Access Profile Rules Configuration on 200/300 Series Managed Switches

Objectives

Access profile acts as another layer of security for the switch. Access profiles can contain up to 128 rules to increase security. Each rule contains an action and a criteria. If the access method does not match the management method, the user is blocked and cannot access the switch.

This article explains how to configure profile rules on the 200/300 Series Managed Switches.

Applicable Devices

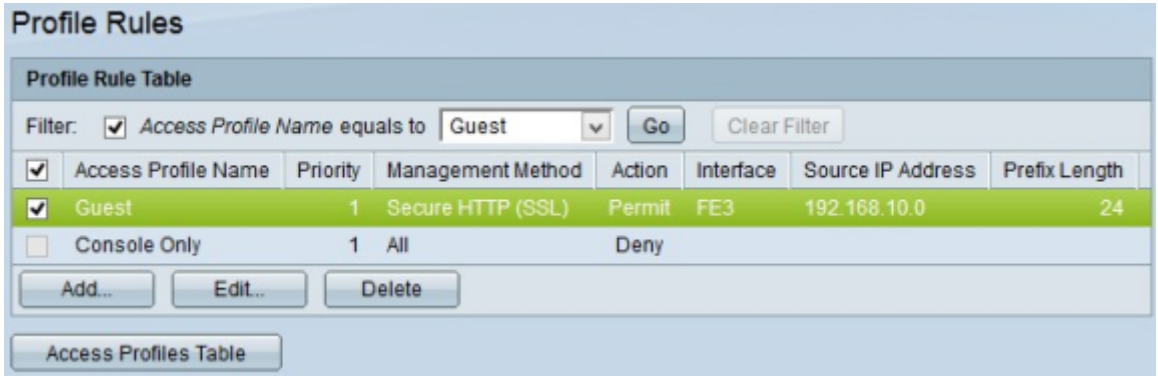
- SF/SG 200 and SF/SG 300 Series Managed Switches

Software Version

- v1.2.7.76

Access Profiles Configuration

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



Step 2. Check the **Filter** check box to display the Access Profile Name that has been created in the *Access Profile* page.

Step 3. Choose the desired access profile from the Access Profile Name equals to drop-down list.

Step 4. Click **Go** to display the desired access profile.

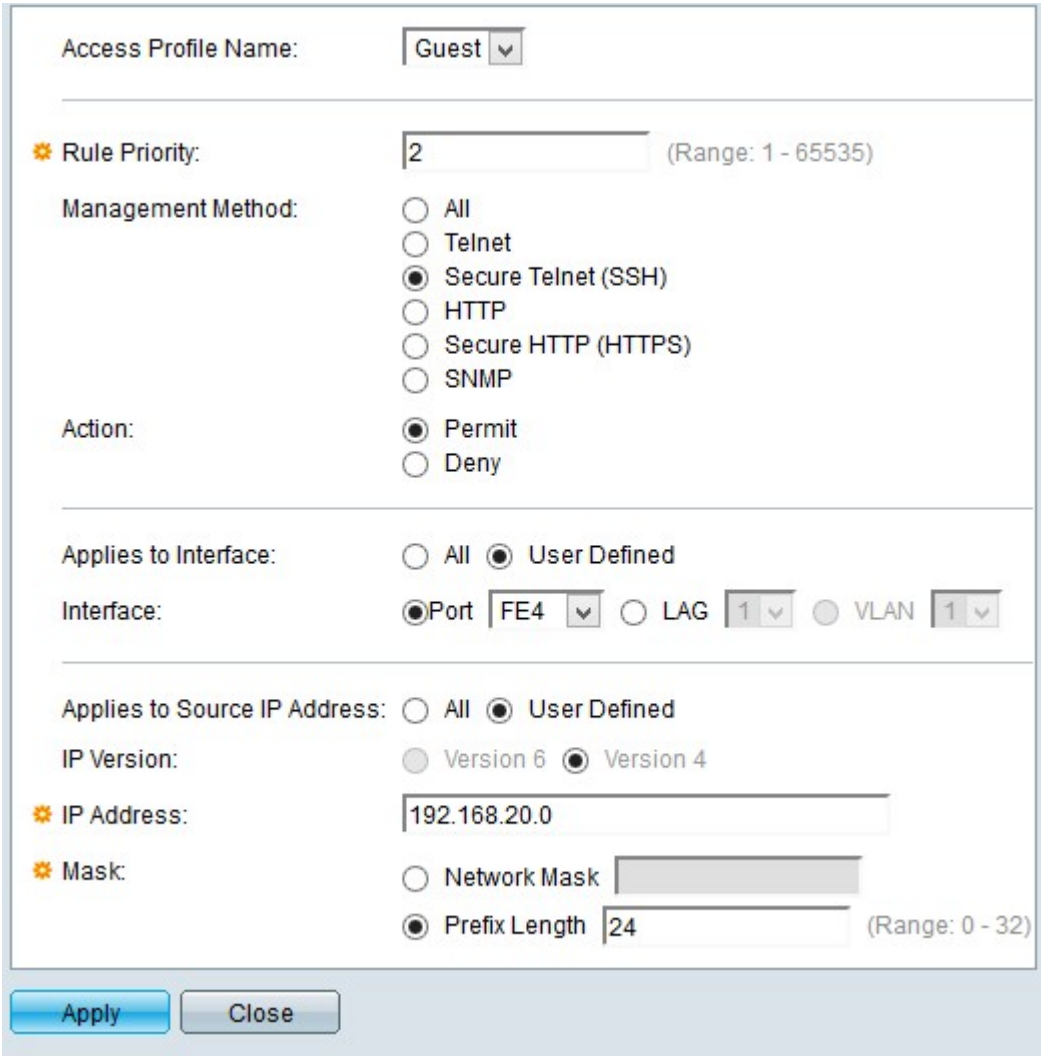
Step 5. (Optional) To start a new search, click **Clear Filter**.

