Cisco DNA Center FAQ

Updated: July 7, 2020

System overview

Q. What is Cisco DNA Center?

A. Cisco DNA Center is the command and control center for Cisco DNA–based networks and the heart of Cisco's intent-based network, helping IT to optimize network performance to dynamically meet business intent via automation, assurance, and security policies. Beyond device management and configuration, Cisco DNA Center gives IT teams the ability to control access through policies using Cisco ® Software-Defined Access (SD-Access), automatically provision through Cisco DNA Automation, virtualize devices through Cisco Network Functions Virtualization (NFV), and lower security risks through segmentation and Encrypted Traffic Analytics (ETA). Furthermore, Cisco DNA Assurance collects streaming telemetry from devices around the network and uses AI and machine learning to help ensure alignment of network operations with business intent. In doing this, Cisco DNA Assurance optimizes network performance, enforces network policies, and reduces time spent on mundane troubleshooting tasks. The Cisco DNA Center Platform provides 360-degree extensibility with a broad ecosystem of partners and Independent Software Vendors (ISVs) that allow you to make your network agile and fully in tune with your business priorities. Cisco's DNA Center is the only centralized network management system to bring all of this functionality into a single pane of glass.

Q. What is Cisco's vision behind Cisco DNA Center?

A. Cisco set out to build the network of the future—a closed-loop system that's self-learning, self-correcting, and self-contained, delivering true intent-based networking. Cisco DNA Center is a single touch point on top of the network that abstracts the complexity of the network underneath and structures processes to align with IT workflows.

- **Hide complexity:** Cisco DNA Center hides the complexity of manual operations that made the network difficult to operate, error-prone, inefficient, and nonscalable, thus making the network easy and efficient to operate at scale.
- **Break silos:** Cisco DNA Center breaks the traditional silos of wired, wireless, and WAN, and enables the network to be operated as a cohesive whole.
- **Enable cross-domain interworking:** Cisco DNA Center connects with campus, data center, security, collaboration, and other domains to enable smooth cross-domain interworking.
- **Bridge to the past and the future:** Cisco DNA Center seamlessly bridges your current and future networks by supporting both new and existing deployments.
- **Cloud connectivity (optional):** If desired, Cisco DNA Center can be configured to be continuously informed by the cloud. This allows Cisco to provide updates and upgrades continually, shifting the paradigm from the traditional network upgrade cycle that can extend into months and years.
- **Airgap functionality:** Because many companies have policies that prohibit connecting their network to the public cloud, Cisco DNA Center can be operated without any connectivity to the public Internet.

- **Scale as you grow:** Cisco DNA Center is architected to manage and automate a large number of devices and endpoints. It is built with microservices that enable true horizontal scaling as needed.
- **Gain a platform for innovation:** Cisco DNA Center provides a mechanism for application developers to write applications that reside on top of the network and build upon Cisco DNA Center's native capabilities, furthering the network's agility to support business objectives.

Q. What are the key features of Cisco DNA Center?

A. Cisco DNA Center is a management portal that supports the deployment, management, and troubleshooting of an intent-based network. It consists of a dashboard and two categories of features—automation and assurance. Its key functions can be described as:

- **Policy:** Translate business intent into policies that govern the functioning of the network and continuously align it to fulfill the intent. One of the critical policies is for Network Access Control (NAC). Cisco Software-Defined Access (SD-Access), which uses Cisco DNA Center and Cisco Identity Services Engine (ISE), relies on group-based policies (as opposed to IP-based) to classify users and devices into logical groups and provides a mechanism to define the rules of communication between groups and within members of the same group. These rules are then enforced by the underlying network infrastructure, which creates a segmented virtual overlay. Such segmentation reduces risk, contains threats, and verifies regulatory compliance. Cisco SD-Access enhances visibility by using artificial intelligence and machine learning to perform advanced analytics for user and device identification and compliance, leverages policy analytics for a thorough analysis of traffic flows to help define and enforce policies using a simple graphical interface, uses macro- and microsegmentation to secure connectivity across wired and wireless network devices for granular two-level segmentation for complete zero-trust security and regulatory compliance, and exchanges operating policies to help ensure consistency by utilizing Cisco's intent-based networking multidomain architecture for enforcement throughout the access, WAN, and multicloud data center networks.
- **Automation:** Fully automate the deployment and management of intent-based network infrastructure. To ensure a comprehensive, end-to-end approach to automation, Cisco DNA Center consists of five key automation pillars—visibility, intent, deployment, management, and extensibility. Through visibility, Cisco DNA Center makes it possible to better see your entire network, including new devices. Automation is driven by policies that translate business intent into action, as outlined above. Those policies can then automate the deployment of new devices as well as the management of the software images in already deployed devices. And, finally, Cisco DNA Center automation uses APIs to expand the capabilities of Cisco DNA to other Cisco solutions, such as Cisco Stealthwatch® and Cisco Umbrella™, as well as third-party solutions. These capabilities help simplify and scale network operations by automating day-to-day configuration, provisioning, updates, and troubleshooting.
- **Assurance:** Cisco DNA Assurance is a powerful capability in Cisco DNA Center. Cisco DNA Assurance provides insights from every device, application, service, and client on your network, and utilizes the latest AI and machine learning technology to make sense of all this data. It adjusts performance thresholds, reduces alarms and false positives, and then automates the process of issue resolution and performance enhancement. It proactively predicts performance through machine learning to correlate user, device, and application data for contextual business and

operational insights. It identifies issues and provides actionable insight to deliver better, more personalized experiences. Assurance also increases network security by identifying unauthorized (rogue) devices on the network and flagging unusual application usage through the "Business Critical Applications" feature.

