TACACS+ Configurtion on SFE / SGE Stackable Managed Switches

Objective

Terminal Access Controller Access Control System (TACACS+) is an access control network protocol. The TACACS+ protocol uses encrypted protocol exchanges between the connected device and the TACACS+ server to ensure network integrity. It separates the authentication and authorization services. TACACS+ authentication provides authentication at login via user names and passwords. TACACS+ authorization is performed at login. Once the authorization process is completed an authorized session is started. The default paramaters are assigned to newly created TACACS+ servers that do not have specified parameters. TACACS+ is only supported with IPv4 addresses.

This article explains how to configure TACACS+ on the SFE / SGE Stackable Managed Switches.

Applicable Devices

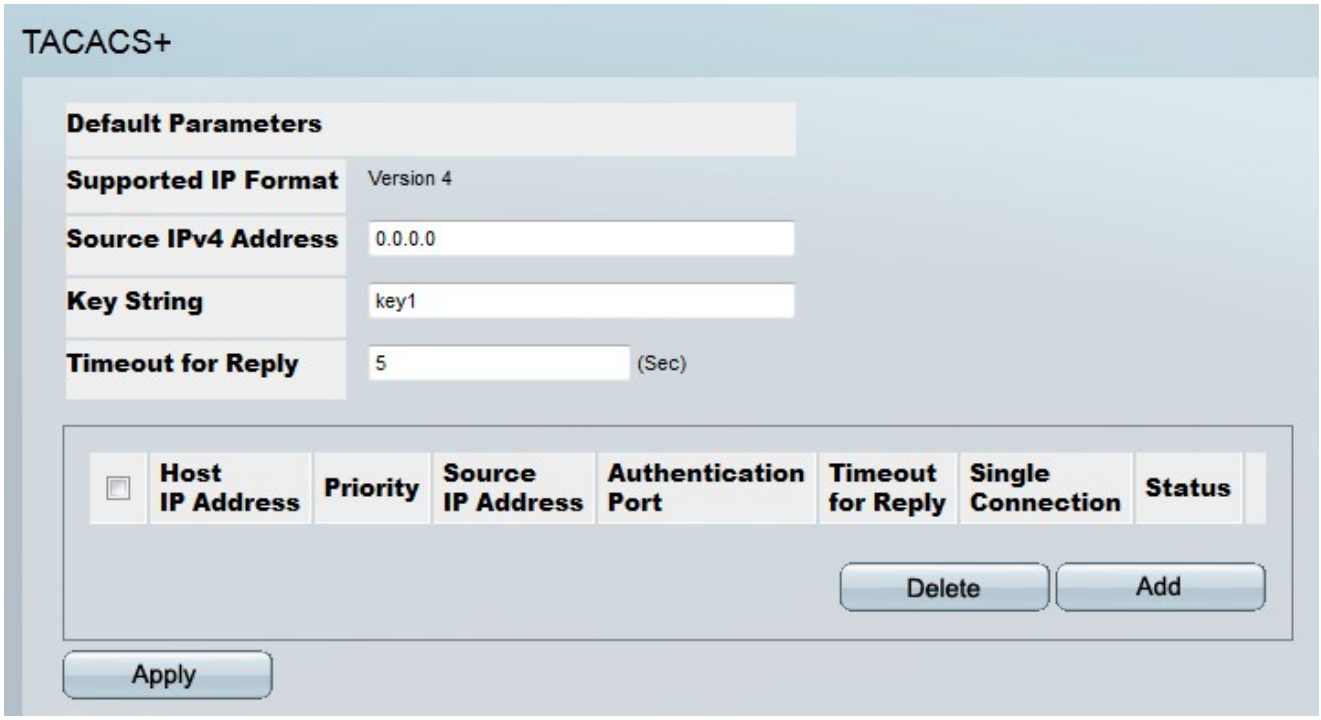
- SFE / SGE Stackable Managed Switches

Software Version

- v3.0.2.0

TACACS+

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



Configure Default Parameters

Step 1. Enter a source address used for the TACACS+ session between the connected device and the TACACS+ server in the Source IPv4 Address field.

Step 2. Enter an authentication key for the TACACS+ server in the Key String field.

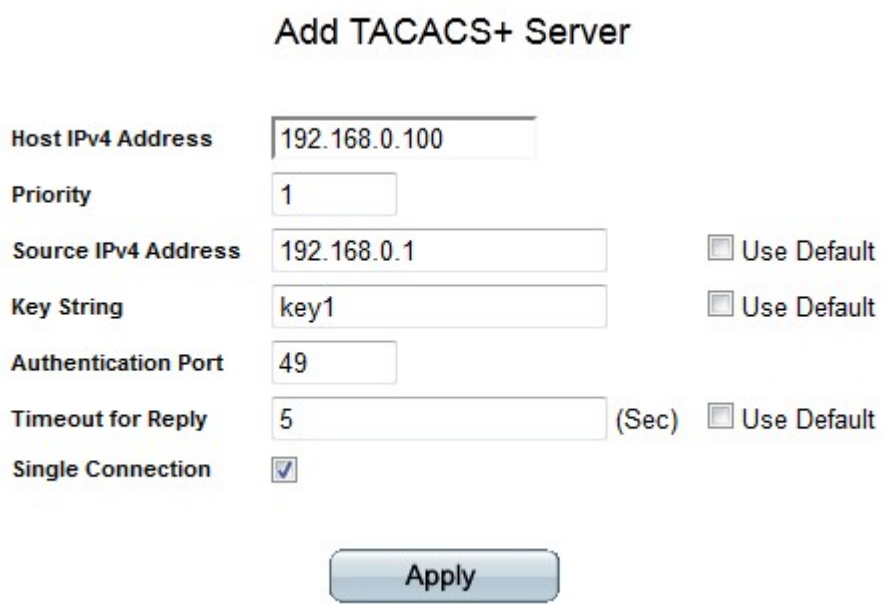
Step 3. Enter a timeout value in the Timeout for Reply field. This value represents the amount of time that passes before the connection between the device and the TACACS+ server times out.

