Data sheet

Cisco public

The bridge to possible

Cisco DNA Center 2.2.2.0

Contents

Introduction

Cisco DNA Center is a powerful network controller and management dashboard that lets you take charge of your network, optimize your Cisco investment, and lower your IT spending. Cisco DNA Center provides a single dashboard for every fundamental management task to simplify running your network. With this platform, IT can respond to changes and challenges faster and more intelligently.

- **Design:** Design your network using intuitive workflows, starting with locations where your network devices will be deployed. Users of Cisco Prime® Infrastructure and the Cisco® Application Policy Infrastructure Controller Enterprise Module (APIC-EM) can simply import existing network designs and device images into Cisco DNA Center.
- **Policy:** Define user and device profiles that facilitate highly secure access and network segmentation based on business needs. Application policies allow your business-critical applications to provide a consistent level of performance regardless of network congestion.
- **Provision:** Use policy-based automation to deliver services to the network based on business priority and to simplify device deployment. Zero-touch device provisioning and software image management features reduce device installation or upgrade time from hours to minutes and bring new remote offices online with plug-and-play ease from an off-the-shelf Cisco® device. Additionally, the Cisco Stealthwatch® Security Analytics service provisions network elements to send NetFlow and Encrypted Traffic Analytics (ETA) to Stealthwatch.
- **Assurance:** Cisco DNA Assurance enables every point on the network to become a sensor, sending continuous streaming telemetry on application performance and user connectivity in real time. This, coupled with automatic path-trace visibility and guided remediation, means network issues are resolved in minutes – before they become problems. Automated NetFlow switch configuration for Cisco Stealthwatch security provides detection and mitigation of threats, even when they are hidden in encrypted traffic.
- **Platform:** An open and extensible platform allows third-party applications and processes to exchange data and intelligence with Cisco DNA Center. By automating workflow processes based on network intelligence coming from Cisco DNA Center, IT operations are improved.

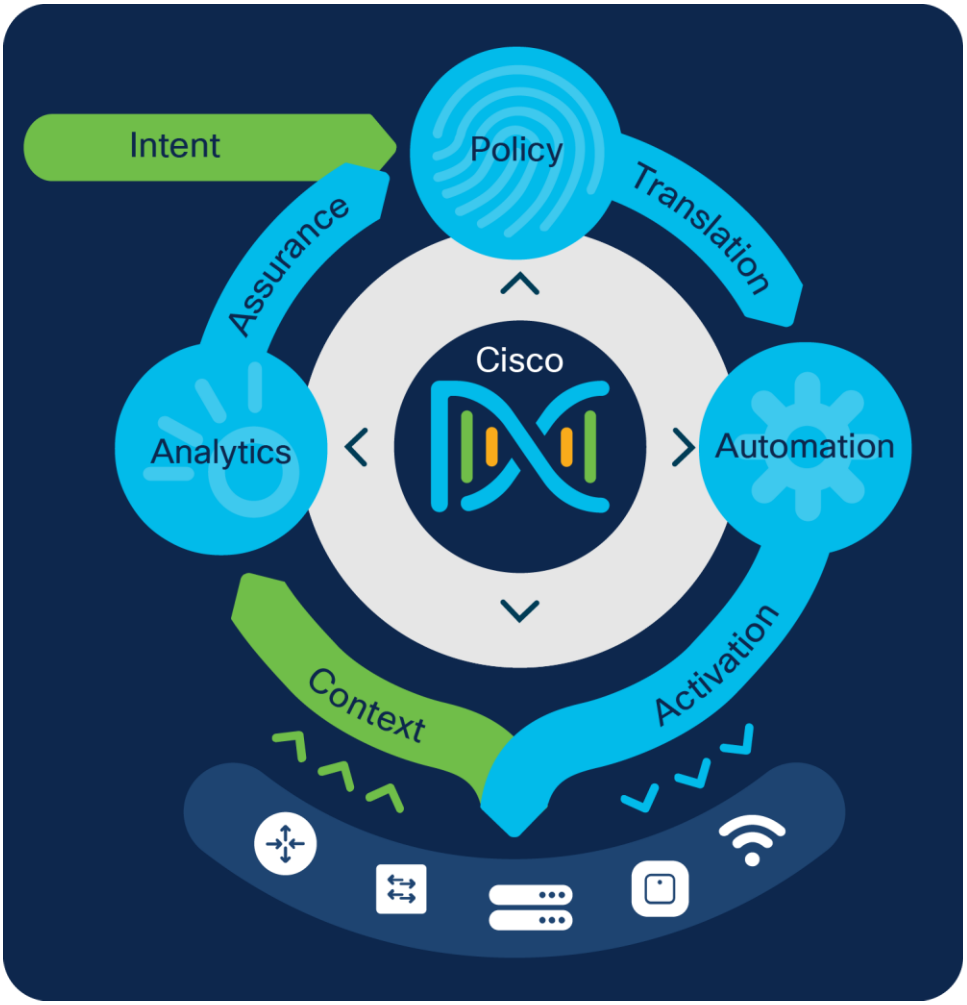


Figure 1.
Cisco DNA Center

Cisco DNA Center is at the heart of the Cisco Digital Network Architecture, or Cisco DNA (https://www.cisco.com/go/dna), and is the only centralized, intent-based network management system to bring all this functionality into an integrated controller and present it through a single pane of glass.

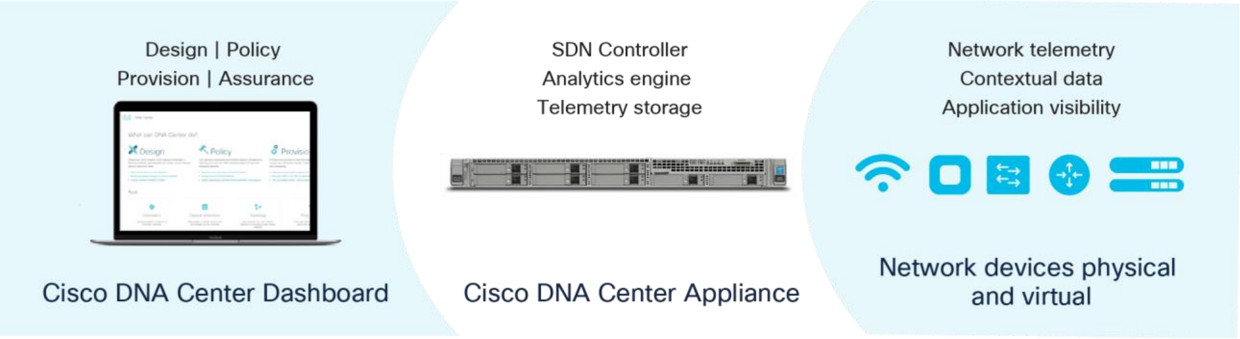


Figure 2.
How Cisco DNA Center works

Licensing

Cisco DNA Center is a software solution that resides on the Cisco DNA Center appliance. The solution receives data in the form of streaming telemetry from every device (switch, router, access point, and wireless access controller) on the network. This data provides Cisco DNA Center with the real-time information it needs for the many functions it performs. For a device to be authorized to send data to Cisco DNA Center, that device must be included in your company's Cisco DNA software license subscription. Cisco encourages customers to purchase complete Cisco DNA Center functionality through a Cisco DNA Advantage license subscription. Limited Cisco DNA Center functionality is also available through a Cisco DNA Essentials license subscription. Wireless, switching, and SD-WAN and routing subscriptions are available for 3- and 5-year terms; wireless and switching are also available in a 7-year term. All Cisco DNA software license subscription options include embedded software support and downloads (SWSS).

The links below open matrices that explain the main features included in each respective suite.

Switching feature matrix

Wireless feature matrix

SD-WAN and routing matrix

In addition to the Cisco DNA licenses, the Cisco DNA Expansion Pack is a flexible way to purchase Cisco ISE, Cisco DNA Spaces, Secure Network Analytics (Stealthwatch), ThousandEyes and other licenses, appliances, and services in one convenient bundle. Enhance your Cisco networking solutions such as SD-Access, Zero Trust solutions, Encrypted Traffic Analytics (ETA), location analytics, and assurance. You can add the pack to your Cisco DNA software licenses and choose the license count that fits your needs.

Introduction to Smart Licensing

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure – you control what users can access. With Smart Licensing you get:

- Easy Activation: Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more Product Activation Keys (PAKs).
- Unified Management: My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- License Flexibility: Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (software.cisco.com).

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

New Features

Cisco DNA Center's latest release, 2.2.2.3 is great news for ThousandEyes fans, as we include automation for this exciting product in Cisco DNA Center. Large enterprises will enjoy the many enhancements to scale, capacity, and redundancy. Customers who were waiting for a more gradual migration to SD-Access will be pleased with our capability to integrate their existing Layer 2 design without having to change operational VLANs. The main deliverables of Cisco DNA Center 2.2.2.3 are:

Enhanced Comparative Analytics

The list of items and locations that can be analyzed in the Network Comparisons dashboard has been expanded to include devices (access point families) and clients (endpoints). This addition allows comparisons among types/models of access points, or the comparison of iPhone models, or iPhones versus Android clients. Customers can now use comparative analytics to view performance differences in the products in their networks. This feature can be used to evaluate the value of an upgraded access point, or more expensive smartphone, or the performance before and after a software version upgrade on a series of devices or clients.

Enhanced Network Heatmaps

This feature facilitates locating specific devices when analyzing KPIs on the Network Heatmap dashboard and searching any heatmap for a specific access point, location, or filter. This feature lets you cross-reference KPIs of a specific access point across Assurance menus or keep track of a specific device over time. Also available are hourly views for these heatmaps, providing granularity on performance metrics throughout the day. The search and filter features greatly facilitate troubleshooting a specific device or area. Cross-referencing a wireless heatmap with the AI/ML-enhanced network heatmap can provide valuable insight as to the reason for poor performance in a given area of the network. Hourly granularity facilitates finding issues that are related to recurring events, such as post-lunchtime data surges, or poor application performance when local servers are backed up.

Additions to the Machine Reasoning Engine

The features in the cloud-based Machine Reasoning Engine (MRE) have been expanded to include additional workflows to manage the most common problems in a campus network, such as Assurance IP address failures, SD-Access wired authentication failures, and Assurance PoE troubleshooting. Customers now have additional MRE tools to troubleshoot complex networking issues. This enables faster time to resolution and fewer escalations.

WAN Performance Monitoring

IT teams need to ensure that the WAN links on the routers are available all the time and are operating within the limits without being overloaded. This feature provides for an event to be triggered in the Assurance menu when the WAN link goes down or when the utilization exceeds 70%. The issue detail captures the specific WAN link and the topology of devices under the router that are likely to see the impact of this issue. This notification is an excellent Assurance feature for legacy WAN connectivity, such as leased line and MPLS WAN.

