COMMSCOPE®

RUCKUS®

# Configuration Guide

Analytics for Hospitality

May 2021

# Table of Contents

# Intended Audience

This document explores the need for naming conventions within the controller, access point, and switches when analytics are being used to yield insights into the performance of networks across a portfolio of properties in hospitality.

This document is written for and intended for use by technical engineers with some background in networking, 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 network (switches, access points and controller) for use with an analytics and reporting platform such as SmartCell Insight or Ruckus Analytics. This document is intended to provide guidance to Hospitality Managed Service Providers to ensure the ability to provide meaningful reporting and analytics of performance metrics collected from RUCKUS network infrastructures deployed across multiple properties.

This document is one in a series of Design and Configuration guides specific to Hospitality. This document is the fifth and final in this series created for the Hospitality market. Please reference the full suite of Design and Configuration Guides for Hospitality.

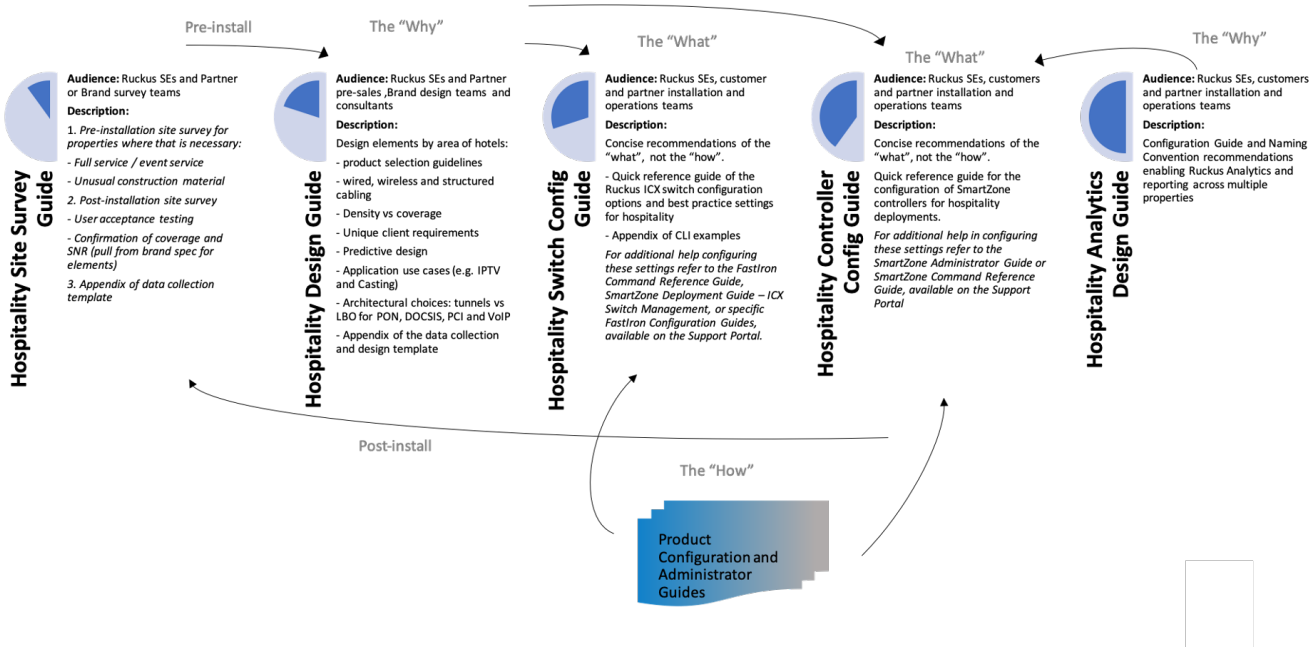



FIGURE 1: SUITE OF DESIGN AND CONFIGURATION GUIDES FOR HOSPITALITY

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.

# Ordering Analytics

CommScope has two Ruckus products for Analytics. SmartCell Insight is primarily a reporting tool with some machine learning algorithms and is sold as an on-premise or hosted solution with perpetual licensing. Customer reports can and have been built for brands and owners to provide meaningful insights into the performance of their hotel networks, their compliance with brand standards and the lifecycle of the assets.

All the functionality of SmartCell Insight has been subsumed into Ruckus Analytics which provides the above functionality as well as additional features such as AI-assisted troubleshooting, natural language queries, service level management and is the platform for on-going investment leading to self-healing networks.

Ruckus Analytics is sold as a subscription service based on the number of devices (access points and switches) to be monitored. When ordering either analytics platform, it is important to collect some basic information for the various stakeholders (owner, operators, brands and partners) to be granted visibility to the information about their property.

### Required Property Information

Property Information is necessary to correlate the property with the controller.

1. Property Name (As specified on your contract with the hotel or identified by the brand)
2. Property Address (Physical Address of Hotel)
3. Property Phone (Main hotel phone number)
4. Property Code (unique property identifier specified by the brand)
5. Brand (Marriott, Hilton, Hyatt etc.)
6. Sub-Brand (Courtyard, Residence Inn, etc.)
7. Management Company (Specified on your contract)
8. Owner/Investor/Franchise

### Contact Details

Contact details are important for making sure provisioning can proceed and to create access rights and credentials for users to view the data. Examples of the types of individuals you will need contact details for include:

1. Property IT
2. Managed Service Provider
3. Brand
4. Ownership Group
5. Consultant: Occasionally, consultants are employed by owners and brands on a project basis and may require access to the analytics platform.

### Controller Details

Finally, it is crucial to have correct controller information to configure the system for analytics.

1. Identify the correct **Controller Type:** ZoneDirector or SmartZone. ZoneDirectors are supported only in SmartCell Insight and are assumed to be **on the property.**
2. Confirm the **Controller Firmware Level** and **Controller URL**. The external IP address must be accurate as this will be used to whitelist the controller in any firewalls gating access to SmartCell Insight if SCI is located off the hotel property. This is not relevant if the controller is a SmartZone connecting to Ruckus Analytics.
3. SmartZones may be deployed on the property or centrally supporting **multiple properties**. Identify which deployment is being used for the SmartZone in question (on the property or multiple properties). This impacts the naming convention for the System ID in SmartCell Insight and has implications for the configuration of the SmartZone if:
    a. The SmartZone also has properties for which SCI or Ruckus Analytics is not purchased
    b. The partner is using the MQTT API of the SmartZone for their own portal
    c. Or Ruckus Diagnostics Dashboard (RDD) is in use

**Note:** If either b or c above are true (the partner is already using the Northbound Interface for their own software platform or RDD is in use) contact the Ruckus Support for additional information.

# Controller Recommendations

## Controller Type

In general, it is highly recommended that the partner use either an on-premise SmartZone (SZ100) or a centrally hosted vSmartZone. ZoneDirectors are approaching end-of-sale and do not support the IoT integrations or the more advanced features available in Ruckus Analytics or the same level of granularity in metrics as current versions of SmartZoneOS .

Mixed deployments with Ruckus ZoneDirectors and SmartZone are, by definition, only supported on the SmartCell Insight platform.

Mixed deployments with Ruckus SmartZones and Ruckus Cloud are outside the scope of this document, though many of the concepts conveyed here, particularly regarding naming conventions, are equally relevant with a Ruckus Cloud deployment. Contact Ruckus Support or a Ruckus System Engineer for more details.

## Controller Firmware

All ZoneDirectors must run the latest version of ZoneDirector software that supports the deployed APs. See Figure 7 – Controller Firmware Recommendations, below, for specific recommendations.

SmartZoneOS is currently recommended to run 5.2.2 unless a later version of firmware is required to support specific models of AP hardware.

| Platform | Firmware Release |
|---|---|
| ZoneDirector | ZD1200 10.2.1.0.183 (MR1 Refresh4) Software Release |
| SmartZone | SmartZone 5.2.2.0.317 (GD) Software Release (SZ-100) (.ximg image) |

TABLE 1: CONTROLLER FIRMWARE RECOMMENDATIONS

## Access Points Firmware

Access Points controlled by a ZoneDirector will be running the same level firmware as the controller. AP Zones on a SmartZone controller can run two long-term trains of code behind that of the controller but in general should be running the latest released firmware, matching the general release of the controller.

