CONFIGURATION GUIDE

Cloudpath Enrollment System MAC Registration Configuration Guide, 5.5

Supporting Cloudpath Software Release 5.5

Part Number: 800-72410-001 Rev A
Publication Date: 28 August 2019

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, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex 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 device's MAC address to allow limited, and secure, network access.

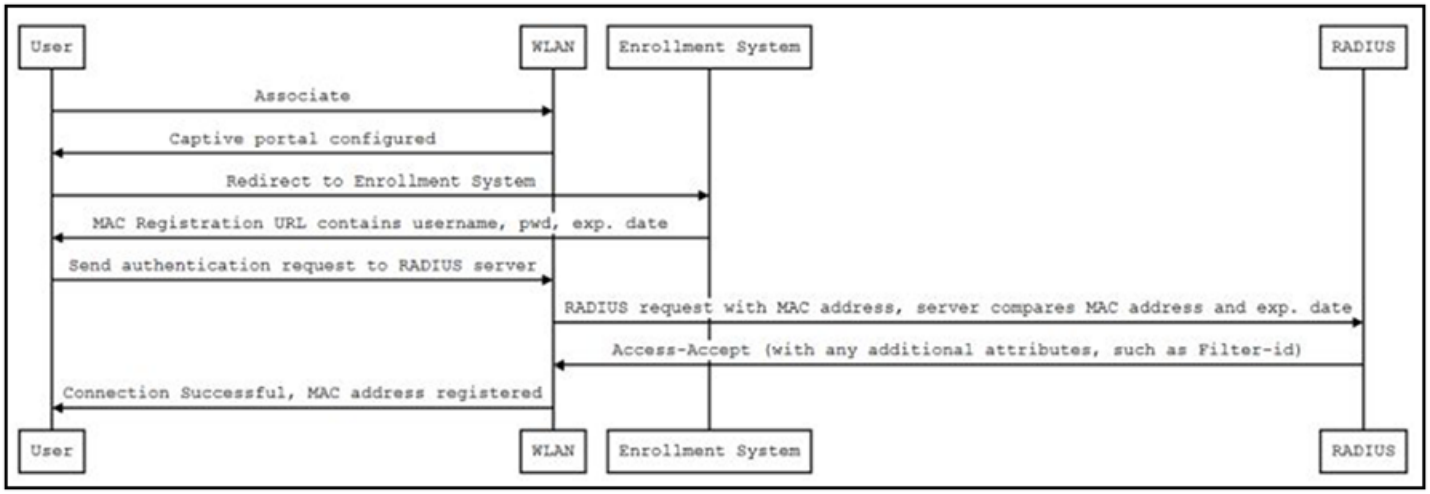
When setting up MAC registration, a list of authorized MAC addresses is maintained on the RADIUS server. When a non-802.1X device attempts to connect to the network, the request is forwarded to the RADIUS server, where the device is checked against the list of authorized MAC addresses. If the registration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

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

MAC Registration Process

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

FIGURE 1 MAC Registration Sequence



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

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

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

Configuring Ruckus Controllers for MAC Registration

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

The screen shots and corresponding instructions about the controllers are based on the following Ruckus Controller versions:

- ZoneDirector 10.1.1
- Virtual SmartZone 3.6.0 (High Scale)
- Unleashed 200.6

If you are using different versions of any controller, please consult your controller documentation because you may encounter some differences in the user interface.

If your environment uses Cisco controllers, see Configuring a Cisco Controller for MAC Registration on page 40.

Setting up Cloudpath as an AAA Authentication Server

Create an AAA authentication server for the Cloudpath onboard RADIUS server. The following images show this configuration on the Ruckus ZoneDirector, SmartZone, and Unleashed controllers.

On ZoneDirector, go to **Services & Profiles > AAA Servers**. On SmartZone, go to **Services & Profiles > Authentication**. On Unleashed, go to **Admin & Services > Services > AAA Servers > Authentication Servers**.

FIGURE 2 Create AAA Authentication Server on ZoneDirector

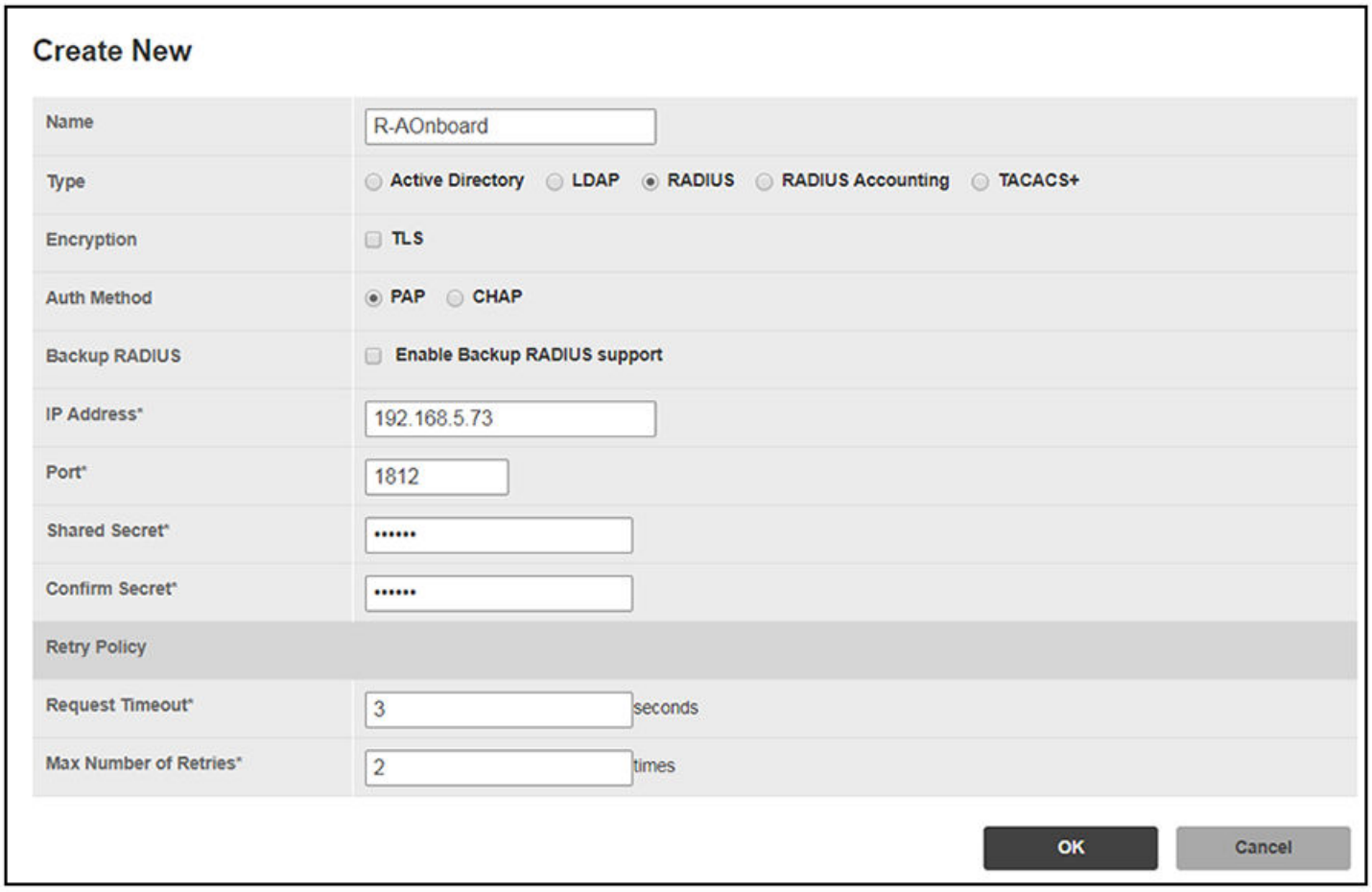


FIGURE 3 Create AAA Authentication Server on SmartZone

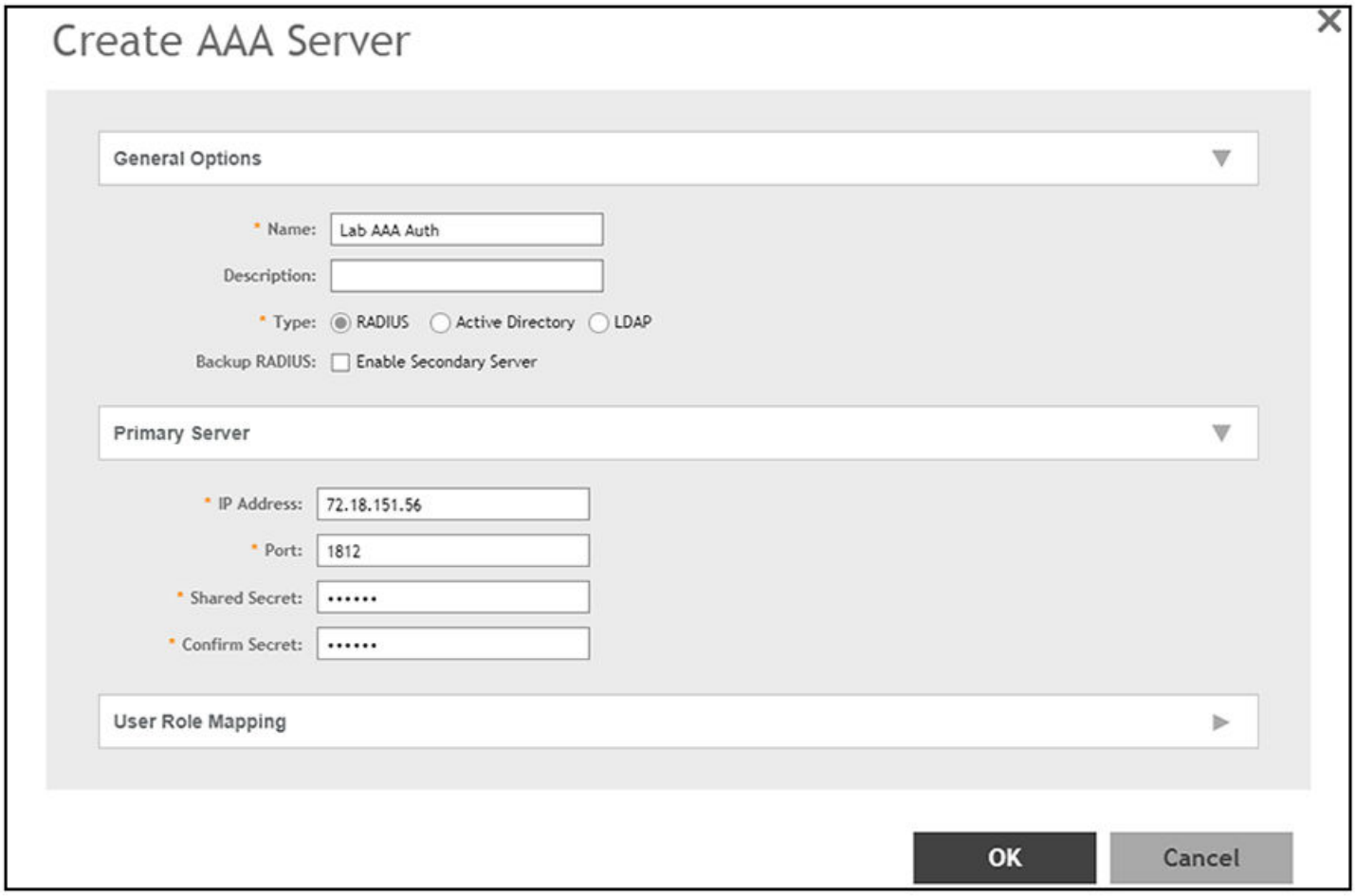
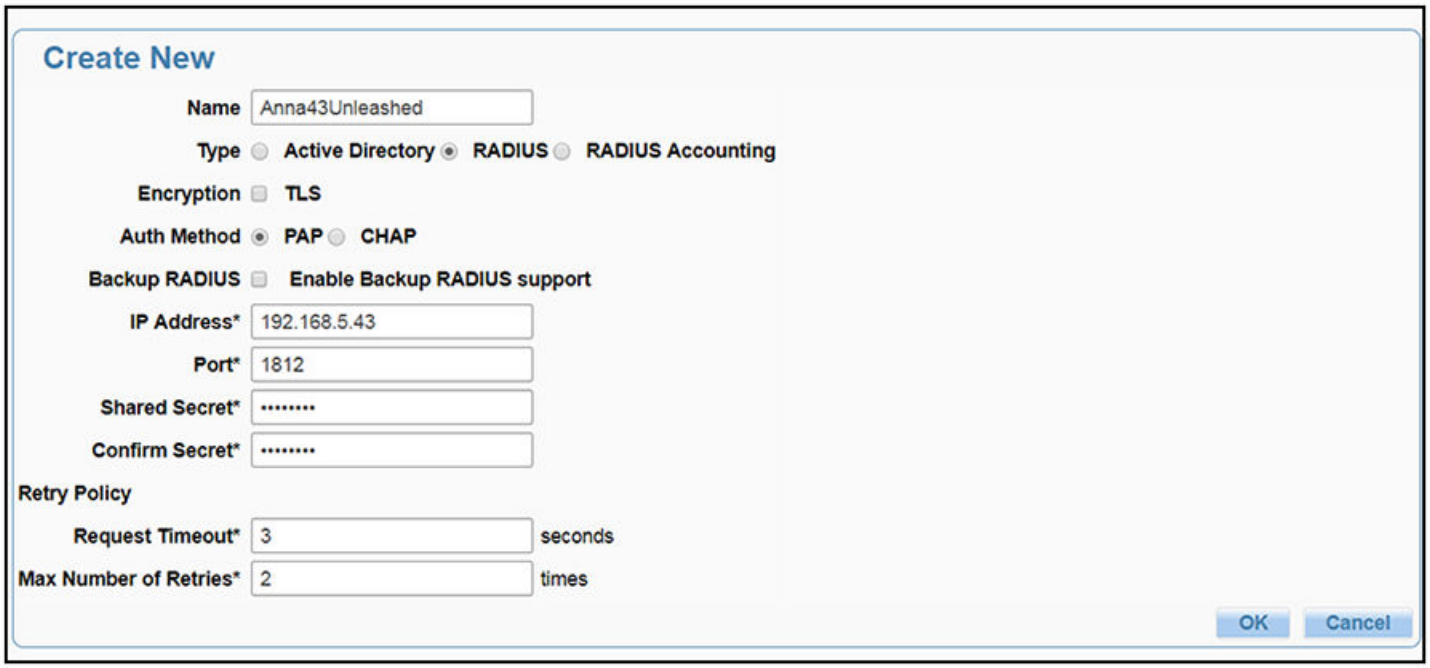


FIGURE 4 Create AAA Authentication Server on Unleashed



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

1. Name
2. Type = RADIUS
3. Auth Method (not applicable for SmartZone) = PAP
4. IP address = The IP address of the Cloudpath ES.
5. Port = 1812
6. Shared Secret = This must match the shared secret for the Cloudpath ES onboard RADIUS server. (**Configuration** > **RADIUS Server**).
7. Leave the default values for the remaining fields.

