

Access Point (AP) Deployment Guide

Introduction

AX83H is an enterprise portable Wi-Fi IP color screen phone that caters to the communication needs of mobile offices. It finds extensive applications in small and medium-sized enterprises, offices, warehouses, supermarkets, hotels, and other mobile office scenarios. Featuring a built-in Bluetooth 5.0 module and a dual-band 2.4G/5G Wi-Fi 6 module, coupled with advanced seamless roaming technology, it enables you to keep pace with the ever-evolving trends in the wireless era and stay ahead of the game.

With the continuous expansion of Wi-Fi network coverage, wireless access points (AP) are now widely employed in small and medium-sized enterprises, multi-story offices, commercial establishments, and branch offices to provide seamless Wi-Fi access and mobile solutions. This guide offers comprehensive insights and step-by-step instructions for deploying an Access Point (AP) environment.

Access Point Feature Requirements

1. Embedded Wireless Controller
2. Wi-Fi roaming Protocol Support 802.11k, 802.11v, 802.11r
3. Wi-Fi Protocol Support 802.11ac, 802.11ax, 802.11n
4. Interfaces: At least 1x 10/100/1000 Base-T (Ethernet) Uplink Interface, support POE
5. Radio Support: 2.4GHz, 5GHz

Recommended AP List

The following table lists the APs that have been tested by Yealink and have good compatibility with AX83H for reference.

Cisco Wireless Access Points

Feature	Cisco Catalyst 9105i Access Point	Cisco Catalyst 9115 Access Point
Embedded Wireless Controller	√	√
Wi-Fi roaming support 802.11k, 802.11v, 802.11r	√	√
Wi-Fi Protocol Support 802.11ac, 802.11ax, 802.11n	√	√
Interfaces: At least 1 * 10/100/1000 Base-T (Ethernet) Uplink Interface, support POE	√	√

Radio Support: 2.4GHz, 5GHz	√	√
-----------------------------	---	---

TIP

AC Controller: Not required (one AC can be reused)

HPE (Aruba) Wireless Access Points

Feature	503 Series	610 Series
Embedded Wireless Controller	×	×
Wi-Fi roaming support 802.11k, 802.11v, 802.11r	√	√
Wi-Fi Protocol Support 802.11ac, 802.11ax, 802.11n	√	√
Interfaces: At least 1 * 10/100/1000 Base-T (Ethernet) Uplink Interface, support POE	√	√
Radio Support: 2.4GHz, 5GHz	√	√

TIP

AC Controller: HPE Aruba Networking 7005 (it is recommended that at least 2 AP management licenses be configured).

Rucks Wireless Access Points

Feature	R350	H350
Embedded Wireless Controller	×	×
Wi-Fi roaming support 802.11k, 802.11v, 802.11r	√	√
Wi-Fi Protocol Support 802.11ac, 802.11ax, 802.11n	√	√
Interfaces: At least 1 * 10/100/1000 Base-T (Ethernet) Uplink Interface, support POE	√	√
Radio Support: 2.4GHz, 5GHz	√	√

TIP

AC Controller: SmartZone 100 (it is recommended that at least 2 AP management licenses be configured).

Deployment Guidance

AP Deployment Requirements

When deploying a Wi-Fi network with multiple APs for AX83H roaming, follow these guidelines:

1. Make sure the AP is properly powered on and connected to your network.
2. Connect your PC to the same network as the AP. This PC is used to configure the AP and other necessary devices through the Web GUI.
3. Access the AP using the PC's Web GUI. Configure the AP for settings.
4. Set the same SSID for all APs. SSID is case-sensitive.
5. Make sure the IP addresses assigned to the APs belong to the same network segment and the same VLAN.

Conventional Obstacle Penetration Loss Comparison Table

Certain building structures and obstacles can directly interfere with or attenuate AP signals. The signal attenuation after penetrating different obstacles can be found in the following table:

Classic Obstacle	Thickness (mm)	2.4G Signal Attenuation (dB)	5G Signal Attenuation (dB)
Regular Brick Wall	120	10	20
Thickened Brick Wall	240	15	25
Concrete	254	25	30
Asbestos	8	3	4
Foam Board	8	3	4
Hollow Wood	20	2	3
Regular Wooden Door	40	3	4
Solid Wood Door	40	10	15
Regular Glass	8	4	7
Thickened Glass	12	8	10
Bulletproof Glass	30	25	35
Load-bearing Column	500	25	30
Roller Shutter Door	10	15	20
Steel Plate	80	30	35
Elevator	80	30	35

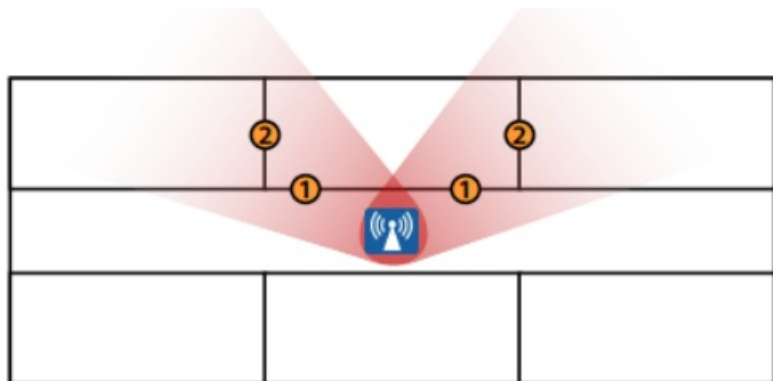
Recommended Overlap Range for AP Signal Coverage

During the deployment phase, it is essential to carefully consider the cell edge coverage for each access point (AP). It is recommended to design the cell edge of each AP with a signal strength of -67dBm to ensure optimal performance. Moreover, it is advised to maintain a 20% - 30% overlap between adjacent APs at this signal level. Failure to meet these requirements may lead to potential packet loss or blind areas at the cell edge, hindering the seamless switchover process for AX83H devices. To ensure uninterrupted roaming capabilities, it is highly recommended that AX83H devices consistently receive an RSSI of -67dBm or higher from the associated access point.

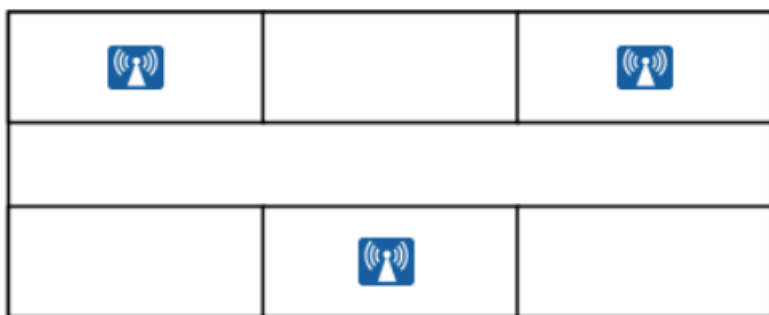
AP Placement

The placement of APs is crucial in the construction of wireless networks. Through a well-designed AP layout, signal interference can be avoided, signal attenuation can be minimized, and better network performance and user experience can be achieved.

