CONFIGURATION GUIDE

Configuring Cloudpath to Redirect Through a Cisco Wireless LAN Controller

Supporting Software Release 5.2

Part Number: 800-71654-001
Publication Date: August 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.

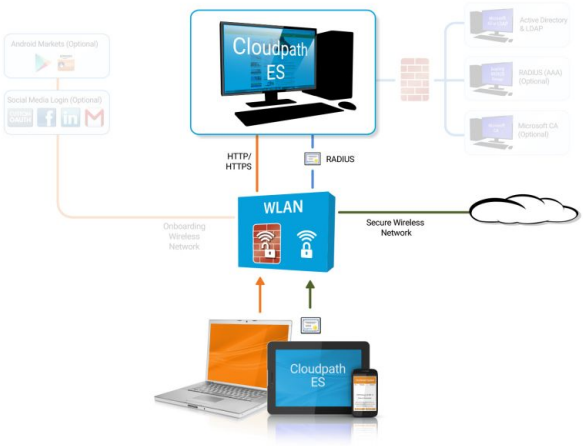
Contents

Overview

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

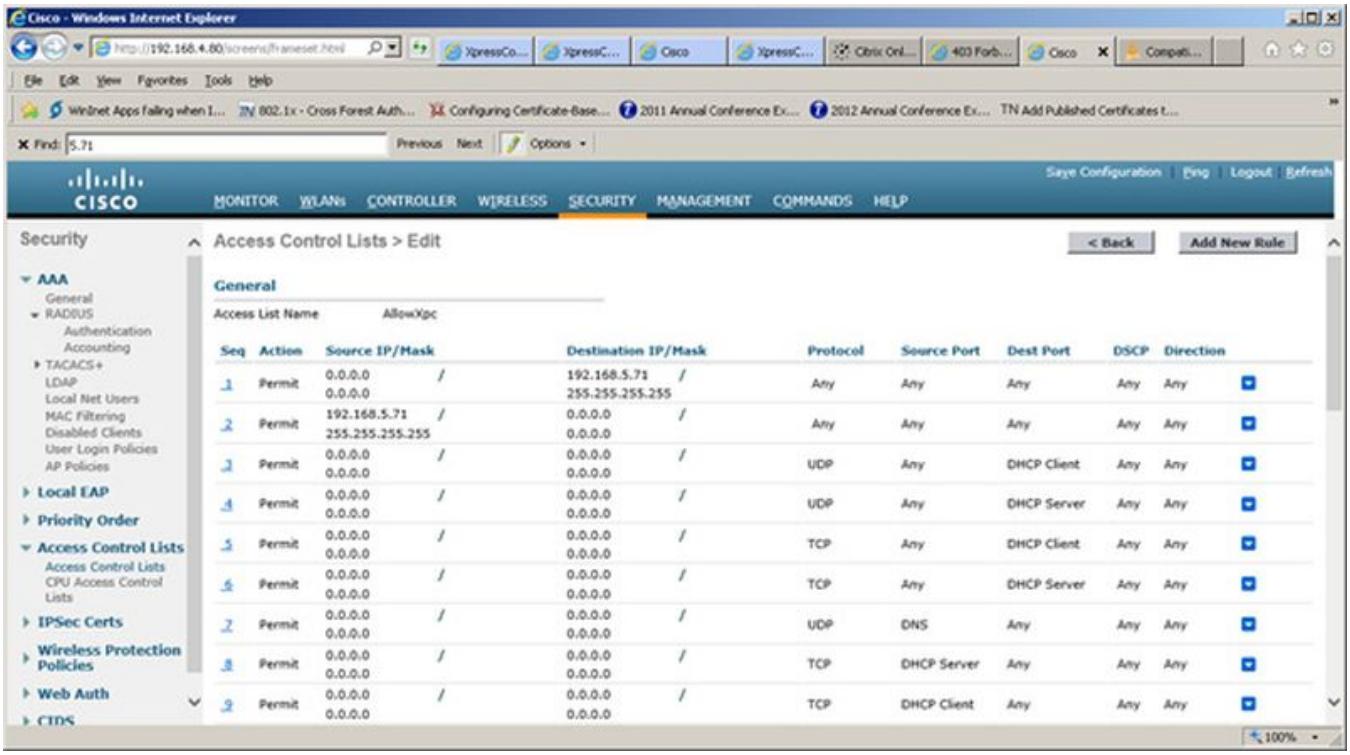
This section describes how set up the preauthentication ACL, the WLAN, and the Web Authentication Page on the Cisco WLC.

