The bridge to possible

Cisco DNA Center 2.2.3

Contents

Introduction

We are excited to announce the Cisco DNA Center 2.2.3 release and General Availability (GA). Cisco DNA Center 2.2.3 continues our journey to modernize the network operating and security model for our customers. This release brings some exciting innovations to help our customers:

Lower the cost of management

- Scale up with 3X endpoint capacity increase to meet the explosion of IoT and mobile devices using existing network infrastructure

Improve operational efficiency of network operations

- Create and visualize WLAN designs with immersive 3D analyzer to maximize wireless network performance
- Conduct deep packet and path trace analysis that include KPIs with True Trace
- Monitor, troubleshoot and improve Cisco WebEx performance from Cisco DNA Center console

Improve security with Zero Trust architecture improvements

- Enable faster policy issue resolution through a new Policy Analytics dashboard
- Make endpoint security policy updates quickly and confidently with an improved and more comprehensive Trust Score

In this release announcement, you will find feature overviews and details regarding the Cisco DNA Center release methodology and terminology and useful links to additional reference documents.

AIOps with Cisco DNA Assurance and Analytics

Wireless 3D Analyzer

Wireless coverage issues can be challenging to identify and locate. Currently available 2D wireless heat maps do not give a true representation of Wi-Fi signal propagation through actual building materials and architectural designs.

The new Wireless 3D Analyzer provides granular analysis of millions of spatial RF data points and the ability to visualize wireless coverage. Network operators can identify the most impacted area by RF strengths, simulate different RF environments, and conduct spatial planning and prediction of the interior environment. After loading basic architectural structural information, network operators can enter a virtual office space and move an access point or create an imaginary wall and see the resulting impact on Wi-Fi signal propagation. The Wireless 3D Analyzer helps network operators maximize WLAN performance and identify trouble spots and WLAN design issues faster.

Application QoS (quality of service) support for industrial switches

The proliferation of IoT devices extends to industrial environments, and Cisco® ruggedized industrial switches can be found deployed in manufacturing facilities and other industrial environments. Setting bandwidth allocations is currently a cumbersome manual process. If a network operator wants to write a QoS policy for an IoT device, they have to not only understand the queuing model for that device but also map the QoS settings among other platforms on their network to manage the end-to-end QoS.

In Cisco DNA Center 2.2.3, network operators can author and push QoS policies to Cisco Catalyst® IE3300 and IE3400 Series Switches from Cisco DNA Center's Application QoS. They can apply default QoS trust settings as well as queuing settings based on Cisco Validated Designs, or they can write a custom QoS policy for these devices. This removes the complexity of pushing a QoS policy and helps organizations ensure a good experience for end users in industrial environments.

