
Simply Better Connections

Deploy a Cloudpath ES Workflow on a Cisco WLAN Controller

Cloudpath as RADIUS server and as a Hotspot (WISPr) Portal

Best Practices and Deployment Guide

Cloudpath on Cisco WLC

Deploying a Cloudpath workflow on a Cisco WLAN Controller

November 2017

Table of Contents

This table of contents can be used as a checklist in the future.

Cloudpath on Cisco WLC

Deploying a Cloudpath workflow on a Cisco WLAN Controller

November 2017

Intent of this Document

Cloudpath Best Practices and Deloyment Guides are meant to address specific subjects in Ruckus Cloudpath deployments and to tackle those subjects in bite sized chunks. Although Cloudpath is simpler and more user-friendly than competitors, there are many options within Cloudpath and network administrators will benefit from a series of targeted Best Practices and Deployment Guides.

What is Ruckus Cloudpath? Cloudpath is a self-service onboarding portal for secure networks. We are all familiar with captive portals for public access/hotspot networks. Unlike those systems, Cloudpath can support self-service secure registration for networks, combining everything necessary for:

- *Policy Management* - Is the user a student or a teacher? Is the device a phone or a laptop?
- *Device Enablement* - Is the anti-virus up-to-date? Is the firewall running and the OS patched?
- *Certificate Deployment and Management* – Certificates are deployed automatically, uniquely identifying all devices

IT gets more control and more information, while spending less time on password problems and basic access issues.

This document walks through the deployment of a Cloudpath workflow (or registration portal), on a Cisco WLAN Conroller (WLC) It supports the typical case of two WLANs (SSIDs) – one for the onboarding portal, one for secure users. The secure SSID is 802.1X certificate secured for users and is accessible only after they have registered their devices at the onboarding portal. The open SSID can serve double duty as both the secure user onboarding portal, and also as the guest WLAN with automatic MAC registration of guest devices. Configuration of both options is described below.

This document is not a Cloudpath installation guide or a complete Cisco WLC configuration guide

Cloudpath ES server should already be fully deployed and accessible, locally or as a cloud system. An external database of users should be available.* A workflow should already be configured on Cloudpath ES. If necessary, consult the Cloudpath Best Practices and Deployment Guide "Basic Cloudpath Workflow - secure users and MAC auth guests".

Similarly, a Cisco WLC should already be deployed, with at least one AP connected to it. To test, Wi-Fi client devices such as tablets, smart phones, or laptops will be needed.

*There is a limited onboard database in Cloudpath that can be used in a lab environment, but it is not recommended for a production environment

Cloudpath on Cisco WLC

Deploying a Cloudpath workflow on a Cisco WLAN Controller

November 2017

Cloudpath Workflow Overview

A workflow is a tree of network access policy/classification steps contained in a series of web pages. A policy is built in a series of steps, and then published as an Onboarding Portal (web pages) on the Cloudpath web server. Adding a step usually involves adding a web page, but it could be a filter or other classification step that automatically flows through to the next step/page. A workflow generally ends in downloading a *Device Configuration* onto a secure client. A Cloudpath *Device Configuration* is typically a WLAN/SSID profile, including security settings and an 802.1X certificate. However, it may end in some alternative grant of network access, such as a PSK, a Ruckus Dynamic PSK, or display of a voucher code for a guest user.

Hotspot Portal SSID and RADIUS Secured SSID

This document describes deployment of a Cloudpath workflow for an environment with two WLANs/SSIDs. The first WLAN is a secure/employee SSID that uses 802.1X certificate authentication (supported by the Cloudpath RADIUS server). Take special note – the Cloudpath ES RADIUS server authenticates the certificates for access to the secure network. At registration, there will need to be an authentication server (database) of employees (secure users) that Cloudpath can check before distributing profiles and certificates.

The second SSID is an open WLAN redirected as a Hotspot/WISPr portal. It serves both as employee registration and as a Guest Access portal. Secure users (employees) initially register their devices and download a certificate on the open SSID. It is a one-time process for each employee device, and once a device is registered and has a unique certificate, it immediately, and always thereafter, connects to the secure network.

Guest users can connect to the open SSID, choose to register as a guest, and their device will be uniquely registered by its MAC address. The portal will open up (the walled garden will open) and they will be granted Internet access.

This is designed to be a simple but effective workflow that can be built on, and necessary configuration of Cloudpath is described in the Cloudpath Best Practices and Deployment Guide "Basic Cloudpath Workflow - Secure Users and MAC-auth Guests".

Cloudpath on Cisco WLC

Deploying a Cloudpath workflow on a Cisco WLAN Controller

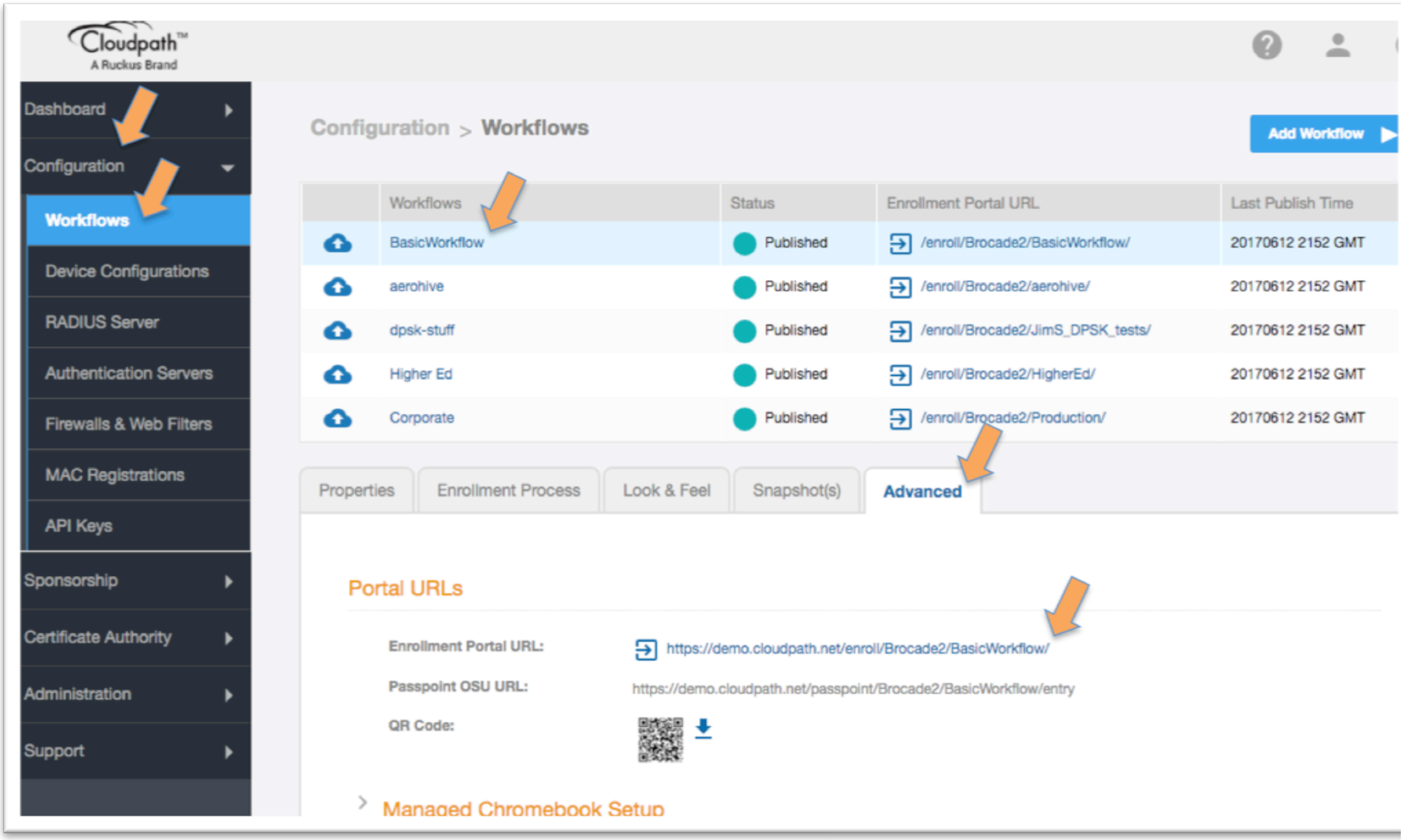
November 2017

Onboarding and Secure WLANs on a Cisco WLAN Controller

1) Get the enrollment URL and the RADIUS shared secret from Cloudpath ES

Configuration of a basic workflow in Cloudpath ES should have already been completed. However, before moving on to a WLAN controller, there are two pieces of information that will be needed:

- The Enrollment Portal URL
- The Cloudpath ES RADIUS settings



Workflows	Status	Enrollment Portal URL	Last Publish Time
BasicWorkflow	Published	/enroll/Brocade2/BasicWorkflow/	20170612 2152 GMT
aerohive	Published	/enroll/Brocade2/aerohive/	20170612 2152 GMT
dpsk-stuff	Published	/enroll/Brocade2/JimS_DPSK_tests/	20170612 2152 GMT
Higher Ed	Published	/enroll/Brocade2/HigherEd/	20170612 2152 GMT
Corporate	Published	/enroll/Brocade2/Production/	20170612 2152 GMT

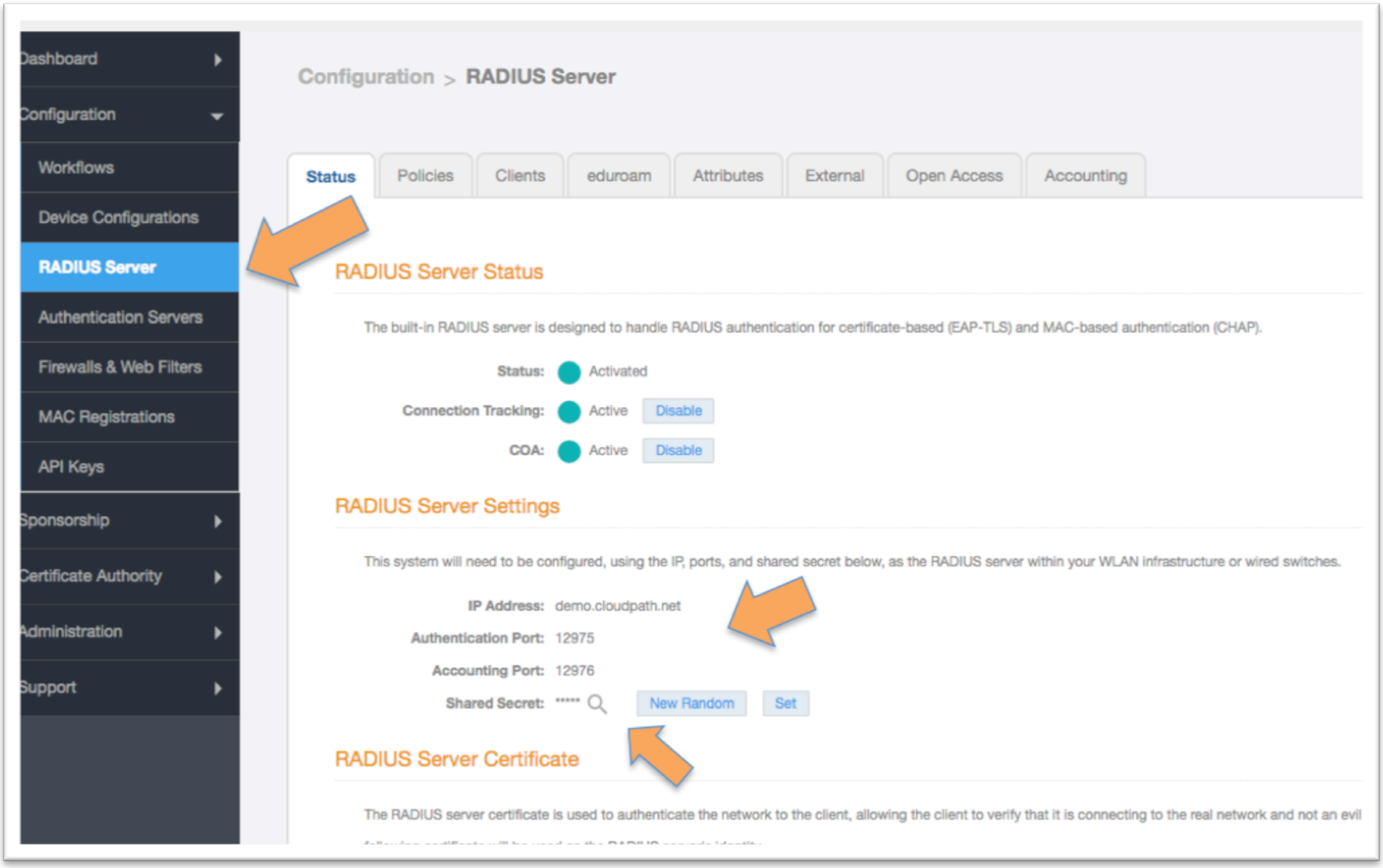
Portal URLs

Enrollment Portal URL: https://demo.cloudpath.net/enroll/Brocade2/BasicWorkflow/

Passpoint OSU URL: https://demo.cloudpath.net/passpoint/Brocade2/BasicWorkflow/entry

QR Code:

- Login to Cloudpath ES and navigate to:
- Configuration
- Workflow
- Click on the workflow to be deployed
- Click on the workflow's **Advanced** tab
- Go to the Enrollment Portal URL.
- Copy this URL to a text editor for later (or be prepare to return to this window).
- This URL will be added to the WLAN in the Cisco WLC as an external portal



RADIUS Server Status

The built-in RADIUS server is designed to handle RADIUS authentication for certificate-based (EAP-TLS) and MAC-based authentication (CHAP).

Status: Activated

Connection Tracking: Active

COA: Active

RADIUS Server Settings

This system will need to be configured, using the IP, ports, and shared secret below, as the RADIUS server within your WLAN infrastructure or wired switches.

