

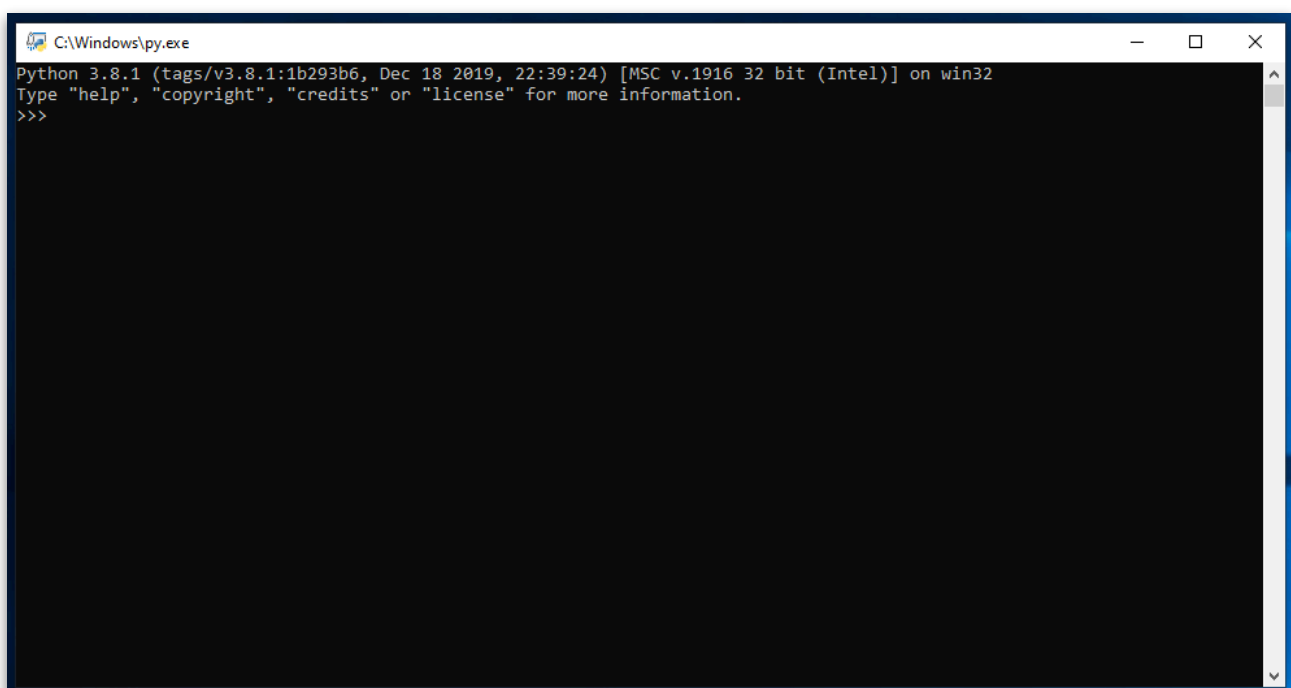
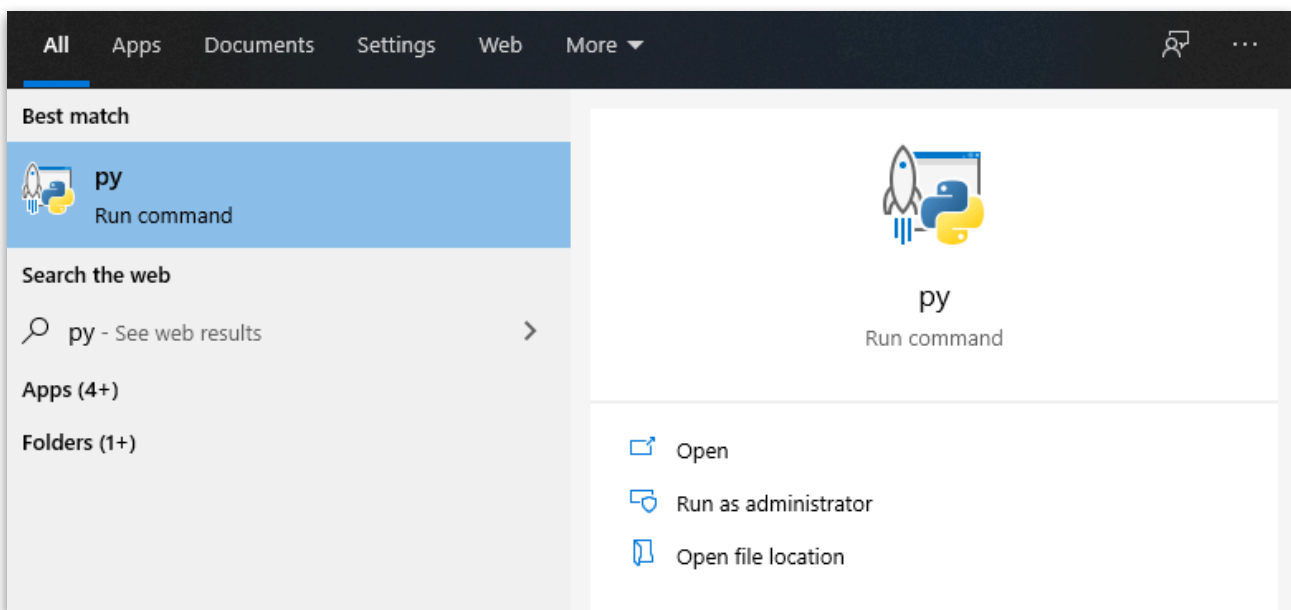
Sophos Central

