New and Changed Information

New and Changed Information

The following table summarizes the new and changed features in Catalyst Center 2.3.7.5 and tells you where they are documented.

Table 1: New and Changed Features in Catalyst Center, Release 2.3.7.5

Feature	Description
Enhancements to the AP Refresh Workflow	The **Access Point Refresh** workflow now supports the following: • The Assurance use case where the new AP isn't provisioned after AP refresh and only the old configuration is copied to the new AP. **Note** If the new AP is onboarded through Plug and Play (PnP), the Assurance use case isn't supported. • A toggle button to enable the automatic detection of the new APs using SwitchPort. **Note** If the new AP is onboarded through PnP, automatic detection isn't supported. See AP Refresh Workflow.
Enhancements to Configuring Global Device Credentials	On the **Device Credentials** window, you can now only assign and unassign device credentials to and from sites. On the **Manage Credentials** slide-in pane, you can manage your device credentials using the **Focus** drop-down list. Depending on which focus you choose (**Current site** or **System**), you can perform specific actions. See Configure Global Device Credentials.

Feature	Description
Enhancements to Custom AP Groups and Flex Groups for Cisco AireOS Wireless Controller	Instead of configuring and applying the newly added custom groups to the APs during wireless controller provisioning, Catalyst Center now configures and applies them during AP provisioning. Effective with this release, you can use the same AP groups and flex groups across multiple sites for Cisco AireOS Wireless Controller. **Note** • You can't use the same AP group on multiple sites with different SSIDs, RF profile, and SSID overrides. • You can't use the same flex group on multiple sites with different native VLAN or AAA override VLAN. See Overview of AP Groups, Flex Groups, Site Tags, and Policy Tags and Custom AP Group and Flex Group Reuse Examples.
Enhancements to Device Onboarding and the Discovery Workflow	The **Add Device** option in the Catalyst Center Inventory is enhanced to include options for adding both new and existing devices. The discovery workflow includes enhancements, such as: • The **Provide Credentials** window now includes the option to configure advance settings along with the CLI and SNMP credentials. • The **Schedule Job** window combines site assignment and scheduling of the discovery job. See: • Add Devices to the Catalyst Center Inventory. • Use a CSV File to Import and Export Device Configurations. • Import Device Configurations from a CSV File. • Discover Devices. • Discover Your Network Using CDP. • Discover Your Network Using an IP Address Range or CIDR. • Discover Your Network Using LLDP.

Feature	Description
Enhancement to Device Resynchronization	Prior to this release, restarting the inventory service would trigger resynchronization for all devices in the inventory. With this release, device resynchronization is triggered after the inventory service restart under the following circumstances only: • After Catalyst Center upgrade. • If the device's synchronization is in terminated or delayed state after the service restart. • If the device's last synchronization time has crossed the configured cutoff time. See About Inventory.
Enhancements to Device Upgrade Readiness Check	• Flash Check: Calculates the space required for upgrading to golden image with add-on and performs flash clean up proactively before image distribution. • Weak Crypto Check: Checks whether the device is configured with weak crypto and blocks image upgrade. This readiness check is applicable only for devices with software image version 17.14 and later. • File Transfer Check for FQDN Setup: Checks whether the name server associated with the device is reachable and displays an error message. See List of Device Upgrade Readiness Prechecks.
Enhancements to Editing LAN Automated Devices	In the **Edit Devices** window, you can now edit the hostname for the devices that are discovered through LAN automation. See LAN Automation and Edit Hostname and Loopback IP Address of LAN Automated Devices.
Enhancements to Port Configuration Within Fabric Sites	The **Port Assignment** tab for a fabric site now displays the authentication template configured for each port. If you don't configure the authentication template for an individual port, the port inherits these settings from the global authentication template configuration. Inherited settings are displayed with an inherit icon next to the setting. See Configure Ports Within the Fabric Site.
Progress Bar Support for Network Devices Provisioning	The **Task Progress** bar on **Activities** > **Tasks** window, displays the progress of the ongoing provisioning task for your network devices. See Provision a Cisco Sensor SSID for Nonfabric Deployment, Provision a Cisco AireOS Controller, Provision a Cisco AP—Day 1 AP Provisioning, Provision Cisco AireOS Controllers in the Existing Deployment, Configure N+1 High Availability from Catalyst Center, Provision a Cisco Catalyst 9800 Series Wireless Controller, Configure Cisco Wireless Controllers on the Existing Infrastructure, Provision Embedded Wireless on Cisco Catalyst 9000 Series Switches, Provision a Meraki Device, Provision a Router, Complete the Provisioning Process, and Visibility and Control of Device Configurations.

