



디바이스 및 서비스 온보딩

라이브 디바이스와 모델 디바이스를 모두 CDO에 온보딩할 수 있습니다. 모델 디바이스는 CDO를 사용하여 보고 편집할 수 있는 업로드된 구성 파일입니다.

대부분의 라이브 디바이스 및 서비스는 보안 디바이스 커넥터가 CDO를 디바이스 또는 서비스에 연결할 수 있도록 개방형 HTTPS 연결을 필요로 합니다.

SDC 및 해당 상태에 대한 자세한 내용은 [SDC\(보안 디바이스 커넥터\)](#)을 참조하십시오.

이 장에는 다음 섹션이 포함되어 있습니다.

- [Meraki MX를 Defense Orchestrator에 온보딩, on page 1](#)
- [Meraki 템플릿을 Defense Orchestrator에 온보딩, on page 4](#)
- [Meraki MX 연결 자격 증명 업데이트, on page 5](#)
- [CDO에서 디바이스 삭제, 6 페이지](#)

Meraki MX를 Defense Orchestrator에 온보딩

MX 디바이스는 CDO(Cisco Defense Orchestrator) 및 Meraki 대시보드 모두에서 관리할 수 있습니다. CDO는 구성 변경 사항을 Meraki 대시보드에 배포하며, 그러면 구성이 디바이스에 안전하게 배포됩니다.

Before you begin

- [Cisco Defense Orchestrator 관리 디바이스에 연결](#)를 검토합니다.
- [CDO가 Meraki와 통신하는 방법](#)을 검토합니다.
- 먼저 Meraki 대시보드에서 Meraki MX를 등록해야 합니다. Meraki 대시보드에 액세스할 수 없는 경우 Meraki 클라우드에서 조직을 인식할 수 없으며 디바이스를 온보딩하기 위한 API 토큰을 생성할 수 없습니다.
- CDO는 호스트와 연결된 모든 비트를 0으로 설정하여 잘못된 CIDR 접두사 표기법 IP 주소 및 IP 주소 범위를 유효한 형식으로 자동 변환합니다.
- Meraki MX 디바이스 또는 템플릿을 온보딩하는 데 더 이상 [SDC\(보안 디바이스 커넥터\)](#)를 통한 연결이 필요하지 않습니다. 이미 온보딩된 Meraki MX 디바이스가 있고 SDC를 사용하여 CDO에

연결된 경우, 디바이스를 제거했다가 다시 온보딩하거나 **연결 자격 증명을 업데이트**하지 않는 한 해당 연결은 계속 작동합니다.

- CDO에서 관리하기 위해 MX 디바이스를 Meraki 클라우드에 연결할 필요는 없습니다. MX 디바이스가 클라우드에 연결된 적이 없는 경우 디바이스 연결은 연결할 수 없음으로 나열됩니다. 이는 정상적인 현상이며, 이 디바이스에 대한 정책을 관리하거나 배포하는 기능에는 영향을 미치지 않습니다.

Procedure

	Command or Action	Purpose
단계 1	Meraki MX 디바이스를 온보딩할 때 Meraki API 키를 생성해야 합니다. 이 키는 대시보드를 인증하고 디바이스를 안전하게 온보딩할 수 있도록 해줍니다. Meraki API 키 생성 및 검색 을 참조하십시오.	
단계 2	API 키를 사용하여 Meraki 디바이스를 CDO에 온보딩합니다.	

Meraki API 키 생성 및 검색

다음 절차를 사용하여 API 액세스를 사용하여 Meraki 대시보드에 대한 CDO 액세스를 활성화합니다.

Before you begin

[Meraki MX를 Defense Orchestrator에 온보딩](#), on page 1에 대한 참고 및 사전 요구 사항을 검토합니다.

단계 1 Meraki 대시보드에 로그인합니다.

단계 2 탐색 패널에서 **Organization(조직)** > **Settings(설정)**를 클릭합니다.

단계 3 **Dashboard API Access(대시보드 API 액세스)**에서 **Enable access to the Cisco Meraki Dashboard API(Cisco Meraki 대시보드 API에 대한 액세스 활성화)**를 선택합니다. 이 옵션이 없는 경우 MX 디바이스를 CDO에 온보딩하기 위한 API 키를 생성할 수 없습니다.

단계 4 **Save Changes(변경 내용 저장)**를 클릭합니다.

단계 5 Meraki 대시보드에서 화면의 오른쪽 상단 모서리에 있는 사용자 이름을 클릭한 다음 **My Profile(내 프로필)**를 클릭합니다.

단계 6 API 액세스 헤더를 찾아 **Generate new API key(새 API 키 생성)**를 클릭합니다. 이 API 키를 복사합니다. 사용할 준비가 될 때까지 참고에 임시로 붙여넣는 것이 좋습니다. API 키를 붙여넣기 전에 복사 소스를 닫으면 복사한 API 키가 손실됩니다.

Note 디바이스당 하나의 API 키만 있으면 됩니다. 새 키를 생성하지 않고 Meraki 디바이스를 다시 온보딩할 수 있습니다.

