CONFIGURATION GUIDE

Cloudpath Enrollment System MAC Registration Configuration Guide, 5.12

Supporting Cloudpath Software Release 5.12

Part Number: 800-73434-001 Rev A
Publication Date: 05 July 2023

© 2023 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates (“CommScope”). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see https://www.commscope.com/trademarks. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

What's New in This Document **5**

Overview **7**

MAC Registration Process **9**

Configuring Ruckus Controllers for MAC Registration **11**

Configuring Virtual SmartZone 11

Setting up Cloudpath as an AAA RADIUS Authentication Server 11

Creating AAA RADIUS Accounting Server (Optional) 11

Testing AAA Servers 12

Creating a Hotspot (WISPr) Portal 12

Setting Up the Walled Garden 12

Creating the Onboarding SSID 13

Configuring Unleashed 13

Setting up Cloudpath as an AAA RADIUS Authentication Server 14

Creating AAA Accounting Server (Optional) 14

Testing AAA Servers 14

Creating a Hotspot (WISPr) Portal 14

Setting Up the Walled Garden 15

Creating the Onboarding SSID 16

Configuring ZoneDirector 16

Setting up Cloudpath as an AAA RADIUS Authentication Server 16

Creating AAA RADIUS Accounting Server (Optional) 16

Testing AAA Servers 17

Creating a Hotspot (WISPr) Portal 17

Setting Up the Walled Garden 17

Creating the Onboarding SSID 18

Configuring Policies **19**

Configuring MAC Registration Lists in the Cloudpath UI **23**

Adding a New MAC Registration Configuration 23

Importing a MAC Registration List 29

Importing Individual MAC Addresses 30

Removing a MAC Registration Configuration List or Its MAC Addresses 30

Adding and Viewing MAC OUI Wildcards 31

Adding Policies to a MAC Registration List **37**

Steps to Add Policies 37

Policy Rules 38

Additional Policy Information **39**

Testing Policies 39

Test Policy Evaluation - Example 1 39

Test Policy Evaluation - Example 2 41

Test Policy Evaluation - Example 3 43

Viewing Policy Information 44

Viewing RADIUS Attribute Information 45

Switching Pre-Release-5.9R4 MAC Registration Lists to Policy-Assigned MAC Registration Lists....47

Creating a MAC Registration Workflow....51

Viewing MAC Registration Records on the Dashboard....55

How to View MAC Registration Records....55

How to Revoke Access for a MAC-Registered Device....55

Configuring a Cisco Controller for MAC Registration....57

What's New in This Document

TABLE 1 Key Features and Enhancements in Cloudpath 5.12 (July 05, 2023)

Feature	Description	Reference
MAC Address OUI Wildcard Registration	**New:** OUI Registration for MAC registration lists lets you add, view, or delete a MAC OUI (Organizationally Unique Identifier) wildcard definitions. MAC OUI wildcards allow for all devices that match the OUI pattern prefix to authenticate via the Mac Registration List without the need for manual entry of individual device MAC addresses.	• Configuring MAC Registration Lists in the Cloudpath UI on page 23
Minor editorial updates	**Updated:** Minor editorial updates were made throughout the Configuration Guide.	All chapters
Updates to address defects	**Updated:** Minor updates on content throughout to address defects.	All chapters

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 MAC address of the device to allow limited, secure network access.

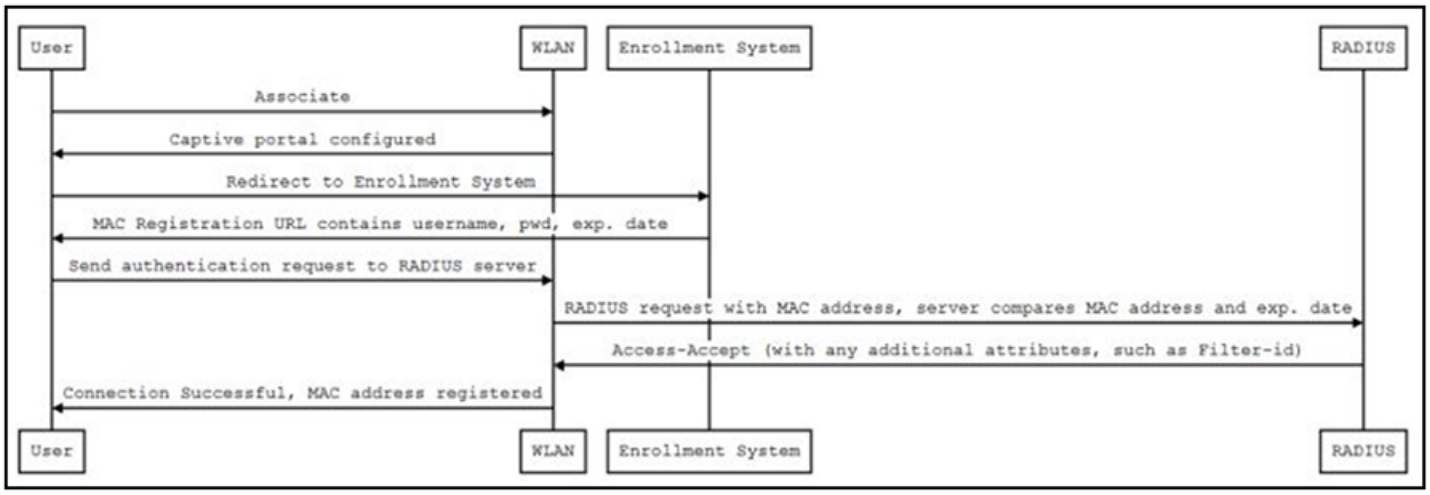
When setting up MAC registration, a list of authorized MAC addresses is maintained on the RADIUS server. When a non-802.1X device attempts to connect to the network, the request is forwarded to the RADIUS server, where the device is checked against the list of authorized MAC addresses. If the registration 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



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

- Configuring Virtual SmartZone..... 11
- Configuring Unleashed..... 13
- Configuring ZoneDirector..... 16

This section describes how to configure RUCKUS Virtual SmartZone, RUCKUS Unleashed, and RUCKUS ZoneDirector for MAC registration for authenticating devices against a RADIUS server. The information provided here is specific to integrating Cloudpath with one of these controllers.

Consult your controller documentation for more information.

If your environment uses Cisco controllers, see Configuring a Cisco Controller for MAC Registration on page 57.

Configuring Virtual SmartZone

This section includes tables of configuration fields and values for setting up the Vitrual SmartZone (vSmartZone) Controller. For more information, such as how to navigate the vSmartZone UI, how to find more information about configuration fields, and to view screen shots of the vSmartZone UI, refer to the *RUCKUS SmartZone 300 and Virtual SmartZone-High Scale Administrator Guide*.

NOTE
For any configuration fields that are not described in the following sections, you can use their default values.

Setting up Cloudpath as an AAA RADIUS Authentication Server

TABLE 2 Fields/Values to Use for vSmartZone AAA Authentication Service

AAA Authentication Service Section in vSmartZone UI	Configuration Field and Corresponding Value
General Options	Name: Any descriptive name for the AAA authentication service
	Type: RADIUS
Primary Server	IP Address: The IP address of the Cloudpath Enrollment System.
	Port: 1812 is typically used and is the default.
	Shared Secret: This must match the shared secret for the Cloudpath ES onboard RADIUS server (**Configuration > RADIUS Server**).
	Confirm Secret: The shared secret (entered again).

Creating AAA RADIUS Accounting Server (Optional)

TABLE 3 Fields/Values to Use for SmartZone AAA Accounting Service

AAA Accounting Service Section in vSmartZone UI	Configuration Field and Corresponding Value
General Options	Name: Any descriptive name for the AAA accounting service
	Type: RADIUS ACCOUNTING

TABLE 3 Fields/Values to Use for SmartZone AAA Accounting Service (continued)

AAA Accounting Service Section in vSmartZone UI	Configuration Field and Corresponding Value
Primary Server	IP Address: The IP address of the Cloudpath Enrollment System.
	Port: 1813 is typically used and is the default.
	Shared Secret: This must match the shared secret for the Cloudpath ES onboard RADIUS server (**Configuration > RADIUS Server**).
	Confirm Secret: The shared secret (entered again).

Testing AAA Servers

To test the connection between the controller and the Cloudpath RADIUS server, RUCKUS strongly recommends testing the AAA server after you set it up. Refer to the instructions in the *RUCKUS SmartZone 300 and Virtual SmartZone-High Scale Administrator Guide*.

Creating a Hotspot (WISPr) Portal

TABLE 4 Fields/Values to Use for Creating a Hotspot (WISPr) Portal

Creating a Hotspot (WISPr) Portal section in vSmartZone UI	Configuration Field and Corresponding Value
General Options	Portal Name: Any descriptive name for the hotspot portal.
Redirection	Login URL: Select "External."
	Redirect unauthenticated user: The Cloudpath Enrollment Portal URL, which should be contained in the applicable workflow in the Cloudpath UI (**Configuration > Workflows**).
	Start Page: After user is authenticated,: Select "Redirect to the URL that the user intends to visit." This lets you set a different page where users will be redirected (for example, your company website). Enter a domain name or an IP address for the redirection.

Setting Up the Walled Garden

To add a walled garden configuration to your existing Hotspot Services, refer to the instructions in the *RUCKUS SmartZone 300 and Virtual SmartZone-High Scale Administrator Guide*.

Also, when configuring the walled garden, include the following steps:

1. Include the DNS or IP address of the Cloudpath system, then click **OK**
2. Optionally, there are some domains that you can add to the walled garden on all controllers to:
   - Prevent the Apple CNA mini-browser from appearing on Apple devices.
   - Avoid being blocked or slowed when attempting to download the Cloudpath wizard.

     NOTE
     There will still be about a 15-to-20-second delay when the full application is 33 percent complete (about 40 MB) in its download.

     The recommended destinations to add for the walled garden are:

```
*.ggpht.com
*.play.googleapis.com
*.googleapis.com
*.play.google.com
android.clients.google.com
*.gvt1.com
```

```
connectivitycheck.android.com
connectivitiycheck.google.com
*.gstatic.com
*.clients3.google.com
*.thawte.com
```

NOTE

The *thawte.com destination is the OCSP URL of the SSL certificate of the Cloudpath server. This URL can be found by clicking the *lock* icon in your web browser and viewing the details of your certificate.

3. If you are still experiencing issues, you can try adding the following destinations to the walled garden:

```
*.clients.google.com
*.l.google.com
*.googleusercontent.com
*.appengine.google.com
*.cloud.google.com
*.android.com
*.cloudfront.net
*.akamaihd.net
172.217.0.0/16
216.58.0.0/16
```

Creating the Onboarding SSID

TABLE 5 Fields/Values to Use for SmartZone Onboarding SSID

Creating a WLAN Configuration (for Onboarding SSID) section in vSmartZone UI	Configuration Field and Corresponding Value
General Options	Name: Name of the SSID
	SSID: Name of the WLAN
	Zone: Zone in which the WLAN will reside
	WLAN Group: Group in which the WLAN will reside
Authentication Options	Authentication Type: Hotspot (WISPr)
	Method: MAC Address
	MAC Authentication: Unchecked
	MAC Address Format: Recommended format is AA:BB:CC:DD:EE:FF
Encryption options	Method: None
Hotspot Portal	Hotspot (WISPr) Portal: Drop-down list to selet the already-created hotspot service.
	Bypass CNA: Enable
	Authentication Server: Drop-down list to select the Cloudpath RADIUS Authentication Server
	Accounting Server: Drop-down list to select the Cloudpath RADIUS Accounting Server

Configuring Unleashed

This section includes tables of configuration fields and values for setting up the RUCKUS Unleashed platform. For more information, such as how to navigate the Unleashed UI, how to find more information about configuration fields, and to view screen shots of the Unleashed UI, refer to the *RUCKUS Unleashed User Guide*.

NOTE
For any configuration fields that are not described in the following sections, you can use their default values.

Setting up Cloudpath as an AAA RADIUS Authentication Server

TABLE 6 Fields/Values to Use for Unleashed AAA Authentication Service

Configuration Field	Corresponding Value
Name	Name: Any descriptive name for the AAA authentication service
Type	RADIUS
Auth Method	PAP
IP Address	The IP address of the Cloudpath Enrollment System.
Port	1812 is typically used and is the default.
Shared Secret	This must match the shared secret for the Cloudpath ES onboard RADIUS server (**Configuration > RADIUS Server**).
Confirm Secret	Confirm Secret: The shared secret (entered again).

Creating AAA Accounting Server (Optional)

TABLE 7 Fields/Values to Use for Unleashed AAA RADIUS Accounting Service

Configuration Field	Corresponding Value
Name	Name: Any descriptive name for the AAA accounting service
Type	RADIUS ACCOUNTING
IP Address	The IP address of the Cloudpath Enrollment System.
Port	1813 is typically used and is the default.
Shared Secret	This must match the shared secret for the Cloudpath ES onboard RADIUS server (**Configuration > RADIUS Server**).
Confirm Secret	Confirm Secret: The shared secret (entered again).

Testing AAA Servers

To test the connection between Unleashed and the Cloudpath RADIUS server, RUCKUS strongly recommends testing the AAA server after you set it up. Refer to the instructions in the *RUCKUS Unleashed User Guide*.

Creating a Hotspot (WISPr) Portal

TABLE 8 Fields/Values to Use for Creating a Hotspot (WISPr) Portal

Creating a Hotspot (WISPr) Portal Section in Unleashed UI	Configuration Field and Corresponding Value
General tab	Name: Any descriptive name for the hotspot portal.
Redirection (General tab)	Redirect unauthenticated user: The Cloudpath Enrollment Portal URL, which should be contained in the applicable workflow in the Cloudpath UI (**Configuration > Workflows**).
	Start Page: After user is authenticated,: Select "Redirect to the URL that the user intends to visit." This lets you set a different page where users will be redirected (for example, your company website). Enter a domain name or an IP address for the redirection.

TABLE 8 Fields/Values to Use for Creating a Hotspot (WISPr) Portal (continued)

Creating a Hotspot (WISPr) Portal Section in Unleashed UI	Configuration Field and Corresponding Value
Authentication/Accounting Servers (Authentication tab)	Authentication Server: Drop-down list to select the Cloudpath RADIUS Authentication Server. **NOTE** Enabling this option allows users with registered MAC addresses to be transparently authorized without having to log in. A user entry on the RADIUS server needs to be created using the client MAC address as both the user name and password. For the MAC address format, RUCKUS recommends using AA:BB:CC:DD:EE:FF.
Authentication/Accounting Servers (Authentication tab)	Accounting Server: Drop-down list to select the Cloudpath RADIUS Accounting Server (if applicable).

Setting Up the Walled Garden

To add a walled garden configuration, refer to the instructions in the *RUCKUS Unleashed User Guide*.

Also, when configuring the walled garden, include the following steps:

1. Include the DNS or IP address of the Cloudpath system, then click **OK**
2. Optionally, there are some domains that you can add to the walled garden on all controllers to:
   - Prevent the Apple CNA mini-browser from appearing on Apple devices.
   - Avoid being blocked or slowed when attempting to download the Cloudpath wizard.

     NOTE
     There will still be about a 15-to-20-second delay when the full application is 33 percent complete (about 40 MB) in its download.

   The recommended destinations to add for the walled garden are:

   ```
   *.ggpht.com
   *.play.googleapis.com
   *.googleapis.com
   *.play.google.com
   android.clients.google.com
   *.gvt1.com
   connectivitycheck.android.com
   connectivitiycheck.google.com
   *.gstatic.com
   *.clients3.google.com
   *.thawte.com
   ```

   NOTE
   The *thawte.com destination is the OCSP URL of the SSL certificate of the Cloudpath server. This URL can be found by clicking the *lock* icon in your web browser and viewing the details of your certificate.

3. If you are still experiencing issues, you can try adding the following destinations to the walled garden:

   ```
   *.clients.google.com
   *.l.google.com
   *.googleusercontent.com
   *.appengine.google.com
   *.cloud.google.com
   *.android.com
   *.cloudfront.net
   *.akamaihd.net
   ```

```
172.217.0.0/16
216.58.0.0/16
```

Creating the Onboarding SSID

TABLE 9 Fields/Values to Use for Unleashed Onboarding SSID

Configuration Field	Corresponding Value
Name	Name of the SSID
Usage Type	Hotspot Service known as WISPr
Hotspot Services	Drop-down list to selet the already-created hotspot service

NOTE
RUCKUS recommends enabling the "Bypass Apple CNA" feature. For instructions, refer to the *RUCKUS Unleashed User Guide*.

Configuring ZoneDirector

This section includes tables of configuration fields and values for setting up the ZoneDirector Controller. For more information, such as how to navigate the ZoneDirector UI, how to find more information about configuration fields, and to view screen shots of the ZoneDirector UI, refer to the *RUCKUS ZoneDirector User Guide*.

NOTE
For any configuration fields that are not described in the following sections, you can use their default values.

Setting up Cloudpath as an AAA RADIUS Authentication Server

TABLE 10 Fields/Values to Use for ZoneDirector AAA Authentication Service

Configuration Field	Corresponding Value
Name	Name: Any descriptive name for the AAA authentication service
Type	RADIUS
Auth Method	PAP
IP Address	The IP address of the Cloudpath Enrollment System.
Port	1812 is typically used and is the default.
Shared Secret	This must match the shared secret for the Cloudpath ES onboard RADIUS server (**Configuration > RADIUS Server**).
Confirm Secret	Confirm Secret: The shared secret (entered again).

Creating AAA RADIUS Accounting Server (Optional)

TABLE 11 Fields/Values to Use for ZoneDirector AAA Accounting Service

Configuration Field	Corresponding Value
Name	Name: Any descriptive name for the AAA accounting service
Type	RADIUS ACCOUNTUING
Auth Method	PAP
IP Address	The IP address of the Cloudpath Enrollment System.

TABLE 11 Fields/Values to Use for ZoneDirector AAA Accounting Service (continued)

Configuration Field	Corresponding Value
Port	1813 is typically used and is the default.
Shared Secret	This must match the shared secret for the Cloudpath ES onboard RADIUS server (**Configuration > RADIUS Server**).
Confirm Secret	Confirm Secret: The shared secret (entered again).

Testing AAA Servers

To test the connection between the controller and the Cloudpath RADIUS server, RUCKUS strongly recommends testing the AAA server after you set it up. Refer to the instructions in the *RUCKUS ZoneDirector User Guide*.

Creating a Hotspot (WISPr) Portal

TABLE 12 Fields/Values to Use for Creating a Hotspot (WISPr) Portal

Creating a Hotspot (WISPr) Portal section in ZoneDirector UI	Configuration Field and Corresponding Value
Top portion of configuration fields area	Name: Any descriptive name for the hotspot portal.
Redirection	Login URL: Select "External."
	Login Page Redirect unauthenticated user: The Cloudpath Enrollment Portal URL, which should be contained in the applicable workflow in the Cloudpath UI (**Configuration > Workflows**).
	Start Page After user is authenticated,: Select "Redirect to the URL that the user intends to visit." This lets you set a different page where users will be redirected (for example, your company website). Enter a domain name or an IP address for the redirection.
Authentication/Accounting Servers (Authentication tab)	Authentication Server: Drop-down list to select the Cloudpath RADIUS Authentication Server. **NOTE** Enabling this option allows users with registered MAC addresses to be transparently authorized without having to log in. A user entry on the RADIUS server needs to be created using the client MAC address as both the user name and password. For the MAC address format, RUCKUS recommends using AA:BB:CC:DD:EE:FF.
Authentication/Accounting Servers (Authentication tab)	Accounting Server: Drop-down list to select the Cloudpath RADIUS Accounting Server (if applicable).

Setting Up the Walled Garden

To add a walled garden configuration to your existing Hotspot Services, refer to the instructions in the *RUCKUS ZoneDirector User Guide*.

