

Configure la detección y la aplicación anómalas de la punto final en ISE 2.2

Contenido

[Introducción](#)

[Prerequisites](#)

[Requisitos](#)

[Componentes usados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Paso 1. Detección anómala del permiso.](#)

[Paso 2. Configure la directiva de la autorización.](#)

[Verifique](#)

[Troubleshooting](#)

[Información Relacionada](#)

Introducción

Este documento describe la detección y la aplicación anómalas de la punto final. Esto es una nueva característica de perfilado introducida en Cisco Identity Services Engine (ISE) para la visibilidad aumentada de la red.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración atada con alambre de puente de la autenticación MAC (MAB) en el conmutador
- Configuración inalámbrica MAB en el regulador inalámbrico LAN (WLC)
- Cambio de la configuración de la autorización (CoA) en ambos dispositivos

Componentes usados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

1. Identity Services Engine 2.2
2. Regulador inalámbrico 8.0.100.0 LAN

3. Conmutador 3750 15.2(3)E2 del Cisco Catalyst
4. Windows 10 con atado con alambre y adaptadores de red inalámbrica

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

La característica anómala de la detección de la punto final permite que el ISE vigile los cambios a los atributos específicos y los perfiles para las puntos finales conectadas. Si un cambio hace juego uno o más de las reglas anómalas preconfiguradas del comportamiento, ISE marcará la punto final como anómala. Una vez que está detectado, ISE puede tomar medidas (con el CoA) y aplicar ciertas directivas para restringir el acceso de la punto final sospechosa. Uno de los casos del uso para esta característica incluye la detección de falsificación de la dirección MAC.

-
- **Note:** Esta característica no dirige todos los decorados potenciales para la falsificación de la dirección MAC. Esté por favor seguro de leer los tipos de anomalías cubiertas por esta característica para determinar su aplicabilidad a sus casos del uso.
-

Una vez que se activa la detección, ISE vigila cualquier nueva información recibida para las puntos finales existentes y controla si estos atributos han cambiado:

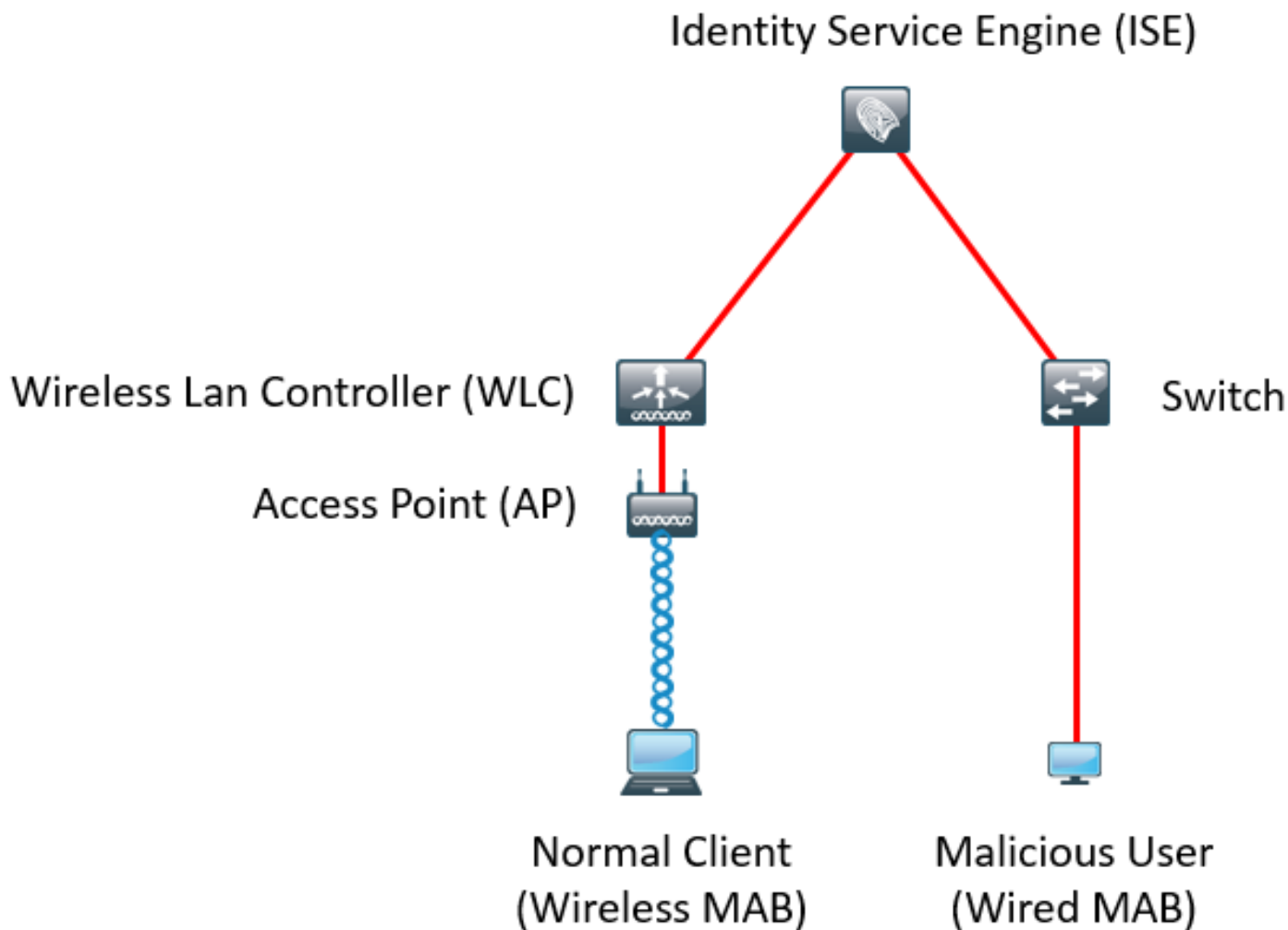
1. **NAS-Puerto-tipo** - Determina si el método de acceso de esta punto final ha cambiado. Por ejemplo, si la misma dirección MAC que conectó vía Dot1x atado con alambre se utiliza para la Tecnología inalámbrica Dot1x y la visa-versa.
2. **Identificación de la clase del DHCP** - Determina si el tipo de cliente/de vendedor de la punto final ha cambiado. Esto se aplica solamente cuando el atributo identificación de la clase del DHCP se puebla con cierto valor y después se cambia a otro valor. Si una punto final se configura con IP estático, el atributo identificación de la clase del DHCP no será poblado en ISE. Después, si otras parodias del dispositivo la dirección MAC y DHCP de las aplicaciones, la identificación de la clase cambian de un valor vacío a una cadena específica. Esto no accionará la detección del comportamiento de Anomouls.
3. **Directiva de la punto final** - Un cambio en el perfil de la punto final de la impresora o del teléfono IP al puesto de trabajo.

Una vez que ISE detecta uno de los cambios mencionados anteriormente, el atributo de AnomalousBehaviour se agrega a la punto final y al conjunto para verdad. Esto se puede utilizar después como una condición en las directivas de la autorización para restringir el acceso para la punto final en las autenticaciones futuras.

Si se configura la aplicación, ISE puede enviar un CoA una vez que el cambio se detecta re-para autenticar o para realizar una despedida del puerto para la punto final. Si en efecto, puede quarantine la punto final anómala dependiendo de las directivas de la autorización que fueron configuradas.

Configurar

Diagrama de la red



Configuraciones

Las configuraciones simples MAB y AAA se realizan en el conmutador y el WLC. Para utilizar esta característica, siga los siguientes pasos:

Paso 1. Detección anómala del permiso.

Navegue a la **administración > al sistema > a las configuraciones > perfilando.**

Profiler Configuration

* CoA Type:

Current custom SNMP community strings:

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

La primera opción permite que ISE detecte cualquier comportamiento anómalo pero no se envía ningún CoA (modo de la visibilidad-Solamente). La segunda opción permite que ISE envíe el CoA una vez que se detecta el comportamiento anómalo (modo de implementación).

Paso 2. Configure la directiva de la autorización.

Configure el atributo de Anomalousbehaviour como condición en la directiva de la autorización, tal y como se muestra en de la imagen:

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	Normal Client	if DEVICE:Location EQUALS All Locations	then PermitAccess

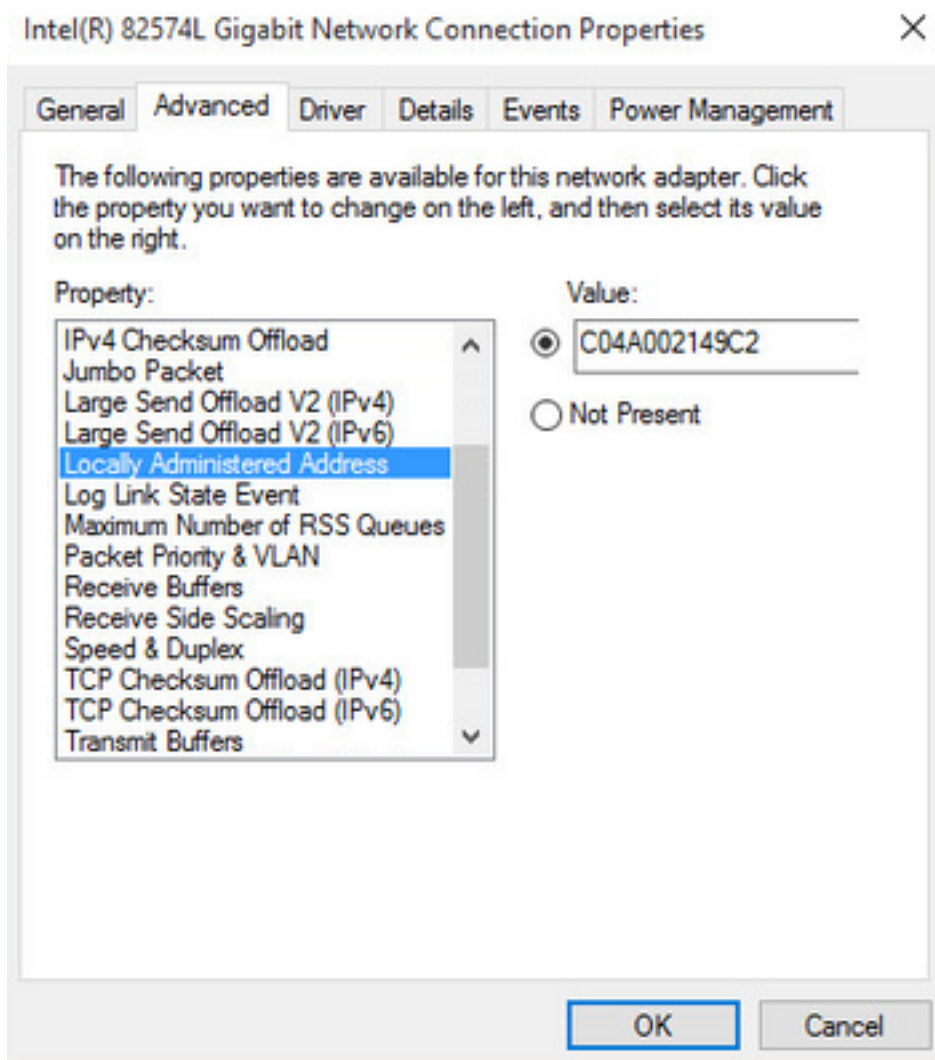
Verifique

Conecte con un adaptador de red inalámbrica. Utilice el comando `ipconfig /all` de encontrar la dirección MAC del adaptador de red inalámbrica, tal y como se muestra en de la imagen:

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 Tcpiip. . . . . : Enabled
```

Para simular a un usuario malintencionado, usted puede spoof la dirección MAC del adaptador de los Ethernetes hacer juego la dirección MAC del usuario normal.



Una vez que el usuario normal conecta, usted puede ver una entrada de la punto final en la base de datos. Luego, el usuario malintencionado conecta usando una dirección MAC spoofed.

De los informes usted puede ver la conexión inicial del WLC. Luego, el usuario malintencionado conecta y 10 segundos después, un CoA es accionado debido a la detección del cliente anómalo. Puesto que el tipo global CoA se fija a **Reauth**, la punto final intenta conectar otra vez. ISE fijó ya el atributo de AnomalousBehaviour para verdad así que ISE hace juego la primera regla y niega al usuario.

Logged At	RADIUS St...	Details	Identity	Endpoint ID	Authorization Rule	Network Device
Match Logged At of the following rules. <input type="text" value="Enter Advanced Filter Nam"/> Save						
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

Tal y como se muestra en de la imagen, usted puede ver los detalles bajo punto final en la tabulación de la visibilidad del contexto:

Endpoints > C0:4A:00:21:49:C2

C0:4A:00:21:49:C2   


 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

Applications Attributes Authentication Threats Vulnerabilities

General Attributes

Description

Static Assignment false

Endpoint Policy TP-LINK-Device

Static Group Assignment false

Identity Group Assignment Profiled

Custom Attributes

Filter 

Attribute Name	Attribute Value
----------------	-----------------

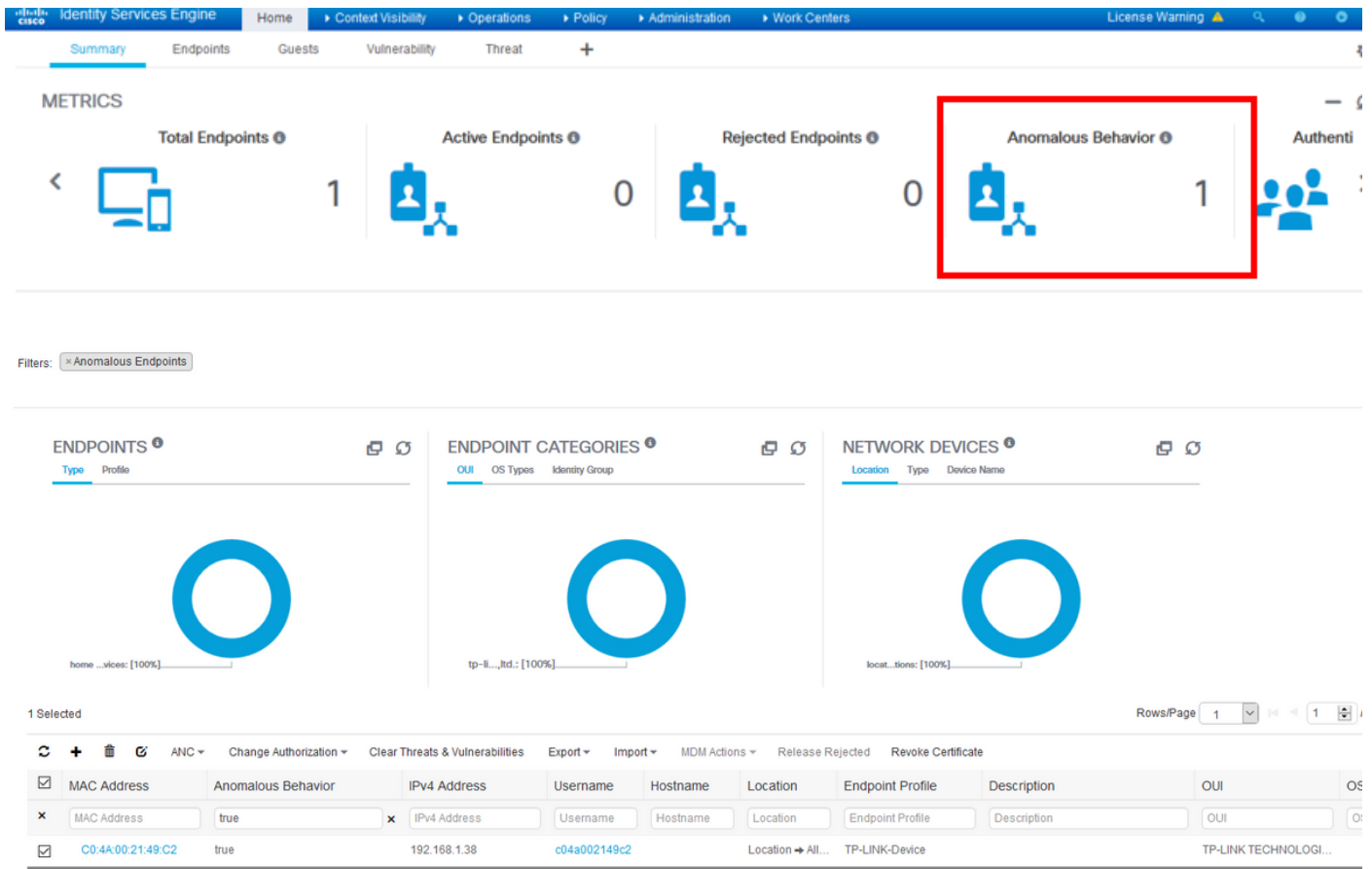
No data found. Add custom attributes [here](#).

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

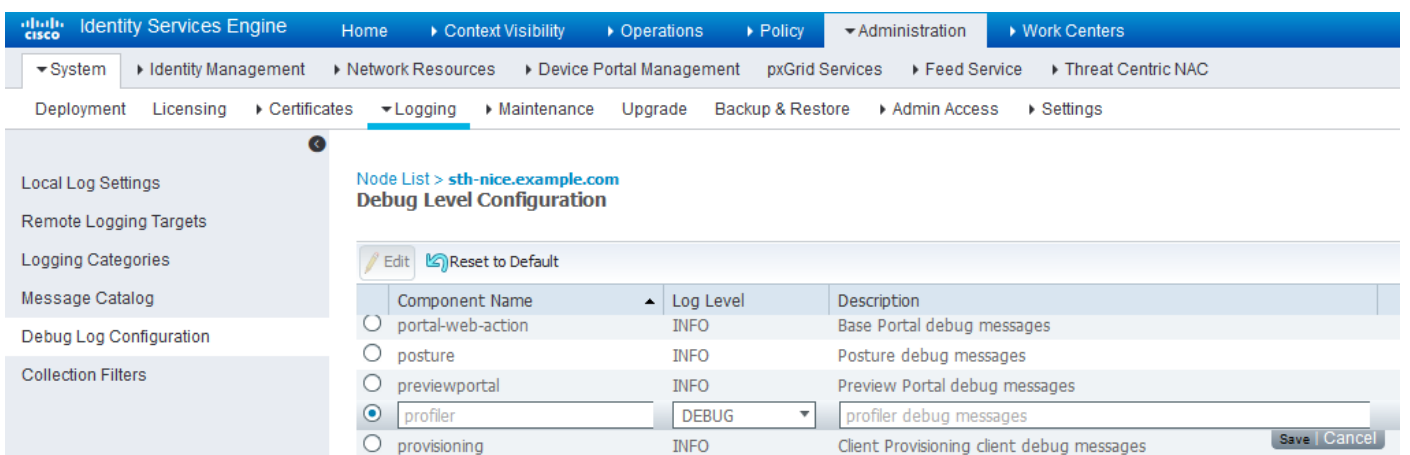
Como usted puede ver, la punto final se puede suprimir de la base de datos para borrar este atributo.

Tal y como se muestra en de la imagen, el panel incluye una nueva tabulación para mostrar el número de clientes que exhiben este comportamiento:



Troubleshooting

Para resolver problemas, activar la depuración del profiler, como usted navega a la **administración > al sistema > a la configuración del registro del registro > de la depuración.**



Para encontrar el fichero ISE Profiler.log, navegue a las **operaciones > a los registros de la transferencia directa > a los registros de la depuración**, tal y como se muestra en de la imagen:

Appliance node list		
sth-nice		

Support Bundle		
Debug Logs		
Debug Log Type	Log File	Description
	prtt-server.log.7	
	prtt-server.log.8	
	prtt-server.log.9	
profiler	profiler.log	Profiler debug messages

Estos registros muestran algunos recortes del fichero de **Profiling.log**. Como usted puede ver, ISE podía detectar que la punto final con la dirección MAC de C0:4A:00:21:49:C2 ha cambiado el método de acceso comparando los viejos y nuevos valores del NAS-Puerto-tipo atributos. Es inalámbrico pero se cambia a los Ethernetes.

```
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
```

Por lo tanto, ISE toma medidas puesto que se activa la aplicación. La acción aquí es enviar un CoA dependiendo de la configuración global en las configuraciones de perfilado mencionadas anteriormente. En nuestro ejemplo, el tipo CoA se fija a Reauth que permita que ISE re-autentique la punto final y que vuelva a inspeccionar las reglas que fueron configuradas. Esta vez, hace juego la regla anómala del cliente y por lo tanto se niega.

```
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
```

Información Relacionada

- [Guía de administración ISE 2.2](#)