IP Address: demo.cloudpath.net

Authentication Port: 12975

Accounting Port: 12976

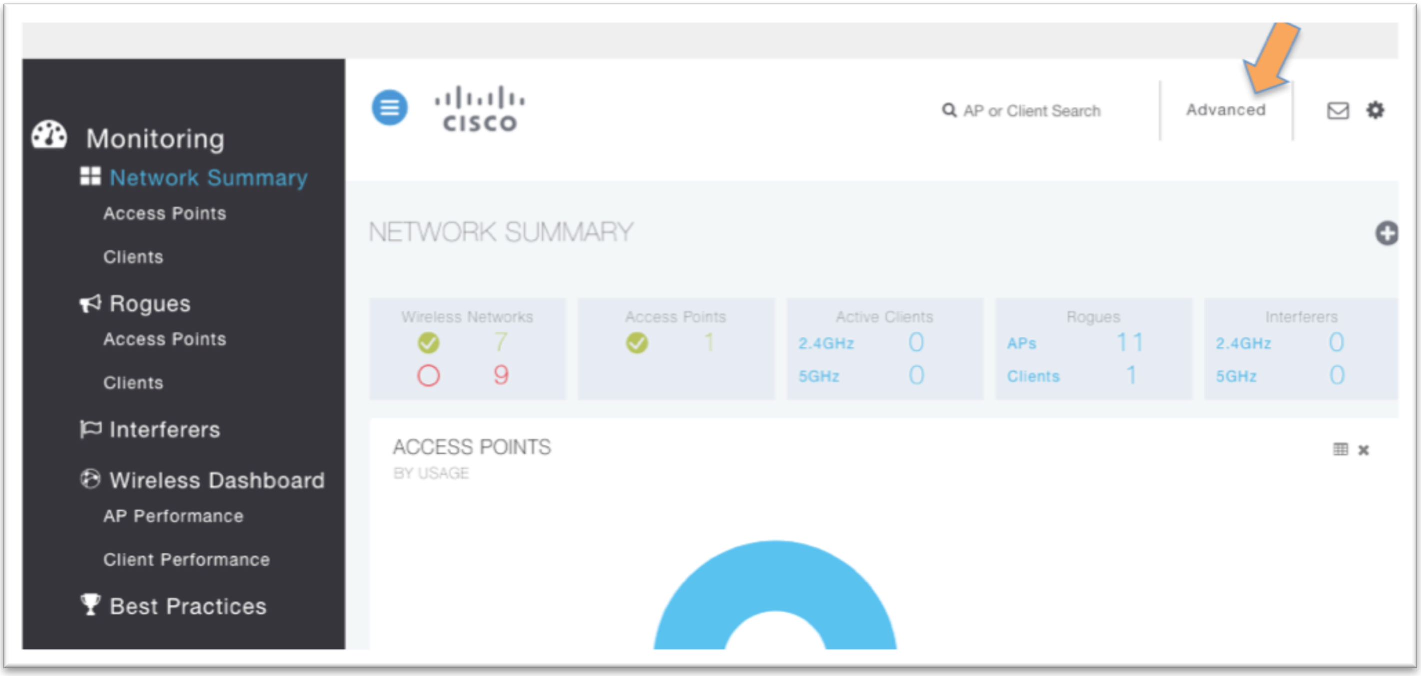
Shared Secret: *****

RADIUS Server Certificate

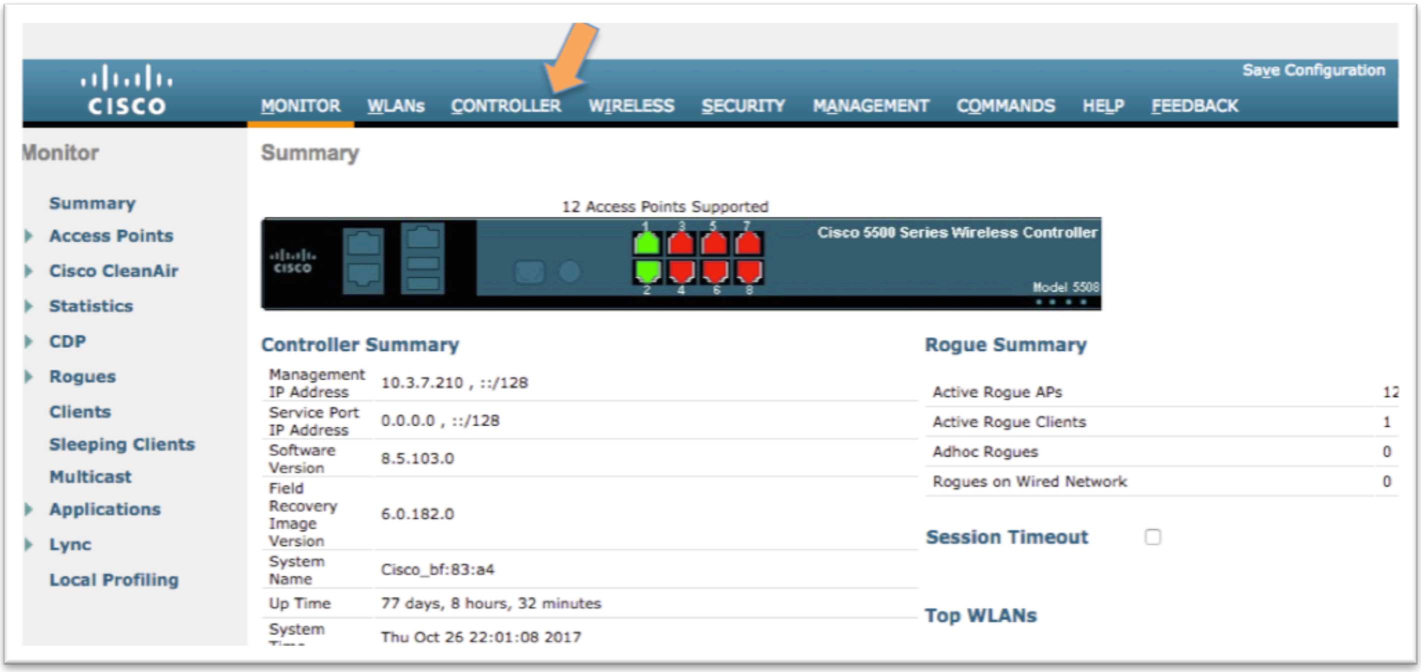
The RADIUS server certificate is used to authenticate the network to the client, allowing the client to verify that it is connecting to the real network and not an evil

- WLC will need the RADIUS server settings. On the main menu bar, navigate to **Configuration -> RADIUS Server**. Copy the following information for later
- The IP address
- NB - must be an IP address. If necessary, a CLI ping will determine the IP from the FQDN
- Authentication port
- The Accounting port (optional)
- The Shared Secret - which can be revealed by clicking on the magnifying glass

2) Login to the WLC and add dynamic user interfaces (VLANs)



- Login to the Cisco WLC
- Navigate to **Advanced**
- Click on **Controller** to access the *Controller menu*



Controller Summary

Management IP Address	10.3.7.210 , ::/128
Service Port IP Address	0.0.0.0 , ::/128
Software Version	8.5.103.0
Field Recovery Image Version	6.0.182.0
System Name	Cisco_bf:83:a4
Up Time	77 days, 8 hours, 32 minutes
System Time	Thu Oct 26 22:01:08 2017

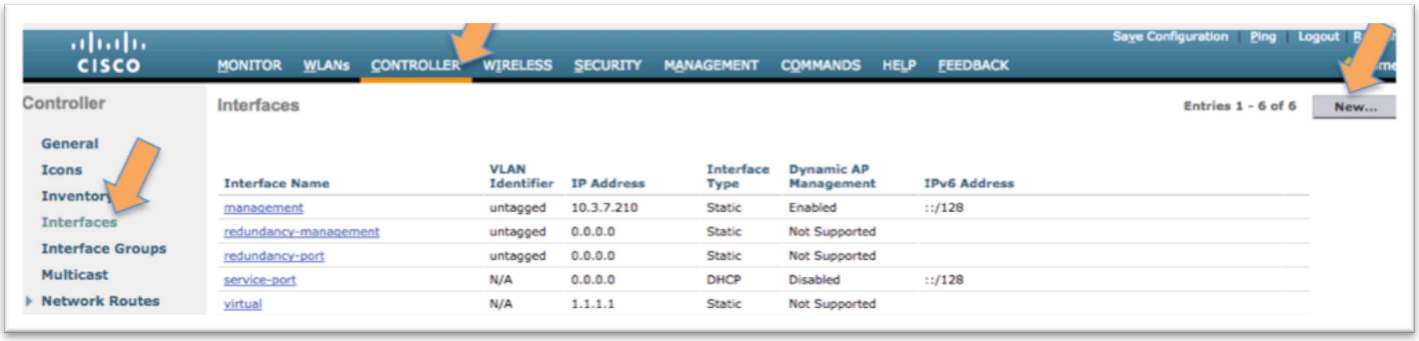
Rogue Summary

Active Rogue APs	12
Active Rogue Clients	1
Adhoc Rogues	0
Rogues on Wired Network	0

Session Timeout □

Top WLANs

Best practices would suggest that authenticated user and guest traffic should be isolated from each other by VLAN. Create VLANS as **Dynamic Interfaces** as appropriate for the network under configuration.

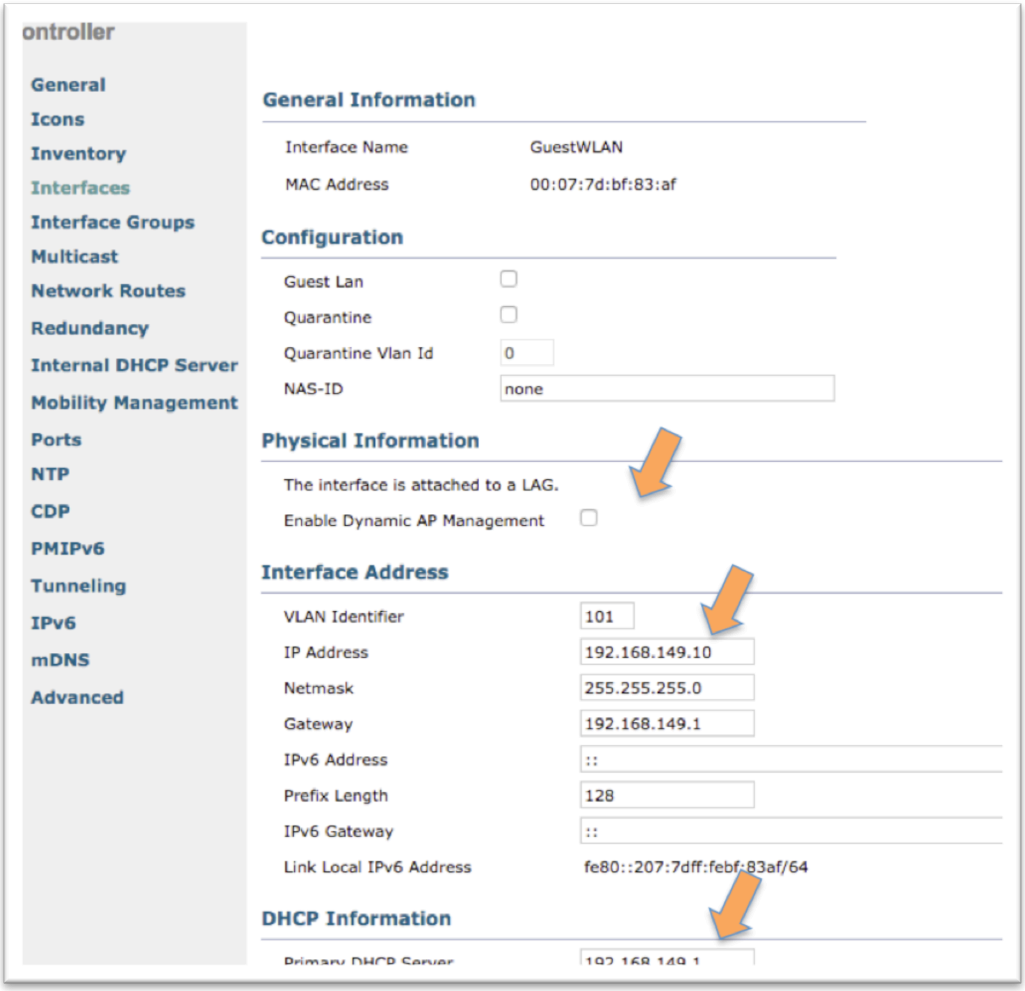


Interfaces

Entries 1 - 6 of 6

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
management	untagged	10.3.7.210	Static	Enabled	::/128
redundancy-management	untagged	0.0.0.0	Static	Not Supported	
redundancy-port	untagged	0.0.0.0	Static	Not Supported	
service-port	N/A	0.0.0.0	DHCP	Disabled	::/128
virtual	N/A	1.1.1.1	Static	Not Supported	

- On the *Controller Menu*, click on **Interfaces** and then on **New**
- Define the interface/VLAN as appropriate for the network
- Repeat, if necessary, for the authenticated users WLAN



General Information

Interface Name	GuestWLAN
MAC Address	00:07:7d:bf:83:af

Configuration

Guest Lan	□
Quarantine	□
Quarantine Vlan Id	0
NAS-ID	none

Physical Information

The interface is attached to a LAG.

Enable Dynamic AP Management	□

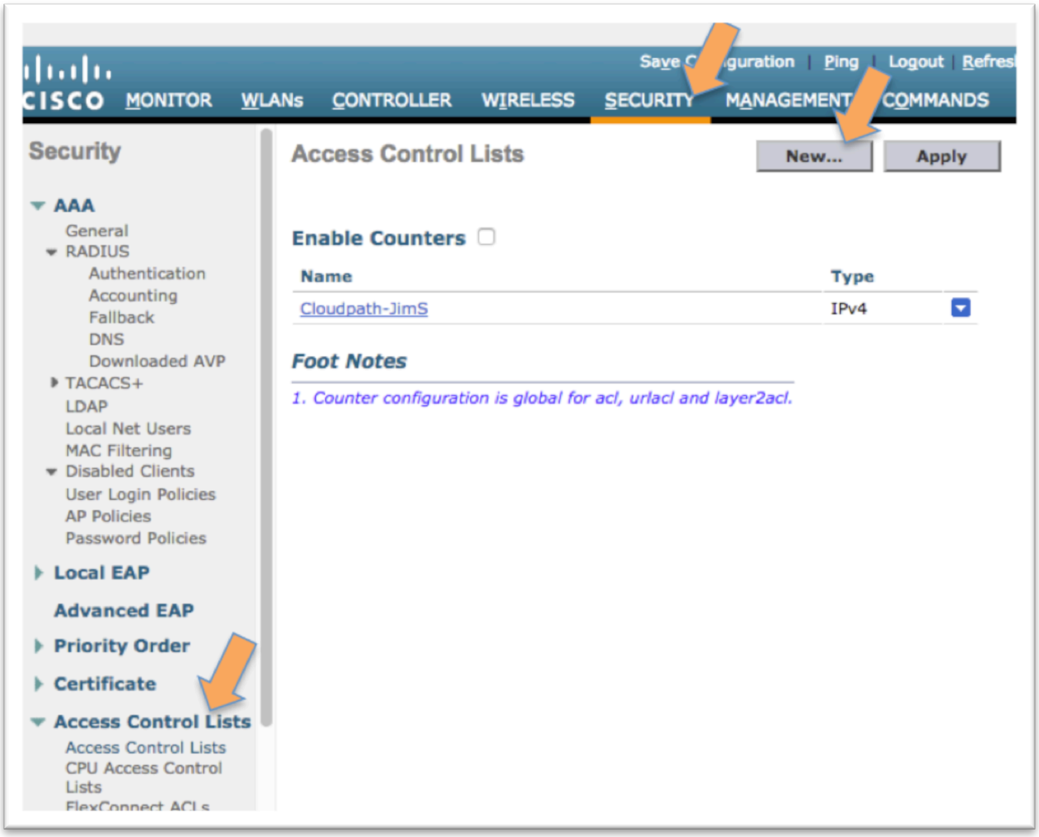
Interface Address

VLAN Identifier	101
IP Address	192.168.149.10
Netmask	255.255.255.0
Gateway	192.168.149.1
IPv6 Address	::
Prefix Length	128
IPv6 Gateway	::
Link Local IPv6 Address	fe80::207:7dff:febf:83af/64

