

AnyConnect의 MAC 주소를 식별하기 위한 ASA DAP 구축

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[ASA의 컨피그레이션](#)

[ASDM의 컨피그레이션](#)

[다음을 확인합니다.](#)

[시나리오 1. 하나의 DAP만 일치함](#)

[시나리오 2. 기본 DAP가 일치함](#)

[시나리오 3. 여러 DAP\(작업: 계속\)가 일치함](#)

[시나리오 4. 여러 DAP\(작업: 종료\)가 일치함](#)

[일반 문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 AnyConnect 연결에 사용된 디바이스의 Mac 주소를 확인하기 위해 ASDM을 통해 DAP(Dynamic Access Policy)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

Cisco Anyconnect 및 Hostscan 구성

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

ASAv 9.18(4)

ASDM 7.20(1)

Anyconnect 4.10.07073

Hostscan 4.10.07073

Windows 10

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

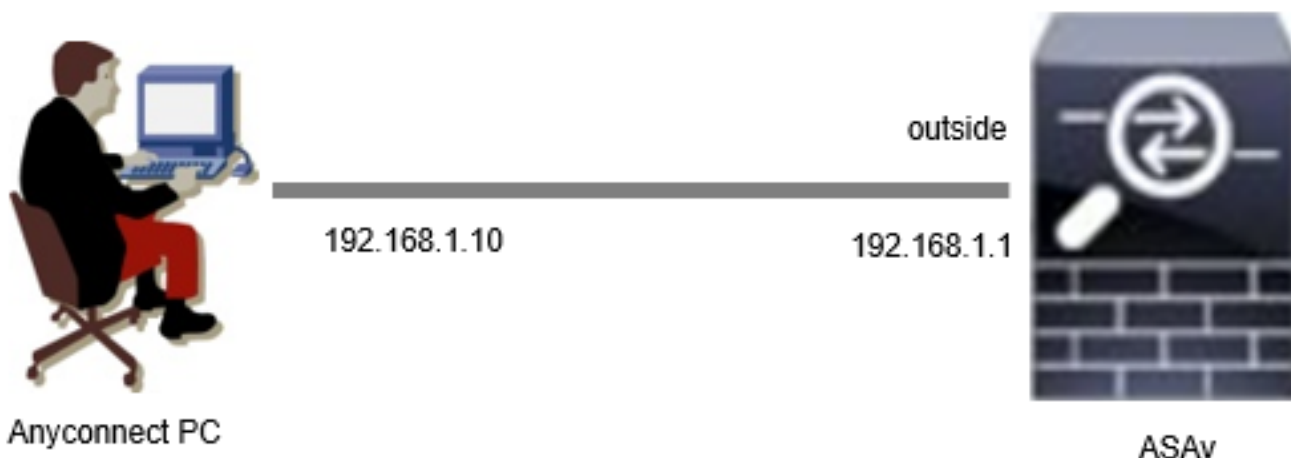
배경 정보

HostScan은 AnyConnect Secure Mobility Client에 네트워크에서 보안 정책을 적용할 수 있는 기능을 제공하는 소프트웨어 모듈입니다. Hostscan 프로세스 중에 클라이언트 디바이스에 대한 다양한 세부 정보가 수집되어 ASA(Adaptive Security Appliance)에 다시 보고됩니다. 이러한 세부 정보에는 디바이스 운영 체제, 안티바이러스 소프트웨어, 방화벽 소프트웨어, MAC 주소 등이 포함됩니다. DAP(Dynamic Access Policies) 기능을 사용하면 네트워크 관리자가 사용자별로 보안 정책을 구성할 수 있습니다. DAP의 endpoint.device.MAC 특성을 사용하여 미리 정의된 정책과 클라이언트 디바이스의 MAC 주소를 일치시키거나 확인할 수 있습니다.

구성

네트워크 다이어그램

이 그림에서는 이 문서의 예에 사용된 토폴로지를 보여줍니다.



다이어그램

ASA의 컨피그레이션

이는 ASA CLI의 최소 컨피그레이션입니다.

```
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
```

