Troubleshooting Web Authentication on a Wireless LAN Controller (WLC)

Document ID: 108501

Contents

Introduction

This document provides tips in order to troubleshoot web authentication issues in a Wireless LAN Controller (WLC) environment.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of Lightweight Access Point Protocol (LWAPP)/Control and Provisioning of Wireless Access Points (CAPWAP)
- Knowledge of configuring Lightweight Access Point (LAP) and WLC for basic operation.
- Basic knowledge of web authentication and configuring web authentication on WLCs. For information on configuring web authentication on WLCs, refer to Wireless LAN Controller Web Authentication Configuration Example.

Components Used

The information in this document is based on a WLC 5500 that runs firmware version 7.0.98.0.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This document can also be used with these hardwares:

- Cisco 5500 Series Wireless Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 4100 Series Wireless LAN Controllers
- Cisco 2500 Series Wireless Controllers

- Cisco 2100 Series Wireless LAN Controllers
- Cisco 2000 Series Wireless LAN Controllers
- Cisco Airespace 3500 Series WLAN Controller
- Cisco Airespace 4000 Series Wireless LAN Controller
- Cisco Wireless LAN Controller Module
- Cisco Catalyst 6500 Series Wireless Services Module (WiSM)
- Cisco Flex 7500 Series Wireless Controllers
- Cisco Wireless Services Module 2 (WiSM2)
- Cisco Catalyst 3750 Series Integrated Wireless LAN Controllers

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Web Authentication on WLCs

Web authentication is a Layer 3 security feature that causes the controller to not allow IP traffic, except DHCP−related packets/ DNS−related packets, from a particular client until that client has correctly supplied a valid username and password with an exception of traffic allowed through Pre−Auth ACL. Web authentication is the only security policy that allows the client to get an IP address before Authentication. It is a simple Authentication method without the need for a supplicant or client utility.Web authentication can be done either locally on a WLC or over a RADIUS server. Web authentication is typically used by customers who want to deploy a guest−access network.

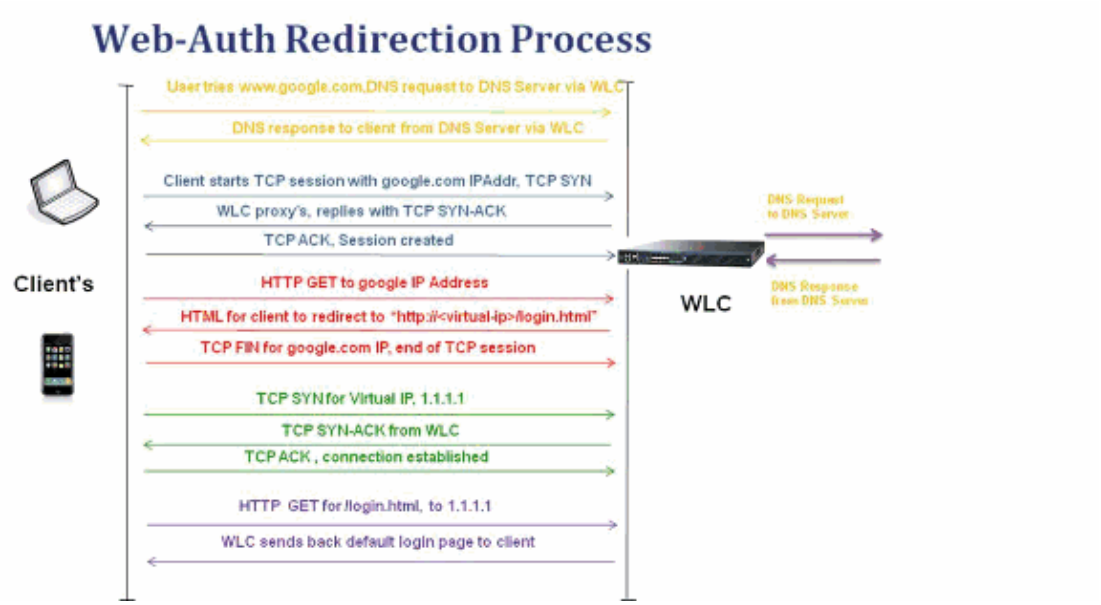
Web authentication starts when the controller intercepts the first TCP HTTP (port 80) GET packet from the client. In order for the client's web browser to get this far, the client must first obtain an IP address, and do a translation of the URL to IP address (DNS resolution) for the web browser. This lets the web browser know which IP address to send the HTTP GET.

