

Configuring Cloudpath to Support MAC Registration

Supporting Software Release 5.2

Copyright, Trademark and Proprietary Rights Information

© 2018 ARRIS Enterprises LLC. All rights reserved.

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

Export Restrictions

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

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

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, ARRIS 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. ARRIS 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. ARRIS 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 ARRIS 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 ARRIS, ARRIS 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 ARRIS 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, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, Edgelron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Overview.....	4
MAC Registration Process.....	4
Configuring Ruckus Controllers for MAC Registration.....	5
Setting up Cloudpath as an AAA Authentication Server.....	5
Creating AAA Accounting Server (Optional).....	8
Running Authentication Test.....	9
Creating Hotspot Services.....	11
Setting Up the Walled Garden.....	16
Creating the Onboarding SSID.....	18
Cloudpath Configuration.....	23
Create a MAC Registration Workflow.....	24
Import MAC Registration List.....	31
Viewing MAC Registration Records on the Dashboard.....	32
Configuring a Cisco Controller for MAC Registration.....	33

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.

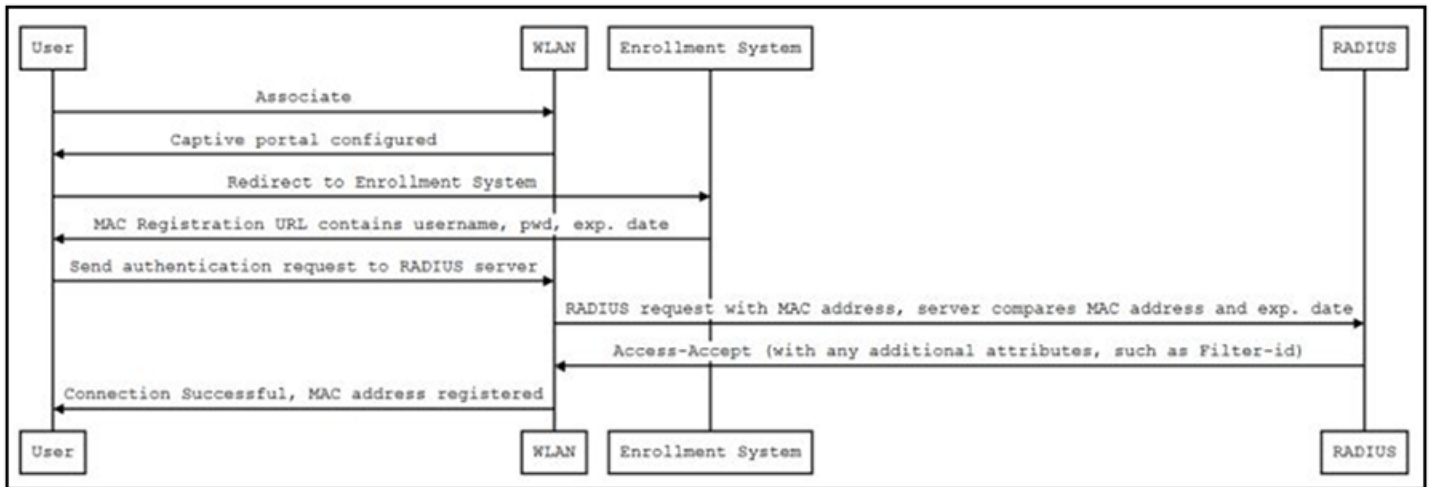
When setting up MAC registration, a list of authorized MAC addresses is maintained on the RADIUS server. When a non-802.1X device attempts to connect to the network, the request is forwarded to the RADIUS server, where the device is checked against the list of authorized MAC addresses. If the registration 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 33.

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

Create New

Name	<input type="text" value="R-AOnboard"/>
Type	<input type="radio"/> Active Directory <input type="radio"/> LDAP <input checked="" type="radio"/> RADIUS <input type="radio"/> RADIUS Accounting <input type="radio"/> TACACS+
Encryption	<input type="checkbox"/> TLS
Auth Method	<input checked="" type="radio"/> PAP <input type="radio"/> CHAP
Backup RADIUS	<input type="checkbox"/> Enable Backup RADIUS support
IP Address*	<input type="text" value="192.168.5.73"/>
Port*	<input type="text" value="1812"/>
Shared Secret*	<input type="password" value="*****"/>
Confirm Secret*	<input type="password" value="*****"/>
Retry Policy	
Request Timeout*	<input type="text" value="3"/> seconds
Max Number of Retries*	<input type="text" value="2"/> times

FIGURE 3 Create AAA Authentication Server on SmartZone

Create AAA Server

General Options

Name: Lab AAA Auth

Description:

Type: RADIUS Active Directory LDAP

Backup RADIUS: Enable Secondary Server

Primary Server

IP Address: 72.18.151.56

Port: 1812

Shared Secret:

Confirm Secret:

User Role Mapping

OK Cancel

FIGURE 4 Create AAA Authentication Server on Unleashed

Create New

Name

Type Active Directory RADIUS RADIUS Accounting

Encryption TLS

Auth Method PAP CHAP

Backup RADIUS Enable Backup RADIUS support

IP Address*

Port*

Shared Secret*

Confirm Secret*

Retry Policy

Request Timeout* seconds

Max Number of Retries* times

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

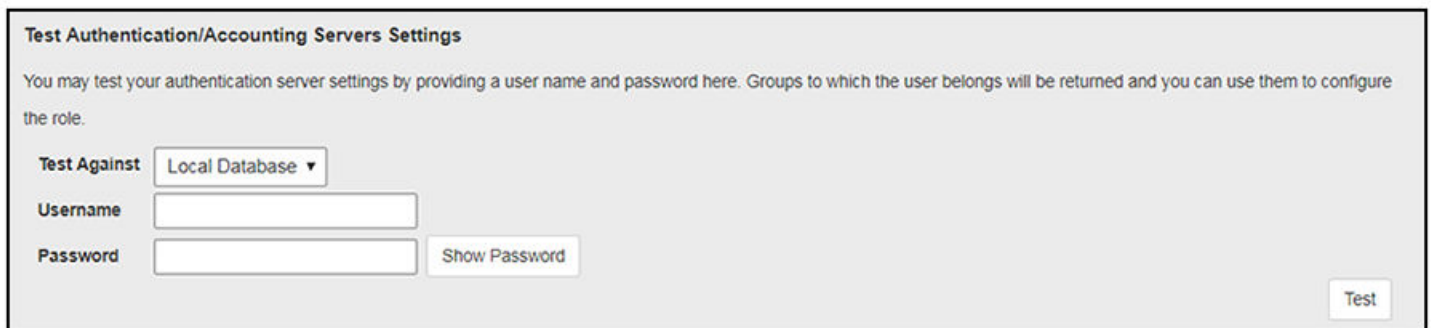
You can test the connection between the controller and the Cloudpath ES RADIUS server.

