CONFIGURATION GUIDE

Cloudpath Enrollment System MAC Registration Configuration Guide, 5.11

Supporting Cloudpath Software Release 5.11

Part Number: 800-73245-001 Rev A
Publication Date: 16 September 2022

Copyright, Trademark and Proprietary Rights Information

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

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

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.

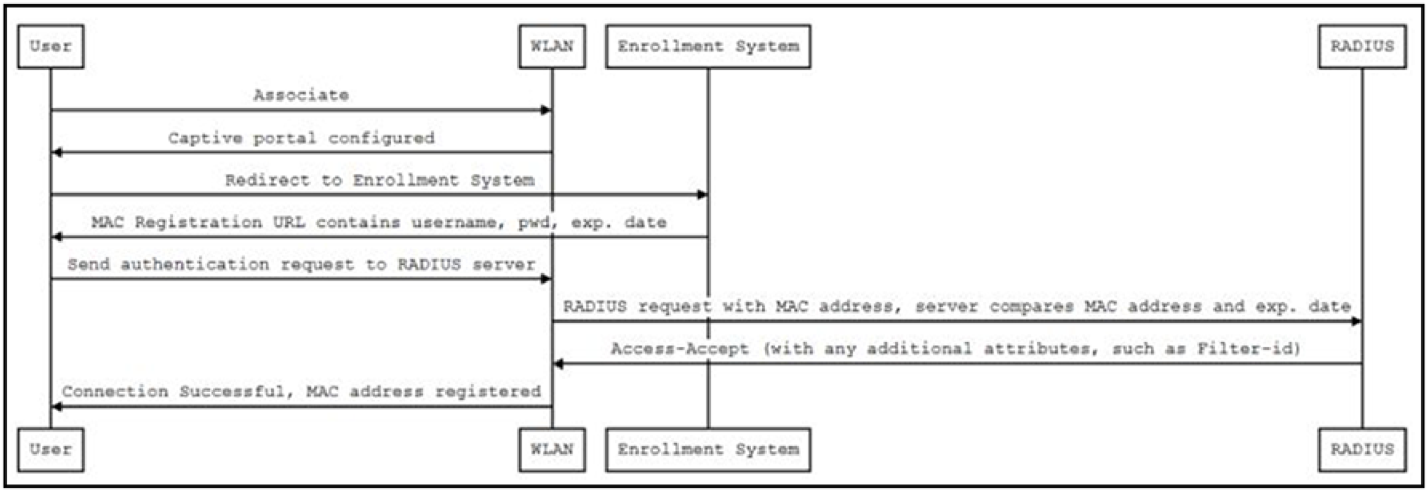
When setting up MAC registration, a list of authorized MAC addresses is maintained on the RADIUS server. When a non-802.1X device attempts to connect to the network, the request is forwarded to the RADIUS server, where the device is checked against the list of authorized MAC addresses. If the registration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


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 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 49.

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 1 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 2 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 2 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 3 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 4 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 5 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 6 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 7 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 7 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 8 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 vSmartZone 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 9 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 10 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 10 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 11 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 12 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.

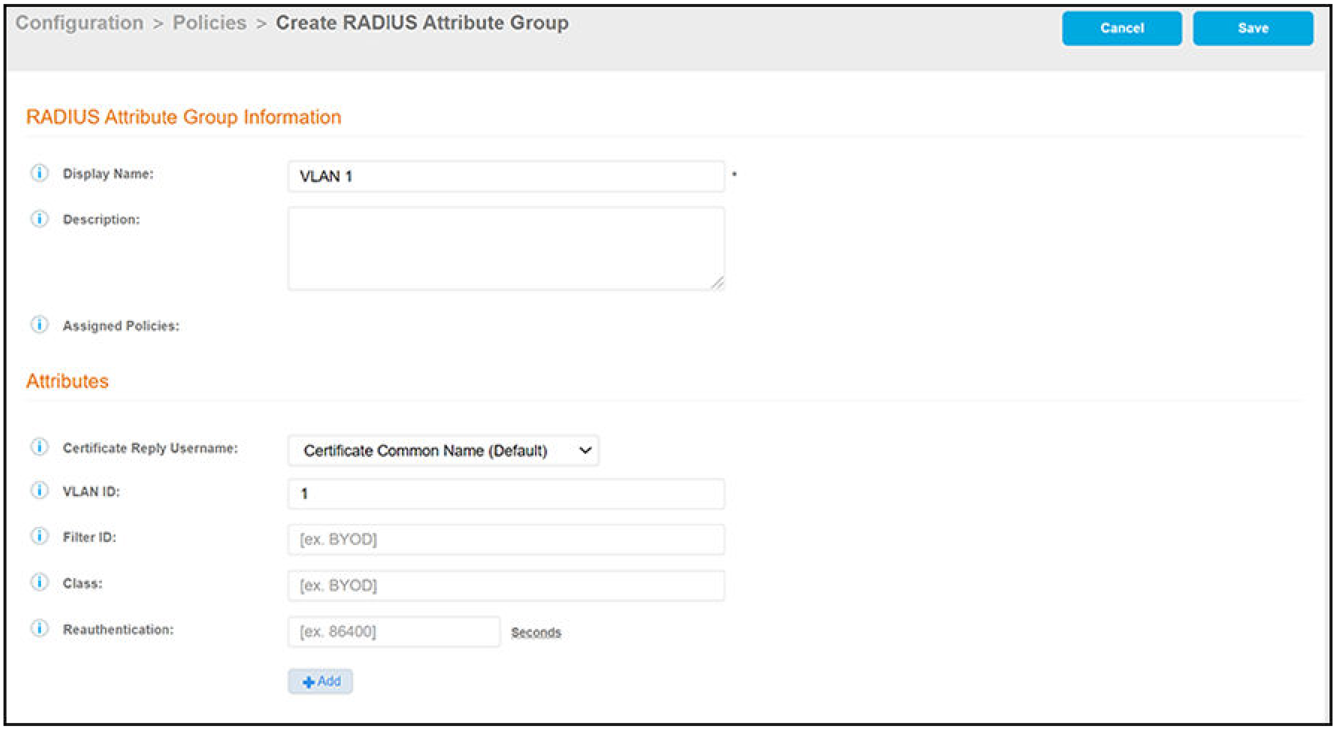
The following procedure guides you first through creating RADIUS attribute groups for your policies, then creating the policies themselves. You must create at least one RADIUS attribute group before you can configure a policy because a policy needs to have at least one RADIUS attribute group available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



RADIUS Attribute Group Information

Display Name: VLAN 1 *

Description:

Assigned Policies:

Attributes

Certificate Reply Username: Certificate Common Name (Default)

VLAN ID: 1

Filter ID: [ex. BYOD]

Class: [ex. BYOD]

Reauthentication: [ex. 86400] Seconds

- 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:

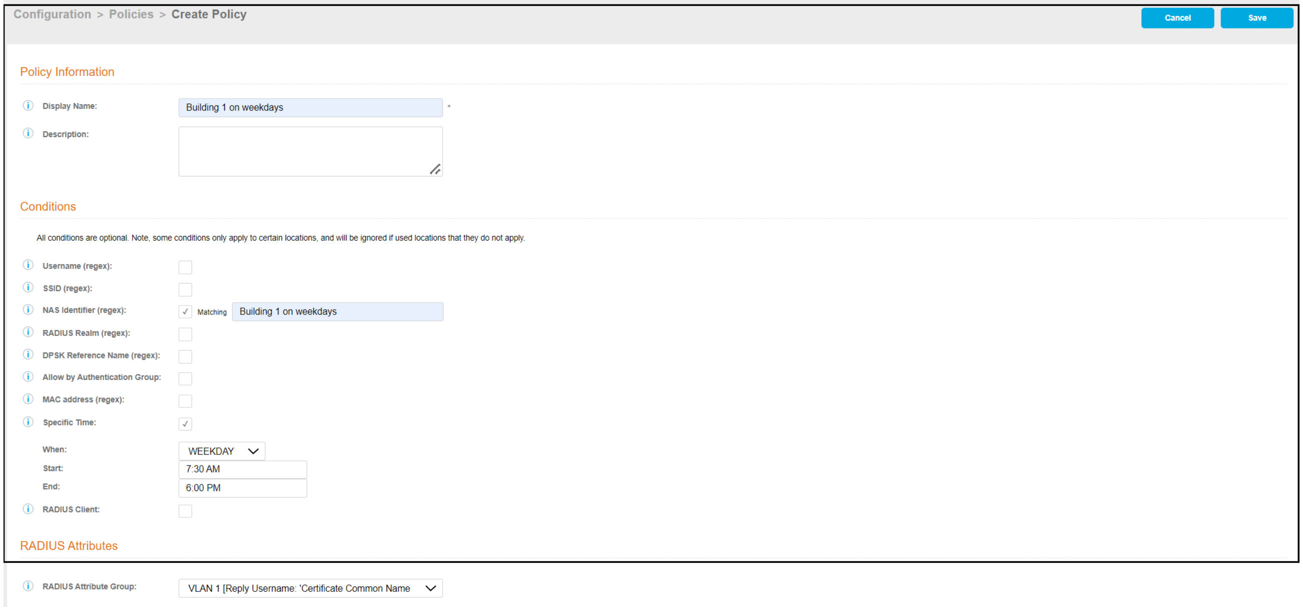
   a. In the **Configuration > Policies** area of the UI, select the **Policies** tab, then click **Add Policies**.

   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



Policy Information

Display Name: Building 1 on weekdays *

Description:

Conditions

All conditions are optional. Note, some conditions only apply to certain locations, and will be ignored if used locations that they do not apply.

Username (regex): □

SSID (regex): □

NAS Identifier (regex): ☑ Matching Building 1 on weekdays

RADIUS Realm (regex): □

DPSK Reference Name (regex): □

Allow by Authentication Group: □

MAC address (regex): □

Specific Time: ☑

When: WEEKDAY

Start: 7:30 AM

End: 6:00 PM

RADIUS Client: □

RADIUS Attributes

RADIUS Attribute Group: VLAN 1 [Reply Username: 'Certificate Common Name

- 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.

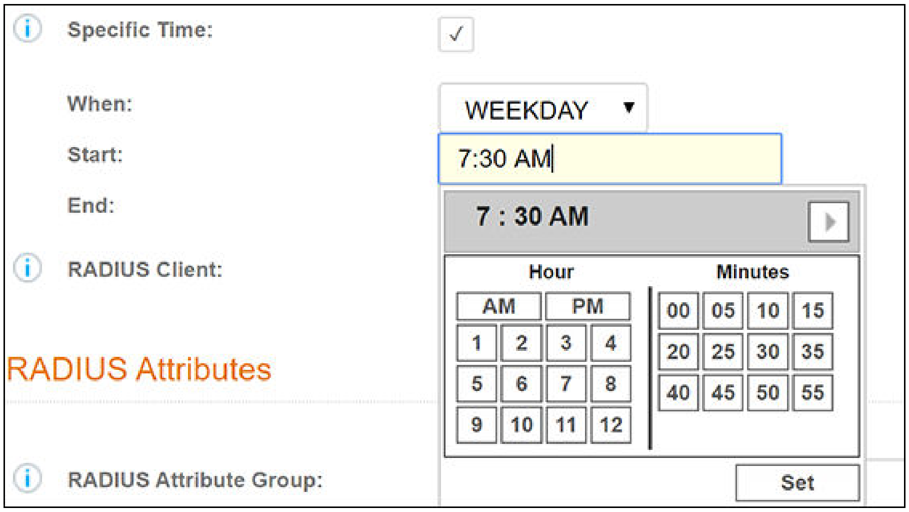
    NOTE
    If you use this field, and no NAS Identifier is provided in the response, the policy will be "false" and will not get applied to a user.

  - 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



Specific Time: ✓

When: WEEKDAY

Start: 7:30 AM

End:

RADIUS Client:

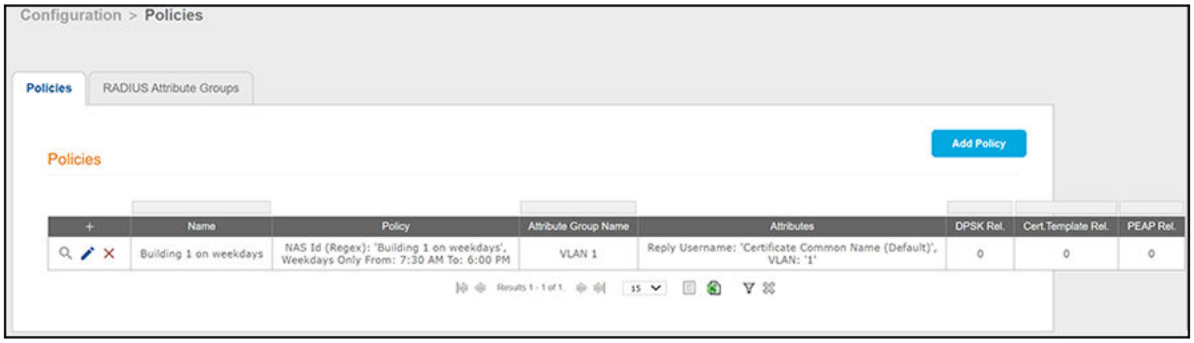
RADIUS Attributes

RADIUS Attribute Group:

- 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



Configuration > Policies

Policies

+	Name	Policy	Attribute Group Name	Attributes	DPSK Rel.	Cert.Template Rel.	PEAP Rel.
🔍 ✎ ✕	Building 1 on weekdays	NAS Id (Regex): 'Building 1 on weekdays', Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN 1	Reply Username: 'Certificate Common Name (Default)', VLAN: '1'	0	0	0

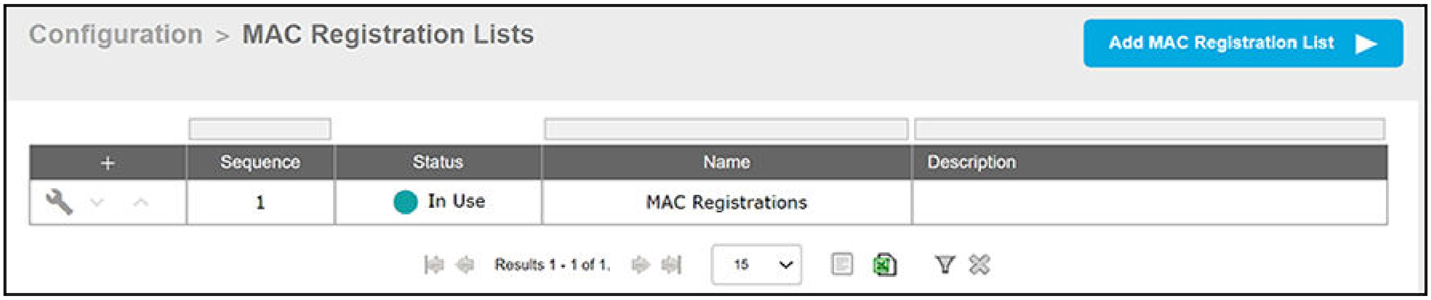
Results 1 - 1 of 1. 15

Configuring MAC Registration Lists in the Cloudpath UI

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 is in use in a workflow (see the Status column).

