تكوين اكتشاف نقطة النهاية الشاذة وتنفيذها على ISE 2.2

المحتويات

المقدمة

يصف هذا وثيقة شاذ نقطة نهاية كشف وفرض. هذه ميزة وصيف جديدة تم إدخالها في Cisco Identity Services Engine (ISE) لتحسين إمكانية رؤية الشبكة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تشكيل مجرى مصادقة MAC السلكي (MAB) على المحول
- تكوين MAB اللاسلكي على وحدة التحكم في الشبكة المحلية اللاسلكية (WLC)
- تغيير تكوين التفويض (CoA) على كل الجهازين

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

1. Identity Services Engine، الإصدار 2.2
2. وحدة التحكم في شبكة LAN اللاسلكية 8.0.100.0
3. المحول Cisco Catalyst Switch 3750 15.2(3)E2
4. نظام التشغيل Windows 10 المزود بمحولات سلكية ولاسلكية

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

تتيح ميزة "اكتشاف نقطة النهاية الشاذة" ل ISE إمكانية مراقبة التغييرات التي تطرأ على سمات وملفات تعريف معينة لنقاط النهاية المتصلة. إذا تطابق تغيير ما مع قاعدة أو أكثر من قواعد السلوك الشاذة المكونة مسبقا، سيقوم ISE بوضع علامة على نقطة النهاية على أنها غير سوية. وبمجرد اكتشافه، يمكن أن يقوم ISE باتخاذ إجراء (مع CoA) وفرض سياسات معينة لتقييد الوصول إلى نقطة النهاية المشتبه بها. يتضمن أحد حالات الاستخدام لهذه الميزة اكتشاف انتحال عنوان MAC.

- ملاحظة: لا تعالج هذه الميزة جميع السيناريوهات المحتملة لانتحال عنوان MAC. يوصى بالتأكد من فراغة أنواع الحالات الشاذة التي تغطيها هذه الميزة لتحديد إمكانية تطبيقها على حالات الاستخدام الخاصة بك.

وبمجرد تمكين الكشف، يراقب ISE أي معلومات جديدة يتم استقبالها لنقاط النهاية الموجودة ويتحقق مما إذا كانت هذه السمات قد تغيرت:

1. **NAS-Port-Type** - يحدد ما إذا كانت طريقة الوصول لنقطة النهاية هذه قد تغيرت. على سبيل المثال، إذا كان عنوان MAC نفسه المتصل عبر Wired Dot1x مستخدم ل Wireless Dot1x و visa-versa.

2. **معرف فئة DHCP** - يحدد ما إذا كان نوع نقطة النهاية العميل/المورد قد تغير. ال ينطبق هذا إال عندما يتم تعبئة سمة معرف فئة DHCP بقيمة معينة ثم يتم تغييرها إلى قيمة أخرى. إذا تم تكوين نقطة نهاية باستخدام IP ثابت، فلن يتم نشر سمة معرف فئة DHCP على ISE. وفيما بعد، إذا قام جهاز آخر بمزاعمة عنوان MAC واستخدام DHCP، فسيتغير معرف الفئة من قيمة فارغة إلى سلسلة محددة. لن يؤدي هذا إلى تشغيل اكتشاف سلوك Anomouls.

