Configurar a detecção e a aplicação anômalas do valor-limite em ISE 2.2

Índice

Introdução

Este original descreve a detecção e a aplicação anômalas do valor-limite. Esta é uma característica de perfilamento nova introduzida no Cisco Identity Services Engine (ISE) para a visibilidade aumentada da rede.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração prendida do desvio da autenticação de MAC (MAB) no interruptor
- Configuração sem fio MAB no controlador do Wireless LAN (WLC)
- Mudança da configuração da autorização (CoA) em ambos os dispositivos

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

1. Identity Services Engine 2.2
2. Controlador 8.0.100.0 do Wireless LAN
3. Interruptor 3750 15.2(3)E2 do Cisco catalyst

4. Windows 10 com prendido e adaptadores Wireless

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos usados neste original começaram com uma configuração cancelada (do padrão). Se sua rede está viva, certifique-se de que você compreende o impacto potencial do comando any.

Informações de fundo

A característica anômala da detecção do valor-limite permite que o ISE monitore mudanças aos atributos específicos e perfis para valores-limite conectados. Se uma mudança combina umas ou várias de regras preconfigured do comportamento anômalo, o ISE marcará o valor-limite como anômalo. Uma vez que detectado, o ISE pode tomar a ação (com CoA) e reforçar determinadas políticas para restringir o acesso do valor-limite suspeito. Um dos exemplos do uso para esta característica inclui a detecção de falsificação do MAC address.

- **Note**: Esta característica não endereça todas as encenações potenciais para a falsificação do MAC address. Seja por favor certo ler os tipos de anomalias cobertas por esta característica para determinar sua aplicabilidade a seus casos do uso.

Uma vez que a detecção é permitida, o ISE monitora toda a informação nova recebida para valores-limite existentes e verifica se estes atributos mudaram:

1. **NAS-Porta-tipo** - Determina se o método de acesso deste valor-limite mudou. Por exemplo, se o mesmo MAC address que conectou através do dot1x prendido é usado para o dot1x e o visto-versa sem fio.

2. **Identificação da classe DHCP** - Determina se o tipo de cliente/vendedor do valor-limite mudou. Isto aplica-se somente quando o atributo identificação da classe DHCP é povoado com algum valor e mudado então a um outro valor. Se um valor-limite é configurado com um IP Estático, o atributo identificação da classe DHCP não estará povoado no ISE. Mais tarde, se umas outras paródias do dispositivo o MAC address e os usos DHCP, a identificação da classe mudarão de um valor vazio a uma corda específica. Isto não provocará a detecção do comportamento de Anomouls.

