

對無線LAN控制器(WLC)上的Web驗證進行排解疑難

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[相關產品](#)

[WLC上的Web驗證](#)

[Web驗證疑難排解](#)

[相關資訊](#)

簡介

本文說明在無線LAN控制器(WLC)環境中排除Web驗證問題的秘訣。

必要條件

需求

思科建議您瞭解以下主題：

- 無線存取點(CAPWAP)的控制和布建。
- 如何設定輕型存取點(LAP)和WLC以達成基本操作。
- Web驗證的基本知識以及如何在WLC上設定Web驗證。

有關如何在WLC上設定Web驗證的資訊，請參閱[無線LAN控制器Web驗證組態範例](#)。

採用元件

本檔案中的資訊是根據執行韌體版本8.3.121的WLC 5500。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

相關產品

本檔案也適用於以下硬體：

- Cisco 5500 系列無線控制器
- Cisco 8500 系列無線控制器
- Cisco 2500 系列無線控制器
- Cisco Aireospace 3500系列WLAN控制器
- Cisco Aireospace 4000系列無線LAN控制器

- Cisco Flex 7500系列無線控制器
- 思科無線服務模組2(WISM2)

WLC上的Web驗證

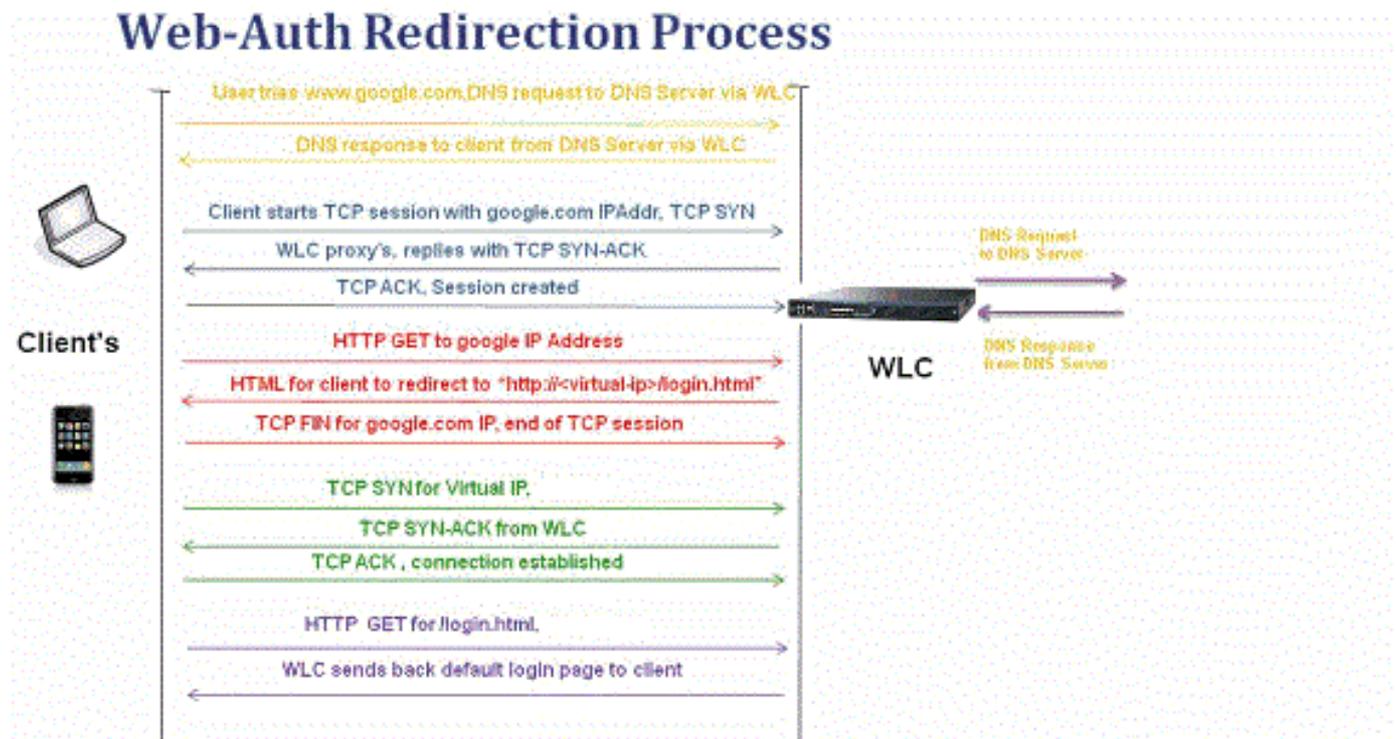
Web驗證是第3層安全功能，會導致控制器不允許來自特定使用者端的IP流量(DHCP相關封包/網域名稱系統(DNS)相關封包除外)，除非該使用者端正確提供有效的使用者名稱和密碼(透過預先驗證存取控制清單(ACL)允許的流量除外)。Web驗證是唯一允許客戶端在驗證之前獲取IP地址的安全策略。這是一種簡單的身份驗證方法，不需要請求方或客戶端實用程式。Web驗證可在WLC本機上或透過RADIUS伺服器執行。Web驗證通常由想要部署訪客存取網路的客戶使用。

