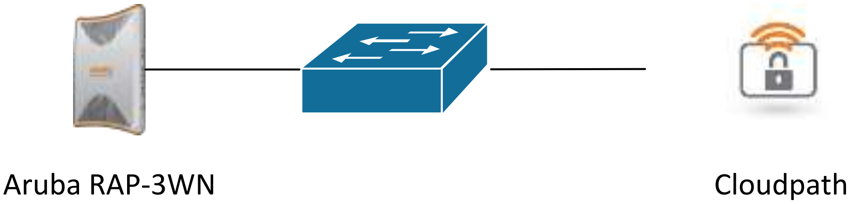
Cloudpath and Aruba Instant Integration

This document describes the process to use Ruckus Cloudpath to secure an Aruba Instant network. The following versions were used for this example:

- Ruckus Cloudpath 5.1.3483
- Aruba RAP-3WN-US
  - OS Version 6.4.4.8-4.2.4.6_58505

Network Diagram:



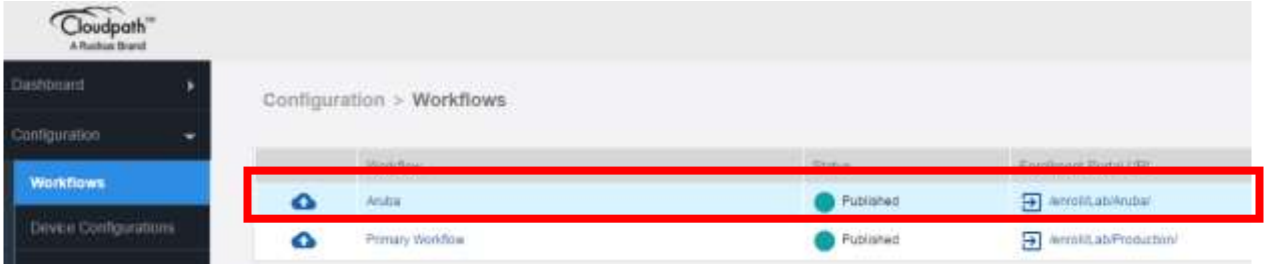
You will need to have the Aruba Instant basic configuration complete before you begin this process (IP Address of Controller, additional APs added, username and password, etc.)

For this example, we will create and Onboarding SSID for clients to receive their certificate from Cloudpath and a secure SSID for the client to be moved to after they receive their certificate. We will also create a workflow in Cloudpath to authenticate a user from AD and issue them a certificate to be authenticated with.

On Ruckus Cloudpath:

Go to Configurations -> Workflows

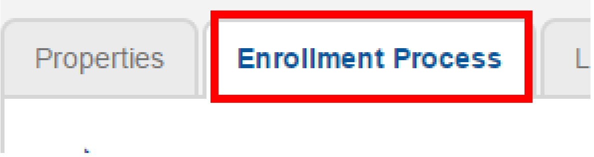
Note: *For this example, I have created a dedicated workflow for this Aruba example. This is not necessary if it is your only network to authenticate for.*



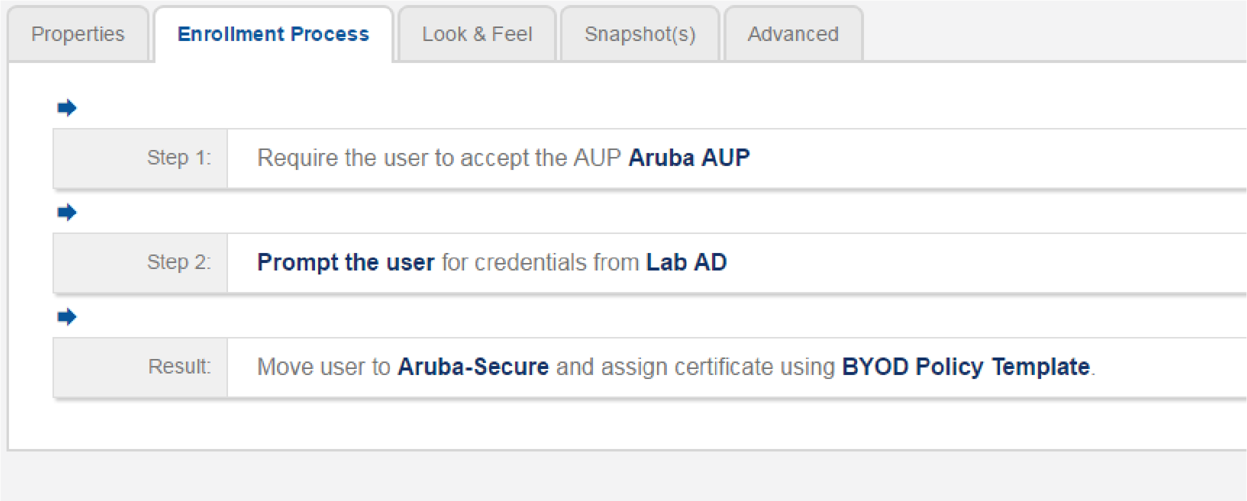
Configuration > Workflows

	Workflow	Status	Enrollment Portal URL
	Aruba	Published	/enroll/Lab/Aruba/
	Primary Workflow	Published	/enroll/Lab/Production/

Select your Workflow and go to Enrollment Process Tab



Here is what our workflow looks like for this example. Please refer to the Cloudpath configuration guide for a through description of workflow creation.



Step 1: Require the user to accept the AUP **Aruba AUP**

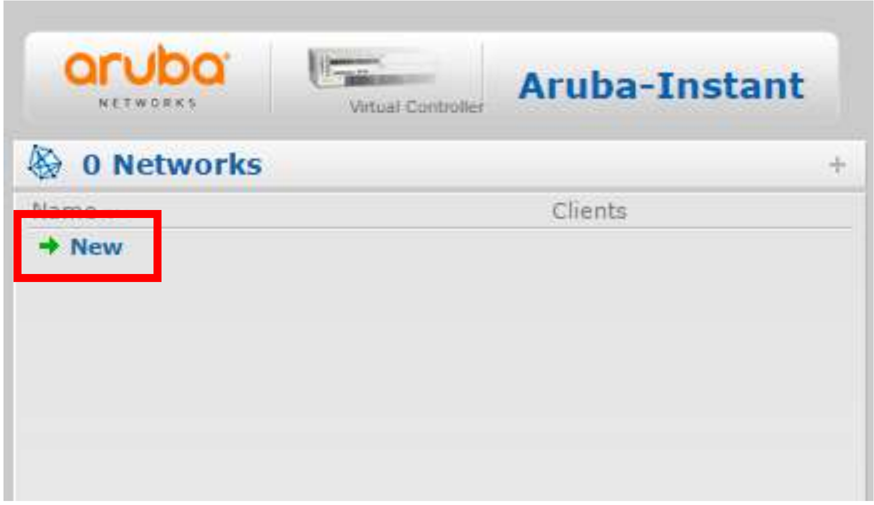
Step 2: **Prompt the user** for credentials from **Lab AD**

Result: Move user to **Aruba-Secure** and assign certificate using **BYOD Policy Template**.

