

# Implementación de ASA DAP para identificar la dirección MAC para AnyConnect

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración en ASA](#)

[Configuración en ASDM](#)

[Verificación](#)

[Situación 1. Sólo se encuentra coincidente un DAP](#)

[Situación 2. El DAP predeterminado coincide](#)

[Situación 3. Se han encontrado varios DAP \(acción: continuar\)](#)

[Situación 4. Se han encontrado varios DAP \(Acción :Terminar\)](#)

[Resolución general de problemas](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe cómo configurar las políticas de acceso dinámico (DAP) a través de ASDM, para verificar la dirección MAC del dispositivo utilizado para la conexión de AnyConnect.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:  
Configuración de Cisco Anyconnect y Hostscan

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

ASAv 9.18 (4)

ASDM 7.20 (1)

Anyconnect 4.10.07073

Hostscan 4.10.07073

## Windows 10

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

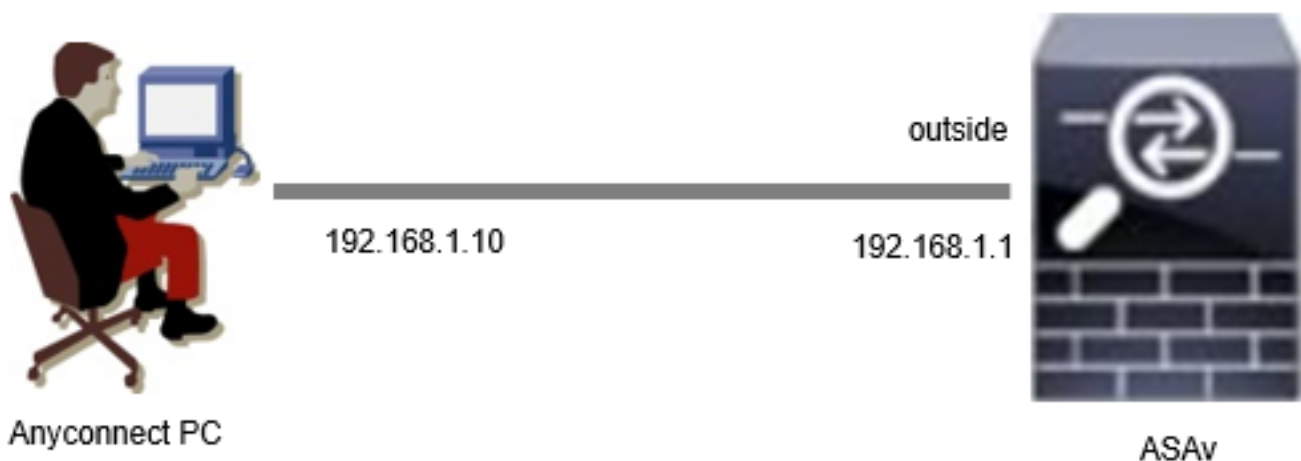
## Antecedentes

HostScan es un módulo de software que proporciona a AnyConnect Secure Mobility Client la capacidad de aplicar políticas de seguridad en la red. Durante el proceso de Hostscan, se recopilan varios detalles sobre el dispositivo cliente y se informa al dispositivo de seguridad adaptable (ASA). Estos detalles incluyen el sistema operativo del dispositivo, el software antivirus, el software de firewall, la dirección MAC y mucho más. La función de políticas de acceso dinámicas (DAP) permite a los administradores de red configurar políticas de seguridad para cada usuario. El atributo `endpoint.device.MAC` de DAP se puede utilizar para comparar o comprobar la dirección MAC del dispositivo cliente con las políticas predefinidas.

## Configurar

### Diagrama de la red

Esta imagen muestra la topología utilizada para el ejemplo de este documento.



