

Configurar detecção e aplicação de endpoints anômalos no ISE 2.2

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Etapa 1. Ative a detecção de anomalias.](#)

[Etapa 2. Configure a Política de Autorização.](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve a detecção e a aplicação de endpoints anômalos. Este é um novo recurso de criação de perfil introduzido no Cisco Identity Services Engine (ISE) para maior visibilidade da rede.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do Wired MAC Authentication Bypass (MAB) no switch
- Configuração de MAB sem fio no Wireless LAN Controller (WLC)
- Alteração da configuração de autorização (CoA) em ambos os dispositivos

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

1. Identity Services Engine 2.2
2. Controlador de LAN sem fio 8.0.100.0
3. Switch Cisco Catalyst 3750 15.2(3)E2

4. Windows 10 com adaptadores com e sem fio

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

O recurso Anomalous Endpoint Detection permite que o ISE monitore alterações em atributos e perfis específicos para terminais conectados. Se uma alteração corresponder a uma ou mais regras de comportamento anômalo pré-configuradas, o ISE marcará o endpoint como Anomalous. Depois de detectado, o ISE pode agir (com CoA) e aplicar certas políticas para restringir o acesso do endpoint suspeito. Um dos casos de uso para esse recurso inclui a detecção de falsificação de endereços MAC.

-
- **Note:** Este recurso não aborda todos os cenários em potencial para falsificação de endereços MAC. Leia os tipos de anomalias cobertos por este recurso para determinar sua aplicabilidade aos casos de uso.
-

Quando a detecção estiver habilitada, o ISE monitora todas as novas informações recebidas para os endpoints existentes e verifica se esses atributos foram alterados:

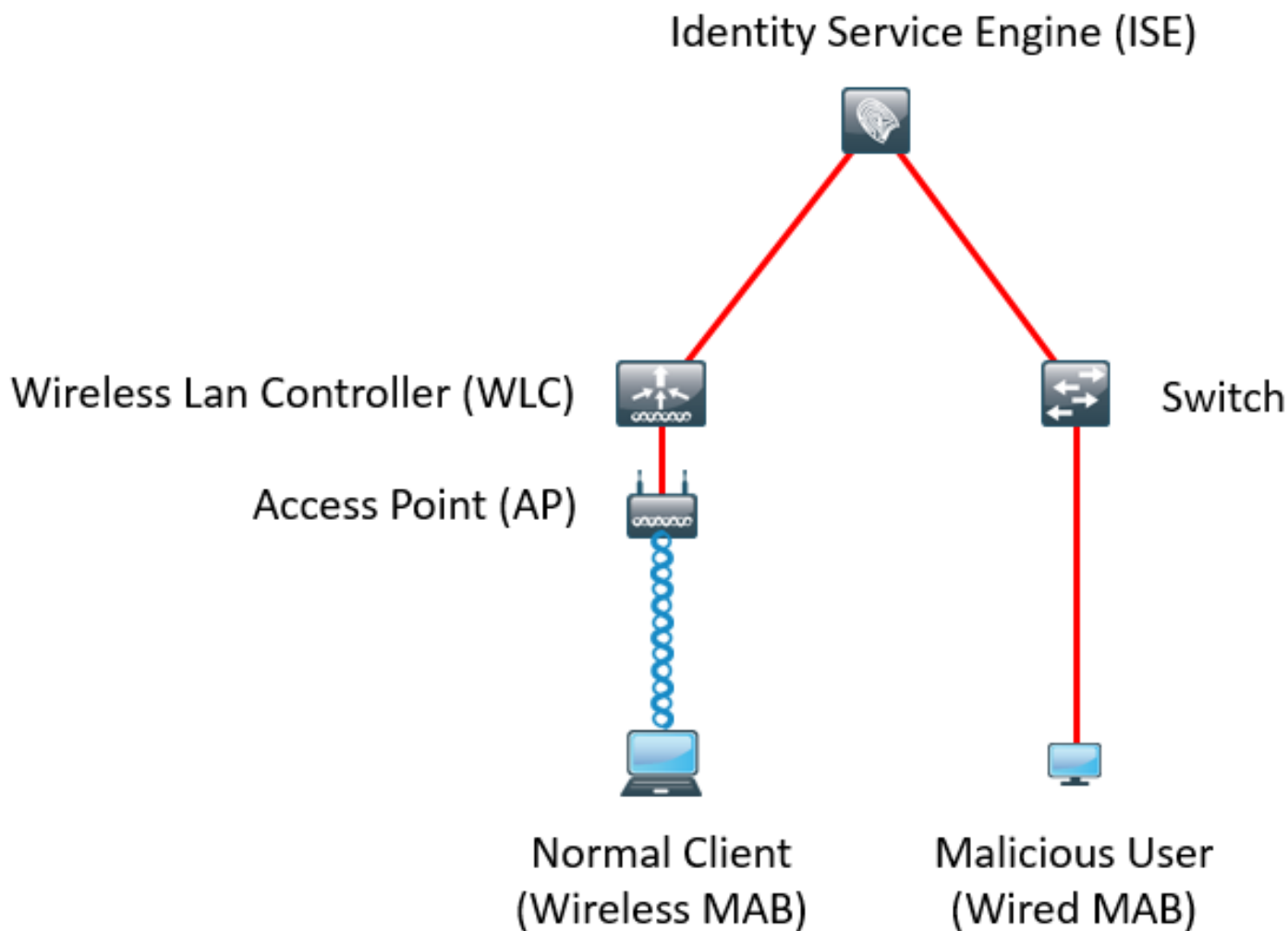
1. **NAS-Port-Type** - Determina se o método de acesso deste endpoint foi alterado. Por exemplo, se o mesmo endereço MAC conectado via Wired Dot1x for usado para Wireless Dot1x e visa-versa.
2. **DHCP Class ID** - Determina se o tipo de cliente/fornecedor do endpoint foi alterado. Isso só se aplica quando o atributo de ID de classe de DHCP é preenchido com um determinado valor e alterado para outro valor. Se um endpoint for configurado com um IP estático, o atributo de ID de classe de DHCP não será preenchido no ISE. Mais tarde, se outro dispositivo falsificar o endereço MAC e usar DHCP, o ID da classe mudará de um valor vazio para uma cadeia específica. Isso não ativará a detecção de comportamento dos Anomouls.
3. **Endpoint Policy** - Uma alteração no perfil de endpoint de **impressora** ou **telefone IP** para **estação de trabalho**.

Quando o ISE detecta uma das alterações mencionadas acima, o atributo AnomalousBehavior é adicionado ao endpoint e definido como True. Isso pode ser usado posteriormente como uma condição nas políticas de autorização para restringir o acesso para o endpoint em autenticações futuras.

Se a imposição estiver configurada, o ISE poderá enviar um CoA depois que a alteração for detectada para autenticar novamente ou executar uma devolução de porta para o endpoint. Se estiver em vigor, ele poderá colocar em quarentena o endpoint anômalo, dependendo das políticas de autorização configuradas.

Configurar

Diagrama de Rede



Configurações

As configurações MAB e AAA simples são executadas no switch e na WLC. Para utilizar esse recurso, siga estas etapas:

Etapa 1. Ative a detecção de anomalias.

Navegue até **Administração > Sistema > Configurações > Criação de perfil**.