Turn on Tamper Protection

The script will check turn on Tamper on all machine where it has been disabled

IT WILL NOT OVERRIDE TAMPER BEING TURNED OFF VIA GLOBAL SETTINGS

- Install Python. Follow the Python install guide provided for your OS
- Check you have requests installed
- Open Py.exe on Windows or use the Terminal on a Mac



- Type - help('modules'). This will list all the modules installed

```

C:\Windows\py.exe
0
>>> help('modules')

Please wait a moment while I gather a list of all available modules...

_future_      _tkinter      getpass       sched
__abc__       _tracemalloc  gettext       secrets
__ast__       _warnings    glob          select
__asyncio__   _weakref     gzip          selectors
__bisect__    _weakrefset  hashlib       setuputils
__blake2__    _winapi      heapq         shelve
__bootlocale__ _xxsubinterpreters hmac          shlex
__bz2__       abc          html          shutil
__codecs__    aifc         http          signal
__codecs_cn__ antigravity  idlelib       site
__codecs_hk__ argparse    imaplib       smtpd
__codecs_iso2022 array        imgchr        smtpplib
__codecs_jp__ ast          importlib     socket
__codecs_kr__ asynchat     inspect       socketserver
__codecs_tw__ asyncio     io            sqlite3
__collections__ atexit       ipaddress     sre_compile
__compat_pickle__ audioop      itertools     sre_constants
__compression__ base64       json          sre_parse
__contextvars__ bdb          keyword       ssl
__csv__       binascii     lib2to3       stat
__ctypes__    binhex       linecache     statistics
__ctypes_test__ bisect       locale        string
__datetime__  builtins     logging       stringprep
__decimal__   bz2          lzma          struct
__dummy_thread__ cProfile     mailbox        subprocess
__elementtree__ calendar    mailcap        sunau
__functools__ cgi          marshal        symbol
__hashlib__   cgiitb       math           symtable
__heapq__     chunk        mimetypes      sys
__imp__       cmath        mmap           sysconfig
__io__        cmd          modulefinder  tabnanny
__json__      code         msilib         tarfile
__locale__    codecs       msvcrt         telnetlib
__lsprof__    codeop       multiprocessing tempfile
__lzma__      collections  netrc          test
__markupbase__ colorsys     nntplib        textwrap
__md5__       compileall   nt             this
__msi__       concurrent  ntpath         threading
__multibytecodec configparser nturl2path     time
__multiprocessing__ contextlib    numbers        timeit
__opcode__    contextvars opcode         tkinter
__operator__  copy        operator       token
__osx_support__ copyreg     optparse       tokenize
__overlapped__ crypt       os             trace
__pickle__    csv         parser         traceback
__py_abc__    ctypes      pathlib        tracemalloc
__pydecimal__ curses      pickle         tty
__pyio__      dataclasses pickletools    turtle
__queue__     datetime   pip            turtledemo
__random__    dbm         pipes          types
__sha1__      decimal    pkg_resources typing
__sha256__    difflib    pkgutil        unicodedata
__sha3__      dis        platform       unittest
__sha512__    distutils  plistlib       urllib
__signal__    doctest    poplib         uu
__sitebuiltins__ dummy_threading posixpath      uuid
__socket__    easy_install pprint         venv
__sqlite3__   email      profile        warnings
__sre__       encodings  pstats         wave
__ssl__       ensurepip  pty            weakref
__stat__      enum       py_compile    webbrowser
__statistics__ errno      pycbr         winreg
__string__    faulthandler pydoc         winsound
__strptime__ filecmp    pydoc_data    wsgiref
__struct__    fnmatch   queue         xdrlib
__symtable__  formatter fractions  xmlrpc
__testbuffer__ fractions  quopri        xxsubtype
__testcapi__

_testconsole  ftplib      random       zipapp
__testimportmultiple__ functools   re           zipfile
__testmultiphase__ gc          reprlib     zipimport
__thread__     genericpath rlcompleter  zlib
__threading_local__ getopt      runpy

Enter any module name to get more help. Or, type "modules spam" to search
for modules whose name or summary contain the string "spam".

>>>

