設定 ISE 2.2 の変則的なエンドポイント 検出および適用

目次

概要

この資料は変則的なエンドポイント 検出および適用を記述したものです。 これは拡張 な ネットワーク表示用の Cisco Identity Services Engine （ISE）で導入される新しいプロファイル機能です。

前提条件

要件

次の項目に関する知識が推奨されます。

- スイッチの配線された MAC 認証バイパス（MAB）設定
- ワイヤレス LAN コントローラ（WLC）のワイヤレス MAB 設定
- 両方のデバイスの許可（CoA）設定の変更

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

1. Identity Services Engine 2.2
2. ワイヤレス LAN コントローラ 8.0.100.0
3. Cisco Catalyst スイッチ 3750 15.2(3)E2

4. 配線されるを用いる Windows 10 およびワイヤレスアダプタ

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

変則的なエンドポイント 検出 機能は ISE が特定の属性への変更および接続されたエンドポイントのためのプロファイルを監察するようにします。 変更が前もって構成された変則的な動作ルールの何れか一つ以上と一致する場合、ISE は変則的ようにエンドポイントを示します。 検出されて、ISE は処置を（CoA と）とり、疑わしい エンドポイントのアクセスを制限するためにある特定のポリシーを実施できます。 この機能のためのユース ケースの 1 つは MAC アドレス スプーフィングの検出が含まれています。

- 注： この機能は MAC アドレス スプーフィングのためのすべての潜在的なシナリオを例にとりません。 ユース ケースに適用を判別するためにこの機能によってカバーされるアノーマリの種類を読むこと確実でであって下さい。

検出が有効に なれば、これらの属性が変更する場合 ISE 既存のエンドポイントのために受け取られる新しい情報をおよびチェックは監察します:

1. **NAS ポート型**-このエンドポイントのアクセス方式が変更したかどうか確認します。 たとえば、配線された Dot1x によって接続した同じ MAC アドレスがワイヤレス Dot1x および査証 versa のために使用される場合。

2. **DHCP クラス ID** -エンドポイントのクライアント/ベンダーの種類が変更したかどうか判別します。 これは DHCP クラス ID アトリビュートがある特定の値と読み込まれ、次に別の値に変更されるときだけ適用します。 エンドポイントが静的な IP で設定される場合、DHCP クラス ID アトリビュートは ISE で読み込まれません。 別のデバイスが MAC アドレスをスプーフィングし、DHCP を使用すればあとで、クラス ID は空の値から特定のストリングに変更します。 これは Anomouls 動作 検出を誘発しません。

