部署ASA DAP以识别AnyConnect的MAC地址

目录

简介

本文档介绍如何通过ASDM配置动态访问策略(DAP)，以检查用于AnyConnect连接的设备的Mac地址。

先决条件

要求

Cisco 建议您了解以下主题：
Cisco Anyconnect和Hostscan的配置

使用的组件

本文档中的信息基于以下软件和硬件版本：
ASAv 9.18 (4)
ASDM 7.20 (1)
Anyconnect 4.10.07073
Hostscan 4.10.07073
Windows 10

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

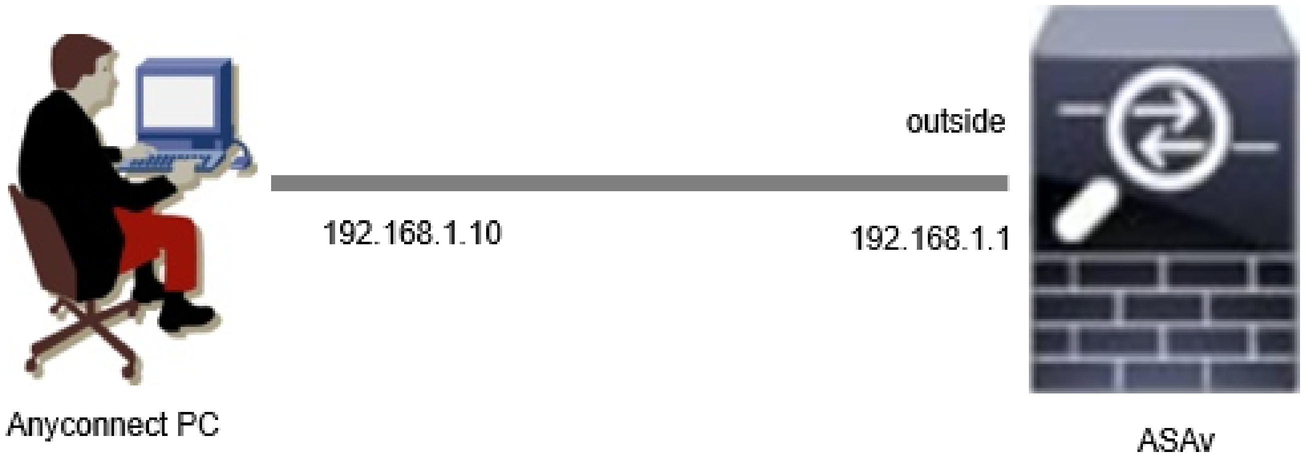
背景信息

HostScan是一个软件模块，可让AnyConnect安全移动客户端在网络上实施安全策略。在Hostscan过程中，将收集有关客户端设备的各种详细信息并向自适应安全设备(ASA)进行报告。这些详细信息包括设备操作系统、防病毒软件、防火墙软件、MAC地址等。动态访问策略(DAP)功能允许网络管理员基于每个用户配置安全策略，DAP中的endpoint.device.MAC属性可用于根据预定义策略匹配或检查客户端设备的MAC地址。

