PERSONAL AREA NETWORK

(PAN Module)

The Personal Area network (PAN) feature works in conjunction with the Wireless Controller dynamic VLAN capability to create a private personal network for each user

Table of Contents

Introduction

The Personal Area network (PAN) feature works in conjunction with the Wireless Controller dynamic VLAN capability to create a private personal network for each user which helps provide the following advantages:

- Increased security
- Protect from privacy intrusion
- Manage and control your own personal and smart devices

Some useful application and usage of PAN includes and is not limited to:

- Hotels that deployed individual in-room device for video casting, e.g. Chromecast or Apple TV
- Service Offices that provides a shared WiFi infrastructure with each tenant devices grouped together in the same network
- MDU WiFi operators

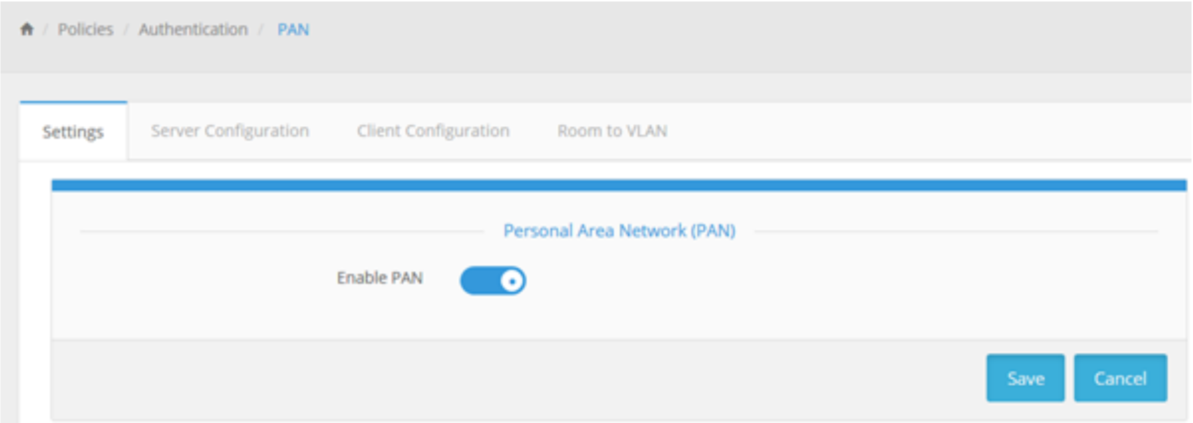
PAN Gateway Requirements

a. The IG4 / SG4 Gateway must be at Update level 30.
b. PAN module must be activated.

PAN Gateway Configuration

1. Enabling PAN

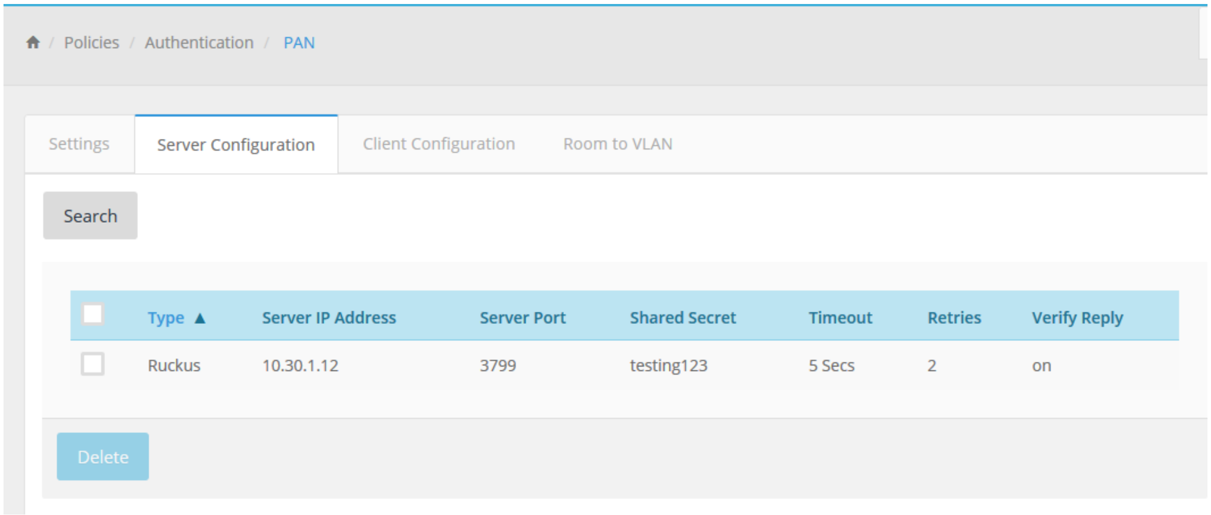
Enable PAN under *Policies > Authentication > PAN*



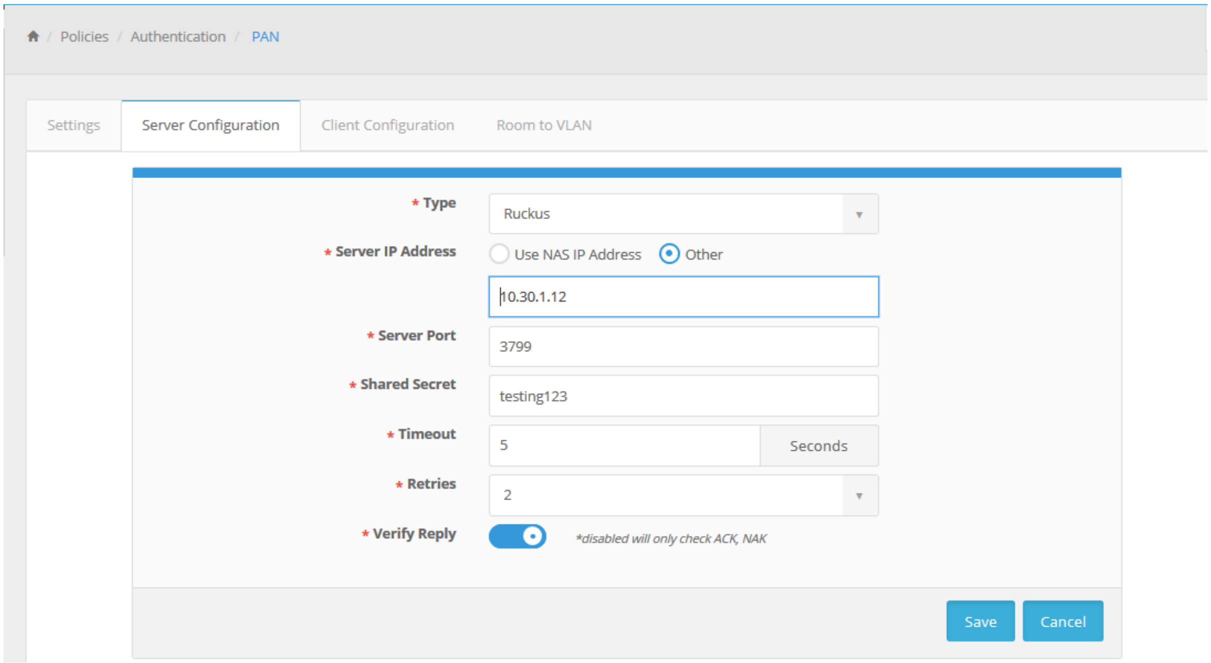
Enable PAN ●

2. Configuring 'Radius DynAuth Server'

Configure Radius DynAuth server to handle Disconnect Message



□	Type ▲	Server IP Address	Server Port	Shared Secret	Timeout	Retries	Verify Reply
□	Ruckus	10.30.1.12	3799	testing123	5 Secs	2	on



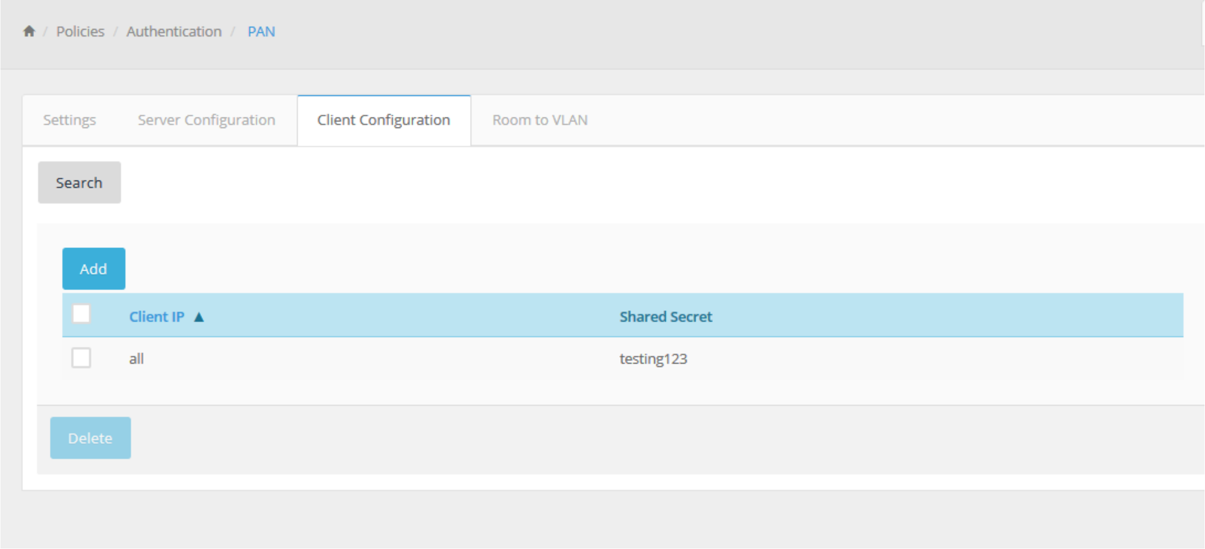
* Type	Ruckus
* Server IP Address	○ Use NAS IP Address ● Other 10.30.1.12
* Server Port	3799
* Shared Secret	testing123
* Timeout	5 Seconds
* Retries	2
* Verify Reply	on *disabled will only check ACK, NAK

Note: Server IP address is WLC controller IP
Shared Secret: (Same as configured for Radius Authentication in WLC)

ANTlabs gateway must be able to communicate to Radius DynAuth server to initiate the Radius Disconnect Message (DM)

3. Adding 'Client Configuration'

Each WLC or AP sending Radius requests to gateway must be configured separately under Client Configuration. Specific shared secret can be configured for each individual client, or a common shared secret can be configured for all clients.

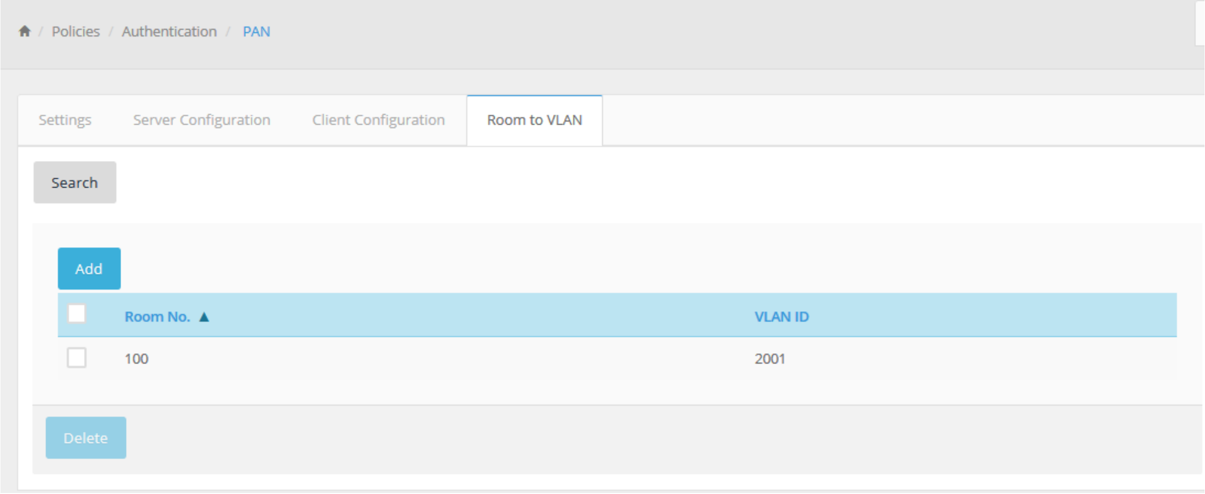


	Client IP ▲	Shared Secret
□	all	testing123

4. Configuring 'Room to VLAN' Mapping (Optional)

If separate room to VLAN mapping is required, configure the mapping under Policies -> Authentication -> PAN -> Room to VLAN.