FIGURE 6 MAC Registrations Lists Main Screen


Configuration > MAC Registration Lists
Add MAC Registration List
Results 1 - 1 of 1.
15

+	Sequence	Status	Name	Description
	1	● In Use	MAC Registrations	

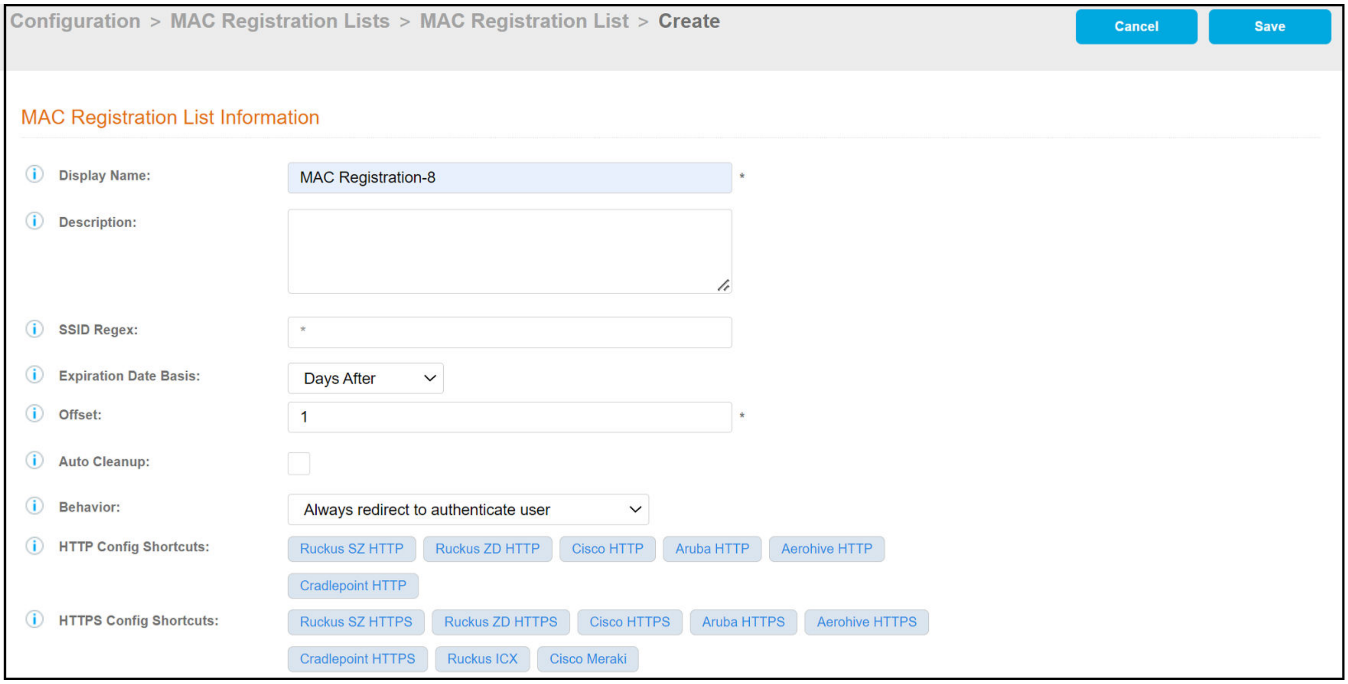
Adding a New MAC Registration Configuration

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



MAC Registration List Information

Display Name: MAC Registration-8 *

Description:

SSID Regex: *

Expiration Date Basis: Days After

Offset: 1 *

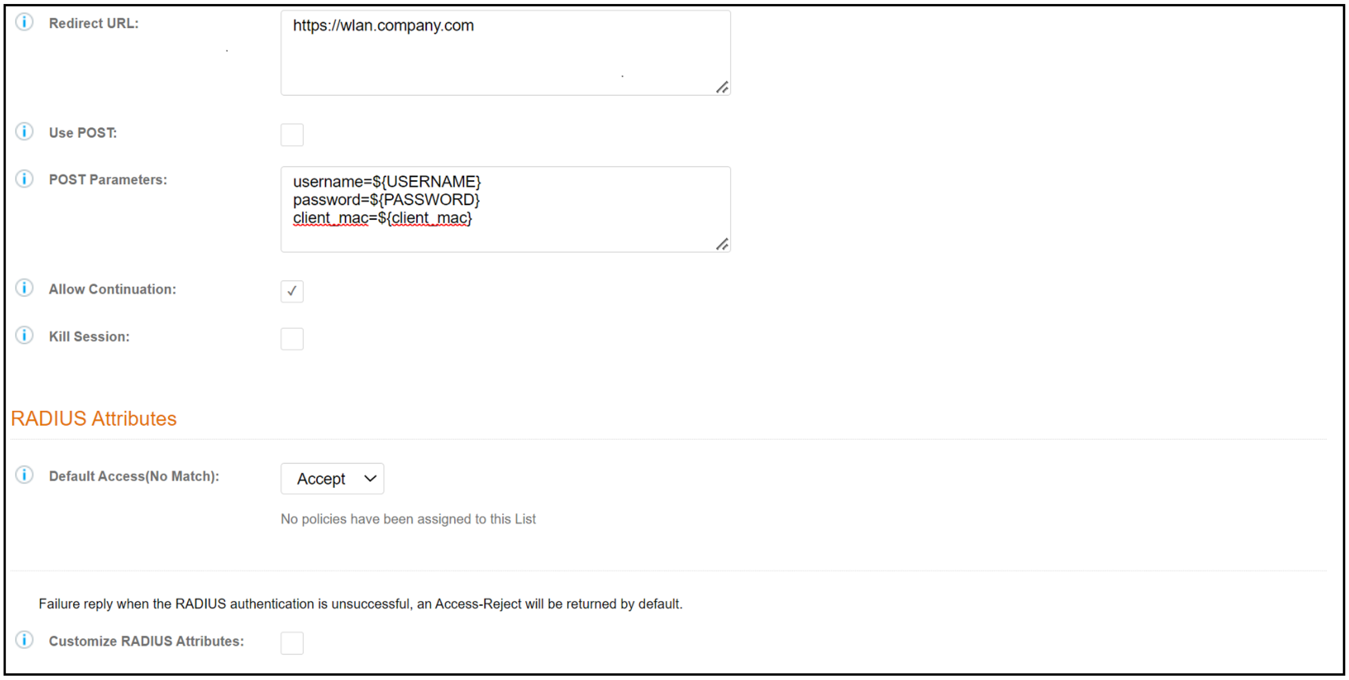
Auto Cleanup: □

Behavior: Always redirect to authenticate user

HTTP Config Shortcuts:

HTTPS Config Shortcuts:

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



Redirect URL: https://wlan.company.com

Use POST: □

POST Parameters:
username=${USERNAME}
password=${PASSWORD}
client_mac=${client_mac}

Allow Continuation: ☑

Kill Session: □

RADIUS Attributes

Default Access(No Match): Accept

No policies have been assigned to this List

Failure reply when the RADIUS authentication is unsuccessful, an Access-Reject will be returned by default.

Customize RADIUS Attributes: □

- Display Name: Any descriptive name you want.
- Description: Optional description of this particular MAC registration configuration.
- 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.

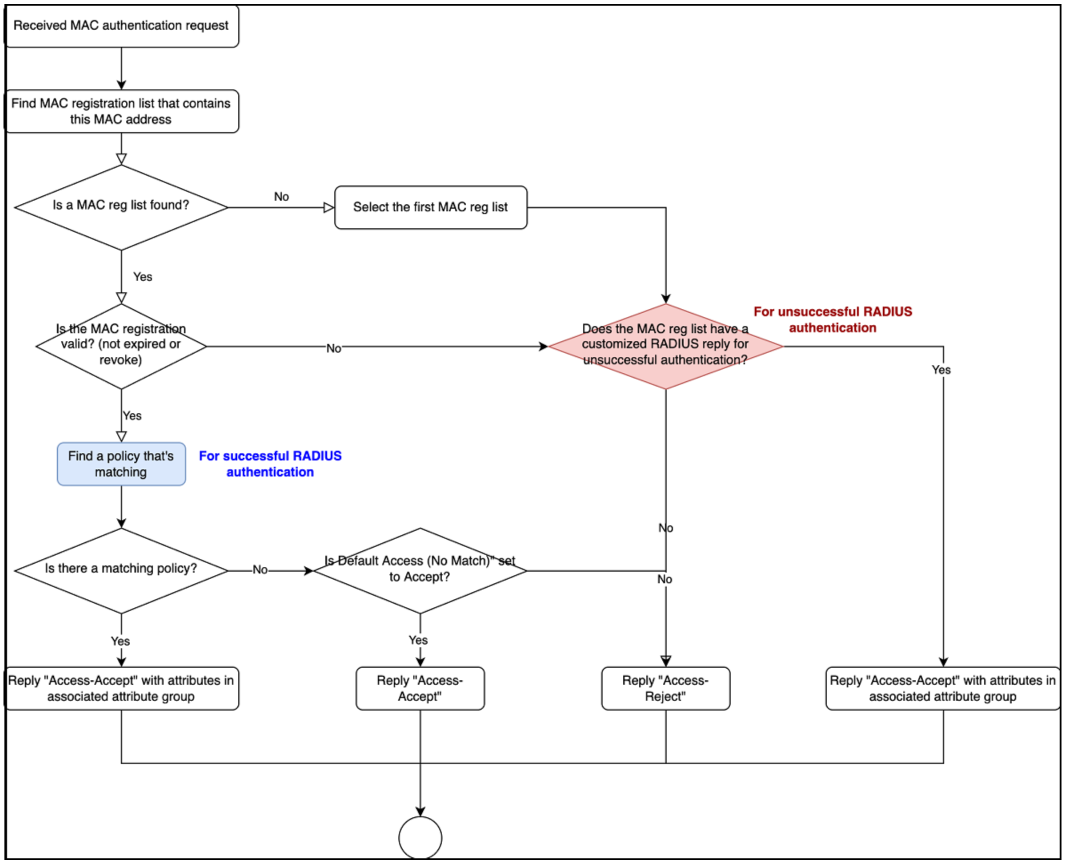
- Behavior: Specifies the prompt and redirect settings for the MAC registration configuration. Behavior settings include:
  - Prompt user when MAC is unknown.
  - Always prompt the user.
  - Redirect when MAC is unknown.
  - Always redirect to authenticate user. (This is the default and the most commonly 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):
  - Default Access (No 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 will be shown in the screen.

  - Customize RADIUS Attributes: By default, the RADIUS server sends an “Access-Reject” reply if authentication fails. You may use the “Customize RADIUS Attributes" feature to customize the RADIUS attributes reply when the RADIUS authentication is unsuccessful. If you check this box, a drop-down list of all configured RADIUS attribute groups appears; 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.

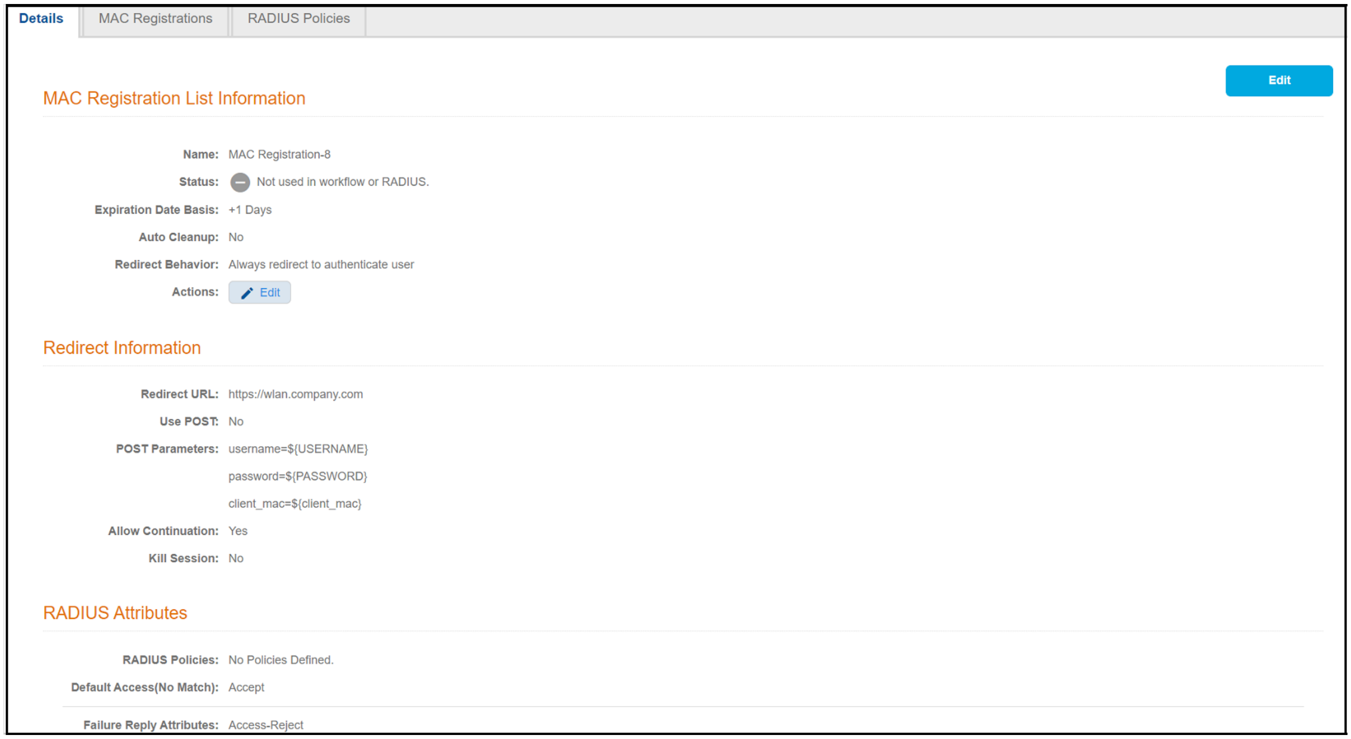
    NOTE
    The RADIUS authentication is unsuccessful if the MAC address is not presented in the registration list, or if it is presented in the registration list as either "revoked" or "expired."

