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

P/N XXXXX-XX

Contents

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**A** – xx – xx – xx – xx – xx
x**6** – xx – xx – xx – xx – xx	x**E** – xx – xx – xx – xx – xx

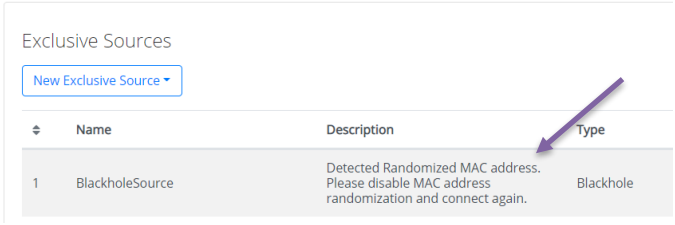
What Options are Available?

- Default approach
  - Treat devices with randomized MAC and unique MAC the same.
- Assign different captive portal workflow
  - 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

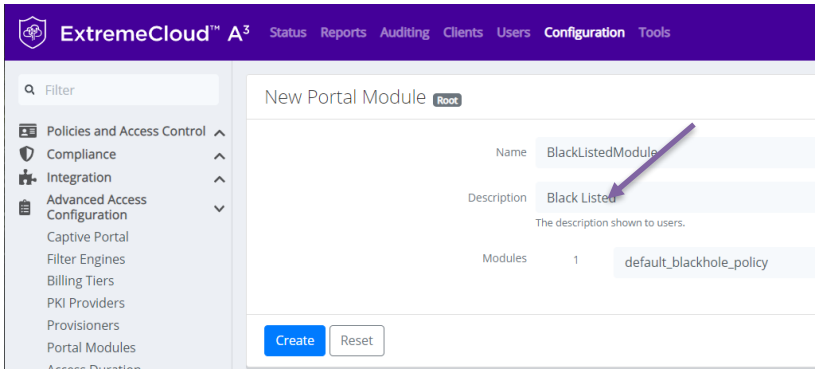
The device with a randomized MAC address will be assigned a custom Authentication Source. This Authentication Source will provide the user with customized captive portal content.

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

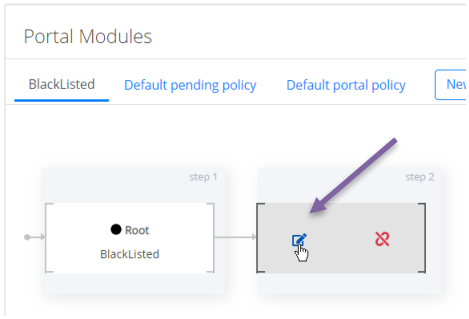


The Description will be displayed to the user in the captive portal.

