

방법:무선 네트워크 보호를 위해 Cisco Umbrella 확장

소개

데이터 보안은 모든 조직의 그룹 노력입니다.직원들은 최소한 그들이 사기를 당하지 않도록 하는 것에 대한 부분적으로 책임이 있다.실제로 보안은 까다롭고 그 이유가 놀랍지 않습니다.기술의 도구들이 해커의 발전에도 동일하게 확장됨에 따라, 모든 배들은 밀도에 따라 일어납니다.LAN에 Umbrella 보호를 통합하는 방법을 자세히 알아보십시오.

목표

이 가이드는 Umbrella의 보안 플랫폼을 무선 네트워크에 통합하는 단계를 보여줍니다.핵심 세부 사항을 살펴보기 전에 Umbrella에 대해 자문해 볼 수 있는 몇 가지 질문에 답변해 드리겠습니다.

적용 가능한 디바이스

- WAP125
- WAP581

소프트웨어 버전

- 1.0.1

요구 사항

활성 Umbrella 계정(계정이 없습니까?[견적 요청](#) 또는 [무료 평가판](#) 시작)

Umbrella란?

Umbrella는 Cisco의 간단하면서도 매우 효과적인 클라우드 보안 플랫폼입니다.Umbrella는 클라우드에서 작동하며 많은 보안 관련 서비스를 수행합니다.긴급 위협에서 사후 이벤트 조사에 이르기까지 Umbrella는 모든 포트 및 프로토콜에서 공격을 검색하고 차단합니다.

작동 방식

Umbrella는 DNS를 방어하는 주 벡터로 사용합니다.사용자가 브라우저 표시줄에 URL을 입력하고 Enter 키를 누르면 Umbrella가 전송에 참여합니다.이 URL은 Umbrella의 DNS 확인자에 전달되며, 보안 경고가 도메인과 연결된 경우 요청이 차단됩니다.이 텔레메트리 데이터는 전송되고 마이크로 초 단위로 분석되므로 레이턴시가 거의 발생하지 않습니다.텔레메트리 데이터는 전 세계 수십억 개의 DNS 요청을 추적하는 로그 및 기기를 사용합니다.이 데이터가 널리 보급될 때 전 세계적으로 데이터를 상호 연결하여 공격이 시작될 때 신속하게 대응할 수 있습니다.자세한 내용은 Cisco의 개인 정보 보호 정책([전체 정책](#), [요약 버전](#))을 참조하십시오.텔레메트리 데이터를 통과 로그에서 파생된 데이터로 간주합니다.

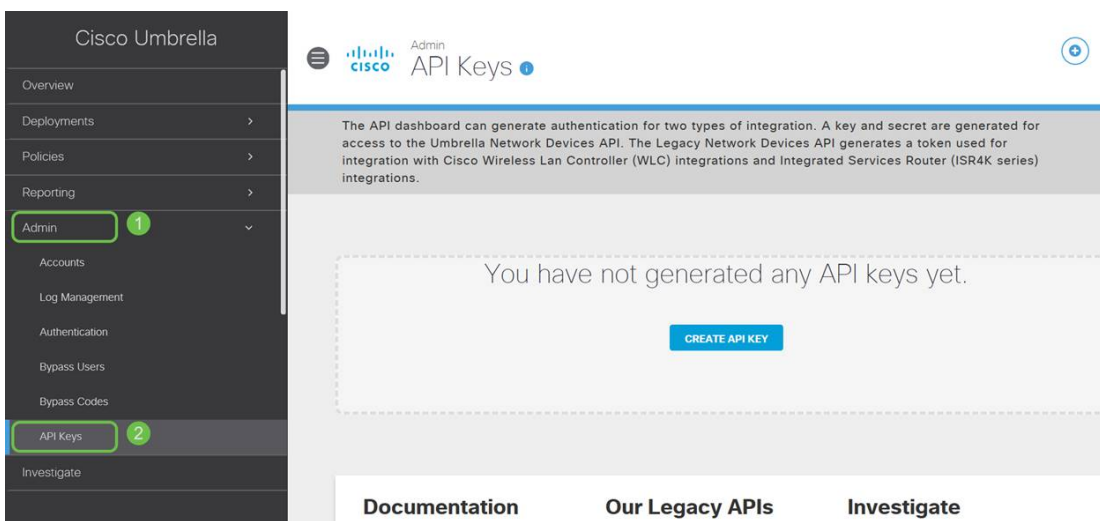
요약하자면, 여러분이 파티에 있다고 상상해 보세요.이 파티에서 모든 사람들은 인터넷을 검색하며 전화한다.조용한 단체 침묵은 파티 참석자들이 그들의 화면을 두드리는 것에 의해 중단됩니다.[멋진](#)

