瞭解無線LAN控制器(WLC)上的Web驗證

目錄

簡介

本檔案介紹無線LAN控制器(WLC)上的Web驗證程式。

必要條件

需求

思科建議您瞭解 WLC 組態的基本知識。

採用元件

本文件中的資訊係根據所有 WLC 硬體型號。

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。

Web 驗證內部程序

定位為安全功能的 Web 驗證

Web 驗證 (WebAuth) 是第 3 層安全機制，為執行瀏覽器的任何站台提供方便好用的安全功能。

它可以與任何預先共用金鑰(PSK)安全性（第2層安全原則）結合使用。

雖然WebAuth和PSK的組合減少了使用者友好部分，但它具有加密客戶端流量的優點。

WebAuth 是一種不加密的驗證方式。

設定WebAuth時不能搭配802.1x/RADIUS（遠端驗證撥入使用者服務），除非同時安裝和設定WLC軟體7.4版。

客戶端必須通過dot1x和Web身份驗證。此版本旨在為員工（需使用802.1x）而非訪客新增Web輸入網站。

員工的 dot1x 或訪客的 Web 輸入網站沒有多合一服務組識別元 (SSID)。

WebAuth 的運作方式

802.11 驗證程序為開放式，因此您可以順利進行驗證和建立關聯，而不會出現問題。程式完成後，您會與其他專案建立關聯，但不會在WLC中 **RUN** 狀態.

啟用Web驗證後，您將停留在 **WEBAUTH_REQD** 其中無法訪問任何網路資源。

您必須收到 DHCP IP 位址，該位址中需包含選項中的 DNS 伺服器位址。

在瀏覽器中輸入有效的URL。用戶端會透過 DNS 通訊協定解析 URL。然後用戶端將其 HTTP 要求傳送到網站的 IP 位址。

WLC會攔截該要求並返回 **webauth** 模仿網站IP地址的登入頁面。透過外部WebAuth，WLC會使用HTTP回應進行回應，包括您的網站IP位址，並宣告頁面已移動。

該頁面已移至 WLC 使用的外部 Web 伺服器。預設情況下，您通過驗證之後，會取得對所有網路資源的存取許可權，且系統會將您重新導向至最初要求的URL（除非已在WLC上設定強制重新導向）。

總而言之，WLC允許使用者端解析DNS，並在其中自動取得IP位址 **WEBAUTH_REQD** 狀態.

要觀察另一個埠而不是埠80，請使用 **config network web-auth-port** 也在此連線埠上建立重新導向。

例如，存取控制伺服器 (ACS) Web 介面位於連接埠 2002 或其他類似應用程式中。

> **有關 HTTPS 重新導向的附註**：預設情況下，WLC不會重新導向HTTPS流量。這表示如果您在瀏覽器中輸入HTTPS位址，系統不會執行任何操作。您必須輸入 HTTP 位址，才能重新導向到以 HTTPS 提供的登入頁面。
>
> 在8.0及更新版本中，可以使用CLI指令啟用HTTPS流量重新導向 **config network web-auth https-redirect enable.**
>
> 在傳送許多HTTPS要求的情況下，這會使用WLC的大量資源。建議不要在WLC 8.7之前的版本中使用此功能，因為此版本以後這個功能的可擴充性有所增強。另請注意，這種情況下無法避免憑證警告。如果使用者端要求任何URL(例如https://www.cisco.com),WLC仍會出示為了虛擬介面IP位址核發的專屬憑證。此指令從來不會與使用者端要求的URL/IP位址相符，且憑證不受信任，除非使用者端在瀏覽器中強制執行例外狀況。

在 WLC 軟體 8.7 之前的版本中測量到指標性效能下降：

Webauth	達到的速率
3 個 URL - HTTP	140/秒
第一個 URL - HTTP 第二和第三個 URL - HTTPS	20/秒
3 個 URL - HTTPS（大型部署）	<1/秒
3 個 URL - HTTPS（最多 100 個用戶端）	10/秒

