

部署ASA DAP以確定AnyConnect的MAC地址

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[ASA中的配置](#)

[ASDM中的配置](#)

[驗證](#)

[案例1.僅匹配一個DAP](#)

[案例2.預設DAP匹配](#)

[案例3.匹配多個DAP \(操作：繼續\)](#)

[案例4.匹配多個DAP\(Action：Terminate\)](#)

[一般疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹如何透過ASDM配置動態訪問策略(DAP)，以檢查用於AnyConnect連線的裝置的Mac地址。

必要條件

需求

思科建議您瞭解以下主題：
[Cisco Anyconnect和Hostscan的配置](#)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

ASAv 9.18 (4)

ASDM 7.20 (1)

Anyconnect 4.10.07073

Hostscan 4.10.07073

Windows 10

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設

) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

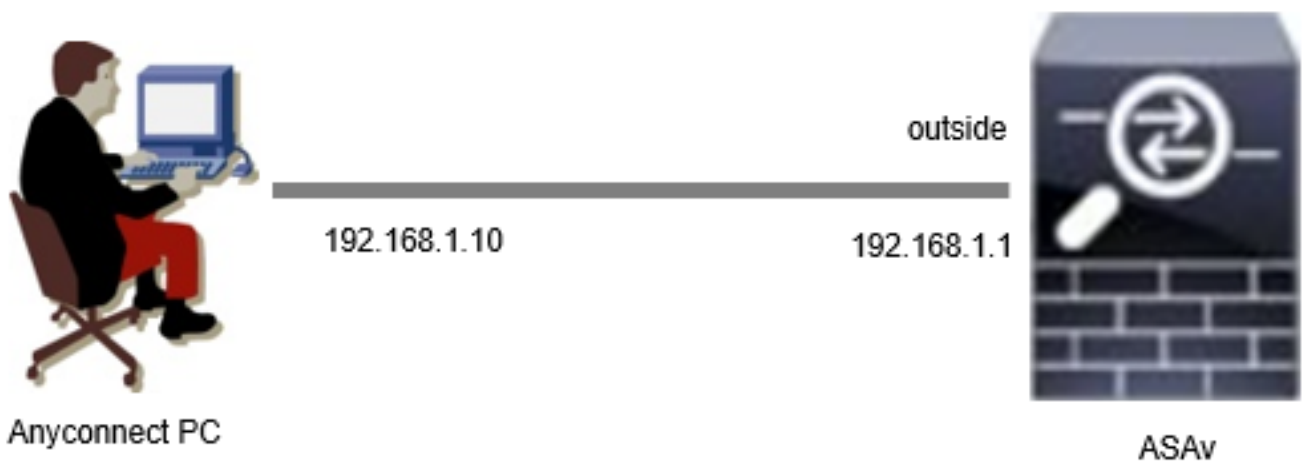
背景資訊

HostScan是一個軟體模組，可為AnyConnect安全移動客戶端提供在網路上實施安全策略的能力。在Hostscan過程中，將收集有關客戶端裝置的各種詳細資訊並報告回自適應安全裝置(ASA)。這些詳細資訊包括裝置作業系統、防病毒軟體、防火牆軟體、MAC地址等。動態訪問策略(DAP)功能允許網路管理員基於每個使用者配置安全策略，DAP中的endpoint.device.MAC屬性可用於根據預定義策略匹配或檢查客戶端裝置的MAC地址。