當控制器從使用者端擷取第一個TCP HTTP (連線埠80) GET封包時，Web驗證就會啟動。為了讓使用者端Web瀏覽器達到此目的，使用者端必須首先取得IP位址，然後對Web瀏覽器執行URL到IP位址 (DNS解析) 的轉譯。這樣可讓Web瀏覽器知道要傳送HTTP GET的IP地址。

在WLAN上設定Web驗證時，控制器會封鎖來自使用者端的所有流量 (直到驗證程式完成)，DHCP和DNS流量除外。當使用者端將第一個HTTP GET傳送到TCP連線埠80時，控制器會將使用者端重新導向到<https://192.0.2.1/login.html> (如果這是已設定的虛擬IP) 以進行處理。此程式最終會啟動登入網頁。

注意：使用外部Web伺服器進行Web驗證時，WLC平台需要外部Web伺服器的預先驗證ACL。

本節詳細介紹Web驗證重新導向程式。



- 開啟Web瀏覽器並鍵入URL，例如http://www.site.com。使用者端會傳送對此URL的DNS要求，以取得目的地的IP。WLC將DNS請求傳遞到DNS伺服器，DNS伺服器使用DNS回覆進行響應，其中包含目標www.site.com的IP地址，然後將該地址轉發到無線客戶端。
- 然後使用者端嘗試開啟具有目的地IP位址的TCP連線。它發出一個目的地為www.site.com的

IP地址的TCP SYN資料包。

- WLC有為使用者端設定的規則，因此可以作為www.site.com的代理。它將TCP SYN-ACK資料包發回給客戶端，源地址為www.site.com。客戶端發回TCP ACK資料包以完成三向TCP握手，並且TCP連線已完全建立。
- 使用者端將目的地為www.site.com的HTTP GET封包傳送。WLC會攔截此封包並將其傳送以進行重新導向處理。HTTP應用網關準備一個HTML正文，並將其作為客戶端請求的HTTP GET的回覆傳送回來。此HTML讓使用者端前往WLC的預設網頁URL，例如<http://<Virtual-Server-IP>/login.html>。
- 使用者端會關閉具有IP位址的TCP連線，例如www.site.com。
- 現在，使用者端想要前往<http://<virtualip>/login.html>，因此嘗試使用WLC的虛擬IP位址開啟TCP連線。它會將192.0.2.1 (此處的虛擬IP)的TCP SYN封包傳送到WLC。
- WLC會使用TCP SYN-ACK作出回應，而使用者端會將TCP ACK傳送回WLC以完成握手。
- 使用者端向/login.html傳送一個目的地為192.0.2.1的HTTP GET以要求登入頁面。
- 此要求允許傳至WLC的Web伺服器，且伺服器使用預設登入頁面做出回應。使用者端會收到瀏覽器視窗上的登入頁面，使用者可以在該頁面中繼續登入。

在本例中，客戶端IP地址為192.168.68.94。客戶端解析了它訪問的Web伺服器10.1.0.13的URL。您可以看到，客戶端通過三次握手來啟動TCP連線，然後傳送一個以資料包96開始的HTTP GET資料包(00是HTTP資料包)。這不是由使用者觸發，而是作業系統自動觸發門戶檢測(我們可以從請求的URL猜測)。控制器會攔截封包並以代碼200回覆。代碼200封包中包含重新導向URL:

```
<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.apple.com/hotspot-detect.html">
</HEAD></HTML>
```

