

# TTA(Traffic Telemetry Appliance) 및 Cisco DNA Center App Assurance 활용: 이유와 방법

## 목차

---

[소개](#)

[사전 요구 사항](#)

[애플리케이션 보증](#)

[애플리케이션 가시성\(AppVis\)](#)

[애플리케이션 환경\(AppX\)](#)

[트래픽 텔레메트리 어플라이언스를 사용해야 하는 이유](#)

[TTA 디바이스 세부 정보](#)

[보증을 위한 Cisco DNA Center 사전 요구 사항](#)

[운영 Cisco DNA Center 클러스터](#)

[ISE와 Cisco DNA Center 통합](#)

[텔레메트리를 위한 Cisco DNA Center 요구 사항](#)

[Cisco DNA Center 주요 패키지](#)

[텔레메트리 컬렉터로서의 Cisco DNA Center](#)

[Cisco AI 클라우드](#)

[NBAR\(Network Based Application Recognition\) 클라우드](#)

[CBAR\(컨트롤러 기반 애플리케이션 인식\) 및 SD-AVC](#)

[Microsoft Office 365 Cloud Connector\(가 없어야 함\)](#)

[TTA 구현](#)

[TTA 워크플로 개요](#)

[TTA 구축: 하이 레벨 다이어그램](#)

[TTA 소프트웨어 및 라이선싱 요구 사항](#)

[TTA 온보딩 및 Day-0 컨피그레이션](#)

[Cisco DNA Center 인벤토리에 TTA 어플라이언스 추가](#)

[SPAN 컨피그레이션](#)

[수집된 보증](#)

[다음을 확인합니다.](#)

---

## 소개

이 문서에서는 Cisco DNA Traffic Telemetry Appliance(Cisco 부품 번호 DN-APL-TTA-M) 플랫폼과 함께 Cisco DNA Center에서 애플리케이션 보증을 활성화하는 방법에 대해 설명합니다. 또한 TTA를 구성 및 확인 프로세스와 함께 네트워크에서 어떻게 어디에 배치할 수 있는지도 조명합니다. 이 문서에서는 관련된 다양한 전제 조건도 다룹니다.

## 사전 요구 사항

Cisco는 Cisco DNA Center Assurance 및 Application Experience가 어떻게 작동하는지 알고 있는 것이 좋습니다.

## 애플리케이션 보증

보증은 네트워크 데이터의 비즈니스 잠재력을 크게 높일 수 있는 다목적 실시간 네트워크 데이터 수집 및 분석 엔진입니다. Assurance는 복잡한 애플리케이션 데이터를 처리하고 그 결과를 Assurance 상태 대시보드에 표시하여 네트워크에서 사용되는 애플리케이션의 성능에 대한 통찰력을 제공합니다. 데이터가 수집되는 위치에 따라 다음 중 일부 또는 전체를 볼 수 있습니다.

- 애플리케이션 이름
- 처리량
- DSCP 표시
- 성능 메트릭(레이턴시, 지터, 패킷 손실)

애플리케이션 보증은 수집된 데이터의 양에 따라 다음 두 가지 모델로 분류할 수 있습니다.

- 애플리케이션 가시성(AppVis) 및
- 애플리케이션 환경(AppX)

애플리케이션 이름 및 처리량을 총칭하여 정량적 메트릭이라고 합니다. 정량적 메트릭에 대한 데이터는 애플리케이션 가시성을 활성화하는 것에서 비롯됩니다.

DSCP 마킹 및 성능 메트릭(레이턴시, 지터, 패킷 손실)을 정성적 메트릭이라고 통칭합니다. 정성적 메트릭스에 대한 데이터는 Application Experience를 활성화한 결과입니다.

### 애플리케이션 가시성(AppVis)

애플리케이션 가시성 데이터는 Cisco IOS® XE를 실행하는 스위치와 AireOS를 실행하는 무선 컨트롤러에서 수집됩니다. Cisco IOS XE를 실행하는 스위치의 경우, 물리적 레이어 액세스 스위치 포트에 양방향으로(인그레스 및 이그레스) 적용되는 사전 정의된 NBAR 템플릿을 사용하여 애플리케이션 가시성 데이터를 수집합니다. AireOS를 실행하는 무선 컨트롤러의 경우, Application Visibility(애플리케이션 가시성) 데이터가 무선 컨트롤러에서 수집된 다음 스트리밍 텔레메트리를 사용하여 이 데이터를 Cisco DNA Center로 전송합니다.

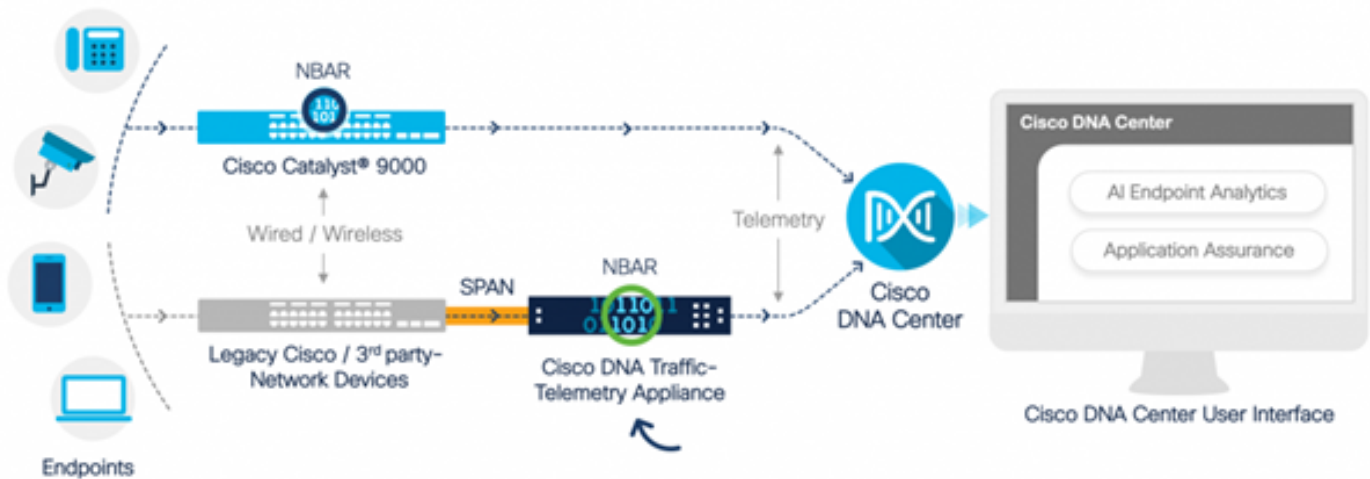
### 애플리케이션 환경(AppX)

애플리케이션 경험 데이터는 Cisco IOS XE 라우터 플랫폼에서 수집되며, 특히 PerfMon(Cisco Performance Monitor) 기능과 Cisco ART(Application Response Time) 메트릭을 사용합니다. 라우터 플랫폼의 예에는 ASR 1000, ISR 4000 및 CSR 1000v가 포함됩니다. Cisco DNA Center와의 디바이스 호환성에 대해서는 [Cisco DNA Center 호환성 매트릭스를 참조하십시오.](#)

## 트래픽 텔레메트리 어플라이언스를 사용해야 하는 이유

Cisco Catalyst 9000 Series 유무선 디바이스는 DPI(Deep Packet Inspection)를 수행하고 Cisco DNA Center에서 Cisco AI Endpoint Analytics 및 Application Assurance와 같은 서비스를 위한 데이터 스트림을 제공합니다. 그러나 네트워크에 텔레메트리를 추출할 Catalyst 9000 Series 장치가 없

다면 어떻게 될까요? 몇몇 조직에서는 여전히 네트워크 인프라 중 일부가 Cisco Catalyst 9000 Series 플랫폼으로 마이그레이션되지 않았습니다. Catalyst 9000 플랫폼은 AppVis 텔레메트리를 생성하지만, AppX에 대한 추가 통찰력을 얻기 위해 Cisco DNA Traffic Telemetry Appliance를 사용하여 격차를 해소할 수 있습니다. TTA의 목표는 Cisco DNA Center에 Application Experience 데이터를 제공하는 기능이 없는 다른 네트워크 디바이스에서 SPAN 포트를 통해 수신하는 트래픽을 모니터링하는 것입니다. 레거시 인프라 디바이스는 고급 분석에 필요한 심층 패킷 검사를 수행할 수 없으므로 Cisco DNA Traffic Telemetry Appliance를 사용하여 기존 레거시 구축에서 AppX 텔레메트리를 생성할 수 있습니다.



