Ruckus Integration Guide

Identity Access Control and Device Security for Wireless BYOD and Managed Devices with Ruckus ZoneDirector and Impulse SafeConnect

Table of Contents

About This Integration Guide

This integration guide describes the different components and configurations required to enable network access for wireless endpoints using Ruckus Zone Director, Ruckus ICX and Impulse SafeConnect.

This guide is based on a validated topology. Ruckus validated integrations are extensively tested using both simulation and live network elements to ensure comprehensive validation of all published solutions. Customer use cases, common examples, and field experience are combined to generate prescriptive configurations to guide customer and partner implementations of Ruckus solutions.

Use Case Overview

Ruckus ICX Series switches are designed to meet the demands of today's high-performance businesses. ICX Series Ethernet switches allow companies to grow their networks at their own pace, minimizing large up-front investments. Based on open standards, ICX Series switches provide the carrier-class reliability, security risk management, virtualization, application control, and lower total cost of ownership (TCO) that businesses need today while allowing them to scale in an economically sensible way for years to come.

SafeConnect Identity Access Control recognizes when devices attempt access to the wireless network and provides agentless device type profiling, user authentication, network "non-browser" device registration, guest access self-enrollment management, and real-time or historical contextual intelligence-based reporting. This is an ideal solution for customers that desire context-aware network access assignment and visibility for computing devices based on identity/role, device type, location, IP-MAC Address, and ownership (managed or BYOD).

SafeConnect Device Security enhances the security posture of your network by providing real-time policy assessment, enforcement, and self-remediation for Windows and MAC OS X devices. SafeConnect's Policy Key (agent) provides in-depth compliance assessment prior to granting network access to ensure that the device adheres to the organization's acceptable use policies (anti-virus, operating patches, personal firewalls, P2P, etc.) as well as on a continuous basis after access is granted. Web-based self-remediation guidance enables users to conform to security policies without end user help desk support involvement. The SafeConnect Policy Key can be pre-deployed to managed devices using standard AD Domain Group Policies or via the organization's chosen software distribution product. BYOD users will be prompted to install the SafeConnect Policy Key (if required) prior to accessing the network.

Multiple use cases can be addressed with this integration. This document describes an example of how to configure a Ruckus ICX 7450 switch, Ruckus ZoneDirector and SafeConnect for Network Access Assignment and Control of various devices including BYOD devices.

Related Documentation

Ruckus ZoneDirector 9.13 (GA) User Guide

Ruckus FastIron Layer 3 Routing Configuration Guide

SafeConnect RADIUS Server Configuration Guide

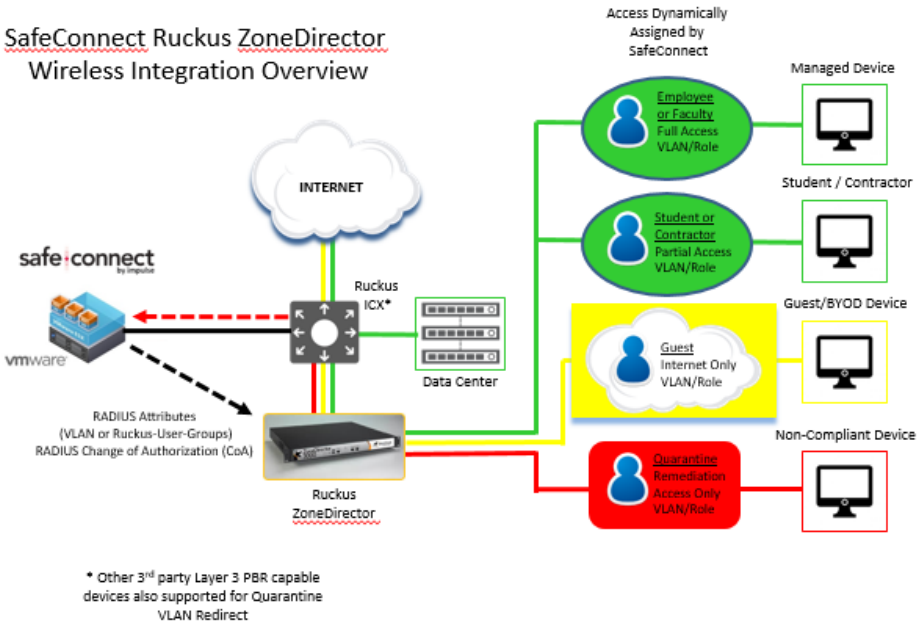
SafeConnect Policy Manager Configuration Guide

Use Case Details

In addition to Employees or Faculty, enterprises typically have other types of users such as Students, Contractors and Guests who would require access to the network. In each case, different levels of access may be required. These access levels can be customized to full network access, partial network access or Internet only depending on a variety of criteria such as identity, device type, device ownership, device location and compliance status to name a few.

