

Troubleshooting Web Authentication on a Wireless LAN Controller (WLC)

Document ID: 108501

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Web Authentication on WLCs

Troubleshooting Web Authentication

Related Information

Introduction

This document provides tips 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)
- 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 4400 that runs firmware version 5.1.

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 2000 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 4100 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/7600 Series Wireless Services

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 designed for guest access. It does not allow the client to browse until that client has correctly supplied a valid username and password. When you use web authentication to authenticate clients, you must define a username and password for each client. Then, when the clients attempt to join the wireless LAN, users must enter the username and password when prompted by a login page.

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.

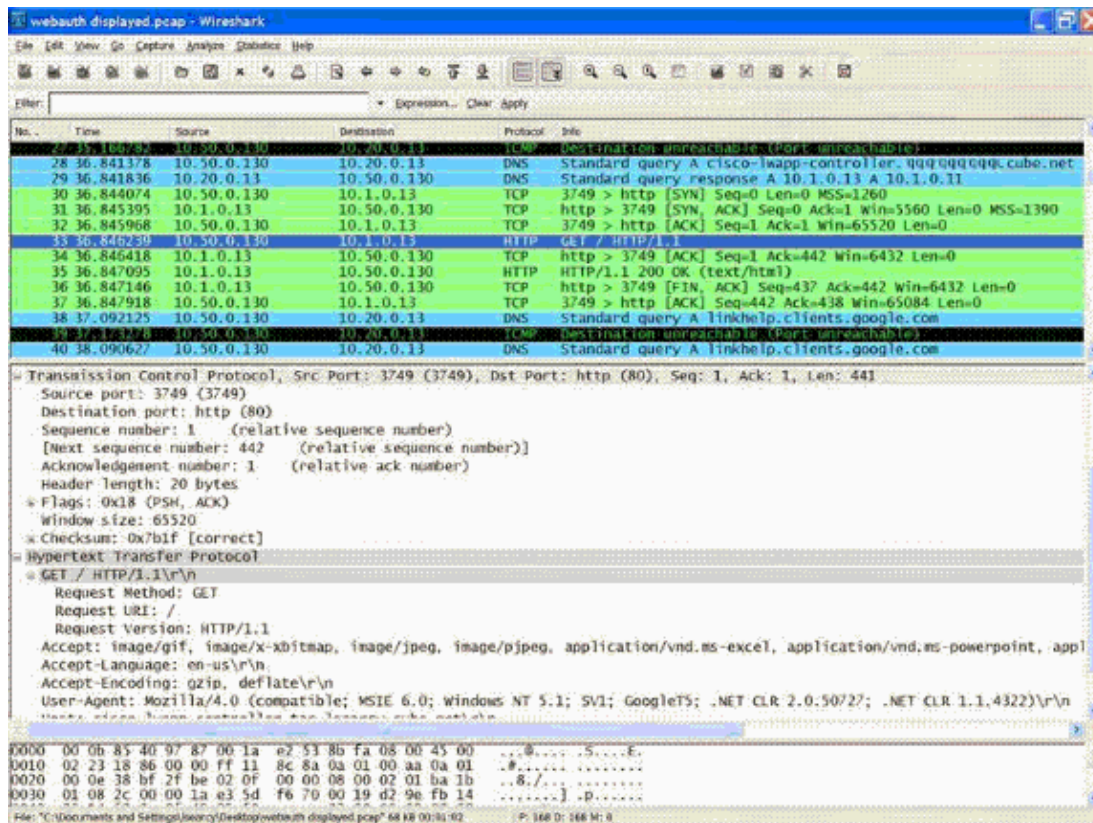
When web authentication is configured on the WLAN, the controller blocks all traffic (until the authentication process is completed) from the client, except for DHCP and DNS traffic. When the client sends the first HTTP GET to TCP port 80, the controller redirects the client to <https://1.1.1.1/login.html>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

Note: For 2000 Series WLCs, you need to configure a preauthentication ACL on the WLAN to allow wireless clients to be redirected to the external web server login URL (for external web authentication). This ACL should be set as the WLAN preauthentication ACL under Web Policy.

