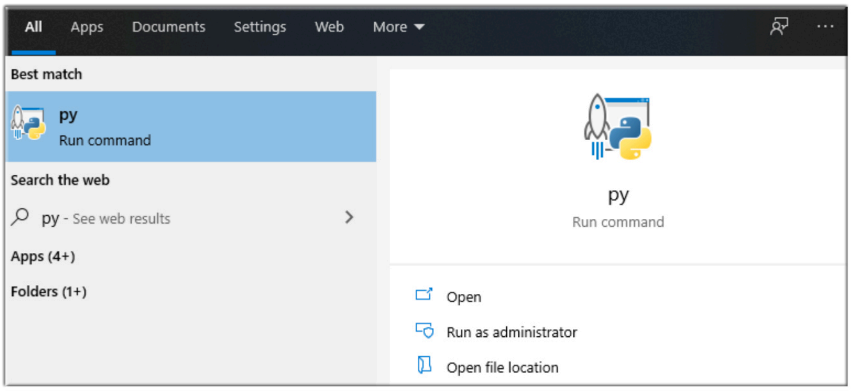
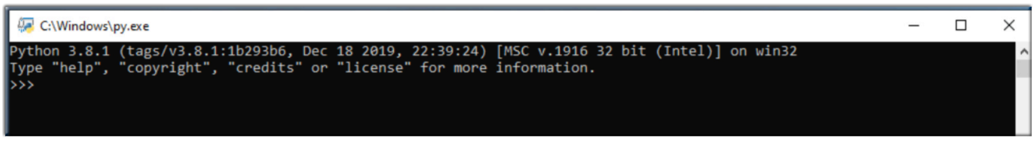
Sophos Central Health Report

The script will check the health of every Endpoint and Server in Sophos Central Console/Sophos Central Enterprise Dashboard or MSP

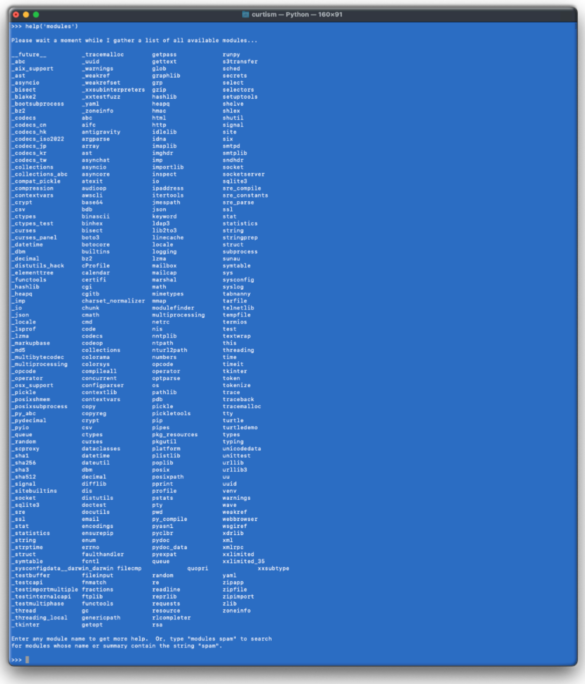
Make sure you have the ‘requests‘ module installed. To do this open py.exe (Windows) or Terminal on a Mac





```
Python 3.8.1 (tags/v3.8.1:1b293b6, Dec 18 2019, 22:39:24) [MSC v.1916 32 bit (Intel)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

Type, help(‘modules). This will list all the modules installed. Note csv and datetime are already installed. If ‘requests’ is not installed we will need to install it



```
>>> help('modules')

