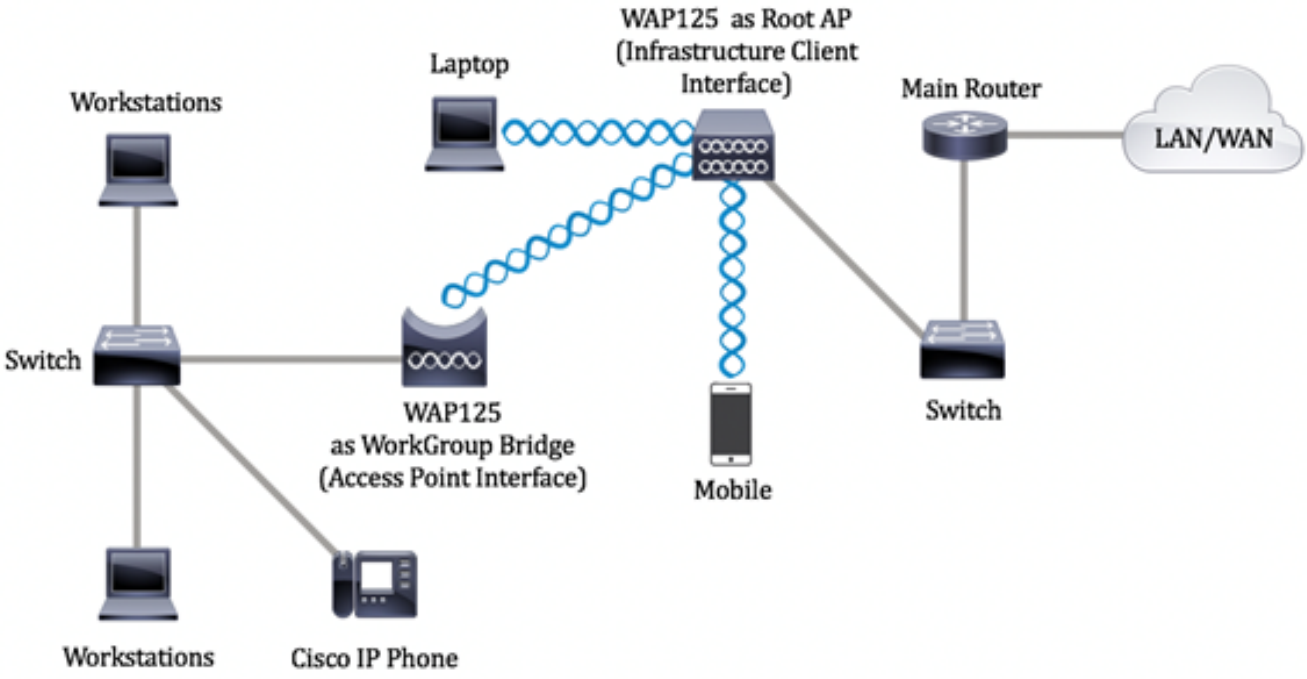
# 在WAP125或WAP581接入點上配置工作組網橋設定

## 目標

WorkGroup Bridge功能使無線接入點(WAP)能夠橋接遠端客戶端與與WorkGroup Bridge模式連線的無線區域網(LAN)之間的流量。與遠端介面關聯的WAP裝置稱為接入點介面，而與無線LAN關聯的WAP裝置稱為基礎設施介面。WorkGroup Bridge允許僅具有有線連線的裝置連線到無線網路。當無線分佈系統(WDS)功能不可用時，建議使用WorkGroup Bridge Mode作為備用模式。

以下拓撲圖說明了一個工作組網橋模型示例。有線裝置與連線到WAP LAN介面的交換機相連。在下面的示例中，WAP125充當連線到基礎設施客戶端介面的接入點介面。




本文提供有關如何在兩個無線接入點之間配置工作組網橋設定的說明。

## 適用裝置

- WAP125
- WAP581

## 軟體版本

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

## 配置工作組網橋設定

在WAP裝置上配置工作組橋之前，請注意以下准則：

- 所有參與工作組網橋的WAP裝置必須具有以下相同的設定：

— 無線電

- IEEE 802.11模式

— 通道頻寬

— 通道（不建議使用自動）

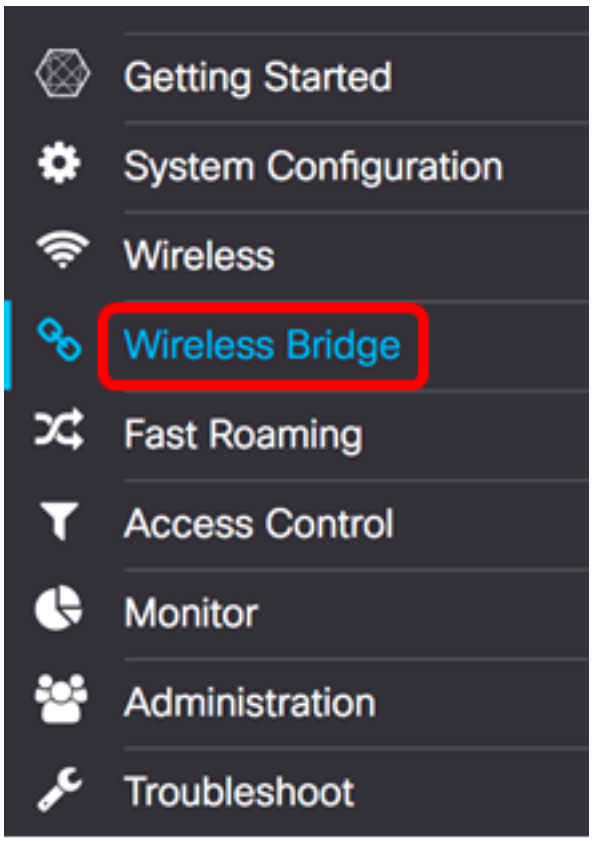
**附註：**要瞭解如何在WAP125上配置這些設定，請按一下此處獲取說明。對於WAP581，請按一下此處。