For more details on assigning VLAN using PMS Guest Room number, please refer to subsection 7.

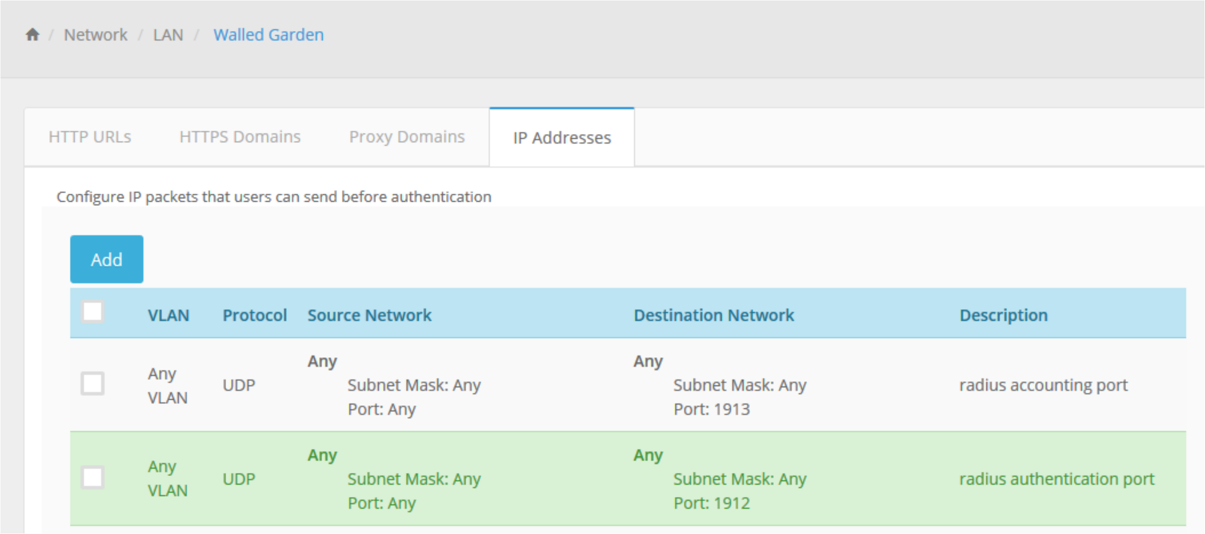


	Room No. ▲	VLAN ID
□	100	2001

5. Allowing WLC / AP to communicate with Gateway

The WLC / AP radius must be configured to point to ports 1912 for auth and 1913 for acct.

If the radius traffic is coming in to the gateway from the LAN network, 2 walled garden entries must be added under *Network -> LAN -> Walled Garden -> IP address*



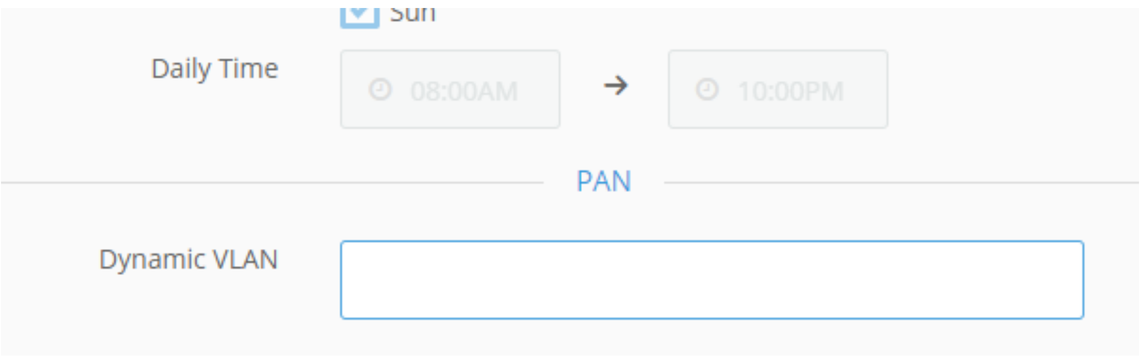
Configure IP packets that users can send before authentication

☐	VLAN	Protocol	Source Network	Destination Network	Description
☐	Any VLAN	UDP	Any Subnet Mask: Any Port: Any	Any Subnet Mask: Any Port: 1913	radius accounting port
☐	Any VLAN	UDP	Any Subnet Mask: Any Port: Any	Any Subnet Mask: Any Port: 1912	radius authentication port

6. Assigning Dynamic VLAN when creating Account

Dynamic VLAN can be specified when creating or editing an account under *Policies > Authentication > Accounts*.

This is typically used in Service office and MDU deployments where the administrator creates individual account with unique VLAN for each user. By logging in their multiple devices using the individual account, the same VLAN is dynamically assigned for all these devices, this creating a Personal Network.



Daily Time: 08:00AM → 10:00PM

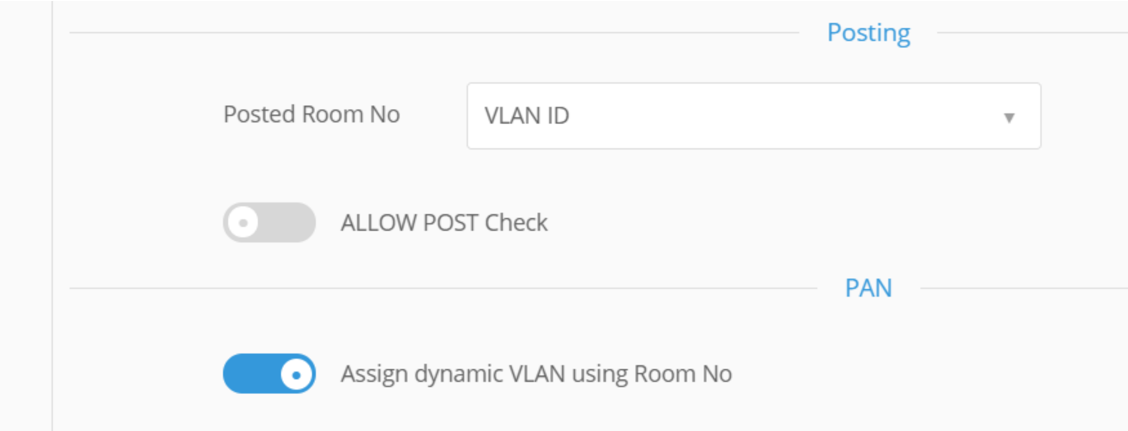
Dynamic VLAN:

7. Assigning Dynamic VLAN using PMS

Dynamic VLAN can also be assigned via PMS using the Guest Room number. This is used by hotels to ensure that individual guest is placed into the same VLAN as all the other devices in the room, thus creating a Personal Network.

Note: Each room must also be assigned a separate unique VLAN for this to work.

To do so, enable the option 'Assign dynamic VLAN using Room No' under *Policies > Locations > Authentication > PMS.* By default, the dynamic VLAN will be assigned using the Room Number.



Posting

Posted Room No: VLAN ID ▾

○ ALLOW POST Check

PAN

● Assign dynamic VLAN using Room No

Note: If your deployment requires a different mapping of VLANs based on Room number, you can configure it under *Policies > Authentication > PAN > Room to VLAN*.

8. VLAN Creation

ANTlabs Gateway - Dynamic VLANs assigned for PAN must be pre-configured.
Ruckus WLC - Pre-defined Dynamic VLANs configuration in APs is not needed as Ruckus AP will create them on fly
Aruba WLC - Dynamic VLANs must be preconfigured in APs.
Meraki AP - Pre-defined Dynamic VLANs configuration in APs is not needed as Meraki AP will create them on fly
Xirrus AP - Dynamic VLANs must be preconfigured in APs.

Ruckus SmartZone WLC Configuration

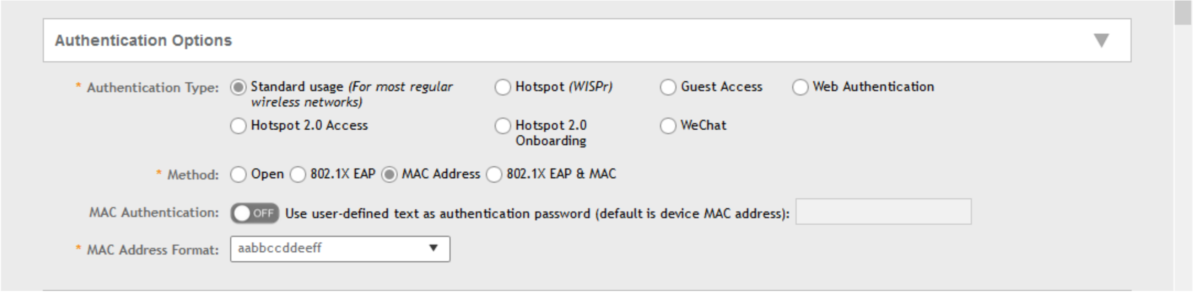
Requires Version 3.6.2.0.78 and above

1. Enable MAC-based Authentication

Under 'Wireless LANs', select the WLAN Config profile and then click 'Configure'

Authentication Options

- Authentication Type - Standard usage
- Method - MAC address
- MAC Address Format: aabbccddeeff



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 EAP & MAC

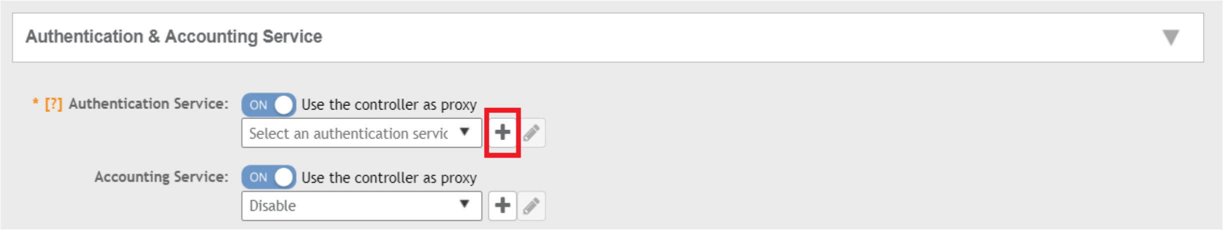
MAC Authentication: OFF Use user-defined text as authentication password (default is device MAC address):

* MAC Address Format: aabbccddeeff ▼

2. Configure AAA server profile

Authentication Service

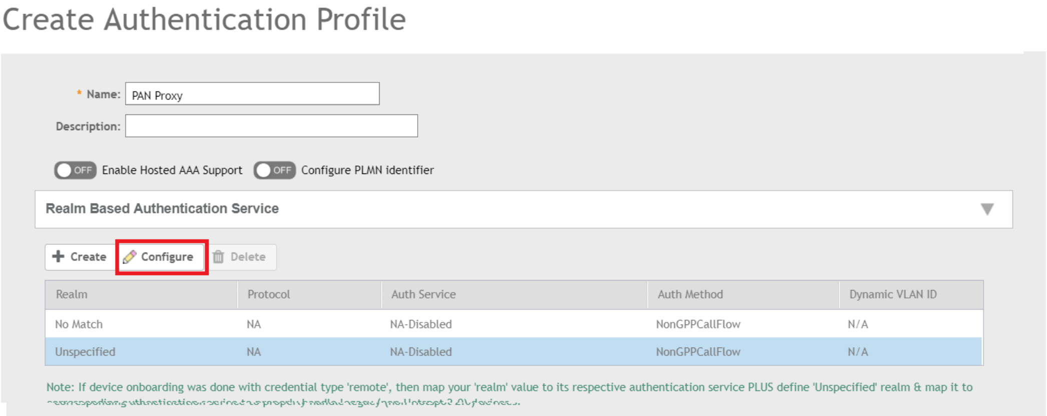
- Authentication Service – Use the proxy controller as proxy (set to ON)
- Click + to add an Authentication Profile.