Also, when configuring the walled garden, include the following steps:

1. Include the DNS or IP address of the Cloudpath system, then click **OK**
2. Optionally, there are some domains that you can add to the walled garden on all controllers to:
   - Prevent the Apple CNA mini-browser from appearing on Apple devices.
   - Avoid being blocked or slowed when attempting to download the Cloudpath wizard.

NOTE
There will still be about a 15-to-20-second delay when the full application is 33 percent complete (about 40 MB) in its download.

The recommended destinations to add for the walled garden are:

```
*.ggpht.com
*.play.googleapis.com
*.googleapis.com
*.play.google.com
android.clients.google.com
*.gvt1.com
connectivitycheck.android.com
connectivitiycheck.google.com
*.gstatic.com
*.clients3.google.com
*.thawte.com
```

NOTE
The *thawte.com destination is the OCSP URL of the SSL certificate of the Cloudpath server. This URL can be found by clicking the *lock* icon in your web browser and viewing the details of your certificate.

3. If you are still experiencing issues, you can try adding the following destinations to the walled garden:

```
*.clients.google.com
*.l.google.com
*.googleusercontent.com
*.appengine.google.com
*.cloud.google.com
*.android.com
*.cloudfront.net
*.akamaihd.net
172.217.0.0/16
216.58.0.0/16
```

Creating the Onboarding SSID

TABLE 13 Fields/Values to Use for ZoneDirector Onboarding SSID

Creating a WLAN Configuration (for Onboarding SSID) section in ZoneDirector UI	Configuration Field and Corresponding Value
General Options	Name/ESSID: Name of the SSID
	Zone: Zone in which the WLAN will reside
WLAN Usages	Type: Hotspot (WISPr)
Authentication Options	Method: Open
Encryption Options	Method: None
Options	Hotspot Services Drop-down list to selet the already-created hotspot service.

NOTE
RUCKUS recommends enabling the "Bypass Apple CNA" feature. For instructions, refer to the *RUCKUS ZoneDirector User Guide*.

Configuring Policies

Policies allow for mapping incoming successful RADIUS authentication requests to a set of RADIUS response attributes based on dynamic conditions of the request. Each policy has an associated RADIUS attribute group which defines the RADIUS response attributes (such as VLAN ID, filter ID, and class). Each authentication is matched against an assigned list of candidate policies in sequential order. Criteria of a policy can include dynamic conditions such as a user's physical location, username, or the time of day.

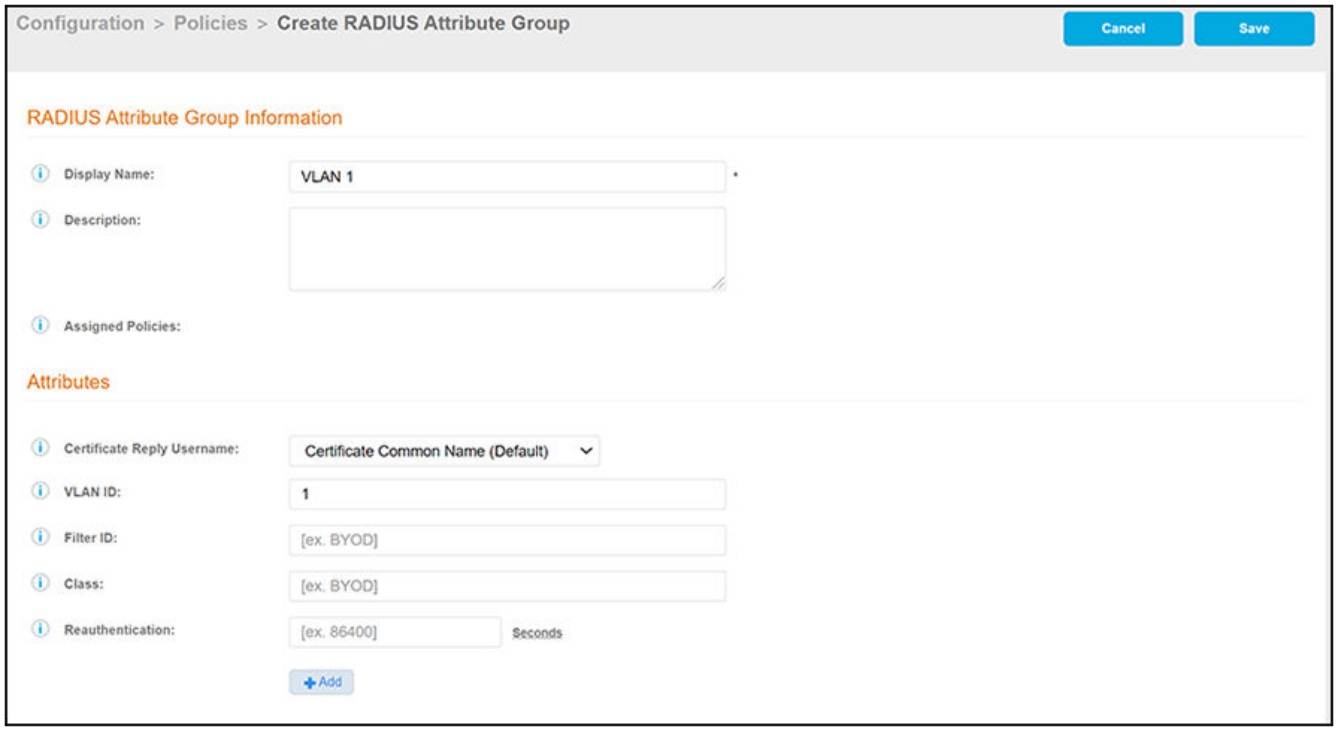
The following procedure guides you first through creating RADIUS attribute groups for your policies, then creating the policies themselves. You must create at least one RADIUS attribute group before you can configure a policy because a policy needs to have at least one RADIUS attribute group available for selection.

1. In the Cloudpath UI, go to **Configuration > Policies**.
2. Select the **RADIUS Attribute Groups** tab, then click the **Add RADIUS Attribute Group** button.
3. In the ensuing Create Radius Attribute Group screen, enter the information to create the group, then click **Save**.

   NOTE
   You can configure as many RADIUS Attribute groups as you want. One RADIUS Attribute group will later be assigned to each policy you create.

   An example screen and field descriptions follow:

   FIGURE 2 Create RADIUS Attribute Screen



- Display Name: The name of the RADIUS attribute group. This should be a descriptive name. It is visible only to Cloudpath administrators

- Description: Optionally, enter a description of this RADIUS attribute group. It is visible only to Cloudpath administrators.
- Assigned Policies: This field lists the names of all the policies that are using this RADIUS attribute group. There will be no policies listed here during the initial configuration of the group.
- Certificate Reply Username: This setting is applied only when the RADIUS attribute group is associated with certificate-based authentications, and is therefore described in the Cloudpath documentation of certificate templates.
- VLAN ID: If this field is populated, the VLAN ID is included in the RADIUS reply to the controller for successful authentications. Cloudpath sends Tunnel-Type, Tunnel-Medium-Type, and Tunnel-Private-Group-ID. If your network policy is wireless, the Tunnel-Type value is VLAN, the Tunnel-Medium-Type value is 802 (this includes all 802 media plus Ethernet canonical format), and the Tunnel-Private-Group-ID is the integer that represents the VLAN number to which group members will be assigned.

  If the VLAN ID field is left blank, Cloudpath will not return a VLAN ID in the RADIUS reply; therefore the controller assigns the VLAN ID based on its own configuration.
- Filter ID: If this field is populated, the Filter ID is included in the RADIUS reply for successful authentications. If this field is left blank, Cloudpath will not return a Filter ID in the RADIUS reply.
- Class: If this field is populated, the Class is included in the RADIUS reply for successful authentications. If this field is left blank, Cloudpath will not return a Class in the RADIUS reply.
- Reauthentication: The number of seconds included in the RADIUS reply for successful authentications. If the device stays connected for longer than this period, the WLAN or switch requires that the device be reauthenticated. In wireless devices, this causes the encryption keys to rotate.
- Additional Attributes: You can add other attributes in the "Attributes" section of the screen by clicking the **+** button, and selecting the desired fields and values. These attributes will be returned to the controller in an access-accept RADIUS server packet.

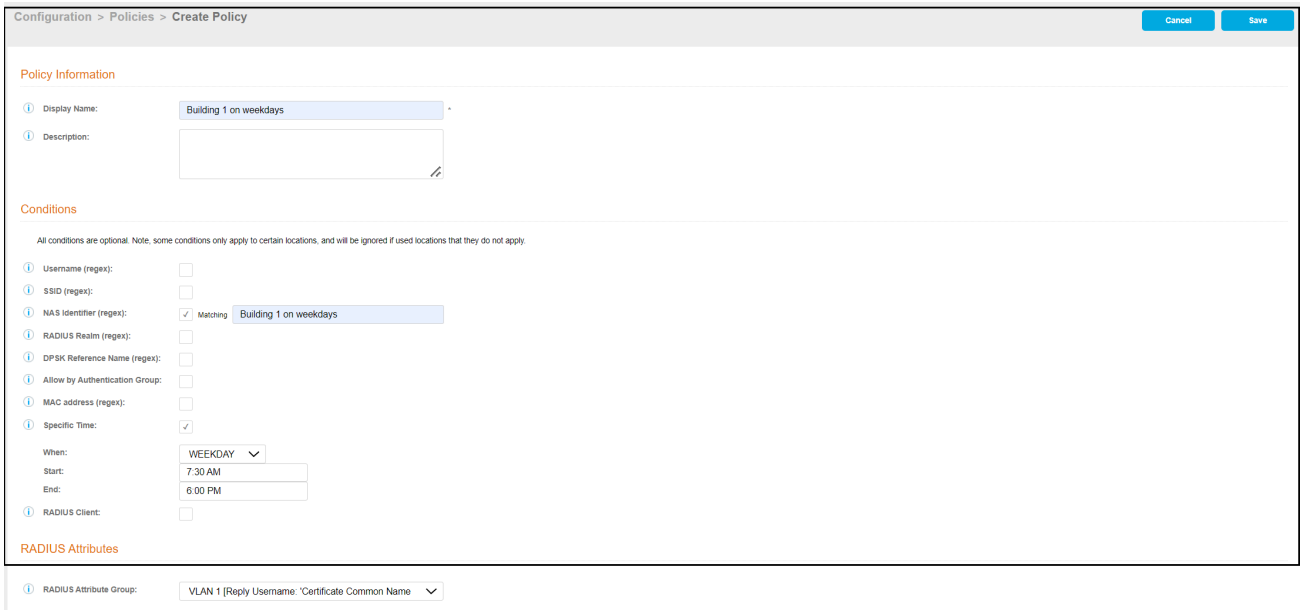
  NOTE
  For example, to return a Filter-Id for a guest user, enter Filter-Id in the Attribute field, and Guest in the Value field. If the authentication request is authorized, the RADIUS server returns the Filter- Id=Guest, along with the Access-Accept attribute to the user device.

4. Configure your policies:
   a. In the **Configuration > Policies** area of the UI, select the **Policies** tab, then click **Add Policies**.
   b. In the ensuing Create Policy screen, enter the information to create the policy, then click **Save**.

      NOTE
      You can configure as many policies as you want.

      An example screen and field descriptions follow:

FIGURE 3 Create Policy Screen



- Display Name: The name of the policy. This should be a descriptive name. It is visible only to Cloudpath administrators
- Description: Optionally, enter a description of this policy. It is visible only to Cloudpath administrators.
- "Conditions": In the Conditions section, use any or all of these fields to create the matching criteria you desire so that the appropriate policy gets applied to each user.

  NOTE
  You can use the asterisks that appear in some of the Conditions fields, when selected, to denote that any value is acceptable in the place of the asterisk.

  - Username Regex: When the user is prompted for credentials, the username specified by the user will be verified against this regular expression for proper format. For example, ^d{8}$ will ensure that the user enters an 8-digit id.

    NOTE
    Due to the complexity of regular expressions, it is recommended to use this field only if you are experienced with regular expressions. If you need assistance creating a regular expression to match your needs, contact support.

  - SSID (regex): A regular expression that lists any Wi-Fi SSID(s) to which you want to limit this policy.
  - NAS Identifier: The Network access server (NAS) identifier to limit the policy.

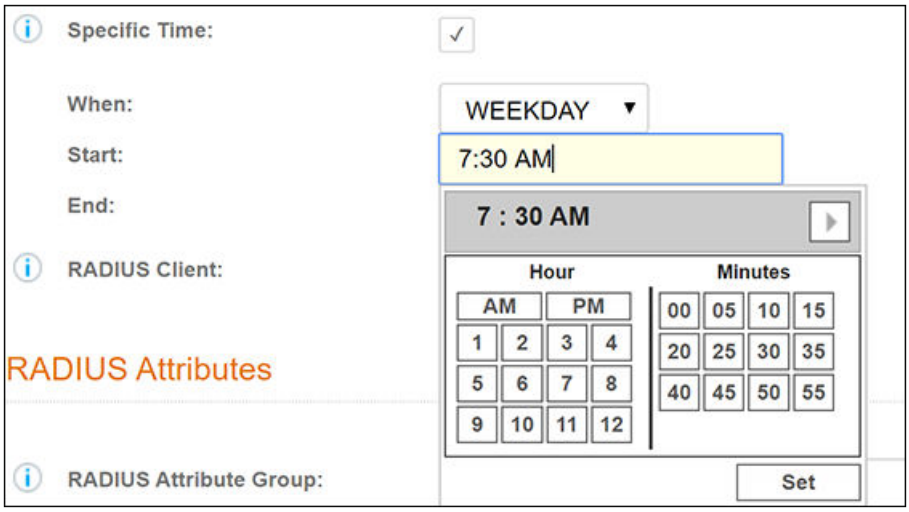
    NOTE
    If you use this field, and no NAS Identifier is provided in the response, the policy will be "false" and will not get applied to a user.

  - RADIUS Realm (regex): The RADIUS realm to use in this policy, in the form of @company.com or company.com
  - DPSK Reference Name (regex): A regular expression to test against the DPSK Reference Name.

    NOTE
    This field is applicable only when the policy is applied to a DPSK pool.

- Allow by Authentication Group: A regular expression defining which authentication groups are permitted within the Authentication Server.
- MAC address (regex): A regular expression defining the MAC address for the purpose of limiting this policy. If you select this box, but no MAC address is provided in the RADIUS response, the policy will always be "false."
- Specific Time: If checked, drop-downs appear where you can specify the days and times that this policy allows enrollment. Be sure to click the **Set** button to set the desired time (see the following illustration):

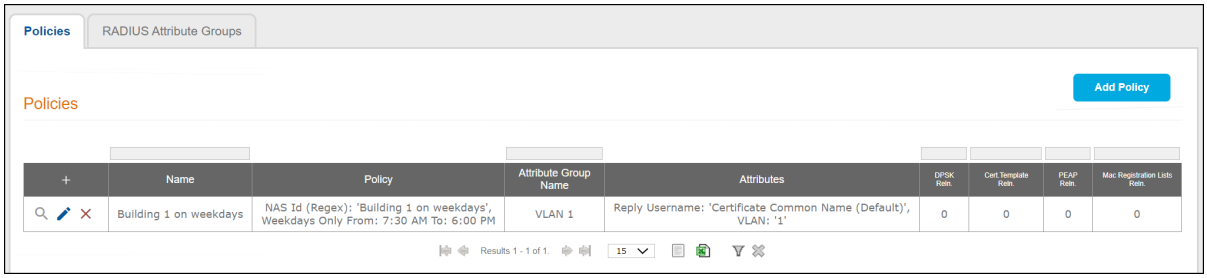
FIGURE 4 Setting a Time for a Policy



- RADIUS Client: If you check this box, you are presented with a drop-down where you can then select a RADIUS client if you have already configured this client in the **Configuration > RADIUS Server** > Clients tab. This RADIUS client would then be associated with this policy.
- RADIUS Attribute Group: From this drop-down, select the attribute group that you want associated with this policy.

The following illustration shows the Policies tab after one policy has been added. The information shown in the table represents the policy configuration shown in the example in Figure 3. The attribute group name and its attributes come from the attribute group name selected in the Create Policy Screen drop-down list. (The "Certificate Reply Username" applies only to certificate-based authentications, and is therefore described in the Cloudpath documentation of certificate templates.) The RADIUS attribute information shown below comes from the example in Figure 2.

FIGURE 5 Policies Table Example After One Policy Is Configured



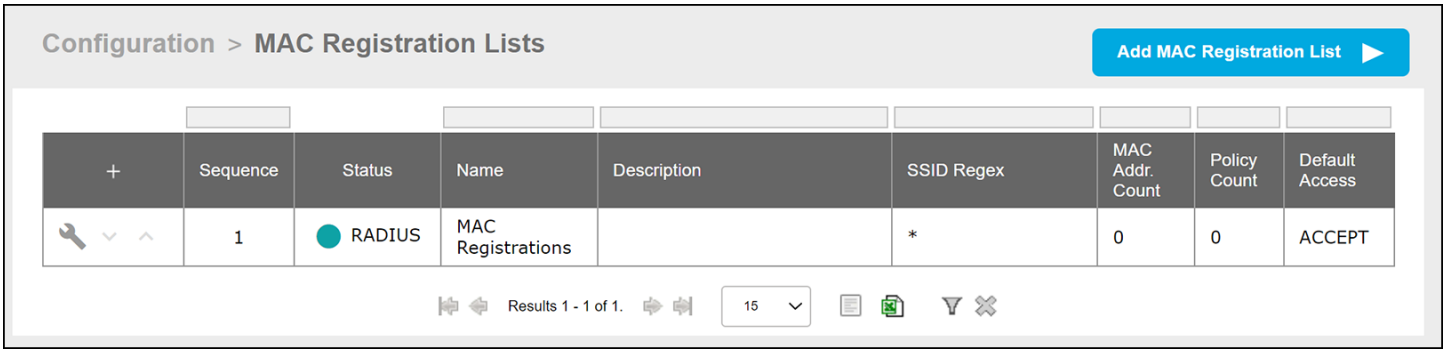
Configuring MAC Registration Lists in the Cloudpath UI

- Adding a New MAC Registration Configuration..... 23
- Importing a MAC Registration List..... 29
- Importing Individual MAC Addresses..... 30
- Removing a MAC Registration Configuration List or Its MAC Addresses..... 30
- Adding and Viewing MAC OUI Wildcards..... 31

The MAC Registration Lists area of the UI lets you create MAC registrations, and import MAC registration lists or individual MAC addresses into these configurations. MAC Registrations can also be used in a workflow.

Navigate to **Configuration > MAC Registration Lists**. From here, you can add new MAC registration lists, view current lists, and click the wrench icon next to any list to perform actions on that list. The following screen is an example of the MAC Registrations List main screen where one list called "MAC Registrations" already exists and whose status is enabled for incoming RADIUS MAC Registration-based authentications (described in Figure 7 on page 24.

FIGURE 6 MAC Registrations Lists Main Screen



NOTE
If you hover over the status of a MAC registration list with your cursor, the status will also indicate if the list is currently referenced from within a workflow.

Adding a New MAC Registration Configuration

Follow these steps to create a new MAC Registration configuration which you can then use to import MAC addresses.

1. Click **Add MAC Registration List** in the upper right of the screen shown above.

2. In the Create MAC Registrations screen (see the example screens below), configure the values (described after the example screens), then click **Save**.