Improper placement of APs: Signals pass through multiple walls



Reasonable placement of APs: Signals pass through a single wall



❗ IMPORTANT

1. Minimize the number of obstacles that the signal passes through.
2. Ensure that the AP is facing the target coverage area and is placed away from interference sources.
3. For scenarios that require a PoE power supply, the distance between the AP placement location and the weak current room (PoE power supply end) must be considered. The distance is recommended to be less than 100 meters.

Important WI-FI Parameters on APs

There are several crucial parameters in Wi-Fi configuration for APs. Proper configuration of these parameters will enhance the roaming performance of AX83H.

Parameter	Description
Beacon Interval	The beacon interval defines the frequency at which the AP sends 802.11 beacon management frames. The default value is typically set to 100ms. It is recommended to keep the default value on the AP.

DTIM	This is the Delivery Traffic Indication Message (DTIM) period within the beacon.  TIP It is recommended to set it to 2.
Unicast Mode and Multicast Mode	In unicast mode, the controller unicasts each multicast data packet to every associated access point. In multicast mode, the controller sends multicast data packets to the CAPWAP multicast group. This method reduces the overhead on the controller's processor and offloads the packet replication work to your network. It is recommended that unicast mode be used to ensure call quality.
WMM (Wi-Fi Multimedia)	WMM is a wireless QoS protocol and a subset of the 802.11e protocol used to ensure high-priority packets are sent first, thus guaranteeing quality of service for applications such as voice and video.  TIP QoS for SIP Layer 3 Defines the QoS parameters for Layer 3 packets of SIP messages in decimal format. This value is used for IP precedence, Diff-Serv, or MPLS. The default setting is 26, equivalent to the DSCP name constant CS6. QoS for Audio Layer 3 Defines the QoS parameters for Layer 3 packets of RTP messages in decimal format. This value is used for IP precedence, Diff-Serv, or MPLS. The default setting is 46, equivalent to the DSCP name constant CS6.
Band Steering	Dual-band operation with band steering detects clients capable of operating at 5 GHz frequency and guides them to that frequency, making the more congested 2.4 GHz band available for traditional clients. This helps improve the end-user experience by reducing channel utilization, especially in high-density environments. It is recommended to enable band steering on the AP, which means that by default, the 5 GHz band should be used (if the 5 GHz signal is weak, users can switch to 2.4 GHz).

For the above important parameters, the following sections provide configuration methods for different vendor APs for reference.

