

Introduction

Bradford Network Sentry is a purpose-built Network Access Control (NAC) physical/virtual appliance. It dynamically leverages the continuously growing library of security commands and controls built into today's switches, routers, wireless controllers and wireless access points to perform pre-connect risk assessments on every device attempting to connect to the network.

This note provides step by step instructions on setting up a Ruckus-Bradford solutions environment. It assumes that the reader is reasonably familiar with both Ruckus and Bradford products.

Versions:

Ruckus Zone Director: 9.8.2

Ruckus SmartZone (SZ100, vSZ-E, vSZ-H, SCG200): 3.2

Bradford: 7.1 (for Zone Director); 7.3.2 for Smartzone

Setup Overview

1. Two VLANs: "Production" and "Isolation". Unauthenticated users are placed into the Isolation VLAN and authenticated users are placed into the Production VLAN.
2. Two SSIDs/WLANs are setup corresponding to the Production and Isolation VLANs. The Production SSID is broadcast over the air whereas the Isolation SSID is a dummy.
3. The Production SSID/WLAN is set up with Dynamic VLAN (DVLAN) capabilities and MAC Authentication. The Bradford Network Sentry appliance acts as the Radius Server.
4. The Isolation SSID/WLAN is a "dummy" and is not broadcast over the air.
5. The Network Sentry Appliance acts as the DHCP/DNS server for the Isolation VLAN. The Production VLAN uses the organization's regular DHCP/DNS servers.
6. The Network Sentry Appliance "reads" the WLAN/VLAN configuration from the Ruckus Controllers via SNMP.

User Experience

1. New user connects to the Production SSID. Ruckus sends a Radius Request to the Network Sentry appliance. On seeing that the device is unregistered, Network Sentry places this device into the Isolation VLAN via the DVLAN capability in the Radius Response. The user is assigned an IP address on the Isolation VLAN by the Network Sentry Appliance.
2. User browses to say, google.com and is re-directed to the Network Sentry Appliance portal page. User authenticates
3. Network Sentry sends Radius DM message to the Ruckus Controller and the user is disconnected from the SSID. In older versions, the Network Sentry would disconnect

the user via CLI commands issued to the Ruckus Zone Director.

4. User automatically reconnects and now the Network Sentry Appliance places this authenticated user into the Production VLAN. The IP address is obtained from the organization's regular DHCP/DNS servers.

Towards the end, this note also addresses the issue of wired clients on the Access Points. A brief troubleshooting section going through the Radius exchange follows.

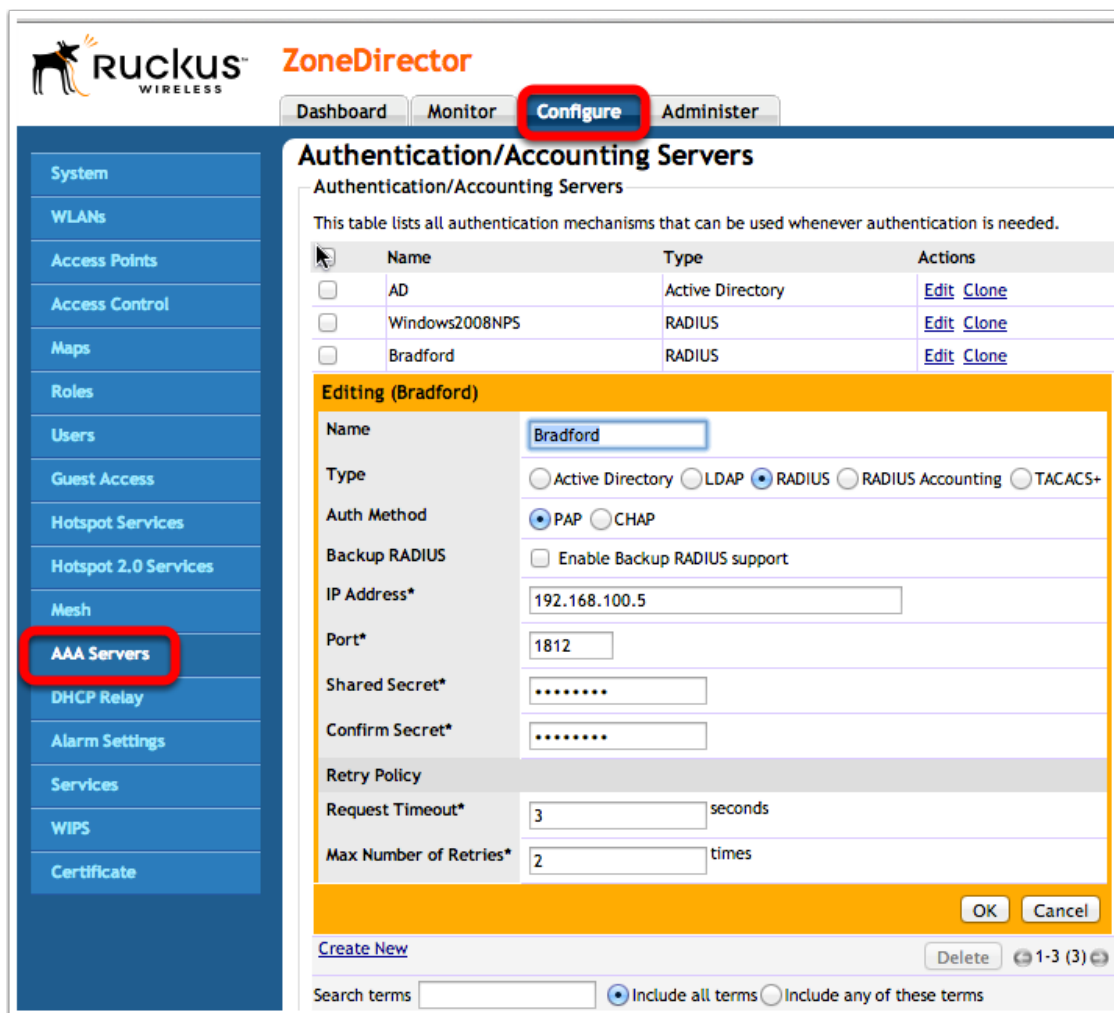
Ruckus Zone Director Setup

This involves the following:

1. Setting up the Network Sentry Appliance as the Radius Server
2. Setting up the Production and Isolation SSIDs/WLANs (the latter as a dummy).
3. Enabling SNMP with the appropriate accounts/passphrases.

Network Sentry As Radius Server

After logging into the Zone Director, go to Configure->AAA Servers and set up the Network Sentry Appliance as a Radius Server (IP Address, shared secret, etc.)



The screenshot shows the Ruckus ZoneDirector web interface. The top navigation bar includes 'Dashboard', 'Monitor', 'Configure' (highlighted with a red box), and 'Administer'. The left sidebar contains a menu with 'AAA Servers' highlighted in a red box. The main content area is titled 'Authentication/Accounting Servers' and contains a table of existing servers:

Name	Type	Actions
AD	Active Directory	Edit Clone
Windows2008NPS	RADIUS	Edit Clone
Bradford	RADIUS	Edit Clone

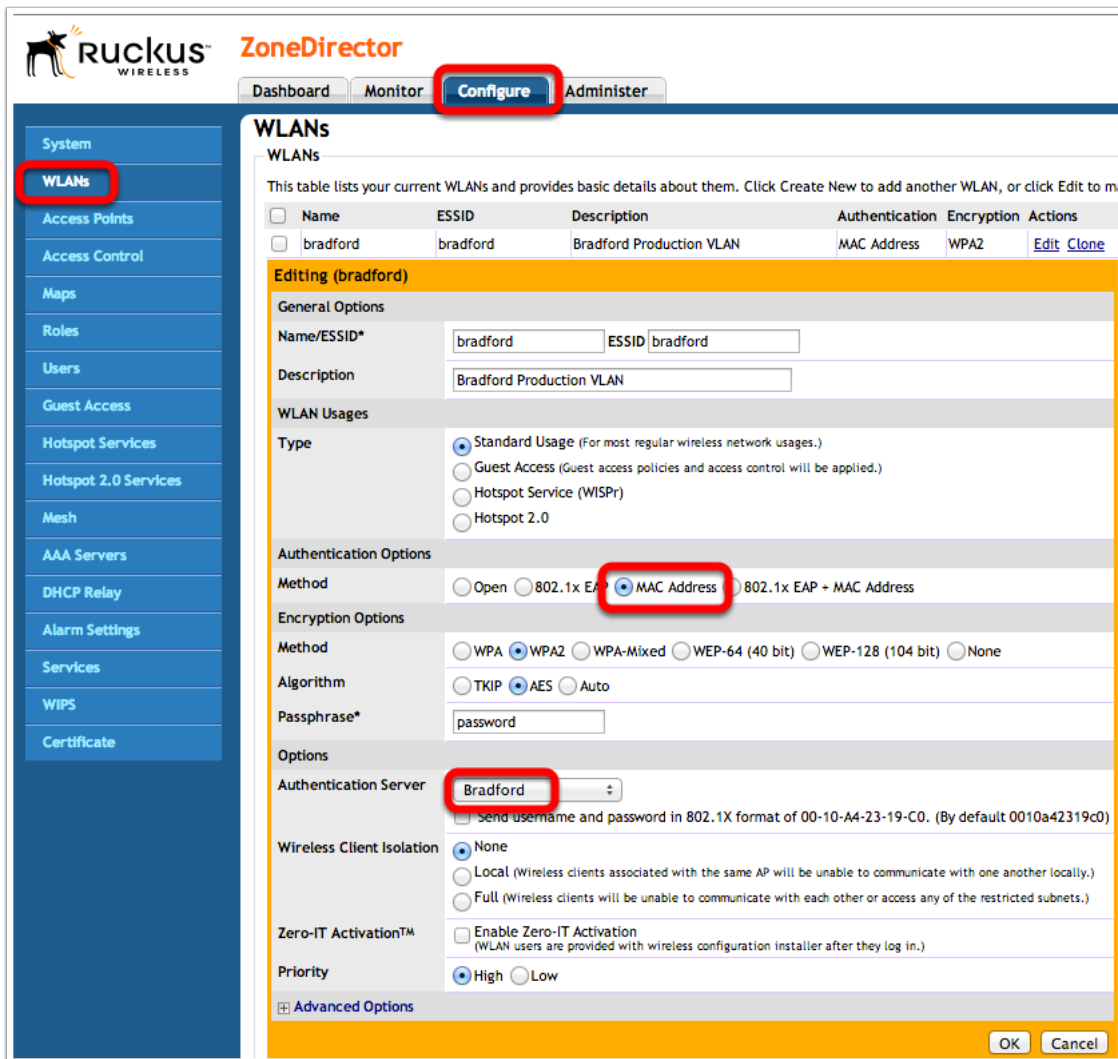
Below the table is the 'Editing (Bradford)' form. The fields are as follows:

- Name: Bradford
- Type: Active Directory LDAP RADIUS RADIUS Accounting TACACS+
- Auth Method: PAP CHAP
- Backup RADIUS: Enable Backup RADIUS support
- IP Address*: 192.168.100.5
- Port*: 1812
- Shared Secret*: [masked]
- Confirm Secret*: [masked]
- Retry Policy:
 - Request Timeout*: 3 seconds
 - Max Number of Retries*: 2 times

At the bottom of the form are 'OK' and 'Cancel' buttons. Below the form is a 'Create New' link, a 'Delete' button, and a search filter showing '1-3 (3)' items. A search terms field is also present with radio buttons for 'Include all terms' (selected) and 'Include any of these terms'.

Production SSID/WLAN

From the Configure->WLANs tab, create a new SSID for the Production WLAN/VLAN. This should be set up for (a) Mac Authentication (b) Network Sentry Appliance as the Authentication Server and (c) Dynamic VLAN capabilities.



The screenshot shows the Ruckus ZoneDirector web interface. The 'Configure' tab is selected, and the 'WLANs' section is active. A table lists the current WLANs, with 'bradford' selected. The configuration page for 'bradford' is displayed, showing various options:

- General Options:** Name/ESSID* is 'bradford', and Description is 'Bradford Production VLAN'.
- WLAN Usages:** Type is 'Standard Usage' (selected).
- Authentication Options:** Method is 'MAC Address' (selected).
- Encryption Options:** Method is 'WPA2' (selected), and Algorithm is 'AES' (selected). Passphrase is 'password'.
- Options:** Authentication Server is 'Bradford' (selected).
- Wireless Client Isolation:** 'None' is selected.
- Zero-IT Activation™:** 'Enable Zero-IT Activation' is unchecked.
- Priority:** 'High' is selected.

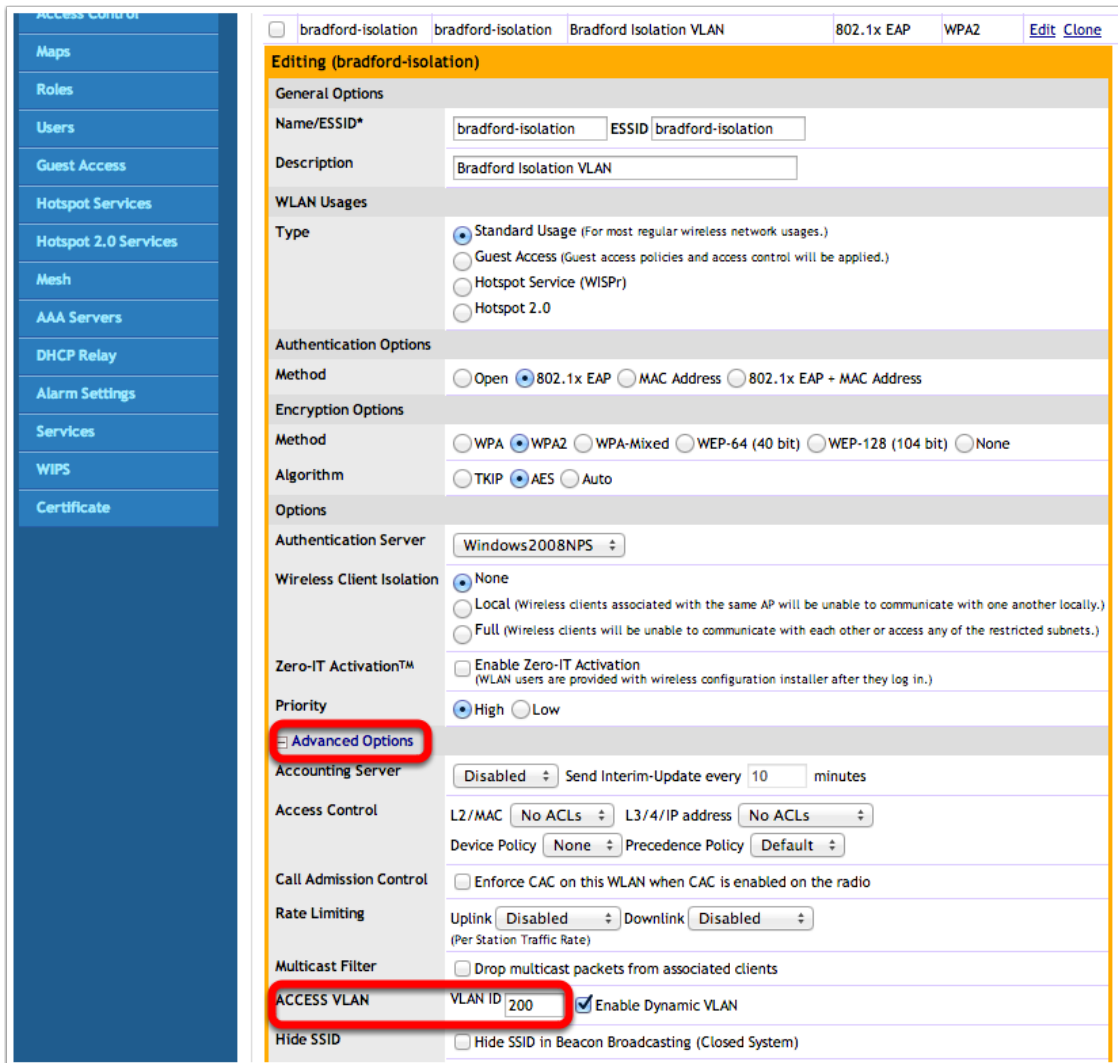
The 'Advanced Options' section is collapsed. The 'OK' and 'Cancel' buttons are visible at the bottom right.