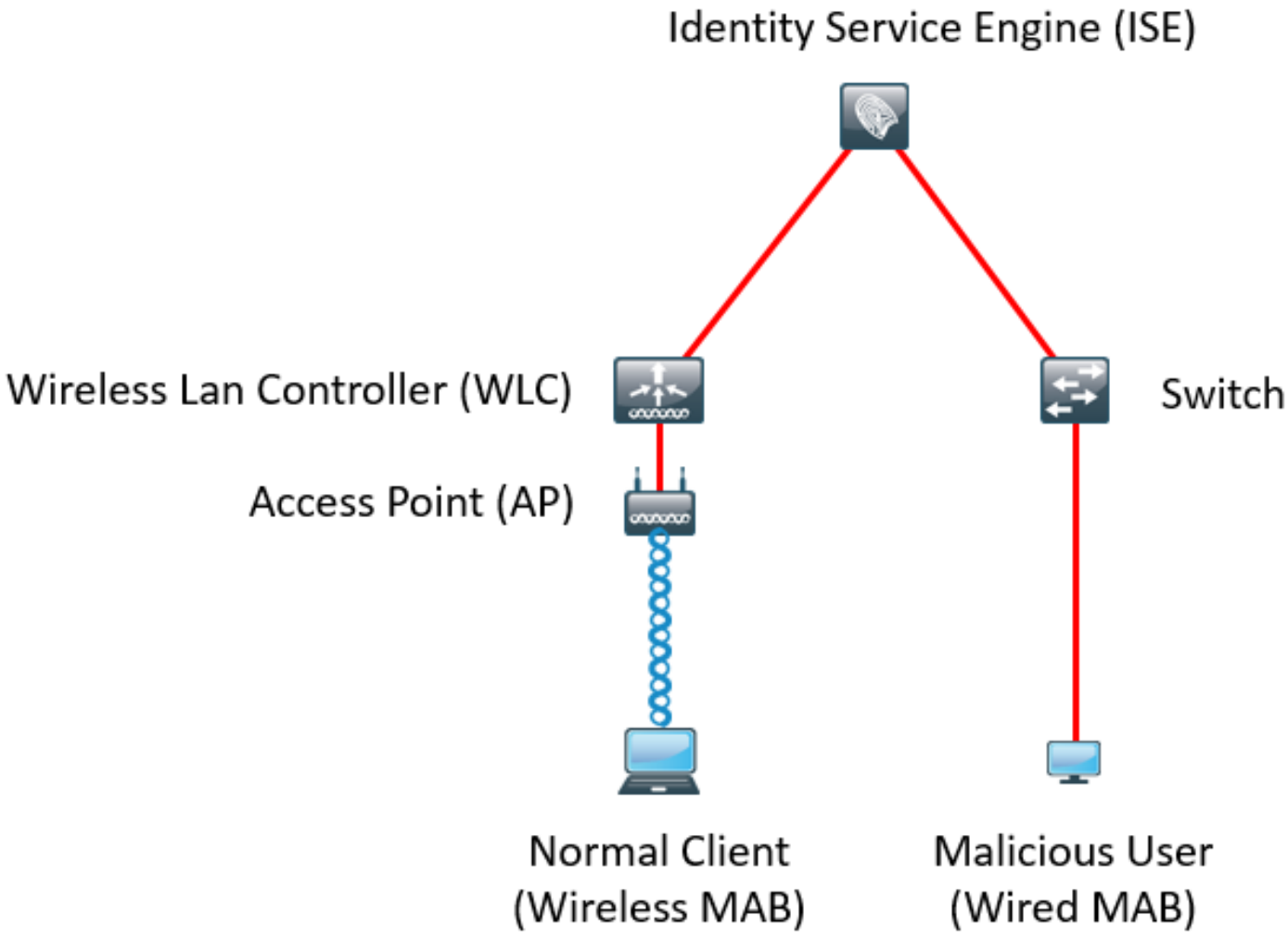
3. **سياسة نقطة النهاية** - تغيير في ملف تعريف نقطة النهاية من **الطابعة** أو **هاتف IP** إلى **محطة العمل**.

بمجرد أن يكتشف ISE أحد التغييرات المذكورة أعاله، تتم إضافة سمة AnomalousBehavior إلى نقطة النهاية ويتم تعيينها على True. يمكن إستخدام هذه في بعد كشرط في سياسات التخويل لتقييد الوصول إلى نقطة النهاية في عمليات المصادقة المستقبلية.

إذا تم تكوين الإنذار، فيمكن أن يرسل ISE CoA بمجرد الكشف عن التغيير إلعادة المصادقة وأ تنفيذ إرتداد من نقطة النهاية. وفي حالة التنفيذ، يمكنها إجراء عزل لنقطة النهاية الشاذة وفقا لسياسات التخويل التي تم تكوينها.

