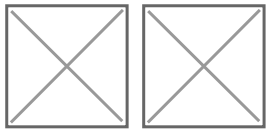
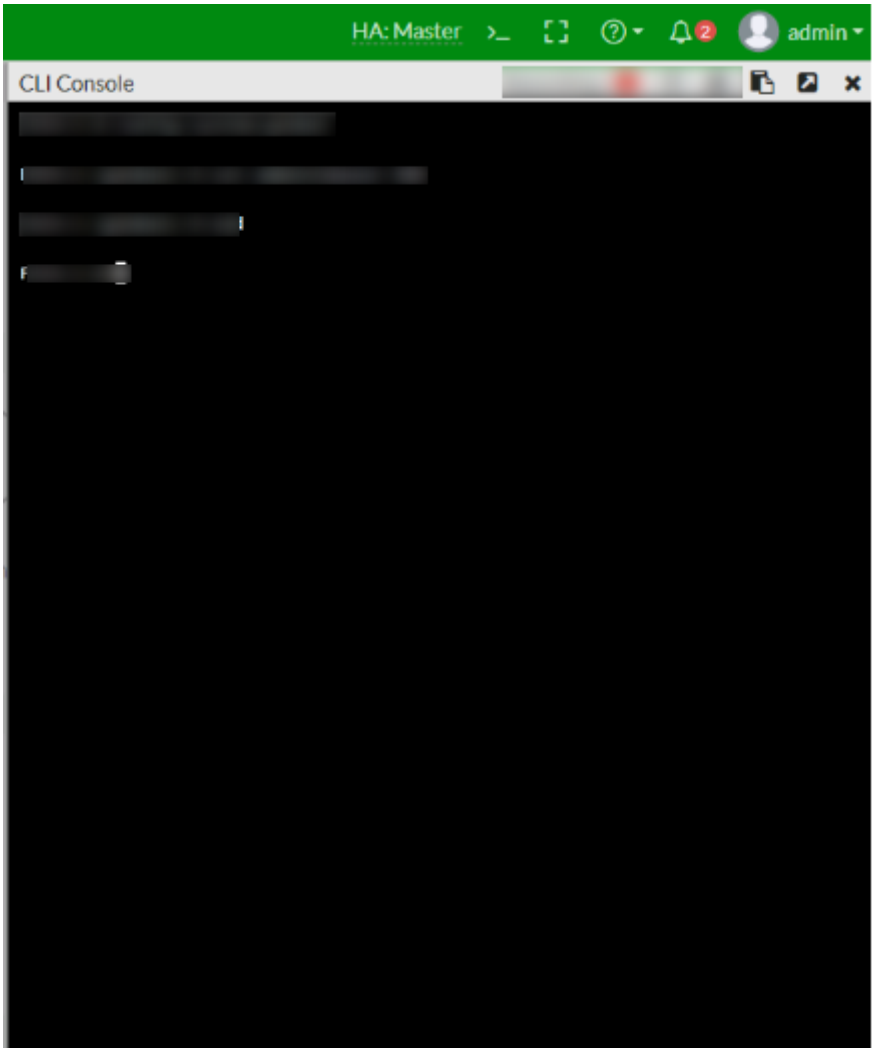
AQUILA - Fortinet FortiGate Integration

Please follow these instructions:

Step 1: Log in to your Fortinet FortiGate Admin portal and navigate to CLI console. Please refer to the images below.



Step 2: In your CLI Console execute these commands.



To configure FortiGate to send logs to the syslog server, we need you to provide the following details:

1. **Server IP(Log Collector - Elastic Agent Host)** – This is the IP address of your remote syslog server where the logs will be sent.
2. **Source IP(Fortinet FortiGate Device)**– This is the specific IP address on the FortiGate device that will be used to send the logs.

Since these values depend on your network setup, we require you to provide them so we can proceed with the configuration.
Please execute these commands.

For Syslog Setting:

```
config log syslogd setting
    set status enable
    set server <Address of remote syslog server - Log Collector>
    set facility user
    set source-ip <Source IP address of syslog - Fortinate Device>
    set port 10514
    set mode tcp
    set format default
end
```

We recommend using port 10514 if 514 is already used.
For Syslog Filter:

```
config log syslogd filter
    set anomaly enable
    set forward-traffic enable
    set local-traffic enable
    set multicast-traffic disable
    set netscan-discovery enable
    set netscan-vulnerability enable
    set severity warning
    set sniffer-traffic enable
    set voip disable
    set ztna-traffic enable
end
```

NOTE: In your **Server IP**, please allow inbound and outbound for the specified **Port** and **Protocol**. For the **Source IP**, allow the outbound for the specified **Port** and **Protocol**.

Important!!
Please provide screenshots of the configurations after executing the commands.
For our integration we need the Server IP and Port number.

*****Please provide screenshots of the configurations after executing the commands.**
For our integration we need the Server IP and Port number.

Source Link for full Documentation Manual:

https://docs.cytechint.io/books/system-integrations/page/fortinet-fortigate-syslog-setting-and-syslog-filter

Source Link Documentation for Syslog Setting:

https://docs.fortinet.com/document/fortigate/6.4.4/cli-reference/444620/config-log-syslogd-setting:

Source Link Documentation for Syslog Filter:

https://docs.fortinet.com/document/fortigate/7.0.9/cli-reference/456620/config-log-syslogd-filter

https://help.fortinet.com/fgt/handbook/cli52_html/index.html#page/FortiOS%205.2%20CLI/config_log.16.17.html

Source link to better understand Log Priority Level:

https://help.fortinet.com/fweb/551/log/Content/FortiWeb/fortiweb-log/Priority_level.htm

---

Revision #7
Created 26 February 2025 07:32:39 by Richmond Abella
Updated 18 June 2026 11:42:53 by Richmond Abella