Cloudpath

XpressConnect Enrollment System

Configuring MAC Registration

Software Release 4.2

December 2015

Summary: This document describes the MAC registration process, how to set up MAC registration on a wireless LAN controller, how to configure the Enrollment System for MAC registration, including RADIUS attributes, how to view and revoke MAC registration enrollments, and troubleshooting information.
Document Type: Configuration
Audience: Network Administrator

Cloudpath

Configuring MAC Registration with the XpressConnect Enrollment System

Software Release 4.2

December 2015

Configuring MAC Registration

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, the XpressConnect Enrollment System 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 Enrollment System for onboarding to the secure network.

This document describes how to configure the XpressConnect Enrollment System and a Cisco Wireless LAN Controller to support MAC Registration.

Use Case

Your security policy includes a network registration system. A user with a gaming console, who wants to set it up for use on the network, is required to register the device for network access. The network administrator provides a method for obtaining the MAC address of the device and adds this as an authorized MAC address in the RADIUS server.

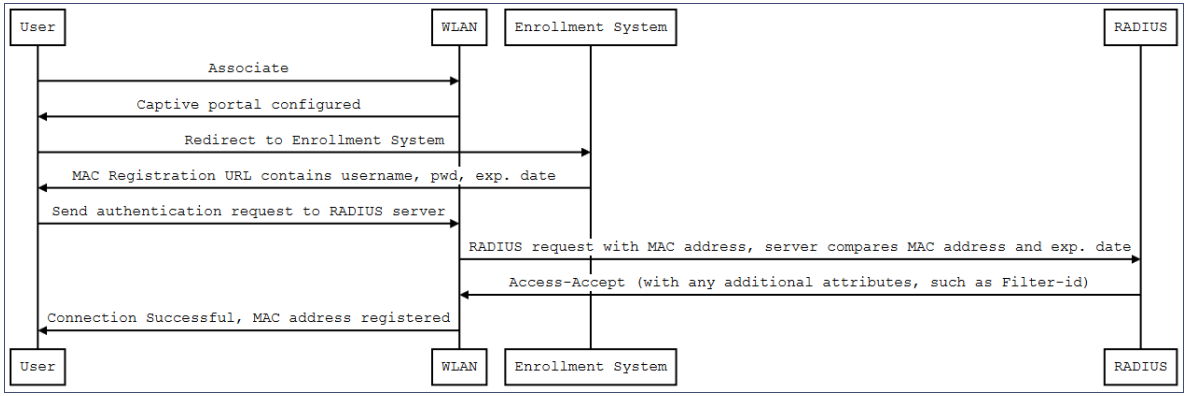
During network setup, the device detects the onboarding SSID, is authenticated against the RADIUS server, and is redirected to the Enrollment System for onboarding to the secure network.

During the enrollment process, a workflow step detects the user-agent of the gaming device and moves it to the workflow branch for MAC registration. After the device is registered, a message displays the SSID for the PSK network. The user manually configures the device and connects to the secure PSK network.

MAC Registration Process

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

FIGURE 1. MAC Registration Sequence



At the MAC registration step, the Enrollment System 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.

> **Note >>**
> The format of the URL varies, depending on the controller vendor. For example, a Cisco controller expects the redirect URL to be in the format: *https://1.1.1.1/?username=name&pwd=pwd1*.

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 the Cisco Wireless LAN Controller

This section describes how to configure the Cisco Wireless LAN Controller for MAC registration, authenticating devices against a RADIUS server.

