CONFIGURATION GUIDE

# Cloudpath Enrollment System Cisco Wireless LAN Controller-Redirect Configuration Guide, 5.8

Supporting Cloudpath Software Release 5.8

*Part Number: 800-72848-001 Rev A*
*Publication Date: 26 February 2021*

# Copyright, Trademark and Proprietary Rights Information



## Export Restrictions

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

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

## Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

## Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

## Trademarks

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

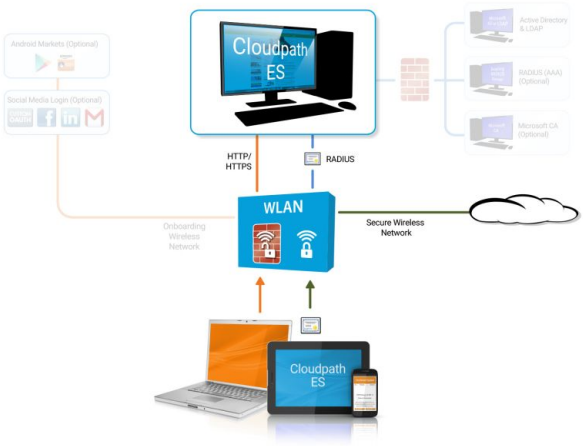
# Contents

# Overview

If you use Cloudpath to onboard wireless devices to a secure SSID, and would like to implement a Cisco Wireless LAN Controller to manage network policy, you can easily configure Cloudpath to redirect users through the WLAN Controller.

Cloudpath manages the entire enrollment process, opening the firewall to the open SSID, and passing the user through your policy management system before onboarding them to your secure WPA2- Enterprise wireless network.

**FIGURE 1** Cloudpath With WLC Passthrough




## Prerequisites

Before you can configure Cloudpath and Cisco WLAN Controller for web passthrough, you must have the following set up in your network.

- Cisco Wireless LAN Controller configured in your network
- IP address of Cloudpath system
- A Cloudpath enrollment workflow configured for your network

# Configuring the Cisco WLC for Web Passthrough

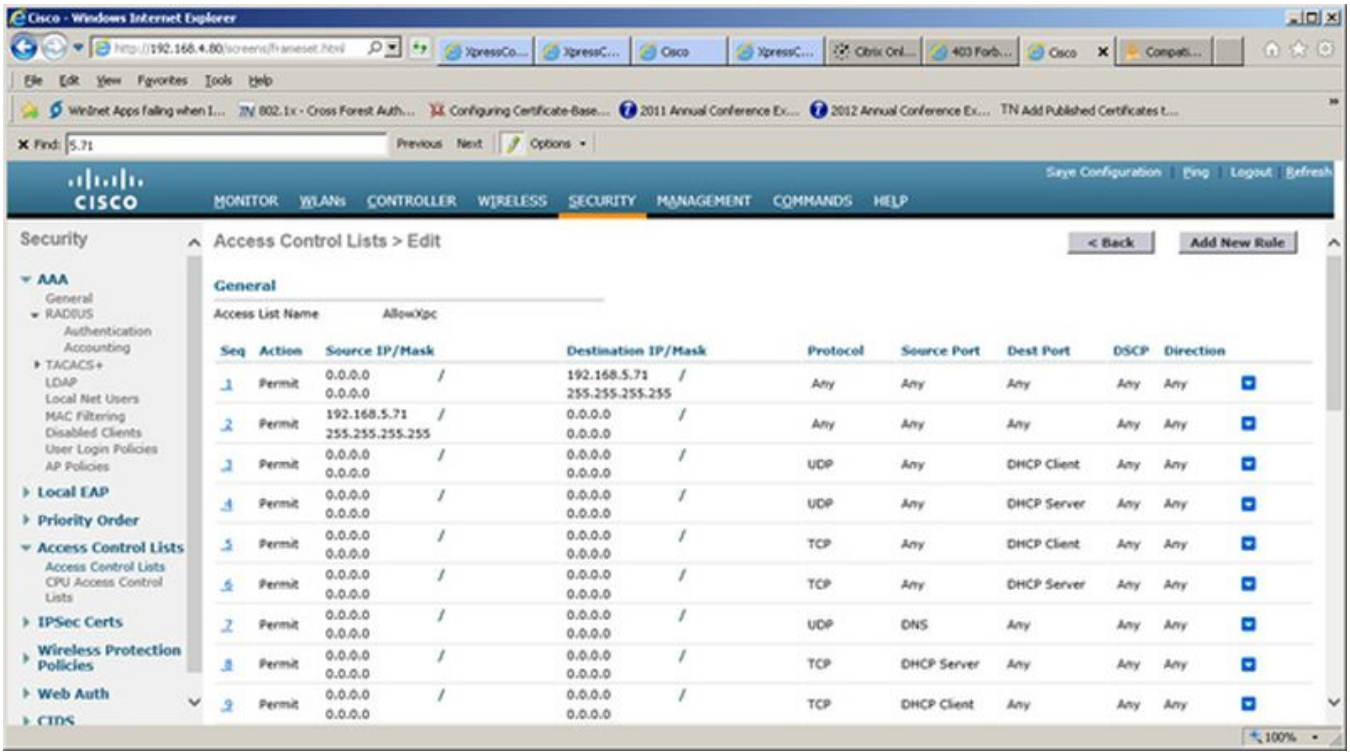
This section describes how set up the preauthentication ACL, the WLAN, and the Web Authentication Page on the Cisco WLC.