Authentication & Accounting Service ▼

* [?] Authentication Service: ON Use the controller as proxy
Select an authentication servic ▼ + ✎

Accounting Service: ON Use the controller as proxy
Disable ▼ + ✎



Create Authentication Profile

* Name:	PAN Proxy
Description:	

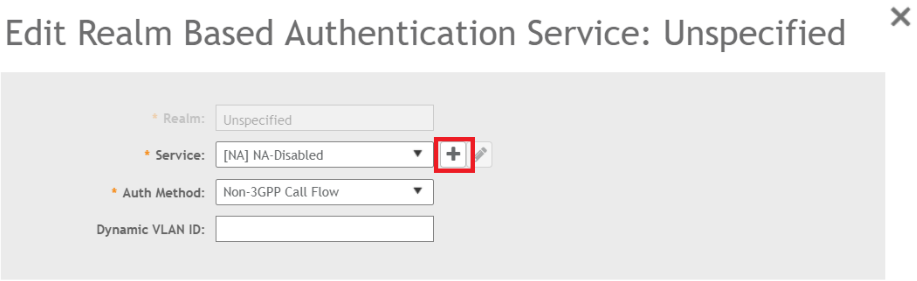
OFF Enable Hosted AAA Support OFF Configure PLMN identifier

Realm Based Authentication Service

Realm	Protocol	Auth Service	Auth Method	Dynamic VLAN ID
No Match	NA	NA-Disabled	NonGPPCallFlow	N/A
Unspecified	NA	NA-Disabled	NonGPPCallFlow	N/A

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

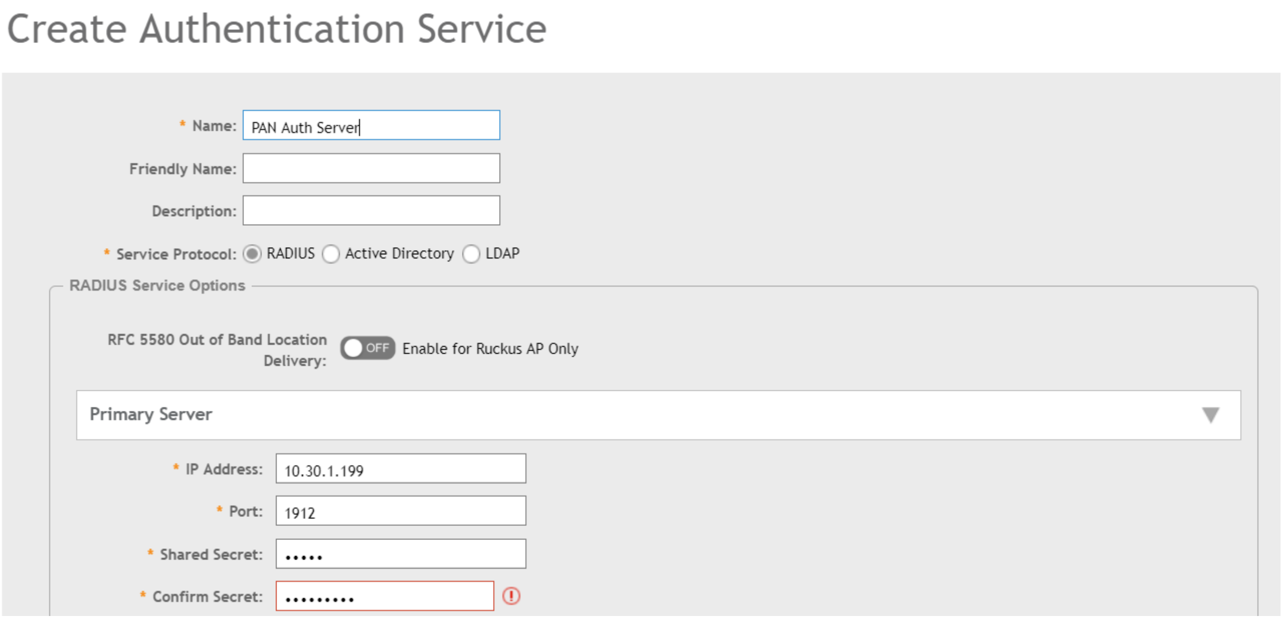
- Select Realm 'Unspecified' and click 'Configure'.
  Note: SZ 100 does not support realm based authentication



Edit Realm Based Authentication Service: Unspecified

* Realm:	Unspecified
* Service:	[NA] NA-Disabled
* Auth Method:	Non-3GPP Call Flow
Dynamic VLAN ID:	

- Click + to add Authentication Server.



Create Authentication Service

* Name:	PAN Auth Server
Friendly Name:	
Description:	
* Service Protocol:	● RADIUS ○ Active Directory ○ LDAP

RADIUS Service Options

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

Primary Server

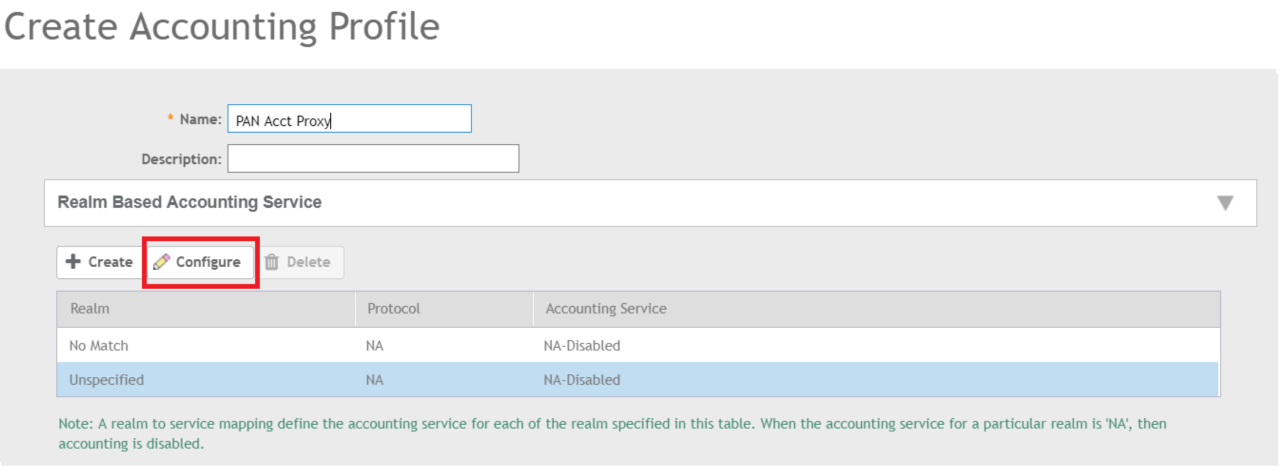
* IP Address:	10.30.1.199
* Port:	1912
* Shared Secret:	•••••
* Confirm Secret:	•••••••••

- Configure Gateway IP address and port 1912
  Note: Shared secret should be same as configured in gateway under *Policies > authentication > PAN > Client Configuration*.

Accounting Service

- Accounting Service – Use the proxy controller as proxy (set to ON)

- Click + to add an Accounting Profile.



Create Accounting Profile

* Name: PAN Acct Proxy

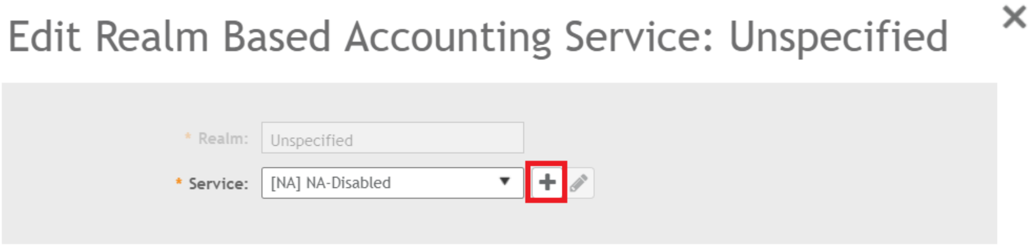
Description:

Realm Based Accounting Service ▼

Realm	Protocol	Accounting Service
No Match	NA	NA-Disabled
Unspecified	NA	NA-Disabled

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 'NA', then accounting is disabled.

- Select Realm 'Unspecified' and click 'Configure'.
  Note: SZ 100 does not support realm based accounting

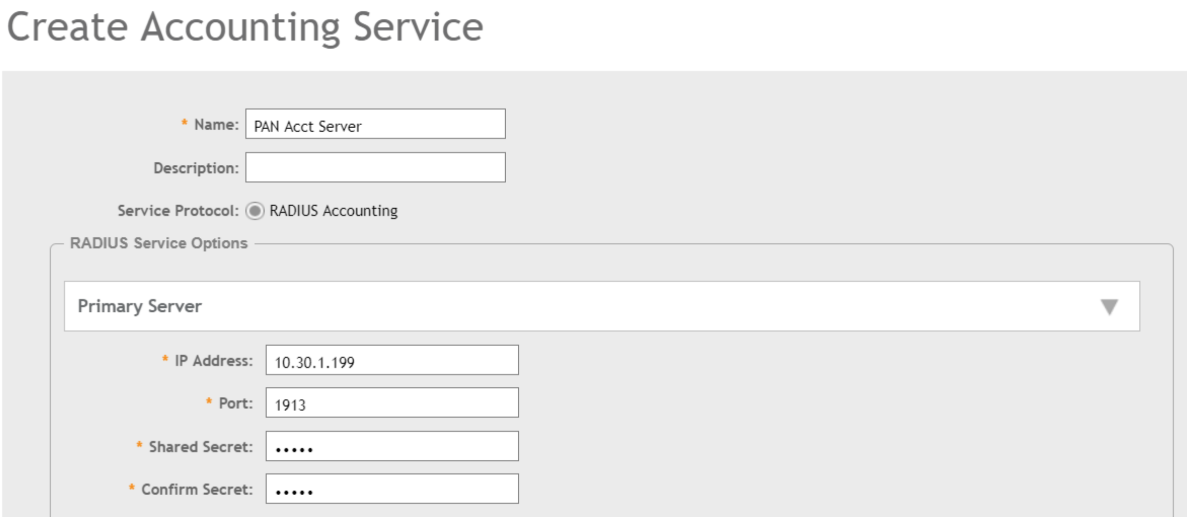


Edit Realm Based Accounting Service: Unspecified

* Realm: Unspecified

* Service: [NA] NA-Disabled ▼

- Click + to add Accounting Server.



Create Accounting Service

* Name: PAN Acct Server

Description:

Service Protocol: ● RADIUS Accounting

RADIUS Service Options

Primary Server ▼

* IP Address: 10.30.1.199

* Port: 1913

* Shared Secret: •••••

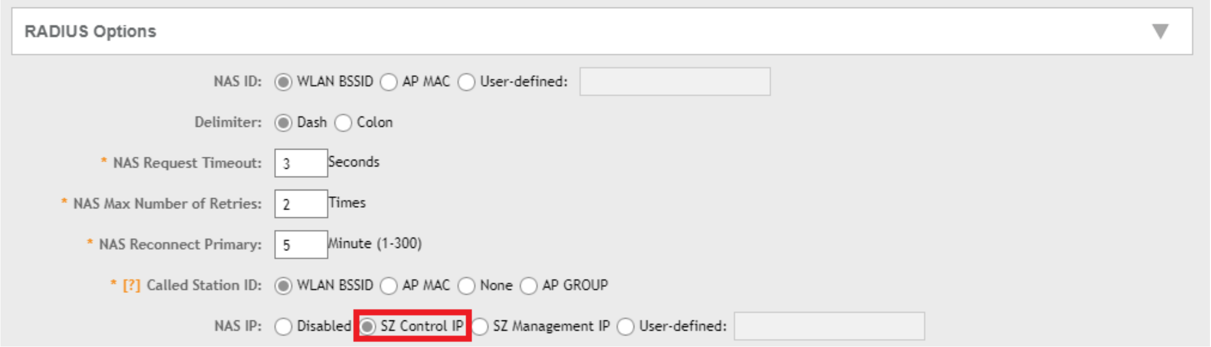
* Confirm Secret: •••••

- Configure Gateway IP address and port 1913
  Note: shared secret should be same as configured in gateway under *Policies > authentication > PAN > Client Configuration*.