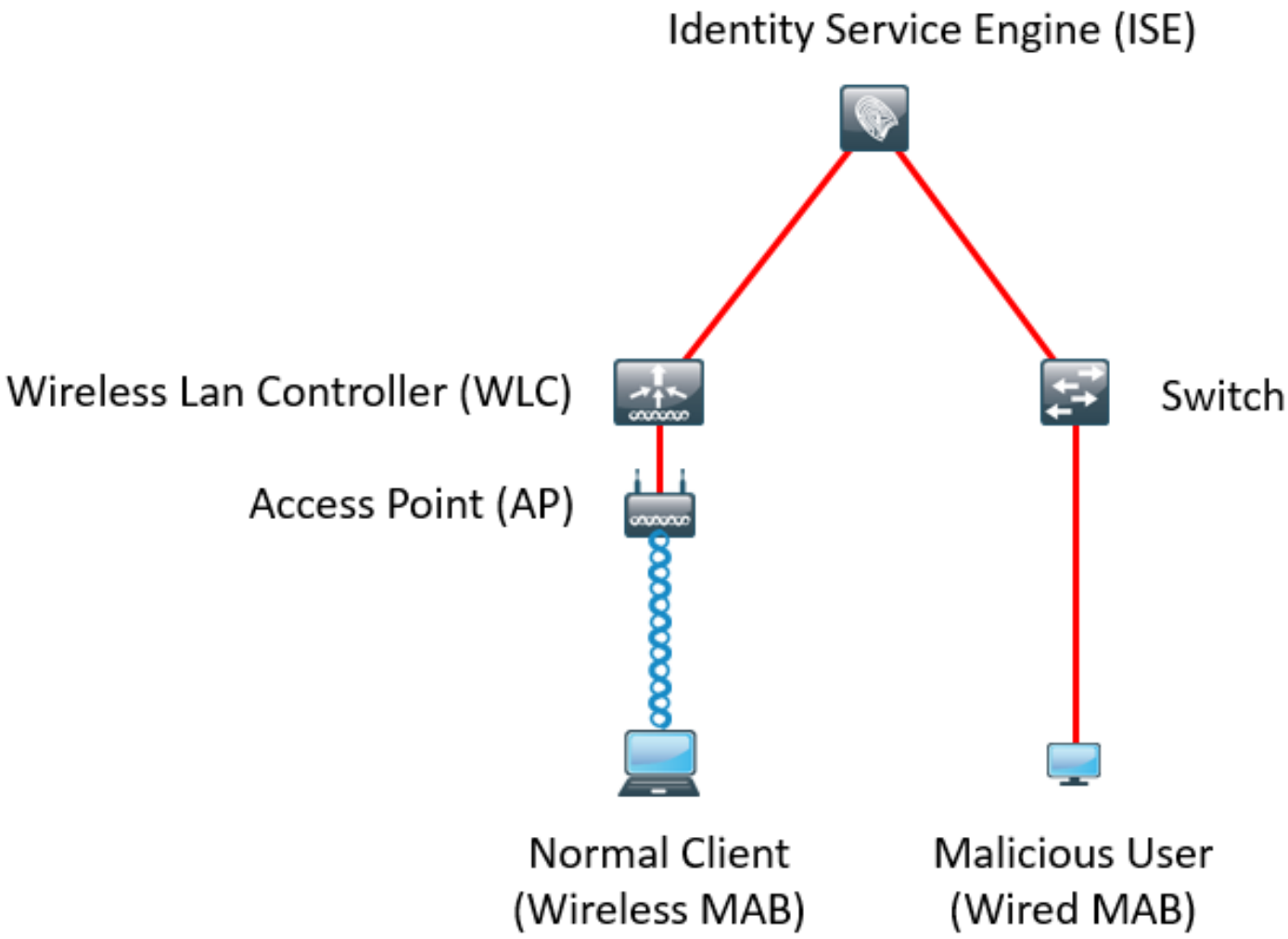
3. **Política do valor-limite -** Uma mudança no perfil do valor-limite da **impressora** ou do **telefone IP à estação de trabalho**.

Uma vez que o ISE detecta uma das mudanças mencionadas acima, o atributo de AnomalousBehaviour está adicionado ao valor-limite e ao grupo para retificar. Isto pode ser usado mais tarde como uma circunstância em políticas da autorização para restringir o acesso para o valor-limite nas autenticações futuras.

Se a aplicação é configurada, o ISE pode enviar um CoA uma vez que a mudança é detectada para autenticar novamente ou executar um salto da porta para o valor-limite. Se de fato, pode quarantine o valor-limite anômalo segundo as políticas da autorização que estiveram configuradas.

