

# 在交換機上配置802.1x埠身份驗證設定

## 目標

IEEE 802.1x標準便於客戶端和伺服器之間的訪問控制。在區域網(LAN)或交換器可向使用者端提供服務之前，連線到交換器連線埠的使用者端必須透過執行遠端驗證撥入使用者服務(RADIUS)的驗證伺服器進行驗證。

802.1x身份驗證限制未經授權的客戶端通過公開訪問的埠連線到LAN。802.1x身份驗證是客戶端 — 伺服器模型。在此模型中，網路裝置具有以下特定角色：

**客戶端或請求方** — 客戶端或請求方是請求訪問LAN的網路裝置。客戶端連線到身份驗證器。

**驗證器** — 驗證器是提供網路服務並將請求埠連線的網路裝置。支援以下身份驗證方法：

**基於802.1x** — 所有身份驗證模式都支援。在基於802.1x的身份驗證中，身份驗證器從802.1x消息或EAP over LAN(EAPoL)資料包中提取可擴展身份驗證協定(EAP)消息，並使用RADIUS協定將其傳遞到身份驗證伺服器。

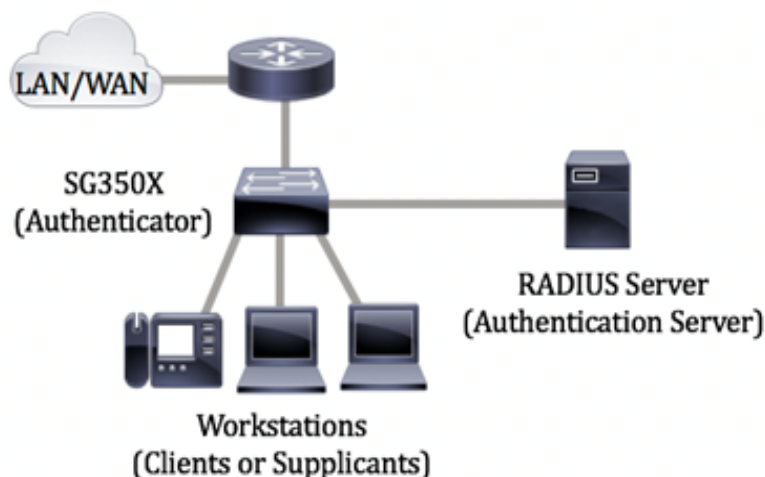
**基於MAC** — 所有身份驗證模式都支援。基於媒體訪問控制(MAC)，驗證器本身代表尋求網路訪問的客戶端執行軟體的EAP客戶端部分。