Where necessary to support deployments running older access point hardware, it is recommended to deploy those APs in a contiguous Zone to minimize roaming and to use the latest patch of 3.6.2 AP firmware.

| AP Zone | Firmware Release |
|---|---|
| N-2 AP Zone | SmartZone 3.6.2 (MR2) New AP Model Bundle for R730 (b509) |
| Current AP Zone | latest 5.2.2 release |

TABLE 2: AP ZONE FIRMWARE RECOMMENDATIONS

# Configuring Controllers for Analytics

## Configuring SmartZone

The following provides directions for configuring a SmartZone to connect to an analytics platform (SCI or Ruckus Analytics). There are multiple steps in verifying a configuration is appropriate for connecting and reporting data. Be sure to follow all steps using the checklist at the end of this section.

### Configuring Time Synchronization (NTP)

It is crucial for the timestamp of all reported metrics from the controllers be in sync amongst all properties. In this case all properties for a brand or owner, possibly across different servicing partners, must be in sync. If a controller sends data out of sync, that data will be dropped and lost.

To maintain data synchronization, you must ensure that NTP synchronization is happening properly. This is true for both SmartZones and ZoneDirectors.

On a SmartZone, navigate to System > General Settings and select the Time tab.

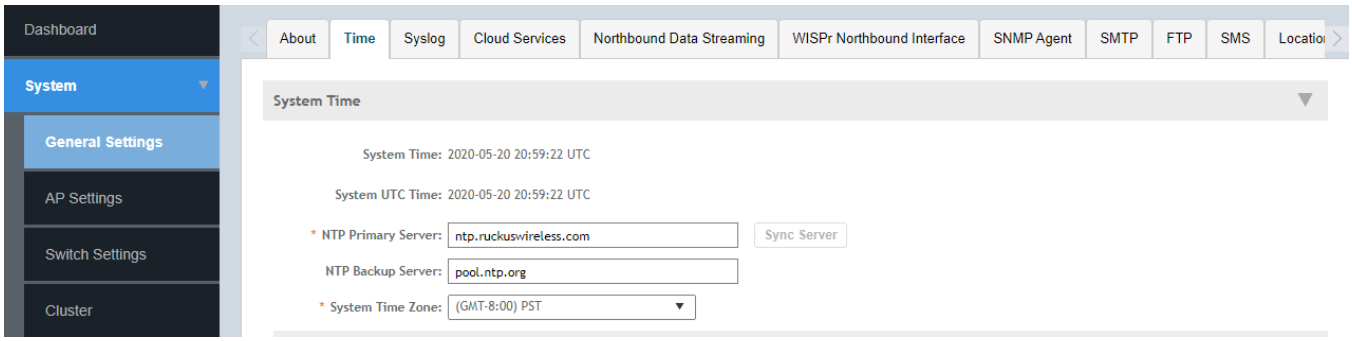



FIGURE 2: SMARTZONE NTP CONFIGURATION

Configure the Primary NTP server for ntp.ruckuswireless.com and the System Time Zone for the correct local time zone and click Apply.

if the controller is on-premises, and a secondary NTP source is available, it should be configured as the secondary NTP server (e.g., a local firewall that supports NTP services).

Ensure the local firewall does not block access to UDP port 123 and to monitor the controller for NTP issues via syslog and SNMP Alarms.

Note: If the controller is left in Coordinated Universal Time (UTC) but the time set at installation is the current local, data will be sent with the wrong timestamp and deleted. Put the controller into the local time zone and set current time equal to local time.

### On-boarding to SmartCell Insight (SCI)

Once the system is configured in SCI, a System ID is created that will be used to configure the controller.

On a SmartZone, navigate to System> General Settings> Northbound Data Streaming.

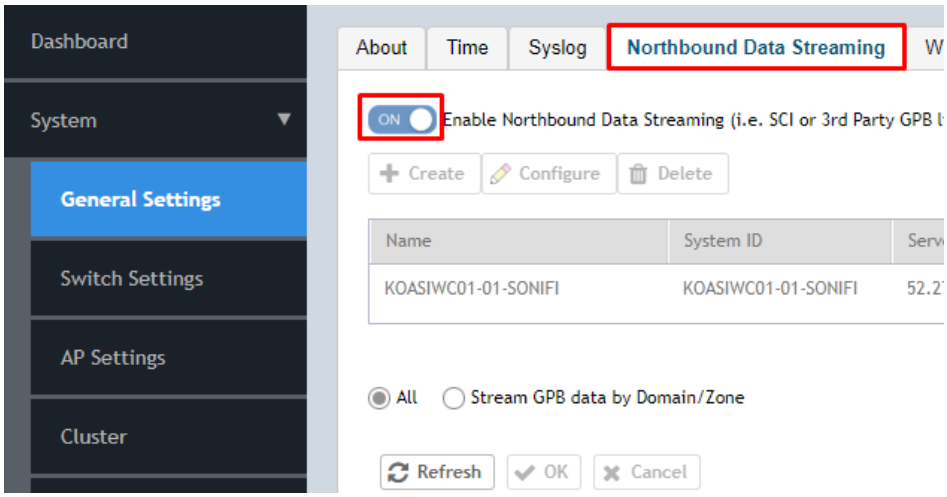



FIGURE 3: SMARTZONE NORTHBOUND DATA STREAMING

1. Enable Northbound Data Streaming
2. If you are running SmartZoneOS ≥ 5.1, you can also define which Domains and Zones will send data Northbound. If you have properties which purchased SCIaaS in addition to those that did not, place all properties that require SCI in their own Domain and only select that Domain for streaming, otherwise select "All"

**Note:** It is recommended that all properties (represented by Zones in SmartZoneOS) that belong to a specific brand be put in the same Domain. If a brand has some properties that require the use of SCI and others that do not, use another Domain to differentiate them.

3. Select "+Create" to create the Northbound Streaming Profile:

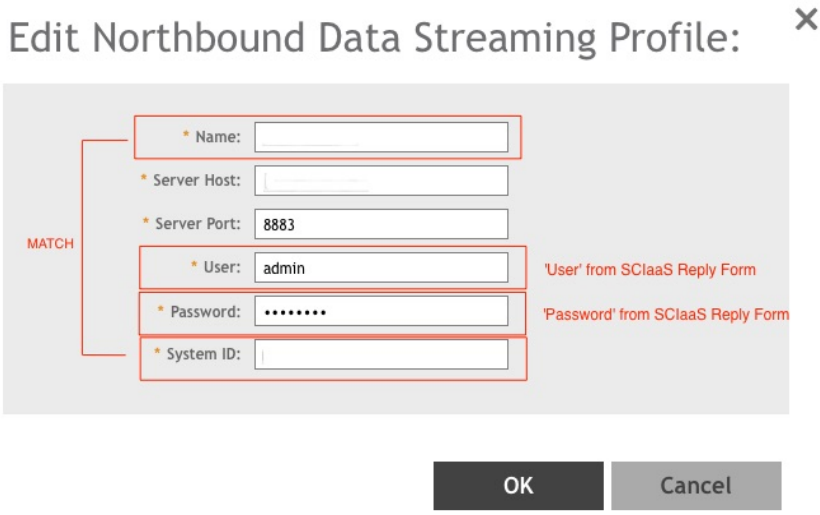



FIGURE 4: CONFIGURE NORTHBOUND INTERFACE DETAILS

**Note:** The System ID, User and Password **must match** the information configured in SCI in the System Settings.

1. Name is locally relevant and can be any value
2. Server Host: the IP address of SCI
3. User and Password
4. System ID must match what is in SCI

**Note:** SmartZoneOS 5.2 and greater allows you to specify which Data Types to forward in the Northbound Data Streaming Profile. Leave these at default with **all** selected.