3. Configure NAS IP

RADIUS Options

- Specify SZ Control IP as the NAS IP



RADIUS Options

NAS ID: ● WLAN BSSID ○ AP MAC ○ User-defined:

Delimiter: ● Dash ○ Colon

* NAS Request Timeout: 3 Seconds

* NAS Max Number of Retries: 2 Times

* NAS Reconnect Primary: 5 Minute (1-300)

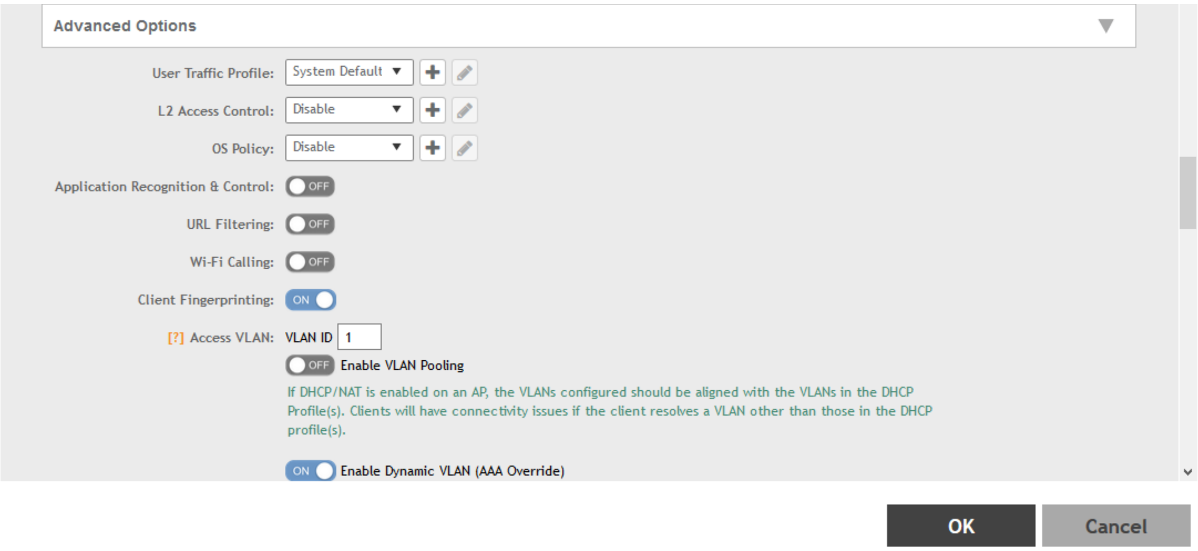
* [?] Called Station ID: ● WLAN BSSID ○ AP MAC ○ None ○ AP GROUP

NAS IP: ○ Disabled ● SZ Control IP ○ SZ Management IP ○ User-defined:

4. Enable Dynamic VLAN Option

Advanced Options

- Must sure 'Enable Dynamic VLAN (AAA Override)' is ON



Advanced Options

User Traffic Profile: System Default

L2 Access Control: Disable

OS Policy: Disable

Application Recognition & Control: OFF

URL Filtering: OFF

Wi-Fi Calling: OFF

Client Fingerprinting: ON

[?] Access VLAN: VLAN ID 1

OFF Enable VLAN Pooling

If DHCP/NAT is enabled on an AP, the VLANs configured should be aligned with the VLANs in the DHCP Profile(s). Clients will have connectivity issues if the client resolves a VLAN other than those in the DHCP profile(s).

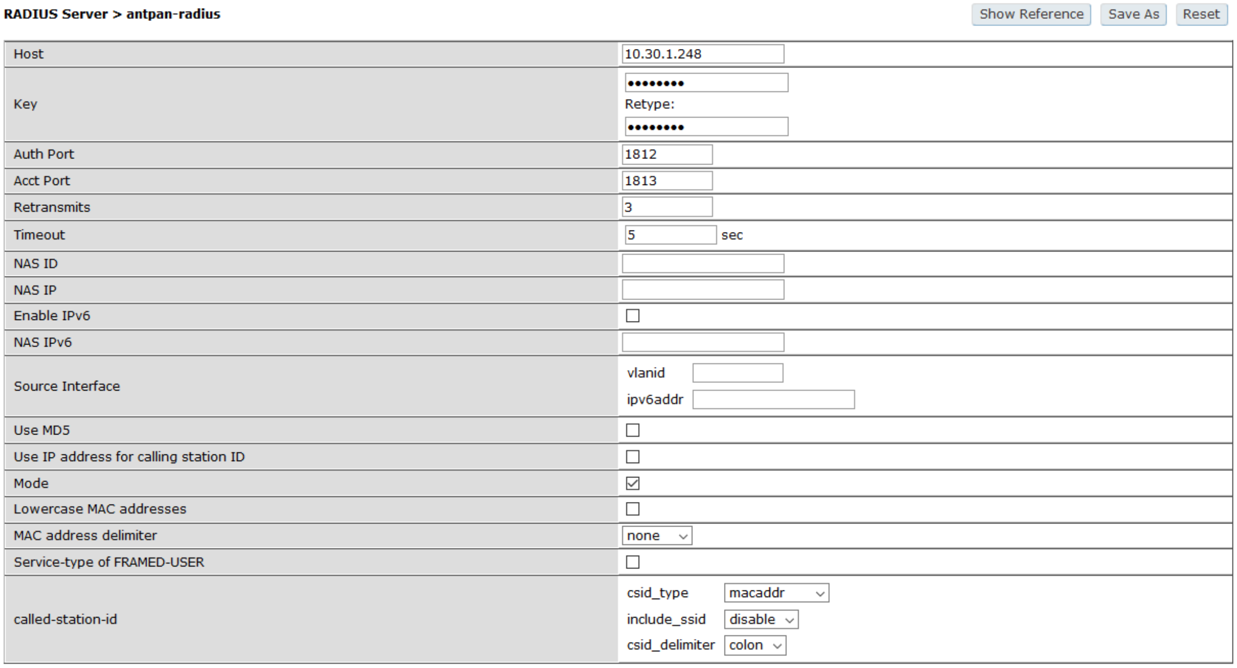
ON Enable Dynamic VLAN (AAA Override)

Aruba 'Mobility Controller' Configuration

Requires Version 6.4.0.0 and above

1. Create Radius Server

- Add a new profile under *Configuration ->Security -> Authentication -> Servers -> RADIUS Server* (e.g. antpan-radius)
- Specify ANTlabs gateway IP as the radius server

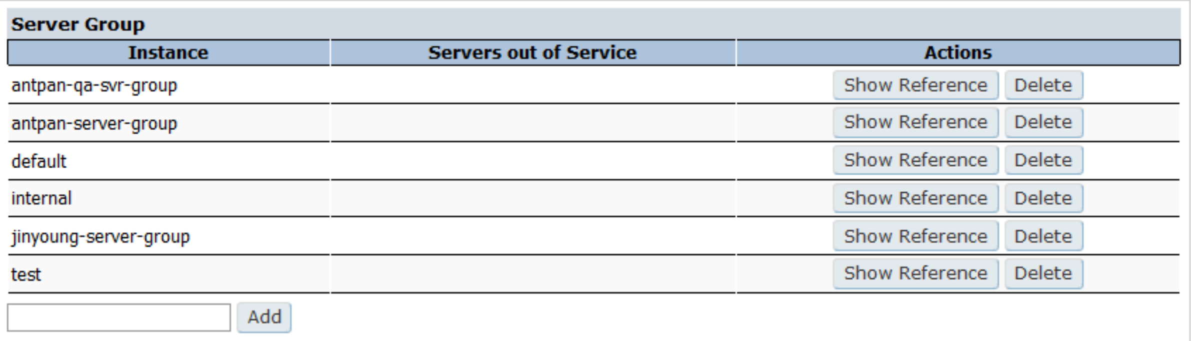


RADIUS Server > antpan-radius

Host	10.30.1.248
Key	•••••••• Retype: ••••••••
Auth Port	1812
Acct Port	1813
Retransmits	3
Timeout	5 sec
NAS ID	
NAS IP	
Enable IPv6	□
NAS IPv6	
Source Interface	vlanid ipv6addr
Use MD5	□
Use IP address for calling station ID	□
Mode	☑
Lowercase MAC addresses	□
MAC address delimiter	none
Service-type of FRAMED-USER	□
called-station-id	csid_type macaddr include_ssid disable csid_delimiter colon

2. Add Radius Server to Server Group

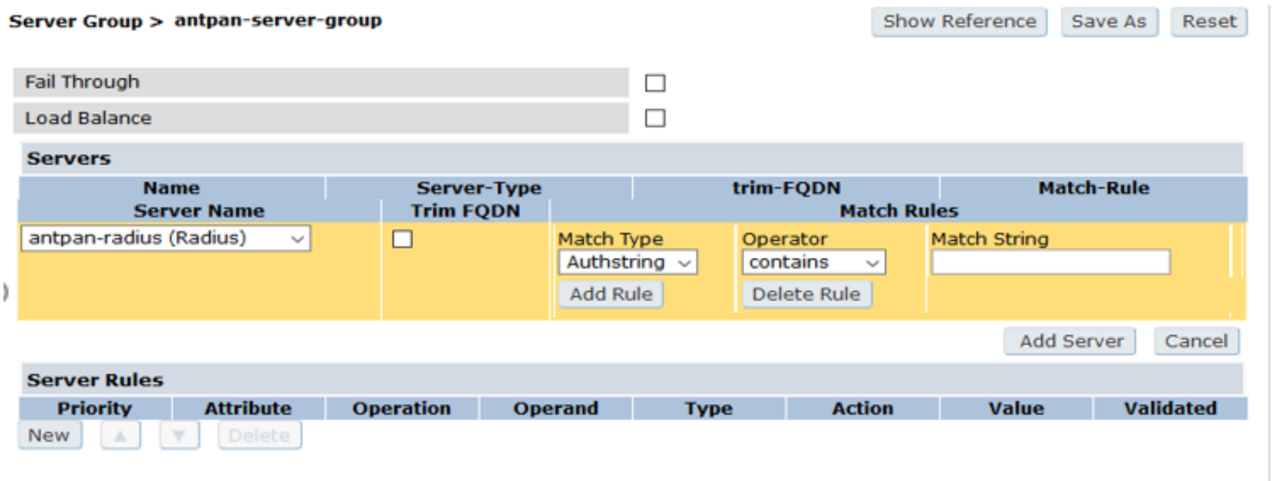
- Create a new server group profile under *Configuration ->Security -> Authentication -> Servers –> Server group* (e.g. antpan-server-group)



Server Group

Instance	Servers out of Service	Actions
antpan-qa-svr-group		Show Reference Delete
antpan-server-group		Show Reference Delete
default		Show Reference Delete
internal		Show Reference Delete
jinyoung-server-group		Show Reference Delete
test		Show Reference Delete

- Link the Radius Server (antpan-radius) to the server group.



Server Group > antpan-server-group

Fail Through	☐
Load Balance	☐

Servers

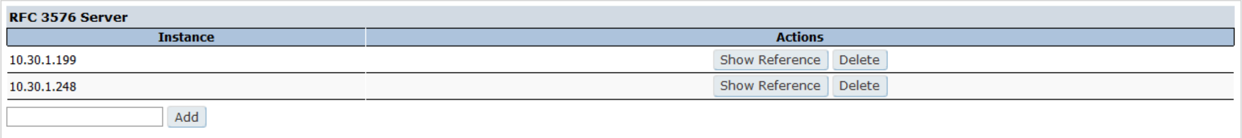
Name Server Name	Server-Type Trim FQDN	trim-FQDN Match Rules		Match-Rule
antpan-radius (Radius)	☐	Match Type Authstring	Operator contains	Match String

Server Rules

Priority	Attribute	Operation	Operand	Type	Action	Value	Validated

3. Create RFC 3576 Server (for CoA/DM)

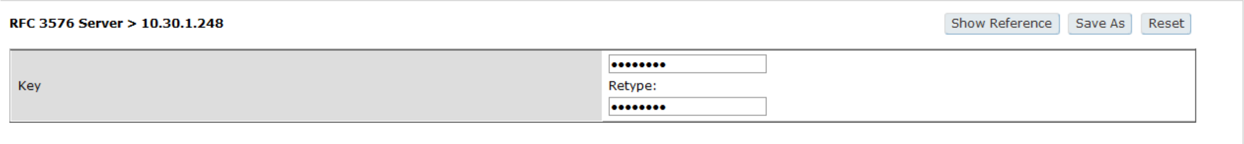
- Add a new gateway Instance (IP address of ANTlabs gateway) under *Configuration ->Security -> Authentication -> Servers –> RFC 3576 Server*



RFC 3576 Server

Instance	Actions
10.30.1.199	Show Reference Delete
10.30.1.248	Show Reference Delete

- Click on newly created IP address and input secret key.

