# mfe$_{s}aw$*Documentation*

***Release 0.0.7***

**Andy Walden**

**Nov 19, 2019**

# Contents

MFE_SAW is a wrapper around the McAfee ESM API versions 10.x and above.

Getting Started

# CHAPTER 1

## Migrated to https://github.com/mfesiem/msiempy

McAfee SIEM API Wrapper: MFE_SAW

MFE_SAW is a wrapper around the McAfee ESM API versions 10.x and above.

**It is time to SAW through repetitive SIEM tasks!**

This project aims to provide a basic API wrapper around the McAfee SIEM API to help make it more accessible to as many people as possible.

Whether it be to add the day's new datasources, querying the raw logs for 200 IP addresses for different date ranges or integrating a list of datasources that have been silent the past 24 hours into a report, when you're responsible for a repetitive task you should be spending your time automating, not repeating. It's time for MFE_SAW!

For SIEM operators, the project includes a CLI front end to automate tasks that would otherwise be time consuming or repetitive in the user interface.

For developers, this project attempts to provide a pythonic interface for specific aspects of the product including:

- ESM Monitoring
- Datasource Management (add, edit, del - including Client datasources)
- Simplified Query interface [TBD]
- Watchlist Operations [TBD]

The first target of this project is datasource management. With this library and accompanied front-end CLI interface, datasources can be easily added by putting a few details into a file and dropping into a directory. When the script runs, it will check the directory, validate the datasource and add it to the ESM. Client datasources are supported also.

dsconf/new_ds_cfg.txt

```
name=DC01_DNS
ip=10.10.1.34
rec_ip=172.16.15.10
type=linux
```

```
$ mfe_saw -a
DataSource successfully added: DC01_DNS
```

```
```

For the developers, here is another example:

```
>>> from mfe_saw.esm import ESM
    >>> from mfe_saw.datasource import DataSource, DevTree
    >>> esm = ESM()
    >>> esm.login('10.10.22.60', 'NGCP', 'password')
    >>> esm.time()
    '2017-07-25T13:32:57.0+0000'
    >>> tree = DevTree()
    >>> len(tree)
    1738
    >>> 'testbox-1' in tree
    True
    >>> tree.search('testbox-1')
{"ds_id": "1441195861726996 48", "child_enabled": "false", "child_count": "0", "child_
↪type": "0", "zone_id": "0", "url": null, "enabled": "T", "idm_id": "0", "hostname":
↪"", "tz_id": "", "dorder": null, "maskflag": null, "port": "", "syslog_tls": "F",
↪"vendor": "InterSect Alliance", "model": "Snare for Windows", "client_groups": "0",
↪"desc_id": "256", "name": "testbox-1", "ds_ip": "10.10.23.17", "type_id": "0",
↪"date_order": "", "zone_name": "", "client": true, "parent_id": "144119586172698624
↪", "idx": 1691, "desc": "client", "parameters": [{"desc_id": "256", "hostname": "",
↪"vendor": "InterSect Alliance", "model": "Snare for Windows", "tz_id": "", "date_
↪order": "", "port": "", "syslog_tls": "F", "client_groups": "0", "zone_name": "",
↪"client": true, "idx": 1691, "desc": "client"}]}
    >>>
    >>> testbox1 = tree.search('testbox-1')
    >>> type(testbox1)
    <class 'mfe_saw.datasource.DataSource'>
    >>> testbox1.delete()
    >>> tree.refresh()
    >>> tree.search('testbox-1')
    >>> 'testbox-1' in tree
    False
    >>> len(tree)
    1737
```

## 1.1 Feature Support

- Pythonic implementation
- Authentication and session tracking across objects
- Built-in multiprocessing for high performance
- Pass through of native API methods
- CLI interface
- Get info for existing datasources
- Add new datasources
- ESM status methods
- More to come!

mfe_saw officially supports Python 3.3–3.7 on Windows and Linux.

## 1.2 Installation

To install MFE_SAW, use pip:

```
$ pip install mfe_saw
```

## 1.3 Documentation

Documentation is available at http://mfe-saw.readthedocs.io/en/latest/index.html

## 1.4 Disclaimer

_Note: This is an **UNOFFICIAL** project and is **NOT** sponsored or supported by **McAfee, Inc**. If you accidentally delete all of your datasources, don't call support (or me). Product access will always be limited to 'safe' methods and with respect to McAfee's intellectual property. This project is released under the [ISC license](https://en.wikipedia.org/wiki/ISC_license), which is a permissive free software license published by the Internet Systems Consortium (ISC) and without warranty._

CHAPTER 2

# Installation

At the command line:

```
$ easy_install mfe_saw
```

Or, if you have virtualenvwrapper installed:

```
$ mkvirtualenv mfe_saw
$ pip install mfe_saw
```

CHAPTER 3

# CLI Guide

```
$ mfe_saw -h
```

CHAPTER 4

# API Reference

## 4.1 Structure

**Objects**

- ESM
- DataSource
- DevTree
- Query
- Watchlist