Cisco DNA Center 1.3

Contents

Improving your Network from a Single Control and Command Center

Cisco DNA Center is the foundational controller and analytics platform at the heart of Cisco's intent-based network for large and midsize organizations. 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.
- **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. Integration with 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. This improves IT operations by automating workflow processes based on network intelligence coming from Cisco DNA Center.

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 1.3

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. These subscriptions are available for 3-, 5-, or 7-year terms. Cisco allows customers to purchase complete Cisco DNA Center functionality through a Cisco DNA Advantage license subscription or limited functionality through a Cisco DNA Essentials license subscription. Customers may also benefit from Cisco's all-in-one software license, Cisco DNA Premier (formerly Cisco ONE). The Cisco DNA Premier license includes all Cisco DNA Advantage benefits plus the Cisco Identity Services Engine (ISE) for user identity policy and Cisco Stealthwatch for advanced security and Encrypted Traffic Analytics (ETA). All Cisco DNA Software license subscription options include Cisco SWSS (software support and downloads). The table below shows the main features included with the Cisco DNA Essentials, Cisco DNA Advantage, and Cisco DNA Premier licenses.

Table 1. Cisco DNA Center licensing overview

Cisco DNA Essentials Basic monitoring and automation	Cisco DNA Advantage All Cisco DNA Essentials features plus	Cisco DNA Premier All Cisco DNA Advantage features plus
Overall health dashboard	Time travel (14 days)	Cisco Stealthwatch with ETA
Network health dashboard	Cisco AI Network Analytics	Cisco ISE Base (identity policy)
Client health dashboard	360-degree health scores	Cisco ISE Plus (identity policy)
Application health dashboard	360-degree device view	
Predefined reports	Apple iOS insights	
Custom threshold KPIs	Active sensor tests	
Inventory	Wireless location heat maps	
Discovery	Guided remediation	
Topology	Custom reports	
Software image management (SWIM)	Third-party integrations	
Network Plug and Play provisioning	Application policy	
Network Functions Virtualization (NFV) provisioning	Software Maintenance Upgrade (SMU) patching	
Cisco Virtual Network Functions (VNF)	Software-Defined Access	

New features for Cisco DNA Center 1.3

Cisco is making intent-based networking smarter at scale with Cisco DNA Center 1.3. The latest release of Cisco DNA Center includes artificial intelligence and machine learning (AI/ML) functionality that reduces the number of trivial and noncritical alerts while highlighting more critical issues. The result is quicker resolution of issues and less time spent troubleshooting overall. In conjunction with this, Cisco DNA Center 1.3 boasts a four-times jump in scale, up to 100,000

connected clients and 18,000 network devices. In addition to this, the new v1.3 version has the latest innovations in kernel mode threat protection to the software image for increased security and uses the latest version of Kubernetes (K8s v1.14).

Cisco DNA Center's new increased capacity is supported by three different hardware appliances as follows:

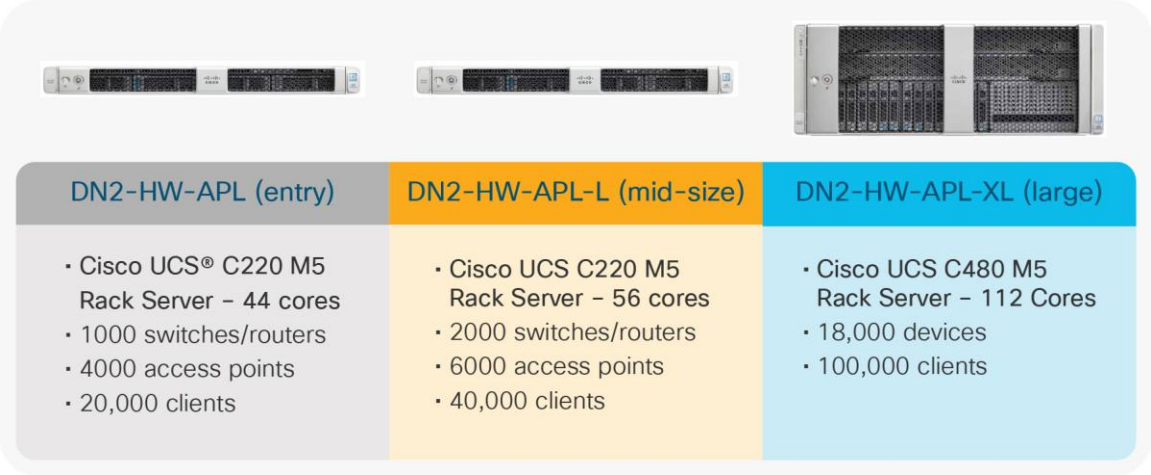

Figure 3.
Cisco DNA Center appliance options

Installation simplification includes a new web-based GUI and provides the ability to bring up a new Cisco DNA Center appliance in less time than before.

