Implante o ASA DAP para identificar o endereço MAC para o AnyConnect

Contents

Introdução

Pré-requisitos

- Requisitos
- Componentes Utilizados

Informações de Apoio

Configurar

- Diagrama de Rede
- Configuração no ASA
- Configuração no ASDM

Verificar

- Cenário 1. Somente um DAP é correspondido
- Cenário 2. O DAP padrão é correspondente
- Cenário 3. Vários DAPs (Ação : Continuar) são correspondidos
- Cenário4. Vários DAPs (Ação: Terminar) são correspondidos

Troubleshooting Geral

Informações Relacionadas

Introdução

Este documento descreve como configurar Políticas de Acesso Dinâmico (DAP) através do ASDM, para verificar o Endereço Mac do dispositivo usado para a conexão do AnyConnect.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:
Configuração do Cisco Anyconnect e Hostscan

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:
ASAv 9.18 (4)
ASDM 7.20 (1)
Anyconnect 4.10.07073
Hostscan 4.10.07073
Windows 10

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

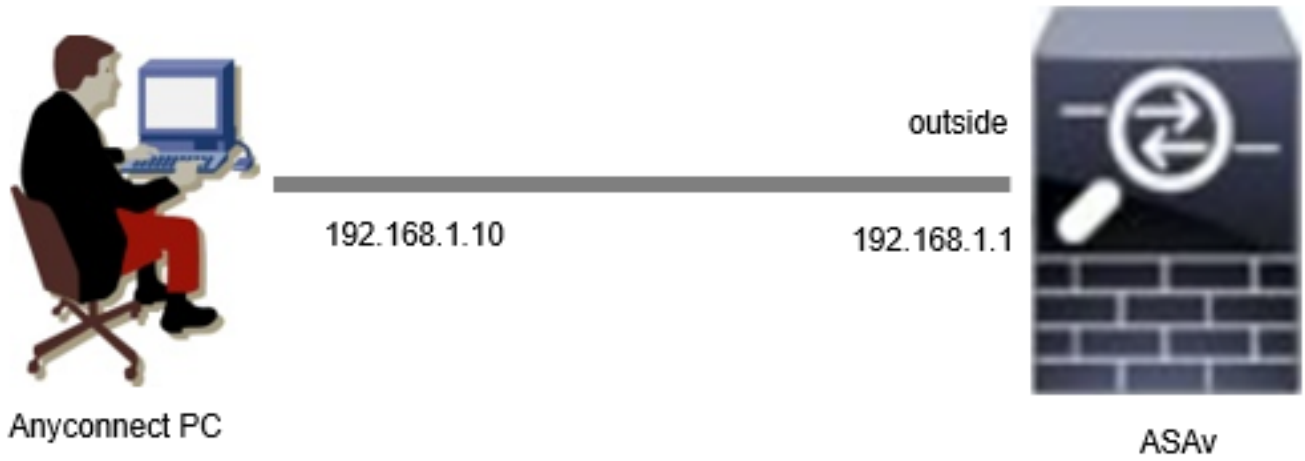
Informações de Apoio

O HostScan é um módulo de software que fornece ao AnyConnect Secure Mobility Client a capacidade de aplicar políticas de segurança na rede. Durante o processo do Hostscan, vários detalhes sobre o dispositivo cliente são coletados e relatados ao Adaptive Security Appliance (ASA). Esses detalhes incluem o sistema operacional do dispositivo, software antivírus, software de firewall, endereço MAC e muito mais. O recurso de Políticas de Acesso Dinâmico (DAP - Dynamic Access Policies) permite que os administradores de rede configurem políticas de segurança em uma base por usuário, o atributo endpoint.device.MAC no DAP pode ser usado para corresponder ou verificar o endereço MAC do dispositivo cliente em relação a políticas predefinidas.

Configurar

Diagrama de Rede

Esta imagem mostra a topologia usada para o exemplo deste documento.



Diagrama

Configuração no ASA

Essa é a configuração mínima no ASA CLI.

```
tunnel-group dap_test_tg type remote-access
tunnel-group dap_test_tg general-attributes
default-group-policy dap_test_gp
tunnel-group dap_test_tg webvpn-attributes
group-alias dap_test enable
```

```
group-policy dap_test_gp internal
group-policy dap_test_gp attributes
vpn-tunnel-protocol ssl-client
address-pools value ac_pool
webvpn
anyconnect keep-installer installed
always-on-vpn profile-setting

ip local pool ac_pool 172.16.1.11-172.16.1.20 mask 255.255.255.0

webvpn
 enable outside
 hostscan image disk0:/hostscan_4.10.07073-k9.pkg
 hostscan enable
 anyconnect image disk0:/anyconnect-win-4.10.07073-webdeploy-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
```

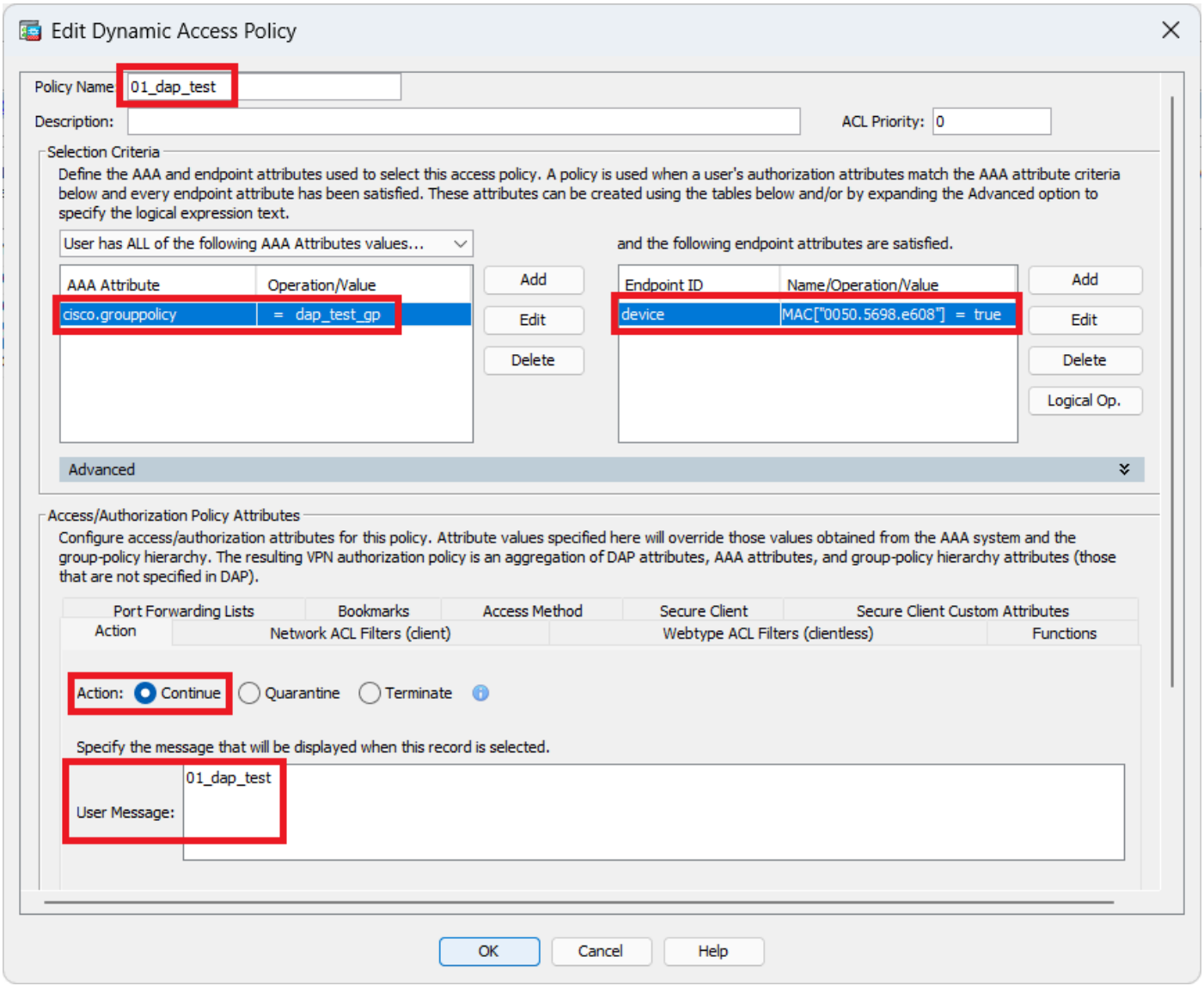
Configuração no ASDM

Esta seção descreve como configurar o registro DAP no ASDM. Neste exemplo, defina 3 registros DAP que usam o atributo endpoint.device.MAC como uma condição.