What to do next

계속해서 [CDO에 MX 디바이스 온보딩](#)합니다.

CDO에 MX 디바이스 온보딩

다음 절차를 사용하여 Cisco Meraki 디바이스를 온보딩합니다.

Before you begin

[Meraki API 키 생성 및 검색, on page 2.](#)

단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 파란색 플러스 버튼  을 클릭하고 **Meraki** 타일을 클릭합니다.

단계 3 이 디바이스가 통신할 **SDC(보안 디바이스 컨넥터)**를 선택합니다. 기본 SDC가 표시되지만 파란색 **Change**(변경) 링크를 클릭하여 변경할 수 있습니다.

단계 4 복사한 API 액세스 키를 붙여넣습니다. 키가 불완전하거나 올바르지 않으면 디바이스를 온보딩할 수 없습니다. 연결을 클릭합니다.

단계 5 드롭다운 메뉴를 사용하여 올바른 조직을 선택합니다. 생성된 조직 목록은 Meraki 대시보드에서 검색되며 디바이스 및 템플릿을 포함합니다. 원하는 디바이스를 선택하고 **Select**(선택)를 클릭합니다.

단계 6 드롭다운 메뉴를 사용하여 올바른 네트워크를 선택합니다. 생성된 네트워크 목록은 Meraki 네트워크에서 검색됩니다. **Select**(선택)를 클릭합니다.

단계 7 선택적으로 디바이스에 고유한 레이블을 추가할 수 있습니다. 나중에 이 레이블을 기준으로 디바이스 목록을 필터링할 수 있습니다.

단계 8 **Continue**(계속)를 클릭합니다. 디바이스는 온보딩 프로세스입니다. 완료되면 CDO는 **Inventory**(인벤토리)로 리디렉션합니다.

관련 정보

- [Meraki MX 템플릿](#)
- [Meraki 템플릿을 CDO에 온보딩, on page 5](#)
- [CDO가 Meraki와 통신하는 방법](#)
- [Meraki 액세스 제어 정책 관리](#)
- [Meraki 네트워크 개체 또는 네트워크 그룹 생성 또는 편집](#)
- [Meraki 서비스 개체 또는 서비스 그룹 생성 또는 편집](#)

Meraki 템플릿을 Defense Orchestrator에 온보딩

Meraki 템플릿은 단일 정책으로 여러 위치 또는 네트워크를 관리하는 훌륭한 방법입니다. Meraki 템플릿은 CDO(Cisco Defense Orchestrator) 및 Meraki 대시보드에서 모두 관리할 수 있습니다. CDO는 구성 변경 사항을 Meraki 대시보드에 배포하며, 그러면 구성이 템플릿에 안전하게 배포됩니다. 자세한 내용은 [CDO가 Meraki와 통신하는 방법](#)을 참조하십시오.



Note CDO에 템플릿을 온보딩하려면 먼저 Meraki 대시보드에서 템플릿을 생성해야 합니다. Meraki 대시보드에 액세스할 수 없는 경우 Meraki 클라우드에서 조직을 인식할 수 없으며 디바이스를 온보딩하기 위한 API 토큰을 생성할 수 없습니다. Meraki 대시보드에서 **Organization(조직) > Configuration templates(구성 템플릿)**을 클릭하고 [Managing Multiple Networks with Configuration Templates\(구성 템플릿을 사용하여 여러 네트워크 관리\)](#)에서 자세한 내용을 참조하십시오.

Meraki 템플릿을 온보딩하려면 3단계를 수행해야 합니다.

- 단계 1 Meraki 대시보드에서 템플릿 네트워크를 생성합니다. 자세한 내용은 [Meraki 템플릿 모범 사례](#)를 참조하십시오.
- 단계 2 [Meraki API 키 생성 및 검색](#). Meraki 템플릿을 온보딩할 때 Meraki API 키를 생성해야 합니다. 이 키는 대시보드를 인증하고 디바이스를 안전하게 온보딩할 수 있도록 해줍니다.
- 단계 3 [Meraki 템플릿을 CDO에 온보딩](#).

Meraki API 키 생성 및 검색

다음 절차를 사용하여 API 액세스를 사용하여 Meraki 대시보드에 대한 CDO 액세스를 활성화합니다.

- 단계 1 Meraki 대시보드에 로그인합니다.
- 단계 2 탐색 패널에서 **Organization(조직) > Settings(설정)**를 클릭합니다.
- 단계 3 **Dashboard API Access(대시보드 API 액세스)**에서 **Enable access to the Cisco Meraki Dashboard API(Cisco Meraki 대시보드 API에 대한 액세스 활성화)**를 선택합니다. 이 옵션이 없는 경우 MX 디바이스를 CDO에 온보딩하기 위한 API 키를 생성할 수 없습니다.
- 단계 4 **Save Changes(변경 내용 저장)**를 클릭합니다.
- 단계 5 Meraki 대시보드에서 화면의 오른쪽 상단 모서리에 있는 사용자 이름을 클릭한 다음 **My Profile(내 프로필)**를 클릭합니다.
- 단계 6 API 액세스 헤더를 찾아 **Generate new API key(새 API 키 생성)**를 클릭합니다. 이 API 키를 복사합니다. 사용할 준비가 될 때까지 참고에 임시로 붙여넣는 것이 좋습니다. API 키를 붙여넣기 전에 복사 소스를 닫으면 복사한 API 키가 손실됩니다.

