FingerPrint DB/ Custom DB/Creation of Custom DB

FingerPrint DB Package :

A Fingerprint package is a file named as fpdb-<version>.pkg eg(fpdb-50.pkg) that is required to upload on the profiler Basic configuration page to enable profiler services.
It is used for classification of devices based on DHCP fingerprint, NAMP fingerprint and TCP fingerprint
It consists of 2 main sqlite databases packaged together.

- packaged.sqlite3.pkg - Static database taken from fingerbank org(https://www.fingerbank.org/)
- nmap.sqlite3.pkg -Referred as Custom Database which has to be updated regularly by Ivanti with new finger print classification ,for newer devices reported by customer or QA .

Apart from above 2 , there is another db calld admindb(admindb.sqlite3) which is database created on Profiler whenever admin adds a fingerprint on DDR page.(this is local to the system
this db gets first priority during classification before the finger print is checked against other dbs).
Custom Database or nmap.sqlite3 - Whenever the fpdb package is upgraded , this is the database that is upgraded by Profiler team and a new fpdb package is created.

It consists of tables related to

DHCP fingerprints
NMAP fingerprints
TCP fingerprints

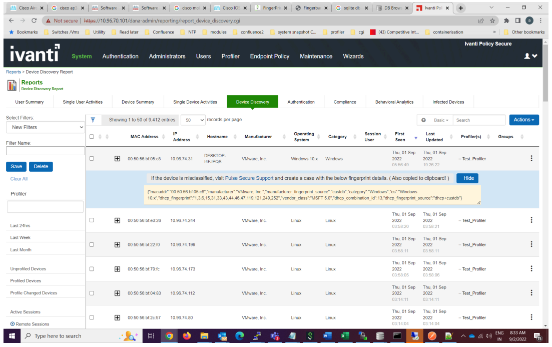
Paths for databases in a PPS box.

./data/runtime/profiler/nmap.sqlite3
./data/runtime/profiler/packaged.sqlite3

To view these databases and contents , you can copy them to windows system and use a database browser from https://sqlitebrowser.org/

Process For Upgrading nmap/custom db .

- If a new device discovered at customer site or QA lab OR customer notices the device is getting misclassified by DHCP or NMAP, a service ticket is raised by the admin for pulse to add the fingerprint to the custom db



MAC Address	IP Address	Hostname	Manufacturer	Operating System	Category	Session User	First Seen	Last Updated	Profiler(s)	Groups
00:50:56:bf:05:c8	10.96.74.31	DESKTOP-I4FJPQS	VMware, Inc.	Windows 10.x	Windows		Thu, 01 Sep 2022 05:56:49	Thu, 01 Sep 2022 19:26:22	Test_Profiler	
00:50:56:bf:e3:26	10.96.74.244		VMware, Inc.	Linux	Linux		Thu, 01 Sep 2022 03:58:20	Thu, 01 Sep 2022 03:58:21	Test_Profiler	
00:50:56:bf:22:f0	10.96.74.199		VMware, Inc.	Linux	Linux		Thu, 01 Sep 2022 03:58:11	Thu, 01 Sep 2022 03:58:11	Test_Profiler	
00:50:56:bf:79:fc	10.96.74.173		VMware, Inc.	Linux	Linux		Thu, 01 Sep 2022 03:58:05	Thu, 01 Sep 2022 03:58:06	Test_Profiler	
00:50:56:bf:04:83	10.96.74.112		VMware, Inc.	Linux	Linux		Thu, 01 Sep 2022 03:14:11	Thu, 01 Sep 2022 03:14:11	Test_Profiler	
00:50:56:bf:2c:57	10.96.74.80		VMware, Inc.	Linux	Linux		Thu, 01 Sep 2022 03:14:04	Thu, 01 Sep 2022 03:14:04	Test_Profiler	