- **Platform:** Cisco DNA Center provides an open, extensible platform that Cisco partners can use to create value-added applications that build on the native capabilities of Cisco DNA Center. Such applications can simplify IT workflows, integrate with other technologies such as WAN and data-center technologies, and even interact with third-party network equipment.

Q. How can Cisco DNA Center accelerate organizations' digital transformation?

A. By making networks more virtualized and programmable, Cisco DNA Center allows quick changes so as to keep enterprise networks in sync with business process requirements, allowing quick introductions, modifications, and deletions of business applications. Cisco DNA Center exposes APIs that enable integration with external applications. Using these APIs, these applications can further automate networks to keep pace with changing business needs. This is particularly useful to organizations that are transforming themselves digitally and require their networks to be agile and support rapid changes through the following services:

- **Intent-based policies:** Translate business intent into policies that govern access control, application delivery, and various network functions such as the creation of virtual networks.
- **Insights and actions:** Understand user behavior and application performance to make better business decisions and support new experiences.
- **Automation and assurance:** Dynamically adapt policies across the entire network, monitor service levels, and automatically adjust to the demands of digitization.
- **Security and compliance:** Gain a strategic vantage point into risk and threats by using the network as a sensor and enforcer to quickly identify and mitigate threats.
- **Distributed data and applications:** Optimize user experience as they access applications that increasingly reside in public and private clouds with path optimization and application prioritization.

Q. How does Cisco DNA Center work with but differ from other network management systems?

A. Cisco DNA Center is a powerful intent-based networking controller that allows companies to maximize their investment in Cisco Catalyst ® software-defined devices. It truly provides a single-pane-of-glass control for your enterprise network, saving your team from mundane configurations and troubleshooting, while maximizing network user experience and security. It combines basic network management functions with integrations with Cisco Identity Services Engine (ISE), Cisco Stealthwatch, Cisco Umbrella, Cisco ACI ®, and Cisco Meraki ®, so that organizations can benefit from the single management of multiple software solutions and cross-domain integrations.

Q. How does Cisco DNA Center participate in cross-domain policy integration?

A. Building a common policy framework across the otherwise siloed technologies of campus/branch, SD-WAN, data center, and native clouds presents a challenge to enterprises, since traditionally each technology domain has defined and enforced its own access and service policies. This can lead to inconsistencies and possible security and compliance violations. Cisco SD-Access solution consisting of Cisco DNA Center and Cisco Identity Services Engine, defines and exchanges group-based policies with Cisco ACI, which ensures consistent access control policy application between campus, branch, and data center, and protects sensitive data and critical applications.

Q. What analytic functions does Cisco DNA Center provide?

A. The most common analytic functions enabled by the wealth of data collected are increased visibility, proactive troubleshooting, and guided remediation. Visibility into network operations is enhanced by the breadth of data collected from several sources and placed into a single consistent view. “Network time travel” in which the exact conditions in the past can be examined to determine the root cause of any trouble helps in proactive troubleshooting, where any fleeting situations can be caught and resolved before they can become major problems. Finally, Cisco has put its 30 years of networking experience into Cisco DNA Center and is able to provide step-by-step instructions for solving problems ranging from wireless degradation to a lack of sufficient WAN bandwidth.

Q. I have a Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) installation that controls my network. How can I migrate to Cisco DNA Center?

A. Cisco offers an upgrade path to Cisco DNA Center for current APIC-EM users. Not only are all APIC-EM capabilities included in Cisco DNA Center, but APIC-EM configurations can be imported into Cisco DNA Center for a seamless migration process. After migration to Cisco DNA Center, APIC-EM users will also benefit from many additional features such as Cisco DNA Assurance and Cisco DNA Center Platform.

Q. How does Cisco DNA Center work with Cisco Prime ® Infrastructure?

A. Cisco Prime Infrastructure 3.5 Update 2 includes a Cisco DNA Center coexistence and migration feature that allows users to export data from Cisco Prime Infrastructure to Cisco DNA Center. The two management and control systems can be operated in parallel in order for IT teams to train and get familiar with Cisco DNA Center before a complete system migration is performed. Teams can begin to migrate as soon as they are comfortable with the new paradigm for automation, assurance, and security that Cisco DNA Center offers. The data that can be exported from Cisco Prime Infrastructure to Cisco DNA Center includes sites and their hierarchy along with floor maps, wireless map settings, access point placements, devices, and Connected Mobile Experiences (CMX) settings. The existing infrastructure managed by Cisco Prime Infrastructure can be exported to Cisco DNA Center to enable the assurance functionality.

Q. What does Cisco DNA Center mean for service providers?

A. The Cisco DNA Center with its intent-based APIs represents a large opportunity for service providers to add greater value to their business customers by creating and delivering managed business service offers in an effective, differentiable, and profitable way.

Q. What types of managed service might a service provider offer using Cisco DNA Center?

A. Cisco has a rich portfolio in SD-Access which extends across the LAN, wireless infrastructure, and IoT infrastructure that an enterprise client will typically have or be planning. A service provider can take this portfolio to create and deliver a Managed SD-Access Service using Cisco DNA Center as the domain controller. The REST APIs in the Cisco DNA Center enable the service provider to manage the service from their operations centers, including all the necessary provisioning, service assurance, and security. A range of managed service offers could be conceived for a service provider such as, but not limited to, Managed Wi-Fi, Managed LAN, Managed Surveillance, Managed Campus, and Managed SD-Branch.

