


Single Console Endpoint AD Audit

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	<div><div><div>AllAppsDocumentsSettingsWebMore</div><div>Best match</div><div><div><div><div><div></div></div><div>py</div></div><div>Run command</div></div></div><div><div>Search the web</div><div><div><div></div></div>py - See web results</div></div><div>Apps (4+)</div><div>Folders (1+)</div></div></div> <div><div><div><div></div></div>py</div><div>Run command</div></div> <div><div><div></div></div>Open</div> <div><div><div></div></div>Run as administrator</div> <div><div><div></div></div>Open file location</div>

	<div><div><div>C:\Windows\py.exe</div><div><pre>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 antigra idlelib site _codecs_hk argparse imaplib smtpd _codecs_iso2022 array imghdr smtpplib _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 _func tools 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 _multibytecode 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 turtle demo _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 pycldr winsound _strptime filecmp pydoc wsgiref _struct fileinput pydoc_data xdrlib _symtable fnmatch pyexpat xml _testbuffer formatter queue xmlrpc _testcapi fractions quopri xxsubtype</pre></div></div></div>
<div><div>Note csv and datetime are installed</div><div>We will need to install some Modules</div></div>	<div><div><pre>_testconsole ftplib random zipapp _testimportmultiple func tools re zipfile _testmultiphase gc reprlib zipimport _thread genericpath rlc ompleter 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". >>> _</pre></div></div>
PC	Open an Elevated Command Prompt
<div><div>Type - python -m pip install requests</div><div>we also need LDAP3</div><div>python -m pip install ldap3</div><div>Note there is a module called request. We need requests</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.

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

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 Copy
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.

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

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

[DOMAIN]
SearchDomain:<put search domain here example - dc=ukps,dc=co,dc=uk>
SearchUser:<put ldap search account here example - ukpsaws\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>
```

<p>Example</p> <p>Note the file path has a \ on the end</p>	<p>[DEFAULT] ClientID:33d15ef8-3274-075743e8ff2f ClientSecret:d8a713157dda2536b62c74b94abb4bedb8f504891821129ca34989924cbdc37d2ef1cf7c4ef887</p> <p>[REPORT] ReportName:Unprotected_Machines ReportFilePath:c:\users\michael\desktop\reports\ ConsoleName:UK PS</p> <p>[DOMAIN] SearchDomain:dc=domain,dc=co,dc=uk SearchUser:domain\dap.l SearchUserPassword:password DomainController:10.0.1.250 LDAPPort:636</p>
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 Console_Unprotected_Machines_v1
Mac	
From Terminal run the Python script	Python3 Console_Unprotected_Machines_v1