



Wireless Automation MoP for Cisco DNA Center, Release 2.3.5.5

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL:
<https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners.
The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)
© 2023 Cisco Systems, Inc. All rights reserved.

Contents

Scope	5
MoP Summary	5
Detailed Guidelines	6
New Features and Parameters Guidelines	9
SSID and Guest Anchor Parameters List.....	9
RF Profile: New Parameters for Cisco Catalyst 9800 Series Wireless Controllers (Cisco IOS-XE) ..	10
AP Profile/Site Tag Parameters List.....	11
RLAN Workflow – L2 Fallback Authentication	12
Guidelines to Adjust New Features and Parameters Defaults	13
SSID: New Parameters.....	13
RF Profile: New Parameters.....	15
New Feature: AP Authorization List.....	18
New Feature: Anchor Group (Multiple Anchor Support)	19
New Feature: AP Profile	19
New Feature: SSID Scheduler	22
Compliance Report Review Guidelines (Feature-Based)	22
AP Profile Compliance Guidelines	22
RF Profile Compliance Guidelines.....	24
RLAN Feature Compliance Guidelines.....	24
Configuration Preview Guidelines (Feature-Based)	24
SSID and Mobility Anchor Config Preview Guidelines	24
RF Profile Configuration Preview Guidelines.....	28
RLAN Feature Config Preview Guidelines.....	28
SSID and Guest Anchor Parameters List for Cisco AireOS Wireless Controllers	29
RF Profile: New Parameters for Cisco AireOS Wireless Controllers	33
AP Profile: New Parameters for Cisco AireOS Wireless Controller	34

Scope

This document acts as a standard protocol for wireless automation provisioning operations for customers looking to upgrade to Cisco DNA Center Release 2.3.5.5 from Release 2.3.3.x or 2.3.5.x.

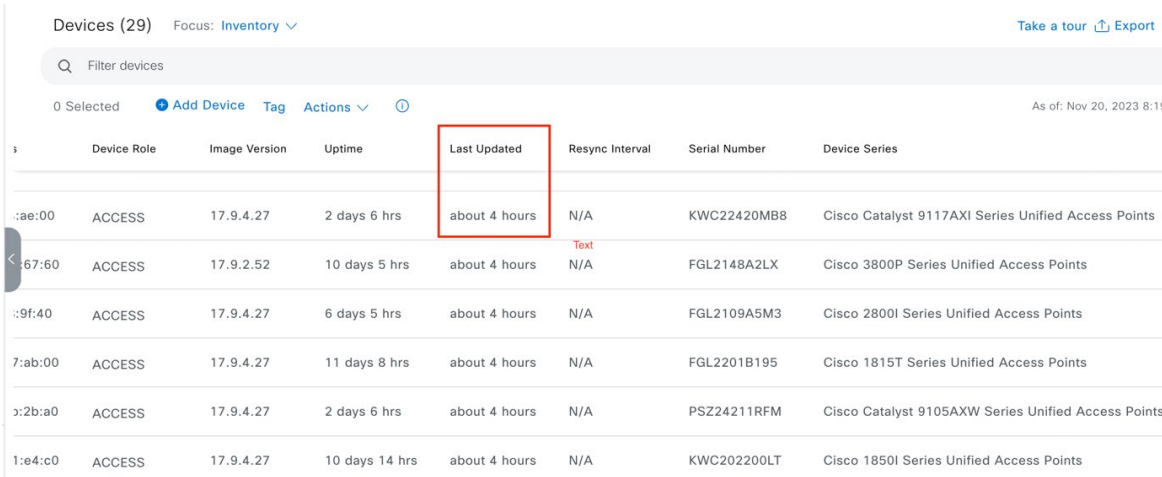
This document assesses the provisioning impact of new features and new parameters added to the existing features introduced **exclusively between Release 2.3.3.x and 2.3.5.5**.

MoP Summary

1. Upgrade to Cisco DNA Center Release 2.3.5.5.
2. After the upgrade, manually run compliance for all Cisco Wireless Controllers per the guidelines listed in [Detailed Guidelines](#) and review the compliance report.
3. To evaluate the impact of any violations reported in the compliance report, see [Detailed Guidelines](#).
4. If the compliance reports have any violations, adjust the Cisco DNA Center intent (under **Design > Network Settings > Wireless** and **Design > Network Profiles**) to match the values on the wireless controller.
5. Reprovision the wireless controller. Ensure that you review the reprovision summary and configuration preview before deploying the configuration.
6. Follow the guidelines in [Configuration Preview Guidelines \(Feature-Based\)](#) and ensure that unintended configurations aren't getting pushed.
7. Run compliance and ensure that there are no violations in the report.
8. We recommend that you remove any conflicting CLIs from the CLI template, if used. If you need further assistance, contact the Cisco Technical Assistance Center (TAC).

Detailed Guidelines

1. **After upgrade:** Check the last inventory synchronization status and last update time interval for all wireless controllers in the **Inventory** window as shown in the following figure.



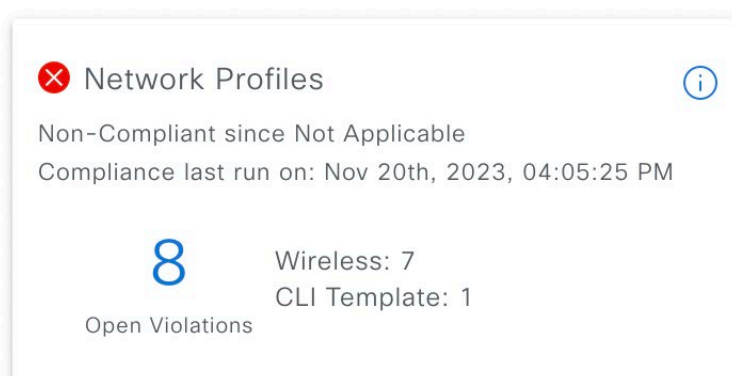
Devices (29) Focus: Inventory Take a tour Export

Filter devices

0 Selected Add Device Tag Actions ? As of: Nov 20, 2023 8:15

Device Role	Image Version	Uptime	Last Updated	Resync Interval	Serial Number	Device Series
ACCESS	17.9.4.27	2 days 6 hrs	about 4 hours	N/A	KWC22420MB8	Cisco Catalyst 9117AXI Series Unified Access Points
ACCESS	17.9.2.52	10 days 5 hrs	about 4 hours	N/A	FGL2148A2LX	Cisco 3800P Series Unified Access Points
ACCESS	17.9.4.27	6 days 5 hrs	about 4 hours	N/A	FGL2109A5M3	Cisco 2800I Series Unified Access Points
ACCESS	17.9.4.27	11 days 8 hrs	about 4 hours	N/A	FGL2201B195	Cisco 1815T Series Unified Access Points
ACCESS	17.9.4.27	2 days 6 hrs	about 4 hours	N/A	PSZ24211RFM	Cisco Catalyst 9105AXW Series Unified Access Points
ACCESS	17.9.4.27	10 days 14 hrs	about 4 hours	N/A	KWC202200LT	Cisco 1850I Series Unified Access Points

2. If the inventory synchronization hasn't finished after the upgrade, either wait for its completion or initiate a manual resynchronization.
3. Review the compliance status of all wireless controllers on the **Inventory** window.



4. If the last compliance run didn't occur after the most recent inventory resynchronization, initiate a compliance check, and review the report.

Foreign-WLC

🟢 Reachable | 🟢 Managed | IP Address: 10.76.41.92 | Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud | Device Role: ACCESS | Uptime: 68 days 10 hrs 47 mins | Site: Global/Bengaluru/BLD-14/Floor-1

- DETAILS
- Interfaces >
- Hardware & Software
- User Defined Fields
- Config Drift
- Wireless Info
- Mobility
- SECURITY
- Advisories
- COMPLIANCE
- Summary

You can now fix all configuration compliance issues on this device. You will be able to review before the fix is applied. [Fix All Configuration Compliance Issues](#)

Compliance Summary

[View Preference for Acknowledged Violations](#)

Next Compliance check is scheduled on Nov 20, 2023 11:38 PM

[Run Compliance Check](#)

✔ Network Settings 🔄

Compliant since Nov 20th, 2023, 04:05:23 PM
Compliance last run on: Nov 20th, 2023, 04:05:23 PM

0

Open Violations

✔ EoX - End of Life 🔄

Compliance last run on: Nov 20th, 2023, 05:20:05 PM

Software : ✔ Compliant
Hardware : ✔ Compliant
Module : ✔ Compliant

✔ Startup vs Running Configuration 🔄

Compliance last run on: Nov 20th, 2023, 04:05:23 PM

2 days

since in sync

Lines added: 0
Lines removed: 0
Lines modified: 0

✘ Network Profiles 🔄

Non-Compliant since Nov 15th, 2023, 01:02:22 PM
Compliance last run on: Nov 20th, 2023, 04:05:25 PM

22

Open Violations

CLI Template: 3
Wireless: 19

⊖ Software Image 🔄

Compliance last run on: Nov 20th, 2023, 04:05:23 PM

NA

Golden image is not available.

