Detección y aplicación anómalas del punto final de la configuración en ISE 2.2

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Configurar](#)
[Diagrama de la red](#)
[Configuraciones](#)
[Paso 1. Detección anómala del permiso.](#)
[Paso 2. Directiva de la autorización de la configuración.](#)
[Verificación](#)
[Troubleshooting](#)
[Información Relacionada](#)

Introducción

Este documento describe la detección y la aplicación anómalas del 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 de MAC (MAB) en el Switch
- Configuración inalámbrica MAB en el regulador del Wireless LAN (WLC)
- Cambio de la configuración de la autorización (CoA) en ambos dispositivos

Componentes Utilizados

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

1. Identity Services Engine 2.2
2. Regulador 8.0.100.0 del Wireless LAN

3. Switch 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

El ISE puede detectar los puntos finales que están implicados en el spoofing del MAC address. Una vez que se detecta, el ISE puede tomar medidas (con el CoA) y aplicar ciertas directivas para restringir el acceso del punto final sospechoso.

Una vez que se habilita la detección, el ISE monitorea cualquier nueva información recibida para los puntos finales existentes y marca si estos atributos han cambiado:

1. **NAS-Puerto-tipo** - Determina si el método de acceso de este punto final ha cambiado. Por ejemplo, si la misma dirección MAC que conectó vía el dot1x atado con alambre se utiliza para el dot1x inalámbrico y la visa-versa.

2. **Clase ID del DHCP** - Determina si el tipo de cliente/de vendedor del punto final ha cambiado. Esto se aplica solamente cuando el atributo de la clase ID del DHCP se puebla con cierto valor y después se cambia a otro valor. Si un punto final se configura con IP estático, el atributo de la clase ID del DHCP no será poblado en el ISE. Después, si otras parodias del dispositivo la dirección MAC y DHCP de las aplicaciones, la clase ID cambian de un valor vacío a una cadena específica. Esto no accionará la detección del comportamiento de Anomouls.

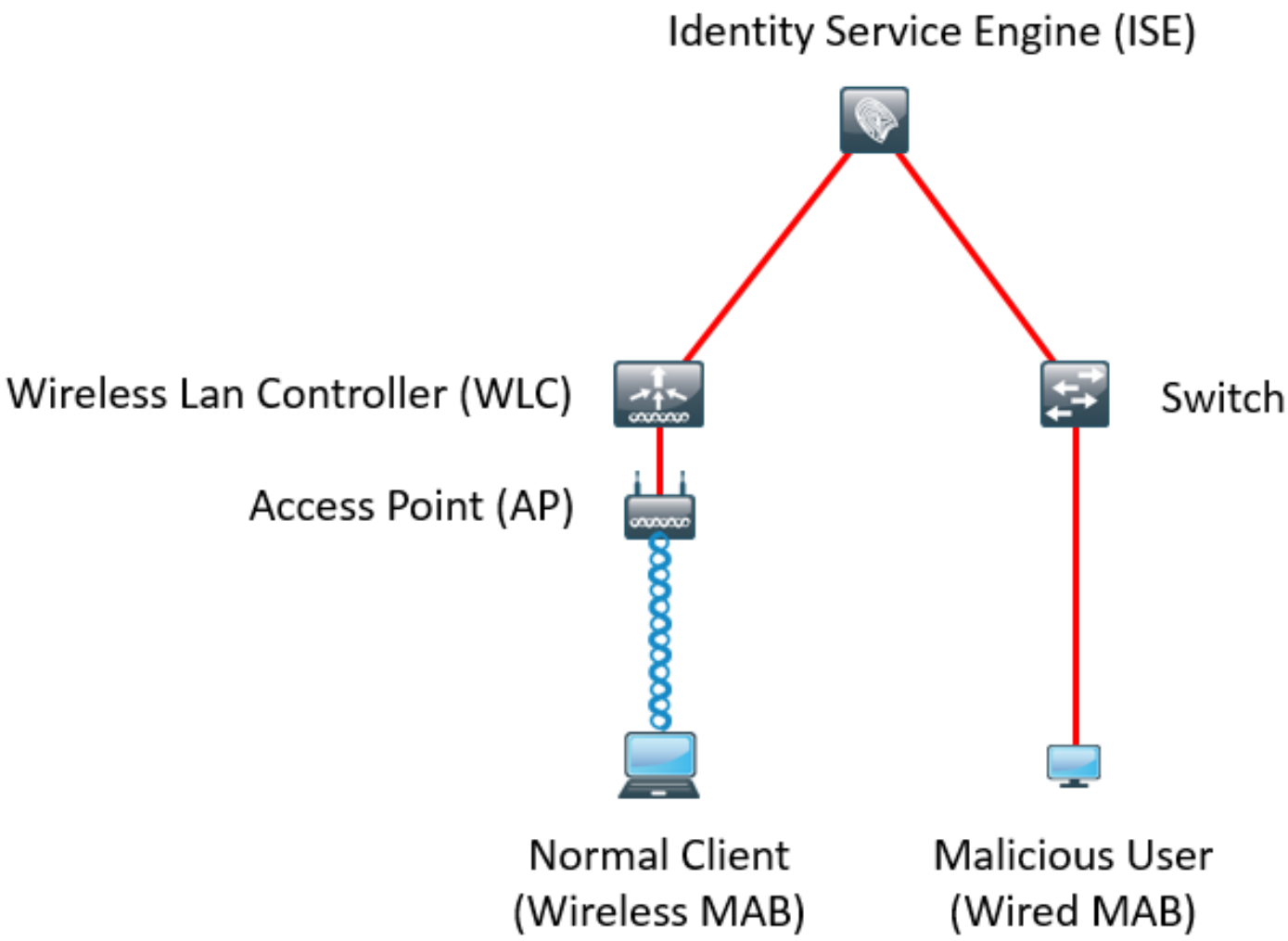
3. **Directiva del punto final -** Un cambio en el perfil del punto final de la **impresora** o del **teléfono del IP al puesto de trabajo**.

Una vez que el ISE detecta uno de los cambios mencionados anteriormente, el atributo de AnomalousBehaviour se agrega al 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 el punto final en las autenticaciones futuras.

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

Configurar

Diagrama de la red

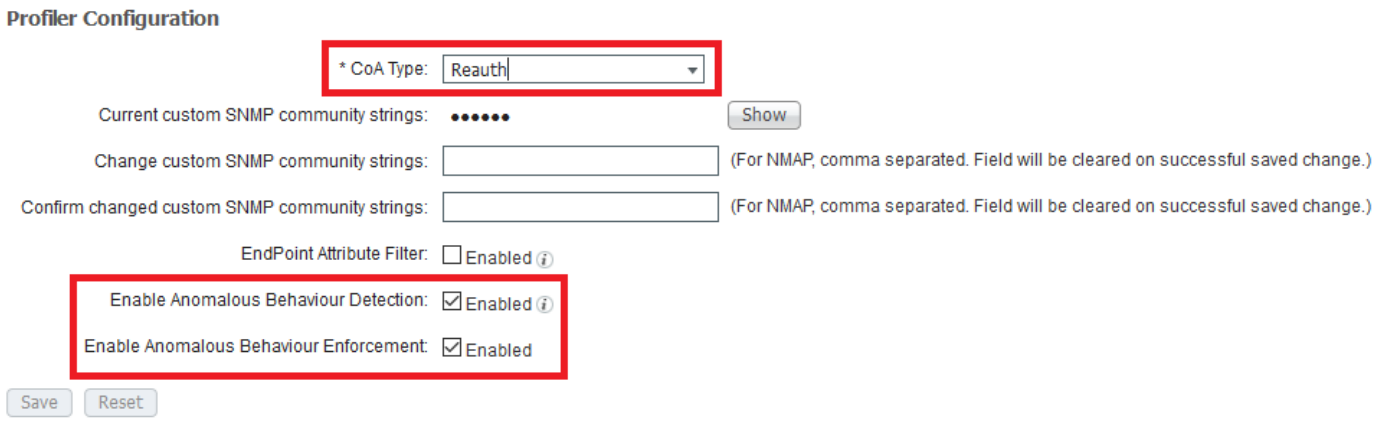


Configuraciones

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

Paso 1. Detección anómala del permiso.

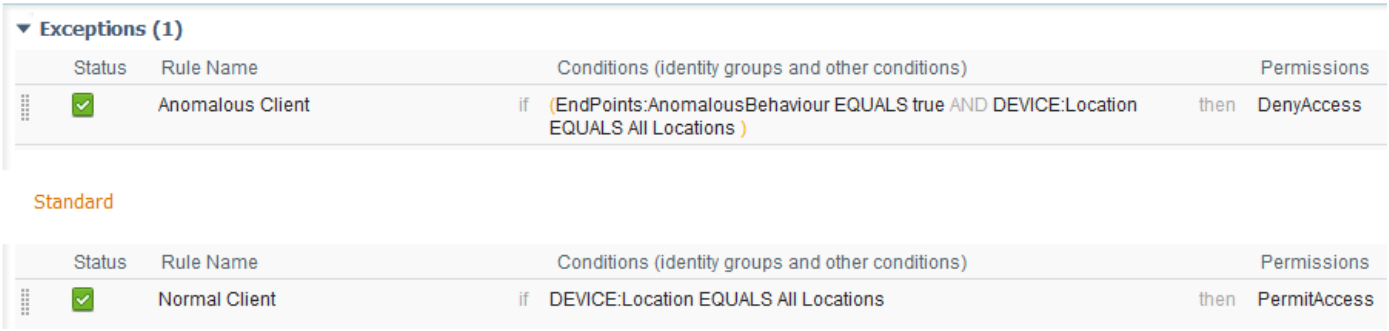
Navegue a la **administración > al sistema > a las configuraciones > perfilando**.



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

Paso 2. Directiva de la autorización de la configuración.

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



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

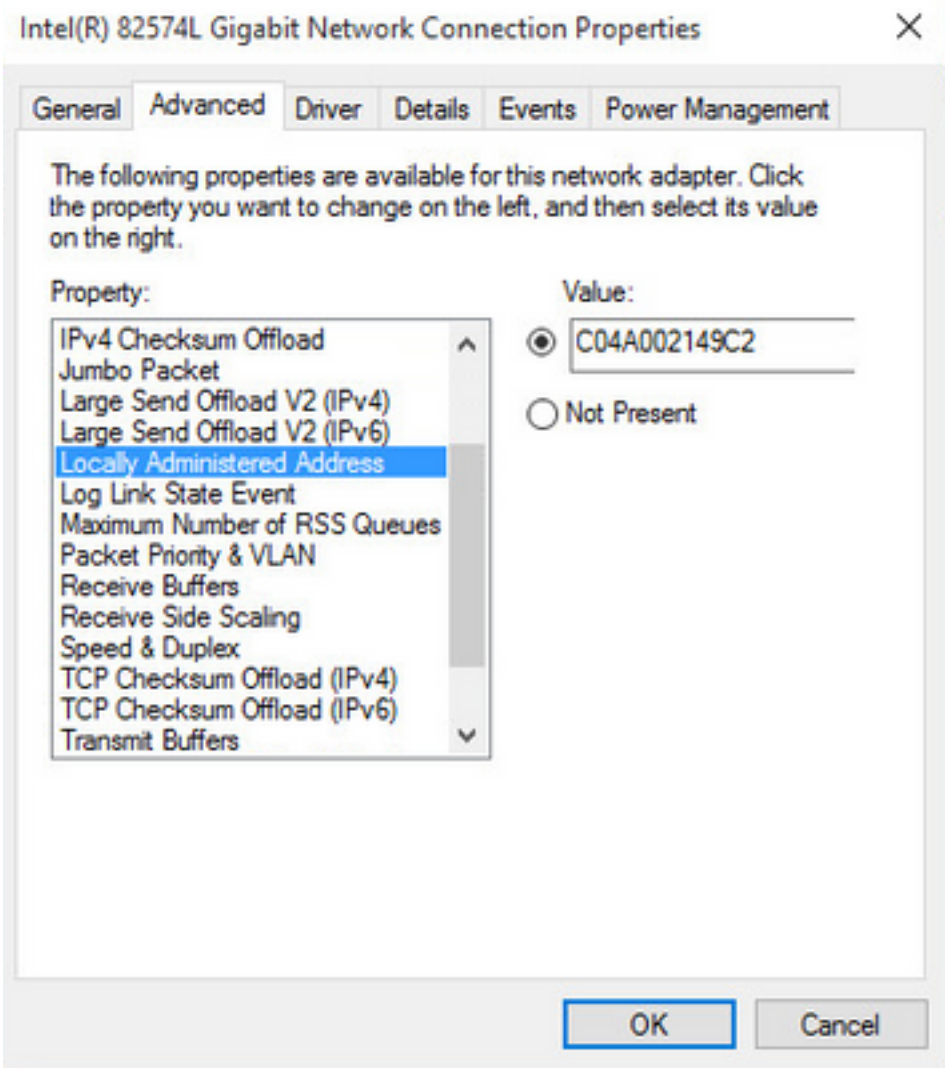
Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Normal Client	if	DEVICE:Location EQUALS All Locations	then	PermitAccess

Verificación

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:

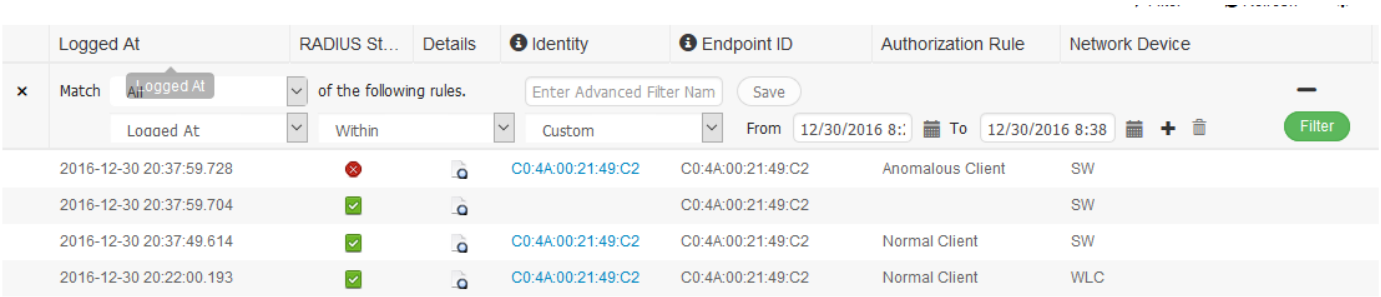
```
Wireless LAN adapter Wi-Fi:

   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 Tcpip. . . . . . . . : Enabled
```

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

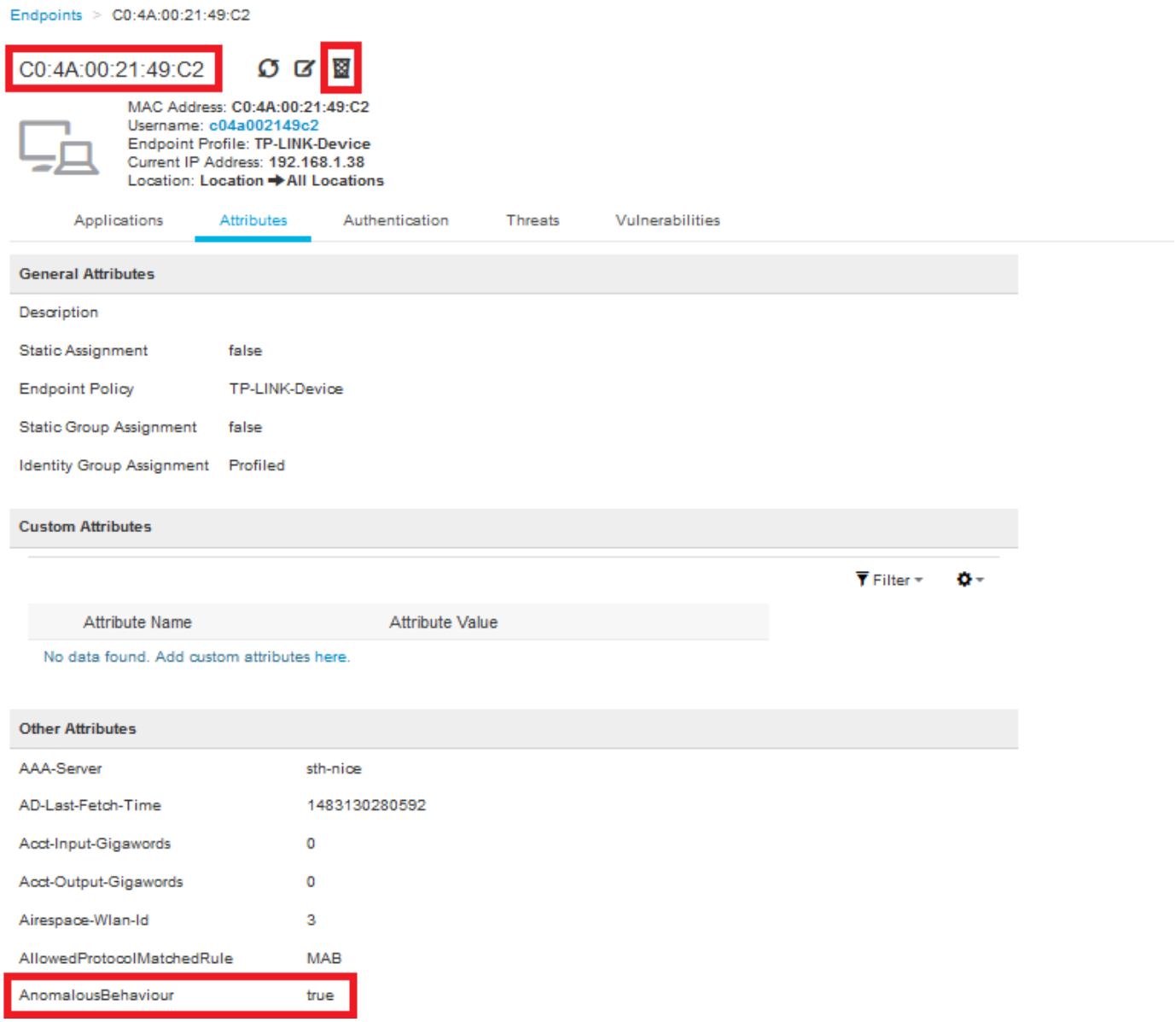


Una vez que el usuario normal conecta, usted puede ver una entrada del punto final en la base de datos. Luego, el usuario malintencionado conecta usando una dirección MAC del spoofed.

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 fijan al tipo global CoA a **Reauth**, el punto final intenta conectar otra vez. El ISE fijó ya el atributo de AnomalousBehaviour para verdad así que el ISE hace juego la primera regla y niega al usuario.

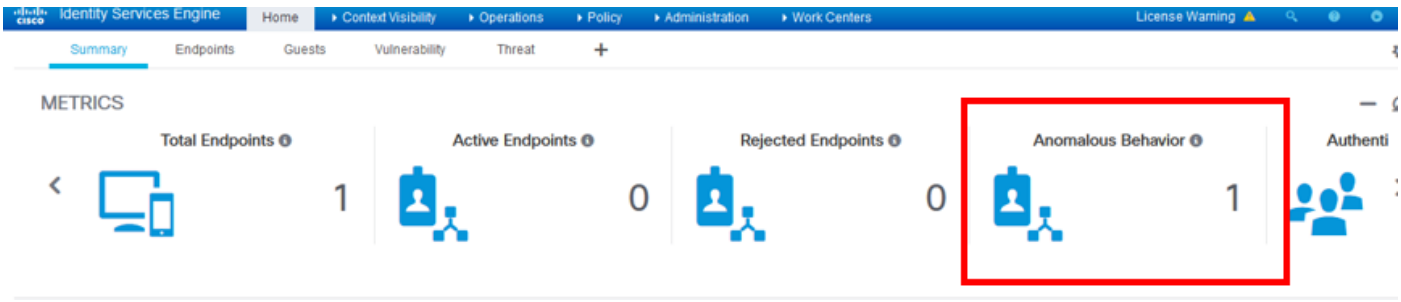


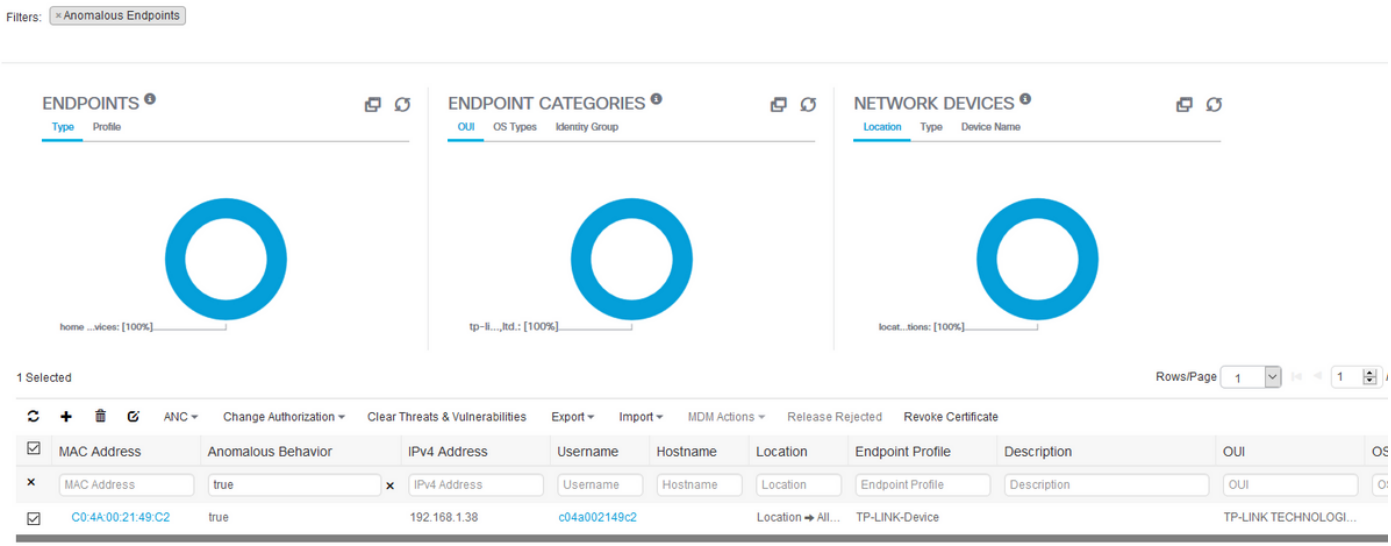
Tal y como se muestra en de la imagen, usted puede ver los detalles conforme al punto final en la lengueta de la visibilidad del contexto:



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

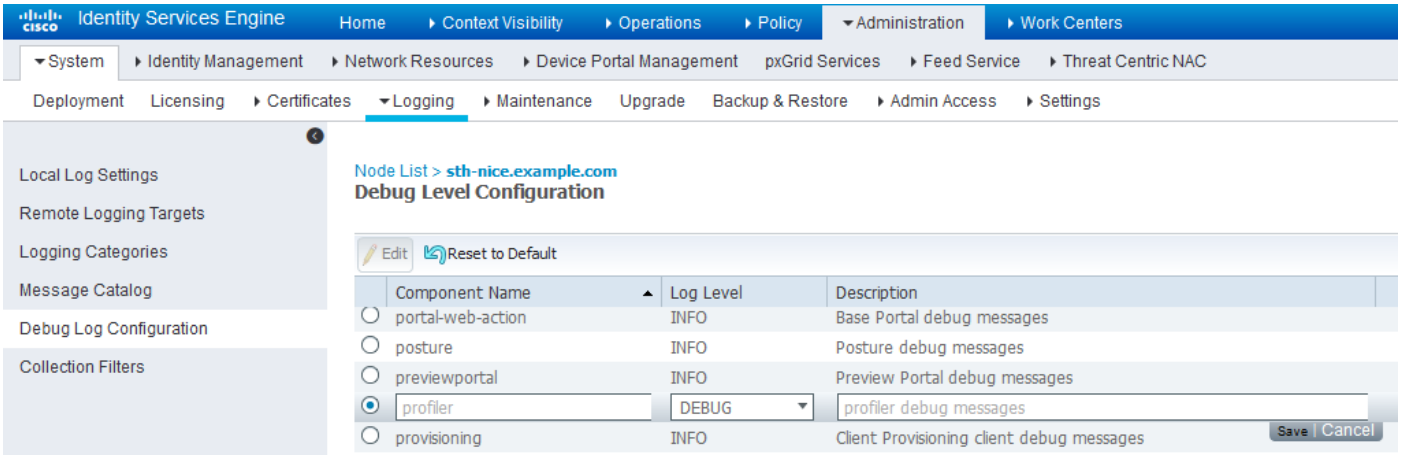
Tal y como se muestra en de la imagen, el panel incluye una nueva lengueta para mostrar el número de clientes que exhiben este comportamiento:



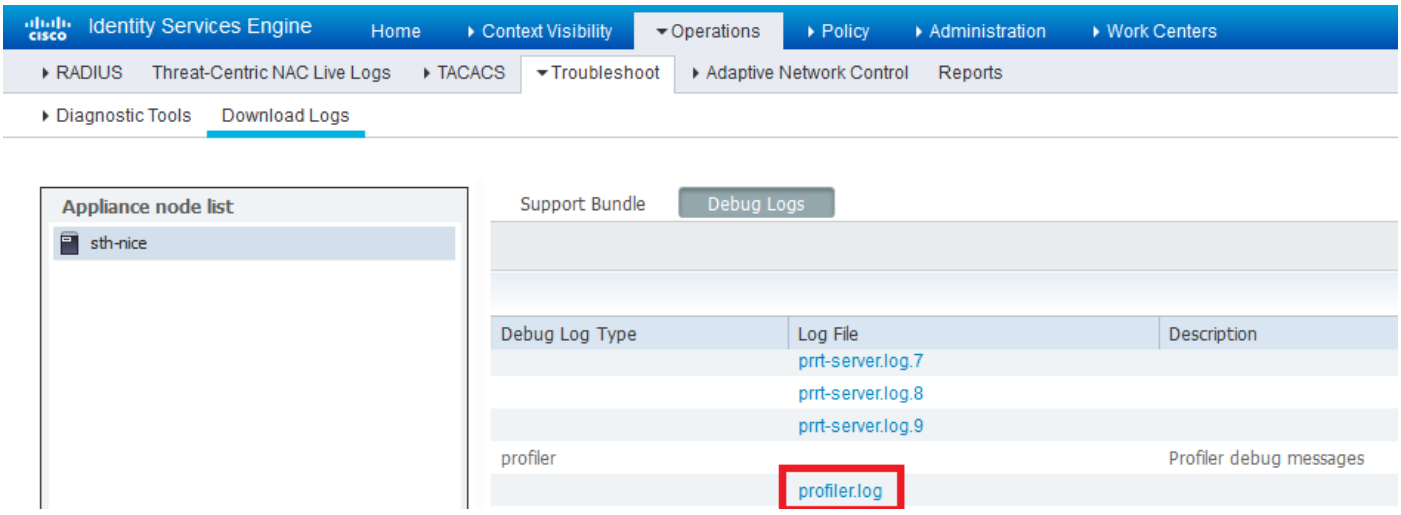


Troubleshooting

Para resolver problemas, habilitar el debug del profiler, como usted navega a la **administración > al sistema > a la configuración del registro del registro > del debug**.



Para encontrar el archivo ISE **Profiler.log**, navegue a las **operaciones > a los registros de la descarga > a los registros del debug**, tal y como se muestra en de la imagen:



Estos registros muestran algún snippets del archivo de **Profiling.log**. Como usted puede ver, el ISE podía detectar que el 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 de los atributos del NAS-Puerto-tipo. 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, el ISE toma medidas puesto que se habilita la aplicación. La acción aquí es enviar un CoA dependiendo de la configuración global en las configuraciones de perfilado mencionadas anteriormente. En nuestro ejemplo, fijan al tipo CoA a Reauth que permita que el ISE reautentifique el 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