CONFIGURATION GUIDE

Configuring Cloudpath to Support MAC Registration

Supporting Software Release 5.2

Part Number: 800-71670-001 Rev B
Publication Date: 2 November 2017

Copyright Notice and Proprietary Information

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

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

Limitation of Liability

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

Trademarks

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and in other countries. Brocade, the B-wing symbol, MyBrocade, and ICX are trademarks of Brocade Communications Systems, Inc. in the United States and in other countries. Other trademarks may belong to third parties.

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.

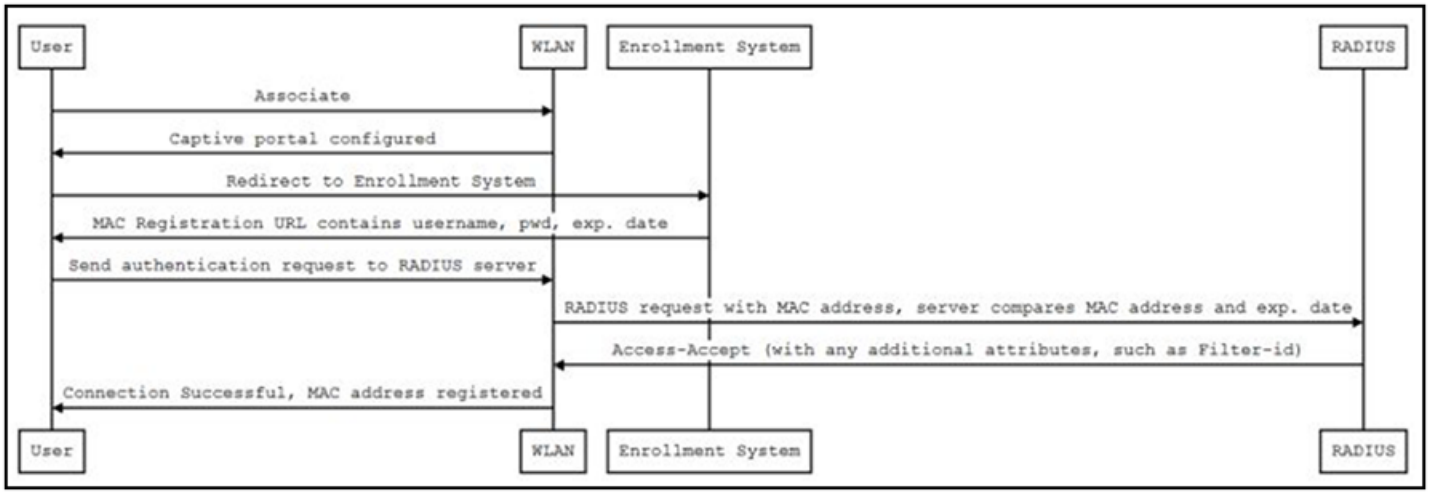
When setting up MAC registration, a list of authorized MAC addresses is maintained on the RADIUS server. When a non-802.1X device attempts to connect to the network, the request is forwarded to the RADIUS server, where the device is checked against the list of authorized MAC addresses. If the registration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

If your environment uses Cisco controllers, see Configuring a Cisco Controller for MAC Registration on page 25.

Set up Cloudpath as an AAA Authentication Server

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

FIGURE 2 Create AAA Authentication Server on Zone Director

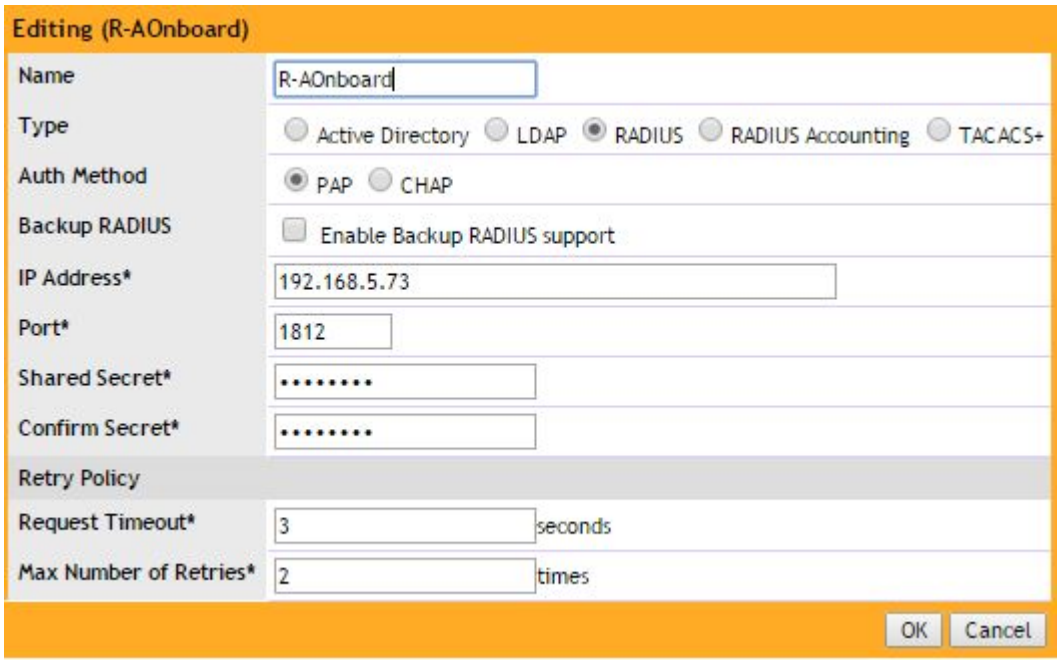
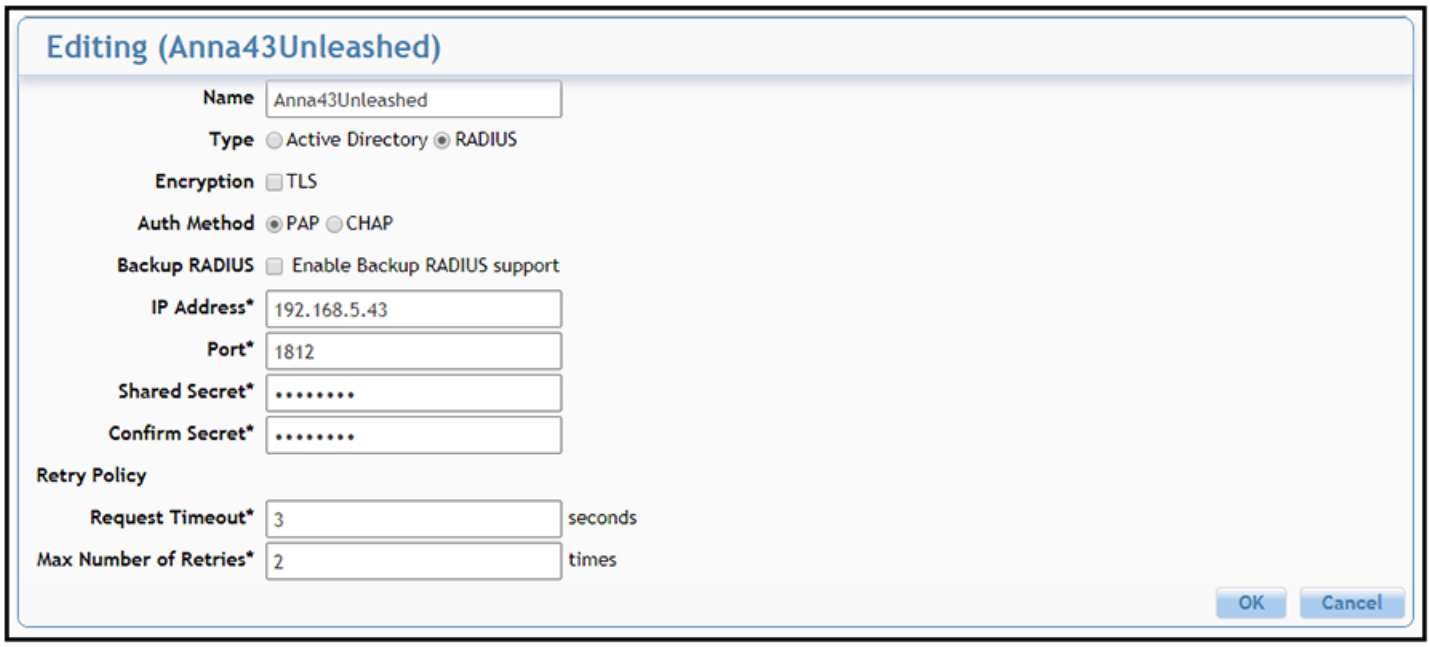


FIGURE 3 Create AAA Authentication Server on SmartZone

FIGURE 4 Create AAA Authentication Server on Unleashed



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

1. Name
2. Type = RADIUS
3. Auth Method = PAP
4. IP address = The IP address of the Cloudpath system.
5. Port = 1812
6. Shared Secret = This must match the shared secret for Cloudpath onboard RADIUS server. (Configuration > RADIUS Server).
7. Leave the default values for the remaining fields.

Create AAA Accounting Server (Optional)

Use the same process to create the AAA Accounting Server.

