2022의 주요 기능

이 장에서는 2022년에 Cisco Defense Orchestrator에 추가된 몇 가지 기능에 대해 설명합니다.

- 2022년 12월, 1 페이지
- 2022년 10월, 2 페이지
- 2022년 8월 , 3 페이지
- 2022년 6월, 3 페이지
- 2022년 5월, 7 페이지
- 2022년 4월, 7 페이지
- 2022년 2월, 8 페이지
- 2022년 1월, 9 페이지

2022년 12월

2022년 12월 15일

Cisco Defense Orchestrator 클라우드 제공 Firewall Management Center의 플랫폼에 대한 업데이트를 릴리스했습니다. 업데이트에 포함된 새로운 기능에 대해 알아보려면 클라우드 제공 Firewall Management Center에 대한 릴리스 노트를 읽어보십시오.

2022년 12월 1일

ASA에 대한 경로 기반 사이트 간 **VPN** 지원

이제 Cisco Defense Orchestrator를 사용하여 가상 터널 인터페이스가 구성된 피어 사이에 사이트 간 VPN 터널을 생성할 수 있습니다. 이것은 각 터널 끝에 IPsec 프로파일이 연결된 라우팅 기반 VPN을 지원합니다. IPSec 터널로 라우팅되는 모든 트래픽은 소스/대상 서브넷에 관계없이 암호화됩니다.

VTI 기반 VPN은 다음 간에 생성할 수 있습니다.

- CDO 관리 ASA 및 모든 경로 기반 VPN 지원 디바이스.
- CDO 관리 ASA 2개.

자세한 정보는 사이트 간 가상 프라이빗 네트워크를 참조하십시오.

글로벌 검색

CDO에서 전역 검색 기능을 사용하면 CDO에서 관리하는 장치를 찾아 이동할 수 있습니다. 이제 이 기능은 CDO 사용자 인터페이스의 클라우드 제공 Firewall Management Center에서 관리되는 디바이스에 대한 검색 기능을 지원합니다. 검색 결과에서 클라우드 제공 Firewall Management Center의 해당 페이지로 이동할 수 있습니다.

자세한 내용은 전역 검색을 참조하십시오.

2022년 10월

2022년 10월 27일

Duo Admin Panel 온보딩 및 다단계 인증 로깅

이제 CDO는 Duo Admin Panel을 온보딩하고 대시보드 및 표 형식에 로그를 MFA 이벤트로 표시할 수 있습니다. 하나 이상의 디바이스의 MFA 세션을 쉼표로 구분된 값을 포함하는 파일(.csv)로 내보낼 수 있습니다.

Duo Admin Panel에서는 사용자의 이중 인증 성공 또는 실패 여부에 대한 정보가 포함된 MFA(Multi-Factor Authentication, 다단계 인증) 로그를 기록합니다.

자세한 내용은 Cisco Defense Orchestrator 가이드의 "Duo Admin Panel 온보딩" 및 "다단계 인증 이벤트 모니터링"을 참조하십시오.

2023년 10월 12일

ASA용 정책 기반 사이트 간 **VPN** 마법사

이제 CDO에서는 두 피어 사이에 정책 기반 사이트 간 VPN 터널을 구성할 수 있습니다. 즉, IPSec 터널로 라우팅되는 모든 트래픽은 소스/대상 서브넷에 관계없이 암호화됩니다.

정책 기반 사이트 간 VPN을 구성하려면 다음 조건 중 하나를 충족해야 합니다.

- 두 피어 모두 CDO 관리 ASA입니다.
- 피어 중 하나는 CDO 관리 ASA이고 다른 하나는 정책 기반 VPN 지원 디바이스입니다.

자세한 정보는 사이트 간 가상 프라이빗 네트워크를 참조하십시오.

2022년 8월

2022년 8월 4일

FDM-관리 디바이스**,** 버전 **7.2** 에 대한 **CDO** 지원

CDO는 이제 FDM 관리 디바이스용 버전 7.2를 지원합니다. CDO 지원은 다음과 같은 측면을 제공합니다.

- 버전 7.2를 실행하는 지원되는 물리적 또는 가상 FDM 관리 디바이스를 CDO에 온보딩합니다.
- 버전 6.4 이상에서 버전 7.2로 FDM 관리 디바이스를 업그레이드합니다.
- 기존 Secure Firewall Threat Defense 기능을 지원합니다.
- 버전 7.2를 실행하는 지원되는 물리적 또는 가상 디바이스를 클라우드 제공 Firewall Management Center에 온보딩합니다.