然後透過三次交握關閉TCP連線。

然後使用者端啟動與重新導向URL的HTTPS連線，重新導向URL會將其傳送到192.0.2.1(控制器的虛擬IP位址)。使用者端必須驗證伺服器憑證或將其忽略，才能啟動SSL通道。在這種情況下，這是自簽名的證書，因此客戶端忽略了它。登入網頁透過此SSL通道傳送。資料包112開始事務。

No.	Time	Source	Destination	Protocol	Length	TID	Time delta from previous	Info
97	13:15:33.045038	17.253.21.208	192.168.68.94	TCP	74		0.0033616000	80 -> 50755 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1250 SACK_PERM=1 TSval=
98	13:15:33.045100	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	13:15:33.045711	192.168.68.94	17.253.21.208	HTTP	197		0.000611000	GET /hotspot-detect.html HTTP/1.0
100	13:15:33.047912	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	13:15:33.047915	17.253.21.208	192.168.68.94	HTTP	565		0.000003000	HTTP/1.1 200 OK (text/html)
102	13:15:33.047916	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=1585208304
103	13:15:33.047972	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=1450324338
104	13:15:33.047973	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=1450324338
105	13:15:33.049232	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=1450324338
106	13:15:33.050572	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=1585208304
107	13:15:33.014358	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	IGMP	46		0.020571000	Leave group 224.0.0.251
109	13:15:33.934929	192.168.68.94	224.0.0.251	IGMP	46		0.000000000	Membership Report group 224.0.0.251
110	13:15:34.004031	192.168.68.94	224.0.0.251	MDNS	491		0.149102000	Standard query 0x0000 PTR _airport._tcp.local, "QM" question PTR _raop._tcp.local
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, CWI] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=1585209337 TSecr=1450325384
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 TSval=
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=1585209337
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=1585209337
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=1450325384

您可以選擇為WLC的虛擬IP地址配置域名。如果為虛擬IP地址配置域名，則此域名會從控制器返回到HTTP OK資料包中，以響應來自客戶端的HTTP GET資料包。然後，您必須對此域名執行DNS解析。從DNS解析獲取IP地址後，它會嘗試開啟具有該IP地址的TCP會話，該IP地址是在控制器的虛擬介面上配置的IP地址。

最終，網頁會透過通道到達使用者端，而使用者會透過安全通訊端層(SSL)通道傳回使用者名稱/密

碼。

Web驗證使用以下三種方法之一執行：

- 使用內部網頁（預設）。
- 使用自訂登入頁面。
- 使用外部Web伺服器中的登入頁面。

附註：

— 自訂Web驗證套件組合中檔案名稱不得超過30個字元。請確保套件組合中的檔案名稱不超過30個字元。

— 從WLC 7.0版開始，如果在WLAN上啟用Web驗證，且您也有CPU ACL規則，則只要使用者端在WebAuth_Reqd狀態下未進行驗證，以使用者端為基礎的Web驗證規則便一律優先使用。一旦客戶端進入RUN狀態，就會應用CPU ACL規則。

— 因此，如果在WLC中啟用了CPU ACL，則在以下情況下需要虛擬介面IP的allow規則（在ANY方向）：

- 當CPU ACL沒有兩個方向的allow ALL規則。
- 如果存在allow ALL規則，但埠443或80也存在較高優先順序的DENY規則。

— 如果禁用secureweb，則虛擬IP的允許規則必須為TCP協定和埠80，如果啟用secureweb，則必須為埠443。當CPU ACL就位時，要允許客戶端在成功身份驗證後訪問虛擬介面IP地址，需要執行此操作。