Cisco TTA 적용 사례

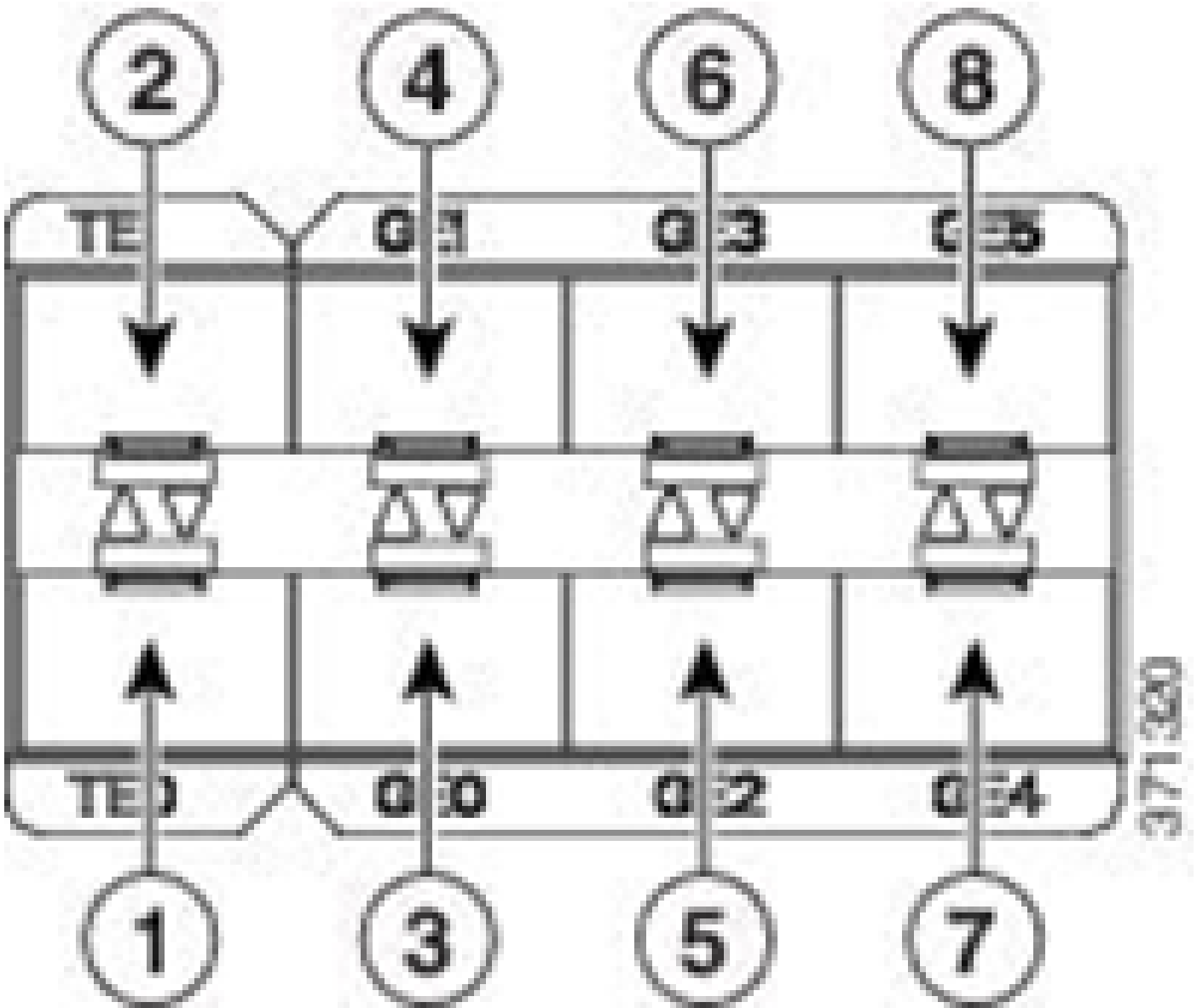
## TTA 디바이스 세부 정보

Cisco IOS XE 기반 텔레메트리 센서 플랫폼은 스위치 및 무선 컨트롤러의 SPAN(Switched Port Analyzer) 세션에서 미러링된 IP 네트워크 트래픽으로부터 텔레메트리를 생성합니다. 어플라이언스는 NBAR(Network-Based Application Recognition) 기술을 사용하여 수천 개의 프로토콜을 검사하여 Cisco DNA Center가 분석을 수행할 수 있도록 텔레메트리 스트림을 생성합니다. Cisco DNA Traffic Telemetry Appliance는 20Gbps의 지속적인 처리량 트래픽을 처리하고 디바이스 프로파일링을 위해 40,000개의 엔드포인트 세션을 검사할 수 있습니다.



Cisco Traffic Telemetry Appliance

TTA에는 SPAN 수집에 사용되는 10기가비트 및 1기가비트 링크가 혼합되어 있습니다. 이 포트 중 Gig0/0/5는 IP 주소로 구성할 수 있으며 Cisco DNA Center와의 통신에 사용할 수 있는 유일한 포트입니다. 인터페이스 매트릭스는 다음과 같습니다.



TTA 인터페이스 매트릭스

TTA 인터페이스 매트릭스	
1 10GE SFP+ 포트 0/0/0	5 GE SFP 포트 0/0/2
2 10GE SFP+ 포트 0/0/1	6 GE SFP 포트 0/0/3
3 GE SFP 포트 0/0/0	7 GE SFP 포트 0/0/4
4 GE SFP 포트 0/0/1	8 GE SFP 포트 0/0/5

## 보증을 위한 Cisco DNA Center 사전 요구 사항

이 섹션에서는 Cisco DNA Center에서 텔레메트리를 처리하기 전에 충족해야 하는 컨피그레이션 및 전제 조건을 중점적으로 살펴봅니다.

### 운영 Cisco DNA Center 클러스터

TTA 관리 및 텔레메트리 처리에 사용되는 Cisco DNA Center 클러스터는 다음 조건으로 프로비저닝해야 합니다.

- 네트워크 계층: 설계 워크플로우의 네트워크 계층 섹션을 사용하여 서로 다른 사이트 캠퍼스, 해당 캠퍼스 내의 건물 및 해당 건물 내의 개별 층을 정의하고 이를 세계 지도에 표시합니다. 적절한 사이트/네트워크 계층을 구성해야 합니다.
- 네트워크 설정: Network Settings(네트워크 설정) 섹션에서는 네트워크 내의 디바이스에서 사용할 일반적인 기본 네트워크 설정을 생성할 수 있습니다. 이러한 설정은 사이트, 건물 또는 층 수준뿐만 아니라 전역 방식으로도 적용할 수 있습니다. 구축에 필요한 대로 DNS, 도메인 이름, syslog, NTP, 시간대 및 로그인 배너 정보를 입력합니다.
- 디바이스 자격 증명: 이러한 자격 증명은 TTA를 포함하여 네트워크에서 디바이스를 액세스하고 검색하는 데 사용됩니다. 적절한 CLI 및 SNMP 자격 증명을 사용하여 Cisco DNA Center를 구성해야 합니다. 이 NetConf 자격 증명과 함께 사용하면 좋습니다.
- Cisco CCO 계정: 어플라이언스를 연결하고 Cisco AI Cloud의 기능을 활용하고, SWIM용 이미지를 다운로드하고, TTA 및 기타 디바이스용 프로토콜 팩을 다운로드하려면 유효한 CCO 계정이 필요합니다.

### ISE와 Cisco DNA Center 통합

Cisco ISE(Identity Services Engine) 및 Cisco DNA Center는 ID 및 정책 자동화를 위해 통합될 수 있습니다. ISE는 Cisco AI Endpoint Analytics를 활용하기 위해 엔드포인트에 대한 정보를 수집하는 데에도 사용됩니다. PxGrid는 ISE와 Cisco DNA Center 간의 통합을 구현하는 데 사용됩니다.

Cisco DNA Center 및 ISE 통합 요구 사항은 다음과 같습니다.

- pxGrid 서비스는 ISE에서 활성화되어야 합니다.
- ERS 읽기/쓰기 액세스를 활성화해야 합니다.
- ISE 관리자 인증서는 주체 이름 또는 SAN 필드에 ISE의 IP 주소 또는 FQDN을 포함해야 합니다.
- Cisco DNA Center 시스템 인증서는 주체 이름 또는 SAN 필드에 Cisco DNA Center의 모든 IP 주소 또는 FQDN을 포함해야 합니다.
- ISE ERS 관리자 자격 증명은 ISE와 Cisco DNA Center 간의 ERS 통신을 신뢰 설정하는 데 사용됩니다.
- pxGrid 노드는 Cisco DNA Center에서 연결할 수 있어야 합니다.

### 텔레메트리를 위한 Cisco DNA Center 요구 사항

Cisco DNA Center에서 Application Assurance를 사용하려면 구현해야 할 요구 사항이 있습니다. 이

러한 요구 사항은 다음 섹션에서 자세히 설명합니다.

## Cisco DNA Center 주요 패키지

Cisco DNA Center에서 텔레메트리 데이터를 활성화하고 분석하려면 이 세 가지 패키지를 설치해야 합니다.

- AI 엔드포인트 분석
- AI 네트워크 분석
- 애플리케이션 가시성 서비스

# Cisco DNA Center

Version 2.1.2.0

Release Notes

▼ Packages

Access Control Application	2.1.260.62555
AI Endpoint Analytics	1.2.1.320
AI Network Analytics	2.4.15.0
Application Registry	2.1.260.170177
Application Visibility Service	2.1.260.170177
Assurance - Base	2.1.2.273
Automation - Base	2.1.260.62555
Cisco DNA Center Global Search	1.2.5.9
Cisco DNA Center Platform	1.3.99.194
Cisco DNA Center UI	1.5.1.26
Cloud Connectivity - Data Hub	1.6.0.162
Cloud Connectivity - Tethering	1.3.1.86
Command Runner	2.1.260.62555
Device Onboarding	2.1.260.62555

> [Serial number](#)

© 2020 Cisco Systems Inc. All Rights Reserved.