Baselines Dashboard

The Baselines dashboard provides a view of onboarding KPIs with issue overlays going back up to 14 days. This allows IT to identify SSIDs and buildings that need extra attention based on aggregated deviation details for the selected time period. Network engineers don't have visibility into the client onboarding experience across different locations in the network and history of deviations from baselines. This new dashboard provides a single pane of glass to view the predicted onboarding performance KPIs (baselines) across every building and SSID combination.

ThousandEyes Deployment

This feature provides a GUI installation process for the deployment of the new Cisco ThousandEyes agent application on Cisco Catalyst 9000 devices. The ThousandEyes app can be installed on supported Catalyst 9000 devices in a single, streamlined workflow. New ThousandEyes agent releases are then upgraded automatically. Now that the powerful ThousandEyes performance monitoring tools are included in your Cisco DNA Advantage license, you have a simple, quick way to deploy this solution.

Native IPv6 Support

Cisco DNA Center supports managing a native IPv6 network. Customers can now configure the appliance using IPv6 addresses and walk through the install process. The use cases supported are discovery of the network devices using IPv6 addresses, inventory, and Assurance, including iCAP. Maps display the IPv6-enabled APs and clients along with the CMX integration.

StackWise Virtual ISSU

StackWise Virtual in-service software upgrades (ISSU) provides a mechanism to perform software upgrades and downgrades (major or minor releases) without taking the complete StackWise Virtual out of service. This provides a seamless, unified workflow for both wired or wireless network devices. ISSU for Cisco switches and wireless devices is already a valued feature in the Catalyst family. This feature adds the ability to upgrade a StackWise Virtual switch cluster without taking devices out of service.

SWIM Scale Package

This new addition to SWIM provides the ability to upgrade up to one thousand Catalyst 9000 devices in an hour. Devices must be running Cisco IOS-XE 17.3 or later. This unparalleled device upgrade automation results in huge productivity gains and less network downtime for an upgrade.

Enhanced Mapping Capability with GPS Markers

Maps on Cisco DNA Center have been enhanced with capabilities that several customers are using on Cisco Prime Infrastructure. Cisco DNA Center users can now add GPS markers to maps as well as import GPS markers from their Prime deployments. Cisco DNA Center users can also see IDS heatmaps on Cisco DNA Center, a useful capability when using radios in monitor mode.

Simplify Wireless Planning with the Ekahau Planning Tool

With this release, users can simplify their wireless planning using the Ekahau Planning tool within Cisco DNA Center. Users can export their floor maps from Cisco DNA Center as Ekahau Pro projects. Users can edit and augment the maps in Ekahau and reimport the maps back to Cisco DNA Center without losing items such as sensors, markers, and coverage areas that are unrecognized by Ekahau. This capability simplifies life for network designers when making map edits.

AI/ML Capability to Optimize AP Placements

Users can use AI/ML in Cisco DNA Center maps when deciding AP placements. Users can view the planned heatmap or the coverage heatmap resulting from prospective new APs operating in the vicinity of existing APs.

Existing Access VLANs Support

SD-Access introduces the ability to retain your existing access VLAN IDs when creating macrosegments in fabric. The Custom Access VLAN capability enables you to connect external switches and VLAN-capable endpoints without reconfiguring VLANs IDs, obviating a potentially disruptive and time-consuming effort when creating macrosegments.

You can retain existing access VLAN IDs when VLAN-capable endpoints or third-party switches connect directly to the SD-Access Fabric Edge to simplify and speed up your SD-Access segmentation journey.

Template-Based MACsec Support

This feature allows the creation of a template to support MACsec (802.1AE) encryption in campus network switches. Customers who require all data traversing their campus network to be encrypted can use this new template-based MACsec support feature. This feature enables devices on Ethernet networks to provide confidentiality, integrity, and authenticity for data in transit with the 802.1AE MACsec standard for encryption.

AAAs per SSID

This feature provides support for multiple AAA servers per wireless SSID. This feature provides a solution for customers with multiple AAA servers per site. Cisco DNA Center allows up to six AAA servers per SSID.

Daisy Chain for Extended Nodes

This feature allows an extended node or fabric extended node to be connected to one another in daisy-chain fashion to deploy a device beyond the normal maximum distance from the fabric edge. Often customers are faced with challenges when connecting an extended node to a fabric edge due to cabling limitations. This is particularly common in IoT and industrial IoT environments. Daisy chain enables an extended node or fabric extended node to connect to another extended node instead of a direct connect to the fabric edge, simplifying the management of extended nodes. Extended nodes are added automatically to the SDA fabric using PnP; up to 14 hops are supported.

1-1-1 Disaster Recovery with Notifications Support

This feature enables full redundancy failover with a 1-1-1 DR cluster with the same level of monitoring support available previously for 3-3-1 configurations. Customers no longer requires a 3-3-1 DR cluster for redundancy and failover. With 1-1-1 DR, you have the same net value with a smaller cluster footprint, reducing the costs of deployment and management.

Security APIs for Integration with Existing Tools and Services

This feature provides APIs for integrating Security Advisories with a customer's third-party security systems. This allows a third-party software system to receive information on Cisco device-related Security Advisories for tracking updates in other software systems.

Heartbeat IPAM Network Services

This feature employs a " heartbeat" algorithm to continually monitor the state of a customer's IP Address Management services and raises appropriate alarms when a failure is detected. This feature offers constant monitoring of critical IPAM systems and ensures minimal downtime and faster mitigation for any outage.

Increased Endpoint Scale on XL Appliances

Deployments using a three-node XL-cluster now enjoy twice the scale for endpoint clients. This includes existing three-node XL-clusters, or new three-node XL-cluster deployments and brings the total supported concurrent endpoints from 100,000 to 200,000.

Uno for Connected Enterprise

Uno is a cloud connector service that enables cloud apps and services to exchange context with Cisco products on your campus network. Often, a lack of contextual exchange between Cisco products on your network and cloud applications results in a suboptimal experience. This is because IT teams are unable to cohesively manage hybrid environments with pre-existing tools and services. Uno for Connected Experiences allows bidirectional communication between cloud and campus network devices. The solution improves operational efficiency when using products and services in the Cisco ecosystem while seamlessly and securely integrating with third-party solutions, whether on premises or in the cloud.

In-Product ROI Reports

This feature provides automated insights into productivity improvements to help visualize the value of Cisco DNA Center. The reports provide time and money savings calculated for key use cases based on product usage. Customize the units and inputs for localized and personalized output, or use anonymized cloud-based data to benchmark usage against other customers in the same vertical, geography, or device range.

Installation

This feature provides an option for a streamlined installation workflow using manufacturing defaults, which can provide appliance installation, core setup, and device discovery in under an hour. The Install includes features for automation, Assurance, and most common features. Additional features (such as Cloud-based AI/ML and the Machine Reasoning Engine) can be installed later as needed or required using the Advanced Install option. Customers can achieve a faster time to value and get started with Cisco DNA Center quickly.

Compliance API support

This set of APIs allows northbound applications to receive Cisco DNA Center compliance updates. Lack of compliance APIs makes it harder to check for overall compliance in the network, especially when Cisco DNA Center is used in a headless manner. These APIs provide the ability to integrate Cisco DNA Center compliance capabilities into other northbound systems. Additionally, Cisco partners can use compliance APIs to generate their own custom reports.

Assurance Features

For more information on Cisco DNA Assurance, go to cisco.com/go/assurance.

Table 1. Cisco DNA Assurance features and benefits

Feature	Description and benefits
Overall health dashboard	The main Assurance dashboard, which gives a high-level overview of the health of every network device and client on the network, wired and wireless. Provides the top 10 global issues and allows administrators to expand views by geographical site, device list, client list, or topology.
Network health dashboard	General overview of the operational status of every network device managed through Cisco DNA Center. Any poorly connected devices or communication issues are highlighted, with suggested remediation.
Client health dashboard	General overview of the operational status of every client connected to the network and managed through Cisco DNA Center. Any poorly connected clients or communication issues are highlighted, with suggested remediation.
Application health dashboard	General overview of the health of all applications on the network. Includes a special section on applications that have been tagged as business relevant. Business-relevant application issues are highlighted, with suggested remediation for any anomalies.
Wireless sensor dashboard	Overview of tests that have been run using Cisco Aironet™ Active Sensors. Shows overall tests, connectivity statistics, and top wireless issues discovered by sensors. Includes test results for Dynamic Host Configuration Protocol (DHCP), DNS, host reachability, RADIUS, email, Microsoft Exchange Server, web, FTP, and a complete IP SLA for data throughput speed, latency, jitter, and packet loss. Guided remediation for any test failures.
Streaming telemetry	Enables network devices to send near-real-time telemetry information to Cisco DNA Center, reducing delays in data collection. Some of the other benefits of streaming telemetry include: • Low and quantifiable CPU overhead • Optimized data export (key performance indicators [KPIs], events) • Event-driven notifications
Device 360 and Client 360	Enables viewing and troubleshooting devices or clients from any angle or context. Includes information on health trends, topology, application experience, and KPIs.
Path trace	Allows the operator to visualize the path of an application or service from the client through all devices and to the server. A common, and critical, troubleshooting task that normally requires 6 to 10 minutes is displayed instantly upon clicking a client or application. Troubleshoots issues along the network path. • Run a path trace from source to destination to quickly get key performance statistics for each device along the network path • Identify Access Control Lists (ACLs) that may be blocking or affecting the traffic flow
Network time travel	Allows the operator to see device or client performance in a timeline view to understand the network state when an issue occurred. Allows an operator to go back in time up to 14 days and see the cause of a network issue, instead of trying to recreate the issue in a lab. • Rewind time to when the issue occurred • See a history of critical events • All the information on the user or network device changes to the selected time