Profiler Configuration

* CoA Type: Reauth

Current custom SNMP community strings: ●●●●●

Show

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

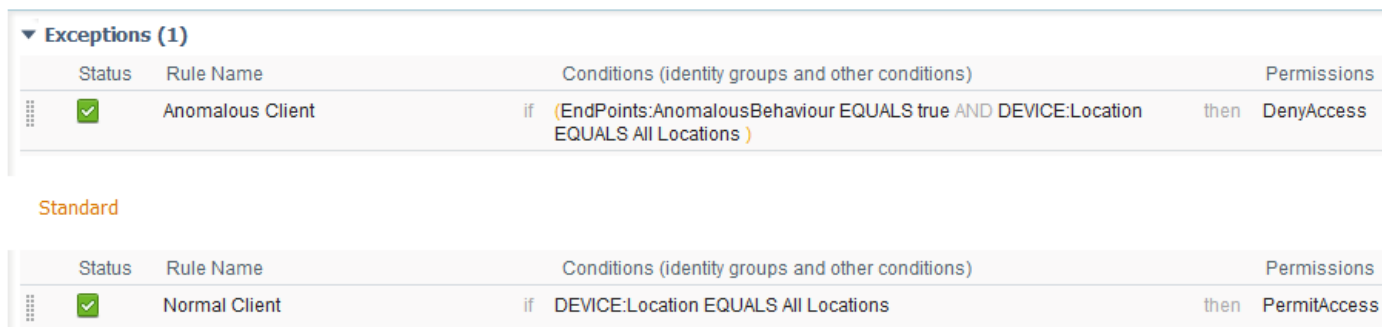
Save

Reset

A primeira opção permite que o ISE detecte qualquer comportamento anômalo, mas nenhuma CoA é enviada (modo somente de visibilidade). A segunda opção permite que o ISE envie o CoA depois que um comportamento anômalo é detectado (modo de aplicação).

Etapa 2. Configure a Política de Autorização.

Configure o atributo Anomalous como uma condição na política de autorização, como mostrado na imagem:



The screenshot shows the ISE policy configuration interface. It displays two rules under the 'Exceptions (1)' section. The first rule, 'Anomalous Client', is enabled (checked) and has a condition 'if (EndPoints:AnomalousBehaviour EQUALS true AND DEVICE:Location EQUALS All Locations)' and a permission 'then DenyAccess'. The second rule, 'Normal Client', is also enabled (checked) and has a condition 'if DEVICE:Location EQUALS All Locations' and a permission 'then PermitAccess'.

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
<input checked="" type="checkbox"/>	Normal Client	if DEVICE:Location EQUALS All Locations	then PermitAccess

Verificar

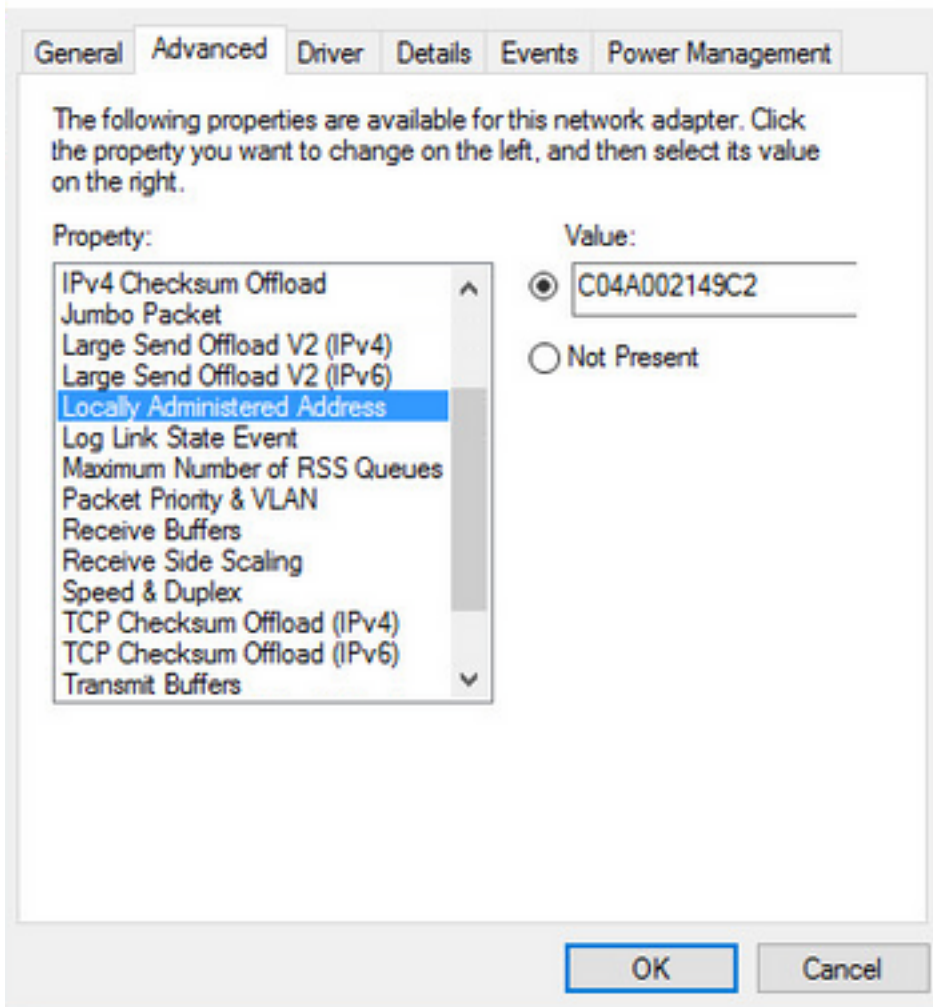
Conecte-se com um adaptador sem fio. Use o comando `ipconfig /all` para localizar o endereço MAC do adaptador sem fio, como mostrado na imagem:

```
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
```

