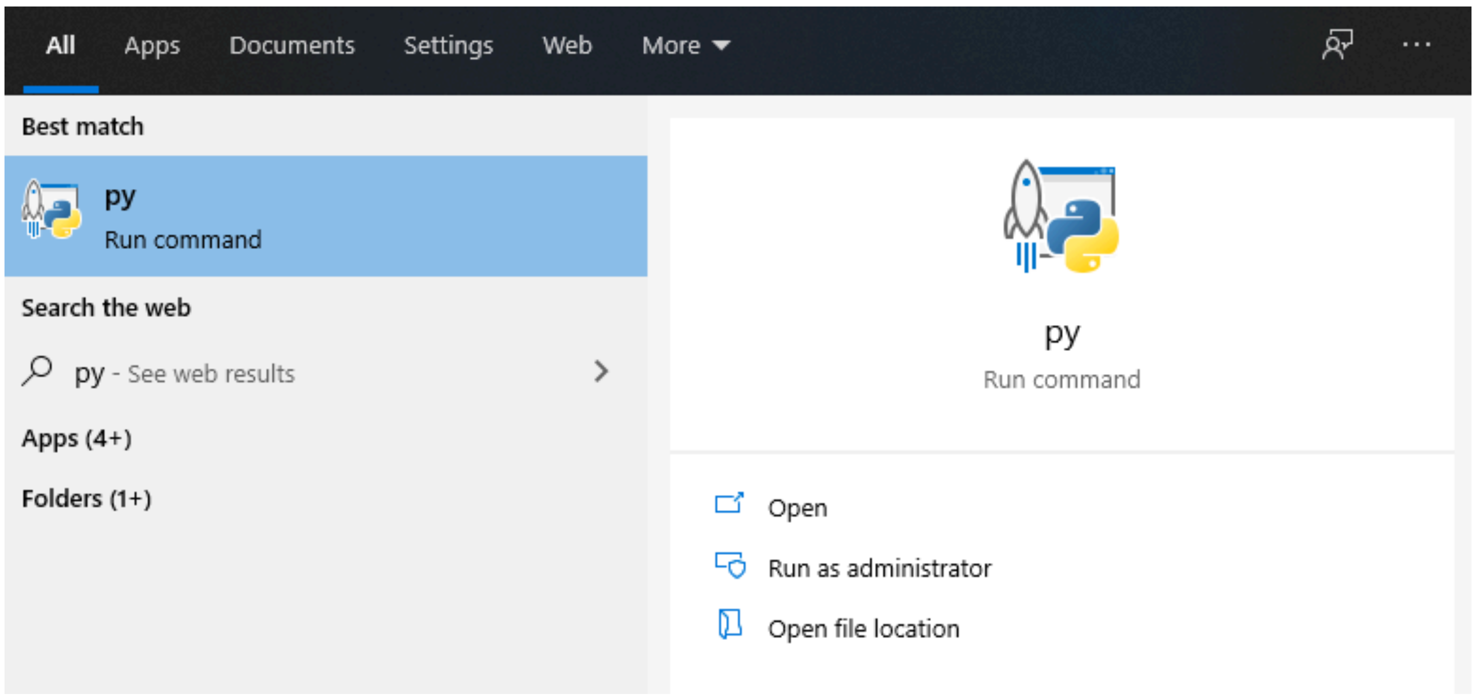