Feature	Description
SD-Access Compatibility Check	A device is added to the SD-Access fabric only if the device runs a software release that is compatible with the Catalyst Center release. See Add a Device to a Fabric, Add a Device as a Border Node, Steps to Configure an Extended Node.
SD-Access Application Health Check	The health of SD-Access application is checked periodically and the status is displayed on the System Health page. See Fabric Health Check.
Support for Displaying IOS CLI in Configuration Preview for Cisco Catalyst 9800 Series Wireless Controller	For Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 17.13.1 or later, you can generate IOS CLI from YANG configuration in the configuration preview. See Visibility and Control of Wireless Device Configurations.
Support for Standard Power Service	For APs with the standard power capability, compliance with FCC regulations requires the activation of Automatic Frequency Coordination (AFC). The **Standard Power Service** toggle button in the **Create Wireless Radio Frequency Profile** and **Create AI Radio Frequency Profile** window enables you to activate AFC for the 6-GHz band within an RF profile. **Note** This feature is applicable only for Cisco Catalyst 9800 Series Wireless Controllers. When you provision the corresponding APs, the **Summary** window displays the standard power service configuration details. See Create a Wireless Radio Frequency Profile and Create an AI Radio Frequency Profile.
Support for the Workflow Progression View in Visibility- and Control-Enabled Provisioning Workflows	If a visibility- and control-enabled provisioning workflow supports the workflow progression view, the **Preparing Devices and Configuration Models** window displays the steps the system takes to prepare a listed device. See Visibility and Control of Device Configurations, Visibility and Control of Wireless Device Configurations, and Visibility and Control of Fabric Configurations.

Feature	Description
Support for Third-Generation Catalyst Center Appliances	Catalyst Center now supports the following third-generation appliances, which are based on the Cisco UCS C220 and C240 M6 servers: • 32-core appliance: Cisco part number DN3-HW-APL • 32-core promotional appliance: Cisco part number DN3-HW-APL-U • 56-core appliance: Cisco part number DN3-HW-APL-L • 56-core promotional appliance: Cisco part number DN3-HW-APL-L-U • 80-core appliance: Cisco part number DN3-HW-APL-XL • 80-core promotional appliance: Cisco part number DN3-HW-APL-XL-U For more information, see the *Cisco Catalyst Center Third-Generation Appliance Installation Guide, Release 2.3.7.x*.
Support for Viewing and Editing Layer 2 Configurations of a Device	You can view and edit the Layer 2 configurations of a device in the Catalyst Center inventory. **Note** This feature is in beta. See Display Information About a Device, View Layer 2 Configuration of a Device, and Edit Layer 2 Configuration of a Device.
Third-Party Devices Support	Catalyst Center allows third-party devices to populate SNMP MIB-II values. See, Add a Third-Party Device.
Weak Crypto Check	To ensure a secure network connection Catalyst Center performs weak crypto check to evaluate the device configuration, and blocks the device provisioning/upgrade/site assignment for devices that are configured only with MD5 authentication for SNMP credentials. This is applicable only for devices with software image version or golden tagged image version 17.14.1 and later. See Discovery Credentials, Add a Network Device, Update Network Device Credentials, Add a Compute Device, Add a Third-Party Device, Add a Device to a Site, Add Global SNMPv3 Credentials, Provision a Switch or Router Device, Provision a Wireless or Sensor Device and Complete the Provisioning Process.
Enhancements to the disaster recovery witness site upgrade process.	Using an SSH client, you can upgrade a disaster recovery system's witness site using the **witness upgrade** command. See the "Upgrade the Current Witness Site" topic in the *Cisco Catalyst Center Administrator Guide, Release 2.3.7.x*.