Para simular um usuário mal-intencionado, você pode falsificar o endereço MAC do adaptador Ethernet para corresponder ao endereço MAC do usuário normal.

Intel(R) 82574L Gigabit Network Connection Properties



Quando o usuário Normal se conectar, você poderá ver uma entrada de ponto final no banco de dados. Depois, o usuário mal-intencionado se conecta usando um endereço MAC falsificado.

Nos relatórios, você pode ver a conexão inicial do WLC. Depois, o usuário mal-intencionado se conecta e, 10 segundos depois, um CoA é acionado devido à detecção do cliente anômalo. Como o tipo de CoA global está definido como **Reauth**, o ponto final tenta estabelecer ligação novamente. O ISE já definiu o atributo AnomalousBehavior como True para que o ISE corresponda à primeira regra e negue o usuário.

Logged At	RADIUS St...	Details	Identity	Endpoint ID	Authorization Rule	Network Device
2016-12-30 20:37:59.728	✘	of the following rules.	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

Como mostrado na imagem, você pode ver os detalhes no endpoint na guia Visibilidade de contexto:

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
AnomalousBehaviour	true

Como você pode ver, o endpoint pode ser excluído do banco de dados para limpar esse atributo.

Como mostrado na imagem, o painel inclui uma nova guia para mostrar o número de clientes que exibem esse comportamento:

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

Summary Endpoints Guests Vulnerability Threat +

METRICS

Total Endpoints 1	Active Endpoints 0	Rejected Endpoints 0	Anomalous Behavior 1	Authenti
-------------------	--------------------	----------------------	-----------------------------	----------

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...	

Troubleshoot

Para solucionar problemas, habilite o profiler debug, conforme você navega para **Administration > System > Logging > Debug Log 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

Para localizar o arquivo ISE **Profiler.log**, navegue para **Operations > Download Logs > Debug Logs**, como mostrado na imagem:

Debug Log Type	Log File	Description
	prrt-server.log.7	
	prrt-server.log.8	
	prrt-server.log.9	
profiler	profiler.log	Profiler debug messages

Esses registros mostram alguns trechos do arquivo **Profiles.log**. Como você pode ver, o ISE foi capaz de detectar que o endpoint com endereço MAC de C0:4A:00:21:49:C2 alterou o método de

acesso comparando os valores antigos e novos dos atributos do tipo de porta NAS. É sem fio, mas é alterado para 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
```

Portanto, o ISE toma medidas, já que a aplicação está habilitada. A ação aqui é enviar um CoA dependendo da configuração global nas configurações de criação de perfil mencionadas acima. Em nosso exemplo, o tipo de CoA é definido como Reauth, o que permite que o ISE autentique novamente o endpoint e verifique novamente as regras que foram configuradas. Desta vez, ele corresponde à regra do cliente Anomalous e, portanto, é negado.

```
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

Informações Relacionadas

- [Guia de administração do ISE 2.2](#)