設定

網路圖表

下圖顯示本文檔示例中使用的拓撲。



圖表

ASA中的配置

這是ASA CLI中的最小配置。

```
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

本節介紹如何在ASDM中配置DAP記錄。在本示例中，設定3個使用endpoint.device.MAC屬性作為條件的DAP記錄。

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

1. 配置名為01_dap_test的第一個DAP。

導航到配置 > 遠端接入VPN > 網路 (客戶端) 接入 > 動態接入策略。點選Add，然後設定策略名稱、AAA屬性、終端屬性、操作、使用者消息，如圖所示：

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... and the following endpoint attributes are satisfied.

AAA Attribute	Operation/Value	Endpoint ID	Name/Operation/Value
disco.grouppolicy	= dap_test_gp	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).

Port Forwarding Lists	Bookmarks	Access Method	Secure Client	Secure Client Custom Attributes
Action	Network ACL Filters (client)		Webytype ACL Filters (clientless)	Functions
Action: <input checked="" type="radio"/> Continue <input type="radio"/> Quarantine <input type="radio"/> Terminate				
Specify the message that will be displayed when this record is selected.				
User Message: 01_dap_test				

OK Cancel Help

配置第一個DAP

配置AAA屬性的組策略。

Add AAA Attribute ✕

AAA Attribute Type: Cisco

Group Policy: = dap_test_gp

Assigned IPv4 Address: =

Assigned IPv6 Address: =

Connection Profile: = DefaultRAGroup

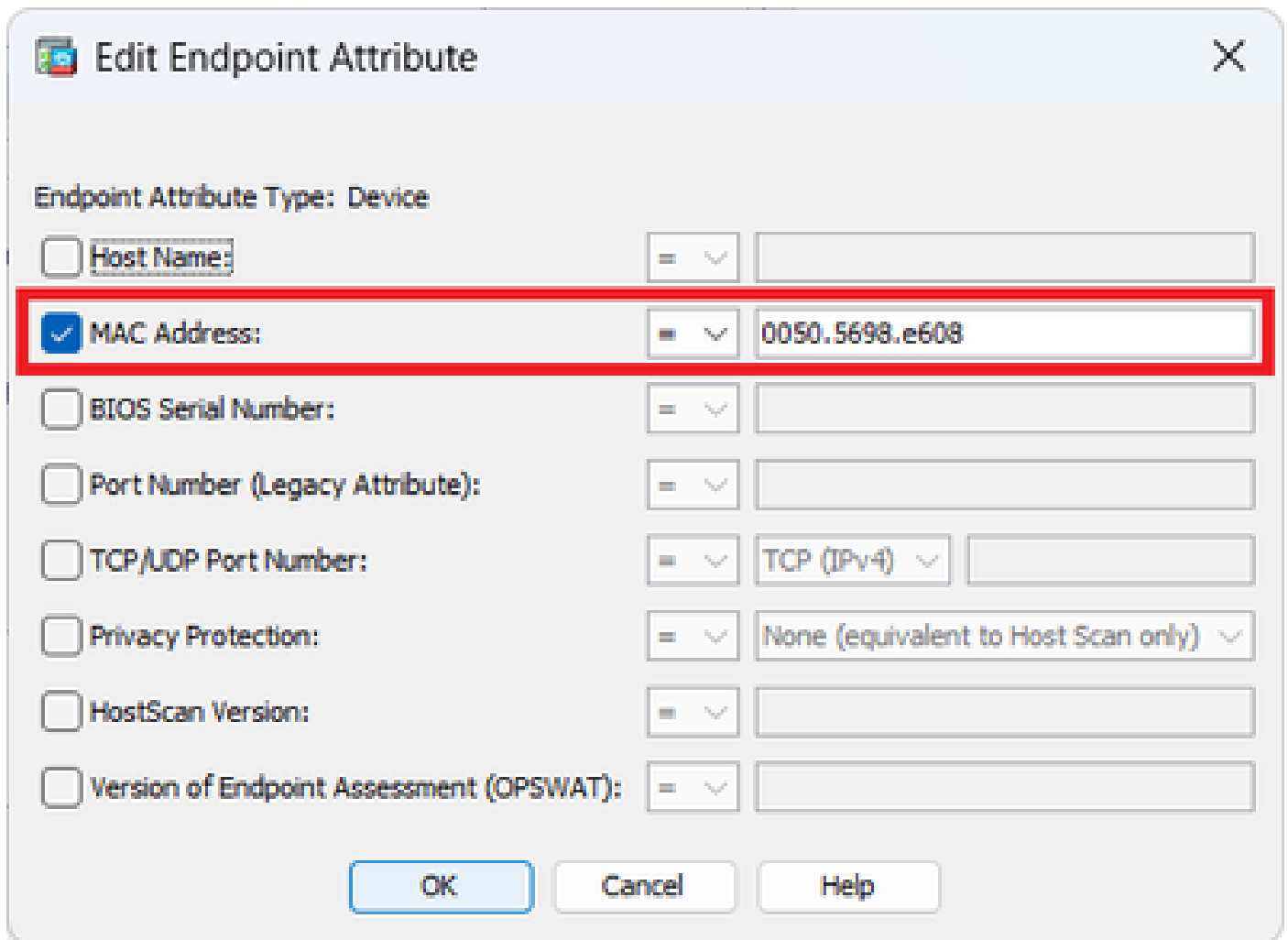
Username: =

Username2: =

SCEP Required: = true

配置DAP記錄的組策略

為終端屬性配置MAC地址。

