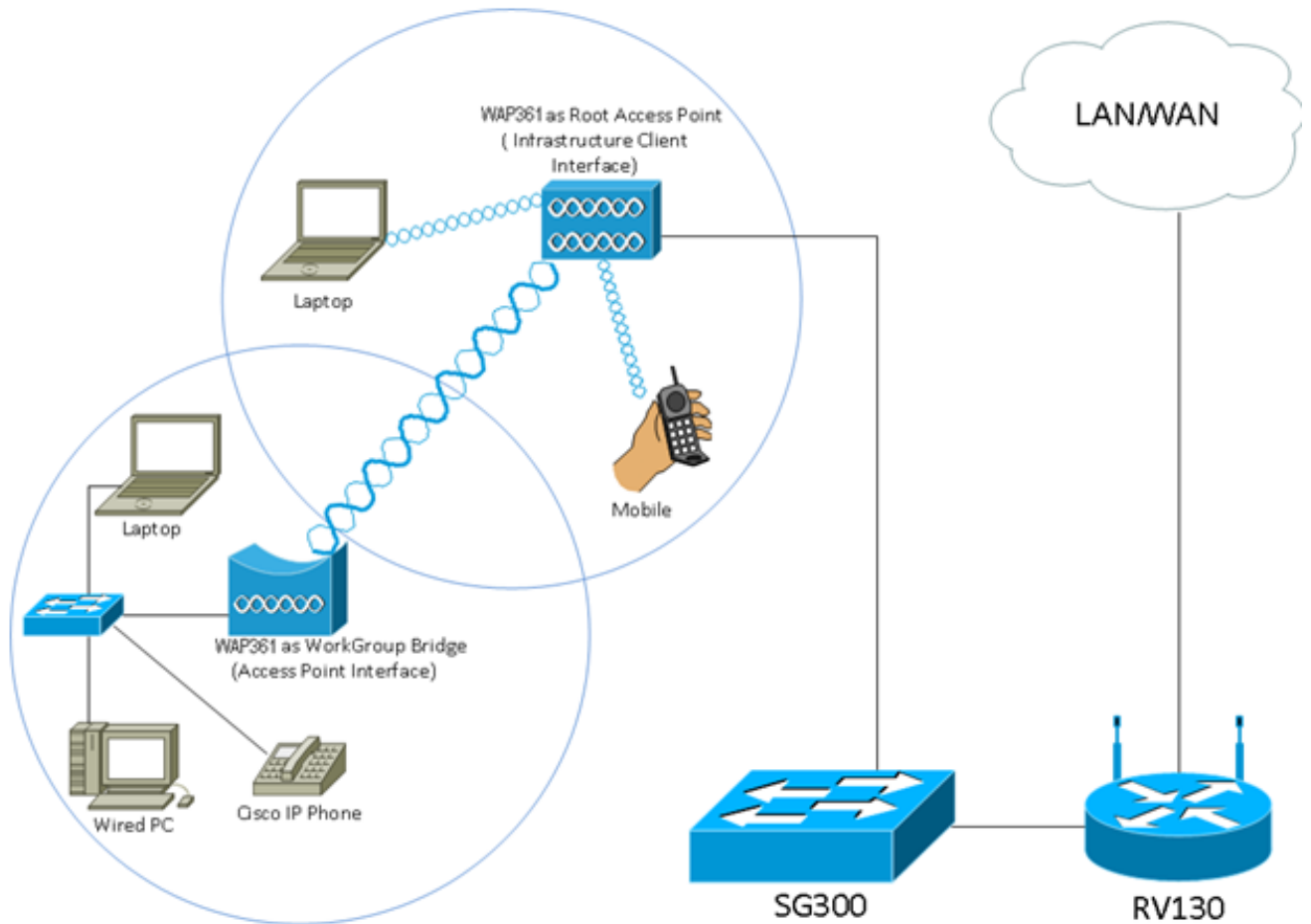


在無線接入點(WAP)上配置工作組網橋

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。



附註：上面的拓撲圖說明了一個WorkGroup網橋模型示例。有線裝置與連線到WAP LAN介面的交換機相連。WAP充當接入點介面，連線到基礎設施介面。

本文旨在展示如何在兩個WAP之間配置工作組網橋。

適用裝置

- WAP100系列
- WAP300系列
- WAP500系列

軟體版本

- 1.0.0.17 — WAP571、WAP571E
- 1.0.1.7 — WAP150、WAP361

- 1.0.2.5 — WAP131、WAP351
- 1.0.6.5 — WAP121、WAP321
- 1.2.1.3 — WAP551、WAP561
- 1.3.0.3 — WAP371

配置工作組網橋

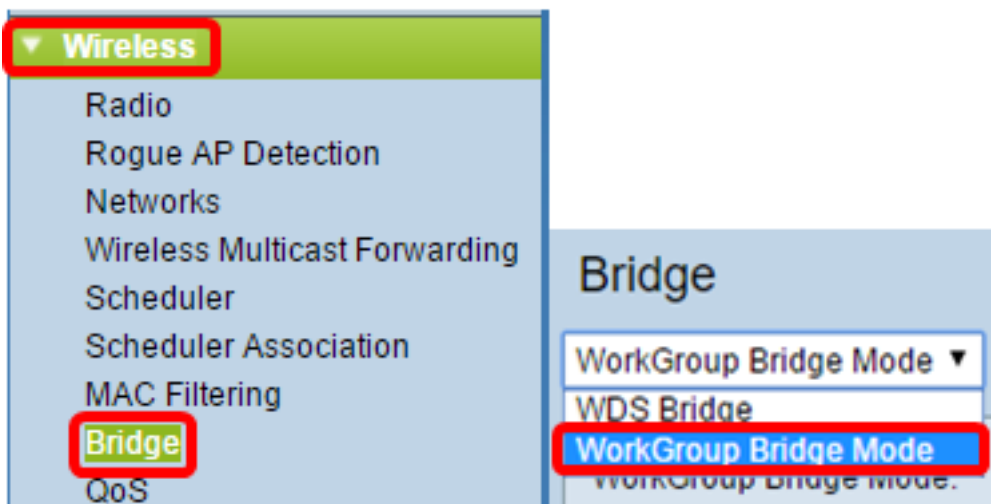
基礎架構使用者端介面

