

# Configuratie van analoge Endpoint Detectie en handhaving op ISE 2.2

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Stap 1. Schakel detectie van abnormaliteiten in.](#)

[Stap 2. Het machtigingsbeleid configureren.](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

## Inleiding

In dit document wordt beschreven hoe endpoints worden gedetecteerd en afgedwongen. Dit is een nieuwe Profileringsfunctie die in Cisco Identity Services Engine (ISE) is geïntroduceerd voor een verbeterde netwerkzichtbaarheid.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Wired MAC-verificatie Bypass (MAB)-configuratie op de switch
- Draadloze LAN-configuratie voor draadloze LAN-controller (WLC)
- Verandering van de configuratie van de vergunning (CoA) op beide apparaten

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

1. Identity Services Engine 2.2
2. Draadloze LAN-controller 8.0.10.0
3. Cisco Catalyst switch 3750 15.2(3)E2

#### 4. Windows 10 met bekabelde en draadloze adapters

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Achtergrondinformatie

Met de functie Anomalous Endpoint Detection kunt u de ISE in staat stellen om wijzigingen in specifieke eigenschappen en profielen te controleren voor verbonden endpoints. Als een verandering één of meer van vooraf gevormde anomaliegedragsregels aanpast, zal ISE het eindpunt als Anomaleus markeren. Wanneer ISE is gedetecteerd, kan deze actie ondernemen (met CoA) en bepaalde beleidsmaatregelen afdwingen om de toegang tot het verdachte eindpunt te beperken. Eén van de gebruikcases voor deze functie is de detectie van MAC-adresspoofing.

- 
- **Opmerking:** Deze eigenschap richt niet alle mogelijke scenario's voor het spoofing van het adres van MAC aan. Lees de typen anomalieën die onder deze functie vallen ook door om te bepalen of deze op uw gevallen van toepassing zijn.
- 

Als detectie is ingeschakeld, controleert ISE alle nieuwe informatie die voor bestaande endpoints wordt ontvangen en controleert u of deze eigenschappen zijn gewijzigd:

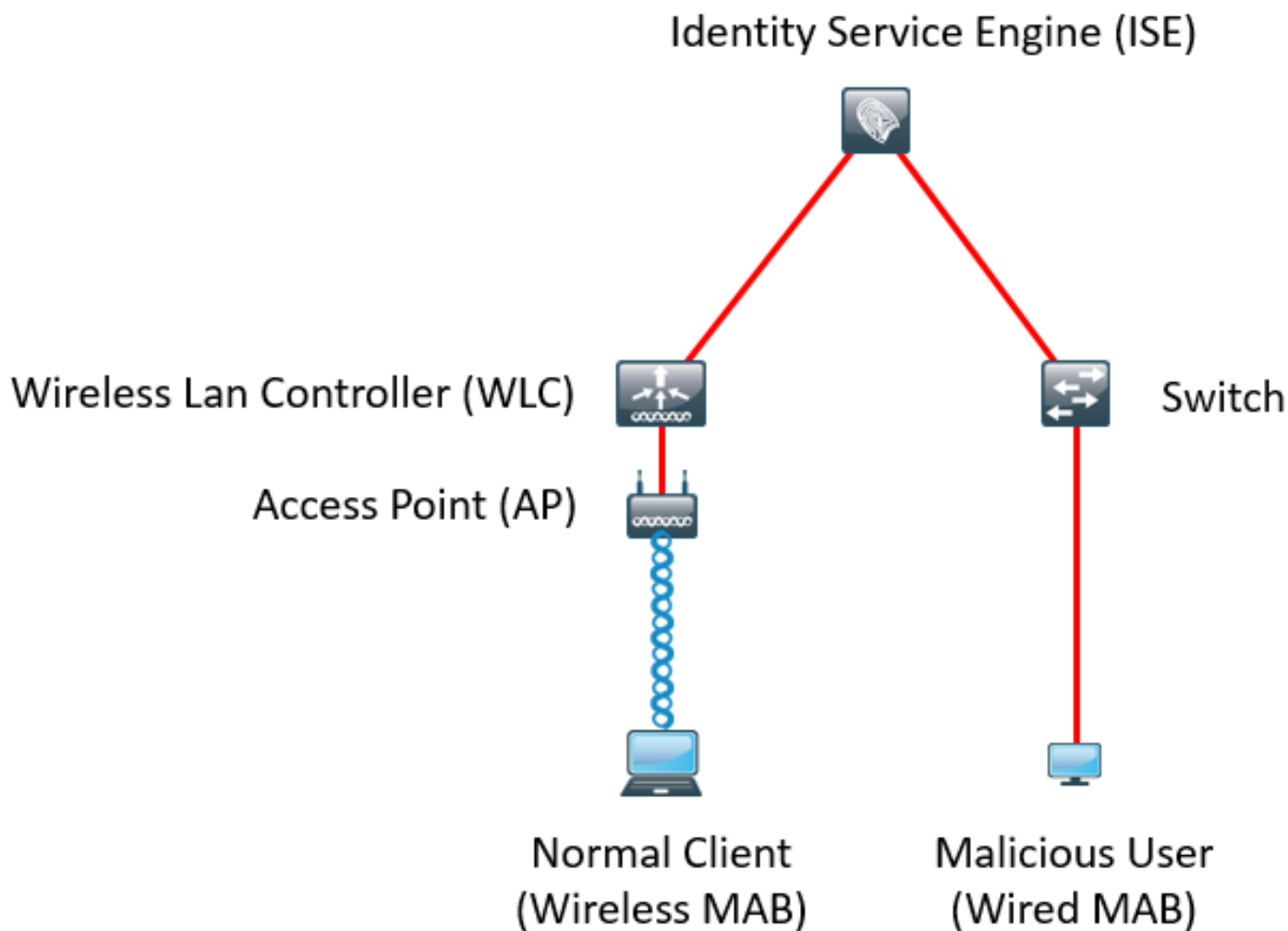
1. **NAS-poorts-type** - bepaalt of de toegangsmethode voor dit eindpunt is gewijzigd. Bijvoorbeeld, als het zelfde MAC adres dat via Wired Dot1x verbonden is gebruikt voor Wireless Dot1x en visum-versa.
2. **DHCP-klasse-ID** - bepaalt of het type client/verkoper van eindpunt is gewijzigd. Dit is alleen van toepassing wanneer de eigenschap DHCP-klasse ID met een bepaalde waarde wordt ingevuld en vervolgens wordt gewijzigd in een andere waarde. Als een eindpunt met een statische IP wordt ingesteld, zal de eigenschap DHCP-klasse ID niet op ISE worden ingevuld. Later, als een ander apparaat het adres van MAC spooft en DHCP gebruikt zal DHCP, zal de Klasse ID van een lege waarde in een specifieke string veranderen. Dit zal geen gedragsdetectie van Anomouls veroorzaken.
3. **Endpoint Policy** - een verandering in endpointprofiel van **printer** of **IP-telefoon** naar **werkstation**.