在此效能表中，3 個 URL 指的是：

- 終端使用者輸入的原始URL
- WLC將瀏覽器重新導向到的URL
- 最終認證提交

此效能表提供下列情況下的WLC效能：全部3個URL都是HTTP、全部3個URL都是HTTPS，或是使用者端從HTTP移至HTTPS（典型）。

如何讓內部（本機）WebAuth 與內部頁面互相配合

要配置帶有運行動態介面的WLAN，客戶端還會通過DHCP接收DNS伺服器IP地址。

在任何之前 **webauth** 設定，驗證WLAN是否正常工作，DNS請求是否可以解析(**nslookup**)，並且可以瀏覽網頁。

將Web驗證設定為第3層安全功能。在本地資料庫或外部RADIUS伺服器上建立使用者。

請參閱無線 LAN 控制器 Web 驗證組態範例文件。

如何使用自訂頁面設定自訂本機 WebAuth

自定義 **webauth** 可以配置 **redirectUrl** 從 **Security** 頁籤。這麼做會強制重新導向至您輸入的特定網頁。

使用者通過驗證時，系統會覆寫使用者端要求的原始URL，並顯示為重新導向指定的頁面。

自訂功能讓您可使用自訂 HTML 頁面，而不是使用預設登入頁面。將 html 和影像檔套件組合上傳

到控制器。

在上傳頁面中，尋找 **webauth bundle** 採用tar格式。PicoZip會建立與WLC相容且可搭配使用的tar檔案。

有關 WebAuth 套件組合的範例，請參閱無線控制器 WebAuth 套件組合的下載軟體頁面。為您的WLC選擇適當的版本。

建議自訂已存在的套件組合；請勿建立新套件組合。

有一些限制 **custom webauth** 因版本和錯誤而異。

- .tar 檔案的大小（不超過 5MB）
- .tar 中的檔案數量
- 檔案的檔案名稱長度（不超過30個字元）

如果該包不起作用，請嘗試使用簡單的自定義包。分別新增檔案和複雜性以訪問使用者嘗試使用的包。這有助於確定問題。

若要設定自訂頁面，請參閱建立自訂Web驗證登入頁面(思科無線區域網路控制器組態設定指南7.6版中的一節)。

覆寫全域組態的技巧

使用**override global config**指令進行設定，並為每個WLAN設定WebAuth型別。這允許內部/預設WebAuth與另一個WLAN的自訂內部/預設WebAuth。

這允許為每個WLAN設定不同的自訂頁面。

合併同一套件組合中的所有頁面，並將其上傳到WLC。

在每個WLAN上使用**override global config**指令以設定自訂頁面，並從套件組合里的所有檔案中選擇哪個檔案是登入頁面。

為每個WLAN選擇套件組合中的不同登入頁面。

重新導向問題

HTML 套件組合中有一個變數可用於重新導向。請勿將強制重新導向 URL 放在此處。

遇到自訂WebAuth中的重新導向問題時，思科建議檢查套件組合。

如果您在 WLC GUI 中輸入含有 **+= 的重新導向 URL，可能會覆寫***或新增到套件組合中定義的 URL。*

例如，在WLC GUI中， **redirectURL** 欄位設定為www.cisco.com;但是套件組合中顯示： **redirectURL+=** '(網站URL)'。 **+=**使用者重新導向至無效的URL。

如何讓外部（本機）Web 驗證與外部頁面互相配合

利用外部WebAuth伺服器只是為了登入頁面的外部存放庫。使用者認證仍會由 WLC 進行驗證。外部Web伺服器僅允許特殊或不同的登入頁面。

對外部WebAuth執行的步驟：

1. 用戶端（一般使用者）開啟 Web 瀏覽器並輸入 URL。

2. 如果用戶端未通過驗證且使用外部 Web 驗證，則 WLC 會將使用者重新導向到外部 Web 伺服器 URL。WLC會傳送一個HTTP重新導向給使用者端，其中包含模仿的IP位址，且指向外部伺服器IP位址。外部Web驗證登入URL附加了引數，例如 **AP_Mac_Address**,其 **client_url** (**使用者端URL位址**)，以及 **action_URL** 需要聯絡交換機web伺服器。

3. 外部 Web 伺服器 URL 將使用者傳送到登入頁面。使用者可以使用預先驗證存取控制清單(ACL)來存取伺服器。

4. 登入頁面將使用者憑證請求傳送回 **action_URL**(例如http://192.0.2.1/login.html)中。這是作為重新導向URL的輸入引數提供的，其中192.0.2.1是交換器上的虛擬介面位址。

