Configurazione del rilevamento e dell'applicazione di endpoint anomali su ISE 2.2

Sommario

Introduzione

In questo documento viene descritto il rilevamento e l'applicazione di endpoint anomali. Questa è una nuova funzione di profilatura introdotta in Cisco Identity Services Engine (ISE) per migliorare la visibilità della rete.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione MAB (Wired MAC Authentication Bypass) sullo switch
- Configurazione MAB wireless su controller WLC
- Configurazione della modifica dell'autorizzazione (CoA) su entrambi i dispositivi

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

1. Identity Services Engine 2.2
2. Controller LAN wireless 8.0.100.0

3. Cisco Catalyst Switch 3750 15.2(3)E2
4. Windows 10 con schede di rete cablate e wireless

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La funzione di rilevamento degli endpoint anomali consente all'ISE di monitorare le modifiche agli attributi e ai profili specifici degli endpoint connessi. Se una modifica soddisfa una o più regole di comportamento anomalo preconfigurate, ISE contrassegnerà l'endpoint come Anomalo. Una volta rilevata, ISE può agire (con il CoA) e applicare determinate policy per limitare l'accesso all'endpoint sospetto. Uno degli scenari di utilizzo di questa funzionalità include il rilevamento dello spoofing degli indirizzi MAC.

- Nota: Questa funzionalità non consente di risolvere tutti i potenziali scenari di spoofing degli indirizzi MAC. Leggere attentamente i tipi di anomalie trattati da questa funzione per determinarne l'applicabilità ai casi di utilizzo.

Dopo aver abilitato la funzione di rilevamento, ISE controlla le nuove informazioni ricevute sugli endpoint esistenti e controlla se gli attributi sono stati modificati:

1. **NAS-Port-Type**: determina se il metodo di accesso di questo endpoint è stato modificato. Ad esempio, se lo stesso indirizzo MAC connesso tramite Wired Dot1x viene utilizzato per Wireless Dot1x e vice versa.

2. **ID classe DHCP**: determina se il tipo di client/fornitore dell'endpoint è stato modificato. Questo si applica solo quando l'attributo ID classe DHCP viene popolato con un certo valore e quindi modificato in un altro valore. Se un endpoint è configurato con un IP statico, l'attributo ID della classe DHCP non verrà popolato con ISE. In seguito, se un altro dispositivo falsifica l'indirizzo MAC e utilizza DHCP, l'ID di classe passerà da un valore vuoto a una stringa specifica. Questo non attiva il rilevamento del comportamento anomalo.