**基於Web** — 僅在多會話模式下支援。使用基於Web的身份驗證，身份驗證器本身代表尋求網路訪問的客戶端執行軟體的EAP客戶端部分。

**身份驗證伺服器** — 身份驗證伺服器執行客戶端的實際身份驗證。裝置的身份驗證伺服器是具有EAP擴展的RADIUS身份驗證伺服器。

**附註：**網路裝置可以是客戶端，也可以是請求方、驗證方，或者每個埠都可以。

下圖顯示了根據特定角色配置裝置的網路。本示例使用SG350X交換機。



設定802.1x的准則：

建立虛擬存取網路(VLAN)。要使用交換機的基於Web的實用程式建立VLAN，請按一下[此處](#)。有關基於CLI的說明，請按一下[此處](#)。

在交換機上配置埠到VLAN設定。要使用基於Web的實用程式進行配置，請按一下[此處](#)。要使用CLI，請按一下[此處](#)。

在交換機上配置802.1x屬性。應在交換機上全域性啟用802.1x以啟用802.1x基於埠的身份驗證。有關說明，請按一下[此處](#)。

(可選)在交換機上配置時間範圍。若要瞭解如何配置交換機上的時間範圍設定，請按一下[此處](#)。

配置802.1x埠身份驗證。本文提供如何在交換機上配置802.1x埠身份驗證設定的說明。

若要瞭解如何配置交換機上的基於MAC的身份驗證，請按一下[此處](#)。

## 適用裝置

Sx300系列

Sx350系列

SG350X系列

Sx500系列

Sx550X系列

## 軟體版本

1.4.7.06 — Sx300、Sx500

2.2.8.04 — Sx350、SG350X、Sx550X

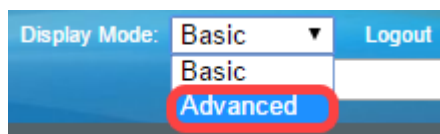
## 在交換機上配置802.1x埠身份驗證設定

[配置RADIUS客戶端設定](#)

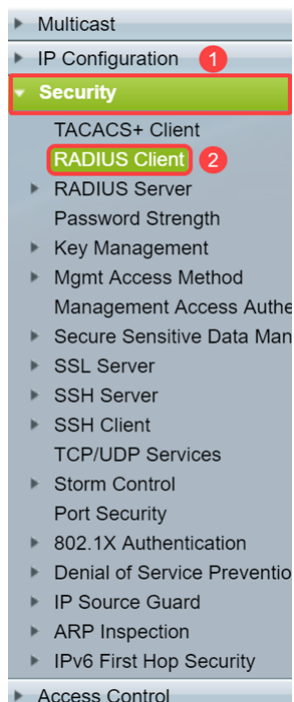
步驟1. 登入交換器的網路型公用程式，然後在「Display Mode」下拉式清單中選擇Advanced

。

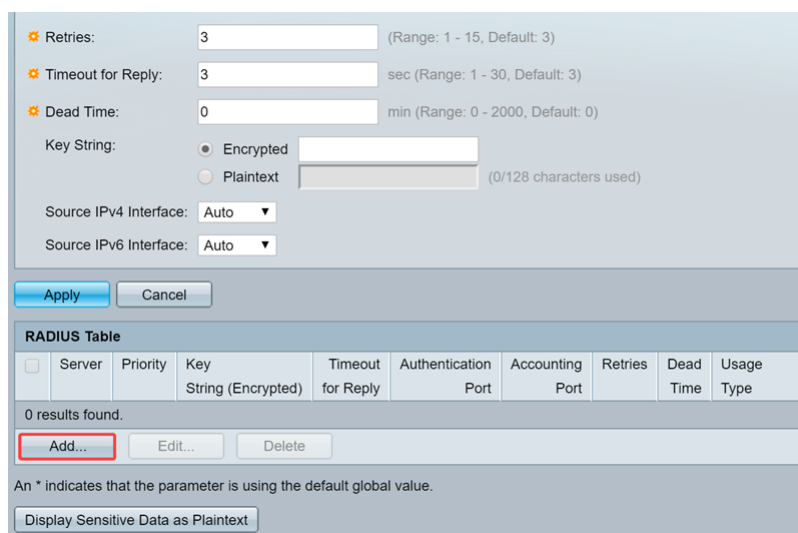
附註：可用選單選項可能會因裝置型號而異。本例中使用的是SG550X-24。



步驟2. 導覽至Security > RADIUS Client。



步驟3. 向下滾動到RADIUS Table部分，然後按一下Add...以新增RADIUS伺服器。



Server	Priority	Key String (Encrypted)	Timeout for Reply	Authentication Port	Accounting Port	Retries	Dead Time	Usage Type
0 results found.								

