

在WAP351上配置802.1X設定

目標

IEEE 802.1X身份驗證允許WAP裝置訪問安全的有線網路。您可以將WAP裝置配置為有線網路上的802.1X請求方(客戶端)。WAP351還可以配置為身份驗證器。可以配置加密的使用者名稱和密碼以允許WAP裝置使用802.1X進行身份驗證。

在使用基於IEEE 802.1X埠的網路訪問控制的網路上，請求方無法訪問該網路，直到802.1X驗證方授予訪問許可權。如果您的網路使用802.1X，您必須在WAP裝置上設定802.1X驗證資訊，以便它能將其提供給驗證器。

本文檔的目標是向您展示如何在WAP351上配置802.1X Supplicant客戶端設定。

適用裝置

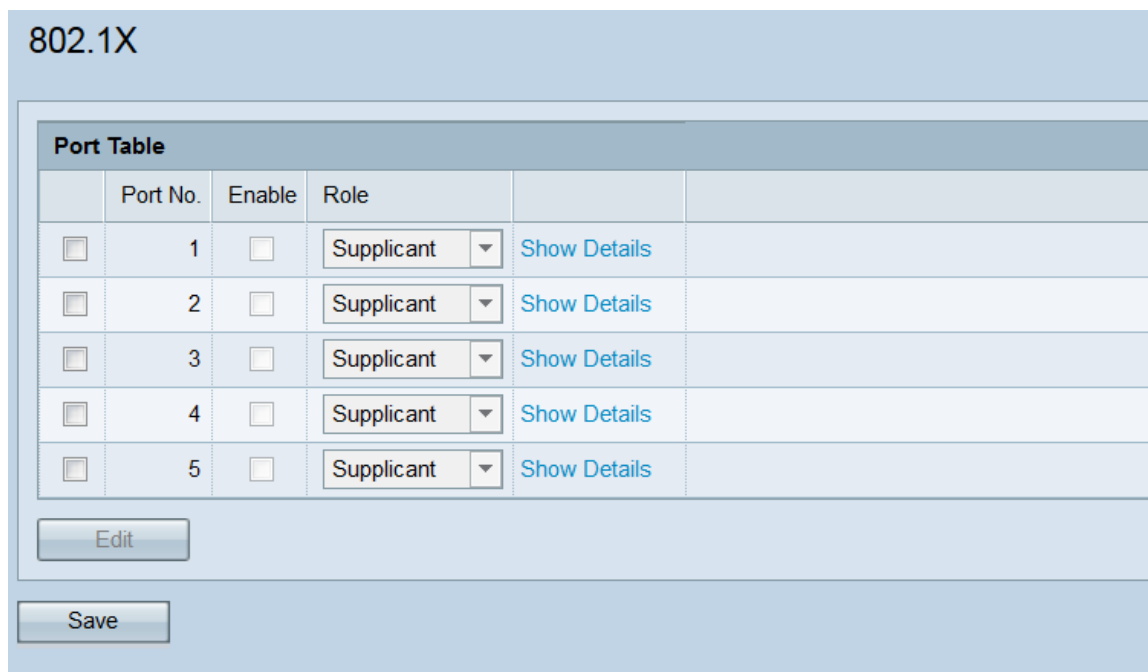
·WAP351

軟體版本

·v1.0.1.3

配置802.1X請求方設定

步驟1. 登入到Web配置實用程式並選擇**System Security > 802.1X**。802.1X頁面隨即開啟。



802.1X

Port Table					
	Port No.	Enable	Role		
<input type="checkbox"/>	1	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	5	<input type="checkbox"/>	Supplicant	Show Details	

Edit

Save

步驟2. 連線埠表顯示五個可設定為802.1X驗證的LAN介面。勾選與您要編輯的連線埠對應的覈取方塊。

802.1X

Port Table					
	Port No.	Enable	Role		
<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	5	<input type="checkbox"/>	Supplicant	Show Details	

