

# 使用WLC設定外部Web驗證

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[背景資訊](#)

[外部Web驗證程式](#)

[網路設定](#)

[設定](#)

[為訪客使用者建立動態介面](#)

[建立預先驗證ACL](#)

[在WLC上為訪客使用者建立本機資料庫](#)

[設定WLC以進行外部Web驗證](#)

[為訪客使用者配置WLAN](#)

[驗證](#)

[疑難排解](#)

[已重定向到外部Web身份驗證伺服器的客戶端收到證書警告](#)

[錯誤：「無法顯示頁面」](#)

[相關資訊](#)

## 簡介

本文說明如何使用外部Web伺服器設定無線LAN控制器(WLC)以進行Web驗證。

## 必要條件

### 需求

嘗試此組態之前，請確保符合以下要求：

- 輕量型存取點(LAP)和Cisco WLC組態的基本知識
- 輕量型存取點通訊協定(LWAPP)以及無線存取點控制和布建(CAPWAP)的基本知識
- 瞭解如何設定和配置外部Web伺服器
- 瞭解如何設定和配置DHCP和DNS伺服器

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 4400 WLC ( 執行韌體版本7.0.16.0 )
- Cisco 1131AG系列LAP
- 執行韌體版本3.6的Cisco 802.11a/b/g無線使用者端配接器
- 承載Web驗證登入頁面的外部Web伺服器
- DNS和DHCP伺服器，用於向無線客戶端分配地址解析和IP地址

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

## 背景資訊

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和DNS相關封包除外 )，直到該使用者端正確提供了有效的使用者名稱和密碼。Web驗證是一種簡單的驗證方法，不需要請求方或客戶端實用程式。

可以使用以下工具執行Web驗證：

- WLC上的預設登入視窗
- WLC上預設登入視窗的修改版本
- 在外部Web伺服器上配置的自定義登入視窗 ( 外部Web身份驗證 )
- 可下載到控制器的自訂登入視窗

本文提供一個組態範例，說明如何設定WLC以使用外部Web伺服器的登入指令碼。

## 外部Web驗證程式

使用外部Web驗證時，用於Web驗證的登入頁面會儲存在外部Web伺服器上。以下是無線使用者端嘗試存取已啟用外部Web驗證的WLAN網路時的事件序列：

1. 使用者端 ( 一般使用者 ) 連線到WLAN，然後開啟Web瀏覽器並輸入URL，例如www.cisco.com。
2. 使用者端向DNS伺服器傳送DNS要求，以便將www.cisco.com解析為IP位址。
3. WLC將要求轉送到DNS伺服器，而DNS伺服器會將www.cisco.com解析為IP位址，並傳送DNS回覆。控制器將回覆轉送到使用者端。
4. 使用者端嘗試透過將TCP SYN封包傳送到www.cisco.comwww.cisco.com的IP位址來啟動TCP連線。
5. WLC有為使用者端設定的規則，因此可以作為www.cisco.com的代理。它將TCP SYN-ACK資料包發回客戶端，源地址為www.cisco.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。
6. 使用者端將目的地為www.google.com的HTTP GET封包傳送到。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。
7. 然後使用者端會啟動與重新導向URL的HTTPS連線，此重新導向URL會將其傳送到1.1.1.1。

這是控制器的虛擬IP地址。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。

8. 由於外部Web驗證已啟用，WLC會將使用者端重新導向到外部Web伺服器。
9. 外部Web驗證登入URL附加了引數，例如AP\_Mac\_Address、client\_url(www.cisco.com)，以及使用者端需要與控制器Web伺服器連線的action\_URL。**注意：**action\_URL通知Web伺服器使用者名稱和密碼儲存在控制器上。憑證必須傳回控制器才能通過驗證。
10. 外部Web伺服器URL將使用者導向登入頁面。
11. 登入頁面取得使用者憑證輸入，並將要求傳回WLC Web伺服器的action\_URL，例如http://1.1.1.1/login.html。
12. WLC Web 伺服器提交使用者名稱和密碼以進行驗證。
13. WLC起始RADIUS伺服器要求或使用WLC上的本機資料庫並驗證使用者的身分。
14. 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或使用者端用來啟動的URL，例如www.cisco.com。
15. 如果驗證失敗，WLC Web伺服器會將使用者重新導向回客戶登入URL。

**注意：**若要將外部Web驗證設定為使用HTTP和HTTPS以外的連線埠，請發出以下命令：

```
(Cisco Controller) >config network web-auth-port
```

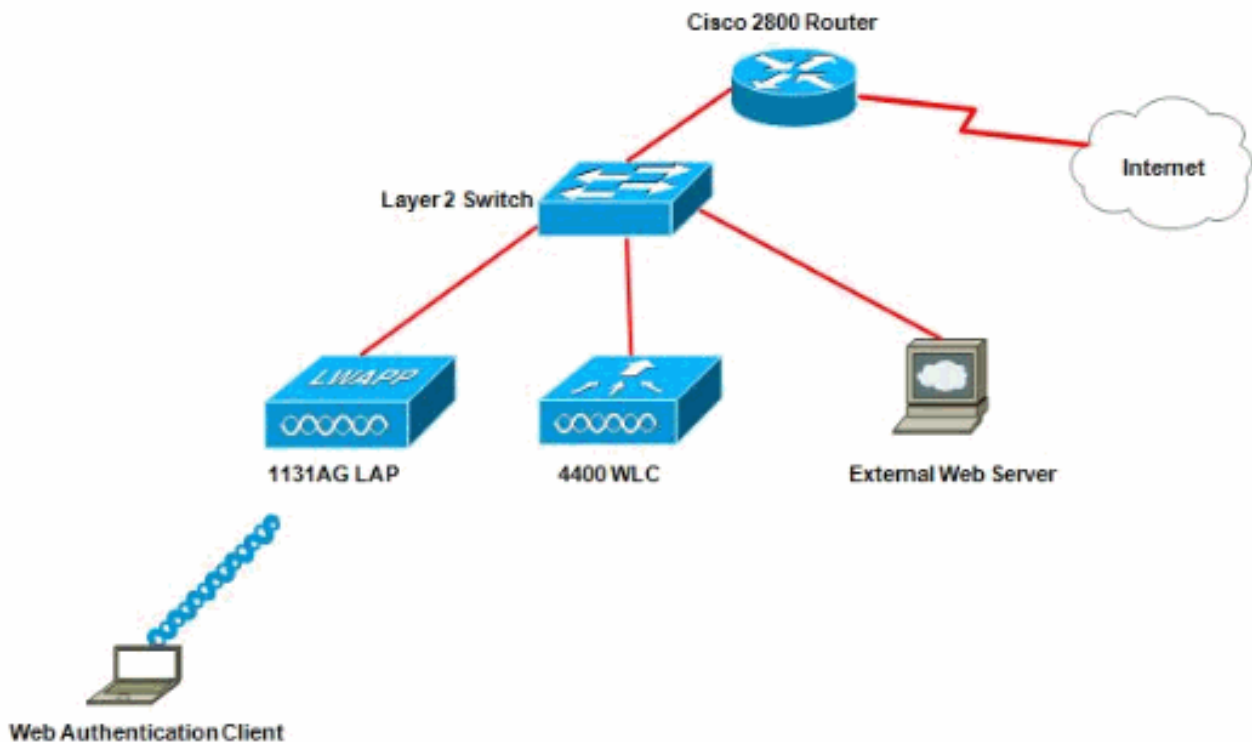
```
<port> Configures an additional port to be redirected for web authentication.
```