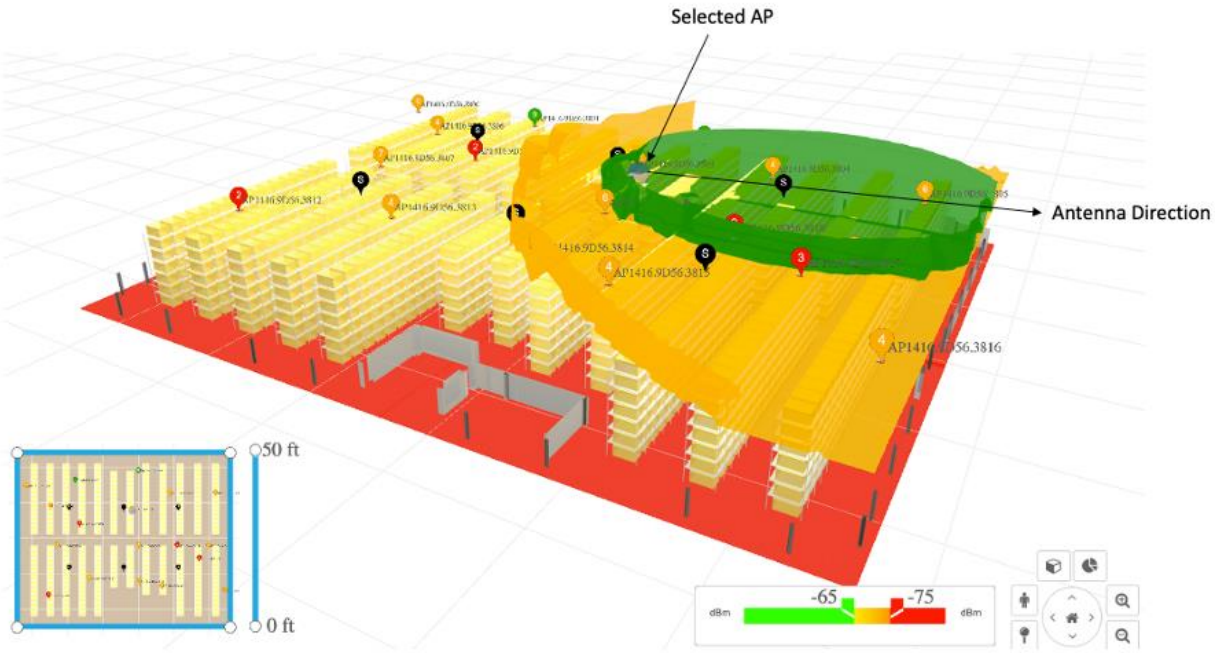

Figure 1.
Wireless 3D Analyzer

Webex integration with Cisco DNA Center

The unprecedented shift to remote work has made Cisco Webex® a critical productivity enabler for businesses. Troubleshooting Webex performance issues has become a top priority for IT. Currently, network operators must switch between the Webex and Cisco DNA Center user interfaces to resolve issues.

The Webex Integration provides visibility into the performance of the Webex application by integrating the quality metrics into the Cisco DNA Center Client 360 feature. The integration enables consolidation of quality metrics for audio and video and for sharing components with NetFlow to provide administrators with a single pane of glass for troubleshooting WebEx performance. Network operators can quickly identify and resolve issues in Cisco DNA Center without having to switch between multiple interfaces.

Access point reports with 12-month data retention

Reporting enables network operators to understand and communicate the enterprise network performance with key stakeholders in their organization. Historical reports offer valuable information for network operators, IT executives, and CIOs as they use this information to plan and implement network enhancements and upgrades.

Cisco DNA Center 2.2.3 provides new client trend and access point Key Performance Indicator (KPI) reports that have data retention periods of up to 12 months and empower network operators to track and measure their wireless network performance. These new reports enable network operators to adjust wireless capacity on their networks and view seasonality and longer-term patterns to improve their wireless planning and budgeting.

