Wireless Automation MoP for Cisco DNA Center, Release 2.3.5.5

Contents

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.

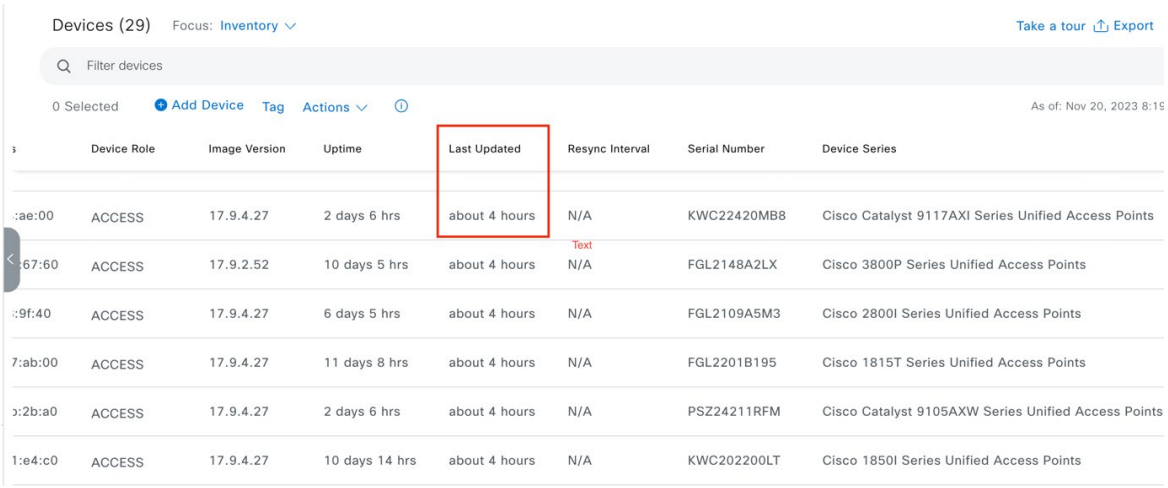
This document assesses the provisioning impact of new features and new parameters added to the existing features introduced **exclusively between Release 2.3.3.x and 2.3.5.5**.

MoP Summary

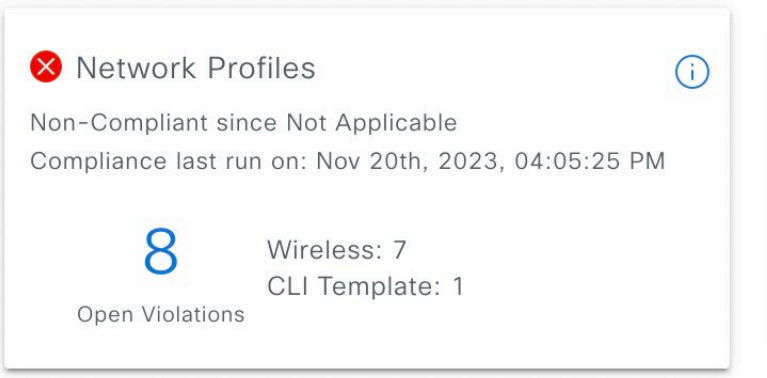
1. Upgrade to Cisco DNA Center Release 2.3.5.5.
2. After the upgrade, manually run compliance for all Cisco Wireless Controllers per the guidelines listed in Detailed Guidelines and review the compliance report.
3. To evaluate the impact of any violations reported in the compliance report, see Detailed 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 preprovision 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

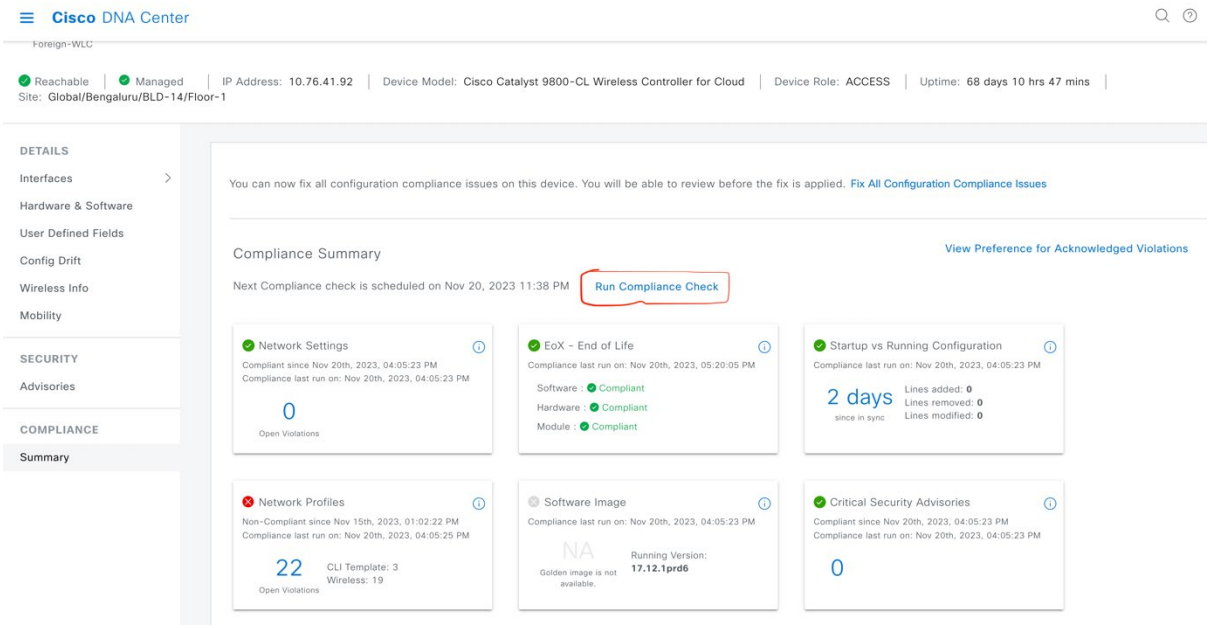
1. **After upgrade:** Check the last inventory synchronization status and last update time interval for all wireless controllers in the **Inventory** window as shown in the following figure.



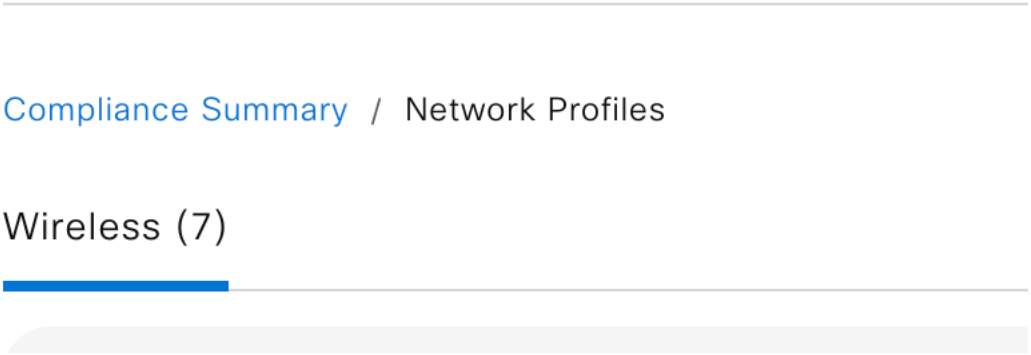
2. If the inventory synchronization hasn't finished after the upgrade, either wait for its completion or initiate a manual resynchronization.
3. Review the compliance status of all wireless controllers on the **Inventory** window.



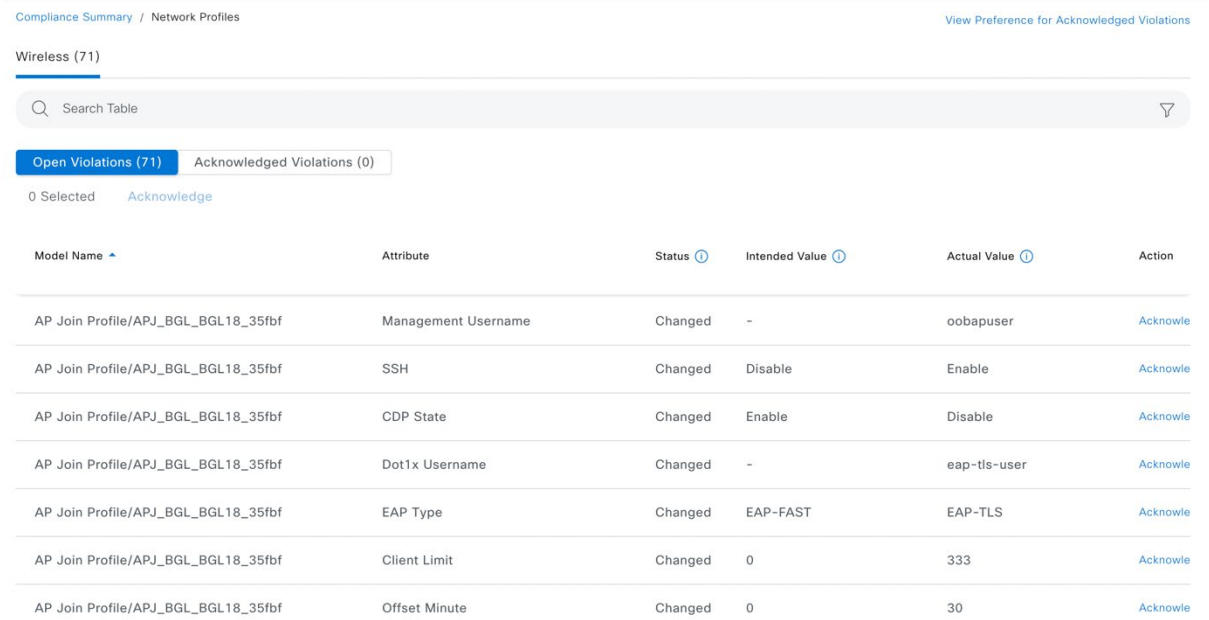
4. If the last compliance run didn’t occur after the most recent inventory resynchronization, initiate a compliance check, and review the report.