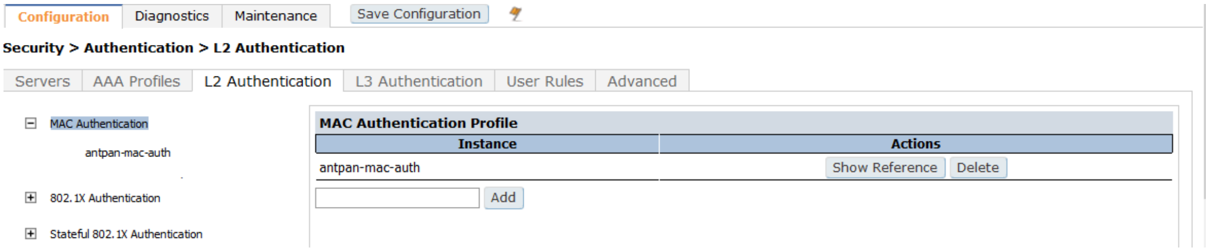


RFC 3576 Server > 10.30.1.248

Key	•••••••• Retype: ••••••••

4. Configure L2 Authentication Profile

- Create a new profile under *Configuration -> Security -> Authentication -> L2 Authentication -> MAC Authentication* (e.g. antpan-mac_auth)



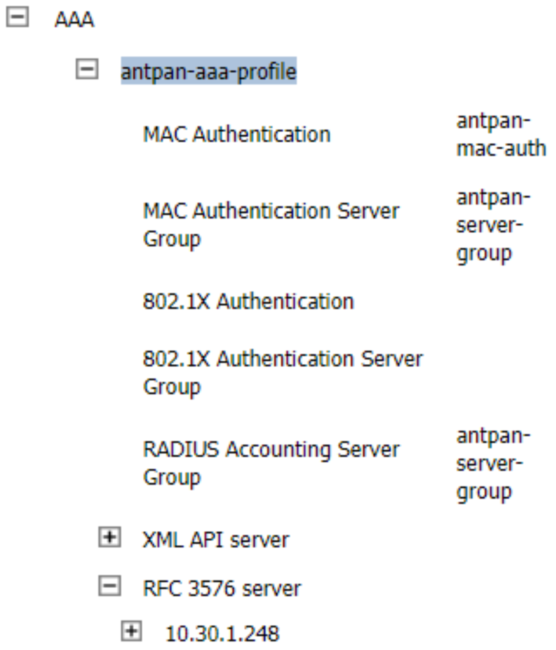
Security > Authentication > L2 Authentication

MAC Authentication Profile

Instance	Actions
antpan-mac-auth	Show Reference Delete

5. Create AAA Profile

- Create a new AAA profile under *Configuration ->Security -> Authentication -> AAA Profile -> AAA* (e.g. antpan-aaa-profile)



⊟ AAA

⊟ antpan-aaa-profile

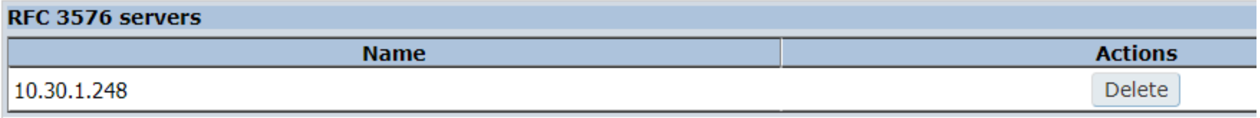
MAC Authentication	antpan-mac-auth
MAC Authentication Server Group	antpan-server-group
802.1X Authentication	
802.1X Authentication Server Group	
RADIUS Accounting Server Group	antpan-server-group

⊞ XML API server

⊟ RFC 3576 server

⊞ 10.30.1.248

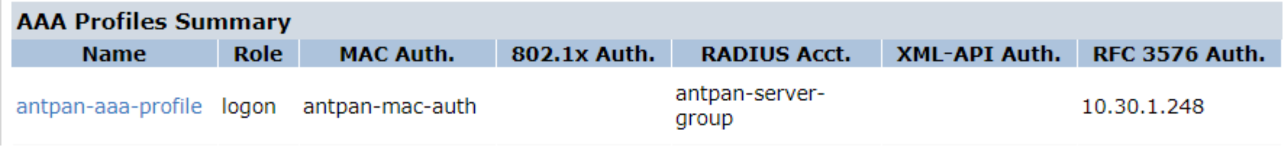
- Configure the created AAA profile (antpan-aaa-profile)
  - MAC Authentication - 'antpan-mac-auth'
  - MAC Authentication Server Group' – 'antpan-server-group'
  - 802.1X Authentication - 'N/A'
  - 802.1X Authentication Server Group - 'N/A'
  - 802.1X Accounting Server Group – antpan-server-group
  - RFC 3576 server – select ANTlabs gateway IP



RFC 3576 servers

Name	Actions
10.30.1.248	Delete

- Configured profile should look like this

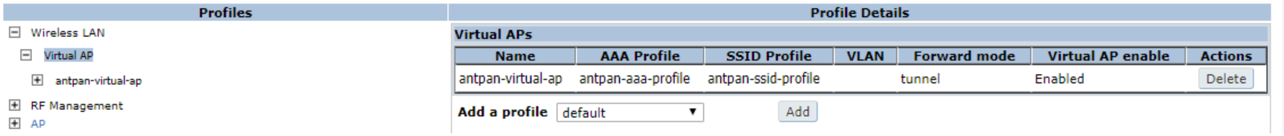


AAA Profiles Summary

Name	Role	MAC Auth.	802.1x Auth.	RADIUS Acct.	XML-API Auth.	RFC 3576 Auth.
antpan-aaa-profile	logon	antpan-mac-auth		antpan-server-group		10.30.1.248

6. Link AAA Profile to Wireless AP Configuration

- Select created AAA profile for the required Wireless AP configuration under *Wireless -> AP Configuration*



Profiles

⊟ Wireless LAN
⊟ Virtual AP
⊞ antpan-virtual-ap
⊞ RF Management
⊞ AP

Profile Details

Virtual APs

Name	AAA Profile	SSID Profile	VLAN	Forward mode	Virtual AP enable	Actions
antpan-virtual-ap	antpan-aaa-profile	antpan-ssid-profile		tunnel	Enabled	Delete

Add a profile: default ▼ Add

Cisco WLC Configuration

Requires Cisco 4400 WLC that runs firmware release 8.5.135.0 and above

1. Configure the WLC with the Details of the Authentication Server

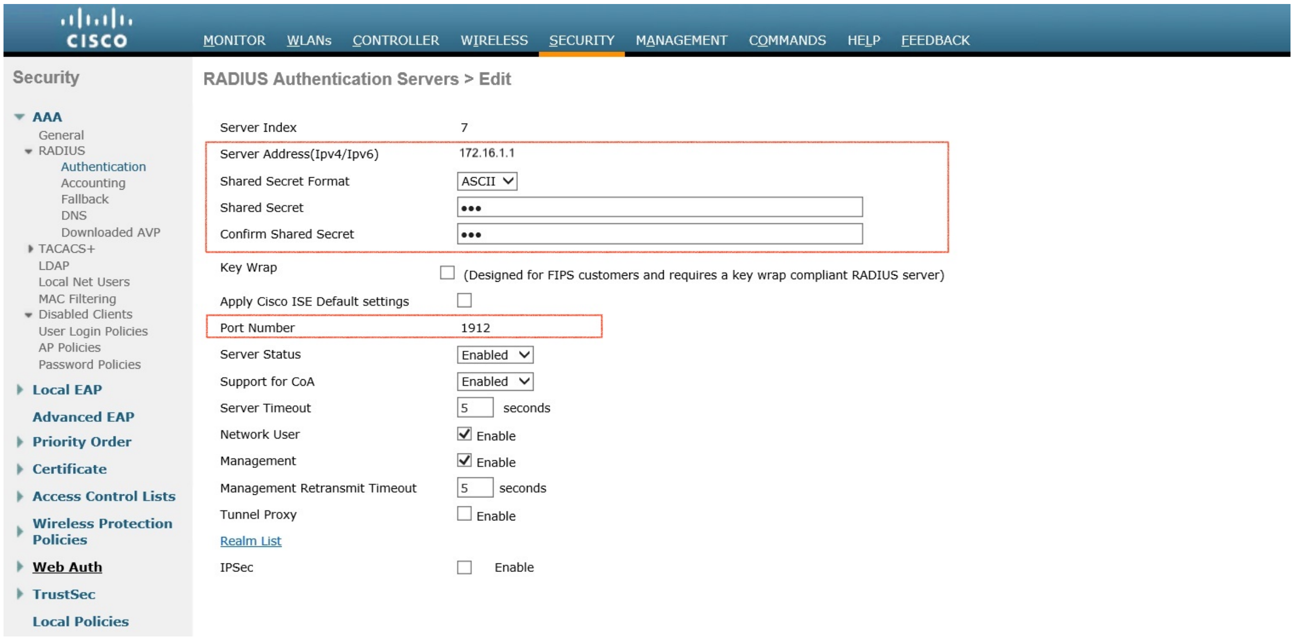
It is necessary to configure the WLC so it can communicate with the RADIUS server to authenticate the clients, and also for any other transactions.

Complete these steps:

1. From the controller GUI, click **Security**.

2. Enter the IP address of the RADIUS server and the Shared Secret key used between the RADIUS server and the WLC.

   This Shared Secret key should be the same as the one configured in the RADIUS server under Network Configuration > AAA Clients > Add Entry. Here is an example window from the WLC:



RADIUS Authentication Servers > Edit

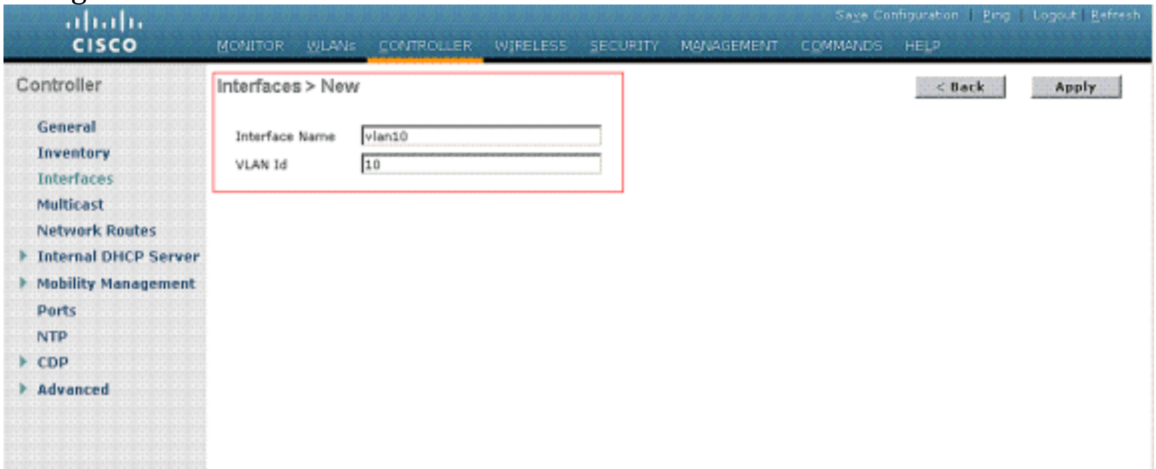
Server Index	7
Server Address(Ipv4/Ipv6)	172.16.1.1
Shared Secret Format	ASCII
Shared Secret	•••
Confirm Shared Secret	•••
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Apply Cisco ISE Default settings	□
Port Number	1912
Server Status	Enabled
Support for CoA	Enabled
Server Timeout	5 seconds
Network User	☑ Enable
Management	☑ Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	□ Enable
Realm List	
IPSec	□ Enable

2. Configure the Dynamic Interfaces (VLANs)

This procedure explains how to configure dynamic interfaces on the WLC. As explained earlier in this document, the VLAN ID specified under the Tunnel-Private-Group ID attribute of the RADIUS server must also exist in the WLC.

In the example, the user1 is specified with the **Tunnel-Private-Group ID of 10 (VLAN =10)** on the RADIUS server. See the IETF RADIUS Attributessection of the user1 User Setup window.

You can see the same dynamic interface (VLAN=10) configured in the WLC in this example. From the controller GUI, under the Controller > Interfaces window, the dynamic interface is configured.