Configurar

Diagrama da rede

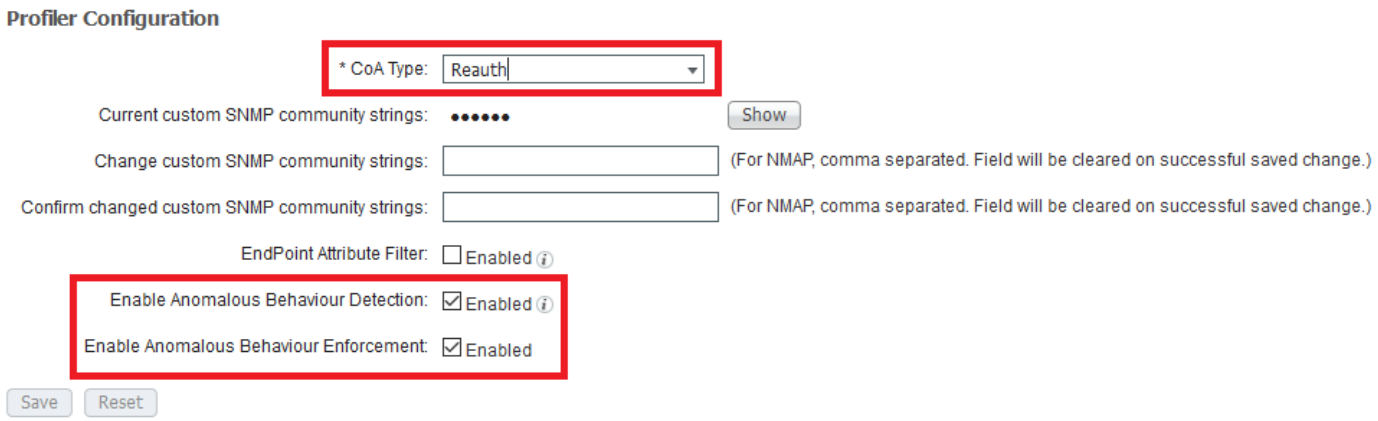


Configurações

Os MAB simples e as configurações de AAA são executados no interruptor e no WLC. Para utilizar esta característica, siga estas etapas:

Etapa 1. Permita a detecção anômala.

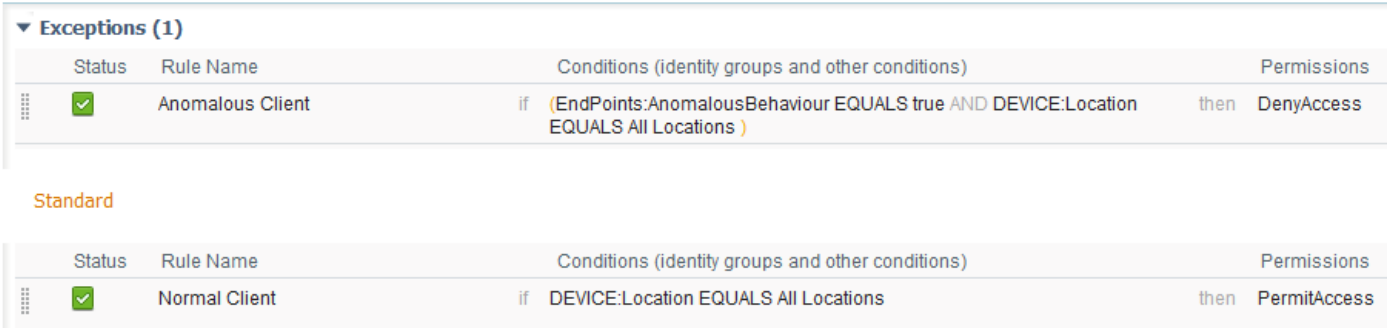
Navegue à **administração > ao sistema > aos ajustes > perfilando**.



A primeira opção permite que o ISE detecte todo o comportamento anômalo mas nenhum CoA é enviado (modo da visibilidade-Somente). A segunda opção permite que o ISE envie o CoA uma vez que o comportamento anômalo é detectado (modo da aplicação).

Etapa 2. Configurar a política da autorização.