Creating AAA Accounting Server (Optional)

Use the same process to create the AAA Accounting Server.

> **NOTE**
> To navigate to the correct screen on Ruckus SmartZone, go to **Services & Profiles > Accounting**.

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

1. Name
2. Type = RADIUS ACCOUNTING.
3. IP address = The IP address of the Cloudpath ES.

4. Port = 1813

   NOTE
   The Authentication server uses port 1812. The Accounting server uses port 1813.

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

Running Authentication Test

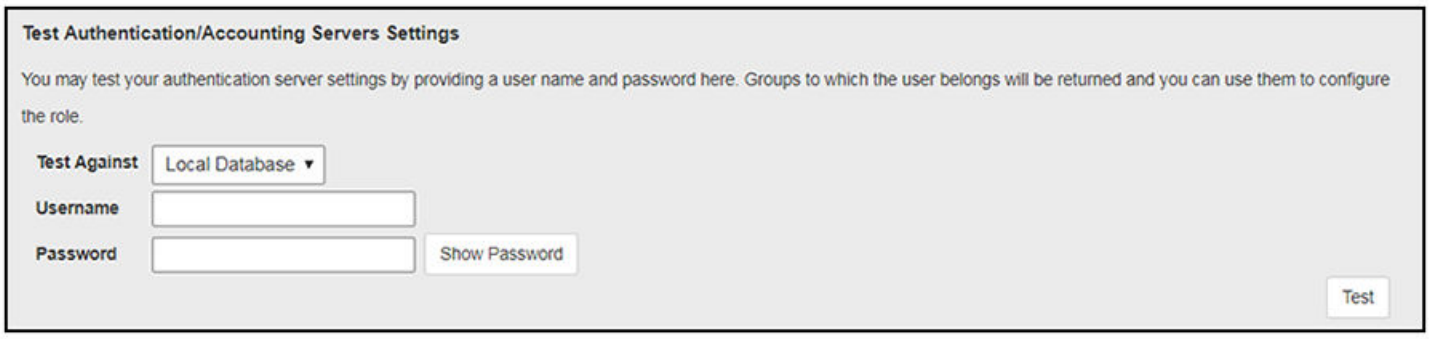
You can test the connection between the controller and the Cloudpath ES RADIUS server.

Follow the instructions for the applicable controller. For the possible results, see Possible Results from Authentication Test.

ZoneDirector

At the bottom of the AAA server page, there is a section called "Test Authentication/Accounting Servers Settings." The Test Against field should be Local Database, as shown below. Enter a test User Name and Password, then click the **Test** button.

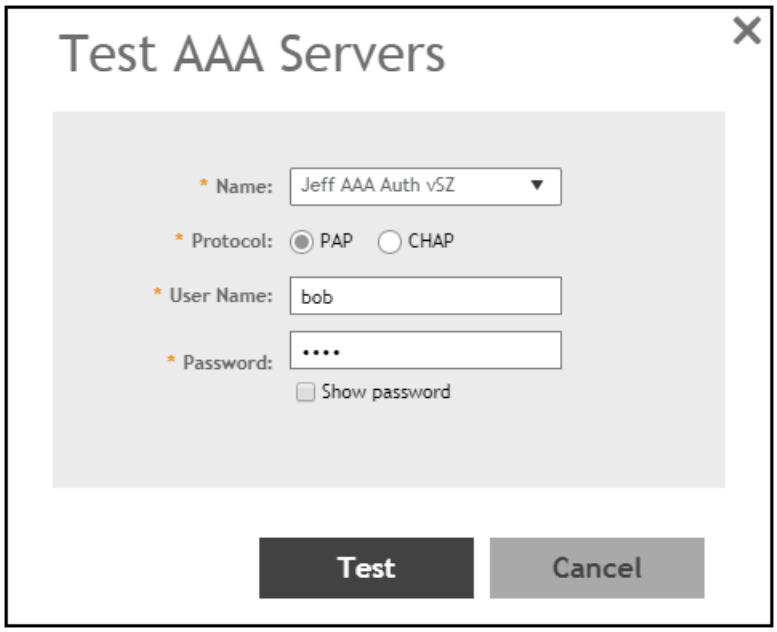
FIGURE 5 Authentication Test on ZoneDirector



SmartZone

When you save a configuration for an AAA Authentication server in SmartZone, you can click the **Test AAA** tab at the top of the screen, select the server from the drop-down list, enter your credentials, then click the **Test** button.

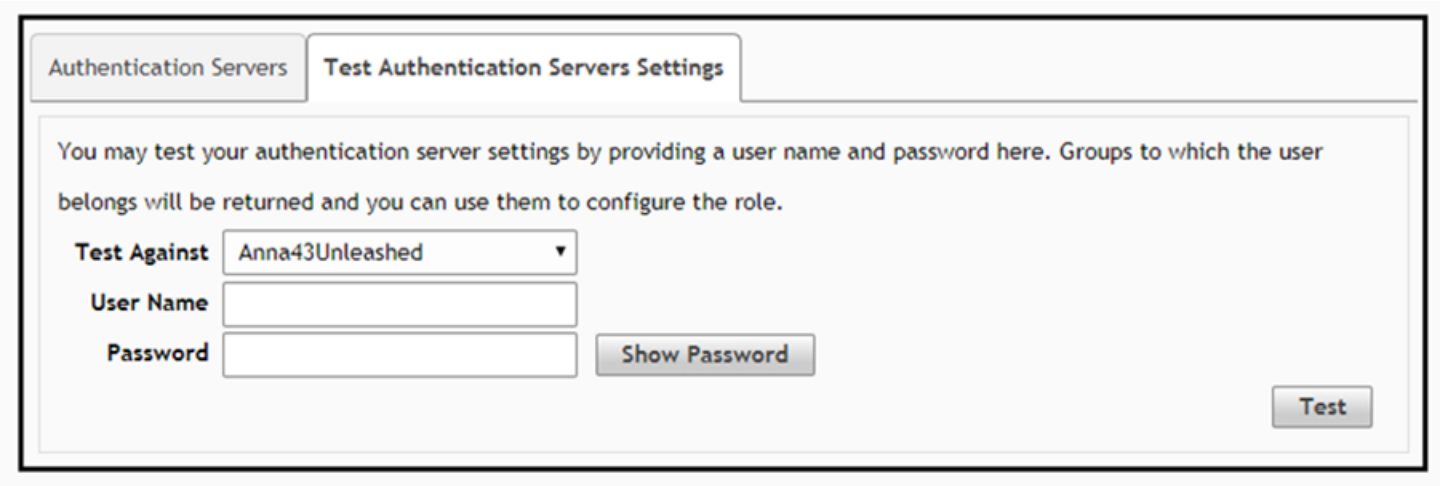
FIGURE 6 Authentication Test on SmartZone



Unleashed

Enter the test credentials on the Test Authentication Servers Settings tab, then click the **Test** button.

FIGURE 7 Authentication Test on Unleashed



Possible Results from Authentication Test

If you run the authentication test, you receive one of these responses:

- `Failed! Connection timed out`
- `Failed! Invalid username and password`

- `Authentication Failed`

The only one of these responses that means that connectivity was established is:

```
Failed! Invalid username or password
```

Creating Hotspot Services

You can configure the Hotspot Service on the ZoneDirector, SmartZone, or Unleashed controllers.

1. Navigate to: For ZoneDirector, go to **Services & Profiles > Hotspot Services**. For SmartZone, go to **Services & Profiles > Hotspots & Portals > Hotspot WISPr**. For Unleashed, go to **Admin & Services > Services > Hotspot Services**, then use both the **General** tab and the **Authentication** tab, as instructed later in this section.