Edit

Save

步驟3.按一下**Edit**按鈕。選中的埠現在可用於編輯。

Port Table					
	Port No.	Enable	Role		
<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	5	<input type="checkbox"/>	Supplicant	Show Details	

Edit

Save

步驟4.在**Enable**欄位中，勾選您要在其上啟用802.1X設定的連線埠的覈取方塊。

802.1X

Port Table					
	Port No.	Enable	Role		
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	5	<input type="checkbox"/>	Supplicant	Show Details	

Edit

Save

步驟5.在Role下拉選單中，選擇將相應的埠配置為Supplicant客戶端還是Authenticator。如果選擇了Supplicant客戶端，請轉到[Supplicant Settings Configuration](#)部分。如果選擇驗證器，請轉到[驗證器設定配置](#)部分。驗證器位於想要存取網路的使用者端（要求者）和RADIUS伺服器本身之間。它負責處理兩者之間的所有通訊。請求方向身份驗證器提供憑證以訪問網路。WAP351上的典型設定將使WAN埠成為請求方（因此WAP可以訪問網路），並使LAN埠成為驗證方（因此WAP可以授權其下面的裝置）。

802.1X

Port Table					
	Port No.	Enable	Role		
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	5	<input type="checkbox"/>	Supplicant	Show Details	

Edit

Save

請求方設定配置

步驟1.按一下Show Details以顯示請求方設定資訊。

Port Table				
	Port No.	Enable	Role	
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Supplicant	Hidden Details
<p>EAP Method: <input type="text" value="MD5"/></p> <p>Username: <input type="text"/> (Range: 1 - 64 Characters)</p> <p>Password: <input type="text"/> (Range: 1 - 64 Characters)</p> <hr/> <p>Certificate File Status <input type="button" value="Refresh"/></p> <p>Certificate File Present: No</p> <p>Certificate Expiration Date: Not Present</p> <hr/> <p>Browse to the location where your certificate file is stored and click the "Upload" button. To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.</p> <p>Certificate File Upload</p> <p>Transfer Method: <input checked="" type="radio"/> HTTP <input type="radio"/> TFTP</p> <p>Filename <input type="button" value="Browse..."/> No file selected.</p> <p><input type="button" value="Upload"/></p>				
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant	Show Details

附註：在模式欄位中進行選擇後，此資訊可能會自動開啟。

步驟2.在EAP Method下拉選單中，選擇用於加密使用者名稱和密碼的演算法。EAP代表可擴展身份驗證協定，並用作加密演算法的基礎。

EAP Method: MD5 ▼
MD5
PEAP
TLS

Username: (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

Certificate File Status

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename No file selected.

可用選項包括：

- MD5 - MD5消息摘要演算法利用雜湊函式來提供基本的安全性。不建議使用此演算法，因為其他兩個具有更高的安全性。
- PEAP - PEAP代表受保護的可擴展身份驗證協定。它封裝了EAP，通過使用TLS隧道傳輸資料，可提供比MD5更高的安全性。
- TLS — TLS代表傳輸層安全性，是提供高安全性的開放標準。

步驟3.在 *Username* 欄位中，輸入WAP裝置在回應802.1X驗證器要求時將使用的使用者名稱。使用者名稱長度必須為1到64個字元，並且可以包含字母數字字元和特殊字元。

EAP Method: MD5 ▼

Username: (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

Certificate File Status

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename No file selected.

步驟4.在密碼欄位中，輸入WAP裝置在回應802.1X驗證器要求時將使用的密碼。使用者名稱長度必須為1到64個字元，並且可以包含字母數字字元和特殊字元。

EAP Method: MD5 ▾

Username: username1 (Range: 1 - 64 Characters)

Password: ●●●●●●●● (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename Browse... No file selected.

