Implementación de ASA DAP para identificar la dirección MAC para AnyConnect

Contenido

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.

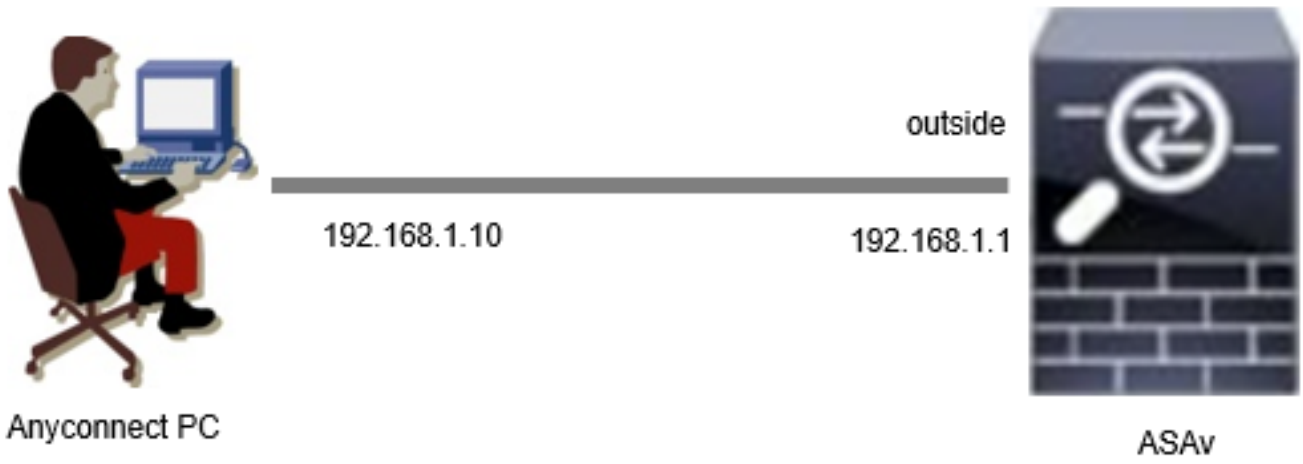
Antecedentes

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
```

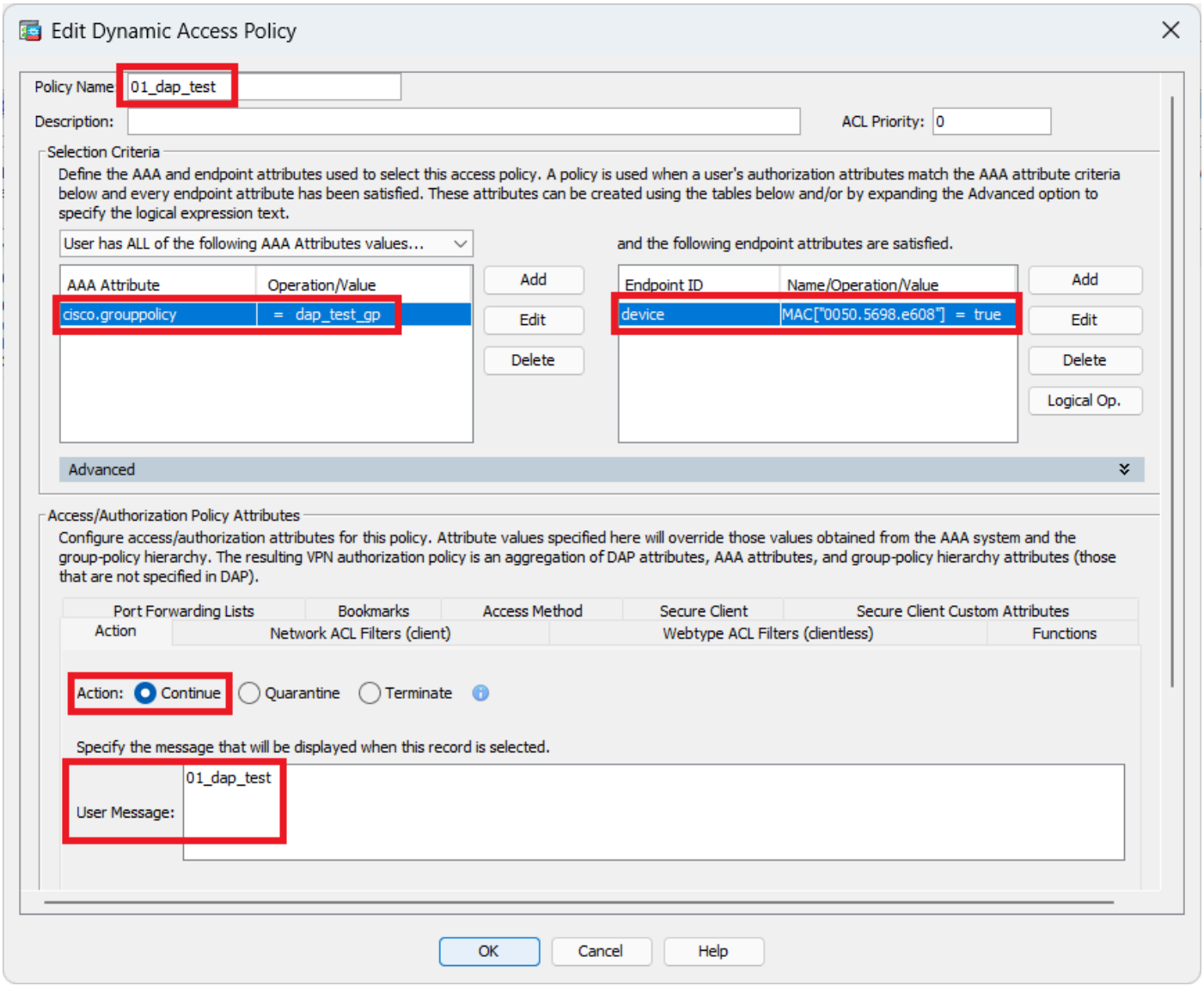