التكوين

الرسم التخطيطي للشبكة

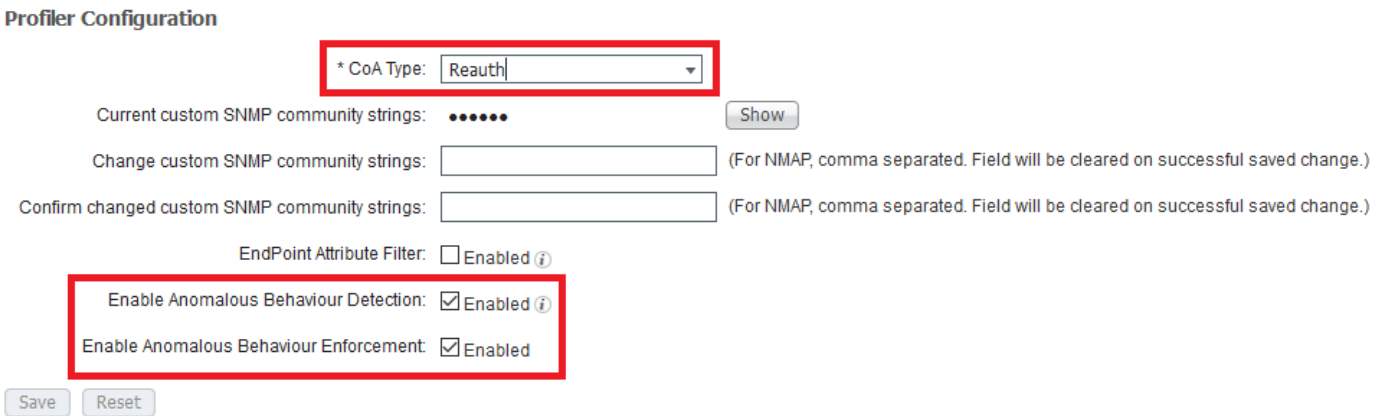


التكوينات

يتم إجراء تكوينات MAB و AAA البسيطة على الموجه و WLC. لاستخدام هذه الميزة، اتبع الخطوات التالية:

الخطوة 1. قم بتمكين الكشف عن الأخطاء.

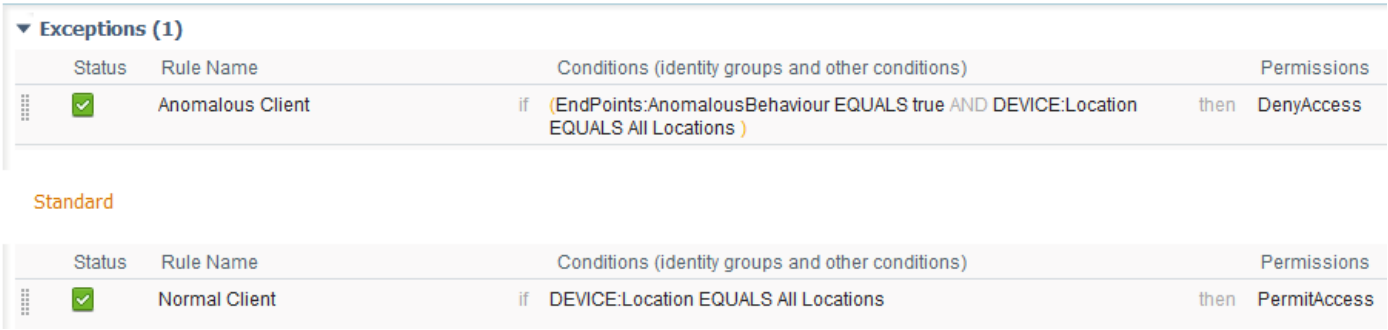
انتقل إلى **إدارة > نظام > إعدادات > إنشاء ملفات التعريف**.



يسمح الخيار الأول ISE باكتشاف أي سلوك شاذ ولكن لا يتم إرسال CoA (وضع الرؤية فقط). يسمح الخيار الثاني ISE بإرسال CoA بمجرد اكتشاف سلوك شاذ (وضع الفرض).

الخطوة 2. تكوين نهج التخويل.