Upload

步驟5. *Certificate File Status*區域顯示WAP裝置上是否存在HTTP SSL證書檔案。如果憑證存在，*Certificate File Present*欄位會顯示「Yes」；預設值為「No」。如果存在證書，則會顯示證書到期日；否則，預設值為「Not present」。要顯示最新資訊，請按一下**Refresh**按鈕以獲得最新的證書資訊。

EAP Method: MD5 ▼

Username: username1 (Range: 1 - 64 Characters)

Password: ●●●●●●●● (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename No file selected.

步驟6。如果您不想上傳HTTP SSL憑證檔案，請跳至[步驟12](#)。否則，在**Transfer Method**欄位中選擇「HTTP」或「TFTP」單選按鈕以選擇要用於上傳憑證的通訊協定。

EAP Method: MD5 ▾

Username: username1 (Range: 1 - 64 Characters)

Password: ●●●●●●●● (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP TFTP

Filename Browse... No file selected.

Upload

步驟7.如果選擇TFTP，請繼續步驟8。如果選擇HTTP，請按一下Browse...按鈕在PC上查詢證書檔案。跳至[步驟10](#)。

EAP Method: MD5 ▼

Username: username1 (Range: 1 - 64 Characters)

Password: ●●●●●●●● (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename No file selected.

步驟8.如果您在 *Transfer Method* 欄位中選擇了 TFTP，請在 *Filename* 欄位中輸入憑證的名稱。

EAP Method: (Range: 1 - 64 Characters)

Username: (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

Certificate File Status

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP TFTP

Filename: (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: (xxx.xxx.xxx.xxx)

附註：檔案必須以.pem結尾。

步驟9.在「*TFTP Server IPv4 Address*」欄位中輸入TFTP伺服器的IP地址。

EAP Method: MD5 ▼

Username: username1 (Range: 1 - 64 Characters)

Password: ●●●●●●●● (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP TFTP

Filename: certificate.pem (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: 192.0.2.100 (xxx.xxx.xxx.xxx)

Upload

[步驟10](#). 按一下Upload。

EAP Method: MD5 ▼

Username: username1 (Range: 1 - 64 Characters)

