在交換機上配置基於MAC的身份驗證

目標

802.1X是一種管理工具，允許列出裝置，確保不對您的網路進行未經授權的訪問。本文顯示如何使用圖形使用者介面(GUI)在交換機上配置基於MAC的身份驗證。 若要瞭解如何使用命令列介面(CLI)配置基於MAC的身份驗證，請按一下此處。

附註：本指南在9節和1節中有很長的篇幅用於驗證主機是否已經過身份驗證。喝咖啡、喝茶或者喝水，確保您有充足的時間回顧並執行相關步驟。

請參閱辭彙表以瞭解其他資訊。

RADIUS 如何運作？

802.1X驗證有三個主要元件：請求方（使用者端）、驗證者(網路裝置（例如交換器）和驗證伺服器(RADIUS)。 遠端身份驗證撥入使用者服務(RADIUS)是一種使用身份驗證、授權和記帳(AAA)協定的訪問伺服器，可幫助管理網路訪問。RADIUS使用使用者端 — 伺服器型號，其中在RADIUS伺服器和一個或多個RADIUS使用者端之間交換安全驗證資訊。它驗證客戶端的身份並通知交換機客戶端是否有權訪問LAN。

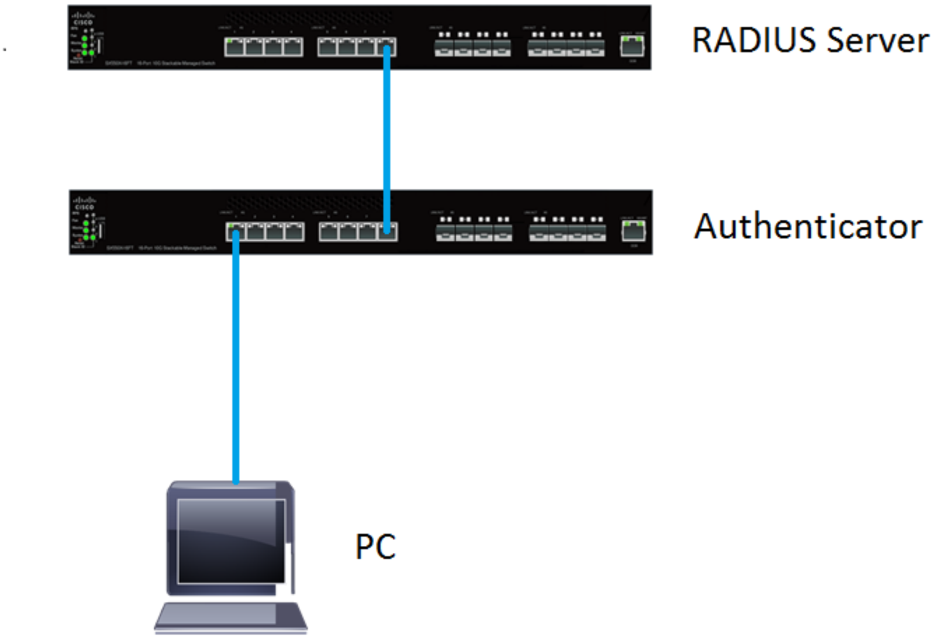
驗證器在客戶端和驗證伺服器之間工作。首先，向客戶端請求身份資訊。作為響應，驗證器將驗證與驗證伺服器之間的資訊。最後，它將向客戶端轉發響應。在本文中，驗證器將是包含RADIUS使用者端的交換器。交換器將能夠封裝和解除封裝可擴充驗證通訊協定(EAP)訊框，以便與驗證伺服器互動。

基於MAC的身份驗證呢？

在基於MAC的身份驗證中，當請求方不知道如何與驗證方通話或無法與驗證方通話時，它會使用主機的MAC地址進行身份驗證。使用純RADIUS（不使用EAP）對基於MAC的請求方進行身份驗證。RADIUS伺服器有一個專用主機資料庫，其中只包含允許的MAC位址。伺服器不是將基於MAC的身份驗證請求視為密碼身份驗證協定(PAP)身份驗證，而是通過屬性6 [Service-Type] = 10識別此類請求。它們會將Calling-Station-Id屬性中的MAC地址與儲存在主機資料庫中的MAC地址進行比較。

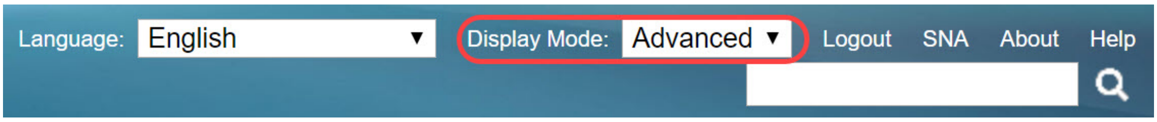
2.4版增加了配置為基於MAC的客戶端傳送的使用者名稱格式的功能，可以定義EAP身份驗證方法或純RADIUS。在此版本中，您還可以為基於MAC的Supplicant客戶端配置使用者名稱格式，以及配置不同於使用者名稱的特定密碼。

拓撲：



附註：在本文中，我們將對RADIUS伺服器和身份驗證器使用SG550X-24。RADIUS伺服器的靜態IP位址為192.168.1.100，而驗證器的靜態IP位址為192.168.1.101。

本檔案中的步驟在**進階顯示**模式下執行。若要將模式更改為高級，請轉到右上角，然後在「*顯示模式」下拉選單中選擇***Advanced**。


Language: English

Display Mode: Advanced

目錄

適用裝置

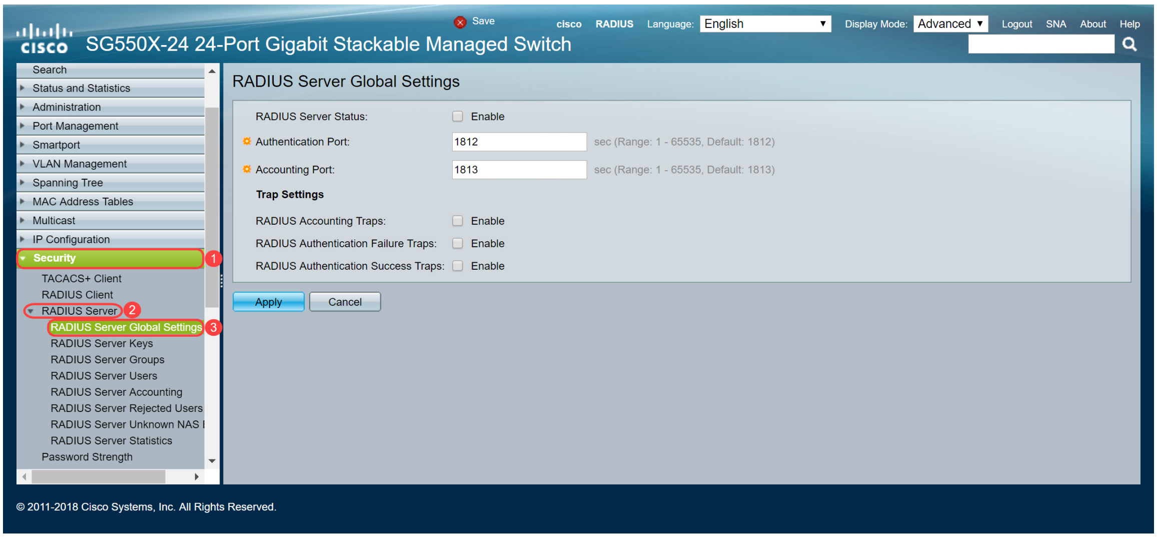
- Sx350X系列
- SG350XG系列
- Sx550X系列
- SG550XG系列

軟體版本

- 2.4.0.94

RADIUS伺服器全域性設定

步驟1。登入將設定為RADIUS伺服器的交換器的網路型公用程式，然後導覽至**Security > RADIUS Server > RADIUS Server Global Settings**。



RADIUS Server Global Settings

RADIUS Server Status: □ Enable

Authentication Port: 1812 sec (Range: 1 - 65535, Default: 1812)

Accounting Port: 1813 sec (Range: 1 - 65535, Default: 1813)

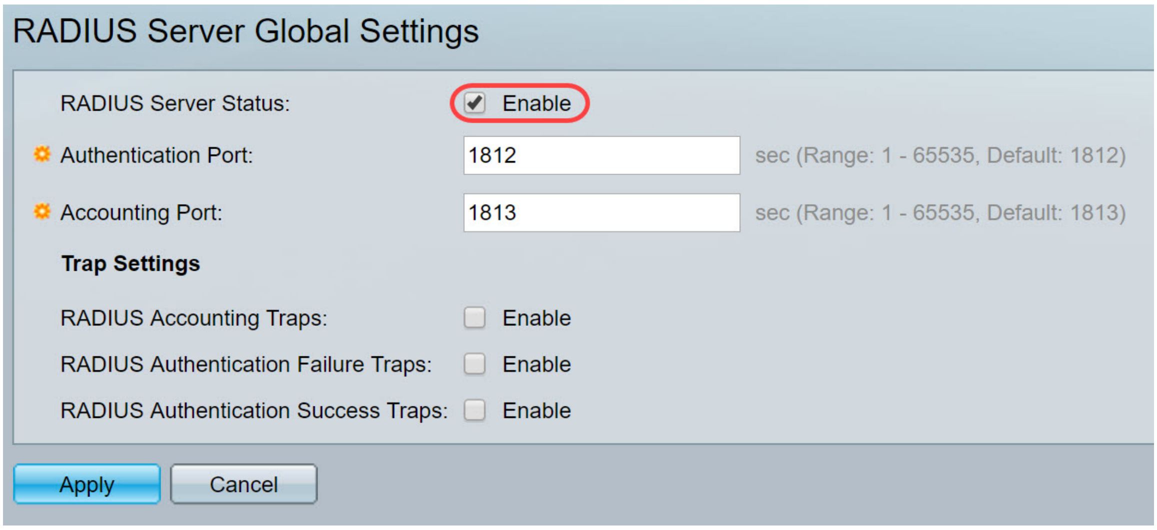
Trap Settings

RADIUS Accounting Traps: □ Enable

RADIUS Authentication Failure Traps: □ Enable

RADIUS Authentication Success Traps: □ Enable

步驟2.要啟用RADIUS伺服器功能狀態，請選中*RADIUS伺服器狀態*欄位中的**啟用**覈取方塊。



RADIUS Server Global Settings

RADIUS Server Status: ☑ Enable

Authentication Port: 1812 sec (Range: 1 - 65535, Default: 1812)

Accounting Port: 1813 sec (Range: 1 - 65535, Default: 1813)

Trap Settings

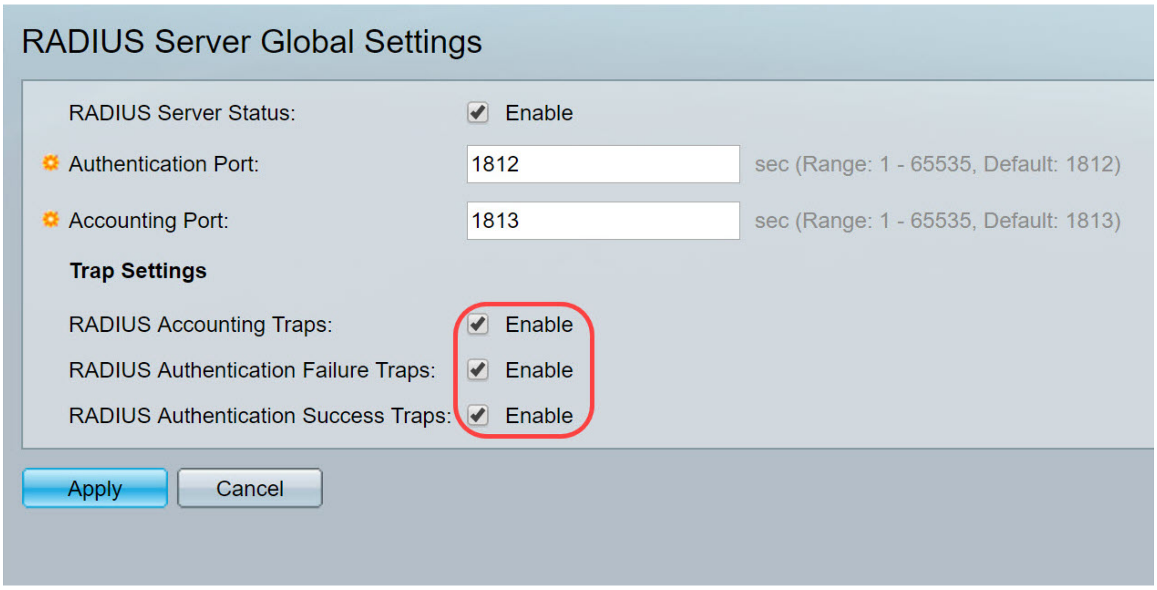
RADIUS Accounting Traps: □ Enable

RADIUS Authentication Failure Traps: □ Enable

RADIUS Authentication Success Traps: □ Enable

步驟3.要為RADIUS記帳事件、失敗的登入或成功的登入生成陷阱，請選中所需的**啟用**覈取方塊以生成陷阱。陷阱是通過簡單網路管理協定(SNMP)生成的系統事件消息。發生違規時，陷阱會傳送到交換器的SNMP管理員。以下陷阱設定：

- RADIUS記帳陷阱 — 選中可為RADIUS記帳事件生成陷阱。
- RADIUS身份驗證失敗陷阱 — 選中為失敗的登入生成陷阱。
- RADIUS身份驗證成功陷阱 — 選中為成功的登入生成陷阱。



RADIUS Server Global Settings

RADIUS Server Status: ☑ Enable

Authentication Port: 1812 sec (Range: 1 - 65535, Default: 1812)

Accounting Port: 1813 sec (Range: 1 - 65535, Default: 1813)

Trap Settings

RADIUS Accounting Traps: ☑ Enable

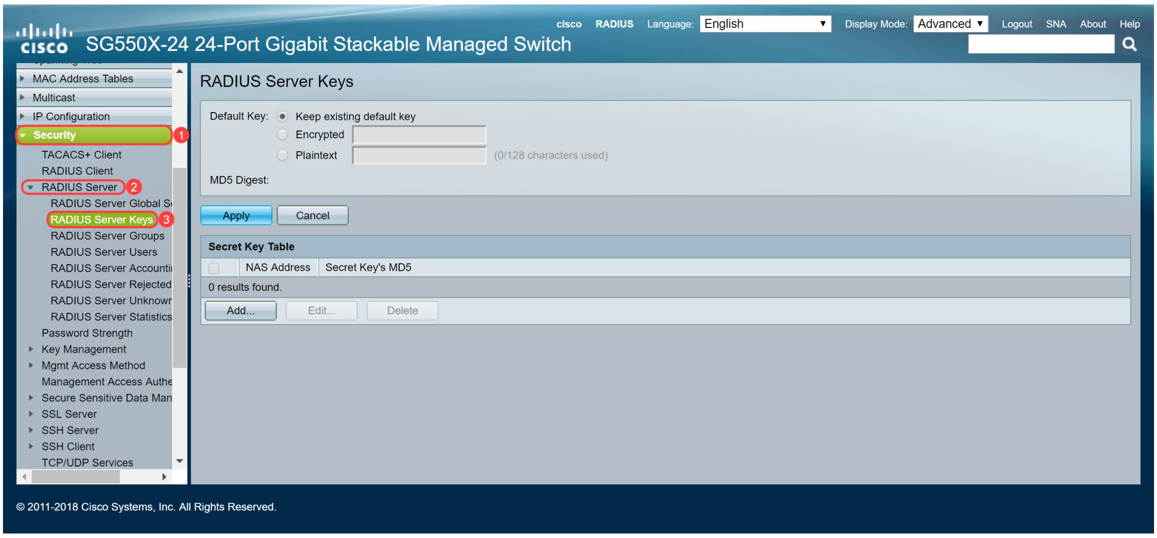
RADIUS Authentication Failure Traps: ☑ Enable

RADIUS Authentication Success Traps: ☑ Enable

步驟4.按一下**Apply**以儲存設定。

RADIUS伺服器金鑰

步驟1。導覽至**Security > RADIUS Server > RADIUS Server Keys**。將開啟「*RADIUS伺服器金鑰*」頁面。



RADIUS Server Keys

Default Key: ● Keep existing default key
○ Encrypted
○ Plaintext (0/128 characters used)

MD5 Digest:

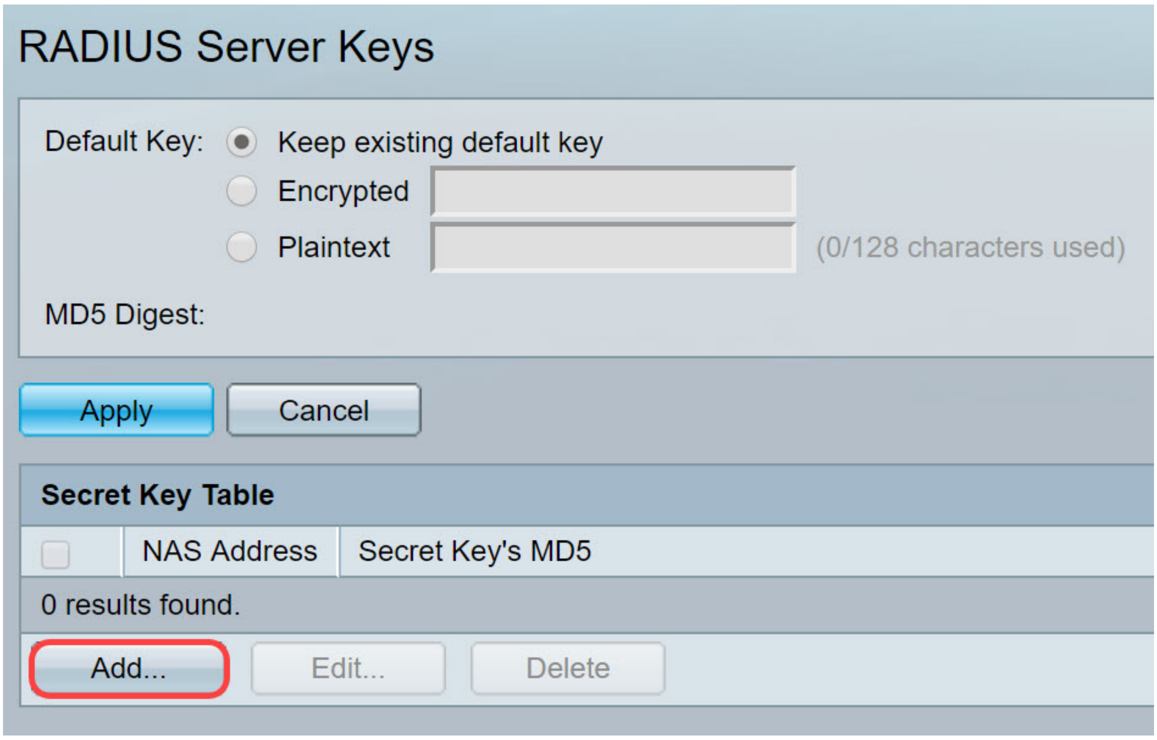
Secret Key Table

□	NAS Address	Secret Key's MD5

0 results found.

© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

步驟2.在「*Secret Key Table*」部分，按一下**Add...** 新增金鑰。



RADIUS Server Keys

Default Key: ● Keep existing default key
○ Encrypted
○ Plaintext (0/128 characters used)

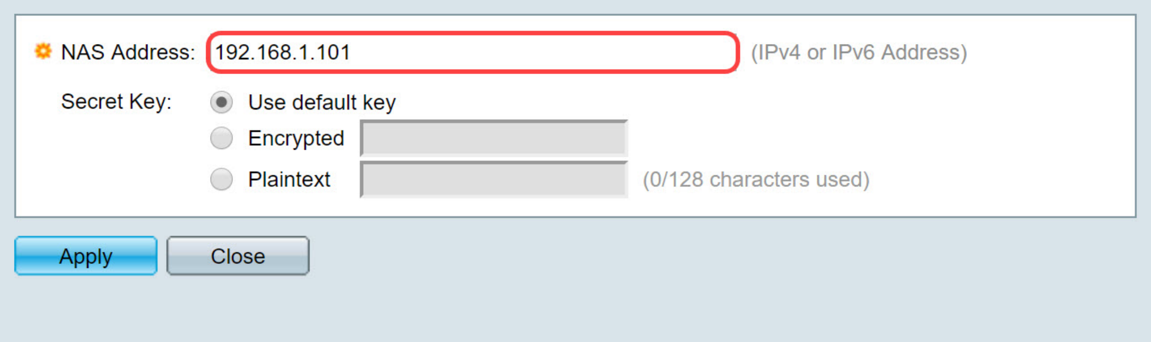
MD5 Digest:

Secret Key Table

□	NAS Address	Secret Key's MD5

0 results found.

步驟3.*Add Secret Key視窗*頁面開啟。在「*NAS Address*」欄位中，輸入包含RADIUS使用者端的交換器位址。在本例中，我們將使用IP地址192.168.1.101作為RADIUS客戶端。



NAS Address: 192.168.1.101 (IPv4 or IPv6 Address)

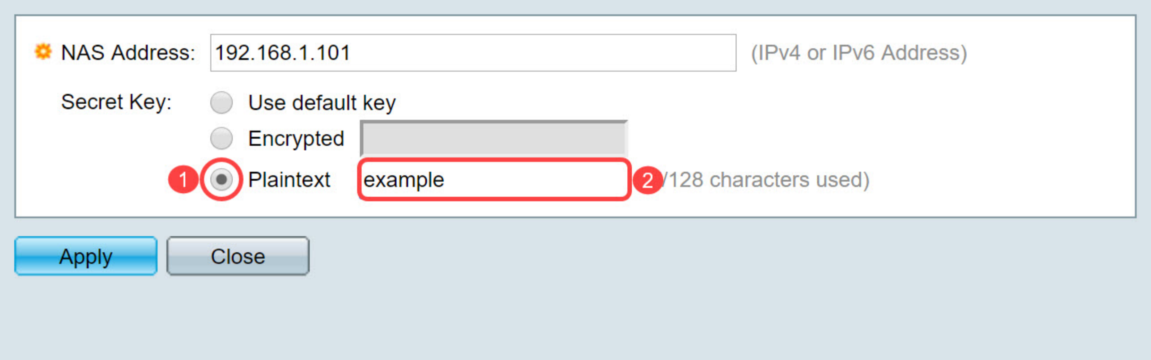
Secret Key: ● Use default key
○ Encrypted
○ Plaintext (0/128 characters used)

步驟4.選擇一個單選按鈕作為密鑰。以下選項是：

- 使用預設金鑰 — 對於指定的伺服器，裝置會嘗試使用現有的預設金鑰字串對RADIUS客戶端進行身份驗證。
- 已加密 — 若要使用訊息摘要演演算法5(MD5)加密通訊，請按加密格式輸入金鑰。
- 明文 — 在明文模式下輸入金鑰字串。

在本例中，我們將選擇*Plaintext*，然後使用**example**一詞作為*金鑰*。按下apply後，您的金鑰將採用加密形式。

附註：建議不要將example一詞用作金鑰。請使用更強金鑰。最多可使用128個字元。如果密碼太複雜而無法記憶，那麼它是一個不錯的密碼，但更棒的是，你可以把密碼變成一個讓人難忘的密碼短語，裡面會有特殊字元和數字來替代母音 — 「P@55w0rds@reH@rdT0Remember」。 最好不要使用字典裡的任何單詞。最好選擇短語，並將一些字母換成特殊字元和數字。如需詳細資訊，請參閱此思科部落格。



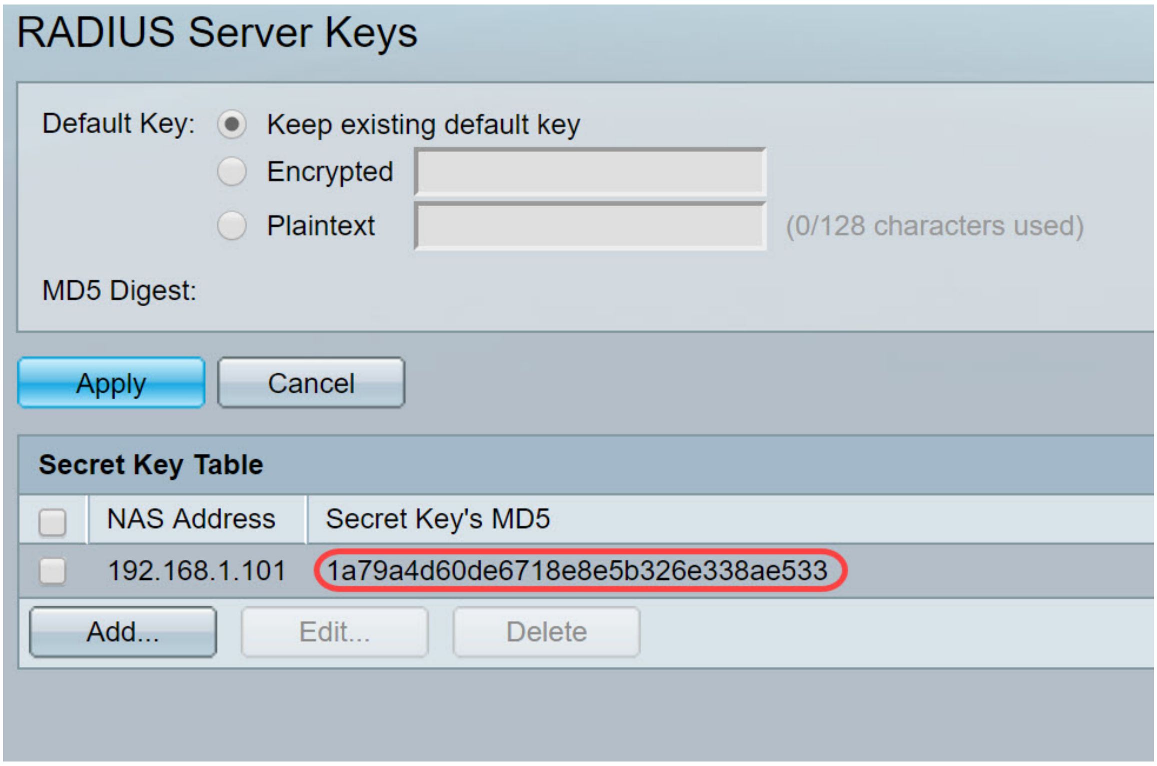
NAS Address: 192.168.1.101 (IPv4 or IPv6 Address)

Secret Key: ○ Use default key

○ Encrypted

● Plaintext example /128 characters used)

步驟5.按一下**Apply**以儲存組態。金鑰現在使用MD5加密。MD5是一個加密雜湊函式，它獲取資料並建立了一個典型的不可重複的唯一十六進位制輸出。MD5使用128位雜湊值。



RADIUS Server Keys

Default Key: ● Keep existing default key

○ Encrypted

○ Plaintext (0/128 characters used)

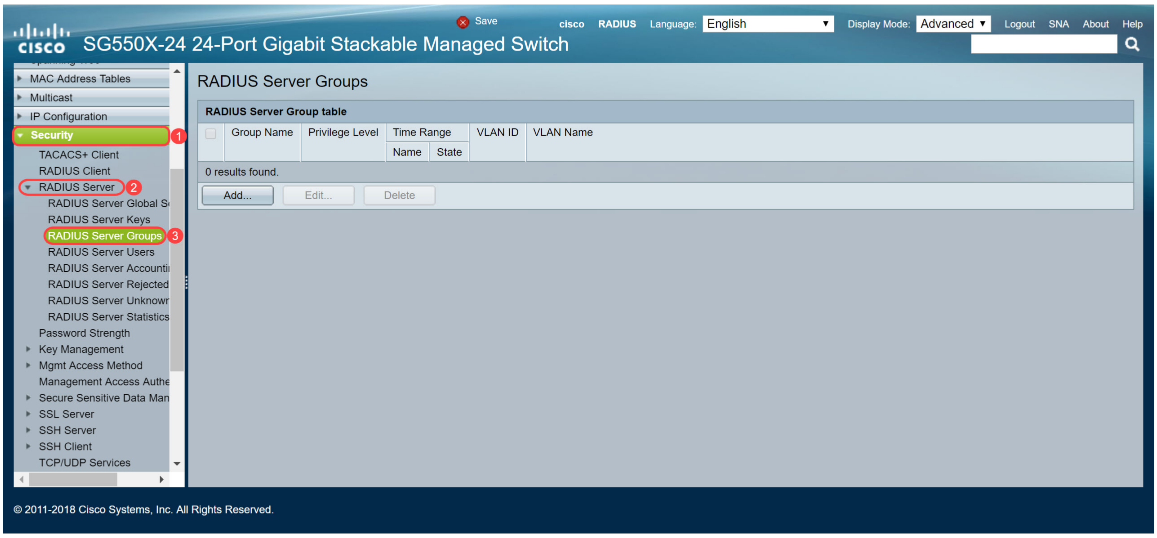
MD5 Digest:

Secret Key Table

□	NAS Address	Secret Key's MD5
□	192.168.1.101	1a79a4d60de6718e8e5b326e338ae533

RADIUS伺服器群組

步驟1。導覽至**Security > RADIUS Server > RADIUS Server Groups**。



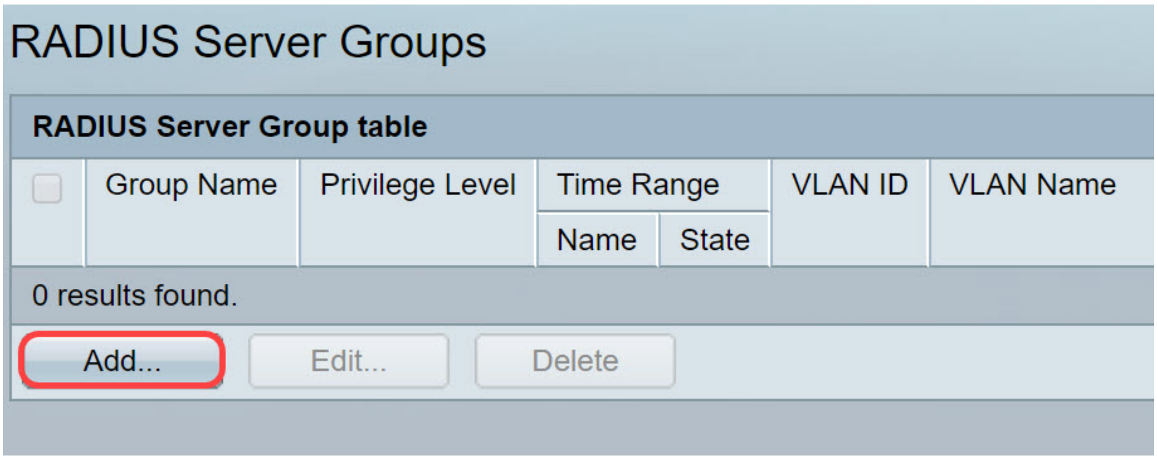
RADIUS Server Groups

RADIUS Server Group table

□	Group Name	Privilege Level	Time Range		VLAN ID	VLAN Name
			Name	State		

0 results found.

步驟2.按一下「**Add...**」 新增新的RADIUS伺服器組。

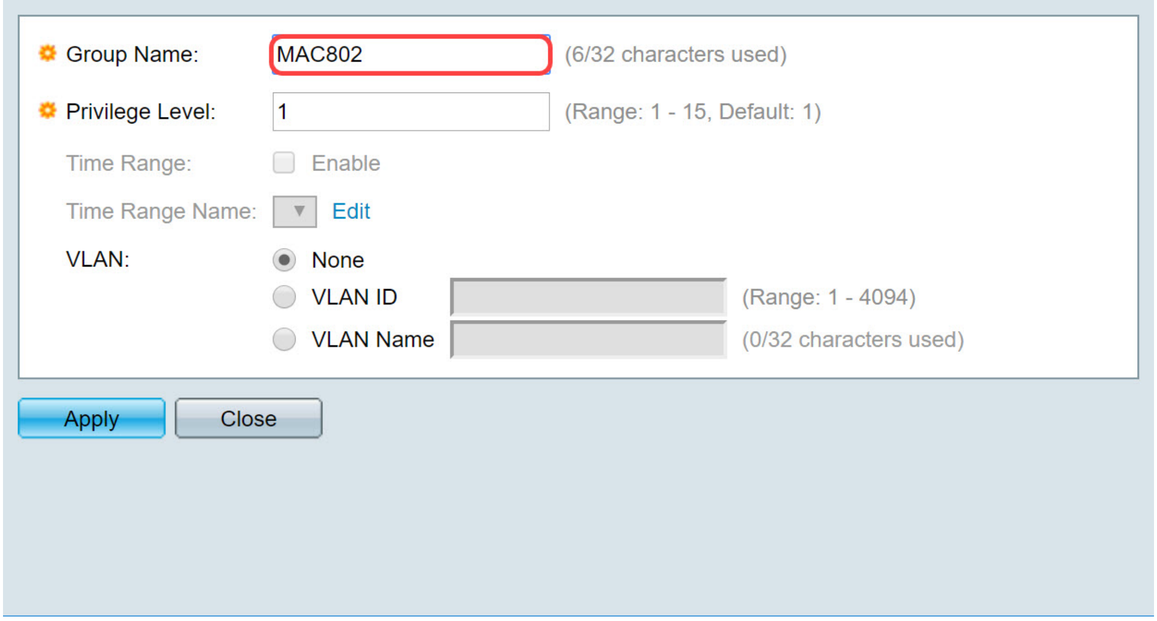


RADIUS Server Groups

RADIUS Server Group table

□	Group Name	Privilege Level	Time Range		VLAN ID	VLAN Name
			Name	State		
0 results found.						

步驟3. *Add RADIUS Server Group* 頁面隨即開啟。輸入組的名稱。在本例中，我們將使用**MAC802**作為我們的組名。



Group Name: MAC802 (6/32 characters used)

Privilege Level: 1 (Range: 1 - 15, Default: 1)

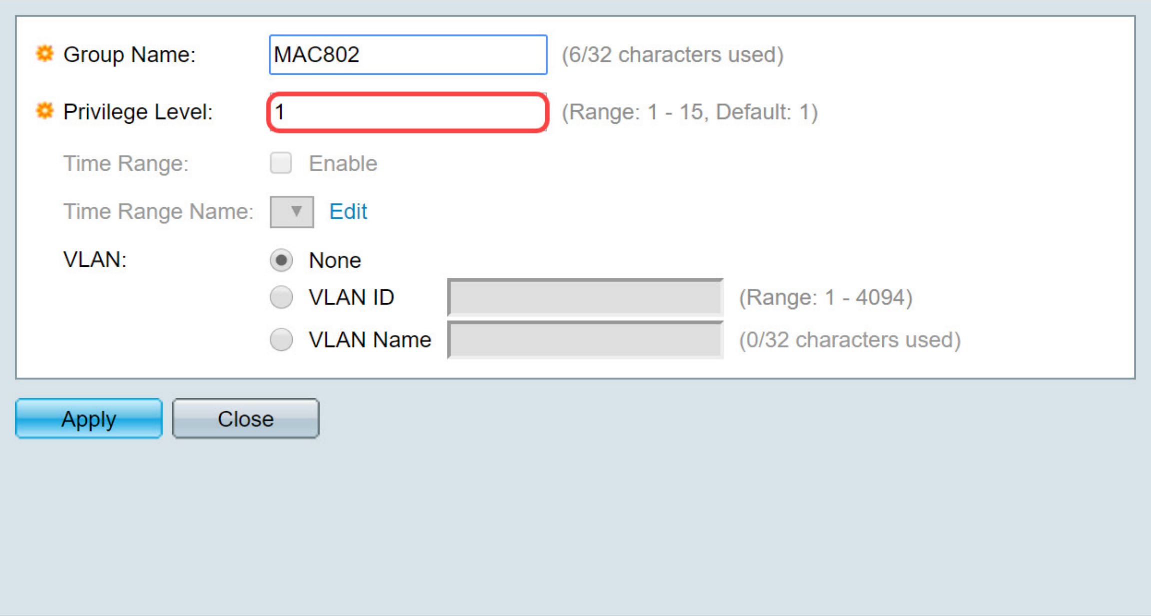
Time Range: □ Enable

Time Range Name: ▼ Edit

VLAN: ● None
○ VLAN ID (Range: 1 - 4094)
○ VLAN Name (0/32 characters used)

步驟4.在「許可權級別」欄位中輸入組的管理*訪問許可權*級別。範圍是1 - 15，其中15表示最高許可權，預設值為1。在本示例中，我們將保留許可權級別為1。

附註：我們不會在本文中配置*時間範圍*或*VLAN*。



Group Name: MAC802 (6/32 characters used)

Privilege Level: 1 (Range: 1 - 15, Default: 1)

Time Range: □ Enable

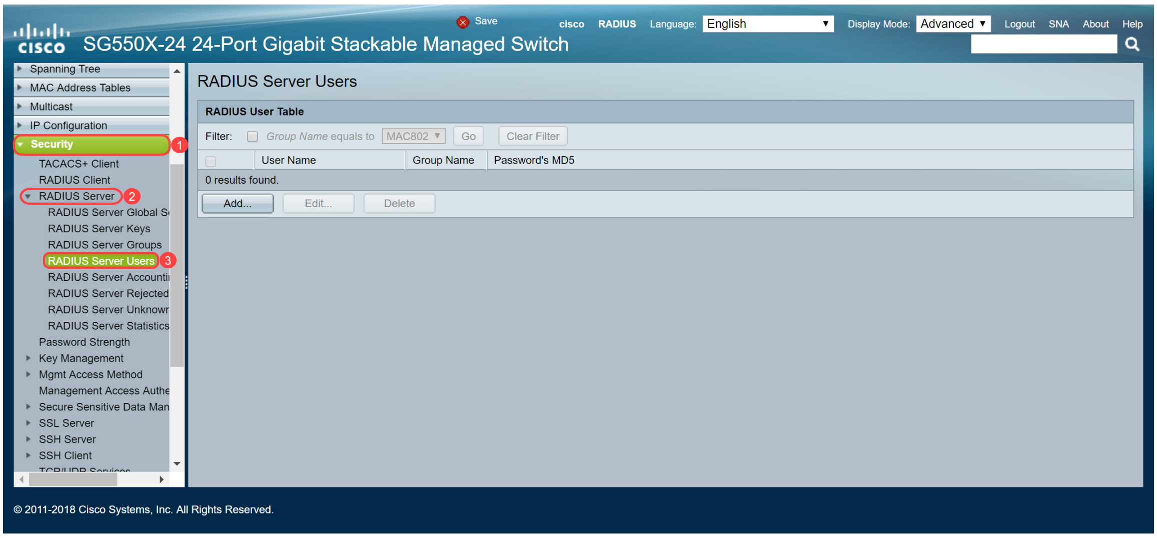
Time Range Name: ▼ Edit

VLAN: ● None
○ VLAN ID (Range: 1 - 4094)
○ VLAN Name (0/32 characters used)

