

# WAP125和WAP581的1.0.1版本中的功能

## 目標

本文旨在重點介紹和概述此無線接入點(WAP)韌體更新中的最新功能。

## 適用裝置

- WAP125
- WAP581

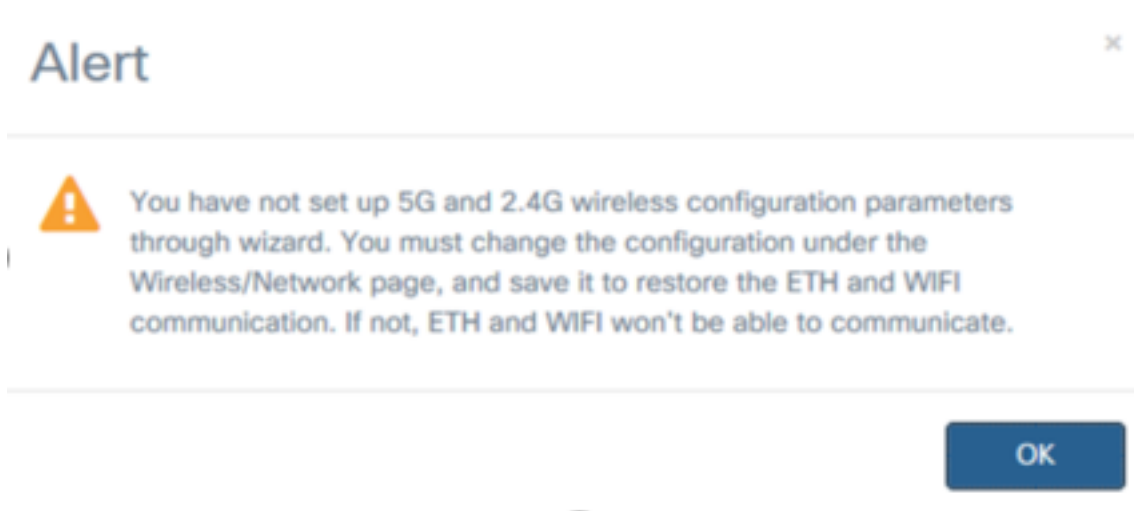
## 軟體版本

- 1.0.1

## 安裝嚮導

在WAP125和WAP581的早期版本中，如果取消安裝嚮導，您將從WAP註銷。

1.0.1韌體允許您取消安裝嚮導。系統將向您傳送警報。



確認警報後，您可以為WAP設定本地密碼。

## Change Password

You may also change the username. A valid username contains 1-32 alphanumeric, hyphens, or underscore characters.

Username:

For security reasons, you should change the password from its default settings.

The minimum requirements are as follows:

- \* Cannot be the same as the user name.
- \* Cannot be the same as the current password.
- \* Minimum length is 8.
- \* Minimum number of character classes is 3.

Character classes are upper case, lower case, numeric, and special characters.

Old Password:

New Password:

Confirm Password:

Password Strength Meter  Below Minimum

Password Complexity:  Disable

您可以在其他時間手動配置所有設定。

## 移動最佳化設定嚮導

WAP125和WAP581裝置現在包括針對流動裝置最佳化的管理頁面、強制網路門戶頁面和設定嚮導。

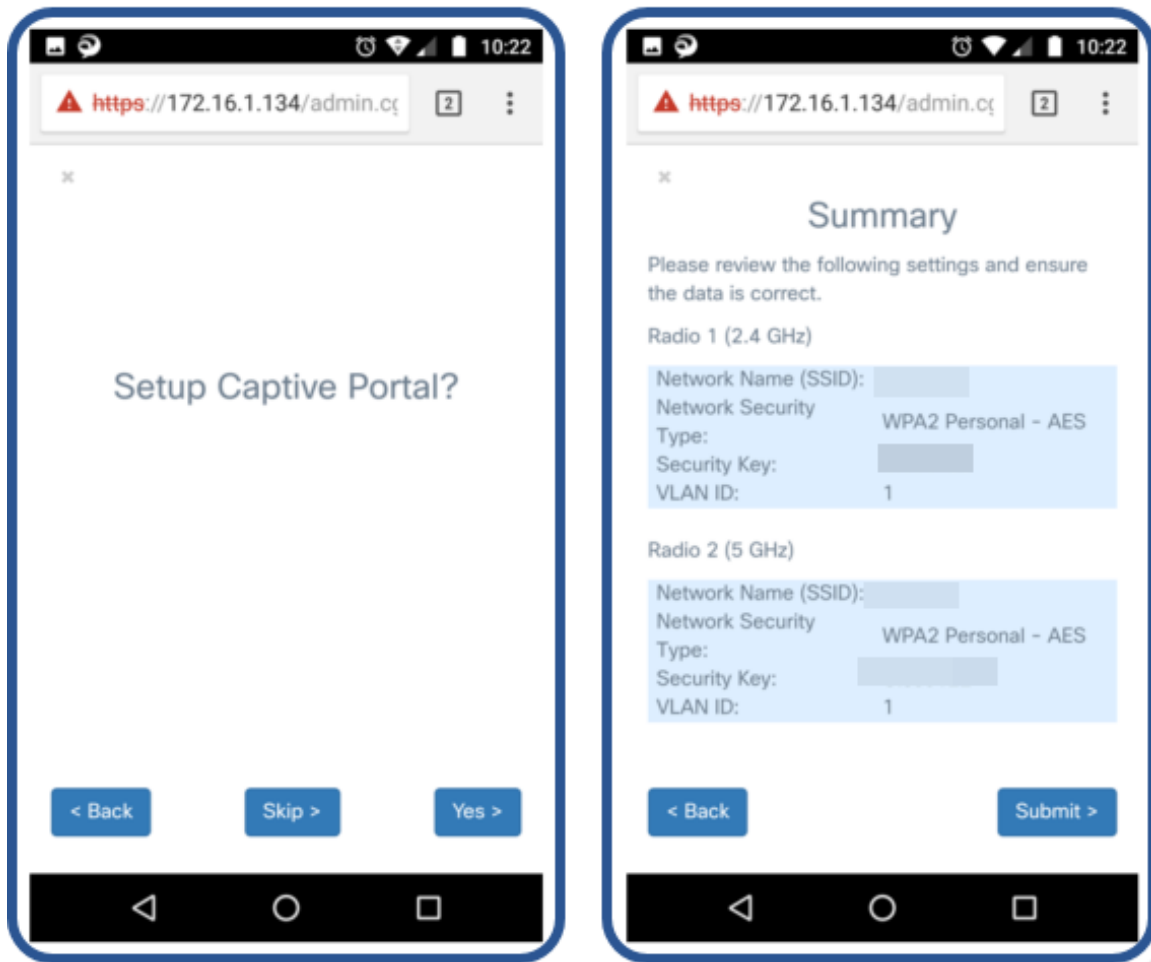
您可以使用新的移動最佳化設定頁面通過流動裝置運行設定嚮導來配置WAP。

連線到ciscoSB-Setup SSID並轉到WAP的IP地址或預設IP 192.168.1.245配置裝置。



移動最佳化頁面上的安裝嚮導與標準頁面上的安裝嚮導相同。





## 第三方訪客驗證

第三方訪客身份驗證允許您使用Facebook或Google身份驗證（由第三方驗證的安全身份驗證）配置訪客網路。WAP125允許一個訪客接入例項，而WAP581允許多個例項。

要求:

- Facebook或Google的Internet連線
- 使用者必須擁有或建立一個Facebook或Google帳戶，並且可以通過無線方式訪問其公共檔案
- 在身份驗證完成之前，必須能夠訪問Facebook或Google，以便終端使用者可以登入以驗證其憑據。

