TECHNICAL DOCUMENTATION

Cloudpath
Enrollment System

Configuring Cloudpath ES to Support MAC Registration

Software Release 5.0

November 2016

Summary: This document describes the MAC registration process, how to set up MAC registration on a wireless LAN controller, how to configure Cloudpath to support MAC registration, including RADIUS attributes, how to view and revoke MAC registration enrollments, and troubleshooting information.

Document Type: Configuration

Audience: Network Administrator

Configuring Cloudpath ES to Support MAC Registration

Software Release 5.0

November 2016

This document contains Ruckus Wireless confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without express written authorization of a Customer Advocacy representative of Ruckus Wireless, Inc. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing, RUCKUS WIRELESS PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Configuring Cloudpath to Support MAC Registration

Overview

Using 802.1X authentication with WPA2-Enterprise provides the best security option for wireless devices on your network. However, for devices that do not have 802.1X support, such as gaming consoles or printers, Cloudpath offers a method for registering these devices on the network.

MAC registration allows network access to devices that do not have the 802.1X supplicant capability. The registration process provides authentication using the device's MAC address to allow limited, and secure, network access.

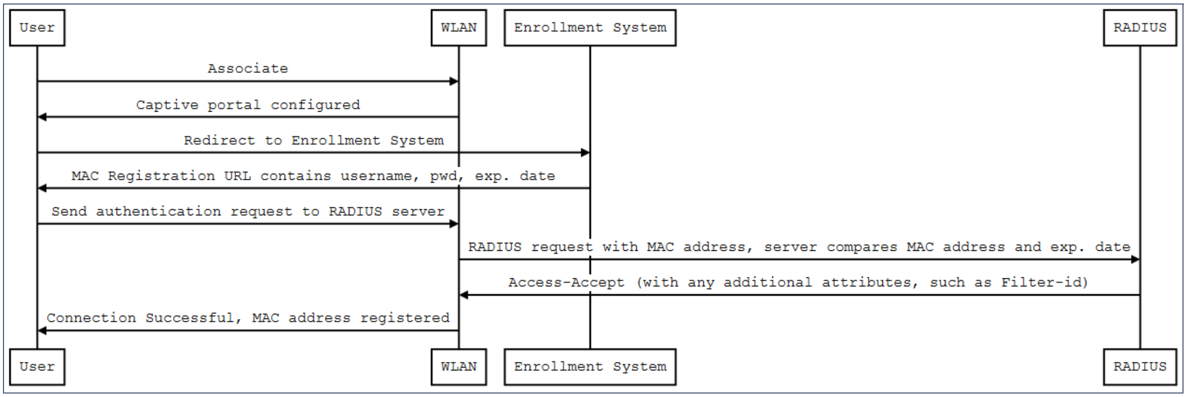
When setting up MAC registration, a list of authorized MAC addresses is maintained on the RADIUS server. When a non-802.1X device attempts to connect to the network, the request is forwarded to the RADIUS server, where the device is checked against the list of authorized MAC addresses. If the registration is not expired, the RADIUS server authenticates the device and sends a redirect URL, which points to the Cloudpath Enrollment System (ES) for onboarding to the secure network.

This document describes how to configure Cloudpath and a Wireless LAN Controller to support MAC Registration.

MAC Registration Process

In this example, the user attempts to access the Internet, is redirected to the captive portal on Cloudpath and proceeds through the enrollment workflow, during which, the user is prompted for information.

FIGURE 1. MAC Registration Sequence


User
WLAN
Enrollment System
RADIUS
Associate
Captive portal configured
Redirect to Enrollment System
MAC Registration URL contains username, pwd, exp. date
Send authentication request to RADIUS server
RADIUS request with MAC address, server compares MAC address and exp. date
Access-Accept (with any additional attributes, such as Filter-id)
Connection Successful, MAC address registered
User
WLAN
Enrollment System
RADIUS

At the MAC registration step, Cloudpath sends a registration URL to the client for use in the RADIUS authentication request. The registration URL contains the username, password, and validity period for the MAC registration.

The access point obtains the MAC address of the user device and sends this information in the RADIUS request to the RADIUS server. The RADIUS server compares the MAC address and expiration date with existing user information. If the validity period and expiration period matches, the RADIUS server authorizes the authentication and returns an Access-Accept to the access point. If other RADIUS attributes are configured, such as the Filter-Id, they are returned with the Access-Accept.

Subsequent access requests from the user to the access point cause the AP to open the firewall to allow access to the Internet. This occurs until the validity period expires and the user must re-enroll.

Configuring Ruckus Controllers for MAC Registration

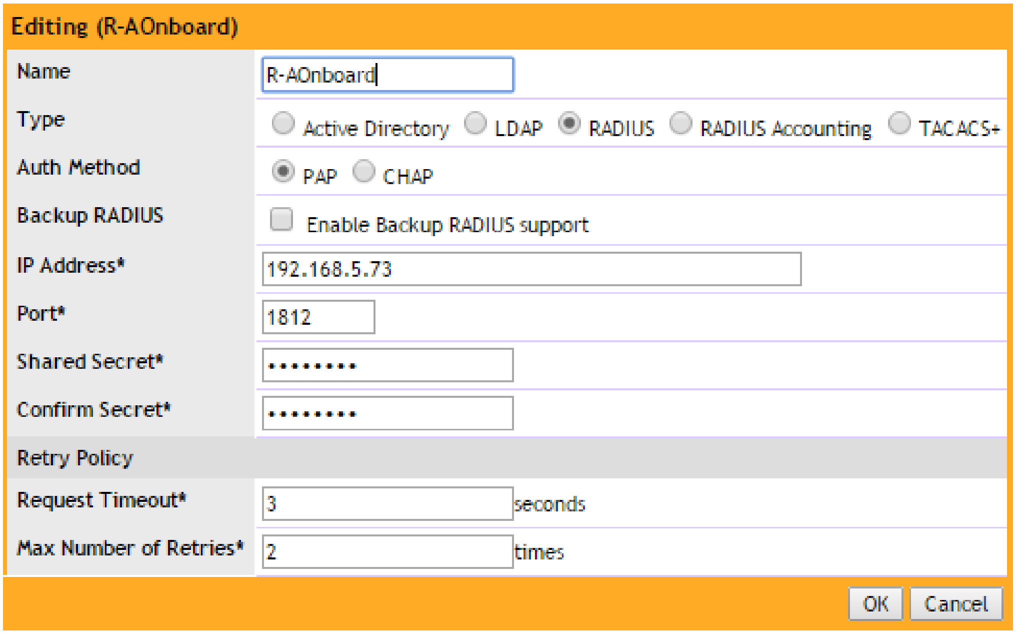
This section describes how to configure the Ruckus Zone Director and SmartZone controllers for MAC registration, authenticating devices against a RADIUS server.

If your environment uses Cisco controllers, see “Configuring a Cisco Controller for MAC Registration” on page 21.

Set up Cloudpath as an AAA Authentication Server

Create AAA authentication and accounting servers for Cloudpath onboard RADIUS server. The following images show this configuration on the Ruckus Zone Director and SmartZone controllers.

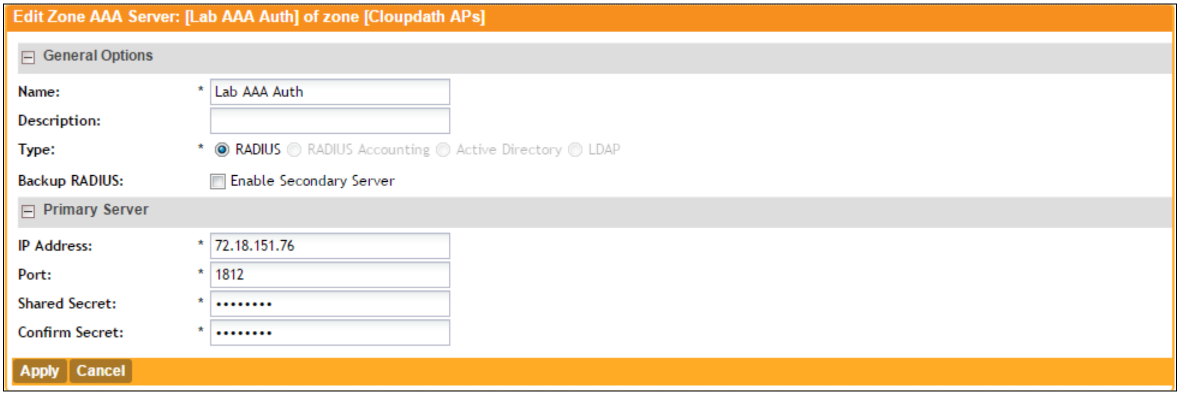
FIGURE 2. Create AAA Authentication Server on Zone Director



Editing (R-AOnboard)

Name	R-AOnboard
Type	○ Active Directory ○ LDAP ● RADIUS ○ RADIUS Accounting ○ TACACS+
Auth Method	● PAP ○ CHAP
Backup RADIUS	□ Enable Backup RADIUS support
IP Address*	192.168.5.73
Port*	1812
Shared Secret*	••••••••
Confirm Secret*	••••••••
Retry Policy	
Request Timeout*	3 seconds
Max Number of Retries*	2 times

FIGURE 3. Create AAA Authentication Server SmartZone



Edit Zone AAA Server: [Lab AAA Auth] of zone [Cloudpath APs]

⊟ General Options

Name: *	Lab AAA Auth
Description:	
Type: *	● RADIUS ○ RADIUS Accounting ○ Active Directory ○ LDAP
Backup RADIUS:	□ Enable Secondary Server

⊟ Primary Server

IP Address: *	72.18.151.76
Port: *	1812
Shared Secret: *	••••••••
Confirm Secret: *	••••••••

Enter the following values for the **Authentication** Server:

1. Name
2. Type = RADIUS
3. Auth Method = PAP
4. IP address = The IP address of the Cloudpath system.

5. Port = 1812
6. Shared Secret = This must match the shared secret for Cloudpath onboard RADIUS server. (*Configuration > Advanced > RADIUS Server*).
7. Leave the default values for the remaining fields.