Diagrama

### Configuración en ASA

Esta es la configuración mínima en 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
```

## Configuración en ASDM

Esta sección describe cómo configurar el registro DAP en ASDM. En este ejemplo, establezca 3 registros DAP que utilicen el atributo endpoint.device.MAC como condición.

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

1. Configure el primer DAP denominado 01\_dap\_test.

Vaya a Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies . Haga clic en Agregar y establezca el Nombre de la política, el Atributo AAA, los atributos de punto final, Acción, Mensaje del usuario, como se muestra en la imagen:

**Edit Dynamic Access Policy**

Policy Name: **01\_dap\_test**

Description: \_\_\_\_\_ ACL Priority: 0

**Selection Criteria**  
 Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ALL of the following AAA Attributes values... and the following endpoint attributes are satisfied.

AAA Attribute	Operation/Value	Endpoint ID	Name/Operation/Value
disco.grouppolicy	= dap_test_gp	device	MAC["0050.5698.e608"] = true

Advanced

**Access/Authorization Policy Attributes**  
 Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Port Forwarding Lists | Bookmarks | Access Method | Secure Client | Secure Client Custom Attributes  
 Action | Network ACL Filters (client) | Webytype ACL Filters (clientless) | Functions

Action:  Continue  Quarantine  Terminate

Specify the message that will be displayed when this record is selected.

User Message: **01\_dap\_test**

OK Cancel Help

Configurar el primer DAP

Configure la política de grupo para el atributo AAA.

**Add AAA Attribute** [X]

AAA Attribute Type: Cisco

Group Policy: = dap\_test\_gp

Assigned IPv4 Address: =

Assigned IPv6 Address: =

Connection Profile: = DefaultRAGroup

Username: =

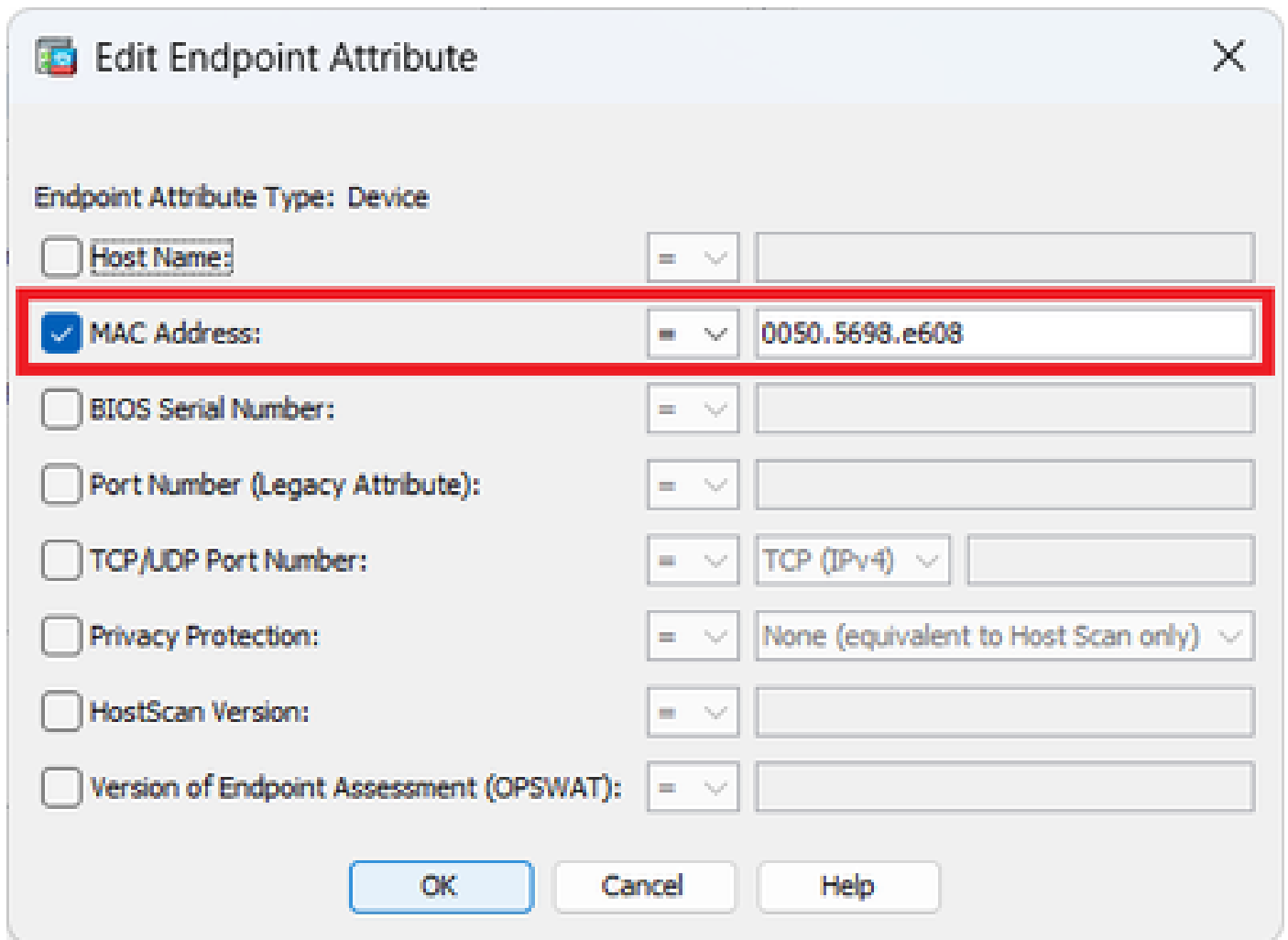
Username2: =

SCEP Required: = true

OK Cancel Help

Configurar la directiva de grupo para el registro DAP

Configure la dirección MAC para el atributo de terminal.

The image shows a dialog box titled "Edit Endpoint Attribute" with a close button (X) in the top right corner. The "Endpoint Attribute Type" is set to "Device". There are seven attribute rows, each with a checkbox, a label, an equals sign, a dropdown arrow, and a text input field. The "MAC Address" row is highlighted with a red border and has its checkbox checked and its value set to "0050.5698.e608".