The following table summarizes the new and changed features in Catalyst Center 2.3.7.4 and tells you where they are documented.

Table 2: New and Changed Features in Catalyst Center, Release 2.3.7.4

Feature	Description
Name Change to Catalyst Center	As part of our vision to converge our products around an integrated platform, we are changing the name of Cisco DNA Center to Catalyst Center in this release. The capability and functionality of Catalyst Center remains the same as Cisco DNA Center. This name change is part of our simplified branding for the Catalyst Center Stack. Cisco is now connecting the power and flexibility of the Catalyst brand across the entire enterprise networking stack with Catalyst Center (formerly Cisco DNA Center), Catalyst Software and Licensing (formerly Cisco DNA Software and Licensing), Catalyst Wireless, Catalyst Switching, Catalyst Routing, and Catalyst SD-WAN (formerly Cisco SD-WAN or Viptela SD-WAN).
Enhancements to AP Provisioning for N+1 High Availability	Effective with this release, if you are using N+1 High Availability (HA) and modify any nonflex SSIDs that are already provisioned on the primary and secondary controllers to flex SSIDs (or conversely), ensure that the states of WLANs are consistent across both the primary and secondary controllers on the corresponding site. See Provision a Cisco AP—Day 1 AP Provisioning.
Enhancements to Custom Flex Profile Creation	A custom flex profile is created during Cisco Wireless Controller provisioning (with model configurations) or during AP provisioning (without model configurations). In both scenarios, the custom profile is configured with settings that are similar to the default flex profile except for the Catalyst Center intent configurations. Catalyst Center also provides an option to autogenerate a flex profile name. See Add AP Groups, Flex Groups, Site Tags, and Policy Tags to a Network Profile.
Enhancements to Default AP Profiles During Upgrade	In earlier releases, the default AP profile was pushed to the wireless controller during upgrade. When you upgrade to this release from an earlier version, by default, Catalyst Center doesn't push the default AP profile to the wireless controller. To update the default AP profile on the wireless controller, you must explicitly save it on the **Design** > **Network Settings** > **Wireless** > **AP Profiles** window. After you save the default AP profile, if there is a difference between the current wireless controller configuration and the AP profile configuration saved on Catalyst Center, the default AP profile is pushed to the wireless controller during subsequent reprovisioning. See AP Profiles.

Feature	Description
Enhancements to the Embedded Wireless Controller Image Installation for Switches	Following are the enhancements to the embedded wireless controller image installation process for switches: • The **Activate image on device** option is removed. • During the image import, you can exit the window, and view the progress of the import and schedule the installation later using the **Close** option. • After the image is imported, you can install it immediately or schedule the image installation for a later date or time. • You can check the status of image installation on the **Activities** > **Tasks** window. See Add a Device to a Fabric and Provision Embedded Wireless on Cisco Catalyst 9000 Series Switches.
Enhancements to Preauthentication ACLs	Preauthentication Access Control Lists (ACLs) have the following enhancements: • The **Include auto rules** toggle button lets you enable or disable pushing the Catalyst Center-generated rules to the applicable SSIDs. • For **Walled Garden URLs**, a valid URL must have at least one period. Cisco AireOS Wireless Controllers don't support other special characters. Cisco Catalyst 9800 Series Wireless Controllers support the special characters . * - _. See Create Preauthentication Access Control Lists.
Enhancements to the Provisioning of Wireless Changes on Fabric Devices	If the wireless capability is enabled for a fabric device in the SD-Access device slide-in pane and there are changes in the wireless settings, you must click **Configure** in the slide-in pane to push the changes to the device. **Note** These enhancements are also applicable for the N+1 configurations. See Add a Device to a Fabric.
Enhancements to the Catalyst Center Home Page	The Catalyst Center home page displays a new welcome message and displays license and release banner messages relevant to Catalyst Center. The Tools area is removed and is accessible from the menu in the top-left corner. See Default Home Page.