참고 CDO는 버전 7.2 릴리스에 도입된 기능을 지원하지 않습니다.

2022년 6월

2022년 6월 30일

Cisco Secure Firewall 마이그레이션 툴**, Cisco Secure Firewall Threat Defense** 마이그레이션 지원

Secure Firewall 마이그레이션 툴을 사용하면 Secure Firewall ASA 구성을 온프레미스 또는 가상 Secure Firewall Management Center 또는 Cisco Defense Orchestrator의 새로운 클라우드 제공 Firewall Management Center에서 관리하는 Cisco Secure Firewall Threat Defense로 마이그레이션할 수 있습니다. 데스크톱 툴은 서드파티 벤더인 Check Point, Palo Alto Networks 및 Fortinet의 마이그레이션도 지원합니다.

Cisco Secure Firewall 마이그레이션 툴 버전 3.0은 Threat Defense 소프트웨어 버전 7.2를 실행하는 Secure Firewall Threat Defense 디바이스로의 마이그레이션을 지원합니다. 해당 버전의 위협 방어는 CDO의 클라우드 제공 Firewall Management Center에서 관리할 수 있습니다. 마이그레이션 프로세스는 CDO의 일부이며 CDO 라이선스 이외의 특정 라이선스가 필요하지 않습니다.

Software Download(소프트웨어 다운로드) 페이지에서 Secure Firewall 마이그레이션 툴을 다운로드할 수 있습니다.

CDO는 ASA에서 실행 중인 구성의 다음 요소를 위협 방어 템플릿으로 마이그레이션하는 데 도움이 되는 마법사를 제공합니다.

- 액세스 제어 규칙(ACL)
- 인터페이스
- NAT(네트워크 주소 변환) 규칙
- 네트워크 개체 및 네트워크 그룹 개체
- 경로

구성을 실행하는 ASA의 이러한 요소가 마이그레이션되면 CDO의 클라우드 제공 Firewall Management Center에서 관리하는 새로운 위협 방어 디바이스에 구성을 구축할 수 있습니다.

자세한 내용은 Cisco Secure Firewall 마이그레이션 툴을 사용하여 ASA 방화벽을 Cisco Secure Firewall Threat Defense로 마이그레이션을 참고하십시오.

2022년 6월 9일

클라우드 제공 **Firewall Management Center**를 사용하여 **Cisco Secure Firewall Threat Defense** 디바이스 관리

CDO(Cisco Defense Orchestrator)는 이제 클라우드 제공 Firewall Management Center의 플랫폼입니다.

클라우드 제공 Firewall Management Center는 Secure Firewall Threat Defense 디바이스를 관리하는 SaaS(Software-as-a-Service) 제품입니다. 이는 온프레미스 Secure Firewall Management Center와 동일한 여러 기능을 제공하며, 온프레미스 Secure Firewall Management Center와 모양과 동작이 동일하며, 동일한 FMC API를 사용합니다.

이 제품은 Secure Firewall Management Center의 온프레미스 버전에서 SaaS 버전으로 이동하려는 Secure Firewall Management Center 고객을 위해 설계되었습니다.

SaaS 제품인 CDO 운영 팀은 이를 유지 관리합니다. 새로운 기능이 도입되면 CDO 운영 팀이 CDO 및 클라우드 제공 방화벽 관리자를 업데이트합니다.

마이그레이션 마법사를 사용하면 온프레미스 Secure Firewall Management Center에 등록된 Secure Firewall Threat Defense 디바이스를 클라우드 제공 Firewall Management Center로 마이그레이션할 수 있습니다.

Secure Firewall Threat Defense 디바이스 온보딩은 일련 번호를 사용하여 디바이스를 온보딩하거나 등록 키가 포함된 CLI 명령을 사용하는 등 친숙한 프로세스를 사용하여 CDO에서 수행됩니다. 디바이스가 온보딩되면 CDO와 클라우드 제공 Firewall Management Center에 모두 표시되지만 클라우드 제공 Firewall Management Center에서 디바이스를 구성합니다. 버전 7.2 이상을 실행하는 Secure Firewall Threat Defense 디바이스를 온보딩할 수 있습니다.

