ISE 2.2 上での異常エンドポイントの検出と適用の設定

内容

概要

このドキュメントでは、異常なエンドポイントの検出および強制適用について説明します。これは、拡張的なネットワーク可視性を実現するため、Cisco Identity Services Engine（ISE）に導入された新たなプロファイリング機能です。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- スイッチの有線 MAC 認証バイパス（MAB）の設定
- ワイヤレス LAN コントローラ（WLC）のワイヤレス MAB 設定
- 両方のデバイスの認可変更（CoA）

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いています。

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. 有線およびワイヤレス アダプタを備えた Windows 10

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

異常なエンドポイント検出機能を使用すると、ISEは接続されたエンドポイントの特定の属性およびプロファイルの変更を監視できます。変更が1つ以上の設定済みの異常動作ルールに一致する場合、ISEはエンドポイントを異常としてマークします。検出されると、ISEは（CoAとともに）アクションを実行し、特定のポリシーを適用して、疑わしいエンドポイントのアクセスを制限できます。 この機能の使用例の1つに、MACアドレススプーフィングの検出が含まれます。

- 注：この機能は、MACアドレスのスプーフィングに関する潜在的なシナリオすべてに対処するわけではありません。 この機能でカバーされている異常のタイプを必ずお読みになり、ご使用のユースケースへの適用可能性を確認してください。

検出を有効にすると、ISE は既存の各エンドポイントに関して受信した新たな情報をモニタし、以下の属性が変化したかどうかを調べます。

1. **NAS ポート タイプ：このエンドポイントのアクセス方式が変更されたかどうかを判断します。**たとえば、有線Dot1x経由で接続された同じMACアドレスが無線Dot1xに使用され、その逆も使用されます。

2. **DHCP クラス ID：クライアントのタイプ、またはエンドポイントのベンダーが変更されたかどうかを判断します。**これは、DHCPクラスID属性に特定の値が入力された後、別の値に変更された場合にのみ適用されます。エンドポイントにスタティックIPが設定されている場合、DHCPクラスID属性はISEに設定されません。後で、別のデバイスがMACアドレスをスプーフィングしてDHCPを使用すると、クラスIDが空の値から特定の文字列に変更されます。これにより、Anomols Behaviorの検出はトリガーされません。

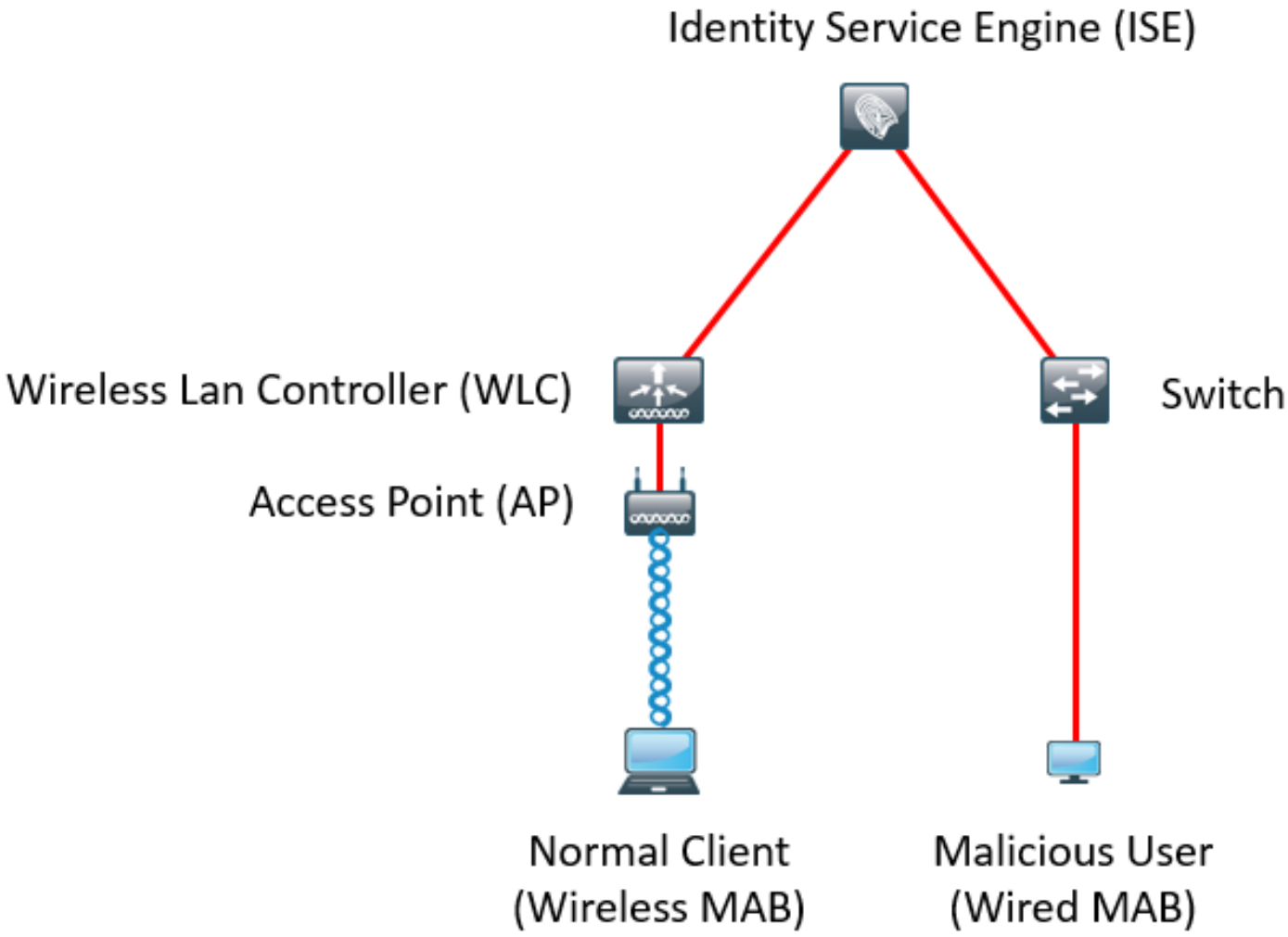
3. **エンドポイントポリシー**:プリンタまたは**IP** Phoneからワークス**テーションに**よるエンドポイ**ンプロファイル**の**変更**。