قم بتكوين سمة Anomlousbehavior كشرط في نهج التخويل، كما هو موضح في الصورة:

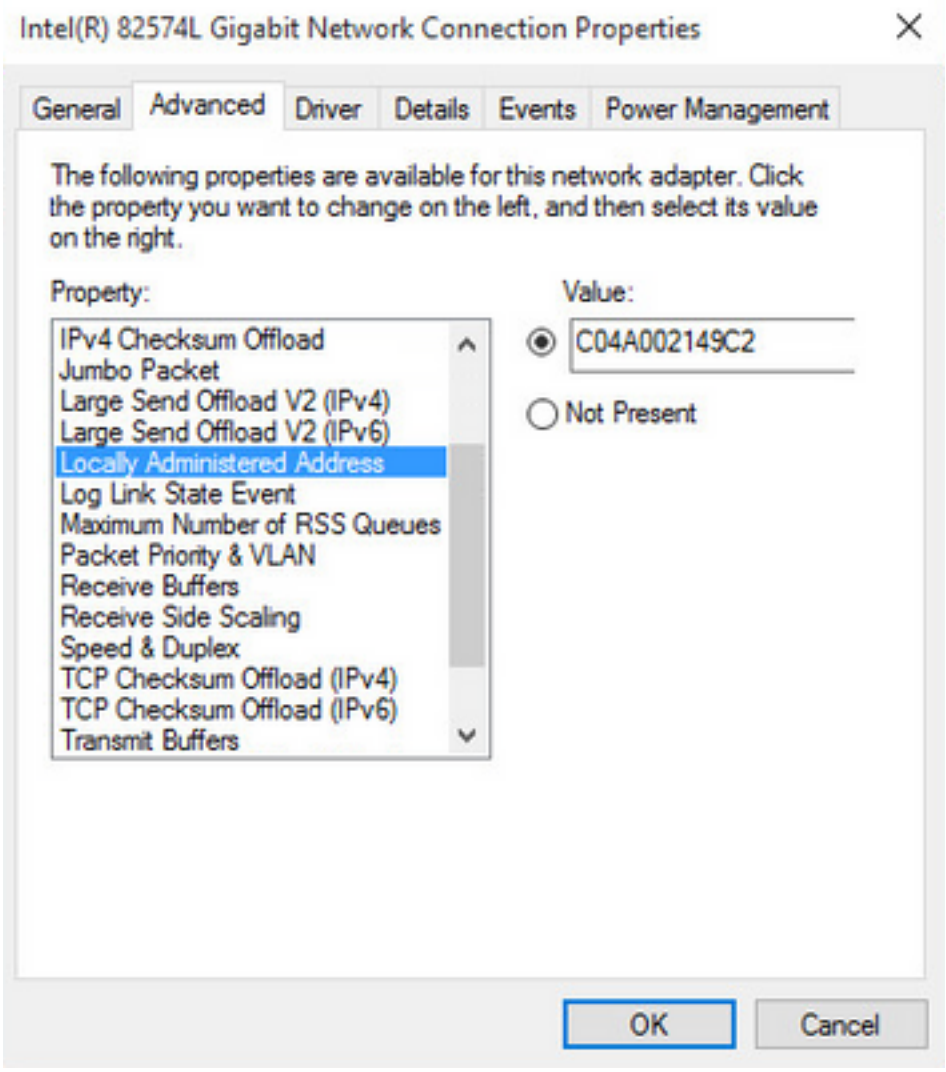


التحقق من الصحة

الاتصال بمحول السلكي. أستخدم الأمر **ipconfig /all** للعثور على عنوان MAC للمحول اللاسلكي، كما هو موضح في الصورة:

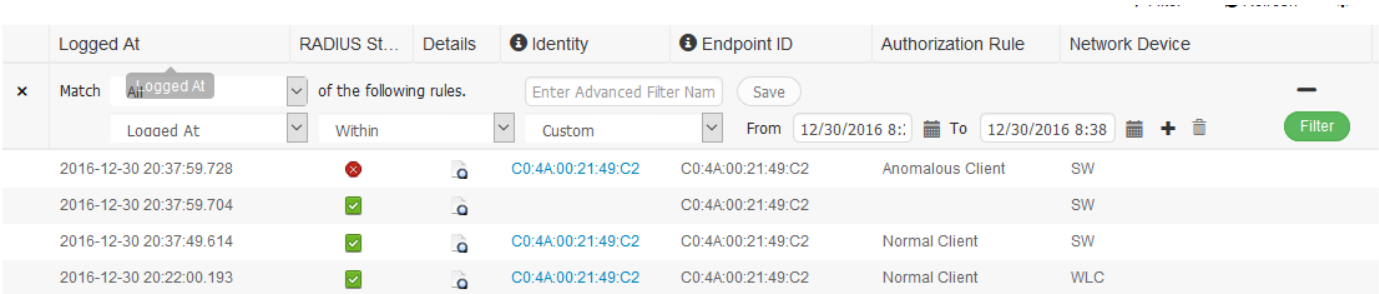
```
Wireless LAN adapter Wi-Fi:

   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
```

لمحاكاة مستخدم ضار، قد تنتحال عنوان MAC لمهاجم الإنترنت ليطابق عنوان MAC للمستخدم العادي.

