Cisco Secure Firewall Management Center용 Umbrella DNS 커넥터 구성

초판: 2023년 2월 8일

최종 변경: 2023년 7월 27일

Cisco Secure Firewall Management Center용 Umbrella DNS 커넥터 구성

이 문서에서는 Secure Firewall Management Center에서 Umbrella DNS 커넥터를 설정하는 방법을 설명합니다.

Umbrella 커넥터의 이점

management center의 Cisco Umbrella DNS 연결은 DNS 쿼리를 Cisco Umbrella로 리디렉션하는 데 도움이 됩니다. 이렇게 하면 Cisco Umbrella에서 도메인 이름을 기준으로 허용 또는 차단 여부를 확인하고 요청에 DNS 기반 보안 정책을 적용할 수 있습니다. Cisco Umbrella를 사용하는 경우 Cisco Umbrella 연결을 구성하여 DNS 쿼리를 Cisco Umbrella로 리디렉션할 수 있습니다.

Umbrella Connector는 시스템 DNS 검사의 일부입니다. 기존 DNS 검사 정책 맵이 DNS 검사 설정에 따라 요청을 차단하거나 삭제하기로 결정한 경우 해당 요청은 Cisco Umbrella로 전달되지 않습니다. 따라서 로컬 DNS 검사 정책과 Cisco Umbrella 클라우드 기반 정책이라는 두 가지 보호 라인이 있습니다.

DNS 조회 요청을 Cisco Umbrella로 리디렉션할 때 Umbrella Connector는 EDNS(Extension 메커니즘 for DNS) 레코드를 추가합니다. EDNS 레코드에는 디바이스 식별자 정보, 조직 ID 및 클라이언트 IP 주소가 포함됩니다. 클라우드 기반 정책은 이러한 기준을 사용하여 FQDN의 평판 외에도 액세스를 제어할 수 있습니다. 사용자 이름 및 내부 IP 주소의 프라이버시를 보장하기 위해 DNSCrypt를 사용하여 DNS 요청을 암호화하도록 선택할 수도 있습니다.

시스템 요구 사항

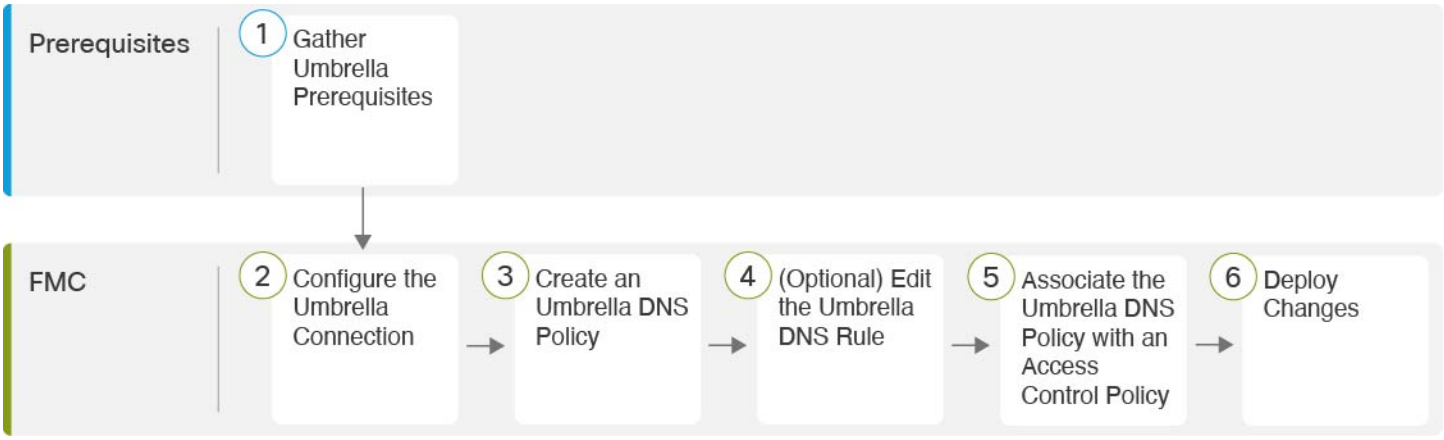
아래 표에는 이 절차에 필요한 제품이 나와 있습니다.