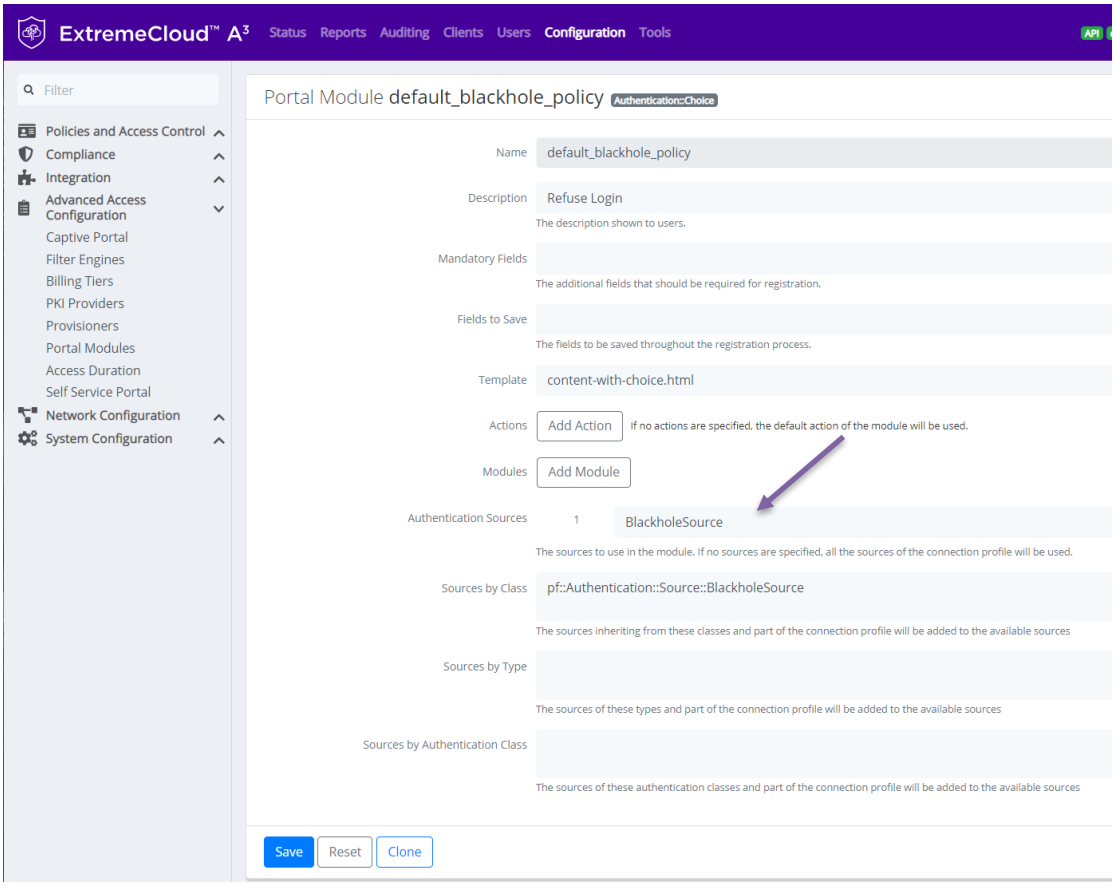
- Create new Root Portal Module.
  - Click Configuration ->Advanced Access Configuration -> Portal Modules -> New Root Module
    - Add module default_blackhole_policy



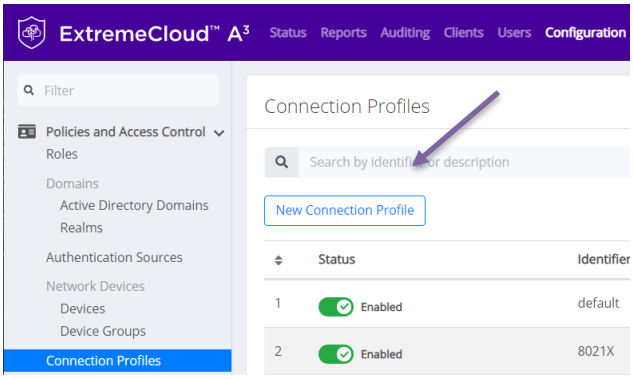
  - Change the Refuse Login behavior (step 2).
    - Click Configuration ->Advanced Access Configuration -> Portal Modules -> BlackListed ->Refuse Login -> edit.