Attribute Type	Value
Host Name:	
<input checked="" type="checkbox"/> MAC Address:	0050.5698.e608
BIOS Serial Number:	
Port Number (Legacy Attribute):	
TCP/UDP Port Number:	TCP (IPv4)
Privacy Protection:	None (equivalent to Host Scan only)
HostScan Version:	
Version of Endpoint Assessment (OPSWAT):	

Buttons: OK, Cancel, Help

Configuración de la condición MAC para DAP

2. Configure el segundo DAP denominado 02\_dap\_test.

**Edit Dynamic Access Policy**

Policy Name: **02\_dap\_test**

Description: \_\_\_\_\_ ACL Priority: 0

**Selection Criteria**  
 Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ANY of the following AAA Attributes values... and the following endpoint attributes are satisfied.

AAA Attribute	Operation/Value	Endpoint ID	Name/Operation/Value
<b>disco.grouppolicy</b>	<b>= dap_test_gp</b>	<b>device</b>	<b>MAC["0050.5698.e605"] = true</b>

Advanced

**Access/Authorization Policy Attributes**  
 Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Port Forwarding Lists | Bookmarks | Access Method | Secure Client | Secure Client Custom Attributes  
 Action | Network ACL Filters (client) | Webytype ACL Filters (clientless) | Functions

Action:  Continue  Quarantine  Terminate

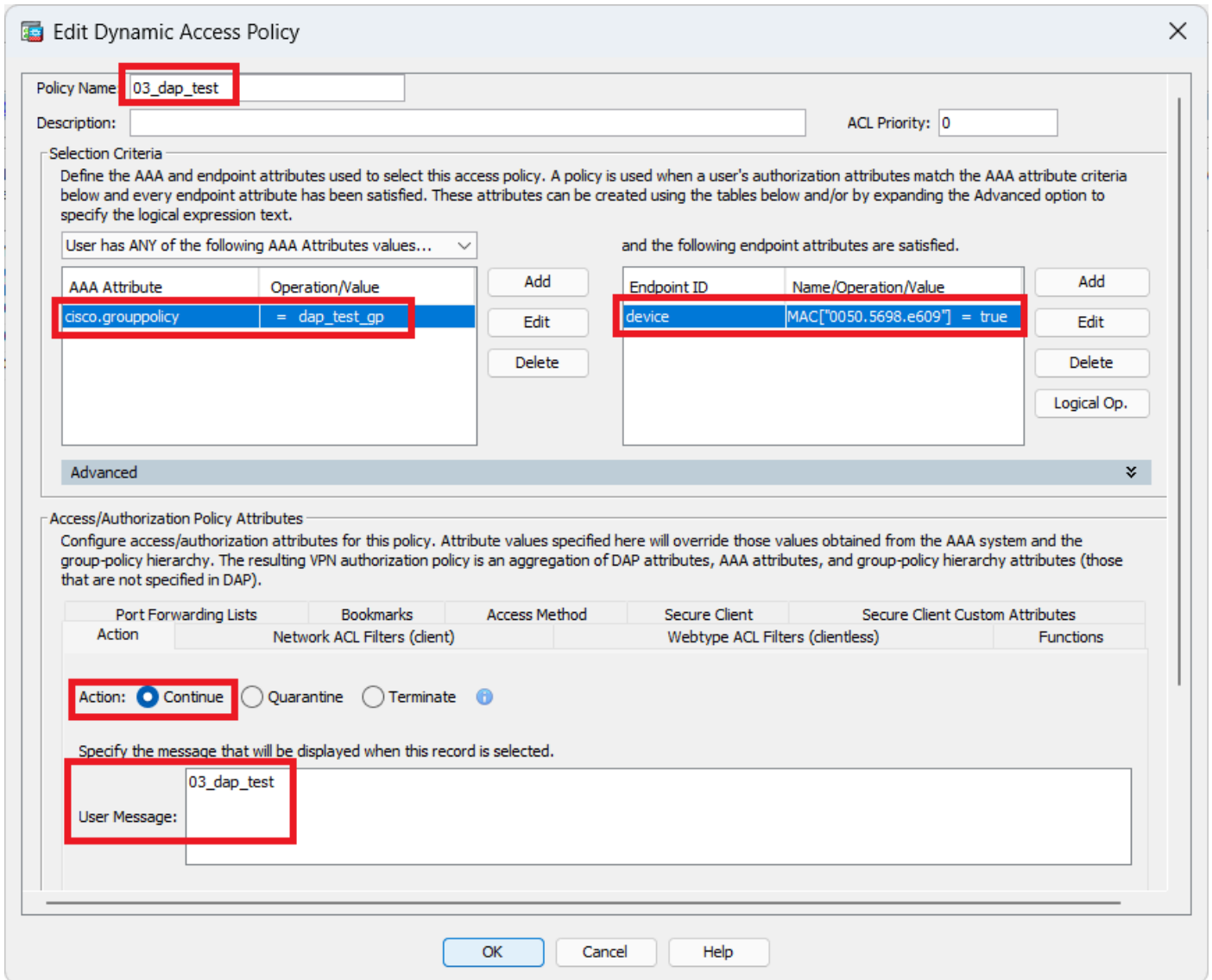
Specify the message that will be displayed when this record is selected.

User Message: **02\_dap\_test**

OK Cancel Help

Configuración del segundo DAP

3. Configure el tercer DAP denominado 03\_dap\_test.



Configuración del tercer DAP

4. Utilice el **more flash:/dap.xml** comando para confirmar la configuración de los registros DAP en dap.xml.

Los detalles de los registros DAP establecidos en ASDM se guardan en la memoria flash ASA como dap.xml. Una vez completada esta configuración, se generan tres registros DAP en dap.xml. Puede confirmar los detalles de cada registro DAP en dap.xml.





**Nota:** El orden en el que se realiza la correspondencia de DAP es el orden de visualización en dap.xml. El DAP predeterminado (DfltAccessPolicy) es el último que coincide.

---