FIGURE 9 RADIUS Attributes Flowchart


Received MAC authentication request
Find MAC registration list that contains this MAC address
Is a MAC reg list found?
No
Select the first MAC reg list
Yes
Is the MAC registration valid? (not expired or revoke)
No
Does the MAC reg list have a customized RADIUS reply for unsuccessful authentication?
For unsuccessful RADIUS authentication
Yes
Yes
Find a policy that's matching
For successful RADIUS authentication
No
Is there a matching policy?
No
Is Default Access (No Match)" set to Accept?
No
Yes
Yes
Reply "Access-Accept" with attributes in associated attribute group
Reply "Access-Accept"
Reply "Access-Reject"
Reply "Access-Accept" with attributes in associated attribute group

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

FIGURE 10 Three-Tab View for Newly Added Mac Registration List



MAC Registration List Information

Name: MAC Registration-8
Status: Not used in workflow or RADIUS.
Expiration Date Basis: +1 Days
Auto Cleanup: No
Redirect Behavior: Always redirect to authenticate user
Actions: Edit

Redirect Information

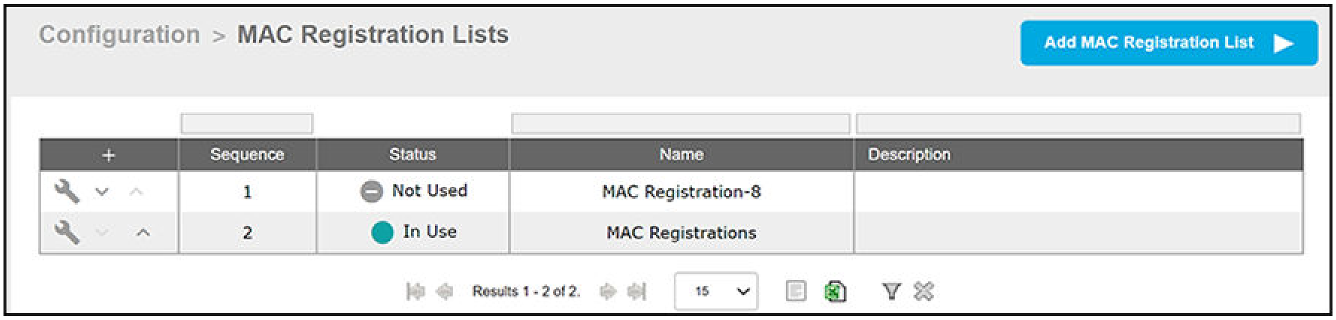
Redirect URL: https://wlan.company.com
Use POST: No
POST Parameters: username=${USERNAME}
password=${PASSWORD}
client_mac=${client_mac}
Allow Continuation: Yes
Kill Session: No

RADIUS Attributes

RADIUS Policies: No Policies Defined.
Default Access(No Match): Accept
Failure Reply Attributes: Access-Reject

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 11 MAC Registration Lists Screen After Adding a Second Registration Configuration


Configuration > MAC Registration Lists
Add MAC Registration List
Results 1 - 2 of 2.
15

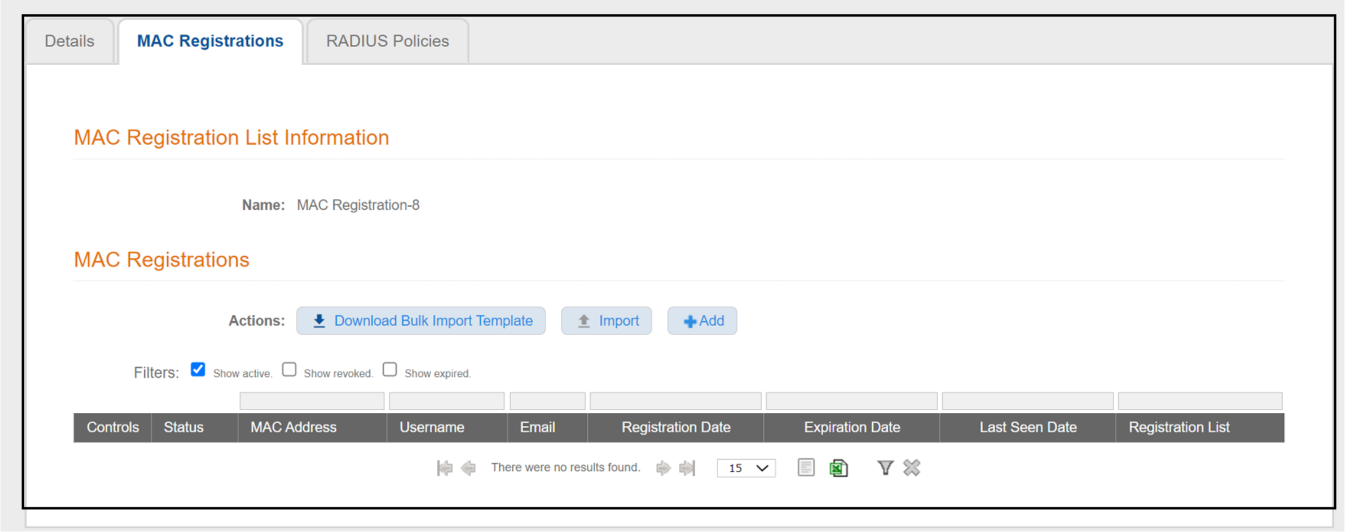
+	Sequence	Status	Name	Description
	1	Not Used	MAC Registration-8	
	2	In Use	MAC Registrations	

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 12 MAC Registrations Tab of a MAC Registration List



Name: MAC Registration-8

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

Controls	Status	MAC Address	Username	Email	Registration Date	Expiration Date	Last Seen Date	Registration List

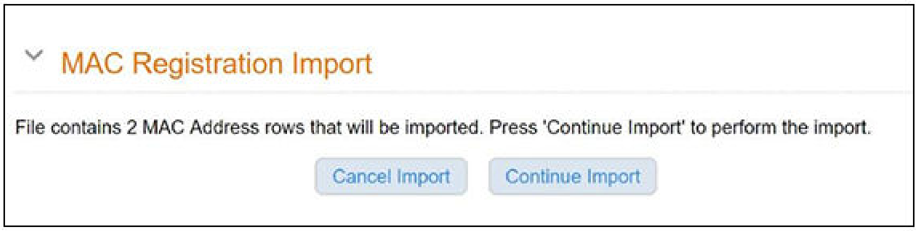
There were no results found.

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 13 Popup Asking You to Confirm Import of MAC Address List File



File contains 2 MAC Address rows that will be imported. Press 'Continue Import' to perform the import.

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 12 on page 26), 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.

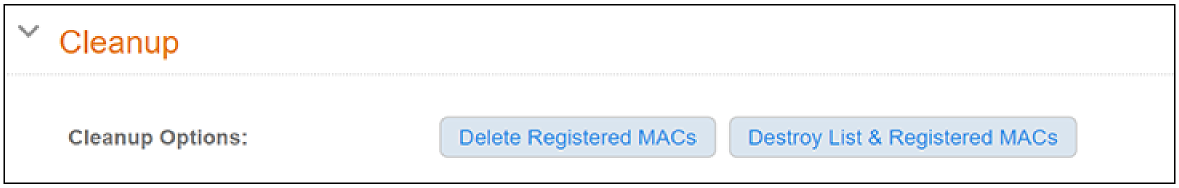
   You are returned to the MAC Registrations tab, and there should be a confirmation message at the top, indicating that the MAC addresses have been successfully added. They will also appear at the bottom of that screen.

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 14 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 Policies to a MAC Registration List

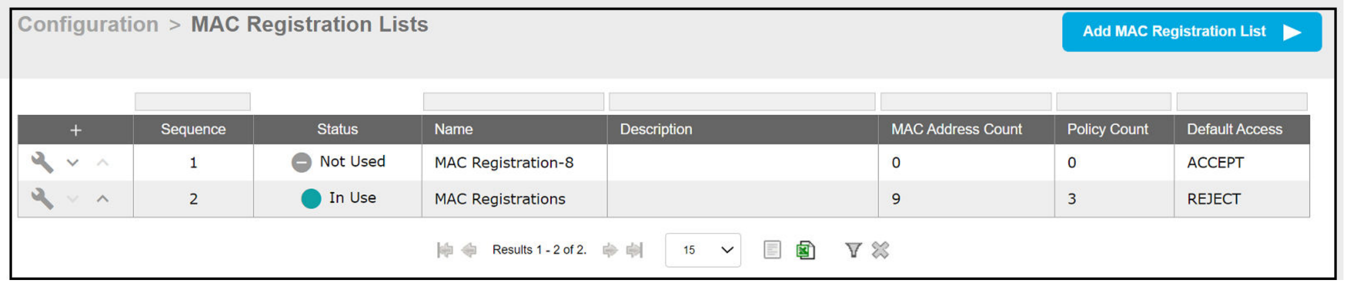
You can add as many policies as you want; policies are evaluated in the order they are listed, and the RADIUS attributes of the first matching policy are used. For a user to successfully connect to the network, the user must be a match for at least one policy (or you can allow users to connect even if 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 15 MAC Registration Lists View

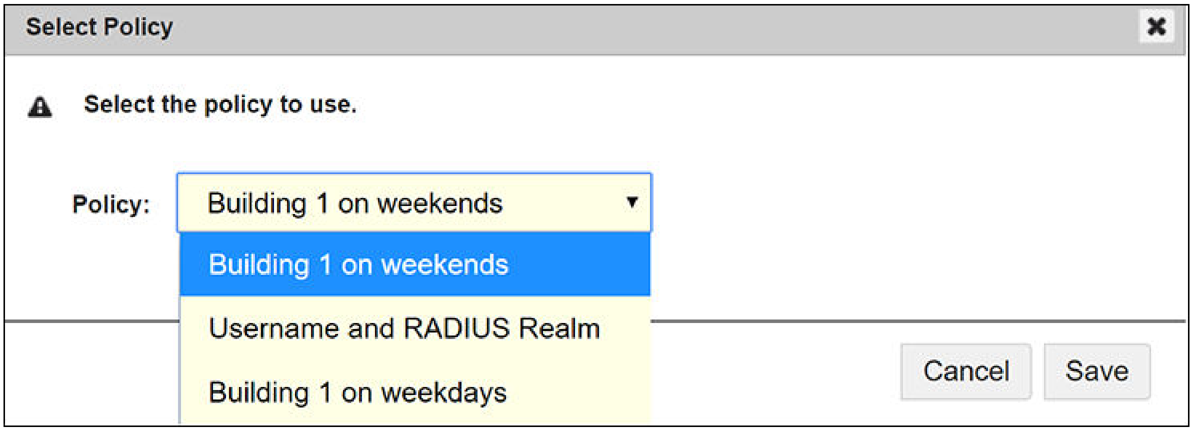
   Configuration > MAC Registration Lists

+	Sequence	Status	Name	Description	MAC Address Count	Policy Count	Default Access
	1	Not Used	MAC Registration-8		0	0	ACCEPT
	2	In Use	MAC Registrations		9	3	REJECT

   Results 1 - 2 of 2. 15

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 16 Select Policy Drop-down List

   Select Policy

   Select the policy to use.

   Policy: Building 1 on weekends

   - Building 1 on weekends
   - Username and RADIUS Realm
   - Building 1 on weekdays

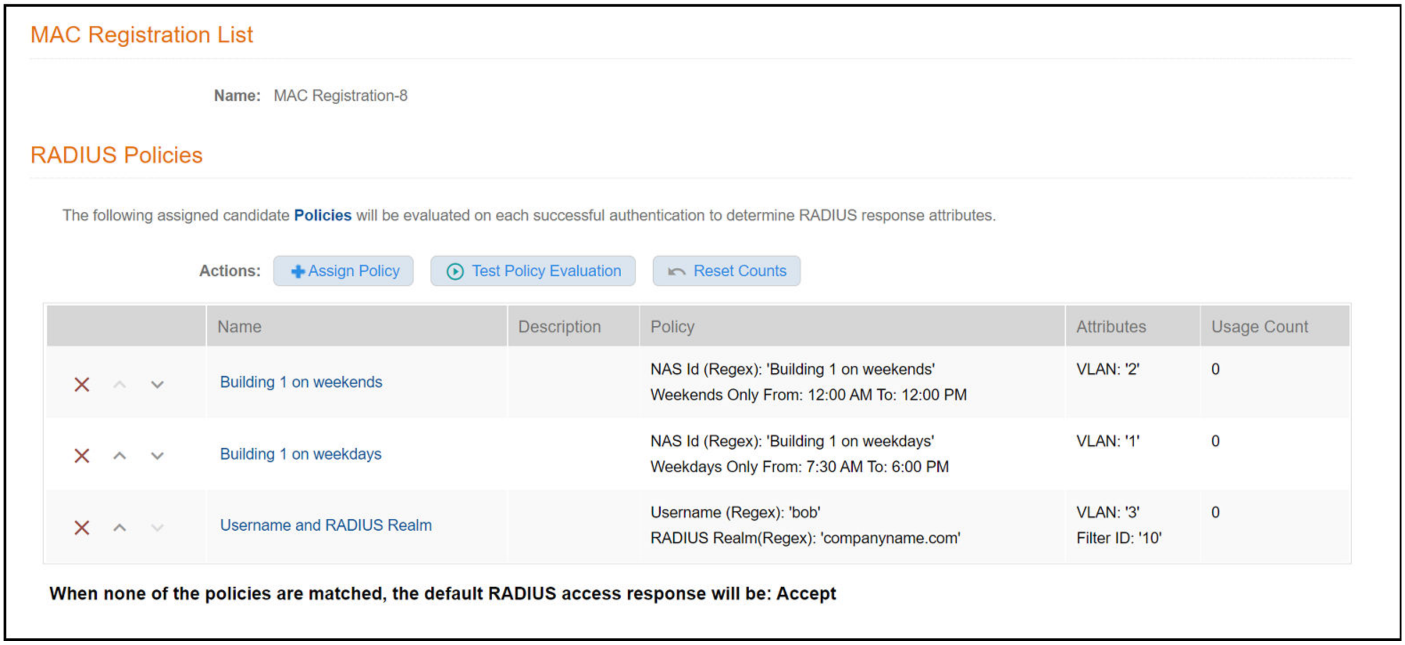
4. Select the policy you wish to add, then click **Save**.