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



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



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 preprovision 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

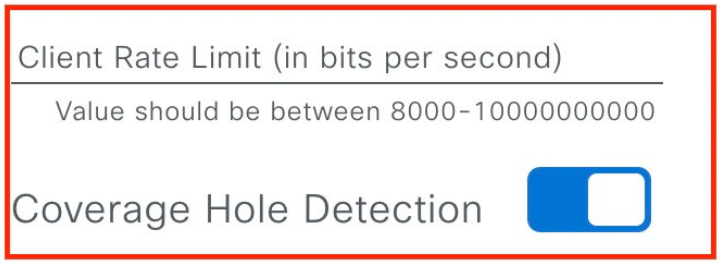
Compliance Table Entry	Platform	Feature Name	Parameter Name	Default Value in Cisco DNA Center	Impact Severity	Impact Details
Fallback Authentication	9800	RLAN	MAC Filtering on Dot1x failure Dot1x on MAC Filtering failure	None	High	RLAN wired clients can't achieve the fallback mechanism for L2 authentication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

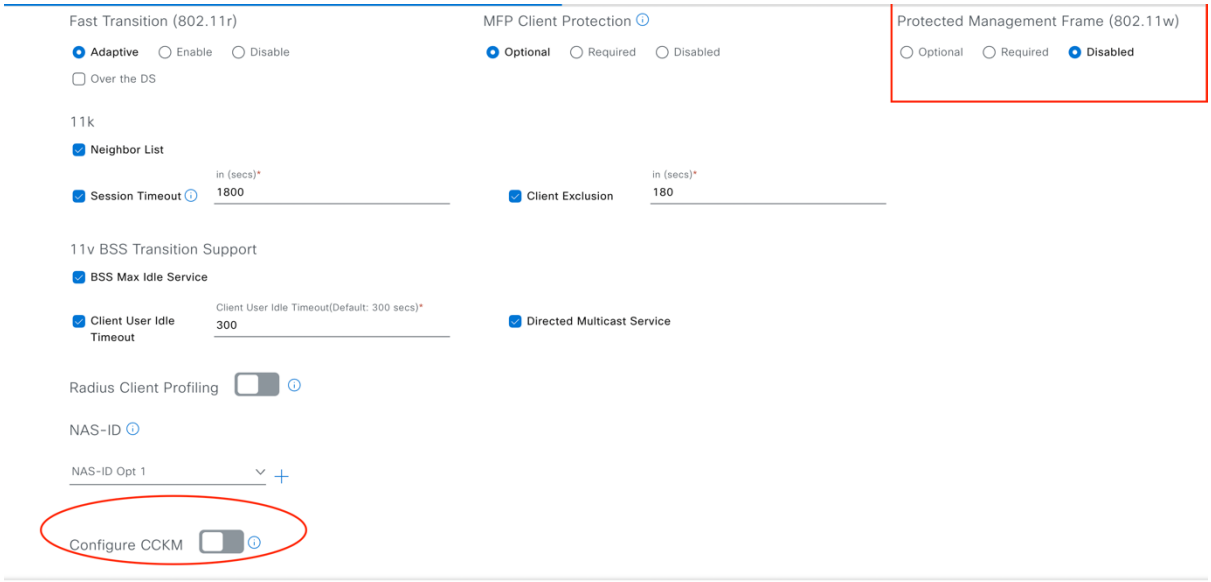
Guidelines to Adjust New Features and Parameters Defaults

SSID: New Parameters

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

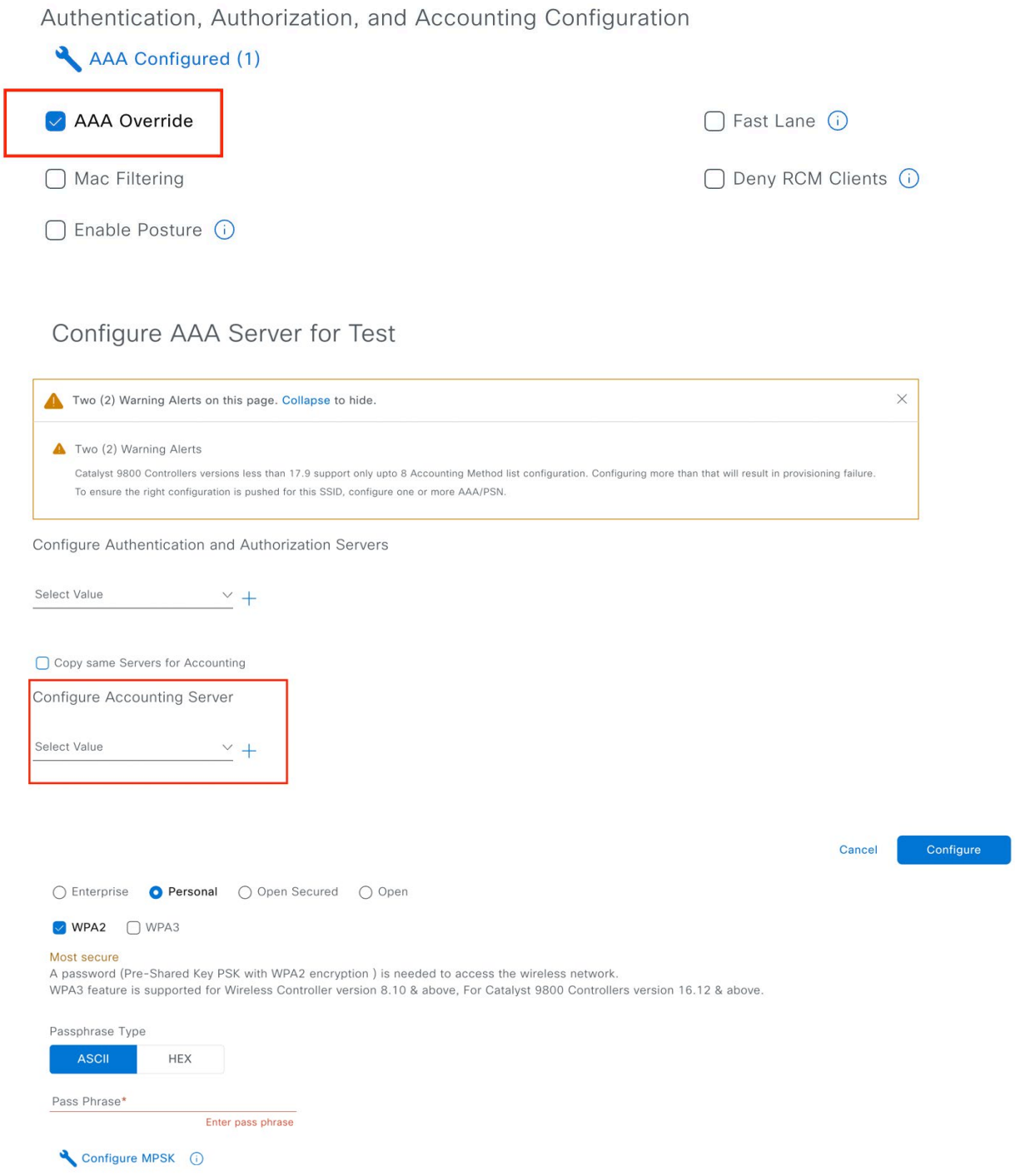
Parameter Names: Client Rate Limit, Coverage Hole Detection (CHD), Protected Management Frame (802.11w), Configure CCKM

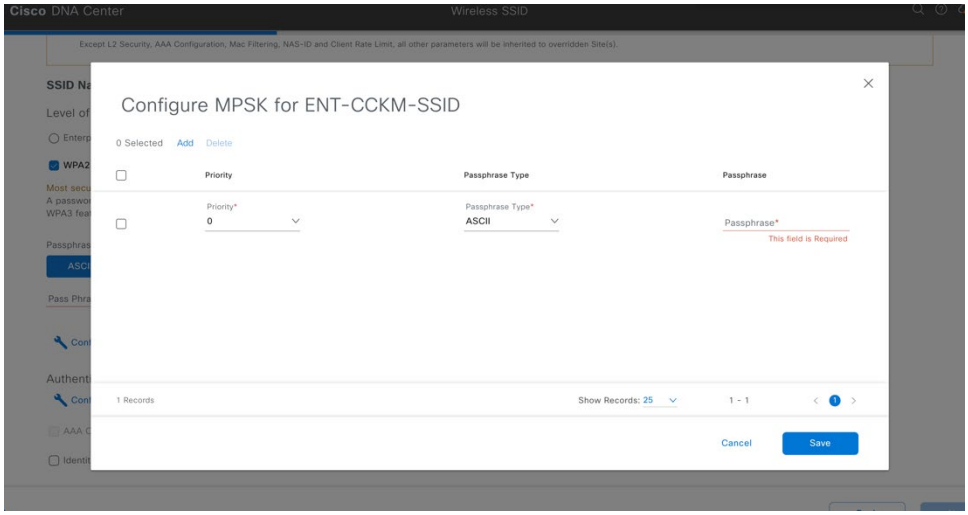




Path: **Design > Network Settings > Wireless > SSID > Security Settings**

Parameter Names: AAA Override, Accounting Servers, MPSK

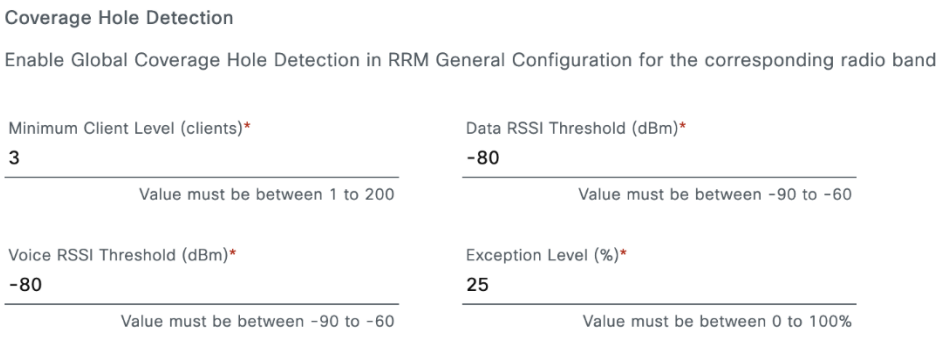




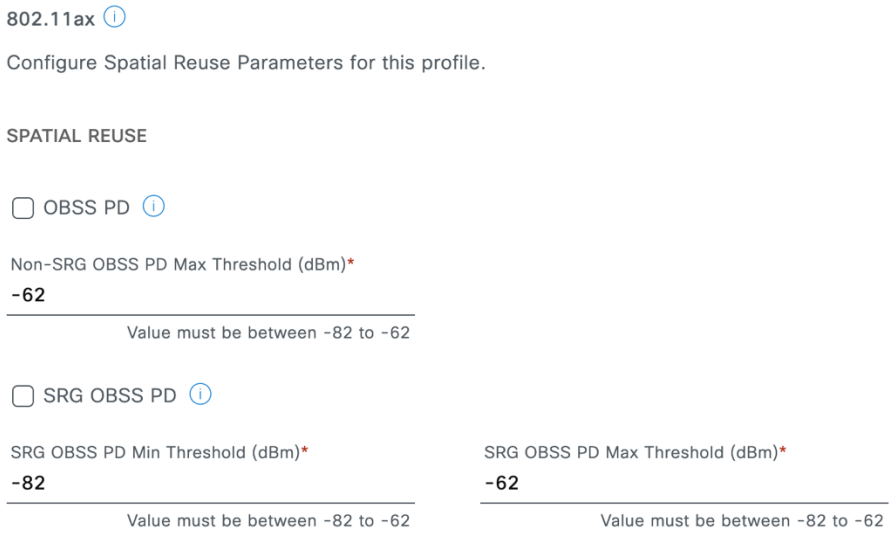
RF Profile: New Parameters

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

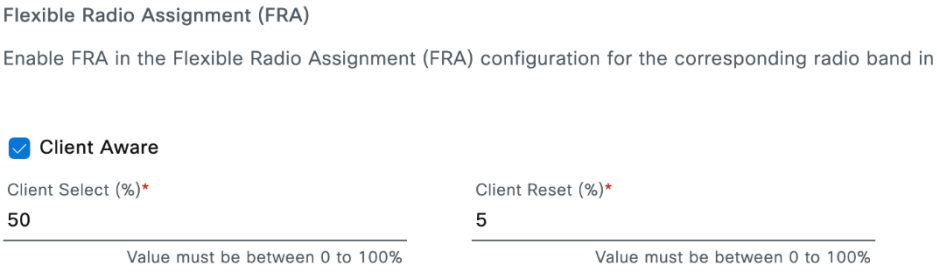
Coverage Hole Detection (applicable for the 2.4-GHz, 5-GHz and 6-GHz RF bands)