- 工作組橋接模式當前僅支援IPv4流量。
- 單點設定不支援工作組橋接模式。如果您有WAP581接入點，請先禁用SPS或群集，然後再配置工作組橋接設定。有關如何在WAP上配置SPS設定的說明，請按一下此處。

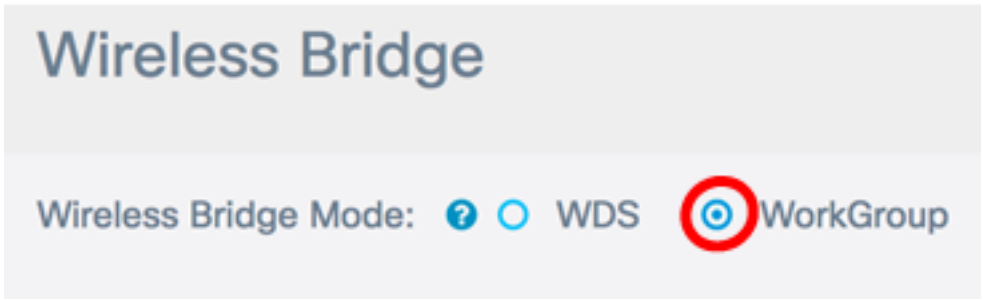
## 配置基礎設施客戶端介面

步驟1.登入到WAP的基於Web的實用程式，然後選擇**Wireless Bridge**。

**附註：**可用選項可能會因裝置的具體型號而異。本示例使用WAP125。



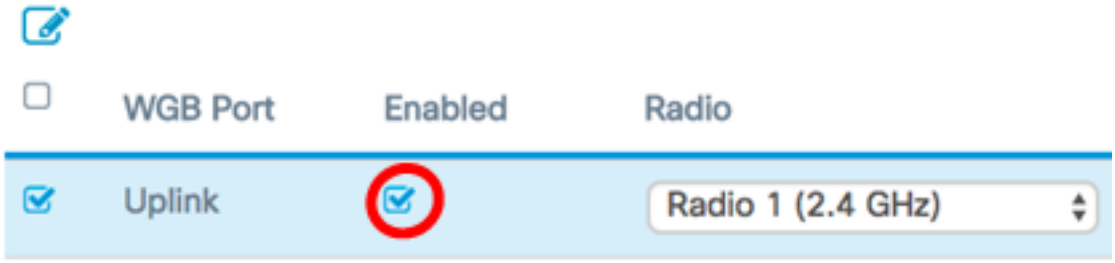

步驟2.按一下**WorkGroup**單選按鈕。



步驟3.選中**Uplink**覈取方塊。


步驟4.按一下**Edit**圖示。


步驟5.選中**Enabled**覈取方塊以啟用基礎設施客戶端介面。




步驟6.選擇工作組網橋的無線電介面。將一個無線電配置為WorkGroup Bridge時，另一個無線電保持運行。無線電介面對應於WAP的無線電頻帶。WAP配備用於在兩個不同的無線電介面上廣播。配置一個無線電介面的設定不會影響另一個無線電介面。


**附註**：在本示例中，選擇無線電2(5 GHz)。

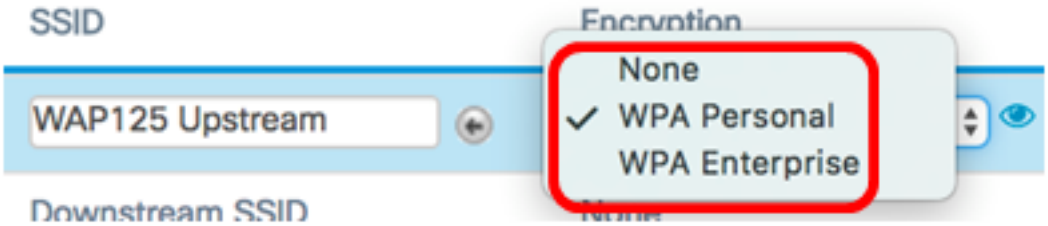
步驟7.在*SSID*欄位中輸入服務集識別符號(SSID)名稱。充當裝置和遠端客戶端之間的連線。您可以輸入2到32個字元作為基礎設施客戶端SSID。