[파티는 아니지만](#), 휴대폰에서는 거부할 수 없는 새끼 GIF의 하이퍼링크를 볼 수 있습니다.그러나 URL이 의심스러운 것으로 나타나므로 탭할지 여부를 확신할 수 없습니다.따라서 하이퍼링크를 누르기 전에 나머지 파티에 대해 "이 링크가 잘못되었습니까?"라고 소리칩니다. 만약 그 당의 다른 사람이 그 링크에 가본 적이 있고 그것이 사기였다는 것을 알게 되면, 그들은 "그래, 내가 했고 그것은 사기야!"라고 다시 소리칠 것이다. 그 사람이 당신을 구해준 것에 대해 감사하고, 조용히 귀여운 동물의 사진을 계속해서 찾아.물론 Cisco의 규모에서는 이러한 유형의 요청 및 콜백 보안 검사가 초당 수백만 번 발생합니다.

좋습니다, 어떻게 시작할까요?

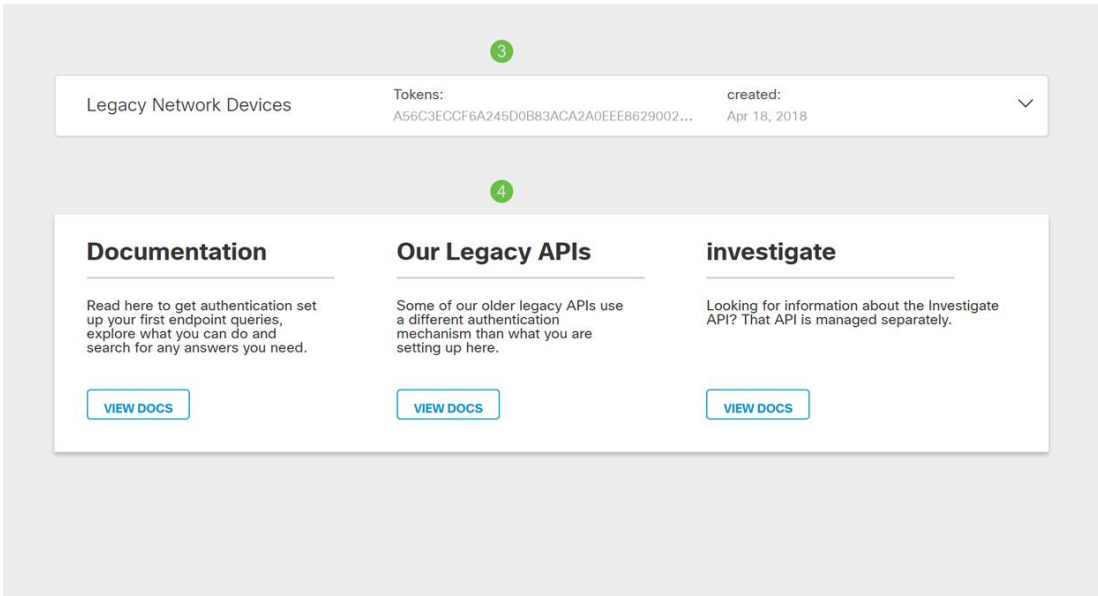
이 설명서에서 Umbrella 어카운트 대시보드에서 API 키와 Secret 키를 사용하여 시작합니다.그런 다음 WAP 디바이스에 로그인하여 API 및 Secret 키를 추가합니다.문제가 발생한 경우 [여기](#)에서 [설명서](#)를 확인하고 [여기](#)에서 Umbrella [Support 옵션을 확인하십시오](#).

