

# Konfigurieren der Erkennung und Durchsetzung anomalöser Endgeräte auf ISE 2.2

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Schritt 1: Ermöglichen Sie die Erkennung anomaler Ereignisse.](#)

[Schritt 2: Konfigurieren der Autorisierungsrichtlinie](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einführung

In diesem Dokument werden die Erkennung und Durchsetzung von ungewöhnlichen Endgeräten beschrieben. Dies ist eine neue Profiling-Funktion, die in der Cisco Identity Services Engine (ISE) eingeführt wurde, um die Netzwerktransparenz zu verbessern.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Konfiguration von MAB (Wired MAC Authentication Bypass) auf dem Switch
- Wireless MAB-Konfiguration auf dem Wireless LAN Controller (WLC)
- Änderung der CoA-Konfiguration (Authorization) auf beiden Geräten

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

3. Cisco Catalyst Switch 3750 15.2(3)E2

4. Windows 10 mit kabelgebundenen und Wireless-Adaptoren

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrundinformationen

Die Funktion zur Erkennung anomalöser Endgeräte ermöglicht der ISE die Überwachung von Änderungen an spezifischen Attributen und Profilen für verbundene Endpunkte. Wenn eine Änderung mit einer oder mehreren vorkonfigurierten Regeln für ungewöhnliches Verhalten übereinstimmt, kennzeichnet die ISE den Endpunkt als anomalös. Sobald die ISE erkannt wurde, kann sie Maßnahmen (mit CoA) ergreifen und bestimmte Richtlinien durchsetzen, um den Zugriff auf verdächtige Endgeräte einzuschränken. Einer der Anwendungsfälle für diese Funktion ist die Erkennung von MAC-Adressen-Spoofing.

- 
- **Hinweis:** Diese Funktion behandelt nicht alle potenziellen Szenarien für MAC-Adressen-Spoofing. Lesen Sie unbedingt die Typen von Anomalien, die von dieser Funktion abgedeckt werden, um ihre Anwendbarkeit auf Ihre Anwendungsfälle zu ermitteln.
- 

Sobald die Erkennung aktiviert ist, überwacht die ISE alle neuen Informationen, die sie für vorhandene Endgeräte erhält, und prüft, ob diese Attribute geändert wurden:

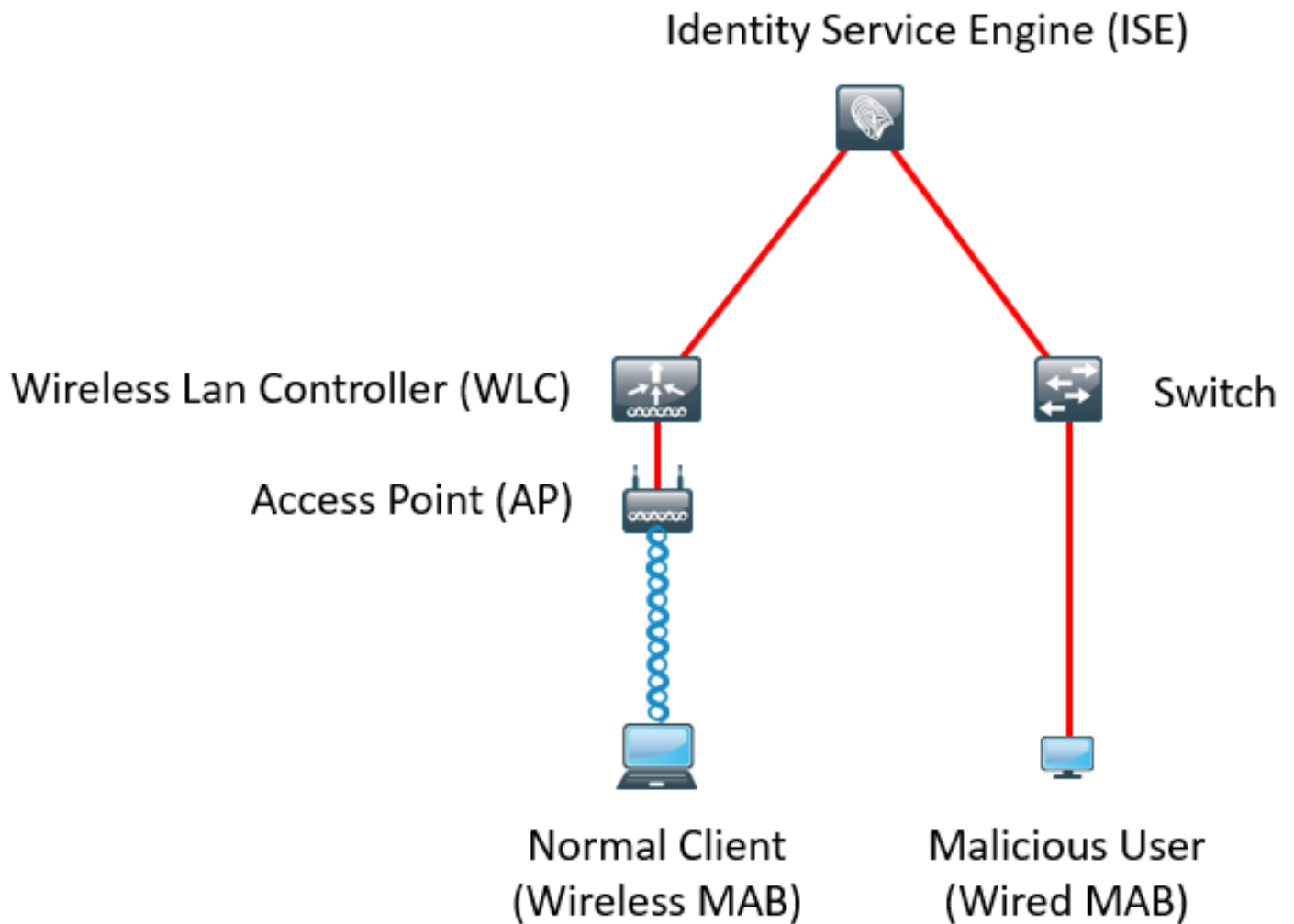
1. **NAS-Port-Typ:** Legt fest, ob die Zugriffsmethode für diesen Endpunkt geändert wurde. Wenn z. B. dieselbe MAC-Adresse, die über kabelgebundene Dot1x verbunden ist, auch für Wireless Dot1x und Visa-Vers verwendet wird.
2. **DHCP Class ID** - Legt fest, ob sich der Client-/Anbieterendgerätetyp geändert hat. Dies gilt nur, wenn das DHCP-Klasse-ID-Attribut mit einem bestimmten Wert gefüllt und dann in einen anderen Wert geändert wird. Wenn ein Endpunkt mit einer statischen IP-Adresse konfiguriert ist, wird das DHCP-Klasse-ID-Attribut nicht in die ISE übernommen. Wenn später ein anderes Gerät die MAC-Adresse spuckt und DHCP verwendet, ändert sich die Klassen-ID von einem leeren Wert in eine bestimmte Zeichenfolge. Dies löst keine Erkennung von Anomalous-Verhalten aus.
3. **Endpunktrichtlinie** - Eine Änderung des Endgeräteprofils vom **Drucker** oder **IP-Telefon** zur **Workstation**.

Sobald die ISE eine der oben genannten Änderungen erkennt, wird das AnomalousBehavior-Attribut dem Endpunkt hinzugefügt und auf True festgelegt. Dies kann später als Bedingung in Autorisierungsrichtlinien verwendet werden, um den Zugriff für den Endpunkt bei zukünftigen Authentifizierungen zu beschränken.

Wenn die Durchsetzung konfiguriert ist, kann die ISE eine CoA senden, sobald die Änderung erkannt wurde, um sie erneut zu authentifizieren oder einen Port-Bounce für den Endpunkt auszuführen. In diesem Fall kann der ungewöhnliche Endpunkt in Abhängigkeit von den konfigurierten Autorisierungsrichtlinien unter Quarantäne gestellt werden.

# Konfigurieren

## Netzwerkdiagramm



## Konfigurationen

Auf dem Switch und dem WLC werden einfache MAB- und AAA-Konfigurationen ausgeführt. Um diese Funktion zu verwenden, gehen Sie wie folgt vor:

**Schritt 1: Ermöglichen Sie die Erkennung anomaler Ereignisse.**

Navigieren Sie zu **Administration > System > Settings > Profiling**.

## 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

Die erste Option ermöglicht der ISE die Erkennung ungewöhnlicher Verhaltensweisen, jedoch wird kein CoA gesendet (Nur-Transparenz-Modus). Bei der zweiten Option kann die ISE CoA senden, sobald ein ungewöhnliches Verhalten erkannt wurde (Durchsetzungsmodus).