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



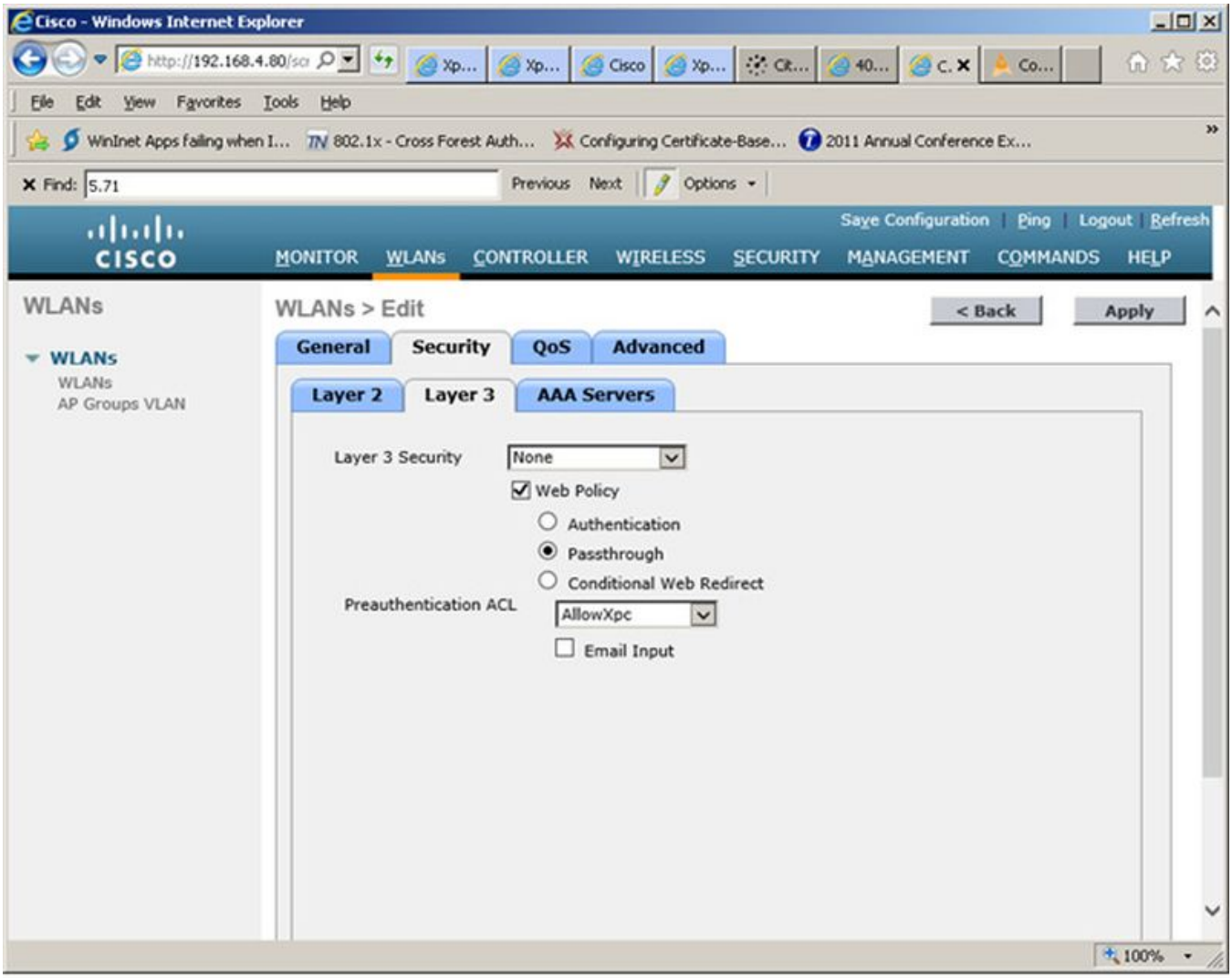
2. **Edit** the ACL to add rules to permit the client to and from Cloudpath.
3. **Apply** changes.