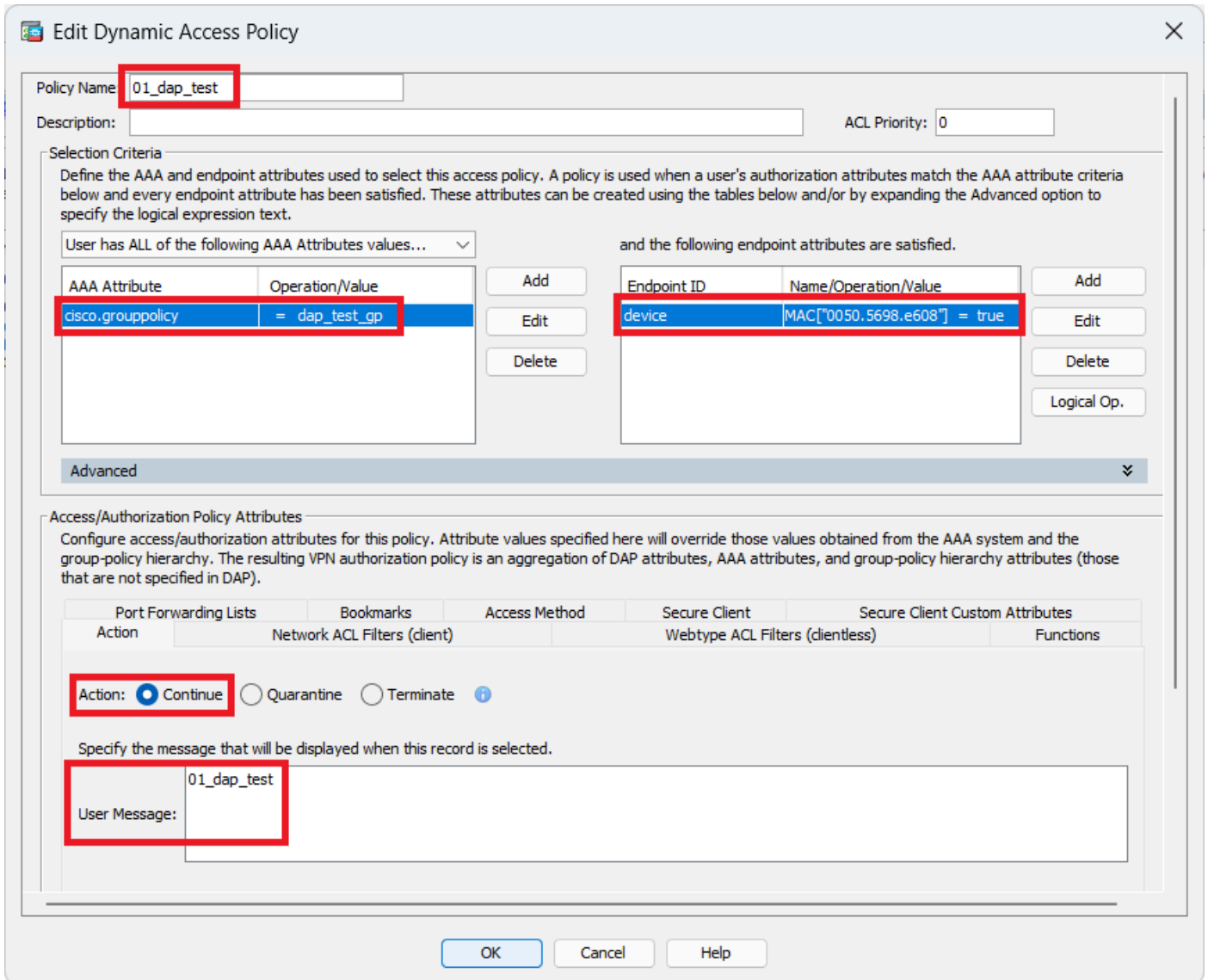
ASDM의 컨피그레이션

이 섹션에서는 ASDM에서 DAP 레코드를 구성하는 방법에 대해 설명합니다. 이 예에서는 endpoint.device.MAC 특성을 조건으로 사용하는 3개의 DAP 레코드를 설정합니다.

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

1. 01_dap_test라는 첫 번째 DAP를 구성합니다.

Configuration(컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Dynamic Access Policies(동적 액세스 정책)로 이동합니다. Add(추가)를 클릭하고 이미지에 표시된 대로 Policy Name(정책 이름), AAA Attribute(AAA 특성), endpoint attributes(엔드포인트 특성), Action(작업), User Message(사용자 메시지)를 설정합니다.



첫 번째 DAP 구성

AAA 특성에 대한 그룹 정책을 구성합니다.

Add AAA Attribute [X]

