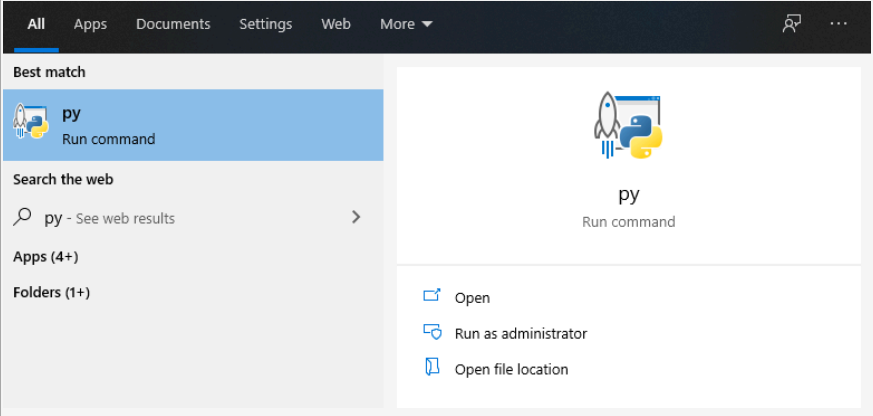
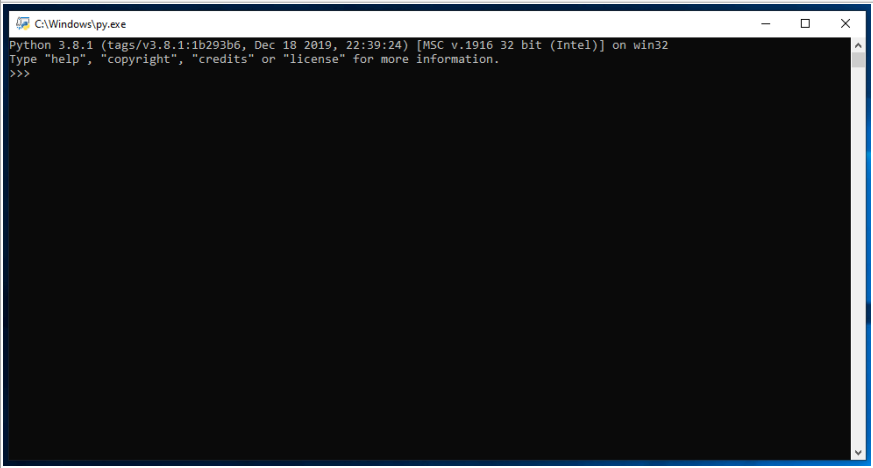


Overview	This script will list all the machines that are in the Active Directory and NOT in the Sophos Central console
Install Python	Follow the Python install guide provided for your OS
Check you have ldap3 and requests installed	
Open Py.exe on Windows Use the Terminal on a Mac	 <p>The screenshot shows the Windows Start menu search interface. The search bar contains 'py'. Under 'Best match', there is a result for 'py' with the icon of a rocket and the text 'Run command'. Below this, there is a section 'Search the web' with a magnifying glass icon and the text 'py - See web results'. Further down, there are sections for 'Apps (4+)' and 'Folders (1+)'. On the right side of the search results, there is a larger preview of the 'py' result, showing the rocket icon and the text 'py Run command'. Below this preview, there are three options: 'Open', 'Run as administrator', and 'Open file location'.</p>
	 <p>The screenshot shows a Windows terminal window titled 'C:\Windows\py.exe'. The terminal displays the following text: '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.', and a prompt '>>>'.</p>

Type - help('modules')

This will list all the modules installed

```
C:\Windows\python.exe
>>> 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
bz2            abc            html            shutil
codecs         aifc            http            signal
codecs_cn      antigra        http            site
codecs_hk      argparse       imaplib         smtpd
codecs_iso2022 array          imghdr         smtplib
codecs_jp      ast            imap            sndhdr
codecs_kr      asynchat       inputlib        socket
codecs_tw      asyncio        inspect         socketserver
collections     asyncore       io              sqlite3
collections_abc atexit         ipaddress       sre_compile
compat_pickle  audiopack      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             cml            modulefinder    tabnanny
json           code           msilib          tarfile
locale         codecs         msvcrt          telnetlib
lsprof         codeop         multiprocessing tempfile
lzma           collections    nntplib         test
markupbase     colorsys       nt              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     turledemo
random         dbm           pip             types
sha1           decimal       pipes           typing
sha256         difflib       pkg_resources   unicodedata
sha3           dis           platform        unittest
sha512         distutils     plistlib        urllib
signal         doctest       poplib          uu
sitebuiltins  dummy_threading
socket         easy_install  posixpath       uuid
sqlite3        email         pprint          venv
sre            encodings     profile         warnings
ssl            ensurpip      patats          wave
stat           enum          pty             weakref
statistics     errno         py_compile     webbrowser
string         faulthandler  pycbr           winreg
stringprep     filecmp       pydoc           winsound
struct         fileinput     pydoc_data      wsgiref
symtable       fnmatch       pyexpat         xdrlib
testbuffer     format        queue           xml
testcapi       fractions     quopri          xmlrpc
                            xxsubtype
```