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

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

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

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

Run Authentication Test

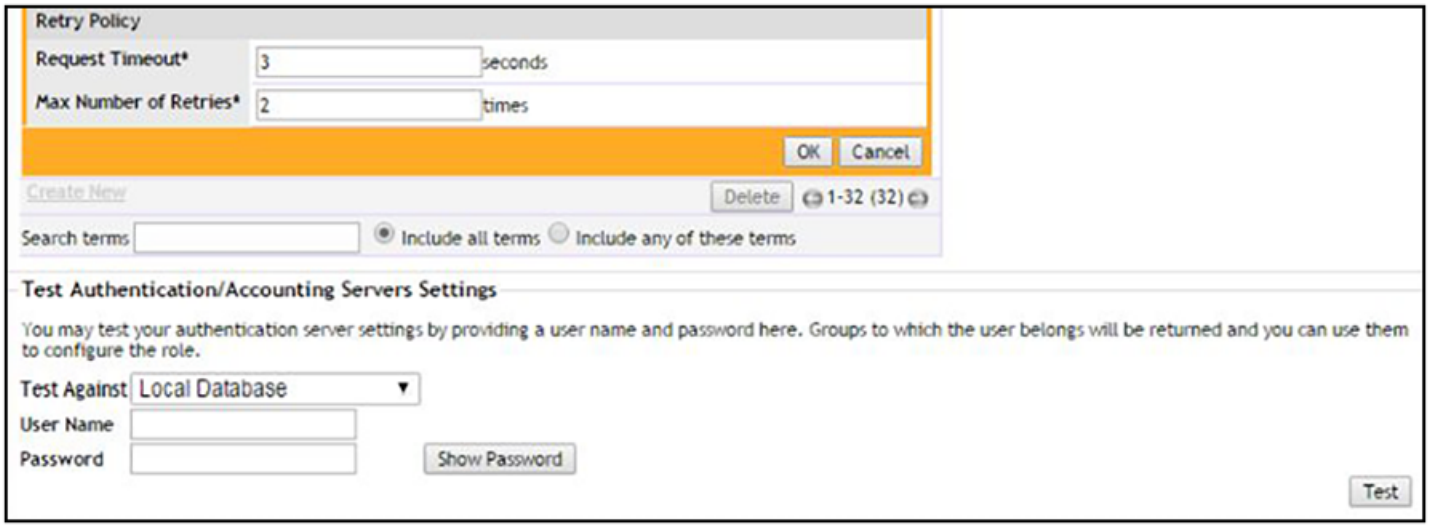
You can test the connection between the controller and the Cloudpath ES RADIUS server.

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.

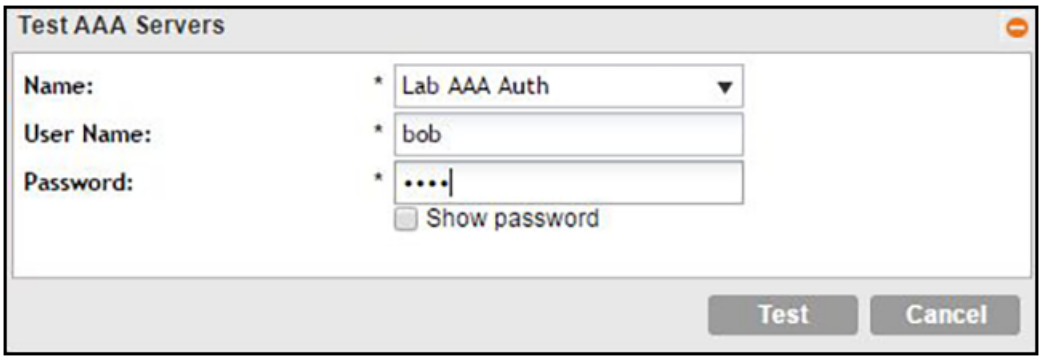
FIGURE 5 Authentication Test on ZoneDirector



SmartZone

You are prompted to Test Authentication when you save a configuration for an AAA Authentication server. Enter your credentials, then click the **Test** button.

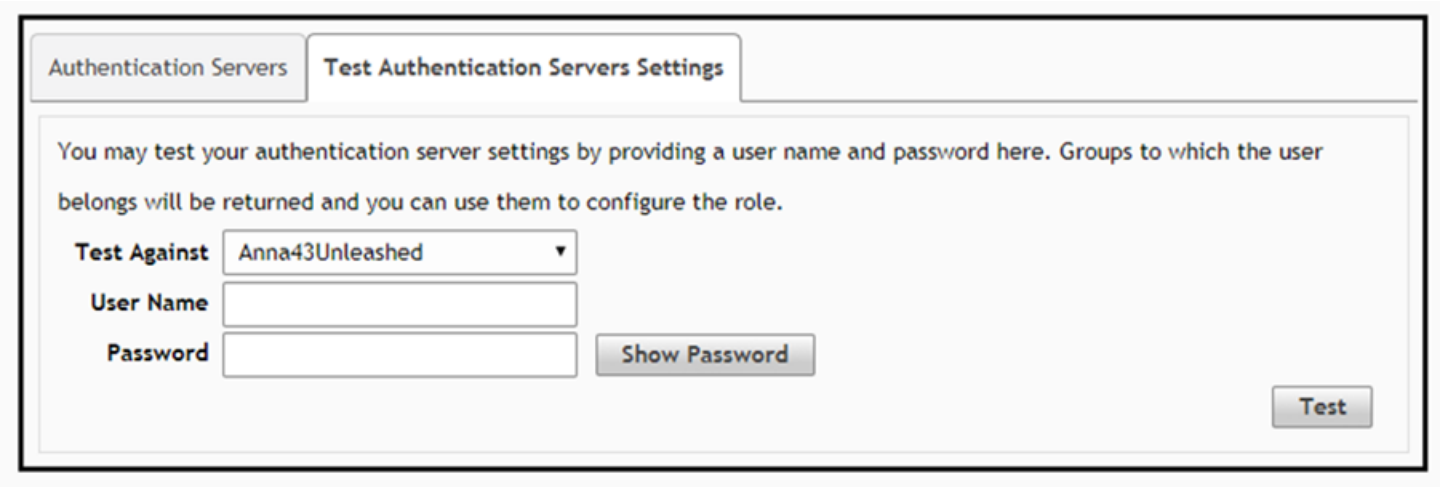
FIGURE 6 Authentication Test on SmartZone



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 get one of these responses:

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

If you receive:

`Failed! Invalid username or password`

This means that connectivity was established.

Create Hotspot Services

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

1. Navigate to: Hotspot Services on ZoneDirector, Hotspot WISPr on SmartZone, or Services > Hotspot Services on Unleashed.