When web authentication is configured on the WLAN, the controller blocks all traffic (until the authentication process is completed) from the client, except for DHCP and DNS traffic. When the client sends the first HTTP GET to TCP port 80, the controller redirects the client to https:1.1.1.1/login.html for processing. This process eventually brings up the login web page.

Note: When you use an external web server for web authentication, some of the WLC platforms need a pre−authentication ACL for the external web server, which includes the Cisco 5500 Series Controller, a Cisco 2100 Series Controller ,Cisco 2000 series and the controller network module. For the other WLC platforms the pre−authentication ACL is not mandatory.

Note: But, it is a good practice to configure a preauthentication ACL for the external web server when you use an external web authentication.

This section explains the Web authentication redirection process in detail.

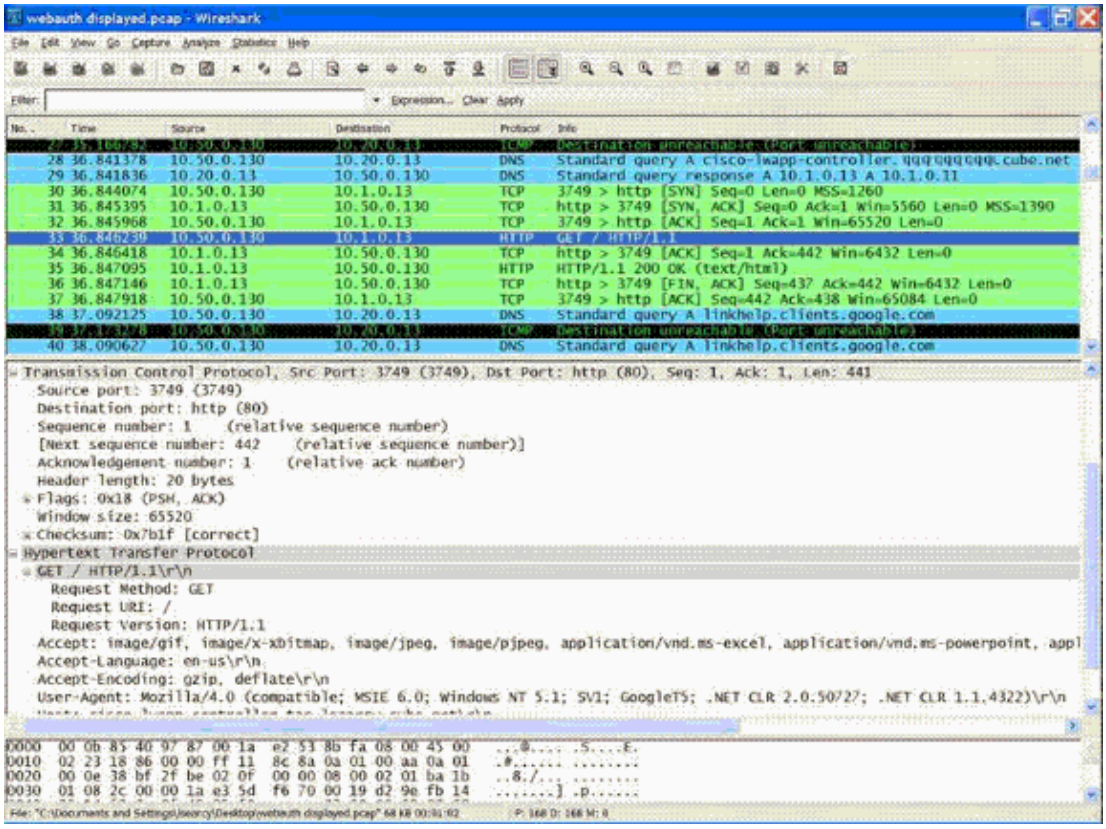


- You open the web browser and type in a URL, for example, `http://www.google.com`. The client sends out a DNS request for this URL to get the IP for the destination. WLC bypasses the DNS request to the DNS server and DNS server responds back with a DNS reply, which contains the IP address of the destination `www.google.com`,which in turn is forwarded to the wireless clients
- The client then tries to open a TCP connection with the destination IP address. It sends out a TCP SYN packet destined to the IP address of `www.google.com`.
- The WLC has rules configured for the client and hence can act as a proxy for `www.google.com`. It sends back a TCP SYN−ACK packet to the client with source as the IP address of `www.google.com`. The client sends back a TCP ACK packet in order to complete the three way TCP handshake and the TCP connection is fully established.