AAA Attribute Type: Cisco

Group Policy: = dap_test_gp

Assigned IPv4 Address: =

Assigned IPv6 Address: =

Connection Profile: = DefaultRAGroup

Username: =

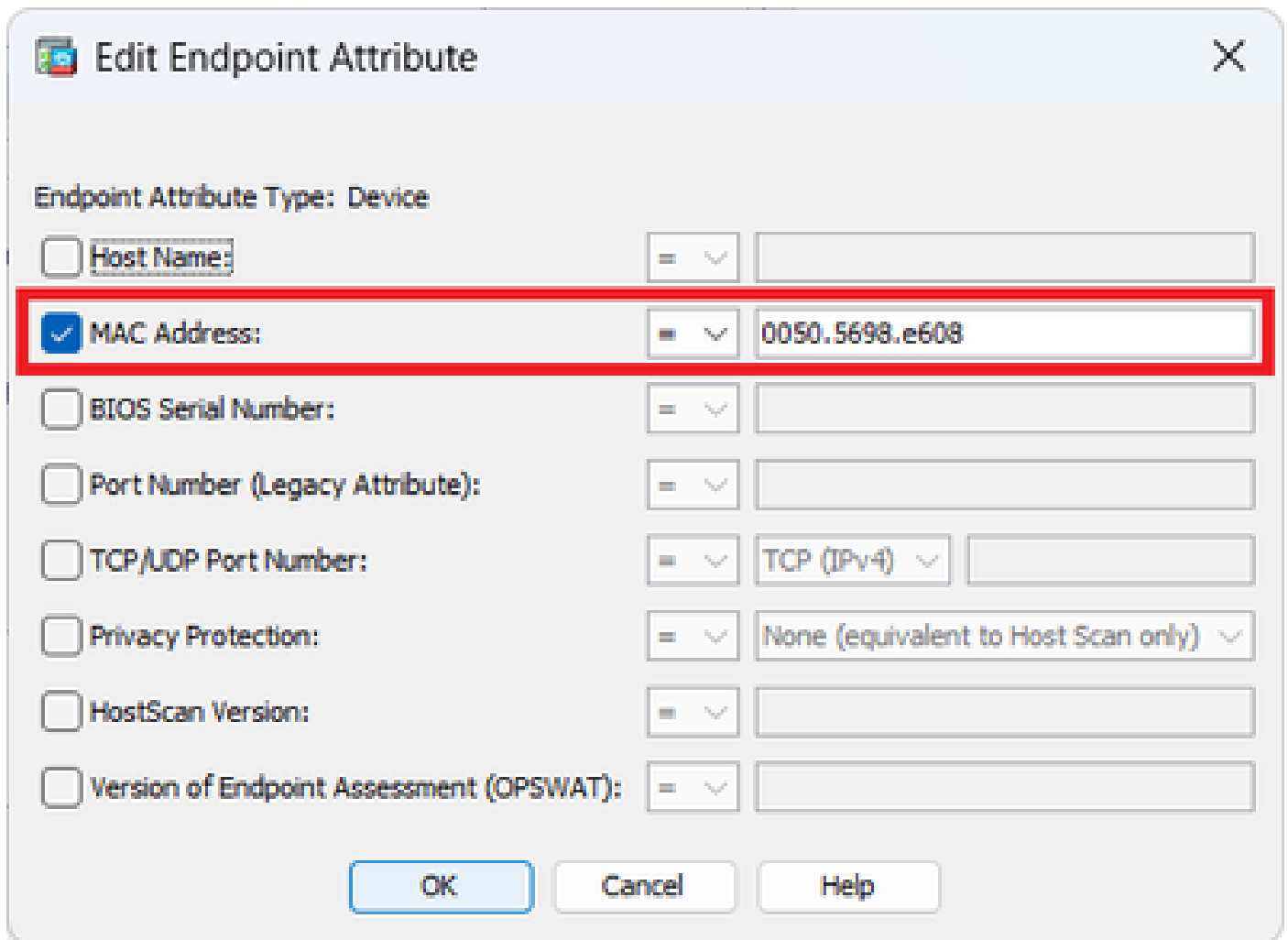
Username2: =

SCEP Required: = true

OK Cancel Help

DAP 레코드에 대한 그룹 정책 구성

엔드포인트 특성에 대한 MAC 주소를 구성합니다.

The image shows a dialog box titled "Edit Endpoint Attribute" with a close button (X) in the top right corner. Below the title bar, it says "Endpoint Attribute Type: Device". There are seven rows of attributes, 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. The "MAC Address" checkbox is checked, and its value is "0050.5698.e608". The other rows are: "Host Name:" (unchecked), "BIOS Serial Number:" (unchecked), "Port Number (Legacy Attribute):" (unchecked), "TCP/UDP Port Number:" (unchecked, with a dropdown menu set to "TCP (IPv4)"), "Privacy Protection:" (unchecked, with a dropdown menu set to "None (equivalent to Host Scan only)"), "HostScan Version:" (unchecked), and "Version of Endpoint Assessment (OPSWAT):" (unchecked). At the bottom, there are three buttons: "OK", "Cancel", and "Help".

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

DAP에 대한 MAC 조건 구성

2. 02_dap_test라는 두 번째 DAP를 구성합니다.

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
<u>disco.grouppolicy</u>	<u>= dap_test_gp</u>	<u>device</u>	<u>MAC["0050.5698.e605"] = true</u>

