Utilize the Traffic Telemetry Appliance (TTA) and Cisco DNA Center App Assurance: the why and the how

Contents

Introduction

This document describes the **Cisco DNA Traffic Telemetry Appliance (Cisco part number DN-APL-TTA-M)** platform along with how to enable **Application Assurance in Cisco DNA Center**. It also sheds some light on how and where the TTA can be positioned in a network along with the configuration and verification process. This article also addresses the various prerequisites involved.

Prerequisites

Cisco recommends that you have knowledge of how Cisco DNA Center Assurance and Application Experience each work.

Application Assurance

Assurance is a multipurpose, real-time, network data collection and analytics engine that can significantly increases the business potential of network data. Assurance processes complex application data and presents the findings in Assurance health dashboards to provide insight into the performance of applications used in the network. Depending on where the data is collected from you can see some or all of the following:

- Application Name
- Throughput
- DSCP Markings
- Performance Metrics (Latency, Jitter, and Packet Loss)

Based on the amount of data collected Application Assurance can be categorized into two models:

- **Application Visibility (AppVis)** and
- **Application Experience (AppX)**

Application Name and **Throughput** are collectively referred to as **quantitative metrics**. Data for the quantitative metrics comes from enabling Application Visibility.

DSCP Markings and **Performance Metrics (Latency, Jitter, and Packet Loss)** are collectively referred to as **qualitative metrics.** Data for the qualitative metrics comes from enabling Application Experience.

Application Visibility (AppVis)

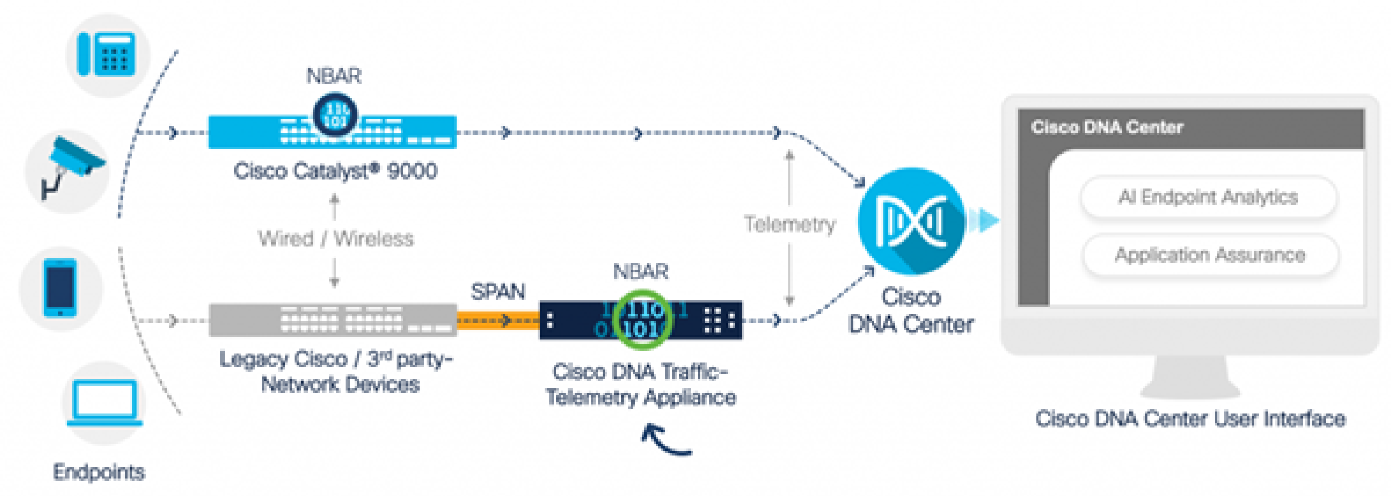
Application Visibility data is collected from switches running Cisco IOS® XE, and from wireless controllers running AireOS. For switches running Cisco IOS XE, Application Visibility data is collected using a predefined NBAR template that is applied bidirectionally (ingress and egress) to the physical layer access switch ports. For wireless controllers running AireOS, Application Visibility data is collected at the wireless controller, and then streaming telemetry is used to transport this data to Cisco DNA Center.

Application Experience (AppX)

Application Experience data is collected from Cisco IOS XE router platforms, specifically using the Cisco Performance Monitor (PerfMon) feature and the Cisco Application Response Time (ART) metrics. Examples of router platforms include the ASR 1000, ISR 4000, and CSR 1000v. For device compatibility with Cisco DNA Center, see the Cisco DNA Center Compatibility Matrix.

Why a Traffic Telemetry Appliance?

The Cisco Catalyst 9000 series wired and wireless devices conduct deep packet inspection (DPI) and provide data streams for services such as the Cisco AI Endpoint Analytics and Application Assurance in Cisco DNA Center. But what if there are no Catalyst 9000 series devices in the network to extract telemetry from? Several organizations still have a portion of their network infrastructure that has not been migrated to the Cisco Catalyst 9000 series platforms. The Catalyst 9000 platform generates AppVis telemetry, but to get additional AppX insights the Cisco DNA Traffic Telemetry Appliance can be used to bridge the gap. The goal of the TTA is to monitor the traffic that it receives via SPAN ports from other network devices that do not have the capability of providing Application Experience data to Cisco DNA Center. Since the legacy infrastructure devices cannot perform the deep packet inspection required for advanced analytics the Cisco DNA Traffic Telemetry Appliance can be used to generate AppX telemetry from existing legacy deployments.



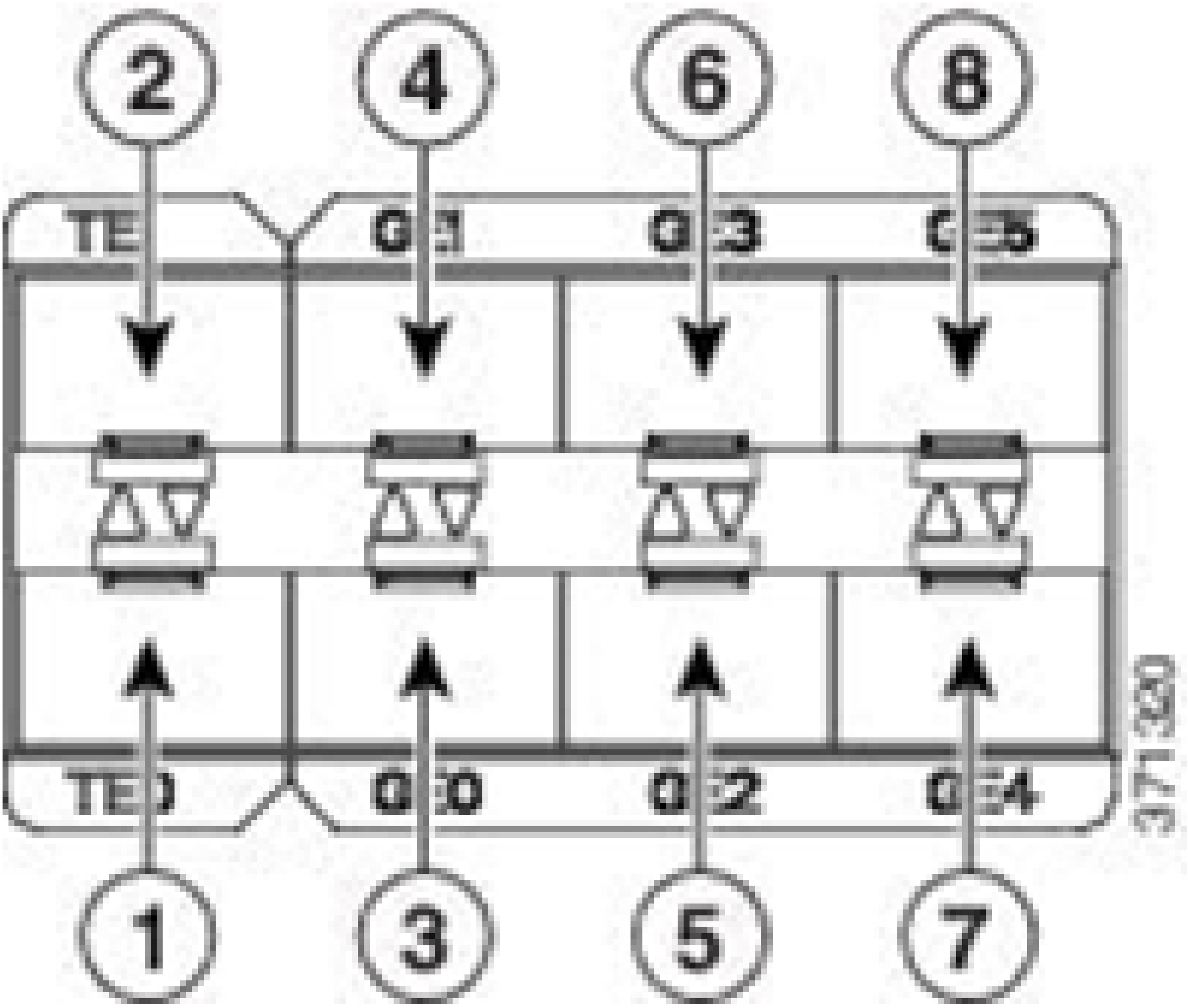
Cisco TTA in Action

TTA Device Details

The Cisco IOS XE-based telemetry sensor platform generates telemetry from mirrored IP network traffic from **Switched Port Analyzer (SPAN)** sessions of switches and wireless controllers. The appliance inspects thousands of protocols using the **Network-Based Application Recognition (NBAR)** technology to produce a telemetry stream for Cisco DNA Center to perform analytics. The Cisco DNA Traffic Telemetry Appliance can handle 20-Gbps of sustained throughput traffic and inspect 40,000 endpoint sessions for device profiling.

The Cisco Traffic Telemetry Appliance

The TTA has a mix of 10-Gig and 1-Gig links which are used for SPAN ingestion. Out of these ports Gig0/0/5 is the only port that can be configured with an IP address and can be used for communicating with Cisco DNA Center. The interface matrix is shown below.



TTA Interface Matrix

TTA Interface Matrix			
1	10 GE SFP+ Port 0/0/0	5	GE SFP Port 0/0/2
2	10 GE SFP+ Port 0/0/1	6	GE SFP Port 0/0/3
3	GE SFP Port 0/0/0	7	GE SFP Port 0/0/4
4	GE SFP Port 0/0/1	8	GE SFP Port 0/0/5

Cisco DNA Center Prerequisites for Assurance

This section highlights the configurations and prerequisites that need to be met before Cisco DNA Center can process telemetry.

Operational Cisco DNA Center Cluster

The Cisco DNA Center cluster used to manage the TTA and process telemetry must be provisioned with these criteria:

- **Network Hierarchy:** The Network Hierarchy section within the Design workflow is used to define different site campuses, buildings within those campuses, and the individual floors within those buildings and display them on a world map. The appropriate site/network hierarchy must be configured.
- **Network Settings:** The Network Settings section allows the creation of common default network settings that will be used by the devices within the network. These settings can be applied in a global manner as well as on a per-site, building, or floor level. Input DNS, domain name, syslog, NTP, timezone, and login banner information as required by the deployment.
- **Device Credentials:** These credentials will be used to access and discover devices in the network including the TTA. It is required that Cisco DNA Center be configured with the appropriate CLI, and SNMP credentials. Along with this NetConf credentials are good to have.
- **Cisco CCO Account:** A valid CCO account is required to tether the appliance and leverage the capabilities of the Cisco AI Cloud, download images for SWIM and download protocol packs for TTA and other devices.