1단계. Umbrella Account에 로그인한 후 *Dashboard* 화면에서 **Admin > API Keys**를 클릭합니다.

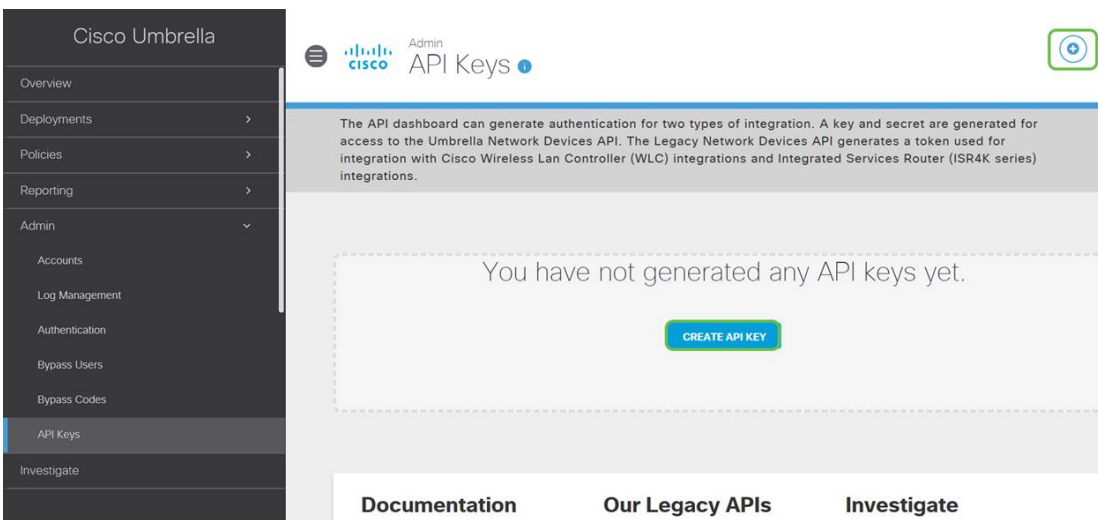


API 키 화면 구조 -

1. *Add API Key*(API 키 추가) - Umbrella API와 함께 사용할 새 키 생성을 시작합니다.
2. *추가 정보* - 이 화면에 대한 설명과 함께 아래로/위로 슬라이딩합니다.
3. *Token Well*(토큰 웰) - 이 계정에서 만든 모든 키와 토큰이 들어 있습니다.(키가 생성되면 입력 됨)
4. *지원 문서* - 각 섹션의 항목과 관련된 Umbrella 사이트의 문서 링크



2단계. 오른쪽 상단 모서리에 있는 **Add API Key(API 키 추가)** 버튼을 클릭하거나 **Create API Key(API 키 생성)** 버튼을 클릭합니다. 둘 다 같은 기능을 합니다.



3단계. **Umbrella Network Devices(Umbrella 네트워크 디바이스)**를 선택한 다음 **Create(생성)** 버튼을 클릭합니다.

What should this API do?

Choose the API that you would like to use.

1



Umbrella Network Devices

To be used to integrate Umbrella-enabled hardware with your organization. In addition, allows you to create, update, list and delete identities in Umbrella.



Legacy Network Devices

A Network Devices token enables hardware network devices such as Cisco Wireless Lan Controllers and Cisco Integrated Services Routers 4000 series to integrate with Umbrella.

i You can only generate one token. Refresh your current token to get a new token.



Umbrella Reporting

Enables API access to query for Security Events and traffic to specific Destinations

CANCEL


2


CREATE

4단계. 비밀 키 오른쪽에 있는 복사 버튼을 클릭하면 팝업 알림이 키를 클립보드에 복사했는지 확인합니다.