**附註**：在此示例中，使用WAP125 Upstream。


**附註**：SSID旁邊的箭頭可用於SSID掃描。此功能預設處於禁用狀態，只有在無管理AP檢測中

啟用了AP檢測時才會啟用，預設情況下也會禁用AP檢測。

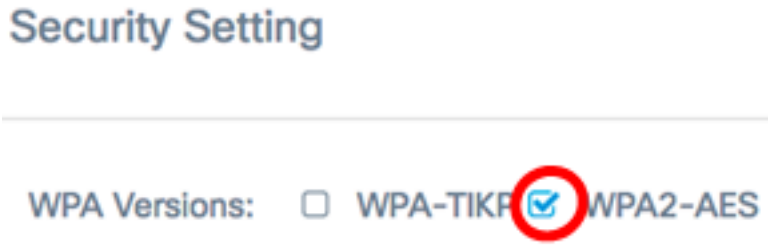
步驟8.從Encryption下拉選單中選擇要作為上游WAP裝置上的客戶端工作站進行身份驗證的安全型別。選項包括：




- 無 — 開啟或無安全性。這是預設設定。如果選擇此選項，請跳至步驟22。
- WPA個人 — WPA個人可以支援長度為8-63個字元的金鑰。建議使用WPA2，因為它具有更強大的加密標準。
- WPA企業 — WPA企業比WPA個人更高級，是推薦的身份驗證安全性。它使用受保護的可擴展身份驗證協定(PEAP)和傳輸層安全性(TLS)。 跳至步驟12進行配置。這種安全型別通常在辦公室環境中使用，需要配置遠端身份驗證撥入使用者服務(RADIUS)伺服器。按一下此處以瞭解有關RADIUS伺服器的詳細資訊。

**附註：**在此示例中，選擇了WPA個人。

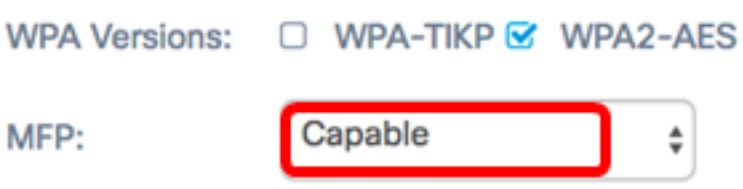
步驟9.按一下該圖  標並選中WPA-TKIP或WPA2-AES覈取方塊，以確定基礎架構客戶端介面將使用的WPA加密型別。




**附註：**如果所有無線裝置都支援WPA2，請將基礎設施客戶端安全設定為WPA2-AES。WPA的加密方法是RC4,WPA2的加密方法是「高級加密標準」(AES)。建議使用WPA2，因為它的加密標準更強大。本範例中使用的是WPA2-AES。

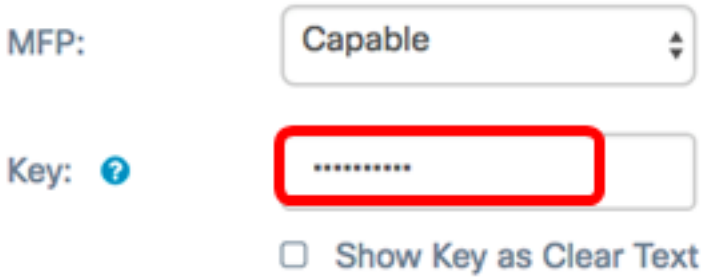
步驟10。（可選）如果在步驟9中選中了WPA2-AES，則從「管理幀保護(MFP)」下拉選單中選擇一個選項，以決定是否希望WAP要求具有受保護的幀。要瞭解有關MFP的更多資訊，請按一下此處。選項包括：

- 不需要 — 禁用MFP的客戶端支援。
- Capable — 允許支援MFP的客戶端和不支援MFP的客戶端加入網路。這是WAP上的預設MFP設定。
- 必需 — 僅當協商了MFP時，才允許客戶端關聯。如果裝置不支援MFP，則不允許它們加入網路。



**附註：**在此範例中，選擇「Capable（能力）」。

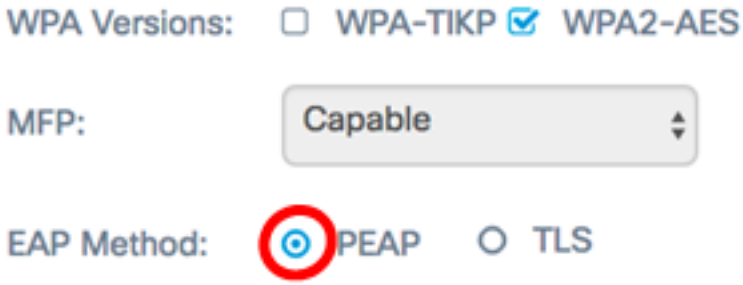
步驟11.在金鑰欄位中輸入WPA加密金鑰。金鑰的長度必須為8-63個字元。這是字母、數字和特殊字元的組合。這是首次連線到無線網路時使用的密碼。然後，跳至步驟21。