ISE and Cisco DNA Center Integration

Cisco Identity Services Engine (ISE) and Cisco DNA Center can be integrated for identity and policy automation. ISE is also used to gather information about the endpoints to leverage Cisco AI Endpoint Analytics. PxGrid is used to implement the integration between ISE and Cisco DNA Center.

Cisco DNA Center and ISE integration requirements follow:

- pxGrid service must be enabled on ISE.
- ERS Read/Write access must be enabled.
- The ISE admin certificate must contain ISE's IP address or FQDN in either the subject name or the SAN field.
- The Cisco DNA Center system certificate must contain all of Cisco DNA Center's IP addresses or FQDNs in either the subject name or the SAN field.
- ISE ERS Admin credentials will be used for trust establishment of ERS communication between ISE and Cisco DNA Center.
- The pxGrid node must be reachable from Cisco DNA Center.

Cisco DNA Center Requirements for Telemetry

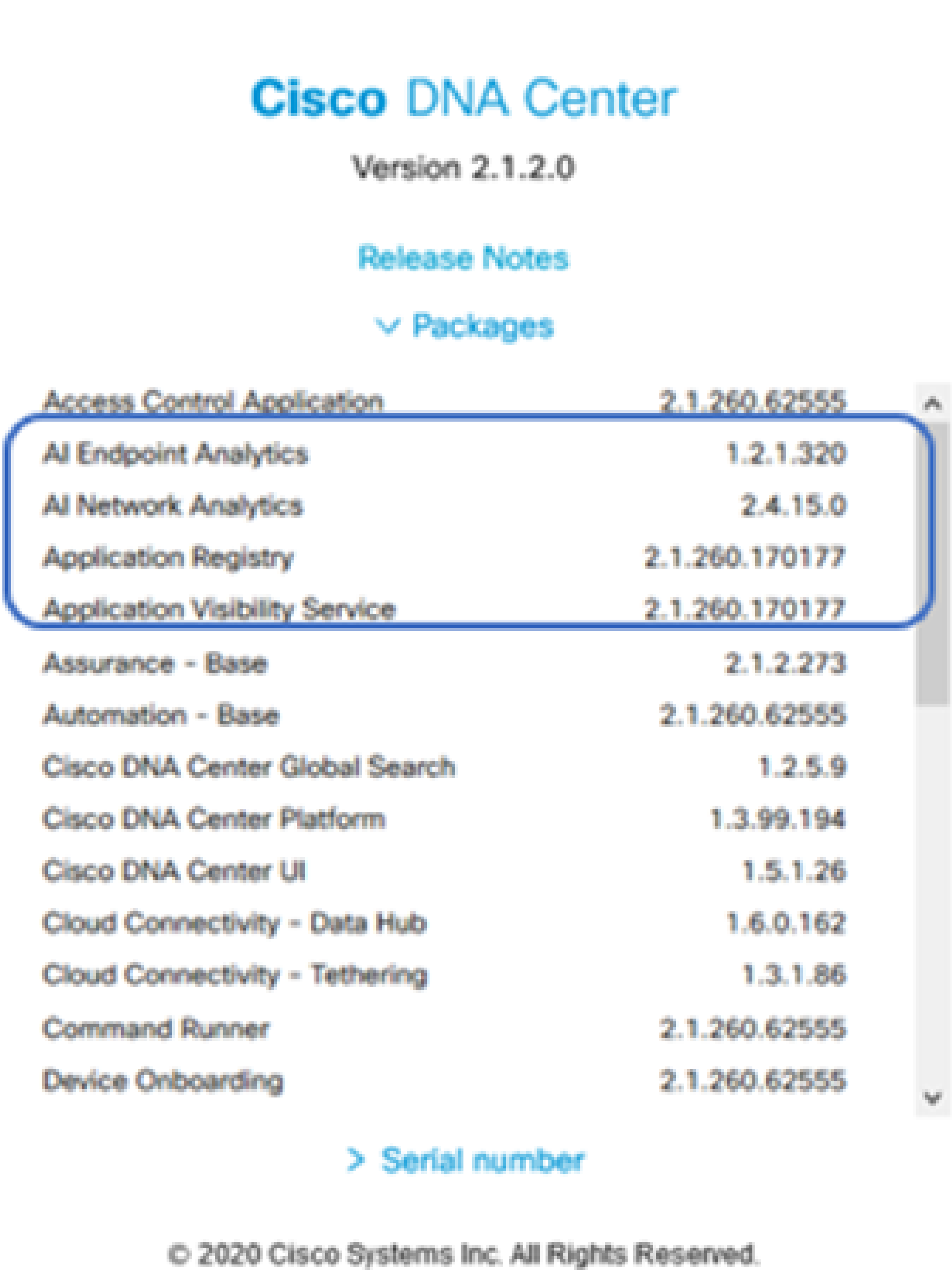
There are requirements that must be implemented to enable Application Assurance in Cisco DNA Center. These requirements are explained in detail in the sections that follow.

Cisco DNA Center key packages

Cisco DNA Center requires these three packages to be installed in order to enable and analyze telemetry data.

- AI Endpoint Analytics
- AI Network Analytics

- Application Visibility Services



Cisco DNA Center

Version 2.1.2.0

Release Notes

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

© 2020 Cisco Systems Inc. All Rights Reserved.

Cisco DNA Center Packages Required

A quick way to access this info is to click on the **"About"** link under the **question mark** icon on the upper right corner of Cisco DNA Center's main page. If these applications are missing they need to be installed before proceeding with telemetry setup. Use this guide to install these packages in Cisco DNA Center from the Cisco cloud. Cisco DNA Center Upgrade Guide

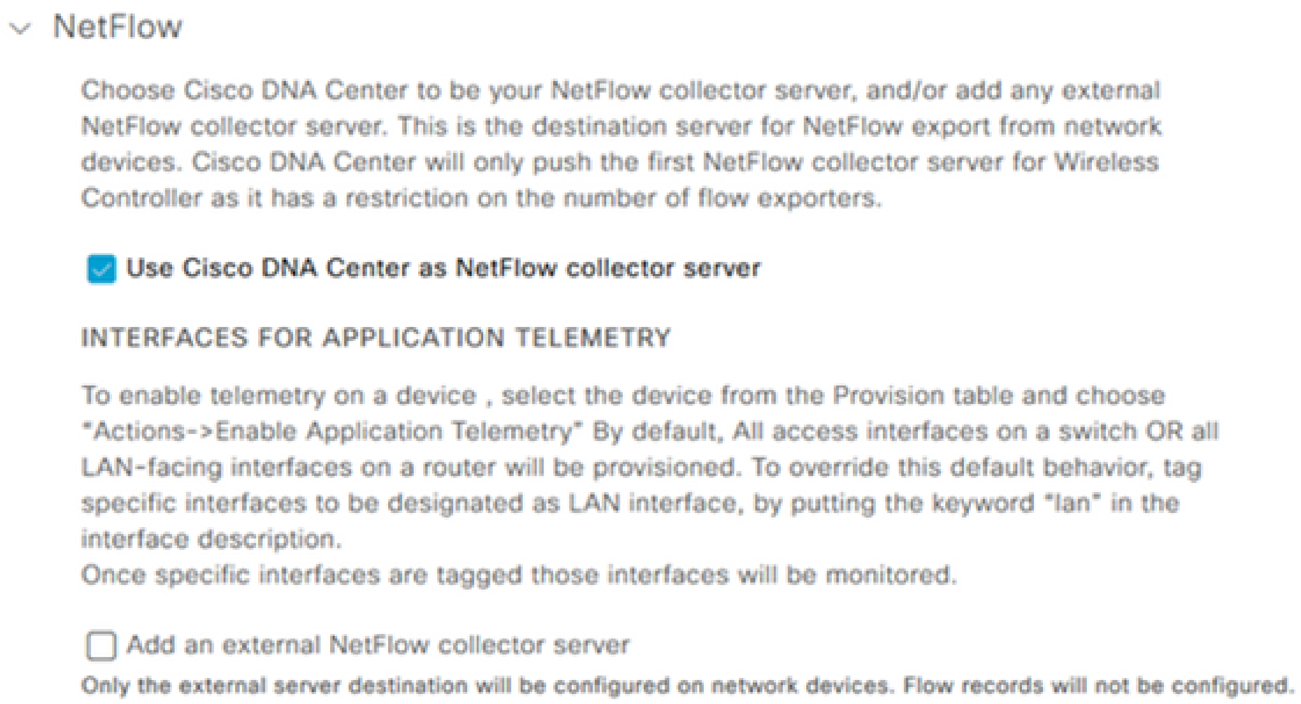
Cisco DNA Center as the Telemetry Collector

NetFlow data export is the technology transport that provides the telemetry data that will be forwarded to Cisco DNA Center for in depth analysis. To enable data collection for machine learning and reasoning for endpoint analytics NetFlow needs to be exported to Cisco DNA Center. The TTA is a telemetry sensor platform that is used to generate telemetry from mirrored IP network traffic and share it with Cisco DNA Center for application and endpoint visibility.

- Network traffic is received from switches and routers via Switched Port Analyzer (SPAN) mirroring and fed into the Cisco DNA Traffic Telemetry Appliance mirroring interfaces.
- The Cisco DNA Traffic Telemetry Appliance analyzes the received traffic to produce a telemetry stream for Cisco DNA Center.

To enable Cisco DNA Center as the telemetry collector complete these steps.

- In Cisco DNA Center, click **Menu** > **Design** > **Network Settings** and enable telemetry for Cisco DNA Center to collect NetFlow.



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 TELEMETRY

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.