## On-boarding to Ruckus Analytics

If on-boarding the controller to Ruckus Analytics instead of SmartCell Insight, simply enable Cloud Services on the SmartZone:

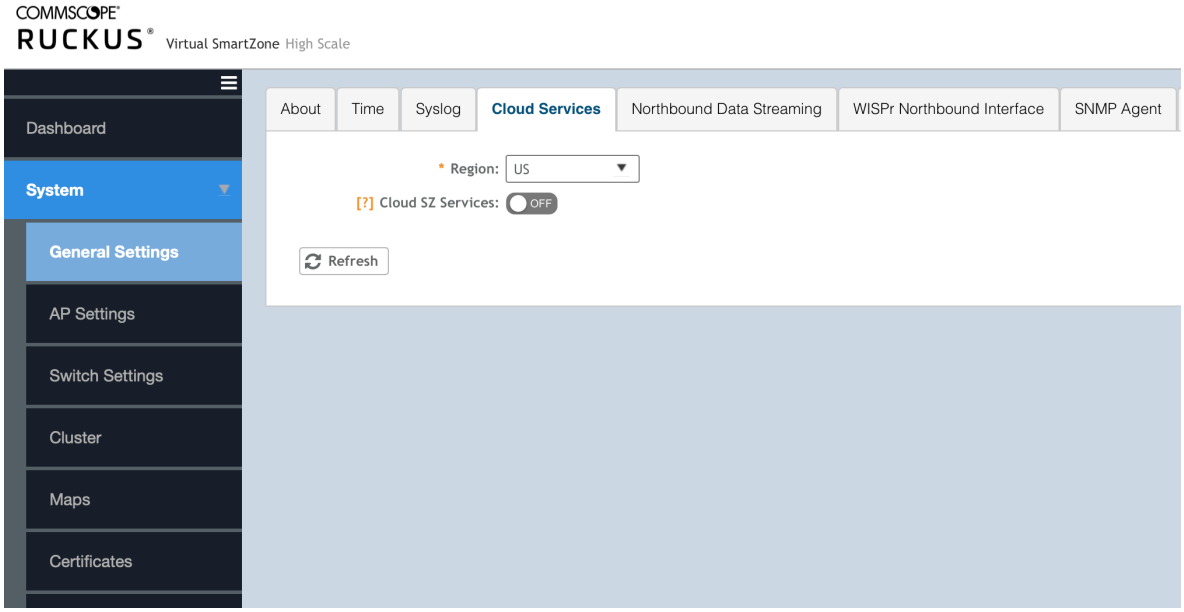



FIGURE 5: CONFIGURE CLOUD ANALYTICS

After sliding the button to the right for “Cloud SZ Services” you should get a Pop-Up screen for logging into Ruckus Analytics.

Enter the e-mail address and password of your support account with Ruckus Wireless. This could be the same e-mail address used to activate the license.

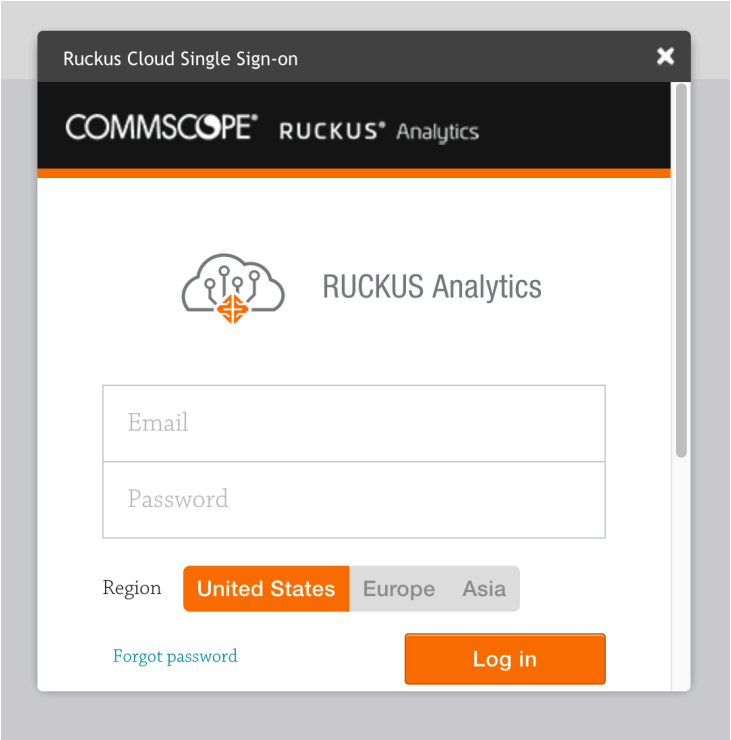



FIGURE 6: CONFIGURE CLOUD ANALYTICS

After successfully logging In, the system will display an image showing the Connection Status as “Connected”.

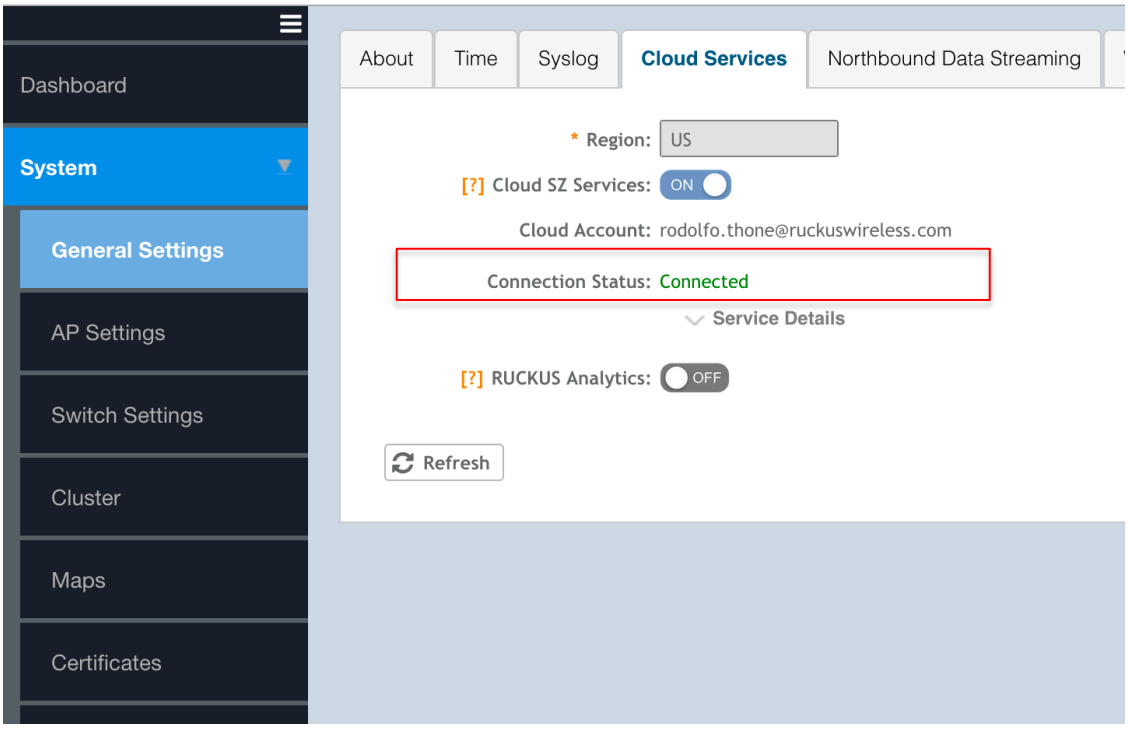



FIGURE 7: CONFIGURE CLOUD ANALYTICS

After validating your support account, enable Ruckus Analytics by clicking on the slider to move it to the right to the "ON" position.