步驟12.如果在步驟8中選擇了WPA Enterprise，請按一下EAP方法的單選按鈕。

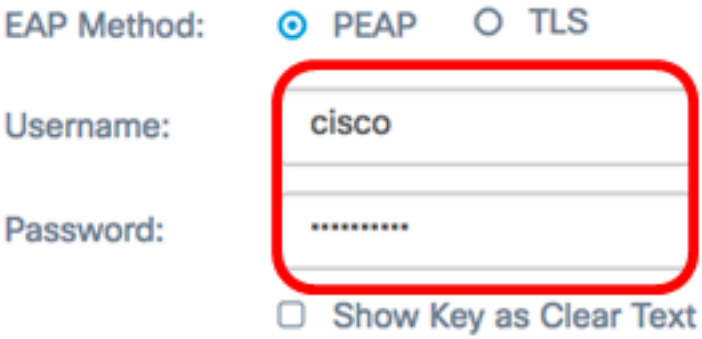
可用選項定義如下：

- PEAP — 此協定為WAP下的每個無線使用者提供支援AES加密標準的個人使用者名稱和密碼。由於PEAP是基於密碼的安全方法，您的Wi-Fi安全基於客戶端的裝置憑證。如果您有弱密碼或不安全的客戶端，PEAP可能會帶來嚴重的安全風險。它依賴TLS，但避免在每個客戶端上安裝數位證書。相反，它通過使用者名稱和密碼提供身份驗證。
- TLS - TLS要求每個使用者具有授予訪問許可權的附加證書。如果您有額外的伺服器和驗證網路使用者身份所需的基礎設施，TLS將更加安全。如果選擇此選項，請跳至步驟14。

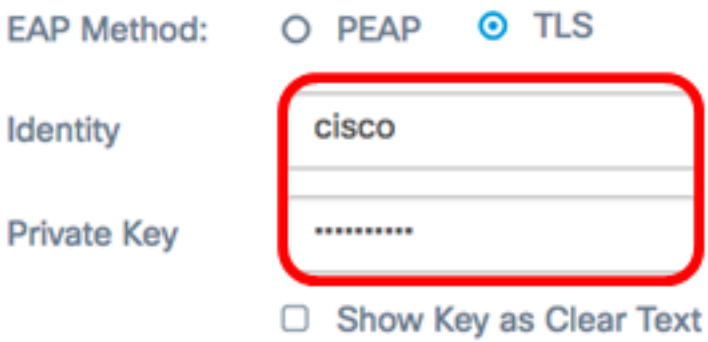



**附註：**在本示例中，選擇了PEAP。

步驟13.在「使用者名稱」和「密碼」欄位中輸入基礎設施客戶端的使用者名稱和密碼。這是用於連線到基礎架構客戶端介面的登入資訊；請參閱您的基礎設施客戶端介面以查詢此資訊。然後，跳至步驟21。




步驟14.如果按一下步驟12中的TLS，請在「身份」和「私鑰」欄位中輸入基礎設施客戶端的身份和私鑰。




步驟15.在傳送方法區域中，按一下以下選項的單選按鈕：

- TFTP — 簡單式檔案傳輸通訊協定(TFTP)是檔案傳輸通訊協定(FTP)的簡化且無安全保護版本。 它主要用於在公司網路之間分發軟體或驗證裝置。如果按一下TFTP，請跳至步驟18。
- HTTP — 超文本傳輸協定(HTTP)提供客戶端可用於提供身份驗證框架的簡單質詢 — 響應身份驗證框架。

