New and Changed Information

• New and Changed Information , on page 1

New and Changed Information

The following table summarizes the new and changed features in Cisco DNA Center 2.3.6 and tells you where they are documented.

Feature	Description
Add Third-Party Device to Inventory	You can add a third-party device to your **Inventory** manually. See Add a Third-Party Device.
Automatic NETCONF Enablement Support	NETCONF is automatically configured on port 830 during device onboarding using plug and play. Automatic NETCONF enablement support is available only for Cisco Catalyst 9000 Series Switches running Cisco IOS-XE Version 17.3 or later. See Provision a Device with Plug and Play.
Cisco AI Endpoint Analytics Dashlet on Home Page	The Cisco DNA Center home page has a dashlet that takes you to the AI Endpoint Analytics dashboard (or lets you enable AI Endpoint Analytics if it isn't already installed). The dashlet provides information about the endpoints that are connected to your network, including profiled endpoints, trust score alerts, and AI rules. See Default Home Page.
Create Network Device Group (NDG) Tag	You can create a new NDG tag and add it to the devices in the **Inventory** window. See Create a Network Device Group Tag.
Credential Update Restriction for Third-Party Devices	You cannot update the credentials of third-party devices discovered by Cisco DNA Center. See Update Network Device Credentials.
Customize the TCP MSS Adjustment Value	You can choose a desired TCP MSS Adjustment value for the TCP sessions on the Layer 3 handoff interfaces. See Add a Device as a Border Node.

New and Changed Information

Feature	Description
Dynamic Channel Assignment (DCA) Validation	DCA channel support is based on the regulatory domain of a device. During AP provisioning, only the channels that are supported as per the country code are considered, and the unsupported channels are ignored. You can view the list of unsupported channels in the Preprovision Summary window. See Create a Wireless Radio Frequency Profile and About Wireless Devices and Country Codes.
Enable AP Impersonation	The wireless network settings dashboard now includes an option to configure an AP impersonation. See Configure AP Impersonation.
Enhancements to Accounting Server Configuration	Effective with this release, you must configure an accounting server for an SSID to push the accounting configuration for the SSID. See Configure AAA Server for an Enterprise Wireless Network and Configure AAA Server for a Guest Wireless Network.
Enhancements to AP Location Configuration	During AP provisioning and AP Plug and Play (PnP) onboarding, Cisco DNA Center doesn't configure the assigned site as the AP location. You can configure the AP location using the **Configure Access Points** workflow. See Provision a Cisco AP—Day 1 AP Provisioning, Provision a Wireless or Sensor Device, and Configure AP Workflow.
Enhancements to AP Selection in the AP Configuration Workflow	The **Configure Access Points** workflow has the following enhancements on the **Select Access Points** window: • You can select a maximum of 2000 sites. • You can choose the necessary APs from the **Assigned APs** and **Unassigned APs** tab. • You can use the search icon to filter the APs listed in the **Access Points** table using quick filters, advanced filters, and recent filters. • You can click the gear icon in the top-right corner of the **Access Points** table to edit or customize the table. See Configure AP Workflow.
Enhancements to Application Hosting on APs	When the **App Hosting Status** of an AP is **Ready**, to configure the updates on the AP, you can use the **Resync** option. See View Installed Hosting Applications on Cisco Catalyst 9100 Series Access Points.
Enhancements to Authentication using AAA Server for Wireless Networks	Effective with this release, you must configure an AAA server for an SSID to push the authentication configuration for the SSID. If an AAA server is not configured for the SSID, Cisco DNA Center pushes the **aaa authentication dot1x default local** command to the wireless controller and the default method list that points to local authentication is mapped to the SSID. See Configure AAA Server for an Enterprise Wireless Network and Configure AAA Server for a Guest Wireless Network.