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

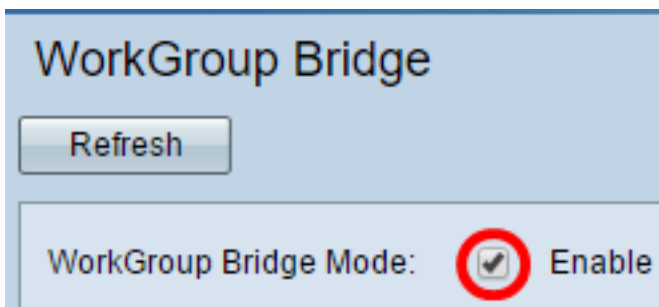
附註：選單選項可能會因所使用的裝置型號而異。除另有說明外，以下影象均取自WAP361。



對於WAP571和WAP571E，請選擇**Wireless > Bridge > WorkGroup Bridge Mode**。



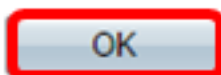
步驟2. 選中**Enable WorkGroup Bridge Mode**竅取方塊。



附註：如果在WAP上啟用了集群，彈出視窗將通知您禁用集群，以便工作組網橋工作。按一下OK繼續。要禁用集群，請從導航窗格中選擇Single Point Setup，然後選擇Access Points > Disable Single Point Setup。

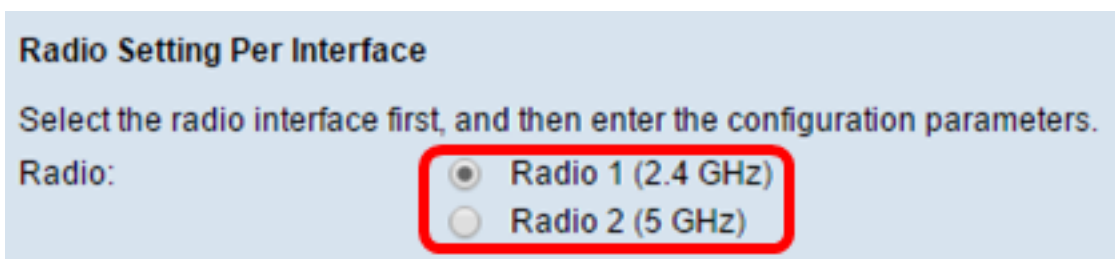


Workgroup Bridge cannot be enabled when clustering is enabled.