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

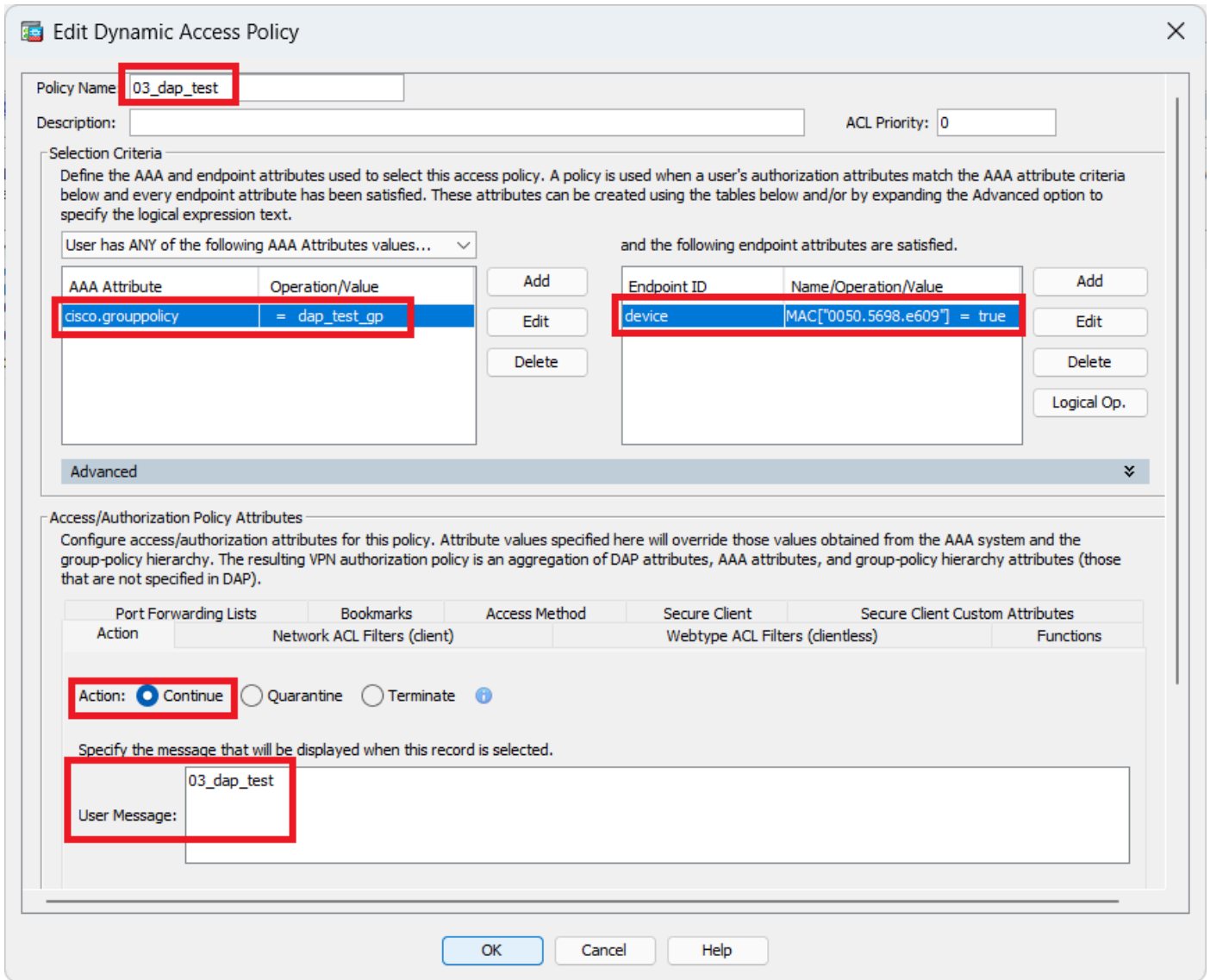
Specify the message that will be displayed when this record is selected.

User Message: 02_dap_test

OK Cancel Help

두 번째 DAP 구성

3. 03_dap_test라는 세 번째 DAP를 구성합니다.



세 번째 DAP 구성

4. `dap. more flash:/dap.xml` xml에서 DAP 레코드의 설정을 확인하려면 명령을 사용합니다.

ASDM에 설정된 DAP 레코드의 세부 정보는 ASA 플래시에 `dap.xml`로 저장됩니다. 이러한 설정이 완료되면 `dap.xml`에서 3개의 DAP 레코드가 생성됩니다. `dap.xml`에서 각 DAP 레코드의 세부 정보를 확인할 수 있습니다.

참고: 일치하는 DAP의 순서는 dap.xml의 표시 순서입니다. 기본 DAP(DfltAccessPolicy)가 마지막으로 일치합니다.

```
<#root>
```

```
ciscoasa#
```

```
more flash:/dap.xml
```