·01_dap_test:endpoint.device.MAC=0050.5698.e608
·02_dap_test:endpoint.device.MAC=0050.5698.e605 = MAC do endpoint Anyconnect
·03_dap_test:endpoint.device.MAC=0050.5698.e609

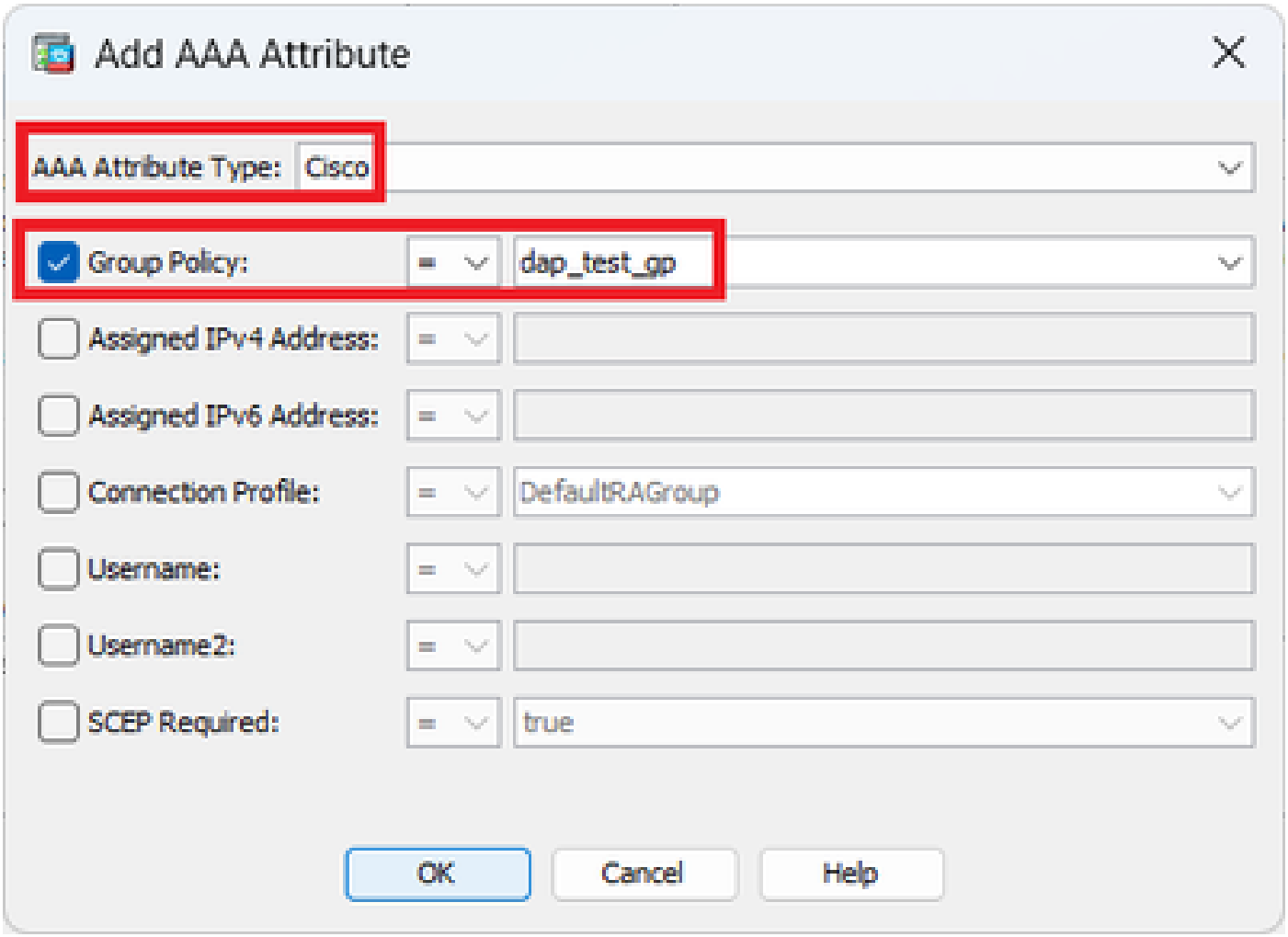
1. Configure o primeiro DAP chamado 01_dap_test.

Navegue até Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies. Clique em Adicionar e defina o Nome da política, o Atributo AAA, os atributos do ponto final, Ação, Mensagem do usuário, como mostrado na imagem:



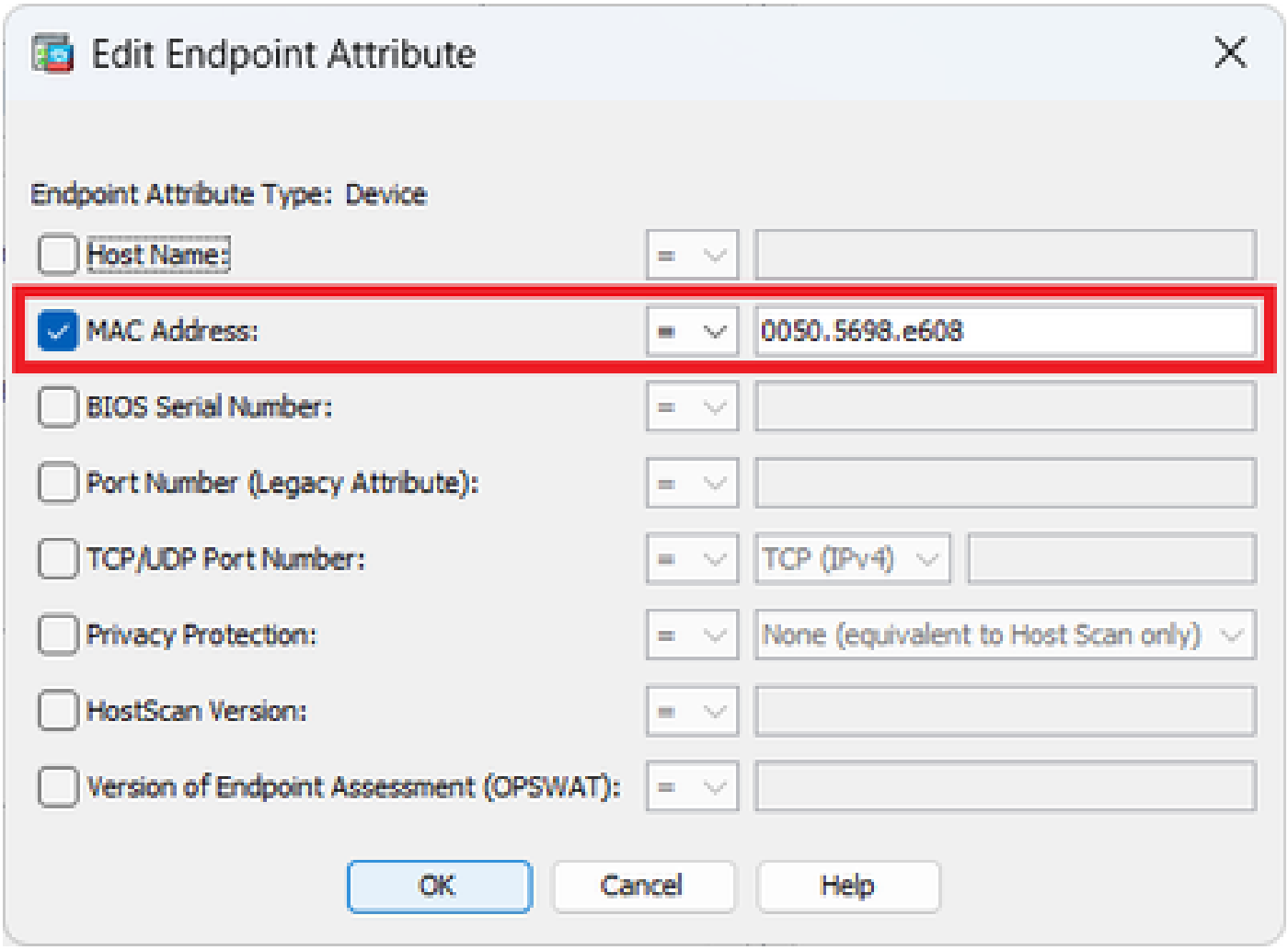
Configurar primeiro DAP

Configure a Diretiva de Grupo para o Atributo AAA.



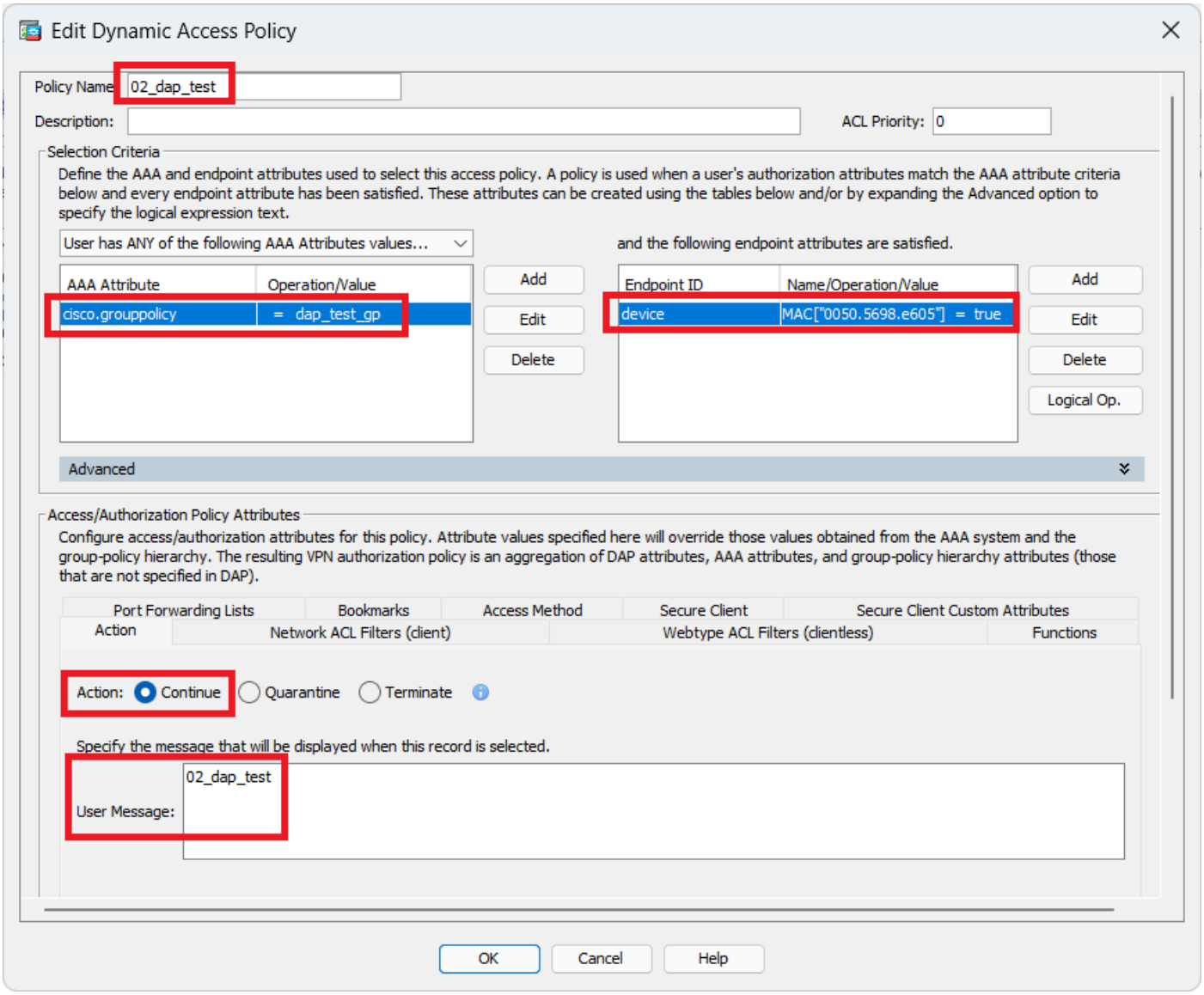
Configurar Diretiva de Grupo para Registro DAP

Configure o endereço MAC para o atributo de ponto final.



