RAP split-tunnel (802.1X authentication)

Release 6.2.0.0 controller – June 2013

Contents

MUST READ - BACKGROUND!

This configuration example is based on two previous examples posted:

For the Beginner – Configuring an 802.1X WLAN with the Controller GUI

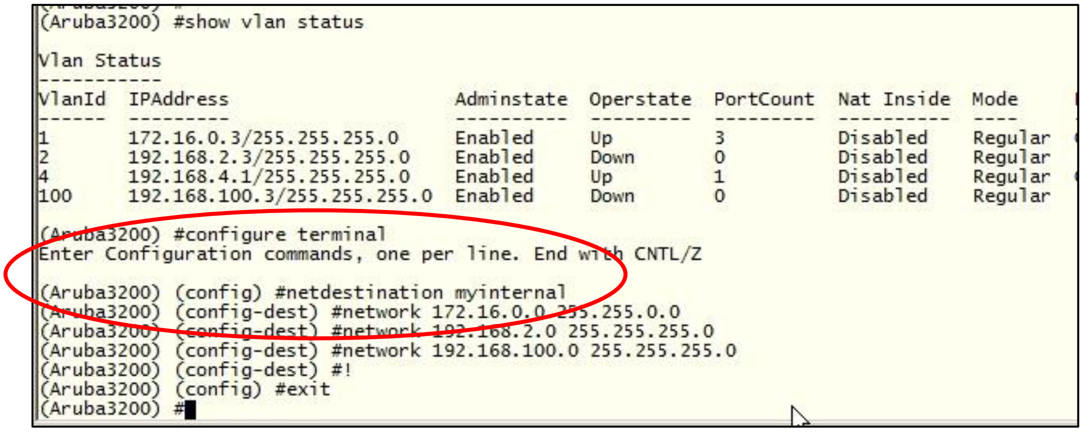
For the Beginner - RAP Installation-Basic

It is recommended you read and understand the above two examples as well as have your version of the configurations installed on your controller. VLAN's and IP address in the examples may have changed but the overall process is still valid to follow.

Create an internal network ‘netdestination’

The key to split tunnel mode is in the User Policy. It is the User Policy that determines what is forwarded through the tunnel and what is placed on the local network. The netdestination definition should contain all the internal network IP addresses the client can connect to. These are the network destinations you want the RAP to forward via the RAP/Controller VPN tunnel to the main site. This can be done with the CLI (shown) or the GUI (Configuration > Stateful Firewall > Destinations).

In this example the internal networks (netdestination myinternal) are the 172.16.0.0, 192.168.2.0 and 192.168.100.0.

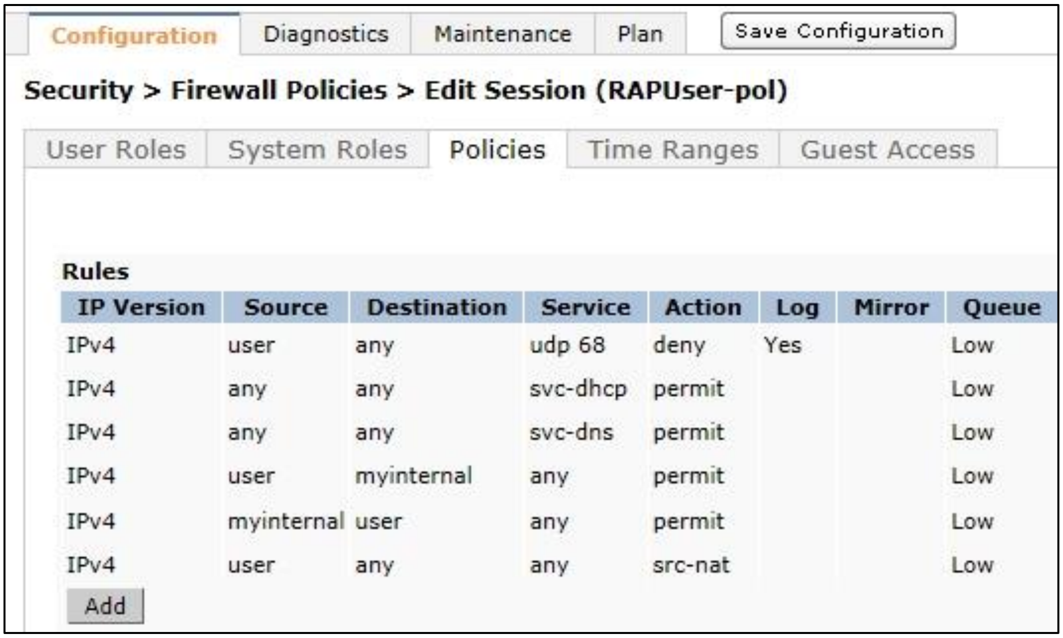


```
(Aruba3200) #show vlan status

Vlan Status
-----------
VlanId  IPAddress                 Adminstate  Operstate  PortCount  Nat Inside  Mode
------  ---------                 ----------  ---------  ---------  ----------  ----
1       172.16.0.3/255.255.255.0  Enabled     Up         3          Disabled    Regular
2       192.168.2.3/255.255.255.0 Enabled     Down       0          Disabled    Regular
4       192.168.4.1/255.255.255.0 Enabled     Up         1          Disabled    Regular
100     192.168.100.3/255.255.255.0 Enabled   Down       0          Disabled    Regular

(Aruba3200) #configure terminal
Enter Configuration commands, one per line.  End with CNTL/Z

(Aruba3200) (config) #netdestination myinternal
(Aruba3200) (config-dest) #network 172.16.0.0 255.255.0.0
(Aruba3200) (config-dest) #network 192.168.2.0 255.255.255.0
(Aruba3200) (config-dest) #network 192.168.100.0 255.255.255.0
(Aruba3200) (config-dest) #!
(Aruba3200) (config) #exit
(Aruba3200) #
```