```
<#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
```

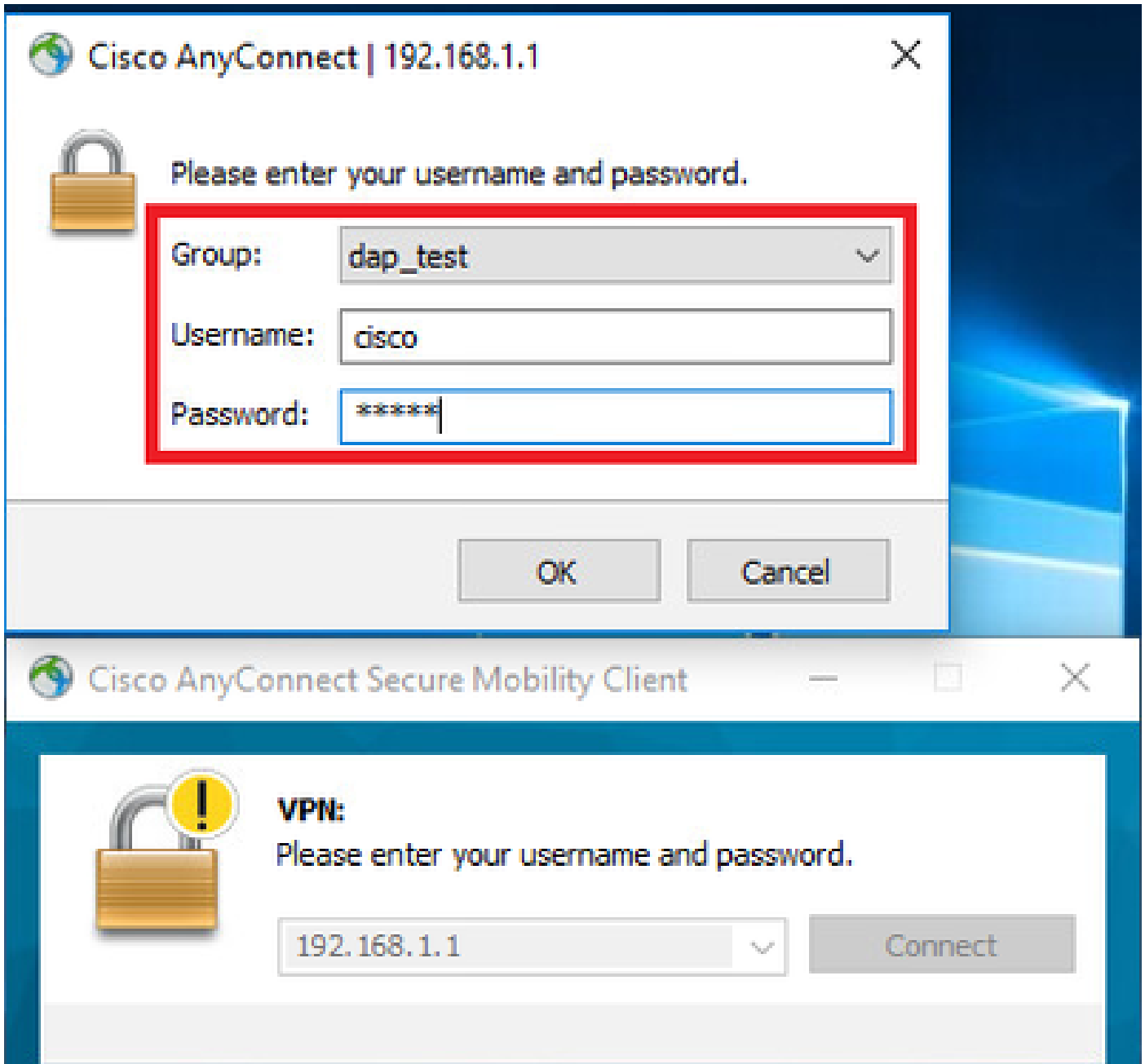
```
endpoint.device.MAC["0050.5698.e609"]
```

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

Verificación

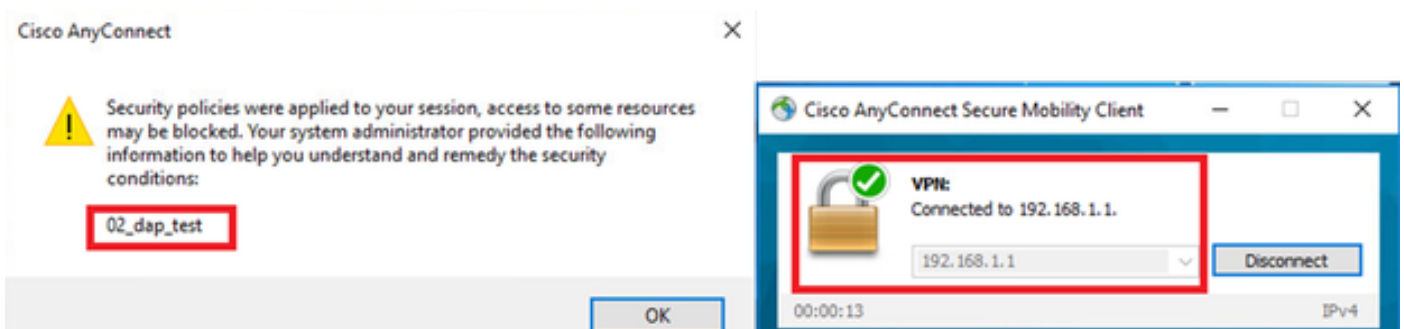
Situación 1. Sólo se encuentra coincidente un DAP

1. Asegúrese de que el MAC del punto final sea 0050.5698.e605 que coincida con la condición MAC en 02\_dap\_test.
2. En el terminal, ejecute Anyconnect connection e introduzca el nombre de usuario y la contraseña.



Introducir nombre de usuario y contraseña

3. En la interfaz de usuario de Anyconnect, confirme que 02\_dap\_test coincide.



Confirmar mensaje de usuario en IU

4. En el syslog ASA, confirme que 02\_dap\_test coincide.

---

**Nota:** Asegúrese de que debug dap trace esté habilitado en 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
```

```
: ,
```