Configuración en ASDM

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

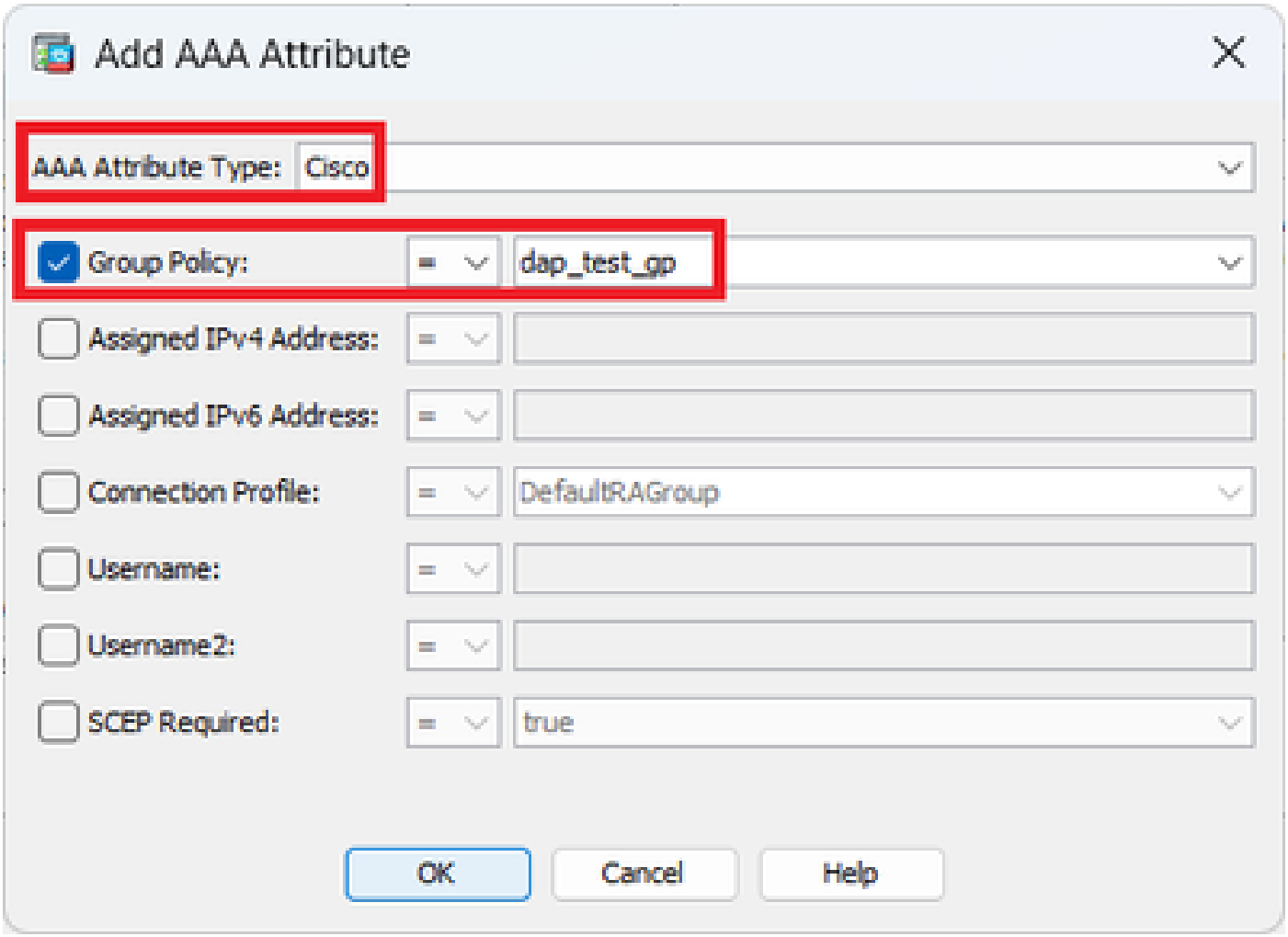
1. Configure el primer DAP denominado 01_dap_test.

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:



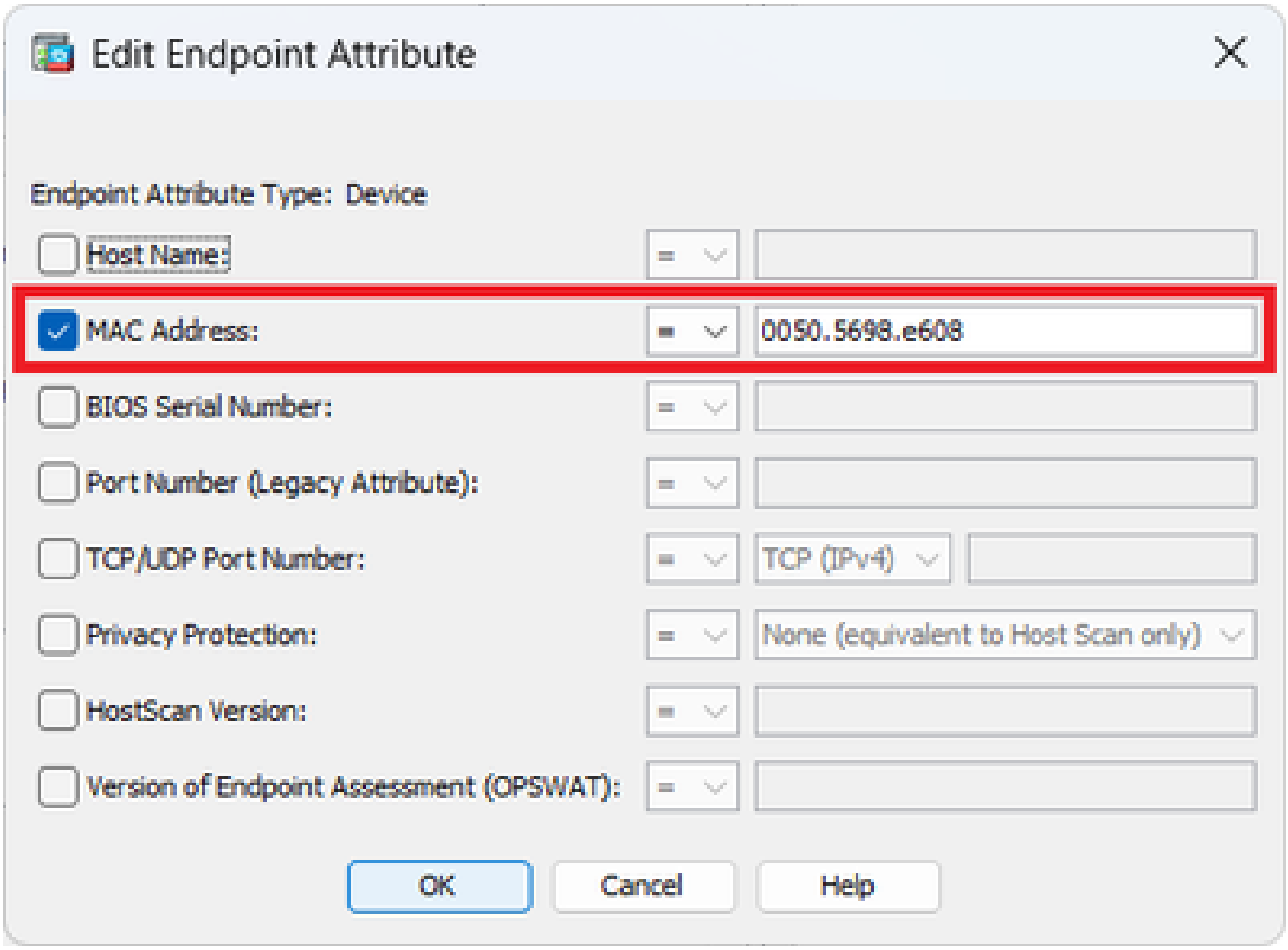
Configurar el primer DAP