Create the RAP User Policy

Configuration > Access Control > Policies

Use the netdestination alias of the internal network accordingly in the RAP user policy. Note the last rule is source NAT (src-nat). This policy states that if the destination does not match the myinternal rule the traffic will **NOT** be forwarded to the controller through the VPN connection but ‘src-nat’ from the RAP to the local subnet.



Security > Firewall Policies > Edit Session (RAPUser-pol)

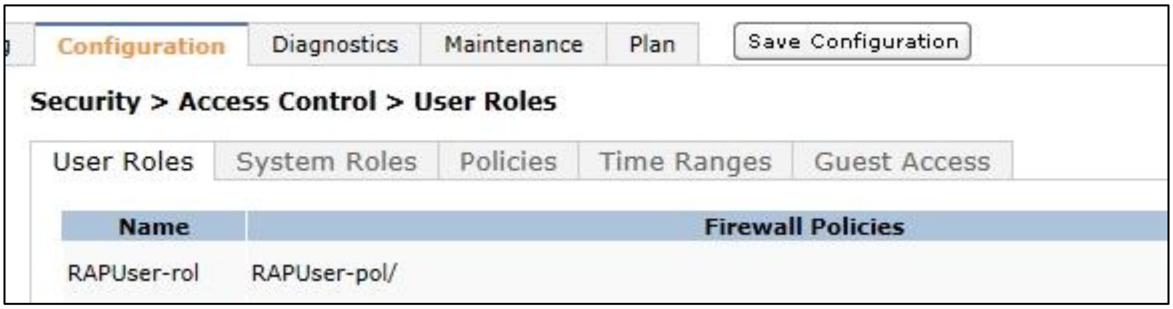
Rules

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue
IPv4	user	any	udp 68	deny	Yes		Low
IPv4	any	any	svc-dhcp	permit			Low
IPv4	any	any	svc-dns	permit			Low
IPv4	user	myinternal	any	permit			Low
IPv4	myinternal	user	any	permit			Low
IPv4	user	any	any	src-nat			Low

Create the RAP User Role

Configuration > Access Control > User Roles

Configure a RAP user role and add the ‘RAPUser-pol’ policy to it. This is the role the user will be assigned when logging into the RAP wifi and authenticated by the AAA policy (next step).