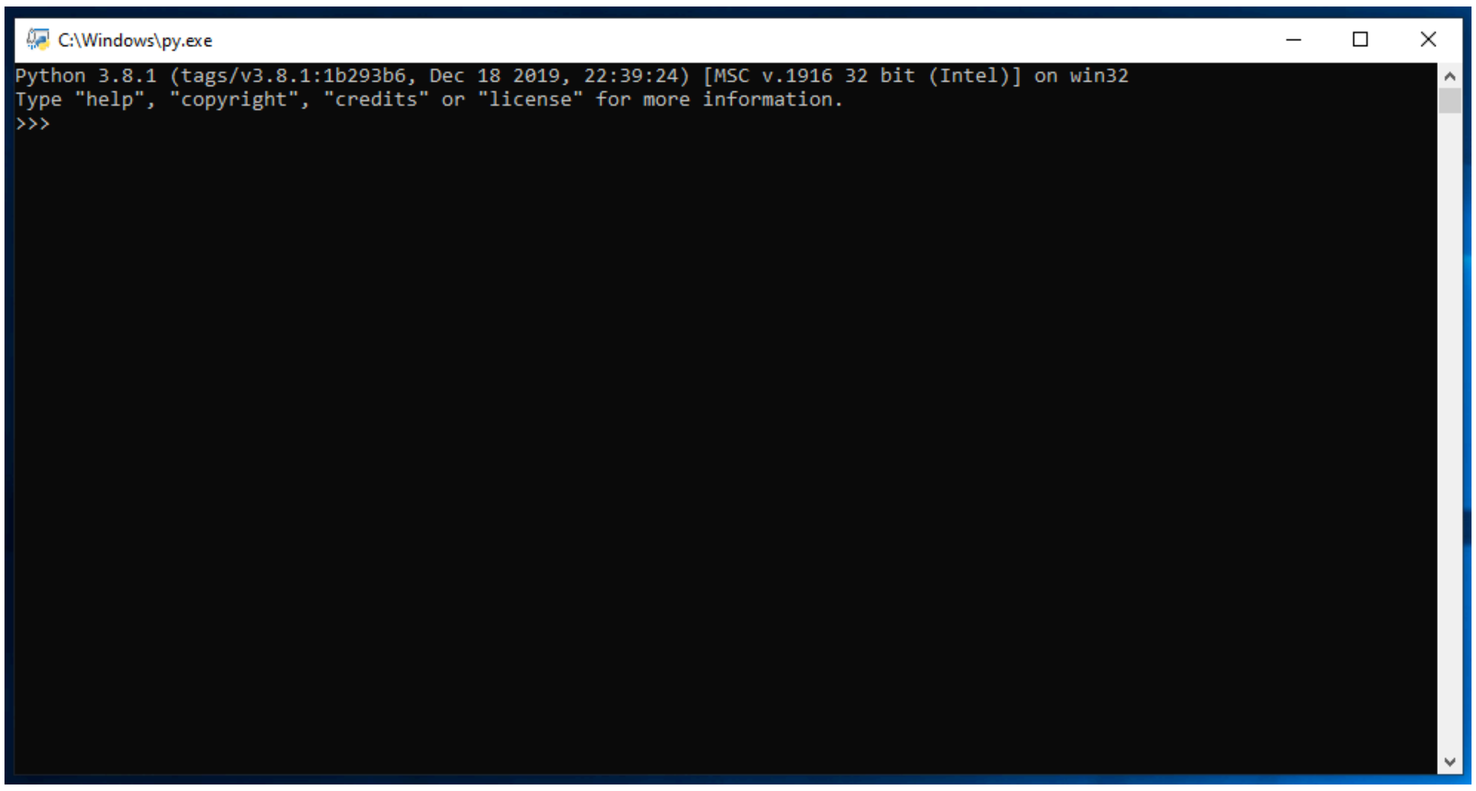