步驟5.按一下**Apply**以儲存設定。

RADIUS伺服器使用者

步驟1。導覽至**Security > RADIUS Server > RADIUS Server Users**，以設定RADIUS使用者。



RADIUS Server Users

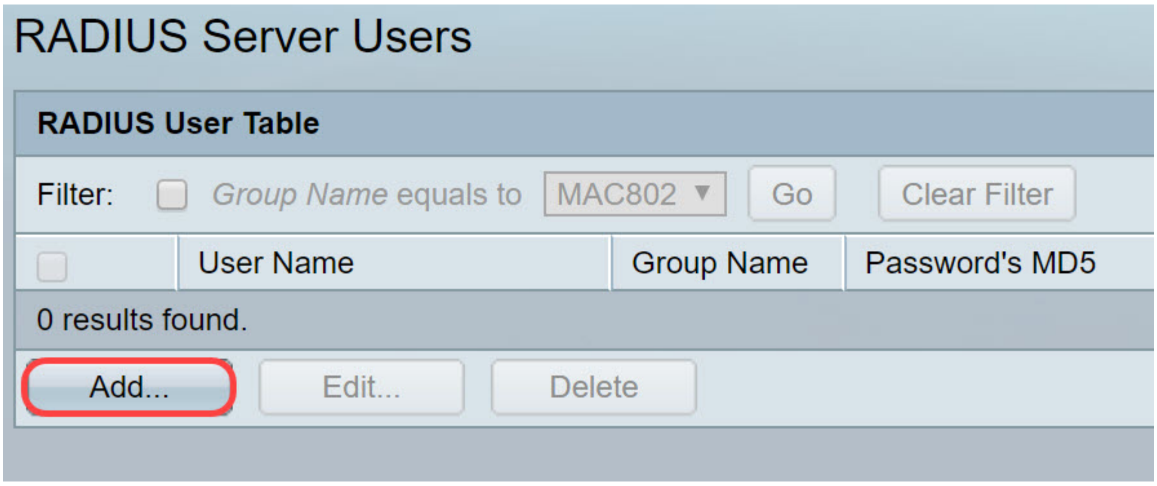
RADIUS User Table

Filter: □ *Group Name* equals to MAC802 ▼ Go Clear Filter

□	User Name	Group Name	Password's MD5
0 results found.			

© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

步驟2.按一下「**Add...**」 新增新使用者。



RADIUS Server Users

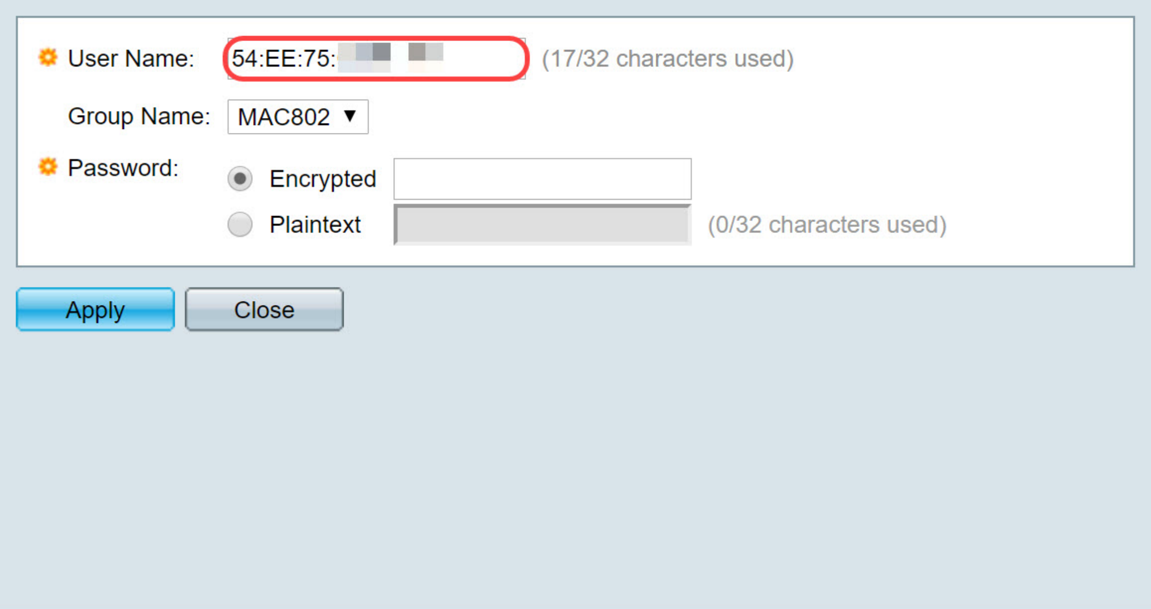
RADIUS User Table

Filter: □ *Group Name* equals to MAC802 ▼ Go Clear Filter

□	User Name	Group Name	Password's MD5
0 results found.			

步驟3. *Add RADIUS Server User* 頁面隨即開啟。在*User Name*欄位中，輸入使用者的MAC地址。在本例中，我們將在電腦上使用我們的乙太網MAC地址。

附註：部分MAC地址已模糊。



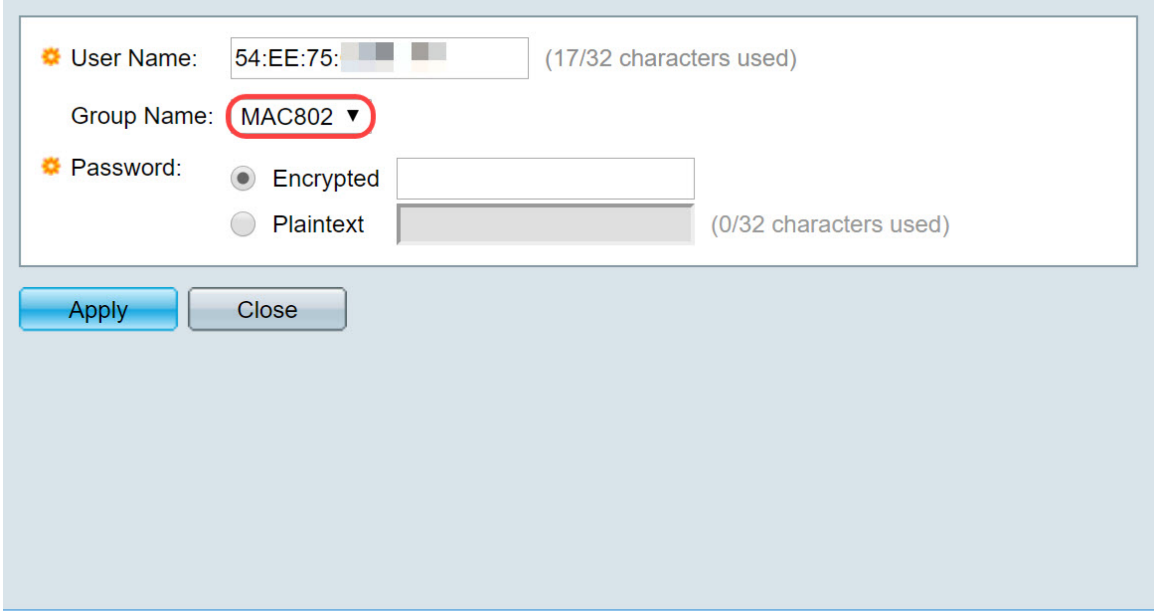
User Name: 54:EE:75:[redacted] (17/32 characters used)

Group Name: MAC802 ▼

Password: ● Encrypted

○ Plaintext (0/32 characters used)

步驟4.在*Group Name*下拉式清單中選擇一個組。如RADIUS伺服器群組一節的步驟3所強調，我們將為此使用者選擇MAC802作為我們的群組名稱。



User Name: 54:EE:75:[redacted] (17/32 characters used)

Group Name: MAC802 ▼

Password: ● Encrypted

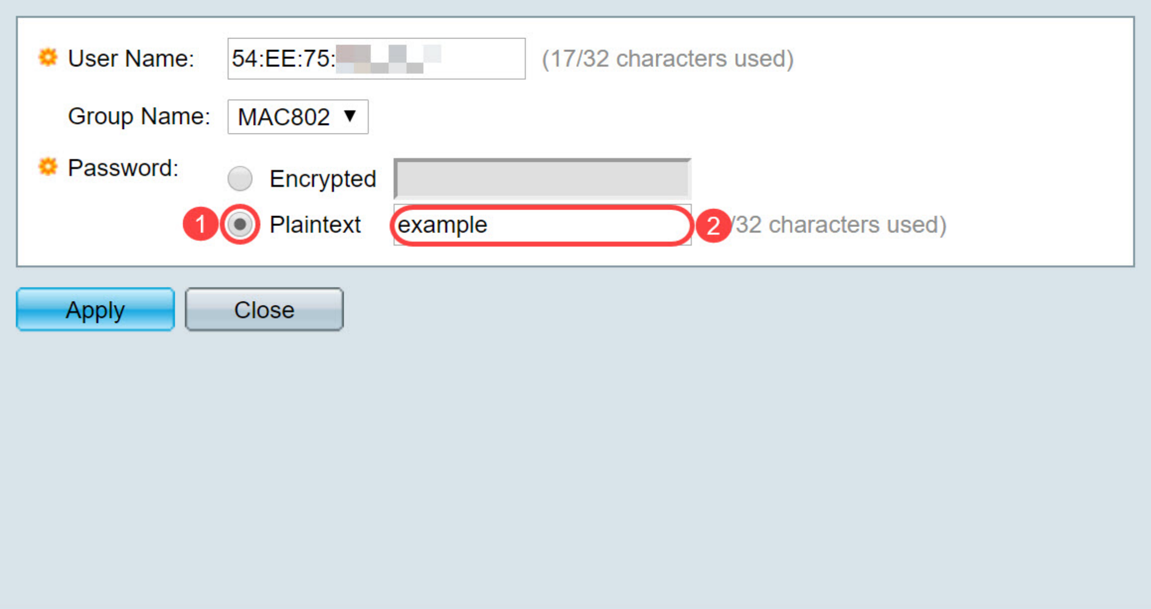
○ Plaintext (0/32 characters used)

步驟5.選擇以下單選按鈕之一：

- 已加密 — 使用MD5加密通訊所使用的金鑰。要使用加密，請以加密形式輸入金鑰。
- 明文 — 如果您沒有加密的金鑰字串（來自其他裝置），請在明文模式下輸入金鑰字串。生成並顯示加密金鑰字串。

我們將選擇*明文*作為此使用者的密碼，並鍵入**example**作為我們的明文密碼。

附註：建議不要使用**example**作為明文密碼。建議使用更強密碼。



User Name: 54:EE:75:[redacted] (17/32 characters used)

Group Name: MAC802 ▼

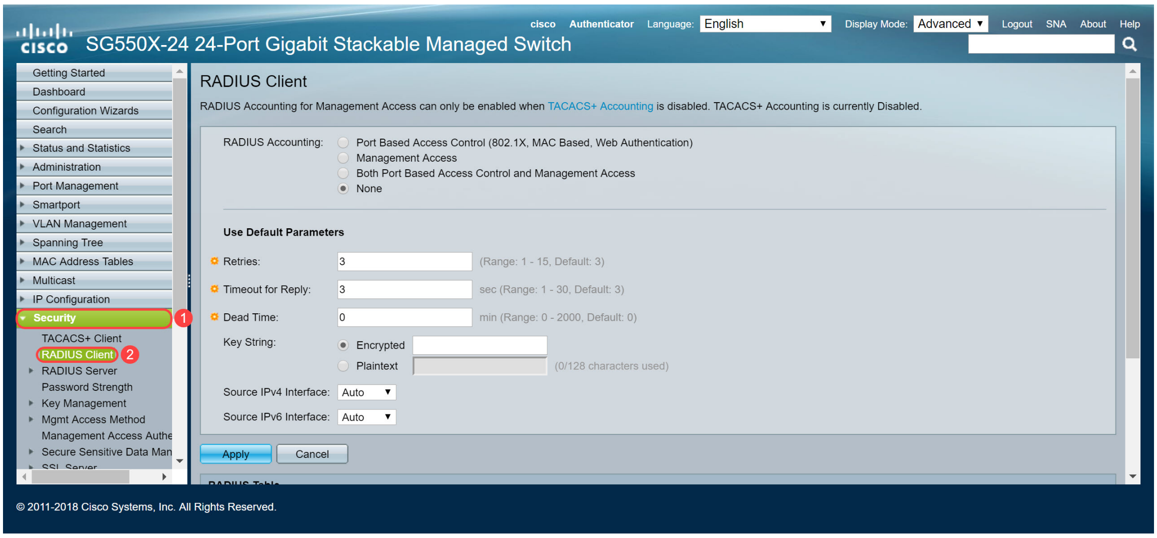
Password:
○ Encrypted
● Plaintext example (/32 characters used)

步驟6.完成配置後，按一下**Apply**。

現在，您已完成配置RADIUS伺服器。在下一部分中，我們將配置第二台交換機作為身份驗證器。

RADIUS使用者端

步驟1.登入到將配置為身份驗證器的交換機的基於Web的實用程式，然後導航至**安全> RADIUS客戶端**。



RADIUS Client

RADIUS Accounting for Management Access can only be enabled when TACACS+ Accounting is disabled. TACACS+ Accounting is currently Disabled.

RADIUS Accounting:
○ Port Based Access Control (802.1X, MAC Based, Web Authentication)
○ Management Access
○ Both Port Based Access Control and Management Access
● None

Use Default Parameters

Retries: 3 (Range: 1 - 15, Default: 3)

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

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

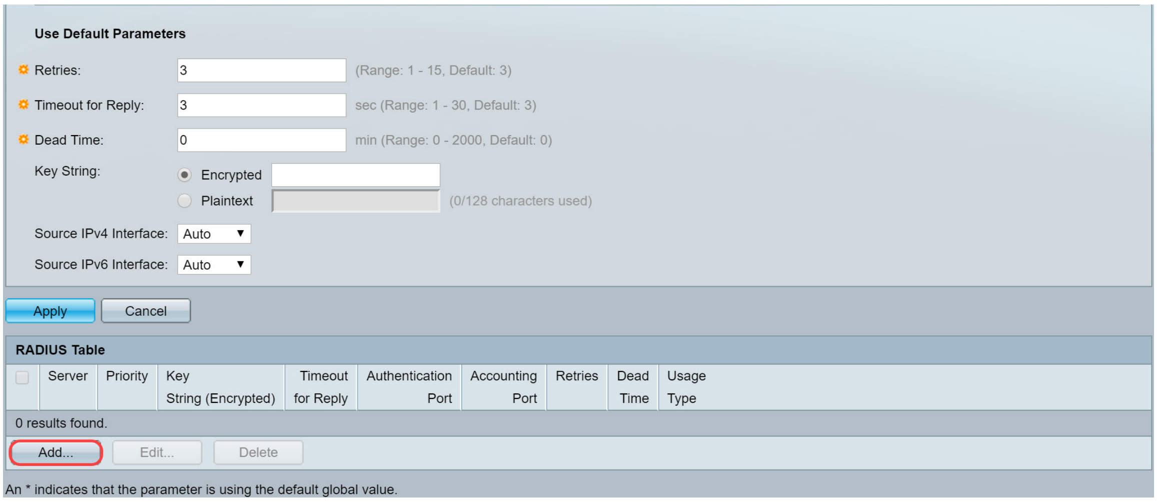
Key String:
● Encrypted
○ Plaintext (0/128 characters used)

Source IPv4 Interface: Auto ▼

Source IPv6 Interface: Auto ▼

© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

步驟2.向下滾動到*RADIUS Table*部分，然後按一下**Add...** 新增RADIUS伺服器。



Use Default Parameters

Retries: 3 (Range: 1 - 15, Default: 3)

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

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

Key String: ● Encrypted ○ Plaintext (0/128 characters used)

Source IPv4 Interface: Auto

Source IPv6 Interface: Auto

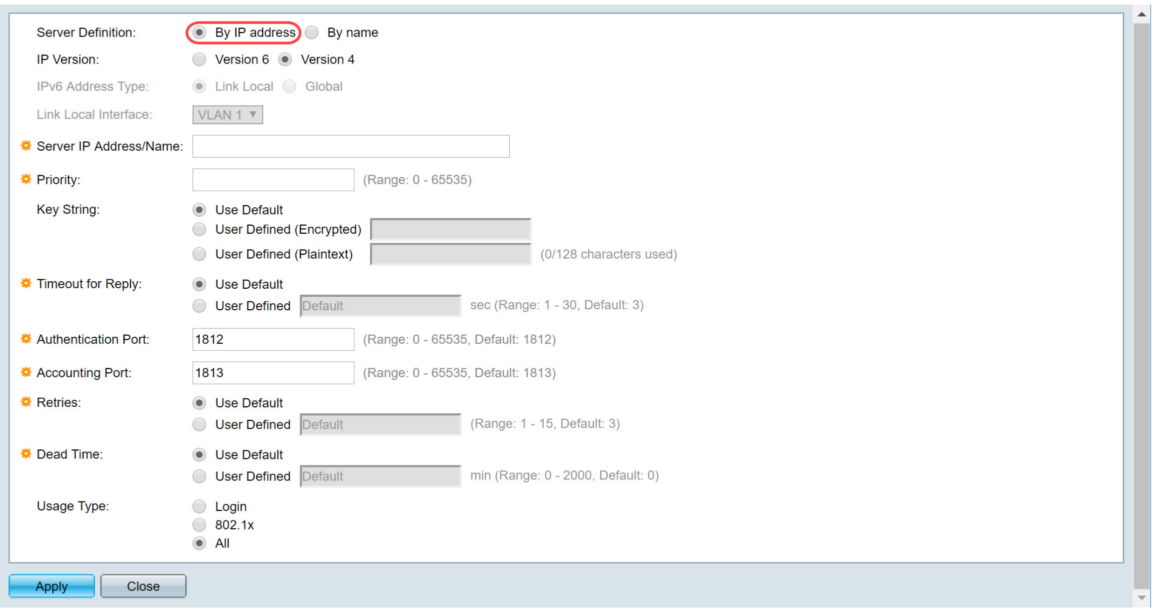
RADIUS Table

□	Server	Priority	Key String (Encrypted)	Timeout for Reply	Authentication Port	Accounting Port	Retries	Dead Time	Usage Type

0 results found.

