Troubleshoot Web Authentication on a Wireless LAN Controller (WLC)

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products

Web Authentication on WLCs

Troubleshoot Web Authentication

Related Information

Introduction

This document describes 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:

- Control and Provisioning of Wireless Access Points (CAPWAP).
- How to configure Lightweight Access Point (LAP) and WLC for basic operation.
- Basic knowledge of web authentication and how to configure web authentication on WLCs.

For information on how to configure 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 8.3.121.

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, ensure that you understand the potential impact of any command.

Related Products

This document can also be used with this hardware:

- Cisco 5500 Series Wireless Controllers

- Cisco 8500 Series Wireless Controllers
- Cisco 2500 Series Wireless Controllers
- Cisco Airespace 3500 Series WLAN Controller
- Cisco Airespace 4000 Series Wireless LAN Controller
- Cisco Flex 7500 Series Wireless Controllers
- Cisco Wireless Services Module 2 (WiSM2)

Web Authentication on WLCs

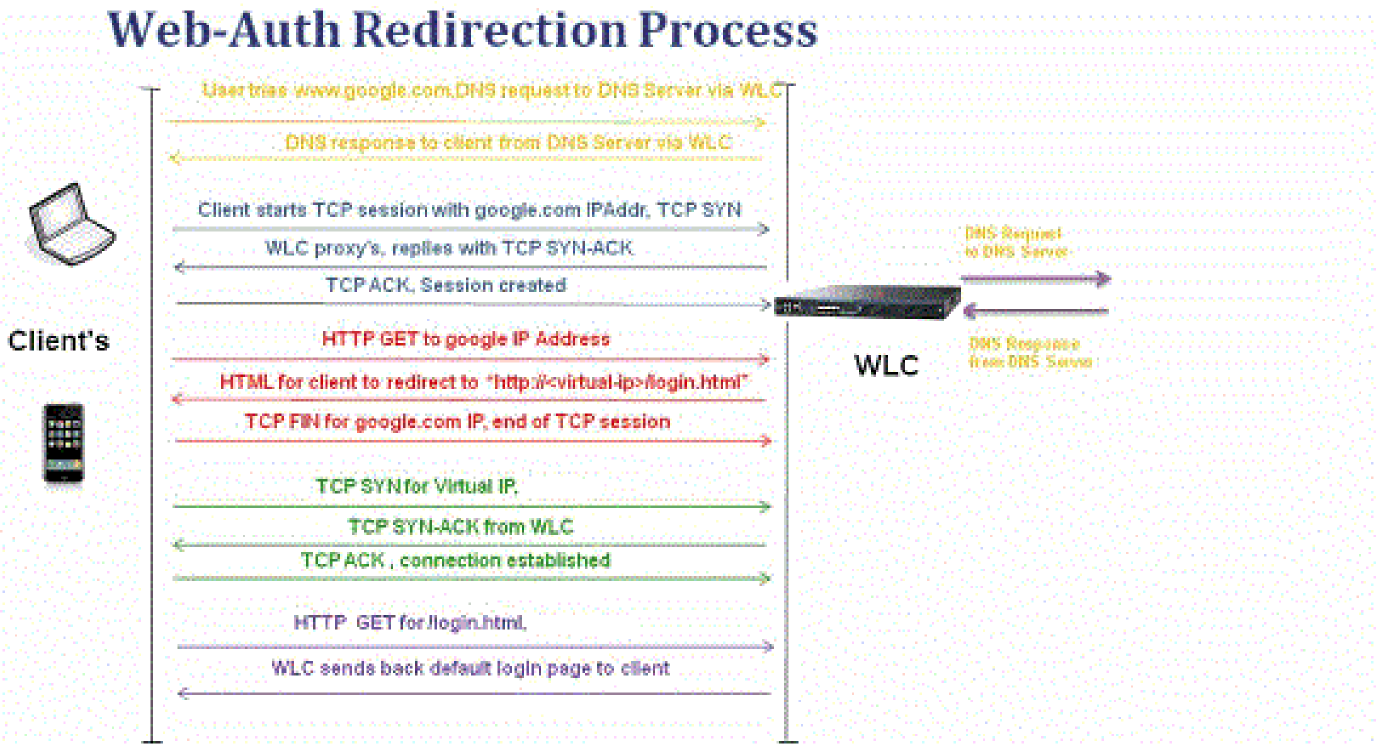
Web authentication is a Layer 3 security feature that causes the controller to not allow IP traffic, except DHCP-related packets/ Domain Name System (DNS)-related packets, from a particular client until that client has correctly supplied a valid username and password with an exception of traffic allowed through a pre-auth access control list (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 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://192.0.2.1/login.html (if this is the virtual IP that is configured) for processing. This process eventually brings up the login web page.

