COMMSCOPE®

RUCKUS®

Configuration Guide

RUCKUS Wireless Controller Configuration: Hospitality

October 2020

Table of Contents

Intended Audience

This document addresses factors and concerns related to configuring the RUCKUS SmartZone controller for hospitality environments. Many factors can affect both the initial work and final performance. These are considered here.

This document is written for and intended for use by technical engineers with some background in Wi-Fi design and 802.11/wireless engineering principles.

For more information on how to configure CommScope products, please refer to the appropriate CommScope user guide available on the CommScope support site. https://www.commscope.com/SupportCenter/.

Overview

This document provides network designers, architects, and WLAN professionals guidance for configuring a WLAN controller using CommScope's RUCKUS networking equipment and software. This document is one in a series of design and configuration guides. This document is the fourth in this series created for the Hospitality market. Please reference the full suite of Guides for Hospitality.

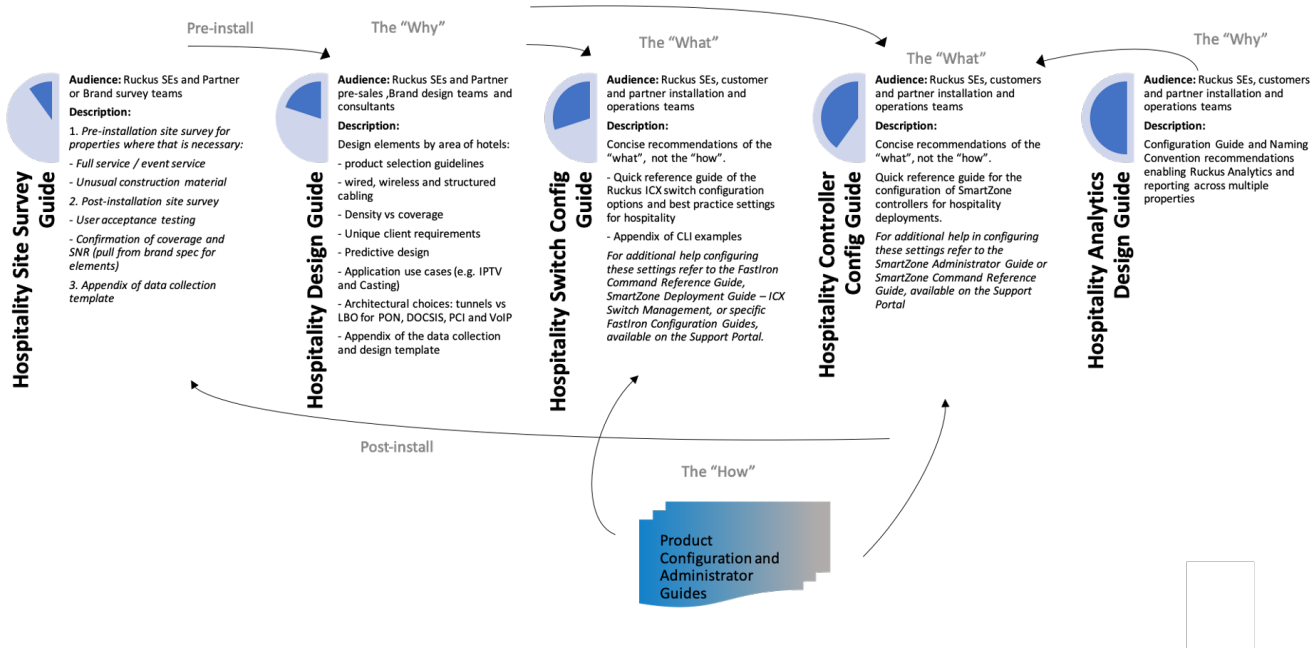

FIGURE 1: SUITE OF DESIGN AND CONFIGURATION GUIDES FOR HOSPITALITY

This document is intended to provide guidance to Hospitality Managed Service Providers to ensure consistency and optimal performance of deployed RUCKUS WLAN infrastructures across properties.

This document is one in a series of Design and Configuration Guides specific to the Hospitality vertical. Please refer to the other documents to provide a more complete picture. The intended audience for this body of work includes Ruckus Systems Engineers and customer and/or partner installation and operations teams. These documents are intended to primarily cover the "What" and some of the "Why", not necessarily the "How", when it comes to configurations. Ruckus provides separate additional resources, both in the form of online and offline configuration guides, internal/partner support portal knowledge base, and How-to videos posted to YouTube. Partners can always engage Ruckus Systems Engineers or Field Engineers with questions or assistance as needed.

System Settings

System configurations will vary from controller to controller but following these best practices will help establish a consistent support, administration, and user experience.