Running Version: 17.12.1prd6

✔ Critical Security Advisories 🔄

Compliant since Nov 20th, 2023, 04:05:23 PM
Compliance last run on: Nov 20th, 2023, 04:05:23 PM

0

5. Check the **Wireless** tab under **Network Profiles**.

Compliance Summary / Network Profiles

Wireless (7)

6. Sample compliance report (**Wireless** tab of **Network Profiles**):

Compliance Summary / Network Profiles [View Preference for Acknowledged Violations](#)

Wireless (71)

🔍 Search Table

Open Violations (71) Acknowledged Violations (0)

0 Selected Acknowledge

Model Name	Attribute	Status	Intended Value	Actual Value	Action
AP Join Profile/APJ_BGL_BGL18_35fbf	Management Username	Changed	-	oobapuser	Acknowle
AP Join Profile/APJ_BGL_BGL18_35fbf	SSH	Changed	Disable	Enable	Acknowle
AP Join Profile/APJ_BGL_BGL18_35fbf	CDP State	Changed	Enable	Disable	Acknowle
AP Join Profile/APJ_BGL_BGL18_35fbf	Dot1x Username	Changed	-	eap-tls-user	Acknowle
AP Join Profile/APJ_BGL_BGL18_35fbf	EAP Type	Changed	EAP-FAST	EAP-TLS	Acknowle
AP Join Profile/APJ_BGL_BGL18_35fbf	Client Limit	Changed	0	333	Acknowle
AP Join Profile/APJ_BGL_BGL18_35fbf	Offset Minute	Changed	0	30	Acknowle

7. Following are the guidelines to understand the compliance report based on the reported status:
 - a. **"Added"**: Cisco DNA Center will delete the corresponding configurations during the next remediation or reprovision operation.
 - b. **"Deleted"**: Cisco DNA Center will add the corresponding configurations during the next remediation or reprovision operation.
 - c. **"Changed"**: Cisco DNA Center will replace the corresponding configuration values with the intended values during the next remediation or reprovision operation.
8. If there are any discrepancies, we recommend that you adjust the network settings or network profiles and ensure that the default values for any new parameters or features align with the CLI Template or out-of-band values.
9. For the feature-based and parameter-based guidelines, see the tables in [New Features and Parameters Guidelines](#).
10. To configure new parameters and features on the Cisco DNA Center Design windows, see [Guidelines to Adjust New Features and Parameters Defaults](#).
11. Review the reprovision summary information before deploy during the provision workflow and confirm that all the parameter values align with the intended values.
12. View all the new parameters introduced in Cisco DNA Center Release 2.3.5.4 listed in [New Features and Parameters Guidelines](#). If you need to adjust these values, adjust them as necessary.
13. We recommend that you run the configuration preview before each provision. Look for any configurations that can potentially impact the network based on the information in [New Features and Parameters Guidelines](#) and [Configuration Preview Guidelines \(Feature-Based\)](#). If any unintended configurations are detected, determine if they're due to a mismatch in the compliance report. If not, report the issue to Cisco TAC.
14. We recommend that you remove any conflicting CLIs from the CLI template, if used. For further assistance, contact Cisco TAC.

New Features and Parameters Guidelines

SSID and Guest Anchor Parameters List

Compliance Table Entry	Platform	Cisco DNA Center Feature Name	Cisco DNA Center Parameter Name	Default Value in Cisco DNA Center	Impact Severity	Impact Details
Accounting List name	9800	SSID	Accounting Server	Same as Authentication Servers	High	Client flap due to policy profile update; accounting function won't work
Coverage Hole Detection	9800	SSID	Coverage Hole Detection	Enabled	Low	Client flap due to WLAN update
Protected Management Frame	9800	SSID	Protected Management Frame (802.11w)	Enabled	Low	Client flap due to WLAN update
Auth Key Mgmt/CCKM	9800	SSID	CCKM	Disabled	Medium	CCKM fast secure roaming is impacted
Primary	9800	Anchor Group	Anchor WLC	None	High	Wireless Client disruption due to missing mobility anchors for nonguest SSID
Calendar-profile	9800	SSID Scheduler	Calendar-profile	None	High	As the scheduler won't work, if WLAN is down due to the scheduler, it won't be enabled automatically
AP Authorization List	9800	AP Authorization List	AP Authorization List	NA	NA – No Impact	No Impact

RF Profile: New Parameters for Cisco Catalyst 9800 Series Wireless Controllers (Cisco IOS-XE)

Profile	Parameter Name per the Compliance Report	Parameter Name per the Cisco DNA Center Design Windows	Band	Cisco DNA Center Defaults	Impact Severity	Impact Details
RF Profile	CHD Voice RSSI Threshold	Voice RSSI Threshold (dBm)	6GHz/5GHz/2.4 GHz	-80	Low	No Impact
RF Profile	CHD Data RSSI Threshold	Data RSSI Threshold (dBm)	6GHz/5GHz/2.4 GHz	-80	Low	No Impact
RF Profile	CHD Min Client Level	Minimum Client Level (clients)	6GHz/5GHz/2.4 GHz	3	Low	No Impact
RF Profile	CHD Exception Level (%)	Exception Level (%)	6GHz/5GHz/2.4 GHz	0.25	Low	No Impact
RF Profile	OBSS PD	OBSS PD	6GHz/5GHz/2.4 GHz	Disable	Low	Can cause a momentary radio reset
RF Profile	Non-SRG OBSS PD Max Threshold	Non-SRG OBSS PD Max Threshold (dBm)	6GHz/5GHz/2.4 GHz	-62	Low	Can cause a momentary radio reset
RF Profile	SRG OBSS PD	SRG OBSS PD	6GHz/5GHz/2.4 GHz	Disable	Low	Can cause a momentary radio reset
RF Profile	SRG OBSS PD Min Threshold	SRG OBSS PD Min Threshold (dBm)	6GHz/5GHz/2.4 GHz	-82	Low	Can cause a momentary radio reset
RF Profile	SRG OBSS PD Max Threshold	SRG OBSS PD Max Threshold (dBm)	6GHz/5GHz/2.4 GHz	-62	Low	Can cause a momentary radio reset
RF Profile	Client Aware	Client Aware	5GHz	Disabled	Low	No Impact
RF Profile	Client Reset (%)	Client Reset (%)	5GHz	50	Low	No Impact
RF Profile	Client Select (%)	Client Select (%)	5GHz	5	Low	No Impact
RF Profile	Zero Wait DFS	Zero Wait DFS	5GHz	Disabled	Low	No Impact
RF Profile	Client Reset Count	Client Reset Count	6GHz	1	Low	No Impact
RF Profile	Broadcast Probe Response Interval	Broadcast Probe Response Interval (msec)	6GHz	20	Low	Can cause a momentary radio reset
RF Profile	PSC Enforcing	Enable PSC Enforcing	6GHz	Disabled	Low	No Impact
RF Profile	Multi BSSID Profile Name	Same as RF Profile name	6GHz	default-multi-bssid-profile	Low	Can cause a momentary radio reset
RF Profile	6 GHz Discovery Frames	6 GHz Discovery Frames	6GHz	None	Low	No Impact

RF Profile	Client Utilization Threshold (%)	Client Utilization Threshold (%)	6GHz	0.05	Low	No Impact
RF Profile	Downlink OFDMA	Downlink OFDMA	6GHz	Enabled	Low	Can cause a momentary radio reset
RF Profile	Uplink MU-MIMO	Uplink MU-MIMO	6GHz	Enabled	Low	Can cause a momentary radio reset
RF Profile	Uplink OFDMA	Uplink OFDMA	6GHz	Enabled	Low	Can cause a momentary radio reset
RF Profile	TWT Broadcast Support	TWT Broadcast Support	6GHz	Enabled	Low	Can cause a momentary radio reset
RF Profile	Target Waketime	Target Waketime	6GHz	Enabled	Low	Can cause a momentary radio reset
RF Profile	Downlink MU-MIMO	Downlink MU-MIMO	6GHz	Enabled	Low	Can cause a momentary radio reset