클라우드 제공 Firewall Management Center의 라이선스는 디바이스별 매니지드 라이선스이며 클라우드 제공 FMC 자체에는 라이선스가 필요하지 않습니다. 기존 보안 방화벽 위협 방어 디바이스는 기존 스마트 라이선스를 재사용하며, 새 보안 방화벽 위협 방어 디바이스는 FTD에서 구현된 각 기능에 대해 새 스마트 라이선스를 프로비저닝합니다.

원격 지사 구축에서 위협 방어 디바이스의 데이터 인터페이스는 디바이스의 관리 인터페이스 대신 Cisco Defense Orchestrator 관리에 사용됩니다. 대부분의 원격 지사에서는 단일 인터넷 연결만 가능하

므로 외부 CDO 액세스를 통해 중앙 집중식 관리가 가능합니다. 원격 지사 구축의 경우 CDO는 데이터 인터페이스를 통해 관리하는 위협 방어 디바이스에 대한 고가용성 지원을 제공합니다.

Security Analytics and Logging(SaaS) 또는 Security Analytics and Logging(온프레미스)을 사용하여 온보딩된 위협 방어 디바이스에서 생성된 시스템 로그 이벤트를 분석할 수 있습니다. SaaS 버전은 클라우드에 이벤트를 저장하며 CDO에서 이벤트를 볼 수 있습니다. 온프레미스 버전은 온프레미스 Secure Network Analytics 어플라이언스에 이벤트를 저장하며, 분석은 온프레미스 Secure Firewall Management Center에서 수행됩니다. 두 경우 모두 오늘날의 온프레미스 FMC와 마찬가지로 센서에서 직접 선택한 로그 컬렉터로 로그를 전송할 수 있습니다.

FTD 대시보드는 클라우드 제공 Firewall Management Center에서 관리하는 모든 위협 방어 디바이스에서 수집 및 생성된 이벤트 데이터를 포함하여 상태를 한눈에 볼 수 있도록 제공합니다. 이 대시보드를 사용하여 디바이스 상태 및 구축에 있는 디바이스의 전반적인 상태와 관련된 종합적인 정보를 볼 수 있습니다. FTD 대시보드가 제공하는 정보는 시스템에서 디바이스의 라이선스, 구성 및 구축 방법에 따라 달라집니다. FTD 대시보드에는 모든 CDO 매니지드 위협 방어 디바이스에 대한 데이터가 표시됩니다. 그러나 디바이스 기반 데이터를 필터링하도록 선택할 수 있습니다. 특정 시간 범위에 대해 표시할 시간 범위를 선택할 수도 있습니다.

Cisco Secure Dynamic Attributes Connector를 사용하면 클라우드 제공 Firewall Management Center 액세스 제어 규칙에서 다양한 클라우드 서비스 플랫폼의 서비스 태그 및 범주를 사용할 수 있습니다. IP 주소와 같은 네트워크 구성은 워크로드의 동적 특성과 IP 주소 중복의 불가피성으로 인해 가상, 클라우드 및 컨테이너 환경에서 일시적일 수 있습니다. 고객은 IP 주소 또는 VLAN이 변경되는 경우에도 방화벽 정책이 유지되도록 VM 이름 또는 보안 그룹과 같은 비 네트워크 구문을 기반으로 정책 규칙을 정의해야 합니다.

하나 이상의 매니지드 디바이스의 프록시 시퀀스를 사용하여 LDAP, Active Directory 또는 ISE/ISE-PIC 서버와 통신할 수 있습니다. 이는 Cisco Defense Orchestrator(CDO)가 Active Directory 또는 ISE/ISE-PIC 서버와 통신할 수 없는 경우에만 필요합니다. 예를 들어 CDO은(는) 퍼블릭 클라우드에 있지만 Active Directory 또는 ISE/ISE-PIC는 프라이빗 클라우드에 있을 수 있습니다.

하나의 매니지드 디바이스를 프록시 시퀀스로 사용할 수 있지만, 둘 이상의 매니지드 디바이스를 설정하는 것이 좋습니다. 그러면 하나의 매니지드 디바이스가 Active Directory 또는 ISE/ISE-PIC와 통신할 수 없는 경우 다른 매니지드 디바이스가 인계받을 수 있습니다.