配置

网络图

下图显示本文档示例中使用的拓扑。



图解

ASA中的配置

这是ASA CLI中的最低配置。

```
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
```

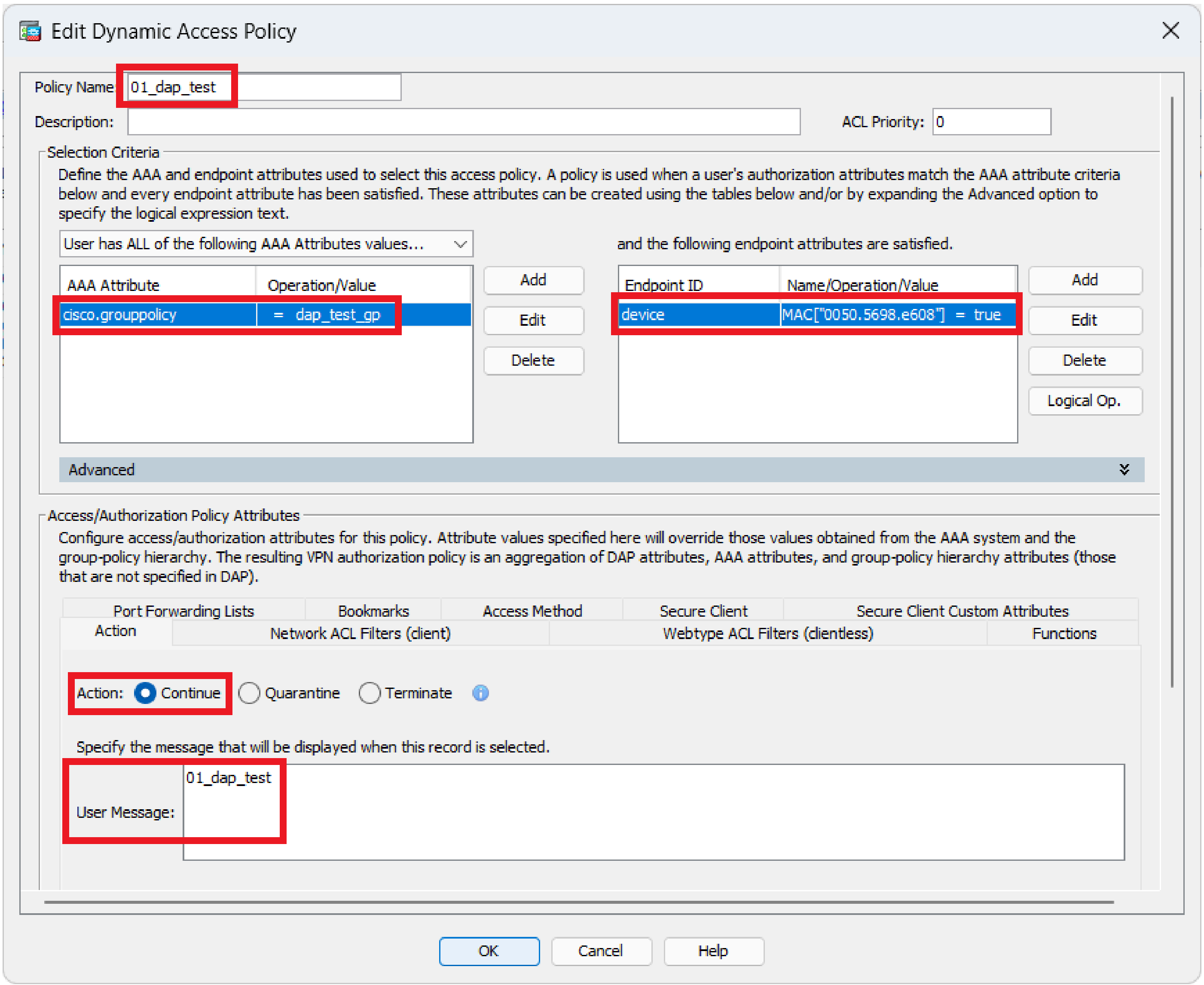
ASDM中的配置

本节介绍如何在ASDM中配置DAP记录。在本示例中，设置3个使用endpoint.device.MAC属性作为条件的DAP记录。

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

1. 配置名为01_dap_test的第一个DAP。

导航到配置 > 远程接入VPN > 网络（客户端）接入 > 动态接入策略。点击Add，然后设置Policy Name、AAA Attribute、endpoint attributes、Action、User Message，如图所示：



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...

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.e608"] = 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).

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

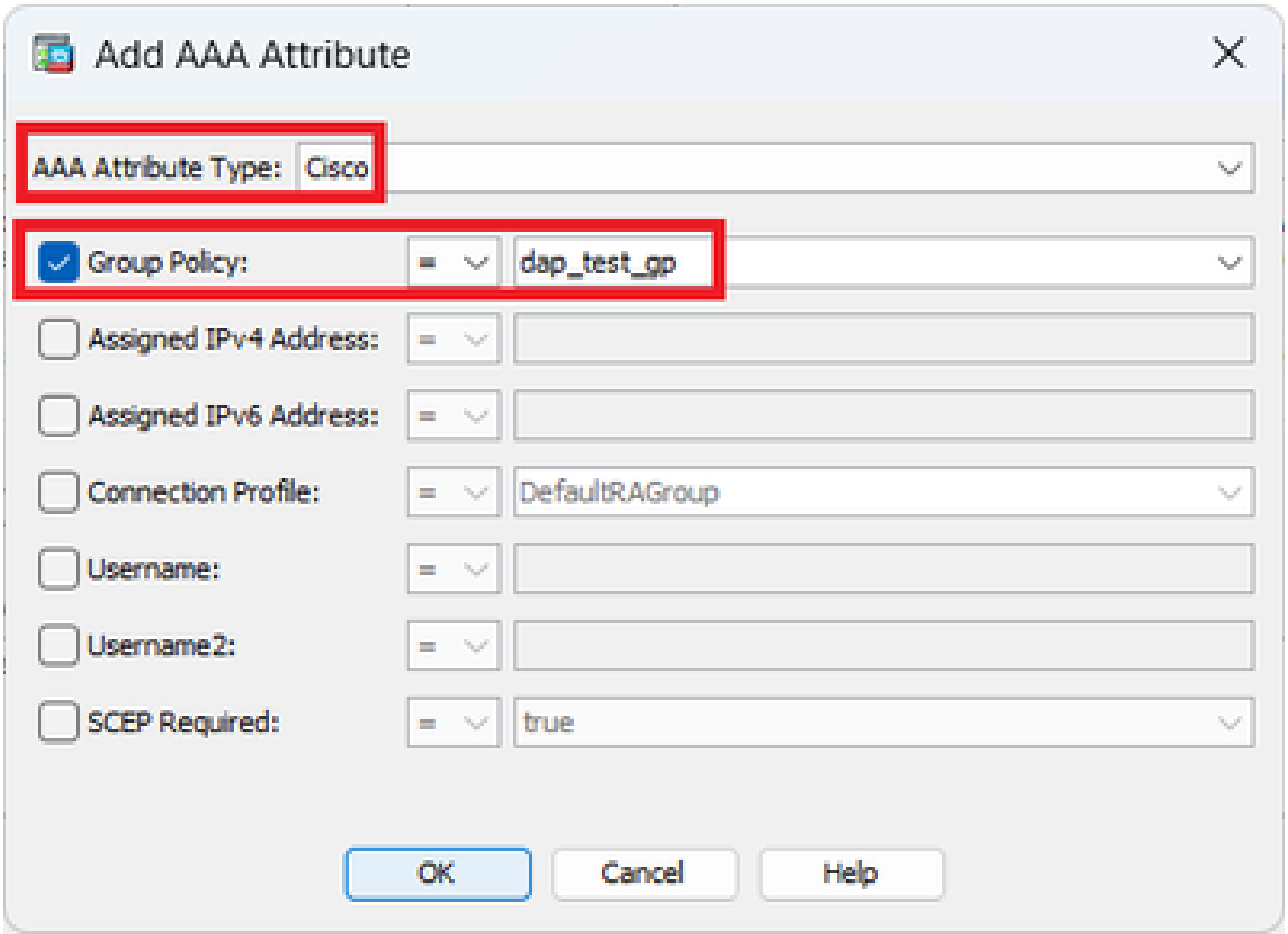
Action: ● Continue ○ Quarantine ○ Terminate

