在ISE 2.2上配置异常终端检测和实施

目录

简介

本文档介绍异常终端检测和实施。这是思科身份服务引擎(ISE)中引入的新分析功能，用于增强网络可视性。

先决条件

要求

Cisco 建议您了解以下主题：

- 交换机上的有线MAC身份验证绕行(MAB)配置
- 无线局域网控制器(WLC)上的无线MAB配置
- 两台设备上的授权更改(CoA)配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

1. 身份服务引擎2.2
2. 无线局域网控制器8.0.100.0
3. 思科Catalyst交换机3750 15.2(3)E2
4. 带有有线和无线适配器的Windows 10

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

异常终端检测功能允许ISE监控对所连接终端的特定属性和配置文件的更改。如果更改与一个或多个预配置的异常行为规则匹配，ISE会将终端标记为异常。检测到后，ISE可以采取操作（使用CoA）并实施某些策略以限制可疑终端的访问。 此功能的使用案例之一包括MAC地址欺骗检测。

- 注意：此功能不能解决MAC地址欺骗的所有潜在场景。 请务必阅读此功能涵盖的异常类型，以确定其适用于您的使用案例。

启用检测后，ISE会监控现有终端收到的任何新信息，并检查这些属性是否已更改：

1. **NAS-Port-Type** — 确定此终端的访问方法是否已更改。例如，如果无线Dot1x使用通过有线Dot1x连接的相同MAC地址，反之亦然。

2. **DHCP类ID** — 确定终端的客户端/供应商类型是否已更改。仅当DHCP类ID属性填充了特定值并随后更改为其他值时，才适用。如果终端配置了静态IP，ISE上不会填充DHCP类ID属性。稍后，如果另一台设备欺骗MAC地址并使用DHCP，则类ID将从空值更改为特定字符串。这不会触发异常行为检测。