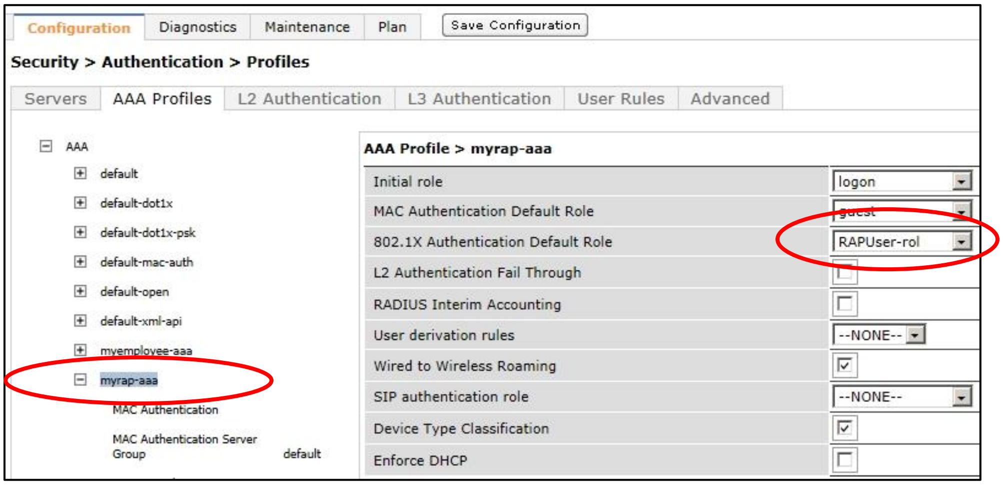
Security > Access Control > User Roles

Name	Firewall Policies
RAPUser-rol	RAPUser-pol/

Create a new RAP AAA server

Configuration > Authentication > AAA Profiles

Create a new RAP AAA Profile and ensure you select in the “802.1X Authenticated default role” the RAPUser-rol role created earlier. When authenticated with this AAA profile the user will be placed in the RAPUser-rol



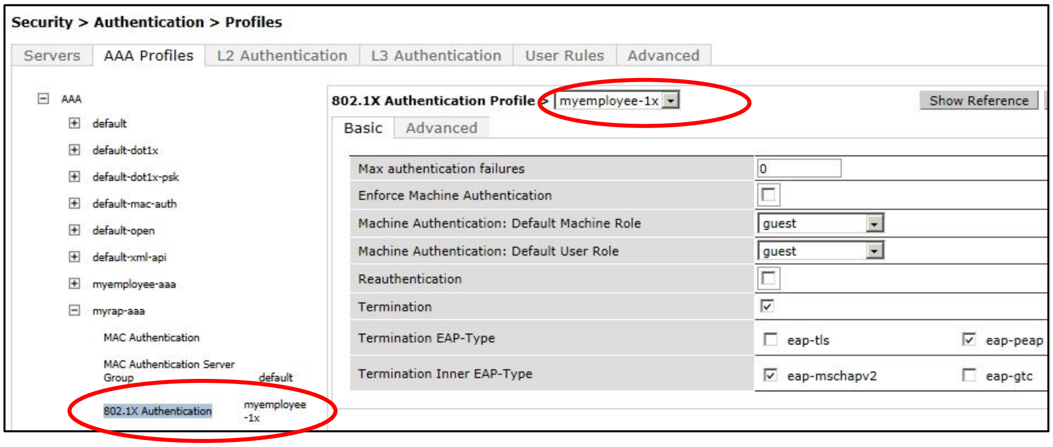
Security > Authentication > Profiles

AAA Profile > myrap-aaa

Initial role	logon
MAC Authentication Default Role	guest
802.1X Authentication Default Role	RAPUser-rol
L2 Authentication Fail Through	□
RADIUS Interim Accounting	□
User derivation rules	--NONE--
Wired to Wireless Roaming	☑
SIP authentication role	--NONE--
Device Type Classification	☑
Enforce DHCP	□

Continue configuration of the new RAP AAA Profile

Select and expand the 802.1X Authentication section of the new RAP AAA profile. Select the already existing corporate location 802.1X profile (in this example ‘myemployee-1x’)



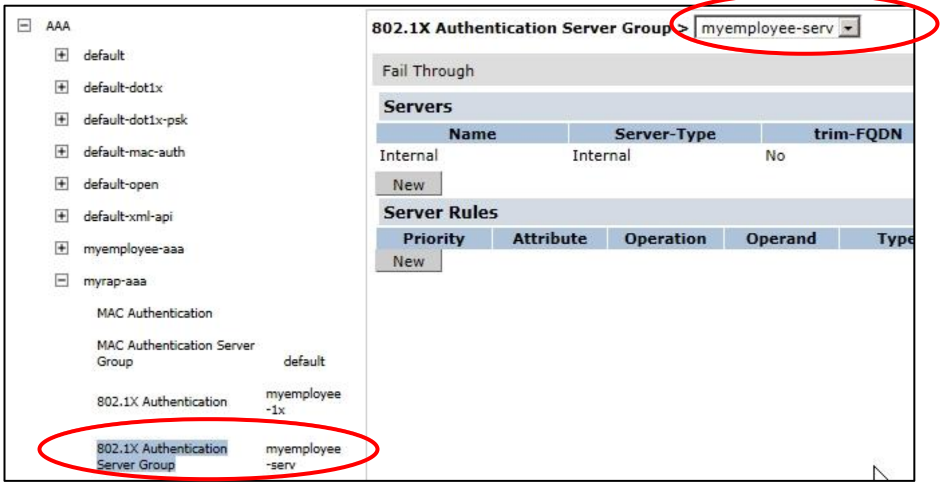
Security > Authentication > Profiles

802.1X Authentication Profile > myemployee-1x

Max authentication failures	0	
Enforce Machine Authentication	□	
Machine Authentication: Default Machine Role	guest	
Machine Authentication: Default User Role	guest	
Reauthentication	□	
Termination	☑	
Termination EAP-Type	□ eap-tls	☑ eap-peap
Termination Inner EAP-Type	☑ eap-mschapv2	□ eap-gtc

