ExtremeControl / ExtremeNAC Cross Reference

Creating a new DHCP Fingerprint (new Device Type)

Abstract: **This guide is designed to show a user how certain common tasks in ExtremeControl are accomplished in ExtremeNAC. Both products are very capable, however, the workflow of accomplishing tasks is different.**

Published: **August 2020**

Extreme Networks, Inc.

Phone / +1 408.579.2800
Toll-free / +1 888.257.3000
www.extremenetworks.com

P/N XXXXX-XX

Contents

Use Case

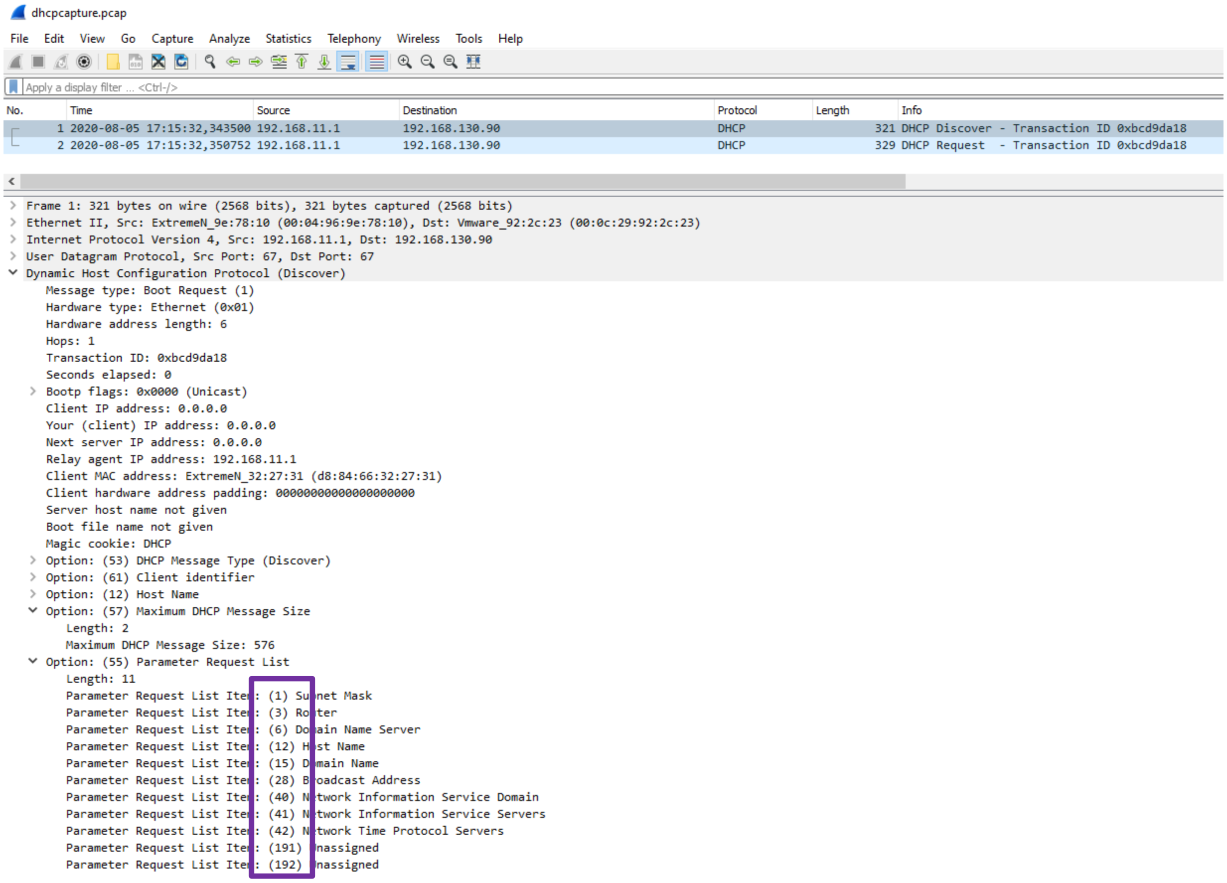
The endpoint is classified as Device Family / Device Class Access Point based on endpoint DHCP behavior. The outcome is better visibility and the Device Family / Device Class can be used to assign proper authorization.

Gathering information needed for the fingerprint

- Leverage the DHCP pcap
  - Following command can be used on a Linux based OS:

    ```
    tcpdump -ni eth0 -s 0 -w /tmp/dhcpcapture.pcap port 67
    ```

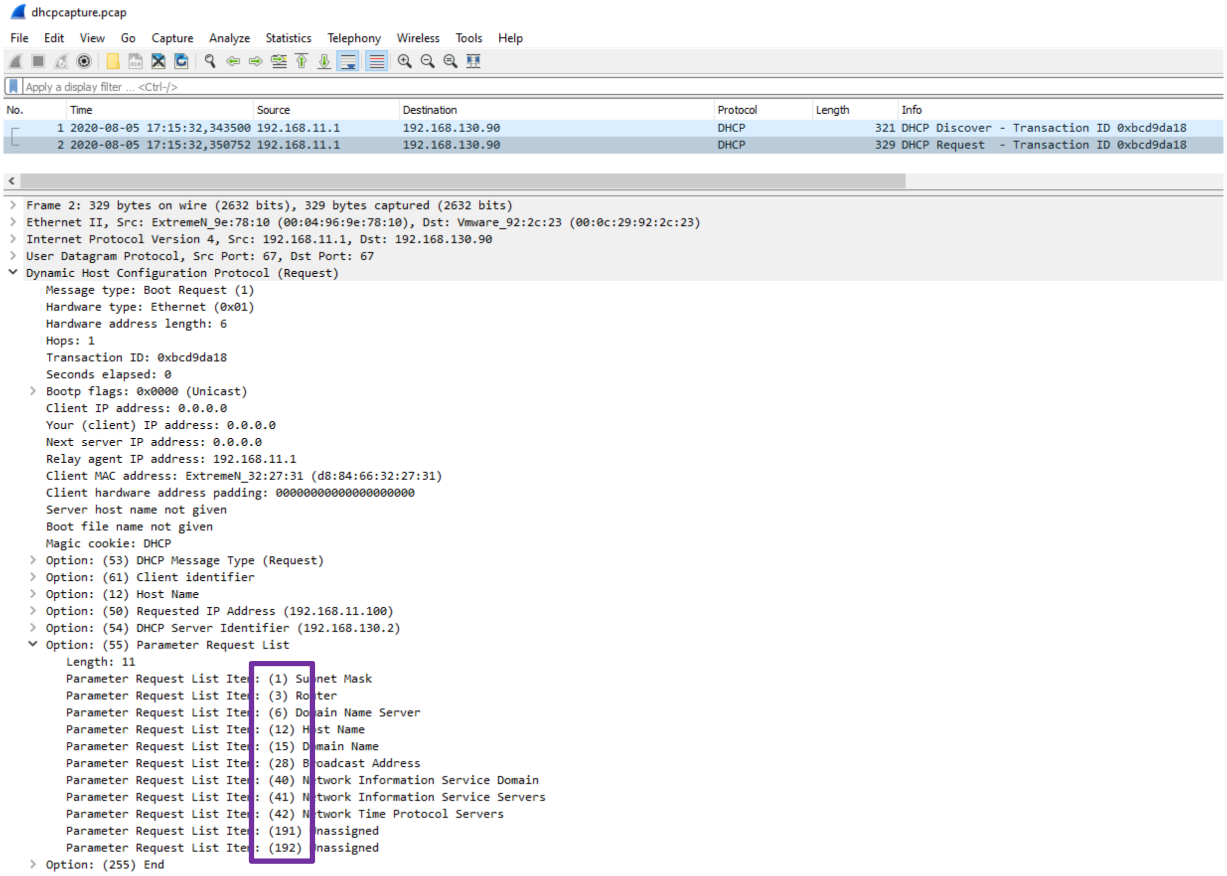
  - Extract the list of items from the option 55 from DHCP Discover:



```
No.     Time                           Source          Destination       Protocol  Length  Info
      1 2020-08-05 17:15:32,343500 192.168.11.1    192.168.130.90    DHCP         321 DHCP Discover - Transaction ID 0xbcd9da18
      2 2020-08-05 17:15:32,350752 192.168.11.1    192.168.130.90    DHCP         329 DHCP Request  - Transaction ID 0xbcd9da18
```

```
> Frame 1: 321 bytes on wire (2568 bits), 321 bytes captured (2568 bits)
> Ethernet II, Src: ExtremeN_9e:78:10 (00:04:96:9e:78:10), Dst: Vmware_92:2c:23 (00:0c:29:92:2c:23)
> Internet Protocol Version 4, Src: 192.168.11.1, Dst: 192.168.130.90
> User Datagram Protocol, Src Port: 67, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0xbcd9da18
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 192.168.11.1
    Client MAC address: ExtremeN_32:27:31 (d8:84:66:32:27:31)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (61) Client identifier
  > Option: (12) Host Name
  v Option: (57) Maximum DHCP Message Size
      Length: 2
      Maximum DHCP Message Size: 576
  v Option: (55) Parameter Request List
      Length: 11
      Parameter Request List Item: (1) Subnet Mask
      Parameter Request List Item: (3) Router
      Parameter Request List Item: (6) Domain Name Server
      Parameter Request List Item: (12) Host Name
      Parameter Request List Item: (15) Domain Name
      Parameter Request List Item: (28) Broadcast Address
      Parameter Request List Item: (40) Network Information Service Domain
      Parameter Request List Item: (41) Network Information Service Servers
      Parameter Request List Item: (42) Network Time Protocol Servers
      Parameter Request List Item: (191) Unassigned
      Parameter Request List Item: (192) Unassigned
```

