

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

©2020 Extreme Networks, Inc. All rights reserved.

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names are the property of their respective owners. All other registered trademarks, trademarks, and service marks are property of their respective owners. For additional information on Extreme Networks trademarks, see www.extremenetworks.com/company/legal/trademarks.

Contents

Use Case	.2
Gathering information needed for the fingerprint	.2
A3 how to	.4
ExtremeControl version 8.5 how to	.7
Document revision history	.9

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:

dhcpcapture.pcap					
File Edit View Go Capture Analyze Statistics Telephony	Wireless Tools Help				
📶 🗏 🖉 🕒 🔚 🛣 🗳 🔍 🗢 🗢 🕾 🐨 🕹 🜉 🗮					
Apply a display filter <ctrl-></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
2					
> Frame 1: 321 bytes on wire (2568 bits), 321 bytes cap	tured (2568 bits)				
> Ethernet 11, Src: ExtremeN_9e:/8:10 (00:04:96:9e:/8:1 Internet Dectoral Version 4, Sec. 102 168 11 1, Det.	0), Dst: Vmware_92:2c:23 (00:0c:29:92:2c:23)				
/ Internet Protocol Version 4, Src: 192.100.11.1, DSt: // User Datagram Protocol Src Port: 67 Dst Port: 67	192.100.150.90				
 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					
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: 0000000000000000	000				
Server host name not given					
Boot file name not given					
Augue Cookie: DHCP Message Type (Discover)					
> Option: (61) Client identifier					
> Option: (12) Host Name					
✓ Option: (57) Maximum DHCP Message Size					
Length: 2					
Maximum DHCP Message Size: 576					
✓ Option: (55) Parameter Request List					
Length: 11					
Parameter Request List Iter: (1) Subnet Mask					
Parameter Request List Iter: (6) Domain Name Se	rver				
Parameter Request List Iter: (0) Board Name					
Parameter Request List Iter: (15) Domain Name					
Parameter Request List Iter: (28) B oadcast Add	ress				
Parameter Request List Iter: (40) Network Infor	mation Service Domain				
Parameter Request List Iter: (41) N twork Infor	mation Service Servers				
Parameter Request List Iter: (42) N twork Time	Protocol Servers				
Parameter Request List Iter: (191) nassigned					
ndssigned					
					/
etworks, Inc. All rights reserved.					

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

dhcpcapture.pcap				
le Edit View Go Capture Analyze Statistics Telephony	y Wireless Tools Help			
(🔳 🖉 💿 📙 🛅 🗙 🕒 🍳 🗢 🗢 🕾 🕢 💆 🜉				
Apply a display filter <ctrl-></ctrl->				
. 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 0xbcd
2 2020-08-05 17:15:32,350752 192.168.11.1	192.168.130.90	DHCP		329 DHCP Request - Transaction ID 0xbcd
Frame 2: 329 bytes on wire (2632 bits), 329 bytes (captured (2632 bits)			
Ethernet II, SrC: Extremen_98:78:10 (00:04:90:98:78	5:10), DSC: VMWare_92:20:25 (00:00:29:92:20:25)			
User Datagram Protocol Src Port: 67 Dat Port: 67	1: 192.100.150.90			
Dynamic Host Configuration Protocol (Pequest)				
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: 000000000000000	00000			
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 (192.168.11.10)	90)			
> Option: (54) DHCP Server Identifier (192.168.130	0.2)			
✓ Option: (55) Parameter Request List				
Length: 11				
Parameter Request List Iter: (1) Subhet Mask				
Parameter Request List Item: (5) Rolter	Forward			
Parameter Request List Iter, (0) Donali Name	Sei vei			
Parameter Request List Iter, (12) Dirst Name				
Parameter Request List Iter: (15) Bundlin Name	ddress			
Parameter Request List Iter: (40) Network Inf	formation Service Domain			
Parameter Request List Iter: (41) Network Inf	formation Service Servers			
Parameter Request List Iter: (42) Network Tim	e Protocol Servers			
Parameter Request List Iter: (191) Inassigned				
Parameter Request List Item: (192) Unassigned				

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

ExtremeCloud IQ	A3 Status Reports Auditing Clients Users Configuration Tools
Q Filter	MAC d8:84:66:32:27:31
Search Create Import	Edit Info Fingerbank Timeline IPv4 3 IPv6 Location 6
Standard Searches Offline Clients Online Clients	Device Class Device Manufacturer
Device Groups	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
	Refresh Fingerbank

• 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



Insert the DHCP Fingerprint and hit Create



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

Filter	Fingerbank Profiling
Policies and Access Control	
Compliance	Client Change Detection Combinations Devices DHCP Fingerprints DHCP Vendors
Fingerbank Profiling	DHCPv6 Fingerprints DHCPv6 Enterprises MAC Vendors User Agents
Client Change Detection	
Combinations	Devices and All Local Linstream
Devices	
DHCP Vendors	
DHCPv6 Fingerprints	Q Search by identifier or client Clear Search
DHCPv6 Enterprises	
MAC Vendors	New Client 1000 \diamondsuit « < 1 > »
User Agents	
Scans	Identifier () Device () Created () Updated () Approved ()
Scan Engines	
WMI Rules	
Security Events	
Integration	NO Clients Touna
Advanced Access Configuration	Please refine your search.
Network Configuration	^
System Configuration	

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

New Fingerbank Client Device 🚾					
Name	Extreme Identifi AccessPoint				
Parent Device	Enterasys HiPath Wireless Access Point	Ŧ			
Create					

• <u>Hit New Combination in Configuration -> Compliance -> Fingerbank Profiling -> Combinations -> Local</u>

ExtremeCloud	A3 Status Reports Auditing Clients Users Configuration Tools 🖓 🕌 🕃 admin@local
Q Filter	Fingerbank Profiling
 Policies and Access Control Compliance Eingerbank Profiling 	Client Change Detection Combinations Devices DHCP Fingerprints DHCP Vendors
Client Change Detection Combinations Devices	Combinations real All Local Upstream
DHCP Fingerprints DHCP Vendors DHCPV6 Fingerprints	Q Search by identifier or client Clear Search
DHCPv6 Enterprises MAC Vendors User Agents	New Combination 25 ♀ « < 1 → »
Scan Engines WMI Rules	
Advanced Access Configuration ^	No local combinations found Please refine your search.
Network Configuration ^ System Configuration ^	

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



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

MAC d8:84:66:32:27:31 C								
Edit Info Fing	erbank Timeline IPv4 5 IPv6 Location 6 Se	curity Events						
Device Class	Extreme Identifi AccessPoint							
Device Type	Extreme Identifi AccessPoint							
Fully Qualified Device Name	Router, Access Point or Femtocell/Wireless Access Point/Enterasys WA HiPath Wireless Access Point/Extreme Identifi AccessPoint	P/Enterasys						
Score	75%							
Mobile	Unknown							
DHCP Fingerprint DHCP Vendor	1,3,6,12,15,28,40,41,42,191,192							
DHCPv6 Fingerprint								
DHCPv6 Enterprise								
Refresh Fingerbank								

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.



•

< Profiles	Users	Server Informat	tion Certificates	Options	Device	e Types	Backu
Detection a	nd Profiling	MAC OUI Ver	ndors				
O Add [🦻 Edit	\ominus Delete 🚢	Import				
Edit Device	Type Profil	e: Extreme Identif	Fi Wireless Access P	oint			×
Group:	Wireless A	Access Point					•
Description:							
URL:	http://www	extremenetworks.co	om				
Author:	brady@ex	tremenetworks.com					
Detection T	ests						
O Add	🔯 Edi	t 🥥 Remove					
Match Ty	/pe Wei	ght Type	Parameter Requ	est List	DHC	P TTL	Option
Match Ty	rpe Wei	ght Type Detection Test	Parameter Requ	est List	DHC	P TTL	Option
Match Ty Add E	ype Wei Device Type	ght Type Detection Test	Parameter Requ	est List	DHC	rp TTL X	Option
Match Ty Add D Match	ype Wei Device Type Type: Ex	ght Type Detection Test (act	Parameter Requ	est List	DHC	CP TTL X	Option
Match Ty Add D March Weigh	ype Wei Device Type Type: Ex t: 7 r Name:	ght Type Detection Test cact	Parameter Requ	est List	DHC	;P TTL ★	Option ¢
Match Ty Add D Match Weigh Vendo	ype Wei voice Type Type: Ex- t: 7 r Name: 1 voice 1	ght Type Detection Test cact	Parameter Requ	est List	DHC	P TTL X	Option Contraction
Match Ty Add D March Weigh Vendo Hostn	ype Wei Device Type Type: E t: 7 r Name: arm: 2	ght Type Detection Test cact	Parameter Requ	est List		P TTL *	Option
Match Ty Add D March Weigh Vendo Hostn DHCI	ype Wei Device Type Type: E t: 7 r Name: arti- a	ght Type Detection Test cact Discover	Parameter Requ	est List		CP TTL	Option
Match Ty Add E March Weigh Vendo Hostn DHCI Typ	ype Wei Device Type Type: ED t. 7 r Name: arfin a e:	ght Type Detection Test Cact Discover	Parameter Requ	est List		P TTL * Is Partia	Option C
Match Ty Add E Weigh Vendo Hostn DHCI Typ TTL	ype Wei Device Type Type: ED t: 7 r Name: antr: c e: c ions:	ght Type Detection Test Cact Discover	Parameter Requ	est List		P TTL 3 C Is Partia	Option
Match Ty Add D March Weigh Vendo Hostn DHCI Typ TTL Opt	ype Wei Device Type Type: E: t: 7 r Name: arth: c e: ions: ameter Requi	ght Type Detection Test Cact Discover Set 1,3,6,12,7	Parameter Requ	est List		CP TTL * Is Partial	Option

.

Profiles	Users Ser	ver Informatio	n Certificates Options	Device Types	Backup/Restor
Detection ar	nd Profiling	MAC OUI Vend	lors		
O Add	🦻 Edit 🥥 🛙	Delete 🏝 I	Import		
Edit Device	Type Profile: E	dreme IdentiFi	Wireless Access Point		× lass
Group:	Wireless Acces	s Point			• inux
Description:					
URL:	http://www.extre	emenetworks.com	n		oIP Ph
Author	brady@extrem	enetworks com			olP Ph
Detection T	aete				
Detection	ESIS				/ireless
J Add.	👔 Edit	Remove		DUCD	/ireless
Match Ty	pe Weight	Tune	Decementes De muset List	DHCP	Ontine (ireless
Event	5	Туре	Parameter Request List	IIL	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	Anv	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



• The result may look like

		are may io							
Ε	Das	hboard Policy	Access Control	nd-Systems F	Reports			Q ?	≡
#	< 1	🔏 Add To Group	Force Reauthentication	n 🎲 Tools 🔻	◎ Live 👻 🔲 All E	nd-System Events 🛛 🖓 🛛 Devices: All	▼ D8:84:66:32	2:27:31	>
	State	Last Seen	MAC Address	MAC OUI Vendor	Device Family	Device Type	IP Address	Host Nan	ne
6	0	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