Enable Dynamic VLAN under Advanced options

Zero-IT Activation™	<input type="radio"/> Full (Wireless clients will be unable to communicate with each other or access any of the restricted subnets.)
	<input type="checkbox"/> Enable Zero-IT Activation (WLAN users are provided with wireless configuration installer after they log in.)
Priority	<input checked="" type="radio"/> High <input type="radio"/> Low
Advanced Options	
Accounting Server	Disabled <input type="button" value="v"/> Send Interim-Update every 10 minutes
Access Control	L2/MAC <input type="button" value="v"/> No ACLs L3/4/IP address <input type="button" value="v"/> No ACLs Device Policy <input type="button" value="v"/> None Precedence Policy <input type="button" value="v"/> Default
Call Admission Control	<input type="checkbox"/> Enforce CAC on this WLAN when CAC is enabled on the radio
Rate Limiting	Uplink <input type="button" value="v"/> Disabled Downlink <input type="button" value="v"/> Disabled (Per Station Traffic Rate)
Multicast Filter	<input type="checkbox"/> Drop multicast packets from associated clients
ACCESS VLAN	VLAN ID <input type="text" value="110"/> <input checked="" type="checkbox"/> Enable Dynamic VLAN
Hide SSID	<input type="checkbox"/> Hide SSID in Beacon Broadcasting (Closed System)
Tunnel Mode	<input type="checkbox"/> Tunnel WLAN traffic to ZoneDirector (Recommended for VoIP clients and PDA devices.)
Proxy ARP	<input type="checkbox"/> Enable Proxy ARP
Background Scanning	<input type="checkbox"/> Do not perform background scanning for this WLAN service. (Any radio that supports this WLAN will not perform background scanning)
Load Balancing	<input type="checkbox"/> Do not perform client load balancing for this WLAN service. (Applies to this WLAN only. Load balancing may be active on other WLANs)
Max Clients	Allow only up to 100 clients per AP radio to associate with this WLAN
802.11d	<input checked="" type="checkbox"/> Support for 802.11d (only applies to radios configured to operate in 2.4 GHz band)
DHCP option 82	<input type="checkbox"/> Enable DHCP Option 82
Client Tx/Rx Statistics	<input type="checkbox"/> Ignore unauthorized client statistics
Client Fingerprinting	<input checked="" type="checkbox"/> Enable Client Fingerprinting
Service Schedule	<input checked="" type="radio"/> Always on <input type="radio"/> Always off <input type="radio"/> Specific
Auto-Proxy	<input type="checkbox"/> Enable Auto-Proxy configuration
Inactivity Timeout	Terminate idle user session after 5 minutes of inactivity

Isolation SSID/WLAN

Similarly create an Isolation SSID/WLAN of any type with the Access VLAN being set to the correct desired Isolation VLAN (Advanced Options).



The screenshot shows the configuration page for a WLAN named "bradford-isolation". The left sidebar contains a navigation menu with items like "Access Control", "Maps", "Roles", "Users", "Guest Access", "Hotspot Services", "Hotspot 2.0 Services", "Mesh", "AAA Servers", "DHCP Relay", "Alarm Settings", "Services", "WIPS", and "Certificate". The main content area is titled "Editing (bradford-isolation)" and contains several sections:

- General Options:** Name/ESSID* is "bradford-isolation", ESSID is "bradford-isolation", and Description is "Bradford Isolation VLAN".
- WLAN Usages:** Type is "Standard Usage (For most regular wireless network usages.)".
- Authentication Options:** Method is "802.1x EAP".
- Encryption Options:** Method is "WPA2", Algorithm is "AES".
- Options:** Authentication Server is "Windows2008NPS".
- Wireless Client Isolation:** "None" is selected.
- Zero-IT Activation™:** "Enable Zero-IT Activation" is unchecked.
- Priority:** "High" is selected.
- Advanced Options:** This section is highlighted with a red box. It includes:
 - Accounting Server: "Disabled", Send Interim-Update every "10" minutes.
 - Access Control: L2/MAC "No ACLs", L3/4/IP address "No ACLs", Device Policy "None", Precedence Policy "Default".
 - Call Admission Control: "Enforce CAC on this WLAN when CAC is enabled on the radio" is unchecked.
 - Rate Limiting: Uplink "Disabled", Downlink "Disabled" (Per Station Traffic Rate).
 - Multicast Filter: "Drop multicast packets from associated clients" is unchecked.
 - ACCESS VLAN:** "VLAN ID 200" is entered, and "Enable Dynamic VLAN" is checked. This entire section is highlighted with a red box.
 - Hide SSID: "Hide SSID in Beacon Broadcasting (Closed System)" is unchecked.

Remove Isolation WLAN from Default Group

Remove this isolation WLAN from the Default WLAN Group, so that the SSID is not broadcast over the air.

- Roles
- Users
- Guest Access
- Hotspot Services
- Hotspot 2.0 Services
- Mesh
- AAA Servers
- DHCP Relay
- Alarm Settings
- Services
- WIPS
- Certificate

<input type="checkbox"/>	DynamicVLAN	DynamicVLAN		802.1X EAP	WPA2
<input type="checkbox"/>	Filewave	Filewave	Filewave BYOD	Open	WPA2
<input type="checkbox"/>	Interop	Interop	General Interop	Open	WPA2
<input type="checkbox"/>	OpenBYOD	OpenBYOD	Open SSID for Ruckus BYOD	Open	None
<input type="checkbox"/>	OpenFilewave	OpenFilewave	Open SSID for Filewave BYOD	Open	None
<input type="checkbox"/>	Students	Students	BYOD SSID for Students	Open	WPA2
<input type="checkbox"/>	Teachers	Teachers	BYOD SSID for Teachers	Open	WPA2

[Create New](#) [Delete](#)

Search terms Include all terms Include any of these terms

WLAN Groups

This table lists your current WLAN groups and provides basic details about them. Click Create New to add and

<input type="checkbox"/>	Name	Description	Actions
<input type="checkbox"/>	Default	Default WLANs for Access Points	Edit Clone

Editing (Default)

Name*

Description

Group Settings

Members	WLANs	Original VLAN	VLAN override
<input checked="" type="checkbox"/>	Interop	110	<input checked="" type="radio"/> No Change <input type="radio"/> Tag: <input type="text"/>
<input type="checkbox"/>	Filewave	110	<input type="radio"/> No Change <input type="radio"/> Tag: <input type="text"/>
<input type="checkbox"/>	OpenFilewave	110	<input type="radio"/> No Change <input type="radio"/> Tag: <input type="text"/>
<input type="checkbox"/>	OpenBYOD	1	<input type="radio"/> No Change <input type="radio"/> Tag: <input type="text"/>
<input type="checkbox"/>	Students	120	<input type="radio"/> No Change <input type="radio"/> Tag: <input type="text"/>
<input type="checkbox"/>	Teachers	130	<input type="radio"/> No Change <input type="radio"/> Tag: <input type="text"/>
<input type="checkbox"/>	DynamicVLAN	1	<input type="radio"/> No Change <input type="radio"/> Tag: <input type="text"/>
<input type="checkbox"/>	BYODGuestAccess	1	<input type="radio"/> No Change <input type="radio"/> Tag: <input type="text"/>
<input type="checkbox"/>	bradford	110	<input type="radio"/> No Change <input type="radio"/> Tag: <input type="text"/>
<input type="checkbox"/>	bradford-isolation	200	<input type="radio"/> No Change <input type="radio"/> Tag: <input type="text"/>

Enable SNMP

From Configure->System->Network Management (towards the bottom of the page), enable the SNMP v3 Agent together with the appropriate users, authentication and privacy types and passphrases. These will be used for the corresponding entries in the Network Sentry appliance.

SNMPv2 Agent

ZoneDirector supports SNMPv2 agent. Enter the Read-Only and Read-Write communities.

Enable SNMP Agent

System Contact*

System Location*

SNMP RO community*

SNMP RW community*

SNMPv3 Agent

ZoneDirector supports SNMPv3 agent.

Enable SNMPv3 Agent

Privilege	User	Authentication	Auth Pass Phrase	Privacy	Privacy Phrase
Read Only	<input type="text" value="admin"/>	MDS ▾	<input type="text" value="bradford"/>	DES ▾	<input type="text" value="bradford"/>
Read/Write	<input type="text" value="admin"/>	MDS ▾	<input type="text" value="bradford"/>	DES ▾	<input type="text" value="bradford"/>

SNMP Trap

Enter the SNMP Trap server IP where ZoneDirector will send SNMP Traps to.

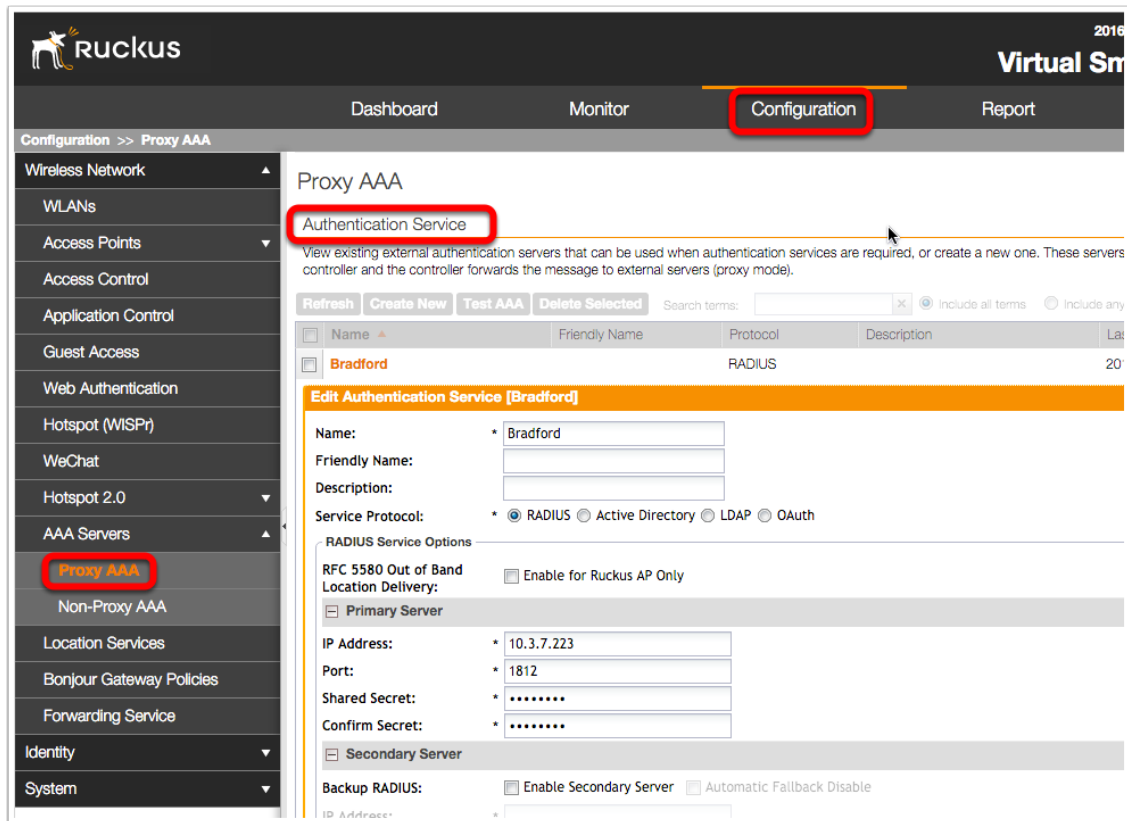
Ruckus SmartZone Setup (SZ100, vSZ-E)

This involves the following:

1. Setting up the Network Sentry Appliance as the Radius and Radius Accounting Server
2. Setting up the Production and Isolation SSIDs/WLANs (the latter as a dummy).
3. Enabling SNMP with the appropriate accounts/passphrases.

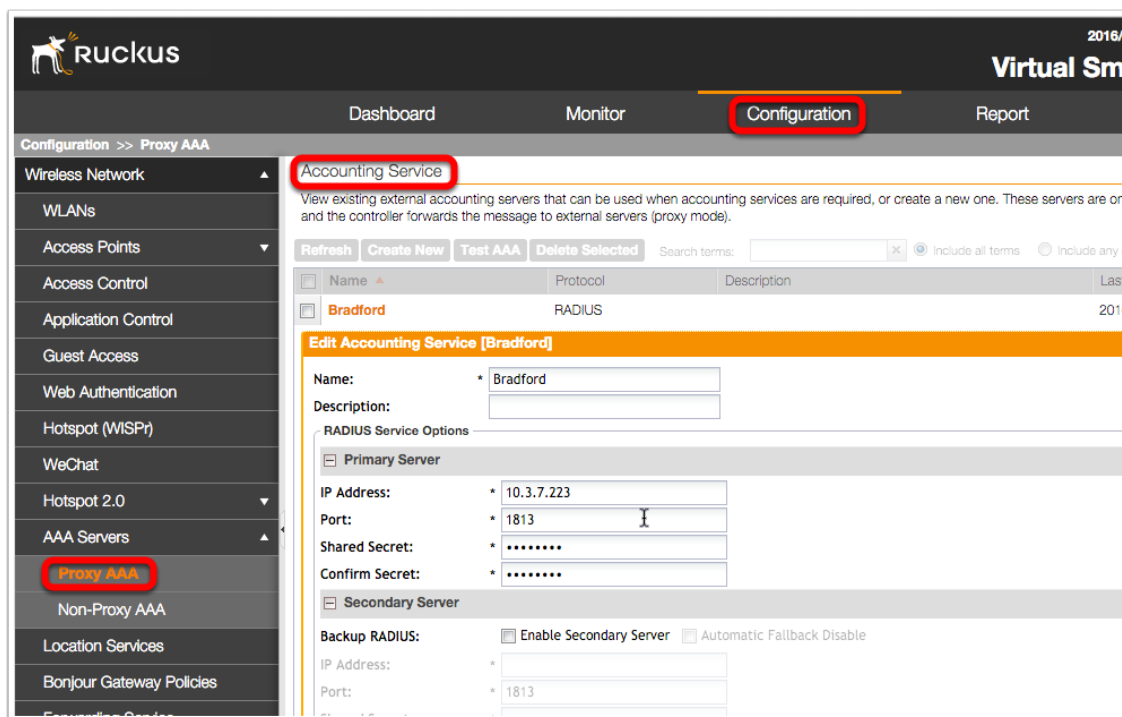
Network Sentry as Radius Server

From Configuration->AAA Servers->Proxy AAA, setup the Network Sentry Appliance as the Radius as well as Radius Accounting Server as shown below.