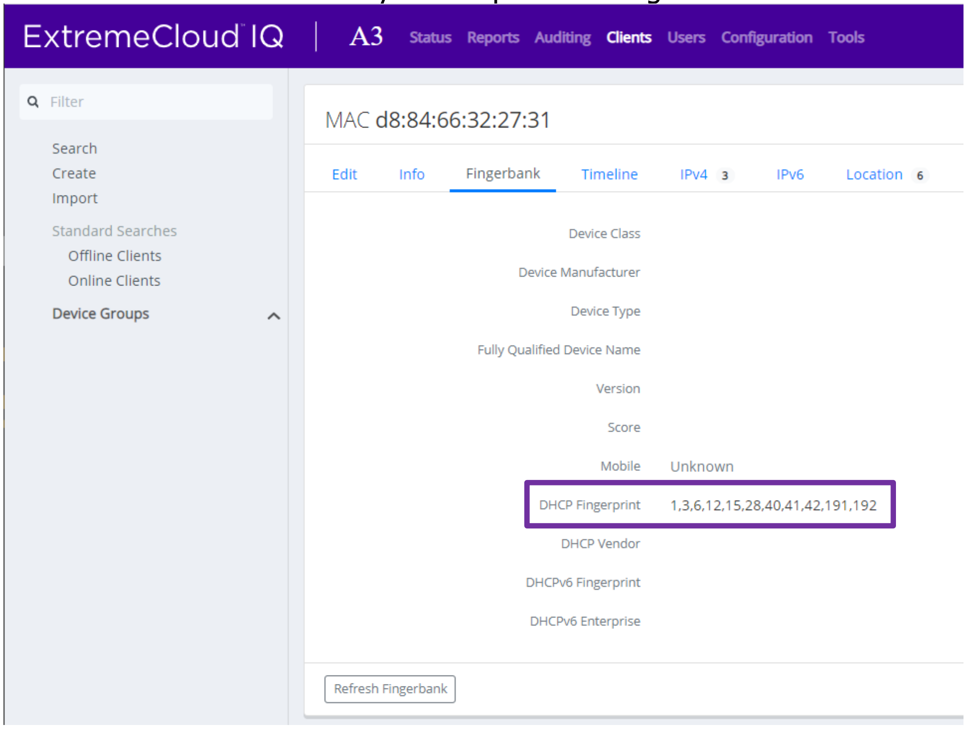
- Extract the list of items from the option 55 from DHCP Request:


dhcpcapture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time                       Source        Destination      Protocol  Length  Info
    1 2020-08-05 17:15:32,343500 192.168.11.1  192.168.130.90   DHCP         321  DHCP Discover - Transaction ID 0xbcd9da18
    2 2020-08-05 17:15:32,350752 192.168.11.1  192.168.130.90   DHCP         329  DHCP Request  - Transaction ID 0xbcd9da18