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



Test Authentication/Accounting Servers Settings

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

Test Against Local Database ▾

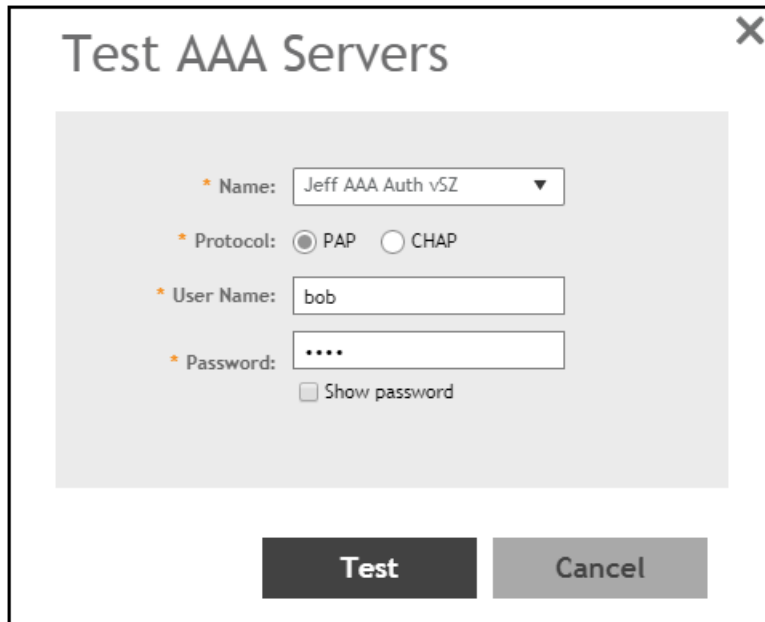
Username

Password

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.

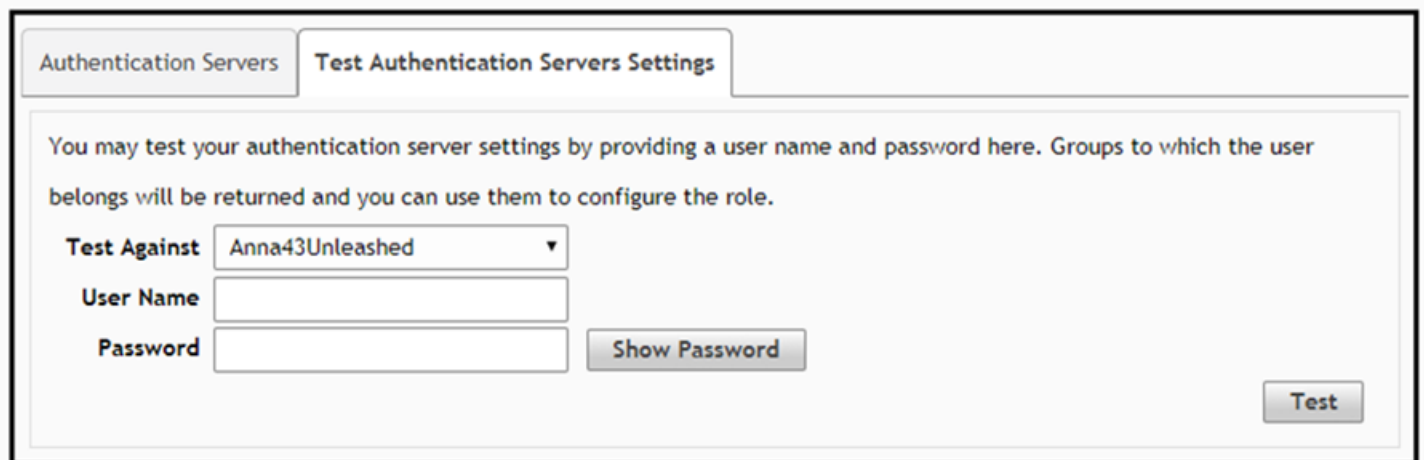
FIGURE 6 Authentication Test on SmartZone



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

Create New

Name: Lab Hotspot Services

Redirection

WISPr Smart Client Support: None Enabled Only WISPr Smart Client allowed

Login Page*: Redirect unauthenticated user to https://training.cloudpath.net/e for authentication.

Start Page: After user is authenticated, redirect to the URL that the user intends to visit. redirect to the following URL: []

User Session

Session Timeout: Terminate user session after 1440 minutes

Grace Period: Allow users to reconnect without re-authentication for 30 minutes

Authentication/Accounting Servers

Authentication Server: Jeff AAA Auth

Enable MAC authentication bypass(no redirection).

Use device MAC address as authentication password. Use [] as authentication password.

MAC Address Format: AA:BB:CC:DD:EE:FF

Accounting Server: Jeff AAA acct Send Interim-Update every 5 minutes

Wireless Client Isolation

Isolate wireless client traffic from other clients on the same AP.

Isolate wireless client traffic from all hosts on the same VLAN/subnet.

No WhiteList

(Requires whitelist for gateway and other allowed hosts.)