Umbrella Network Devices Key: aae [REDACTED] Created: Jul 26, 2018

The API key and secret here are used to perform API requests against your Umbrella organization, such as identity management, reporting and more. If you are using an Umbrella-integrated hardware device that uses basic authentication, this allows management of Umbrella from the device and vice versa.

Your Key: aae [REDACTED] 

Your Secret: 352 [REDACTED] 

To keep it secure, we only display your key's secret once. For future reference, copy this secret and keep it in a safe place. Tick this box to acknowledge this.

Check out the [documentation](#) for step by step instructions.

[DELETE](#) [REFRESH](#) [CLOSE](#)

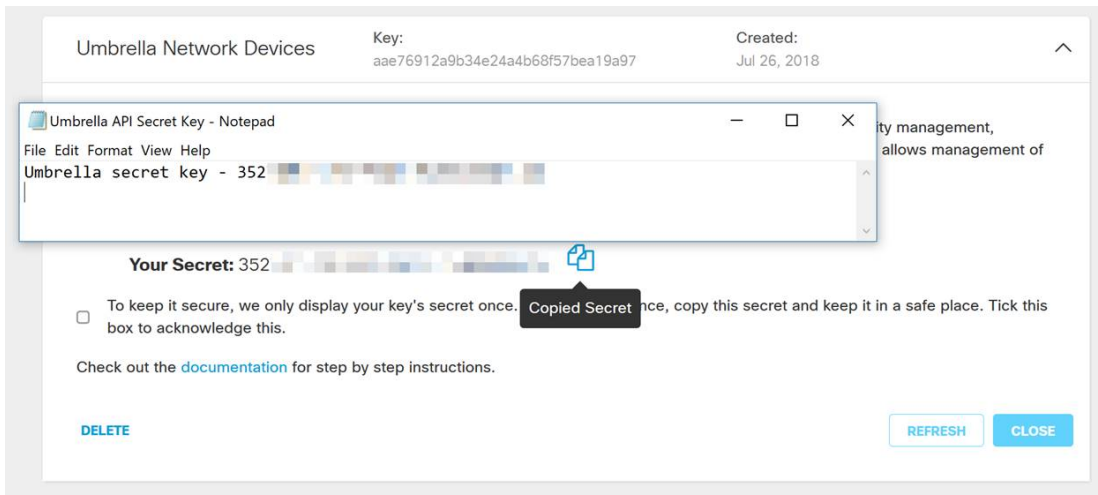
키와 비밀 키를 안전한 위치에 복사한 후 확인 **확인란**을 클릭하여 확인을 완료한 다음 닫기 버튼을 클릭합니다.

To keep it secure, we only display your key's secret once. For future reference, copy this secret and keep it in a safe place. Tick this box to acknowledge this.

Check out the [documentation](#) for step by step instructions.

[DELETE](#) [REFRESH](#) [CLOSE](#)

5단계. 메모장과 같은 텍스트 편집기를 열고 기밀 및 API 키를 문서에 붙여 넣고 나중에 참조할 수 있도록 레이블을 지정합니다. 이 경우 레이블은 "Umbrella 비밀 키"입니다. API 키를 비밀 키와 함께 이 동일한 텍스트 파일에서 사용 방법에 대한 간단한 설명을 포함합니다. 그런 다음 나중에 필요할 때 쉽게 액세스할 수 있는 안전한 위치에 텍스트 파일을 저장합니다.