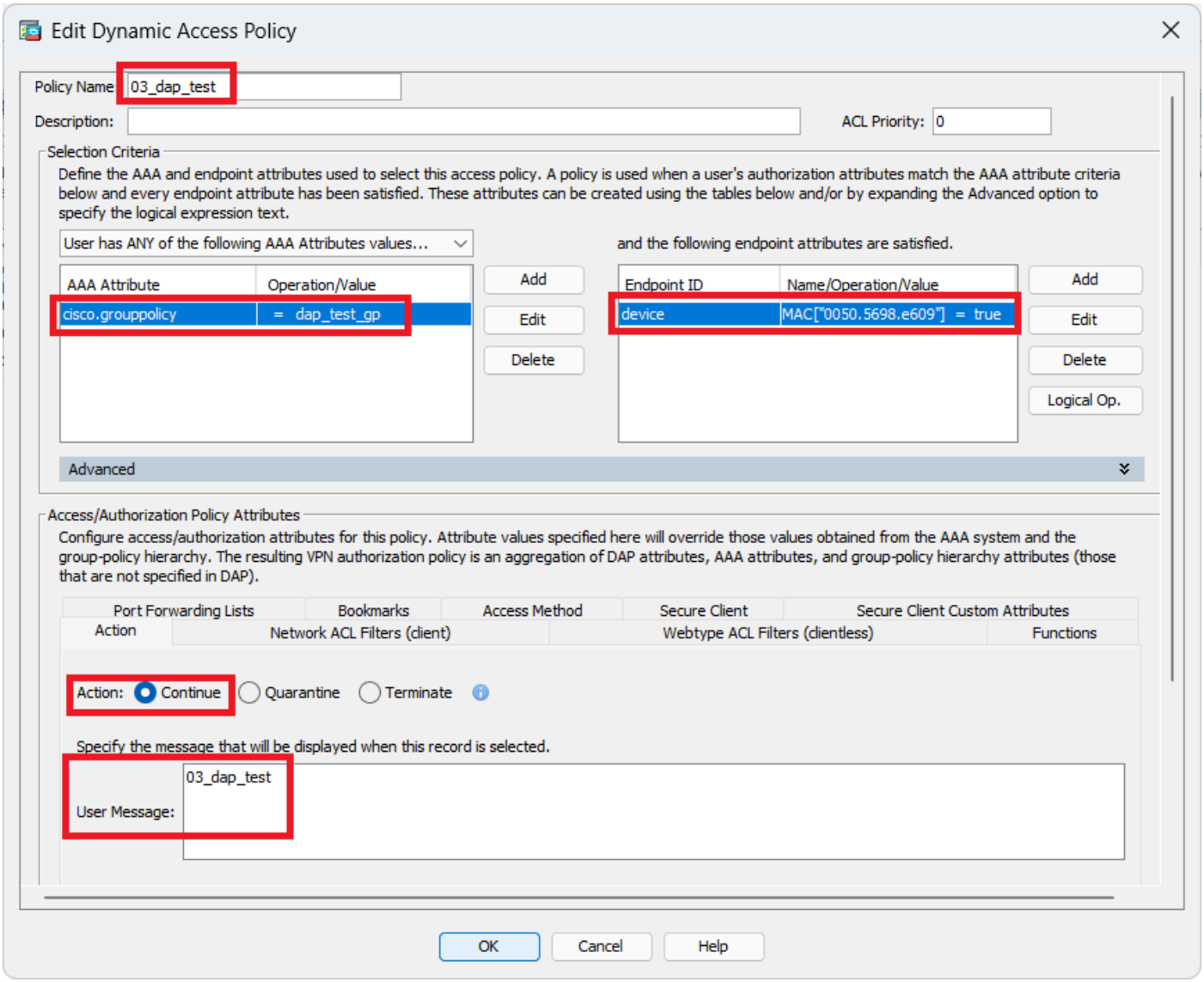
Configurar Condição MAC para DAP

2. Configure o segundo DAP chamado 02_dap_test.



Configurar Segundo DAP

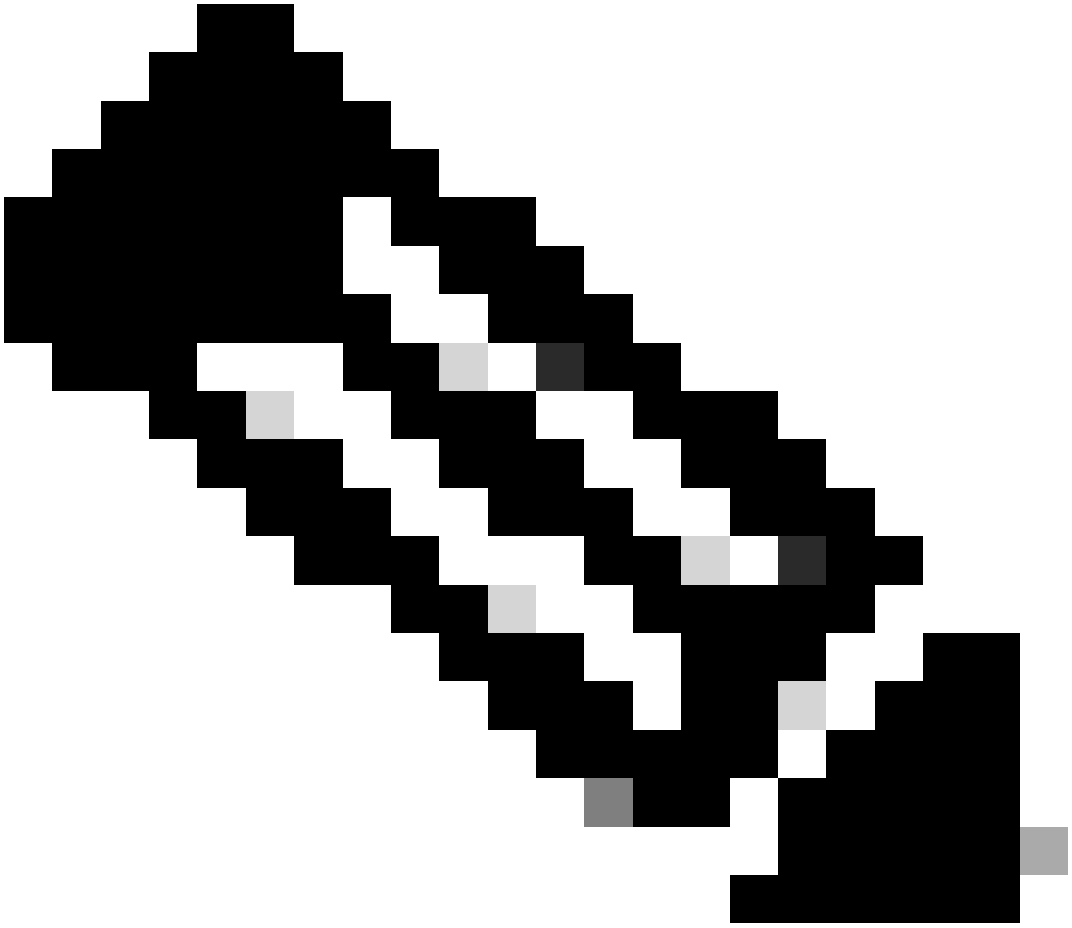
3. Configure o terceiro DAP chamado 03_dap_test.



Configurar terceiro DAP

4. Use o **more flash:/dap.xml** comando para confirmar a configuração dos registros LDAP em dap.xml.

Os detalhes dos registros DAP definidos no ASDM são salvos na flash do ASA como dap.xml. Após a conclusão dessas configurações, três registros DAP são gerados em dap.xml. Você pode confirmar os detalhes de cada registro DAP em dap.xml.



Observação: a ordem na qual o DAP está sendo correspondido é a ordem de exibição em dap.xml. O DAP (DfltAccessPolicy) padrão é correspondido pela última vez.

<#root>

ciscoasa#

more flash:/dap.xml

<dapRecordList> <dapRecord> <dapName> <value>

01_dap_test

</value> <--- 1st DAP name </dapName> <dapViewsRelation> <value>and</value> </dapViewsRelation> <dapBas

dap_test_gp

</value> <--- 1st DAP group policy <operation>EQ</operation> <type>caseless</type> </attr> </dapSelecti

endpoint.device.MAC["0050.5698.e608"]

</name> <--- 1st DAP MAC Address condition <value>true</value> <type>caseless</type> <operation>EQ</ope

02_dap_test

</value> <--- 2nd DAP name </dapName> <dapViewsRelation> <value>and</value> </dapViewsRelation> <dapBas

dap_test_gp

</value> <--- 2nd DAP group policy <operation>EQ</operation> <type>caseless</type> </attr> </dapSelecti

endpoint.device.MAC["0050.5698.e605"]

</name> <--- 2nd DAP MAC Address condition <value>true</value> <type>caseless</type> <operation>EQ</ope

03_dap_test

</value> <--- 3rd DAP name </dapName> <dapViewsRelation> <value>and</value> </dapViewsRelation> <dapBas

dap_test_gp

</value> <--- 3rd DAP group policy <operation>EQ</operation> <type>caseless</type> </attr> </dapSelecti

endpoint.device.MAC["0050.5698.e609"]