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



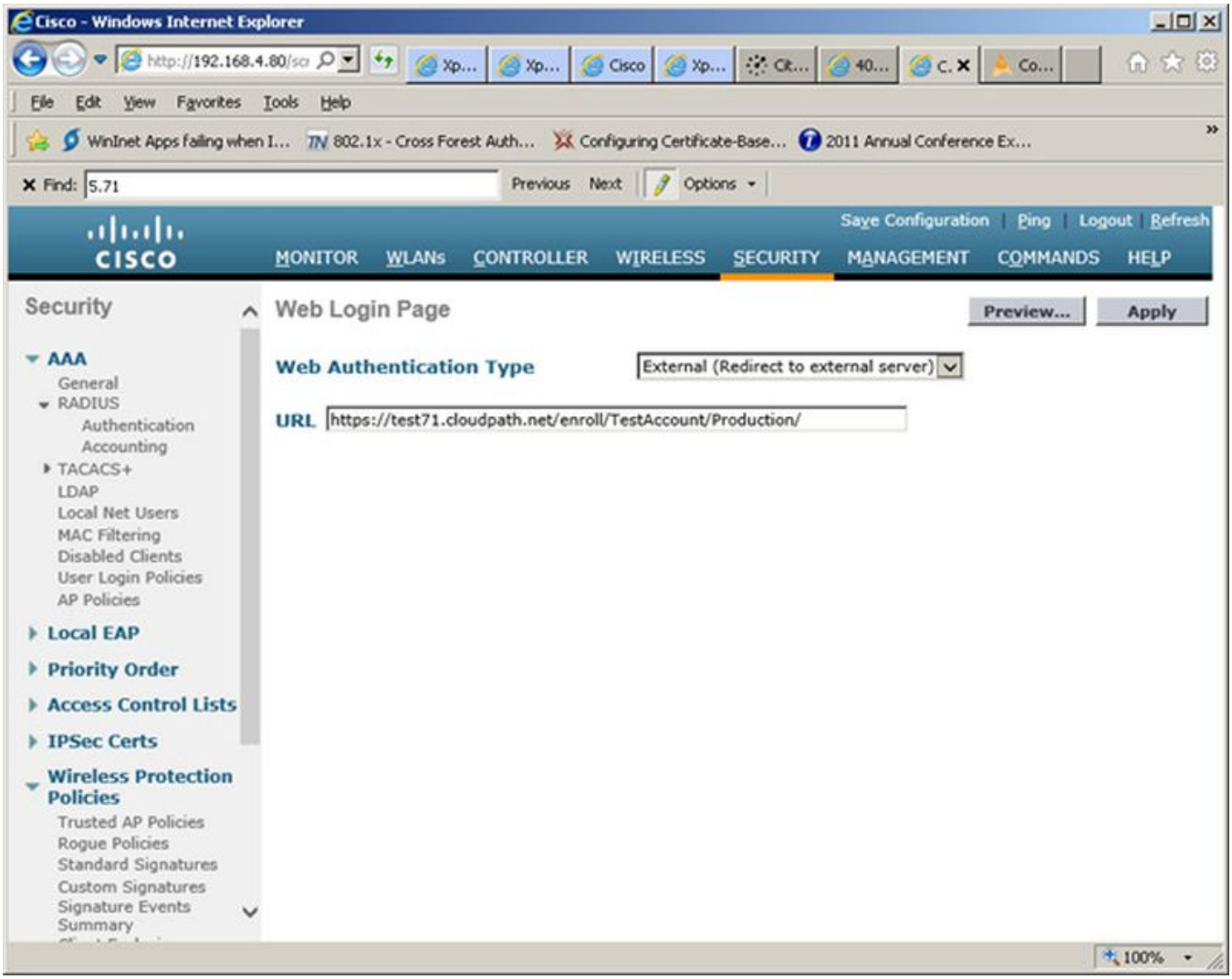
2. Select the **Security** tab and the **Layer 3** tab.
3. In the **Layer 3 Security** section, check the **Web Policy** box and select **Passthrough**. Leave **Layer 3 Security** at **None**.
4. Set the **Preauthentication ACL**. Leave **Email Input** unchecked.
5. **Apply** changes.