2. Name the Hotspot Service.

FIGURE 8 Create Hotspot Service on Zone Director

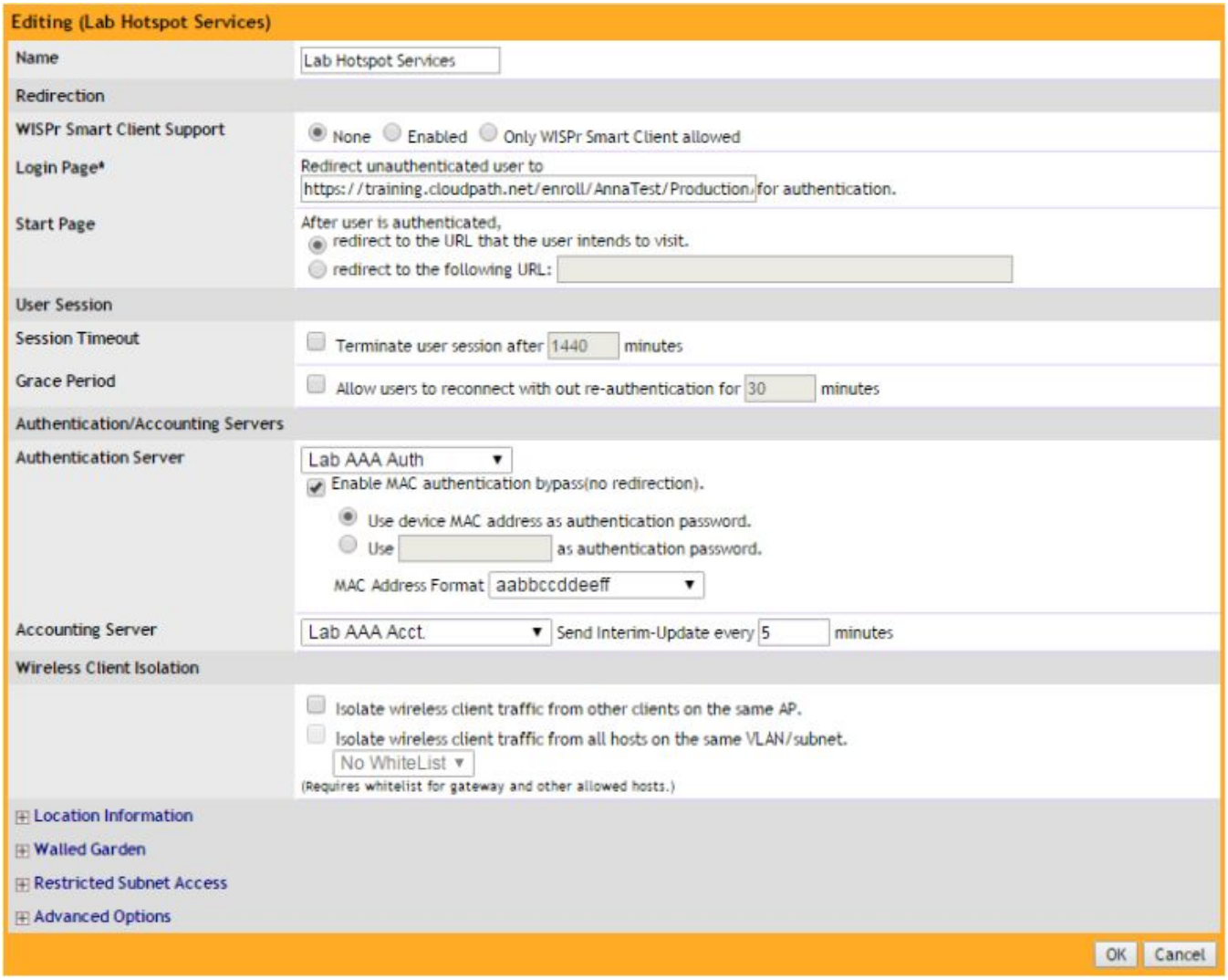


FIGURE 9 Create Hotspot WISPr on SmartZone

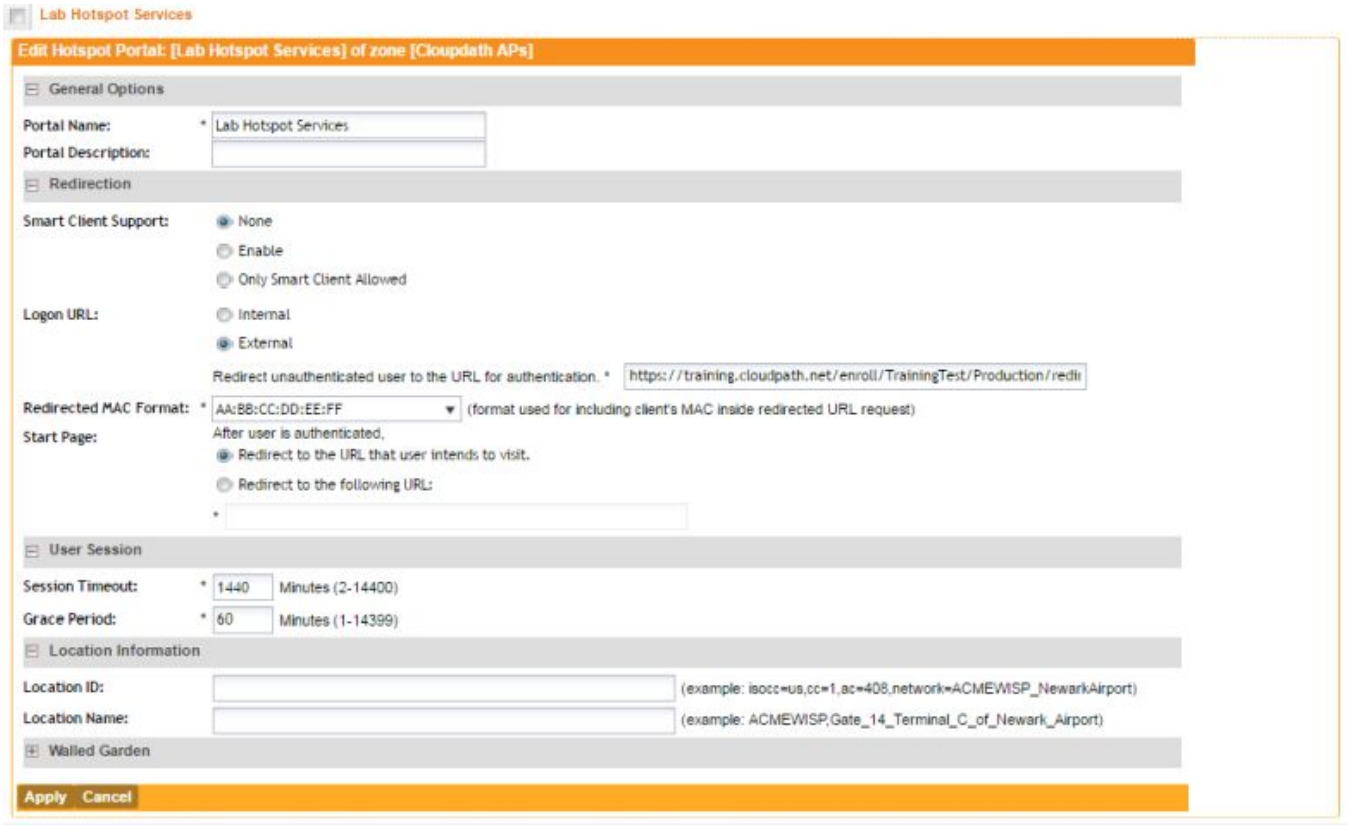
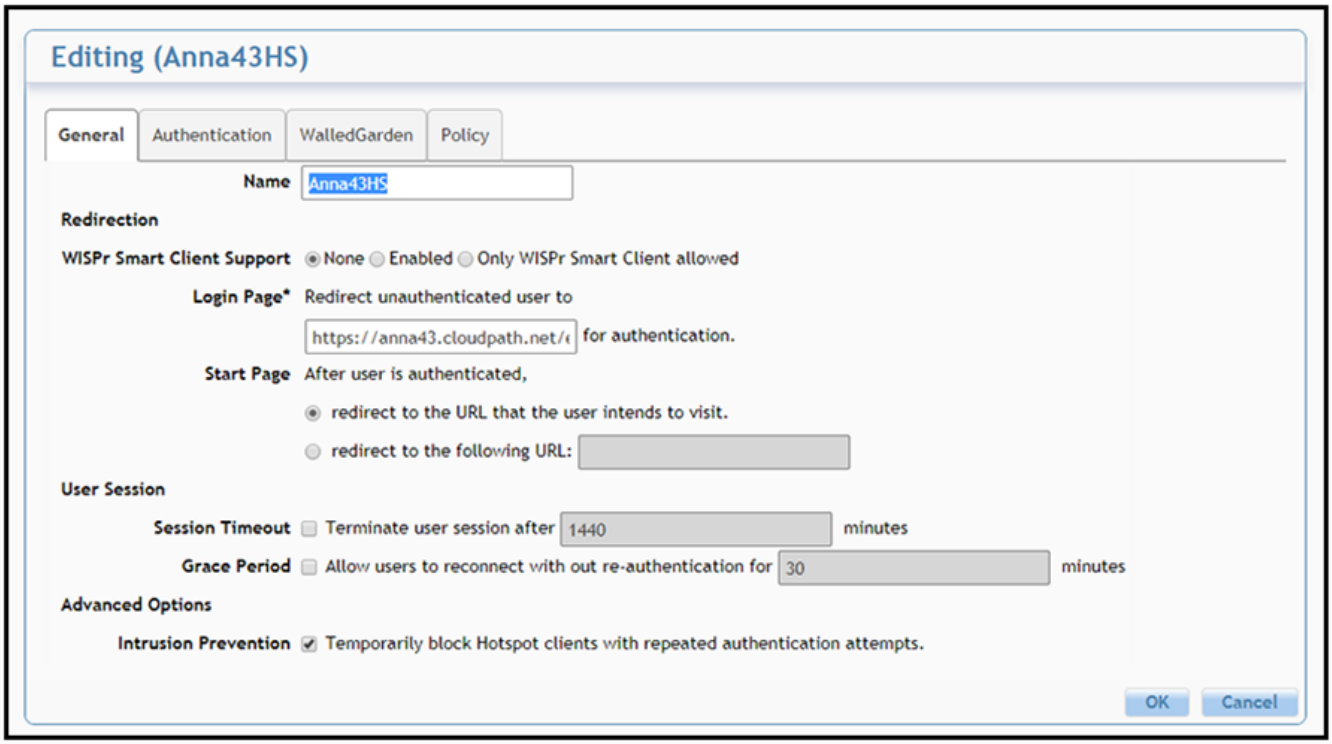


FIGURE 10 Create Hotspot Service on Unleashed



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** (ZoneDirector only).
6. Enable **MAC authentication bypass redirection** (ZoneDirector only).
7. Select the Cloudpath RADIUS **Accounting Server** (ZoneDirector only).
8. Leave the defaults for the remaining settings. Click **OK**.