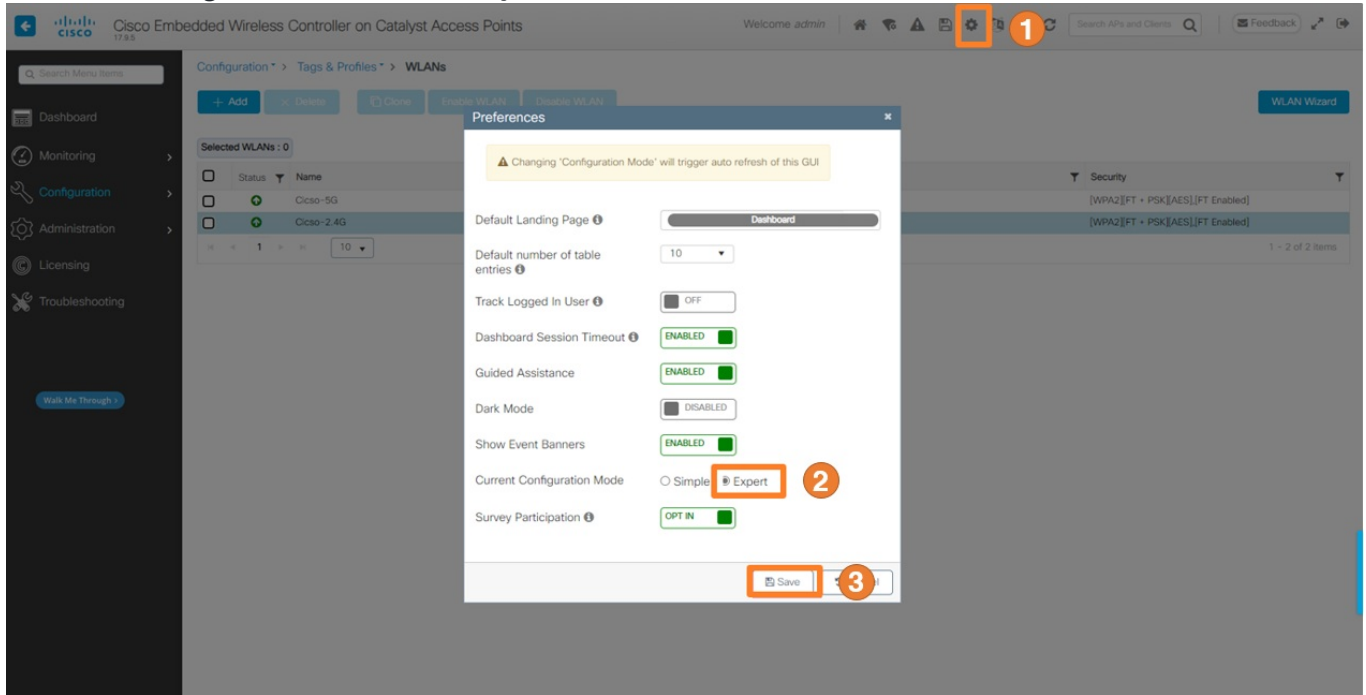
Cisco Embedded Wireless Controller

 TIP

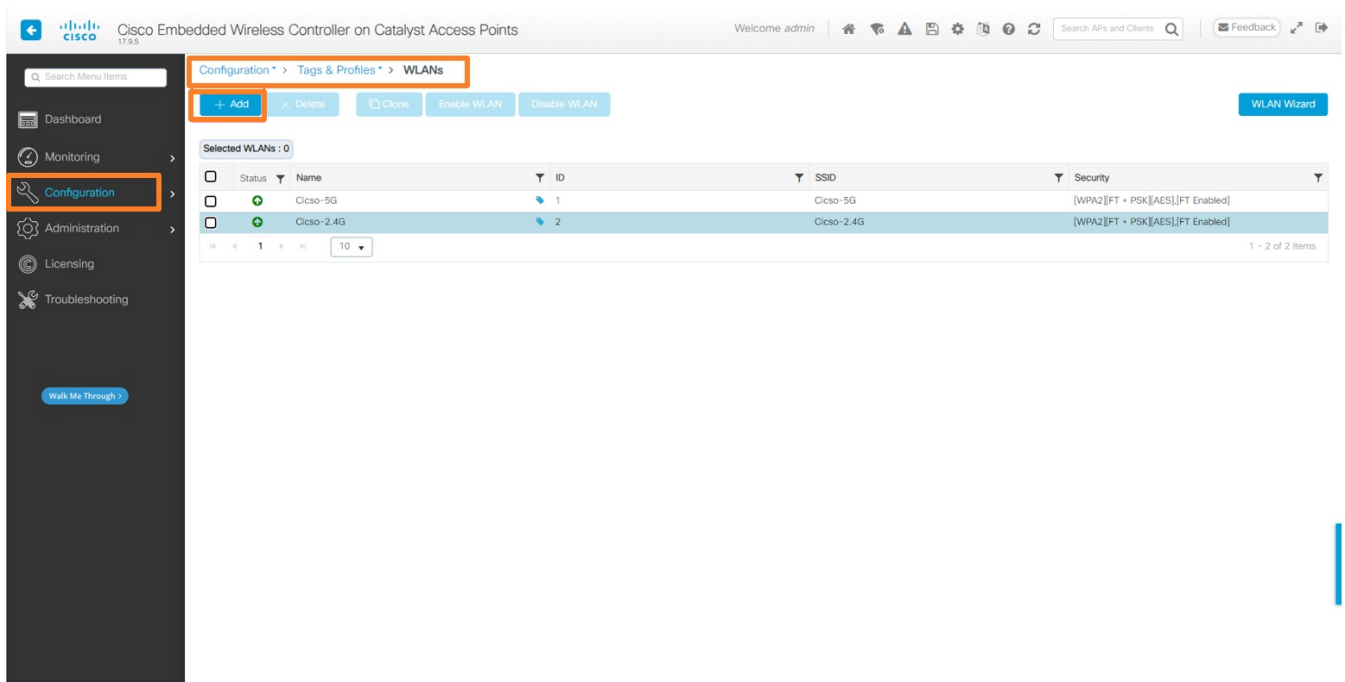
If you need more detailed information, you can visit the [Cisco Support](#) website.

1. Log in to the web user interface.

2. Switch the configuration mode to the **Expert** mode.



3. Add new WLAN. Go to **Configuration > Tags & Profiles > Wlans > Add**.



Edit WLAN

⚠️ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General

Security

Advanced

Add To Policy Tags

⚠️ Please add the WLANs to Policy Tags for them to broadcast.

Profile Name*

Cisco-2.4G

SSID*

Cisco-2.4G

WLAN ID*

2

Status

ENABLED

Broadcast SSID

ENABLED

Radio Policy ⓘ

Show slot configuration

5 GHz

Status

DISABLED

2.4 GHz

Status

ENABLED

802.11b/g Policy

802.11b/g

Cancel

Update & Apply to Device

4. Set the authentication method and fast roaming 802.11r.

Edit WLAN

General

Security

Advanced

Add To Policy Tags

Layer2

Layer3

AAA

☒ WPA + WPA2
 ☐ WPA2 + WPA3
 ☐ WPA3
 ☐ Static WEP
 ☐ None

MAC Filtering

☐

WPA Parameters

WPA Policy

☐

WPA2 Policy

☒

GTK Randomize

☐

OSEN Policy

☐

WPA2 Encryption

AES(CCMP128)

☒

CCMP256

☐

GCMP128

☐

GCMP256

☐

Protected Management Frame

PMF

Disabled

Fast Transition

Status

Enabled

Over the DS

☐

Reassociation Timeout *

20

Auth Key Mgmt

802.1x

☐

PSK

☐

CCKM

☐

FT + 802.1x

☐

FT + PSK

☒

802.1x-SHA256

☐

PSK-SHA256

☐

PSK Format

ASCII

PSK Type

Unencrypted

Pre-Shared Key*

MPSK Configuration

Enable MPSK

☐

Cancel

Update & Apply to Device

5. Set the fast roaming 802.11k, 802.11v, and Wi-Fi 6.

Edit WLAN

Per AP Per WLAN

0

Per AP Radio Per WLAN

200

11v BSS Transition Support

802.11v

BSS Transition

☒

Dual Neighbor List

☐

BSS Max Idle Service

☒

BSS Max Idle Protected

☐

Directed Multicast Service

☒

Configuration of '11v BSS Disassociation Imminent' is supported from Command Line Interface (CLI) only

11ax

Wi-Fi 6

Enable 11ax

☒

Downlink OFDMA

☒

Uplink OFDMA

☒

Downlink MU-MIMO

☒

Uplink MU-MIMO

☒

BSS Target Wake Up Time

☐

Assisted Roaming (11k)

802.11k

Prediction Optimization

☐

Neighbor List

☒

Dual Band Neighbor List

☐

DTIM Period (in beacon intervals)

5 GHz Band (1-255)

1

2.4 GHz Band (1-255)

1

Device Analytics

Advertise Support

☒

Advertise PC Analytics Support

☒

Share Data with Client

☐

11k Beacon Radio Measurement

Client Scan Report

On Association

☐

On Roam

☐

Cancel

Update & Apply to Device

- After saving and submitting, edit and assign the policy profile again.

The screenshot shows the 'Edit WLAN' interface with a warning banner at the top: 'Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.' Below the banner are tabs for 'General', 'Security', 'Advanced', and 'Add To Policy Tags'. The 'Add To Policy Tags' tab is selected and highlighted with an orange box. In the 'Add To Policy Tags' section, there is a '+ Add' button and a 'Delete' button, both highlighted with orange boxes. Below these buttons is a table with columns 'Policy Tag' and 'Policy Profile'. The table is empty, showing '0' items and 'No items to display'. To the right of the table is a modal dialog box for adding a new policy tag. It contains two dropdown menus: 'Policy Tag' with 'default-policy-tag' selected and 'Policy Profile' with 'default-policy-profil' selected. Below the dropdowns are 'Save' and 'Cancel' buttons, with the 'Save' button highlighted by an orange box. At the bottom right of the interface, there is an 'Update & Apply to Device' button, also highlighted with an orange box.

Aruba

TIP

If you need more detailed information, you can visit the [Aruba Support](#) website.