2. Name the Hotspot Service.

FIGURE 8 Create Hotspot Service on ZoneDirector

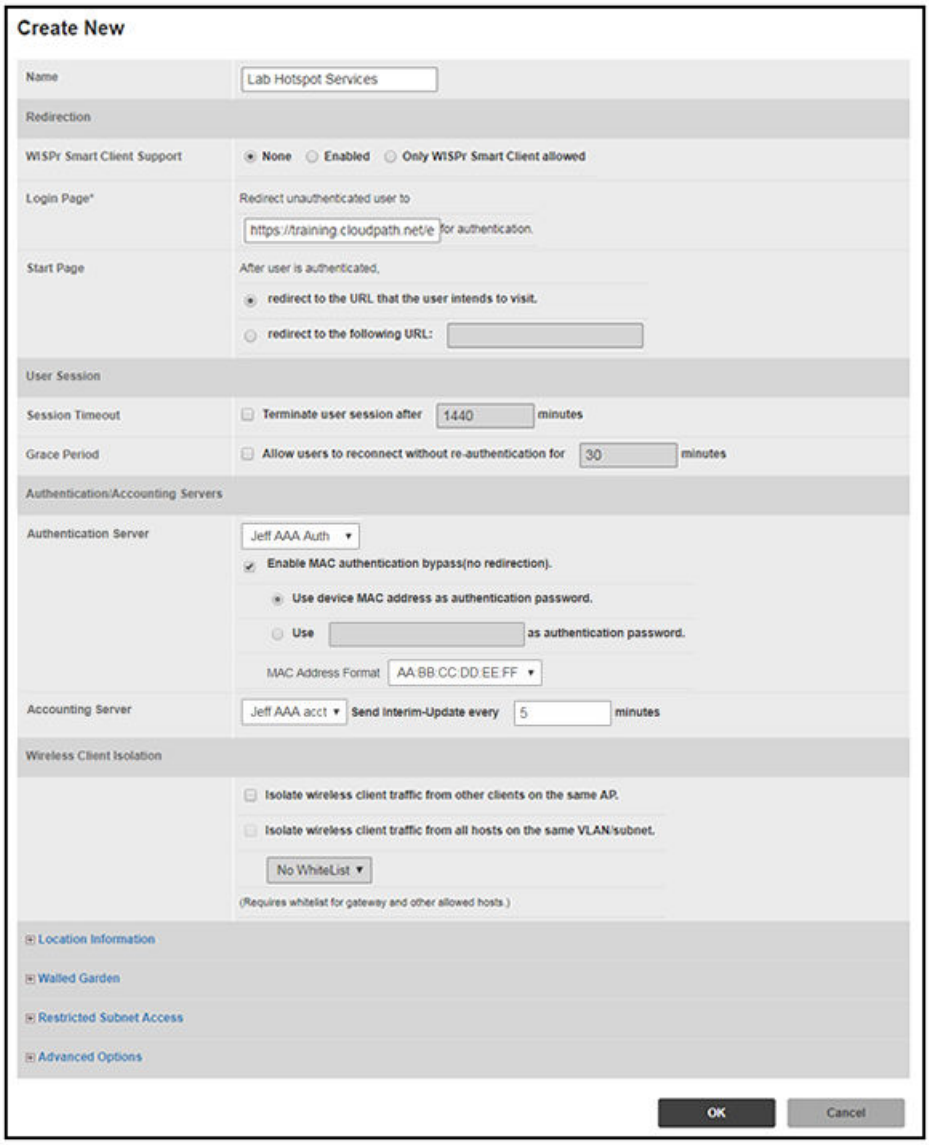


FIGURE 9 Create Hotspot WISPr on SmartZone

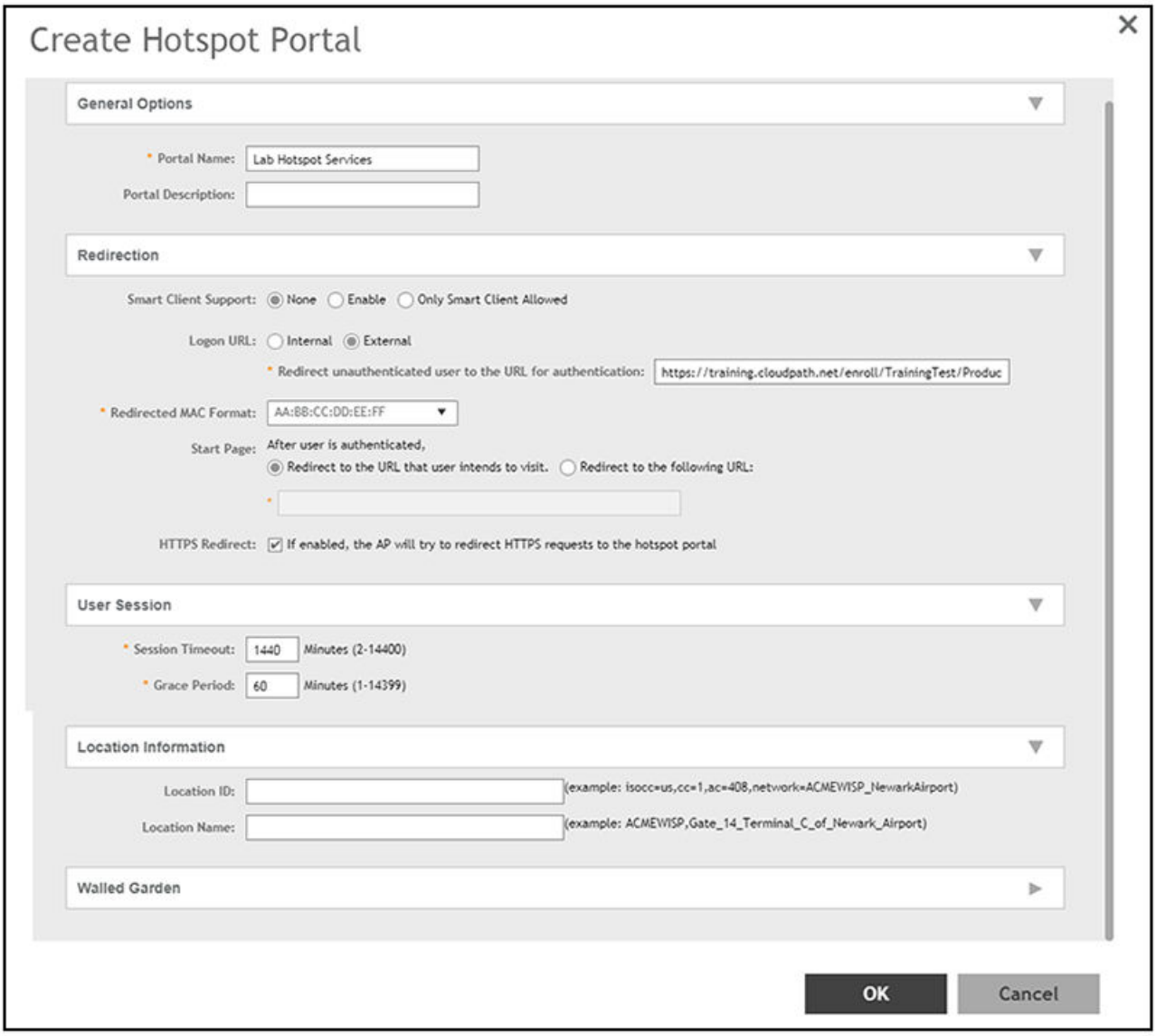


FIGURE 10 Create Hotspot Service on Unleashed - General Tab

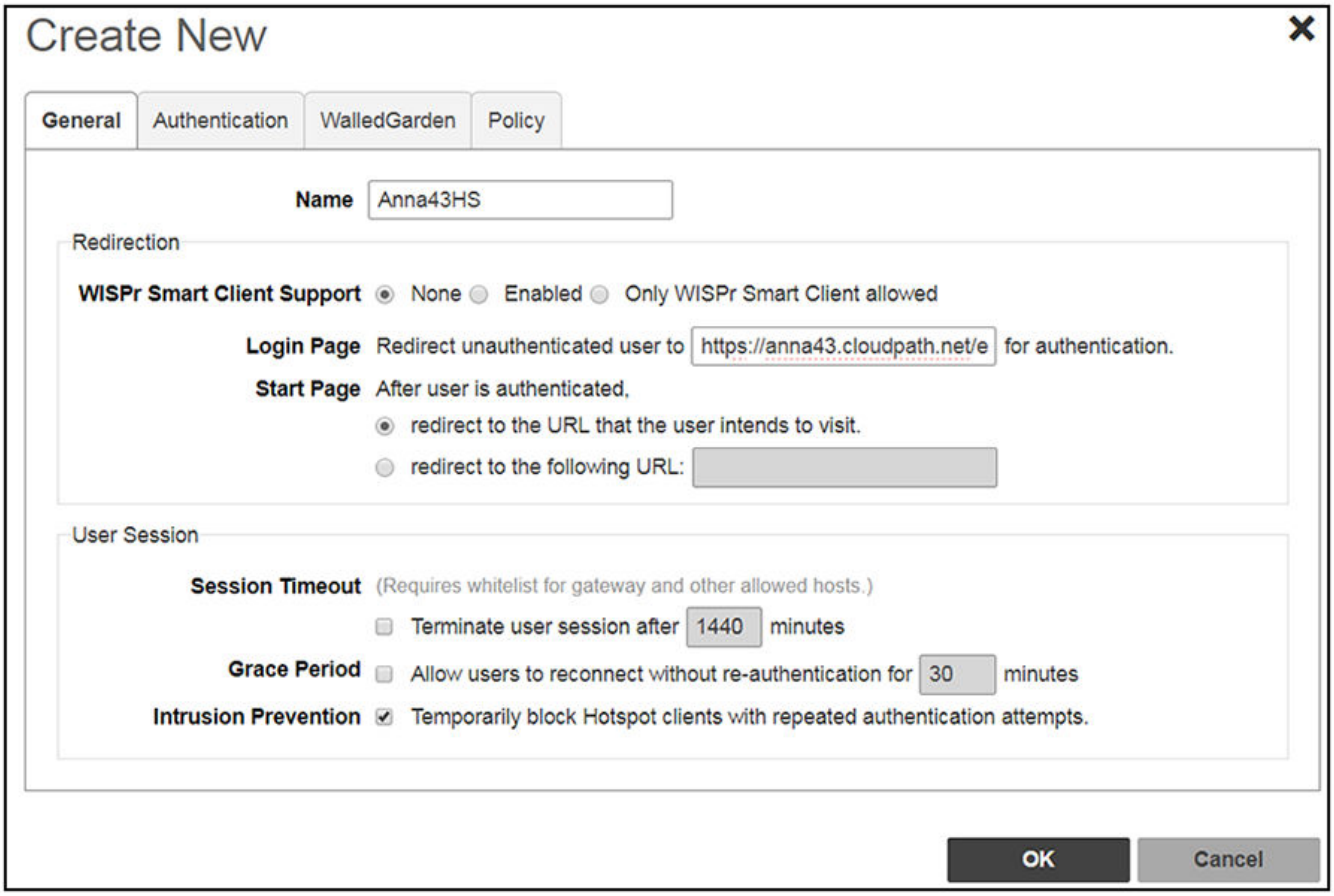
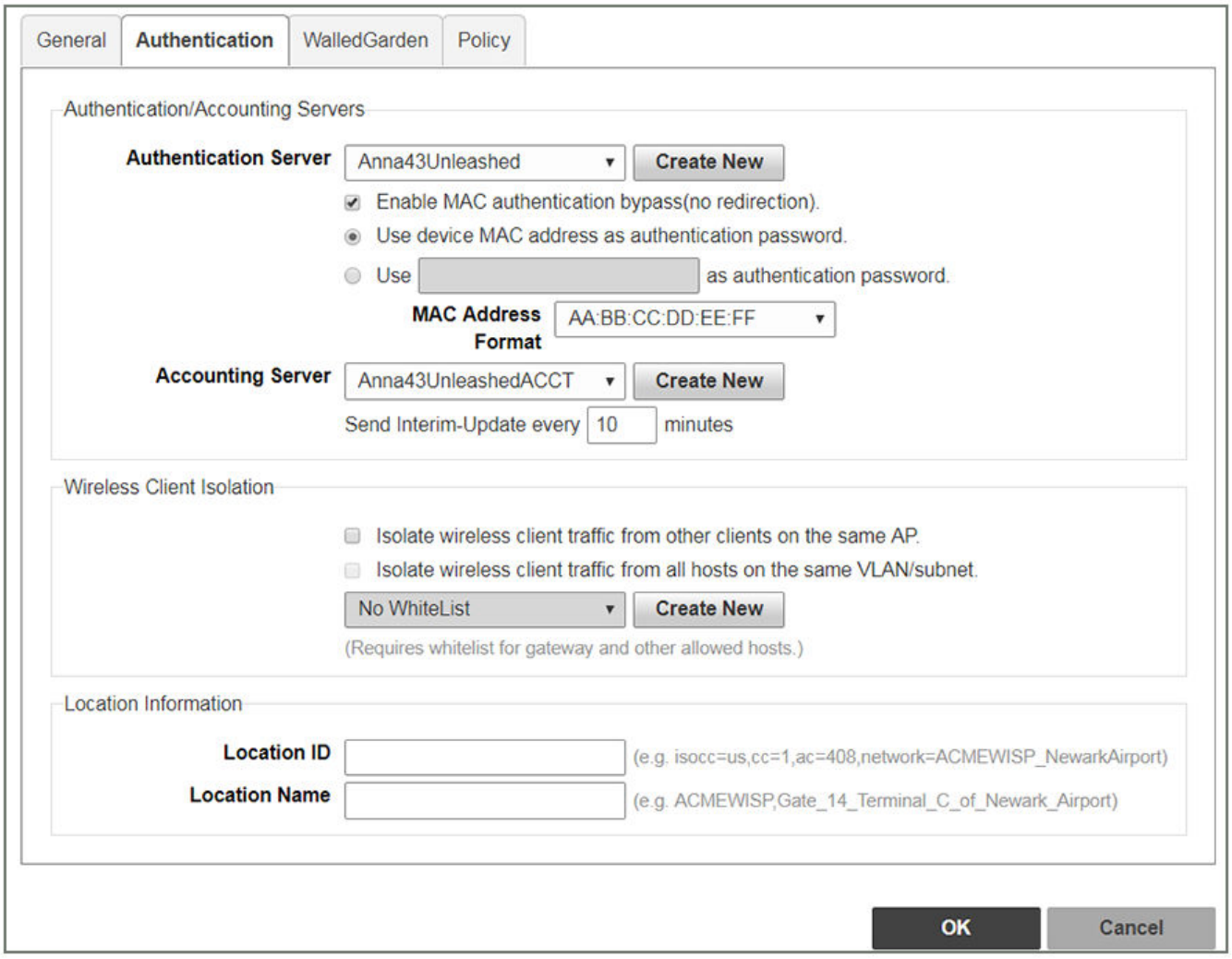


FIGURE 11 Create Hotspot Service on Unleashed - Authentication Tab



3. Point the unauthenticated user to the **Cloudpath Enrollment Portal URL**, which can be found on the **Cloudpath Admin UI Configuration** > **Workflows** page, in the **Workflows** table.
4. Check **Redirect to the URL that the user intends to visit**.
5. Select the **Cloudpath RADIUS Authentication Server**. Applicable only for ZoneDirector and Unleashed (**Authentication** tab) in this screen.
6. Select **Enable MAC authentication bypass (no redirection)**. Applicable only for ZoneDirector and Unleashed (**Authentication** tab) in this screen. Selecting this field allows users with registered MAC addresses to be transparently authorized without having to log in.
7. For MAC Address Format (which appears when you select **Enable MAC authentication bypass (no redirection)** in the preceding step, it is recommended that you select the following option from the drop-down list: AA:BB:CC:DD:EE:FF
8. Select the **Cloudpath RADIUS Accounting Server**. Applicable only for ZoneDirector and Unleashed (**Authentication** tab).
9. Leave the defaults for the remaining settings. Click **OK**.

Setting Up the Walled Garden

Perform the following steps to add a walled garden configuration to your existing Hotspot Services configuration:

1. Navigate to: For ZoneDirector, go to **Services & Profiles > Hotspot Services**. For SmartZone, go to **Services & Profiles > Hotspots & Portals > Hotspot WISPr**. For Unleashed, go to **Admin & Services > Services > Hotspot Services**.

2. For ZoneDirector and SmartZone, use the **edit** function on the existing Hotspot Services configuration, then scroll to the **Walled Garden** section and expand this section. For Unleashed, click the **WalledGarden** on the existing Hotspot Services configuration.