표 *1:* 최소 지원되는 플랫폼

제품	**Version**(버전)
Firepower Threat Defense	6.6.0 이상
Firewall Management Center	7.2+

FMC Umbrella DNS 커넥터 구성

그림 *1:* 엔드 투 엔드 절차



1	사전 요건	Umbrella 사전 요건 수집, 2 페이지
2	FMC	Umbrella 연결 구성, 5 페이지
3	FMC	Umbrella DNS 정책 생성, 6 페이지
4	FMC	(선택 사항) Umbrella DNS 규칙 편집, 6 페이지
5	FMC	Umbrella DNS 정책을 액세스 제어 정책에 연결 , 6 페이지
6	FMC	변경 구축 , 7 페이지

Umbrella 사전 요건 수집

시작하기 전에

- https://umbrella.cisco.com에서 Cisco Umbrella에 계정을 설정하고 http://login.umbrella.com에서 Umbrella에 로그인합니다.
- Cisco Umbrella 서버에서 management center로 CA 인증서를 가져옵니다. Cisco Umbrella에서 **Deployments(**구축**) > Configuration(**구성**) > Root Certificate(**루트 인증서**)**를 선택하고 인증서를 다운로드합니다.

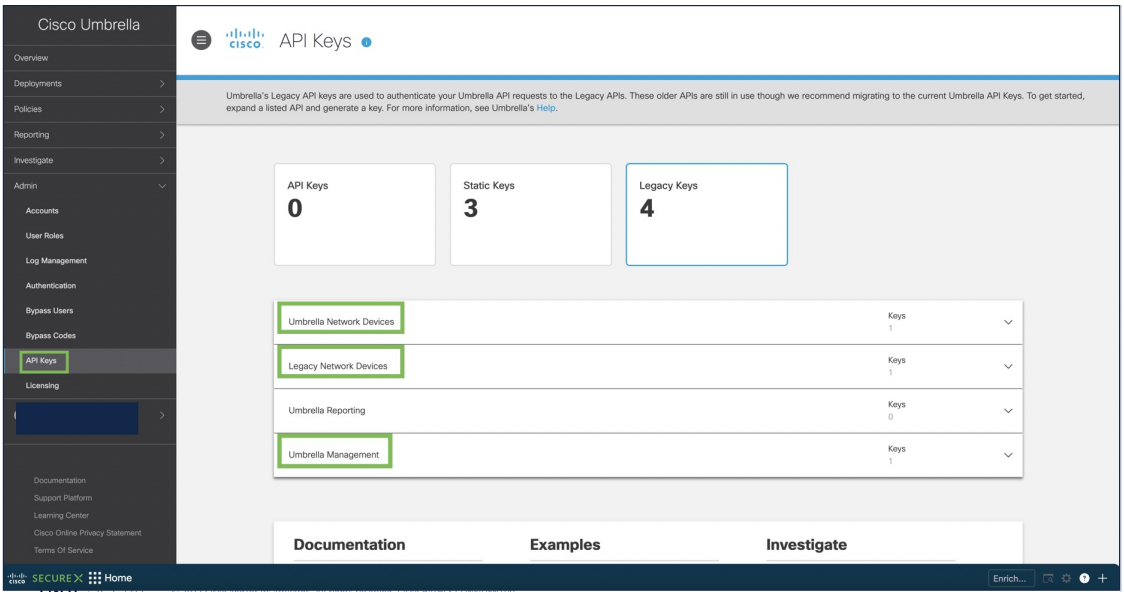
Cisco Umbrella 등록 서버와의 HTTPS 연결을 설정하기 위해 루트 인증서를 가져와야 합니다. management center에서 기본값이 아닌 옵션인 SSL 서버 검증을 위해 인증서를 신뢰해야 합니다. management center에서 디바이스의 인증서를 복사하여 붙여넣습니다(**Device(**디바이스**) > Certificates(**인증서**)**).

- 디바이스에서 인증서를 설치합니다.
- Umbrella에서 다음 데이터를 가져옵니다.
  - 조직 ID
  - 네트워크 디바이스 키
  - 네트워크 디바이스 암호
  - 레거시 네트워크 디바이스 토큰
- management center가 인터넷에 연결되어 있는지 확인합니다.
- 내보내기 제어 기능 옵션이 포함된 기본 라이센스가 management center에서 활성화되어 있는지 확인합니다.
- DNS 서버가 api.opendns.com을 확인하도록 구성되었는지 확인합니다.
- management center가 정책 구성에 대해 management.api.umbrella.com을 확인할 수 있는지 확인합니다.
- api.opendns.com에 대한 threat defense 경로를 구성합니다.

프로시저

단계 **1** Umbrella 대시보드에서 **Admin(**관리자**)** > **API Keys(API** 키**)** > **Legacy Keys(**레거시 키**)**를 선택합니다.