DHCP Information

Primary DHCP Server	192.168.149.1

3) Create a preauthentication Access Control List (ACL) for the onboarding WLAN



Access Control Lists

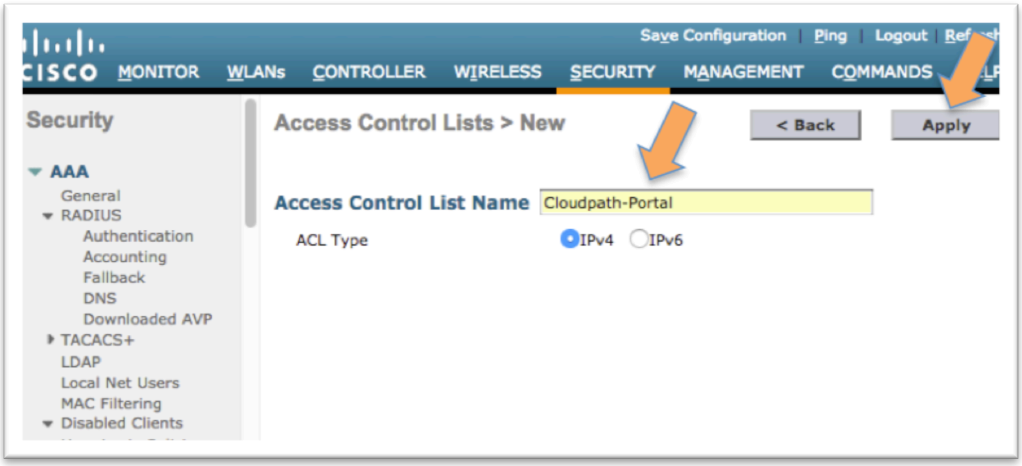
Enable Counters □

Name	Type
Cloudpath-JimS	IPv4

Foot Notes

1. Counter configuration is global for acl, urlacl and layer2acl.

- Click on **Security** to access the *Security menu*
    - Expand **Aceess Control Lists** and then click on **Access Control Lists** (yes, it appears twice)
    - Click **New** (alternatively, click on an existing ACL that you will modify)

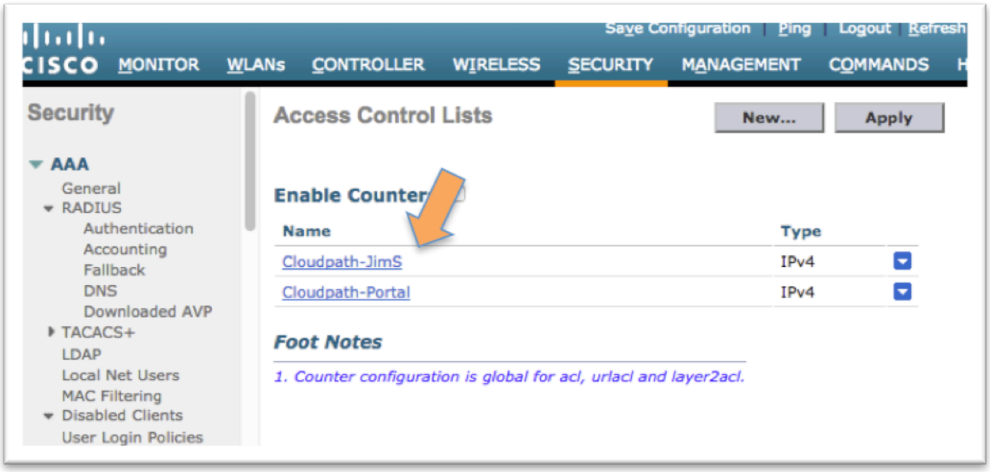


Access Control Lists > New

Access Control List Name: Cloudpath-Portal

ACL Type ● IPv4 ○ IPv6

- Name the ACL and click **Apply**



Access Control Lists

Enable Counters □

Name	Type
Cloudpath-JimS	IPv4
Cloudpath-Portal	IPv4

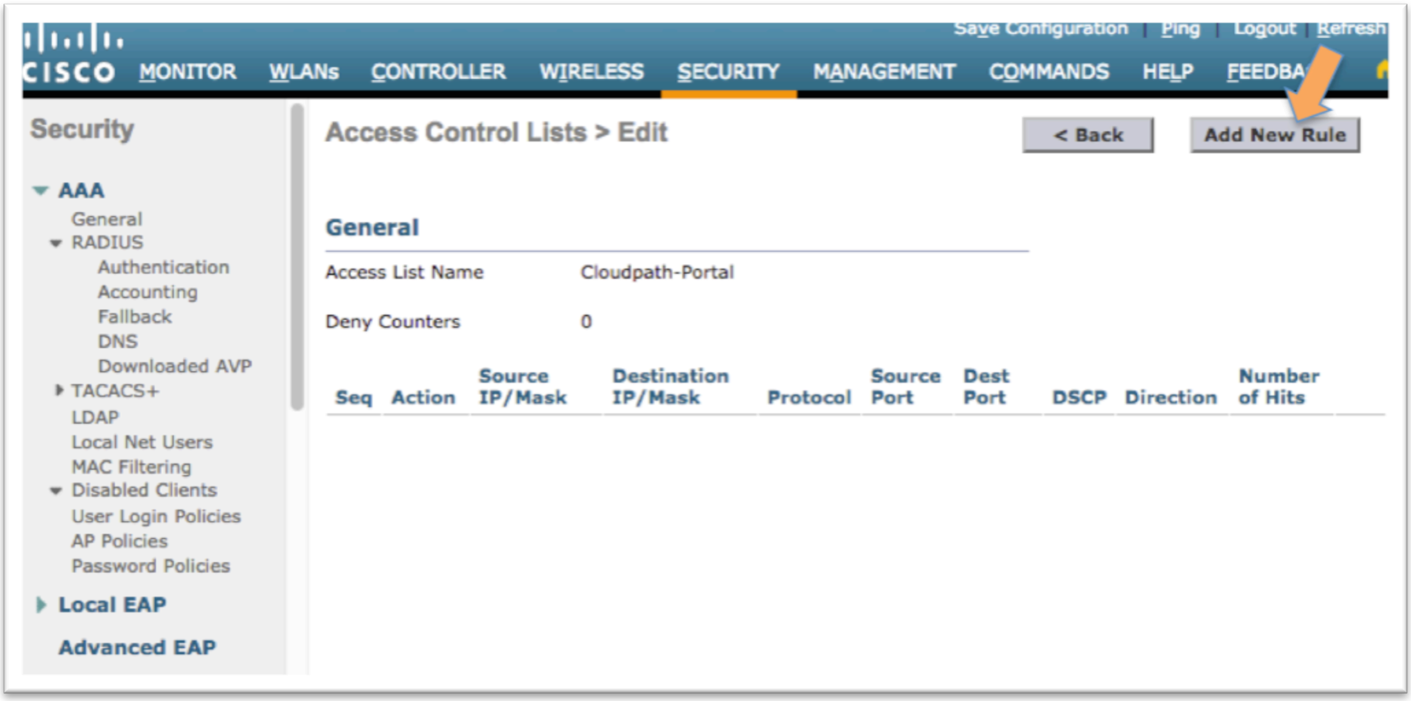
Foot Notes

1. Counter configuration is global for acl, urlacl and layer2acl.

- Now click on the ACL name to edit it

Walled Garden In order for the Onboarding Portal to function, specific network traffic must be allowed before the user is authenticated in order to support the authentication process. The exact entries depend on the local network. The following are generally required

- DHCP server – the client generally needs an IP address
- DNS server
- Gateway (in many case, all three are the same)
- Cloudpath server, including subdomains of the enrollment URL



Access Control Lists > Edit

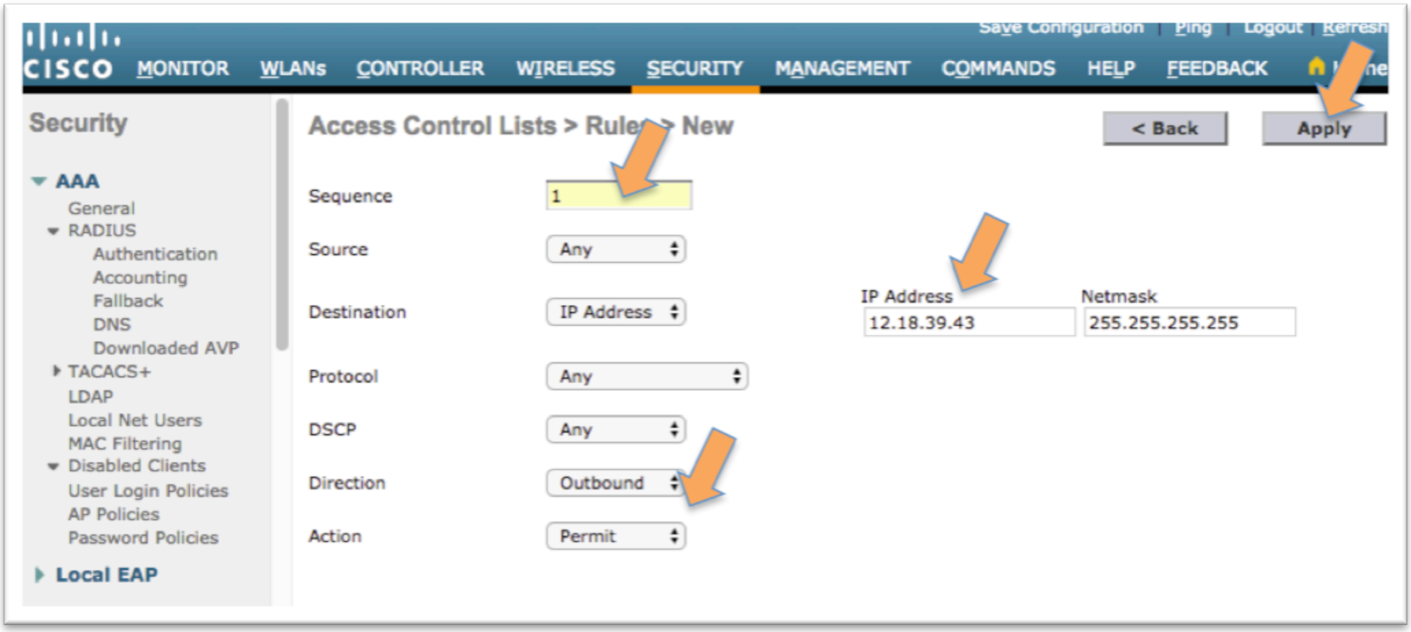
General

Access List Name Cloudpath-Portal

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits

- Use the **Add New Rule** button to add the first rule



Access Control Lists > Rules > New

Sequence 1

Source Any

Destination IP Address — IP Address 12.18.39.43 Netmask 255.255.255.255

Protocol Any

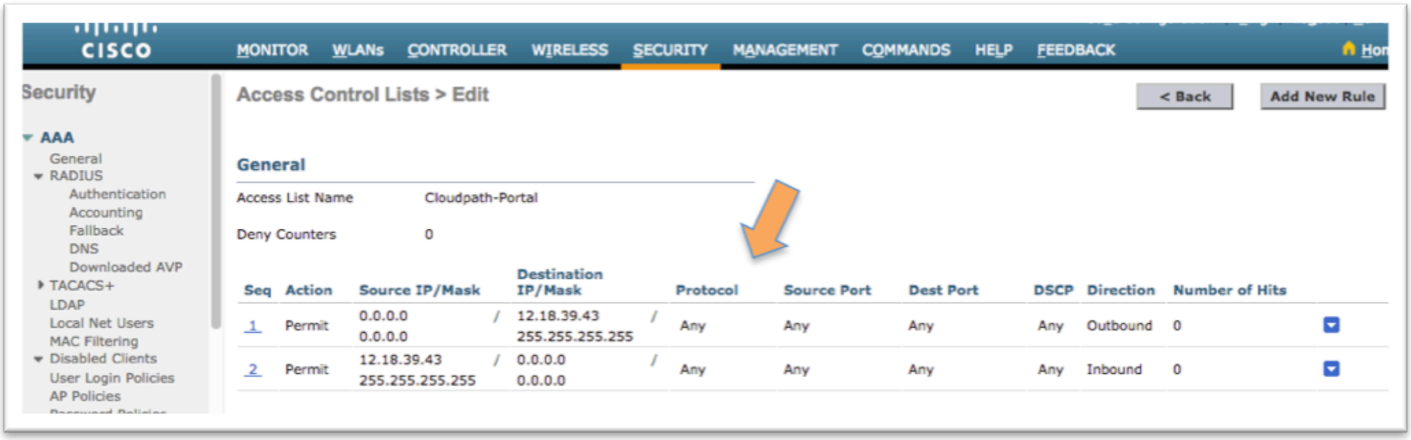
DSCP Any

Direction Outbound

Action Permit

- Create a rule that allows traffic to the Cloudpath server and click **Apply**
- Similarly, create another rule that allows inbound traffic from the Cloudpath server.
- Continue as necessary to allow access to the gateway, DHCP and DNS server(s)

- Details of the ACL rules depend on the network in questions and its security standards
- For more detailed discussion, see the Cisco documentation



Access Control Lists > Edit

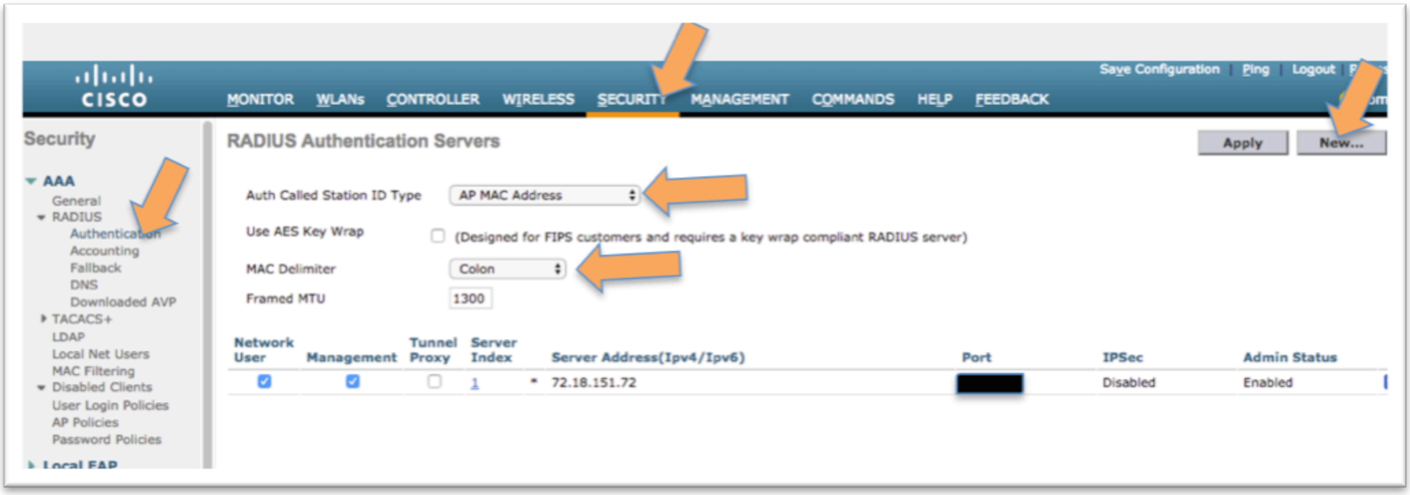
General

Access List Name: Cloudpath-Portal

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	12.18.39.43 / 255.255.255.255	Any	Any	Any	Any	Outbound	0
2	Permit	12.18.39.43 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Inbound	0