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

User Message: 01_dap_test

配置第一个DAP

配置AAA属性的组策略。



Add AAA Attribute

AAA Attribute Type: Cisco

☑ Group Policy: = dap_test_gp

□ Assigned IPv4 Address: =

□ Assigned IPv6 Address: =

□ Connection Profile: = DefaultRAGroup

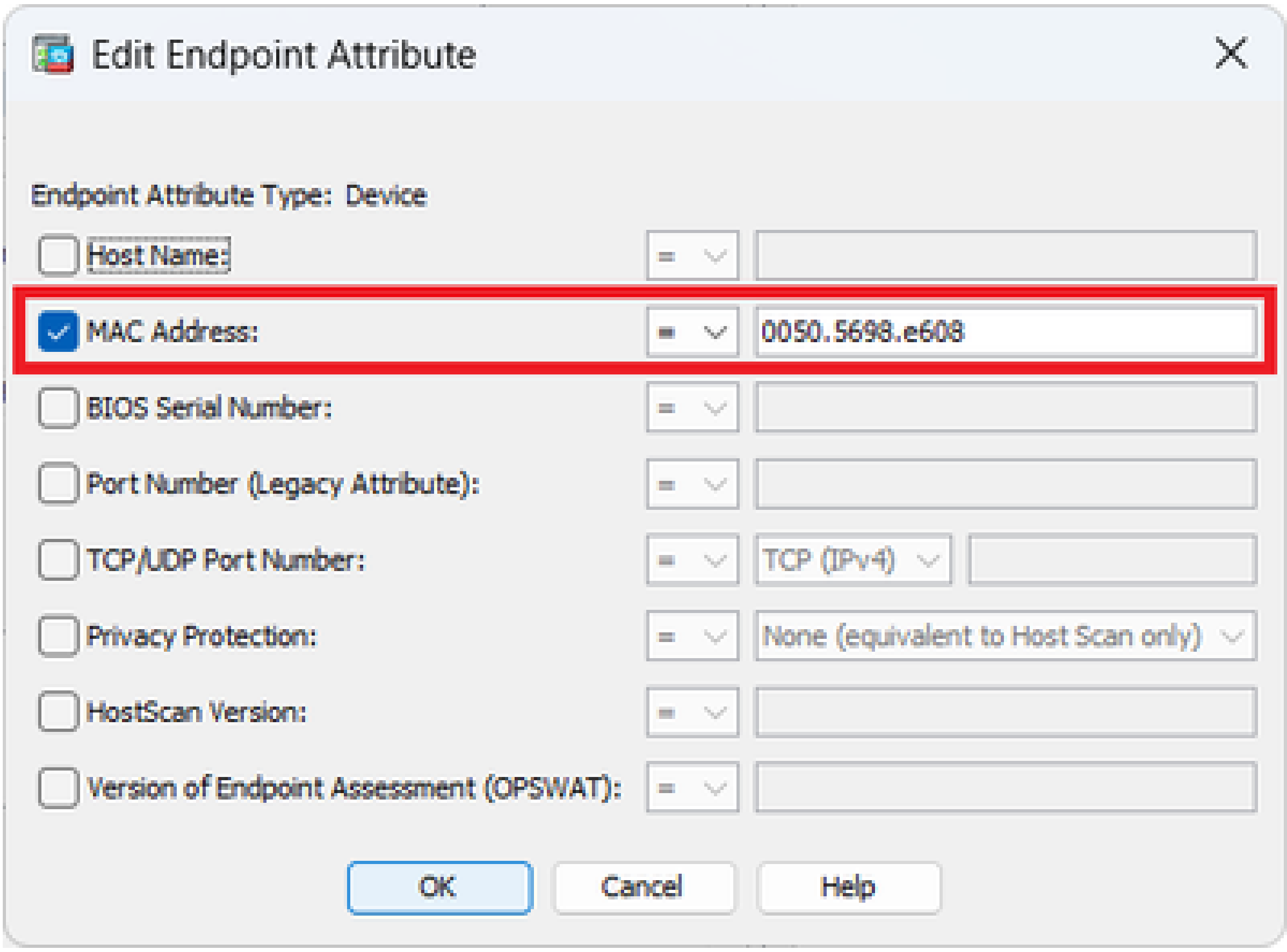
□ Username: =

□ Username2: =

□ SCEP Required: = true

配置DAP记录的组策略

为终端属性配置MAC地址。



Endpoint Attribute Type: Device

☐ Host Name: =

☑ MAC Address: = 0050.5698.e608

☐ BIOS Serial Number: =

☐ Port Number (Legacy Attribute): =

☐ TCP/UDP Port Number: = TCP (IPv4)