## 網路設定

配置示例使用此設定。LAP已註冊到WLC。您需要為訪客使用者設定WLAN **guest**，且必須為使用者啟用Web驗證。您還需要確保控制器將使用者重新導向到外部Web伺服器URL（用於外部Web驗證）。外部Web伺服器承載用於驗證的Web登入頁面。

必須根據控制器上維護的本地資料庫驗證使用者憑據。驗證成功後，應允許使用者訪問WLAN訪客。需要為此設定配置控制器和其他裝置。

**注意：**您可以使用自定義版本的登入指令碼，該指令碼將用於Web身份驗證。您可以從[思科軟體下載](#)頁面下載範例Web驗證指令碼。例如，若是4400控制器，請導覽至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，然後下載webauth\_bundle.zip檔案。



**注意：**自訂Web身份驗證套件最多只能包含30個字元的檔名。請確保套件組合中的檔案名稱不超過30個字元。

**注意：**本文檔假定配置了DHCP、DNS和外部Web伺服器。有關如何配置DHCP、DNS和外部Web伺服器的資訊，請參閱相應的第三方文檔。

## 設定

設定WLC以進行外部Web驗證之前，必須設定WLC以達成基本操作並將LAP註冊到WLC。本檔案假定WLC已設定為基本操作，且LAP已註冊到WLC。如果您是嘗試設定WLC以進行LAP基本操作的新使用者，請參閱[向無線LAN控制器\(WLC\)註冊輕量AP\(LAP\)](#)。

完成以下步驟，以便為此設定配置LAP和WLC：

1. [為訪客使用者建立動態介面](#)
2. [建立預先驗證ACL](#)
3. [在WLC上為訪客使用者建立本機資料庫](#)
4. [設定WLC以進行外部Web驗證](#)
5. [為訪客使用者配置WLAN](#)

## 為訪客使用者建立動態介面

完成以下步驟，為訪客使用者建立動態介面：

1. 在WLC GUI中選擇**Controllers > Interfaces**。出現Interfaces視窗。此視窗列出控制器上配置的介面。這包括預設介面，即管理介面、ap-manager介面、虛擬介面和服務埠介面以及使用者定義的動態介面。

The screenshot shows the Cisco Controller configuration page. The 'CONTROLLER' tab is selected. On the left, the 'Interfaces' menu item is highlighted. The main area displays a table of interfaces:

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
ap-manager	untagged	10.78.177.27	Static	Enabled
management	untagged	10.78.177.26	Static	Not Supported
service-port	N/A	192.168.1.25	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported

2. 按一下「New」以建立一個新的動態介面。
3. 在Interfaces > New視窗中，輸入介面名稱和VLAN Id。然後按一下Apply。在本例中，動態介面命名為guest，且VLAN Id指派為10。

The screenshot shows the Cisco Controller configuration page with the 'CONTROLLER' tab selected. The 'Interfaces > New' dialog box is open, showing the following fields:

- Interface Name: guest
- VLAN Id: 10

4. 在Interfaces > Edit視窗中，為動態介面輸入IP地址、子網掩碼和預設網關。將其分配給WLC上的物理埠，並輸入DHCP伺服器的IP地址。然後，按一下「Apply」。

The screenshot shows the Cisco WLC GUI with the 'CONTROLLER' tab selected. The left sidebar lists various configuration options, with 'Interfaces' highlighted. The main area displays the configuration for the 'guest' interface, which is highlighted with a red border. The configuration is organized into several sections:

- General Information:** Interface Name: guest; MAC Address: 00:0b:85:48:53:c0
- Configuration:** Guest Lan: ; Quarantine: ; Quarantine Vlan Id: 0
- Physical Information:** Port Number: 2; Backup Port: 0; Active Port: 0; Enable Dynamic AP Management:
- Interface Address:** VLAN Identifier: 10; IP Address: 172.18.1.10; Netmask: 255.255.255.0; Gateway: 172.18.1.20
- DHCP Information:** Primary DHCP Server: 172.18.1.20; Secondary DHCP Server: (empty)
- Access Control List:** ACL Name: none