4) Define a RADIUS Authentication Server as the Cloudpath RADIUS server



RADIUS Authentication Servers

Auth Called Station ID Type: AP MAC Address

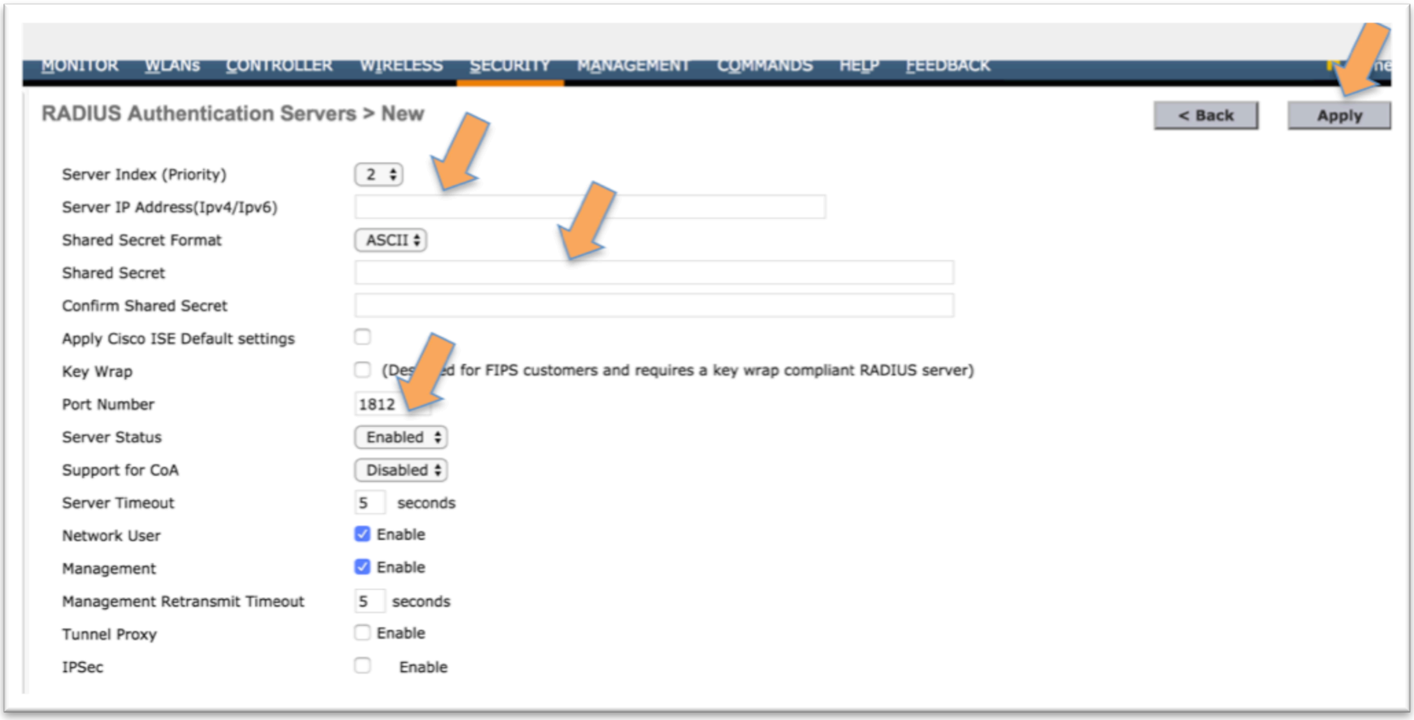
Use AES Key Wrap: □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: Colon

Framed MTU: 1300

Network User	Management	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
☑	☑	□	1	72.18.151.72	[redacted]	Disabled	Enabled

- Click on **Security** to access the *Security menu*
  - Expand **AAA,** expand **RADIUS** and then click on **Authentication**
  - Accept Auth Called Station ID Type as AP MAC Address the default)
  - Accept **MAC Delimiter** as **Colon** (the default)
  - Click **New**


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
< Back
Apply

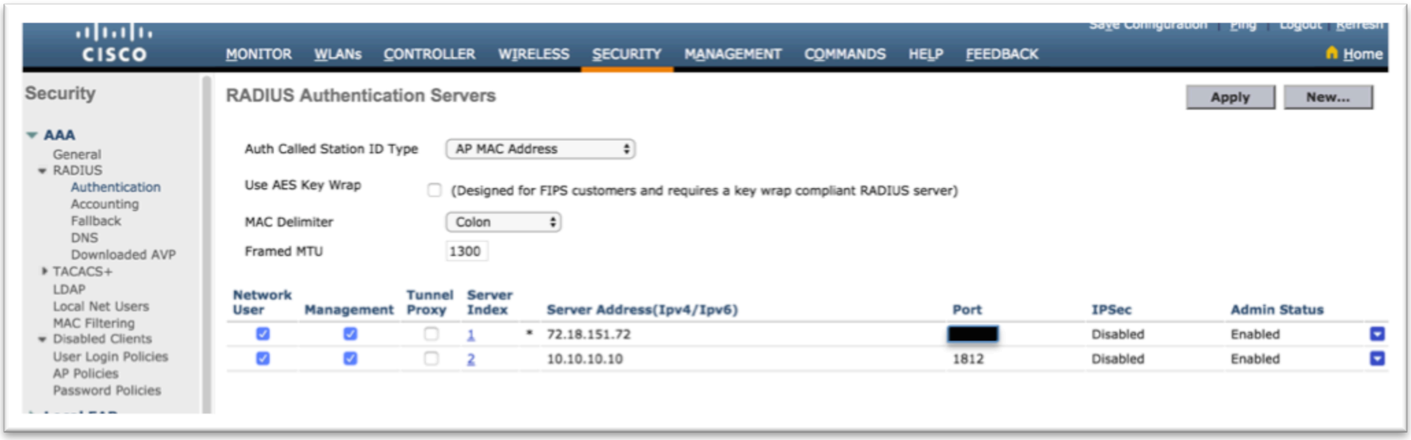
RADIUS Authentication Servers > New

Server Index (Priority)	2
Server IP Address(Ipv4/Ipv6)	
Shared Secret Format	ASCII
Shared Secret	
Confirm Shared Secret	
Apply Cisco ISE Default settings	□
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for CoA	Disabled
Server Timeout	5 seconds
Network User	☑ Enable
Management	☑ Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	□ Enable
IPSec	□ Enable

- The *RADIUS Authentication Server* is the Cloudpath RADIUS server from section 1

- Fill in the Server **IP Address** of the Cloudpath Server
- Fill in the **Shared Secret** and the **Confrim Shared Secret** with the Shared Secret from the Cloudpath ES RADIUS server
- Fill in the **Port Number**
- The defaults should be correct for the rest
- Click **Apply**

The RADIUS Authentication Server is defined in the list



RADIUS Authentication Servers

Auth Called Station ID Type: AP MAC Address

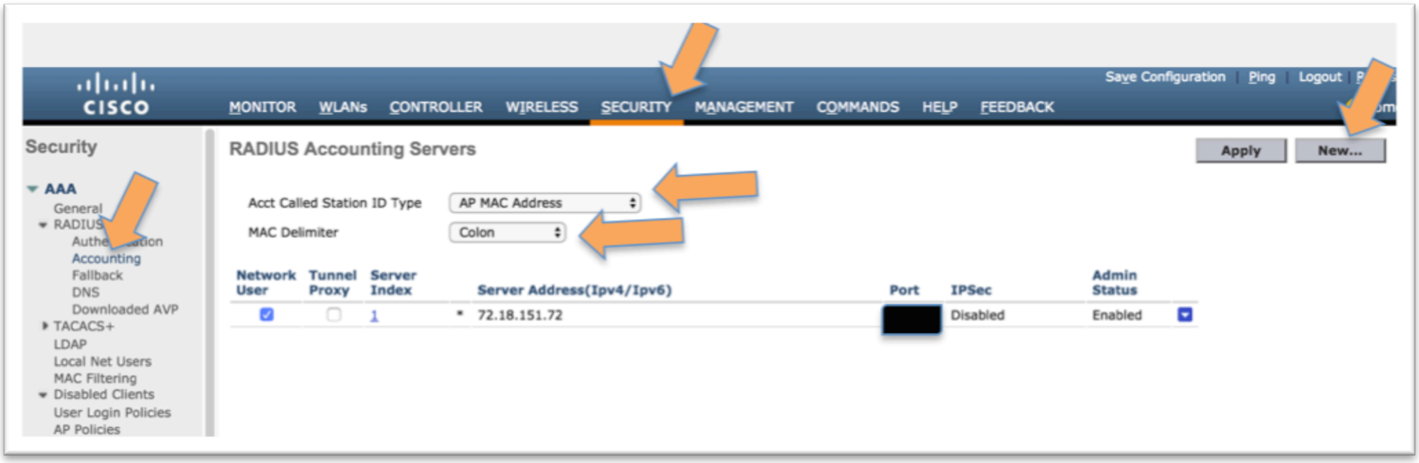
Use AES Key Wrap: □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: Colon

Framed MTU: 1300

Network User	Management	Tunnel Proxy	Server Index		Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
☑	☑	□	1	*	72.18.151.72	[redacted]	Disabled	Enabled
☑	☑	□	2		10.10.10.10	1812	Disabled	Enabled

5) Define the RADIUS Accounting Server as the Cloudpath RADIUS server



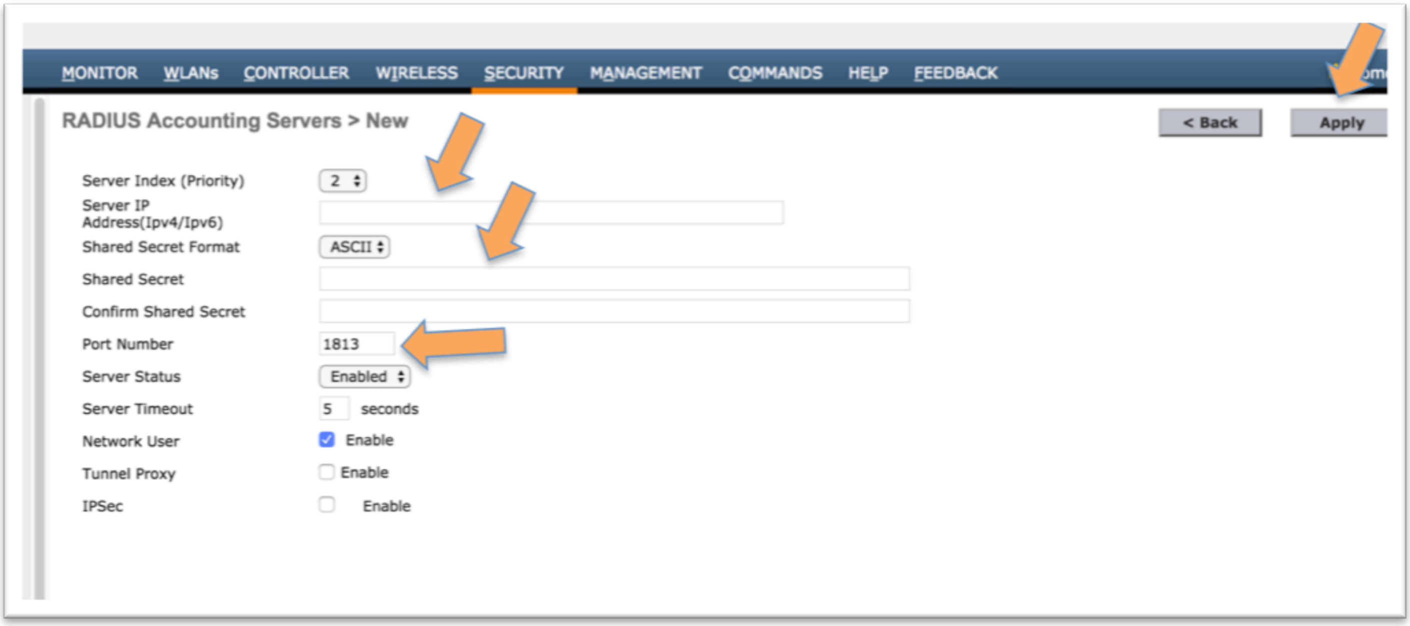
RADIUS Accounting Servers

Acct Called Station ID Type: AP MAC Address

MAC Delimiter: Colon

Network User	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
☑	□	1	72.18.151.72	[redacted]	Disabled	Enabled

- Click on **Security** to access the *Security menu*
  - Expand **AAA,** expand **RADIUS** and then click on **Accounting**
  - Accept **Auth Called Station ID Type** as *AP MAC Address* (the default)
  - Accept **MAC Delimiter** as **Colon** (the default)
  - Click **New**



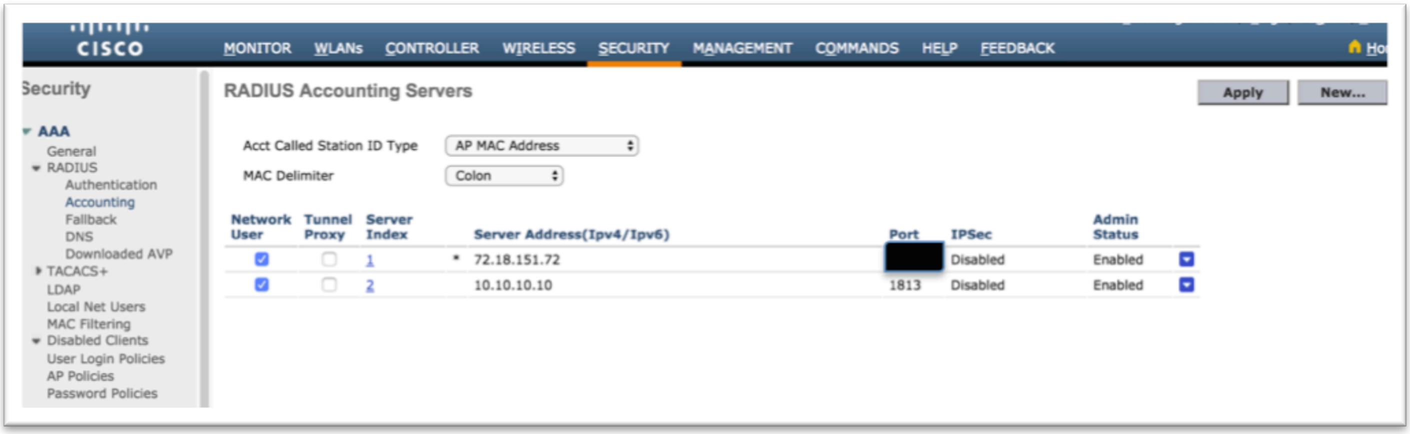
RADIUS Accounting Servers > New

Server Index (Priority)	2
Server IP Address(Ipv4/Ipv6)	
Shared Secret Format	ASCII
Shared Secret	
Confirm Shared Secret	
Port Number	1813
Server Status	Enabled
Server Timeout	5 seconds
Network User	☑ Enable
Tunnel Proxy	□ Enable
IPSec	□ Enable