Employee, Faculty or Student users may be authenticated and assigned the appropriate level of network access. Guest users may be redirected to a guest self-enrollment portal where the user can submit a request for guest credentials to authenticate to the guest network without involving help desk personnel. After the guest authentication is successful, the guest user gets limited access to the network, typically Internet only. Ruckus ZoneDirector, ICX Series switches and SafeConnect enable this workflow by providing support for WPA2E, MAC authentication, Dynamic VLAN or Role Assignment and RADIUS Change of Authorization capabilities.

Figure1: Use Case Topology



In this use case above, the WPA2E or Open SSID with MAC authentication in the Ruckus ZoneDirector are configured to authenticate against the SafeConnect RADIUS Server.

For Employees, Faculty or Students connecting to the WPA2E SSID, 802.1X authentication will be performed. After authentication takes place, the SafeConnect RADIUS server will dynamically assign the Employee/Faculty or Student the appropriate level of access. This can be achieved by leveraging VLAN RADIUS attributes or the Ruckus-User-Groups Vendor Specific Attribute (VSA) which correspond to Roles in ZoneDirector.

For a Guest connecting to the Open SSID, MAC authentication is performed. If an encrypted SSID is preferred, PSK or DPSK SSIDs with MAC authentication configured are also supported. The MAC authentication will initially place the user in the Quarantine VLAN or Role for Captive Portal user authentication to capture identity. Policy Based Routing (PBR) configuration on the ICX will redirect traffic received in the Quarantine VLAN to SafeConnect. After authentication takes place, a RADIUS Change of Authorization (CoA) will be sent from the SafeConnect RADIUS server to the ZoneDirector and the user will be placed in the Guest VLAN or Role.

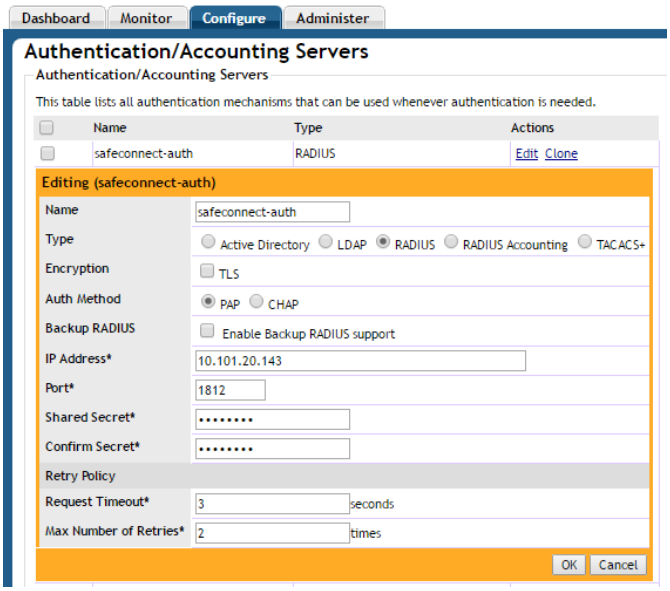
Components

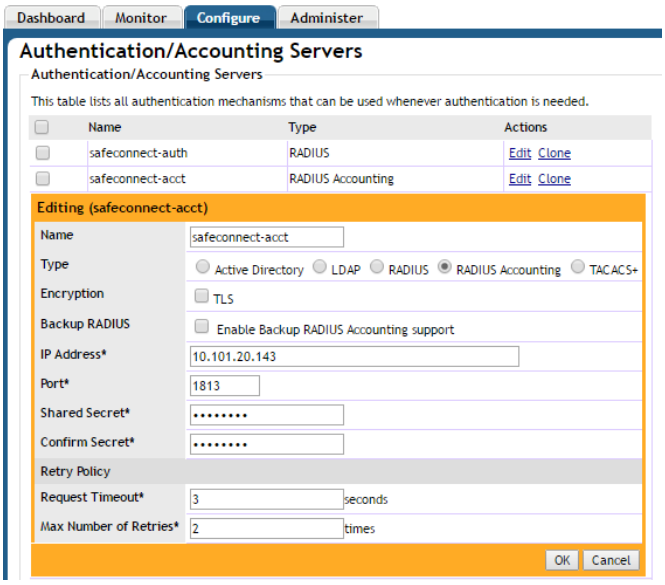
- Ruckus ZoneDirector
  - 9.13 preferred (9.10 or later supported)
- Ruckus ICX Series Layer 3 Switch
  - Premium Layer 3 Software License Required for PBR
- Impulse SafeConnect
  - 6.4 or later