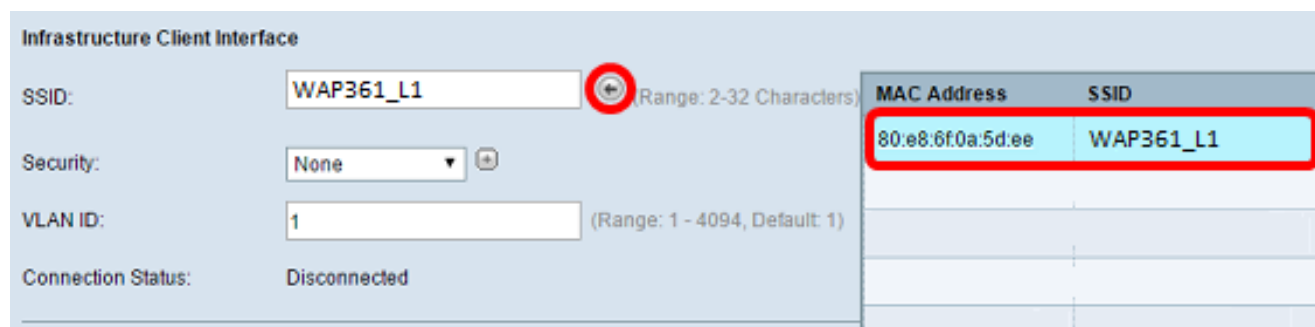
步驟3. 按一下工作組網橋的無線電介面。將一個無線電配置為WorkGroup Bridge時，另一個無線電保持運行。無線電介面對應於WAP的無線電頻帶。WAP配備用於在兩個不同的無線電介面上廣播。配置一個無線電介面的設定不會影響另一個無線電介面。無線電介面選項可能因WAP型號而異。有些WAP顯示Radio 1為2.4 GHz，而一些Radio 2為2.4 GHz。

附註：此步驟僅適用於以下具有雙頻段的WAP: WAP131、WAP150、WAP351、WAP361、WAP371、WAP561、WAP571、WAP571E。在本示例中，選擇無線電1。



步驟4. 在SSID欄位中輸入服務集識別符號(SSID)名稱，或者按一下該欄位旁邊的箭頭按鈕掃描鄰居。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。

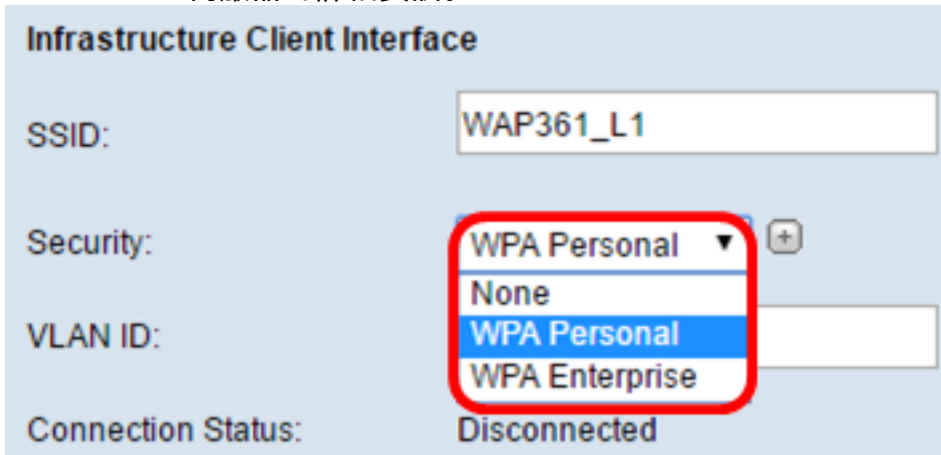
附註：啟用欺詐AP檢測非常重要。要瞭解有關啟用所述功能的詳細資訊，請按一下[此處](#)。在本示例中，按一下箭頭按鈕選擇WAP361_L1作為基礎設施客戶端介面的SSID。



步驟5. 在Infrastructure Client Interface區域中，從Security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18](#)。
- 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。跳至[步驟6](#)進行配置。
- 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9](#)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。



Infrastructure Client Interface

SSID: WAP361_L1

Security: WPA Personal (selected) +

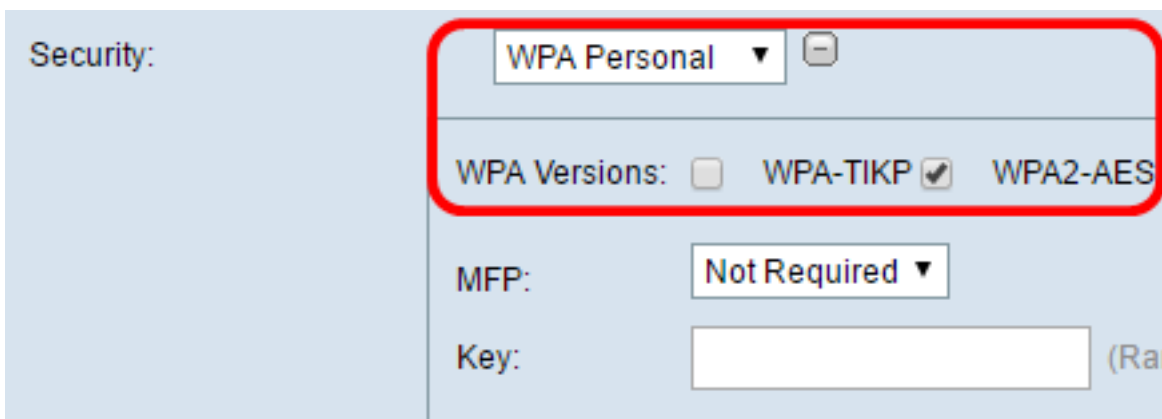
VLAN ID:

Connection Status: Disconnected

附註：在此示例中，選擇了WPA個人。

[步驟6](#) 點選+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。在本示例中，使用WPA2-AES。



Security: WPA Personal -

WPA Versions: WPA-TKIP WPA2-AES

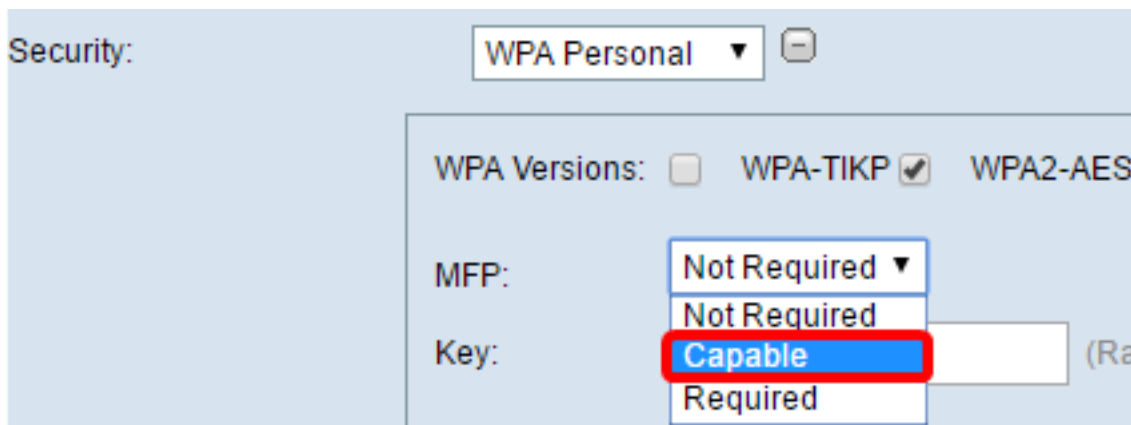
MFP: Not Required

Key: (Rare)

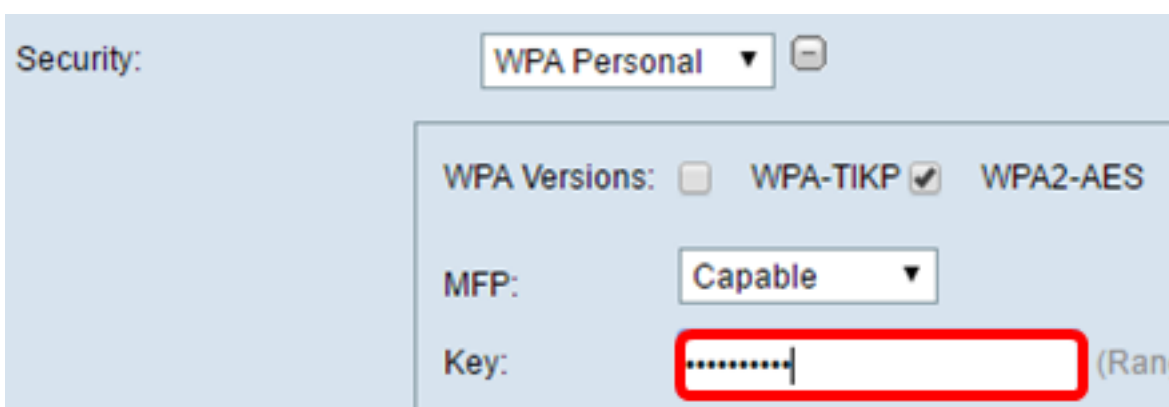
步驟7. (可選) 如果在步驟6中選中了WPA2-AES，請從Management Frame Protection(MFP)下拉選單中選擇一個選項，以決定是否希望WAP要求具有受保護的幀。要瞭解有關MFP的更多資訊，請按一下[此處](#)。選項包括：