Continue configuration of the new RAP AAA Profile

Select and expand the 802.1X Authentication Server Group of the new RAP AAA profile. This is the server the username and password will be authenticated against. Select the already existing corporate location server (in this example 'myemployee-serv')



- AAA
  - default
  - default-dot1x
  - default-dot1x-psk
  - default-mac-auth
  - default-open
  - default-xml-api
  - myemployee-aaa
  - myrap-aaa
    - MAC Authentication
    - MAC Authentication Server Group: default
    - 802.1X Authentication: myemployee-1x
    - 802.1X Authentication Server Group: myemployee-serv

802.1X Authentication Server Group > myemployee-serv

Fail Through

Servers

Name	Server-Type	trim-FQDN
Internal	Internal	No

New

Server Rules

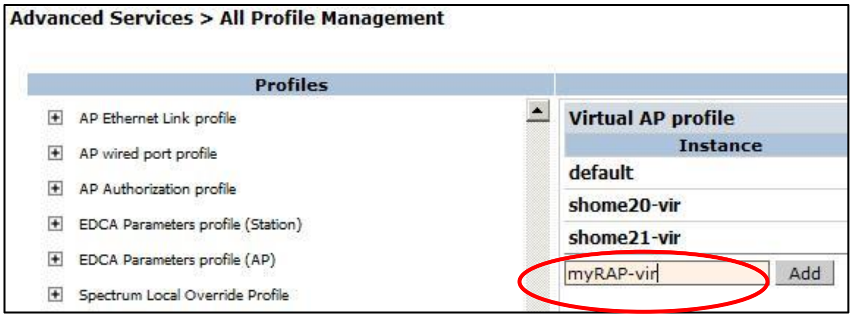
Priority	Attribute	Operation	Operand	Type

New

Create the myRAP Virtual AP

Configuration > Advanced Services > All Profiles

Add a new virtual AP for the myRAP group (Advanced Services > All Profile Management > Wireless LAN > Virtual AP profile)



Advanced Services > All Profile Management

Profiles

- AP Ethernet Link profile
- AP wired port profile
- AP Authorization profile
- EDCA Parameters profile (Station)
- EDCA Parameters profile (AP)
- Spectrum Local Override Profile

Virtual AP profile

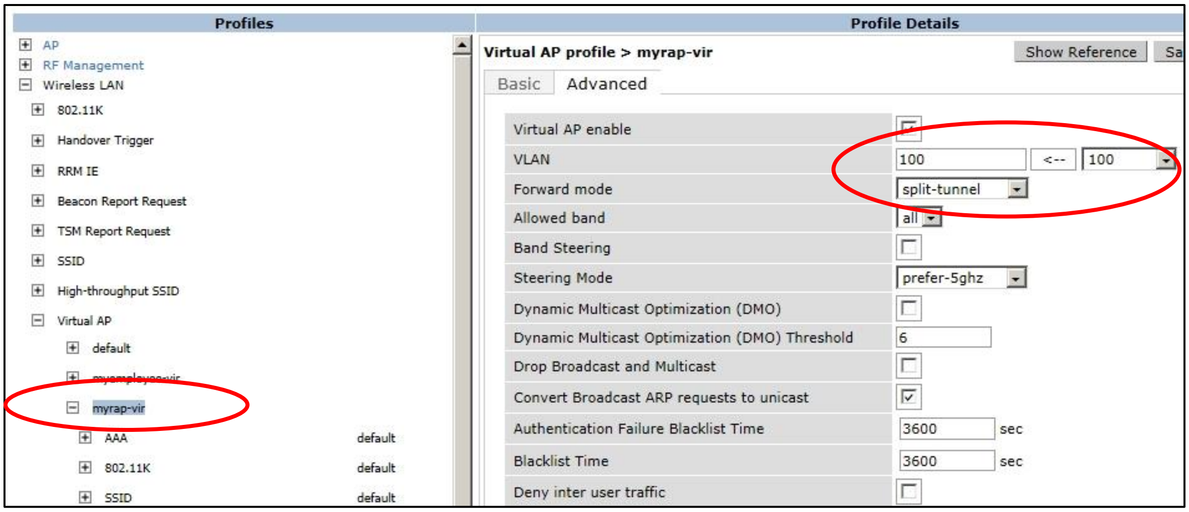
Instance
default
shome20-vir
shome21-vir
myRAP-vir