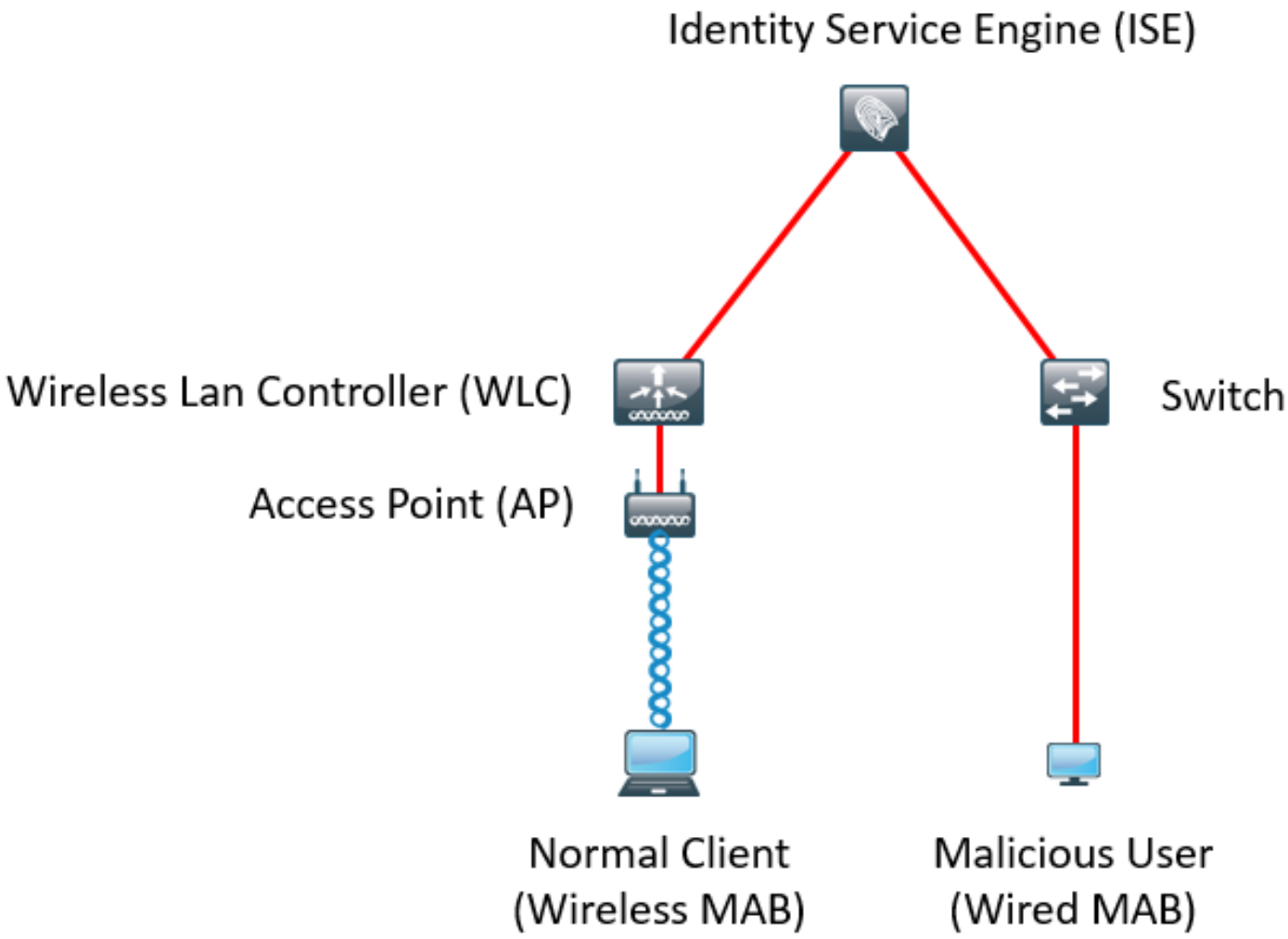
3. **Criteri endpoint:** modifica nel profilo dell'endpoint da **stampante** o **telefono IP** a **workstation**.

Una volta rilevata una delle modifiche sopra menzionate, l'attributo AnomalousBehavior viene aggiunto all'endpoint e impostato su True. Questa opzione può essere utilizzata in seguito come condizione nei criteri di autorizzazione per limitare l'accesso all'endpoint nelle autenticazioni future.

Se è stata configurata l'imposizione, ISE può inviare un CoA una volta rilevata la modifica per ripetere l'autenticazione o eseguire un rimbalzo della porta per l'endpoint. Se attivo, può mettere in quarantena l'endpoint anomalo a seconda dei criteri di autorizzazione configurati.

