Configure Anomalous Endpoint Detection and Enforcement on ISE 2.2

Contents

Introduction

This document describes Anomalous Endpoint Detection and Enforcement. This is a new Profiling feature introduced in Cisco Identity Services Engine (ISE) for enhanced network visibility.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Wired MAC Authentication Bypass (MAB) configuration on the switch
- Wireless MAB configuration on Wireless LAN Controller (WLC)
- Change of Authorization (CoA) configuration on both devices

Components Used

The information in this document is based on these software and hardware versions:

1. Identity Services Engine 2.2
2. Wireless LAN Controller 8.0.100.0
3. Cisco Catalyst Switch 3750 15.2(3)E2

4. Windows 10 with wired and wireless adapters

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

ISE can detect endpoints that are involved in MAC address spoofing. Once it has been detected, ISE can take action (with CoA) and enforce certain policies to restrict access of the suspicious endpoint.

Once detection is enabled, ISE monitors any new information received for existing endpoints and checks if these attributes have changed:

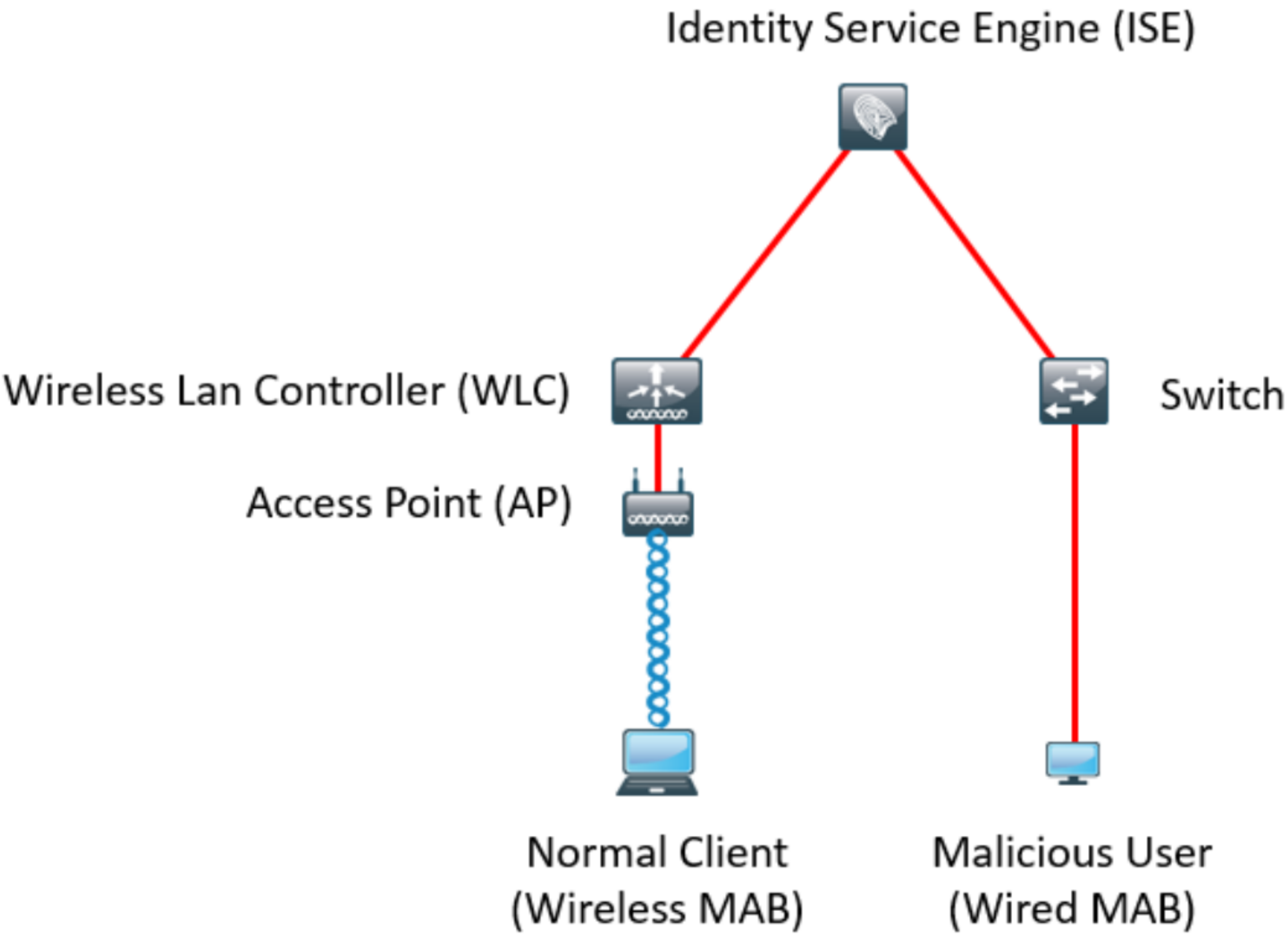
1. **NAS-Port-Type** - Determines if the access method of this endpoint has changed. For example, if the same MAC address that connected via Wired Dot1x has been used for Wireless Dot1x and visa-versa.
2. **DHCP Class ID** - Determines whether the type of client/vendor of endpoint has changed.
3. **Operating System -** Significant OS changes such as Windows to Apple iOS.
4. **Endpoint Policy -** Significant profile changes. For example, a change from Phone or Printer to PC.