Q. How does a service provider support multiservice and multitenancy with Cisco DNA Center?

A. A service provider would deploy Cisco DNA Center as a domain controller in or near the enterprise site receiving the managed service. Cisco DNA Center, through its intent-based APIs, easily integrates into the SP management systems. The recommended solution from Cisco is that such integration be done via the Cisco Managed Services Accelerator (MSX), formerly the Virtual Managed Services (VMS) software platform. MSX provides a single point of integration with the OSS/BSS and inherently supports multiple services, such as SD-WAN and SD-Branch, multitenancy across multiple enterprise clients, and the ability to orchestrate multivendor gear. MSX provides full rebranding for the service provider, and both operations and end-customer portals for visibility and control.

Q. Are any Cisco Services available for Cisco DNA Center?

A. As your intent-based networking journey continues, Cisco Services helps you extract relevant network data and insights with customized software and integrations that simplify network operations and lower operating costs. In support of Cisco DNA Center and Cisco DNA Center Platform capabilities, Cisco Services provides advisory, implementation, software integration, optimization, solution support, technical training, and managed services. Our Cisco Services experts will help you achieve extraordinary business outcomes and anticipate change so you can pivot quickly, securely, and confidently. View all services.

Q. Are specific professional services available to help me design and implement Cisco DNA Center?

A. The Cisco DNA Center Advise and Implement service helps ensure rapid deployment of Cisco DNA Center for simplified control of wired and wireless environments and intent-based networking across the campus, branch, and WAN. Taking an architectural approach to policy automation and assurance, Cisco experts work with your IT staff to develop a business strategy and use case requirements for Cisco DNA Center. Validated custom designs reduce deployment risk, and proven best practices, tools, and methodologies result in implementation success. Cisco experts work with you to extend the value of Cisco DNA Center with third-party software integration and customized feature enhancements. Using Cisco DNA Center Platform extensibility, this service helps you integrate Cisco DNA Center with IT and business systems for greater IT efficiency.

Q. What kind of technical support is available to support my solution?

A. Cisco Solution Support is a best-in-class technical service that provides the right kind of support for your Cisco DNA ecosystem. Solution Support includes Cisco product support and is essential for the Cisco DNA Center appliance. Your team of solution experts provides centralized support and addresses the Cisco DNA environment as a whole, resolving solution-level issues on average 43 percent more quickly than product support alone to help you maintain reliability and increase ROI.

Q. How do I purchase Cisco DNA Center?

A. The Cisco DNA Center software image (ISO) is shipped with a Cisco DNA Center appliance ready for installation. Please refer to the ordering guide.

Q. What Cisco infrastructure products can be managed through Cisco DNA Center?

A. As Cisco DNA Center continues to evolve and add greater value, the number of Cisco products and solutions that can be managed through the dashboard continues to grow. For the more current list of supported products, visit https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/cisco-digital-network-architecture/nb-06-cisco-dna-ready-infrastructure-brochure-cte-en.html

Q. What kind of data does Cisco DNA Center collect, how does it use the data, where does it keep the data, and for how long does it keep the data?

A. Before diving into the answer, it is important to note that (1) Cisco is very transparent about explaining exactly what is collected and where it is stored (see below) and (2) Cisco offers its customers incredible flexibility in what types of data is shared and how it is shared. Your data-sharing decision does not need to be an all-or-nothing decision, because your corporate data-sharing policy may allow you to share some types of data (for example, de-identified data). There are many benefits from crowd-sharing de-identified data (similar to anonymized data), as everyone knows from smartphone apps that help you avoid traffic on your drive home or find the best price on a new car. Cisco DNA Center allows customers to choose between a completely "air-gapped" installation of Cisco DNA Center (completely and totally disconnected from the Internet) to many stages of data sharing so that the right balance between telemetry insights and corporate policy is achieved.

There are three types of data telemetry that are collected by Cisco DNA Center. Customers can opt-in to these in order to enjoy the benefits or opt-out in order to comply with corporate policies:

Local Network Telemetry: Cisco DNA Center collects data from several different sources and protocols on the local network, including the following: traceroute; syslog; NetFlow; Authentication, Authorization, and Accounting (AAA); routers; Dynamic Host Configuration Protocol (DHCP); Telnet; wireless devices; Command-Line Interface (CLI); Object IDs (OIDs); IP SLA; DNS; ping; Simple Network Management Protocol (SNMP); IP Address Management (IPAM); MIB; Cisco Connected Mobile Experiences (CMX); and AppDynamics ®. The great breadth and depth of data collection allows Cisco DNA Center to give a clearer picture of the state of the network, clients, and applications. This data is kept on the Cisco DNA Center appliance locally (at your location) and is available for a period of 14 days. Local Network Telemetry is not transported to any other server nor is it sent to the cloud.

De-identified Cloud Telemetry: Cisco DNA Center customers with active Cisco DNA Advantage software licenses can elect to use Cisco AI Network Analytics for increased network performance and easier troubleshooting. Cisco AI Network Analytics uses a cloud-based machine-learning engine to provide this additional level of intelligence. In this case, the Local Network Telemetry is de-identified so that any specific local information is not included in the data sent to the cloud. This includes the following: product serial numbers, product MAC addresses, network usernames, network group (SGT) names, and other customer-specific information within the data. Once the Local Network Telemetry is completely de-identified, it is uploaded to the Cisco AI Network Analytics cloud server for processing. By default, Cisco DNA Center does not send De-identified Cloud Telemetry. Customers must turn on the Cisco AI Network Analytics option in the "Cisco DNA Center Settings" menu and accept the terms for De-identified Cloud Telemetry before this data is sent to the cloud. Cisco AI Network Analytics offers some of the industry's greatest network intelligence benefits, greatly enhancing networking assurance and analytics capabilities. These benefits are included in your Cisco DNA Advantage license for those that choose to opt-in to de-identified cloud telemetry.