Configure la política de grupo para el atributo AAA.



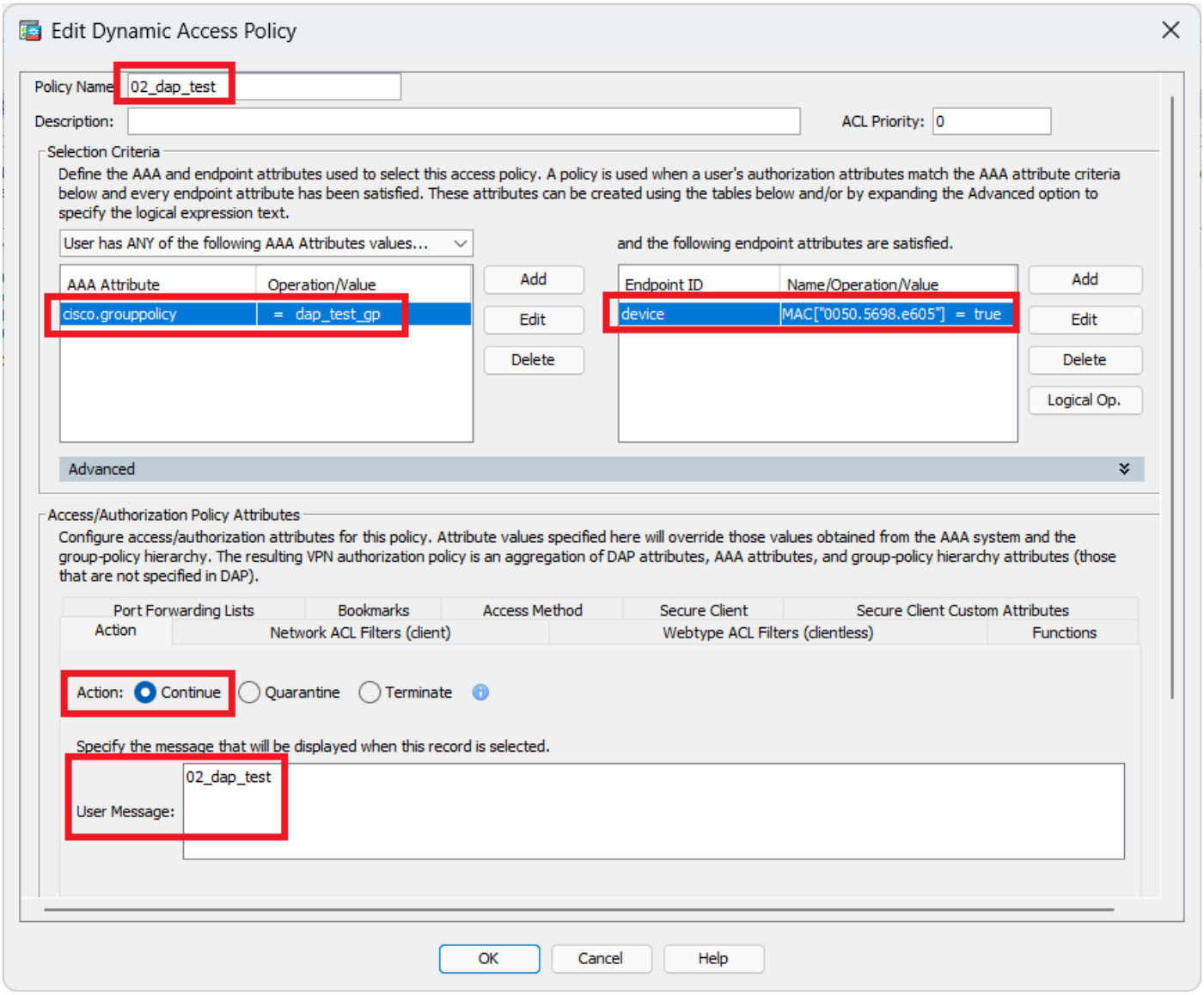
Configurar la directiva de grupo para el registro DAP

Configure la dirección MAC para el atributo de terminal.



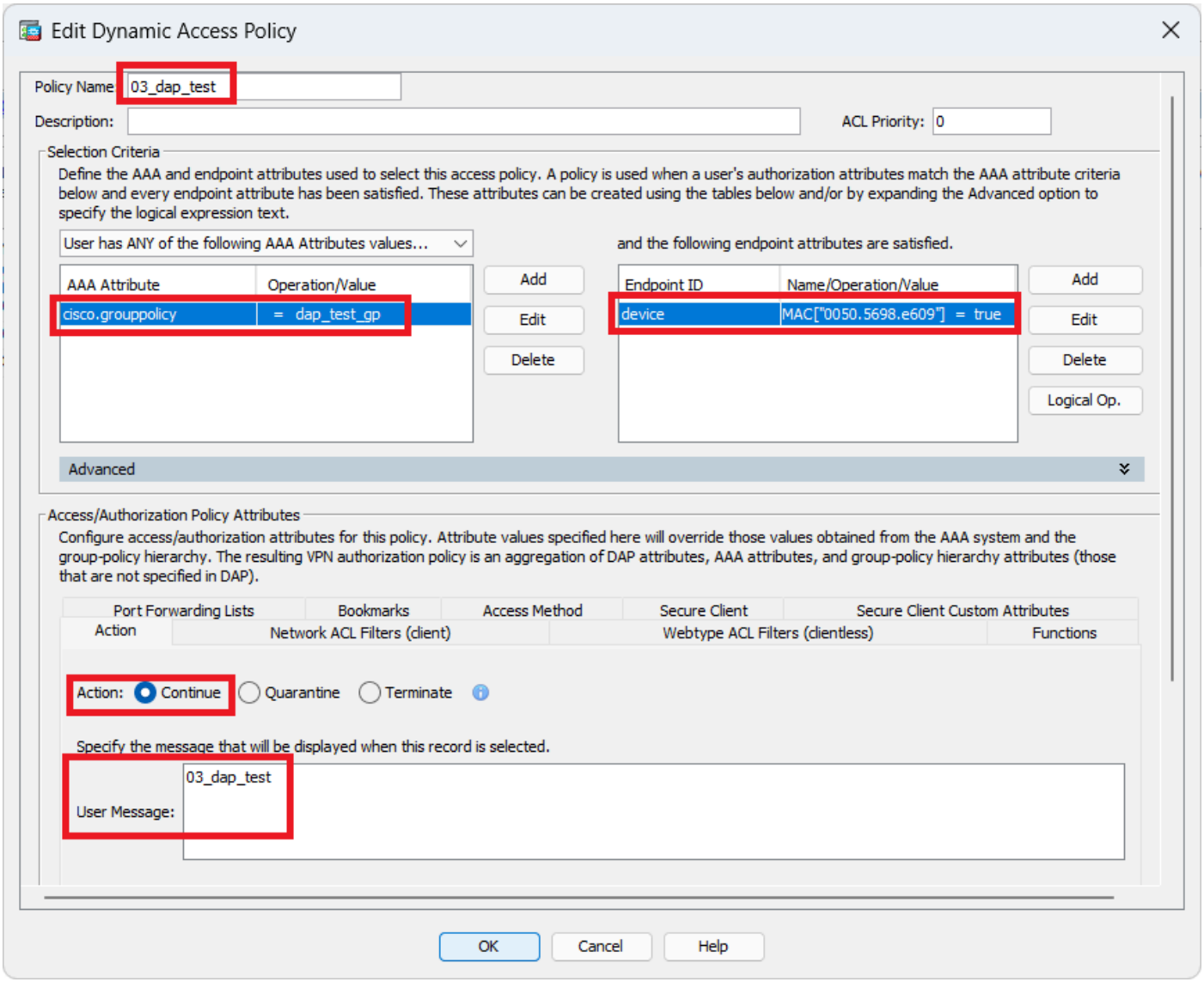
Configuración de la condición MAC para DAP

