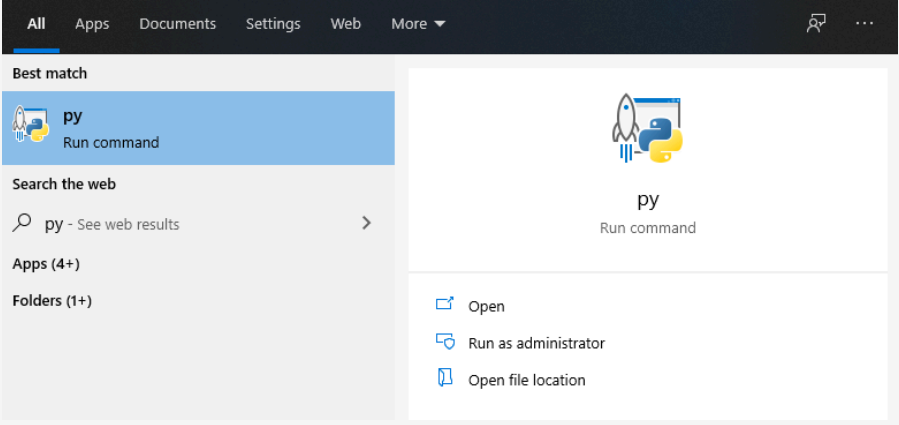
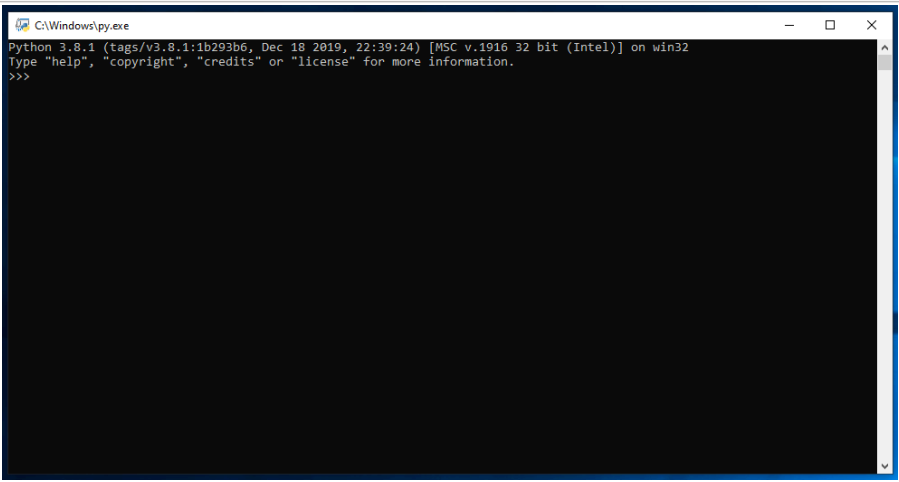
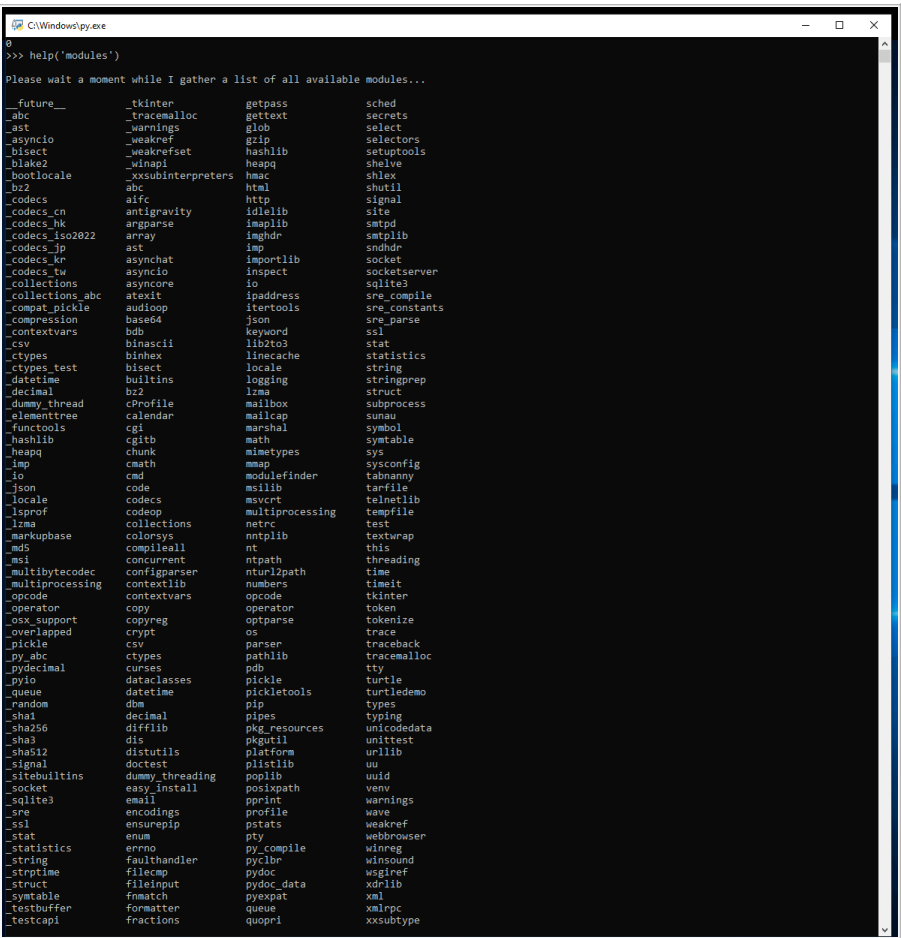
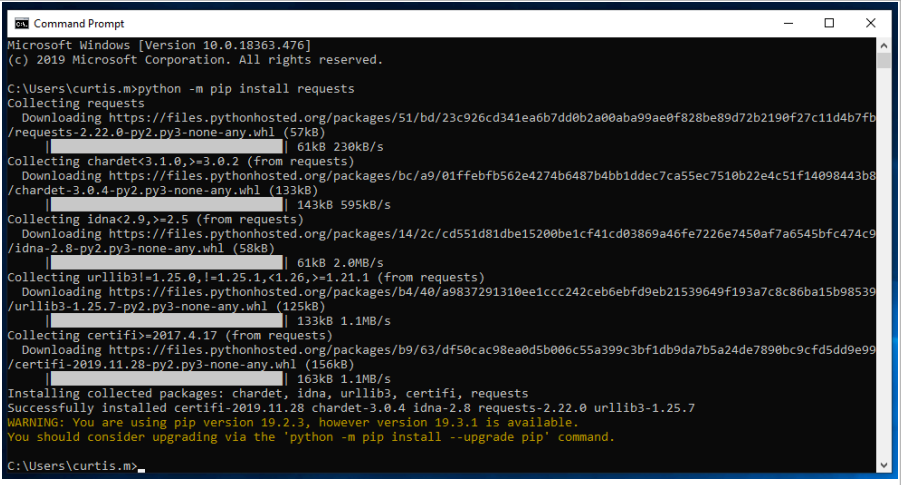