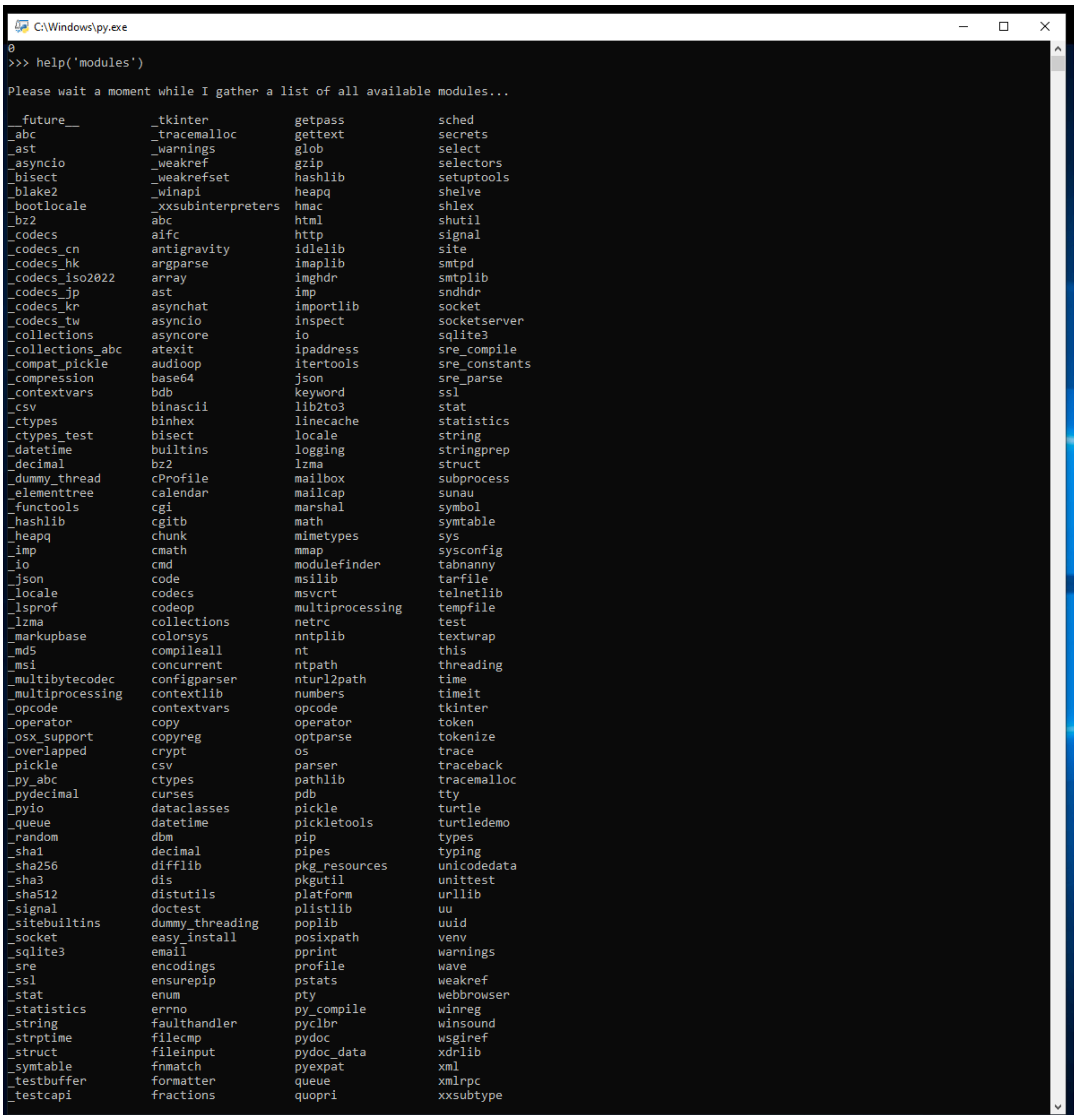
EDB Endpoint AD Audit