步驟4. 在Server Definition欄位中選擇是按IP地址或名稱指定RADIUS服務器。在IP Version欄位中選擇RADIUS伺服器的IP位址的版本。

附註：在本例中，我們將使用By IP address和Version 4。

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1

Server IP Address/Name:

Priority:  (Range: 0 - 65535)

Key String:  Use Default  User Defined (Encrypted)   User Defined (Plaintext)  (0/128 characters used)

Timeout for Reply:  Use Default  User Defined  sec (Range: 1 - 30, Default: 3)

Authentication Port:  1812 (Range: 0 - 65535, Default: 1812)

Accounting Port:  1813 (Range: 0 - 65535, Default: 1813)

Retries:  Use Default  User Defined  (Range: 1 - 15, Default: 3)

Dead Time:  Use Default  User Defined  min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  802.1x  All

步驟5.按IP地址或名稱輸入RADIUS伺服器。

附註：我們將在Server IP Address/Name欄位中輸入IP地址192.168.1.146。

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1

Server IP Address/Name:  192.168.1.146

Priority:  (Range: 0 - 65535)

Key String:  Use Default  User Defined (Encrypted)   User Defined (Plaintext)  (0/128 characters used)

Timeout for Reply:  Use Default  User Defined  sec (Range: 1 - 30, Default: 3)

Authentication Port:  1812 (Range: 0 - 65535, Default: 1812)

Accounting Port:  1813 (Range: 0 - 65535, Default: 1813)

Retries:  Use Default  User Defined  (Range: 1 - 15, Default: 3)

Dead Time:  Use Default  User Defined  min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  802.1x  All

步驟6.輸入伺服器的優先順序。優先順序確定裝置嘗試聯絡伺服器以驗證使用者的順序。裝置首先從優先順序最高的RADIUS伺服器開始。0是最高優先順序。

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String:  Use Default  
 User Defined (Encrypted)   
 User Defined (Plaintext)  (0/128 characters used)

Timeout for Reply:  Use Default  
 User Defined Default sec (Range: 1 - 30, Default: 3)

Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

Retries:  Use Default  
 User Defined Default (Range: 1 - 15, Default: 3)

Dead Time:  Use Default  
 User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  
 802.1x  
 All

步驟7.輸入用於驗證和加密裝置與RADIUS伺服器之間通訊的金鑰字串。此金鑰必須與RADIUS伺服器上配置的金鑰匹配。可以以**加密**或**明文**格式輸入。如果選擇**Use Default**，裝置會嘗試使用預設金鑰字串向RADIUS伺服器進行身份驗證。

附註：我們將使用**User Defined(Plaintext)**並輸入金鑰示例。

若要瞭解如何配置交換機上的RADIUS伺服器設定，請按一下[此處](#)。

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String:  Use Default  
 User Defined (Encrypted)   
 User Defined (Plaintext) **example** (7/128 characters used)

Timeout for Reply:  Use Default  
 User Defined Default **2** sec (Range: 1 - 30, Default: 3)

Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

Retries:  Use Default  
 User Defined Default (Range: 1 - 15, Default: 3)

Dead Time:  Use Default  
 User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  
 802.1x  
 All

步驟8.在**Timeout for Reply**欄位中，選擇**Use Default**或**User Defined**。如果選擇「**User Defined**」，請輸入裝置在重試查詢之前等待來自RADIUS伺服器的應答的秒數；如果重試的最大次數，則切換到下一個伺服器。如果選擇了**Use Default**，則裝置使用預設超時值。

附註：在本示例中，選擇了**Use Default**。

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String:  Use Default  User Defined (Encrypted)  User Defined (Plaintext) example (7/128 characters used)

Timeout for Reply:  Use Default  User Defined Default sec (Range: 1 - 30, Default: 3)

Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

Retries:  Use Default  User Defined Default (Range: 1 - 15, Default: 3)

Dead Time:  Use Default  User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  802.1x  All

Apply Close

步驟9.在 *Authentication Port* 欄位中輸入用於身份驗證請求的RADIUS伺服器埠的UDP埠號。在 *Accounting Port* 欄位中為記帳請求輸入RADIUS伺服器埠的UDP埠號。

附註：在本例中，我們將對身份驗證埠和記帳埠使用預設值。

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String:  Use Default  User Defined (Encrypted)  User Defined (Plaintext) example (7/128 characters used)