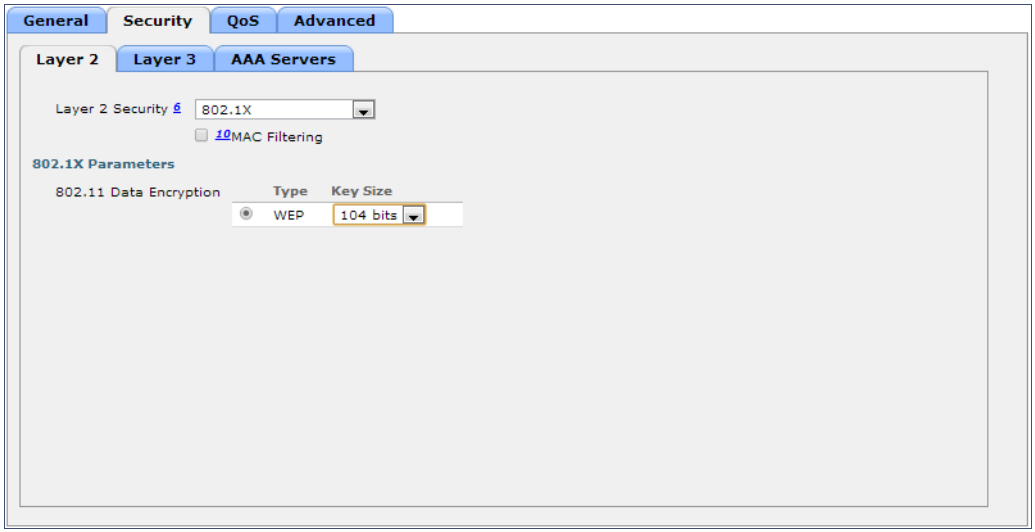
Prerequisites

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.

How to Set up MAC Registration

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 2. 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 3. Using Layer 2 Mac Filtering

When NOT using Layer 2 Mac Filtering

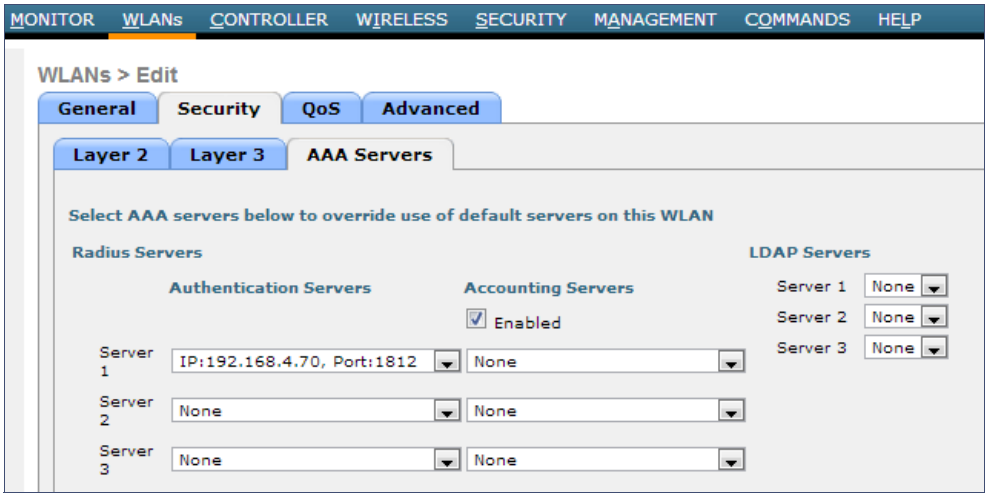
Web Policy - Authentication - If you select this option, the user is prompted for username and password while connecting the client to the wireless network.

FIGURE 4. Not Using Layer 2 Mac Filtering

Select *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 the Enrollment System as a RADIUS server, define the ES RADIUS server in the Cisco WLC in the *Security* > *Radius* Authentication window.

FIGURE 5. Select RADIUS Server



6. *Apply* changes. The wireless controller is configured for MAC registration against the RADIUS server.

Configuring the Enrollment System

This section describes how to create an enrollment workflow that registers a gaming device and moves it to the PSK network.