Feature	Description and benefits
On-device analytics	Assurance and analytics are performed on a Cisco switch, router, or wireless controller where the anomaly was discovered. Critical metrics can be identified and immediately acted on before an incident occurs. KPIs that are core to business operations can be maintained in real time, and close to the users who rely on them.
Cisco AI Network Analytics	Using AI and machine learning, Cisco AI Network Analytics drives intelligence in the network, empowering administrators to improve performance and issue resolution accurately and effectively. We are taking network analytics to a new level where noise and false positives are significantly reduced and enabling customers to very accurately identify issues, trends, anomalies, and root causes. **Intelligent issue detection and analysis** • AI-driven personalized baselining: No two networks are the same. AI-driven technologies can learn the 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. From there, the AI-driven analytics engine (both on premises and in the Cisco cloud) can make accurate decisions for what is normal and what is not, based on this personalized baseline. • AI-driven anomaly detection: This capability surfaces any deviation from our AI-created personalized baseline for this network, allowing Cisco DNA Center to make sense of all the network data. The system can accurately detect performance issues and ignore unusual but harmless network anomalies. This reduces noise while accurately identifying anomalies that have the greatest impact on your network. AI-driven predictive analytics and proactive insights allow users to anticipate and prevent failures. Here, the machine learning engine can predict increases in Wi-Fi interference, onboarding delays, and office traffic load. This is because in IP networks, a problematic event is often preceded by a benign event or series of events. By learning how series of events are correlated to one another, predictive analytics can help network administrators anticipate the unexpected. • AI-driven accelerated remediation: Cisco AI Network Analytics provides accelerated remediation through machine learning, which identifies the most critical variables related to the root cause of a given problem. This helps users detect issues and vulnerabilities, perform complex root cause analysis (using a machine reasoning engine), and execute corrective actions faster than ever. In coming releases, we will enable machine reasoning to execute the logical troubleshooting steps that an engineer would perform in order to resolve a problem. Both of these capabilities accelerate remediation, making your team more precise in problem solving and more productive overall.
Machine Reasoning Engine (MRE)	MRE defines the next intelligence evolution and helps in complex workflows where the result of one action determines the next. It closely resembles how human beings themselves reason things out and accomplish multistep tasks. An example where Cisco DNA Center uses MRE is to find and fix potentially crippling routing loops that require a careful analysis spanning multiple devices. This allows your new IT team members to accomplish complex tasks instead of escalating them, and for your more seasoned IT team members it saves time by automating tedious workflows. For more information, see https://blogs.cisco.com/networking/machine-reasoning-is-the-new-ai-ml-technology-that-will-save-you-time-and-facilitate-offsite-netops.
Extended application visibility to switch and wireless controllers	Application visibility allows Cisco DNA Assurance to monitor a user's application usage, even from a switch or wireless controller. By using switches and wireless controllers, Cisco DNA Center customers have a complete view of application visibility across the campus network infrastructure.
Power-over-Ethernet analytics	This feature provides visibility on the power loads that a switch is experiencing. Endpoint devices that are pulling too much power, as well as switches that are approaching overload, are flagged. Granular visibility shows the available power on any switch for quick installation of IoT endpoint devices.

Feature	Description and benefits
Wi-Fi client analytics for Apple iOS clients	A joint development with Apple, Wi-Fi client analytics offers Cisco DNA Assurance insights into the performance and experience of iOS clients (iPhone/iPad) on the wireless network. It allows the administrator to view wireless performance from the perspective of the client. • Supports per-device group policies and analytics ◦ Client details, such as iPhone model and iOS information • Provides insights into the client's view of the network ◦ Basic Service Set Identifier (BSSID) ◦ Received Signal Strength Indicator (RSSI) ◦ Channel number • Provides clarity regarding the reliability of connectivity ◦ Client reasons, such as error codes for last disconnection
Traffic telemetry appliance	This hardware solution collects networking data, processes it, and provides streaming telemetry to Cisco DNA Center. This can be useful in areas of your network where you do not have devices that support the types of telemetry that you need to collect from the local network, including NetFlow, AVC, NBAR, and NBAR2. This appliance can also perform Deep Packet Inspection (DPI) on network traffic to support Cisco AI Endpoint Analytics. This is a strong solution for areas with only Layer 2 network devices or for branch offices with third-party switches that do not support transmission of real-time telemetry. For more information, see https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-traffic-telemetry-appliances/datasheet-c78-744352.html.
Samsung client analytics	Retrieves client device profile information (model, OS version, sales code) and more than 20 onboarding error states from the client. Cisco's partnership with Samsung allows a Cisco network to get the client's point of view of the network – what access points it sees, the reasons for disconnections, and the current state of the user experience – provided through Cisco DNA Assurance.
Wireless sensor advancements	Location-based test templates for running sensor tests, external WebAuth assessment for guest onboarding to Cisco Identity Services Engine (ISE), location-based sensor heatmap, Sensor 360 with Access Point (AP) neighbor map view, enhanced day-0 Cisco DNA Center discovery, and dedicated wireless backhaul, including the following: • Improved day-0 discovery of sensors with dedicated wireless backhaul and secure shell (SSH) support with Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) support on wireless backhaul. • Customers have the ability to standardize on the proactive sensor tests that they want to run across hundreds of sites that are part of the enterprise in a consistent fashion by leveraging sensor test templates and flexible scheduling capabilities. • Sensors can simulate the guest onboarding experience in ISE. • After the tests are set up, customers can centrally monitor them from the newly built heatmap-based sensor dashboard. Using location heatmaps and Sensor 360, customers can then drill down to specific locations where client onboarding is failing or where there is poor Radio Frequency (RF) coverage. Enhancement to day-N sensor management use cases, including sensor status monitoring, SSH control with user name, LED flash control, name change with bulk change options, site hierarchy management, and support for bundle access for Cisco Technical Assistance Center (TAC) troubleshooting.

Feature	Description and benefits
Executive summary report	Weekly and daily reports provide executives a summary of how their network is performing, with insights into network devices, clients, and applications: • View a summary of weekly and daily network and client health and application performance • View a comparison with and changes made since the previous period • Analyze the number of network devices and clients seen on the network • View the top client types seen on the network • Analyze issue trends and top issues
Custom network health scores	Enables the customer to customize how the health score in Cisco DNA Assurance is computed.
Application experience	Tracks performance of predefined critical-business applications. Shows user experience and performance metrics. Provides specialized rapid troubleshooting per application and per client. 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 key to their company role.
Intelligent Capture	Intelligent Capture uses network sensors within the Aironet Active Sensor and the Aironet 4800 AP to provide advanced troubleshooting for wireless issues. It includes anomaly-based packet captures, on-demand RF scanning, real-time client location, and Wi-Fi application analytics. This feature offers a high level of wireless service guarantee based on detailed and proactive analysis of wireless performance per access point or per Wi-Fi client. It allows system administrators to prepare for special events or VIP visits, or simply to troubleshoot a stubborn wireless issue.
Wi-Fi 6 readiness dashboard	This dashboard can prepare your network for the new Wi-Fi standard, verify your hardware and configuration compatibility, and check your capacity readiness. This visibility speeds your upgrade and ensures that you are upgrading the neediest locations first. After upgrading, advanced wireless analytics indicate performance and capacity gains as a result of the Wi-Fi 6 deployment. Included are features that check network devices for support of critical Wi-Fi 6 requirements (IPv6, wireless controller software versions, switch support) and look for software or hardware that is not compatible. It categorizes wireless clients by Wi-Fi version (protocol) and indicates areas where upgrade is most urgent. Shows wireless system performance after an upgrade. The Wi-Fi 6 dashboard allows customers to visualize two main aspects: first, the readiness of their network with respect to Wi-Fi 6 across several different sites and locations; key aspects of readiness assessment include how many Wi Fi 6-capable clients are seen in the network, does the user have the right AP model to support Wi-Fi 6, are the APs and Wireless LAN Controllers (WLCs) running the right OS version, is the Wi-Fi 6 configuration enabled, and so on. Second, the Wi-Fi 6 dashboard allows the user to visualize the benefits of the Wi-Fi 6 network in terms of higher capacity, superior connectivity, and lower latencies on Cisco DNA Analytics and Assurance. After upgrading, advanced wireless analytics indicate performance and capacity gains as a result of the Wi-Fi 6 deployment. The dashboard contains the following windows: • Insights: overview of Wi-Fi 6 readiness with insights and suggestions to prepare the network prior to upgrade. • Wi-Fi 6 network readiness: graphical view of overall network readiness. • Top locations by Wi-Fi 6: readiness based on your network design locations (for example, buildings, floors, and branch sites). • Client distribution by capability: graphical representation of client support for protocol (Wi-Fi 6, 11ac, 11n, 11abg). • AP distribution by protocol: graphical representation of AP support for protocol (Wi-Fi

Feature	Description and benefits
	6, 11ac, 11n, 11abg). - Wireless airtime efficiency: graph of bytes per millisecond, indicating the overall efficiency of the wireless network. - Wireless latency by client count: latency of APs organized by number of clients per AP. - Wireless latency by traffic: graph of latency organized by total number of packets. - Traffic distribution by MCS index: overall wireless network traffic organized by wireless modulation rate (MCS). For more information, read the following blogs: https://blogs.cisco.com/networking/ciscos-ai-ml-can-make-your-wi-fi-6-upgrade-a-success https://blogs.cisco.com/networking/cisco-dna-your-fastest-route-to-wi-fi-6
ServiceNow/ITSM closed loop integration	Cisco DNA Center can automatically resolve open ticket numbers in ServiceNow and other ITSM platforms. When Cisco DNA Assurance detects that a fault has been resolved, it checks for an ITSM ticket number. If one exists, it sends a ticket status change with the ticket number to the ITSM system, which automatically closes the open ticket in that system.

Table of Correlated Insights

Table 2. Correlated insights

Category	Insights
Wireless issues	**Client onboarding** - Association failures - Authentication failures - IP address failures - Client exclusion - Excessive onboarding time - Excessive authentication time - Excessive IP addressing time - AAA, DHCP reachability **Client experience** - Throughput analysis - Roaming pattern analysis - Sticky client - Slow roaming - Excessive roaming - RF, roaming pattern - Dual-band clients prefer 2.4 GHz - Excessive interference - Apple iOS client disconnect **Network coverage and capacity** - Coverage hole - AP license utilization - Client capacity

Category	Insights
	• Radio utilization **Network device monitoring** • Availability • Crash, AP join failure • High availability • CPU, memory • Flapping AP, hung radio • Power supply failures
Sensor issues	**Sensor onboarding** • Association failures • Authentication failures • IP address failures • Sensor exclusion • Excessive onboarding time • Excessive authentication time • Excessive IP addressing time • AAA, DHCP reachability **Sensor experience** • Throughput analysis • Outlook web response time • Web server response time • SSH server response time • Mail server response time • FTP server response time • Excessive radio interference
Routing issues	**Router health** • High CPU • High memory **Routing technologies** • BGP AS mismatch, flap • OSPF adjacency failure • Enhanced Interior Gateway Routing Protocol (EIGRP) adjacency failure **Connectivity** • Interface high utilization • LAN connectivity down/flap • IP SLA-to-SP gateway connectivity

Category	Insights
Switching issues (nonfabric)	**Client onboarding** • Client or device DHCP • Client or device DNS • Client authentication or authorization **Switch** • CPU, memory, temperature • Line card • Modules • Power over Ethernet (PoE) power • Ternary content-addressable memory (TCAM) table
SD-Access issues	**Border and edge reachability** • Control plane reachability • Edge reachability • Border reachability • Routing protocol • MAP server **Data plane** • Border and edge connectivity • Border node health • Access node health • Network services DHCP, DNS, AAA **Policy plane** • ISE or pxGrid connectivity • Border node policy • Edge node policy **Client onboarding** • Client or device DHCP • Client or device DNS • Client authentication or authorization **Switch** • CPU, memory, temperature • Line card • Modules • PoE power • TCAM table

Automation features

For more information on Cisco DNA Automation, go to cisco.com/go/dnaautomation.