Cisco DNA Center 패키지 필요

Cisco DNA Center의 메인 페이지 오른쪽 상단에 있는 물음표 아이콘 아래에 있는 "정보" 링크를 클릭하면 이 정보에 빠르게 액세스할 수 있습니다. 이러한 애플리케이션이 누락된 경우 텔레메트리 설정을 진행하기 전에 해당 애플리케이션을 설치해야 합니다. Cisco 클라우드에서 Cisco DNA Center에 이 패키지를 설치하려면 이 가이드를 사용하십시오. [Cisco DNA Center 업그레이드 가이드](#)

## 텔레메트리 컬렉터로서의 Cisco DNA Center

NetFlow 데이터 내보내기는 심층 분석을 위해 Cisco DNA Center로 전달될 텔레메트리 데이터를 제공하는 기술 전송입니다. 기계 학습 및 엔드포인트 분석을 위한 추론을 위한 데이터 수집을 활성화하려면 NetFlow를 Cisco DNA Center로 내보내야 합니다. TTA는 텔레메트리 센서 플랫폼으로, 미러링된 IP 네트워크 트래픽에서 텔레메트리를 생성하고 애플리케이션 및 엔드포인트 가시성을 위해 Cisco DNA Center와 공유하는 데 사용됩니다.

- 네트워크 트래픽은 SPAN(Switched Port Analyzer) 미러링을 통해 스위치와 라우터에서 수신되며 Cisco DNA Traffic Telemetry Appliance 미러링 인터페이스로 전달됩니다.
- Cisco DNA Traffic Telemetry Appliance는 수신된 트래픽을 분석하여 Cisco DNA Center용 텔레메트리 스트림을 생성합니다.

Cisco DNA Center를 텔레메트리 컬렉터로 활성화하는 절차는 다음과 같습니다.

- Cisco DNA Center에서 Menu(메뉴) > Design(설계) > Network Settings(네트워크 설정)를 클릭하고 Cisco DNA Center에서 NetFlow를 수집하기 위한 텔레메트리를 활성화합니다.

### NetFlow

Choose Cisco DNA Center to be your NetFlow collector server, and/or add any external NetFlow collector server. This is the destination server for NetFlow export from network devices. Cisco DNA Center will only push the first NetFlow collector server for Wireless Controller as it has a restriction on the number of flow exporters.

Use Cisco DNA Center as NetFlow collector server

#### INTERFACES FOR APPLICATION TELEMTRY

To enable telemetry on a device , select the device from the Provision table and choose "Actions->Enable Application Telemetry" By default, All access interfaces on a switch OR all LAN-facing interfaces on a router will be provisioned. To override this default behavior, tag specific interfaces to be designated as LAN interface, by putting the keyword "lan" in the interface description.

Once specific interfaces are tagged those interfaces will be monitored.

Add an external NetFlow collector server

Only the external server destination will be configured on network devices. Flow records will not be configured.

DNAC를 NetFlow 컬렉터로 구성

## Cisco AI 클라우드

Cisco AI Network Analytics는 Cisco DNA Center 내의 애플리케이션으로, 머신 러닝 및 머신 추론의 기능을 활용하여 네트워크 구축에 특화된 정확한 통찰력을 제공함으로써 신속하게 문제를 해결할 수 있도록 합니다. 네트워크 및 텔레메트리 정보는 Cisco DNA Center에서 익명으로 처리된 다음 암호화된 보안 채널을 통해 Cisco AI Analytics 클라우드 기반 인프라로 전송됩니다. Cisco AI



Analytics 클라우드는 이 이벤트 데이터로 머신 러닝 모델을 실행하고 이슈와 전반적인 통찰력을 Cisco DNA Center로 다시 가져옵니다. 클라우드에 대한 모든 연결은 TCP/443에서 아웃바운드입니다. 인바운드 연결이 없으며 Cisco AI Cloud는 Cisco DNA Center로 향하는 TCP 흐름을 시작하지 않습니다. 이 문서를 작성할 때 HTTPS 프록시 및/또는 방화벽에서 허용하는 데 사용할 수 있는 FQDN(정규화된 도메인 이름)은 다음과 같습니다.

- <https://api.use1.prd.kairos.ciscolabs.com>(미국 동부 지역)
- <https://api.euc1.prd.kairos.ciscolabs.com>(EU 중부 지역)

구축된 Cisco DNA Center 어플라이언스는 Cisco에서 호스팅하는 인터넷상의 다양한 도메인 이름을 확인하고 연결할 수 있어야 합니다.

다음 단계에 따라 Cisco DNA Center를 Cisco AI 클라우드에 연결합니다.

- Cisco DNA Center 어플라이언스 웹 UI로 이동하여 AI 클라우드 등록을 완료합니다.
- 탐색 System(시스템) > Settings(설정) > External Services(외부 서비스) > Cisco AI Analytics
- Configure(구성)를 클릭하고 Endpoint Smart Grouping and AI spoof detection(엔드포인트 스마트 그룹화 및 AI 스푸핑 탐지) 옵션을 활성화합니다.
- 엔드포인트 스마트 그룹화에서는 AI/ML 클라우드를 사용하여 알 수 없는 엔드포인트를 클러스터링하여 관리자가 해당 엔드포인트에 레이블을 지정할 수 있도록 지원합니다. 이 기능은 네트워크에서 알 수 없는 순 네트워크 수를 줄이는 데 매우 유용합니다.
- AI 스푸핑 탐지는 Cisco가 추가적인 NetFlow/텔레메트리 정보를 수집하고 엔드포인트를 모델링하는 데 도움이 됩니다.
- 구축의 지리적 지역에서 가장 가까운 위치를 선택합니다. 클라우드 연결 확인이 완료되고 연결에 성공하면 녹색 확인란이 표시됩니다.

# Cisco AI Analytics

## AI Network Analytics

AI Network Analytics harnesses machine learning to drive intelligence in the network, empowering administrators to effectively improve network performance and accelerate issue resolution. AI Network Analytics eliminates noise and false positives significantly by learning the network behavior and adapting to your network environment.

## AI Endpoint Analytics

Provides fine-grained endpoint identification and assigns labels to a variety of Endpoints.

### ENDPOINT SMART GROUPING

Using AI and Machine Learning, Endpoint Smart Grouping reduces the number of unknown endpoints in the network by providing AI based endpoint groupings, automated custom profiling rules and crowdsourced endpoint labels.

### AI SPOOFING DETECTION **PREVIEW**

AI Spoofing Detection will detect endpoints being spoofed based on behavioral models. Models are currently being built using collected flow information from devices. If you are interested in this for your network, please enable data collection to help build these behavioral models.

[Configure](#)

[Recover from a config file](#) ⓘ

[AI Network Analytics Privacy Data Sheet](#) ⓘ

## Cisco AI Analytics GUI 구성

- 연결에 실패할 경우, 프록시가 사용 중인 경우 System(시스템) > Settings(설정) > System Configuration(시스템 컨피그레이션) > Proxy config(프록시 컨피그레이션) 페이지에서 Cisco DNA Center의 프록시 설정을 확인합니다. 또한 이 통신을 차단하는 방화벽 규칙을 확인하는 것이 좋습니다.

## ENDPOINT SMART GROUPING

Using AI and Machine Learning, Endpoint Smart Grouping reduces the number of unknown endpoints in the network by providing AI based endpoint groupings, automated custom profiling rules and crowdsourced endpoint labels.

Enable Endpoint Smart Grouping

## AI SPOOFING DETECTION PREVIEW

AI Spoofing Detection will detect endpoints being spoofed based on behavioral models. Models are currently being built using collected flow information from devices. If you are interested in this for your network, please enable data collection to help build these behavioral models.

Send data to help Cisco improve the model

Please choose the region you want to store your data, and make sure the cloud is successfully connected.

Where should we securely store your data?

Europe (Germany)

Cloud connection verified

Cisco AI/ML 클라우드 연결 확인

- AI 분석을 활성화하려면 Cisco Universal Cloud 계약에 동의해야 합니다.
- 이제 온보딩이 완료되고 표시된 대로 이를 나타내는 대화 상자가 표시됩니다.



## Success

You have successfully onboarded AI Analytics! You are about to download the configuration file that enables AI Analytics. This contains the key used for your data in the cloud. Please treat this confidentially and keep this in a secure location. Access to this configuration should be controlled.