그림 2: 통합을 위한 *Umbrella* 키



단계 **2** 다음 URL에서 조직 **ID**를 가져옵니다. `dashboard.umbrella.com/o/[Organization ID]/#/admin/apikeys`

URL에 표시된 번호를 복사하여 management center Umbrella Connection Details(Umbrella 연결 세부 정보) 페이지의 **Organization ID(조직 ID)** 필드에 붙여넣습니다.

단계 **3** **Umbrella Network Devices(Umbrella** 네트워크 디바이스**)**를 클릭합니다.

a) **Key(**키**)** 및 **Secret(**암호**)**을 사용할 수 없거나 알 수 없는 경우 **Refresh(**새로 고침**)**를 클릭하여 키 및 암호 쌍을 생성합니다.

b) 키를 복사하여 management center Umbrella Connection Details(Umbrella 연결 세부 정보) 페이지의 **Network Device Key(**네트워크 디바이스 키**)**필드에 붙여넣습니다.

c) 암호를 복사하여 management center Umbrella Connection Details(Umbrella 연결 세부 정보) 페이지의 **Network Device Secret(**네트워크 디바이스 암호**)**에 붙여넣습니다.

단계 **4** **Legacy Network Devices(**레거시 네트워크 디바이스**)**를 클릭합니다.

a) 키를 사용할 수 없거나 알 수 없는 경우 **Refresh(**새로 고침**)**를 클릭하여 키를 생성합니다.

b) 키를 복사하여 management center Umbrella Connection Details(Umbrella 연결 세부 정보) 페이지의 **Legacy Network Device Token(**레거시 네트워크 디바이스 토큰**)**필드에 붙여넣습니다.

Umbrella 연결 구성

프로시저

단계 **1** management center에서 **Integration(**통합**)** > **Other Integrations(**기타 통합**)** > **Cloud Services(**클라우드 서비스**)** > **Cisco Umbrella Connection(Cisco Umbrella** 연결**)**을 선택합니다.

단계 **2** 다음 세부 정보를 가져와 **General(**일반**)** 설정에 추가합니다.

- **Organization ID(**조직 **ID)** — Cisco Umbrella에서 조직을 식별하는 고유한 번호입니다. 모든 Umbrella 조직은 별도의 Umbrella 인스턴스이며 자체 대시보드가 있습니다. 조직은 이름 및 조직 ID(Org ID)로 식별됩니다.
- **Network Device Key(**네트워크 디바이스 키**)** - Cisco Umbrella에서 Umbrella 정책을 가져오기 위한 키입니다.
- **Network Device Secret(**네트워크 디바이스 암호**)** - Cisco Umbrella에서 Umbrella 정책을 가져오기 위한 암호입니다.
- **Legacy Network Device Token(**레거시 네트워크 디바이스 토큰**)** - Umbrella 레거시 네트워크 디바이스 API 토큰은 Cisco Umbrella 대시보드를 통해 발급됩니다. Umbrella에서 네트워크 디바이스를 등록하려면 API 토큰이 필요합니다.

단계 **3** **Advanced(**고급**)** 아래에서 다음과 같은 선택적 설정을 구성합니다.

- **DNSCrypt Public Key(DNSCrypt** 공개 키**)** - DNSCrypt는 엔드포인트와 DNS 서버 간의 DNS 쿼리를 인증하고 암호화합니다. DNScrypt를 활성화하기 위해 인증서 확인을 위한 DNScrypt 공개 키를 구성할 수 있습니다. 키는 32바이트 16진수 값이며 Umbrella 애니캐스트 서버의 공개 키인 B735:1140:206F:225d:3E2B:d822:D7FD:691e:A1C3:3cc8:D666:8d0c:BE04:bfab:CA43:FB79로 사전 구성됩니다.
- 관리 키 - VPN 정책에 대해 Umbrella 클라우드에서 데이터 센터 세부 정보를 가져오는 키입니다.
- 관리 암호 - VPN용 Umbrella 클라우드에서 데이터 센터를 가져오는 데 사용되는 암호입니다.

단계 **4** **Test Connection(**연결 테스트**)** 클릭 - management center에서 Cisco Umbrella Cloud에 연결할 수 있는지 테스트합니다. 필요한 조직 ID 및 네트워크 디바이스 세부 정보를 제공하면 Umbrella 연결이 생성됩니다.

단계 **5** 정보가 추가되면 **Save(**저장**)**를 클릭하여 연결 세부 정보를 저장합니다.

Umbrella DNS 정책 생성

프로시저

단계 1 management center에서 **Policies(**정책**)** > **DNS**를 선택합니다. 모든 기존 DNS 정책이 표시됩니다.

