

在WAP125接入點上配置訪客訪問例項表

目標

WAP125接入點的訪客接入功能為裝置範圍內的臨時無線客戶端提供無線連線。它的工作原理是讓接入點廣播兩個不同的服務集識別符號(SSID):一個用於主網路，另一個用於訪客網路。然後，訪客將被重定向到強制網路門戶，要求他們輸入其憑證。實際上，這樣可以保證主網路安全，同時仍然允許訪客訪問網際網路。

在WAP125基於Web的實用程式的「訪客訪問例項表」中配置強制網路門戶的設定（如會話超時和重定向統一資源定位器[URL]）。訪客訪問功能在酒店和辦公大堂、餐館和商場中特別有用。

本文旨在展示如何配置WAP125接入點的訪客接入例項表。假設已配置Web門戶區域設定表和訪客組表的設定。有關配置這兩種設定的說明，請按一下[此處](#)。

適用裝置

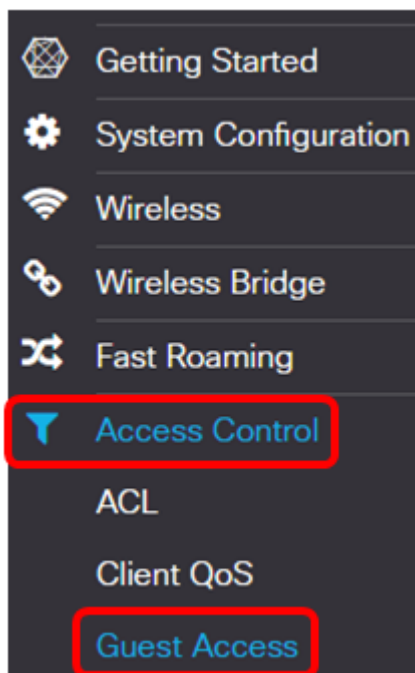
- WAP125

軟體版本

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

配置訪客訪問例項表

步驟1.登入到WAP125的基於Web的實用程式，然後選擇**Access Control > Guest Access**。



附註：本文中的圖片取自WAP125。選單選項可能會因裝置型號而異。

步驟2.驗證是否已選中Guest Access Instance **Enable** 覆取方塊以確保訪客訪問處於活動狀態

。

Enable	Guest Access Instance	Protocol
<input checked="" type="checkbox"/>	CiscoTest	HTT ▼ : 80

步驟3.在 *Guest Access Instance* 欄位中輸入例項的名稱。最多可包含32個字母數字字元。

Enable	Guest Access Instance	Protocol
<input checked="" type="checkbox"/>	CiscoTest	HTT ▼ : 80

附註：在此範例中，輸入CiscoTest。

步驟4.為訪客訪問例項選擇協定。選項包括：

- HTTP — 此選項也稱為超文本傳輸協定(HTTP)。它在驗證請求的網頁期間不提供加密。
- HTTPS — 此選項也稱為超文本傳輸協定安全(HTTPS)。這意味著電腦與其所聯絡的網站之間的所有通訊均經過加密。

Protocol
HTT ▼ : 80
<input checked="" type="radio"/> HTTP
<input type="radio"/> HTTPS

附註：在此範例中，選擇HTTP。

步驟5.在「協定」欄位旁輸入埠號。當協定到達伺服器時，埠號有助於識別協定。

Guest Access Instance	Protocol
CiscoTest	HTT ▼ : 80

附註：在此示例中，輸入80。

步驟6.從Authentication Method下拉選單中選擇身份驗證方法。當客戶端通過強制網路門戶進行身份驗證時，接入點將使用此功能。選項包括：

- 本地資料庫 — 此選項允許WAP裝置從本地儲存的檔案驗證使用者的憑據。如果選擇此選項，請完成[步驟7](#)到[步驟10](#)，然後繼續配置[Guest Group Table](#)。
- RADIUS驗證 — 此選項允許存取點透過遠端驗證撥入使用者服務(RADIUS)伺服器驗證使用者。如果選擇此選項，請完成[步驟7](#)到[步驟10](#)，然後繼續配置[RADIUS身份驗證](#)。
- No Authentication — 此選項禁用身份驗證，並允許無線客戶端連線到訪客網路而不輸入其憑據。如果選擇此選項，請跳至[步驟11](#)。