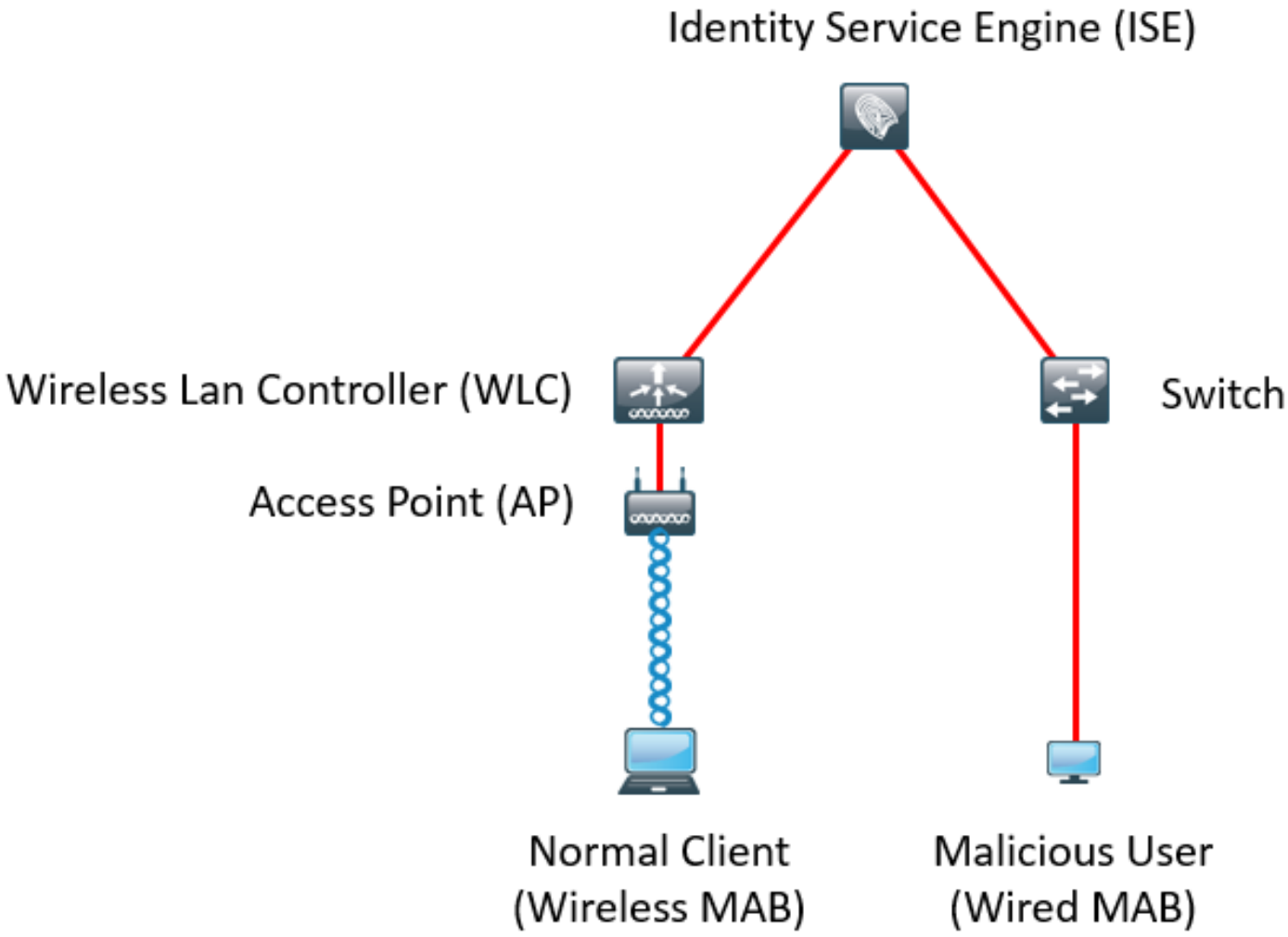
3. **エンドポイント ポリシー-プリンタ**または **IP 電話**からの**ワークステーション**へのエンドポイント プロファイルの変更。

ISE が上記される変更の 1 つを検出すれば AnomalousBehaviour アトリビュートは本当へのエンドポイントおよびセットに追加されます。 未来の認証のエンドポイントのためのアクセスを制限するのに承認ポリシーでこれがように条件あとで使用することができます。

適用が設定される場合、ISE はエンドポイントのためのポート バウンスを再認証するか、または行うために変更が検出されれば CoA を送信できます。 事実上、それが設定された承認ポリシーによって変則的なエンドポイントを検疫できれば。

設定

ネットワーク図

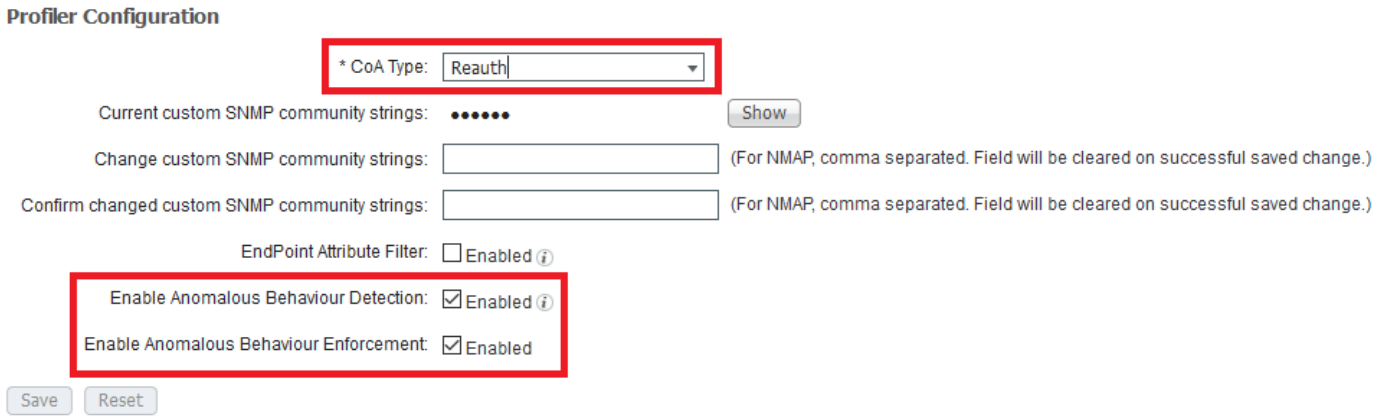


設定

簡単な MAB および AAA 設定はスイッチおよび WLC で行われます。 この機能を利用するために、次の手順に従って下さい:

ステップ 1.有効変則的な検出。

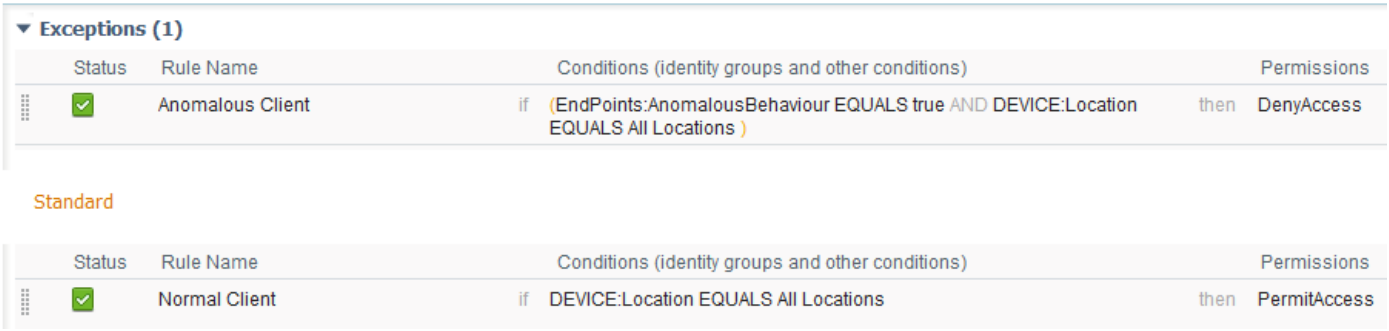
Administration > システム > 設定への移動 **> プロファイルします。**



変則的な動作しかし CoA を検出しない優先買受権割り当て ISE は送信 されます (表示だけモード)。 第 2 オプションは変則的な動作が検出されれば ISE が CoA を送信 するようにします (適用モード)。

ステップ 2.設定承認ポリシー。

イメージに示すように承認ポリシーの条件で Anomlousbehaviour アトリビュートを、設定して下さい:

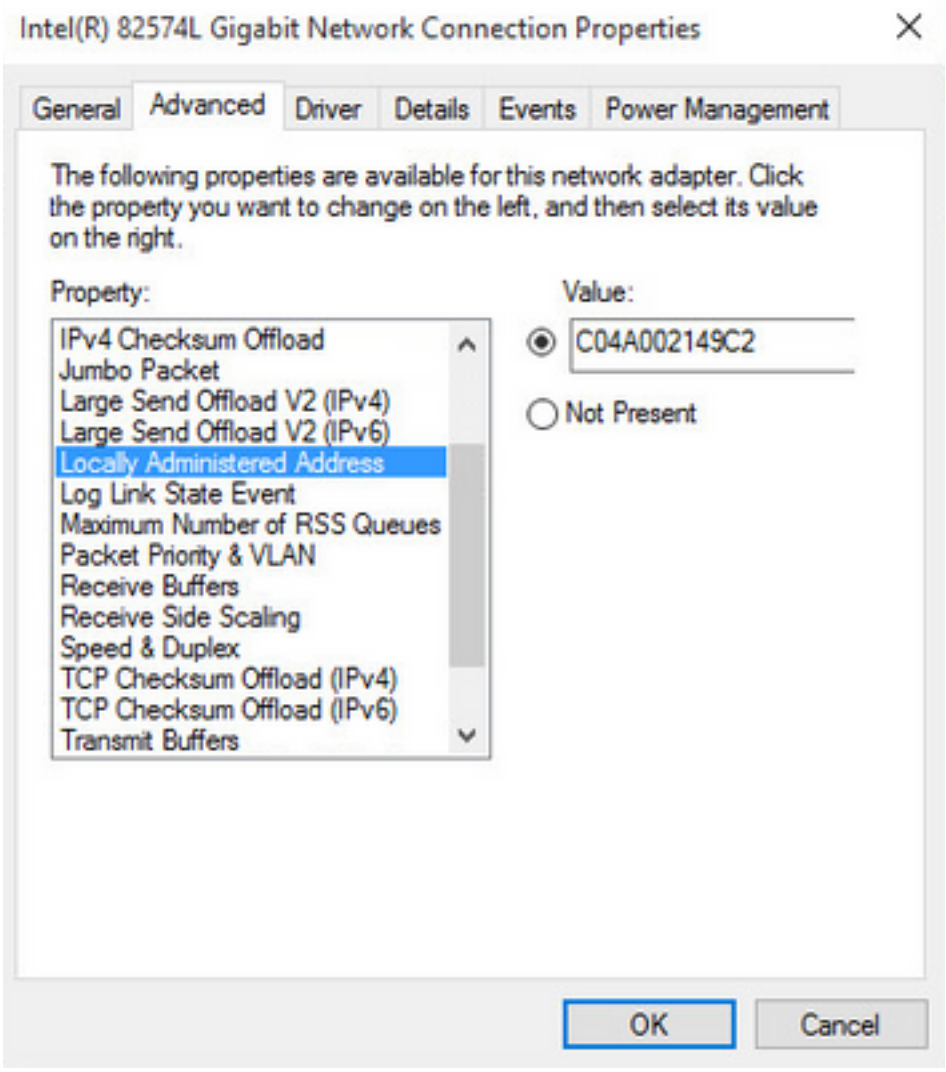


確認

ワイヤレスアダプタによって接続して下さい。 イメージに示すようにワイヤレスアダプタの MAC アドレスを、見つけるのにコマンド **ipconfig /all** を使用して下さい:

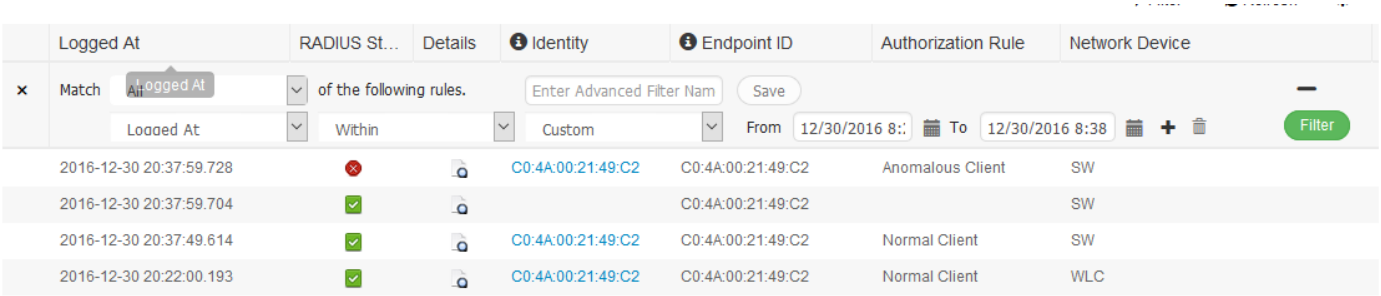
```
Wireless LAN adapter Wi-Fi:

   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
```

悪意のあるユーザを模倣するために、通常のユーザーの MAC アドレスを一致するためにイーサネット アダプタの MAC アドレスをスプーフィングすることができます。