# Configure Access Control Lists

Configure a preauthentication ACL to allow access from the controller to and from Cloudpath.

1. On the Cisco WLAN Controller, under **Security**, expand **Access Control Lists**, and select the ACL to use for preauthentication.

   **FIGURE 2** Set Up the Preauthentication ACL



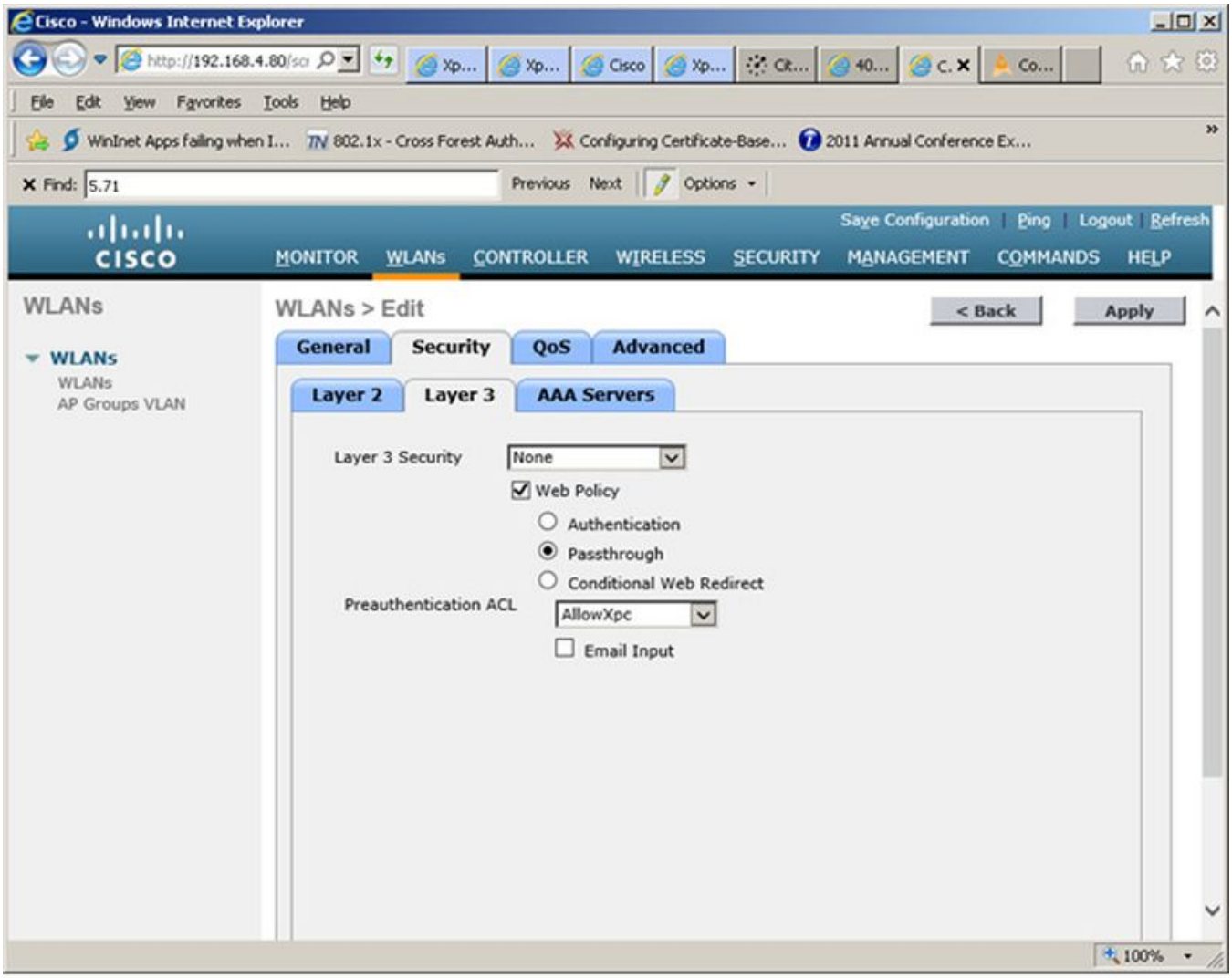

2. **Edit** the ACL to add rules to permit the client to and from Cloudpath.
3. **Apply** changes.

# Configure WLAN

Configure the WLAN to enable web passthrough and allow the preauthentication ACL created in the previous step.