Cisco DNA Center Product Usage Telemetry: Cisco DNA Center is configured to automatically connect and transmit product usage data to Cisco. Product usage telemetry is used by Cisco to improve appliance lifecycle management for IT teams deploying Cisco DNA. This data helps product teams serve customers better. Product Usage Telemetry is fed into an aggregated analytics engine to proactively identify potential issues, improve services and support, facilitate discussions to gather additional value from new and existing features, and assist IT teams with inventory report of license entitlement and upcoming renewals. Users may opt-out of the collection of Product Usage Telemetry by turning this feature off in the "Cisco DNA Center Settings" menu.

Policy

Q. What is Cisco DNA Center Policy?

A. Cisco DNA enables you to create policies that reflect your organization's business intent for a particular aspect of the network, such as network access or application priorities, or both. Cisco DNA Center takes the information collected in a policy and translates it into network-specific and device-specific configurations required by the different network device types, makes, models, operating systems, roles, and resource constraints of your network devices. In this way, Cisco DNA Center can effectively translate the business requirements for each job role (sales, marketing, finance, guests, etc.) or endpoint client (camera, smart-alarm, heartrate monitor, water system valve, video conference panel, etc.) and the requirements for that entity.

Q. Why is policy critical to Intent-Based Networking (IBN)?

A. Correct policy configuration is critical to intent-based networks because policy defines the way users and endpoints experience the network. With IBN, users and endpoints are grouped based on their requirements, both requirements to resources (servers, cloud providers, etc.) and requirements for application performance. We used to configure these parameters with manual segmentation (VLANs) for resource access, and QoS for application and services priority. But this was complex and unmanageable. Like a Rubik's cube, when you solve one side, you scramble the other sides. In the old days, network access, QoS, and service priority were an exercise in "give to one – take away from another." Each time new applications, or IoT clients, were added to the network, decisions needed to be made as to where to add QoS, and where to take it away? With IBN, we group users based on the requirements to do their job. And we group endpoint clients based on what is needed for them to perform. Then we create policies for each group, and these policies follow any member to that group. When users move from one access point to another, the policies for QoS, services, and network access follow them.

Q. What is the "Access Control Application" (ACA) in Cisco DNA Center?

A. ACA is the interface you will see when you open the policy dashboard in Cisco DNA Center. The ACA interface allows you to create and edit group-based policies where you can define the policies that each user group or endpoint group has, and that define their experience on the Cisco DNA network. ACA is a simple, visual matrix where IT can create groups of users or endpoints and assign policies for application performance and resource access. Cisco DNA Center will then configure segments and microsegments based on these groups and policies. This simplifies the creation of policies and segmentation for both fabric and nonfabric networks. It enables the clear visualization of policies and segmentation between source and destination groups.

Q. What is group-based policy analytics?

A. Group-based policy analytics discovers activities between endpoints, groups, and applications and uses AI/ML to model groups and policies. It will submit candidate groups, contracts, and policies for authoring and enabling on the network. It's AI/ ML engine models segmentation outcomes in order to facilitate complex network policy assignments. This better equips IT teams to test and model segmentation policies and their effect on network performance.

Q. Why are analytics needed to create and optimize policy?

A. The complexity of creating and managing network policies in today's immense networks cannot be underestimated. The AI/ML powered analytical engine can solve for the complex combination of priorities between application, services, and access within the limited resources in your network. – For example, imagine a hospital with 10,000 connected IoT healthcare devices in 700 categories (this is not uncommon). That means we need to create 700 groups to support the different policies for each category of IoT device. We also need groups for users (doctors, nurses, supervisors, finance, patients, etc.). Recall the example of the Rubik's cube above – imagine a Rubik's cube with 700+ sides. How do you design the policies for each group, understanding that improving one group's application QoS can be detrimental to another group or service? This is the kind of math-intensive puzzle for which analytics with AI/ ML is perfectly served. Group-based policy analytics can crunch the numbers for all 700+ groups and create "candidate groups" with predefined policies. Then it can TEST these candidate groups simultaneously to verify functionality. No other IBN controller offers this powerful capability today.

Q. How does Cisco DNA Assurance play a role in policies?

A. Cisco DNA Assurance is looking to see that users and endpoints have the network experience that is defined in their group policies. If they don't, why? Assurance will display the top issues that are negatively effecting users and endpoints and offer guided remediation (with click-through solutions) for each issue. This allows even Level-1 support technicians to verify that the network polices that ensure business requirements are being met.

Q. What is "AI endpoint analytics" and what is its function in network policy?

A. Cisco AI endpoint analytics * is a feature in Cisco DNA Center that can identify new endpoint clients (cameras, machines, and other IoT devices) as they are connected to the network in order to determine (1) if they are authorized, (2) what profile they should have, and (3) what policies should be applied to this profile. AI endpoint analytics implements DPI (packet inspection) and other analytic methods to identify endpoint clients upon accessing the network. Then it uses AI/ ML to place them into logical groups so that policies can be assigned based on the endpoint requirements. This feature greatly facilitates onboarding and provisioning IoT endpoints in larger facilities, such as hospitals and manufacturing plants. It provides immediate identification of unauthorized endpoints connecting to the network.