AP Profile/Site Tag Parameters List

Feature Name	Parameter Name per the Compliance Report	Cisco DNA Center Parameter Name in the Design Windows	Cisco DNA Center Defaults	Impact Severity	Impact Details
AP Profile	EAP Type	Access Points Authentication	None	High	If the EAP Type is changed, it can result in the AP disconnection
AP Profile	Country Code	Country Code	Unconfigured	High	Change in country code can cause the AP dissociation
AP Profile	Management Username	Username (under SSH and Telnet Section)	Unconfigured	Medium	Overwriting or erasing the AP management username can result in an inability to log in and affect the troubleshooting operations
AP Profile	SSH	SSH	Disabled	Medium	SSH can get disabled
AP Profile	Telnet	Telnet	Disabled	Low	Telnet can get disabled
AP Profile	Offset Minute	OFFSET MM	0	Medium	Can result in the AP not getting the correct time/time zone information from the wireless controller
AP Profile	aWIPS	aWIPS	Enabled	Medium	AWIPS can get enabled inadvertently
AP Profile	Time Zone	Time Zone	None	Medium	Can cause the AP not to get the right time/time zone information
AP Profile	Client Limit	Client Limit	0	Medium	This sets no client limit on the AP profile
AP Profile	aWIPS Forensic	Forensic Capture	Disabled	Medium	Forensic capture can get disabled inadvertently
AP Profile	Rogue Detection	Rogue Detection	Enabled	Medium	Rogue detection can get disabled inadvertently
AP Profile	CDP State	CDP State	Enabled	Medium	CDP neighbor discovery doesn't work
AP Profile	Dot1x Username	Username under Access Point	Unconfigured	High	Change in the Dot1x username can result in the AP not getting associated

		Authentication when EAP-FAST or EAP-PEAP is selected			
AP Profile	Offset Hour	OFFSET HH	0	Medium	Can cause the AP not to get the right time/time zone information
AP Profile	Mesh Profile Name	Same as AP Profile Name	default-mesh-profile	High	Mesh Settings changes can cause the AP to reboot
Site Tag	AP Join Profile	AP Profile	default-ap-profile	High	Change of the AP profile mapping within the site tag can cause the AP to reboot
Mesh Profile	Dot11bg Backhaul Rate Type	2.4GHz Band Radio Type	Auto	Medium	Can cause a mesh link flap when the data rate type is changed
Mesh Profile	Bridge Group Name	Bridge Group Name	Blank/Empty	High	Change in BGN can cause the AP dissociation
Mesh Profile	Range	Range – Root AP to Mesh AP (in feet)	12000	High	Change in the range can cause the AP to reboot
Mesh Profile	Backhaul Client Access	Backhaul Client Access	Disabled	High	Change in the backhaul client access can cause the AP to reboot
Mesh Profile	Dot11a Backhaul Rate Type	5GHz Band Radio Type	Auto	Medium	Can cause a mesh link flap when the data rate type is changed

RLAN Workflow – L2 Fallback Authentication

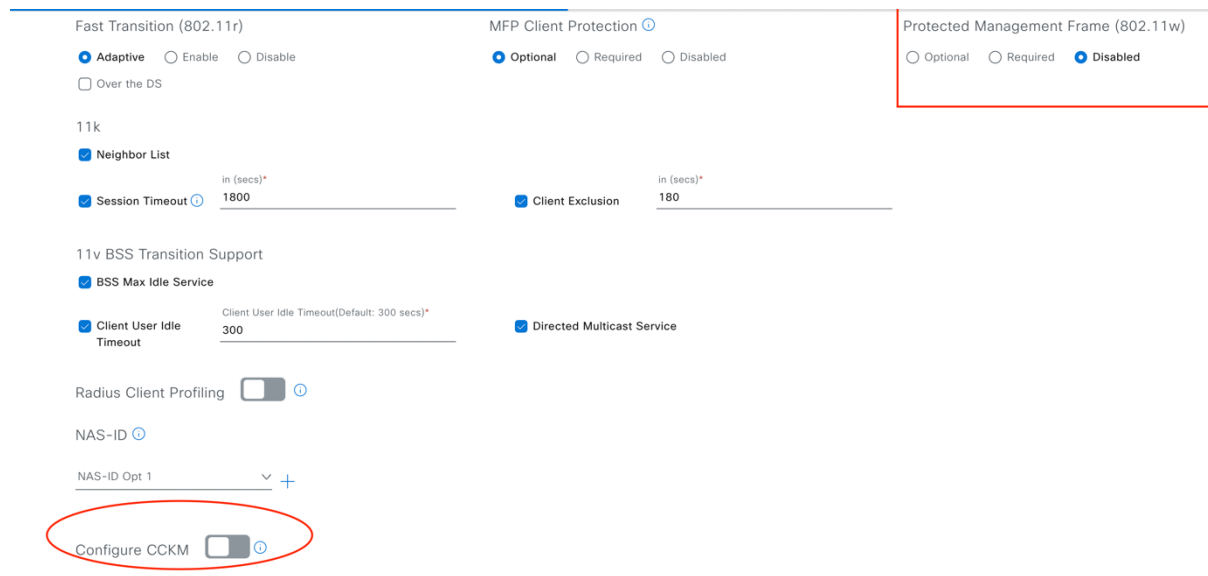
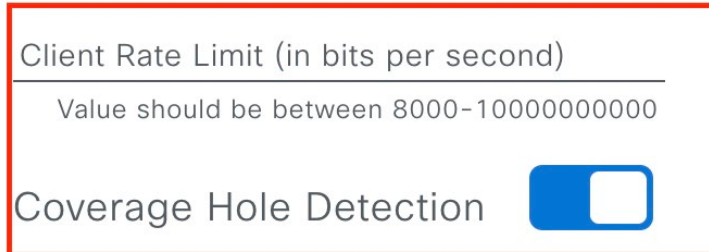
Compliance Table Entry	Platform	Feature Name	Parameter Name	Default Value in Cisco DNA Center	Impact Severity	Impact Details
Fallback Authentication	9800	RLAN	MAC Filtering on Dot1x failure Dot1x on MAC Filtering failure	None	High	RLAN wired clients can't achieve the fallback mechanism for L2 authentication if there is Dot1x or Mac filter failure

Guidelines to Adjust New Features and Parameters Defaults

SSID: New Parameters

Path: **Design > Network Settings > Wireless > SSID > Advanced Settings**

Parameter Names: Client Rate Limit, Coverage Hole Detection (CHD), Protected Management Frame (802.11w), Configure CCKM



Path: **Design > Network Settings > Wireless > SSID > Security Settings**

Parameter Names: AAA Override, Accounting Servers, MP SK

Authentication, Authorization, and Accounting Configuration

 AAA Configured (1)

AAA Override



Mac Filtering


Enable Posture 

Fast Lane 

Deny RCM Clients 

Configure AAA Server for Test

 Two (2) Warning Alerts on this page. [Collapse](#) to hide. 

 Two (2) Warning Alerts



Catalyst 9800 Controllers versions less than 17.9 support only upto 8 Accounting Method list configuration. Configuring more than that will result in provisioning failure. To ensure the right configuration is pushed for this SSID, configure one or more AAA/PSN.

Configure Authentication and Authorization Servers

Select Value  

Copy same Servers for Accounting

Configure Accounting Server

Select Value  

Cancel

Configure

Enterprise Personal Open Secured Open

WPA2 WPA3

Most secure

A password (Pre-Shared Key PSK with WPA2 encryption) is needed to access the wireless network.

WPA3 feature is supported for Wireless Controller version 8.10 & above, For Catalyst 9800 Controllers version 16.12 & above.