- Log in to the web user interface.
- Go to **Dashboard > Configuration > WLANs** >  to add a new WLAN.

aruba MOBILITY CONTROLLER Aruba7005_5D_AD_7E

ACCESS POINTS 2 0 CLIENTS 1 0 ALERTS 0

admin

← Mobility Controller > Aruba7005_5D_AD_7E

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

System

Tasks

Redundancy

IoT

Diagnostics

Maintenance

WLANs 3

NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION
aruba-2.4g	default; test	WPA2-Personal	--
aruba-5g	default; test	WPA-Personal	--
test	default	WPA2-Personal	--

+

aruba MOBILITY CONTROLLER Aruba7005_5D_AD_7E

ACCESS POINTS 2 0 CLIENTS 1 0 ALERTS 0

admin

← Mobility Controller > Aruba7005_5D_AD_7E

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

System

Tasks

Redundancy

IoT

Diagnostics

Maintenance

New WLAN

General VLANs Security Access

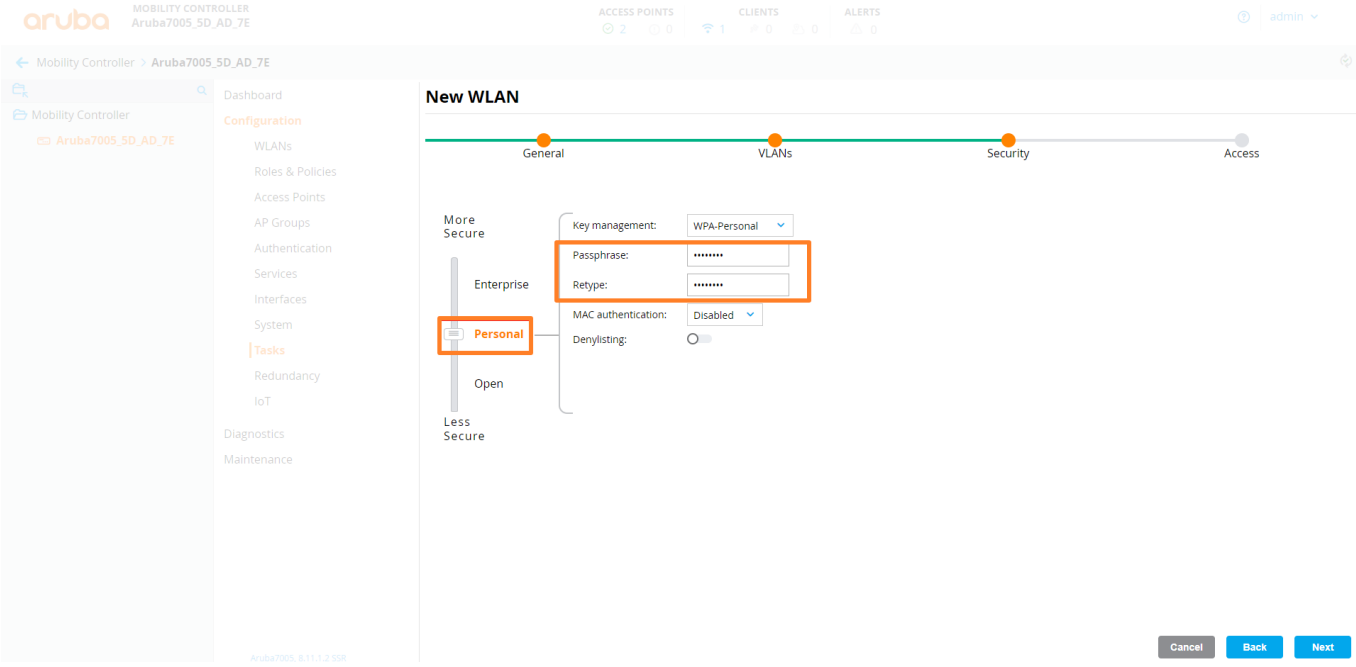
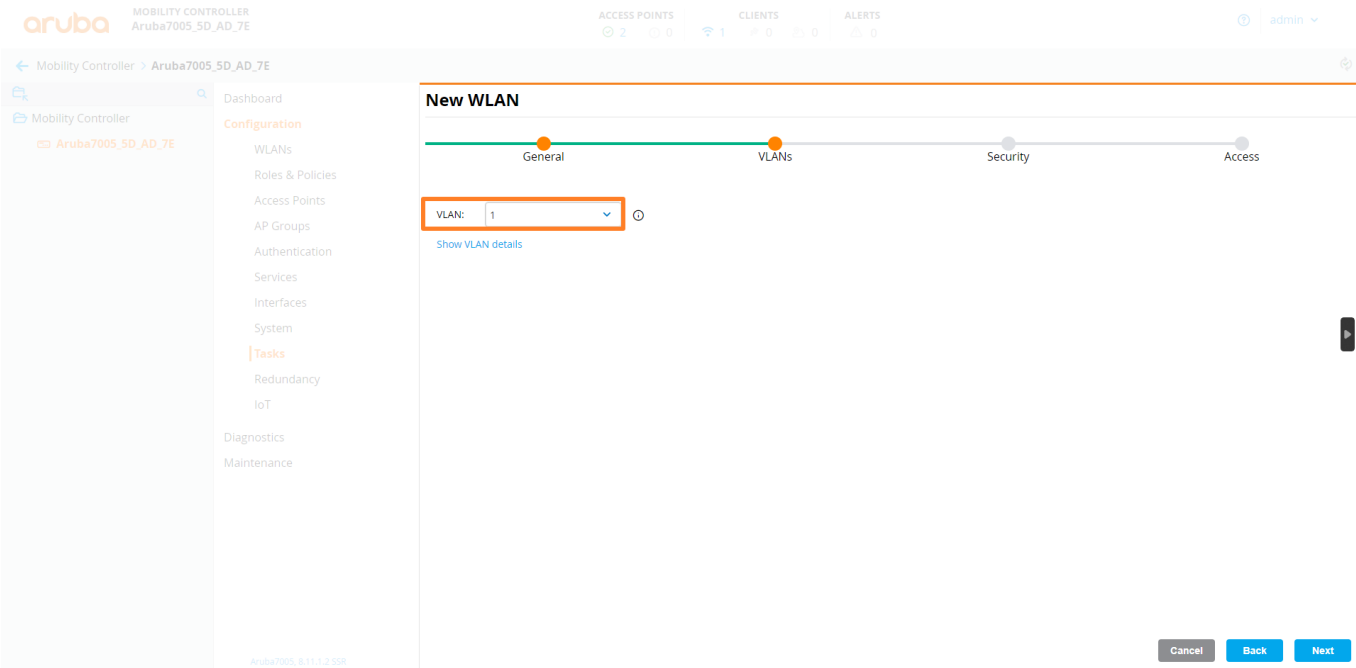
Name (SSID): aruba-2.4g-kvr