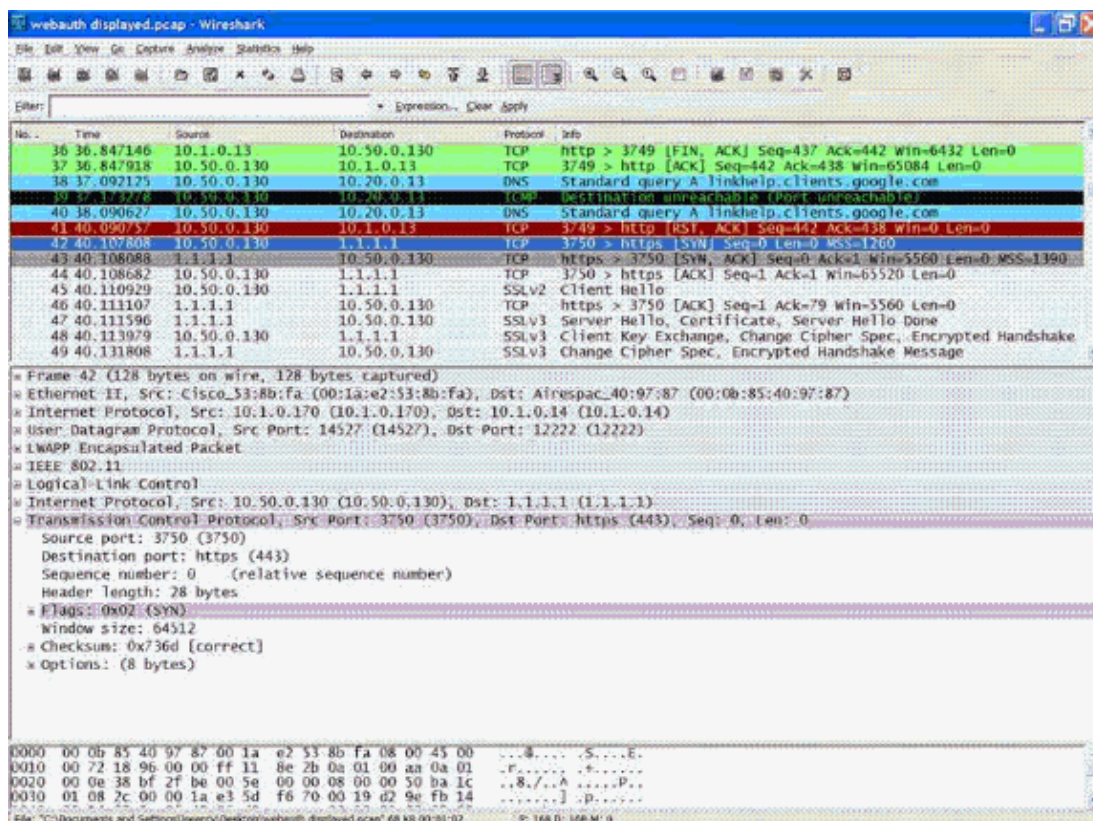
Here is an example. In this example, the client's IP address is 10.50.0.130. The client resolved the URL to the web server it was accessing 10.1.0.13. As you can see, the client did the three way handshake to start up the TCP connection and then sent an HTTP GET packet starting with packet 30. The controller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



The client then starts the HTTPS connection to the redirect URL which sends it to the 1.1.1.1 (the controller's virtual IP address). The client has to validate the server certificate or ignore it 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.



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

Web authentication is performed by one of these three methods:

- Web authentication using an Inbuilt web page (default). For information on using the default web page, refer to *Choosing the Default Web Authentication Login Page*.
- Web authentication using a Customized login page. For information on using the Customized login page, refer to *Creating a Customized Web Authentication Login Page*.
- Web authentication using a login page from an external web server. For information on using a login page from an external web server, refer to *Using a Customized Web Authentication Login Page from an External Web Server*.

