

ExtremeNAC/A3

Addressing MAC Address Randomization

Abstract: This guide details options for using ExtremeNAC/A3 with MAC address randomization.

Published: October 2020, version 1.2.1

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

About MAC randomization	3
Expected Impact of MAC Randomization on Current NAC Installations	3
How to Recognize a Randomized MAC Address?	4
What Options are Available?	4
Deny Access to Devices with Randomized MAC Addresses	5
User Experience When Denied access	8
Assign Guest Access to Devices with Randomized MAC Addresses	9
Assign Captive Portal Workflow1	.2
Resources1	.4

/ 2

About MAC randomization

- In response to these privacy vulnerabilities, most OSs—including Android, iOS, and Windows—began to implement their own variant of MAC address randomization while probing the Wi-Fi network. This probe mode guarantees anonymity until the client gets associated with an access point. IEEE 802.11 also stepped up to specify a similar feature in the IEEE 802.11aq Pre-Association Service Discovery amendment to the 802.11-2016 standard.
- More recently, OSs have started to implement the use of MAC address randomization for device association to the network. The address is kept consistent per network (i.e., Service Set Identifier [SSID]), so the user does not have to authenticate each time it connects to the same SSID.
- In Google Android versions 10 and 11
 - MAC address randomization is enabled by default.
 - Randomization can be disabled per network profile (SSID).
 - Random MAC addresses are persistent per SSID. The same random MAC address is used even if the network profile is deleted and recreated.
- In Apple iOS 14, watchOS 7, and iPadOS 14
 - MAC address randomization is enabled by default.
 - Randomization can be disabled per network profile (SSID).
 - Random MAC addresses are persistent per SSID. The same random MAC address is used even if the network profile is deleted and recreated.
 - MAC address randomization is enabled for all existing network profiles upon OS upgrade.
- In Microsoft Windows 10
 - MAC address randomization is disabled by default.
 - Randomization can be enabled both per network profile (SSID) and globally for all wireless profiles.
 - Random MAC addresses are persistent per SSID. The same random MAC address is used as long as the user does not delete the network profile.

Expected Impact of MAC Randomization on Current NAC Installations

- The list of MAC addresses in the NAC configuration may need to be updated after an endpoint is upgraded to the new OS that has MAC randomization enabled.
- There should not be a significant impact on licensing:
 - ExtremeNAC/AC calculates active sessions. The physical MAC and randomized MAC will not be active at the same time.
- Search for end-systems will return both physical and randomized MACs.

- If integration between NAC and MDM (or similar 3rd party solutions) systems is used, then the Randomization should be disabled. The MDM usually reports the physical MAC, but physical MAC is not seen in the network if the Randomization is enabled.
- A majority of customers will not see a significant impact of MAC address randomization in their standard NAC deployments.

How to Recognize a Randomized MAC Address?

MAC address randomization uses locally administered addresses. Universally administered and locally administered addresses are distinguished by setting the second-least-significant bit of the first octet of the address. This bit is also referred to as the U/L bit, short for Universal/Local, which identifies how the address is administered. If the bit is 1, the address is locally administered. The table below shows which MAC addresses are considered local MAC addresses.

Local MAC ranges	
x 2 - xx - xx - xx - xx - xx	$x\mathbf{A} - xx - xx - xx - xx - xx$
x6 - xx - xx - xx - xx - xx	$x\mathbf{E} - xx - xx - xx - xx - xx$

What Options are Available?

- Default approach
 - Treat devices with randomized MAC and unique MAC the same.
- Assign different captive portal workflow
 - $_{\odot}$ $\,$ The user will be redirected to the captive portal and provided with instructions.
 - See chapter: Assign Captive Portal Workflow
- Deny access to devices with randomized MAC addresses
 - The user will not get network access. The user is presented with captive portal message.
 - See chapter: Deny Access to Devices with Randomized MAC Addresses
- Permit access to devices with randomized MAC addresses
 - The user will be presented Acceptable use Policy.
 - See chapter: Assign Guest Access to Devices with Randomized MAC Addresses

Deny Access to Devices with Randomized MAC Addresses

The device with a randomized MAC address will be assigned a custom Authentication Source. This Authentication Source will provide the user with customized captive portal content.

- Create new Exclusive Authentication Source.
 - Click Configuration -> Policies and Access Control -> Authentication Sources -> New Exclusive Source
 Blackhole.

	usive Sources		
New	Name	Description	Туре
1	BlackholeSource	Detected Randomized MAC address. Please disable MAC address randomization and connect again.	Blackhole

The Description will be displayed to the user in the captive portal.

- Create new Root Portal Module.
- Click Configuration ->Advanced Access Configuration -> Portal Modules -> New Root Module
 - Add module default_blackhole_policy

Þ	ExtremeCloud	™ A ³	Status	Reports	Auditing	Clients	Users	Configuratio	n Tools
٩	Filter		New F	Portal N	/lodule (Root			
	Policies and Access Control	~							
Ð	Compliance	~					Name	BlackListed	Nodule
÷.	Integration	~							
自	Advanced Access	~				Des	cription	Black Listeo	
_	Configuration							The description s	nown to users.
	Captive Portal								
	Filter Engines					N	lodules	1	default_blackhole_policy
	Billing Tiers								
	PKI Providers								
	Provisioners								
	Portal Modules		Create	Reset	t				
	Access Duration								

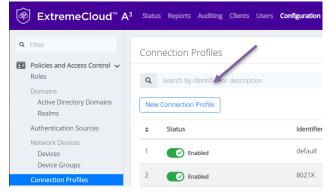
- Change the Refuse Login behavior (step 2).
 - Click Configuration ->Advanced Access Configuration -> Portal Modules -> BlackListed >Refuse Login -> edit.

Portal Mo	dules		
BlackListed	Default pending policy	Default portal policy	Nev
	step 1	step 2	
•	• Root	× ×	
	llackListed		

• Select the Authentication Source created in the previous step.

¢)ExtremeCloud [™] A	³ Status Reports Auditing Clients Users	Configuration Tools
۹	Filter	Portal Module default_blackhol	e_policy (Authentication:Choice)
⊡ €	Policies and Access Control	Name	default_blackhole_policy
Ê	Advanced Access Configuration Captive Portal Filter Engines	Description Mandatory Fields	Refuse Login The description shown to users.
	Billing Tiers PKI Providers Provisioners Portal Modules	Fields to Save	The additional fields that should be required for registration. The fields to be saved throughout the registration process.
~	Access Duration Self Service Portal Network Configuration	Template	content-with-choice.html Add Action If no actions are specified, the default action of the module will be used.
¢ŝ	System Configuration	Modules	Add Module
		Authentication Sources	1 BlackholeSource The sources to use in the module. If no sources are specified, all the sources of the connection profile will be used.
		Sources by Class	pf::Authentication::Source::BlackholeSource
		Sources by Type	
		Sources by Authentication Class	The sources of these types and part of the connection profile will be added to the available sources
		Save Reset Clone	The sources of these authentication classes and part of the connection profile will be added to the available sources

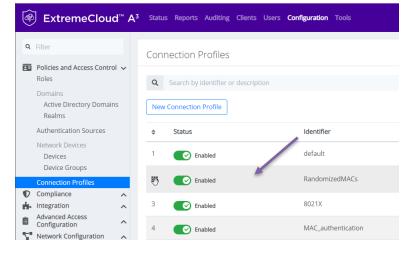
- Create a Connection profile for randomized MACs.
 - Click Configuration -> Policies and Access Control -> Connection Profiles -> New Connection Profile.



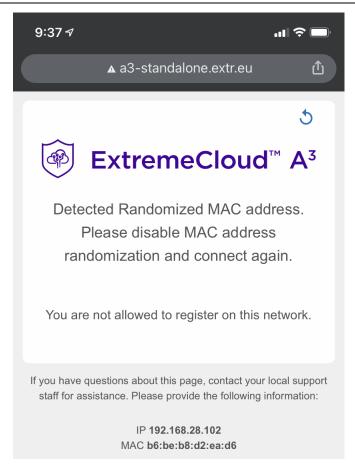
- In the profile disable all options except:
 - Enable Profile: yes
 - Root Portal Module: BlackListed
 - Define Advanced Filter as:
 - mac =~ "[0-9,A-F,a-f][2,6,A,E]:[0-9,A-F,a-f][0-9,A-F,a-f]:[0-9,A-F,a-f][0-9,A-F,a-f]:[0-9,A-F,a-F,a-F]:[0-9,A-F,a-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F]:[0-9,A-F]:[0-9,A-F]:[0-9,A-F]:[0-9,A-F]:[0-9,A-F]:[0-9,A-F]:[0-9,A-F]:[0-9,A-F]:[0-9,A-F]:[0-9,A-F]:[0-9,A-F]:[0-9,A-F]:[0-9

🛞 Extreme	Cloud [™] A	3 Status Ro	ports Auditing	Clients User	s Configuration	Tools		
Q Filter		Connect	ion Profile R	Randomize		~ C		
Policies and Acces Roles	ss Control 🗸	Settings	Captive Portal	Files				
Domains Active Directory Realms	/ Domains			Profile Name		ACs contaipalphanumeric chara		
Authentication So	urces		F	Profile Description	Access for Ray	domized MACs		
Network Devices Devices Device Groups				Enable Profile				
Connection Profile Compliance	es 🔨		R	oot Portal Module	BlackListed	ule to use		
Filters	any							.
Filter	Add Filter	With no filter speci	îed, an advanced filte	er must be specified	L			
Advanced Filter	mac =~ "[0-9 f][0-9,A-F,a-f),A-F,a-f][2,6,A,E]]"	:[0-9,A-F,a-f][0-9,A	A-F,a-f]:[0-9,A-F,	a-f][0-9,A-F,a-f]:[0-!	9,A-F,a-f][0-9,A-F,a-f]:[0	-9,A-F,a-f][0-9,A-F,a	a-f]:[0-9,A-F,a-
Sources	Add Source	If no source is sp	ecified, all internal an	id external sources	are used.			4
Billing Tiers	Add Billing 1	ier If no billing t	iers are specified, all l	billing tiers are use	d.			
Provisioners	Add Provisio	oner If no provis	ioners are specified, t	the provisioners in t	the default profile are u	used.		
Scanners	Add Scanne	r If no scanners	are specified, scannin;	g is not be perform	ed.			
Self service policy								-

• Reorder the connection profiles based on your need.



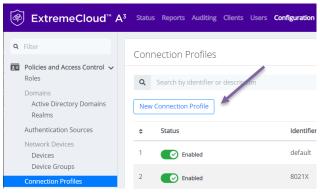
User Experience When Denied access



Assign Guest Access to Devices with Randomized MAC Addresses

The device with a randomized MAC address is automatically assigned Guest Access after Acceptable Use Policy is accepted.

- Create Connection profile for randomized MACs.
- Click Configuration -> Policies and Access Control -> Connection Profiles -> New Connection Profile.



- In the profile disable all options except:
 - Enable Profile: yes
 - Root Portal Module: Default portal policy (the guest will be given Acceptable Use Policy)
 - Automatically Register Clients = yes
 - Define Advanced Filter as:
 - mac =~ "[0-9,A-F,a-f][2,6,A,E]:[0-9,A-F,a-f][0-9,A-F,a-f]:[0-9,A-F,a-f][0-9,A-F,a-f][0-9,A-F,a-f]:[0-9,A-F,a-f]:[0-9,A-F,a-f]:[0-9,A-F,a-f]"
 - Sources = null

🖗 Extre	meCloud™	A ³ Status	Reports Auditing	Clients User	s Configuration Tools
Q Filter		Conne	ection Profile R	Randomize	
Policies and Roles	Access Control 🥆			Files	
Domains Active Din Realms	ectory Domains		_	Profile Name	RandomizedMACs Profile IDs may only contage alphanumeric characters, dashes, periods, and underss.
Authenticati Network De			Ρ	Profile Description	Automatically register Randomized MACs
Devices Device Gr	oups			Enable Profile	
Connection Compliance			Ro	oot Portal Module	Default portal policy The Root Portal Module to use.
 Integration Advanced Advanced Advanced Advanced Configuration Network Control 	on 🖌		Activa	ate Preregistration	If enabled, a local accouncreated during registration is displayed instead of to the enable "Create local account" on all the sources associated with this connection pro
System Con	0		Automatical	lly Register Clients	Automatically register clients for this profile. Clients will not be shown a captive port authentication.
Filters	any				Ÿ
Filter	Add Filter Wi	th no filter specified,	an advanced filter must b	be specified.	
Advanced Filter	mac =~ "[0-9,A- f][0-9,A-F,a-f]"	F,a-f][2,6,A,E]:[0-	9,A-F,a-f][0-9,A-F,a-f]:	:[0-9,A-F,a-f][0-9	,A-F,a-f]:[0-9,A-F,a-f][0-9,A-F,a-f]:[0-9,A-F,a-f][0-9,A-F,a-f]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F,a-F]:[0-9,A-F]:[0-9
Sources	1 ni	ll			- 00
Billing Tiers	Add Billing Tier	If no billing tiers	are specified, all billing tie	ers are used.	
Provisioners	Add Provisione	r If no provisione	ers are specified, the provi	isioners in the defau	ult profile are used.
Scanners	Add Scanner	If no scanners are s	specified, scanning is not b	be performed.	
elf service policy					*

• Reorder the connection profiles based on your need.

(Providence) (Prov	ExtremeCloud	d™ A³	Status	Reports Auditing C	Clients Users Configuration	Tools						
٩	Filter		Conn	ection Profiles								
	Policies and Access Contro Roles		Search by Identifier or description									
	Domains Active Directory Domain Realms	s	New (New Connection Profile								
	Authentication Sources		\$	Status	Identifier		Description					
	Network Devices Devices		1	Enabled	default		Default Profile					
	Device Groups Connection Profiles		15	Enabled	Randomiz	edMACs	Automatically register Randomized MACs					
€ E	Compliance Integration	^	3	Enabled	8021X		Dot1x profile wired and wireless					
Ê	Advanced Access Configuration	^	4	Enabled	MAC_auth	entication	Mac Authentication					
	Network Configuration	~										

• The Guest role and behavior is defined in the source.

Click Configuration -> Policies and Access Control -> Authentication Sources -> External Sources -> null

(a)	Extreme	Clou	d [™] A ³ Status Reports Auditin	ig Clients	Users	Config	juration Tools		API dashboar	0	1	admin@local
٩	Filter		Authentication Source nu	II Null								×
	Policies and Access Control Roles	~	Name	null								
	Domains		Description	Null Source								
	Active Directory Domains Realms		Email Required									
	Authentication Sour	ces	Authentication Rules	1 📀	catchal	ll (catcl	hall)					0 0
	Network Devices			N	lame	catchal	I					
	Devices Device Groups			Descri	intion	catchal						
				Descri	ipiion	catchai						
	Connection Profiles Compliance			Mat	tches	All						~
÷.	Integration			Condi	itions	Add Co	ondition					
	Advanced Access								le la			
Ê	Configuration	^		AC	tions	1	Role	~	guest			- 0 0
1	Network Configuration	^				2	Access duration	Ŧ	1 day			- 00
\$00	System Configuration	^										

Assign Captive Portal Workflow

The device with a randomized MAC address is automatically assigned a custom captive portal workflow. The Role can be assigned in the Authentication Source. The Authentication Source is referenced in the Captive Portal configuration.

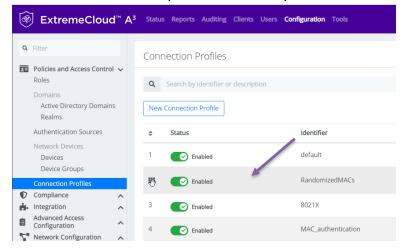
- Create a new Root Portal Module.
 - Click Configuration -> Advanced Access Configuration -> Portal Modules -> New Root Module.
 Configure the desired workflow.
- Create a Connection profile for randomized MACs.
- Click Configuration -> Policies and Access Control -> Connection Profiles -> New Connection Profile.

€ ExtremeCloud [™] A ³	Statu	is Reports	Auditing	Clients	Users	Configuration
 Q. Filter Image: Policies and Access Control ↓ 	Con	nection I	Profiles		,	
Roles Domains Active Directory Domains Realms	Q Nev	Search by Connection	identifier o	r descript	tion	
Authentication Sources	\$	Status				Identifier
Network Devices Devices Device Groups	1	💽 Er	nabled			default
Connection Profiles	2	💽 Er	nabled			8021X

- In the profile disable all options except:
 - Enable Profile: yes
 - Root Portal Module: choose the portal behavior you created in previous step
 - Define Advanced Filter as:
 - $\circ \quad \max = \sim "[0-9, A-F, a-f][2, 6, A, E]: [0-9, A-F, a-f][0-9, A-F, a-f]: [0-9, A-F, a-f][0-9, A-F, a-f][0-9, A-F, a-f]: [0-9, A-F, a-F]: [0-9$

🖗 Extreme	Cloud [™] A	³ Status Reports Auditing Clients Users	Configuration Tools
Q Filter		Connection Profile Randomized	IMACs Preview 🗗
Policies and Acces Roles	ss Control 🗸	Settings Captive Portal Files	
Domains Active Director Realms	y Domains	Profile Name	RandomizedMACs Profile IDs may only contaignalphanumeric characters, dashes, periods, and under
Authentication So Network Devices		Profile Description	Access for Randomized MACs
Devices Device Groups		Enable Profile	
Connection Profil Compliance	les	Root Portal Module	default_policy
Advanced Access	^	Activate Preregistration	Default portal policy
Configuration Configuration Network Configura System Configura	ration 🔨	Automatically Register Clients	Default pending policy BlackListed
Filters			Automatically contents climate for this profile. Climate will only be chosen a continue or ${\bf v}$
Filter	Add Filter	With no filter specified, an advanced filter must be specified.	
Advanced Filter	mac =~ "[0-9, f][0-9,A-F,a-f]		f][09,A-F,a-f]:[09,A-F,a-f][09,A-F,a-f]:[09,A-F,a-f][09,A-F,a-f]:[09,A-F,a-F]:[09,A-F]:[00
Sources	Add Source	If no source is specified, all internal and external sources are	e used.
Billing Tiers	Add Billing Ti	If no billing tiers are specified, all billing tiers are used.	
Provisioners	Add Provision	ner If no provisioners are specified, the provisioners in the	a default profile are used.
Scanners	Add Scanner	If no scanners are specified, scanning is not be performed.	L
Self service policy			*

• Reorder the connection profiles based on your need.



Resources

• https://en.wikipedia.org/wiki/MAC_address