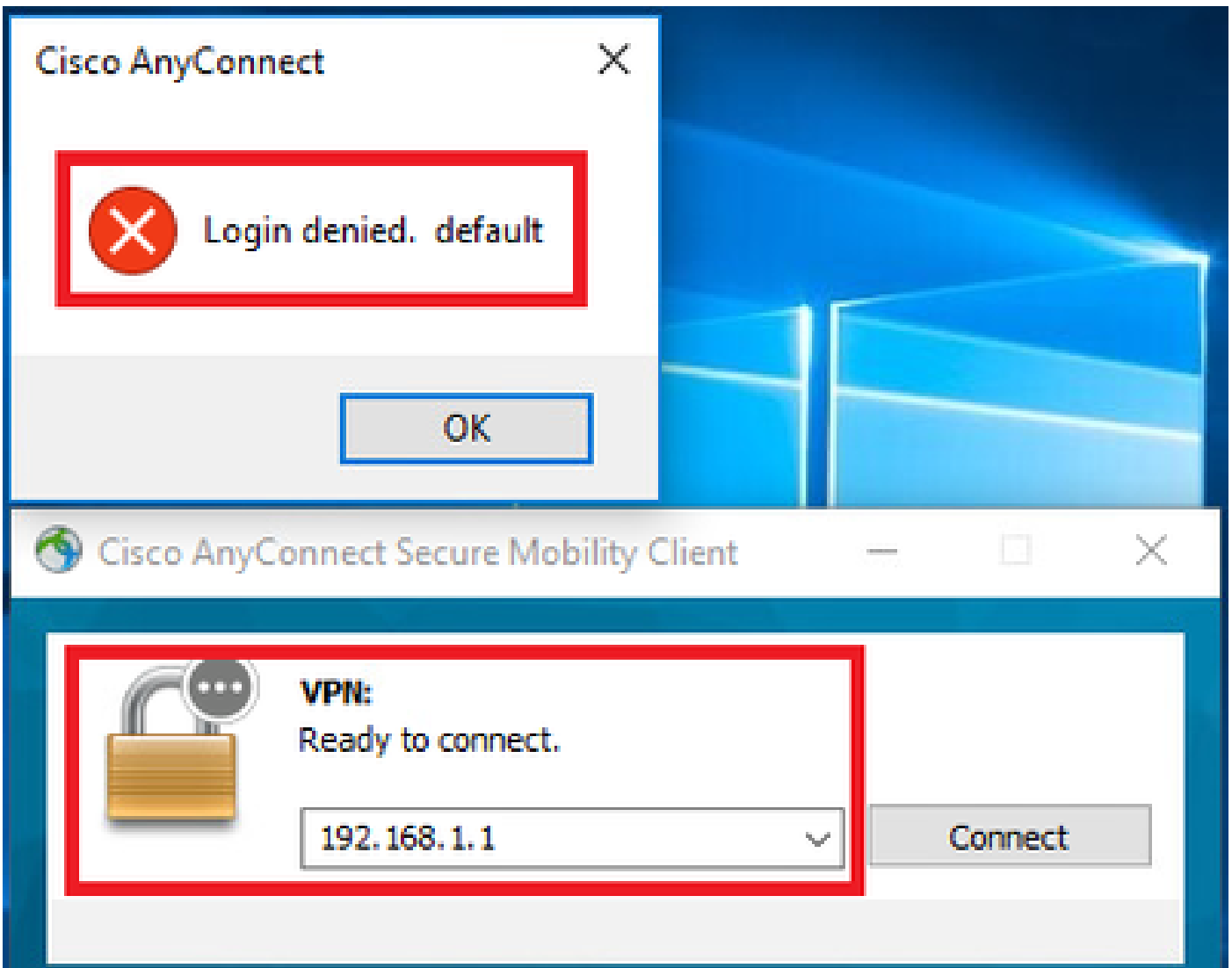
02\_dap\_test

```
Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Dec 30 2023 11:46:11: %ASA-4-711001: dap_process_select  
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: I
```