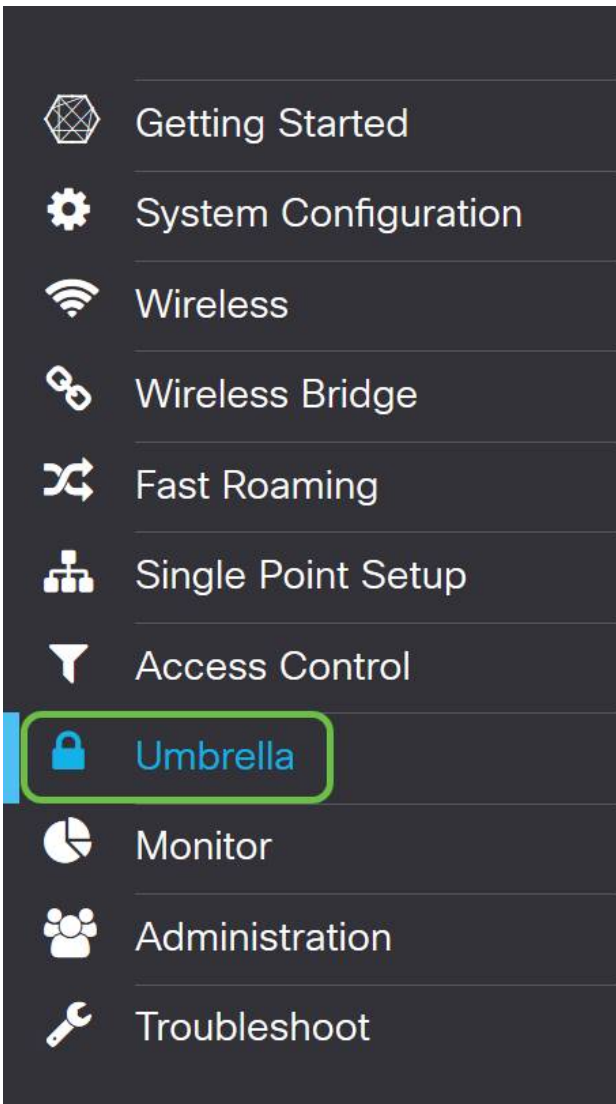
중요 참고 사항:비밀 키를 분실하거나 실수로 삭제하면 이 키를 검색하기 위해 호출할 기능 또는 지원 번호가 없습니다. [비밀로 하고 안전하게 지켜라](#). 분실된 경우 키를 삭제하고 Umbrella로 보호하려는 각 WAP 디바이스로 API 키를 다시 인증해야 합니다.

모범 사례:USB Thumb 드라이브와 같은 장치에 이 문서의 단일 사본만 보관하면 어떤 네트워크에서도 액세스할 수 없습니다.

WAP 장치에 Umbrella 구성

이제 Umbrella에서 API 키를 생성했으므로 해당 키를 가져와 WAP 디바이스에 설치합니다.여기서는 WAP581을 사용합니다.

1단계. WAP 디바이스에 로그인한 후 사이드바 메뉴에서 Umbrella를 클릭합니다.



2단계. Umbrella(우산) 화면은 간단하지만 여기에서 정의할 만한 두 필드가 있습니다.

- *Local Domains to Bypass*(우회할 로컬 도메인) - 이 필드에는 Umbrella 서비스에서 제외하려는 내부 도메인이 포함됩니다.
- *DNSCrypt* - DNS 클라이언트와 DNS 확인자 간의 패킷 전송을 보호합니다.이 기능은 기본적으로 설정되어 있습니다. 이 기능을 비활성화하면 네트워크의 보안이 약화됩니다.

A screenshot of the Cisco Umbrella configuration page for device WAP581-WAP581. The page title is "Umbrella" and it has "Save" and "Cancel" buttons. The page contains the following fields:

- Enable:
- API Key:
- Secret:
- Local Domains to Bypass (optional):
- Device Tag (optional):
- DNSCrypt: Enable
- Registration Status:

3단계. API 및 비밀 키를 해당 필드에 붙여넣습니다.

WAP581-WAP581

Umbrella

Save Cancel

Cisco Umbrella is a cloud security platform that provide the first line of defense against threats on the internet wherever users go.
 With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.
 This device will appear in the [Umbrella dashboard](#) as a network device for applying policy and viewing reports.

Enable:

API Key:

Secret:

Local Domains to Bypass (optional):

Device Tag (optional):

DNSCrypt: Enable

Registration Status:

4단계. Enable(활성화) 및 DNSCrypt의 확인란이 확인 상태로 전환되었는지 확인합니다.

