TACACS+ Server Configuration on the 300 Series Managed Switches

Objective

TACACS+ is a Cisco proprietary protocol which provides authentication and authorization via username and password. To configure a TACACS+ server, the user must have privilege 15 access, which let the user access to all the configuration features of the switch. The 300 Series Managed Switches can act as a TACACS+ client, where all the users connected can be authenticated and authorized in the network via a properly configured TACACS+ server. This article explains how to configure a TACACS+ server on the 300 Series Managed Switches.

Note: For more information on how to assign privilege access 15 to users, refer to the article *User Account Configuration on 300 Series Managed Switches.*

Applicable Devices

- SF/SG 300 Series Managed Switches

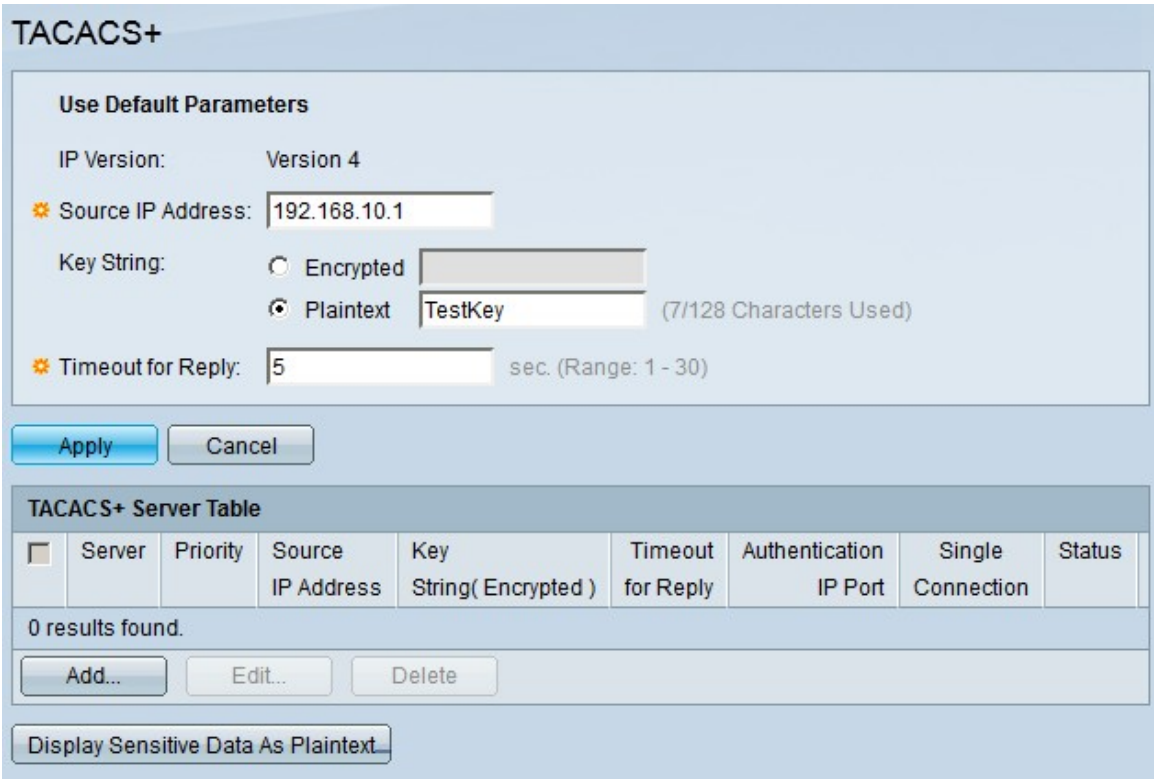
Software Version

- v1.2.7.76

Configure Default Parameters of a TACACS+ Server

This section explains how to configure the default parameters of a TACACS+ server. These parameters are used in the case that no other custom configuration for the server is used.

Step 1. Log in to the web configuration utility and choose **Security > TACACS+**. The *TACACS+* page opens:



Step 2. In the Source IP Address field, enter the desired default IP address for the TACACS+ server.

Step 3. In the Key String field, choose how to enter the key. This key is used to exchange messages between the switch and TACACS+ servers. This is the default key string used. This key must be the same key configured on the TACACS+ server. If a TACAS+ server is added with a new key string, then the newly added key string takes precedence over the default key string. Click the radio button of one of the available options:

- Encrypted — This option lets you enter an encrypted key.
- Plaintext — This option lets you enter a key in plain text format.

