

在交換機上配置遠端身份驗證撥入使用者服務 (RADIUS)伺服器設定

目標

遠端驗證撥入使用者服務(RADIUS)是一種網路通訊協定，為連線和使用網路服務的使用者提供集中式驗證、授權和計量 (AAA或Triple A) 管理。RADIUS伺服器透過輸入的登入憑證驗證使用者的身分，以調控網路的存取。例如，在大學校園中安裝了公共Wi-Fi網路。只有具有密碼的學生才能訪問這些網路。RADIUS伺服器會檢查使用者輸入的密碼，並在適當情況下允許或拒絕存取。

設定RADIUS伺服器對於增強安全性很有用，因為它在授權客戶端或使用者訪問網路之前進行身份驗證。RADIUS伺服器會回應與伺服器可用性、重新傳輸和逾時相關的使用者端問題。RADIUS伺服器也會處理使用者連線要求、驗證使用者，並將所需的組態資訊傳送給使用者端，以便向使用者提供服務。

RADIUS伺服器是一種伺服器，可集中控制由啟用RADIUS的裝置組成的網路。RADIUS伺服器根據其轉送決定執行802.1X或媒體存取控制(MAC)位址。

本文說明了如何在Sx350、SG350X和Sx550X系列交換機上配置RADIUS設定。

適用裝置

- Sx350系列
- SG350X系列
- Sx550X系列

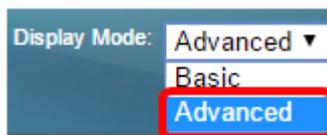
軟體版本

- 2.2.5.68

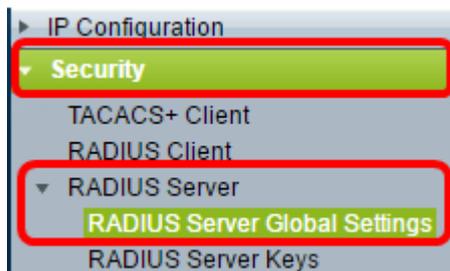
配置RADIUS伺服器設定

配置RADIUS伺服器全域性設定

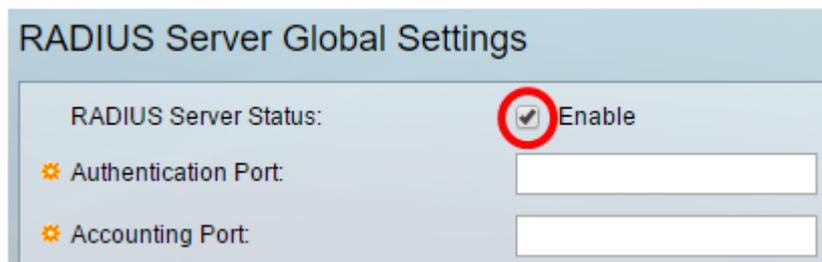
步驟1.登入到交換機基於Web的實用程式，並從Display Mode下拉選單中選擇Advanced。



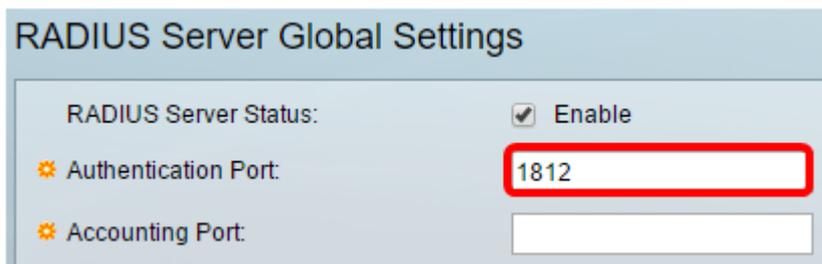
步驟2.選擇Security > RADIUS Server > RADIUS Server Global Settings。