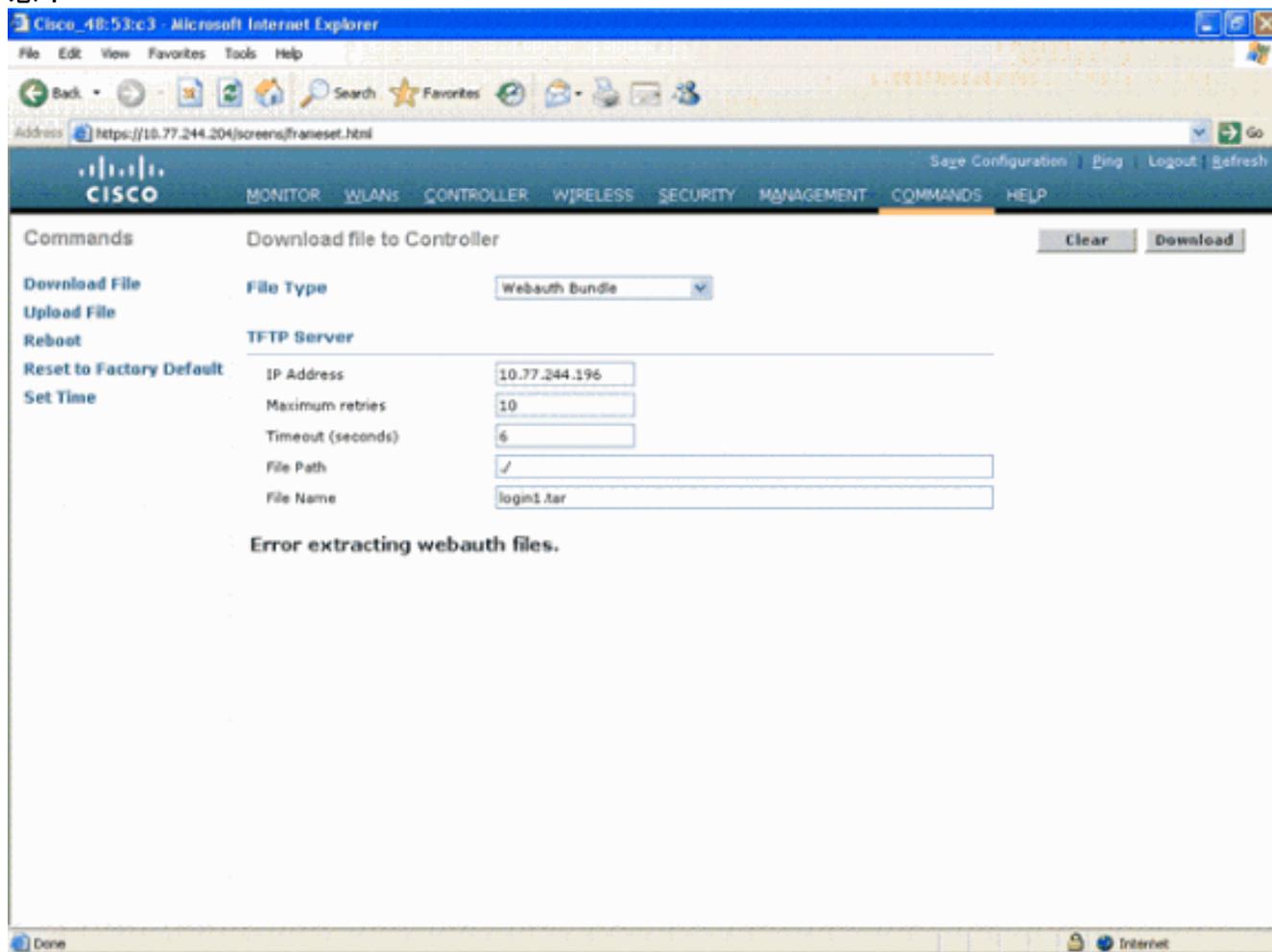
Web驗證疑難排解

設定Web驗證後，如果功能無法按預期運作，請完成以下步驟：

1. 檢查客戶端是否獲得IP地址。如果沒有，使用者可以取消選中WLAN上的**DHCP Required**覈取方塊，並為無線客戶端提供靜態IP地址。假設與接入點關聯。
2. 此程式的下一步是使用Web瀏覽器對URL進行DNS解析。當WLAN客戶端連線到為Web身份驗證配置的WLAN時，客戶端從DHCP伺服器獲取IP地址。使用者開啟Web瀏覽器並輸入網站地址。然後，客戶端執行DNS解析以獲取網站的IP地址。現在，當使用者端嘗試連線至網站時，WLC會攔截使用者端的HTTP GET作業階段，並將使用者重新導向到Web驗證登入頁面。
3. 因此，請確保使用者端能夠執行DNS解析，以便重新導向生效。在Microsoft Windows中，選擇**開始>運行**，輸入**CMD**以開啟命令視窗，然後執行「nslookup www.cisco.com」並檢視IP地址是否返回。在Mac/Linux中，開啟終端視窗並執行「nslookup www.cisco.com」，然後檢視IP地址是否返回。如果您認為使用者端未取得DNS解析，您可以：輸入URL的IP位址(例如，<http://www.cisco.com>是<http://192.168.219.25>)。嘗試鍵入必須通過無線介面卡解析的任何（即使不存在）IP地址。輸入此URL時，它會啟動網頁嗎？如果是，則很可能是DNS問題。這也可能是憑證問題。預設情況下，控制器使用自簽名證書，大多數Web瀏覽器會警告其不要使用。
4. 對於使用自定義網頁的Web身份驗證，請確保自定義網頁的HTML代碼適當。您可以從[思科軟體下載](#)範例Web驗證指令碼。例如，對於5508控制器，選擇**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**，然後下載webauth_bundle.zip檔案。使用者的Internet瀏覽器重新導向至自訂登入頁面時，系統會將這些引數新增到URL:ap_mac — 無線使用者所關聯的接入點的