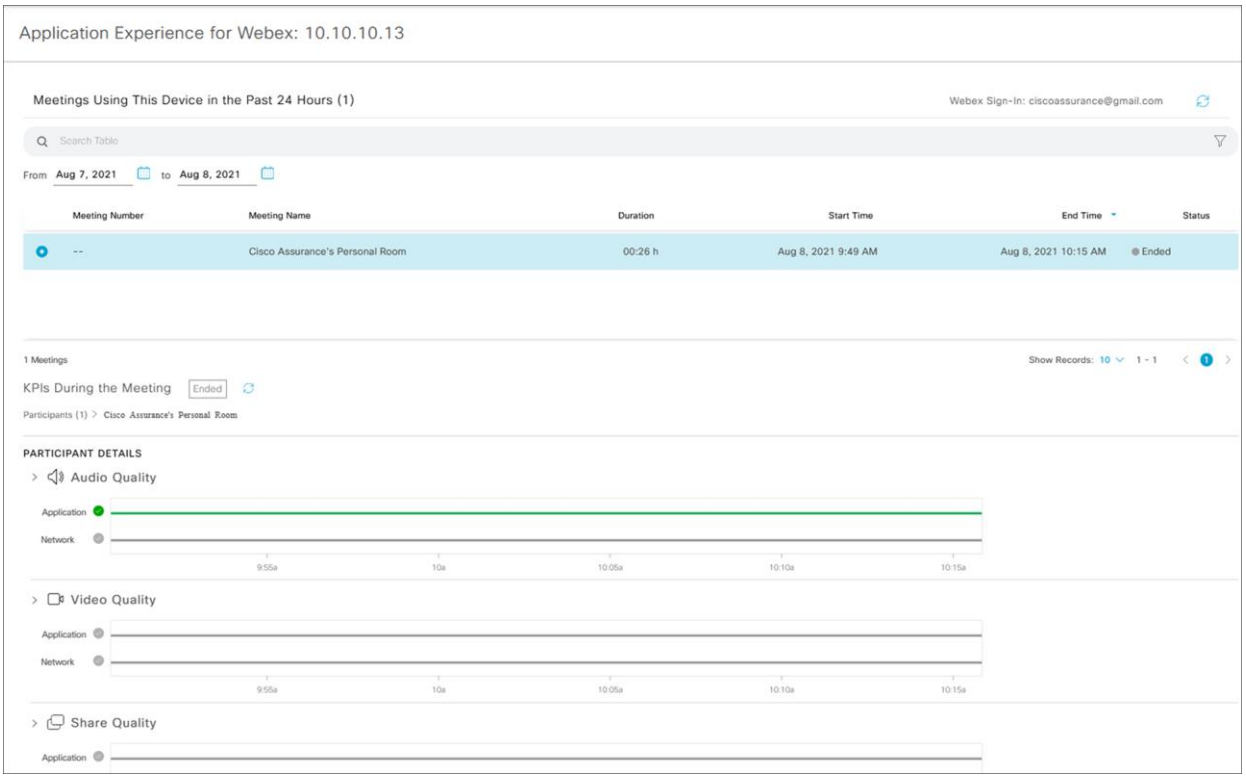

Figure 2.
WebEx metrics in Client 360

Wireless network service analytics

For a mobile device or any other end device to connect to the internet, it must connect to three service servers for:

- Authentication of devices (authentication, authorization, and accounting, or AAA)
- Getting an IP address (Dynamic Host Configuration Protocol, or DHCP)
- Finding the IP address of a targeted website (DNS)

If any of the three servers has an issue, users will have limited internet availability. Network operators would have to check each service for problem resolution.

In Cisco DNA Center 2.2.3, network operators can view AAA and DHCP services for wireless devices across Cisco and all third-party servers in a global comprehensive view. The release also integrates Cisco AAA servers' (Identity Services Engine, or ISE) AI-based root cause analysis. These new features provide a snapshot of the overall health of these critical services all in one place, highlighting the worst-performing service server, site-level impact, and scope of end user impact. This helps network operators reduce overall issue ticket resolution time and eventually leads to lower ticket volume.

True Trace

With the growing complexity of today's networks, conducting the root cause analysis of network issues requires the ability to perform thorough analyses. Network operators today struggle with a lack of path trace on live traffic, which leaves them with an incomplete picture. This can also make it difficult for them to do a deeper analysis when troubleshooting.

In Cisco DNA Center 2.2.3, network operators can capture live traffic on devices for path analysis. Cisco DNA Center's True Trace extends the current Path Trace capability and provides KPIs for each hop, granular reasons for path degradation, and downloadable packet capture files. These deep insights enable faster troubleshooting in enterprise deployments and lead to operational savings.