Q. What is a “User Defined Network?”

A. Cisco User Defined Network (UDN) * is a Cisco network solution that allows IT staff to give end-users oversight of their very own network partition. End users can remotely and securely register their devices on their private network. Perfect for university dormitories or extended hospital stays, Cisco User Defined Network grants both device security and control, allowing end users the choice of who can connect to their network. Endusers are able to register their devices from their homes or from anywhere before they reach their destinations or connect to shared networks via an intuitive mobile app. Once they arrive on campus, their devices are connected to their personal network and are ready to be used.

*Feature release planned for Q3 2020

Q. How does the User Defined Network solution work?

A. A student is able to register his or her devices while at home or anywhere through the User Defined Network application. This registration is brought to the organization’s shared network such as a university network via the UDN Cloud Service. From there the data is transitioned to the university and thanks to Cisco DNA Center/ISE/and Catalyst hardware, a separate partition is created for each end user. Aside from sending the initial email instructions and going through the network’s workflow on Cisco DNA Center, the IT department is pretty much out of the picture.

Q. What makes the User Defined Network so unique?

A. Devices can be registered from any location via the Cisco User Defined Network. This is not available through the competition’s solution.

Simplified Day One experience allows users to access their registered devices as soon as they move in.

A mobile app allows flexibility from anywhere; the competition only has a web portal.

The mobile app allows the user to invite familiar people and their devices to their personal network.

Client 360 view and the User Defined Network Assurance dashboard provide detailed information on a private network.

The flexibility to enable private network on location of choice and use case.

The ability to contain mDNS, broadcast, link-local multicast, and unicast traffic.

Automation

Q. What is Cisco DNA Automation?

A. Cisco DNA Automation is a set of capabilities delivered by Cisco DNA Center that helps simplify deployment and automate the configuration of network devices based on policies. It is also used for operations to create, change, update, or delete network services. Included are features such as Plug and Play, or PnP, for zero- touch provisioning, Software Image Management (SWIM), as well as all day-0, day-1, and day-N functionality. Features of Cisco DNA Automation include day-0 bulk update, zero-touch device replacement for Return Material Authorizations (RMAs), and NetFlow automation for Cisco Stealthwatch ETA support, rogue device detection, Wireless Intrusion Prevention System (wIPS) detection, and Cisco Umbrella integration for DNS security. For complete details on these features, please consult the Cisco DNA Center data sheet: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-data-sheet-cte-en.html

Q. What are the key principles that enable Cisco DNA Automation to deliver more effective end-to-end network automation?

A. To provide a more effective end-to-end network automation tool, Cisco DNA automation supports five principles of automation—visibility, intent, deployment, management, and extensibility:

- **Visibility** enables users to see what devices are connected to their infrastructure, and which configurations are resident on these devices.

- **Intent** translates business intent into policies that guide the automated processes.
- **Deployment** streamlines the process of adding new devices and applying consistent configurations.
- **Management** supports the on-going management of network devices, especially the identification of software versions and configurations, the correct deployment of new software features, updates and patches, and the ability to continually monitor compliance across the network.
- **Extensibility** enables Cisco DNA Center to use configurations and network telemetry generated through automation processes to extend the capabilities of the solutions to include network assurance and security integrations.

Q. What is Inventory Insights?

A. Cisco DNA Automation has a Machine-Reasoning Engine (MRE) that can locate incorrect and inconsistent device configurations and verify device image compliance. To achieve this, inventory insights sorts devices by model and configuration and then looks for anomalies. Let's say you have 48 of the same model of switch and they all have an almost identical image version and configuration. But one of the 48 switches has an older software image, and three of the switches have the latest image but slightly different configurations. Inventory insights will flag all of these switches for your review because it is likely that one switch was not upgraded to the latest image and three of the switches have configuration errors. Normally, these types of consistency reviews are done monthly or quarterly as part of your IT network quality control. But these reviews are extremely time consuming and very tedious work. Inventory insights improve your network consistency and save your team many hours of tedious work.

Q. What is Rogue management?

A. This is a feature within the inventory menu that provides detection of unauthorized access points plugged into local switches (rogue access points) or access points that have valid corporate Service Set Identifiers (SSIDs) but are not connected to the customer's wired network (honey pots). Rogue management provides a critical level of defense against simple attempts at unauthorized network access.

Assurance

Q. What is Cisco DNA Assurance?

A. Cisco DNA Assurance employs advanced analytics and AI/ML combined with Cisco best practices to optimize your network's performance, reduce troubleshooting time, and lower the cost of network operations. It is a fundamental solution within Cisco DNA Center that enables IT to get a rich context for the user-to-application experience with historical, real-time, and predictive insights across users, devices, applications, and the network. With telemetry capabilities across the broadest sources of inputs, IT can proactively monitor and be notified of network conditions that require attention, helping ensure that the network operation is delivering on the intent of services, policies, and security.

Q. How does Assurance improve my network performance?

A. Cisco DNA Center collects data from every point in the network. It then uses Cisco AI Network Analytics to define the levels of performance required for optimal user experience on your network and to derive insights on optimization options. The clean and simple dashboard shows overall status and flags issues. Guided remediation then automates resolution to keep your network performing at an optimal level with fewer tedious and time-consuming troubleshooting tasks.