Primary usage: ☒ Employee ☐ Guest

Broadcast on: All APs

Forwarding mode: Bridge

Cancel Back Next



aruba

MOBILITY CONTROLLER
Aruba7005_5D_AD_7E

ACCESS POINTS
2 0 0

CLIENTS
1 0 0

ALERTS
0 0

admin

← Mobility Controller > Aruba7005_5D_AD_7E

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

System

Tasks

Redundancy

IoT

Diagnostics

Maintenance

Aruba7005, 8.11.1.2 SSR

New WLAN

General

VLANs

Security

Access

Default role: logon

Cancel

Back

Finish

aruba

MOBILITY CONTROLLER
Aruba7005_5D_AD_7E

ACCESS POINTS
2 0 0

CLIENTS
1 0 0

ALERTS
0 0

admin

← Mobility Controller > Aruba7005_5D_AD_7E

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

System

Tasks

Redundancy

IoT

Diagnostics

Maintenance

Aruba7005, 8.11.1.2 SSR

WLANs 4

NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION
aruba-2.4g	default, test	WPA2-Personal	--
aruba-2.4g-kvr	default, test	WPA-Personal	--
aruba-5g	default, test	WPA-Personal	--
test	default	WPA2-Personal	--

aruba-2.4g

General

VLANs

Security

Access

Profiles

Name (ssid):

aruba-2.4g

Primary usage:

Employee

Guest

Broadcast on:

All APs

Forwarding mode:

Bridge

Cancel

Submit

3. 5G cannot be turned off individually, but 2.4G can be enabled individually when **Allowed band** is set to **a** or **g**.

The screenshot shows the Aruba Mobility Controller web interface for the 'Aruba7005_5D_AD_7E' controller. The left sidebar shows the navigation menu with 'Configuration' selected. The main content area shows the 'WLANs' table with 4 entries. The 'aruba-2.4g-kvr' entry is selected, and the 'Profiles' tab is active. The 'Virtual AP profile: aruba-2.4g-kvr' is shown, with the 'General' tab selected. The 'Allowed band' dropdown menu is open, showing options 'g', 'a', 'none', and 'all'. The 'a' option is highlighted. The 'Allowed 5G radio' dropdown menu is also open, showing options 'none' and 'all'. The 'Steering Mode' is set to 'prefer-5ghz'.

The screenshot shows the Aruba Mobility Controller web interface for the 'Aruba7005_5D_AD_7E' controller. The left sidebar shows the navigation menu with 'Configuration' selected. The main content area shows the 'WLANs' table with 4 entries. The 'aruba-2.4g-kvr' entry is selected, and the 'Profiles' tab is active. The 'Virtual AP profile: aruba-2.4g-kvr' is shown, with the 'General' tab selected. The '802.11k Profile: default' is shown, and the 'Advertise 802.11k Capability' checkbox is checked. The '802.11k Profile: default' is shown, and the 'Advertise 802.11k Capability' checkbox is checked. The '802.11k Profile: default' is shown, and the 'Advertise 802.11k Capability' checkbox is checked.

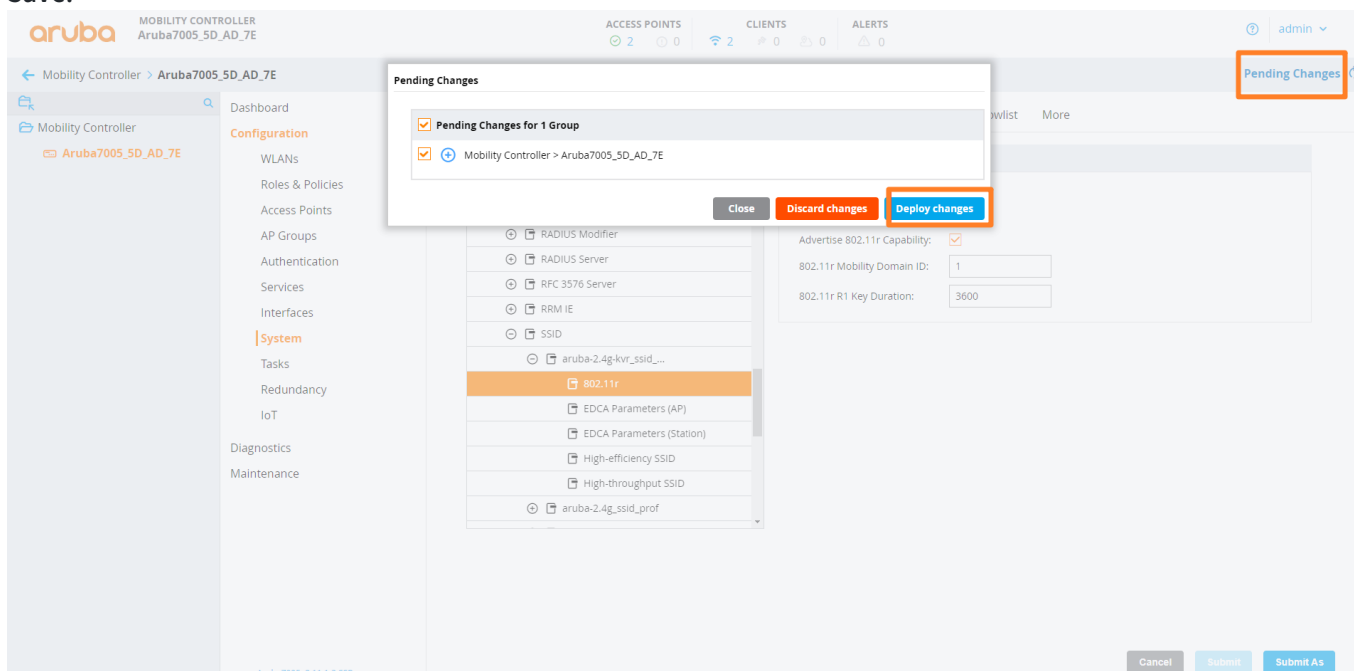
4. Set the 802.11R fast roaming feature profile.

The screenshot shows the Aruba Mobility Controller web interface for the device 'Aruba7005_5D_AD_7E'. The 'Profiles' tab is selected in the top navigation bar. In the left sidebar, the 'System' option under 'Interfaces' is highlighted. The main content area displays the 'All Profiles' list on the left, where '802.11r' is selected. On the right, the '802.11r Profile: default' configuration page is shown. The 'Advertise 802.11r Capability' checkbox is checked. The '802.11r Mobility Domain ID' is set to '1' and the '802.11r R1 Key Duration' is set to '3600'. At the bottom right, there are 'Cancel', 'Submit', and 'Submit As' buttons.