An * indicates that the parameter is using the default global value.

步驟3.（可選）在*Server Definition*（伺服器定義）欄位中選擇是否按IP地址或名稱指定RADIUS伺服器。在本例中，我們將保留**By IP address**的預設選擇。



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 Default sec (Range: 1 - 30, Default: 3)

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

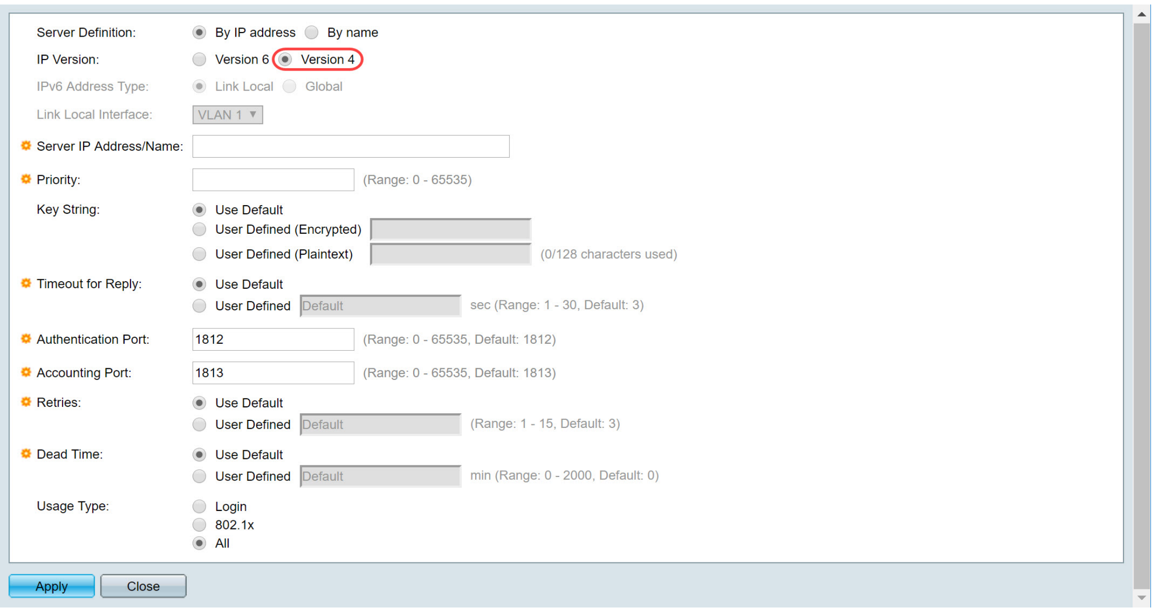
Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

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4.（可選）在*IP Version*欄位中選擇RADIUS伺服器的IP位址*的版*本。在本例中，我們將保留**版本4**的預設選擇。



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 Default sec (Range: 1 - 30, Default: 3)

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

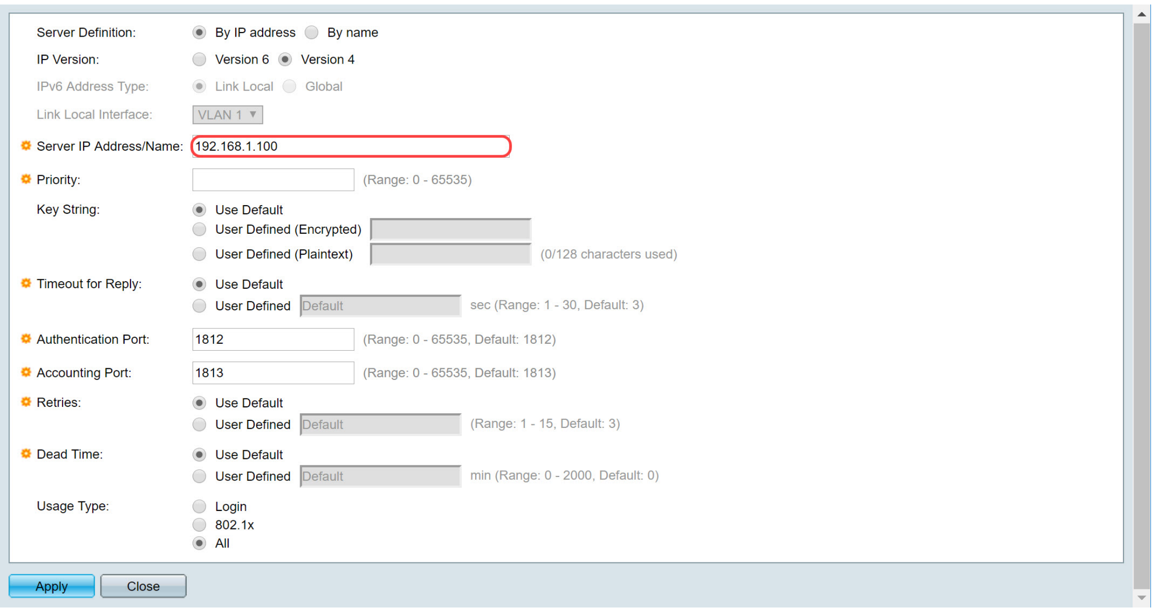
Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

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5.按IP地址或名稱輸入RADIUS伺服器。我們將在*Server IP Address/Name*欄位中輸入IP地址**192.168.1.100**。



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: 192.168.1.100

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 Default sec (Range: 1 - 30, Default: 3)

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

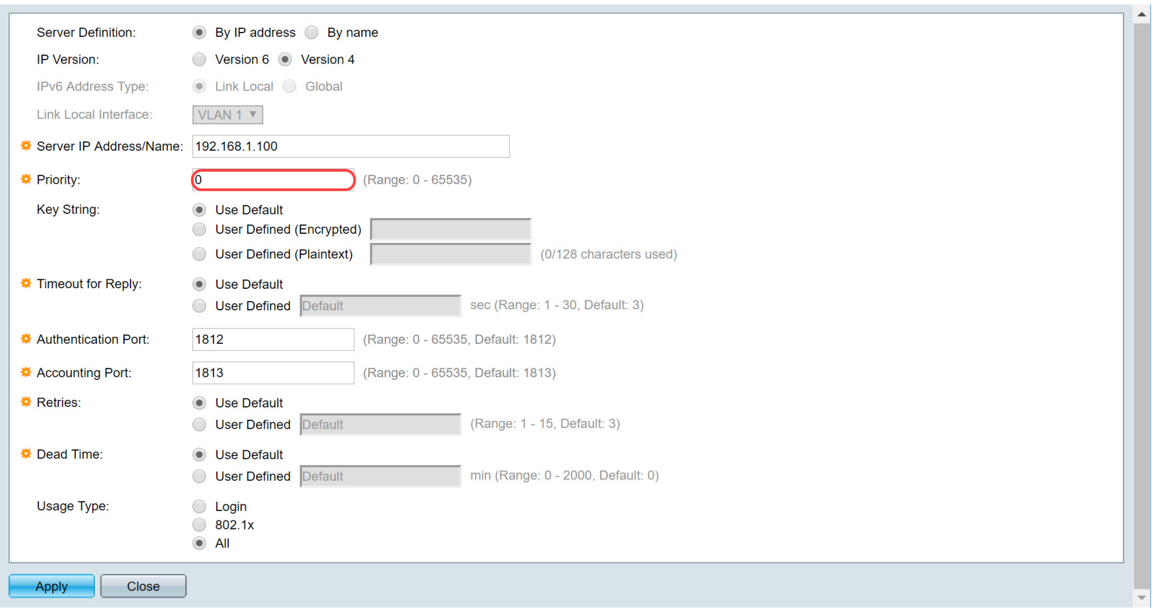
Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

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。零是最高優先順序。



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: 192.168.1.100

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)

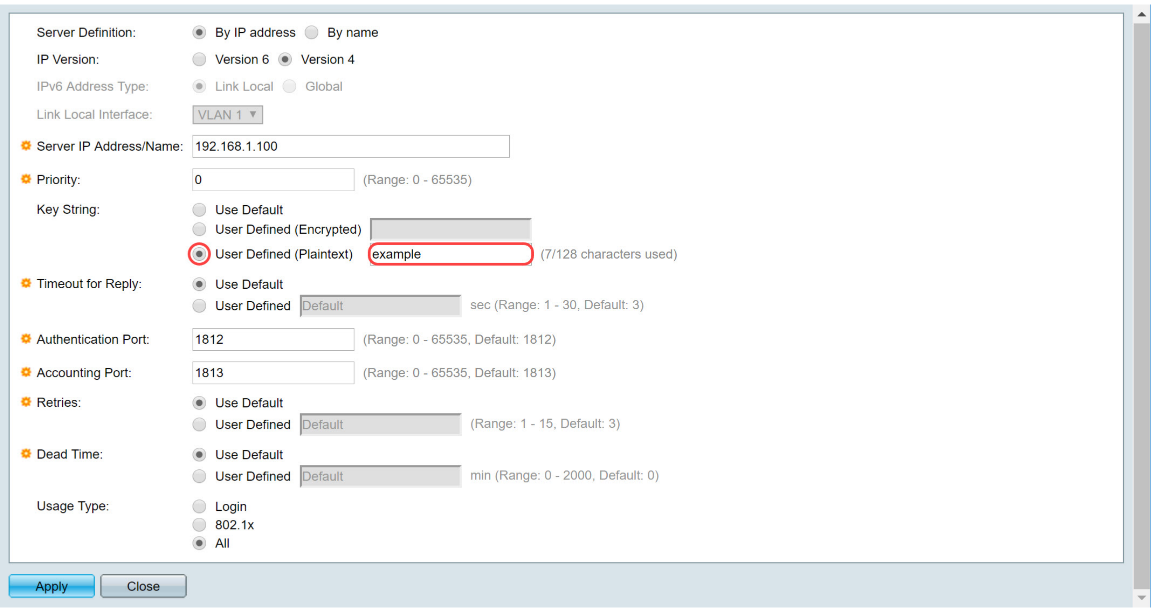
Retries:
● Use Default
○ User Defined Default (Range: 1 - 15, Default: 3)

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

附註：我們將保留配置的其餘部分為預設值。如果需要，可以配置它們。



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: 192.168.1.100

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)

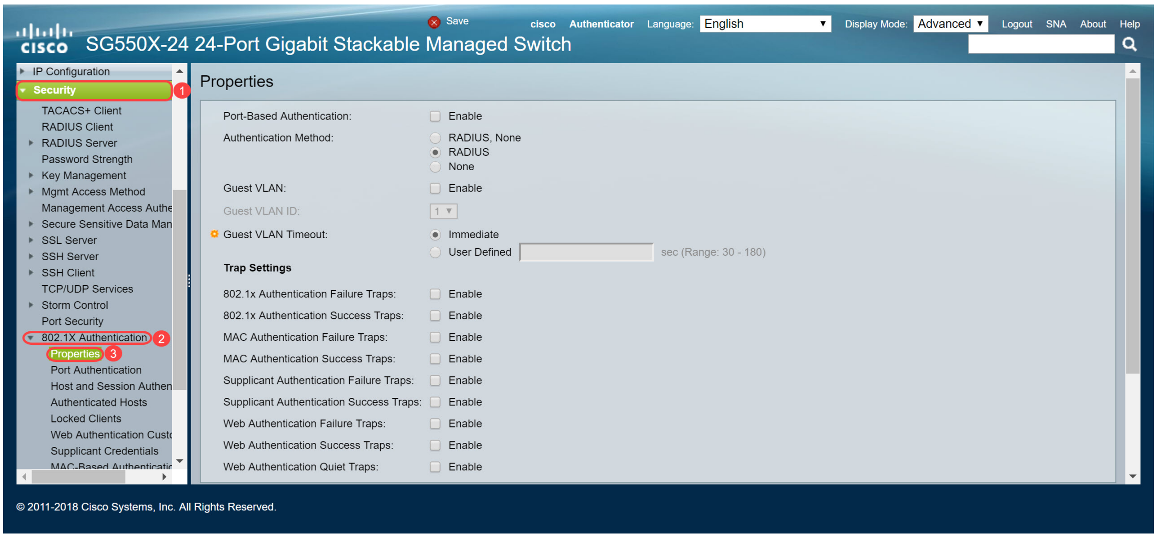
Usage Type: ○ Login
○ 802.1x
● All

步驟8.按一下**Apply**以儲存組態。

802.1X身份驗證屬性

屬性頁用於全域性啟用埠/裝置身份驗證。要使身份驗證正常工作，必須在每個埠上全域性和單獨啟用該身份驗證。

步驟1.導航到**安全> 802.1X身份驗證>屬性**。



Properties

Port-Based Authentication: □ Enable

Authentication Method: ○ RADIUS, None
● RADIUS
○ None

Guest VLAN: □ Enable

Guest VLAN ID: 1

Guest VLAN Timeout: ● Immediate
○ User Defined sec (Range: 30 - 180)

Trap Settings

802.1x Authentication Failure Traps: □ Enable

802.1x Authentication Success Traps: □ Enable

MAC Authentication Failure Traps: □ Enable

MAC Authentication Success Traps: □ Enable

Supplicant Authentication Failure Traps: □ Enable

Supplicant Authentication Success Traps: □ Enable

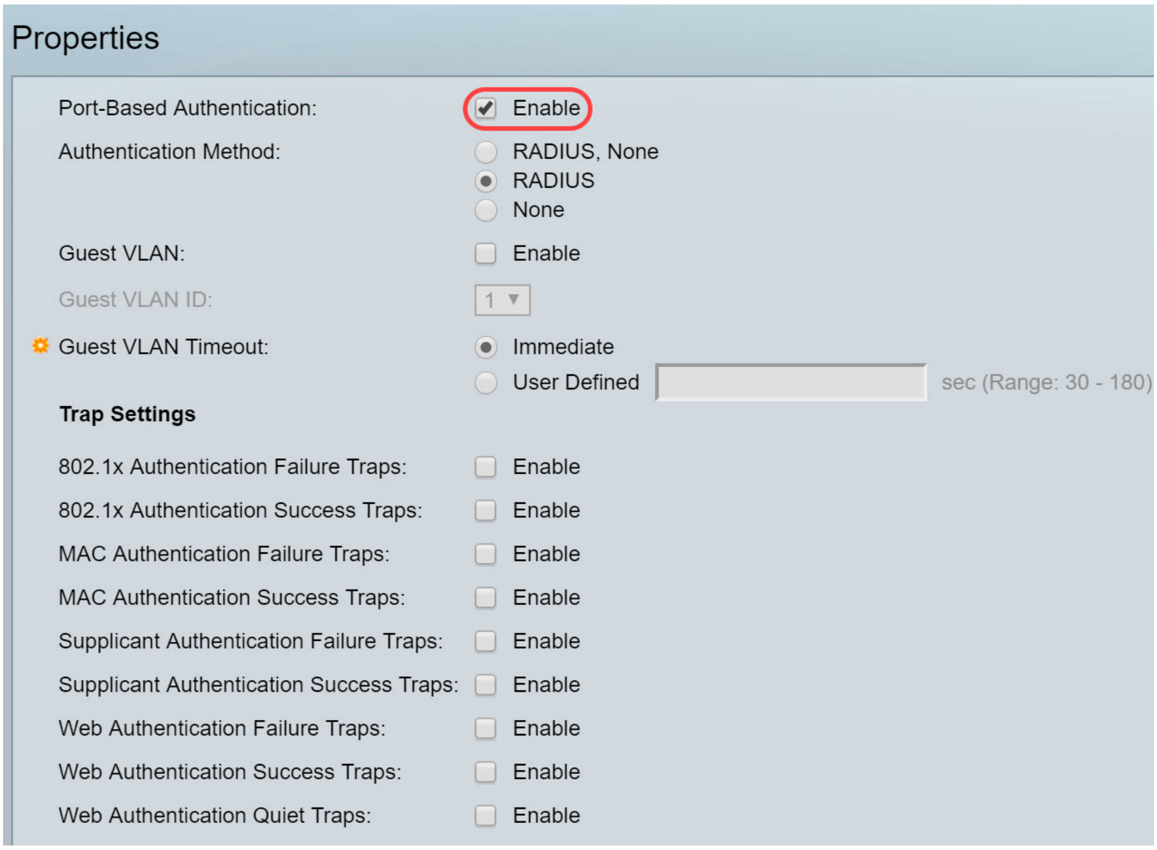
Web Authentication Failure Traps: □ Enable

Web Authentication Success Traps: □ Enable

Web Authentication Quiet Traps: □ Enable

© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

步驟2.選中**Enable**覈取方塊以啟用基於埠的身份驗證。



Properties

Port-Based Authentication: ☑ Enable

Authentication Method: ○ RADIUS, None ● RADIUS ○ None

Guest VLAN: □ Enable

Guest VLAN ID: 1

Guest VLAN Timeout: ● Immediate ○ User Defined sec (Range: 30 - 180)

Trap Settings

802.1x Authentication Failure Traps: □ Enable

802.1x Authentication Success Traps: □ Enable

MAC Authentication Failure Traps: □ Enable

MAC Authentication Success Traps: □ Enable

Supplicant Authentication Failure Traps: □ Enable

Supplicant Authentication Success Traps: □ Enable

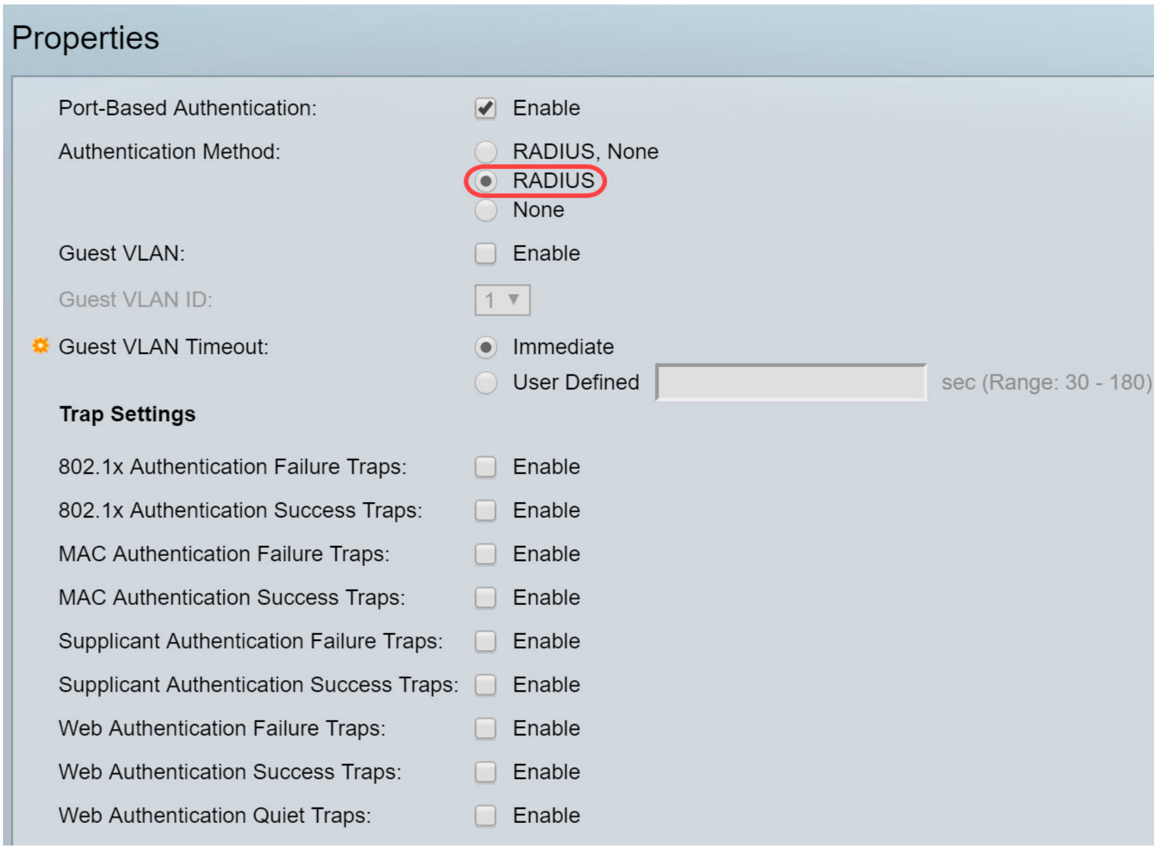
Web Authentication Failure Traps: □ Enable

