ASA DAP implementeren om MAC-adres voor AnyConnect te identificeren

Inhoud

Inleiding

In dit document wordt beschreven hoe u Dynamic Access Policies (DAP) via ASDM kunt configureren om het Mac-adres van het apparaat te controleren dat wordt gebruikt voor de AnyConnect-verbinding.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:
Configuratie van Cisco AnyConnect en Hostscan

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:
ASAv 9.18 (4)
ASDM 7.20 (1)
AnyConnect 4.10.07073
Hostscan 4.10.07073

Windows 10

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

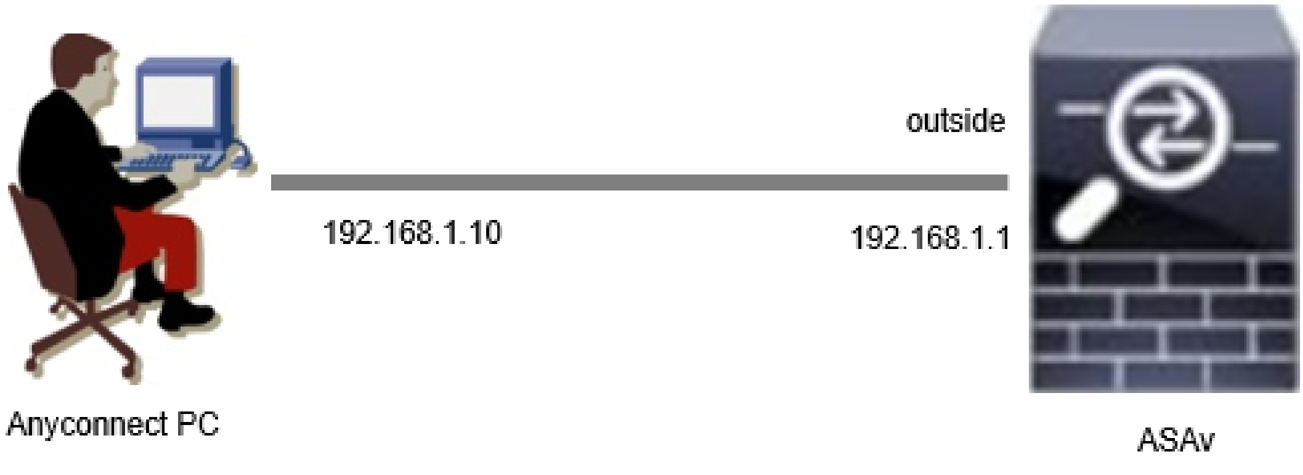
Achtergrondinformatie

HostScan is een softwaremodule die de AnyConnect Secure Mobility Client de mogelijkheid biedt om beveiligingsbeleid op het netwerk af te dwingen. Tijdens het proces van Hostscan worden verschillende gegevens over het clientapparaat verzameld en doorgegeven aan de adaptieve security applicatie (ASA). Deze details omvatten het apparaat besturingssysteem, antivirus software, firewall software, MAC-adres, en meer. De functie Dynamic Access Policies (DAP) stelt netwerkbeheerders in staat om beveiligingsbeleid per gebruiker te configureren. De eigenschap endpoint.device.MAC in DAP kan worden gebruikt om het MAC-adres van het clientapparaat te vergelijken met of te controleren op vooraf bepaald beleid.

Configureren

Netwerkdiagram

Dit beeld toont de topologie die bij het voorbeeld van dit document wordt gebruikt.