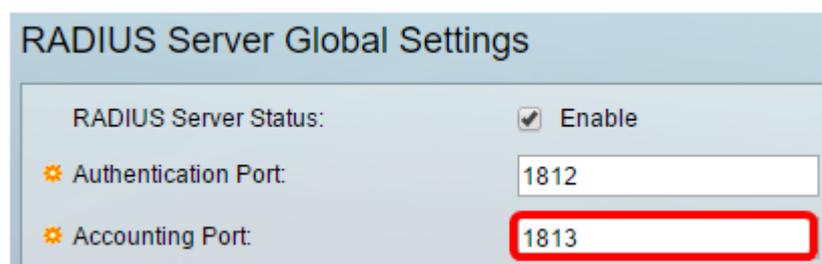
步驟3.選中**Enable**覈取方塊以檢視RADIUS伺服器狀態。



步驟4.輸入用於身份驗證請求的RADIUS伺服器埠的使用者資料包協定(UDP)埠號。範圍為1至65535，預設值為1812。



步驟5.輸入RADIUS伺服器埠的UDP埠號，用於記帳請求。範圍為1至65535，預設值為1813。



步驟6. (可選) 要為RADIUS記帳事件生成陷阱，請選中Trap Settings下的**Enable**覈取方塊，以查詢RADIUS記帳陷阱。



步驟7. (可選) 要為失敗的登入生成陷阱，請選中RADIUS身份驗證失敗陷阱的**啟用**覈取方塊。

Trap Settings

RADIUS Accounting Traps: Enable

RADIUS Authentication Failure Traps: Enable

RADIUS Authentication Success Traps: Enable

Apply Cancel

步驟8. (可選) 要為成功的登入生成陷阱，請選中RADIUS身份驗證成功陷阱的**啟用**覈取方塊。

Trap Settings

RADIUS Accounting Traps: Enable

RADIUS Authentication Failure Traps: Enable

RADIUS Authentication Success Traps: Enable

Apply Cancel

步驟9. 按一下**Apply**。

步驟10. 圖  標表示配置已成功儲存。要永久儲存配置，請轉到「檔案操作」頁或單  擊該頁頂部的圖示。否則，請按一下**關閉**。

配置RADIUS伺服器金鑰

步驟1. 選擇RADIUS Server下的RADIUS Server Keys。

- ▼ Security
 - TACACS+ Client
 - RADIUS Client
 - ▼ RADIUS Server
 - RADIUS Server Global Settings
 - RADIUS Server Keys**

步驟2. (可選) 如果需要，輸入預設RADIUS金鑰。在Default Key中輸入的值將應用到所有已配置的伺服器 (在Add RADIUS Server頁面中) 以使用預設金鑰。

RADIUS Server Keys

Default Key: Keep existing default key

Encrypted

Plaintext (0/128 characters used)

MD5 Digest: bed128365216c019988915ed3add75fb

Apply Cancel

Default Key — 選擇要在裝置和RADIUS客戶端之間進行身份驗證和加密的預設金鑰字串。選項包括：

- 保留現有預設金鑰 — 對於指定的伺服器，裝置會嘗試使用現有預設金鑰字串對RADIUS客戶端進行身份驗證。
- 已加密 — 要使用消息摘要5(MD5)演算法加密通訊，請以加密形式輸入金鑰。
- 明文 — 在明文模式下輸入金鑰字串。

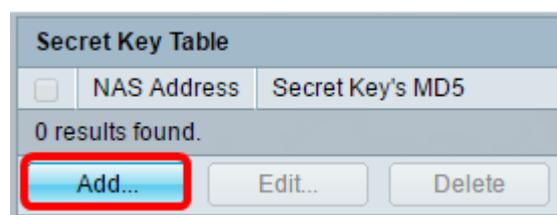
MD5摘要 — 顯示使用者輸入的密碼的MD5摘要。

附註：在本示例中，選擇了Keep existing default key under Default Key。

步驟3.按一下**Apply**。

步驟4.圖  標指示配置已成功儲存。要永久儲存配置，請轉到「檔案操作」頁或單擊該頁頂部的圖示 。

步驟5. (可選) 在Secret Key Table區域下，按一下**Add**按鈕新增金鑰。



步驟6.在NAS Address欄位中輸入NAS或包含RADIUS客戶端的交換機的IP地址。

附註：在下面的影象中，192.168.1.118用作IP地址的示例。

✱ NAS Address:

Secret Key: Use default key

Encrypted

Plaintext

步驟7.選擇您首選的金鑰。

附註：在下圖中，選擇明文作為示例。

✱ NAS Address:

Secret Key: Use default key

Encrypted

Plaintext

選項包括：

- 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 — 要使用MD5加密通訊，請輸入加密形式的金鑰。
- 明文 — 在明文模式下輸入金鑰字串。最多可輸入128個字元。

步驟8.按一下**Apply**。

步驟9.圖  標指示配置已成功儲存。要永久儲存配置，請轉到「檔案操作」頁或單  擊該頁頂部的圖示。否則，請按一下關閉。

設定RADIUS伺服器群組

RADIUS伺服器組是指將裝置用作其RADIUS伺服器的使用者組。要設定組，請遵循以下說明：

步驟1.選擇RADIUS Server下的RADIUS Server Groups。

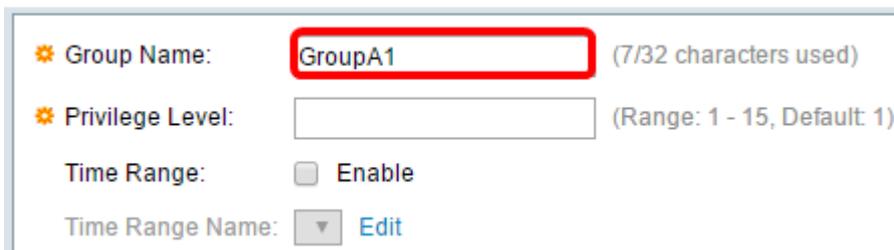


步驟2.按一下RADIUS Server Group表下的Add按鈕。



步驟3.在彈出視窗中，在Group Name欄位中輸入組的名稱。最多可輸入32個字元。

附註：下圖以GroupA1為例。



A screenshot of the configuration form for a RADIUS Server Group. The 'Group Name' field is highlighted with a red box and contains the text 'GroupA1'. To the right of the field, it says '(7/32 characters used)'. Other fields include 'Privilege Level' (empty), 'Time Range' (checkbox 'Enable' is unchecked), and 'Time Range Name' (dropdown menu with 'Edit' button).

步驟4.輸入要分配給組的許可權級別。許可權級別決定您分配給您建立的每個組的訪問級別。您可以設定從1到15的級別。預設值為1。

附註：在此示例中，使用7。

Group Name: GroupA1 (7/32 characters used)
Privilege Level: 7 (Range: 1 - 15, Default: 1)
Time Range: Enable
Time Range Name:

- 1 (只讀CLI訪問) — 組中的使用者無法訪問GUI，並且只能訪問不更改裝置配置的CLI命令。
- 7 (讀/限寫CLI訪問) — 組中的使用者無法訪問GUI，並且只能訪問某些更改裝置配置的CLI命令。有關詳細資訊，請參閱[CLI參考指南](#)。
- 15 (讀/寫管理訪問) — 組中的使用者可以訪問GUI，並可以配置裝置。

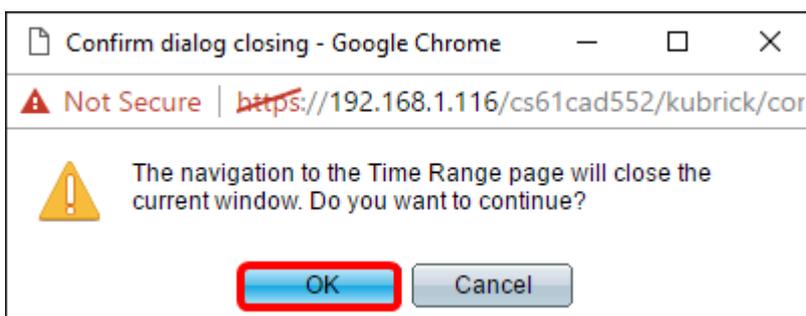
步驟5. (可選) 如果要為此組應用時間範圍，請選中時間範圍的**啟用**竅取方塊。否則，請跳至[步驟15](#)。