Table 3. Cisco DNA Automation features and benefits

Feature	Description and benefits
Network discovery	Automatically discovers and maps network devices to a physical topology with detailed device-level data. The discovery function uses the following protocols and methods to retrieve device information, such as IP addresses, neighboring devices, and hosts connected to the device: • Cisco Discovery Protocol (CDP) • Link Layer Discovery Protocol (LLDP) for endpoints • IP Device Tracking (IPDT) and Address Resolution Protocol (ARP) entries for host discovery • LLDP Media Endpoint Discovery (LLDP-MED) for discovering IP phones and some servers • Simple Network Management Protocol (SNMP) versions 2 and 3
Network Information Database (NIDB)	Periodically scans the network to create a “single source of truth” for IT. This inventory includes all network devices, along with an abstraction for the entire enterprise network. It keeps an updated inventory of devices and software images on that device for version control. The NIDB provides data to applications (such as SWIM and Cisco EasyQoS) so that the correct device and image version are used. It allows applications to be device independent, so configuration differences between devices aren’t a problem.
Meraki® discovery and integration	Provides for the discovery of all Meraki devices on the network and integrates them into the Cisco DNA Center dashboard. It provides for a single pane of glass for both Cisco and Meraki devices.
Network design and profile-based management	Allows you to manage your network in a hierarchical fashion by letting you add areas and buildings on a geospatial map. You can start by defining your sites, then add buildings to sites, and finally add floors with detailed floor plans to the buildings. Cisco DNA Center lets the user define profiles, which consist of common network settings such as device credentials, DHCP, DNS server, AAA server, and IP address pool. Wireless settings such as SSIDs and RF profiles can be created globally and customized at site levels. These profiles form the basis for network automation.
Network Plug and Play (PnP)	Zero-touch provisioning for new device installation. Allows off-the-shelf Cisco devices to be provisioned simply by connecting them to the network. Cisco Network PnP provides a highly secure, scalable, seamless, and unified zero-touch-deployment experience for customers across Cisco's entire enterprise network portfolio of wired and wireless devices. Deploy new devices in minutes, and without onsite support visits. Eliminate repetitive tasks and eliminate staging. Network PnP reduces the burden on enterprises by greatly simplifying the deployment process for new devices, which can significantly lower Operating Expenditures (OpEx). For more details, refer to the data sheet for the Network Plug and Play application: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Plug-and-Play/solution/guidexml/b_pnp-solution-guide.html

Feature	Description and benefits
Software Image Management (SWIM)	Manages software upgrades and controls the consistency of image versions and configurations across your network. Speeds and simplifies the deployment of new software images and patches. Pre- and post-checks help ensure no adverse effects from an upgrade. This is an easy way to build a central repository of software images and apply them to devices. Administrators can mark software images as golden for a device family, allowing them to upgrade devices to the software image and patch versions that are in compliance with the golden versions defined in the repository. • Golden images: Intent-based network upgrades allow for image standardization, much desired by network administrators. • Pre- and post-checks allow network administrators more control over and visibility into network upgrades. Patches are supported in Cisco DNA Center from intent to pre- and post-checks in the same way that we manage regular images.
ROMMon support for SWIM	The SWIM ROMMon upgrade feature optimizes already scheduled downtime by allowing users to join ROMMon upgrades with regular upgrades. The ROMMon feature in SWIM eases the task of upgrading ROMMon images on supported Cisco devices.
Device replacement and RMA workflows	Workflow templates allow for the replacement (RMA) of switches and routers. Includes restoration of IOS, configurations, and licenses. Also completes device replacement in operational systems such as Cisco ISE, certificate servers, and Cisco DNA Center inventory. Saves time and retains existing setup, licenses, and KPI trends.
PMP Bulk Update (day 0)	Simplified workflows for updating device images and configurations via easy day-0 steps.
Fog Director	Ability to manage and view Cisco industrial devices via connection with Cisco Fog Director. Fog Director delivers the capability to manage large-scale production deployments of Cisco IOx-enabled fog applications.
SMU patching	Provides patching for Software Maintenance Upgrade (SMU) recommendations and reduces the effort required to manually search for, identify, and analyze SMUs that are needed for a device. Cisco DNA Center automatically provides SMU management for multiple Cisco IOS® XR platforms and releases. Automates the patching process and allows most bug fixes to be patched with minimal network disruption.
Branch deployment automation	Simplified workflows for physical and virtual branch automation; day-0 router/NFV design. Onboard WAN devices and services via easy steps: 1. Configure network settings, service provider, and IP pools. 2. Design a router or virtual profile. 3. Assign to sites and provision network devices.
Enterprise Network Functions Virtualization (ENFV) automation	Facilitates branch virtualization on any hardware device, Cisco or third-party. Saves time in setting up network virtual services. Supports existing branch migration without hardware upgrade. This feature includes full NFV management.
Wireless automation	Intent-based workflows for simplified wireless deployment and automation: • Network profiles: A container of wireless properties that can represent single or multiple sites • Simplified guest and SSID creation • Advanced RF support for wireless networks • A single workflow to enable FlexConnect or centralized wireless deployment • PnP provisioning for APs • IP ACL support • Access and access control policy for SD-Access wireless only

Feature	Description and benefits
Device tagging	An administrator can tag network devices to associate devices that share a common attribute. For example, you can create a tag and use it to group devices based on a platform ID, Cisco IOS release, or location. Allows for grouping of devices based on specialized needs.
Policy creation	Allows the creation of policies based on business intent for a particular part of the network. Users can be assigned policies for the services that they consume, and these policies follow them throughout the network. Policies are translated by Cisco DNA Center into network-specific and device-specific configurations that can be adjusted dynamically based on network conditions. Of foundational importance for intent-based networking, policies define the business intent that is desired and allow the network to guarantee services.
Application policy creation	Allows policies to be assigned to applications based on business relevance. These applications can then be attached to sites (locations) where the policy should be applied. This feature allows business-critical applications to have greater QoS priority in the sites where their use is relevant. It is important for mission-critical applications such as machine-to-machine control in manufacturing or life-saving devices in healthcare, as well as for business-critical applications such as video in customer experience centers or voice in support sites.
Rogue management and aWIPS	Support for the detection of rogue and aWIPS threats on your campus network from within Cisco DNA Center. The Rogue and aWIPS dashboard provides detailed threat analysis and a global view of all rogue access points detected in the network, with insight into the highest priority threats so that they can be quickly identified. The Threat 360 view on this dashboard provides further details on any specific threat. This includes a map view for quick location, and all affected clients.
StackWise Virtual support	Base automation (inventory, discovery, SWIM, topology, template programmer) and Assurance support for Cisco Catalyst® 9500 and 9400 Series StackWise Virtual switches. StackWise Virtual technology on the Cisco Catalyst 9000 platform allows the clustering of two physical switches together into a single logical entity, resulting in enhancements in all areas of network design, including high availability, scalability, management, and maintenance. Customers can use Cisco DNA Center to manage the StackWise Virtual device, along with monitoring the health and status of StackWise Virtual ports and links.
Device ID certificate provisioning during Plug and Play (PnP)	API support for provisioning of device ID certificates during Plug-and-Play device claims. With this feature, the customer can push the device ID certificate to the spoke routers during Plug and Play. Certificates for spoke routers need to be pushed as part of the day-0 configuration for a critical customer deployment so that when spokes come online after day-0 configuration and the certificate is applied to them, they can establish VPN (DMVPN) connectivity to hubs right away.
Meraki wireless provisioning	Provision SSIDs in Meraki APs through Cisco DNA Center. This feature allows Meraki APs to be assigned SSIDs through Cisco DNA Center, without having to open the Meraki dashboard application.
Enterprise Network Functions Virtualization (ENFV): Advanced configuration mode	Provides advanced configurations for ENFV topologies and routing, such as switched port analyzer (SPAN) sessions, port mirroring, and packet capture. Integrates advanced configuration support for ENVF into Cisco DNA Center capabilities. This allows greater management of remote virtual servers via Cisco DNA Center.
Firewall (ASA) support	Base automation support (inventory, topology, SWIM, and configuration template) for ASA firewalls running ASA software.
Cisco Umbrella integration	This feature allows Cisco Umbrella to be deployed across sites and SSIDs from within the Cisco DNA Center dashboard. Cisco Umbrella provides DNS-layer security and is one of the quickest and most effective ways to improve your security stack. Read the blog: https://blogs.cisco.com/networking/cisco-dna-center-and-cisco-umbrella-automate-your-journey-towards-dns-security.

SD-Access features

For more information on Cisco SD-Access, go to cisco.com/go/sdaccess.

Table 4. Cisco SD-Access features and descriptions

Feature	Description
Fabric infrastructure	• Automated external connectivity handoff using Virtual Routing and Forwarding Lite (VRF-lite). • "Fabric in a box" without a control plane • Bonjour support for Cisco SD-Access
Fabric assurance	• KPIs, 360-degree views for client, AP, Wireless LAN Controller (WLC), and switch ◦ Underlay and overlay correlation ◦ Device health: fabric border and edge, CPU, memory, temperature, line cards, modules, stacking, PoE power, TCAM ◦ Data plane connectivity: reachability to fabric border, edge, control plane, and DHCP, DNS, and AAA ◦ Policy: fabric border and edge policy, ISE, and pxGrid connectivity ◦ Client onboarding: client and device DHCP and DNS, client authentication and authorization
Fabric wireless	• Wireless guest with ISE (Central Web Authentication) • Wireless guest support on separate guest border, control plane, and wireless guest support as a separate VN on the enterprise border and control plane • Same SSID for traditional and fabric on the same WLC (mixed mode) • WLC Stateful Switchover (SSO) • Wireless multicast • Multiple VNs for guest • Embedded wireless support on fabric edge • Guest web passthrough • Sleeping client timeout
Management	• Pre-check and post-check workflow validations • ISE Primary Administration Node (PAN) High Availability (HA) support (includes pxGrid and Monitoring and Troubleshooting [M&T]) • Distributed ISE Policy Service Node (PSN) support (two per site) • Same ISE instance for fabric and traditional (brownfield) deployments • Cisco Secure Access Control System (ACS) and ISE for TACACS+ authentication of network devices • HA support for Cisco DNA Center • Policy-protected CLI configuration • Software image and patch management • License management • Backup and restore • Task scheduler • Group-based access control policies
Distributed campus	• Automated intersite connectivity • End-to-end policy and segmentation