Note: When you use an external web server for web authentication, WLC platforms need a pre-authentication ACL for the external web server.

This section explains the Web authentication redirection process in detail.


Web-Auth Redirection Process
User tries www.google.com,DNS request to DNS Server via WLC
DNS response to client from DNS Server via WLC
Client starts TCP session with google.com IPAddr, TCP SYN
WLC proxy's, replies with TCP SYN-ACK
TCP ACK, Session created
HTTP GET to google IP Address
HTML for client to redirect to "http://<virtual-ip>/login.html"
TCP FIN for google.com IP, end of TCP session
TCP SYN for Virtual IP.
TCP SYN-ACK from WLC
TCP ACK , connection established
HTTP GET for /login.html.
WLC sends back default login page to client
Client's
WLC
DNS Request to DNS Server
DNS Response from DNS Server

- You open the web browser and type in a URL, for example, http://www.example.com. The client sends out a DNS request for this URL to get the IP for the destination. WLC passes 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.example.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.example.com.

- The WLC has rules configured for the client and hence can act as a proxy for www.example.com. It sends back a TCP SYN-ACK packet to the client with source as the IP address of www.example.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.example.com. The WLC intercepts this packet and 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 go to the default webpage URL of the WLC, for example, http://<Virtual-Server-IP>/login.html.

- The client closes the TCP connection with the IP address, for example www.example.com.

- Now the client wants to go to http://<virtualip>/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 192.0.2.1 (which is our virtual IP here) 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.

- The client sends an HTTP GET for /login.html destined to 192.0.2.1 in order to request the login page.

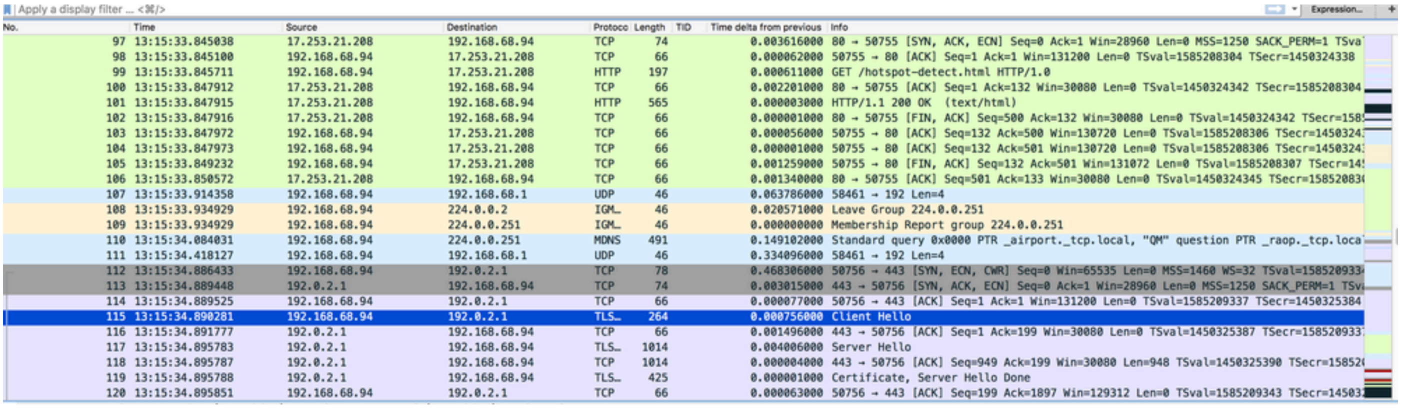
- This request is allowed up to the web server of the WLC and the server responds back with the default login page. The client receives the login page on the browser window where the user can go ahead and login.