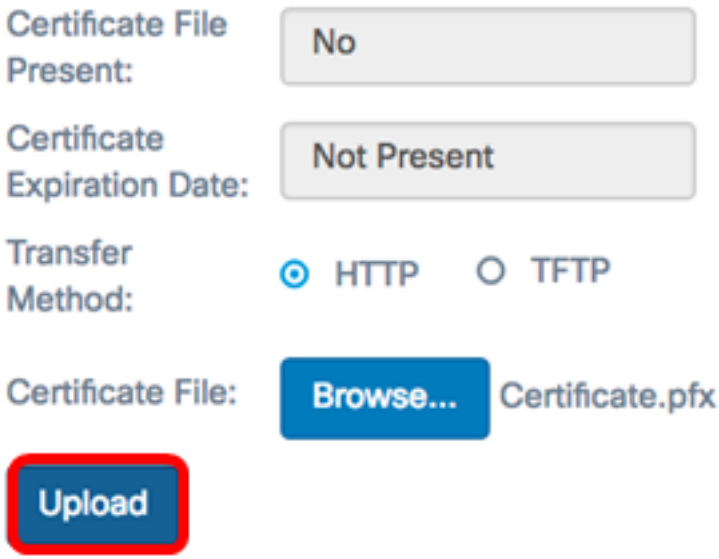

**附註**：如果WAP上已經存在證書檔案，則證書檔案存在和證書到期日期欄位將會填入相關資訊。否則，它們將是空白的。

**HTTP**

步驟16.按一下**Browse**按鈕查詢並選擇證書檔案。檔案必須具有正確的證書副檔名(如.pem或.pfx)，否則將不會接受該檔案。


**附註**：在本示例中，選擇了Certificate.pfx。

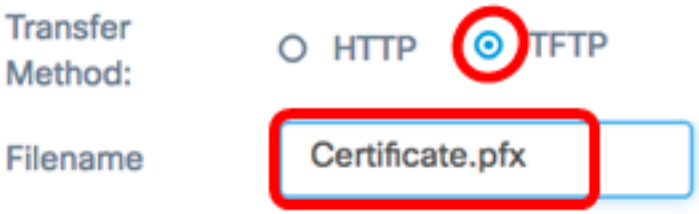
步驟17.按一下**Upload**以上傳選取的憑證檔案。跳至步驟21。




證書檔案存在和證書到期日期欄位將自動更新。

**TFTP**

步驟18。（可選）如果您在步驟15中按一下了TFTP，請在*Filename*欄位中輸入證書文*件的*檔名。




**附註：**在本示例中，使用了Certificate.pfx。

步驟19.在「*TFTP Server IPv4地址」欄位中輸入TFTP伺服器*地址。

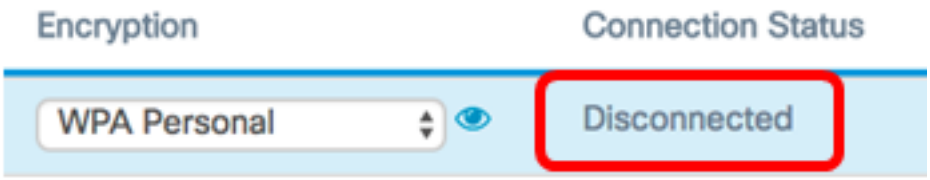

**附註：**在本例中。192.168.100.108用作TFTP伺服器地址。

步驟20.按一下**Upload**按鈕以上傳指定的憑證檔案。

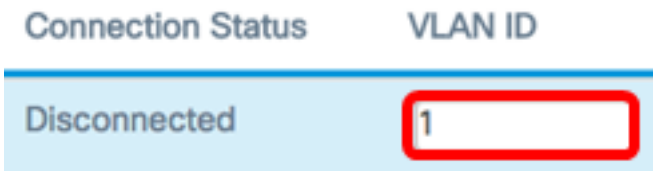

證書檔案存在和證書到期日期欄位將自動更新。

步驟21.按一下**OK**以關閉「安全設定」視窗。


連線狀態區域指示WAP是否連線到上游WAP裝置。

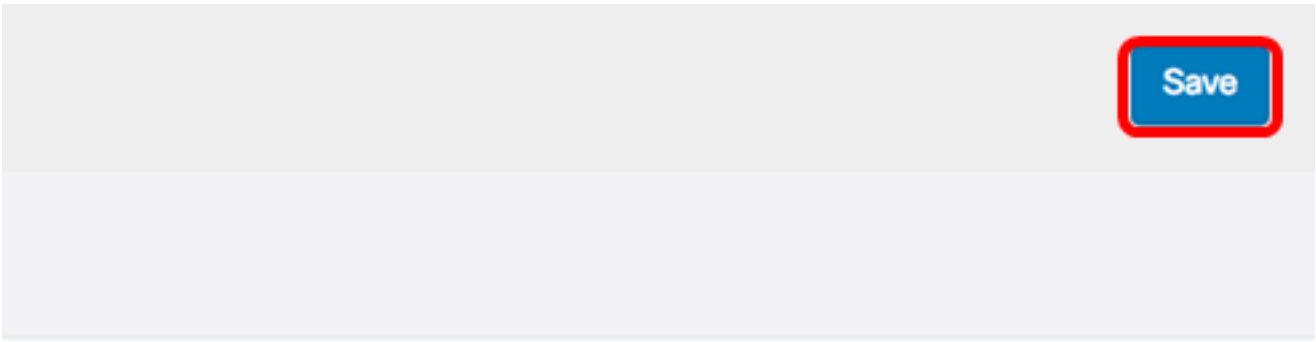



步驟22.輸入基礎設施客戶端介面的VLAN ID。預設值為1。




**附註：**在本例中，使用了預設VLAN ID。

步驟23.按一下**Save**以儲存已設定的設定。



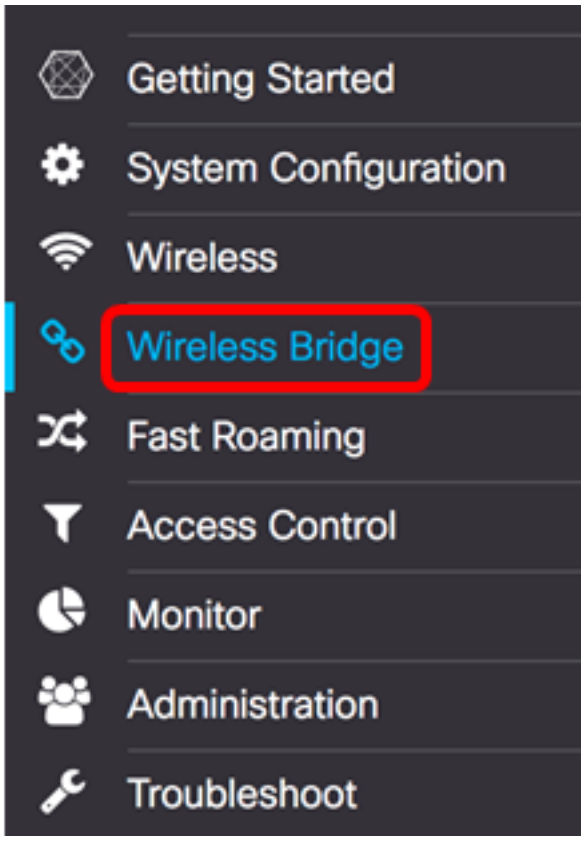

| Connection Status | VLAN ID | SSID Broadcast | Client Filter |
|---|---|---|---|
| Disconnected | 1 | N/A | N/A |
| N/A | 1 | ☑ | Disabled |