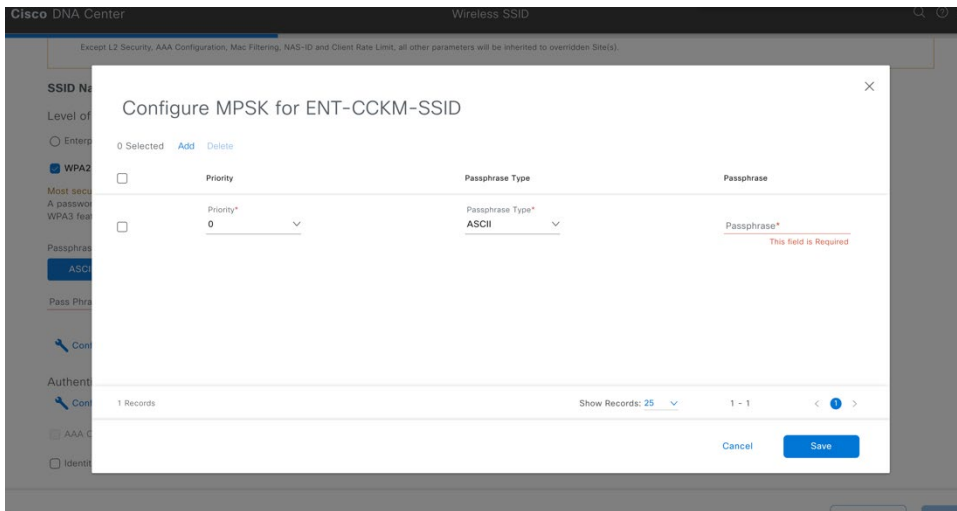
Passphrase Type

ASCII HEX

Pass Phrase*

Enter pass phrase

 Configure MP SK 



RF Profile: New Parameters

Path: **Design > Network Settings > Wireless > Wireless Radio Frequency Profile**

Parameter Names: CHD Voice RSSI Threshold, CHD Data RSSI Threshold, CHD Min Client Level, CHD Exception Level (%), OBSS PD, Non-SRG OBSS PD Max Threshold, SRG OBSS PD, SRG OBSS PD Min Threshold, SRG OBSS PD Max Threshold, Client Aware, Client Reset (%), Client Select (%), Client Reset Count, Broadcast Probe Response Interval, Multi BSSID Profile Name, 6 GHz Discovery Frames, Client Utilization Threshold (%), Downlink OFDMA, Uplink MU-MIMO, Uplink OFDMA, TWT Broadcast Support, Target Waketime, Downlink MU-MIMO

Coverage Hole Detection (applicable for the 2.4-GHz, 5-GHz and 6-GHz RF bands)

Coverage Hole Detection

Enable Global Coverage Hole Detection in RRM General Configuration for the corresponding radio band

Minimum Client Level (clients)*

3

Value must be between 1 to 200

Data RSSI Threshold (dBm)*

-80

Value must be between -90 to -60

Voice RSSI Threshold (dBm)*

-80

Value must be between -90 to -60

Exception Level (%)*

25

Value must be between 0 to 100%

802.11ax Spatial Reuse Parameters (applicable for the 2.4-GHz, 5-GHz and 6-GHz RF bands)

802.11ax ⓘ

Configure Spatial Reuse Parameters for this profile.

SPATIAL REUSE

OBSS PD ⓘ

Non-SRG OBSS PD Max Threshold (dBm)*

-62

Value must be between -82 to -62

SRG OBSS PD ⓘ

SRG OBSS PD Min Threshold (dBm)*

-82

Value must be between -82 to -62

SRG OBSS PD Max Threshold (dBm)*

-62

Value must be between -82 to -62

Client Aware FRA (Applicable for the 5-GHz RF band)

Flexible Radio Assignment (FRA)

Enable FRA in the Flexible Radio Assignment (FRA) configuration for the corresponding radio band in

Client Aware

Client Select (%)*

50

Value must be between 0 to 100%

Client Reset (%)*

5

Value must be between 0 to 100%

6-GHz FRA Parameters

Flexible Radio Assignment (FRA) ⓘ

Enable FRA in the Flexible Radio Assignment (FRA) configuration for the corresponding radio band

Client Reset Count*

1

Value must be between 1 to 10

Client Utilization Threshold (%)*

5

Value must be between 0 to 100%

6-GHz 802.11ax Parameters including Multi BSSID Profile

802.11ax

Configure Multi-BSSID and Spatial Reuse Parameters for this profile.

6 GHz Discovery Frames

None



[Learn More](#)

Broadcast Probe Response Interval (msec)*

20

Value must be between 5 to 25

MULTI BSSID

Enable Multi BSSID in Dot11ax configuration for the corresponding radio band in the [Model Config Editor](#) :

- Downlink OFDMA
- Uplink OFDMA
- Downlink MU-MIMO
- Uplink MU-MIMO
- Target Waketime
- TWT Broadcast Support

Path: **Design-> Network Settings-> Wireless -> Wireless Radio Frequency Profile**

Parameter Names: Enable PSC Enforcing (applicable for 6GHz RF only)

2.4 GHz

5 GHz

6 GHz

6 GHz ⓘ



Channel Width

Best

Enable PSC Enforcing ⓘ



Path: **Design > Network Settings > Wireless > Wireless Radio Frequency Profile**

Parameter Names: Zero Wait DFS (Applicable for 5-GHz RF only)

5 GHz



Parent Profile

High	Medium (Typical)	Low	Custom
------	------------------	-----	---------------

Channel Width

20 MHz



Zero Wait DFS

New Feature: AP Authorization List

Path: **Design > Network Settings > Wireless > AP Authorization List**

Design / Network Settings 🔍 ? ⚠️ 🔔

Telemetry ×

AP Authorization List

You can create a list to authorize an Access Point. Local Authorization for Access Point(s) happens through MAC address, Serial Number or both against local database. For AAA Authorization, specify the list of AAA Servers for authorization. [Refer to AP Authorization List Guidelines](#)

For AireOS wireless controllers, Cisco DNA Center supports only MAC Address for AP Authorization. If both Serial Numbers and MAC Address are configured, only MAC Address will be provisioned for AireOS devices.

List name*

Local Auth AAA Auth

Number of

2 (MAC A) Configure Local Authorization

3 (MAC A)

New Feature: Anchor Group (Multiple Anchor Support)

Path: **Design > Network Settings > Wireless > Anchor Group**

Design / Network Settings 🔍 ? 🚨 🔔

lemetr ✕

MAC A

MAC A

You can create anchor groups of maximum 3 controllers with different priorities acting as anchors, to manage the traffic of the SSIDs.

Anchor Group Name*

[Add Managed WLC](#) [Add External WLC](#) [Add Existing External WLC](#)

Anchor WLC ▲	Wireless Management IP	Manageability	Priority Order ①	Actions
No data to display				

New Feature: AP Profile

Path: **Design > Network Settings > Wireless > AP Profile- default-ap-profile**

SSH and Telnet

Enable SSH and Telnet to add credentials for device management. If SSH and Telnet are disabled, credentials can still be added for console access.

SSH Telnet

Username* admin [View Username Policy](#)

Password* ***** [SHOW](#) [View Password Policy](#)

Enable Password* **** [SHOW](#) [View Password Policy](#)

Cisco Discovery Protocol (CDP) State

Enable CDP in order to make Cisco Access Points known to its neighboring devices and vice-versa.

CDP State

aWIPS and Forensic Capture Enablement

aWIPS ⓘ Forensic Capture ⓘ

Rogue Detection

Detect Access Points that have been installed on a secure network without explicit authorization from a system administrator

Rogue Detection

[Wireless](#) / [Edit AP Profile](#)

Mesh Settings

MAC address of APs in mesh mode must be added to the AP Authorization list.

Mesh ⓘ

Range - Root AP to Mesh AP (in feet)

12000

Value should be between 150-132000

Backhaul Client Access

RAP Downlink Backhaul

5 GHz 2.4 GHz

BACKHAUL DATA RATES

5GHz Band Radio Type

auto ▼

2.4GHz Band Radio Type

auto ▼

BRIDGE GROUP ⓘ

Bridge Group Name _____

AP Power Profile

Select the AP Power Profile that should be applied to Access Points. If an Access Point does not receive the required power, it will function in a derated state as defined by the sequence of rules in the Power Profile.

Only Power profiles with rules will be listed below.

This setting is applicable only for IOS-XE based Wireless Controllers running 17.10.1 and above.

Select Value ▼

Calendar Power Profile

Select the AP Power Profile that should be applied to Access Points in power save mode. You can map multiple Power Profiles to different calendar schedules based on your requirement. All rules defined in the Power Profile take effect simultaneously in the configured schedule.

Calendar Power Profile (0)

Search Table

Country Code ⓘ

Set the country code for ROW Access Points that have no country code configured already. This setting will not impact the Access Points that already have a country code configured.

Select Value ▼

Time Zone ⓘ

Not Configured

If the Time Zone is not configured, Access Points operate in the UTC Time Zone

Controller

Access Points operate in the Controller Time Zone

Delta from Controller

Set the offset time from the Controller Time Zone

Client Limit ⓘ

Maximum Client Limit

0

Value should be between 0-1200

New Feature: SSID Scheduler

The screenshot shows the Cisco DNA Center interface for configuring an SSID Scheduler. The main panel is titled 'Create Scheduler' and contains the following fields and options:

- SSID Scheduler Name***: A text input field.
- Scheduler Function**: A section with explanatory text and two radio button options: Client Deny and Enable SSID.
- Scheduler Type**: A section with explanatory text and three radio button options: DAILY, WEEKLY, and MONTHLY. Below these are seven circular icons representing days of the week (S, M, T, W, T, F, S).
- Start time*** and **End time***: Text input fields with a plus sign icon between them.
- Time Zone**: A dropdown menu currently set to 'Asia/Bangkok'.