## 建立預先驗證ACL

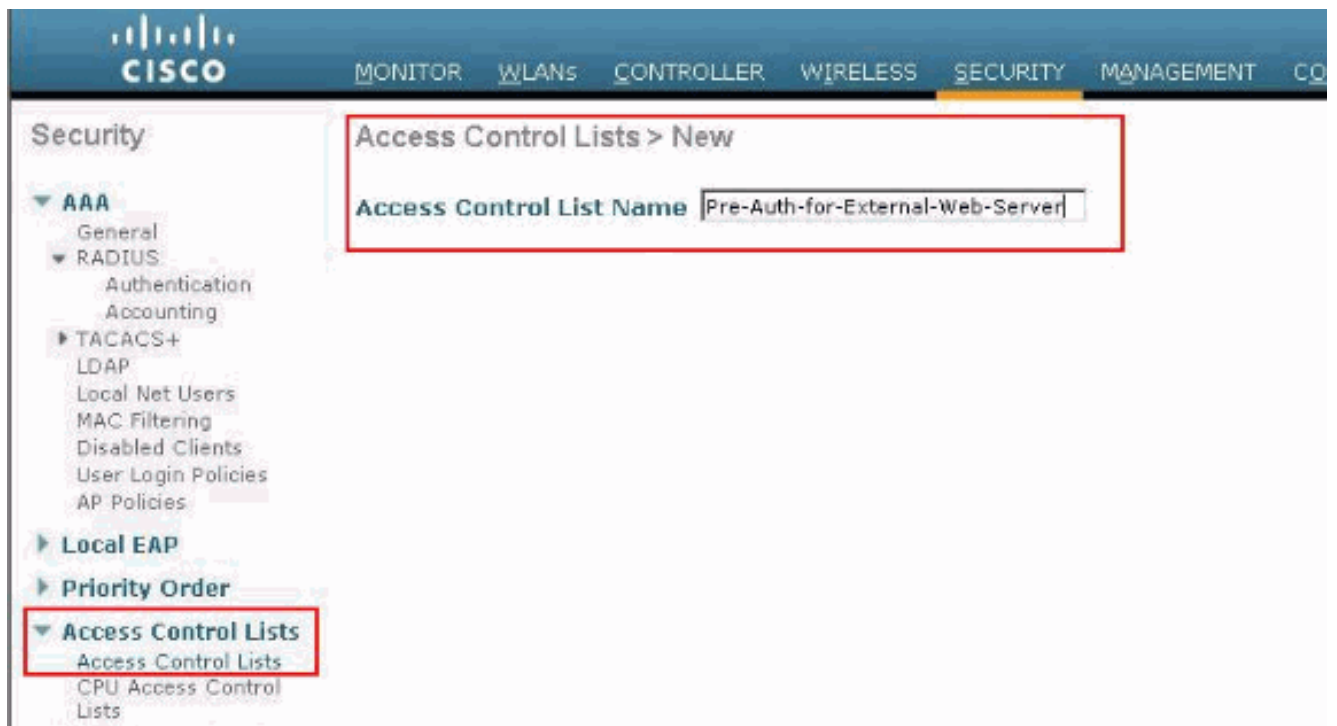
使用外部Web伺服器進行Web驗證時，某些WLC平台需要外部Web伺服器（Cisco 5500系列控制器、Cisco 2100系列控制器、Cisco 2000系列和控制器網路模組）的預驗證ACL。對其他WLC平台，預身份驗證ACL不是強制性的。