Password: ●●●●●●●● (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

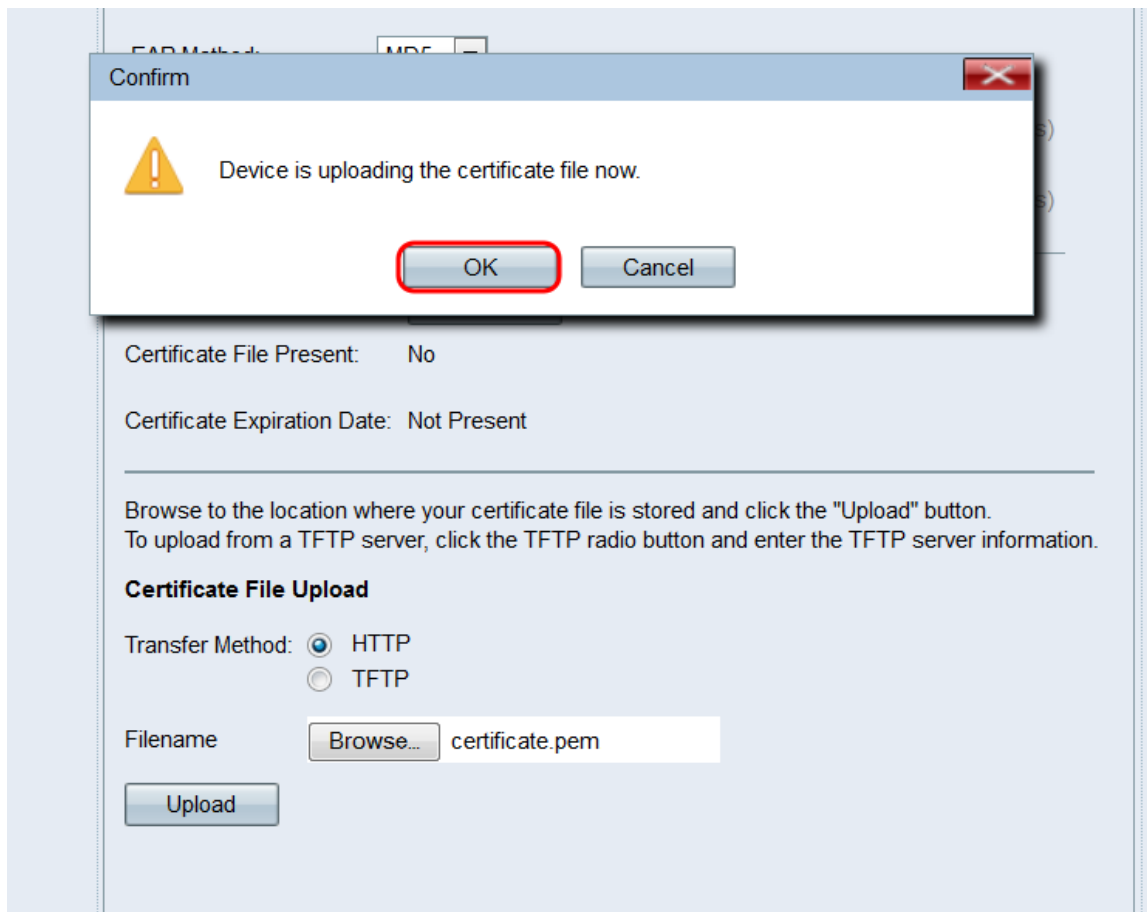
Certificate File Upload

Transfer Method: HTTP
 TFTP

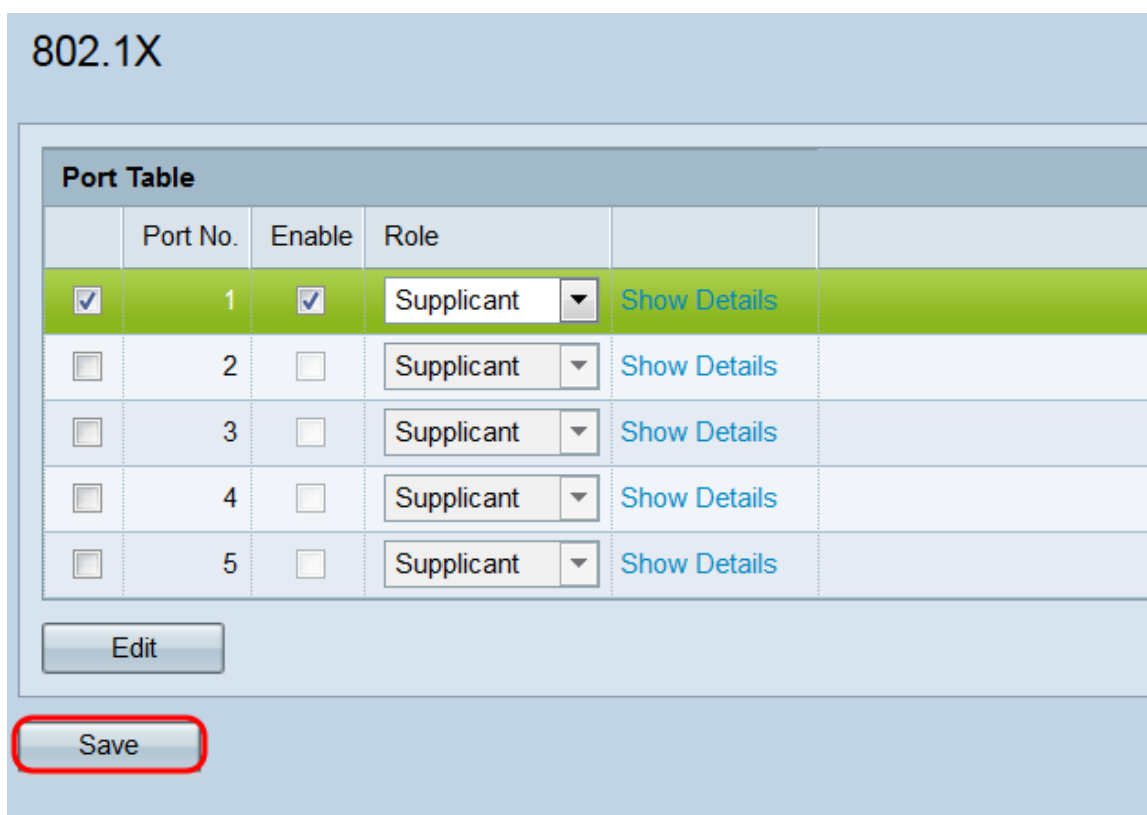
Filename Browse... certificate.pem

Upload

步驟11.出現確認視窗。按一下「OK」開始上傳。



步驟 12. 對要配置為 802.1X 請求方的每個埠重複此部分。然後按一下 **Save**。



身份驗證器設定配置

步驟 1. 按一下 **Show Details** 以顯示驗證器設定資訊。

Port Table																							
Port No.	Enable	Role																					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Authenticator	Hidden Details																				
<input checked="" type="checkbox"/> Use global RADIUS server settings Server IP Address Type: <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <table border="1"> <thead> <tr> <th>No.</th> <th>Server IP Address (xxx.xxx.xxx.xxx)</th> <th>Key (Range: 1 - 64 Characters)</th> <th>Authentication Port (Range: 0 - 65535, Default: 1812)</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>0.0.0.0</td> <td></td> <td>1812</td> </tr> <tr> <td>2</td> <td></td> <td></td> <td>1812</td> </tr> <tr> <td>3</td> <td></td> <td></td> <td>1812</td> </tr> <tr> <td>4</td> <td></td> <td></td> <td>1812</td> </tr> </tbody> </table> <input type="checkbox"/> Enable RADIUS Accounting Active Server: Server IP Address-1 Periodic Reauthentication: <input type="checkbox"/> Enable Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)				No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)	1	0.0.0.0		1812	2			1812	3			1812	4			1812
No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)																				