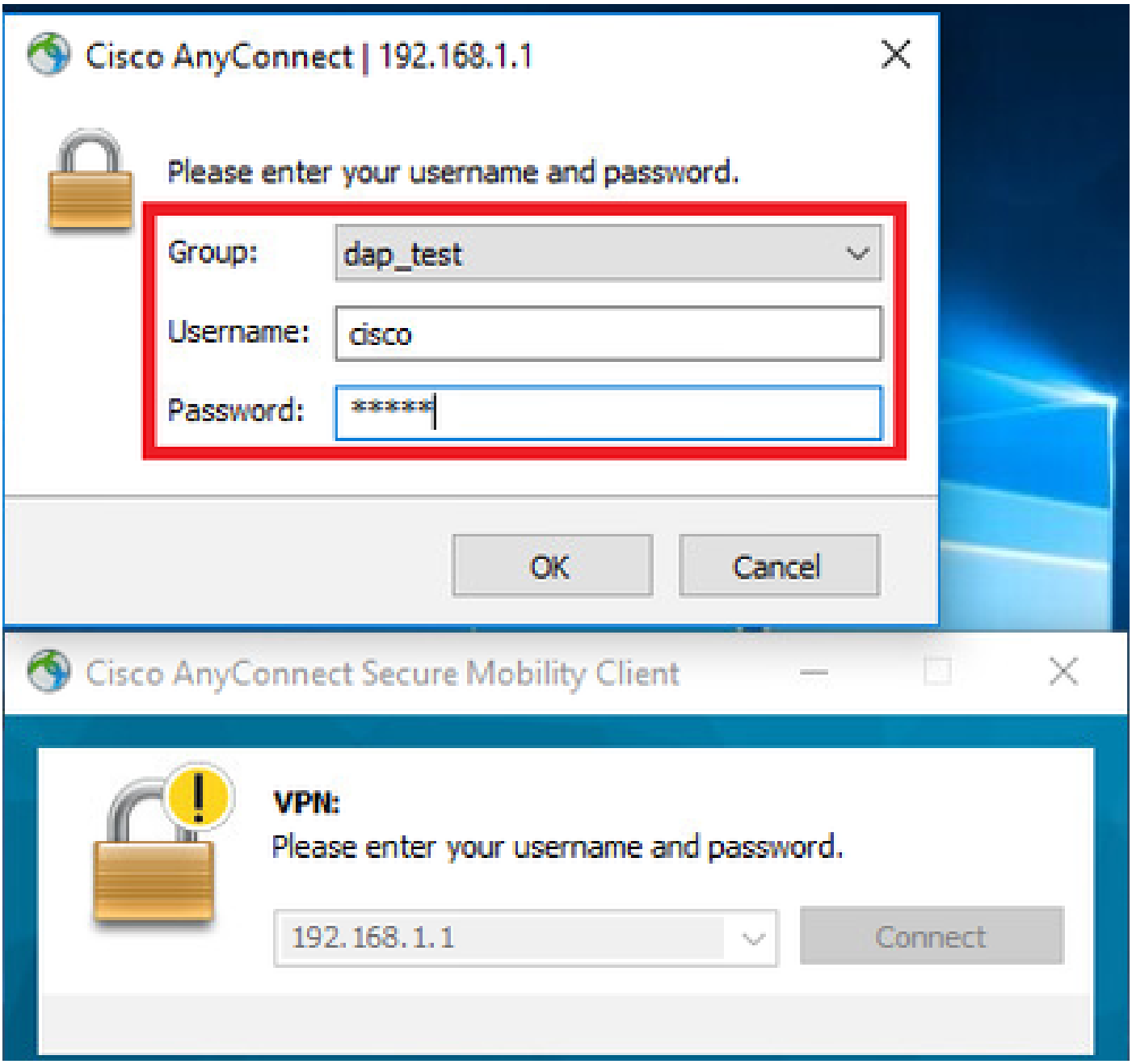
</name> <--- 3rd DAP MAC Address condition <value>true</value> <type>caseless</type> <operation>EQ</ope

Verificar

Cenário 1. Somente um DAP é correspondido

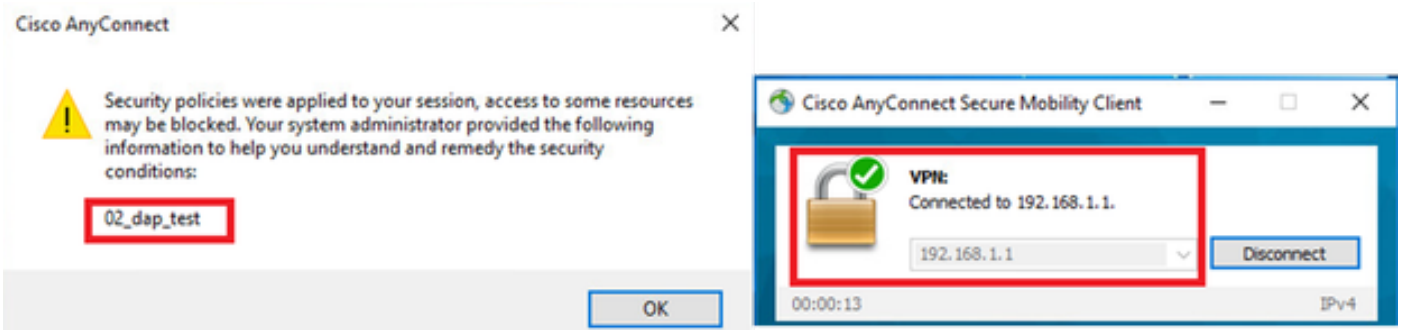
1. Certifique-se de que o MAC do ponto final seja 0050.5698.e605, que corresponde à condição MAC em 02_dap_test.