Note 템플릿당 하나의 API 키만 있으면 됩니다. 새 키를 생성하지 않고 템플릿을 다시 온보딩할 수 있습니다.

Meraki 템플릿을 CDO에 온보딩

Meraki 템플릿을 온보딩하려면 다음 절차를 수행합니다.

- 단계 1 탐색 창에서 **Inventory**(인벤토리)를 클릭하고 파란색 플러스 버튼  을 클릭한 다음 **Connect to Cisco Meraki(Cisco Meraki)**에 연결)를 클릭합니다.
- 단계 2 복사한 API 액세스 키를 붙여넣습니다. 키가 불완전하거나 올바르지 않으면 디바이스를 온보딩할 수 없습니다. 연결을 클릭합니다.
- 단계 3 드롭다운 메뉴를 사용하여 템플릿 이름을 **ab Organization**(조직)으로 선택합니다. 생성된 조직 목록은 Meraki 대시보드에서 검색되며 디바이스 및 템플릿을 포함합니다. 원하는 템플릿을 선택하고 **Select**(선택)를 클릭합니다.
- 단계 4 선택적으로 디바이스에 고유한 레이블을 추가할 수 있습니다. 나중에 이 레이블을 기준으로 디바이스 목록을 필터링할 수 있습니다.
- 단계 5 **Continue**(계속)를 클릭합니다. 디바이스는 온보딩 프로세스입니다. 완료되면 CDO는 **Inventory**(인벤토리)로 리디렉션합니다. 템플릿이 CDO에 동기화되면 **Inventory**(재고 목록) 페이지에 템플릿과 연결된 디바이스의 이름이 표시되고 **Device**(디바이스) **Details**(세부 정보) 창에 템플릿에 바인딩된 네트워크 수가 표시됩니다.

관련 정보

- [CDO가 Meraki와 통신하는 방법](#)
- [Meraki 액세스 제어 정책 관리](#)
- [Meraki 디바이스와 연결된 개체](#)
- [Meraki 네트워크 개체 또는 네트워크 그룹 생성 또는 편집](#)
- [Meraki 서비스 개체 또는 서비스 그룹 생성 또는 편집](#)
- [Meraki MX를 Defense Orchestrator에 온보딩](#)

Meraki MX 연결 자격 증명 업데이트

Meraki 대시보드에서 새 API 키를 생성하는 경우 CDO에서 연결 자격 증명을 업데이트해야 합니다. 새 키를 생성하려면 [Meraki API 키 생성 및 검색](#), on page 2에서 자세한 내용을 확인합니다. CDO에서는 디바이스 자체에 대한 연결 자격 증명을 업데이트할 수 없습니다. 필요한 경우 Meraki 대시보드에서 API 키를 수동으로 새로 고칠 수 있습니다. 자격 증명을 업데이트하고 통신을 다시 설정하려면 CDO UI에서 API 키를 수동으로 업데이트해야 합니다.



Note CDO가 디바이스를 동기화하지 못하면 CDO의 연결 상태에 "Invalid Credentials(유효하지 않은 자격 증명)"가 표시될 수 있습니다. 이 경우 API 키를 사용하려고 시도했을 수 있습니다. 선택한 Meraki MX의 API 키가 올바른지 확인합니다.

Meraki MX 디바이스에 대한 자격 증명을 업데이트하려면 다음 절차를 사용합니다.

단계 1 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭한 다음 **Meraki** 탭을 클릭합니다.

단계 3 연결 자격 증명을 업데이트할 Meraki MX를 선택합니다.

단계 4 **Device Actions**(디바이스 작업) 창에서 **Update Credentials**(자격 증명 업데이트)를 클릭합니다.

단계 5 CDO가 디바이스에 로그인하는 데 사용하는 **API 키**를 입력하고 **Update**(업데이트)를 클릭합니다. 변경하지 않는 한 이 API 키는 Meraki MX를 온보딩하는 데 사용한 것과 동일한 자격 증명입니다. 이러한 변경 사항을 디바이스에 배포할 필요는 없습니다.

CDO에서 디바이스 삭제

CDO에서 디바이스를 삭제하려면 다음 절차를 따르십시오.

단계 1 CDO에 로그인합니다.

단계 2 **Inventory**(인벤토리) 페이지로 이동합니다.

단계 3 삭제할 디바이스를 찾아 디바이스 행에서 디바이스를 확인하고 선택합니다.

단계 4 오른쪽에 있는 디바이스 작업 패널에서 **Remove**(제거)를 선택합니다.

단계 5 메시지가 표시되면 **OK**(확인)를 선택하여 선택한 디바이스 제거를 확인합니다. 디바이스를 온보딩 상태로 유지하려면 **Cancel**(취소)을 선택합니다.

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.