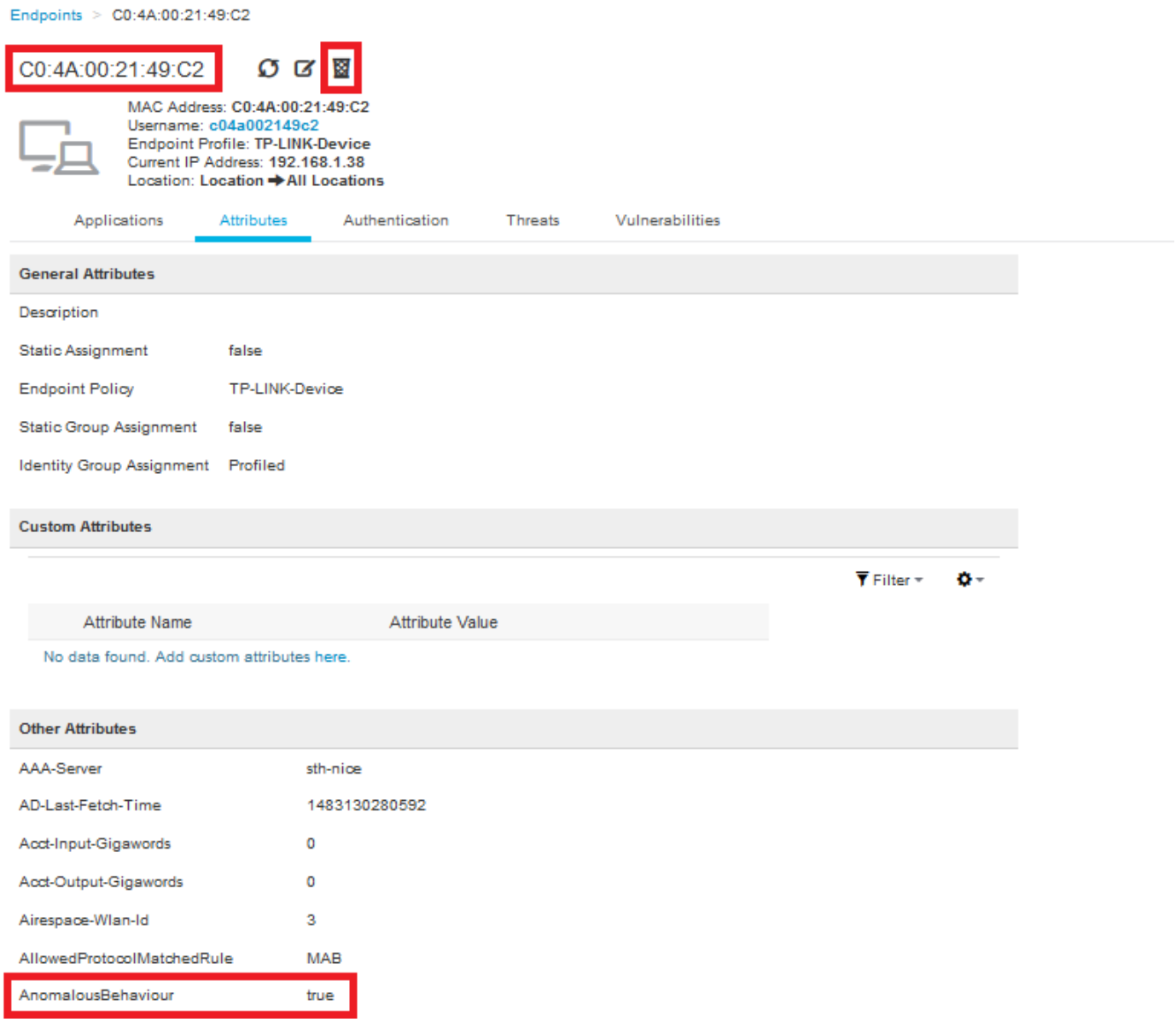


بمجرد اتصال المستخدم العادي، يمكنك رؤية إدخال نقطة نهاية في قاعدة البيانات. بعد ذلك، يتصل المستخدم الضار باستخدام عنوان MAC منتحل.

من التقارير يمكنك رؤية الاتصال الأولي من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). بعد ذلك، يتصل المستخدم الضار وبعد 10 ثوان، يتم تشغيل CoA بسبب اكتشاف العميل غير الطبيعي. نظرا لتعيين النوع CoA العام على **Reauth**، تحاول نقطة النهاية الاتصال مرة أخرى. قام ISE بتعيين سمة AnomalousBehavior بالفعل إلى True بحيث يتطابق ISE مع القاعدة الأولى ويرفض المستخدم.

