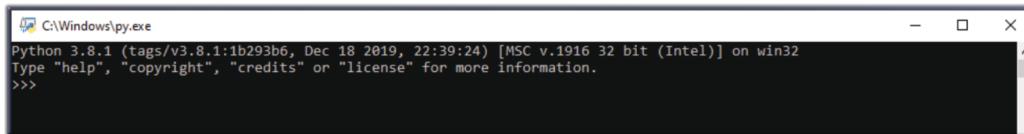
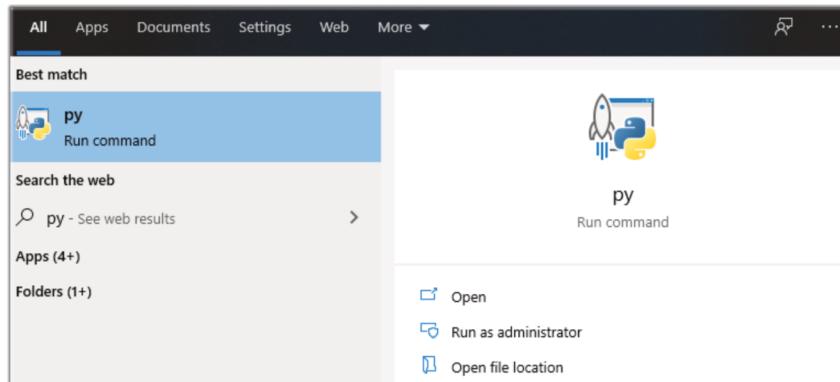


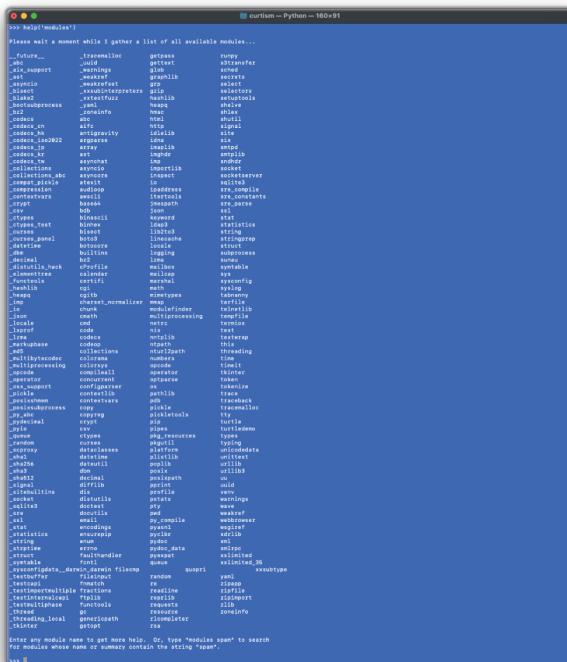
Sophos Central Health Report

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



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



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/a9/01ffebfb562e4274b6487b4bb1ddcc7ca55ec7510b22e4c51f14098443b8
  /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,!<1.26,>=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/df50cac98ea0d5b006c55a399c3bf1db9da7b5a24de7890bc9cf5dd9e99
  /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/df50cac98ea0d5b006c55a399c3bf1db9da7b5a24de7890bc9cf5dd9e99
  /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/a9/01ffebfb562e4274b6487b4bb1ddcc7ca55ec7510b22e4c51f14098443b8
  /chardet-3.0.4-py2.py3-none-any.whl
Collecting urllib3!=1.25.0,!<1.26,>=1.21.1 (from requests)
  Using cached https://files.pythonhosted.org/packages/e8/74/6e4f91745020f967d09332b2b8b9b10090957334692e888ea4afe91b77f
  /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
_tesimportmultiple ftplib       random      xxsubtype
_tesmultiphase   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

The screenshot shows the Sophos Central Admin interface. On the left, there's a sidebar with 'Overview' and several icons: Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings (which is highlighted in blue), and Protect Devices. The main content area is titled 'Global Settings: Manage your settings'. It contains five sections: 'Administration' (with 'AD Sync Settings/Status' and 'Role Management'), 'API Token Management' (with 'Manage API tokens used for secure access to Sophos Central APIs.'), 'API credentials' (with 'Create and manage API credentials.'), and 'Federated Sign-in' (with 'Federated Sign-in enables users to sign in with Microsoft credentials.'). There's also a note at the bottom: 'Upon clicking the Add button, a Client ID and Client Secret will be generated. Credentials will expire in 36 months.'

Click API Credentials Management

The screenshot shows a modal dialog titled 'Add credential'. It has a 'Credential name*' field containing 'Script Access', a 'Description' field also containing 'Script Access', and a 'Notes' section with two bullet points: 'Upon clicking the Add button, a Client ID and Client Secret will be generated.' and 'Credentials will expire in 36 months.' At the bottom right are 'Cancel' and 'Add' buttons.

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

The screenshot shows an 'API credential summary' page. It lists the following details:

Name	Script Access
Created on	Feb 1, 2020
Expires on	Jan 31, 2023
Description	Script Access
Client ID	984bc1a1-02b6-44ff-89eb-6c1622c8cc2c
Client Secret	Show Client Secret

A note at the bottom states: "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." A 'Copy' button is also visible next to the Client ID.

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

The API key only needs to be Service Principal Read-Only

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

Include MAC addresses

MAC_Address:1

Include components versions

Versions:0

Include Windows build version

Windows_Build_Version:1

Include cloud provider and instanceID

Cloud_Servers:1

Include alerts

```
# Include alerts
Include_Alerts:1
# Include full service status - Used for support
Full_Services_List:0
# Split Sophos Central Enterprise Dashboard reports by sub estate
Split_EDB_Reports:1
# Include sub estate ID
Include_Sub_EstateID:0
# Report only contains machines with issues
List_Machines_With_Issues_Only:0
# Show the menu to Health Check individual sub estates
Show_sse_menu:0
# Report only contains machines in the group defined Leave blank for all machines
# and comma separated for multiple groups (case sensitive)
List_Machines_In_Group:
```

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
```