- The client sends an HTTP GET packet destined to `www.google.com`. The WLC intercepts this packet, sends it for redirection handling. The HTTP application gateway prepares a HTML body and sends it back as the reply to the HTTP GET requested by the client. This HTML makes the client to go to the default webpage URL of the WLC, for example, `http://<Virtual−Server−IP>/login.html`.
- Client closes the TCP connection with the IP address, for example `www.google.com`.
- Now the client wants to go to `http://1.1.1.1/login.html` and so it tries to open a TCP connection with the virtual IP address of the WLC. It sends a TCP SYN packet for 1.1.1.1 to the WLC.
- The WLC responds back with a TCP SYN−ACK and the client sends back a TCP ACK to the WLC in order to complete the handshake.
- Client sends a HTTP GET for /login.html destined to 1.1.1.1 in order to request for the login page.
- This request is allowed up to the Web Server of the WLC, and the server responds back with the default login page. The client receives the login page on the browser window where the user can go ahead and log in.

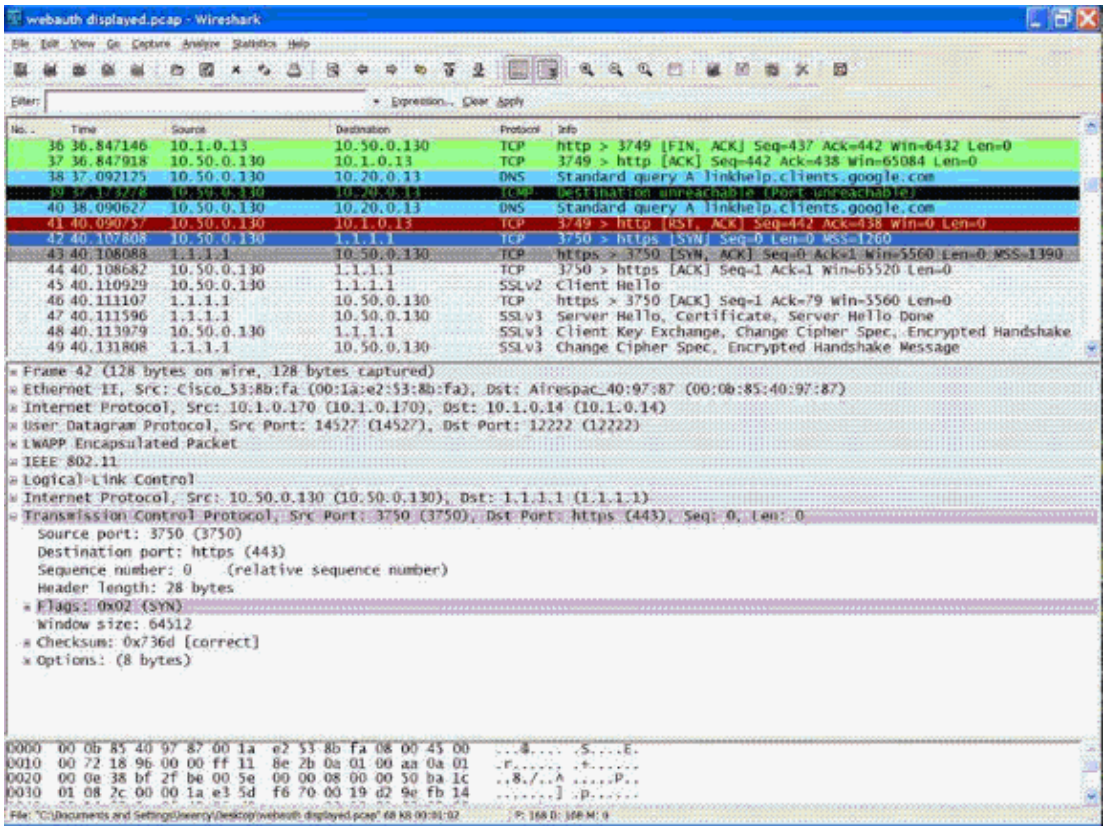
Here is an example. In this example, the client's IP address is 10.50.0.130. The client resolved the URL to the web server it was accessing 10.1.0.13. As you can see, the client did the three way handshake to start up the TCP connection and then sent an HTTP GET packet starting with packet 30. The controller is intercepting the packets and replying with code 200. The code 200 packet has a redirect URL in it:

```
<HTML><HEAD><TITLE>Cisco Systems Inc. Web Authentication Redirect</TITLE><META
http−equiv="Cache−control" content="no−cache"><META http−equiv="Pragma"
content="no−cache"><META http−equiv="Expires" content="−1"><META http−equiv="refresh"
content="1; URL=https://1.1.1.1/login.html?redirect=cisco−lwapp−controller.qqq.qqqqq.
cube.net/"></HEAD></HTML>
```