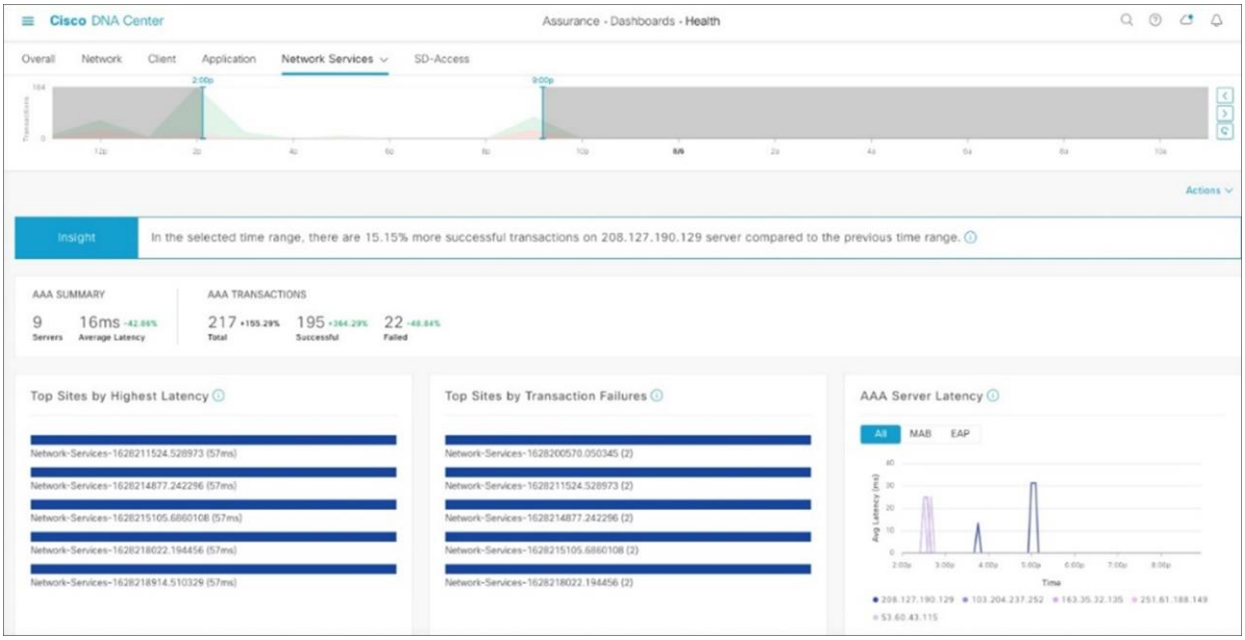

Figure 3.
Wireless network service analytics

NetOps with Cisco DNA Automation

Network Compliance Audit and Remediation

Compliance auditing is required to improve confidence that the network is operating securely and reliably. At times, network operators make device configuration changes and forget to replicate changes into the startup configuration. When a device reboots, the running or production configuration can be lost. Checking for out-of-sync devices and remediating them can be a lengthy manual process. The new Network Compliance Audit feature allows network operators to quickly assess the devices that do not adhere to the corporate standards.

The new Network Compliance Remediation feature in this release allows network operators to automatically sync running (production) configurations with startup configurations for all the network elements. Network operators can select one or many devices, view and validate the change, select and sync those devices, and remediate them to maintain compliance. The two new features together reduce human involvement and error and help ensure that the network is running the intended configuration standards.

Device replacement workflows for automated LANs

LAN automation enables network operators to automate the setup and deployment of their wired fabric and nonfabric networks. As automated LANs grow, so does the possibility of device failures. Until now, network operators had to manually replace failed devices in their automated LANs. This often involved manually replicating the configuration, verifying fabric role, and replicating credentials. All of these activities are time-consuming and error prone.

Cisco DNA Center 2.2.3 brings a simplified one-touch workflow to easily replace failed devices in the automated LAN. Using this workflow, network operators simply mark the failed device for replacement, plug in the replacement device, and discover the replacement device. Cisco DNA Center takes care of the rest, including retaining configurations, licenses, and fabric roles and completely onboarding the replacement device. This feature minimizes network downtime due to device failure, reduces the risk of user error during device replacement, and improves network operator productivity by minimizing the manual effort.