A new Prime Infrastructure migration tool gives IT teams the ability to import all maps and configurations from Prime Infrastructure to Cisco DNA Center and then to run Cisco DNA Center and Prime Infrastructure in parallel as they get familiarized with this new paradigm in network control and management.

Version 1.3 allows automated configuration of network switches for Stealthwatch and encrypted traffic analytics (ETA) — a task that used to require as much as 30-minutes per switch.

Cisco DNA Center 1.3 provides enhancements and new technologies that allow intent-based networking to grow faster and smarter.

Below is a more complete list of the major upgrades in Cisco DNA Center 1.3:

Feature	Description and benefits
Cisco AI Network Analytics	Using AI and machine learning, Cisco AI Network Analytics drives intelligence in the network, empowering administrators to accurately and effectively improve performance and issue resolution. We are taking network analytics to a new level where noise and false positives are significantly reduced when enabling customers to accurately identify issues, trends, anomalies, and root causes.
AI-driven baselining (on premises)	A set of ML features that enable network administrators to accurately identify, understand, and troubleshoot the most important issues in their network. This feature runs on the AI/ML engine that is located on the Cisco DNA Center appliance on site.
New entry appliance (44 cores)	A more powerful version of the existing Cisco DNA Center appliance. This appliance has the same device and client capacity as the previous version, but has additional power to support current and future on-device AI/ML capabilities. Capacity for this device: 5,000 wired devices (1000 switch/router/WLCs - 4000 APs) 20,000 concurrent clients (8000 wired clients, 12,000 wireless clients)

Feature	Description and benefits
Mid-size appliance (56 cores)	8000 wired devices (2000 switch/router/WLCs - 6000 APs) 30,000 concurrent clients (12,000 wired clients, 18,000 wireless clients)
Large-size appliance (112 cores)	18,000 wired devices (5000 switch/router/WLCs - 13,000 APs) 100,000 concurrent clients (40,000 wired clients, 60,000 wireless clients)
Application policy support for SDA	This feature extends application policy to an SDA overlay network. Packets are classified and marked on the underlay and copied to the overlay within an SDA network. Application policy works seamlessly on switches that are part of the SDA fabric.
Intelligent capture	Intelligent capture uses network sensors within the Aironet Active Sensor and the Aironet 4800 AP to provide advanced troubleshooting for wireless issues. Includes anomaly-based packet captures, on-demand RF scanning, real-time client location, and Wi-Fi application analytics. 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. Allows system administrators to prepare for special events, VIP visits, or simply to troubleshoot a stubborn wireless issue.
Media application monitoring	Ability to monitor using Perfmon processing for Real-Time Protocol (RTP) streams. This allows teams to verify the quality of critical real-time applications.
URL monitoring	Allows Cisco DNA Assurance to have visibility into cloud-based (URL-based) applications and their performance and feeds information into Cisco DNA Center's "Application Experience" feature so that cloud-based application performance is optimized.
Prime to DNA Center migration tool	Tool within Prime Infrastructure that pushes configurations (design, maps, inventory, and AP licenses) to Cisco DNA Center.
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, oilfields, mining, and outdoor video surveillance.
IPv6 endpoint support	This feature introduces the capability to support IPv6 wired and wireless endpoints that are dual stacked.
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.

Telemetry data collection: The Cisco DNA Center service is configured to automatically connect and transmit telemetry data, in near real time, to Cisco. Telemetry information will be used by Cisco to improve network lifecycle management for IT teams who have deployed Cisco DNA. It uses aggregated analytics to proactively identify potential issues in networks to prevent future problems, improve managed services and support, facilitate adoption of new features that result in increased value, and assist IT teams in tracking and maintaining license entitlement and renewals, while at the same time helping Cisco improve our products. Telemetry information is transported securely to keep customer data private. Data collected includes network device inventory information (such as serial numbers and IP addresses), network device license information (such as license entitlement and software version), and feature usage data. Users may opt out of data collection by turning this feature off in the "Cisco DNA Center Settings" menu. For detailed telemetry information, please see Table 2.