It then closes the TCP connection through the three way handshake.



The client then starts the HTTPS connection to the redirect URL which sends it to the 1.1.1.1, which is the virtual IP address of the controller. The client has to validate the server certificate or ignore it in order to bring up the SSL tunnel. In this case, it is a self−signed certificate so the client ignored it. The login web page is sent through this SSL tunnel. Packet 42 begins the transactions.



You have an option to configure the domain name for the virtual IP address of Wireless LAN Controller. If you configure the domain name for the virtual IP address, this domain name is returned in the HTTP OK packet from the controller in response to the HTTP GET packet from the client. You then have to perform a DNS resolution for this domain name and once it gets an IP address from the DNS resolution, it attempts to open a TCP session with that IP address, which is an IP configured on a virtual interface of the controller.

Eventually, the web page is passed through the tunnel to the client and the user sends back the username/password through the SSL tunnel.

Web authentication is performed by one of these three methods:

- Web authentication using an Internal web page (default).. Refer to Choosing the Default Web Authentication Login Page for more information on the use of the default web page.
- Web authentication using a Customized login page. Refer to Creating a Customized Web Authentication Login Page for more information on how to use the Customized login page.
- Web authentication using a login page from an external web server. Refer to Using a Customized Web Authentication Login Page from an External Web Server for more information on how to use a login page from an external web server.

Note: The customized web auth bundle has a limit of up to 30 characters for filenames. Ensure that no filenames within the bundle are greater than 30 characters.

Note: From WLC release 7.0 onwards, if Web Authentication is enabled on the WLAN and you also have CPU ACL rules, the client based Web−Authentication rules always take higher precedence as long as the client is unauthenticated in `WebAuth_Reqd` state. Once the client goes to the `RUN` state, CPU ACL rules get applied.

Note: Therefore If CPU ACLs are enabled in the WLC, an allow rule for the virtual interface IP is required (In ANY direction) in these conditions:

- When the CPU ACL does not have an allow ALL rule for both directions.
- When there exists an allow ALL rule, but there also exists a DENY rule for port 443 or 80 of higher precedence.

Note: The allow rule for the virtual IP should be for TCP protocol and port 80, if secureweb is disabled, or port 443, if secureweb is enabled. This is needed in order to allow the access of the client to the virtual interface IP address post successful authentication when CPU ACLs are in place.

Troubleshooting Web Authentication

After you configure web authentication, if the feature does not work as expected, complete these troubleshooting steps:

1. Check if the client gets an IP address. If not, users can uncheck **DHCP Required** on the WLAN and give the wireless client a static IP address. This assumes association with the access point. Refer to the *IP addressing issues* section of *Troubleshooting Client Issues in the Cisco Unified Wireless Network for troubleshooting DHCP related issues*.
2. On WLC versions earlier than 3.2.150.10, you must manually enter **https://1.1.1.1/login.html** in order to navigate to the web authentication window.

   The next step in the process is DNS resolution of the URL in the web browser. When a WLAN client connects to a WLAN configured for web authentication, the client obtains an IP address from the DHCP server. The user opens a web browser and enters a website address. The client then performs the DNS resolution to obtain the IP address of the website. Now, when the client tries to reach the website, the WLC intercepts the HTTP Get session of the client and redirects the user to the web authentication login page.
3. Therefore, ensure that the client is able to perform DNS resolution for the redirection to work. On Windows, choose **Start > Run**, enter **CMD** in order to open a command window, and do a nslookup www.cisco.com" and see if the IP address comes back.

   On Macs/Linux: open a terminal window and do a nslookup www.cisco.com" and see if the IP address comes back.