Firmware Recommendation

Category	Devices	Firmware	Rationale
SmartZone	Controller	smartzone-5-1-2-0-302	Best visibility
Cloud	Controller	5.2.0	maintained by Ruckus directly
ZoneDirector	Controller	zd1200-10-2-1-0-183	strongly recommend upgrading to SmartZone or Cloud in your next refresh cycle

TABLE 1: FIRMWARE RECOMMENDATION

General Settings

	Setting	Value	Rationale
Time	NTP Servers	primary: ntp.ruckuswireless.com secondary: pool.ntp.org Secondary should be set to Local NTP server	Imperative to connect controllers with NTP for reporting and analytics.
	Time Zone	Varies	Ensure the proper time zone and correct time for that zone are chosen where the server physically exists
	NTP Primary Server Auth	None	
	NTP Backup Server Auth	None	
Syslog	Logging	Enabled	The full scope and detail for each partner's syslog servers will vary, but CommScope strongly recommends enabling the full capabilities of a remote syslog servers
Cloud	Cloud SZ Services	disabled	
Northbound Data	Northbound Data Stream	enabled	For use with SCI or Analytics
	Create Profile:	Varies	Please consult your Ruckus engineering team for details
	Stream GPB Data by Domain/Zone	enabled	Applicable only to vSZ-H or SZ300 deployments. Restrict Northbound data streaming to the pertinent domains/zones in your controller.
WISPr	Northbound Portal Interface Support	Disabled	

SNMP	SNMP Notification Global	Enable	Allow SNMP v2/v3 Traps to be sent to Trap Host
SMTP	SMTP Server	Enabled (optional)	Settings will vary per partner. Recommend enabling for email notifications.
FTP	Create FTP Profile:	None/disabled	
SMS	Twilio SMS Server	Enabled (optional)	Settings will vary per partner. Recommend enabling for text/sms notifications. Additional costs will apply via Twilio account and usage.
Location Services	server:	None	limited use cases in Hosp

TABLE 2: GENERAL SETTINGS

AP Settings

	Setting	Value	Rationale
AP Registration	Create Rule:	varies	These settings will vary from zone to zone. Can be left disabled for more granular control.
Critical AP Tagging	Auto Tagging Critical APs	disabled	
Tunnel UDP Port	UDP Port	23233	Default
Country Code	Country Code	varies	Please ensure the correct country is set. This will change available radio options based on local country's regulations.
AP Number Allocation	AP Number Allocation	disabled	disable by default. helps track available licenses.
AP MAC OUI Validation	AP MAC OUI validation	disabled	Added layer of security for devices attempting to join controller

TABLE 3: AP SETTINGS

Switch Settings

	Setting	Value	Rationale
Registration	Create Rule:	varies	These settings will vary from zone to zone. Can be left disabled for more granular control.

TABLE 4: SWITCH SETTINGS

Cluster

Controller clustering is a unique technology to RUCKUS SmartZone (SZ) controller products. SmartZone controllers can be installed as an appliance (SZ144 or SZ300) or as a virtual machine (vSZ-Essentials or vSZ-High Scale) on supported hypervisors. In addition, SZ controllers can be installed in Amazon Web Service, Microsoft Azure and Google Compute Engine. Depending on the installation type, the table below highlights key configuration options to be considered during the initial installation process. For complete hardware requirements for scaling and clustering of virtual SZs, please reference to the Virtual SmartZone Getting Started Guide which is released with each major release of code.

SmartZone Type	Network Interfaces	Port Groups	IP Subnet Requirements	Rationale
SZ144	2	2	2	SZ144 should be configured with 2 Port Groups, one for Control, Management and Cluster. The second Port Group is for tunneling AP traffic
SZ300	4	0	Min 3, Max 4	SZ300 have four physical interfaces. Control, Management, Cluster and Data Plane. Control and Data Plane can be grouped into the same subnet. All others must be in separate subnets.
vSZ-H	3	0	Min 3	VSZ-H can be configured with a single interface for Control, Management and Clustering. However, for security reasons all three interfaces should be placed in separate subnets. AWS only supports a single interface. If tunneling is required, vSZ-H platforms require a vSZ-D (SZ Data Plane) in order to terminate tunnels.
vSZ-E	1	1	1	If tunneling is required, vSZ-E platform requires a vSZ-D (SZ Data Plane) in order to terminate tunnels so a second Port Group is not required.

TABLE 5: CLUSTERS

Maps

Maps are hugely beneficial when remotely troubleshooting a network. Please add accurate scaled floorplans and properly place access points for best results.