The left sidebar shows the navigation path: 'Wireless / SSID Scheduler'. Below this is a table with columns: 'SSID Scheduler Name', 'Scheduler Function', 'Scheduler Type', 'Scheduler Timezone', and 'Schedule'. The table currently displays 'No data to display'.

Compliance Report Review Guidelines (Feature-Based)

AP Profile Compliance Guidelines

If any out-of-band custom AP profiles are created and mapped to the Cisco DNA Center-configured site tag, review them as shown in the following figure.

The screenshot shows the 'Compliance Summary / Network Profiles' page. The main section is titled 'Wireless (71)'. Below this is a table with columns: 'Model Name', 'Attribute', 'Status', 'Intended Value', 'Actual Value', and 'Action'. The table contains three rows, with the last row highlighted by a red border:

Model Name	Attribute	Status	Intended Value	Actual Value	Action
RF Profile/BGL17-RF-PROFILE_6	6 GHz Discovery Frames	Changed	0	1	Acknowledge
RF Profile/BGL18-F2-RF-PROFILE_6	6 GHz Discovery Frames	Changed	0	2	Acknowledge
Site Tag/ST_BGL_BGL16_d114e_0	AP Join Profile	Changed	default-ap-profile	bgl16-ooob-ap-profile	Acknowledge

If this configuration isn't intended, create the AP profile from **Design > Network Settings > Wireless > AP Profiles** and create the AP profile with the same name as the one which was created out-of-band earlier, while running Cisco DNA Center Release 2.3.3.7. Map this AP profile to either the Cisco DNA Center-generated site tag or the custom site tag under **Design > Network Profiles** for this network profile.

1. If the default-AP-profile is updated on the wireless controller out of band, then the configuration mismatches aren't displayed in compliance. Review the following sections in the configuration preview.

Provision Device - Configuration preview

Nov 20, 2023 5:13 PM | Status: ✔ Success

The screenshot shows the 'Configuration Preview' for a device with IP 10.76.34.85. The configuration tree is as follows:

- Cisco-IOS-XE-wireless-site-cfg
 - site-cfg-data
 - ap-cfg-profiles
 - ap-cfg-profile
 - profile-name : default-ap-profile
 - awips-enabled : true
 - description : Default AP Profile for IOS-XE
 - awips-forensic-enabled : false
 - rogue-detection
 - lsc-ap-auth-type-info
 - ap-country
 - capwap-window
 - cdp
 - login-credentials
 - oeap
 - client-limit
 - ap-prof-pp-cfg
 - dot1x-eap-type-info
 - ap-tz-config
 - device-mgmt** (highlighted)
 - telnet : false
 - ssh : false
 - mesh

The management configuration ssh/telnet is highlighted in the preceding figure. The same is applicable for all other configurations shown in the preceding preview that are modified out-of-band.

The screenshot shows the 'Cisco DNA Center' interface. The 'CLI Deviations' section is active, showing a table of deviations for the device 'WLAN_01'. The right pane displays the resulting configuration commands, including:

```
telnet disable
ssh disable
telnet enable
ssh enable
```

RF Profile Compliance Guidelines

After the compliance is run, all the mismatches in the RF profile settings are shown as follows, if there are any out-of-band changes.

<input type="checkbox"/>	RF Profile/BGL18-F2-RF-PROFILE_b	SRG OBSS PD Min Threshold	Changed	-82	-80	Acknowledge
<input type="checkbox"/>	RF Profile/BGL18-F2-RF-PROFILE_a	CHD Data RSSI Threshold	Changed	-80	-82	Acknowledge
<input type="checkbox"/>	RF Profile/BGL18-F2-RF-PROFILE_a	CHD Exception Level (%)	Changed	25	27	Acknowledge
<input type="checkbox"/>	RF Profile/BGL18-F2-RF-PROFILE_a	CHD Min Client Level	Changed	3	5	Acknowledge
<input type="checkbox"/>	RF Profile/BGL18-F2-RF-PROFILE_a	CHD Voice RSSI Threshold	Changed	-80	-82	Acknowledge
<input type="checkbox"/>	RF Profile/BGL18-F2-RF-PROFILE_a	Client Aware	Changed	Disable	Enable	Acknowledge
<input type="checkbox"/>	RF Profile/BGL18-F2-RF-PROFILE_a	Client Reset (%)	Changed	5	7	Acknowledge
<input type="checkbox"/>	RF Profile/BGL18-F2-RF-PROFILE_a	Client Select (%)	Changed	50	52	Acknowledge
<input type="checkbox"/>	RF Profile/BGL18-F2-RF-PROFILE_a	Non-SRG OBSS PD Max Threshold	Changed	-62	-72	Acknowledge
<input type="checkbox"/>	RF Profile/BGL18-F2-RF-PROFILE_a	OBSS PD	Changed	Disable	Enable	Acknowledge
<input type="checkbox"/>	RF Profile/BGL18-F2-RF-PROFILE_a	SRG OBSS PD	Changed	Disable	Enable	Acknowledge
<input type="checkbox"/>	RF Profile/BGL18-F2-RF-PROFILE_a	SRG OBSS PD Max Threshold	Changed	-62	-65	Acknowledge
<input type="checkbox"/>	RF Profile/BGL18-F2-RF-PROFILE_a	SRG OBSS PD Min Threshold	Changed	-82	-75	Acknowledge
<input type="checkbox"/>	RF Profile/BGL18-F2-RF-PROFILE_a	Zero Wait DFS	Changed	false	true	Acknowledge

RLAN Feature Compliance Guidelines

Compliance summary with mismatch of RLAN fallback parameters:

The screenshot shows the Cisco DNA Center interface with a compliance summary for RLAN fallback parameters. The table below represents the data shown in the interface:

Model Name	Attribute	Status	Intended Value	Actual Value	Action
Rlan/prof-1/Building-01/A1-B1-F1-P1	Fallback Authentication	Changed	Not Configured	MAC Filtering on Dot1x failure	Acknowledge
Rlan/prof-1/Building-01/A1-B1-F1-P2	Fallback Authentication	Changed	Not Configured	MAC Filtering on Dot1x failure	Acknowledge
Rlan/prof-1/Building-01/A1-B1-F1-P3	Fallback Authentication	Changed	Not Configured	Dot1x on MAC Filtering failure	Acknowledge
Rlan/prof-1/Building-01/A1-B1-F2-P1	Fallback Authentication	Changed	Not Configured	Dot1x on MAC Filtering failure	Acknowledge
Rlan/prof-1/Building-01/A1-B1-F2-P3	Fallback Authentication	Changed	Not Configured	MAC Filtering on Dot1x failure	Acknowledge
Rlan/prof-1/Building-01/A1-B1-F3-P1	Fallback Authentication	Changed	Not Configured	Dot1x on MAC Filtering failure	Acknowledge
Rlan/prof-1/Building-01/A1-B1-F3-P2	Fallback Authentication	Changed	Not Configured	MAC Filtering on Dot1x failure	Acknowledge

Configuration Preview Guidelines (Feature-Based)

SSID and Mobility Anchor Config Preview Guidelines

Configuration preview displaying delete and removal of attribute

Configuration preview and relevant compliance mismatches

<input type="checkbox"/>	Policy Profile/Primary-9.60.1.94	Primary-9.60.1.94	Added	-	View Details	Acknowledge
<input type="checkbox"/>	Policy Profile/Secondary-9.60.1.94	Secondary-9.60.1.94	Added	-	View Details	Acknowledge
<input type="checkbox"/>	Policy Profile/Self-anchored_Global_NF_f0a3357e	isAnchor	Changed	Disable	Enable	Acknowledge
<input type="checkbox"/>	Policy Profile/Tertiary-9.60.1.100	Tertiary-9.60.1.100	Added	-	View Details	Acknowledge
<input type="checkbox"/>	Policy Profile/Tertiary-9.60.1.105	Tertiary-9.60.1.105	Added	-	View Details	Acknowledge
<input type="checkbox"/>	Policy Profile/Tertiary-9.60.1.106	Tertiary-9.60.1.106	Added	-	View Details	Acknowledge
<input type="checkbox"/>	Policy Profile/Tertiary-Disconnect	Tertiary-9.60.1.93	Added	-	View Details	Acknowledge
<input type="checkbox"/>	Policy Profile/Tertiary-9.60.1.94	Tertiary-9.60.1.94	Removed	View Details	-	Acknowledge
<input type="checkbox"/>	Policy Profile/Tertiary-9.60.1.94	Tertiary-9.60.1.94	Added	-	View Details	Acknowledge
<input type="checkbox"/>	Policy Profile/Tertiary-9.60.1.95	Tertiary-9.60.1.95	Added	-	View Details	Acknowledge
<input type="checkbox"/>	Policy Profile/Tertiary-9.60.1.99	Tertiary-9.60.1.99	Added	-	View Details	Acknowledge