Feature	Description
Enhancements to the Menus	To streamline workflows and standard nomenclature, we changed several menu option names, moved several submenu options, and added a secondary launch point for Interactive Help. The menu option changes include: • **Design** > **Network Settings** > **Network** is now **Design** > **Network Hierarchy** > **Servers**. • **Design** > **Network Settings** > **SP Profiles** is now **Design** > **Service Provider Profiles**. • **Provision** > **Stealthwatch Security Analytics** is now **Provision** > **Stealthwatch Security**. • **Tools** > **Template Hub** is now **Design** > **CLI Templates**. • **Tools** > **Model Config Editor** is now **Design** > **Feature Templates**. • The **Activities** menu option now lists two submenu options: **Audit Logs** and **Tasks**. • **System** > **System Health** is now **System** > **System 360** > **System Health**. • **System** > **Settings** > **Telemetry Collection** is now **System** > **Settings** > **Product Telemetry**. • The **Help** icon lists the new secondary launch point for **Interactive Help**.
Enhancements to the Configure AI-Enhanced RRM Workflow	You can configure an AI-enabled radio frequency profile without device provisioning. See Configure AI-Enhanced RRM.
Enhancements to VLAN ID Configuration for Wireless Interfaces	In earlier releases, the valid range for VLAN ID for wireless interfaces was from 0 through 4094. Effective with this release, the valid range for VLAN ID for wireless interfaces is from 1 through 4094. **Note** • For Cisco AireOS Wireless Controller, the valid range is from 1 through 4094. • For Cisco Catalyst 9800 Series Wireless Controllers, the valid range is from 2 through 4094. See Create a Wireless Interface and Configure Additional Interfaces for a Network Profile.

Feature	Description
Device Compliance and Pending Operation Prechecks for a Seamless Deployment	To ensure a seamless deployment, Catalyst Center performs a set of prechecks to ensure that any pending operations that conflict with the current task and any device compliance issues are addressed. See Network Provisioning Prechecks.
Log Collection for a Device	When a resync is done for a specific device, the debug log is enabled automatically for that device, and XDE and device pack logs are collected. See Resynchronize Device Information.
Reconfiguration of a Fabric for IP Address Pool Changes	When you modify the IP address pools that are used in a fabric, you must reconfigure the fabric. **Note** The IP address pool changes are not provisioned automatically. See Edit IP Address Pools and Reconfigure a Fabric.
Software Image Compatibility Check for Fabric Devices	To ensure the network devices (before and after a fabric deployment) are compatible with the recommended or supported software image versions based on the Catalyst Center package version, Catalyst Center performs an Image Compatibility check to evaluate the network devices. See Fabric Readiness, Image Compatibility, and Compliance Checks and Types of Compliance.
Unsupported SD-Access Configuration Detection on Fabric Devices	You can detect any unsupported SD-Access configurations on fabric devices using the **SD-Access Unsupported Configuration** compliance check. **Note** This feature is in beta. See Types of Compliance and View Compliance Summary.
Usability Enhancements to Previewing Configurations in Visibility- and Control-Enabled Workflows	When previewing configurations in a visibility- and control-enabled workflow, you can display the device configurations in a side-by-side comparison view. **Note** The side-by-side comparison view doesn't support viewing YANG configurations. See Visibility and Control of Device Configurations, Visibility and Control of Wireless Device Configurations, and Visibility and Control of Fabric Configurations.

Feature	Description
Usability Enhancements to Support Service	Support Service has the following enhancements: • When creating a remote support authorization, you must first accept the **Access Permission Agreement**. • "SR" is replaced with "case number." • The **Past Authorizations** table is searchable and contains a column for the case number. See View the Remote Support Authorization Dashboard, Configure SSH Credentials, and Create a Remote Support Authorization.
Visibility and Control of AI RF Profile Configurations	With the Visibility and Control of Configurations feature, you can preview AI RF profile configurations and send those configurations to IT Service Management (ITSM) for approval before deploying them. See Configure AI-Enhanced RRM, Assign a Location to an Existing AI RF Profile, and Unassign a Location from an Existing AI RF Profile.