FIGURE 12 Walled Garden Configuration for ZoneDirector

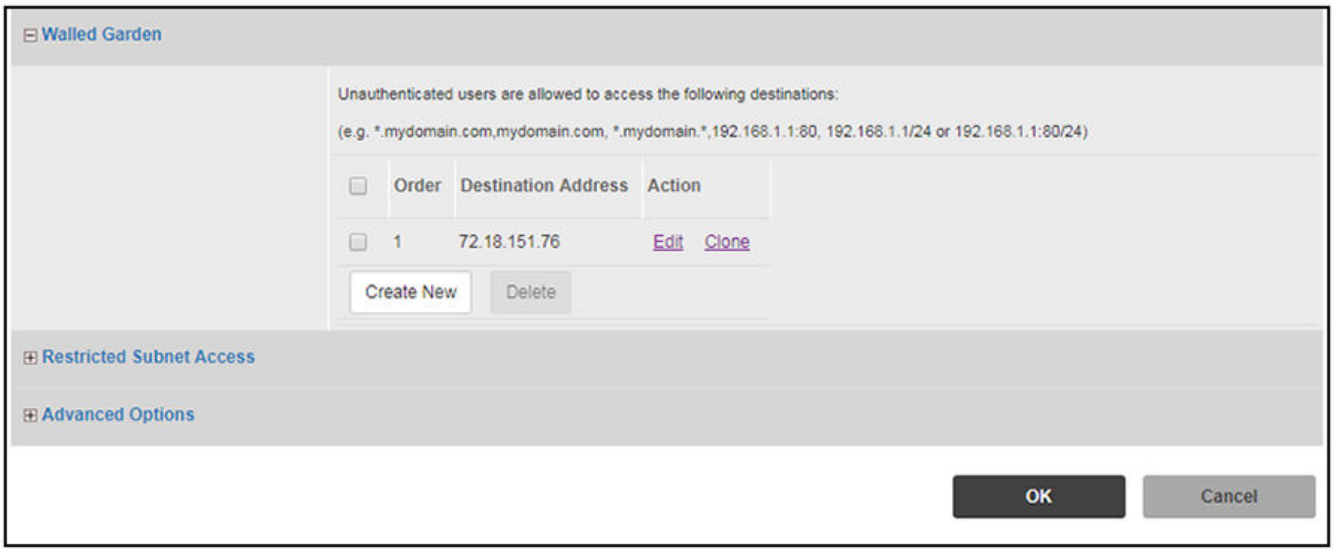


FIGURE 13 Walled Garden Configuration for SmartZone

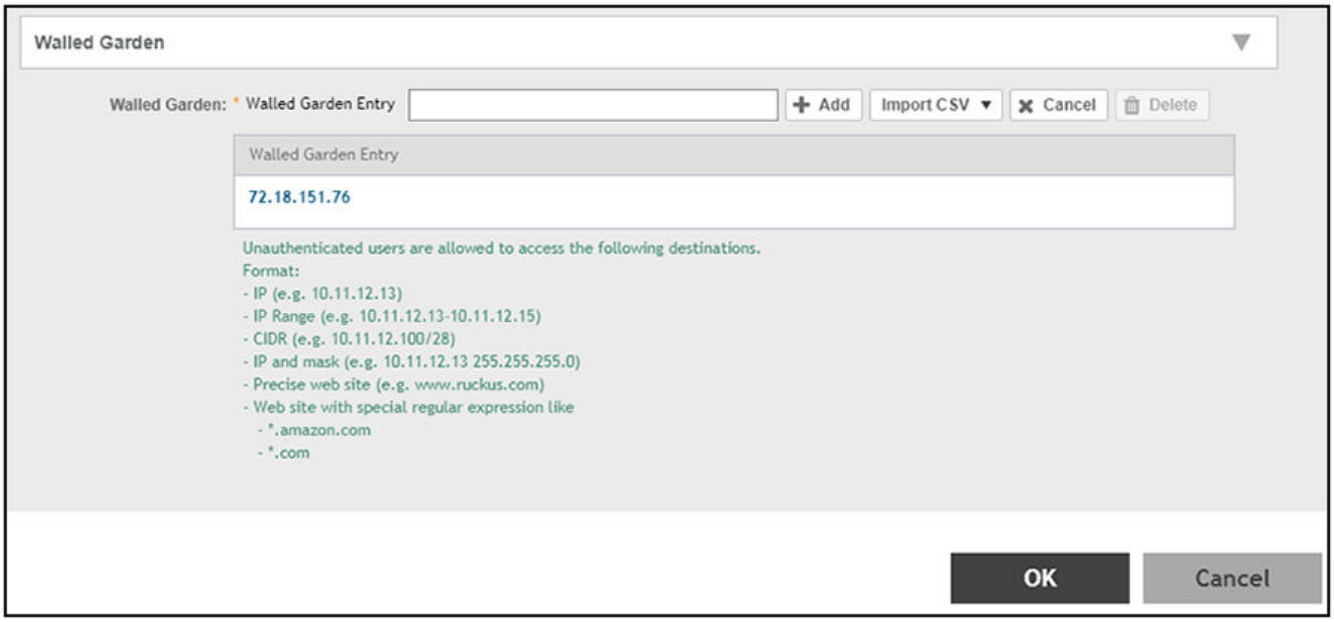
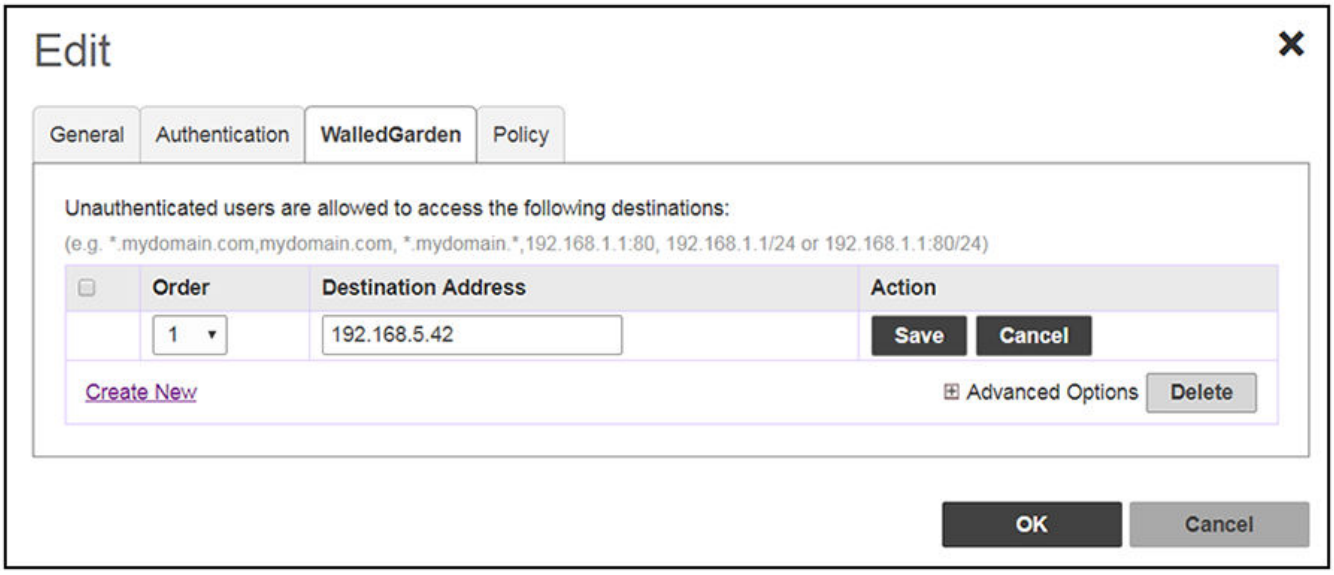


FIGURE 14 Walled Garden Configuration for Unleashed



3. Include the DNS or IP address of the Cloudpath system, then click **OK**.
4. 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.

5. 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

To configure the onboarding SSID, navigate to: For ZoneDirector and SmartZone, go to the Wireless LANS section of the controller UI; for Unleashed, go to **Wifi Networks** to create the WLAN.

1. Name the SSID.

2. Type=Hotspot Service (WISPr).

FIGURE 15 Onboarding SSID Configuration on ZoneDirector

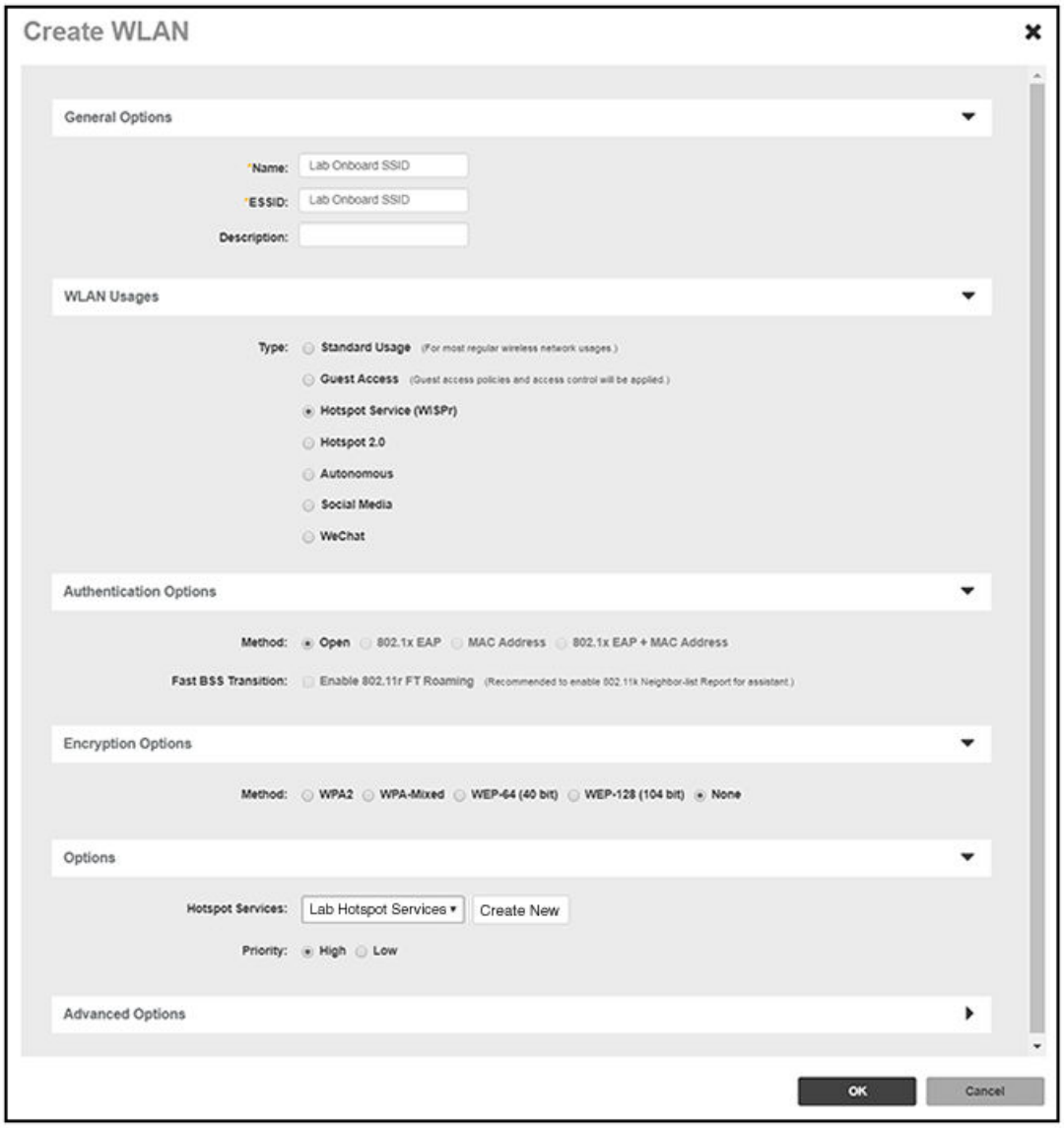


FIGURE 16 Onboarding SSID Configuration on SmartZone

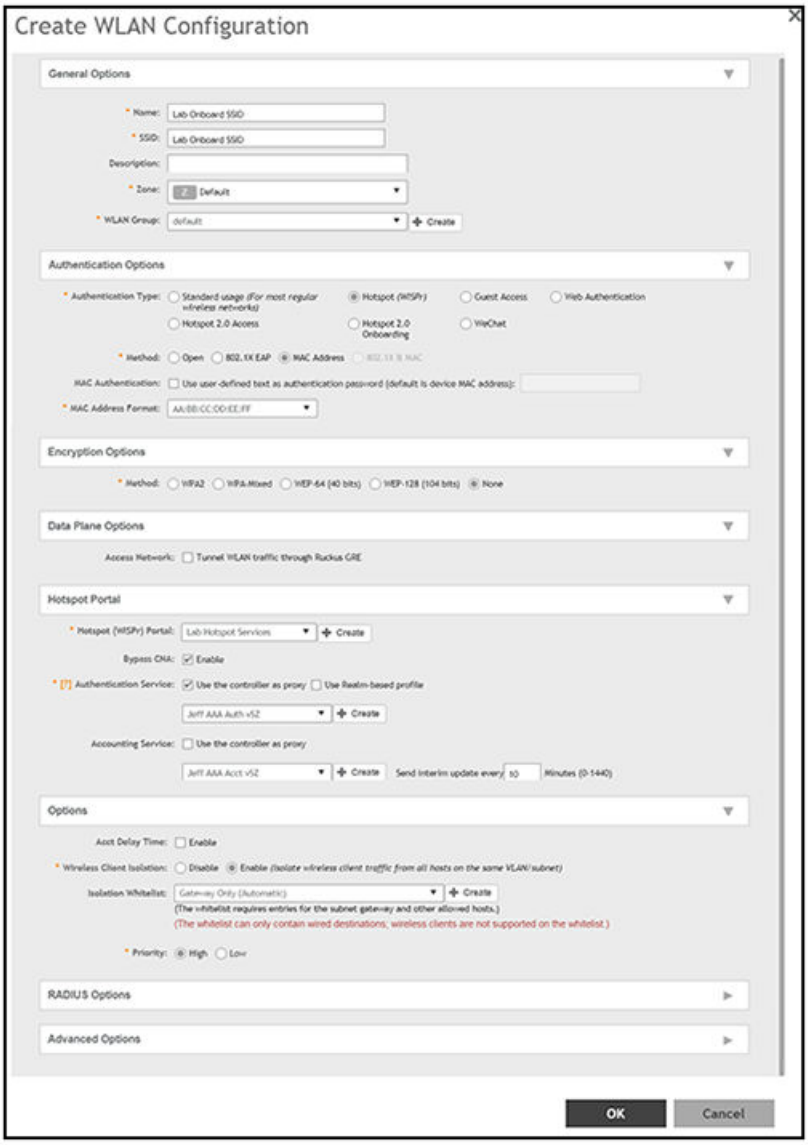
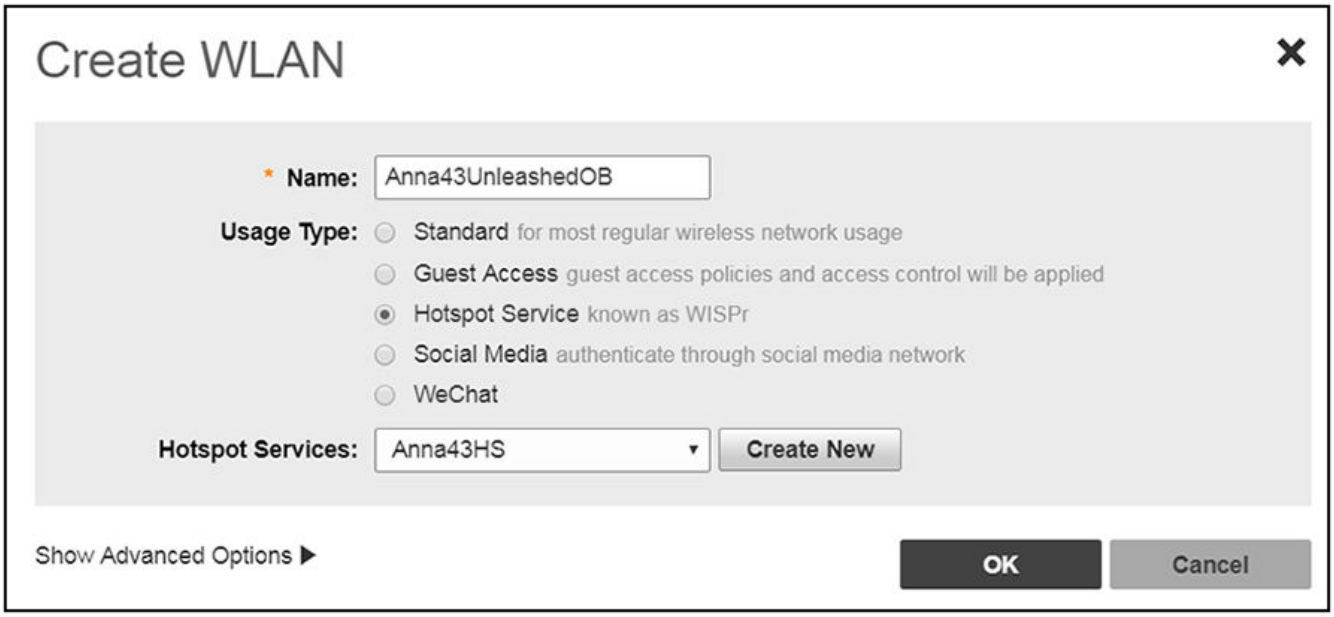