Overview	This script will list all the machines that are in the Active Directory and NOT in any Sophos Central Enterprise Dashboard sub estates
Install Python	Follow the Python install guide provided for your OS
Check you have ldap3 and requests installed	
Open Py.exe on Windows Use the Terminal on a Mac	 All Apps Documents Settings Web More Best match py Run command Search the web py - See web results Apps (4+) Folders (1+) py Run command Open Run as administrator Open file location

	
	`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	



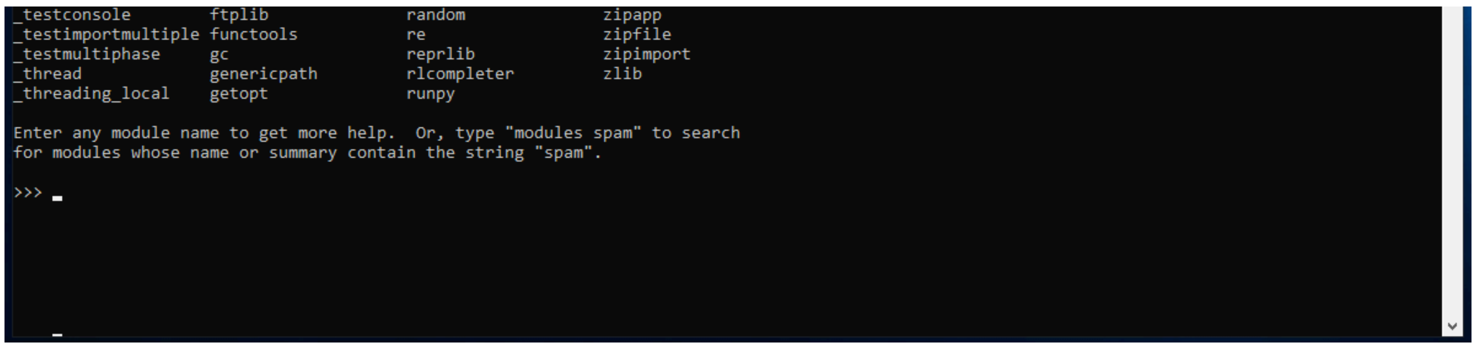
```
0
>>> help('modules')

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             setuptools
_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               imghdr              smtplib
_codecs_jp          ast                 imp                 sndhdr
_codecs_kr          asynchat            importlib           socket
_codecs_tw          asyncio             inspect             socketserver
_collections        asyncore            io                  sqlite3
_collections_abc    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            cgitb               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              pdb                 tty
_pyio               dataclasses         pickle              turtle
_queue              datetime            pickletools         turtledemo
_random             dbm                 pip                 types
_sha1               decimal             pipes               typing
_sha256             difflib             pkg_resources       unicodedata
_sha3               dis                 pkgutil             unittest
_sha512             distutils           platform            urllib
_signal             doctest             plistlib            uu
_sitebuiltins       dummy_threading     poplib              uuid
_socket             easy_install        posixpath           venv
_sqlite3            email               pprint              warnings
_sre                encodings           profile             wave
_ssl                ensurepip           pstats              weakref
_stat               enum                pty                 webbrowser
_statistics         errno               py_compile          winreg
_string             faulthandler        pyclbr              winsound
_strptime           filecmp             pydoc               wsgiref
_struct             fileinput           pydoc_data          xdrlib
_symtable           fnmatch             pyexpat             xml
_testbuffer         formatter           queue               xmlrpc
_testcapi           fractions           quopri              xxsubtype
```

Note csv and datetime are installed

We will need to install some Modules



```
_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".

>>> _
```