The screenshot shows the Ruckus configuration interface. The top navigation bar includes 'Dashboard', 'Monitor', 'Configuration' (highlighted with a red box), and 'Report'. The left sidebar lists various configuration categories, with 'Proxy AAA' highlighted in red. The main content area is titled 'Proxy AAA' and contains an 'Authentication Service' section, also highlighted in red. Below this, there is a table of authentication services with one entry named 'Bradford' using the 'RADIUS' protocol. The 'Edit Authentication Service [Bradford]' form is visible, showing fields for Name, Friendly Name, Description, Service Protocol (RADIUS selected), and RADIUS Service Options (IP Address: 10.3.7.223, Port: 1812, Shared Secret, Confirm Secret).

Network Sentry as Radius Accounting Server



The screenshot shows the Ruckus NMS Configuration page for Accounting Service. The interface includes a top navigation bar with 'Dashboard', 'Monitor', 'Configuration', and 'Report'. The left sidebar lists various configuration categories, with 'Proxy AAA' highlighted. The main content area is titled 'Accounting Service' and contains a table of existing services. Below the table is the 'Edit Accounting Service [Bradford]' form, which includes fields for Name, Description, RADIUS Service Options (Primary and Secondary Servers), and Backup RADIUS settings.

Configuration >> Proxy AAA

Accounting Service

View existing external accounting servers that can be used when accounting services are required, or create a new one. These servers are on and the controller forwards the message to external servers (proxy mode).

Refresh Create New Test AAA Delete Selected Search terms: [] Include all terms Include any c

Name	Protocol	Description	Last
Bradford	RADIUS		2014

Edit Accounting Service [Bradford]

Name: * Bradford

Description:

RADIUS Service Options

Primary Server

IP Address: * 10.3.7.223

Port: * 1813

Shared Secret: *

Confirm Secret: *

Secondary Server

Backup RADIUS: Enable Secondary Server Automatic Fallback Disable

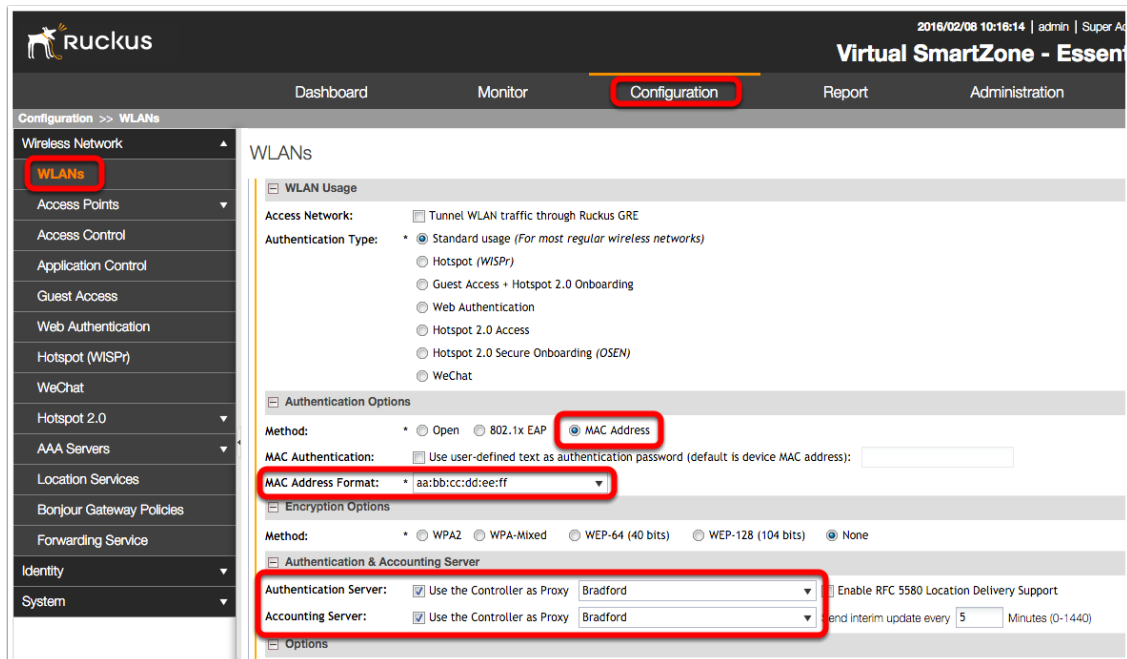
IP Address: *

Port: * 1813

Production SSID/WLAN

Setup the Production SSID with the following:

1. MAC Authentication and MAC Address format as aa:bb:cc:dd:ee:ff
2. Network Sentry as the Radius and Radius Accounting Server.
3. Dynamic VLAN (VLAN Override)



2016/02/08 10:16:14 | admin | Super Ad

Virtual SmartZone - Essen

Dashboard Monitor **Configuration** Report Administration

Configuration >> WLANs

Wireless Network

- WLANs**
- Access Points
- Access Control
- Application Control
- Guest Access
- Web Authentication
- Hotspot (WISPr)
- WeChat
- Hotspot 2.0
- AAA Servers
- Location Services
- Bonjour Gateway Policies
- Forwarding Service
- Identity
- System

WLANs

WLAN Usage

Access Network: Tunnel WLAN traffic through Ruckus GRE

Authentication Type: Standard usage (For most regular wireless networks)

- Hotspot (WISPr)
- Guest Access + Hotspot 2.0 Onboarding
- Web Authentication
- Hotspot 2.0 Access
- Hotspot 2.0 Secure Onboarding (OSEN)
- WeChat

Authentication Options

Method: Open 802.1x EAP MAC Address

MAC Authentication: Use user-defined text as authentication password (default is device MAC address):

MAC Address Format:

Encryption Options

Method: WPA2 WPA-Mixed WEP-64 (40 bits) WEP-128 (104 bits) None

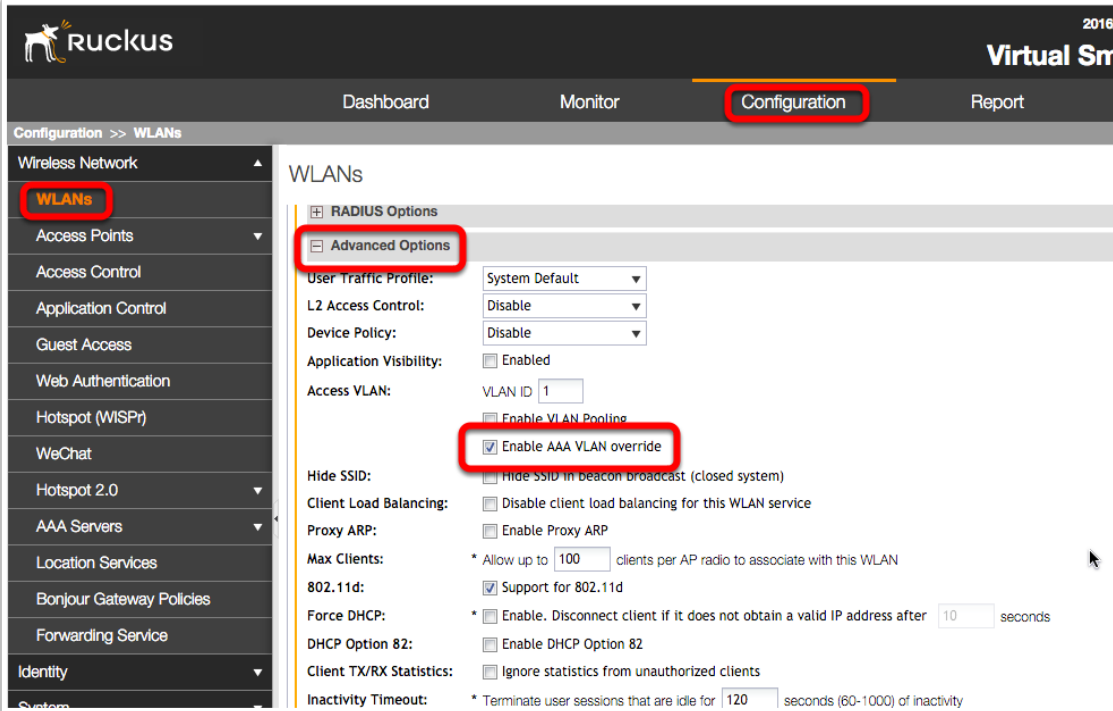
Authentication & Accounting Server

Authentication Server: Use the Controller as Proxy Enable RFC 5580 Location Delivery Support

Accounting Server: Use the Controller as Proxy Send interim update every Minutes (0-1440)

Options

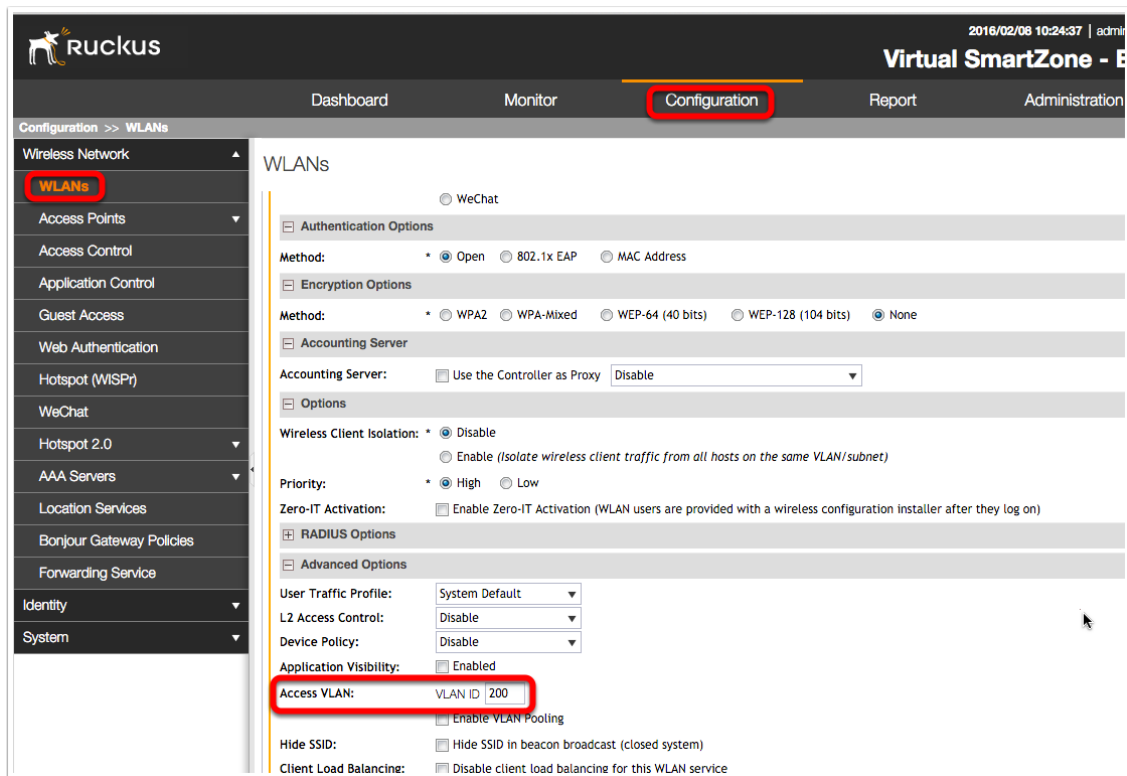
Enable VLAN Override in Advanced Options



The screenshot shows the Ruckus configuration interface. The top navigation bar includes 'Dashboard', 'Monitor', 'Configuration' (highlighted), and 'Report'. The left sidebar shows a tree view under 'Wireless Network' with 'WLANs' selected. The main content area is titled 'WLANs' and contains two sections: 'RADIUS Options' and 'Advanced Options'. The 'Advanced Options' section is expanded, showing various settings. The 'Enable AAA VLAN override' checkbox is checked and highlighted with a red box. Other settings include 'User Traffic Profile' (System Default), 'L2 Access Control' (Disable), 'Device Policy' (Disable), 'Application Visibility' (Enabled), 'Access VLAN' (VLAN ID 1), 'Hide SSID' (Hide SSID in beacon broadcast), 'Client Load Balancing' (Disable client load balancing), 'Proxy ARP' (Enable Proxy ARP), 'Max Clients' (100), '802.11d' (Support for 802.11d), 'Force DHCP' (Enable), 'DHCP Option 82' (Enable DHCP Option 82), 'Client TX/RX Statistics' (Ignore statistics from unauthorized clients), and 'Inactivity Timeout' (120 seconds).

Isolation SSID/WLAN

Setup the Isolation SSID as any type and assign it the Isolation VLAN. This is a dummy WLAN and needs to be removed from the Default WLAN Group, so that it is not broadcast over the air.