```

- Note csv and datetime are installed already. We will need to install some Modules

PC

- Open an Elevated Command Prompt

- Type - python -m pip install requests
- Note there is a module called request. We need requests

```

Command Prompt
Microsoft Windows [Version 10.0.18363.476]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\curtis.m>python -m pip install requests
Collecting requests
  Downloading https://files.pythonhosted.org/packages/51/bd/23c926cd341ea6b7dd0b2a00aba99ae0f828be89d72b2190f27c11d4b7fb/requests-2.22.0-py2.py3-none-any.whl (57kB)
    | 61kB 230kB/s
Collecting chardet<3.1.0,>=3.0.2 (from requests)
  Downloading https://files.pythonhosted.org/packages/bc/a9/01ffebfb562e4274b6487b4bb1ddec7ca55ec7510b22e4c51f14098443b8/chardet-3.0.4-py2.py3-none-any.whl (133kB)
    | 143kB 595kB/s
Collecting idna<2.9,>=2.5 (from requests)
  Downloading https://files.pythonhosted.org/packages/14/2c/cd551d81dbe15200be1cf41cd03869a46fe7226e7450af7a6545bfc474c9/idna-2.8-py2.py3-none-any.whl (58kB)
    | 61kB 2.0MB/s
Collecting urllib3!=1.25.0,!1.25.1,<1.26,>=1.21.1 (from requests)
  Downloading https://files.pythonhosted.org/packages/b4/40/a9837291310ee1ccc242ceb6ebfd9eb21539649f193a7c8c86ba15b98539/urllib3-1.25.7-py2.py3-none-any.whl (125kB)
    | 133kB 1.1MB/s
Collecting certifi>=2017.4.17 (from requests)
  Downloading https://files.pythonhosted.org/packages/b9/63/df50cac98ea0d5b006c55a399c3bf1db9da7b5a24de7890bc9cfd5dd9e99/certifi-2019.11.28-py2.py3-none-any.whl (156kB)
    | 163kB 1.1MB/s
Installing collected packages: chardet, idna, urllib3, certifi, requests
Successfully installed certifi-2019.11.28 chardet-3.0.4 idna-2.8 requests-2.22.0 urllib3-1.25.7
WARNING: You are using pip version 19.2.3, however version 19.3.1 is available.
You should consider upgrading via the 'python -m pip install --upgrade pip' command.

C:\Users\curtis.m>