FIGURE 17 Onboarding SSID Configuration for Unleashed



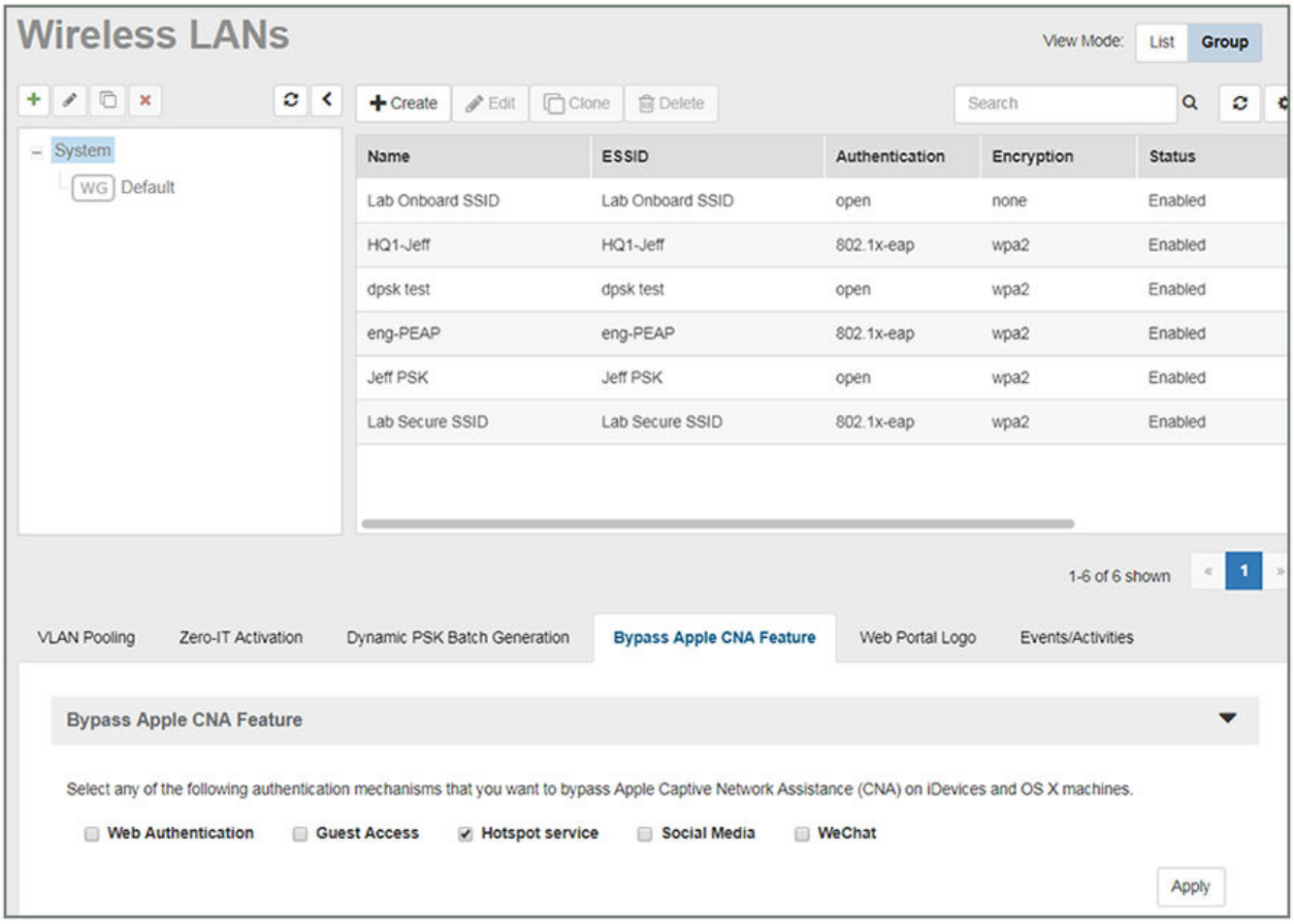
3. Authentication Options Method=Open for ZoneDirector, MAC Address for SmartZone. (Not applicable for Unleashed.)
4. The checkbox next to MAC Authentication (SmartZone only) called "Use user defined text as authentication password (default is device MAC address):" can be left unchecked.
5. The MAC Address Format (SmartZone only) recommended selection is: AA:BB:CC:DD:EE:FF. This is the default for most RADIUS servers.
6. Encryption Options Method=None (ZoneDirector and SmartZone).
7. Select the Hotspot Service from the drop-down list that you should already have created in a previous step procedure.
8. Enable the **Bypass CNA** feature as follows, depending on the controller:
   - For SmartZone: Check the box to enable "Bypass CNA," as shown in Figure 16.
   - For ZoneDirector, after you finish configuring the onboarding SSID, refer to Figure 18 on page 23.
   - For Unleashed, after you finish configuring the onboarding SSID, refer to Figure 20 on page 24.
9. Select the Cloudpath RADIUS Authentication Server (SmartZone only).
10. Select the Cloudpath RADIUS Accounting Server (SmartZone only).
11. Leave the defaults for the remaining settings and click **OK** (or **Apply**).

Enabling Bypass CNA on ZoneDirector

It is recommended to enable the "Bypass Apple CNA Feature," which you can do globally for wireless LANs in ZoneDirector.

1. In the Wireless LANs main screen, click on **Bypass Apple CNA Feature**, as shown in the following figure:

FIGURE 18 Enabling the Bypass Apple CNA Feature Globally on ZoneDirector



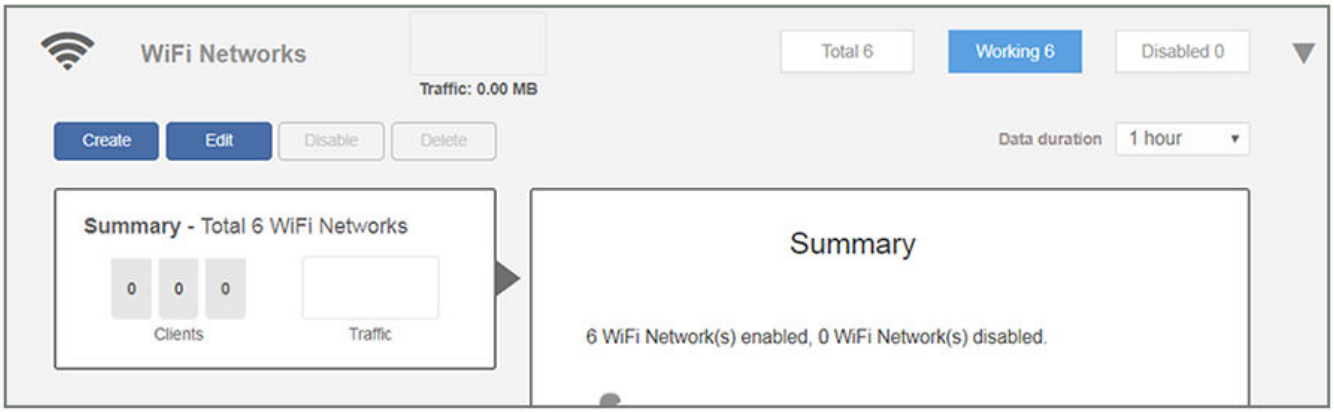
2. In the "Bypass Apple CNA Feature" area of the screen, check the "Hotspot service" box.
3. Click **Apply** to enable the "Bypass Apple CNA Feature" globally on all Wireless LANs that are configured as type "Hotspot Service (WISPr)."

Enabling Bypass CNA on Unleashed

It is recommended to enable the "Bypass Apple CNA Feature," which you can do globally for wireless LANs in Unleashed.

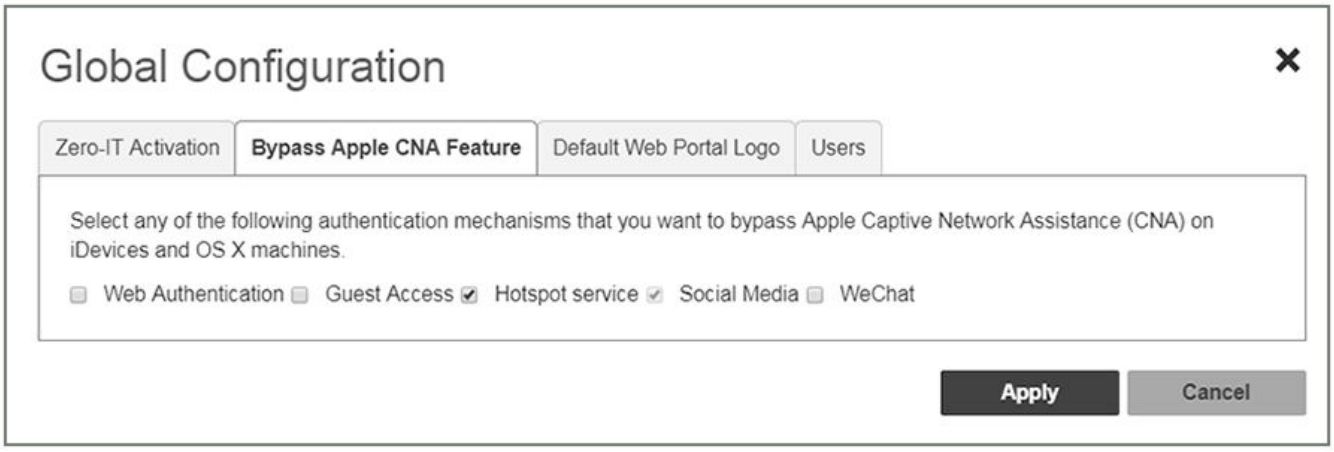
1. In the WiFi Networks main screen (see figure below), click **Edit**.

   FIGURE 19 Clicking the Edit Button Brings you to Global Configuration



2. In the Global Configuration screen that pops up, click **Bypass Apple CNA Feature**.

   FIGURE 20 Enabling the Bypass Apple CNA Feature Globally on Unleashed



3. In the "Bypass Apple CNA Feature" area of the screen, check the "Hotspot service" box.
4. Click **Apply** to enable the "Bypass Apple CNA Feature" globally on all Wireless LANs that are configured as type "Hotspot Service (WISPr)."

Cloudpath Configuration

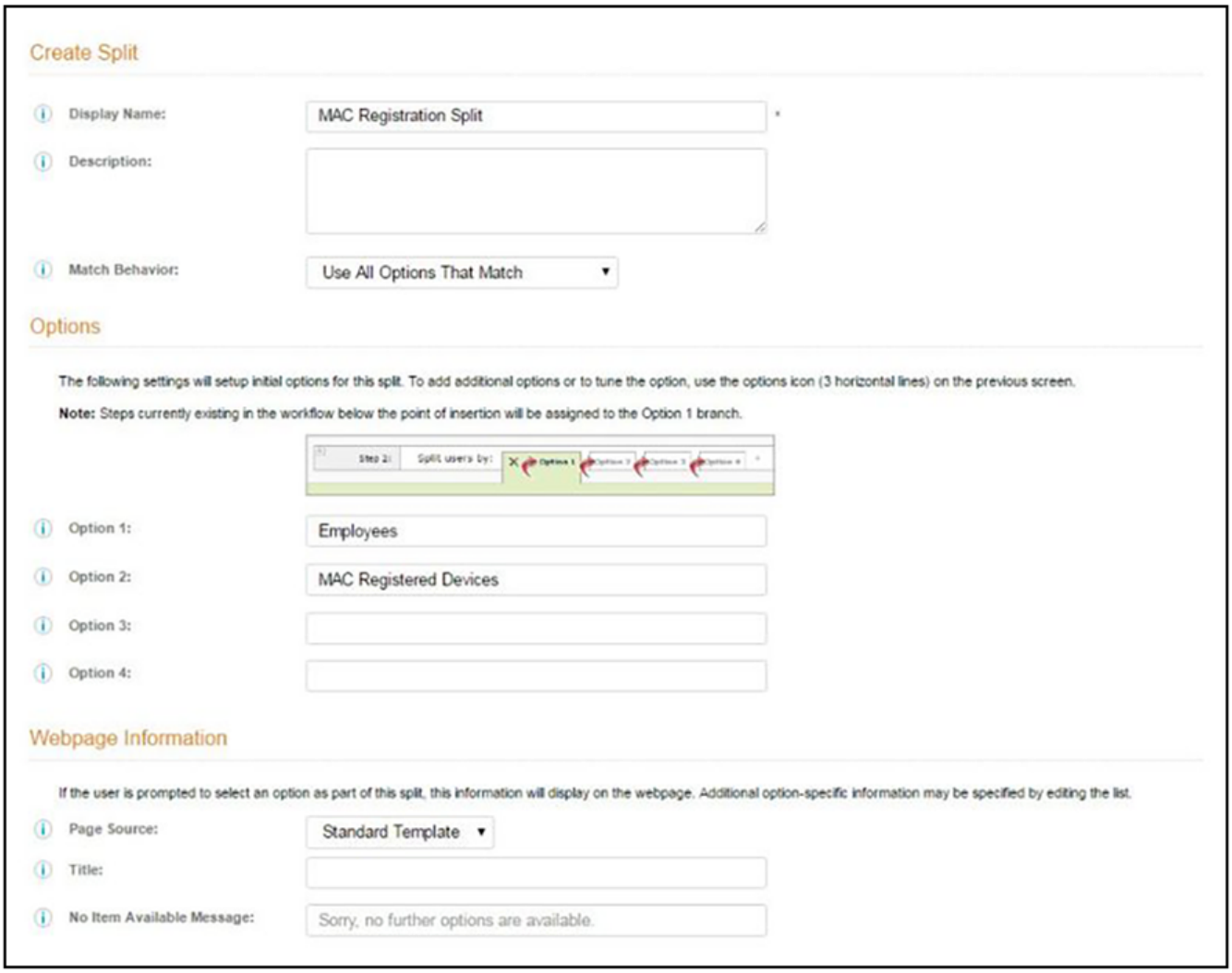
This section describes how to create a workflow for MAC registration, add RADIUS attributes to a MAC registration configuration, and how to import a file of MAC addresses to a MAC registration list.