모든 고객은 CDO를 사용하여 보안 방화벽 ASA, Meraki, Cisco IOS 디바이스, Secure Firewall Cloud Native, Umbrella 및 AWS 가상 프라이빗 클라우드와 같은 다른 디바이스 유형을 관리할 수 있습니다. Firepower Device Manager에서 로컬 관리용으로 구성된 Secure Firewall Threat Defense 디바이스를 CDO를 사용하여 관리하는 경우 CDO로도 계속 관리할 수 있습니다. CDO를 처음 사용하는 경우 클라우드에서 제공하는 새로운 Firewall Management Center 및 기타 모든 디바이스 유형을 사용하여 Secure Firewall Threat Defense 디바이스를 관리할 수 있습니다.

클라우드 제공 Firewall Management Center에서 지원하는 Firewall Management Center 기능에 대해 자세히 알아보십시오.

- 상태 모니터링
- Secure Firewall Threat Defense 디바이스 백업/복원
- 일정 예약
- 가져오기/내보내기

- 알림 응답을 사용한 외부 알림
- 투명 방화벽 또는 라우팅 방화벽 모드
- Secure Firewall Threat Defense 디바이스의 고가용성
- 인터페이스
- NAT(Network Access Control)
- 고정 및 기본 경로 및 기타 라우팅 구성
- 개체 관리 및 인증서
- 원격 액세스 VPN 및 사이트 간 VPN 구성
- Access Control(액세스 컨트롤) 정책
- Cisco Secure Dynamic Attributes Connector
- 침입 탐지 및 방지 정책
- 네트워크 악성코드 및 보호 및 파일 정책
- 암호화된 트래픽 처리
- 사용자 ID
- FlexConfig 정책

SecureX를 사용하여 온프레미스 **management center** 온보딩

이미 Securex 계정과 연결된 온프레미스 management center가 있는 경우 SecureX를 통해 management center를 CDO에 온보딩할 수 있습니다. SecureX를 통해 온보딩된 디바이스는 기존 방법을 통해 온보딩된 management center와 동일한 수준의 기능 지원 및 기능을 경험합니다. SecureX를 통해 management center를 CDO에 온보딩하려면 SecureX를 사용하여 온프레미스 FMC 온보딩을 참조하십시오.

참고 management center 계정이 SecureX와 연결되어 있더라도 management center 온보딩을 시도하기 전에 CDO 계정을 SecureX와 병합하는 것이 좋습니다. 자세한 내용은 CDO 및 SecureX 계정 병합을 참조하십시오.

2022년 5월

2022년 5월 12일

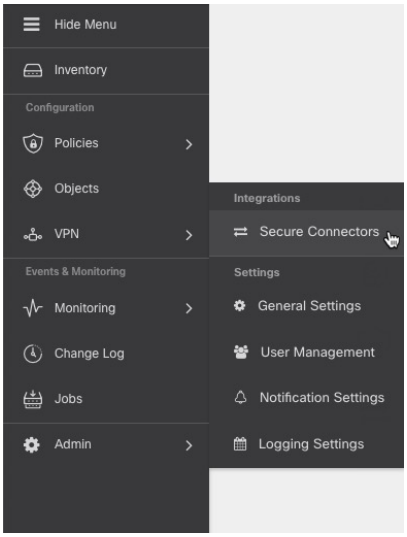
IPv6에 대한 ASA 정책 지원

이제 ASA 액세스 정책 및 NAT 구성에서 IPv6 주소를 포함하는 네트워크 개체 및 네트워크 그룹을 사용하는 규칙을 지원합니다. 또한 이러한 규칙은 ICMP 및 ICMPv6 프로토콜을 지정할 수 있습니다. 마지막으로, 이제 ASA는 IPv6 주소를 포함하는 AnyConnect 연결 프로파일을 지원합니다. 자세한 내용은 ASA 네트워크 정책을 참조하십시오.

보안 커넥터 페이지로 이동

CDO 메뉴 모음에서 Secure Connector(보안 커넥터) 페이지에 액세스할 수 있습니다. Secure Connector(보안 커넥터) 페이지를 보려면 **Admin(관리자)** > **Secure Connector(보안 커넥터)**를 선택합니다.

그림 *1:* 보안 커넥터 메뉴



2022년 4월

2022년 4월 14일

AWS Transit Gateway를 사용하여 AWS VPC 터널 모니터링

CDO는 이제 AWS Transit Gateway를 사용하여 AWS VPC 터널을 모니터링할 수 있습니다. 자세한 내용은 AWS Transit Gateway를 사용하여 AWS VPC 터널 모니터링을 참조하십시오.