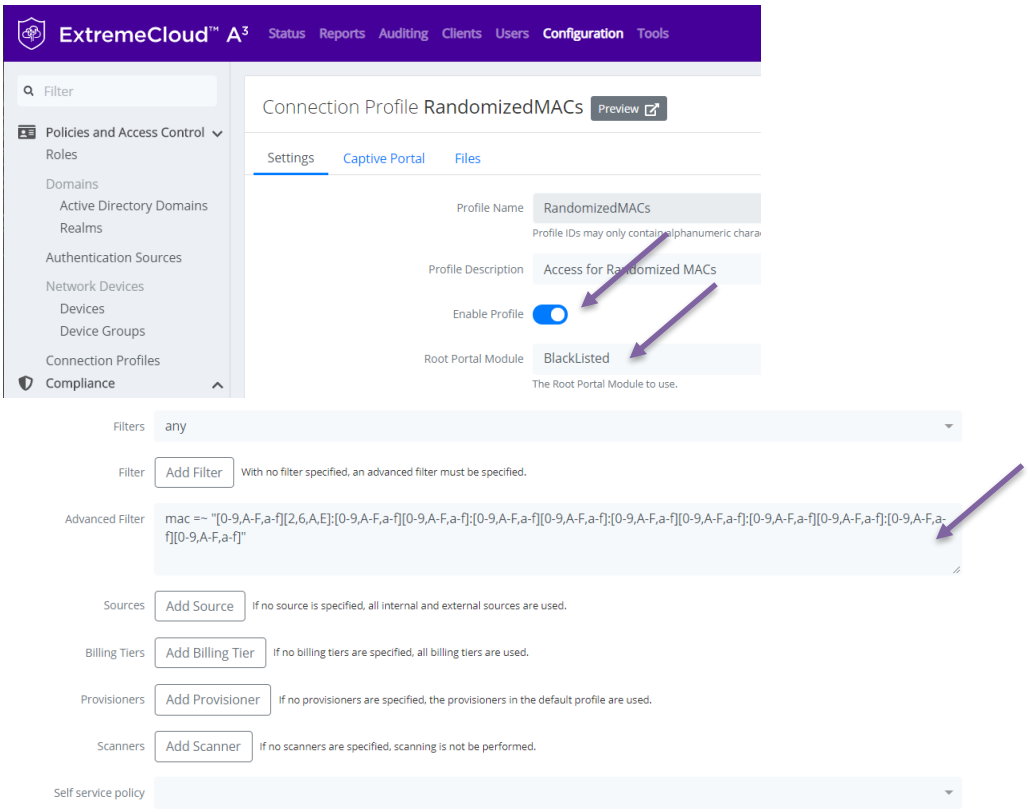
- Select the Authentication Source created in the previous step.



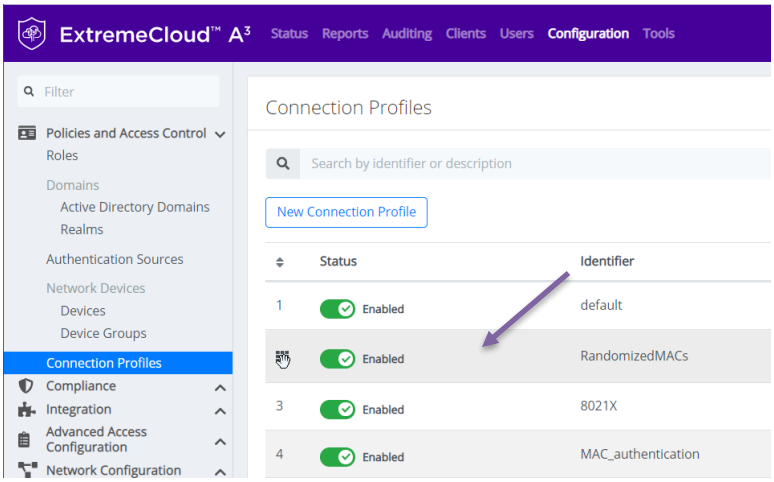
- Create a Connection profile for randomized MACs.
  - Click Configuration -> Policies and Access Control -> Connection Profiles -> New Connection Profile.