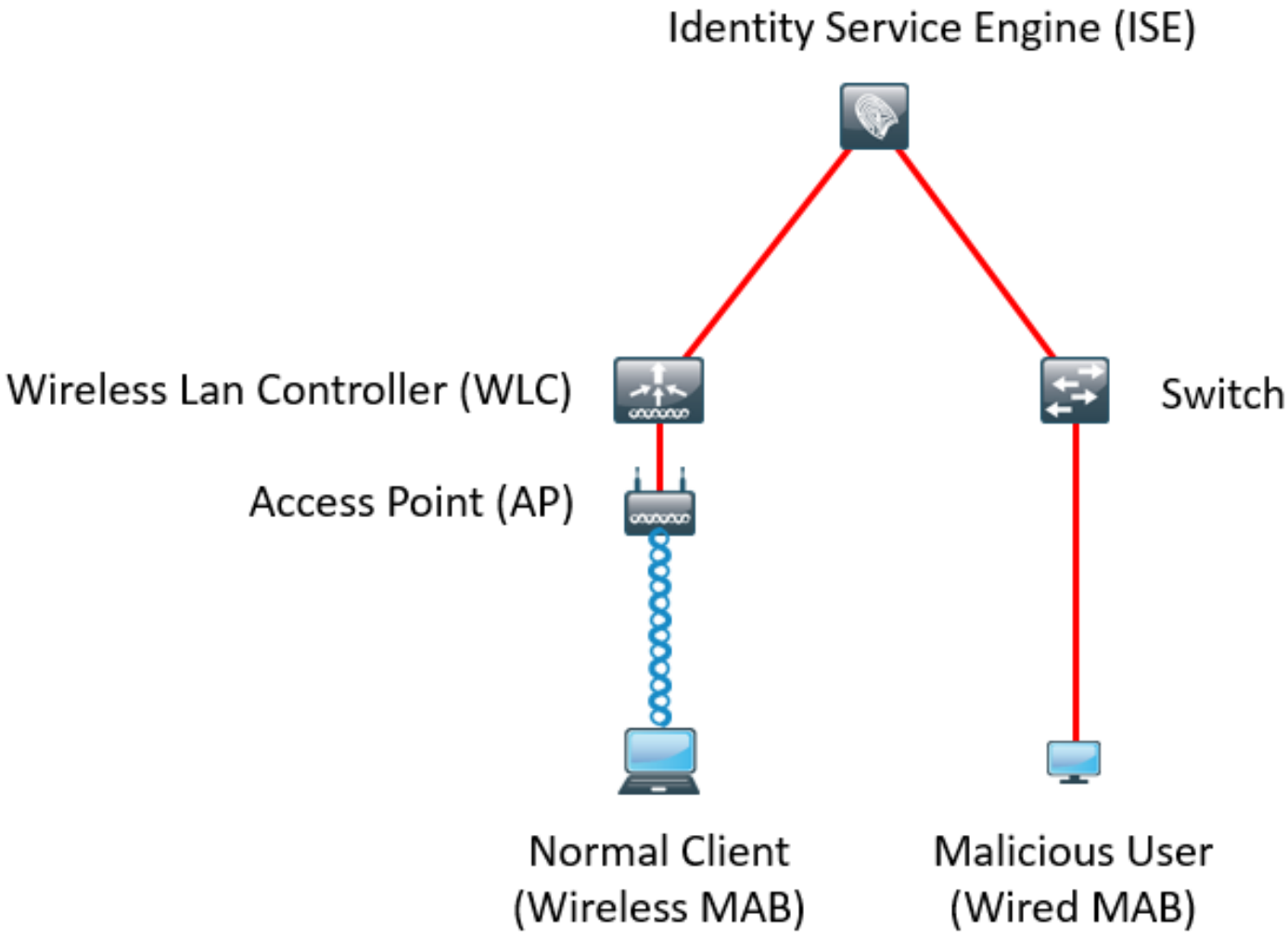
3. **终端策略** — 终端配置文件从打印机或IP电话更改到工作站的更改。

一旦ISE检测到上述更改之一，AnnogualBehavior属性将添加到终端并设置为True。稍后，可将其用作授权策略中的条件，以限制终端在未来身份验证中的访问。