> Frame 2: 329 bytes on wire (2632 bits), 329 bytes captured (2632 bits)
> Ethernet II, Src: ExtremeN_9e:78:10 (00:04:96:9e:78:10), Dst: Vmware_92:2c:23 (00:0c:29:92:2c:23)
> Internet Protocol Version 4, Src: 192.168.11.1, Dst: 192.168.130.90
> User Datagram Protocol, Src Port: 67, Dst Port: 67
v Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0xbcd9da18
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 192.168.11.1
    Client MAC address: ExtremeN_32:27:31 (d8:84:66:32:27:31)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (50) Requested IP Address (192.168.11.100)
  > Option: (54) DHCP Server Identifier (192.168.130.2)
  v Option: (55) Parameter Request List
      Length: 11
      Parameter Request List Item: (1) Subnet Mask
      Parameter Request List Item: (3) Router
      Parameter Request List Item: (6) Domain Name Server
      Parameter Request List Item: (12) Host Name
      Parameter Request List Item: (15) Domain Name
      Parameter Request List Item: (28) Broadcast Address
      Parameter Request List Item: (40) Network Information Service Domain
      Parameter Request List Item: (41) Network Information Service Servers
      Parameter Request List Item: (42) Network Time Protocol Servers
      Parameter Request List Item: (191) Unassigned
      Parameter Request List Item: (192) Unassigned
  > Option: (255) End
```

- Leverage the A3 fingerprint
  - Clients -> Search -> choose your endpoint -> Fingerbank



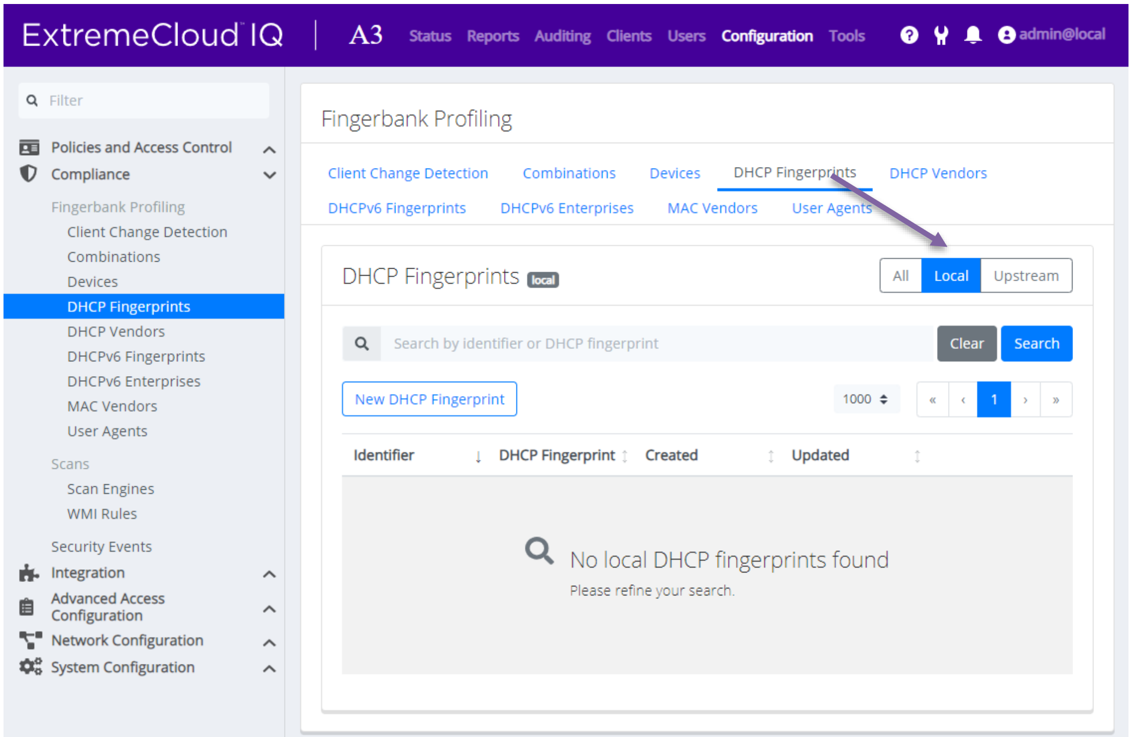
MAC d8:84:66:32:27:31

Device Class	
Device Manufacturer	
Device Type	
Fully Qualified Device Name	
Version	
Score	
Mobile	Unknown
DHCP Fingerprint	1,3,6,12,15,28,40,41,42,191,192
DHCP Vendor	
DHCPv6 Fingerprint	
DHCPv6 Enterprise	

- The DHCP fingerprint is: 1,3,6,12,15,28,40,41,42,191,192

A3 how to

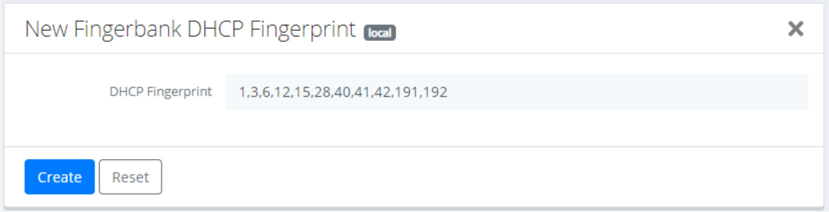
- Hit New DHCP Fingerprint in Configuration -> Compliance -> Fingerbank Profiling -> DHCP Fingerprints -> Local



No local DHCP fingerprints found

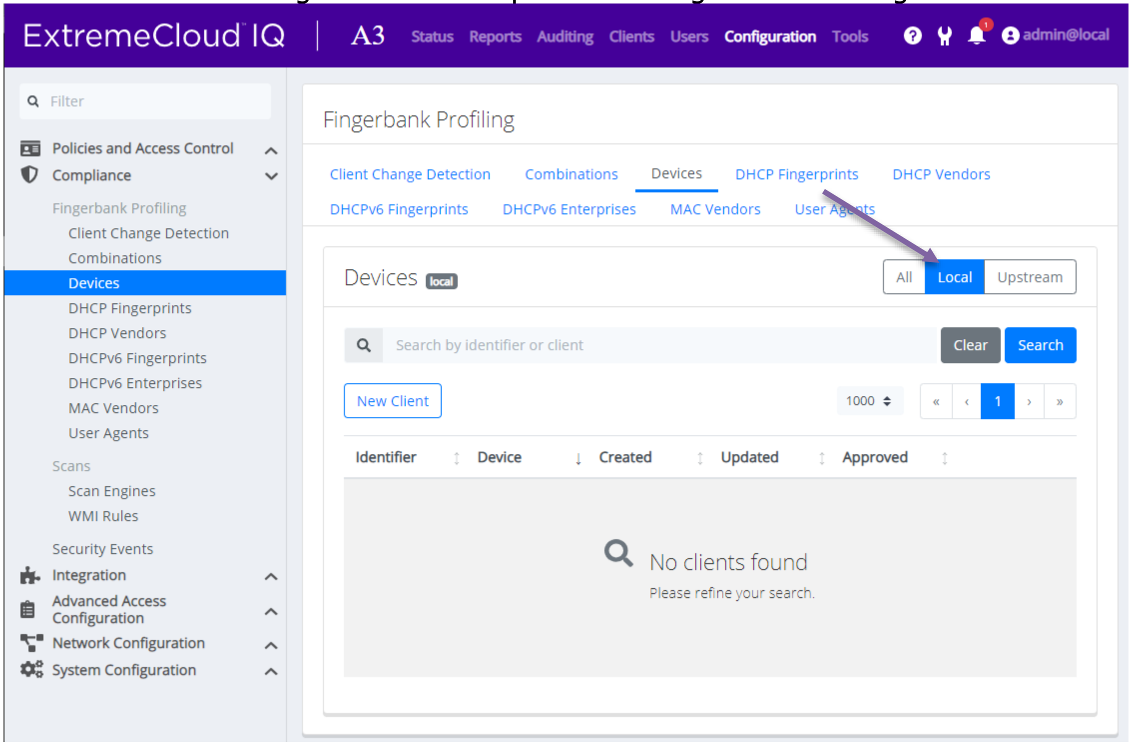
Please refine your search.

- Insert the DHCP Fingerprint and hit Create



DHCP Fingerprint 1,3,6,12,15,28,40,41,42,191,192

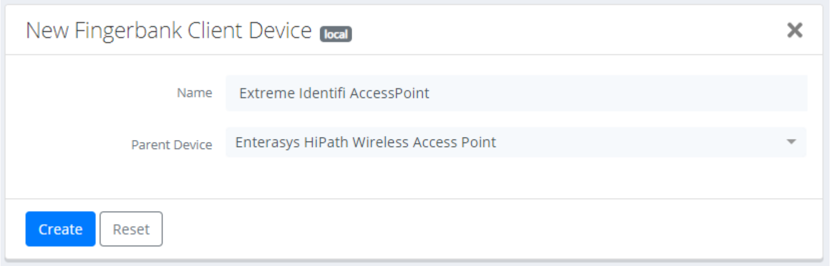
- Hit New Client in Configuration -> Compliance -> Fingerbank Profiling -> Devices -> Local



No clients found

Please refine your search.

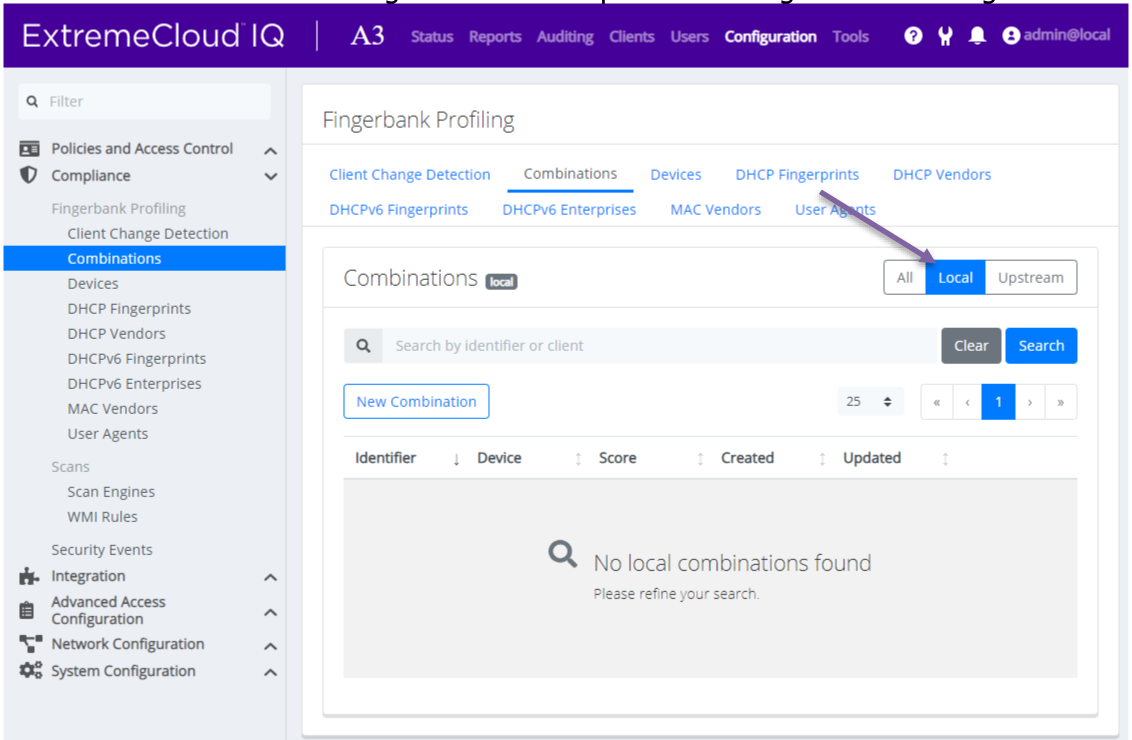
- Define the Name of the new device class. You may assign the device type to the parent device. Hit Create