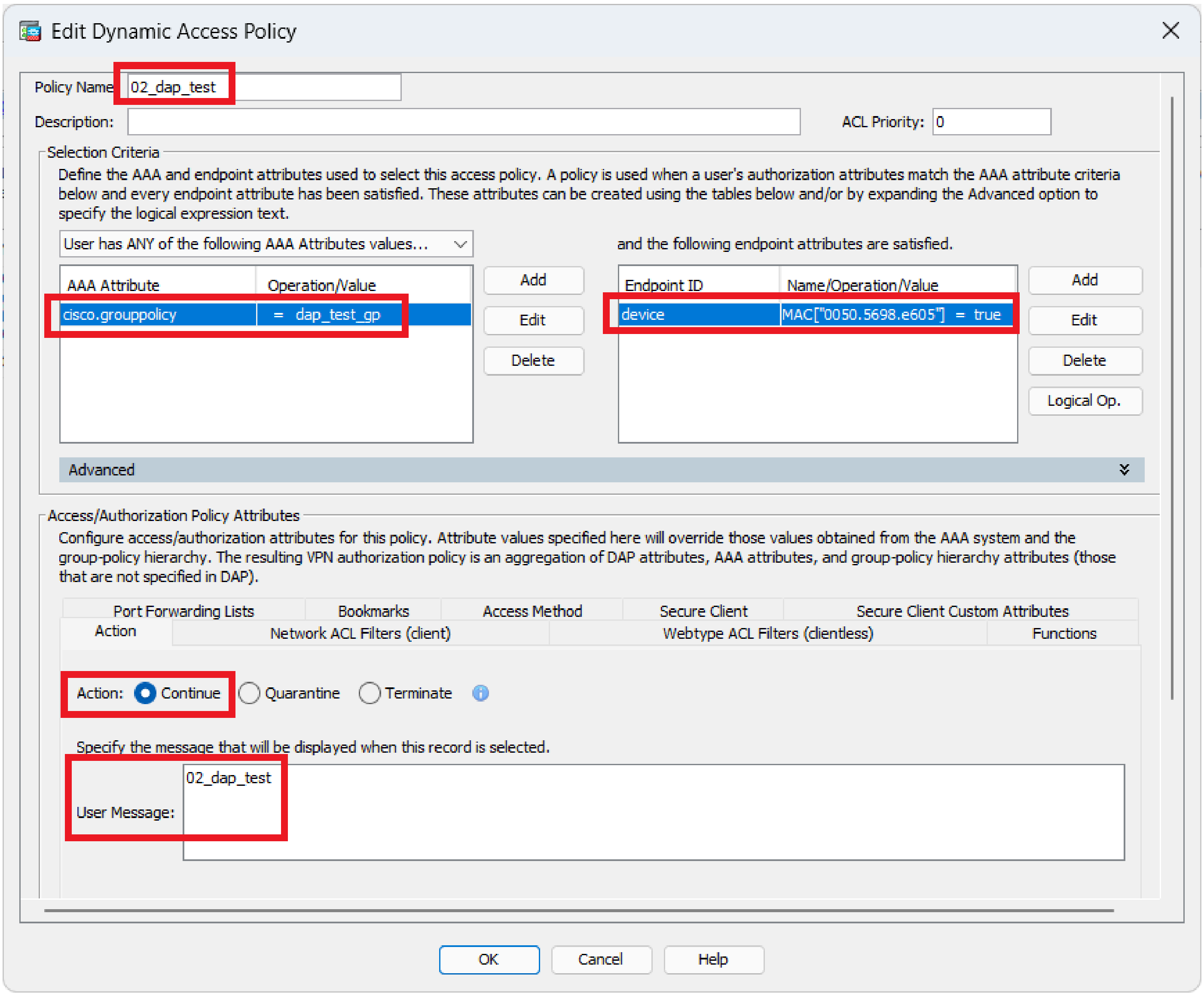
☐ Privacy Protection: = None (equivalent to Host Scan only)

☐ HostScan Version: =

☐ Version of Endpoint Assessment (OPSWAT): =

配置DAP的MAC条件

2. 配置第二个名为02_dap_test的DAP。



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).