Certificates

The default Ruckus certificates will enable and allow all functionality. For individual sites, the defaults will suffice. For a hosted SZ or vSZ serving multiple sites, we recommend installing and maintaining a fully qualified domain name (FQDN) as well as corresponding certificates. Please refer to the Certificates guidelines available on the Ruckus support website for additional configuration options that are outside the scope of this document.

Templates

Templates are available to ensure Zone, AP, and WLAN configuration remain consistent. Create a template for your zones based on the Zone section below and improve staging times while decreasing potential misconfiguration errors. Templates can be exported and imported between controllers, allowing for easier administration. For additional information, refer to the Configuring Templates section in the SmartZone Administrator's Guide.

Naming Conventions

Creating and standardizing on specific naming conventions are key to all SmartZone installations. Naming conventions not only allow for easy to understand Domain/Subdomain, Zone, AP Group, WLAN Group, Switch Group and Switch Subgroups structures, but assist in identification of trouble areas within the SZ installation for troubleshooting. Following these naming conventions will ensure consistent user experience and accurate support.

Naming conventions are needed to enable brand-wide and ownership-group-wide views of the performance and metrics related to properties. The brand standards may specify specific naming conventions related to SSIDs and hostnames, but many internal fields are left unspecified, e.g. Zone names and AP Groups. Consequently, many partners have their own naming conventions or leave them unspecified.

Controller Configuration Hierarchy

Ruckus controllers have a similar, but slightly different, naming hierarchy depending on the type of controller in use. SmartZone OS offers the most robust, and flexible, grouping mechanism. The vSZ-H, being intended for high-scale deployments has built-in multi-tenancy with the concept of domains and sub-domains, enabling managed service providers to offer fully isolated environments for their tenants to operate within on a single vSZ-H cluster .

The SmartZone hierarchy looks as follows:

Access points: Controller > System > Domain > Sub-domain > Zone > AP group > AP

Switches: Controller> System> Domain> Sub-domain > Switch Group> Switch Sub-group > Switch

- Controllers – are used when a controller comprises multiple nodes for scale and/or redundancy
- System - Highest order that comprises multiple domains and zones
- Domains - Broad classification that represents an administrative domain comprising multiple Zones
- Sub-Domains – sub-groups within an administrative domain
- Zones - Comprise multiple AP groups, this is the finest granularity for upgrades
- Switch Groups – function like Zones but for Ruckus ICX switches
- AP Groups – aggregate APs by area with similar configuration requirements
- Switch Sub-group – the functional equivalent of AP Groups, representing groups of switches within a property

Note: SmartZone144 and vSZ-E, being intended for enterprise deployments, do not employ the Domain and Sub-Domain constructs.

Configuration Hierarchy Naming Recommendations

Domain / Sub-Domain

For Managed Service Providers (MSPs) that maintain networks across different brands utilizing a centrally hosted vSmartZone-H, we suggest:

- Domain should denote the brand
- Sub-Domains, if utilized, align to brand area IT management

Zones

- Zones to Denote Properties
- Zones below the brand domain should reflect the unique property ID, a delimiter, followed by the full name of the property. For example: <XXXXX> - <20-character text name of property>
- where XXXXX is the brand's hotel identification code and the 20-character text name of the property is the commonly known name

AP Groups

Zone configuration parameters are meant to be used as blanket default settings for property wide configurations based on the information in this document. AP Groups should be used to override AP specific parameters at a more granular level. For example, indicating where on a property an AP, or group of APs, reside and share common configuration values. We recommend AP Group names be used consistently across properties:

- Administration
- Basement
- Back_of_House
- Ballroom Ballroom - <name>
- Salon <a>
- Business Center
- Conference Space
- Conference Room_<n>
- Lobby
- Restaurant
- Outdoor Common
- Casino
- Fitness Area
- Guest Hallway

- Guest Rooms Guest Rooms - Floor _<n> Guest Rooms - Lobby
- Meeting Room
- Public Space
- Pool
- Restaurant
- Spa
- Valet

Switch Groups

Switch Groups should be named the same as the Zone name that matches the property the Switch Group is aligned to. For example, <XXXXX>-<20-character text name of property>, where XXXXX is the brand's hotel identification code and the 20-character text name of the property is the commonly known name

__ or __

<XXXXX>-<20-character text name of property> | <Partner Property ID>, where XXXXX is the brand's hotel identification code, the 20-character text name of the property is the commonly known name, and the Partner Property ID is the unique identifier assigned by the partner

Switch Subgroups

Switch Subgroups provide the same function as AP Groups denoting APs in a common location with a common set of configuration requirements. In this case, the switches already enjoy a naming convention as dictated by brands:

"Hotel Identity Code"+"Device_Code"+"Device_Sequence_Number"-"Floor_Number"_"Room_Number"

Therefore, the Switch Subgroup should be denoted as:

<Hotel Identity Code>-<Floor_Number>_<Room Number>

Zone Configuration

These settings are the first in the pecking order and thus set the baseline. These settings can and should be overridden at more granular levels further down the line, such as AP Groups, WLAN Groups, and/or individual AP and WLAN settings.