2. No endpoint, execute a conexão do Anyconnect e insira o nome de usuário e a senha.



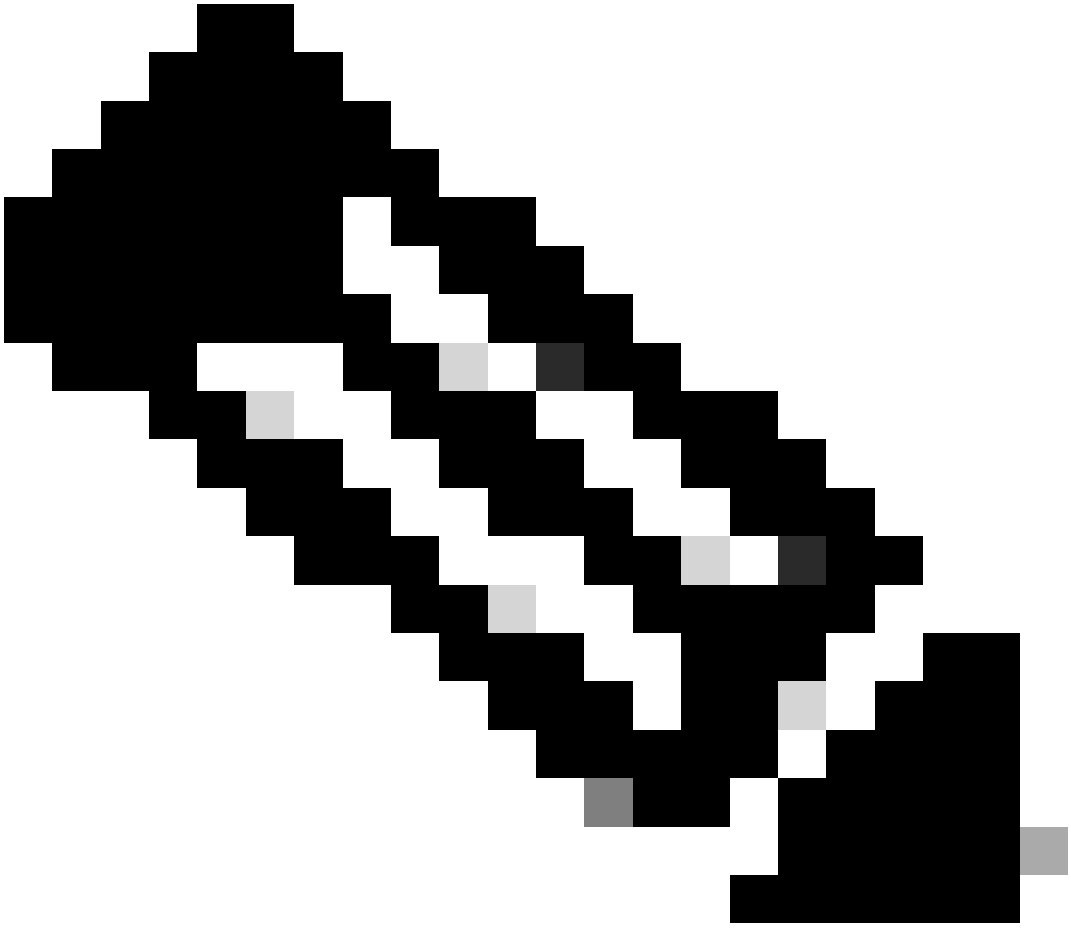
Inserir nome de usuário e senha

3. Na interface do usuário do Anyconnect, confirme se 02_dap_test foi correspondido.



Confirmar mensagem do usuário na interface do usuário

4. No syslog ASA, confirme se 02_dap_test foi correspondido.



Observação: certifique-se de que debug dap trace esteja habilitado no ASA.

<#root>

Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["

0050.5698.e605

"] = "true"

Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 11:46:11: %ASA-4-711001:

Selected DAPs

: ,

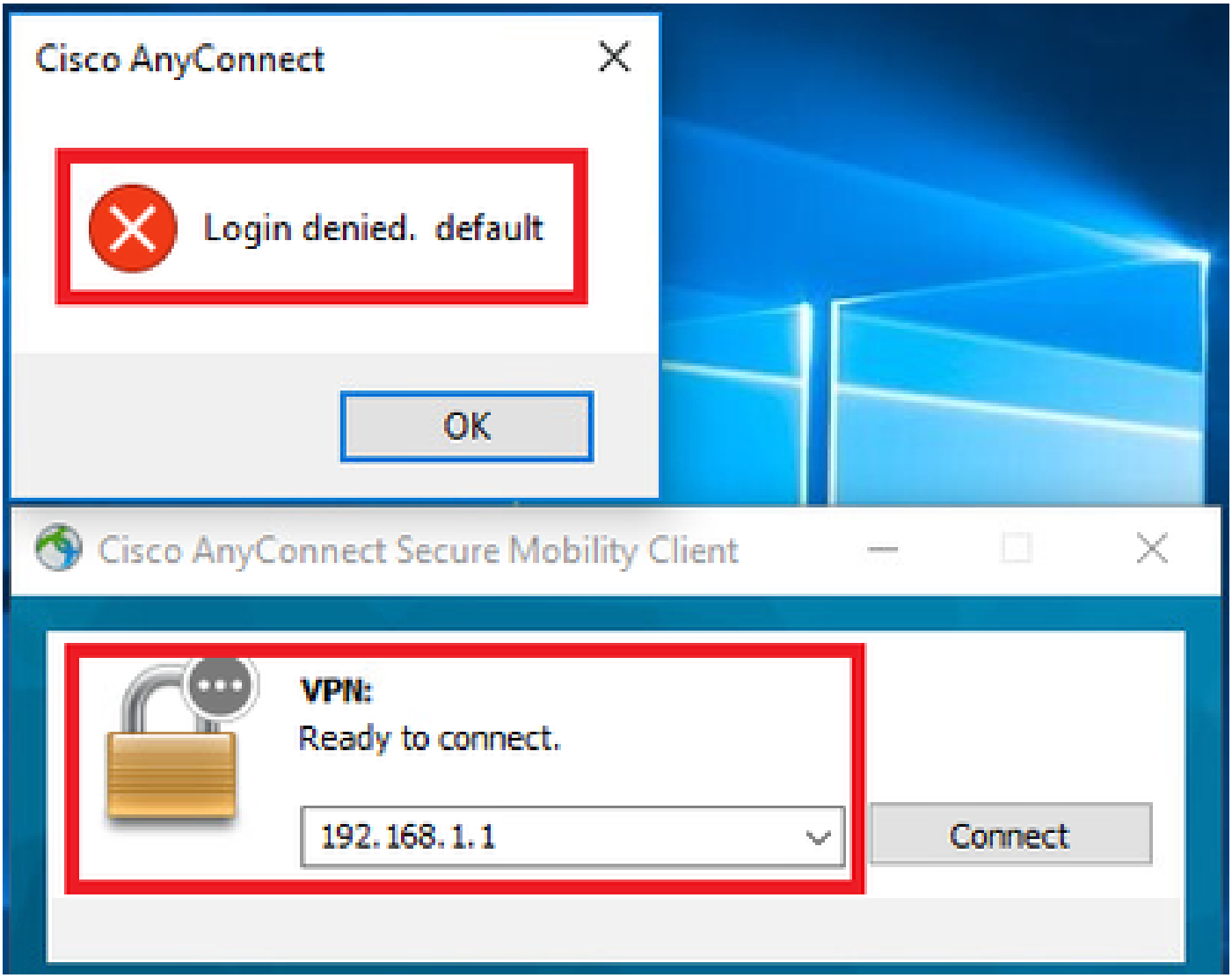
```
02_dap_test

 Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Dec 30 2023 11:46:11: %ASA-4-711001: dap_process_selec
selected 1 records

 Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 11:46:11: %ASA-4-711001:
```

Cenário 2. O DAP padrão é correspondente

1. Altere o valor de endpoint.device.MAC em 02_dap_test para 0050.5698.e607, que não corresponde ao MAC do endpoint.

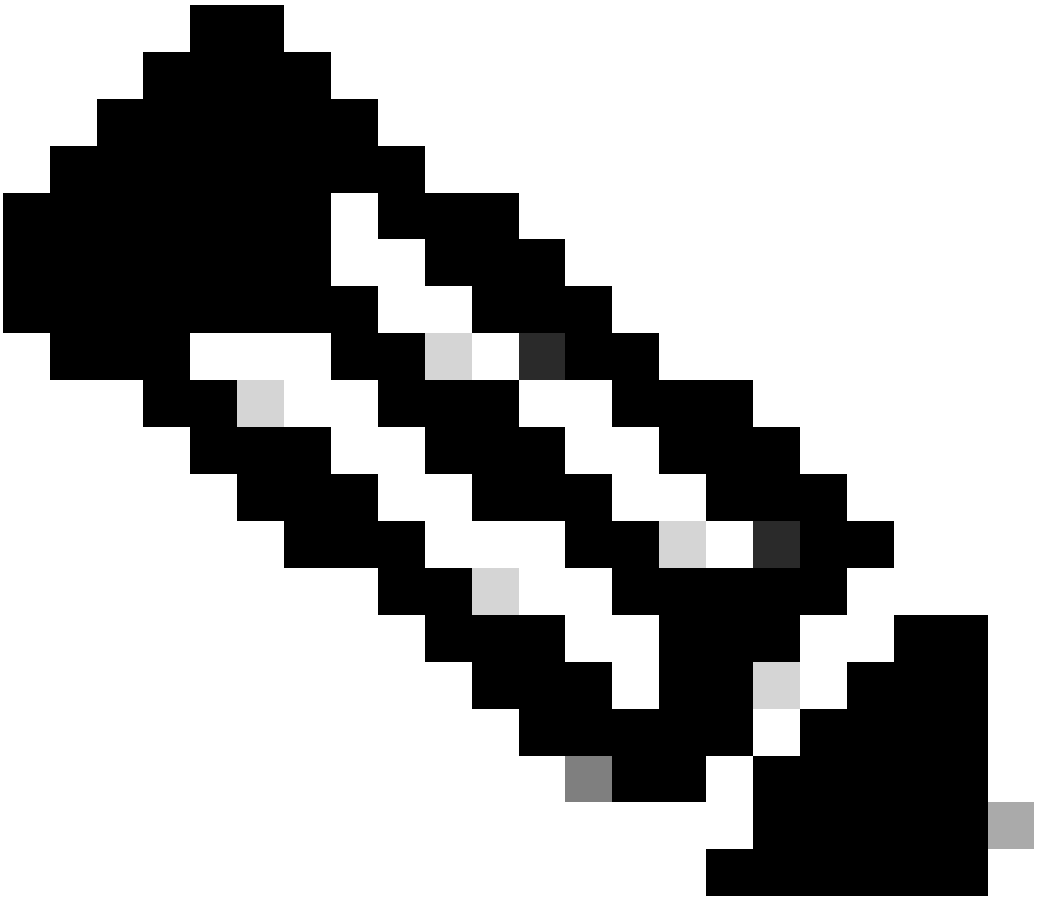
2. No endpoint, execute a conexão do Anyconnect e insira o nome de usuário e a senha.