Add

Edit the myrap Virtual AP

Click on and open the new myRAP-vir virtual profile

Set the VLAN the RAP User will be placed in, and received DHCP from, and set the Forwarding Mode to 'split-tunnel'



Profiles

- AP
- RF Management
- Wireless LAN
  - 802.11K
  - Handover Trigger
  - RRM IE
  - Beacon Report Request
  - TSM Report Request
  - SSID
  - High-throughput SSID
  - Virtual AP
    - default
    - myemployee-vir
    - myrap-vir
      - AAA: default
      - 802.11K: default
      - SSID: default

Profile Details

Virtual AP profile > myrap-vir

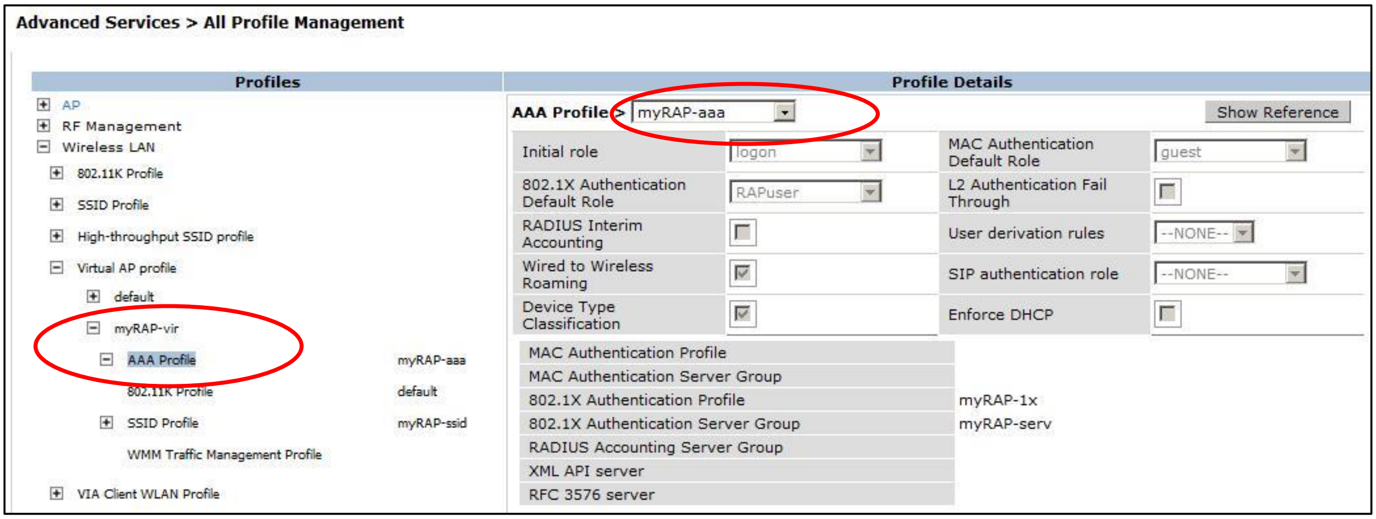
Show Reference | Sa

Basic | Advanced

Virtual AP enable	☑
VLAN	100 <-- 100
Forward mode	split-tunnel
Allowed band	all
Band Steering	□
Steering Mode	prefer-5ghz
Dynamic Multicast Optimization (DMO)	□
Dynamic Multicast Optimization (DMO) Threshold	6
Drop Broadcast and Multicast	□
Convert Broadcast ARP requests to unicast	☑
Authentication Failure Blacklist Time	3600 sec
Blacklist Time	3600 sec
Deny inter user traffic	□

Continue setting up the myrap-vir – the AAA Profile

Expand the section AAA Profile and use the pull down to select the previously created new RAP AAA Profile



Advanced Services > All Profile Management

Profiles

- ⊞ AP
- ⊞ RF Management
- ⊟ Wireless LAN
  - ⊞ 802.11K Profile
  - ⊞ SSID Profile
  - ⊞ High-throughput SSID profile
  - ⊟ Virtual AP profile
    - ⊞ default
    - ⊟ myRAP-vir
      - ⊟ AAA Profile — myRAP-aaa
      - 802.11K Profile — default
      - ⊞ SSID Profile — myRAP-ssid
      - WMM Traffic Management Profile
  - ⊞ VIA Client WLAN Profile