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

```
01_dap_test
```

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

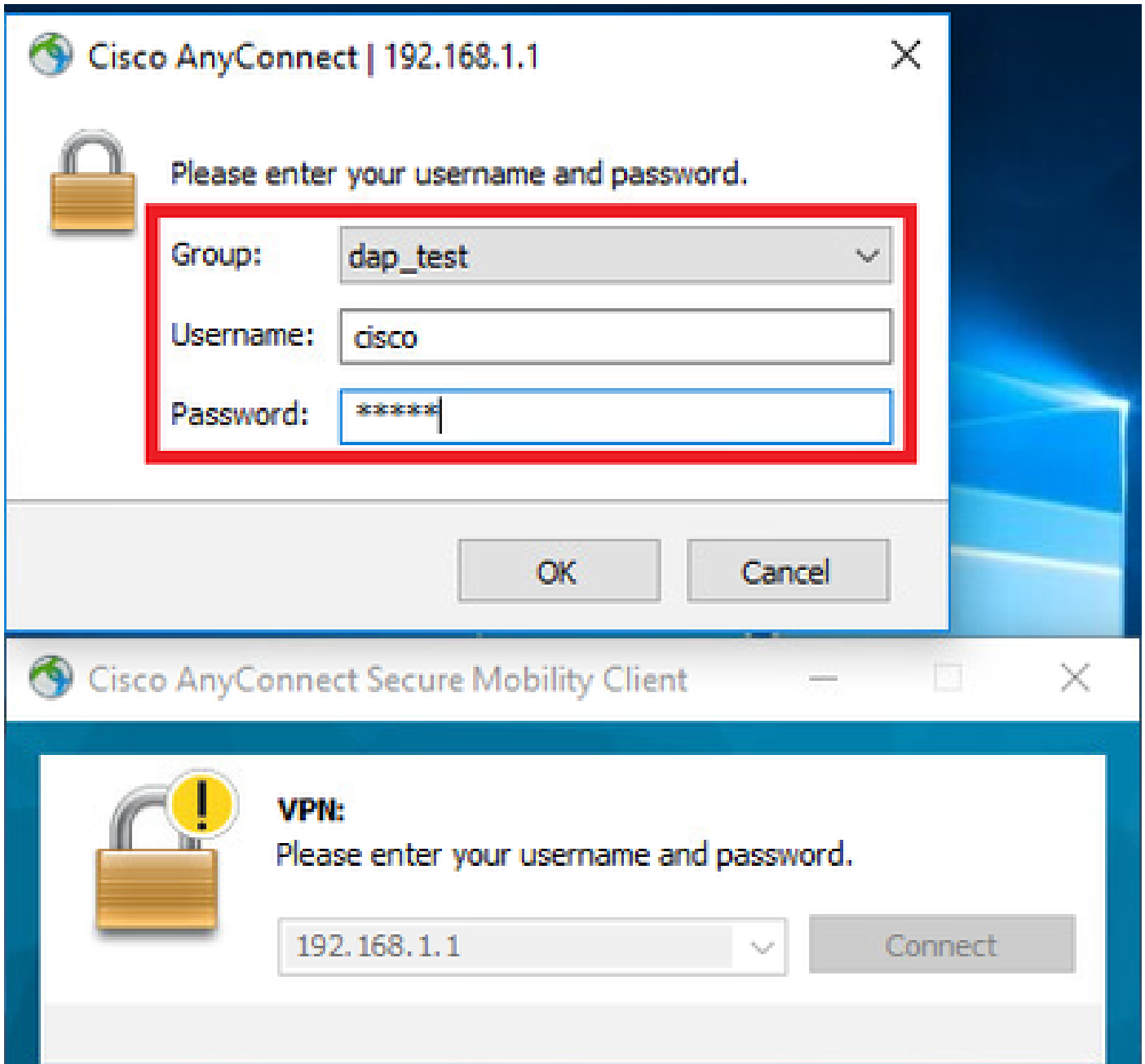
```
dap_test_gp
```

```
</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
```

다음을 확인합니다.

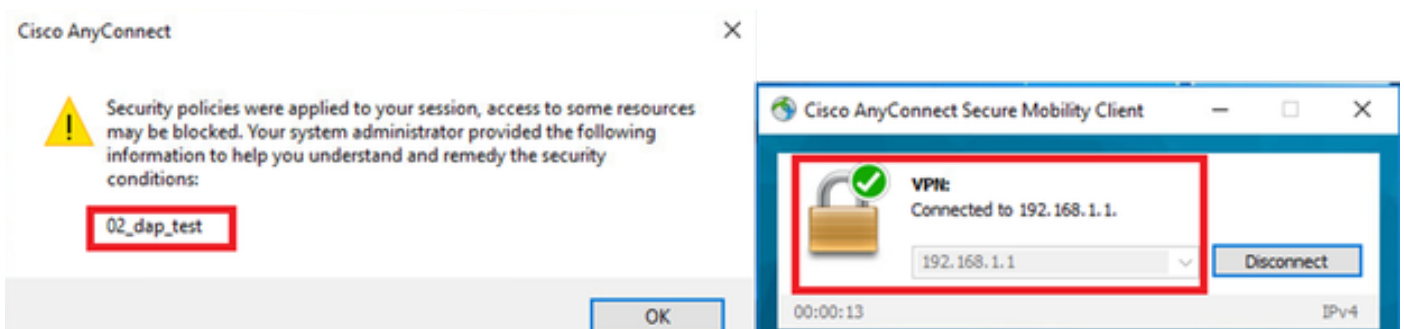
시나리오 1. 하나의 DAP만 일치함

1. 엔드포인트의 MAC가 02_dap_test의 MAC 조건과 일치하는 0050.5698.e605인지 확인합니다.
2. 엔드포인트에서 Anyconnect 연결을 실행하고 사용자 이름과 비밀번호를 입력합니다.



사용자 이름 및 비밀번호 입력

3. Anyconnect UI에서 O2_dap_test가 일치하는지 확인합니다.



UI에서 사용자 메시지 확인

4. ASA syslog에서 O2_dap_test가 일치하는지 확인합니다.

참고: ASA에서 debug dap trace가 활성화되어 있는지 확인합니다.