Q. What is Cisco AI Network Analytics?

A. Cisco AI Networks Analytics works inside Cisco DNA Assurance to increase intelligence in the network, empowering administrators to accurately and effectively improve performance and facilitate issue

resolution through three main capabilities:

- **Visibility – AI-driven baselining:** No two networks are the same. AI-driven technologies can learn user trends, services, and application metrics that are specific to your network. Cisco DNA Assurance can then create a customized performance curve for analytical decisions. The AI-driven baseline for the performance parameters that are unique to your network is constantly adapted as your network grows and changes.
- **Insight – intelligent issue analysis:** When every device is sending streaming telemetry, every client is communicating errors, and applications are subject to deep packet inspection, the IT team can suffer from data overload. There is too much noise from too much data! Cisco AI Network Analytics uses machine learning to make sense of all this data, accurately detect performance issues, and ignore unusual, but harmless, network anomalies. This reduces noise and false positives while identifying issues that have the greatest impact on your network. Comparative analytics leverage AI technologies to improve network performance consistency across branch offices through comparative benchmarking between peers or sites. Teams can correctly identify network optimization opportunities and allocate IT resources intelligently.
- **Action – accelerated remediation:** Cisco AI Network Analytics uses machine reasoning to perform the logical troubleshooting steps that an engineer would execute to resolve a problem. This helps users detect issues and vulnerabilities, perform complex root cause analysis, and execute corrective actions faster than ever. Machine reasoning accelerates remediation, making your team more precise in problem solving and more productive overall.

Cisco AI Network Analytics is a standard part of Cisco DNA Assurance and is included in the Cisco DNA Advantage licensing tier.

Q. How does Cisco DNA Assurance use “machine reasoning” to improve the network?

A. Cisco DNA Assurance has a Machine-Reasoning Engine (MRE) that steps through the logical processes that an IT engineer would take to troubleshoot a problem or abnormality. This MRE capability is integrated within many of Cisco DNA Assurance features in order to alleviate your team of these time-consuming and tedious troubleshooting tasks. A great example is Layer-2 STP (Spanning Tree Protocol) loops. Cisco DNA Center as a course of normal operation will proactively look for Layer-2 loops in nonfabric networks. It is very common for Layer-2 loops to be created as new switches are added to the network and existing device configurations are not reviewed. MRE capabilities in Cisco DNA Center are everywhere, helping save your team time and improve your network performance.

Q. What is the “application experience” feature, and how does it assist assurance?

A. Application experience is a feature in Cisco DNA Assurance that tracks the performance of predefined “critical business applications.” It shows user-experience and performance metrics and provides specialized rapid troubleshooting per application and per client. It provides unparalleled visibility and performance control over the applications that are critical to your core business, on a per-user basis. Multimedia monitoring uses Perfmon processing for Real-Time Protocol (RTP) streams, allowing teams to verify the quality of critical real-time applications such as multimedia. URL monitoring provides visibility into cloud-based (URL-based) applications so that their performance is optimized. Application experience provides users the performance they need on the applications that are key to their company role.

Q. What is a “Cisco Wireless Active Sensor?”

A. This is a compact network hardware device (the size of a smartphone) designed to monitor your wired or wireless network. This device connects anywhere to your network and constantly monitors the wired and wireless connectivity. Cisco DNA Center includes location-based sensor heatmaps for each sensor, in order to quickly identify failed tests and potential network issues. The device simulates real-world

client experiences in order to validate wireless performance for critical venues and high-value locations such as conference halls and meeting rooms. It is also very useful in remote branches where local IT staff are not located.

Q. What is the new “Wi-Fi 6 readiness dashboard?”

A. This is a new dashboard in the assurance menu of Cisco DNA Center. It will look through the inventory of all devices on the network and verify device, software, and client compatibility for the new Wi-Fi 6 standard. Do your wireless LAN controllers support Wi-Fi 6? Do they have the latest software image? How many Wi-Fi clients on your network are Wi-Fi 6 compatible? As you start to upgrade your access points, what locations are best served by an upgrade? Then, after upgrading, advanced wireless analytics will indicate performance and capacity gains as a result of the Wi-Fi 6 deployment. This is an incredible tool that will help your team define where and how the wireless network should be upgraded. It will also give you insights into the AP distribution by protocol (802.11 ac/n/abg), wireless airtime efficiency by protocol, and granular performance metrics.

Q. What are the agreements that Cisco has with Apple and Samsung that provide insights for wireless devices?

A. Samsung analytics and iOS analytics are features that allow smartphones and tablets to send operational information and error codes to Cisco DNA Assurance. This allows IT teams to know the exact reason for a problem. For example, an iPhone 10 cannot connect to the wireless network. Is the problem (1) incorrect user credentials, (2) no IP address from the Dynamic Host Configuration Protocol (DHCP) server, or (3) the AP where the iPhone is located has a maximum number of associations configured and cannot accept any more clients? – Client device analytics allows the smartphone to send the error code so that the IT team knows EXACTLY what the problem is, and resolve it quickly – before the user even knows there is a problem.

Q. Many other analytics and assurance systems exist. Why is Cisco DNA Assurance different?

A. Cisco DNA Assurance is integrated within Cisco DNA Center and included in the pricing for the Cisco DNA Advantage license. This means that it works as part of a complete intent-based network controller. Recall that IBN means translating business intent into network policies, automating these policies into device configurations, and then verifying that these configurations are maximizing the user experience on the network. Network policy, automation, and assurance work very closely together in a “closedloop” functionality in order to achieve true intent-based networking. These three functionalities need to be very closely integrated with each other in order to deliver a true IBN experience. Separate systems (1) will never achieve this level of tight integration, (2) will require viewing and operating on separate user-interface dashboards, and (3) will require separate licensing and payment.