如果配置了Enforcement，ISE可以在检测到更改后发送CoA，以重新验证或执行终端的端口退回。如果有效，它可以根据配置的授权策略隔离异常终端。

配置

网络图

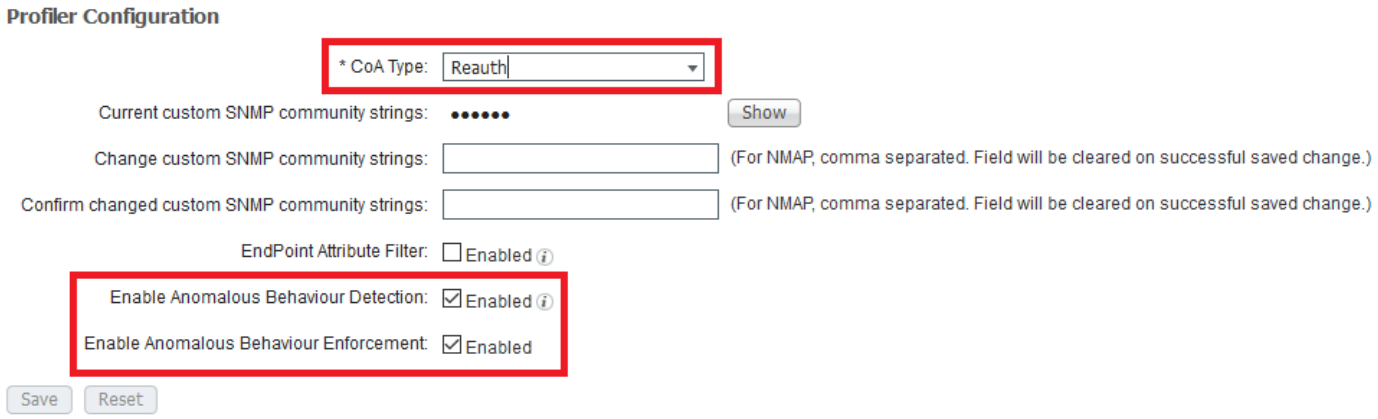


配置

在交换机和WLC上执行简单的MAB和AAA配置。要使用此功能，请执行以下步骤：

步骤1.启用异常检测。

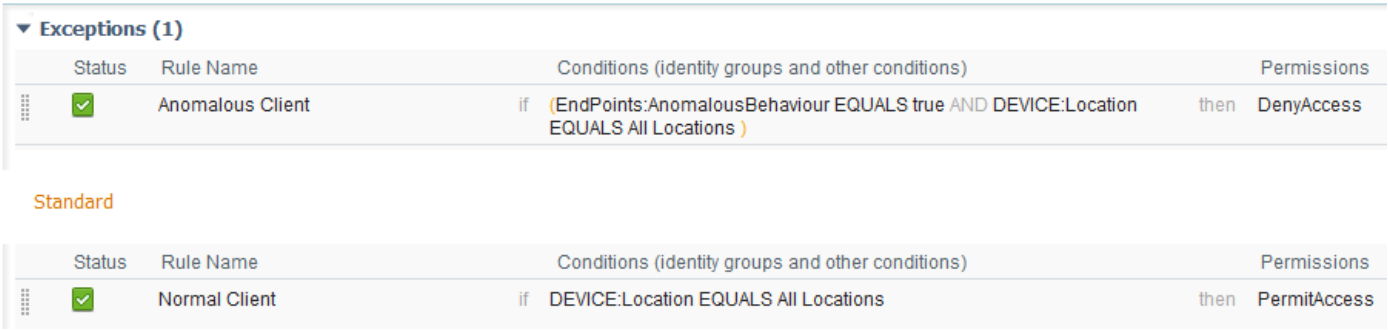
导航至**管理>系统>设置>分析**。



第一个选项允许ISE检测任何异常行为，但不发送CoA（仅可视模式）。 第二个选项允许ISE在检测到异常行为（实施模式）后发送CoA。