Authentication Method	Guest Group
Local Da ▾	Default ▾
Local Database	
Radius Authentication	
No Authentication	

附註：在本示例中，選擇了[本地資料庫]。

步驟7.從Guest Group下拉選單中選擇一個組。

Guest Group
Default ▾
Default

附註：在本示例中，將自動選擇「Default (預設)」。

步驟8.在Redirect URL欄位中輸入憑證後，輸入要重新導向的地址。

Redirect URL	Session Timeout (Min.)
https://www.cis	30

附註：地址應以HTTP或HTTPS開頭。在此範例中，輸入<https://www.cisco.com>。

步驟9.在Session Timeout(Min.)欄位中輸入會話超時前的分鐘數。

Redirect URL	Session Timeout (Min.)	Web Portal Locale
http://www.cisc	30	Cisco_Samr ▾

附註：在此範例中輸入30。

步驟10.從Web門戶區域設定下拉選單中選擇一個Web門戶配置檔案。

Web Portal Locale
Cisco_Samr ▾
Cisco_Sample

附註：在本示例中，會自動選擇Cisco_Sample。有關如何配置Web門戶區域設定的說明，請按一下[此處](#)。

現在應配置訪客訪問例項表。

[配置訪客組表](#)

步驟7.在 *Guest Group Name* 欄位中輸入訪客組的名稱。Guest Group Name最長可為32個字元。

Guest Group Name	Idle Timeout (Min.)
CiscoGuests	5

附註：在此範例中，輸入CiscoGuests。

步驟8.在 *Idle Timeout(Min.)* 欄位中輸入提示超時之前的分鐘數。

Guest Group Name	Idle Timeout (Min.)
CiscoGuests	5

附註：在此範例中輸入5。

步驟9.在 *Maximum Bandwidth Up(Mbps)* 欄位中輸入最大上傳速度。這是無線客戶端在使用強制網路門戶時可以傳送的最大頻寬(Mbps)。最大頻寬可以是0到300，其中0是預設值。

Maximum Bandwidth Up (Mbps)	Maximum Bandwidth Down (Mbps)	Total Guest Users
10	30	2

附註：在此示例中，輸入10。

步驟10.在 *Maximum Bandwidth Down(Mbps)* 欄位中輸入最大下載速度。這是無線客戶端在使用強制網路門戶時可以接收的最大頻寬(Mbps)。最大頻寬可以是0到300，其中0是預設值。

Maximum Bandwidth Up (Mbps)	Maximum Bandwidth Down (Mbps)	Total Guest Users
10	30	2

附註：在此範例中輸入30。

步驟11.按一下「Save」。

Guest Access

Save

Guest Access Instance Table

Enable	Guest Access Instance	Protocol	Authentication Method	Guest Group	Redirect URL	Session Timeout (Min.)	Web Portal Locale
<input checked="" type="checkbox"/>	CiscoTest	HTTP : 80	Local Datab	Default	https://www.cisco.c	15	Cisco_Sample

Guest Group Table

Guest Group Name	Idle Timeout (Min.)	Maximum Bandwidth Up (Mbps)	Maximum Bandwidth Down (Mbps)	Total Guest Users
Default	5	10	30	2

現在應該使用本地資料庫身份驗證配置訪客訪問例項表。

RADIUS 驗證

步驟1.按一下「檢視」按鈕。

Authentication Method

Radius Auth



步驟2.在「安全設定」彈出視窗中，從「RADIUS IP網路」下拉選單中選擇RADIUS IP網路。選項包括：

- IPv4 — 此選項是網路中最常用的IP編址形式。它使用32位格式來標識網路中的主機。
- IPv6 — 此選項是旨在取代IPv4格式的下一代IP地址標準。IPv6使用128位編址系統而不是IPv4中使用的32位系統解決了地址稀缺問題。

Security Setting

RADIUS IP Network:

IPv4

Global RADIUS:

IPv4

IPv6

附註：在此範例中，選擇IPv4。

步驟3. (可選) 選中Global RADIUS **Enable** 覆取方塊，使強制網路門戶使用另一組RADIUS伺服器。

Security Setting

RADIUS IP Network:	IPv4
Global RADIUS:	<input checked="" type="checkbox"/> Enable
RADIUS Accounting:	<input type="checkbox"/> Enable
Server IP Address-1: ?	
Server IP Address-2: ?	
Key-1: ?	
Key-2: ?	