In this example, the client IP address is 192.168.68.94. The client resolved the URL to the web server that it accessed, 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 that started with packet 96 (00 is the HTTP packet). This was not triggered by the user, but was the operating system automated portal detection triggers (as we can guess from the requested URL). The controller intercepts the packets and replies with code 200. The code 200 packet has a redirect URL in it:

```
<HTML><HEAD>
<TITLE> 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://192.0.2.1/login.html?redirect=http://captive.ap
</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 192.0.2.1, 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 112 begins the transactions.



No.	Time	Source	Destination	Protoco	Length	TID	Time delta from previous	Info
97	13:15:33.845038	17.253.21.208	192.168.68.94	TCP	74		0.003616000	80 → 50755 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1250 SACK_PERM=1 TSva
98	13:15:33.845100	192.168.68.94	17.253.21.208	TCP	66		0.000062000	50755 → 80 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=1585208304 TSecr=1450324338
99	13:15:33.845711	192.168.68.94	17.253.21.208	HTTP	197		0.000611000	GET /hotspot-detect.html HTTP/1.0
100	13:15:33.847912	17.253.21.208	192.168.68.94	TCP	66		0.002201000	80 → 50755 [ACK] Seq=1 Ack=132 Win=30080 Len=0 TSval=1450324342 TSecr=1585208304
101	13:15:33.847915	17.253.21.208	192.168.68.94	HTTP	565		0.000003000	HTTP/1.1 200 OK (text/html)
102	13:15:33.847916	17.253.21.208	192.168.68.94	TCP	66		0.000001000	80 → 50755 [FIN, ACK] Seq=500 Ack=132 Win=30080 Len=0 TSval=1450324342 TSecr=158
103	13:15:33.847972	192.168.68.94	17.253.21.208	TCP	66		0.000056000	50755 → 80 [ACK] Seq=132 Ack=500 Win=130720 Len=0 TSval=1585208306 TSecr=1450324
104	13:15:33.847973	192.168.68.94	17.253.21.208	TCP	66		0.000001000	50755 → 80 [ACK] Seq=132 Ack=501 Win=130720 Len=0 TSval=1585208306 TSecr=1450324
105	13:15:33.849232	192.168.68.94	17.253.21.208	TCP	66		0.001259000	50755 → 80 [FIN, ACK] Seq=132 Ack=501 Win=131072 Len=0 TSval=1585208307 TSecr=14
106	13:15:33.850572	17.253.21.208	192.168.68.94	TCP	66		0.001340000	80 → 50755 [ACK] Seq=501 Ack=133 Win=30080 Len=0 TSval=1450324345 TSecr=15852083
107	13:15:33.914358	192.168.68.94	192.168.68.1	UDP	46		0.063786000	58461 → 192 Len=4
108	13:15:33.934929	192.168.68.94	224.0.0.2	IGM…	46		0.020571000	Leave Group 224.0.0.251
109	13:15:33.934929	192.168.68.94	224.0.0.251	IGM…	46		0.000000000	Membership Report group 224.0.0.251
110	13:15:34.084031	192.168.68.94	224.0.0.251	MDNS	491		0.149102000	Standard query 0x0000 PTR _airport._tcp.local, "QM" question PTR _raop._tcp.loca
111	13:15:34.418127	192.168.68.94	192.168.68.1	UDP	46		0.334096000	58461 → 192 Len=4
112	13:15:34.886433	192.168.68.94	192.0.2.1	TCP	78		0.468306000	50756 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=158520933
