Manage System Logs on the 200/300 Series Managed Switches

Objective

System logs give information about the different events that occurs that the switch saves. System logs can be used in case of a failure in the switch; you can track down the different events in the logs and see where and when the failure occurs. This article explain how to manage the system logs on the 200/300 Series Managed Switches.

Applicable Devices

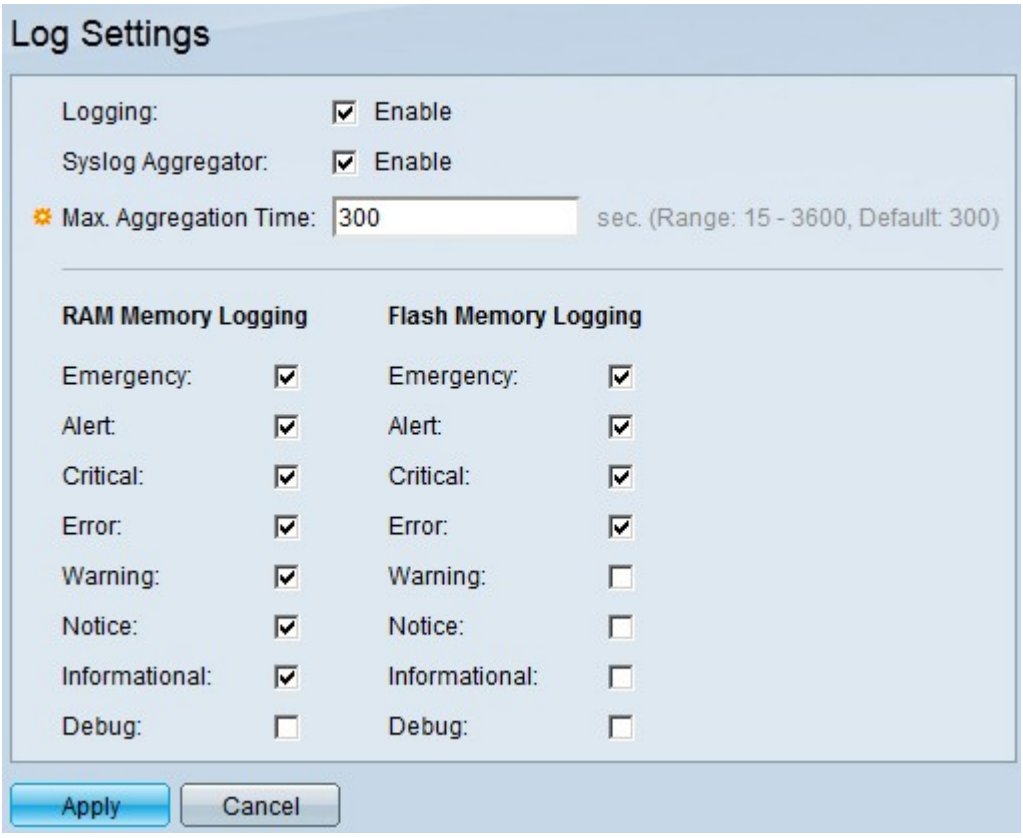
SF/SG 200 and SF/SG 300 Series Managed Switches

Software Version

• 1.3.0.62

System Log Setup

Step 1. Log in to the web configuration utility and choose **Administration > System Log > Log Settings**. The *System Logs Settings* page opens:



Step 2. In the Logging field, check the **Enable** check box to enable system logs.

Step 3. (Optional) In the Syslog Aggregator field, check the **Enable** check box to enable syslog aggregator. A Syslog Aggregator adds identical and contiguous syslog messages and

traps according to the specific Max Aggregation Time value and sends it in a single message.

Step 4. If syslog aggregator is enabled, in the Max Aggregation Time field, enter the time in seconds the syslog aggregator will accumulate syslog messages to be sent as a single message.

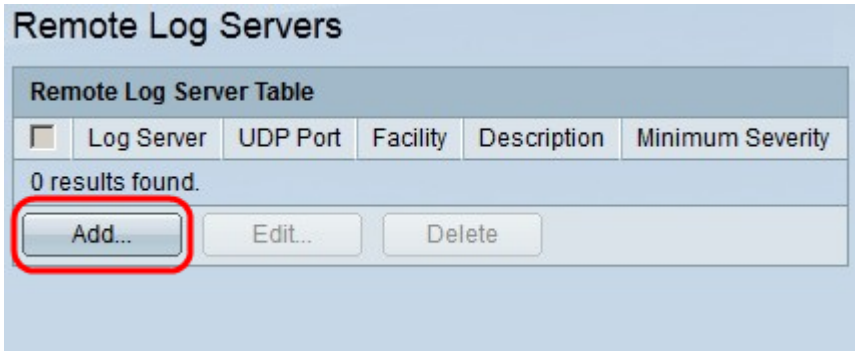
Step 4. The switch keeps information about its events in two places: in RAM memory, and in Flash memory. Under RAM Memory Logging and Flash Memory Logging, check the appropriate check boxes respectively:

- Emergency — The system is not usable.
- Alert — Action is needed.
- Critical — System is in critical condition.
- Error — A system error has occurred.
- Warning — A current or potential system condition has generated a warning.
- Notice — The system is functioning properly, but a system notice has been generated.
- Informational — General system and functional information.
- Debug — Provides extremely detailed information about system events.