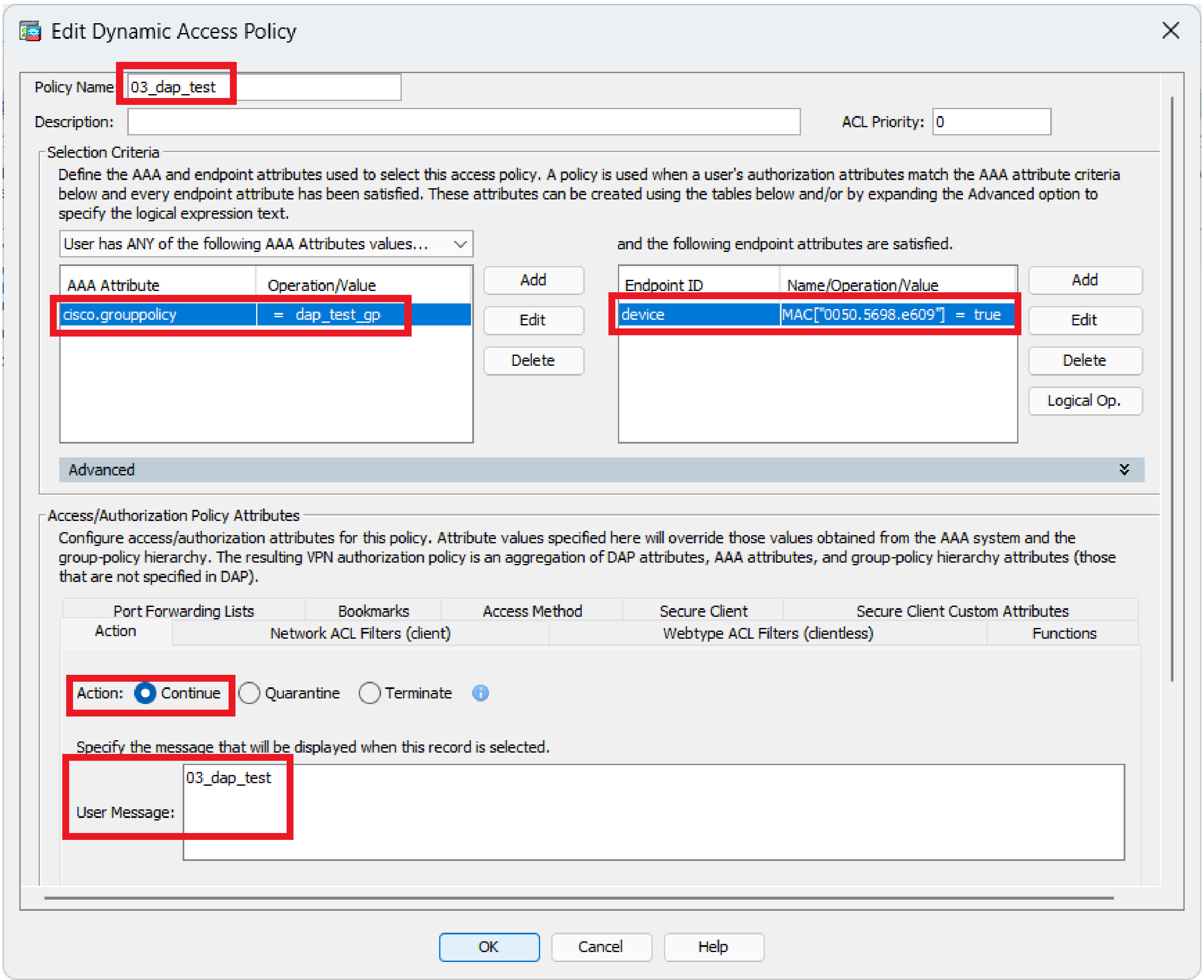
Action: ● Continue ○ Quarantine ○ Terminate

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

User Message: 02_dap_test

配置第二个DAP

3. 配置名为03_dap_test的第三个DAP。



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).

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

Action: ● Continue ○ Quarantine ○ Terminate

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

User Message: 03_dap_test

配置第三个DAP

4. 使用 **more flash:/dap.xml** 命令确认dap.xml中DAP记录的设置。

在ASDM上设置的DAP记录的详细信息以dap.xml形式保存在ASA闪存中。完成这些设置后，将以dap.xml形式生成三个DAP记录。您可以在dap.xml中确认每个DAP记录的详细信息。