Configurazione

Esempio di rete

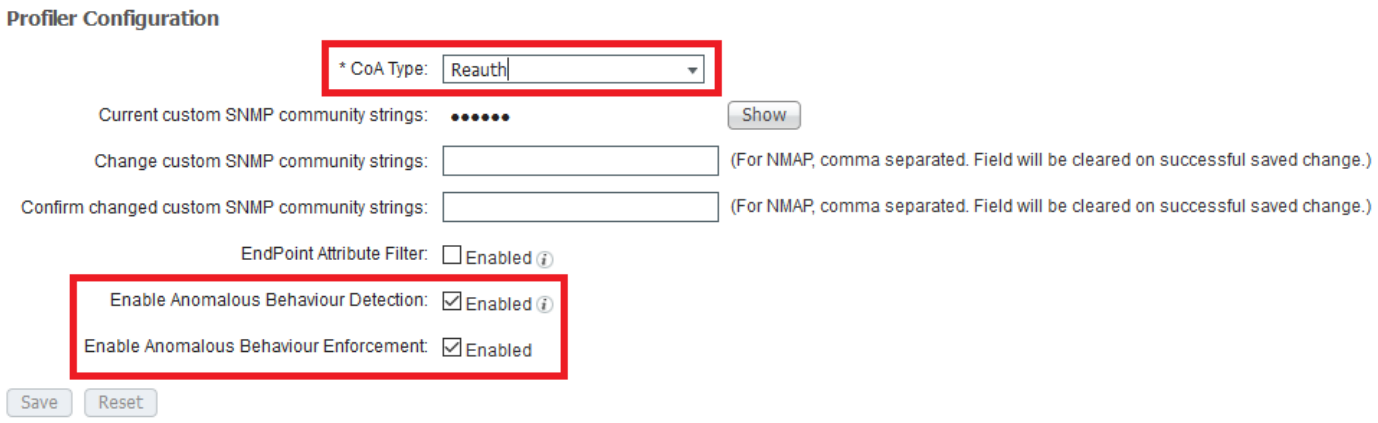


Configurazioni

Sullo switch e sul WLC, vengono eseguite semplici configurazioni MAB e AAA. Per utilizzare questa funzione, effettuare le seguenti operazioni:

Passaggio 1. Abilitare il rilevamento delle anomalie.

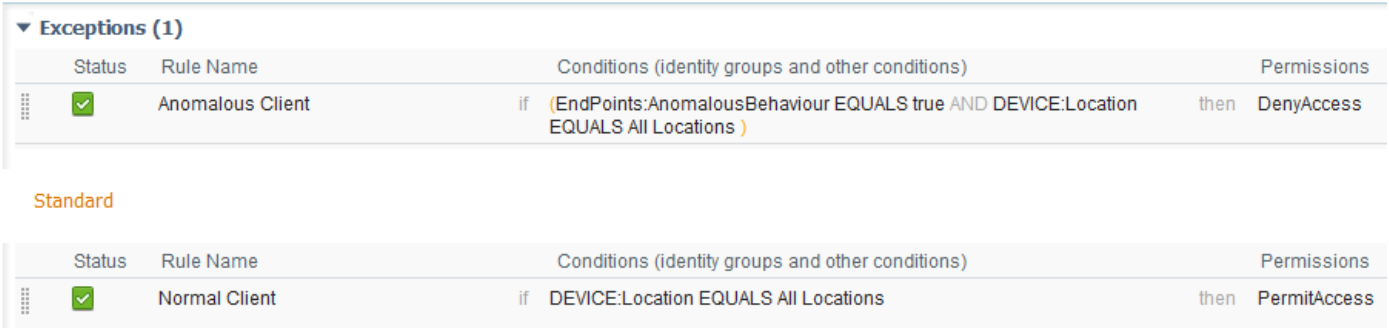
Selezionare **Amministrazione > Sistema > Impostazioni > Profiling**.



La prima opzione consente ad ISE di rilevare comportamenti anomali ma non viene inviato alcun CoA (modalità Visibility-Only). La seconda opzione permette all'ISE di inviare il CoA quando viene rilevato un comportamento anomalo (modalità di imposizione).

Passaggio 2. Configurare i criteri di autorizzazione.