5. WLC Web 伺服器提交使用者名稱和密碼以進行驗證。

6. WLC 起始 RADIUS 伺服器要求或使用 WLC 上的本機資料庫，然後驗證使用者的身分。

7. 如果驗證成功，WLC Web 伺服器會將使用者轉送到已設定的重新導向 URL 或用戶端輸入的 URL。

8. 如果驗證失敗，WLC Web伺服器會將使用者重新導向回使用者登入URL。

   注意：本檔案中使用192.0.2.1作為虛擬IP的例子。建議將 192.0.2.x 範圍用於虛擬 IP，因為它不可路由。舊文檔可能指的是「1.1.1.x」，或者仍是WLC中配置的預設設定。但是請注意，此 IP 現在是有效的可路由 IP 位址，因此建議改用 192.0.2.x 子網路。

如果存取點(AP)處於FlexConnect模式，則 **preauth** ACL不相關。Flex ACL 可用於允許未經驗證的用戶端存取 Web 伺服器。

請參閱使用無線 LAN 控制器的外部 Web 驗證組態範例。

USB 傳輸

Web傳輸是內部Web驗證的變體。它會顯示一個包含警告或警示語句的頁面，但不會提示輸入認證。

然後使用者按一下**ok**。啟用電子郵件輸入，且使用者可以輸入其電子郵件地址（會成為其使用者名稱）。

使用者連線時，請檢查您的作用中使用者端清單，並確認使用者清單中是否已列出其輸入作為使用者名稱的電子郵件地址。

如需詳細資訊，請參閱無線LAN控制器5760/3850 Web傳輸組態範例。

條件式 Web 重新導向

如果啟用條件式 Web 重新導向，則 802.1x 驗證成功完成後，系統會有條件地將使用者重新導向到特定網頁。

您可以指定重新導向頁面，以及在 RADIUS 伺服器上進行重新導向的條件。

條件可包括密碼（當密碼即將到期），或是使用者需要支付帳單款項才能繼續使用/存取時。

如果RADIUS伺服器傳回Cisco AV配對 **url-redirect**，則使用者開啟瀏覽器時，系統會將其重新導向到指定的URL。

如果伺服器也傳回Cisco AV配對 **url-redirect-acl**，則系統會為此客戶端安裝指定的ACL作為預身份驗證ACL。

此時用戶端還不視為獲得完整授權，且只能傳遞預先驗證 ACL 允許的流量。用戶端在指定的 URL 完成特定操作後（例如變更密碼或支付帳單款項），用戶端必須重新進行驗證。

當RADIUS伺服器沒有傳回 **url-redirect**中，使用者端視為獲得完整授權且允許傳遞流量。

> **附註**：條件式 Web 重新導向功能僅適用於針對 802.1x 或 WPA+WPA2 第 2 層安全性設定的 WLAN。

設定RADIUS伺服器後，使用控制器GUI或CLI，在控制器上設定條件式Web重新導向。請參閱以下逐步指南：設定Web重新導向(GUI)和設定Web重新導向(CLI)。

啟動顯示頁面 Web 重新導向

如果啟用啟動顯示頁面 Web 重新導向，則 802.1x 驗證成功完成後，系統會將使用者重新導向到特定網頁。重新導向後，使用者會獲得網路的完整存取權限。

您可以在 RADIUS 伺服器上指定重新導向頁面。如果RADIUS伺服器傳回Cisco AV配對 **url-redirect**，則使用者開啟瀏覽器時，系統會將其重新導向到指定的URL。

此時使用者端視為獲得完整授權，且允許其傳遞流量，即使RADIUS伺服器沒有傳回 **url-redirect**.

> **附註**：啟動顯示頁面重新導向功能僅適用於針對802.1x或WPA+WPA2第2層安全性設定的 WLAN。

設定RADIUS伺服器後，使用控制器GUI或CLI，在控制器上設定啟動顯示頁面Web重新導向。

MAC 過濾器失敗時的 WebAuth

MAC Filter FaFailure上的WebAuth要求您在第2層安全功能表上設定MAC過濾器。

如果使用者成功使用其MAC位址通過驗證，便會接進入 **run** 狀態.