The image shows a dialog box titled "Edit Endpoint Attribute" with a close button (X) in the top right corner. The dialog is set to "Endpoint Attribute Type: Device". It contains several rows of configuration options, 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". Other rows include "Host Name:", "BIOS Serial Number:", "Port Number (Legacy Attribute):", "TCP/UDP Port Number:" (with a sub-dropdown for "TCP (IPv4)"), "Privacy Protection:" (with a sub-dropdown for "None (equivalent to Host Scan only)"), "HostScan Version:", and "Version of Endpoint Assessment (OPSWAT):". At the bottom are "OK", "Cancel", and "Help" buttons.

Attribute	Value
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條件

2. 配置名為02_dap_test的第二個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... and the following endpoint attributes are satisfied.

AAA Attribute	Operation/Value	Endpoint ID	Name/Operation/Value
disco.grouppolicy	= dap_test_gp	device	MAC["0050.5698.e605"] = 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).

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

配置第二個DAP

3. 配置名為03_dap_test的第三個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	Endpoint ID	Name/Operation/Value
disco.grouppolicy	= dap_test_gp	device	MAC["0050.5698.e609"] = 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).

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: **03_dap_test**

OK Cancel Help

配置第三個DAP

4. 使用 `more flash:/dap.xml` 命令確認dap.xml中DAP記錄的設定。

在ASDM上設定的DAP記錄的詳細資訊儲存在ASA快閃記憶體中的dap.xml中。完成這些設定後，會在dap.xml中產生三個DAP記錄。您可以在dap.xml中確認每個DAP記錄的詳細資訊。

注意：匹配的DAP的順序是dap.xml中的顯示順序。預設的DAP (DfltAccessPolicy)是最後相符的專案。

