New and Changed Information

• New and Changed Information, on page 1

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 2.2.3

Feature	Description	Where Documented
Rebranding of Application Policy as Application QoS Policy	The navigation menu for Application Policies is changed from **Policy** > **Application** to **Policy** > **Application QoS**.	Manage Application Policies
Define Custom Applications for Devices Without QoS Policy	You can configure custom applications with attribute sets and maps on Cisco DNA Traffic Telemetry Appliance without configuring QoS policy.	Application Visibility Service Support for the Cisco DNA Traffic Telemetry Appliance
Application Policy Support	Application Policy support is available for Cisco Catalyst IE3300 Series and IE3400 Series switches.	—
Share Topology Map	You can share your topology view with others.	Share a Topology Map Layout
Compliance	When Startup and Running configurations for a device are mismatched, you can run compliance checks and synchronize running configurations across multiple devices under **Action** > **Compliance** in the **Inventory** window.	Synchronize Startup and Running Configurations of a Device
RADIUS Profiling Configuration on Controllers	You can enable RADIUS client profiling on Enterprise SSIDs.	Create SSIDs for an Enterprise Wireless Network
Manage Device Credentials	You can create, edit, assign, and apply credentials to devices.	Manage Device Credentials
Enable Telemetry on Switches	You can configure SPAN and ERSPAN sessions on switches to share IP traffic for application assurance and endpoint analytics.	Enable Telemetry on Switches

Feature	Description	Where Documented
Fixed Versions for Security Advisories	The **Fixed Versions** column has been added to the **Security Advisories** window. This column lists the minimum known fixed version for security advisories. You can remove an advisory on your device by upgrading to the version mentioned in this column.	View Security Advisories
Change the Protocol Order of an Image Distribution Server	You can choose the required protocol for software image distribution by changing the protocol order of an image distribution server. Protocol order helps in performing verification checks on the image distribution servers.	Change the Protocol Order of an Image Distribution Server
Deny RCM Clients	Cisco DNA Center prevents the clients that are using random MAC addresses from joining the network. You can choose to deny or allow the clients with random MAC addresses when creating Enterprise SSIDs and Guest SSIDs.	Create SSIDs for an Enterprise Wireless Network Create SSIDs for a Guest Wireless Network
Flash Cleanup	You can store only the running software image and remove all the previous software images saved on a device when provisioning a software image or upgrading a software image with ISSU.	Provision a Software Image Upgrade a Software Image with ISSU
Retry Image Update Tasks	You can retry the image update for failed image update tasks.	View Image Update Status
Port Actions	You can clear the MAC address of a port and shut it down. To activate an error-disabled port, clear the MAC address and then shut down the port.	Display Information About Your Inventory
Different Views for Templates and Model Configs	You can view the templates and model configurations in the **Cards** view or the **Table** view when creating a network profile for Switching or Wireless.	Associate Templates to Network Profiles
New Model Config Design for AAA RADIUS Attributes	The AAA RADIUS **Called-station-id** parameter that is configured on Cisco AireOS Controllers and Cisco Catalyst 9800 Series Wireless Controllers is no longer restricted to be the ap-macaddress-ssid attribute value. You can now create a model configuration for AAA RADIUS attributes and choose from a list of several attribute values.	Create a Model Config Design for AAA RADIUS Attributes
FlexConnect VLAN Mapping for AAA Override	For FlexConnect deployments, you can configure AAA override VLANs for dynamic VLAN assignment of locally switched clients.	Configure a FlexConnect VLAN