Feature	Description
Fabric infrastructure optimizations	• Device sensor for host onboarding • Server connectivity for fabric edge • Support for up to six control-plane nodes • LAN automation hardening • Cisco DNA Center template-based configurations in fabric deployments for key use cases • Border handoff enhancements: 4-byte ASN support • Two fabrics in a box at a site are supported without embedded wireless • LAN automation support for Cisco Nexus® 9500 as intermediate node but not as seed
Simplified migrations	• Layer 2 handoff at border: common subnet inside and outside fabric for SD-Access migration in brownfield network • Layer 2 flooding: fabric support for end hosts that require Layer 2 flooding; for example, building management systems or audio-visual equipment • Cisco Catalyst 9500H series support for Layer 2 handoff
SD-Access extension for IoT	Automation functionality is extended to the fabric edge to support IoT deployments where extended node devices are outside the " carpeted network." Allows greater functionality to wired and wireless devices in applications such as industrial process control, digital cities, oil fields, mining, and outdoor video surveillance.
IPv6 endpoint support	This feature introduces the capability to support IPv6 wired and wireless endpoints that are dual stacked.
AI Endpoint Analytics	This feature allows Cisco DNA Center to identify and classify endpoint devices on a campus network. Through the use of various profiling methods, including Deep Packet Inspection (DPI) and machine learning, AI Endpoint Analytics establishes visibility of what is on the network so that new endpoints can be authenticated and assigned an appropriate policy for network usage, security, and segmentation. For more information, visit the following: Informational page: https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-endpoint-analytics.html White paper: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/nb-06-ai-endpoint-analytics-wp-cte-en.html?oid=wpretr023097 Podcast: https://soundcloud.com/user-327105904/s7e29-increase-visibility-and-enhance-security-with-cisco-ai-endpoint-analytics Customer story 1: https://blogs.cisco.com/networking/north-carolina-dhhs-uses-ai-endpoint-analytics-to-simplify-network-control Customer story 2: https://blogs.cisco.com/networking/adventist-health-deploys-ai-endpoint-analytics-to-keep-its-network-in-shape
Group-based policy	A major capability in Cisco DNA Center for configuring, viewing, and editing groups and policies. Through a logical matrix interface, administrators can manage user access controls and segmentation using scalable groups, instead of IP addresses or VLANs. Users and endpoints are identified (see AI Endpoint Analytics above), categorized, and granular access privileges are provided to the resources that each endpoint requires, while segmenting them from everything else. This segmentation helps protect your users and business assets from security threats. IT teams can create and manage SGTs from within Cisco DNA Center without having to open ISE or other network policy servers. For more information on how Cisco DNA Center can provide zero-trust networking, see https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/nb-06-gbp-zero-trust-security-wp-cte-pte-en.html?oid=wprswt024194.

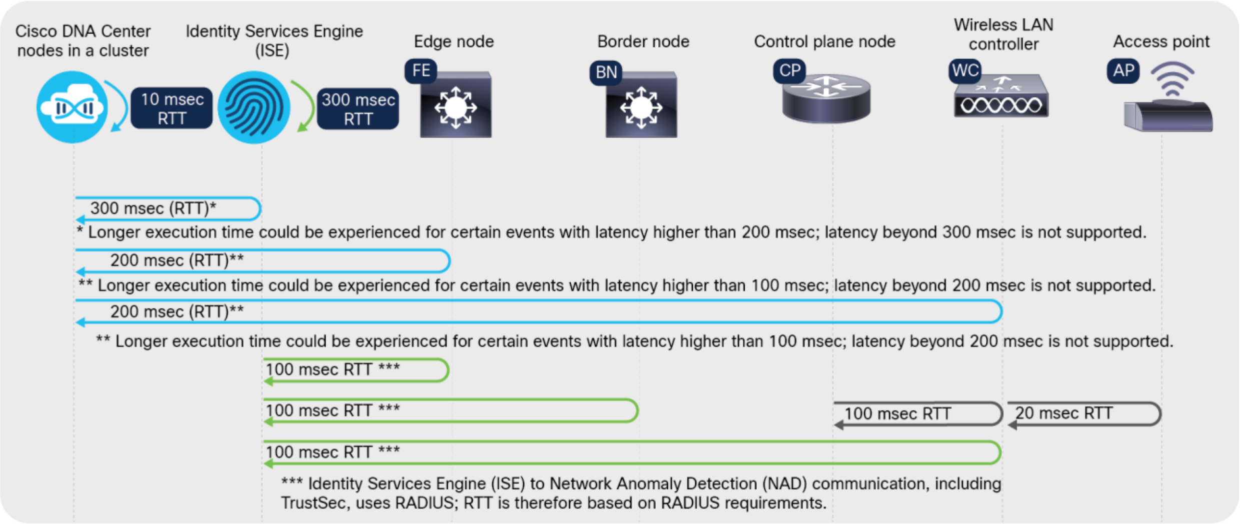
Feature	Description
Group-based policy analytics	This is an application that runs on Cisco DNA Center and accelerates and simplifies the delivery of segmentation policies. It uses analytical models to visualize the activity between endpoint profiles, scalable groups, and host groups to verify that the network policies are optimizing performance and security. For more information, visit the following: Blog: https://blogs.cisco.com/networking/write-policies-for-right-segmentation White paper: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/nb-06-gbp-zero-trust-security-wp-cte-pte-en.html?oid=wprswt024194 Analyst paper: https://www.cisco.com/c/m/en_us/products/security/identity-services-engine/removing-the-complexities-from-network-segmentation.html Recorded webinar: https://engage2demand.cisco.com/LP=21776
User-defined network	This feature in Cisco DNA Center works in conjunction with a smartphone app to allow end users to install personal endpoint devices, such as TV streaming boxes, video game consoles, and video doorbells. User-defined network allows people who reside in a large campus network, such as students in a dorm or residents in a homecare facility, to create their own wireless network partitions. These end users can then remotely and securely deploy their private devices on this network. For more information, visit the following: Landing page: https://www.cisco.com/c/en/us/solutions/enterprise-networks/user-defined-network.html Solution Overview: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/nb-06-user-defined-nw-so-cte-en.html Infographic: https://www.cisco.com/c/m/en_us/solutions/enterprise-networks/digital-network-architecture/nb-06-udn-infographic-cte-en.html?oid=ifgwls020989 Blog: https://blogs.cisco.com/networking/cisco-user-defined-network-defining-the-boundaries-of-your-network
Third-party NPS	Support for third-party Network Policy Servers (NPS) has been a request from our users, and now it is here. Cisco DNA Center can now integrate with either your third-party NPS or Cisco ISE.
AI Analytics security advisories	This feature uses the Machine Reasoning Engine (MRE) to identify potential vulnerabilities in the network. The MRE can be dynamically updated from the Machine Reasoning Knowledge Base to identify new security issues. Cisco DNA Center-supported switches and routers can be scanned to identify software images that have security advisories. Identifying security advisories is a time-consuming task that can be automated through the advanced MRE technology.
NetFlow automation for Encrypted Traffic Analytics (ETA) support	For Stealthwatch to detect malware in encrypted traffic, network devices must be configured to send NetFlow and encrypted traffic to Stealthwatch. This Cisco DNA Center feature allows users to configure select switches and routers to send data to Stealthwatch by using the Stealthwatch Security Analytics service. The service also allows users to configure select switches to send NetFlow to Stealthwatch for devices that do not support ETA.

Feature	Description
Authentication enhancements	• Users can change the authentication mode from open to closed without having to remove the device from the fabric. • The site-specific authorization template enables customers to have a unique template for each site and continue to have a global authorization template. • Critical VLAN are not pushed by default using Cisco DNA Center templates. • Seamless authorization changes provide granularity and allow the user to make authentication changes without having to remove the device from the fabric. • Users can have different authentication templates based on the deployment model. If ISE goes down, customers have the flexibility to choose not to immediately move all the clients into a single critical VLAN/pool.
Cisco Software-Defined Access (SD-Access): Layer 2 intersite	Layer 2 sites can be connected via SD-Access transit; /32s are propagated to the transit control plane. Previously, we could not use the same IP space across fabric sites. This use case is centered around sharing an IP subnet across multiple fabric-enabled sites and for allowing intersite communication for Layer 2 traffic over SD-Access transit.
Unique multicast group	For Layer 2 intersite, there is a unique multicast group per site. The blast radius of Layer 2 flooding is contained within this unique multicast group.
SD-Access: StackWise Virtual Link (SVL) support at border, edge, control plane, and Fabric in a Box	SVL support has been added on edge and border nodes. Base automation discovers manually configured SVL devices. The user can configure fabric roles such as edge/border or border + edge (B+E). SVL brings physical redundancy and provides dual homing to the devices/servers connected to the border/edge. With B+E, (noncollocated) control plane users can connect servers at the border. Cisco Catalyst 9400/9500/9500H Series Switches, when configured as StackWise Virtual, can be added to the fabric as an edge, border, border with collocated control plane, or Fabric-in-a-Box device. Cisco Catalyst 9600 Series Switches, when configured as StackWise Virtual, can be added to the fabric as a border, a control plane, or a border with collocated control plane. Note the following: • Edge nodes that are connected as SVL support only wired clients. • SVL configuration on the device must be done manually before adding the device to the inventory.
VLAN-based L2VNI	Provides Layer 2 channeling from edge to firewall or to any other node that acts as a gateway. Firewall can be used as a gateway if there are strict security compliances for intra-VLAN and inter-VLAN traffic inspection.
Cisco Catalyst 9000 Series Switches as Policy-Extended Nodes (PENs)	Many campus deployments have extended enterprises with multiple endpoints on a network spread across several miles. For security and compliance, all the endpoints need to be centrally managed. This feature provides a secure and automated device onboarding solution and central policy automation and management. Except for the Cisco Catalyst 9600 series, all other Cisco Catalyst 9000 Series Switches can act as PENs.
IP-directed broadcast	This feature provides the ability to wake up power-save hosts by sending a subnet-directed broadcast packet or magic packets.
Multicast enhancement for Cisco Vision™: custom Source-Specific Multicast (SSM) and external Rendezvous Point (RP)	With the external RP automation workflow and custom SSM range, users can bring up devices that require custom SSM, such as Cisco Vision, into the SD-Access fabric. Sites such as convention centers and stadiums can automate their digital billboards. External RP support removes the need for a dedicated RP within each site. This further reduces the TCO of a small site.