注意：DAP的匹配顺序是dap.xml中的显示顺序。 最后匹配默认DAP (DfltAccessPolicy)。

<#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
```

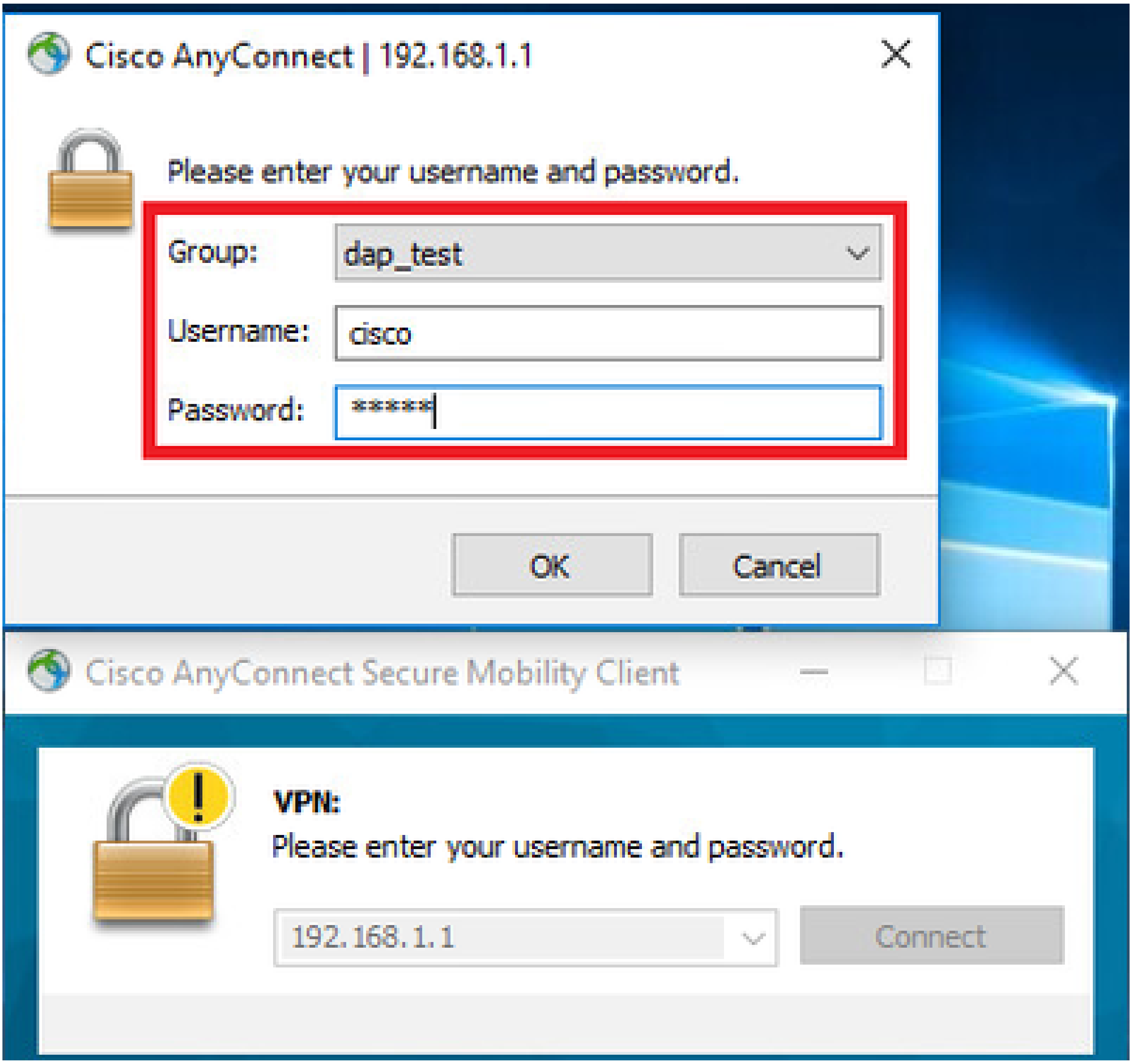
```
</value> <--- 1st DAP group policy <operation>EQ</operation> <type>caseless</type> </attr> </dapSelecti