Create AAA Accounting Server (Optional)

Use the same process to create the AAA Accounting Server.

Enter the following values for the **Accounting** Server:

1. Name
2. Type = RADIUS
3. Auth Method = PAP
4. IP address = The IP address of the Cloudpath system.
5. Port = 1813

> **Note >>**
> The Authentication server uses port 1812. The Accounting server uses port 1813.

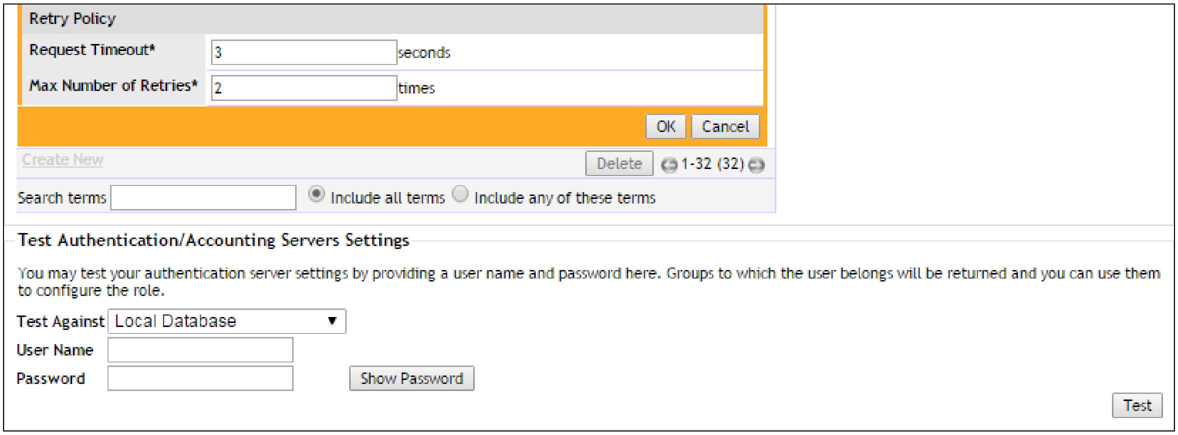
6. Shared Secret = This must match the shared secret for Cloudpath onboard RADIUS server. (*Configuration > Advanced > RADIUS Server*).
7. Leave the default values for the remaining fields.

Run Authentication Test

You can test the connection between the controller and Cloudpath RADIUS server.

At the bottom of the AAA server page, there is a section called Test Authentication/Accounting Servers Settings.

FIGURE 4. Authentication Test Zone Director



Retry Policy

Request Timeout* 3 seconds

Max Number of Retries* 2 times

OK Cancel

Create New Delete 1-32 (32)

Search terms ● Include all terms ○ Include any of these terms

Test Authentication/Accounting Servers Settings

You may test your authentication server settings by providing a user name and password here. Groups to which the user belongs will be returned and you can use them to configure the role.

Test Against Local Database ▼

User Name

Password Show Password

Test

Enter a test User Name and Password and click the Test button on the bottom right of the page.

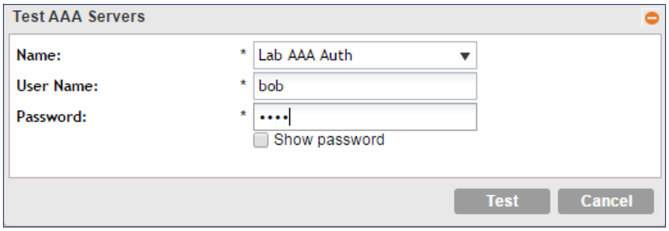
If you receive:

Failed! Invalid username or password

This means that connectivity was established.

On the SmartZone controller, you are prompted to Test Authentication when you save a configuration for an AAA Authentication server.

FIGURE 5. Authentication Test SmartZone



Test AAA Servers

Name: * Lab AAA Auth ▼

User Name: * bob

Password: * ••••

□ Show password

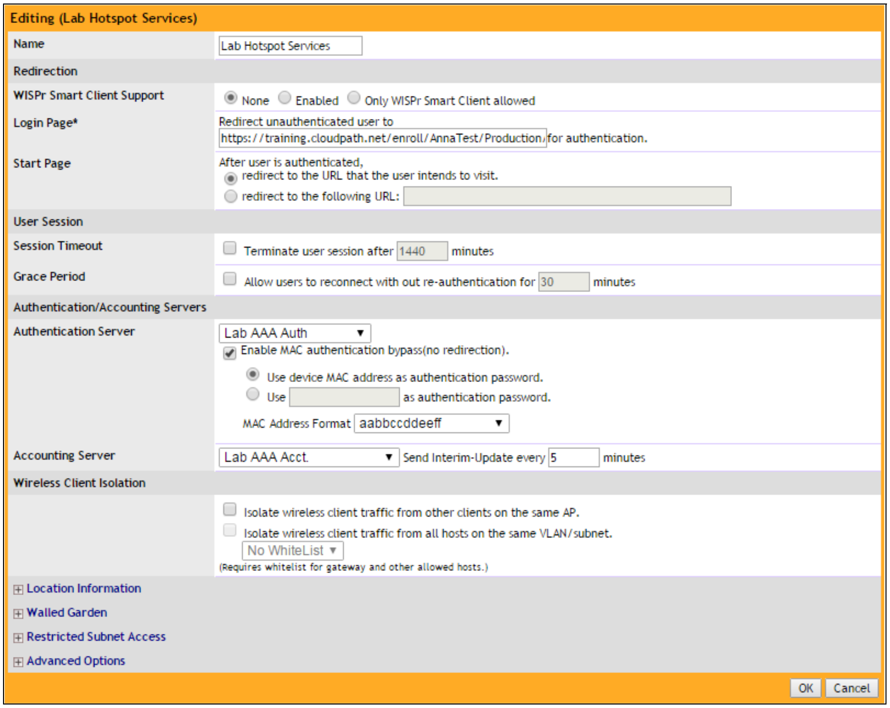
Test Cancel

Create Hotspot Services

Enter the following values for the **Hotspot Service**:

1. Navigate to Hotspot Services (Hotspot WISPr on SmartZone).
2. Name the Hotspot Service.

FIGURE 6. Create Hotspot Service on Zone Director



Editing (Lab Hotspot Services)

Name	Lab Hotspot Services
Redirection	
WISPr Smart Client Support	● None ○ Enabled ○ Only WISPr Smart Client allowed
Login Page*	Redirect unauthenticated user to https://training.cloudpath.net/enroll/AnnaTest/Production for authentication.
Start Page	After user is authenticated, ● redirect to the URL that the user intends to visit. ○ redirect to the following URL:
User Session	
Session Timeout	□ Terminate user session after 1440 minutes
Grace Period	□ Allow users to reconnect with out re-authentication for 30 minutes
Authentication/Accounting Servers	
Authentication Server	Lab AAA Auth ▾ ☑ Enable MAC authentication bypass(no redirection). ● Use device MAC address as authentication password. ○ Use as authentication password. MAC Address Format aabbccddeeff ▾
Accounting Server	Lab AAA Acct. ▾ Send Interim-Update every 5 minutes
Wireless Client Isolation	
	□ Isolate wireless client traffic from other clients on the same AP. □ Isolate wireless client traffic from all hosts on the same VLAN/subnet. No WhiteList ▾ (Requires whitelist for gateway and other allowed hosts.)