Feature	Description
SD-Access: extended node: 802.1X and MAC Authentication Bypass (MAB); multicast; Authentication, Authorization, and Accounting (AAA); secure extended nodes	802.1X, MAB, AAA, multicast, and secure support on extended nodes: • Customers can onboard Internet of Things (IoT) devices, APs, and end devices with 802.1X and MAB authentication. • Devices connected to extended nodes can join scalable groups for secure onboarding. This feature adds value for customers who want to leverage microsegmentation. Extended nodes have multicast support. IoT devices such as surveillance devices can join multicast groups. The source and receiver can hang from extended nodes.
SD-Access: new devices (Shockley, Hyper-V-WLC, Cisco Industrial Wireless 3700 Series [IW3700], Axel, Duplo)	Support for Shockley, Hyper-V-WLC, IW3700, Axel, and Duplo has been added to SD-Access.
Airgap support	Customers can install or upgrade to the latest software versions in an airgap (when the appliance is not connected to the public network or internet). This enables a customer to stay current with Cisco DNA Center versions while complying with their security policy.
Scale: filtering for IP pools	Cisco DNA Center can enforce filtering for IP pools that were configured via third-party IP Address Management (IPAM) products. This capability provides increased IPAM integration with Cisco DNA Center.
Multisite remote border	Multisite remote border enables users to configure policies for connecting to an external network (such as DMZ) through specific exit points (borders) in the SDA fabric. With multisite remote border traffic for any VN, the guest at each site tunnels back to a central location over VXLAN, allowing a single subnet to be deployed across all sites. This is ideal for environments where the requirement is for all untrusted traffic to be sent to a firewall at the DMZ.
IPv6 support for Cisco Catalyst 9800, 9800-L, and eWLC controllers	IPv6 is supported on Cisco Catalyst 9800 Series Wireless Controllers, eWLCs, and as embedded wireless solutions. IPv6 support is enabled in the overlay of the fabric. The underlay continues to be IPv4. Endpoints can have IPv4 addresses or dual-stack (IPv4+IPv6) addresses. IPv6 address assignment can be static IP, using SLAAC and/or DHCP. SLAAC can be enabled only if CIDR is /64. IPv6 DHCP and DNS are needed for pooling with IPv6. The ISE, syslog, and SNMP server are still IPv4.
N+1 rolling upgrade	N+1 rolling AP upgrade with SDA wireless enables a wireless controller image upgrade using N+1 staging controller. N+1 rolling upgrade is only applicable for Cisco Catalyst 9800 wireless controllers. N+1 High Availability (HA) is supported on AireOS on Cisco Catalyst 9800 and the Embedded Wireless Controller (EWC). N+1 rolling AP upgrades help ensure seamless client connectivity. Customers can upgrade wireless networks without network downtime when the same version SKU is supported between the controller and the APs. This enables the APs to be upgraded in a staggered manner, while still being connected to the same controller. If one WLC goes down, the AP should be able to join a secondary WLC on that fabric site. Each WLC can have its own stack, which means the first SSO should work, and only if the whole stack goes down does the AP move to a secondary embedded wireless.

Feature	Description
FlexConnect Over the Top(OTT) with SD-Access	Historically with the SD-Access solution, there was a requirement to have a wireless LAN controller in every SD-Access site. With the FlexConnect OTT feature, wireless traffic from a remote site or branch can tunnel through the Control and Provisioning of Wireless Access Points (CAPWAP) protocol to a central WLC through the Over the Top model. FlexConnect enables customers to configure and control APs in a branch or remote office from the corporate office through a WAN link without deploying a controller in each office. Supported platforms: • Cisco 5520 Wireless LAN Controller, Cisco 8540 Wireless LAN Controller, Cisco Catalyst 9800 Series Wireless Controller, Cisco Catalyst 9800-CL Wireless Controller • Cisco Aironet 1800, 2800, 3800, and 4800 APs • Cisco Aironet 9115, 9117, 9120, and 9130 APs

SD-Access requirements



Cisco DNA Center nodes in a cluster
Identity Services Engine (ISE)
Edge node
Border node
Control plane node
Wireless LAN controller
Access point
10 msec RTT
300 msec RTT
FE
BN
CP
WC
AP
300 msec (RTT)*
* Longer execution time could be experienced for certain events with latency higher than 200 msec; latency beyond 300 msec is not supported.
200 msec (RTT)**
** Longer execution time could be experienced for certain events with latency higher than 100 msec; latency beyond 200 msec is not supported.
200 msec (RTT)**
** Longer execution time could be experienced for certain events with latency higher than 100 msec; latency beyond 200 msec is not supported.
100 msec RTT ***
100 msec RTT ***
100 msec RTT
20 msec RTT
100 msec RTT ***
*** Identity Services Engine (ISE) to Network Anomaly Detection (NAD) communication, including TrustSec, uses RADIUS; RTT is therefore based on RADIUS requirements.

Figure 3.
Maximum latency supported, round-trip time

SD-Access platform scale

The following tables outline the Cisco SD-Access platform scale. The limits in this section are not necessarily dependent on Cisco DNA Center, but rather the model of device and its capacity design.

Table 5. Cisco SD-Access control plane node scale

Cisco SD-Access control plane node scale										
Family	**Cisco Catalyst**							**ASR1K/ ISR4K**	**ASR1K/ ISR4K**	**CSR**
Device	**3850**	**9300/L**	**9400 Sup-XL/Y**	**9500**	**9500H**	**9600**	**6800**	**8GB RAM**	**16GB RAM**	**1000v**
Endpoints	3000	16,000	80,000	80,000	150,000	150,000	50,000	100,000	200,000	200,000

Control-plane scale does not depend on TCAM; it only consumes memory.

Table 6. Cisco SD-Access border node scale

Cisco SD-Access border node scale											
Family	**Cisco Catalyst**								**Cisco Nexus**[1]	**ASR1K/ ISR4K**	**ASR1K/ ISR4K**
Device	**3850**	**9300/L**	**9400 Sup-XL/Y** **SDA sdm** **template**	**9500** **SDA sdm** **template**	**9500H**	**9600**	**6840/ 6880LE**	**6880XL**	**7700**	**8GB RAM**	**16GB RAM**
Virtual networks[2]	64	256	256	256	256	256	128	128	128	128	128
IPv4 routes	8000	8000	64,000	64,000	48,000	48,000	60,000	450,000	500,000	1,000,000	4,000,000
Fabric host entries[3] **(host /32 or /128)**	16,000	16,000	70,000	70,000	150,000	150,000	180,000	450,000	32,000	1,000,000	4,000,000
IPv4: SGT bindings	12,000	10,000	40,000	40,000	40,000	200,000	256,000	256,000	200,000	750,000	750,000
SGT/DGT policies	4000	8000	8000	8000	16,000	32,000	30,000	30,000	16,000	64,000	64,000
SG-ACEs (contract actions)	1500	5000	18,000	18,000	13,000	27,000	12,000	30,000	128,000	64,000	64,000

[1] Cisco Nexus 7700 can be an external border only.

[2] Virtual network scale also depends on the Cisco DNA Center platform VN scale. See Table 7 for SD-Access scale.

[3] If an endpoint has multiple IPv4 or IPv6 addresses, each address is counted as an individual entry.

Fabric host entries include access points and classic and policy-extended nodes.

Additional border node scale considerations:

/32 (IPv4) or /128 (IPv6) entries are used when the border node forwards traffic from outside the fabric to a host in the fabric.

For all switches except Cisco Catalyst 9500 High Performance and Cisco Catalyst 9600 Series Switches:

- IPv4 uses one TCAM entry (fabric host entry) for every IPv4 IP address
- IPv6 uses two TCAM entries (fabric host entries) for every IPv6 IP address

For the Cisco Catalyst 9500 High Performance and Cisco Catalyst 9600 Series Switches:

- IPv4 uses one TCAM entry (fabric host entry) for every IPv4 IP address
- IPv6 uses one TCAM entry (fabric host entry) for every IPv6 IP address

Table 7. Cisco SD-Access Layer 2 handoff border node scale considerations

Cisco SD-Access Layer 2 handoff border node scale considerations										
Family	**Cisco Catalyst**							**Nexus**	**ASR1K/ ISR4K**	**ASR1K/ ISR4K**
Device	**3850**	**9300/L**	**9400**	**9500**	**9500H**	**9600**	**6800**	**7700**	**8GB RAM**	**16GB RAM**
Endpoints	Supported	8000	16,000	16,000	32,000	32,000	Supported	Not supported	Not supported	Not supported

These numbers are the sum of the total numbers of endpoints both inside and outside the fabric site when the site has a border node with a Layer 2 handoff.

A maximum of 6000 hosts can be connected outside the fabric for all platforms that support Layer 2 border handoff.

The border node with a Layer 2 handoff contains a combination of local and remote LISP entries.

Local entries = LISP database.

Remote entries = LISP map-cache.

Example:

The Cisco Catalyst 9300 supports 8000 total entries.

If the fabric site has 6000 endpoints (map-cache), only 2000 endpoints (database) can be in the traditional network beyond the Layer 2 handoff.

Table 8. Cisco SD-Access edge node scale

Cisco SD-Access edge node scale									
Family	**Cisco Catalyst**								
Device	**3650**	**3850**	**9200-L**	**9200**	**9200 Enhanced VNs**	**9300/L**	**4500**	**9400**	**9500/H**
Virtual networks	64	64	1[1]	4[2]	32[3]	256	64	256	256
Endpoints	2000	4000	2000	4000	4000	6000	4000	6000	6000
IPv4: SGT bindings	12,000	12,000	8000	10,000	10,000	10,000	128,000	40,000	40,000

Cisco SD-Access edge node scale									
Family	**Cisco Catalyst**								
Device	**3650**	**3850**	**9200-L**	**9200**	**9200 Enhanced VNs**	**9300/L**	**4500**	**9400**	**9500/H**
SGT/DGT policies	4000	4000	2000	2000	2000	8000	2000	8000	8000
SG-ACEs (contract actions)	1350	1350	1000	1000	1000	5000	64,000	18,000	18,000

[1] 9200-L = One (1) user-defined VN (VRF)

[2] 9200 = Four (4) user-defined VNs (VRFs)

[3] 9200 “Enhanced VN” SKUs = Thirty-two (32) user-defined VNs (VRFs)

Additional notes:

INFRA_VN is not a VRF definition. It is associated with the global routing table.

DEFAULT_VN is not user-defined; it is automatically created in Cisco DNA Center. It is present for historical (backward compatibility) reasons; its use is neither necessary nor recommended.

DEFAULT_VN, if used in host onboarding, is provisioned as a VRF definition and counts as a “user-defined VN.”

Table 9. Cisco SD-Access Wireless LAN Controller (WLC) scale

Cisco SD-Access Wireless LAN Controller (WLC) scale		
Device	**Number of access points**	**Number of clients**
Aironet 3504	150	3000
Aironet 5520	1500	20,000
Aironet 8540	6000	40,000
Cisco Catalyst 9800-L	250	5000
Cisco Catalyst 9800-40	2000	32,000
Cisco Catalyst 9800-80	6000	64,000
Cisco Catalyst 9800-CL (4 CPU / 8 GB RAM)	1000	10,000
Cisco Catalyst 9800-CL (6 CPU / 16 GB RAM)	3000	32,000
Cisco Catalyst 9800-CL (10 CPU / 32 GB RAM)	6000	64,000

Table 10. Cisco SD-Access wireless edge node scale for directly connected access points and endpoints

Cisco SD-Access wireless edge node scale for directly connected access points and endpoints			
Family	**Cisco Catalyst**		
Device	**9200-L**	**9200**[1]	**9300-L**[1]
Access points	Not supported	25	50
Wireless endpoints	Not supported	500	1000

[1] A single switch and a switch stack have the same scale.