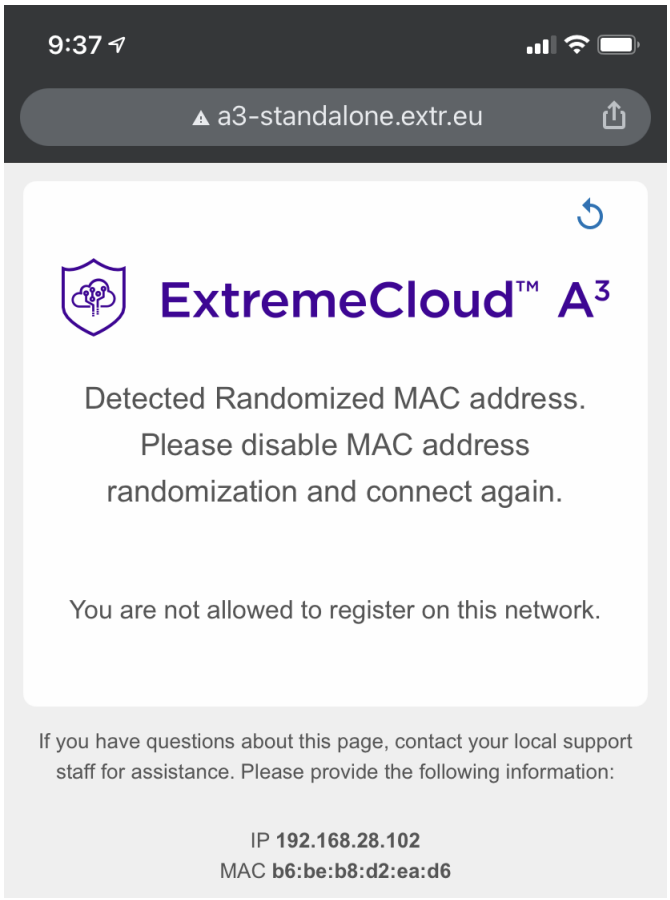
    - In the profile disable all options except:
      - Enable Profile: yes
      - Root Portal Module: BlackListed
      - Define Advanced Filter as:
        - mac =~ "[0-9,A-F,a-f][2,6,A,E]:[0-9,A-F,a-f][0-9,A-F,a-f]:[0-9,A-F,a-f][0-9,A-F,a-f]:[0-9,A-F,a-f][0-9,A-F,a-f]:[0-9,A-F,a-f][0-9,A-F,a-f]:[0-9,A-F,a-f][0-9,A-F,a-f]:[0-9,A-F,a-f][0-9,A-F,a-f]"



- Reorder the connection profiles based on your need.