Diagram

Configuratie in ASA

Dit is de minimale configuratie in 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
```

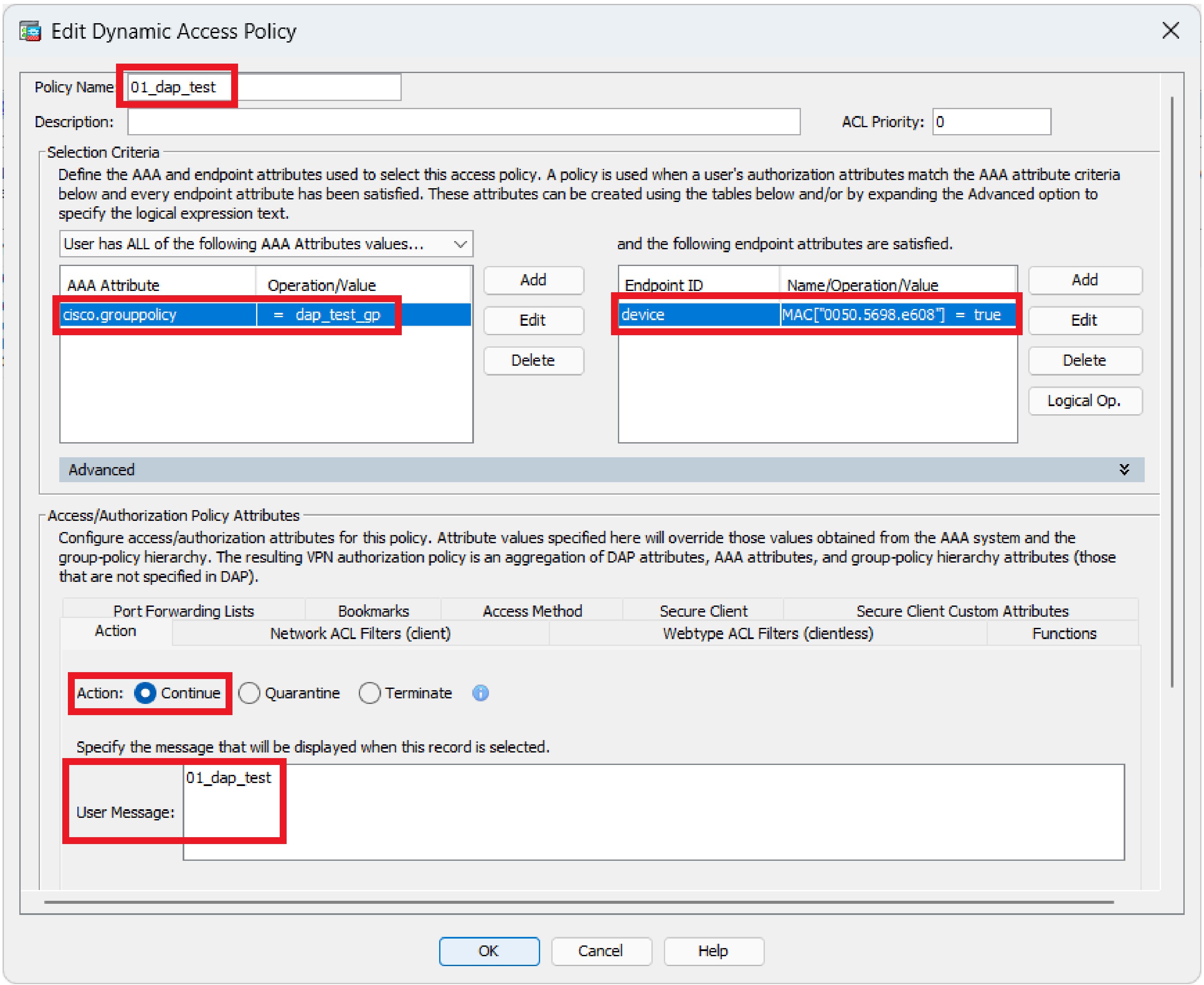
Configuratie in ASDM

In dit gedeelte wordt beschreven hoe de DAP-record in ASDM kan worden geconfigureerd. In dit voorbeeld, plaats 3 DAP records die gebruiken endpoint.device.MAC attributen als voorwaarde.

·01_dap_test:endpoint.device.MAC=0050.5698.e608
·02_dap_test:endpoint.device.MAC=0050.5698.e605 = MAC van AnyConnect-endpoint
·03_dap_test:endpoint.device.MAC=0050.5698.e609

1. Configureer de eerste DAP met de naam 01_dap_test.

Navigeer naar Configuratie > Externe toegang VPN > Netwerktoegang (client) > Dynamisch toegangsbeleid. Klik op Add en stel de beleidsnaam, AAA-kenmerk, endpointkenmerken, Actie, Gebruikersbericht in, zoals in de afbeelding:



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