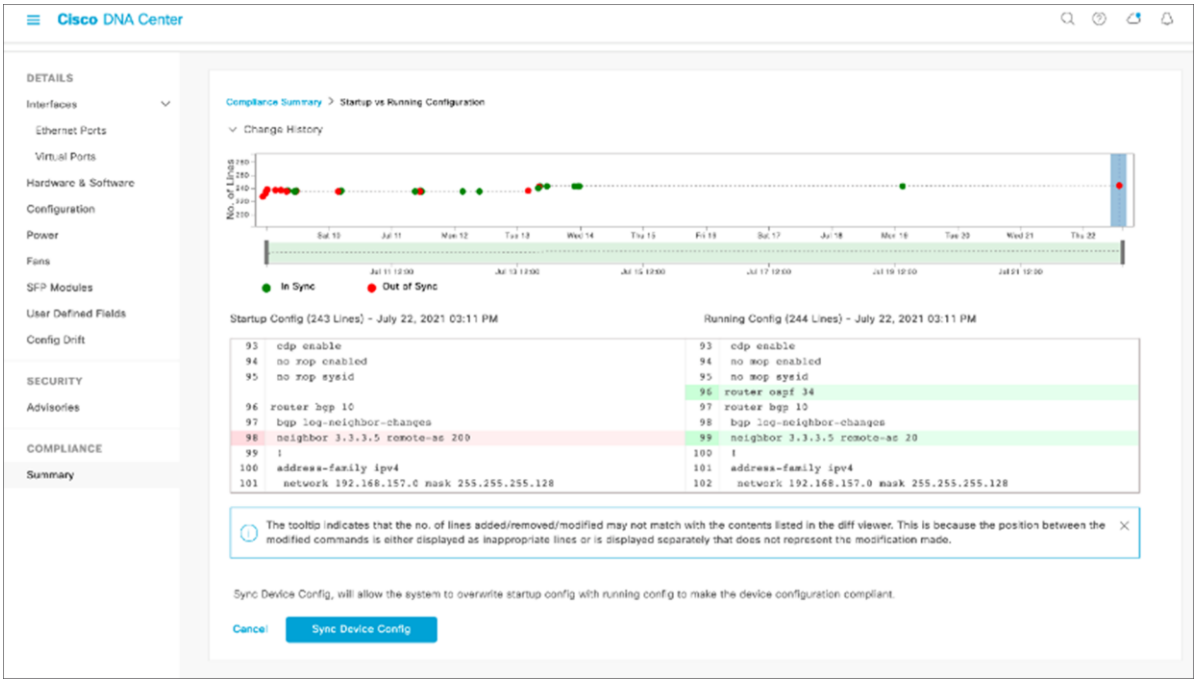

Figure 4.
Network compliance summary

SecOps: Zero Trust Workplace with Cisco SD-Access

Policy Analytics dashboard

In the past, when users navigated to group-based access control, they landed on the Policy Matrix page, which does not provide policy activity and alerts. With this release, instead of having to search for insights and specific alerts, they have a consolidated view of policy activities and alerts with the Policy Analytics dashboard. Users can select the alerts and policies to attend to, which helps them save time and manage the network policy more efficiently.

Enhanced Endpoint Analytics integration with ISE

Creating ISE authorization policies requires network operators to manually create ISE endpoint profiles that reference Endpoint Analytics attributes. Enhanced Endpoint Analytics shares these attributes, removing the manual process of creating profiles. Endpoint Analytics can also share ServiceNow configuration management database (CMDB) attributes and trust score attributes with ISE through this integration. This new integration greatly reduces the time and repetition of creating ISE endpoint profiles.

NAT device detection

Network Address Translation (NAT) devices create unauthorized and unmanaged entry points on the network. Identifying and removing these security threats quickly is important. The new NAT device detection feature on Endpoint Analytics identifies threats and helps organizations detect NAT devices quickly and more accurately.

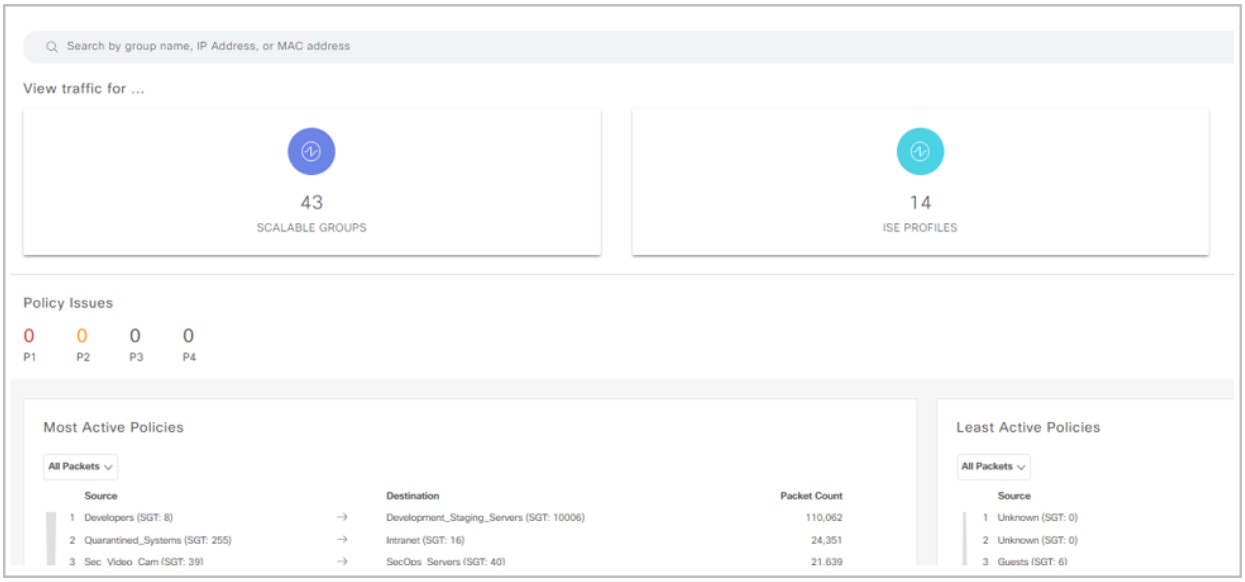

Figure 5.
Policy Analytics dashboard

New inputs for trust score

Network security administrators have difficulty processing multiple sources of endpoint security information that commonly conflict with each other to assess the safety of the endpoint.