2. Configure el segundo DAP denominado 02_dap_test.



Configuración del segundo DAP

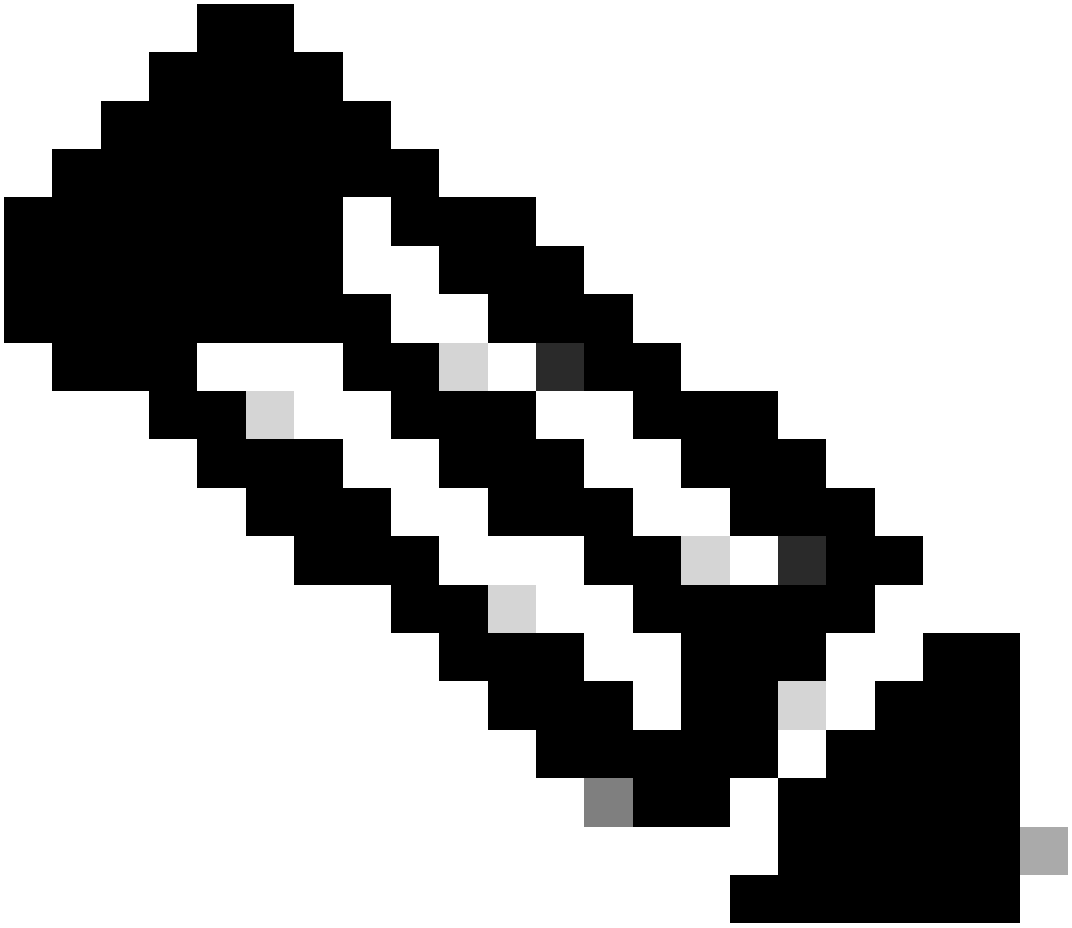
3. Configure el tercer DAP denominado 03_dap_test.



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"]

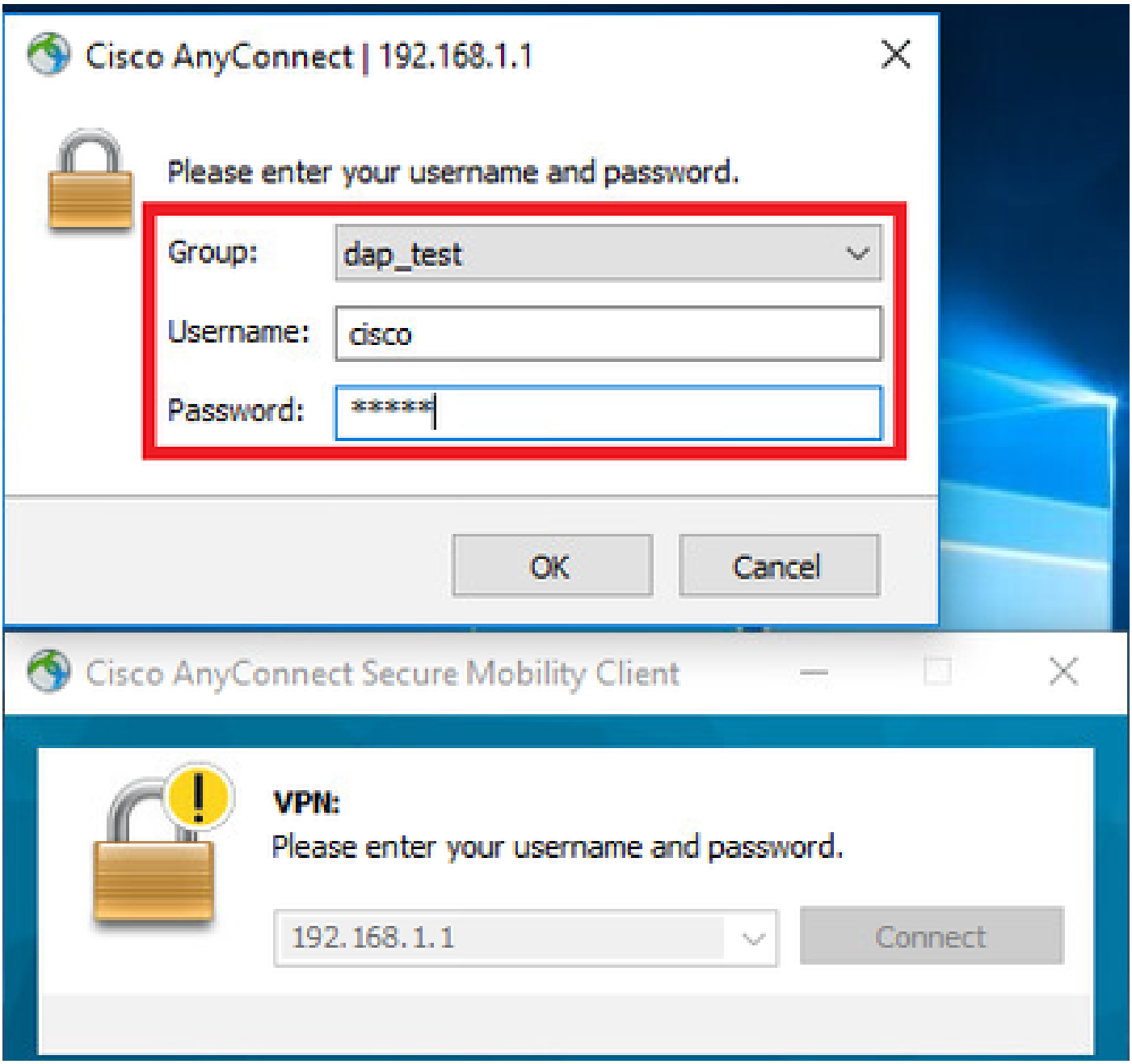