如果不是，則進入 **WEBAUTH_REQD** 進行狀態和常規web驗證。

附註：Web傳輸不支援此功能。如需詳細資訊，請依照增強功能要求Cisco錯誤ID CSCtw73512上的活動執行

中央 Web 驗證

中央 Web 驗證指的是 WLC 不再託管任何服務的情況。使用者端直接傳送到ISE Web輸入網站，而不通過WLC上的192.0.2.1。登入頁面和整個輸入網站都外部化。

在已啟用的 WLAN 和 MAC 過濾器進階設定中，若已啟用 RADIUS 網路許可控制 (NAC)，便會進行中央 Web 驗證。

WLC將RADIUS驗證（通常用於MAC過濾器）傳送到ISE，而ISE會使用 **redirect-url** 屬性值(AV)配對。

然後使用者進入 **POSTURE_REQD** 在ISE通過授權更改(CoA)請求提供授權之前進行狀態。安全狀態或中央 WebAuth 會出現相同的情況。

中央 WebAuth 與 WPA-Enterprise/802.1x 不相容，因為訪客輸入網站無法像使用可擴充驗證通訊協定 (EAP) 時一樣傳回工作階段金鑰以進行加密。

外部使用者驗證 (RADIUS)

當WLC處理憑證或啟用第3層Web原則時，外部使用者驗證(RADIUS)僅對本機WebAuth有效。在本地或WLC上或透過RADIUS驗證使用者身分。

WLC 會依照特定順序檢查使用者認證。

1. 在任何情況下，它會先在自己的資料庫中查找。
2. 如果沒有在資料庫中找到使用者，則會前往在訪客 WLAN 中設定的 RADIUS 伺服器（如果有已設定的伺服器）。
3. 接下來會檢查全域RADIUS伺服器清單中的RADIUS伺服器， **network user** 已選中。

第三點回答了那些沒有為該WLAN設定RADIUS的人的問題，但請注意，如果在控制器上找不到該使用者，WLC仍會檢查RADIUS。

這是因為 **network user** 已針對全域清單中您的RADIUS伺服器進行檢查。

WLC 可以使用密碼驗證通訊協定 (PAP)、Challenge Handshake 驗證通訊協定 (CHAP) 或 EAP-MD5 (Message Digest5) 來向 RADIUS 伺服器驗證使用者身分。

這是一個全域參數，可在 GUI 或 CLI 上設定：

在 GUI 上：導航至 **Controller > Web RADIUS Authentication**

在 CLI 上：輸入 **config custom-web RADIUSauth**

註:NAC訪客伺服器僅使用PAP。

如何設定有線訪客 WLAN

有線訪客WLAN配置類似於無線訪客配置。可以設定一個或兩個控制器（僅適用於有一個控制器是自動錨點時）。

選擇一個VLAN作為有線訪客使用者的VLAN，例如VLAN 50。當有線訪客想要存取網際網路，可將筆記型電腦連線到為VLAN 50設定的交換器連線埠。

這個 VLAN 50 必須獲得允許且位於通過 WLC 主幹連接埠的路徑上。

在有兩個 WLC 的情況下（一個錨點和一個外部），此有線訪客 VLAN 必須通向外部 WLC（名稱為 WLC1）而不是錨點。

接下來WLC1負責連線到DMZ WLC（錨點，名稱為WLC2）的流量通道，後者會釋出路由網路中的流量。

以下是設定有線訪客存取的五個步驟：

1. **為有線訪客使用者存取設定動態介面 (VLAN)。**

   在WLC1上建立一個動態介面VLAN50。在 **interface configuration** 頁面，請檢查 **Guest LAN** 框。然後，欄位，例如 **IP address** 和 **gateway** 消失。WLC需要識別流量是從VLAN 50路由而來。這些使用者端是有線訪客。

2. **為訪客使用者存取建立有線 LAN。**

   在控制器上，與 WLAN 相關聯時會使用介面。接下來，在總部控制器上建立WLAN。導航至 **WLANs** 然後按一下 **New**.在 **WLAN Type**，選擇 **Guest LAN**.

   在 Profile Name 和 WLAN SSID 中，輸入用於識別此 WLAN 的名稱。可以使用不同名稱，但不能包含空格。此處使用了 WLAN 一詞，但這個網路設定檔與無線網路設定檔無關。

   其 **General** 頁籤提供兩個下拉選單： **Ingress** 和 **Egress**.輸入 (Ingress) 是使用者所來自的 VLAN (VLAN 50)；輸出(Egress)是您要傳送使用者的目的地VLAN。

   對於 **Ingress**，選擇 **VLAN50**.

   對於 **Egress**，情況有所不同。如果只有一個控制器，請建立另一個動態介面 **standard** 這一次（不是訪客LAN），並將有線使用者傳送到此介面。在這種情況下，請將其傳送到 DMZ 控制器。因此，就 **Egress** 介面，選擇 **Management Interface**.