Web Authentication Success Traps: □ Enable

Web Authentication Quiet Traps: □ Enable

步驟3.選擇使用者身份驗證方法。我們將選擇RADIUS作為我們的驗證方法。以下選項是：

- RADIUS， None — 首先使用RADIUS伺服器執行埠身份驗證。如果沒有收到來自RADIUS的回應（例如伺服器關閉），則不會執行驗證且允許作業階段。如果伺服器可用，但使用者憑據不正確，則訪問將被拒絕，會話將終止。
- RADIUS — 在RADIUS伺服器上驗證使用者身分。如果未執行身份驗證，則不允許會話。
- 無 — 不對使用者進行身份驗證。允許會話。



Properties

Port-Based Authentication: ☑ Enable

Authentication Method: ○ RADIUS, None ● RADIUS ○ None

Guest VLAN: □ Enable

Guest VLAN ID: 1

Guest VLAN Timeout: ● Immediate ○ User Defined sec (Range: 30 - 180)

Trap Settings

802.1x Authentication Failure Traps: □ Enable

802.1x Authentication Success Traps: □ Enable

MAC Authentication Failure Traps: □ Enable

MAC Authentication Success Traps: □ Enable

Supplicant Authentication Failure Traps: □ Enable

Supplicant Authentication Success Traps: □ Enable

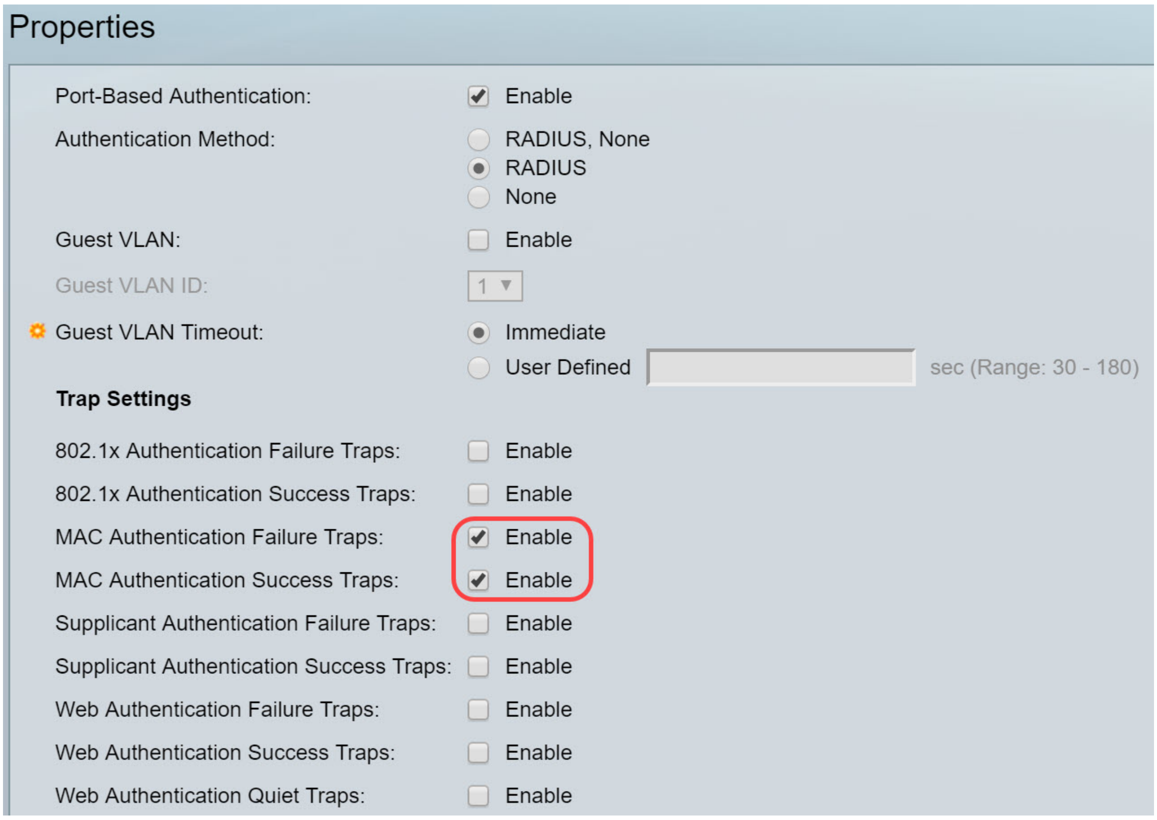
Web Authentication Failure Traps: □ Enable

Web Authentication Success Traps: □ Enable

Web Authentication Quiet Traps: □ Enable

步驟4.（可選）選中*MAC Authentication Failure Traps*和*MAC Authentication Success Traps*的

Enable覈取方塊。如果MAC身份驗證失敗或成功，這將生成陷阱。在本示例中，我們將啟用*MAC身份驗證失敗陷阱*和*MAC身份驗證成功陷阱*。



Properties

Port-Based Authentication: ☑ Enable

Authentication Method: ○ RADIUS, None ● RADIUS ○ None

Guest VLAN: □ Enable

Guest VLAN ID: 1

Guest VLAN Timeout: ● Immediate ○ User Defined sec (Range: 30 - 180)

Trap Settings

802.1x Authentication Failure Traps: □ Enable

802.1x Authentication Success Traps: □ Enable

MAC Authentication Failure Traps: ☑ Enable

MAC Authentication Success Traps: ☑ Enable

Supplicant Authentication Failure Traps: □ Enable

Supplicant Authentication Success Traps: □ Enable

Web Authentication Failure Traps: □ Enable

Web Authentication Success Traps: □ Enable

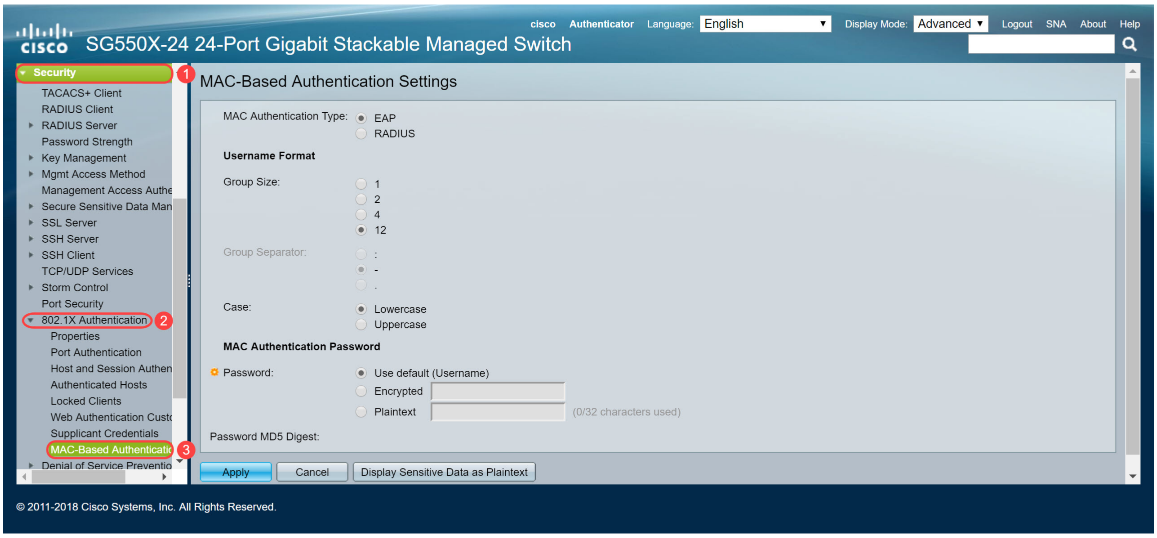
Web Authentication Quiet Traps: □ Enable

步驟5.按一下**Apply**。

802.1X身份驗證MAC身份驗證設定

使用此頁可以配置適用於基於MAC的身份驗證的各種設定。

步驟1.導覽至**Security > 802.1X Authentication > MAC-Based Authentication Settings**。



MAC-Based Authentication Settings

MAC Authentication Type: ● EAP ○ RADIUS

Username Format

Group Size: ○ 1 ○ 2 ○ 4 ● 12

Group Separator: ○ : ● - ○ .

Case: ● Lowercase ○ Uppercase

MAC Authentication Password

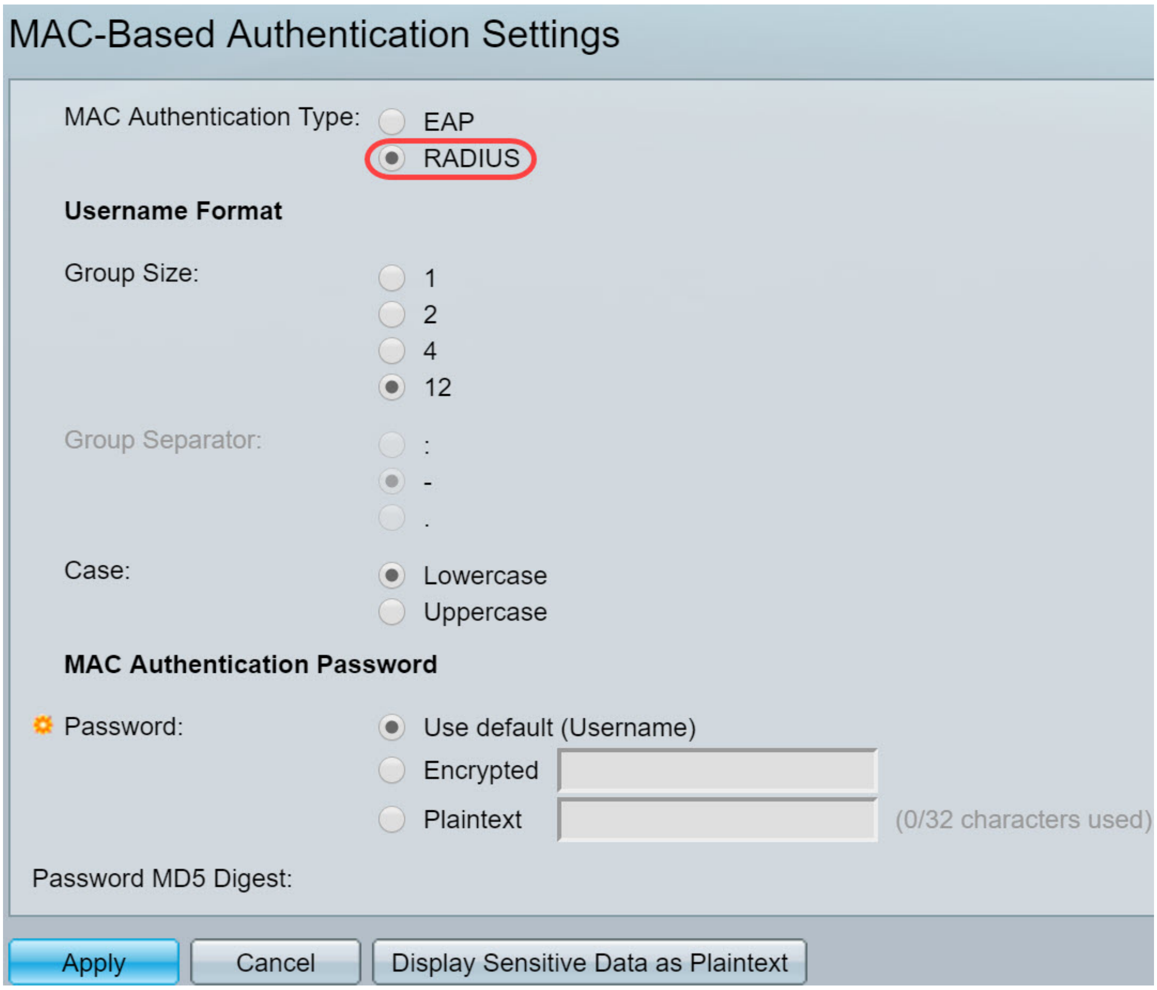
Password: ● Use default (Username) ○ Encrypted ○ Plaintext (0/32 characters used)

Password MD5 Digest:

步驟2.在*MAC Authentication Type*中選擇以下選項之一：

- EAP — 對交換機（RADIUS客戶端）和RADIUS伺服器（驗證基於MAC的請求方）之間的流量使用RADIUS和EAP封裝。
- RADIUS — 對交換器（RADIUS使用者端）和RADIUS伺服器（其會驗證基於MAC的要求者）之間的流量使用不含EAP封裝的RADIUS。

在本範例中，我們將選擇RADIUS作為我們的MAC驗證型別。



MAC-Based Authentication Settings

MAC Authentication Type: ○ EAP
● RADIUS

Username Format

Group Size: ○ 1
○ 2
○ 4
● 12

Group Separator: ○ :
● -
○ .

Case: ● Lowercase
○ Uppercase

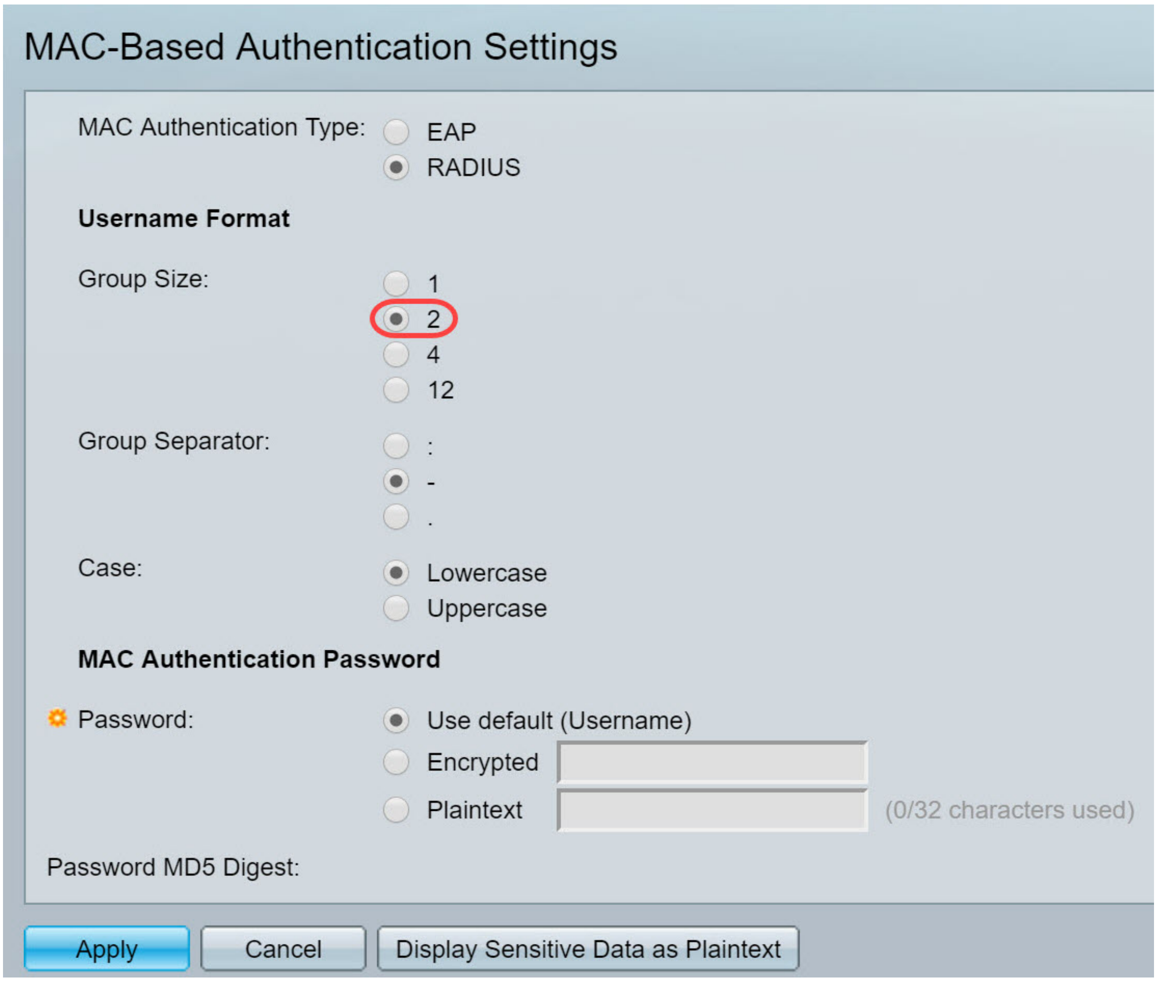
MAC Authentication Password

Password: ● Use default (Username)
○ Encrypted
○ Plaintext (0/32 characters used)

Password MD5 Digest:

步驟3.在*使用者名稱格式*中，選擇作為使用者名稱傳送的MAC地址分隔符之間的ASCII字元數。在本例中，我們將選擇2作為組大小。

附註：確保使用者名稱格式與您在*Radius Server Users*部分輸入MAC地址的方式相同。



MAC-Based Authentication Settings

MAC Authentication Type: ○ EAP ● RADIUS

Username Format

Group Size: ○ 1 ● 2 ○ 4 ○ 12

Group Separator: ○ : ● - ○ .