</name> <--- 3rd DAP MAC Address condition <value>true</value> <type>caseless</type> <operation>EQ</ope

Verificación

Situación 1. Sólo se encuentra coincidente un DAP

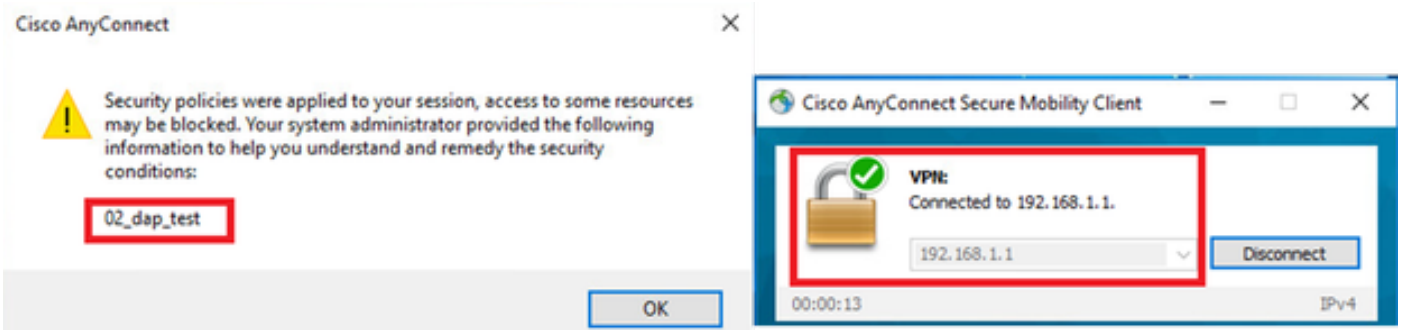
1. Asegúrese de que el MAC del punto final sea 0050.5698.e605 que coincida con la condición MAC en 02_dap_test.