Set Up the Walled Garden (Zone Director and SmartZone only)

Enter the following values for the Walled Garden:

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

FIGURE 11 Walled Garden Configuration for Zone Director

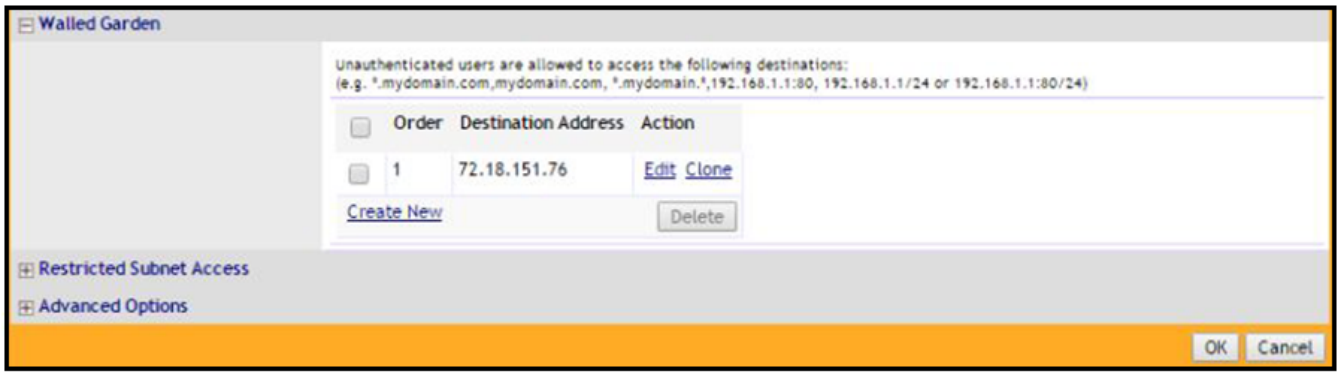


FIGURE 12 Walled Garden Configuration for SmartZone

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

Create the Onboarding SSID

Enter the following values for the onboarding SSID:

1. Name the SSID.

2. Type=Hotspot Service (WISPr).

FIGURE 13 Onboarding SSID Configuration on Zone Director

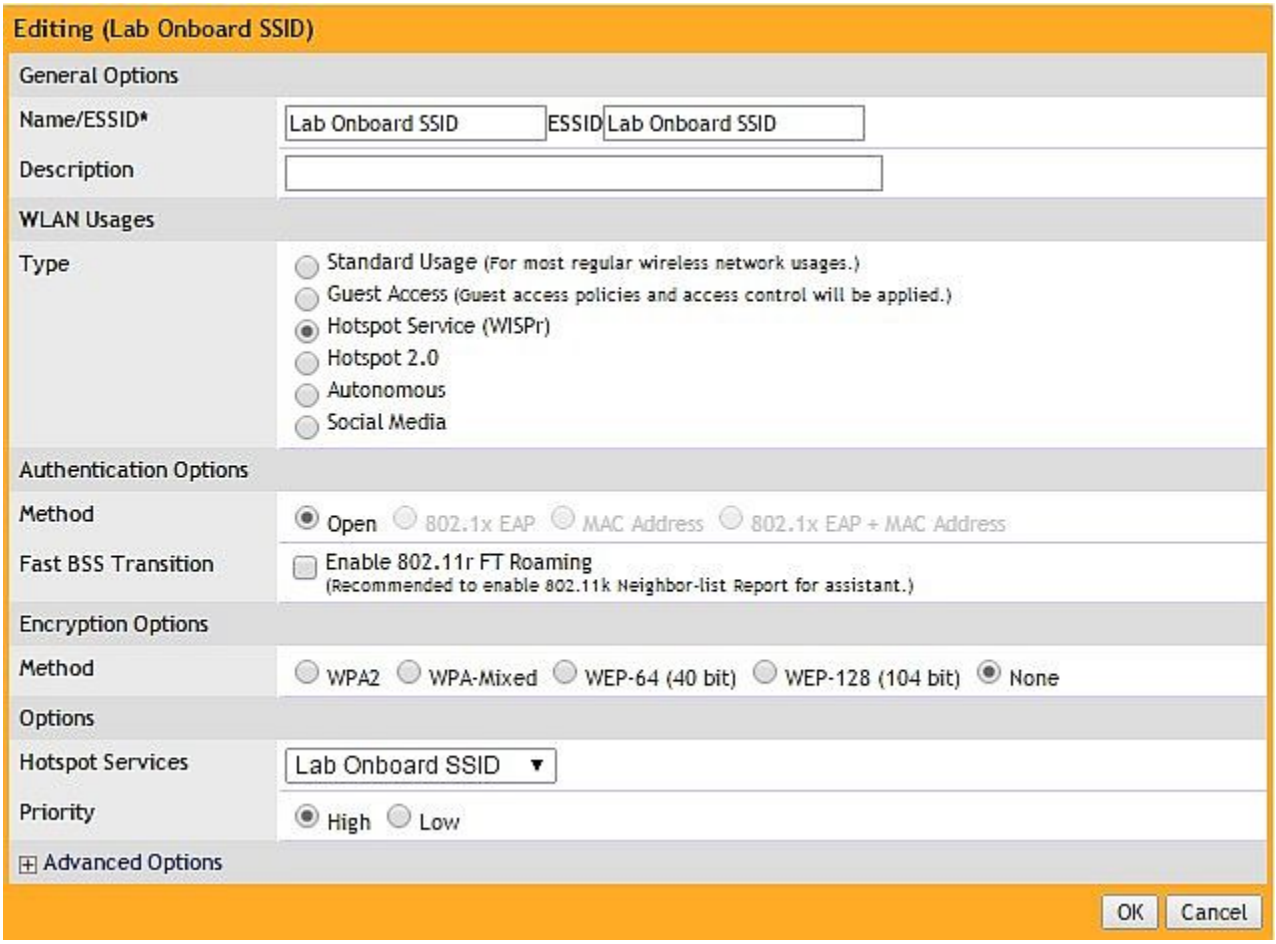


FIGURE 14 Onboarding SSID Configuration on SmartZone

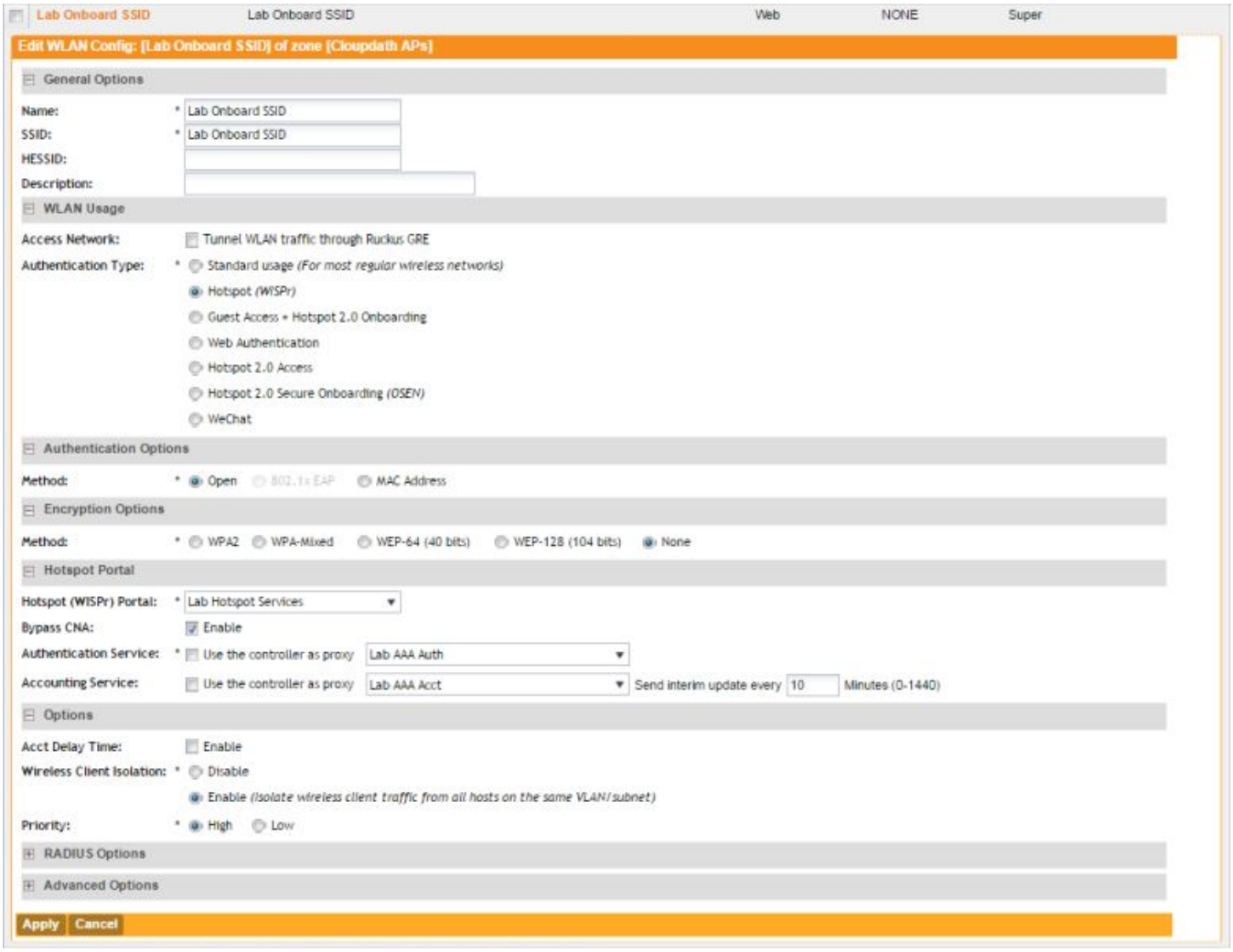
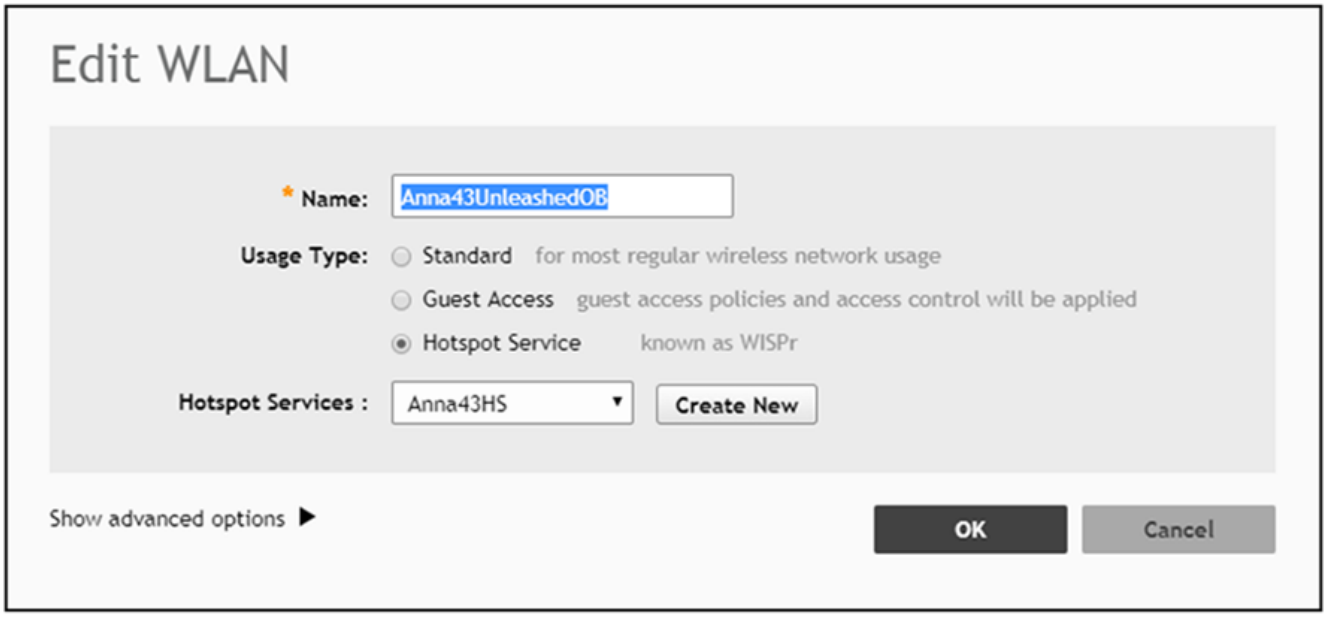