Create a MAC Registration Workflow

NOTE
Creating this workflow includes a step for adding a MAC registration step. At that time, you have the option of creating a new registration configuration or selecting an existing configuration. If you want to create a registration configuration before creating your workflow, refer to Using the MAC Registrations Main Page on page 32

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

FIGURE 21 Create Split



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

   For example, you can name Option 1, **Employees**, and Option 2, **MAC-Registered**.
8. Leave the defaults for the other fields and **Save**.

The named branches appear as tabs in the split workflow step.

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

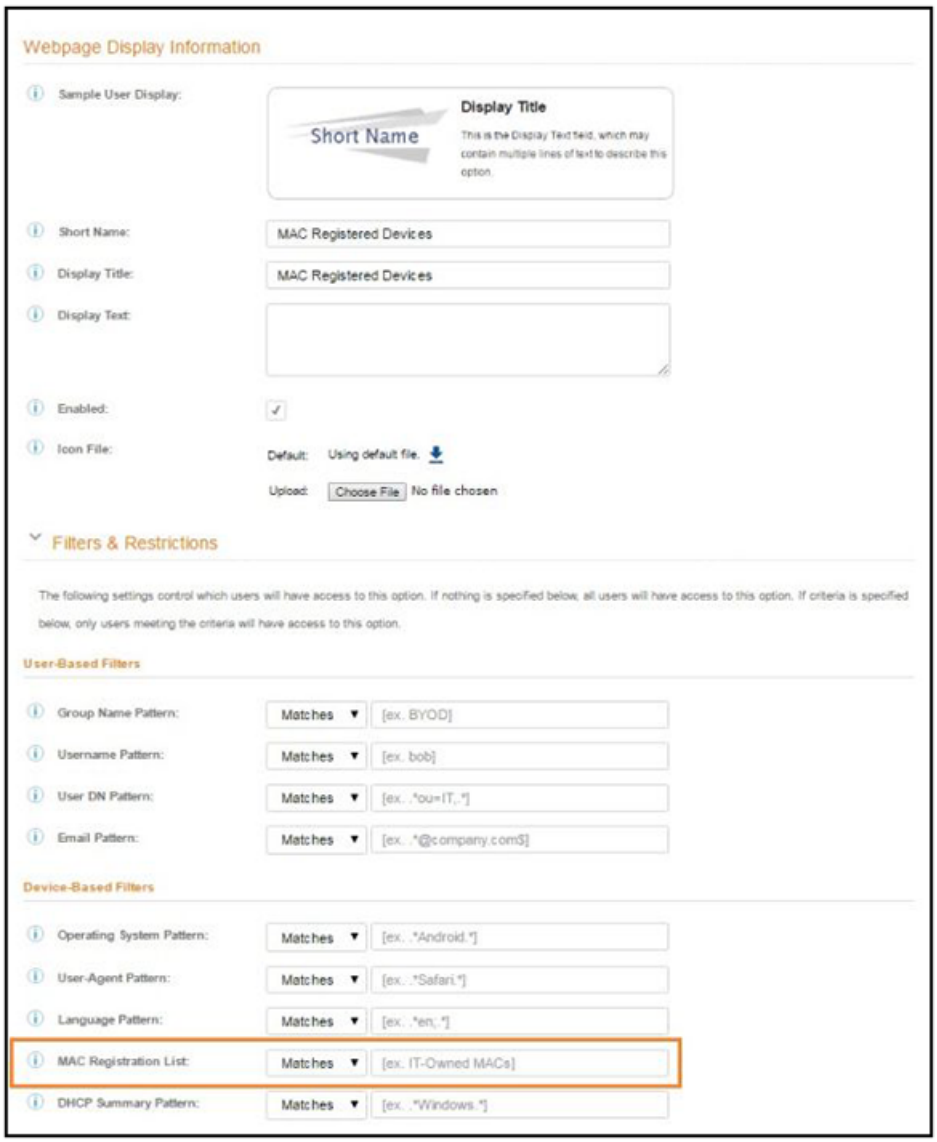
How to Create a Filter in the Workflow for MAC-Registered Devices

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

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

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

FIGURE 22 Modify Split Options



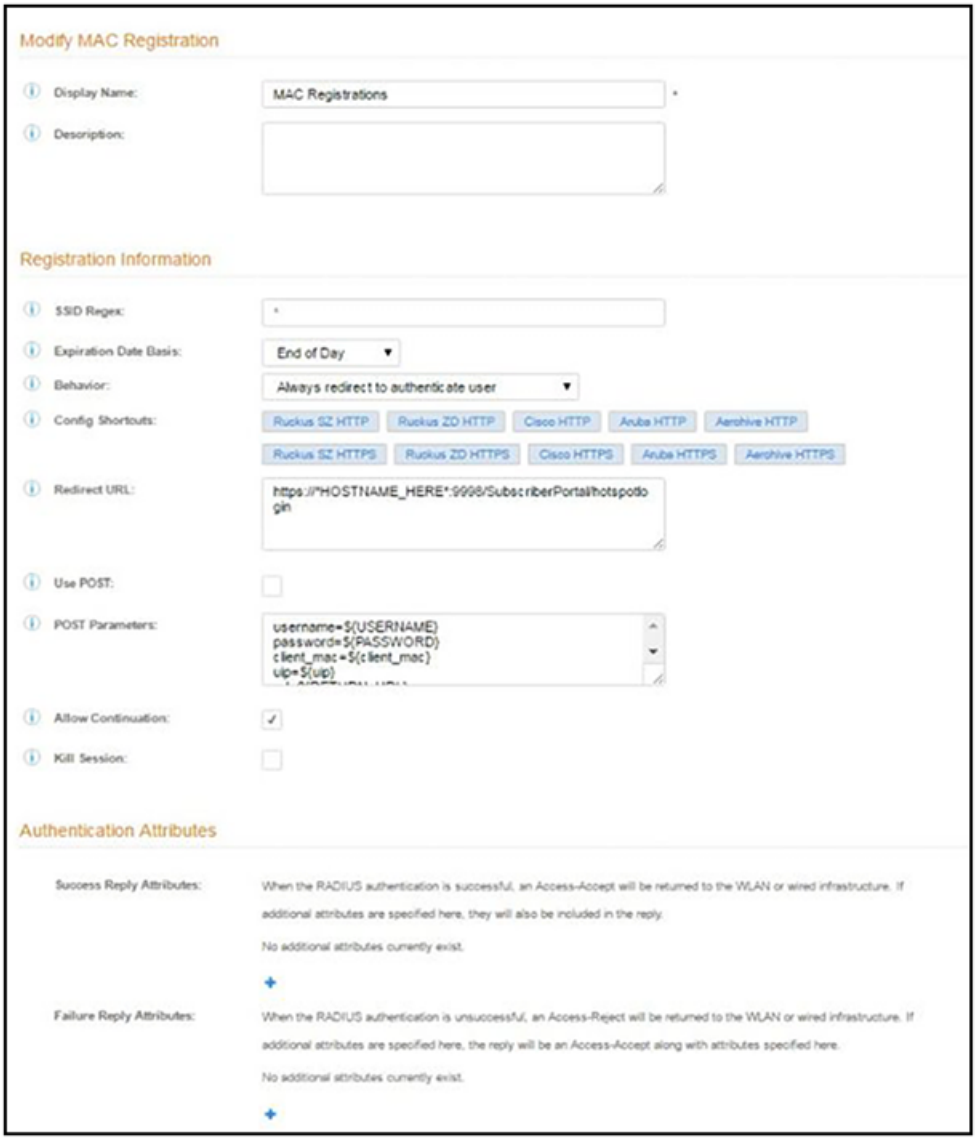
4. **Save** the changes to the option filter.
5. Click **Done** to return to the workflow.

How to Add a MAC Registration Step to the Workflow

1. On the workflow page, click the **Insert** arrow to create a step Enter the values in the Registration Information section:in the enrollment workflow.

2. Select **Register device for MAC-based authentication**.
3. Create a new registration configuration. The **Create MAC Registration** page opens.

FIGURE 23 Create MAC Registration



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

5. Enter the values in the **Registration Information** section:
   - SSID Regex - This is the SSID to which MAC registered devices are assigned.

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

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

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

   - 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 disappear, depending on your selection for Expiration Date Basis. For example, in the screen shown above, "End of Day" has been selected for Expiration Date Basis, which makes the "Offset" field unnecessary.

   - Behavior - Specifies the prompt and redirect settings for the MAC registration configuration. Use the **Web Page Information** section to configure the user prompt or redirect URL. Behavior settings include:
     - Prompt user when MAC is unknown.
     - Always prompt the user.
     - Redirect when MAC is unknown.
     - Always redirect to authenticate user. (This is the default and the most commonly used setting).
     - Skip registration when MAC is unknown.
   - Use the **Config Shortcuts** buttons to populate the **Redirect URL** and **POST Parameters** according to your controller vendor and preferred protocol.
   - Allow Continuation - If checked, the submit-redirect call is processed, if unchecked, the submit- redirect call is ignored.
   - Kill Session - If checked, the user's session will be killed as they are redirected and, if they return, they will be forced to start over.

Adding RADIUS Attributes

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

1. In the **Authentication Attributes** section, click **Add Attribute** for Successful (or Unsuccessful) Attempts.
2. Enter the **Attribute**, **Operator**, and **Value**. The attribute is added to the MAC Registration configuration.

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

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

How to Add a Message to Users

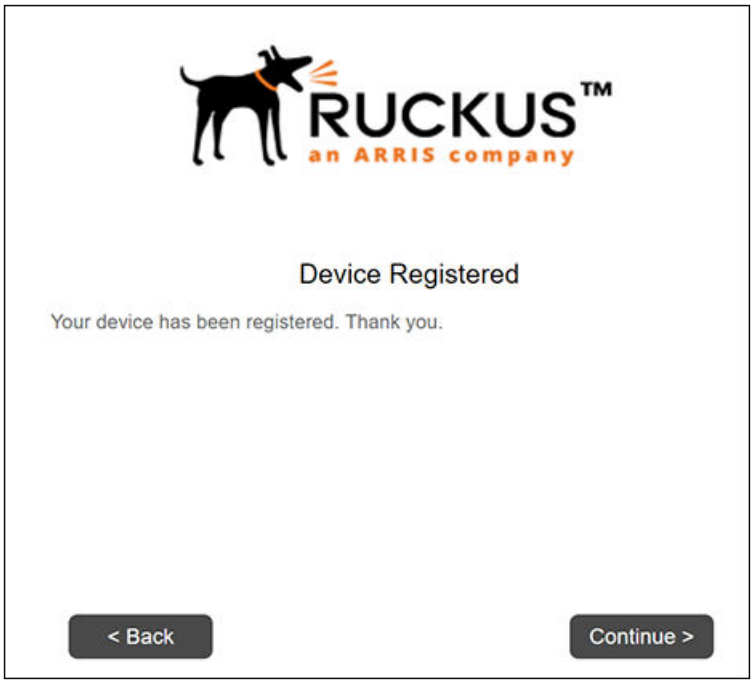
As a best practice, add a workflow step to display a message to the user indicating that the authentication was successful.

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

5. **Save** the configuration.

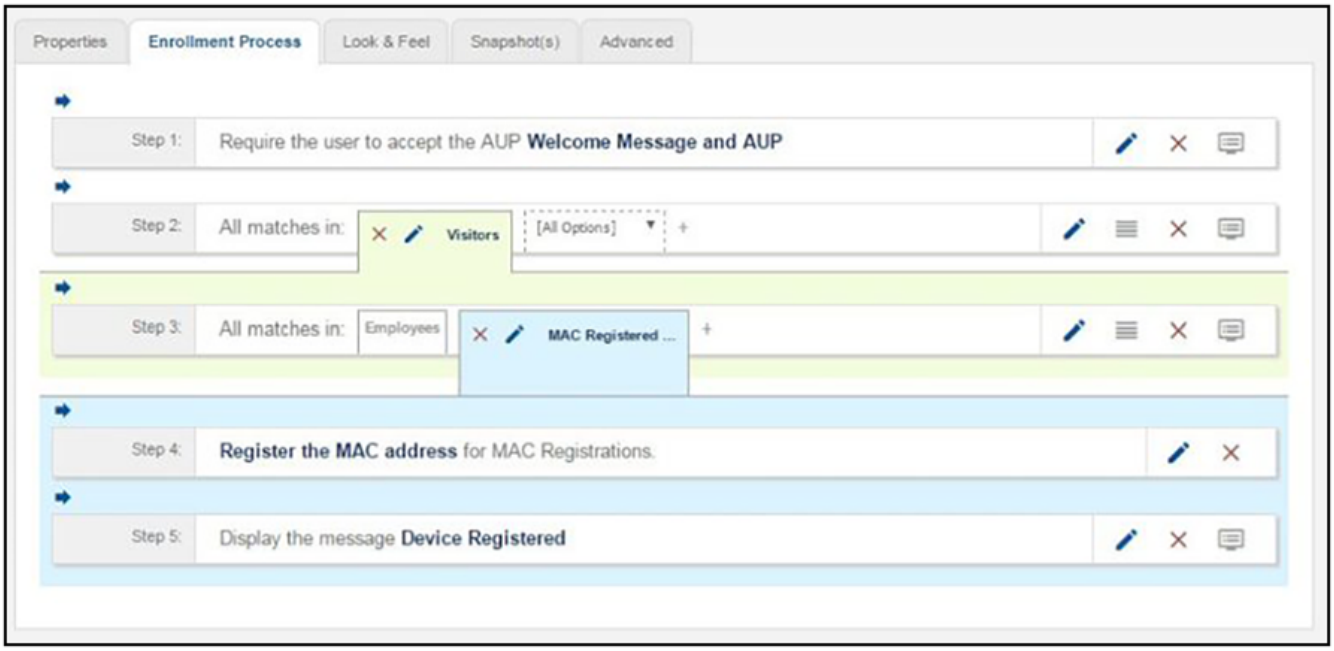
   On the workflow page, click the **view** icon next to the **Display Message** step to see a preview of the message.