- The *RADIUS Accounting Server* is the Cloudpath RADIUS server from section 1
  - Fill in the **Server IP Address** of the Cloudpath Server

- Fill in the **Shared Secret** and the **Confrim Shared Secret** with the Shared Secret from the Cloudpath ES RADIUS server
- Fill in the **Port Number**
- The defaults should be correct for the rest
- Click **Apply**

The *RADIUS Accounting Server* is defined in the list



RADIUS Accounting Servers

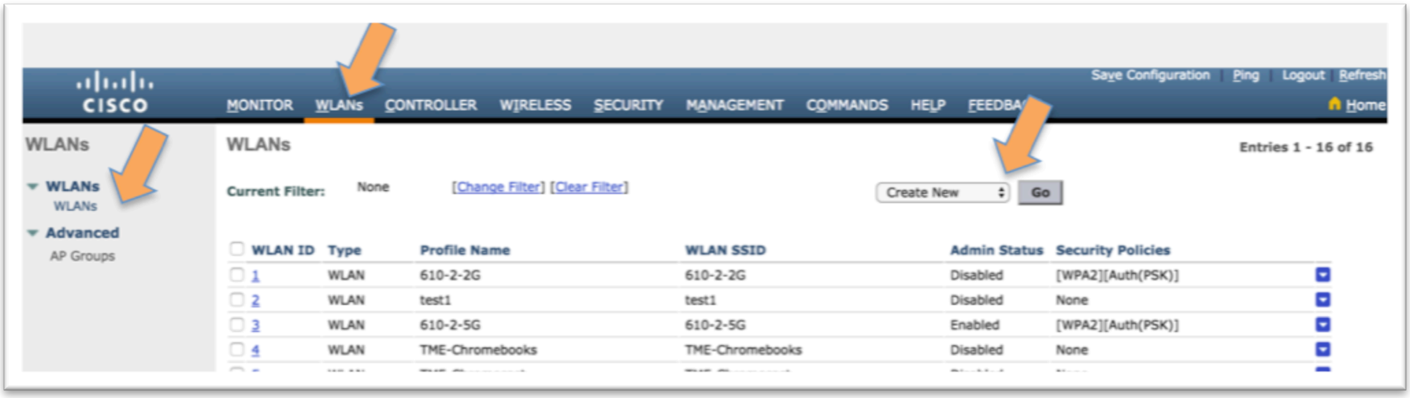
Acct Called Station ID Type: AP MAC Address

MAC Delimiter: Colon

Network User	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
☑	□	1	* 72.18.151.72	[redacted]	Disabled	Enabled
☑	□	2	10.10.10.10	1813	Disabled	Enabled

6) Create Two WLAN profiles

One profile is for the secure/802.1X WLAN, the second for the onboarding/guest WLAN



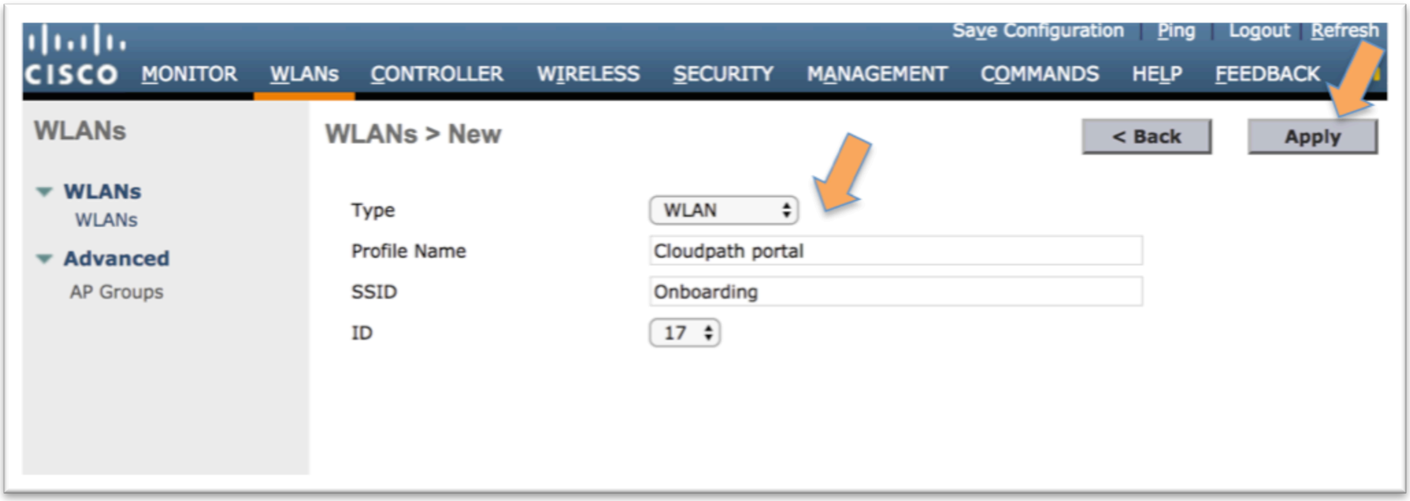
WLANs

Entries 1 - 16 of 16

Current Filter: None

□ WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
□ 1	WLAN	610-2-2G	610-2-2G	Disabled	[WPA2][Auth(PSK)]
□ 2	WLAN	test1	test1	Disabled	None
□ 3	WLAN	610-2-5G	610-2-5G	Enabled	[WPA2][Auth(PSK)]
□ 4	WLAN	TME-Chromebooks	TME-Chromebooks	Disabled	None

- Click on **WLANs** to access the *WLANs menu*
  - Expand **WLANs,** and then click on **WLANs** (yes, it appears twice)
  - Choose Creat New and Click **Go**
  - Alternately, modify an existing WLAN by clicking on the *WLAN ID*



WLANs > New

Type	WLAN
Profile Name	Cloudpath portal
SSID	Onboarding
ID	17

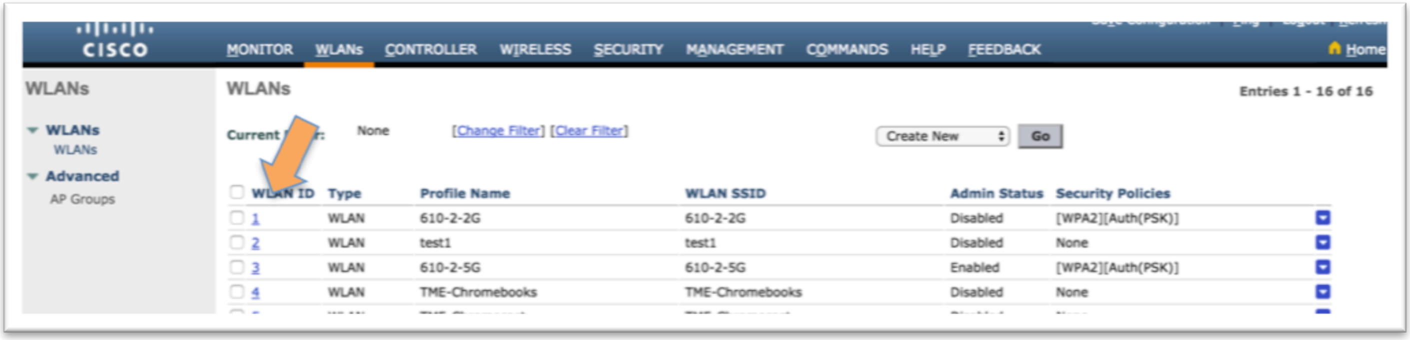
  - Choose type **WLAN**
  - Type a **Profile Name** for the Secure/802.1X WLAN
  - Type an **SSID** for the Secure/802.1X WLAN
- Click **Apply**

Repeat for the Onboarding/Guest WLAN

- Choose Create New and Click **Go**

- Choose type **WLAN**
- Type a **Profile Name** for the Onboarding/Guest WLAN
- Type an **SSID** for the Onboarding/Guest WLAN
- Click **Apply**

7) Edit the Secure (802.1X) WLAN profile



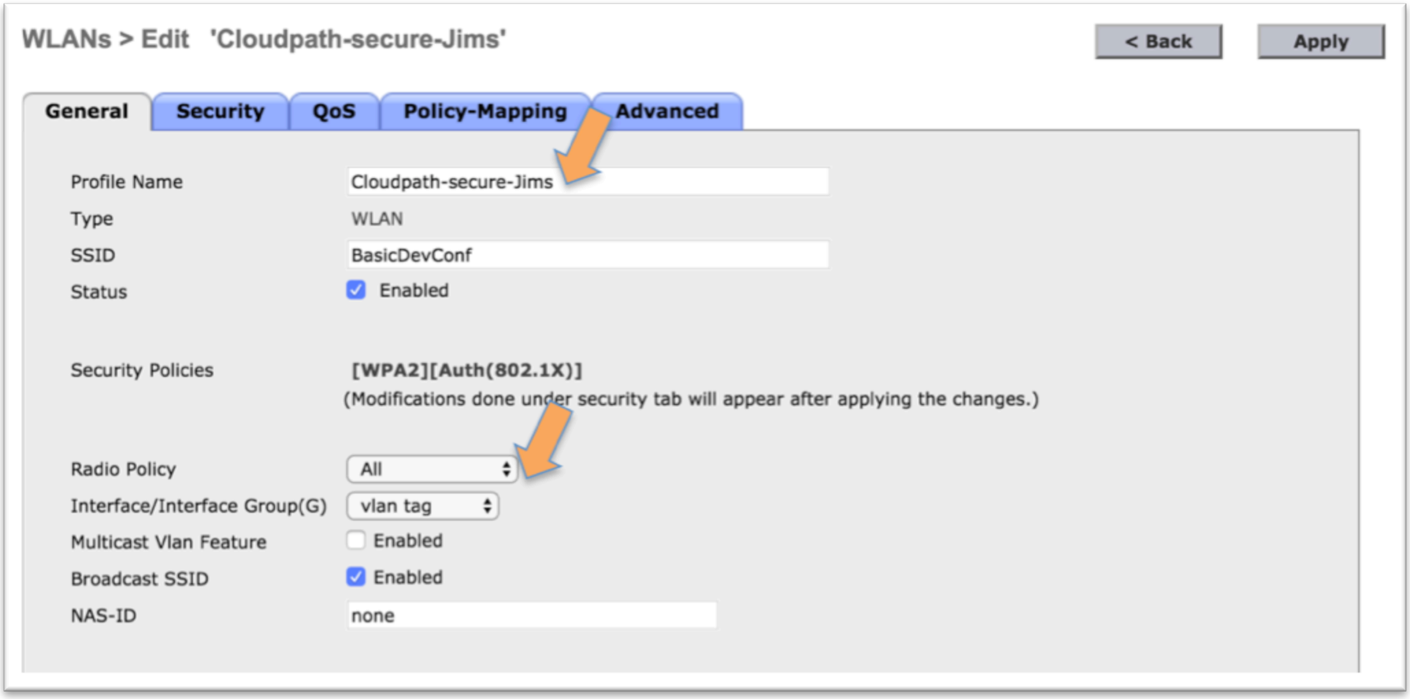
WLANs

Entries 1 - 16 of 16

Current Filter: None [Change Filter] [Clear Filter]

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	610-2-2G	610-2-2G	Disabled	[WPA2][Auth(PSK)]
2	WLAN	test1	test1	Disabled	None
3	WLAN	610-2-5G	610-2-5G	Enabled	[WPA2][Auth(PSK)]
4	WLAN	TME-Chromebooks	TME-Chromebooks	Disabled	None

- Click on the **WLAN ID** of the Secure WLAN profile

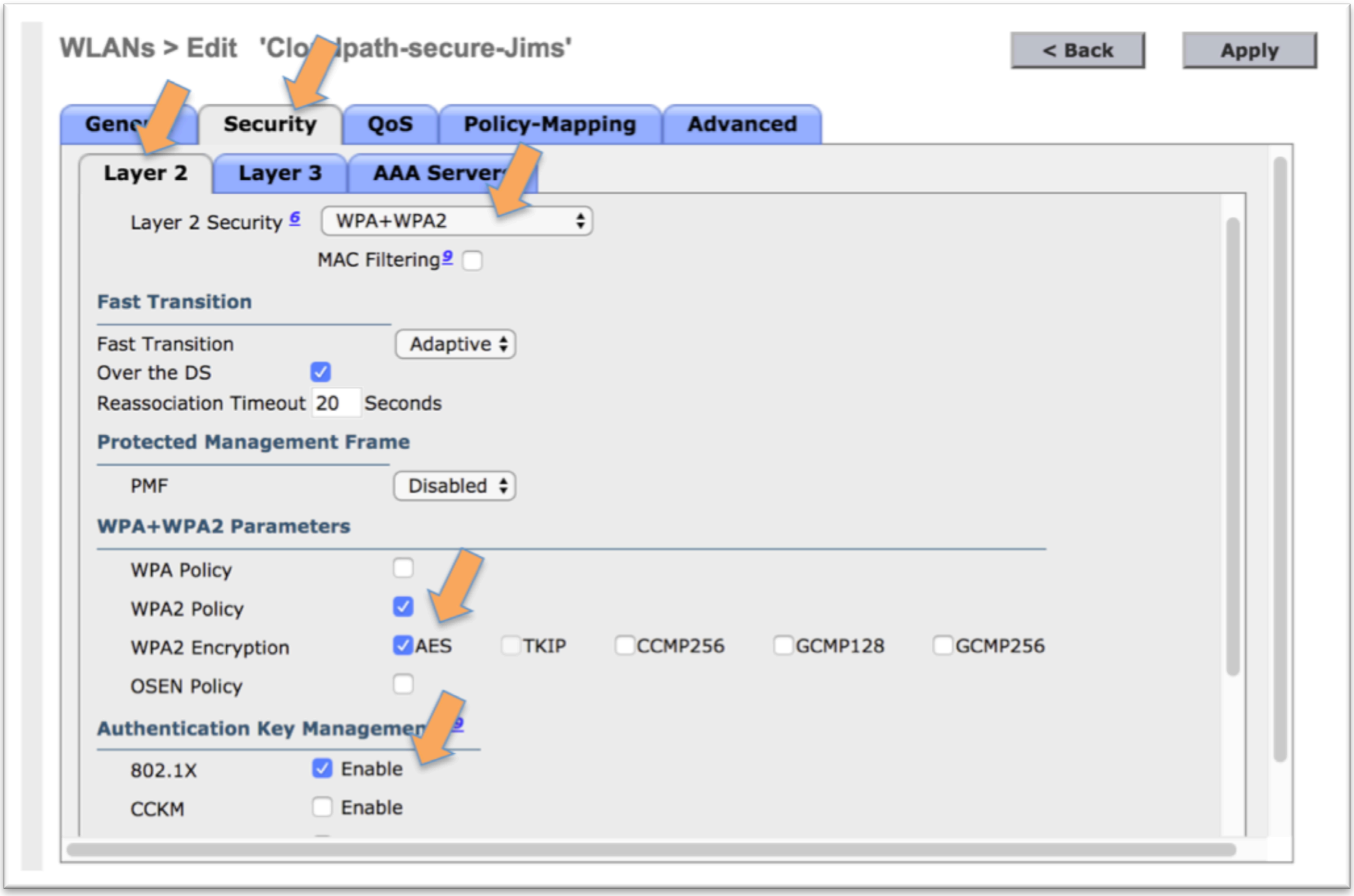


WLANs > Edit 'Cloudpath-secure-Jims'