cisco.grouppolicy	= dap_test_gp

Endpoint ID	Name/Operation/Value
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).

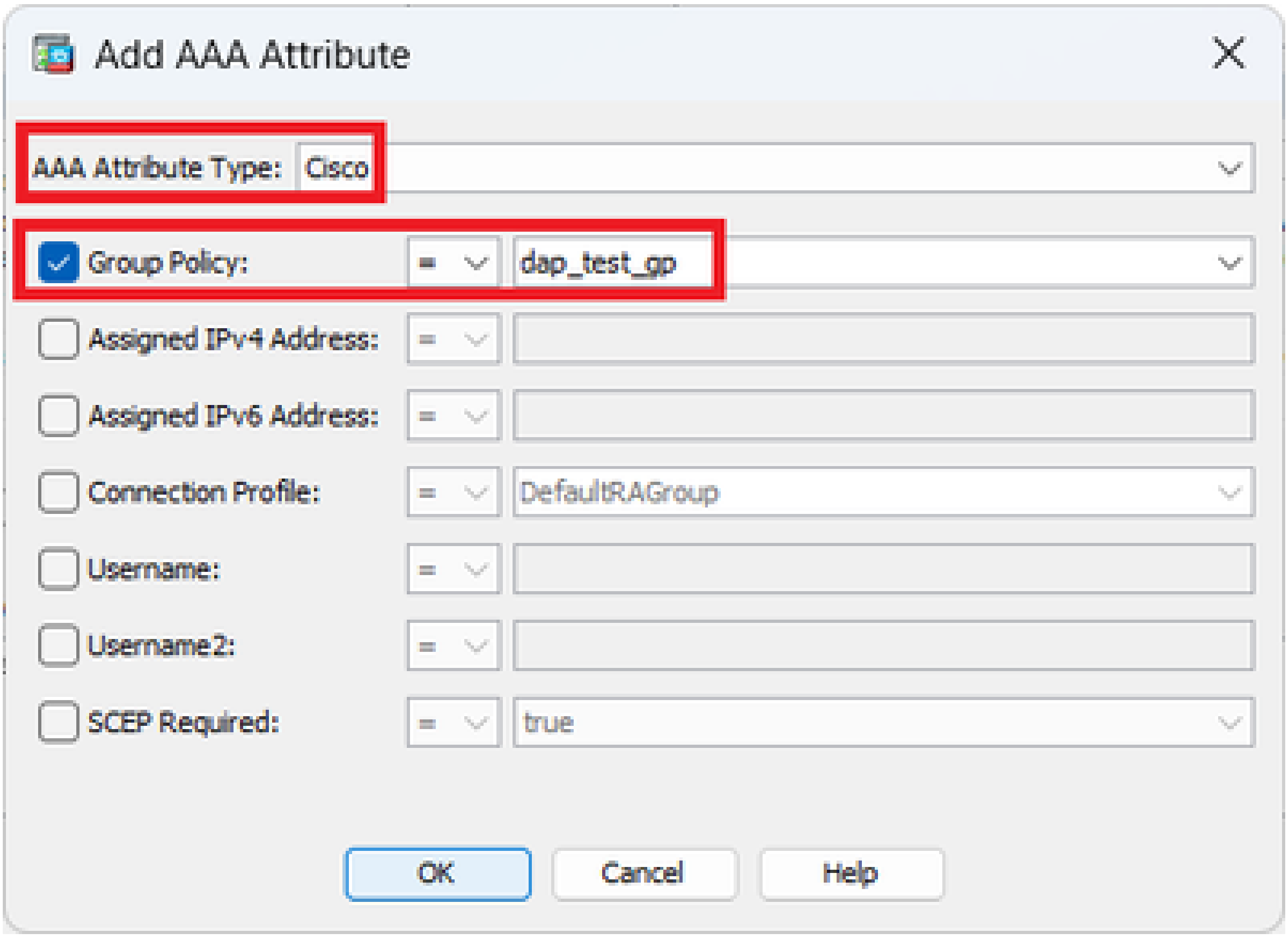
Action: ● Continue ○ Quarantine ○ Terminate

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

User Message: 01_dap_test

Eerste DAP configureren

Groepsbeleid configureren voor AAA-kenmerken.



Add AAA Attribute

AAA Attribute Type: Cisco

☑ Group Policy: = dap_test_gp

□ Assigned IPv4 Address: =

□ Assigned IPv6 Address: =

□ Connection Profile: = DefaultRAGroup

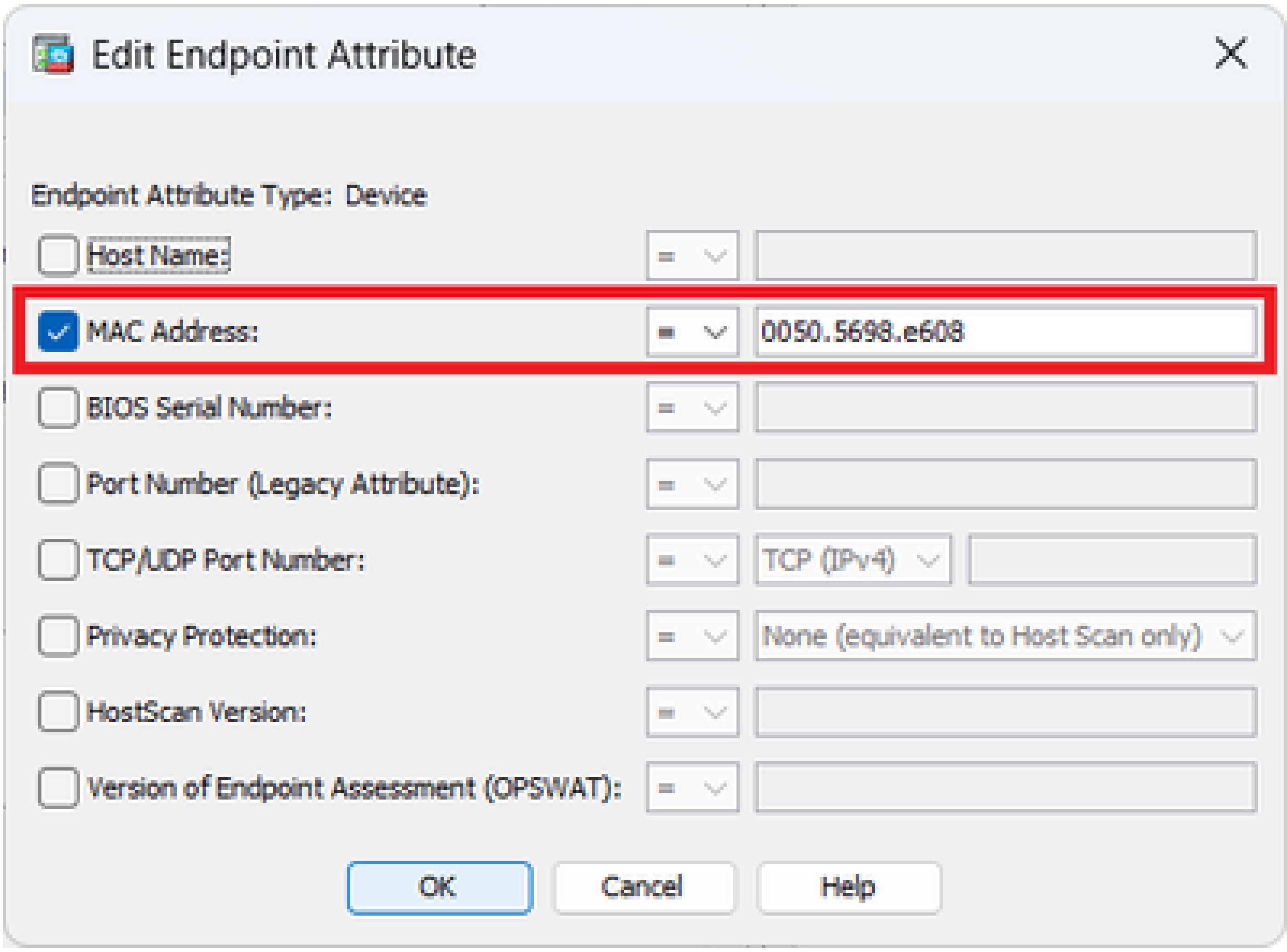
□ Username: =

□ Username2: =

□ SCEP Required: = true

Groepsbeleid voor DAP-record configureren

Configureer MAC-adres voor endpointkenmerken.



Endpoint Attribute Type: Device

□ Host Name: =

☑ MAC Address: = 0050.5698.e608

□ BIOS Serial Number: =

□ Port Number (Legacy Attribute): =