Create a MAC Registration Workflow

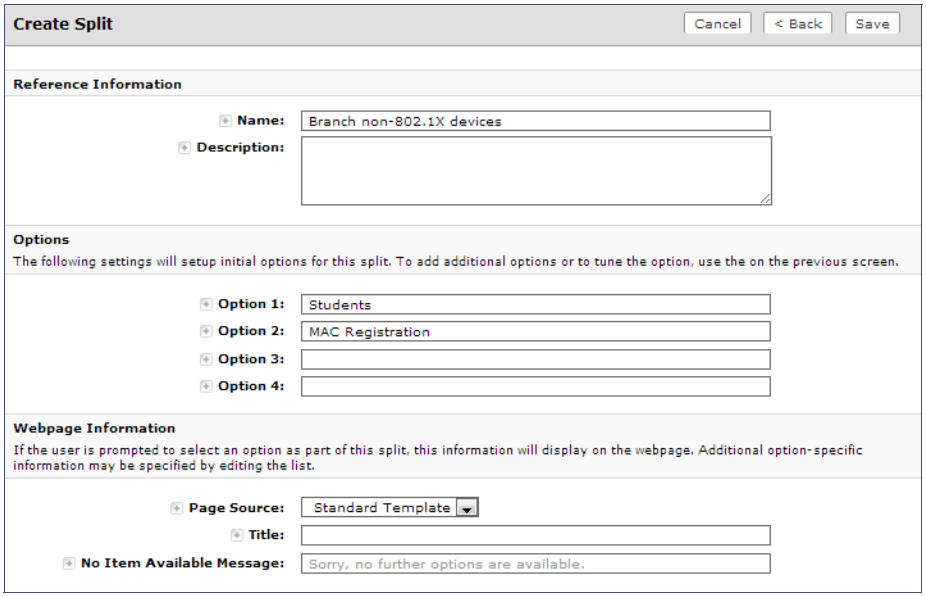
The ES configuration includes creating a branch in the workflow, defining a filter for gaming devices, adding a MAC registration workflow step, and moving the user to the PSK network.

How to Create a Workflow to Move Gaming Devices to a Specific Branch

1. Go to *Configuration* > *Enrollment* and select *Add New Configuration* from the *Configuration* drop-down menu.
2. On the *Create Configuration* page, enter the new workflow information and *Save*.
3. Click *Add* to add a workflow step.
4. Add an *Acceptable User 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 6. Create Split



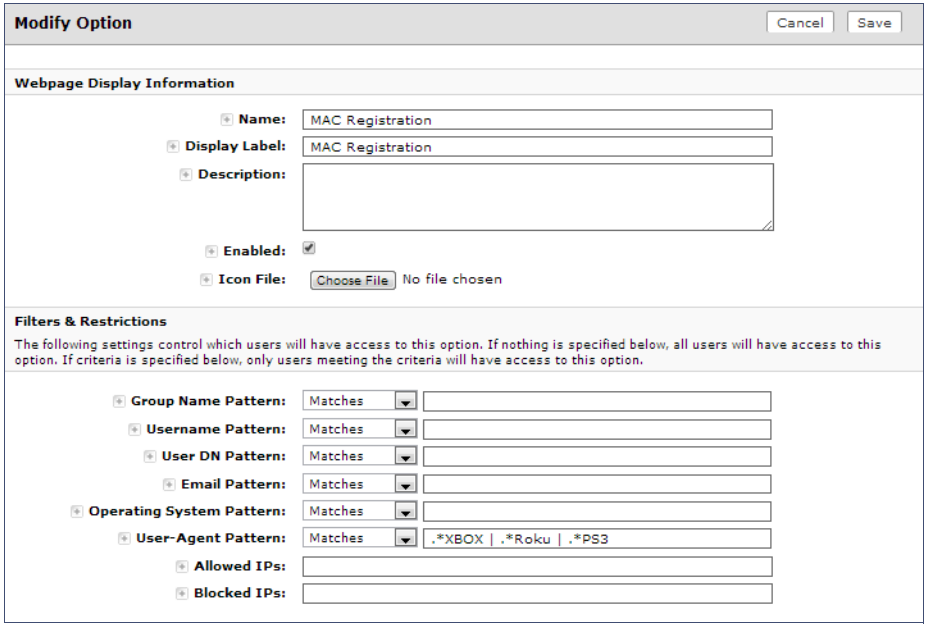
7. On the *Create Split* page, in the Options section, enter the names for the two workflow branches. For example, you can name Option 1, *Students*, and Option 2, *MAC-Registered*.
8. *Save* the split information. The named branches appear as tabs in the split workflow step.

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

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, in the *User-Agent Pattern* field, enter a regex pattern that matches known gaming devices. This moves all devices that match this user-agent pattern to the *MAC Registration* workflow branch.

> **Tip >>**
> For example, in the *User-Agent Pattern* field, enter .*Xbox | .*Roku | .*PS3 to ensure that specific gaming devices move to the MAC registration workflow.