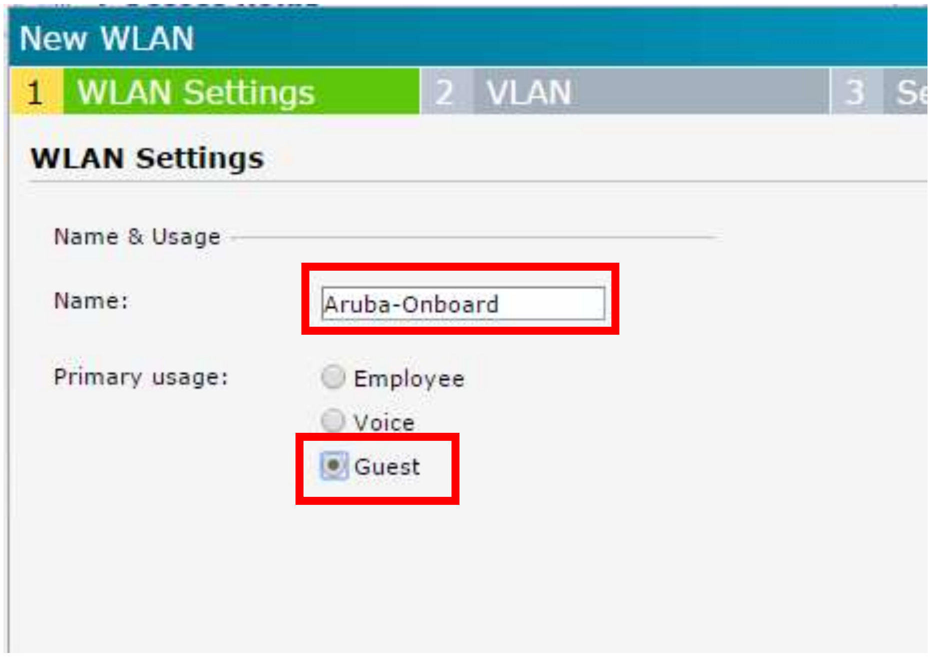
<u>On the Aruba Instant Controller:</u>

<u>Create the Onboarding SSID</u>

Select New under Networks.



Name the SSID and select Guest as the Primary Usage. Click Next



WLAN Settings

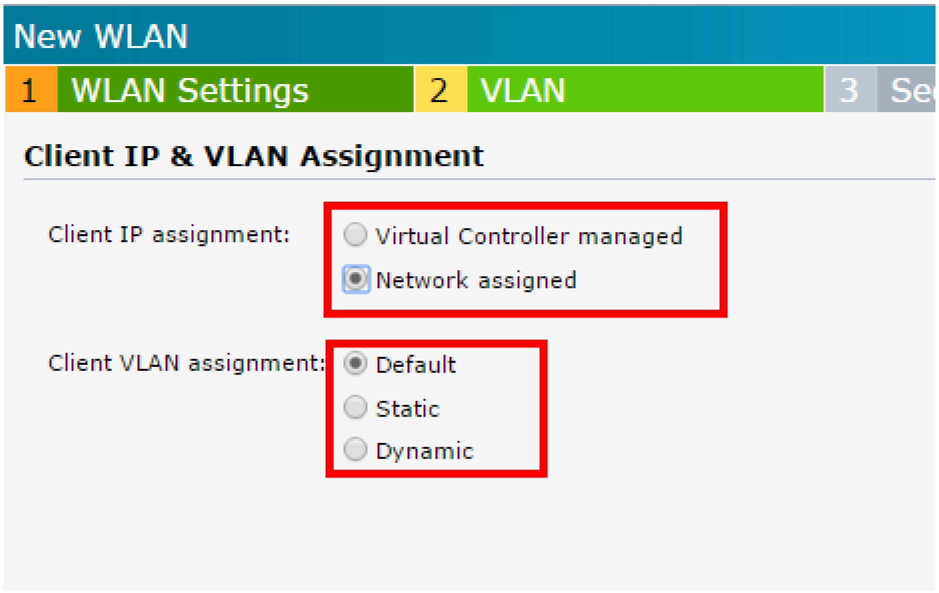
Name & Usage

Name: Aruba-Onboard

Primary usage:
○ Employee
○ Voice
● Guest

Select Client IP Assignment and Client VLAN assignment to match your network requirements. We are going to use Network assigned and the default VLAN.

Click Next.

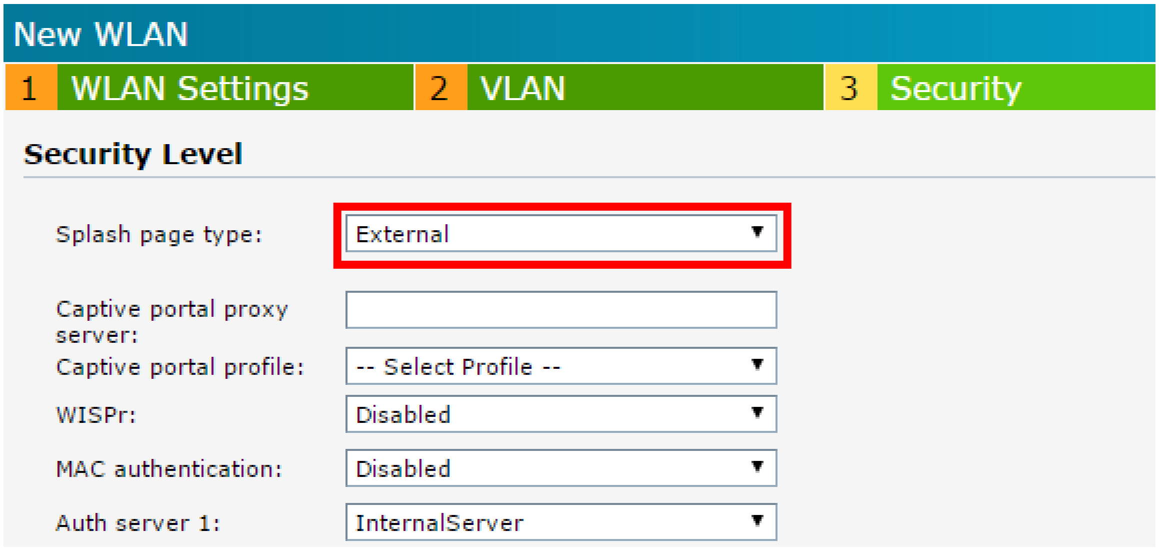


Client IP & VLAN Assignment

Client IP assignment:
○ Virtual Controller managed
● Network assigned

Client VLAN assignment:
● Default
○ Static
○ Dynamic

Select External from the Splash page type drop down menu.