1	0.0.0.0		1812																				
2			1812																				
3			1812																				
4			1812																				
<input type="checkbox"/>	<input type="checkbox"/>	Supplicant	Show Details																				

附註：在模式欄位中進行選擇後，此資訊可能會自動開啟。

步驟2.如果您希望連線埠在驗證期間使用全域RADIUS設定，請勾選使用全域RADIUS伺服器設定竅取方塊。如果您希望連線埠使用不同的RADIUS伺服器（或伺服器），請取消選中此竅取方塊；否則，請跳至[步驟8](#)。

<input checked="" type="checkbox"/> Use global RADIUS server settings			
Server IP Address Type: <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6			
No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	0.0.0.0		1812
2			1812
3			1812
4			1812
<input type="checkbox"/> Enable RADIUS Accounting			
Active Server: Server IP Address-1			
Periodic Reauthentication: <input type="checkbox"/> Enable			
Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)			

附註：有關詳細資訊，請參閱[在WAP131和WAP351上配置全域性RADIUS伺服器設定](#)一文。

步驟3.在「Server IP Address Type」欄位中，選擇RADIUS伺服器使用的IP版本的單選按鈕

。可用的選項有IPv4和IPv6。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	0.0.0.0		1812
2			1812
3			1812
4			1812

Enable RADIUS Accounting

Active Server: Server IP Address-1 ▼

Periodic Reauthentication: Enable

Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)

附註：您可以在地址型別之間切換以配置IPv4和IPv6 RADIUS地址設定，但WAP裝置僅聯絡具有您在此欄位中選擇的地址型別的RADIUS伺服器。不能讓多個伺服器在一個配置中使用不同的地址型別。

步驟4.在 *Server IP Address 1* 或 *Server IPv6 Address 1* 欄位中，根據您在步驟3中選擇的地址型別，輸入RADIUS伺服器的IPv4或IPv6地址。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1		1812
2			1812
3			1812
4			1812