Profile Details

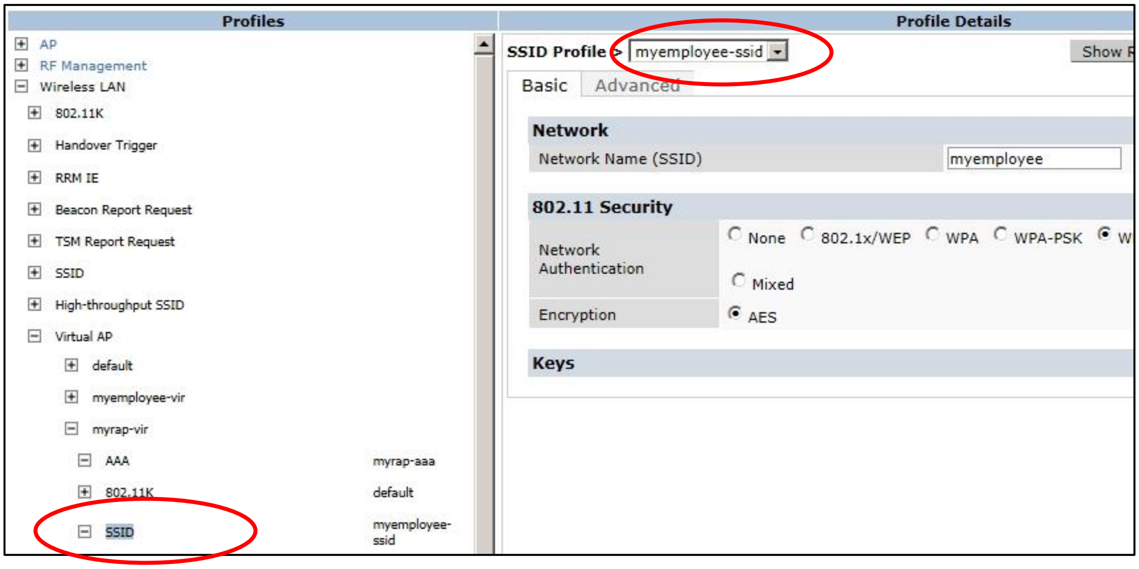
AAA Profile > myRAP-aaa ▾ — Show Reference

Initial role	logon ▾	MAC Authentication Default Role	guest ▾
802.1X Authentication Default Role	RAPuser ▾	L2 Authentication Fail Through	□
RADIUS Interim Accounting	□	User derivation rules	--NONE-- ▾
Wired to Wireless Roaming	☑	SIP authentication role	--NONE-- ▾
Device Type Classification	☑	Enforce DHCP	□

MAC Authentication Profile	
MAC Authentication Server Group	
802.1X Authentication Profile	myRAP-1x
802.1X Authentication Server Group	myRAP-serv
RADIUS Accounting Server Group	
XML API server	
RFC 3576 server	

Continue setting up the myRAP-vir – the SSID profile

Previously an SSID Profile was created for user authentication at the corporate site (For the Beginner – Configuring an 802.1X WLAN with the Controller GUI). We will reuse this SSID for the RAP Virtual AP profile.



Profiles

- ⊞ AP
- ⊞ RF Management
- ⊟ Wireless LAN
  - ⊞ 802.11K
  - ⊞ Handover Trigger
  - ⊞ RRM IE
  - ⊞ Beacon Report Request
  - ⊞ TSM Report Request
  - ⊞ SSID
  - ⊞ High-throughput SSID
  - ⊟ Virtual AP
    - ⊞ default
    - ⊞ myemployee-vir
    - ⊟ myrap-vir
      - ⊟ AAA — myrap-aaa
      - ⊞ 802.11K — default
      - ⊟ SSID — myemployee-ssid