If the device is misclassified, visit Pulse Secure Support and create a case with the below fingerprint details. (Also copied to clipboard!)

```
{"macaddr":"00:50:56:bf:05:c8","manufacturer":"VMware, Inc.","manufacturer_fingerprint_source":"custdb","category":"Windows","os":"Windows 10.x","dhcp_fingerprint":"1,3,6,15,31,33,43,44,46,47,119,121,249,252","vendor_class":"MSFT 5.0","dhcp_combination_id":13,"dhcp_fingerprint_source":"dhcp+custdb"}
```

- We check if the misclassification is due to missing fingerprint classification in db. If so we update the db
- The data base update can happen by (based on requirement)

  1- New DHCP fingerprint

  2-New NMap fingerprint

  3-New TCP fingerprint

  4-Mac ouis- received from IEEE

  5-Os lists

- The repository for fingerprint files ivantiinc/ostp-fingerprintdb

1-DHCP Fingerprint Update Process :

- When Admin raises the service ticket for addition of new finger print , he must also provide the correct category and OS for the device. The developer also should try to verify the OS and category from other sources, e.g product datasheets, or querying from fingerbank.org .
- There are 3 files need to be changed
  changes.md
  custom_fingerprint.csv
  version.txt
- Sample PR: https://github.com/ivantiinc/ostp-fingerprintdb/commit/f96adc985a02482bc401eb0563caecb938441a55
- Check the README files in repo on compiling and creating the package.
- Get the changes reviewed and merged to master.
- Checkout this session for more details: https://ivanti.atlassian.net/wiki/display/download/attachments/80746418/KT-1%20_%20Fingerprint%20DB%20%28fpdb%29-20220117_140435-Meeting%20Recording.mp4?version=1&modificationDate=1643262642000&api=v2
- For Testing Use the below script to send dhcp packets to profiler server and check the classification on DDR page , change the fields marked in bold below.

```
def main():
#use encapsulated vendor-specific extensions:
OPTION['vendor_specific'] = Option(code=43, data=_list)
client = Client({
'chaddr': '70:70:8b:77:d8:04',
# ++++++ End Device IP, It can be anything +++++++
'ciaddr': '10.14.104.198',
#'listen':"192.168.1.13",
# ++++++ PPS IP +++++++ -----------⟶ TO BE CHANGED AS PER YOUR IPS
'server':'10.96.70.100',–IPS IP Address
#'server':'10.204.89.174',
#'client_identifier':'test123',
# ++++++ End Device IP, It can be anything +++++++
'request_ip_address': '10.14.104.198',
#'parameter_request_list': [50, 51, 'classless_static_route'],
'relay_agent': {'CIRCUIT-ID':'vci', 'REMOTE-ID':'vpi'},
'vendor_specific': {1:'vs1', 2:'vs2'},
'path_mtu_table': "1000 2000",
# ++++++++++++ FINGER PRINT TO BE ADDED ++++++++++++++
#'parameter_request_list': (1,121,3,6,15,114,119,252),
#'parameter_request_list': (1,121,3,6,15,114,119,252,95,44,46),
#'parameter_request_list': (1,15,3,28,12,6,7,26,43),
#'parameter_request_list': (1,3,6,15,26,28,51,58,59,43,108),
#'parameter_request_list': (1,3,6,15,26,28,51,58,59,43,114),
#'parameter_request_list': (1,3,6,15,26,28,51,58,59,43,114,108),
#'parameter_request_list': (1,33,3,6,15,28,51,58,59,43),
'parameter_request_list': (1,28,3,15,6,12,42,119,242,120,66,150,43,252),-DHCP Fingerprint
'vendor_class_identifier': 'Cisco:Codec:1.0',
'host_name': 'TESTHOST1_DHCP2',
})
floodPackets(client, 'f0:7f:06:29:2e:5e') =⟹MAC of device to be classified
```

2- NMAP Fingerprint Update process

space reservered.

3- TCP fingerprint update

4- Mac ouis

5-OS lists