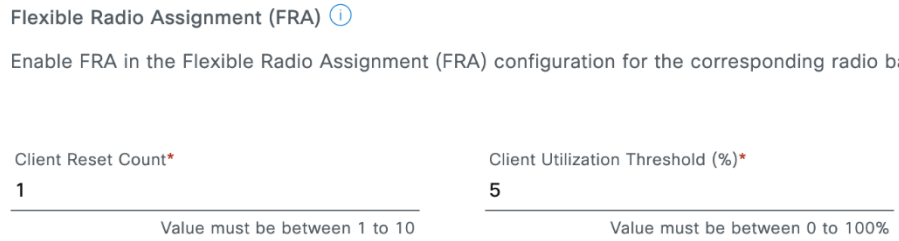
802.11ax Spatial Reuse Parameters (applicable for the 2.4-GHz, 5-GHz and 6-GHz RF bands)



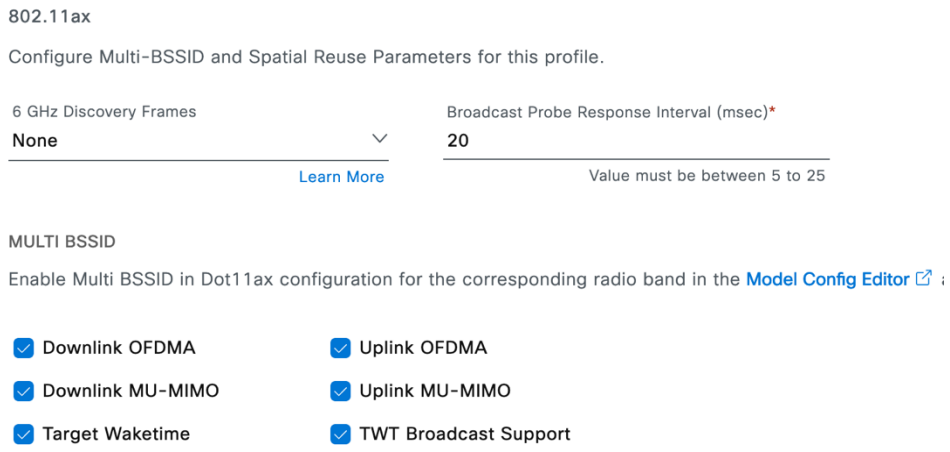
Client Aware FRA (Applicable for the 5-GHz RF band)



6-GHz FRA Parameters

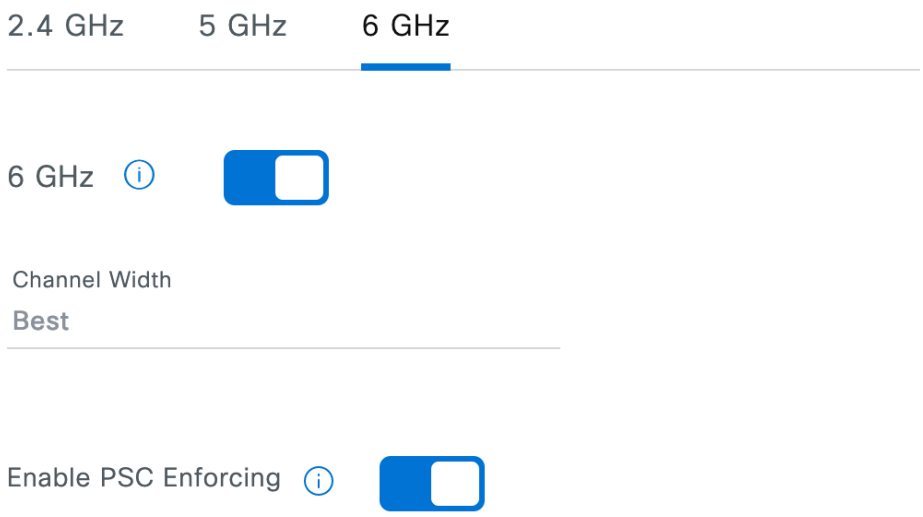


6-GHz 802.11ax Parameters including Multi BSSID Profile



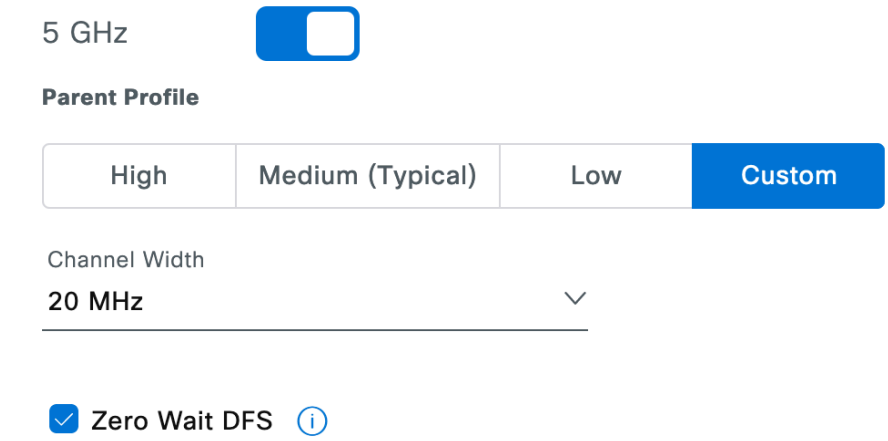
Path: **Design-> Network Settings-> Wireless -> Wireless Radio Frequency Profile**

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



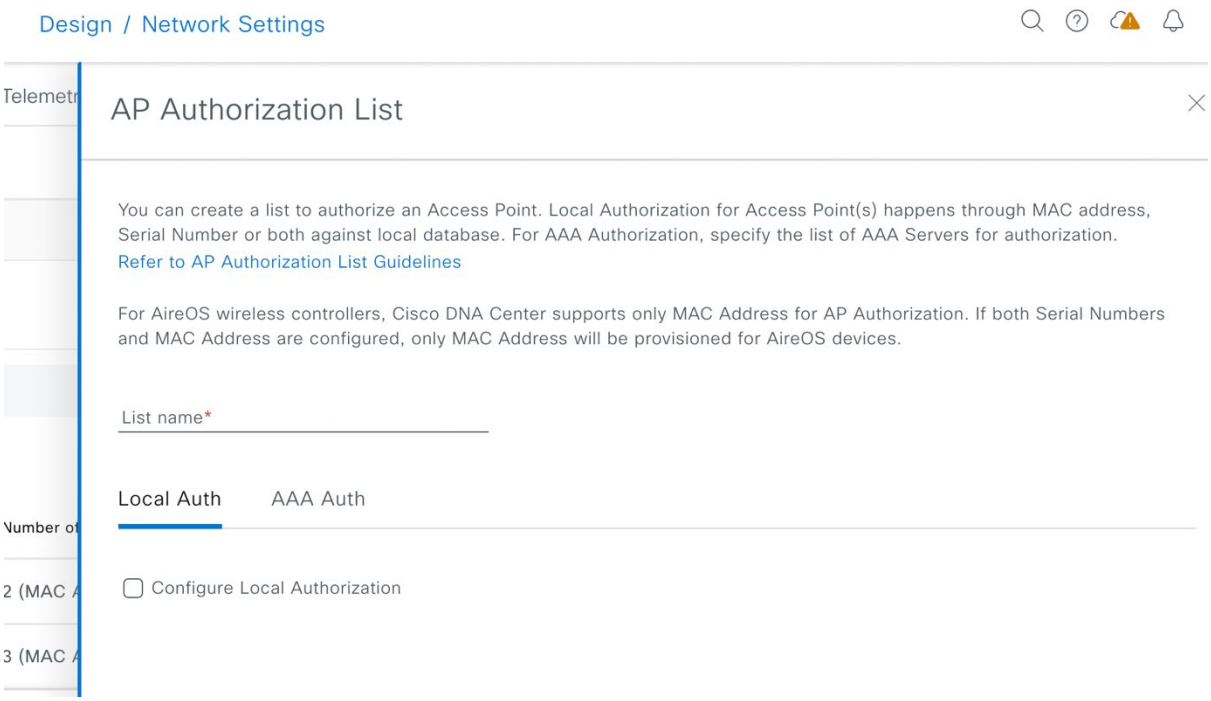
Path: **Design > Network Settings > Wireless > Wireless Radio Frequency Profile**

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



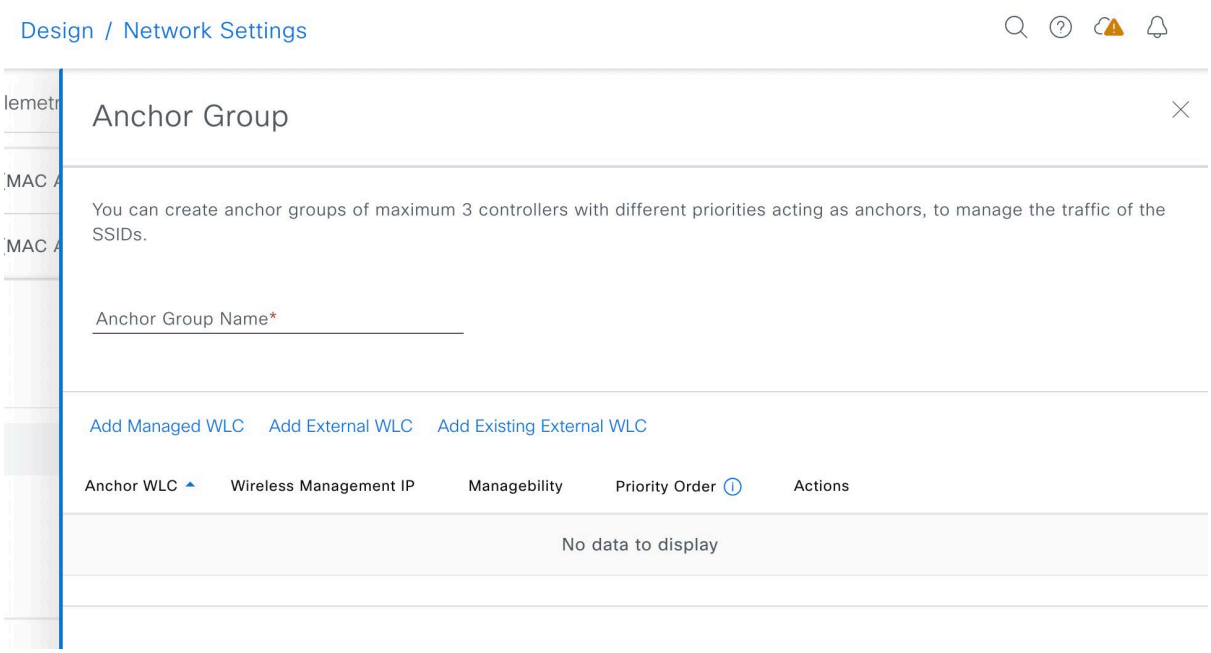
New Feature: AP Authorization List

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



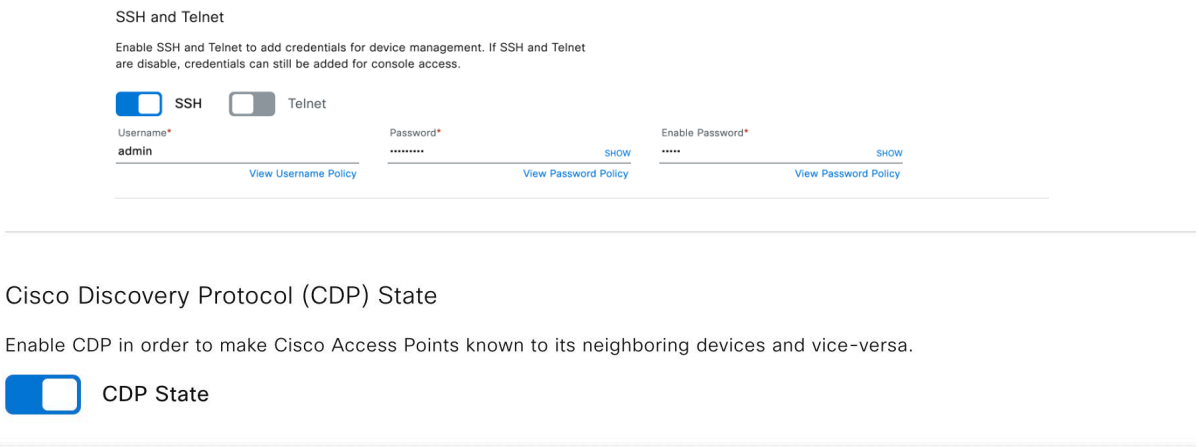
New Feature: Anchor Group (Multiple Anchor Support)