FIGURE 7 Creating a New MAC Registration Configuration - Screen 1 of 2

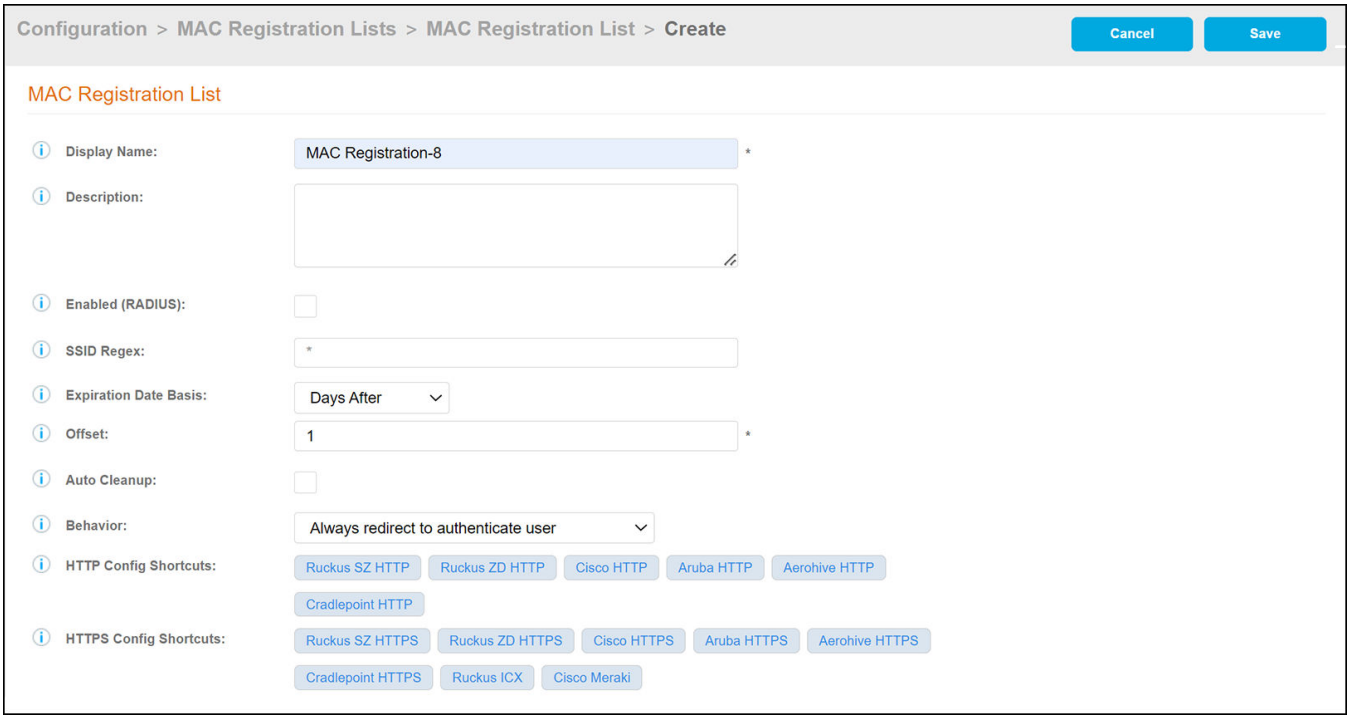
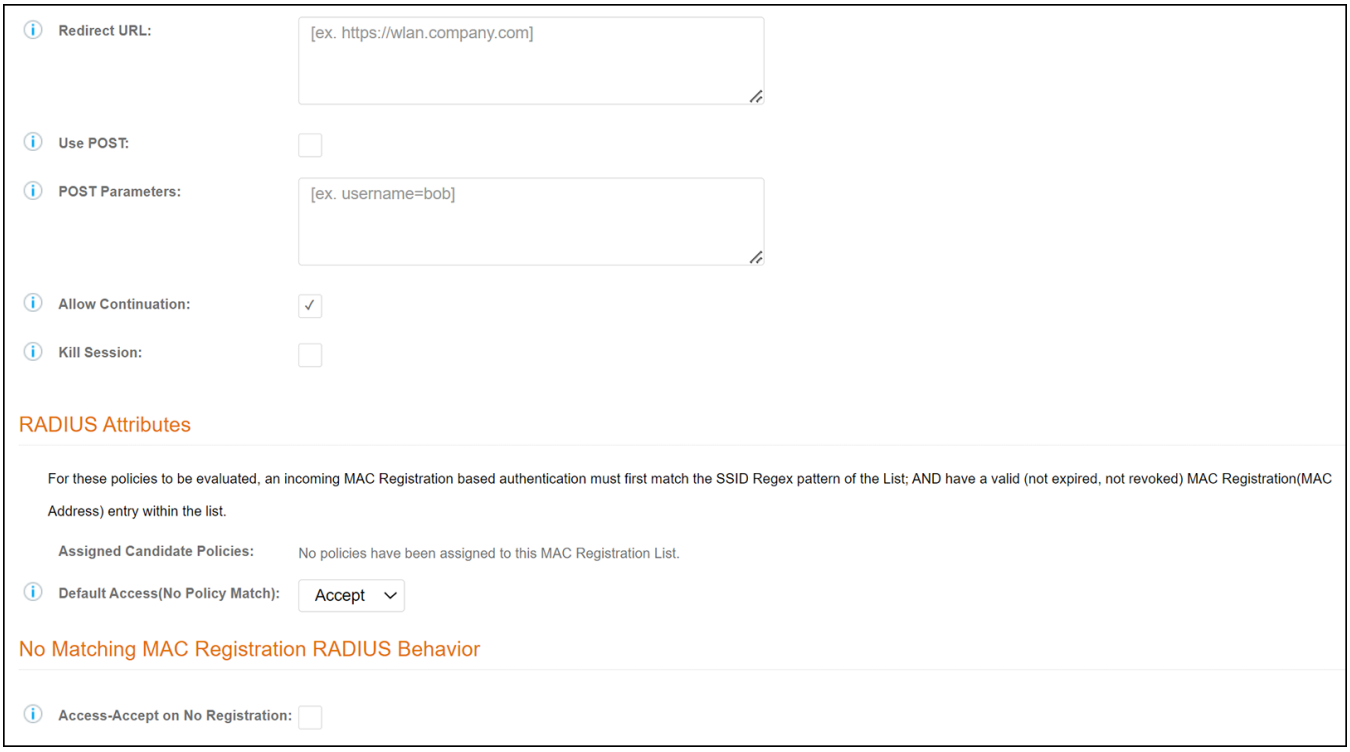


FIGURE 8 Creating a New MAC Registration Configuration - Screen 2 of 2



- Display Name: Any descriptive name you want.
- Description: Optional description of this particular MAC registration configuration.
- Enabled (RADIUS): This field is enabled by default (but shown as unchecked in the example screen). When a list is enabled for RADIUS, an incoming MAC Registration-based authentication request is considered successful if there is a corresponding valid (not expired, not revoked) MAC Registration (MAC address) entry within the list. If you want to disable this field, uncheck the box; workflows may still use and add MAC addresses to this MAC Registration list even if you disable this option.

  NOTE
  Disabling a list for RADIUS effectively disables the devices with MAC Addresses within the list from authenticating. One reason for doing this could be if you want to build a MAC registration list before enabling it for authentications in a live environment.

- SSID Regex: 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. *Cloudpath Enrollment System Sponsored Guest Access Configuration Guide*, located on the **Support** tab, for details.

- 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.

  NOTE
  This field may be unnecessary and therefore disappear, depending on your selection for Expiration Date Basis.

- Behavior: Specifies the prompt and redirect settings for the MAC registration configuration. 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 is killed as the user is redirected. If returned, the user is forced to start over.
- RADIUS Attributes (also see the flowchart below):

  NOTE

  :

  - Assigned Candidate Policies: A list of policies that have been assigned to this MAC registration list; if no policies have yet been assigned, this is indicated, as in the earlier example screen.

    NOTE
    For these policies to be evaluated, an incoming MAC Registration based authentication must first match the SSID Regex pattern of the List; AND have a valid (not expired, not revoked) MAC Registration(MAC Address) entry within the list.

  - Default Access (No Policy Match): A drop-down where you can select whether to allow a user onto the network even if there is no matching policy for the user. When no policies are assigned, or when policies are assigned but no match is found against any of the policies, the default RADIUS access response will either be accepted or rejected. When the authentication is successful, the RADIUS attributes from the matched policy are sent in the RADIUS reply.

    NOTE
    Once you assign policies (described later) to a MAC registration list, a policies table is included if you edit this screen.

  - No Matching MAC Registration RADIUS Behavior: By default, the RADIUS server sends an “Access-Reject” reply if authentication fails. However, you can use the “Access-Accept on No Registration:" feature to send a RADIUS Access-ACCEPT response for authentications to this list *without* a matching MAC Registration(MAC Address) entry within the list. If you check the“Access-Accept on No Registration:" box, a drop-down list of all configured RADIUS attribute groups appears (see the screen below); select the group you want. In this case, be sure you have already configured the RADIUS attribute group you want to use. With this field enabled and an attribute group selected, the attributes defined in the group are sent along with an “Access-Accept” RADIUS reply.

FIGURE 9 RADIUS Attribute Group Down-Down List for Accept-Accept with No MAC Registration Match

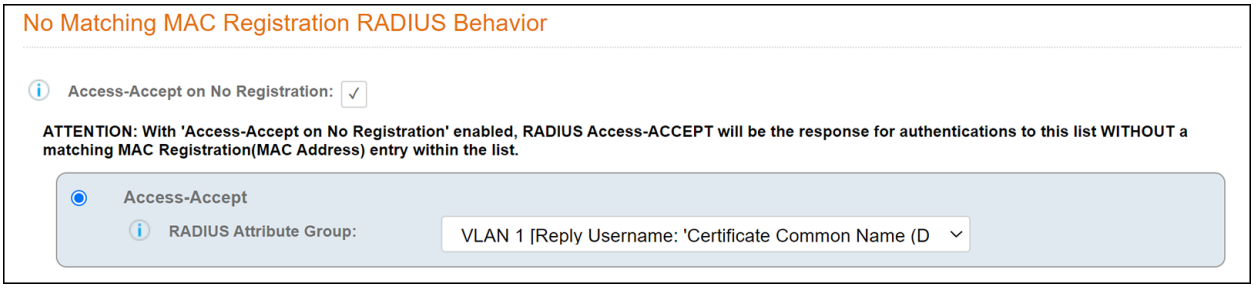
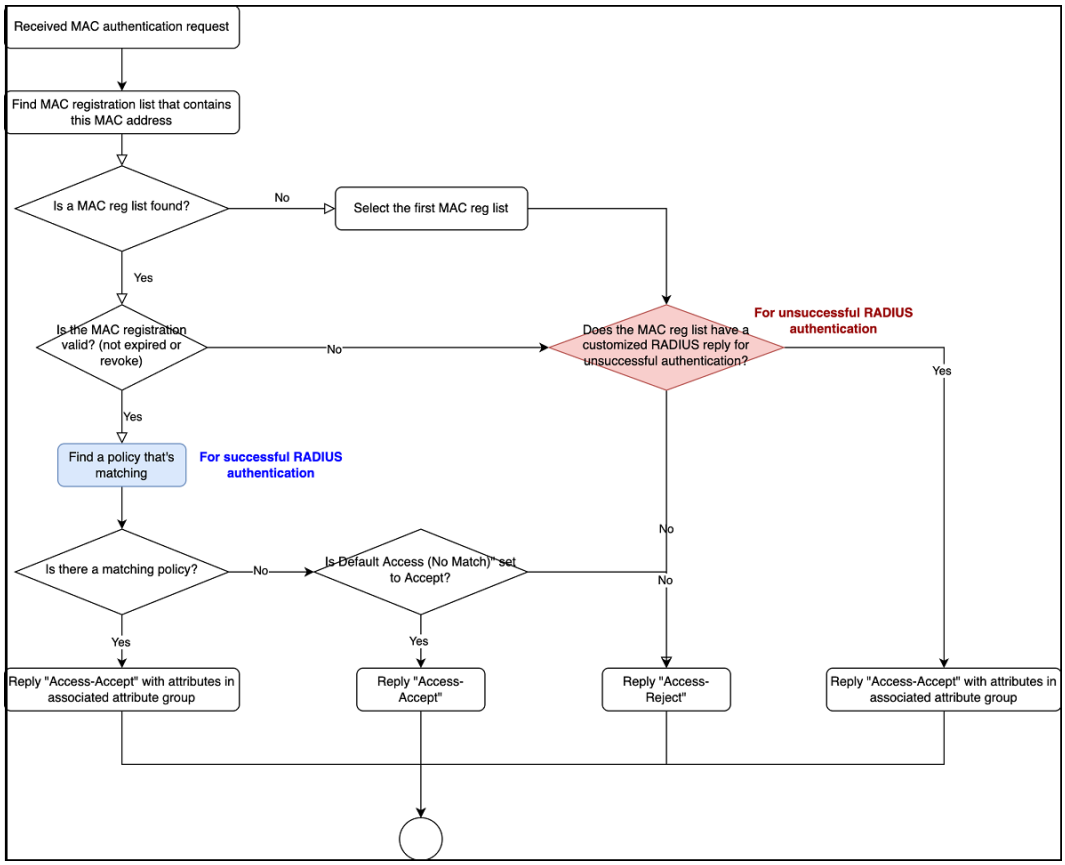


FIGURE 10 RADIUS Attributes Flowchart



3. After you click **Save**, you are returned to a four-tab of the MAC Registration List screen for the list you just configured, as shown in the following example screens:

FIGURE 11 Four-Tab View for Newly Added Mac Registration List (Top Portion of Screen)

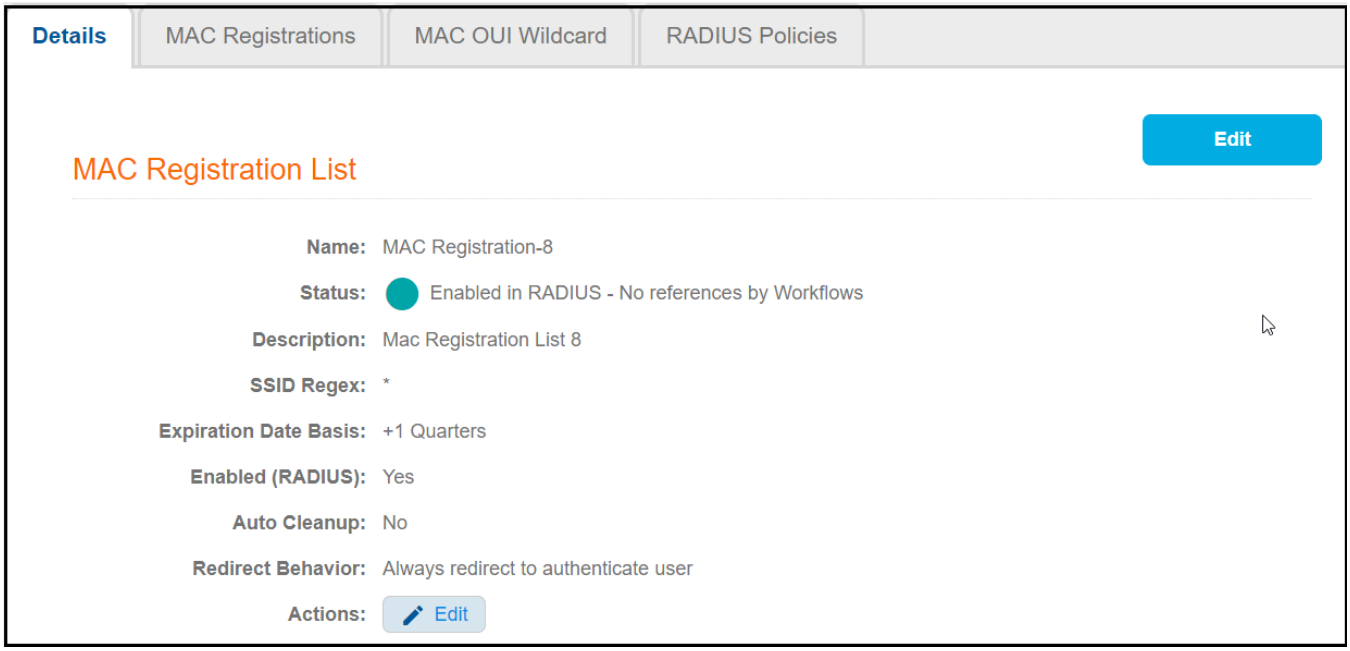
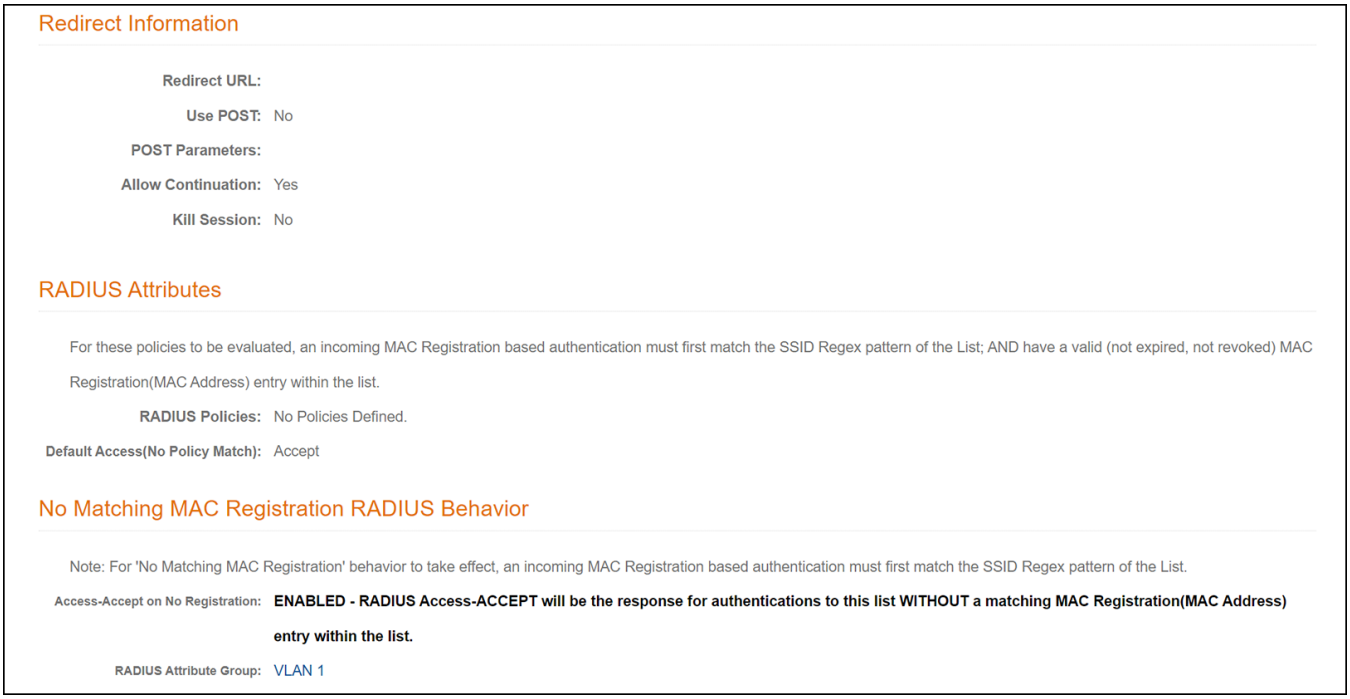
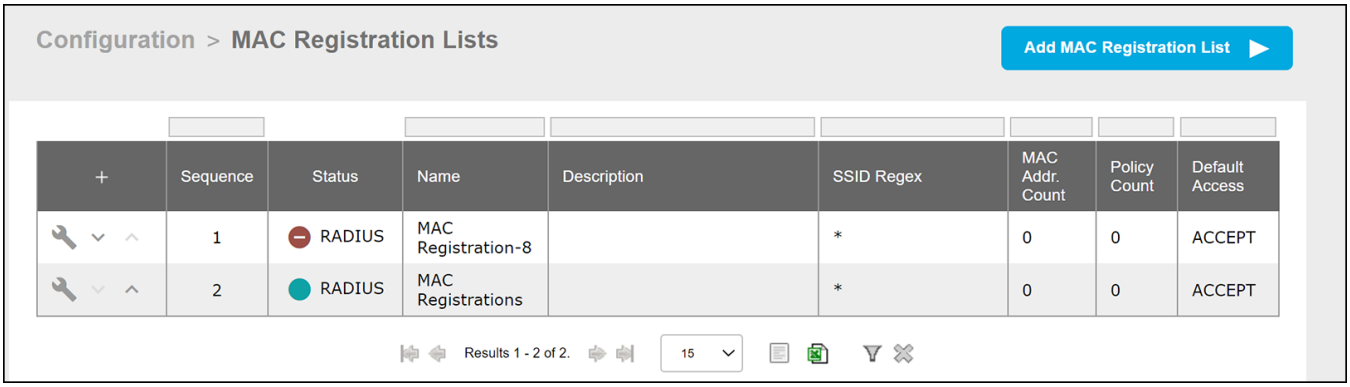