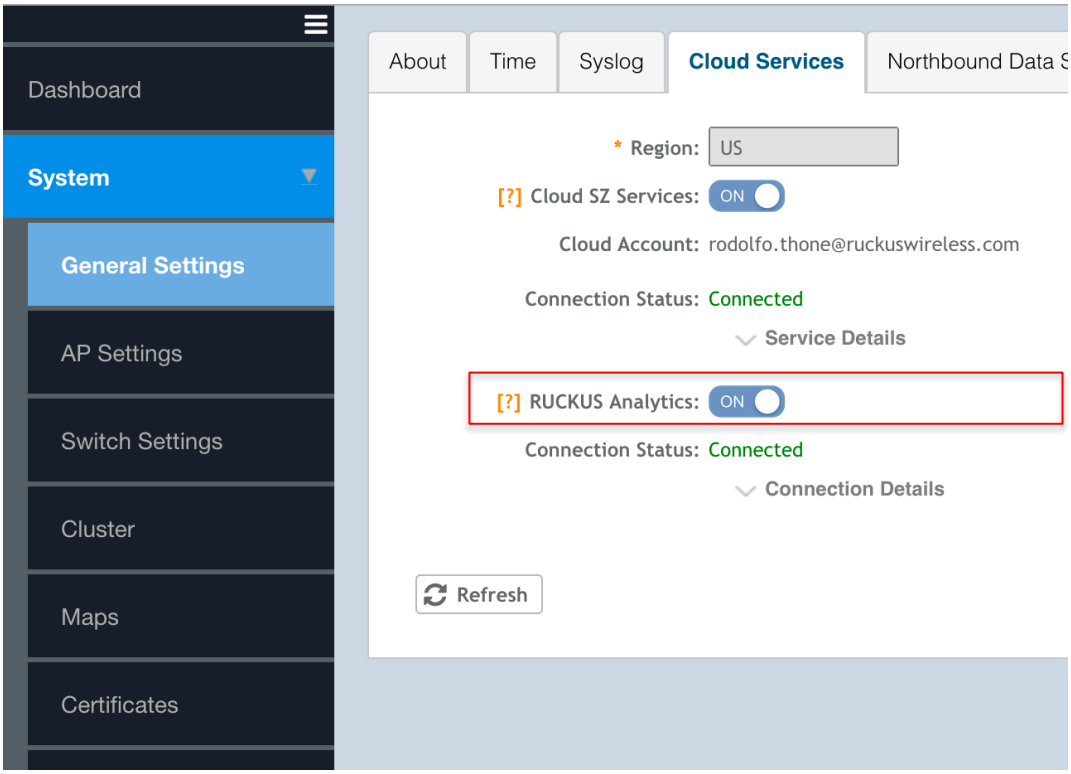



FIGURE 8: CONFIGURE CLOUD ANALYTICS

Successfully enabling Cloud Services will be reflected in the System Events under "Events & Alarms". See Figure 10 below:

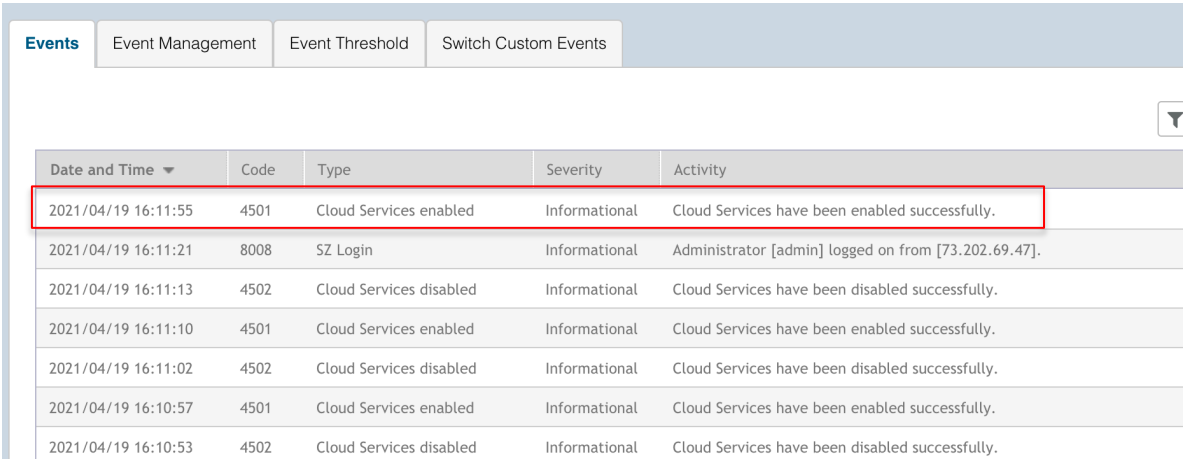



FIGURE 9: CONFIGURE CLOUD ANALYTICS

After the SmartZone is connected, check the Ruckus Analytics tab for “Onboarded Systems”. A green dot means the SmartZone has been successfully activated.

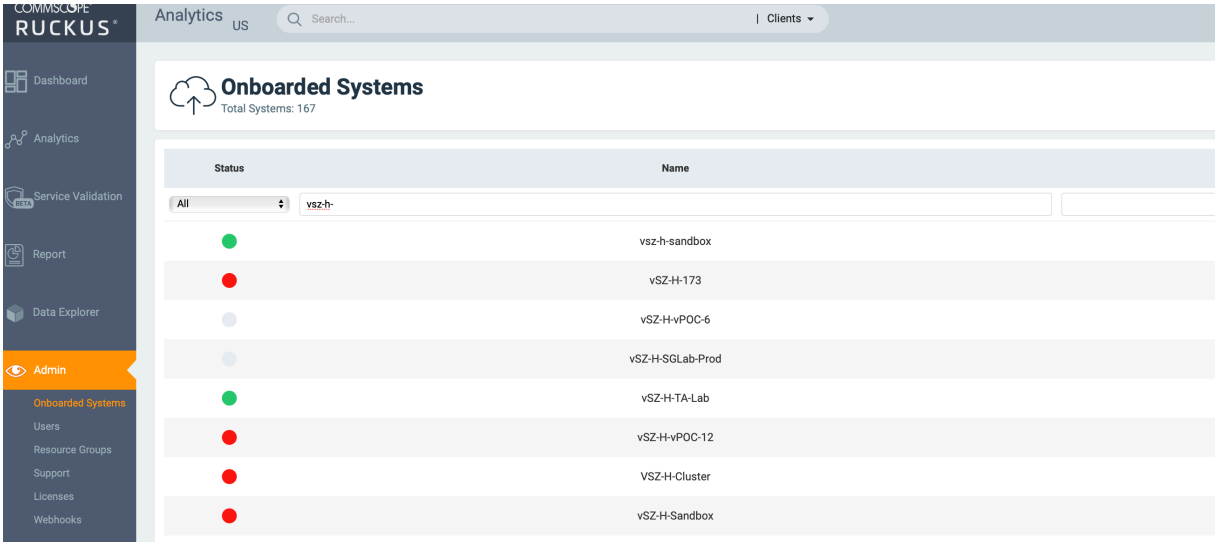



FIGURE 10: CONFIGURE CLOUD ANALYTICS

### Enabling Application Recognition and Client Fingerprinting

For client applications and device types to be available in the analytics platform of choie, Application Recognition and Client Fingerprinting must be enabled on the WLAN.

On **SmartZone**, navigate to Wireless LANs:

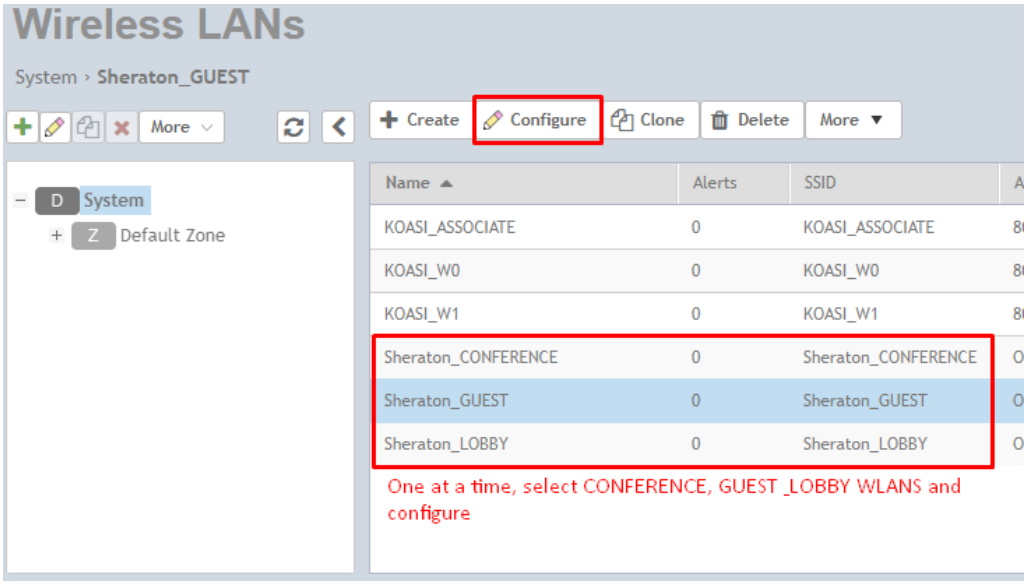



FIGURE 11: CONFIGURE WLANS

1. Select each WLAN one at a time
2. Enable Client Fingerprinting and Application Recognition & Control

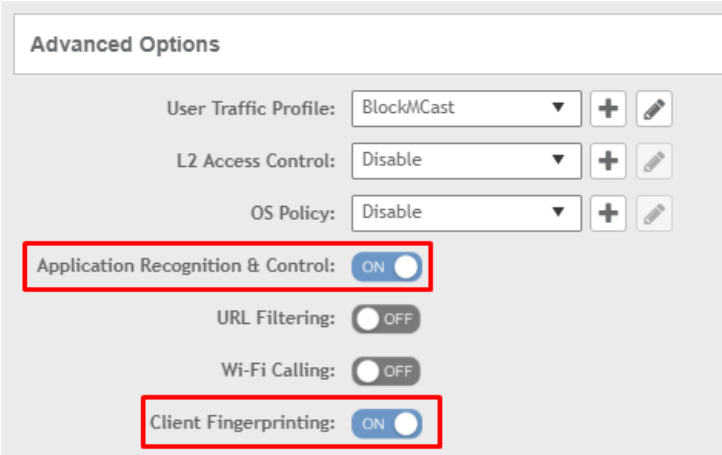



FIGURE 12: CLIENT FINGERPRINTING AND APPLICATION RECOGNITION

**Note:** In SmartZoneOS 5.2 Application Recognition and Control is under Firewall Options while Client Fingerprinting is under Advanced Options.