   其 **Security** 此訪客LAN「WLAN」的模式為WebAuth，這是可接受的。按一下 **Ok** 以便驗證。

3. **設定外部控制器（總部）。**

   從 **WLAN list**，按一下 **Mobility Anchor** 在 **Guest LAN** 線路，然後選擇您的DMZ控制器。這裡假設兩個控制器可以識別彼此。如果沒有，請轉至 **Controller** > **Mobility Management** > **Mobility group**，然後在WLC1上新增**DMZWLC**。接著在DMZ上新增**WLC**1。兩個控制器不應位於同一個行動群組中，否則基本安全規則會被破壞。

4. **設定錨點控制器（DMZ 控制器）。**

   總部控制器已準備就緒。現在準備DMZ控制器。開啟與 DMZ 控制器的網頁瀏覽器工作階段，然後導覽至 **WLANs**。建立一個新的 WLAN。在 **WLAN Type**，選擇 **Guest LAN**.

   在 **Profile Name** 和 **WLAN SSID**，輸入用於識別此WLAN的名稱。使用對總部控制器輸入的相同值。

   其 **Ingress** 介面是 **None**.這無關緊要，因為流量是透過Ethernet over IP(EoIP)通道接收的。無需指定任何輸入介面。

   其 **Egress** 介面是客戶端傳送的位置。例如， **DMZ VLAN** 是VLAN 9。為DMZWLC上的VLAN 9建立一個標準動態介面，然後選擇 **VLAN 9** 作為輸出介面。

   設定行動錨點通道的終端。在**WLAN list**中選擇 **Mobility Anchor for Guest LAN**.將流量傳送到本機控制器 **DMZWLC**。兩端現在均已就緒。

5. **微調訪客 LAN。**

   您也可以微調兩端的 WLAN 設定。兩端的設定必須相同。例如，如果您在 **WLAN Advanced** 頁籤， **Allow AAA override** 在WLC1上，勾選DMZWLC上的相同方塊。如果任一端的WLAN有任何不同，通道就會中斷。DMZWLC 拒絕流量；你可以看到 **run debug mobility**.

   請記住，實際上所有值都是從 DMZWLC 取得：IP 位址、VLAN 值等。以相同項目設定 WLC1 端，以便要求它轉送到 WLCDMZ。

登入頁面的憑證

本節提供在WebAuth頁面上放置自己的憑證，或隱藏192.0.2.1 WebAuth URL並顯示具名URL的程式。

上傳控制器 Web 驗證的憑證

通過GUI(**WebAuth > Certificate**)或CLI(傳輸型別 **webauthcert**)您可以在控制器上上傳憑證。

無論是使用憑證授權單位(CA)還是第三方官方憑證建立的憑證，都必須採用.pem格式。

傳送之前，您還必須輸入憑證的金鑰。

上傳後，需要重新開機才能讓憑證就緒。重新開機後，前往GUI中的WebAuth憑證頁面，尋找您上傳憑證的詳細資訊（有效性等）。

重要欄位為一般名稱 (CN)，亦即核發給憑證的名稱。本文件的「憑證授權單位和控制器上的其他憑證」一節中將說明此欄位。

重新開機並驗證憑證的詳細資訊後，系統會在WebAuth登入頁面上顯示新的控制器憑證。但是可能出現兩種情況。

1. 如果您的憑證是由每台電腦信任的幾個主要根 CA 中其中一個所核發，則可正常使用。VeriSign 便是其中一個例子，但您通常是由 Verisign 子 CA 簽署，而不是根 CA。如果您認為此處提到的 CA 值得信任，可以簽入您的瀏覽器憑證庫中。

2. 如果您的憑證來自較小型的公司/CA，則所有電腦都不會信任。還向客戶端提供公司/CA證書，然後其中一個根CA會頒發該證書。最終會產生「CA x已核發憑證> CA y已核發CA x憑證>此受信任的根CA已核發CA y憑證」這樣的憑證鏈。 最終目標是聯繫到用戶端信任的 CA。

憑證授權單位和控制器上的其他憑證

若要清除「此憑證不受信任」警告，請輸入在控制器上核發控制器憑證的CA憑證。

接下來控制器會顯示兩個憑證（控制器憑證及其CA憑證）。 CA憑證必須是受信任的CA或是有資源可驗證該CA。實際上，您可以建立一個 CA 憑證鏈，通往頂端的受信任 CA。