New WLAN

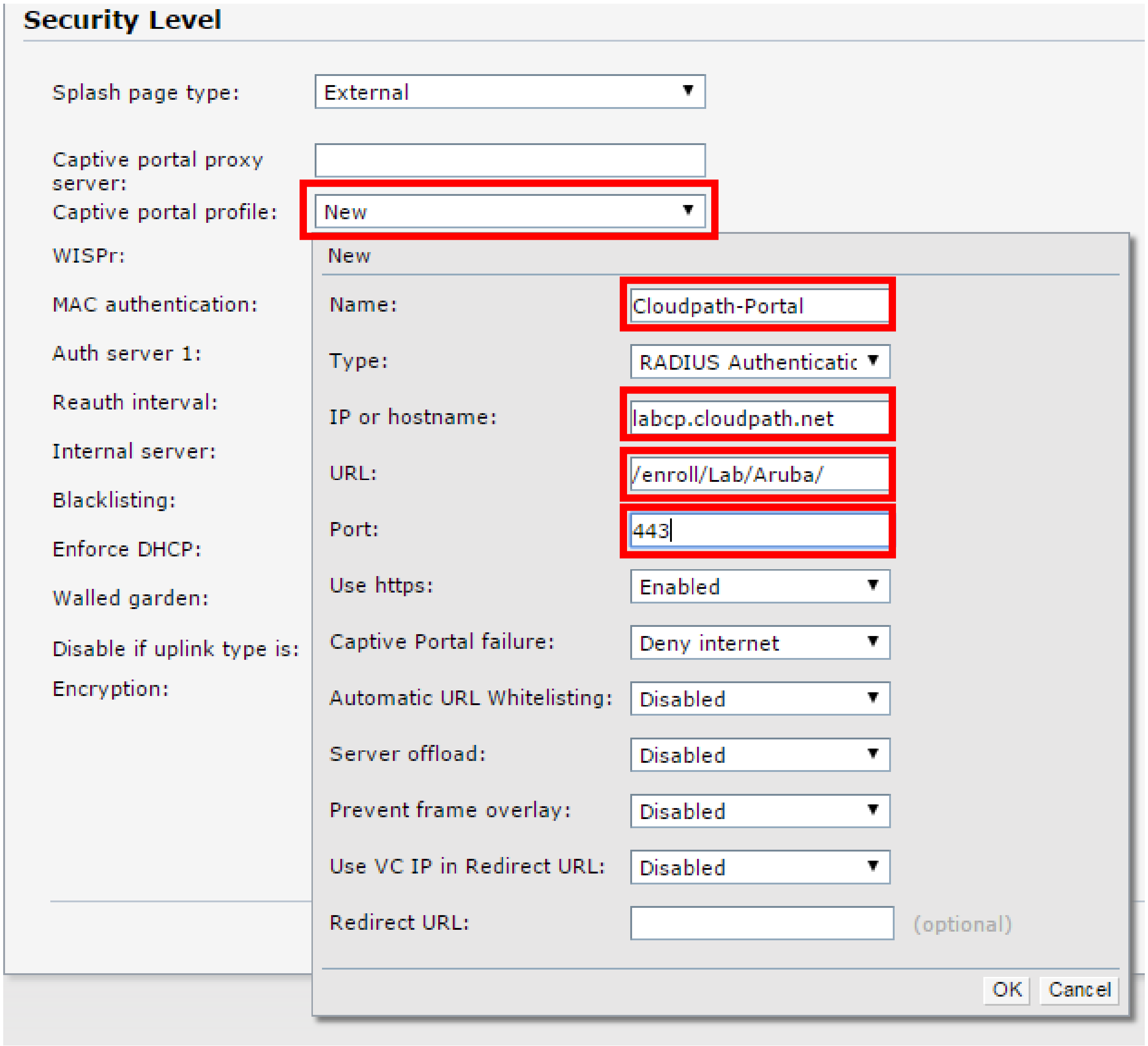
1 WLAN Settings | 2 VLAN | 3 Security

Security Level

Splash page type:	External ▼
Captive portal proxy server:	
Captive portal profile:	-- Select Profile -- ▼
WISPr:	Disabled ▼
MAC authentication:	Disabled ▼
Auth server 1:	InternalServer ▼

Select New from the Captive portal profile drop down menu. Complete the boxes highlighted in the New Profile Box. Click OK

***Note:** The Hostname or IP is of the Cloudpath Server and the URL is from the Cloudpath Workflow Enrollment Portal URL.*



Security Level

Splash page type: External

Captive portal proxy server:

Captive portal profile: New

WISPr:

MAC authentication:

Auth server 1:

Reauth interval:

Internal server:

Blacklisting:

Enforce DHCP:

Walled garden:

Disable if uplink type is:

Encryption:

New

Name: Cloudpath-Portal

Type: RADIUS Authenticatic

IP or hostname: labcp.cloudpath.net

URL: /enroll/Lab/Aruba/

Port: 443

Use https: Enabled

Captive Portal failure: Deny internet

Automatic URL Whitelisting: Disabled

Server offload: Disabled

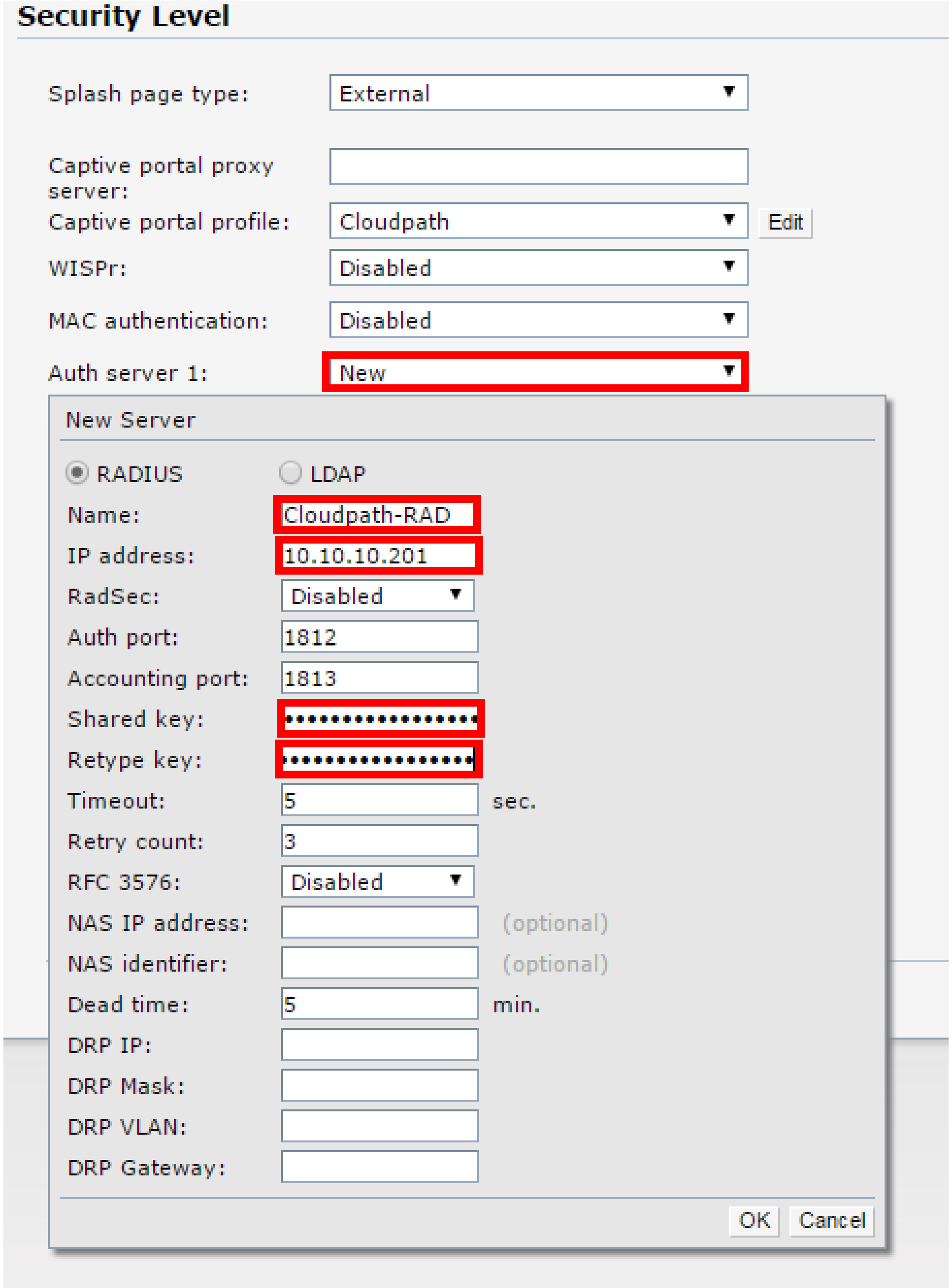
Prevent frame overlay: Disabled

Use VC IP in Redirect URL: Disabled

Redirect URL: (optional)

Select New from the Auth server 1 drop down menu. Complete the boxes highlighted in the New Profile Box. Click OK.

Note: *The below information can be found in Cloudpath under Configuration -> Radius Server*



Security Level

Splash page type: External

Captive portal proxy server:

Captive portal profile: Cloudpath

WISPr: Disabled

MAC authentication: Disabled

Auth server 1: New

New Server

● RADIUS ○ LDAP

Name: Cloudpath-RAD

IP address: 10.10.10.201

RadSec: Disabled

Auth port: 1812

Accounting port: 1813

Shared key: •••••••••••••••••

Retype key: •••••••••••••••••

Timeout: 5 sec.

Retry count: 3

RFC 3576: Disabled

NAS IP address: (optional)

NAS identifier: (optional)

Dead time: 5 min.

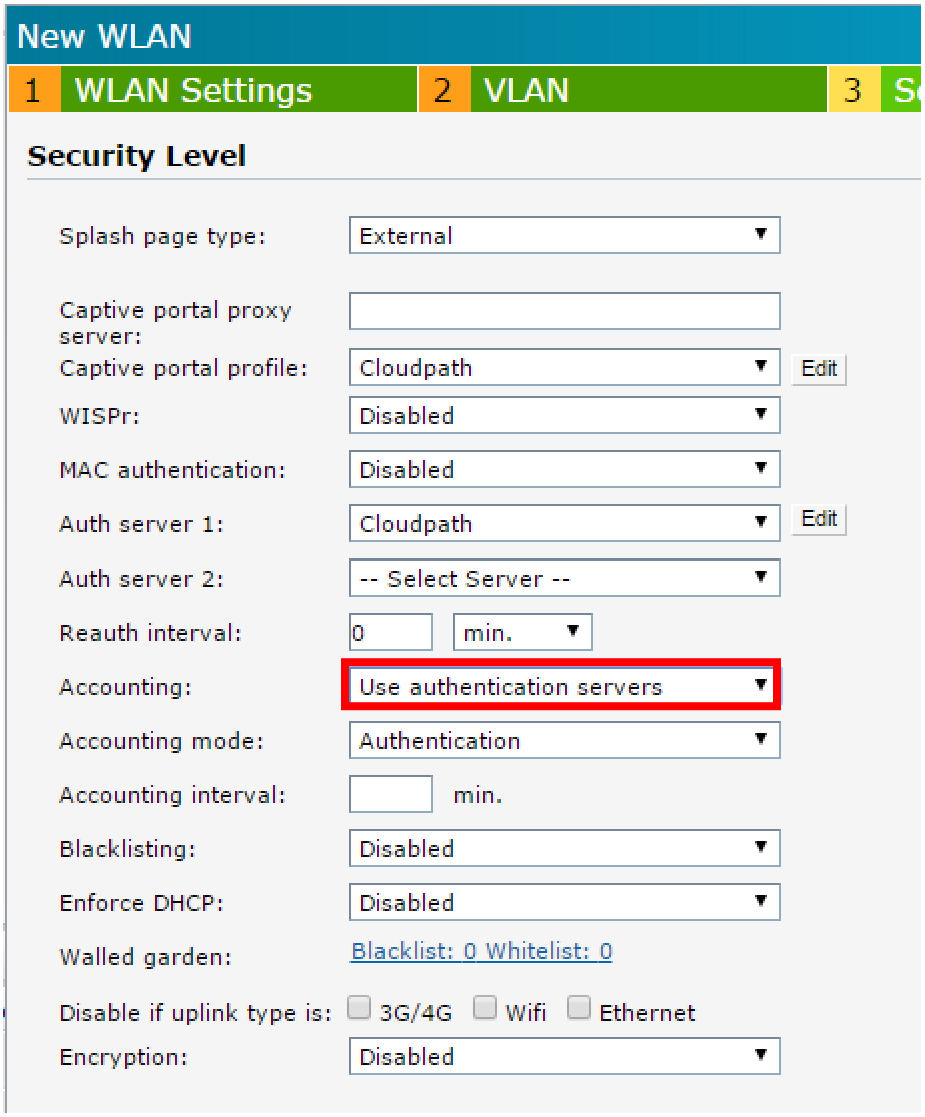
DRP IP:

DRP Mask:

DRP VLAN:

DRP Gateway:

Select Use authentication servers under the Accounting drop-down menu. Leave the rest at the default values and select Next.