Feature	Description	Where Documented
Group-Based Access Control Policy Dashboard	In the Group-Based Access Control Policy dashboard, you can view a summary of network activity, policy-related issues, and traffic trends. In the Cisco DNA Center GUI, click the **Menu** icon and choose **Policy** > **Group-Based Access Control** > **Overview** to view this dashboard.	Group-Based Access Control Policy Dashboard
802.1x Authentication Support for Access Points	You can configure the authentication settings for secure onboarding of APs using Plug and Play (PnP). Based on the authentication settings configured at the Global-level or Site-level hierarchy in Cisco DNA Center, PnP pushes the 802.1x (Dot1x) supplicant and certificates when claiming APs.	Configure 802.1x Authentication Settings for APs
Locator/ID Separation Protocol Publish/Subscribe (LISP Pub/Sub)-Based Control Plane	You can configure your fabric site to use a LISP Pub/Sub control plane. LISP Pub/Sub configuration provides native LISP support to handle the advertisement of LISP endpoint identifiers to the border.	Configure LISP Pub/Sub
Support for Scoped Subnets and Fabric Zones	You can divide a fabric site into fabric zones that have fewer segments and devices to manage. A fabric zone can have its own edge and extended nodes, but depends on its parent site for its border and control plane.	Configure a Fabric Zone
Security Advisory Support for Wireless controllers	In the Security Advisories dashboard, you can view security advisories for wireless controllers running Cisco IOS-XE software.	View Security Advisories
3D Wireless Maps	A 3D mode has been added for viewing wireless maps. With 3D wireless maps, you can view a 3D visualization of your wireless network.	Visualize Your Wireless Network in 3D
Template Editor UI Enhancements	When you start entering the system variable name in the **Template** window, all the relevant attributes appear as a drop-down list. You can expand or collapse the tree hierarchy in the **Template Editor** window. This feature allows you to view the **Template** window in a larger size.	—

New and Changed Information

Feature	Description	Where Documented
Mesh Configuration	You can configure access points as root access points or mesh access points. On both AireOS and Cisco Catalyst 9800 Wireless Controllers, you can configure authorized access points, Bridge Group Name (BGN), and root access points downlink backhaul. On Cisco Catalyst 9800 Wireless Controllers, you can configure the maximum range of the mesh access points, backhaul client access, and backhaul data rates.	About Wireless Mesh Networks Configure Mesh Settings on WLCs Configure AP Workflow Provision a Cisco AP—Day 1 AP Provisioning
Wireless Devices and Country Codes	Cisco DNA Center provisions controllers and access points with country codes, and displays the country code information on the **Device 360** window for controllers and access points.	About Wireless Devices and Country Codes
Replace Device Workflow	The workflow guides you step-by-step to replace a faulty device.	Replace Device Workflow
New Device Support for Return Material Authorization (RMA)	You can replace a failed device with a new device and use the RMA workflow to replace the image, license, and configuration on the new device. Cisco DNA Center provides one-touch RMA support for the following switches: • Switches that are discovered and configured using LAN automation, including the seed devices (LAN automation primary and peer devices) • Devices configured as fabric in a box (standalone only)	—

Feature	Description	Where Documented
Cisco AI Endpoint Analytics Enhancements	Cisco AI Endpoint Analytics assigns Trust Scores to endpoints based on the number and frequency with which the following anomalies are detected for an endpoint: • AI Spoofing Detection • Changes in Profile Labels • NAT Mode Detection • Concurrent MAC Addresses	Key Features of Cisco AI Endpoint Analytics
Detect Endpoints That Use Random MAC Addresses	With Cisco AI Endpoint Analytics, you can detect endpoints that use random MAC addresses. Cisco AI Endpoint Analytics enables you to handle the issue of random and changing MAC addresses by receiving from Cisco ISE a unique endpoint identifier called the DUID (also known as the GUID in Cisco ISE). Cisco AI Endpoint Analytics then uses the DUID as the identifier for an endpoint, instead of its MAC address.	
Purge Endpoints After Inactivity	You can define an Endpoint Purge Policy to remove from your network the endpoints that have been inactive for a defined time. You can define the period of inactivity after which an endpoint must be removed. You can also customize a purge policy to act on a particular set of endpoints based on a profiling attribute.	

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

New and Changed Information