Configurare l'attributo Anomlousbehavior come condizione nei criteri di autorizzazione, come illustrato nell'immagine:

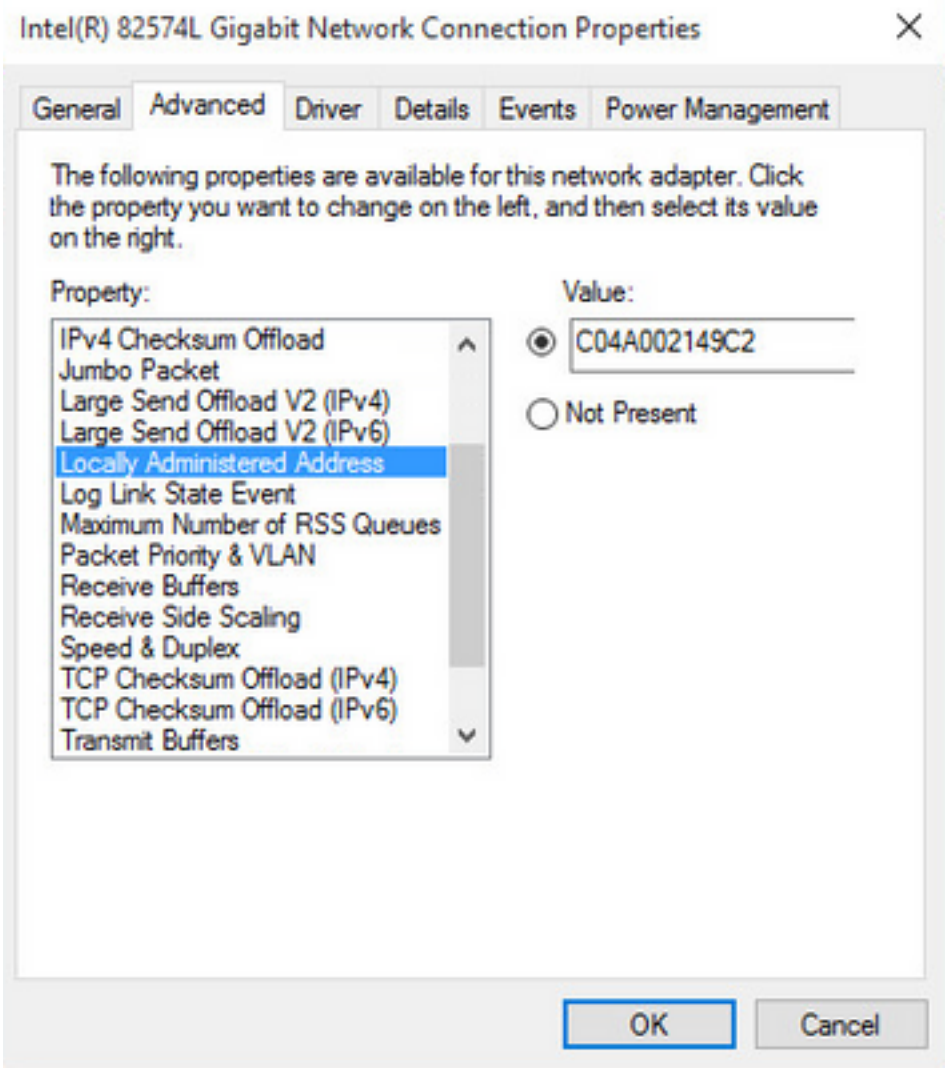


Verifica

Connettersi con una scheda di rete wireless. Utilizzare il comando **ipconfig /all** per trovare l'indirizzo MAC della scheda di rete wireless, come mostrato nell'immagine:

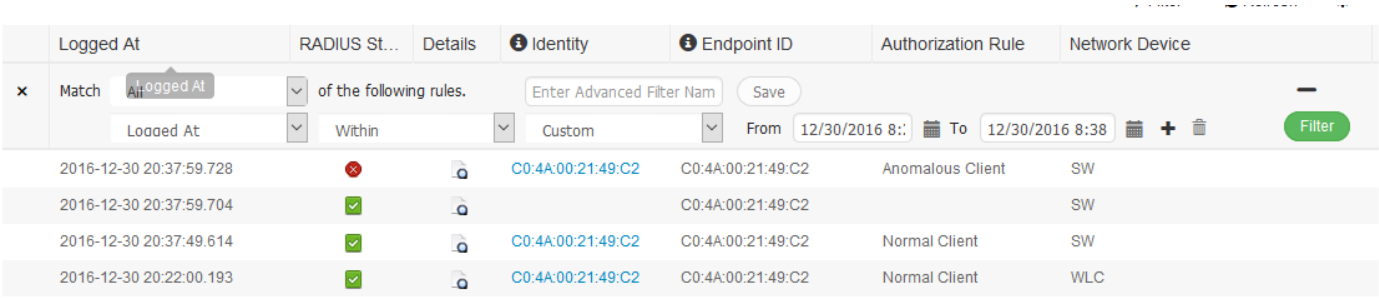
```
Wireless LAN adapter Wi-Fi:

   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
```

Per simulare un utente malintenzionato, è possibile contraffare l'indirizzo MAC della scheda Ethernet in modo che corrisponda all'indirizzo MAC dell'utente normale.