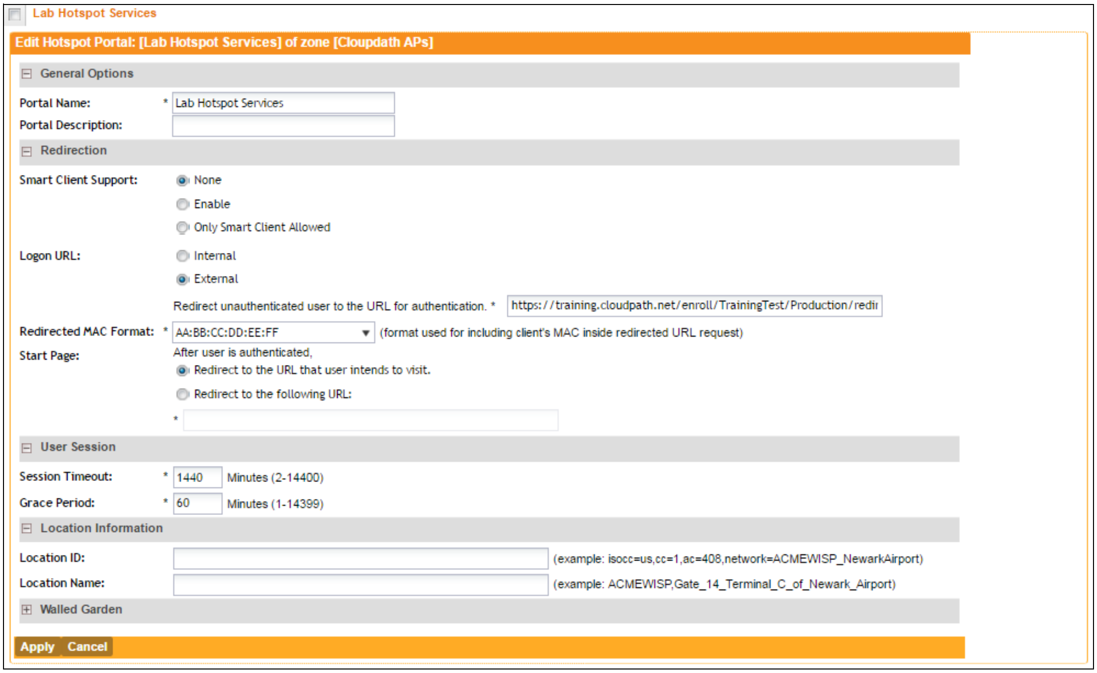
⊞ Location Information

⊞ Walled Garden

⊞ Restricted Subnet Access

⊞ Advanced Options

FIGURE 7. Create Hotspot WISPr on SmartZone



□ Lab Hotspot Services

Edit Hotspot Portal: [Lab Hotspot Services] of zone [Cloudpath APs]

⊟ General Options

Portal Name: * Lab Hotspot Services

Portal Description:

⊟ Redirection

Smart Client Support: ● None ○ Enable ○ Only Smart Client Allowed

Logon URL: ○ Internal ● External

Redirect unauthenticated user to the URL for authentication. * https://training.cloudpath.net/enroll/TrainingTest/Production/redir

Redirected MAC Format: * AA:BB:CC:DD:EE:FF (format used for including client's MAC inside redirected URL request)

Start Page: After user is authenticated,
● Redirect to the URL that user intends to visit.
○ Redirect to the following URL:
*

⊟ User Session

Session Timeout: * 1440 Minutes (2-14400)

Grace Period: * 60 Minutes (1-14399)

⊟ Location Information

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

Location Name: (example: ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport)

⊞ Walled Garden

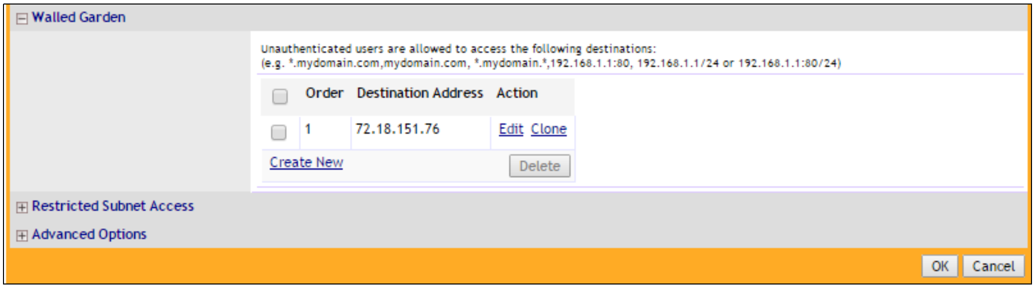
3. Point the unauthenticated user to the Cloudpath redirect URL. Enter the WLAN Redirect URL, which can be found on the Cloudpath Admin UI Configure > Deploy page.
4. Check Redirect to the URL that the user intends to visit.
5. Select the Cloudpath RADIUS Authentication Server (ZoneDirector only).
6. Enable MAC authentication bypass redirection (ZoneDirector only).
7. Select Use device MAC address as authentication password.
8. Select the Cloudpath RADIUS Accounting Server (ZoneDirector only).
9. Leave the defaults for the remaining settings. Click OK.

Set Up the Walled Garden

Enter the following values for the Walled Garden:

1. On the *Hotspot Service* > *Configure* page, scroll to the bottom to the **Walled Garden** section below the Hotspot Service configuration created in the previous section.

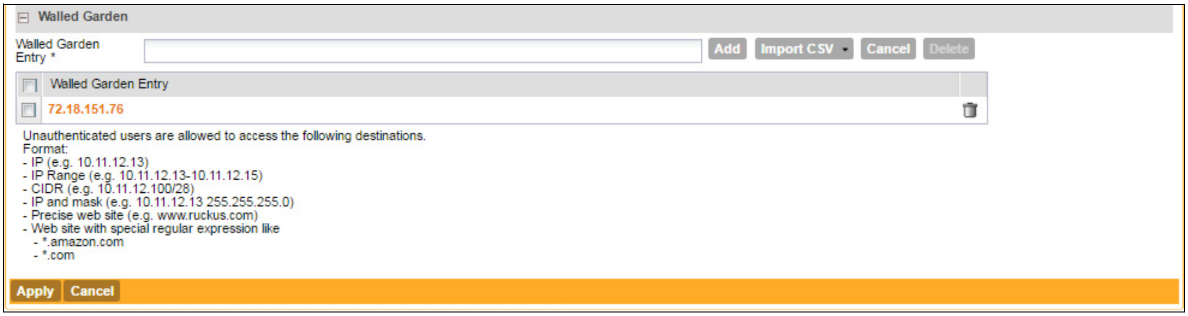
FIGURE 8. Walled Garden Configuration for Zone Director



Unauthenticated users are allowed to access the following destinations:
(e.g. *.mydomain.com,mydomain.com, *.mydomain.*,192.168.1.1:80, 192.168.1.1/24 or 192.168.1.1:80/24)

□	Order	Destination Address	Action
□	1	72.18.151.76	Edit Clone

FIGURE 9. Walled Garden Configuration for SmartZone



□	Walled Garden Entry
□	72.18.151.76

Unauthenticated users are allowed to access the following destinations.
Format:
- IP (e.g. 10.11.12.13)
- IP Range (e.g. 10.11.12.13-10.11.12.15)
- CIDR (e.g. 10.11.12.100/28)
- IP and mask (e.g. 10.11.12.13 255.255.255.0)
- Precise web site (e.g. www.ruckus.com)
- Web site with special regular expression like
  - *.amazon.com
  - *.com

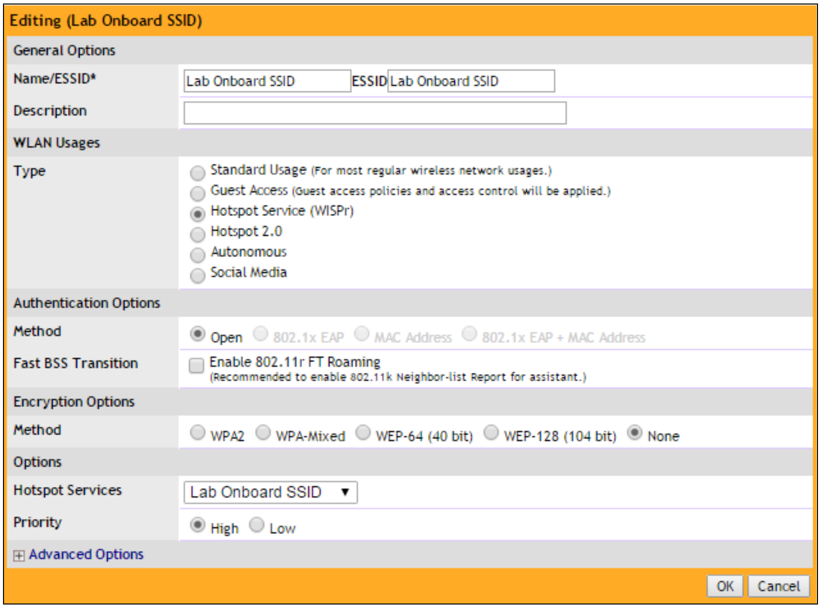
2. Include the DNS or IP address of the Cloudpath system and **Save** (or Apply)

Create the Onboarding SSID

Enter the following values for the onboarding SSID:

1. Name the SSID.
2. Type=Hotspot Service (WISPr).

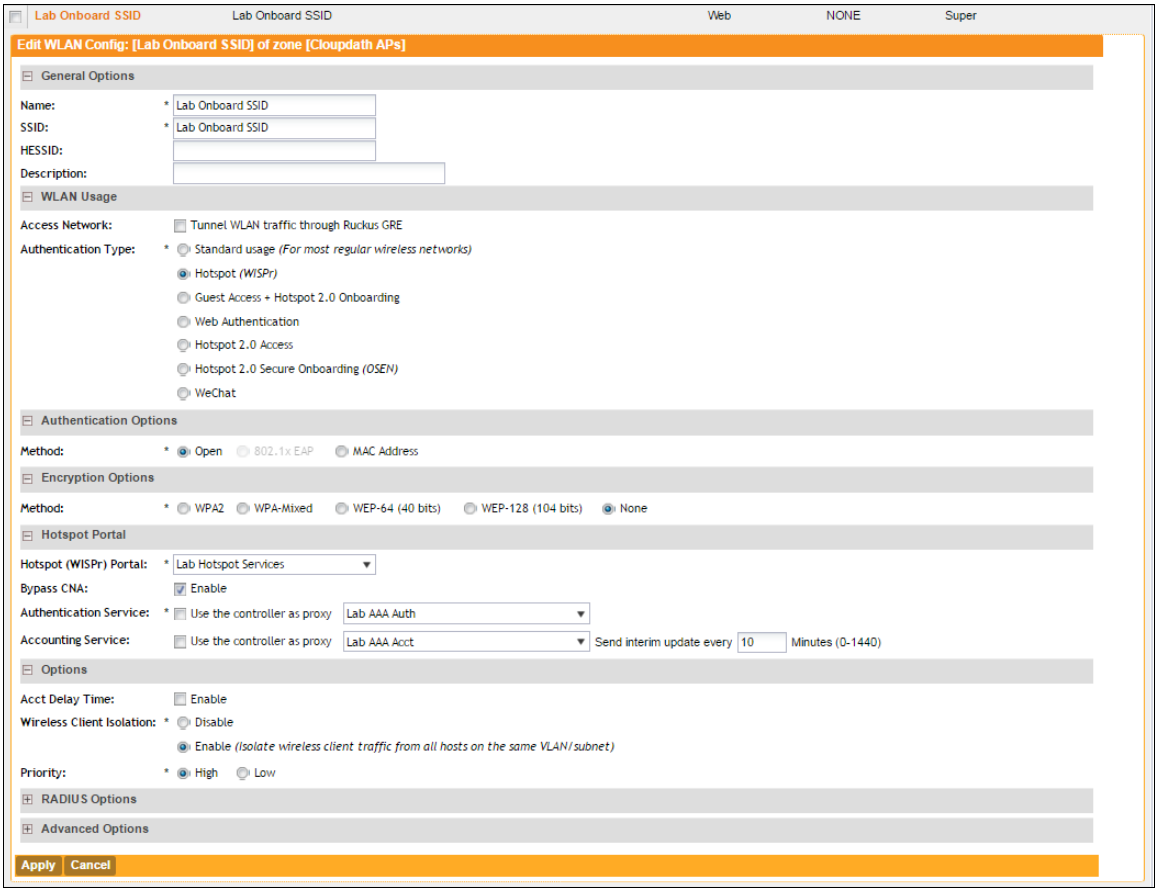
FIGURE 10. Onboarding SSID Configuration on Zone Director



Editing (Lab Onboard SSID)

General Options	
Name/ESSID*	Lab Onboard SSID ESSID Lab Onboard SSID
Description	
WLAN Usages	
Type	○ Standard Usage (For most regular wireless network usages.) ○ Guest Access (Guest access policies and access control will be applied.) ● Hotspot Service (WISPr) ○ Hotspot 2.0 ○ Autonomous ○ Social Media
Authentication Options	
Method	● Open ○ 802.1x EAP ○ MAC Address ○ 802.1x EAP + MAC Address
Fast BSS Transition	□ Enable 802.11r FT Roaming (Recommended to enable 802.11k Neighbor-list Report for assistant.)
Encryption Options	
Method	○ WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ● None
Options	
Hotspot Services	Lab Onboard SSID ▼
Priority	● High ○ Low
⊞ Advanced Options	

FIGURE 11. Onboarding SSID Configuration on SmartZone



☐ Lab Onboard SSID Lab Onboard SSID Web NONE Super

Edit WLAN Config: [Lab Onboard SSID] of zone [Cloudpath APs]

⊟ General Options

Name: * Lab Onboard SSID

SSID: * Lab Onboard SSID

HESSID:

Description:

⊟ WLAN Usage

Access Network: ☐ Tunnel WLAN traffic through Ruckus GRE

Authentication Type: * ○ Standard usage *(For most regular wireless networks)*
● Hotspot *(WISPr)*
○ Guest Access + Hotspot 2.0 Onboarding
○ Web Authentication
○ Hotspot 2.0 Access
○ Hotspot 2.0 Secure Onboarding *(OSEN)*
○ WeChat

⊟ Authentication Options

Method: * ● Open ○ 802.1x EAP ○ MAC Address

⊟ Encryption Options

Method: * ○ WPA2 ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ● None

⊟ Hotspot Portal

Hotspot (WISPr) Portal: * Lab Hotspot Services ▼

Bypass CNA: ☑ Enable

Authentication Service: * ☐ Use the controller as proxy Lab AAA Auth ▼

Accounting Service: ☐ Use the controller as proxy Lab AAA Acct ▼ Send interim update every 10 Minutes (0-1440)

⊟ Options

Acct Delay Time: ☐ Enable

Wireless Client Isolation: * ○ Disable
● Enable *(Isolate wireless client traffic from all hosts on the same VLAN/subnet)*

Priority: * ● High ○ Low

⊞ RADIUS Options

⊞ Advanced Options

3. Authentication Option Method=Open.

4. Encryption Option Method=None.

5. Select the Hotspot Service created in Task 2.

6. Enable Bypass CNA.

   - For ZoneDirector, this setting is at the bottom of the screen in the Bypass Apple CNA Feature section. Check the Hotspot service box.
   - For SmartZone, this setting is in the Hotspot Portal Section.

7. Select the Cloudpath RADIUS Authentication Server (SmartZone only).

8. Select the Cloudpath RADIUS Accounting Server (SmartZone only).

9. Leave the defaults for the remaining settings and click OK (or Apply).

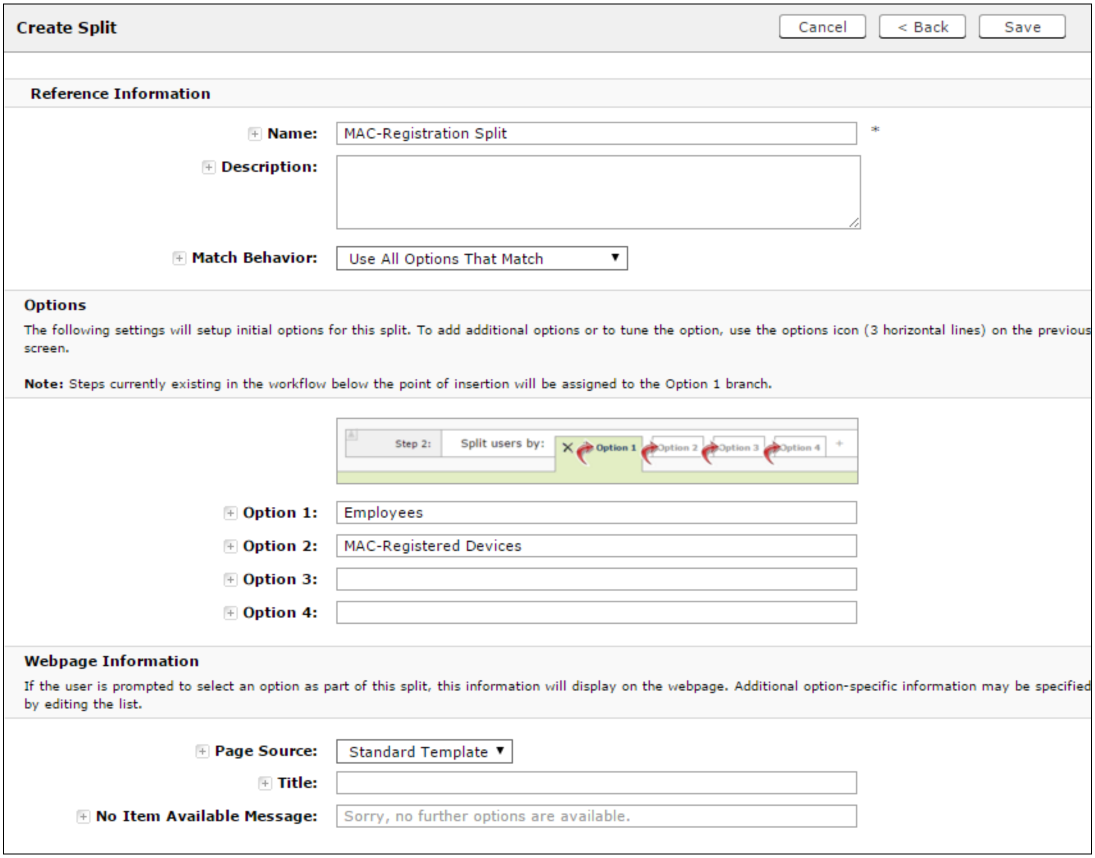
Cloudpath ES Configuration

This section describes how to create a workflow for MAC registration, add RADIUS attributes to a MAC registration configuration, and how to import a file of MAC addresses to a MAC registration list.