Location Information

Walled Garden

Restricted Subnet Access

Advanced Options

OK Cancel

FIGURE 9 Create Hotspot WISPr on SmartZone

Create Hotspot Portal

General Options

Portal Name: Lab Hotspot Services
Portal Description:

Redirection

Smart Client Support: None Enable Only Smart Client Allowed

Logon URL: Internal External

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

Redirected MAC Format: AA:BB:CC:DD:EE:FF

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

HTTPS Redirect: If enabled, the AP will try to redirect HTTPS requests to the hotspot portal

User Session

Session Timeout: 1440 Minutes (2-14400)
Grace Period: 60 Minutes (1-14399)

Location Information

Location ID: (example: isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport)
Location Name: (example: ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport)

Walled Garden

OK Cancel

FIGURE 10 Create Hotspot Service on Unleashed - General Tab

The screenshot shows a 'Create New' dialog box with a close button (X) in the top right corner. The dialog has four tabs: 'General', 'Authentication', 'WalledGarden', and 'Policy'. The 'General' tab is selected and contains the following configuration options:

- Name:** A text input field containing 'Anna43HS'.
- Redirection:**
 - WISPr Smart Client Support:** Radio buttons for 'None' (selected), 'Enabled', and 'Only WISPr Smart Client allowed'.
 - Login Page:** Text 'Redirect unauthenticated user to' followed by a text input field containing 'https://anna43.cloudpath.net/e' and the text 'for authentication.'
 - Start Page:** Text 'After user is authenticated,' followed by two radio button options:
 - 'redirect to the URL that the user intends to visit.' (selected)
 - 'redirect to the following URL:' followed by an empty text input field.
- User Session:**
 - Session Timeout:** Text '(Requires whitelist for gateway and other allowed hosts.)' followed by a checkbox 'Terminate user session after' and a text input field containing '1440' and the text 'minutes'.
 - Grace Period:** A checkbox 'Allow users to reconnect without re-authentication for' and a text input field containing '30' and the text 'minutes'.
 - Intrusion Prevention:** A checked checkbox 'Temporarily block Hotspot clients with repeated authentication attempts.'

At the bottom right of the dialog are two buttons: 'OK' and 'Cancel'.

FIGURE 11 Create Hotspot Service on Unleashed - Authentication Tab

General **Authentication** WalledGarden Policy

Authentication/Accounting Servers

Authentication Server Anna43Unleashed

Enable MAC authentication bypass(no redirection).

Use device MAC address as authentication password.

Use [] as authentication password.

MAC Address Format AA:BB:CC:DD:EE:FF

Accounting Server Anna43UnleashedACCT

Send Interim-Update every 10 minutes

Wireless Client Isolation

Isolate wireless client traffic from other clients on the same AP.

Isolate wireless client traffic from all hosts on the same VLAN/subnet.

No WhiteList

(Requires whitelist for gateway and other allowed hosts.)

Location Information

Location ID [] (e.g. isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport)

Location Name [] (e.g. ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport)

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**.