2022년 4월 6일

글로벌 검색

글로벌 검색은 CDO 내에서 사용 가능한 모든 온보딩 디바이스 및 관련 개체를 검색할 수 있는 옵션을 제공합니다. 검색 결과를 통해 해당 디바이스 및 개체 페이지로 이동할 수 있습니다.

현재 CDO는 ASA, Firepower Management Center, Secure Firewall Threat Defense, Meraki 및 Secure Firewall Cloud Native 디바이스에 대한 글로벌 검색을 지원합니다.

자세한 내용은 다음 문서에서 "글로벌 검색"을 참조하십시오.

- Cisco Defense Orchestrator를 사용한 ASA 관리
- Cisco Defense Orchestrator를 사용한 FMC 관리
- Cisco Defense Orchestrator를 사용한 FTD 관리
- Cisco Defense Orchestrator를 사용한 Meraki 관리
- Cisco Defense Orchestrator를 사용하여 Cisco Secure Firewall Cloud Native 관리

Cisco Secure Firewall 3100에 대한 지원

Cisco Defense Orchestrator는 새로운 Cisco Secure Firewall 3100 Series 디바이스에서 실행되는 온보딩 ASA 및 Secure Firewall Threat Defense 디바이스를 지원합니다.

Secure Firewall Threat Defense 디바이스는 로우 터치 프로비저닝을 사용하거나 등록 키 또는 일련 번호를 사용하여 온보딩할 수 있습니다.

2022년 2월

2022년 2월 3일

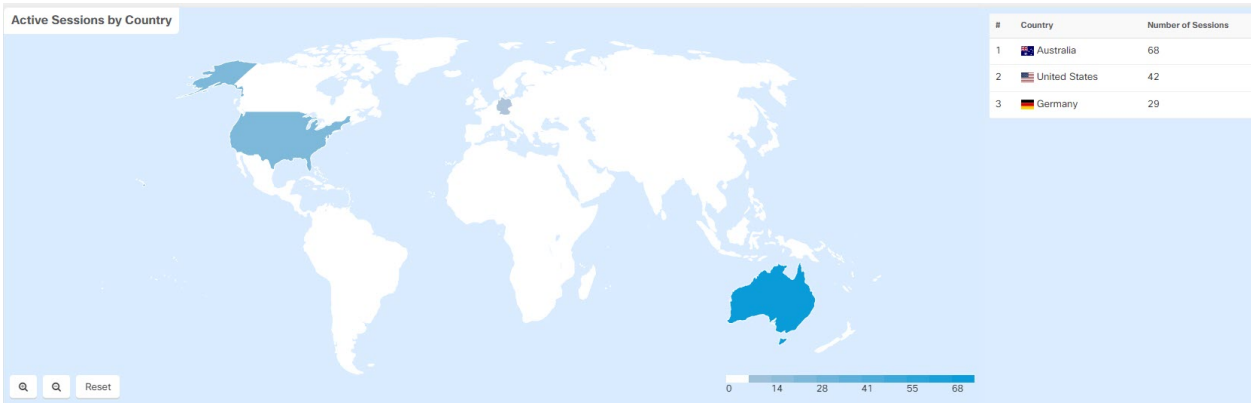
사용자 관리의 **AD(Active Directory)** 그룹

CDO에서 사용자를 더 쉽게 관리하기 위해 개별 사용자를 관리하는 대신 CDO에서 AD(Active Directory) 그룹을 매핑할 수 있습니다. 새 사용자 추가, 기존 사용자 제거 또는 역할 변경과 같은 사용자 변경 사항은 이제 CDO 내에서 아무것도 변경하지 않고 Active Directory에서 수행할 수 있습니다. 이제 CDO는 AD를 사용하는 사용자당 여러 역할도 지원합니다. 자세한 내용은 디바이스 구성 가이드의 사용자 관리 장의 "사용자 관리의 Active Directory 그룹" 섹션을 참조하십시오.

활성 원격 액세스 **VPN** 세션에 대한 향상된 차트 보기

이제 CDO는 활성 RA VPN 세션에 대한 새롭고 향상된 차트 보기를 제공합니다. 이미 익숙한 차트 외에도 CDO는 이제 RA VPN 헤드엔드에 연결된 사용자 위치의 히트맵을 표시합니다. 이 맵은 라이브 보기에서만 사용할 수 있습니다.