Create a MAC Registration Workflow

1. Go to *Configuration > Workflow* and select *Add New Configuration* from the *Configuration* drop-down menu.
2. On the *Create Configuration* page, enter the new workflow information and *Save*.
3. Click *Add* to add a workflow step.
4. Add an *Acceptable Use Policy* for the network.
5. Click the *Insert* arrow to create a step in the enrollment workflow.
6. Add a step to split users into two branches.

FIGURE 12. Create Split



Create Split

Reference Information

Name: MAC-Registration Split *

Description:

Match Behavior: Use All Options That Match

Options

The following settings will setup initial options for this split. To add additional options or to tune the option, use the options icon (3 horizontal lines) on the previous screen.

Note: Steps currently existing in the workflow below the point of insertion will be assigned to the Option 1 branch.

Option 1: Employees

Option 2: MAC-Registered Devices

Option 3:

Option 4:

Webpage Information

If the user is prompted to select an option as part of this split, this information will display on the webpage. Additional option-specific information may be specified by editing the list.

Page Source: Standard Template

Title:

No Item Available Message: Sorry, no further options are available.

7. On the *Create Split* page, in the Options section, enter the names for the two workflow branches. For example, you can name Option 1, *Employees*, and Option 2, *MAC-Registered*.
8. Leave the defaults for the other fields and *Save*. The named branches appear as tabs in the split workflow step.

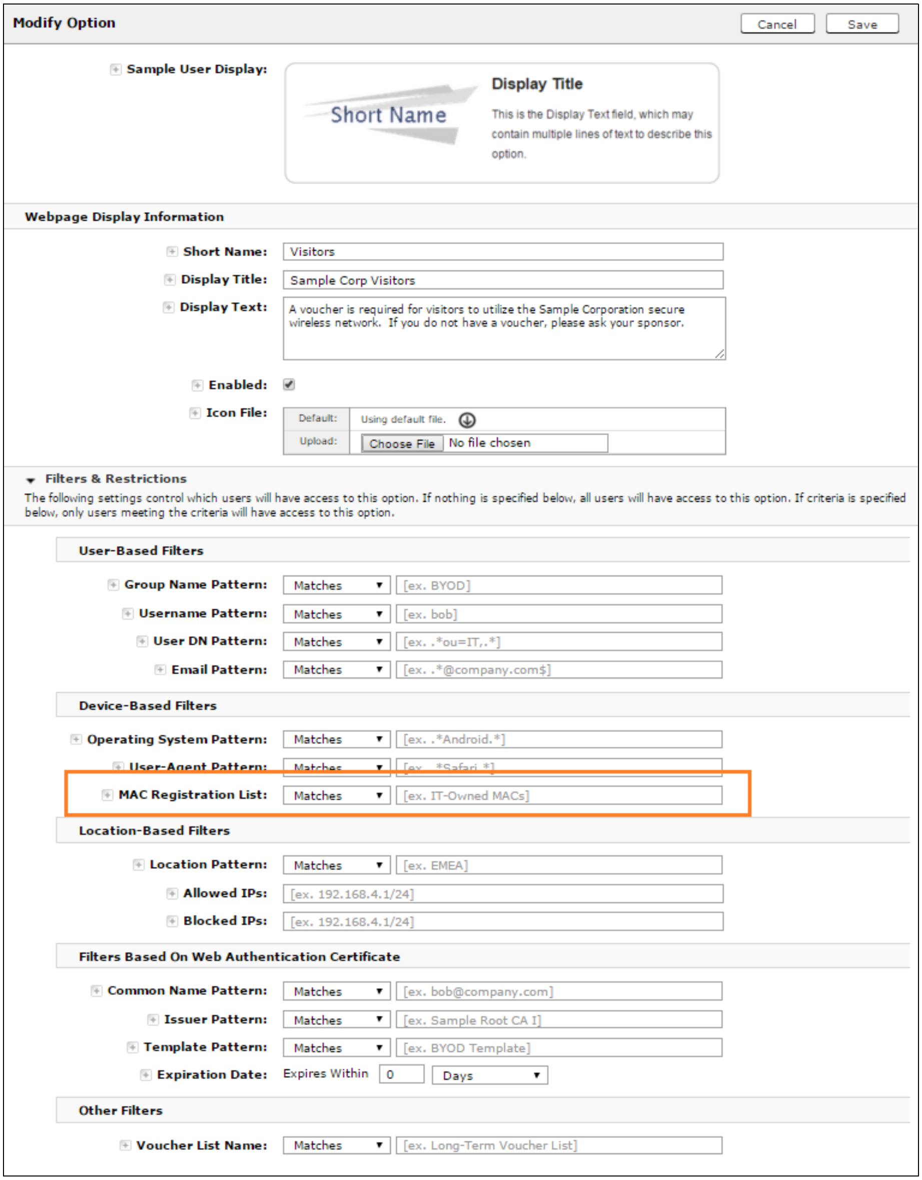
The remaining sections describe how to configure the *MAC Registered* workflow. The *Employees* workflow is configured per your network needs.

How to Create a Filter in the Workflow for MAC-Registered Devices

1. On the workflow page, select the *MAC Registration* tab, created in the previous section, and click the *Edit List* icon ≣ .
2. Edit the *MAC Registration* option.

3. On the *Modify Option* page, open the *Filters and Restrictions* section. in the *MAC Registration List* field, leave the default, *Matches*, and enter the *Name* of the MAC Registration list to use for this workflow. This moves all devices in the specified MAC Registration list to the *MAC Registered* workflow branch.

FIGURE 13. Modify Split Options



Modify Option

Sample User Display:

Short Name

Display Title

This is the Display Text field, which may contain multiple lines of text to describe this option.

Webpage Display Information

Short Name: Visitors

Display Title: Sample Corp Visitors

Display Text: A voucher is required for visitors to utilize the Sample Corporation secure wireless network. If you do not have a voucher, please ask your sponsor.

Enabled: ☑

Icon File: Default: Using default file. Upload: Choose File No file chosen

Filters & Restrictions

The following settings control which users will have access to this option. If nothing is specified below, all users will have access to this option. If criteria is specified below, only users meeting the criteria will have access to this option.

User-Based Filters

Group Name Pattern: Matches [ex. BYOD]

Username Pattern: Matches [ex. bob]

User DN Pattern: Matches [ex. .*ou=IT,.*]

Email Pattern: Matches [ex. .*@company.com$]

Device-Based Filters

Operating System Pattern: Matches [ex. .*Android.*]

User-Agent Pattern: Matches [ex. .*Safari.*]

MAC Registration List: Matches [ex. IT-Owned MACs]

Location-Based Filters

Location Pattern: Matches [ex. EMEA]

Allowed IPs: [ex. 192.168.4.1/24]

Blocked IPs: [ex. 192.168.4.1/24]

Filters Based On Web Authentication Certificate

Common Name Pattern: Matches [ex. bob@company.com]

Issuer Pattern: Matches [ex. Sample Root CA I]

Template Pattern: Matches [ex. BYOD Template]

Expiration Date: Expires Within 0 Days

Other Filters

Voucher List Name: Matches [ex. Long-Term Voucher List]

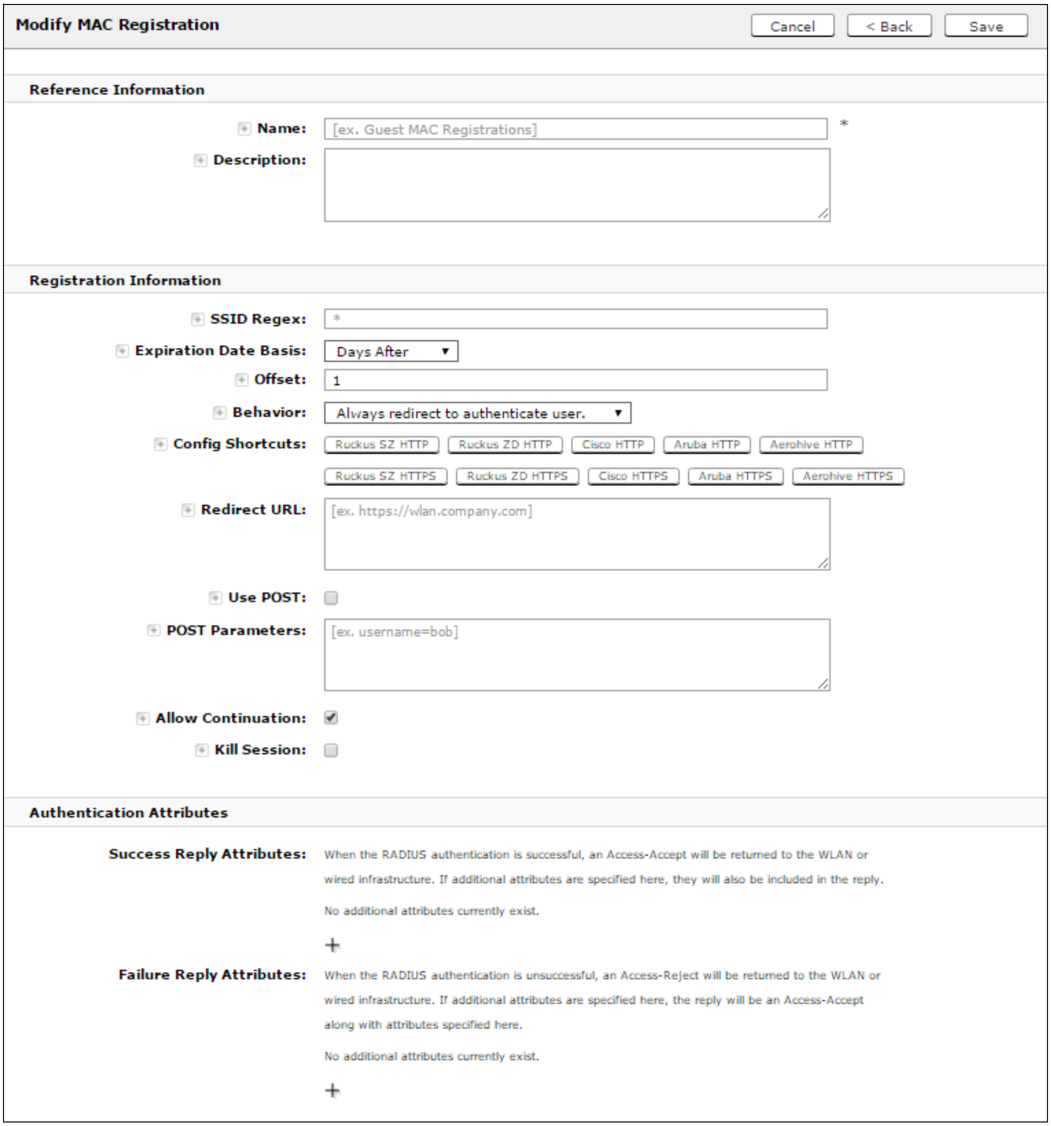
4. *Save* the changes to the option filter.
5. Click *Done* to return to the workflow.