PC

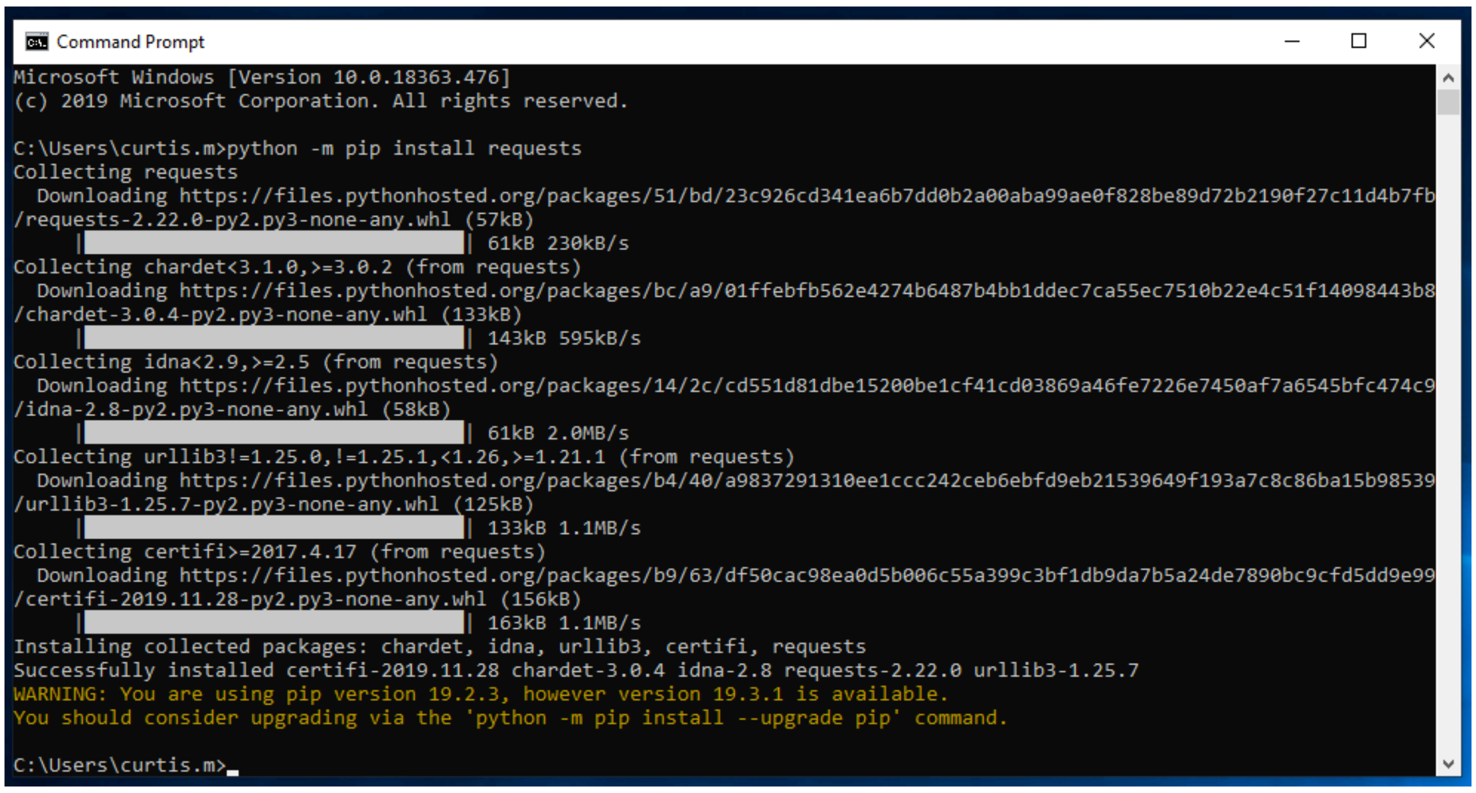
Open an Elevated Command Prompt

Type - python -m pip install requests

we also need LDAP3

python -m pip install ldap3

Note there is a module called request. We need requests



```
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

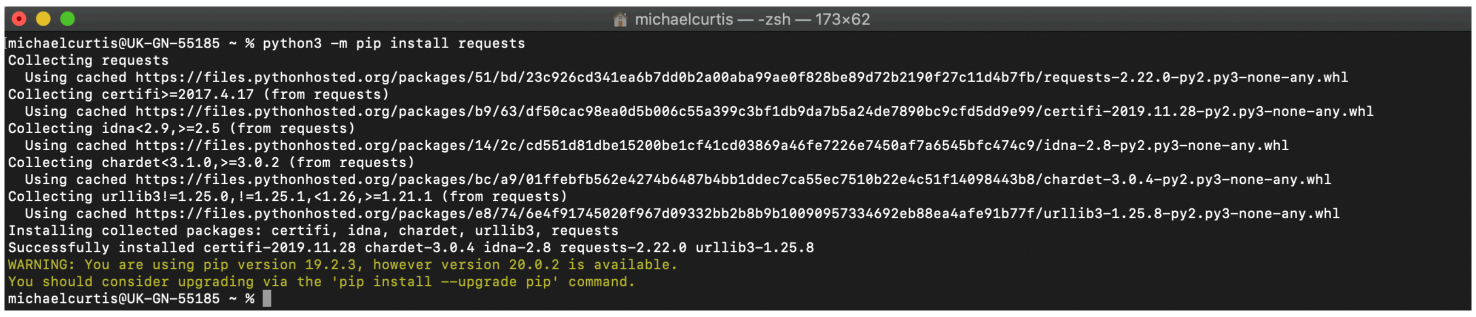
