Deploy ASA DAP to Identify MAC Address for AnyConnect

Contents

Introduction

This document describes how to configure Dynamic Access Policies (DAP) via ASDM, to check Mac Address of the device used for AnyConnect connection.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:
Configuration of Cisco Anyconnect and Hostscan

Components Used

The information in this document is based on these software and hardware versions:
ASAv 9.18 (4)
ASDM 7.20 (1)
Anyconnect 4.10.07073
Hostscan 4.10.07073
Windows 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure

that you understand the potential impact of any command.

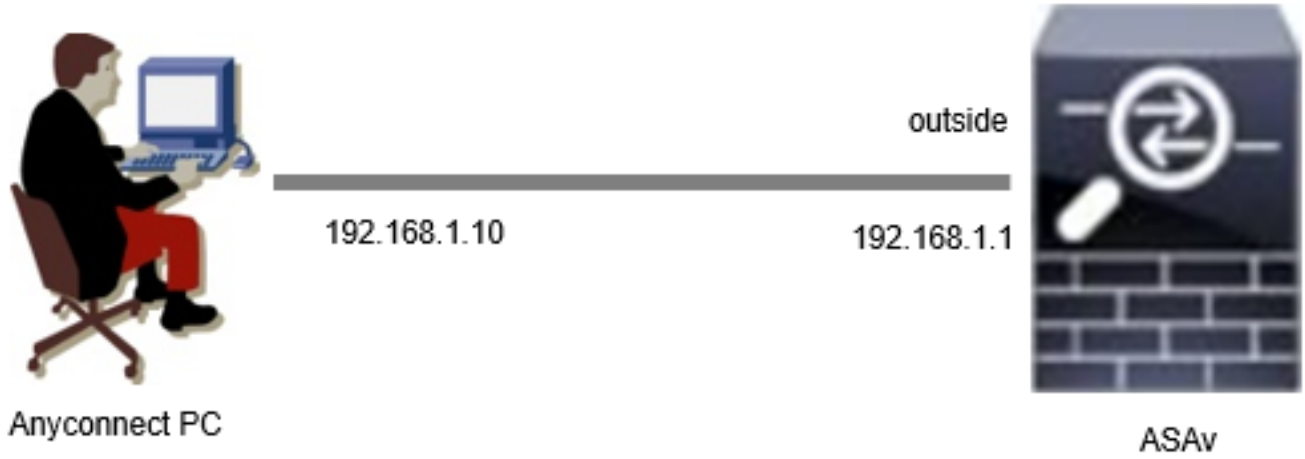
Background Information

HostScan is a software module that provides the AnyConnect Secure Mobility Client the ability to enforce security policies on the network. During the process of Hostscan, various details about the client device are gathered and reported back to the Adaptive Security Appliance (ASA). These details include the device operating system, antivirus software, firewall software, MAC address, and more. Dynamic Access Policies (DAP) feature allows network administrators to configure security policies on a per-user basis, the endpoint.device.MAC attribute in DAP can be used to match or check the MAC address of the client device against predefined policies.

Configure

Network Diagram

This image shows the topology that is used for the example of this document.