The Cisco DNA Center Trust Score engine aggregates various endpoint security inputs and evaluates endpoint trust into a single but comprehensive score. In this release, new trust score inputs include NAT detection, concurrent MAC address detection, posture, authentication, and anomalous changes in profile label detection for better and more reliable trust scores. The new trust score helps network security administrators make security decisions more quickly and confidently.

Increased internet resiliency through Improved SD-Access architecture

Using publish/subscribe (pub/sub) for messaging drives an evolution of the Cisco SD-Access control plane architecture, expanding the capabilities of Cisco Locator/ID Separation Protocol (LISP). The LISP pub/sub solution eliminates the need for Border Gateway Protocol (BGP) for control plane communications. It tracks and signals the presence of an internet default route at a single fabric site and across all connected fabric sites, allowing for dynamic path optimization toward available internet services.

Elimination of BGP bypasses peering limits and increases the SD-Access transit scale. The LISP pub/sub solution helps network operators by increasing internet resiliency through routing convergence, simplifying fabric site design, and troubleshooting issues.

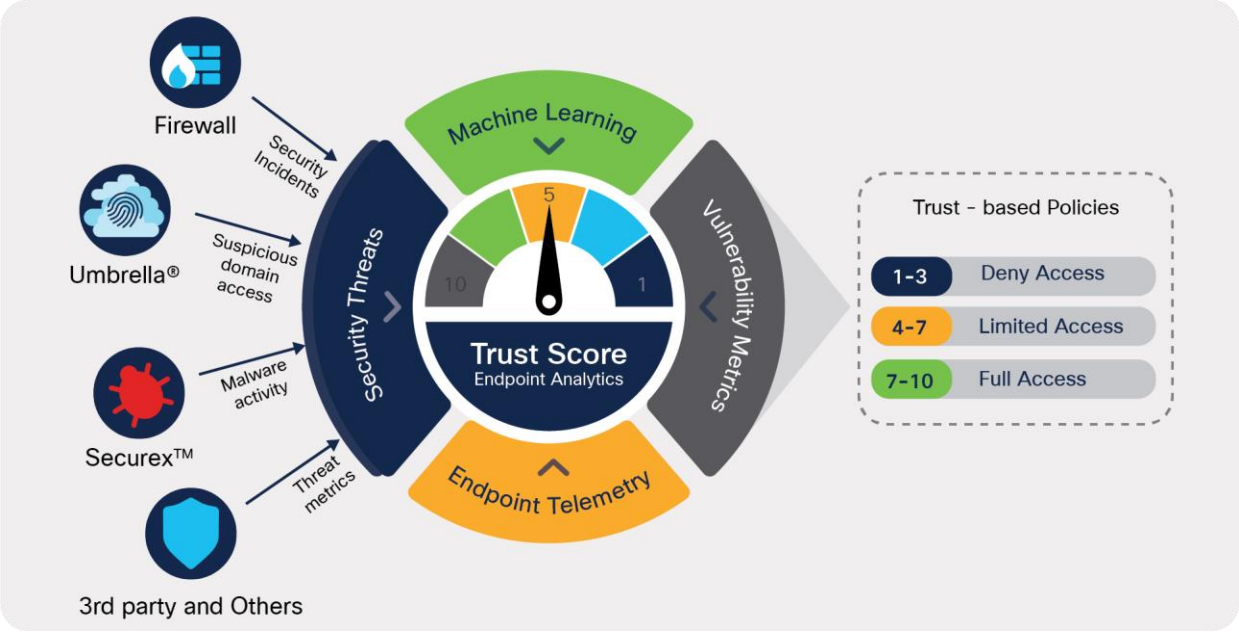

Figure 6.
Trust Score engine

Deployment readiness with Cisco DNA platform

3x increase in endpoint scale

Organizations face an explosion of mobility and IoT devices on their networks. This release allows Cisco DNA Center to manage three times the number of endpoints handled under the previous release, helping to avoid the need to launch an entirely new Cisco DNA Center cluster and install a new controller. This enables enterprises to provide the same level of service to their users at a much lower cost per endpoint and minimizes costly errors in governance and policy.