FIGURE 15 Onboarding SSID Configuration for Unleashed



3. Authentication Option Method=Open (SZ and ZD).
4. Encryption Option Method=None (SZ and ZD).
5. Select the Hotspot Service created in Task 2.
6. Enable **Bypass CNA** (SZ and ZD).
   - For ZoneDirector, this setting is at the bottom of the screen in the **Bypass Apple CNA Feature** section. Check the **Hotspot service** box.
   - For SmartZone, this setting is in the **Hotspot Portal** Section.
7. Select the Cloudpath **RADIUS Authentication Server** (SmartZone only).
8. Select the Cloudpath **RADIUS Accounting Server** (SmartZone only).
9. Leave the defaults for the remaining settings and click **OK** (or **Apply**).

Cloudpath Configuration

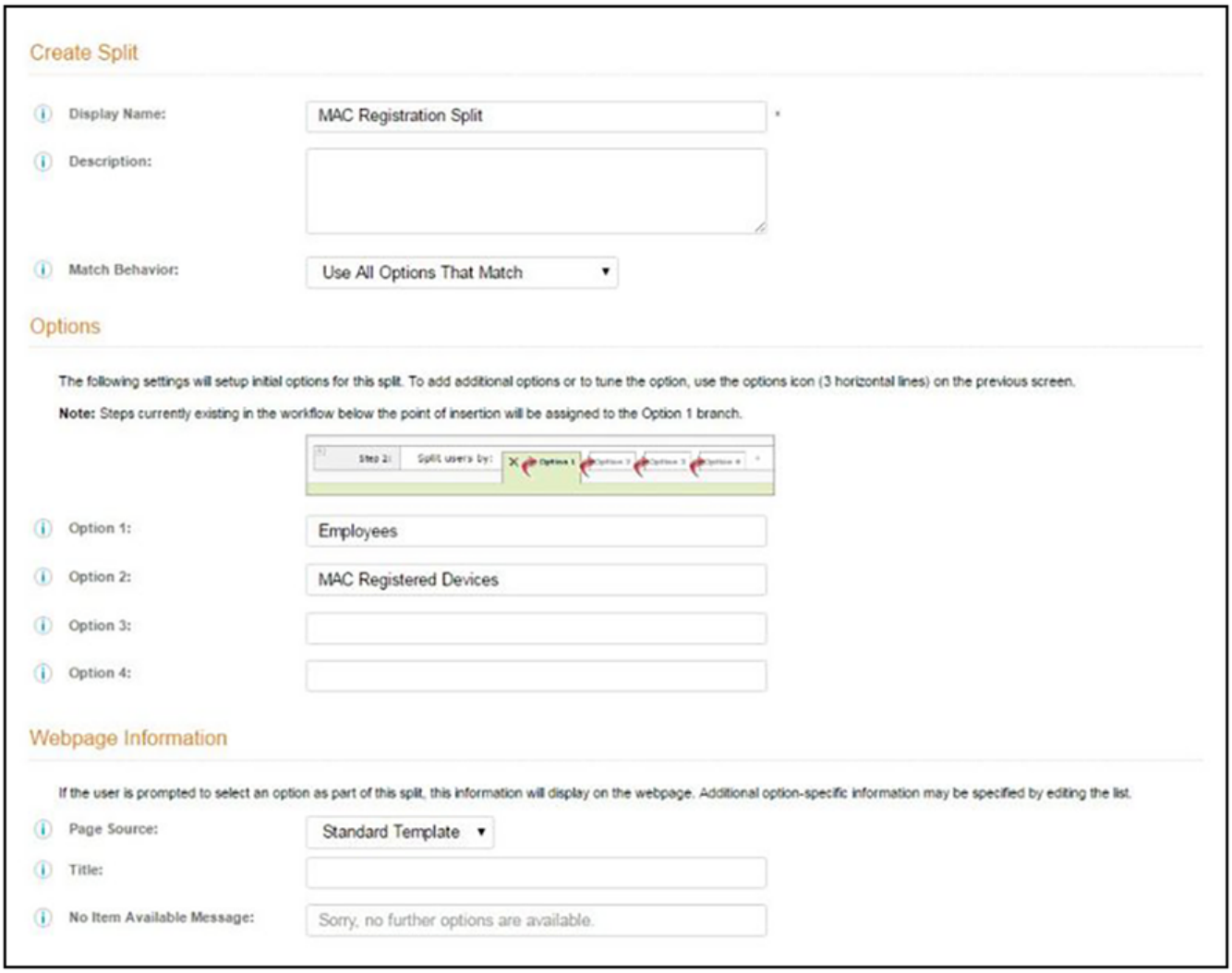
This section describes how to create a workflow for MAC registration, add RADIUS attributes to a MAC registration configuration, and how to import a file of MAC addresses to a MAC registration list.

Create a MAC Registration Workflow

1. Go to **Configuration** > **Workflow** and select **Add 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 16 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.