將整個憑證鏈放在同一個檔案中。然後檔案包含類似以下示例的內容：

```
BEGIN CERTIFICATE ------ device certificate*   END CERTIFICATE ------ BEGIN
CERTIFICATE ------ intermediate CA certificate* END CERTIFICATE ------ BEGIN
CERTIFICATE ------ Root CA certificate* END CERTIFICATE ------
```

如何使憑證與 URL 相符

WebAuth URL 設定為 192.0.2.1 以便自行驗證，且憑證已核發（這是 WLC 憑證的 CN 欄位）。

例如，若要將WebAuth URL變更為「myWLC.com」，請進入 **virtual interface configuration** (192.0.2.1介面)，您可以在此輸入 **virtual DNS hostname**，如myWLC.com。

如此一來會取代掉URL列中的192.0.2.1。此名稱也必須可解析。監聽器追蹤軌跡可顯示其運作方式，但當 WLC 傳送登入頁面時，WLC 會顯示 myWLC.com 位址，且用戶端會使用其 DNS 解析此名稱。

此名稱必須解析為192.0.2.1。這表示如果您也有使用名稱來管理WLC，請對WebAuth使用不同的名稱。

如果您使用對映到WLC管理IP位址的myWLC.com，則必須為WebAuth使用不同的名稱，例如myWLCwebauth.com。

排解憑證疑難問題

本節說明如何檢查及排解憑證疑難問題。

如何檢查

下載OpenSSL（Windows系統請搜尋OpenSSL Win32）並進行安裝。如果沒有任何組態，您可以前往bin目錄，嘗試使用 **openssl s_client –connect (your web auth URL):443**中，

如果此URL是您的DNS上WebAuth頁面所連結的URL，請參閱本檔案下一節中的「需檢查的專案」。

如果您的憑證使用私人CA，請將根CA憑證放在本機電腦上的目錄中，並使用openssl選項 - **CApath**.如果您有中繼CA，請將其放在同一個目錄中。

若要取得有關憑證的一般資訊和檢查憑證，請使用：

```
openssl x509 -in certificate.pem -noout -text
openssl verify certificate.pem
```