步骤2.配置授权策略。

在授权策略中将异常行为属性配置为条件，如图所示：

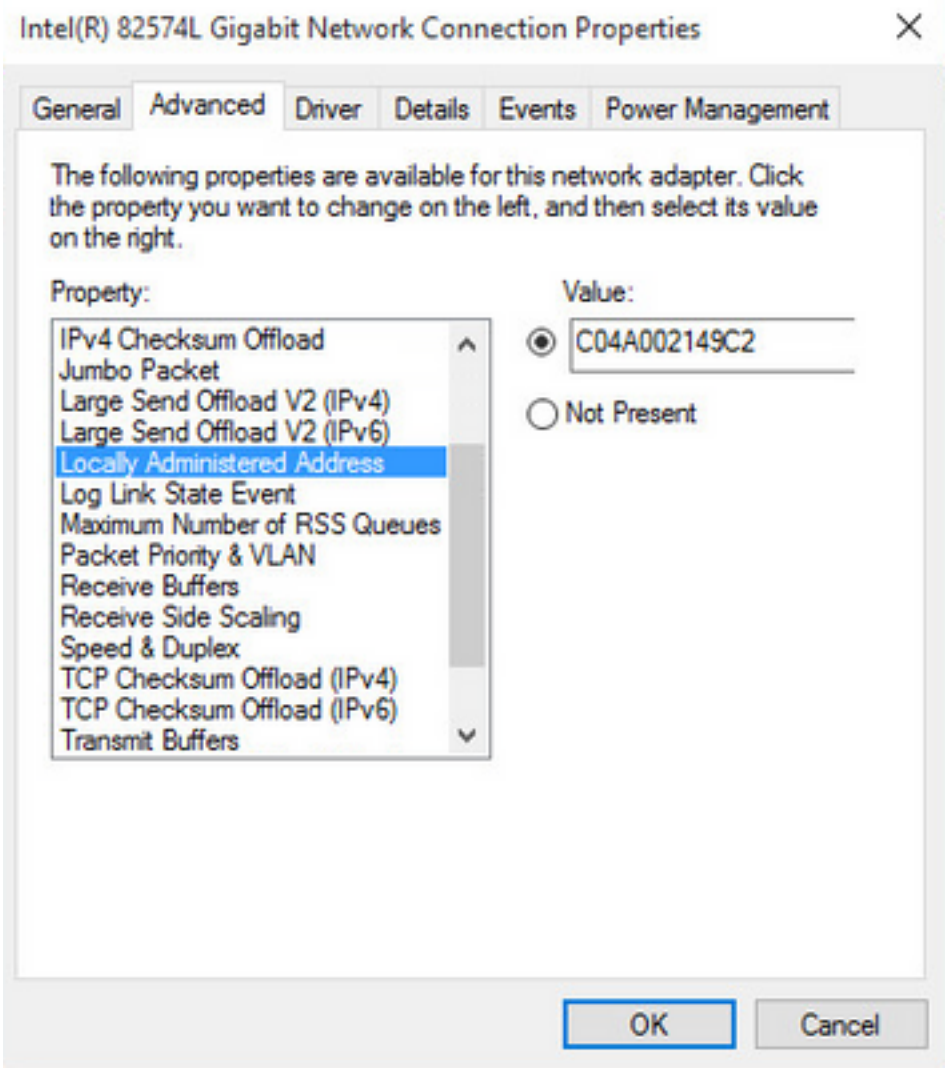


验证

连接无线适配器。使用命令**ipconfig /all**查找无线适配器的MAC地址，如图所示：

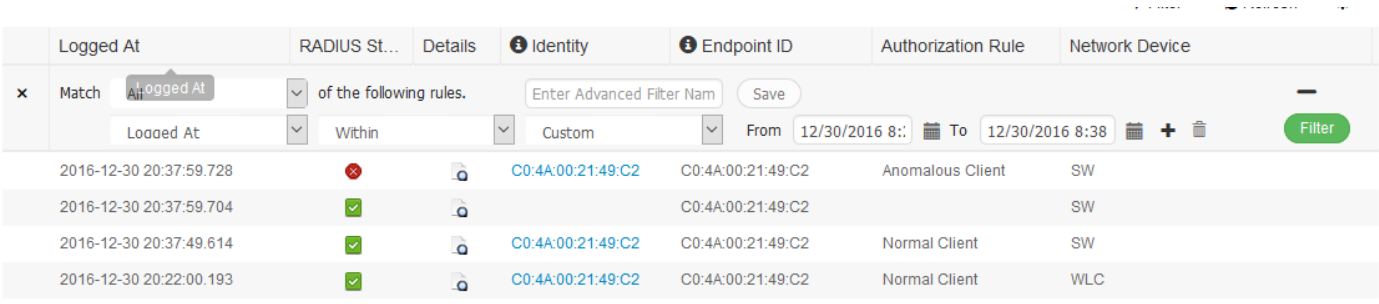
```
Wireless LAN adapter Wi-Fi:

   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
```

