# Cisco Meraki - Configuring a Syslog Server

## Method 1: Using GUI

### Configure log forwarding

1. Sign in to the **Meraki Dashboard** with administrator permissions.
2. If your account is a member of multiple organizations, select the organization that you want to configure in the **Organization** list.
3. In the **Network** list, select the network that you want to configure.
4. In the navigation menu, click **Network-wide** > **Configure** > **General**.
5. In the **Reporting** section, click **Add a syslog server**.
6. In the **Syslog servers** table, configure these settings:
    - **Server IP** - Enter the IP address of your Syslog Server.
    - **Port** - the default UDP port value of 514.
    - **Roles** - Select **Security events**, **Flows**, and **URL**.
7. In the **Traffic Analysis** section, select **Detailed: collect destination hostnames**.
8. Click **Save**.
9. In the navigation menu, click **Security & SD-WAN > Firewall**.
10. In the **Layer 3** section, mark the **Syslog** checkbox for every rule.
11. Click **Save**.

## Method 2 : Linux System

### Step 1:  Install the syslog application:

sysadmin@ubuntu:~$ **sudo apt-get install syslog-ng**

Once syslog-ng has been installed it needs to be configured to receive log messages from the MX. These instructions will configure syslog-ng to store each of the role categories in their own log file. There will be an individual log file for URLs, Event Logs, etc.  Alternatively, it could be configured to store all logs in one file.  Use any appropriate editor to make changes to the syslog-ng configuration file.  In this example nano is used to edit the file.

sysadmin@ubuntu:~$ **sudo nano /etc/syslog-ng/syslog-ng.conf**

The LAN IP of the MX in this example will be 192.168.10.1. The syslog server is listening on 192.168.10.241 UDP port 514. Update as needed to reflect the LAN IP of the MX and the syslog server being configured.  The first section of code will configure all syslog messages from the MX to be stored in /var/log/meraki.log.  The second section of code will use regular expressions to match each of the role categories and store them in individual log files.  Only one of the options needs to be configured.

## Step 2: Log all messages to /var/log/meraki.log:

#define syslog source

**source s_net { udp(ip(192.168.10.241) port(514)); };**

#create filter to match traffic (this filter will catch all syslog messages that come from the MX

**filter f_meraki { host( "192.168.10.1" ); };**

#define a destination for the syslog messages

**destination df_meraki { file("/var/log/meraki.log"); };**

#bundle the source, filter, and destination rules together with a logging rule

**log { source ( s_net ); filter( f_meraki ); destination ( df_meraki ); };**

## Step 3: Restart the syslog-ng process:

sysadmin@ubuntu:~$ **sudo /etc/init.d/syslog-ng restart**

*Source:*
*https://documentation.meraki.com/General_Administration/Monitoring_and_Reporting/Syslog_Server_Overview_and_Configuration#Configuring_a_Syslog_Server*

# Cisco Meraki - Configuring a Syslog Server Integration Procedures

Please provide the following information to CyTech:

Requirements:Collect logs via syslog over UDP or TCP

*Listen Address-> Syslog Collector IP address where the Elastic-Agent is installed
*Listen Port-> Port Number (Please identify if TCP or UDP)

If you need further assistance, kindly contact our support at **support@cytechint.com** for prompt assistance and guidance.

---

Revision #6
Created 16 January 2025 07:44:38 by Richmond Abella
Updated 17 January 2025 09:45:21 by Richmond Abella