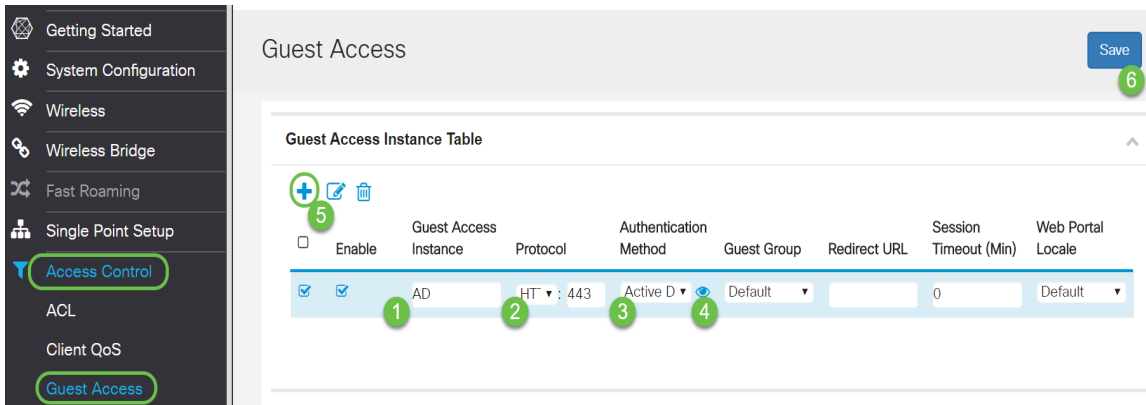
企業還可以選擇在身份驗證之前使用其他站點，如其企業網站。

按一下**Access Control > Guest Access**，然後按一下*plus*符號。

以下每個數字的簡要說明：

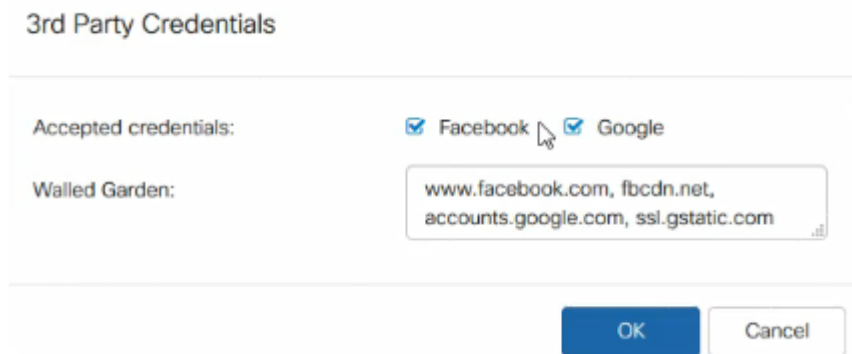
1. 新增Active Directory的名稱
2. 您應將強制網路門戶頁面配置為使用**HTTPS**，而不是HTTP。如果選擇HTTP，則可以通過無線方式以未加密的明文傳輸使用者名稱和密碼，從而無意中暴露使用者名稱和密碼。建議使用安全HTTPS強制網路門戶頁面。
3. 選擇**第三方憑證**。
4. 按一下眼睛的圖形以選擇**接受**的憑證和正確的網站。
5. 如果您選擇新增其他訪客訪問例項，請按一下此處。

## 6. 請務必執行儲存。



Enable	Guest Access Instance	Protocol	Authentication Method	Guest Group	Redirect URL	Session Timeout (Min)	Web Portal Locale
<input checked="" type="checkbox"/>	AD	HT : 443	Active D	Default		0	Default

此示例顯示Facebook和Google已選擇。網站列出的是圍牆花園。

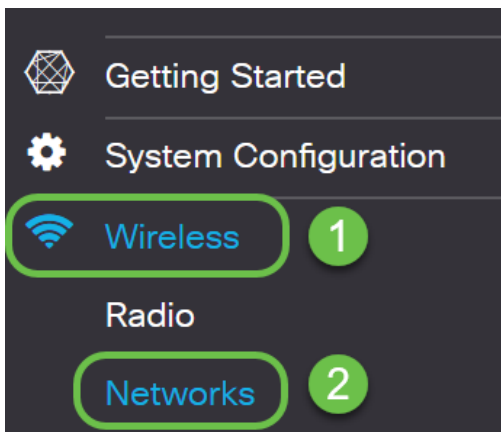


Accepted credentials:  Facebook  Google

Walled Garden: www.facebook.com, fbcdn.net, accounts.google.com, ssl.gstatic.com

OK Cancel

然後，您需要導航到導航窗格中的**無線>網路**，將訪客訪問例項新增或更改為Active Directory的名稱。



**附註：**WAP125允許一個訪客訪問例項，因此您必須決定是否要配置第三方身份驗證或Active Directory身份驗證。WAP581允許多種身份驗證方式。

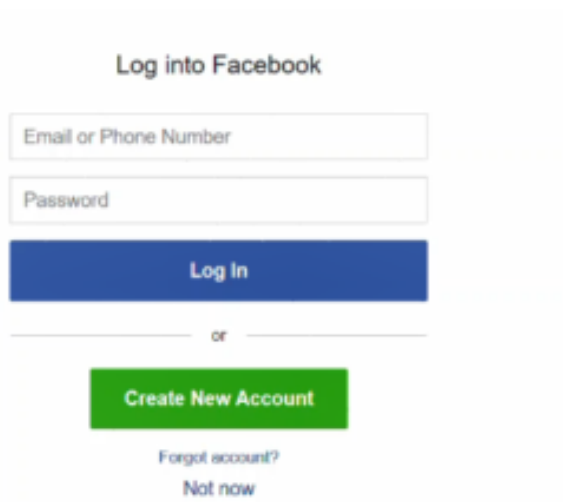
## 第三方客戶端身份驗證

當客戶端按一下以加入無線連線時，強制網路門戶將開啟。在這個例子中，Facebook和Google是選項。客戶需要選中此框以表明他們已閱讀並接受接受使用策略，然後使用Facebook或Google選項登入。

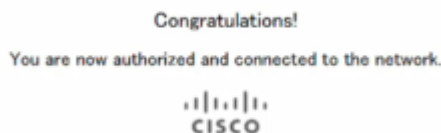
**附註：**首次登入客戶端時，會收到詢問使用者是否要使用強制網路門戶的問題。他們需要選擇yes。