Cisco DNA hardware solutions (Catalyst, Aironet ®, Cisco Integrated Services Routers, etc.) and Cisco DNA software solutions (ISE, Stealthwatch, Cisco Umbrella, etc.) have been optimized to work with Cisco DNA Center to maximize Cisco DNA Assurance performance. Cisco hardware is programmed to automatically send usage and performance telemetry in real time; other solutions depend solely on polling, NetFlow, and/or packet inspection for hardware performance data. Cisco DNA Center has tight integration with our software suite, which allows these software products to benefit from the insights that Cisco DNA Assurance provides. Other solutions have no reliable means to integrate security and policy software functionality into the insights their analytics program provides. Nor can they verify critical software performance within the policies that have been defined in their third-party AAA, RADIUS, NAC, NAS, and other access, policy, and security software solutions.

Cisco offers many options for the collection of network telemetry in order to support your corporate policy on data sharing and data security. Cisco is completely transparent in the different ways that Cisco DNA Center collects data, where that data is stored, how and what data is de-identified, and how customers can limit, or even completely opt out of telemetry data collection. Customers have the option to allow de-identified (similar to anonymized) telemetry data to be sent to the cloud so that their network can be enhanced by lessons learned by similar network configurations in other parts of the world (see "What is Cisco AI Network Analytics?" above).

Platform extensibility

Q. What makes Cisco DNA Center extensible?

A. Cisco DNA Center Platform offers several types of integrations that can be used to develop external applications that build business value by extending core Cisco DNA Center capabilities. These integrations are classified as:

- **Intent-based APIs** that enable continuous network alignment to changing IT and business needs
- **Integration APIs** that enable integration of Cisco and third-party IT and network systems for streamlining IT operations across domains that were previously silos
- **Multivendor Software Development Kits (SDKs)** that allow interaction with network equipment from different vendors

Q. How do you define APIs, SDKs, and adapters used in Cisco DNA Center Platform?

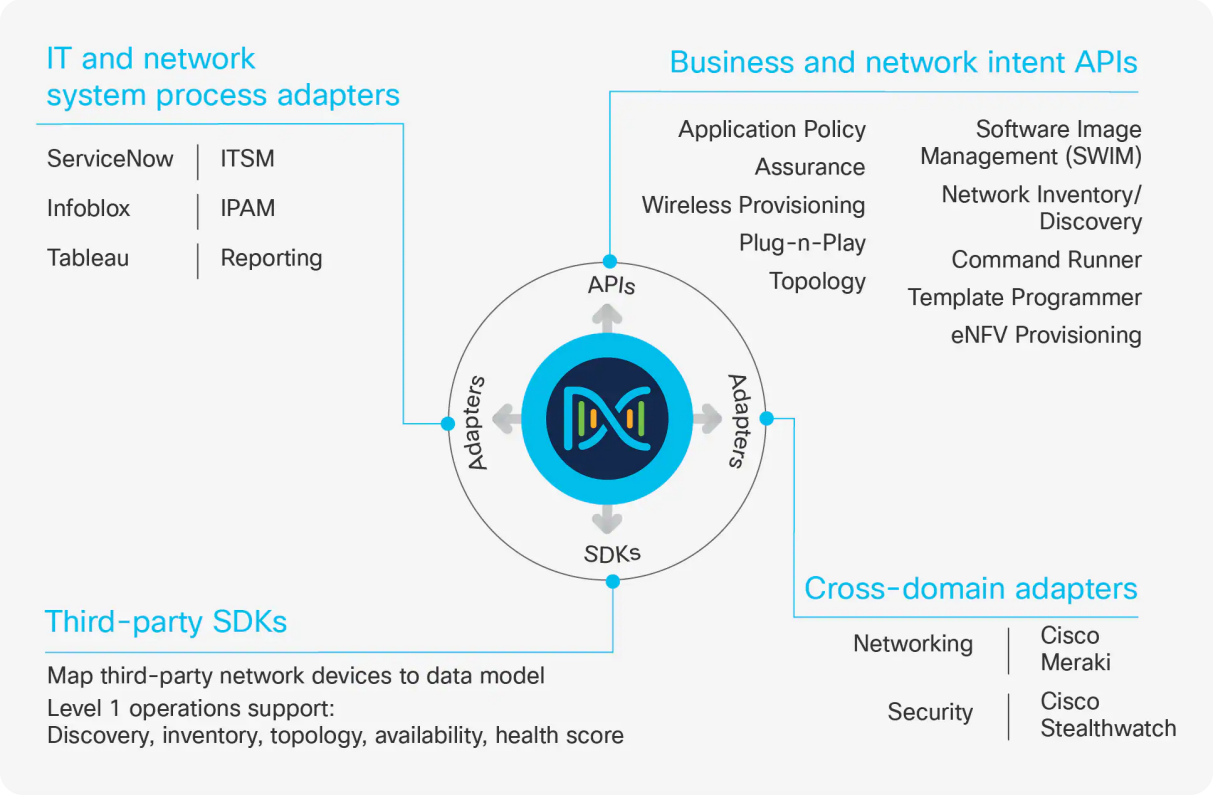
A. Cisco DNA Center Platform exposes intent-based Representational State Transfer (REST) APIs that allow external applications to invoke native automation and assurance services within Cisco DNA Center programmatically. These APIs simplify the process of creating workflows that consolidate multiple network actions and allow users to move away from doing repetitive tasks and towards creating value-added solutions.