1. On the Cisco WLAN Controller, under **WLANs**, edit the WLAN to use for the passthrough.

**FIGURE 3** Edit WLANs



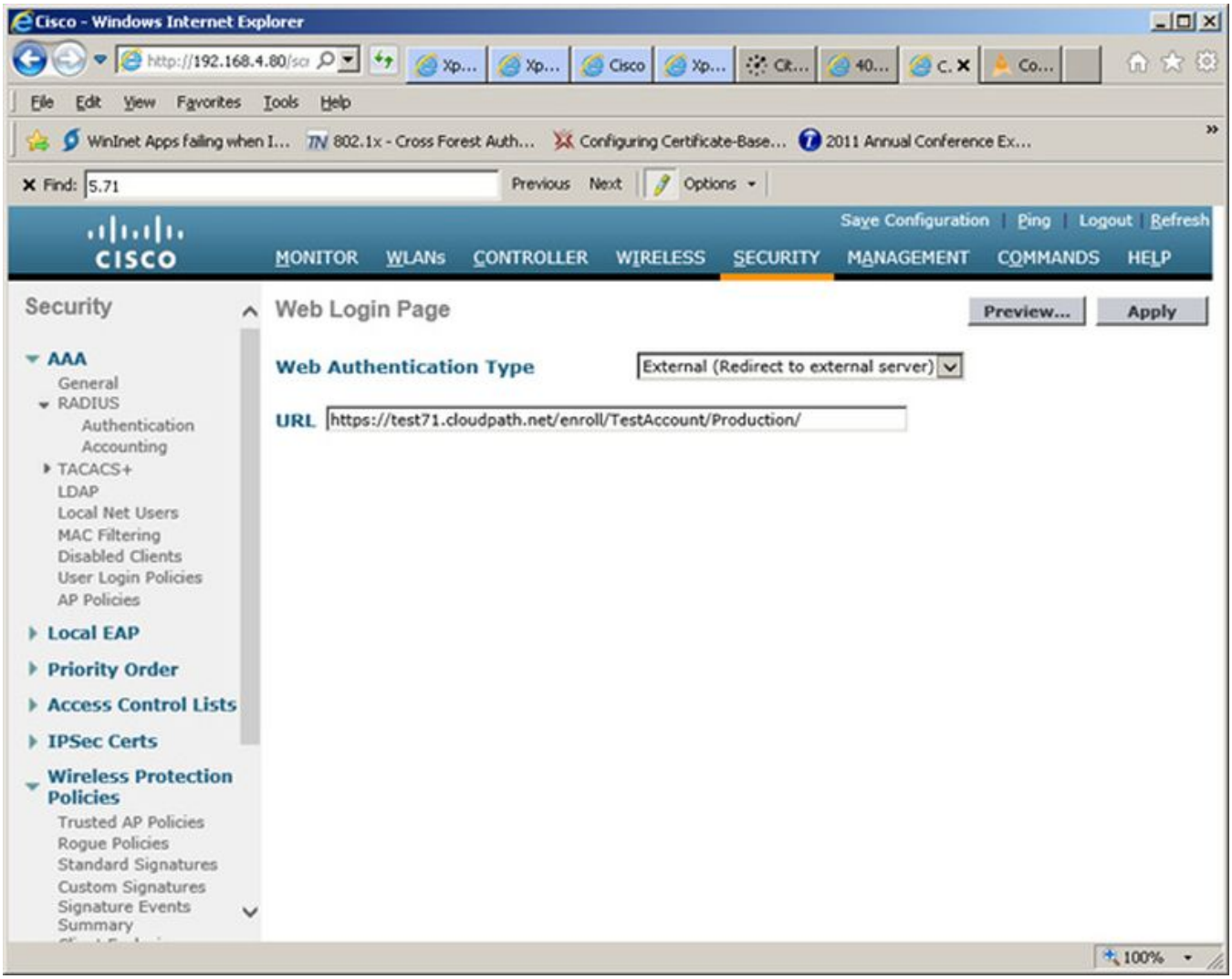

2. Select the **Security** tab and the **Layer 3** tab.
3. In the **Layer 3 Security** section, check the **Web Policy** box and select **Passthrough**. Leave **Layer 3 Security** at **None**.
4. Set the **Preauthentication ACL**. Leave **Email Input** unchecked.
5. **Apply** changes.

# Configure the Web Login Page

Set up the Cloudpath captive portal page. The WLC redirects the users to the Cloudpath captive portal, where they must accept the network AUP before they are moved to the open SSID for onboarding. Cloudpath manages the onboarding process instead of the WLC.

1. On the Cisco WLAN Controller, under **Security**, expand **Web Auth**, and select **Web Login Page**.