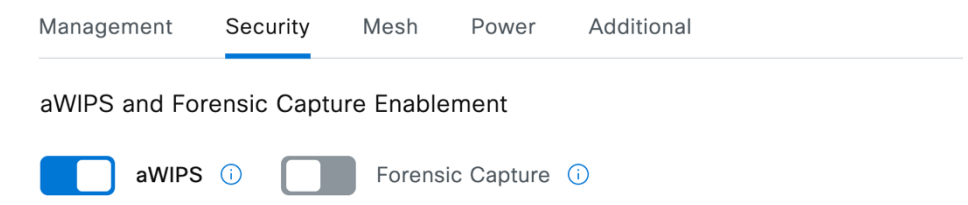
Path: **Design > Network Settings > Wireless > Anchor Group**

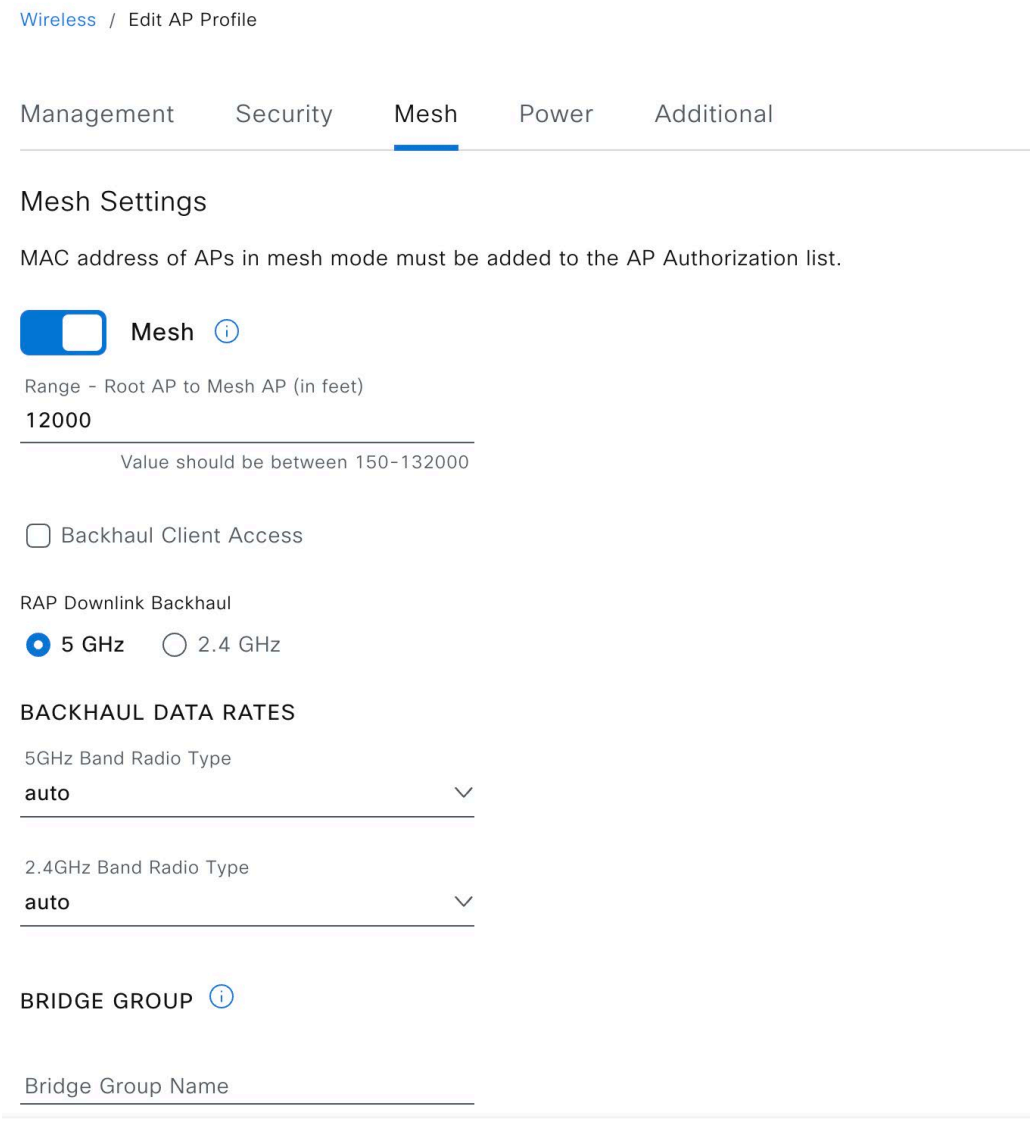


New Feature: AP Profile

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




Management
Security
Mesh
Power
Additional
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
Management
Security
Mesh
Power
Additional
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

Management Security Mesh Power Additional

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 shoud 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

Management Security Mesh Power Additional

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

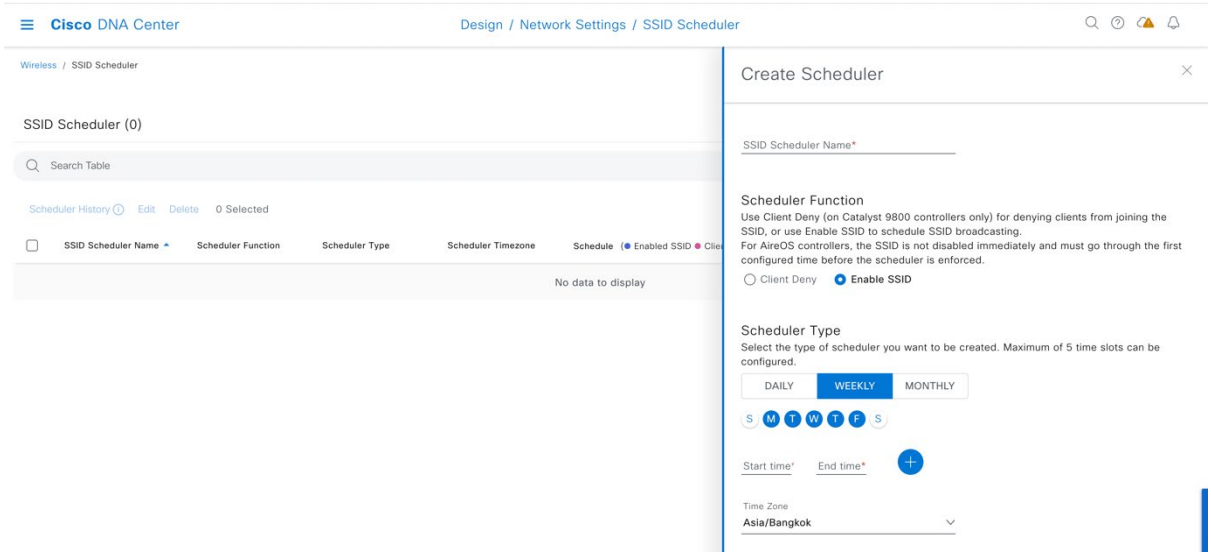
Client Limit

Maximum Client Limit

0

Value should be between 0-1200

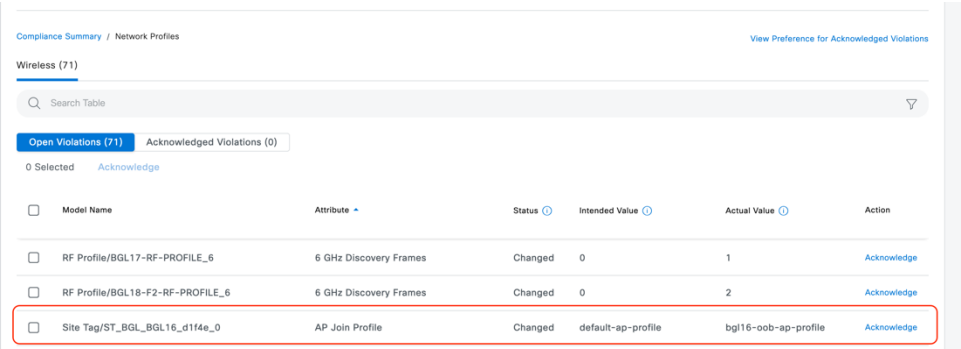
New Feature: SSID Scheduler



Compliance Report Review Guidelines (Feature-Based)

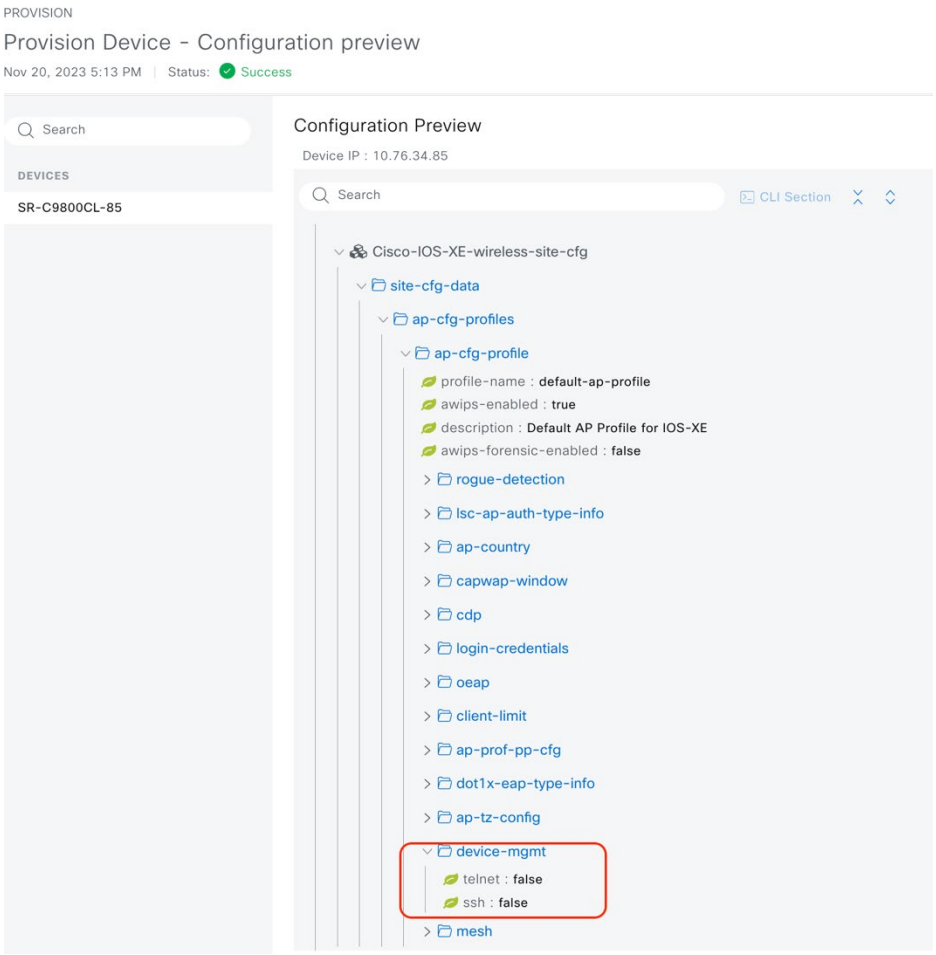
AP Profile Compliance Guidelines

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.