OK

Cancel

附註：啟用時，不需要配置安全設定區域的其它配置。繼續執行[步驟9](#)。在此範例中，全域RADIUS已啟用。

步驟4. (可選) 選中RADIUS Accounting **Enable** 覈取方塊以讓接入點跟蹤和測量特定使用者已使用的資源，例如系統時間和傳輸和接收的資料量。

Security Setting

RADIUS IP Network:	IPv4
Global RADIUS:	<input type="checkbox"/> Enable
RADIUS Accounting:	<input checked="" type="checkbox"/> Enable
Server IP Address-1: ?	10.10.100.123
Server IP Address-2: ?	10.10.100.124
Key-1: ?
Key-2: ?

OK

Cancel

步驟5. (可選) 在 *Server IP Address-1* 欄位中輸入主RADIUS伺服器的IPv4或IPv6地址。

Security Setting

RADIUS IP Network:	IPv4
Global RADIUS:	<input type="checkbox"/> Enable
RADIUS Accounting:	<input checked="" type="checkbox"/> Enable
Server IP Address-1: ?	10.10.100.123
Server IP Address-2: ?	10.10.100.124
Key-1: ?
Key-2: ?

附註：在此示例中，輸入了10.10.100.123。

步驟6。（可選）在*Server IP Address-2*欄位中輸入備份RADIUS伺服器的IPv4或IPv6地址。

Security Setting

RADIUS IP Network:	IPv4
Global RADIUS:	<input type="checkbox"/> Enable
RADIUS Accounting:	<input checked="" type="checkbox"/> Enable
Server IP Address-1: ?	10.10.100.123
Server IP Address-2: ?	10.10.100.124
Key-1: ?
Key-2: ?

附註：在此示例中，輸入了10.10.100.124。

步驟7。（可選）在*Key-1*欄位中輸入接入點用於驗證主RADIUS伺服器的密碼。此欄位中的條目區分大小寫，並且必須與主RADIUS伺服器上配置的條目匹配。金鑰最多可包含63個字母數字字元。

Security Setting

RADIUS IP Network:	IPv4
Global RADIUS:	<input type="checkbox"/> Enable
RADIUS Accounting:	<input checked="" type="checkbox"/> Enable
Server IP Address-1: ?	10.10.100.123
Server IP Address-2: ?	10.10.100.124
Key-1: ?
Key-2: ?

OK

Cancel

步驟8。(可選)在Key-2欄位中輸入接入點用於驗證輔助RADIUS伺服器的密碼。此欄位中的條目區分大小寫，並且必須與主RADIUS伺服器上配置的條目匹配。金鑰最多可包含63個字母數字字元。

Security Setting

RADIUS IP Network:	IPv4
Global RADIUS:	<input type="checkbox"/> Enable
RADIUS Accounting:	<input checked="" type="checkbox"/> Enable
Server IP Address-1: ?	10.10.100.123
Server IP Address-2: ?	10.10.100.124
Key-1: ?
Key-2: ?

OK

Cancel

步驟9.按一下OK。

Security Setting

RADIUS IP Network:

Global RADIUS: Enable

RADIUS Accounting: Enable

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

步驟10.按一下「Save」。

WAP125-wap5e0940

Guest Access

Guest Access Instance Table

Enable	Guest Access Instance	Protocol	Authentication Method	Guest Group	Redirect URL	Session Timeout (Min.)	Web Portal Locale	
<input checked="" type="checkbox"/>	CiscoTest	HTTP	80	Local Data	Default	https://www.cisco.c	15	Cisco_Sample

Guest Group Table

Guest Group Name	Idle Timeout (Min.)	Maximum Bandwidth Up (Mbps)	Maximum Bandwidth Down (Mbps)	Total Guest Users
Default	5	10	30	2

現在應該使用RADIUS身份驗證方法配置訪客訪問例項表。