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 17 Policies Added to MAC Registration List



MAC Registration List

Name: MAC Registration-8

RADIUS Policies

The following assigned candidate **Policies** will be evaluated on each successful authentication to determine RADIUS response attributes.

	Name	Description	Policy	Attributes	Usage Count
✕ ˄ ˅	Building 1 on weekends		NAS Id (Regex): 'Building 1 on weekends' Weekends Only From: 12:00 AM To: 12:00 PM	VLAN: '2'	0
✕ ˄ ˅	Building 1 on weekdays		NAS Id (Regex): 'Building 1 on weekdays' Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN: '1'	0
✕ ˄ ˅	Username and RADIUS Realm		Username (Regex): 'bob' RADIUS Realm(Regex): 'companyname.com'	VLAN: '3' Filter ID: '10'	0

When none of the policies are matched, the default RADIUS access response will be: Accept

- 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.

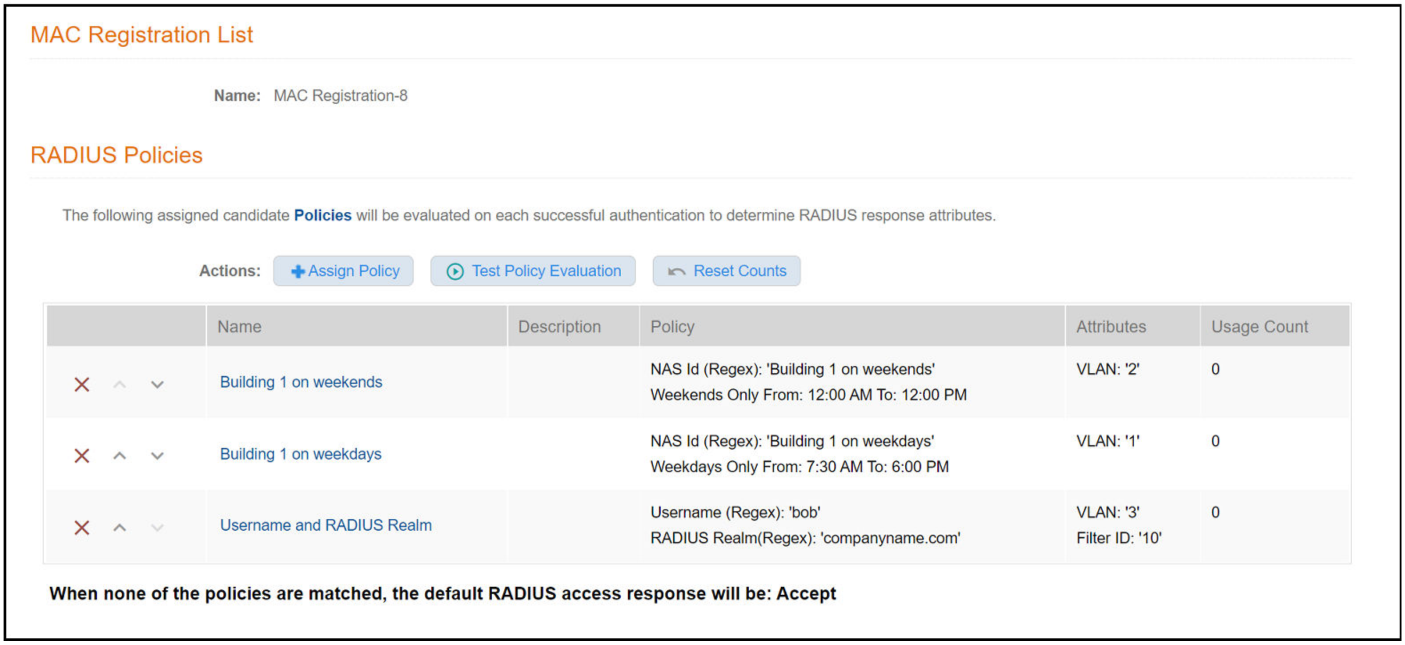
Additional Policy Information

Testing Policies

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 18 Three-Policy Example



MAC Registration List

Name: MAC Registration-8

RADIUS Policies

The following assigned candidate **Policies** will be evaluated on each successful authentication to determine RADIUS response attributes.

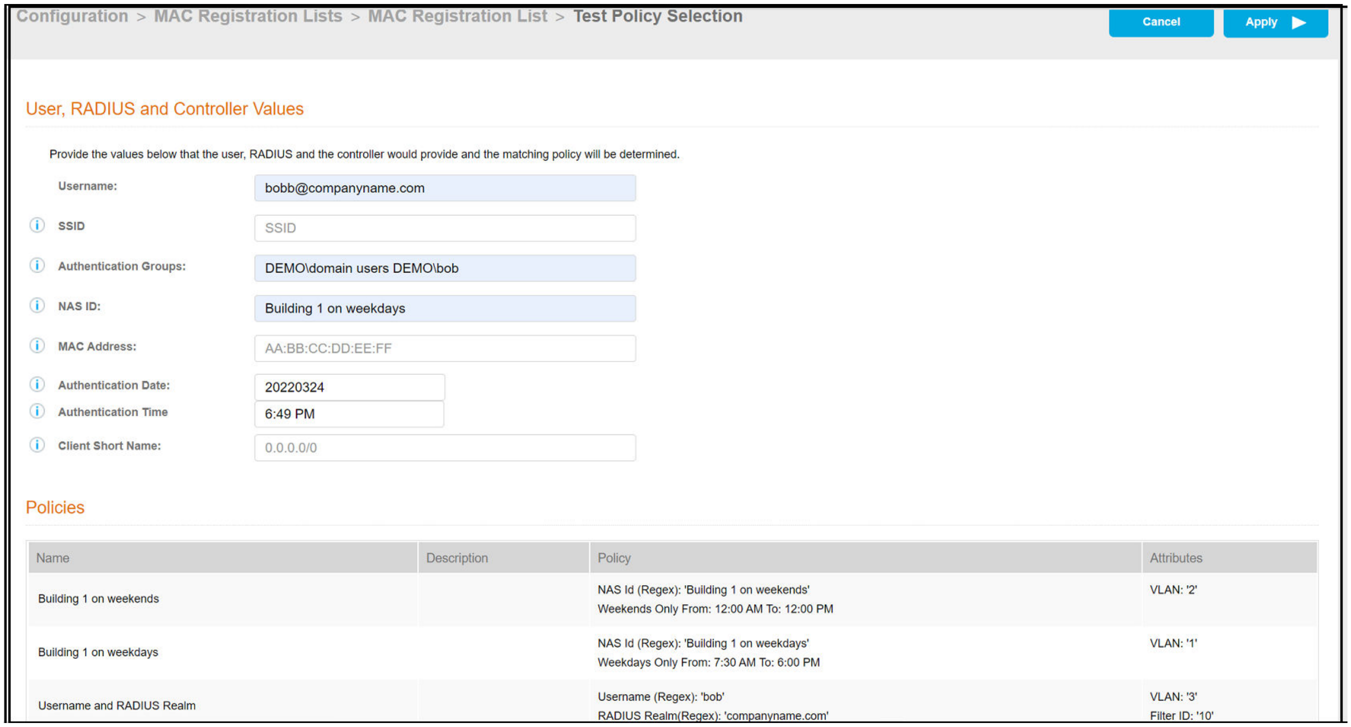
	Name	Description	Policy	Attributes	Usage Count
✕ ^ ˅	Building 1 on weekends		NAS Id (Regex): 'Building 1 on weekends' Weekends Only From: 12:00 AM To: 12:00 PM	VLAN: '2'	0
✕ ^ ˅	Building 1 on weekdays		NAS Id (Regex): 'Building 1 on weekdays' Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN: '1'	0
✕ ^ ˅	Username and RADIUS Realm		Username (Regex): 'bob' RADIUS Realm(Regex): 'companyname.com'	VLAN: '3' Filter ID: '10'	0

When none of the policies are matched, the default RADIUS access response will be: Accept

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 19 Test Policy Selection - Example 1 Values


Configuration > MAC Registration Lists > MAC Registration List > Test Policy Selection
Cancel
Apply ▶

User, RADIUS and Controller Values

Provide the values below that the user, RADIUS and the controller would provide and the matching policy will be determined.

Username: bobb@companyname.com
SSID: SSID
Authentication Groups: DEMO\domain users DEMO\bob
NAS ID: Building 1 on weekdays
MAC Address: AA:BB:CC:DD:EE:FF
Authentication Date: 20220324
Authentication Time 6:49 PM
Client Short Name: 0.0.0.0/0

Policies

Name	Description	Policy	Attributes
Building 1 on weekends		NAS Id (Regex): 'Building 1 on weekends' Weekends Only From: 12:00 AM To: 12:00 PM	VLAN: '2'
Building 1 on weekdays		NAS Id (Regex): 'Building 1 on weekdays' Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN: '1'
Username and RADIUS Realm		Username (Regex): 'bob' RADIUS Realm(Regex): 'companyname.com'	VLAN: '3' Filter ID: '10'

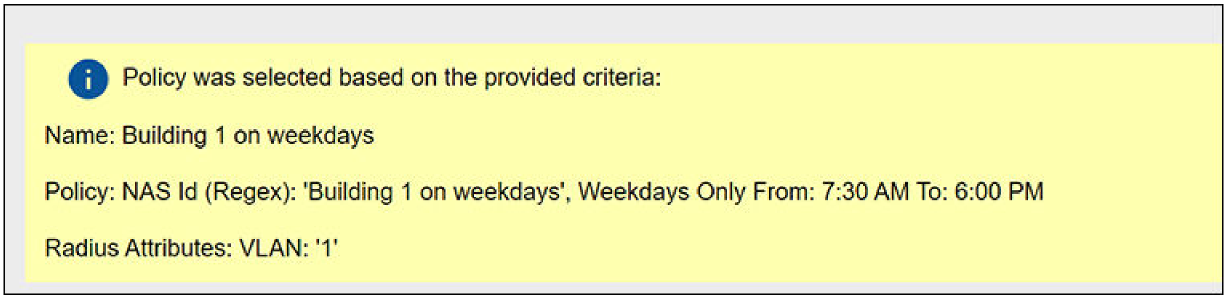
The sample values shown above have been entered to test that the "Building 1 on weekdays" policy will be applied to users who match the criteria defined by that policy (refer to the information in the "Policy" column in the figure above).

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 20 Test Policy Selection - Example 1 Results



Policy was selected based on the provided criteria:

Name: Building 1 on weekdays

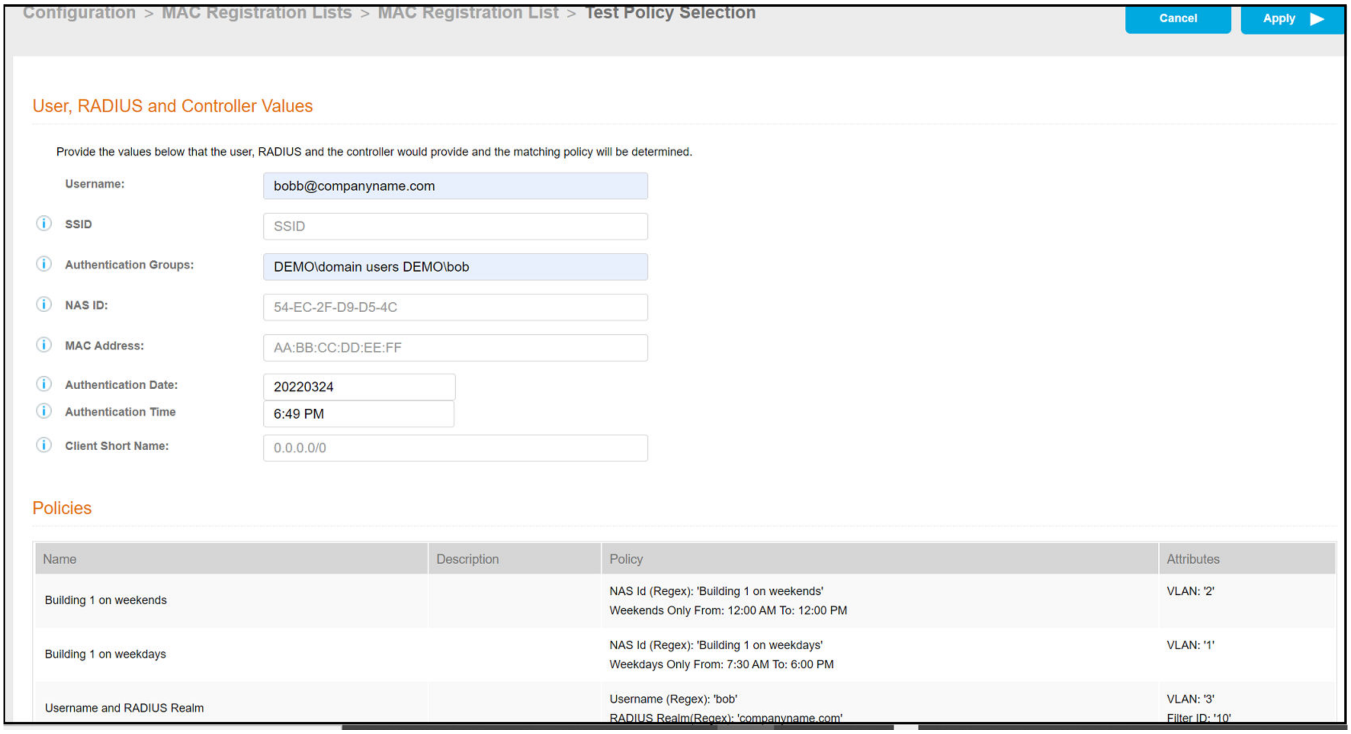
Policy: NAS Id (Regex): 'Building 1 on weekdays', Weekdays Only From: 7:30 AM To: 6:00 PM

Radius Attributes: VLAN: '1'

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 21 Test Policy Selection - Example 2 Values


Configuration > MAC Registration Lists > MAC Registration List > Test Policy Selection
Cancel
Apply ▶

User, RADIUS and Controller Values

Provide the values below that the user, RADIUS and the controller would provide and the matching policy will be determined.