Access Points > Zone	Setting	Value	Rationale
General Options	Country Code	varies	Choose correct country where AP's within group physically exist.
	AP Admin Login	custom	Choose a unique ap-admin and password
	admin Password	custom	
	DP Zone Affinity	varies	disabled if you do not plan to tunnel traffic
Mesh Options	Mesh	Disabled	
Radio Options	2.4Ghz Channel Range	1,6,11	
	DFS Channels	Allow	DFS should be allowed barring any nearby RADAR interference in the area.
	Channel 144	Enabled	
	5Ghz Channel Range (indoor)	All checked	
	5Ghz Channel Range (outdoor)	All checked*	A site survey can help determine any congested channels from nearby interference sources that may lead to disabling certain channels as needed
	Channelization	Auto	
	Channel	Auto	
	Auto Cell Sizing	Disabled	Requires 5.2.1 code unless custom AP_CLI scripts are created and utilized.
	Tx power	Full	N/A when Auto Cell Size enabled
AP GRE Tunnel		defaults	
Syslog		Off	
AP SNMP		Off	
AP Model Specific		defaults	More granular settings should be further defined in AP groups instead of the entire Zone
Cellular		defaults	Specific to M510
Advanced	Auto Channel Selection	enabled, Background Scanning for both 2.5/5 GHz	
	Background Scan	enabled, Background Scan and set scan interval	

		for 2.4/5HGz to 30 sec	
	Bonjour Fencing	disabled	
	Smart Monitoring	Disabled	
	AP ping latency interval	Enabled	
	Rouge AP Detection	Enabled	
	Rogue Protection:	DISABLED	Detection is great, but mitigation is potentially illegal depending on jurisdictions or regional restrictions
	Band Balancing	Proactive, 10%	Drive majority of clients onto the 5Ghz spectrum.
	Recovery SSID	Disabled	
	Directed Multicast	Enabled (Wired, Wireless, and Network)	
	Health Check Sites	Disabled	
	AP Reboot	Enabled, Gateway and Controller 24 hours	

TABLE 6: ZONE CONFIGURATION

WLAN Configuration

WLANs have different characteristics depending on their use for High Speed Internet Access (HSIA) or Back-of-House applications (BoH) and location or density requirements.

WLAN	Application	Model
Guest	HSIA	Coverage
Conference	HSIA	Density
Public	HSIA	Density
BOH-1	BoH	Coverage
BOH-2	BoH	Coverage

TABLE 7 - WLAN CONFIGURATION

Wireless Settings

The following table identifies a set of standard WLAN parameters impacting client performance and behavior and the appropriate configuration settings. Specific SSIDs will be unique to individual brand properties.

WLAN	Guest	Conference	Public	BOH-1	BOH-2
Auth Type	Standard	Standard	Standard	Standard	Standard
Auth method	Open	open	open	802.1x EAP	MAC/eDPSK
Encryption Method	None	None	None	WPA2	None/DPSK
802.11r	Disabled	Disabled	Disabled	Disabled	Disabled
802.11w	Disabled	Disabled	Disabled	Disabled	Disabled
Dynamic PSK	Disabled	Disabled	Disabled	Disabled	Enabled(optional)
Tunnel Traffic	Disabled	Disabled	Disabled	Disabled	Disabled
Accounting Service	Disabled	Disabled	Disabled	Disabled	Disabled
Client isolation	Enabled	Enabled	Enabled	Enabled	Enabled
Application visibility	Enabled	Enabled	Enabled	Enabled	Enabled
Wi-Fi Calling	Enabled	Enabled	Enabled	Enabled	Enabled
Client Fingerprinting	Enabled	Enabled	Enabled	Enabled	Enabled
Hide SSID	No	No	No	Yes	Yes
client load balance	Disabled	Enabled	Enabled	Disabled	Disabled
MAX clients	100	250	200	100	100
802.11d	Enabled	Enabled	Enabled	Enabled	Enabled
802.11k	Enabled	Enabled	Enabled	Enabled	Enabled
Inactivity timeout	600s	300s	300s	600s	600s
OFDM-only	Enabled	Enabled	Enabled	Enabled	Enabled
BSS MinRate	12Mbps	12Mbps	12Mbps	12Mbps	12Mbps
MGMT TX rate	12Mbps	12Mbps	12Mbps	12Mbps	12Mbps
Band Balancing	Enabled	Enabled	Enabled	Enabled	Enabled
Airtime Decongestion**	off	on	on	off	off
Transient Client Management**	off	off	off	off	off