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

__future__          _tracemalloc        getpass             runpy
_abc                _uuid               gettext             s3transfer
_aix_support        _warnings           glob                sched
_ast                _weakref            graphlib            secrets
_asyncio            _weakrefset         grp                 select
_bisect             _xxsubinterpreters  gzip                selectors
_blake2             _xxtestfuzz         hashlib             setuptools
_bootsubprocess     _yaml               heapq               shelve
_bz2                _zoneinfo           hmac                shlex
_codecs             abc                 html                shutil
_codecs_cn          aifc                http                signal
_codecs_hk          antigravity         idlelib             site
_codecs_iso2022     argparse            idna                six
_codecs_jp          array               imaplib             smtpd
_codecs_kr          ast                 imghdr              smtplib
_codecs_tw          asynchat            imp                 sndhdr
_collections        asyncio             importlib           socket
_collections_abc    asyncore            inspect             socketserver
_compat_pickle      atexit              io                  sqlite3
_compression        audioop             ipaddress           sre_compile
_contextvars        awscli              itertools           sre_constants
_crypt              base64              jmespath            sre_parse
_csv                bdb                 json                ssl
_ctypes             binascii            keyword             stat
_ctypes_test        binhex              ldap3               statistics
_curses             bisect              lib2to3             string
_curses_panel       boto3               linecache           stringprep
_datetime           botocore            locale              struct
_dbm                builtins            logging             subprocess
_decimal            bz2                 lzma                sunau
_distutils_hack     cProfile            mailbox             symtable
_elementtree        calendar            mailcap             sys
_functools          certifi             marshal             sysconfig
_hashlib            cgi                 math                syslog
_heapq              cgitb               mimetypes           tabnanny
_imp                charset_normalizer  mmap                tarfile
_io                 chunk               modulefinder        telnetlib
_json               cmath               multiprocessing     tempfile
_locale             cmd                 netrc               termios
_lsprof             code                nis                 test
_lzma               codecs              nntplib             textwrap
_markupbase         codeop              ntpath              this
_md5                collections         nturl2path          threading
_multibytecodec     colorama            numbers             time
_multiprocessing    colorsys            opcode              timeit
_opcode             compileall          operator            tkinter
_operator           concurrent          optparse            token
_osx_support        configparser        os                  tokenize
_pickle             contextlib          pathlib             trace
_posixshmem         contextvars         pdb                 traceback
_posixsubprocess    copy                pickle              tracemalloc
_py_abc             copyreg             pickletools         tty
_pydecimal          crypt               pip                 turtle
_pyio               csv                 pipes               turtledemo
_queue              ctypes              pkg_resources       types
_random             curses              pkgutil             typing
_scproxy            dataclasses         platform            unicodedata
_sha1               datetime            plistlib            unittest
_sha256             dateutil            poplib              urllib
_sha3               dbm                 posix               urllib3
_sha512             decimal             posixpath           uu
_signal             difflib             pprint              uuid
_sitebuiltins       dis                 profile             venv
_socket             distutils           pstats              warnings
_sqlite3            doctest             pty                 wave
_sre                docutils            pwd                 weakref
_ssl                email               py_compile          webbrowser
_stat               encodings           pyasn1              wsgiref
_statistics         ensurepip           pyclbr              xdrlib
_string             enum                pydoc               xml
_strptime           errno               pydoc_data          xmlrpc
_struct             faulthandler        pyexpat             xxlimited
_symtable           fcntl               queue               xxlimited_35
_sysconfigdata__darwin_darwin filecmp             quopri              xxsubtype
_testbuffer         fileinput           random              yaml
_testcapi           fnmatch             re                  zipapp
_testimportmultiple fractions           readline            zipfile
_testinternalcapi   ftplib              reprlib             zipimport
_testmultiphase     functools           requests            zlib
_thread             gc                  resource            zoneinfo
_threading_local    genericpath         rlcompleter
_tkinter            getopt              rsa

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

>>> 
```

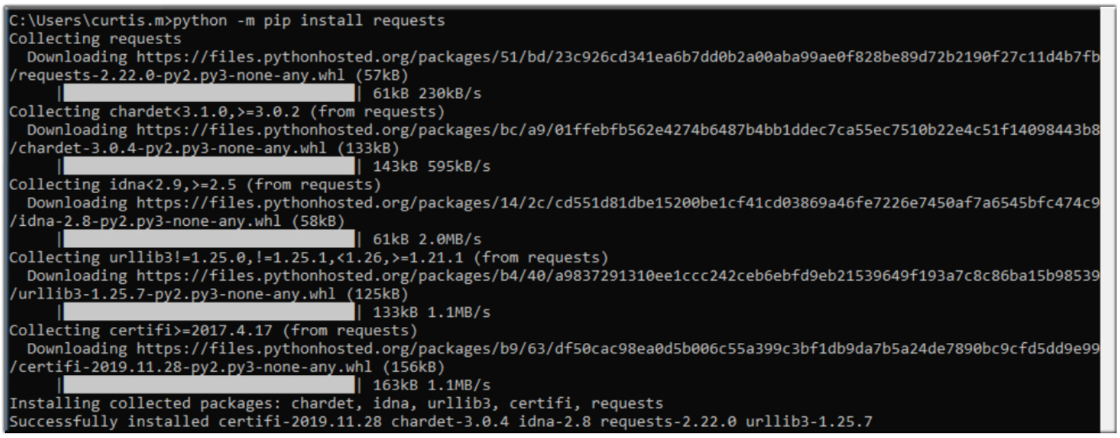
Install Modules

PC

Open an Elevated Command Prompt

Type - python -m pip install requests

Note there is a module called ‘request’. We need ‘requests’