Note csv and datetime are installed

We will need to install some Modules

```
testconsole    ftplib         random          zipapp
testimportmultiple
testmultiphase gc              re              zipfile
thread         genericpath    reprlib         zipimport
threading_local getopt         rncompiler      zlib
               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

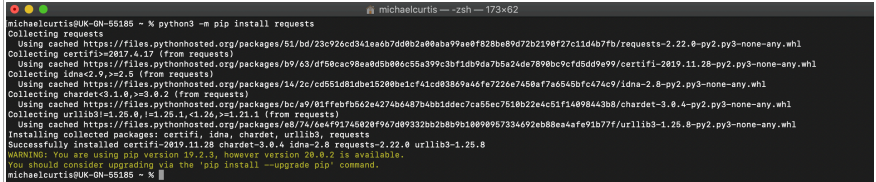

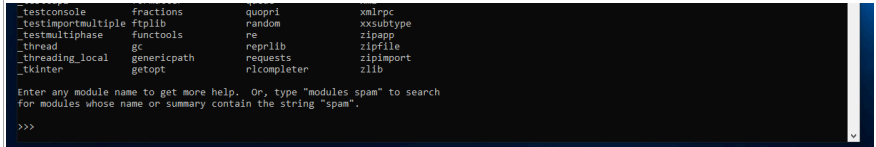
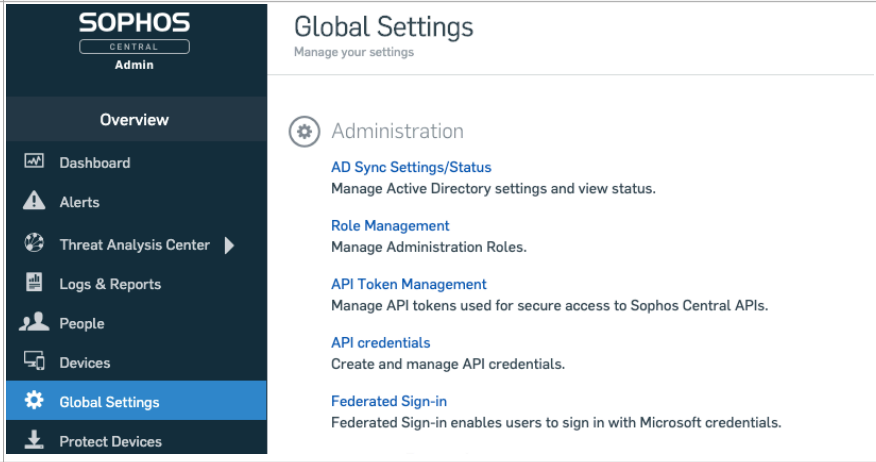
```
Command Prompt
Microsoft Windows [Version 10.0.18363.476]
(c) 2019 Microsoft Corporation. All rights reserved.

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/a9/01ffebfb562e4274b6487b4bb1ddcec7ca55ec7510b22e4c51f14098443b8/chardet-3.0.4-py2.py3-none-any.whl (133kB)
    [143kB 595kB/s]
Collecting idna<2.0,>=2.5 (from requests)
  Downloading https://files.pythonhosted.org/packages/14/2c/cd551d81dbe15280be1cf41cd03869a46fe7226e7450af7a6545bfc474c9/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/a9837291310ee1ccc242ce6ebfd9eb21539649f193a7c8c86ba15b98539/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

<p>Type - python3 -m pip install requests</p> <p>The 3 is important or it will install requests to version 2 of Python</p> <p>we also need LDAP3</p> <p>python3 -m pip install ldap3</p> <p>Note there is a module called request. We need requests</p>	 <pre> michaelcurtis@UK-QN-55185 ~ % python3 -m pip install requests Collecting requests Using cached https://files.pythonhosted.org/packages/51/bd/23c926cd34eab67dd8b2a88aba99ae0f828be89d72b2196f27c1d4b7fb/requests-2.22.8-py2.py3-none-any.whl Collecting certifi<=2021.4.12 (from requests) Using cached https://files.pythonhosted.org/packages/b9/63/d58cac98ea8d5b08cc5a399c3b71db9da7b5a24de7898bc9cfd5dd9e99/certifi-2019.11.28-py2.py3-none-any.whl Collecting idna<2.9,>=2.5 (from requests) Using cached https://files.pythonhosted.org/packages/1a/2c/cd551d81d9e15288b1c41cd03849a46fe7226e7458af746545bf4c74c9/idna-2.8-py2.py3-none-any.whl Collecting charset<3.1.0,>=3.0.2 (from requests) Using cached https://files.pythonhosted.org/packages/bc/a9/81ff6b7b502e4274b6487b4bb1ddec7ca55ec7518b22e4c51f14898443b8/charset-3.0.4-py2.py3-none-any.whl Collecting urllib3<1.26.0,=>1.25.1 (from requests) Using cached https://files.pythonhosted.org/packages/e8/74/6e4f91745028f967d09332bb2b8b9b10898957334692ab88eaafe91b77f/urllib3-1.25.8-py2.py3-none-any.whl Installing collected packages: certifi, idna, charset, urllib3, requests Successfully installed certifi-2019.11.28 charset-3.0.4 idna-2.8 requests-2.22.8 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-QN-55185 ~ % </pre>
	 <pre> michaelcurtis@UK-QN-55185 ~ % python3 -m pip install ldap3 Collecting ldap3 Using cached https://files.pythonhosted.org/packages/06/a8/d5315e4c465b7a8dd57685e6473e483e3b9484a381fbd78383b57a28/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/094a8d63fa3ca4cfc7f686803548d8a2447ae76fd5ca5392970fe3083f/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-QN-55185 ~ % </pre>
<p>Note help('modules') now lists requests and ldap3 in the Python shell</p>	 <pre> testconsole fractions quopri xmlrpc testimportmultiple ftplib random xxsubtype testmultiphase functools re zipapp _thread gc reprlib zipfile _threading_local genericpath requests zipimport _tkinter getopt ricompleter 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". >>> </pre>
<p>Log into Sophos Central. We will need to make our API credentials</p>	
<p>Click on Global Settings</p>	 <div> <div> SOPHOS CENTRAL Admin </div> <div> Overview <div> Dashboard Alerts Threat Analysis Center Logs & Reports People Devices Global Settings Protect Devices </div> </div> <div> 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. </div> </div>
<p>Click API Credentials</p>	

<p>Click Add</p>	<div> <div>Add credential</div> <div> <div>Credential name*</div> <div>Script Access</div> </div> <div> <div>Description</div> <div>Script Access</div> </div> <div> <div>Notes:</div> <ul style="list-style-type: none"> Upon clicking the Add button, a Client ID and Client Secret will be generated. Credentials will expire in 36 months </div> <div> <div>Cancel</div> <div>Add</div> </div> </div>												
<p>Click show secret. Once you close this screen you won't be able to see this again</p> <p>Record this information. You will need it for the config file</p>	<div> <div>API credential summary</div> <table> <tr> <td>Name</td><td>Script Access</td></tr> <tr> <td>Created on</td><td>Feb 1, 2020</td></tr> <tr> <td>Expires on</td><td>Jan 31, 2023</td></tr> <tr> <td>Description</td><td>Script Access</td></tr> <tr> <td>Client ID</td><td>984bc1a1-02b6-44ff-89eb-6c1622c6cc2c</td></tr> <tr> <td>Client Secret</td><td>Show Client Secret</td></tr> </table> <div> <div>Copy</div> </div> <div> <div>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.</div> </div> </div>	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
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												
<p>We now need to edit the Sophos_Central_Unprotected_Machines file</p>	<div> <div>[DEFAULT]</div> <div>ClientID:<put clientID here></div> <div>ClientSecret:<put clientSecret here or leave blank to enter manually></div> <div>[REPORT]</div> <div>ReportName:<put report name here></div> <div>ReportFilePath:<put file path here></div> <div>ConsoleName:<put console name here></div> <div>[DOMAIN]</div> <div>SearchDomain:<put search domain here example - dc=ukps,dc=co,dc=uk></div> <div>SearchUser:<put ldap search account here example - ukpsaws\dap.l></div> <div>DomainController:<Put domain controller name FQDN or IP address here></div> <div>LDAPPort:<put the LDAP port here 389 or 636></div> </div>												

Example	<p>[DEFAULT] ClientID:33d15ef8-3274-075743e8ff2f ClientSecret:d8a713157d536b62c74b94abb4bedb8f50489182112</p> <p>[REPORT] ReportName:Unprotected_Machines ReportFilePath:c:\users\ps\desktop\reports\ ConsoleName:UK PS</p> <p>[DOMAIN] SearchDomain:dc=domain,dc=co,dc=uk SearchUser:domain\dap.l DomainController:10.0.1.250 LDAPPort:636</p>
Make sure the config file is in the same folder as the script	
PC	
From the cmd run the Python script	python Sophos_Central_Unprotected_Machines.py
Mac	
From Terminal run the Python script	Python3 Sophos_Central_Unprotected_Machines.py