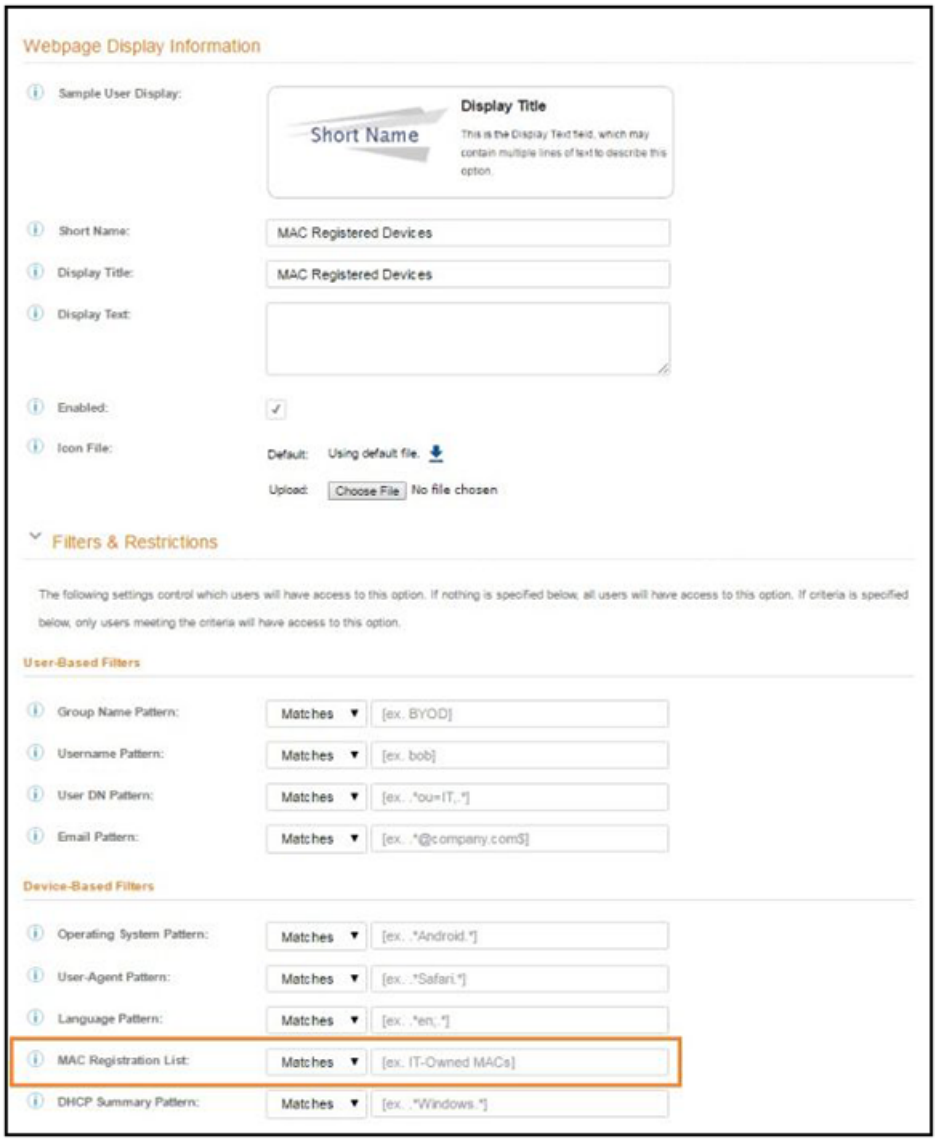
The remaining sections describe how to configure the **MAC Registered** workflow. The **Employees** workflow is configured per your network needs.

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 17 Modify Split Options



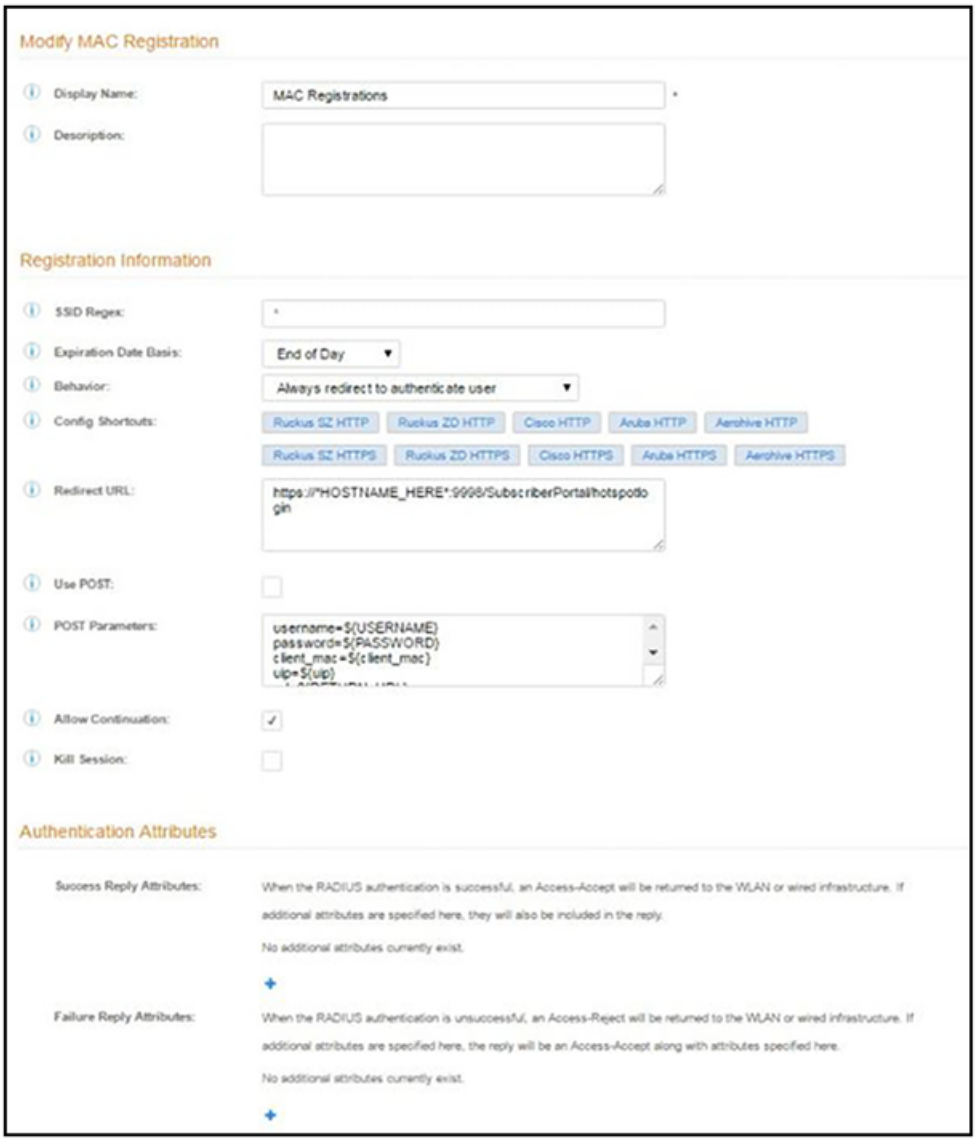
4. **Save** the changes to the option filter.

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 18 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.

   - Expiration Date Offset - The number of hours/days/months/etc to be offset from the event date when calculating the registration validity period. If **Specified Date** is selected, this should be the date in YYYY/MM/DD format.
   - Behavior - Specifies the prompt and redirect settings for the MAC registration configuration. Use the **Web Page Information** section to configure the user prompt or redirect URL. Behavior settings include:
     - Prompt user when MAC is unknown.
     - Always prompt the user.
     - Redirect when MAC is unknown.
     - Always redirect to authenticate user. (This is the default and the most commonly used setting).
     - Skip registration when MAC is unknown.
   - Use the **Config Shortcuts** buttons to populate the **Redirect URL** and **POST Parameters** according to your controller vendor and preferred protocol.
   - Allow Continuation - If checked, the submit-redirect call is processed, if unchecked, the submit- redirect call is ignored.
   - Kill Session - If checked, the user's session will be killed as they are redirected and, if they return, they will be forced to start over.

Adding RADIUS Attributes

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

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

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

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

How to Add a Message to Users

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

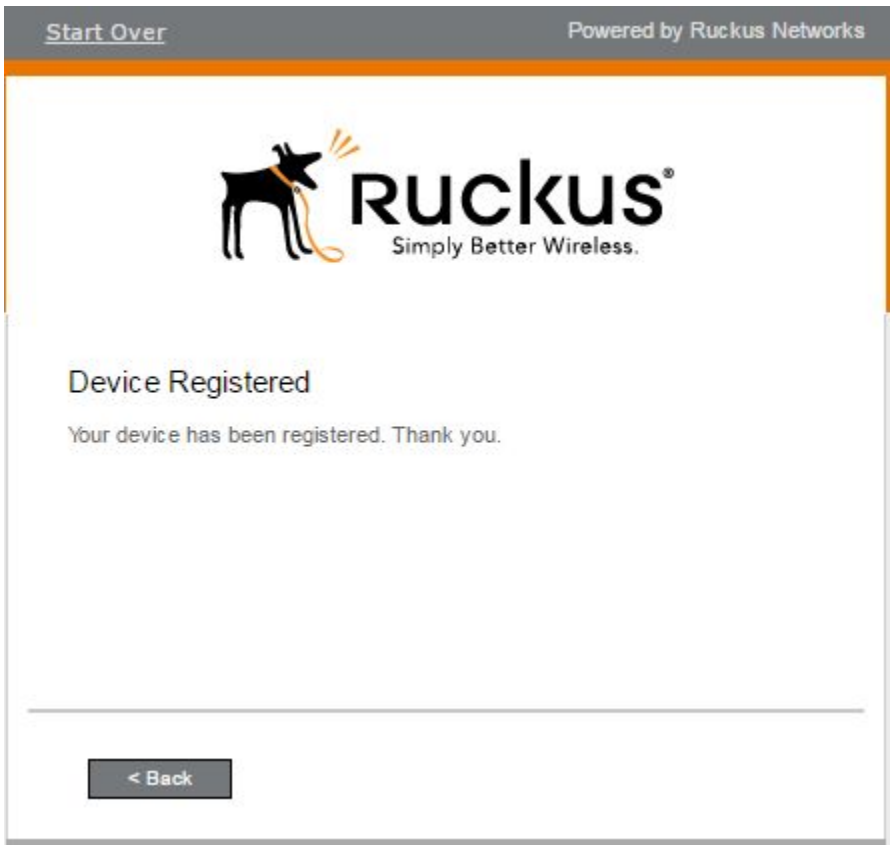
1. On the workflow page, click the **Insert** arrow to create a step in the enrollment workflow.
2. Select **Display a message**.

