

SmartZone

WNAM Ruckus SmartZone Virtual SmartZone (vSZ).

:

1

WNAM (- 192.18.0.200) , Wi-Fi . , , .

2

- RADIUS- (- 192.18.0.200), WNAM. "Service & Profiles" "Authentication" "Proxy (SZ Authenticator)" ("WNAM-AUTH").

Dashboard

System ▶

Access Points

Wireless LANs

Clients ▶

Applications

Services & Profiles ▼

Hotspots & Portals

Access Control

Application Control

URL Filtering

Authentication

Non-Proxy (AP Authenticator)Proxy (SZ Authenticator)

+ Create

Configure

Clone

Test AAA

Delete

Name ▲	Friendly Name	Protocol	Description
Guest	N/A	GUEST	N/A
Local Database	N/A	LOCAL_DB	N/A
WNAM-AUTH	N/A	RADIUS	N/A

Protocol

RADIUS

Name

WNAM-AUTH

Manage By

System

Description

N/A

IP Address

198.18.0.200

Port

1812

Secondary IP Address

N/A

Port

N/A

Last Modified By

admin

Last Modified On

2019/07/01 12:10:59

"wnam-auth" : "RADIUS", RADIUS-, .

Edit Authentication Service WNAM-AUTH

* Name: WNAM-AUTH

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: 198.18.0.200

* Port: 1812

* Shared Secret:

* Confirm Secret:

Secondary Server

Backup RADIUS: ☐ Enable Secondary Server ☐ Automatic Fallback Disable

* IP Address:

* Port: 1812

* Shared Secret:

* Confirm Secret:

Health Check Policy

* Response Window: 20 Seconds

* Zombie Period: 40 Seconds

* Revive Interval: 120 Seconds

OK

Cancel

"wnam-acct", : "RADIUS Accounting", RADIUS-, .

Dashboard

System ▶

Access Points

Wireless LANs

Clients ▶

Applications

Services & Profiles ▼

Hotspots & Portals

Access Control

Application Control

URL Filtering

Authentication

Accounting

Non-ProxyProxy

+ Create

Configure

Clone

Test AAA

Delete

Name ▲	Protocol	Description
WNAM-ACCT	RADIUS	N/A

Name

WNAM-ACCT

Manage By

System

protocol

RADIUS

Description

N/A

IP Address

198.18.0.200

Port

1813

Enable Secondary Server

No

Secondary IP Address

N/A

Port

N/A

Last Modified By

admin

Last Modified On

2019/07/01 12:11:12

Edit Accounting Service: WNAM-ACCT

Name: WNAM-ACCT

Description:

Service Protocol: ☒ RADIUS Accounting

RADIUS Service Options

Primary Server

IP Address: 198.18.0.200

Port: 1813

Shared Secret:

Confirm Secret:

Secondary Server

Backup RADIUS: ☐ Enable Secondary Server ☐ Automatic Fallback Disable

IP Address:

Port: 1813

Shared Secret:

Confirm Secret:

Health Check Policy

Response Window: 20 Seconds

Zombie Period: 40 Seconds

Revive Interval: 120 Seconds

Rate Limiting

OK

Cancel

3.

() "Services & Portals" "Hotspot & Portals" "Hotspo (WISPr)" ("System").

Dashboard

System ▶

Access Points

Wireless LANs

Clients ▶

Applications

Services & Profiles ▼

Hotspots & Portals

Guest AccessHotspot (WISPr)Web AuthWeChatHotspot 2.0UA Blacklist

↺

↩

+ Create

✎ Configure

📄 Clone

🗑 Delete

-

D System

Z Default Zone

Z

Name ▲	Description
WNAM	N/A

Edit Hotspot Service: [WNAM]

General Options

* Portal Name:

Portal Description:

Redirection

Smart Client Support: ☒ None ☐ Enable ☐ Only Smart Client Allowed

Logon URL: ☐ Internal ☒ External

* Redirect unauthenticated user to the URL for authentication:

* Redirected MAC Format:

Start Page: After user is authenticated,

☒ Redirect to the URL that user intends to visit. ☐ Redirect to the following URL:

*

HTTPS Redirect: ☒ If enabled, the AP will try to redirect HTTPS requests to the hotspot portal

User Session

* Session Timeout: Minutes (2-14400)

* Grace Period: Minutes (1-14399)

Location Information

Location ID: (example: isoc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport)

Location Name: (example: ACMEWISP_Gate_14_Terminal_C_of_Newark_Airport)

Walled Garden

Walled Garden: * Walled Garden Entry

Walled Garden Entry

Unauthenticated users are allowed to access the following destinations.