   FIGURE 24 Example Message to User



   The completed workflow is displayed below.

FIGURE 25 Completed Workflow for MAC Registration

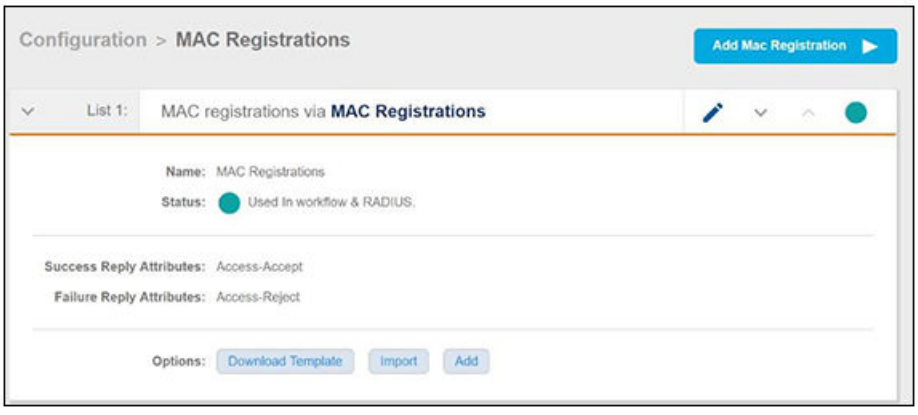


Using the MAC Registrations Main Page

From the main MAC Registration page, you can create MAC registration configurations, and import MAC registration lists or individual MAC addresses into these configurations for use in a workflow.

Navigate to **Configuration > MAC Registrations**. The figure below shows the page as it would appear if you already were using a configuration called "MAC Registrations" in a workflow, as the green status circle indicates.

FIGURE 26 MAC Registrations Main Page



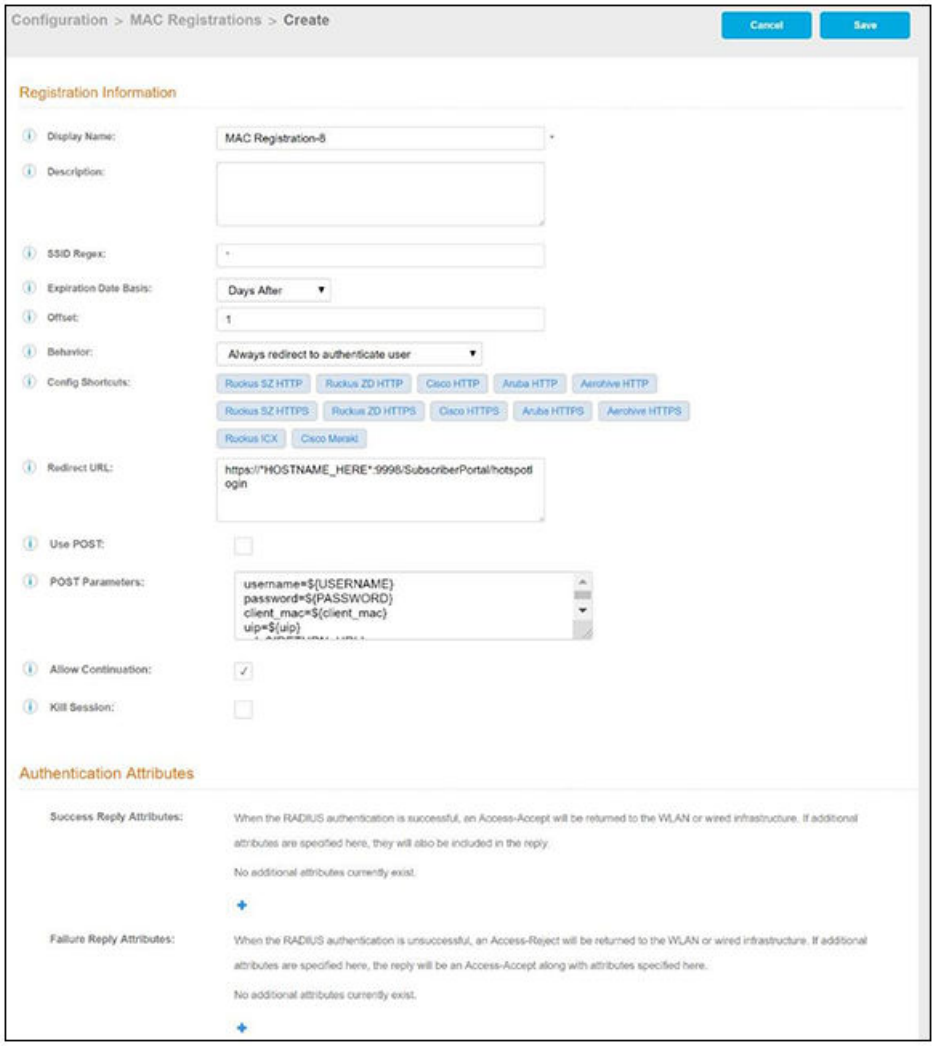
Adding a New MAC Registration Configuration

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

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

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

FIGURE 27 Creating a New MAC Registration Configuration



- 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.

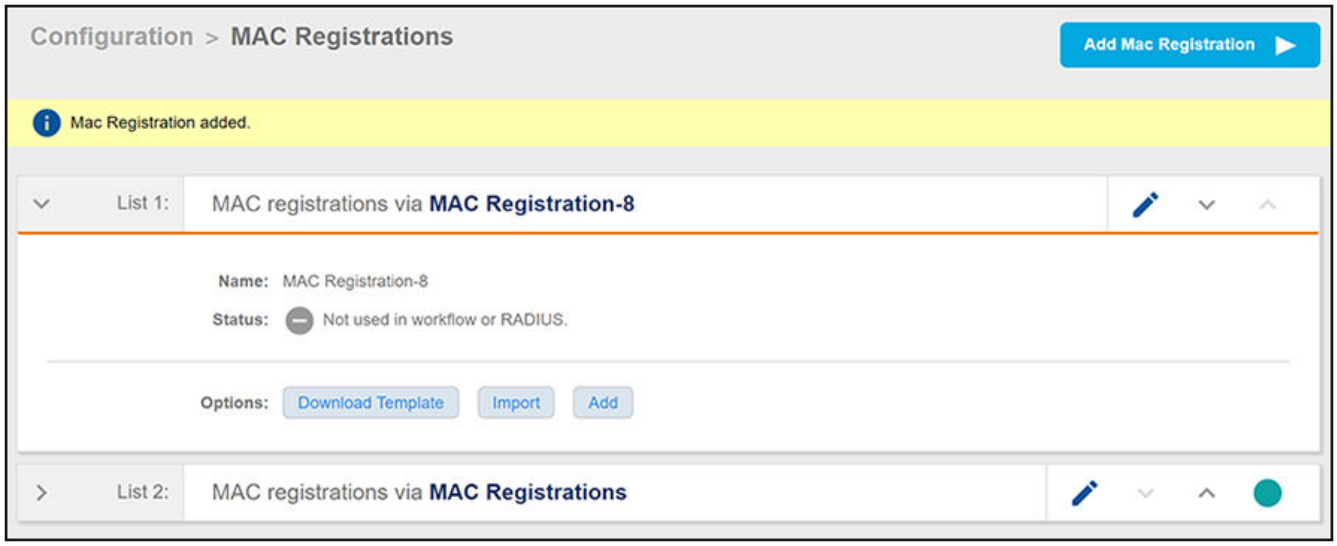
- Offset: The number of hours/days/months/etc to be offset from the event date when calculating the registration validity period. If **Specified Date** is selected, this should be the date in YYYY/MM/DD format.

  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. Use the **Web Page Information** section to configure the user prompt or redirect URL. Behavior settings include:
  - Prompt user when MAC is unknown.
  - Always prompt the user.
  - Redirect when MAC is unknown.
  - Always redirect to authenticate user. (This is the default and the most commonly used setting).
  - Skip registration when MAC is unknown.
- Use the **Config Shortcuts** buttons to populate the **Redirect URL** and **POST Parameters** according to your controller vendor and preferred protocol.
- Allow Continuation - If checked, the submit-redirect call is processed, if unchecked, the submit- redirect call is ignored.
- Kill Session - If checked, the user's session will be killed as they are redirected and, if they return, they will be forced to start over.
- Authentication Attributes: Refer to Adding RADIUS Attributes on page 29

3. After you click **Save**, 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 28 MAC Registrations Page After Adding a Second Registration Configuration



Importing a MAC Registration List

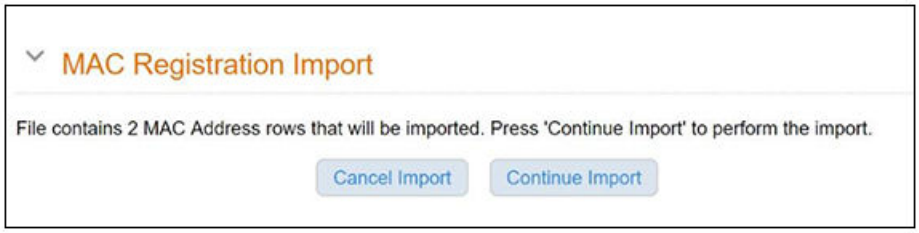
Follow these steps to import a MAC registration list into a MAC registration configuration.

1. Open the MAC registration configuration in which you want to import a MAC address list. You may have to click the arrow to the left of the MAC registration list number to expand the list, thus displaying the option buttons of "Download Template," "Import," and "Add."
2. If you first need a template for adding MAC addresses to an .xls file, click **Download Template**.
3. 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.

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

   FIGURE 29 Popup Asking You to Confirm Import of MAC Address List File



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

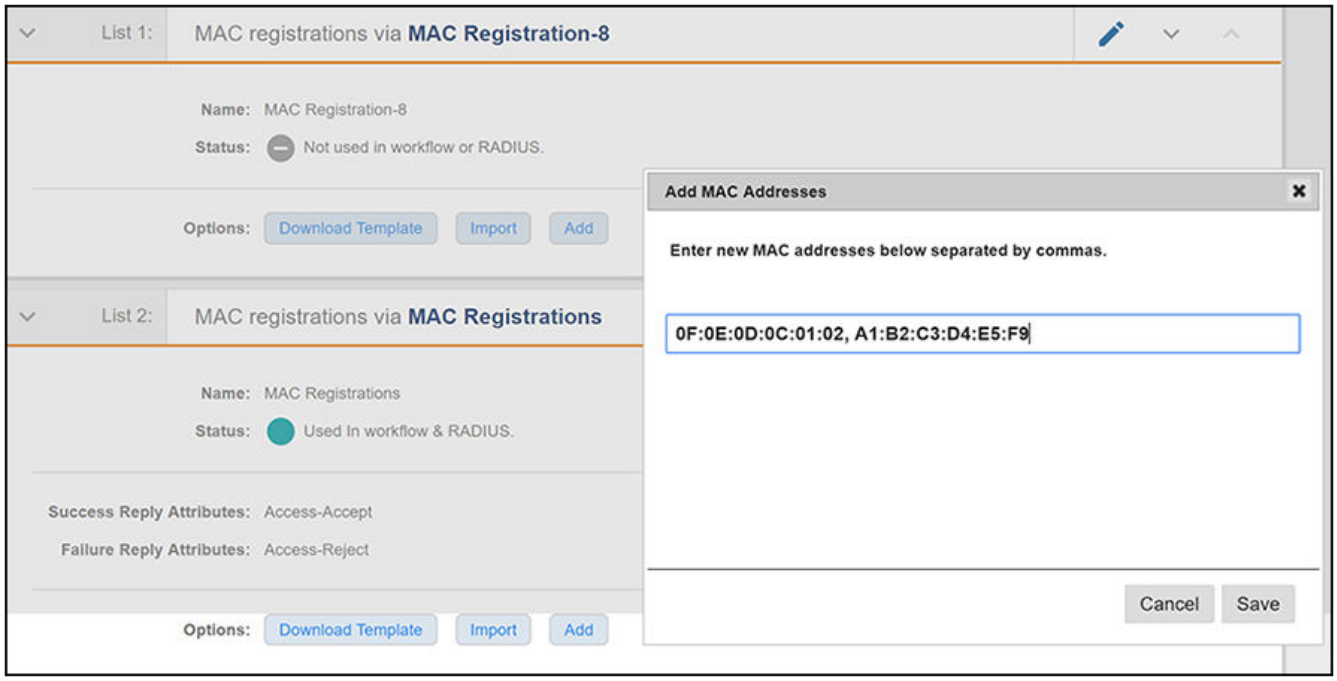
Importing Individual MAC Addresses

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

1. Open the MAC registration configuration in which you want to import a MAC address list. You may have to click the arrow to the left of the MAC registration list number to expand the list, thus displaying the option buttons of "Download Template," "Import," and "Add."
2. Click **Add**.