現在，您應該已經在WAP上成功配置基礎設施客戶端介面設定。

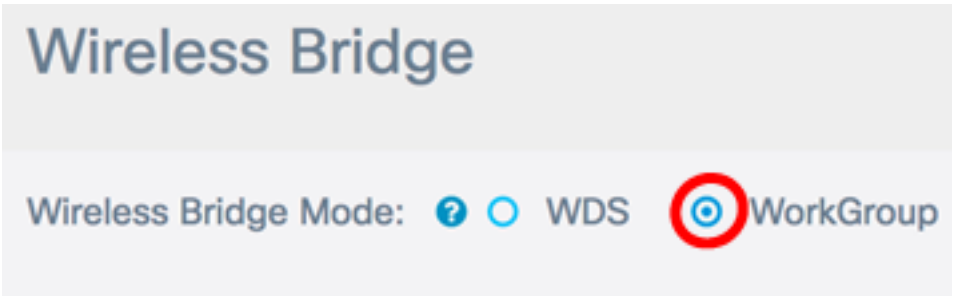
## 配置接入點客戶端介面

步驟1.登入到WAP的基於Web的實用程式，然後選擇**Wireless Bridge**。

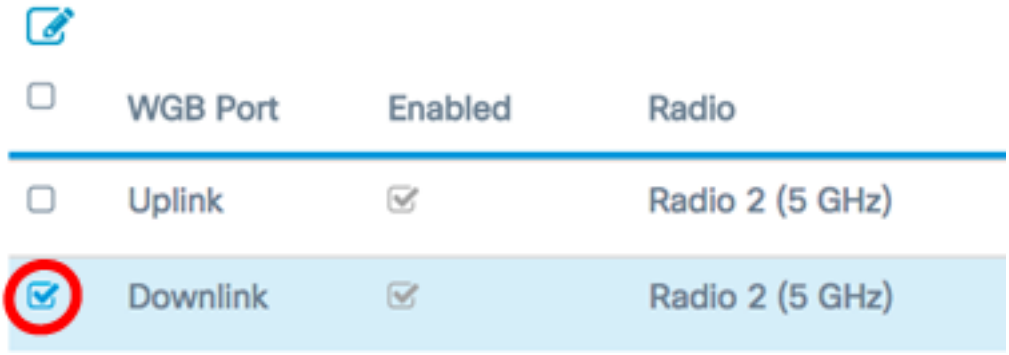
**附註：**可用選項可能會因裝置的具體型號而異。本示例使用WAP125。



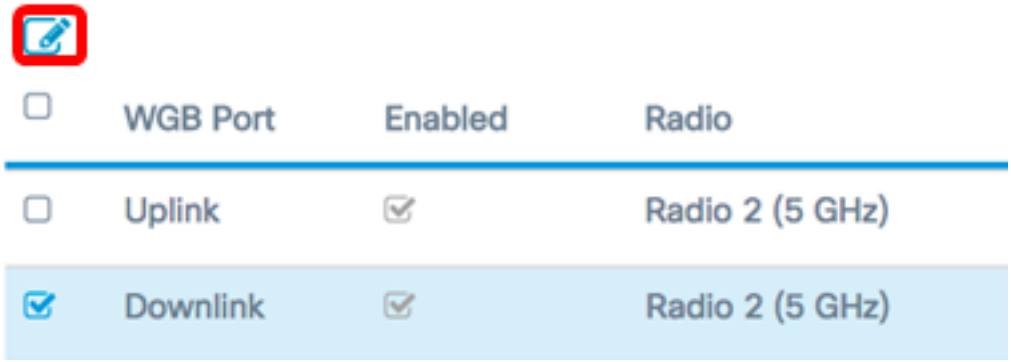

步驟2.按一下**WorkGroup**單選按鈕。



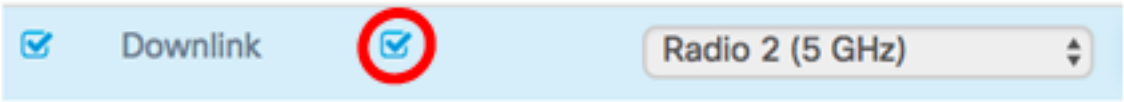

步驟3.勾選**Downlink**覈取方塊。




步驟4.按一下**Edit**按鈕。




步驟5.選中**Enabled**覈取方塊以在接入點介面上啟用橋接。




步驟6.在*SSID*欄位中輸入接入點的SSID。SSID長度必須介於2到32個字元之間。預設設定為下游SSID。


**附註：**在本示例中，使用的SSID是WAP125 Downstream。

步驟7.從Security下拉選單中選擇安全型別，以向WAP驗證下遊客戶端站。

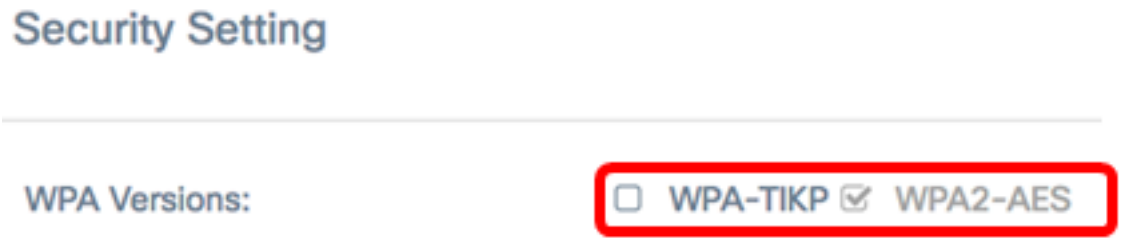
可用選項定義如下：

- 無 — 開啟或無安全性。這是預設值。如果選擇此選項，請跳至步驟13。
- WPA個人 — Wi-Fi保護訪問(WPA)個人可以支援8到63個字元長的金鑰。加密方法為TKIP或計數器密碼模式，採用分組鏈消息驗證代碼協定(CCMP)。建議使用帶有CCMP的

WPA2，因為與僅使用64位RC4標準的臨時金鑰完整性協定(TKIP)相比，WPA2具有更強大的加密標準「高級加密標準(AES)」。


步驟8.（可選）選中WPA-TKIP覈取方塊以確定接入點介面將使用的WPA-TKIP加密。預設情況下啟用。

**附註：**WPA-AES呈灰色顯示，無法禁用。在此示例中，WPA-TKIP未選中。




步驟9.在「金鑰」欄位中輸入共用WPA金鑰。金鑰的長度必須為8-63個字元，並且可以包含字母數字字元、大小寫字元以及特殊字元。


步驟10.在Broadcast Key Refresh Rate欄位中輸入速率。廣播金鑰刷新率指定為該接入點關聯的客戶端刷新安全金鑰的時間間隔。速率必須介於0到86400之間，並且值為0可禁用該功能。