Configuration Preview

Device IP : 10.76.41.92

Show in tree view

CLI Section ✕ ↕

- ▼ 📁 guest-mm-db-export-entry [-] Remove
 - 🍃 ip : 9.60.1.94
- ▼ 📁 guest-mm-db-export-entry [-] Remove
 - 🍃 ip : 9.60.1.105
- ▼ 📁 guest-mm-db-export-entry [-] Remove
 - 🍃 ip : 9.60.1.106
- ▼ 📁 guest-mm-db-export-entry [-] Remove
 - 🍃 ip : 9.60.1.94
- ▼ 📁 guest-mm-db-export-entry [-] Remove
 - 🍃 ip : 9.60.1.105
- ▼ 📁 guest-mm-db-export-entry [-] Remove
 - 🍃 ip : 9.60.1.106
- ▼ 📁 per-ssid-qos

- ▼ 📁 guest-mm-db-export-entry [-] Remove
 - 🍃 ip : 9.60.1.93
- ▼ 📁 guest-mm-db-export-entry [-] Remove
 - 🍃 ip : 9.60.1.94
- ▼ 📁 guest-mm-db-export-entry [-] Remove
 - 🍃 ip : 9.60.1.95
- ▼ 📁 guest-mm-db-export-entry [-] Remove
 - 🍃 ip : 9.60.1.99
- ▼ 📁 guest-mm-db-export-entry [-] Remove
 - 🍃 ip : 9.60.1.100
- ▼ 📁 guest-mm-db-export-entry [-] Remove
 - 🍃 ip : 9.60.1.93

- policy-profile-calendar-configs
 - policy-profile-calendar-config [-] Delete
 - calendar-profile-name : test-10

- mpsk-keys
 - mpsk-key [-] Remove
 - mpsk-key-format : key-ascii

Cisco DNA Center

					Actual Value
<input type="checkbox"/>	Policy Profile/Self-anchored_Global_NF_f0a3357e	isAnchor	Changed		
<input type="checkbox"/>	Policy Profile/Tertiary-9.60.1.100	Tertiary-9.60.1.100	Added		
<input type="checkbox"/>	Policy Profile/Tertiary-9.60.1.105	Tertiary-9.60.1.105	Added		Wlan/17-1
<input type="checkbox"/>	Policy Profile/Tertiary-9.60.1.106	Tertiary-9.60.1.106	Added		Details MPSK Key Format: key-ascii MPSK priority: 1
<input type="checkbox"/>	Policy Profile/Tertiary-9.60.1.93	Tertiary-9.60.1.93	Added		
<input type="checkbox"/>	Policy Profile/Tertiary-9.60.1.94	Tertiary-9.60.1.94	Removed		
<input type="checkbox"/>	Policy Profile/Tertiary-9.60.1.94	Tertiary-9.60.1.94	Added		
<input type="checkbox"/>	Policy Profile/Tertiary-9.60.1.95	Tertiary-9.60.1.95	Added		
<input type="checkbox"/>	Policy Profile/Tertiary-9.60.1.99	Tertiary-9.60.1.99	Added		
<input type="checkbox"/>	Wlan/17-1	17-1	Added		
<input type="checkbox"/>	Wlan/17-2	17-2	Added		
<input type="checkbox"/>	Wlan/ENT-CCKM-S_Global_NF_976f193d	Auth Key Mgmt/CCKM	Changed		
<input type="checkbox"/>	Wlan/ENT-SSID-N_Global_NF_a51020c8	Coverage Hole Detection	Changed		
<input type="checkbox"/>	Wlan/ENT-SSID-N_Global_NF_a51020c8	Protected Management Frame	Changed		
<input type="checkbox"/>	Policy Profile/EWA-SSID-P_Global_NF_909a82c5	Accounting List Name	Changed	-	accounting-server-1 Acknowledge

- wlan-timeout
 - session-timeout : 1800
 - idle-timeout : 300
 - accounting-list
- wlan-policy ENT-SSID-Q_Global_NF_c69904d5
 - policy-profile-name : ENT-SSID-Q_Global_NF_c69904d5
 - interface-name : 1

```
api-vap-tu-data PSK-SSID_Global_INF_423ea5b9  
  
broadcast-ssid : true  
ccx-aironet-ie : false  
ssid : PSK-SSID  
wlan-status : true  
chd : true
```

PROVISION

Provision Device - Configuration preview

Nov 20, 2023 4:46 PM | Status: Success | Last updated: 9:10:31 AM [Refresh](#)