```

Mac

- Open Terminal
- Type - python3 -m pip install requests. The 3 is important or it will install requests to version 2 of Python
- Note there is a module called request. We need requests

```

michaelcurtis@UK-GN-55185 ~ % python3 -m pip install requests
Collecting requests
  Using cached https://files.pythonhosted.org/packages/51/bd/23c926cd341ea6b7dd0b2a00aba99ae0f828be89d72b2190f27c11d4b7fb/requests-2.22.0-py2.py3-none-any.whl
Collecting certifi>=2017.4.17 (from requests)
  Using cached https://files.pythonhosted.org/packages/b9/63/df50cac98ea0d5b006c55a399c3bf1db9da7b5a24de7890bc9cfd5dd9e99/certifi-2019.11.28-py2.py3-none-any.whl
Collecting idna<2.9,>=2.5 (from requests)
  Using cached https://files.pythonhosted.org/packages/14/2c/cd551d81dbe15200be1cf41cd03869a46fe7226e7450af7a6545bfc474c9/idna-2.8-py2.py3-none-any.whl
Collecting chardet<3.1.0,>=3.0.2 (from requests)
  Using cached https://files.pythonhosted.org/packages/bc/a9/01ffebfb562e4274b6487b4bb1ddec7ca55ec7510b22e4c51f14098443b8/chardet-3.0.4-py2.py3-none-any.whl
Collecting urllib3!=1.25.0,!1.25.1,<1.26,>=1.21.1 (from requests)
  Using cached https://files.pythonhosted.org/packages/e8/74/6e4f91745020f967d09332bb2b8b9b10090957334692eb88ea4afe91b77f/urllib3-1.25.8-py2.py3-none-any.whl
Installing collected packages: certifi, idna, chardet, urllib3, requests
Successfully installed certifi-2019.11.28 chardet-3.0.4 idna-2.8 requests-2.22.0 urllib3-1.25.8
WARNING: You are using pip version 19.2.3, however version 20.0.2 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
michaelcurtis@UK-GN-55185 ~ %

```

- Note help('modules') now lists requests in the Python shell

```

testconsole      fractions        quopri           xmlrpc
testimportmultiple  ftplib          random           xsubdtype
testmultiphase    functools       re               zipapp
thread            gc              reprlib          zipfile
threading_local   genericpath     requests         zipimport
tkinter           getopt          rlcompleter      zlib

Enter any module name to get more help. Or, type "modules spam" to search
for modules whose name or summary contain the string "spam".

>>>

```

Sophos Central

- Log into Sophos Central. We will need to make our API credentials
- Click on Global Settings

SOPHOS
CENTRAL
Admin

Global Settings
Manage your settings

Overview

- Dashboard
- Alerts
- Threat Analysis Center
- Logs & Reports
- People
- Devices
- Global Settings**
- Protect Devices

Administration

- [AD Sync Settings/Status](#)
Manage Active Directory settings and view status.
- [Role Management](#)
Manage Administration Roles.
- [API Token Management](#)
Manage API tokens used for secure access to Sophos Central APIs.
- [API credentials](#)
Create and manage API credentials.
- [Federated Sign-in](#)
Federated Sign-in enables users to sign in with Microsoft credentials.

- Click API Credentials
- Click Add

Add credential ×

Credential name*

Script Access

Description

Script Access

Notes:

- Upon clicking the Add button, a Client ID and Client Secret will be generated.
- Credentials will expire in 36 months

Cancel Add

- Click show secret. Once you close this screen you won't be able to see this again. Record this information. You will need it for the config file

API credential summary

Name	Script Access
Created on	Feb 1, 2020
Expires on	Jan 31, 2023
Description	Script Access
Client ID	984bc1a1-02b6-44ff-89eb-6c1622c6cc2c Copy
Client Secret	Show Client Secret

Note: For security reasons, the Client Secret will only be shown one time. Click the Show Client Secret link only when you are ready to implement it.

- We now need to edit the console_tamper_config.config

[DEFAULT]

ClientID:<put clientID here>

ClientSecret:<put clientSecret here>

[REPORT]

ReportName:<put report name here>

ReportFilePath:<put file path here>

ConsoleName:<put console name here>

Example

[DEFAULT]

ClientID:33d15ef8-3274-075743e8ff2f

ClientSecret:d8a7160f094abb4bedb8f504891821129ca34989924cbdc37d2ef1cf7c4ef887

[REPORT]

ReportName:UK_PS_Health_

ReportFilePath:c:\users\michael\desktop\reports\

ConsoleName:UK PS South

- Make sure the config file is in the same folder as the script
- If the file was sent to you as a .txt file change it to .py

PC

- From the cmd run the Python script
 - python name_of_script.py

Mac

- From Terminal run the Python script
 - Python3 name_of_script.py