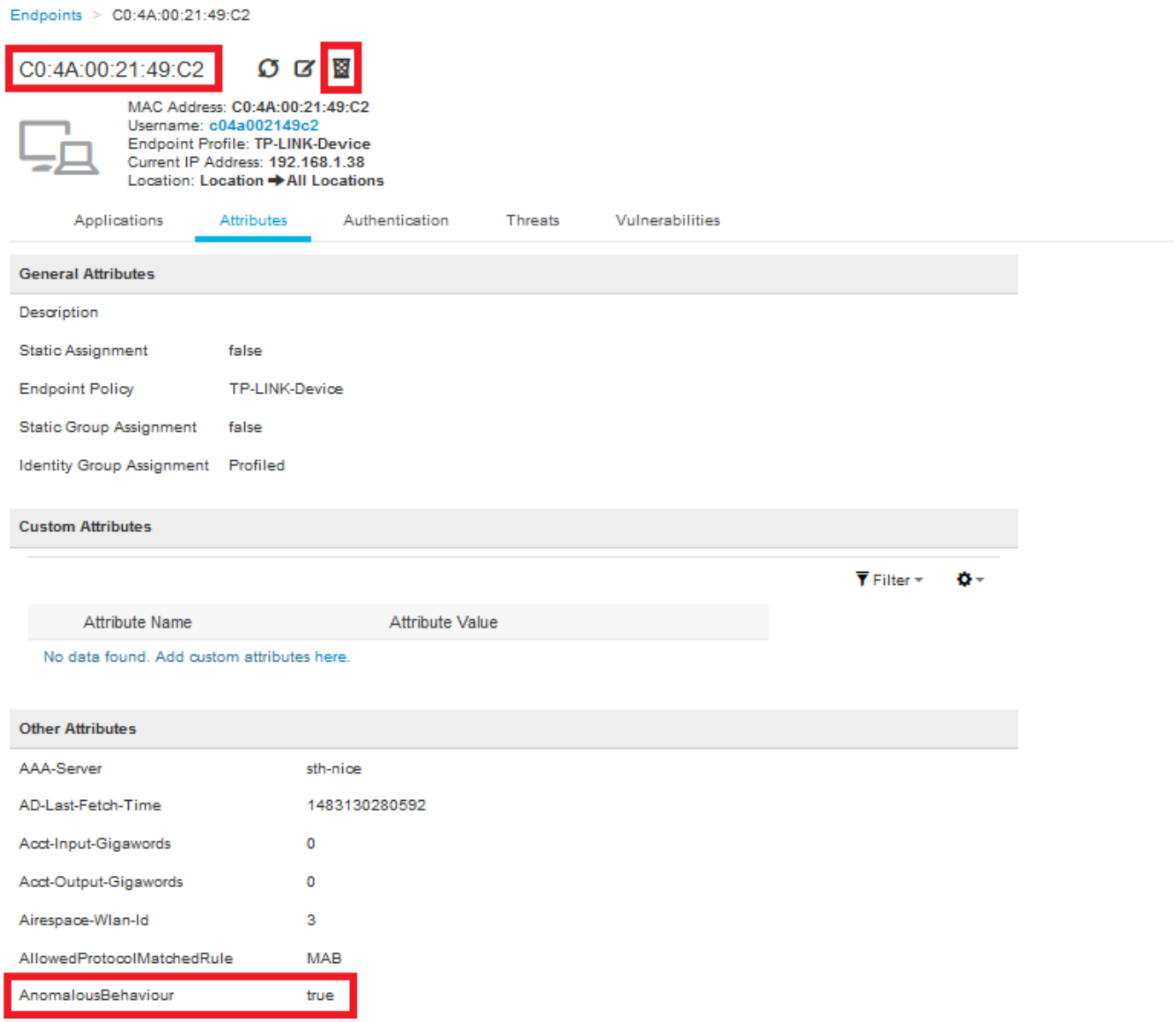


Dopo la connessione dell'utente Normal, sarà possibile visualizzare una voce dell'endpoint nel database. In seguito, l'utente malintenzionato si connette utilizzando un indirizzo MAC oggetto di spoofing.

Dai report è possibile vedere la connessione iniziale dal WLC. In seguito, l'utente malintenzionato si connette e 10 secondi dopo, viene attivata una CoA a causa del rilevamento del client anomalo. Poiché il tipo di CoA globale è impostato su **Reauth**, l'endpoint tenta di connettersi di nuovo. ISE ha già impostato l'attributo AnomalousBehavior su True, quindi ISE corrisponde alla prima regola e nega l'utente.