### Enabling Rogue AP Detection and AP Ping Latency

Information about the RF environment is made visible by enabling Rogue AP detection. This can be safely enabled at the Zone level with **no** impact on clients. Unless explicitly forbidden by the Brand, it is recommended to enable Rogue AP detection under the Advanced Options of the Zone **but** be sure **not** to enable "Protect the network from malicious rogue access points".

AP Ping latency reveals information about the latency in the control plane, i.e., between the AP management interface and the controller. For on-premise controllers this will only reflect latency on the property but for a centralized controller (vSmartZone) it also reflects the latency of the WAN interface to the Internet.

On a **SmartZone**, enable AP Ping Latency and Rogue AP Detection under the Advanced Options of the Zone.

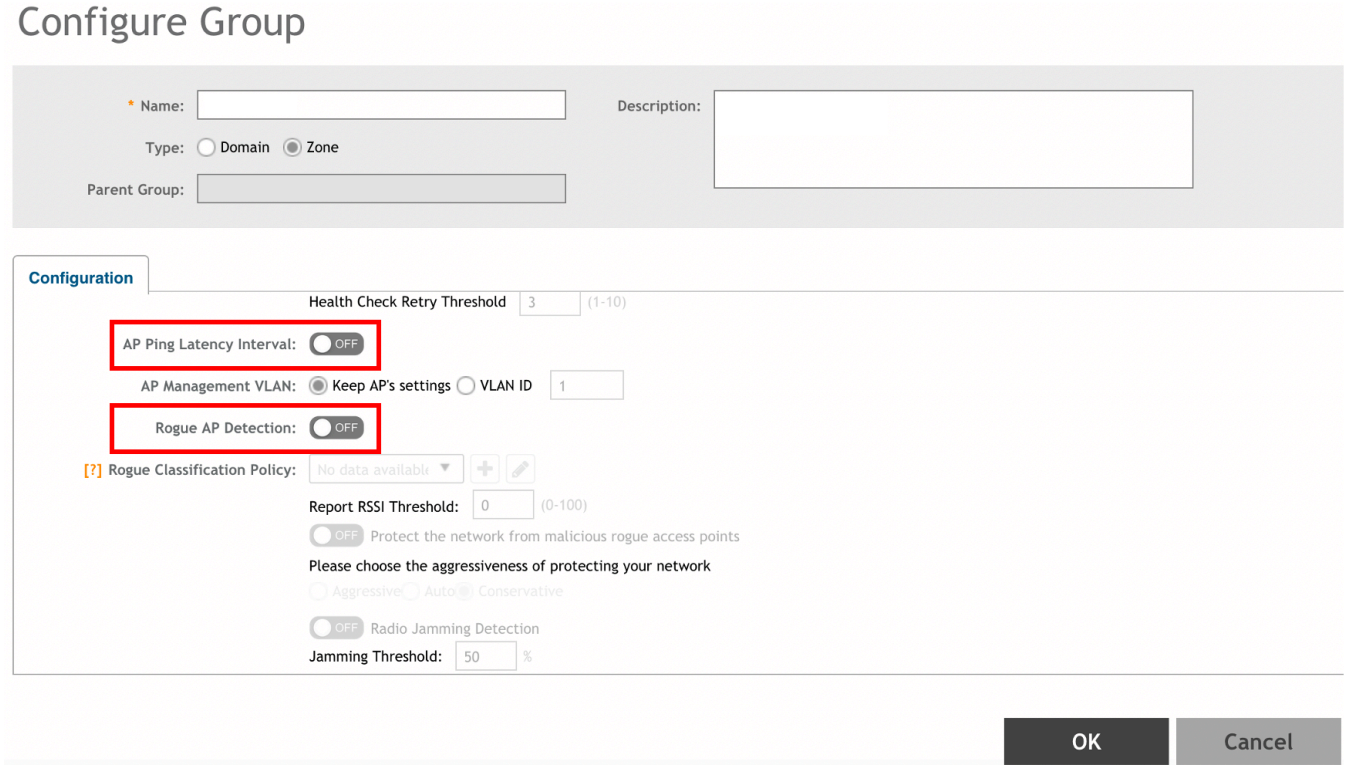



FIGURE 13: ENABLE ROGUE AP DETECTION AND AP PING LATENCY

## Configuring ZoneDirector

The following provides directions for configuring a ZoneDirector to connect to SmartCell Insight (SCI)-as-a-Service. There are multiple steps in verifying a configuration is appropriate for having a ZoneDirector connect to SCI and reporting data to SCI. Be sure to follow all steps using the checklist at the end of this section.

If configuring a SmartZone, skip to the section Configuring SmartZone.

### Configuring Time Synchronization (NTP)

It is crucial for the timestamp of all reported metrics from the controllers be in sync across amongst all properties. If a controller sends data out of sync, that data will be dropped and lost.

To maintain data synchronization, you must ensure that NTP synchronization is happening properly. This is true for both SmartZones and ZoneDirectors.

On a ZoneDirector, navigate to Configure > System and scroll down to System Time.

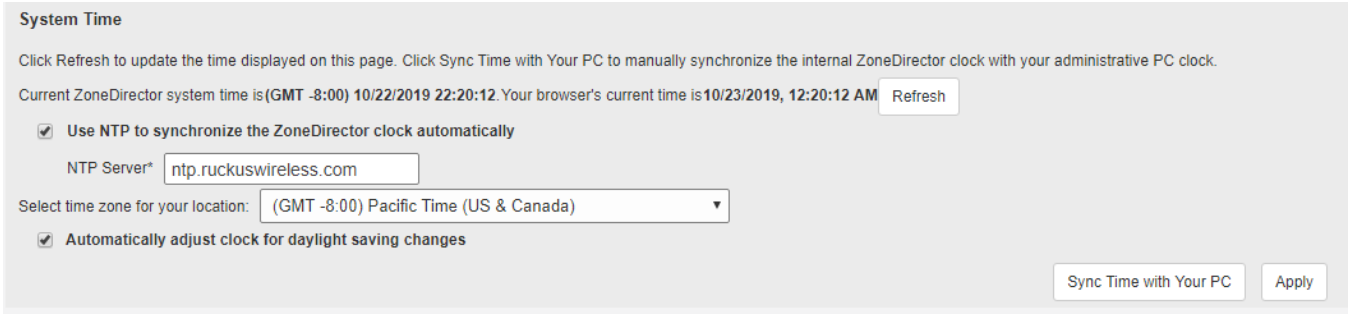



FIGURE 14: ZONEDIRECTOR NTP CONFIGURATION

Configure the NTP Server to use ntp.ruckuswireless.com and the correct local time zone and click Apply.

Click Refresh to ensure the controller synchronized and the correct current local time is displayed.

Be sure to ensure the local firewall does not block access to UDP port 123 and to monitor the controller for NTP issues via syslog and SNMP Alarms.

Note: If the controller is left in the Coordinated Universal Time (UTC) Time Zone, the time set at installation must match UTC not the local time where the controllers is installed. Either way works but it may be less confusing to put the controller into the local time zone and set current time equal to local time.

### On-boarding to SmartCell Insight

Once the system is configured in SCI, a System ID will be created that must be used to configure the ZoneDirector.

A Username and Password is necessary for communication to SCI and must match the credential configured in SCI for this ZoneDirector or group of ZoneDirectors.