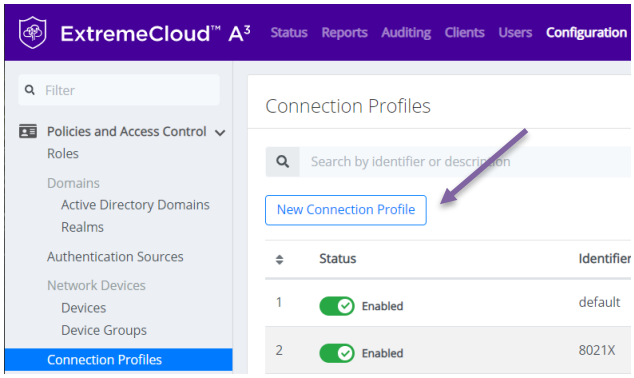
User Experience When Denied access



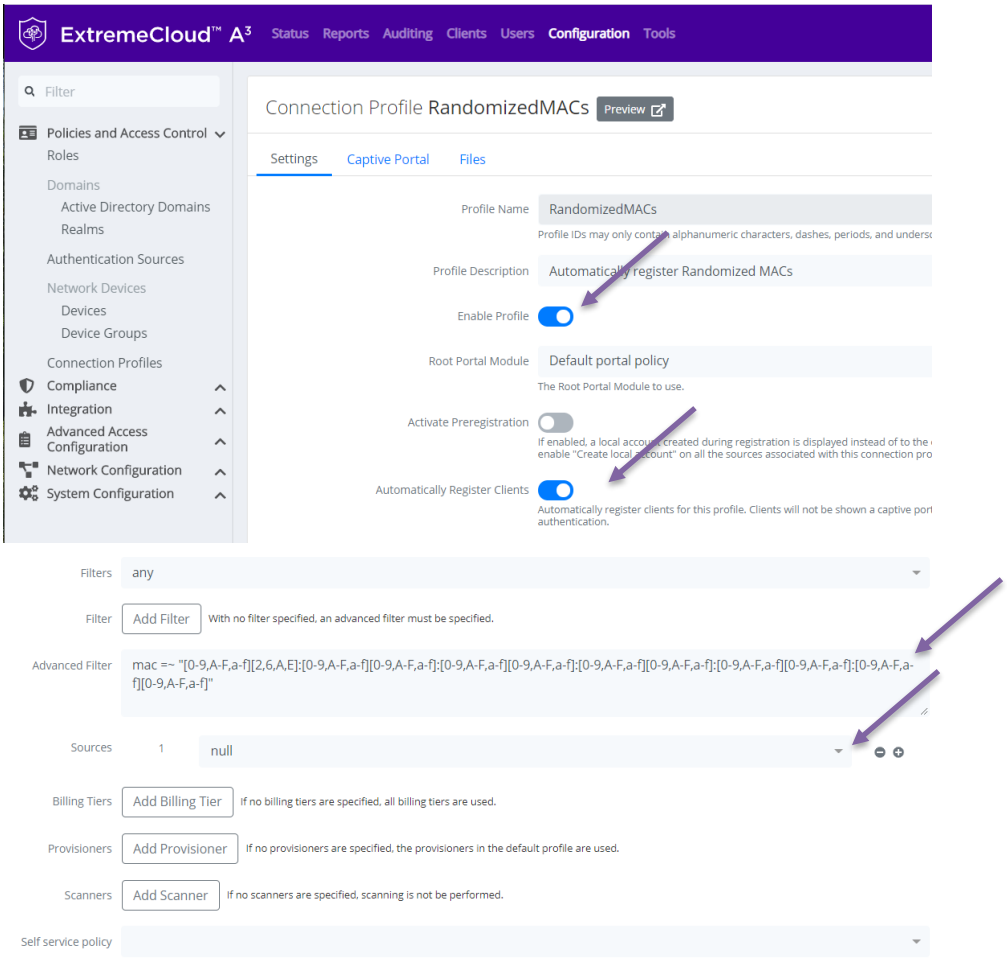
Assign Guest Access to Devices with Randomized MAC Addresses

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

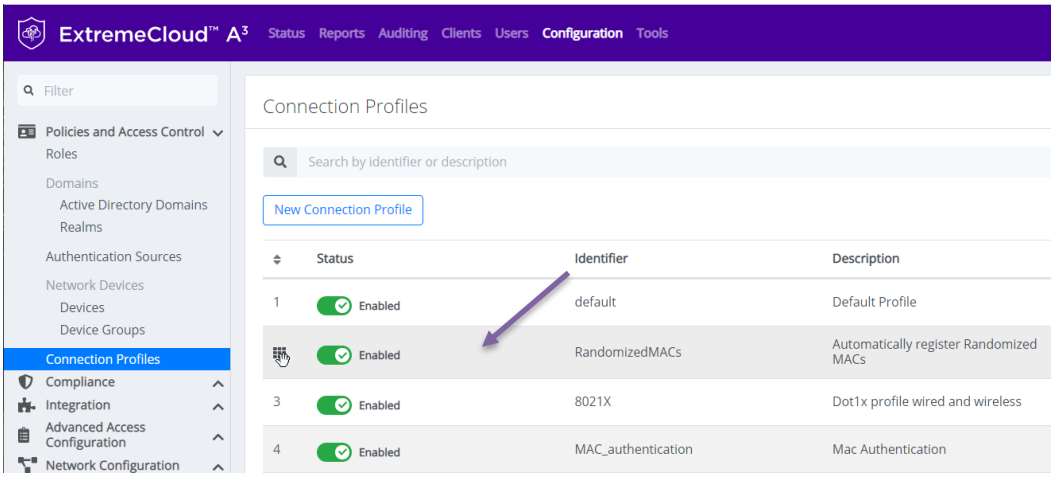
- Create Connection profile for randomized MACs.
  - Click Configuration -> Policies and Access Control -> Connection Profiles -> New Connection Profile.