Configuring DNAC as a NetFlow Collector

The Cisco AI Cloud

Cisco AI Network Analytics is an application within Cisco DNA Center that leverages the power of machine learning and machine reasoning to provide accurate insights that are specific to your network deployment, which allows you to quickly troubleshoot issues. Network and telemetry information is anonymized in Cisco DNA Center then sent through a secure encrypted channel to the Cisco AI Analytics cloud-based infrastructure. The Cisco AI Analytics cloud runs the machine learning model with this event data and brings the issues and overall insights back to Cisco DNA Center. All connections to the cloud are outbound on TCP/443. There are no inbound connections, the Cisco AI Cloud does not initiate any TCP flows towards Cisco DNA Center. Fully Qualified Domain Names (FQDN) that can be used to allow in the

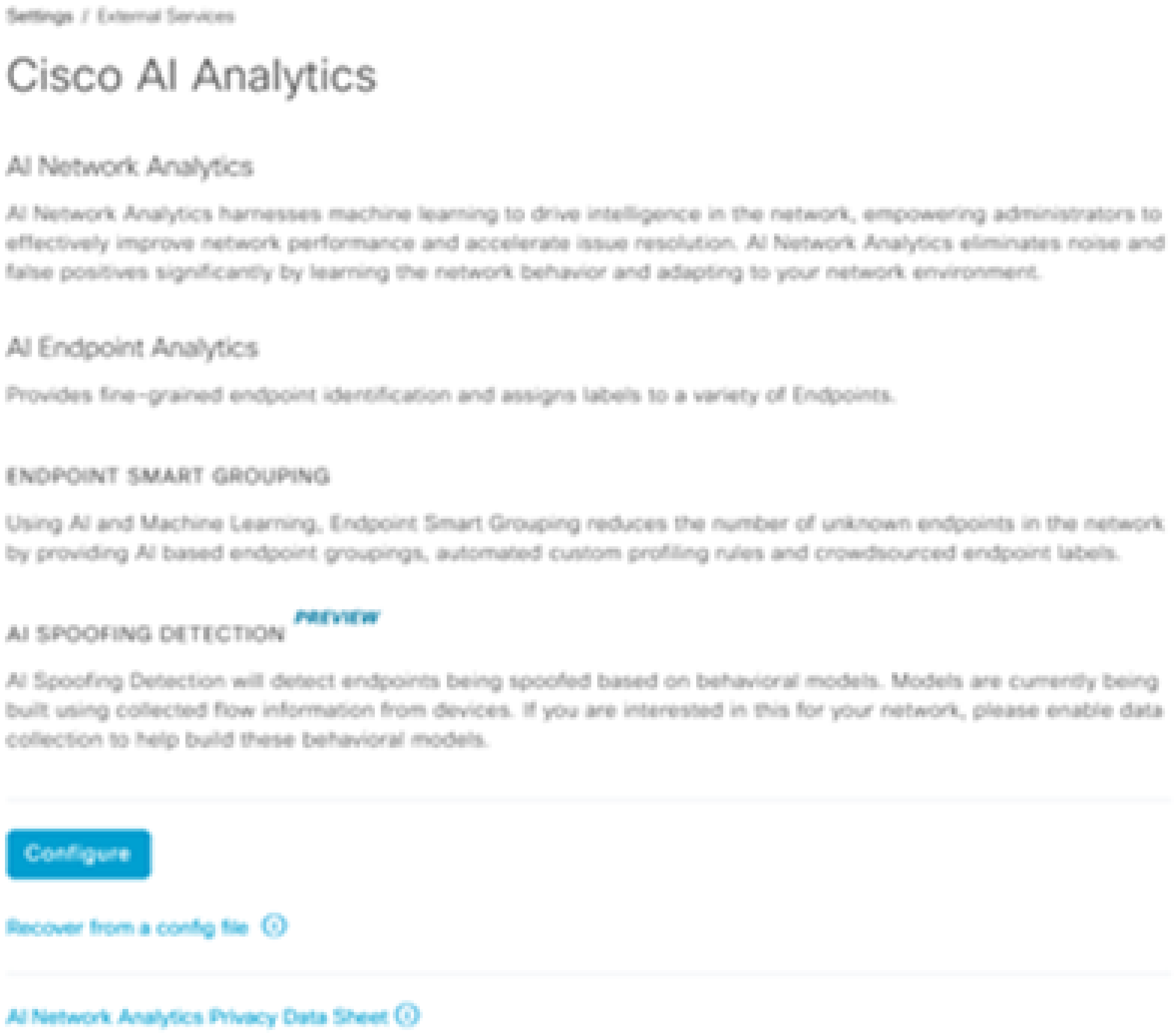
HTTPS proxy and/or firewall at the time of writing this article are:

- https://api.use1.prd.kairos.ciscolabs.com (US East Region)
- https://api.euc1.prd.kairos.ciscolabs.com (EU Central Region)

The deployed Cisco DNA Center appliance must be able to resolve and reach the various domain names on the internet that are hosted by Cisco.

Follow these steps to tether Cisco DNA Center to the Cisco AI Cloud.

- Go to the Cisco DNA Center appliance web UI to complete the AI Cloud registration:
- Navigate to **System > Settings > External Services > Cisco AI Analytics**
- Click on **Configure** and enable the **Endpoint Smart Grouping and AI spoof detection option.**
- Endpoint Smart Grouping uses the AI/ML cloud to cluster unknown endpoints to help admins label those endpoints. This is very useful to reduce the net unknowns in the network.
- AI spoof detection will help Cisco gather additional NetFlow/telemetry information and helps in modelling the endpoint.
- Choose the closest location to the geographic region of the deployment. Once the cloud connection verification is done and the connection is successful, you will see a green checkbox.



Settings / External Services

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.

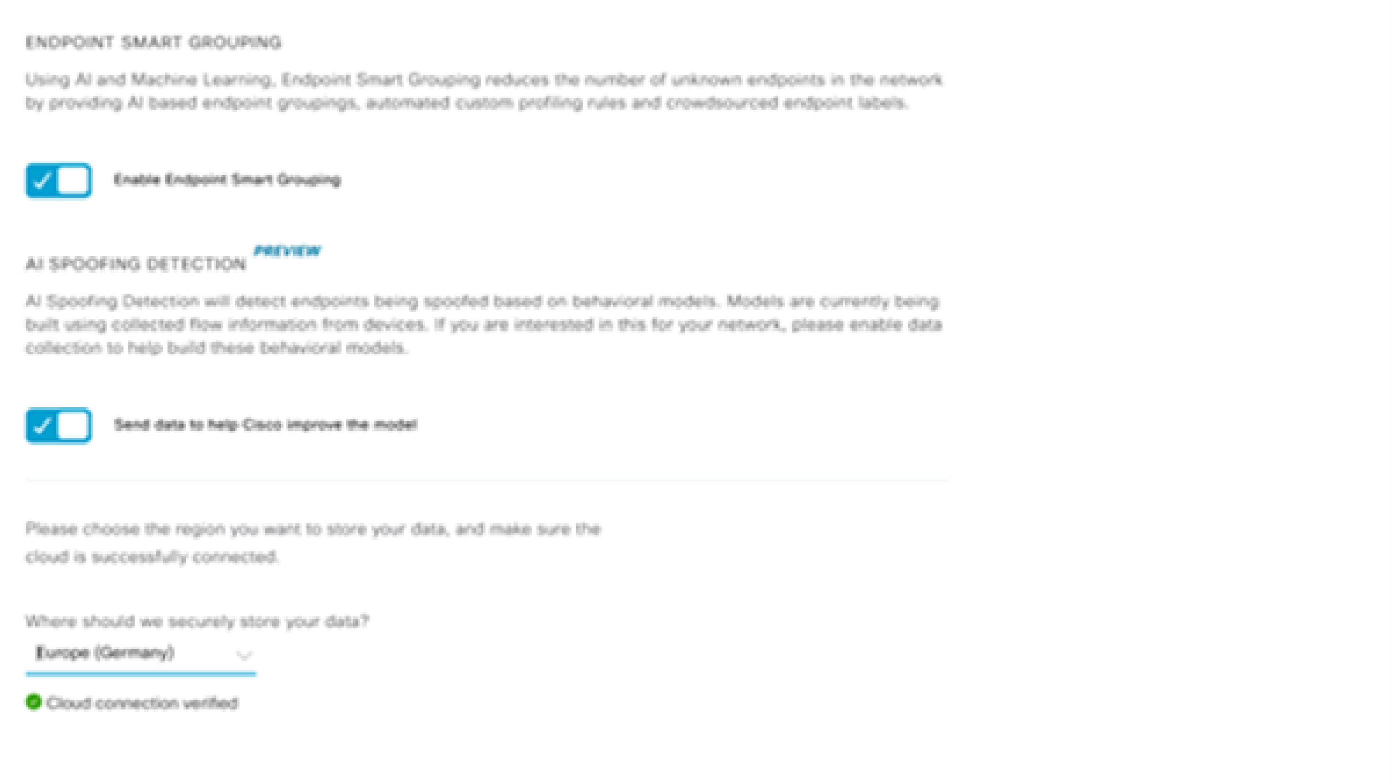
AI SPOOFING DETECTION PREVIEW

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

Configuring Cisco AI Analytics GUI

- If the connection is unsuccessful, check the proxy settings in Cisco DNA Center from the **System** > **Settings > System Configuration > Proxy config page** if a proxy is being used. It is also a good idea to check any firewall rules which might be blocking this communication.



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.

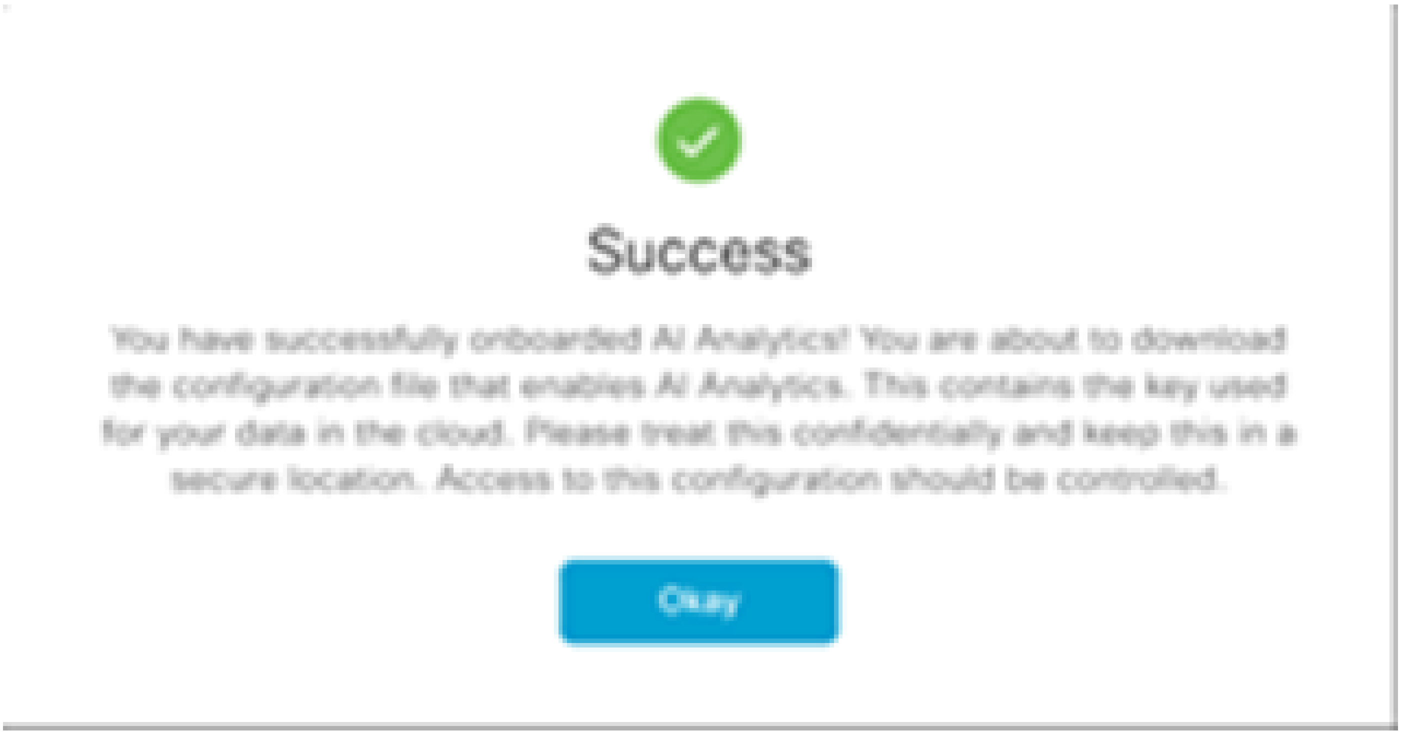
Where should we securely store your data?

