

WAP321接入點上的強制網路門戶例項配置

目標

強制網路門戶允許您阻止連線到WAP網路的客戶端。客戶端在允許正常使用Internet之前，會看到用於身份驗證的特殊網頁。強制網路門戶驗證適用於訪客和經過身份驗證的使用者，通過將Web瀏覽器轉換為身份驗證裝置來使用。強制網路門戶例項是一組已定義的配置，用於對WAP網路上的客戶端進行身份驗證。可以配置不同的例項（最多兩個），在使用者嘗試訪問關聯的虛擬接入點時，以不同的方式響應使用者。許多Wi-Fi熱點都使用強制網路門戶，向使用者收取訪問網際網路的費用。

本文檔介紹如何在WAP321接入點上配置強制網路門戶全域性配置。

適用裝置

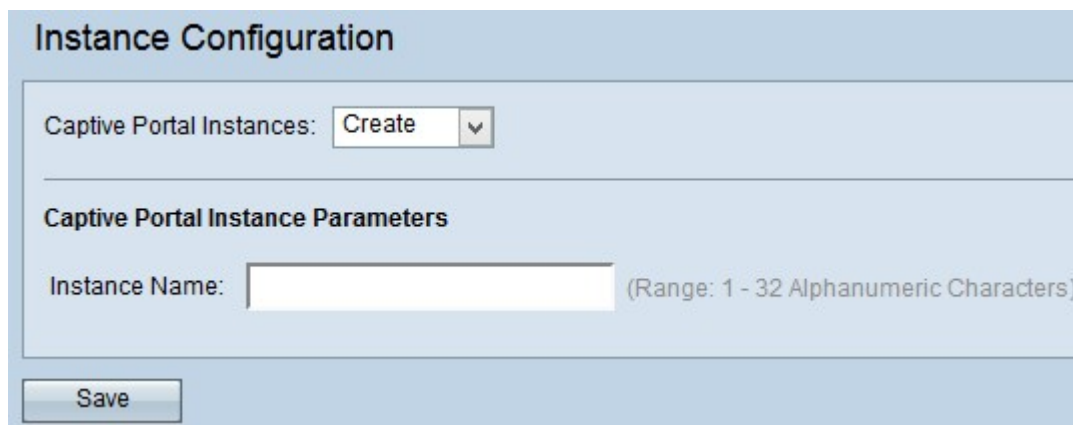
·WAP321

軟體版本

•1.0.3.4

強制網路門戶例項配置

步驟1.登入到Web配置實用程式，然後選擇Captive Portal > Instance Configuration。此時將開啟「例項配置」頁：



步驟2.如果要建立新配置，請從Captive Portal Instances下拉選單中選擇**Create**。要編輯當前配置，請從下拉選單中選擇當前例項並跳至步驟5。

附註：最多可以建立兩個配置。

步驟3.在「例項名稱」欄位中輸入配置的名稱。範圍是1到32個字母數字字元。

Instance Configuration

Captive Portal Instances: ▼

Captive Portal Instance Parameters

Instance Name: (Range: 1 - 32 Alphanumeric Characters)