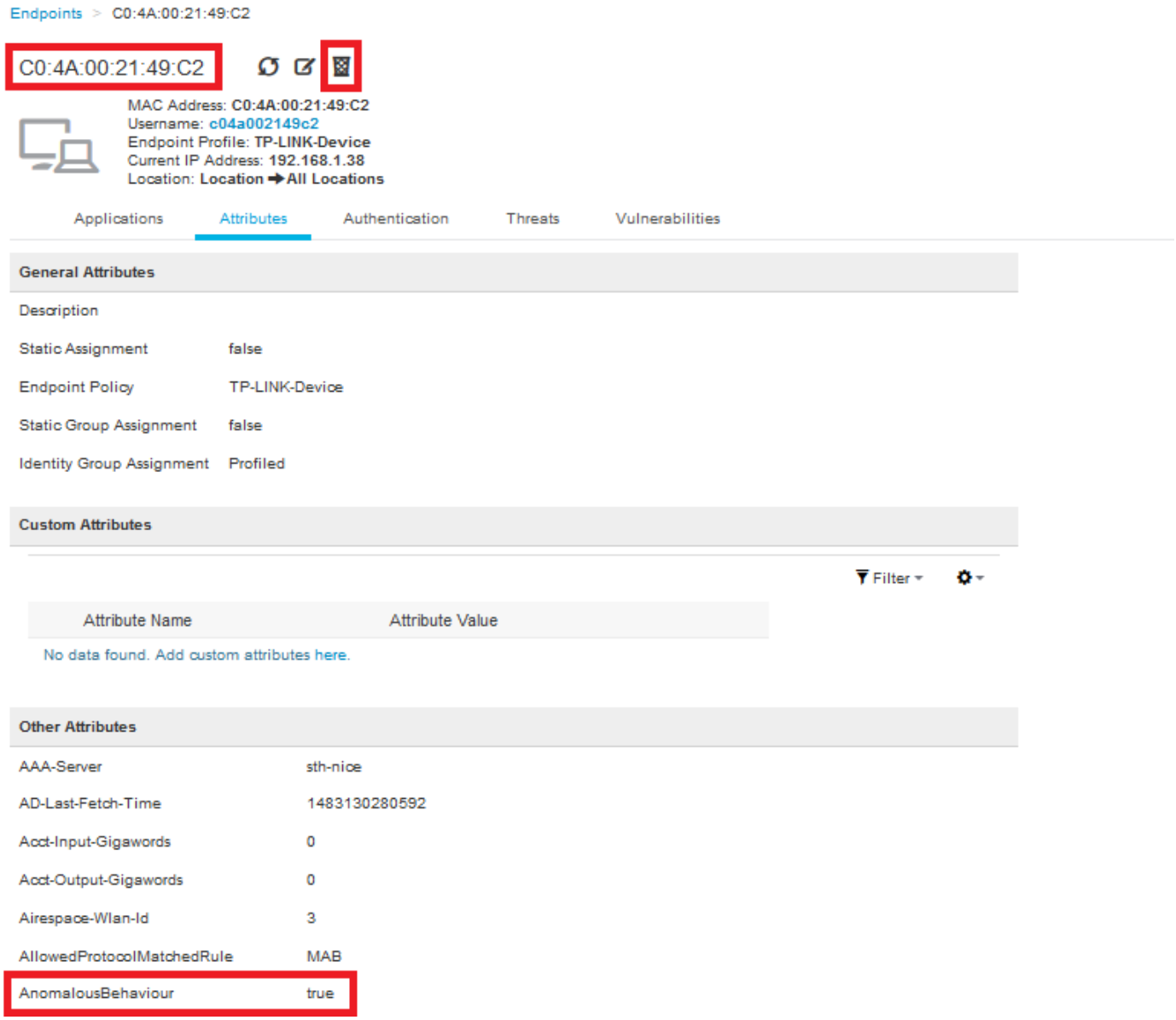


通常のユーザーが接続すれば、データベースのエンドポイント エントリを表示できます。 その後、悪意のあるユーザはスプーフィングされた MAC アドレスを使用して接続します。

レポートから WLC からの最初の接続を表示できます。 その後、悪意のあるユーザは接続し、10 は数秒後、CoA 変則的なクライアントの検出が誘発された原因です。 グローバル な CoA 型が **Reauth** に設定 されるので、エンドポイントは再度接続することを試みます。 ISE は本当に既に AnomalousBehaviour アトリビュートを設定 して いました従って ISE は最初のルールと一致し、ユーザを否定します。