但是，使用外部Web驗證時，最好為外部Web伺服器設定預先驗證ACL。

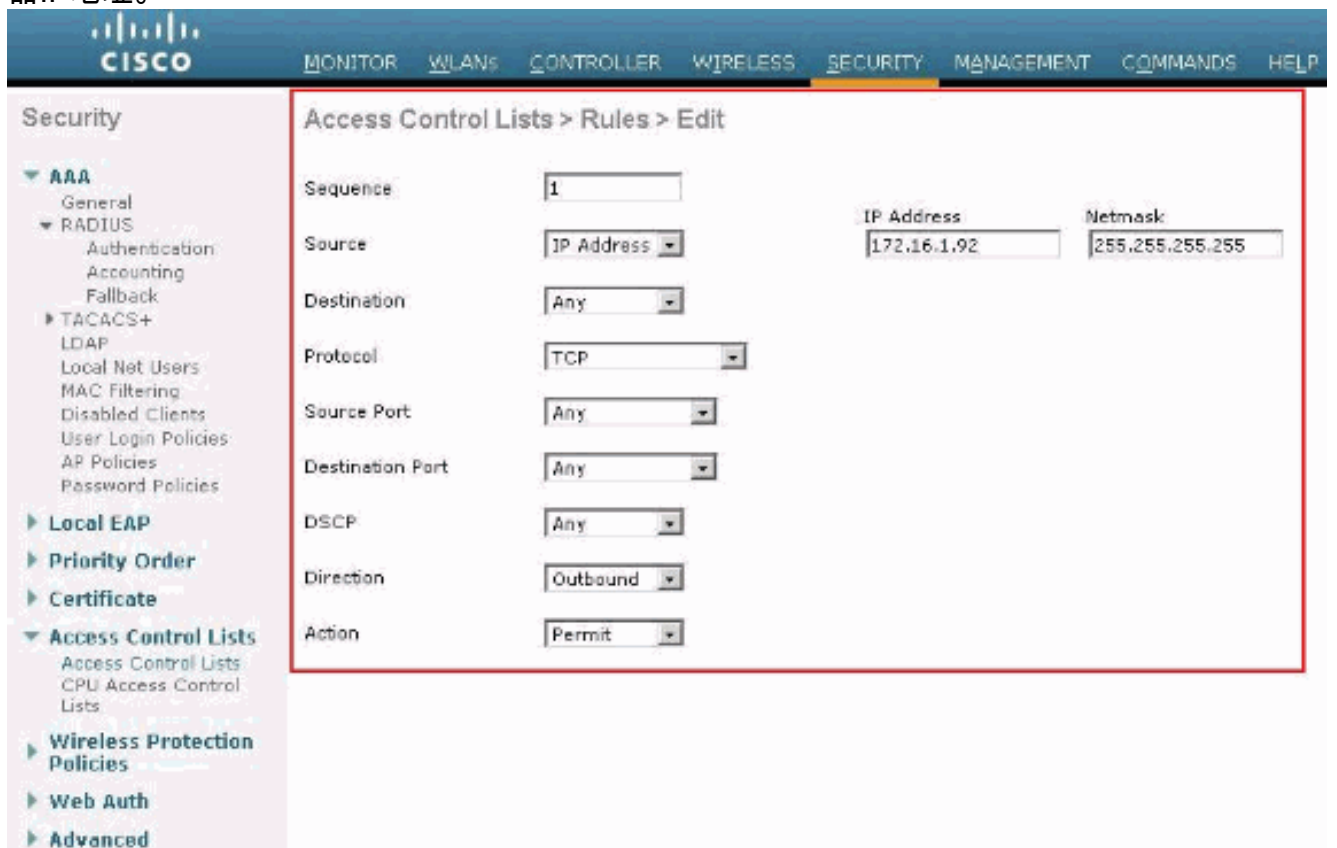
完成以下步驟，以便為WLAN設定預先驗證ACL：

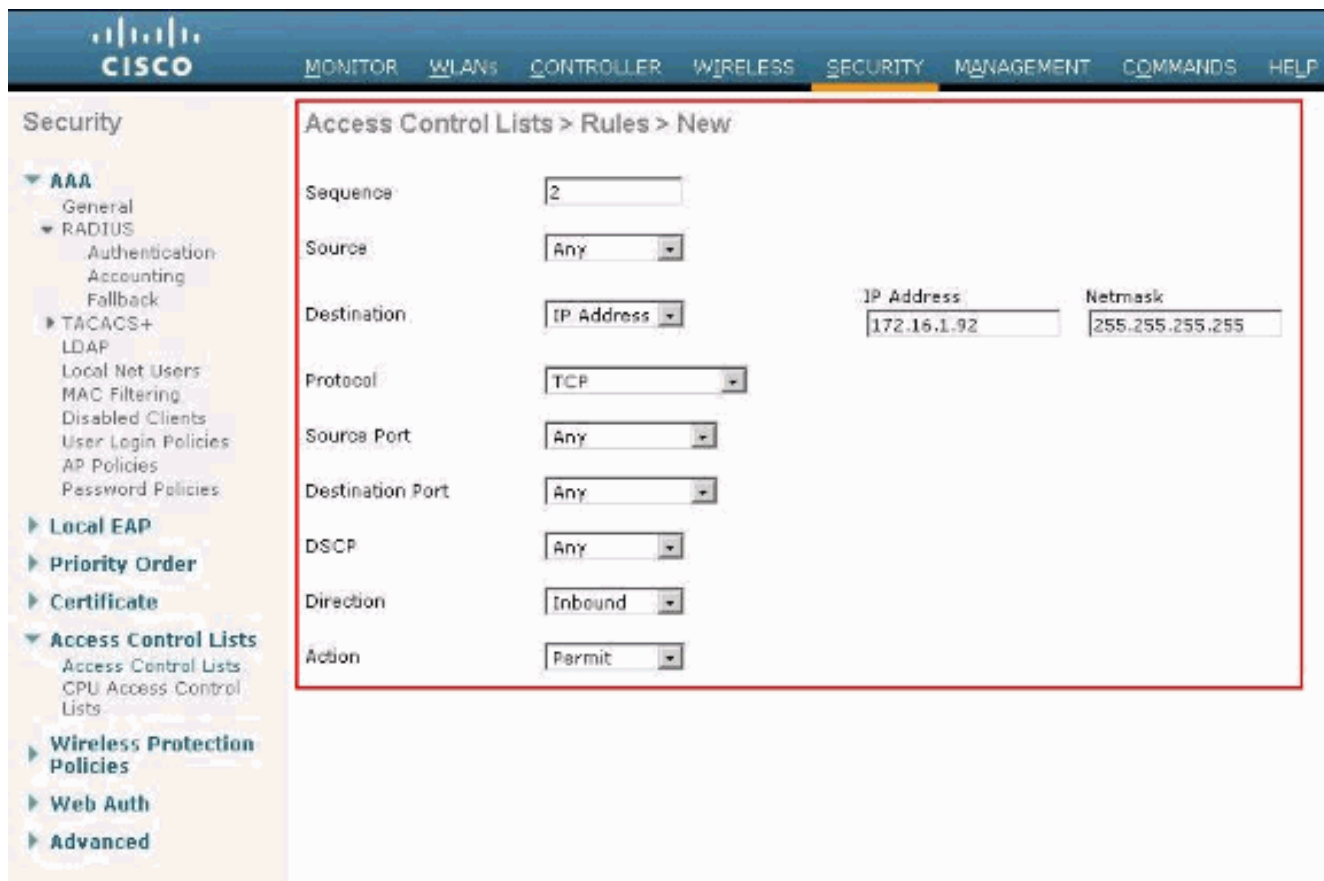
1. 在WLC GUI中選擇**Security > Access Control Lists**。此視窗允許您檢視與標準防火牆ACL類似的當前ACL。
2. 按一下**New**以建立一個新的ACL。
3. 輸入ACL的名稱，然後按一下**Apply**。在本範例中，ACL命名為**Pre-Auth-for-External-Web-Server**。



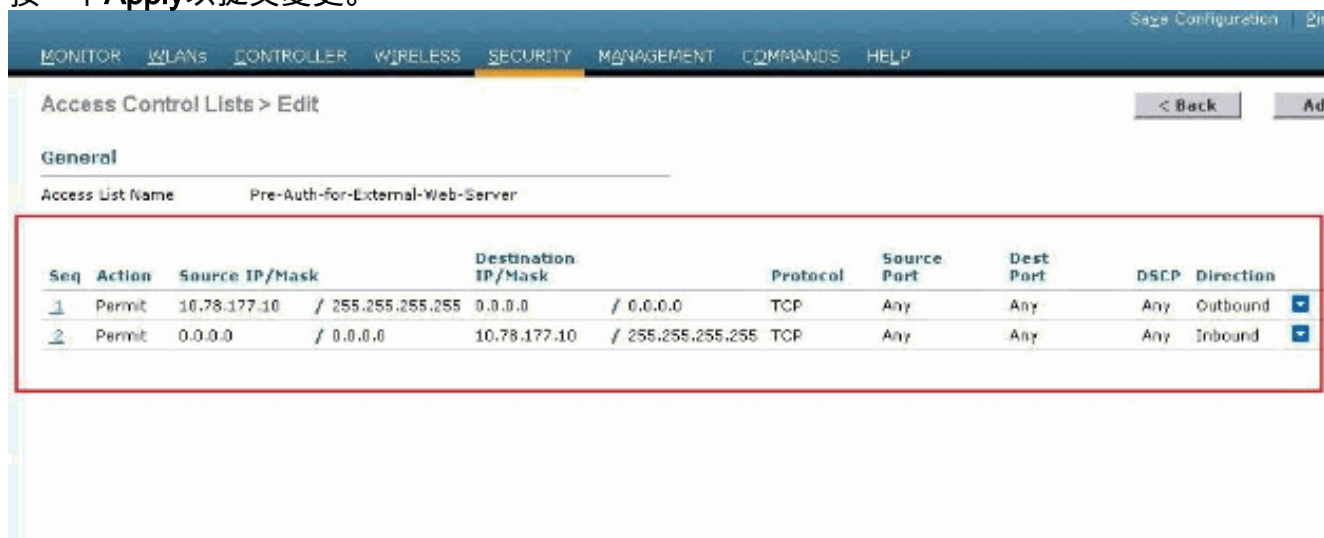


4. 對於建立的新ACL，請點選**Edit**。此時會顯示ACL > Edit視窗。此視窗允許使用者定義新規則或修改現有ACL的規則。
5. 按一下「**Add New Rule**」。
6. 定義允許客戶端訪問外部Web伺服器的ACL規則。在本示例中，172.16.1.92是外部Web伺服器IP地址。





7. 按一下Apply以提交變更。



## 在WLC上為訪客使用者建立本機資料庫

訪客使用者的使用者資料庫可以儲存在無線LAN控制器的本地資料庫中，也可以儲存在控制器的外部。

本檔案中使用控制器上的本機資料庫對使用者進行驗證。您必須建立本地網路使用者並定義Web身份驗證客戶端登入的密碼。完成以下步驟，以便在WLC上建立使用者資料庫：

1. 在WLC GUI中選擇**Security**。
2. 從左側的AAA選單中按一下**Local Net Users**。



The screenshot shows the Cisco SCA interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, and COMMANDS. The left sidebar shows the 'Security' menu with 'Local Net Users' selected. The main content area is titled 'Local Net Users' and contains a table with the following columns: User Name, WLAN Profile, Guest User, Role, and Description.