단계 2 **Add DNS Policy(DNS** 정책 추가**)** > **Umbrella DNS Policy(Umbrella DNS** 정책**)**를 클릭합니다.

단계 3 정책의 이름과 설명을 입력한 다음 **Save(**저장**)**를 클릭합니다.

(선택 사항) Umbrella DNS 규칙 편집

이 절차에 설명된 설정을 변경해야 하는 경우 Umbrella DNS 규칙을 편집합니다.

프로시저

단계 1 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **DNS**로 이동합니다.

단계 2 구성할 DNS 정책에서 **Edit(**수정**)** ( ) 아이콘을 클릭합니다.

단계 3 올바른 규칙으로 이동하고 **Edit(**수정**)** ( ) 아이콘을 다시 클릭하여 규칙을 편집합니다.

a) **Umbrella** 태그는 Umbrella에 구성된 것과 일치해야 합니다.

b) **Bypass Domain(**우회 도메인**)**은 Cisco Umbrella를 우회하여 DNS 서버로 직접 이동할 도메인을 지정합니다.

c) **DNSCrypt**는 디바이스와 Cisco Umbrella 사이의 연결을 암호화하는 데 사용됩니다. 새 규칙이 생성되면 **DNSCrypt**의 기본 설정은 **YES**입니다.

d) **Idle Timeout(**유휴 시간 제한**)**은 응답하지 않는 경우 Umbrella 서버에서 제거되는 시간을 조정합니다. 새 규칙이 생성되면 **Idle Timeout(**유휴 시간 제한**)**의 기본 설정은 00:02:00입니다.

유휴 시간 제한의 형식은 (hh:mm:ss)입니다.

Umbrella DNS 정책을 액세스 제어 정책에 연결

프로시저

단계 1 **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동하고 편집할 액세스 정책을 선택합니다.

단계 2 **Security Intelligence(**보안 인텔리전스**)**를 선택합니다.

단계 3 **Umbrella DNS Policy(Umbrella DNS** 정책**)**에서 Umbrella DNS 정책에 사용할 정책을 선택합니다.

단계 **4** 모든 변경 사항을 저장하려면 **Save(**저장**)**를 선택합니다.

변경 구축

프로시저

단계 **1** management center 메뉴 모음에서 **Deploy(**구축**)**를 클릭한 다음 **Deployment(**구축**)**를 선택합니다.

단계 **2** 컨피그레이션 변경 사항을 구축할 디바이스를 식별하여 선택합니다.

- Search(검색)-검색 상자에서 디바이스 이름, 유형, 도메인, 그룹 또는 상태를 검색합니다.
- Expand(확장)-구축할 디바이스 별 구성 변경 사항을 보려면 **Expand Arrow(**확장 화살표**)**( )을 클릭합니다.

  디바이스 확인란을 선택하면 디바이스 아래에 나열된 디바이스에 대한 모든 변경 사항이 푸시되어 구축됩니다. 그러나 **Policy selection(**정책 선택**)** ( )를 사용하면 구축하지 않고 나머지 변경 사항을 보류하면서 구축할 개별 정책 또는 구성을 선택할 수 있습니다.

  선택적으로, 수정되지 않은 관련 정책을 선택적으로 보거나 숨기는 데 **Show or Hide Policy(**정책 표시 또는 숨기기**)** ( )을(를) 사용할 수 있습니다.

단계 **3** (선택 사항) 대략적인 구축 기간을 확인하려면 **Estimate(**견적**)**를 클릭합니다.

단계 **4** **Deploy(**구축**)**를 클릭합니다.

단계 **5** 구축할 변경 사항에서 오류나 경고를 식별하면 시스템은 **Validation Messages(**검증 메시지**)** 창에 이를 표시합니다. 전체 세부 사항을 보려면 경고 또는 오류 앞에 있는 화살표 아이콘을 클릭합니다.

다음 옵션을 이용할 수 있습니다.

- Deploy(구축) - 경고 조건을 해결하지 않고 구축을 계속합니다. 오류가 식별되는 경우 계속 진행할 수 없습니다.
- Close(닫기) -구축하지 않고 종료합니다. 오류 및 경고 조건을 해결하고 컨피그레이션을 재구축합니다.

구축 검증

프로시저

단계 **1** 구축이 완료되면 management center에서 구축을 검증합니다.

단계 **2** 구축을 선택한 다음 구축 기록 아이콘을 선택합니다.

단계 **3** Umbrella 커넥터와 연결된 작업을 선택합니다.