Profile Name	Cloudpath-secure-Jims
Type	WLAN
SSID	BasicDevConf
Status	☑ Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	vlan tag
Multicast Vlan Feature	□ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	none

- The **General** tab appears – if not, click on it
- Confirm the **Profile Name** and **SSID** are correct (or modify as necessary)
- Set Status to Enabled

- As appropriate for the WLAN, choose **Radio Policy, Interface**, etc.
- Move on to the **Security** tab



WLANs > Edit 'Cloudpath-secure-Jims'

Layer 2 Security: WPA+WPA2
MAC Filtering ☐

Fast Transition

Fast Transition: Adaptive
Over the DS ☑
Reassociation Timeout 20 Seconds

Protected Management Frame

PMF: Disabled

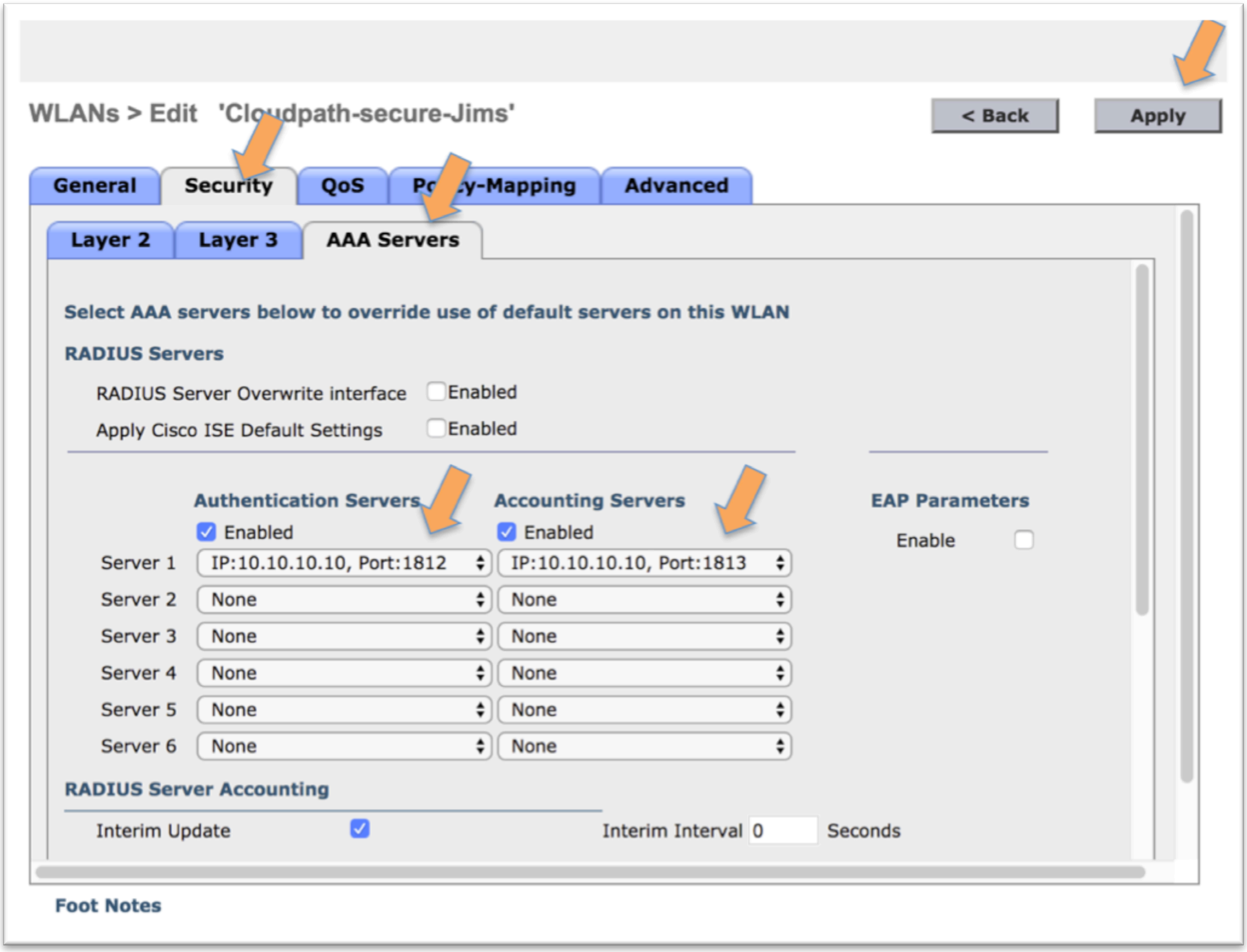
WPA+WPA2 Parameters

WPA Policy ☐
WPA2 Policy ☑
WPA2 Encryption ☑AES ☐TKIP ☐CCMP256 ☐GCMP128 ☐GCMP256
OSEN Policy ☐

Authentication Key Management

802.1X ☑ Enable
CCKM ☐ Enable

- Under the **Security** tab, go to the **Layer 2** tab
  - For Layer 2 Security choose WPA_WPA2
  - Under **WPA + WPA2 Parameters** choose **WPA2** and **WPA** if required, and choose **AES** for encryption
  - Under Authentication Key Management, **Enable** *802.1X*
  - Move on the **AAA Servers** tab



WLANs > Edit 'Cloudpath-secure-Jims'

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:10.10.10.10, Port:1812	IP:10.10.10.10, Port:1813
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

EAP Parameters

Enable □

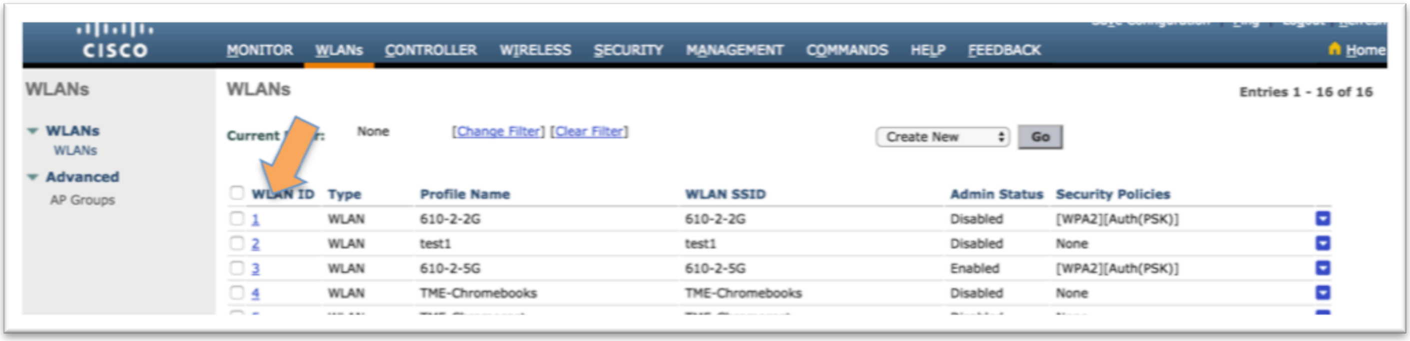
RADIUS Server Accounting

Interim Update ☑ Interim Interval 0 Seconds

- Under the **Security** tab, go to the **AAA Servers** tab
  - Choose and Enable the **Authentication Server** and the **Accounting Server** previously defined – that is, the Cloudpath RADIUS server
  - Click **Apply**

The Secure 802.1X WLAN is defined.

8) Edit the onboarding WLAN profile


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
WLANs
WLANs
WLANs
Advanced
AP Groups
Create New
Go

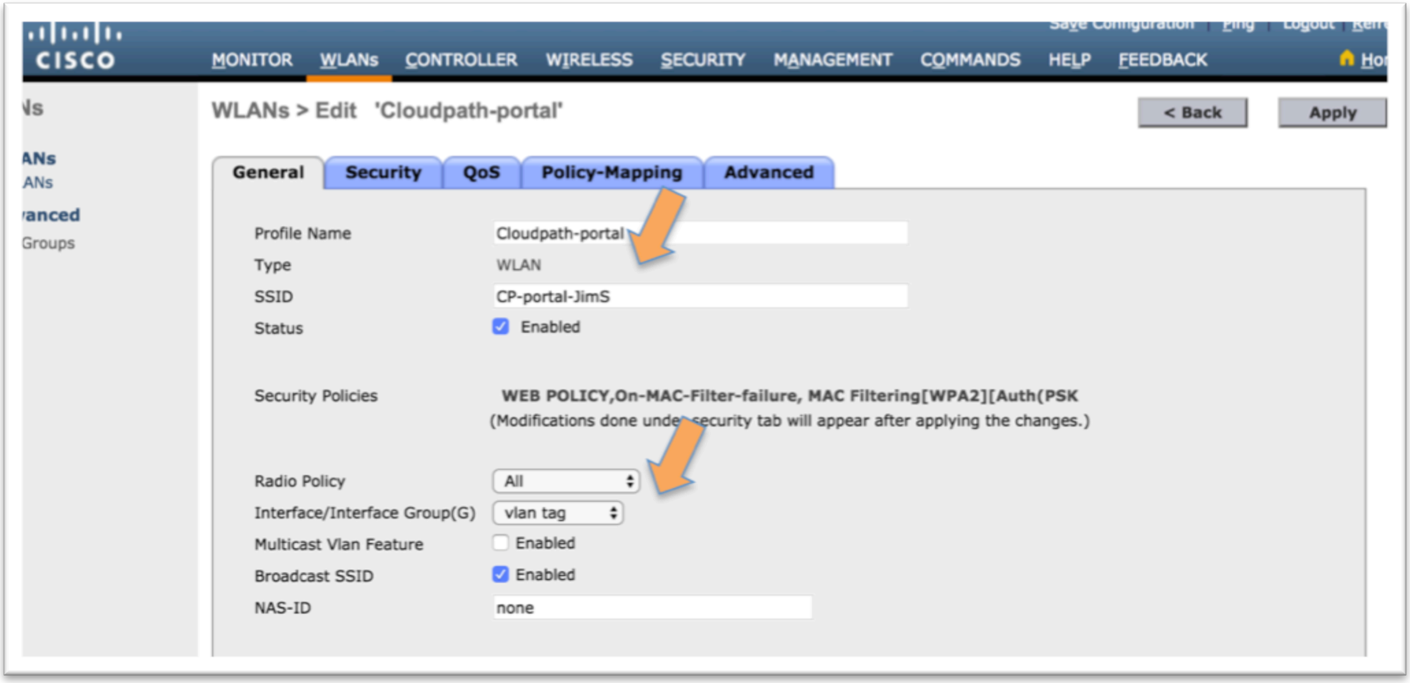
WLANs

Entries 1 - 16 of 16

Current Filter: None [Change Filter] [Clear Filter]

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	610-2-2G	610-2-2G	Disabled	[WPA2][Auth(PSK)]
2	WLAN	test1	test1	Disabled	None
3	WLAN	610-2-5G	610-2-5G	Enabled	[WPA2][Auth(PSK)]
4	WLAN	TME-Chromebooks	TME-Chromebooks	Disabled	None

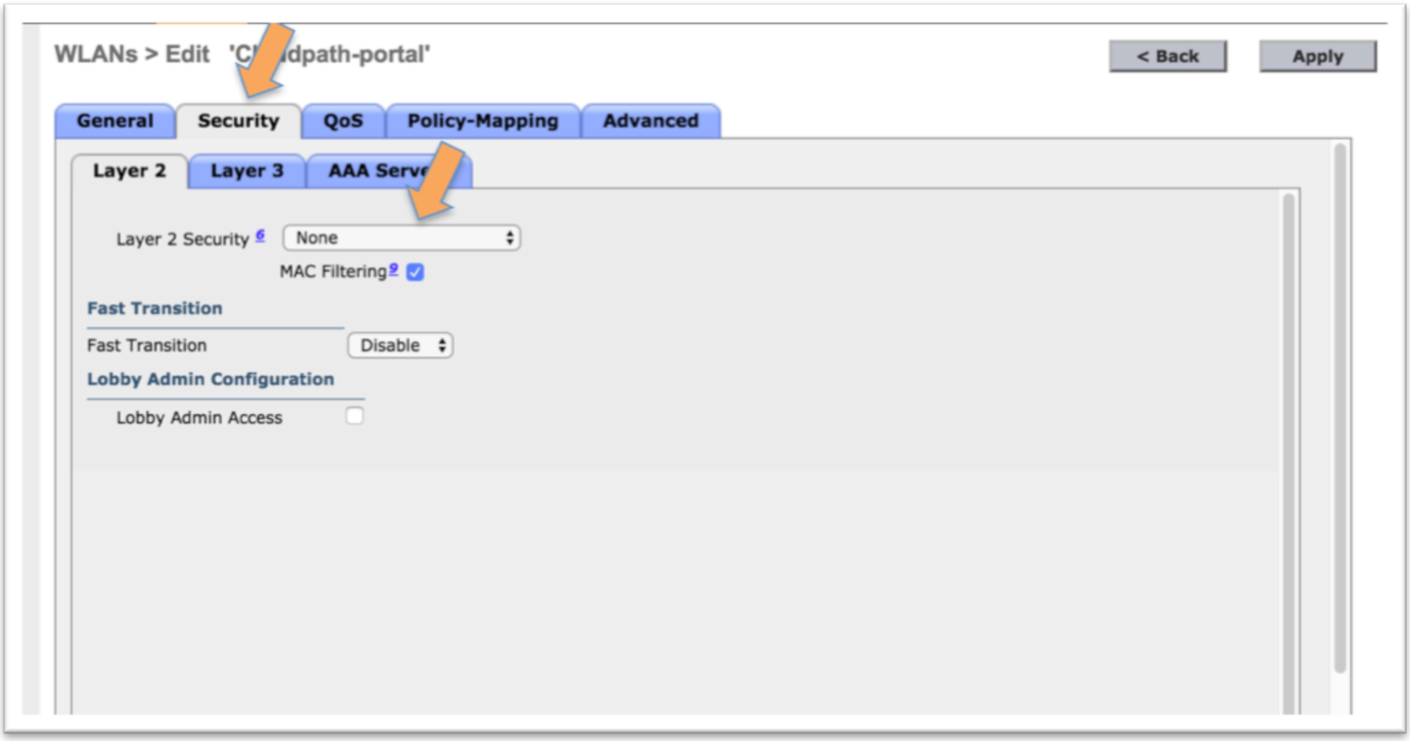
- Click on the **WLAN ID** of the onboarding WLAN profile


CISCO
Save Configuration | Ping | Logout | Refr
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Ho
Ns
ANs
ANs
anced
Groups
< Back
Apply
General
Security
QoS
Policy-Mapping
Advanced

WLANs > Edit 'Cloudpath-portal'

Profile Name	Cloudpath-portal
Type	WLAN
SSID	CP-portal-JimS
Status	☑ Enabled
Security Policies	WEB POLICY,On-MAC-Filter-failure, MAC Filtering[WPA2][Auth(PSK (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	vlan tag
Multicast Vlan Feature	□ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	none