Okay

등록 후 성공 대화 상자

## NBAR(Network Based Application Recognition) 클라우드

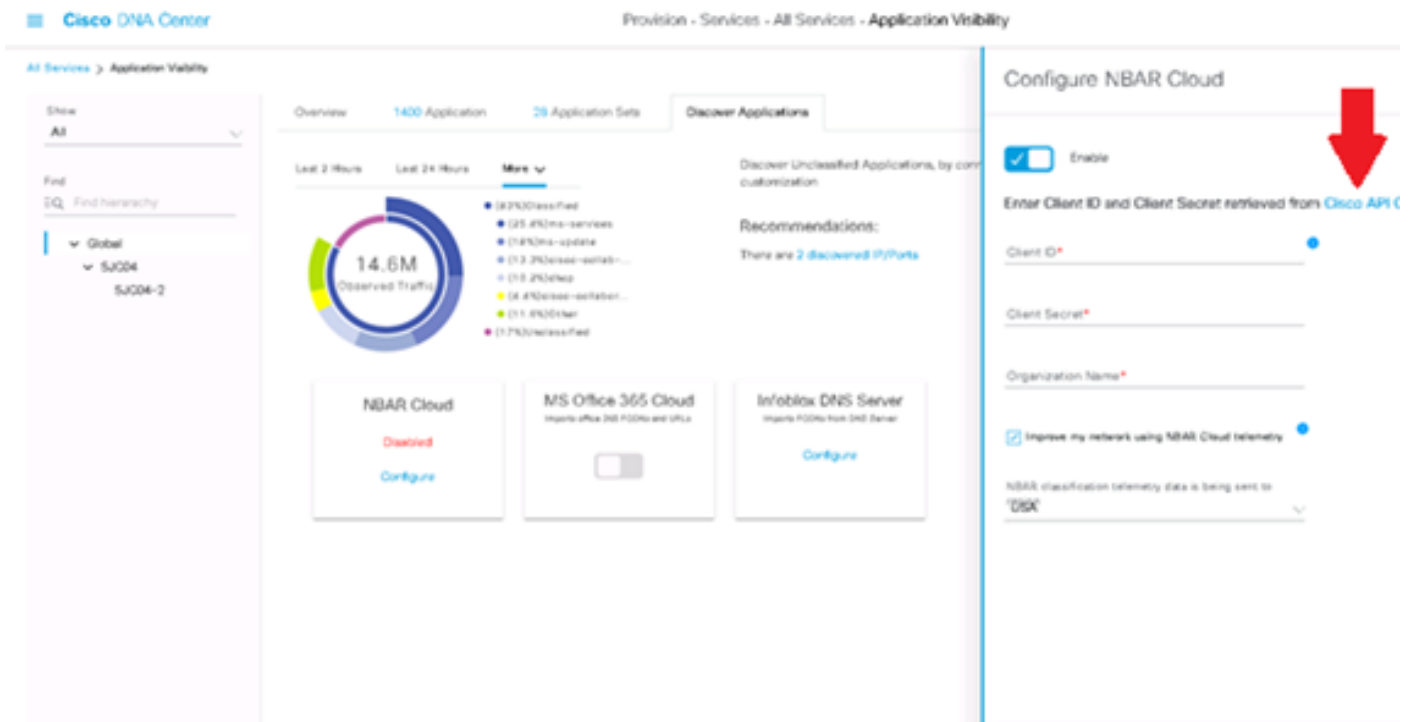
Telemetry Appliance 및 Catalyst 9000 플랫폼은 패킷 흐름의 심층적인 패킷 검사를 사용하여 엔드

포인트 메타데이터를 수집하고 NBAR(Network Based Application Recognition)를 적용하여 네트워크에서 어떤 프로토콜과 애플리케이션이 사용되고 있는지 확인합니다. Cisco DNA Center에는 업데이트 가능한 NBAR 프로토콜 팩이 내장되어 있습니다. 추가 분석 및 알 수 없는 프로토콜 시그니처 탐지를 위해 텔레메트리 데이터를 Cisco NBAR 클라우드로 전송할 수 있습니다. 이를 위해서는 Cisco DNA Center 어플라이언스를 클라우드에 연결해야 합니다. NBAR(Network-Based Application Recognition)는 Cisco에서 개발한 고급 애플리케이션 인식 엔진으로, 여러 가지 분류 기술을 활용하며 분류 규칙을 손쉽게 업데이트할 수 있습니다.

Cisco NBAR Cloud에 Cisco DNA Center를 연결하는 절차는 다음과 같습니다.

- Cisco DNA Center UI에서 Provision(프로비저닝) > Services(서비스) > Application Visibility(애플리케이션 가시성)로 이동합니다. NBAR Cloud(NBAR 클라우드)에서 Configure(구성)를 클릭하면 패널이 열립니다. 서비스를 활성화합니다.
- 클라이언트 ID, 클라이언트 암호 및 조직 이름이 있는 경우, 조직 및 용도에 따라 고유한 이름을 부여하십시오.
- 현재 사용 가능한 유일한 NBAR 클라우드 리전을 작성하는 시점에는 미국에 있으며, 향후 더 많은 리전이 제공될 수 있습니다. 구축 환경 설정에서 하나를 선택하고 저장합니다.

클라이언트 ID 및 클라이언트 암호 자격 증명을 가져오려면 "Cisco API Console" 링크를 클릭합니다. 그러면 포털이 열립니다. 적절한 CCO ID로 로그인하고, 새 앱을 만들고, NBAR 클라우드에 해당하는 옵션을 선택하고 양식을 작성합니다. 완료되면 클라이언트 ID와 암호를 받게 됩니다. 아래 그림을 참조하십시오.



클라이언트 ID 및 암호 검색을 위한 Cisco API 링크

이 그림에서는 NBAR 클라우드에 등록하는 데 사용되는 옵션을 보여 줍니다.

### Application Details

Name of your application: \*

Your Org. DNAC NBAR Integration

Application description (optional):

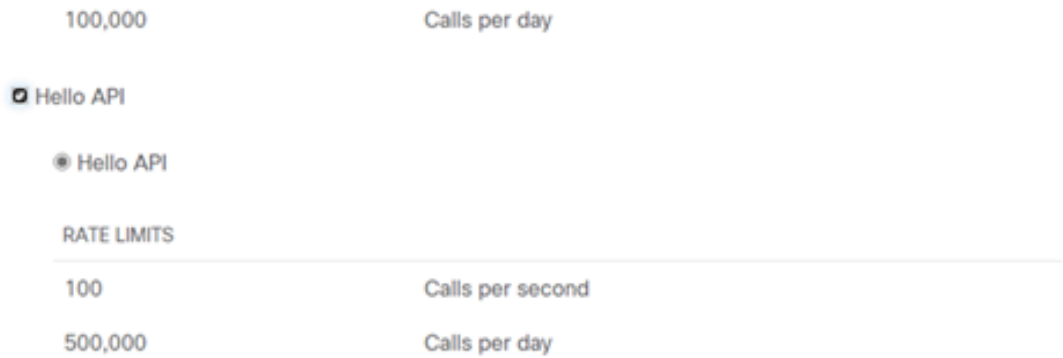
### OAuth2.0 Credentials

Choose at least one Grant Type:

- Resource Owner Credentials    Authorization Code    Client Credentials    Implicit  
 Refresh Token (the grant type you selected allows you to refresh the token)

NBAR 클라우드 앱 세부 정보

- API 요청의 세부 정보를 완료하는 동안 이 이미지를 참조로 사용하십시오.



앱 API 세부 정보

- Cisco 포털에서 가져온 클라이언트 ID 및 암호를 Cisco DNA Center에 입력합니다.

# Configure NBAR Cloud



Disable

Enter Client ID and Client Secret retrieved from [Cisco API Console](#)

Client ID\*

Your Client ID



Client Secret\*

.....

SHOW

Organization Name\*

Your Org Name



Improve my network using NBAR Cloud telemetry



NBAR classification telemetry data is being sent to region

Asia



DNAC에서 클라이언트 ID 및 암호 구성

## CBAR(컨트롤러 기반 애플리케이션 인식) 및 SD-AVC

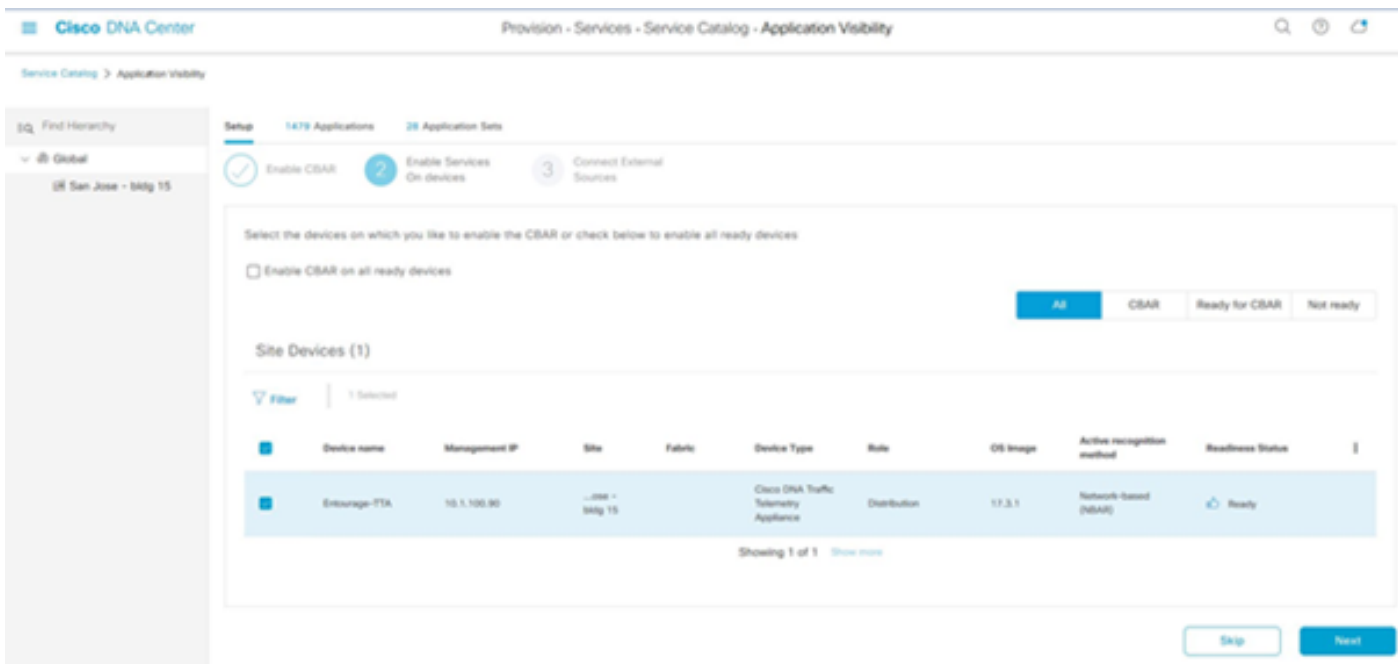
CBAR는 수천 개의 네트워크 애플리케이션, 자체 개발 애플리케이션 및 일반적인 네트워크 트래픽을 분류하는 데 사용됩니다. Cisco DNA Center에서는 네트워크 인프라에서 사용되는 애플리케이션에 대해 동적으로 알아볼 수 있습니다. CBAR는 새로운 애플리케이션의 네트워크 프레즌스가 계속 증가하고 프로토콜 팩에 대한 업데이트가 가능해짐에 따라 이를 식별하여 네트워크를 최신 상태로 유지하도록 지원합니다. 애플리케이션 가시성이 오래된 프로토콜 팩을 통해 엔드 투 엔드로 손실되는 경우 잘못된 분류 및 후속 전달이 발생할 수 있습니다. 이로 인해 네트워크 내에 가시성 구멍이 생길 뿐만 아니라 잘못된 큐잉 또는 포워딩 문제가 발생합니다. CBAR는 업데이트된 프로토콜 팩을 네트워크 전체에 푸시할 수 있도록 허용함으로써 이 문제를 해결합니다.