2016/02/08 10:24:37 | admin

Virtual SmartZone - B

Dashboard Monitor **Configuration** Report Administration

Configuration >> WLANs

Wireless Network

WLANs

Access Points

Access Control

Application Control

Guest Access

Web Authentication

Hotspot (WISPr)

WeChat

Hotspot 2.0

AAA Servers

Location Services

Bonjour Gateway Policies

Forwarding Service

Identity

System

WLANs

WeChat

Authentication Options

Method: Open 802.1x EAP MAC Address

Encryption Options

Method: WPA2 WPA-Mixed WEP-64 (40 bits) WEP-128 (104 bits) None

Accounting Server

Accounting Server: Use the Controller as Proxy

Options

Wireless Client Isolation: Disable
 Enable (isolate wireless client traffic from all hosts on the same VLAN/subnet)

Priority: High Low

Zero-IT Activation: Enable Zero-IT Activation (WLAN users are provided with a wireless configuration installer after they log on)

RADIUS Options

Advanced Options

User Traffic Profile:

L2 Access Control:

Device Policy:

Application Visibility: Enabled

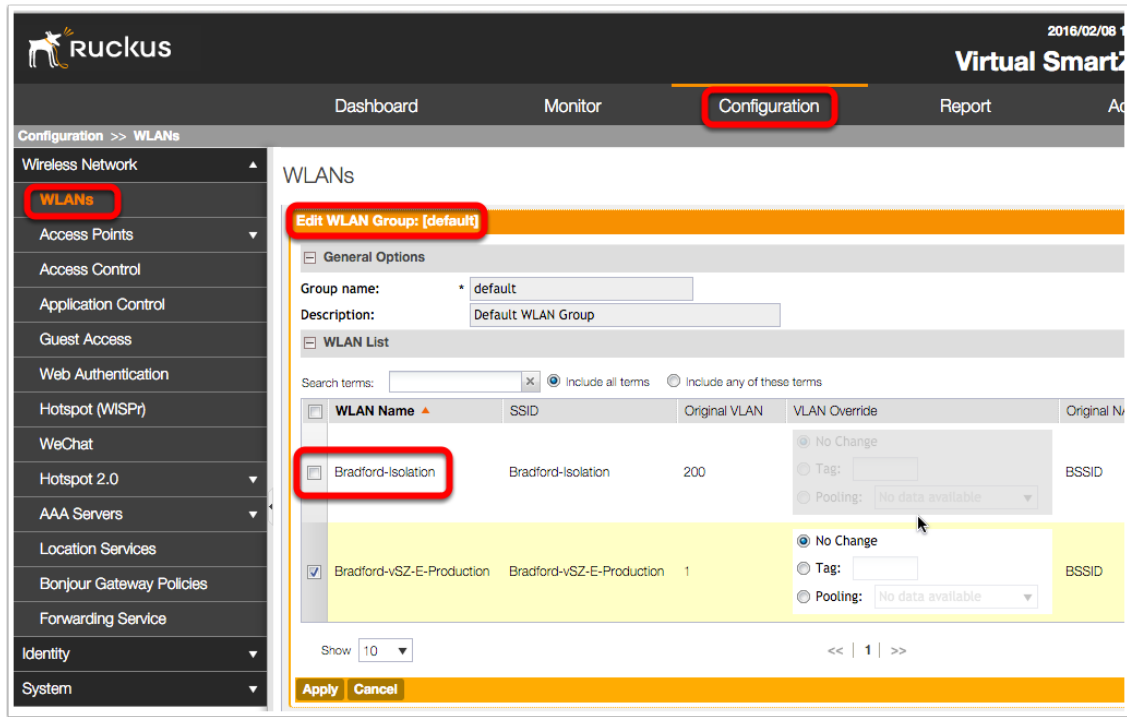
Access VLAN:

Enable VLAN Pooling

Hide SSID: Hide SSID in beacon broadcast (closed system)

Client Load Balancing: Disable client load balancing for this WLAN service

Remove Isolation WLAN from Default Group



2016/02/08 1
Virtual SmartZone

Dashboard Monitor **Configuration** Report Ad

Configuration >> WLANs

Wireless Network
WLANs
Access Points
Access Control
Application Control
Guest Access
Web Authentication
Hotspot (WISPr)
WeChat
Hotspot 2.0
AAA Servers
Location Services
Bonjour Gateway Policies
Forwarding Service
Identity
System

WLANs

Edit WLAN Group: [default]

General Options

Group name: default
Description: Default WLAN Group

WLAN List

Search terms: [x] Include all terms Include any of these terms

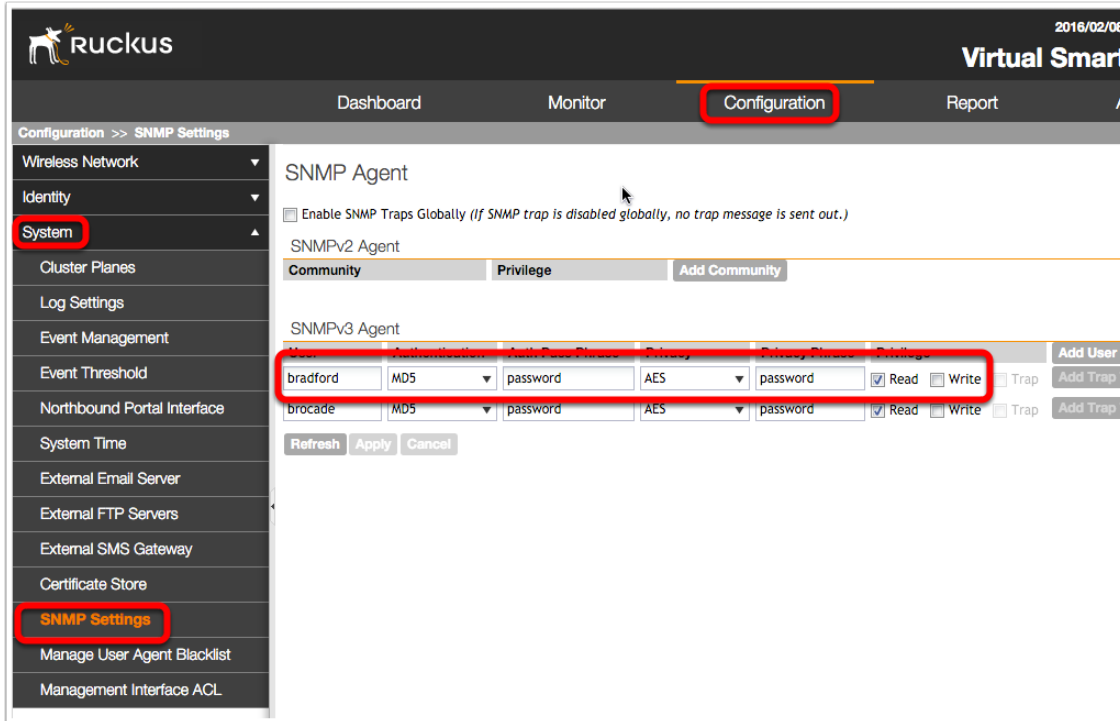
<input type="checkbox"/>	WLAN Name	SSID	Original VLAN	VLAN Override	Original N
<input type="checkbox"/>	Bradford-Isolation	Bradford-Isolation	200	<input checked="" type="radio"/> No Change <input type="radio"/> Tag: [] <input type="radio"/> Pooling: No data available	BSSID
<input checked="" type="checkbox"/>	Bradford-vSZ-E-Production	Bradford-vSZ-E-Production	1	<input checked="" type="radio"/> No Change <input type="radio"/> Tag: [] <input type="radio"/> Pooling: No data available	BSSID

Show 10 << | 1 | >>

Apply Cancel

Enable SNMP

Enable the v3 SNMP Agent as shown below.



The screenshot shows the Ruckus SmartZone configuration interface. The 'Configuration' tab is selected and highlighted with a red box. The left sidebar shows 'System' and 'SNMP Settings' highlighted with red boxes. The main content area is titled 'SNMP Agent' and includes the following settings:

- Enable SNMP Traps Globally (if SNMP trap is disabled globally, no trap message is sent out.)
- SNMPv2 Agent
 - Community: [tabbed]
 - Privilege: [tabbed]
 - Add Community: [button]
- SNMPv3 Agent
 - User: bradford
 - Authentication: MD5
 - Auth Pass Phrase: password
 - Privacy: AES
 - Privacy Pass Phrase: password
 - Read:
 - Write:
 - Trap:
 - Add User: [button]
 - brocade
 - MD5
 - password
 - AES
 - password
 - Read:
 - Write:
 - Trap:
 - Add Trap: [button]
- Buttons: Refresh, Apply, Cancel

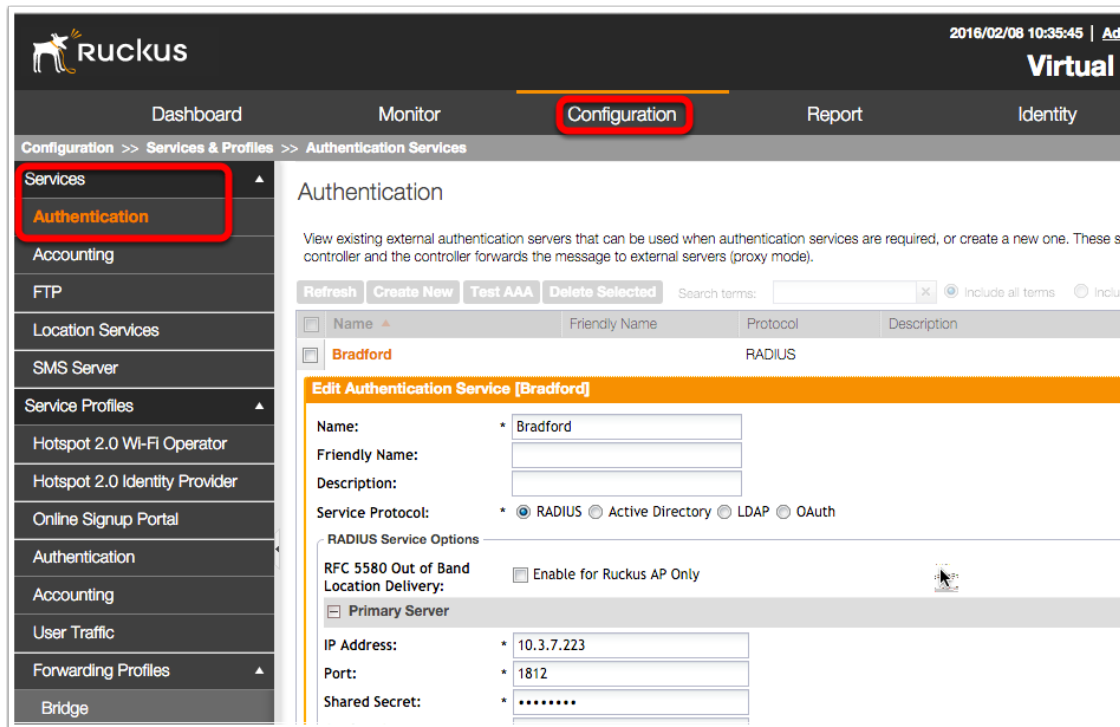
Ruckus Smartzone (vSZ-H, SCG200) Setup

This involves the following:

1. Setting up the Network Sentry Appliance as the Radius and Radius Accounting Server
2. Setting up the Production and Isolation SSIDs/WLANs (the latter as a dummy).
3. Enabling SNMP with the appropriate accounts/passphrases.

Network Sentry as Radius Server

As shown below, (a) Under Services, setup Network Sentry as the Radius Server and (b) Enable the Authentication Profile under Service Profiles.



The screenshot shows the Ruckus configuration interface. The top navigation bar includes 'Dashboard', 'Monitor', 'Configuration' (highlighted with a red box), 'Report', and 'Identity'. The breadcrumb trail is 'Configuration >> Services & Profiles >> Authentication Services'. The left sidebar menu has 'Authentication' highlighted with a red box. The main content area is titled 'Authentication' and contains a table of existing services. One service, 'Bradford', is selected and its configuration is shown in an 'Edit Authentication Service [Bradford]' form. The form includes fields for Name, Friendly Name, Description, Service Protocol (RADIUS is selected), and RADIUS Service Options (RFC 5580 Out of Band Location Delivery, Primary Server, IP Address, Port, and Shared Secret).

Name	Friendly Name	Protocol	Description
Bradford		RADIUS	

Edit Authentication Service [Bradford]

Name: * Bradford
Friendly Name:
Description:
Service Protocol: * RADIUS Active Directory LDAP OAuth

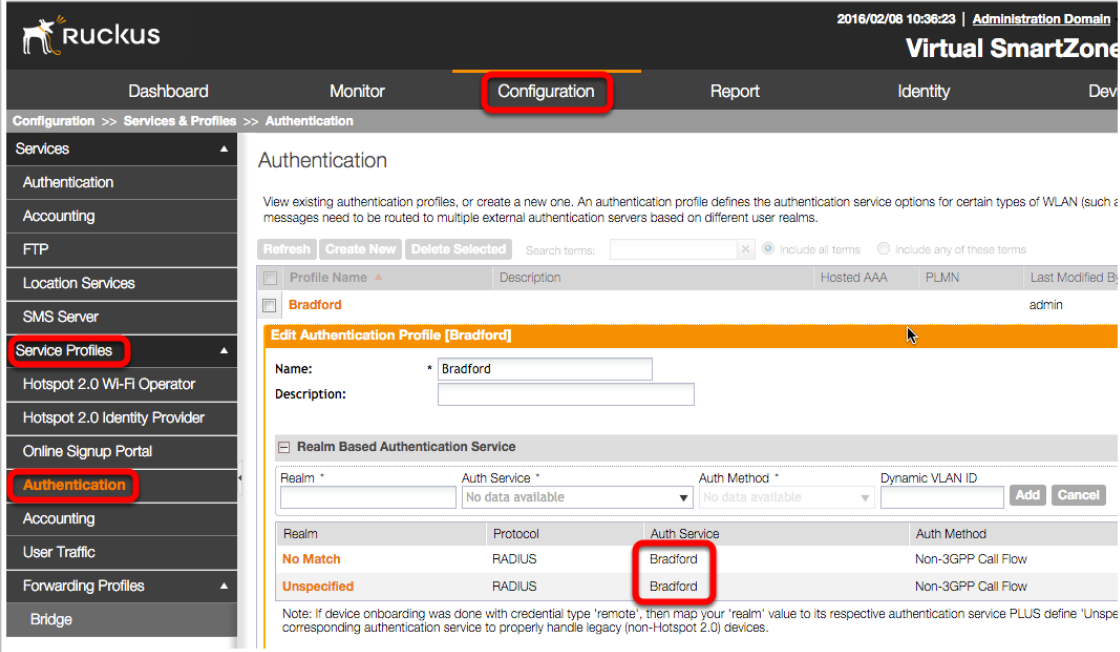
RADIUS Service Options

RFC 5580 Out of Band Location Delivery: Enable for Ruckus AP Only

Primary Server

IP Address: * 10.3.7.223
Port: * 1812
Shared Secret: *

Authentication Service Profile



2016/02/08 10:38:23 | Administration Domain

Virtual SmartZone

Dashboard Monitor **Configuration** Report Identity Dev

Configuration >> Services & Profiles >> Authentication

Services

- Authentication
- Accounting
- FTP
- Location Services
- SMS Server
- Service Profiles**
- Hotspot 2.0 Wi-Fi Operator
- Hotspot 2.0 Identity Provider
- Online Signup Portal
- Authentication**
- Accounting
- User Traffic
- Forwarding Profiles
- Bridge

Authentication

View existing authentication profiles, or create a new one. An authentication profile defines the authentication service options for certain types of WLAN (such as Hotspot 2.0) and messages need to be routed to multiple external authentication servers based on different user realms.