3. 按一下「New」以建立一個新使用者。此時將顯示一個要求輸入使用者名稱和密碼資訊的新視窗。
4. 輸入使用者名稱和密碼以建立新使用者，然後確認要使用的密碼。此示例建立名為User1的使用者。
5. 如果您選擇，請新增說明。此示例使用Guest User1。
6. 按一下「Apply」以儲存新使用者組態。

The screenshot shows the 'Local Net Users > New' configuration form. The form fields are as follows:

User Name	User1
Password	.....
Confirm Password	.....
Guest User	<input checked="" type="checkbox"/>
Lifetime (seconds)	86400
Guest User Role	<input type="checkbox"/>
WLAN Profile	Guest
Description	GuestUser1

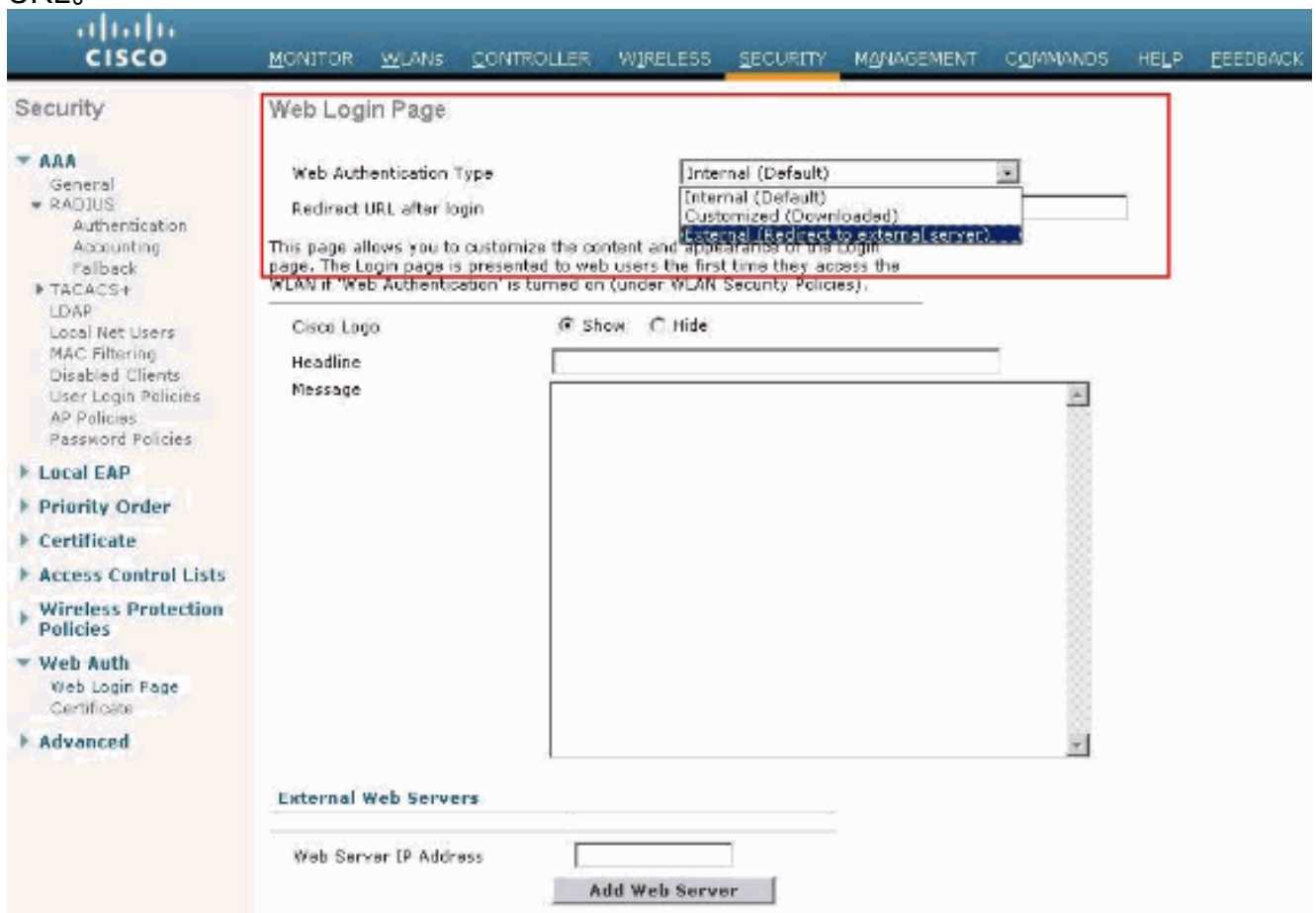


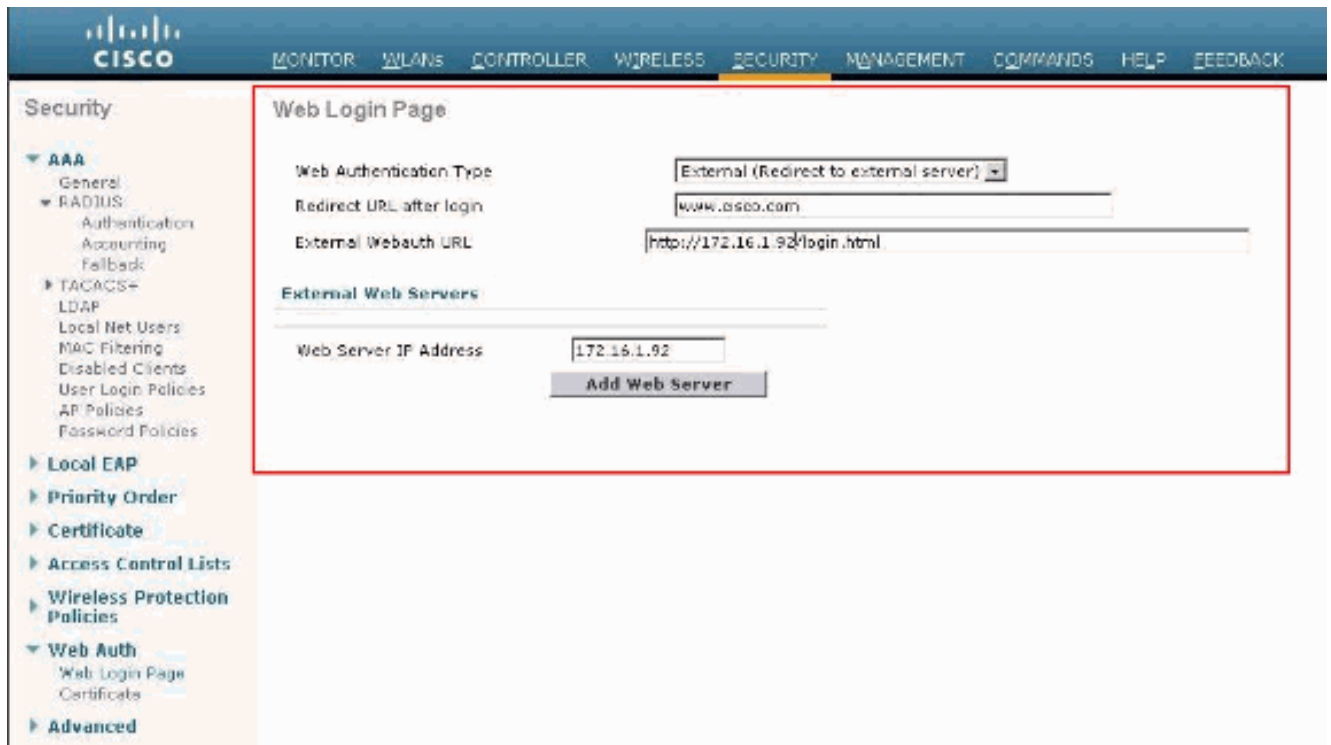
7. 重複步驟3-6，向資料庫新增更多使用者。

## 設定WLC以進行外部Web驗證

下一步是為外部Web驗證設定WLC。請完成以下步驟：

1. 在控制器GUI上，選擇**Security > Web Auth > Web Login Page**以存取Web Login Page。