5. In SSID, select Apply 802.11r Profile.

The screenshot shows the same Aruba Mobility Controller web interface. The 'Profiles' tab is still selected. In the left sidebar, the 'System' option under 'Interfaces' is highlighted. The main content area displays the 'All Profiles' list on the left, where 'SSID' is selected. On the right, the '802.11r Profile: default' configuration page is shown. The '802.11r Profile' dropdown menu is set to 'default'. The 'Advertise 802.11r Capability' checkbox is checked. The '802.11r Mobility Domain ID' is set to '1' and the '802.11r R1 Key Duration' is set to '3600'. At the bottom right, there are 'Cancel', 'Submit', and 'Submit As' buttons.

6. Save.



Ruckus



TIP

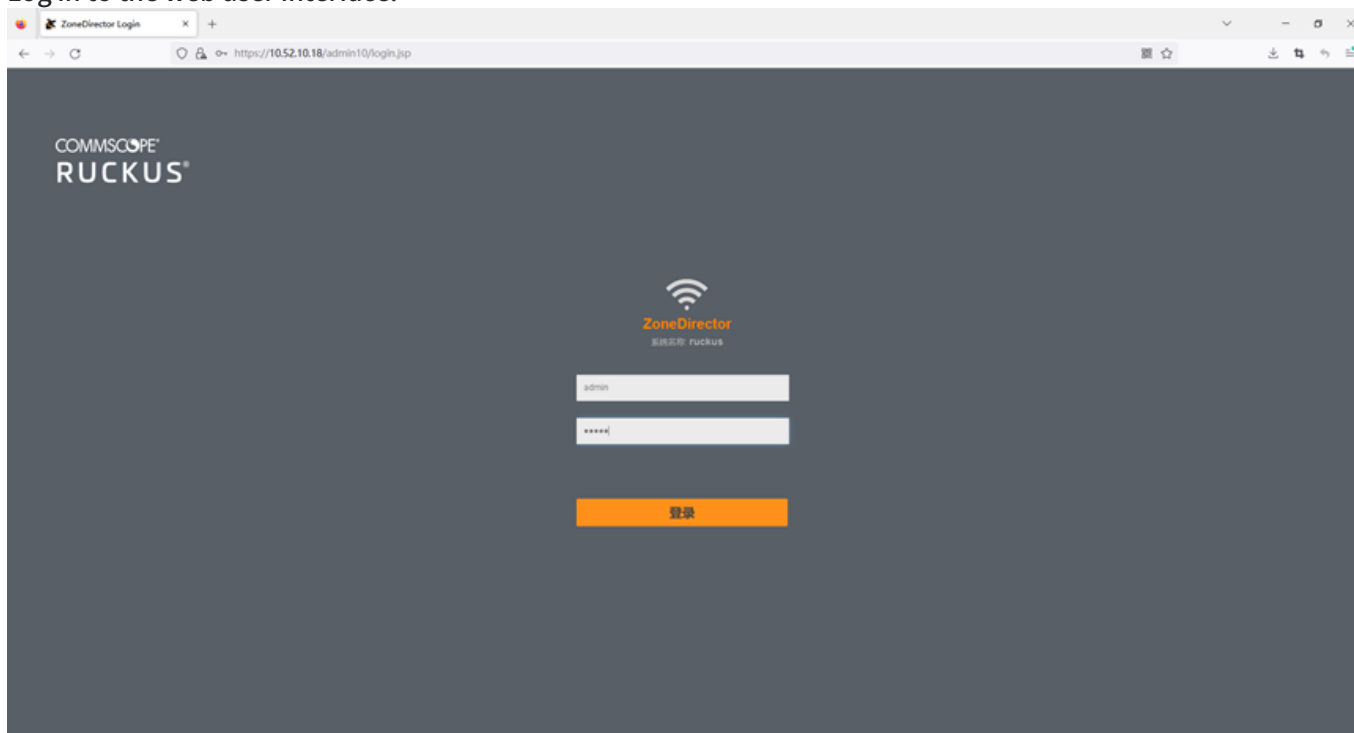
If you need more detailed information, you can visit the [Ruckus Support](#) website.



NOTE

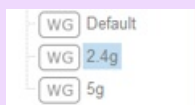
802.11v is enabled by default and cannot be configured in the GUI or the CLI.

1. Log in to the web user interface.



2. Add a new WLAN. We will add a 2.44GHZ WLAN as an example.

NOTE



The WLAN group **Default** is used for dual-band WLAN.

The WLAN group **2.4g** is used for 2.4GHZ WLAN.

The WLAN group **5g** is used for 5GHZ WLAN.

The screenshot displays the Ruckus ZoneDirector ZD1200 web interface. The main menu on the left includes options like 'Overview', 'Enter Point', 'Wireless Local Area Network', 'Client', 'Configuration', 'System', and 'Management'. The 'Wireless Local Area Network' (无线局域网) page is active, showing a list of WLAN groups (WG Default, WG 2.4g, WG 5g). The 'New WLAN' (新建 WLAN) dialog box is open, allowing the user to configure a new WLAN. The 'Name' (名称) is set to 'ruXus-2.4g' and the 'ESSID' is set to 'ruXus-2.4g'. The 'WLAN Usage' (WLAN 使用情况) section shows 'Type' (类型) set to 'Default Usage' (默认使用状况). The 'Authentication' (身份验证) section shows 'Method' (方法) set to 'Open' (开放). The 'Fast BSS Transition' (快速漫游) section shows 'Fast BSS Transition' (快速漫游) checked, with a red box highlighting the '802.11r Fast Transition' (802.11r 快速漫游) option. A red text label '802.11r快速漫游功能选项' points to this option.