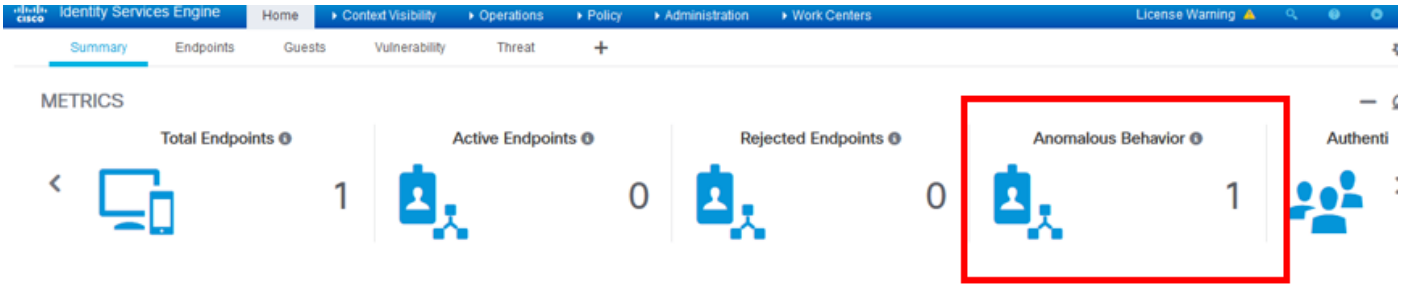


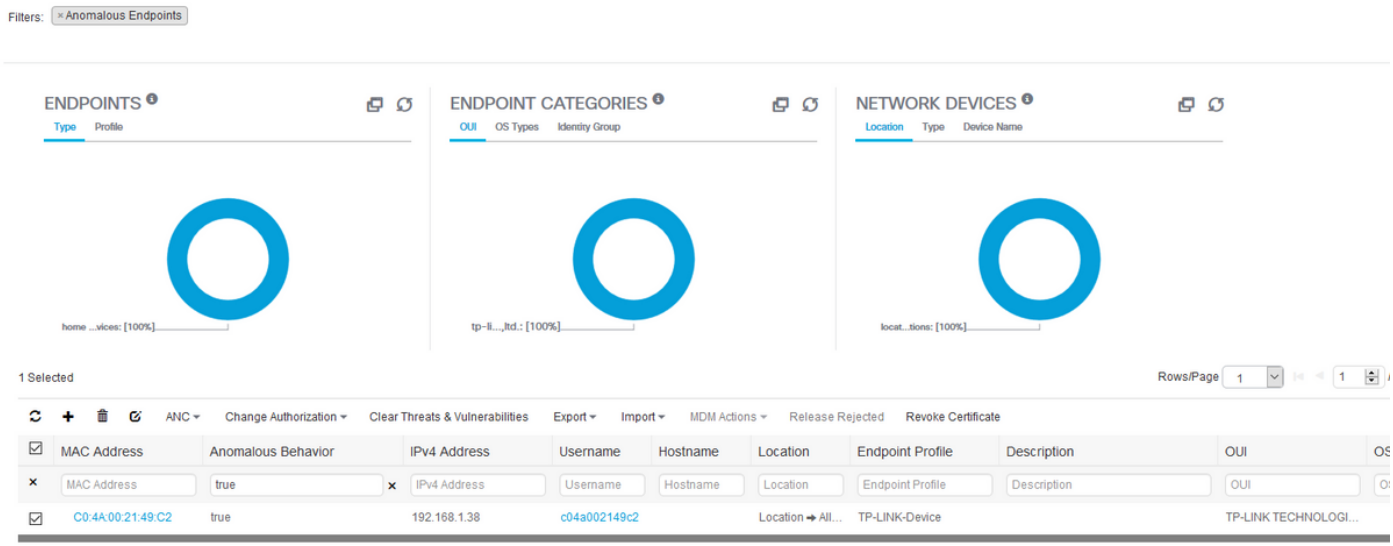
كما هو موضح في الصورة، يمكنك رؤية التفاصيل تحت نقطة النهاية في علامة التبويب رؤية السياق:



كما ترى، يمكن حذف نقطة النهاية من قاعدة البيانات لمسح هذه السمة.

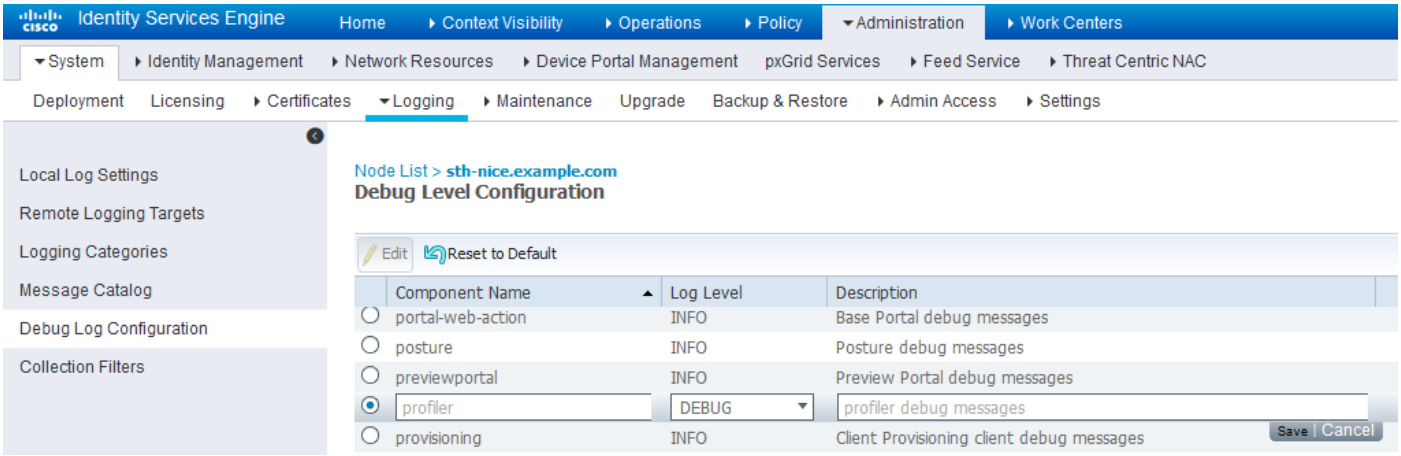
كما هو موضح في الصورة، تتضمن لوحة المعلومات عالمة تبويب جديدة لإظهار عدد العملاء الذين يقومون بعرض هذا السلوك:



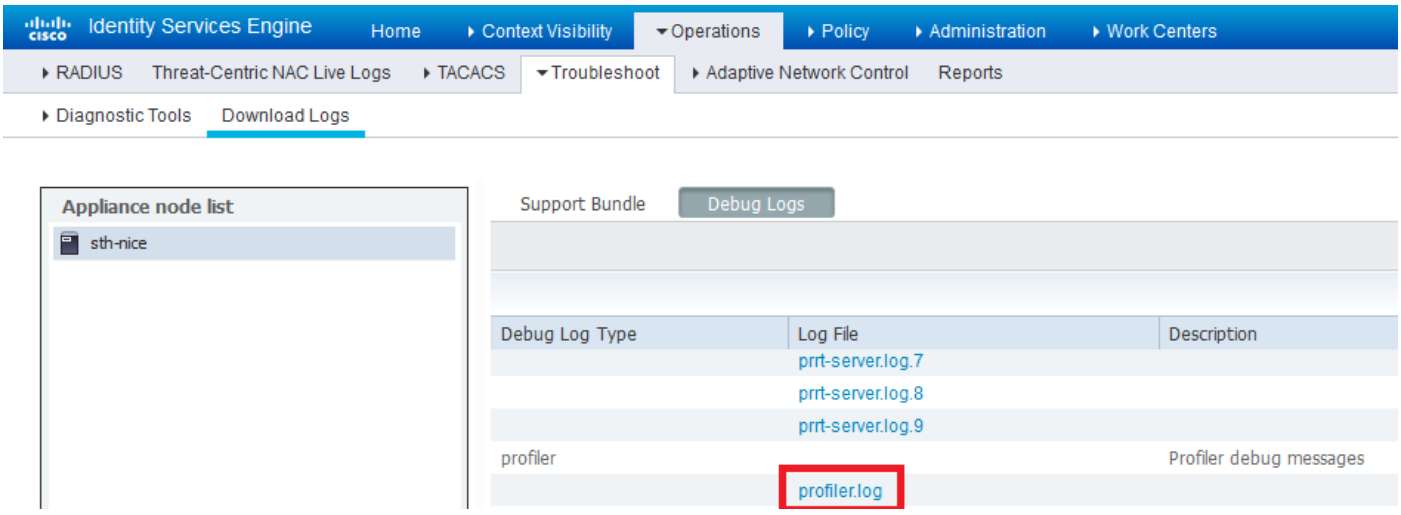


استكشاف الأخطاء وإصلاحها

لاستكشاف الأخطاء وإصلاحها، قم بتمكين تصحيح أخطاء منشئ ملفات التعريف، أثناء التنقل إلى **الإدارة > النظام > التسجيل > تكوين سجل تصحيح الأخطاء**.



للعثور على ملف **ISE Profiler.log**، انتقل إلى **العمليات > سجلات التنزيل > سجلات تصحيح الأخطاء**، كما هو موضح في الصورة:



تظهر هذه السجلات بعض القصاصات من ملف **Profile.log**. كما ترى، كان ISE قادرا على الكشف عن أن نقطة النهاية ذات عنوان MAC من C0:4a:00:21:49:C2 قد غيرت طريقة الوصول

بمقارنة القيم القديمة والجديدة لخصائص NAS-Port. إنها السلكية ولكنها تتغير إلى إيثرنت.

```
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
```

ولذلك، يتخذ مكتب خدمات الرقابة الداخلية إجراء ما دام الإنفاذ ممكنا. الإجراء هنا هو إرسال CoA بناء على التكوين العام في إعدادات التحليل المشار إليها أعلاه. في مثالنا، يتم تعيين نوع CoA على Reauth الذي يسمح لـ ISE بإعادة مصادقة نقطة النهاية وإعادة التحقق من القواعد التي تم تكوينها. هذه المرة، تتطابق مع قاعدة العميل غير العادية وبالتالي يتم رفضها.

```
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

معلومات ذات صلة

- دليل إدارة ISE 2.2

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).