- 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：在本例中，選擇了Capable。



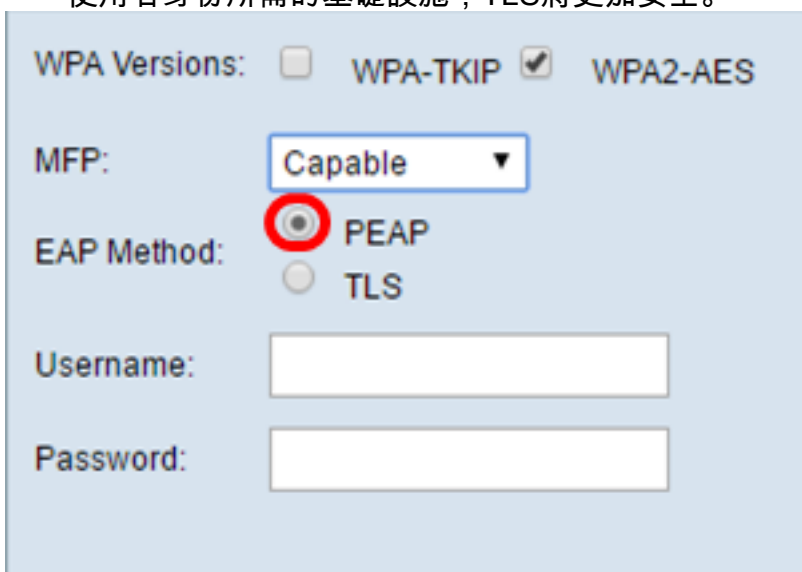
步驟8.在 金鑰欄位中輸入WPA加密金鑰。金鑰的長度必須為8-63個字元。這是字母、數字和特殊字元的組合。這是首次連線到無線網路時使用的密碼。然後，跳至[步驟18](#)。



[步驟9](#).如果您在步驟5中選擇了WPA企業，請按一下EAP方法的單選按鈕。

可用選項定義如下：

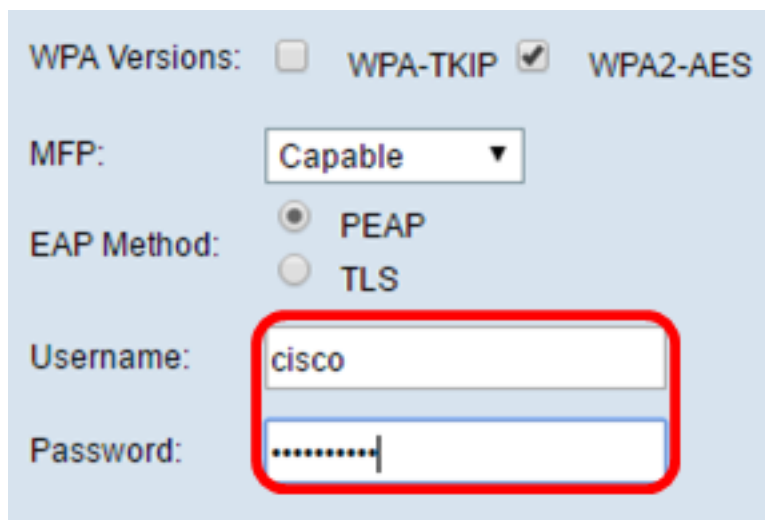
- PEAP — 此協定為WAP下的每個無線使用者提供支援AES加密標準的個人使用者名稱和密碼。由於PEAP是基於密碼的安全方法，您的Wi-Fi安全基於客戶端的裝置憑證。如果您有弱密碼或不安全的客戶端，PEAP可能會帶來嚴重的安全風險。它依賴TLS，但避免在每個客戶端上安裝數位證書。相反，它通過使用者名稱和密碼提供身份驗證。
- TLS - TLS要求每個使用者具有授予訪問許可權的附加證書。如果您有額外的伺服器 and 驗證網路使用者身份所需的基礎設施，TLS將更加安全。



附註：在本示例中，選擇了PEAP。

步驟10.在 *Username* 和 *Password* 欄位中輸入基礎設施客戶機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18](#)。



WPA Versions: WPA-TKIP WPA2-AES

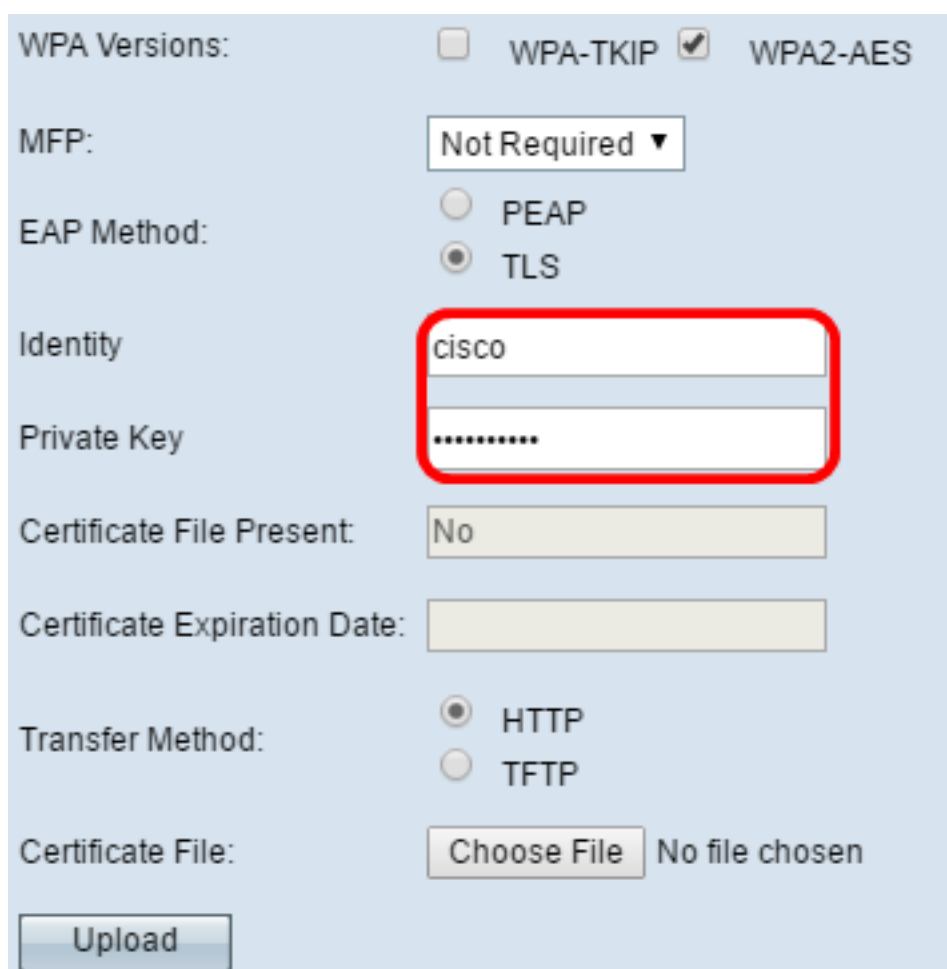
MFP:

EAP Method: PEAP TLS

Username:

Password:

步驟11.如果您在步驟9中按一下了TLS，請在*Identity*和*Private Key*欄位中輸入基礎設施客戶端的身分 and 私鑰。



WPA Versions: WPA-TKIP WPA2-AES

MFP:

EAP Method: PEAP TLS

Identity:

Private Key:

Certificate File Present:

Certificate Expiration Date:

Transfer Method: HTTP TFTP

Certificate File: No file chosen

[步驟12](#).在傳輸方法區域中，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15](#)。
- 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。

WPA Versions: WPA-TKIP WPA2-AES

MFP:

EAP Method: PEAP TLS

Identity:

Private Key:

Certificate File Present:

Certificate Expiration Date:

Transfer Method: HTTP TFTP

Certificate File: No file chosen

註：如果WAP上已經存在證書檔案，則Certificate File Present和Certificate Expiration Date欄位已經填寫了相關資訊。否則，它們將是空白的。

HTTP

步驟13. 按一下**Choose File**按鈕以尋找並選擇憑證檔案。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mini_httpd(2)。pfx。

Transfer Method: HTTP TFTP

Filename: mini_httpd (2).pfx

步驟14. 按一下**Upload** 以上傳選取的憑證檔案。跳至[步驟18](#)。

Transfer Method: HTTP TFTP

Filename mini_httpd (2).pfx

*Certificate File Present*和*Certificate Expiration Date*欄位將自動更新。

WPA Versions: WPA-TKIP WPA2-AES

MFP:

EAP Method: PEAP TLS

Identity

Private Key

Certificate File Present:

Certificate Expiration Date:

Transfer Method: HTTP TFTP

Certificate File: No file chosen

TFTP

[步驟15](#)。如果您在[步驟12](#)中按下了TFTP，請在*Filename*欄位中輸入證書檔案的文件名。

附註：在此範例中使用的是mini_httpd.pem。

Transfer Method: HTTP TFTP

Filename: mini_httpd.pem

TFTP Server IPv4 Address: 192.168.1.20

Upload

步驟16.在「*TFTP Server IPv4 Address*」欄位中輸入TFTP伺服器地址。

附註：在本例中。192.168.1.20用作TFTP伺服器地址。

Transfer Method: HTTP TFTP

Filename: mini_httpd.pem

TFTP Server IPv4 Address: 192.168.1.20

Upload

步驟17.按一下**Upload**按鈕以上傳指定的憑證檔案。

Transfer Method: HTTP TFTP

Filename: mini_httpd.pem

TFTP Server IPv4 Address: 192.168.1.20

Upload

*Certificate File Present*和*Certificate Expiration Date*欄位將自動更新。

WPA Versions: WPA-TKIP WPA2-AES

EAP Method: PEAP TLS

Identity:

Private Key:

Certificate File Present:

Certificate Expiration Date:

Transfer Method: HTTP TFTP

Filename:

TFTP Server IPv4 Address:

[步驟18](#).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。

VLAN ID: (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

存取點介面

步驟1.選中Enable Status覆取方塊以在接入點介面上啟用橋接。

Access Point Interface

Status: Enable

SSID: (Range: 2-32 Characters)

SSID Broadcast: Enable

Security: ▼

MAC Filtering: ▼

VLAN ID: (Range: 1 - 4094, Default: 1)