On a ZoneDirector, navigate to Configure > System and scroll down to the bottom to expand the Network Management section:

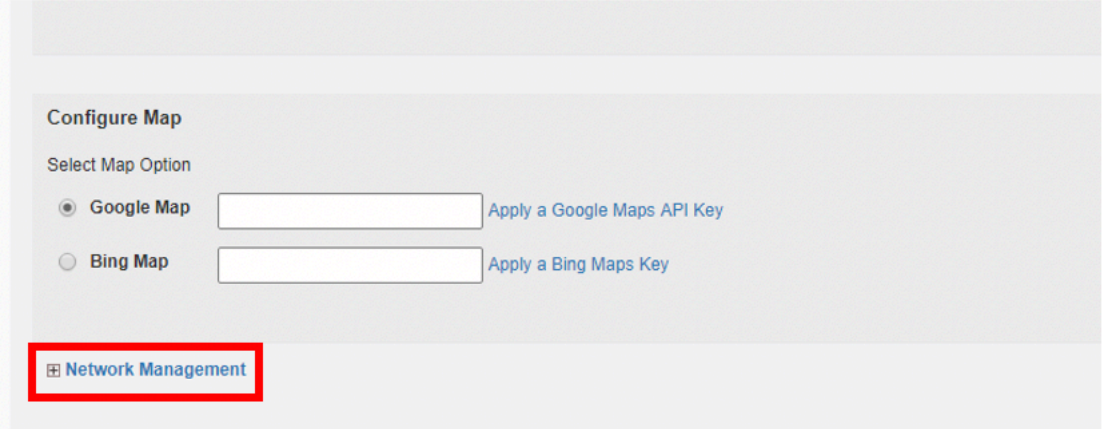



FIGURE 15: EXPAND NETWORK MANAGEMENT

Then scroll **up** to SmartCell Insight Management:

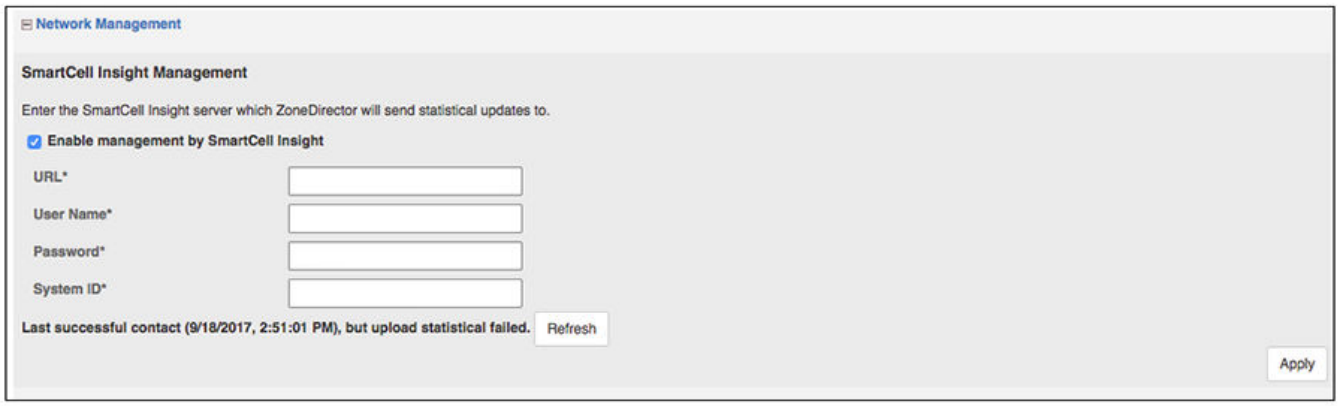



FIGURE 16: SMARTCELL INSIGHT MANAGEMENT

Make the following configuration changes:

1. **URL:** the URL or IP address of SmartCell Insight server
2. **Username** and **Password**: as configured in SCI
3. **System ID:** must match what was created in SCI

Additionally, for a ZoneDirector 1200, the following CLI command must be issued to enable sending session data to SCI:

```
ruckus> en
ruckus# config
You have all rights in this mode.
ruckus(config)# system
ruckus(config-sys)# session-stats-resv
The session statistics function has been enabled.
ruckus(config-sys)# quit
No changes have been saved.
ruckus(config-sys)# show
Session Statistics:
Enable= true
Limited Unauthorized Session= true
ruckus(config)# quit
```

## Enabling Application Recognition and Client Fingerprinting

For client applications and device types to be available in SmartCell Insight, Application Recognition and Client Fingerprinting must be enabled on the WLAN.

On a ZoneDirector, navigate to WLANs:

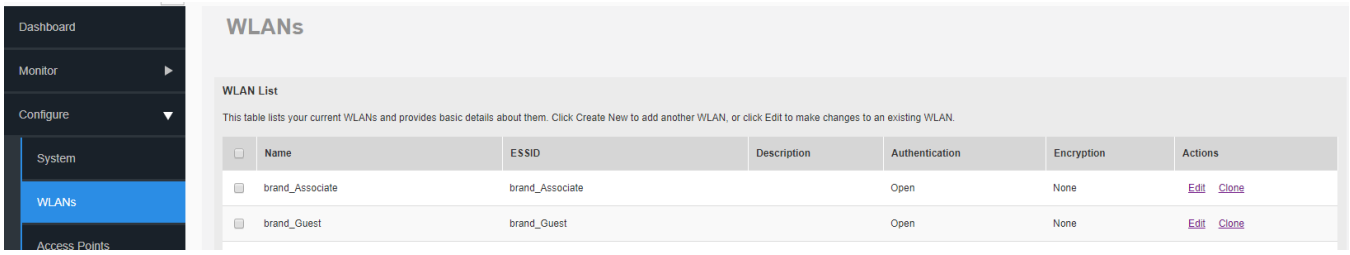



FIGURE 17: ZONEDIRECTOR WLANS

Edit each WLAN individually, scrolling down to expand the Advanced Options to enable Application Recognition & Control and Client Fingerprinting.

## Enabling Rogue AP Detection

Information about the RF environment is made visible by enabling Rogue AP detection. This can be safely enabled at the Zone level with **no** impact on clients. Unless explicitly forbidden by the Brand it is recommended to enable Rogue AP detection under the Advanced Options of the Zone **but** be sure **not** to enable "Protect the network from malicious rogue access points".

On **ZoneDirector**, navigate to Configure > WIPS (Wireless Intrusion Detection and Prevention System):

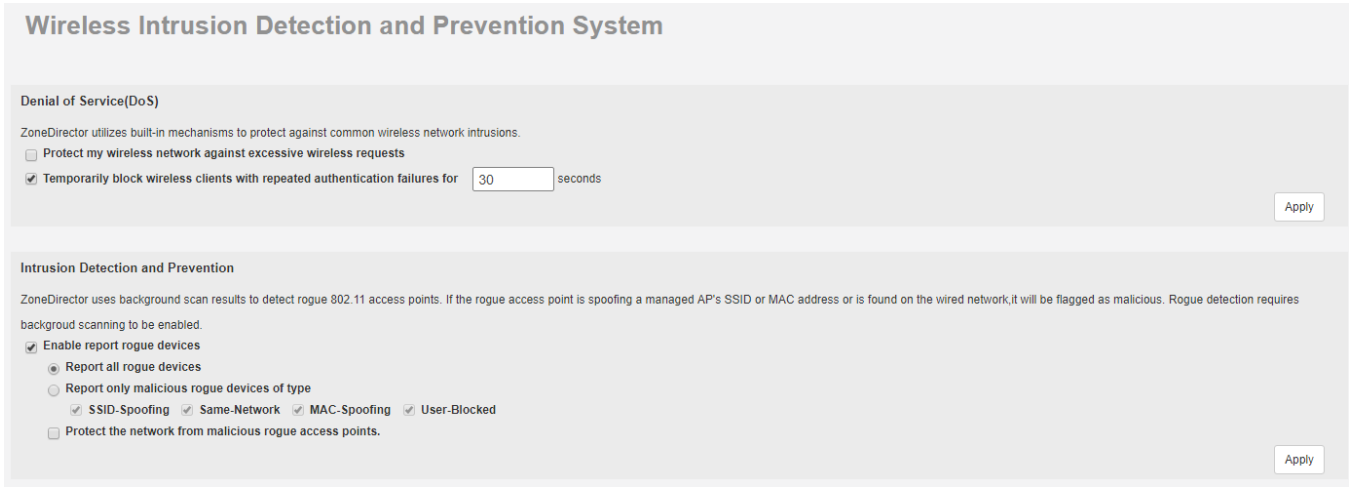



FIGURE 18: ZONEDIRECTOR ROGUE DEVICE DETECTION

Enable report rogue devices as above.