- 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

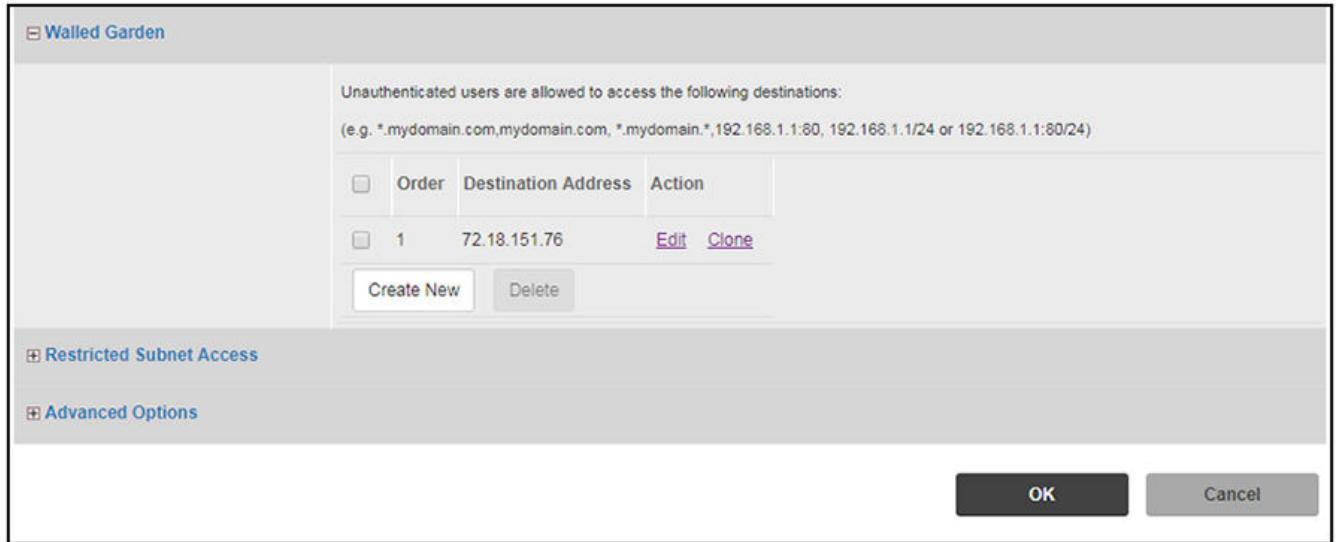


FIGURE 13 Walled Garden Configuration for SmartZone

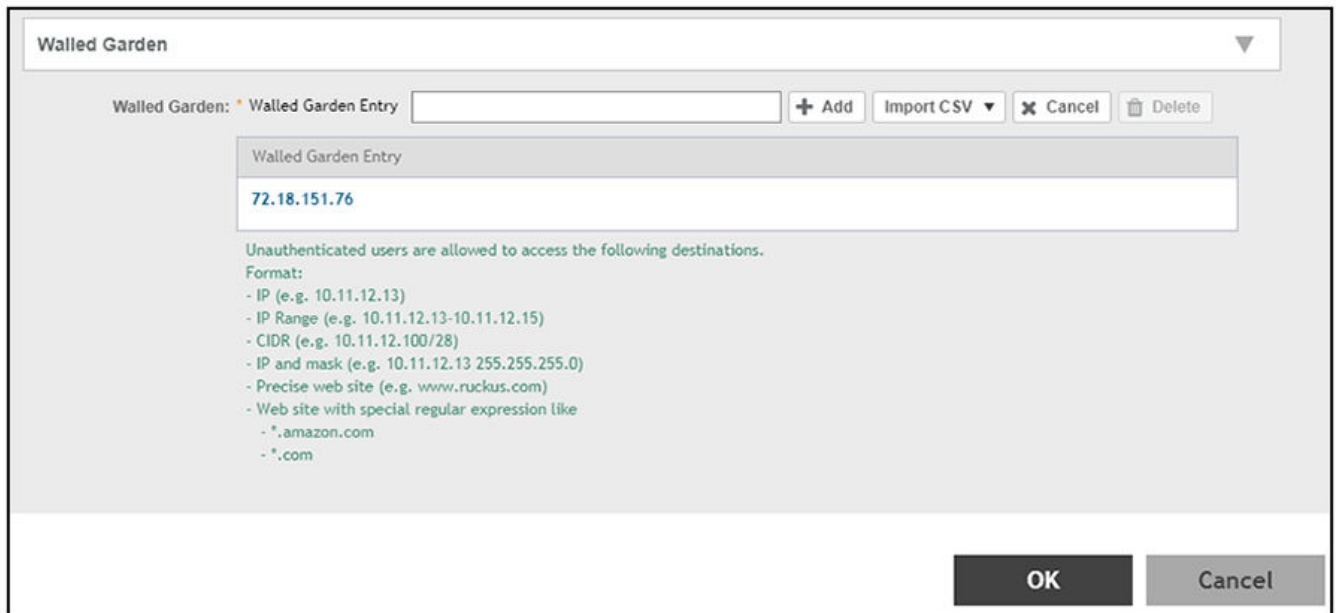
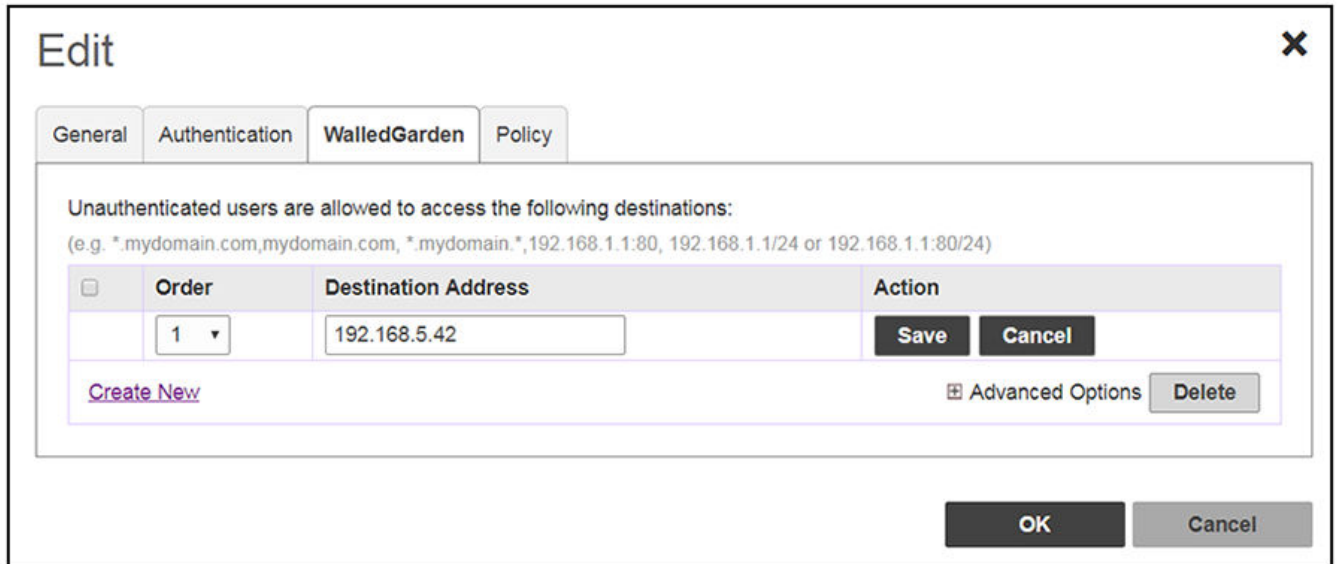


FIGURE 14 Walled Garden Configuration for Unleashed



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.

These recommended destinations for the walled garden are:

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

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

Create WLAN

General Options

Name: Lab Onboard SSID
ESSID: Lab Onboard SSID
Description:

WLAN Usages

Type: Standard Usage (For most regular wireless network usages.)
 Guest Access (Guest access policies and access control will be applied.)
 Hotspot Service (WISPr)
 Hotspot 2.0
 Autonomous
 Social Media
 WeChat

Authentication Options

Method: Open 802.1x EAP MAC Address 802.1x EAP + MAC Address
Fast BSS Transition: Enable 802.11r FT Roaming (Recommended to enable 802.11k Neighbor-list Report for assistant.)

Encryption Options

Method: WPA2 WPA-Mixed WEP-64 (40 bit) WEP-128 (104 bit) None

Options

Hotspot Services: Lab Hotspot Services Create New
Priority: High Low

Advanced Options

OK Cancel

FIGURE 16 Onboarding SSID Configuration on SmartZone

Create WLAN Configuration

General Options

- Name: Lab Onboard SSID
- SSID: Lab Onboard SSID
- Description:
- Zone: Default
- WLAN Group: default **Create**

Authentication Options

- Authentication Type: Standard usage (for most regular wireless networks) Hotspot (HSP) Guest Access Web Authentication
- Hotspot 2.0 Access Hotspot 2.0 Onboarding WNet
- Method: Open 802.1X EAP MAC Address 802.1X RADIUS
- MAC Authentication: Use user-defined text as authentication password (default is device MAC address):
- MAC Address Format: AA:BB:CC:DD:EE:FF

Encryption Options

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

Data Plane Options

- Access Network: Tunnel WLAN traffic through Ruckus GRE

Hotspot Portal

- Hotspot (HSP) Portal: Lab Hotspot Services **Create**
- Bypass CNA: Enable
- Authentication Service: Use the controller as proxy Use RADIUS-based profile
- AAA Auth: Jiff AAA Auth v52 **Create**
- Accounting Service: Use the controller as proxy
- AAA Acc: Jiff AAA Acc v52 **Create** Send interim update every: 10 Minutes (0-1440)

Options

- Acct Delay Time: Enable
- Wireless Client Isolation: Disable Enable (isolate wireless client traffic from all hosts on the same VLAN/subnet)
- Isolation Whitelist: Gateway Only (Automatic) **Create**
(The whitelist requires entries for the subnet gateway and other allowed hosts.)
(The whitelist can only contain wired destinations, wireless clients are not supported on the whitelist.)
- Priority: High Low

