

New and changed features in Catalyst Center

This table summarizes the new and changed features in Catalyst Center 3.3.2 and tells you where they are documented.

Table 1: New and changed features in Catalyst Center 3.3.2

Feature	Description
Shared wireless controller for multiple fabric sites	Catalyst Center now supports sharing a Cisco Catalyst 9800 Series Wireless Controller across multiple SD-Access fabric sites. **Note** This feature is in beta. A wireless controller can be shared across a maximum of 16 fabric sites. You can select eligible remote fabric sites, validate network profile compatibility, resolve configuration conflicts, and prepare site-specific wireless intent before deployment. Refer to Shared wireless controllers for multiple fabric sites and Provision a Cisco Catalyst 9800 Series Wireless Controller.

This table summarizes the new and changed features in Catalyst Center 3.3.1 and tells you where they are documented.

Table 2: New and changed features in Catalyst Center 3.3.1

Feature	Description
Decouple templates configuration from network profile	If you want to configure one or a few devices with specific configurations that do not apply to the rest of the devices at the same site, you can provision the CLI template without associating it with a network profile. The compliance check is skipped if you provision the template without associating it with a network profile. Refer to Provision CLI templates
Enhancements to application hosting	Catalyst Center supports multi-architecture app packages across CPU architectures such as x86_64 and aarch64. Refer to Install an application using application hosting

Feature	Description
Enhancements to delete a REP ring.	If any device in the REP ring is unreachable, you cannot delete the ring. Use Catalyst Center to rediscover the REP ring so you can remove unreachable devices and then delete the ring. Refer to Delete a REP ring
Enhancements to MRP monitoring	When the link between two devices goes down in an MRP ring, Catalyst Center indicates the affected MRP Ring node. Refer to View MRP ring topology overlay
Enhancements to the AP configuration workflow	The **Configure Access Points** workflow is enhanced for improved usability. Refer to Configure APs, Schedule recurring events for APs, and Configure APs using existing templates.
Enhancements to per-device configurations for Cisco Catalyst Switches in Catalyst Center	Catalyst Center supports these enhancements for Cisco Catalyst Switches: • Configuration of QoS, BFD, OSPF, and AAA attributes in the per-device configurations. • Per-device configuration support for fabric devices. Refer to View and edit service configurations of a device, View and edit Layer 3 configuration of a device, View and edit the network settings of a device, and Manage per-device configurations for Cisco Catalyst Switches.
Enhancements to Per-Device Configurations for Cisco Catalyst 9800 Series Wireless Controllers	Per-Device Configurations for Cisco Catalyst 9800 Series Wireless Controllers are enhanced to support new and updated configurations for Cisco IOS XE Release 26.2.1. Refer to Configure ThousandEyes for a Cisco Catalyst 9800 Series Wireless Controller, Create a radio profile for a Cisco Catalyst 9800 Series Wireless Controller, Create an AP join profile for a Cisco Catalyst 9800 Series Wireless Controller, Create a WLAN profile for a Cisco Catalyst 9800 Series Wireless Controller, Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, Create a policy profile for a Cisco Catalyst 9800 Series Wireless Controller, Configure global wireless parameters for a Cisco Catalyst 9800 Series Wireless Controller, and Edit default RF settings for a Cisco Catalyst 9800 Series Wireless Controller.
Enhancements to port configuration profiles for Cisco Catalyst Switches in campus networks workflow	The configuration profiles for Cisco Catalyst Switches has been enhanced to support additional profiles for port configurations. Refer to Create port configuration profiles for switching device groups.
Enhancements to REP ring configuration	You can configure REP ring with MACsec encryption. Refer to Configure a REP ring for devices.

Feature	Description
Enhancements to the scheduling experience in the Visibility and Control of Configurations workflow	Catalyst Center streamlines the scheduling experience in the Visibility and Control of Configurations workflow: • Configure scheduling and preview from one page. • Enable configuration preview using the **Preview** check box. Refer to Visibility and control of device configurations, Preview and deploy your device configurations, and Deploy your device configurations now or later.
Enhancements to the wireless controller provisioning workflow in campus networks	Catalyst Center supports these enhancements for provisioning wireless controllers in a campus network: • Associate configuration profiles to multiple wireless controllers. • Create new configuration profile for wireless controllers. • Support for additional configurations for wireless controller configuration profile. • Configure and review device overrides for wireless controller configuration profiles. Refer to Manage configuration profiles, Create configuration profiles for wireless controllers, Assign configuration profiles to a wireless controller, and Configure per-device overrides for wireless controller configuration profiles.
Enhancements to the switching provisioning workflow in campus networks	Catalyst Center supports these features for provisioning switching devices in a campus network. • Configuration of Industrial configuration profile. • Configuration of device-level overrides for configuration profile attributes. Refer to Provision a switching device group.
Enhancements to the wireless SSID creation workflow for enterprise and guest wireless networks	The wireless SSID creation workflow has these enhancements for enterprise and guest wireless networks: • The **Associate SSID to Wireless Network Profile** window is enhanced. • Under **Auth Key Management**, **FT + 802.1x** and **802.1x-SHA256 (802.1X-SHA2)** options are supported for the **GCMP256** encryption. Refer to Create SSIDs for an enterprise wireless network and Create SSIDs for a guest wireless network.