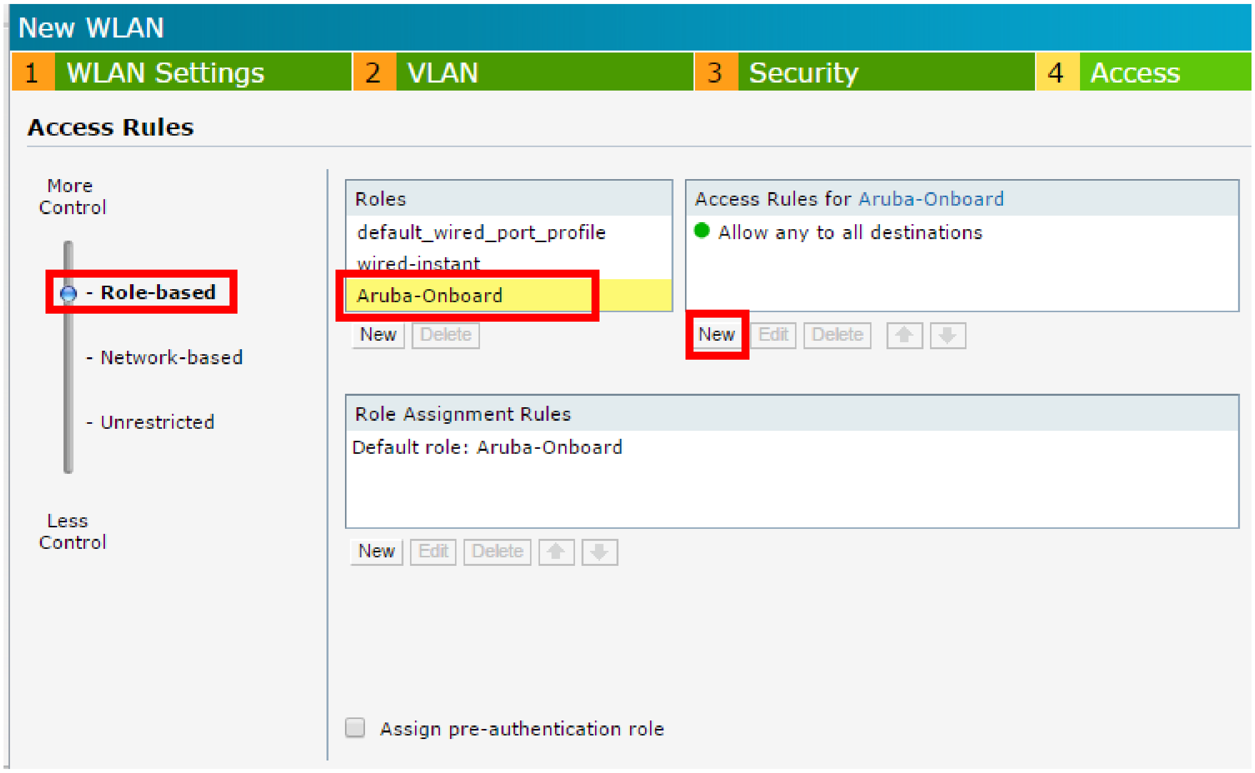


New WLAN

Security Level

Splash page type:	External
Captive portal proxy server:	
Captive portal profile:	Cloudpath Edit
WISPr:	Disabled
MAC authentication:	Disabled
Auth server 1:	Cloudpath Edit
Auth server 2:	-- Select Server --
Reauth interval:	0 min.
Accounting:	Use authentication servers
Accounting mode:	Authentication
Accounting interval:	min.
Blacklisting:	Disabled
Enforce DHCP:	Disabled
Walled garden:	Blacklist: 0 Whitelist: 0
Disable if uplink type is:	□ 3G/4G □ Wifi □ Ethernet
Encryption:	Disabled

On the Access Rules Screen, select Role-based on the slider and under Roles Select the Onboarding SSID name you are creating. Under Access Rules, select New.



New WLAN

1 WLAN Settings | 2 VLAN | 3 Security | 4 Access

Access Rules

More Control

- Role-based
- Network-based
- Unrestricted

Less Control

Roles

default_wired_port_profile

wired-instant

Aruba-Onboard

Access Rules for Aruba-Onboard

● Allow any to all destinations

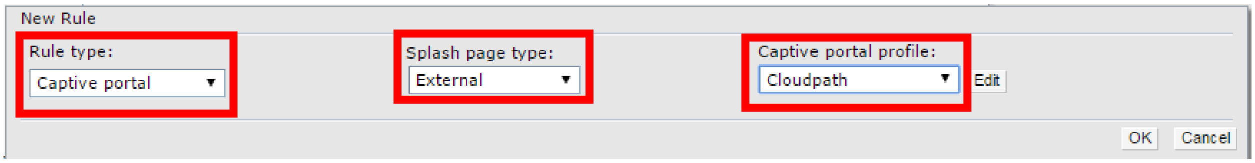
Role Assignment Rules

Default role: Aruba-Onboard

□ Assign pre-authentication role

On the New Access Rule Box, create the following rules:

Captive Portal – External – Portal Profile you created



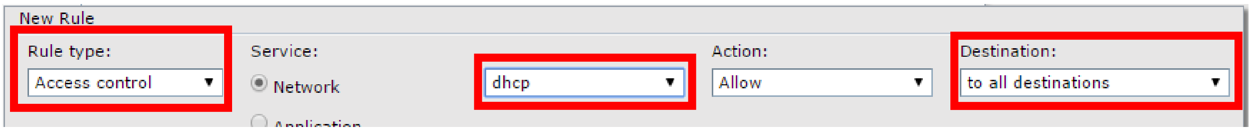
New Rule

Rule type: Captive portal

Splash page type: External

Captive portal profile: Cloudpath

Access control – Network – dhcp – Allow – to all destinations



New Rule

Rule type: Access control

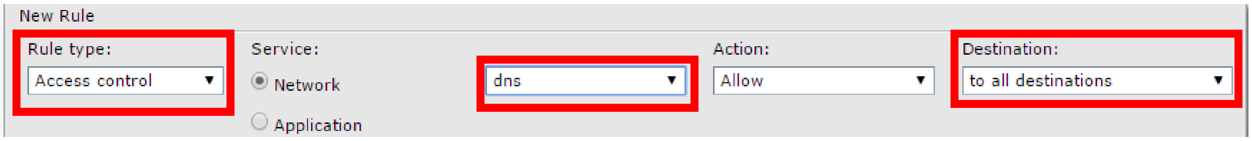
Service: ● Network ○ Application

dhcp

Action: Allow

Destination: to all destinations

Access control – Network – dns – Allow – to all destinations



New Rule

Rule type: Access control

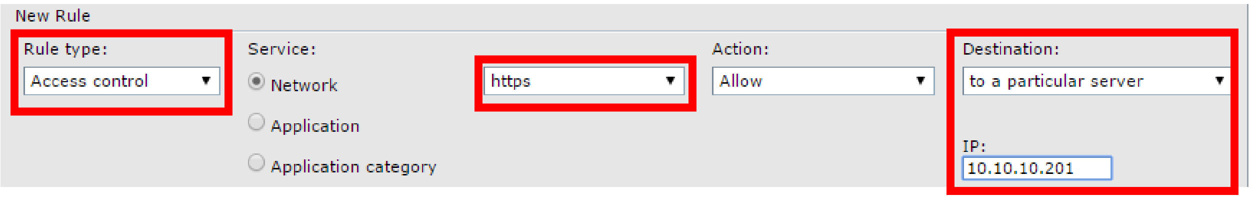
Service: ● Network ○ Application

dns

Action: Allow

Destination: to all destinations

Access control – Network – https – Allow – to a particular destination - Cloudpath Server IP