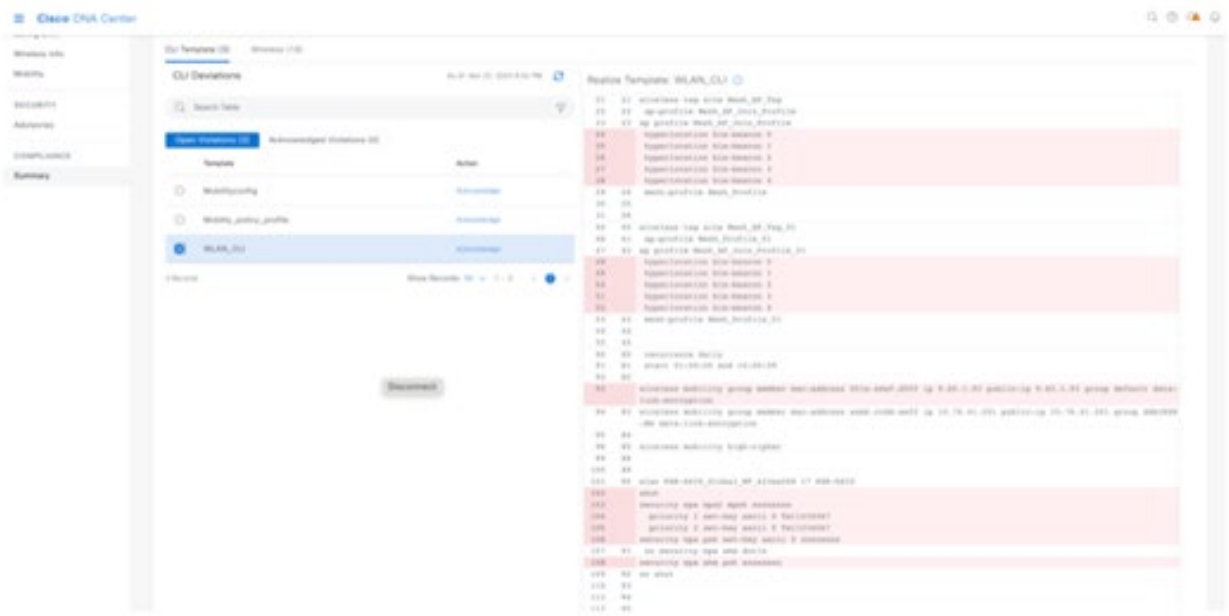


If this configuration isn't intended, create the AP profile from **Design > Network Settings > Wireless > AP Profiles** and create the AP profile with the same name as the one which was created out-of-band earlier, while running Cisco DNA Center Release 2.3.3.7. Map this AP profile to either the Cisco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



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.



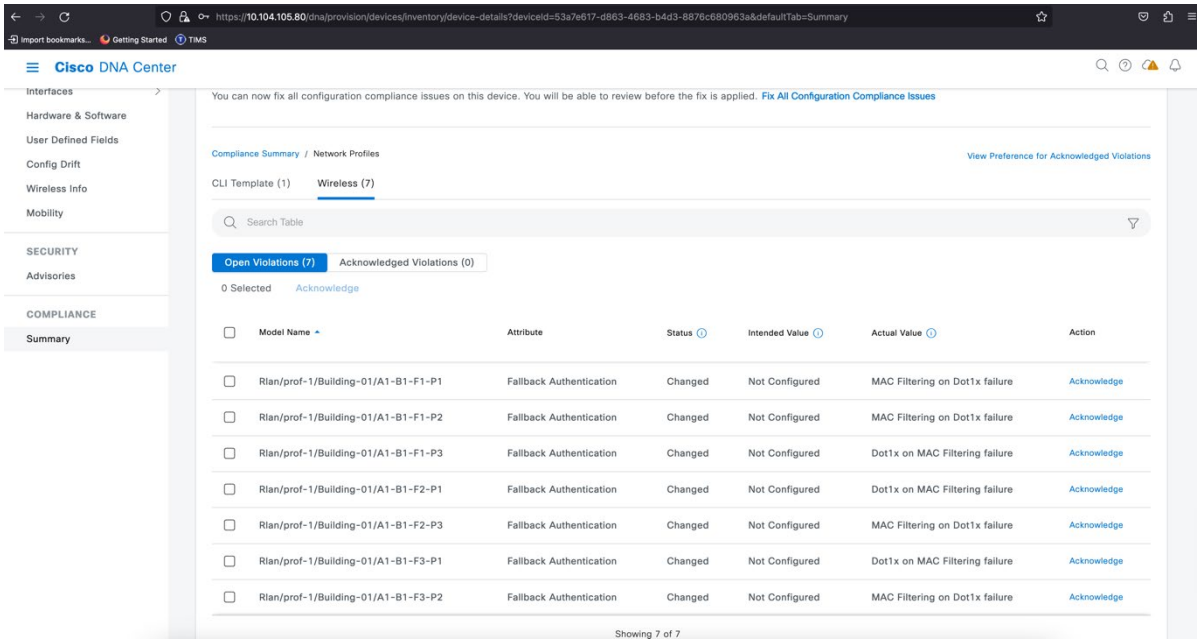
RF Profile Compliance Guidelines

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.

RF Profile/BGL18-F2-RF-PROFILE_b	SRG OBSS PD Min Threshold	Changed	-82	-80	Acknowledge
RF Profile/BGL18-F2-RF-PROFILE_a	CHD Data RSSI Threshold	Changed	-80	-82	Acknowledge
RF Profile/BGL18-F2-RF-PROFILE_a	CHD Exception Level (%)	Changed	25	27	Acknowledge
RF Profile/BGL18-F2-RF-PROFILE_a	CHD Min Client Level	Changed	3	5	Acknowledge
RF Profile/BGL18-F2-RF-PROFILE_a	CHD Voice RSSI Threshold	Changed	-80	-82	Acknowledge
RF Profile/BGL18-F2-RF-PROFILE_a	Client Aware	Changed	Disable	Enable	Acknowledge
RF Profile/BGL18-F2-RF-PROFILE_a	Client Reset (%)	Changed	5	7	Acknowledge
RF Profile/BGL18-F2-RF-PROFILE_a	Client Select (%)	Changed	50	52	Acknowledge
RF Profile/BGL18-F2-RF-PROFILE_a	Non-SRG OBSS PD Max Threshold	Changed	-62	-72	Acknowledge
RF Profile/BGL18-F2-RF-PROFILE_a	OBSS PD	Changed	Disable	Enable	Acknowledge
RF Profile/BGL18-F2-RF-PROFILE_a	SRG OBSS PD	Changed	Disable	Enable	Acknowledge
RF Profile/BGL18-F2-RF-PROFILE_a	SRG OBSS PD Max Threshold	Changed	-62	-65	Acknowledge
RF Profile/BGL18-F2-RF-PROFILE_a	SRG OBSS PD Min Threshold	Changed	-82	-75	Acknowledge
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:

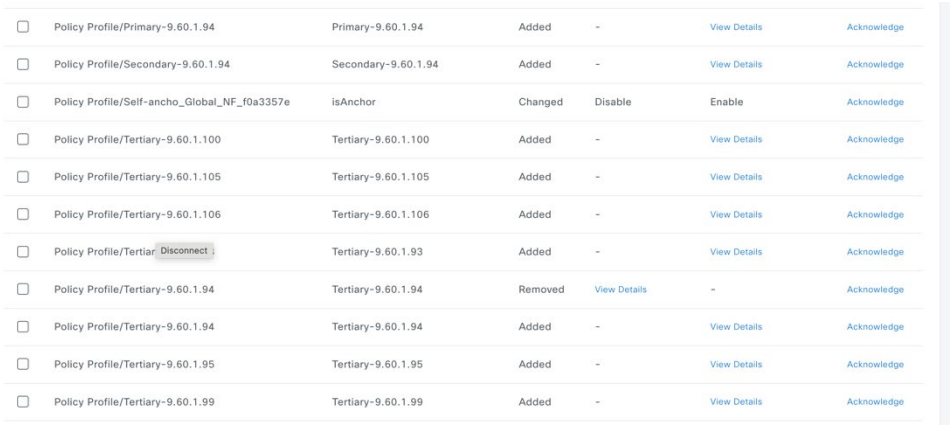


Configuration Preview Guidelines (Feature-Based)

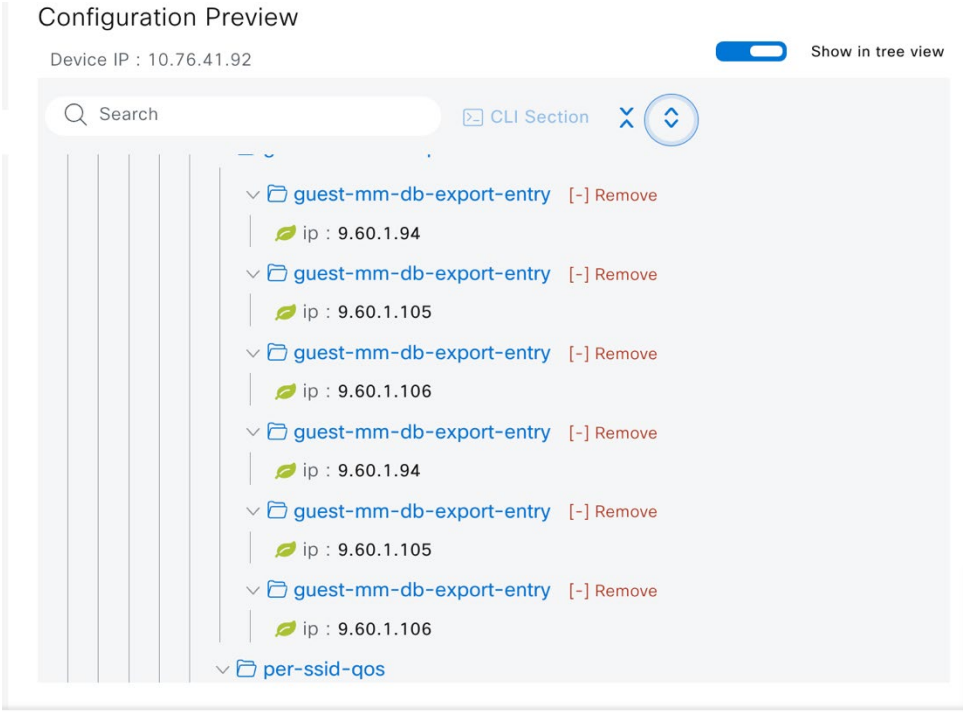
SSID and Mobility Anchor Config Preview Guidelines