113	13:15:34.889448	192.0.2.1	192.168.68.94	TCP	74		0.003015000	443 → 50756 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1250 SACK_PERM=1 TSv
114	13:15:34.889525	192.168.68.94	192.0.2.1	TCP	66		0.000077000	50756 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=1585209337 TSecr=1450325384
115	13:15:34.890281	192.168.68.94	192.0.2.1	TLS…	264		0.000756000	Client Hello
116	13:15:34.891777	192.0.2.1	192.168.68.94	TCP	66		0.001496000	443 → 50756 [ACK] Seq=1 Ack=199 Win=30080 Len=0 TSval=1450325387 TSecr=15852093
117	13:15:34.895783	192.0.2.1	192.168.68.94	TLS…	1014		0.004006000	Server Hello
118	13:15:34.895787	192.0.2.1	192.168.68.94	TCP	1014		0.000004000	443 → 50756 [ACK] Seq=949 Ack=199 Win=30080 Len=948 TSval=1450325390 TSecr=15852
119	13:15:34.895788	192.0.2.1	192.168.68.94	TLS…	425		0.000001000	Certificate, Server Hello Done
120	13:15:34.895851	192.168.68.94	192.0.2.1	TCP	66		0.000063000	50756 → 443 [ACK] Seq=199 Ack=1897 Win=129312 Len=0 TSval=1585209343 TSecr=14503

You have the option to configure the domain name for the virtual IP address of the WLC. 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. 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 address 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 Secure Sockets Layer (SSL) tunnel.

Web authentication is performed by one of these three methods:

- Use an Internal web page (default).
- Use a customized login page.
- Use a login page from an external web server.

Notes:

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

- 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 the WebAuth_Reqd state. Once the client goes to the RUN state, CPU ACL rules get applied.

- 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.

- The allow rule for the virtual IP must 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.

Troubleshoot Web Authentication

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

1. Check if the client gets an IP address. If not, users can uncheck the **DHCP Required** check box on the WLAN and give the wireless client a static IP address. This assumes association with the access point.
2. 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. In Microsoft 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.

   In 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 does not get DNS resolution, you can either:

   - Enter either the IP address of the URL (for example, http://www.cisco.com is http://192.168.219.25).
   - Try to type any (even non-existing) IP address that must resolve through the wireless adapter.

   When you enter this URL, does it bring up the web page? If yes, it is most likely a DNS problem. It can also be a certificate problem. The controller, by default, uses a self-signed certificate and most web browsers warn against their use.

4. For web authentication with a 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 5508 controllers, choose **Products** > **Wireless** > **Wireless LAN Controller** >