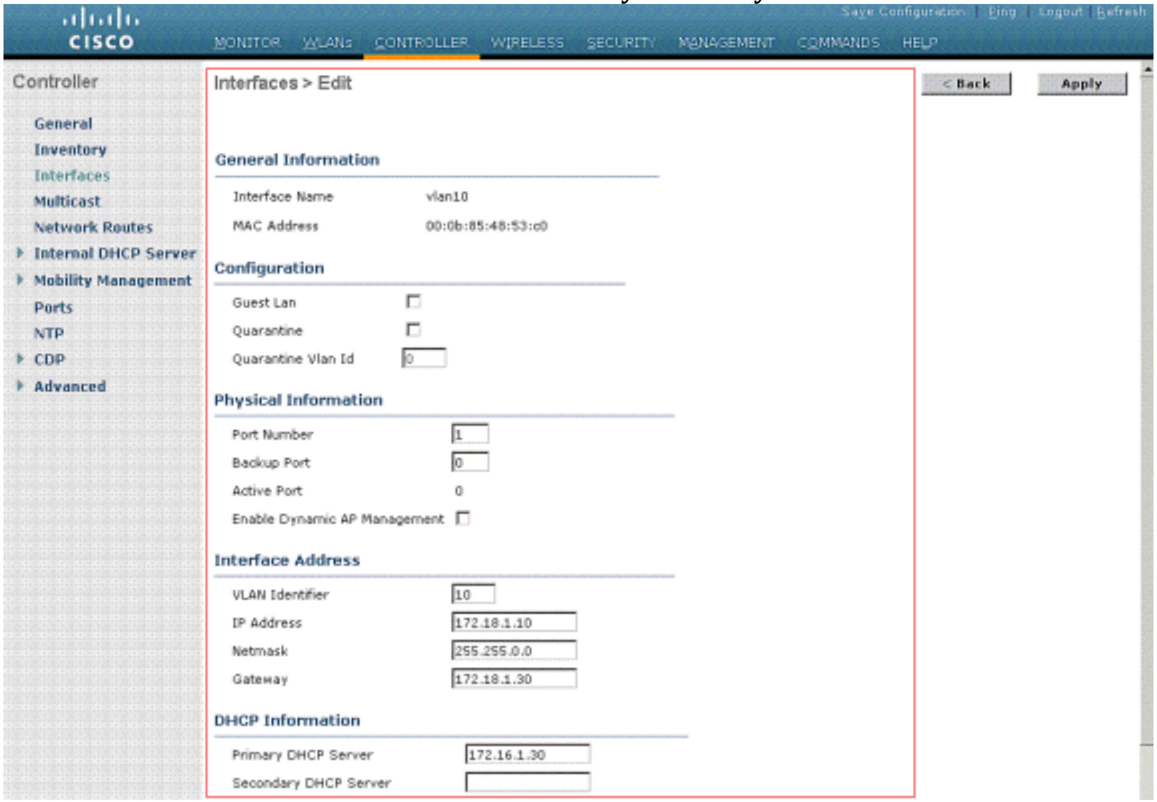
Interfaces > New

Interface Name: vlan10

VLAN Id: 10

1. Click **Apply** on this window.
   This takes you to the Edit window of this dynamic interface (VLAN 10 here).

2. Enter the IP Address and default Gateway of this dynamic interface.



Interfaces > Edit

General Information

Interface Name: vlan10

MAC Address: 00:0b:85:48:53:c0

Configuration

Guest Lan ☐

Quarantine ☐

Quarantine Vlan Id: 0

Physical Information

Port Number: 1

Backup Port: 0

Active Port: 0

Enable Dynamic AP Management ☐

Interface Address

VLAN Identifier: 10

IP Address: 172.18.1.10

Netmask: 255.255.0.0

Gateway: 172.18.1.30

DHCP Information

Primary DHCP Server: 172.16.1.30

Secondary DHCP Server:

Note: Because this document uses an internal DHCP server on the controller, the primary DHCP server field of this window points to the Management Interface of the WLC itself. You can also use an external DHCP server, a router, or the RADIUS server itself as a DHCP server to the wireless clients. In such cases, the primary DHCP server field points to the IP address of that device used as the DHCP server. Refer to your DHCP server documentation for more information.

3. Click **Apply**.

Now you are configured with a dynamic interface in your WLC. Similarly, you can configure several dynamic interfaces in your WLC. However, remember that the same VLAN ID must also exist in the RADIUS server for that particular VLAN to be assigned to the client.

3. Configure the WLANs (SSID)

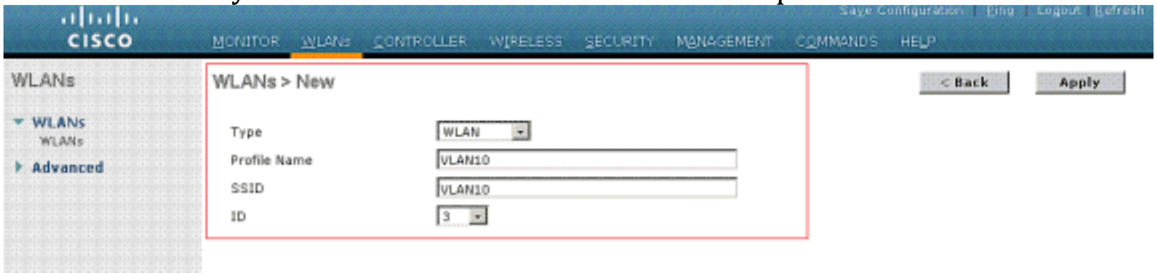
This procedure explains how to configure the WLANs in the WLC.
Complete these steps:

1. From the controller GUI, choose WLANs > New in order to create a new WLAN.

The New WLANs window is displayed.

2. Enter the WLAN ID and WLAN SSID information.

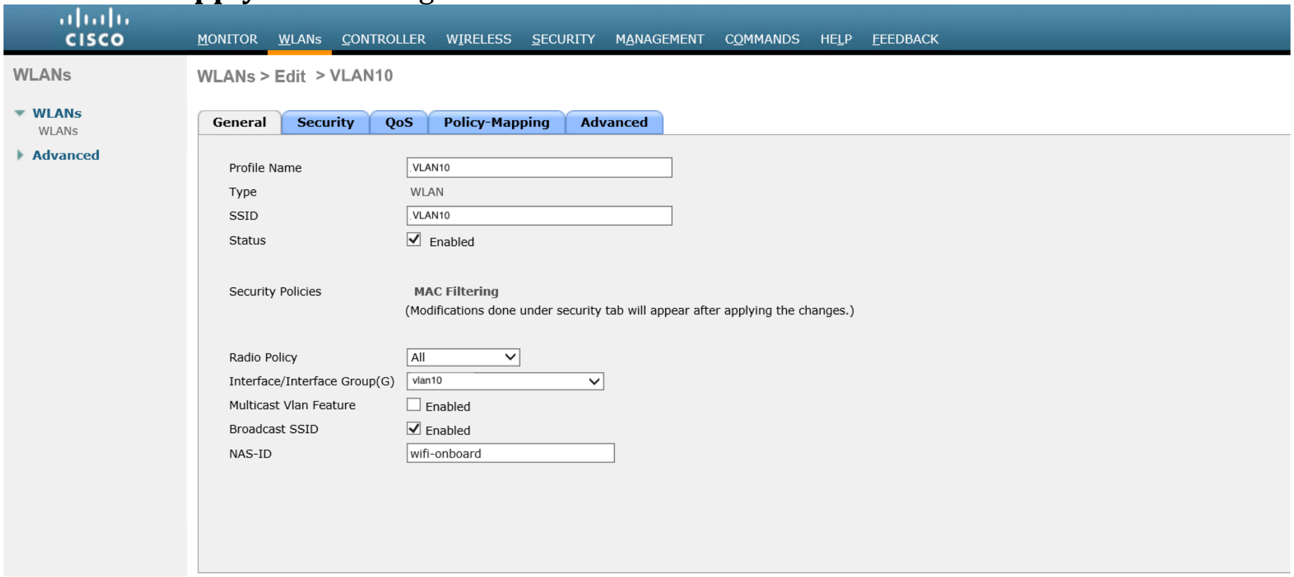
You can enter any name to be the WLAN SSID. This example uses VLAN10 as the WLAN SSID.



WLANs > New

Type: WLAN
Profile Name: VLAN10
SSID: VLAN10
ID: 3

3. Click **Apply** in order to go to the Edit window of the WLAN SSID VLAN10.

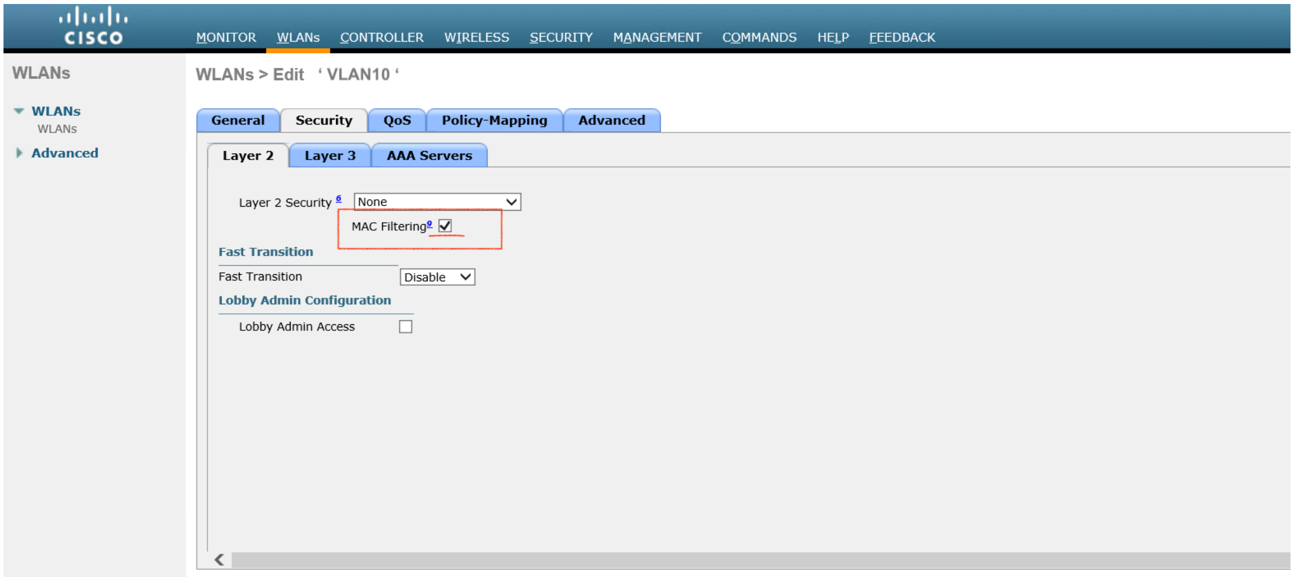


WLANs > Edit > VLAN10

Profile Name: VLAN10
Type: WLAN
SSID: VLAN10
Status: ☑ Enabled

Security Policies: MAC Filtering
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All
Interface/Interface Group(G): vlan10
Multicast Vlan Feature: □ Enabled
Broadcast SSID: ☑ Enabled
NAS-ID: wifi-onboard



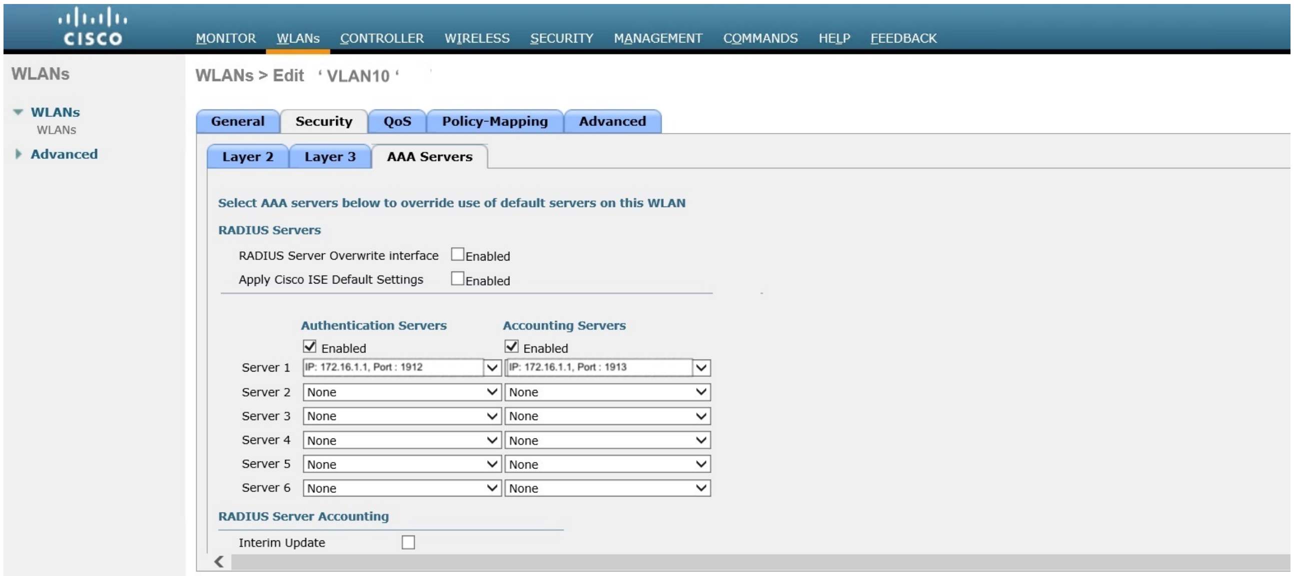
WLANs > Edit 'VLAN10'

Layer 2 Security: None
MAC Filtering ☑

Fast Transition
Fast Transition: Disable

Lobby Admin Configuration
Lobby Admin Access ☐

Normally, in a wireless LAN controller, each WLAN is mapped to a specific VLAN (SSID) so that a particular user that belongs to that WLAN is put into the specific VLAN mapped. This mapping is normally done under the Interface Name field of the WLAN SSID window.