새 차트 보기를 보려면 RA VPN Monitoring(RA VPN 모니터링) 페이지에서 화면의 오른쪽 상단에 표시되는 **Show Charts View(**차트 보기 표시**)** 아이콘을 클릭합니다.



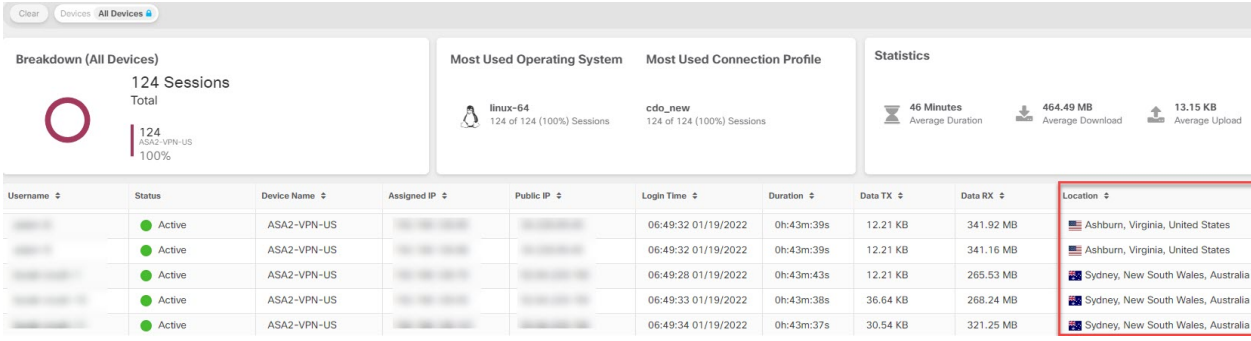
자세한 내용은 방화벽에 따라 Cisco Defense Orchestrator를 사용하여 FTD 관리, Cisco Defense Orchestrator를 사용하여 ASA 관리 또는 Cisco Defense Orchestrator를 사용하여 Cisco Secure Firewall Cloud Native 관리의 "원격 액세스 가상 사설 네트워크 세션 모니터링"을 참조하십시오.