FIGURE 12 Four-Tab View for Newly Added Mac Registration List (Lower Portion of Screen)



4. If you click **View All MAC Registration Lists** (in the preceding screen though not shown in the illustration), you are returned to the main screen, with the new configuration (MAC Registration-8 in this example) appearing in the list, as shown below:

FIGURE 13 MAC Registration Lists Screen After Adding a Second Registration Configuration

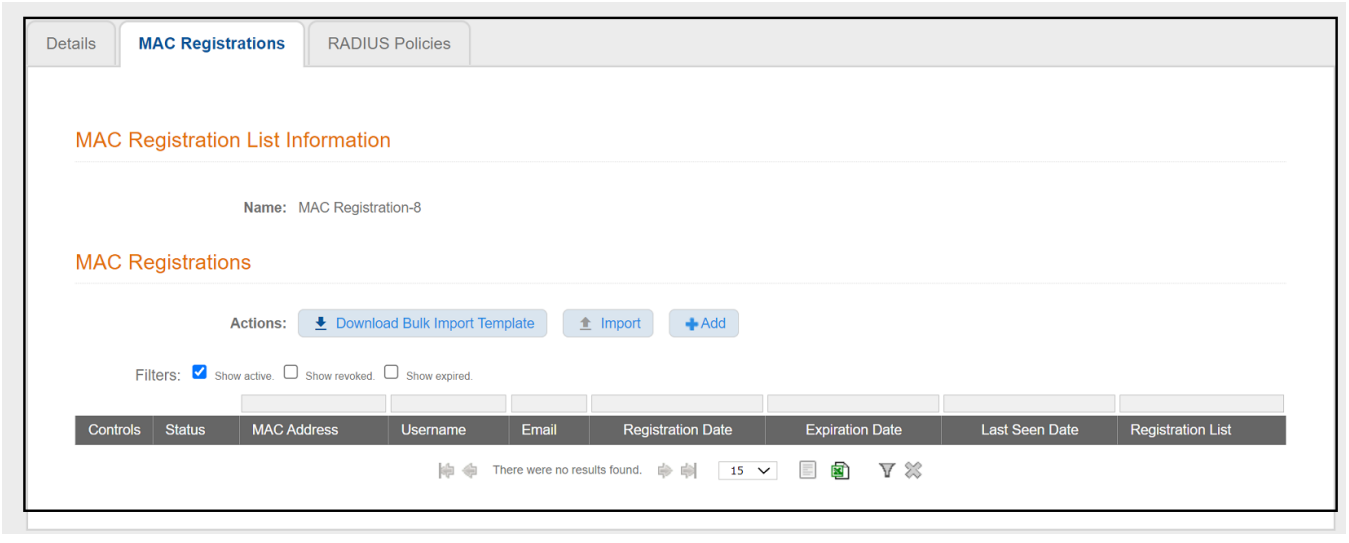


Importing a MAC Registration List

Follow these steps to import a MAC registration list into a MAC registration configuration.

1. From the main MAC Registrations Lists screen, click the wrench icon for the list in which you want to import a MAC address list.
2. On the ensuing screen, click the **MAC Registrations** tab. A screen such as the following is invoked:

FIGURE 14 MAC Registrations Tab of a MAC Registration List



3. If you first need a template for adding MAC addresses to an .xls file, click **Download Bulk Import Template**.

4. Once you are ready to import the list of MAC addresses to the MAC registration list, click **Import**.

   NOTE
   If importing from a .csv file, the following date formats are supported: yyyyMMdd, HHmmss, yyyyMMdd HHmm, yyyyMMdd, MM/dd/yyyy HHmmss, MM/dd/yyyy HHmm, MM/dd/yyyy, yyyy-MM-dd HH:mm:ss, yyyy-MM-dd.

5. Browse to select your MAC address list, then click **Continue**.
6. A popup message appears, where you click **Continue Import**:

   FIGURE 15 Popup Asking You to Confirm Import of MAC Address List File

7. The file is imported and the MAC addresses are added to the applicable MAC Registration list.

Importing Individual MAC Addresses

Follow these steps to import individual MAC addresses into a MAC registration configuration.

1. From the MAC Registrations tab of the desired MAC Registrations List (refer to the example in Figure 14 on page 29), click the **Add** button in the "MAC Registrations" portion of the screen.
2. In the popup window, enter the MAC addresses, separated by commas, that you wish to add.
3. Click **Save**.
4. Confirm the import on the ensuing popup window.

   You are returned to the MAC Registrations tab, and there should be a confirmation message at the top, indicating that the MAC addresses have been successfully added. They will also appear at the bottom of that screen.

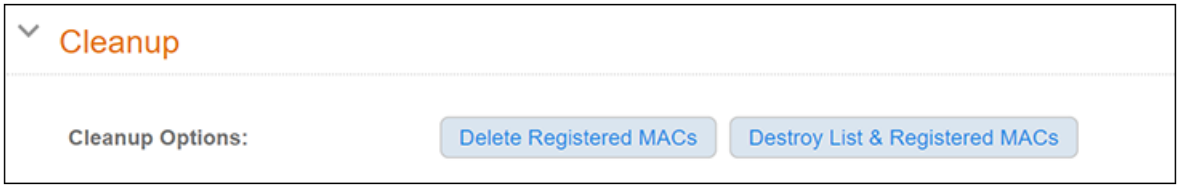
Removing a MAC Registration Configuration List or Its MAC Addresses

Follow these steps to either remove the MAC addresses from a MAC registration configuration list or to remove both the MAC addresses and the list itself:

1. Click the **Details** tab from an open MAC Registration List screen.
2. Click **Edit**.

3. Scroll to the bottom of the screen until you get to the **Cleanup** area, and click **Cleanup** to display the options:

   FIGURE 16 Cleanup Options for MAC Registration Configuration List



   NOTE
   You cannot destroy the entire list if it is currently part of a workflow.

4. Click on the desired option.

   A Warning popup appears.

5. If you wish to continue, be sure to check the box to indicate that you "understand the warning," then click **Continue**.

   You are returned to the **Details** tab, where you should see a message indicating that your action has taken effect.

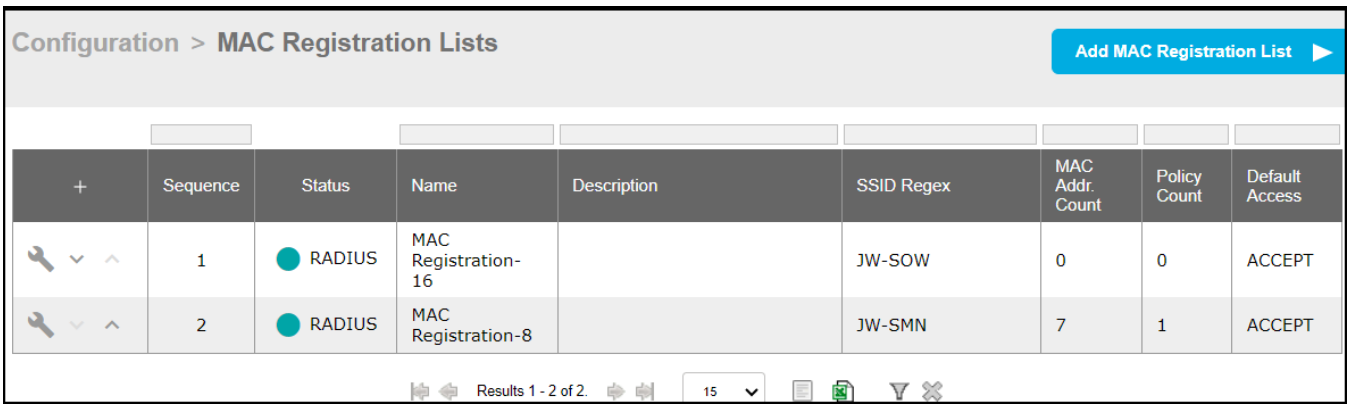
Adding and Viewing MAC OUI Wildcards

The **MAC OUI Wildcard** tab for a MAC registration list lets you add, view, or delete a MAC OUI (Organizationally Unique Identifier) wildcard definitions. MAC OUI wildcards allow for all devices that match the OUI pattern prefix to authenticate via the Mac Registration List without the need for manual entry of individual device MAC addresses.

Follow these steps to add a MAC OUI wildcard to a MAC registration list and view the details:

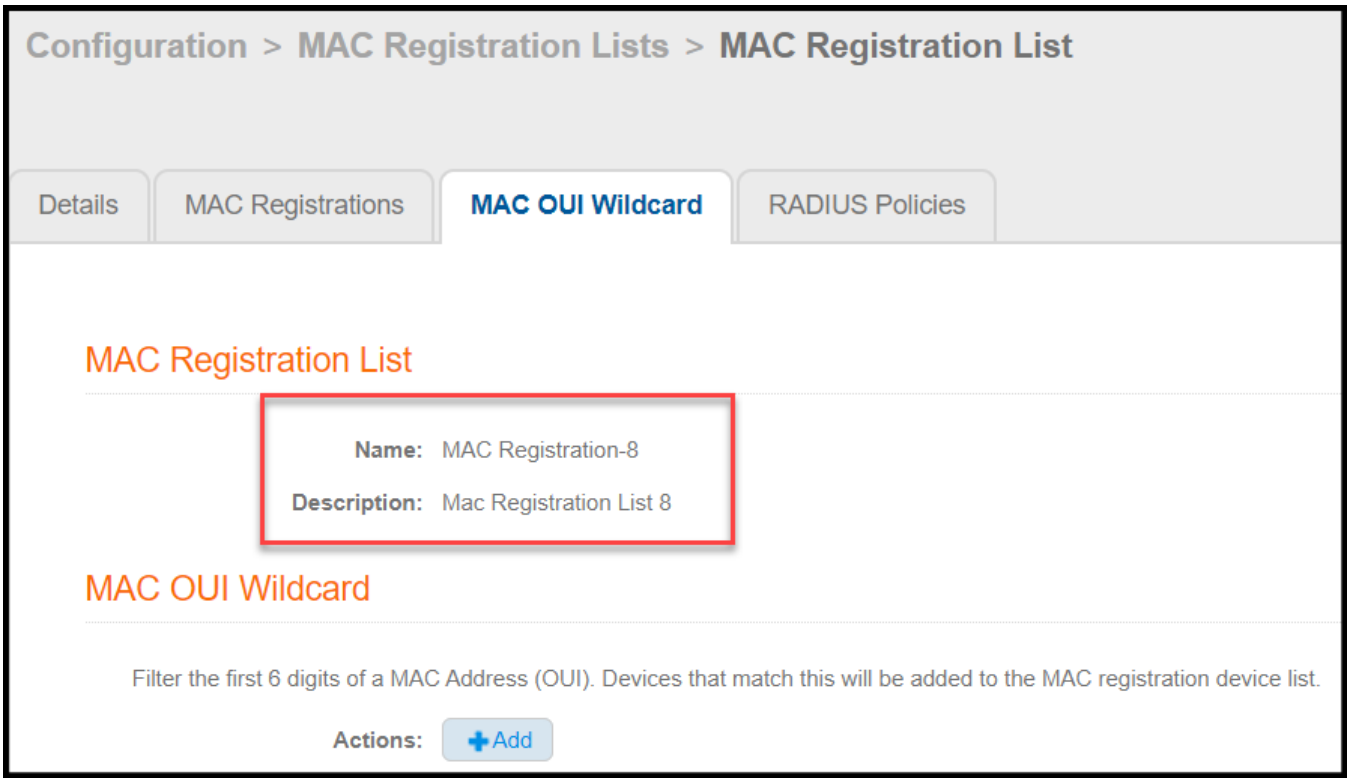
1. In the Cloudpath UI, go to **Configuration > MAC Registration Lists** to view all existing MAC registration lists:

   FIGURE 17 MAC Registration Lists View



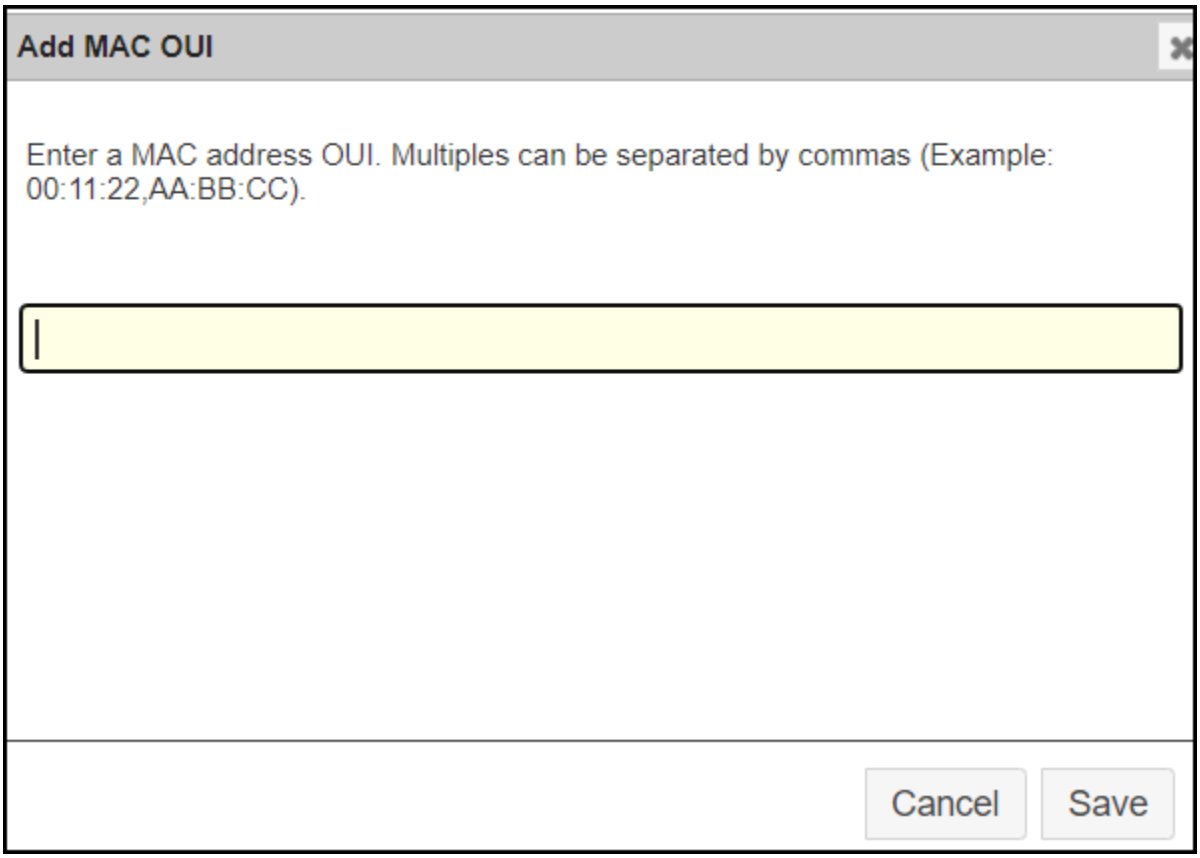
2. Click the wrench icon for the desired MAC registration list; for example the MAC-Registration-8 entry in the screen above. The four-tab MAC Registration List screen for the list you selected appears. Select the **MAC OUI Wildcard** tab. The screen below shows the **MAC OUI Wildcard** tab for the MAC-Registration-8 MAC registration list.

FIGURE 18 MAC Registration List Screen with MAC OUI Tab



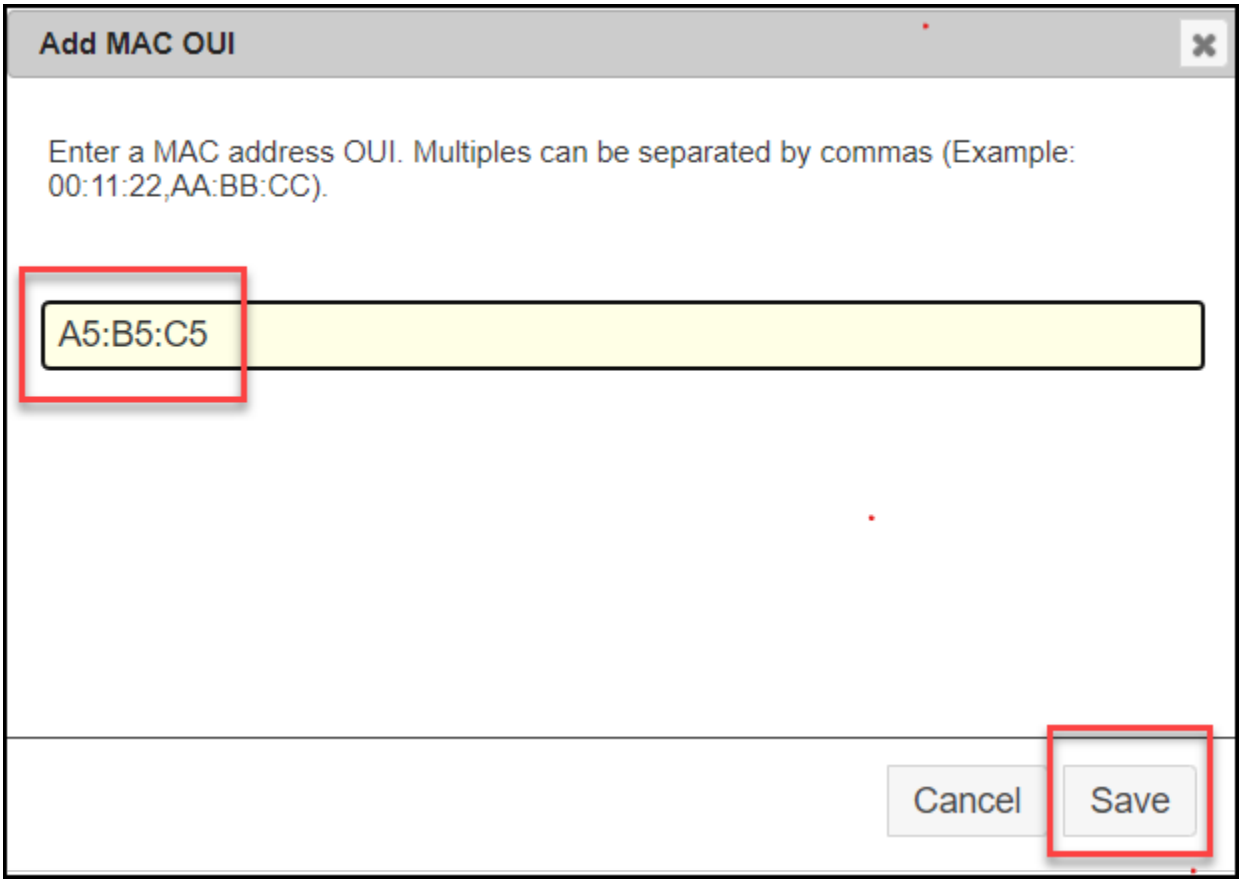
3. Click **Add**. The Add MAC OUI popup window appears.