Cisco SD-AVC(Software-Defined AVC)는 Cisco AVC(Application Visibility and Control)의 구성 요소입니다. 네트워크에서 특정 참여 디바이스로 작동하는 중앙 집중식 네트워크 서비스로 작동합니다. SD-AVC는 애플리케이션 데이터의 DPI도 지원합니다. SD-AVC가 제공하는 현재의 기능 및 이점은 다음과 같습니다.

- 네트워크 전반에서 일관성 있는 네트워크 수준 애플리케이션 인식
- 대칭 및 비대칭 라우팅 환경에서 애플리케이션 인식 향상
- 향상된 첫 번째 패킷 인식
- 네트워크 레벨에서의 프로토콜 팩 업데이트
- 보안 브라우저 기반 SD-AVC 대시보드(HTTPS를 통해) - SD-AVC 기능 및 통계 모니터링 및 프로토콜 팩 구성 - 네트워크 전반에서 업데이트

관련 디바이스에 대해 CBAR를 활성화하려면 다음 단계를 수행합니다.

- Cisco DNA Center의 메뉴인 Provision(프로비저닝) > Application Visibility(애플리케이션 가시성)로 이동합니다. 이 Application Visibility(애플리케이션 가시성) 페이지가 처음 열리면 사용자에게 아래에 표시된 컨피그레이션 마법사가 표시됩니다.
- 각 사이트에 대해 Cisco DNA Center에서 디바이스를 검색한 후 CBAR를 활성화할 디바이스를 선택하고 다음 단계로 진행합니다.



디바이스에서 CBAR 활성화

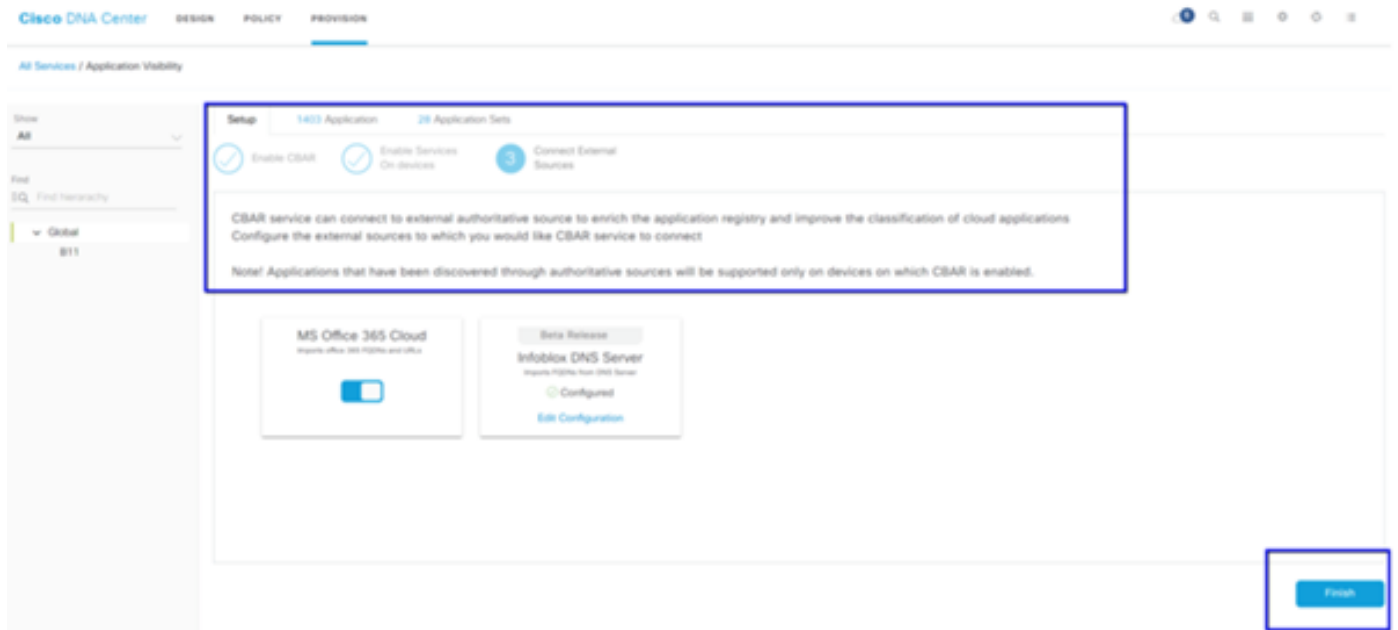
### Microsoft Office 365 Cloud Connector(가 없어야 함)

Cisco DNA Center는 Microsoft RSS 피드와 직접 통합되어 Office 365의 애플리케이션 인식이 게시된 지침에 부합하도록 할 수 있습니다. 이러한 통합을 Cisco DNA Center의 Microsoft Office 365 Cloud Connector라고 합니다. 사용자가 네트워크에서 Microsoft Office 365 응용 프로그램을 실행 중인 경우 이 응용 프로그램을 배포하는 것이 좋습니다. Microsoft Office 365와의 통합은 필수 사항이 아니며, 이 기능이 활성화되어 있지 않으면 Microsoft Office 365 호스트 데이터를 처리하고 분류하는 Cisco DNA Center의 기능에만 영향을 줍니다. Cisco DNA Center에는 이미 Microsoft Office 365 애플리케이션 인식 기능이 내장되어 있지만 애플리케이션 공급업체와 직접 통합하면 Cisco

DNA Center에서 Microsoft Office 365 제품군에서 사용하는 현재 지적 재산 블록 및 URL에 대한 정확한 정보를 업데이트하고 확인할 수 있습니다.

Cisco DNA Center를 Microsoft Office 365 Cloud와 통합하려면 다음 단계를 수행합니다.

- Menu(메뉴) 아이콘을 클릭하고 Provision(프로비저닝) > Services(서비스) > Application Visibility(애플리케이션 가시성)를 선택합니다
- Discover Applications(애플리케이션 검색)를 클릭합니다.
- MS Office 365 Cloud(MS Office 365 클라우드) 토글 버튼을 클릭하여 Cisco DNA Center를 Microsoft Office 365 클라우드와 통합합니다.