上述のいずれかの変化が ISE によって検出されると、このエンドポイントに AnomalousBehaviour 属性が追加され、True に設定されます。この属性を後で、認証ポリシーの条件として使用できます。これにより、以降の認証で、このエンドポイントによるアクセスを制限できます。

強制適用を設定しておくと、このような変化が検出された時点で ISE は CoA を送信し、エンドポイントに対して再認証またはポート バウンスを実行できます。この機能を有効化すると、設定された認証ポリシーに基づき、異常なエンドポイントに対する検疫が実行されます。

設定

ネットワーク図

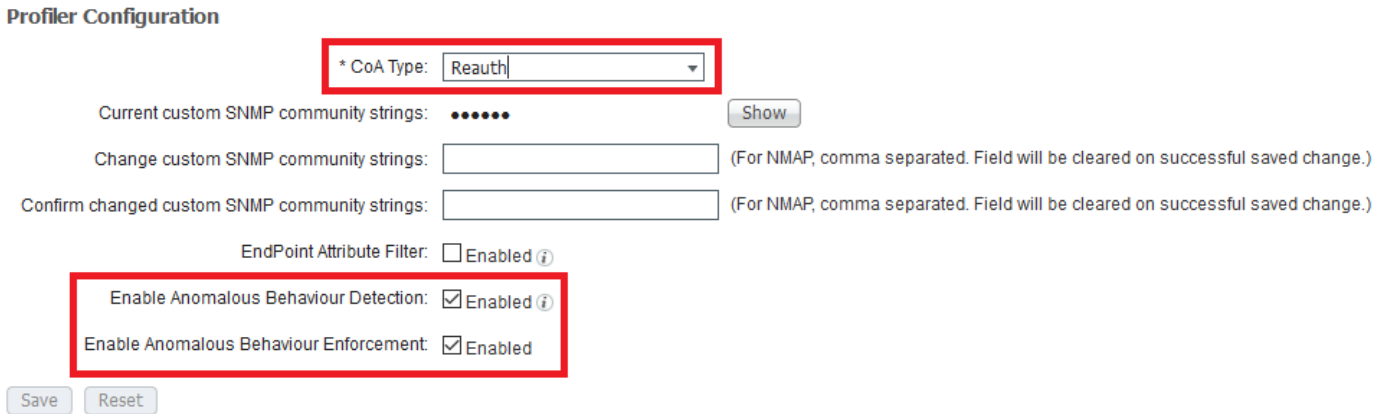


設定

スイッチおよび WLC に対し、単純な MAB および AAA 設定を行います。この機能を使用するには、次の手順を実行します。

手順 1：異常の検出の有効化

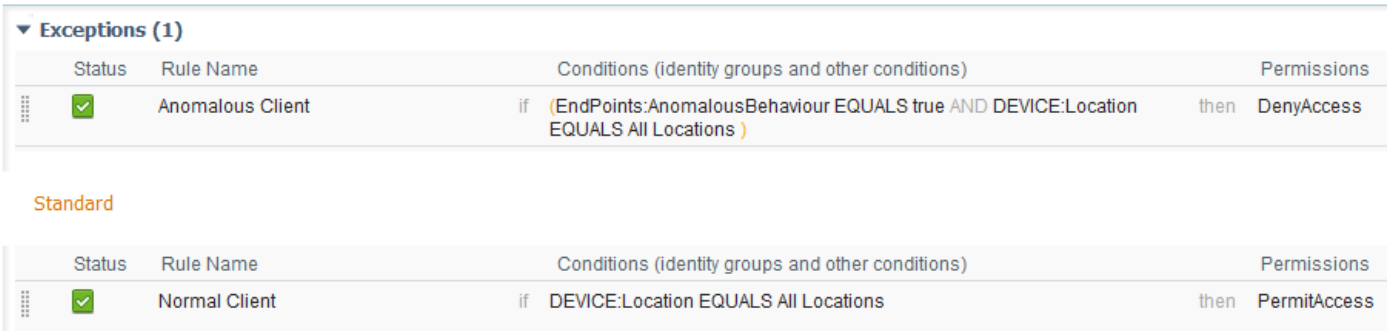
[Administration] > [System] > [Settings] > [Profiling] の順に選択します。



最初のオプションでは、異常な動作がすべて検出されますが、CoA は送信されません（可視性のみのモード）。 2 番目のオプションでは、異常の動作が検出された時点で、CoA が送信されます（強制適用モード）。