Table 2. Cisco DNA Center telemetry usage and benefits

Data collected	Telemetry usage and benefits
• Deployment information (Cisco DNA Center appliance serial number, Cisco DNA Center appliance platform, Cisco DNA Center appliance machine ID) • Feature usage (application stack deployment and usage, workflow hierarchy, dwell time in applications, connectivity with Cisco DNA Center)	Identify potential issues in customers' environments to prevent problems and improve the product
• Customer identity (Cisco.com ID) • Feature usage (application stack deployment and usage, workflow hierarchy, dwell time in applications, connectivity with Cisco DNA Center) • License entitlement information (hardware support contract coverage)	Provide managed services and support
• Customer identity (Cisco.com ID) • License entitlement information (Cisco Smart Software Manager registration status, Cisco DNA Center subscription level, number of days until license expires)	Facilitate customer adoption and customer value
• Network device inventory (serial number, software version, platform ID, reachability errors) • 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 more detailed information please refer to Cisco's Personal Data Privacy page:

https://www.cisco.com/c/en/us/about/trust-center/data-privacy.html#~privacydatadocs

Cisco DNA Center 1.3 feature descriptions

Cisco DNA assurance detailed feature description

Table 3. 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, Cisco and Meraki®. Provides the top 10 global issues and allows administrator to expand views by geographical site, device list, client list, or

Feature	Description and benefits
	topology.
Network health dashboard	General overview of the operational status of every network device connected to Cisco DNA Center. Any poorly connected devices or communication issues will be highlighted, with suggested remediation.
Client health dashboard	General overview of the operational status of every client connected to Cisco DNA Center. Any poorly connected clients or communication issues will be 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 all Aironet Active Sensors on the network. Shows overall tests, connectivity statistics, and top wireless issues discovered by sensors. Includes test results for Received Signal Strength Indicator (RSSI), Signal-to-Noise Ratio (SNR), Dynamic Host Configuration Protocol (DHCP), DNS, host reachability, RADIUS, email, 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 [KPI], events) • Event-driven notifications
Device 360 and Client 360	An Assurance feature allowing viewing of device or client connectivity from any angle or context. Included are information on topology, throughput, and latency from different times and applications. Gives a detailed view of any device or client performance over time and from any application context. Provides for very granular troubleshooting in seconds. • History of performance for each user device • Proactive identification of any issues affecting the user experience • Connectivity graph with health score of all devices on the path • Application experience • Device 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 on 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 re-create the issue in a lab. • Rewind time to when the issue occurred • History shows critical events • All the information on the user or network device changes to the selected time
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 that rely on them.
Wi-Fi Analytics for Apple iOS	A joint development with Apple, Wi-Fi Analytics for Apple iOS offers Cisco DNA Assurance insights

Feature	Description and benefits
clients	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 iOS 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) ◦ RSSI ◦ Channel number • Provides clarity regarding the reliability of connectivity ◦ Client reasons, such as error codes for last disconnection
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. Allows users the performance they need on the applications key to their company role.
Proactive network insights	Network insights for issues affecting performance, reliability, or security. Detailed drill-downs to identify impacts quickly. Guided remediation to resolve issue.
Application policy support for SDA	This feature extends application policy to an SDA overlay network. Packets are classified and marked on the underlay and copied to the overlay within an SDA network. Application policy works seamlessly on switches that are part of the SDA fabric.
Intelligent Capture	Intelligent Capture uses network sensors within the Aironet Active Sensor and the Aironet 4800 AP to provide advanced troubleshooting for wireless issues. Includes anomaly-based packet captures, on-demand RF scanning, real-time client location, and Wi-Fi application analytics. 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. Allows system administrators to prepare for special events, VIP visits, or simply to troubleshoot a stubborn wireless issue.
Media application monitoring	Ability to monitor using Perfmon processing for Real-Time Protocol (RTP) streams. This allows teams to verify the quality of critical real-time applications.
URL monitoring	Allows Cisco DNA Assurance to have visibility into cloud-based (URL-based) applications and their performance and feeds information into Cisco DNA Center's "Application Experience" feature so that cloud-based application performance is optimized.
Cisco AI Network Analytics	Using AI and machine learning, Cisco AI Network Analytics drives intelligence in the network, empowering administrators to accurately and effectively improve performance and issue resolution. We are taking network analytics to a new level where noise and false positives are significantly reduced when enabling customers to accurately identify issues, trends, anomalies, and root causes.
AI-driven baselining (on-premises)	A set of ML features that enable network administrators to accurately identify, understand, and troubleshoot the most important issues in their network. This feature runs on the AI/ML engine that is located on the Cisco DNA Center appliance on site.