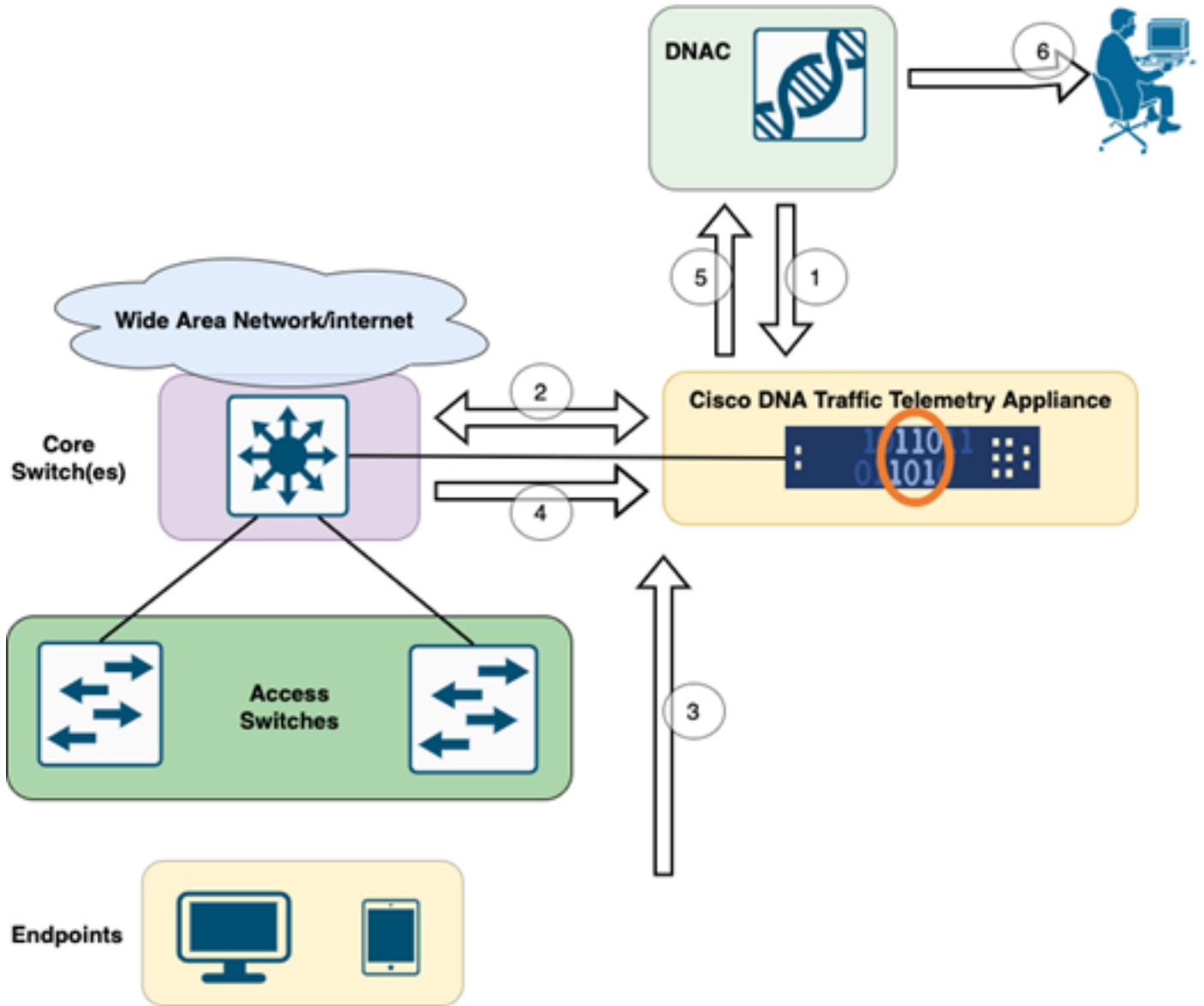
MS O365 클라우드 통합

## TTA 구현

이 섹션에서는 네트워크에서 TTA를 구현하는 데 필요한 단계를 다룹니다.

## TTA 워크플로 개요





TTA - DNAC 워크플로

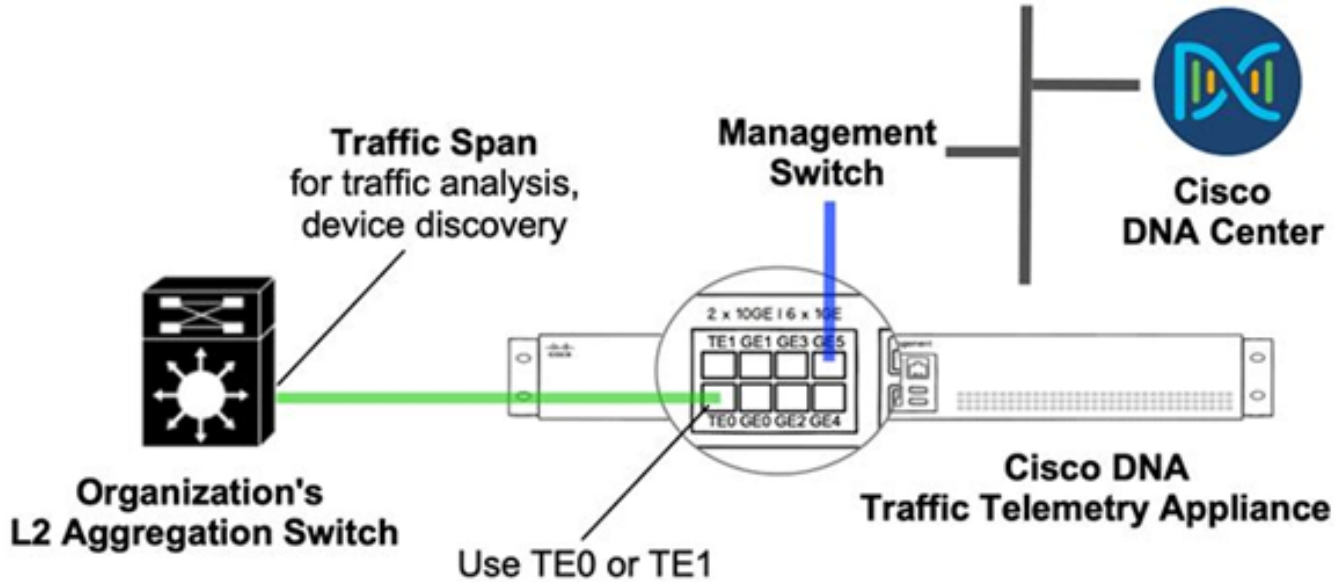
이 다이어그램에서 강조 표시된 단계는 TTA와 Cisco DNA Center 간의 프로세스 및 텔레메트리 흐름을 요약한 것입니다. 여기서 이러한 단계는 더 자세히 설명됩니다.

1. Cisco Traffic Telemetry Appliance는 네트워크 인프라 내의 사이트 어그리게이션 스위치 또는 코어 스위치에 연결됩니다. 이 연결을 통해 어플라이언스는 네트워크의 다양한 액세스 스위치에서 트래픽 데이터를 수신할 수 있습니다.
2. Cisco Traffic Telemetry Appliance는 네트워크 관리 플랫폼 역할을 하는 Cisco DNA Center와 통합됩니다. 이러한 통합으로 어플라이언스와 Cisco DNA Center 간의 원활한 통신 및 데이터 교환이 가능합니다.
3. 사용자 트래픽이 네트워크를 통과하면서 Cisco Traffic Telemetry Appliance에 스펠 또는 미러링됩니다. 즉, 네트워크 트래픽의 복사본이 모니터링 및 분석을 위해 어플라이언스로 전송되는 반면, 원래 트래픽은 정상적인 경로를 계속 유지합니다.
4. Cisco Traffic Telemetry Appliance는 수신된 트래픽 데이터를 수집하고 처리합니다. 또한 미러링된 트래픽에서 패킷 레벨 세부사항, 플로우 통계, 성능 메트릭과 같은 관련 정보를 추출합니다.
5. 처리된 텔레메트리 정보는 Cisco Traffic Telemetry Appliance에서 Cisco DNA Center로 전송됩니다. 이러한 커뮤니케이션을 통해 Cisco DNA Center는 네트워크의 트래픽 패턴, 애플리케이션

이선 성능, 이상 징후에 대한 통찰력과 업데이트를 실시간으로 수신할 수 있습니다.

6. Cisco DNA Center에서 생성된 텔레메트리 인사이트는 네트워크 관리자에게 중요한 정보를 제공합니다. Cisco DNA Center의 인터페이스를 사용하여 수집된 데이터를 보고 분석하고, 네트워크의 상태 및 애플리케이션 성능에 대한 가시성을 확보하고, 잠재적 문제를 식별하고, 네트워크 최적화 및 문제 해결에 대한 정보에 입각한 결정을 내릴 수 있습니다.

## TTA 구축: 하이 레벨 다이어그램



TTA 구축: 하이 레벨

위 다이어그램은 TTA가 네트워크에서 어떻게 연결될 수 있는지를 보여줍니다. 10Gig 및 1Gig 인터페이스는 라인 레이트로 SPAN 수집에 사용할 수 있습니다. Gi0/0/5 인터페이스는 Cisco DNA Center와의 통신, 오케스트레이션, 텔레메트리 정보를 Cisco DNA Center에 전달하는 데 사용됩니다. 이 인터페이스는 SPAN 수집에 사용할 수 없습니다.

## TTA 소프트웨어 및 라이선싱 요구 사항

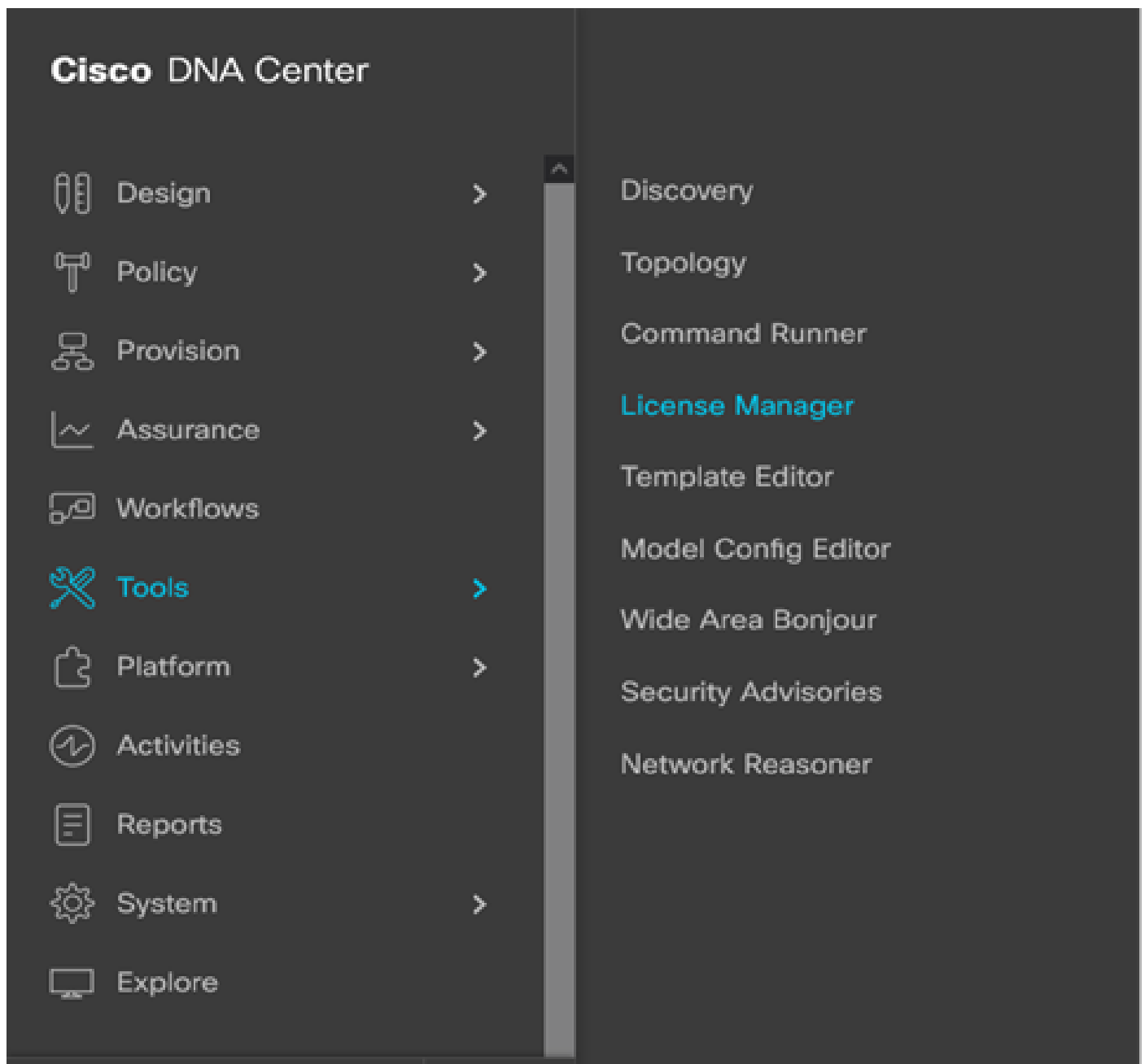
네트워크에 구축된 TTA 어플라이언스는 사용자 데이터 및 사용자 엔드포인트에 대한 텔레메트리 정보를 제공하는 데 매우 중요합니다. 솔루션을 성공적으로 구축하려면 이러한 요구 사항을 충족해야 합니다.