FIGURE 7. Modify Split Options



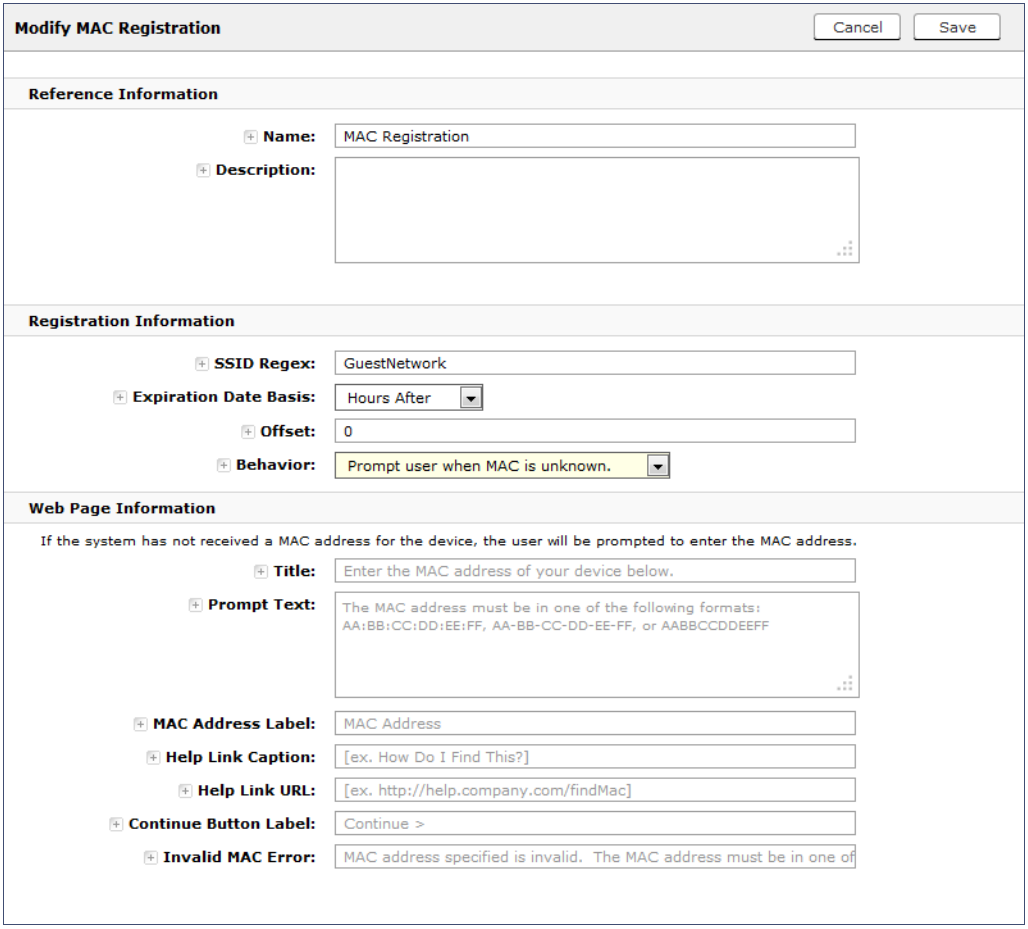
4. *Save* the changes to the option filter.
5. Click *Done* to return to the workflow.

> **Tip >>**
>
> 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.

How to Add a MAC Registration Step to the Workflow

1. On the workflow page, click the *Insert* arrow to create a step 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 8. Create MAC Registration



4. Enter the *Name* and *Description* for the MAC Registration step. For this example, enter the validity period as the *Name*. For example, enter *90 days*. In the workflow, the step will display as *Register the MAC address for 90 days*.
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 the XpressConnect Enrollment System* 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.

  -Skip registration when MAC is unknown.

> **Note >>**
> You can add RADIUS attributes to a MAC registration configuration. See How to Add RADIUS Attributes for MAC Registration.