Configuration

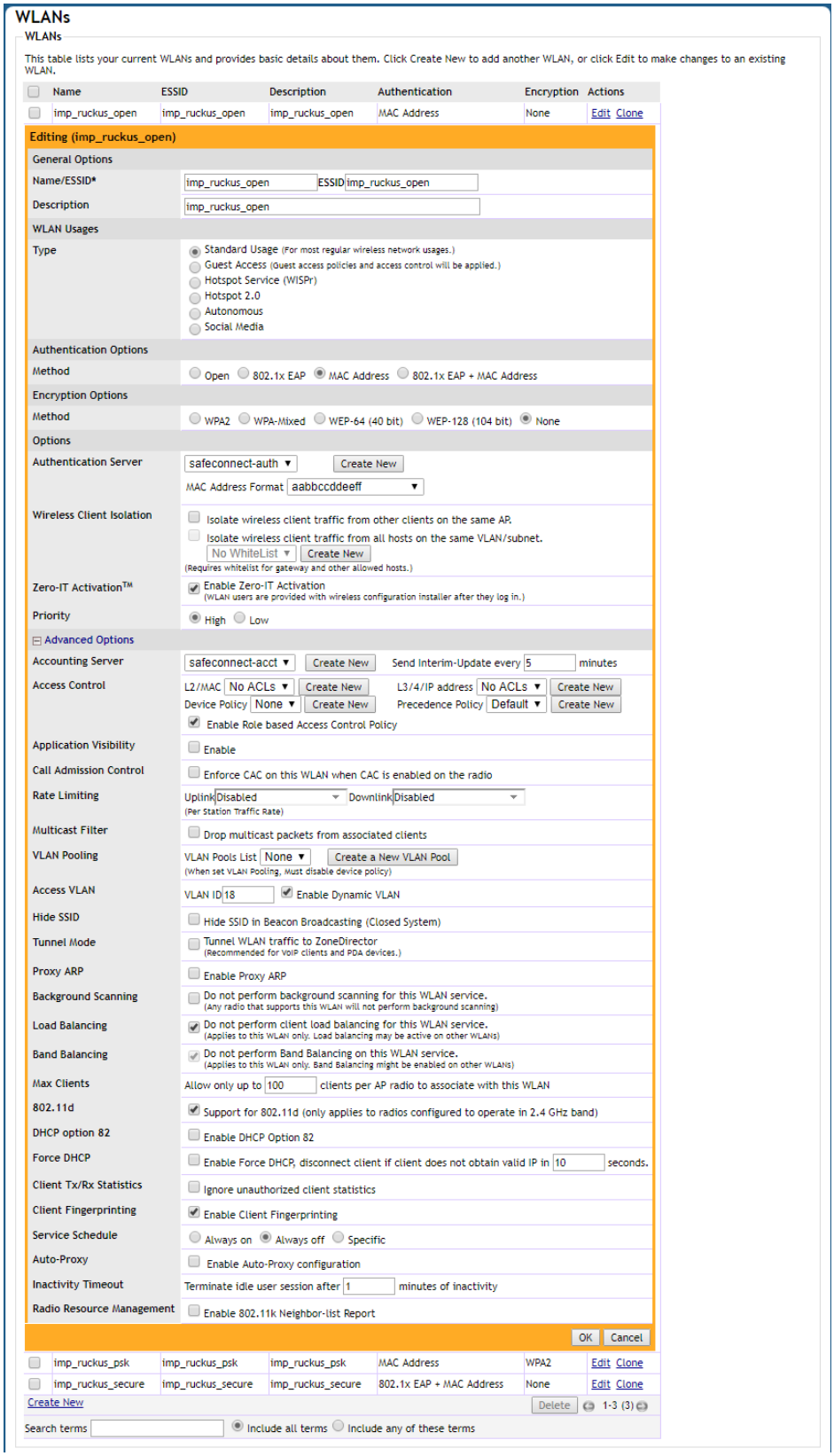
Configuring ZoneDirector

Add SafeConnect Authentication and SafeConnect Accounting Server:





Configure WLANs/ESSIDs for SafeConnect. Note – The VLAN ID should match the VLAN that compliant devices are assigned. The following examples show Open, PSK and WPA2E SSIDs.