Timeout for Reply:  Use Default  User Defined Default sec (Range: 1 - 30, Default: 3)

Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

Retries:  Use Default  User Defined Default (Range: 1 - 15, Default: 3)

Dead Time:  Use Default  User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  802.1x  All

Apply Close

步驟10.如果為 *重試* 欄位選擇 **User Defined**，請輸入在認為發生故障之前傳送到RADIUS伺服器的請求數。如果選擇 **Use Default**，裝置將使用重試次數的預設值。

如果為 *Dead Time* 選擇了 **User Defined**，請輸入必須經過的分鐘數，然後才會為服務請求跳過無響應的RADIUS伺服器。如果選擇了 **Use Default**，則裝置將使用死時間的預設值。如果輸入0分鐘，則沒有死亡時間。

附註：在本例中，我們將為這兩個欄位選擇 **Use Default**。

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String:  Use Default  User Defined (Encrypted)   
 User Defined (Plaintext) example (7/128 characters used)

Timeout for Reply:  Use Default  User Defined Default sec (Range: 1 - 30, Default: 3)

Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

Retries:  Use Default  User Defined Default (Range: 1 - 15, Default: 3)

Dead Time:  Use Default  User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  802.1x  All

Apply Close

步驟11.在 *Usage Type* 欄位中，輸入RADIUS伺服器驗證型別。選項包括：

登入 - RADIUS伺服器用於驗證要求管理裝置的使用者。

802.1x - RADIUS伺服器用於802.1x身份驗證。

全部 - RADIUS伺服器用於驗證要求管理裝置的使用者和802.1x驗證。

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String:  Use Default  User Defined (Encrypted)   
 User Defined (Plaintext) example (7/128 characters used)

Timeout for Reply:  Use Default  User Defined Default sec (Range: 1 - 30, Default: 3)

Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

Retries:  Use Default  User Defined Default (Range: 1 - 15, Default: 3)

Dead Time:  Use Default  User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  802.1x  All

Apply Close

步驟12.按一下Apply。

Not secure | https://192.168.1.125/cs30a6baef/mts/mgmtauthen/security\_authen\_radius\_a\_jq.htm

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String:  Use Default  User Defined (Encrypted)  User Defined (Plaintext) example (7/128 characters used)

Timeout for Reply:  Use Default  User Defined Default sec (Range: 1 - 30, Default: 3)

Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

Retries:  Use Default  User Defined Default (Range: 1 - 15, Default: 3)

Dead Time:  Use Default  User Defined Default min (Range: 0 - 2000, Default: 0)

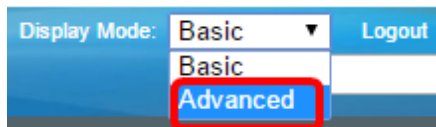
Usage Type:  Login  802.1x  All

Apply Close

## 配置802.1x埠身份驗證設定

步驟1. 登入交換器的網路型公用程式，然後在「Display Mode」下拉式清單中選擇Advanced。

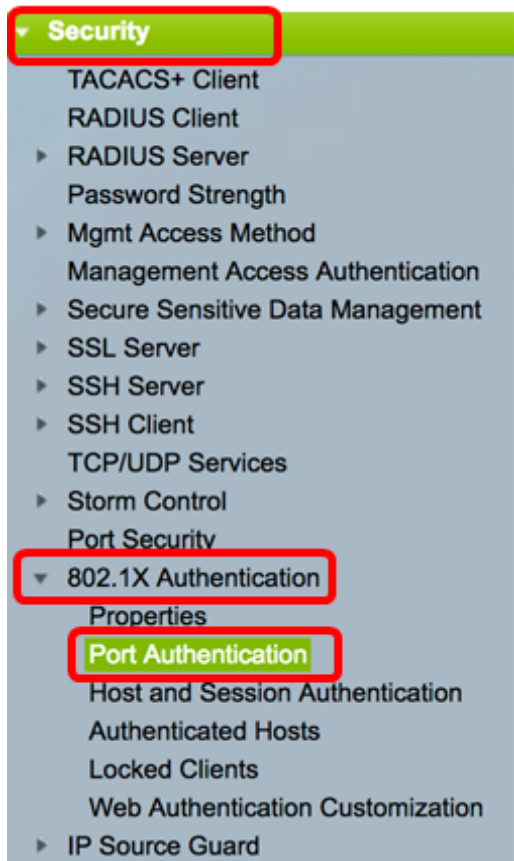
附註：可用選單選項可能會因裝置型號而異。在本示例中，使用了SG350X-48MP。