New Rule

Rule type: Access control

Service: ● Network ○ Application ○ Application category

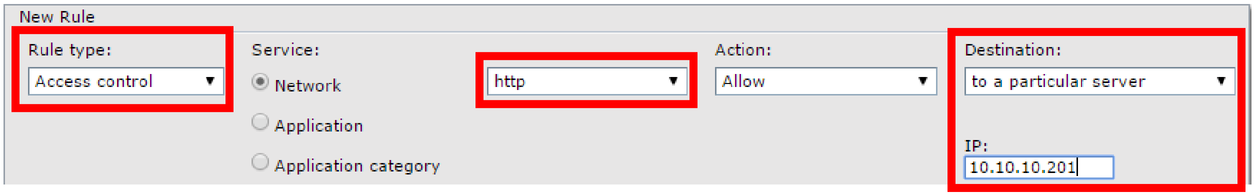
https

Action: Allow

Destination: to a particular server

IP: 10.10.10.201

Access control – Network – http – Allow – to a particular destination - Cloudpath Server IP



New Rule

Rule type: Access control

Service: ● Network ○ Application ○ Application category

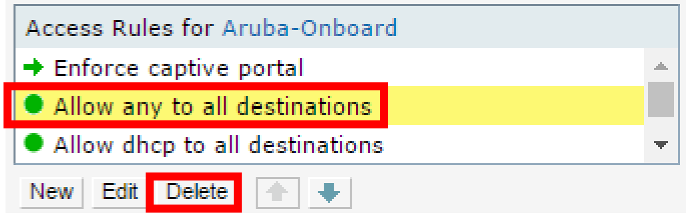
http

Action: Allow

Destination: to a particular server

IP: 10.10.10.201

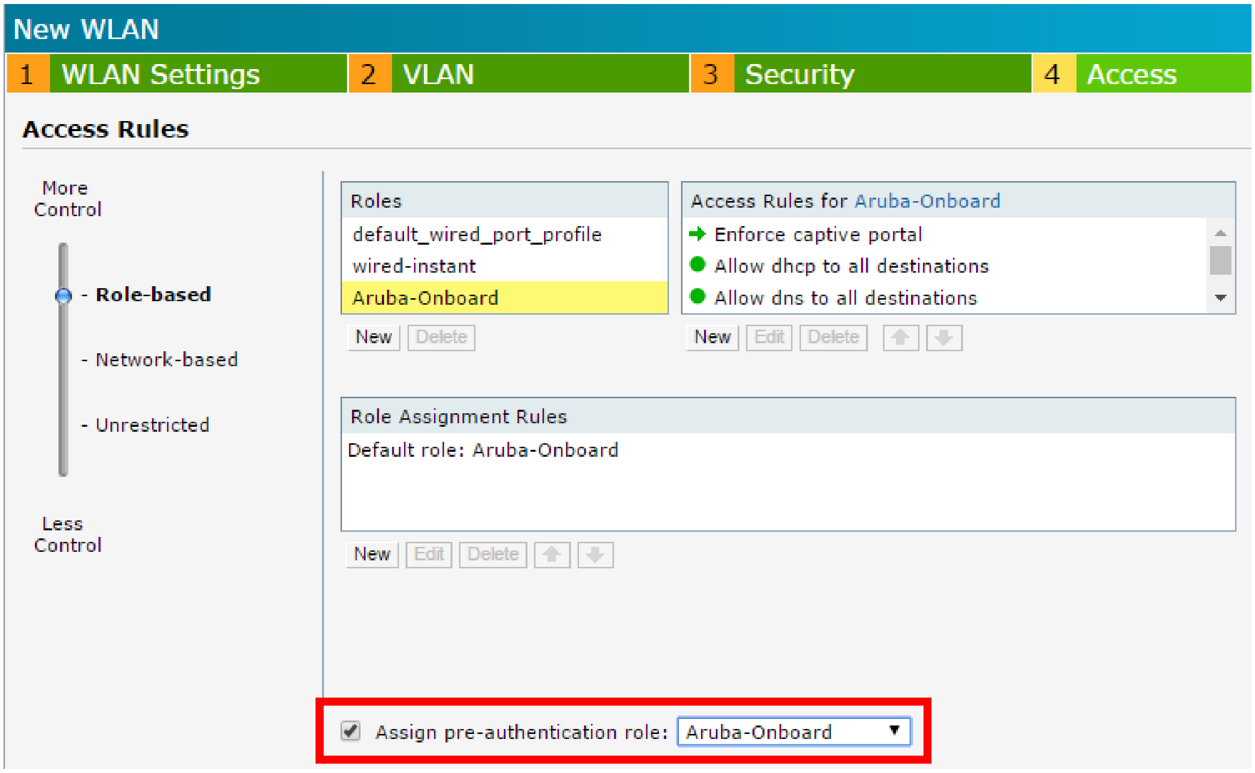
Delete the rule for Allow any to all destinations:



Access Rules for Aruba-Onboard

- Enforce captive portal
- Allow any to all destinations
- Allow dhcp to all destinations

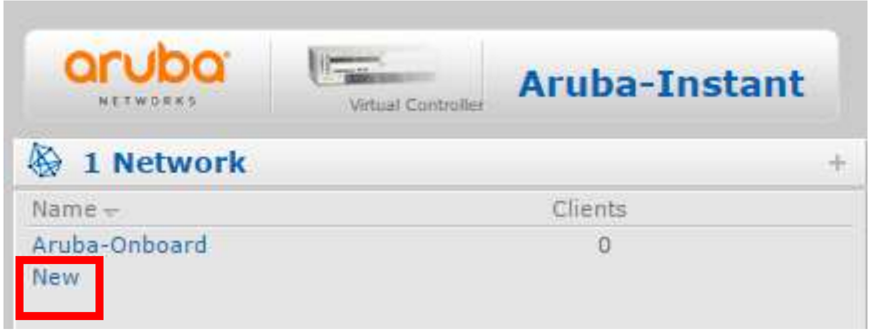
Select Assign pre-authentication role checkbox and choose the Onboarding SSID you are creating from the drop-down menu. Select Finish.