Once ISE detects one of the changes mentioned above, the AnomalousBehaviour attribute is added to the endpoint and set to True. This can be used later on as a condition in Authorization policies to restrict access for the endpoint in future authentications.

If Enforcement is configured, ISE can send a CoA once the change is detected to re-authenticate or perform a port bounce for the endpoint. If in effect, it can quarantine the anomalous endpoint depending on the Authorization policies that were configured.

Configure

Network Diagram

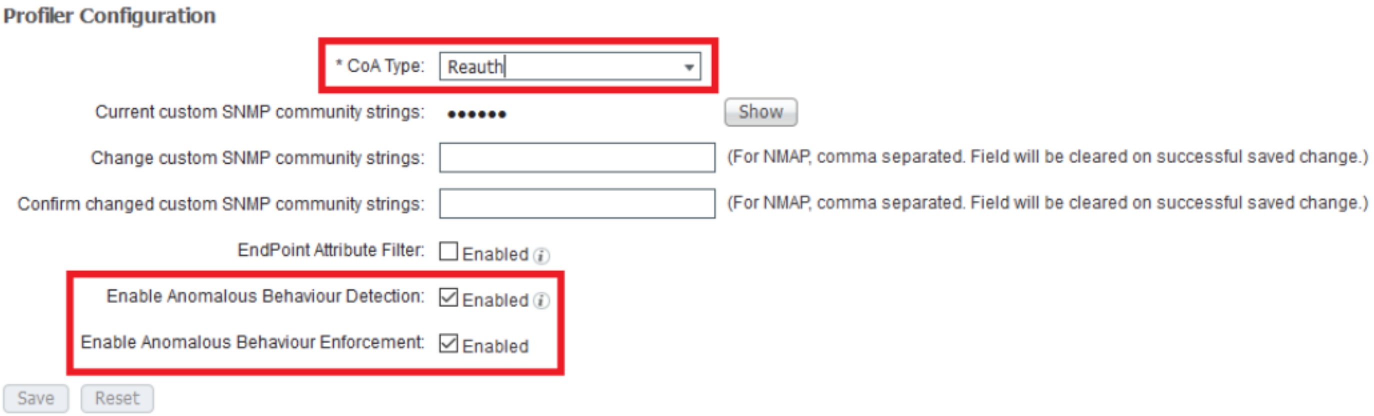

Identity Service Engine (ISE)
Wireless Lan Controller (WLC)
Switch
Access Point (AP)
Normal Client (Wireless MAB)
Malicious User (Wired MAB)

Configurations

Simple MAB and AAA configurations are performed on the switch and WLC. To utilize this feature, follow these steps:

Step 1. Enable Anomalous Detection.

Navigate to **Administration > System > Settings > Profiling**.



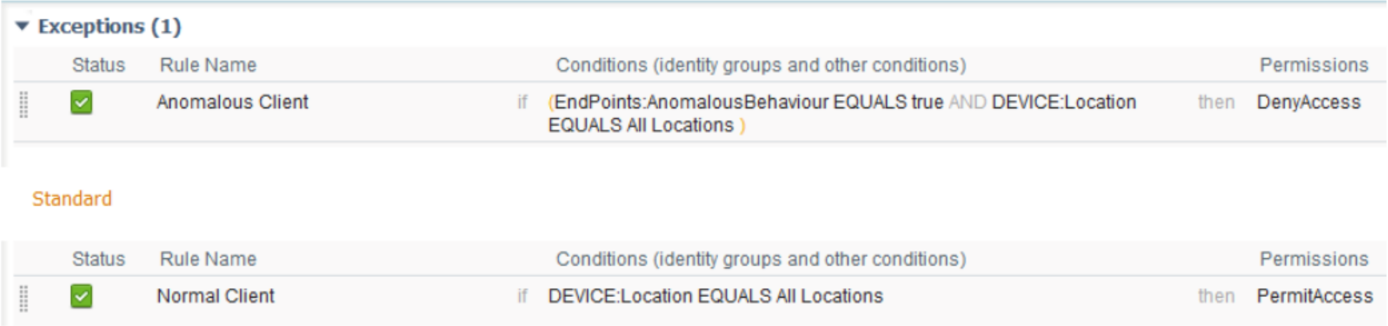
Profiler Configuration

* CoA Type:	Reauth
Current custom SNMP community strings:	•••••• Show
Change custom SNMP community strings:	(For NMAP, comma separated. Field will be cleared on successful saved change.)
Confirm changed custom SNMP community strings:	(For NMAP, comma separated. Field will be cleared on successful saved change.)
EndPoint Attribute Filter:	□ Enabled
Enable Anomalous Behaviour Detection:	☑ Enabled
Enable Anomalous Behaviour Enforcement:	☑ Enabled

First option allows ISE to detect any anomalous behavior but no CoA is sent (Visibility-Only Mode). Second option allows ISE to send CoA once anomalous behaviour is detected (Enforcement Mode).

Step 2. Configure Authorization policy.

Configure the Anomlousbehaviour attribute as a condition in the Authorization policy, as shown in the image:



▾ Exceptions (1)

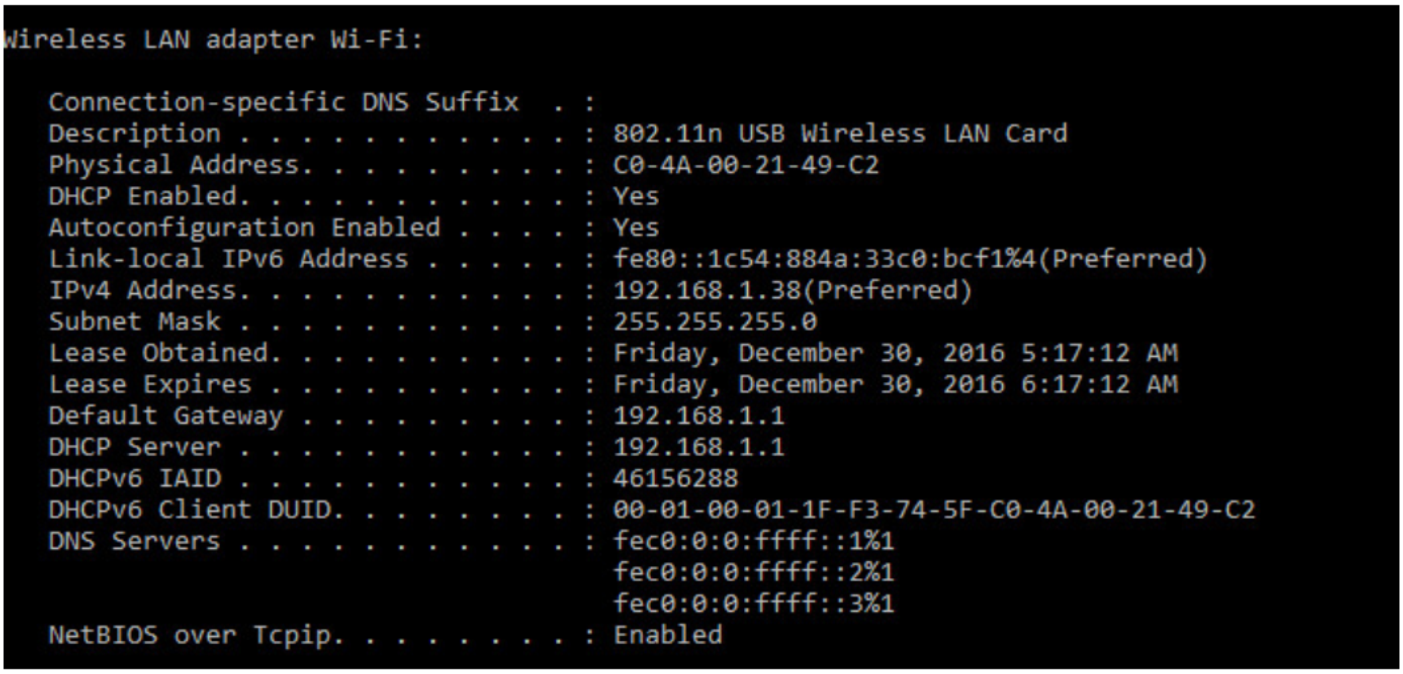
Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
☑	Anomalous Client	if	(EndPoints:AnomalousBehaviour EQUALS true AND DEVICE:Location EQUALS All Locations)	then	DenyAccess

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
☑	Normal Client	if	DEVICE:Location EQUALS All Locations	then	PermitAccess

Verify

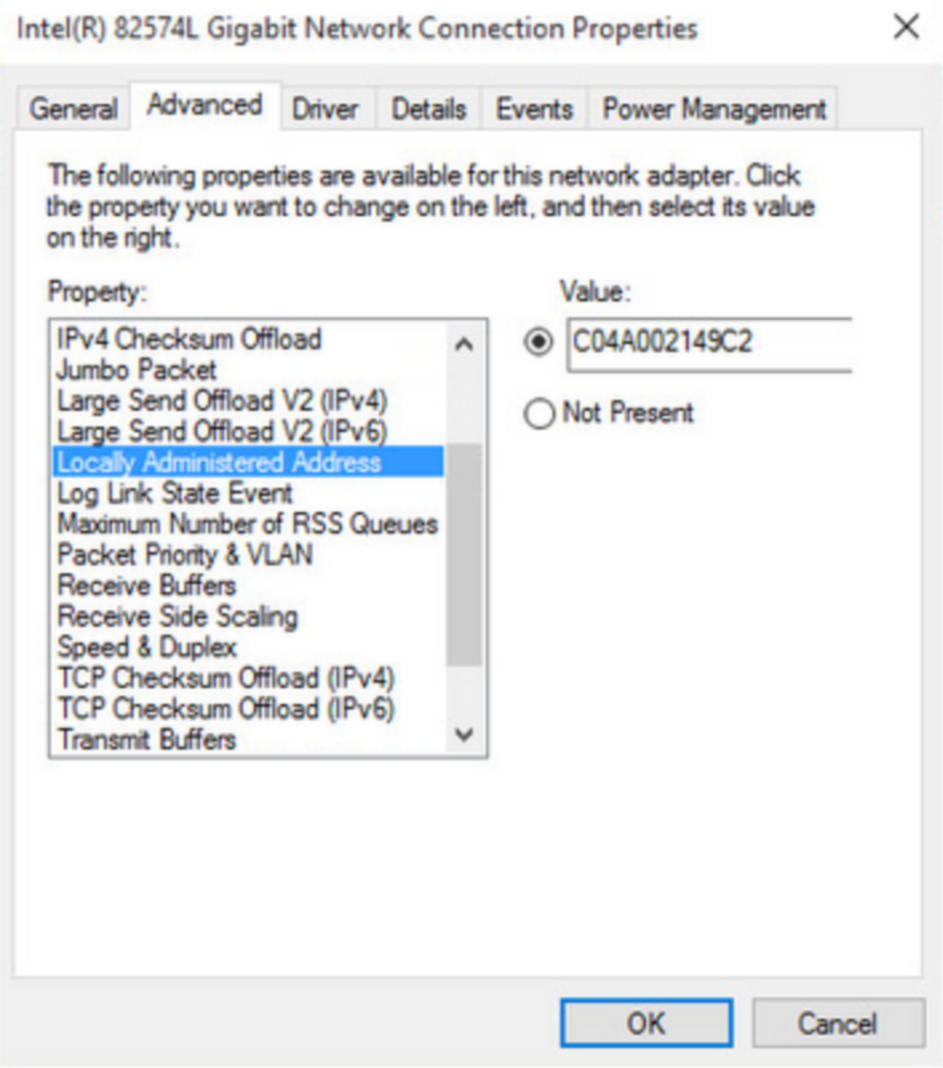
Connect with a wireless adapter. Use command **ipconfig /all** to find MAC address of wireless adapter, as shown in the image:



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : 802.11n USB Wireless LAN Card
   Physical Address. . . . . . . . . : C0-4A-00-21-49-C2
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::1c54:884a:33c0:bcf1%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.38(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, December 30, 2016 5:17:12 AM
   Lease Expires . . . . . . . . . . : Friday, December 30, 2016 6:17:12 AM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 46156288
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1F-F3-74-5F-C0-4A-00-21-49-C2
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

To simulate a malicious user, you may spoof the MAC address of the Ethernet adapter to match the MAC address of the normal user.



Intel(R) 82574L Gigabit Network Connection Properties

The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

- IPv4 Checksum Offload
- Jumbo Packet
- Large Send Offload V2 (IPv4)
- Large Send Offload V2 (IPv6)
- Locally Administered Address
- Log Link State Event
- Maximum Number of RSS Queues
- Packet Priority & VLAN
- Receive Buffers
- Receive Side Scaling
- Speed & Duplex
- TCP Checksum Offload (IPv4)
- TCP Checksum Offload (IPv6)
- Transmit Buffers

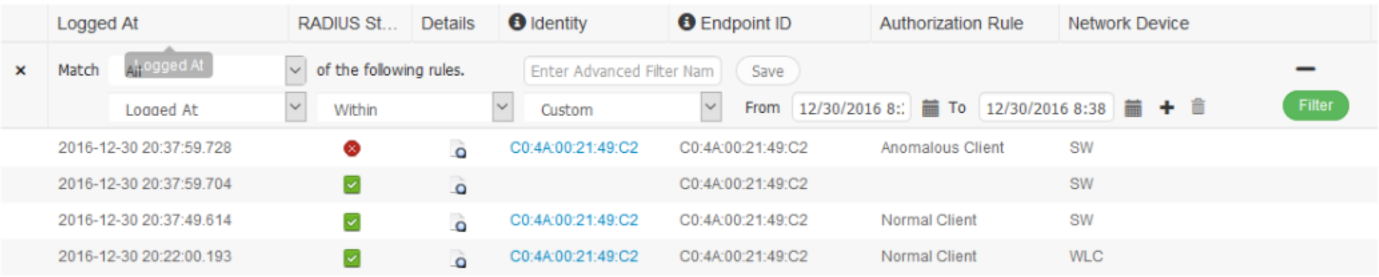
Value:

● C04A002149C2

○ Not Present

Once the Normal user connects, you can see an endpoint entry in the database. Afterwards, the malicious user connects using a spoofed MAC address.

From the reports you can see the initial connection from the WLC. Afterwards, the malicious user connects and 10 seconds later, a CoA is triggered due to the detection of the anomalous client. Since the global CoA type is set to **Reauth**, the endpoint tries to connect again. ISE already set the AnomalousBehaviour attribute to True so ISE matches the first rule and deny the user.

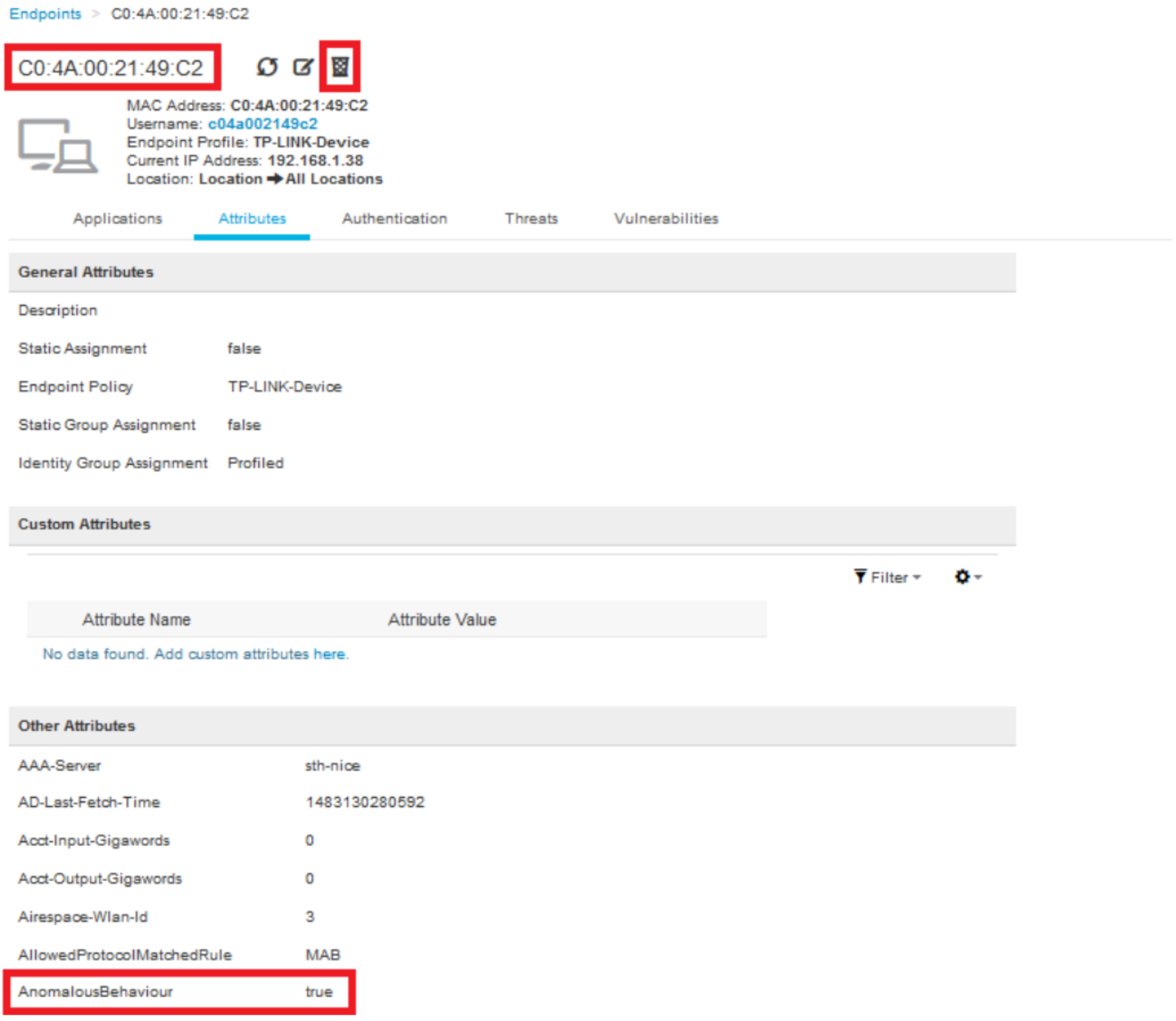


Match All of the following rules. Enter Advanced Filter Nam Save

Logged At Within Custom From 12/30/2016 8:: To 12/30/2016 8:38

Logged At	RADIUS St...	Details	Identity	Endpoint ID	Authorization Rule	Network Device
2016-12-30 20:37:59.728	☒	🔍	C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Anomalous Client	SW
2016-12-30 20:37:59.704	✓	🔍		C0:4A:00:21:49:C2		SW
2016-12-30 20:37:49.614	✓	🔍	C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Normal Client	SW
2016-12-30 20:22:00.193	✓	🔍	C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Normal Client	WLC

As shown in the image, you can see the details under the endpoint in Context Visibility Tab:



MAC Address: **C0:4A:00:21:49:C2**
Username: **c04a002149c2**
Endpoint Profile: **TP-LINK-Device**
Current IP Address: **192.168.1.38**
Location: **Location ➔All Locations**

General Attributes

Description	
Static Assignment	false
Endpoint Policy	TP-LINK-Device
Static Group Assignment	false
Identity Group Assignment	Profiled

Custom Attributes

Attribute Name	Attribute Value

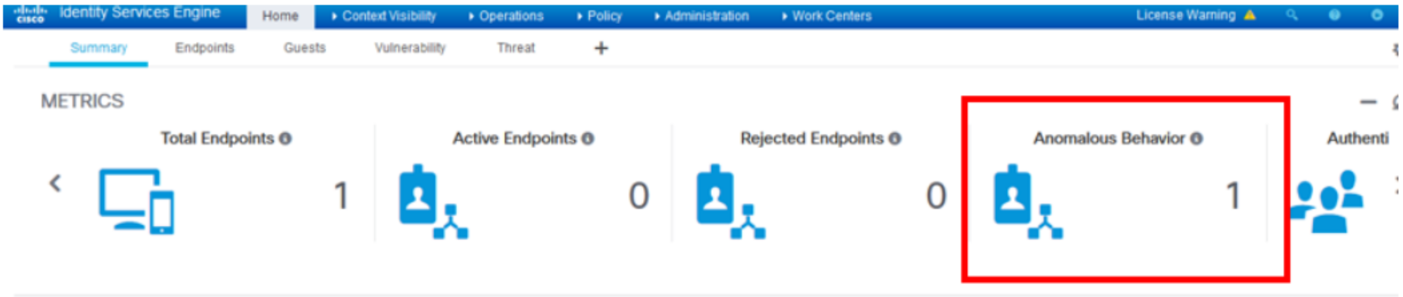
No data found. Add custom attributes here.

Other Attributes

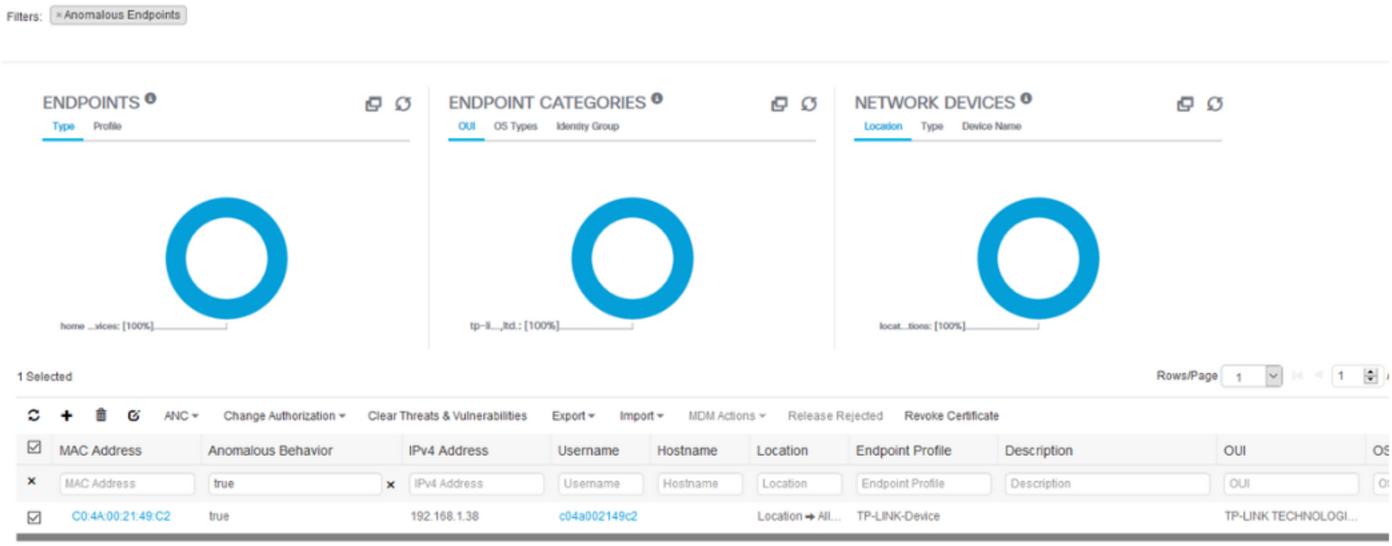
AAA-Server	sth-nice
AD-Last-Fetch-Time	1483130280592
Acct-Input-Gigawords	0
Acct-Output-Gigawords	0
Airespace-Wlan-Id	3
AllowedProtocolMatchedRule	MAB
AnomalousBehaviour	true

As you can see, the endpoint can be deleted from the database to clear this attribute.

As shown in the image, the dashboard includes a new tab to show the number of clients exhibiting this behaviour:



Total Endpoints	Active Endpoints	Rejected Endpoints	Anomalous Behavior
1	0	0	1



Filters: × Anomalous Endpoints

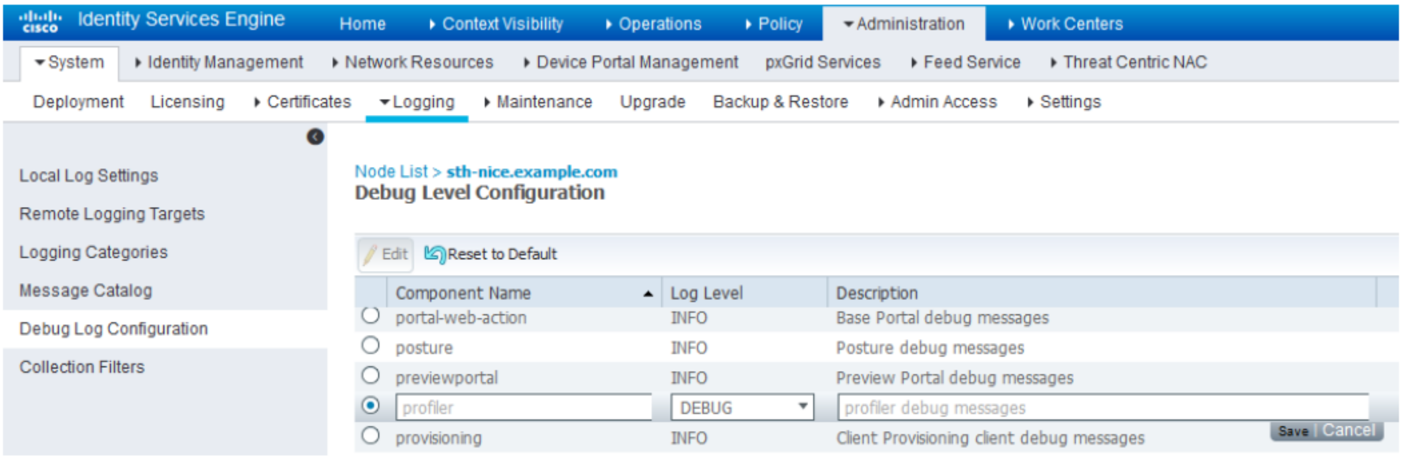
1 Selected

Rows/Page 1

☑	MAC Address	Anomalous Behavior	IPv4 Address	Username	Hostname	Location	Endpoint Profile	Description	OUI	OS
×	MAC Address	true	IPv4 Address	Username	Hostname	Location	Endpoint Profile	Description	OUI	O
☑	C0:4A:00:21:49:C2	true	192.168.1.38	c04a002149c2		Location ➔ All...	TP-LINK-Device		TP-LINK TECHNOLOGI...	

Troubleshoot

In order to troubleshoot, enable profiler debug, as you navigate to **Administration > System > Logging > Debug Log Configuration**.

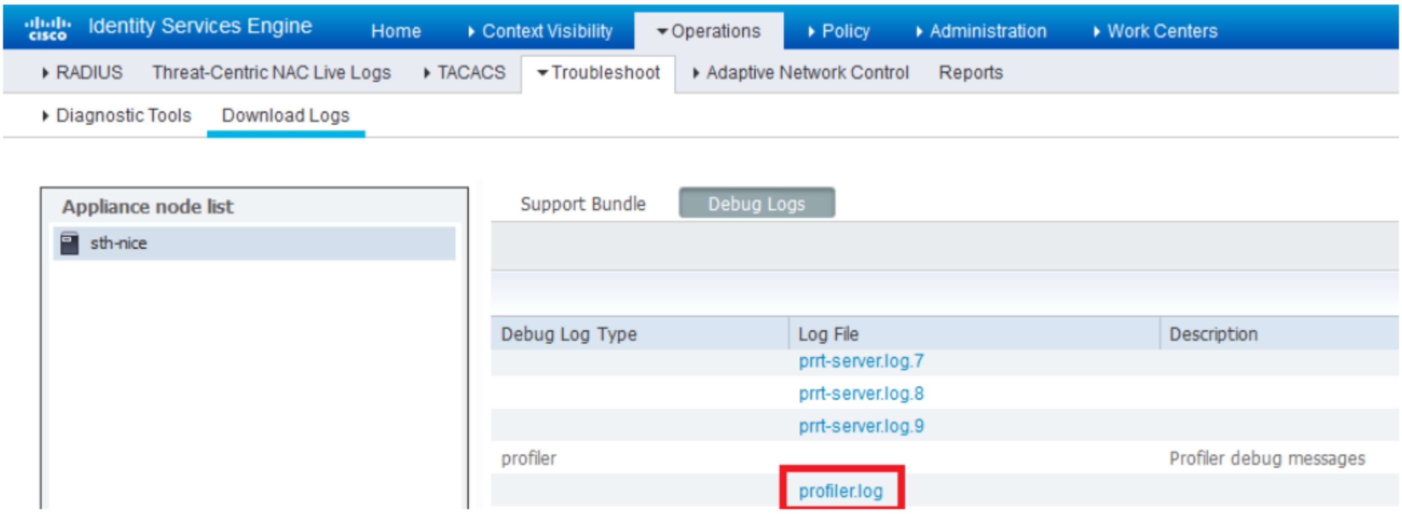


Node List > sth-nice.example.com

Debug Level Configuration

	Component Name	Log Level	Description
○	portal-web-action	INFO	Base Portal debug messages
○	posture	INFO	Posture debug messages
○	previewportal	INFO	Preview Portal debug messages
●	profiler	DEBUG	profiler debug messages
○	provisioning	INFO	Client Provisioning client debug messages

In order to find the ISE **Profiler.log** file, navigate to **Operations > Download Logs > Debug Logs**, as shown in the image:



Debug Log Type	Log File	Description
	prrt-server.log.7	
	prrt-server.log.8	
	prrt-server.log.9	
profiler		Profiler debug messages
	profiler.log	

These logs show some snippets from the **Profiling.log** file. As you can see, ISE was able to detect that the endpoint with MAC address of C0:4A:00:21:49:C2 has changed the access method by comparing the old and new values of the NAS-Port-Type attributes. It's wireless but is changed to Ethernet.

```
2016-12-30 20:37:43,874 DEBUG  [EndpointHandlerWorker-2-34-thread-1][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:Profiling:- Classify hierarchy
C0:4A:00:21:49:C2
2016-12-30 20:37:43,874 DEBUG  [MACSpoofingEventHandler-52-thread-1][]
profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -:ProfilerCollection:- Received
AttrsModifiedEvent in MACSpoofingEventHandler MAC: C0:4A:00:21:49:C2 2016-12-30 20:37:49,618
DEBUG [MACSpoofingEventHandler-52-thread-1][]
profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -:ProfilerCollection:- Received
AttrsModifiedEvent in MACSpoofingEventHandler MAC: C0:4A:00:21:49:C2 2016-12-30 20:37:49,618
INFO [MACSpoofingEventHandler-52-thread-1][] com.cisco.profiler.api.MACSpoofingManager -
:ProfilerCollection:- Anomalous Behaviour Detected: C0:4A:00:21:49:C2 AttrName: NAS-Port-Type
Old Value: Wireless - IEEE 802.11 New Value: Ethernet 2016-12-30 20:37:49,620 DEBUG
[MACSpoofingEventHandler-52-thread-1][] cisco.profiler.infrastructure.cache.EndPointCache -
:ProfilerCollection:- Updating end point: mac - C0:4A:00:21:49:C2 2016-12-30 20:37:49,621 DEBUG
[MACSpoofingEventHandler-52-thread-1][] cisco.profiler.infrastructure.cache.EndPointCache -
:ProfilerCollection:- Reading significant attribute from DB for end point with mac
C0:4A:00:21:49:C2 2016-12-30 20:37:49,625 DEBUG [MACSpoofingEventHandler-52-thread-1][]
profiler.infrastructure.probemgr.event.EndpointPersistEventHandler -:ProfilerCollection:- Adding
to queue endpoint persist event for mac: C0:4A:00:21:49:C2
```

Therefore, ISE takes action since enforcement is enabled. The action here is to send a CoA depending on the global configuration in the Profiling settings mentioned above. In our example, the CoA type is set to Reauth which allows ISE to re-authenticate the endpoint and recheck the rules that were configured. This time, it matches the Anomalous client rule and therefore it is denied.

```
2016-12-30 20:37:49,625 INFO   [MACSpoofingEventHandler-52-thread-1][]
profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -:ProfilerCollection:- Taking mac
spoofing enforcement action for mac: C0:4A:00:21:49:C2 2016-12-30 20:37:49,625 INFO
[MACSpoofingEventHandler-52-thread-1][]
profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -:ProfilerCollection:- Triggering
Delayed COA event. Should be triggered in 10 seconds 2016-12-30 20:37:49,625 DEBUG [CoAHandler-
40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Received
CoAEvent notification for endpoint: C0:4A:00:21:49:C2 2016-12-30 20:37:49,625 DEBUG [CoAHandler-
40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Configured
Global CoA command type = Reauth 2016-12-30 20:37:49,626 DEBUG [CoAHandler-40-thread-1][]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Received
FirstTimeProfileCoAEvent for endpoint: C0:4A:00:21:49:C2 2016-12-30 20:37:49,626 DEBUG
[CoAHandler-40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:-
Wait for endpoint: C0:4A:00:21:49:C2 to update - TTL: 1 2016-12-30 20:37:49,626 DEBUG
[CoAHandler-40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:-
Setting timer for endpoint: C0:4A:00:21:49:C2 to: 10 [sec] 2016-12-30 20:37:49,626 DEBUG
[CoAHandler-40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:-
Rescheduled event for endpoint: C0:4A:00:21:49:C2 to retry - next TTL: 0 2016-12-30 20:37:59,644
DEBUG [CoAHandler-40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -
:ProfilerCoA:- About to call CoA for nad IP: 10.62.148.106 for endpoint: C0:4A:00:21:49:C2 CoA
Command: Reauth 2016-12-30 20:37:59,645 DEBUG [CoAHandler-40-thread-1][]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Applying CoA-REAUTH by AAA
Server: 10.48.26.89 via Interface: 10.48.26.89 to NAD: 10.62.148.106
```

Related Information

- ISE 2.2 Administration Guide