要模拟恶意用户，您可能会假冒以太网适配器的MAC地址，以匹配普通用户的MAC地址。

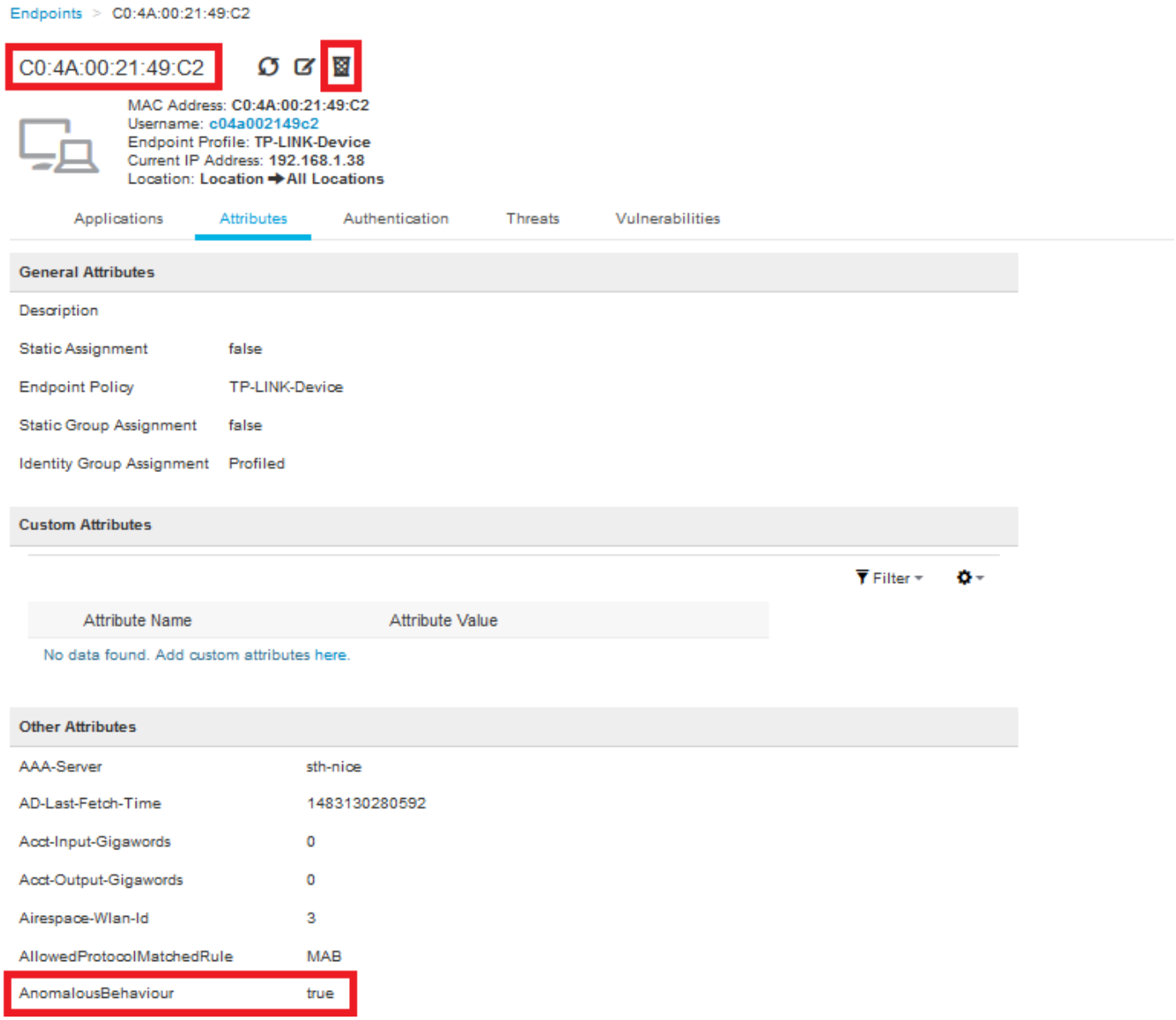


正常用户连接后，您可以在数据库中看到终端条目。之后，恶意用户使用伪造的MAC地址进行连接。

从报告中，您可以看到WLC的初始连接。之后，恶意用户连接，10秒后，由于检测到异常客户端，CoA被触发。由于全局CoA类型设置为**Reauth**，因此终端将尝试重新连接。ISE已将AnnogualBehavior属性设置为True，因此ISE匹配第一个规则并拒绝用户。