   **FIGURE 4** Configure Web Login Page




2. Select **External (Redirect to external server)**.
3. Enter the URL of Cloudpath.
4. **Apply** changes.

# Configuring Cloudpath for Web Passthrough

This section describes how to configure Cloudpath to manage the redirect URL from the WLC, including any parameters that must exist on the inbound request, and move the user to the captive portal to complete the onboarding process.

## Add the Redirect Step to the Workflow

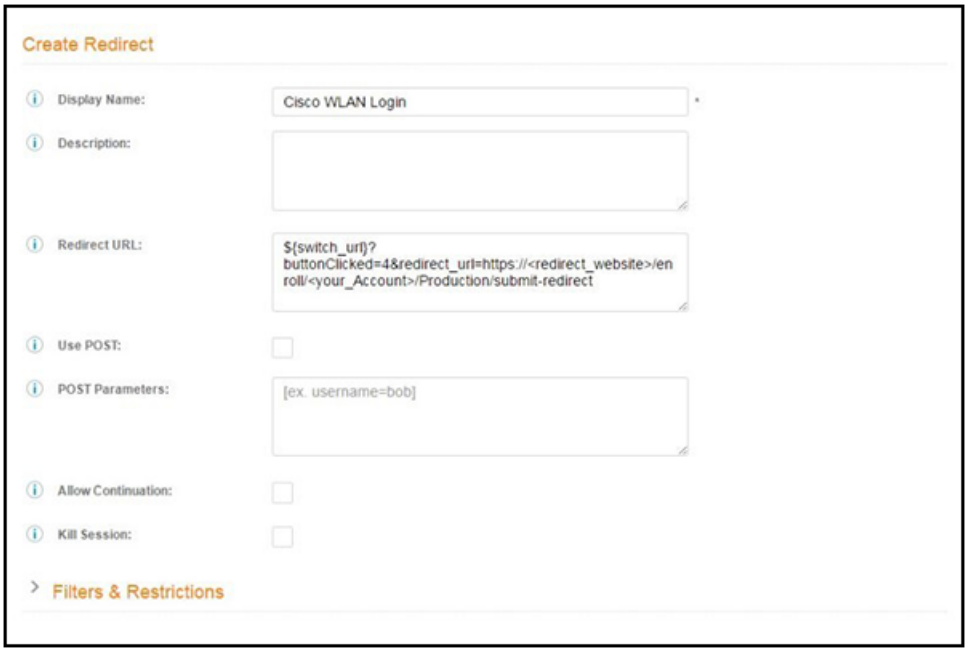
This section describes how to create a redirect step to the enrollment workflow to allow Cloudpath to accept an inbound connection request from the WLC, redirect the user to an Cloudpath-managed captive portal, and provide the onboarding process.