RADIUS Options

Advanced Options

OK **Cancel**

FIGURE 17 Onboarding SSID Configuration for Unleashed

Create WLAN [X]

* **Name:**

Usage Type:

- Standard** for most regular wireless network usage
- Guest Access** guest access policies and access control will be applied
- Hotspot Service** known as WISPr
- Social Media** authenticate through social media network
- WeChat**

Hotspot Services:

Show Advanced Options ▶

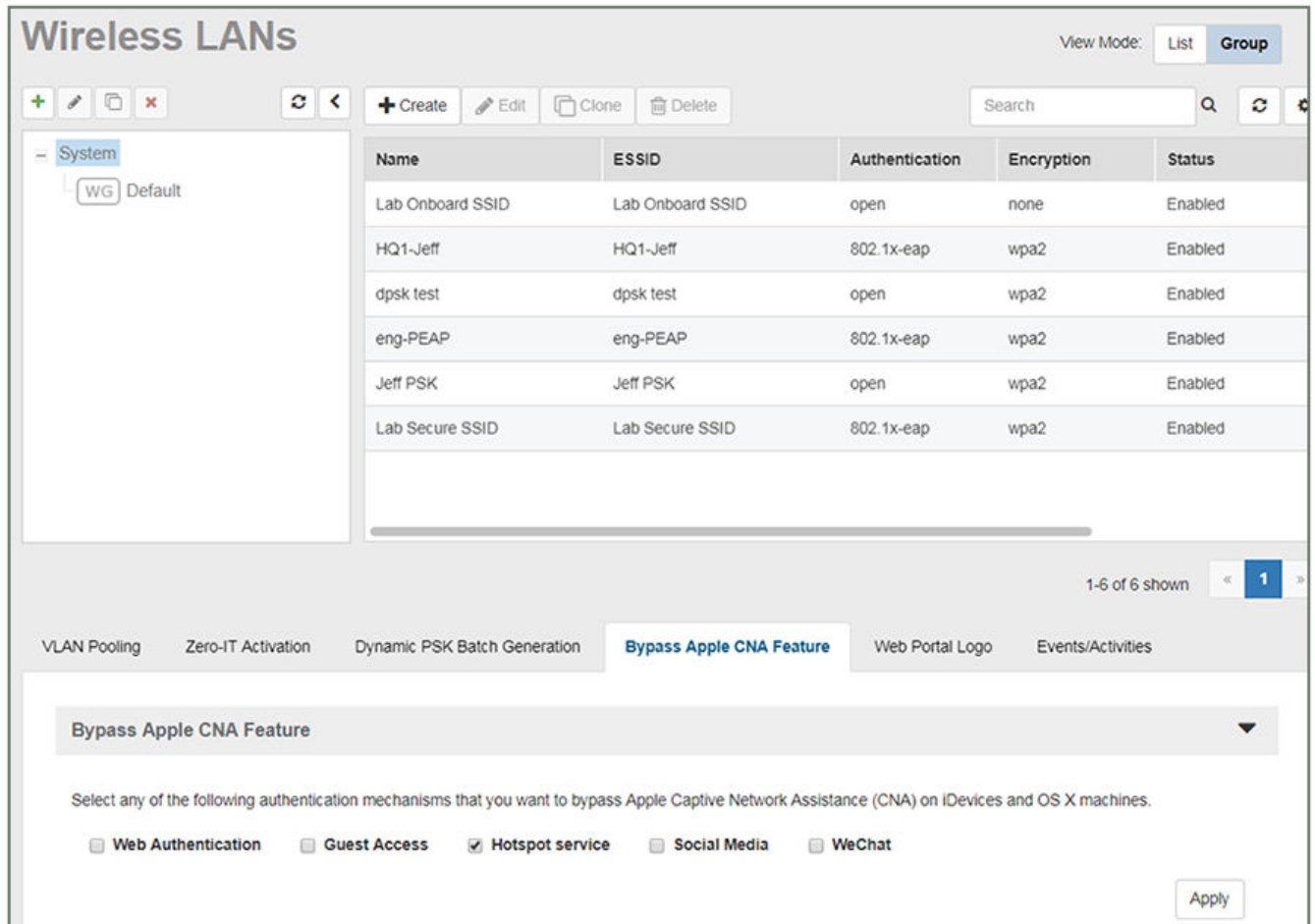
3. Authentication Options Method=Open for ZoneDirector, MAC Address for SmartZone. (Not applicable for Unleashed.)
4. The checkbox next to MAC Authentication (SmartZone only) called "Use user defined text as authentication password (default is device MAC address):" can be left unchecked.
5. The MAC Address 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 22.
 - For Unleashed, after you finish configuring the onboarding SSID, refer to [Figure 20](#) on page 23.
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



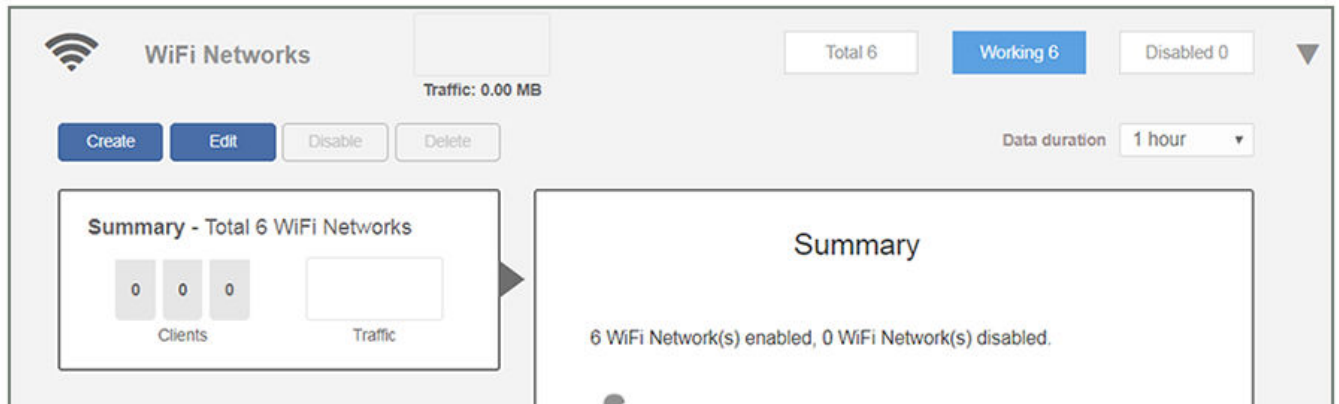
2. In the "Bypass Apple CNA Feature" area of the screen, check the "Hotspot service" box.
3. Click **Apply** to enable the "Bypass Apple CNA Feature" globally on all Wireless LANs that are configured as type "Hotspot Service (WISPr)."