```
<#root>
```

```
ciscoasa#
```

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

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

```
01_dap_test
```

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

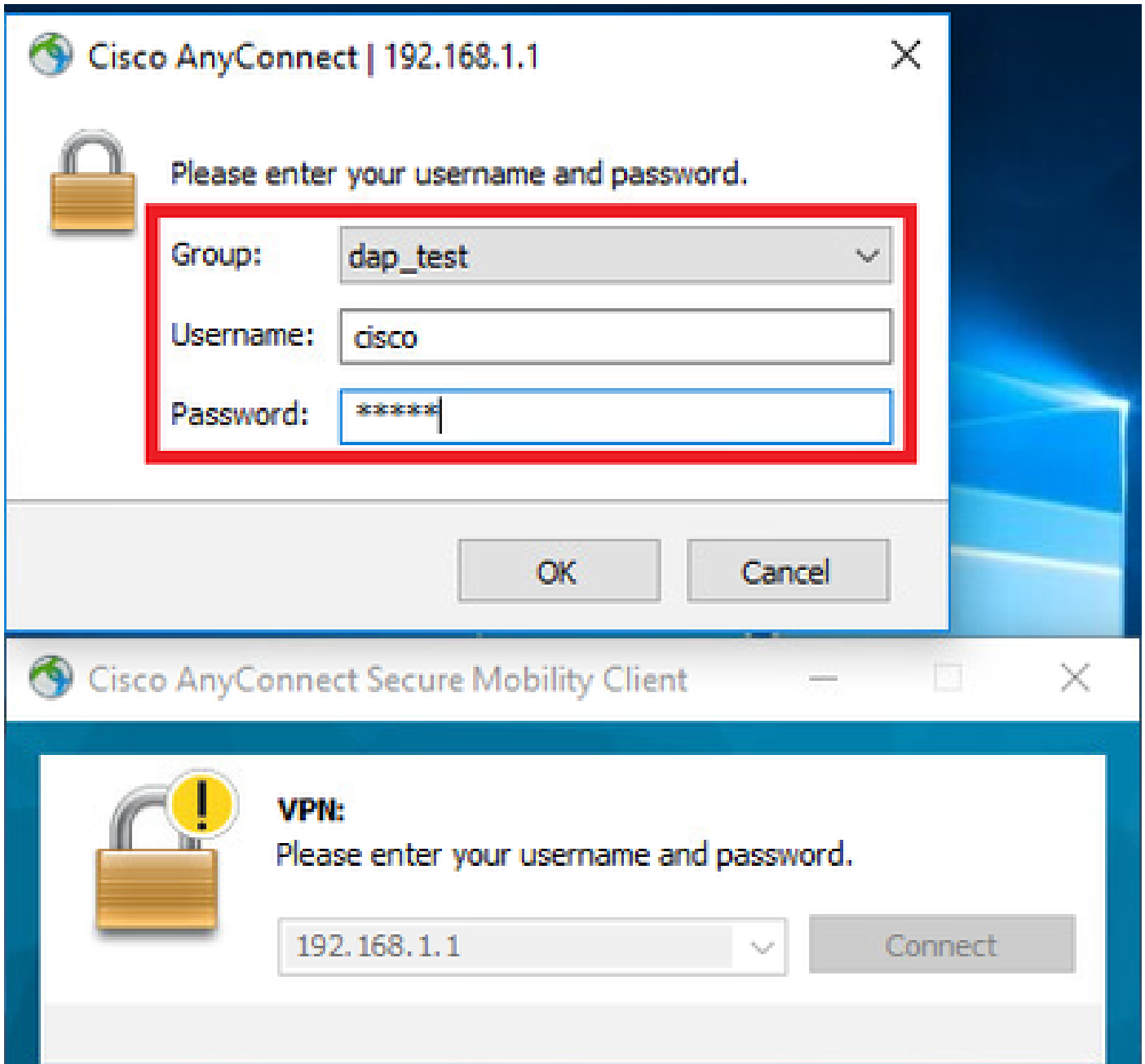
```
dap_test_gp
```