** SmartZone feature

TABLE 8 – RUCKUS CONTROLLER WLAN CONFIGURATION PARAMETERS

Wi-Fi Calling

Wi-Fi calling is a feature especially helpful in the Hospitality environment where location or construction material of a property may limit cellular coverage inside a particular property. In the past, a typical deployment used best effort Wi-Fi calling where any type of prioritization was enabled on the client device only. Potential problems arise when the client device switches from Wi-Fi to LTE or back because the network/wireless settings did not prioritize the Wi-Fi call's traffic. This, in turn, would cause the call to drop. Wi-Fi Calling allows a set of calling profiles to be loaded onto a WLAN specific to any specific carrier or multiple carriers. A Wi-Fi Calling profile that has been created and deployed contains the FQDN of the carrier or carriers ePDG (evolved Packet Data Gateway). The main function of the ePDG is to secure the data transmission with a UE (client device) connected to the EPC over untrusted non-3GPP access, such as a hotel's wired and wireless network. For this purpose, the ePDG acts as a termination node of IPsec tunnels established with the UE.

Below are the basic steps that happen to a client when Wi-Fi calling has been abled on a WLAN.

- A client associated to the WLAN with the Wi-Fi Calling profile is enabled and initiates a call over Wi-Fi.
- Ruckus SmartZone QOS features identify this as a Wi-Fi call and can sense the carrier requested based on the Wi-Fi Calling Profile associated with the WLAN.
- The client establishes an IPSec tunnel to the ePDG.
- The clients voice traffic is placed in the Voice queue of the AP where the client is associated.

Setting up Wi-Fi Calling on SmartZone

- Create Wi-Fi Calling Profile under Service and Profiles > Wi-Fi Calling> Profile
- Please refer to the Wi-Fi Calling Deployment Guide for FQDNs of various carrier's ePDGs: https://support.ruckuswireless.com/documents/2832-ruckus-wi-fi-calling-deployment-guide
- Add Wi-Fi Calling Profiles under Wireless LANs> "Select WLAN" > Wi-Fi Calling> Select appropriate profiles for the Carriers.

DPSK

Dynamic Pre-Shared Key (DPSK) is a patented technology that can provide robust, secure wireless access with a specific key for each network connected device, including devices that only accept PSK-level security. Dynamic PSK creates a unique encryption key (up to 63 bytes) for each device accessing a PSK WLAN. With Ruckus SmartZone DPSK, devices that do not support 802.1X and certificates can still be uniquely registered and tracked on the network with a record of the registering owner. Additionally, in situations where a full certificate PKI is not desirable, DPSK can be used with all WLAN connected devices.

Ruckus Legacy DPSK creates dynamic pre-shared keys on the Ruckus SmartZone WLAN controller. The WLAN controller creates a unique 63-byte encryption key for each user upon accessing the wireless LAN for the first time and then automatically configures end devices with the requisite wireless settings, such as SSID and unique passphrase, without manual intervention.

Recently, Ruckus has introduced eDPSK, which is one of several encryption methods you can use with Cloudpath. The eDPSKs are generated by Cloudpath as opposed to being generated by a controller (thus, they are "external" to the controller). An advantage to using external DPSKs with Cloudpath encryption as opposed to legacy (internal) DPSKs is that the Cloudpath administrator has better control over the use of DPSKs.

Benefits of Cloudpath External DPSK (eDPSK):

- Increase scale of total DPSKs supported to potentially tens of thousands
- Roaming support across multiple zones and SmartZone controllers
- Policy-based access via RADISU VSAs
- API support to integrate external platforms
- Support for headless devices
- Out-of-band passphrase distribution (email/SMS)
- User association across 802.1X and DPSK devices
- Can co-exist with any workflow supported
- Benefits of Radius authentication without the complexity for end users

Please refer to the Cloudpath External DPSK and SmartZone DPSK Deployment Guides.

WLAN Parameter Rationale

These setting recommendations are based on both theoretical and empirical information regarding the expected or possible client performance and behavior with specific settings values as noted below.