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
```

验证

场景1.仅匹配一个DAP

1. 确保终端的MAC地址为0050.5698.e605，这与02_dap_test中的MAC条件匹配。

2.在终端上，运行Anyconnect连接并输入用户名和密码。



Cisco AnyConnect | 192.168.1.1

Please enter your username and password.

Group: dap_test

Username: cisco

Password: *****

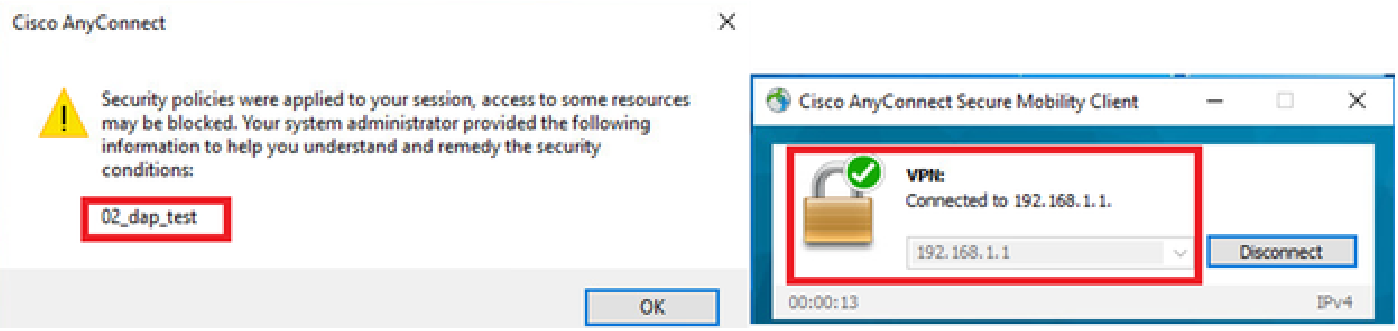
Cisco AnyConnect Secure Mobility Client

VPN:
Please enter your username and password.

192.168.1.1

输入用户名和密码

3.在Anyconnect UI中，确认02_dap_test匹配。



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

在*UI*中确认用户消息

4.在ASA syslog中，确认02_dap_test匹配。

注意：确保在ASA中启用debug dap trace。

<#root>

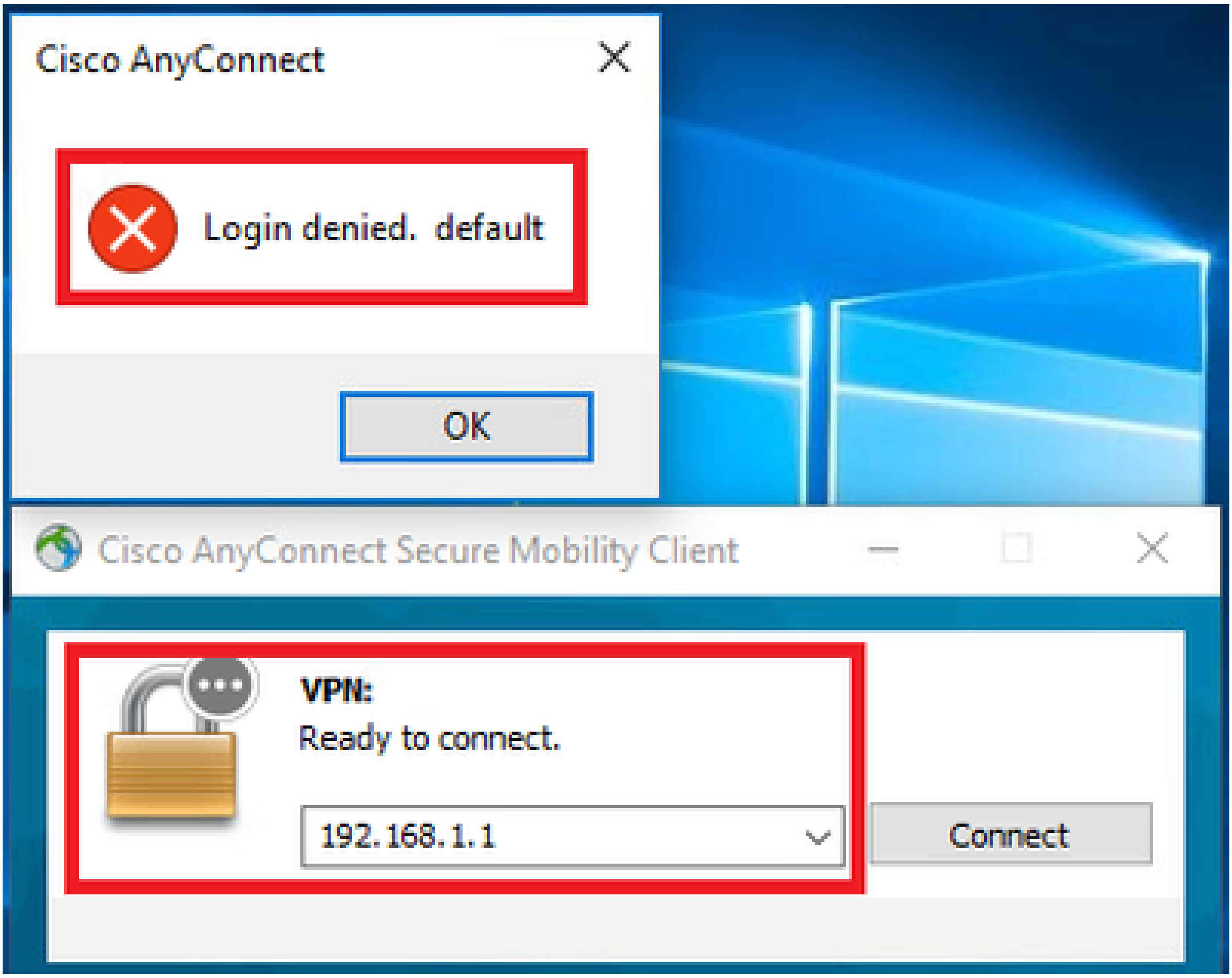
```
Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["

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: 
```

场景2.默认DAP匹配

1.将02_dap_test中的endpoint.device.MAC值更改为不匹配终端的MAC的0050.5698.e607。

2.在终端上，运行Anyconnect连接并输入用户名和密码。

3. 确认Anyconnect连接被拒绝。


Cisco AnyConnect

Login denied. default

VPN:
Ready to connect.

192.168.1.1

在*UI*中确认用户消息

4. 在ASA syslog中，确认DfltAccessPolicy匹配。

注意：默认情况下，DfltAccessPolicy的操作为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
```

场景3.匹配多个DAP（操作：继续）

1. 更改每个DAP中的操作和属性。

·01_dap_test：
  dapSelection（MAC地址）= endpoint.device.MAC[0050.5698.e605] = Anyconnect终端的MAC
  操作=继续
·02_dap_test：