## Schritt 2: Konfigurieren der Autorisierungsrichtlinie

Konfigurieren Sie das Anomalousverhalten-Attribut als Bedingung in der Autorisierungsrichtlinie, wie im Bild gezeigt:

▼ Exceptions (1)				
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

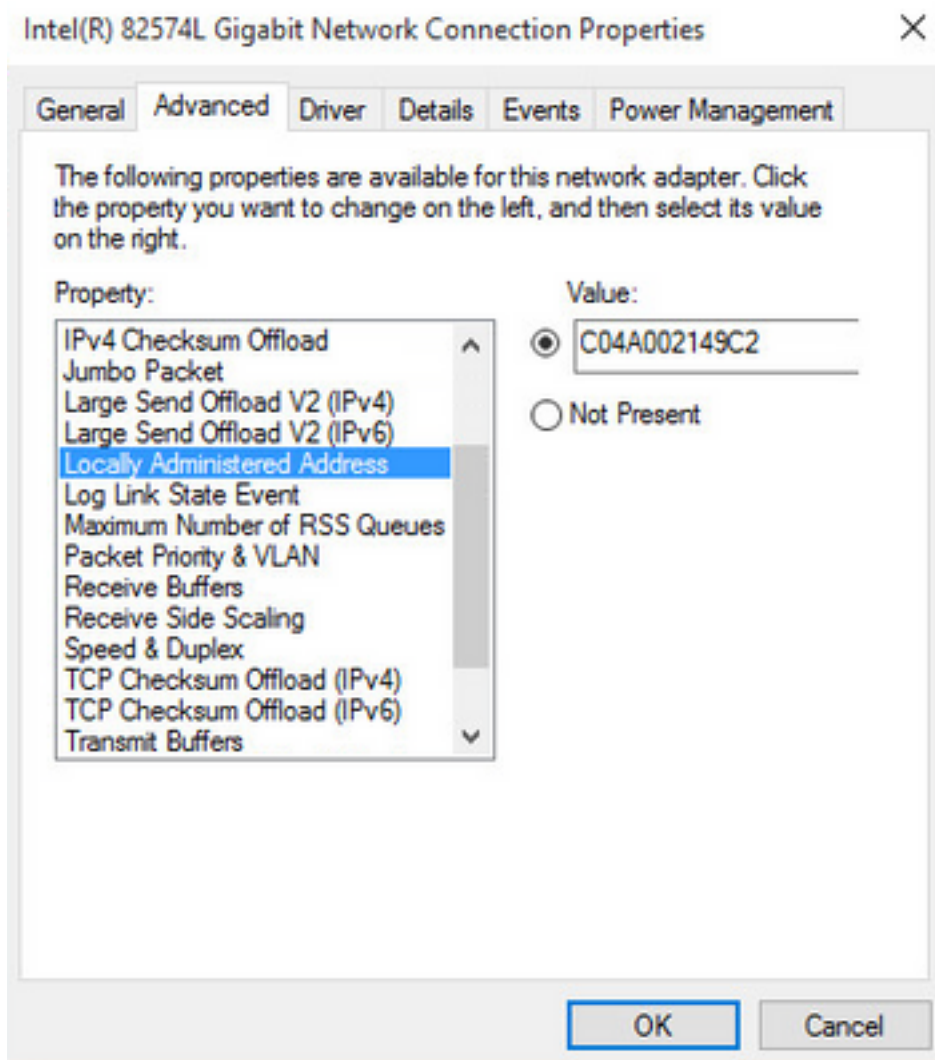
## Überprüfen

Stellen Sie eine Verbindung mit einem Wireless-Adapter her. Verwenden Sie den Befehl `ipconfig /all`, um die MAC-Adresse des Wireless-Adapters zu finden, wie im Bild gezeigt:

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 Tcpiip. . . . . : Enabled
```

Um einen böswilligen Benutzer zu simulieren, können Sie die MAC-Adresse des Ethernet-Adapters mit der MAC-Adresse des normalen Benutzers vergleichen.






Sobald der normale Benutzer eine Verbindung hergestellt hat, wird ein Endpunkt-Eintrag in der Datenbank angezeigt. Anschließend stellt der böswillige Benutzer eine Verbindung über eine gefälschte MAC-Adresse her.


In den Berichten wird die Erstverbindung vom WLC aus angezeigt. Anschließend stellt der böswillige Benutzer eine Verbindung her und 10 Sekunden später wird ein CoA ausgelöst, da der ungewöhnliche Client erkannt wird. Da der globale CoA-Typ auf **Reauth** festgelegt ist, versucht der Endpunkt erneut, eine Verbindung herzustellen. Die ISE legt das AnomalousBehavior-Attribut bereits auf True fest, sodass die ISE mit der ersten Regel übereinstimmt und dem Benutzer verweigert.

Match	Logged At	RADIUS St...	Details	Identity	Endpoint ID	Authorization Rule	Network Device
×	Match	of the following rules.	Enter Advanced Filter Nam	Save			
	Logged 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	C0:4A:00:21:49:C2	Normal Client	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

Wie im Bild gezeigt, können Sie die Details unter dem Endpunkt auf der Registerkarte "Context Visibility" (Kontexttransparenz) anzeigen:

Endpoints > C0:4A:00:21:49:C2

**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. <a href="#">Add custom attributes here.</a>	

**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>

Wie Sie sehen, kann der Endpunkt aus der Datenbank gelöscht werden, um dieses Attribut zu löschen.

Wie im Bild gezeigt, enthält das Dashboard eine neue Registerkarte, um die Anzahl der Clients anzuzeigen, die dieses Verhalten zeigen:

Filters: Anomalous Endpoints

MAC Address	Anomalous Behavior	IPv4 Address	Username	Hostname	Location	Endpoint Profile	Description	OUI	OS
C0-4A-00-21-49-C2	true	192.168.1.38	c04a002149c2		Location → All...	TP-LINK-Device		TP-LINK TECHNOLOGI...	

## Fehlerbehebung

Aktivieren Sie zur Fehlerbehebung das Debuggen von Profilen, wenn Sie zu **Administration > System > Logging > Debug Log Configuration** navigieren.

Node List > sth-nice.example.com  
Debug Level Configuration

Component Name	Log Level	Description
<input type="radio"/> portal-web-action	INFO	Base Portal debug messages
<input type="radio"/> posture	INFO	Posture debug messages
<input type="radio"/> previewportal	INFO	Preview Portal debug messages
<input checked="" type="radio"/> profiler	DEBUG	profiler debug messages
<input type="radio"/> provisioning	INFO	Client Provisioning client debug messages

Save | Cancel

Um die Datei ISE Profiler.log zu finden, wählen Sie **Operations > Download Logs > Debug Logs (Vorgänge > Download-Protokolle > Debug-Protokolle)**, wie im Bild gezeigt:

**Appliance node list**

- sth-nice

Support Bundle Debug Logs

Debug Log Type	Log File	Description
	<a href="#">prtt-server.log.7</a>	
	<a href="#">prtt-server.log.8</a>	
	<a href="#">prtt-server.log.9</a>	
profiler	<a href="#">profiler.log</a>	Profiler debug messages

Diese Protokolle zeigen einige Ausschnitte aus der Datei **Profiling.log** an. Wie Sie sehen können, konnte die ISE erkennen, dass der Endpunkt mit der MAC-Adresse C0:4A:00:21:49:C2 die Zugriffsmethode geändert hat, indem die alten und neuen Werte der NAS-Port-Type-Attribute verglichen wurden. Es ist drahtlos, wird aber zu Ethernet geändert.

```

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.probemgr.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.probemgr.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.probemgr.event.EndpointPersistEventHandler -:ProfilerCollection:- Adding
to queue endpoint persist event for mac: C0:4A:00:21:49:C2
  
```

Daher ergreift die ISE Maßnahmen, da die Durchsetzung aktiviert ist. Die Aktion besteht hier darin, eine CoA zu senden, abhängig von der globalen Konfiguration in den oben genannten Profileinstellungen. Im vorliegenden Beispiel ist der CoA-Typ auf Reauth festgelegt, sodass die ISE den Endpunkt erneut authentifizieren und die konfigurierten Regeln erneut überprüfen kann. Diesmal entspricht es der Anomalous-Clientregel und wird daher abgelehnt.

```

2016-12-30 20:37:49,625 INFO [MACSpooferEventHandler-52-thread-1][]
profiler.infrastructure.probemgr.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.probemgr.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
```

## Zugehörige Informationen

- [ISE 2.2 Administrationsleitfaden](#)