Group Name: GroupA1 (7/32 characters used)
Privilege Level: 7 (Range: 1 - 15, Default: 1)
Time Range: Enable

步驟6. 按一下Time Range Name旁邊的**Edit**連結以配置Time設定。

Group Name: GroupA1 (7/32 characters used)
Privilege Level: 7 (Range: 1 - 15, Default: 1)
Time Range: Enable
Time Range Name:

步驟7. 將出現一個彈出視窗，通知您當前視窗將關閉，以便您可以繼續時間範圍設定。按一下「OK」(確定)。



然後您將轉到「時間範圍」頁。

步驟8. 按一下Time Range表下面的**Add**按鈕。

Time Range

Time Range Table			
<input type="checkbox"/>	Time Range Name	Absolute Starting Time	Absolute Ending Time
0 results found.			
Add...	Edit...	Delete	

步驟9.在「時間範圍名稱」欄位中輸入時間範圍的名稱。

附註：在下圖中，以「重新連線」為例。

✱ Time Range Name: (9/32 characters used)

Absolute Starting Time: Immediate
 Date Time HH:MM

Absolute Ending Time: Infinite
 Date Time HH:MM

步驟10.按一下單選按鈕選擇首選的絕對開始和結束時間。

✱ Time Range Name: (12/32 characters used)

Absolute Starting Time: Immediate
 Date Time HH:MM

Absolute Ending Time: Infinite
 Date Time HH:MM

- 絕對開始時間 — 要定義開始時間，請選擇以下選項：
- 立即 — 如果希望時間範圍立即開始，請選擇此選項。
- 日期、時間 — 如果要指定時間範圍開始的日期和時間，請選擇此選項。
- 絕對結束時間 — 要定義開始時間，請選擇以下選項：
- Infinite — 如果希望時間範圍永不結束，請選擇此選項。
- 日期、時間 — 如果要指定時間範圍結束的日期和時間，請選擇此選項。

附註：在此示例中，選擇「日期和時間」。

步驟11.按一下Apply。

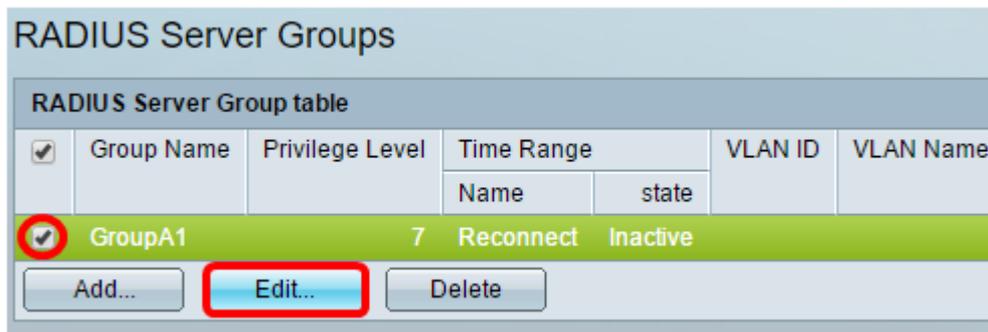
步驟12.圖  標表示配置已成功儲存。要永久儲存配置，請轉到「檔案操作」頁或單擊該頁頂部的圖示。否則，請按一下關閉。

然後您將轉到首頁。

步驟13.再次按一下RADIUS Server下的RADIUS Server Groups。



步驟14.新建立的組現在將顯示在「RADIUS伺服器組」(RADIUS Server Group)表格下。選中組名稱旁邊的框，然後按一下**Edit**。



步驟15。(可選)選擇群組的VLAN。選項包括：

- 無 — 未指定VLAN。
- VLAN ID — 指定VLAN ID。
- VLAN名稱 — 指定VLAN名稱。

A screenshot of the configuration form for a RADIUS Server Group. Fields include: Group Name (GroupA1), Privilege Level (7), Time Range (Enable checked), Time Range Name (Reconnect), and VLAN options. Under 'VLAN', 'VLAN ID' is selected with a radio button, and the value '8' is entered in the adjacent text box. 'Apply' and 'Close' buttons are at the bottom.