- TTA는 Cisco DNA Center(TTA 부트스트랩 컨피그레이션)에서 검색할 수 있도록 초기 부트스트랩 컨피그레이션으로 구성해야 합니다
- TTA 어플라이언스를 Cisco DNA Center로 온보딩해야 Cisco DNA Center에서 관리할 수 있습니다(Cisco DNA Center 인벤토리에 텔레메트리 상자 추가).
- TTA(TTA 어플라이언스 라이선스)에 올바른 라이선스를 설치해야 합니다.

어플라이언스는 하나의 운영 체제만 지원하며 텔레메트리를 수집하려면 Cisco DNA TTA Advantage 라이선스가 필요합니다. 기능 라이선스(예: IP Base 또는 Advanced IP Services) 또는 영구 라이선스 패키지(예: Network Essentials 또는 Network Advantage)가 필요하지 않습니다.

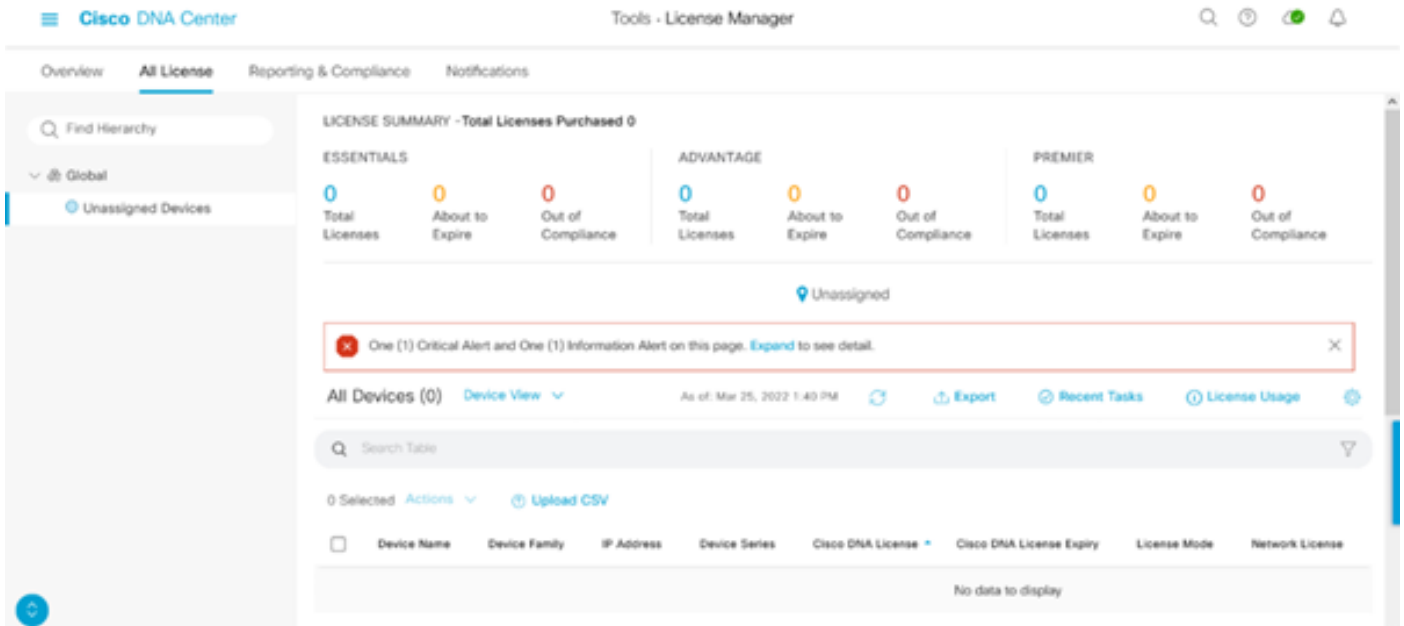
Cisco DNA Center에서 라이선스를 관리하려면 Menu(메뉴) 아이콘을 클릭하여 Cisco DNA

Center의 드롭다운 메뉴에서 Tools(툴) > License Manager(라이선스 관리자)로 이동하여 라이선스 관리자로 이동합니다



DNAC의 라이선스 관리자

- All License(모든 라이선스) 페이지로 이동합니다. 이 이미지와 비슷합니다. 이 페이지에서 관리자는 TTA와 같은 네트워크 디바이스 라이선스를 관리할 수 있습니다.



DNAC의 모든 라이선스 페이지

## TTA 온보딩 및 Day-0 컨피그레이션

Cisco DNA Center에서 TTA 어플라이언스를 쉽게 검색하고 온보딩할 수 있도록 사이트의 TTA 어플라이언스에 구성해야 하는 부트스트랩 명령이 있습니다. 부트스트랩 컨피그레이션이 구축되면 Cisco DNA Center 대시보드에서 TTA를 검색할 수 있습니다. 다음은 TTA 어플라이언스에 대한 day-0 컨피그레이션 항목입니다. 디바이스가 사이트 계층에 온보딩되면 TTA 어플라이언스는 Cisco DNA Center에서 나머지 컨피그레이션 항목을 상속합니다.

```
hostname TTA
interface GigabitEthernet0/0/5
description ***** Management Interface *****
ip address x.x.x.x <SUBNET MASK>
negotiation auto
cdp enable

ip route 0.0.0.0 0.0.0.0 x.x.x.y
username dna privilege 15 algorithm-type scrypt secret
.
.
.
enable secret
.
.
.
service password-encryption
ip domain name <domain name>
ip ssh version 2
line vty 0 15
login local
transport input ssh
transport preferred none
ip ssh source-interface GigabitEthernet0/0/5
```

```

aaa new-model
aaa authentication login default local
aaa authorization exec default local

**SNMPv2c or SNMPv3 paramters as applicable**
snmp-server community <string> RO
snmp-server community <string> RW

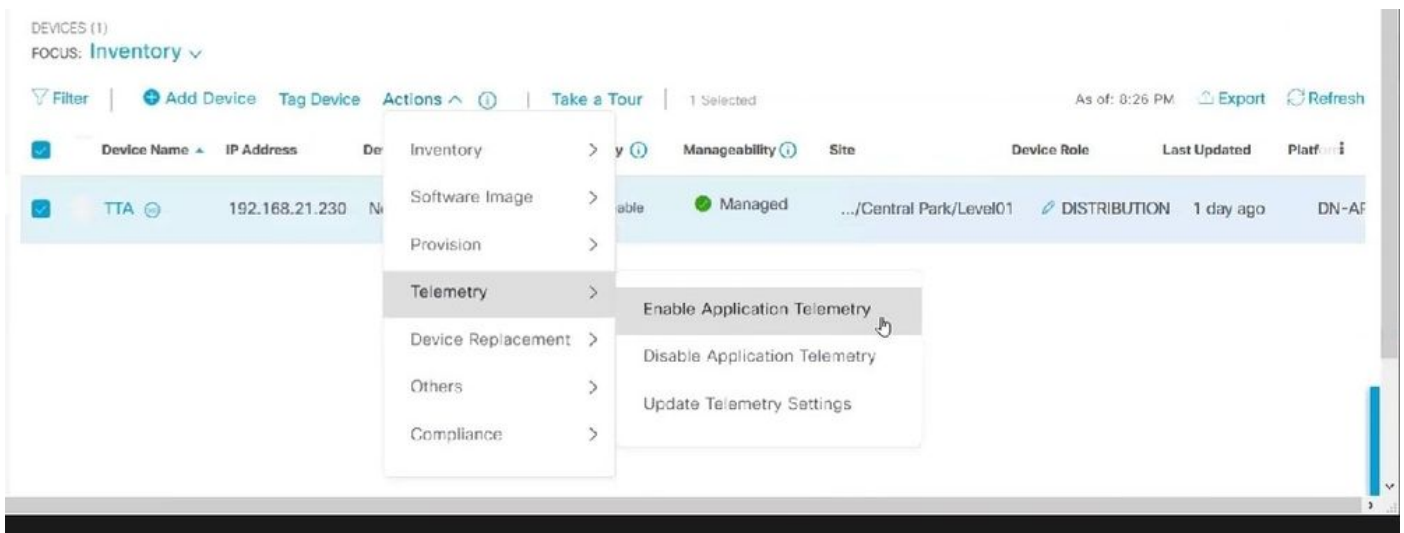
```

이러한 항목이 TTA에 구성되면 Cisco DNA Center에서 검색할 수 있습니다.