手順 2：許可ポリシーの設定

図に示すように、認証ポリシーの条件として AnomlousBehaviour 属性を設定します。

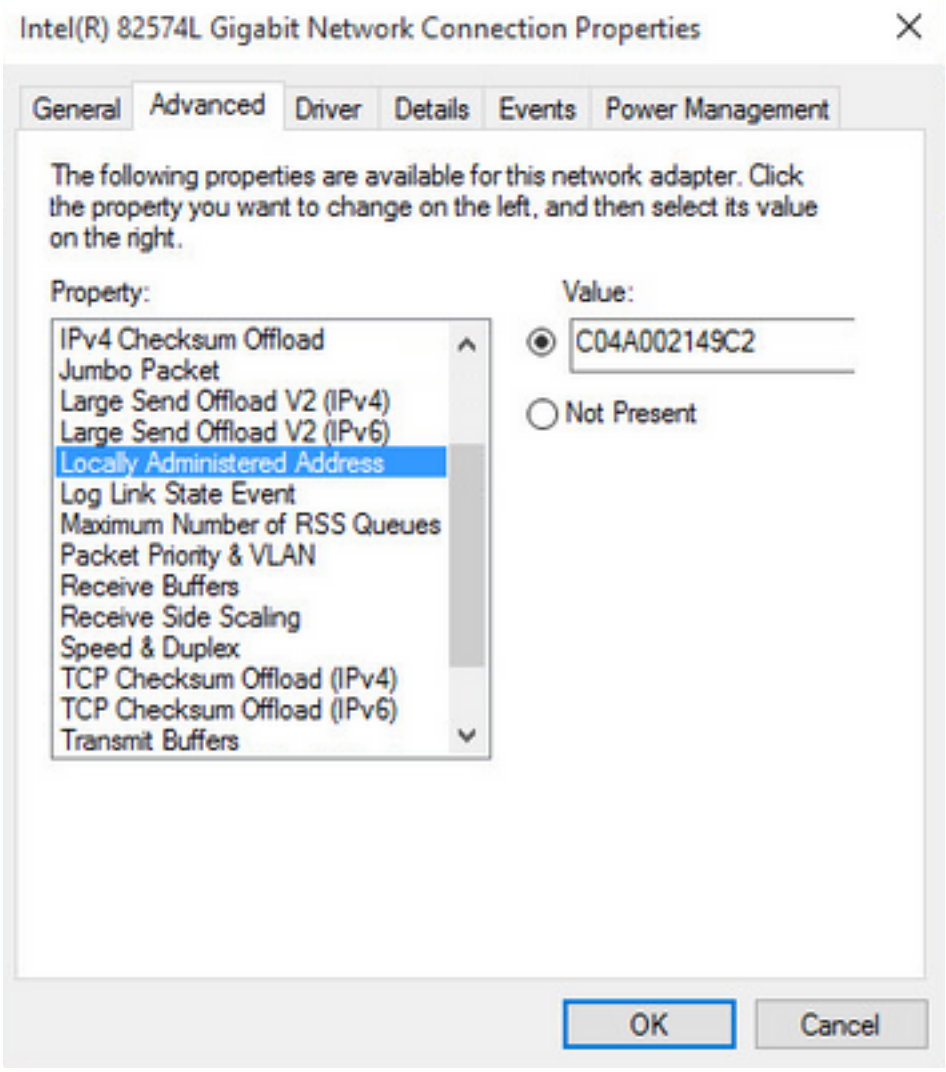


確認

ワイヤレス アダプタを介して接続します。**ipconfig /all コマンドを使用して、ワイヤレス アダプタの MAC アドレスを特定します。次に、出力例を示します。**

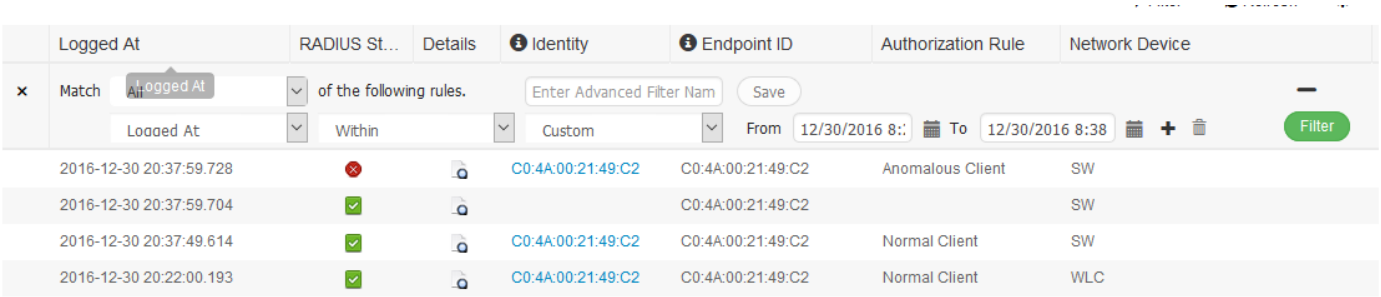
```
Wireless LAN adapter Wi-Fi:

   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
```