WLANs > Edit 'VLAN10'

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface ☐Enabled
Apply Cisco ISE Default Settings ☐Enabled

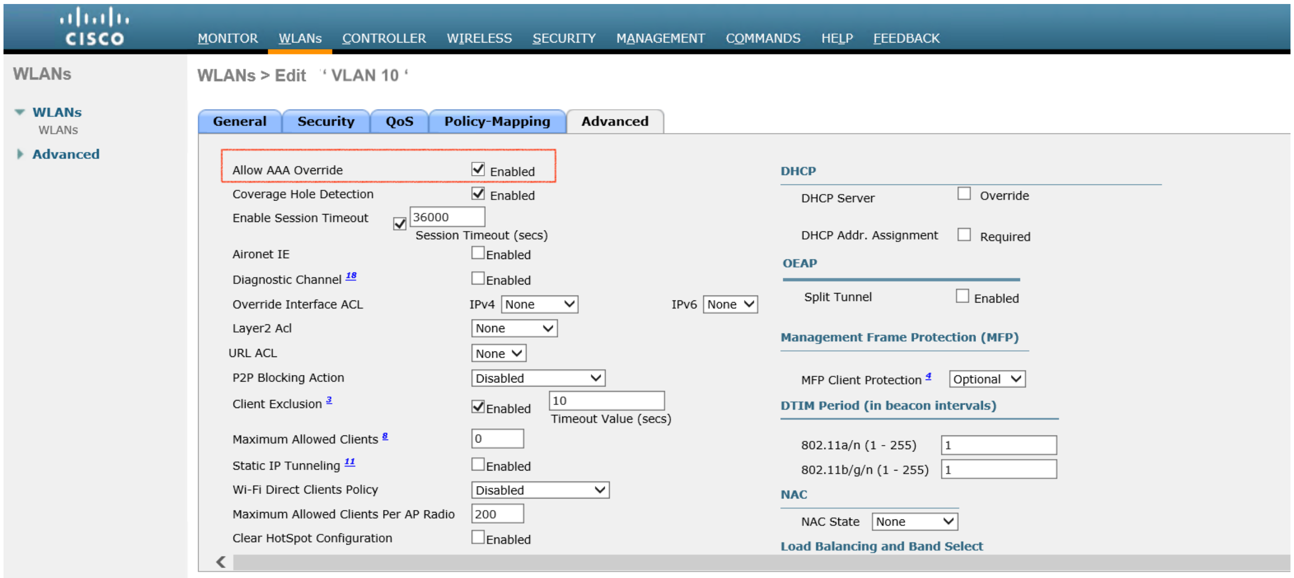
	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP: 172.16.1.1, Port : 1912	IP: 172.16.1.1, Port : 1913
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

RADIUS Server Accounting
Interim Update ☐

In the example provided, it is the job of the RADIUS server to assign a wireless client to a specific VLAN upon successful authentication. The WLANs need not be mapped to a specific dynamic interface on the WLC. Or, even though the WLAN to dynamic interface mapping is done on the WLC, the RADIUS server overrides this mapping and assigns the user that comes through that WLAN to the VLAN specified under the user Tunnel-Group-Private-ID field in the RADIUS server.

4. Check the Allow AAA Override check box in order to override the WLC configurations by the RADIUS server.

5. Enable the Allow AAA Override in the controller for each WLAN (SSID) configured.



WLANs > Edit 'VLAN 10'

Allow AAA Override ☑ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 36000 Session Timeout (secs)
Aironet IE □ Enabled
Diagnostic Channel [18] □ Enabled
Override Interface ACL IPv4 None IPv6 None
Layer2 Acl None
URL ACL None
P2P Blocking Action Disabled
Client Exclusion [3] ☑ Enabled 10 Timeout Value (secs)
Maximum Allowed Clients [8] 0
Static IP Tunneling [11] □ Enabled
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 200
Clear HotSpot Configuration □ Enabled

DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required
OEAP
Split Tunnel □ Enabled
Management Frame Protection (MFP)
MFP Client Protection [4] Optional
DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1
NAC
NAC State None
Load Balancing and Band Select

When AAA Override is enabled, and a client has AAA and controller WLAN authentication parameters that conflict, client authentication is performed by the AAA (RADIUS) server. As part of this authentication, the operating system moves clients to a VLAN returned by the AAA server. This is predefined in the controller interface configuration.

For instance, if the corporate WLAN primarily uses a Management Interface assigned to VLAN 2, and if the AAA Override returns a redirect to VLAN 100, the operating system redirects all client transmissions to VLAN 100 even if the physical port to which VLAN 100 is assigned. When AAA Override is disabled, all client authentication defaults to the controller authentication parameter settings, and authentication is only performed by the AAA server if the controller WLAN does not contain any client-specific authentication parameters.

4. Configure Radius Change of Authorization

Refer to this link
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-rad-coa.html#GUID-46B9CBDC-1F98-4606-B742-F33323268EDC

Cisco Meraki Configuration

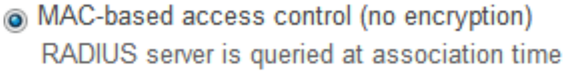
Requires MR 24.0 and MS 8.10 or higher

1. Enabling MAC based access control on an SSID

MAC-based access control admits or denies wireless association based on the connecting device's MAC address. In this authentication method wireless devices use their MAC address as the username and password. Follow the steps below to configure an SSID to require MAC based access control with RADIUS.

1. From Dashboard navigate to **Configure > Access control**.

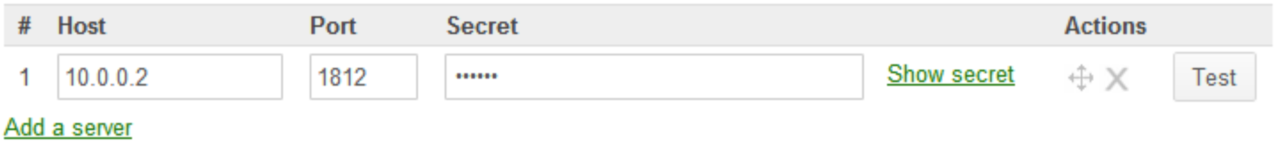
2. Select **MAC-based access control (no encryption)** for **Association requirements.**



● MAC-based access control (no encryption)
RADIUS server is queried at association time

3. For **Splash page** choose **None. Click through splash** can be selected if desired.

4. For **RADIUS server**, click **Add a server.** Enter the RADIUS server IP address, listening port, and RADIUS shared secret to be used by your APs which are configured RADIUS clients on the server.

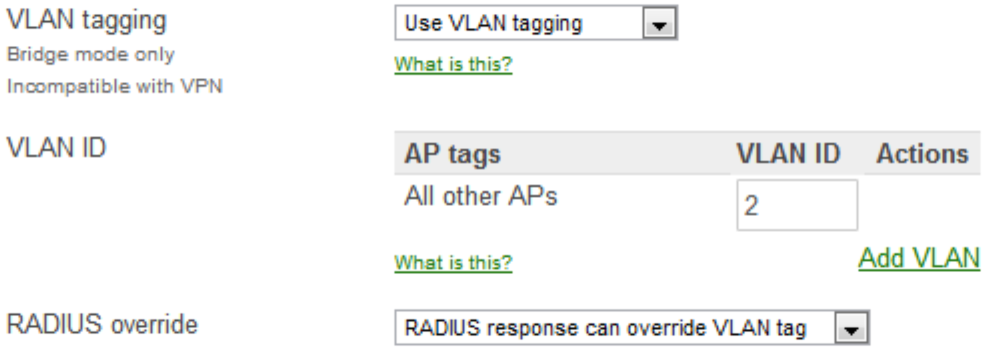


#	Host	Port	Secret		Actions	
1	10.0.0.2	1812	••••••	Show secret	✥ ✕	Test

Add a server

5. For **Addressing and traffic** choose **Bridge mode** in a VLAN environment. **NAT mode** could be used without VLANs if desired.

6. An SSID can bridge wireless devices onto different VLANs. A default SSID VLAN can be set using the VLAN tag drop down. Then by setting the **RADIUS response** it can override VLAN tag from VLAN override drop down. RADIUS accept messages containing a different VLAN tag will be able to override the default VLAN for the SSID.



VLAN tagging: Use VLAN tagging
Bridge mode only
Incompatible with VPN
What is this?

VLAN ID:

AP tags	VLAN ID	Actions
All other APs	2	

What is this? Add VLAN

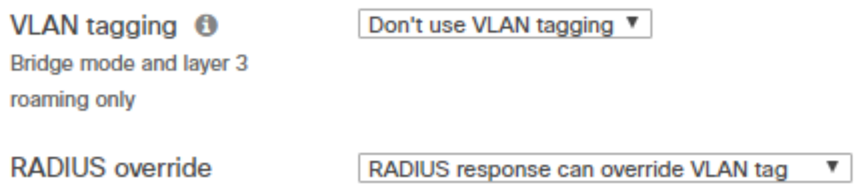
RADIUS override: RADIUS response can override VLAN tag

7. Click **Save changes.**

2. Configuring AP to accept VLAN information

To configure the AP to accept the VLAN information sent from by the RADIUS server, navigate to **Wireless > Configure > Access Control** and see the Addressing and Traffic section. Enable set "Radius Override" to "RADIUS Response Can Override VLAN tag."

This setting can override the configured SSID VLAN or apply a VLAN if one is not specified:

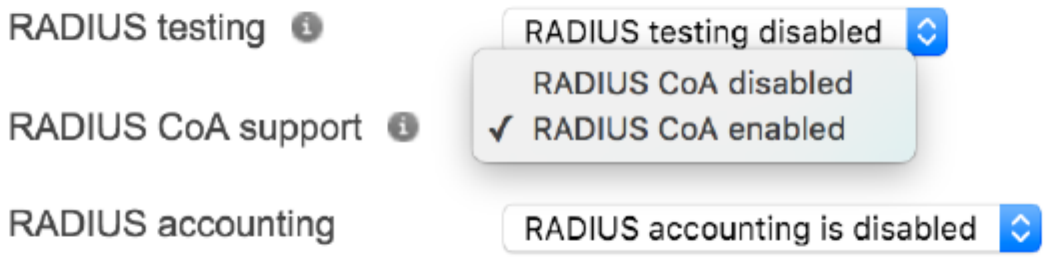


VLAN tagging: Don't use VLAN tagging
Bridge mode and layer 3 roaming only

RADIUS override: RADIUS response can override VLAN tag

3. Enable RADIUS CoA support

Enable CoA support. Meraki devices will act as a RADIUS Dynamic Authorization Server (CoA) and will respond to RADIUS Disconnect and Change of Authorization messages sent by the RADIUS server.



RADIUS testing: RADIUS testing disabled

RADIUS CoA support:
RADIUS CoA disabled
✓ RADIUS CoA enabled

RADIUS accounting: RADIUS accounting is disabled

4. Dynamic Authorization Port Settings

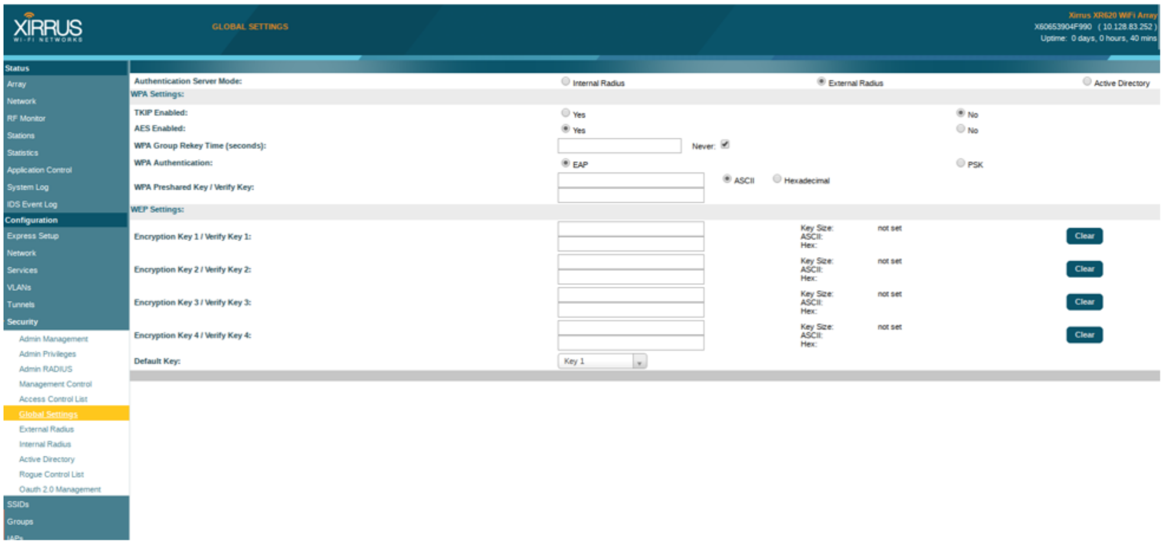
The access point's UDP Port for CoA must be reachable from your RADIUS server:
Port 3799 must be accessible

Xirrus Configuration

Requires version 8.4.6 and above.