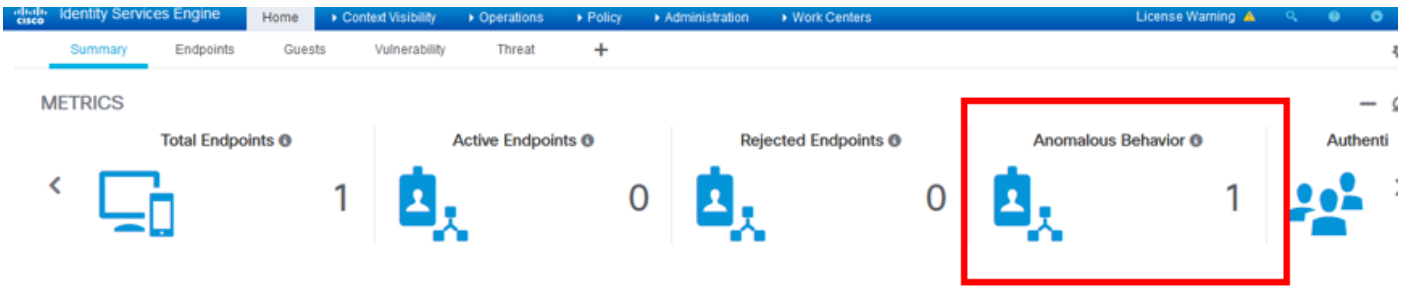


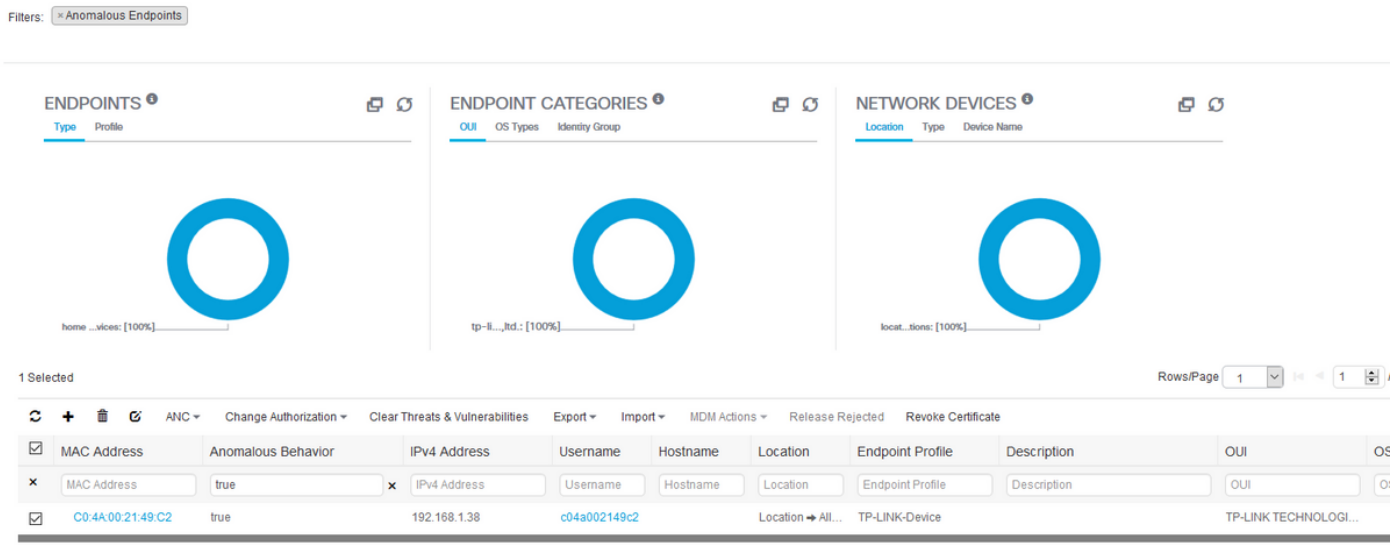
Come mostrato nell'immagine, è possibile visualizzare i dettagli sotto l'endpoint nella scheda Visibilità contesto:



Come si può vedere, l'endpoint può essere eliminato dal database per cancellare questo attributo.

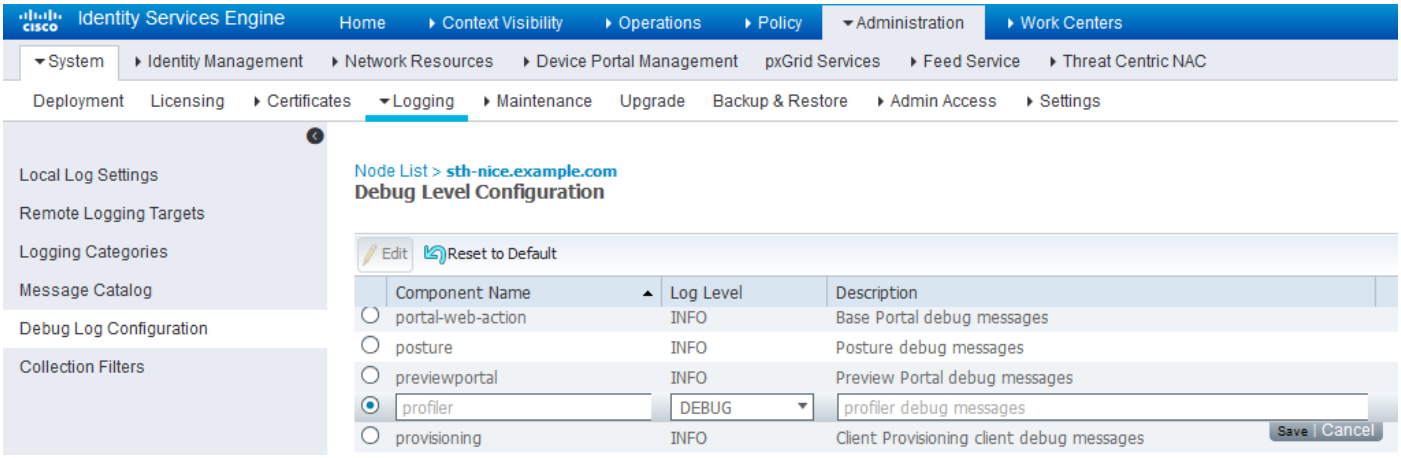
Come mostrato nell'immagine, il dashboard include una nuova scheda che mostra il numero di client che presentano questo comportamento:



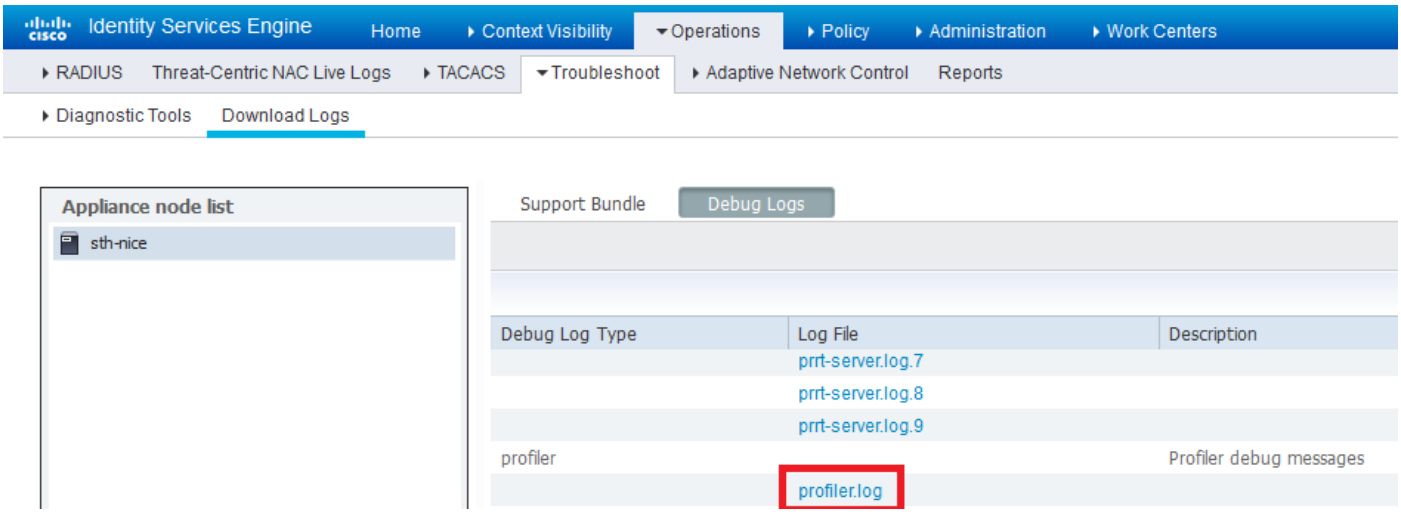


Risoluzione dei problemi

Per risolvere il problema, abilitare il debug del profiler selezionando **Amministrazione > Sistema > Registrazione > Configurazione log di debug**.



Per trovare il file **Profiler.log di** ISE, selezionare **Operazioni > Log di download > Log di debug**, come mostrato nell'immagine:



In questi registri vengono visualizzati alcuni frammenti del file **Profiling.log**. Come si può vedere, ISE è stata in grado di rilevare che l'endpoint con indirizzo MAC C0:4A:00:21:49:C2 ha modificato

il metodo di accesso confrontando i valori vecchi e nuovi degli attributi NAS-Port-Type. È wireless ma viene cambiato in 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
```

Pertanto, ISE interviene poiché l'imposizione è abilitata. L'azione qui consiste nell'inviare un CoA a seconda della configurazione globale nelle impostazioni di profilatura sopra menzionate. Nell'esempio, il tipo CoA è impostato su Reauth, il che consente ad ISE di autenticare nuovamente l'endpoint e verificare nuovamente le regole configurate. Questa volta, corrisponde alla regola client Anomalo e pertanto viene negata.

```
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
```

Informazioni correlate

- Guida all'amministrazione di ISE 2.2