FIGURE 19 Add MAC OUI Popup Window



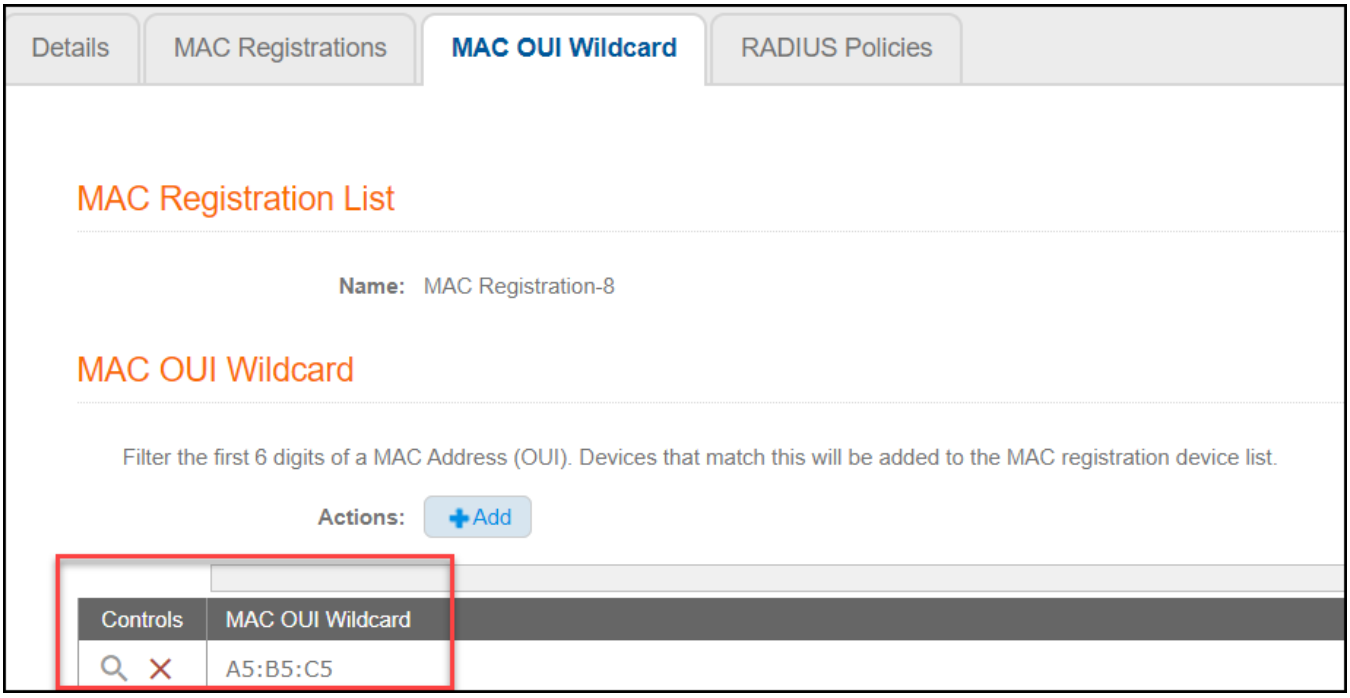
4. In the popup window, enter the first six digits of the MAC address (MAC OUI wildcard) that you want to use, and click **Save**. In the screen below the first six digits of the MAC address entered are A5:B5:C5.

FIGURE 20 Entering the MAC OUI address



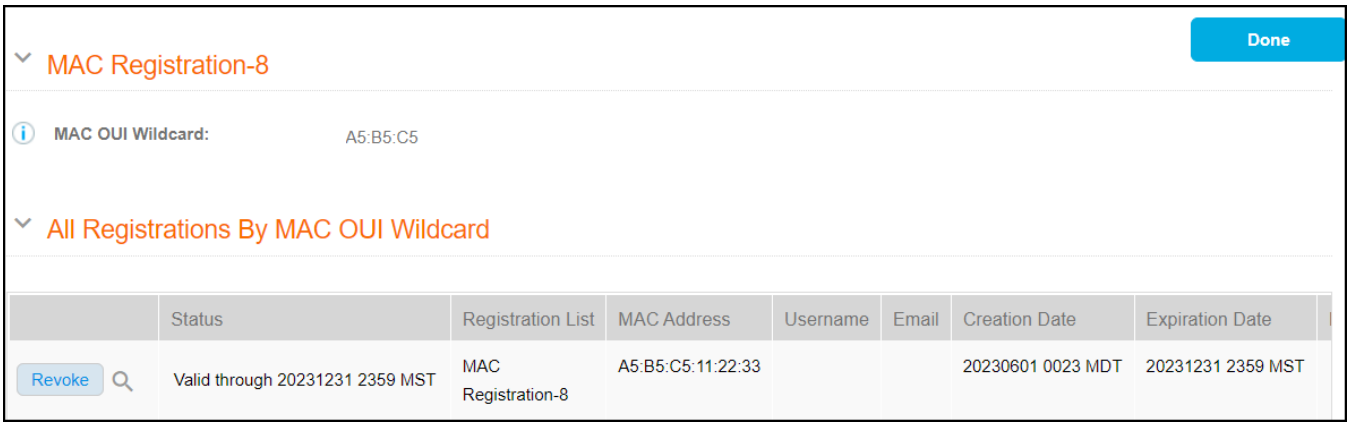
5. You are returned to the **MAC OUI Wildcard** tab for the MAC Registration List. Verify that the A5:B5:C5 MAC OUI has been added to the MAC OUI Wildcard list, as displayed in the following screen.

FIGURE 21 Successfully Added MAC OUI Wildcard



6. Once the MAC OUI wildcard has been succesfully added, you can view details about the MAC OUI wildcard. To view the MAC OUI wildcard details, click the magnifying glass icon next to the MAC OUI wildcard that you want to view. The screen below shows details for the A5:B5:C5 MAC OUI wildcard. All devices with a MAC address where the first six digits contain A5:B5:C5 have been added to the MAC OUI wildcard. Any MAC addresses that are prefixed with this MAC OUI wildcards will be able to self-register to the registration list without the need for individual MAC registrations.

FIGURE 22 MAC OUI Wildcard Details



7. If you want to delete a MAC OUI wildcard from a MAC registration list:, click **X** next to the MAC OUI wildcard that you want to remove. A popup window appears reminding you that this action does not affect existing MAC Registration lists. Only the MAC OUI wildcard is removed. Click **OK**. The selected MAC OUI wildcard is removed.

Adding Policies to a MAC Registration List

You can add as many policies as you want; policies are evaluated in the order they are listed, and the RADIUS attributes of the first matching policy are used. For a user to successfully connect to the network, the user must be a match for at least one policy (or you can allow users to connect even if they do not match a policy).

Steps to Add Policies

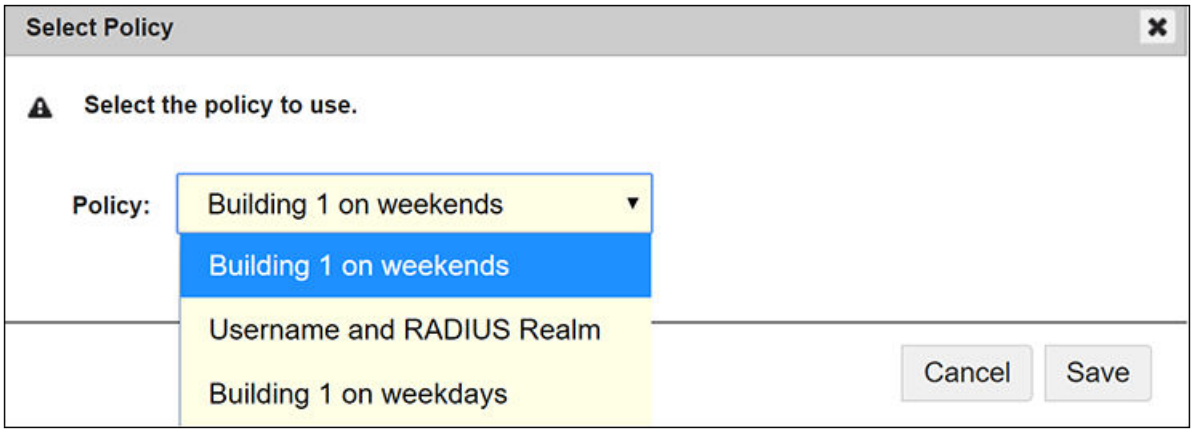
Follow these steps to add a policy:

1. In the Cloudpath UI, go to **Configuration > MAC Registration Lists** to view all existing MAC registration lists:

   FIGURE 23 MAC Registration Lists View

2. Click the wrench icon for the desired MAC registration list; for example the MAC-Registration-8 entry in the screen above.
3. In the ensuing screen, click the RADIUS Policies tab, then click **Assign Policy**. The Select Policy Drop-down list appears, as shown in the following example list. The policies that you have already configured are available for you to add:

   FIGURE 24 Select Policy Drop-down List



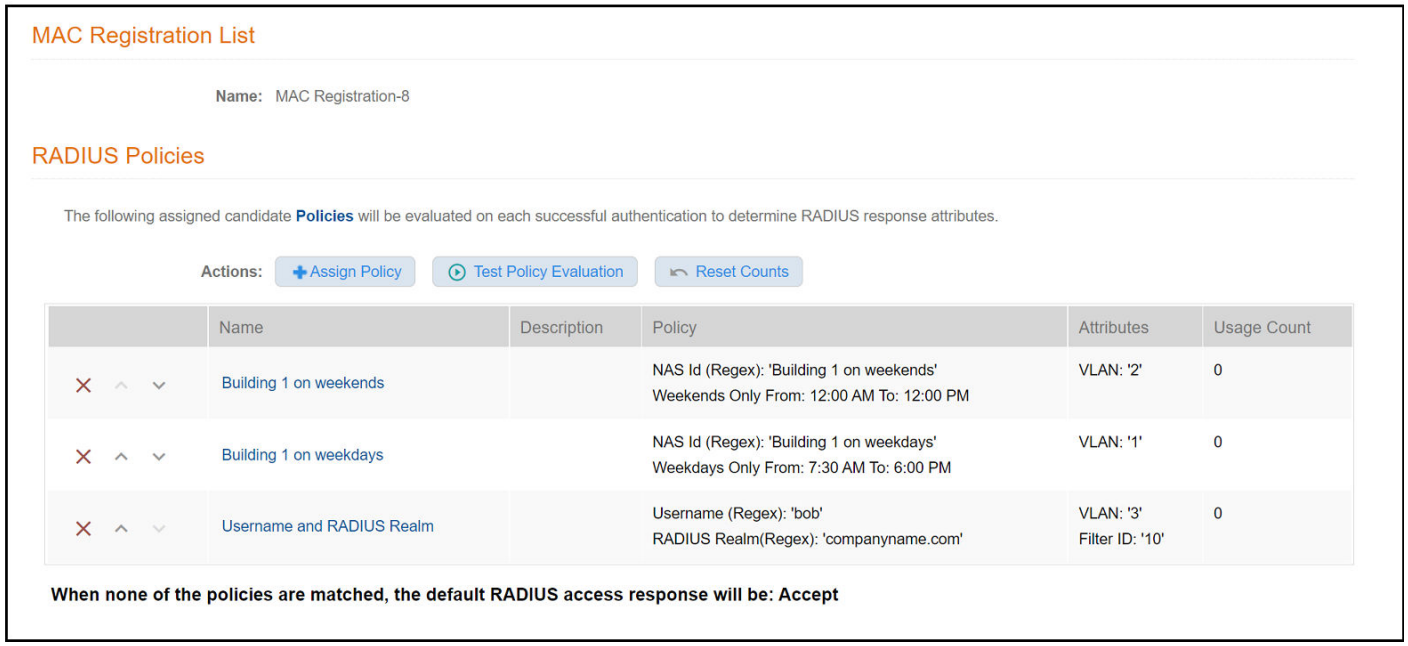
4. Select the policy you wish to add, then click **Save**.

5. Continue to add policies as you desire. If you have added all available policies, you will receive the message: " All Defined Policies have been assigned."

Policy Rules

The following illustration shows an example of how the page appears after three policies have been added:

FIGURE 25 Policies Added to MAC Registration List



- There may be many policies whose criteria are matched by a user, but the first policy that is a match is the one that gets applied. For example, if you have three policies, as shown above, the order in which you have them listed is the order in which they will be tested for matches with an enrolling user.

  NOTE
  You can use the arrows in the screen show above to list the policies in the desired order. If you want to remove a policy from being used in a specific MAC registration list, click the X next to the policy, then confirm the removal of the policy when prompted.

- Because the "Building 1 on weekends" policy is listed first, the matching criteria in that policy (listed in the Policy column) will first be checked against an enrolling user. If there is a match, the policy is applied to the user (meaning that the attributes listen in the Attributes column are applied to the user). If there is no match, the next policy ("Building 1 on weekdays") is checked against the enrolling user, and so on.

  NOTE
  If none of the policies match a specific user, the default access setting (configured when you create a MAC registration list) is used to either accept or reject the user. In the example above, at the bottom of the illustration, the default access it to accept the user because that is how the field was set when MAC Registration-8 (the example MAC registration list above) was configured.

Additional Policy Information

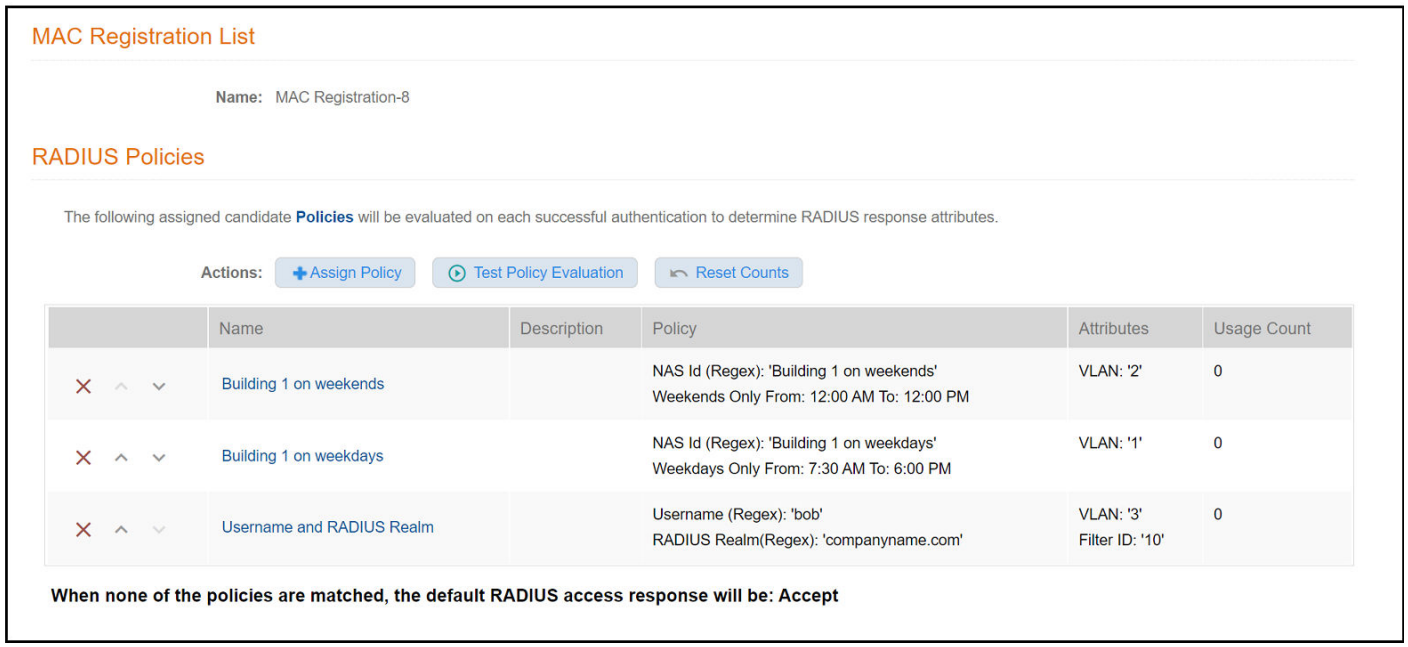
- Testing Policies..... 39
- Viewing Policy Information..... 44
- Viewing RADIUS Attribute Information..... 45

Testing Policies

You can test your policies to be sure they are working as desired before you implement them in a live environment.

The following screen shows an example of three policies that have been added to a MAC registration list. To get to this screen, go to **Configuration > MAC Registration Lists**, click the Wrench icon next to the desired MAC registration list, then click the **RADIUS Policies** tab.

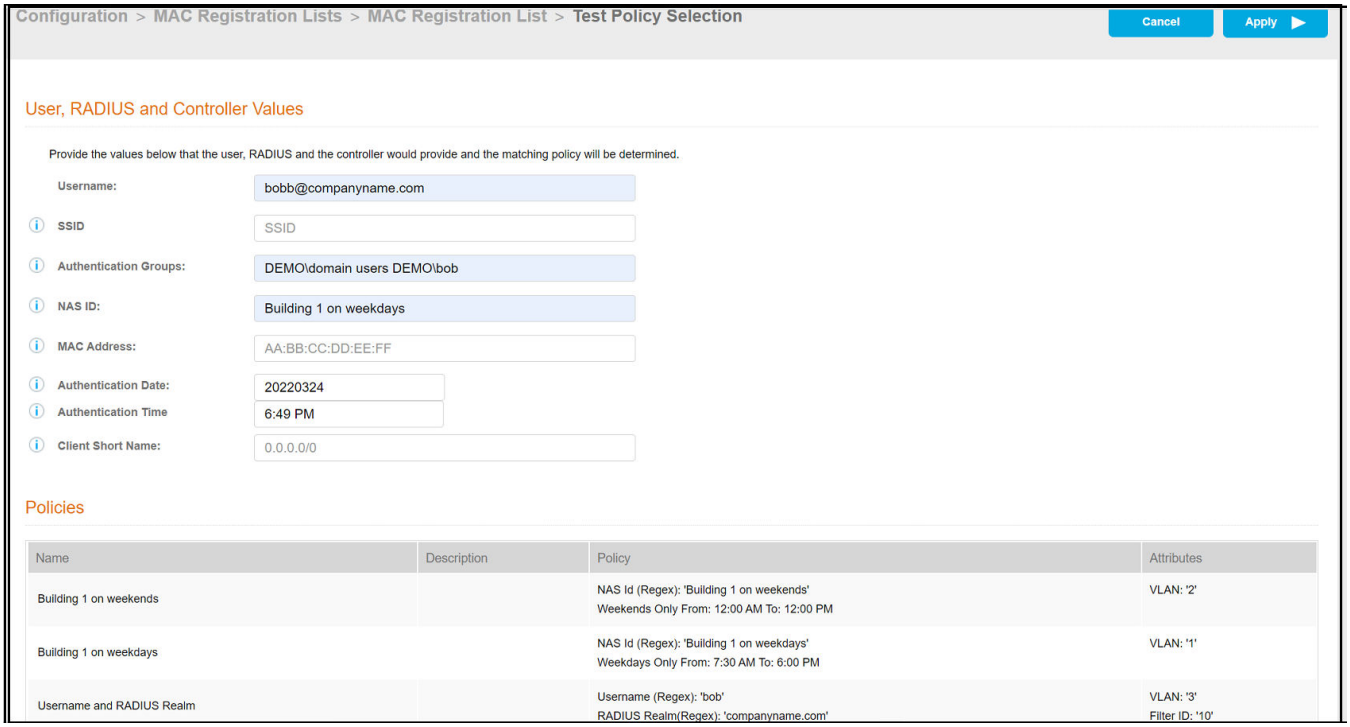
FIGURE 26 Three-Policy Example



Test Policy Evaluation - Example 1

1. Click the **Test Policy Evaluation** button (see the screen above).
2. In the ensuing Test Policy Selection screen, enter the values that would be provided during user enrollment to determine which policy, if any, is a match. The screen below contains sample values, which are described below the screen:

FIGURE 27 Test Policy Selection - Example 1 Values



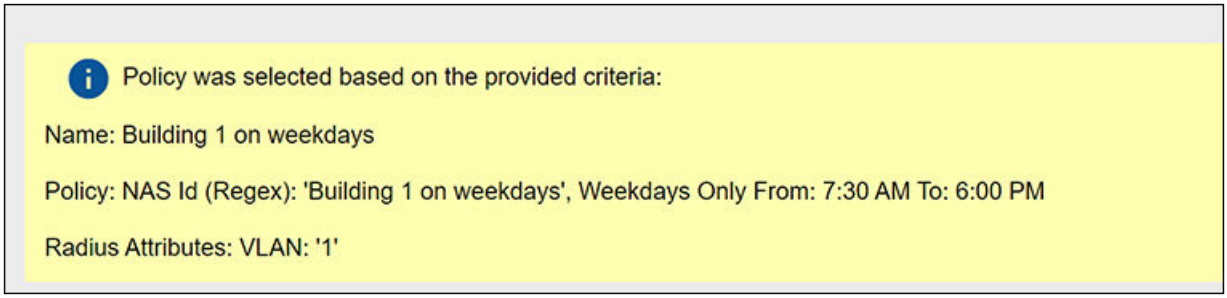
The sample values shown above have been entered to test that the "Building 1 on weekdays" policy will be applied to users who match the criteria defined by that policy (refer to the information in the "Policy" column in the figure above).