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



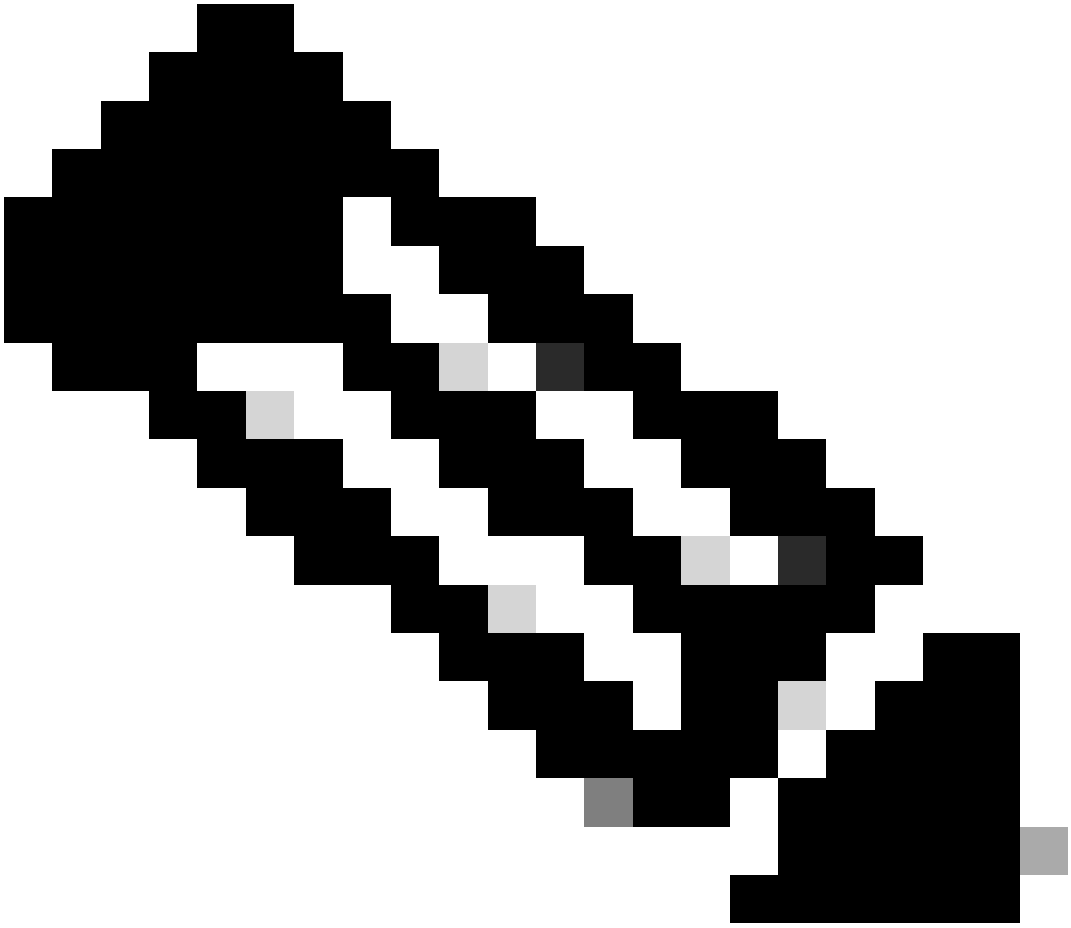
Introducir nombre de usuario y contraseña

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

: ,

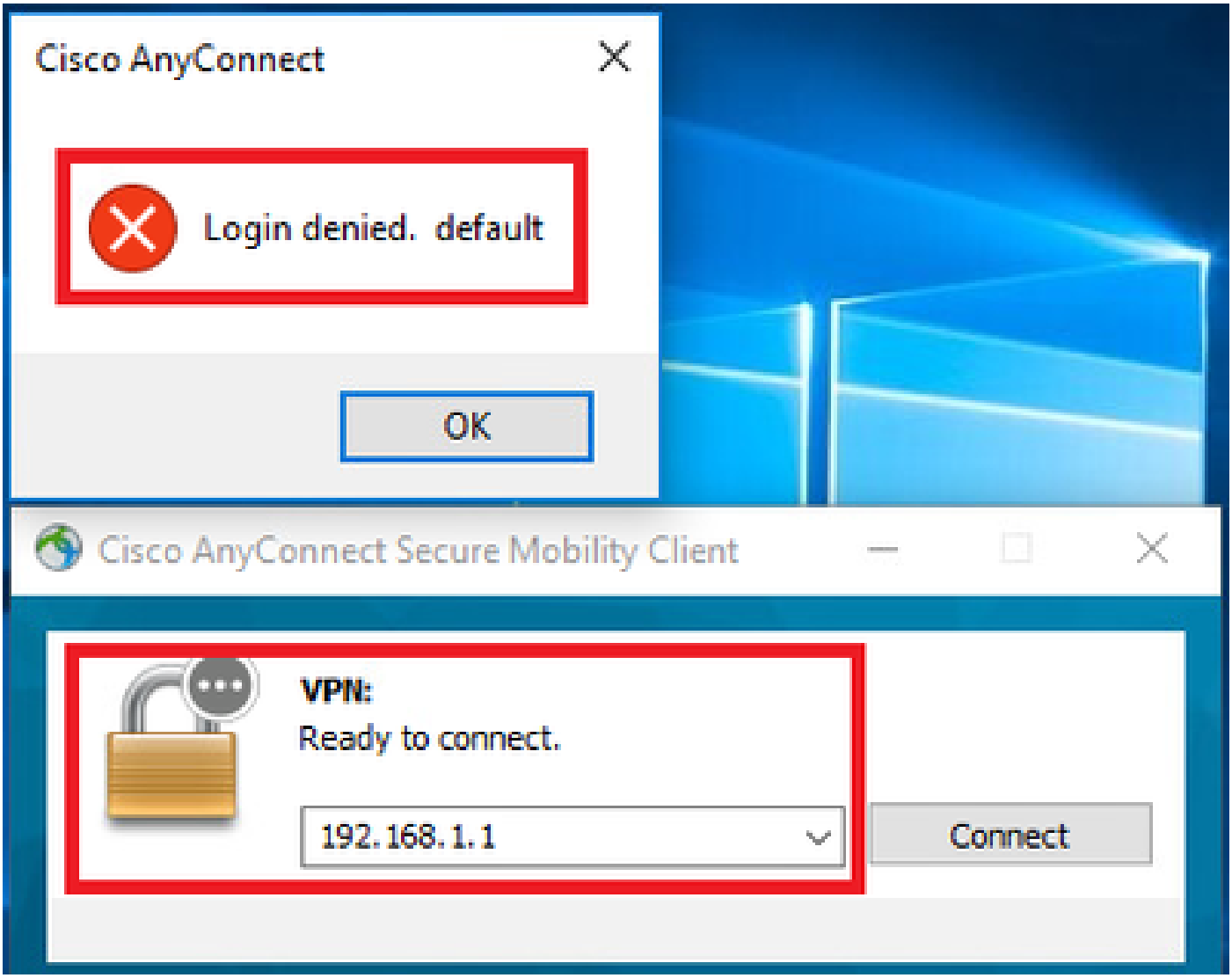
```
02_dap_test