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.

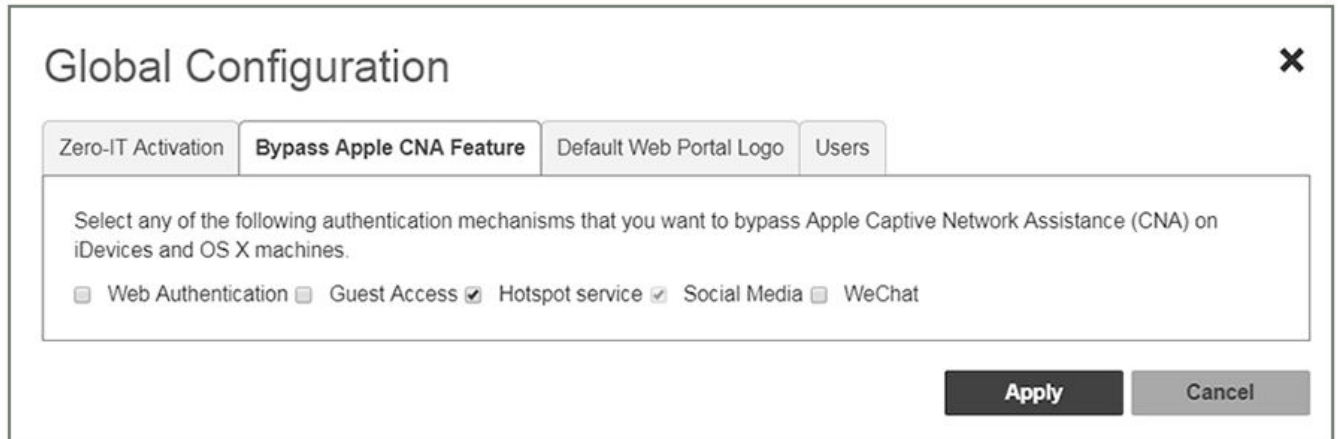
1. In the WiFi Networks main screen (see figure below), click **Edit**.

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

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

Create Split

Display Name:

Description:

Match Behavior:

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.

Step 2: Split users by:

Option 1:

Option 2:

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:

Title:


No Item Available Message:


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

The screenshot shows a configuration page for a workflow option. It is divided into two main sections: 'Webpage Display Information' and 'Filters & Restrictions'.
Webpage Display Information:
- **Sample User Display:** A preview box showing 'Short Name' and 'Display Title'.
- **Short Name:** Text input field containing 'MAC Registered Devices'.
- **Display Title:** Text input field containing 'MAC Registered Devices'.
- **Display Text:** A large text area for additional description.
- **Enabled:** A checked checkbox.
- **Icon File:** A section with a 'Default' dropdown set to 'Using default file.' and an 'Upload' section with a 'Choose File' button and 'No file chosen' text.
Filters & Restrictions:
- A note explains that these settings control user access.
- **User-Based Filters:**
 - **Group Name Pattern:** Matches [ex. BYOD]
 - **Username Pattern:** Matches [ex. bob]
 - **User DN Pattern:** Matches [ex. .*ou=IT,*]
 - **Email Pattern:** Matches [ex. .*@company.com]
- **Device-Based Filters:**
 - **Operating System Pattern:** Matches [ex. *Android*]
 - **User-Agent Pattern:** Matches [ex. *Safari*]
 - **Language Pattern:** Matches [ex. *en*]
 - **MAC Registration List:** Matches [ex. IT-Owned MACs] (This field is highlighted with an orange border).
 - **DHCP Summary Pattern:** Matches [ex. *Windows*]

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

Modify MAC Registration

① Display Name:

① Description:

Registration Information

① SSID Regex:

① Expiration Date Basis:

① Behavior:

① Config Shortcuts:

① Redirect URL:

① Use POST:

① POST Parameters:

① Allow Continuation:

① Kill Session:

Authentication Attributes

Success Reply Attributes: When the RADIUS authentication is successful, an Access-Accept will be returned to the WLAN or wired infrastructure. If additional attributes are specified here, they will also be included in the reply.
No additional attributes currently exist.

Failure Reply Attributes: When the RADIUS authentication is unsuccessful, an Access-Reject will be returned to the WLAN or wired infrastructure. If additional attributes are specified here, the reply will be an Access-Accept along with attributes specified here.
No additional attributes currently exist.

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

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

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

NOTE

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

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

NOTE

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

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

Adding RADIUS Attributes

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

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

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

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

How to Add a Message to Users

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

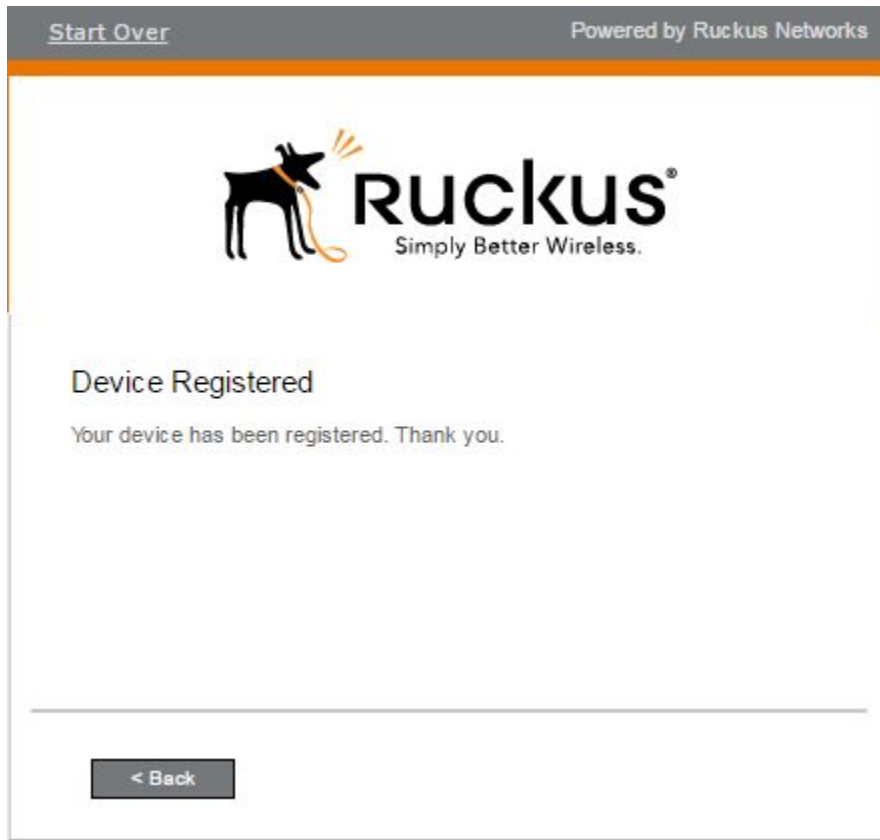
1. On the workflow page, click the **Insert** arrow to create a step in the enrollment workflow.