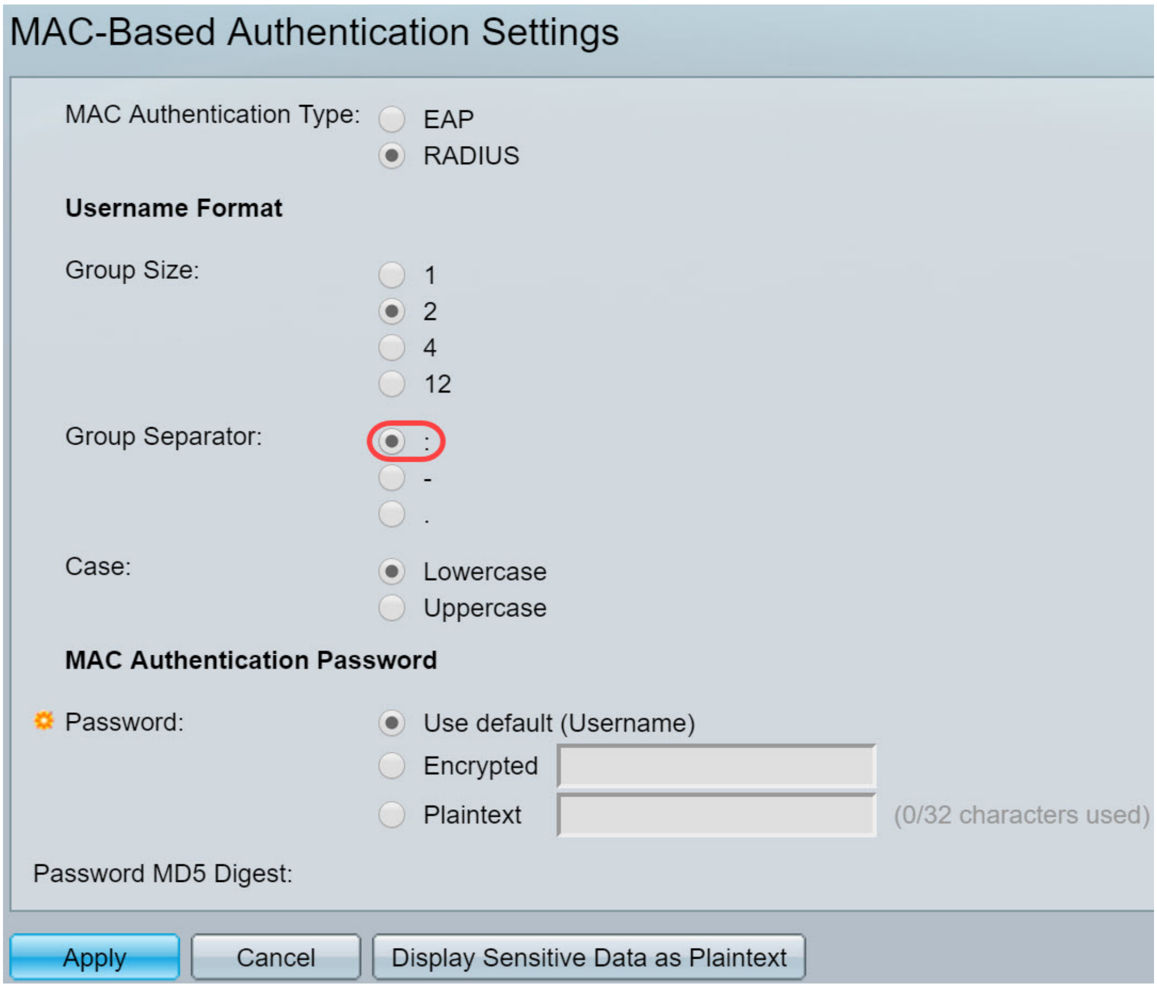
Case: ● Lowercase ○ Uppercase

MAC Authentication Password

Password: ● Use default (Username) ○ Encrypted ○ Plaintext (0/32 characters used)

Password MD5 Digest:

步驟4.選擇在MAC地址中定義的字元組之間用作分隔符的字元。在本例中，我們將選擇:作為組分隔符。



MAC-Based Authentication Settings

MAC Authentication Type: ○ EAP ● RADIUS

Username Format

Group Size: ○ 1 ● 2 ○ 4 ○ 12

Group Separator: ● : ○ - ○ .

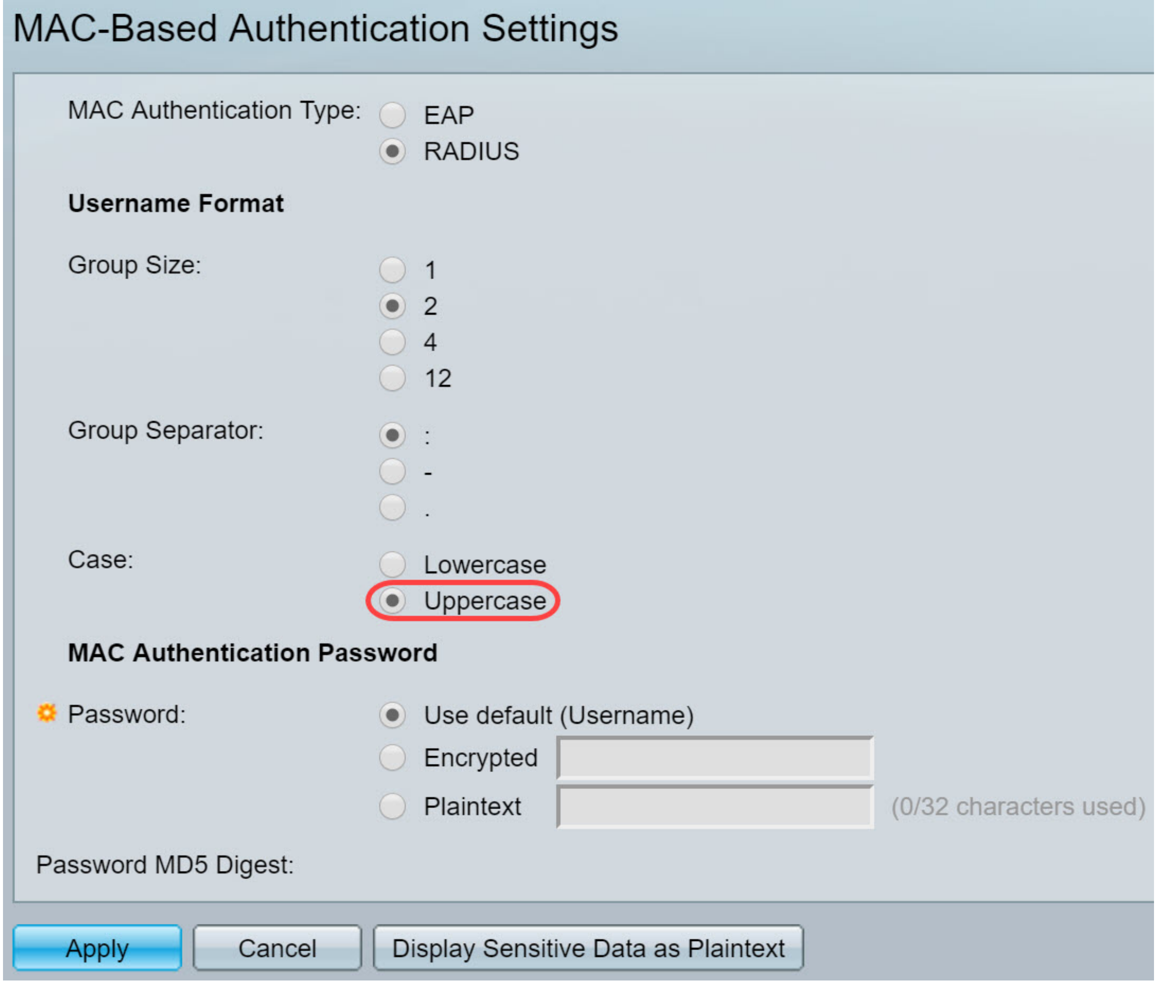
Case: ● Lowercase ○ Uppercase

MAC Authentication Password

Password: ● Use default (Username) ○ Encrypted ○ Plaintext (0/32 characters used)

Password MD5 Digest:

步驟5.在*Case*欄位中，選擇**Lowercase**或**Uppercase**以大寫或小寫形式傳送使用者名稱。



MAC-Based Authentication Settings

MAC Authentication Type: ○ EAP ● RADIUS

Username Format

Group Size: ○ 1 ● 2 ○ 4 ○ 12

Group Separator: ● : ○ - ○ .

Case: ○ Lowercase ● Uppercase

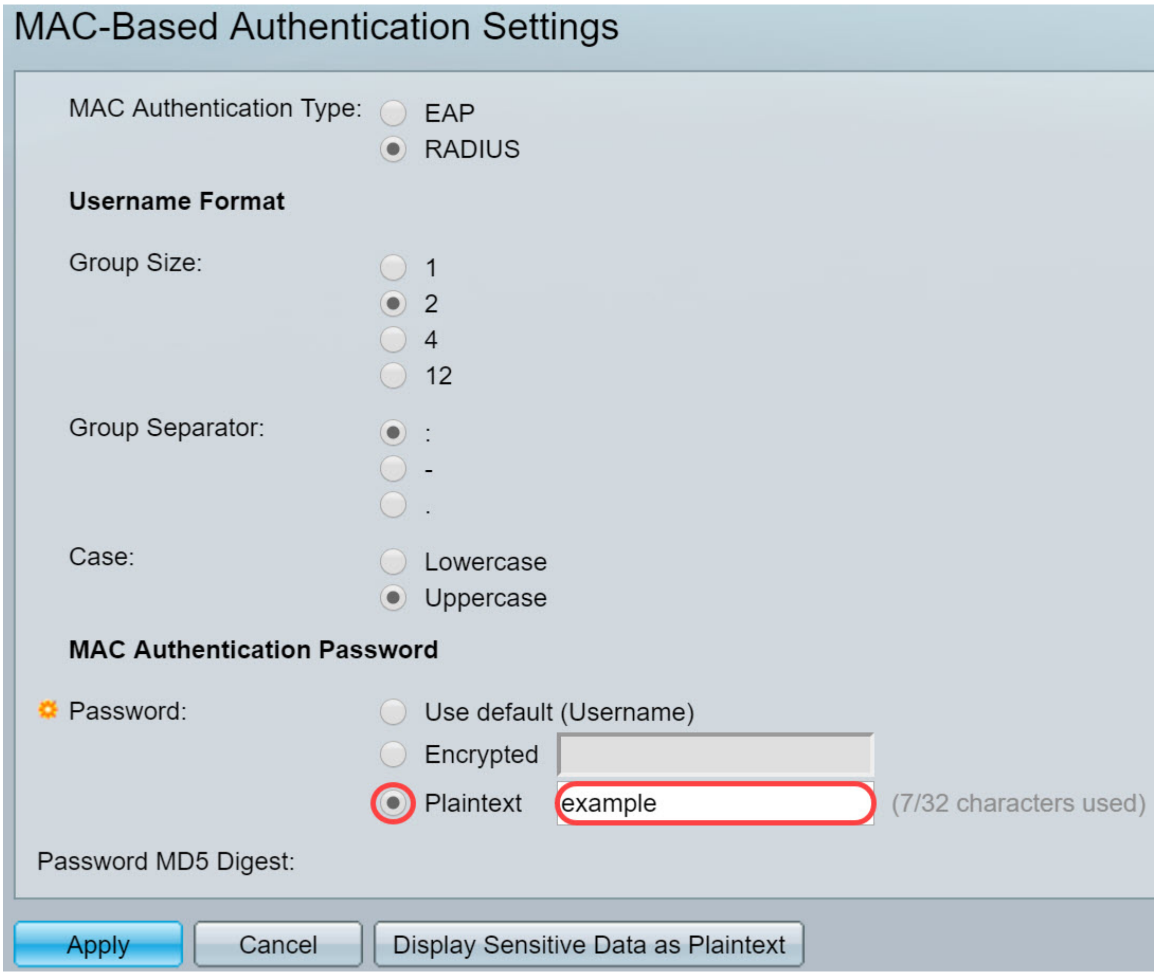
MAC Authentication Password

Password: ● Use default (Username) ○ Encrypted ○ Plaintext (0/32 characters used)

Password MD5 Digest:

步驟6.密碼定義交換機如何通過RADIUS伺服器進行身份驗證。選擇以下選項之一：

- Use default(Username) — 選擇該選項以使用定義的使用者名稱作為密碼。
- 已加密 — 以加密格式定義密碼。
- 明文(Plaintext) — 以明文格式定義密碼。



MAC-Based Authentication Settings

MAC Authentication Type: ○ EAP ● RADIUS

Username Format

Group Size: ○ 1 ● 2 ○ 4 ○ 12

Group Separator: ● : ○ - ○ .

Case: ○ Lowercase ● Uppercase

MAC Authentication Password

Password: ○ Use default (Username) ○ Encrypted ● Plaintext example (7/32 characters used)

Password MD5 Digest:

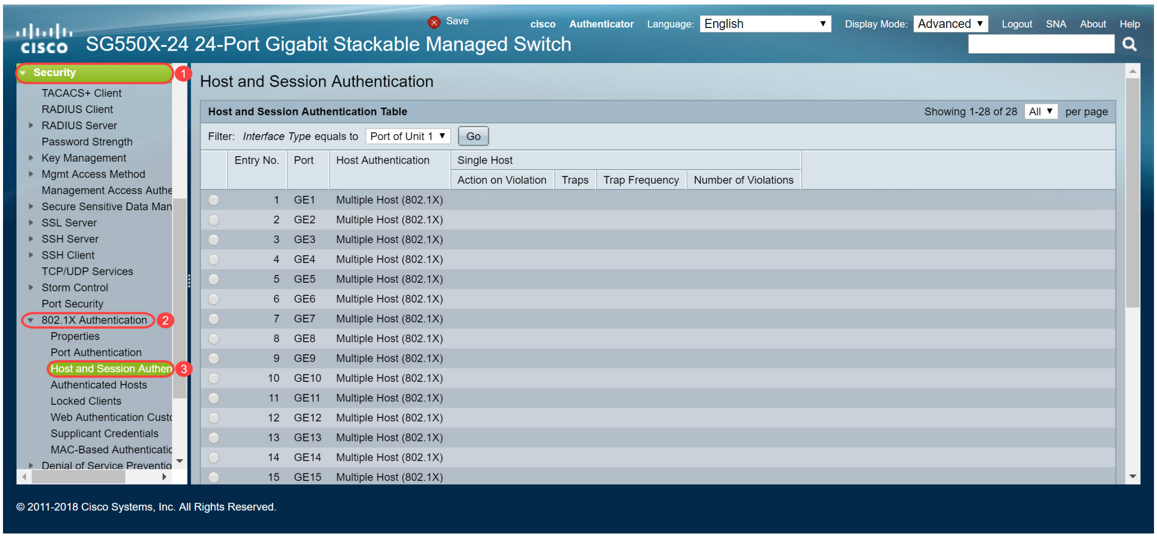
注意：*Password Message-Digest Algorithm 5(MD5)摘要顯*示MD5摘要密碼。MD5是一個加密雜湊函式，它獲取資料並建立了一個典型的不可重複的唯一十六進位制輸出。MD5使用128位雜湊值。

步驟7.按一下**Apply**，並將設定儲存到執行組態檔中。

802.1X驗證主機和會話驗證

*Host and Session Authentication*頁用於定義802.1X在埠上運行的模式以及檢測到違規時要執行的操作。

步驟1。導覽至**Security > 802.1X Authentication > Host and Session Authentication**。



Host and Session Authentication

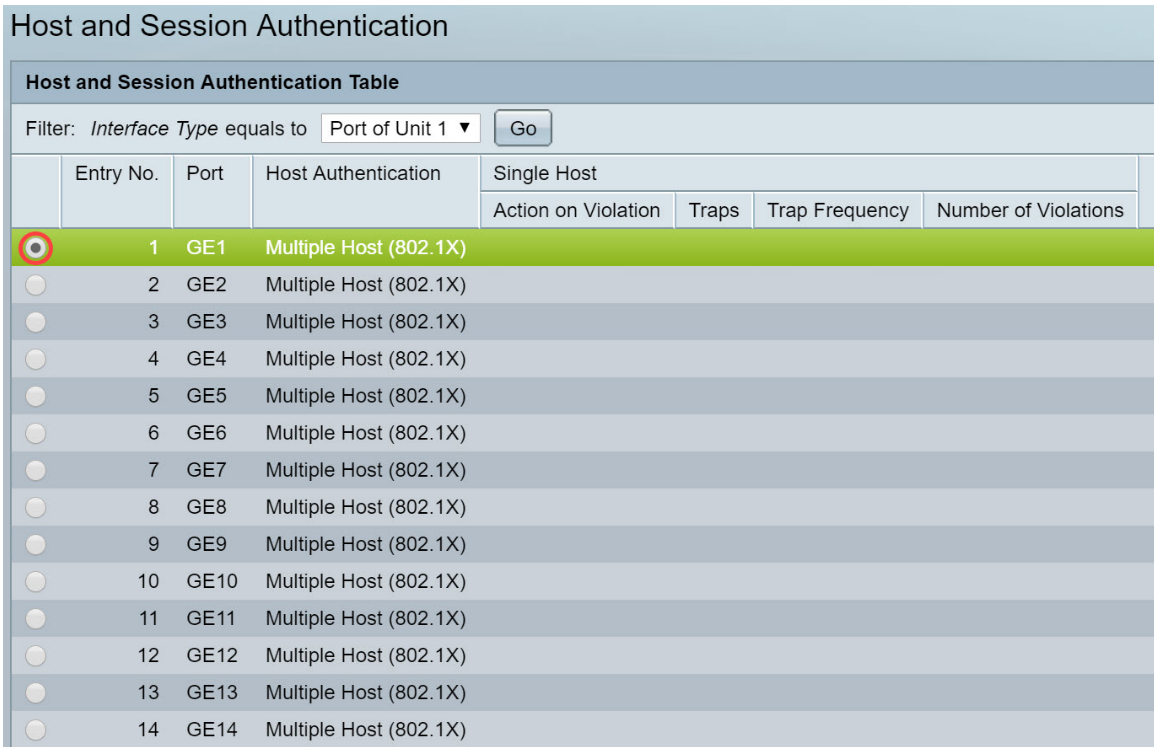
Host and Session Authentication Table — Showing 1-28 of 28 All per page

Filter: *Interface Type* equals to Port of Unit 1 Go

	Entry No.	Port	Host Authentication	Single Host			
				Action on Violation	Traps	Trap Frequency	Number of Violations
○	1	GE1	Multiple Host (802.1X)				
○	2	GE2	Multiple Host (802.1X)				
○	3	GE3	Multiple Host (802.1X)				
○	4	GE4	Multiple Host (802.1X)				
○	5	GE5	Multiple Host (802.1X)				
○	6	GE6	Multiple Host (802.1X)				
○	7	GE7	Multiple Host (802.1X)				
○	8	GE8	Multiple Host (802.1X)				
○	9	GE9	Multiple Host (802.1X)				
○	10	GE10	Multiple Host (802.1X)				
○	11	GE11	Multiple Host (802.1X)				
○	12	GE12	Multiple Host (802.1X)				
○	13	GE13	Multiple Host (802.1X)				
○	14	GE14	Multiple Host (802.1X)				
○	15	GE15	Multiple Host (802.1X)				

© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

步驟2.選擇要配置主機身份驗證的埠。在本例中，我們將配置GE1連線到終端主機。



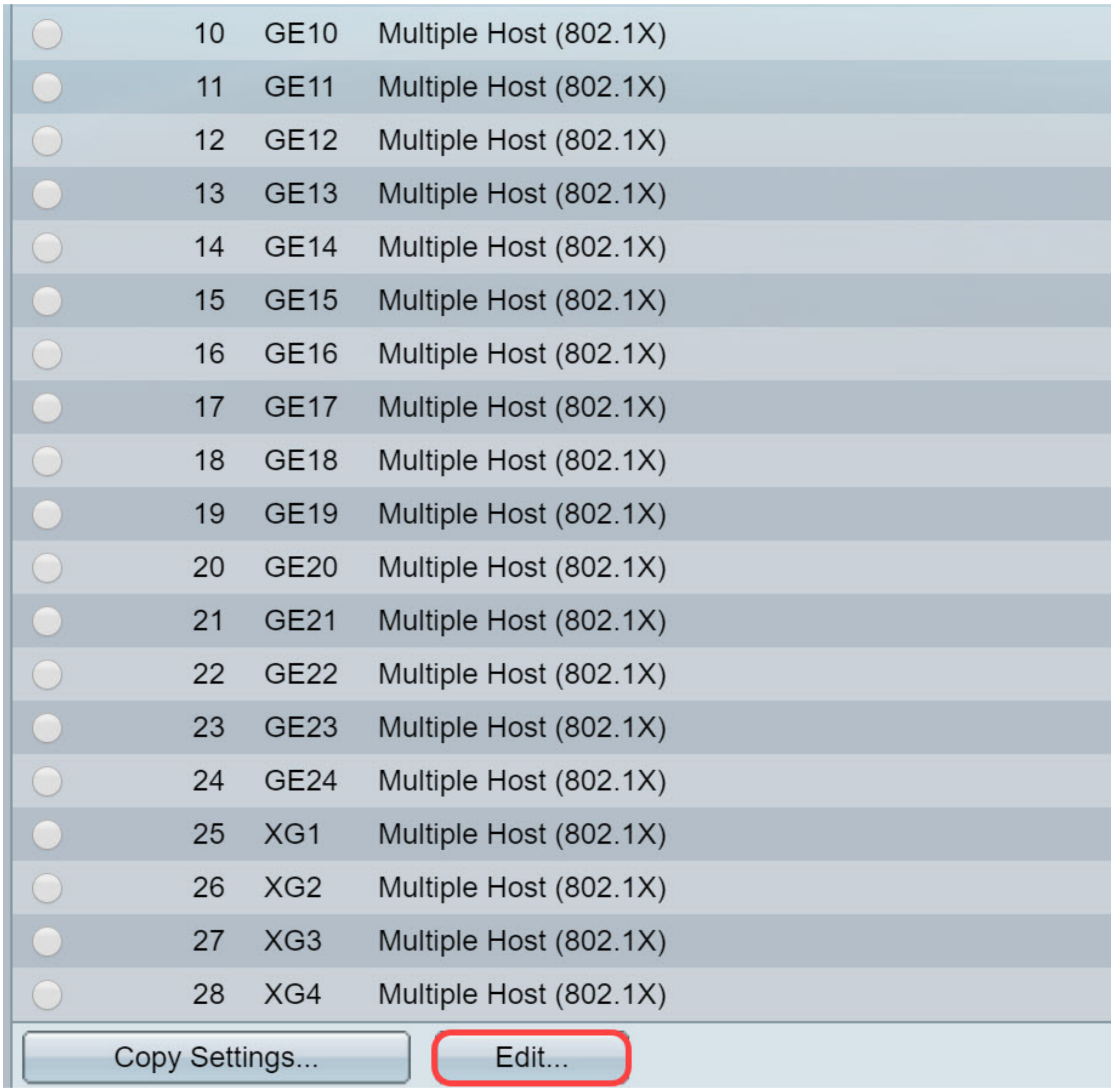
Host and Session Authentication

Host and Session Authentication Table

Filter: *Interface Type* equals to Port of Unit 1 ▼ Go

	Entry No.	Port	Host Authentication	Single Host			
				Action on Violation	Traps	Trap Frequency	Number of Violations
●	1	GE1	Multiple Host (802.1X)				
○	2	GE2	Multiple Host (802.1X)				
○	3	GE3	Multiple Host (802.1X)				
○	4	GE4	Multiple Host (802.1X)				
○	5	GE5	Multiple Host (802.1X)				
○	6	GE6	Multiple Host (802.1X)				
○	7	GE7	Multiple Host (802.1X)				
○	8	GE8	Multiple Host (802.1X)				
○	9	GE9	Multiple Host (802.1X)				
○	10	GE10	Multiple Host (802.1X)				
○	11	GE11	Multiple Host (802.1X)				
○	12	GE12	Multiple Host (802.1X)				
○	13	GE13	Multiple Host (802.1X)				
○	14	GE14	Multiple Host (802.1X)				

步驟3.單**擊Edit...** 配置埠。



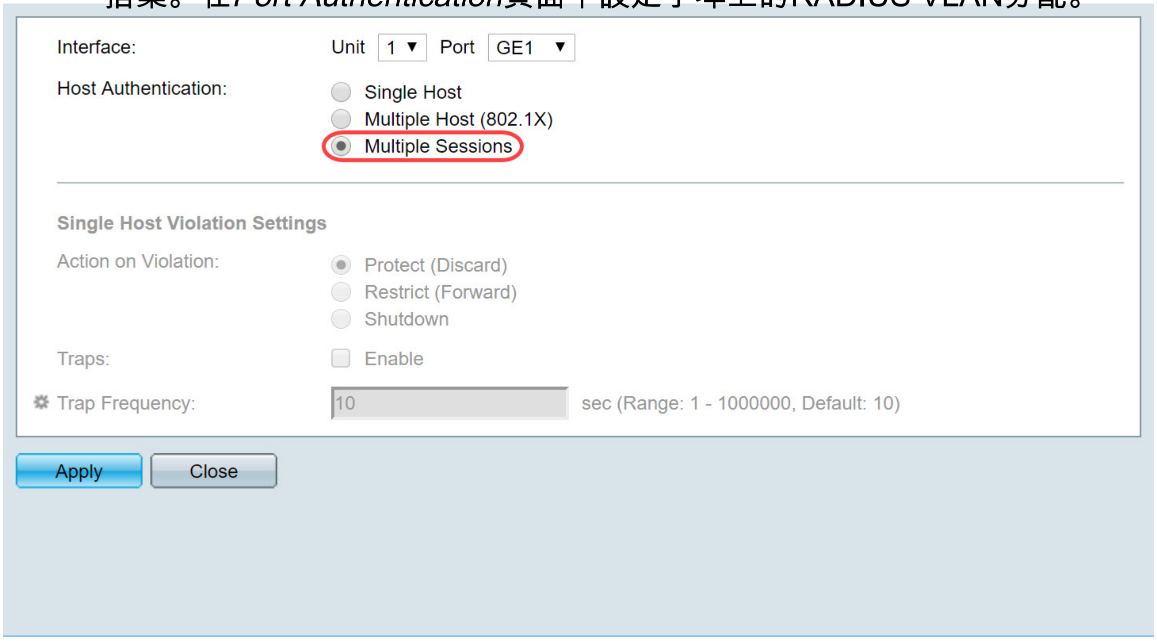
○	10	GE10	Multiple Host (802.1X)
○	11	GE11	Multiple Host (802.1X)
○	12	GE12	Multiple Host (802.1X)
○	13	GE13	Multiple Host (802.1X)
○	14	GE14	Multiple Host (802.1X)
○	15	GE15	Multiple Host (802.1X)
○	16	GE16	Multiple Host (802.1X)
○	17	GE17	Multiple Host (802.1X)
○	18	GE18	Multiple Host (802.1X)
○	19	GE19	Multiple Host (802.1X)
○	20	GE20	Multiple Host (802.1X)
○	21	GE21	Multiple Host (802.1X)
○	22	GE22	Multiple Host (802.1X)
○	23	GE23	Multiple Host (802.1X)
○	24	GE24	Multiple Host (802.1X)
○	25	XG1	Multiple Host (802.1X)
○	26	XG2	Multiple Host (802.1X)
○	27	XG3	Multiple Host (802.1X)
○	28	XG4	Multiple Host (802.1X)

步驟4.在*Host Authentication*欄位中，選擇以下選項之一：

1. 單主機模式

- 如果存在經授權的客戶端，則埠是經授權的。一個埠上只能授權一台主機。
- 當連線埠未授權且訪客VLAN啟用時，未標籤的流量會重新對映到訪客VLAN。除非標籤的流量屬於訪客VLAN或屬於未經驗證的VLAN，否則會將其捨棄。如果在連線埠上未啟用訪客VLAN，則只會橋接屬於未經驗證VLAN的已標籤流量。
- 當連線埠獲得授權時，來自授權主機的未標籤和已標籤流量會根據靜態VLAN成員身分連線埠組態橋接。來自其他主機的流量將被丟棄。
- 使用者可以指定來自授權主機的未標籤流量在身份驗證過程中重新對映到RADIUS伺服器分配的VLAN。除非標籤的流量屬於RADIUS指派的VLAN或未經驗證的VLAN，否則會將其捨棄。連線埠上的RADIUS VLAN分配在「*Port Authentication*」頁面中設定。

2. 多主機模式
   - 如果至少有一個授權客戶端，則埠是授權的。
   - 當連線埠未授權且訪客VLAN啟用時，未標籤的流量會重新對映到訪客VLAN。除非標籤的流量屬於訪客VLAN或屬於未經驗證的VLAN，否則會將其捨棄。如果在連線埠上未啟用訪客VLAN，則只會橋接屬於未經驗證VLAN的已標籤流量。
   - 當連線埠獲得授權時，會根據靜態VLAN成員身分連線埠組態，橋接來自連線到連線埠的所有主機的未標籤且已標籤的流量。
   - 您可以指定來自授權連線埠的未標籤流量會在驗證過程中重新對映到RADIUS伺服器指派的VLAN。除非標籤的流量屬於RADIUS指定的VLAN或未經驗證的VLAN，否則該流量會遭到捨棄。連線埠上的RADIUS VLAN分配在「*Port Authentication*」頁面中設定。
3. 多會話模式
   - 與單主機和多主機模式不同，多會話模式下的埠沒有身份驗證狀態。此狀態會指派給連線到連線埠的每個使用者端。
   - 無論主機是否獲得授權，都會橋接屬於未經驗證的VLAN的已標籤流量。
   - 來自非屬於未驗證VLAN的未授權主機的已標籤和未標籤流量如果已在VLAN上定義並啟用，則會重新對映到訪客VLAN；如果訪客VLAN未在埠上啟用，則會丟棄該流量。
   - 您可以指定來自授權連線埠的未標籤流量會在驗證過程中重新對映到RADIUS伺服器指派的VLAN。除非標籤的流量屬於RADIUS指定的VLAN或未經驗證的VLAN，否則該流量會遭到捨棄。在*Port Authentication*頁面中設定了埠上的RADIUS VLAN分配。



Interface: Unit 1 Port GE1

Host Authentication:
○ Single Host
○ Multiple Host (802.1X)
● Multiple Sessions

Single Host Violation Settings

Action on Violation:
● Protect (Discard)
○ Restrict (Forward)
○ Shutdown

Traps: □ Enable

Trap Frequency: 10 sec (Range: 1 - 1000000, Default: 10)

步驟5.按一下**Apply**以儲存組態。

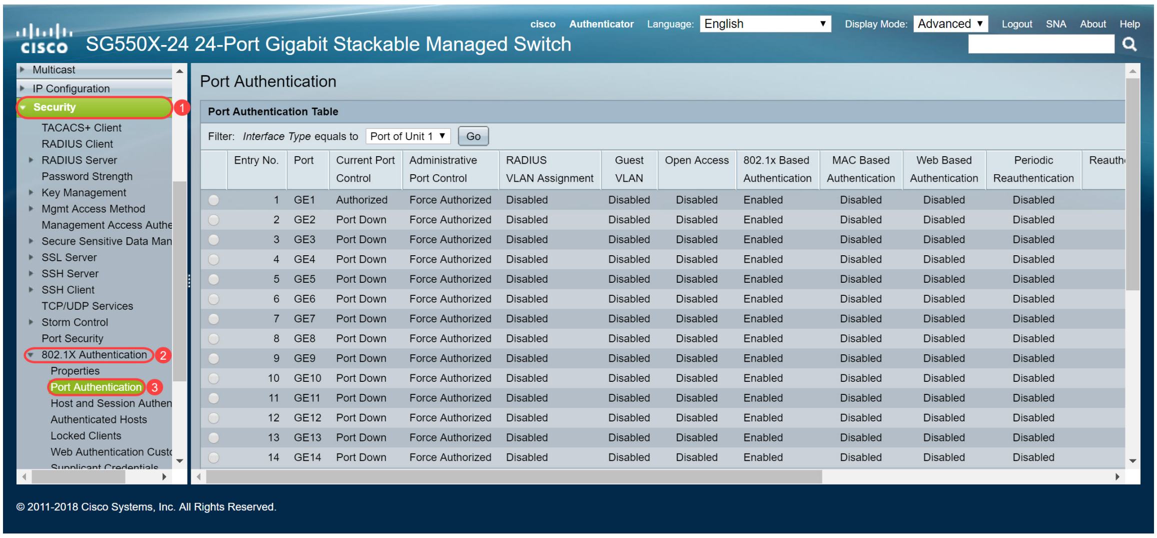
附註：使用*複製設定......*將GE1的相同配置應用到多個埠。將連線到RADIUS伺服器的埠保留為*多主機(802.1X)*。

802.1X驗證連線埠驗證

*Port Authentication*頁為每個埠啟用引數配置。由於某些配置更改僅在埠處於「強制授權」狀態（如主機身份驗證）時才可能發生，因此建議您在更改之前將埠控制更改為「強制授權」。配置完成後，將埠控制返回到其先前狀態。

附註：我們將僅配置基於MAC的身份驗證所需的設定。其餘配置將保留為預設值。

步驟1.導航到**安全> 802.1X身份驗證>埠身份驗證**。



Port Authentication

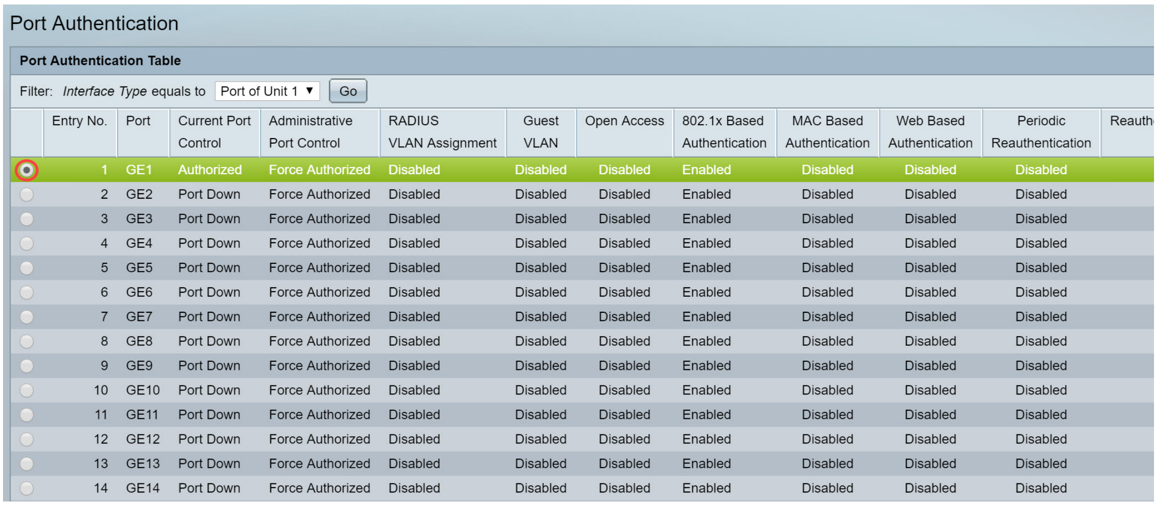
Port Authentication Table

Filter: *Interface Type* equals to Port of Unit 1 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	Periodic Reauthentication	Reauth
○	1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	2	GE2	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	3	GE3	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	4	GE4	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	6	GE6	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	7	GE7	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	8	GE8	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	9	GE9	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	10	GE10	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	11	GE11	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	12	GE12	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	13	GE13	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	14	GE14	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	

步驟2.選擇要配置埠授權的埠。

附註：請勿設定交換器連線的連線埠。交換機是受信任裝置，因此將該埠保留為*強制授權*。



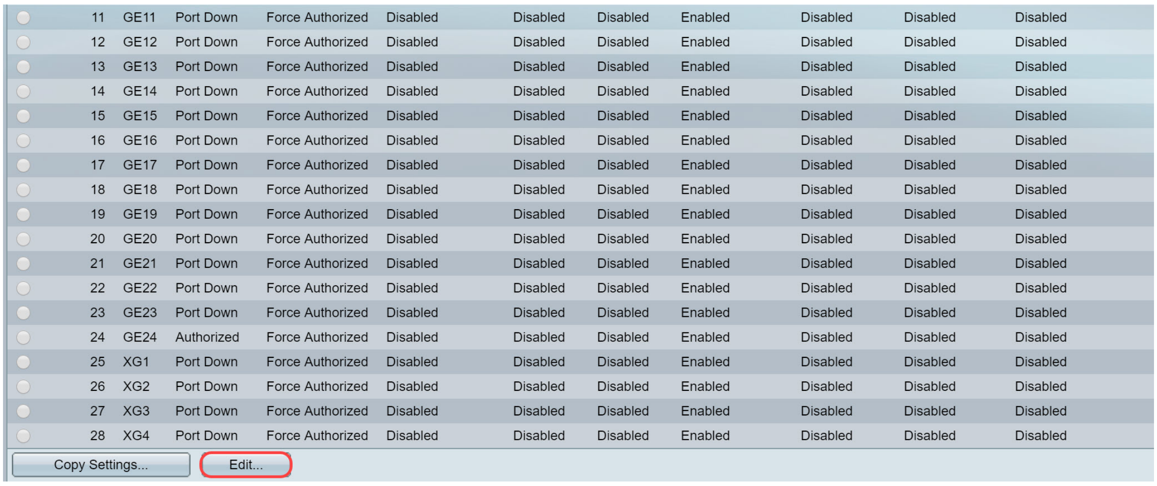
Port Authentication

Port Authentication Table

Filter: *Interface Type* equals to Port of Unit 1 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	Periodic Reauthentication	Reauth
●	1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	2	GE2	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	3	GE3	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	4	GE4	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	6	GE6	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	7	GE7	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	8	GE8	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	9	GE9	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	10	GE10	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	11	GE11	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	12	GE12	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	13	GE13	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
○	14	GE14	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	

