Management Access Method Access Profile Settings on Sx500 Series Stackable Switches

Objective

The objective of this document is to help configure access profile settings on Sx500 Series Stackable Switches. Access profiles use access methods to classify access requests based on authorization and authentication. Each access profile is associated with a set of rules to manage the security of an organization. Access profiles helps the user to access the network devices through certain management methods like telnet, SSH, HTTP etc and they can be configured in access profiles

Applicable Devices

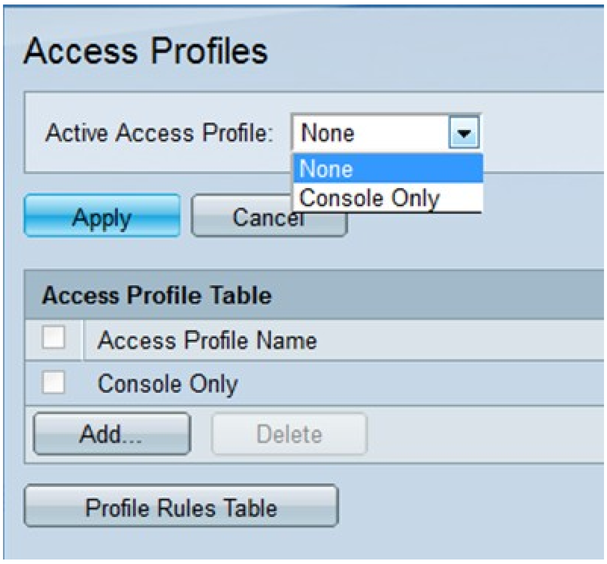
- Sx500 Series Stackable Switches

Software Version

- 1.3.0.62

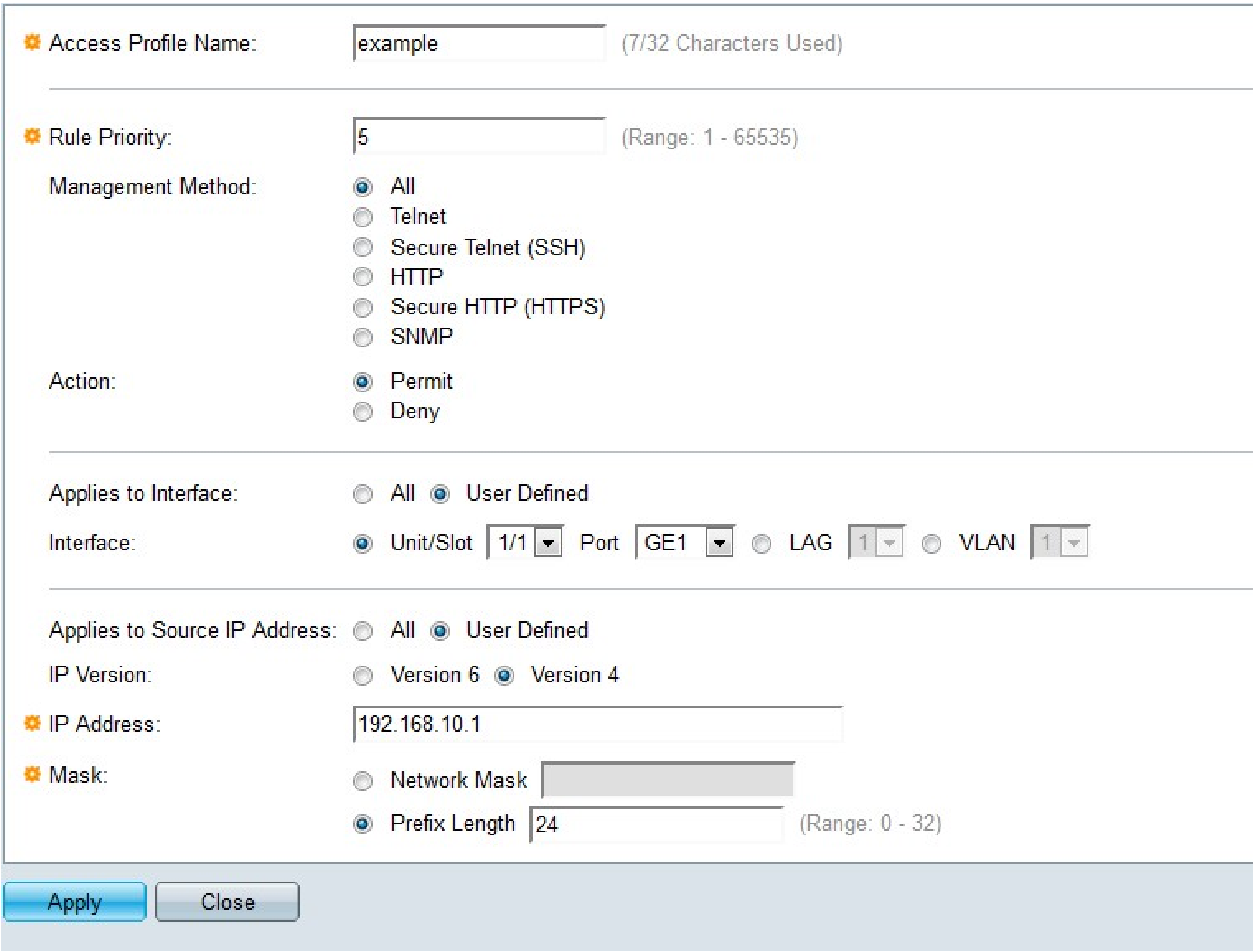
Access Profile Settings

Step 1. Log in to the web configuration utility and choose **Security > Mgmt Access Method > Access Profiles**. The *Access Profile* page opens:



Step 2. In the Active Access Profile field, choose one of the access profiles to be activated from the drop-down list.

Step 3. To add a new access profile, click **Add**. The *Add New Access Profile* window appears.



Access Profile Name: example (7/32 Characters Used)

Rule Priority: 5 (Range: 1 - 65535)

Management Method: ● All ○ Telnet ○ Secure Telnet (SSH) ○ HTTP ○ Secure HTTP (HTTPS) ○ SNMP

Action: ● Permit ○ Deny

Applies to Interface: ○ All ● User Defined

Interface: ● Unit/Slot 1/1 Port GE1 ○ LAG 1 ○ VLAN 1

Applies to Source IP Address: ○ All ● User Defined

IP Version: ○ Version 6 ● Version 4

IP Address: 192.168.10.1

Mask: ○ Network Mask ● Prefix Length 24 (Range: 0 - 32)

Step 4. In the Access Profile Name field, enter the desired name of the access profile.

Step 5. In the Rule Priority field, enter a rule priority number. It should be between 1 and 65535. The packet should match the rule for it to either grant or deny access to the switch.

Step 6. In the Management Method field, click the radio button for which the rule should be defined.

- All — This assigns the rule to all the management methods.

- Telnet — Access is either permitted or denied only to the users that meet the telnet access profile criteria.

- Secure telnet (SSH) — Access is either permitted or denied only to the users that meet the SSH access profile criteria.