Feature	Description
Enhancements to CleanAir Pro and CleanAir Spectrum Intelligence Settings During AP Configuration	In the **Configure Access Points** workflow, the CleanAir Pro and CleanAir spectrum intelligence settings are enhanced. You can now enable or disable the radio band-specific CleanAir Pro and CleanAir spectrum intelligence parameter settings for APs in the **Configure AP Parameters** window. **Note** These settings are no longer available in the **Configure 5 GHz Radio Parameters**, **Configure 2.4 GHz Radio Parameters**, **Configure Dual-Band (XOR) Radio Parameters**, and **Configure Tri-Radio Parameters** windows of the AP configuration workflow. To configure these settings, in the **How do you want to configure APs?** window, you must check the **Configure AP Parameters** check box. See Configure AP Workflow.
Enhancements to Editing RF Profiles	Effective with this release, when you update an RF profile that is already provisioned on a wireless controller and AP, you must reprovision either the wireless controller or AP. Wireless controller reprovisioning also pushes the RF profiles updates to the devices and AP reprovisioning is not necessary. If you don't need the RF profile updates during the wireless controller reprovisioning, you can check the **Skip AP Provision** check box See Edit or Delete a Basic Radio Frequency Profile and Edit an AI Radio Frequency Profile.
Enhancements to RF Profiles	Effective with this release, for Cisco Catalyst 9800 Series Wireless Controllers, disabling a radio band on the RF profile doesn't disable the Admin status of the respective radios on all APs that use the RF profile. Instead, Cisco DNA Center disables the Admin status of the corresponding RF profile. See Create a Wireless Radio Frequency Profile and Create an AI Radio Frequency Profile.
Enhancements to Site Tags, Policy Tags, and AP Zone Provisioning	Site tags, policy tags, and AP zone provisioning have the following enhancements: • If an AP zone is already provisioned on an AP and you update the AP zone configuration, you must reprovision the wireless controller. Reprovisioning the AP is not necessary. • Newly added custom site tag and policy tag configurations are applied only when you provision the APs. Provisioning the wireless controller alone doesn't configure the new custom tags on the APs. If there are any updates to the tags after the first provisioning, you must reprovision the wireless controller or APs. See Add AP Zones to a Network Profile and Add AP Groups, Flex Groups, Site Tags, and Policy Tags to a Network Profile.
Enhancements to the Wireless Network Settings Dashboard	The wireless network settings dashboard is enhanced to display the network settings in a card-based view. You can use the **Search All Settings** option to search for specific settings in the dashboard. You can customize the wireless network settings dashboard to update the priorities of the settings displayed in the dashboard using the **Edit Dashboard** option. See Configure Global Wireless Settings and Customize the Wireless Network Settings Dashboard.

New and Changed Information

Feature	Description
Feature-Based Trials	You can create feature-based trials for security advisories and system bug identifier. See View Security Advisories, View Field Notices and Scan Cisco DNA Center for Bugs.
MRE-Based Cisco Wireless Controller HA Health Check and Troubleshooting	You can troubleshoot any high-availability (HA) issues on Cisco Catalyst 9800 Series Wireless Controllers using the Machine Reasoning Engine (MRE) workflow. MRE workflow analyzes the HA health of wireless controllers by processing the relevant command outputs. See Troubleshoot HA on Cisco Wireless Controller Using the MRE Workflow.
Multiple Cisco DNA Center—Limited Availability	Multiple Cisco DNA Center allows you to define a single global set of virtual networks for Software-defined access across multiple Cisco DNA Center clusters integrated with a single Cisco ISE system. This Multiple Cisco DNA Center functionality is a Limited Availability offering. Because there are significant caveats for the Multiple Cisco DNA Center functionality, the Cisco SD-Access Design Council reviews the requests and provides guidance for use of the Multiple Cisco DNA Center to participants in the Limited Availability program. Contact your account team to submit a request to the Cisco SD-Access Design Council to participate in the Limited Availability program. Customers who are using Cisco ISE Version 3.1 or earlier must request and install the Limited Availability package before enabling Multiple Cisco DNA Center. **Note** After this functionality is enabled, it can be disabled only by deleting Cisco ISE. In addition, if this functionality is enabled, because pxGrid is a required component of the solution, pxGrid cannot be disabled subsequently.
My Favorites	For ease of use, you can add any window on Cisco DNA Center to **My Favorites**. **My Favorites** is a list of windows that you have marked as favorites with hyperlinked pathways, to help you navigate to a window quickly and easily. See Add a Window to My Favorites and Manage My Favorites.
Resilient Ethernet Protocol (REP) Ring	You can add a device to an existing REP ring for nonfabric deployment. See Add a Node to a REP Ring for Nonfabric Deployment.
Rogue General Configuration	You can create a model configuration design for rogue general parameters. See Create a Model Config Design for Rogue General Parameters.
Show Firepower Threat Defense (FTD) High Availability (HA) Paired Device Details in Inventory	The **Inventory** window shows the available FTD HA pairs with details of active and standby FTDs. See Integrate Firepower Management Center.
Single Connection Enablement for TACACS	You can configure switches with a single connection between the device and the TACACS server. See Add Cisco ISE or Other AAA Servers.
Software Image (SWIM) Workflow Upgrade	The **Software Image Update** workflow is enhanced in this release. See Provision a Software Image.