Name: Extreme Identifi AccessPoint

Parent Device: Enterasys HiPath Wireless Access Point

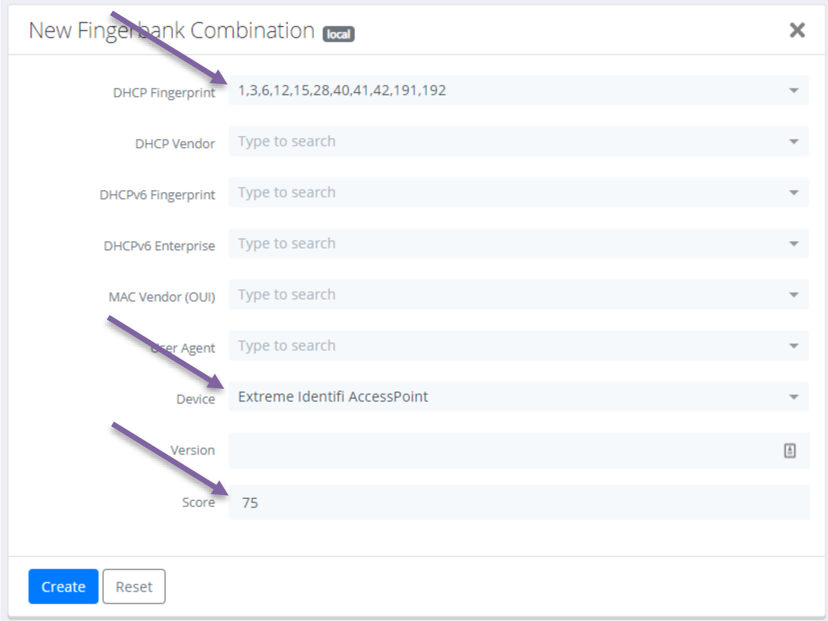
- Hit New Combination in Configuration -> Compliance -> Fingerbank Profiling -> Combinations -> Local



No local combinations found

Please refine your search.

- Enter DHCP Fingerprint, Device Type, Score. Hit Create



DHCP Fingerprint 1,3,6,12,15,28,40,41,42,191,192

DHCP Vendor Type to search

DHCPv6 Fingerprint Type to search

DHCPv6 Enterprise Type to search

MAC Vendor (OUI) Type to search

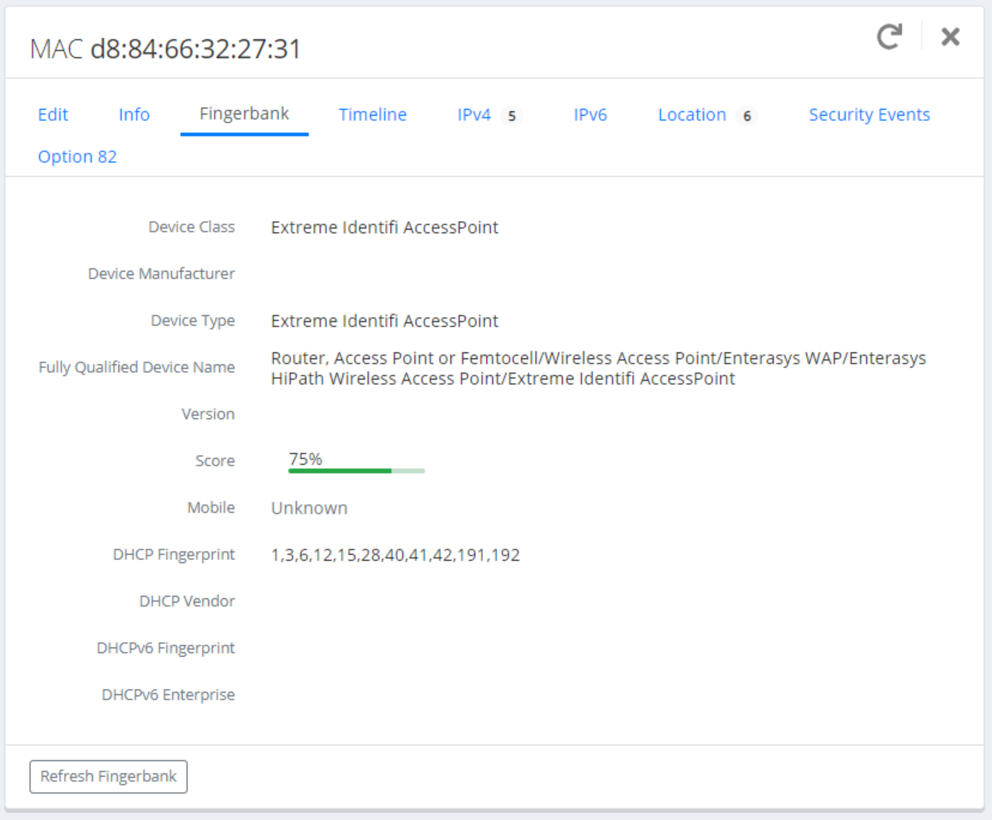
User Agent Type to search

Device Extreme Identifi AccessPoint

Version

Score 75

- When new DHCP is seen by A3, the Device Type is updated

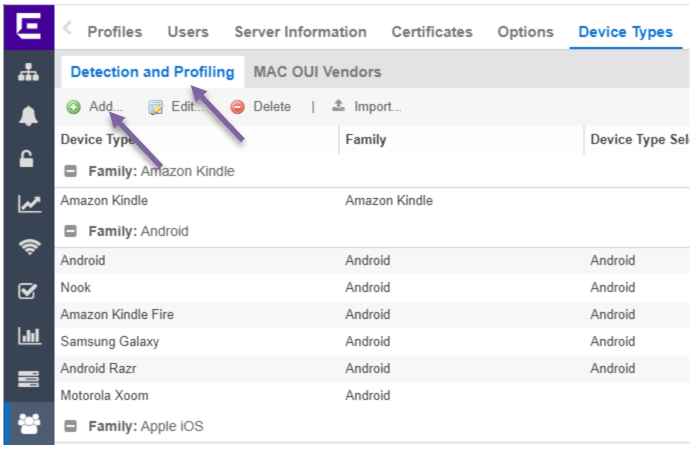


MAC d8:84:66:32:27:31

Device Class	Extreme Identifi AccessPoint
Device Manufacturer	
Device Type	Extreme Identifi AccessPoint
Fully Qualified Device Name	Router, Access Point or Femtocell/Wireless Access Point/Enterasys WAP/Enterasys HiPath Wireless Access Point/Extreme Identifi AccessPoint
Version	
Score	75%
Mobile	Unknown
DHCP Fingerprint	1,3,6,12,15,28,40,41,42,191,192
DHCP Vendor	
DHCPv6 Fingerprint	
DHCPv6 Enterprise	

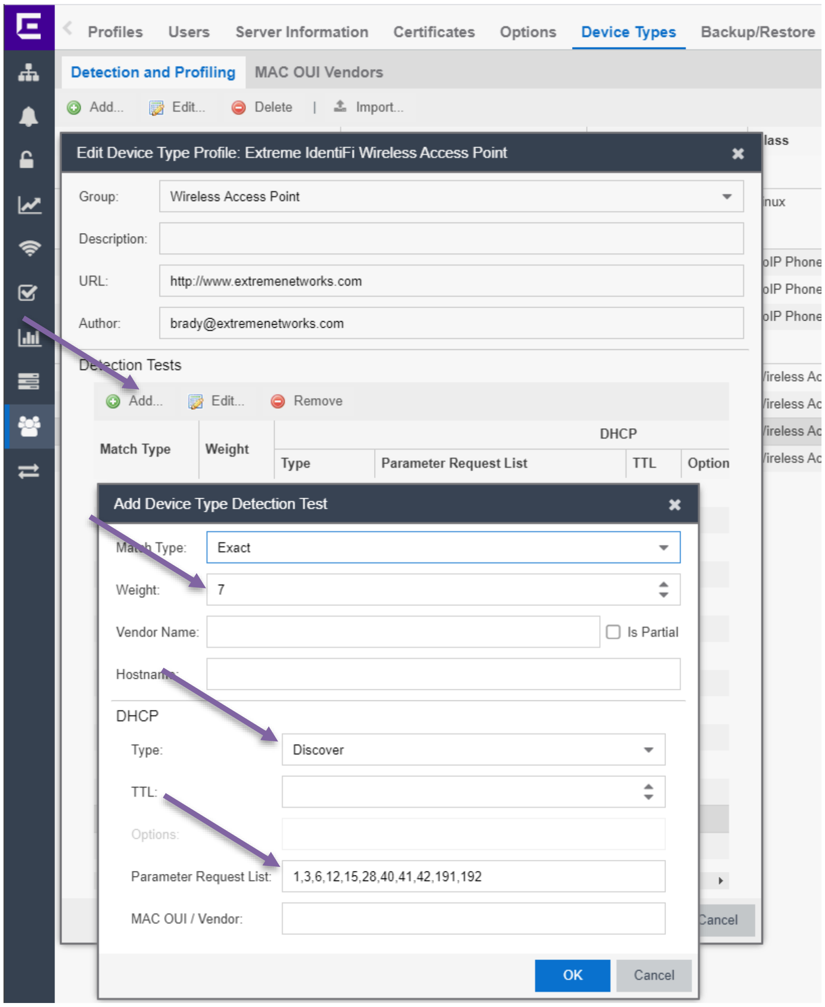
