



## Purpose

This document describes how to configure Mac OS X to send logs to Nagios Log Server.

## Target Audience

This document is intended for use by Nagios Log Server Administrators who wish to configure Mac OS X to send logs to Nagios Log Server.

## Overview

The steps for receiving logs from Mac OS X are quite simple, you only need to add a line to a configuration file and restart a service. Nagios Log Server does not require any additional configuration, it is ready to receive logs from Mac OS X out of the box.

## Configure Mac OS X

On your Mac OS X machine you will need to open the **Terminal** application (**Utilities > Terminal**).

Once in the terminal execute the following command to edit the `/etc/syslog.conf` file:

```
vi /etc/syslog.conf
```

You will be prompted to provide your password to edit this file.

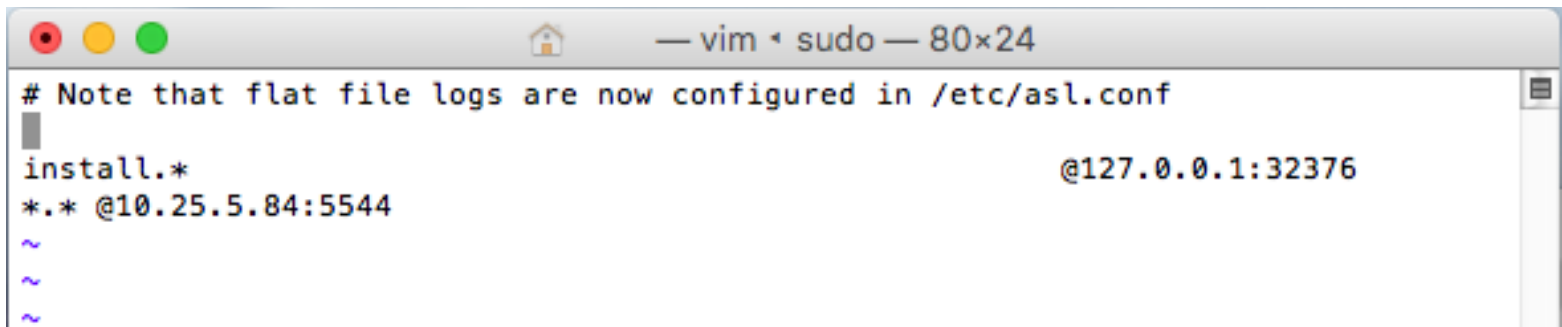
*When using the vi editor, to make changes press `i` on the keyboard first to enter insert mode. Press `Esc` to exit insert mode.*

## Nagios Log Server Sending Mac OS X Logs To Nagios Log Server

Add the following line to the end of the file, replacing `xxx.xxx.xxx.xxx` with the IP Address of your Nagios Log Server instance that will receive the logs:

```
*.* @xxx.xxx.xxx.xxx:5544
```

Here is an example of how it should look:



```
# Note that flat file logs are now configured in /etc/asl.conf
install.* @127.0.0.1:32376
*.* @10.25.5.84:5544
~
~
~
```

When you have finished, save the changes in vi by typing:

```
:wq
```

and press Enter.

The next step is to restart the `syslogd` daemon so the new configuration is applied and it starts sending logs to Nagios Log Server. Execute the following commands:

```
sudo launchctl stop com.apple.syslogd
sudo launchctl start com.apple.syslogd
```

There should be no output on the screen from executing these commands. Execute the following command to force a log entry to be sent to Nagios Log Server:

```
logger test
```

# Nagios Log Server

## Sending Mac OS X Logs To Nagios Log Server

### Verify Logs

In Nagios Log Server navigate to **Dashboards** and perform a query using the IP address of the Mac OS X machine:

The screenshot shows the Nagios Log Server web interface. The top navigation bar includes 'Home', 'Dashboards', 'Alerting', 'Configure', 'Help', and 'Admin'. A search bar is present with the text 'Search logs ...'. The user is logged in as 'nagiosadmin'.

The main content area shows a 'My Default Dashboard' with a query input field containing 'host:10.25.254.134'. Below the query is a 'FILTERING' section and an 'EVENTS OVER TIME' bar chart. The chart shows event counts over time for the specified host, with a peak around 18:09:30.

Below the chart is the 'ALL EVENTS' section, which displays a table of log entries. The table has columns for '@timestamp', 'host', 'type', 'message', and 'Actions'. The first three entries are visible:

@timestamp	host	type	message	Actions
2017-11-05T18:12:31.000+11:00	10.25.254.134	syslog	sample offset -0.000389 s @ 17.253.66.253	Q
2017-11-05T18:12:12.000+11:00	10.25.254.134	syslog	test	Q
2017-11-05T18:12:09.000+11:00	10.25.254.134	syslog	Process IPv6 address change: en0: 1	Q

In the screenshot above you can see the test log entry, this confirms that Nagios Log Server is receiving logs from the Mac OS X machine.

## Finishing Up

This completes the documentation on sending Mac OS X logs to Nagios Log Server.

If you have additional questions or other support related questions, please visit us at our Nagios Support Forums:

<https://support.nagios.com/forum>

The Nagios Support Knowledgebase is also a great support resource:

<https://support.nagios.com/kb>