Type - python3 -m pip install requests

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

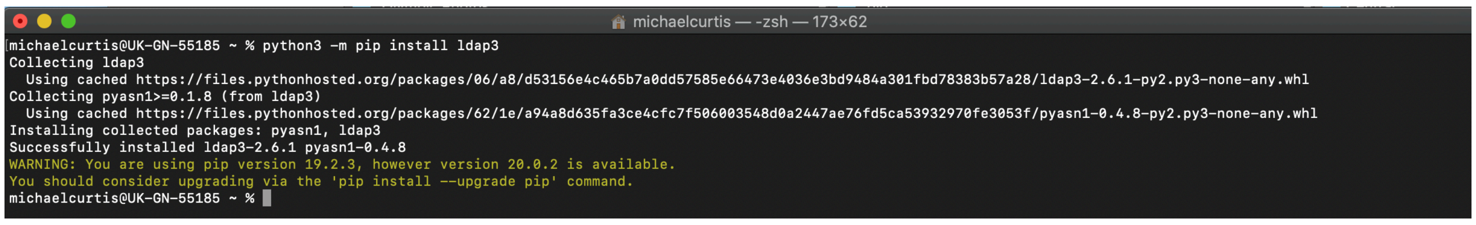
we also need LDAP3

python3 -m pip install ldap3

Note there is a module called request. We need requests

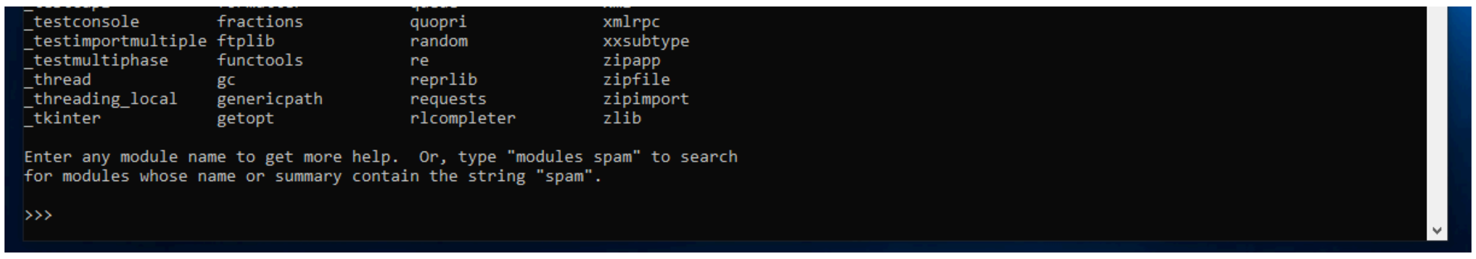