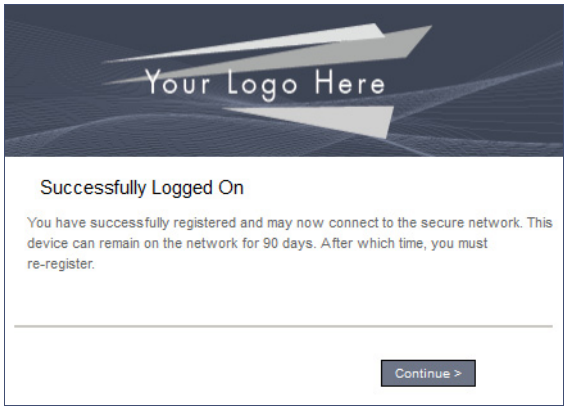
How to Add a Message to Users

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 PSK network. No user action is required.
5. *Save* the configuration.

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

FIGURE 9. Example Message to User



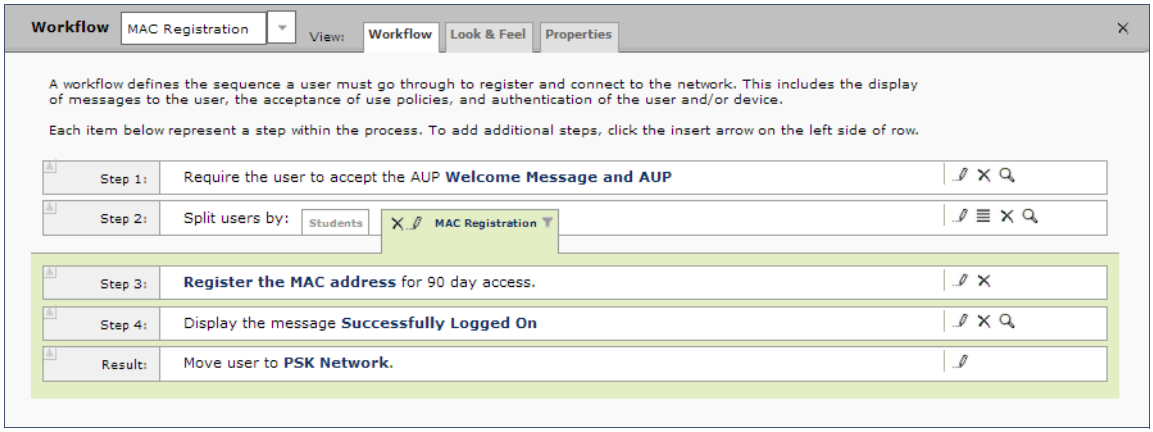
How to Create a Device Configuration for MAC-Registered Devices

This section describes how to create a device configuration for moving MAC-registered devices to a PSK network.

1. On the right side of the enrollment workflow, click the pencil to *Edit* the final enrollment step.
2. Select *A new device configuration.*
3. Select *Wireless Connections*.
4. Name the configuration. For example, name the configuration *PSK network*.
5. Enter the *SSID* of the PSK network.
6. In the *Authentication* field, select *WPA2-Personal PSK*.
7. Leave the default values for *Encryption (AES)* and *Broadcast (Yes, the SSID is broadcast)*.
8. Enter any *Conflicting SSIDs*.
9. Select the device *OSes* to allow with this configuration.
10. Select your configured *RADIUS server.*
11. Optional. Enable additional settings.
12. Select *Do not issue a certificate to the user.*

The workflow is updated to move a MAC-registered device to the PSK network.

FIGURE 10. Completed Workflow for MAC Registration



All clear-text authentication attempts coming from the onboarding SSID are redirected to the Enrollment System, where they are moved to the PSK network, according to the workflow configured in the previous section.