The switches listed above have a limit on the number of access tunnels that can be created on them. An access tunnel is created between the fabric edge node and a fabric-mode AP that is either directly attached or attached via a directly connect extended node.

Table 11. Cisco SD-Access embedded wireless controller scale

Cisco SD-Access embedded wireless controller scale						
Family	**Cisco Catalyst**					
Device	**9200/L**	**9300-L**	**9300 standalone**	**9300 stack**	**9400**	**9500/H**
Access points	Not supported	50	100	200	200	200
Wireless endpoints	Not supported	1000	2000	4000	4000	4000

The embedded wireless scale is the same regardless of the role of the device (edge/FIAB/border/CP).

System capabilities

Table 12. Cisco DNA Center system capabilities

Feature	Description and benefits
Role-Based access control (RBAC)	Allows users to be mapped to predefined roles. The role determines what types of operations a user can perform in the system.
Backup and restore	Supports complete backup and restore of the entire database for added protection.
ISE integration	Integrates with ISE through pxGrid or API for fabric overlay support.
Workflows	Cisco DNA Center workflows are a step-by-step guide through a particular task; for example, “Create a role” and “Refresh AP.” Workflows can be paused and revisited through the in-progress library on the workflow homepage. The home page has a library of workflows along with in-progress workflows.

Feature	Description and benefits
Activity center	The activity center is a centralized space to find audit logs and scheduled tasks. Audit logs record system events that occurred, when and where they occurred, and which users initiated them. With audit logging, configuration changes to the system are logged in separate log files for auditing. The scheduled tasks tab allows you to view upcoming, in-progress, completed, and failed administrative tasks, such as OS updates or device replacements.

Platform capabilities

Table 13. Cisco DNA Center platform capabilities

Feature	Description and benefits
Northbound REST APIs	The Cisco DNA Center platform supports Representational State Transfer (REST) APIs at the northbound layer for programmability. The Cisco DNA Center API provides support for the following features: ● Discovery, device inventory, and network topology ● SWIM, Plug and Play (PnP), wireless, SDA, and application policy ● Template programmer and command runner ● Assurance: site, device, and client health monitoring and path tracing ● NFV provisioning ● Configuring event management notifications through APIs
IT Service Management (ITSM) integration	The ITSM integration minimizes the need for handoffs, deduplicates issues, and optimizes processes for proactive insights and faster remediation. Out-of-the-box integration exists with ServiceNow. The generic APIs exposed by the Cisco DNA Center platform enable partners and developers to integrate with any ITSM system.
IP Address Management (IPAM) integration	This integration allows for a seamless import of IP pools for Cisco DNA Center workflows from external IPAM systems and the synchronization of IP pool and subpool usage information between the two systems. Out-of-the-box integration exists with Infoblox and BlueCat. The Cisco DNA Center platform provides generic APIs to integrate with any IPAM system.
Events and notifications	The Cisco DNA Center platform webhooks allow third-party applications to receive notifications and listen to any events detected by Cisco DNA Assurance, automation, and other task-based operational workflows.
Multivendor SDK	The Cisco DNA Center Multivendor Device Pack SDK allows partners to add support for managing third-party devices directly through Cisco DNA Center.

Meraki integration

For existing Meraki branch customers who want to explore using Cisco DNA Center and the Cisco Catalyst 9000 family switches, or for customers with mixed environments, Cisco DNA Center offers a single management pane of glass. This is an API-driven dashboard integration that supports all existing Meraki hardware and software at no additional license cost.

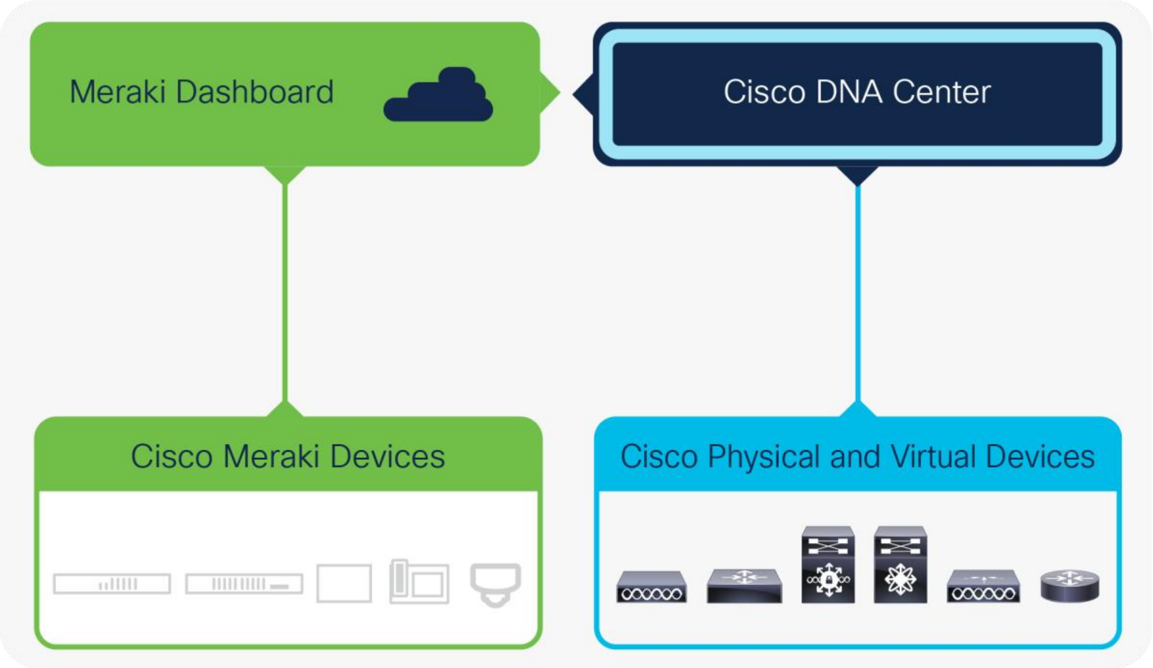


Figure 4.
Meraki and Cisco DNA Center integration

Features and benefits of Meraki integration

- Single dashboard inventory across all platforms (Meraki, Cisco Catalyst, Cisco Integrated Services Routers [ISRs], Aironet)
- Up-or-down status of all devices in a single platform
- Use existing Meraki API keys; no additional license required
- Combined topology mapping of hybrid environments
- Ability to assign SSIDs to Meraki access points from within Cisco DNA Center (Release 2.2.2.0 and later)

Appliance scale

The second generation (Gen2) of the Cisco DNA Center appliance is available in three form factors and comes with the Cisco DNA Center image preloaded and ready for installation. The entry-level Gen2 appliance (DN2-HW-APL) has the same size, performance, and capacity specifications as the first-generation (Gen1) Cisco DNA Center appliance (DN1-HW-APL). The reason for the change is to put all three Gen2 appliances on the newer Cisco UCS® M5 series of servers. If you currently have a Gen1 appliance (based on the Cisco UCS M4 series), there is no need to upgrade, and there is no advantage to upgrading, since both Gen1 and Gen2 entry appliances are based on the same 44-core processing units, have the same performance specifications, and support the same capacity of devices, sites, and IP pools. Customers looking for greater performance and capacity are advised to upgrade to the 56-core "midsize" Gen2 appliance (DN2-HW-APL-L) or the 112-core "large" Gen2 appliance (DN2-HW-APL-XL). The appliance DN1-HW-APL is currently end of life (no longer being sold); software maintenance ends in June 2022.

Table 14 captures the scale information for Cisco DNA Center 2.2.2.0.

Table 14. Scale and hardware specifications

	DN2-HW-APL[*]	DN2-HW-APL-L	DN2-HW-APL-XL
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[1] (switch, router, wireless controller)	1000	2000	5000
Number of wireless access points	4000	6000	13,000
Number of wireless sensors	600	800	1600
Number of concurrent endpoints	25,000	40,000	100,000[6]
Number of transient endpoints (over 14-day period)	75,000	120,000	250,000
Ratio of endpoints: wired wireless	Any Any	Any Any	Any Any
Number of elements in hierarchy / on single site (inclusive of areas, buildings, and floors)	500	1000	2000
Number of wireless controllers	500	1000	2000

	DN2-HW-APL[*]	DN2-HW-APL-L	DN2-HW-APL-XL
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**
Number of ports[2]	48,000	192,000	480,000
API rate limit	50 APIs/min	50 APIs/min	50 APIs/min
Netflows	30,000 flows/sec	48,000 flows/sec	250,000 flows/sec
Cisco DNA Center SD-Access scale			
Number of fabric domains	10	20	20
Number of fabric sites	500	1000	2000
Number of access points	4000	6000	12,000
Cisco DNA Center per fabric site scale			
Number of virtual networks	64/site	64/site	256/site
Fabric devices per fabric site[3]	500/site	600/site	1000/site
Number of scalable groups	4000	4000	4000
Number of access contracts	500	500	500
Number of group-based policies	25,000	25,000	25,000
Number of IP pools per site[5]	100	300	1000

Notes:

[*] Capacity for the older DN1-HW-APL is identical to the DN2-HW-APL.

[1] A switch stack of any number of switches counts as a single device.
A StackWise Virtual pair is counted as a single device.
A Virtual Switching System (VSS) pair is counted as a single device.
A WLC HA SSO pair is counted as a single device.

[2] Includes all physical ports except the console ports.
Includes Redundancy Ports (RPs) on WLCs.

[3] Cisco DNA Center supports 13,000 access points, but Cisco SD-Access supports 12,000 access points.

[4] If any Cisco DNA Center scale parameter (for example, endpoints) maxes out in a single-fabric site, the deployment cannot be further scaled with additional fabric sites. Cisco DNA Center Release 1.3.1.0 and later supports tracking up to only 1.2 million separate interfaces on the managed devices. Interfaces include physical and virtual interfaces such as Switched Virtual Interfaces (SVIs), loopbacks, dot1Q, tunnels, LISP, and so on.

[5] A single site can max out the IP pools supported.

[6] For three-node DN2-HW-APL-XL only, release 2.2.2.3 or later, capacity is increased as follows:

Number of concurrent endpoints increases to 200,000.
Number of transient endpoints increases to 500,000
Total port support is 1,500,000, of which 480,000 are physical ports and 1,020,000 are logical ports.