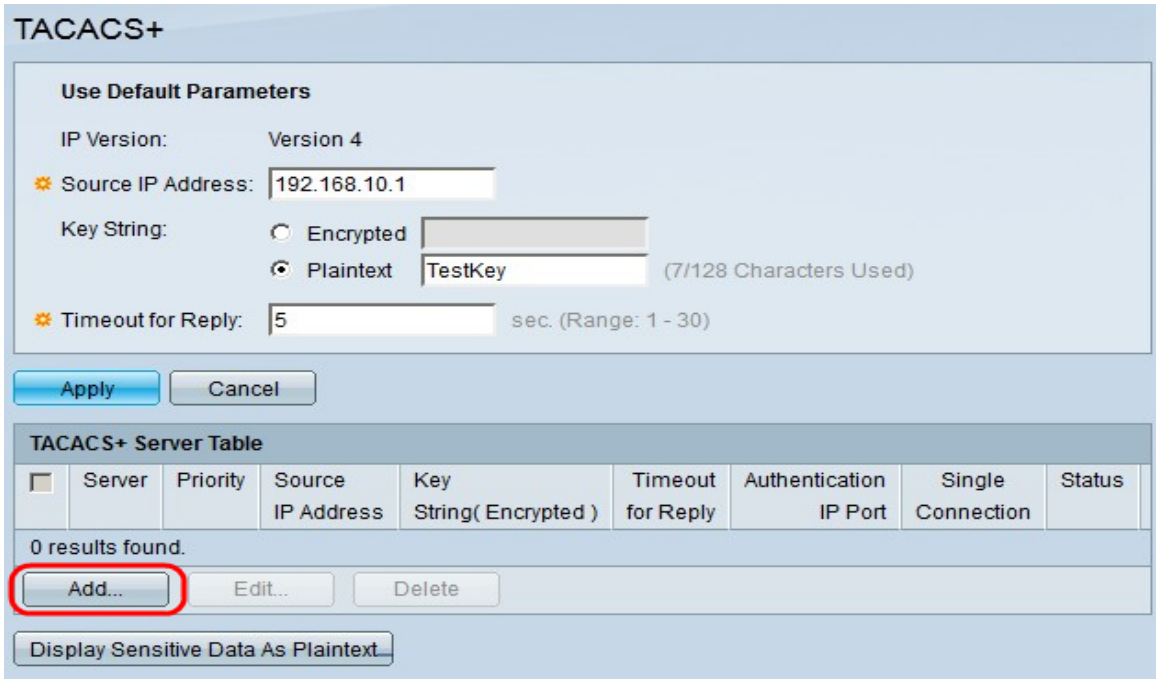
Step 4. In the Timeout for Reply field enter the time, in seconds, that should elapse before the connection between a TACACS+ server and the switch expires.

Step 5. Click **Apply** to save the default parameters of the TACACS+ server.

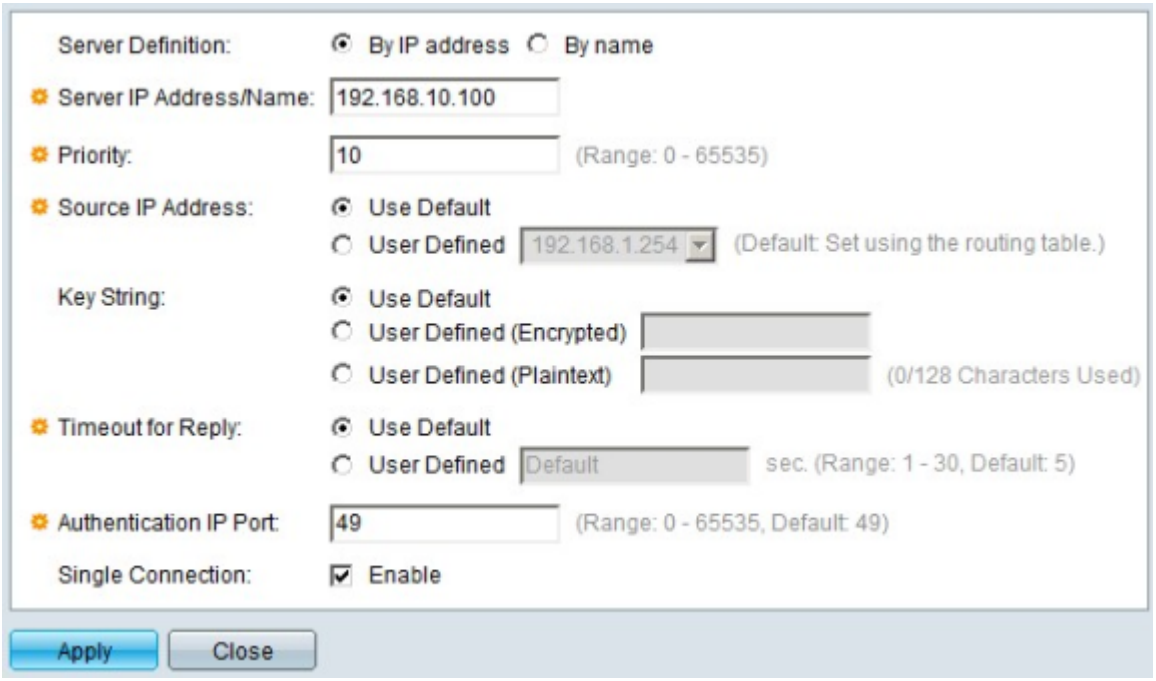
Add a TACACS+ Server

This section explains how to add a TACACS+ server to a 300 Series Managed Switch.