Device Interoperability

The HSIA is subject to any device made possibly coming through the doors. Back-of-house applications often use older technology devices. Hospitality properties are challenged by the possible presence of legacy devices which may not support the latest standards and technologies. Due to this, the configuration specifications err on the side of maximizing client device interoperability. These include:

Technology	Setting	Rationale
802.11k (RRM)	Varies	Speeds up client's radio searching for viable roaming targets. Disabled for admin spaces and enabled for guest/public/conf.
802.11w	Disabled	802.11w helps prevent some forms of DoS by encrypting 802.11 management frames. Unfortunately, not all clients support this and for client interoperability this is recommended to be disabled for all WLANs.
Hidden SSID	Varies	Broadcast SSID for all guest/public/conf. Hidden non-broadcast SSID for all admin groups.
802.11d	Enabled	Enabled to allow devices to determine the regulatory domain and remain compliant

TABLE 9: DEVICE INTEROPERABILITY

Device Security

Network security is a key area of concern for any enterprise deployment and the following configurations settings represent best practices for Hospitality deployments:

Technology	Setting	Rationale
Authentication Method	Varies	Open for HSIA but with as secure an authentication methodology as is supported by the devices for BoH.
Encryption	Varies	Enabled for BoH. Protocol determined by individual hotel or brand standards
802.11r	Disabled	802.11r provides for improved roaming performance for latency sensitive secure networks (WPA2). Fast BSS Transitions are still a concern for clients. For all HSIA WLANs this should be disabled. For voice roaming in BoH applications this can be enabled.
Client Isolation	Enabled FoH, Disabled BoH	Table stakes for HSIA this feature prevents clients from communicating with other clients on the same WLAN allowing only traffic to go to the upstream gateway.
Application visibility	Enabled	On for non-remediation and future monetization provides additional information for SCI and Ruckus Analytics.
Client fingerprinting	Enabled	Provides greater insight into the client install base and provides additional information for SCI and Ruckus Analytics.

TABLE 10: DEVICE SECURITY

System Performance

Many features can be tuned to impact performance vs coverage in various deployment models. Some are geared primarily towards high density environments, but some are applicable to all areas of a deployment:

Technology	Setting	Rationale
Tunnel traffic	Disabled	Tunneling can increase overhead on the AP if not needed for roaming
Hide SSID	Disabled FoH, Enabled BoH	Network visibility is critical for HSIA clients
Client Load Balance	Enabled Conf/Public	Improves the distribution of new wireless clients across APs
MAX clients	Varies	Allows you to cap the number of clients per radio on an AP to tune spectrum utilization to the APs capabilities. In guest areas, the default value of 100 is fine. For public spaces, this needs to be increased to 200.
OFDM-Only	Enabled	Exclude legacy 802.11b clients from joining the network to improve usable Airtime for the majority of clients
BSS MinRate	12Mbps	Sets the minimum transmission rates for the BSS to a higher value than default values to reduce cell size, improve broadcast/multicast transmit speeds and encourage clients to roam to a nearer AP
MGMT TX rate	12Mbps	This can be impacted by the BSS MinRate as well. It sets the minimum data rate used for 802.11 management traffic to a higher than default value to reduce management overhead
Band Balance	Enabled	Attempts to balance the client load on radios by distributing clients between the 2.4 GHz and 5 GHz radios, specifically favoring 5Ghz
Airtime Decongestion	Enabled Conf/Public	Limits management frame exchanges between APs and clients in ultra-high dense environments
Transient Client Management	Disabled	Delays associations of Ruckus AP's with transient clients (devices that are in the AP's coverage area for a short time) using statistical methods

TABLE 11: SYSTEM PERFORMANCE

Access Points

AP Configuration

The following settings affect spectral utilization and access point behavior and are configured on a per-radio basis though some parameters can be overridden at the WLAN level. Configuration at the AP radio level is important to tune the radio performance to the space and density requirements while WLANs are typically universally configured across all or most radios. The use of AP Zones within the Ruckus Networks WLAN controller enables an easy way of configuring groups of access points with common characteristics.

Each column in the below table represents AP Groups which could even be further divided into more granular AP groupings as needed. Please refer to the Naming Conventions Section for additional details on more specific groups that could be utilized.

Access Point Settings	Guest Rooms	Conference	Public Space	Back of House
AP IP Mode	IPv4 only	IPv4 only	IPv4 only	IPv4 only
ChannelFly	Disabled	Disabled	Disabled	Disabled
DFS Channels	allow	allow	allow	allow
2.4Ghz Channelization	20MHz	20MHz	20MHz	20MHz
5Ghz Channelization *	20MHz	20MHz	20MHz	20MHz
Channel	auto	auto	auto	auto
Auto Cell Size**	Disabled	Disabled	Disabled	Disabled
Auto Channel Selection	background	background	background	background
Background Scan on 2.4Ghz	30s	30s	30s	30s
Background Scan on 5Ghz	30s	30s	30s	30s
Smart Monitor	Disabled	Disabled	Disabled	Disabled
Rogue AP Detection	On	On	On	On
Protect from Rogue APs	Off	Off	Off	Off
Client Load Balance on 2.4Ghz	Disabled	Enabled	Enabled	Disabled
Client Load Balance on 5Ghz	Disabled	Enabled	Enabled	Disabled
Band Balancing	Enabled	Enabled	Enabled	Enabled

* If DFS enabled, conference space 40Mhz channels could be utilized, depending on spectrum analysis

** SmartZone feature, disabled until 5.2.1

TABLE 12 – RUCKUS CONTROLLER AP CONFIGURATION PARAMETERS

Note: A key takeaway is that access points should NOT be left in the default group. The Default AP group should be treated as a “staging area” only.

