New and Changed Information

The following table summarizes the new and changed features and tells you where they are documented.

Table 1: New and Changed Features for Cisco DNA Center, Release 2.2.2

Feature	Description	Where Documented
Deregister faulty device from CSSM	The RMA workflow deregisters the faulty device from CSSM and registers the replacement device with CSSM.	Limitations of the RMA Workflow in Cisco DNA Center Replace a Faulty Device
Automatic download option for ThousandEyes Enterprise Agent application	Within a few minutes of starting the Application Hosting Service, the ThousandEyes Enterprise Agent application is automatically downloaded. In the absence of an internet connection, you can set a proxy connection from the console to download the application.	Automatic Download of ThousandEyes Enterprise Agent Application
Firepower Management Center	Cisco DNA Center supports the integration of Firepower Management Center (FMC). FMC provides complete and unified management over Firepower Threat Defense (FTD) devices for managing Cisco network security solutions.	Integrate Firepower Management Center
Create Network Profiles for Firewall	Cisco DNA Center allows you to create network profiles for firewalls. You can create custom configurations to set up security devices like the Cisco Adaptive Security Appliance (ASA) family of devices and create FTD configurations to configure FTD devices.	Create Network Profiles for Firewall
Retry option in RMA workflow	Cisco DNA Center allows you to retry the RMA workflow with the click of a single button.	Replace a Faulty Device
Preview Device 2.0	The **Preview Devices 2.0** toggle button is new in the top-right corner of the **Provision** > **Inventory** page. Click the **Preview Devices 2.0** toggle button to view the devices, site profiles, software images, topology, RMA, PnP, templates, and PSIRTs in a new 2.0 framework.	—

Feature	Description	Where Documented
Explore menu	The following features are moved from the Cisco DNA Center home page to the **Explore** menu: • Design • Policy • Provision • Assurance • Platform	—
Topology support for new devices	Topology support is provided for the following devices: • Cisco Catalyst IR8100 Heavy Duty Series Routers (IR8140H-K9 and IR8140H-P-K9) • Cisco Catalyst 9124AX Access Point (C9124AXI and C9124AXD)	—
Cisco Umbrella configuration support for new devices	Cisco Umbrella configuration support is available for the following devices: • Cisco Catalyst 9200 Access Switch with Cisco IOS-XE software version 17.3.1 or later • Cisco Catalyst 9300 Access Switch with Cisco IOS-XE software version 17.3.1 or later	About Cisco Umbrella Provision Cisco Umbrella on Network Devices
Cisco Umbrella - Review Internal Domains	You can add and delete the list of internal domains from Cisco Umbrella.	Provision Cisco Umbrella on Network Devices
Configuration Drift Visibility	The **Config Drift** page displays configuration changes and allows you to pick any two versions of the same device and compare their running configuration data. **Note** With this release, the information under **Previous Running vs Current Running** has been moved to the **Config Drift** page.	Display Information About Your Inventory
Cisco Group-Based Policy Analytics	The **Access Contracts** can now be created and modified directly from the **Analytics** tab.	Access Contracts
Group-Based Access Control	You can now view the policy enforcement statistics data in the Policies listing window. The total numbers of policy permits and denies are displayed for the selected time period. Group-based access control policies can be created or updated based on the traffic flows for a given source and destination group pair. You can also create custom views of the policy matrix to focus only on the policies that you are interested.	Create Group-Based Access Control Policy
Plug and Play support for Cisco DNA Traffic Telemetry Appliance	You can claim a Cisco DNA Traffic Telemetry Appliance from the Plug and Play Devices list.	Provision a Cisco DNA Traffic Telemetry Appliance