2. 在「Web Authentication Type」下拉框中選擇**External(Redirect to external server)**。
3. 在「外部Web伺服器」部分，新增新的外部Web伺服器。
4. 在「登入後重新導向URL」欄位中，輸入在成功驗證時將終端使用者重新導向到的頁面的URL。在「External Web Auth URL」欄位中，輸入登入頁面儲存在外部Web伺服器上的URL。



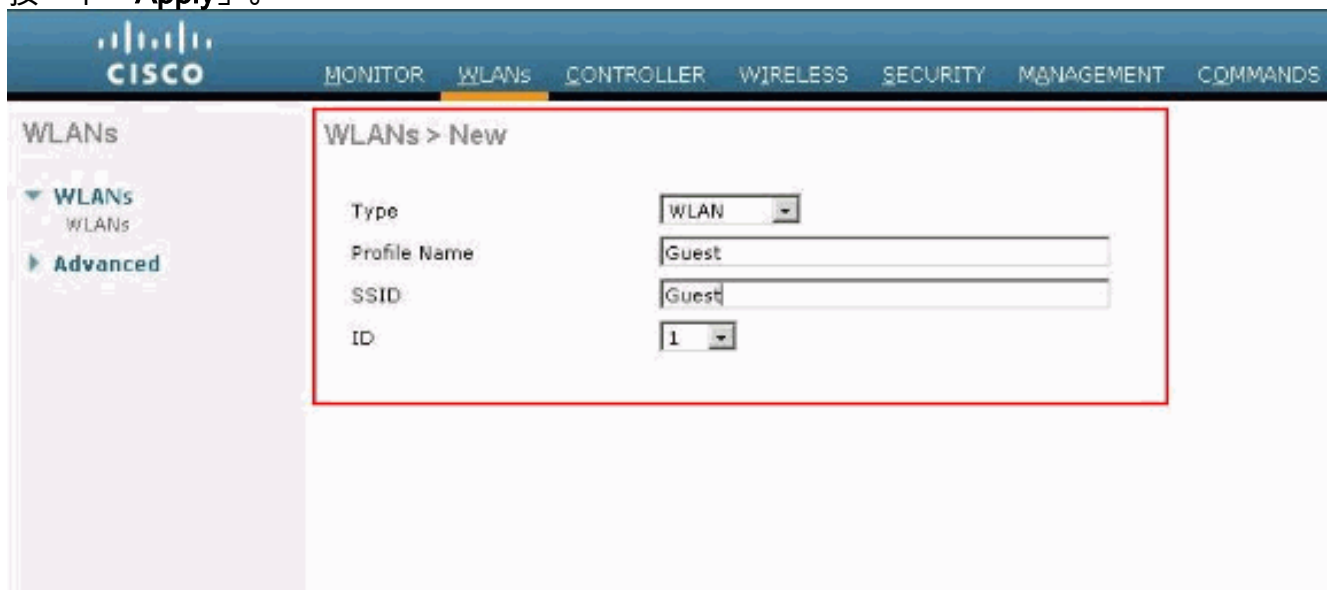


注意：在WLC 5.0及更新版本中，也可自訂Web驗證的註銷頁面。有關如何配置它的詳細資訊，請參閱無線LAN控制器組態設定指南5.2的[每WLAN分配登入、登入失敗和登出頁面](#)一節。

## 為訪客使用者配置WLAN

最後一步是為訪客使用者建立WLAN。請完成以下步驟：

1. 在控制器GUI上按一下「**WLANs**」以建立WLAN。出現WLANs視窗。此視窗列出控制器上設定的WLAN。
2. 按一下**New**以設定新的WLAN。在本範例中，WLAN命名為**Guest**,WLAN ID為**1**。
3. 按一下「**Apply**」。



4. 在WLAN > Edit視窗中，定義特定於WLAN的引數。對於訪客WLAN，在General頁籤中，從Interface Name欄位選擇適當的介面。此範例將先前建立的動態介面**guest**對應到WLAN **guest**。