Configuration Preview

Device IP : 10.106.133.143 Show in tree view

DEVICES

SR-BGL18-9800LC-143.cisco.com

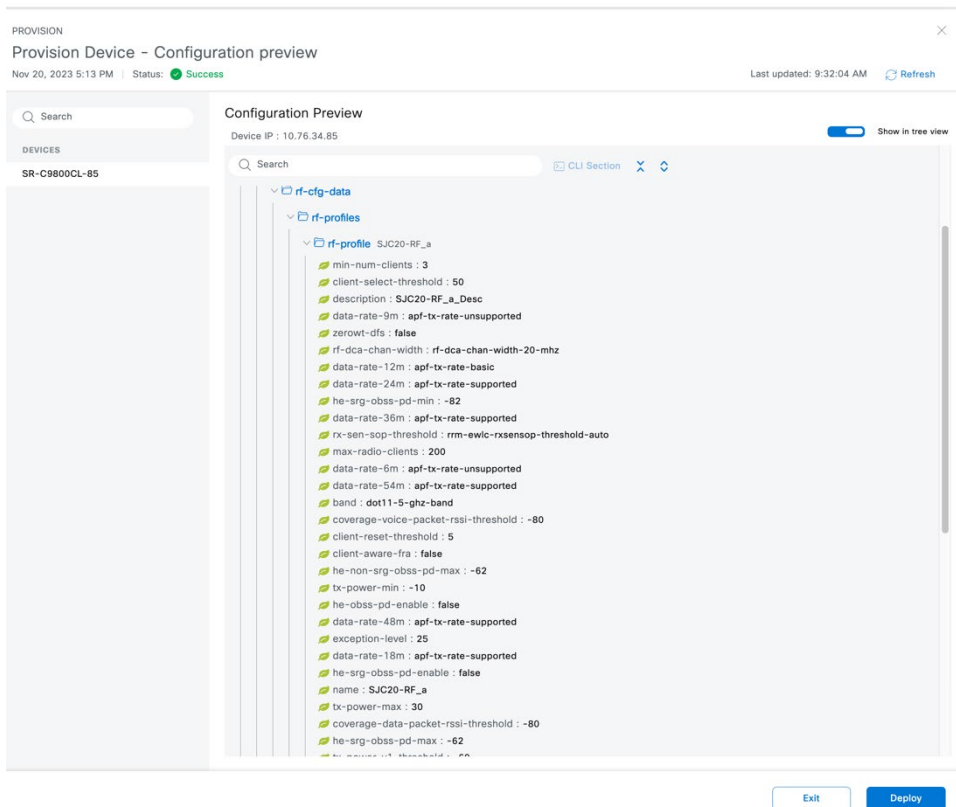
Search

CLI Section

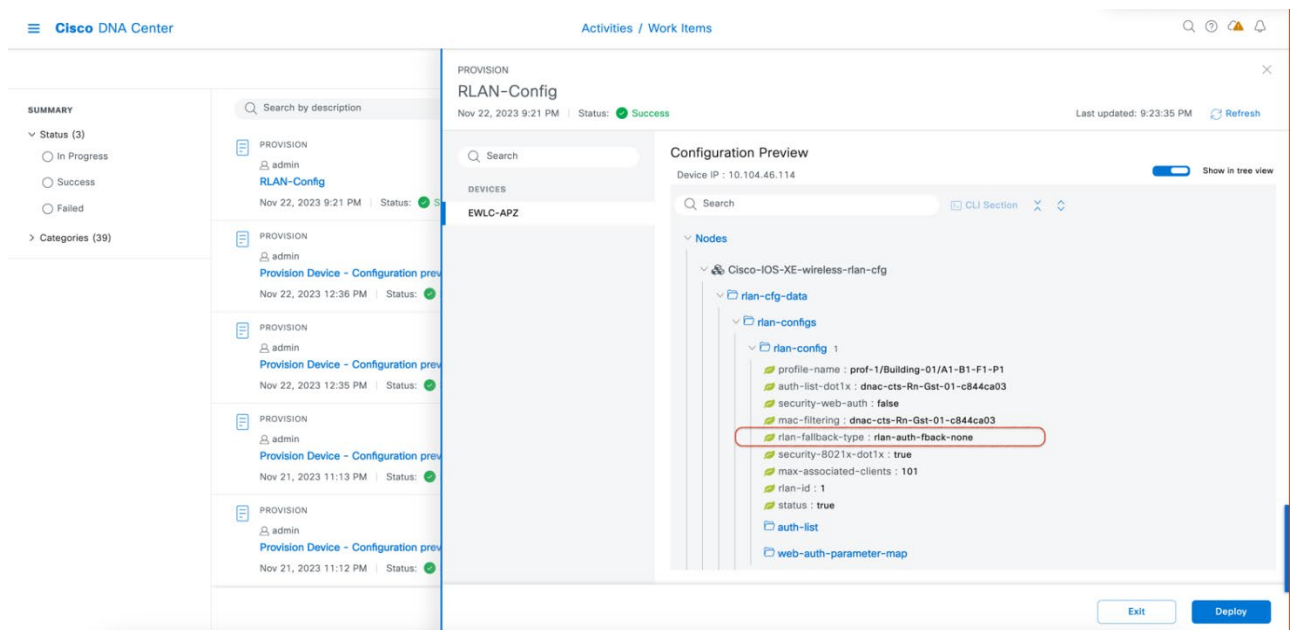
- > policy-list-entries
- Cisco-IOS-XE-wireless-site-cfg
 - site-cfg-data
 - ap-cfg-profiles
 - Cisco-IOS-XE-wireless-site-cfg
 - site-cfg-data
 - site-tag-configs
 - site-tag-config ST_BGL_BGL16_d1f4e_0
 - ap-join-profile : default-ap-profile
 - site-tag-name : ST_BGL_BGL16_d1f4e_0
 - arp-caching : true
 - description : Site Tag ST_BGL_BGL16_d1f4e_0
 - dhcp-bcast : false
 - is-local-site : true

Exit Deploy

RF Profile Configuration Preview Guidelines



RLAN Feature Config Preview Guidelines



Note: After you upgrade to Cisco DNA Center Release 2.3.5.4, if you directly launch the RLAN workflow before the wireless controller reprovisioning, the current out-of-band L2 fallback values from the Catalyst 9800 Series Wireless Controller will be automatically learned and displayed in the RLAN workflow as shown in the following figure.

Cisco DNA Center Configure WLAN

Remote LAN Configuration

If Access Point has only one RLAN port available, then port 2 and port 3 configurations will be ignored for that Access Point. The RLAN client VLANs configured on secondary WLC will be same as that configured on the primary WLC, when the site is managed by a secondary WLC.

Port 1
Port 2
Port 3

Enable RLAN

Connectivity Settings

Forwarding Mode: Local Switching VLAN*: 530
Only 31 characters are allowed.

Security Settings

Maximum End points*: 101 Timeout Period*: 1801
Only between 0-10000 Only between 0-86400 sec

Layer 2: Dot1x MAC Filtering

Layer 3: Open Select a AAA Server Group: 10.104.46.58

Fallback Authentication
 MAC Filtering on Dot1x failure

This OOB Fallback authentication value for the RLAN profile is automatically learned from the C9800 WLC by RLAN Workflow

[Exit](#)
[Review](#)
[Back](#)
[Next](#)

SSID and Guest Anchor Parameters List for Cisco AireOS Wireless Controllers

Compliance Table entry	Platform	Feature Name	Parameter Name	Default Value in Cisco DNA Center	Network Impact & Severity
Accounting List name	AireOS	SSID	Accounting Server		No Impact in Cisco AireOS Wireless Controller, Cisco DNA Center will not push any value for AAA accounting server. No compliance mismatch and no configuration push.
Coverage Hole Detection	AireOS	SSID	Coverage Hole Detection		No Impact in Cisco AireOS Wireless Controller, Cisco DNA Center will not push any value for CHD. No compliance mismatch and no configuration push.
Protected Management Frame	AireOS	SSID	Protected Management Frame (802.11w)	enabled	Compliance mismatch shows in Cisco DNA Center and Cisco DNA Center will push the intent configuration to the device.
Auth Key Mgmt/CCKM	AireOS	SSID	CCKM	disabled	No Impact in Cisco AireOS Wireless Controller, Cisco DNA Center will not push any value for CCKM. No compliance mismatch and no configuration push.
primary	AireOS	Anchor Group	Anchor WLC	None	No Impact for guest anchor enabled SSID, Cisco DNA Center will not remove any configuration from the device. Impact for non-guest anchor enabled SSID, Cisco DNA Center will remove the out-of-band guest anchor configured: High Impact : Client disconnection.

calendar-profile	AireOS	SSID Scheduler	calendar-profile	None	No Impact in Cisco AireOS Wireless Controller, Cisco DNA Center will not push any value for calendar profile. No compliance mismatch and no configuration push.
AP AAA Auth	AireOS	AAA auth	AP Authorization List	NA	Impact on AP auth on the device, AP auth list will get disabled. High Impact: AP will not join back
PSK	AireOS	PSK			

Cisco DNA Center 🔍 🔄 ⚠️

User Defined Fields

- Config Drift
- Wireless Info
- Mobility
- SECURITY**
- Advisories
- COMPLIANCE
- Summary

Compliance Summary / Network Profiles View Preference for Acknowledged Violations

CLI Template (1) Wireless (2)

CLI Deviations As of: Nov 23, 2023 9:41 AM 🔄

🔍 Search Table

Open Violations (1) Acknowledged Violations (0)

Template	Action
CLI-template	Acknowledge

1 Records Show Records: 10 ▾

1 - 1 < 1 >

Realize Template: CLI-template 🔄

```

1 config radius auth disable 1
2 config radius auth add 1 9.60.16.174 1812 ascii Tel12345
3 config radius auth management 1 disable
4 config radius auth disable 1
5 config radius auth retransmit-timeout 1 4
6 config radius auth rfc3576 enable 1
7 config radius auth enable 1
8 config radius acct disable 1
9 config radius acct add 1 9.60.16.174 1813# ascii Tel12345
10 config radius acct disable 1
11 config radius acct retransmit-timeout 1 4
12 config radius acct enable 1
13 config wlan radius_server auth add 19 1
14 config wlan security web-auth server-precedence 19 radius
15 config wlan radius_server acct add 19 1
16
17
18
19 config wlan chd 19 enable
20 config wlan security wpa akm cckm enable 19
21 config wlan security pmf required 19
22 config wlan aaa-override enable 19
23
24 config policy test0 create
25 config policy test0 wlan-schedule add enable hours 04:20 04:
22 days tue

```

You can now fix all configuration compliance issues on this device. You will be able to review before the fix is applied. [Fix All Configuration Compliance Issues](#)

Compliance Summary / Network Profiles View Preference for Acknowledged Violations

CLI Template (1) **Wireless (2)**

🔍 Search Table

Open Violations (2) Acknowledged Violations (0)

0 Selected Acknowledged

<input type="checkbox"/>	Model Name ▲	Attribute	Status 📄	Intended Value 📄	Actual Value 📄	Action
<input type="checkbox"/>	Ap Auth Policy	authorizeAp	Changed	0	1	Acknowledge
<input type="checkbox"/>	Wlan/ENT-SSID-0_Global_NF_91533b44	Protected Management Frame	Changed	Disabled	Required	Acknowledge

Showing 2 of 2

You can now fix all configuration compliance issues on this device. You will be able to review before the fix is applied. [Fix All Configuration Compliance Issues](#)

[Compliance Summary](#) / Network Profiles

[View Preference for Acknowledged Violations](#)

CLI Template (1) **Wireless (2)**

Search Table ⌵

Open Violations (2) Acknowledged Violations (0)

0 Selected [Acknowledge](#)

<input type="checkbox"/>	Model Name ▲	Attribute	Status ⓘ	Intended Value ⓘ	Actual Value ⓘ	Action
<input type="checkbox"/>	Ap Auth Policy	authorizeAp	Changed	0	1	Acknowledge
<input type="checkbox"/>	Wlan/ENT-SSID-0_Global_NF_91533b44	Protected Management Frame	Changed	Disabled	Required	Acknowledge