```
</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
```

驗證

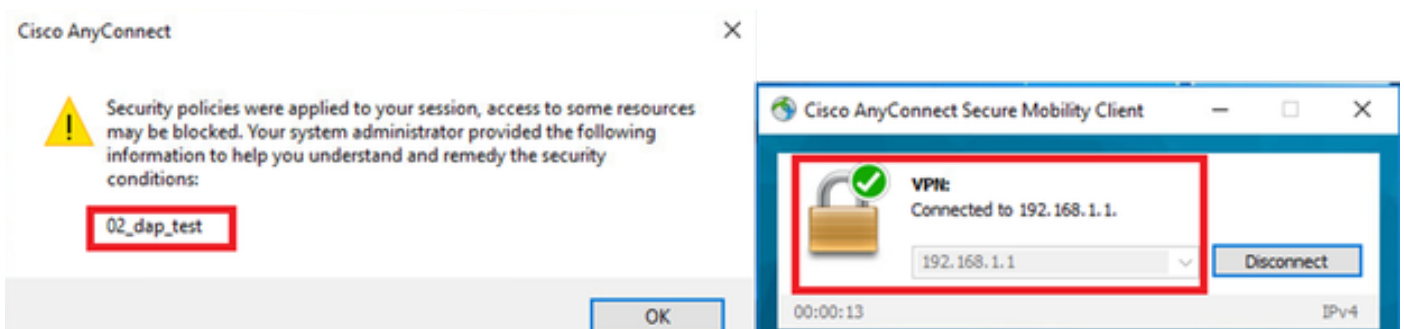
案例1.僅匹配一個DAP

1. 確保終端的MAC為0050.5698.e605，這與02_dap_test中的MAC條件匹配。
2. 在終端上，運行Anyconnect連線並輸入使用者名稱和密碼。



輸入使用者名稱和密碼

3.在Anyconnect UI中，確認02_dap_test匹配。



在UI中確認使用者訊息

4.在ASA系統日誌中，確認02_dap_test匹配。

注意：確保在ASA中啟用了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