1. Navigate to **Configuration** > **Workflow**.
2. Select your passthrough workflow configuration.
3. In the workflow, insert the redirect step.

   **NOTE**
   In this example, the redirect occurs after the user accepts the AUP. However, the redirect step can be placed anywhere in the enrollment workflow.

4. The workflow plug-in selection page opens.
5. Click **Redirect the User**.
6. Select **Use a new redirect** and click **Next**. The **Create Redirect** page opens.

   **FIGURE 5** Create Redirect




7. Enter the **Reference information** for the Cisco WLAN passthrough.

8. Enter the **Redirect URL** in this format:

   ```
   ${switch_url}?buttonClicked=4&redirect_url=https://<redirect_website>/enroll/<your_Account>/
   Production/submit-redirect
   ```

   Note: The first part of this URL (`${switch_url}?buttonClicked=4&redirect_url`) takes the inbound request from the WLC and opens the firewall. The second part of this URL (`https://<redirect_website>/enroll/<your_Account>/Production/submit-redirect`) points the user to the Cloudpath captive portal.

9. Leave **Use POST** unchecked.

   Note: Cisco WLAN Controllers allow both **Get** and **POST** for the URL call, but we recommend using **Get**.

10. Check the **Allow Continuation** box. If this is left unchecked, the submit-redirect call is ignored.

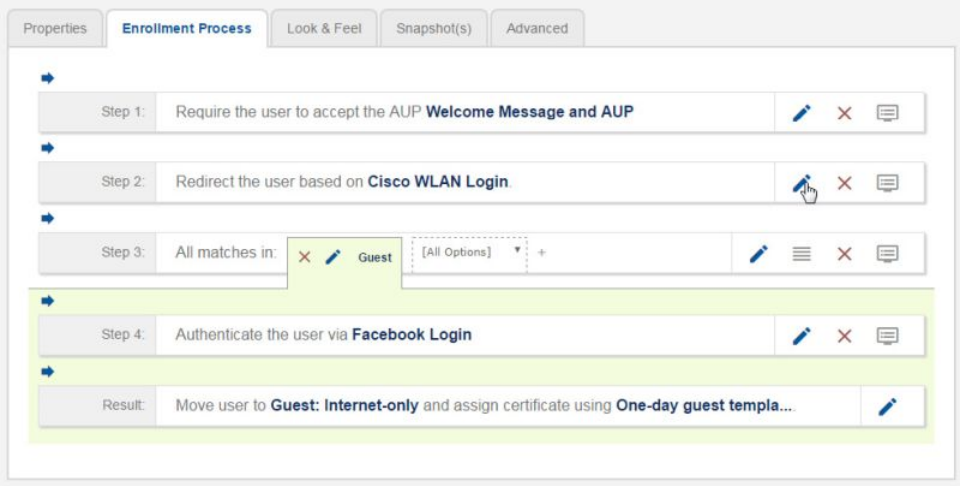
11. If needed, configure **Filters & Restrictions** to control when this redirect is utilized.

    By default the redirect is applied to all users. However, you can specify a filter such that the redirect is applied only to enrollments matching the filter.

12. **Save** the workflow.

In this workflow example, the WLC passes the user to the Cloudpath captive portal, to accept the AUP. The Cisco WLAN redirect opens the firewall so that the client can access Cloudpath for the onboarding process. If the user selects the guest enrollment path, the device is moved to the **Guest - Internet Only:** network and given a short-term guest client certificate.

**FIGURE 6** Completed Enrollment Workflow with Redirect Step




# Testing the Configuration

This section describes how to test the configuration for Cloudpath redirect through a Cisco WLAN Controller.