```
michaelcurtis@UK-GN-55185 ~ % python3 -m pip install requests
Collecting requests
  Using cached https://files.pythonhosted.org/packages/51/bd/23c926cd341ea6b7dd0b2a00aba99ae0f828be89d72b2190f27c11d4b7fb/requests-2.22.0-py2.py3-none-any.whl
Collecting certifi>=2017.4.17 (from requests)
  Using cached 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 ~ % 
```



```
michaelcurtis@UK-GN-55185 ~ % python3 -m pip install ldap3
Collecting ldap3
  Using cached https://files.pythonhosted.org/packages/06/a8/d53156e4c465b7a0dd57585e66473e4036e3bd9484a301fbd78383b57a28/ldap3-2.6.1-py2.py3-none-any.whl
Collecting pyasn1>=0.1.8 (from ldap3)
  Using cached https://files.pythonhosted.org/packages/62/1e/a94a8d635fa3ce4cfc7f506003548d0a2447ae76fd5ca53932970fe3053f/pyasn1-0.4.8-py2.py3-none-any.whl
Installing collected packages: pyasn1, ldap3
Successfully installed ldap3-2.6.1 pyasn1-0.4.8
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 and ldap3 in the Python shell



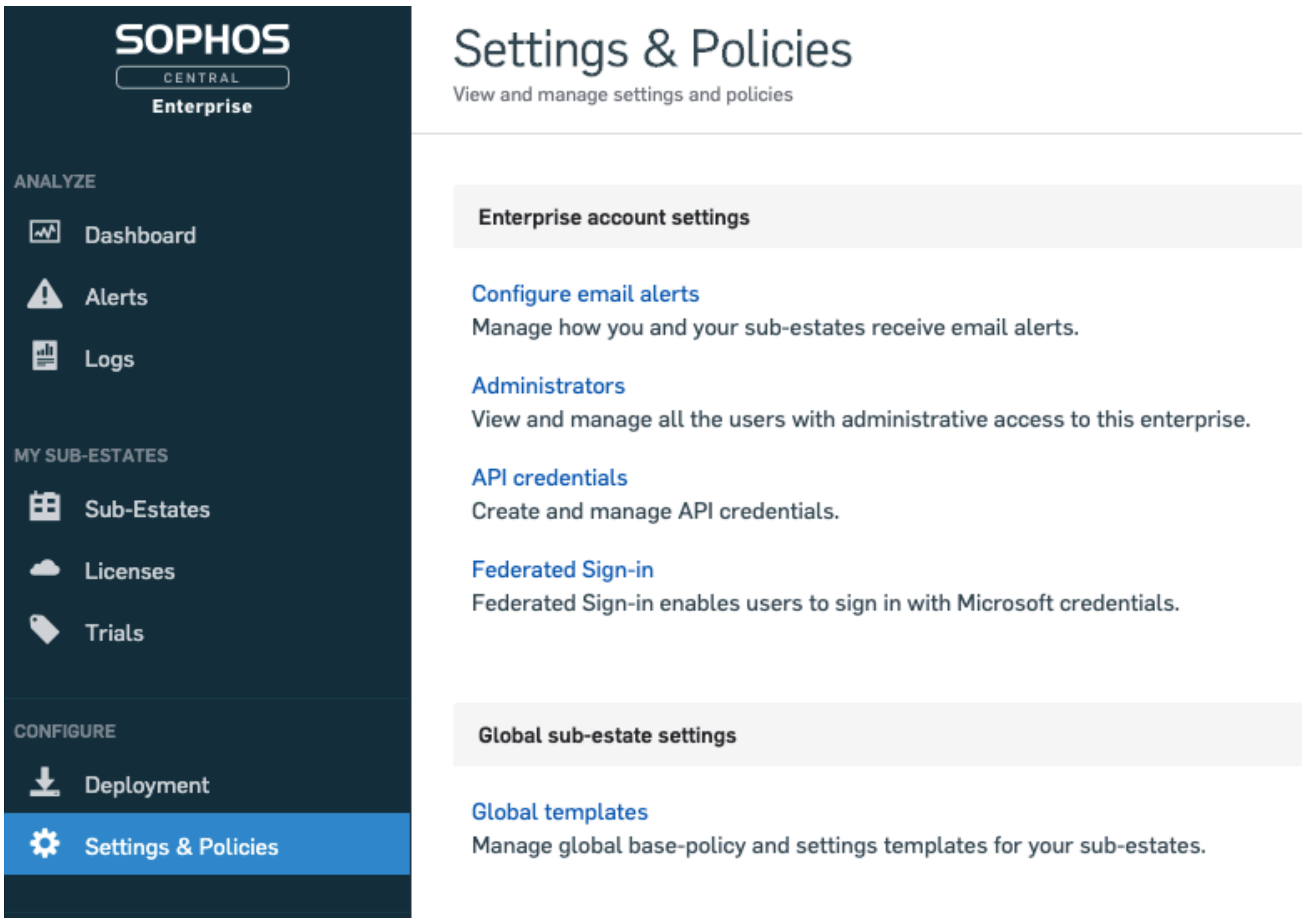
```
_testconsole        fractions           quopri              xmlrpc
_testimportmultiple ftplib              random              xxsubtype
_testmultiphase     functools           re                  zipapp
_thread             gc                  reprlib             zipfile
_threading_local    genericpath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

>>>
```

Log into Sophos Central. We will need to make our API credentials

Click on Settings & Policies



Settings & Policies

View and manage settings and policies

Enterprise account settings

Configure email alerts

Manage how you and your sub-estates receive email alerts.

Administrators

View and manage all the users with administrative access to this enterprise.

API credentials

Create and manage API credentials.