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

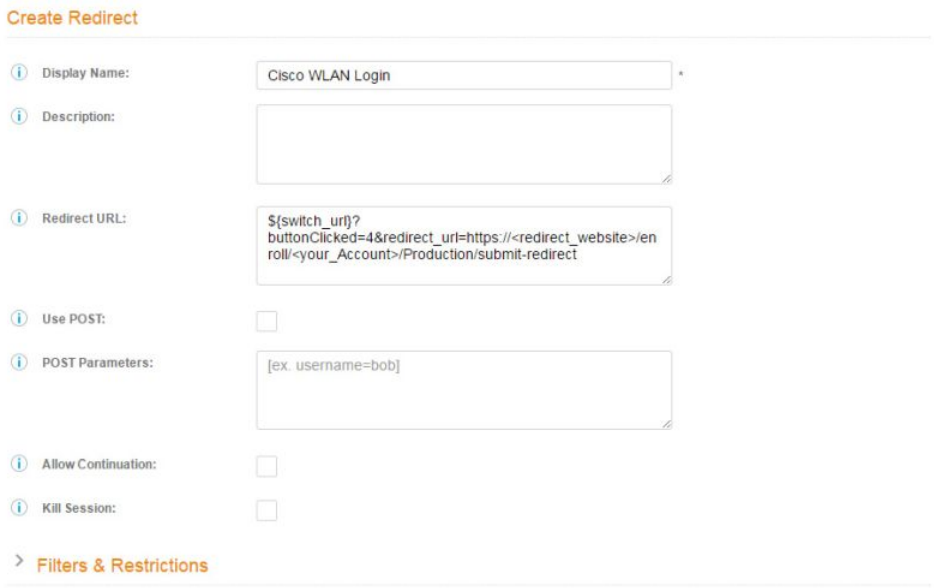
This section describes how to create a redirect step to the enrollment workflow to allow Cloudpath to accept an inbound connection request from the WLC, redirect the user to an Cloudpath-managed captive portal, and provide the onboarding process.

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. Select **Redirect the User** and click **Next**.
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**.

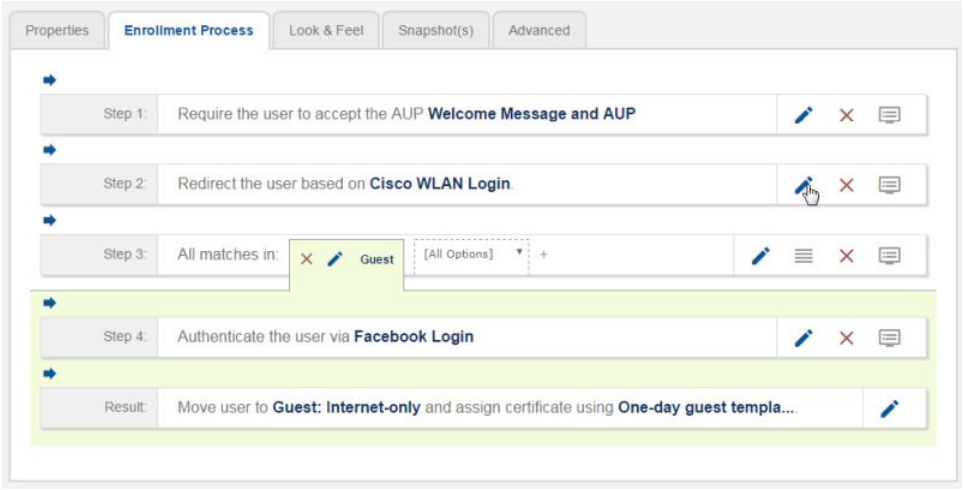
10. Check the **Allow Continuation** box. If this is left unchecked, the submit-redirect call is ignored.
11. If needed, configure **Filters & Restrictions** to control when this redirect is utilized.