Configurar o atributo de Anomlousbehaviour como uma condição na política da autorização, segundo as indicações da imagem:

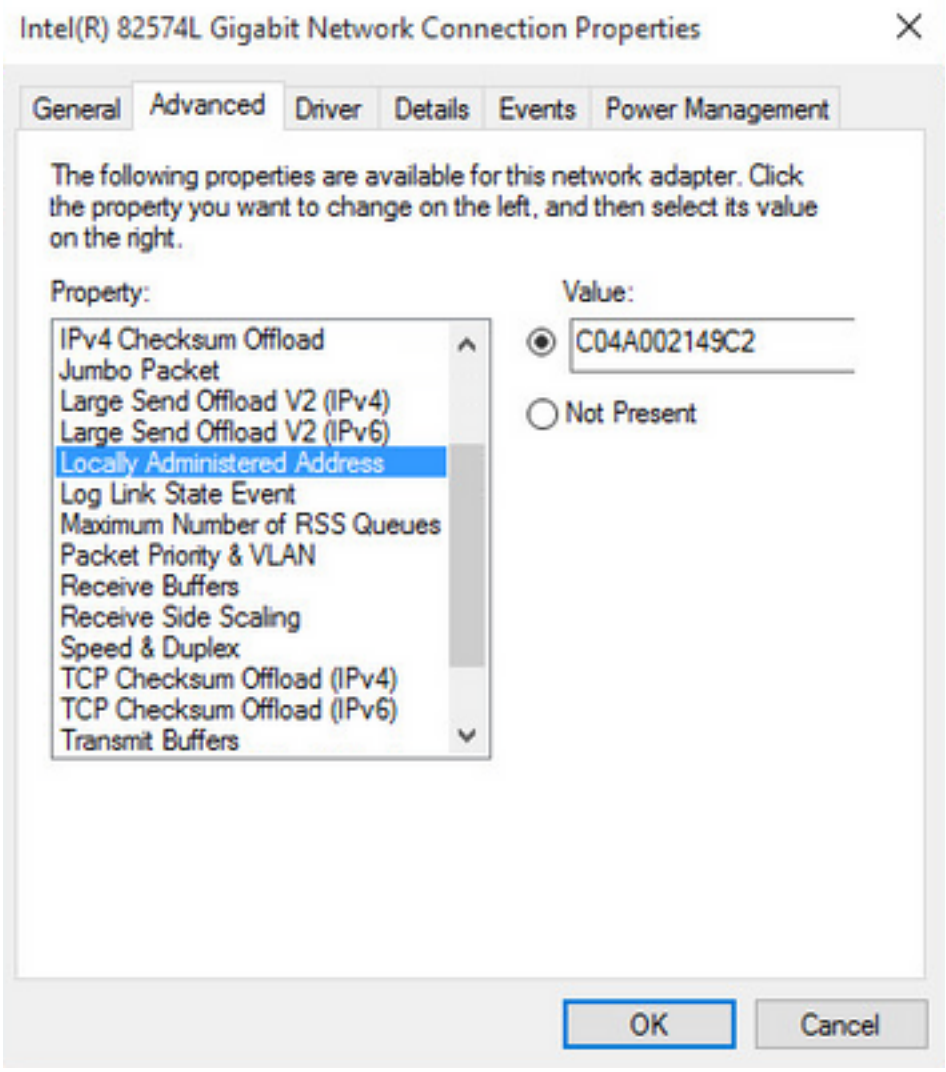


Verificar

Conecte com um adaptador Wireless. Use o comando ipconfig **/all** encontrar o MAC address do adaptador Wireless, segundo as indicações da imagem:

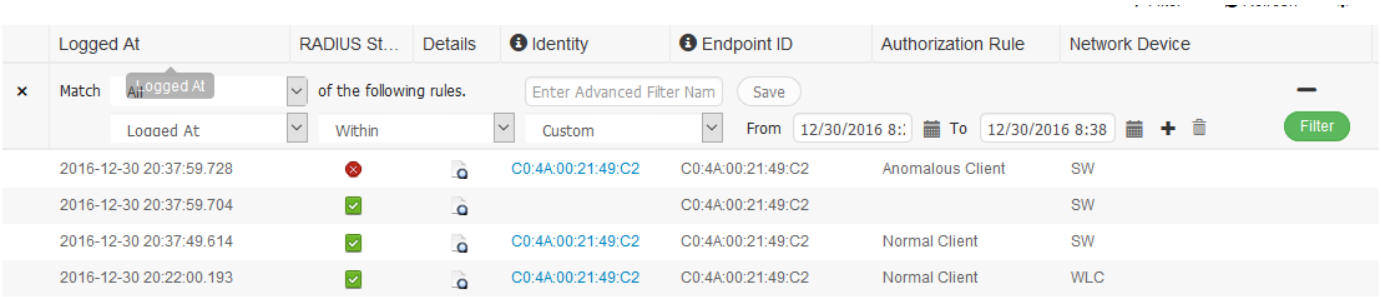
```
Wireless LAN adapter Wi-Fi:

   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 um usuário malicioso, você pode spoof o MAC address do adaptador do Ethernet combinar o MAC address do usuário normal.

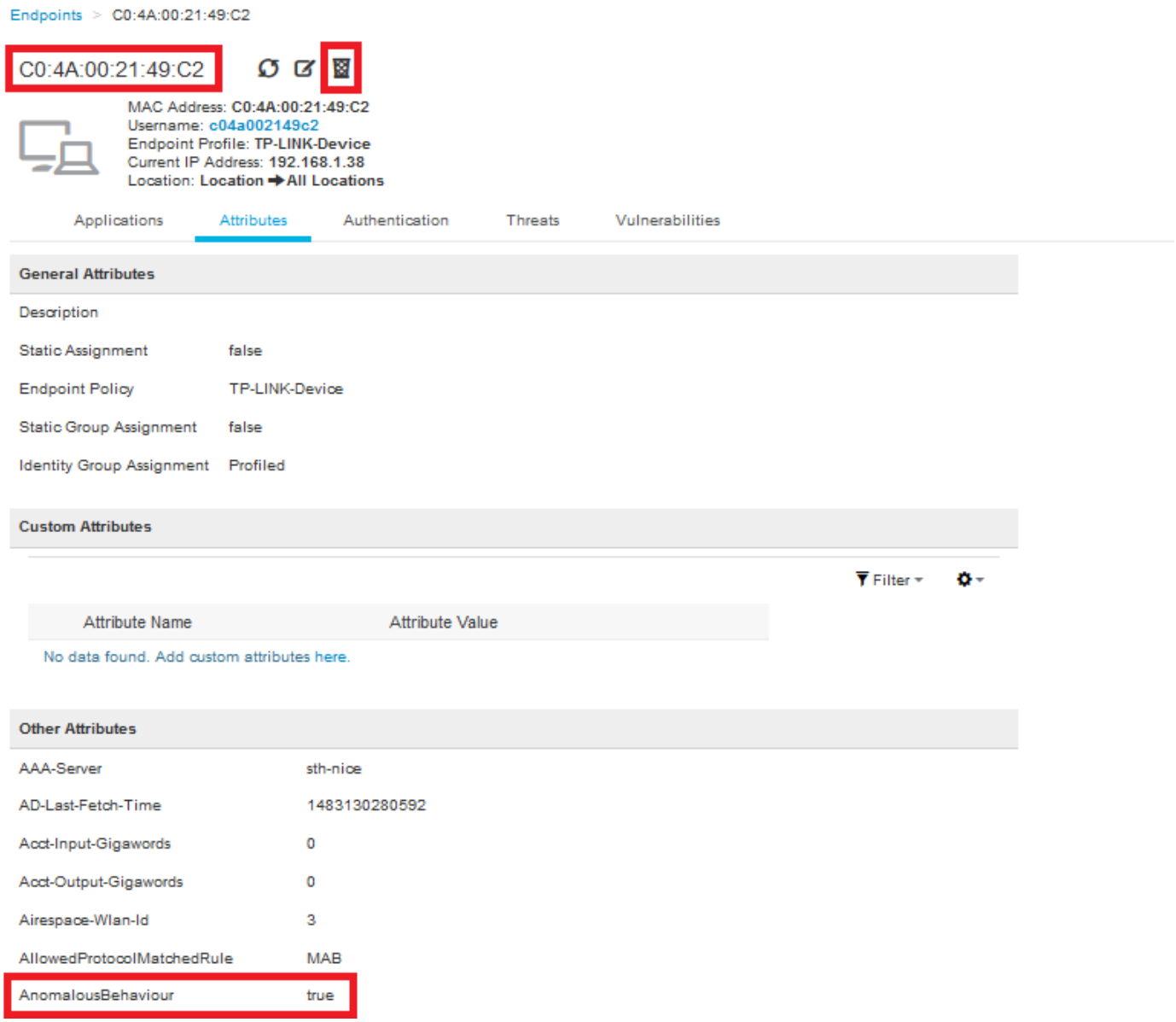


Uma vez que o usuário normal conecta, você pode ver uma entrada do valor-limite no base de dados. Mais tarde, o usuário malicioso conecta usando um MAC address falsificado.

Dos relatórios você pode ver a conexão inicial do WLC. Mais tarde, o usuário malicioso conecta e o 10 segundos depois, um CoA é provocado devido à detecção do cliente anômalo. Desde