List of correlated insights

Table 4. Correlated insights

Category	Insights
Wireless issues	**Client onboarding** • Association failures

Category	Insights
	• 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 • 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

Category	Insights
	• 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
Switching issues (non fabric)	**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

Category	Insights
	Switch • CPU, memory, temperature • Line card • Modules • PoE power • TCAM table

Cisco DNA automation detailed feature description

Table 5. 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 • Link Layer Discovery Protocol (LLDP) for endpoints • IP Device Tracking (IPDT) and 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 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, IP address pool, etc., 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) as well. 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
Software Image Management	Manages software upgrades and controls the consistency of image versions and configurations

Feature	Description and benefits
(SWIM)	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 to 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.
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 flex or centralized wireless deployment • PnP provisioning for APs • IP ACL support • Access and access control policy for SD-Access Wireless only
Device tagging	An administrator can tag network devices in order to associate devices that share a common attribute. For example, you can create a tag and use it to group devices based upon 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

Feature	Description and benefits
	devices in healthcare, as well as for business-critical applications such as video in customer experience centers or voice in support sites.

Cisco Software-Defined Access (SD-Access) 1.3 key features

Table 6. SD-Access features and description

Feature	Description
Fabric infrastructure	• Automated external connectivity handoff using Virtual Routing and Forwarding Lite (VRF-Lite), and BGP Ethernet VPN (BGP-EVPN)
Fabric assurance	• KPIs, 360-degree views for client, AP, wireless 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 and control plane and wireless guest support as separate Virtual Network (VN) on enterprise border and control plane • Same SSID for traditional and fabric on same WLC (mixed mode) • WLC Stateful Switchover (SSO) • Wireless multicast
Management	• Pre-check and post-check workflow validations • ISE Primary Administration Node (PAN) High Availability (HA) support (includes pxGrid, 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 Command-Line Interface (CLI) configuration • Software image and patch management • License management • Backup and restore • Task scheduler
Distributed campus	• Automated intersite connectivity • End-to-end policy and segmentation
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
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, audio-visual equipment, etc.

Feature	Description
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, oilfields, mining, and outdoor video surveillance.
IPv6 endpoint support	This feature introduces the capability to support IPv6 wired and wireless endpoints that are dual stacked.

For more details on Software-Defined Access, visit SD-Access solution on Cisco.com.

Cisco DNA Center system capabilities

Table 7. System capabilities

Feature	Description and benefits
Role-Based Access Control (RBAC)	Allows users to be mapped to one of the four predefined roles. The role determines what types of operations a user can perform within 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.

Cisco DNA Center platform capabilities

Table 8. 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, network topology • SWIM, Plug and Play (PnP) • Template programmer, command runner • Assurance: Site, device, and client health monitoring, path trace • NFV provisioning
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

Feature	Description and benefits
	third-party devices directly via Cisco DNA Center.

Meraki Visibility in Cisco DNA Center

For existing Meraki branch customers who want to explore using Cisco DNA Center and Cisco Catalyst® 9000 family switches, or for customers with mixed environments, Cisco DNA Center now 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.