## Cisco DNA Center 인벤토리에 TTA 어플라이언스 추가

TTA를 활용하려면 Cisco DNA Center에서 TTA 어플라이언스를 검색하고 관리해야 합니다. TTA가 Cisco DNA Center에 온보딩되면 Cisco DNA Center에서 관리할 수 있습니다. TTA 어플라이언스를 발견하기 전에 사이트에 대한 전체 사이트 계층 구조가 있는지 확인해야 합니다. 그런 다음 Menu(메뉴) > Provision(프로비저닝) > Devices(디바이스) > Inventory(인벤토리) 페이지의 다음 단계에 따라 특정 사이트 계층에 TTA 어플라이언스를 추가하여 디바이스를 사이트에 추가합니다.

1. 디바이스에 연결하는 데 필요한 사용자 이름/비밀번호(CLI) 및 SNMP 커뮤니티 및 enable 비밀번호를 제공합니다. 디바이스가 성공적으로 추가될 때까지 기다렸다가 계속합니다.
2. 디바이스 이름, 제품군(TTA의 경우 네트워크 관리), 연결성 - 연결 가능, 관리 가능, 디바이스 역할 - 배포를 확인합니다. 디바이스는 처음에는 "Non-Compliant"가 되지만, 일단 완전히 프로비저닝되면 상태가 변경됩니다.
3. TTA가 온보딩되면 Cisco DNA Center에서 컨피그레이션 템플릿을 푸시하여 고급 텔레메트리 기능으로 구성합니다.



TTA 검색 및 애플리케이션 텔레메트리 활성화

## SPAN 컨피그레이션

코어 스위치의 하드웨어 기능에 따라 VLAN 그룹 또는 인터페이스를 TTA에 연결된 인터페이스에 SPAN하도록 SPAN 세션을 구성할 수 있습니다. 샘플 컨피그레이션이 여기에 제공됩니다.

```
Switch#configure terminal
Switch(config)#monitor session 1 source vlan|interface rx|tx|both
Switch(config)#monitor session 1 destination interface intx/y/z
```

## 보장 수집됨

설치된 Traffic Telemetry Appliance에서 수집한 보증 데이터에 액세스하려면 Assurance(보증) 섹션으로 이동하여 Health(상태)를 클릭합니다.


# Cisco DNA Center

 Design >

 Policy >

 Provision >

 Assurance >

 Workflows

 Tools >

 Platform >

 Activities

 Reports

 System >

 Explore

## DASHBOARDS

**Health**

Issues & Events

Sensors

Wi-Fi 6

Rogue and aWIPS

PoE

Dashboard Library

## AI NETWORK ANALYTICS

Trends and Insights

Network Heatmap

Peer Comparison

Network Comparison

Baselines

AI-Enhanced RRM

## SETTINGS

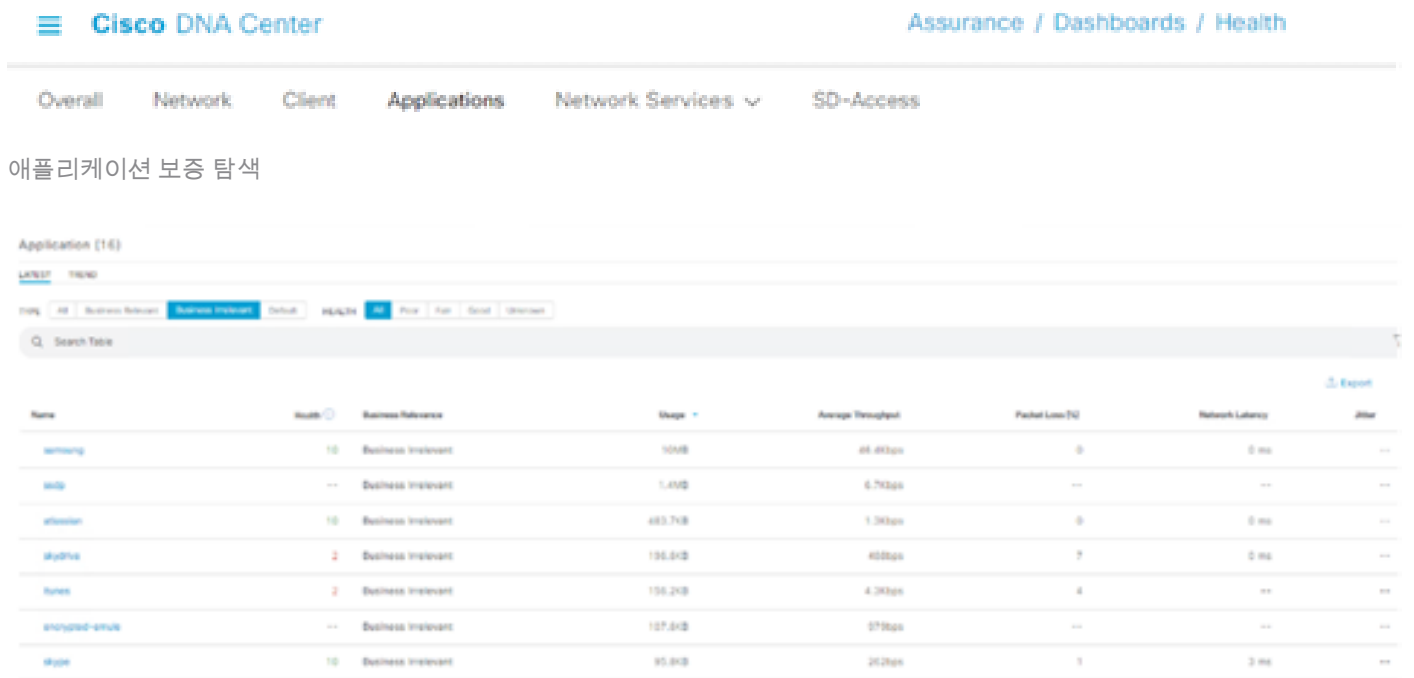
Issue Settings

Health Score Settings

Sensors

Intelligent Capture Settings

Applications(애플리케이션)를 선택하면 특정 애플리케이션 유형에 따라 TTA에서 캡처한 지연 시간 및 지터를 비롯한 애플리케이션 데이터의 포괄적인 개요를 확인할 수 있습니다.



자세한 애플리케이션 보증 UI

보다 자세한 분석을 위해 사용자는 특정 애플리케이션을 클릭하고 Traffic Telemetry Appliance로 내보내기(Exporter)를 선택하여 개별 애플리케이션을 탐색하고 사용량, 처리량, 패킷 손실 데이터, 클라이언트 네트워크 레이턴시, 서버 네트워크 레이턴시, 애플리케이션 서버 레이턴시 등의 특정 메트릭을 조사할 수 있습니다.



예: 애플리케이션 세부 사항 Pt.1





예: 애플리케이션 세부 사항 Pt.2

## 다음을 확인합니다.

1. CBAR를 활성화한 후 Cisco Traffic Telemetry Appliance에 로그인하고 이 CLI 명령을 실행하여 디바이스에서 SD-AVC(Application Visibility Control) 서비스가 활성화되었는지 확인합니다. 출력은 컨트롤러의 IP 주소와 연결된 상태를 나타내는 이 샘플과 유사합니다.

```
Cisco-TTA#sh avc sd-service info summary
Status: CONNECTED
Device ID: Cisco-TTA
Device segment name: AppRecognition
Device address: <TTA IP Address>
Device OS version: 17.03.01
Device type: DN-APL-TTA-M
Active controller:
Type : Primary
IP : <Cisco DNA Center IP Address>
Status: Connected
Version : 4.0.0
```

2. TTA CLI에서 "show license summary" 명령을 사용하여 관련 디바이스 라이선스 세부사항을 확인합니다.

```
Device# show license summary
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - SPECIFIC LICENSE RESERVATION
  Export-Controlled Functionality: ALLOWED

License Authorization:
  Status: AUTHORIZED - RESERVED
```

License Usage:

License	Entitlement tag	Count	Status
-----			
Cisco_DNA_TTA_Advantage	(DNA_TTA_A)	1	AUTHORIZED

3. SPAN 세션이 코어/어그리게이션 스위치에 올바르게 구성되었는지 확인합니다.

```
AGG_SWITCH#show monitor session 1
Session 1
-----
Type : Local Session
Source VLANs : 300-320
RX Only :
Destination Ports : TenGigx/y/z
Encapsulation : Native
Ingress : Disabled
```

4. TTA가 성공적으로 프로비저닝되면 이러한 명령이 디바이스로 푸시됩니다(또는 푸시되었습니다).

```
avc sd-service
segment AppRecognition
controller
address <Cisco DNA Center IP Address>
.....
!
flow exporter <Cisco DNA Center IP Address>
destination <Cisco DNA Center IP Address>
!
crypto pki trustpoint DNAC-CA
.....
!
performance monitor context tesseract profile application-assurance
exporter destination <Cisco DNA Center IP Address> source GigabitEthernet0/0/5 transport udp port 6007
.....
!
All interfaces must have
ip nbar protocol-discovery
performance monitor context tesseract
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.