Appliance specifications

The Cisco DNA Center appliance is available in three form factors and comes with the Cisco DNA Center image preloaded and ready for installation. For more information on these Cisco UCS appliances, click the data sheet link beside each hardware series in Table 15.

Table 15. Physical specifications

Physical specifications	DN2-HW-APL and DN2-HW-APL-L	DN2-HW-APL-XL
Part number for ordering	DN2-HW-APL and DN2-HW-APL-L	DN2-HW-APL-XL
Hardware series	UCSC-C220-M5SX (data sheet)	UCSC-C480-M5 (data sheet)
Power supply	Dual 770W AC	Hot-pluggable, redundant 1600W AC
Physical dimensions (H x W x D)	Height: 1.7 in. (4.32 cm) Width: 16.89 in. (43.0 cm); including handles: 18.98 in. (48.2 cm) Depth: 29.8 in. (75.6 cm); including handles: 30.98 in. (78.7 cm)	Height: 6.9 in. (17.6 cm) Width: 19 in. (48.3 cm) Depth including handles and power supplies: 32.7 in. (83.0 cm)
Temperature: operating	1° to 95°F (5° to 35°C) Derate the maximum temperature by 1°C per every 1000 ft. (305 m) of altitude above sea level.	1° to 95°F (5° to 35°C) Derate the maximum temperature by 1°C per every 1000 ft. (305 m) of altitude above sea level.
Temperature: nonoperating	-40° to 149°F (-40° to 65°C)	-40° to 149°F (-40° to 65°C)
Humidity: operating	10% to 90%, noncondensing at 82°F (28°C)	10% to 90%, noncondensing at 82°F (28°C)
Humidity: nonoperating	5% to 93% at 82°F (28°C)	5% to 93% at 82°F (28°C)
Altitude: operating	0 to 3000 m (0 to 10,000 ft)	0 to 3000 m (0 to 10,000 ft)
Altitude: nonoperating	0 to 12,192 m (0 to 40,000 ft)	0 to 12,192 m (0 to 40,000 ft)
Network and management I/O	Supported connectors: One 1-Gigabit Ethernet dedicated management port Two 1-Gigabit BASE-T Ethernet LAN ports One RS-232 serial port (RJ-45 connector) One 15-pin VGA2 connector Two USB 3.0 connectors One front-panel KVM connector that is used with a KVM cable, which provides two USB 2.0s, one VGA, and one serial (DB-9) connector	Supported connectors: One 1-Gigabit Ethernet dedicated management port Two 1-Gigabit BASE-T Ethernet LAN ports One RS-232 serial port (RJ-45 connector) One 15-pin VGA2 connector Three USB 3.0 connectors One front-panel KVM connector that is used with a KVM cable, which provides two USB 2.0s, one VGA, and one serial (DB-9) connector

Physical specifications	DN2-HW-APL and DN2-HW-APL-L	DN2-HW-APL-XL
Regulatory standards compliance: Safety and EMC		
Regulatory compliance	Products should comply with CE Markings according to directives 2004/108/EC and 2006/95/EC	
Safety	NEBS • UL 60950-1 Second Edition • CAN/CSA-C22.2 No. 60950-1 Second Edition • EN 60950-1 Second Edition • IEC 60950-1 Second Edition • AS/NZS 60950-1 • GB4943	
EMC: Emissions	• 47CFR Part 15 (CFR 47) Class A • AS/NZS CISPR22 Class A • CISPR22 Class A • EN55022 Class A • ICES003 Class A • VCCI Class A • EN61000-3-2 • EN61000-3-3 • KN22 Class A • CNS13438 Class A	
EMC: Immunity	• EN55024 • CISPR24 • EN300386 • KN35 KN24	

Fabric VN scale

Table 16 captures the fabric VN limits for devices in the fabric when deploying Cisco DNA Center Release 2.2.2.0.

Table 16. Fabric VN limits (The current maximum VRF validation is based on a lower limit of 1 and an upper limit of 128, even if the device can support more than 128.)

Device series	Max VRFs
Cisco Catalyst 3650 Series Switches	64
Cisco Catalyst 3850 Series Switches	64
Cisco Catalyst 4500 Series Switches	64
Cisco Catalyst 6800 Series Switches	1000 (128)
Cisco Catalyst 6500 Series Switches	1000 (128)
Data center switches (Cisco Nexus 7000 Series Switches)	4000 (128)

Device series	Max VRFs
Cisco Cloud Services Router 1000V Series	4000 (128)
Cisco ASR 1000 Series Aggregation Services Routers	4000 (128)
Cisco 4000 Series Integrated Services Routers	4000 (128)
Cisco 4400 Series Integrated Services Routers	4000 (128)
Cisco 4200 Series Integrated Services Routers	4000 (128)
Cisco 4300 Series Integrated Services Routers	4000 (128)
Cisco Catalyst 9300 Series Switches	256
Cisco Catalyst 9300 L Series Switches	256
Cisco Catalyst 9500 Series Switches	256
Cisco Catalyst 9500H Series Switches	256
Cisco Catalyst 9400 Series Switches	256
Cisco Catalyst 9200-L Switch Stack	1
Cisco Catalyst 9200 Switch Stack	4
Cisco Catalyst 9200-24PB Switch	32
Cisco Catalyst 9200-48PB Switch	32
Cisco Catalyst 9600 Series Switches	256

Roles and privileges

Table 17. Role-based access control

Role	Privilege
Network-Admin-Role	Users with this role have full access to all of the network-related Cisco DNA Center functions. They do not have access to system-related functions, such as application management, users (except for changing their own passwords), and backup and restore.
Observer-Role	Users with this role have view-only access to all Cisco DNA Center functions.
Telemetry-Admin-Role	Users with this role have the ability to perform system-level functions within Cisco DNA Center.
Super-Admin-Role	Users with this role have full access to all of the Cisco DNA Center functions. They can create other user profiles with various roles, including those with the Super-Admin-Role.

Device Support

Cisco DNA Center provides coverage for Cisco enterprise switching, routing, and mobility products. For a complete list of Cisco products supported, download our support spreadsheet, which is regularly updated:

https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-device-support-tables-list.html

Cisco environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environment Sustainability" section of Cisco's Corporate Social Responsibility (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the "Environment Sustainability" section of the CSR Report) are provided in the following table.

Links to information about key environmental sustainability topics

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance

Reference links to **product-specific environmental sustainability information** that is mentioned in relevant sections of this data sheet are provided in the following table.

Table 18. Links to product-specific environmental sustainability information

Sustainability topic	Reference
General	
Product compliance	Safety and compliance information
Power	
Power supply	Power supplies and typical and maximum power specifications
Material	
Dimensions	Physical dimensions

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

Product usage telemetry

Product usage telemetry provides valuable information about the status and capabilities of the Cisco DNA Center appliance. 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 who have deployed Cisco DNA. Collecting this data helps the product teams serve customers better. This data and related insights enable Cisco 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.

All product usage telemetry data is transmitted to Cisco through an encrypted channel. The categories of data collected in the product usage telemetry are the Cisco.com ID, system telemetry, feature usage telemetry and network device (for example, switch or router) inventory, and license entitlement. The collection of product usage telemetry is enabled by default and cannot be disabled from the product. Customers may contact the Cisco Technical Assistance Center (TAC) for changes in collection settings.

For detailed product usage telemetry information collected, see the following table.

Table 19. Cisco DNA Center product usage telemetry usage and benefits*

Category	Data elements	Purpose of collection
Cisco.com	• Cisco.com user ID	Identify customer account
System	• Deployment information (Cisco DNA Center appliance serial number, Cisco DNA Center appliance platform, Cisco DNA Center appliance machine ID) • Connectivity with Cisco DNA Center • Operational metrics (CPU, memory, file system, uptime) for pods • Signed End-User License Agreement (EULA) flag • Application stack and packages deployed	Identify potential issues in customers' environments to prevent problems and improve the product
Feature usage	• Customer dwell time in application UI pages. • Site_member_details: name of site, instance UUID of device, support level of device, device family, host name. • Assurance usage: number of sites, area, building, floor, Wireless LAN Controller (WLC), switch, Access Point (AP), number of clients (wired and wireless) and health score, sensor counts, sensor tests count, AI network analytics configuration flag, AP count with RF stats enabled, number of anomaly captures enabled, number of data packet captures enabled, network telemetry max input rate (NetFlow, syslogs, traps). • SD-Access usage: number of fabrics created, number of fabric domains per domain type, number of devices per fabric role by site, number of edge nodes and of border nodes and of control-plane nodes by device type, number of clients on fabric, number of access contracts, number of scalable group tags, number of virtual networks by site, number of IP pools, number of SSIDs, Cisco Identity Services Engine (ISE) version and status, number of group-based policies, number of access policy contracts, number of Cisco ACI® scalable groups, number of APs and WLCs in fabric, number of each transit type, number of rogue AP/client messages, number of fabric sites by authentication mode, number of ports by static port assignment.	Facilitate customer adoption and customer value

Category	Data elements	Purpose of collection
	• Automation usage: number of devices provisioned using PnP, number of PnP devices by source, number of golden images and image repository details, number of successful/failed image activations and/or distributions, number of SMU images by type, number of application policies created and/or deployed, number of favorite applications, number of custom applications (sets), number of consumer applications, number of queueing profiles, number of excluded devices, number of devices in each policy, number of draft policies, number of policies using nondefault queueing profiles, device controllability check, site area/building/floor counts, number of SSA enablement/disablement tasks by status, number of SSA precheck failures by type and successes/failures per device family, Stealthwatch registration status, number of devices by SSA-enabled status, number of devices with security advisory match, number of security advisory scans, vManage integration status, MRE root cause analysis count and duration, number of MRE user feedbacks, number of devices with CVSS scores, number of devices by replacement status, WAB SDG node count, number of onboarding templates created and provisioned successfully on devices, number of devices with templates applied, number of network profiles by site and namespace. • DNACaaP usage: number of event subscriptions by state, DaaS-runtime usage.	
Network device inventory and license entitlement	• Network device inventory (serial number, software version, platform ID, reachability errors). Number of devices per device support level, number of devices per device role, number of port types per device type, IDP instances enabled, number of devices by Ethernet channel control method, number of devices by aclType associated site information, uptime in days by device type, host count by device type, number of devices by configuration type. • License entitlement information (network device type, IP address of network device, Cisco Smart Software Manager registration status, Cisco DNA Center subscription level, hardware support contract coverage, number of days until license expires).	Assist customers in tracking and maintaining license entitlement and renewals

For information on Cisco DNA Center privacy, see https://www.cisco.com/c/en/us/about/trust-center/data-privacy.html#~privacydatadocs.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital® makes it easier to get the right technology to achieve your objectives, enable business transformation, and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

For more information

See how Cisco DNA Center helps you move faster, lower costs, and reduce risk at https://cisco.com/go/dnacenter.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-739686-15 09/21