3. Confirme se a conexão do Anyconnect foi negada.



Confirmar mensagem do usuário na interface do usuário

4. No syslog do ASA, confirme se DfltAccessPolicy é correspondido.



Observação: por padrão , a ação de DfltAccessPolicy é Terminar.

<#root>

Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["

0050.5698.e605

"] = "true"

Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 12:13:39: %ASA-4-711001: S
Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Dec 30 2023 12:13:39: %ASA-4-711001: dap_process_selecte

selected 0 records

Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 12:13:39: %ASA-4-711001:

Selected DAPs

:

DfltAccessPolicy

Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 12:13:39: %ASA-4-711001: DA

Cenário 3. Vários DAPs (Ação : Continuar) são correspondidos

1. Altere a ação e o atributo em cada DAP.

- 01_dap_test:
  dapSelection (endereço MAC) = endpoint.device.MAC[0050.5698.e605] = MAC do endpoint Anyconnect
  Ação = **Continuar**
- 02_dap_test:

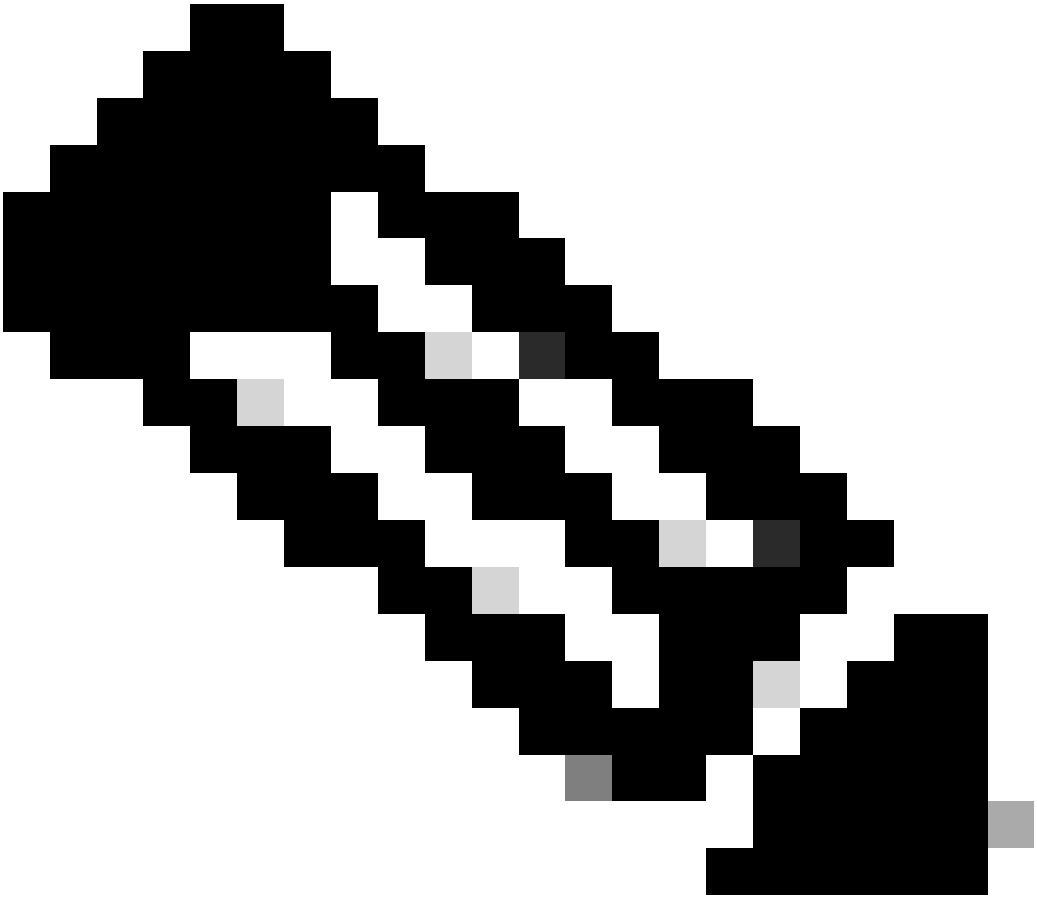
dapSelection (Nome do Host) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Nome do Host do Endpoint Anyconnect
Ação = **Continuar**

·Apagar o registro 03_dap_test DAP

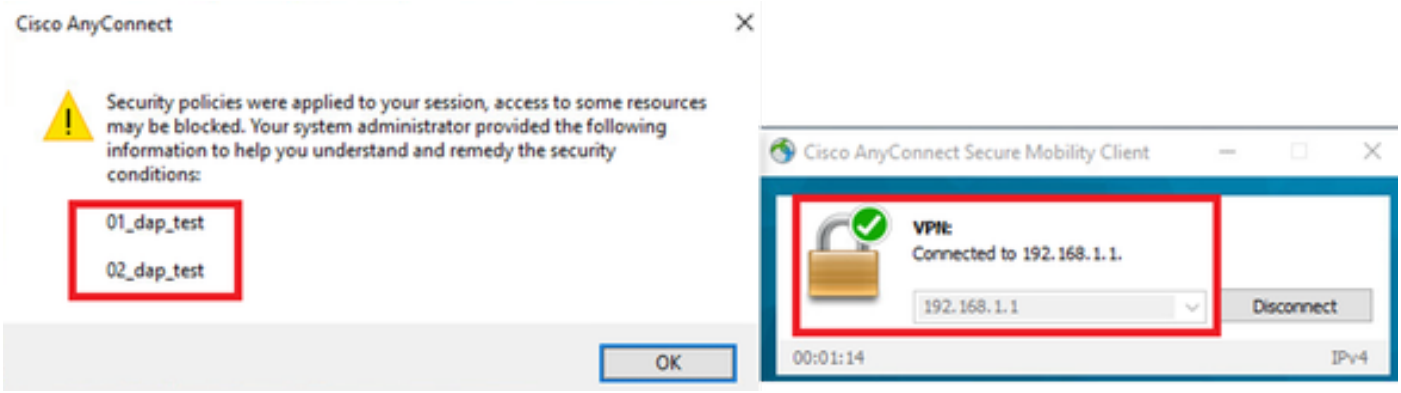
2. No endpoint, execute a conexão do Anyconnect e insira o nome de usuário e a senha.