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

5. **Save** the configuration.

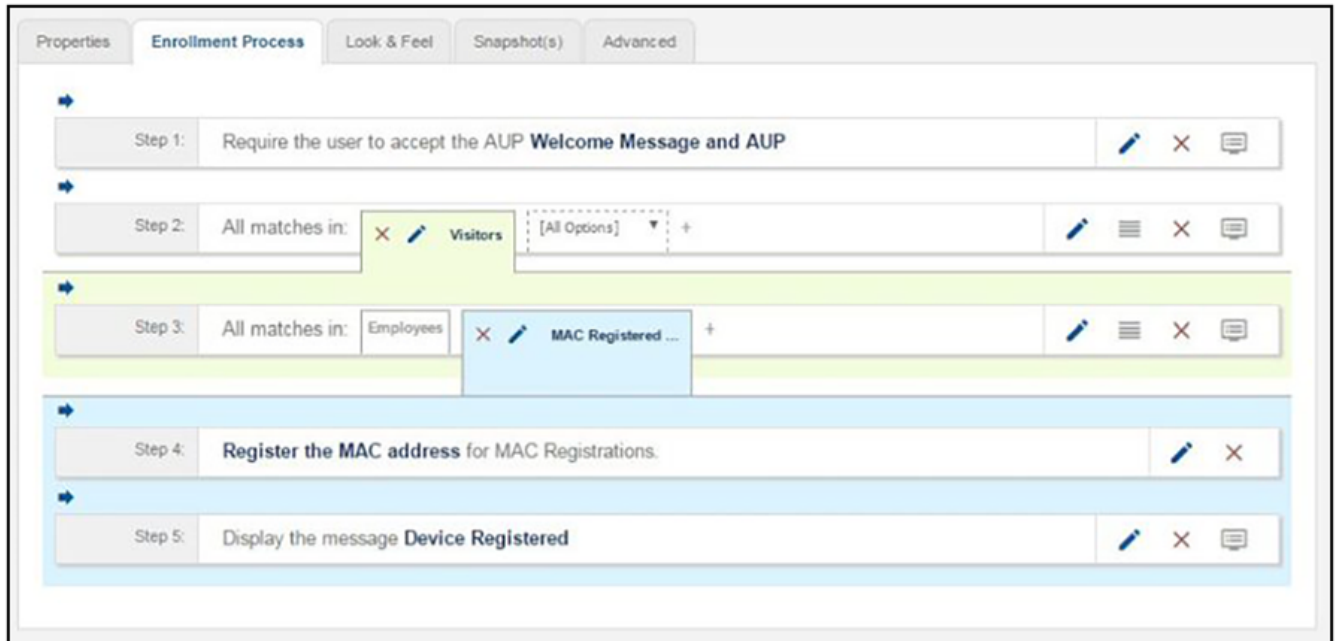
On the workflow page, click the **view** icon next to the **Display Message** step to see a preview of the message.

FIGURE 24 Example Message to User



The completed workflow is displayed below.

FIGURE 25 Completed Workflow for MAC Registration

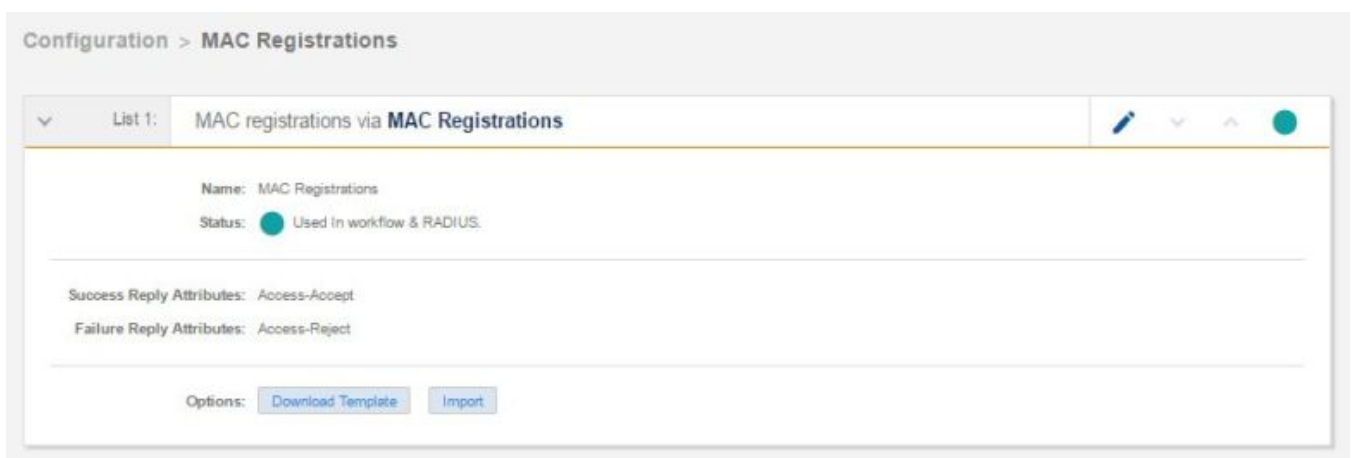


Import MAC Registration List

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 26 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.