步驟2.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。預設值為Access Point SSID。

附註：在本示例中，使用的SSID是bridge_lobby。



Access Point Interface

Status: Enable

SSID: (Range: 2-32 Characters)


SSID Broadcast: Enable

Security: (+)

MAC Filtering: ▾

VLAN ID: (Range: 1 - 4094, Default: 1)

步驟3. (可選) 如果您不想廣播SSID，請取消選中**Enable** SSID Broadcast覈取方塊。這樣做將使搜尋無線接入點的人無法看到接入點；它只能由已知道SSID的人員連線到。SSID廣播預設啟用。



Access Point Interface

Status: Enable

SSID: (Range: 2-32 Characters)

SSID Broadcast: Enable

Security: (+)

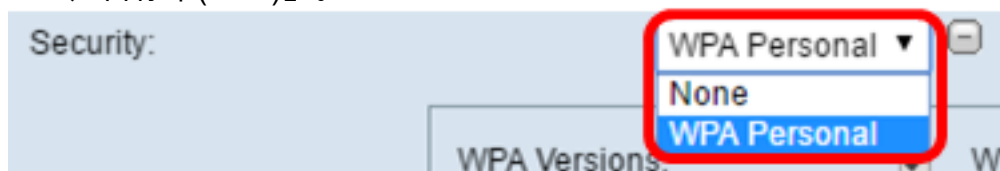
MAC Filtering: ▾

VLAN ID: (Range: 1 - 4094, Default: 1)

步驟4. 從Security下拉選單中選擇安全型別，以向WAP驗證下游客戶端站。

可用選項定義如下：

- 無 — 開啟或無安全性。這是預設值。如果選擇此項，請跳至[步驟10](#)。
- 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)」。

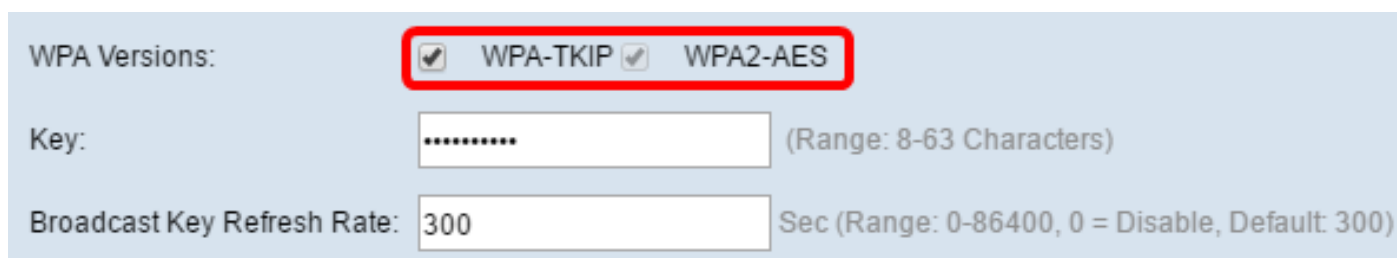


Security: ▾ (+)

WPA Versions: ▾ WI

步驟5.選中WPA-TKIP或WPA2-AES覈取方塊以確定接入點介面將使用的WPA加密型別。預設情況下，這些選項處於啟用狀態。

附註：如果所有無線裝置都支援WPA2，則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。在本示例中，使用WPA2-AES。

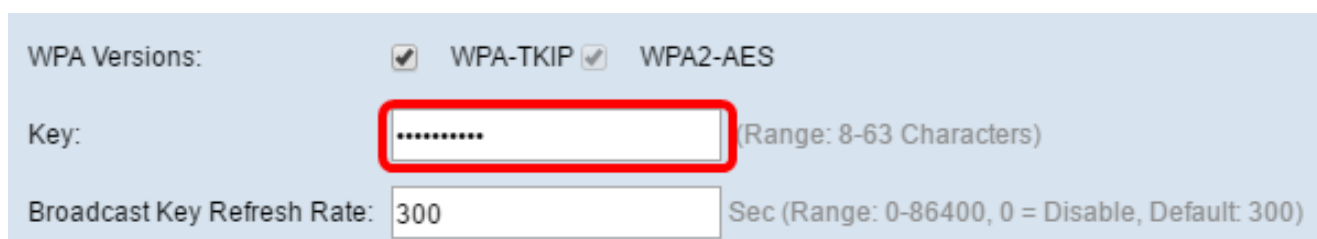


WPA Versions: WPA-TKIP WPA2-AES

Key: (Range: 8-63 Characters)