新建 WLAN



加密选项

方法: ☒ WPA2 ☐ WPA3 ☐ WPA2/WPA3-Mixed ☐ OWE ☐ WPA-Mixed ☐ None算法: ☒ AES ☐ 自动 (TKIP+AES)

密码: 12345678

802.11w MFP: ☒ 已禁用 ☐ 可选择的 ☐ 必须的

高级选项

无线用户隔离: ☐ 在相同的AP上的其他用户隔离无线用户频道。☐ 在相同的AP或子网上的所有用户隔离无线用户频道。不使用白名单

(网关和其他被允许的主机需要白名单)

WLAN 优先级: ☒ 高 ☐ 低记帐服务器: 禁用 发送周期更新, 间隔为 10 分钟访问控制: L2/MAC 无 ACL L3/4/IP 地址 无 ACL 设备访问策略 无 优先级策略 Default ☐ 启用基于角色的访问控制策略

需要在“管理 > 服务”->“角色”中启用基于角色的访问控制策略

应用识别控制: ☐ 启用应用识别控制URL 过滤: ☐ 启用URL过滤

确定

取消

新建 WLAN

802.11d: ☒ 支持 802.11d(仅作用于2.4G频段)DHCP option 82: ☐ 启用 DHCP Option 82Force DHCP: ☐ 使能 Force DHCP, 请断开客户端, 如果客户端没有获得有效的IP地址在 秒后.DTIM 间隔: (1-255)定义包含DTIM的信标频率管理 MC/BC 阈值: (0-128)定义当AP停止将组寻址数据流量转换为单播时客户端计数客户端收发统计: ☐ 忽略未认证的客户端统计客户端指纹识别: ☒ 启用客户端指纹识别OFDM Only: ☐ 使能 OFDM OnlyBSS Min Rate: Mgmt Tx Rate: (5 GHz 不支持 CCK 速率 (1, 2, 5.5, 11 Mbps).)服务时间表: ☒ Always on ☐ Always off ☐ SpecificAuto-Proxy: ☐ 启用自动代理配置空闲超时: 在以下时间后, 终止空闲用户会话: 分钟空闲时间无线资源管理: ☒ 启用 802.11k 邻居表报告

802.11K快速漫游功能选项

客户端流量日志: ☐ 将客户端数据流发送到syslog服务器☐ 将连接记录发送到syslog服务器

(也可在客户端连接日志中的故障排除->诊断中下载。)