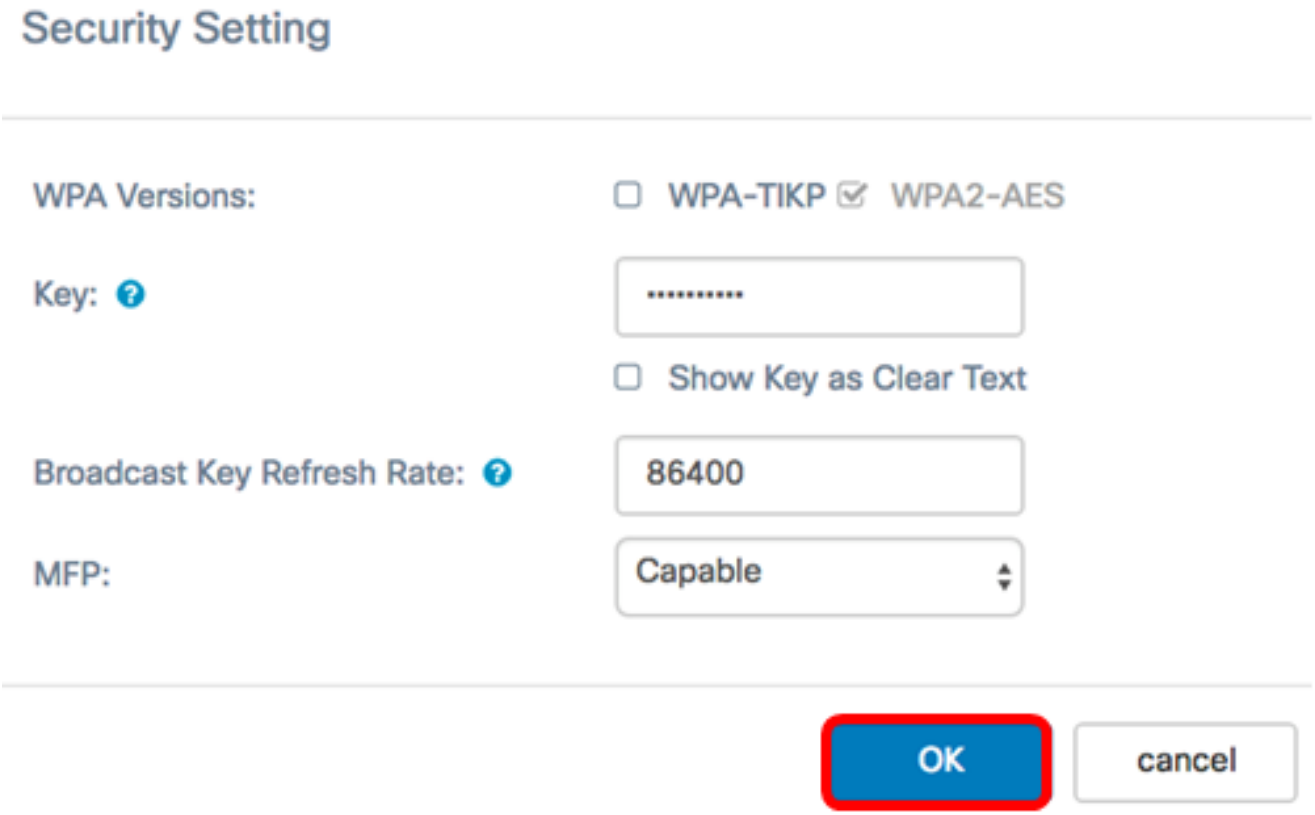

**附註：**在本例中，使86400了ACL。

步驟11.從MFP下拉選單中選擇一個選項，以決定是否希望WAP具有受保護的幀。要瞭解有關MFP的更多資訊，請按一下此處。選項包括：

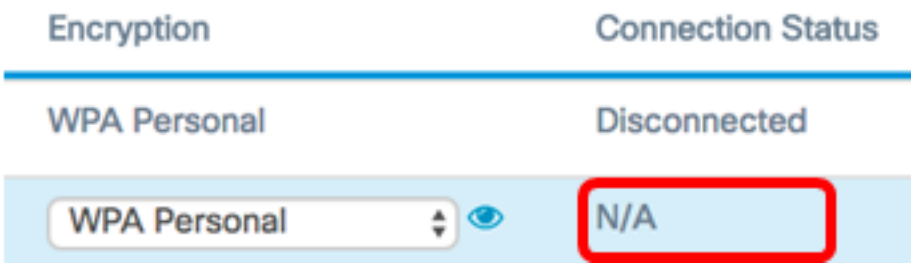
- 不需要 — 禁用MFP的客戶端支援。
- Capable — 允許支援MFP的客戶端和不支援MFP的客戶端加入網路。這是WAP上的預設MFP設定。
- 必需 — 僅當協商了MFP時，才允許客戶端關聯。如果裝置不支援MFP，則不允許它們加入網路。


**附註**：在本例中，選擇了Capable。

步驟12.按一下**OK**以儲存安全性設定。

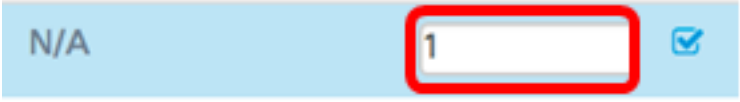



「連線狀態」區域指示「不適用」或「不適用」。

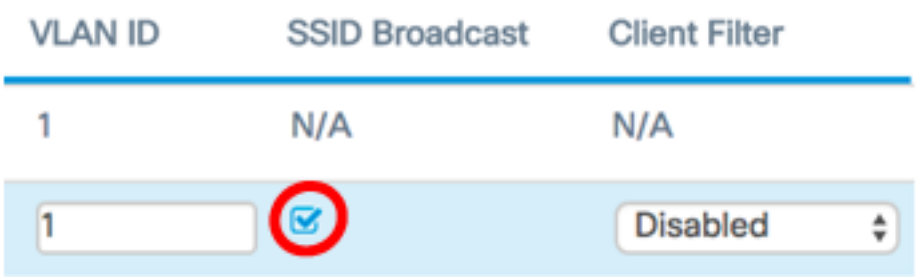



步驟13.在VLAN ID欄位中輸入接入點介面的VLAN ID。