   If you believe the client is not getting DNS resolution, you can either:

   - Enter either the IP address of the URL (for example, http://www.cisco.com is http://198.133.219.25)
   - Try to directly reach the controller's webauth page with https://<Virtual_interface_IP_Address>/login.html. Typically this is http://1.1.1.1/login.html.

   Does entering this URL bring up the web page? If yes, it is most likely a DNS problem. It might also be a certificate problem. The controller, by default, uses a self−signed certificate and most web browsers warn against using them.
4. For web authentication using customized web page, ensure that the HTML code for the customized web page is appropriate.

   You can download a sample Web Authentication script from Cisco Software Downloads. For example, for the 4400 controllers, choose **Products > Wireless > Wireless LAN Controller > Standalone Controllers > Cisco 4400 Series Wireless LAN Controllers > Cisco 4404 Wireless LAN Controller > Software on Chassis > Wireless Lan Controller Web Authentication Bundle−1.0.1** and download the **webauth_bundle.zip** file.

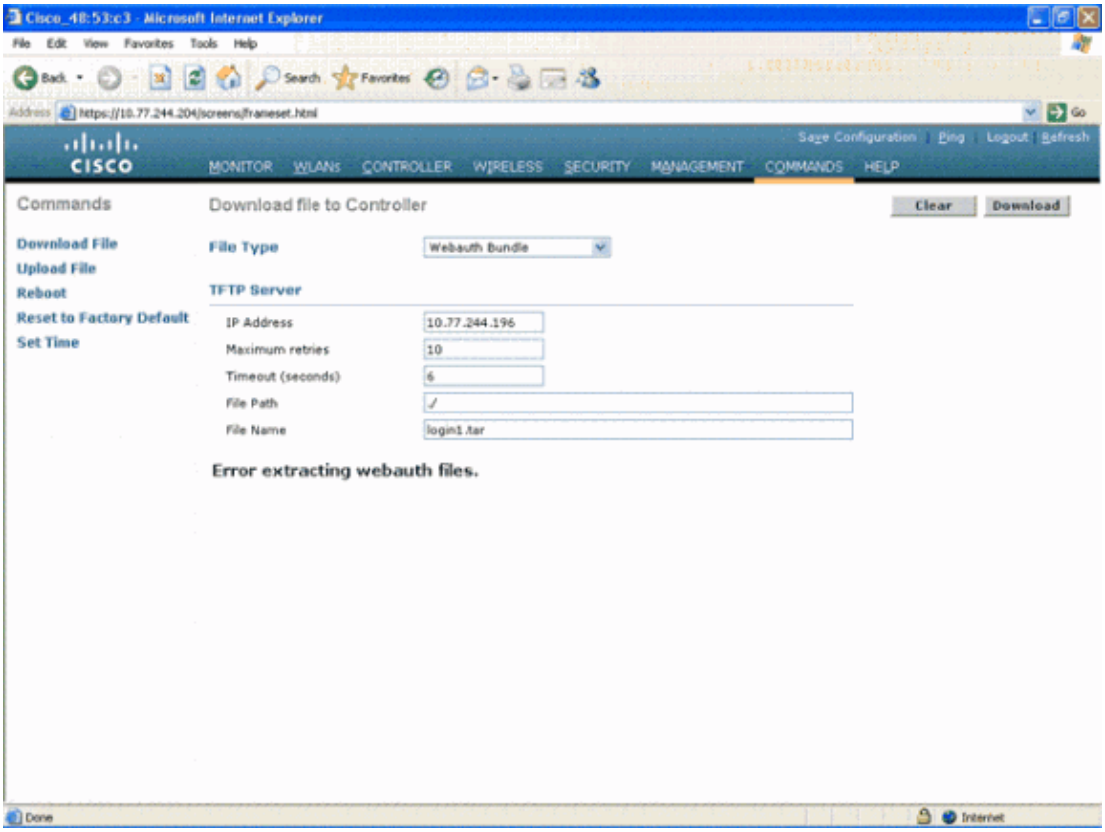
   These parameters are added to the URL when the user's Internet browser is redirected to the customized login page:

- ap_mac The MAC address of the access point to which the wireless user is associated.
- switch_url The URL of the controller to which the user credentials should be posted.
- redirect The URL to which the user is redirected after authentication is successful.
- statusCode The status code returned from the controller's web authentication server.
- wlan The WLAN SSID to which the wireless user is associated.