> **NOTE**
> The sample values can include fields that are not configured in a policy, and could still be a match for the policy. For example, there could be a value entered in the Client Short Name field in the example above, and it would have no impact on the results of the policy evaluation test because none of the three policies shown above show a value for Client Short Name (as evidenced by the values shown in the Policy column for each policy).

- Username (required): Must be a valid username that your Cloudpath system will accept when this user attempts enrollment.
- SSID: Matches the Wi-Fi SSID name for the connecting device. If this field is populated, this will match only the Wi-Fi based connections.
- Authentication Groups (required): The list of groups returned from a user (as configured in your authorization server; you need a workflow step that requires authentication to an authorization server for the user to have groups).
- MAC Address: The address assigned to the MAC address list that is being evaluate by the policy.
- NAS ID: The NAS ID that is expected to be returned from the controller. In the example above, the value "Building 1 on weekdays" is entered because it matches the NAS ID of the "Building 1 on weekdays" policy.
- Authentication Date: The date on which the user would attempt to authenticate. In the example above, the date is on a weekday because the "Building 1 on weekdays" policy specifies weekdays only for authentication.
- Authentication Time: The time when the user would attempt to authenticate. In the example above, the time is 5:10 p.m., which falls in the range of 7:30 a.m. to 6 p.m. that the policy specifies for authentication.
- Client Short Name: RADIUS Client-Shortname expected to be returned from the controller.

3. Before you click the **Apply** button, check the values you have entered. In the above example, the expected behavior is:
   a. The values entered in the upper portion of the screen are first compared to the policy named "Building 1 on weekends" because that is the policy listed first (see Policies section in the screen above). However, you can see that the values entered for testing do not match the conditions shown in the Policy column for the "Building 1 on weekends" policy.
   b. The values entered are next compared to the second policy in the list, which is the "Building 1 on weekdays" policy. You can see that the values entered for testing all *do* match those listed for this policy. Therefore, the expected behavior is that, when you click the **Apply** button, the "Building 1 on weekdays" will indicate a successful match, and the corresponding attributes would be applied to the enrolling user.
   c. To confirm these results, now click the **Apply** button. The following response is received:

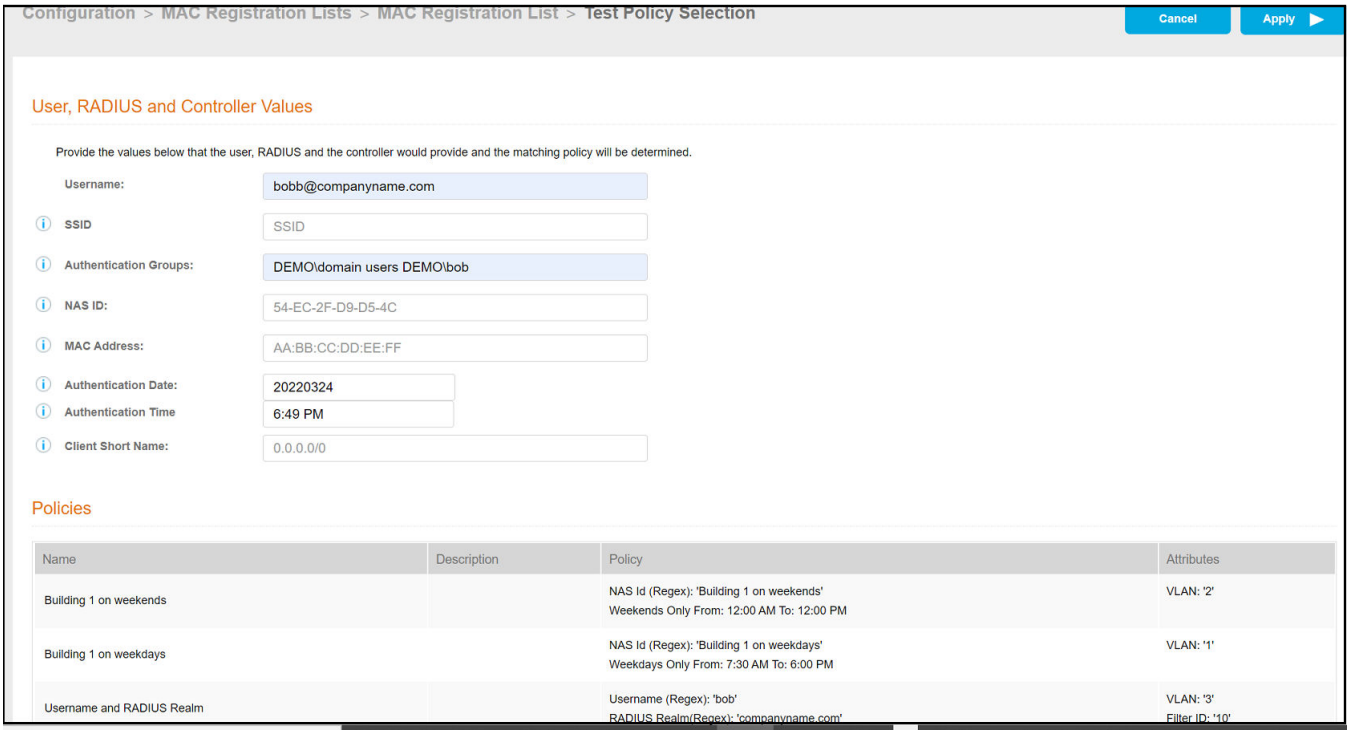
FIGURE 28 Test Policy Selection - Example 1 Results



Test Policy Evaluation - Example 2

1. Click the **Test Policy Evaluation** button.
2. In the ensuing Test Policy Selection screen, enter the values that would be provided during user enrollment to determine which policy, if any, is a match. The screen below contains sample values, which are described below the screen:

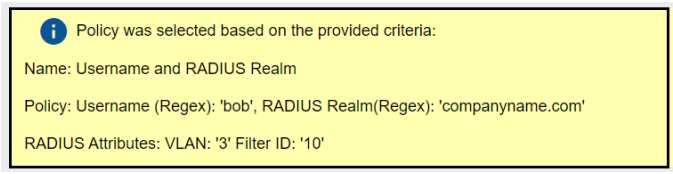
FIGURE 29 Test Policy Selection - Example 2 Values



The sample values shown above have been entered to test that the "Username and RADIUS Realm" policy will be applied to users who match the criteria defined by that policy (refer to the information in the "Policy" column in the figure above).

3. Before you click the **Apply** button, check the values you have entered. In the above example, the expected behavior is:
   a. The values you entered in the upper portion of the screen are first compared to the policy named "Building 1 on weekends" because that is the policy listed first (see Policies section in the screen above). However, you can see that the values entered for testing do not match the conditions shown in the Policy column for the "Building 1 on weekends" policy. For example, the "Building 1 on weekends" policy includes a Regex value of "Building 1 on weekends," but the sample test values entered in the screen above do not include any value for NAS ID, eliminating any chance of a match to this policy.
   b. The values entered in the upper portion of the screen are next compared to the policy named "Building 1 on weekdays" because that is the next policy listed (see Policies section in the screen above). However, you can see that the values entered for testing do not match the conditions shown in the Policy column for the "Building 1 on weekdays" policy either. For example, the "Building 1 on weekdays" policy includes a Regex value of "Building 1 on weekdays," but the sample test values entered in the screen above do not include any value for NAS ID, eliminating any chance of a match to this policy.
   c. The values entered are next compared to the third policy in the list, which is the "Username and RADIUS Realm" policy. You can see that the values entered for testing all *do* match the conditions listed for this policy: A username in the form of bob* (where the * can be replaced with any value) and a RADIUS realm (in the username field for the sample test values) in the form of companyname.com. Therefore, the expected behavior is that, when you click the **Apply** button, the "Username and RADIUS Realm" will indicate a successful match, and the corresponding attributes would be applied to the enrolling user.
   d. To confirm these results, now click the **Apply** button. The following response is received:

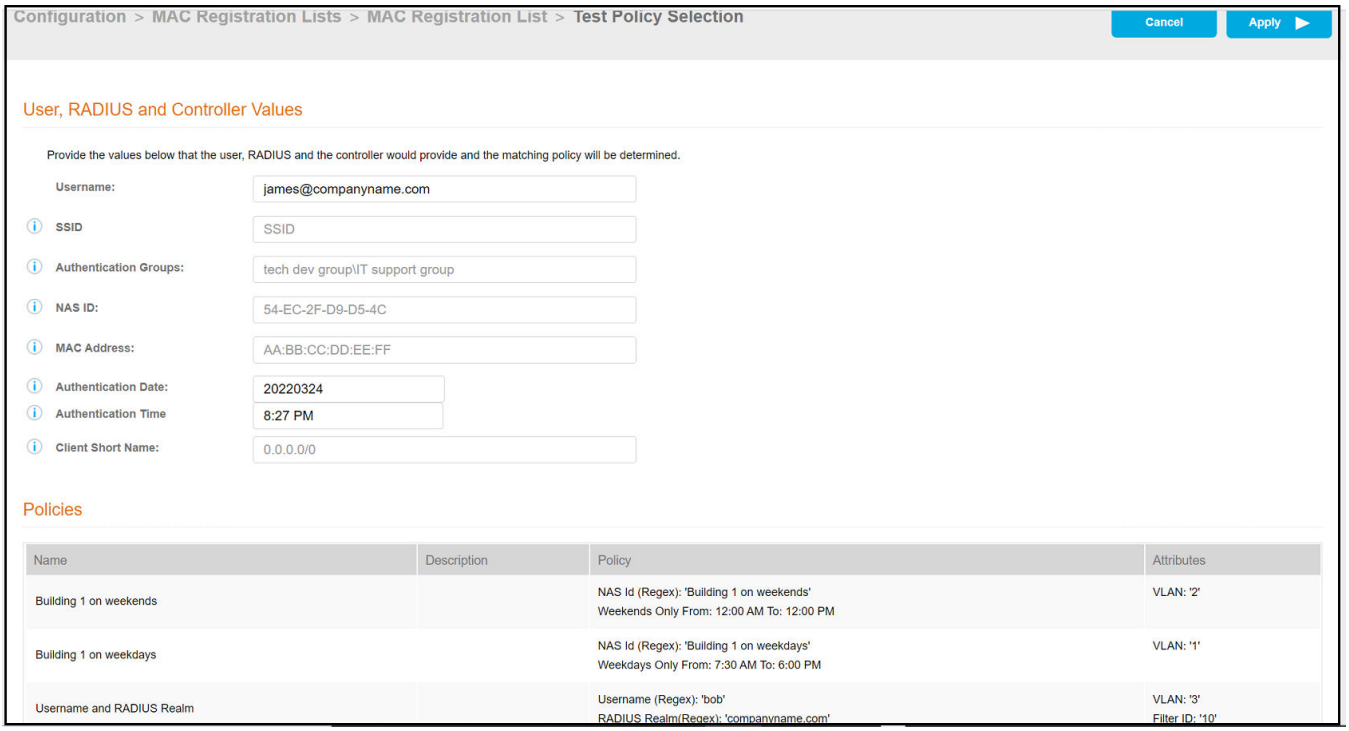
FIGURE 30 Test Policy Selection - Example 2 Results



Test Policy Evaluation - Example 3

1. Click the **Test Policy Evaluation** button.
2. In the ensuing Test Policy Selection screen, enter the values that would be provided during user enrollment to determine which policy, if any, is a match. The screen below contains sample values, which are described below the screen:

FIGURE 31 Test Policy Selection - Example 3 Values



The sample values shown above have been entered to test that no policy will be applied to users who do not match the criteria defined by any of the policies belonging to the pool (refer to the information in the "Policy" column in the figure above).

3. Before you click the **Apply** button, check the values you have entered. In the above example, the expected behavior is:
   a. The values you entered in the upper portion of the screen are first compared to the policy named "Building 1 on weekends" because that is the policy listed first (see Policies section in the screen above). However, you can see that the values entered for testing do not match the conditions shown in the Policy column for the "Building 1 on weekends" policy. For example, the "Building 1 on weekends" policy includes a Regex value of "Building 1 on weekends," but the sample test values entered in the screen above do not include any value for NAS ID, eliminating any chance of a match to this policy.

b. The values entered in the upper portion of the screen are next compared to the policy named "Building 1 on weekdays" because that is the next policy listed (see Policies section in the screen above). However, you can see that the values entered for testing do not match the conditions shown in the Policy column for the "Building 1 on weekdays" policy either. For example, the "Building 1 on weekdays" policy includes a Regex value of "Building 1 on weekdays," but the sample test values entered in the screen above do not include any value for NAS ID, eliminating any chance of a match to this policy.

c. The values entered are next compared to the third policy in the list, which is the "Username and RADIUS Realm" policy. You can see that the username does not match the conditions listed for this policy, eliminating any chance of a match to this policy. Therefore, the expected behavior is that, when you click the **Apply** button, you should receive a message indicating that no policies matched, but that the user is still accepted onto the network. provided that the " Default Access (No Match)" field was configured to "Accept" a user if there was no policy match.

d. To confirm these results, now click the **Apply** button. The following response is received:

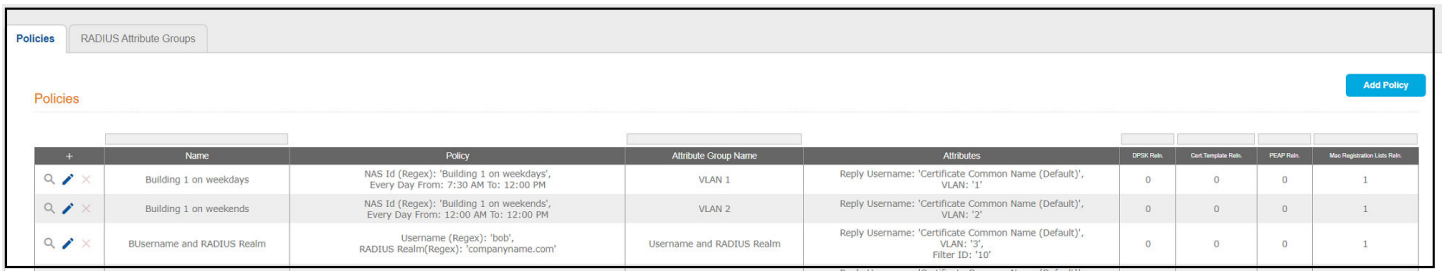
FIGURE 32 Test Policy Selection - Example 3 Results

Viewing Policy Information

To view your currently configured policies, go to **Configuration > Policies** in the UI, and be sure to highlight the **Policies** tab.

The following table shows you an example of what a policy table looks like after three different policies have been created and assigned to DPSK pools, certificate templates, PEAP, or MAC registration lists.

FIGURE 33 Policy Table Example



You can use the policy table as follows:

TABLE 14 Description of Policy Table

Column Title	Description
+	• You can view details of the policy by clicking on the magnifying glass icon. • You can edit the policy by clicking on the pencil icon. • If the policy has not yet been assigned (such as to PEAP or a DPSK pool), there will be a **X** next to the policy name. Clicking that X deletes the policy. However, in the example above, all three policies are in use; therefore the - sign denotes that you cannot delete the policy as long as it remains in use. You would first need to remove the policy from where it is being used before you can delete the policy from the table shown above.
Name	The name of the policy as configured in the Display Name field in the Policy configuration screen, an example of which is shown in Figure 3 on page 21.

TABLE 14 Description of Policy Table (continued)

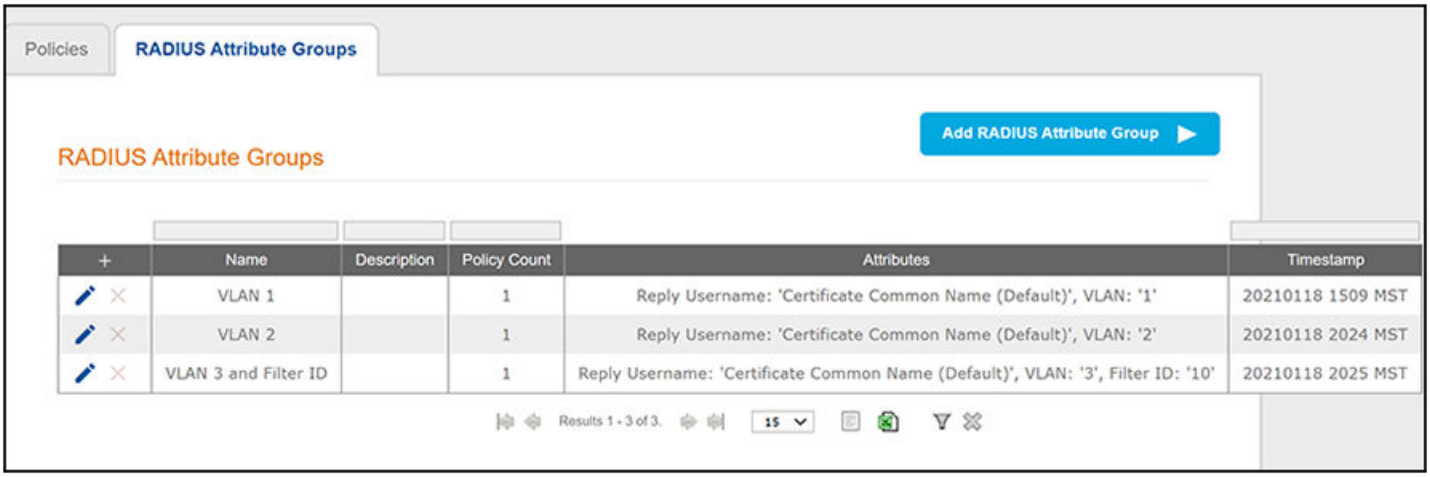
Column Title	Description
Policy	All the conditions that you set when you created the policy are listed in this column. For example, the "Building 1 on weekdays" policy conditions are the ones that were configured in the example shown in Figure 3 on page 21.
Attribute Group Name	The name of the group that has been selected in the RADIUS Attribute Group drop-down when the policy was created. For the "Building 1 on weekdays" policy shown in this example, the group name VLAN 1 matches the selection that was shown in the example in Figure 3 on page 21.
Attributes	Lists all the attributes that were set for the corresponding RADIUS attribute group name. For the "VLAN 1" attribute group name shown in this example, the attribute "VLAN 1" is listed because that is the only attribute that was set during the configuration of the VLAN 1 RADIUS attribute group name, as shown in Figure 2 on page 19. **NOTE** The "Reply Username" attribute applies only to certificate templates.
DPSK Rel, Cert Template Rel, PEAP Rel, and MAC Registration List Rel	The number of times that a policy has been assigned to each category of authentication.

