1 **System**(시스템) > **Licenses**(라이선스) > **Smart Licenses**(스마트 라이선스)를 선택합니다.

단계 2 등록 취소 아이콘( )을 클릭합니다.

Cisco Smart Software Manager에서 Firepower Threat Defense 디바이스 등록 취소에 Firepower Device Manager 사용

단계 1 메뉴의 디바이스 이름을 클릭한 다음 스마트 라이선스 요약에서 **View Configuration**(컨피그레이션 보기)을 클릭합니다.

단계 2 기어 드롭다운 목록에서 디바이스 등록 취소를 선택합니다.

단계 3 경고를 확인한 후에 디바이스를 등록 취소하려면 등록 취소를 클릭합니다.

이미지 재설치 또는 구축 후

(모든 구축에서) 시스템이 항상 최신 위협에 대한 새로운 정보를 수집하도록 VDB(vulnerability database)를 업데이트합니다. *Firepower Management Center*는 컨피그레이션 가이드의 취약점 데이터베이스 업데이트 항목을 참조하십시오.

11 장

알려진 문제

다음 표에서는 이 릴리스 노트의 발표 시점에 열린 상태인 알려진 문제를 다룹니다. 알려진 문제의 최신 목록을 보려면 버그 검색 툴에서 제공된 쿼리를 실행합니다.

Cisco 지원 계약이 유효한 고객은 다음 동적 검색을 사용하여 버전 6.2.1에서 열린 상태이고 심각도 3 이상인 모든 버그를 찾을 수 있습니다. https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286259685&rls=6.2.1&sb=afr&sts=open&svr=3nH&bt=custV

고지 **ID** 번호	설명
CSCve19910	액세스 제어 정책이 네트워크 탭에서 개체를 호출할 때 IP 주소를 팝업하지 않음
CSCvd45772	inlineApplicationFilter를 사용하여 REST API를 통해 AC 규칙을 생성하면 정책 수정 UI 페이지가 불안정해짐
CSCve00784	[FMC] AC 검증 최적화에서 SSL 정책에 대해 유튜브/세이프서치 처리
CSCve21032	네트워크 카운트 표시 부정확
CSCve37832	CSSM이 FMC HA env에 있을 때 라이선스 동기화 실패
CSCve17347	진단 인터페이스에 도메인/디바이스 재정의 IP 풀을 지정할 수 없음
CSCve06445	설명을 변경할 때 레이어 화면에서 고급 설정 중복
CSCve32346	Firepower Management Center 고가용성의 SIGABRT ActionQueueScrape 코어
CSCve34792	FTD-NAT: 인라인 값을 갖는 NAT 그룹 개체가 인터페이스 IP로 중복되면 구축 실패
CSCvc84182	RAVPN 정책에 디바이스를 추가/제거하면 기존에 지정된 디바이스가 오래된 것으로 표시
CSCve31687	풀을 사용하는 활성 상태의 VPN 세션이 있으면 IPv6 풀 변경 사항 구축 실패

고지 **ID** 번호	설명
CSCve30147	서브도메인 SI 개체를 삭제할 수 없음
CSCvd64182	연결된 스위치 포트가 종료된 경우에도 관리 인터페이스 표시
CSCve24555	6.2.1 FMC가 최대 다운로드/업로드 값을 6.2.0/6.1.0 디바이스에 구축할 때 구축 장애 발생
CSCve36289	samba/SMB 파일 모니터 회피
CSCve17433	AWS Firepower Management Center에서 정책 구축 실패
CSCvc64185	클라우드 관리 옵션이 선택될 때마다 작업 생성됨
CSCve03171	KP. sig가 있는 NSE의 Snort 코어가 장기간의 SSL CPS 테스트 과정에서 중단
CSCve12691	맞춤 설정 토폴로지 삭제 후 표시되는 해시 구문
CSCvd85133	Radius 개체의 영역 변경 시 Firepower Management Center 활성 사용자는 여전히 오래된 세션

12 장

해결된 문제

다음 표에서는 이 릴리스 노트의 발표 시점에 열린 상태인 해결된 문제를 다룹니다. 알려진 문제의 최신 목록을 보려면 버그 검색 툴에서 제공된 쿼리를 실행합니다.

Cisco 지원 계약이 유효한 고객은 다음 동적 검색을 사용하여 버전 6.2.1에서 해결 상태이고 심각도 3 이상인 모든 버그를 찾을 수 있습니다. https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286259685&rls=6.2.1&sb=afr&sts=fd&svr=3nH&bt=custV

고지 **ID** 번호	설명
CSCvd05552	액세스 제어 정책에서 규칙이 업데이트되지 않음
CSCvb80473	오프박스에서 온박스로 전환한 후 SGT 태그 "Any"를 사용할 수 없음(Elektra)
CSCvc71619	백업 이미지를 재설치하고 복원한 다음 자동 구축 실패
CSCvc91372	업그레이드 실패 후 000_start/106_check_HA_sync.pl을 건너뛸 수 없음
CSCvc51459	manage_pruning.pl 실행 중 경고 메시지
CSCvc59613	netmode 변경 후 인터페이스와의 FTD-HA 액티브/스탠바이 MAC 연결이 제거되지 않음
CSCvd01376	169.254.0.0/16에서 임의의 IP로 페일오버 링크 IP를 설정하지 않아야 함
CSCvb45291	최초 설정에서 처음으로 가져오기 실패
CSCvb82008	Huge NAT 컨피그레이션(12,000개 규칙, 24,000개 개체) 가져오기 실패
CSCvc66889	데이터 인터페이스 internal_route 문제로 전환한 직후 네트워크 표시
CSCvc51439	원본 소스 IP는 연속 규칙에서 평가하지 않음
CSCvd30259	Chrome 및 자체 서명 인증서 사용 시 성능 통계 아티팩트(JS, png)가 캐시되지 않음

고지 **ID** 번호	설명
CSCvc68127	FDM: S2SVPN/수출 컴플라이언스
CSCvd71863	6.2.0-362에서 패치 업그레이드한 후 DatabaseInfo에서 소프트웨어 버전이 업데이트되지 않음

13 장

지원이 필요한 경우

Firepower를 선택해주셔서 감사합니다.

설명서 다운로드, Cisco BST(Bug Search Tool) 사용, 서비스 요청 제출, Cisco NGFW 및 NGIPS 디바이스 관련 추가 정보 수집에 대한 자세한 내용은 *What's New in Cisco Product Documentation(Cisco* 제품 설명서의 새로운 소식*)*(http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html)을 참조하십시오.

Cisco의 새로운 기술 문서 및 개정된 기술 문서를 모두 나열하는 *Cisco Product Documentation*의 새로운 사항을 RSS 피드로 구독하면 콘텐츠가 데스크톱으로 곧바로 배달되어 리더 애플리케이션으로 읽어볼 수 있습니다. RSS 피드는 무료로 제공되는 서비스입니다.

버전 6.2.1 설치 또는 실행에 대해서는 Cisco TAC에 문의하십시오.

- Cisco 지원 웹사이트: http://support.cisco.com/
- 이메일 문의: mailto:tac@cisco.com
- 전화 문의: 1.408.526.7209 또는 1.800.553.2447.