Faster disaster recovery time

Customers who chose to deploy Cisco DNA Center's Disaster Recovery configuration can enjoy an even faster recovery time that is reduced from 30 minutes to 15 minutes (excluding the time to detect the failure), allowing them to get back to operations faster. Failover detection is minimized to 3 minutes. This provides improved fault tolerance and near-constant availability for Cisco DNA Center.

Security Advisory updates

Finding Security Advisory updates and patching security bugs takes a lot of time and is very repetitive. Customers who don't address these network security issues in a timely manner remain vulnerable. Security Advisory leverages Cisco's Machine Reasoning Engine (MRE), which is Cisco's cloud-based AI/ML knowledge base. Security Advisory packages 35 years of Cisco network expertise to automatically flag security issues from the advisory notes.

In this release, Disaster Recovery, Easy Trigger Port, and new API updates provide different types of images to help organizations resolve the open vulnerabilities on their networks. This feature saves network operators valuable time by automating repetitive tasks and automatically identifying important vulnerabilities in minutes rather than what has taken hours or days when done manually.

Figure 7.
3x times increase in endpoint scale

Create and share custom topology layouts

Every network is unique in terms of devices deployed, the interconnections and its link status. The topology needs to support custom layout of devices for different users and groups within an organization. In DNA Center 2.2.3 the topology enhancements allow users to create, modify, and set their default topology view based on individual preferences and share their custom topologies with other users.

Easily triggered port actions

Network operators need to be able to update VLANs, update port descriptions, and reset interfaces for troubleshooting purposes. Currently these operations can't be easily triggered from the UI. Starting with Cisco DNA Center 2.2.3, network operators can take these actions from a new device view, saving the network operations team's valuable time.

New APIs

Running Cisco DNA Center in headless mode allows enterprises to use the APIs to scale and automate various Cisco DNA Center functions. New APIs include ones for provisioning SD-Access fabric, handling IP Address Manager (IPAM) certificates, and providing additional integrations with third-party vendors. They help save valuable time for developers and enterprises by reducing the dependence on the GUI to perform repetitive network functions.

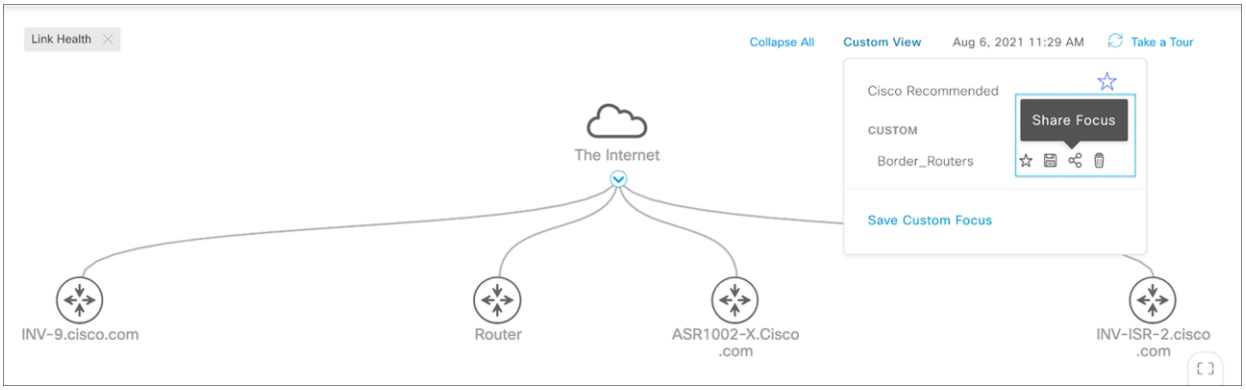

Figure 8.
Custom topology layouts

Cisco DNA Center useful links

- Release Notes for Cisco DNA Center 2.2.3.0
- Cisco DNA Center home page
- Cisco DNA Solution Builder
- Device Support Compatibility Matrix on Cisco.com

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 C80-2611301-00 10/21