MAC地址。switch_url — 必須向其發佈使用者憑據的控制器URL。redirect — 身份驗證成功後使用者重定向到的URL。statusCode — 控制器Web驗證伺服器傳回的狀態碼。wlan — 無線使用者關聯的WLAN SSID。以下是可用的狀態代碼：狀態代碼1 - 「You are already logged in.您無需進一步操作。」狀態代碼2 - 「You are not configured to authenticate against Web portal. (未配置您對Web門戶進行身份驗證。)」您無需進一步操作。」狀態代碼3 — 「此時無法使用指定的使用者名稱。使用者名稱可能已經登入系統？」狀態代碼4 — 「You have been excluded.」狀態代碼5 — 「您輸入的使用者名稱和密碼組合無效。請再試一次。」

5. 上傳到WLC之前，需要在自定義網頁上顯示的所有檔案和圖片必須捆綁到.tar檔案中。確保.tar套件組合中包含的檔案之一是login.html。如果不包括login.html檔案，則會收到以下錯誤消息：



有關如何建立自訂Web驗證視窗的詳細資訊，請參閱[無線LAN控制器Web驗證組態範例的自訂Web驗證準則](#)一節。注意：檔案過大且檔名稱過長可能會導致解壓縮錯誤。建議圖片採用.jpg格式。

6. 確保Scripting選項在客戶端瀏覽器上未被阻止，因為WLC上的自定義網頁基本上是HTML指令碼。
7. 如果您為WLC的虛擬介面設定了主機名稱，請確保DNS解析對虛擬介面的主機名稱可用。注意：從WLC GUI導覽至Controller > Interfaces選單，以便為虛擬接口分配DNS主機名。
8. 有時，客戶端電腦上安裝的防火牆會阻止Web身份驗證登入頁。嘗試存取登入頁面之前，請先停用防火牆。完成Web驗證後，可以再次啟用防火牆。
9. 拓撲/解決方案防火牆可以放置在客戶端和web-auth伺服器之間，這取決於網路。對於實施的每個網路設計/解決方案，終端使用者必須確保網路防火牆上允許這些埠。
10. 若要進行Web驗證，使用者端必須首先與WLC上的適當WLAN建立關聯。導覽至WLC GUI上

的**Monitor > Clients**功能表，以便檢視使用者端是否與WLC關聯。檢查客戶端是否具有有效的IP地址。

11. 在Web驗證完成之前，在客戶端瀏覽器上禁用代理設定。
12. 預設的Web驗證方法是密碼驗證通訊協定(PAP)。確保在RADIUS伺服器上允許PAP身份驗證，以便此命令生效。若要檢查使用者端驗證的狀態，請檢查RADIUS伺服器的偵錯和記錄訊息。您可以在WLC上使用**debug aaa all**命令來檢視RADIUS伺服器的偵錯。
13. 將電腦上的硬體驅動程式從製造商網站更新為最新代碼。
14. 驗證請求方中的設定 (筆記型電腦上的程式) 。
15. 使用內建於Windows中的Windows零配置請求方時： 驗證使用者是否安裝了最新的修補程式。對請求方運行調試。
16. 在客戶端上，從命令視窗開啟EAPOL(WPA+WPA2)和RASTLS日誌。選擇**開始>運行> CMD:**

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

若要停用日誌，請執行相同的命令，但將enable替換為disable。對於XP，所有日誌都可以位於C:\Windows\tracing。
17. 如果仍然沒有登入網頁，請收集並分析來自單個客戶端的此輸出：

```
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. 如果完成這些步驟後問題未解決，請收集這些調試並使用[Support Case Manager](#)以開啟服務請求。

```
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>
```

相關資訊

- [無線 LAN 控制器 Web 驗證組態範例](#)
- [使用無線 LAN 控制器的外部 Web 驗證組態範例](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。