Refresh Create New Delete Selected Search terms: X Include all terms Include any of these terms

Profile Name	Description	Hosted AAA	PLMN	Last Modified By
<input type="checkbox"/> Bradford				admin

Edit Authentication Profile [Bradford]

Name: *

Description:

Realm Based Authentication Service

Realm * Auth Service * Auth Method * Dynamic VLAN ID

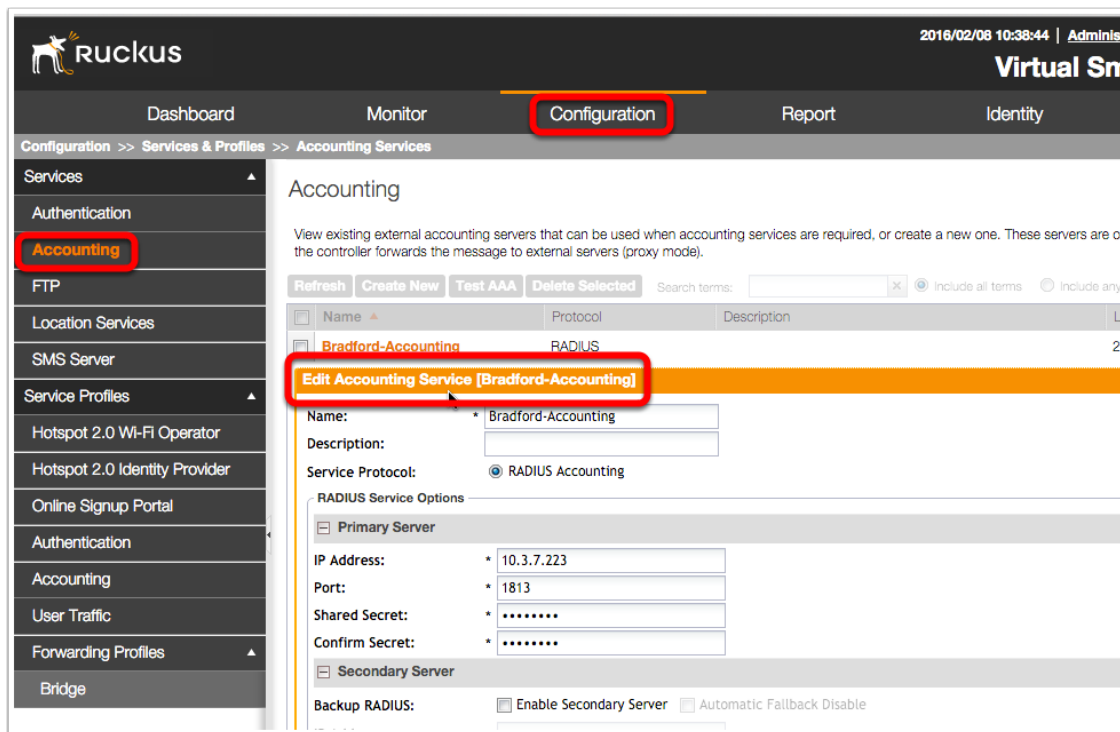
No data available No data available

Realm	Protocol	Auth Service	Auth Method
No Match	RADIUS	Bradford	Non-3GPP Call Flow
Unspecified	RADIUS	Bradford	Non-3GPP Call Flow

Note: If device onboarding was done with credential type 'remote', then map your 'realm' value to its respective authentication service PLUS define 'Unspecified' corresponding authentication service to properly handle legacy (non-Hotspot 2.0) devices.

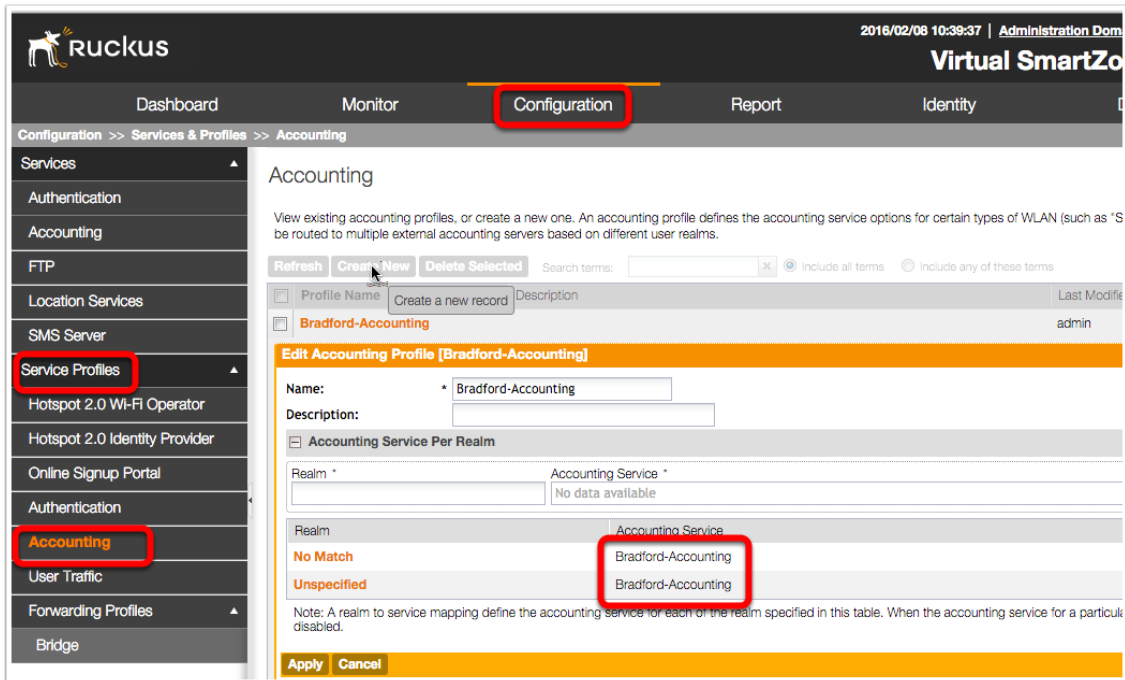
Network Sentry as Radius Accounting Server

Under Services, setup Network Sentry as a Radius Accounting Server and under Service Profiles, enable the Accounting Profile.



The screenshot shows the Ruckus Network Manager interface. The top navigation bar includes 'Dashboard', 'Monitor', 'Configuration' (highlighted with a red box), 'Report', and 'Identity'. The breadcrumb trail is 'Configuration >> Services & Profiles >> Accounting Services'. On the left sidebar, 'Accounting' is highlighted with a red box. The main content area is titled 'Accounting' and contains a table of existing accounting servers. One server, 'Bradford-Accounting', is selected and highlighted with a red box. Below the table, the 'Edit Accounting Service [Bradford-Accounting]' form is visible. The form includes fields for 'Name' (Bradford-Accounting), 'Description', and 'Service Protocol' (RADIUS Accounting). Under 'RADIUS Service Options', the 'Primary Server' section is expanded, showing fields for 'IP Address' (10.3.7.223), 'Port' (1813), 'Shared Secret', and 'Confirm Secret'. The 'Secondary Server' section is collapsed. At the bottom, there are checkboxes for 'Enable Secondary Server' and 'Automatic Falback Disable'.

Accounting Service Profile



2016/02/08 10:39:37 | Administration Dom
Virtual SmartZone

Dashboard Monitor **Configuration** Report Identity

Configuration >> Services & Profiles >> Accounting

Services

- Authentication
- Accounting
- FTP
- Location Services
- SMS Server
- Service Profiles**
- Hotspot 2.0 Wi-Fi Operator
- Hotspot 2.0 Identity Provider
- Online Signup Portal
- Authentication
- Accounting**
- User Traffic
- Forwarding Profiles
- Bridge

Accounting

View existing accounting profiles, or create a new one. An accounting profile defines the accounting service options for certain types of WLAN (such as "S" be routed to multiple external accounting servers based on different user realms.

Refresh Create New Delete Selected Search terms: [] [x] [] include all terms [] include any of these terms

Profile Name	Create a new record	Description	Last Modified
Bradford-Accounting			admin

Edit Accounting Profile [Bradford-Accounting]

Name: * Bradford-Accounting

Description: []

Accounting Service Per Realm

Realm *	Accounting Service *
[]	No data available
Realms	Accounting Service
No Match	Bradford-Accounting
Unspecified	Bradford-Accounting

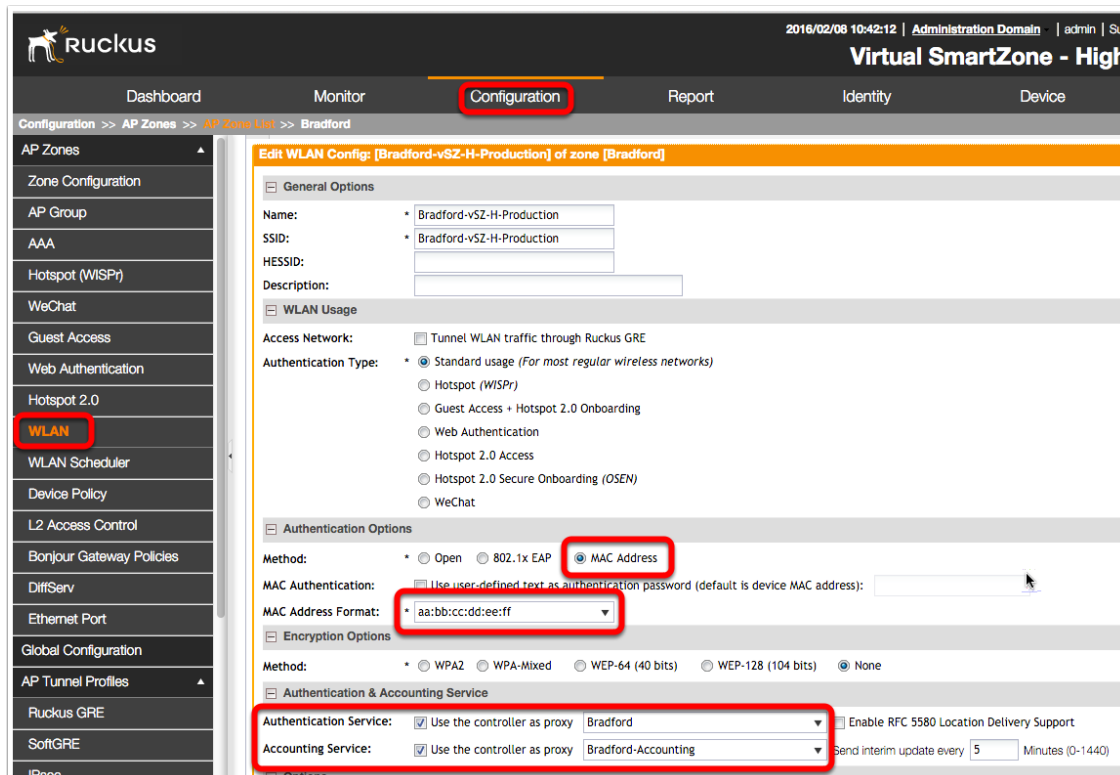
Note: A realm to service mapping define the accounting service for each of the realm specified in this table. When the accounting service for a particular realm is disabled.

Apply Cancel

Production SSID/WLAN

Under the desired Zone, setup the Production SSID/WLAN with

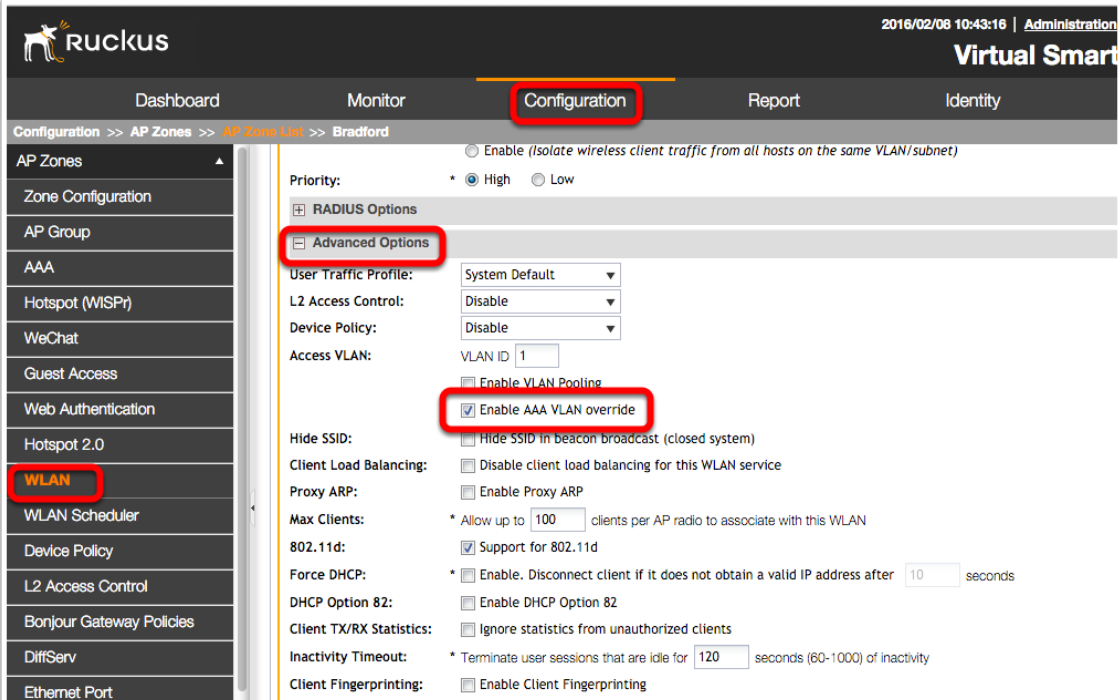
1. MAC Authentication and MAC Address format as aa:bb:cc:dd:ee:ff
2. Network Sentry as the Radius and Radius Accounting Server.
3. Dynamic VLAN (VLAN Override)



The screenshot shows the Ruckus configuration interface for a Virtual SmartZone - High. The 'Configuration' tab is selected, and the 'WLAN' option in the left sidebar is highlighted. The main content area displays the 'Edit WLAN Config' for a zone named 'Bradford'. The configuration is as follows:

- General Options:**
 - Name: Bradford-vSZ-H-Production
 - SSID: Bradford-vSZ-H-Production
 - HESSID: (empty)
 - Description: (empty)
- WLAN Usage:**
 - Access Network: Tunnel WLAN traffic through Ruckus GRE
 - Authentication Type: Standard usage (For most regular wireless networks)
 - Hotspot (WISPr)
 - Guest Access + Hotspot 2.0 Onboarding
 - Web Authentication
 - Hotspot 2.0 Access
 - Hotspot 2.0 Secure Onboarding (OSEN)
 - WeChat
- Authentication Options:**
 - Method: Open 802.1x EAP MAC Address
 - MAC Authentication: Use user-defined text as authentication password (default is device MAC address): (empty)
 - MAC Address Format: aa:bb:cc:dd:ee:ff
- Encryption Options:**
 - Method: WPA2 WPA-Mixed WEP-64 (40 bits) WEP-128 (104 bits) None
- Authentication & Accounting Service:**
 - Authentication Service: Use the controller as proxy Bradford Enable RFC 5580 Location Delivery Support
 - Accounting Service: Use the controller as proxy Bradford-Accounting Send interim update every 5 Minutes (0-1440)

Enable VLAN Override in Advanced options



2016/02/08 10:43:16 | Administration

Virtual SmartZone

Dashboard Monitor **Configuration** Report Identity

Configuration >> AP Zones >> AP Zone List >> Bradford

AP Zones

- Zone Configuration
- AP Group
- AAA
- Hotspot (WISPr)
- WeChat
- Guest Access
- Web Authentication
- Hotspot 2.0
- WLAN**
- WLAN Scheduler
- Device Policy
- L2 Access Control
- Bonjour Gateway Policies
- DiffServ
- Ethernet Port

Enable (Isolate wireless client traffic from all hosts on the same VLAN/subnet)

Priority: * High Low

Advanced Options

User Traffic Profile: System Default

L2 Access Control: Disable

Device Policy: Disable

Access VLAN: VLAN ID 1

Enable VLAN Pooling

Enable AAA VLAN override

Hide SSID: Hide SSID in beacon broadcast (closed system)