Feature	Description	Where Documented
IPv6 search	Cisco DNA Center allows you search for devices using their IPv6 addresses. You can search for a device using its full IPv6 address, any abbreviated form, or double column in the IPv6 address with prefix and postfix combinations.	Use Global Search
User-defined fields	User-defined fields are custom labels that you can create and assign to any device in Cisco DNA Center. By assigning these labels to a device and adding values to them, you can show more details about the device in the device details page.	Manage User-Defined Fields
Inventory Insights	Cisco DNA Center provides insights about the devices in your network if there are any inconsistencies in the device configuration of two connected devices.	Inventory Insights
Persistence across inventory views	The device selection and the number of devices shown in the inventory table persist across inventory views in Cisco DNA Center.	Display Information About Your Inventory
Separation of golden tagging and download	From this release, you can separate download and golden tagging of software images. Cisco DNA Center allows you to download the software images by not marking them as golden.	Specify a Golden Software Image
Cisco sensor provisioning SSID	Cisco DNA Center sensors use the Cisco sensor provisioning Service Set Identifier (SSID) to communicate with the Plug and Play (PnP) server and obtain day-0 configurations for running tests.	Provision a Cisco Sensor SSID for Nonfabric Deployment
Interface/VLAN groups	Cisco DNA Center allows you to configure networks to have multiple broadcast domains through different VLANs. The Cisco DNA Center interface groups are logical groups of interfaces that facilitate user configuration, where the same interface group can be configured on multiple WLANs or while overriding a WLAN interface per AP group.	Design and Provision Interface/VLAN Groups to Nonfabric Deployments
Troubleshoot network connectivity	You can now troubleshoot network connectivity using Cisco DNA Center.	Troubleshoot Network Connectivity
Migration support for Cisco SD-Access	Cisco DNA Center provides Machine Reasoning Engine (MRE) workflows to assist you in planning your network migration to Cisco SD-Access.	Validate Cisco SD-Access Migration Using the MRE Workflow
Security Advisory Knowledge Bundle (KB)	You can enable notifications for new security advisory KBs. After notification is enabled, Cisco DNA Center provides visual notification and actionable alerts for any new security advisory KBs that are available from the cloud.	Add Notification for a New Security Advisory KB
Security Advisories view in Inventory	The Cisco DNA Center security focus view allows you to view the list of security advisories for your devices, based on the data retrieved from the previous security scan. The device data that you retrieve from the Security Advisories tool is now displayed in the Inventory page.	View Security Advisories in Inventory Page
Authentication check using security option	Cisco DNA Center security focus allows you to view the results of trustworthy checks on your devices.	Perform an Integrity Verification Check

Feature	Description	Where Documented
Cisco AI Endpoint Analytics	• **AI Endpoint Spoofing Detection**: Cisco AI Endpoint Analytics analyzes NetFlow telemetry data to detect spoofed endpoints. If an endpoint's behavior is not in line with its profile, Cisco AI Endpoint Analytics flags the anomaly, assigns a Trust Score to the endpoint, and lists it as a spoofed endpoint. You then review the details of the flagged endpoints and apply Adaptive Network Control (ANC) policies (created in Cisco ISE) from the Cisco AI Endpoint Analytics window. • **Automatic Profiling Rule Updates**: Cisco provides automatic system rule updates to enhance endpoint profiling accuracy. These updates help you profile endpoints more granularly and help profile previously unknown endpoints. Review the profiling changes suggested in an update. Then, you can either apply these changes or ignore the update. Major and minor profiling changes to existing endpoint profiles are displayed for your review. • **Cisco ISE MDM Attributes Support**: Cisco AI Endpoint Analytics receives MDM attributes from Cisco ISE if Cisco ISE is integrated with an MDM server. These MDM attributes are available for creating endpoint profiles using custom rules. • **Global Search Support**: In the Cisco DNA Center global search, when you search for endpoints by their IP address or MAC address, a link to AI Endpoint Analytics is displayed along with available profiling details for the endpoint. The profiling details and other information about the endpoint are displayed in the search result.	Cisco AI Endpoint Analytics
Network Bug Identifier	The Cisco DNA Center network bug identifier tool allows you to scan the network for a selected set of defects or bugs that have been identified previously and are known to Cisco.	Enable Network Bug Identifier
System Bug Identifier	The System Bug Identifier tool provides an option to identify bugs in Cisco DNA Center.	Enable System Bug Identifier
View IP Address Pools	• In the **IPv4** and **IPv6** columns, an **i** icon appears next to the corresponding used percentage of **IPv4** and **IPv6** for a given IP address pool. The tooltip displays the percentage of **Free**, **Unassignable**, **Assigned**, and **Default Assigned** IP addresses. • In the IP address pool slide-in pane, the **Used** area displays **Assigned** and **Unassigned** IP addresses to a network device. • Global and site IP address pools can have blocklisted IP addresses. • Subpools cannot have blocklisted IP addresses. • Cisco DNA Center rejects the IP address pool creation request of a CIDR address pool if it contains blocklisted IP addresses. • In the next free IP address pool request, Cisco DNA Center skips the blocklisted IP addresses to find the next free IP address pool.	View IP Address Pools