3. Create a new message from a standard template. On the **Create New Message** page, enter an appropriate **Title** and **Message**.
4. Uncheck the **Show Continue Button** box. After the message is displayed, the device should be moved to the specified SSID. No user action is required.

5. **Save** the configuration.

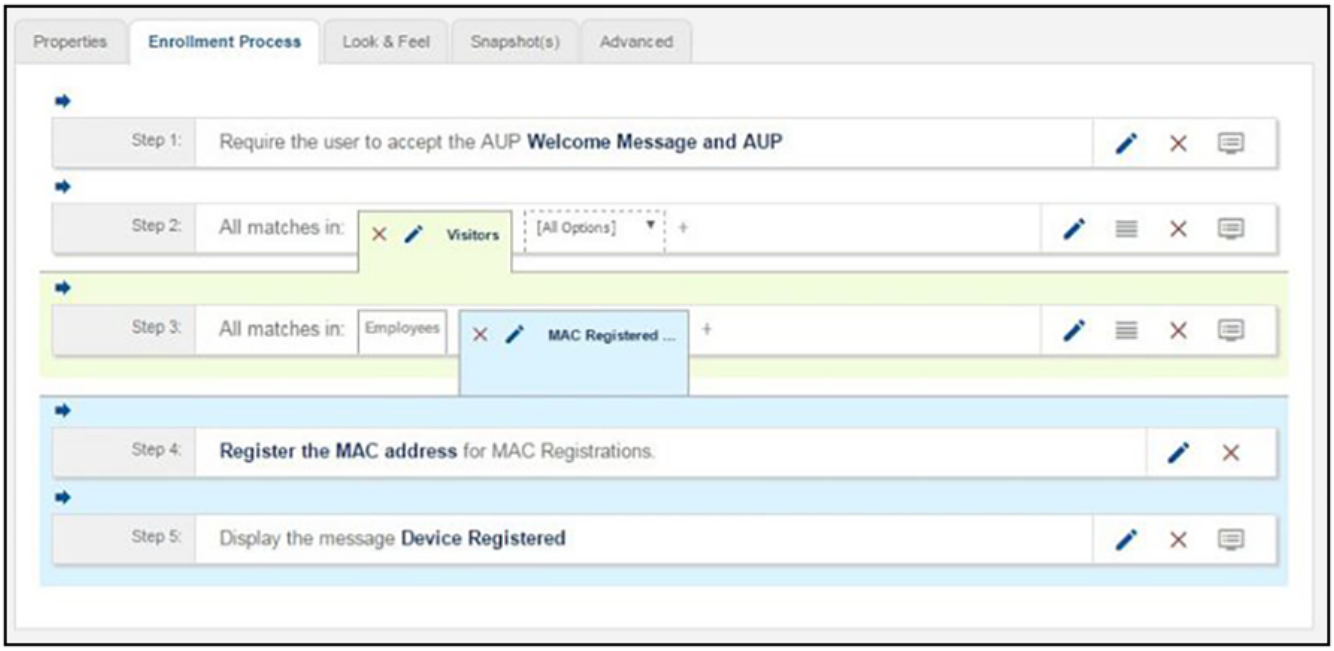
   On the workflow page, click the **view** icon next to the **Display Message** step to see a preview of the message.

   FIGURE 19 Example Message to User



   The completed workflow is displayed below.

FIGURE 20 Completed Workflow for MAC Registration

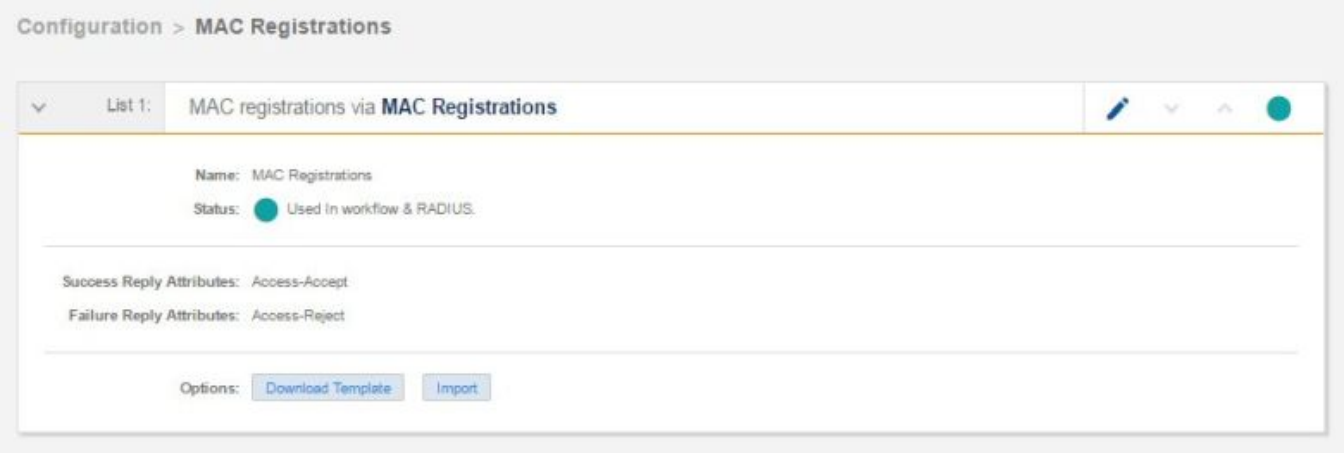


Import MAC Registration List

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

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

FIGURE 21 Import MAC Registration List



2. Open the MAC Registration list for which you will import a device list.

3. 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 device list and **Continue**.
5. The file is imported and the device list is added to the MAC Registration list.

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

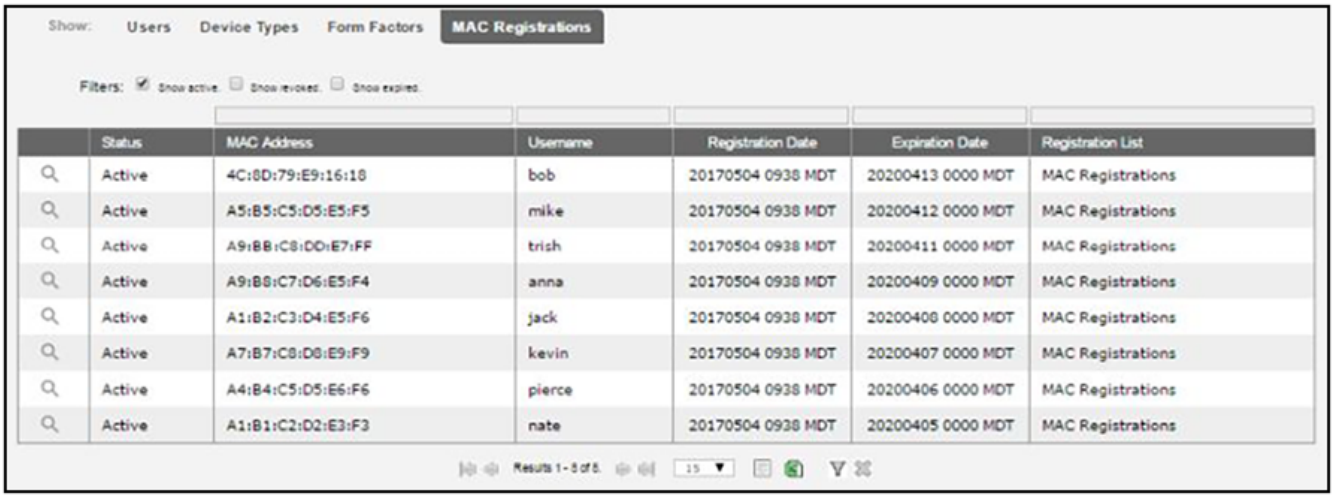
Viewing MAC Registration Records on the Dashboard