イーサネット アダプタの MAC アドレスを、正常なユーザの MAC アドレスと一致するようになりすますことで、悪意のあるユーザをシミュレーションできます。

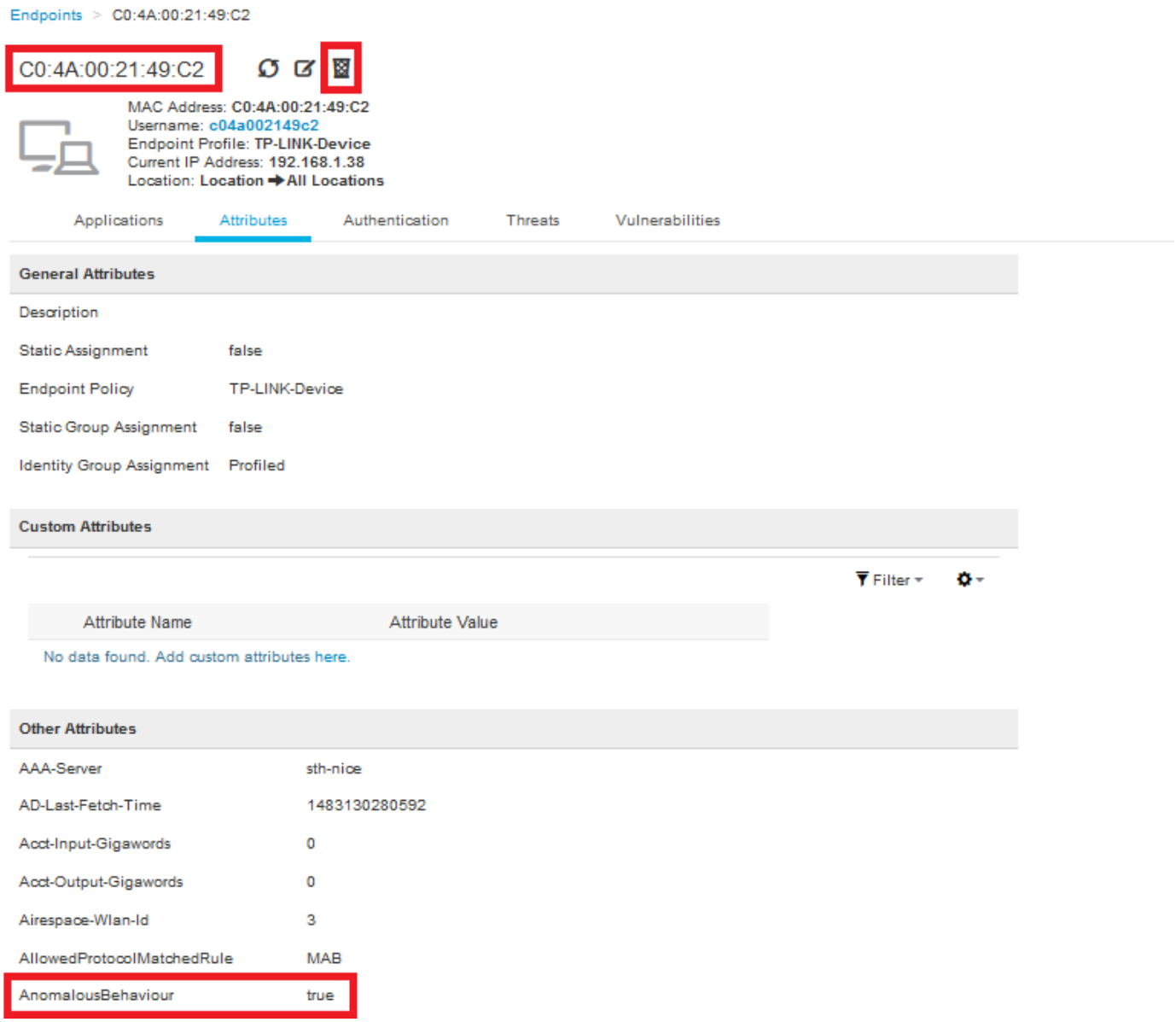


正常なユーザが接続すると、データベース内にエンドポイントのエントリが作成されます。この後、悪意のあるユーザは、なりすました MAC アドレスを使用することで接続できます。

このレポートから、最初の接続が WLC から行われていたことが分かります。その後、悪意のあるユーザが接続し、10 秒後に CoA が送信されています。異常なクライアントが検出されたためです。グローバル CoA タイプが [Reauth] に設定されているため、エンドポイントは再度接続を試みます。ISE ではすでに AnomalousBehaviour 属性が True に設定されているため、最初のルールとの照合に基づき、このユーザは拒否されます。