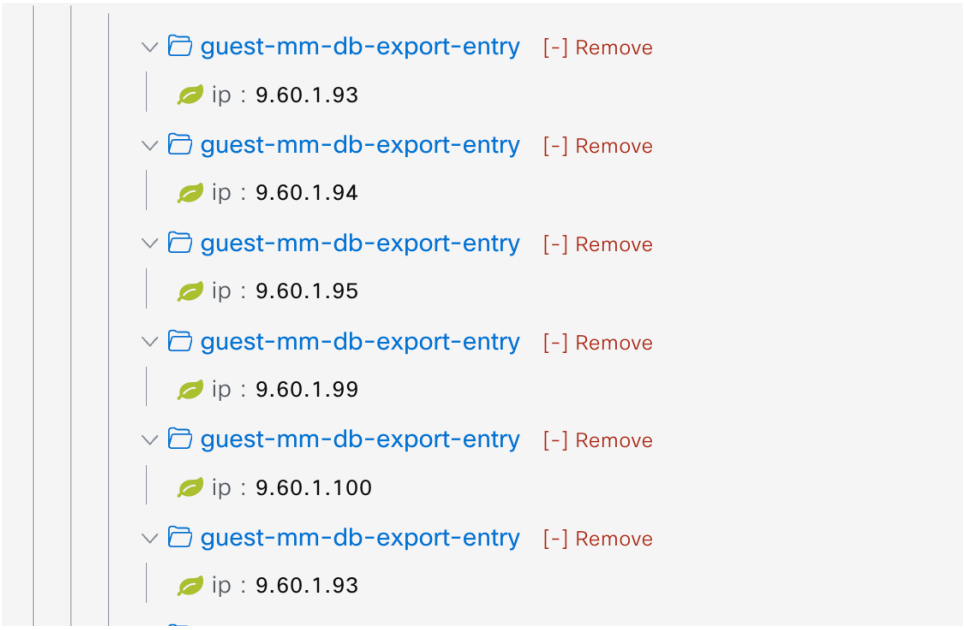
Configuration preview displaying delete and removal of attribute

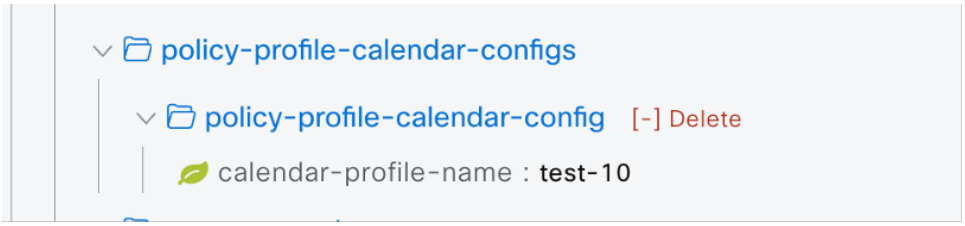
Configuration preview and relevant compliance mismatches

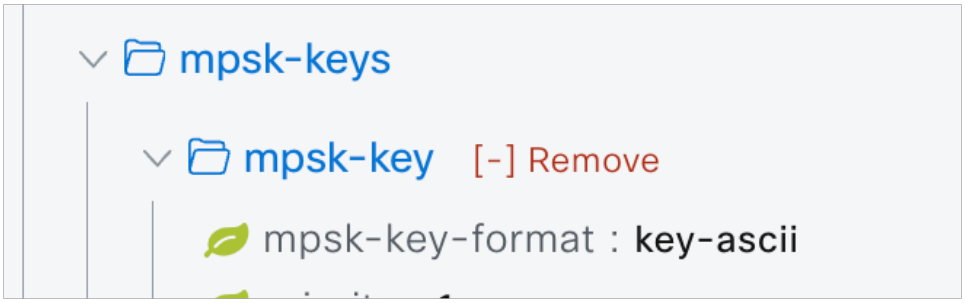


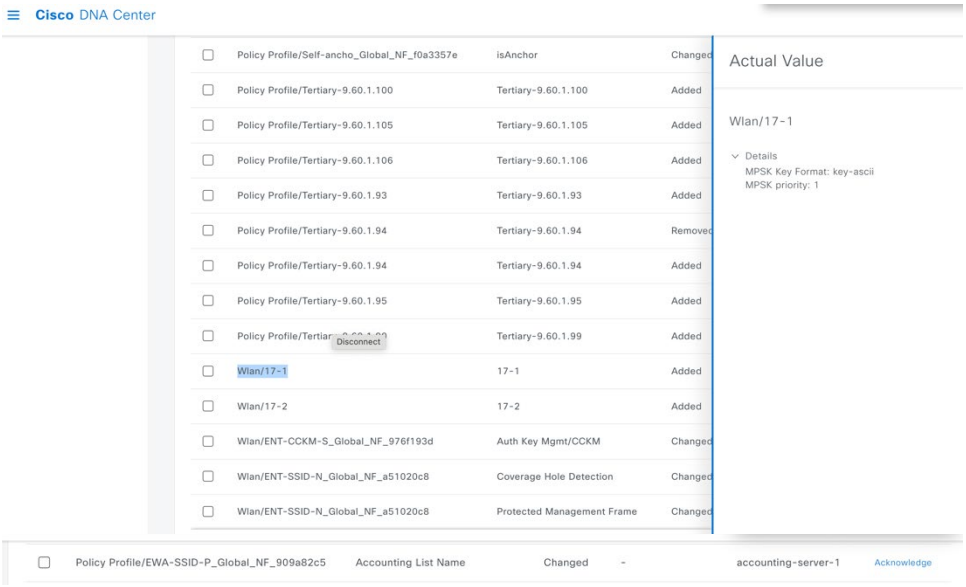
Policy Profile/Primary-9.60.1.94	Primary-9.60.1.94	Added	-	View Details	Acknowledge
Policy Profile/Secondary-9.60.1.94	Secondary-9.60.1.94	Added	-	View Details	Acknowledge
Policy Profile/Self-ancho_Global_NF_f0a3357e	isAnchor	Changed	Disable	Enable	Acknowledge
Policy Profile/Tertiary-9.60.1.100	Tertiary-9.60.1.100	Added	-	View Details	Acknowledge
Policy Profile/Tertiary-9.60.1.105	Tertiary-9.60.1.105	Added	-	View Details	Acknowledge
Policy Profile/Tertiary-9.60.1.106	Tertiary-9.60.1.106	Added	-	View Details	Acknowledge
Policy Profile/Tertiar Disconnect	Tertiary-9.60.1.93	Added	-	View Details	Acknowledge
Policy Profile/Tertiary-9.60.1.94	Tertiary-9.60.1.94	Removed	View Details	-	Acknowledge
Policy Profile/Tertiary-9.60.1.94	Tertiary-9.60.1.94	Added	-	View Details	Acknowledge
Policy Profile/Tertiary-9.60.1.95	Tertiary-9.60.1.95	Added	-	View Details	Acknowledge
Policy Profile/Tertiary-9.60.1.99	Tertiary-9.60.1.99	Added	-	View Details	Acknowledge

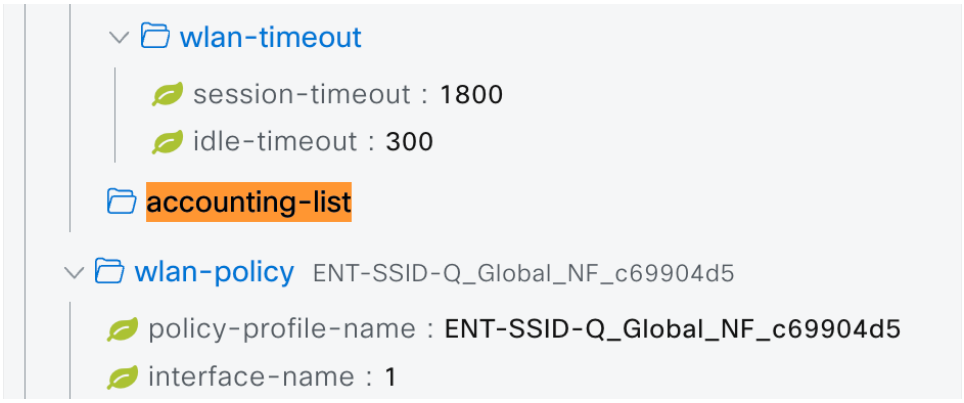




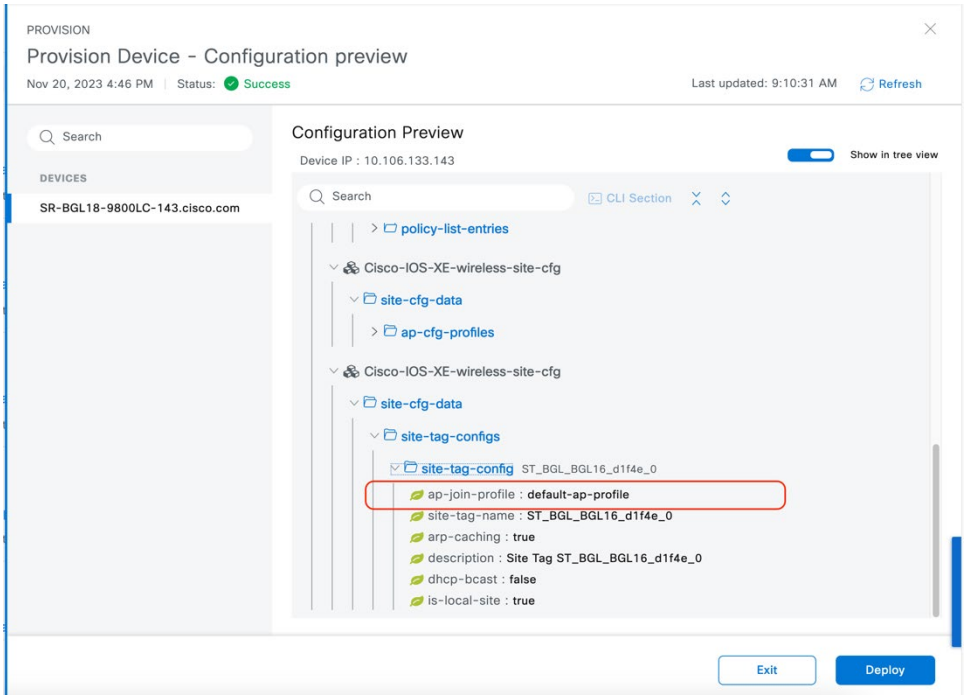

policy-profile-calendar-configs
policy-profile-calendar-config [-] Delete
calendar-profile-name : test-10