Europe (Germany)

● Cloud connection verified

Cisco AI/ML Cloud Connection Verification

- Accept the Cisco Universal Cloud Agreement to enable AI Analytics.
- At this point the onboarding will be complete and a dialog box indicating this will be displayed as shown.



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.

Success Dialog Box Post Enrolment

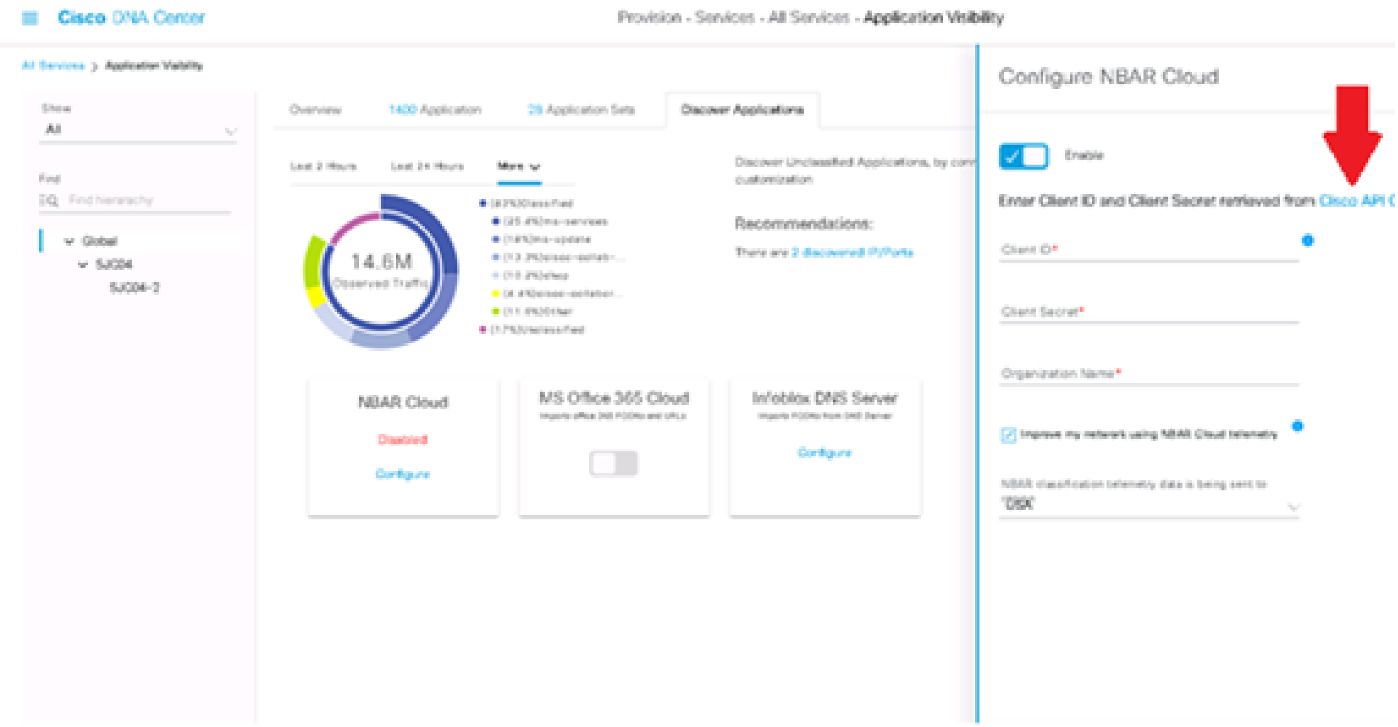
The Network Based Application Recognition (NBAR) Cloud

The Telemetry Appliance and the Catalyst 9000 platform collect endpoint metadata using deep packet inspection of packet flows and applies Network Based Application Recognition (NBAR) to determine what protocols and applications are being utilized in the network. Cisco DNA Center has a built-in NBAR protocol pack that can be updated. The telemetry data can be sent to the Cisco NBAR cloud for additional analysis and for detecting unknown protocol signatures. In order for this to happen, the Cisco DNA Center appliance needs to be tethered to the cloud. Network-Based Application Recognition (NBAR) is an advanced application recognition engine developed by Cisco that utilizes several classification techniques and can easily update its classification rules.

To tether Cisco DNA Center to the Cisco NBAR Cloud complete these steps.

- From the Cisco DNA Center UI, go to **Provision** > **Services** > **Application Visibility**. Click Configure under NBAR Cloud and a panel will open. Enable the service.
- If you have the Client ID, Client Secret and Organization Name, please give them unique names depending on the organization and use.
- At the time of writing the only NBAR Cloud region currently available is in the USA; more regions may become available in the future. Select the one in deployment preferences and save it.

To get the Client ID and Client Secret credentials, click on the “Cisco API Console” link, this opens up a portal. Login with the appropriate CCO id, create a new app, select the options corresponding to NBAR cloud and complete the form. Once completed you will get a client ID and secret. Refer the figure shown below.



Configure NBAR Cloud

Enable

Enter Client ID and Client Secret retrieved from Cisco API C

Client ID*

Client Secret*

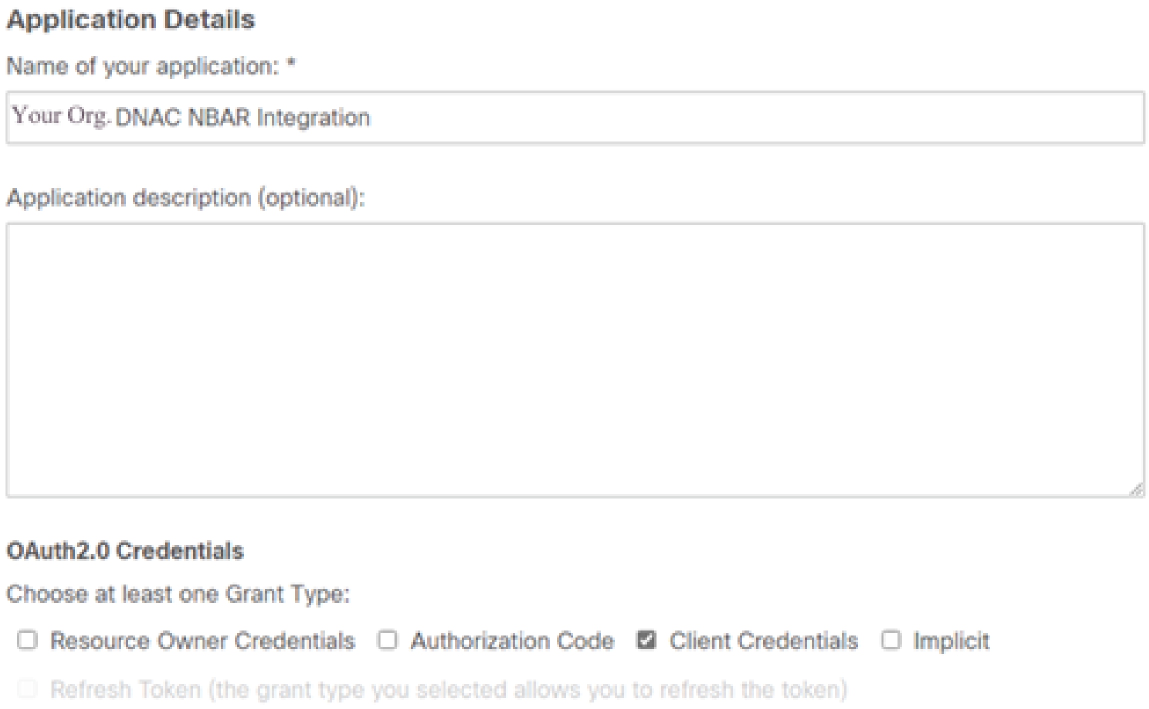
Organization Name*

☑ Improve my network using NBAR Cloud telemetry

NBAR classification telemetry data is being sent to
USA

Cisco API Link to Retrieve Client ID and Secret

These images demonstrate the options that are used for registering to the NBAR cloud.



Application Details

Name of your application: *

Your Org. DNAC NBAR Integration

Application description (optional):

OAuth2.0 Credentials

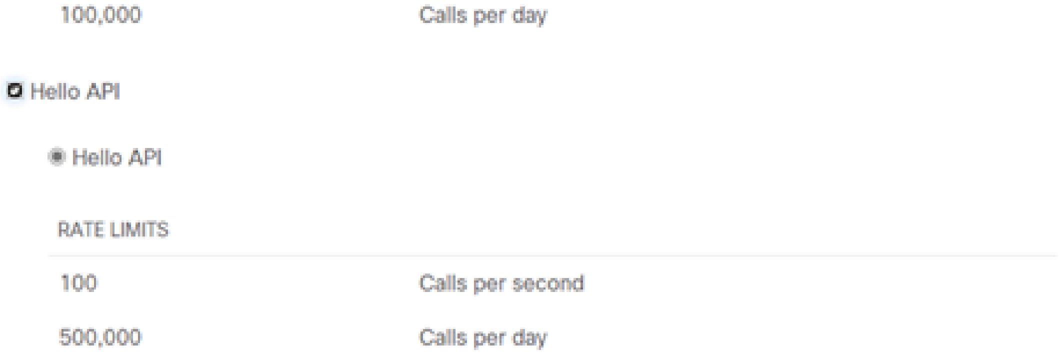
Choose at least one Grant Type:

☐ Resource Owner Credentials ☐ Authorization Code ☑ Client Credentials ☐ Implicit

☐ Refresh Token (the grant type you selected allows you to refresh the token)

NBAR Cloud App Details

- Use this image as a reference while completing the API request's details.