Enable RADIUS Accounting

Active Server: Server IP Address-1 ▼

Periodic Reauthentication: Enable

Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)

附註：在此欄位中輸入的地址將指定埠的主RADIUS伺服器。在後續欄位(*伺服器IP地址2至4*

)中輸入的地址將指定在主伺服器身份驗證失敗時按順序嘗試的備份RADIUS伺服器。

步驟5.在Key欄位中，輸入與WAP裝置用來向RADIUS伺服器驗證的主要RADIUS伺服器對應的共用金鑰。可以使用1到64個標準字母數字和特殊字元。在Key 2至4欄位中針對連線埠設定的每個後續的RADIUS伺服器重複此步驟。

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1	••••••••	1812
2			1812
3			1812
4			1812

Enable RADIUS Accounting

Active Server: ▼

Periodic Reauthentication: Enable

Reauthentication Period: sec. (Range: 300 - 4294967295, Default: 3600)

附註：這些金鑰區分大小寫，並且必須與RADIUS伺服器上配置的金鑰相匹配。

步驟6.在Authentication Port欄位中，輸入WAP將用來連線到RADIUS伺服器的連線埠。在Authentication Port 2至4欄位中設定的每個備份RADIUS伺服器重複此步驟。預設值為1812。

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1	••••••••	1812
2			1812
3			1812
4			1812

Enable RADIUS Accounting

Active Server: ▼

Periodic Reauthentication: Enable

Reauthentication Period: sec. (Range: 300 - 4294967295, Default: 3600)

步驟7.選中**啟用RADIUS記帳**竅取方塊以啟用跟蹤和測量使用者已使用的資源（系統時間、傳輸的資料量等）。選中此竅取方塊將為主伺服器 and 備份伺服器啟用RADIUS記帳。

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1	••••••••	1812
2	192.0.2.2	••••~••••	2500
3			1812
4			1812

Enable RADIUS Accounting

Active Server: ▼

Periodic Reauthentication: Enable

Reauthentication Period: sec. (Range: 300 - 4294967295, Default: 3600)

步驟8.在「Active Server」下拉選單中，選擇其中一個已配置的RADIUS伺服器以設定為活動伺服器。此設定允許WAP立即嘗試聯絡活動伺服器，而不是嘗試按順序聯絡每台伺服器並選擇第一個可用伺服器。

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1	••••••••	1812
2	192.0.2.2	••••••••	2500
3			1812
4			1812

Enable RADIUS Accounting

Active Server: Server IP Address-1 ▼
Server IP Address-1
Server IP Address-2
Server IP Address-3
Server IP Address-4

Periodic Reauthentication: Enable

Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)

步驟9.在 *Periodic Reauthentication* 欄位中，選中 **Enable** 釁取方塊以啟用EAP重新身份驗證。如果您不想啟用EAP重新身份驗證，請跳至 [步驟11](#)。

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1	••••••••	1812
2	192.0.2.2	••~••••••	2500
3			1812
4			1812

Enable RADIUS Accounting

Active Server: Server IP Address-1 ▼

Periodic Reauthentication: Enable

Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)

步驟10.如果在 *Periodic Reauthentication* 欄位中選中 **Enable** 釁取方塊，請在 *Reauthentication Period* 欄位中輸入EAP重新身份驗證時間段（以秒為單位）。預設值為3600。有效範圍為300 - 4294967295秒。

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1	••••••••	1812
2	192.0.2.2	••••••••	2500
3			1812
4			1812

Enable RADIUS Accounting

Active Server:

Periodic Reauthentication: Enable

Reauthentication Period: sec. (Range: 300 - 4294967295, Default: 3600)

步驟11.對要配置為802.1X驗證器的每個埠重複此部分。然後按一下**Save**。

802.1X

Port Table

	Port No.	Enable	Role	
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Authenticator ▼	Show Details
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	5	<input type="checkbox"/>	Supplicant ▼	Show Details

Edit

Save