que o tipo global CoA é ajustado a **Reauth**, o valor-limite tenta conectar outra vez. O ISE já ajustou o atributo de AnomalousBehaviour para retificar assim que o ISE combina a primeira regra e nega o usuário.

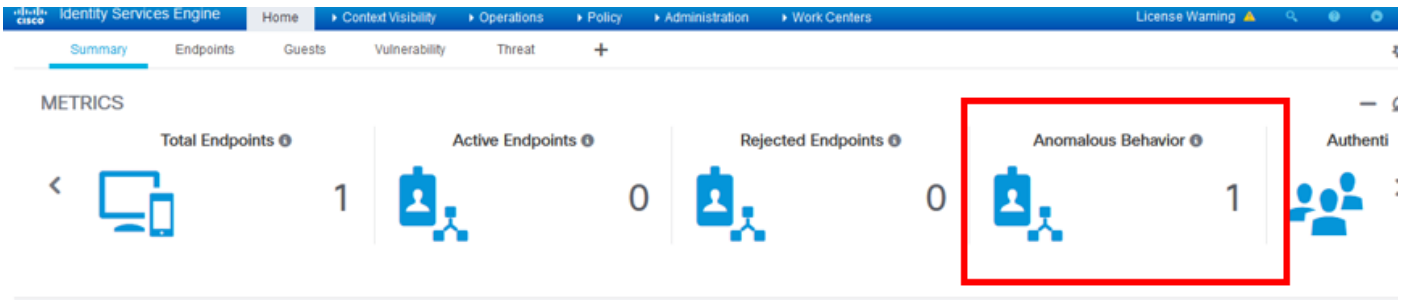


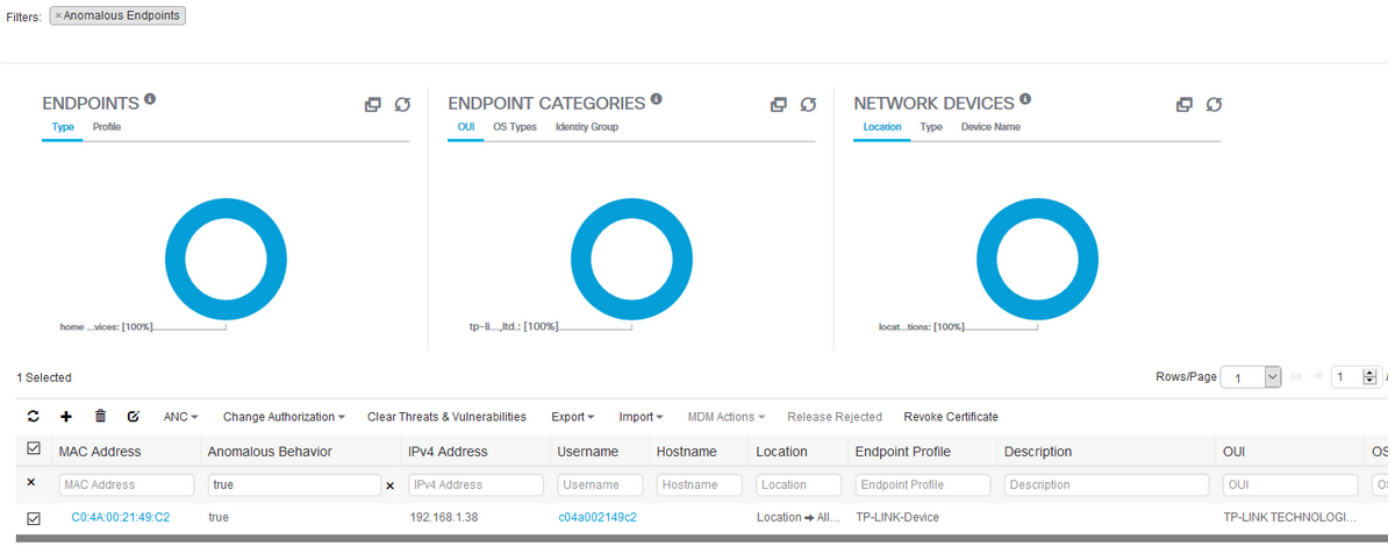
Segundo as indicações da imagem, você pode ver os detalhes sob o valor-limite na aba da visibilidade do contexto:



Como você pode ver, o valor-limite pode ser suprimido do base de dados para cancelar este atributo.

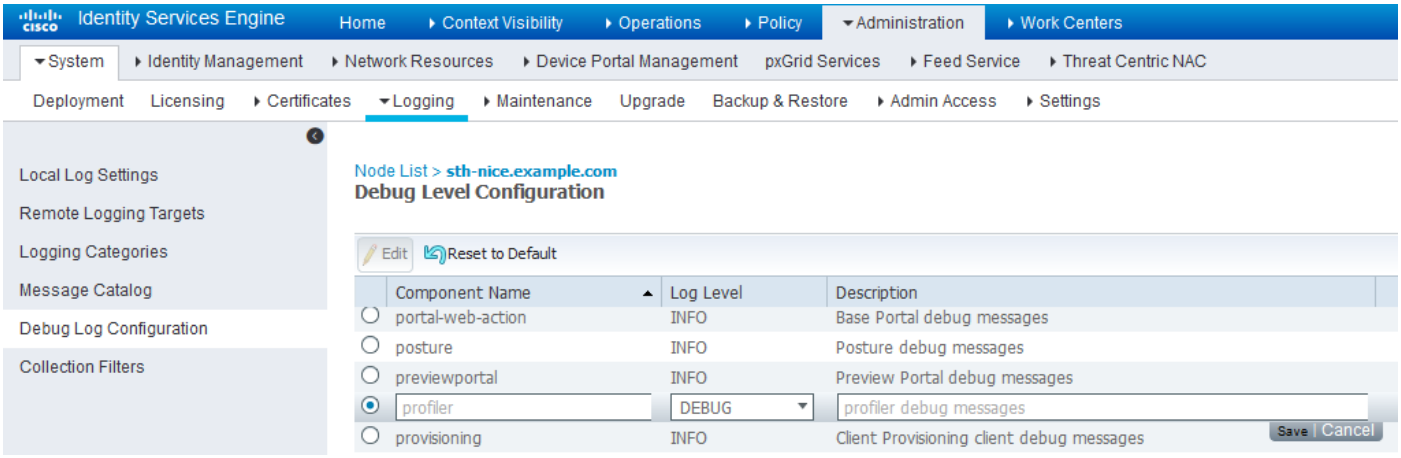
Segundo as indicações da imagem, o painel inclui uma aba nova para mostrar o número de clientes que exibem este comportamento:



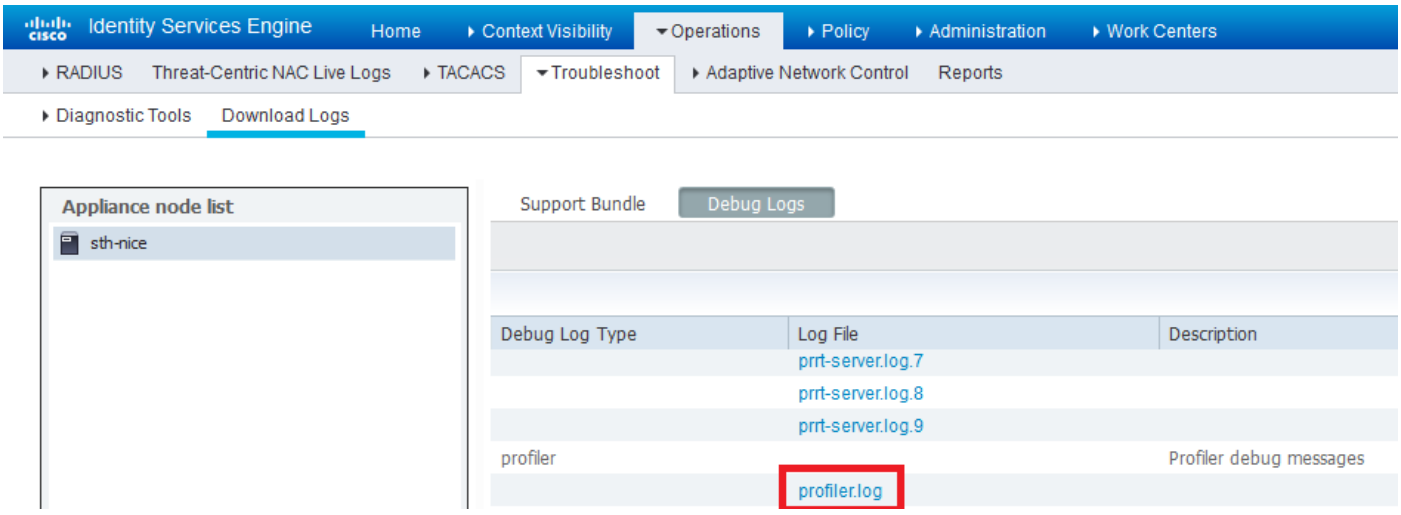


Troubleshooting

A fim pesquisar defeitos, permita o perfilador debugam, como você navega à **administração > ao sistema > registrando > debuga a configuração do log**.



A fim encontrar o arquivo ISE **Profiler.log**, navegue às **operações > aos logs da transferência > debugam logs**, segundo as indicações da imagem:



Estes logs mostram algumas pequenas notícias do arquivo de **Profiling.log**. Como você pode ver, o ISE podia detectar que o valor-limite com MAC address de C0:4A:00:21:49:C2 mudou o método

de acesso comparando os valores velhos e novos do NAS-Porta-tipo atributos. É sem fio mas é mudado aos 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
```

Consequentemente, o ISE toma a ação desde que a aplicação é permitida. A ação aqui é enviar um CoA segundo a configuração global nos ajustes de perfilamento mencionados acima. Em nosso exemplo, o tipo CoA é ajustado a Reauth que permite que o ISE autenticar novamente o valor-limite e verifique novamente as regras que foram configuradas. Esta vez, combina a regra anômala do cliente e consequentemente nega-se.

```
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
```

Informações Relacionadas

- Guia de Administração ISE 2.2