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

How to View MAC Registration Records

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

FIGURE 22 MAC Registrations on the Dashboard



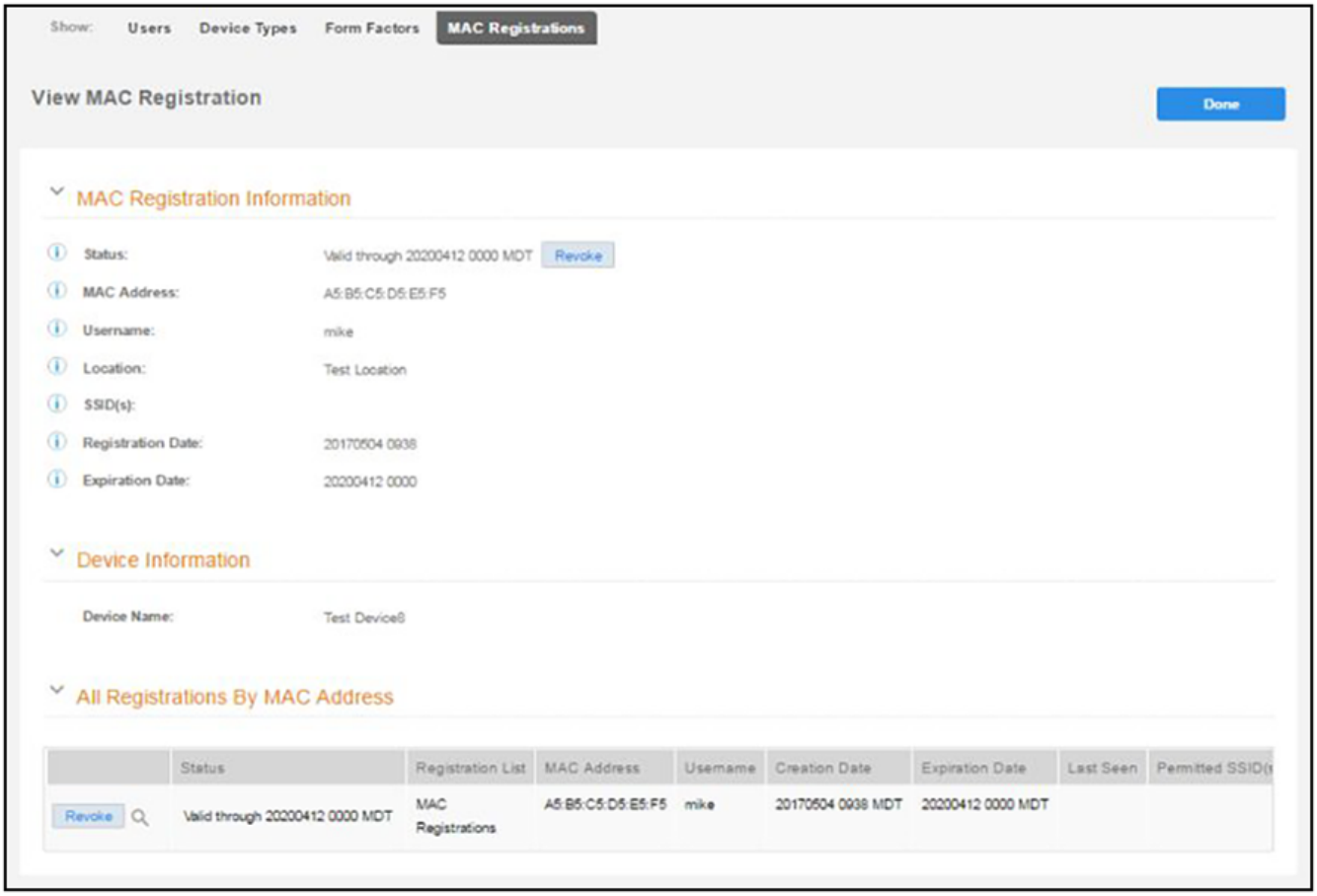
4. You can also access MAC registration information in the enrollment record. Go to **Operational** > **Dashboard** > **Enrollments** > **View Enrollment Record**.

How to Revoke Access for a MAC-Registered Device

1. Go to **Operational** > **Dashboard** > **MAC Registrations**.

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

FIGURE 23 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.

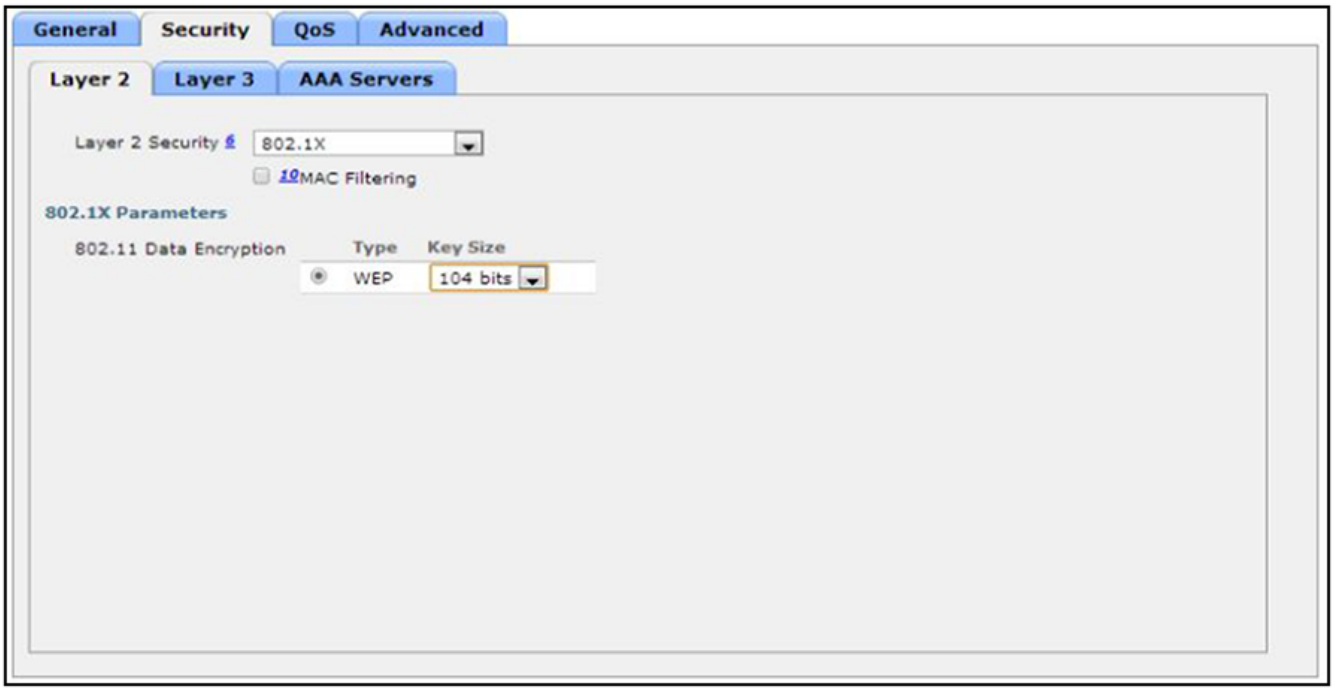
Configuring a Cisco Controller for MAC Registration

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 24 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 25 Layer 3 Settings when Using Layer 2 Mac Filtering

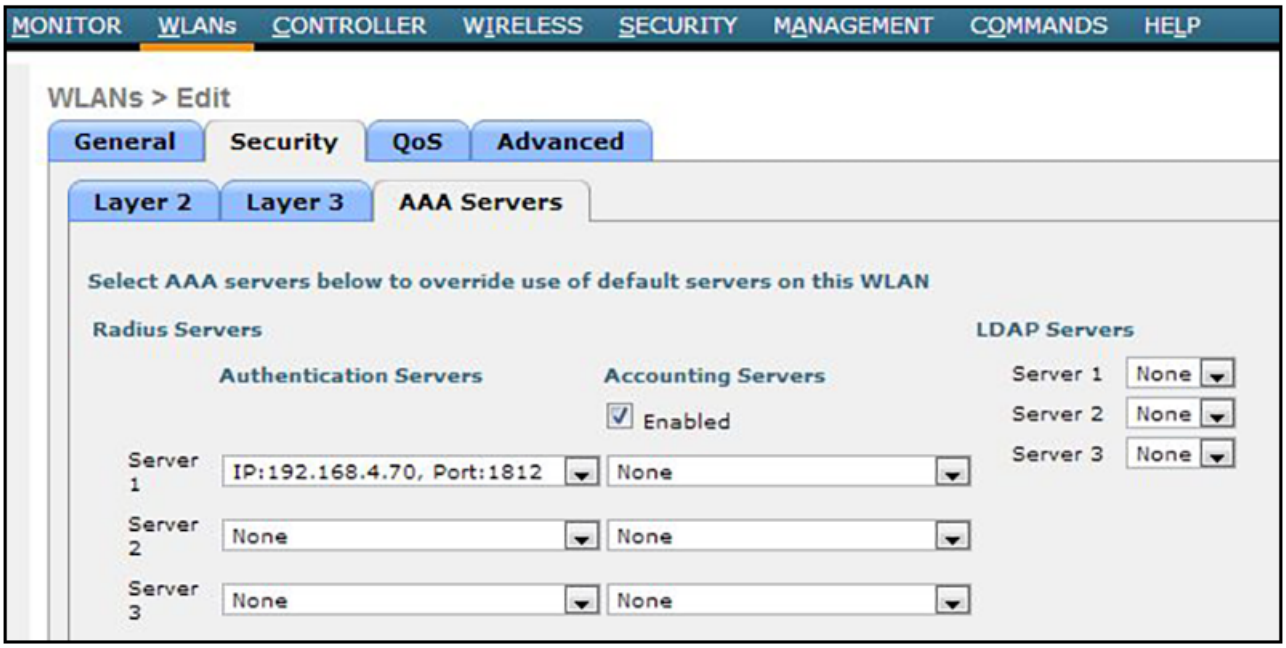
- When NOT using Layer 2 Mac Filtering: Web Policy - Authentication - If you select this option, the user is prompted for username and password while connecting the client to the wireless network.

FIGURE 26 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 27 Select RADIUS Server



7. **Apply** changes.

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