AP Parameter Rationale

These setting recommendations are based on both theoretical and empirical information regarding the expected or possible client performance and behavior with specific settings values as noted below:

Setting	Rationale
AP IP Mode	Access Points and WLAN controllers typically reside on a management-only subnet in the private IP address space. Only IPv4 is required.
ChannelFly	Assesses all available channels to measure capacity improvement each one can provide before it directs the AP to switch channels. Compared to Background Scanning, ChannelFly takes considerably longer for the network to settle down. If you have clients that do not support the 802.11h standard, ChannelFly may cause significant connectivity issues during the initial capacity assessment stage.
DFS Channels	Enabling DFS channels can dramatically increase available capacity for the network
2.4Ghz Channelization	The use of 20Mhz channels maximizes the number of channels available
5Ghz Channelization	The use of 20Mhz channels maximizes the number of channels available
Channel	Channels are assigned automatically using either background scanning or ChannelFly
Auto Cell Size**	uses AP to AP communication to share information on the degree of interference seen by each other. Based on this information, the APs dynamically adjust their radio Tx power and Rx parameters (or cell size) to mitigate interference. Enabling the Auto Cell Sizing option, disables the TX Power Adjustment configuration.
Auto Channel Selection	Use background scanning for the channel selection
Background Scan on 2.4Ghz	Background scanning must be on for rogue AP detection. Reducing the scan interval minimizes impact to clients.
Background Scan on 5Ghz	Background scanning must be on for rogue AP detection. Reducing the scan interval minimizes impact to clients.
Smart Monitor	The AP checks for the upstream gateway and disables the WLAN when the IP gateway is unavailable.
Rogue AP Detection	Disabled to avoid multitude of false positives, especially in densely populated cities.
Protect from Rogue APs	Disabled to avoid impacting neighboring networks
Client Load Balance on 2.4Ghz	Disabled in the guest rooms where the RF design is primarily for coverage. Enabled in public areas with high density to improve performance. This has implications on the AP Zone architecture in the controller.
Client Load Balance on 5Ghz	Disabled in the guest rooms where the RF design is primarily for coverage. Enabled in public areas with high density to improve performance. This has implications on the AP Zone architecture in the controller.
Band Balancing	Band balancing is now incorporating elements of 802.11v to inform and guide the client. However, the RF design must support this and it is primarily useful in high density areas with adequate 5Ghz coverage and signal strength. Use of 802.11v is still subject to client implementations and adherence while manipulation of the 802.11 management frames to guide clients can result in

	higher latency when associating with the network and incomplete information regarding a client's capabilities due to erratic scan behavior or random MACs. Alternative approach is to use no automatic band balancing and name SSIDs to socially engineer the solution, or a combination of both.

TABLE 13: AP PARAMETER RATIONALE

Switches

Key Point: Do NOT leave switches in the default staging group. In fact, you should disable/block as many settings as possible in the default groups just in case devices end up in there temporarily, so they will not cause undesired results in your networks.

Refer to the Hospitality Switching Configuration Best Practices for full detail.

Events and Alarms

The default settings provided with the SmartZone installation will suite most of the requirements for a standard network installation, however, further tweaking these settings will provide more pertinent information to a hospitality focused network. If you choose to enable SNMP Traps, Syslog messages and/or email messages make sure you enable and configure the server information on each of the desired protocols.

Refer to the SmartZone Alarms and Events Reference Guide for more detailed information on specific alarms and events.

Events and Alarms >	Setting	Value	Rationale
Events	Filter	All Fields Enabled	Best visibility
Event Management	SMTP	Off/On	If email messages are desired be sure to enable the SMTP email server in System > General Settings to enable email notifications. Refer to the Event specific table under Events and Alarms> Event Management to view all events and their individual configurations. Currently, no events are set to send SMTP notifications. All desired events will require SMTP to be enabled on each event separately.
	SNMP	Off/On	If SNMP traps are desired be sure to enable the SNMP v2/v3 server in System > General Settings to enable SNMP traps. Refer to the Event specific table under Events and Alarms> Event Management to view all events and their individual configurations. Ruckus has enabled a standard set of events to send SNMP traps on if SNMP is enabled.
	Syslog	Off/On	Configure syslog parameters based on your syslog server environment Refer to the Event specific table under Events and Alarms> Event Management to view all events and their individual configurations. All

			events will be sent to the syslog server if enabled. All Log facility and Event Severity configurations are done under System> General> Syslog
Switch Custom Events	Events:	Varied	Defaults will suffice

TABLE 14: EVENTS AND ALARMS

The table below provides some additional guidance on additional events that should be considered depending on the specific network deployment.