These are the available status codes:

- Status Code 1: "You are already logged in. No further action is required on your part."
- Status Code 2: "You are not configured to authenticate against web portal. No further action is required on your part."
- Status Code 3: "The username specified cannot be used at this time. Perhaps the username is already logged into the system?"
- Status Code 4: "You have been excluded."
- Status Code 5: "The User Name and Password combination you have entered is invalid. Please try again."

5. All the files and pictures that need to appear on the Customized web page should be bundled into a .tar file before uploading to the WLC. Ensure that one of the files included in the tar bundle is login.html. You receive this error message if you do not include the login.html file:



Refer to the Guidelines for Customized Web Authentication section of Wireless LAN Controller Web Authentication Configuration Example for more information on how to create a customized web authentication window.

Note: Files that are large and files that have long names will result in an extraction error. It is recommended that pictures are in .jpg format.

6. Internet Explorer 6.0 SP1 or later is the browser recommended for the use of web authentication. Other browsers may or may not work.
7. Ensure that the **Scripting** option is not blocked on the client browser as the customized web page on the WLC is basically an HTML script. On IE 6.0, this is disabled by default for security purposes.

Note: The Pop Up blocker needs to be disabled on the browser if you have configured any Pop Up messages for the user.

Note: If you browse to an **https** site, redirection does not work. Refer to Cisco bug ID CSCar04580 (registered customers only) for more information.

8. If you have a **host name** configured for the **virtual interface** of the WLC, make sure that the DNS resolution is available for the host name of the virtual interface.

   Note: Navigate to the **Controller > Interfaces** menu from the WLC GUI in order to assign a **DNS hostname** to the virtual interface.
9. Sometimes the firewall installed on the client computer blocks the web authentication login page. Disable the firewall before you try to access the login page. The firewall can be enabled again once the web authentication is completed.
10. Topology/solution firewall can be placed between the client and web−auth server, which depends on the network. As for each network design/solution implemented, the end user should make sure these ports are allowed on the network firewall.

Protocol	Port
HTTP/HTTPS Traffic	TCP port 80/443
CAPWAP Data/Control Traffic	UDP port 5247/5246
LWAPP Data/Control Traffic (before rel 5.0)	UDP port 12222/12223
EOIP packets	IP protocol 97
Mobility	UDP port 16666 (non secured) UDP port 16667 (secured IPSEC tunnel)

11. For web authentication to occur, the client should first associate to the appropriate WLAN on the WLC. Navigate to the **Monitor > Clients** menu on the WLC GUI in order to see if the client is associated to the WLC. Check if the client has a valid IP address.
12. Disable the Proxy Settings on the client browser until web authentication is completed.
13. The default web authentication method is PAP. Ensure that PAP authentication is allowed on the RADIUS server for this to work. In order to check the status of client authentication, check the debugs and log messages from the RADIUS server. You can use the **debug aaa all** command on the WLC to view the debugs from the RADIUS server.
14. Update the hardware driver on the computer to the latest code from manufacturer's website.
15. Verify settings in the supplicant (program on laptop).
16. When you use the Windows Zero Config supplicant built into Windows:

    - Verify user has latest patches installed.
    - Run debugs on supplicant.
17. On the client, turn on the EAPOL (WPA+WPA2) and RASTLS logs from a command window, Start > Run > CMD:

    ```
    netsh ras set tracing eapol enable
          netsh ras set tracing rastls enable
    ```

    In order to disable the logs, run the same command but replace enable with disable. For XP, all logs will be located in C:\Windows\tracing.
18. If you still have no login web page, collect and analyze this output from a single client:

    ```
    debug client <mac_address in format xx:xx:xx:xx:xx:xx>
    debug dhcp message enable
    ```

```
debug aaa all enable
debug dot1x aaa enable
debug mobility handoff enable
```

19. If the issue is not resolved after you complete these steps, collect these debugs and use the TAC Service Request Tool (registered customers only) in order to open a Service Request.

```
debug pm ssh-appgw enable
debug pm ssh-tcp enable
debug pm rules enable
debug emweb server enable
debug pm ssh-engine enable packet <client ip>
```

Related Information

- **Wireless LAN Controller Web Authentication Configuration Example**
- **External Web Authentication with Wireless LAN Controllers Configuration Example**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jul 26, 2011 Document ID: 108501