

300系列託管交換器上的TACACS+伺服器組態

目標

TACACS+是思科專有通訊協定，透過使用者名稱和密碼提供驗證和授權。要配置TACACS+伺服器，使用者必須具有15個訪問許可權，該許可權允許使用者訪問交換機的所有配置功能。300系列託管交換器可以充當TACACS+使用者端，所有連線的使用者均可以透過正確設定的TACACS+伺服器進行網路中的驗證和授權。本文說明如何在300系列託管交換器上設定TACACS+伺服器。

附註：有關如何將許可權訪問15分配給使用者的詳細資訊，請參閱[300系列託管交換機上的使用者帳戶配置](#)一文。

適用裝置

·SF/SG 300系列託管交換器

軟體版本

·v1.2.7.76

設定TACACS+伺服器的預設引數

本節說明如何設定TACACS+伺服器的預設引數。在沒有使用伺服器的其他自定義配置的情況下，使用這些引數。

步驟1.登入到Web配置實用程式並選擇**Security > TACACS+**。TACACS+頁面隨即開啟：

TACACS+

Use Default Parameters

IP Version: Version 4

Source IP Address: 192.168.10.1

Key String: Encrypted Plaintext TestKey (7/128 Characters Used)

Timeout for Reply: 5 sec. (Range: 1 - 30)

Apply Cancel

TACACS+ Server Table

Server	Priority	Source IP Address	Key String (Encrypted)	Timeout for Reply	Authentication IP Port	Single Connection	Status
0 results found.							

Add... Edit... Delete

Display Sensitive Data As Plaintext

步驟2.在「來源IP位址」欄位中，輸入TACACS+伺服器所需的預設IP位址。

步驟3.在「金鑰字串」欄位中，選擇如何輸入金鑰。此金鑰用於在交換機和TACACS+伺服器之間交換消息。這是使用的預設金鑰字串。此金鑰必須與TACACS+伺服器上配置的金鑰相同。如果使用new key string新增了TACAS+伺服器，則新新增的金鑰字串優先於預設金鑰字串。按一下其中一個可用選項的單選按鈕：

- 已加密 — 此選項可讓您輸入加密的金鑰。
- 純文字檔案 — 此選項允許您以純文字檔案格式輸入金鑰。

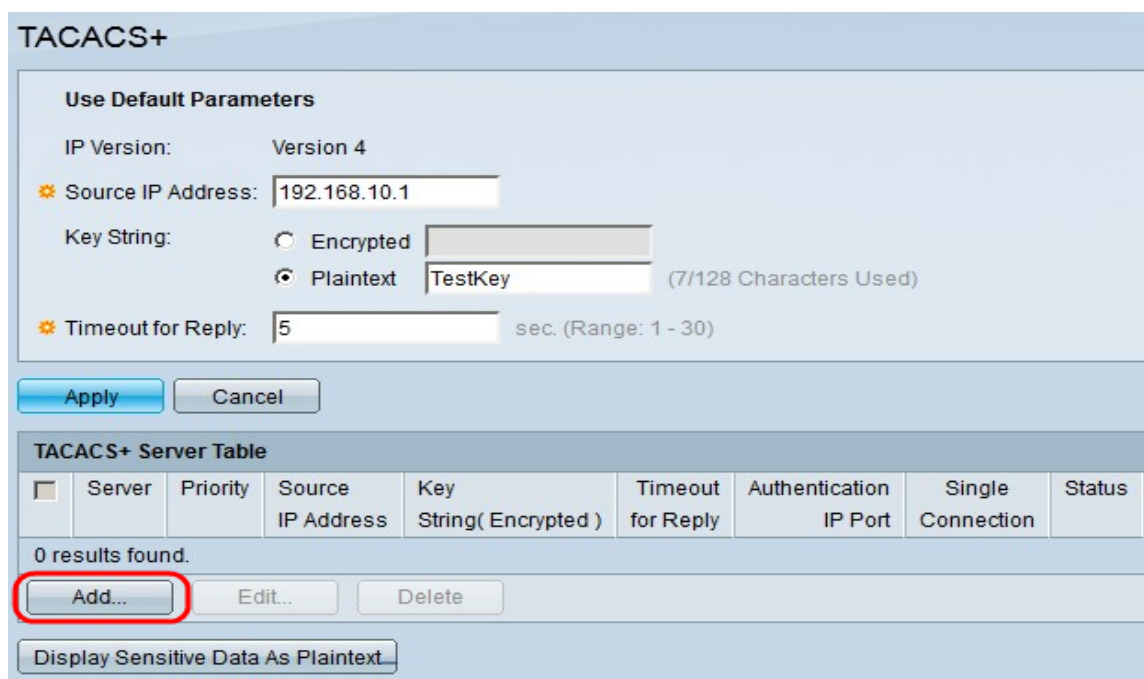
步驟4.在Timeout for Reply欄位中輸入在TACACS+伺服器和交換機之間的連線到期之前所經過的時間（以秒為單位）。