WLANs

WLANs

This table lists your current WLANs and provides basic details about them. Click Create New to add another WLAN, or click Edit to make changes to an existing WLAN.

Name	ESSID	Description	Authentication	Encryption	Actions
imp_ruckus_open	imp_ruckus_open	imp_ruckus_open	MAC Address	None	Edit Clone
imp_ruckus_psk	imp_ruckus_psk	imp_ruckus_psk	MAC Address	WPA2	Edit Clone

Editing (imp_ruckus_psk)

General Options

Name/ESSID* imp_ruckus_psk ESSID imp_ruckus_psk

Description imp_ruckus_psk

WLAN Usages

Type
- (•) Standard Usage (For most regular wireless network usages.)
- ( ) Guest Access (Guest access policies and access control will be applied.)
- ( ) Hotspot Service (WISPr)
- ( ) Hotspot 2.0
- ( ) Autonomous
- ( ) Social Media

Authentication Options

Method ( ) Open ( ) 802.1x EAP (•) MAC Address ( ) 802.1x EAP + MAC Address

Encryption Options

Method (•) WPA2 ( ) WPA-Mixed ( ) WEP-64 (40 bit) ( ) WEP-128 (104 bit) ( ) None

Algorithm ( ) AES (•) Auto (TKIP+AES)

Passphrase* Impuls351

Options

Authentication Server safeconnect-auth ▼ Create New

MAC Address Format aabbccddeeff ▼

Wireless Client Isolation
- [ ] Isolate wireless client traffic from other clients on the same AP.
- [ ] Isolate wireless client traffic from all hosts on the same VLAN/subnet.

No WhiteList ▼ Create New

(Requires whitelist for gateway and other allowed hosts.)

Zero-IT Activation™ [ ] Enable Zero-IT Activation (WLAN users are provided with wireless configuration installer after they log in.)

Priority (•) High ( ) Low

Advanced Options

Accounting Server safeconnect-acct ▼ Create New Send Interim-Update every 5 minutes

Access Control L2/MAC No ACLs ▼ Create New L3/4/IP address No ACLs ▼ Create New
Device Policy None ▼ Create New Precedence Policy Default ▼ Create New
[x] Enable Role based Access Control Policy

Application Visibility [ ] Enable

Call Admission Control [ ] Enforce CAC on this WLAN when CAC is enabled on the radio

Rate Limiting Uplink Disabled Downlink Disabled
(Per Station Traffic Rate)

Multicast Filter [ ] Drop multicast packets from associated clients

VLAN Pooling VLAN Pools List None ▼ Create a New VLAN Pool
(When set VLAN Pooling, Must disable device policy)

Access VLAN VLAN ID 18 [x] Enable Dynamic VLAN

Hide SSID [ ] Hide SSID in Beacon Broadcasting (Closed System)

Tunnel Mode [ ] Tunnel WLAN traffic to ZoneDirector (Recommended for VoIP clients and PDA devices.)

Proxy ARP [ ] Enable Proxy ARP

Background Scanning [ ] Do not perform background scanning for this WLAN service. (Any radio that supports this WLAN will not perform background scanning)

Load Balancing [x] Do not perform client load balancing for this WLAN service. (Applies to this WLAN only. Load balancing may be active on other WLANs)

Band Balancing [x] Do not perform Band Balancing on this WLAN service. (Applies to this WLAN only. Band Balancing might be enabled on other WLANs)

Max Clients Allow only up to 100 clients per AP radio to associate with this WLAN

802.11d [x] Support for 802.11d (only applies to radios configured to operate in 2.4 GHz band)

DHCP option 82 [ ] Enable DHCP Option 82

Force DHCP [ ] Enable Force DHCP, disconnect client if client does not obtain valid IP in 10 seconds.

Client Tx/Rx Statistics [ ] Ignore unauthorized client statistics

Client Fingerprinting [x] Enable Client Fingerprinting

Service Schedule ( ) Always on (•) Always off ( ) Specific

Auto-Proxy [ ] Enable Auto-Proxy configuration

Inactivity Timeout Terminate idle user session after 5 minutes of inactivity

Radio Resource Management [ ] Enable 802.11k Neighbor-list Report

OK Cancel

WLANs

WLANs

This table lists your current WLANs and provides basic details about them. Click Create New to add another WLAN, or click Edit to make changes to an existing WLAN.