WAP581-WAP581

Umbrella

Save Cancel

Cisco Umbrella is a cloud security platform that provide the first line of defense against threats on the internet wherever users go.
 With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.
 This device will appear in the [Umbrella dashboard](#) as a network device for applying policy and viewing reports.

Enable:

API Key:

Secret:

Local Domains to Bypass (optional):

Device Tag (optional):

DNSCrypt: Enable

Registration Status:

참고:DNSCrypt는 DNS 클라이언트와 DNS 확인자 간의 DNS 통신을 보호합니다.기본값은 enabled입니다.

5단계. (선택 사항) Umbrella에서 DNS 확인 프로세스를 통해 허용할 로컬 도메인을 입력합니다.

WAP581-WAP581

Umbrella

Save Cancel

Cisco Umbrella is a cloud security platform that provide the first line of defense against threats on the internet wherever users go.
 With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.
 This device will appear in the [Umbrella dashboard](#) as a network device for applying policy and viewing reports.

Enable:

API Key:

Secret:

Local Domains to Bypass (optional):

Device Tag (optional):

DNSCrypt: Enable

Registration Status:

참고:이는 모든 인트라넷 도메인 및 스플릿 DNS 도메인에 필요합니다.네트워크에서 라우팅을 위해 로컬 영역 도메인을 사용해야 하는 경우 Umbrella 지원에 문의하여 이 기능을 설치하고 실행해야 합니다.대부분의 사용자는 이 옵션을 사용할 필요가 없습니다.

6단계. 변경 내용에 만족하거나 *Local Domains to Bypass*(우회에 사용자의 로컬 도메인을 추가한 후 오른쪽 상단 모서리의 Save(저장) 버튼을 클릭합니다.



7단계. 변경이 완료되면 *Registration Status*(등록 상태) 필드에 "Successful(성공)"이 표시됩니다.


A screenshot of the Cisco Umbrella configuration form. The form contains several fields and checkboxes. 'Enable:' is checked. 'API Key:' contains 'aae' followed by a blurred area. 'Secret:' contains '352' followed by a blurred area. 'Local Domains to Bypass (optional):' contains 'Multiple inputs separated by comma'. 'Device Tag (optional):' contains 'WAP581'. 'DNSCrypt:' is checked and labeled 'Enable'. The 'Registration Status:' field at the bottom is highlighted with a green border and contains the text 'Successful'.

모든 것이 제대로 갖춰져 있는지 확인

축하합니다. 이제 Cisco의 Umbrella를 보호하고 계십니다.아니면 당신은?Cisco는 페이지가 로드되는 즉시 이를 확인하는 데 필요한 전용 웹 사이트를 만들었습니다.[여기를](#) 클릭하거나 브라우저 표시줄에 <https://InternetBadGuys.com>을 입력합니다.

Umbrella가 올바르게 구성된 경우 이와 유사한 화면이 표시됩니다.

SECURITY THREAT DETECTED AND BLOKED



SECURITY THREAT DETECTED AND BLOKED

Based on Cisco Umbrella security threat information, access to the web site **Not_Found** has been blocked to prevent an attack on your browser.

Malware protection has shifted from the endpoint, deeper into the network, in order to cater to a growing number and variety of devices. In order to offer the most effective protection to computing assets on the Cisco network, Infosec, Cisco IT, and the Security Business Group have jointly rolled out Umbrella protection for Cisco's corporate DNS infrastructure. This service will block access to hostnames that are known bad and has been deployed to prevent malicious actors from serving malware or content otherwise harmful to users of the Cisco corporate network.

If you believe this page should not be blocked, [open a case](#) providing the following information:

- Text or screenshot of the corresponding debug information below
- Business justification for use of the website

Block Reason: Umbrella DNS Block

Date: July 26, 2018
Time: 22:58:17
Host Requested: Not_Found
URL Requested: Not_Found
Client IP address: [REDACTED]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Request Method: GET

이 문서와 관련된 비디오 보기...

[여기를 클릭하여 Cisco의 다른 기술 대화를 확인하십시오.](#)