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

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.

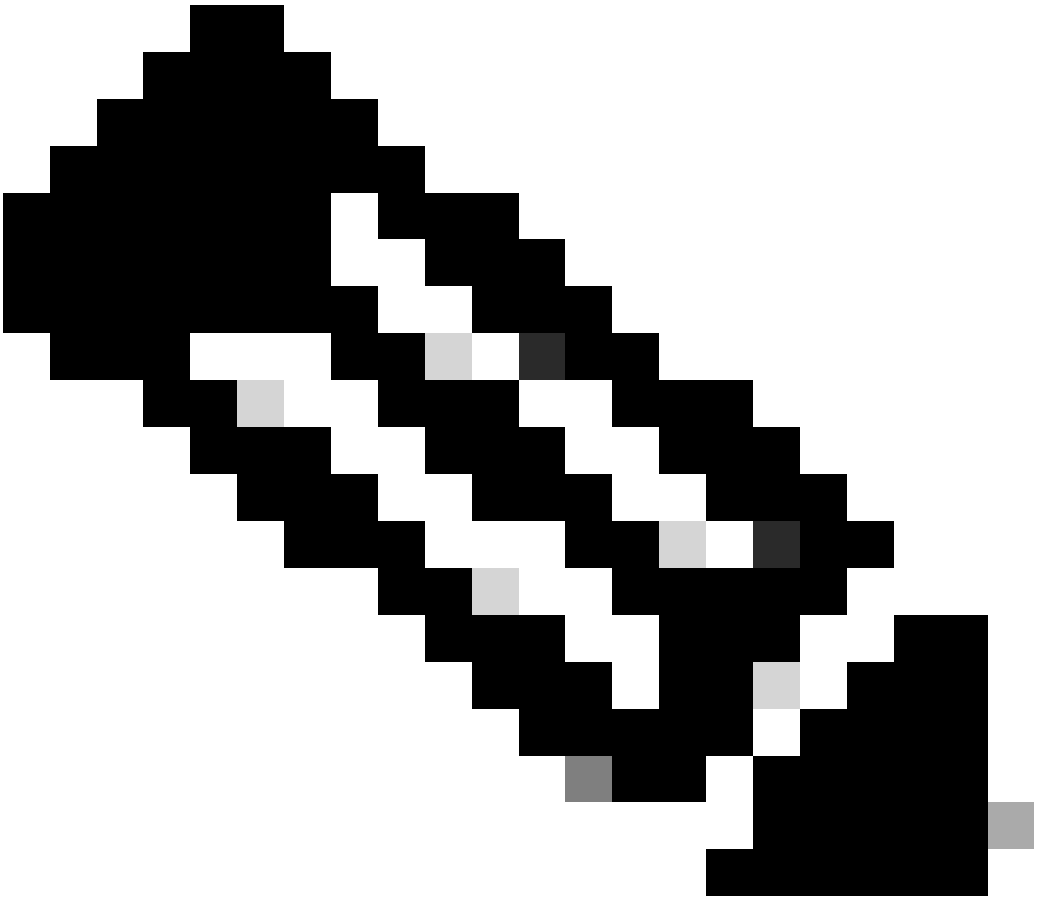
2. En el terminal, ejecute Anyconnect connection e introduzca el nombre de usuario y la contraseña.

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_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

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:

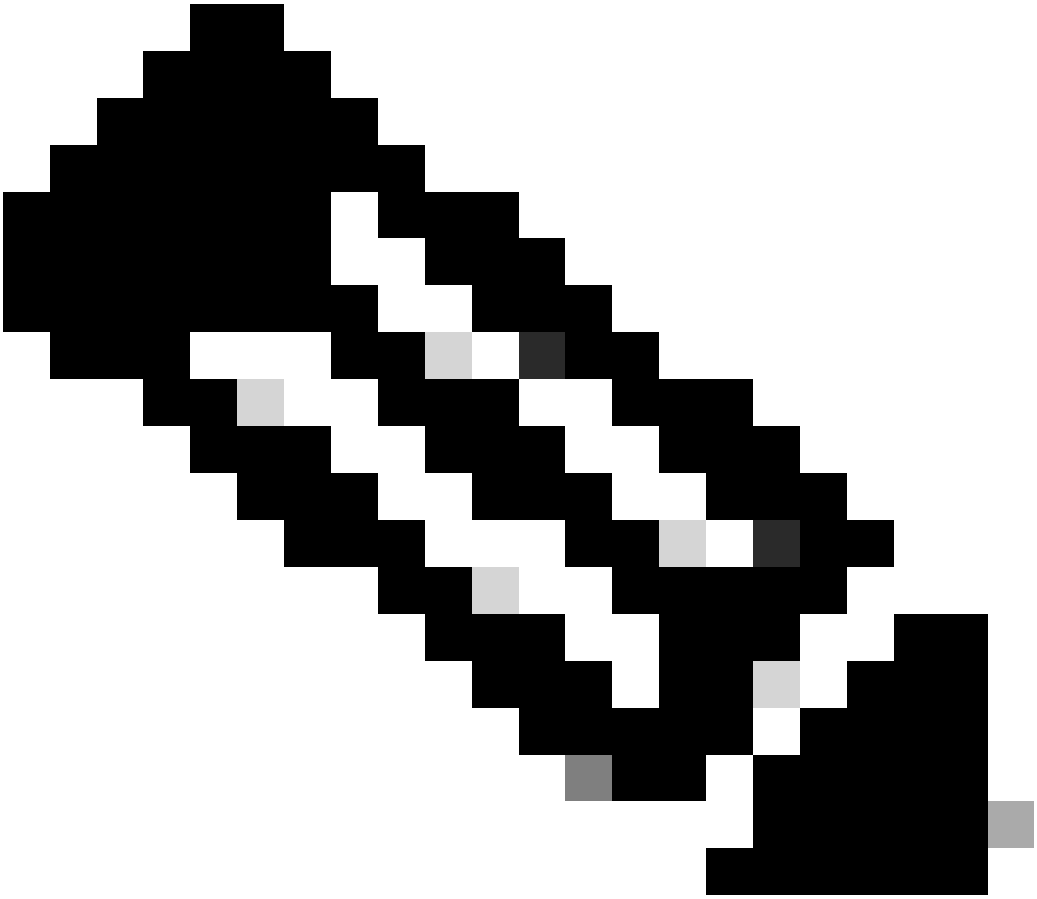
dapSelection (nombre de host) = terminal.device.hostname[DESKTOP-VCKHRG1] = nombre de host del terminal de Anyconnect
Acción = **Continuar**

·Eliminar registro DAP 03_dap_test

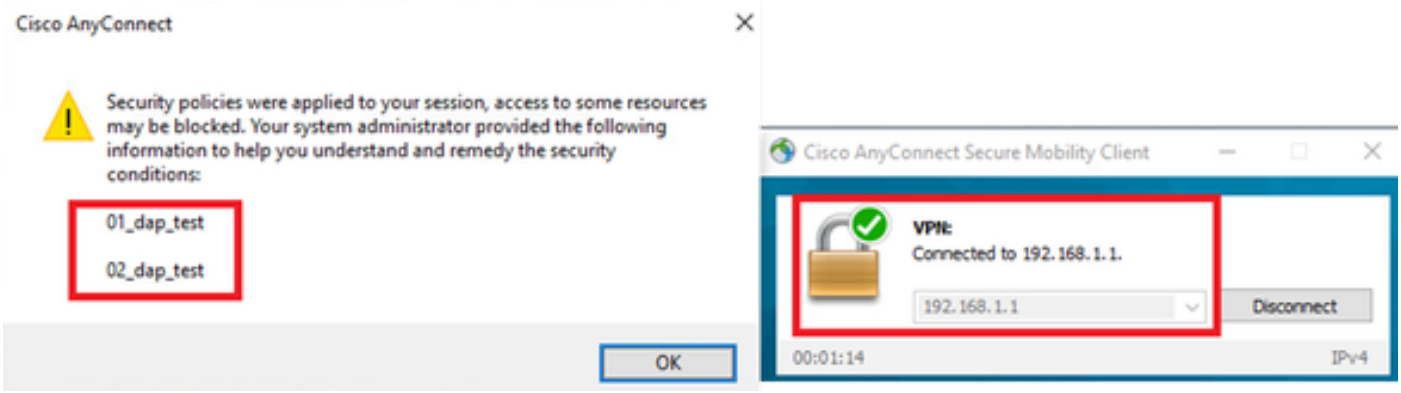
2. En el terminal, ejecute Anyconnect connection e introduzca el nombre de usuario y la contraseña.