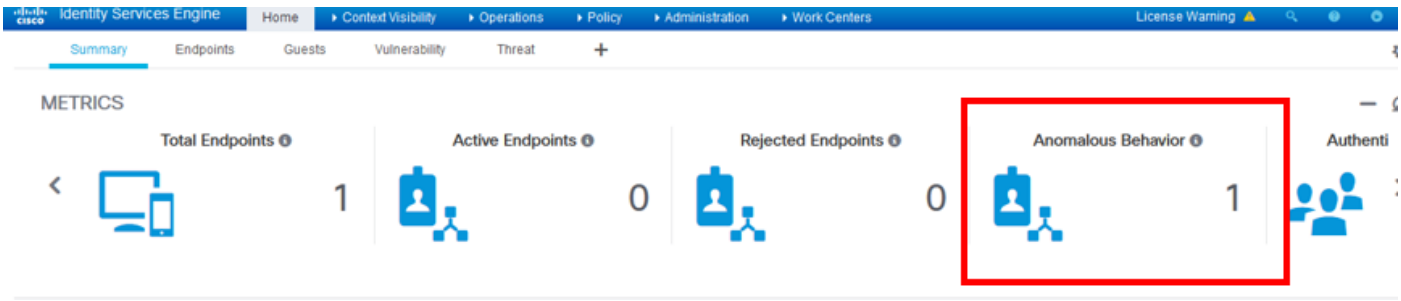


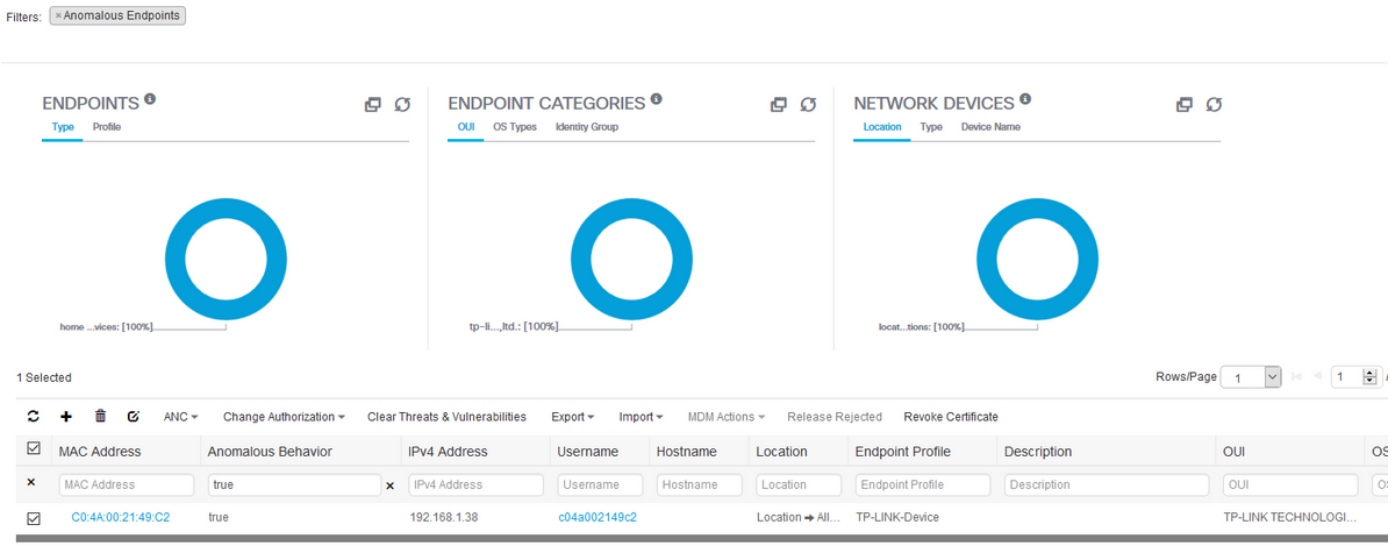
如图所示，您可以在“情景可视性”(Context Visibility)选项卡中查看终端下的详细信息：