Integration APIs are also REST APIs that are used to create adapters whose purpose is to connect Cisco DNA Center with external services as a means for data exchange. Using process adapters, you can connect Cisco DNA Center with IT and network system processes such as ITSM, IPAM, and reporting systems for the exchange of operating information as a means to improve workflows. Similarly, cross-domain adapters allow integration with other infrastructure domains such as the data center, WAN, and security to deliver a consistent intent-based infrastructure across the entire IT environment.

Cisco DNA Center uses device-specific entities called device packs to communicate with various network elements. SDKs provide the framework on which new device packs can be built. Building new device packs can extend Cisco DNA Center to manage third-party devices.

Figure 1 illustrates the role that Intent-based APIs, Integration APIs, and SDKs play and the extensions they make possible with Cisco DNA Center Platform.

Figure 1. Using Cisco DNA Center Platform intent-based APIs, integration APIs, and SDK s



Q. What are the potential benefits of Cisco DNA Center extensibility?

A. Cisco DNA Center extensibility offers many benefits, such as:

- Streamlining of IT operations by integrating networking into the IT process
- Moving resources from low-value administrative tasks to high-value policy orchestration and business-enabling tasks
- Continuous alignment of the network to meet business needs
- Investment protection that will grow with your organization's changing needs and expanding business opportunities

Q. How does Cisco DNA Center integrate with Cisco Stealthwatch?

A. Cisco Stealthwatch provides continuous real-time monitoring of, and pervasive views into, all network traffic. Stealthwatch can identify a wide range of attacks, including malware, zero-day attacks, Distributed Denial-of-Service (DDoS) attempts, Advanced Persistent Threats (APTs), and insider threats. Stealthwatch can also help you detect potential threats within encrypted traffic via Encrypted Traffic Analytics (ETA). Cisco DNA Automation can detect and enable ETA devices and send ETA and other telemetry to Stealthwatch. Cisco DNA Assurance enables you to view ETA threat detections right from the dashboard.

Q. How does Cisco DNA Center integrate with Cisco Meraki?

A. Cisco DNA Center offers a single management dashboard for Cisco DNA and Meraki customers. Cisco DNA Center uses APIs provided by Meraki to obtain inventory and status of devices. No additional licenses are required for this integration. Additionally, Meraki access points can be provisioned from within Cisco DNA Center. This allows Meraki access points to be installed at a branch office and then provisioned remotely from your corporate headquarters. From there, these Meraki access points can be managed from regional sites, branch sites, or the corporate office via the Meraki dashboard. This allows corporate headquarters to centralize the on-boarding of new devices and then provide regional or branch offices access to manage them through the Meraki dashboard.

Q. How does Cisco DNA Center integrate with Cisco Umbrella?

A. Through an easy registration process executed through their dashboards, Cisco DNA Center and Cisco Umbrella share device configurations and policies. Users can select active devices and preconfigured policies to be deployed automatically throughout the network. The integration makes it easy to streamline the security processes and ensure consistency across the network and security posture.

Q. How does Cisco DNA Center integrate with Cisco ACI?

A. Cisco ACI and Cisco DNA Center policy integration allows the marrying of ACI's application-based microsegmentation in the data center with Cisco SD-Access user group-based segmentation across the campus and branches. Simply put, Cisco DNA Center will discover SGTs on the campus network that originate in the data center through ACI configurations. These policies are then added to Cisco DNA Center's policy enforcement and extend the security and performance requirements as outlined in the original ACI policy. This is true multidomain integration.

Q. How does Cisco DevNet provide additional capabilities with Cisco DNA Center?

A. Cisco DNA Center automates much of the previously manual process of deploying configurations and managing software images. Through DevNet, even the creation of configurations and profiles can be automated. DevNet provides a library of tools that help automate these processes. The library can be found at: https://developer.cisco.com/network-automation/?utm_campaign=automation20&utm_source=carousel&utm_medium=carousel2-home

Q. How can developers learn about Cisco DNA Center Platform's intent-based APIs, integration APIs, and SDKs for device packs?

A. DevNet, Cisco's 500,000-strong developer community, provides the tools, documentation, APIs, SDKs, and use cases needed for you to get hands-on experience with Cisco DNA Center Platform:

- Learn the platform capabilities and APIs with DevNet Learning Tracks
- Practice on actionable coding with the DevNet Sandbox
- Leverage code from the community with DevNet Code Exchange
- Build solutions with the DevNet Ecosystem Exchange
- Connect with the DevNet Community

  See https://developer.cisco.com/dnacenter.

Hardware appliances

Q. What hardware options are available for Cisco DNA Center?

A. Cisco DNA Center is a software solution, which is delivered in the form of an executable ISO preinstalled on a Cisco UCS ® hardware appliance. There are three options for the Cisco DNA Center Appliance depending on the size, or potential future size, of the enterprise network. The details for these three hardware appliances are given in Figure 2.

Figure 2. Details on hardware appliances for Cisco DNA Center

	DN2-HW-APL (entry)	DN2-HW-APL-L (mid-size)	DN2-HW-APL-XL (large)
Hardware description	Cisco UCS C220 M5 Rack Server 44 cores	Cisco UCS C220 M5 Rack Server 56 cores	Cisco UCS C480 M5 Rack Server 112 cores
Cisco DNA Center System Scale			
Number of devices (switch, router, wireless controller)	1,000	2,000	5,000
Number of wireless access points	4,000	6,000	13,000
Number of concurrent endpoints	25,000	40,000	100,000

For more detailed information on these hardware appliances, please consult the Cisco DNA Center data sheet: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-data-sheet-cte-en.html

Q. Where can I get more information about Cisco DNA Center?

A. https://www.cisco.com/go/dnacenter