Profile Details

SSID Profile > myemployee-ssid ▾ — Show R

Basic | Advanced

Network

Network Name (SSID): myemployee

802.11 Security

Network Authentication: ○ None ○ 802.1x/WEP ○ WPA ○ WPA-PSK ● W
○ Mixed

Encryption: ● AES

Keys

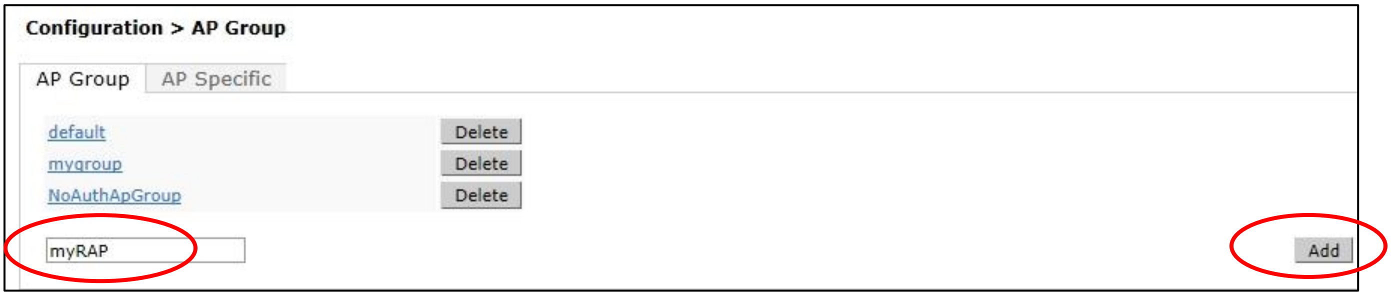
Create the RAP AP Group

Setup a new AP Group for the RAP's (if not already completed)

"Configuration" > "Wireless" > "AP Configuration" > New

Add the new AP Group Name (in this example "myRAP")

Click "Add" to finish and "Save Configuration"



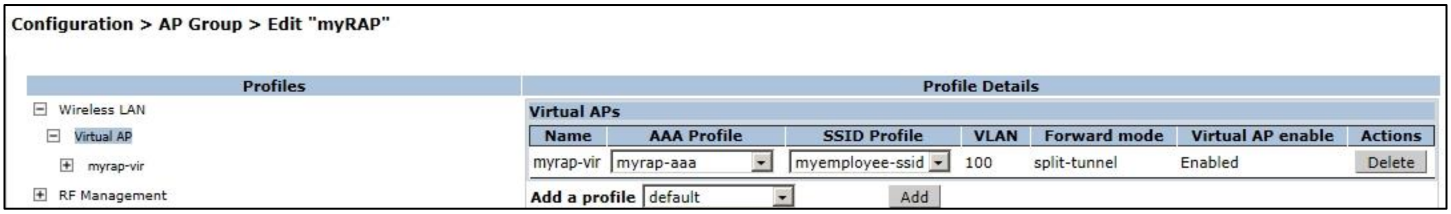
Configuration > AP Group

AP Group | AP Specific

default	Delete
mygroup	Delete
NoAuthApGroup	Delete

myRAP — Add

Expand the Wireless LAN section
Click on the Virtual AP
Use the pull down to select the myrap-vir created earlier in this example.



Configuration > AP Group > Edit "myRAP"

Virtual APs

Name	AAA Profile	SSID Profile	VLAN	Forward mode	Virtual AP enable	Actions
myrap-vir	myrap-aaa	myemployee-ssid	100	split-tunnel	Enabled	Delete

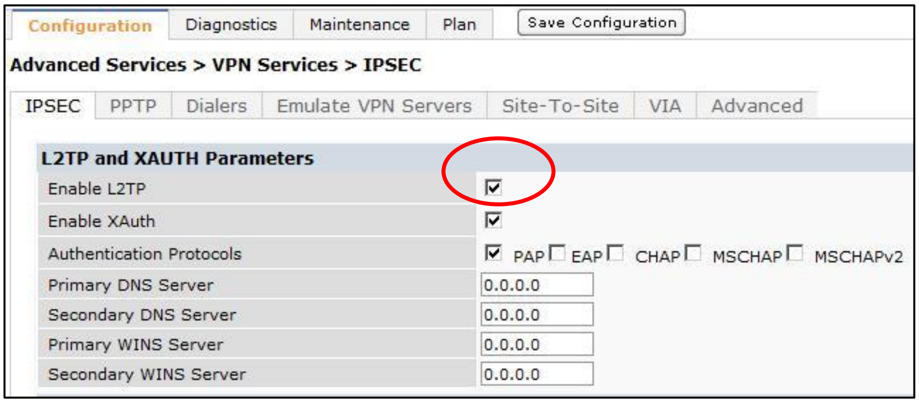
Add a profile: default — Add

Configure the Controller VPN for RAP Access

These steps have been included in the example "For the Beginner - RAP Installation-Basic" as well here, if already completed do not duplicate.