□ TCP/UDP Port Number: = TCP (IPv4)

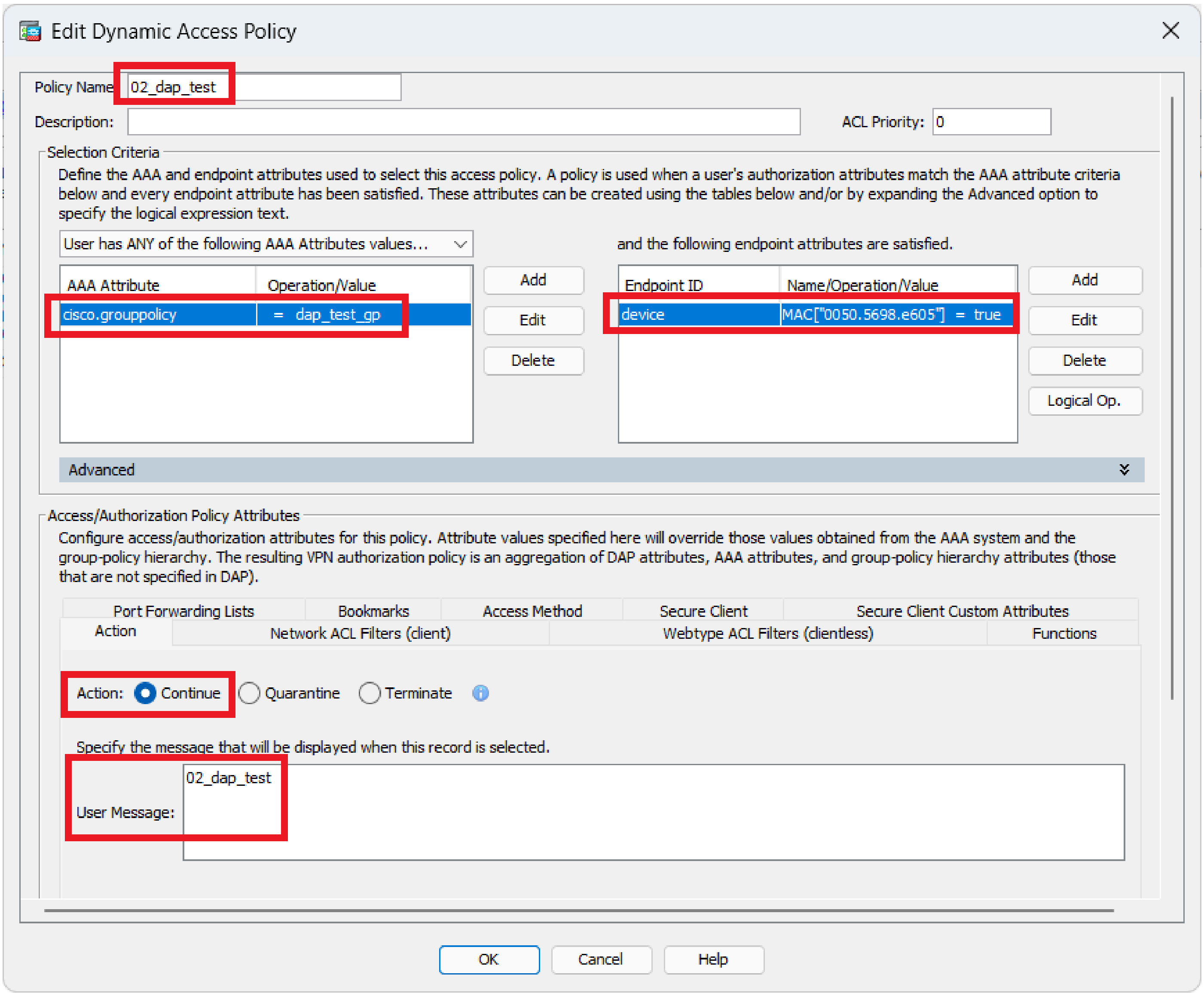
□ Privacy Protection: = None (equivalent to Host Scan only)

□ HostScan Version: =

□ Version of Endpoint Assessment (OPSWAT): =

MAC-voorwaarde voor DAP configureren

2. Configureer de tweede DAP met de naam 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...

AAA Attribute	Operation/Value
cisco.grouppolicy	= dap_test_gp

and the following endpoint attributes are satisfied.

Endpoint ID	Name/Operation/Value
device	MAC["0050.5698.e605"] = true

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).

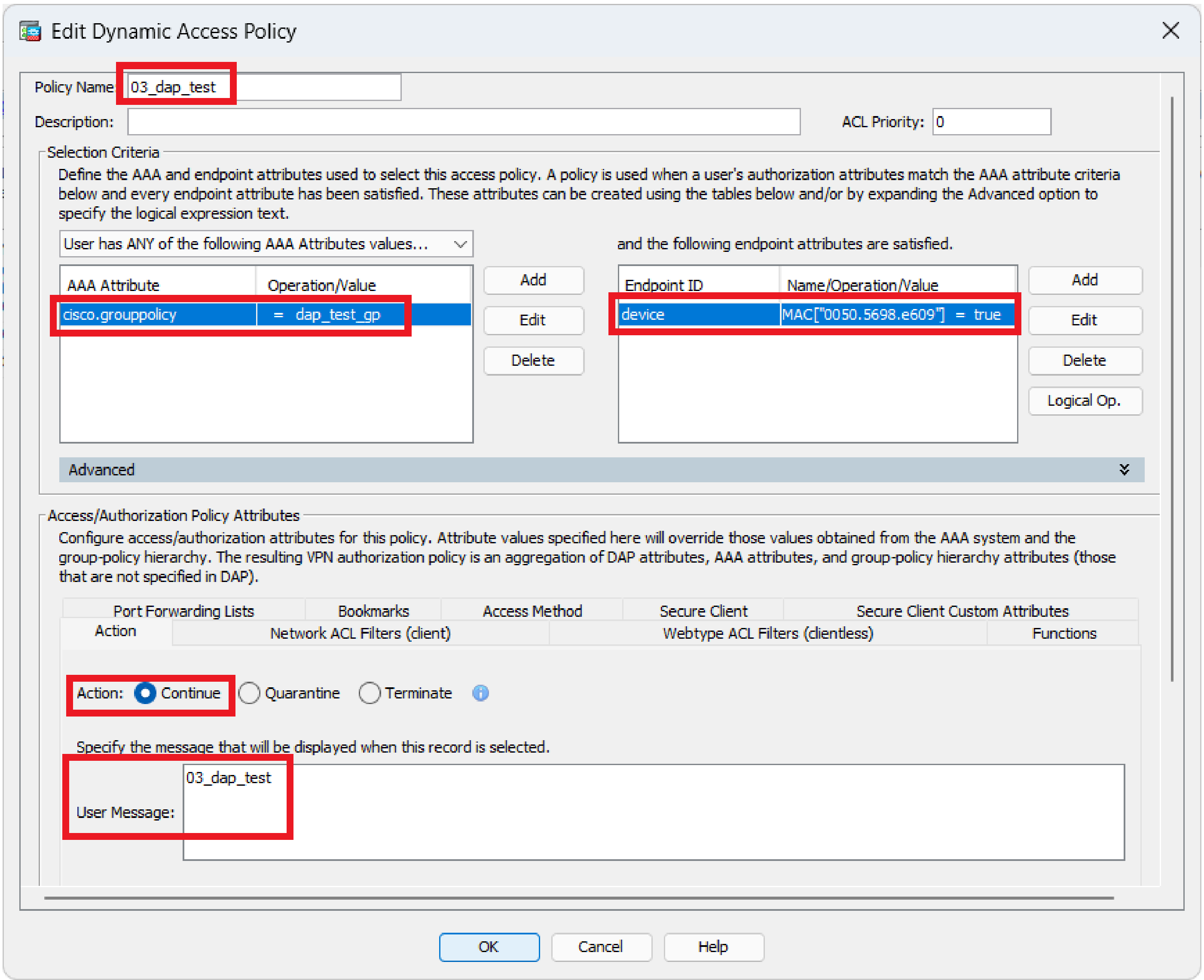
Action: ● Continue ○ Quarantine ○ Terminate

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

User Message: 02_dap_test

Tweede DAP configureren

3. Configureer de derde DAP met de naam 03_dap_test.



Edit Dynamic Access Policy

Policy Name: 03_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
cisco.grouppolicy	= dap_test_gp

Endpoint ID	Name/Operation/Value
device	MAC["0050.5698.e609"] = true

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).

Action: ● Continue ○ Quarantine ○ Terminate

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

User Message: 03_dap_test

Derde DAP configureren

4. Gebruik de **more flash:/dap.xml** opdracht om de instelling van DAP-records in dap.xml te bevestigen.

Details van de DAP-records die op ASDM zijn ingesteld, worden in de ASA-flitser opgeslagen als dap.xml. Nadat deze instellingen zijn voltooid, worden drie DAP records gegenereerd in dap.xml. U kunt de details van elke DAP record in dap.xml bevestigen.

Opmerking: De volgorde waarin DAP wordt aangepast is de weergavevolgorde in dap.xml. De standaard DAP (DFLTAccess Policy) wordt het laatst aangepast.

<#root>