如您所见，可以从数据库中删除终端以清除此属性。

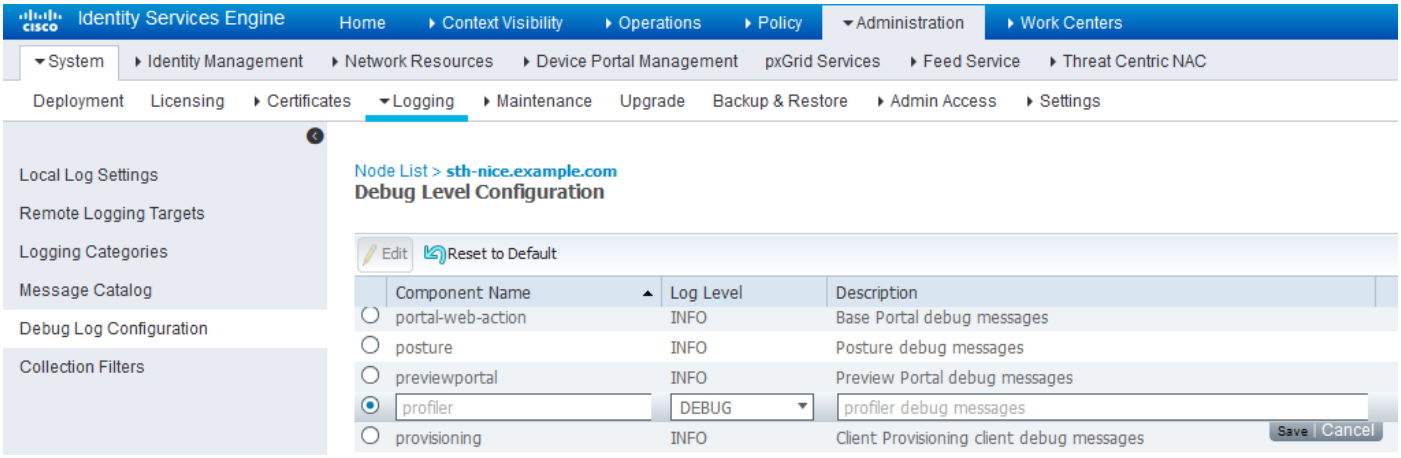
如图所示，控制面板包含一个新选项卡，用于显示表现出此行为的客户端数量：



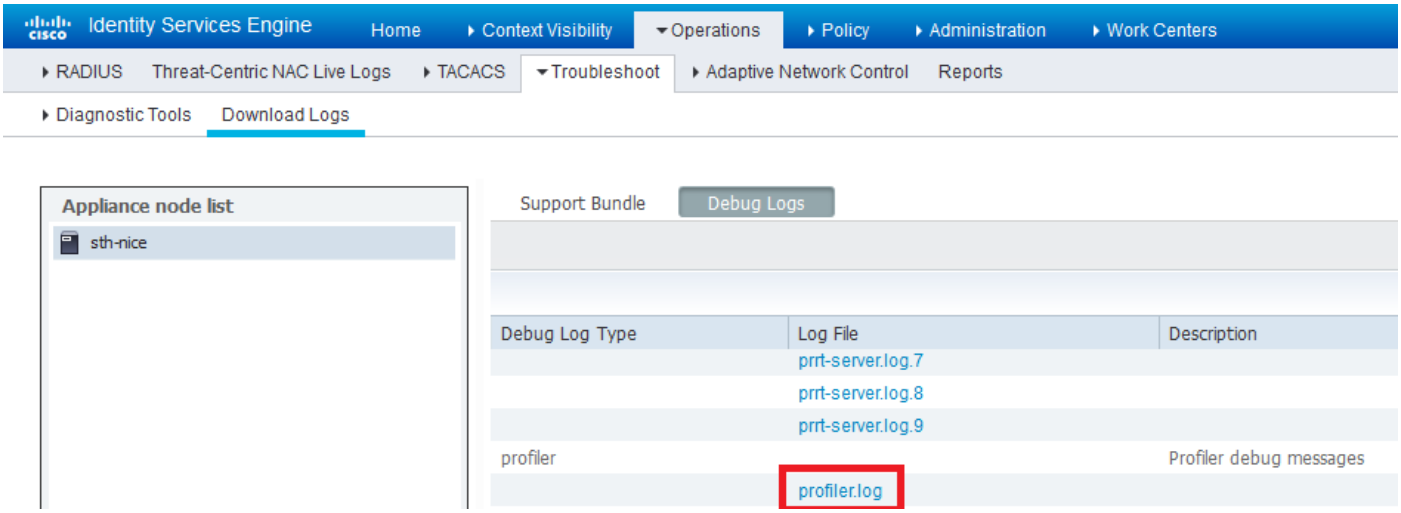


故障排除

要进行故障排除，请在导航到Administration > System > Logging > Debug Log Configuration时启**用分析器调试。**



要查找ISE Profiler.log文**件，请导**航至**操作>下载日志>调试日**志，如图所示：



这些日志显示Profiling.log文**件中的一些**片段。如您所见，ISE通过比较NAS端口类型属性的新旧值来检测MAC地址为C0:4A:00:21:49:C2的终端是否已更改了访问方法。它是无线的，但已更改为以太网。

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

因此，ISE在启用实施后采取操作。此处的操作是根据上述分析设置中的全局配置发送CoA。在我们的示例中，CoA类型设置为Reauth，这允许ISE重新验证终端并重新检查已配置的规则。这次，它与异常客户端规则匹配，因此被拒绝。

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**

相关信息

- ISE 2.2管理指南