How to Add RADIUS Attributes for MAC Registration

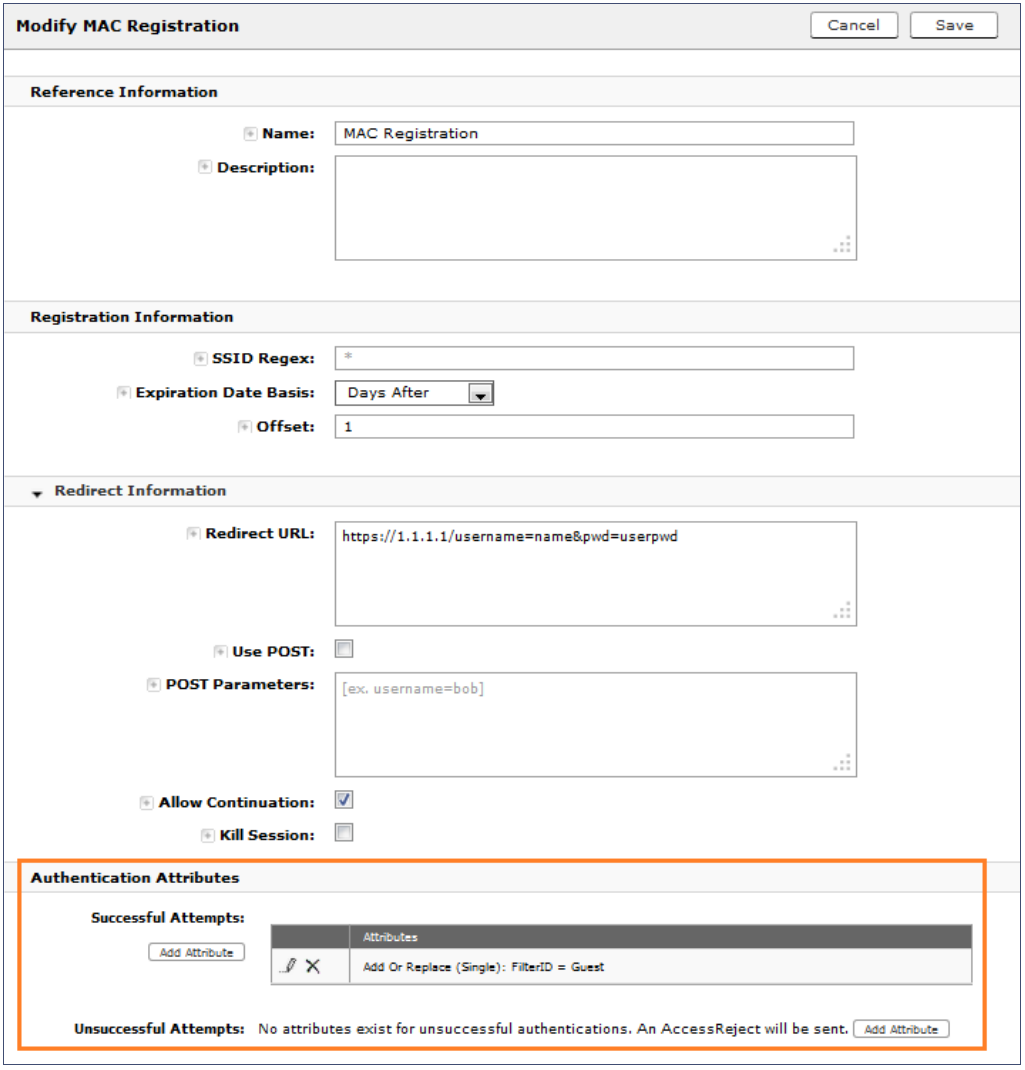
During association, the access point performs a MAC authentication with the RADIUS server. The RADIUS server looks up the MAC address, verifies that it has not expired, and returns an *Access-Accept*. If additional attributes are configured, they are returned with the *Access-Accept*.

> **Tip >>**
> You can add RADIUS attributes to a MAC Registration configuration *AFTER* the MAC Registration step has been configured.

To add attributes:

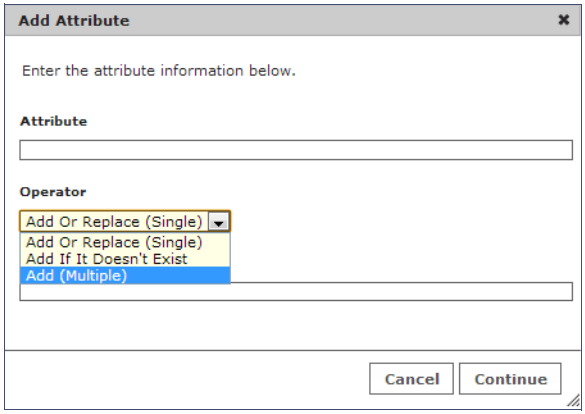
1. Double-click the MAC Registration step in the enrollment workflow to open the *Modify MAC Registration* page.