Feature	Description
Support for Additional Interfaces for Wireless Network Profiles	An additional interface on a Cisco Wireless Controller maps a WLAN to a VLAN or subnet. You can configure additional interfaces for network profiles for wireless. See Create Network Profiles for Wireless, Configure Additional Interfaces for a Network Profile, Provision a Cisco AireOS Controller, and Provision a Cisco Catalyst 9800 Series Wireless Controller.
Support for AP Configuration Using Template in the AP Configuration Workflow	The **Configure Access Points** workflow now includes an option to configure APs using existing templates. You can use the **Create Template for selected Configuration(s)** option in the **Configure AP And Radio Parameters** workflow to create a new template. See Configure AP Using Existing Templates Workflow and Configure AP Workflow.
Support for Cloning RF Profiles	You can clone the existing basic RF profiles and AI RF profiles. See Clone a Basic Radio Frequency Profile and Clone an AI Radio Frequency Profile.
Support for Editing Channel and Tx Power Settings on Planned APs	In 2D and 3D wireless maps, you can change the channel and Tx power settings for the planned APs. See Edit an AP and Edit Multiple APs.
Support for Individual AP Maintenance Mode	You can schedule maintenance individually for one or more APs when the corresponding Cisco Wireless Controller is not under maintenance mode. See Schedule Maintenance for Devices.
Support for Zero-Wait Dynamic Frequency Selection (DFS) on APs	Zero-wait DFS support is now available on the Cisco Catalyst 9136 Wi-Fi 6E Access Point. See Create a Wireless Radio Frequency Profile and Create an AI Radio Frequency Profile.
SWIM Flow Restrictions	For third-party devices, you can only perform basic SWIM operations. You cannot perform image update or image management for third-party devices. See Import a Software Image.
Topology Support for Third-Party Devices	Third-party devices monitored by Cisco DNA Center are shown in the **Topology** map with the generic device icon. You can add tags to the third-party devices using the **Topology** map.
View Field Notices	You can view the **Field Notices** and **Potential Field Notices** in your network. See View Field Notices.
View PSRIT Software Maintenance Update (SMU) details	The Image Update Status workflow is enhanced, you can now view the additional PSRIT SMU related details. See View Image Update Workflow.
Visibility of Compliance Remediation	To fix compliance violations, you can review the configurations that are deployed on the network device. See Fix Compliance Violations.

New and Changed Information

Feature	Description
Visibility of SD-Access Fabric Configurations	During the provisioning of an SD-Access fabric, you can generate a preview of the device configurations (CLI commands) before deploying them. See Visibility of Fabric Configurations.
Visibility of Template Hub	The commands used in the CLI templates can be reviewed prior to deployment on network devices. See Provision CLI Templates and Visibility of Configurations Workflow.
Visibility of Unmanaged Switches	In 2D wireless floor maps, you can view the unmanaged switches that are connected to the managed APs. See View an Unmanaged Switch Connected to Managed APs.
Visibility of Wireless Device Configurations	The Visibility of Wireless Device Configurations feature provides a solution to further secure your planned wireless network configurations before deploying them on your devices. You can enforce previewing the wireless device configurations before deploying them. **Configuration Preview** is enabled by default. You can update this setting on the **System** > **Settings** > **Visibility of Configurations** window. **Note** If there is a conflicting operation when you deploy your planned network configurations, the **Pending Operations** dialog box is displayed. To proceed with the current deployment, you must either wait for the existing, scheduled, or pending-review operations to complete or discard the operations. See Visibility of Wireless Device Configurations, Provision a Cisco AireOS Controller, Provision a Cisco AP—Day 1 AP Provisioning, Provision a Cisco Catalyst 9800 Series Wireless Controller, Configure Mobility Group, Configure Remote LAN, and Workflow to Create an IP-Based and URL-Based Access Control Policy.
Web Content Accessibility Guidelines (WCAG) 2.1 AA Compliance: Keyboard Accessibility Support	You can use the keyboard to access all interactive content in the Cisco DNA Center GUI. Those who cannot use a mouse can access and move between links, buttons, fields, and other controls using the **Tab** key and other keystrokes. See Web Content Accessibility Guidelines (WCAG) 2.1 AA Compliance.