Add a Profile Rule

Step 1. Check the check box that corresponds to the access profile that you would like to

add a rule.

Step 2. Click **Add**. The *Add Profile Rule* window appears.



Step 3. (Optional) To add a profile rule to a different profile name, choose the different profile name from the Access Profile Name drop-down list.

Step 4. Enter the priority of the rule in the Rule Priority field. The rule priority matches packets with rules. Rules with lower priority are checked first. If a packet matches a rule the desired action is performed.

Step 5. Click the radio button that corresponds to the desired management method in the Management Method field. The access method used by the user must match the management method for the action to be performed.

- All — All management methods are assigned to the access profile.
- Telnet — Telnet management method is assigned to the rule. Only users with a Telnet meeting access profile method have access to the device.
- Secure Telnet (SSH) — SSH management method is assigned to the profile. Only users with a Secure Telnet meeting access profile have access to the device.
- HTTP — HTTP management method is assigned to the profile. Users only with HTTP meeting access profile method have access to the device.

• Secure HTTP (SSL) — HTTPS management method is assigned to the profile. Users only with HTTPS meeting access profile method have access to the device.

• SNMP — SNMP management method is assigned to the profile. Users only with SNMP meeting access profile method have access to the device.

Step 6. Choose the action to be attached to the rule from the Action radio buttons. The possible action values are:

• Permit — Access to the switch is permitted.

• Deny — Access to the switch is denied.

Step 7. Click the desired radio button that corresponds to the desired interface type in the Applies to Interface field to define the interface for the access profile.

• All — Includes all the interfaces such as ports, VLANs and LAGs.

Note: LAGs are logical links that combines multiple physical links in order to provide more bandwidth.

• User Defined — Apply only to the desired interface for the user.

– Port — Choose the port From the Port drop-down list for which the access profile is to be defined.

– LAG — Choose the LAG from the LAG drop-down list for which the access profile is to be defined from the LAG drop-down list.

– VLAN — Choose the VLAN from the VLAN drop-down list for which the access profile is to be defined from the VLAN drop-down list.

Step 8. Click the **Source IP Address** radio button to enable the interface source IP address. There are two possible values:

• All — Includes all IP addresses.

• User Defined — Apply only to the desired IP address for the user.

– Version 6 — For IP version 6 addresses.

– Version 4 — For IP version 4 addresses.

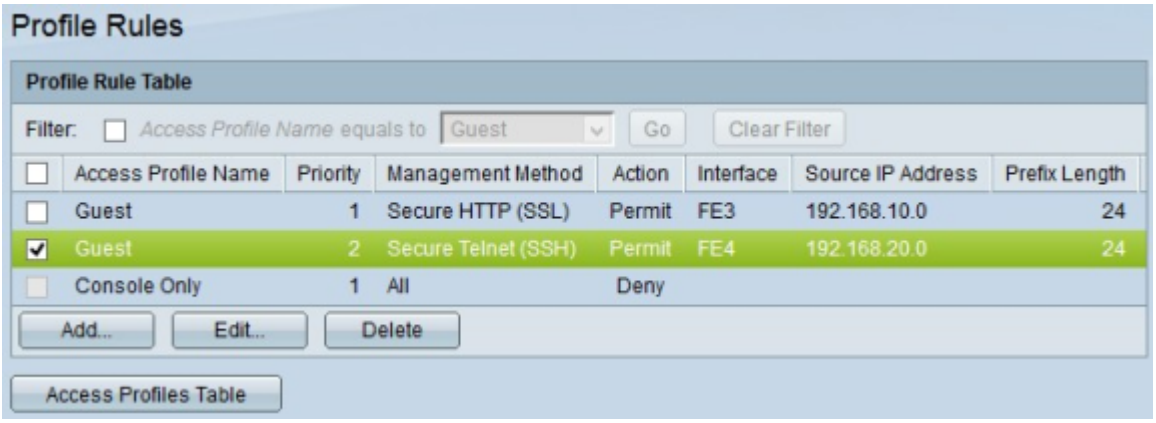
Step 9. If you chose User Defined in Step 7, enter the IP Address of the device in the IP Address field.

Step 10. Click a radio button in the Mask field of one of the options to define the network mask. The available options are:

• Network Mask — Enter the subnet mask that corresponds to the IP address in the dotted decimal format.

• Prefix Length — Enter the subnet mask prefix length that corresponds to the IP address.

Step 11. Click **Apply**.



Step 12. (Optional) To edit a current access profile, check the check box of the access profile name you wish to edit, and click **Edit**.

Step 13. (Optional) To delete an access profile, check the check box of the access profile you wish to delete, and click **Delete**.