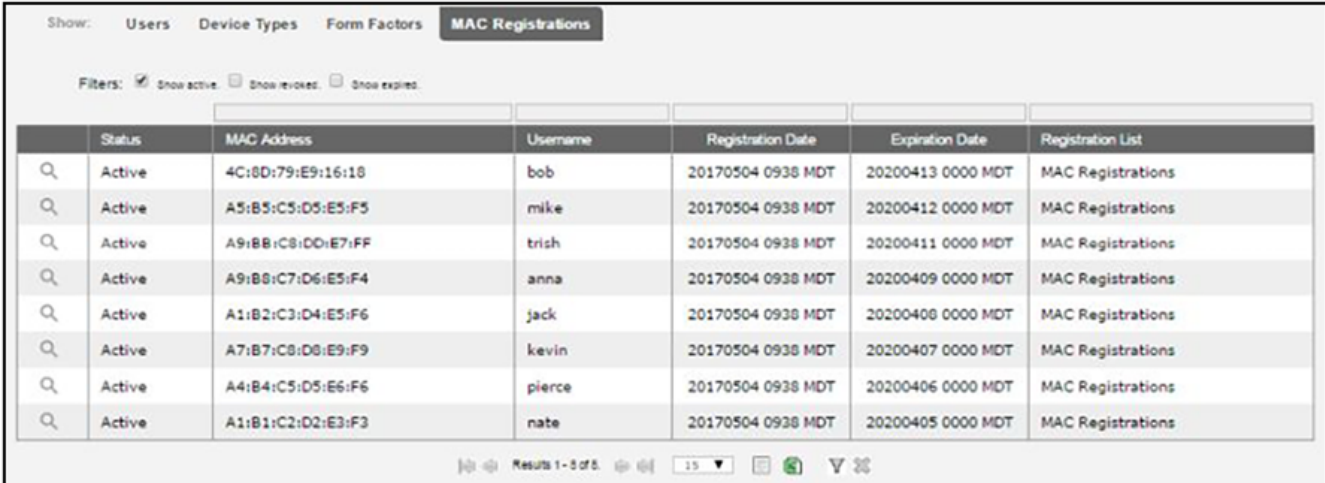
Viewing MAC Registration Records on the Dashboard

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 27 MAC Registrations on the Dashboard



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:BB: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

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**.

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

FIGURE 28 View MAC Registration Details

The screenshot displays the 'View MAC Registration' page in the Cisco Controller interface. At the top, there are tabs for 'Users', 'Device Types', 'Form Factors', and 'MAC Registrations'. The main content is divided into three sections:

- MAC Registration Information:**
 - Status: Valid through 20200412 0000 MDT (with a 'Revoke' button)
 - 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)
Valid through 20200412 0000 MDT	MAC Registrations	A5:B5:C5:D5:E5:F5	mike	20170504 0938 MDT	20200412 0000 MDT		

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

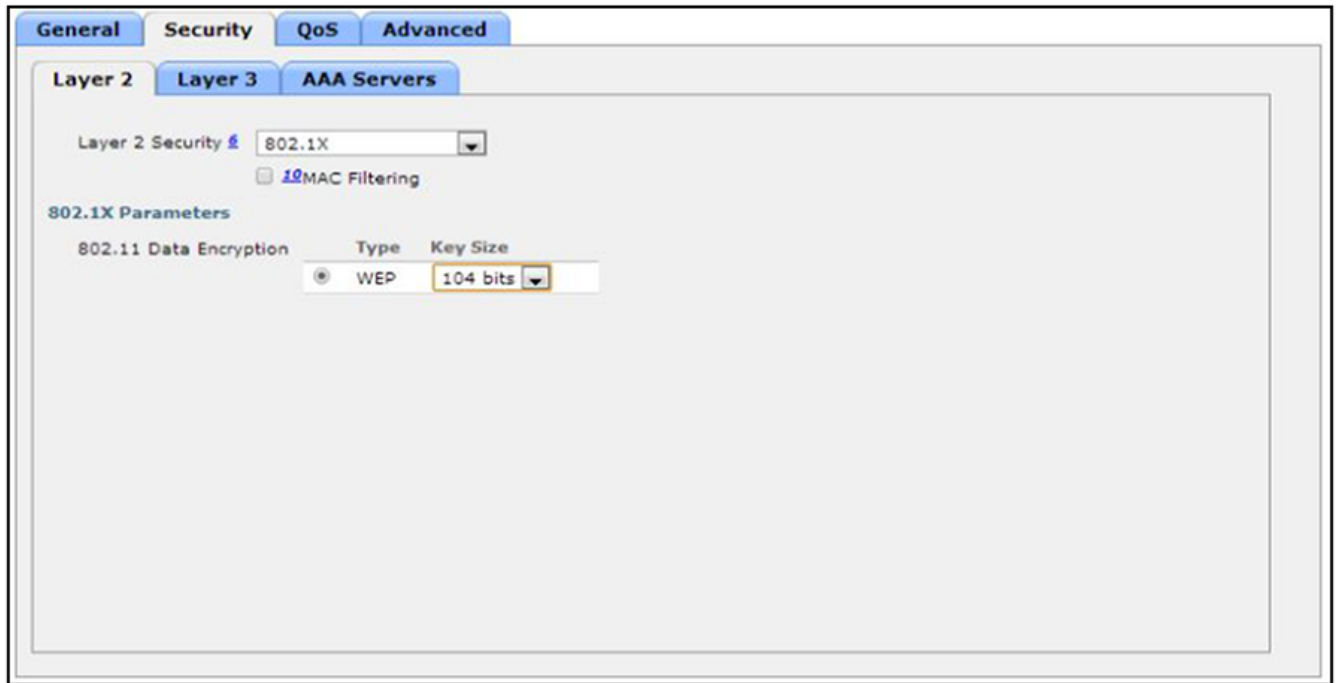
Configuring a Cisco Controller for MAC Registration

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.

- On the wireless controller, go to the **WLANS** tab and select the WLAN for MAC registration.
- 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 29 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 30 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 31 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 32 Select RADIUS Server



7. **Apply** changes.

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



© 2018 ARRIS Enterprises LLC. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com