步驟4.按一下**Save**以儲存所做的變更。該頁面會重新顯示，其中包含用於例項配置的其它欄位。

Instance Configuration

Captive Portal Instances: instance2 ▼

Captive Portal Instance Parameters

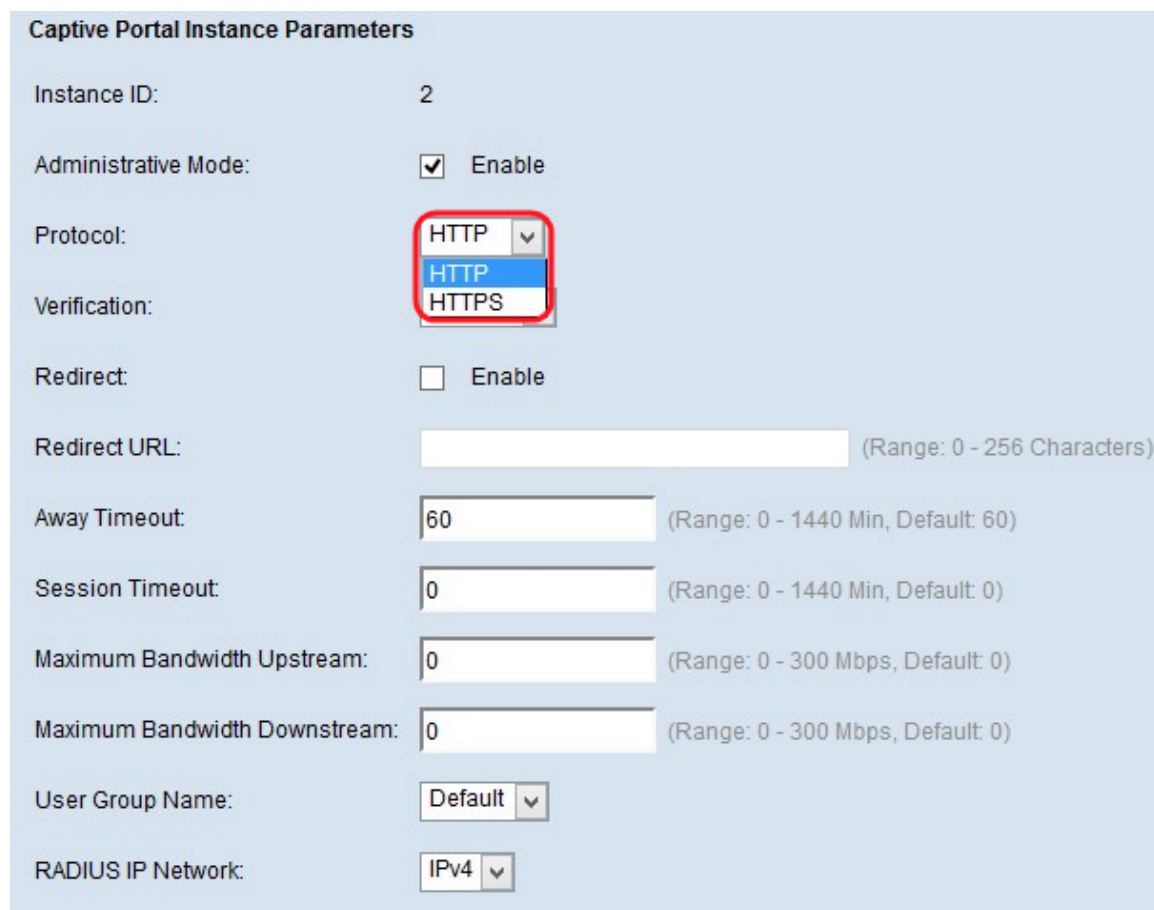
Instance ID:	2
Administrative Mode:	<input checked="" type="checkbox"/> Enable
Protocol:	HTTP ▼
Verification:	Guest ▼
Redirect:	<input type="checkbox"/> Enable
Redirect URL:	<input type="text"/> (Range: 0 - 256 Characters)
Away Timeout:	60 (Range: 0 - 1440 Min, Default: 60)
Session Timeout:	0 (Range: 0 - 1440 Min, Default: 0)
Maximum Bandwidth Upstream:	0 (Range: 0 - 300 Mbps, Default: 0)
Maximum Bandwidth Downstream:	0 (Range: 0 - 300 Mbps, Default: 0)
User Group Name:	Default ▼
RADIUS IP Network:	IPv4 ▼
Global RADIUS:	<input checked="" type="checkbox"/> Enable
RADIUS Accounting:	<input type="checkbox"/> Enable
Server IP Address-1:	<input type="text"/> (xxx.xxx.xxx.xxx)
Server IP Address-2:	<input type="text"/> (xxx.xxx.xxx.xxx)
Server IP Address-3:	<input type="text"/> (xxx.xxx.xxx.xxx)
Server IP Address-4:	<input type="text"/> (xxx.xxx.xxx.xxx)
Key-1:	<input type="text"/> (Range: 1 - 63 Characters)
Key-2:	<input type="text"/> (Range: 1 - 63 Characters)
Key-3:	<input type="text"/> (Range: 1 - 63 Characters)
Key-4:	<input type="text"/> (Range: 1 - 63 Characters)
Locale Count:	0
Delete Instance:	<input type="checkbox"/>

Save

Instance Configuration 頁面包含一些不可配置的欄位，其中顯示以下資訊：

- 例項ID — 指定當前在WAP裝置上配置的CP例項的秩號。
- 區域設定計數 — 指定與例項關聯的區域設定（使用者首選項的語言和國家/地區特定引數集）的數量。

步驟5.選中**Enable**覈取方塊以在Administrative Mode欄位中啟用CP例項。



Captive Portal Instance Parameters

Instance ID: 2

Administrative Mode: Enable

Protocol: **HTTP** (dropdown menu open showing HTTP and HTTPS)

Verification:

Redirect: Enable

Redirect URL: (Range: 0 - 256 Characters)

Away Timeout: (Range: 0 - 1440 Min, Default: 60)

Session Timeout: (Range: 0 - 1440 Min, Default: 0)

Maximum Bandwidth Upstream: (Range: 0 - 300 Mbps, Default: 0)

Maximum Bandwidth Downstream: (Range: 0 - 300 Mbps, Default: 0)

User Group Name: (dropdown)

RADIUS IP Network: (dropdown)

步驟6.在Protocol欄位中選擇希望CP例項用於驗證的協定。可能的值為：

- HTTP — 不加密用於驗證過程的資訊。
- HTTPS — 使用安全套接字層(SSL)，該層要求證書提供身份驗證過程中使用的加密。

Captive Portal Instance Parameters

Instance ID: 2

Administrative Mode: Enable

Protocol: HTTP

Verification: Guest

Redirect:

Redirect URL: (Range: 0 - 256 Characters)

Away Timeout: 60 (Range: 0 - 1440 Min, Default: 60)

Session Timeout: 0 (Range: 0 - 1440 Min, Default: 0)

Maximum Bandwidth Upstream: 0 (Range: 0 - 300 Mbps, Default: 0)

Maximum Bandwidth Downstream: 0 (Range: 0 - 300 Mbps, Default: 0)

User Group Name: Default

RADIUS IP Network: IPv4

Global RADIUS: Enable

步驟7.從Verification下拉選單中選擇用於驗證的CP的驗證方法。身份驗證方法用於拒絕惡意使用者訪問裝置。選擇的驗證方法用於驗證客戶端。可能的值為：

- 訪客 — 不使用任何身份驗證。
- 本地 — 使用本地資料庫進行身份驗證。
- RADIUS — 使用遠端RADIUS伺服器資料庫進行身份驗證。

Verification:	<input type="text" value="Guest"/>	
Redirect:	<input checked="" type="checkbox"/> Enable	
Redirect URL:	<input type="text" value="http://www.example.com"/>	(Range: 0 - 256 Characters)
Away Timeout:	<input type="text" value="75"/>	(Range: 0 - 1440 Min, Default: 60)
Session Timeout:	<input type="text" value="1200"/>	(Range: 0 - 1440 Min, Default: 0)
Maximum Bandwidth Upstream:	<input type="text" value="10"/>	(Range: 0 - 300 Mbps, Default: 0)
Maximum Bandwidth Downstream:	<input type="text" value="300"/>	(Range: 0 - 300 Mbps, Default: 0)
User Group Name:	<input type="text" value="Default"/>	
RADIUS IP Network:	<input type="text" value="IPv4"/>	
Global RADIUS:	<input checked="" type="checkbox"/> Enable	
RADIUS Accounting:	<input type="checkbox"/> Enable	

步驟8.如果要將新驗證的使用者端重新導向到已設定的URL，請勾選Redirect欄位中的**Enable** 覈取方塊。

步驟9.在「Redirect URL」欄位中，輸入首碼為「http://」的URL，新驗證的使用者端將重新導向至該URL。範圍為0到256個字元。

步驟10.在Away Timeout欄位中輸入使用者在自動註銷之前可以保持空閒的時間。如果該值設定為0，則不強制超時。範圍為0至1440分鐘。預設值為60分鐘。

步驟11.在Session Timeout欄位中輸入會話終止之前等待的時間。範圍為0至1440分鐘。預設值為0，表示不實施超時。

步驟12.在Maximum Bandwidth Upstream欄位中輸入客戶端可通過強制網路門戶傳送資料的最大上傳速度。範圍是從0到300 Mbps。預設值為 0。

步驟13.在Maximum Bandwidth Downstream欄位中輸入客戶端可通過強制網路門戶接收資料的最大下載速度。範圍是從0到300 Mbps。預設值為 0。

Verification:	<input type="text" value="Guest"/>	
Redirect:	<input checked="" type="checkbox"/> Enable	
Redirect URL:	<input type="text" value="http://www.example.com"/>	(Range: 0 - 256 Characters)
Away Timeout:	<input type="text" value="75"/>	(Range: 0 - 1440 Min, Default: 60)
Session Timeout:	<input type="text" value="1200"/>	(Range: 0 - 1440 Min, Default: 0)
Maximum Bandwidth Upstream:	<input type="text" value="10"/>	(Range: 0 - 300 Mbps, Default: 0)
Maximum Bandwidth Downstream:	<input type="text" value="300"/>	(Range: 0 - 300 Mbps, Default: 0)
User Group Name:	<input type="text" value="Default"/>	
RADIUS IP Network:	<input type="text" value="Default"/>	
Global RADIUS:	<input checked="" type="checkbox"/> Enable	
RADIUS Accounting:	<input type="checkbox"/> Enable	