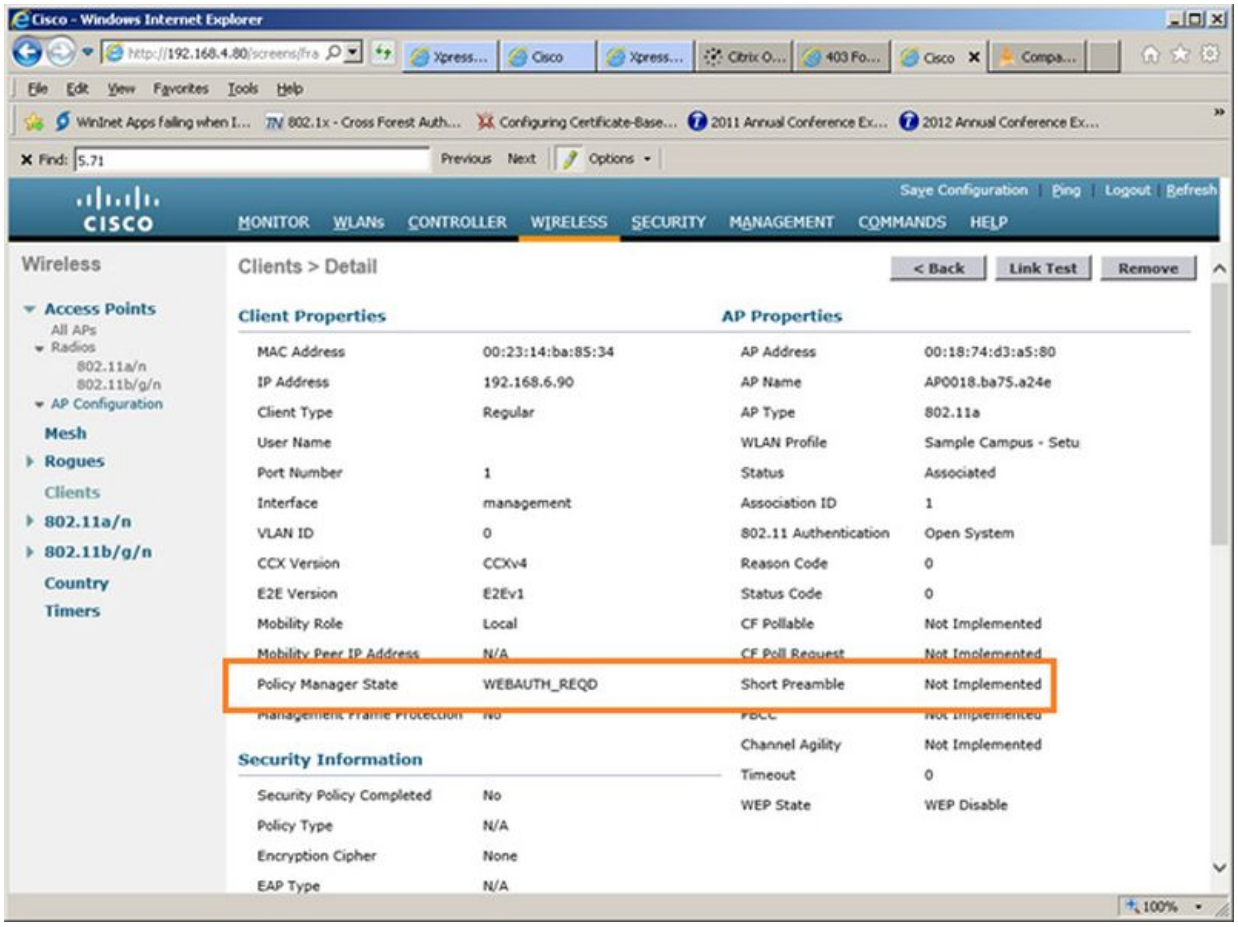
## Verify Client State

Use this information to verify the client state before and after the firewall is opened.

On the Cisco WLAN Controller, under Wireless, view the Client Properties.