3. In the popup window, enter the MAC addresses, separated by commas, that you wish to add:

FIGURE 30 Entering Individual MAC Addresses



4. Click **Save**.
5. Confirm the import on the ensuing popup window.

   You are returned to the main page, and there should be a confirmation message at the top, indicating that the MAC addresses have been successfully added.

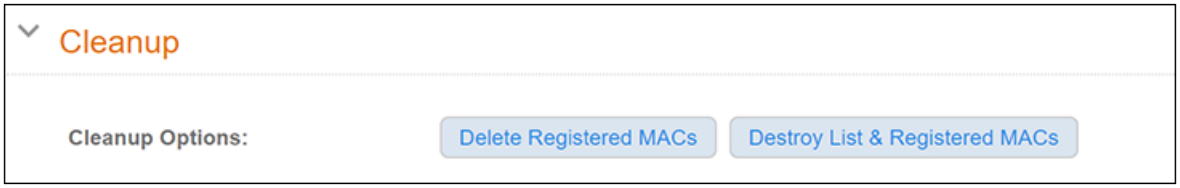
Removing a MAC Registration Configuration List or Its MAC Addresses

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 pencil icon to the right of the desired list.

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

   FIGURE 31 Cleanup Options for MAC Registration Configuration List



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

3. Click on the desired option.

   A Warning popup appears.

4. 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 main screen, where you should see a message indicating that your action has taken effect.

Viewing MAC Registration Records on the Dashboard

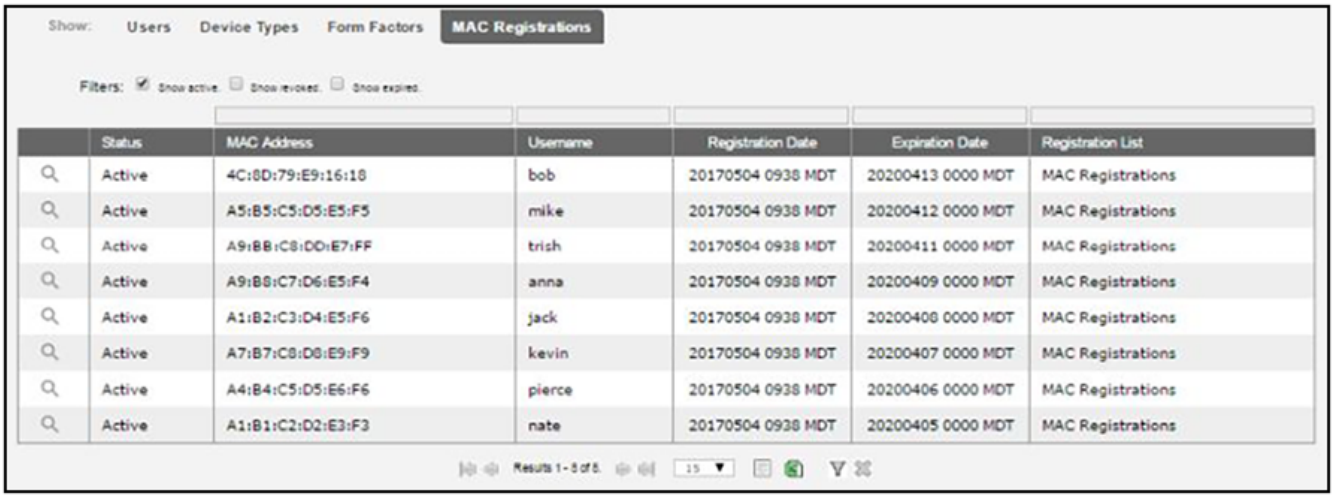
Administrators can view the records for devices that have been registered on the network using the MAC address, and, if needed, can revoke the registration.

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 32 MAC Registrations on the Dashboard



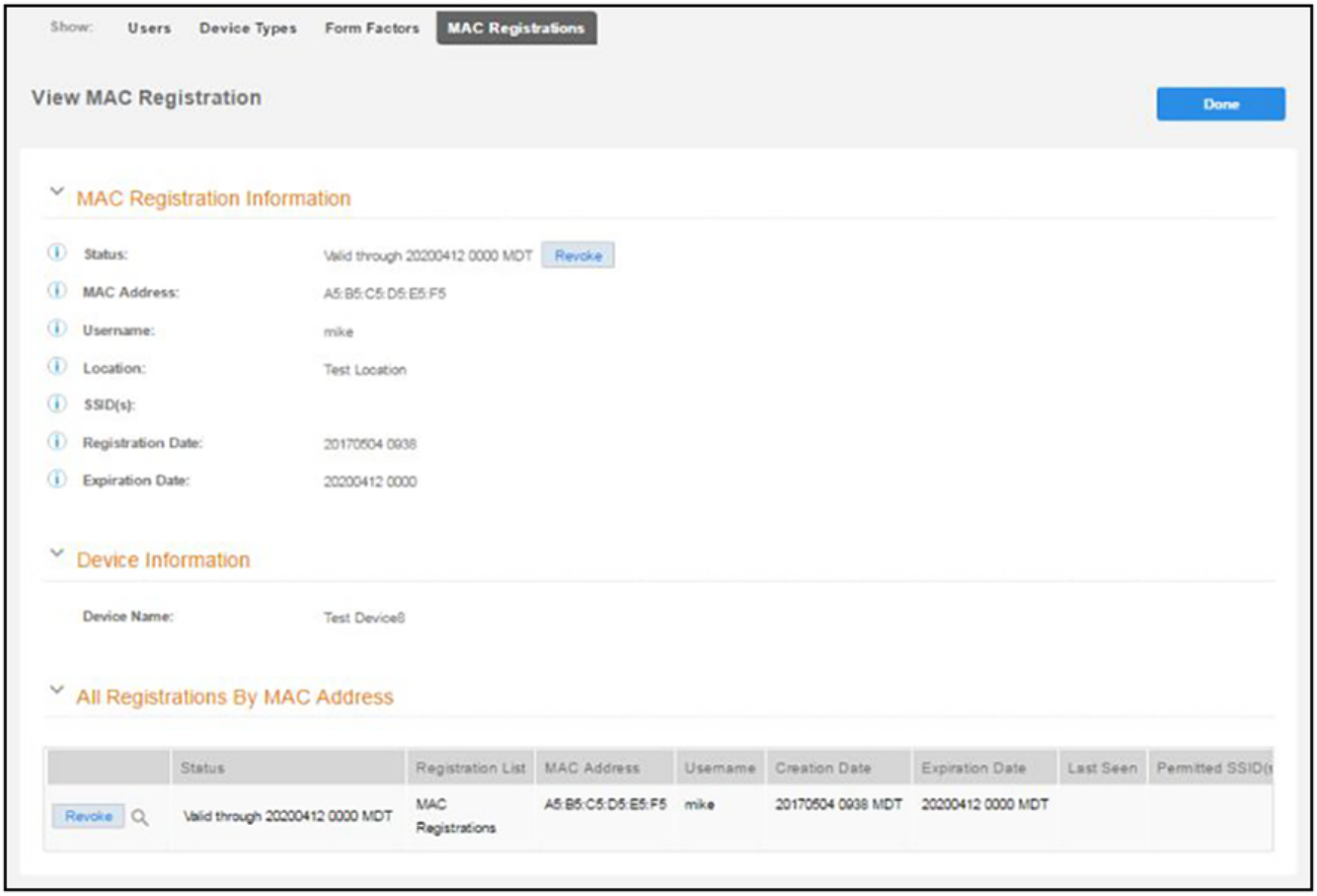
4. You can also access MAC registration information in the enrollment record. Go to **Operational** > **Dashboard** > **Enrollments** > **View Enrollment Record**.

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 33 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.

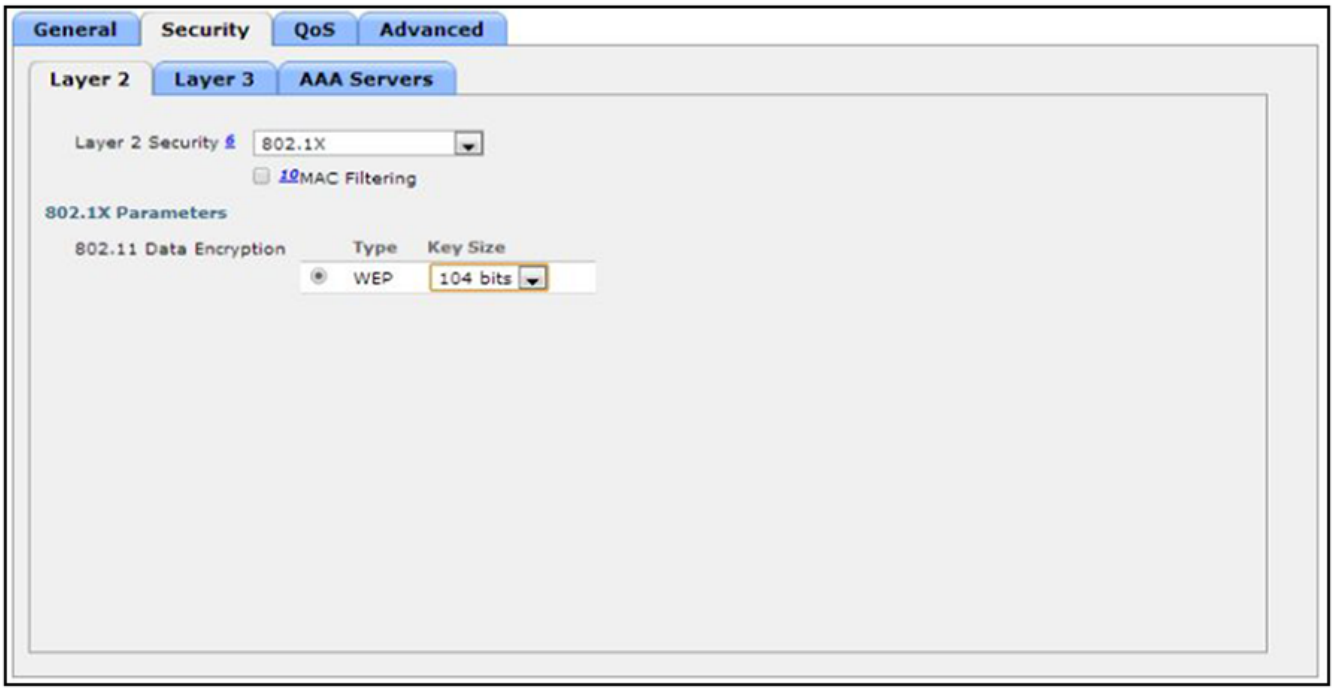
Configuring a Cisco Controller for MAC Registration

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 34 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 35 Layer 3 Settings when Using Layer 2 Mac Filtering

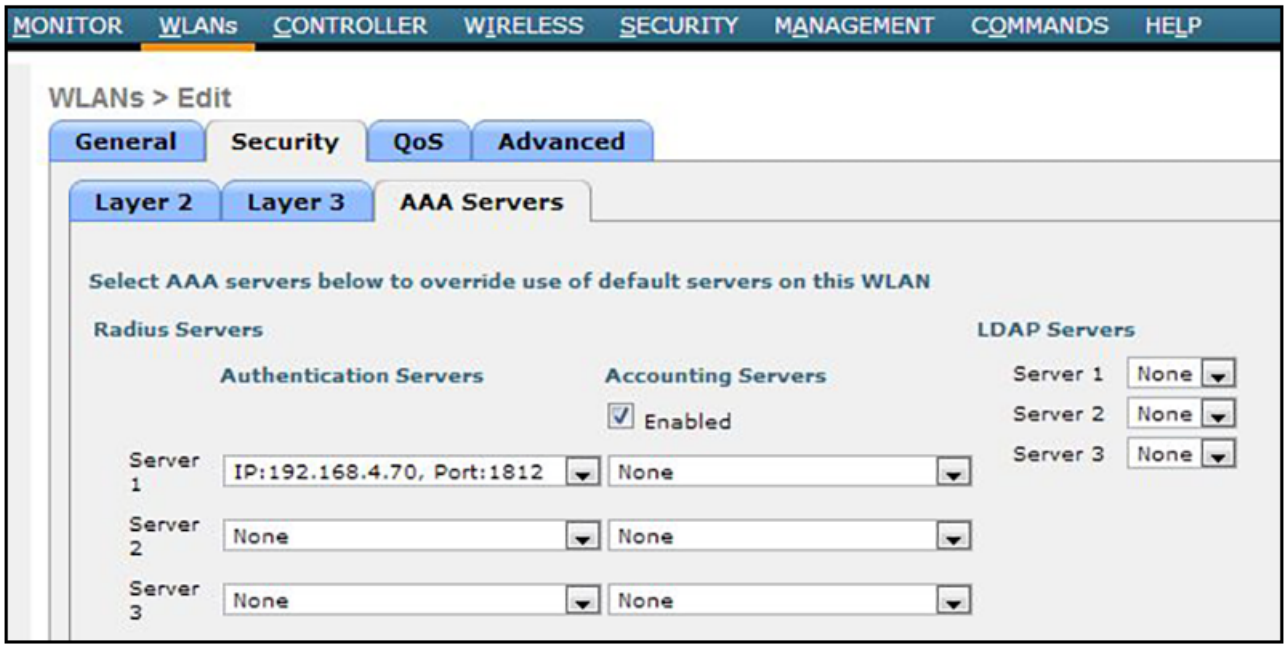
- When NOT using Layer 2 Mac Filtering: Web Policy - Authentication - If you select this option, the user is prompted for username and password while connecting the client to the wireless network.

FIGURE 36 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 37 Select RADIUS Server



7. **Apply** changes.

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

Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com