Overview	<p>The script will check turn on Tamper on all machine where it has been disabled across all sub estates</p> <p><b>IT WILL NOT OVERRIDE TAMPER BEING TURNED OFF VIA GLOBAL SETTINGS</b></p>
Install Python	Follow the Python install guide provided for your OS
Check you have requests installed	
<p>Open Py.exe on Windows</p> <p>Use the Terminal on a Mac</p>	 <p>The screenshot shows a Windows Start menu search for 'py'. The 'Best match' section shows 'py' with the subtext 'Run command'. Below this, there are sections for 'Search the web', 'Apps (4+)', and 'Folders (1+)'. On the right side, there is a larger preview of the 'py' command with the subtext 'Run command' and 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:         <pre>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. &gt;&gt;&gt;</pre> </p>

<p>Type - help('modules')</p> <p>This will list all the modules installed</p>	
<p>Note csv and datetime are installed already</p> <p>We will need to install some Modules</p>	
<p>PC</p>	<p>Open an Elevated Command Prompt</p>
<p>Type - python -m pip install requests</p> <p>Note there is a module called request. We need requests</p>	
<p>Mac</p>	<p>Open Terminal</p>

```
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 ~ ssh - 173x62
michaelcurtis@BUK-GN-55185 ~ % python3 -m pip install requests
Collecting requests
  Using cached https://files.pythonhosted.org/packages/51/bd/23c26dc41aeb07d8062a09ba9ef828be98d72619f27c11d4b7b/requests-2.22.0-py2.py3-none-any.whl
Collecting certifi<2017.4.17, from requests
  Using cached https://files.pythonhosted.org/packages/b9/6c/d58cac79eadd0e0e55a39c3bf1bd97a524c7890bc9fd5dd99ef/certifi-2019.11.28-py2.py3-none-any.whl
Collecting idna<2.9,>=2.5, from requests
  Using cached https://files.pythonhosted.org/packages/44/0c/d551e81d8e1280b01c2280b01c7e722647598776455abcf74c69/d9/certifi-2019.11.28-py2.py3-none-any.whl
Collecting chardet<3.1.0,>=3.0.2, from requests
  Using cached https://files.pythonhosted.org/packages/bc/91/ff6b65626747bb64bb1d8dc7c55ec75c10322eac1f3cf10984338/chardet-3.0.4-py2.py3-none-any.whl
Collecting urllib3<1.25.0,>=1.20, from requests
  Using cached https://files.pythonhosted.org/packages/87/74/6e49f74562697509323b2b2b09143857334692e888a4a4ef1b77f/urllib3-1.25.0-py2.py3-none-any.whl
Successfully installed certifi-2019.11.28 chardet-3.0.4 idna-2.8 requests-2.22.0 urllib3-1.25.0
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@BUK-GN-55185 ~ %

```

Note `help('modules')` 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       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".

```
>>>
```

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


Click on Settings & Policies


SOPHOS


CENTRAL

Enterprise


ANALYZE


 Dashboard


 Alerts

 Logs


MY SUB-ESTATES


 Sub-Estates

 Licenses

 Trials

CONFIGURE

 Deployment

 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

Cancel

Add

<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>	<p>API credential summary</p> <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> <p>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.</p>	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_Turn_On_Tamper.config file</p>	<p>[DEFAULT]  ClientID:&lt;put clientID here&gt;  ClientSecret:&lt;put clientSecret here or leave blank to enter manually&gt;</p> <p>[REPORT]  ReportName:&lt;put report name here&gt;  ReportFilePath:&lt;put file path here&gt;</p>												
<p>Example</p>	<p>[DEFAULT]  ClientID:8477295f-4f16-47378cd50b05  ClientSecret:12a94330c59648151a790ec10e6c6e0fc20f35a4256708</p> <p>[REPORT]  ReportName:EDB_Health_  ReportFilePath:c:\users\michael\desktop\reports\</p>												
<p>Make sure the config file is in the same folder as the script</p>													
<p>PC</p>													
<p>From the cmd run the Python script</p>	<p>python Sophos_Central_Turn_On_Tamper.py</p>												
<p>Mac</p>													
<p>From Terminal run the Python script</p>	<p>python3 Sophos_Central_Turn_On_Tamper.py</p>												