: ,

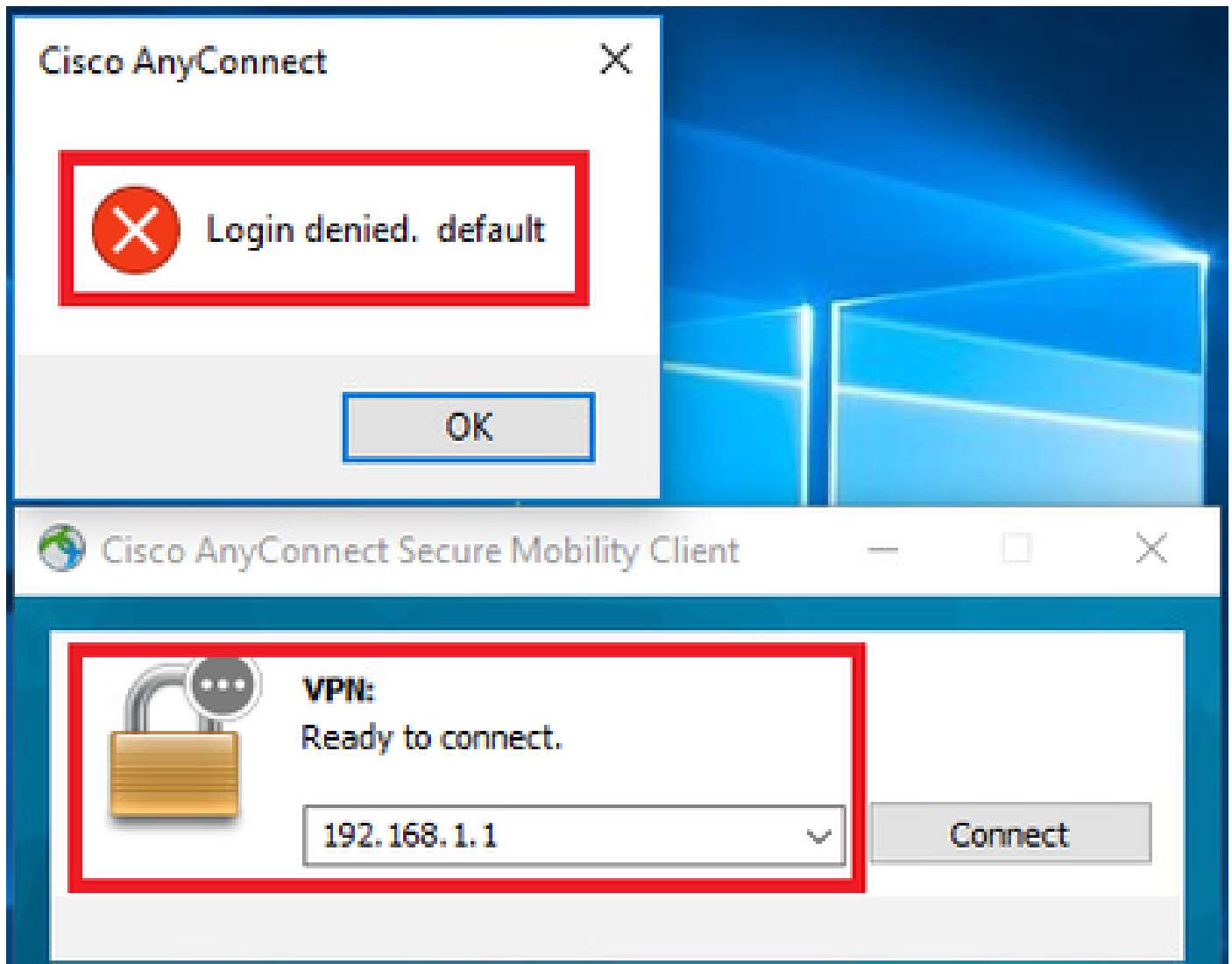
02_dap_test

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

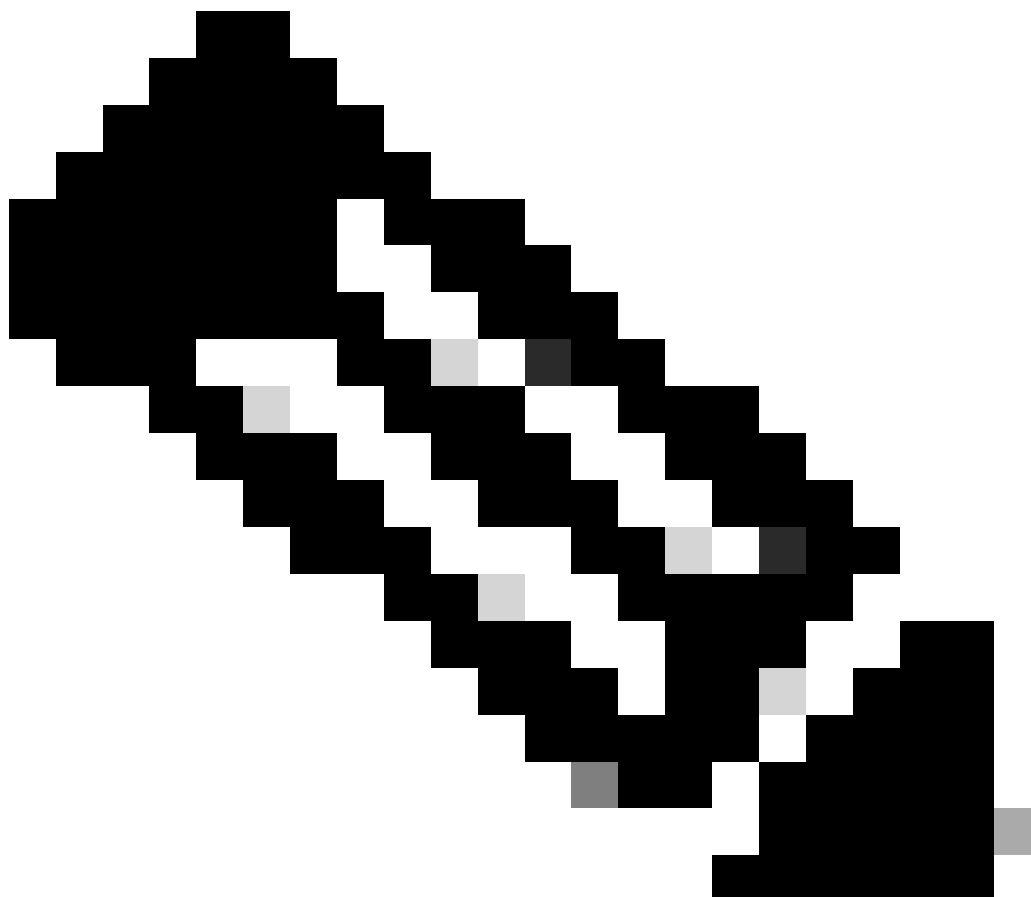
案例2.預設DAP匹配

- 1.將02_dap_test中的endpoint.device.MAC值更改為與終端的MAC不匹配的0050.5698.e607。
- 2.在終端上，運行Anyconnect連線並輸入使用者名稱和密碼。
3. 確認Anyconnect連線被拒絕。



在UI中確認使用者訊息

4. 在ASA syslog中，確認DfltAccessPolicy匹配。