> **Tip >>**
>
> The filter icon ▼ on the *MAC Registration* tab indicates that this option only applies to devices matching the filter criteria. A filter option does not display as a prompt to users during enrollment.

How to Add a MAC Registration Step to the Workflow

1. On the workflow page, click the *Insert* arrow to create a step in the enrollment workflow.
2. Select *Register device for MAC-based authentication*.
3. Create a new registration configuration. The *Create MAC Registration* page opens.

FIGURE 14. Create MAC Registration



Modify MAC Registration

Reference Information

Name: [ex. Guest MAC Registrations] *

Description:

Registration Information

SSID Regex: *

Expiration Date Basis: Days After

Offset: 1

Behavior: Always redirect to authenticate user.

Config Shortcuts:

Redirect URL: [ex. https://wlan.company.com]

Use POST: ☐

POST Parameters: [ex. username=bob]

Allow Continuation: ☑

Kill Session: ☐

Authentication Attributes

Success Reply Attributes: When the RADIUS authentication is successful, an Access-Accept will be returned to the WLAN or wired infrastructure. If additional attributes are specified here, they will also be included in the reply.

No additional attributes currently exist.

Failure Reply Attributes: When the RADIUS authentication is unsuccessful, an Access-Reject will be returned to the WLAN or wired infrastructure. If additional attributes are specified here, the reply will be an Access-Accept along with attributes specified here.

No additional attributes currently exist.

4. Enter the *Name* and *Description* for the MAC Registration step.

5. Enter the values in the *Registration Information* section:

- SSID Regex - This is the SSID to which MAC registered devices are assigned.

> **Note >>**
> This field is case sensitive. Separate multiple SSIDs by a vertical pipe (|). The default (*) is any SSID that is pointed at the RADIUS server.

- Expiration Date Basis - The basis for calculating the default validity period for MAC registration.

> **Note >>**
> A sponsor can override the validity period configured for MAC registration. See *Setting Up Sponsored Guest Access Within Cloudpath* guide, located on the Support tab, for details.

- Expiration Date Offset - The number of hours/days/months/etc to be offset from the event date when calculating the registration validity period. If *Specified Date* is selected, this should be the date in YYYY/MM/DD format.
- Behavior - Specifies the prompt and redirect settings for the MAC registration configuration. Use the *Web Page Information* section to configure the user prompt or redirect URL. Behavior settings include:

  -Prompt user when MAC is unknown.

  -Always prompt the user.

  -Redirect when MAC is unknown.

  -Always redirect to authenticate user. (This is the default and the most commonly used setting).

  -Skip registration when MAC is unknown.

- Use the *Config Shortcuts* buttons to populate the *Redirect URL* and *POST Parameters* according to your controller vendor and preferred protocol.
- Allow Continuation - If checked, the submit-redirect call is processed, if unchecked, the submit-redirect call is ignored.
- Kill Session - If checked, the user's session will be killed as they are redirected and, if they return, they will be forced to start over.

Adding RADIUS Attributes

During association, the access point performs a MAC authentication with the RADIUS server. The RADIUS server looks up the MAC address, verifies that it has not expired, and returns an *Access-Accept*. If additional attributes are configured, they are returned with the *Access-Accept*.

1. In the *Authentication Attributes* section, click *Add Attribute* for Successful (or Unsuccessful) Attempts.

2. Enter the *Attribute*, *Operator*, and *Value*. The attribute is added to the MAC Registration configuration.

   For example, to return a Filter-Id for a guest user, enter *Filter-Id* in the Attribute field, and *Guest* in the Value field. If the authentication request is authorized, the RADIUS server returns the *Filter-Id=Guest*, along with the *Access-Accept* attribute to the user device.

   After the registration expires (or if an unregistered MAC address associates to the SSID), the RADIUS server replies with an *AccessReject*. If additional attributes are configured for unsuccessful authentications, they are returned with the *AccessReject*.

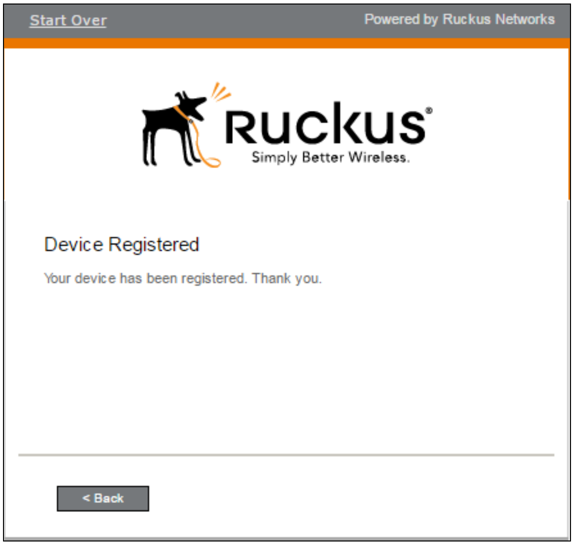
How to Add a Message to Users

As a best practice, add a workflow step to display a message to the user indicating that the authentication was successful.

1. On the workflow page, click the *Insert* arrow to create a step in the enrollment workflow.
2. Select *Display a message*.
3. Create a new message from a standard template. On the *Create New Message* page, enter an appropriate *Title* and *Message*.
4. Uncheck the *Show Continue Button* box. After the message is displayed, the device should be moved to the specified SSID. No user action is required.
5. *Save* the configuration.

> **Tip >>**
> On the workflow page, click the view icon next to the *Display Message* step to see a preview of the message.

FIGURE 15. Example Message to User

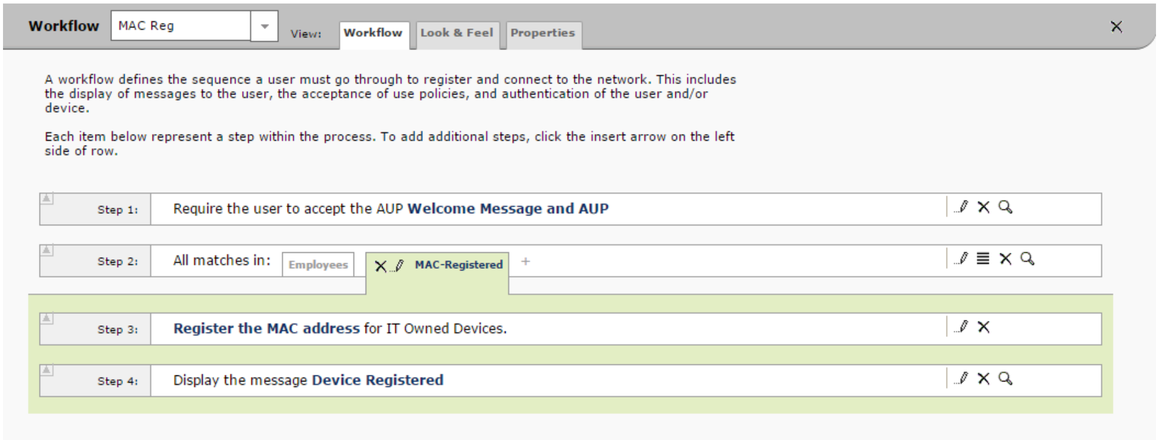


Device Registered

Your device has been registered. Thank you.

The completed workflow is displayed below.