    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.

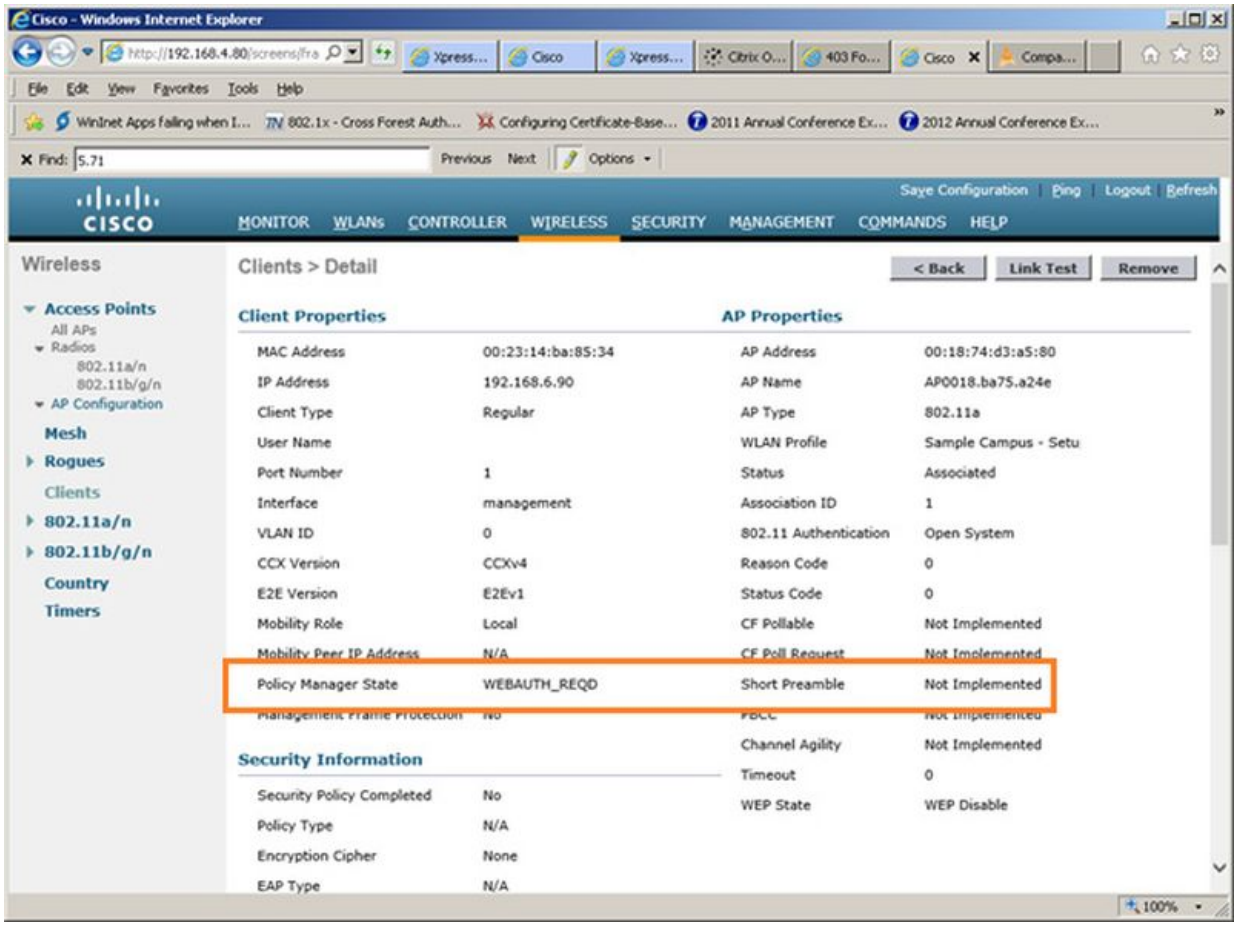
Verify Client State

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