Situación 2. El DAP predeterminado coincide

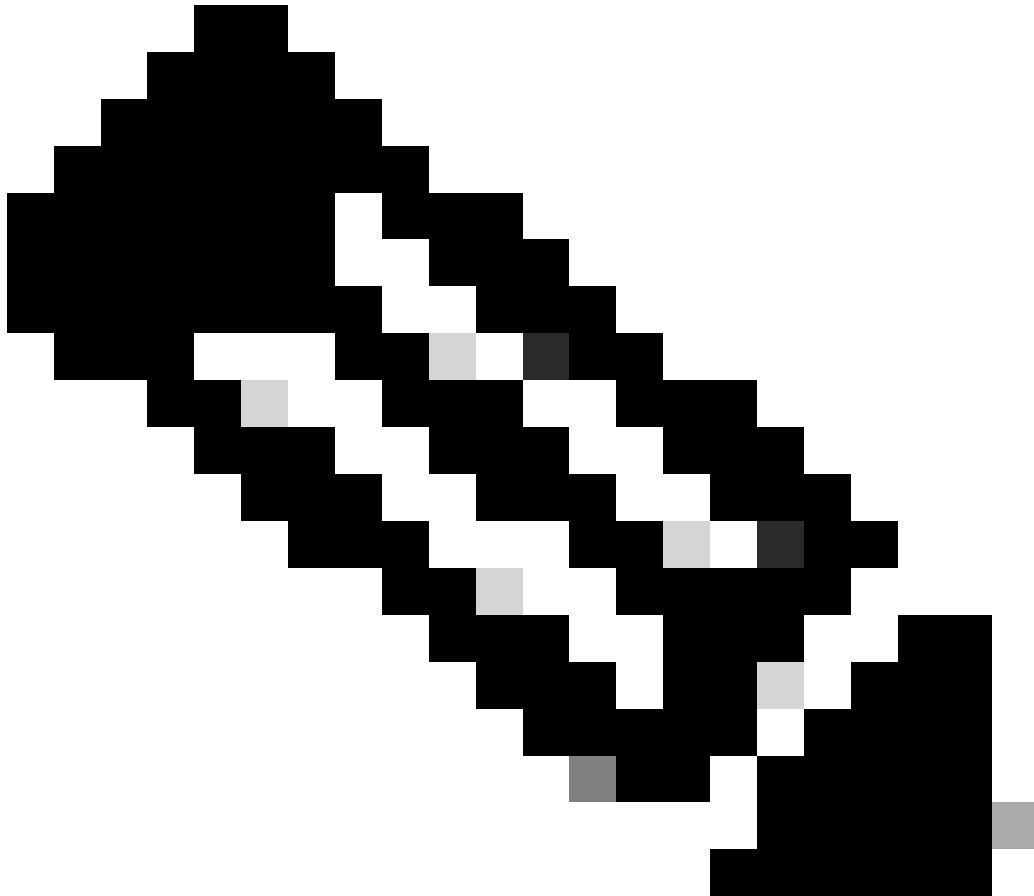
1. Cambie el valor de endpoint.device.MAC en 02\_dap\_test a 0050.5698.e607 que no coincide con MAC del terminal.
2. En el terminal, ejecute Anyconnect connection e introduzca el nombre de usuario y la contraseña.
3. Confirme que se ha denegado la conexión Anyconnect.



Confirmar mensaje de usuario en IU

4. En ASA syslog, confirme que DfltAccessPolicy coincide.

---



**Nota:** De forma predeterminada , la acción de DfltAccessPolicy es Terminate.

---

<#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\_select

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: D

### Situación 3. Se han encontrado varios DAP (acción: continuar)

1. Cambie la acción y el atributo en cada DAP.

.01\_dap\_test:

dapSelection (dirección MAC) = endpoint.device.MAC[0050.5698.e605] = MAC del terminal Anyconnect

Acción = **Continuar**

.02\_dap\_test:

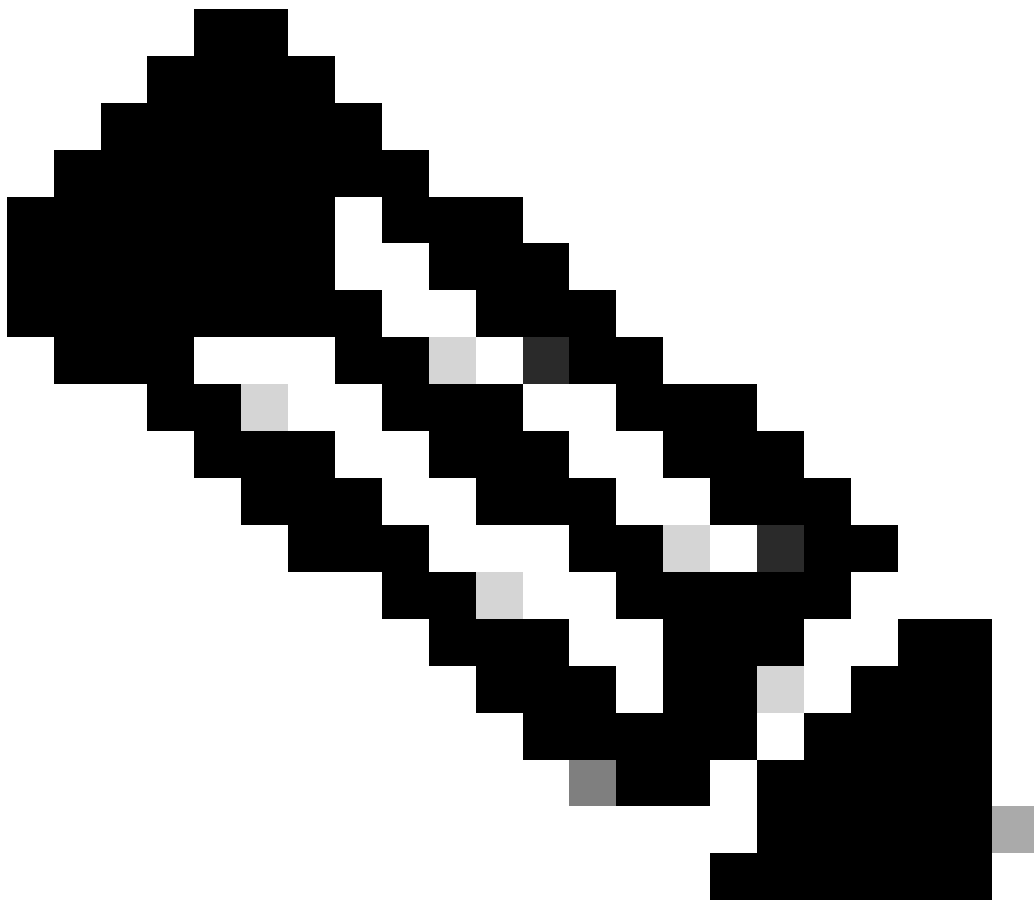
dapSelection (nombre de host) = terminal.device.hostname[DESKTOP-VCKHRG1] = nombre de host del terminal de Anyconnect

Acción = **Continuar**

·Eliminar registro DAP 03\_dap\_test

2. En el terminal, ejecute Anyconnect connection e introduzca el nombre de usuario y la contraseña.

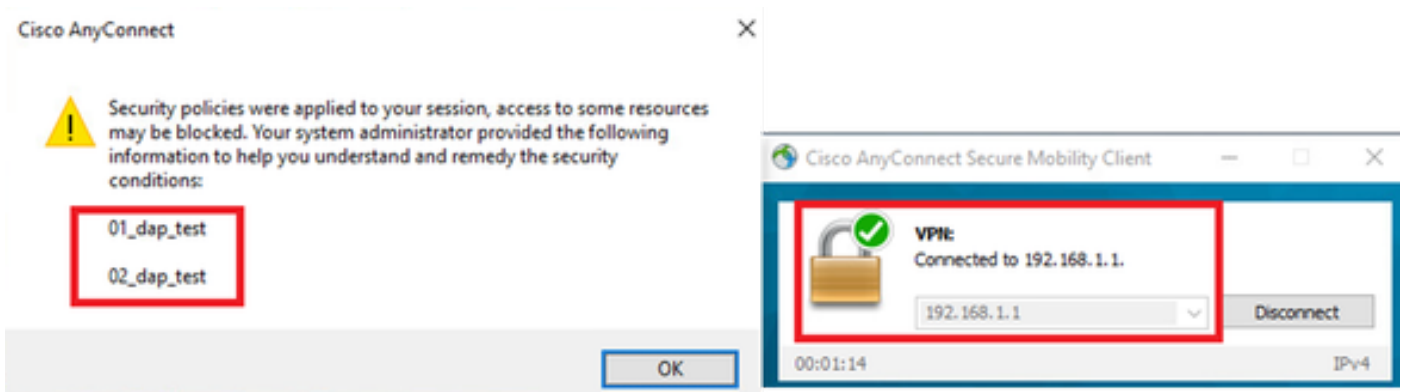
3. En la interfaz de usuario de Anyconnect, confirme que los 2 DAP coinciden



**Nota:** Si una conexión coincide con varios DAP, los mensajes de usuario de varios DAP se integrarán y se mostrarán juntos en la interfaz de usuario de Anyconnect.

---





Confirmar mensaje de usuario en IU

4. En el syslog ASA, confirme que los 2 DAP coinciden.

<#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: D

#### Situación4. Varios DAP (Acción :Terminar) coinciden

1. Cambie la acción de 01\_dap\_test.

·01\_dap\_test:

dapSelection (dirección MAC) = endpoint.device.MAC[0050.5698.e605] = MAC del terminal Anyconnect