FIGURE 16. Completed Workflow for MAC Registration



A workflow defines the sequence a user must go through to register and connect to the network. This includes the display of messages to the user, the acceptance of use policies, and authentication of the user and/or device.

Each item below represent a step within the process. To add additional steps, click the insert arrow on the left side of row.

Step 1: Require the user to accept the AUP **Welcome Message and AUP**

Step 2: All matches in: Employees | MAC-Registered

Step 3: **Register the MAC address** for IT Owned Devices.

Step 4: Display the message **Device Registered**

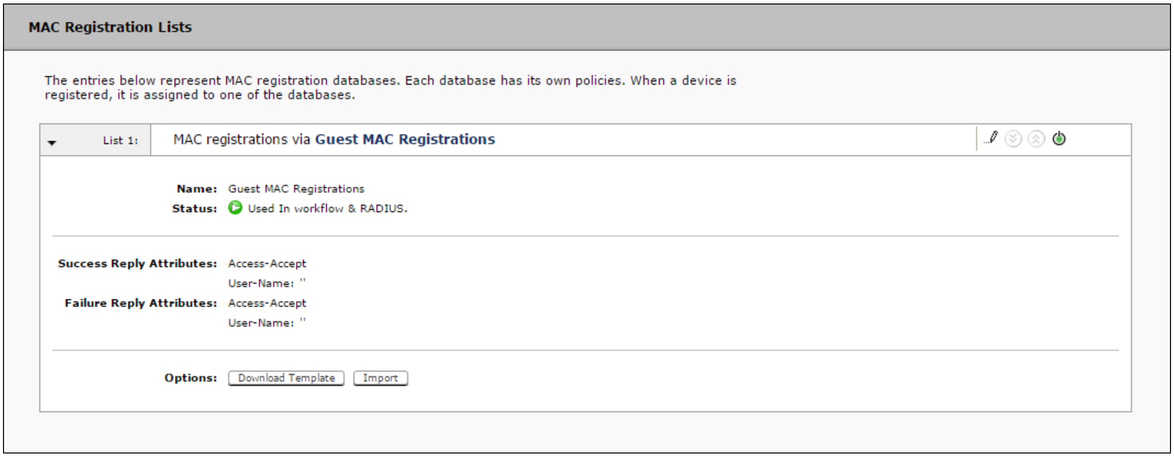
Import MAC Registration List

For IT-owned devices, you might already have a list of MAC Addresses. This section describes how to import that list to be used with the MAC registration workflow.

How to Import a List for MAC Registration

1. Navigate to *Configuration > Advanced > MAC Registrations*.

FIGURE 17. Import MAC Registration List



MAC Registration Lists

The entries below represent MAC registration databases. Each database has its own policies. When a device is registered, it is assigned to one of the databases.

List 1: MAC registrations via **Guest MAC Registrations**

Name: Guest MAC Registrations
Status: Used In workflow & RADIUS.

Success Reply Attributes: Access-Accept
User-Name: ''
Failure Reply Attributes: Access-Accept
User-Name: ''

Options: Download Template | Import

2. Open the MAC Registration list for which you will import a device list.
3. Click *Import*.
4. Browse to select your device list and *Continue*.
5. The file is imported and the device list is added to the MAC Registration list.

The devices on the MAC registration list will meet the filter criteria for the MAC Registered devices split in the workflow and will be registered using the policy set in the MAC Registration configuration.

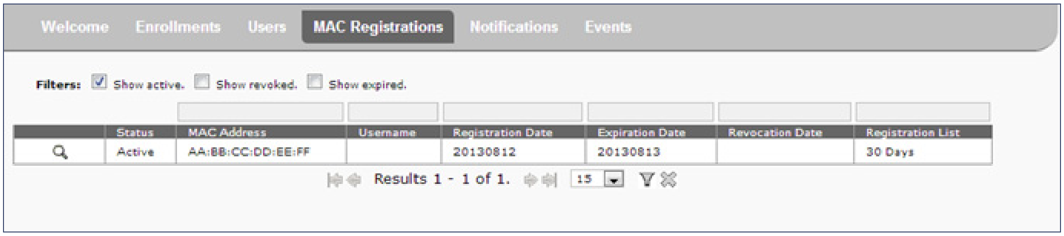
Viewing MAC Registration Records on the Dashboard

Administrators can view the records for devices that have been registered on the network using the MAC address, and, if needed, can revoke the registration.

How to View MAC Registration Records

1. Go to *Operational > Dashboard > MAC Registrations*.
2. The *MAC Registration* table shows the status and validity information for each MAC address. You can view active, expired, and revoked registrations, and sort the registration data using the table filters.
3. Click the view icon to see details.

FIGURE 18. MAC Registrations on the Dashboard



Filters: ☑ Show active. □ Show revoked. □ Show expired.

	Status	MAC Address	Username	Registration Date	Expiration Date	Revocation Date	Registration List
🔍	Active	AA:BB:CC:DD:EE:FF		20130812	20130813		30 Days

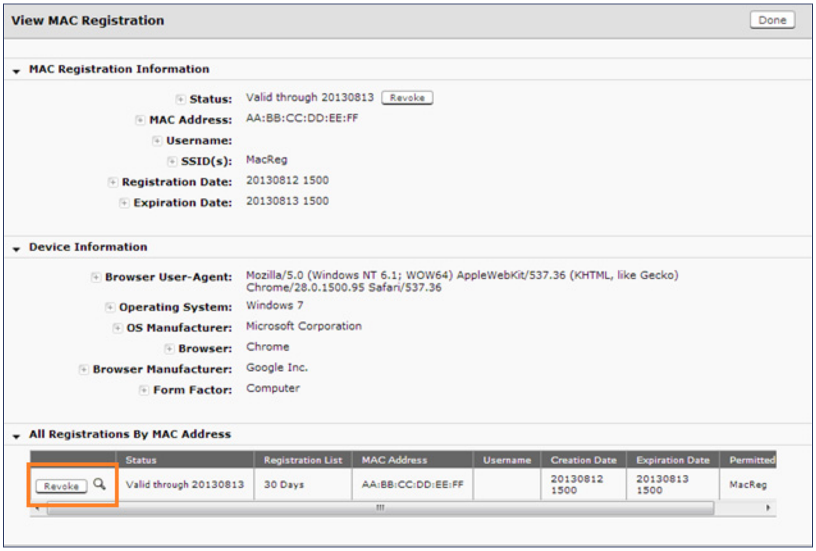
Results 1 - 1 of 1. 15

4. You can also access MAC registration information in the enrollment record. Go to *Operational > Dashboard > Enrollments > View Enrollment Record*.

How to Revoke Access for a MAC-Registered Device

1. Go to *Operational > Dashboard > MAC Registrations*.
2. Click the *View* icon to view the registration information for the device.

FIGURE 19. View MAC Registration Details



MAC Registration Information

Status: Valid through 20130813 Revoke
MAC Address: AA:BB:CC:DD:EE:FF
Username:
SSID(s): MacReg
Registration Date: 20130812 1500
Expiration Date: 20130813 1500

Device Information

Browser User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36
Operating System: Windows 7
OS Manufacturer: Microsoft Corporation
Browser: Chrome
Browser Manufacturer: Google Inc.
Form Factor: Computer

All Registrations By MAC Address

	Status	Registration List	MAC Address	Username	Creation Date	Expiration Date	Permitted
Revoke 🔍	Valid through 20130813	30 Days	AA:BB:CC:DD:EE:FF		20130812 1500	20130813 1500	MacReg

3. In the *All Registrations by MAC Devices* section, click the *Revoke* button next to the device.
4. On the *Revoke* pop-up, list the reason for revocation and click *Revoke*. The MAC address for the device is removed from the list of accepted MAC addresses in the RADIUS server.

Configuring a Cisco Controller for MAC Registration

This section describes how to configure the Cisco Wireless LAN Controller for MAC registration, authenticating devices against a RADIUS server.

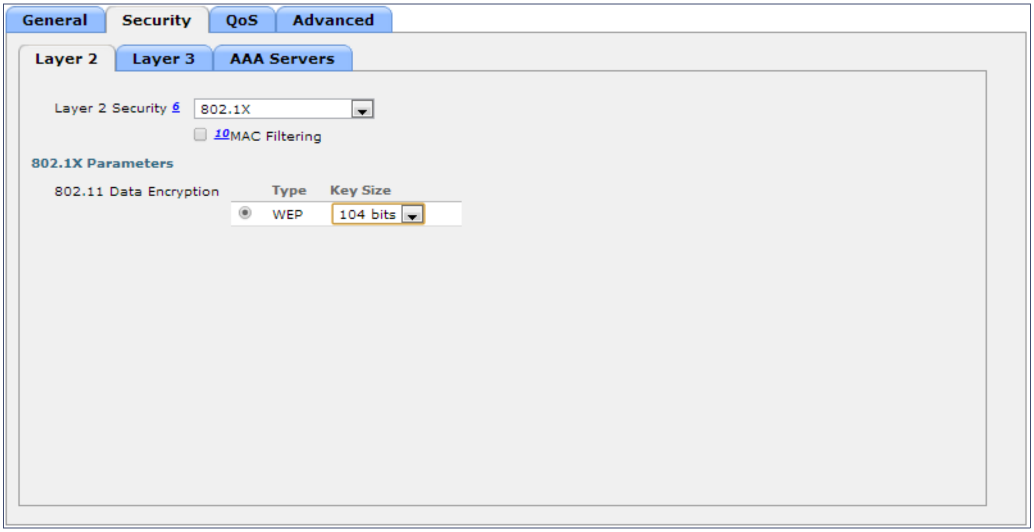
Prerequisites

You must have a RADIUS server defined in the Cisco WLC. From the *WLANs > Edit* window, define the RADIUS server in the *Security > Radius Authentication* window and *Enable* the RADIUS server.