步驟5.按一下Apply以儲存TACACS+伺服器的預設引數。

新增TACACS+伺服器

本節說明如何將TACACS+伺服器新增到300系列代管交換器。

步驟1.登入到Web配置實用程式並選擇**Security > TACACS+**。TACACS+頁面隨即開啟：



TACACS+

Use Default Parameters

IP Version: Version 4

Source IP Address: 192.168.10.1

Key String: Encrypted Plaintext TestKey (7/128 Characters Used)

Timeout for Reply: 5 sec. (Range: 1 - 30)

Apply Cancel

TACACS+ Server Table

<input type="checkbox"/>	Server	Priority	Source IP Address	Key String(Encrypted)	Timeout for Reply	Authentication IP Port	Single Connection	Status
0 results found.								
<input type="button" value="Add..."/>	<input type="button" value="Edit..."/>	<input type="button" value="Delete"/>						

Display Sensitive Data As Plaintext

步驟2.按一下Add。出現Add a TACACS+ Server視窗：

步驟3.在「伺服器定義」欄位中，選擇伺服器的定義方式。按一下其中一個可用選項的單選按鈕：

- 按IP地址 — 此選項可讓您定義具有IP地址的伺服器。
- 按名稱 — 此選項允許您使用完全限定域名(FQDN)定義伺服器。

步驟4.在「伺服器IP地址/名稱」欄位中，根據您在步驟3中的選擇輸入TACACS+伺服器的IP地址或域名。

步驟5.在「優先順序」欄位中輸入伺服器的所需優先順序。如果交換器無法與優先順序最高的伺服器建立作業階段，則交換器會嘗試與優先順序次高的伺服器建立作業階段。零被視為最高優先順序。

步驟6.在Source IP Address欄位中，按下一個選項以定義源IP地址。可用選項包括：

- 使用者預設值 — 此選項使用在預設引數部分配置的預設源IP地址。
- 使用者定義 — 此選項使用使用者定義的交換機源IP地址。從下拉選單中選擇一個可用的使用者定義IP地址。

步驟7.在「金鑰字串」欄位中，輸入TACACS+伺服器和交換機之間的加密金鑰。此金鑰必須與TACACS+伺服器上配置的金鑰相同。按一下其中一個可用選項的單選按鈕以輸入以下資訊：

- 使用預設值 — 此選項使用以前配置的預設引數。
- 使用者定義 (加密) — 此選項可讓您輸入新的加密金鑰。
- 使用者定義 (明文) — 此選項可讓您以純文字檔案格式輸入金鑰。

步驟8.在Timeout for Reply欄位中，輸入伺服器與交換機之間的連線到期之前應經過的時間 (以秒為單位)。按一下其中一個可用選項的單選按鈕：

- 使用預設值 — 此選項使用以前配置的預設引數。
- 使用者定義 — 此選項可讓您輸入新值。

步驟9.在Authentication Port欄位中，輸入用於建立TACACS+會話的埠號。

步驟10。（可選）在Single Connection欄位中，勾選**Enable**覈取方塊，以便交換器在TACACS+和交換器之間維持單一開放連線。由於交換器不會針對每次TACACS+作業開啟或關閉連線，因此此選項更有效率。相反，透過單一連線，交換器可以處理多個TACACS+作業。

步驟11.按一下**Apply**以進行儲存。

附註：下圖說明設定之後的變更：

The screenshot displays the TACACS+ configuration interface. The top section, titled "Use Default Parameters", includes the following settings:

- IP Version: Version 4
- Source IP Address: 192.168.10.1
- Key String: Encrypted (selected) with the value msllBwBuYnGQnhhO. The Plaintext option is also visible with a note "(0/128 Characters Used)".
- Timeout for Reply: 5 sec. (Range: 1 - 30)

Below these settings are "Apply" and "Cancel" buttons. The "TACACS+ Server Table" section contains a table with the following data:

<input type="checkbox"/>	Server	Priority	Source IP Address	Key String(Encrypted)	Timeout for Reply	Authentication IP Port	Single Connection	Status
<input type="checkbox"/>	192.168.10.100	10	192.168.10.1	msllBwBuYnGQnh...	5	49	Enabled	Not Connected

At the bottom of the table are "Add...", "Edit...", and "Delete" buttons. A checkbox at the very bottom is labeled "Display Sensitive Data As Plaintext".