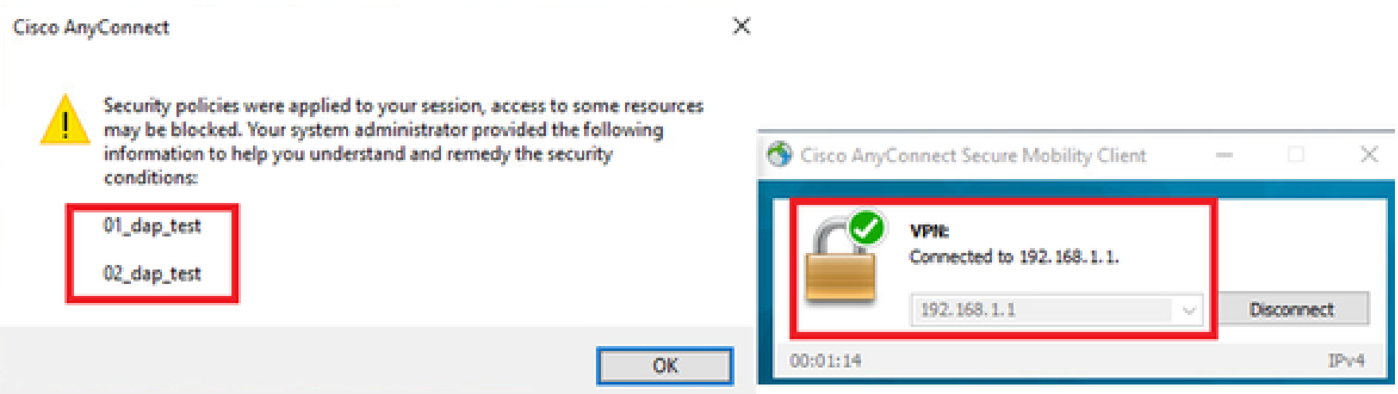
dapSelection（主机名）= endpoint.device.hostname[DESKTOP-VCKHRG1] = Anyconnect终端的主机名
操作=继续

· 删除03_dap_test DAP记录

2. 在终端上，运行Anyconnect连接并输入用户名和密码。

3. 在Anyconnect UI中，确认所有2个DAP都匹配

注意：如果连接匹配多个DAP，则多个DAP的用户消息将集成并一起显示在Anyconnect UI中。



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:

01_dap_test

02_dap_test

OK
Cisco AnyConnect Secure Mobility Client
VPN:
Connected to 192.168.1.1.
192.168.1.1
Disconnect
00:01:14
IPv4

在UI中确认用户消息

4. 在ASA syslog中，确认所有2个DAP均匹配。

<#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
```

场景4.多个DAP (Action ： Terminate)匹配

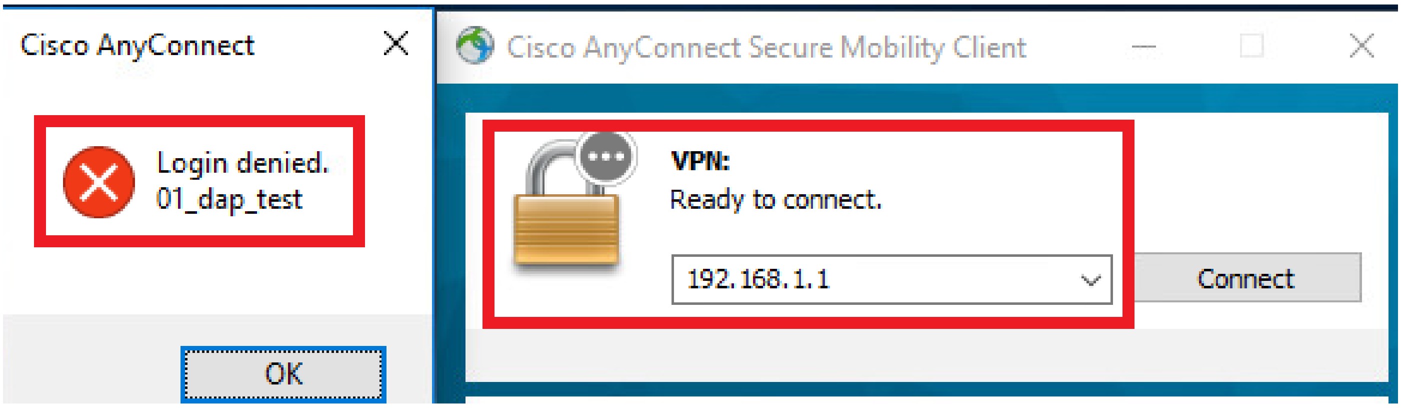
1. 更改01_dap_test的操作。

·01_dap_test：
dapSelection（MAC地址）= endpoint.device.MAC[0050.5698.e605] = Anyconnect终端的MAC
操作=终止
·02_dap_test：
dapSelection（主机名）= endpoint.device.hostname[DESKTOP-VCKHRG1] = Anyconnect终端的主机名
操作=继续

2. 在终端上，运行Anyconnect连接并输入用户名和密码。

3. 在Anyconnect UI中，确认仅匹配**01_dap_test**。

注意：连接与已设置为终止操作的DAP记录匹配。终止操作后不再匹配后续记录。



Login denied.
01_dap_test

VPN:
Ready to connect.

192.168.1.1

在*UI*中确认用户消息

4. 在ASA syslog中，确认仅匹配01_dap_test。

<#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: 
```

一般故障排除

这些调试日志可帮助您确认ASA中DAP的详细行为。

```
 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
```

相关信息

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。