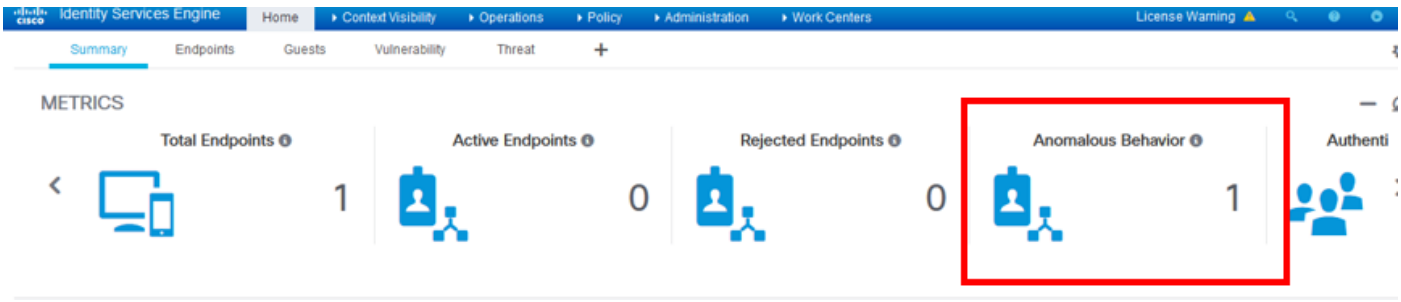


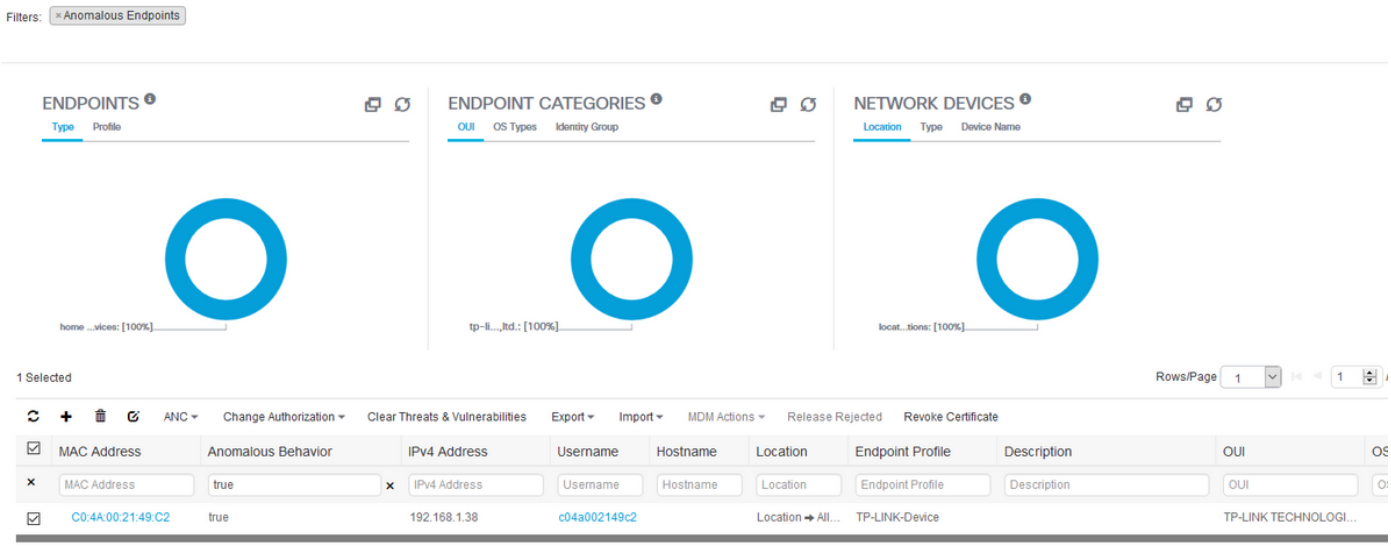
イメージに示すように、コンテキスト表示タブのエンドポイントの下で詳細を次のように表示できます:



見てわかるように、このアトリビュートをクリアするためにエンドポイントはデータベースから削除することができます。

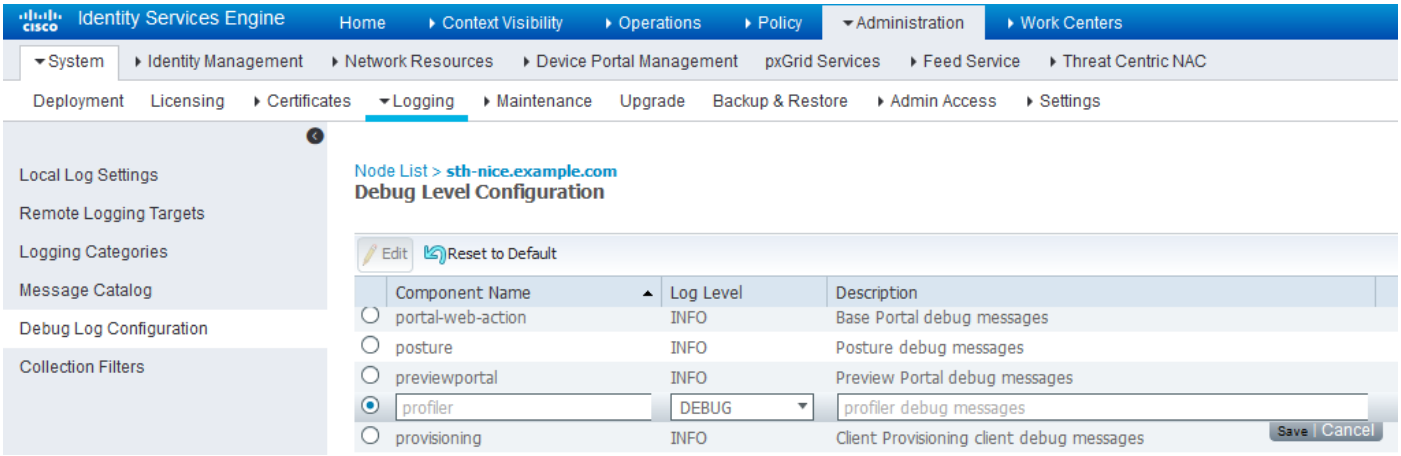
イメージに示すように、ダッシュボードはこの動作を表わしているクライアントの数を示すために New タブが含まれています:



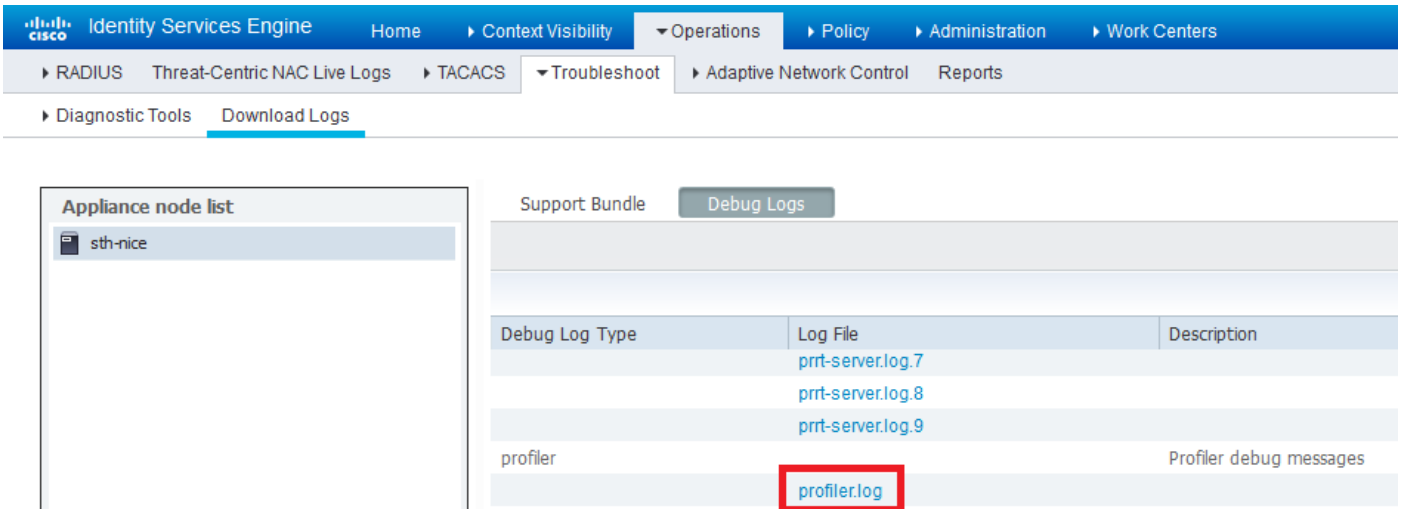


トラブルシューティング

Administration > システム > ロギング > デバッグ ログ 設定にナビゲートするように、プロファイラー デバッグを有効に するため解決するため。



ISE **Profiler.log** ファイルを、移動、イメージに示すように**オペレーション > ダウンロード ログ > デバッグ ログ**に見つけるため:



これらのログは **Profiling.log** ファイルからのいくつかの断片を示します。 見てわかるように、ISE は C0:4A:00:21:49:C2 の MAC アドレスのエンドポイントが NAS ポート型属性ことをの古く

、新しい値の比較によってアクセス方式を変更したことを検出できました。 それはワイヤレスでが、イーサネットに変更されます。

```
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
```

従って、ISE は適用が有効に なるので処置をとります。 ここの操作は上記されるプロファイル設定のグローバル な 設定によって CoA を送信 することです。 例では、CoA 型は ISE がエンドポイントを再認証し、設定されたルールを再確認するようにする Reauth に設定 されます。 今回、それは変則的なクライアント ルールと一致し、従って否定されます。

```
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
```

関連情報

- ISE 2.2 管理 ガイド