```
ciscoasa#

more flash:/dap.xml


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

01_dap_test

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

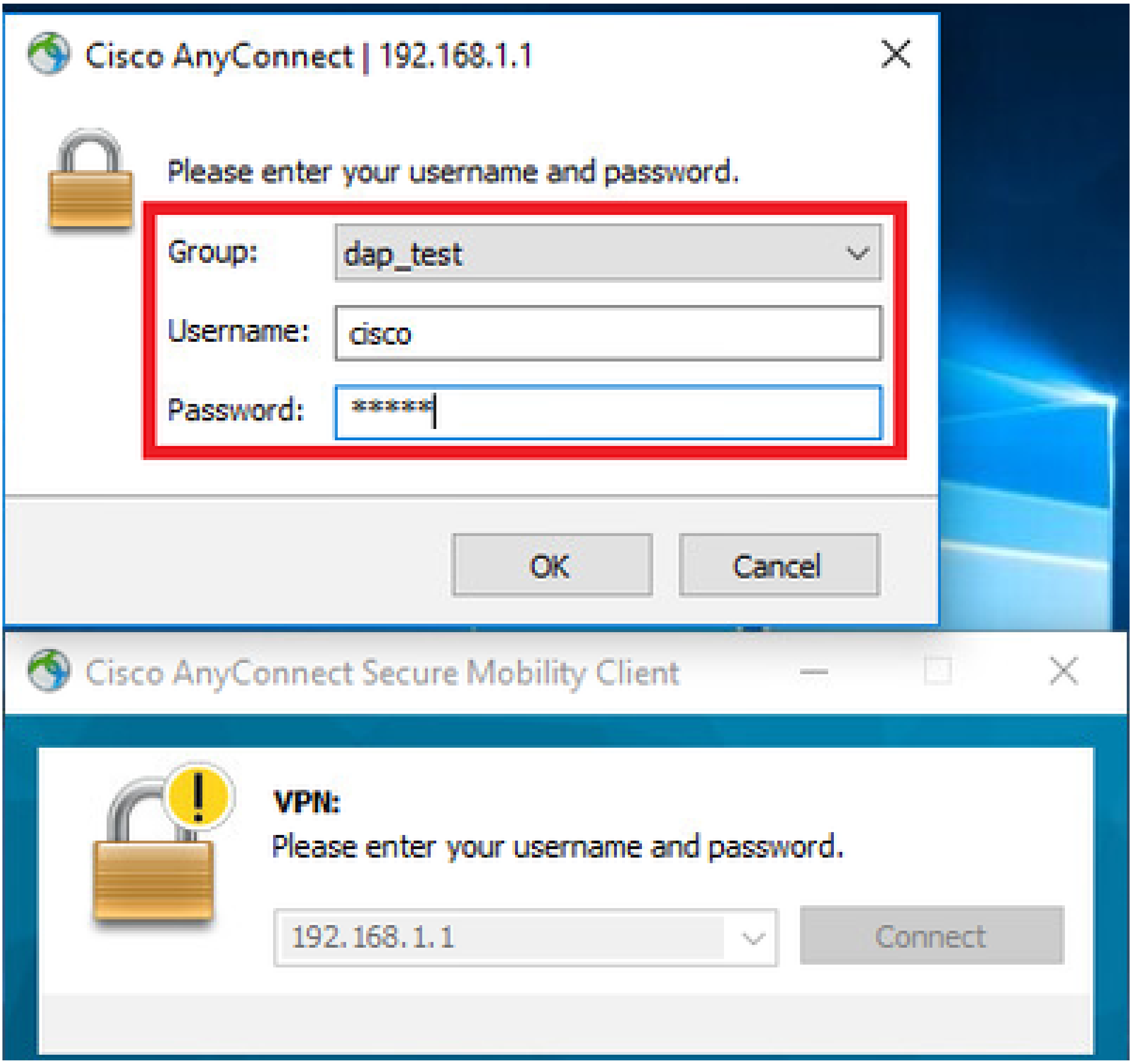
```
dap_test_gp

</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
```

Verifiëren

Scenario 1. Slechts één DAP wordt geëvenaard

1. Zorg ervoor dat de MAC van het eindpunt 0050.5698.e605 is die de voorwaarde van MAC in 02_dap_test aanpast.

2. Voer op endpoint de AnyConnect-verbinding en de invoergebruikersnaam en het wachtwoord uit.



Cisco AnyConnect | 192.168.1.1

Please enter your username and password.

Group: dap_test

Username: cisco

Password: *****

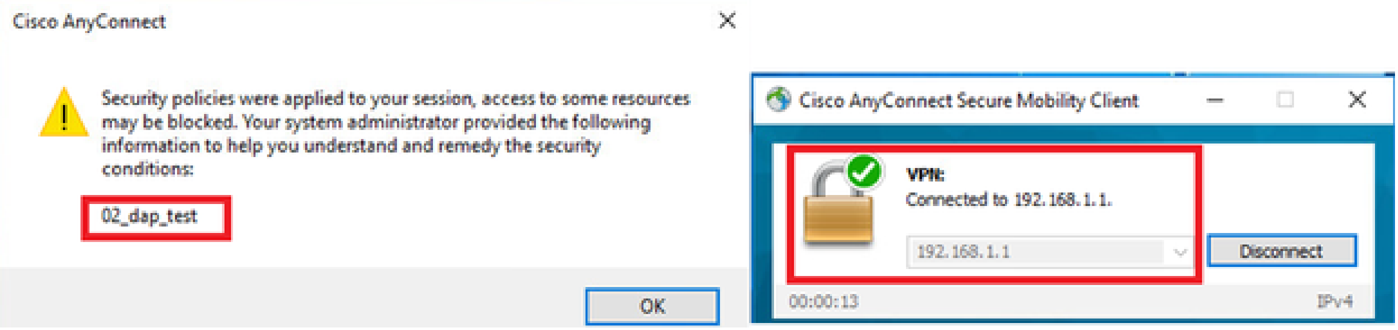
Cisco AnyConnect Secure Mobility Client

VPN:
Please enter your username and password.

192.168.1.1

Gebruikersnaam en wachtwoord invoeren

3. Bevestig in de AnyConnect UI dat 02_dap_test is gekoppeld.



Cisco AnyConnect

Security policies were applied to your session, access to some resources may be blocked. Your system administrator provided the following information to help you understand and remedy the security conditions:

02_dap_test

Cisco AnyConnect Secure Mobility Client

VPN:
Connected to 192.168.1.1.

192.168.1.1

00:00:13

IPv4

Gebruikersbericht bevestigen in UI

4. Bevestig in de ASA syslog dat 02_dap_test is gekoppeld.

Opmerking: zorg ervoor dat debug datumspoor in ASA is ingeschakeld.