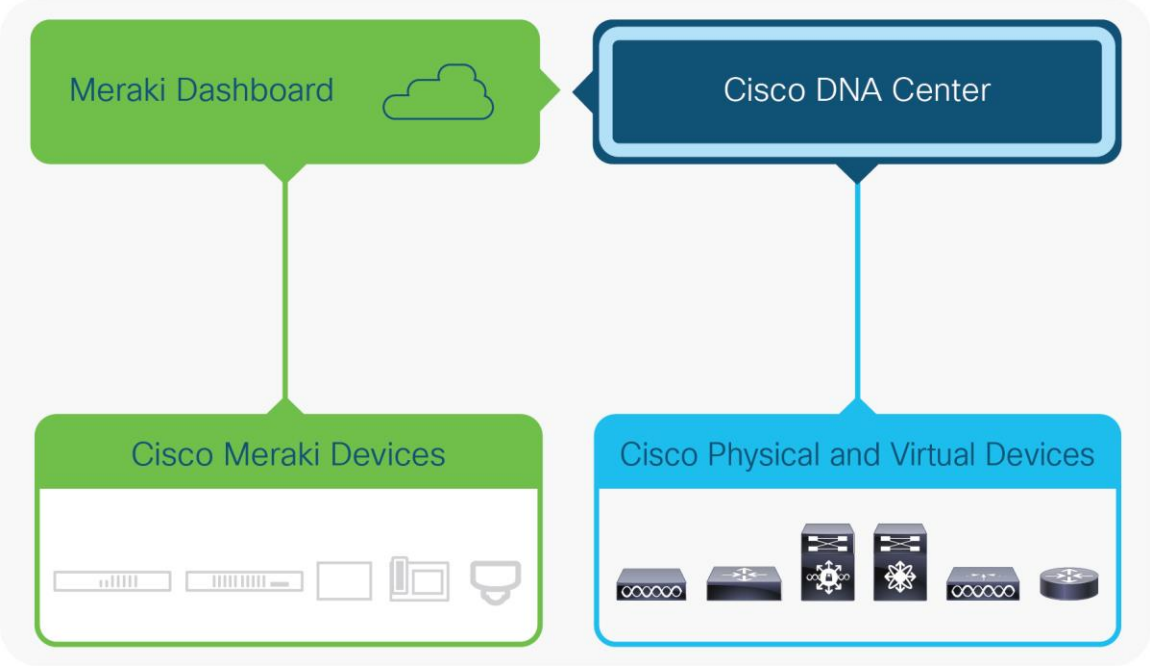

Figure 4.
Meraki and Cisco DNA Center integration

Features and benefits

- 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

Cisco DNA Center 1.3 appliance: scale and hardware specifications

The new second generation (Gen2) of Cisco DNA Center appliance is available in three form factors and comes with the Cisco DNA Center image preloaded on it and ready for installation. Notice that 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 "M5 Series" UCS. If you currently have a Gen1 appliance (based on the "M4 Series" UCS), there is no need to upgrade, and there is no advantage to upgrading since both Gen1 and Gen2 entry appliances are based on 44 core processing units. Customers looking for greater performance, in order to support more capacity, are advised to upgrade to the 56 core "mid-size" Gen2 appliance (DN2-HW-APL-L) or the 112 core "large" Gen2 appliance (DN2-HW-APL-XL).

Figure 5 captures the scale information for Cisco DNA Center Release 1.3.

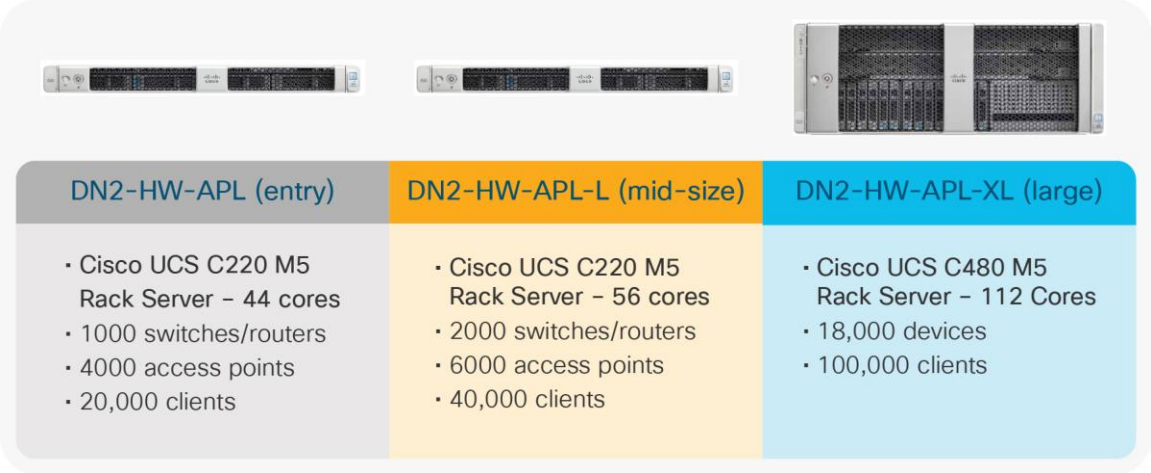

Figure 5.
Scale and hardware specifications

Cisco DNA Center appliance physical specifications

Table 9 shows the three different appliance specifications.

Table 9. Physical specifications

Part number for ordering	DN2-HW-APL and DN2-HW-APL-L	DN2-HW-APL-XL
Hardware series	UCSC-C220-M5SX	UCSC-C480-M5
Power supply	Dual 770W AC	Dual 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 2.0, 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 2.0, one VGA, and one serial (DB-9) connector

Cisco DNA Center 1.3 device-aware fabric VN limit (fabric VN scale)

Table 10 captures the fabric VN limits for devices in the fabric when deploying Cisco DNA Center Release 1.3.

Table 10. 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)
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)

Device series	Max VRFs
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 (128)
Cisco Catalyst 9500 Series Switches	256 (128)
Cisco Catalyst 9500H Series Switches	256 (128)
Cisco Catalyst 9400 Series Switches	256 (128)
Cisco Catalyst 9200-L Series Switches	1
Cisco Catalyst 9200 Series Switches	4

Roles and privileges

Table 11. 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, please 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 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: 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 USAs

C78-739686-07 06/19