Zodra ISE een van de hierboven vermelde veranderingen detecteert, wordt de eigenschap AnomalousBehavior toegevoegd aan het eindpunt en op True ingesteld. Dit kan later als voorwaarde in het machtigingsbeleid worden gebruikt om de toegang voor het eindpunt in toekomstige authenticaties te beperken.

Als Handhaving is ingesteld, kan ISE een CoA verzenden zodra de verandering wordt gedetecteerd om opnieuw authentiek te verklaren of een poortaanval voor het eindpunt uit te voeren. In feite kan het de anomalische eindpunten in quarantaine brengen, afhankelijk van het vergunningsbeleid dat is ingesteld.

## Configureren

## Netwerkdigram



## Configuraties

Eenvoudige MAB- en AAA-configuraties worden uitgevoerd op de switch en WLC. Om deze functie te gebruiken, volgt u de volgende stappen:

### Stap 1. Schakel detectie van abnormaliteiten in.

Navigeer naar **Beheer > Systeem > Instellingen > Profileren**.

#### Profiler Configuration

\* CoA Type:

Current custom SNMP community strings:

Change custom SNMP community strings:  (For NMAP, comma separated. Field will be cleared on successful saved change.)

Confirm changed custom SNMP community strings:  (For NMAP, comma separated. Field will be cleared on successful saved change.)

EndPoint Attribute Filter:  Enabled [?](#)

Enable Anomalous Behaviour Detection:  Enabled [?](#)

Enable Anomalous Behaviour Enforcement:  Enabled

Met de eerste optie kan ISE abnormaal gedrag detecteren, maar er wordt geen CoA verzonden (Visibility-only modus). Een tweede optie geeft ISE de mogelijkheid om CoA te verzenden zodra een abnormaal gedrag is gedetecteerd (handhavingsmodus).