1. Configure Radius Server

Under *Security > Global Settings*, select External Radius for Authentication Server Mode.



Authentication Server Mode: ○ Internal Radius ● External Radius ○ Active Directory

WPA Settings:

TKIP Enabled: ○ Yes ● No

AES Enabled: ● Yes ○ No

WPA Group Rekey Time (seconds): Never: ☑

WPA Authentication: ● EAP ○ PSK

WPA Preshared Key / Verify Key: ● ASCII ○ Hexadecimal

WEP Settings:

Encryption Key 1 / Verify Key 1: Key Size: not set ASCII: Hex:

Encryption Key 2 / Verify Key 2: Key Size: not set ASCII: Hex:

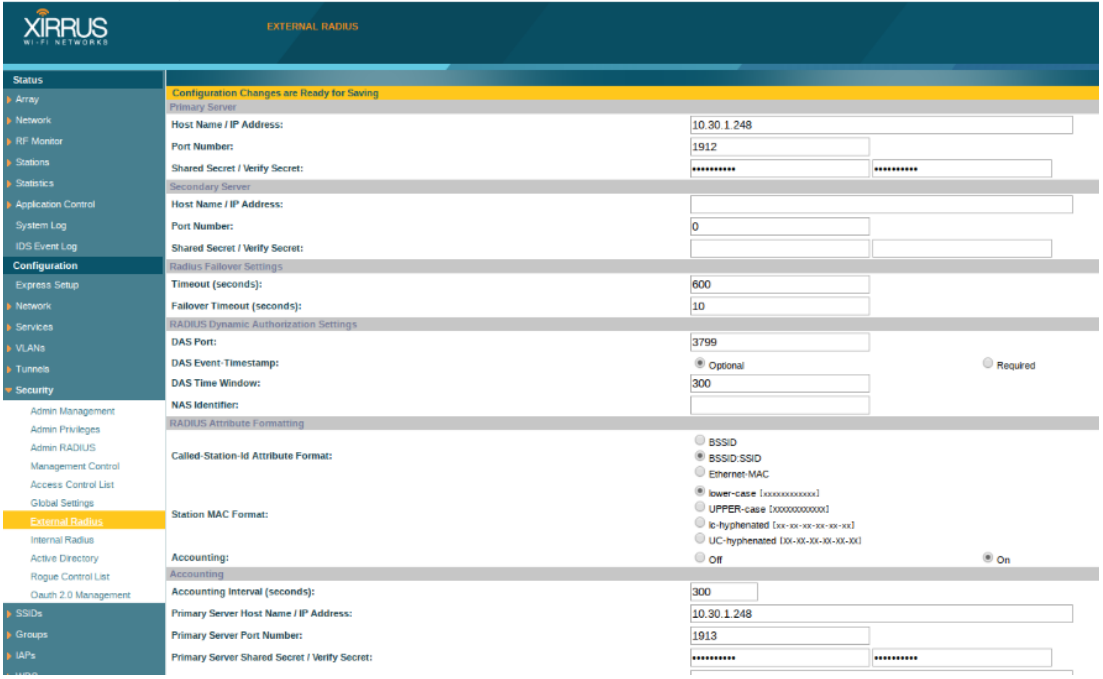
Encryption Key 3 / Verify Key 3: Key Size: not set ASCII: Hex:

Encryption Key 4 / Verify Key 4: Key Size: not set ASCII: Hex:

Default Key: Key 1

Under Security > External Radius,

Configure Primary Server as ANTlabs gateway IP port 1912.
Configure Accounting as ANTlabs gateway IP port 1913.
Configure DAS Port as 3799.
Configure DAS Event-Timestamp as Optional.



Configuration Changes are Ready for Saving

Primary Server

Host Name / IP Address: 10.30.1.248

Port Number: 1912

Shared Secret / Verify Secret: •••••••••• ••••••••••

Secondary Server

Host Name / IP Address:

Port Number: 0

Shared Secret / Verify Secret:

Radius Failover Settings

Timeout (seconds): 600

Failover Timeout (seconds): 10

RADIUS Dynamic Authorization Settings

DAS Port: 3799

DAS Event-Timestamp: ● Optional ○ Required

DAS Time Window: 300

NAS Identifier:

RADIUS Attribute Formatting

Called-Station-Id Attribute Format: ○ BSSID ● BSSID:SSID ○ Ethernet-MAC

Station MAC Format: ● lower-case [xxxxxxxxxxxx] ○ UPPER-case [XXXXXXXXXXXX] ○ lc-hyphenated [xx-xx-xx-xx-xx-xx] ○ UC-hyphenated [XX-XX-XX-XX-XX-XX]

Accounting: ○ Off ● On

Accounting

Accounting Interval (seconds): 300

Primary Server Host Name / IP Address: 10.30.1.248

Primary Server Port Number: 1913

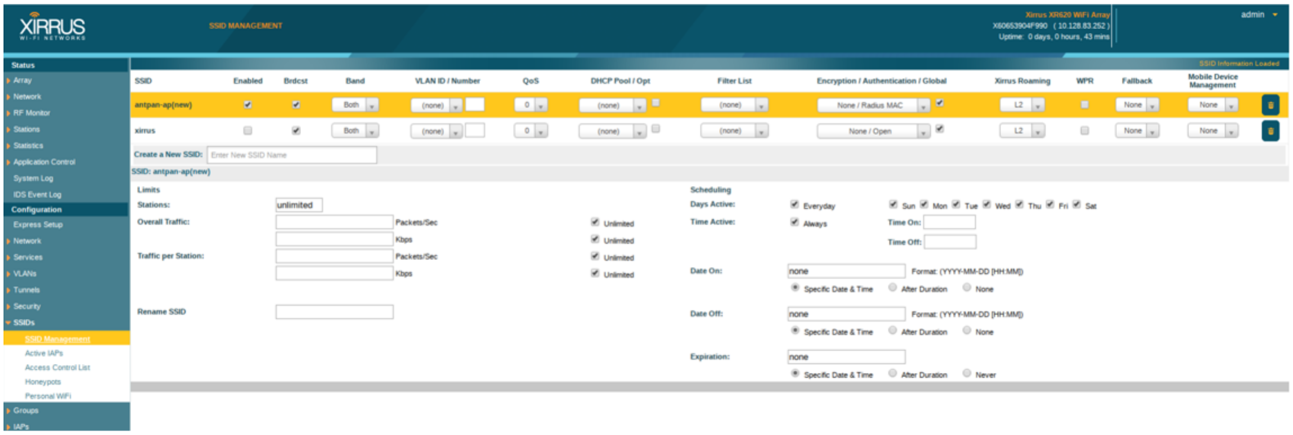
Primary Server Shared Secret / Verify Secret: •••••••••• ••••••••••

2. Configure Mac based Authentication

Under *SSIDs > SSID Management*

Configure 'Authentication' as 'Radius MAC'.

Check 'Global' to use global Radius configuration.



X60653904F990 (10.128.83.252)
Uptime: 0 days, 0 hours, 43 mins

SSID	Enabled	Brdcst	Band	VLAN ID / Number	QoS	DHCP Pool / Opt	Filter List	Encryption / Authentication / Global	Xirrus Roaming	WPR	Fallback	Mobile Device Management
antpan-ap(new)	☑	☑	Both	(none)	0	(none) □	(none)	None / Radius MAC ☑	L2	□	None	None
xirrus	□	☑	Both	(none)	0	(none) □	(none)	None / Open ☑	L2	□	None	None

Create a New SSID: Enter New SSID Name

SSID: antpan-ap(new)

Limits

Stations: unlimited

Overall Traffic: Packets/Sec ☑ Unlimited

Kbps ☑ Unlimited

Traffic per Station: Packets/Sec ☑ Unlimited

Kbps ☑ Unlimited

Rename SSID

Scheduling

Days Active: ☑ Everyday ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time Active: ☑ Always Time On: Time Off:

Date On: none Format: (YYYY-MM-DD [HH:MM])

● Specific Date & Time ○ After Duration ○ None

Date Off: none Format: (YYYY-MM-DD [HH:MM])

● Specific Date & Time ○ After Duration ○ None

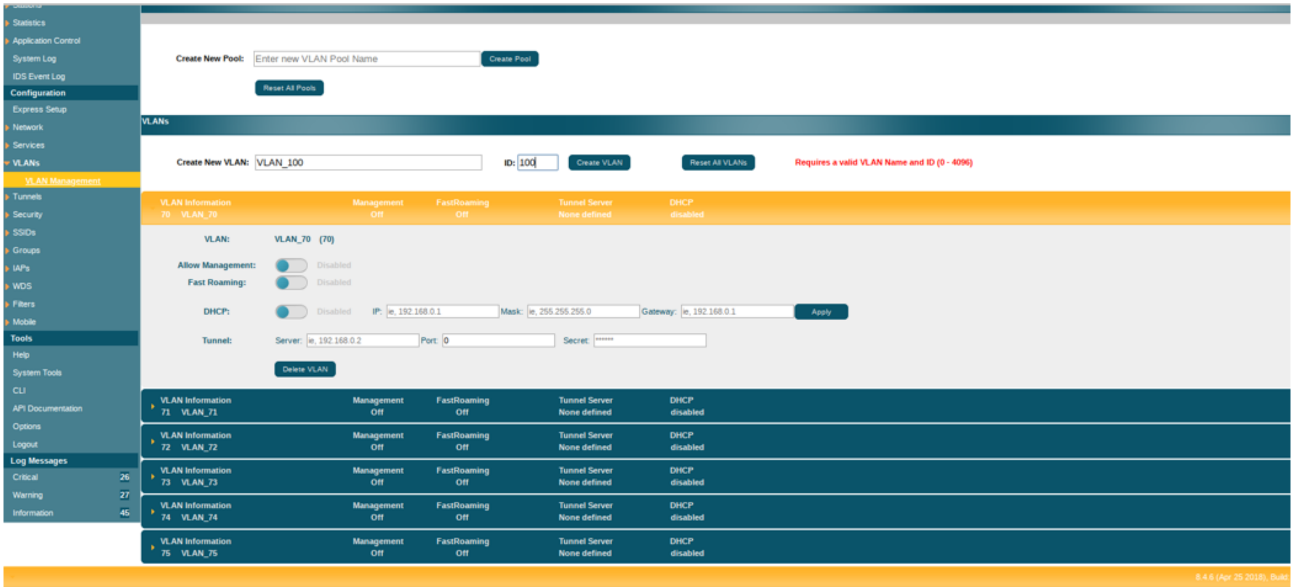
Expiration: none

● Specific Date & Time ○ After Duration ○ Never

3. Creating VLAN

Under *VLANs > VLAN Management*

Add all the dynamic VLANs required.



Create New Pool: Enter new VLAN Pool Name

Create New VLAN: VLAN_100 ID: 100

Requires a valid VLAN Name and ID (0 - 4096)

VLAN Information	Management	FastRoaming	Tunnel Server	DHCP
70 VLAN_70	Off	Off	None defined	disabled

VLAN: VLAN_70 (70)

Allow Management: Disabled

Fast Roaming: Disabled

DHCP: Disabled IP: ie, 192.168.0.1 Mask: ie, 255.255.255.0 Gateway: ie, 192.168.0.1

Tunnel: Server: ie, 192.168.0.2 Port: 0 Secret: ******

VLAN Information	Management	FastRoaming	Tunnel Server	DHCP
71 VLAN_71	Off	Off	None defined	disabled
72 VLAN_72	Off	Off	None defined	disabled
73 VLAN_73	Off	Off	None defined	disabled
74 VLAN_74	Off	Off	None defined	disabled
75 VLAN_75	Off	Off	None defined	disabled

8.4.6 (Apr 25 2018), Build