# Configuring Switches for Analytics

Switches are monitored in SCI and Ruckus Analytics via a SmartZone controller. The following steps are only relevant to a SmartZone deployment.

## Switch Firmware Requirements

For network monitoring, the minimum version of FastIron is v8.0.80. Our recommendations for new controllers are to use SmartZoneOS 5.1.2 and FastIron 8.0.90f.

If the any of the following switches are being deployed on the property, you should use the last Generally Available version FastIron v8.0.92 (currently 8.0.92b):

- ICX 7150-24F
- ICX 7150-C10ZP
- ICX 7150-C08P
- ICX 7150-C08PT

The switches do not need to be configured for full management via the SmartZone if the partner is utilizing other management and operations tools, but we believe the best long-term solution will include the SmartZone fully managing all devices, access points and switches, on the property.

## Other Requirements to Monitor or Manage ICX Switches via SmartZone

Other requirements include:

- Smartzone's IP address should be reachable by the ICX device through the Management interface or through router interfaces.
- The ICX device must be made aware of the configured SmartZone IP address in one of two ways:
  - configuring the DHCP server to use DHCP option 43
  - issuing the following command at the global configuration level:

```
ICX(conf)# sz active-list < SmartZone_Control_IP_Address >
```

- On some ICX 7250, ICX 7450, or ICX 7750 devices, self-signed certificates are used. SmartZone honors these certificates when the following option is configured on the SmartZone console:

```
no non-tpm-switch-cert-validate
```

- When SmartZone or ICX devices are behind NAT, be sure to forward TCP ports 443 and 22 through NAT

On the SmartZone, each switch counts for 5 APs from a scaling perspective.

# Naming Conventions

This document is intended to help Ruckus partners and customers configure their Wireless LAN Controllers, including SmartZone 100, vSmartZone, and various Zone Director models, to work with SmartCell Insight (SCI) to provide analytical insights across multiple properties.

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.

These discrepancies need to be addressed to enable reporting where one or more of these fields are used as a dimension in the report. For example, reporting on the guest experience at a summarized level per property requires a consistent naming convention in the Zone field:

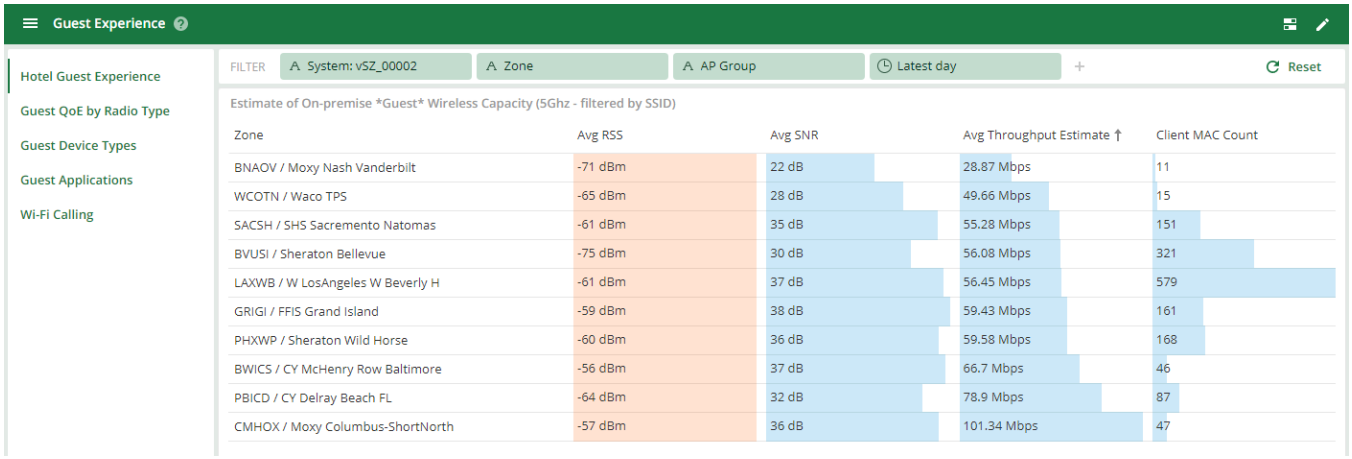



FIGURE 19: ZONE NAMES IN REPORTING

Similarly, if looking at footfall traffic in different areas of a property, or network performance, a clear and consistent naming convention is necessary for AP Groups for the information to be meaningful.

## Controller Configuration Hierarchy

Ruckus controllers have a similar, but slightly different, naming hierarchy depending on the type of controller in use:

SmartZoneOS 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.

The SmartZone hierarchy looks as follows: System > Controller > Domain > Sub-Domain > Zone > AP group > AP

- System - Highest order that comprises multiple domains and zones
- Controllers – are used when a controller comprises multiple nodes for scale and/or redundancy
- 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 Subgroup – the functional equivalent of AP Groups, representing groups of switches within a property

SmartZone100 and vSZ-E, being intended for enterprise deployments, do not employ the Domain and Sub-Domain constructs.

Zones can also comprise multiple WLAN groups

- WLAN Groups—Comprises multiple WLANs
- WLANs - Wireless network services (as represented by an SSID)

Specific recommendations for naming conventions for these groupings are made below.

The ZoneDirector platform is the simplest, intended for smaller deployments, it simply utilizes AP Groups to aggregate like APs. That, and the assumption that a ZoneDirector is deployed at the property led us to modify SmartCell Insight to automatically map the System ID of a ZoneDirector to the Zone name, allowing us carry forward the hierarchical naming convention from SmartZones to ZoneDirectors and use Zone names to map to properties.

## 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

Controller Name is associated with the individual nodes in a multi-node cluster, or the individual controller in the case of a Zone Director and is generally configured to match the brand naming convention at the time of initial installation.

Average Controller Resource Utilization

| System, Controller Name | Avg CPU Utiliz... ↓ | Change | Avg Memory Utili... | Change | Avg Disk Utilization |
|---|---|---|---|---|---|
| vSZ_00001 | 48.40 % | ▲ 2.52 % (5.5%) | 72.18 % | ▼ 2.29 % (3.1%) | 47.18 % |
| vscg-01 | 50.27 % | ▼ 11.87 % (19.1%) | 73.51 % | ▼ 2.39 % (3.1%) | 60.87 % |
| vscg-02 | 49.19 % | ▲ 11.01 % (28.8%) | 70.60 % | ▼ 0.41 % (0.6%) | 40.03 % |
| vscg-03-C | 45.75 % | ▲ 8.41 % (22.5%) | 72.44 % | ▼ 4.07 % (5.3%) | 40.63 % |
| SZ100_00001 | 16.49 % | ▲ 0.14 % (0.9%) | 59.22 % | ▲ 0.15 % (0.3%) | 17.88 % |
| NYCCP-CTL-01 | 16.49 % | ▲ 0.14 % (0.9%) | 59.22 % | ▲ 0.15 % (0.3%) | 17.88 % |
| SZ100_00003 | 16.36 % | ▲ 16.36 % (new) | 66.22 % | ▲ 66.22 % (new) | 19.31 % |
| CHIGSWC01-06-MDF | 16.76 % | ▲ 16.76 % (new) | 66.86 % | ▲ 66.86 % (new) | 20.23 % |
| CHIGSWC02-06-MDF | 16.18 % | ▲ 16.18 % (new) | 67.37 % | ▲ 67.37 % (new) | 19.22 % |

FIGURE 20: SYSTEM ID RELATIONSHIP TO CONTROLLER NAMES

If the controller name is already set and does not follow this convention, do not change it as the process of changing the controller name can impact the network.

## Zones

### Zones to Denote Properties

Zones below the brand domain shall reflect the unique property id. Most brands utilize a unique property ID, and do some partner. We recommend a consistent use of the ID of the property, a delimiter, followed by the name of the property. For example:

<XXXXX>/<20-character text name of property>, where

- XXXXX is the 5-character property code
- And the 20-character text name of the property is the commonly known name
- A forward slash separates the property code and Property name without spaces.