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: DA

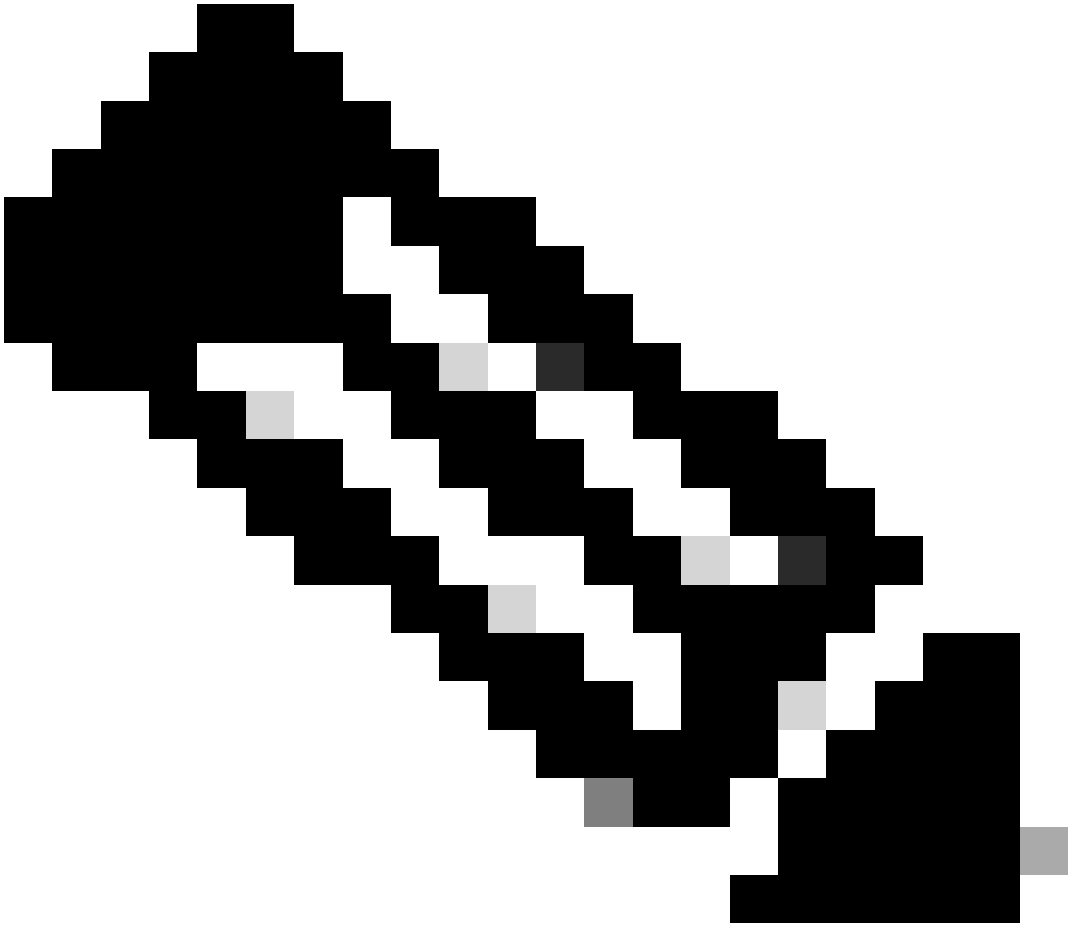
Situación4. Varios DAP (Acción :Terminar) coinciden

1. Cambie la acción de 01_dap_test.

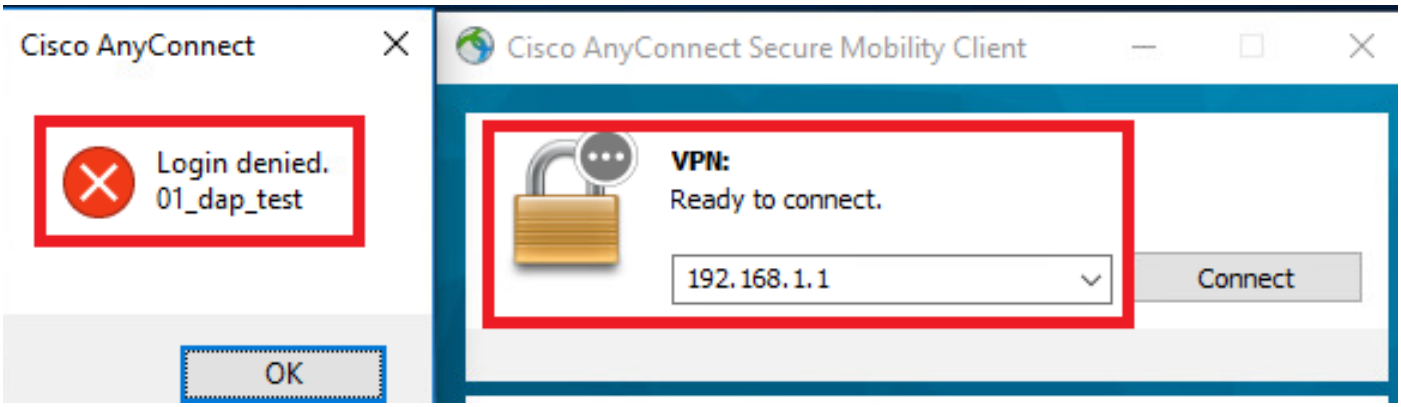
·01_dap_test:
dapSelection (dirección MAC) = endpoint.device.MAC[0050.5698.e605] = MAC del terminal Anyconnect
Acción = **Terminar**
·02_dap_test:
dapSelection (nombre de host) = terminal.device.hostname[DESKTOP-VCKHRG1] = nombre de host del terminal de Anyconnect
Acción = **Continuar**

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:

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).