```
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
```

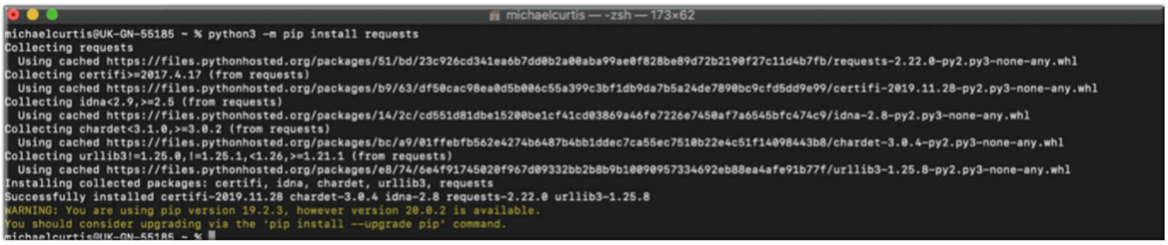
Mac

Open Terminal

Type - python3 -m pip install requests

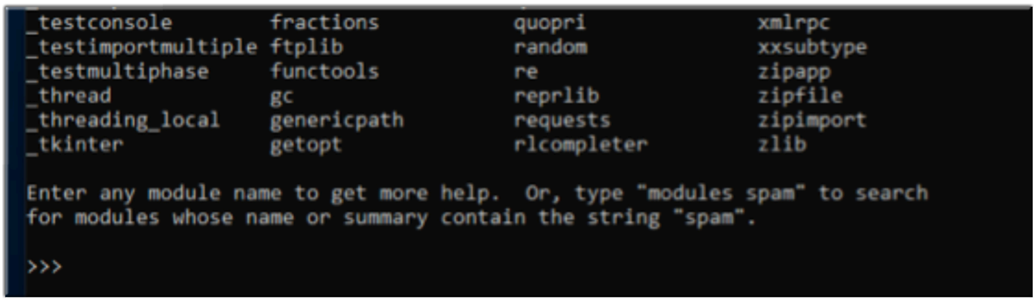
The 3 is important or it will install requests to version 2 of Python

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 ~ % 
```

Now rerun the help(‘modules') command. It now lists requests in the Python shell



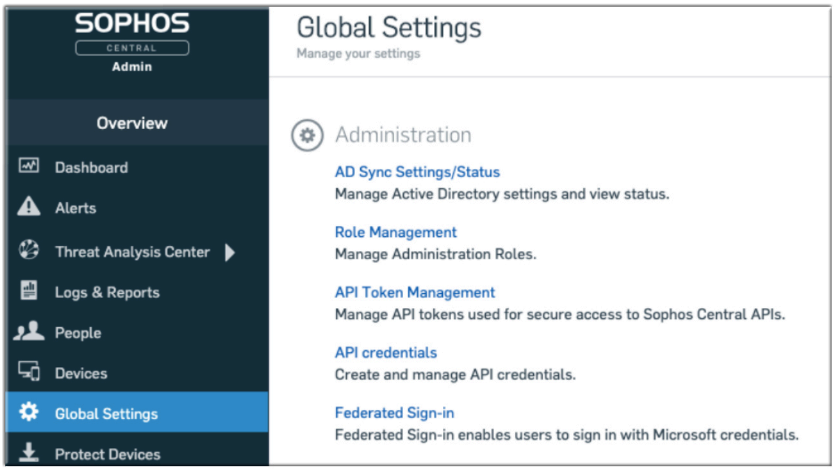
```
_testconsole        fractions           quopri              xmlrpc
_testimportmultiple ftplib              random              xxsubtype
_testmultiphase     functools           re                  zipapp
_thread             gc                  reprlib             zipfile
_threading_local    genericpath         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".

>>>
```

Setting Up Sophos Central API Keys

Log into Sophos Central. We will need to make our API credentials. Click on Global Settings. For Sophos Central Enterprise Dashboard it is under Settings & Policies



Global Settings

Manage your settings

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.