**附註**：為了允許橋接資料包，接入點介面和有線介面的VLAN配置應與基礎設施客戶端介面的VLAN配置相匹配。




步驟14.如果要廣播下游SSID，請選中SSID Broadcast覈取方塊。SSID廣播預設啟用。



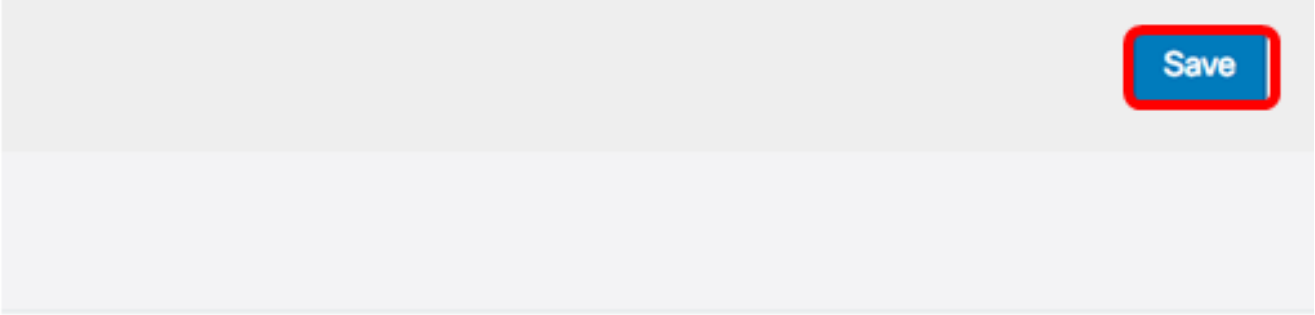

步驟15.從MAC Filtering下拉選單中選擇要為接入點介面配置的MAC過濾型別。啟用時，系統會根據使用者使用的客戶端的MAC地址授予或拒絕使用者訪問WAP。

可用選項定義如下：

- 已禁用 — 所有客戶端都可以訪問上游網路。這是預設值。
- 本地 — 可以訪問上游網路的客戶端集僅限於本地定義的MAC地址清單中指定的客戶端。
- RADIUS — 可存取上游網路的使用者端組限制在RADIUS伺服器上的MAC位址清單中指定的使用者端。

**附註：**在此範例中，選擇「Disabled」。

步驟16.按一下**Save**以儲存變更內容。





您現在應該已經成功配置了無線接入點上的工作組網橋設定。