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

步驟6.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。

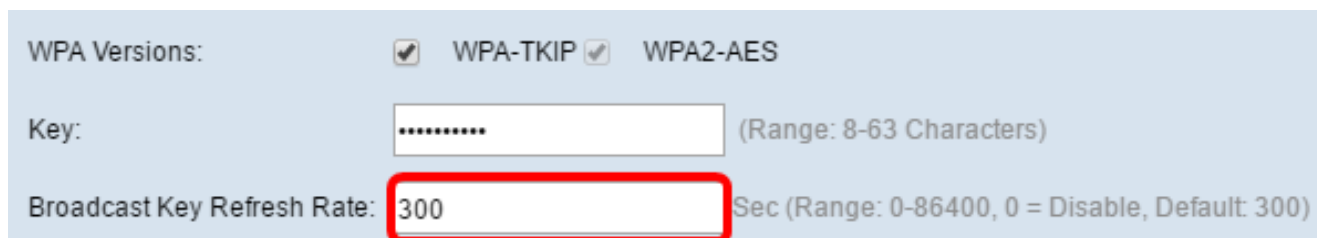


WPA Versions: WPA-TKIP WPA2-AES

Key: (Range: 8-63 Characters)

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

步驟7.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。預設值為300。



WPA Versions: WPA-TKIP WPA2-AES

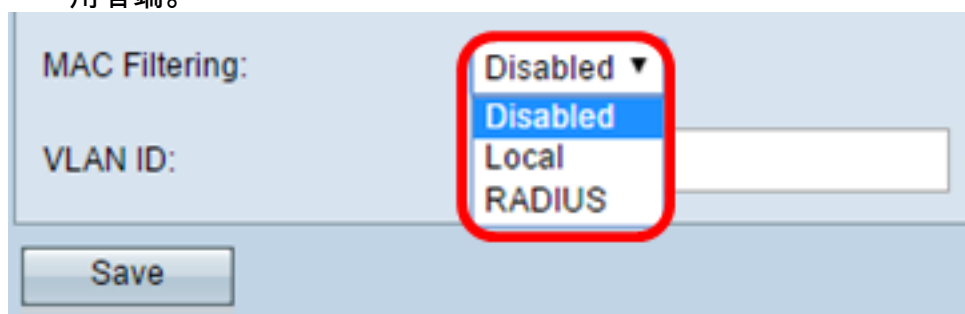
Key: (Range: 8-63 Characters)

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

步驟8.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。



MAC Filtering: ▼

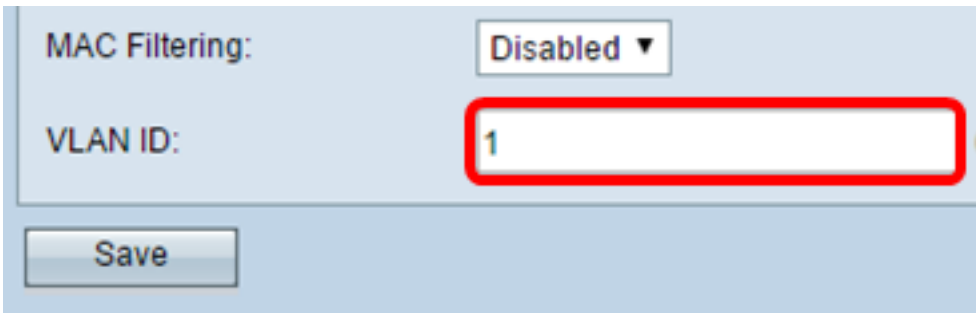
VLAN ID:

Save

附註：在本例中，選擇了Disabled。

步驟9.在 *VLAN ID*欄位中輸入接入點介面的VLAN ID。

注意：要允許橋接資料包，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。

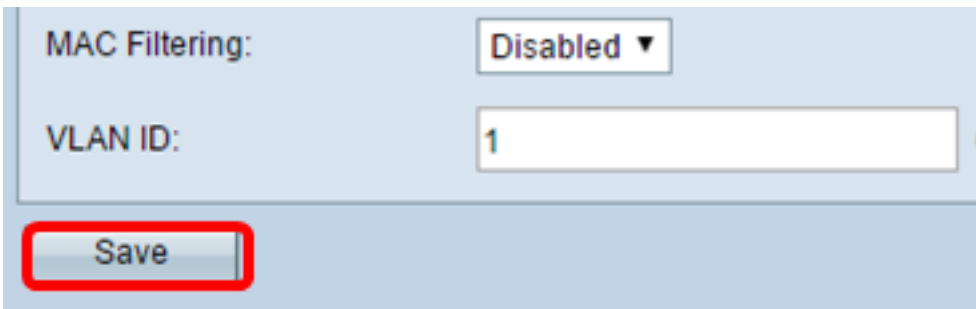


MAC Filtering: Disabled ▾

VLAN ID: 1

Save

[步驟10](#).按一下**Save**以儲存變更內容。



MAC Filtering: Disabled ▾

VLAN ID: 1

Save

現在，您應該已經成功在無線接入點上配置了工作組網橋。