## Stap 2. Het machtigingsbeleid configureren.

Configureer de eigenschap anoniem gedrag als een voorwaarde in het machtigingsbeleid, zoals in de afbeelding wordt weergegeven:

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Anomalous Client	if (EndPoints:AnomalousBehaviour EQUALS true AND DEVICE:Location EQUALS All Locations )	then DenyAccess

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Normal Client	if DEVICE:Location EQUALS All Locations	then PermitAccess

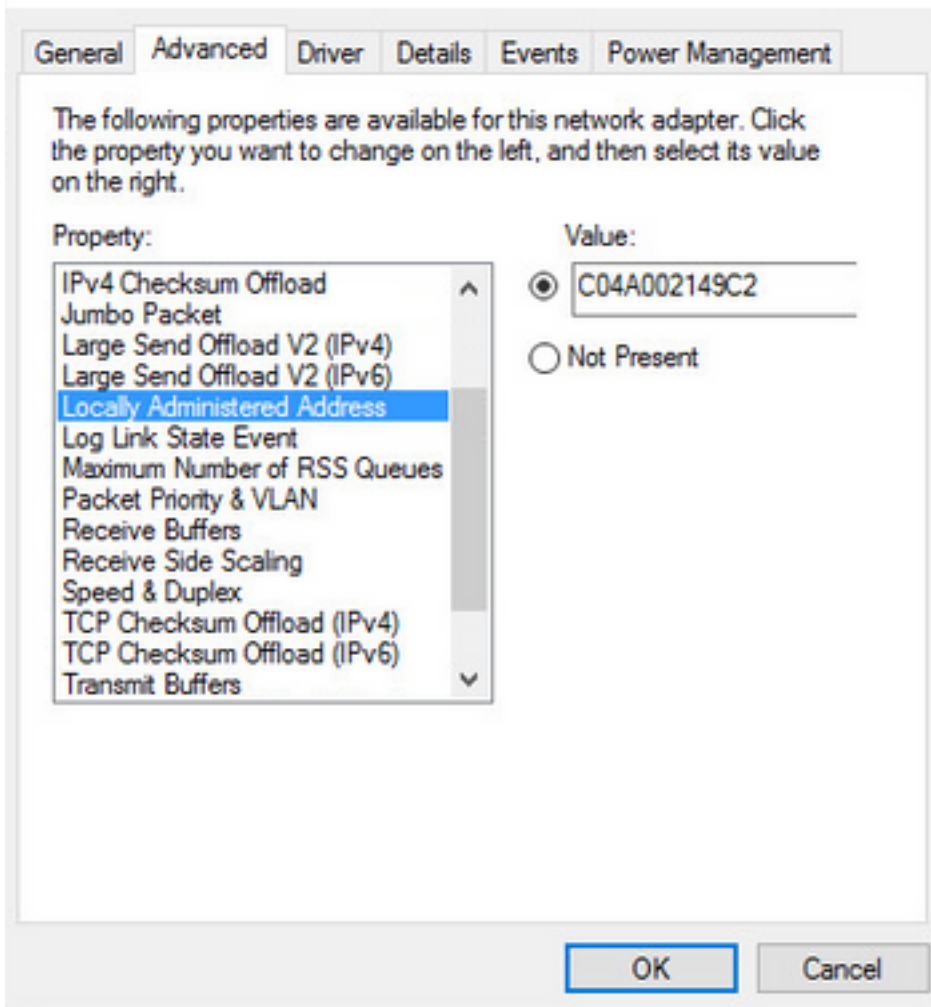
## Verifiëren

Sluit aan op een draadloze adapter. Gebruik opdrachtinvoer `/all` om MAC-adres van draadloze adapter te vinden, zoals in het beeld wordt getoond:

```
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 Tcpi . . . . . : Enabled
```

Om een kwaadaardige gebruiker te simuleren, kunt u het MAC-adres van de Ethernet-adapter benaderen om het MAC-adres van de normale gebruiker aan te passen.



Zodra de normale gebruiker zich aansluit, kunt u een endpointingang in de database zien. Daarna verbindt de kwaadaardige gebruiker zich met een gespoofd MAC-adres.

Aan de hand van de rapporten kunt u de eerste verbinding van de WLC zien. Daarna verbindt de kwaadaardige gebruiker zich en 10 seconden later wordt een CoA geactiveerd vanwege de detectie van de abnormale client. Aangezien het wereldwijde CoA-type op **Reauth** is ingesteld, probeert het eindpunt opnieuw verbinding te maken. ISE stelt de eigenschap AnomalousBehavior al in aan True zodat ISE de eerste regel aanpast en de gebruiker ontkent.