Username:	bobb@companyname.com
SSID	SSID
Authentication Groups:	DEMO\domain users DEMO\bob
NAS ID:	54-EC-2F-D9-D5-4C
MAC Address:	AA:BB:CC:DD:EE:FF
Authentication Date:	20220324
Authentication Time	6:49 PM
Client Short Name:	0.0.0.0/0

Policies

Name	Description	Policy	Attributes
Building 1 on weekends		NAS Id (Regex): 'Building 1 on weekends' Weekends Only From: 12:00 AM To: 12:00 PM	VLAN: '2'
Building 1 on weekdays		NAS Id (Regex): 'Building 1 on weekdays' Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN: '1'
Username and RADIUS Realm		Username (Regex): 'bob' RADIUS Realm(Regex): 'companyname.com'	VLAN: '3' Filter ID: '10'

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:

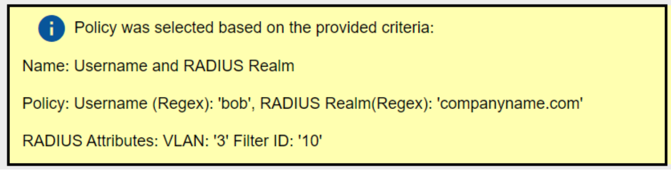
   a. The values you entered in the upper portion of the screen are first compared to the policy named "Building 1 on weekends" because that is the policy listed first (see Policies section in the screen above). However, you can see that the values entered for testing do not match the conditions shown in 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 22 Test Policy Selection - Example 2 Results



Policy was selected based on the provided criteria:

Name: Username and RADIUS Realm

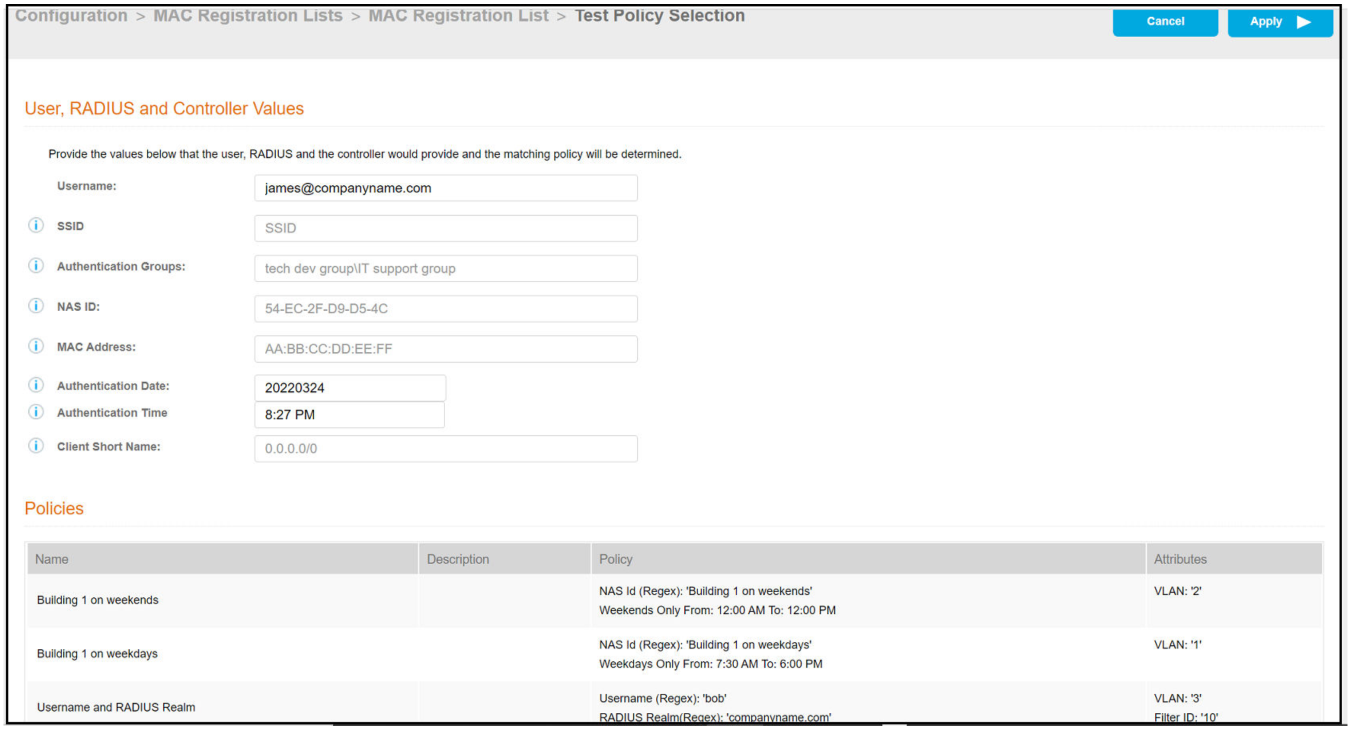
Policy: Username (Regex): 'bob', RADIUS Realm(Regex): 'companyname.com'

RADIUS Attributes: VLAN: '3' Filter ID: '10'

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 23 Test Policy Selection - Example 3 Values



Configuration > MAC Registration Lists > MAC Registration List > Test Policy Selection
Cancel
Apply

User, RADIUS and Controller Values

Provide the values below that the user, RADIUS and the controller would provide and the matching policy will be determined.

Username:	james@companyname.com
SSID	SSID
Authentication Groups:	tech dev group\IT support group
NAS ID:	54-EC-2F-D9-D5-4C
MAC Address:	AA:BB:CC:DD:EE:FF
Authentication Date:	20220324
Authentication Time	8:27 PM
Client Short Name:	0.0.0.0/0

Policies

Name	Description	Policy	Attributes
Building 1 on weekends		NAS Id (Regex): 'Building 1 on weekends' Weekends Only From: 12:00 AM To: 12:00 PM	VLAN: '2'
Building 1 on weekdays		NAS Id (Regex): 'Building 1 on weekdays' Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN: '1'
Username and RADIUS Realm		Username (Regex): 'bob' RADIUS Realm(Regex): 'companyname.com'	VLAN: '3' Filter ID: '10'

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).

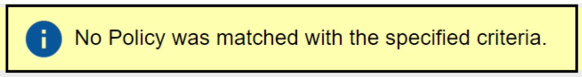
3. Before you click the **Apply** button, check the values you have entered. In the above example, the expected behavior is:
   a. The values you entered in the upper portion of the screen are first compared to the policy named "Building 1 on weekends" because that is the policy listed first (see Policies 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 24 Test Policy Selection - Example 3 Results



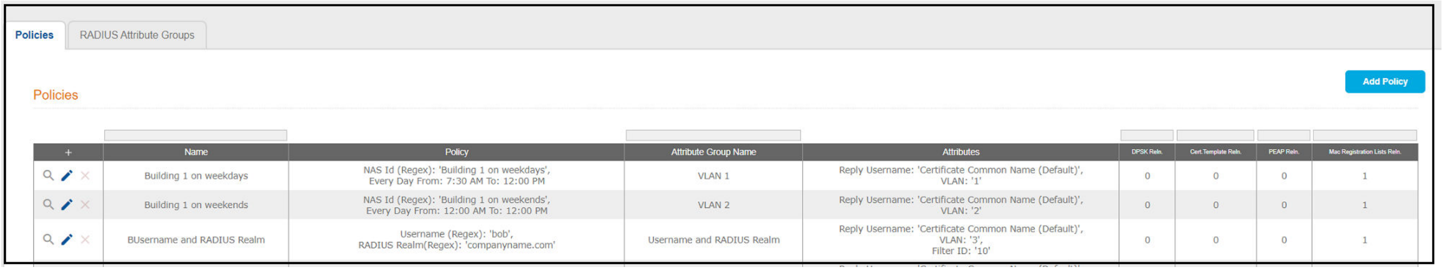
No Policy was matched with the specified criteria.

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 25 Policy Table Example



Policies

+	Name	Policy	Attribute Group Name	Attributes	DPSK Reln.	Cert.Template Reln.	PEAP Reln.	Mac Registration Lists Reln.
🔍 ✎ ✕	Building 1 on weekdays	NAS Id (Regex): 'Building 1 on weekdays', Every Day From: 7:30 AM To: 12:00 PM	VLAN 1	Reply Username: 'Certificate Common Name (Default)', VLAN: '1'	0	0	0	1
🔍 ✎ ✕	Building 1 on weekends	NAS Id (Regex): 'Building 1 on weekends', Every Day From: 12:00 AM To: 12:00 PM	VLAN 2	Reply Username: 'Certificate Common Name (Default)', VLAN: '2'	0	0	0	1
🔍 ✎ ✕	BUsername and RADIUS Realm	Username (Regex): 'bob', RADIUS Realm(Regex): 'companyname.com'	Username and RADIUS Realm	Reply Username: 'Certificate Common Name (Default)', VLAN: '3', Filter ID: '10'	0	0	0	1

You can use the policy table as follows:

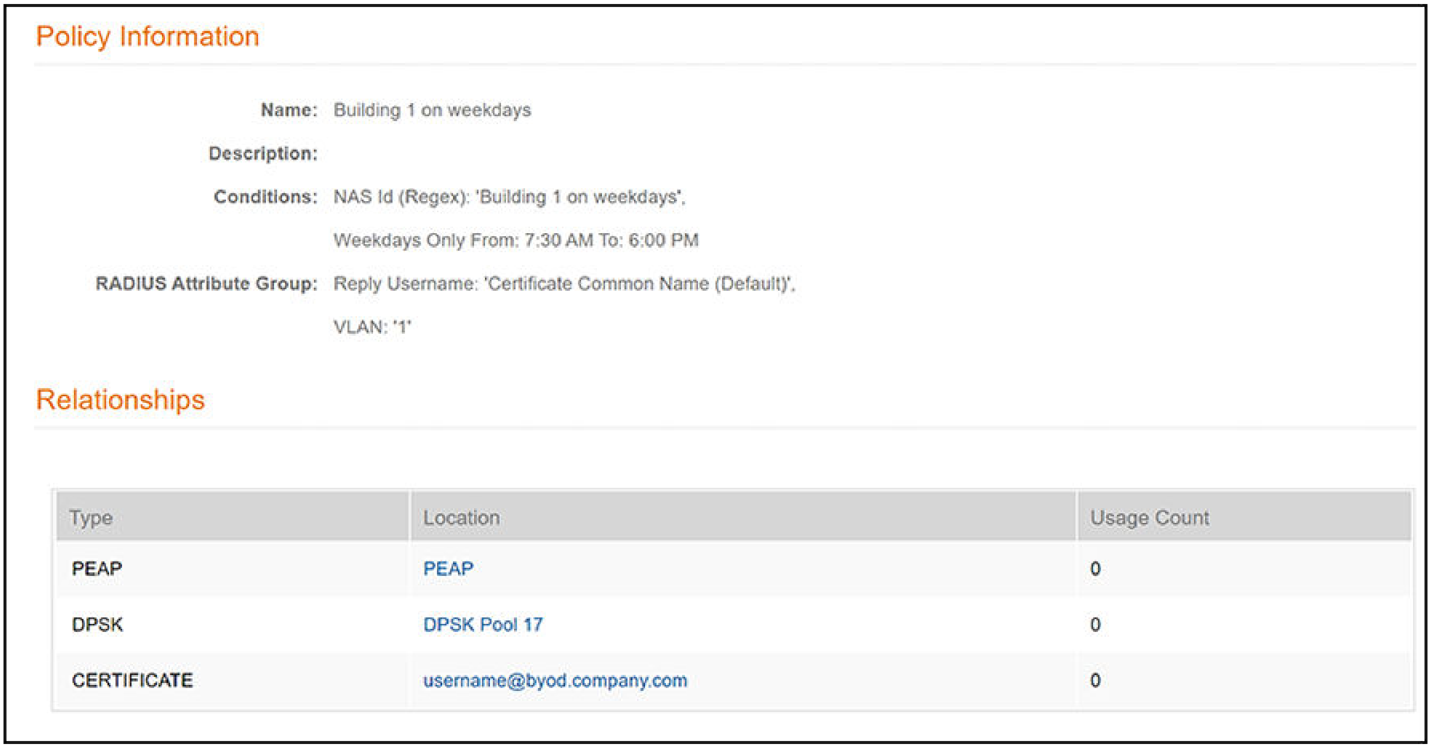
TABLE 13 Description of Policy Table

Column Title	Description
+	• You can view details of the policy by clicking on the magnifying glass icon (for an example of the Policy Information screen that gets invoked, see Figure 26. • 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.

TABLE 13 Description of Policy Table (continued)

Column Title	Description
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 19.
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 19.
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 19.
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 17. **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.

FIGURE 26 Policy Information Screen Example



Policy Information

Name: Building 1 on weekdays

Description:

Conditions: NAS Id (Regex): 'Building 1 on weekdays',
Weekdays Only From: 7:30 AM To: 6:00 PM

RADIUS Attribute Group: Reply Username: 'Certificate Common Name (Default)',
VLAN: '1'

Relationships

Type	Location	Usage Count
PEAP	PEAP	0
DPSK	DPSK Pool 17	0
CERTIFICATE	username@byod.company.com	0

The screen above indicates that the policy is currently being used by PEAP, one DPSK pool, and one certificate. The "Location" column of this screen in the UI provides live links to the specific configuration areas where the policy is used.