FIGURE 11. Modify MAC Registration



2. In the *Authentication Attributes* section, click *Add Attribute* for Successful (or Unsuccessful) Attempts.

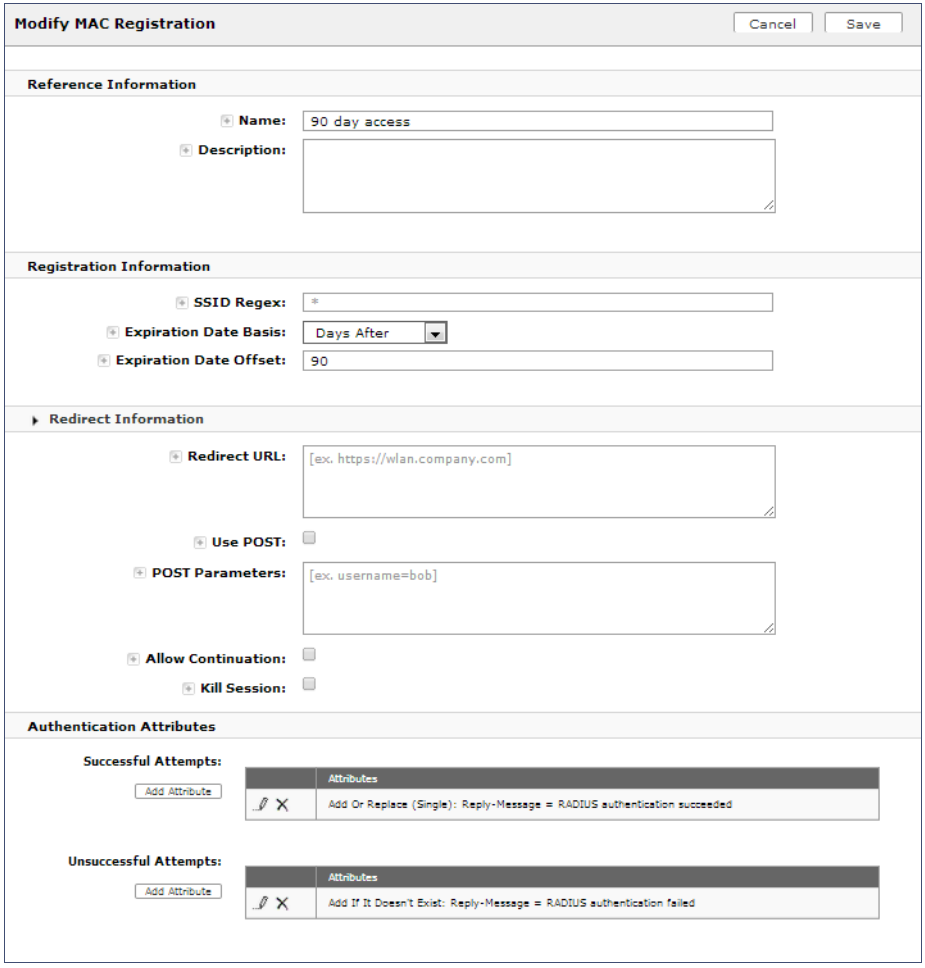
FIGURE 12. Add RADIUS Attribute



3. 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.

FIGURE 13. MAC Registration with Authentication Attributes



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

Tip >>

If you are using an external server (Cisco WLC) for MAC registration, complete the *Redirect Information* section to tell the Enrollment System to redirect to the captive portal. You also need to configure the controller to accept the redirect from the Enrollment System and then redirect back to the ES to continue with the workflow. If you are using a Motorola controller, the *Redirect Information* is not needed.

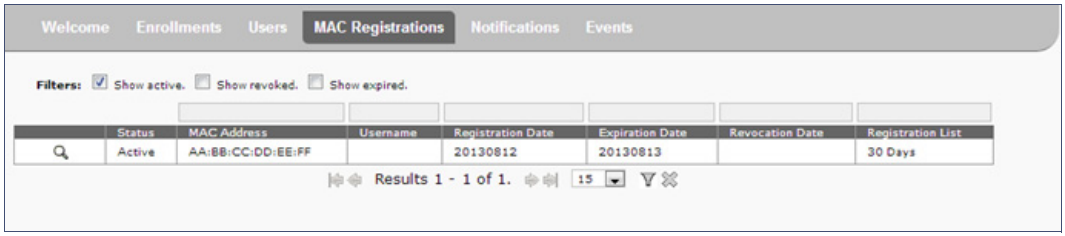
Viewing MAC Registration Records on the Dashboard