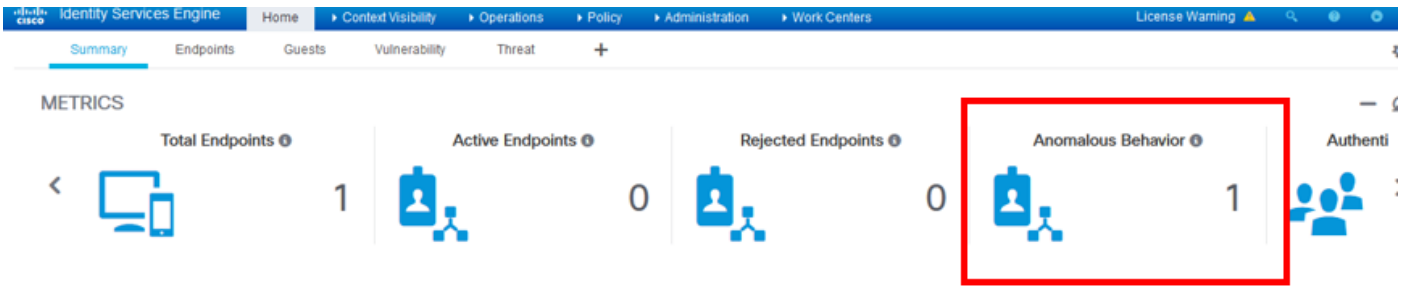


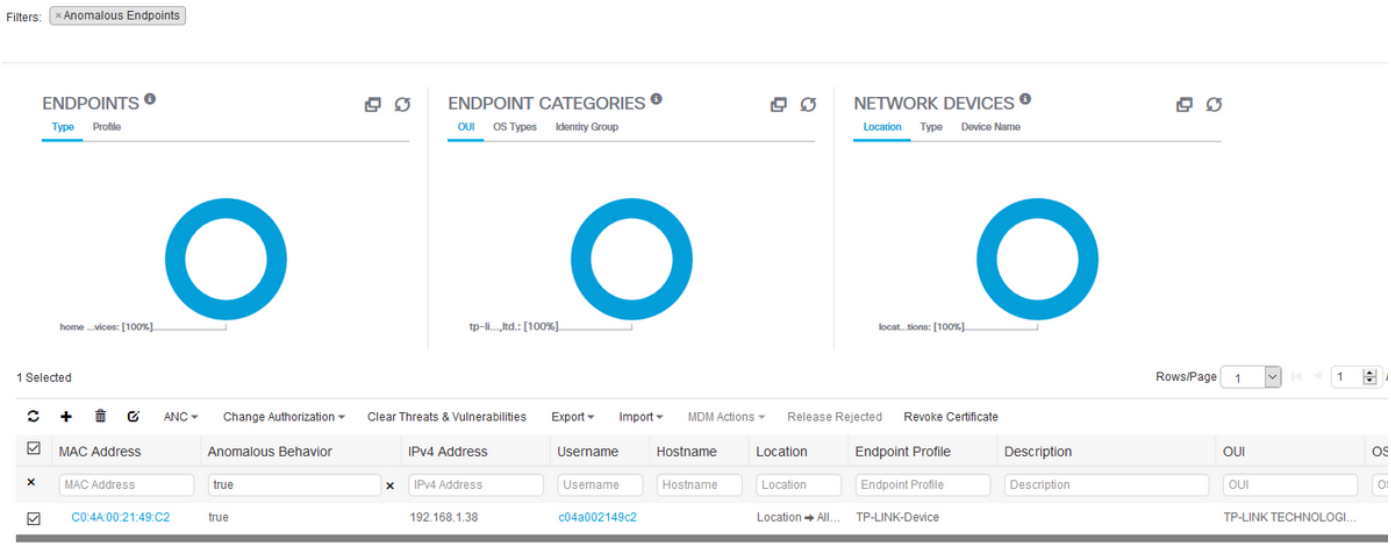
図に示すように、[Context Visibility] タブにはエンドポイントの詳細が表示されます。