Diagram

Configuration in ASA

This is the minimal configuration 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
```

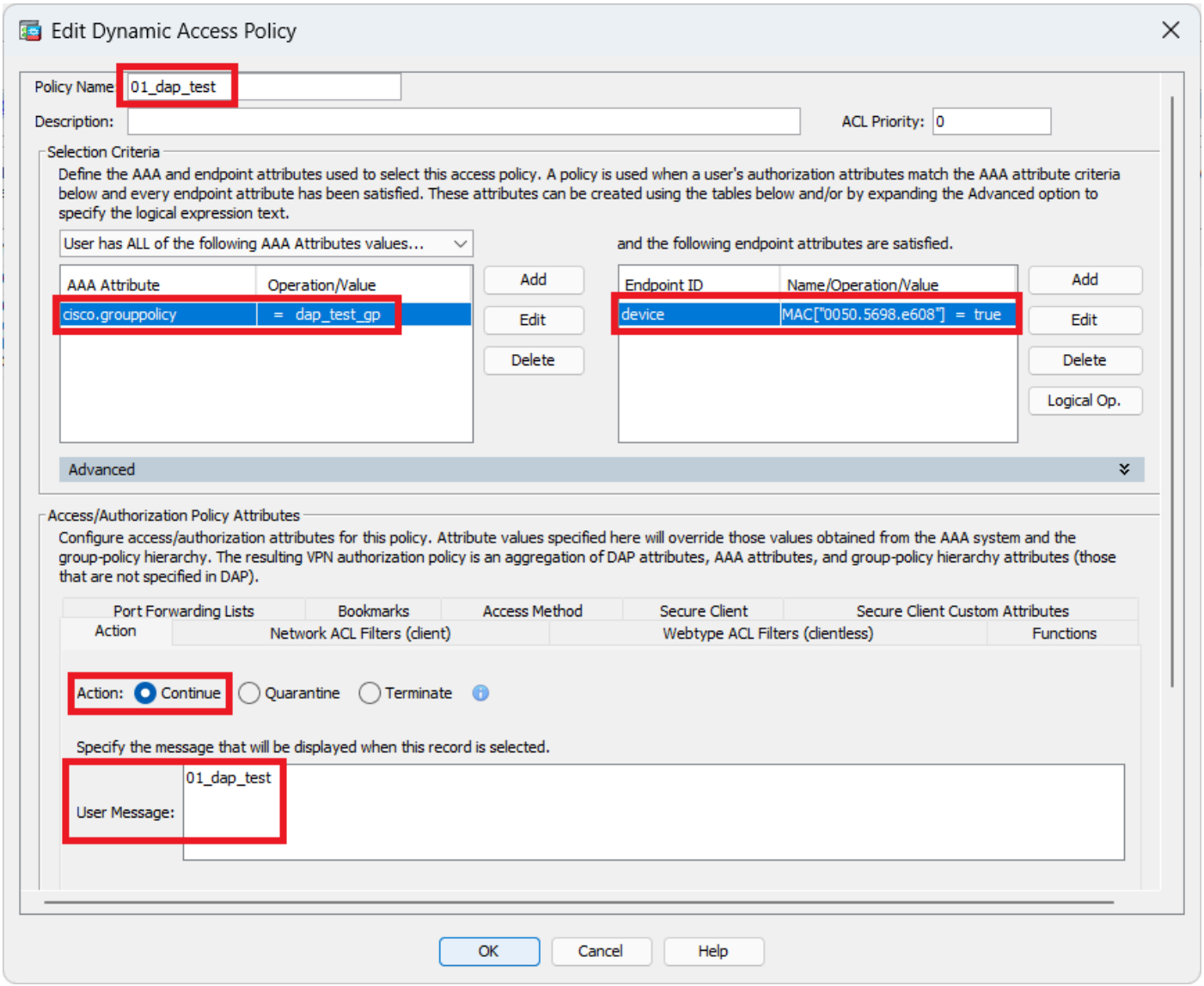
Configuration in ASDM

This section describes how to configure DAP record in ASDM. In this example, set 3 DAP records which using endpoint.device.MAC attribute as an condition.

- 01_dap_test：endpoint.device.MAC=0050.5698.e608
- 02_dap_test：endpoint.device.MAC=0050.5698.e605 = MAC of Anyconnect Endpoint
- 03_dap_test：endpoint.device.MAC=0050.5698.e609

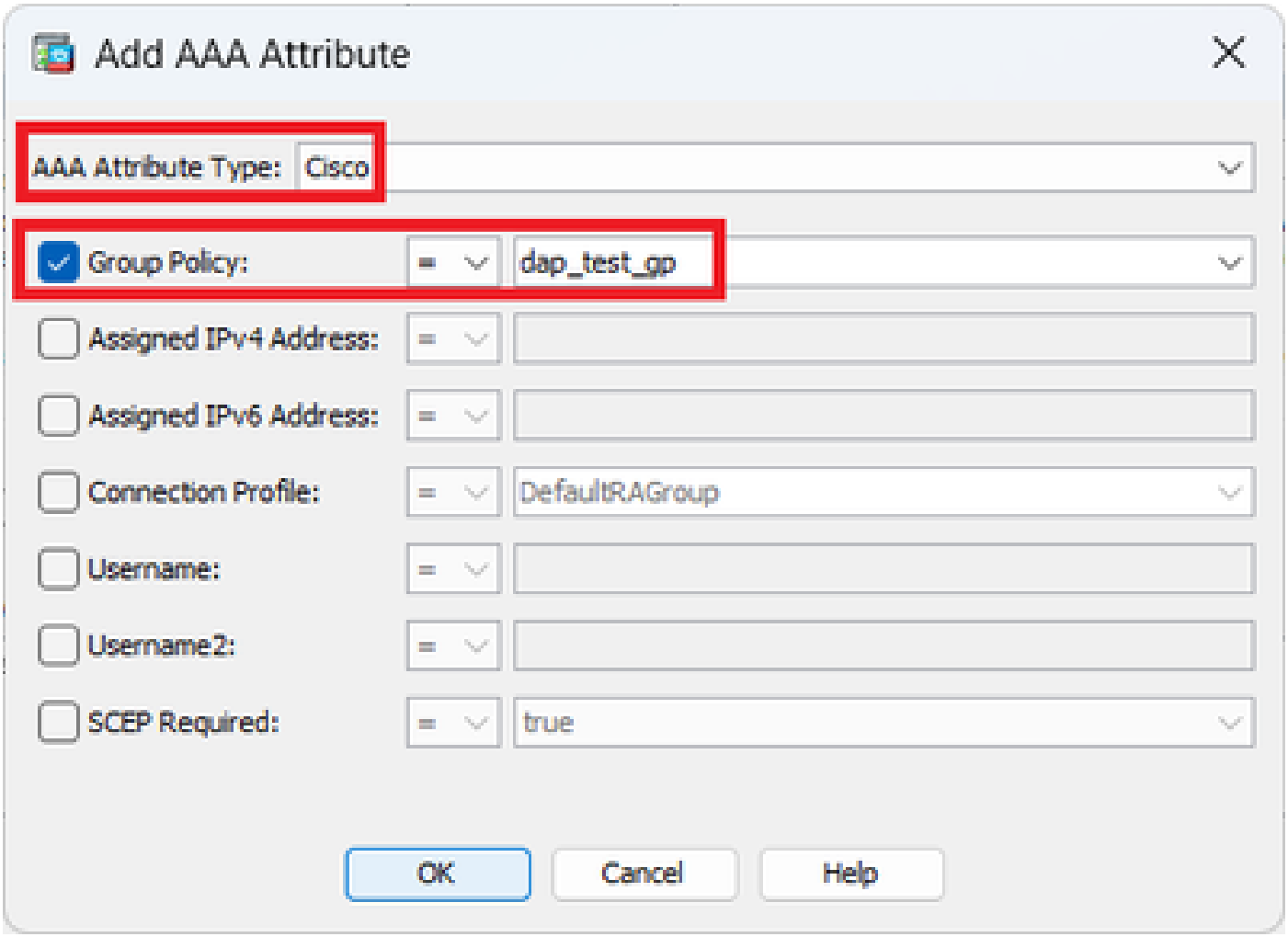
1. Configure first DAP named 01_dap_test.

Navigate to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Dynamic Access Policies**. Click **Add** , and set the **Policy Name**, **AAA Attribute**, **endpoint attributes**, **Action**, **User Message**, as shown in the image:



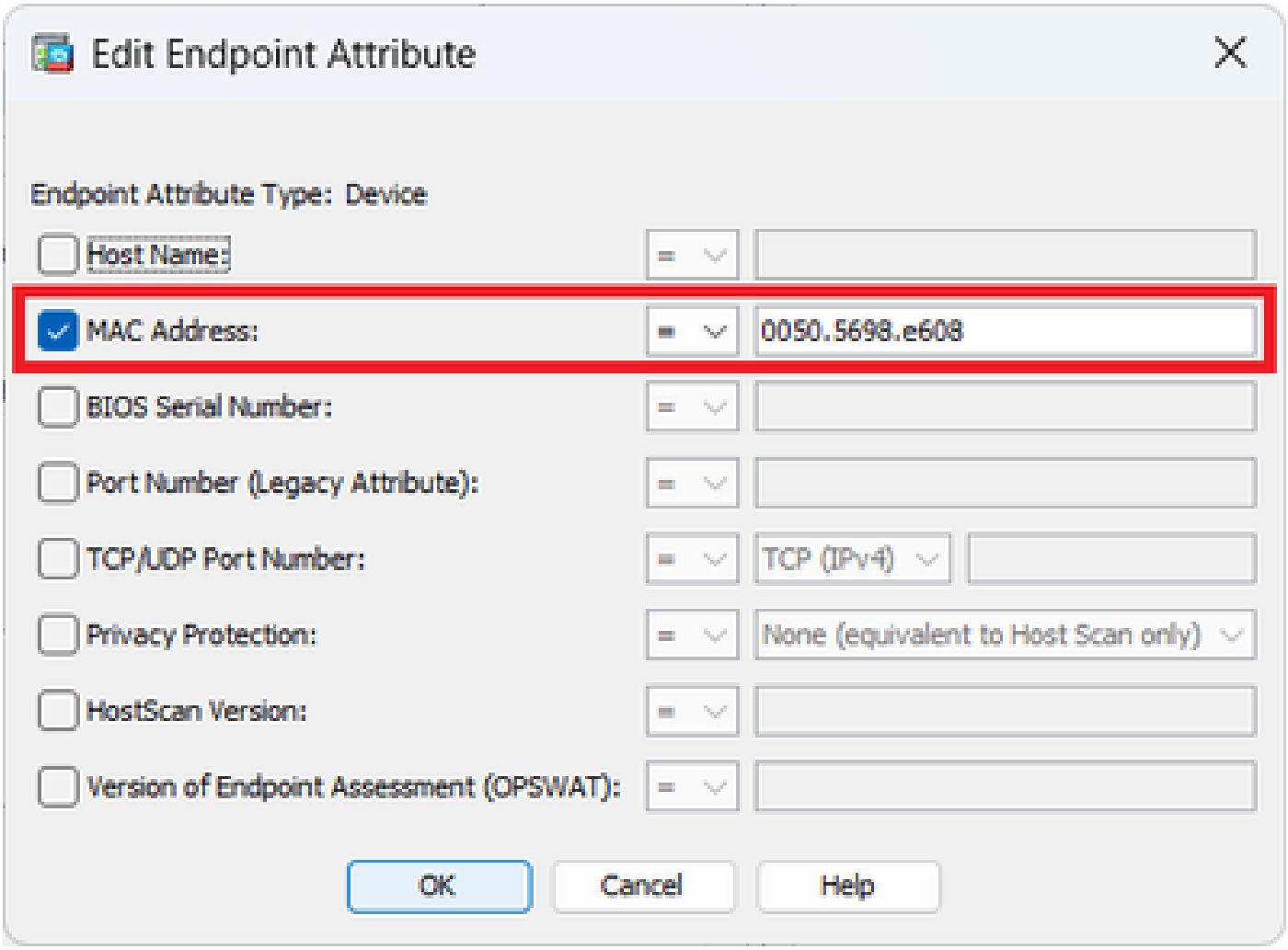
Configure First DAP

Configure **Group Policy** for AAA Attribute.



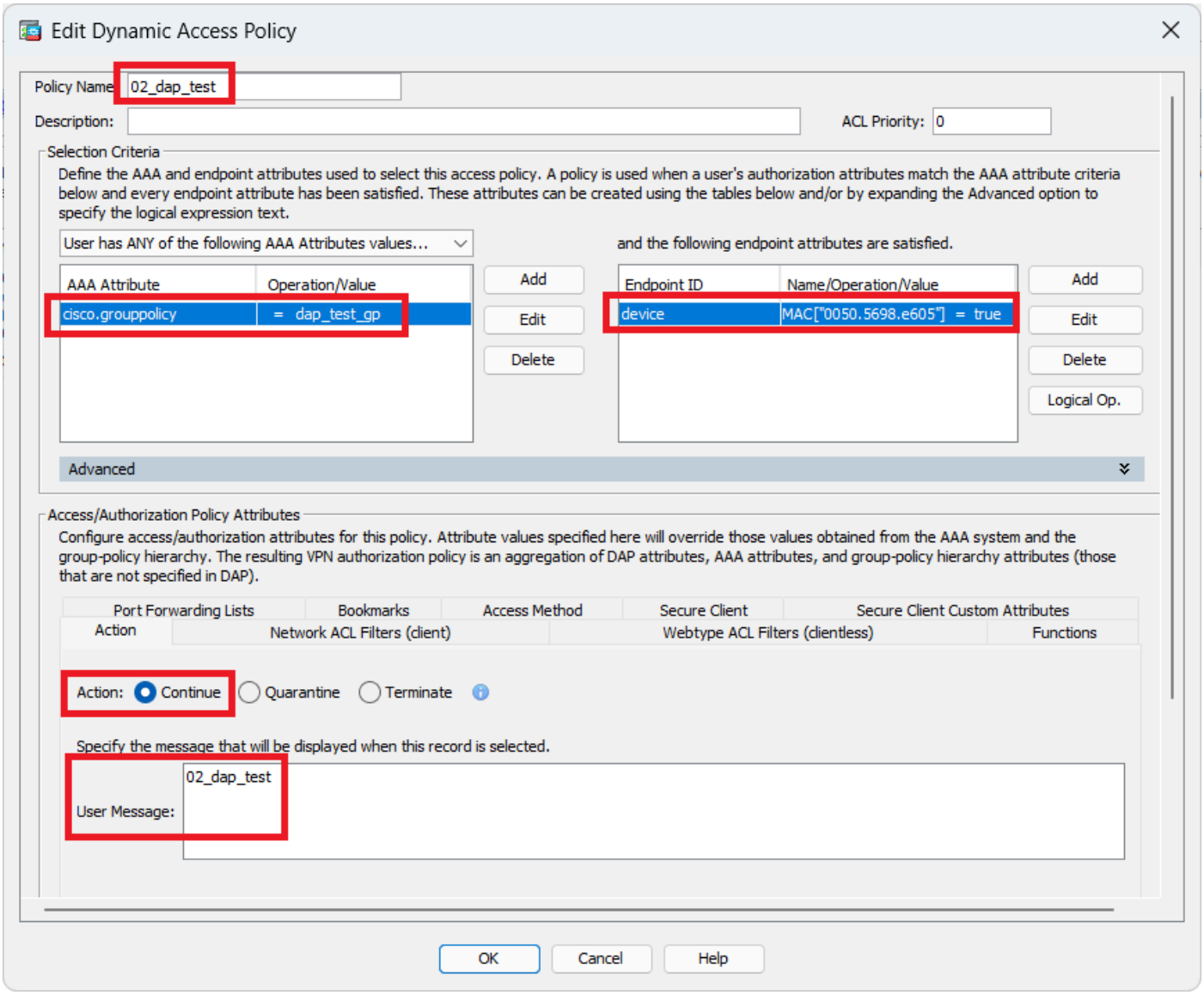
Configure Group Policy For DAP Record

Configure **MAC Address** for Endpoint Attribute.



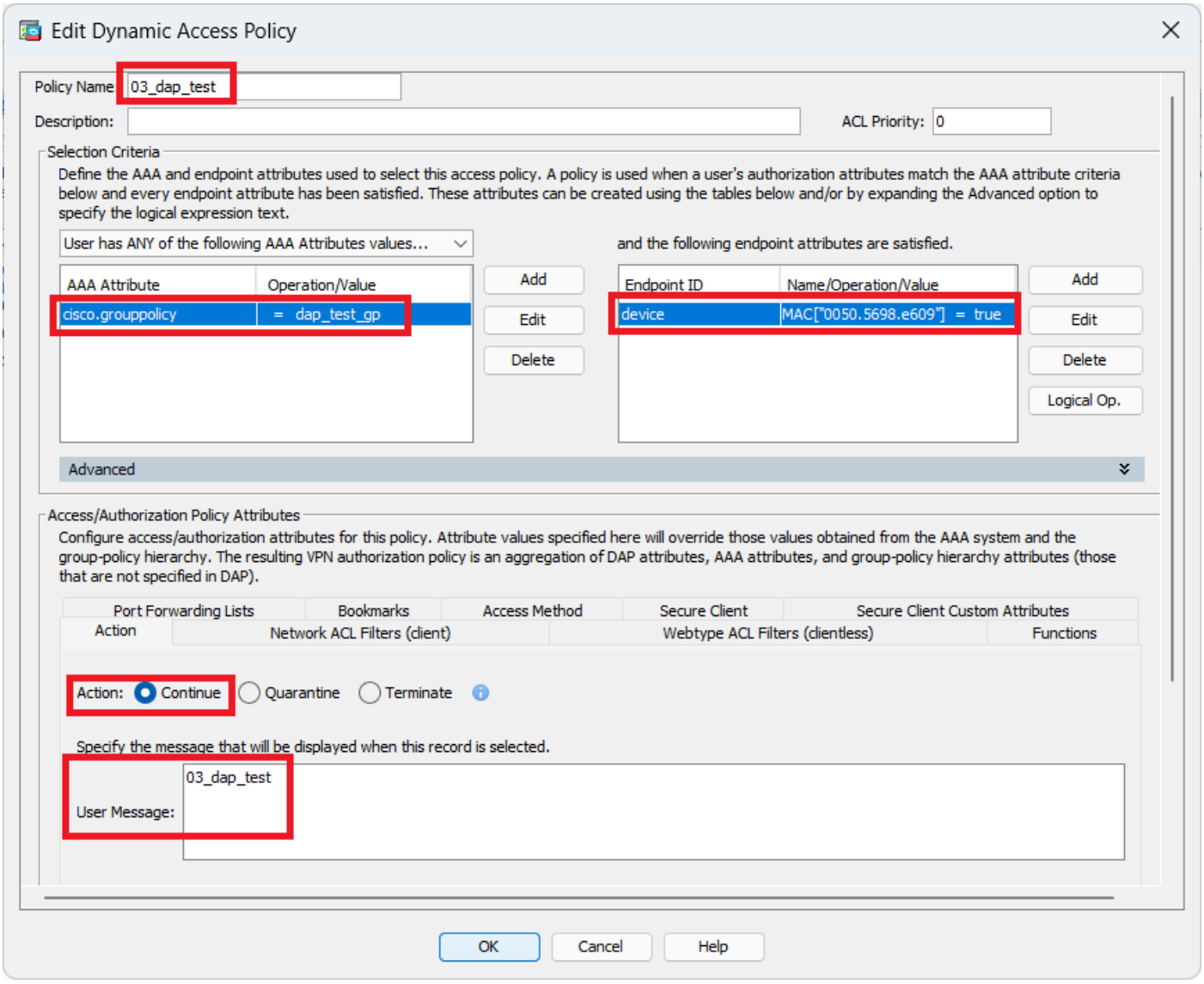
Configure MAC Condition For DAP

2. Configure second DAP named **02_dap_test**.



Configure Second DAP

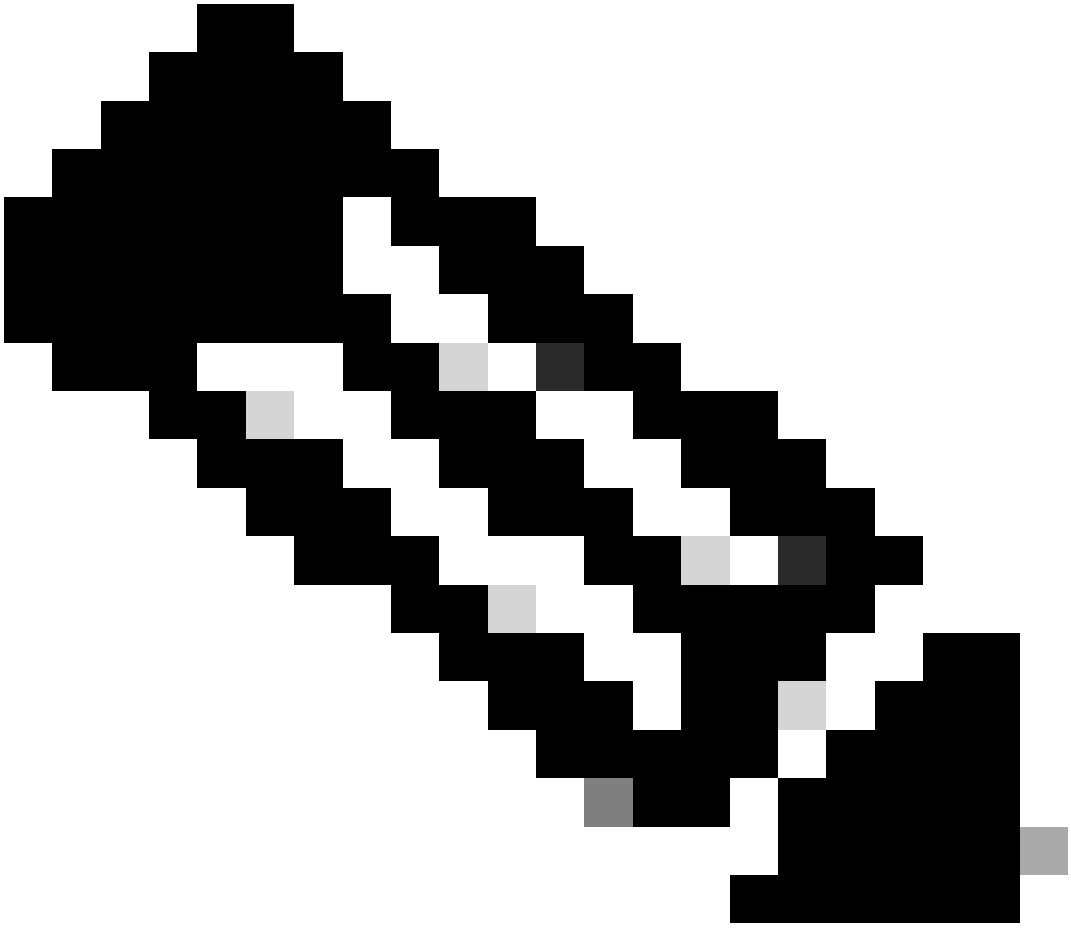
3. Configure third DAP named **03_dap_test**.



Configure Third DAP

4. Use **more flash:/dap.xml** command to confirm the setting of DAP records in dap.xml.

Details of the DAP records set on ASDM is saved in the ASA flash as dap.xml. After these settings are completed, three DAP records are generated in dap.xml. You can confirm the details of each DAP record in dap.xml.



Note: The order in which DAP being matched is the display order in dap.xml. The default DAP (DfltAccessPolicy) is last matched.

<#root>

ciscoasa#

more flash:/dap.xml

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

01_dap_test

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

```
<dapSelection>
<dapPolicy>
<value>match-all</value>
</dapPolicy>
<attr>
<name>aaa.cisco.grouppolicy</name>
<value>
```

dap_test_gp

```
</value>                              <--- 1st DAP group policy
<operation>EQ</operation>
<type>caseless</type>
</attr>
</dapSelection>
<dapSelection>
<dapPolicy>
<value>match-any</value>
</dapPolicy>
<dapSubSelection>
<dapPolicy>
<value>match-all</value>
</dapPolicy>
<attr>
<name>
```

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

```
</name>     <--- 1st DAP MAC Address condition
<value>true</value>
<type>caseless</type>
<operation>EQ</operation>
</attr>
</dapSubSelection>
</dapSelection>
</dapBasicView>
</dapRecord>
<dapRecord>
<dapName>
<value>
```

02_dap_test

```
</value>                               <--- 2nd DAP name
</dapName>
<dapViewsRelation>
<value>and</value>
</dapViewsRelation>
<dapBasicView>
<dapSelection>
<dapPolicy>
<value>match-any</value>
</dapPolicy>
<attr>
<name>aaa.cisco.grouppolicy</name>
<value>
```

dap_test_gp

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

```
<dapSelection>
<dapPolicy>
<value>match-any</value>
</dapPolicy>
<dapSubSelection>
<dapPolicy>
<value>match-all</value>
</dapPolicy>
<attr>
<name>
```

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

```
</name>      <--- 2nd DAP MAC Address condition
<value>true</value>
<type>caseless</type>
<operation>EQ</operation>
</attr>
</dapSubSelection>
</dapSelection>
</dapBasicView>
</dapRecord>
<dapRecord>
<dapName>
<value>
```

03_dap_test

```
</value>                              <--- 3rd DAP name
</dapName>
<dapViewsRelation>
<value>and</value>
</dapViewsRelation>
<dapBasicView>
<dapSelection>
<dapPolicy>
<value>match-any</value>
</dapPolicy>
<attr>
<name>aaa.cisco.grouppolicy</name>
<value>
```

dap_test_gp

```
</value>                               <--- 3rd DAP group policy
<operation>EQ</operation>
<type>caseless</type>
</attr>
</dapSelection>
<dapSelection>
<dapPolicy>
<value>match-any</value>
</dapPolicy>
<dapSubSelection>
<dapPolicy>
<value>match-all</value>
</dapPolicy>
<attr>
<name>
```

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

```
</name>      <--- 3rd DAP MAC Address condition
<value>true</value>
```

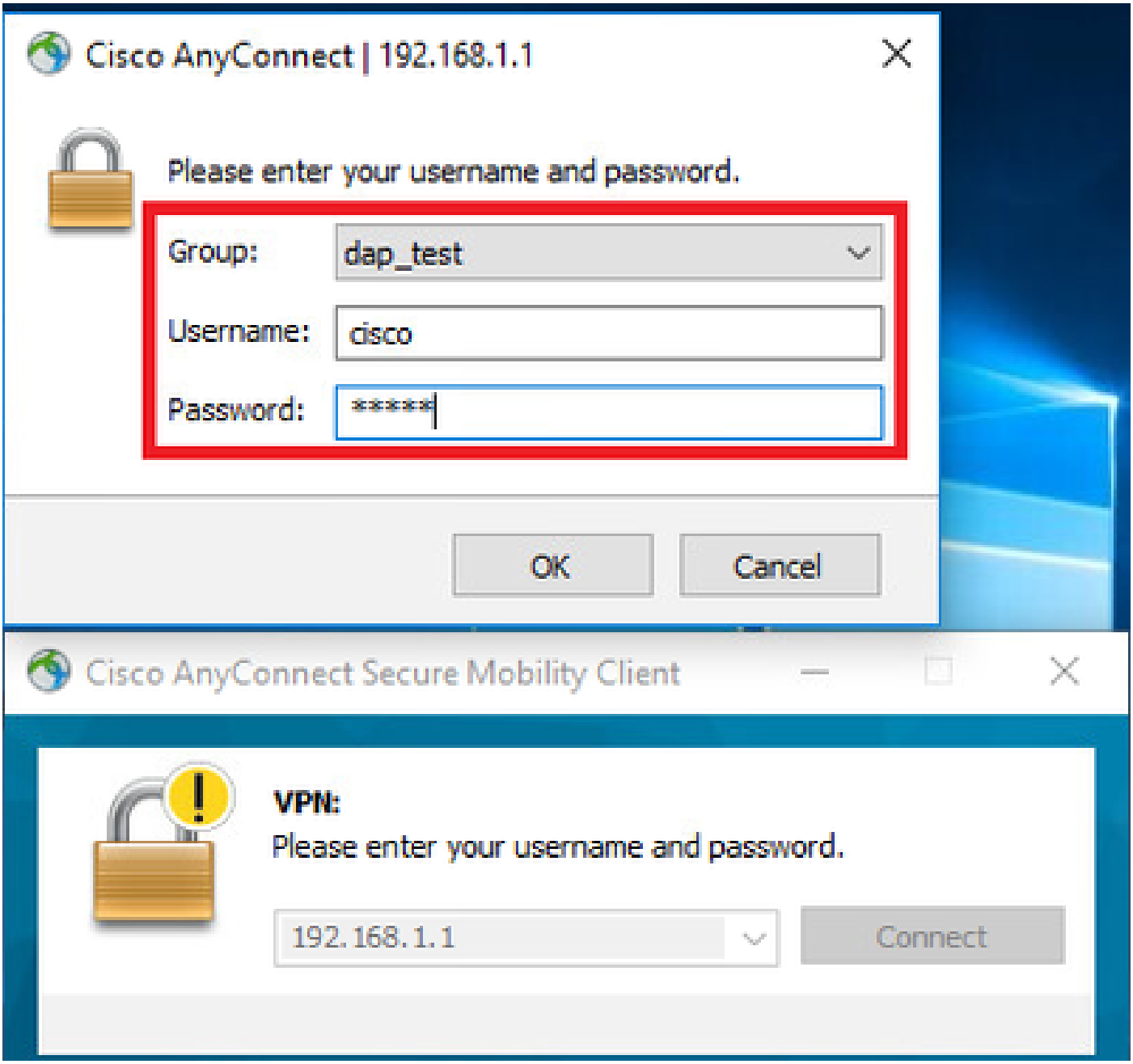
```
<type>caseless</type>
<operation>EQ</operation>
</attr>
</dapSubSelection>
</dapSelection>
</dapBasicView>
</dapRecord>
</dapRecordList>
```

Verify

Scenario1. Only one DAP is matched

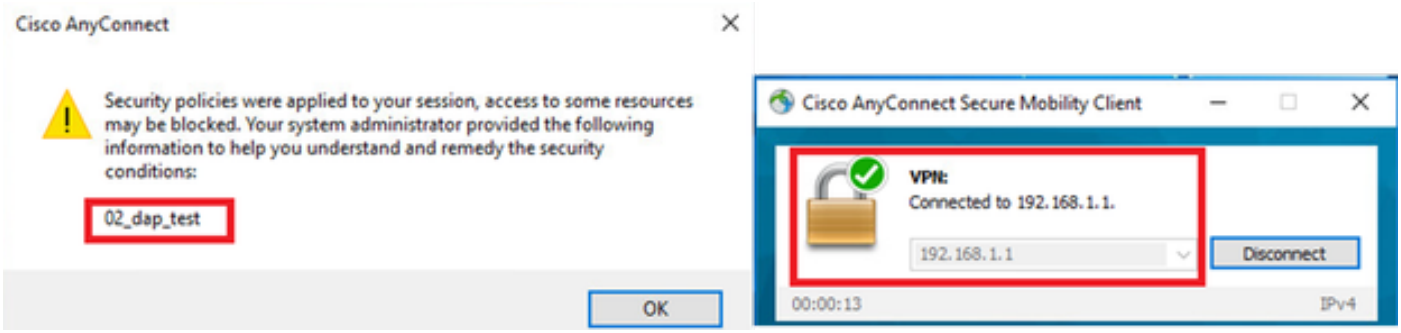
1. Ensure that the MAC of endpoint is 0050.5698.e605 which is matching MAC condition in 02_dap_test.

2. On endpoint, run Anyconnect connection and input username and password.



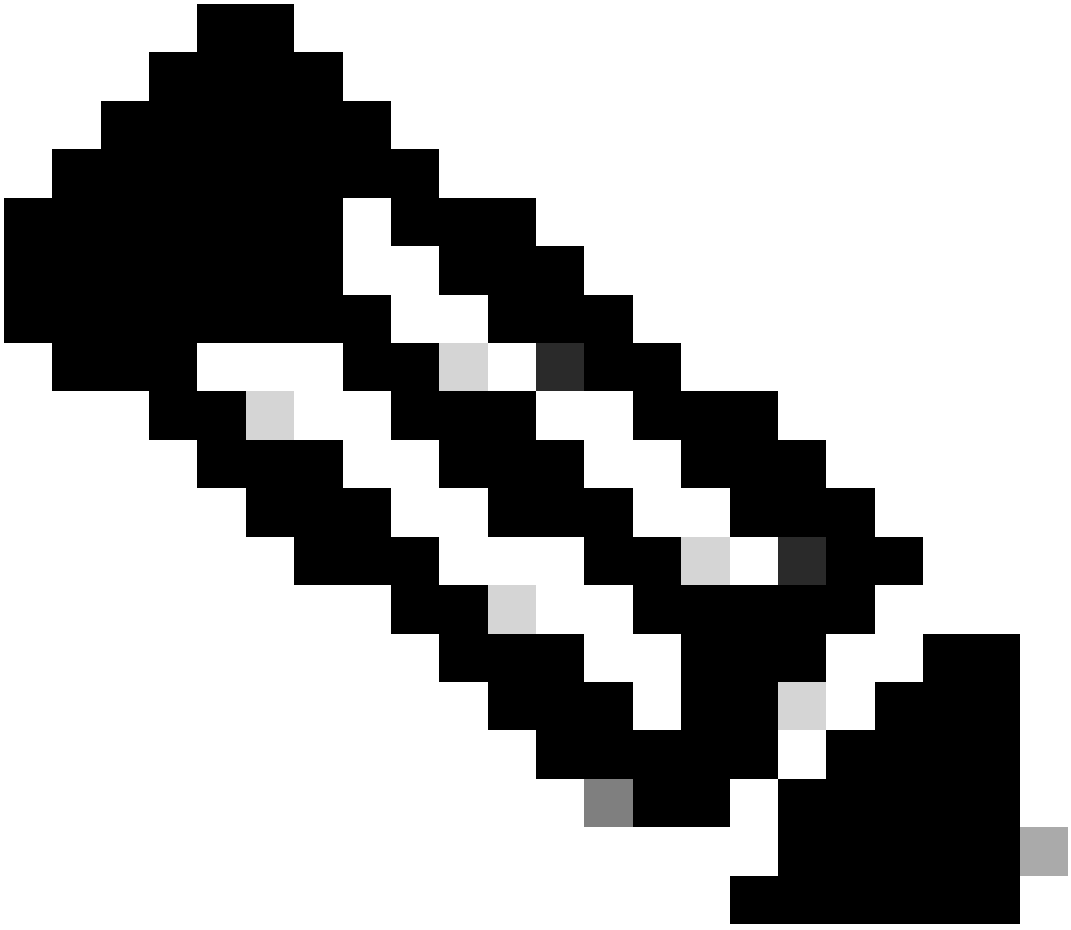
Input username and password

3. In the Anyconnect UI, confirm that 02_dap_test is matched.



Confirm User Message In UI

4. In the ASA syslog, confirm that 02_dap_test is matched.



Note: Ensure debug dap trace is enabled in 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

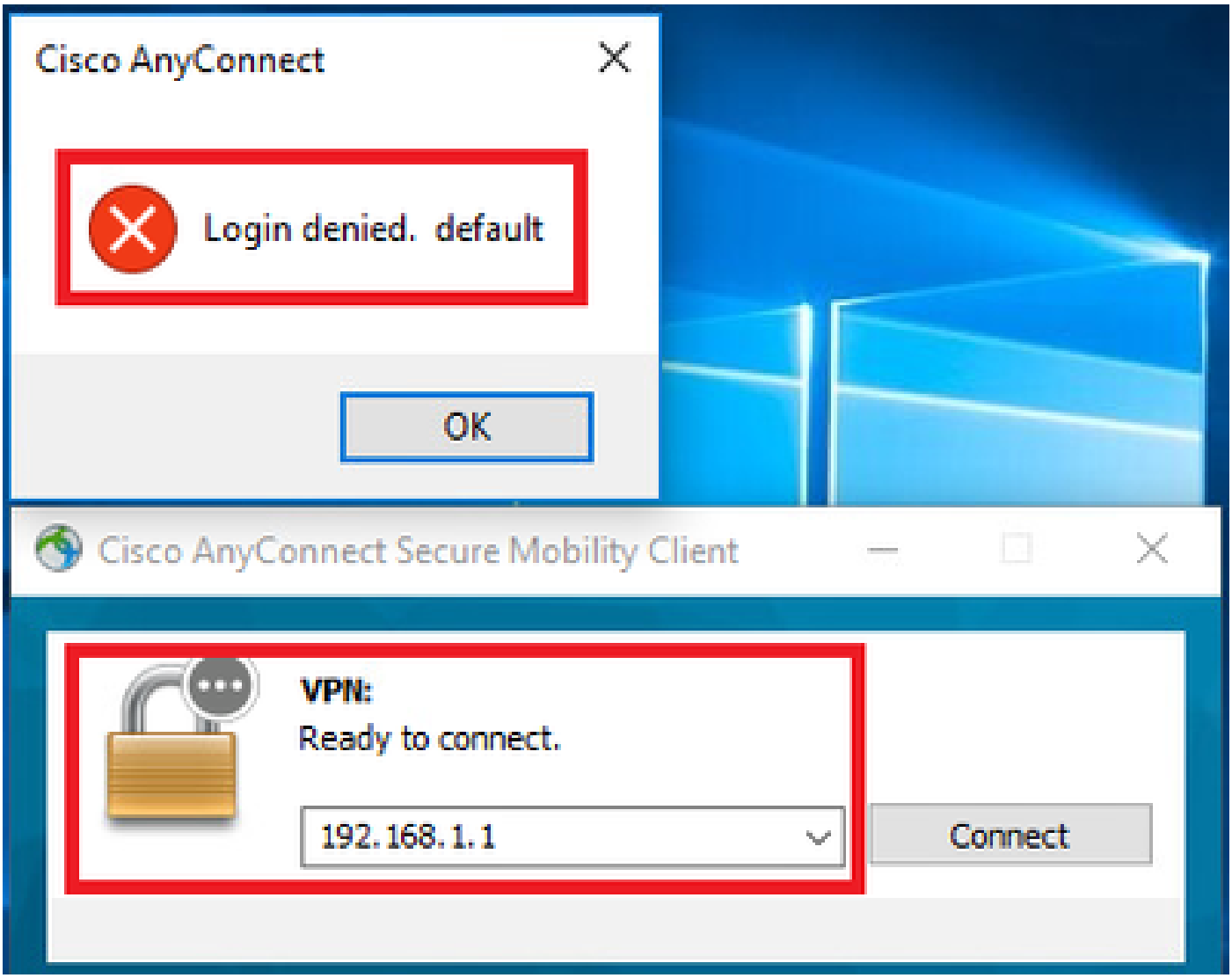
Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 11:46:11: %ASA-4-711001: DA

Scenario2. Default DAP is matched

1. Change the value of endpoint.device.MAC in 02_dap_test to 0050.5698.e607 which is not matching MAC of endpoint.

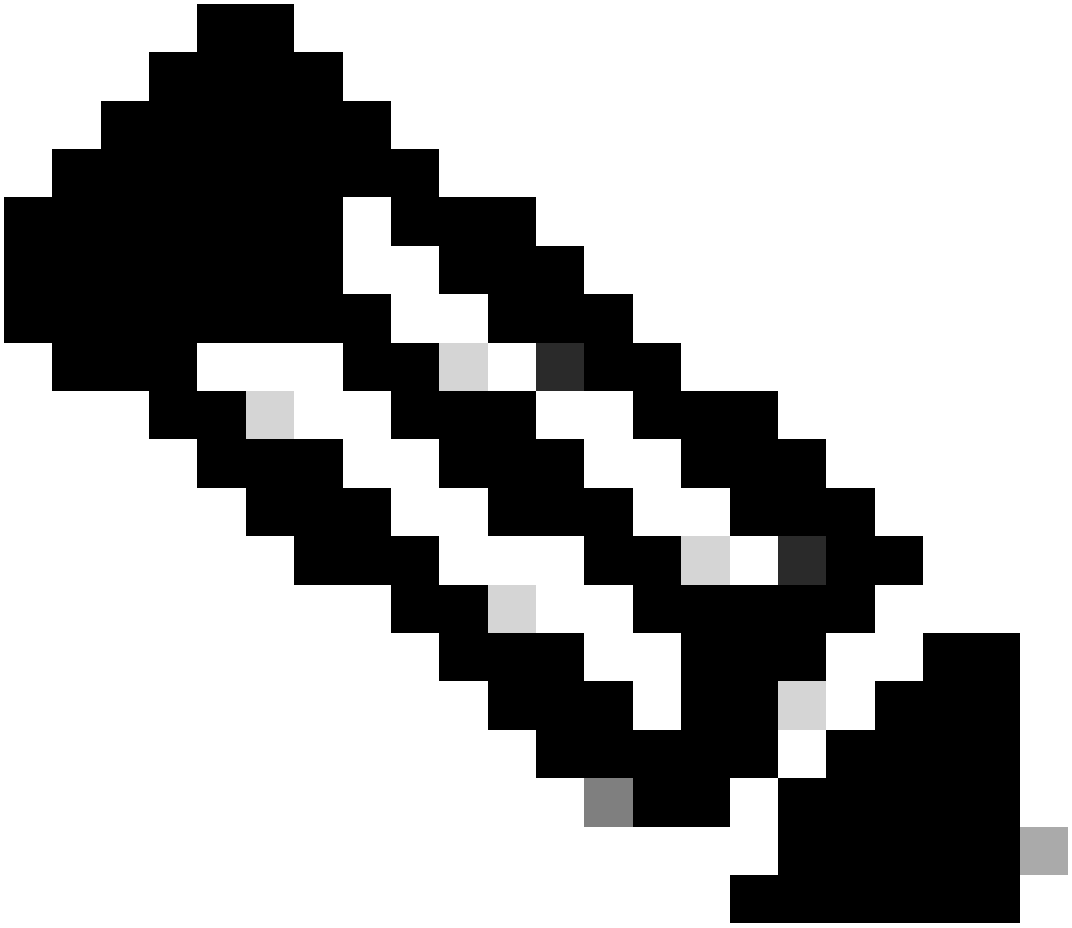
2. On endpoint, run Anyconnect connection and input username and password.

3. Confirm that the Anyconnect connection was denied.



Confirm User Message In UI

4. In the ASA syslog, confirm that DfltAccessPolicy is matched.



Note: By default , the action of DfltAccessPolicy is 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

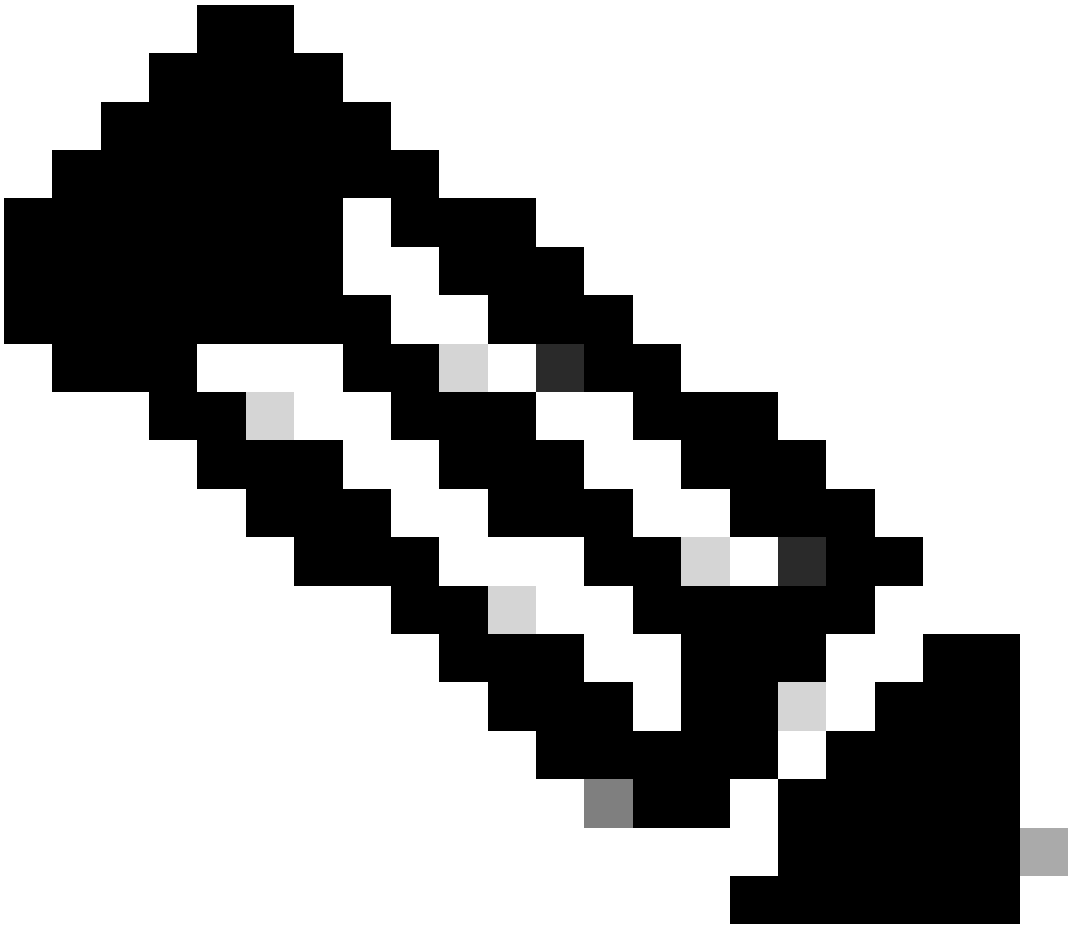
Scenario3. Multiple DAPs (Action : Continue) are matched

1. Change the action and attribute in each DAP.

- 01_dap_test :
  dapSelection (MAC Address) = endpoint.device.MAC[0050.5698.e605] = MAC of Anyconnect Endpoint
  Action = **Continue**
- 02_dap_test :
  dapSelection (Host Name) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Hostname of Anyconnect Endpoint
  Action = **Continue**
- Delete 03_dap_test DAP record

2. On endpoint, run Anyconnect connection and input username and password.

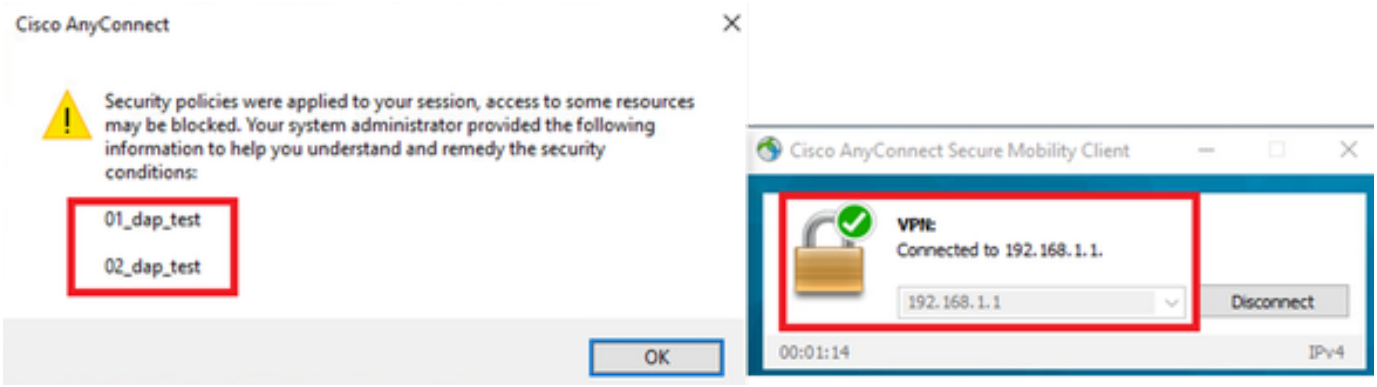
3. In the Anyconnect UI, confirm that all 2 DAPs are matched



Note: If an connection matches multiple DAPs, the user messages of multiple DAPs being

---

integrated and displayed together in Anyconnect UI.



Confirm User Message In UI

4. In the ASA syslog, confirm that all 2 DAPs are matched.

<#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

Scenario4. Multiple DAPs (Action :Terminate) are matched

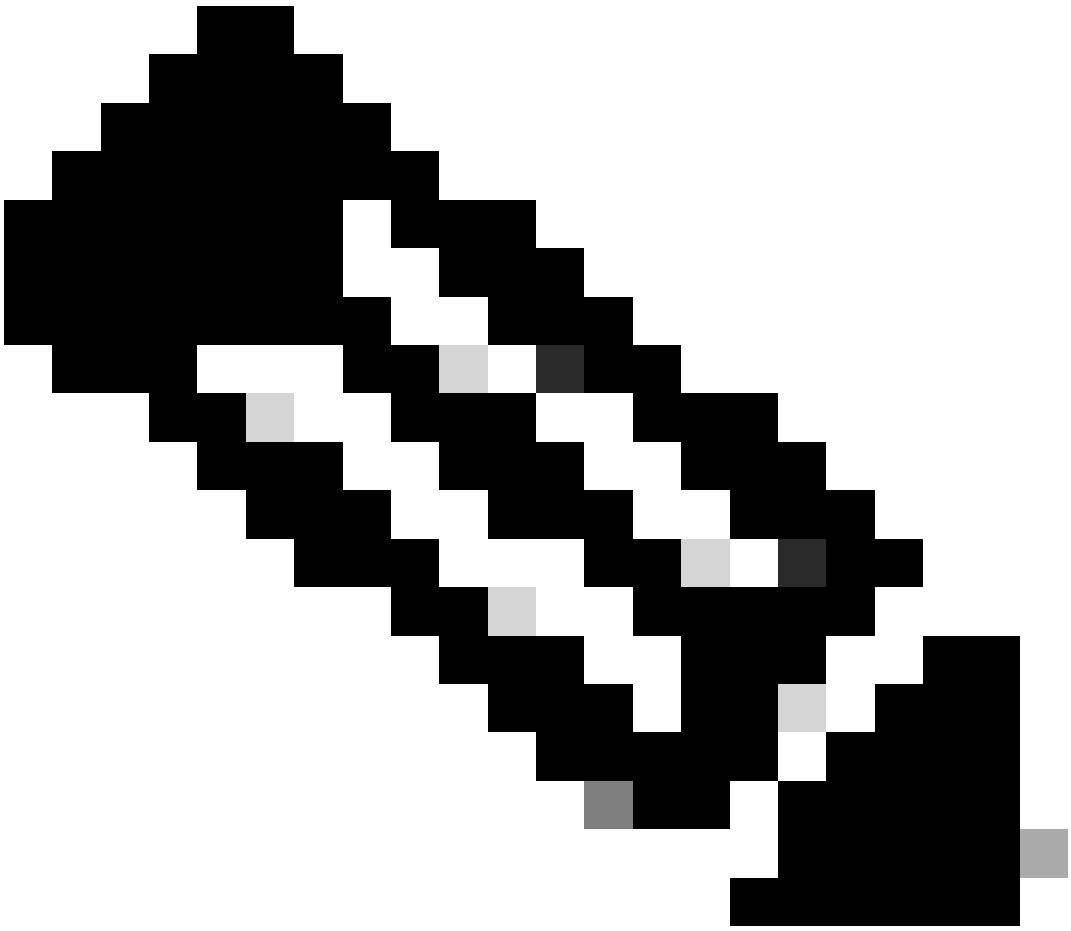
1. Change the action of 01_dap_test.

・ 01_dap_test :
dapSelection (MAC Address) = endpoint.device.MAC[0050.5698.e605] = MAC of Anyconnect Endpoint
Action = **Terminate**
・ 02_dap_test :

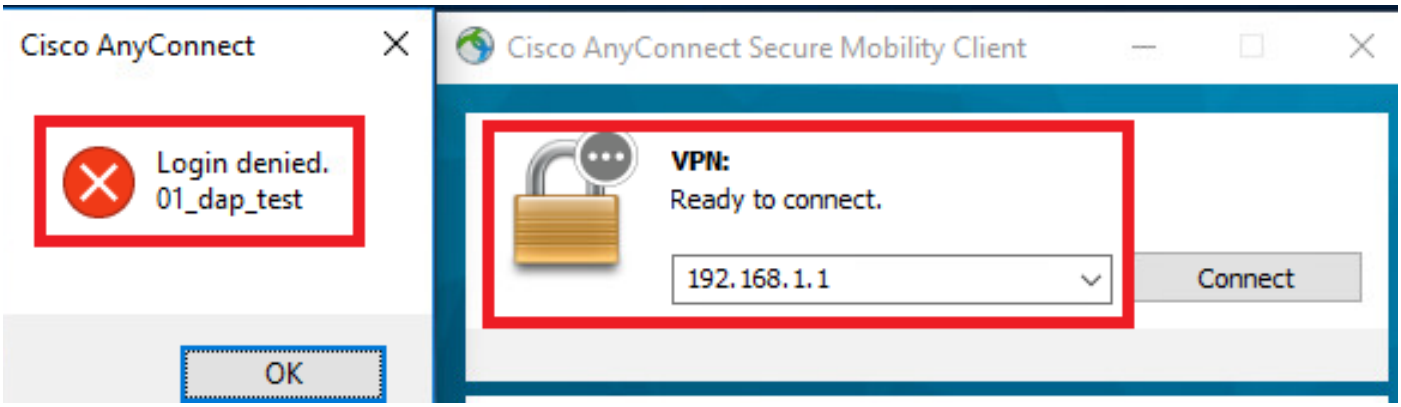
dapSelection (Host Name) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Hostname of Anyconnect Endpoint
Action = **Continue**

2. On endpoint, run Anyconnect connection and input username and password.

3. In the Anyconnect UI, confirm that only **01_dap_test** is matched.



Note: An Connection being matched up to the DAP record which has been set to terminate action. Subsequent records not being matched anymore after the terminate action.



Confirm User Message In UI

4. In the ASA syslog, confirm that only 01_dap_test is matched.

<#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: S

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_selecte

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: DA

General Troubleshooting

These debug logs help you to confirm the detail behavior of DAP in 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 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:49:02: %ASA-4-711001: endpoint.device.hostname = "DESKTOP-VCKHRG1"

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

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-4-711001: dap_process_select

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

Related Information

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