Name	ESSID	Description	Authentication	Encryption	Actions
imp_ruckus_open	imp_ruckus_open	imp_ruckus_open	MAC Address	None	Edit Clone
imp_ruckus_psk	imp_ruckus_psk	imp_ruckus_psk	MAC Address	WPA2	Edit Clone
imp_ruckus_secure	imp_ruckus_secure	imp_ruckus_secure	802.1x EAP	WPA2	Edit Clone

Editing (imp_ruckus_secure)

General Options

Name/ESSID* imp_ruckus_secure ESSID imp_ruckus_secure

Description imp_ruckus_secure

WLAN Usages

Type
- (•) Standard Usage (For most regular wireless network usages.)
- ( ) Guest Access (Guest access policies and access control will be applied.)
- ( ) Hotspot Service (WISPr)
- ( ) Hotspot 2.0
- ( ) Autonomous
- ( ) Social Media

Authentication Options

Method ( ) Open (•) 802.1x EAP ( ) MAC Address ( ) 802.1x EAP + MAC Address

Fast BSS Transition [ ] Enable 802.11r FT Roaming (Recommended to enable 802.11k Neighbor-list Report for assistant.)

Encryption Options

Method (•) WPA2 ( ) WPA-Mixed ( ) WEP-64 (40 bit) ( ) WEP-128 (104 bit) ( ) None

Algorithm (•) AES ( ) Auto (TKIP+AES)

Options

Authentication Server safeconnect-auth ▼ Create New

Wireless Client Isolation
- [ ] Isolate wireless client traffic from other clients on the same AP.
- [ ] Isolate wireless client traffic from all hosts on the same VLAN/subnet.
  No WhiteList ▼ Create New
  (Requires whitelist for gateway and other allowed hosts.)

Zero-IT Activation™ [ ] Enable Zero-IT Activation (WLAN users are provided with wireless configuration installer after they log in.)

Priority (•) High ( ) Low

⊟ Advanced Options

Accounting Server safeconnect-acct ▼ Create New Send Interim-Update every 5 minutes

Access Control
L2/MAC No ACLs ▼ Create New L3/4/IP address No ACLs ▼ Create New
Device Policy None ▼ Create New Precedence Policy Default ▼ Create New
[x] Enable Role based Access Control Policy

Application Visibility [ ] Enable

Call Admission Control [ ] Enforce CAC on this WLAN when CAC is enabled on the radio

Rate Limiting Uplink Disabled Downlink Disabled (Per Station Traffic Rate)

Multicast Filter [ ] Drop multicast packets from associated clients

VLAN Pooling VLAN Pools List None ▼ Create a New VLAN Pool (When set VLAN Pooling, Must disable device policy)

Access VLAN VLAN ID 18 [x] Enable Dynamic VLAN

Hide SSID [ ] Hide SSID in Beacon Broadcasting (Closed System)

Tunnel Mode [ ] Tunnel WLAN traffic to ZoneDirector (Recommended for VoIP clients and PDA devices.)

Proxy ARP [ ] Enable Proxy ARP

Background Scanning [ ] Do not perform background scanning for this WLAN service. (Any radio that supports this WLAN will not perform background scanning)

Load Balancing [x] Do not perform client load balancing for this WLAN service. (Applies to this WLAN only. Load balancing may be active on other WLANs)

Band Balancing [x] Do not perform Band Balancing on this WLAN service. (Applies to this WLAN only. Band Balancing might be enabled on other WLANs)

Max Clients Allow only up to 100 clients per AP radio to associate with this WLAN

802.11d [x] Support for 802.11d (only applies to radios configured to operate in 2.4 GHz band)

DHCP option 82 [ ] Enable DHCP Option 82

Force DHCP [ ] Enable Force DHCP, disconnect client if client does not obtain valid IP in 10 seconds.