Step 1. Log in to the web configuration utility and choose **Security > TACACS+**. The *TACACS+* page opens:



Step 2. Click **Add**. The *Add a TACACS+ Server* window appears:



Step 3. In the Server Definition field, choose how the server is defined. Click the radio button of one of the available options:

- By IP address — This option lets you define the server with an IP address.
- By Name — This option lets you define the server with a fully qualified domain name (FQDN).

Step 4. In the Server IP Address/Name field, enter the IP address or the domain name of the TACACS+ server based on your choice in Step 3.

Step 5. In the Priority field, enter the desired priority for the server. If the switch cannot establish a session with the highest priority server, the switch tries the server with the next highest priority. Zero is considered the highest priority.

Step 6. In the Source IP Address field, click an option to define the source IP address. The available options are:

- User Default —This options uses the default source IP address configured in the default parameter section.
- User Defined —This option uses a user defined source IP address of the switch. Choose from the drop-down list one of the available user defined IP addresses.

Step 7. In the Key String field, enter the encryption key between the TACACS+ server and the switch. This key must be the same key configured on the TACACS+ server. Click the radio button of one of the available options to enter this information:

- Use Default — This option uses the default parameter that was previously configured.
- User Defined (Encrypted) — This option lets you enter a new encrypted key.
- User Defined (Plaintext) — This option lets you enter a key in a plain text format.

Step 8. In the Timeout for Reply field, enter the time in seconds that should elapse before the connection between the server and the switch expires. Click the radio button of one of the available options:

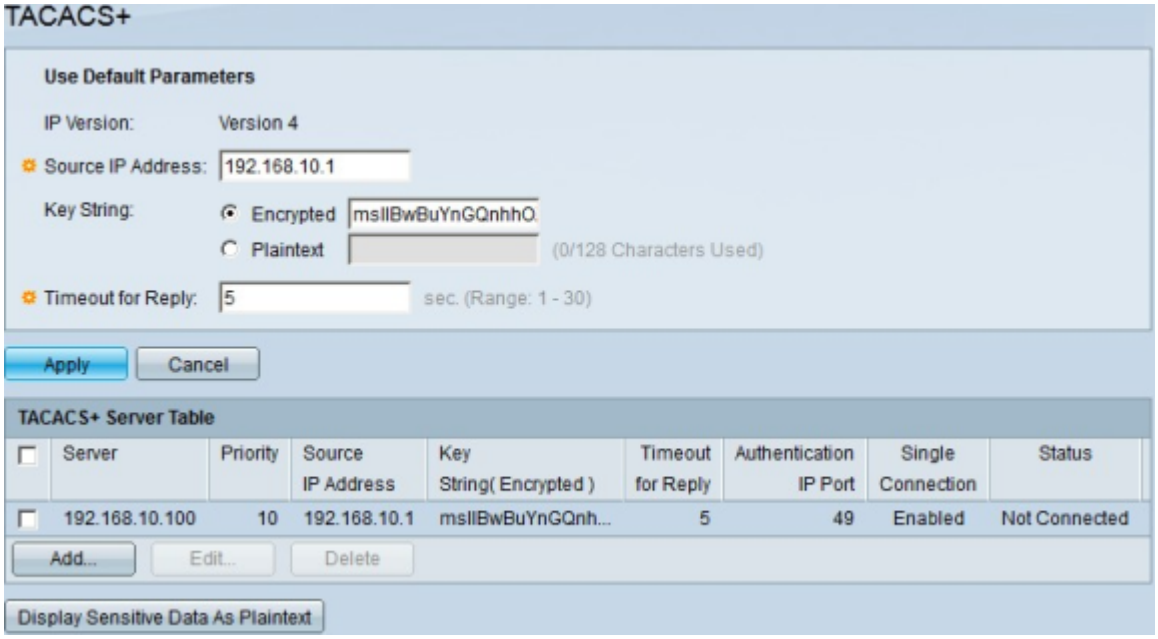
- Use Default — This option uses the default parameter previously configured.
- User Defined — This options lets you enter a new value.

Step 9. In the Authentication Port field, enter the port number used to establish a TACACS+ session.

Step 10. (Optional) In the Single Connection field, check the **Enable** check box so the switch maintains a single open connection between the TACACS+ and the switch. This option is more efficient since the switch does not open or close the connection for every TACACS+ operation. Instead, with a single connection, the switch can handle multiple TACACS+ operations.

Step 11. Click **Apply** to save.

Note: The image below depicts the changes after the configuration:


TACACS+
Use Default Parameters
IP Version:
Version 4
Source IP Address:
192.168.10.1
Key String:
Encrypted
msIIBwBuYnGQnhhO
Plaintext
(0/128 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
192.168.10.100
10
192.168.10.1
msIIBwBuYnGQnh...
5
49
Enabled
Not Connected
Add...
Edit...
Delete
Display Sensitive Data As Plaintext