Code	Severity	Category	Type	Notes	Description
859	Critical	Cluster	NTP server reach failed		This event occurs when system cannot reach NTP server.
827	Informational	Cluster	NTP time synchronized	Clears SNMP event 859	This event occurs when the date and time settings of a node synchronizes with the NTP server.
2000	Critical	Switch	Switch Critical Message	When SZ is managing ICX switches only.	This event occurs when there is a Switch Critical Message
951	Critical	Threshold	Memory threshold exceeded		This event occurs when the memory usage exceeds the threshold limit.
954	Informational	Threshold	Memory threshold back to normal	Clears SNMP event 951	This event occurs when the memory usage gets back to normal.
950	Critical	Threshold	CPU threshold exceeded		This event occurs when the CPU usage exceeds the threshold limit.
953	Informational	Threshold	CPU threshold back to normal	Clears SNMP event 950	
952	Critical	Threshold	Disk usage threshold exceeded		This event occurs when the disk usage exceeds the threshold limit.
955	Informational	Threshold	Disk threshold back to normal	Clears SNMP event 952	This event occurs when the disk usage gets back to normal.
751	Major	System	Syslog Server Unreachable		This event occurs when syslog server is unreachable
750	Informational	System	Syslog server reachable	Clears SNMP event 751	This event occurs when syslog server is reachable.

902	Major	IPMI	ipmiThempBB	SZ144/SZ300 Only	This event occurs when the baseboard temperature status on the control plane is sent.
927	Informational	IPMI	ipmiThempBB	Clears SNMP event 902	This event occurs when the baseboard temperature status recovers from abnormal conditions.
907	Major	IPMI	ipmiThempP	SZ144/SZ300 Only	This event occurs when the processor temperature status on the control plane is sent.
932	Informational	IPMI	ipmiThempP	Clears SNMP event 907	This event occurs when the processor temperature status recovers from abnormal conditions
909	Major	IPMI	ipmiFan	SZ144/SZ300 Only	This event occurs when the system fan module status on the control plane is sent.
934	Informational	IPMI	ipmiFan	Clears SNMP event 909	This event occurs when the system fan module status recovered from abnormal condition.
912	Major	IPMI	ipmiFanStatus	SZ144/SZ300 Only	This event occurs when the fan module status on the control plane is sent.
937	Informational	IPMI	ipmiFanStatus		This event occurs when the fan module status recovered from abnormal condition.
1255	Major	License	License		This event occurs when a license is going to expire
1256	Major	License	License		This event occurs when some connected APs were rejected due to insufficient license capacity.
1280	Major	AP State Change	AP number limit exceeded		This event occurs when an approved AP were rejected dues to exceeding of AP number limit.
1289	Major	License	Insufficient license capacity	When SZ is managing ICX switches only.	This event occurs when some connected switches were rejected due to insufficient license capacity.

1601	Major	Authentication	Authentication server not reachable	Only when Radius is being used for authentication	This event occurs when authentication fails since the primary or secondary servers is not reachable
1602	Major	Accounting	Accounting server not reachable	Only when Radius is being used for accounting	This event occurs when the primary or secondary servers are not reachable.
21000	Major	Switch	Switch Offline	When SZ is managing ICX switches only.	SwitchOffline
4002	Warning	SCI_Service	Disconnect to SCI	Only when using SCI	This event occurs when SZ disconnected to SCI.
4001	Informational	SCI_Service	Connect to SCI	Clears SNMP event 4002	This event occurs when SZ connected to SCI.

TABLE 15: ADDITIONAL EVENTS

Ruckus solutions are part of CommScope's comprehensive portfolio for Enterprise environments (indoor and outdoor).

We encourage you to visit **commscope.com** to learn more about:

- Ruckus Wi-Fi Access Points
- Ruckus ICX switches
- SYSTIMAX and NETCONNECT: Structured cabling solutions (copper and fiber)
- imVision: Automated Infrastructure Management
- Era and OneCell in-building cellular solutions
- Our extensive experience about supporting PoE and IoT

COMMSCOPE®

RUCKUS®

commscope.com

Visit our website or contact your local CommScope representative for more information.