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

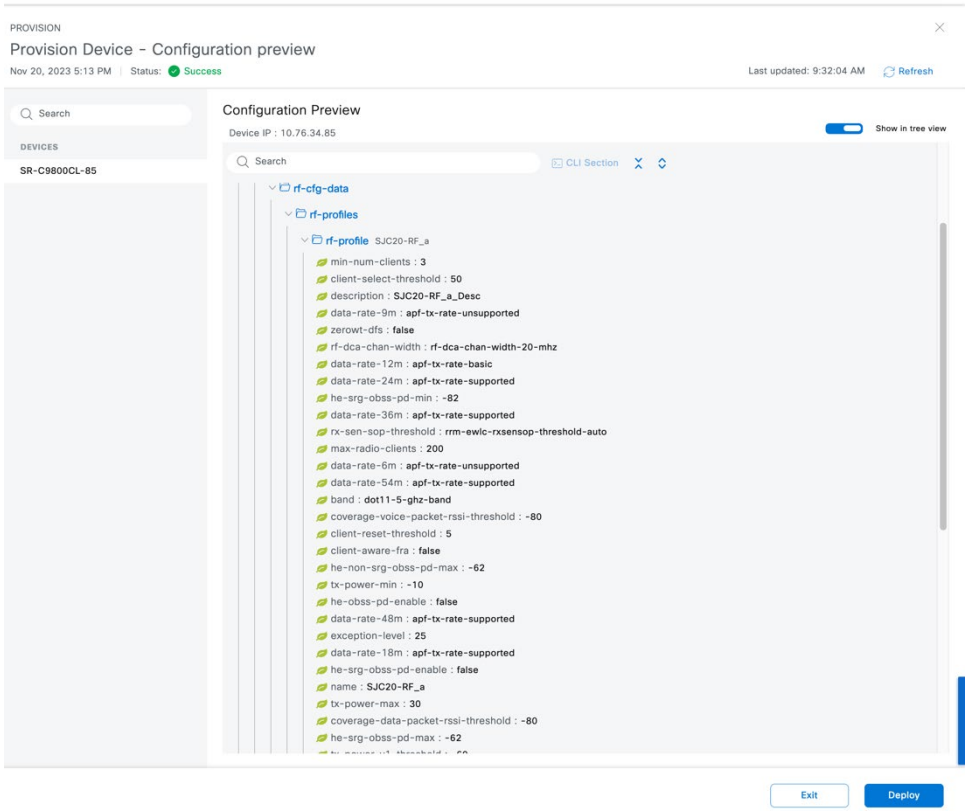

Cisco DNA Center
Actual Value
Wlan/17-1
Details
MPSK Key Format: key-ascii
MPSK priority: 1
Policy Profile/EWA-SSID-P_Global_NF_909a82c5 Accounting List Name Changed - accounting-server-1 Acknowledge


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

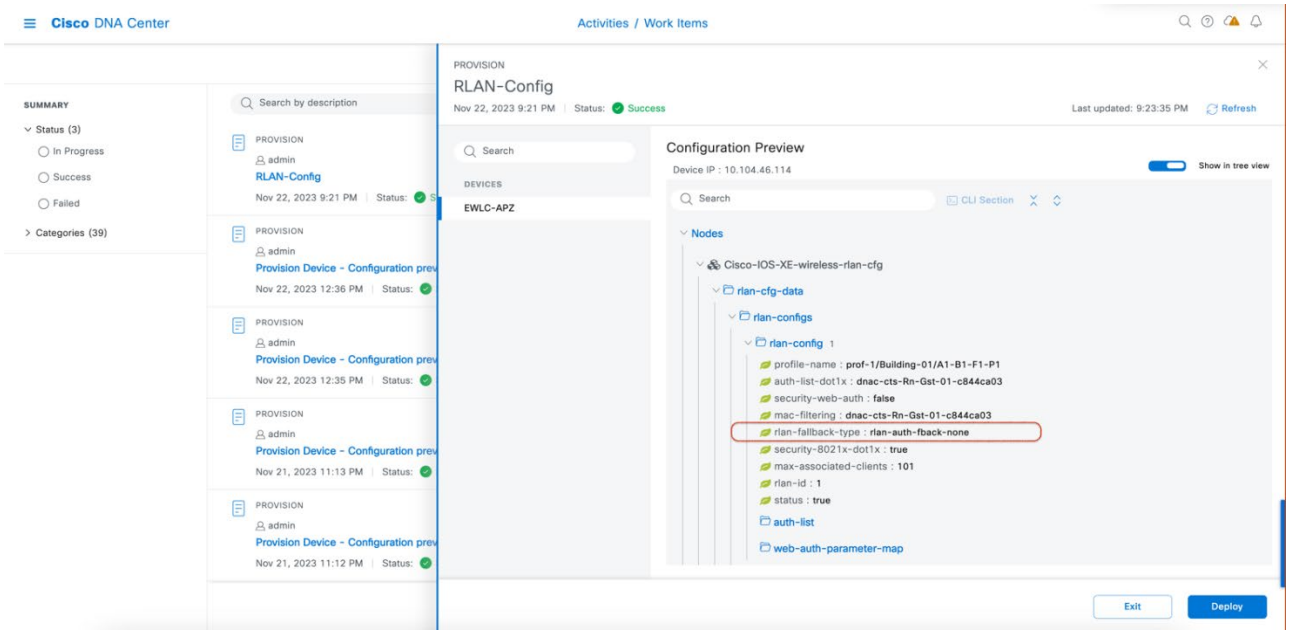

broadcast-ssid : true
ccx-aironet-ie : false
ssid : PSK-SSID
wlan-status : true
chd : true


PROVISION
Provision Device - Configuration preview
Nov 20, 2023 4:46 PM | Status: Success
Last updated: 9:10:31 AM
Refresh
Search
DEVICES
SR-BGL18-9800LC-143.cisco.com
Configuration Preview
Device IP : 10.106.133.143
Show in tree view
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

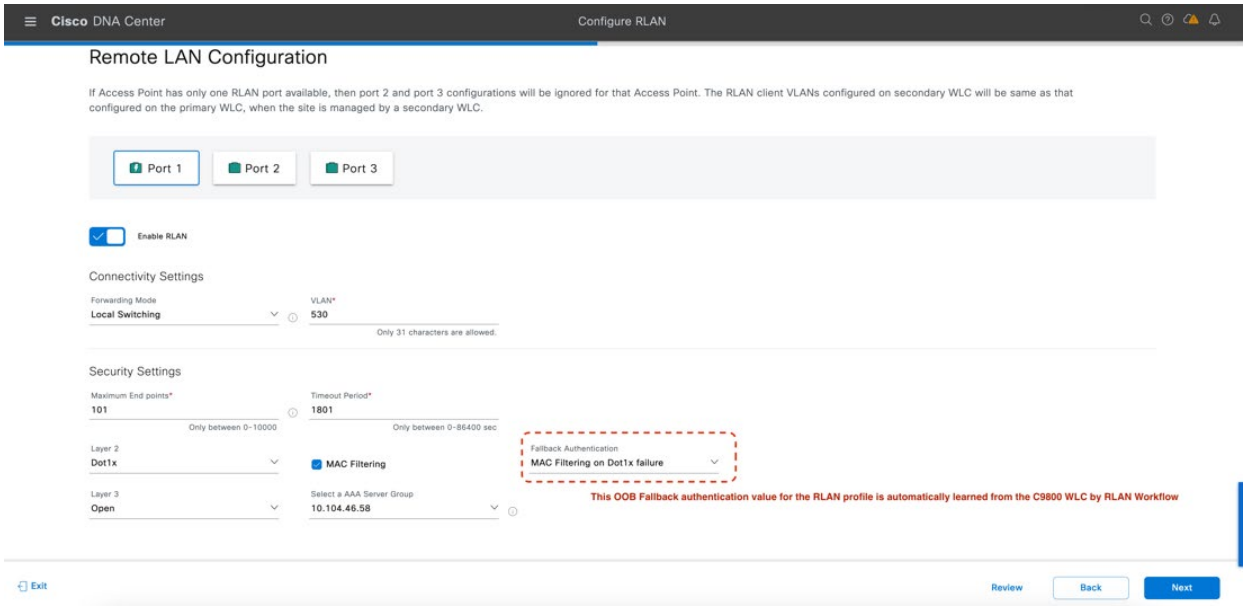
RF Profile Configuration Preview Guidelines



RLAN Feature Config Preview Guidelines



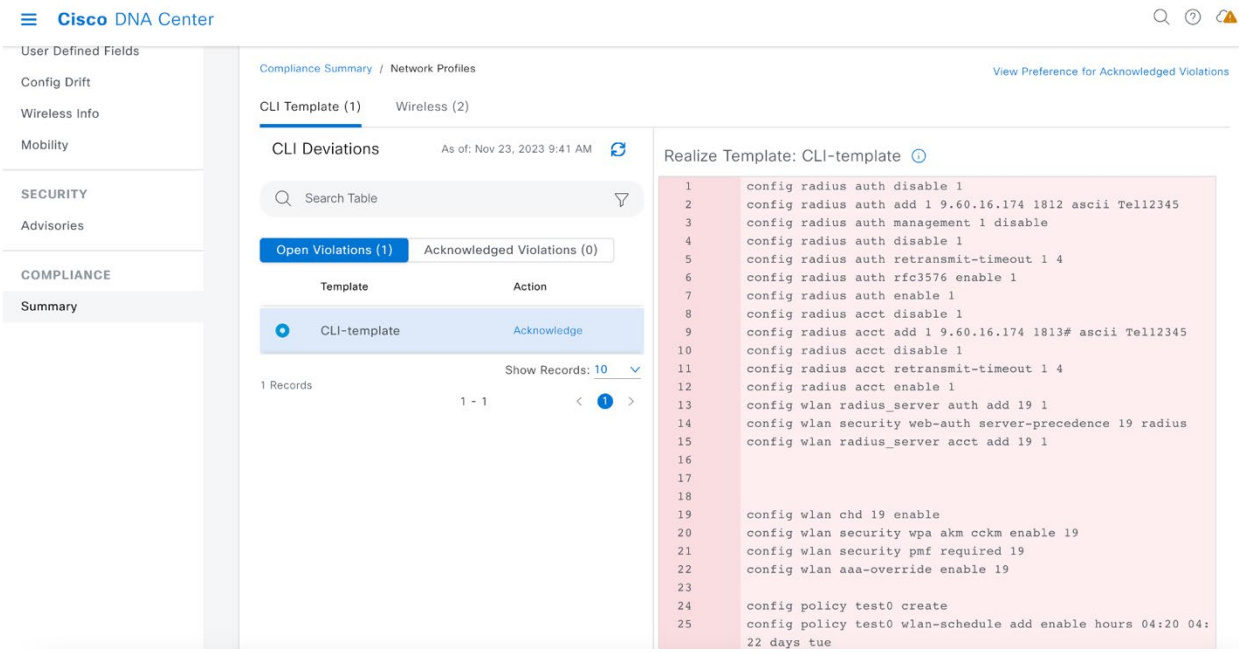
Note: After you upgrade to Cisco DNA Center Release 2.3.5.4, if you directly launch the RLAN workflow before the wireless controller reprovisioning, the current out-of-band L2 fallback values from the Catalyst 9800 Series Wireless Controller will be automatically learned and displayed in the RLAN workflow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