100,000	Calls per day

☑ Hello API

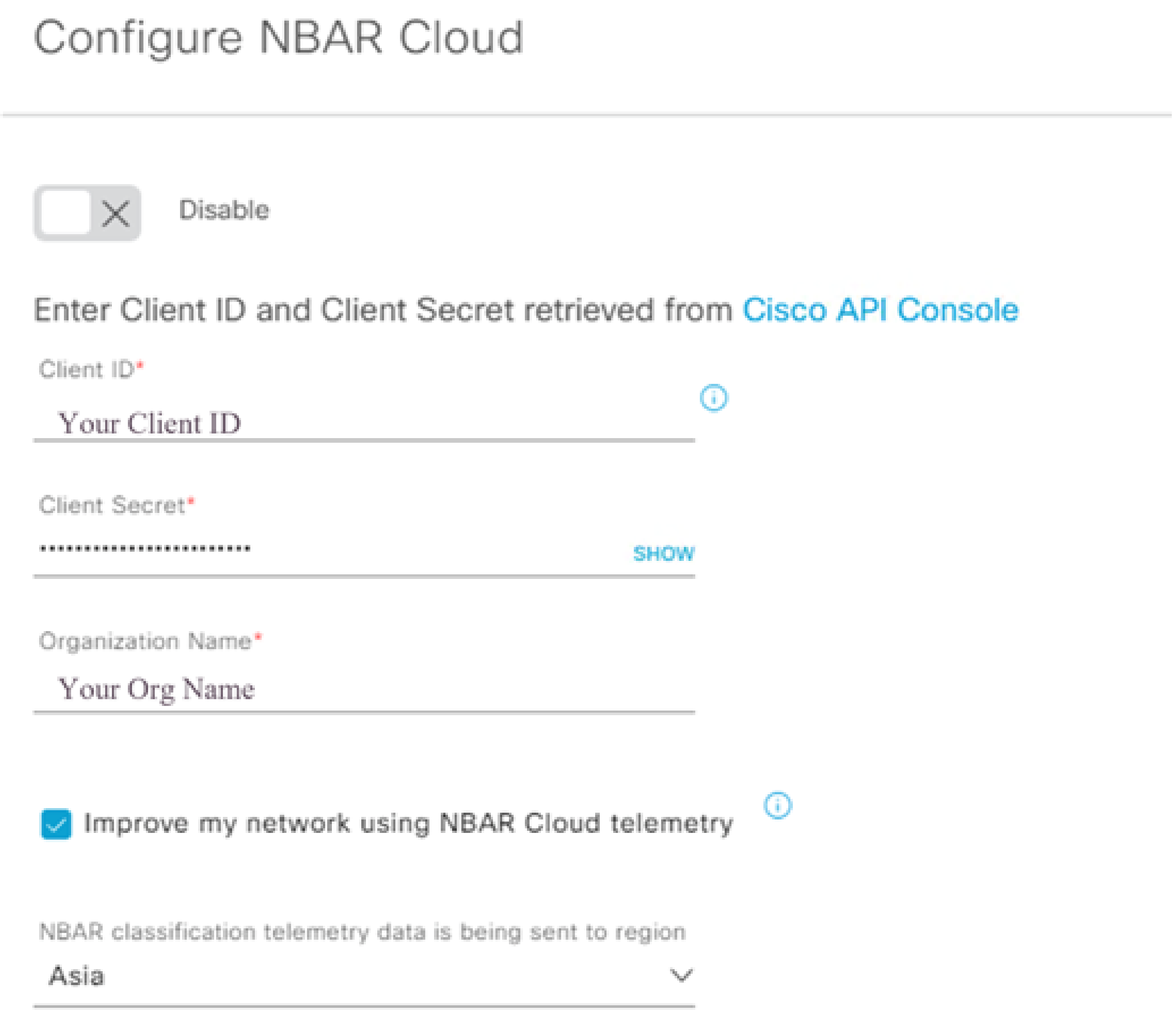
● Hello API

RATE LIMITS

100	Calls per second
500,000	Calls per day

App API Details

- Enter the Client ID and Secret obtained from the Cisco portal into Cisco DNA Center.



Configure NBAR Cloud

☒ Disable

Enter Client ID and Client Secret retrieved from Cisco API Console

Client ID*

Your Client ID

Client Secret*

••••••••••••••••••••••••••

Organization Name*

Your Org Name

☑ Improve my network using NBAR Cloud telemetry

NBAR classification telemetry data is being sent to region

Asia

Configuring Client ID and Secret on DNAC

CBAR (Controller Based Application Recognition) and SD-AVC

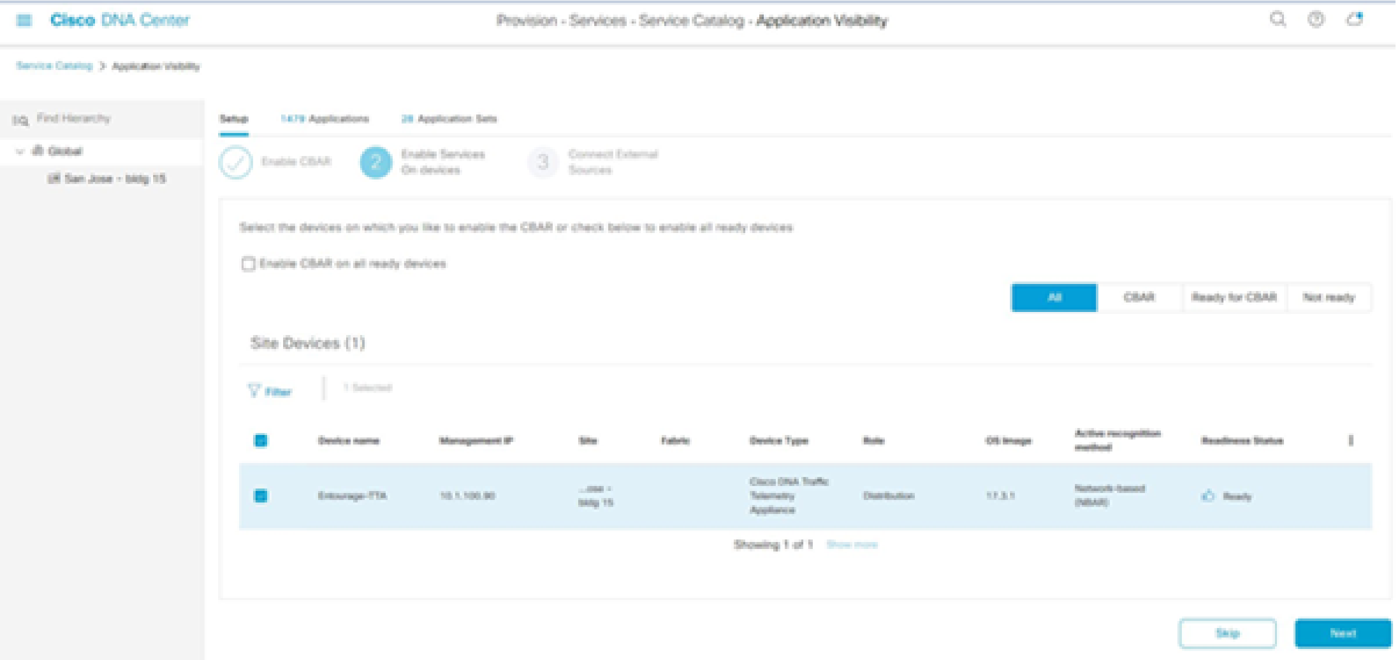
CBAR is used to classify thousands of network applications, home-grown applications and general network traffic. It allows Cisco DNA Center to learn about applications used on the network infrastructure dynamically. CBAR helps to keep the network up to date by identifying new applications as their presence on the network continues to increase and allows updates to protocol packs. If Application Visibility is lost from end-to-end through outdated protocol packs incorrect categorization and subsequent forwarding can occur. This will cause not only visibility holes within the network but also incorrect queuing or forwarding issues. CBAR solves that issue by allowing updated protocol packs to be pushed across the network.

Cisco Software-Defined AVC (SD-AVC) is a component of Cisco Application Visibility and Control (AVC). It functions as a centralized network service operating with specific participating devices in a network. SD-AVC also assists in DPI of the application data. Some of the current features and benefits provided by SD-AVC include:

- Network-level application recognition consistent across the network
- Improved application recognition in symmetric and asymmetric routing environments
- Improved first packet recognition
- Protocol Pack update at the network level
- Secure browser-based SD-AVC dashboard over HTTPS for monitoring SD-AVC functionality and statistics, and for configuring Protocol Pack updates network-wide

To enable CBAR for relevant devices follow these steps.

- Go to Cisco DNA Center's menu, **Provision > Application Visibility.** The first time the Application Visibility page is opened the user will be presented with a configuration wizard shown below.
- After discovering the devices in Cisco DNA Center for each site, select the device to enable CBAR on and proceed to the next step.



Select the devices on which you like to enable the CBAR or check below to enable all ready devices

□ Enable CBAR on all ready devices

Site Devices (1)

☑	Device name	Management IP	Site	Fabric	Device Type	Role	OS Image	Active recognition method	Readiness Status
☑	Entourage-TTA	10.1.100.90	...ose - bldg 15		Cisco DNA Traffic Telemetry Appliance	Distribution	17.3.1	Network-based (NBAR)	Ready

Showing 1 of 1

Enabling CBAR on Device

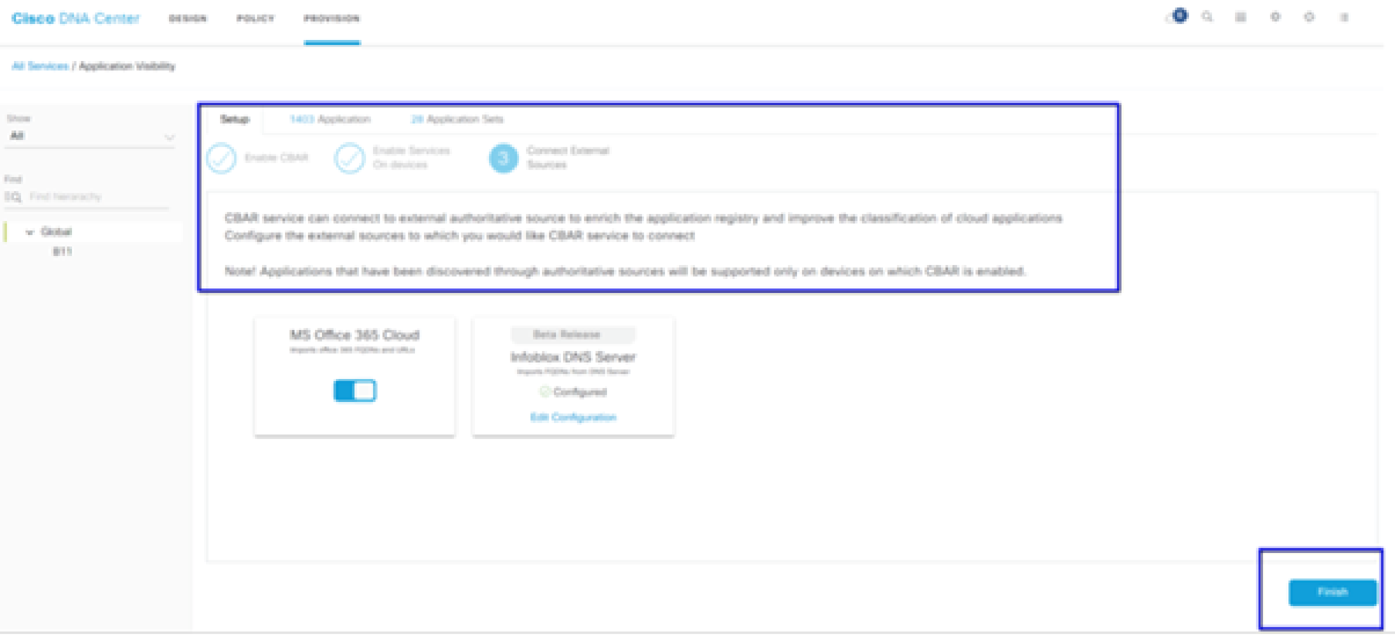
Microsoft Office 365 Cloud Connector (not a must have)

Cisco DNA Center can be integrated directly with the Microsoft RSS feed to ensure that application recognition for Office 365 aligns with their published guidance. This integration is referred to as the Microsoft Office 365 Cloud Connector in Cisco DNA Center. It is a good to have this deployed if the user is running Microsoft Office 365 applications in the network. **Integration with Microsoft Office 365 is not a requirement and if not enabled will only affect Cisco DNA Center's ability to process and classify Microsoft Office 365 host data.** Cisco DNA Center already has Microsoft Office 365 application recognition built-in, but by integrating directly with the application provider Cisco DNA Center can get updated and precise information around the current intellectual property blocks and URLs utilized by the Microsoft Office 365 suite.

To integrate Cisco DNA Center with Microsoft Office 365 Cloud follow these steps.

- Click the Menu icon and choose **Provision > Services > Application Visibility**
- Click **Discover Applications**
- Click the **MS Office 365 Cloud toggle button** to integrate Cisco DNA Center with the Microsoft

Office 365 Cloud.