Viewing RADIUS Attribute Information

To view your currently configured RADIUS attribute groups, go to **Configuration > Policies** in the UI, and be sure to select the RADIUS Attribute Groups tab.

The following table shows you an example of what a RADIUS Attribute Groups table looks like after three different RADIUS attribute groups have been created.

FIGURE 34 RADIUS Attribute Groups Example



You can use the RADIUS Attribute Groups table as follows:

TABLE 15 Description of RADIUS Attribute Groups Table

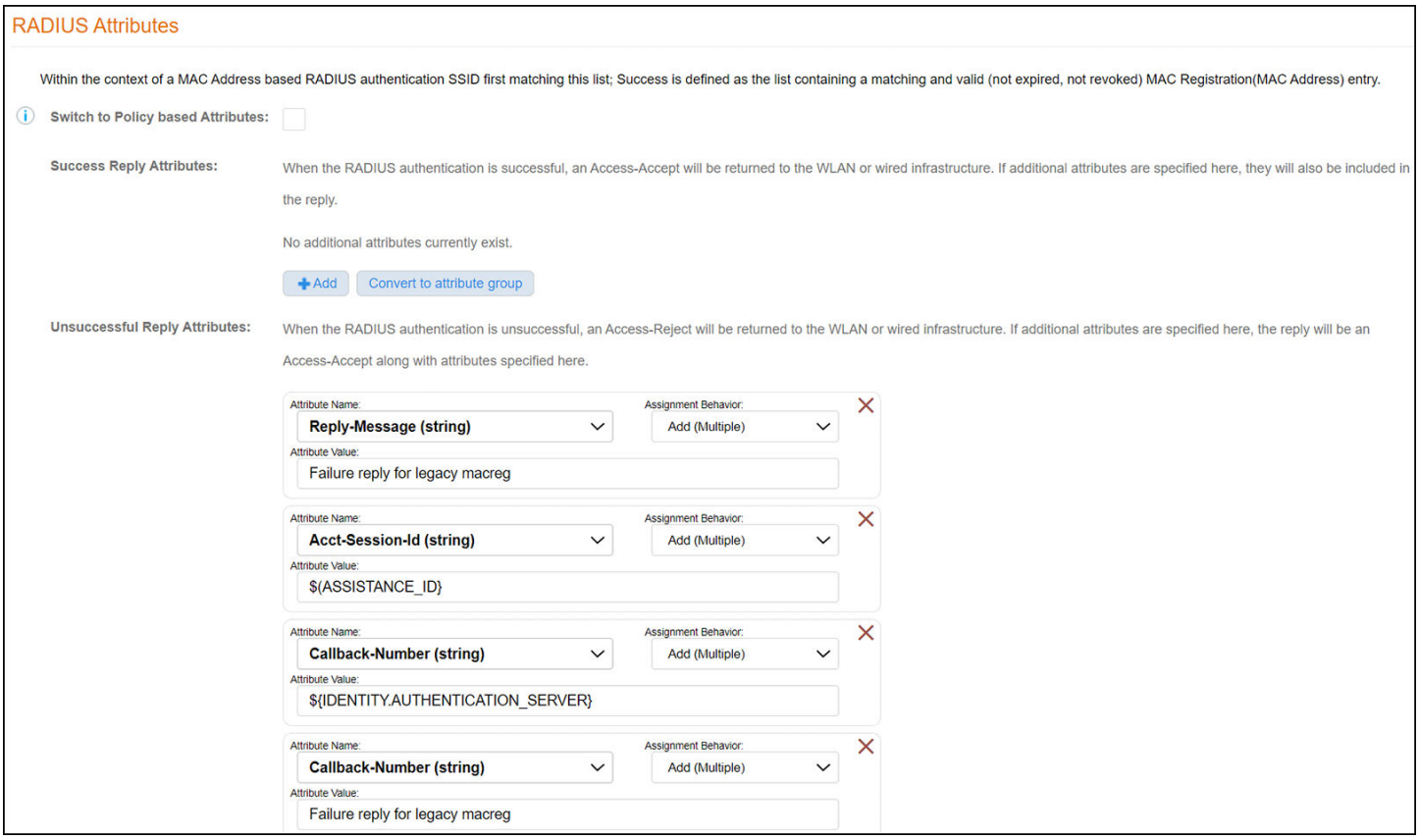
Column Title	Description
+	• You can edit the RADIUS attribute group by clicking on the pencil icon. • If the RADIUS attribute group has not yet been assigned to any policy, there will be a **X** next to the name. Clicking that X deletes the group. However, in the example screen shown above, all the groups have already been assigned to at least one policy; therefore the **X** is not selectable, which denotes that you cannot delete the group as long as it remains in use by one or more policies. You would have to edit the policy itself to remove the RADIUS attribute from the policy if you then want to delete the RADIUS attribute.
Name	The name of the RADIUS attribute group as configured in the Display Name field in the RADIUS Attribute Group configuration screen, an example of which is shown in Figure 2 on page 19.
Description	Any optional description that was entered in the configuration of the RADIUS attribute group.
Policy Count	The number of policies that the RADIUS attribute group is currently assigned to.
Attributes	Lists all the attributes that were set for the corresponding RADIUS attribute group name. For the "VLAN 1" attribute group name shown in this example, the attribute "VLAN 1" is listed because that is the only attribute that was set during the configuration of the VLAN 1 RADIUS attribute group name, as shown in Figure 2 on page 19. **NOTE** The "Reply Username" attribute applies only to certificate authentications.
Timestamp	Time that the RADIUS attribute group was created.

Switching Pre-Release-5.9R4 MAC Registration Lists to Policy-Assigned MAC Registration Lists

MAC Registration Lists are created differently in Release 5.9R4 and later from prior releases. If you have older MAC Registration lists in your system, you can continue to use them the same way in 5.9R4 or later, or you can convert them to the policy-type 5.9R4 lists that are created in Release 5.9R4 going forward. Once you switch an old MAC registration list to the new policy-type format, you cannot revert back to the pre-5.9R4 configuration.

The figure below shows an example of the RADIUS Attributes portion of a MAC registration list configured from a release prior to 5.9R4:

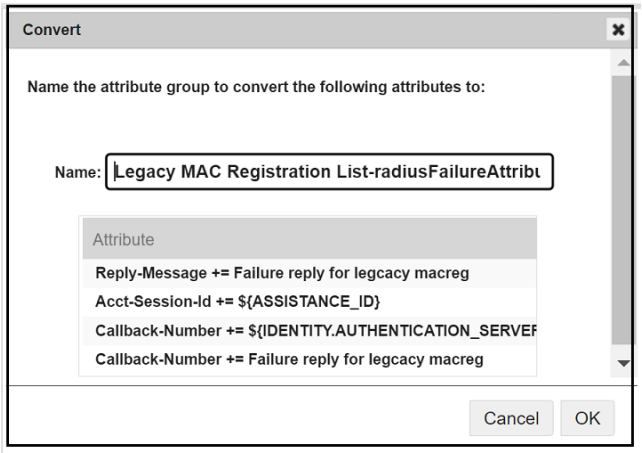
FIGURE 35 Pre-Release 5.9R4 MAC Registration List Configuration Screen - RADIUS Attributes Section



If you want to proceed with switching to the policy model, follow these steps:

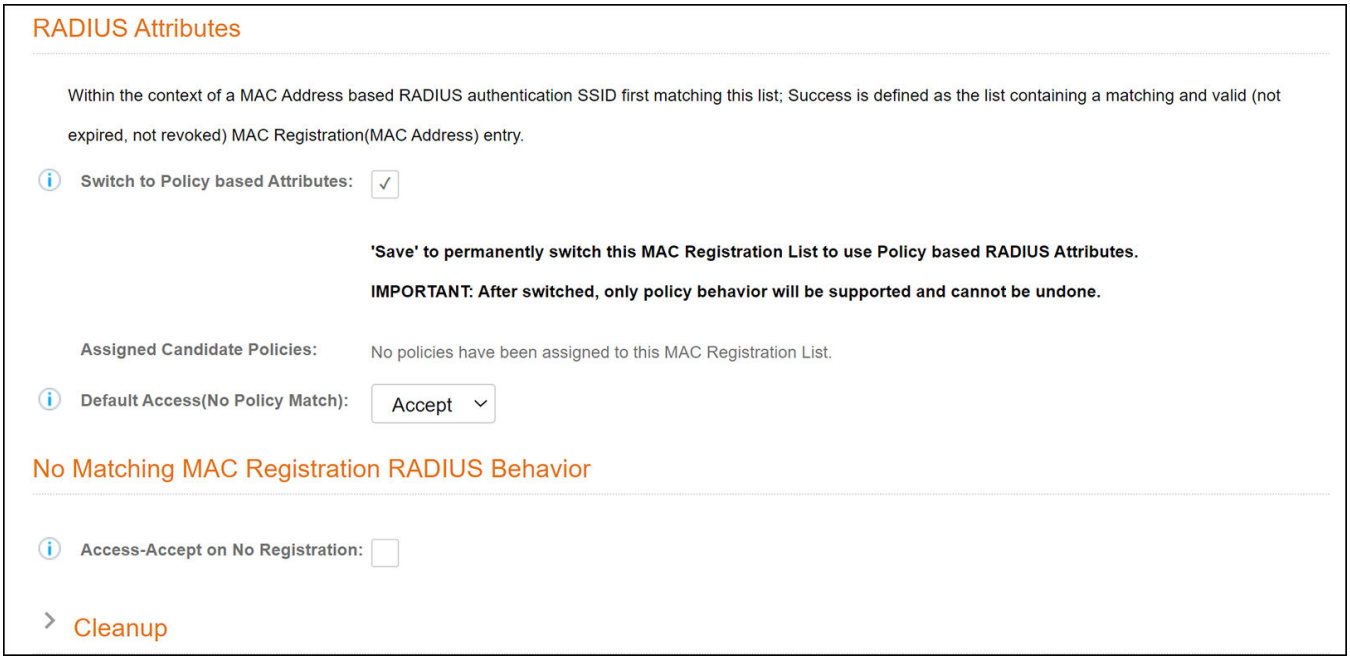
1. You can convert the existing attributes to a RADIUS attribute group by clicking the respective **Convert to attribute group** button on the screen shown above.
2. In the popup that follows, you can name the attribute group, as shown in the example below for the failure reply attributes:

FIGURE 36 Naming the RADIUS Attribute Group for Failure Replies



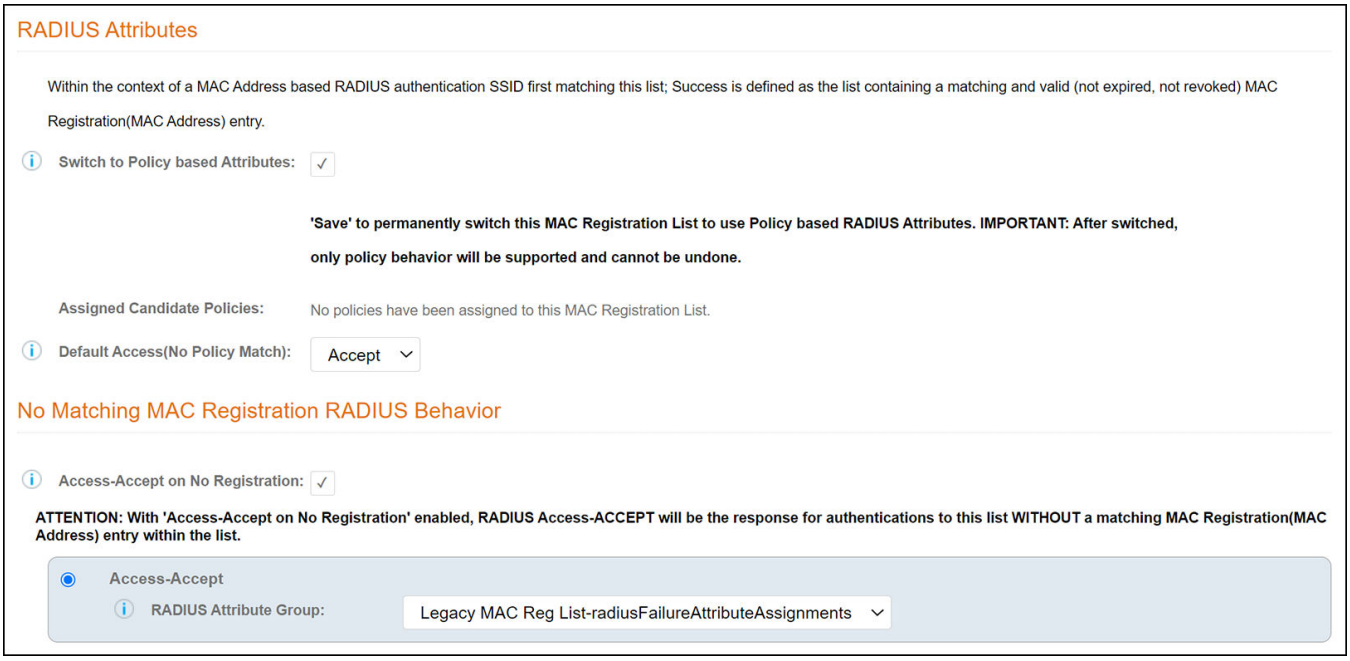
3. Click **OK**.
4. Check the "Switch to Policy-based Atttributes" box (refer to Figure 35 to view the location of the checkbox). The following screen is displayed:

FIGURE 37 New MAC Registration RADIUS Attributes Section



5. You have the option of customizing a RADIUS reply when authentication fails. To do so, check the "Access-Accept on No Registration" box (shown in the screen above).
6. From the ensuing drop-down list, select the RADIUS attribute group, as shown in the example below.

FIGURE 38 RADIUS Attribute Group Selected From Drop-Down List



7. Click **Save**.
8. Once the conversion is complete, you can select the **RADIUS Policies** tab and add any desired policies. For instructions on adding policies, see Adding Policies to a MAC Registration List on page 37.

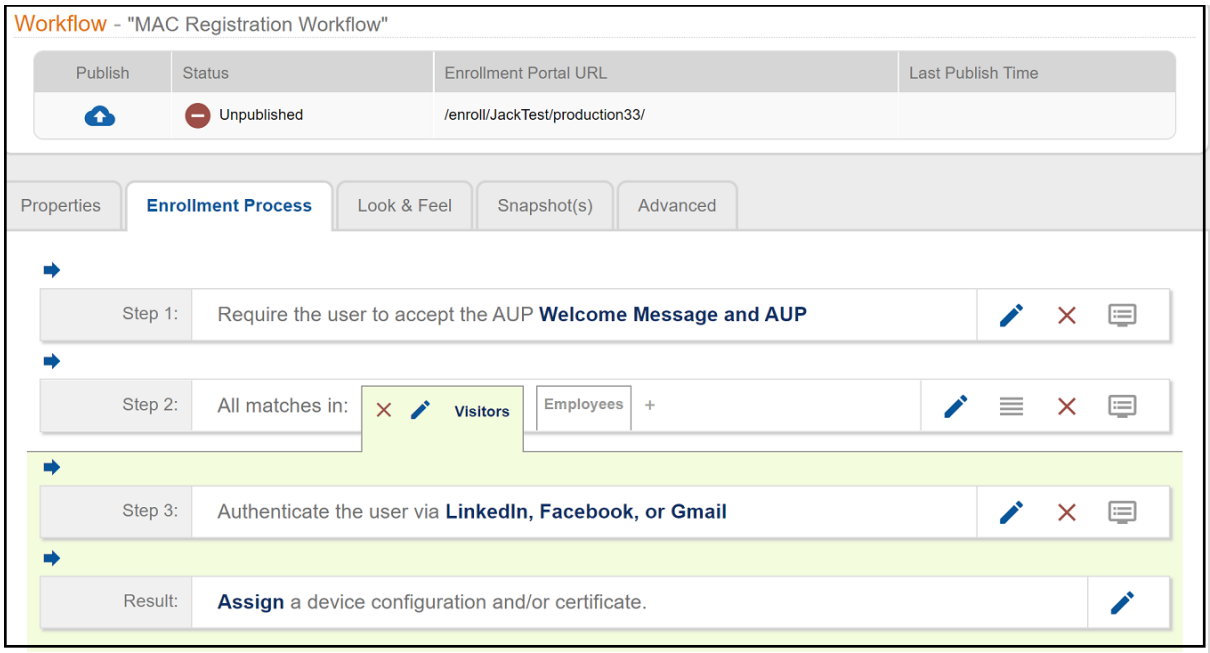
Creating a MAC Registration Workflow

NOTE

Creating a workflow is another method of adding a MAC registration list. Within a workflow, you have the option of creating a new MAC registration list or selecting an existing MAC registration list. If you want to create a registration configuration before creating your workflow, refer to Configuring MAC Registration Lists in the Cloudpath UI on page 23. During a successful enrollment process with the workflow, MAC addresses are be added to the specified MAC registration list. This section uses an example of creating a workflow split as part of the process.

1. Go to **Configuration** > **Workflow** and select **Add Workflow**.
2. With the "Create a new Workflow" button selected, click **Next**.
3. On the **Create Workflow** page, enter the new workflow information and **Save**.

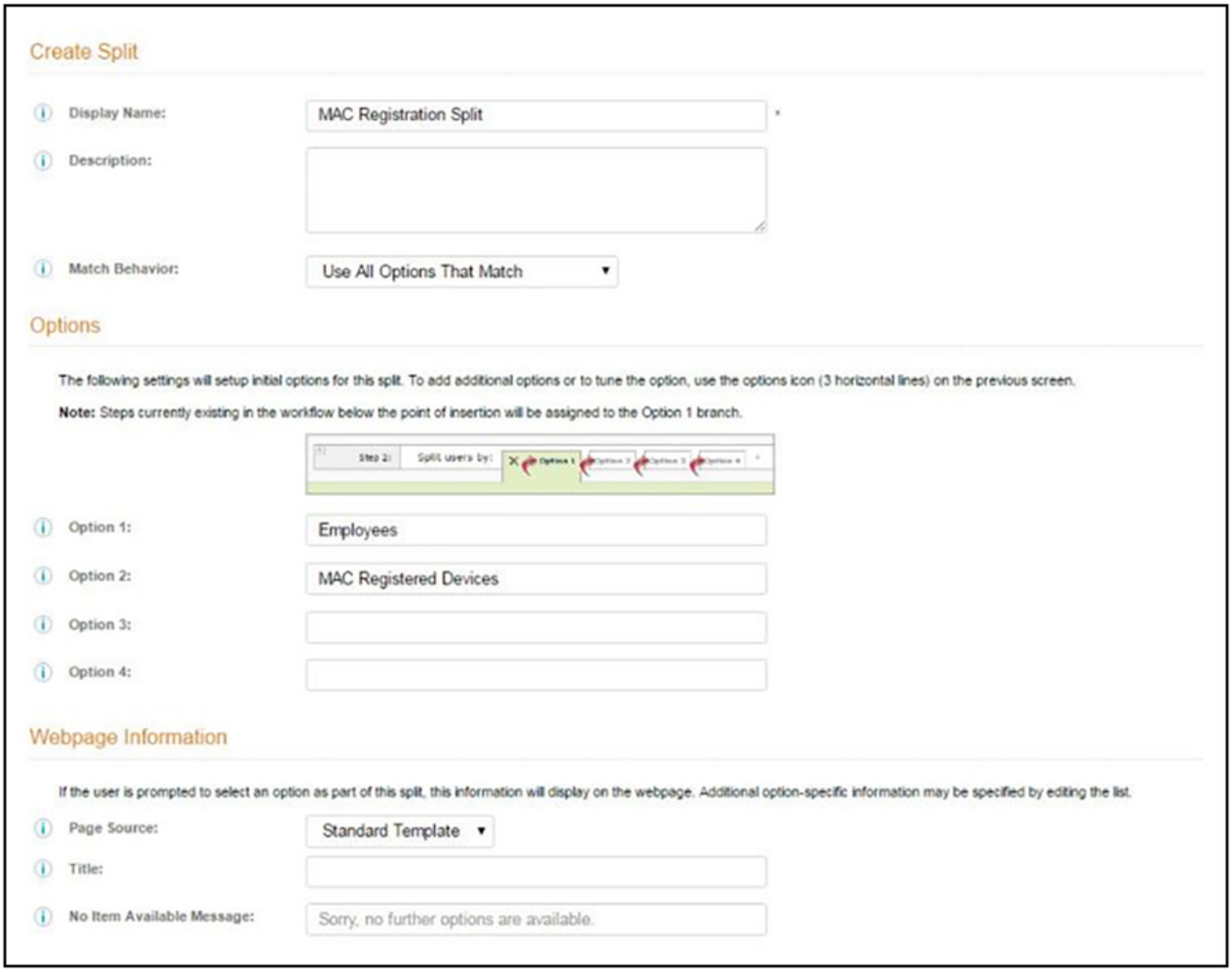
FIGURE 39 Workflow After Initial Creation



4. In the workflow (the illustration above), delete steps 2 and 3.
5. Under the **accept the AUP** workflow step, click the **Insert** arrow to create a new step.
6. On the ensuing screen that has the title of "Which Type Of Step Should Be Added?" click "Split users into different branches."