Federated Sign-in

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

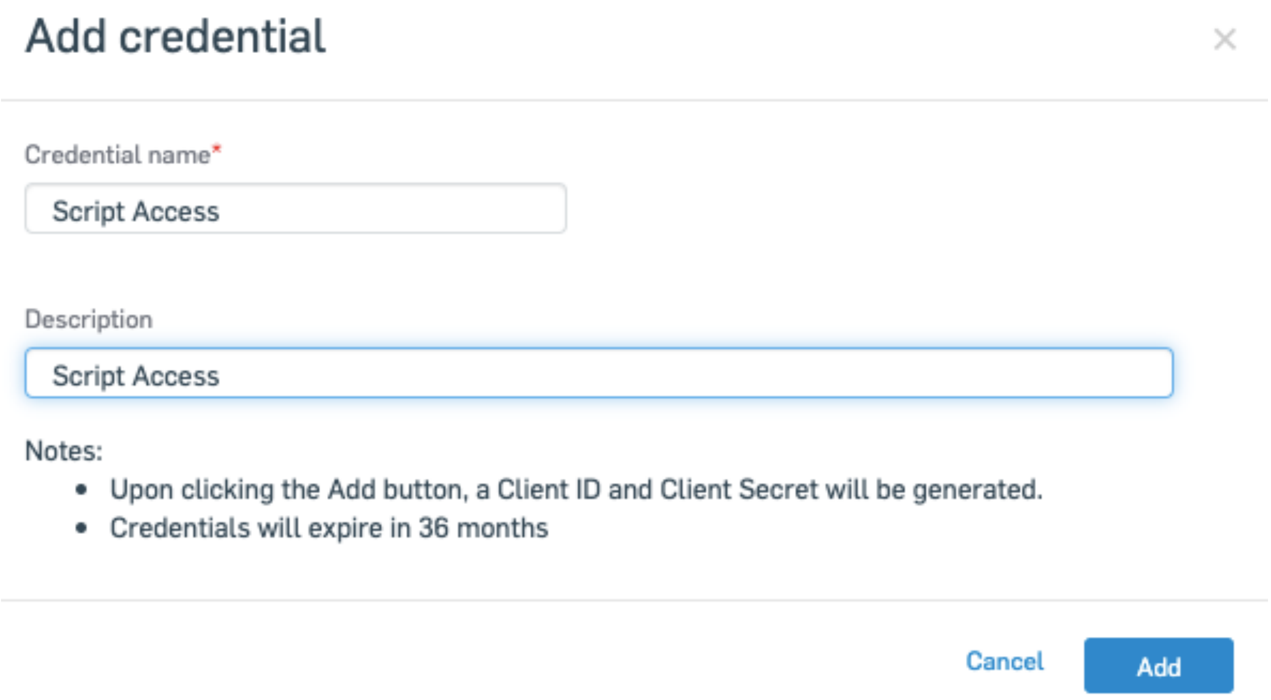
Global sub-estate settings

Global templates

Manage global base-policy and settings templates for your sub-estates.

Click API Credentials

Click Add



Add credential

Credential name*: Script Access

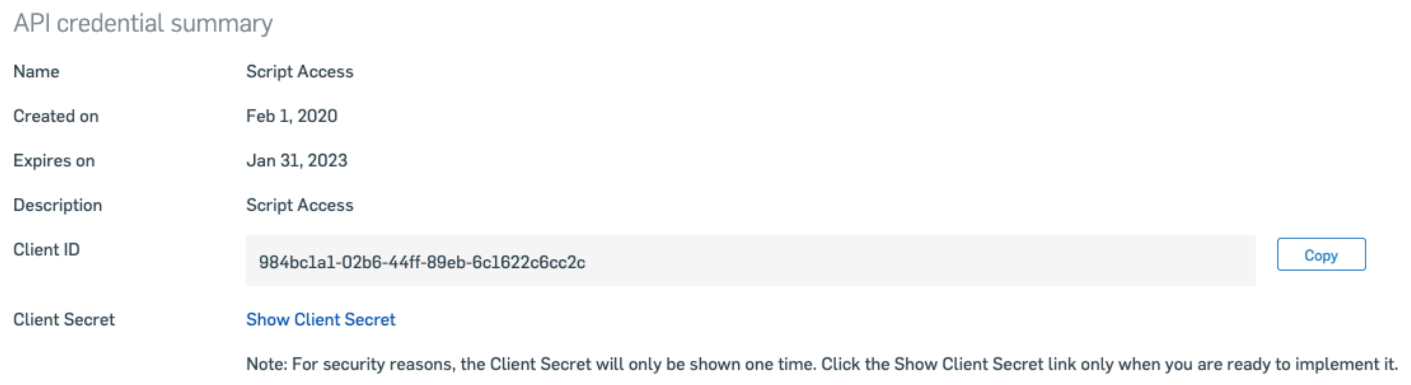
Description: Script Access

Notes:

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

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
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 edb_config.config

```
[DEFAULT]
ClientID:<put clientID here>
ClientSecret:<put clientSecret here>

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

	[DOMAIN] SearchDomain:<put search domain here example - dc=domain,dc=co,dc=uk> SearchUser:<put ldap search account here example - domain\dap.l> SearchUserPassword:<put ldap password here> DomainController:<Put domain controller name FQDN or IP address here> LDAPPort:<put the LDAP port here 389 or 636>
Example Note the file path has a \ on the end	[DEFAULT] ClientID:8477295f-4f16-7378cd50b05 ClientSecret:12a94330c59648c10e60577ae573c6e0fc20f35a425670847eb63d9b1954592d2b8305cd87e3 [REPORT] ReportName:EDB_ ReportFilePath:c:\users\michael\desktop\reports\ [DOMAIN] SearchDomain:dc=domain,dc=co,dc=uk SearchUser:domain\dap.l SearchUserPassword:password DomainController:10.0.1.250 LDAPPort:636
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 EDB_Unprotected_Machines_v1.py
Mac	
From Terminal run the Python script	python3 EDB_Unprotected_Machines_v1.py