CBAR service can connect to external authoritative source to enrich the application registry and improve the classification of cloud applications
Configure the external sources to which you would like CBAR service to connect

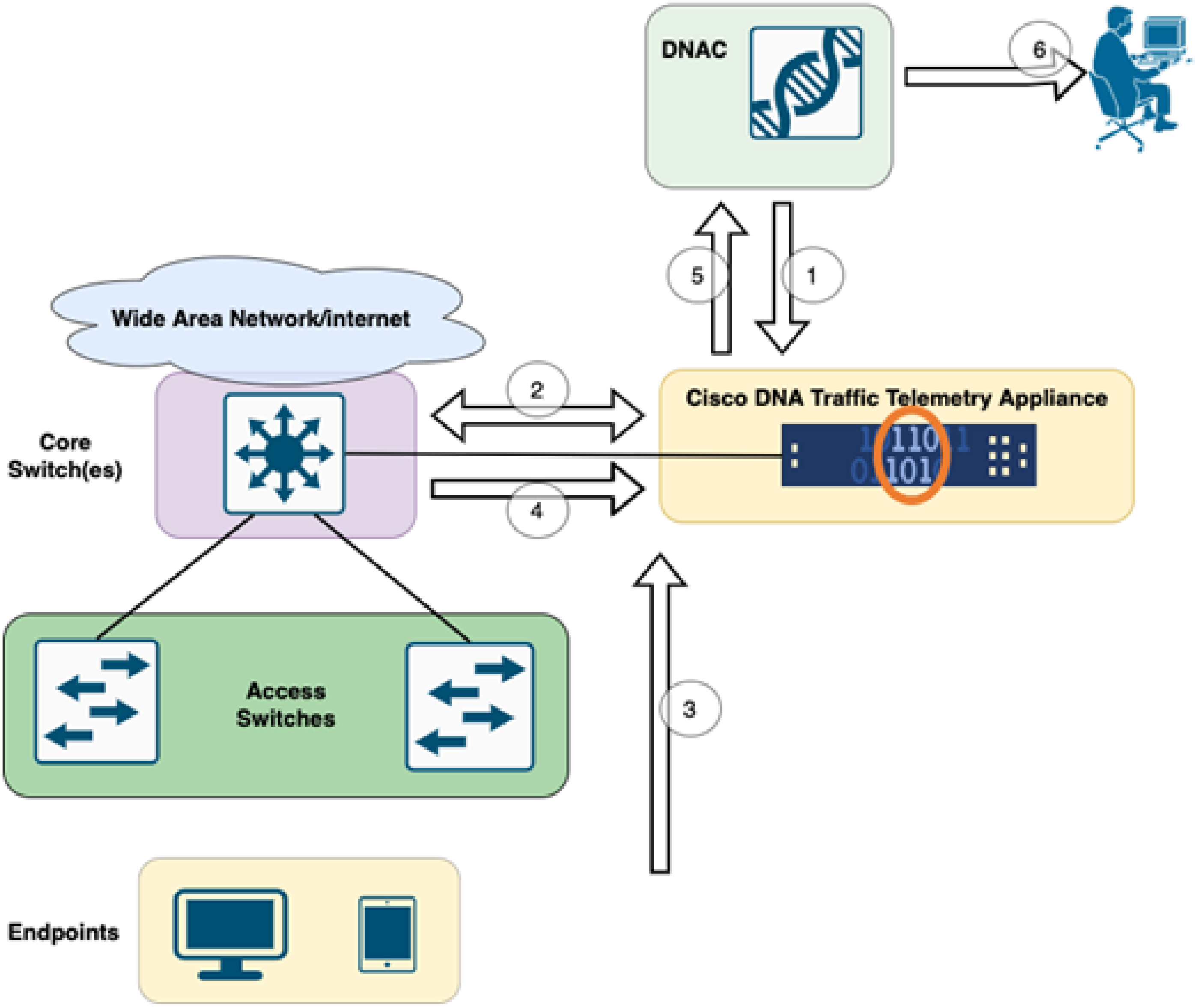
Note! Applications that have been discovered through authoritative sources will be supported only on devices on which CBAR is enabled.

MS O365 Cloud Integration

TTA Implementation

This section covers the steps required to implement TTA in a network.

TTA Workflow Overview


DNAC
6
5
1
Wide Area Network/internet
2
Cisco DNA Traffic Telemetry Appliance
Core Switch(es)
4
Access Switches
3
Endpoints

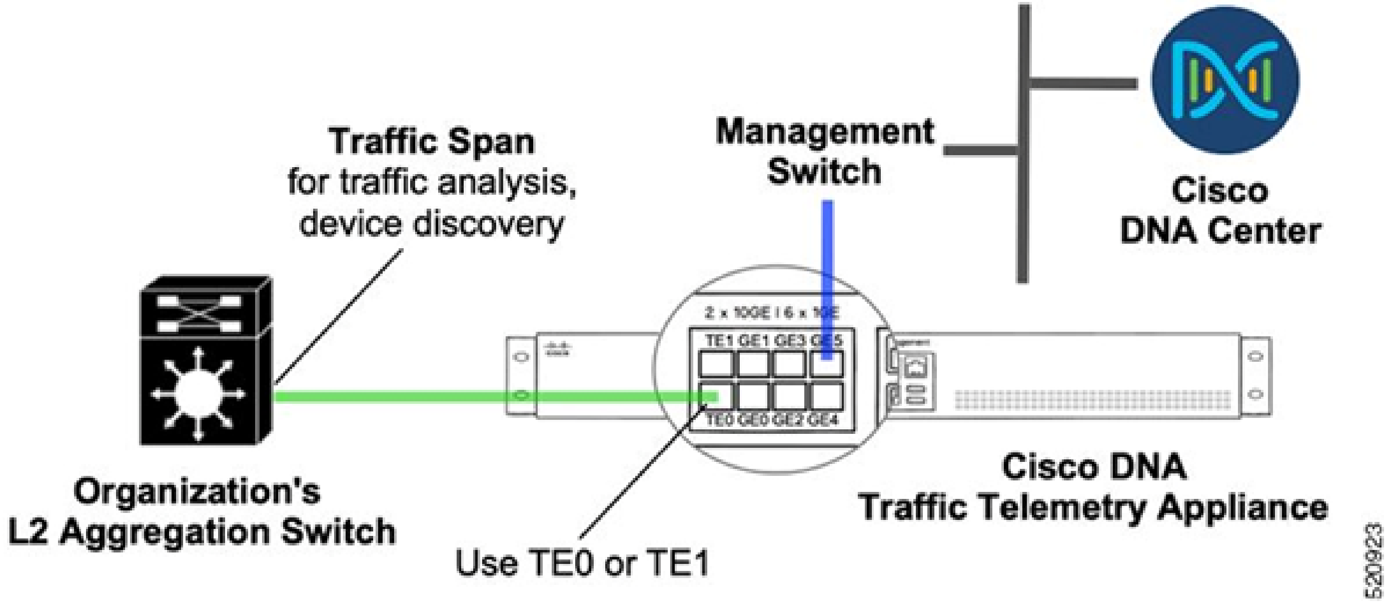
TTA to DNAC Workflow

The steps highlighted in this diagram outline the process and telemetry flow between TTA and Cisco DNA Center. Here these steps are elaborated further.

1. The Cisco Traffic Telemetry Appliance is connected to either the site aggregation switch or the core switch within the network infrastructure. This connection allows the appliance to receive traffic data from various access switches in the network.
2. The Cisco Traffic Telemetry Appliance is integrated with Cisco DNA Center, which serves as the network management platform. This integration enables seamless communication and data exchange between the appliance and Cisco DNA Center.
3. As user traffic flows through the network, it is spanned or mirrored to the Cisco Traffic Telemetry Appliance. This means that a copy of the network traffic is sent to the appliance for monitoring and analysis purposes, while the original traffic continues its normal path.
4. The Cisco Traffic Telemetry Appliance collects and processes the received traffic data. It extracts relevant information, such as packet-level details, flow statistics, and performance metrics, from the mirrored traffic.
5. The processed telemetry information is then sent from the Cisco Traffic Telemetry Appliance to Cisco DNA Center. This communication allows Cisco DNA Center to receive real-time insights and updates about the network's traffic patterns, application performance, and anomalies.
6. The telemetry insights generated by Cisco DNA Center provide valuable information to network

administrators. They can use Cisco DNA Center's interface to view and analyze the collected data, gain visibility into the network's health and application performance, identify potential issues, and make informed decisions for network optimization and troubleshooting.

TTA Deployment: High Level Diagram



TTA Deployment: High Level

The diagram above depicts how TTA can be connected in the network. The 10-Gig and 1-Gig interfaces can be used for SPAN ingestion at line rate. The Gi0/0/5 interface is used for communication with Cisco DNA Center, for orchestration, and for forwarding telemetry insights to Cisco DNA Center; this interface **CANNOT** be used for SPAN ingestion.

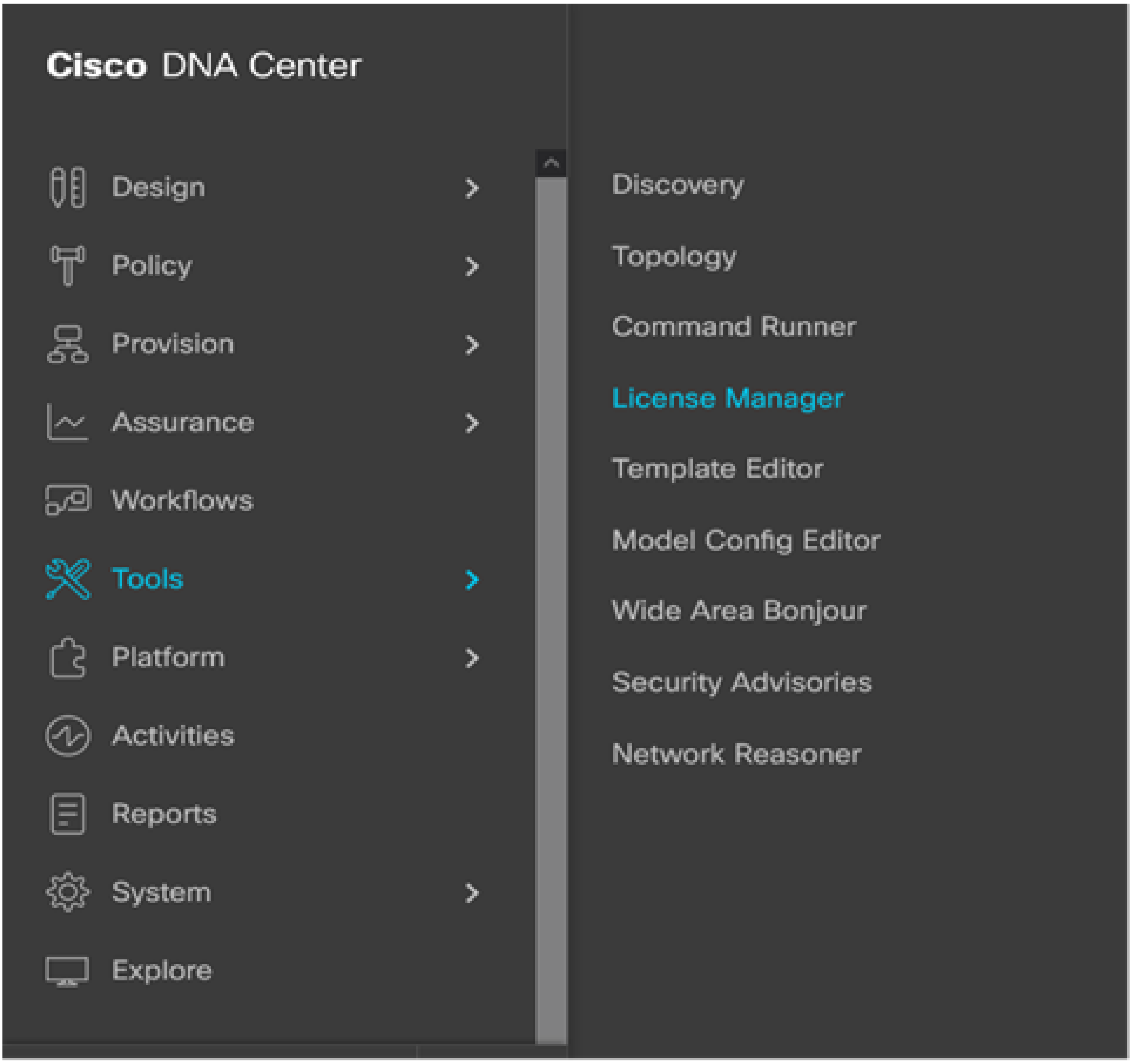
TTA Software and Licensing Requirements

TTA appliances deployed in the network will be crucial for providing telemetry insights on user data and user endpoints. To successfully deploy the solution these requirements must be fulfilled.

