New and Changed Information

New and Changed Information

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

Feature	Description
Configure NBAR Cloud Connector	You can enable a protocol pack auto update. See Configure the NBAR Cloud Connector.
Initiate EoX Scan	You can initiate an EoX scan from the Inventory window. See Display Information About Your Inventory.
Certificate Revocation Check	You can configure a certificate revocation check. See Configure a Certificate Revocation Check.
Add Openings (Atriums) in 2D Wireless Maps	You can add openings, also called atriums, to 2D maps. See Add, Edit, Copy, and Remove Openings.
Wireless Coverage Optimizer	If your wireless coverage isn't meeting its SLA, you can run an optimizer tool. This tool takes your input of the maximum number of APs that you are prepared to move and add and computes a configuration where the wireless coverage is maximized. See Run the Wireless Coverage Optimizer.
Disable Applications and Endpoint Visibility	Applications and Endpoint Visibility is enabled by default; you can disable it. See Add a Device to a Site.
Wireless Maps GUI Enhancements	Minor enhancements have been implemented to make the GUI more robust and consistent. For example, when you remove an element (a sensor, wall, and so on) from a wireless map, the element is only taken out of the map. It is not deleted from Cisco DNA Center. The terminology in the GUI was changed from **Delete** to **Remove** to more precisely reflect this action.

Feature	Description
Resilient Ethernet Protocol (REP) Ring for Nonfabric Devices	You can configure REP Ring for nonfabric devices. See Configure a REP Ring for Devices.
Port Usage Information	For device ports, you can check the last input received and last output transmitted timestamp in the device **Details** window. See Port Usage Information.
Create Secure Tunnel	You can create an automated, secure IPsec tunnel to a new edge device at a branch location. This provides high-speed, secure, IPsec WAN connectivity to Cloud Security (Umbrella and Zscaler), and Enterprise connections. See, Create Secure Tunnel.
Return Material Authorization (RMA) Support	RMA support is extended for the following: • Cisco Switch stacks (hardware stacking): Cisco DNA Center allows you to replace full stack switches. • Supplicant-Based Extended Node (SBEN). See Replace a Faulty Device.
Readiness Check for RMA	The RMA flow includes a readiness check to assess the device preparedness for replacement. See Replace a Faulty Device.
Support for Configuration of Separate Accounting Servers for an SSID	You can configure separate accounting servers that are different from the authentication and authorization server for an SSID. See Configure AAA Server for an Enterprise Wireless Network.
Support for CCKM Configuration on SSID	You can enable CCKM as the authentication key management option in Cisco DNA Center. See Create SSIDs for an Enterprise Wireless Network.
Support for Scheduling SSID Broadcasting	You can create SSID scheduler to enable or disable WLAN based on time zone. See Create SSID Scheduler.
Fallback Mechanism Support for Remote LAN Ports	Remote LAN ports have a mechanism to fall back from a Dot1x failure to MAC filtering, and from a MAC filtering failure to Dot1x. See Configure Remote LAN.
Discovery Workflow Enhancements	The following enhancements are available from this release: • In the **Provide Credentials** window, add **HTTP(S) Read** and **HTTP(S) Write** credentials. • In the **Schedule Task** window, click the toggle button to enable or disable **Discover new devices only** option. See Discover Devices.

Feature	Description
Cisco SD-Access Zero-Trust Workplace	Cisco SD-Access provides a zero-trust security solution for your workplace. The Cisco SD-Access zero-trust security solution provides secure access to all users and devices from all locations across your network. The Cisco SD-Access zero-trust security solution provides the capability to automate network access policies using endpoint visibility, trust monitoring, and network segmentation. The SD-Access **Zero-Trust Overview** dashboard provides an overview of your zero-trust workplace journey. See Cisco SD-Access Zero-Trust Security Solution.
Virtual Network Policy in a fabric	You can create, edit, and delete a virtual network (VN) policy for a single-site fabric and multisite fabric with SD-Access transit. A VN policy allows route leaks between Layer 3 VNs, without using a fusion device. See Virtual Network Policy.
LAN Automation Task View and Status	LAN Automation Status provides detailed Status and Log views for each device, including the primary and the peer device. See Check the LAN Automation Status.
Custom Border Layer 3 Handoff IP Address Allocation	You can choose to either automate the IP routing between the border node and the peer or manually configure the IP addresses. See *Step 11* in Add a Device as a Border Node.
Intrasubnet Routing	Enable Intrasubnet Routing to forward the traffic within the subnet, based on the destination IP address. See Create Anycast Gateways.
Remote LAN Support for Fabric Sites	Cisco DNA Center supports remote LAN (RLAN) configuration for fabric sites on Cisco Catalyst 9800 Series Wireless Controllers. You can configure RLAN ports on APs for fabric sites. Cisco Wireless Controller authenticates the wired clients and allows them to connect to the network. You can configure RLAN for fabric sites on wireless controllers that run Cisco IOS XE Release 17.7 or later. See Configure Remote LAN.
Border Node Affinity-ID	You can configure the border node affinity-ID attribute. Affinity-ID determines the relative geographical location of a border node. You can now choose the preferred border node to route traffic when fabric sites don't have network access using the affinity-ID attribute. See Add a Device as a Border Node.
Modeled Access Contract	If you want Cisco DNA Center to generate the valid commands for the underlying Security Group ACLs (SGACLs), enable the **Modeled Access Contract** option while creating an access contract. When this option is enabled, the access contract is based on a model that allows you to create and edit without the need to know the underlying command line syntax. You can disable this option if you want to enter the SGACL command lines directly and store the access contract as text. See Create an Access Contract.