Client Load Balancing: Disable client load balancing for this WLAN service

Proxy ARP: Enable Proxy ARP

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

802.11d: Support for 802.11d

Force DHCP: * Enable. Disconnect client if it does not obtain a valid IP address after 10 seconds

DHCP Option 82: Enable DHCP Option 82

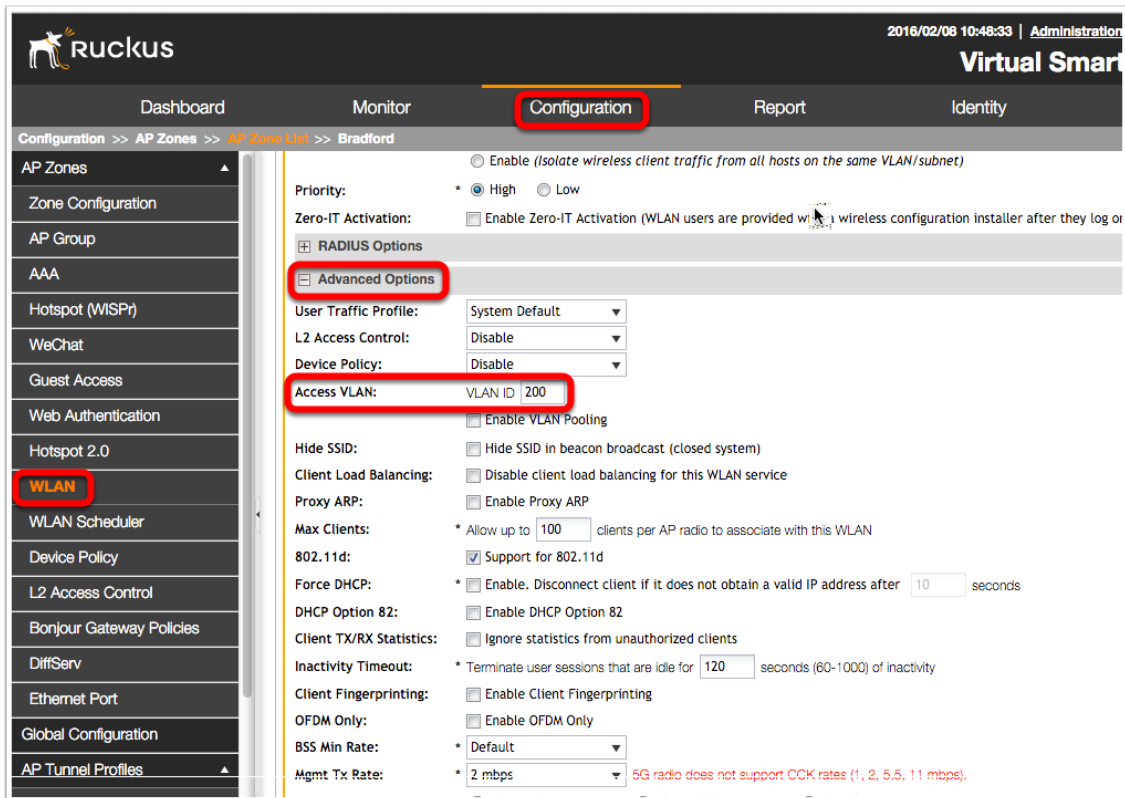
Client TX/RX Statistics: Ignore statistics from unauthorized clients

Inactivity Timeout: * Terminate user sessions that are idle for 120 seconds (60-1000) of inactivity

Client Fingerprinting: Enable Client Fingerprinting

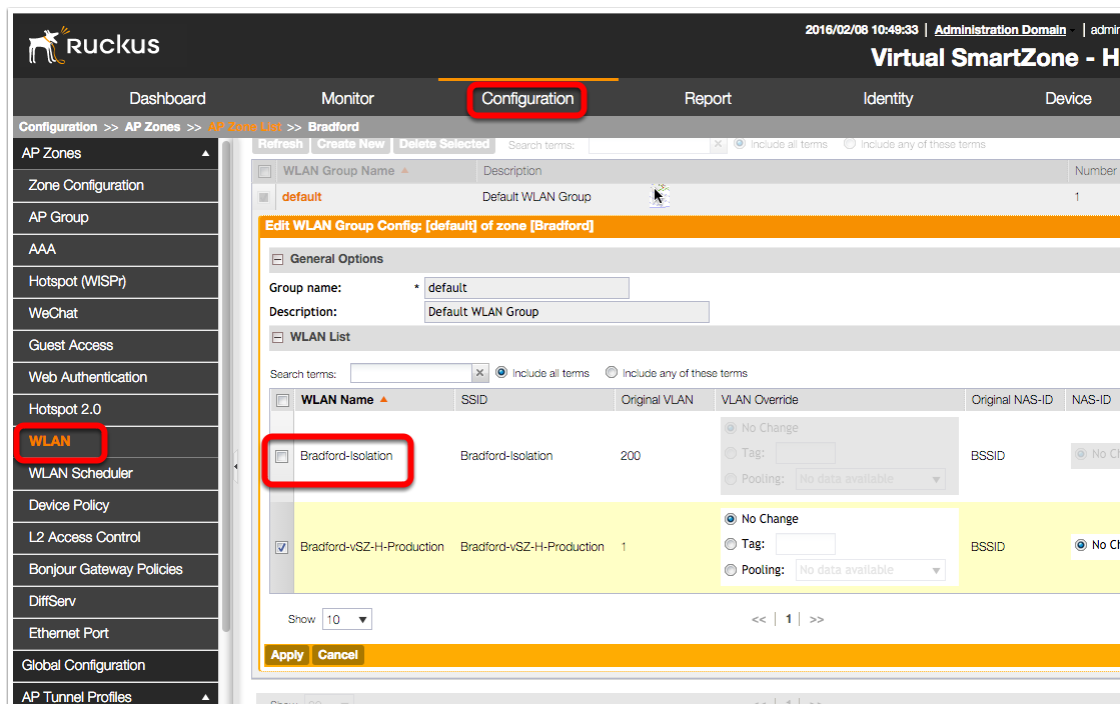
Isolation SSID/WLAN

Setup a dummy SSID/WLAN for Isolation of any type and assign it the appropriate VLAN under Advanced Options



The screenshot shows the Ruckus configuration interface. The top navigation bar includes 'Dashboard', 'Monitor', 'Configuration' (highlighted with a red box), 'Report', and 'Identity'. The breadcrumb trail is 'Configuration >> AP Zones >> AP Zone List >> Bradford'. The left sidebar lists various configuration categories, with 'WLAN' highlighted in orange. The main content area shows the configuration for a specific WLAN. The 'Advanced Options' section is expanded and highlighted with a red box. Within this section, the 'Access VLAN' is set to 'VLAN ID 200' and is also highlighted with a red box. Other settings include: Priority: High; Zero-IT Activation: Disabled; User Traffic Profile: System Default; L2 Access Control: Disable; Device Policy: Disable; Hide SSID: Hide SSID in beacon broadcast (closed system); Client Load Balancing: Disable client load balancing for this WLAN service; Proxy ARP: Enable Proxy ARP; Max Clients: Allow up to 100 clients per AP radio to associate with this WLAN; 802.11d: Support for 802.11d; Force DHCP: Enable. Disconnect client if it does not obtain a valid IP address after 10 seconds; DHCP Option 82: Enable DHCP Option 82; Client TX/RX Statistics: Ignore statistics from unauthorized clients; Inactivity Timeout: Terminate user sessions that are idle for 120 seconds (60-1000) of inactivity; Client Fingerprinting: Enable Client Fingerprinting; OFDM Only: Enable OFDM Only; BSS Min Rate: Default; Mgmt Tx Rate: 2 mbps. A red note at the bottom right states: '5G radio does not support CCK rates (1, 2, 5.5, 11 mbps)'.

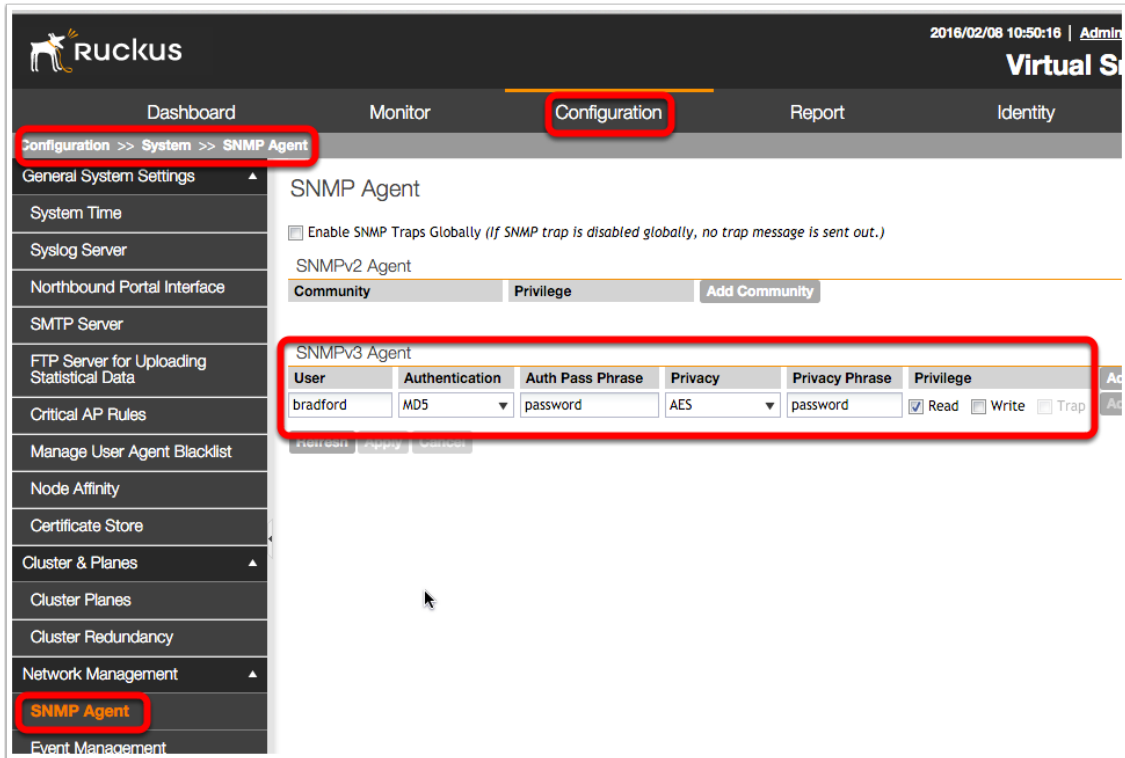
Remove Isolation WLAN from Default WLAN Group



The screenshot shows the Ruckus Virtual SmartZone configuration interface. The 'Configuration' tab is selected, and the 'WLAN' menu item in the left sidebar is highlighted. The main content area displays the 'Edit WLAN Group Config' for the 'default' group. The 'WLAN List' table is visible, with the 'Bradford-Isolation' entry selected. The table columns are: WLAN Name, SSID, Original VLAN, VLAN Override, Original NAS-ID, and NAS-ID.

WLAN Name	SSID	Original VLAN	VLAN Override	Original NAS-ID	NAS-ID
<input type="checkbox"/> Bradford-Isolation	Bradford-Isolation	200	<input type="radio"/> No Change Tag: <input type="text"/> Pooling: No data available	BSSID	<input type="radio"/> No Ch
<input checked="" type="checkbox"/> Bradford-vSZ-H-Production	Bradford-vSZ-H-Production	1	<input checked="" type="radio"/> No Change Tag: <input type="text"/> Pooling: No data available	BSSID	<input checked="" type="radio"/> No Ch

Enable SNMP



2016/02/08 10:50:16 | Admin

Virtual Switch

Dashboard Monitor **Configuration** Report Identity

Configuration >> System >> **SNMP Agent**

General System Settings

System Time

Syslog Server

Northbound Portal Interface

SMTP Server

FTP Server for Uploading Statistical Data

Critical AP Rules

Manage User Agent Blacklist

Node Affinity

Certificate Store

Cluster & Planes

Cluster Planes

Cluster Redundancy

Network Management

SNMP Agent

Event Management

SNMP Agent

Enable SNMP Traps Globally (If SNMP trap is disabled globally, no trap message is sent out.)

SNMPv2 Agent

Community Privilege Add Community

SNMPv3 Agent

User	Authentication	Auth Pass Phrase	Privacy	Privacy Phrase	Privilege
bradford	MD5	password	AES	password	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write <input type="checkbox"/> Trap

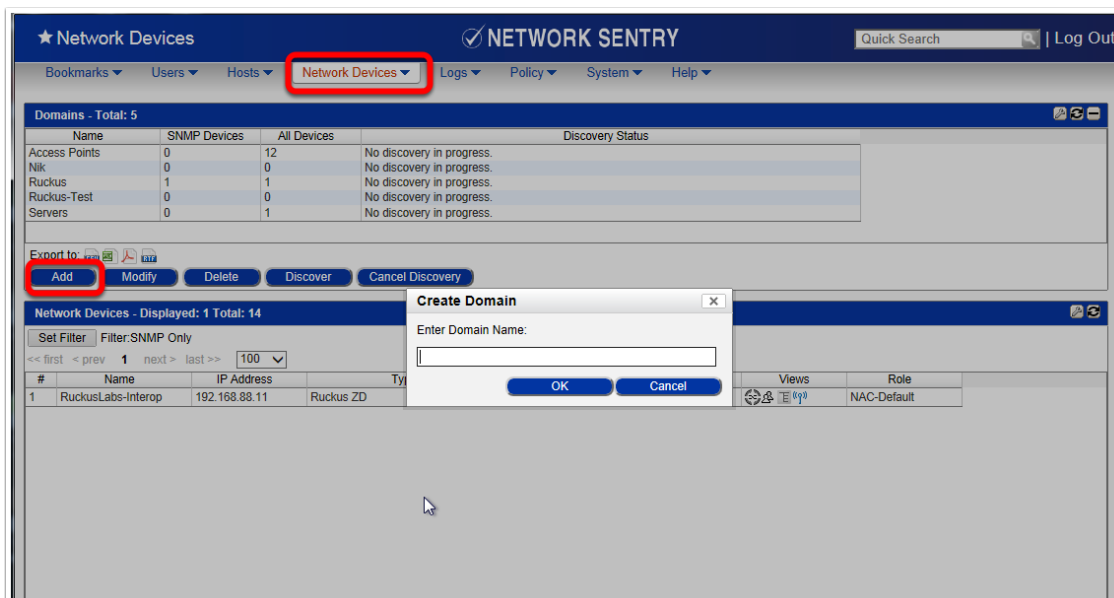
Network Sentry Setup

It is assumed that the Network Sentry Appliance has been setup and needs to be only configured for interoperability with the Ruckus Controllers/Access Points. The overall steps are:

1. Create new domain for Ruckus
2. Add Ruckus Controller (Zone Director or SmartZone) to this domain and model its configuration
3. Read VLANs from Zone Director
4. Set up Test User Accounts

Create Ruckus Domain

From Network Devices->Network Devices create a new domain called Ruckus.