- TTA must be configured with an initial bootstrap configuration so that it can be discovered by Cisco DNA Center (TTA Bootstrap Configuration)
- The TTA appliance needs to be onboarded into Cisco DNA Center so that it can be managed by Cisco DNA Center (Adding Telemetry Box to Cisco DNA Center Inventory)
- The correct license needs to be installed on the TTA (TTA Appliance License)

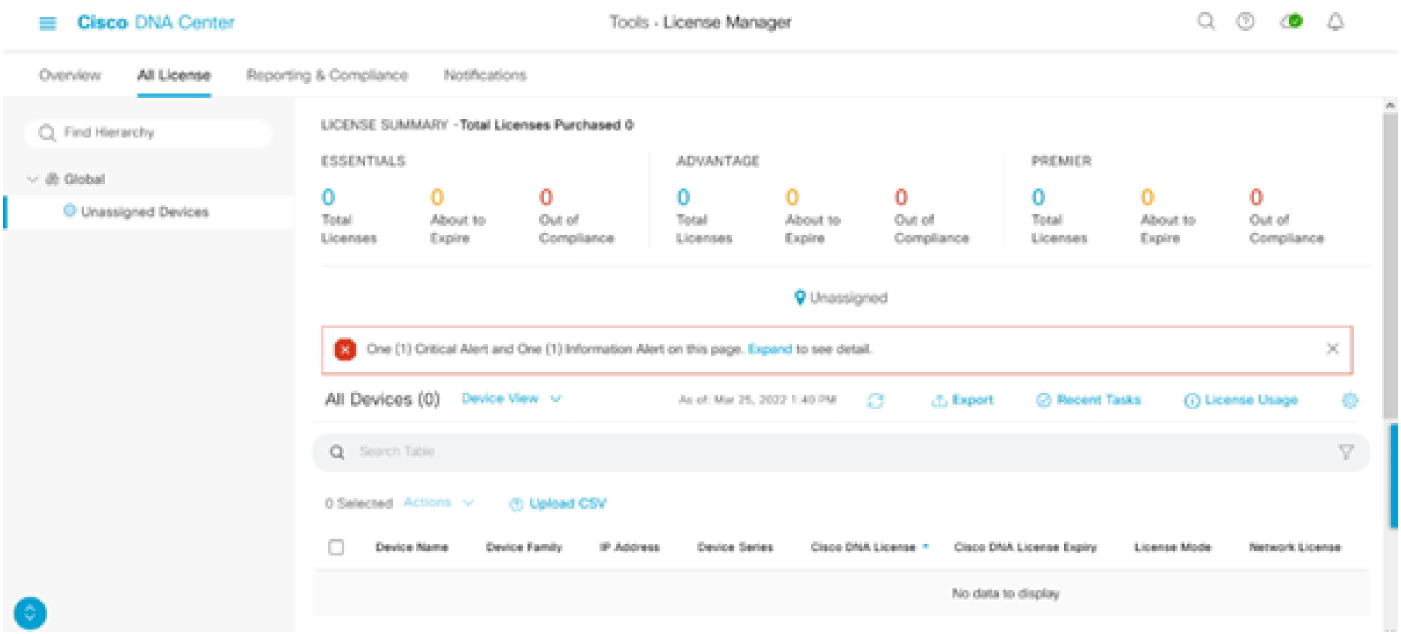
The appliance supports only one operating system and requires the **Cisco DNA TTA Advantage License** to gather telemetry. There is no need for a feature license (such as IP Base or Advanced IP Services) or a perpetual licensing package (such as Network Essentials or Network Advantage.)

To manage licenses in Cisco DNA Center navigate to the license manager by navigating to **Tools** > **License Manager** from Cisco DNA Center's drop down menu by clicking the Menu icon



License Manager on DNAC

- Navigate to the **All License** page; it will look similar to this image. On this page the admin can manage network device licenses like that of the TTA.



Cisco DNA Center

Tools - License Manager

Overview | All License | Reporting & Compliance | Notifications

Find Hierarchy

Global

Unassigned Devices

LICENSE SUMMARY - Total Licenses Purchased 0

ESSENTIALS			ADVANTAGE			PREMIER		
0 Total Licenses	0 About to Expire	0 Out of Compliance	0 Total Licenses	0 About to Expire	0 Out of Compliance	0 Total Licenses	0 About to Expire	0 Out of Compliance

Unassigned

One (1) Critical Alert and One (1) Information Alert on this page. Expand to see detail.

All Devices (0) Device View

As of: Mar 25, 2022 1:40 PM

Export | Recent Tasks | License Usage

Search Table

0 Selected Actions | Upload CSV

□	Device Name	Device Family	IP Address	Device Series	Cisco DNA License	Cisco DNA License Expiry	License Mode	Network License
				No data to display				

All Licenses Page on DNAC

TTA Onboarding and Day-0 Config

To facilitate the discovery and onboarding of the TTA appliance by Cisco DNA Center, there are bootstrap commands that are required to be configured on the TTA appliances of the site. With the bootstrap configuration in place, the TTA will be discoverable from Cisco DNA Center's dashboard. Following are day-0 configuration items for a TTA appliance. Once the device is onboarded to the site hierarchy, the TTA appliance will inherit the remaining configuration items from Cisco DNA Center.

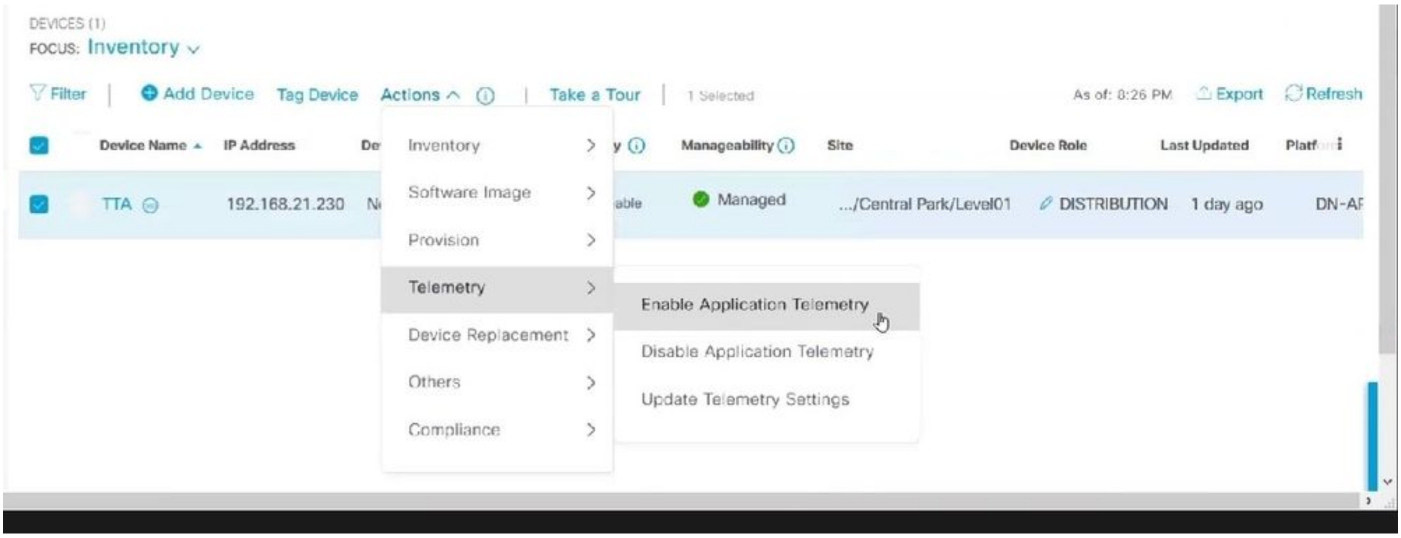
```
hostname TTA
interface GigabitEthernet0/0/5
description ***** Management Interface  ********
ip address x.x.x.x <SUBNET MASK>
negotiation auto
cdp enable

ip route 0.0.0.0 0.0.0.0 x.x.x.y
username dna privilege 15 algorithm-type scrypt secret  <password>
enable secret  <password>
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
```

Once these items are configured on the TTA, it can then be discovered by Cisco DNA Center.

Adding the TTA appliance to Cisco DNA Center's inventory

To leverage the TTA, Cisco DNA Center needs to discover and manage the TTA appliance. Once the TTA is onboarded to Cisco DNA Center it can then be managed from Cisco DNA Center. Before discovering the TTA appliance we need to ensure that the complete site hierarchy is in place for the site. After that we will proceed adding the TTA appliance under the specific site hierarchy by following these steps from the **Menu > Provision > Devices > Inventory** page to add the device to a site.

1. Provide the username/password (CLI) and SNMP community needed to connect to the device and the enable password. Wait until the device is added successfully before continuing.
2. Check the Device Name, Family (Network management in case of TTA), Reachability - Reachable, Manageable, Device Role - Distribution. The device will be “Non-Compliant” initially, however once fully provisioned the status will change.
3. Once the TTA is onboarded then Cisco DNA Center will push configuration templates to configure it with advanced telemetry functions.