エンドポイントをデータベースから削除することで、この属性をクリアできます。

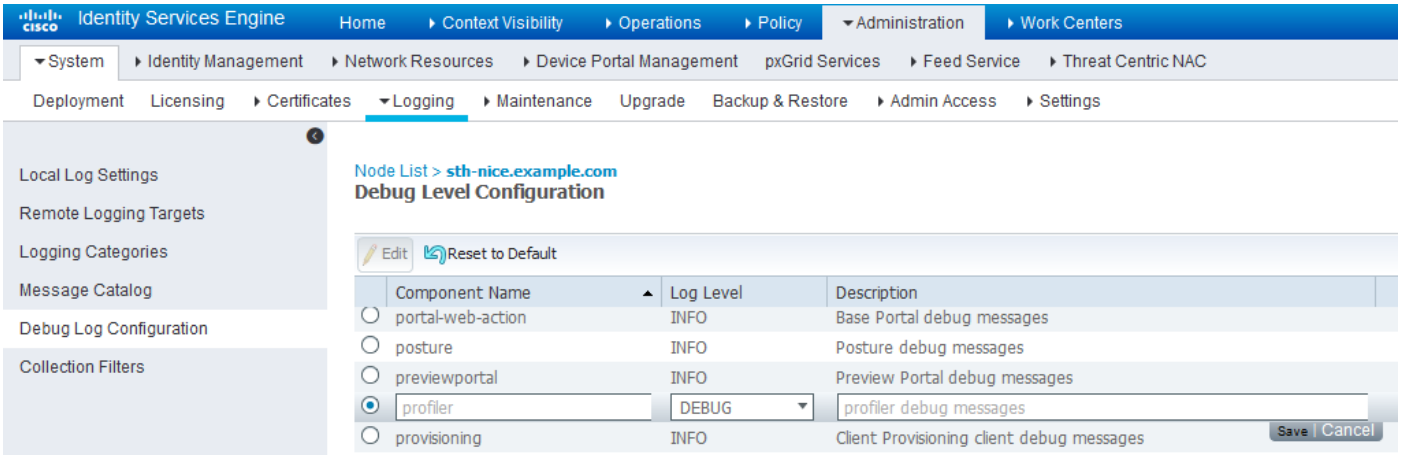
図に示すように、ダッシュボードには、異常な動作を示すクライアント数を表す新しいタブが追加されます。