使用openssl來轉換憑證也很有用：

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

需檢查的項目

您可以看到連接時傳送給用戶端的憑證。讀取裝置憑證；CN必須是網頁可連線的URL。

查看裝置憑證中的「核發者」一行。此項目必須與第二個憑證的 CN 相符。第二個憑證「核發者」必須與下一個憑證的CN相符，以此類推。否則將不會產生真正的憑證鏈。

此處顯示的OpenSSL輸出中，請注意 **openssl** 無法驗證裝置證書，因為其「核發者」與提供的CA證書的名稱不匹配。

SSL 輸出

```
Loading 'screen' into random state - done CONNECTED(00000760) depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=20:unable to get local issuer certificate verify return:1 depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=27:certificate not trusted verify return:1 depth=0 /O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uk verify error:num=21:
unable to verify the first certificate verify return:1 --- Certificate chain
0 s:/O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uki:/C=US/ ST=
Arizona/L=Scottsdale/O=.com/OU=http://certificates.gocompany.com/repository/CN=
Secure Certification Authority/serialNumber=079
692871 s:/C=US/O=Company/OU=Class 2 Certification Authority
i:/C=US/O=Company/OU=Class 2 Certification Authority --- Server certificate

BEGIN CERTIFICATE-----
MIIE/zCCA+egAwIBAgIDRc2iMA0GCSqGSIb3DQEBBQUAMIHKMQswCQYDVQQGEwJV
output cut*
YMaj/NACviEU9J3iot4sfreCQSKkBmjH0kf/Dg1l0kmdSbc=

END CERTIFICATE-----
subject=/O=<company>.ac.uk/OU=Domain Control Validated/CN=<company>c.ac.uk
issuer=/C=US/ST=Arizona/L=Scottsdale/O=.com/OU=http://certificates.
.com/repository/CN=Secure Certification Authority/serialNumber=0
7969287 --- No client certificate CA names sent --- SSL handshake has read
2476 bytes and written 322 bytes --- New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 1024 bit Compression: NONE Expansion: NONE SSL-Session:

Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: A32DB00A7AB7CD1CEF683980F3696C2BBA31A1453324F711F50EF4B86A4A7F03

Session-ID-ctx:Master-Key: C95E1BDAC7B1A964ED7324955C985CAF186B92EA34CD69E10
5F95D969D557E19
```

```
939C6A77C72350AB099B3736D168AB22

Key-Arg : None
Start Time: 1220282986
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

另一個可能發生的問題是無法將憑證上傳到控制器。在這種情況下，不會出現有效性、CA 等問題。

若要驗證這一點，請檢查簡單式檔案傳輸通訊協定(TFTP)連線狀態，並嘗試傳輸組態檔。如果您輸入 **debug transfer all enable** 請注意問題出在憑證的安裝。

這可能是因為搭配憑證使用的金鑰錯誤所造成。也可能是因為憑證格式錯誤或已損毀。

思科建議您將該憑證內容與已知的有效憑證進行比較。這麼做可以看出 **LocalkeyID** 屬性顯示所有0（已發生）。 如果均為0，那麼必須重新轉換證書。

有兩個使用 OpenSSL 的指令可用於從 .pem 轉換回 .p12，然後使用您選擇的金鑰重新核發 .pem。

如果您收到 .pem，其中包含憑證且後面接著一個金鑰，請從 .pem 中複製金鑰部分： **----BEGIN KEY ---- until ------- END KEY ------** ，然後貼到「key. pem」中。

1. **openssl pkcs12 -export -in certificate.pem -inkey key.pem -out newcert.p12** ?系統提示您輸入金鑰；輸入 **check123**.

2. **openssl pkcs12 -in newcert.p12 -out workingnewcert.pem -passin pass:check123 -passout pass:check123** 這會產生具有密碼的可操作.pem **check123**.

須排解的其他疑難情況

雖然本文件未討論行動錨點，但如果您遇到錨點訪客情況，請確保行動交換正確執行，且您看到用戶端確實到達錨點。

任何進一步的 WebAuth 問題都需要在錨點上進行疑難排解。

以下是您可以進行疑難排解的一些常見問題：

- **使用者無法與訪客 WLAN 建立關聯。**

  此問題與 WebAuth 無關。請檢查用戶端組態、WLAN 的安全設定（如果已啟用），以及無線電是否處於作用中或運作中狀態等等。