- The **General** tab appears – if not, click on it
  - Confirm the **Profile Name** and **SSID** are correct (or modify as necessary)
  - Set Status to **Enabled**
  - As appropriate for the WLAN, choose **Radio Policy, Interface**, etc.
  - Move on to the **Security** tab



WLANs > Edit 'Cl dpath-portal'

Layer 2 Security [6]: None

MAC Filtering [9]: ☑

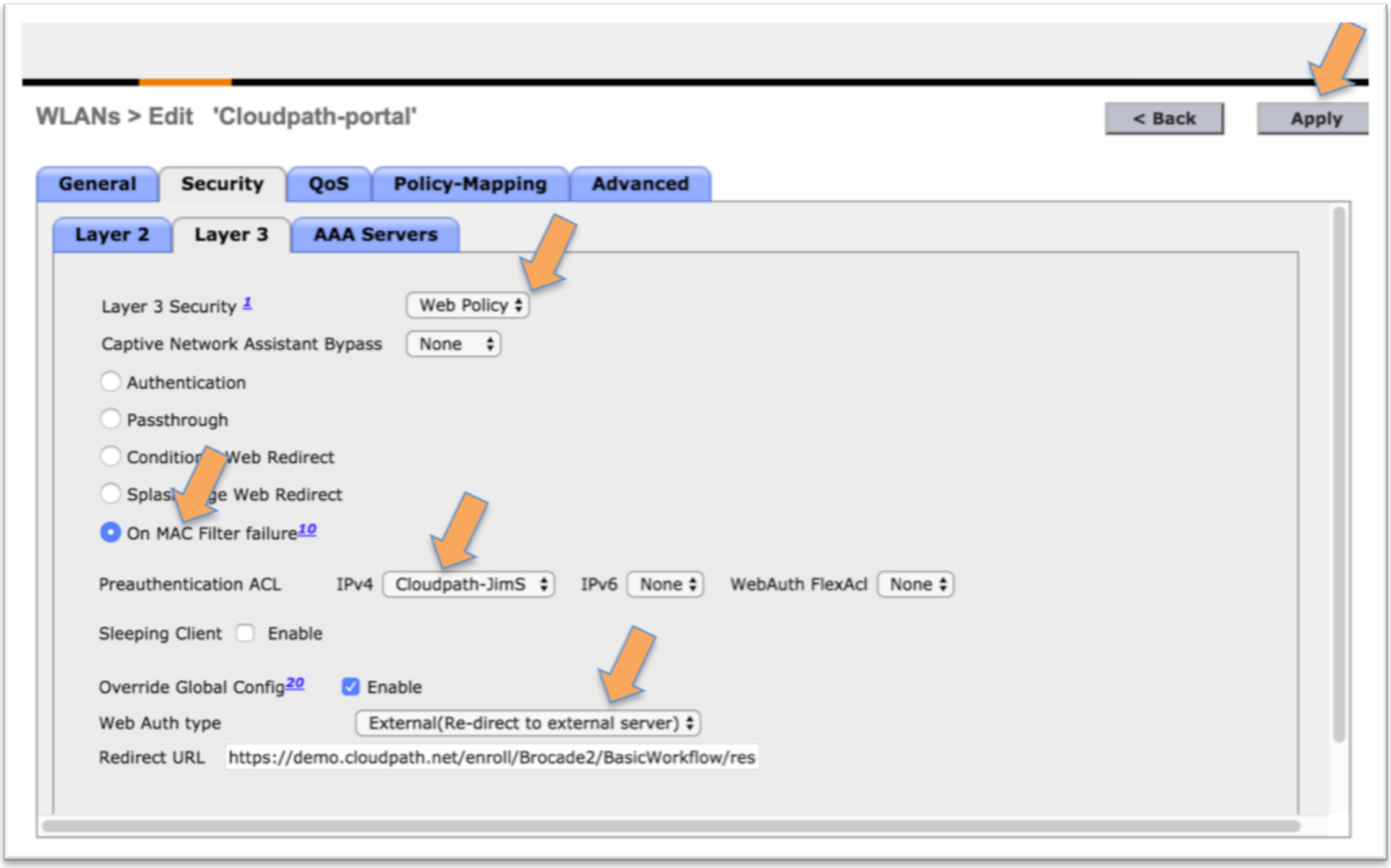
Fast Transition

Fast Transition: Disable

Lobby Admin Configuration

Lobby Admin Access: ☐

- Under the **Security** tab, go to the **Layer 2** tab
  - For *Layer 2 Security* choose **None**
  - Move on to the **Layer 3** tab



WLANs > Edit 'Cloudpath-portal'

Layer 3 Security [1] Web Policy

Captive Network Assistant Bypass None

○ Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

● On MAC Filter failure[10]

Preauthentication ACL IPv4 Cloudpath-JimS IPv6 None WebAuth FlexAcl None

Sleeping Client □ Enable

Override Global Config[20] ☑ Enable

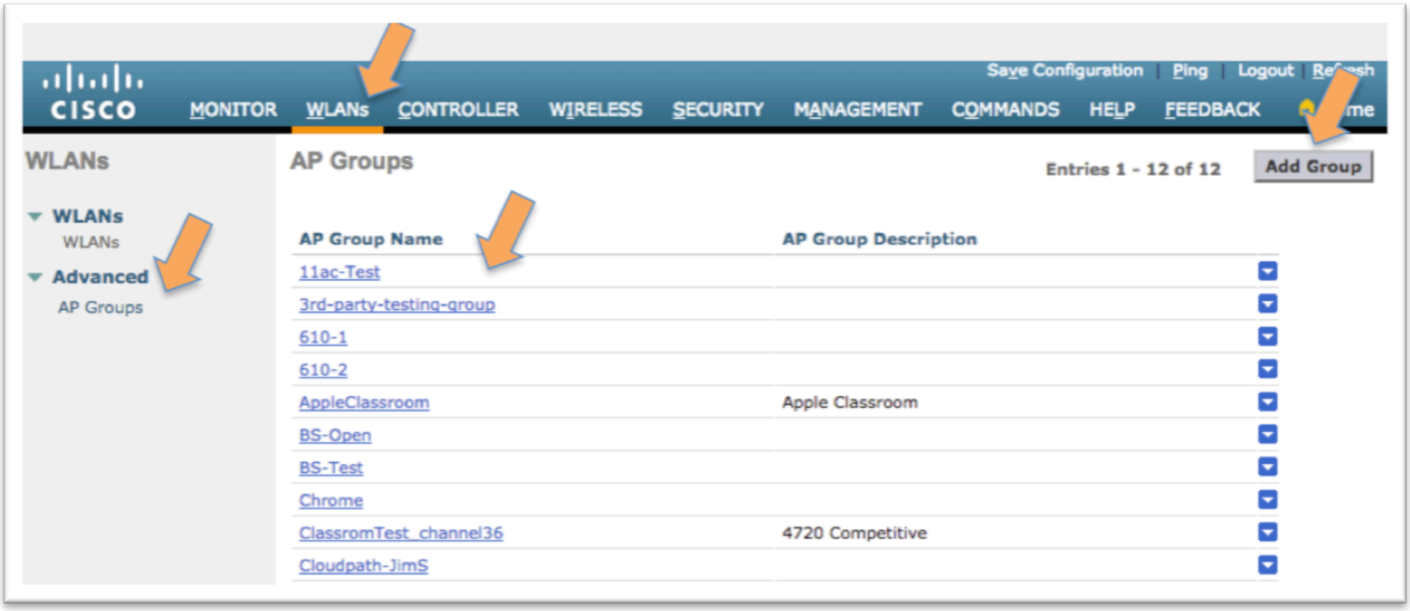
Web Auth type External(Re-direct to external server)

Redirect URL https://demo.cloudpath.net/enroll/Brocade2/BasicWorkflow/res

- Under the **Security** tab, go to the **Layer 3** tab
  - For **Layer 3** Security choose **Web Policy**
  - Among the radio buttons, choose **On MAC Filter failure**
  - For **Preauthentication ACL,** choose the previously defined ACL
  - For *Web Auth Type* choose External (Re-direct to external server)
  - For **Redirect URL** enter the URL of the workflow defined on Cloudpath, as described in section 1
  - Click **Apply**

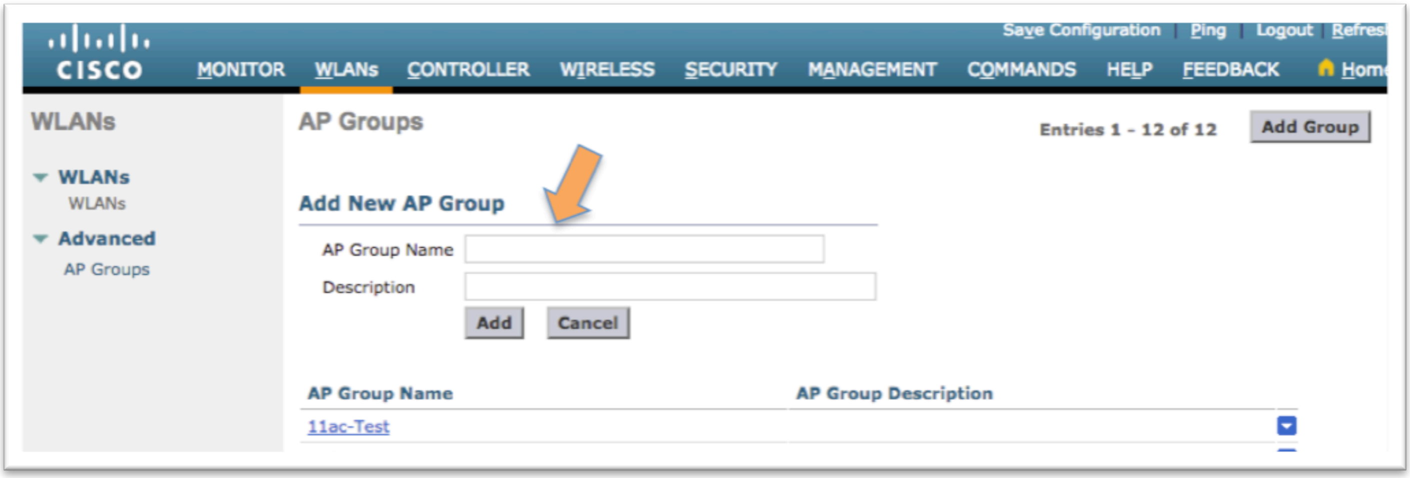
The Onboarding Portal is defined.

9) Create or Edit an AP group to deploy WLANs



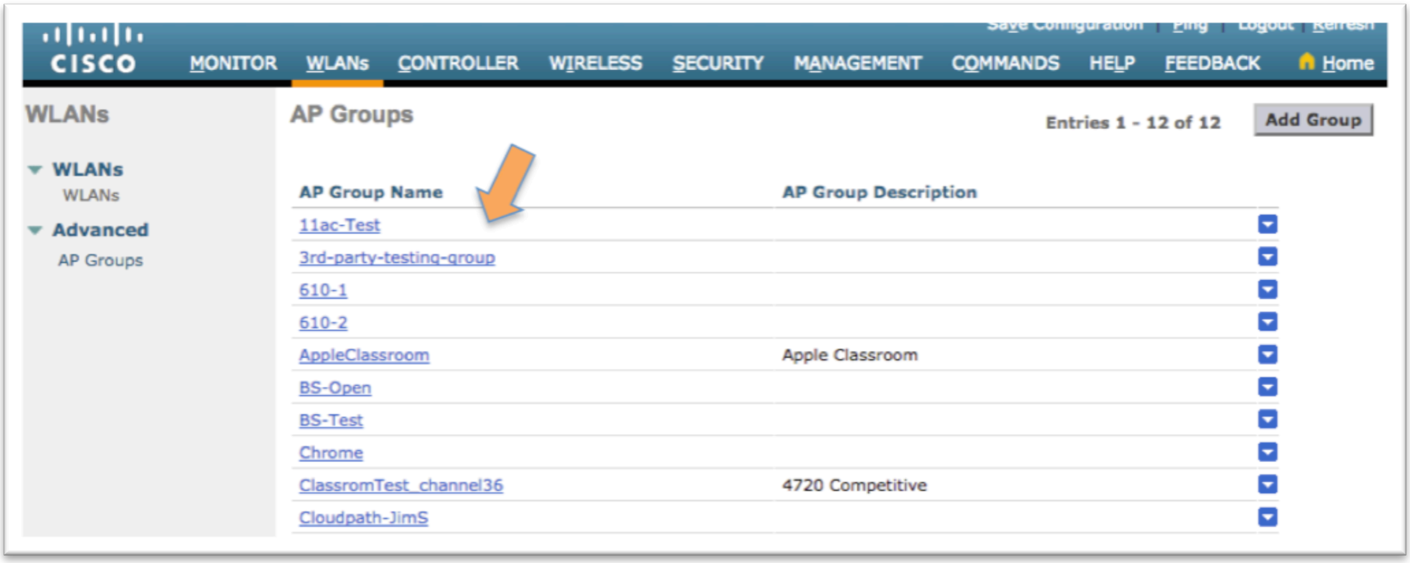
AP Group Name	AP Group Description
11ac-Test	
3rd-party-testing-group	
610-1	
610-2	
AppleClassroom	Apple Classroom
BS-Open	
BS-Test	
Chrome	
ClassromTest_channel36	4720 Competitive
Cloudpath-JimS	

- Click on **WLANs** to access the WLANs menu
  - Expand **Advanced,** and then click on **AP Groupss**
  - Create a new Group by clicking on **Add Group**
  - Alternately, modify an existing Group by clicking on the *AP Group Name*



AP Group Name	AP Group Description
11ac-Test	

- The **Add New AP Group** section appears
  - Enter a name in the **AP Group Name**
  - Optionally, add a **Description**
  - Click **Add**

