

iKnos Corporate

INSTALLATION GUIDE



RUCKUS APS
Integration Guide

iKnos Corporate by Foot Analytics

Last revision
November 2022

Configuration

In *System > General Settings*

For configuring the integration with Ruckus APS, follow the next steps:

1. Click on **Access Points** on left menu.
2. When loaded, click the zone that you want to connect (2) and then press the edit button (3):

Virtual SmartZone - Essentials

Dashboard

System

- General Settings
- Switch Settings
- AP Settings
- Cluster
- Maps
- Certificates
- Templates
- Access Points** (1)
- Switches
- Wireless LANs

Access Points (2) 1 Online 0 Flagged 1 Offline

System > Default Zone

3

1 2

MAC Address	AP Name	Status
44:1E:98:35:5B:40	RuckusAP	Offline
EC:58:EA:2D:71:C0	RuckusAP	Online

General Configuration Health Traffic Alarm Event Clients Wired Clients WI

Group Info

Name	Default Zone

3. A settings pop-up will appear. Then you must go to the **Advanced Options**, enable the **Location Based Service** and select (or create) the venue.

Configure Group ✕

Name: Description:

Type: Zone AP Group

Parent Group:

Configuration

AP SNMP Options

AP Model Specific Configuration

Advanced Options

Channel Mode: OFF Allow indoor channels (allow ZoneFlex outdoor APs to use channels regulated as for indoor use only)

[?] Auto Channel Selection: ON Automatically adjust 2.4 GHz channel using

ON Automatically adjust 5 GHz channel using

[?] Background Scan: ON Run background scan on 2.4 GHz radio every seconds (1-65535)

ON Run background scan on 5 GHz radio every seconds (1-65535)

[?] Bonjour Fencing: OFF * Fence Policy:

Smart Monitor: OFF (WLANs will be disabled automatically if the default gateway of AP is unreachable)

Health Check Interval: seconds (5-60)

Health Check Retry Threshold: (1-10)

AP Ping Latency Interval: ON

AP Management VLAN: Keep AP's settings VLAN ID

Rogue AP Detection: ON

[?] Rogue Classification Policy:

Enable events and alarms for all rogue devices

Enable events and alarms for malicious rogues only

OFF Protect the network from malicious rogue access points

DoS Protection: OFF Block a client for seconds (30-600) after repeat authentication failures (2-25) within seconds (30-600)

Client Load Balancing: Balances the number of clients across adjacent APs.

OFF Run load balancing on 2.4 GHz radio Adjacent Radio Threshold (dB)

OFF Run load balancing on 5 GHz radio Adjacent Radio Threshold (dB)

[?] Band Balancing:

Percentage of client load on 2.4G Band:

Location Based Service: ON 4

[?] Hotspot 2.0 Venue Profile:

[?] Client Admission Control: 2.4 GHz Radio OFF 5 GHz Radio OFF

OK

Cancel