然後，客戶端可以輸入憑證。在本示例中，使用了Facebook。



客戶端現在可以使用Internet。



## Active Directory訪客驗證

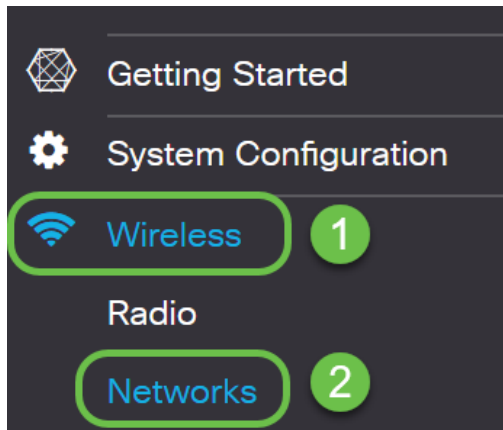
為了支援Active Directory身份驗證，WAP需要與Windows域控制器通訊以提供身份驗證。作為管理員，您最多可以設定三個Windows域控制器以便在WAP581上進行通訊。

按一下**Access Control > Guest Access**，然後按一下**plus**。

以下每個數字的簡要說明：

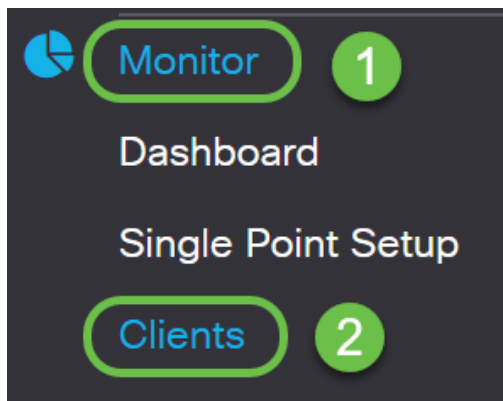
1. 新增Active Directory的名稱
2. 您應將強制網路門戶頁面配置為使用HTTPS，而不是HTTP。如果選擇HTTP，則可以通過無線方式以未加密的明文傳輸使用者名稱和密碼，從而無意中暴露使用者名稱和密碼。建議使用安全HTTPS強制網路門戶頁面。
3. 選擇**Active Directory服務**
4. 按一下**眼睛**的圖形以新增IP地址。您可以從那裡進行測試以檢查連線。
5. 如果您選擇新增其他訪客訪問例項，請按一下此處。
6. 務必儲存。

然後，您需要導航到導航窗格中的**無線>網路**，將訪客訪問例項新增或更改為Active Directory的名稱。



要檢視網路上的客戶端，請在導航窗格中按一下**Monitor > Clients**。

1. *Monitor*顯示連線的客戶端數
2. 客戶端顯示客戶機的詳細資訊。如果要保留連線人員的記錄，可以匯出這些記錄。



有關如何監視訪客的詳細資訊，請按一下[此處](#)。

## Active Directory客戶端身份驗證

當客戶端位於Active Directory中時，它們能夠登入到WAP以訪問Internet。當他們選擇無線接入點時，根據他們使用的Web瀏覽器，他們可能會收到類似的警告消息。如果受信任的證書頒發機構沒有為該頁面分配證書，則會出現警告。使用者端需要按一下**ADVANCED**。



## Your connection is not private

Attackers might be trying to steal your information from [redacted] .net (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID

Automatically send some [system information and page content](#) to Google to help detect dangerous apps and sites. [Privacy policy](#)

ADVANCED

BACK TO SAFETY

客戶端隨後可能會收到類似以下內容的警告消息：

This server could not prove that it is [redacted] .net; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to [redacted] .net (unsafe)

已啟動門戶頁面。在此頁面上，他們應輸入他們的身份證明，並勾選此框以表明他們已經閱讀並接受了接受使用策略。

他們將收到歡迎資訊，並能夠安全地使用網際網路。



Congratulations!

You are now authorized and connected to the network.



現在，您已經熟悉了最新WAP125和WAP581更新附帶的一些最新功能。  
有關這些功能和其他新功能的詳細資訊，請按一下下面的隨附文章連結。

[使用WAP125或WAP581上的安裝嚮導](#)

[使用流動裝置上的WAP125或WAP581安裝嚮導](#)

[如何：Cisco Umbrella整合](#)

[如何：Cisco CloudShark整合](#)

[如何：在WAP<sup>125</sup>或WAP581上配置第三方身份驗證設定](#)

[如何：Microsoft Active Directory訪客身份驗證](#)

[如何：Umbrella — 如果丟失了API金鑰則註冊新裝置](#)

[自定義強制網路門戶的外觀](#)

## 檢視與本文相關的影片.....

[按一下此處檢視思科的其他技術對話](#)