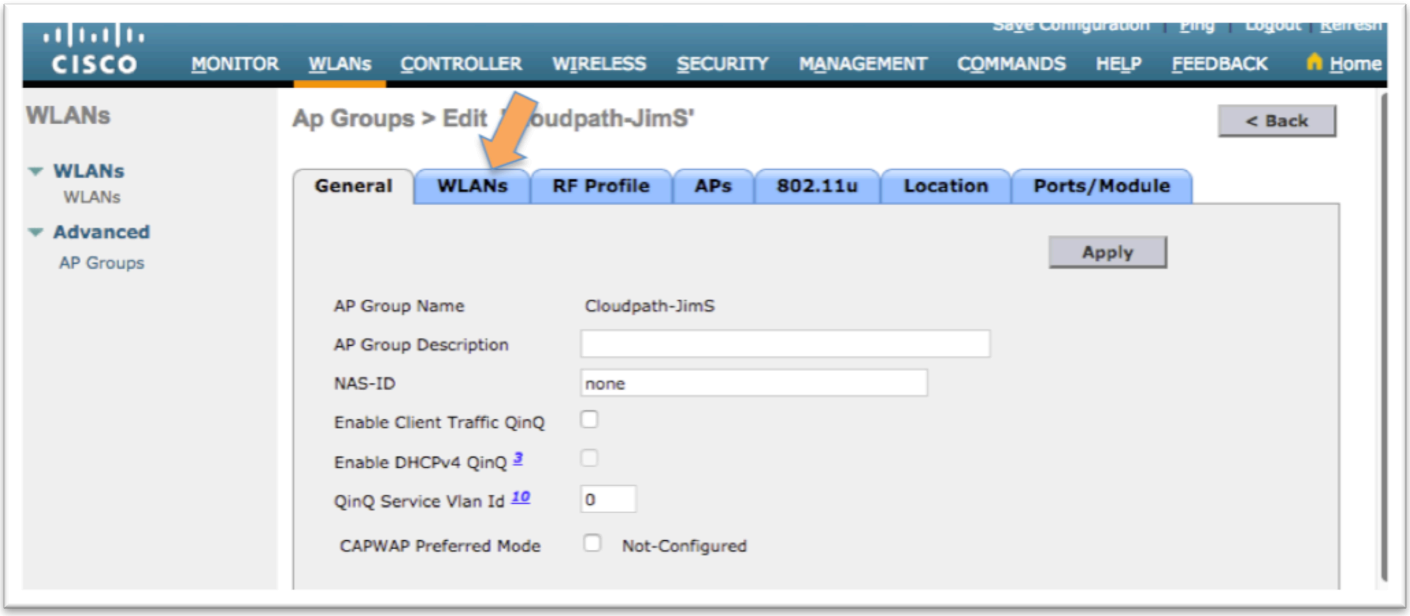


AP Groups

Entries 1 - 12 of 12

AP Group Name	AP Group Description
11ac-Test	
3rd-party-testing-group	
610-1	
610-2	
AppleClassroom	Apple Classroom
BS-Open	
BS-Test	
Chrome	
ClassromTest_channel36	4720 Competitive
Cloudpath-JimS	

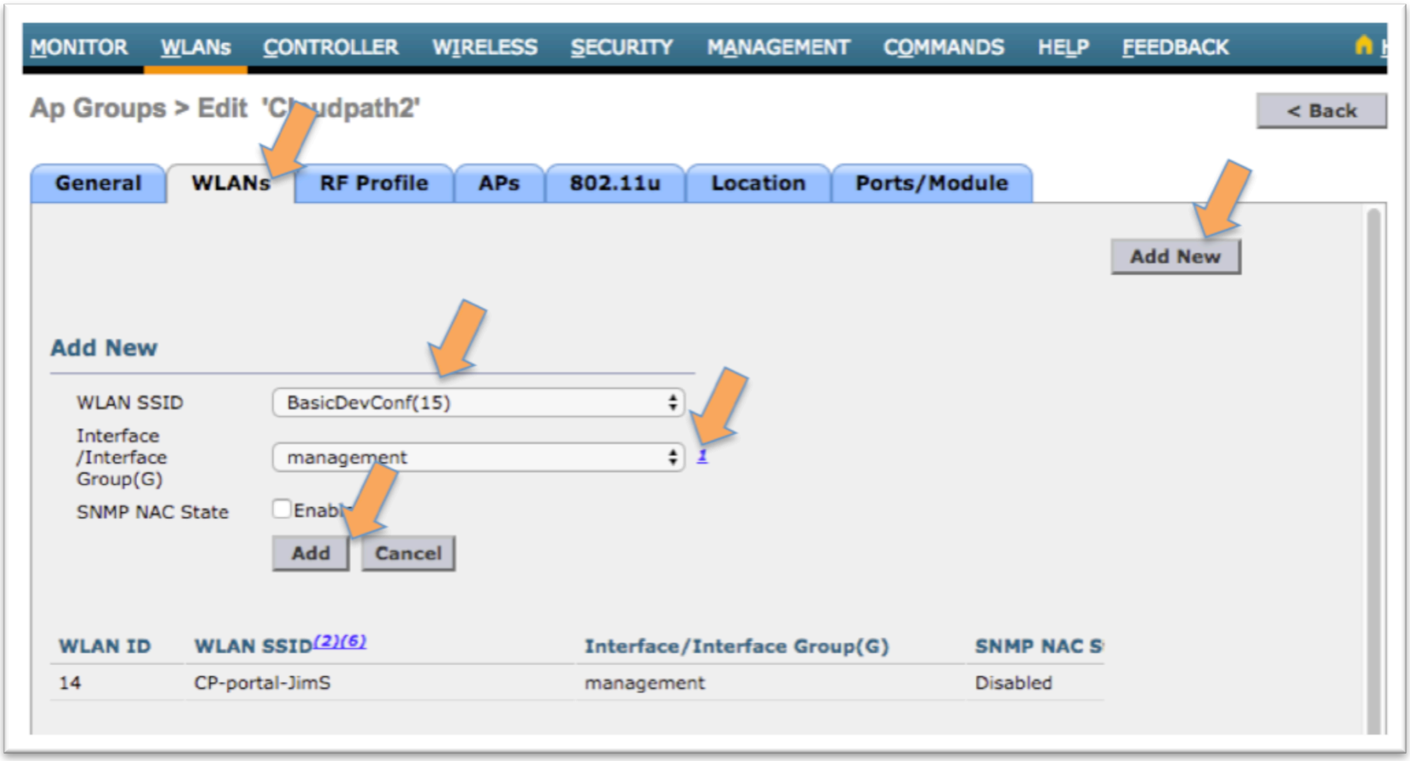
- Now click on the AP Group Name to edit



Ap Groups > Edit 'Cloudpath-JimS'

AP Group Name	Cloudpath-JimS
AP Group Description	
NAS-ID	none
Enable Client Traffic QinQ	□
Enable DHCPv4 QinQ [3]	□
QinQ Service Vlan Id [10]	0
CAPWAP Preferred Mode	□ Not-Configured

- Go to the **WLANs** tab



Ap Groups > Edit 'Cloudpath2'

Add New

WLAN SSID: BasicDevConf(15)

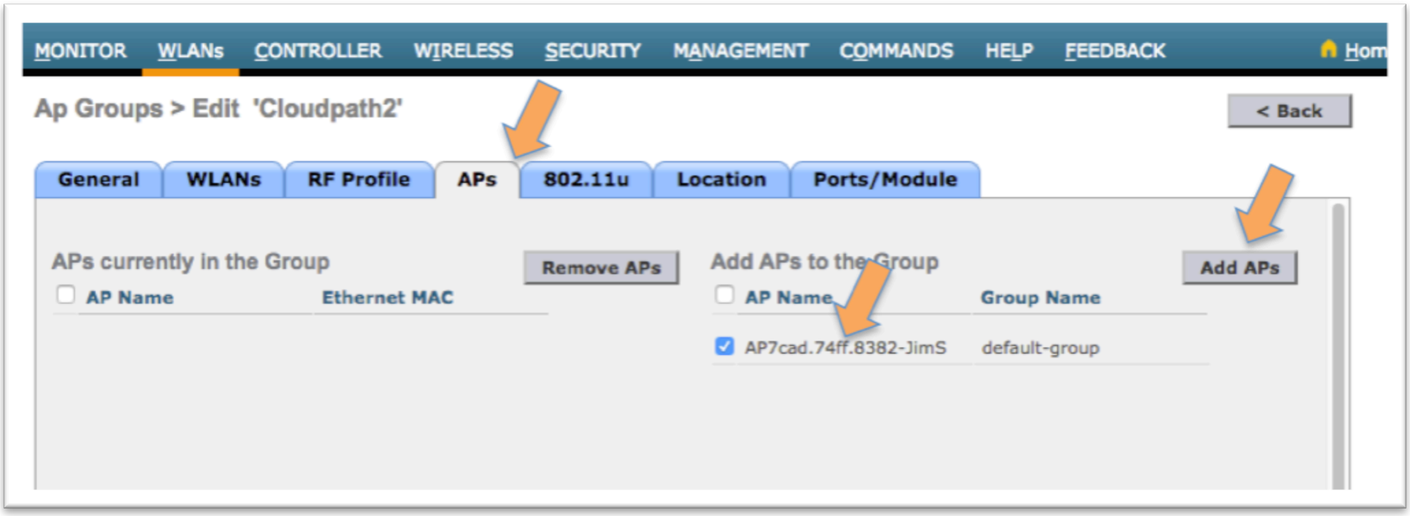
Interface /Interface Group(G): management 1

SNMP NAC State: □ Enable

WLAN ID	WLAN SSID(2)(6)	Interface/Interface Group(G)	SNMP NAC S
14	CP-portal-JimS	management	Disabled

- In the **WLANs** tab, click the **Add New** button
  - Choose the **WLAN SSID** of the onboarding portal
  - Choose the i**nterface** for the WLAN
  - Click **Add**
- repeat for the authenticated WLAN
  - In the **WLANs** tab, click the **Add New** button
  - Choose the **WLAN SSID** of the 802.1X authenticated WLAN
  - Choose the **interface** for the WLAN
  - Click **Add**

Be careful not to add the wrong WLAN or an extra WLAN. To remove a WLAN, the group has to be deleted and recreated.



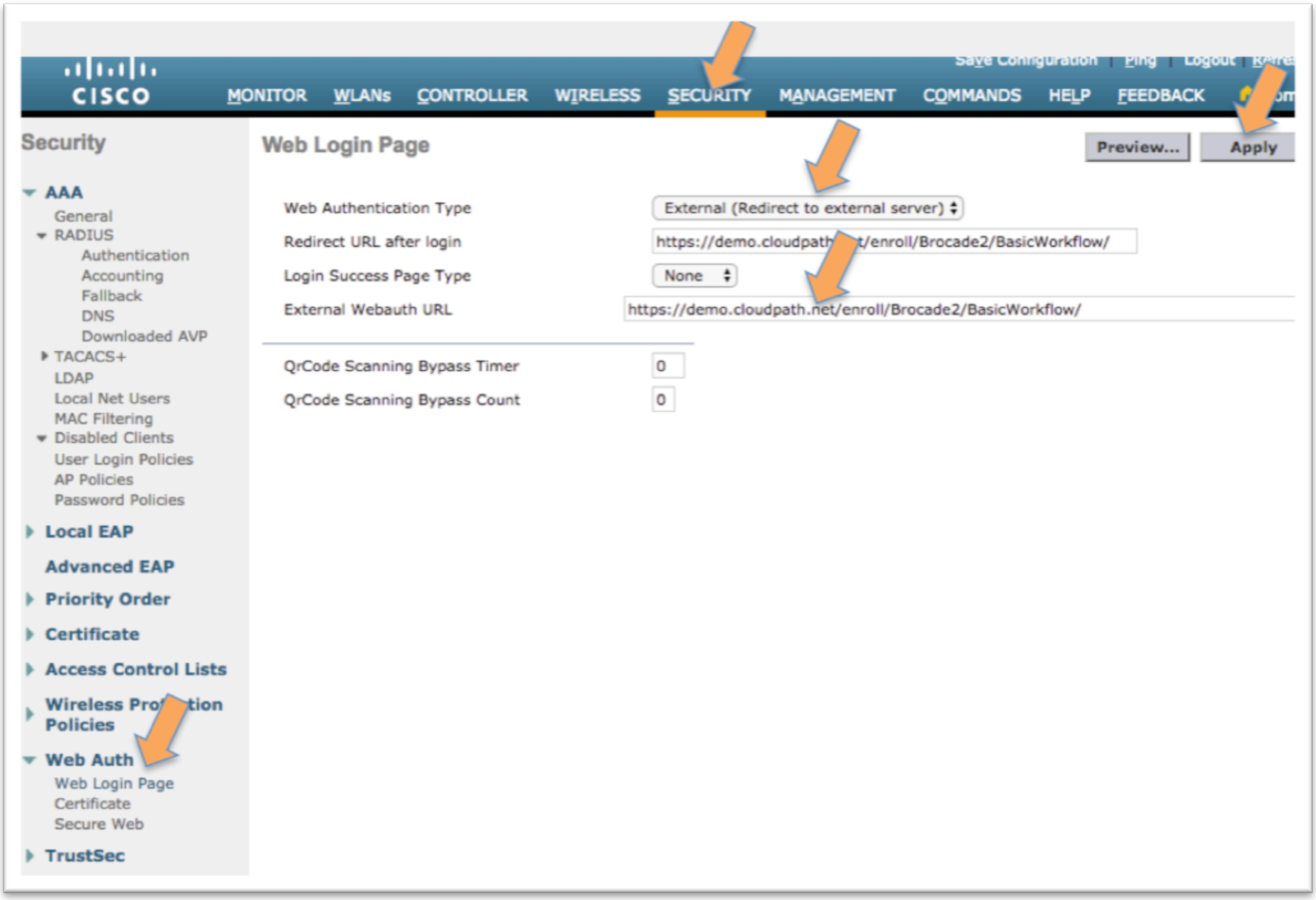
☐ AP Name | Group Name
☑ AP7cad.74ff.8382-JimS | default-group

- Go to the **APs** tab
  - Under **Add APs to the Group,** check the APs that will be part of the group and will service our two WLANs
  - Click Add APs

Configuration of the WLC is done and ready for testing.

10) Don’t do this: Configuring Web Auth default policy option

A global Web Auth policy can be set for the WLAN controller. The Onboarding Portal can be setup under the Security -> Web Auth menu. Best Practices are to add the onboarding Prtal URL to the WLAN profile as we did above. Associating the onboarding profile to only specific SSIDs is cleaner and more flexible. Furthermore, the MAC auth Guest passthrough from the onboarding profile does not work correctly when using the global Web Auth setting. However, if you are NOT using MAC auth passthrough, this configuration does work, and is included here for completeness.



Web Login Page

Web Authentication Type	External (Redirect to external server)
Redirect URL after login	https://demo.cloudpath.net/enroll/Brocade2/BasicWorkflow/
Login Success Page Type	None
External Webauth URL	https://demo.cloudpath.net/enroll/Brocade2/BasicWorkflow/
QrCode Scanning Bypass Timer	0
QrCode Scanning Bypass Count	0

- Click on **Security**
- In the **Security** menu, expand **Web Auth** and choose **Web Login Page**
- **For Web authentication Type** choose External (Redirect to external server)
- At External Webauth URL insert the *Cloudpath ES enrollment URL* found in section 1
- Click apply

Now any WLAN with a L3 security policy set to **Web Policy** will default to the Cloudpath URL

About Ruckus

Headquartered in Sunnyvale, CA, Ruckus Wireless, Inc. is a global supplier of advanced wireless systems for the rapidly expanding mobile Internet infrastructure market. The company offers a wide range of indoor and outdoor "Smart Wi-Fi" products to mobile carriers, broadband service providers, and corporate enterprises, and has over 36,000 end-customers worldwide. Ruckus technology addresses Wi-Fi capacity and coverage challenges caused by the ever-increasing amount of traffic on wireless networks due to accelerated adoption of mobile devices such as smartphones and tablets. Ruckus invented and has patented state-of-the-art wireless voice, video, and data technology innovations, such as adaptive antenna arrays that extend signal range, increase client data rates, and avoid interference, providing consistent and reliable distribution of delay-sensitive multimedia content and services over standard 802.11 Wi-Fi. For more information, visit http://www.ruckuswireless.com.

Cloudpath on Cisco WLC

Deploying a Cloudpath workflow on a Cisco WLAN Controller

November 2017

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of States law is prohibited. It is the reader’s responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN (“MATERIAL”) IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL