Configuración de la detección y aplicación de terminales analógicos en ISE 2.2

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Configurar](#)
[Diagrama de la red](#)
[Configuraciones](#)
[Paso 1. Habilite la detección anómala.](#)
[Paso 2. Configuración de la política de autorización.](#)
[Verificación](#)
[Troubleshoot](#)
[Información Relacionada](#)

Introducción

Este documento describe la detección y aplicación de terminales anómalos. Se trata de una nueva función de definición de perfiles introducida en Cisco Identity Services Engine (ISE) para mejorar la visibilidad de la red.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de derivación de autenticación MAC por cable (MAB) en el switch
- Configuración de MAB inalámbrico en controlador de LAN inalámbrica (WLC)
- Cambio de configuración de 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. Controlador de LAN inalámbrica 8.0.100.0

3. Switch Cisco Catalyst 3750 15.2(3)E2
4. Windows 10 con adaptadores por cable e inalámbricos

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.

Antecedentes

La función de detección de terminales analógicos permite al ISE supervisar los cambios en atributos y perfiles específicos para los terminales conectados. Si un cambio coincide con una o más de las reglas de comportamiento anómalas preconfiguradas, ISE marcará el terminal como Anómalo. Una vez detectados, ISE puede tomar medidas (con CoA) y aplicar ciertas políticas para restringir el acceso al terminal sospechoso. Uno de los casos prácticos de esta función incluye la detección de suplantación de dirección MAC.

- Nota: Esta función no aborda todos los escenarios potenciales para la suplantación de direcciones MAC. Asegúrese de leer los tipos de anomalías que cubre esta función para determinar su aplicabilidad a los casos prácticos.

Una vez habilitada la detección, ISE supervisa cualquier nueva información recibida para los terminales existentes y comprueba si estos atributos han cambiado:

1. **NAS-Port-Type** - Determina si el método de acceso de este punto final ha cambiado. Por ejemplo, si la misma dirección MAC que se conectó a través de Wired Dot1x se utiliza para Wireless Dot1x y visa-versa.

2. **DHCP Class ID** - Determina si el tipo de cliente/proveedor del punto final ha cambiado. Esto sólo se aplica cuando el atributo de ID de clase DHCP se rellena con un valor determinado y luego se cambia a otro valor. Si se configura un extremo con una IP estática, el atributo de ID de clase DHCP no se rellenará en ISE. Más adelante, si otro dispositivo falsifica la dirección MAC y utiliza DHCP, el ID de clase cambiará de un valor vacío a una cadena específica. Esto no activará la detección del comportamiento de Anomouls.

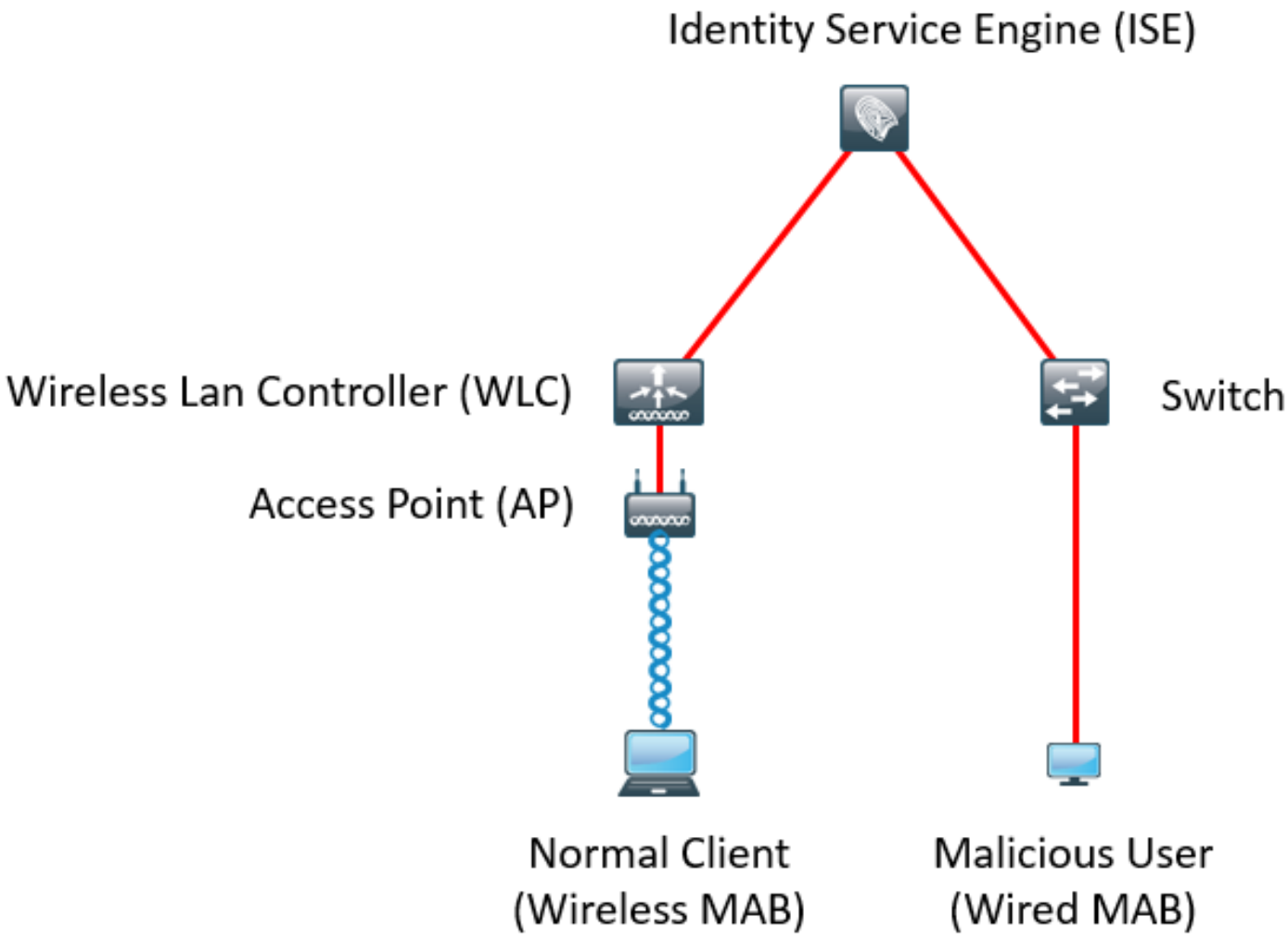
3. **Política de terminales -** Un cambio en el perfil de terminal de **impresora** o **teléfono IP a la** estación de trabajo**.**

Una vez que ISE detecta uno de los cambios mencionados anteriormente, el atributo AnomalousBehavior se agrega al extremo y se establece en True. Esto se puede utilizar más adelante como condición en las políticas de autorización para restringir el acceso del terminal en futuras autenticaciones.

Si se configura la aplicación, ISE puede enviar una CoA una vez que se detecte el cambio para volver a autenticar o realizar un rebote de puerto para el terminal. Si es así, puede poner en cuarentena el terminal anómalo en función de las políticas de autorización que se configuraron.

Configurar

Diagrama de la red

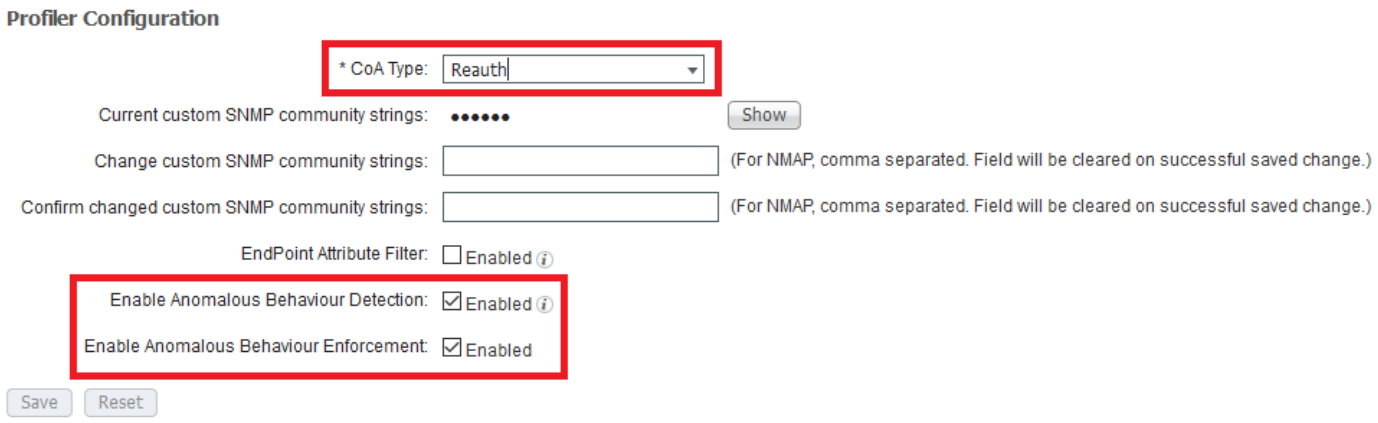


Configuraciones

Las configuraciones MAB y AAA simples se realizan en el switch y el WLC. Para utilizar esta función, siga estos pasos:

Paso 1. Habilite la detección anómala.

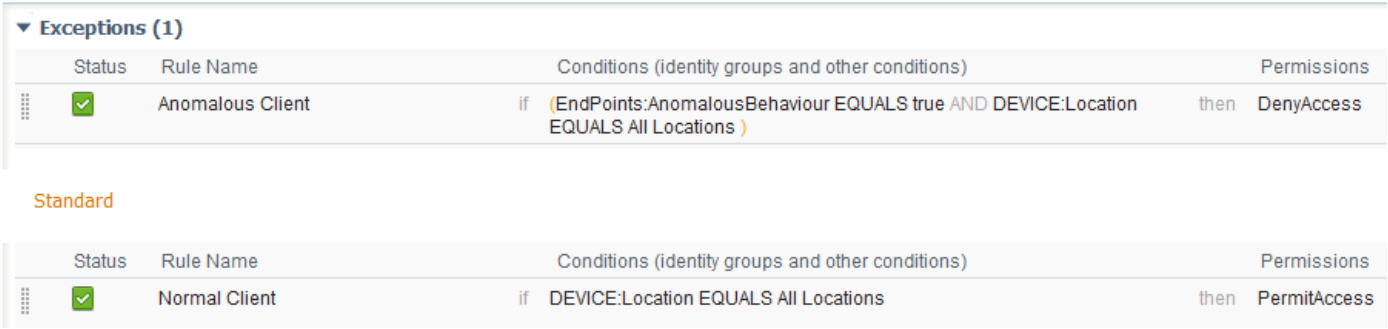
Vaya a **Administración > Sistema > Configuración > Definición de perfiles**.



La primera opción permite a ISE detectar cualquier comportamiento anómalo, pero no se envía ninguna CoA (modo de sólo visibilidad). La segunda opción permite a ISE enviar CoA una vez que se detecta un comportamiento anómalo (modo de aplicación).

Paso 2. Configuración de la política de autorización.

Configure el atributo AnomlousBehavicomo condición en la política de autorización, como se muestra en la imagen:

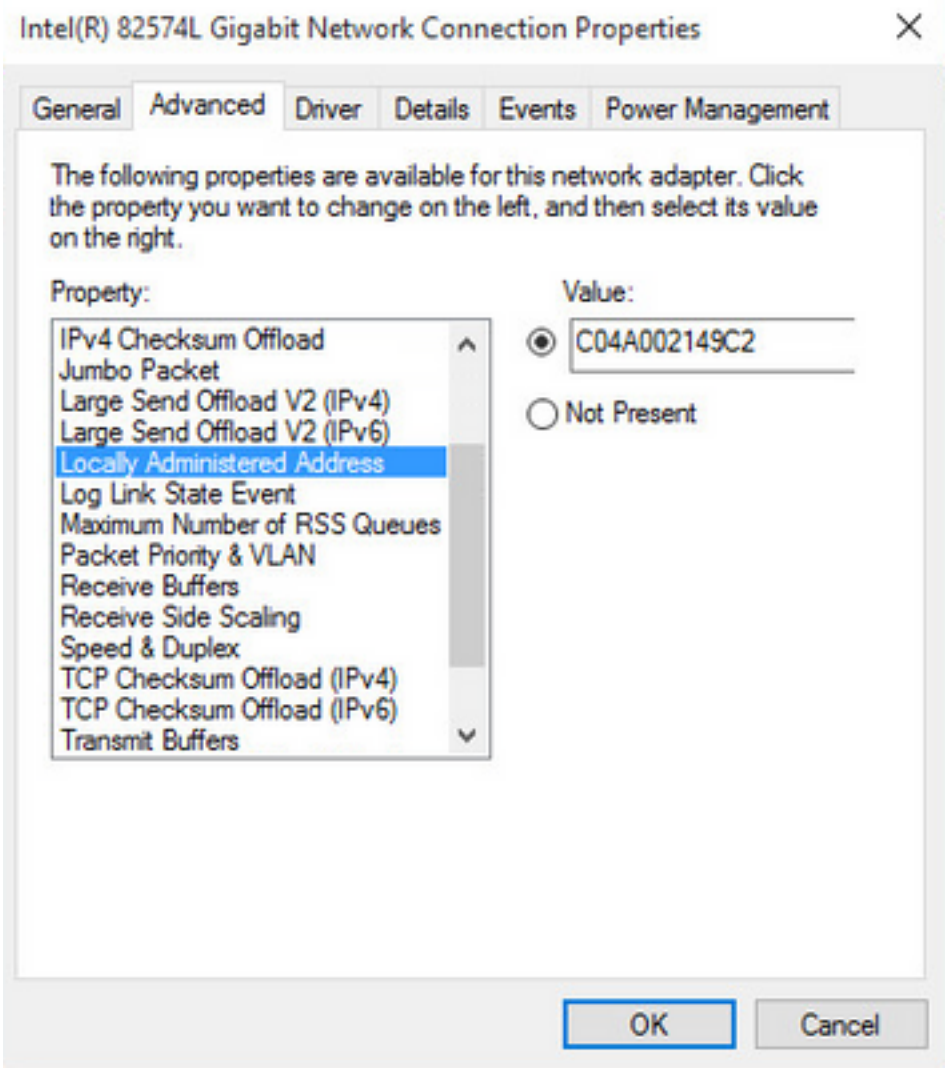


Verificación

Conéctese con un adaptador inalámbrico. Utilice el comando **ipconfig /all** para encontrar la dirección MAC del adaptador inalámbrico, como se muestra en la imagen:

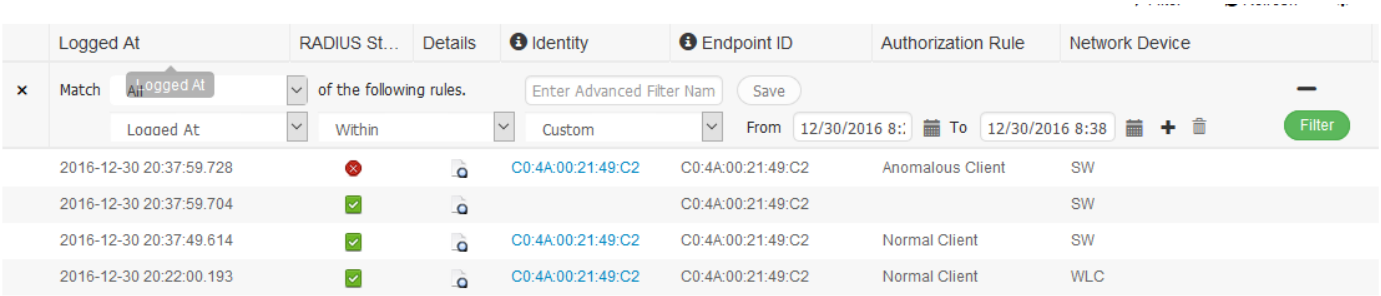
```
Wireless LAN adapter Wi-Fi:

   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 un usuario malintencionado, puede falsificar la dirección MAC del adaptador Ethernet para que coincida con la dirección MAC del usuario normal.

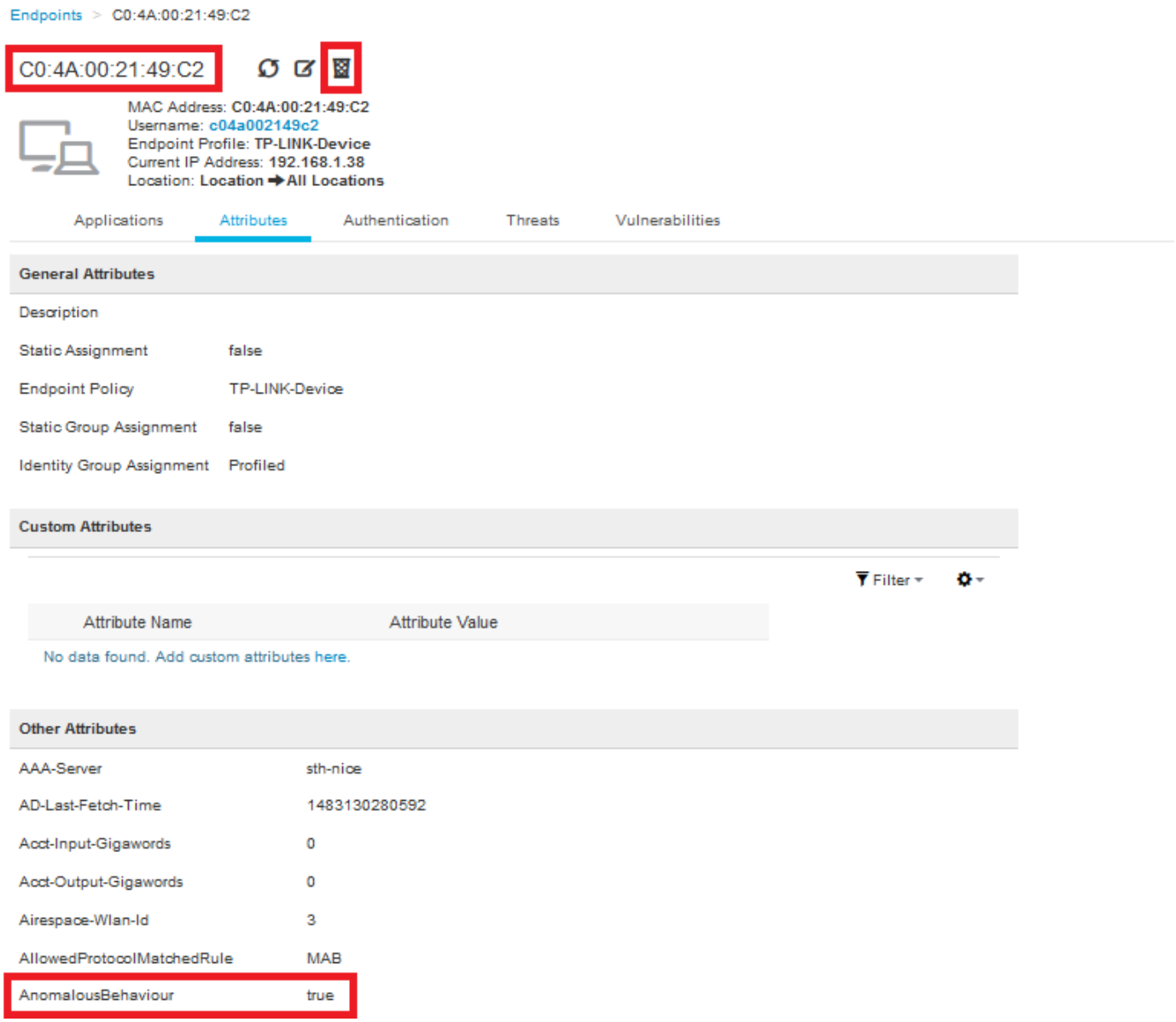


Una vez que el usuario normal se conecta, puede ver una entrada de terminal en la base de datos. Después, el usuario malintencionado se conecta mediante una dirección MAC falsa.

Desde los informes puede ver la conexión inicial del WLC. Después, el usuario malintencionado se conecta y, 10 segundos después, se activa una CoA debido a la detección del cliente anómalo. Dado que el tipo de CoA global se establece en **Reauth**, el punto final intenta conectarse de nuevo. ISE ya ha establecido el atributo AnomalousBehavior en True para que ISE coincida con la primera regla y niegue al usuario.

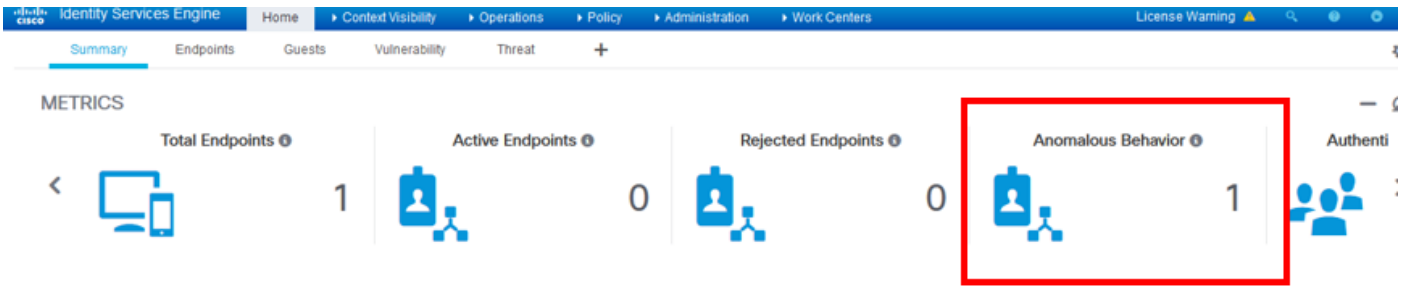


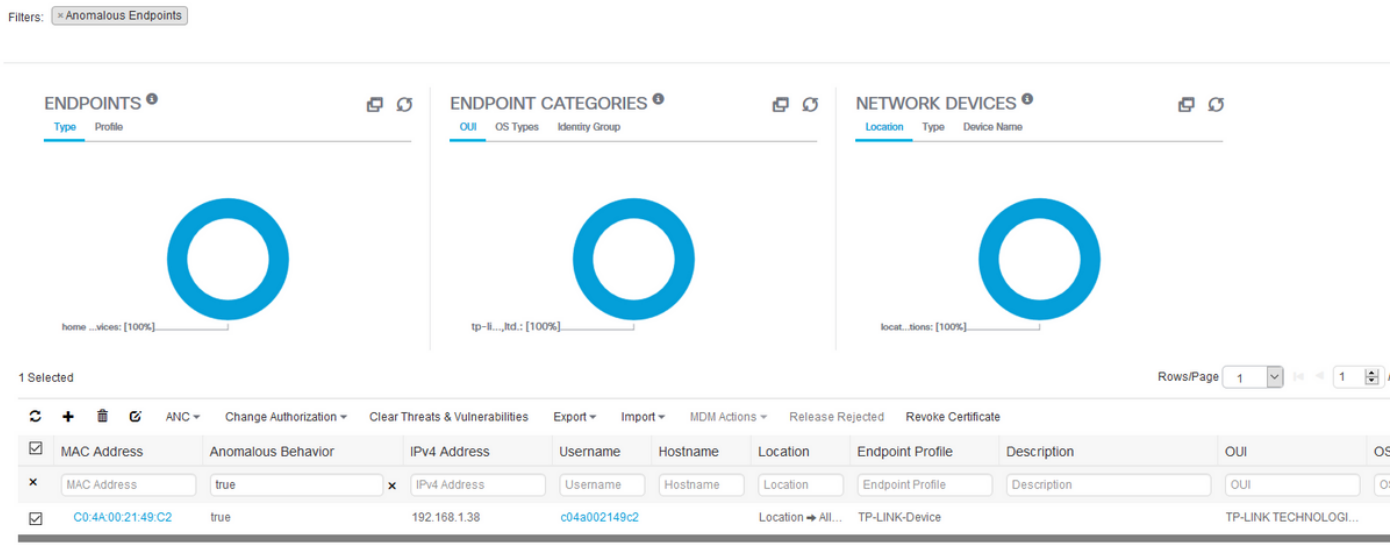
Como se muestra en la imagen, puede ver los detalles en el punto final en la pestaña Visibilidad de contexto:



Como puede ver, el extremo se puede eliminar de la base de datos para borrar este atributo.

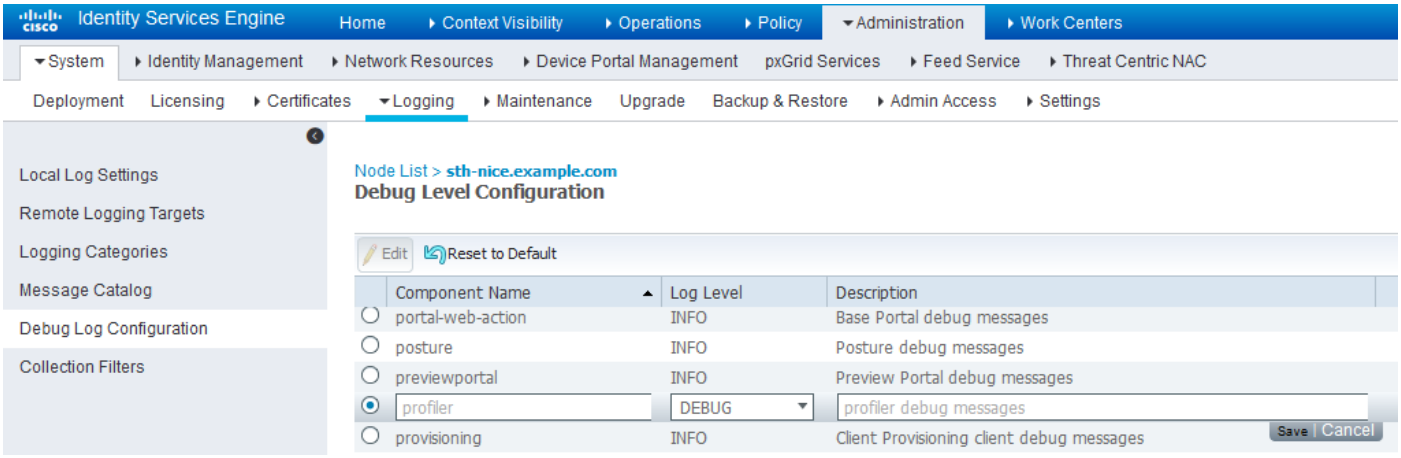
Como se muestra en la imagen, el panel incluye una nueva pestaña para mostrar el número de clientes que muestran este comportamiento:



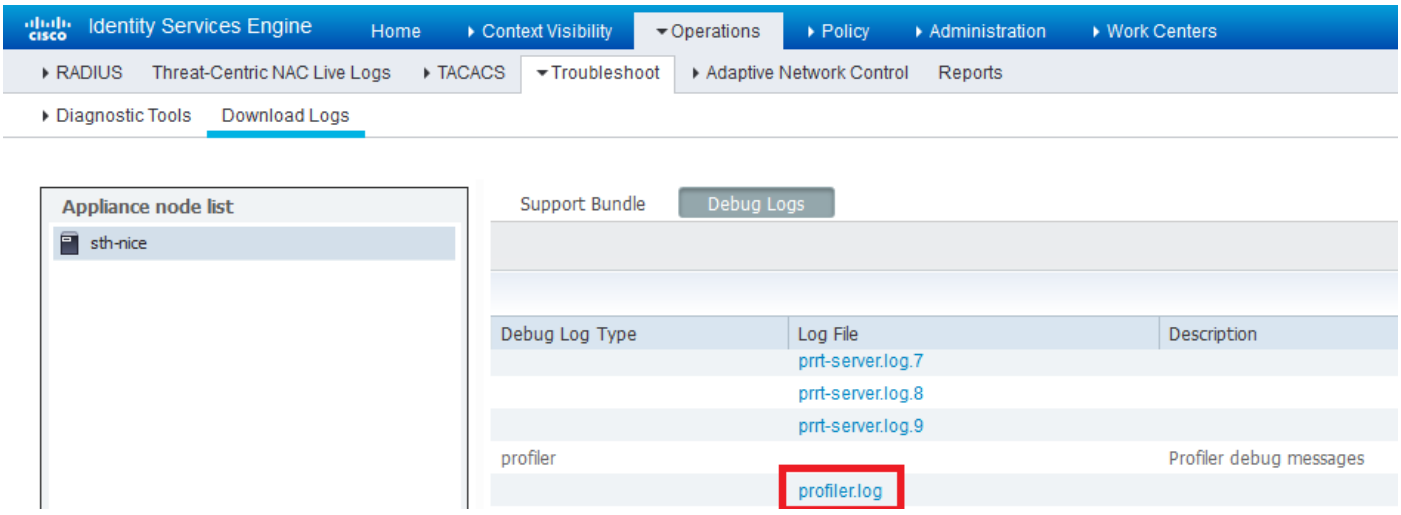


Troubleshoot

Para resolver problemas, habilite la depuración del generador de perfiles, mientras navega a **Administration > System > Logging > Debug Log Configuration**.



Para encontrar el archivo **Profiler.log** de ISE, navegue hasta **Operaciones > Registros de descarga > Registros de depuración**, como se muestra en la imagen:



Estos registros muestran algunos fragmentos del archivo **Profiles.log**. Como puede ver, ISE pudo detectar que el terminal con dirección MAC de C0:4A:00:21:49:C2 ha cambiado el método de

acceso al comparar los valores antiguos y nuevos de los atributos NAS-Port-Type. Es inalámbrico pero se cambia a 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
```

Por lo tanto, ISE actúa ya que la aplicación está habilitada. La acción aquí es enviar una CoA según la configuración global en la configuración de perfiles mencionada anteriormente. En nuestro ejemplo, el tipo CoA se establece en Reauth, lo que permite a ISE volver a autenticar el terminal y volver a verificar las reglas configuradas. Esta vez, coincide con la regla de cliente anómala 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 de ISE 2.2