ExtremeControl version 8.5 how to

- Check if the Device Type exists already. Administration -> Device Types -> Detection and Profiling -> Magnifier tool.
- If the Device Type does not exist then hit the Add button. If the Device Type exists then use the Edit button.



Device Type	Family	Device Type Sel
Family: Amazon Kindle		
Amazon Kindle	Amazon Kindle	
Family: Android		
Android	Android	Android
Nook	Android	Android
Amazon Kindle Fire	Android	Android
Samsung Galaxy	Android	Android
Android Razr	Android	Android
Motorola Xoom	Android	
Family: Apple iOS		

- Add Detection Tests.



Edit Device Type Profile: Extreme IdentiFi Wireless Access Point

Group: Wireless Access Point

Description:

URL: http://www.extremenetworks.com

Author: brady@extremenetworks.com

Detection Tests

Match Type	Weight	DHCP			
		Type	Parameter Request List	TTL	Option

Add Device Type Detection Test

Match Type: Exact

Weight: 7

Vendor Name: □ Is Partial

Hostname:

DHCP

Type: Discover

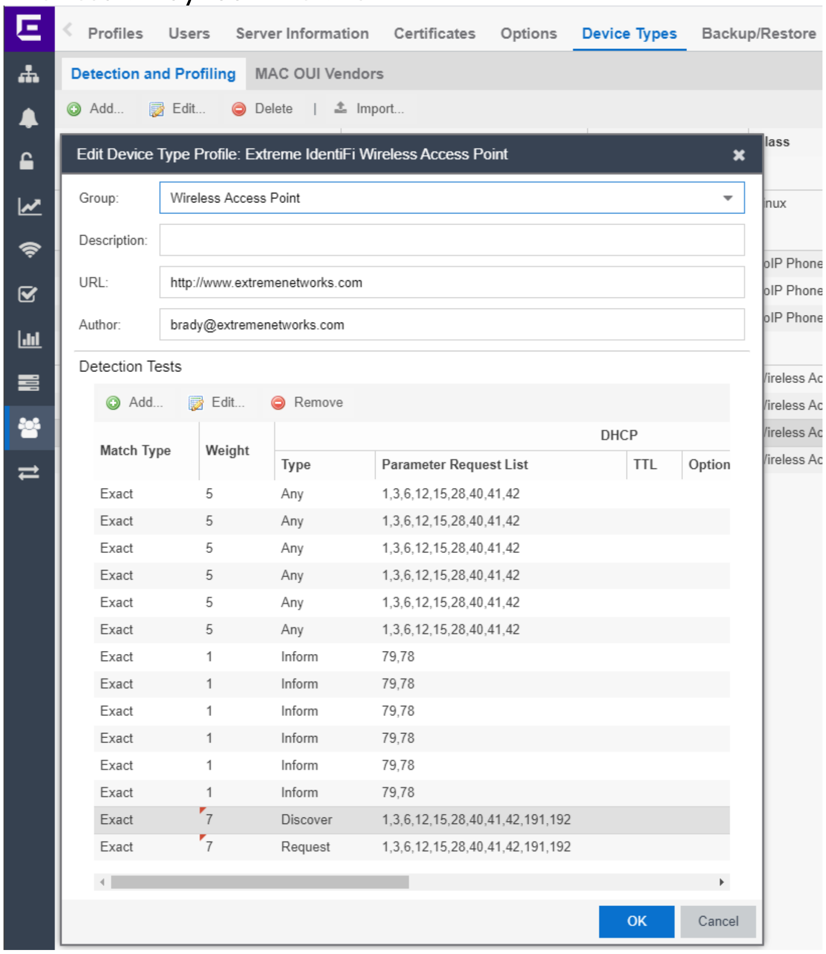
TTL:

Options:

Parameter Request List: 1,3,6,12,15,28,40,41,42,191,192

MAC OUI / Vendor:

- The result may look like this



Edit Device Type Profile: Extreme IdentiFi Wireless Access Point

Group: Wireless Access Point

Description:

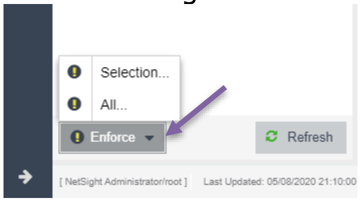
URL: http://www.extremenetworks.com

Author: brady@extremenetworks.com

Detection Tests

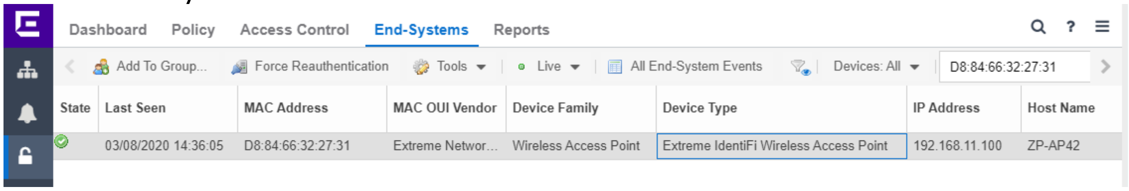
Match Type	Weight	DHCP			
		Type	Parameter Request List	TTL	Option
Exact	5	Any	1,3,6,12,15,28,40,41,42		
Exact	5	Any	1,3,6,12,15,28,40,41,42		
Exact	5	Any	1,3,6,12,15,28,40,41,42		
Exact	5	Any	1,3,6,12,15,28,40,41,42		
Exact	5	Any	1,3,6,12,15,28,40,41,42		
Exact	5	Any	1,3,6,12,15,28,40,41,42		
Exact	1	Inform	79,78		
Exact	1	Inform	79,78		
Exact	1	Inform	79,78		
Exact	1	Inform	79,78		
Exact	1	Inform	79,78		
Exact	1	Inform	79,78		
Exact	7	Discover	1,3,6,12,15,28,40,41,42,191,192		
Exact	7	Request	1,3,6,12,15,28,40,41,42,191,192		

- Enforce settings to Access Control Engines is needed. Control -> Access Control -> Enforce



[NetSight Administrator/root] Last Updated: 05/08/2020 21:10:00

- The result may look like



D8:84:66:32:27:31

State	Last Seen	MAC Address	MAC OUI Vendor	Device Family	Device Type	IP Address	Host Name
✓	03/08/2020 14:36:05	D8:84:66:32:27:31	Extreme Networ...	Wireless Access Point	Extreme IdentiFi Wireless Access Point	192.168.11.100	ZP-AP42

Document revision history

Date	Version	Changes Made	Author
2020/08/05	0.9	Initial draft	Zdeněk Pala