Device Name	IP Address	De	y	Manageability	Site	Device Role	Last Updated	Platf
☑ TTA	192.168.21.230	N	able	● Managed	.../Central Park/Level01	DISTRIBUTION	1 day ago	DN-AF

TTA Discovery & Enabling Application Telemetry

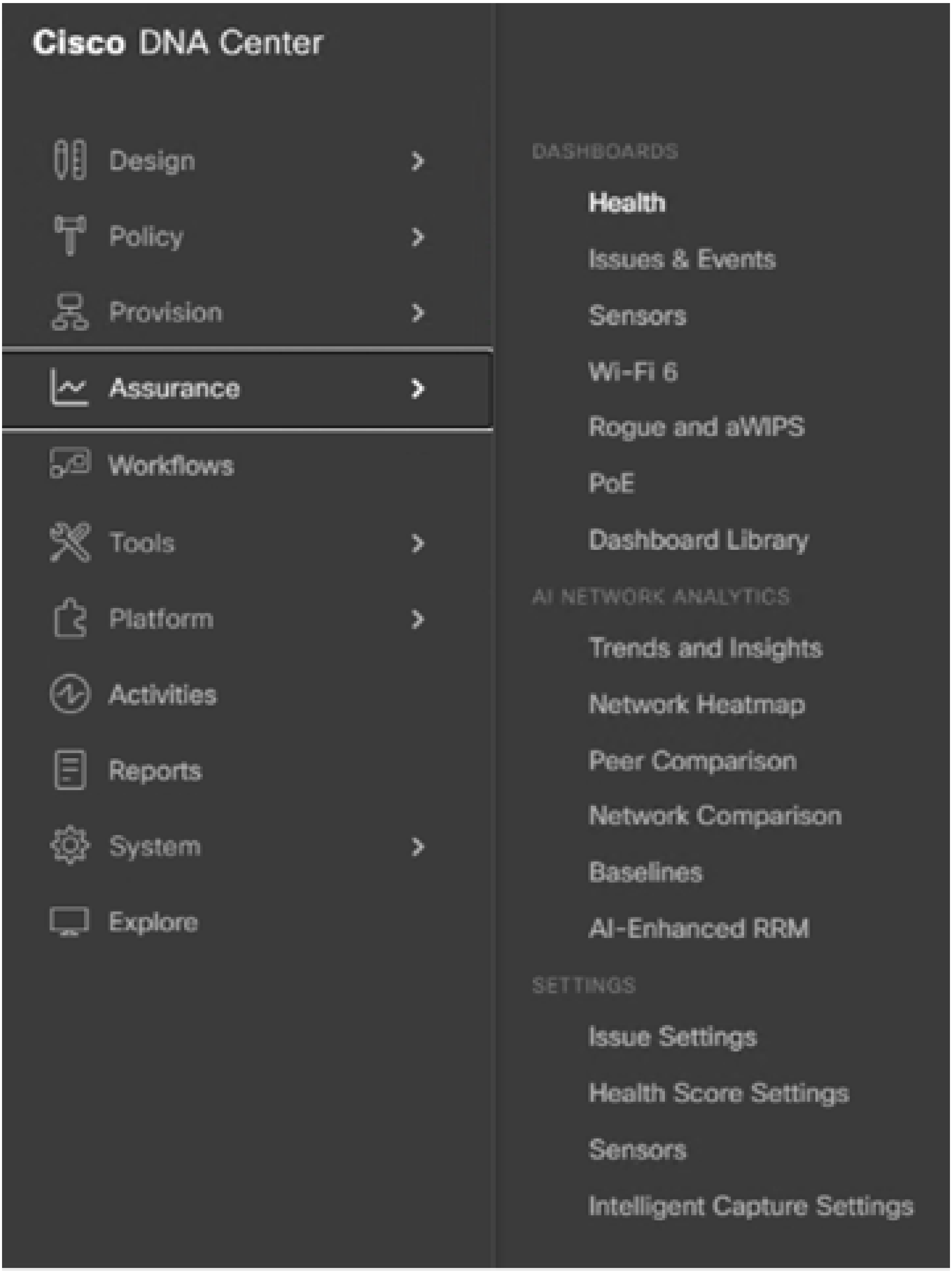
SPAN configuration

Depending on the core switch's hardware capabilities the SPAN session can be configured to SPAN a group of VLANs or interface(s) to the interface connected to the TTA. A sample configuration is given here.

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

Assurance Gathered

To access the Assurance data gathered from the installed Traffic Telemetry Appliance, go to the Assurance section and click on Health.



Cisco DNA Center

Design
Policy
Provision
Assurance
Workflows
Tools
Platform
Activities
Reports
System
Explore

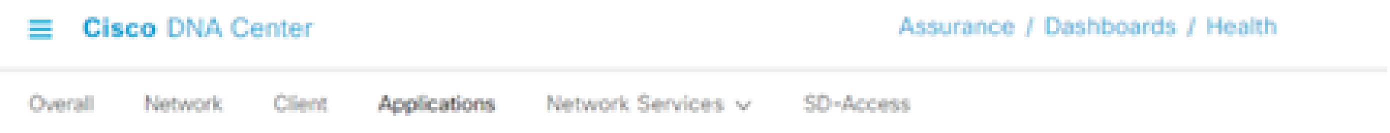
DASHBOARDS
Health
Issues & Events
Sensors
Wi-Fi 6
Rogue and aWIPS
PoE
Dashboard Library

AI NETWORK ANALYTICS
Trends and Insights
Network Heatmap
Peer Comparison
Network Comparison
Baselines
AI-Enhanced RRM

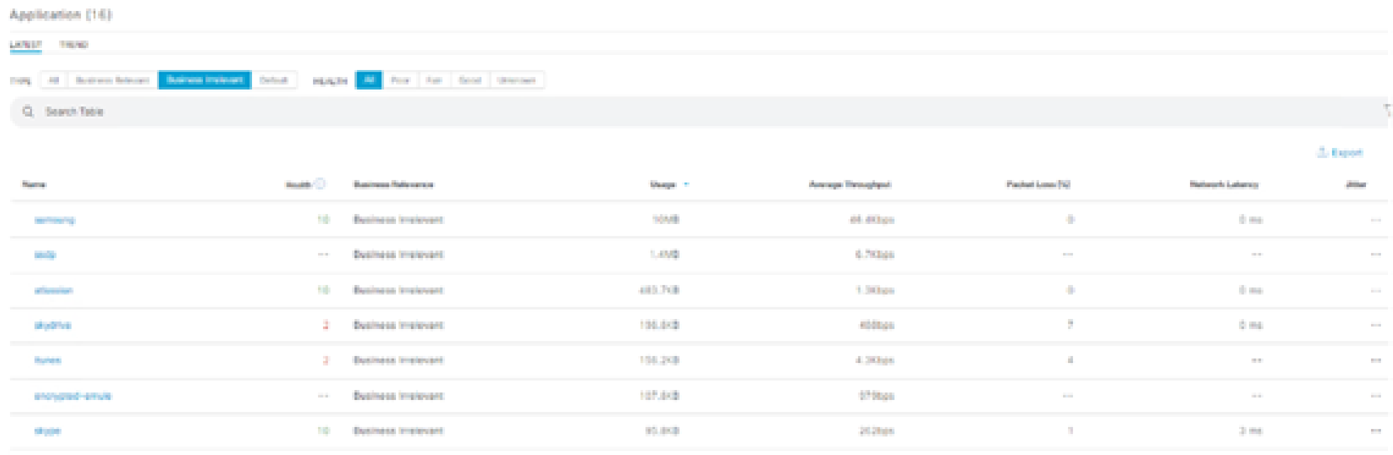
SETTINGS
Issue Settings
Health Score Settings
Sensors
Intelligent Capture Settings

Navigating to App Assurance

Choose Applications, and you will find a comprehensive overview of application data, including latency and jitter captured by the TTA based on the specific application type.



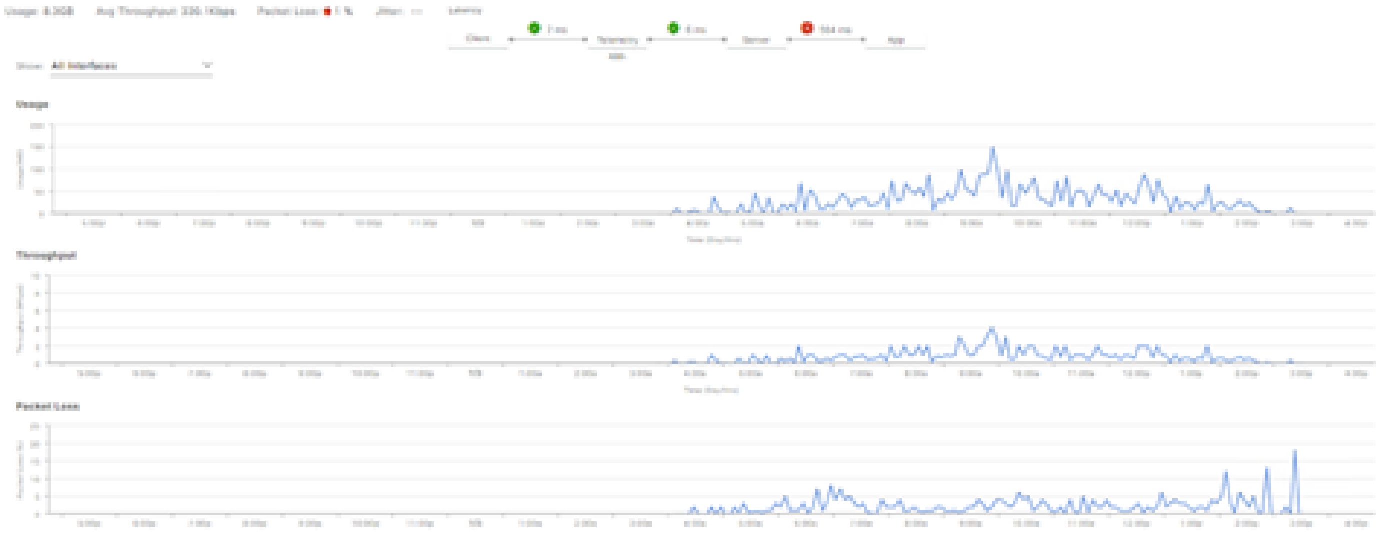
Navigating to Application Assurance



Name	Health	Business Relevance	Usage	Average Throughput	Packet Loss (%)	Network Latency	Jitter
samsung	10	Business Irrelevant	10MB	44.4Kbps	0	0 ms	--
ssdp	--	Business Irrelevant	1.4MB	6.7Kbps	--	--	--
atlassian	10	Business Irrelevant	483.7KB	1.3Kbps	0	0 ms	--
skydrive	2	Business Irrelevant	130.0KB	400bps	7	0 ms	--
itunes	2	Business Irrelevant	156.2KB	4.3Kbps	4	--	--
encrypted-emule	--	Business Irrelevant	107.8KB	579bps	--	--	--
skype	10	Business Irrelevant	95.8KB	20.2bps	1	2 ms	--

Detailed Application Assurance UI

For a more detailed analysis, users can explore individual applications by clicking on the specific application and selecting the Exporter to be the Traffic Telemetry Appliance and examine specific metrics such as Usage, Throughput, and Packet Loss data, Client Network Latency, Server Network Latency, and Application Server Latency.



Example: Application Particulars Pt.1

Network Latency
Client Network Latency
Server Network Latency
Application Server Latency

Example: Application Particulars Pt.2

Verify

1. After enabling CBAR, verify that the SD-AVC (Application Visibility Control) service is enabled on the device by logging into the Cisco Traffic Telemetry Appliance and executing this CLI command. The output will be similar to this sample indicating the **IP address of the controller** and the **status as connected**.

```
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. Use the "**show license summary**" command at the TTA's CLI to check the relevant device license details.

```
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. Verify that the SPAN session has been configured correctly on the core/aggregation switch.

```
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. Once the TTA is provisioned successfully, these commands will be (or have been) pushed to the device.

```
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
```