    - 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]:[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

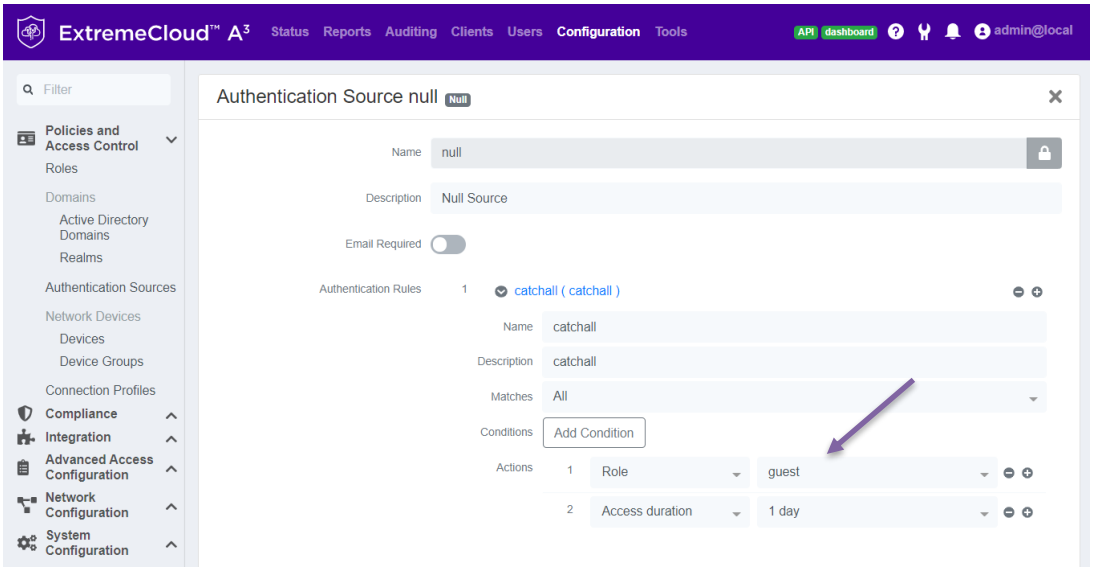


- Reorder the connection profiles based on your need.



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

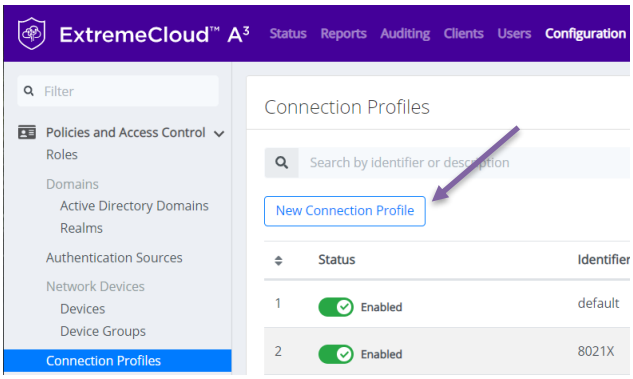
– Click Configuration -> Policies and Access Control -> Authentication Sources -> External Sources -> null



