Management Access Authentication on 200/300 Series Managed Switches

Objective

Management access modes such as SSH, Console, Telnet, HTTP, and HTTPS allow a user to access a device. Authentication can be required of users to improve security. The 200 and 300 Series Managed Switches can authenticate locally or on a TACACS+ or RADIUS server. This document explains how to assign an authentication method on the 200 and 300 Series Managed Switches.

Applicable Devices

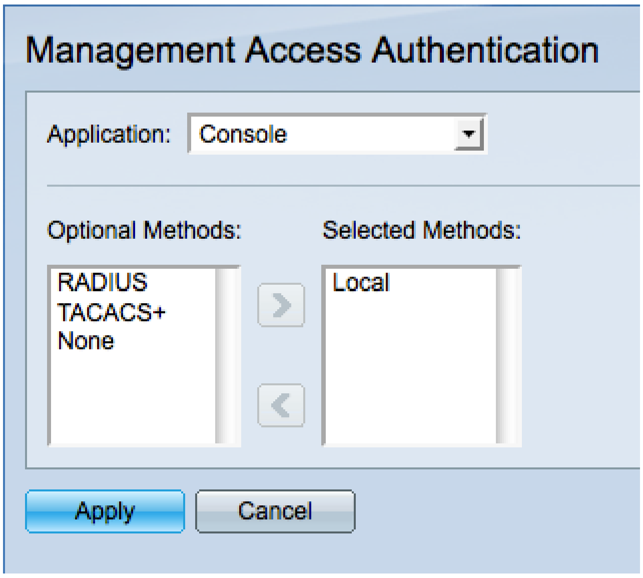
- SF/SG 200 and SF/SG 300 Series Managed Switches

Software Version

- 1.3.0.62

Management Access Authentication

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



Management Access Authentication

Application: Console

Optional Methods: RADIUS, TACACS+, None

Selected Methods: Local

Step 2. Choose the type of application that you would like to assign authentication to from the Application drop-down list. Possible applications are:

- Console — Allows you to manage the switch with a console interface. Allows you to connect to the switch and perform some configurations even if the IP address of the switch is not known.

- Telnet — A character-based communication protocol that allows you to remotely connect to the switch over a TCP/IP network. Telnet is not recommended due to the lack of encryption.

- Secure Telnet (SSH) — Performs the same functions as telnet plus encryption. SSH is recommended for remote connections.

- HTTP — Protocol that allows you to access the graphical user interface (GUI) of the switch. This is in contrast to Telnet and SSH which are command prompt based.

- Secure HTTP (HTTPS) — Performs the same functions as HTTP with the addition of secure communication.

Step 3. Choose a method of authentication from the list of Optional Methods and then click the **>** button to move it to the Selected Methods list. Different methods provide different levels of security.

Note: The order that the authentication methods are selected is the order that user authentication occurs. If RADIUS is selected before local, the device will attempt to authenticate the user by a RADIUS server before the local method.

- RADIUS— RADIUS encrypts just the password. Authentication is on a RADIUS server and requires a configured RADIUS server.

- TACACS+— TACACS+ encrypts all of the data during authentication. Authentication is on a TACACS+ server and requires a configured TACACS+ server.

- None— Authentication is not required to access the switch.

- Local— User information is verified by information stored on the switch.

Step 4. Click **Apply** to save the authentication settings or click **Cancel** to cancel your changes.