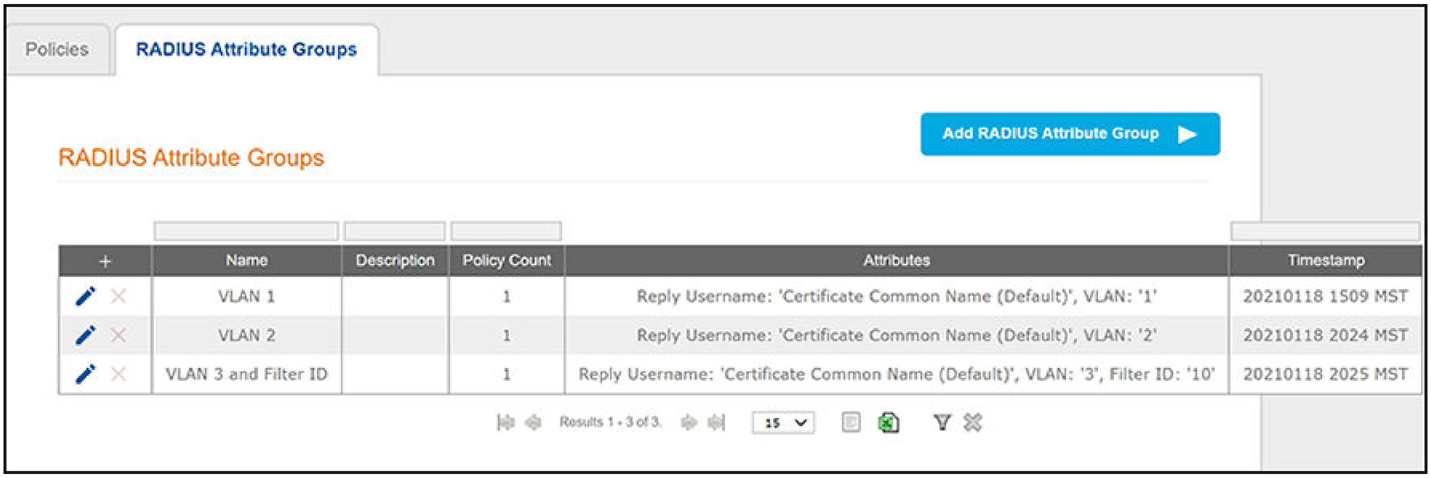
The Usage column will be incremented each time a device is assigned to the policy in question. Also, If a device then gets assigned to a different policy and later gets reassigned to its original policy, the usage count of the original policy will be incremented.

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 27 RADIUS Attribute Groups Example



RADIUS Attribute Groups

+	Name	Description	Policy Count	Attributes	Timestamp
✎ ✕	VLAN 1		1	Reply Username: 'Certificate Common Name (Default)', VLAN: '1'	20210118 1509 MST
✎ ✕	VLAN 2		1	Reply Username: 'Certificate Common Name (Default)', VLAN: '2'	20210118 2024 MST
✎ ✕	VLAN 3 and Filter ID		1	Reply Username: 'Certificate Common Name (Default)', VLAN: '3', Filter ID: '10'	20210118 2025 MST

You can use the RADIUS Attribute Groups table as follows:

TABLE 14 Description of RADIUS Attribute Groups Table

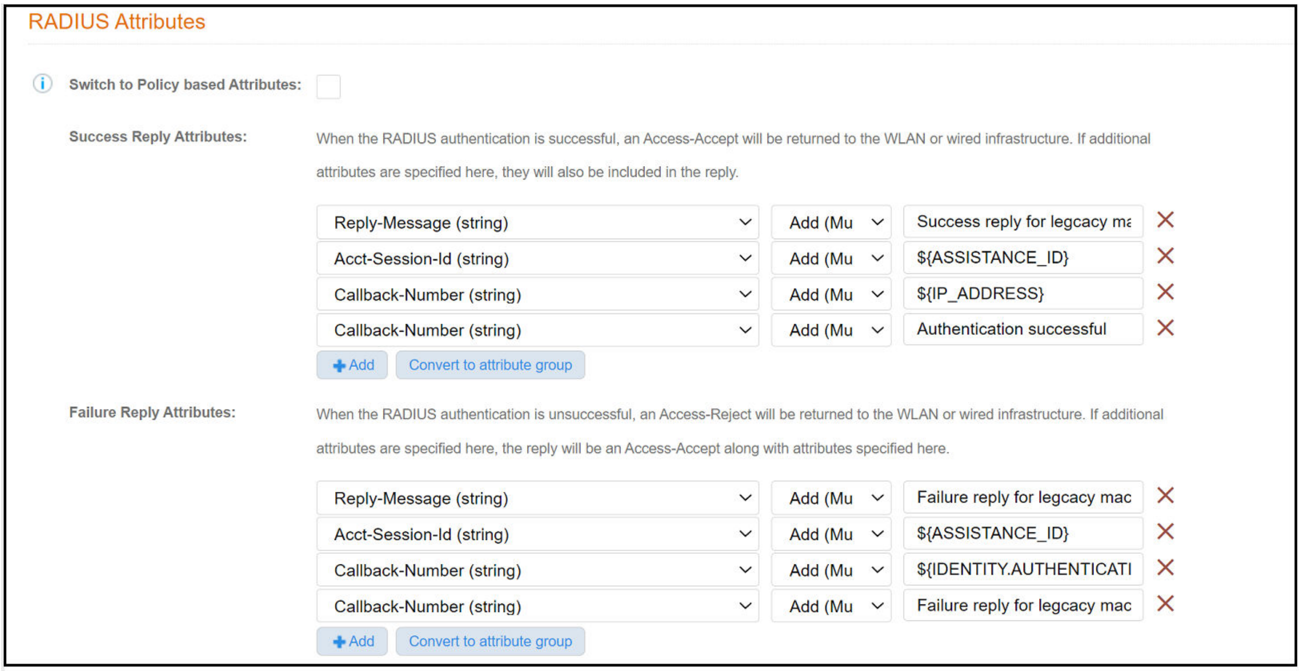
Column Title	Description
+	• You can edit the RADIUS attribute group by clicking on the pencil icon. • If the RADIUS attribute group has not yet been assigned to any policy, there will be a **X** next to the name. Clicking that X deletes the group. However, in the example screen shown above, all the 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 17.
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 17. **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 28 Pre-Release 5.9R4 MAC Registration List Configuration Screen - RADIUS Attributes Section



RADIUS Attributes

Switch to Policy based 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.

Reply-Message (string)	Add (Mu	Success reply for legcacy ma
Acct-Session-Id (string)	Add (Mu	${ASSISTANCE_ID}
Callback-Number (string)	Add (Mu	${IP_ADDRESS}
Callback-Number (string)	Add (Mu	Authentication successful

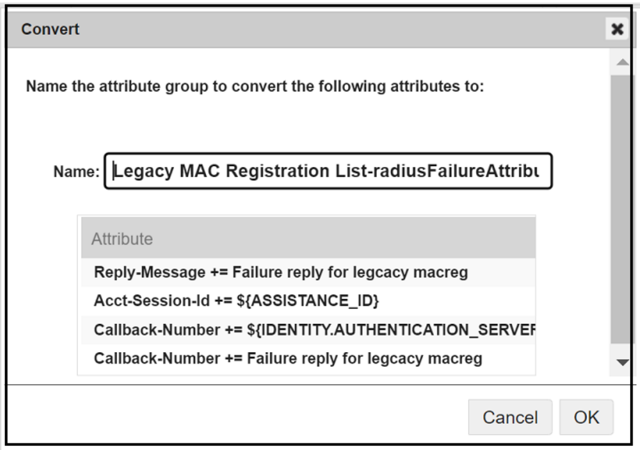
Failure Reply Attributes: When the RADIUS authentication is unsuccessful, an Access-Reject will be returned to the WLAN or wired infrastructure. If additional attributes are specified here, the reply will be an Access-Accept along with attributes specified here.

Reply-Message (string)	Add (Mu	Failure reply for legcacy mac
Acct-Session-Id (string)	Add (Mu	${ASSISTANCE_ID}
Callback-Number (string)	Add (Mu	${IDENTITY.AUTHENTICATI
Callback-Number (string)	Add (Mu	Failure reply for legcacy mac

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 29 Naming the RADIUS Attribute Group for Failure Replies



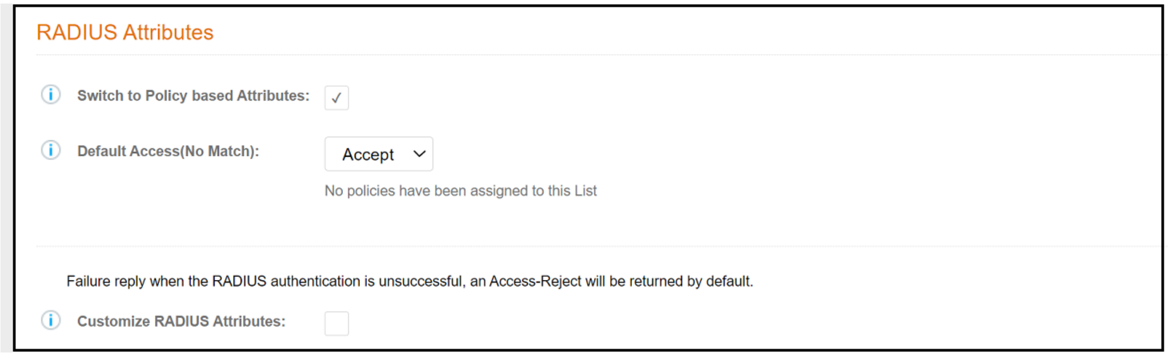
Name the attribute group to convert the following attributes to:

Name: Legacy MAC Registration List-radiusFailureAttribu

Attribute
Reply-Message += Failure reply for legcacy macreg
Acct-Session-Id += ${ASSISTANCE_ID}
Callback-Number += ${IDENTITY.AUTHENTICATION_SERVEF
Callback-Number += Failure reply for legcacy macreg

3. Click **OK**.
4. Check the "Switch to Policy-based Atttributes" box (refer to Figure 28 to view the location of the checkbox). The following screen is displayed:

FIGURE 30 New MAC Registration RADIUS Attributes Section



Switch to Policy based Attributes: ✓

Default Access(No Match): Accept

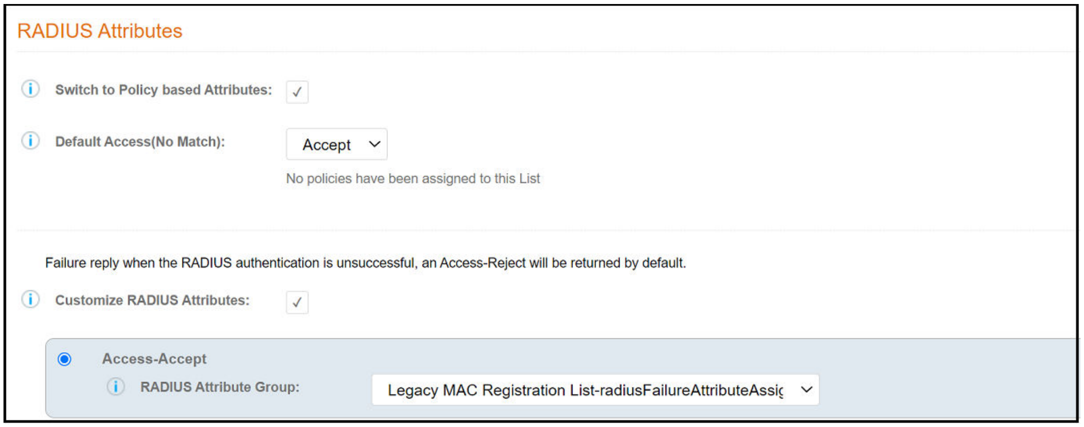
No policies have been assigned to this List

Failure reply when the RADIUS authentication is unsuccessful, an Access-Reject will be returned by default.

Customize RADIUS Attributes: □

5. You have the option of customizing a RADIUS reply when authentication fails. To do so, check the "Customize RADIUS Attributes" 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 31 RADIUS Attribute Group Selected From Drop-Down List



RADIUS Attributes

Switch to Policy based Attributes: ☑

Default Access(No Match): Accept

No policies have been assigned to this List

Failure reply when the RADIUS authentication is unsuccessful, an Access-Reject will be returned by default.

Customize RADIUS Attributes: ☑

● Access-Accept

RADIUS Attribute Group: Legacy MAC Registration List-radiusFailureAttributeAssiç

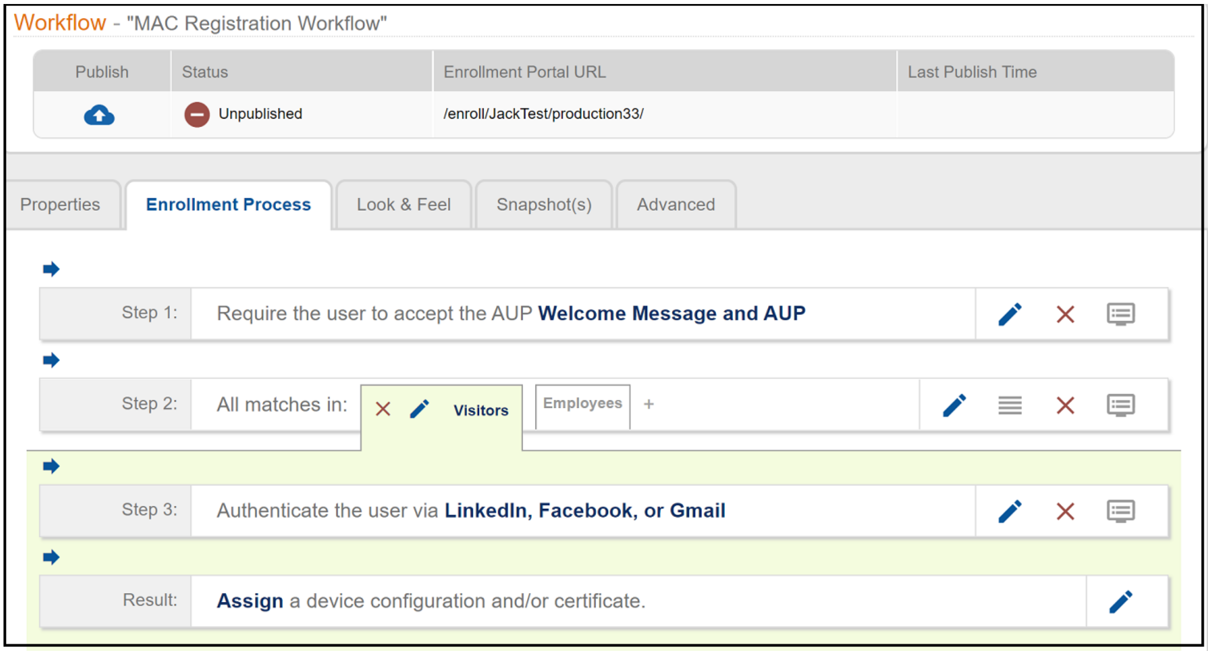
7. Click **Save**.
8. Once the conversion is complete, you can select the **RADIUS Policies** tab and add any desired policies. For instructions on adding policies, see Adding Policies to a MAC Registration List on page 29.