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 14. MAC Registrations on the Dashboard

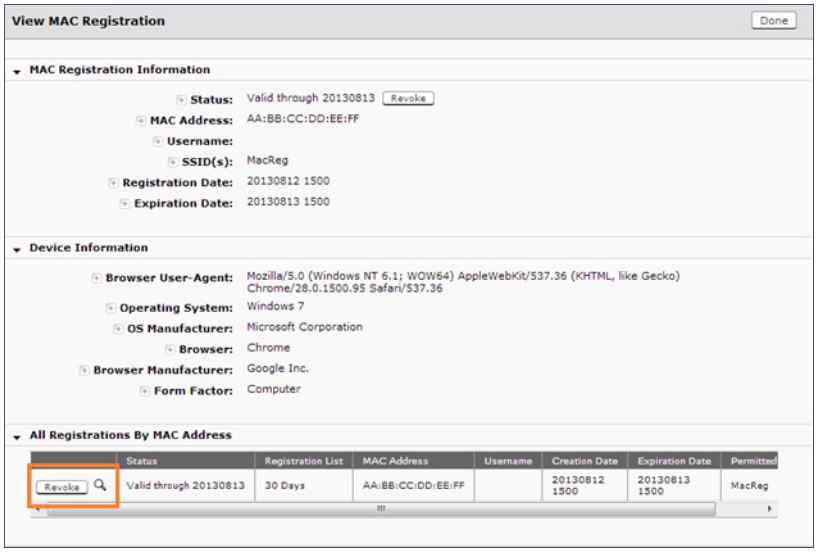


4. You can also access MAC registration information in the enrollment record. Go to *Operational* > *Dashboard* > *Enrollments* > *View Enrollment Record*.

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 15. 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.

Terminology

The following table defines terminology for the MAC registration feature.

TABLE 1. Sponsored Guest Access Terminology

Term	Definition
Enrollment	The process of a user becoming authenticated and ultimately gaining network access.
Enrollment workflow	The sequence a user must go through to register and connect to the network.
MAC address	The media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. A MAC address, also known as a physical address, is an address that is associated with a Network Interface Card (NIC) on an electronic device. Every NIC has its own unique MAC address, which allows a device to be uniquely identified on a network.

TABLE 1. **Sponsored Guest Access Terminology (continued)**

Term	Definition
MAC registration	Registering a device on a network by comparing the MAC address for a device against an authorized list on a RADIUS server.
Onboarding SSID	An open wireless network that provides access to the XpressConnect Enrollment System.
PSK network	A network configuration where access is manage using a pre-shared key.
Secure Wireless Network	A WPA2-Enterprise wireless network.
User-agent	A software user-agent identifies itself, its application type, operating system, software vendor, or software revision, by submitting a characteristic identification string to its operating peer.
Workflow branch	A particular enrollment sequence. This can occur (1) visually by having the user make a selection or (2) it can occur automatically based on criteria associated with each option. For example, a user that selects.

Additional Documentation

You can find detailed information in the Enrollment System configuration guides, located on the left-menu *Support* tab of the ES Admin UI.

About Cloudpath

Cloudpath Networks, Inc. provides software solutions and services that simplify the adoption of standards-based security, including WPA2-Enterprise and 802.1X, in diverse BYOD environments. Our goal is to make secure as simple as insecure; simple for network administrators to deploy and simple for users to access.

To learn more about the XpressConnect Enrollment System and how it can simplify your wireless environment, visit www.cloudpath.net or contact a Cloudpath representative.

If you need technical assistance, discover a bug, or have other technical questions, email support at support@cloudpath.net.

Contact Information

General Inquiries:info@cloudpath.net

Support:support@cloudpath.net

Sales:sales@cloudpath.net

Media:media@cloudpath.net

Marketing:marketing@cloudpath.net

Phone:+1 303.647.1495 (US)
+1 866.472.6053 (US)
+44 (01) 161.261.1400 (UK)
Fax:+1 760.462.4569
Address:1120 W 122nd Ave, Suite 302
Westminster, CO 80234 USA