단계 **4** **Transcript Details(**대화 내용 상세정보**)**( ) 아이콘을 선택합니다.

다음 명령줄 인터페이스 트랜스크립트가 생성됩니다.

예제:

```
FMC >> strong-encryption-disable
FMC >> umbrella-global
FMC >> token umbrella_token
10.0.0.0 >> [info] : Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license
FMC >> local-domain-bypass “test.com"
FMC >> timeout edns hh:mm:ss
FMC >> exit
FMC >> policy-map type inspect dns preset_dns_map
FMC >> parameters
FMC >> umbrella tag “Default Policy”
FMC >> dnscrypt
```

구축 문제 해결

레거시 네트워크 디바이스 토큰이 구성되지 않았음

오류: 레거시 네트워크 디바이스 토큰이 비어 있으므로 Umbrella 전역을 구성할 수 없습니다.

- 가능한 원인 Umbrella 연결 세부 정보가 **Integration(**통합**)** 탭에 추가되지 않았습니다. **Integration(**통합**)** 탭 내에서 세부 정보를 구성하는 데 Umbrella 연결 구성, 5 페이지를 사용합니다.
- 가능한 원인 management center가 인터넷에 연결되어 있지 않습니다. 인터넷에 연결되어 있지 않으면 management center에서 Umbrella 클라우드에 연결할 수 없습니다.
- 가능한 원인 Umbrella 연결 세부 정보가 추가되었지만 정보가 올바르지 않습니다. Umbrella 연결 구성, 5 페이지를 사용하여 적절한 정보를 입력하고 연결을 테스트하여 Umbrella가 연결되어 있는지 확인합니다.

내보내기 제어 기능이 활성화되지 않았음

선택 가능한 라이선스는 활성화(등록)하거나 비활성화(해제)할 수 있습니다. 라이선스를 통해 제어되는 기능을 사용하려면 라이선스를 활성화해야 합니다.

선택적 기간 라이선스가 적용되는 기능을 더 이상 사용하지 않으려는 경우 라이선스를 비활성화할 수 있습니다. 비활성화하는 라이선스는 Cisco Smart Software Manager 어카운트에서 해제되므로 다른 디바이스에 적용할 수 있습니다.

평가 모드에서 실행 중인 경우 이러한 라이선스의 평가 버전을 활성화할 수도 있습니다. 평가 모드에서 라이선스는 디바이스를 등록할 때까지 Cisco Smart Software Manager에 등록되지 않습니다. 그러나 평가 모드에서는 RA VPN 또는 캐리어 라이선스를 활성화할 수 없습니다.

시작하기 전에

라이선스를 비활성화하기 전에 해당 라이선스를 사용하고 있지 않은지 확인합니다. 라이선스가 필요한 정책은 재작성하거나 삭제합니다.

고가용성 컨피그레이션에서 작동 중인 유닛의 경우 액티브 유닛에서만 라이선스를 활성화하거나 비활성화합니다. 다음번 컨피그레이션 구축 시에 스탠바이 유닛이 필요한 라이선스를 요청하거나 해제할 때 변경 사항이 스탠바이 유닛에 반영됩니다. 라이선스를 활성화하는 경우에는 Cisco Smart Software Manager 어카운트에 사용 가능한 라이선스가 충분한지 확인해야 합니다. 그렇지 않으면 각 유닛의 컴플라이언스 상태가 서로 다를 수 있습니다.

프로시저

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

단계 **2** 선택 가능한 각 라이선스에 대해 **Enable(**활성화**)/Disable(**비활성화**)** 컨트롤을 필요한 대로 클릭합니다.

- **Enable(**활성화**)** - Cisco Smart Software Manager 어카운트에 라이선스를 등록하고 제어되는 기능을 활성화합니다. 이제 라이선스를 통해 제어되는 정책을 구성하고 구축할 수 있습니다.
- **Disable(**비활성화**)** - Cisco Smart Software Manager 어카운트에서 라이선스를 등록 취소하고 제어되는 기능을 비활성화합니다. 이렇게 하면 새 정책에서 기능을 구성할 수 없으며 해당 기능을 사용하는 정책을 구축할 수도 없습니다.

단계 **3** **RA VPN** 라이선스를 활성화한 경우 어카운트에서 사용 가능한 라이선스의 유형을 선택합니다.

다음 라이센스를 사용할 수 있습니다. **Plus**, **Apex**, 또는 **VPN** 만. **Plus** 및 **Apex** 라이센스를 둘 다 보유하고 모두 사용하려는 경우 선택할 수 있습니다.