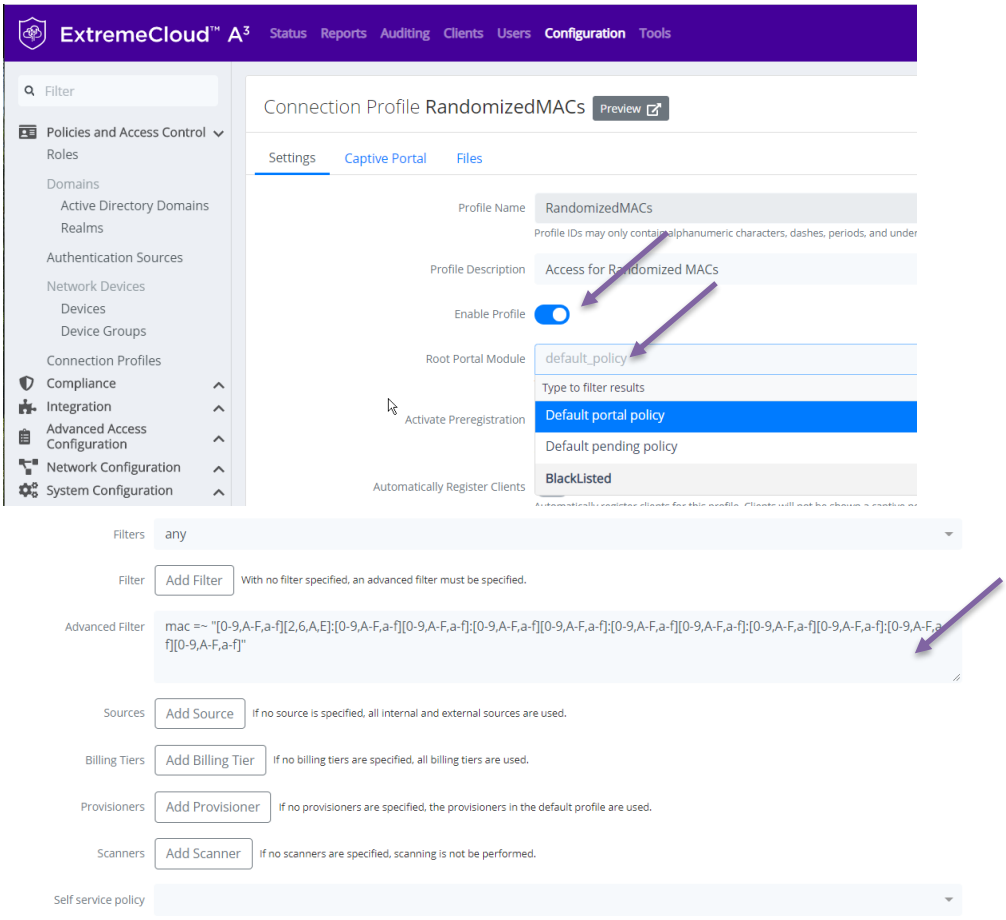
Assign Captive Portal Workflow

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.

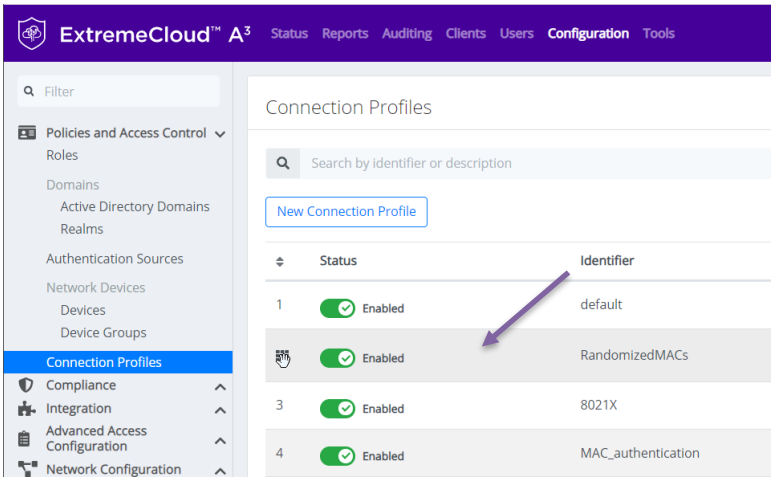
- Create a new Root Portal Module.
  - Click Configuration ->Advanced Access Configuration -> Portal Modules -> New Root Module. Configure the desired workflow.
- Create a Connection profile for randomized MACs.
  - Click Configuration -> Policies and Access Control -> Connection Profiles -> New Connection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



    - 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:
        - 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]:[0-9,A-F,a-f][0-9,A-F,a-f]:[0-9,A-F,a-f][0-9,A-F,a-f]"



- Reorder the connection profiles based on your need.



Resources

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