Tel: +44 (0)1279 408 777
Email: sales@gocomsys.com
Website: www.gocomsys.com

Refurbished CISCO DN1-HW-APL Datasheet

CISCO > CLOUD-SYSTEMS-MANAGEMENT

Cisco DNA Center

Cisco DNA Center New Features for Release 1.3.3.0

Analytics and Assurance	
Samsung client analytics phase 1	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 AP neighbor map view, enhanced day-0 Cisco DNA Center discovery, and dedicated wireless backhaul 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 now also simulate the guest onboarding experience in ISE Once the tests are set up, customers now have the ability to centrally monitor them from the newly built heatmap-based sensor dashboard that can help pinpoint sites having problem and then drill down to specific locations where more client onboarding is failing or where there is poor RF coverage, using location heatmaps and Sensor 360 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
Executive summary report	Weekly and daily report providing 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 the comparison and change against 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
Automation	
Rogue management	Support for Cisco Catalyst 9800 Series Wireless Controller rogue management within Cisco DNA Center. This extends the same capabilities to detect rogues that are supported on AireOS WLCs, including detection of honeypots and on-wire rogues, to the Cisco Catalyst 9800 Series.
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 now 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 certificate during Plug and Play device claim. With this feature the customer will be able to 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 via Cisco DNA Center. This feature allows Meraki access points to be assigned SSIDs via 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.

Security	
Authentication enhancements	Users can now change authentication mode from open to closed without having to remove the device from the fabric The site-specific authorization template will enable customers to have a unique template for each site and continue to have a global authorization template Critical VLAN will not be pushed by default via Cisco DNA Center templates. Seamless authorization changes will provide granularity and allow the user to make authentication changes without removing the device from the fabric Users can have different authentication templates based on the deployment model If the ISE goes down, the customer will 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 will be a unique multicast group per site. The blast radius of Layer 2 flood is contained within this unique multicast group.
SD-Access: StackWise Virtual Link (SVL) border and edge	SVL support has been added on edge and border nodes. Base automation will discover manually configured SVL devices. The user can configure fabric roles such as edge/border or border + edge (B +E). SVL not only brings physical redundancy but also provides dual homing to the devices/servers connected to the border/edge. With B+E (non-colocated) control plan users can connect servers at the border.
Multicast enhancement for Cisco Vision: Custom source-specific multicast (SSM) and external rendezvous point (RP)	With external RP automation workflow and custom SSM range, users can now 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.
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 extended node 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 will add value for customers who want to leverage micro segmentation. Extended nodes will have multicast support. IoT devices such as surveillance devices can join multicast groups. The source and receiver can be hanging off of extended nodes.
SD-Access: New devices (Shockley, Hyper-V-WLC, IW3700, Axel, Duplo)	Support for Shockley, Hyper-V-WLC, IW3700, Axel, and Duplo has been added to SD-Access.
Airgap support	Customers now have the ability to install or upgrade to the latest software versions in an airgap (when the appliance is not connected to the public network/Internet). This enables a customer to update/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.

Cisco DNA Assurance Features and Benefits

Feature	
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 administrator 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 will be 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 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 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, 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 and troubleshooting device or client from any angle or context. Included are 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 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.
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 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, office traffic load, etc. 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. The addition of an intelligent machine reasoning engine (MRE) allows for further intelligence in Cisco DNA Center. Included is the ability to discover Layer 2 spanning tree loops in your non-fabric (legacy Layer 2) network. Additionally, the MRE will scan current switch inventory for outdated images, PSIRT alerts, and suspicious configurations. These abilities are outlined further below under “AI Analytics Security Advisories.”
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 will have a complete view of application visibility across the campus network infrastructure.
Wi-Fi Analytics for Apple iOS clients	A joint development with Apple, Wi-Fi Analytics for Apple iOS 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 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) Received Signal Strength Indicator (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. 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.

Correlated insights

Category

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 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

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

Cisco DNA Automation features and benefits

Feature	
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 (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 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.
Device replacement and RMA workflows	Workflow templates allow for the replacement (RMA) of a switch and router. Includes restoration of IOS, configuration and license. 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 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 devices in healthcare, as well as for business-critical applications such as video in customer experience centers or voice in support sites.

SD-Access Features and Description

Feature	
Fabric infrastructure	Automated external connectivity handoff using Virtual Routing and Forwarding Lite (VRF-Lite), and BGP Ethernet VPN (BGP-EVPN) Fabric in a box without control plane Bonjour support for Cisco SD-Access
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 Multiple virtual networks 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, 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 Group-Based Access Control Policies
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 Border handoff enhancements: 4-byte ASN support Two fabrics in a box at a site are supported without embedded wireless Lan Automation support for 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, audio-visual equipment, etc. 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, 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.
Group-based policy	A major new 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 address or VLANs. IT teams can create and manage SGTs from within Cisco DNA Center without having to open ISE or other network policy servers. Scale for group-based policy is as follows: Up to 4000 scalable groups Up to 500 access contracts Up to 25,000 policies
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 your third-party NPS, or Cisco ISE – the choice is yours.
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 a security advisory or security advisories. Identifying security advisories is a very time-consuming task that can be automated through the advanced MRE technology.
NetFlow automation for Encrypted Traffic Analytics (ETA) support	In order for Stealthwatch to be able to detect malware in encrypted traffic, network devices must be configured to send NetFlow and encrypted traffic to Stealthwatch. This new 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.

System capabilities

Feature	
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.

Platform capabilities

Feature	
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 third-party devices directly via Cisco DNA Center.

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	
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)
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

Role-based access control	
Role	
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.

The next steps...

ORDER NOW

VIEW ONLINE

Tel: +44 (0)1279 408 777

Email: sales@gocomsys.com

Website: www.gocomsys.com