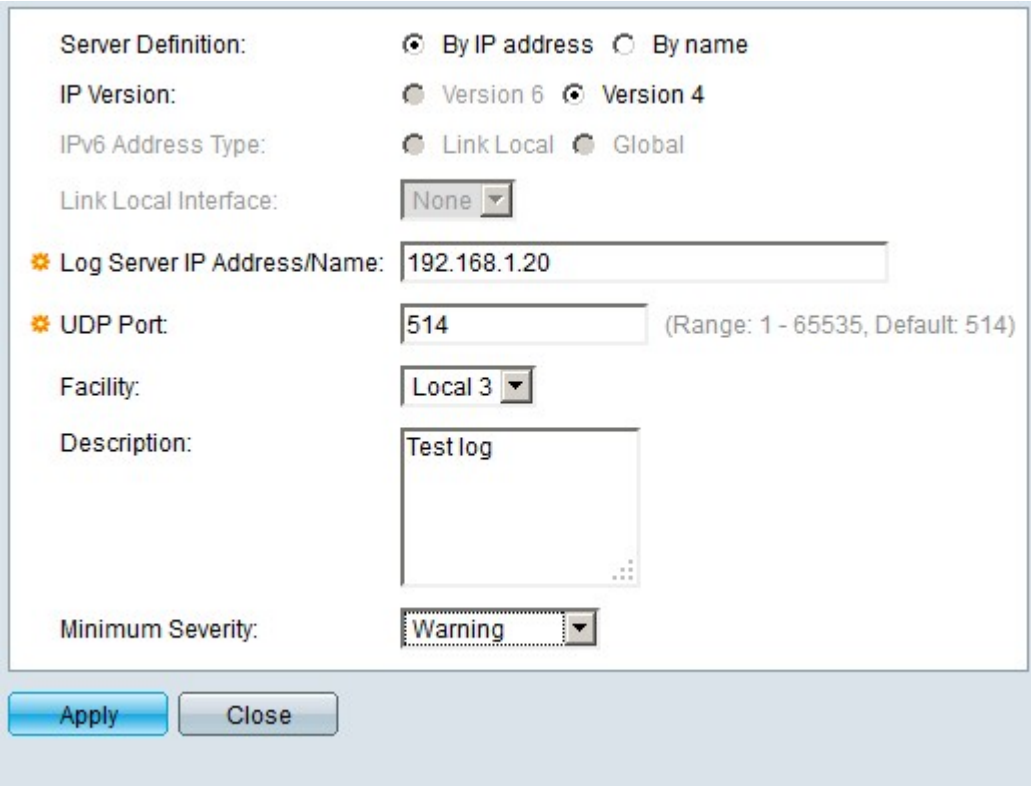
Step 5. Click **Apply**.

Remote Log Servers Setup

Step 1. Log in to the web configuration utility and choose **Administration > system log > Remote Log Servers**. The *Remote Log Server* page opens:



2. Click **Add** to set up a remote log server. The *Add Remote Log Server* window appears.



Step 3. In the Server Definition field, click one of the following radio buttons:

- By Name — The log server is defined with a name.
- By IP Address — The log server is defined with an IP address.

Step 4. In the IP Version field, click Version 6 or Version 4 as the type of IP address of the Log server.

Step 5. If Version 6 is chosen as the IP address in Step 4, in the IPv6 address type, click one of the following radio buttons:

- Link Local — An IPv6 address that only identifies hosts on a single network link.
- Global — an IPv6 address that is reachable from other networks.

Step 6. If Link Local is chosen as the IPv6 address type in Step 5, in the Link Local Interface drop-down list, choose the appropriate interface.

Step 7. In the Log Server IP address/Name field, enter the appropriate IP address or name that identifies the log server.

Step 8. In the Facility drop-down list, choose the facility value from which the log messages are sent to the remote server. The facility value indicates where the system log message originated from.

Step 9. (Optional) In the Description field, enter a description of the log server.

Step 10. In the Minimum Severity drop-down list, choose the minimum severity level of the system log messages that are sent to the server. The severity level indicates the type of log message.

Step 11. Click **Apply**.

Step 12. (Optional) To edit the settings of a remote log server, check the check box of the remote log server and click **Edit**.

Step 13. (Optional) To delete the settings of a remote log server, check the check box of the remote log server and click **Delete**.