3. Na interface do usuário do Anyconnect, confirme se todos os 2 DAPs são correspondentes

---



Observação: se uma conexão corresponder a vários DAPs, as mensagens de usuário de vários DAPs serão integradas e exibidas juntas na interface do usuário do Anyconnect.



Confirmar mensagem do usuário na interface do usuário

4. No syslog do ASA, confirme se todos os 2 DAPs são correspondentes.

```
<#root>

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["

0050.5698.e605

"] = "true"
Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:49:02: %ASA-4-711001: endpoint.device.ho

DESKTOP-VCKHRG1

"
Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Username: cisco, Feb 01 2024 08:49:02: %ASA-4-711001: S

01_dap_test
```

,

02_dap_test

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:49:02: %ASA-4-711001: dap_process_select

selected 2 records

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Username: cisco, Feb 01 2024 08:49:02: %ASA-4-711001: DA

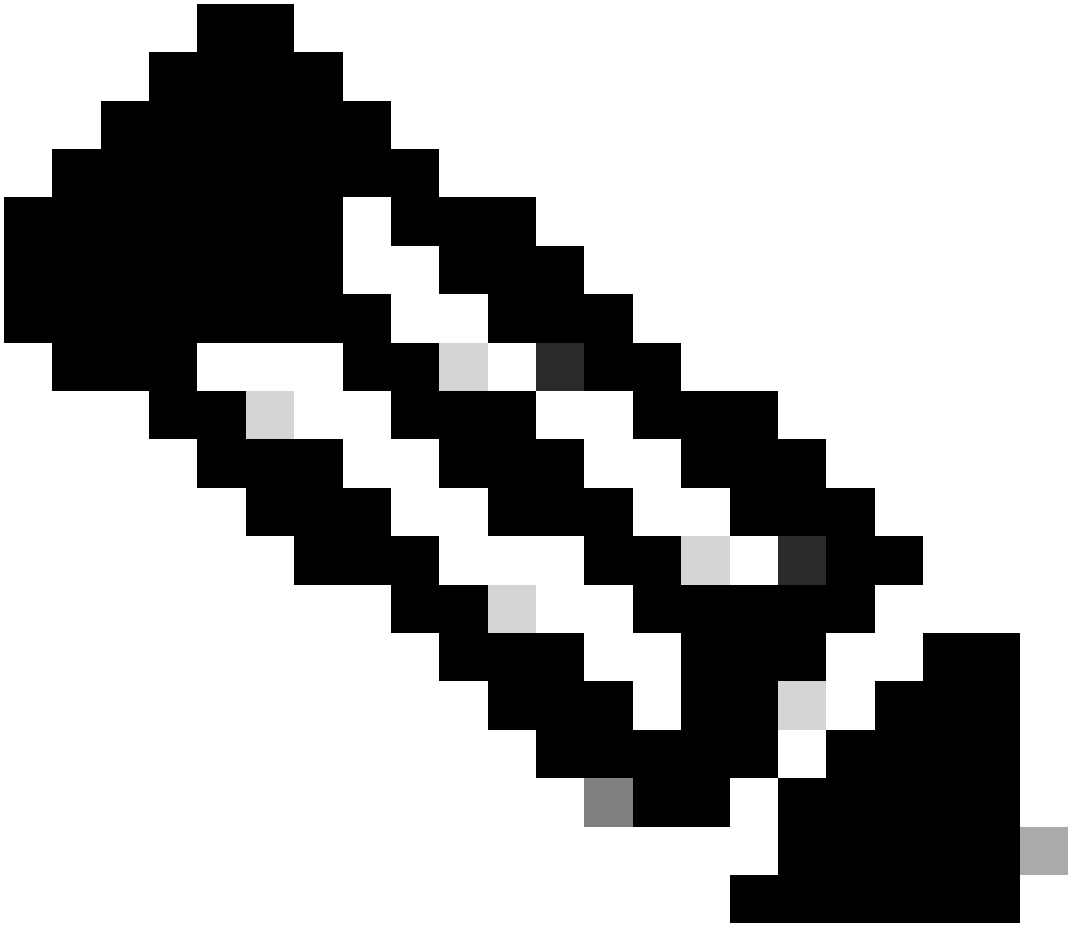
Cenário4. Vários DAPs (Ação:Terminar) são correspondidos

1. Altere a ação de 01_dap_test.

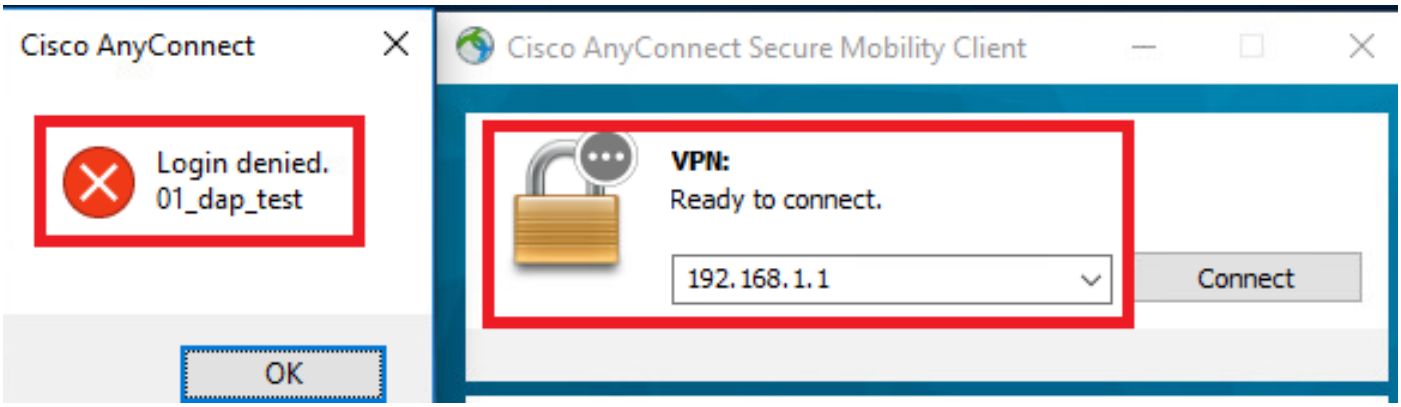
·01_dap_test:
dapSelection (endereço MAC) = endpoint.device.MAC[0050.5698.e605] = MAC do endpoint Anyconnect
Ação = **Finalizar**
·02_dap_test:
dapSelection (Nome do Host) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Nome do Host do Endpoint Anyconnect
Ação = **Continuar**

2. No endpoint, execute a conexão do Anyconnect e insira o nome de usuário e a senha.

3. Na interface do usuário do Anyconnect, confirme se somente **01_dap_test** é correspondido.



Observação: uma conexão que está sendo combinada com o registro DAP que foi definido para encerrar a ação. Os registros subsequentes não serão mais correspondidos após a ação de término.



Confirmar mensagem do usuário na interface do usuário

4. No syslog do ASA, confirme se somente 01_dap_test foi correspondido.

```
<#root>

Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["

0050.5698.e605

"] = "true"
Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.ho

DESKTOP-VCKHRG1

" Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Username: cisco, Feb 01 2024 08:55:37: %ASA-4-711001:

01_dap_test

 Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: dap_process_selec

selected 1 records

 Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Username: cisco, Feb 01 2024 08:55:37: %ASA-4-711001:
```

Troubleshooting Geral

Esses logs de depuração ajudam a confirmar o comportamento detalhado do DAP no ASA.

debug dap trace

debug dap trace errors

```
<#root>

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["0050.5698.e605"] = "true" Feb

Selected DAPs

: ,01_dap_test,02_dap_test Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:49:02: %ASA-4
```

Informações Relacionadas

https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/108000-dap-deploy-guide.html#toc-hId-981572249

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.