Go to Configuration > Advanced Services > VPN Services

Ensure L2TP is enabled



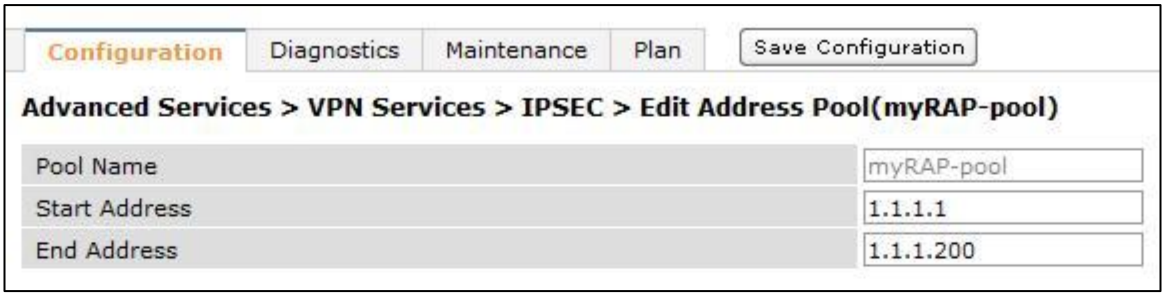
Advanced Services > VPN Services > IPSEC

L2TP and XAUTH Parameters

Enable L2TP	☑
Enable XAuth	☑
Authentication Protocols	☑ PAP ☐ EAP ☐ CHAP ☐ MSCHAP ☐ MSCHAPv2
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Primary WINS Server	0.0.0.0
Secondary WINS Server	0.0.0.0

Assign a RAP Address Pool

This is the inner IP address used between the controller and RAP for the IPSec tunnel (recommended this is NOT an existing IP address space in the network)



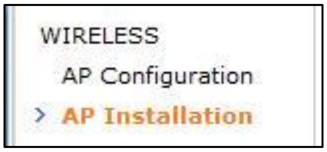
Advanced Services > VPN Services > IPSEC > Edit Address Pool(myRAP-pool)

Pool Name	myRAP-pool
Start Address	1.1.1.1
End Address	1.1.1.200

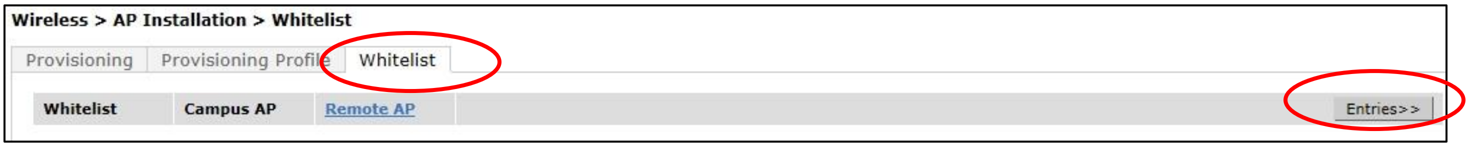
After clicking DONE on the IPSEC > Add Address Pool page ensure you "**APPLY**" the changes at the bottom of the **VPN Services** page

Add the RAP MAC address to the Whitelist

Go to “Configuration” > “Wireless” > “AP Installation”

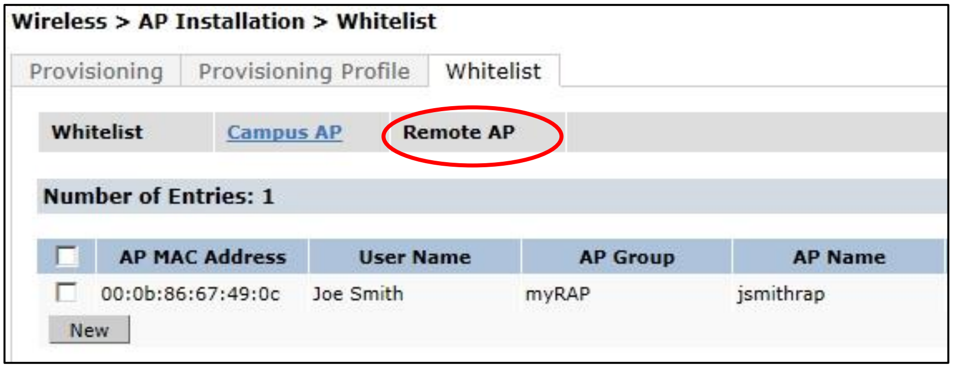


Select the “Whitelist” tab and select Entries



Then elect “Remote AP” and add the NEW entry

Enter the MAC address of the **RAP** and additional data related to the user and assign to the “RAP” AP Group



Number of Entries: 1

☐	AP MAC Address	User Name	AP Group	AP Name
☐	00:0b:86:67:49:0c	Joe Smith	myRAP	jsmithrap

Click “Add” when completed

“Save Configuration”

CLI checks and Troubleshooting is included in the original “For the Beginner - RAP Installation-Basic” document