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: open a command window (start->run, enter CMD) 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 `https://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.

Here is a sample `web_authentication.tar` script that can be used for web authentication.

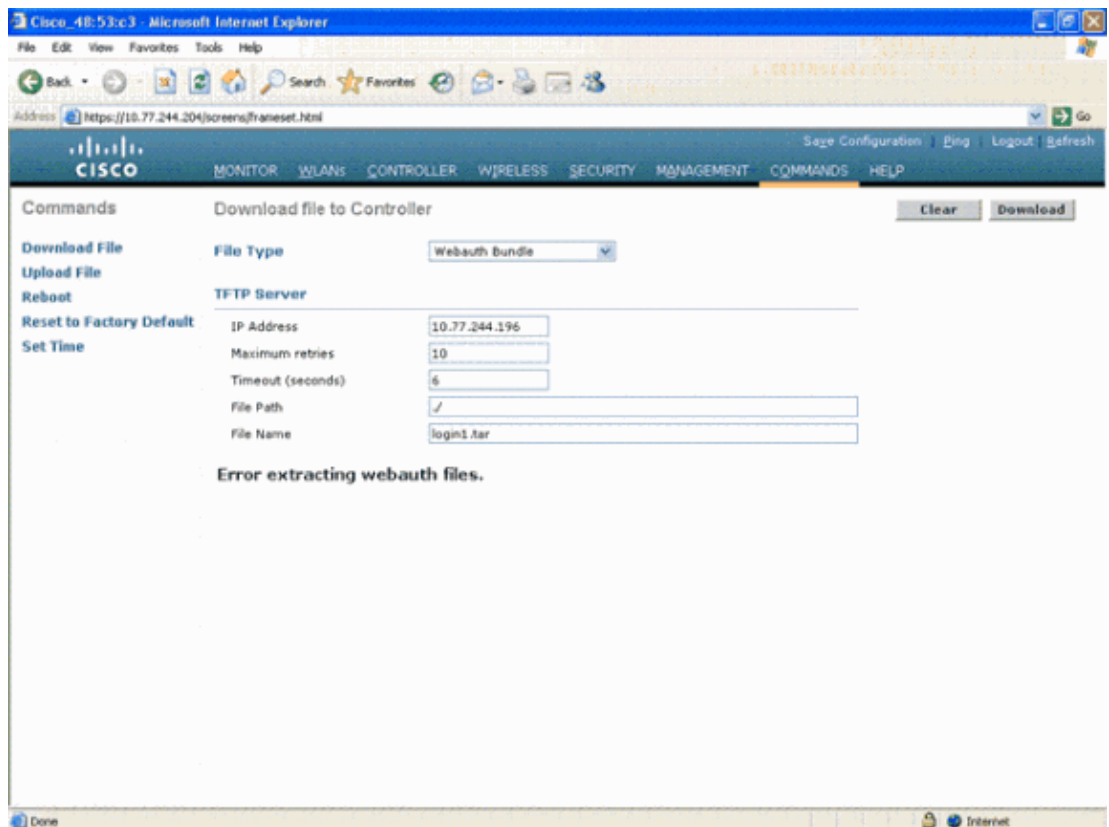
These parameters are added to the URL when the user's Internet browser is redirected to the

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:



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

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. 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. For more information, refer to Cisco bug ID CSCar04580 (registered customers only) .

7. 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.

8. 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.
9. 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.
10. Disable the Proxy Settings on the client browser until web authentication is completed.
11. 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.
12. Update the hardware driver on the computer to the latest code from manufacturer's website.
13. Verify settings in the supplicant (program on laptop).
14. When using the Windows Zero Config supplicant built into Windows:

- ◆ Verify user has latest patches installed.
- ◆ Run debugs on supplicant.

15. 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.

16. 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
debug pm ssh-appgw enable
debug pm ssh-tcp enable
```

Related Information

- [Wireless LAN Controller Web Authentication Configuration Example](#)
 - [External Web Authentication with Wireless LAN Controllers Configuration Example](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