7. On the ensuing screen that has the title of "What split do you want to use?", select the desired option and click **Next**. In the example screen shown below, the assumption is that a "new split" has been selected.

   FIGURE 40 Create Split

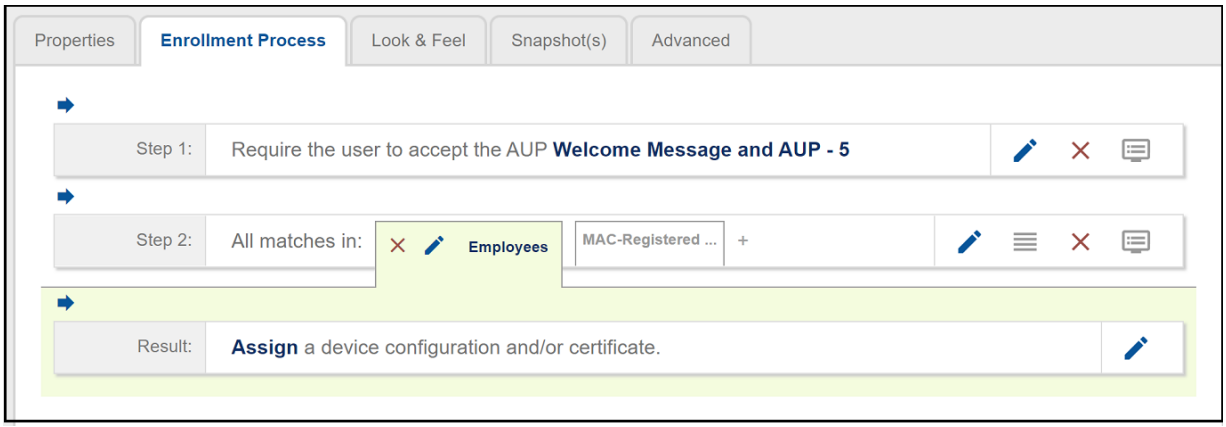


8. On the **Create Split** page, in the **Options** section, enter the names for the two workflow branches.

   For example, you can name Option 1 **Employees**, and Option 2 **MAC-Registered Devices**.

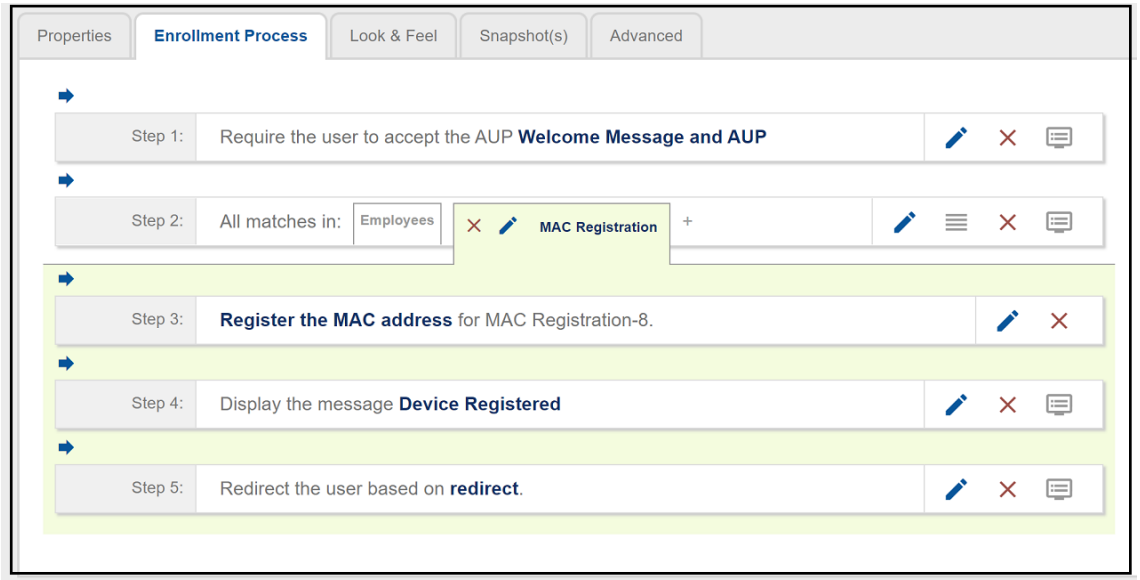
9. Leave the defaults for the other fields and **Save**. The named branches appear as tabs in the split workflow step.

FIGURE 41 MAC Registration List Example Workflow After a Split Is Created



10. Highlight the MAC-Registered Devices branch, then click the **Insert** arrow to below that step to invoke the plugin page titled "Which Type Of Step Should Be Added?"
11. Click **Register device for MAC-based authentication**.
12. You are presented with the option of creating a new MAC registration configuration or selecting an existing MAC registration list. Make your selection, then click **Next**.
13. If you choose to configure a new MAC registration, you are presented with the configuration screen. Follow the guidance in Configuring MAC Registration Lists in the Cloudpath UI on page 23. After configuring a new MAC registration list, or if you choose an existing MAC registration list, you are returned to the workflow.
14. Complete your workflow as desired. The following illustration shows a message to the enrolling user, followed by a redirect step.

FIGURE 42 Completed MAC Registration Workflow Example



Viewing MAC Registration Records on the Dashboard

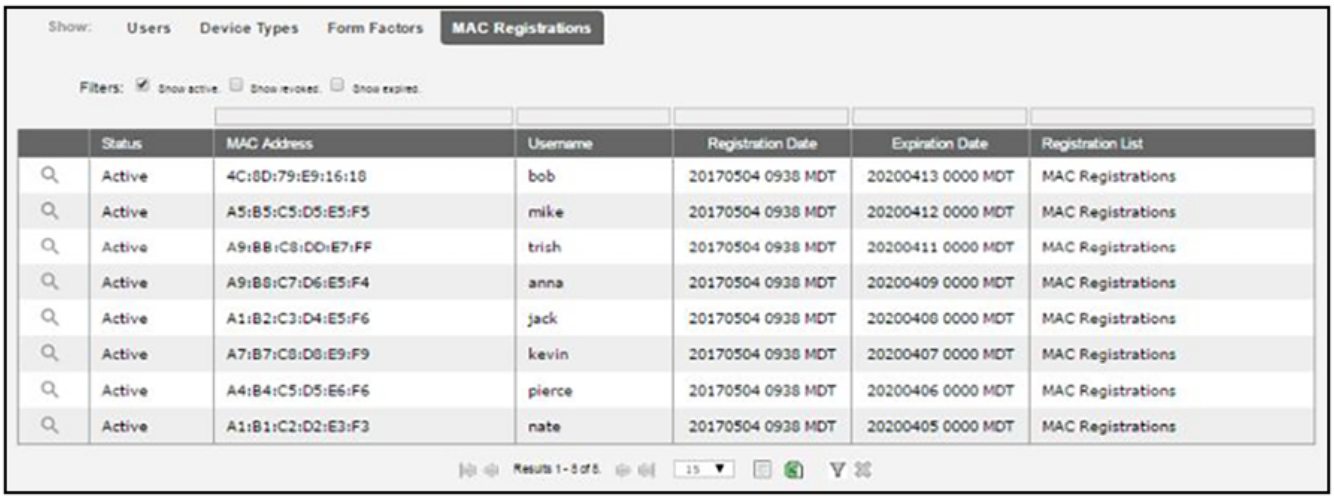
- How to View MAC Registration Records.....55
- How to Revoke Access for a MAC-Registered Device.....55

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 **Dashboard > Users And Devices**, MAC Registrations tab.
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 43 MAC Registrations on the Dashboard



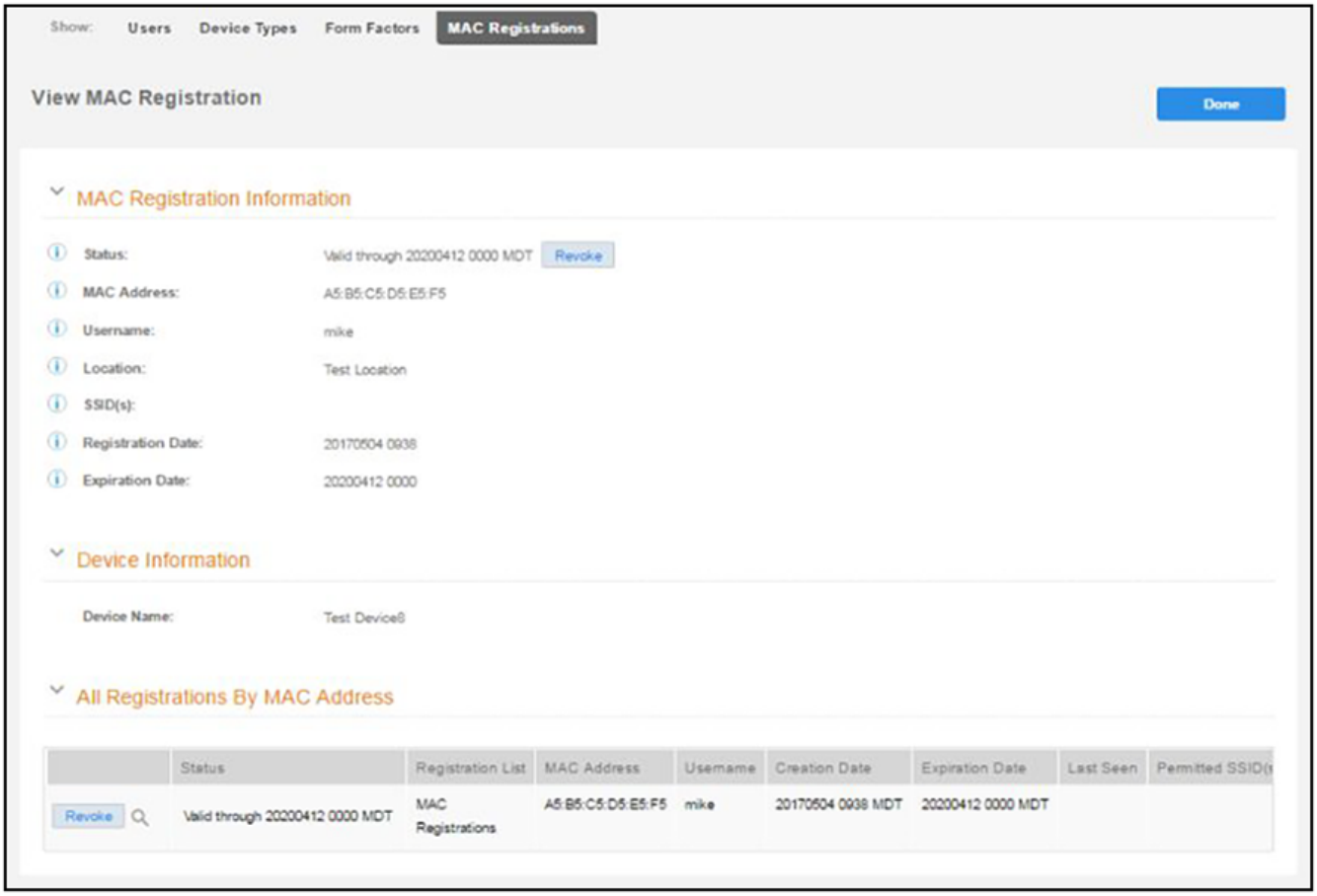
4. You can also access MAC registration information in the enrollment record. Go to **Operational** > **Dashboard** > **Enrollments** > **View Enrollment Record**.

How to Revoke Access for a MAC-Registered Device

1. Go to **Dashboard > Users & Devices**, MAC Registrations tab.

2. Click the **View** icon to view the registration information for the device.

   FIGURE 44 View MAC Registration Details



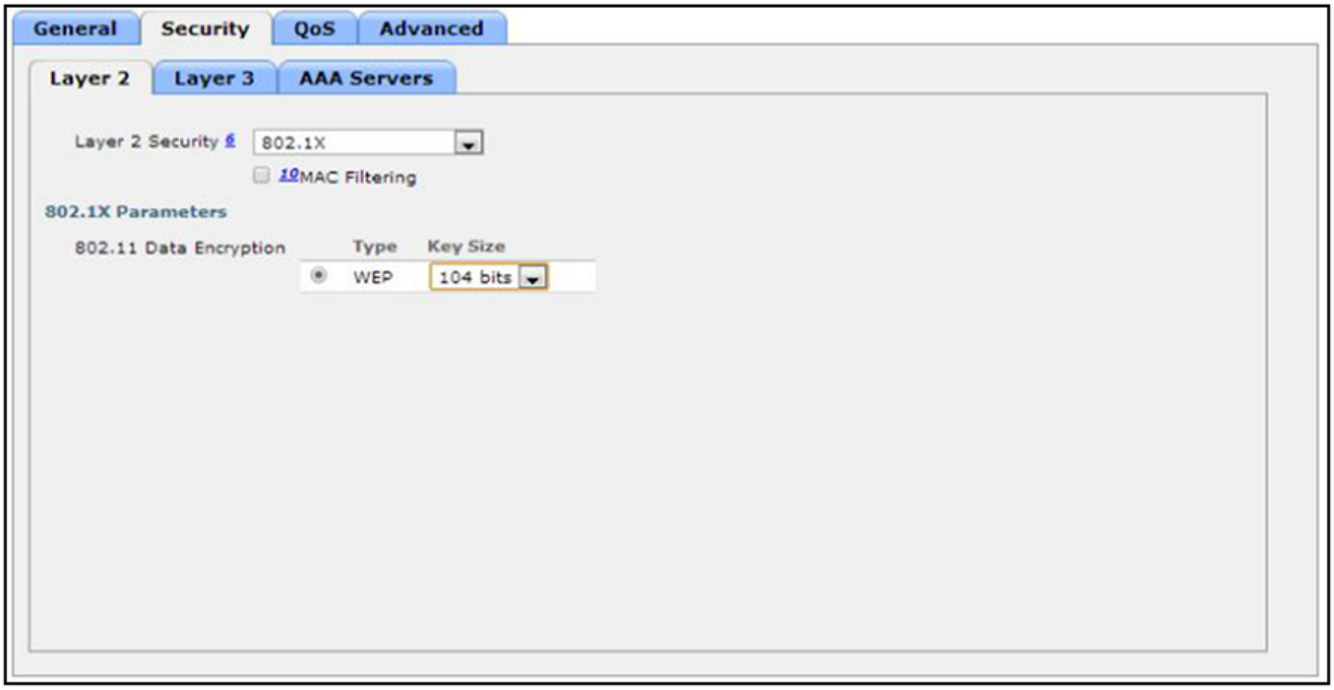
3. In the **All Registrations by MAC Devices** section, click the **Revoke** button next to the device.
4. On the **Revoke** pop-up, list the reason for revocation and click **Revoke**. The MAC address for the device is removed from the list of accepted MAC addresses in the RADIUS server.

Configuring a Cisco Controller for MAC Registration

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.

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 45 Layer 2 Security



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 46 Layer 3 Settings when Using Layer 2 Mac Filtering

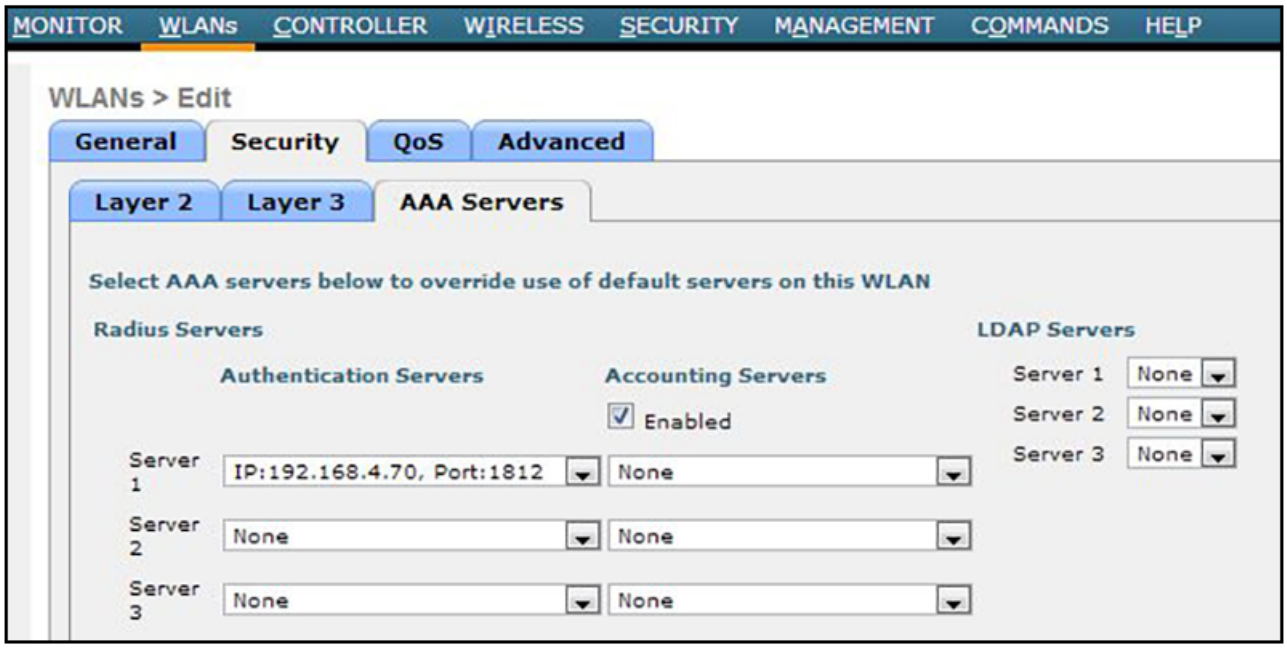
- When NOT using Layer 2 Mac Filtering: Web Policy - Authentication - If you select this option, the user is prompted for username and password while connecting the client to the wireless network.

FIGURE 47 Layer 3 Settings when Not Using Layer 2 Mac Filtering

6. Select the **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 48 Select RADIUS Server



7. **Apply** changes.

The wireless controller is configured for MAC registration against the RADIUS server.

© 2023 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com