2022년 1월

2022년 1월 20일

원격 액세스 **VPN** 사용자의 지리위치 정보

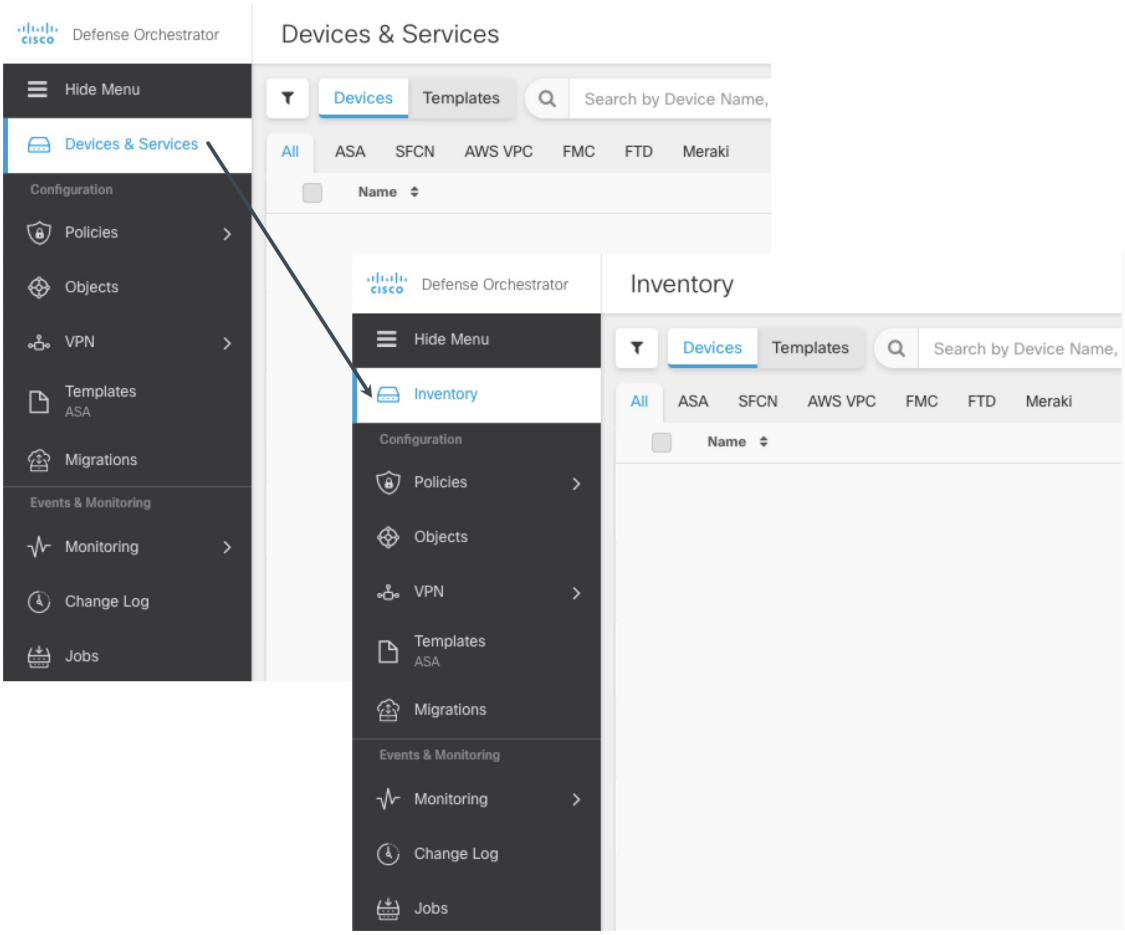
이제 원격 액세스 VPN 모니터링 페이지에 VPN 헤드엔드에 연결된 모든 사용자의 위치가 표시됩니다. CDO는 사용자의 공용 IP 주소를 지리위치로 확인하여 이 정보를 얻습니다. 이 정보는 라이브 및 기록 보기에서 사용할 수 있습니다. 왼쪽 창의 **User Details(**사용자 세부 정보**)** 영역에서 위치를 클릭하면 사용자의 정확한 위치가 맵에 표시됩니다.



참고 이 정보는 새 CDO 구축 이후에 설정된 사용자 세션에서 사용할 수 있으며 기존 사용자 세션에서는 사용할 수 없습니다.

Devices & Services(디바이스 및 서비스**)** 페이지 이름이 **Inventory(**재고 목록**)**로 변경됨

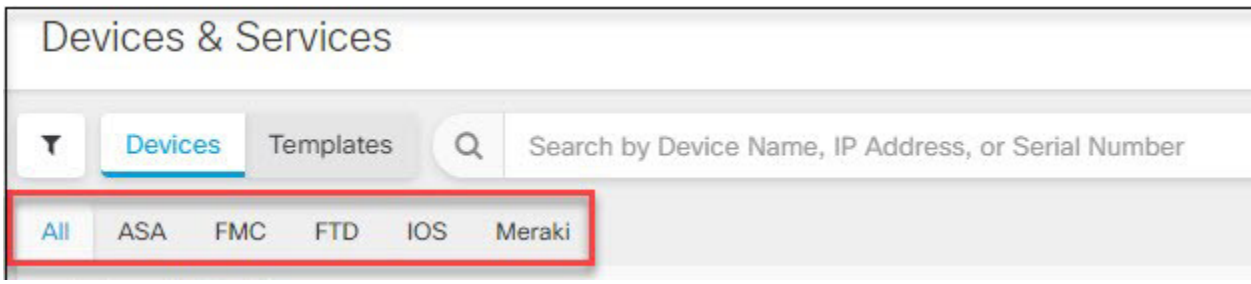
Devices & Services(디바이스 및 서비스) 페이지의 이름이 "Inventory(재고 목록)"로 변경되었습니다. Inventory(재고 목록) 테이블에는 CDO로 관리하는 모든 디바이스 및 서비스가 나열됩니다. 이름 변경으로 인해 추가되거나 제거된 기능은 없습니다.



2022년 1월 13일

향상된 디바이스 및 서비스 인터페이스

이제 CDO 디바이스 및 서비스 인터페이스에서 유형에 따라 디바이스 및 템플릿을 분류하고 각 디바이스 유형 전용의 해당 탭에 표시합니다.


Devices & Services
Devices
Templates
Search by Device Name, IP Address, or Serial Number
All
ASA
FMC
FTD
IOS
Meraki

2022년 1월 13일