附註：如果您有Sx300或Sx500系列交換機，請跳至[步驟2](#)。

步驟2. 選擇Security > 802.1X Authentication > Port Authentication。



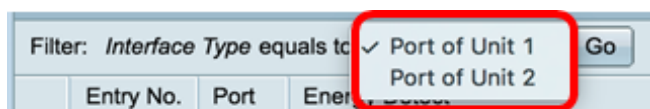


步驟3.從 *Interface Type* 下拉選單中選擇介面。

連線埠 — 如果需要只選擇單一連線埠，請在 *Interface Type* 下拉式清單中選擇 **Port**。

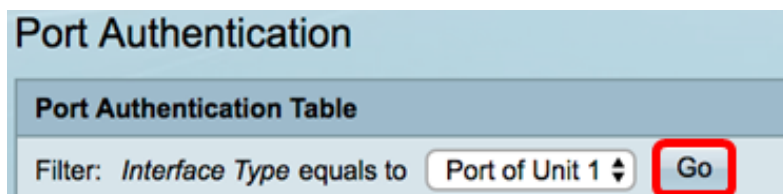
LAG — 從 *Interface Type* 下拉選單中，選擇要配置的LAG。這會影響LAG配置中定義的埠組。

**附註：** 在本示例中，選擇了裝置1的埠。



**附註：** 如果有非堆疊式交換機（例如Sx300系列交換機），請跳至[步驟5](#)。

步驟4.按一下**Go**以顯示介面上的連線埠或LAG清單。



步驟5.點選要配置的埠。

Port Authentication										
Port Authentication Table										
Filter: Interface Type equals to Port of Unit 1 <input type="button" value="Go"/>										
	Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access	802.1x Based Authentication	MAC Based Authentication	Web Based Authentication
<input type="radio"/>	1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
<input type="radio"/>	2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
<input type="radio"/>	3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
<input checked="" type="radio"/>	4	GE4	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
<input type="radio"/>	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
<input type="radio"/>	6	GE6	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled

附註：在本示例中，選擇了GE4。

步驟6. 向下滾動頁面，然後點選Edit。

<input type="radio"/>	46	GE46	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	47	GE47	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	48	GE48	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	49	XG1	Authorized	Force Authorized	Disabled	Disabled
<input type="radio"/>	50	XG2	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	51	XG3	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	52	XG4	Authorized	Force Authorized	Disabled	Disabled

Copy Settings...

步驟7. (可選) 如果要編輯另一個介面，請從Unit and Port下拉選單中選擇。

Interface:

Current Port Control: Authorized

附註：在本示例中，選擇了裝置1的埠GE4。

步驟8. 點選與Administrative Port Control區域中的所需埠控制對應的單選按鈕。選項包括：

強制未授權 — 通過將埠移動到未授權狀態來拒絕介面訪問。連線埠將捨棄流量。

自動 — 根據請求方的身份驗證，埠在已授權或未授權狀態之間移動。

強制授權 — 未經驗證就授權埠。連線埠會轉送流量。

Administrative Port Control:  Force Unauthorized  Auto  Force Authorized

附註：在本示例中，選擇了Auto。

步驟9. 按一下RADIUS VLAN分配單選按鈕，在所選埠上配置動態VLAN分配。選項包括：

禁用 — 功能未啟用。

拒絕 — 如果RADIUS伺服器授權了請求方，但沒有提供請求方VLAN，則請求方被拒絕。

靜態 — 如果RADIUS伺服器授權了請求方，但沒有提供請求方VLAN，則接受請求方。

RADIUS VLAN Assignment:  Disable  
 Reject  
 Static

附註：在此示例中，選擇了Static。

步驟10.選中Guest VLAN覈取方塊中的**Enable**，為未授權的埠啟用訪客VLAN。訪客VLAN使未經授權的埠自動加入在802.1屬性的訪客VLAN ID區域中選擇的VLAN。

Guest VLAN:  Enable

步驟11。(可選)選中**Enable** Open Access覈取方塊以啟用開放訪問。Open Access可幫助您瞭解連線到網路的主機的配置問題，監控不良情況並使這些問題得以解決。

附註：在介面上啟用開放存取時，交換器會將從RADIUS伺服器收到的所有失敗視為成功，並允許連線到介面的站台存取網路，而不論驗證結果如何。在此範例中，開放存取功能已停用。

Guest VLAN:  Enable  
Open Access:  Enable

步驟12.選中**Enable** 802.1x Based Authentication覈取方塊以在埠上啟用802.1X身份驗證。

Guest VLAN:  Enable  
Open Access:  Enable  
802.1x Based Authentication:  Enable

步驟13.選中**Enable** MAC Based Authentication覈取方塊以基於請求方MAC地址啟用埠身份驗證。埠上只能使用八種基於MAC的身份驗證。

附註：要使MAC身份驗證成功，RADIUS伺服器請求方使用者名稱和密碼必須是請求方MAC地址。MAC地址必須用小寫字母輸入，且不能使用。或 — 分隔符（例如0020aa00bcc）。

802.1x Based Authentication:  Enable  
MAC Based Authentication:  Enable

附註：在本示例中，基於MAC的身份驗證被禁用。

步驟14.選中**Enable** Web Based Authentication覈取方塊以在交換機上啟用基於Web的身份驗證。在本示例中，基於Web的身份驗證被禁用。

802.1x Based Authentication:  Enable  
MAC Based Authentication:  Enable  
Web Based Authentication:  Enable

附註：在本示例中，基於Web的身份驗證被禁用。

步驟15。(可選)選中**Enable** Periodic Reauthentication覈取方塊以強制埠在給定時間後重新進行身份驗證。此時間在*Reauthentication Period*欄位中定義。

Web Based Authentication:  Enable  
Periodic Reauthentication:  Enable

附註：在此範例中，啟用期間重新驗證。

步驟16。（可選）在 *Reauthentication Period* 欄位中輸入值。此值表示介面重新驗證連線埠之前的秒數。預設值為3600秒，範圍為300到4294967295秒。

Periodic Reauthentication:  Enable  
Reauthentication Period:  sec

附註：在本例中，配置了6000秒。

步驟17。（可選）選中 **Enable Reauthenticate Now** 覈取方塊以強制立即對埠重新進行身份驗證。在此範例中，停用即時重新驗證。

Periodic Reauthentication:  Enable  
Reauthentication Period:  sec  
Reauthenticate Now:    
Authenticator State: Force Authorized

Authenticator State 區域顯示埠的授權狀態。

步驟18。（可選）勾選 **Enable Time Range** 覈取方塊以對埠獲得授權的時間進行限制。

Time Range:  Enable  
Time Range Name:  Edit

附註：在此示例中，啟用時間範圍。如果您希望跳過此功能，請繼續 [步驟20](#)。

步驟19。（可選）從 Time Range Name 下拉選單中選擇要使用的時間範圍。

Time Range:  Enable  
Time Range Name:  NightShift  
Maximum WBA Login Attempts:

附註：在此示例中，選擇了 Dayshift。

步驟20.在 Maximum WBA Login Attempts 區域中，按一下 Infinite for no limit 或 User Defined 設定限制。如果選擇了「使用者定義」，請輸入基於Web的身份驗證允許的最大登入嘗試次數。

Maximum WBA Login Attempts:  Infinite  User Defined

附註：在此示例中，選擇了 Infinite。

步驟21.在 Maximum WBA Silence Period (最大WBA靜默期) 區域中，按一下 Infinite for no limit (無限制) 或 User Defined (使用者定義) 設定限制。如果選擇使用者定義，請輸入介面上允許的基於Web的身份驗證的靜默期的最大長度。

Maximum WBA Silence Period:  Infinite  User Defined  sec

附註：在此示例中，選擇了Infinite。

步驟22.在「最大主機數」區域中，按一下「無限制」或「使用者定義」以設定限制。如果選擇使用者定義，請輸入介面上允許的最大授權主機數。

Max Hosts:  Infinite  User Defined

附註：將此值設定為1可在多會話模式下模擬單主機模式進行基於Web的身份驗證。在此示例中，選擇了Infinite。

步驟23.在*Quiet Period*欄位中，輸入交換器在驗證交換失敗後保持安靜狀態的時間。當交換機處於安靜狀態時，這意味著交換機沒有偵聽來自客戶端的新身份驗證請求。預設值為60秒，範圍為1到65535秒。

Quiet Period:

附註：在本示例中，安靜時段設定為120秒。

步驟24.在*重新傳送EAP*欄位中，輸入交換機在重新傳送請求之前等待請求方響應消息的時間。預設值為30秒，範圍為1到65535秒。

Quiet Period:   
Resending EAP:

附註：在本示例中，重新傳送EAP設定為60秒。

步驟25.在*Max EAP Requests*欄位中，輸入可以傳送的最大EAP請求數。EAP是在802.1X中使用的一種身份驗證方法，它提供交換機和客戶端之間的身份驗證資訊交換。在這種情況下，會將EAP請求傳送到客戶端進行身份驗證。然後，客戶端必須響應並匹配身份驗證資訊。如果客戶端未響應，則根據重新傳送EAP值設定另一個EAP請求，並重新啟動身份驗證過程。預設值為2，範圍為1到10。

Quiet Period:   
Resending EAP:   
Max EAP Requests:

附註：在本示例中，使用預設值2。

步驟26.在*Supplicant Timeout*欄位中，輸入EAP請求重新傳送到請求方的時間。預設值為30秒，範圍為1到65535秒。

☛ Max EAP Requests:  (Rar

☛ Supplicant Timeout:  sec |

**附註：**在此示例中，請求方超時設定為60秒。

步驟27.在 *Server Timeout* 欄位中，輸入交換器再次向RADIUS伺服器傳送要求之前經過的時間。預設值為30秒，範圍為1到65535秒。

☛ Max EAP Requests:  (Ran

☛ Supplicant Timeout:  sec |

☛ Server Timeout:  sec |

**附註：**在此示例中，伺服器超時設定為60秒。

步驟28.按一下**Apply**，然後按一下**Close**。

Interface:	Unit	1	Port	GE4
Current Port Control:	Unauthorized			
Administrative Port Control:	<input type="radio"/> Force Unauthorized <input checked="" type="radio"/> Auto <input type="radio"/> Force Authorized			
RADIUS VLAN Assignment:	<input type="radio"/> Disable <input type="radio"/> Reject <input checked="" type="radio"/> Static			
Guest VLAN:	<input checked="" type="checkbox"/> Enable			
Open Access:	<input type="checkbox"/> Enable			
802.1x Based Authentication:	<input checked="" type="checkbox"/> Enable			
MAC Based Authentication:	<input type="checkbox"/> Enable			
Web Based Authentication:	<input type="checkbox"/> Enable			
Periodic Reauthentication:	<input checked="" type="checkbox"/> Enable			
Reauthentication Period:	6000	sec (Range: 300 - 4294967295, Default: 3600)		
Reauthenticate Now:	<input type="checkbox"/>			
Authenticator State:	Connecting			
Time Range:	<input type="checkbox"/> Enable			
Time Range Name:	Dayshift <a href="#">Edit</a>			
Maximum WBA Login Attempts:	<input checked="" type="radio"/> Infinite <input type="radio"/> User Defined <input type="text"/> (Range: 3 - 10)			
Maximum WBA Silence Period:	<input checked="" type="radio"/> Infinite <input type="radio"/> User Defined <input type="text"/> sec (Range: 60 - 65535)			
Max Hosts:	<input checked="" type="radio"/> Infinite <input type="radio"/> User Defined <input type="text"/> sec (Range: 1 - 4294967295)			
Quiet Period:	120	sec (Range: 10 - 65535, Default: 60)		
Resending EAP:	60	sec (Range: 30 - 65535, Default: 30)		
Max EAP Requests:	2	(Range: 1 - 10, Default: 2)		
Supplicant Timeout:	60	sec (Range: 1 - 65535, Default: 30)		
Server Timeout:	60	sec (Range: 1 - 65535, Default: 30)		
<b>Apply</b> <input type="button" value="Close"/>				

步驟29。(可選)按一下**Save**，將設定儲存到啟動組態檔中。



Save

### 3-Port Gigabit PoE Stackable Managed Switch

#### Port Authentication

**Port Authentication Table**

Filter: *Interface Type* equals to

	Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access
<input type="radio"/>	1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	4	GE4	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	6	GE6	Port Down	Force Authorized	Disabled	Disabled	Disabled

現在，您應該在交換機上成功配置802.1x埠身份驗證設定。

## 將介面配置設定應用到多個介面

步驟1. 按一下要將身份驗證配置應用到多個介面的介面的單選按鈕。

**Port Authentication Table**

Filter: *Interface Type* equals to

	Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access
<input type="radio"/>	1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input checked="" type="radio"/>	4	GE4	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled

**附註：** 在本示例中，選擇了GE4。

步驟2. 向下滾動，然後按一下「Copy Settings」。

<input type="radio"/>	43	GE43	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	44	GE44	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	45	GE45	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	46	GE46	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	47	GE47	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	48	GE48	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	49	XG1	Authorized	Force Authorized	Disabled	Disabled
<input type="radio"/>	50	XG2	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	51	XG3	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	52	XG4	Authorized	Force Authorized	Disabled	Disabled

步驟3. 在to欄位中輸入要應用所選介面配置的介面範圍。您可以使用介面編號或介面名稱作為輸入。可以輸入以逗號分隔的每個介面（如1、3、5或GE1、GE3、GE5），也可以輸入介面範圍（如1-5或GE1-GE5）。



Copy configuration from entry 4 (GE4)

to:  (Example: 1,3,5-10 or: GE1,GE3-XG4)

附註：在本示例中，配置設定將應用於埠47至48。

步驟4. 按一下Apply，然後按一下Close。

Copy configuration from entry 4 (GE4)

to:  (Example: 1,3,5-10 or: GE1,GE3-XG4)

下圖說明設定之後的變更。

Port Authentication Table							
Filter: <i>Interface Type</i> equals to <input type="text" value="Port of Unit 1"/> <input type="button" value="Go"/>							
	Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access
<input type="radio"/>	1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	4	GE4	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	6	GE6	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	45	GE45	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	46	GE46	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	47	GE47	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	48	GE48	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	49	XG1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	50	XG2	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	51	XG3	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	52	XG4	Authorized	Force Authorized	Disabled	Disabled	Disabled

現在，您應該已經成功複製了一個埠的802.1x身份驗證設定，並將其應用到交換機上的其他埠或埠。