How to Set up MAC Registration

1. On the wireless controller, go to the *WLANs* tab and select the WLAN for MAC registration.
2. Select the *General* tab. In the *Interface/Interface Group* field, select the interface to which the WLAN is mapped.
3. Select *Security > Layer 2* tab.

FIGURE 20. Layer 2 Security



Layer 2 Security 6 802.1X

□ 10MAC Filtering

802.1X Parameters

802.11 Data Encryption		Type	Key Size
	●	WEP	104 bits

4. In the *Layer 2 Security* section:
   - Select *NONE* for an open SSID.
   - Select *WPA+WPA2 +AuthKeyMgmt = PSK* for a PSK SSID.
5. Enable *Mac Filtering*. This enables MAC authentication for the WLAN.

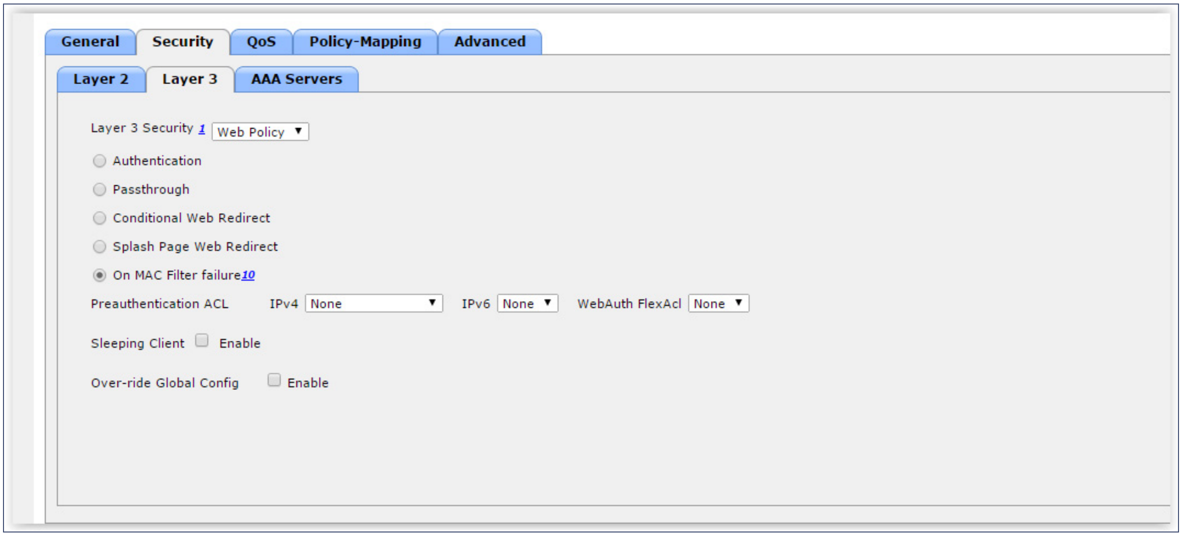
Layer 3 Settings

Layer 2 Mac Filtering - Select to filter clients by MAC address. Locally configure clients by MAC address in the MAC Filters > New page. Otherwise, configure the clients on a RADIUS server.

When using Layer 2 Mac Filtering

Web Policy - On MAC Filter failure - Enables web authentication MAC filter failures.

FIGURE 21. Using Layer 2 Mac Filtering



Layer 3 Security 1 Web Policy ▼

○ Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

● On MAC Filter failure10

Preauthentication ACL IPv4 None ▼ IPv6 None ▼ WebAuth FlexAcl None ▼

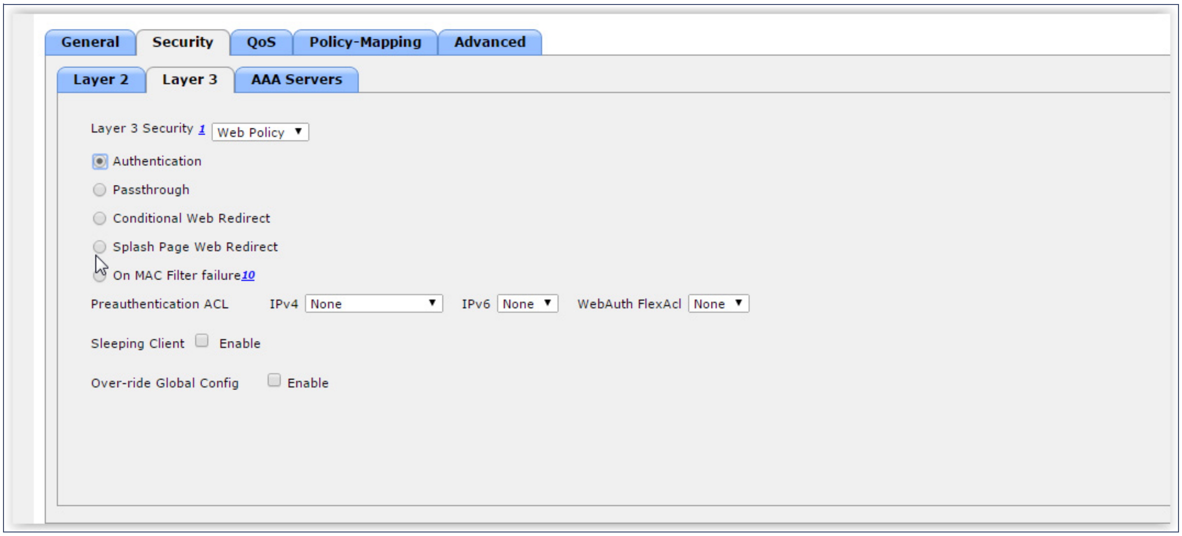
Sleeping Client □ Enable

Over-ride Global Config □ Enable

When NOT using Layer 2 Mac Filtering

Web Policy - Authentication - If you select this option, the user is prompted for username and password while connecting the client to the wireless network.

FIGURE 22. Not Using Layer 2 Mac Filtering



Layer 3 Security 1 Web Policy ▼

● Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

○ On MAC Filter failure10

Preauthentication ACL IPv4 None ▼ IPv6 None ▼ WebAuth FlexAcl None ▼

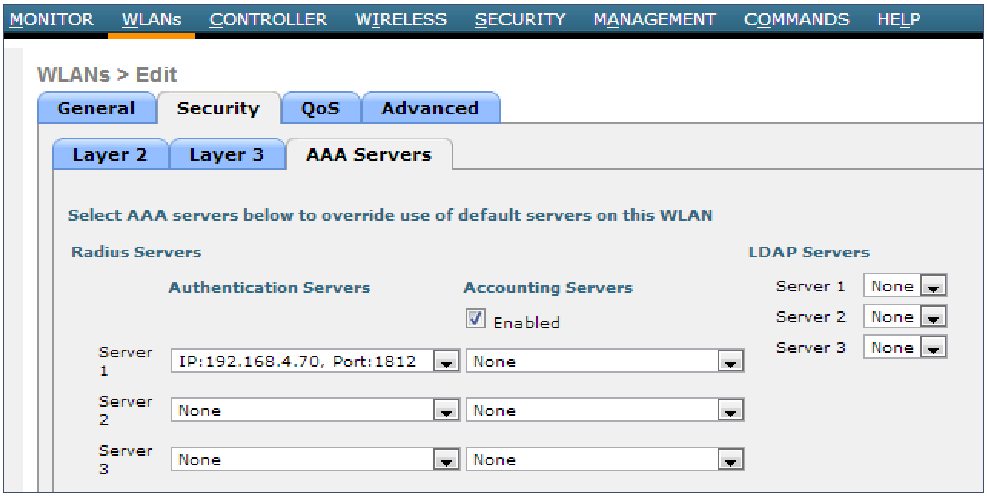
Sleeping Client □ Enable

Over-ride Global Config □ Enable

Select *Security > AAA Servers* tab. In the *Authentication Servers* section, select the RADIUS server that will be used for MAC authentication.

Note >>
If you are using Cloudpath as a RADIUS server, define the ES RADIUS server in the Cisco WLC in the *Security > Radius* Authentication window.

FIGURE 23. Select RADIUS Server



WLANs > Edit

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

Radius Servers

	Authentication Servers	Accounting Servers
		☑ Enabled
Server 1	IP:192.168.4.70, Port:1812	None
Server 2	None	None
Server 3	None	None

LDAP Servers

Server 1	None
Server 2	None
Server 3	None

6. *Apply* changes. The wireless controller is configured for MAC registration against the RADIUS server.