Acción = **Terminar**

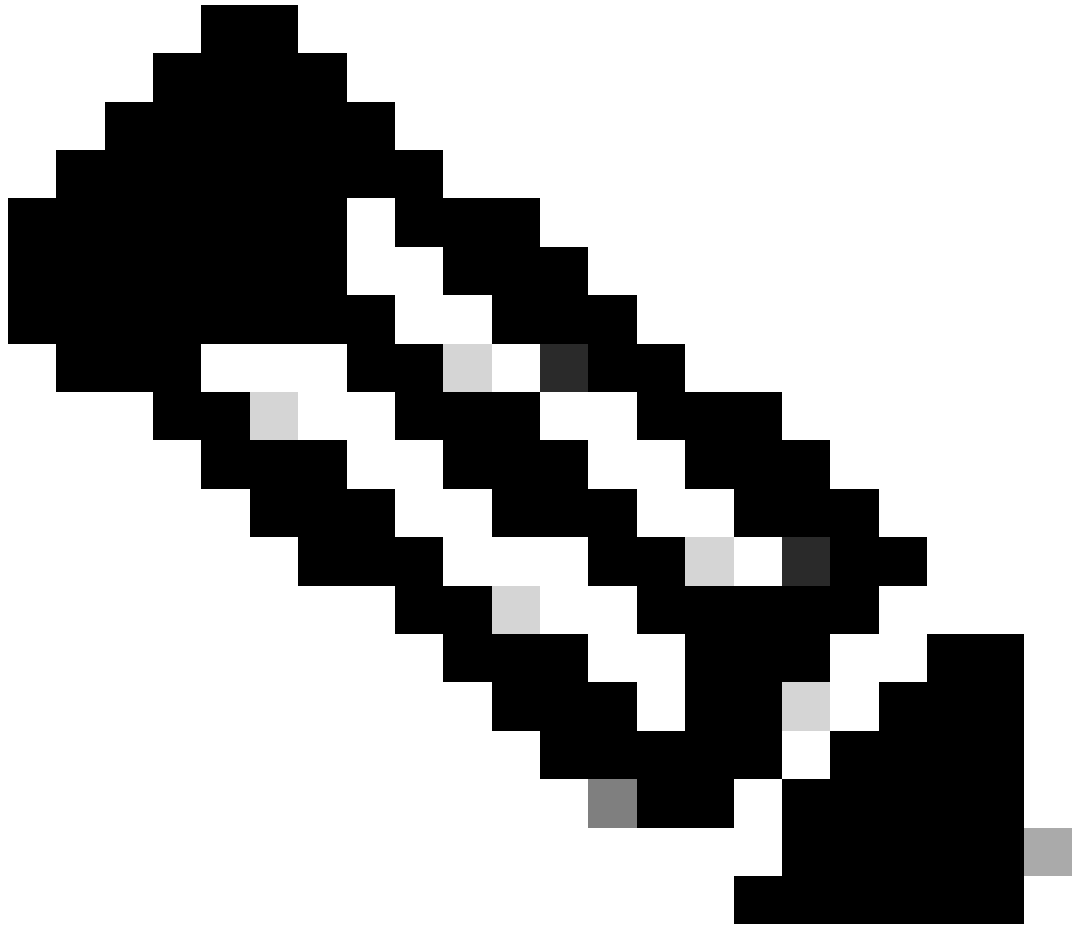
·02\_dap\_test:

dapSelection (nombre de host) = terminal.device.hostname[DESKTOP-VCKHRG1] = nombre de host del terminal de Anyconnect

Acción = **Continuar**

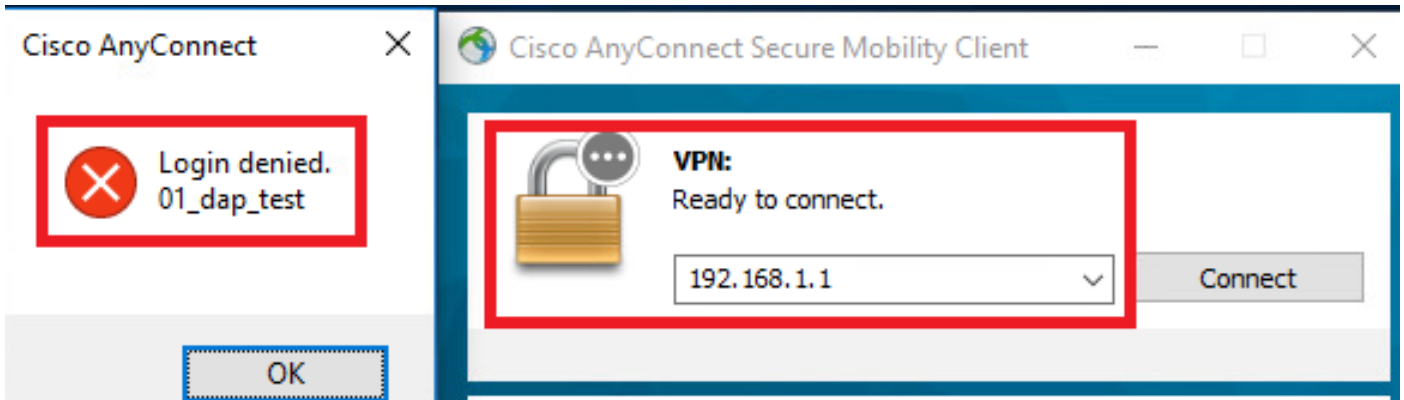
2. En el terminal, ejecute Anyconnect connection e introduzca el nombre de usuario y la contraseña.

3. En la interfaz de usuario de Anyconnect, confirme que sólo **01\_dap\_test** coincide.



**Nota:** Se está haciendo coincidir una conexión con el registro DAP que se ha configurado para finalizar la acción. Los registros subsiguientes ya no coinciden después de la acción de finalización.

---



Confirmar mensaje de usuario en IU

4. En el syslog de ASA, confirme que sólo 01\_dap\_test coincide.

<#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: I
```

Resolución general de problemas

Estos registros de depuración le ayudan a confirmar el comportamiento detallado de DAP en 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-
```

Información Relacionada

<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>

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).