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 21. 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 32 Workflow After Initial Creation



Workflow - "MAC Registration Workflow"

Publish	Status	Enrollment Portal URL	Last Publish Time
	Unpublished	/enroll/JackTest/production33/	

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

Step 2: All matches in: **Visitors** Employees +

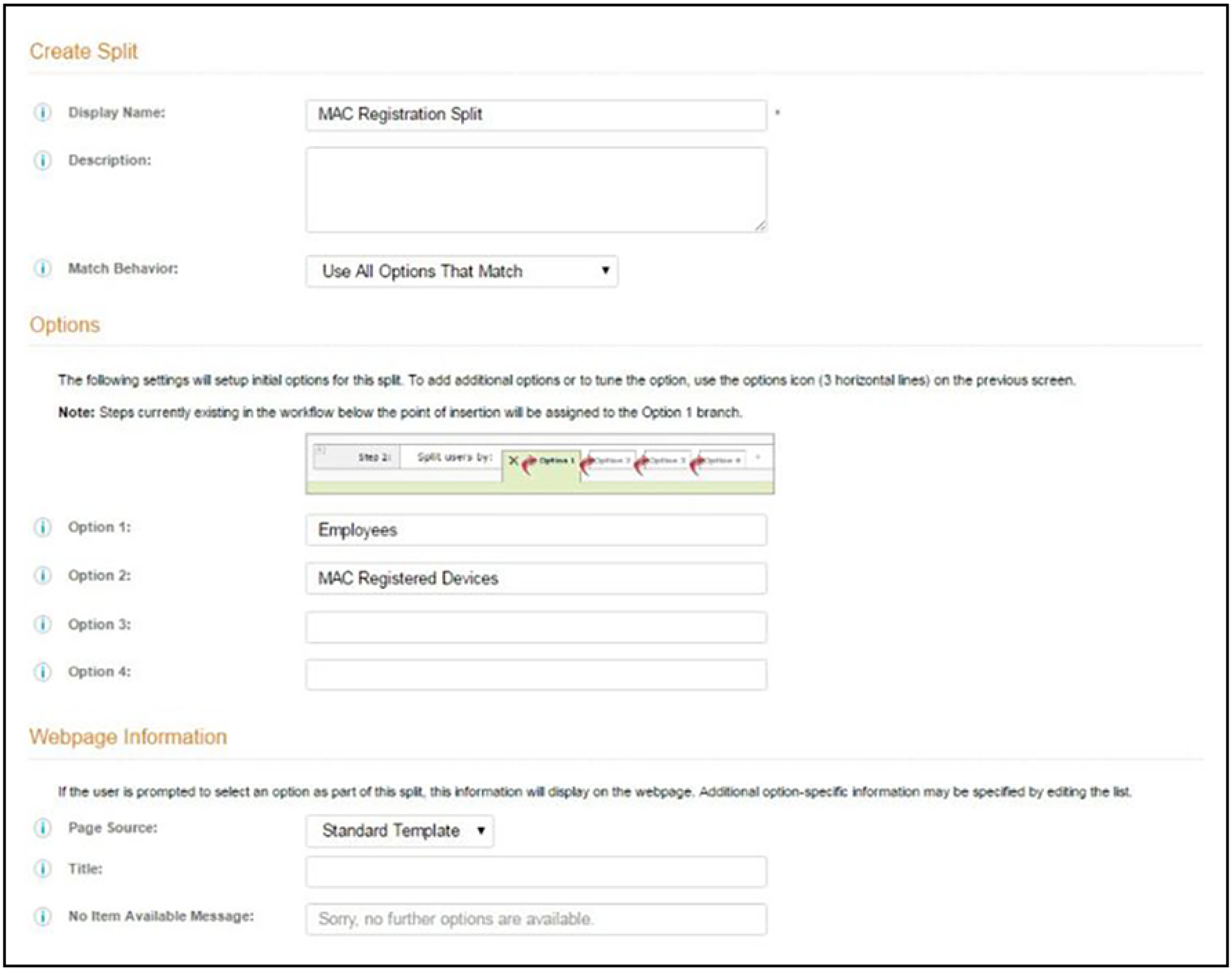
Step 3: Authenticate the user via **LinkedIn, Facebook, or Gmail**

Result: **Assign** a device configuration and/or certificate.

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 33 Create Split



Create Split

Display 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:

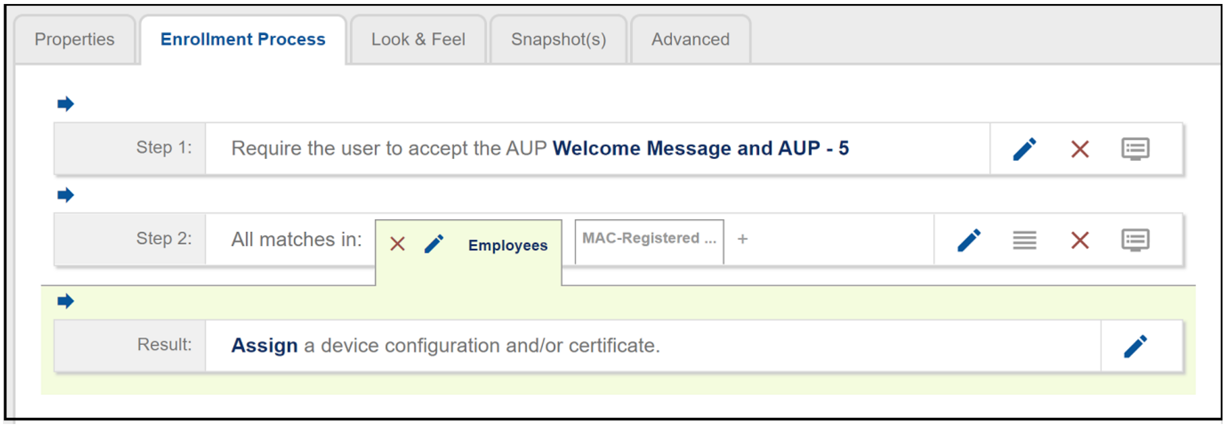
No Item Available Message: Sorry, no further options are available.

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 34 MAC Registration List Example Workflow After a Split Is Created



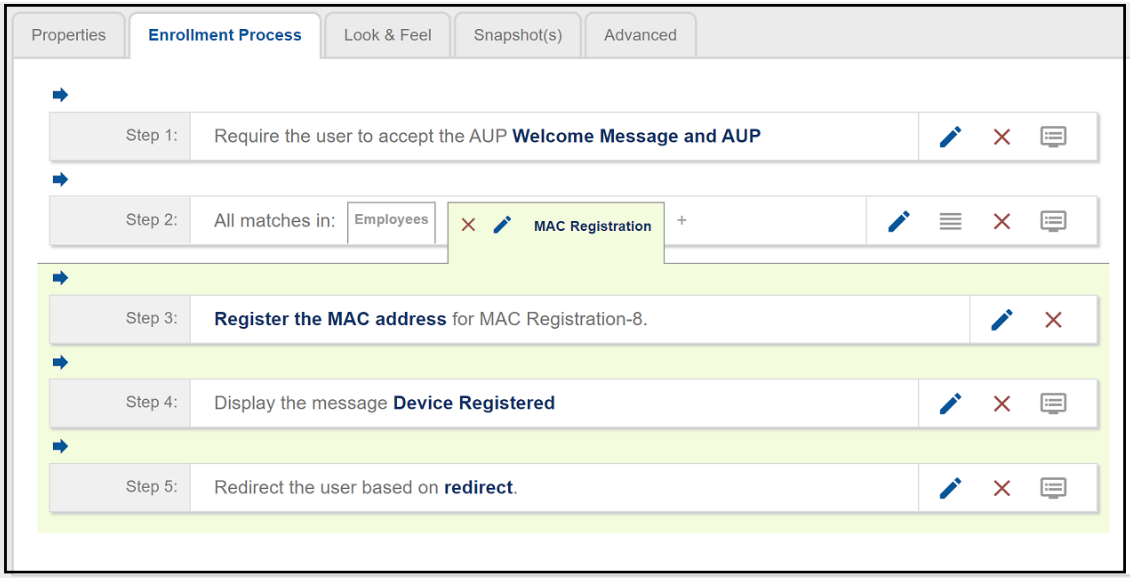
Step 1: Require the user to accept the AUP **Welcome Message and AUP - 5**

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

Result: **Assign** a device configuration and/or certificate.

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 21. 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 35 Completed MAC Registration Workflow Example



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

Step 2: All matches in: Employees | MAC Registration | +

Step 3: **Register the MAC address** for MAC Registration-8.

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

Step 5: Redirect the user based on **redirect**.

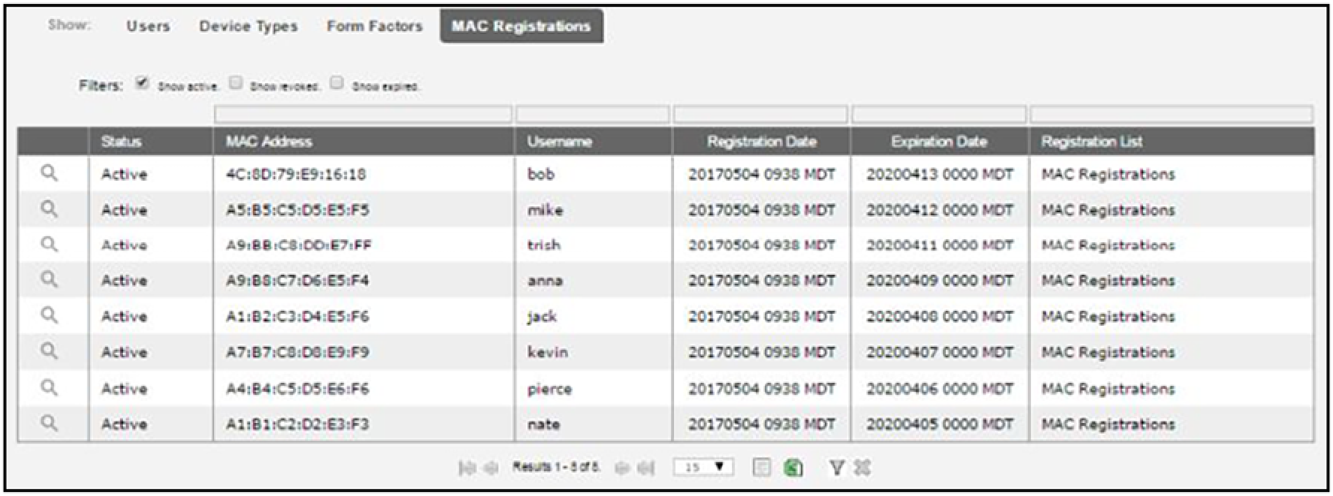
Viewing MAC Registration Records on the Dashboard

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 **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 36 MAC Registrations on the Dashboard



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

	Status	MAC Address	Username	Registration Date	Expiration Date	Registration List
🔍	Active	4C:8D:79:E9:16:18	bob	20170504 0938 MDT	20200413 0000 MDT	MAC Registrations
🔍	Active	A5:B5:C5:D5:E5:F5	mike	20170504 0938 MDT	20200412 0000 MDT	MAC Registrations
🔍	Active	A9:BB:C8:DD:E7:FF	trish	20170504 0938 MDT	20200411 0000 MDT	MAC Registrations
🔍	Active	A9:B8:C7:D6:E5:F4	anna	20170504 0938 MDT	20200409 0000 MDT	MAC Registrations
🔍	Active	A1:B2:C3:D4:E5:F6	jack	20170504 0938 MDT	20200408 0000 MDT	MAC Registrations
🔍	Active	A7:B7:C8:D8:E9:F9	kevin	20170504 0938 MDT	20200407 0000 MDT	MAC Registrations
🔍	Active	A4:B4:C5:D5:E6:F6	pierce	20170504 0938 MDT	20200406 0000 MDT	MAC Registrations
🔍	Active	A1:B1:C2:D2:E3:F3	nate	20170504 0938 MDT	20200405 0000 MDT	MAC Registrations

Results 1 - 8 of 8. 15 ▼

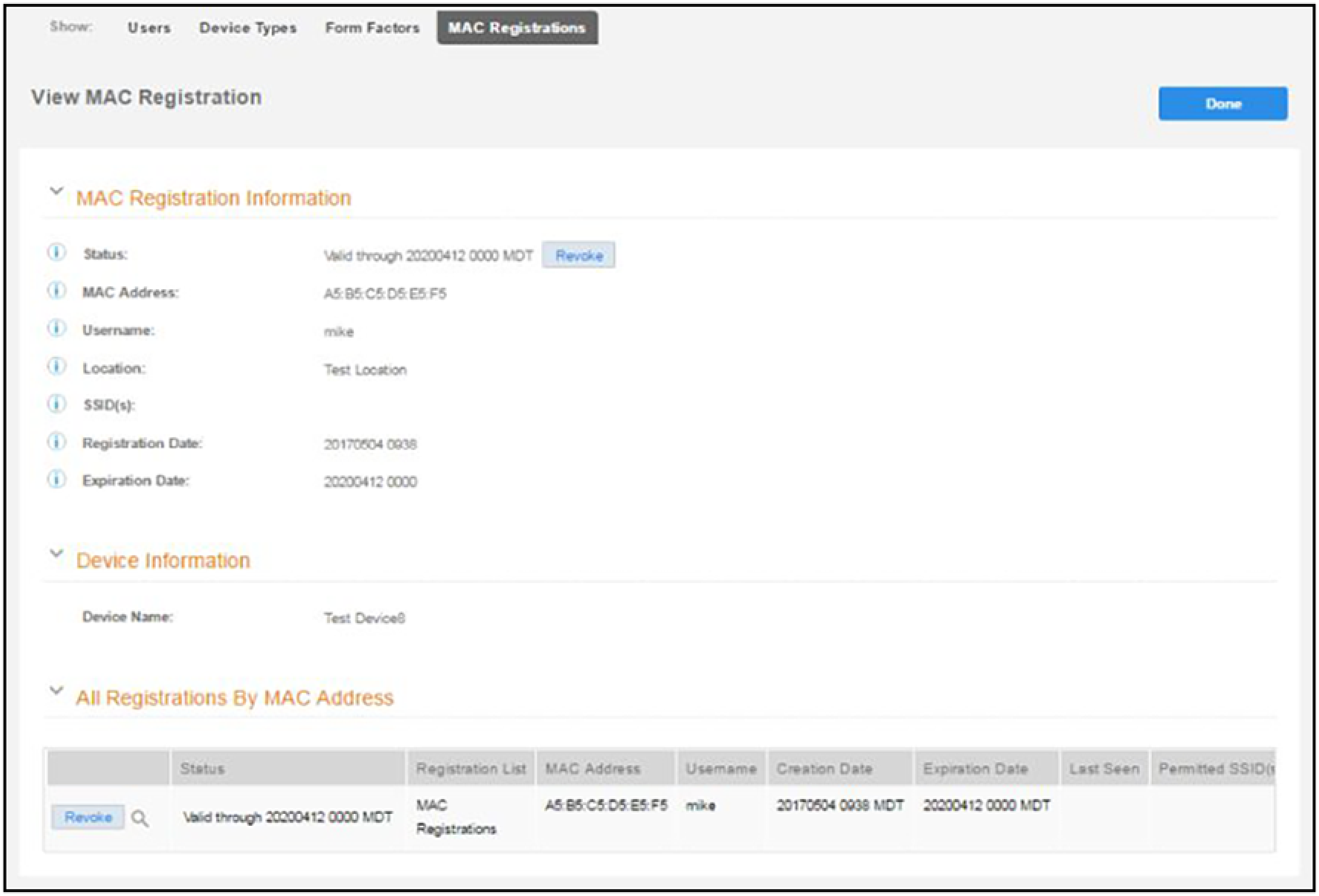
4. You can also access MAC registration information in the enrollment record. Go to **Operational** > **Dashboard** > **Enrollments** > **View Enrollment Record**.