For partners that use their own unique identifiers in the Zone name to facilitate searching via API calls, the partner's property ID can be appended to the Zone name described above following a defined delimiter:

<XXXXX> / <aaaaaaaaaaaaaaaaaaaa> | <Partner Property ID> where

- XXXXX is the 5-character property code
- Aaaaaaaaaaaaaaaaaaaa is the commonly known name
- Partner Property ID is the unique identifier assigned by the partner
- A forward slash separates the property code and Property name without spaces.

This will allow the Partner Property ID to be located following the second delimiter ("|"):

"XXXXX / aaaaaaaaaaaaaaaaaaaa | ppppppppp"

**Other Uses of Zones**

Zones are also used as logical boundaries for APs that share common firmware requirements (e.g. supporting older models such as 802.11n-only APs in a 3.6.2 AP Zone running on a 5.1.2 controller that also support the latest 802.11ax AP).

Zones are also the most granular hierarchical concept at which an upgrade can happen. That is, you can upgrade individual zones but not individual AP Groups.

For either of the above reasons, it may be desirable to break a property into multiple zones. In the event this becomes necessary, the secondary zone shall be named following the same naming convention, appending the AP firmware version in the name, i.e.:

<XXXXX> / <20-character text name of property> | <partner property ID>: <firmware version>

-- or --

<XXXXX> / <20-character text name of property> : <firmware version>

**Note:** ZoneDirectors, despite the name, do not support the hierarchical construct of a Zone. Because of this, the System ID is automatically replicated as the Zone name during data ingestion when receiving data from a ZoneDirector into SmartCell Insight.

**Switch Groups**

Switch Groups shall be named the same as the Zone name that matches the property the Switch Group is aligned to:

<XXXXX> / <20-character text name of property>, where

XXXXX is the property 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 property code

the 20-character text name of the property is the commonly known name

Partner Property ID is the unique identifier assigned by the partner

### AP Groups

AP Groups shall be used to indicate where on a property an AP, or group of APs, resides. Examples of locations of APs that may need to be uniquely identified include:

- Lobby
- Restaurant
- Outdoor common
- Outdoor pool
- Guest room - even floor or specific
- Guest room - odd floor or specific
- Suites
- Lounge
- BOH (back of house)
- Administration
- Business Center
- Kitchen
- Valet or Parking
- Fitness Center
- Spa
- Conference Rooms (individual or group)
- Pre-function Space
- Meeting Congregation
- Meeting room small (< 50 ppl)
- Meeting room medium (51-100 ppl)
- Meeting room large (101-250 ppl)
- Ballroom

FIGURE 21: AP LOCATION EXAMPLES

There are cases where one AP might cover more than one area. The AP in the lobby covers the common space, the outdoor pool AP also covers the common outdoor space, etc. In those instances, use your best judgement and feedback from the owner on how they would like to see the analytics represented (e.g. do they want to understand usage patterns of the fitness room or spa?).

Additionally, the use of RSSI thresholds for probe response will help improve the accuracy of the reporting by trimming the clients associating to an AP to be those we want to capture in the analytics representation.

To be more prescriptive for AP Group names, we recommend the following AP Group names be used consistently across properties:

- Administration
- Basement
- Back_of_House
- Ballroom
- Ballroom - <name>
- Ballroom - <name> Salon <a>
- Business Center
- Conference Space
- Conference Room_<n>
- Casino
- Fitness Area
- Guest Hallway
- Guest Rooms
- Guest Rooms - Floor _<n>
- Guest Rooms
- Lobby
- Meeting Room
- Outdoor Commons
- Pool
- Public Space
- Restaurant
- Spa
- Valet

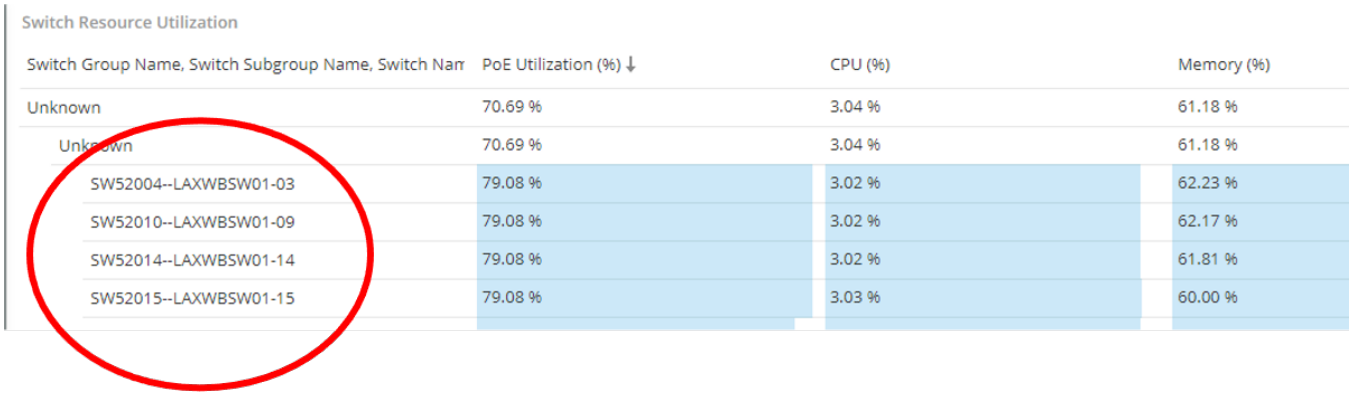
FIGURE 22: AP GROUP NAME SUGGESTIONS

### Switch Subgroups

Switch Subgroups provide the same function as AP Groups, that is 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: something like the following:

<Property_Code>+<Device_Code[22]>+<Device_Sequence_Number[23]>-<Floor_Number[24]>-<Room_Number>[2]

The location is a part of the switch naming convention as seen in these examples:


Switch Resource Utilization

| Switch Group Name, Switch Subgroup Name, Switch Nam | PoE Utilization (%) ↓ | CPU (%) | Memory (%) |
|---|---|---|---|
| Unknown | 70.69 % | 3.04 % | 61.18 % |
| Unknown | 70.69 % | 3.04 % | 61.18 % |
| SW52004--LAXWBSW01-03 | 79.08 % | 3.02 % | 62.23 % |
| SW52010--LAXWBSW01-09 | 79.08 % | 3.02 % | 62.17 % |
| SW52014--LAXWBSW01-14 | 79.08 % | 3.02 % | 61.81 % |
| SW52015--LAXWBSW01-15 | 79.08 % | 3.03 % | 60.00 % |

FIGURE 23: SWITCH NAMING CONVENTION

Therefore, the Switch Subgroup shall be denoted as

<Property Code>-<Floor_Number>_<Room Number>

## Configuration Checklist

The following serves as a check list for the partner to ensure the network infrastructure is configured correctly for representation within the analytics platform:

- Controller Operating System Level
  - ZoneDirector
  - SmartZone
- AP Firmware Level
- Switch Firmware Level
- Switch Configuration to connect to SmartZone
- Controller NTP Configuration
- Controller Northbound Streaming Interface
- Controller Cloud Services
- Application Recognition and Client Fingerprinting
- Rogue AP Detection
- AP Ping Latency (SmartZone only)
- SmartZone Zone Names
- SmartZone Switch Groups
- AP Groups
- SmartZone Switch Sub-Groups

## Resource Groups

Resource Groups are a construct within the analytics platform that establishes the visibility rules for stakeholders. Resource Groups are created for partners, brand representatives, ownership groups and occasionally consultants. The Resource Group defines which properties a stakeholder (brand representative, owner representative, local IT staff or consultant) should be able to access.

## Credentials

The credentials used by any user of the User Interface are mapped to a Resource Group as described above. The user then has visibility to the properties identified in the Resource Group.

One should expect to support for following resource groups at a minimum for an analytics implementation across a portfolio of properties:

1. Brand-wide

   There is a single brand-wide Resource Group for all properties currently flying that brand's flag. Individuals at the brand could have administrative rights to maintain credentials for others at the brand with full brand-wide visibility.

2. Partner-wide

   There is a Resource Group for each partner submitting properties to enable them to see all their managed properties. Individuals at each partner could have administrative rights to maintain credentials for users with access to the partners properties.

3. Local IT

   Local IT staff could have credentials established and assigned to a Resource Group for that property alone.

4. Ownership Groups

   Owners are the one of the most important stakeholders in this data and the group who funds the service.

5. Consultants

   Consultants are an optional entity that may have an interest and requirement to have visibility to set of properties.

**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.