☑ Assign pre-authentication role: Aruba-Onboard

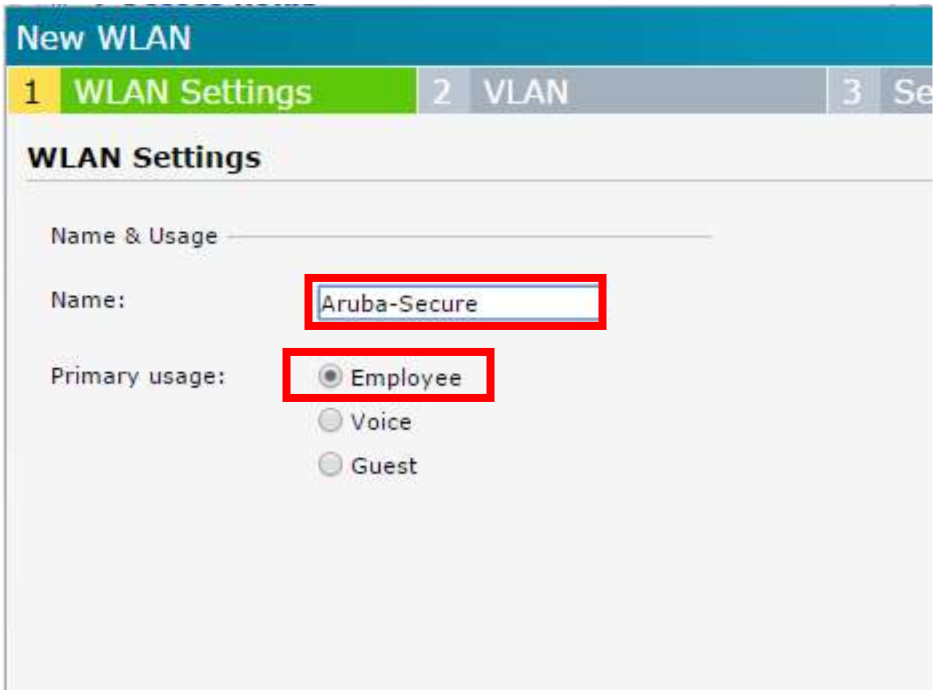
Create the Onboarding SSID

Select New under Networks.



In the New WLAN Box, Name the SSID and select Employee for the Primary usage.

Click Next.



WLAN Settings

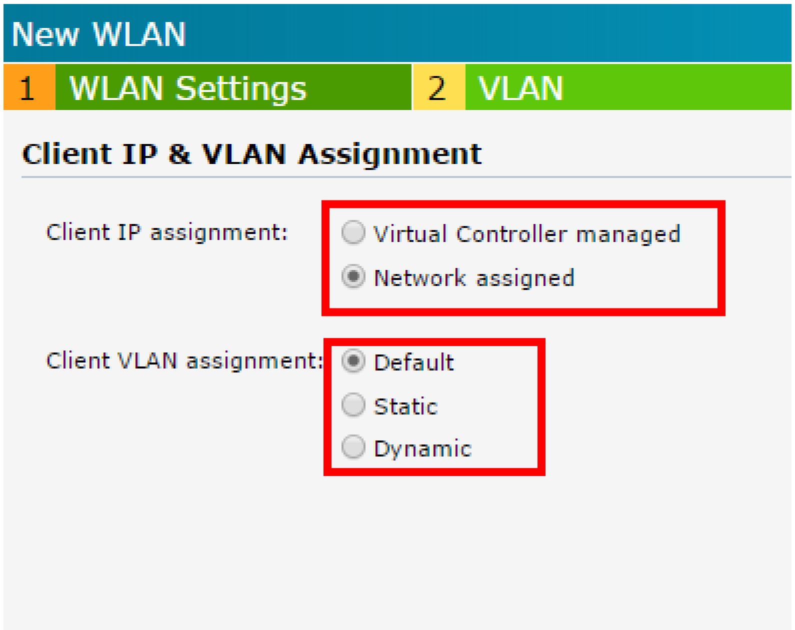
Name & Usage

Name: Aruba-Secure

Primary usage:
● Employee
○ Voice
○ Guest

Select Client IP Assignment and Client VLAN assignment to match your network requirements. We are going to use Network assigned and the default VLAN.

Click Next.



Client IP & VLAN Assignment

Client IP assignment:
○ Virtual Controller managed
● Network assigned

Client VLAN assignment:
● Default
○ Static
○ Dynamic

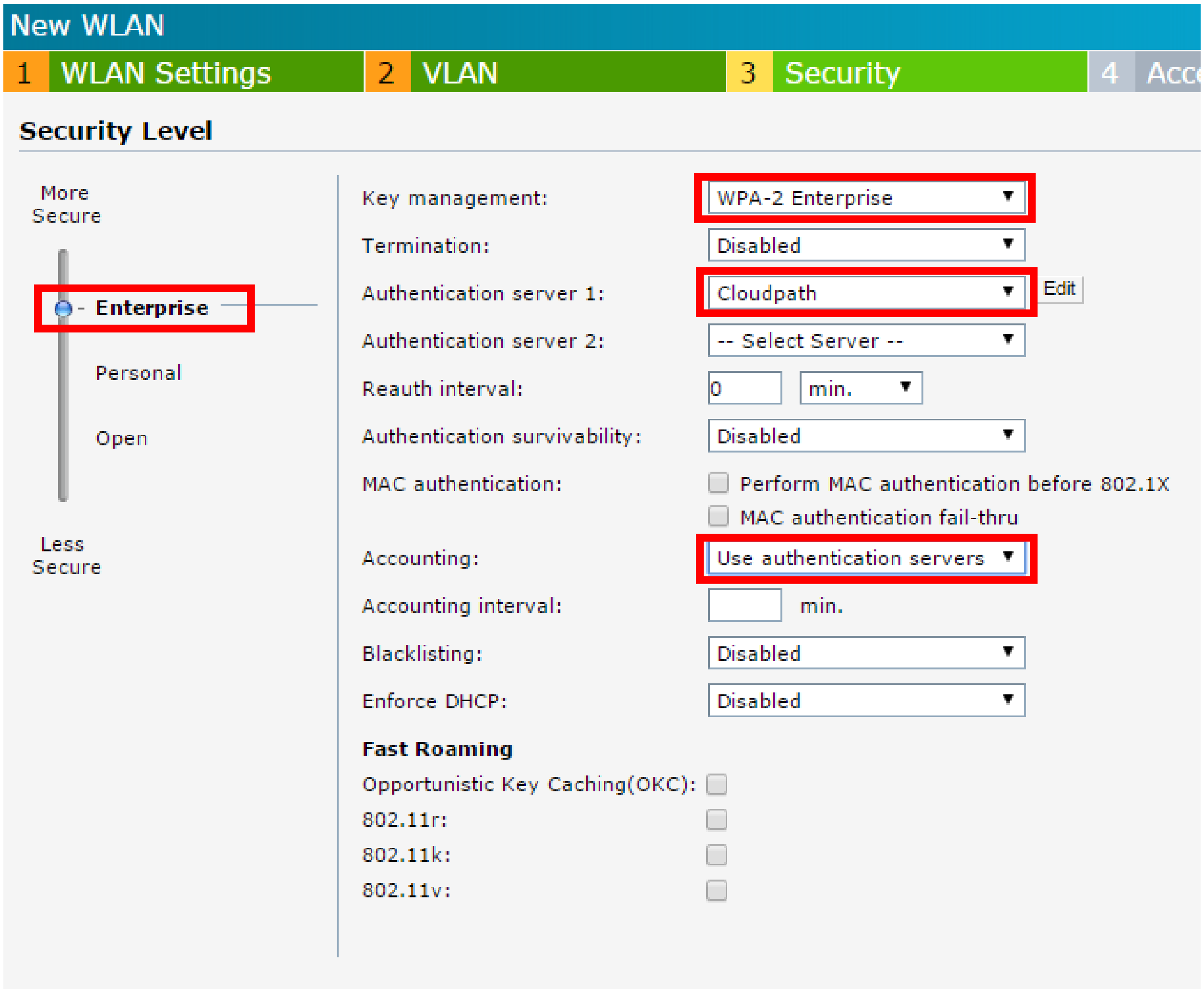
Select Enterprise on the Security Level slider.