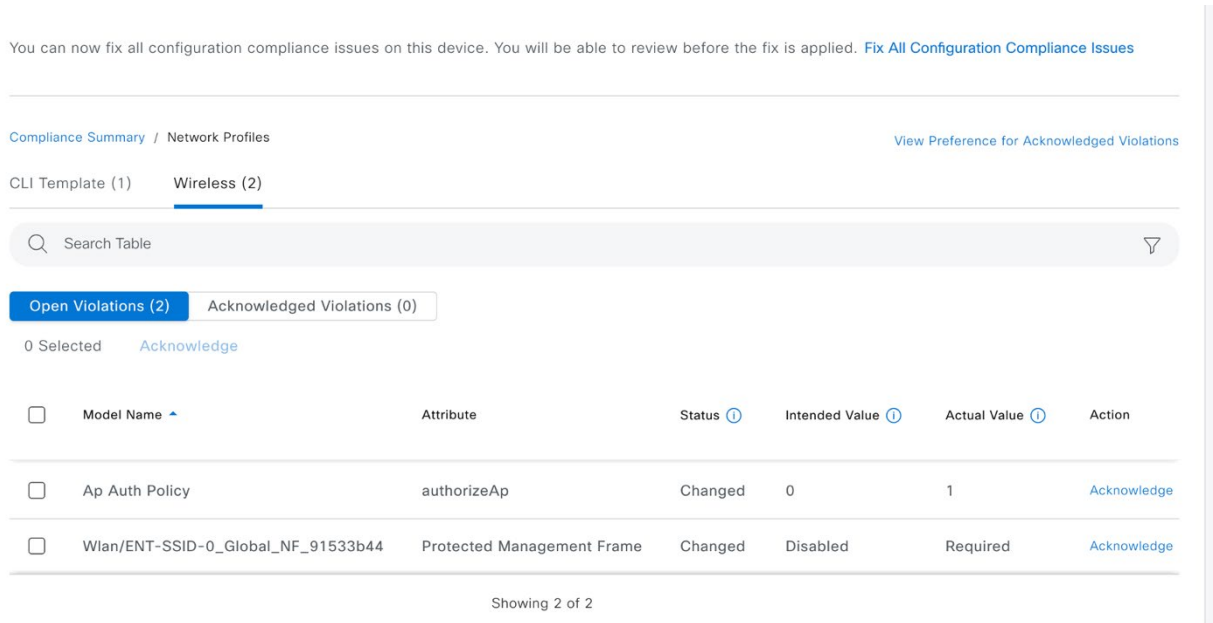


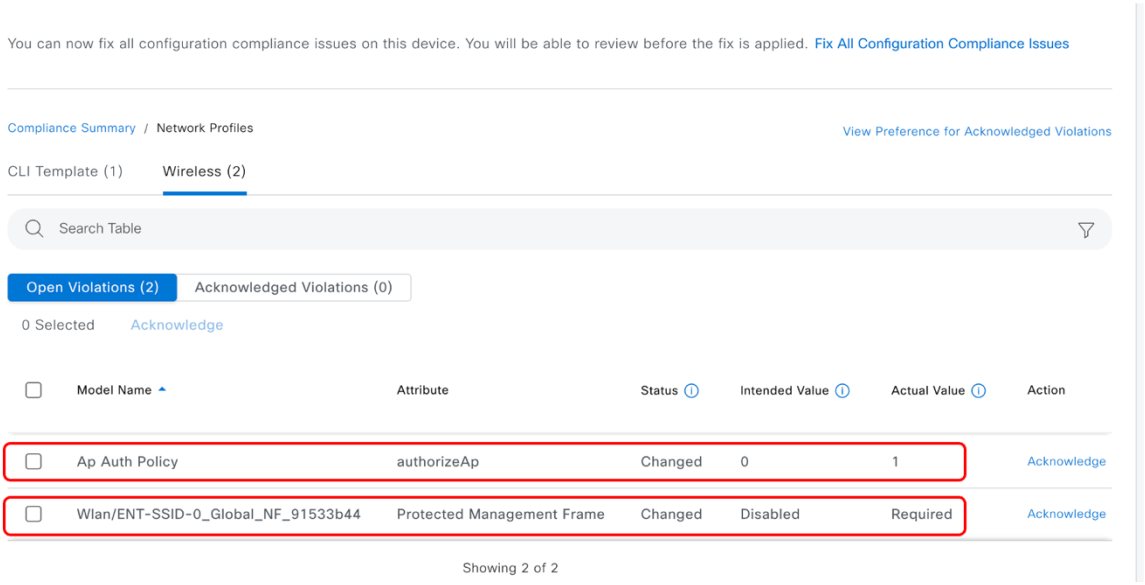
SSID and Guest Anchor Parameters List for Cisco AireOS Wireless Controllers

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.

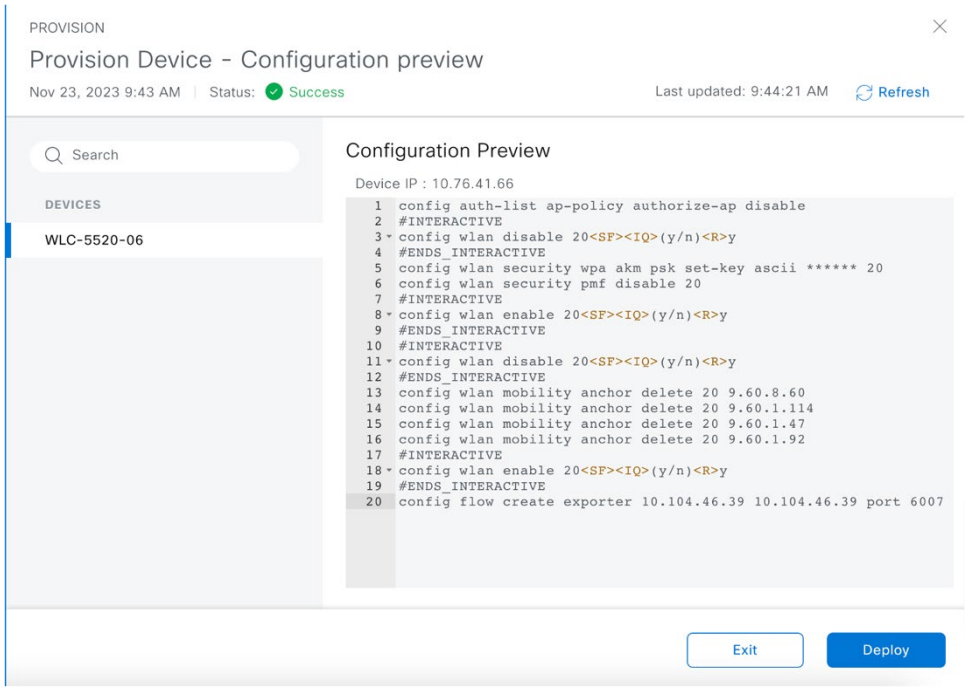
calendar-profile	AireOS	SSID Schedular	calendar-profile	None	No Impact in Cisco AireOS Wireless Controller, Cisco DNA Center will not push any value for calendar profile. No compliance mismatch and no configuration push.
AP AAA Auth	AireOS	AAA auth	AP Authorization List	NA	Impact on AP auth on the device,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







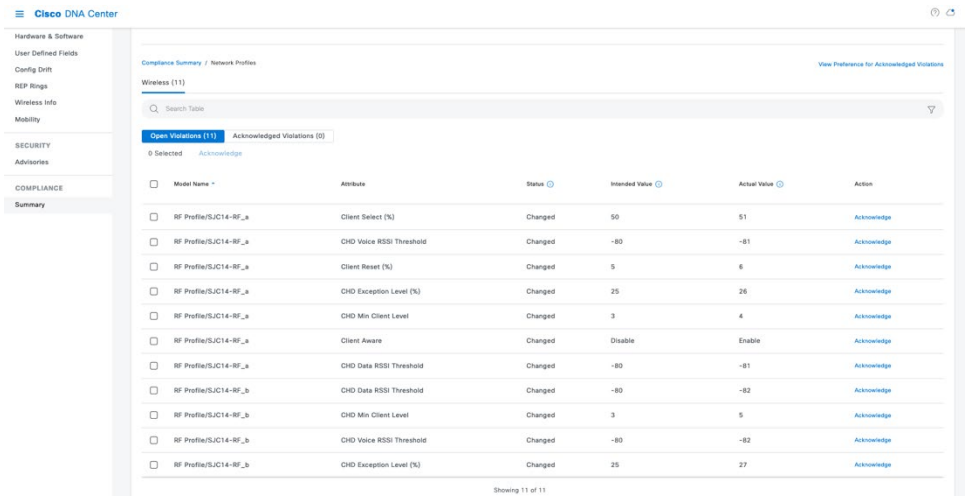
config auth-list ap-policy authorize-ap disable. ➔ compliance shows this
#INTERACTIVE
config wlan disable 20<SF><IQ>(y/n)<R>y
#ENDS_INTERACTIVE
config wlan security wpa akm psk set-key ascii ****** 20 ➔ Why we set PSK again after upgrade
config wlan security pmf disable 20 ➔ compliance shows this
#INTERACTIVE
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
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

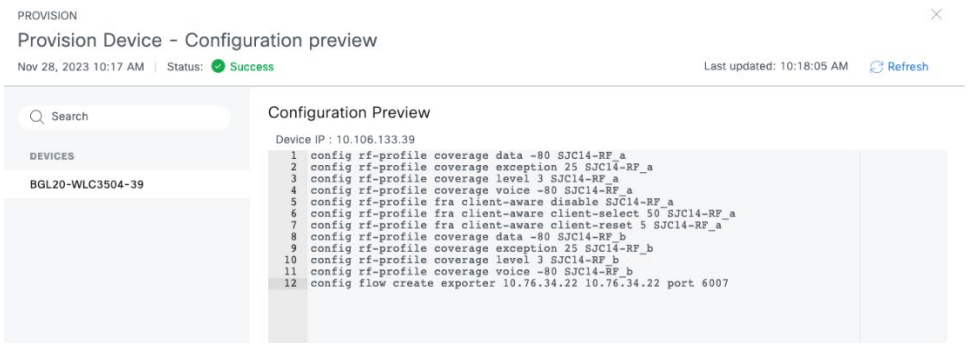
RF Profile: New Parameters for Cisco AireOS Wireless Controllers

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:



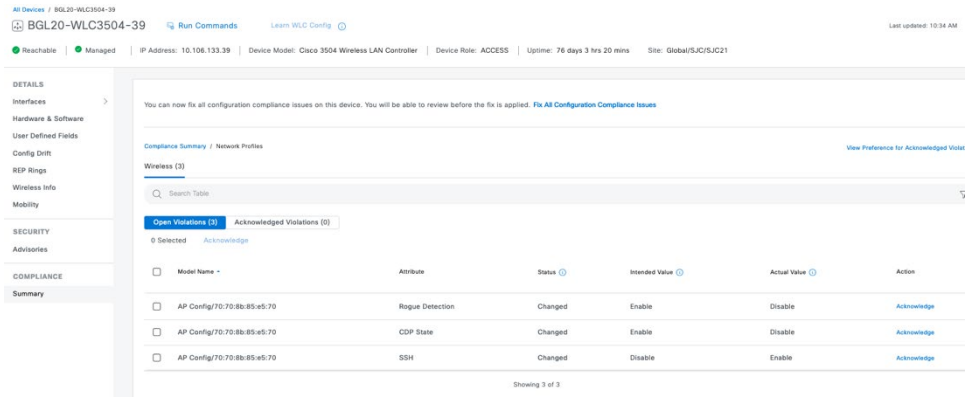
Remediate the compliance mismatches either by reprovisioning the wireless controller or using “Fix All Configuration Compliance Issues” and generate the configuration preview as follows:



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:



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