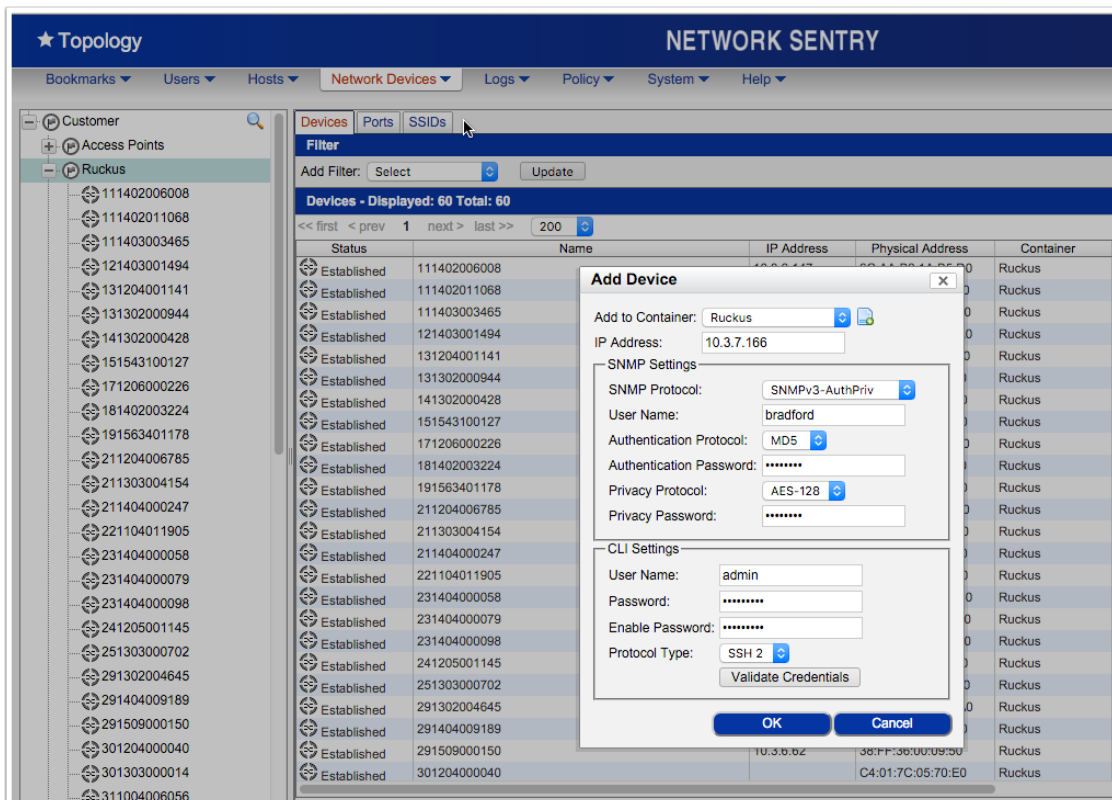
The screenshot shows the Network Sentry web interface. The top navigation bar includes 'Network Devices', 'Users', 'Hosts', 'Network Devices' (highlighted with a red box), 'Logs', 'Policy', 'System', and 'Help'. Below the navigation bar, there is a 'Domains - Total: 5' section with a table listing domains and their discovery status. Below the table, there are buttons for 'Add', 'Modify', 'Delete', 'Discover', and 'Cancel Discovery'. The 'Add' button is highlighted with a red box. A 'Create Domain' dialog box is open, prompting the user to 'Enter Domain Name:'. Below the dialog box, there is a table with columns for '#', 'Name', 'IP Address', and 'Type'. The table contains one entry: '1 RuckusLabs-Interop 192.168.88.11 Ruckus ZD'. To the right of the table, there are 'Views' and 'Role' sections.

Name	SNMP Devices	All Devices	Discovery Status
Access Points	0	12	No discovery in progress.
Nik	0	0	No discovery in progress.
Ruckus	1	1	No discovery in progress.
Ruckus-Test	0	0	No discovery in progress.
Servers	0	1	No discovery in progress.

#	Name	IP Address	Type
1	RuckusLabs-Interop	192.168.88.11	Ruckus ZD

Add Ruckus Controller

From Network Devices -> Topology, add the Ruckus Controller to the Ruckus Domain created above. The SNMP settings are those specified in the Ruckus controllers.

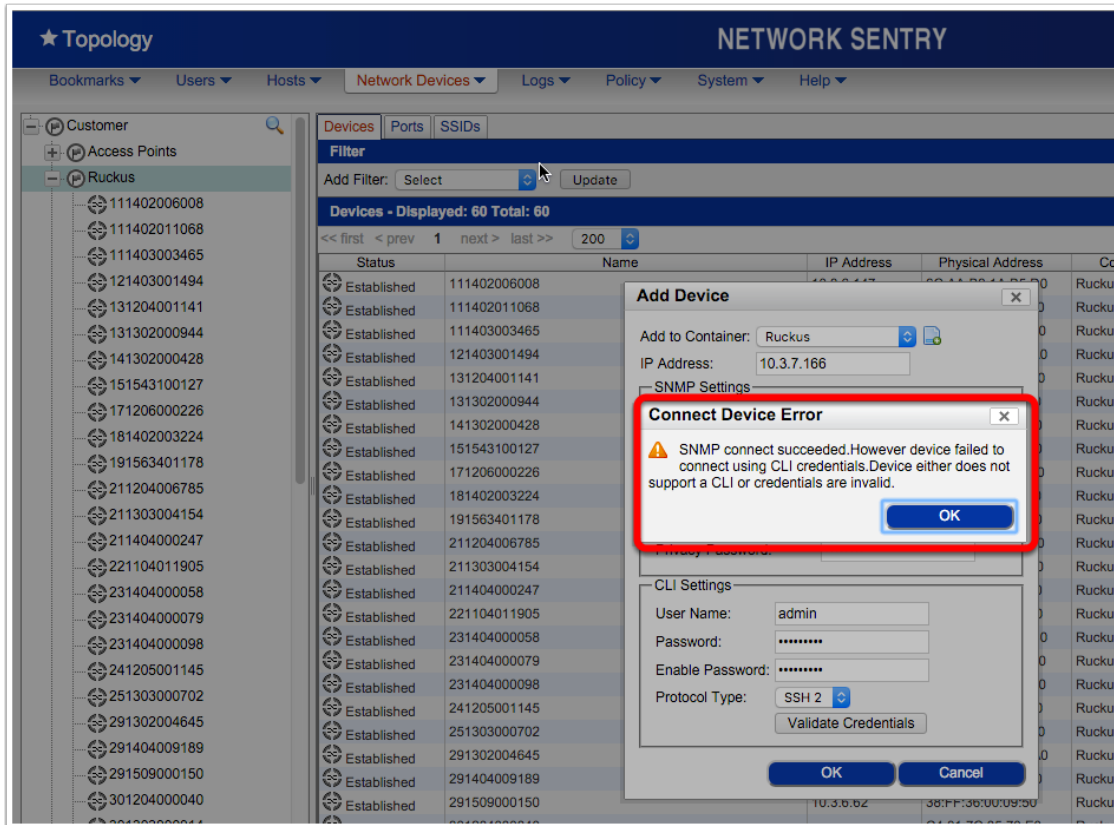


The screenshot shows the 'Network Sentry' interface with the 'Topology' view selected. A list of network devices is displayed under the 'Ruckus' container. An 'Add Device' dialog box is open, allowing the user to configure a new device. The dialog box includes the following fields and options:

- Add to Container:** Ruckus
- IP Address:** 10.3.7.166
- SNMP Settings:**
 - SNMP Protocol: SNMPv3-AuthPriv
 - User Name: bradford
 - Authentication Protocol: MD5
 - Authentication Password: *****
 - Privacy Protocol: AES-128
 - Privacy Password: *****
- CLI Settings:**
 - User Name: admin
 - Password: *****
 - Enable Password: *****
 - Protocol Type: SSH 2
 - Validate Credentials

The dialog box has 'OK' and 'Cancel' buttons at the bottom.

Validate Credentials and Ignore CLI Error Message

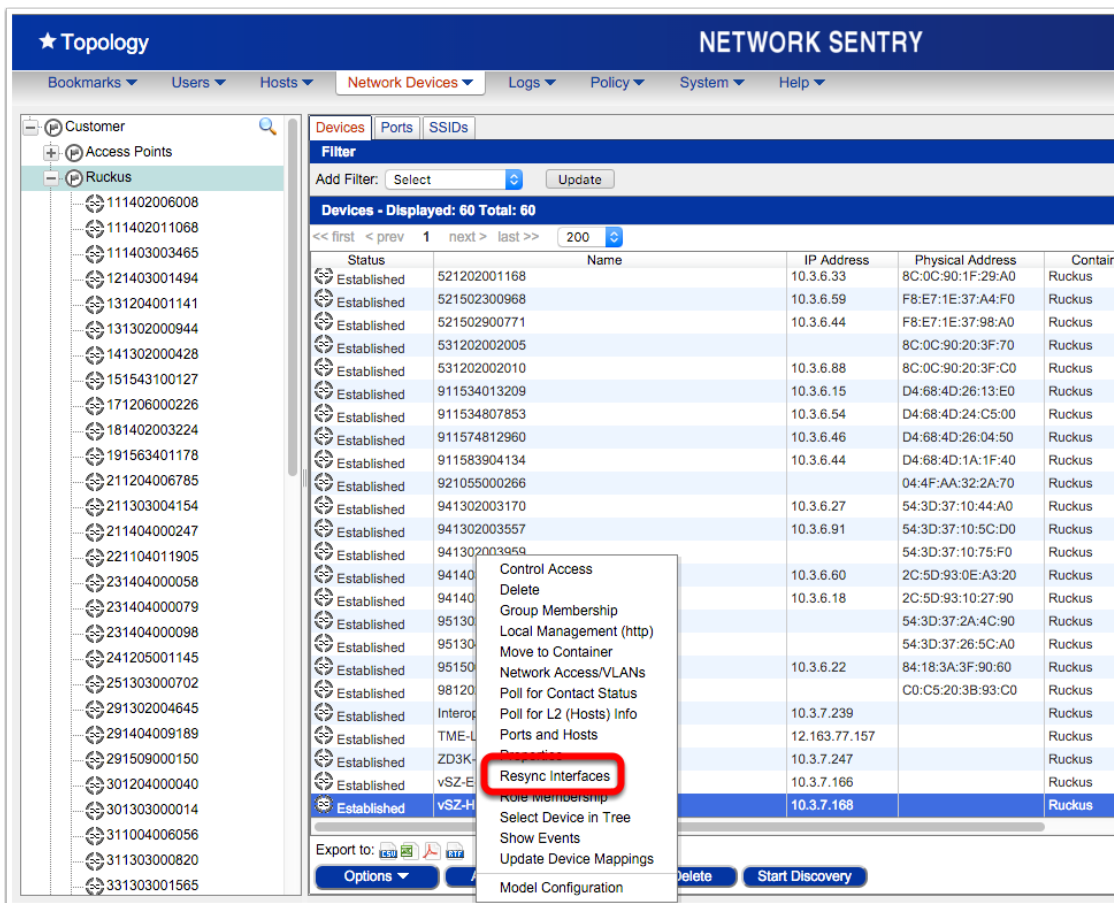


The screenshot shows the Ruckus Network Sentry interface. The main window displays a list of network devices with columns for Status, Name, IP Address, Physical Address, and Cor. A dialog box titled "Add Device" is open, showing fields for "Add to Container" (Ruckus), "IP Address" (10.3.7.166), and "SNMP Settings". Below these fields, a "Connect Device Error" dialog box is displayed, containing the message: "SNMP connect succeeded. However device failed to connect using CLI credentials. Device either does not support a CLI or credentials are invalid." The error dialog box has an "OK" button. The "Add Device" dialog box also has "OK" and "Cancel" buttons at the bottom.

Status	Name	IP Address	Physical Address	Cor
Established	111402006008			Ruckus
Established	111402011068			Ruckus
Established	111403003465			Ruckus
Established	121403001494			Ruckus
Established	131204001141			Ruckus
Established	131302000944			Ruckus
Established	141302000428			Ruckus
Established	151543100127			Ruckus
Established	171206000226			Ruckus
Established	181402003224			Ruckus
Established	191563401178			Ruckus
Established	211204006785			Ruckus
Established	211303004154			Ruckus
Established	211404000247			Ruckus
Established	221104011905			Ruckus
Established	231404000058			Ruckus
Established	231404000079			Ruckus
Established	231404000098			Ruckus
Established	241205001145			Ruckus
Established	251303000702			Ruckus
Established	291302004645			Ruckus
Established	291404009189			Ruckus
Established	291509000150			Ruckus
Established	301204000040			Ruckus

Read Controller Information

Once the Ruckus Controller has been created, read its information by right clicking and using "Resync Interfaces"



The screenshot shows the 'NETWORK SENTRY' interface. On the left, a tree view shows the hierarchy: Customer > Access Points > Ruckus. The main area displays a table of devices. A context menu is open over a device with IP 10.3.7.168, and the 'Resync Interfaces' option is highlighted with a red box.

Status	Name	IP Address	Physical Address	Container
Established	521202001168	10.3.6.33	8C:0C:90:1F:29:A0	Ruckus
Established	521502300968	10.3.6.59	F8:E7:1E:37:A4:F0	Ruckus
Established	521502900771	10.3.6.44	F8:E7:1E:37:98:A0	Ruckus
Established	531202002005		8C:0C:90:20:3F:70	Ruckus
Established	531202002010	10.3.6.88	8C:0C:90:20:3F:C0	Ruckus
Established	911534013209	10.3.6.15	D4:68:4D:26:13:E0	Ruckus
Established	911534807853	10.3.6.54	D4:68:4D:24:C5:00	Ruckus
Established	911574812960	10.3.6.46	D4:68:4D:26:04:50	Ruckus
Established	911583904134	10.3.6.44	D4:68:4D:1A:1F:40	Ruckus
Established	921055000266		04:4F:AA:32:2A:70	Ruckus
Established	941302003170	10.3.6.27	54:3D:37:10:44:A0	Ruckus
Established	941302003557	10.3.6.91	54:3D:37:10:5C:D0	Ruckus
Established	941302003959		54:3D:37:10:75:F0	Ruckus
Established	94140	10.3.6.60	2C:5D:93:0E:A3:20	Ruckus
Established	94140	10.3.6.18	2C:5D:93:10:27:90	Ruckus
Established	95130		54:3D:37:2A:4C:90	Ruckus
Established	95130		54:3D:37:26:5C:A0	Ruckus
Established	95150	10.3.6.22	84:18:3A:3F:90:60	Ruckus
Established	98120		C0:C5:20:3B:93:C0	Ruckus
Established	Interop	10.3.7.239		Ruckus
Established	TME-L	12.163.77.157		Ruckus
Established	ZD3K	10.3.7.247		Ruckus
Established	vSZ-E	10.3.7.166		Ruckus
Established	vSZ-H	10.3.7.168		Ruckus

Model Ruckus Controller

Now Model the Ruckus Controller (right click, Model Configuration) and enter all the appropriate information created earlier for the Radius shared secret and the VLAN assignments.