The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The main heading is 'WLANs > Edit 'Guest''. The left sidebar shows 'WLANs' and 'Advanced' options. The main content area has tabs for 'General', 'Security', 'QoS', and 'Advanced'. The 'General' tab is active and contains the following configuration items:

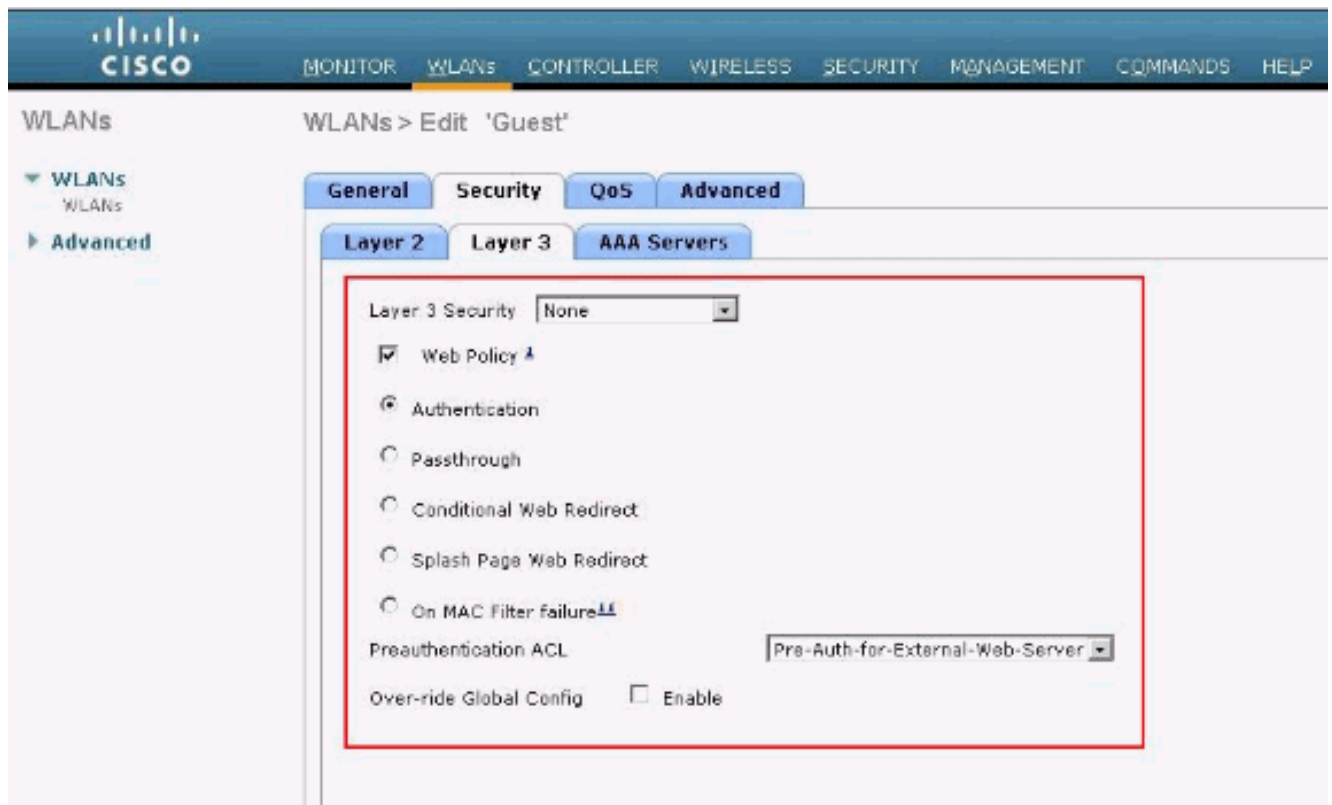
Profile Name	Guest
Type	WLAN
SSID	Guest
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	Web-Auth (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	guest
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

轉到「安全」頁籤。在Layer 2 Security下，本示例中選擇None。注意：802.1x身份驗證不支援Web身份驗證。這表示使用Web驗證時，不能選擇802.1x或具有802.1x的WPA/WPA2作為第2層安全性。所有其他第2層安全引數都支援Web驗證。

The screenshot shows the Cisco WLAN configuration interface, specifically the 'Security' tab for the 'Guest' profile. The top navigation bar is the same as in the previous screenshot. The main heading is 'WLANs > Edit 'Guest''. The left sidebar shows 'WLANs' and 'Advanced' options. The main content area has tabs for 'General', 'Security', 'QoS', and 'Advanced'. The 'Security' tab is active and contains sub-tabs for 'Layer 2', 'Layer 3', and 'AAA Servers'. The 'Layer 2' sub-tab is active and contains the following configuration items:

Layer 2 Security	None
	<input type="checkbox"/> 802.1x MAC Filtering

在Layer 3 Security欄位中，選中Web Policy覈取方塊並選擇Authentication選項。之所以選擇此選項，是因為使用Web驗證來驗證無線訪客使用者端。從下拉選單中選擇適當的預身份驗證ACL。在本範例中，使用先前建立的預先驗證ACL。按一下「Apply」。



## 驗證

無線客戶端啟動，使用者在Web瀏覽器中輸入URL，例如www.cisco.com。由於使用者尚未通過驗證，因此WLC會將使用者重新導向到外部Web登入URL。

系統將提示使用者輸入使用者憑證。使用者提交使用者名稱和密碼後，登入頁面取得使用者憑證輸入，在提交時將要求傳回WLC Web伺服器的action\_URL範例http://1.1.1.1/login.html。提供此項目是要作為客戶重新導向URL的輸入參數，其中1.1.1.1是交換器上的虛擬介面位址。

WLC會根據WLC上設定的本機資料庫驗證使用者的身分。驗證成功後，WLC Web伺服器會將使用者轉送到已設定的重新導向URL或使用者端用來啟動的URL，例如www.cisco.com。

**Security Alert**

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

- ⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
- ✔ The security certificate date is valid.
- ✔ The security certificate has a valid name matching the name of the page you are trying to view.