<#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
```

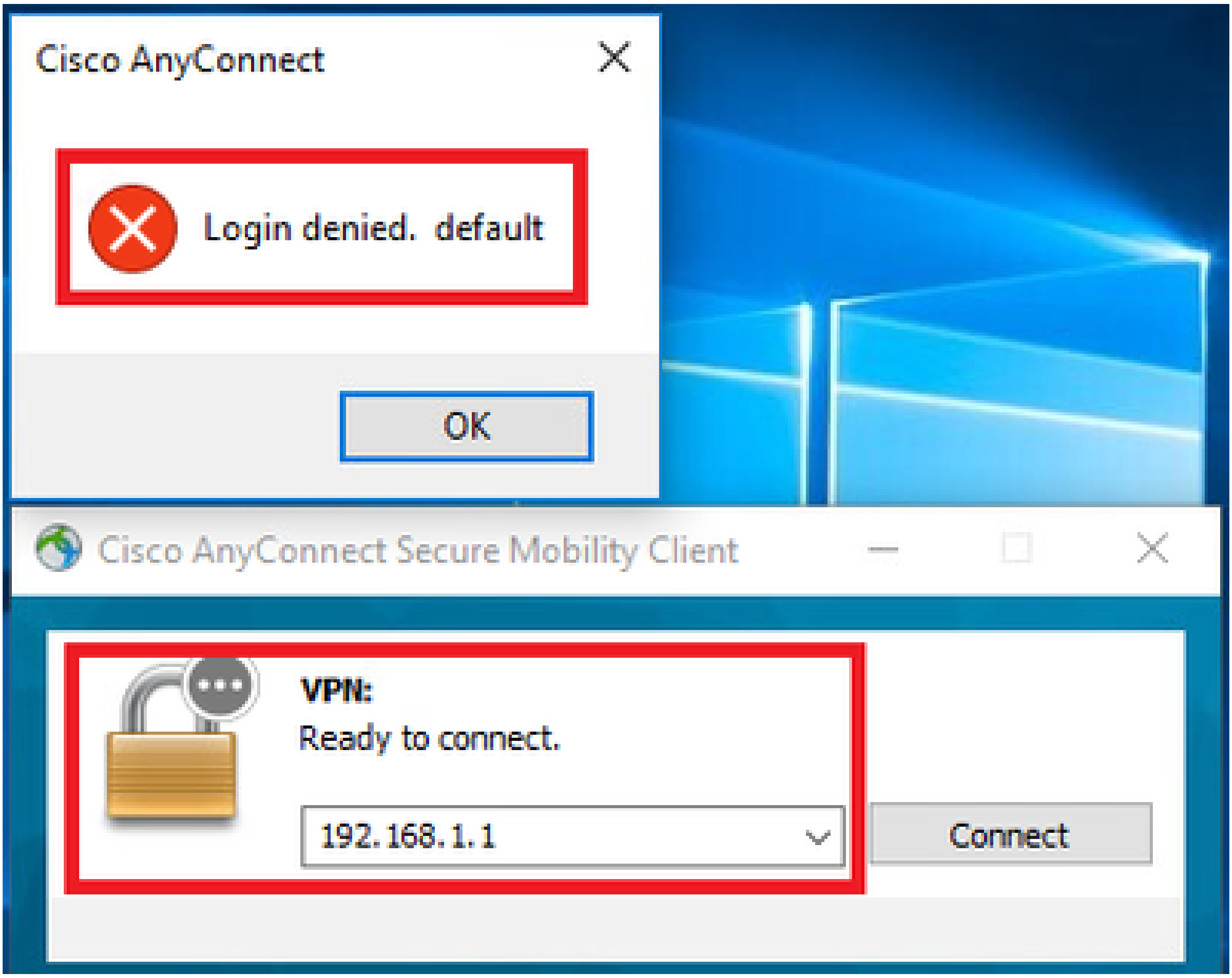
```
 Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 11:46:11: %ASA-4-711001: D
```

Scenario2. Standaard DAP is gekoppeld

1. Verander de waarde van endpoint.device.MAC in 02_dap_test in 0050.5698.e607 die niet overeenkomt met MAC van endpoint.

2. Voer op endpoint de AnyConnect-verbinding en de invoergebruikersnaam en het wachtwoord uit.

3. Bevestig dat de AnyConnect-verbinding is geweigerd.



Cisco AnyConnect

Login denied. default

VPN:
Ready to connect.

192.168.1.1

Gebruikersbericht bevestigen in UI

4. Bevestig in de ASA syslog dat DFLTAccess Policy overeenkomt met.

Opmerking: standaard wordt de handeling van DFLTAccess Policy beëindigd.

