API Log Fetch using Rest API Python Script

1. We require to setup 1 VM that act as a Log Forwarder to forward logs from Menlo MSIP to SIEM
2. The Log Forwarder can also setup with the same OS as the SIEM. No special config require as it would need to support the python software
3. Since the Log Forwarder only function is to execute the python script running
4. Require a token, require to log case to Menlo Support / created by Menlo Customer Success
5. The token would be generated based on your tenant and email address

You need to have Python and pip installed on the environment where you are running the script.

You would receive the error below if the python version installed is not correct

level=ERROR Error while writing the logs to the file logs.csv, error - Unicode-objects must be encoded before hashing

The command-line options are:

usage with python 2, using log\_fetch.py file:

log\_fetch.py [-h] [-o OUTPUT] [-d] [-s STARTTIME] [-e ENDTIME] [-f {CEF,JSON,KVP,CSV,LEEF}] [-t {‘web’,‘safemail’,‘audit’,‘smtp’,‘attachment’}] [-host HOST] [-a APPEND] token

usage with python 3, using log\_fetch\_py3.py file:

log\_fetch\_py3.py [-h] [-o OUTPUT] [-d] [-s STARTTIME] [-e ENDTIME] [-f {CEF,JSON,KVP,CSV,LEEF}] [-t {‘web’,‘safemail’,‘audit’,‘smtp’,‘attachment’}] [-host HOST] [-a APPEND] token

**Where**

-o output file name

-d debug mode

-s starttime using the format YYYYMMDDhhmmss UTC time zone

-e endtime using the format YYYYMMDDhhmmss UTC time zone

-f file format [CEF, JSON, KVP, CSV, LEEF]

-t type of logging [web, safemail, audit, smtp, attachment,dlp]

-host host to query for the logs

-a append a string to all log entries. Apply for KVP, CEF and LEEF format

token - this is a unique key for your tenant and user.

-q query value used for filtering

-h show help message

-l maximum number of events to receive each API call

1. The Log API key cannot be generated via the API Tokens screen in the Admin UI.
2. The key is generated by Customer Success, please raise a support ticket if you do not have a key.
3. The default filename is menlo\_logs.txt
4. If you do not specify an end-time it will default to the current time. We recommend that you ALWAYS specify an end time.
5. If you do not specify a start time it will default to 5 minutes before the end time.
6. If you do not specify a start and end time, it will default to 5 minutes from now.
7. If you are experiencing a 400 error, please ensure you have specified a start time or end time or both

Example Screen Shot

This is my secret token would be replaced with the token generated for you