<#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
```

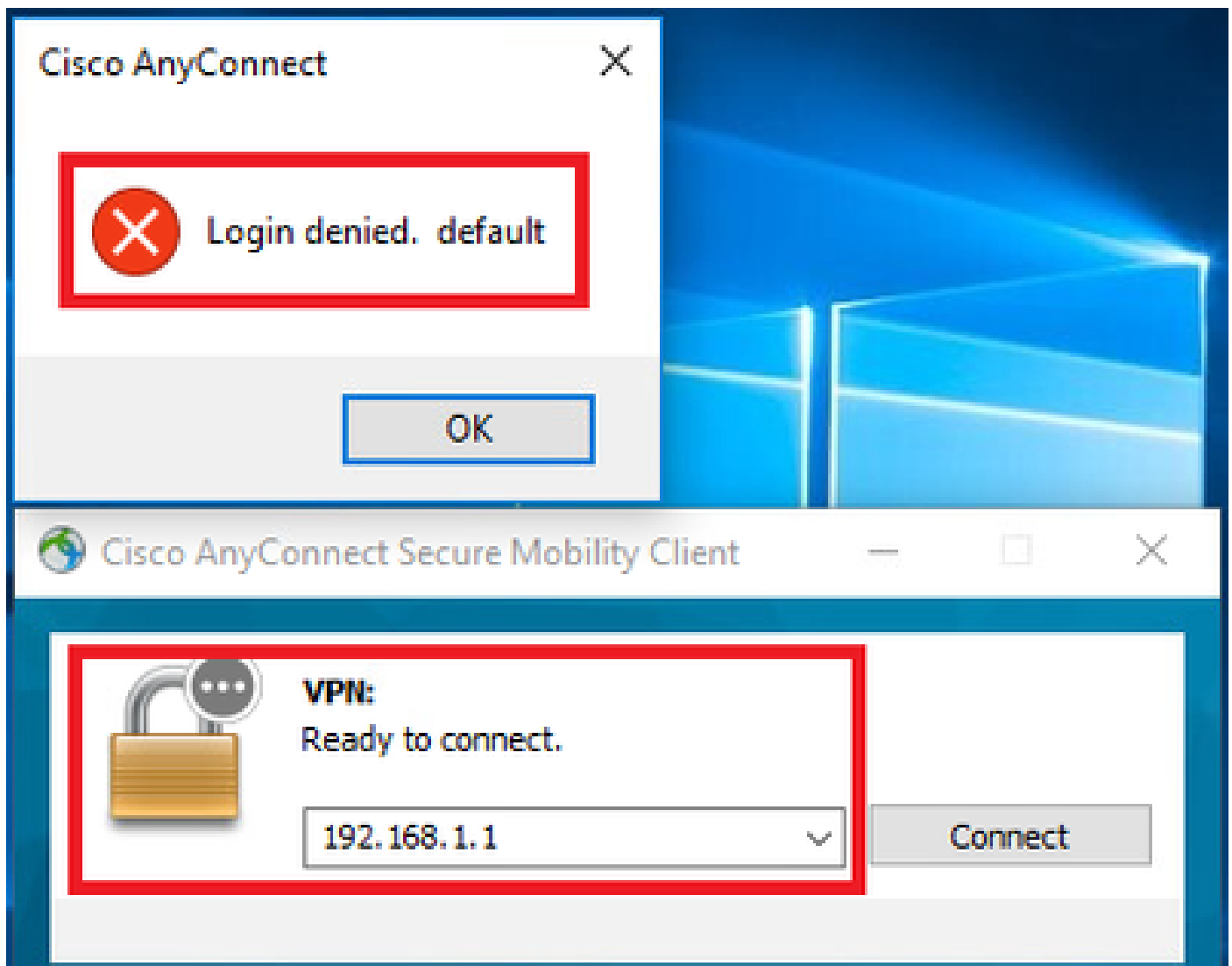
```
Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 11:46:11: %ASA-4-711001: I
```

시나리오 2. 기본 DAP가 일치함

1. 02_dap_test의 endpoint.device.MAC 값을 엔드포인트의 MAC과 일치하지 않는 0050.5698.e607로 변경합니다.

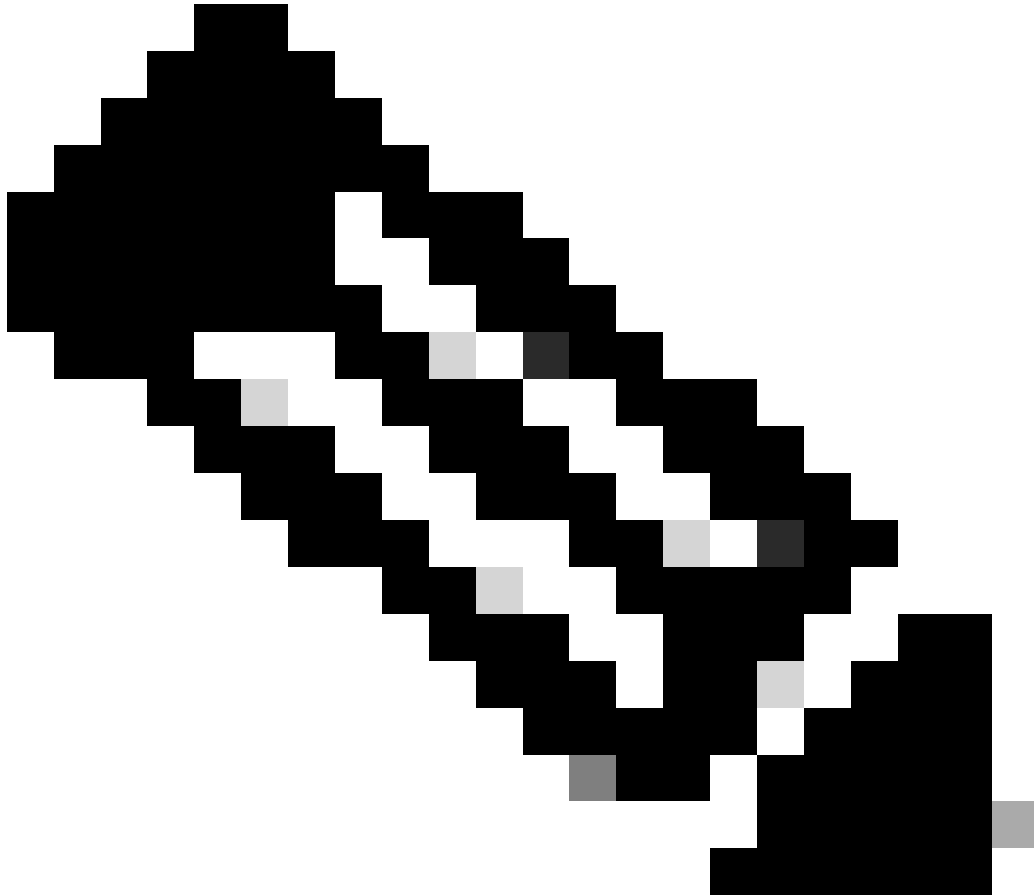
2. 엔드포인트에서 Anyconnect 연결을 실행하고 사용자 이름과 비밀번호를 입력합니다.

3. Anyconnect 연결이 거부되었는지 확인합니다.



UI에서 사용자 메시지 확인

4. ASA syslog에서 DfltAccessPolicy가 일치하는지 확인합니다.



참고: 기본적으로 DfltAccessPolicy의 작업은 Terminate입니다.

<#root>

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

시나리오 3. 여러 DAP(작업: 계속)가 일치함

1. 각 DAP에서 작업과 특성을 변경합니다.

·01_dap_test:

dapSelection(MAC 주소) = endpoint.device.MAC[0050.5698.e605] = Anyconnect 엔드포인트의 MAC

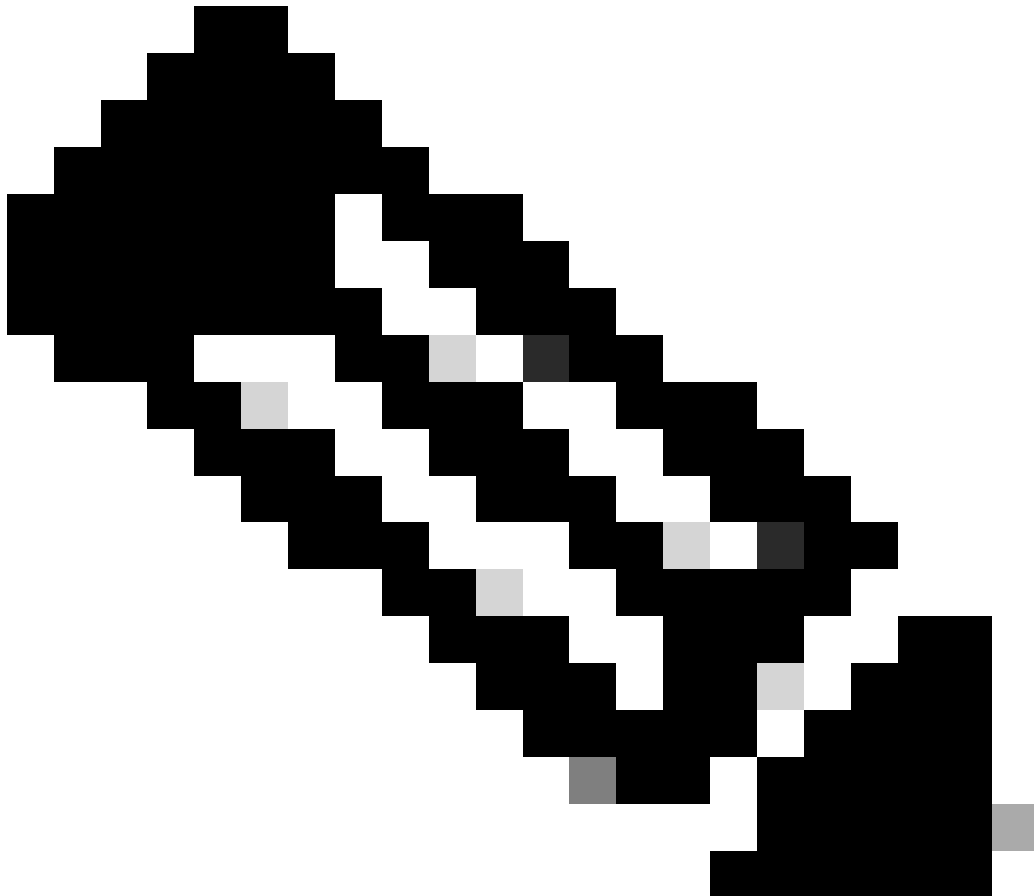
작업 = 계속

·02_dap_test:

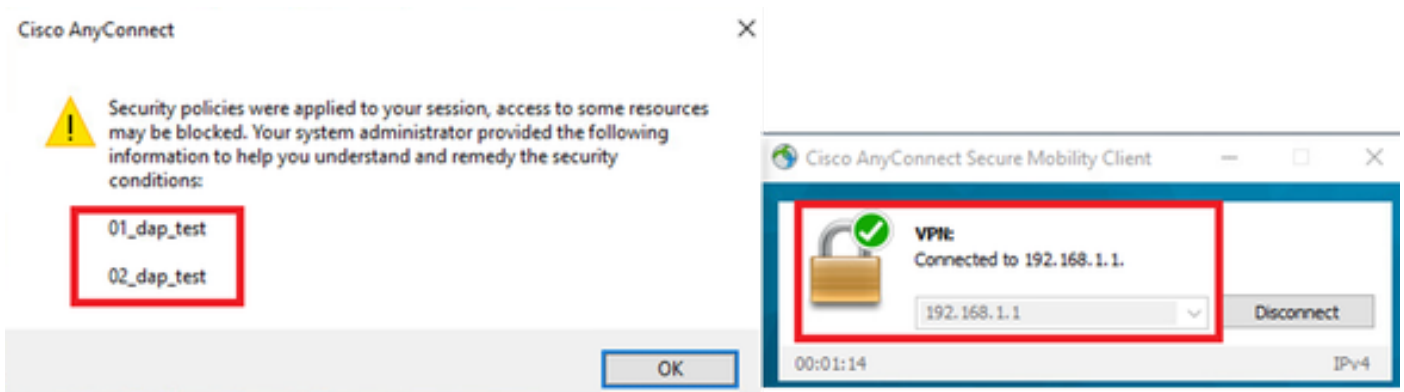
dapSelection(호스트 이름) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Anyconnect 엔드포인트의 호스트 이름
작업 = 계속
·03_dap_test DAP 레코드 삭제

2. 엔드포인트에서 Anyconnect 연결을 실행하고 사용자 이름과 비밀번호를 입력합니다.

3. Anyconnect UI에서 2개의 DAP가 모두 일치하는지 확인합니다



참고: 연결이 여러 DAP와 일치하는 경우 여러 DAP의 사용자 메시지가 통합되어 Anyconnect UI에 함께 표시됩니다.



UI에서 사용자 메시지 확인

4. ASA syslog에서 2개의 DAP가 모두 일치하는지 확인합니다.

<#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

시나리오 4. 여러 DAP(작업:종료)가 일치함

1. 01_dap_test 작업을 변경합니다.

·01_dap_test:

dapSelection(MAC 주소) = endpoint.device.MAC[0050.5698.e605] = Anyconnect 엔드포인트의 MAC

작업 = 종료

·02_dap_test:

dapSelection(호스트 이름) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Anyconnect 엔드포인트의 호스트 이름

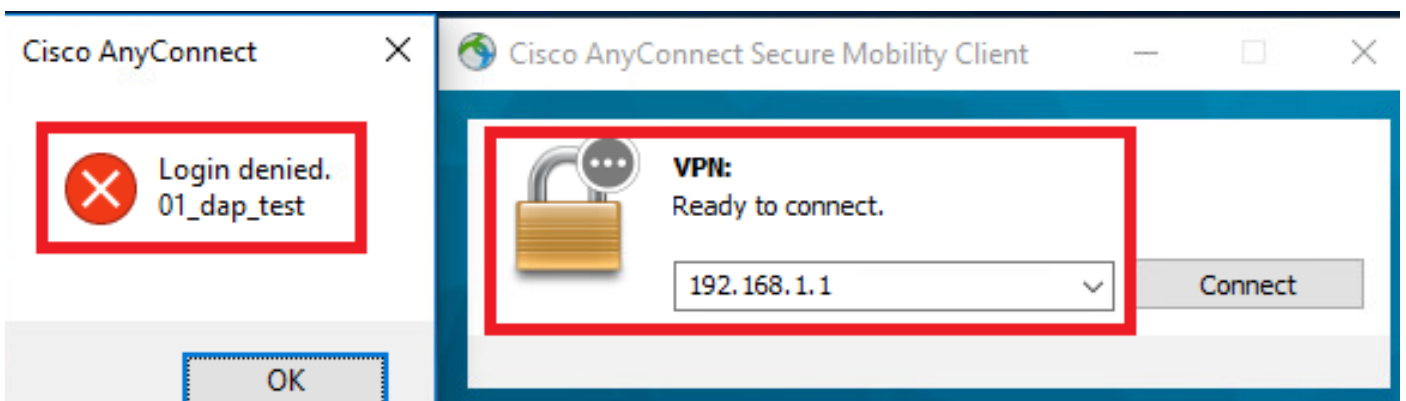
작업 = 계속

2. 엔드포인트에서 Anyconnect 연결을 실행하고 사용자 이름과 비밀번호를 입력합니다.

3. Anyconnect UI에서 01_dap_test만 일치하는지 확인합니다.



참고: 종료 작업으로 설정된 DAP 레코드와 일치하는 연결. 종료 작업 후 후속 레코드가 더 이상 일치하지 않습니다.



UI에서 사용자 메시지 확인

4. ASA syslog에서 01_dap_test만 일치하는지 확인합니다.

<#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
```

일반 문제 해결

이러한 디버그 로그는 ASA에서 DAP의 세부 동작을 확인하는 데 도움이 됩니다.

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-
```

관련 정보

<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>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.