Format:

- IP (e.g. 10.11.12.13)
- IP Range (e.g. 10.11.12.13-10.11.12.15)
- CIDR (e.g. 10.11.12.100/28)
- IP and mask (e.g. 10.11.12.13 255.255.255.0)
- Precise web site (e.g. www.ruckus.com)
- Web site with special regular expression like
 - *.amazon.com
 - *.com

OK

Cancel

("wnam"), WNAM (- <http://198.18.0.200/cp/ruckus>).

"Interim-Update" , 5-15 .

"Session Timeout" .

"Location ID" , WNAM, IP- .

"Walled Garden" IP- W NAM (192.168.0.0/24) , () .

4

(SSID) "Configure" "WLANs".

("w nam"), (WISPr), "Open" "None", "w nam".

Edit WLAN Config: [terra_guest]

General Options

- * Name:
- * SSID:
- Description:
- Zone:
- * WLAN Group: [+ Create](#)

Authentication Options

- * Authentication Type: ☐ Standard usage (For most regular wireless networks) ☒ Hotspot (WISPr) ☐ Guest Access ☐ Web Authentication
- ☐ Hotspot 2.0 Access ☐ Hotspot 2.0 Onboarding ☐ WeChat
- * Method: ☐ Open ☐ 802.1X EAP ☒ MAC Address ☐ 802.1X & MAC
- 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

Data Plane Options

- Access Network: ☐ Tunnel WLAN traffic through Ruckus GRE

Hotspot Portal

- * Hotspot (WISPr) Portal: [+ Create](#)
- Bypass CNA: ☐ Enable
- * Authentication Server: ☒ Use the Controller as Proxy
- [+ Create](#)
- Accounting Server: ☒ Use the Controller as Proxy
- [+ Create](#) Send interim update every Minutes (0-1440)

Options

- Acct Delay Time: ☐ Enable
- * Wireless Client Isolation: ☐ Disable ☒ Enable (Isolate wireless client traffic from all hosts on the same VLAN/subnet)
- Isolation Whitelist: [+ Create](#)
- (The whitelist requires entries for the subnet gateway and other allowed hosts.)
- (The whitelist can only contain wired destinations; wireless clients are not supported on the whitelist.)
- * Priority: ☒ High ☐ Low

RADIUS Options

- * NAS ID: ☒ WLAN BSSID ☐ AP MAC ☐ User-defined:
- Delimiter: ☒ Dash ☐ Colon

* NAS Request Timeout: Seconds

* NAS Max Number of Retries: Times

* NAS Reconnect Primary: Minute (1-300)

* [?] Called Station ID: ☐ WLAN BSSID ☒ AP MAC ☐ None ☐ AP GROUP

NAS IP: ☐ Disabled ☒ SZ Control IP ☐ User-defined:

Single Session ID Accounting: ☐ Enable. APs will maintain one accounting session for client roaming.

Advanced Options ▼

User Traffic Profile:

L2 Access Control:

OS Policy:

Application Recognition & Control: ☐ Enabled

URL Filtering: ☐ Enabled

Client Fingerprinting: ☒ Enable Client Fingerprinting

Access VLAN: VLAN ID

☐ Enable VLAN Pooling

☒ Enable Dynamic VLAN (AAA Override)

Hotspot 2.0 Onboarding: ☐ Allow Hotspot 2.0 Onboarding

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 clients per AP radio to associate with this WLAN

802.11d: ☒ Support for 802.11d (country code shown in beacon)

802.11k Neighbor Report: ☒ Enable 802.11k neighbor reports

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

DHCP Option 82: ☐ Enable DHCP Option 82

DTIM Interval: (1-255) Defines the frequency of beacons that will include a DTIM

[?] Directed MC/BC Threshold: (0-128) Defines the per radio client count at which an AP will stop converting group addressed data traffic to unicast.

Client TX/RX Statistics: ☐ Ignore statistics from unauthorized clients

5

URL, :

```
set scg ip
no encrypt-mac-ip
```

Ruckus vSZ .

6

WNAM "" "" Ruckus vSZ (), IP- (192.168.0.27) " " .

Изменение сервера доступа



Параметры

RADIUS

TACACS+

Категории



Тип

Ruckus ZoneDirector



Имя устройства

rtk-sochi-1

IP адрес (NAS-IP-Address)

83.239.44.11

Внешний IP адрес

83.239.44.11:9080

Местоположение

Krasnodar

Комментарий

Логин

ruckus

Пароль

.....



☒ Использовать счетчики аккаунтинга

получено 0 записей

☐ Менять местами счетчики приёма/передачи

☐ Определять имена устройств абонентов

☐ Принимать детализацию потоков NetFlow

получено 0 записей

Вкл.

Сбросить сессии

Удалить

Сохранить изменения

Закрыть