How to Revoke Access for a MAC-Registered Device

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

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

FIGURE 37 View MAC Registration Details



View MAC Registration

MAC Registration Information

Status:	Valid through 20200412 0000 MDT Revoke
MAC Address:	A5:B5:C5:D5:E5:F5
Username:	mike
Location:	Test Location
SSID(s):	
Registration Date:	20170504 0938
Expiration Date:	20200412 0000

Device Information

Device Name:	Test Device8

All Registrations By MAC Address

	Status	Registration List	MAC Address	Username	Creation Date	Expiration Date	Last Seen	Permitted SSID(s
Revoke	Valid through 20200412 0000 MDT	MAC Registrations	A5:B5:C5:D5:E5:F5	mike	20170504 0938 MDT	20200412 0000 MDT		

3. In the **All Registrations by MAC Devices** section, click the **Revoke** button next to the device.

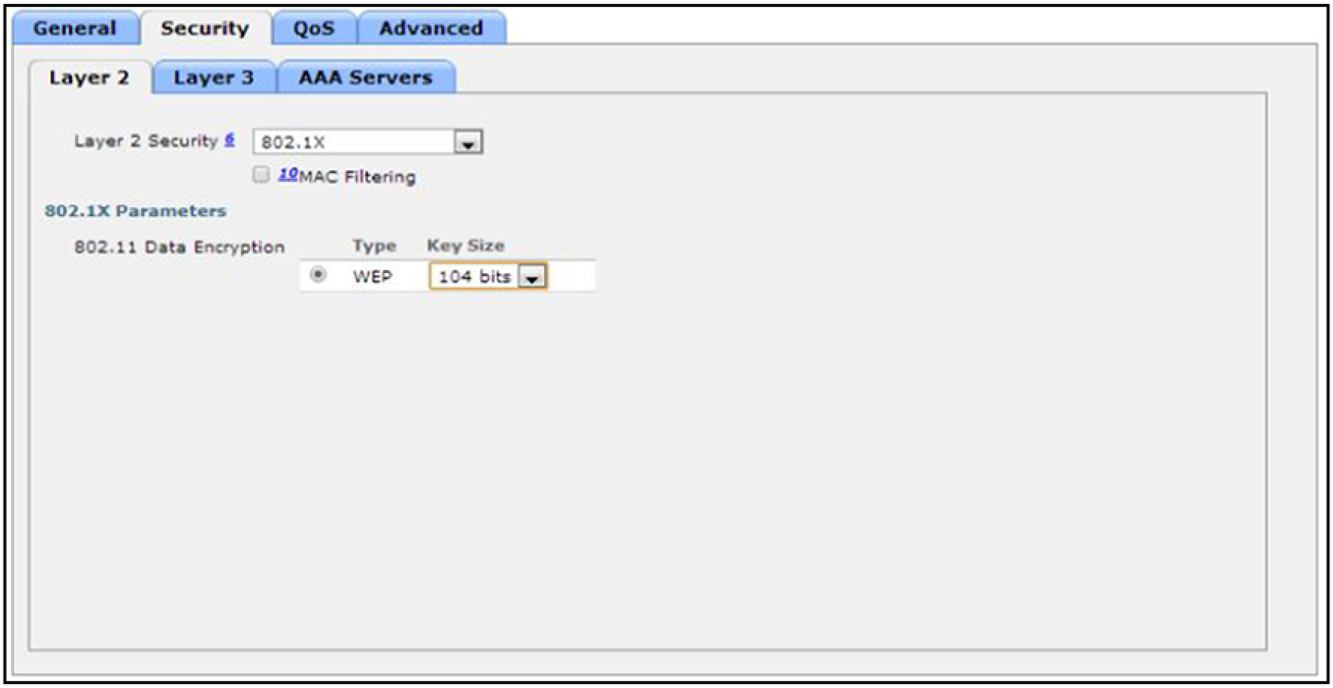
4. On the **Revoke** pop-up, list the reason for revocation and click **Revoke**. The MAC address for the device is removed from the list of accepted MAC addresses in the RADIUS server.

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 38 Layer 2 Security



Layer 2 Security 6 802.1X

□ 10MAC Filtering

802.1X Parameters

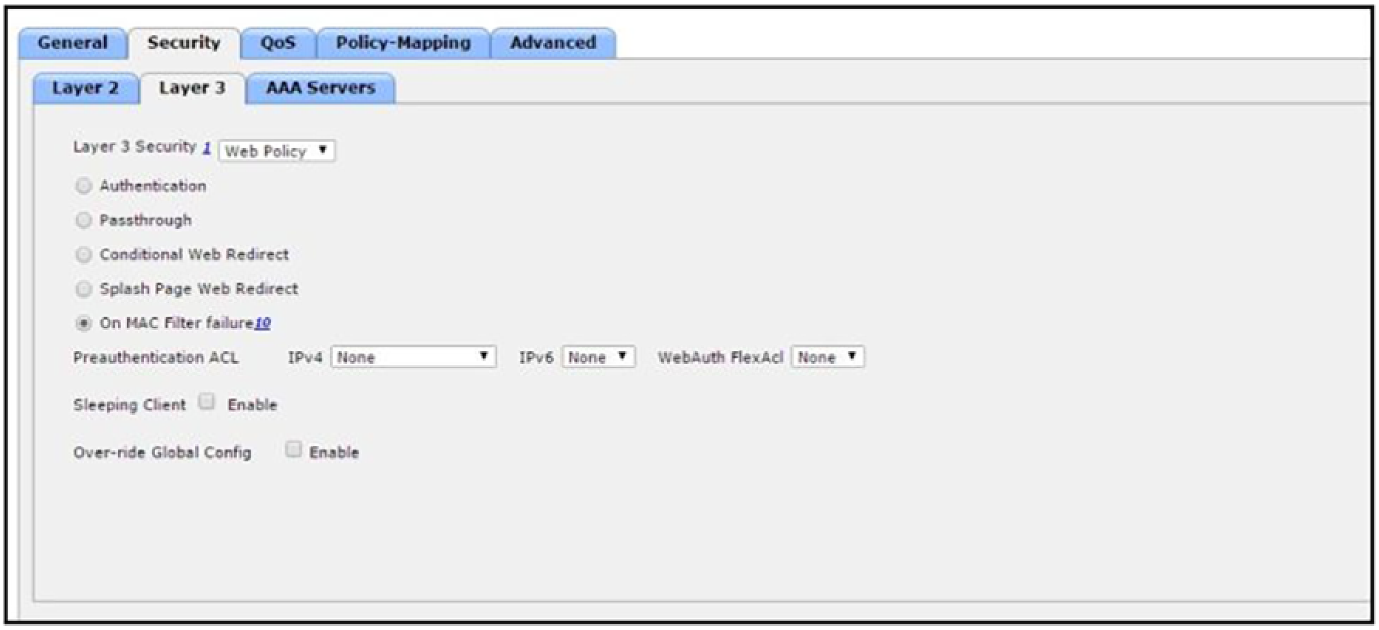
802.11 Data Encryption		Type	Key Size
	●	WEP	104 bits

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 39 Layer 3 Settings when Using Layer 2 Mac Filtering



Layer 3 Security 1 Web Policy ▾

○ Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

● On MAC Filter failure10

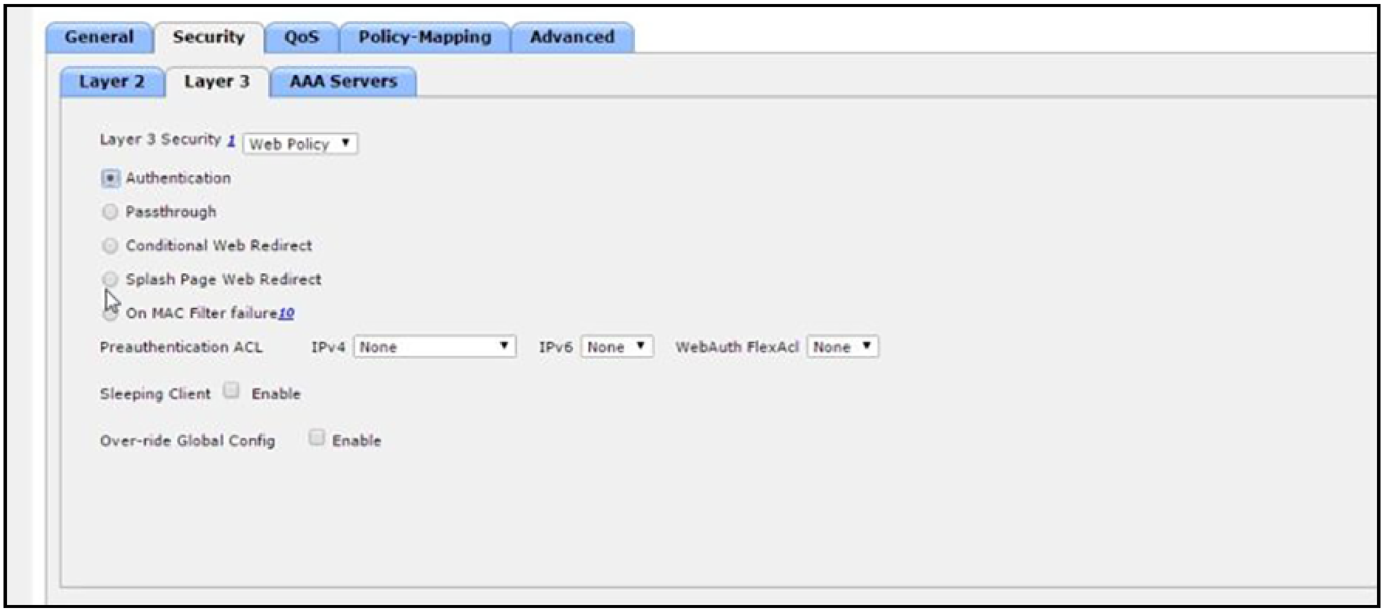
Preauthentication ACL IPv4 None ▾ IPv6 None ▾ WebAuth FlexAcl None ▾

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 40 Layer 3 Settings when 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 ▾

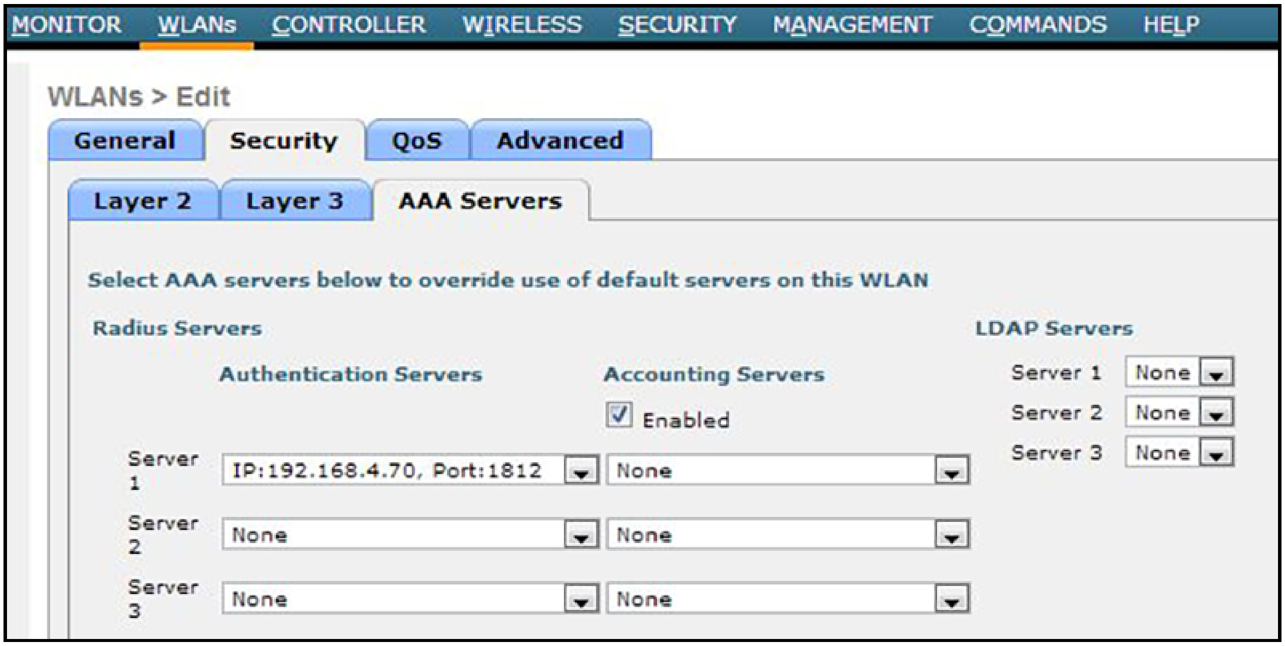
Sleeping Client □ Enable

Over-ride Global Config □ Enable

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 41 Select RADIUS Server



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

7. **Apply** changes.

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

350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com