Feature	Description
Mobility Peer Configuration Enhancements	You can add wireless controllers that are not managed by Cisco DNA Center as mobility peers during mobility group configuration. See Configure Mobility Group and Provision a Cisco AireOS Controller.
Support for Multiple Anchor Configurations	You can configure anchor groups with up to three anchor wireless controllers and set the priority for the anchors. You can add an anchor to an SSID and choose the configured anchor group for a network profile for wireless. See Create an Anchor Group, Edit or Delete an Anchor Group, and Add SSIDs to a Network Profile.
Support for External Guest Anchor Cisco Wireless Controller Configurations	You can add external anchor wireless controllers to an anchor group. See Create an Anchor Group and Edit or Delete an Anchor Group.
Compliance Support for EoX - End of Life	Compliance support is extended for hardware, software, and module of EoX devices. See View Compliance Summary and Types of Compliance.
Software Image Compliance Support	You can check software image compliance for a Cisco switch stack. See View Compliance Summary and Types of Compliance.
Acknowledge Compliance Violations	You can acknowledge less important compliance violations and opt-out the violations from Compliance status calculation. See Acknowledge Compliance Violations.
Tri-Radio Configuration Support for APs	You can configure tri-radio parameters for APs that support the tri-radio configurations. See Configure AP Workflow and Schedule Recurring Events for AP Workflow.
Support for Custom WLAN Profile Configuration	You can configure a custom WLAN profile while creating SSIDs for guest and enterprise wireless networks. See Create SSIDs for a Guest Wireless Network, Create SSIDs for an Enterprise Wireless Network, and Add SSIDs to a Network Profile.
Support for Zero Wait Dynamic Frequency Selection (DFS) on APs	You can configure zero wait DFS as part of custom Radio Frequency (RF) profile configuration for a 5-GHz radio band. Zero wait DFS allows APs with a 5-GHz radio band to switch to a new channel without any waiting time. Zero wait DFS is supported on the following APs with Cisco RF ASIC: • Cisco Catalyst 9120AX Series Access Point • Cisco Catalyst 9124AX Series Access Point • Cisco Catalyst 9130 Wi-Fi 6 Access Point See Create a Wireless Radio Frequency Profile and Create an AI Radio Frequency Profile.

Feature	Description
RF Profile: 6-GHz Radio Band Support	The 6-GHz radio band is supported on the following RF functionalities: • Basic RF profile • AI Radio Frequency Profile • Configure AI RF Profile workflow See Create a Wireless Radio Frequency Profile, Edit or Delete a Basic Radio Frequency Profile, and Create an AI Radio Frequency Profile.
Support for Other AP Models for Remote Teleworker Configuration	Cisco DNA Center supports the following AP models for the remote teleworker configuration, along with support for the existing Cisco Aironet 1815T (Teleworker) AP: • Cisco Aironet 2800 Series Access Point • Cisco Aironet 3800 Series Access Point • Cisco Catalyst 9100 Series Access Point See Remote Teleworker Deployment Overview.
Support for New APs	Cisco DNA Center supports the following APs: • Cisco Catalyst 9164I Series Access Point • Cisco Catalyst 9166I Series Access Point See Configure AP Workflow and AP Refresh Workflow.
Troubleshoot Wireless APs Using the MRE Workflow	Using the MRE workflow, you can troubleshoot wireless AP issues. See Troubleshoot Wireless APs Using the MRE Workflow.
Default Home Page	The Cisco DNA Center default home page help menu support is extended for Cisco CX Cloud Success Tracks, which allows you to access the Cisco CX cloud success tracks website in a new window. See Default Home Page.

Feature	Description
View the Remote Support Authorization Dashboard	The **Remote Support Authorization** dashboard supports the following features: • **Manage SSH Credentials**: Allows you to establish the SSH connection to Cisco DNA Center. • **Configure SSH Credential**: Allows a Cisco specialist to access your Cisco DNA Center setup for troubleshooting. • **Access Permission Agreement** window support is extended for the following check boxes: • Access to network devices • Access to Cisco DNA Center setup See View the Remote Support Authorization Dashboard, Configure SSH Credentials, and Create a Remote Support Authorization.
Inventory User Interface Enhancement	The **Inventory** window user interface is enhanced to provide you the improved filters and layout for better user experience. See Inventory User Interface Enhancement.
View Security Advisories	• Cisco DNA Center security advisory support is extended for Cisco AireOS Wireless Controllers running with Cisco IOS software image version 8.5.120.0 or later. • Cisco DNA Center security advisories supports the **FAILED DEVICES** area, which displays information about device scans that are scheduled for a later date and time. See View Security Advisories.
Layer 3 Virtual Networks, Layer 2 Virtual Networks, Anycast Gateways Workflow Enhancements	The Layer 3 virtual networks, Layer 2 virtual networks, and anycast gateways workflows have been enhanced. You can select and edit up to five Layer 3 virtual networks, Layer 2 virtual networks, and anycast gateways. See Create a Layer 3 Virtual Network, Create a Layer 2 Virtual Network, Create Anycast Gateways, Associate Layer 3 Virtual Networks to Fabric Sites, Associate Layer 3 Virtual Networks to Fabric Zones, Associate Layer 2 Virtual Networks to Fabric Zones, and Associate Anycast Gateways to Fabric Zones.
Device Support for Extended Node	Stacked IE9300 switches can be onboarded as Extended Nodes or Policy Extended Nodes through Plug and Play.