Step 4. Click **Apply**.

Caution: This only saves your configuration to the running configuration file. This means any changes made will be lost if the device is rebooted. If you wish to save these changes even after a system reboot, you need to copy the running configuration file to the startup configuration file. See *Copy Configuration File on SFE/SGE Series Managed Switches* for more information on how to do this.

Add TACACS+ Server

Step 1. Click **Add** to add a new TACACS+ server. The *Add TACACS+ Server* window appears.



Step 2. Enter a TACACS+ server address in the Host IPv4 Address field.

Step 3. Enter a value in the Priority field. This value determines the order in which TACACS+ servers are used. Lower priority numbers are used first.

Step 4. Enter the device source address used for the TACACS+ session between the device and the TACACS+ server in the Source IPv4 Address field. Check **Use Default** to use the default 0.0.0.0 IP address.

Step 5. Enter an authentication key for the TACACS+ server in the Key String field. Check **Use Default** to use the default empty string as the key string.

Step 6. Enter the port number through which the TACACS+ session occurs in the

Authentication Port field.

Step 7. Enter a timeout value in the Timeout for Reply field. This value represents the amount of time that passes before the connection between the device and the TACACS+ server times out. Check **Use Default** to use the default value of 5 seconds.

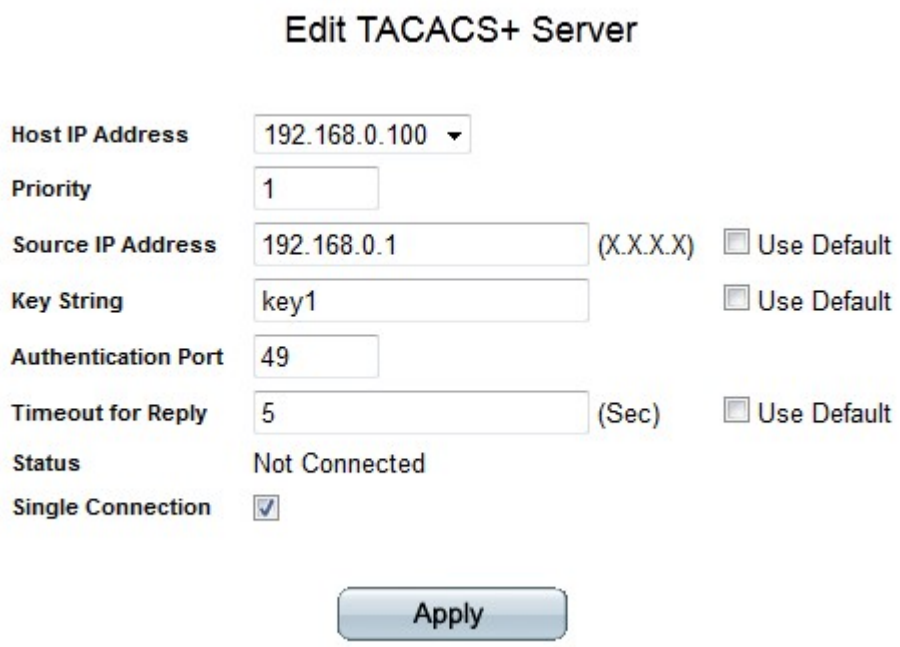
Step 8. Check **Single Connection** to enable a single open connection between the device and the TACACS+ server.

Step 9. Click **Apply**.

Caution: This only saves your configuration to the running configuration file. This means any changes made will be lost if the device is rebooted. If you wish to save these changes even after a system reboot, you need to copy the running configuration file to the startup configuration file. See *Copy Configuration File on SFE/SGE Series Managed Switches* for more information on how to do this.

Edit TACACS+ Server

Step 1. Click **Edit** to edit a TACACS+ server. The Edit TACACS+ Server window appears.



Step 2. From the Host IP address field choose an IP address for the TACACS+ server.

Step 3. Enter a value in the Priority field. This value determines the order in which TACACS+ servers are used. Lower priority numbers are used first.

Step 4. Enter the device source address used for the TACACS+ session between the device and the TACACS+ server in the Source IPv4 Address field. Check **Use Default** to use the default 0.0.0.0 IP address.

Step 5. Enter an authentication key for the TACACS+ server in the Key String field. Check **Use Default** to use the default empty string as the key string.

Step 6. Enter the port number through which the TACACS+ session occurs in the Authentication Port field.

Step 7. Enter a timeout value in the Timeout for Reply field. This value represents the amount of time that passes before the connection between the device and the TACACS+ server times out. Check **Use Default** to use the default value of 5 seconds.

- Status — Displays if a connection is established between the device and TACACS+ server.

Step 8. Check **Single Connection** to enable a single open connection between the device and the TACACS+ server.

Step 9. Click **Apply**.

Caution: This only saves your configuration to the running configuration file. This means any changes made will be lost if the device is rebooted. If you wish to save these changes even after a system reboot, you need to copy the running configuration file to the startup configuration file. See *Copy Configuration File on SFE/SGE Series Managed Switches* for more information on how to do this.