Client Tx/Rx Statistics [ ] Ignore unauthorized client statistics

Client Fingerprinting [x] Enable Client Fingerprinting

Service Schedule (•) Always on ( ) Always off ( ) Specific

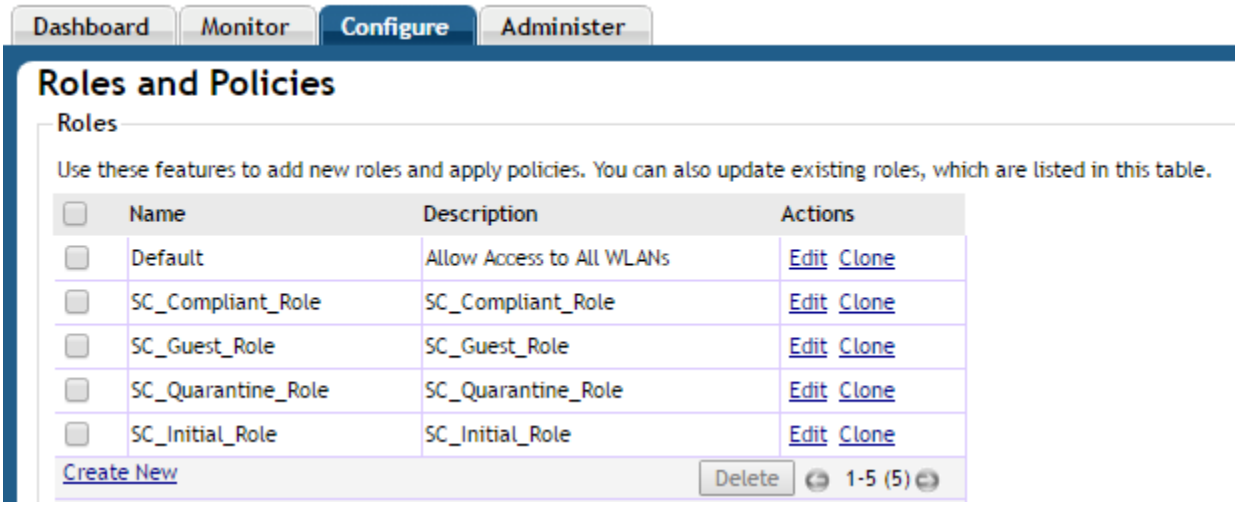
Auto-Proxy [ ] Enable Auto-Proxy configuration

Inactivity Timeout Terminate idle user session after 5 minutes of inactivity

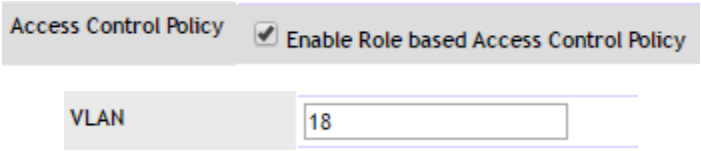
Radio Resource Management [ ] Enable 802.11k Neighbor-list Report

OK Cancel

Configure Roles to be dynamically assigned by SafeConnect. Note – SafeConnect can also dynamically assign any valid, configured VLAN instead if desired. Create the roles shown below by clicking the Create New button and adding each role. Note – Roles will be configured via Auth Servers if using SmartZone.



Ensure each role has the Enable Role based Access Control Policy check box selected and also has a valid VLAN associated with the role. This allows Roles to be tied to the desired VLAN for the appropriate level of access.



Role names are for example purposes only. Any names can be used as long as these names match up with the enforcement roles configured in the SafeConnect RADIUS server. The SC_Quarantine_Role should be tied to the VLAN configured for Layer 3 redirect in the next section.

Configuring the Ruckus ICX Layer 3 Switch Quarantine VLAN Redirect

Configure a route-map on the upstream Layer 3 ICX switch which redirects all traffic to SafeConnect for remediation. Note that SafeConnect must reside in a directly connected subnet on the ICX in order for PBR to function properly.

```
interface ve 10 (example quarantine VLAN Layer 3 interface)
 ip address 10.101.10.1 255.255.255.0
 ip policy route-map quarantine
!
interface ve 20 (example SafeConnect VLAN Layer 3 interface)
 ip address 10.101.20.1 255.255.255.0
!
ip access-list extended quarantine-redirect
 deny udp any any eq 53
 deny udp any any eq bootps
 permit ip any any
!
route-map quarantine
 match ip address quarantine-redirect
 set ip next-hop 10.101.20.143 (SafeConnect)
```

This completes the configuration required on the Ruckus network infrastructure. The next step will be to configure the SafeConnect RADIUS Server.

Configuring the SafeConnect RADIUS Server

Refer to the SafeConnect RADIUS Server Configuration Guide and Policy Manager Configuration Guide to complete the integration with SafeConnect. Login to the SafeConnect management interface at https://x.x.x.x:8443/manage. In a SafeConnect clustered environment, this must be the manager node. If a branded URL is configured, replace IP with the branded URL chosen. Once Logged in, choose Configuration Manger > Enforcement Setup > RADIUS Configuration > RADIUS Configuration to complete the configuration.