步驟3.然後向下滾動並按一下**Edit...** 配置埠。



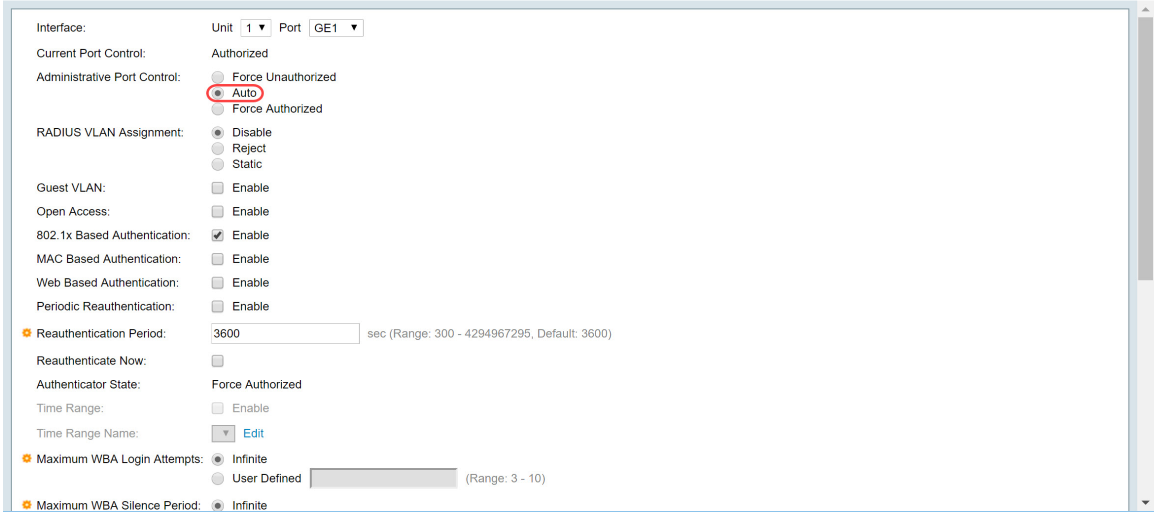
○	11	GE11	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
○	12	GE12	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
○	13	GE13	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
○	14	GE14	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
○	15	GE15	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
○	16	GE16	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
○	17	GE17	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
○	18	GE18	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
○	19	GE19	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
○	20	GE20	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
○	21	GE21	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
○	22	GE22	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
○	23	GE23	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
○	24	GE24	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
○	25	XG1	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
○	26	XG2	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
○	27	XG3	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
○	28	XG4	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled

在*Edit Port Authentication*頁面中，*Current Port Control*欄位顯示當前埠授權狀態。如果狀態是*Authorized*，則連線埠驗證或*Administrative Port Control*是*Force Authorized*。反之，如果狀態為*Unauthorized*，則連線埠未通過驗證或*Administrative Port Control*為*Force Unauthorized*。如果在介面上啟用了Supplicant客戶端，則當前的埠控制將是Supplicant客戶端。

步驟4.選擇管理埠授權狀態。將連線埠設定為**自動**。可用選項包括：

- 強制未授權 — 通過將介面移至未授權狀態來拒絕介面訪問。裝置不通過介面向客戶端提供身份驗證服務。
- 自動 — 在裝置上啟用基於埠的身份驗證和授權。介面根據裝置與客戶端之間的身份驗證交換在授權或未經授權的狀態之間移動。
- 強制授權 — 未經驗證就授權介面。

註： ***Forced Authorized*是預設值。**



Interface: Unit 1 ▾ Port GE1 ▾

Current Port Control: Authorized

Administrative Port Control: ○ Force Unauthorized ● Auto ○ Force Authorized

RADIUS VLAN Assignment: ● Disable ○ Reject ○ Static

Guest VLAN: □ Enable

Open Access: □ Enable

802.1x Based Authentication: ☑ Enable

MAC Based Authentication: □ Enable

Web Based Authentication: □ Enable

Periodic Reauthentication: □ Enable

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

Reauthenticate Now: □

Authenticator State: Force Authorized

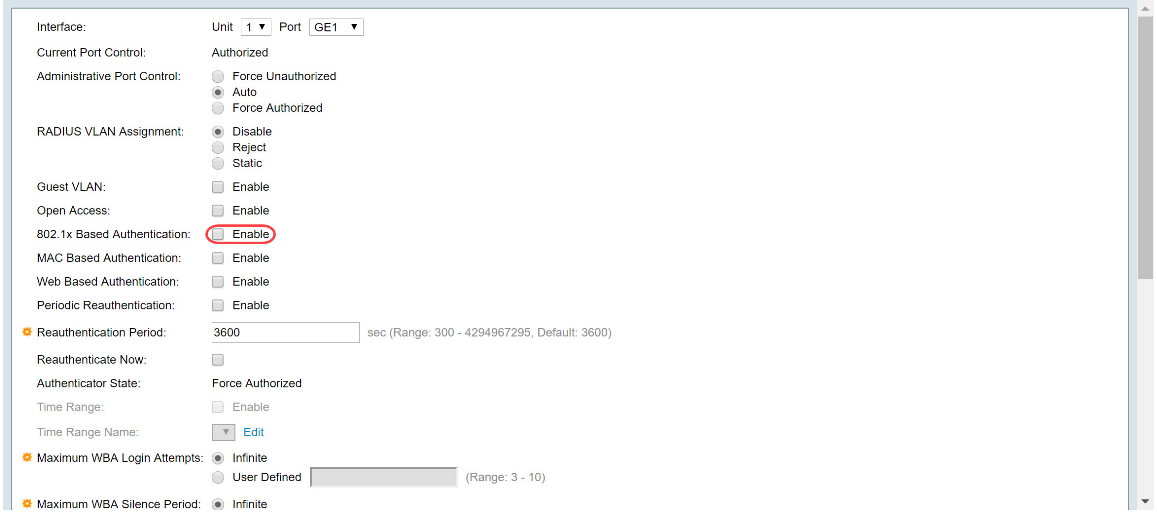
Time Range: □ Enable

Time Range Name: ▾ Edit

Maximum WBA Login Attempts: ● Infinite ○ User Defined (Range: 3 - 10)

Maximum WBA Silence Period: ● Infinite

步驟5.在*802.1X Based Authentication*欄位中，取消選中**Enable**覈取方塊，因為我們不打算使用802.1X作為我們的身份驗證。已啟用基於*802.1x的身份驗證*的預設值。



Interface: Unit 1 ▾ Port GE1 ▾

Current Port Control: Authorized

Administrative Port Control: ○ Force Unauthorized ● Auto ○ Force Authorized

RADIUS VLAN Assignment: ● Disable ○ Reject ○ Static

Guest VLAN: □ Enable

Open Access: □ Enable

802.1x Based Authentication: □ Enable

MAC Based Authentication: □ Enable

Web Based Authentication: □ Enable

Periodic Reauthentication: □ Enable

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

Reauthenticate Now: □

Authenticator State: Force Authorized

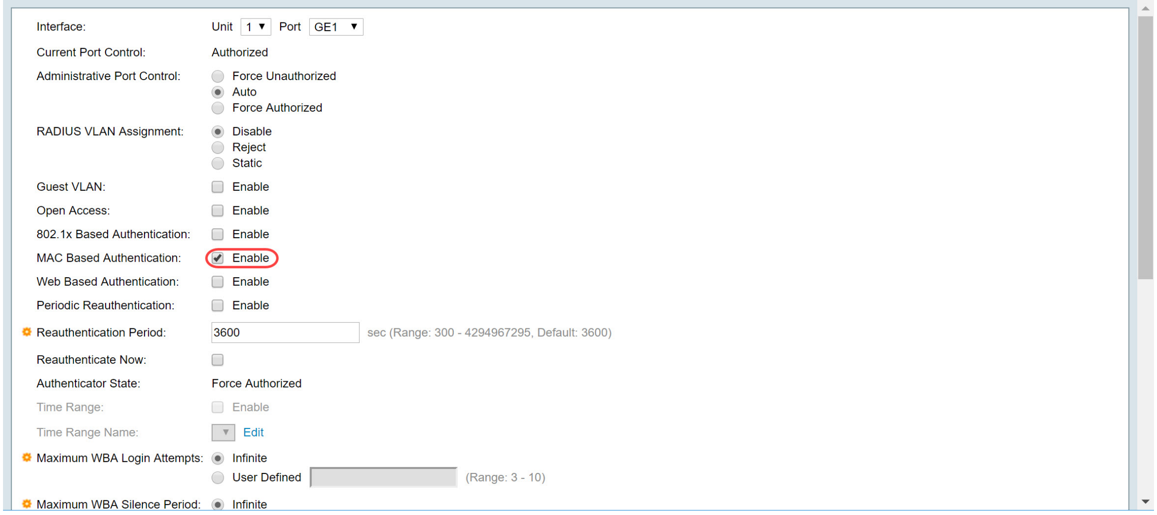
Time Range: □ Enable

Time Range Name: ▾ Edit

Maximum WBA Login Attempts: ● Infinite ○ User Defined (Range: 3 - 10)

Maximum WBA Silence Period: ● Infinite

步驟6.選中*MAC Based Authentication*的**Enable**覈取方塊，因為我們要根據請求方MAC地址啟用埠身份驗證。埠上只能使用8個基於MAC的身份驗證。



Interface: Unit 1 ▾ Port GE1 ▾

Current Port Control: Authorized

Administrative Port Control: ○ Force Unauthorized ● Auto ○ Force Authorized

RADIUS VLAN Assignment: ● Disable ○ Reject ○ Static

Guest VLAN: □ Enable

Open Access: □ Enable

802.1x Based Authentication: □ Enable

MAC Based Authentication: ☑ Enable

Web Based Authentication: □ Enable

Periodic Reauthentication: □ Enable

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

Reauthenticate Now: □

Authenticator State: Force Authorized

Time Range: □ Enable

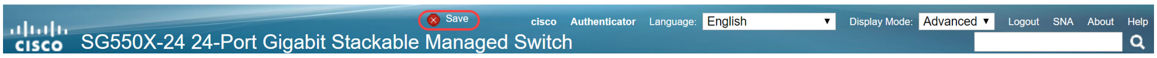
Time Range Name: ▾ Edit

Maximum WBA Login Attempts: ● Infinite ○ User Defined (Range: 3 - 10)

Maximum WBA Silence Period: ● Infinite

步驟7.按一下**Apply** 以儲存變更。

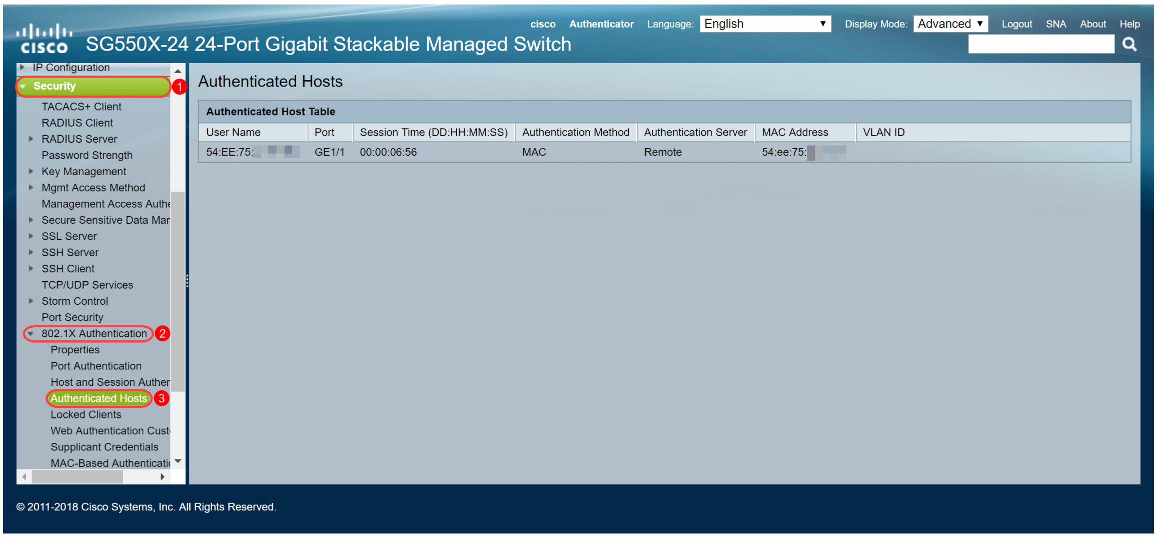
如果要儲存配置，請按螢幕頂部的**Save**按鈕。



結論

現在，您已成功在交換機上配置基於MAC的身份驗證。要驗證基於MAC的身份驗證是否正常工作，請執行以下步驟。

步驟1.導覽至**Security > 802.1X Authentication > Authenticated Hosts**，以檢視有關已驗證使用者的詳細資訊。



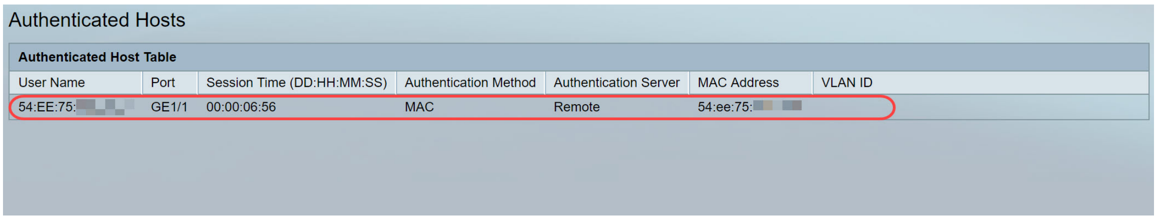
Authenticated Hosts

Authenticated Host Table

User Name	Port	Session Time (DD:HH:MM:SS)	Authentication Method	Authentication Server	MAC Address	VLAN ID
54:EE:75:	GE1/1	00:00:06:56	MAC	Remote	54:ee:75:	

步驟2。在本範例中，您可以看到我們的乙太網路MAC位址在*Authenticated Host Table*中通過驗證。以下欄位定義為：

- 使用者名稱 — 在每個埠上進行身份驗證的請求方名稱。
- Port — 連線埠的編號。
- 作業階段時間(DD:HH:MM:SS) — 請求方在連線埠上通過驗證和授權存取的時間量。
- 驗證方法 — 用於驗證最後一個會話的方法。
- 已驗證伺服器 — RADIUS伺服器。
- MAC Address — 顯示請求方MAC地址。
- VLAN ID — 埠的VLAN。

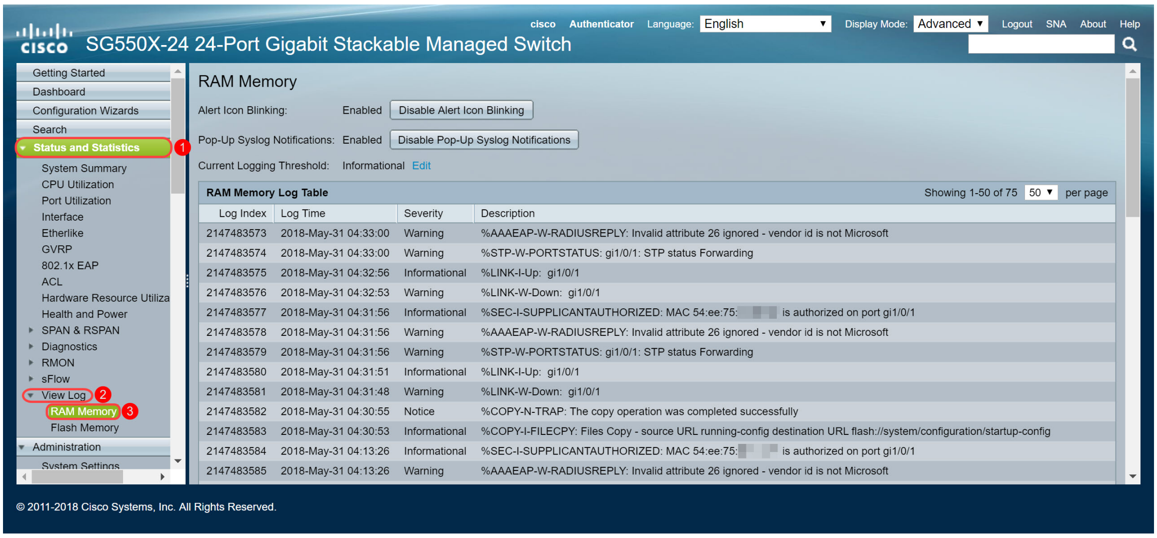


Authenticated Hosts

Authenticated Host Table

User Name	Port	Session Time (DD:HH:MM:SS)	Authentication Method	Authentication Server	MAC Address	VLAN ID
54:EE:75:	GE1/1	00:00:06:56	MAC	Remote	54:ee:75:	

步驟3.（可選）導覽至**Status and Statistics > View Log > RAM Memory**。*RAM Memory*頁面將按時間順序顯示儲存在RAM（快取）中的所有消息。根據*日誌設定*頁面中的配置，條目儲存在RAM日誌中。



RAM Memory

Alert Icon Blinking: Enabled [Disable Alert Icon Blinking]

Pop-Up Syslog Notifications: Enabled [Disable Pop-Up Syslog Notifications]

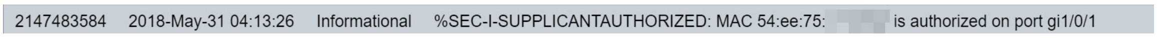
Current Logging Threshold: Informational Edit

RAM Memory Log Table — Showing 1-50 of 75 [50 ▼] per page

Log Index	Log Time	Severity	Description
2147483573	2018-May-31 04:33:00	Warning	%AAAEAP-W-RADIUSREPLY: Invalid attribute 26 ignored - vendor id is not Microsoft
2147483574	2018-May-31 04:33:00	Warning	%STP-W-PORTSTATUS: gi1/0/1: STP status Forwarding
2147483575	2018-May-31 04:32:56	Informational	%LINK-I-Up: gi1/0/1
2147483576	2018-May-31 04:32:53	Warning	%LINK-W-Down: gi1/0/1
2147483577	2018-May-31 04:31:56	Informational	%SEC-I-SUPPLICANTAUTHORIZED: MAC 54:ee:75: is authorized on port gi1/0/1
2147483578	2018-May-31 04:31:56	Warning	%AAAEAP-W-RADIUSREPLY: Invalid attribute 26 ignored - vendor id is not Microsoft
2147483579	2018-May-31 04:31:56	Warning	%STP-W-PORTSTATUS: gi1/0/1: STP status Forwarding
2147483580	2018-May-31 04:31:51	Informational	%LINK-I-Up: gi1/0/1
2147483581	2018-May-31 04:31:48	Warning	%LINK-W-Down: gi1/0/1
2147483582	2018-May-31 04:30:55	Notice	%COPY-N-TRAP: The copy operation was completed successfully
2147483583	2018-May-31 04:30:53	Informational	%COPY-I-FILECPY: Files Copy - source URL running-config destination URL flash://system/configuration/startup-config
2147483584	2018-May-31 04:13:26	Informational	%SEC-I-SUPPLICANTAUTHORIZED: MAC 54:ee:75: is authorized on port gi1/0/1
2147483585	2018-May-31 04:13:26	Warning	%AAAEAP-W-RADIUSREPLY: Invalid attribute 26 ignored - vendor id is not Microsoft

步驟4.在*RAM記憶體日誌表*中，您應該會看到一條資訊性日誌消息，表明您的MAC地址已在埠gi1/0/1上獲得授權。

附註：部分MAC地址模糊不清。



```
2147483584    2018-May-31 04:13:26    Informational    %SEC-I-SUPPLICANTAUTHORIZED: MAC 54:ee:75: [redacted] is authorized on port gi1/0/1
```

檢視本文的影片版本……

按一下此處檢視思科的其他技術對話