- HTTP — Access is either permitted or denied only to the users that meet the HTTP access profile criteria.

- Secure HTTP (HTTPS) — Access is either permitted or denied only to the users that meet the HTTPS access profile criteria.

- SNMP — Access is either permitted or denied only to the users that meet the SNMP access profile criteria.

Step 7. In the Action field, click the radio button of the desired action.

- Permit — If the user settings match the profile settings then the access to the switch is permitted.

- Deny — If the user settings match the profile settings then the access to the switch is denied.

Step 8. In the Applies to Interface field, click the radio button of the interface attached to the rule.

- All — Rule is valid for all the ports, VLANs and LAGs

- User Defined — Rule is only be valid for selected interfaces.

Note: If you choose User Defined in Step 8 proceed with Step 9, otherwise skip to Step 10.

Step 9. In the Interface field, click the radio button for the desired interface.

Step 10. In the Applies to Source IP Address field, click the radio button of the type of source IP address to which the access profile applies.

- All — It is valid for all types of IP addresses.

- User Defined — It is valid for only user defined IP addresses.

Step 11. In the IP Version field, click the radio button of the supported IP version of the source address.

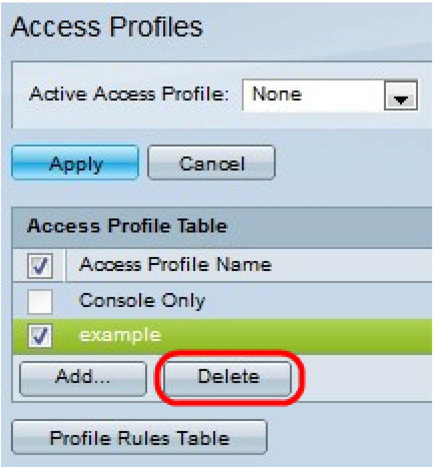
Step 12. In the IP Address field, enter the source IP address.

Step 13. In the Mask field, click the radio button of the desired format of the subnet mask.

- Network Mask — Enter the subnet mask in the 255.255.255.0 format.

- Prefix length — Enter the number of network bits that are comprised in the source IP address.

Step 14. Click **Apply** to save the configuration.



Access Profiles

Active Access Profile: None

Access Profile Table

☑	Access Profile Name
□	Console Only
☑	example

Step 15. (Optional) To delete an access profile, click the desired check box and click **Delete**.

Note: The Profile Rules Table allows you to edit the access profiles, refer to article *Management Access Method Profile Rules Configuration on Sx500 Series Stackable Switches*.