★ Ruckus Model Configuration NETWORK SE

Bookmarks ▾ Users ▾ Hosts ▾ Network Devices ▾ Logs ▾ Policy ▾ System ▾ Help ▾

General

User Name Password

Protocol

Type

RADIUS

Primary RADIUS Server (Not Set)

Secondary RADIUS Server (Not Set)

RADIUS Secret

Network Access

Read VLANs from Device

Host State	Access Enforcement	Access Value
Default		<input type="text" value="(None)"/>
Dead End	<input type="text" value="Enforce"/>	<input type="text" value="200"/>
Registration	<input type="text" value="Enforce"/>	<input type="text" value="200"/>
Quarantine	<input type="text" value="Enforce"/>	<input type="text" value="200"/>
Authentication	<input type="text" value="Enforce"/>	<input type="text" value="200"/>
Roaming Guest	<input type="text" value="Enforce"/>	<input type="text" value="200"/>

Access Enforcement Descriptions

Enforce: Hosts in the given state will be placed into the network designated by the selected access value.

Bypass: The given state will not be enforced. Other states may still apply.

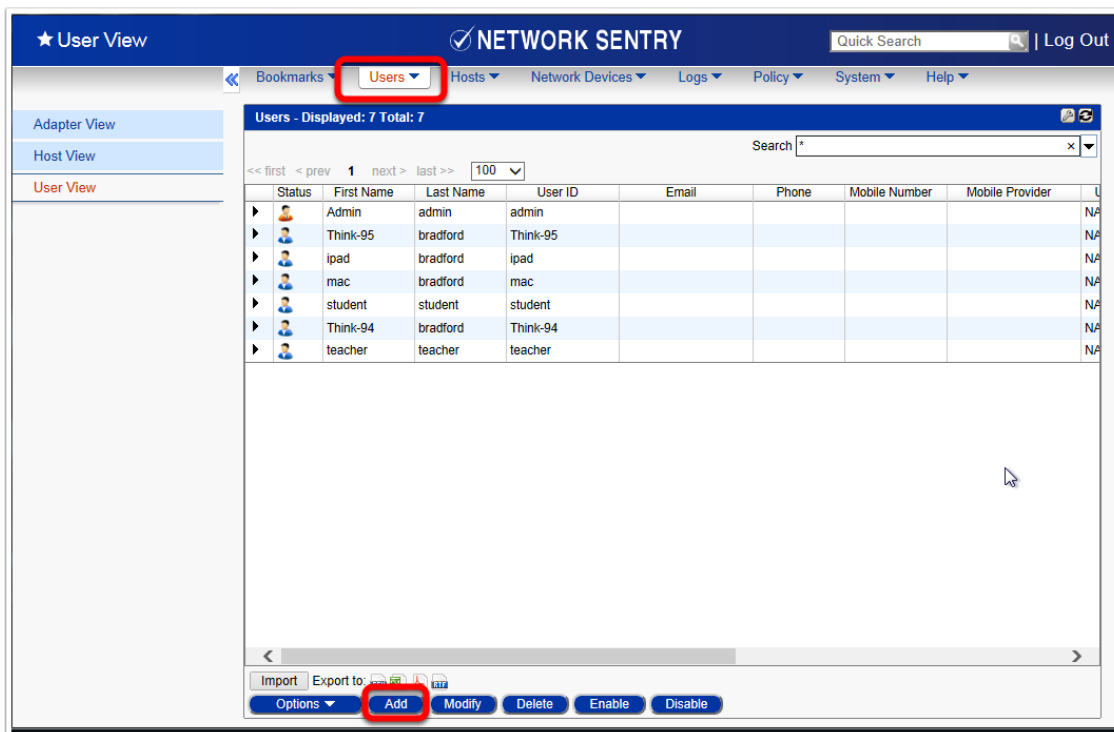
Deny: Hosts in the given state will not be granted access to the network.

Wireless AP parameters

Preferred Container Name:

Add Test User Accounts

Add some test user accounts as shown below.



★ User View NETWORK SENTRY Quick Search | Log Out

Bookmarks **Users** Hosts Network Devices Logs Policy System Help

Adapter View
Host View
User View

Users - Displayed: 7 Total: 7

Search *

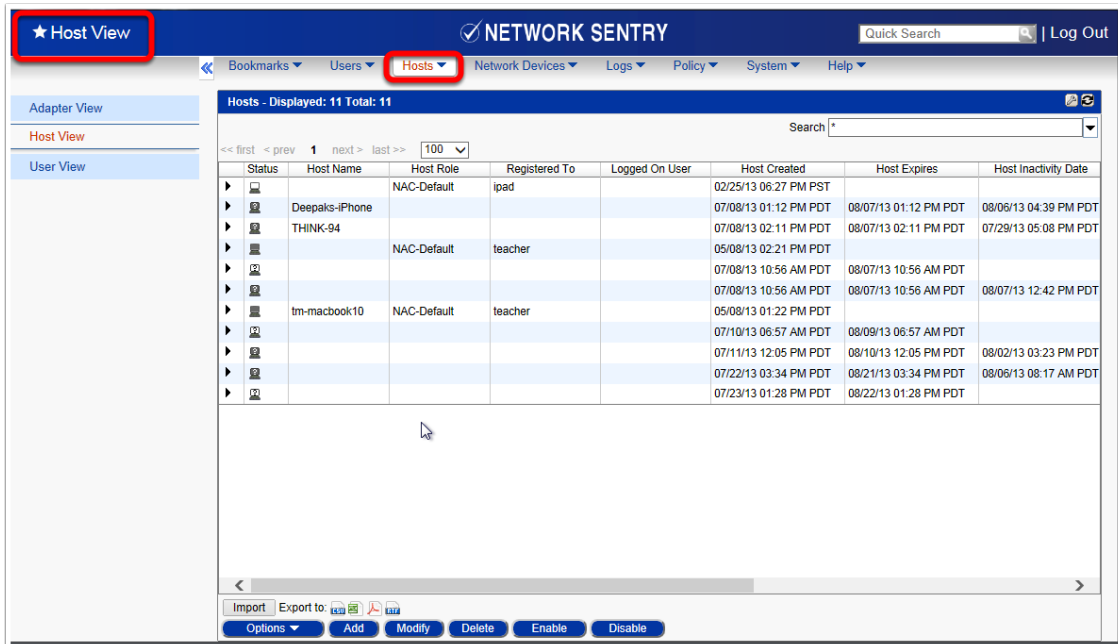
<< first < prev 1 next >> last >> 100

Status	First Name	Last Name	User ID	Email	Phone	Mobile Number	Mobile Provider	U
▶	Admin	admin	admin					NA
▶	Think-95	bradford	Think-95					NA
▶	ipad	bradford	ipad					NA
▶	mac	bradford	mac					NA
▶	student	student	student					NA
▶	Think-94	bradford	Think-94					NA
▶	teacher	teacher	teacher					NA

Import Export to Options **Add** Modify Delete Enable Disable

Test Clients

You can now test by connecting a client to the SSID. It will first be placed in the Isolation VLAN and the user will be asked for credentials (per the test accounts setup in the prior step). Upon authentication, the device will disconnect and be placed in the desired Production VLAN. As shown below, the client device can be seen in the Host View.



★ Host View

NETWORK SENTRY

Quick Search | Log Out

Bookmarks Users **Hosts** Network Devices Logs Policy System Help

Hosts - Displayed: 11 Total: 11

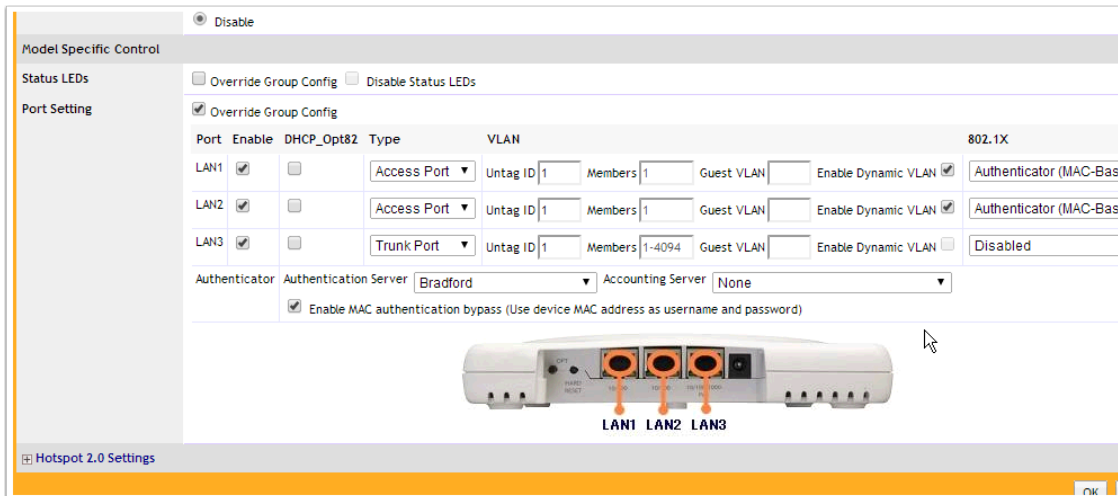
Search *

Status	Host Name	Host Role	Registered To	Logged On User	Host Created	Host Expires	Host Inactivity Date
	Deepaks-iPhone	NAC-Default	ipad		02/25/13 06:27 PM PST	08/07/13 01:12 PM PDT	08/06/13 04:39 PM PDT
	THINK-94	NAC-Default	teacher		07/08/13 01:12 PM PDT	08/07/13 02:11 PM PDT	07/29/13 05:08 PM PDT
		NAC-Default	teacher		05/08/13 02:21 PM PDT	08/07/13 10:56 AM PDT	
		NAC-Default	teacher		07/08/13 10:56 AM PDT	08/07/13 10:56 AM PDT	08/07/13 12:42 PM PDT
	tm-macbook10	NAC-Default	teacher		07/08/13 10:56 AM PDT	08/07/13 10:56 AM PDT	
					05/08/13 01:22 PM PDT	08/09/13 06:57 AM PDT	
					07/10/13 06:57 AM PDT	08/10/13 12:05 PM PDT	08/02/13 03:23 PM PDT
					07/11/13 12:05 PM PDT	08/21/13 03:34 PM PDT	08/06/13 08:17 AM PDT
					07/22/13 03:34 PM PDT	08/22/13 01:28 PM PDT	
					07/23/13 01:28 PM PDT		

Import Export to: Options Add Modify Delete Enable Disable

AP Wired Clients

In order to enable the solution on AP wired clients, the Port Configuration of the AP needs to be changed as shown below (Configure->Access Points->Edit AP). Note that as of this writing, switching from one VLAN to another in this case, may require a physical disconnect/reconnect of the client.



Model Specific Control: Disable

Status LEDs: Override Group Config Disable Status LEDs

Port Setting: Override Group Config

Port	Enable	DHCP_Opt82	Type	VLAN	802.1X
LAN1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Access Port	Untag ID 1 Members 1	Guest VLAN <input type="text"/> Enable Dynamic VLAN <input checked="" type="checkbox"/> Authenticator (MAC-Bas
LAN2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Access Port	Untag ID 1 Members 1	Guest VLAN <input type="text"/> Enable Dynamic VLAN <input checked="" type="checkbox"/> Authenticator (MAC-Bas
LAN3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trunk Port	Untag ID 1 Members 1-4094	Guest VLAN <input type="text"/> Enable Dynamic VLAN <input type="checkbox"/> Disabled

Authenticator: Authentication Server Accounting Server

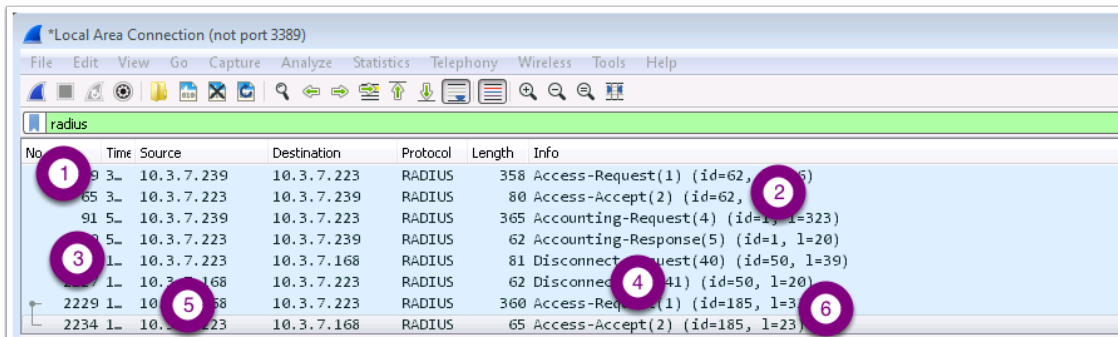
Enable MAC authentication bypass (Use device MAC address as username and password)

Hotspot 2.0 Settings

Troubleshooting

The best way to troubleshoot is to observe the Radius exchange between the Ruckus Controller and the Network Sentry appliance.

1. New User Connects to Production SSID and Ruckus Controller sends Radius Request to Network Sentry
2. Network Sentry responds with Access Accept and assigns user to Isolation VLAN via the DVLAN fields in the Radius response. User connects to the SSID and is assigned a DHCP/DNS Server address by Network Sentry. User browses to say, google.com, and is redirected by Network Sentry to itself. User then authenticates with Network Sentry.
3. Network Sentry sends Radius DM Request message to Ruckus controller.
4. Ruckus Controller acknowledges the DM request and disconnects the user. User now automatically reconnects to the Production SSID.
5. Ruckus Controller sends Radius Request to Network Sentry
6. Network Sentry responds with Radius Accept requesting assignment to the regular VLAN via the DVLAN field in the Accept Response
7. User connects and this time is assigned a DHCP/DNS server by the regular, production infrastructure.



No.	Time	Source	Destination	Protocol	Length	Info
93	3.10.3.7.239	10.3.7.239	10.3.7.223	RADIUS	358	Access-Request(1) (id=62, l=358)
95	3.10.3.7.223	10.3.7.223	10.3.7.239	RADIUS	80	Access-Accept(2) (id=62, l=80)
91	5.10.3.7.239	10.3.7.239	10.3.7.223	RADIUS	365	Accounting-Request(4) (id=1, l=323)
97	5.10.3.7.223	10.3.7.223	10.3.7.239	RADIUS	62	Accounting-Response(5) (id=1, l=20)
101	1.10.3.7.223	10.3.7.223	10.3.7.168	RADIUS	81	Disconnect-Request(40) (id=50, l=39)
107	1.10.3.7.168	10.3.7.168	10.3.7.223	RADIUS	62	Disconnect-Response(41) (id=50, l=20)
2229	1.10.3.7.239	10.3.7.239	10.3.7.223	RADIUS	360	Access-Request(1) (id=185, l=360)
2234	1.10.3.7.223	10.3.7.223	10.3.7.168	RADIUS	65	Access-Accept(2) (id=185, l=23)