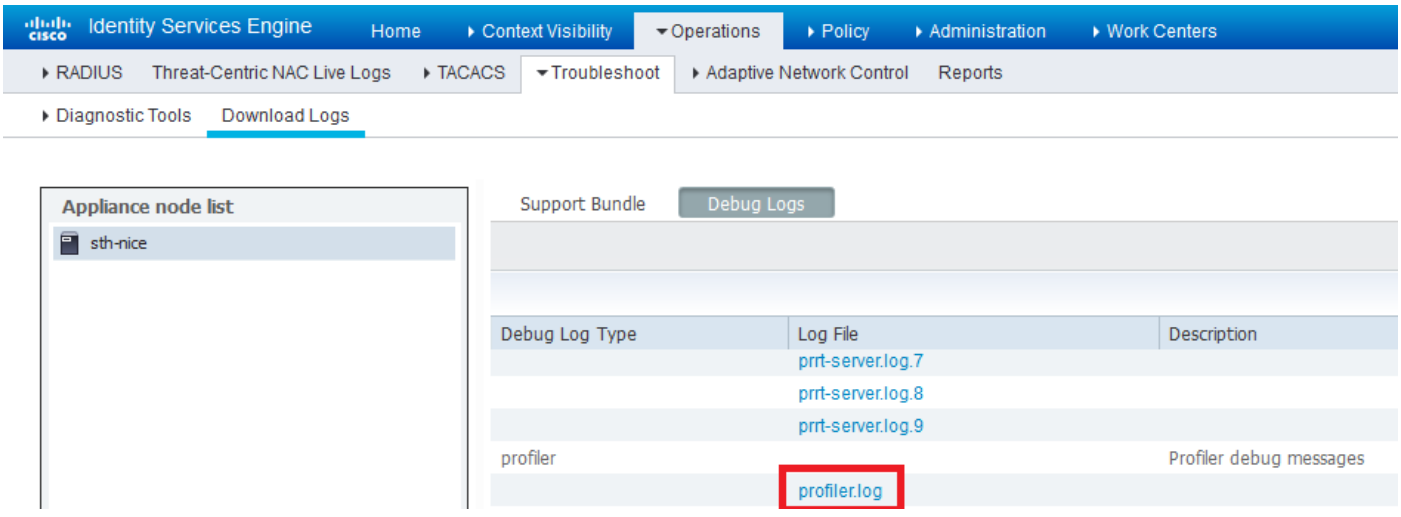


トラブルシュート

トラブルシュートを実行するには、プロファイラのデバッグを有効化します。これには、[Administration] > [System] > [Logging] > [Debug Log] [Configuration] の順に選択します。



ISE の **Profiler.log ファイルを特定するには、図に示すように、[Operations] > [Download Logs] > [Debug Logs] の順に選択します。**



これらの口グには、**Profiling.log ファイルの一部を表すスニペットが表示されます。**図から分かるように、ISE では NAS ポート タイプ属性の古い値と新しい値とを比較することで、MAC アドレ

ス C0:4A:00:21:49:C2 を持つエンドポイントがアクセス方式を変更したことを検出しています。ここでは、アクセス方式がワイヤレスからイーサネットに変わっています。

```
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
```

強制適用が有効化されているため、ISE は規定のアクションを実行します。ここでのアクションは、上述のプロファイル設定で指定したグローバル設定に基づく、CoA の送信です。この例では、CoA のタイプを再認証に設定しているため、ISE はエンドポイントを再認証し、設定されたルールを再度チェックします。このエンドポイントは異常なクライアントのルールに適合したため、拒否されます。

```
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 アドミニストレーション ガイド