

# Management Access Authentication Setup on Sx500 Series Stackable Switches

## Objective

Authentication method helps the network administrators to allow or deny the access of the device through various methods like SSH, Telnet, HTTP etc. RADIUS, TACACS+, and Local are the three types of security that can be enabled in the authentication setup function on the SG500x Series. There is also an option for no security to be present on the switch. RADIUS encrypts just the password in the access-request packet that is transferred from the client to the server. TACACS+ encrypts the whole body of the packet. However, it leaves a standard TACACS+ header. Local just verifies user information that is stored on the switch. User authentication occurs in the order that the authentication methods are selected. If the first authentication method is not available, the next selected method is used. If an authentication method fails or the user has insufficient privilege level, the user is denied access to the switch.

This article explains how to assign authentication methods to access modes like SSH, console, Telnet, HTTP and HTTPS on the SG500x Series Stackable Switches.

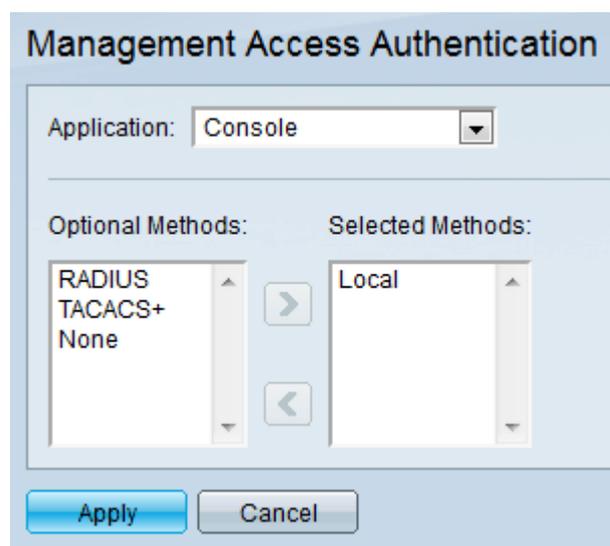
## Applicable Devices

- Sx500 Series Stackable Switches

## Software Version

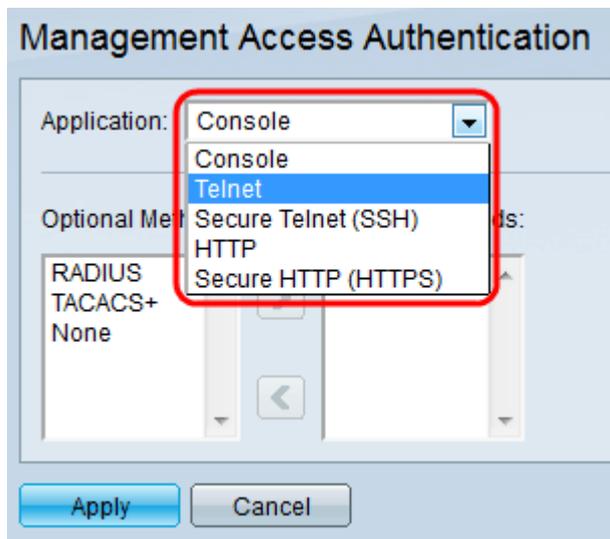
- 1.3.0.62

## Management Access Authentication Setup

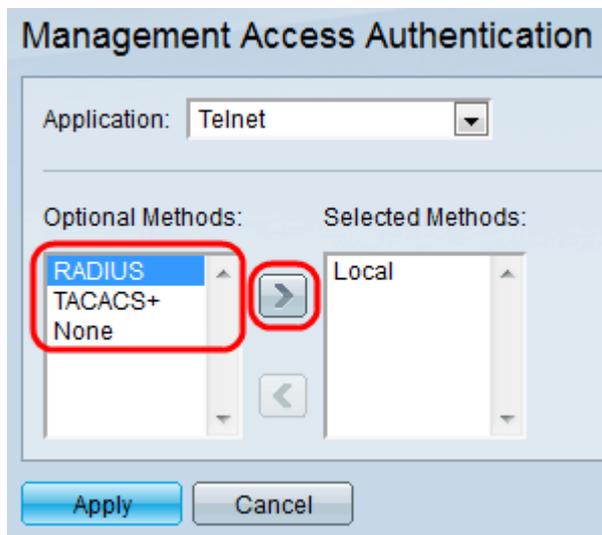


The screenshot shows the 'Management Access Authentication' configuration window. At the top, the 'Application' dropdown menu is set to 'Console'. Below this, there are two columns: 'Optional Methods' and 'Selected Methods'. The 'Optional Methods' list contains 'RADIUS', 'TACACS+', and 'None'. The 'Selected Methods' list contains 'Local'. There are right and left arrow buttons between the two lists. At the bottom of the window, there are 'Apply' and 'Cancel' buttons.

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

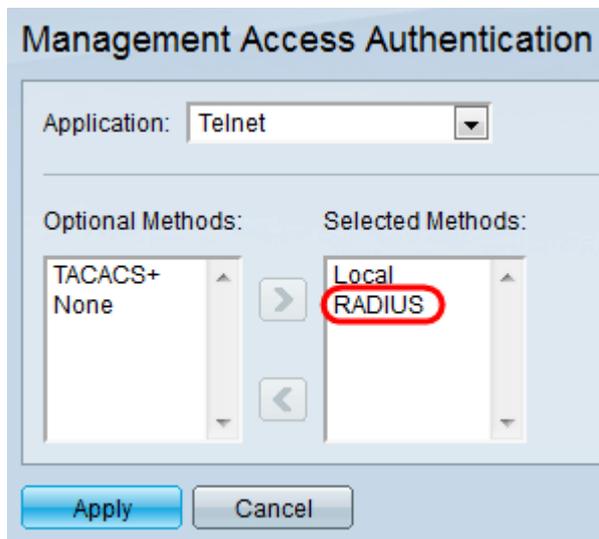


Step 2. Choose the type of application to which you would like to assign authentication from the Application drop-down list.



Step 3. Choose the method of authentication from the Optional Methods list and click the **Right Arrow** icon to move it to the Selected Methods list.

- RADIUS — Authentication is on a RADIUS server. A RADIUS server must be configured.
- TACACS+ — Authentication is on a TACACS+ server. A TACACS+ server must be configured.
- Local — User information is verified by information stored on the switch.
- None — Authentication is not required to access the switch.



Step 4. (Optional) Choose the method from the Selected Methods and click the **Left Arrow** icon to remove from the selected methods and move it to Optional Methods.

Step 5. Click **Apply** to save the authentication settings.