```
<#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: Se
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
```

Scenario 3. Meervoudige DAP's (Actie: Doorgaan) worden gekoppeld

1. Wijzig de actie en het kenmerk in elk DAP.

·01_dap_test :
dapSelection (MAC Address) = endpoint.device.MAC[0050.5698.e605] = MAC van AnyConnect-endpoint
Actie = **Doorgaan**
·02_dap_test :

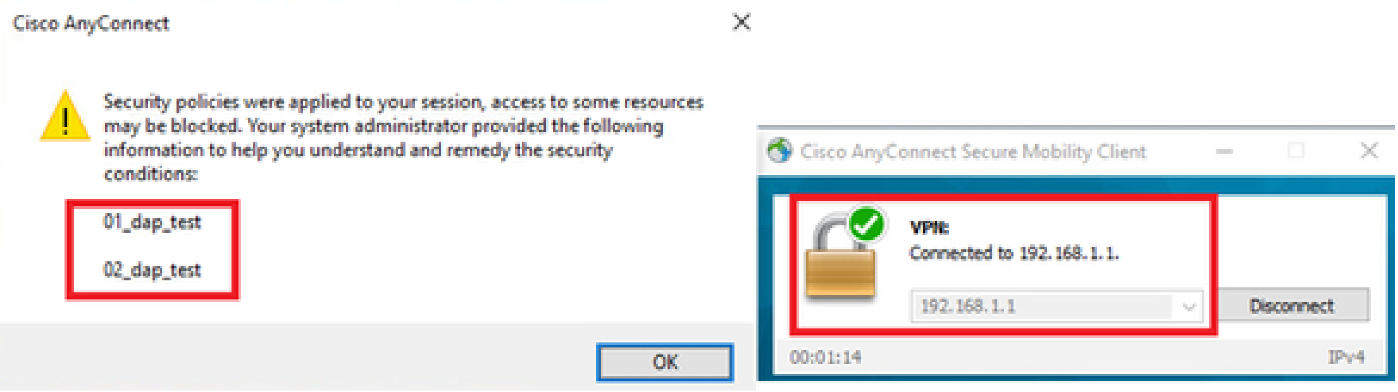
dapSelection (hostnaam) = endpoint.device.hostnaam [DESKTOP-VCKHRG1] = Hostnaam van AnyConnect-endpoint
Actie = **Doorgaan**

·Verwijderen 03_dap_test DAP record

2. Voer op endpoint de AnyConnect-verbinding en de invoergebruikersnaam en het wachtwoord uit.

3. Bevestig in de AnyConnect UI dat alle 2 DAP's worden gekoppeld

Opmerking: Als een verbinding overeenkomt met meerdere DAP's, worden de gebruikersberichten van meerdere DAP's geïntegreerd en samen weergegeven in AnyConnect UI.



Security policies were applied to your session, access to some resources may be blocked. Your system administrator provided the following information to help you understand and remedy the security conditions:

01_dap_test

02_dap_test

VPN:
Connected to 192.168.1.1.

Gebruikersbericht bevestigen in UI

4. Bevestig in de ASA syslog dat alle 2 DAP's worden gematched.

<#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_selecte
```

```
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
```

Scenario 4. Meervoudige DAP's (Action:Terminate) worden toegewezen

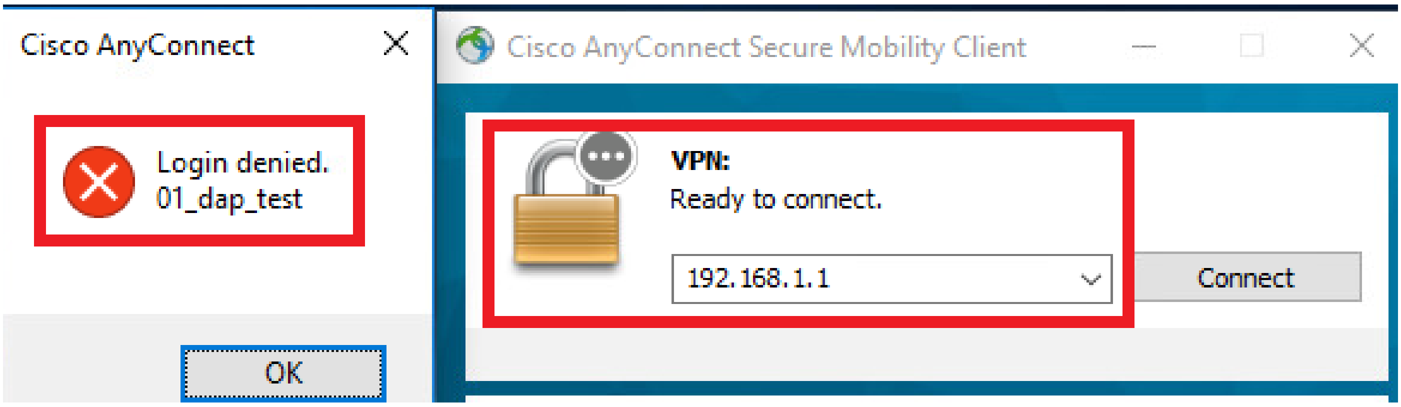
1. Verander de actie van 01_dap_test.

·01_dap_test :
dapSelection (MAC Address) = endpoint.device.MAC[0050.5698.e605] = MAC van AnyConnect-endpoint
Actie = **Beëindigen**
·02_dap_test :
dapSelection (hostnaam) = endpoint.device.hostnaam [DESKTOP-VCKHRG1] = Hostnaam van AnyConnect-endpoint
Actie = **Doorgaan**

2. Voer op endpoint de AnyConnect-verbinding en de invoergebruikersnaam en het wachtwoord uit.

3. Bevestig in de AnyConnect UI dat alleen **01_dap_test** wordt gematched.

Opmerking: een verbinding wordt gekoppeld aan de DAP-record die is ingesteld om de actie te beëindigen. Volgende records worden niet meer gematched na de actie beëindigen.



Login denied.
01_dap_test

VPN:
Ready to connect.

192.168.1.1

Gebruikersbericht bevestigen in UI

4. In ASA syslog, bevestig dat slechts 01_dap_test wordt aangepast.

<#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:
```

Algemene probleemoplossing

Deze debug logboeken helpen u om het detailgedrag van DAP in ASA te bevestigen.

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
```

Gerelateerde informatie

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

Over deze vertaling
Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.