Select WPA-2 Enterprise from the Key Management drop-down menu.

Select the Authentication Server you created earlier under Authentication server 1.

Select Use authentication servers under Accounting.

Note: *These settings can be changed to fit your network requirements.*



New WLAN

1 WLAN Settings | 2 VLAN | 3 Security | 4 Acc

Security Level

More Secure

- Enterprise

Personal

Open

Less Secure

Key management: WPA-2 Enterprise

Termination: Disabled

Authentication server 1: Cloudpath Edit

Authentication server 2: -- Select Server --

Reauth interval: 0 min.

Authentication survivability: Disabled

MAC authentication: ☐ Perform MAC authentication before 802.1X

☐ MAC authentication fail-thru

Accounting: Use authentication servers

Accounting interval: min.

Blacklisting: Disabled

Enforce DHCP: Disabled

Fast Roaming

Opportunistic Key Caching(OKC): ☐

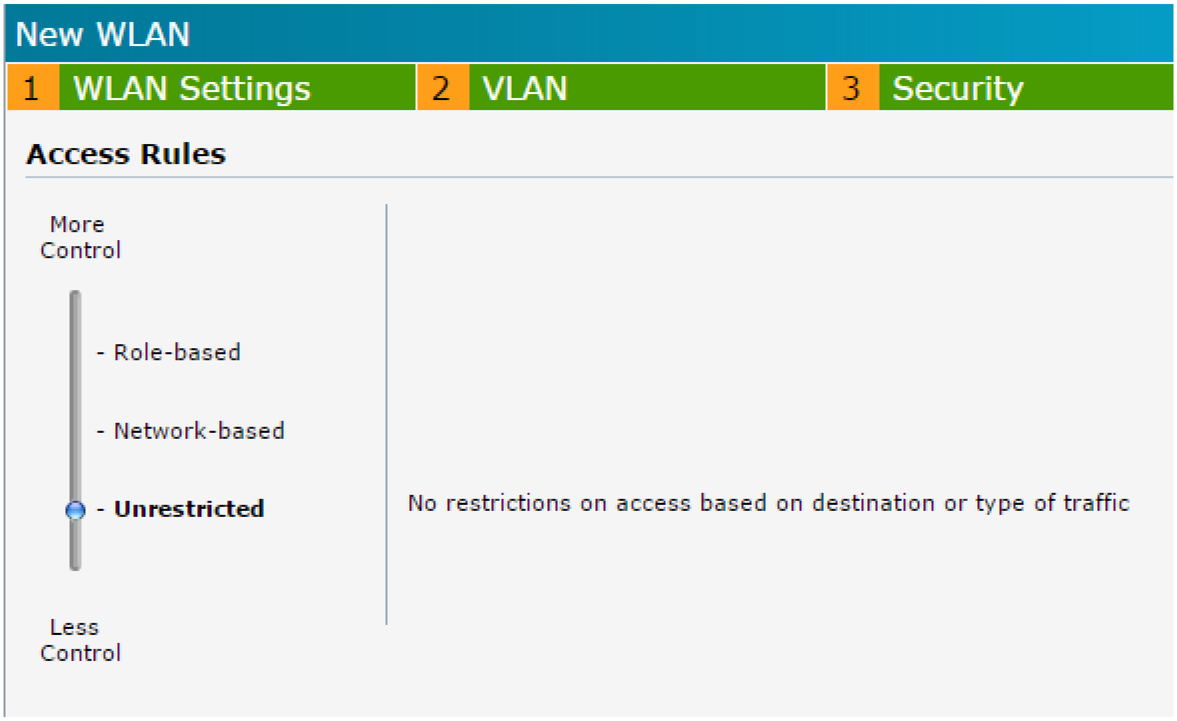
802.11r: ☐

802.11k: ☐

802.11v: ☐

Leave the defaults and click Finish.

Note: *These settings can be changed to fit your network requirements.*



New WLAN

1 WLAN Settings | 2 VLAN | 3 Security

Access Rules

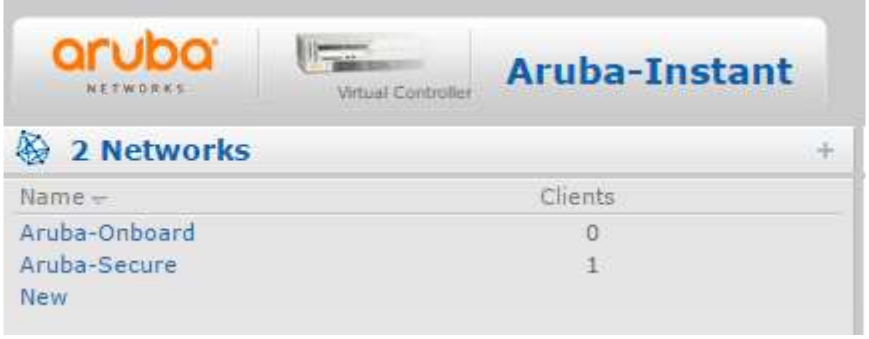
More Control

- Role-based
- Network-based
- **Unrestricted**

Less Control

No restrictions on access based on destination or type of traffic

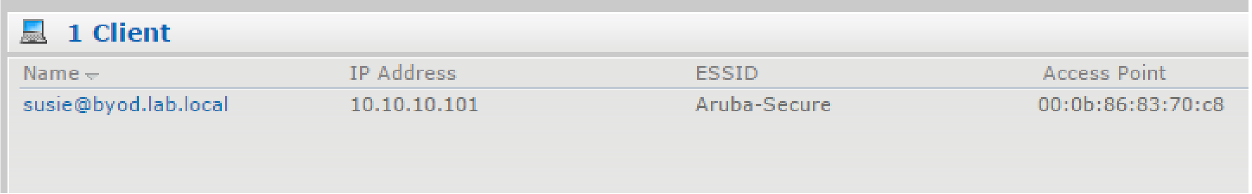
Now you are ready to Onboard clients.



Aruba-Instant

2 Networks

Name	Clients
Aruba-Onboard	0
Aruba-Secure	1
New	



1 Client

Name	IP Address	ESSID	Access Point
susie@byod.lab.local	10.10.10.101	Aruba-Secure	00:0b:86:83:70:c8