Showing 2 of 2

```
config auth-list ap-policy authorize-ap disable. → compliance shows this
#INTERACTIVE
config wlan disable 20<SF><IQ>(y/n)<R>y
#ENDS_INTERACTIVE
config wlan security wpa akm psk set-key ascii ***** 20 → Why we set PSK again after upgrade
config wlan security pmf disable 20 → compliance shows this
#INTERACTIVE
config wlan enable 20<SF><IQ>(y/n)<R>y
#ENDS_INTERACTIVE
#INTERACTIVE
config wlan disable 20<SF><IQ>(y/n)<R>y
#ENDS_INTERACTIVE
config wlan mobility anchor delete 20 9.60.8.60. → Not displayed in compliance
config wlan mobility anchor delete 20 9.60.1.114
config wlan mobility anchor delete 20 9.60.1.47
config wlan mobility anchor delete 20 9.60.1.92
#INTERACTIVE
config wlan enable 20<SF><IQ>(y/n)<R>y
#ENDS_INTERACTIVE
config flow create exporter 10.104.46.39 10.104.46.39 port 6007
```

Provision Device - Configuration preview

Nov 23, 2023 9:43 AM | Status: ✔ Success

Last updated: 9:44:21 AM [Refresh](#)

Search

DEVICES

WLC-5520-06

Configuration Preview

Device IP : 10.76.41.66

```
1 config auth-list ap-policy authorize-ap disable
2 #INTERACTIVE
3 config wlan disable 20<SF><IQ>(y/n)<R>y
4 #ENDS_INTERACTIVE
5 config wlan security wpa akm psk set-key ascii ***** 20
6 config wlan security pmf disable 20
7 #INTERACTIVE
8 config wlan enable 20<SF><IQ>(y/n)<R>y
9 #ENDS_INTERACTIVE
10 #INTERACTIVE
11 config wlan disable 20<SF><IQ>(y/n)<R>y
12 #ENDS_INTERACTIVE
13 config wlan mobility anchor delete 20 9.60.8.60
14 config wlan mobility anchor delete 20 9.60.1.114
15 config wlan mobility anchor delete 20 9.60.1.47
16 config wlan mobility anchor delete 20 9.60.1.92
17 #INTERACTIVE
18 config wlan enable 20<SF><IQ>(y/n)<R>y
19 #ENDS_INTERACTIVE
20 config flow create exporter 10.104.46.39 10.104.46.39 port 6007
```

Exit

Deploy

RF Profile: New Parameters for Cisco AireOS Wireless Controllers

Profile	Parameter Name per the Compliance Report	Parameter Name per the Cisco DNA Center Design Windows	Band	Cisco DNA Center Defaults	Impact Severity	Impact Details
RF Profile	CHD Voice RSSI Threshold	Voice RSSI Threshold (dBm)	5GHz/2.4GHz	-80	LOW	No Impact
RF Profile	CHD Data RSSI Threshold	Data RSSI Threshold (dBm)	5GHz/2.4GHz	-80	LOW	No Impact
RF Profile	CHD Min Client Level	Minimum Client Level (clients)	5GHz/2.4GHz	3	LOW	No Impact
RF Profile	CHD Exception Level (%)	Exception Level (%)	5GHz/2.4GHz	0.25	LOW	No Impact
RF Profile	Client Aware	Client Aware	5GHz	Disabled	LOW	No Impact
RF Profile	Client Reset (%)	Client Reset (%)	5GHz	50	LOW	No Impact
RF Profile	Client Select (%)	Client Select (%)	5GHz	5	LOW	No Impact

Compliance mismatches reported in the compliance report as follows:

The screenshot shows the Cisco DNA Center interface with a compliance report for 11 wireless profiles. The table below summarizes the violations shown in the screenshot:

Model Name	Attribute	Status	Intended Value	Actual Value	Action
RF Profile/SJC14-RF_a	Client Select (%)	Changed	50	51	Acknowledge
RF Profile/SJC14-RF_a	CHD Voice RSSI Threshold	Changed	-80	-81	Acknowledge
RF Profile/SJC14-RF_a	Client Reset (%)	Changed	5	6	Acknowledge
RF Profile/SJC14-RF_a	CHD Exception Level (%)	Changed	25	26	Acknowledge
RF Profile/SJC14-RF_a	CHD Min Client Level	Changed	3	4	Acknowledge
RF Profile/SJC14-RF_a	Client Aware	Changed	Disable	Enable	Enable
RF Profile/SJC14-RF_a	CHD Data RSSI Threshold	Changed	-80	-81	Acknowledge
RF Profile/SJC14-RF_b	CHD Data RSSI Threshold	Changed	-80	-82	Acknowledge
RF Profile/SJC14-RF_b	CHD Min Client Level	Changed	3	5	Acknowledge
RF Profile/SJC14-RF_b	CHD Voice RSSI Threshold	Changed	-80	-82	Acknowledge
RF Profile/SJC14-RF_b	CHD Exception Level (%)	Changed	25	27	Acknowledge

Remediate the compliance mismatches either by reprovisioning the wireless controller or using “Fix All Configuration Compliance Issues” and generate the configuration preview as follows:

The screenshot shows the 'Provision Device - Configuration preview' window. It displays the configuration commands for the device BGL20-WLC3504-39. The configuration includes setting RF profiles for two different bands (a and b) with various parameters like coverage data, exception levels, client-aware settings, and client reset percentages. The configuration is shown as a list of commands:

```

1 config rf-profile coverage data -80 SJC14-RF_a
2 config rf-profile coverage exception 25 SJC14-RF_a
3 config rf-profile coverage level 3 SJC14-RF_a
4 config rf-profile coverage voice -80 SJC14-RF_a
5 config rf-profile fra client-aware disable SJC14-RF_a
6 config rf-profile fra client-aware client-select 50 SJC14-RF_a
7 config rf-profile fra client-aware client-reset 5 SJC14-RF_a
8 config rf-profile coverage data -80 SJC14-RF_b
9 config rf-profile coverage exception 25 SJC14-RF_b
10 config rf-profile coverage level 3 SJC14-RF_b
11 config rf-profile coverage voice -80 SJC14-RF_b
12 config flow create exporter 10.76.34.22 10.76.34.22 port 6007
    
```

AP Profile: New Parameters for Cisco AireOS Wireless Controller

Feature Name	Parameter Name per the Compliance Report	Cisco DNA Center Parameter Name in Design Windows	Cisco DNA Center Defaults	Impact Severity	Impact Details
AP Config	Rogue Detection	Rogue Detection	Enabled	Medium	Rogue detection can get disabled inadvertently
AP Config	CDP State	CDP State	Enabled	LOW	CDP neighbor discovery does not work
AP Config	SSH	SSH	Disabled	Medium	SSH can get disabled and affect the troubleshooting operations

Compliance mismatches for AP profile on Cisco AireOS Wireless Controller:

The screenshot displays the Cisco DNA Center interface for a device named BGL20-WLC3504-39. The 'Compliance' section is active, showing a table of mismatches for the 'Wireless' profile. The table lists three items that have been changed from their intended values:

Model Name	Attribute	Status	Intended Value	Actual Value	Action
AP Config/70:70:8b:85:e5:70	Rogue Detection	Changed	Enable	Disable	Acknowledge
AP Config/70:70:8b:85:e5:70	CDP State	Changed	Enable	Disable	Acknowledge
AP Config/70:70:8b:85:e5:70	SSH	Changed	Disable	Enable	Acknowledge

Configuration preview for remediating the compliance mismatches on Cisco AireOS Wireless Controllers:

The screenshot shows the 'Configuration Preview' window in Cisco DNA Center. The configuration is for device BGL20-WLC3504-39 and includes the following commands:

```

1 config ap location 'A VERY LONG LOCATION NAME ON APs ASSOCIATED TO AIREOS WLCs' SJC21-1815M-EC10
2 config ap ssh disable SJC21-1815M-EC10
3 config ap telnet disable SJC21-1815M-EC10
4 config ap cdp enable SJC21-1815M-EC10
5 config rogue detection enable SJC21-1815M-EC10
6 #INTERACTIVE
7 config ap group-name Floor-2_SJC14-RF_a8e88 SJC21-1815M-EC10 <SF><IQ>(y/n)<R>y
8 #ENDS_INTERACTIVE
9 config flow create exporter 10.76.34.22 10.76.34.22 port 6007
    
```

At the bottom of the window, there are 'Exit' and 'Deploy' buttons.