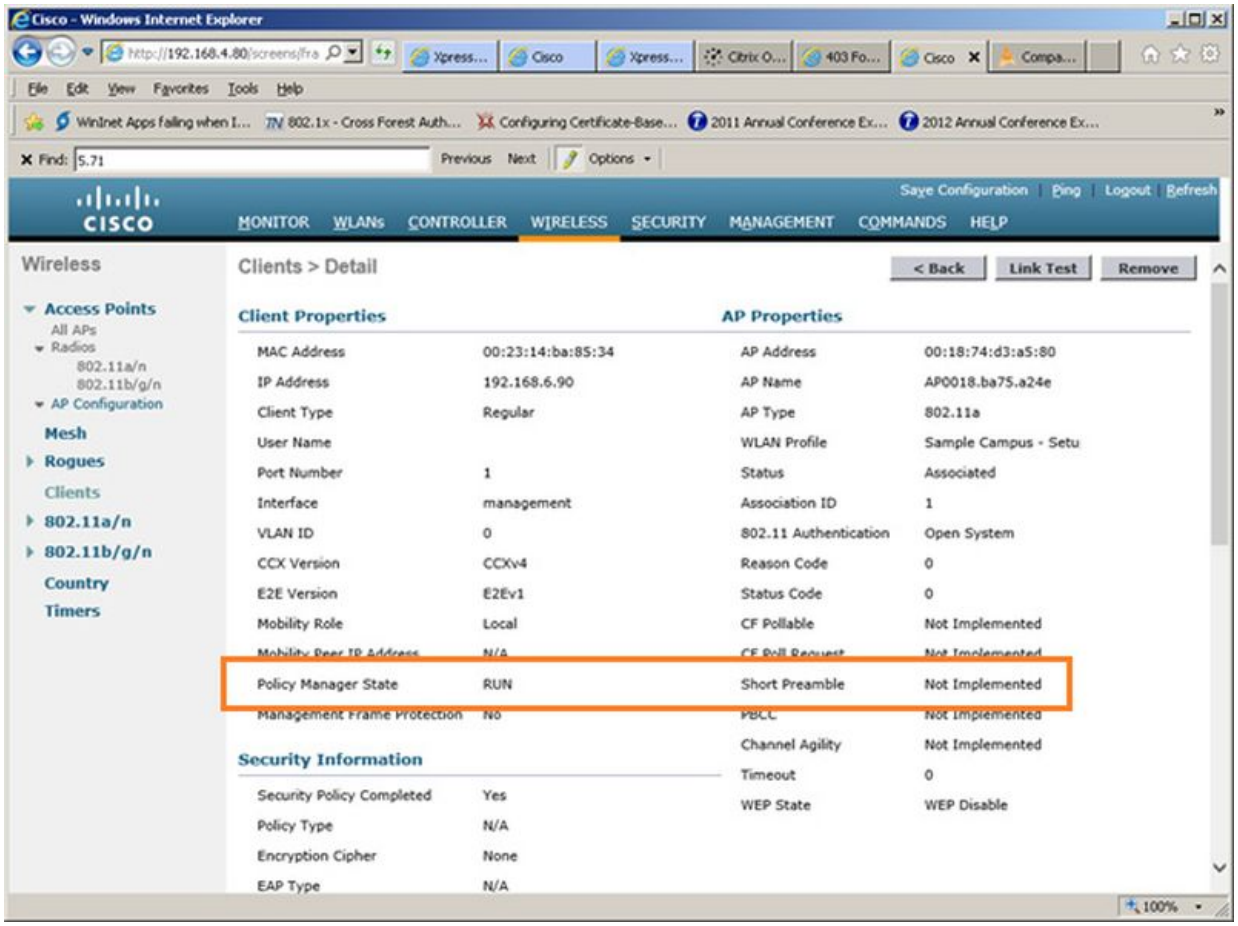
Before the firewall is opened, the **Policy Manager State** for the user should be in the **WEBAUTH_REQD** state. In this state, the WLAN Controller redirects all traffic.

**FIGURE 7** Client Detail Before Redirect




After the firewall is opened, the **Policy Manager State** for the user should be in the **RUN** state.

**FIGURE 8** Client Detail After Redirect



COMMSCOPE®
RUCKUS®


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