- **使用者未取得 IP 位址** 。

  在訪客錨點情況下，這通常是因為外部和錨點的設定沒有完全相同所造成。若不是因為這個原因，請檢查 DHCP 組態、連線等項目。
- 確認其他 WLAN 是否可以順利使用同一個 DHCP 伺服器而沒有出現問題。此問題仍與 WebAuth 無關。

- **使用者沒有重新導向至登入頁面。**

這是最常見的症狀，不過情況更精確。有兩種可能情況。

系統沒有將使用者重新導向（使用者輸入 URL 卻永遠不會到達 WebAuth 頁面）。 若發生這種情況，請檢查：

已透過DHCP將有效的DNS伺服器指派給使用者端(**ipconfig /all**)，

可從使用者端連線至DNS(**nslookup (website URL**)，

使用者輸入的 URL 有效且用於重新導向、

使用者在連接埠 80 上進入 HTTP URL（例如若使用 http://localhost:2002 連線至 ACS，系統不會將您重新導向，因為是在連接埠 2002 而不是 80 上傳送）。

已正確將使用者重新導向到 192.0.2.1，但頁面本身沒有顯示。

這種情況很可能是 WLC 問題（錯誤）或用戶端問題所造成。可能是使用者端存在一些防火牆、軟體或原則封鎖。也可能是對方在其網頁瀏覽器中設定了 Proxy 。

建議：在用戶端 PC 上執行監聽器追蹤。不需要特殊無線軟體，只需使用 Wireshark 即可，它可在無線配接器上執行，並顯示 WLC 是否有回應和嘗試重新導向。可能發生兩種情況：沒有收到 WLC 的回應，或是 WebAuth 頁面的 SSL 交握發生錯誤。針對 SSL 交握問題，您可以檢查使用者瀏覽器是否允許 SSLv3（某些瀏覽器僅允許 SSLv2），以及進行憑證驗證時是否過於積極。

常見步驟是手動輸入 http://192.0.2.1，以檢查網頁是否會在沒有 DNS 的情況下顯示。實際上，輸入 http://10.0.0.0 可以獲得相同的效果。WLC 會重新導向您輸入的任何 IP 位址。因此，如果您輸入 http://192.0.2.1，並無法解決 Web 重新導向問題。如果您輸入 https://192.0.2.1（安全），並不會起作用，因為 WLC 不會重新導向 HTTPS 流量（預設情況下，在 8.0 版及更新版本中這實際上可行）。 直接載入頁面而不進行重新導向的最佳方式是輸入 https://192.0.2.1/login.html。

- **使用者無法進行驗證。**

  請參閱本文件中討論驗證的章節。在 RADIUS 本機上檢查認證。

- **使用者可能透過 WebAuth 成功進行驗證，但之後卻不能存取網際網路。**

  您可以將WebAuth從WLAN安全性中移除，如此一來WLAN會變為開放式。接著您可以嘗試存取 Web、DNS 等項目。如果這時也遇到問題，請完全移除 WebAuth 設定並檢查介面組態。

如需詳細資訊，請參閱：對無線 LAN 控制器 (WLC) 上的 Web 驗證進行排解疑難。

HTTP Proxy 伺服器及其運作方式

您可以使用 HTTP Proxy 伺服器。如果您需要用戶端在其瀏覽器中新增 192.0.2.1 不會通過 Proxy

伺服器的例外狀況，可以讓 WLC 偵聽 Proxy 伺服器連接埠上的 HTTP 流量（通常是 8080）。

為了瞭解這個情況，您需要知道 HTTP Proxy 的作用。這是您在瀏覽器中為用戶端（IP 位址和連接埠）設定的項目。

使用者造訪網站時的常見情況，是使用 DNS 將名稱解析為 IP，然後向 Web 伺服器要求網頁。這個程式一律將頁面的HTTP要求傳送至Proxy。

如有需要，Proxy 會處理 DNS，並將其轉送到 Web 伺服器（如果沒有在 Proxy 上快取該頁面）。此處探討的內容僅適用用戶端對 Proxy 情況。Proxy 是否取得真實的網頁與用戶端無關。

以下是 Web 驗證程序：

- URL 中的使用者類型。
- 用戶端 PC 傳送到 Proxy 伺服器。
- WLC攔截和模仿代理伺服器IP;它會以重新導向至 192.0.2.1 回覆 PC

在這個階段，如果 PC 沒有這項設定，便會要求 Proxy 的 192.0.2.1 WebAuth 頁面，如此一來就不會運作。PC 必須為 192.0.2.1 設定例外狀況；然後向 192.0.2.1 傳送 HTTP 要求，並繼續進行 WebAuth。

通過驗證後，所有通訊都會再次經過 Proxy。例外情況組態通常位於接近 Proxy 伺服器組態的瀏覽器中。然後您會看到以下訊息：「請勿對這些IP位址使用Proxy。」

在WLC 7.0及更新版本中，此功能 **webauth proxy redirect** 可以在全域WLC組態選項中啟用。

啟用後，WLC 會檢查用戶端是否設為手動使用 Proxy。在這種情況下，會將用戶端重新導向至某個頁面，這個頁面會顯示如何修改其 Proxy 設定以便讓一切正常運作。

可以將 WebAuth Proxy 重新導向設定為可在各種連接埠上執行，且與中央 Web 驗證相容。

有關 WebAuth Proxy 重新導向的範例，請參閱無線 LAN 控制器上的 Web 驗證 Proxy 組態範例。

HTTP 上而不是 HTTPS 上的 Web 驗證

您可以在 HTTP 上登入 Web 驗證，而不是 HTTPS。如果登入 HTTP，就不會收到憑證警示。

若使用 WLC 7.2 版以前的版本，必須停用 WLC 的 HTTPS 管理並退出 HTTP 管理。但是這僅允許透過 HTTP 進行 WLC 的 Web 管理。

針對WLC 7.2版，請使用 **config network web-auth secureweb disable** 命令禁用。這只會為 Web 驗證停用 HTTPS，而不會停用管理。請注意，此操作需要重新啟動控制器！

在 WLC 7.3 版和更新版本中，只可透過 GUI 和 CLI 為 WebAuth 啟用/停用 HTTPS。

相關資訊

- **無線 LAN 控制器 Web 驗證組態範例**
- **下載無線控制器 WebAuth 套件組合的軟體**
- **建立自訂 Web 驗證登入頁面**
- **使用無線 LAN 控制器的外部 Web 驗證組態範例**

- 無線LAN控制器5760/3850 Web傳輸組態範例
- 設定Web重新導向(GUI)
- 設定Web重新導向(CLI)
- 對無線 LAN 控制器 (WLC) 上的 Web 驗證進行排解疑難
- 無線 LAN 控制器上的 Web 驗證 Proxy 組態範例
- 要求建議 (RFC)
- 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）。