Logged At	RADIUS St...	Details	Identity	Endpoint ID	Authorization Rule	Network Device
Match	Logged At	of the following rules.	Enter Advanced Filter Nam	Save		
Loaded At	Within	Custom	From	12/30/2016 8:00	To	12/30/2016 8:38
2016-12-30 20:37:59.728	✘		C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Anomalous Client	SW
2016-12-30 20:37:59.704	✔			C0:4A:00:21:49:C2		SW
2016-12-30 20:37:49.614	✔		C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Normal Client	SW
2016-12-30 20:22:00.193	✔		C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Normal Client	WLC

Zoals in het beeld wordt getoond, kunt u de details onder het eindpunt in het tabblad Context Visibility zien:

**C0:4A:00:21:49:C2**   

MAC Address: C0:4A:00:21:49:C2  
Username: c04a002149c2  
Endpoint Profile: TP-LINK-Device  
Current IP Address: 192.168.1.38  
Location: Location → All Locations


Applications **Attributes** Authentication Threats Vulnerabilities

### General Attributes

#### Description

Static Assignment	false
Endpoint Policy	TP-LINK-Device
Static Group Assignment	false
Identity Group Assignment	Profiled

### Custom Attributes

Filter 

Attribute Name	Attribute Value
----------------	-----------------

No data found. [Add custom attributes here.](#)

### Other Attributes

AAA-Server	sth-nice
AD-Last-Fetch-Time	1483130280592
Acct-Input-Gigawords	0
Acct-Output-Gigawords	0
Airespace-Wlan-Id	3
AllowedProtocolMatchedRule	MAB
<b>AnomalousBehaviour</b>	<b>true</b>










Zoals u kunt zien, kan het eindpunt uit de database worden verwijderd om deze eigenschap te wissen.

Zoals in de afbeelding wordt getoond, bevat het dashboard een nieuw tabblad om het aantal klanten weer te geven dat dit gedrag vertoont:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Summary Endpoints Guests Vulnerability Threat +

### METRICS

Total Endpoints 	Active Endpoints 	Rejected Endpoints 	<b>Anomalous Behavior </b>	Authenti
 1	 0	 0	 <b>1</b>	

Filters: Anomalous Endpoints

## Problemen oplossen

Raadpleeg voor probleemoplossing het defect profiler, aangezien u navigeert als beheerder > **System > Vastlegging > Logconfiguratie > Log reinigen.**

Om het ISE **Profiler.log**-bestand te vinden, navigeer naar **Operations > Download logs > Debug Logs**, zoals in de afbeelding getoond:

Deze logs tonen een aantal fragmenten uit het bestand **Profiling.log**. Zoals u kunt zien, kon ISE ontdekken dat het eindpunt met het adres van MAC van C0:4A:00:21:49:C2 de toegangsmethode

door de oude en nieuwe waarden van de eigenschappen van het NAS-Port-type te vergelijken heeft veranderd. Het is draadloos maar veranderd 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 [MACSpooferEventHandler-52-thread-1][]
profiler.infrastructure.problemgr.event.MACSpooferEventHandler -:ProfilerCollection:- Received
AttrsModifiedEvent in MACSpooferEventHandler MAC: C0:4A:00:21:49:C2
2016-12-30 20:37:49,618 DEBUG [MACSpooferEventHandler-52-thread-1][]
profiler.infrastructure.problemgr.event.MACSpooferEventHandler -:ProfilerCollection:- Received
AttrsModifiedEvent in MACSpooferEventHandler MAC: C0:4A:00:21:49:C2
2016-12-30 20:37:49,618 INFO [MACSpooferEventHandler-52-thread-1][]
com.cisco.profiler.api.MACSpooferManager -: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 [MACSpooferEventHandler-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 [MACSpooferEventHandler-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 [MACSpooferEventHandler-52-thread-1][]
profiler.infrastructure.problemgr.event.EndpointPersistEventHandler -:ProfilerCollection:- Adding
to queue endpoint persist event for mac: C0:4A:00:21:49:C2
```

Daarom neemt ISE maatregelen, aangezien handhaving mogelijk is. De actie hier is om een CoA te verzenden afhankelijk van de mondiale configuratie in de hierboven genoemde profielen. In ons voorbeeld wordt het CoA-type ingesteld op Reauth waardoor ISE het eindpunt opnieuw kan bevestigen en de regels die waren geconfigureerd opnieuw kan controleren. In dit geval komt het overeen met de anomaleuze klantenwet en wordt het derhalve ontkend.

```
2016-12-30 20:37:49,625 INFO [MACSpooferEventHandler-52-thread-1][]
profiler.infrastructure.problemgr.event.MACSpooferEventHandler -:ProfilerCollection:- Taking mac
spoofer enforcement action for mac: C0:4A:00:21:49:C2
2016-12-30 20:37:49,625 INFO [MACSpooferEventHandler-52-thread-1][]
profiler.infrastructure.problemgr.event.MACSpooferEventHandler -: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

## Gerelateerde informatie

- [ISE 2.2 beheerdershandleiding](#)