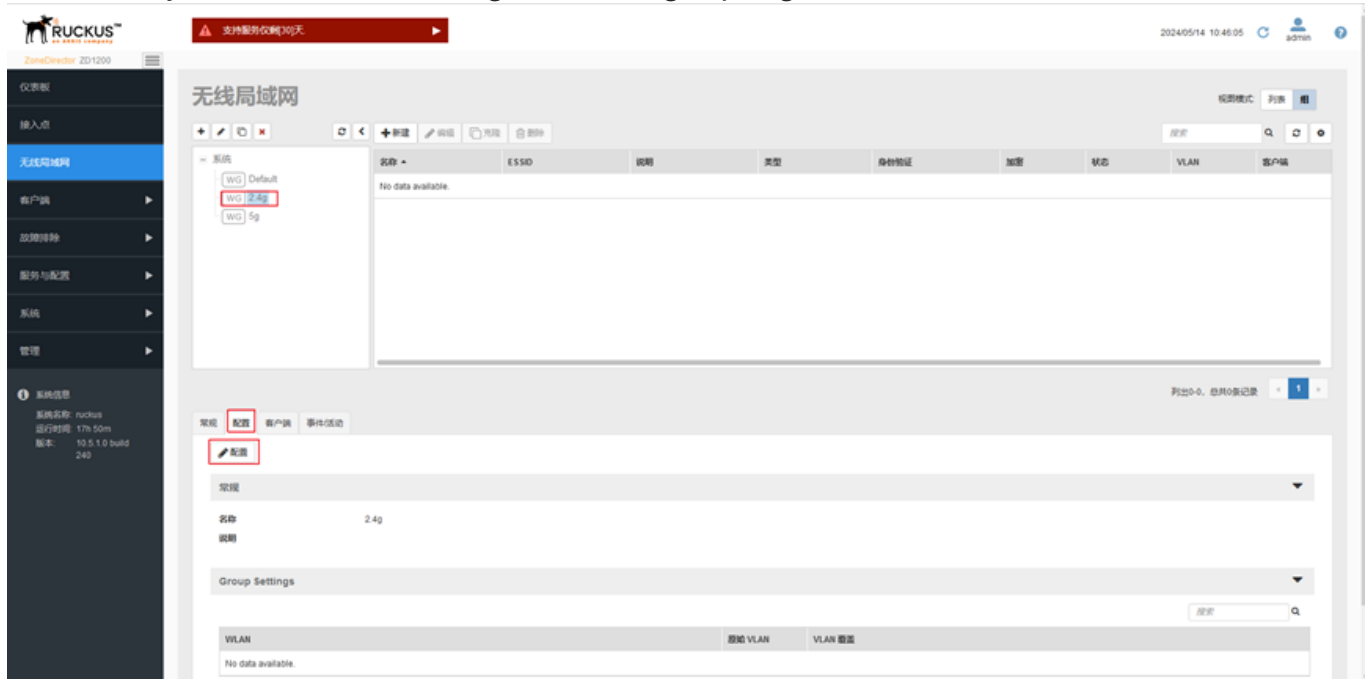
瞬时客户端管理: ☐ 启用瞬时客户端管理Wi-Fi 6: ☒ 启用

WIFI6功能选项

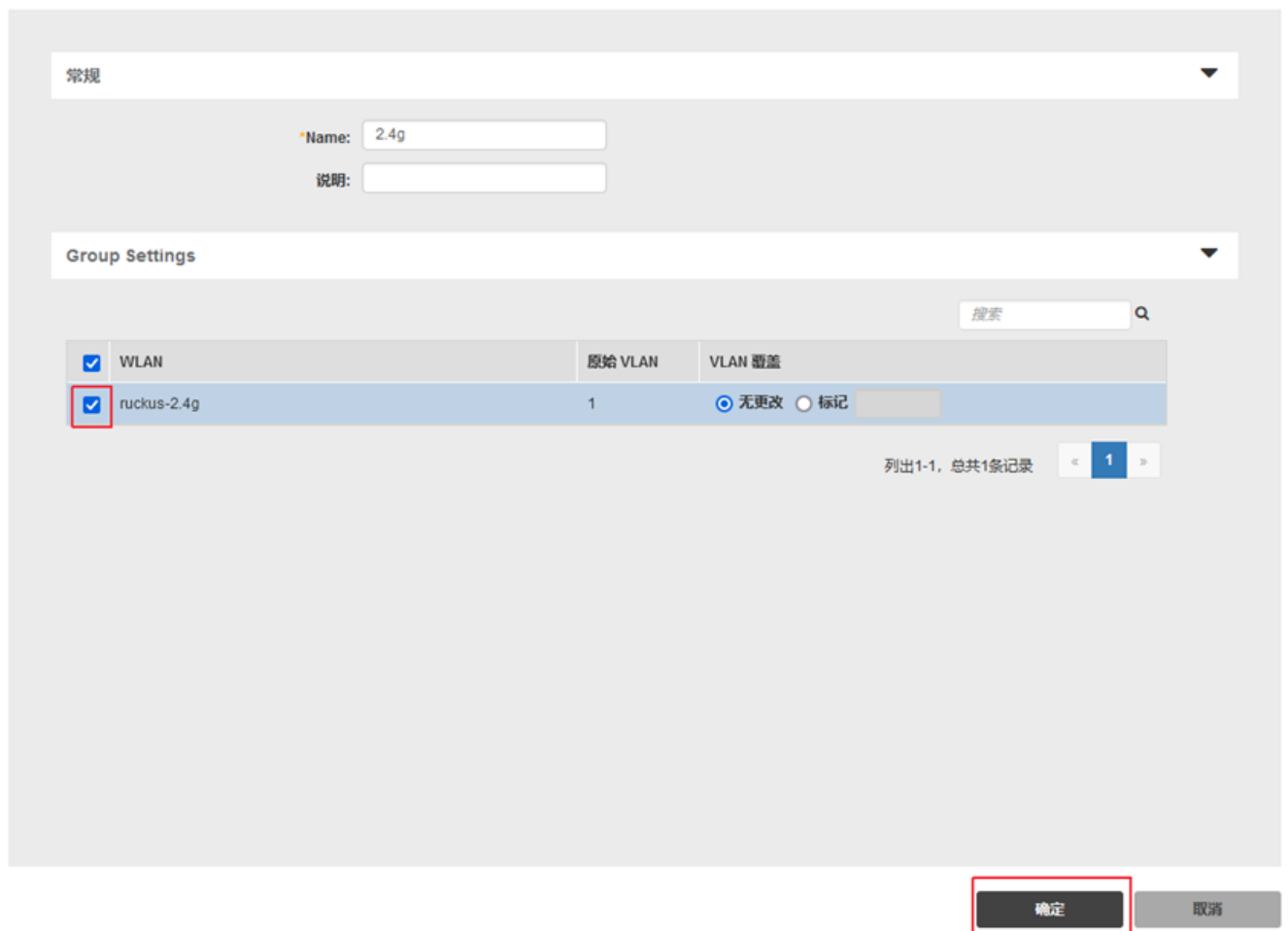
确定

取消

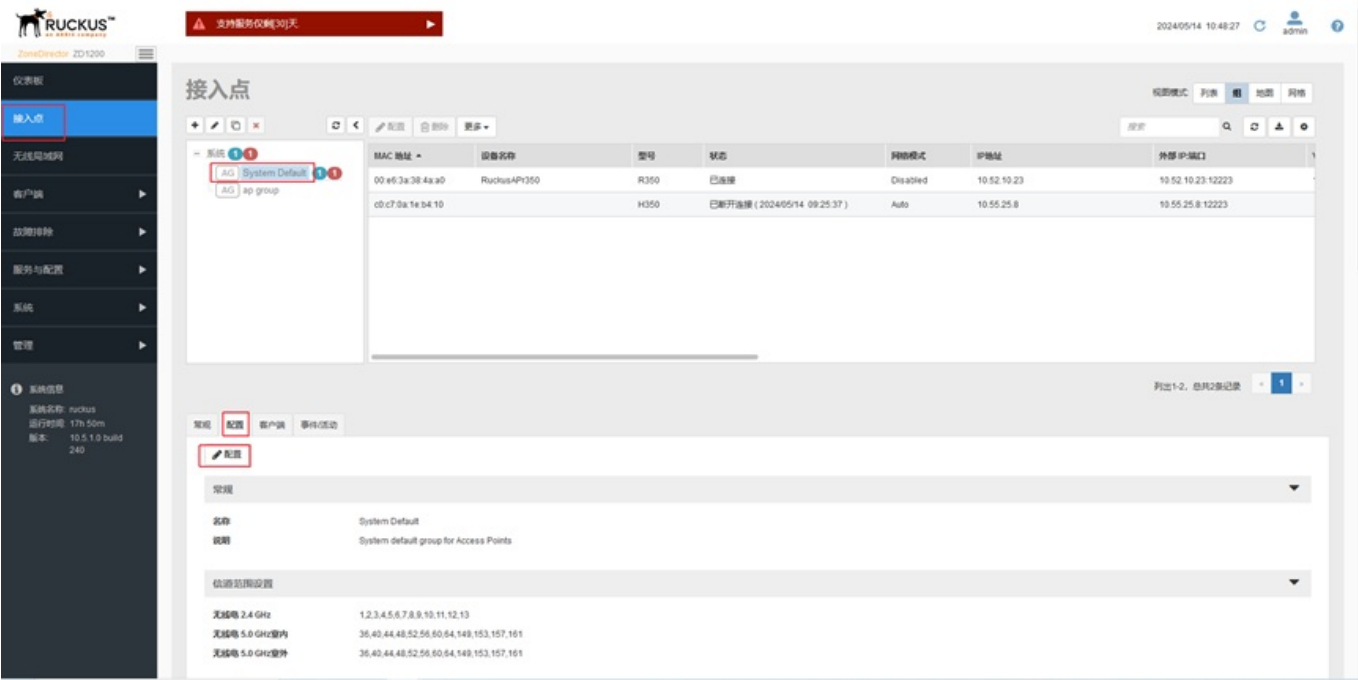
3. Add the newly created WLAN ruckus 2.4g to the WLAN group 2.4g.



编辑 WLAN 组



4. Access Point Configuration.



5. The current configuration is that the WLAN group **2.4g** uses 2.4GHZ, and the WLAN group **5g** uses 5GHZ. If you need WLAN to support dual-band, set the WLAN group in the Radio settings to **Default**. The WLAN in the ****Default**** group can use dual-band transmission signals.

编辑AP组

名称: System Default

说明: System default group for Access Points

信道范围设置

无线电 2.4 GHz: ☒ 1 ☒ 2 ☒ 3 ☒ 4 ☒ 5 ☒ 6 ☒ 7 ☒ 8 ☒ 9 ☒ 10 ☒ 11 ☒ 12 ☒ 13

无线电 5.0 GHz室内: ☒ 36 ☒ 40 ☒ 44 ☒ 48 ☒ 52 ☒ 56 ☒ 60 ☒ 64 ☒ 149 ☒ 153 ☒ 157 ☒ 161

无线电 5.0 GHz室外: ☒ 36 ☒ 40 ☒ 44 ☒ 48 ☒ 52 ☒ 56 ☒ 60 ☒ 64 ☒ 149 ☒ 153 ☒ 157 ☒ 161

Radio设置

无线电 2.4 GHz

无线电 5.0 GHz

信道带宽: 自动

信道: 自动

发射功率: 自动

WLAN 组: 2.4g

呼叫确认控制: 关闭

WLAN 服务: 启用

保护模式: RTS/CTS

自动

室内: 自动

室外: 自动

自动

关闭

启用

网络设置

确定 取消