附註：本範例中使用的是VLAN ID 8。

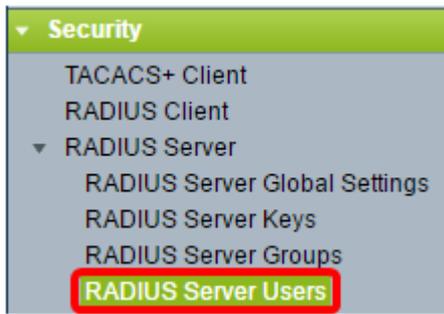
步驟16.按一下**Apply**。

步驟17.圖  標表示配置已成功儲存。要永久儲存配置，請轉到「檔案操作」頁或單擊該頁頂部的圖示。否則，請按一下**關閉**。

配置RADIUS伺服器使用者

要將使用者新增到先前建立的組：

步驟1.按一下「RADIUS Server」底下的**RADIUS Server Users**。

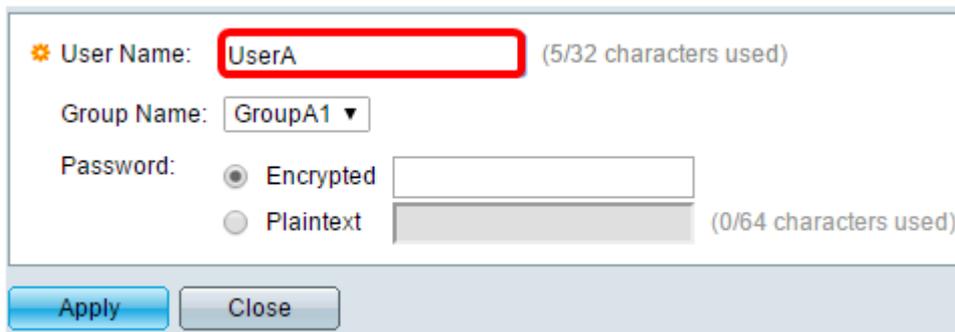


步驟2.按一下RADIUS使用者表底下的**Add**按鈕。

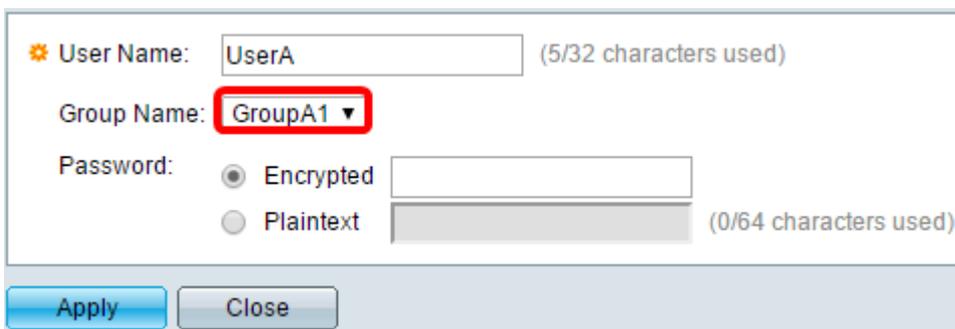


步驟3.在 *User Name* 欄位中輸入用戶的名稱。

附註：在本示例中，使用UserA。



步驟4.從「組名」下拉選單中選擇使用者所屬的組。



步驟5.按一下「密碼」區域中的單選按鈕。

步驟6.輸入您的首選密碼。

User Name: (5/32 characters used)

Group Name:

Password: Encrypted

Plaintext (9/64 characters used)

- 已加密 — 金鑰字串用於使用MD5加密通訊。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。

附註：在此示例中，選擇純文字檔案。

步驟6. 按一下**Apply**。

步驟7. 圖  標指示配置已成功儲存。要永久儲存配置，請轉到「檔案操作」頁或單  擊該頁頂部的圖示。否則，請按一下**關閉**。

現在，您應該已經成功配置了交換機上的RADIUS伺服器設定。

©2016 Cisco Systems, Inc. 保留所有權利。