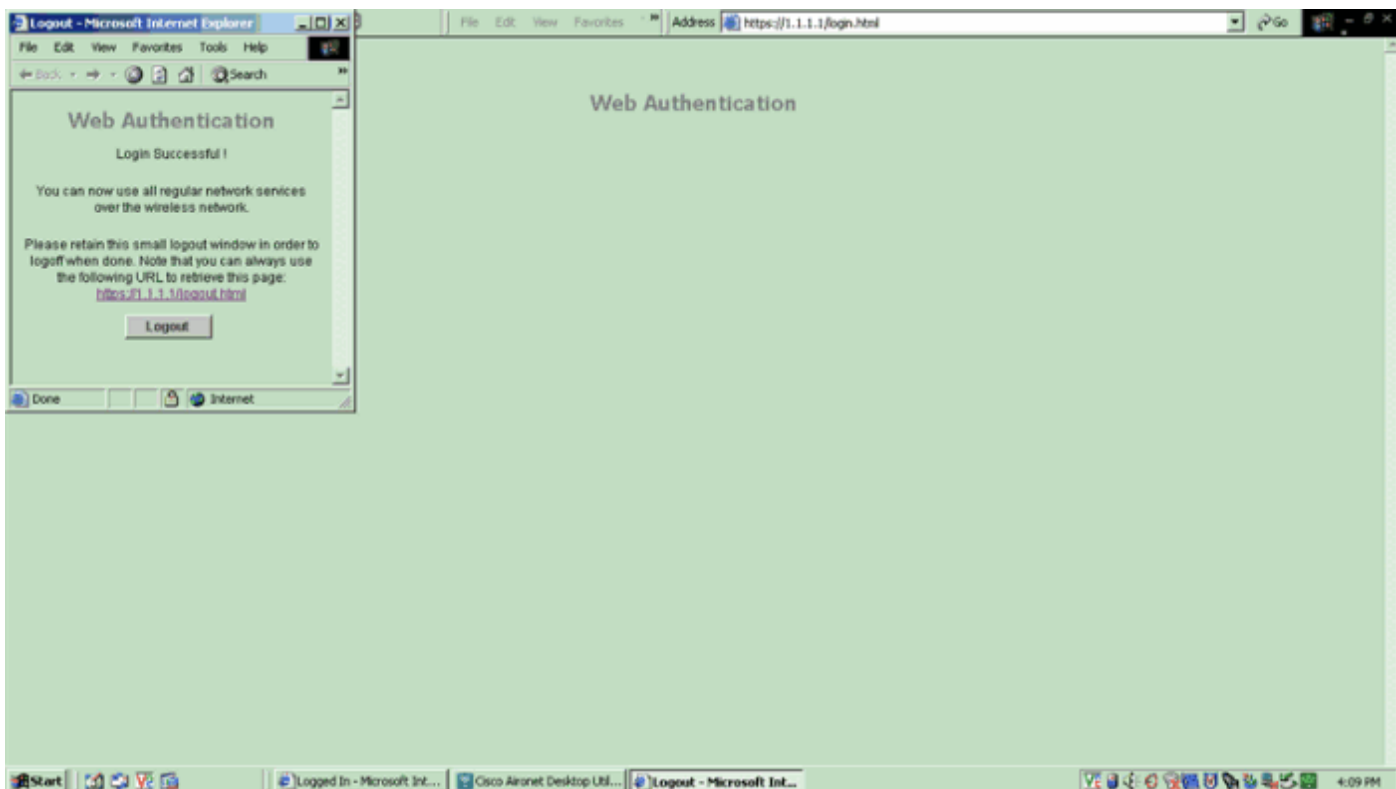
Do you want to proceed?

# Web Authentication

User Name

Password





## 疑難排解

使用這些debug指令可對組態進行疑難排解。

- debug mac addr <client-MAC-address xx:xx:xx:xx:xx:xx>
- debug aaa all enable
- debug pem state enable
- debug pem events enable
- debug dhcp message enable
- debug dhcp packet enable
- debug pm ssh-appgw enable
- debug pm ssh-tcp enable

使用本節內容，對組態進行疑難排解。

## [已重定向到外部Web身份驗證伺服器的客戶端收到證書警告](#)

**問題：**將使用者端重新導向到思科的外部Web驗證伺服器時，會收到憑證警告。伺服器上有一個有效的憑證，如果您直接連線到外部Web驗證伺服器，系統不會收到憑證警告。這是因為WLC的虛擬IP位址(1.1.1.1)會呈現給使用者端，而不是與憑證相關聯的外部Web驗證伺服器的實際IP位址？

**解決方案：**是。無論您執行本機還是外部Web驗證，您仍會按控制器上的內部Web伺服器。重新導向到外部Web伺服器時，除非控制器本身上有有效的憑證，否則您仍會收到控制器傳來的憑證警告。如果將重新導向傳送到https，除非控制器和外部Web伺服器都擁有有效的憑證，否則您會收到憑證警告。

若要一起清除憑證警告，需要發出根級憑證並將其下載到控制器上。系統會為主機名核發憑證，並將該主機名放在DNS主機名框中，位於控制器上的虛擬介面下。您還需要將主機名新增到本地DNS伺服器，並將其指向WLC的虛擬IP地址(1.1.1.1)。

如需詳細資訊，請參閱[在WLAN控制器\(WLC\)上產生第三方憑證的憑證簽署請求\(CSR\)](#)。

## 錯誤：「無法顯示頁面」

**問題：**將控制器升級到4.2.61.0後，當您使用下載的網頁進行Web驗證時，會顯示「page cannot be displayed」錯誤訊息。在升級之前，這種方法運行良好。預設的內部網頁載入沒有任何問題。

**解決方案：**從WLC 4.2及更新版本引入新功能，其中您可以有多個截斷的登入頁面用於Web驗證。

若要正確載入網頁，在**Security > Web Auth > Web login page**中，將Web驗證型別設定為**global customized**是不夠的。也必須在特定的WLAN上設定。為此，請完成以下步驟：

1. 登入WLC的GUI。
2. 按一下**WLANs**索引標籤，然後存取針對Web驗證設定的WLAN設定檔。
3. 在WLAN > Edit頁面上，按一下**Security**頁籤。然後，選擇**第3層**。
4. 在此頁面上，選擇**None**作為Layer 3 Security。
5. 選中**Web Policy**框，然後選擇**Authentication**選項。
6. 勾選**Over-ride Global Config Enable**方塊，選擇**Customized(Downloaded)**作為Web Auth Type，然後從Login Pagepull下拉選單中選擇所需的登入頁面。按一下「**Apply**」。

## 相關資訊

- [無線 LAN 控制器 Web 驗證組態範例](#)
- [影片：思科無線LAN控制器\(WLC\)上的Web驗證](#)
- [無線 LAN 控制器上的 VLAN 組態範例](#)
- [無線LAN控制器和輕量型存取點基本組態範例](#)
- [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）。