Feature	Description
Live Protect	Live Protect validates security shields that protect Cisco products without requiring device reloads or service interruptions. You can deploy security shields in two modes: • Monitoring mode: Provides visibility into potential exploit attempts without enforcement, allowing you to assess threats before taking action. • Enforce (Protecting) mode: Actively applies mitigation policies to reduce exposure to known vulnerabilities. Live Protect allows you to monitor, enforce, disable, and retire the security shields, enabling a smooth transition to remediation. This capability helps businesses maintain continuous operations while managing risks until the software upgrades or patches are deployed. Refer to Live Protect Shields overview.
Regulatory activation for wireless controllers	Catalyst Center supports regulatory activation for Cisco Catalyst 9800 Series Wireless Controllers and Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches in nonfabric deployment. When the APs associated with a wireless controller are unable to obtain a country code through standard geolocation or proximity methods, the AP radios are not operational. Catalyst Center can use the regulatory activation file obtained from the Meraki dashboard to resolve the country code on these APs. Refer to Configure regulatory activation for wireless controllers.
RMA device support	Catalyst Center provides RMA support for Cisco IE3500 and IE3100 Rugged Series switches.
Support for automatic service insertion site updates for edge node and border node addition and deletion in fabric sites	Catalyst Center now automatically updates a service insertion site when an edge node or border node is added to or deleted from the corresponding fabric site. Refer to Manage devices associated with a service insertion site.
Support for Cisco TrustSec (CTS) data download over HTTPS	Catalyst Center allows using HTTPS for CTS policy and data download. You can enable or disable this option in Catalyst Center while configuring the ISE servers under **Design** > **Network Settings** > **Servers**. Refer to Add Cisco ISE or other AAA servers.

Feature	Description
Support for Cisco Wireless 9177D, 9177E, and 9177I Series Access Points	Catalyst Center supports the Cisco Wireless 9177D, 9177E, and 9177I Series Access Points. You can configure these APs with Wi-Fi 7 for Cisco IOS XE Release 26.2.1 or later, enable bridge and mesh roles, and use dual-band (XOR) capability to operate slot 2 in either 5-GHz or 6-GHz radio mode. **Note** When configuring these APs using the **Configure Access Points** workflow, you cannot set radio parameters for slot 2 in the **Configure 6 GHz Radio Parameters** window. Use the **Configure Dual-Band (XOR) Radio Parameters** window to manage these settings. Refer to Configure APs, Schedule recurring events for APs, Enable the Wi-Fi 7 configuration, and Supported hardware platforms.
Support for MACsec encryption in AP profile for Cisco IOS XE devices	Catalyst Center supports MACsec encryption and automatic MACsec configuration in AP profiles for Cisco IOS XE devices. The **MACsec Encrypted** toggle button is applicable for: • Cisco Catalyst 9000 Series Switches running Cisco IOS XE Release 17.18.3 or 26.1.1. • Wireless controllers running Cisco IOS XE Release 26.1.1 or later. **Note** Catalyst Center does not support MACsec encryption for fabric sites that contain Cisco Catalyst 9350 Series Smart Switches. The **Auto-Secure MACsec** toggle button is supported on applicable Wi-Fi 7 APs and Cisco Catalyst 9350 Series Smart Switches running Cisco IOS XE Release 26.2.1 or later. **Note** This configuration is supported only in nonfabric deployments on Cisco Catalyst 9350 Series Smart Switches. It is not supported in fabric deployments. Refer to Configure management settings for an AP profile for Cisco IOS XE devices.
Support for MACsec encryption for fabric APs	For the INFRA_VN virtual network, Catalyst Center supports MACsec encryption of AP uplink traffic for supported APs during anycast gateway configuration. Refer to Create anycast gateways.

Feature	Description
Support for security service insertion for SD-Access over HTTPS	Security service insertion for SD-Access is enhanced to support Cisco TrustSec (CTS) policy and data download over HTTPS: • To enable service insertion on a fabric site on day zero, you must enable CTS policy and data download over HTTPS for the site. • To disable CTS policy and data download over HTTPS for a site configured as a service insertion site, you must delete the security service insertion configuration. **Note** If you upgrade to this release from an earlier release, CTS policy and data download over HTTPS is disabled by default. You must enable CTS policy and data download over HTTPS on the service insertion site after you upgrade to ensure ongoing security service insertion operations on day *n*. Refer to Service insertion sites, Prechecks to enable a service insertion site on day zero and Add Cisco ISE or other AAA servers.
Support for Rule-Based Compliance (RBC) Remediation	Catalyst Center supports the remediation of violations generated by Rule-Based Compliance (RBC) policies, allowing you to automatically fix non-compliant devices by applying user-defined CLI commands.
Ultra Reliable Wireless Backhaul (URWB) network profile support for wireless controller.	You can create a Ultra Reliable Wireless Backhaul (URWB) network profile for a wireless controller and provision it. Refer to Create a URWB network profile for a Cisco Catalyst 9800 Series Wireless Controller
Rule-Based Compliance Remediation	Rule-based compliance remediation helps you manage rule-based violations. You can filter remediable and non-remediable issues and apply fixes through a preview or schedule them for deployments. Refer to Fix compliance violations, and Add a condition to the compliance policy rule.