Standalone Controllers > Cisco 5500 Series Wireless LAN Controllers > Cisco 5508 Wireless LAN Controller > Software on Chassis > Wireless Lan Controller Web Authentication Bundle and download the **webauth_bundle.zip** file.

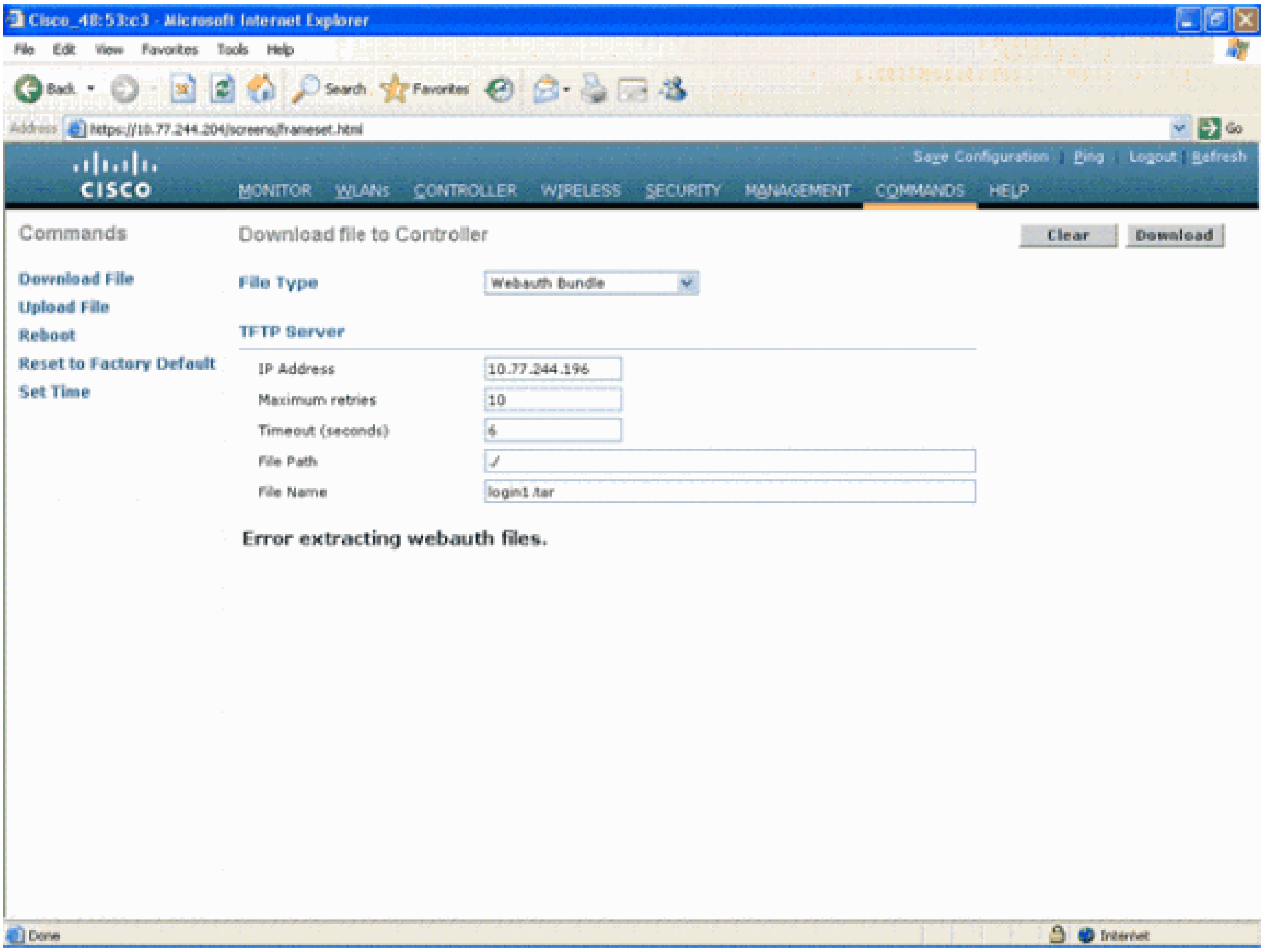
These parameters are added to the URL when the Internet browser of the user is redirected to the customized login page:

- 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 must be posted.
- redirect - The URL to which the user is redirected after authentication is successful.
- statusCode - The status code returned from the controller 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 must be bundled into a .tar file before it is uploaded 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:


Cisco_48:53:c3 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.77.244.204/screens/frameset.html
Go
CISCO
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Commands
Download File
Upload File
Reboot
Reset to Factory Default
Set Time
Clear
Download
Done
Internet

Download file to Controller

File Type: Webauth Bundle

TFTP Server

IP Address: 10.77.244.196

Maximum retries: 10

Timeout (seconds): 6

File Path: ./

File Name: login1.tar

Error extracting webauth files.

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 can 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.
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. The topology/solution firewall can be placed between the client and the web-auth server, which depends on the network. As for each network design/solution implemented, the end user must 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)

10. For web authentication to occur, the client must 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.
11. Disable the proxy settings on the client browser until web authentication is completed.
12. The default web authentication method is Password Authentication Protocol (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 in order to view the debugs from the RADIUS server.
13. Update the hardware driver on the computer to the latest code from website of the manufacturer.
14. Verify settings in the supplicant (program on laptop).
15. When you use the Windows Zero Config supplicant built into Windows:
    - Verify the user has the latest patches installed.
    - Run debugs on the supplicant.
16. On the client, turn on the EAPOL (WPA+WPA2) and RASTLS logs from a command window. Choose **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 can be located in C:\Windows\tracing.

17. 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
```

18. If the issue is not resolved after you complete these steps, collect these debugs and use Support Case Manager 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**
- **Cisco Technical Support & Downloads**