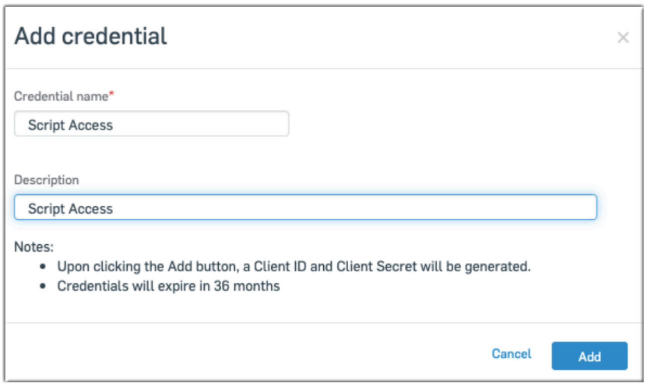
API credentials

Create and manage API credentials.

Federated Sign-in

Federated Sign-in enables users to sign in with Microsoft credentials.

Click API Credentials Management



Add credential

Credential name*: Script Access

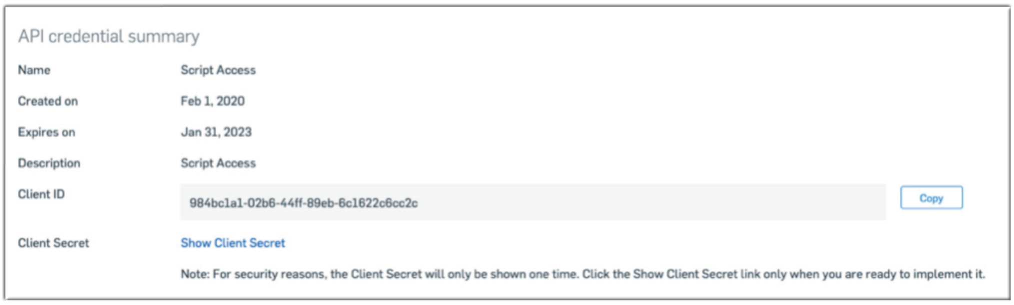
Description: Script Access

Notes:

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

Click show secret. Once you close this screen you won’t be able to see this again

Record this information. Store these keys in a password manager. 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
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 Sophos_Central_Health.config file. Do not leave the ClientSecret in the config file post testing. Leave it blank to be challenged when the script is run

Setting Up The Config File

```
[DEFAULT]
# Do not leave the ClientSecret in the config file
ClientID:<put clientID here>
ClientSecret:<put clientSecret here or leave blank to enter manually>

[REPORT]
ReportName:<put report name here>
ReportFilePath:<put file path here>

[EXTRA_FIELDS]
# 0 is off, 1 is ON
MAC_Address:0
Versions:0
Windows_Build_Version:1
Cloud_Servers:1
Include_Alerts:1
Full_Services_List:0
SplitEDBReports:0
IncludeSubEstateID:0
```

The [EXTRA_FIELDS] are used for the following functions

[EXTRA_FIELDS]

# 0 is off, 1 is ON	
MAC_Address:	Adds the computers MAC address to the report
Versions:	Adds the components versions to the report
Windows_Build_Version:	Adds the Windows build versions to the report
Cloud_Servers:	Adds the Azure, GCP or AWS ID to the report
Include_Alerts:	Adds the Alerts to the report
Full_Services_List:	List all services and their state to the report
SplitEDBReports:	Split sub estates into separate reports
IncludeSubEstateID:	Future use

Example

```
[DEFAULT]
# Do not leave the ClientSecret in the config file
ClientID:33d15ef8-3274-075743e8ff2f
ClientSecret:d8a7160f08211294989924cbdc37d2ef1cf7c4ef887

[REPORT]
ReportName:UK_PS_Health_
ReportFilePath:c:\users\michael\desktop\reports\

[EXTRA_FIELDS]
# 0 is off, 1 is ON
MAC_Address:0
Versions:0
Windows_Build_Version:1
Cloud_Servers:1
Include_Alerts:1
Full_Services_List:0
SplitEDBReports:0
IncludeSubEstateID:0
```

Running the script

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

On a PC run this command from within the folder with the scripts and config file

```
python Sophos_Central_Health.py
```

On a Mac run this command from within the folder with the scripts and config file

```
python3 Sophos_Central_Health.py
```