步驟14.在User Group Name欄位中選擇所需的組，您要將該組從預配置組的下拉選單分配給CP例項。

RADIUS IP Network:	<input type="text" value="IPv4"/>	
Global RADIUS:	<input checked="" type="checkbox"/> Enable	
RADIUS Accounting:	<input type="checkbox"/> Enable	
Server IP Address-1:	<input type="text"/>	(xxx.xxx.xxx.xxx)
Server IP Address-2:	<input type="text"/>	(xxx.xxx.xxx.xxx)
Server IP Address-3:	<input type="text"/>	(xxx.xxx.xxx.xxx)
Server IP Address-4:	<input type="text"/>	(xxx.xxx.xxx.xxx)
Key-1:	<input type="text"/>	(Range: 1 - 63 Characters)
Key-2:	<input type="text"/>	(Range: 1 - 63 Characters)
Key-3:	<input type="text"/>	(Range: 1 - 63 Characters)
Key-4:	<input type="text"/>	(Range: 1 - 63 Characters)
Locale Count:	<input type="text" value="0"/>	
Delete Instance:	<input type="checkbox"/>	

步驟15.在RADIUS IP Network欄位中選擇Internet協定的型別，CP例項將從RADIUS IP network下拉選單中選擇該型別。可能的值為：

- IPv4 - RADIUS使用者端的位址將位於第四版IP中，其位址格式為xxx.xxx.xxx.xxx(192.0.2.10)。

·IPv6 - RADIUS客戶端的地址將位於IP的第六版，地址格式為xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx(2001:DB8::CAD5:7D91)。

RADIUS IP Network:	IPv4
Global RADIUS:	<input type="checkbox"/> Enable
RADIUS Accounting:	<input checked="" type="checkbox"/> Enable
Server IP Address-1:	192.168.1.250 (xxx.xxx.xxx.xxx)
Server IP Address-2:	192.0.2.10 (xxx.xxx.xxx.xxx)
Server IP Address-3:	192.0.2.11 (xxx.xxx.xxx.xxx)
Server IP Address-4:	192.0.2.12 (xxx.xxx.xxx.xxx)
Key-1: (Range: 1 - 63 Characters)
Key-2: (Range: 1 - 63 Characters)
Key-3: (Range: 1 - 63 Characters)
Key-4: (Range: 1 - 63 Characters)
Locale Count:	0
Delete Instance:	<input type="checkbox"/>

Save

步驟16.如果要使用全域RADIUS伺服器清單進行身份驗證，請選中Global RADIUS欄位中的**Enable**覈取方塊。

時間分配器：如果您選擇全域RADIUS，請跳至步驟22。如果您已啟用「全域性RADIUS」選項，則無需輸入RADIUS伺服器IP，因為CP功能將使用預配置的全域性RADIUS伺服器。

步驟17.如果要追蹤和測量WAP網路上客戶端的時間和資料使用情況，請選中RADIUS Accounting欄位中的**Enable**覈取方塊。

步驟18.在Server IP Address-1欄位中輸入要用作主伺服器的RADIUS伺服器的IP地址。IP地址的格式應為IPv4或IPv6，具體取決於您在步驟15中選擇的RADIUS IP網路。

步驟19。（可選）在Server IP Address-2 to Server IP Address-4欄位中輸入備份RADIUS伺服器IP地址。如果主伺服器的身份驗證失敗，則使用這些伺服器。最多可以配置三個備份IP伺服器，如果前置伺服器發生故障，將依次進行身份驗證。

步驟20.在Key-1欄位中輸入共用金鑰，WAP裝置使用該金鑰向主RADIUS伺服器進行身份驗證。最多可使用63個標準字母數字字元和特殊字元。金鑰區分大小寫。

步驟21。（可選）在Key 2 to 4欄位中輸入共用金鑰，WAP裝置將使用該金鑰向各自的備份RADIUS伺服器進行身份驗證。

Locale Count欄位顯示與當前例項關聯的語言環境數。可以從Web自定義頁面建立三個不同的區域設定並將其分配給每個例項。

步驟22。（可選）如果要刪除當前配置的例項，請選中**Delete Instance**覈取方塊以刪除當前配置的例項。

步驟23. 按一下**Save**以儲存所做的所有變更。