注意：預設情況下，DfltAccessPolicy的操作為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

案例3.匹配多個DAP (操作:繼續)

1. 變更每個DAP中的作業與屬性。

·01_dap_test :

dapSelection (MAC地址) = endpoint.device.MAC[0050.5698.e605] = Anyconnect終端的MAC

操作=繼續

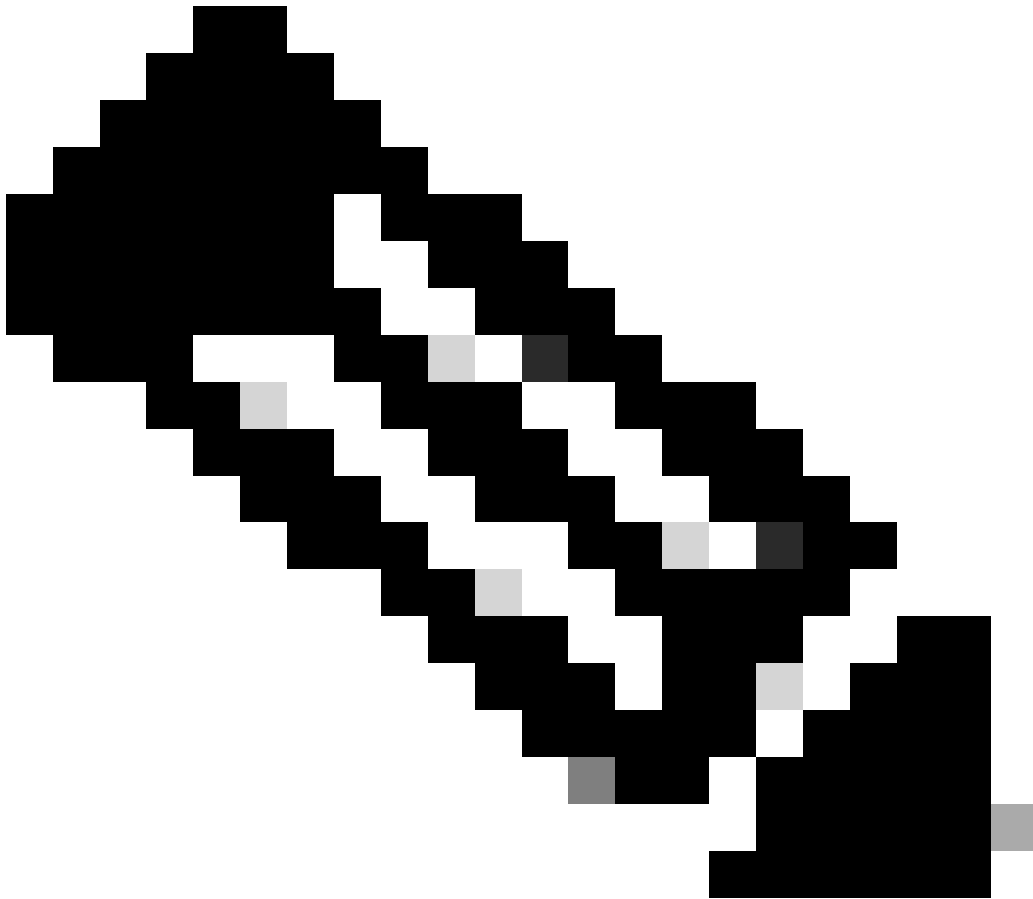
·02_dap_test :

dapSelection (主機名) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Anyconnect終端的主機名
操作=繼續

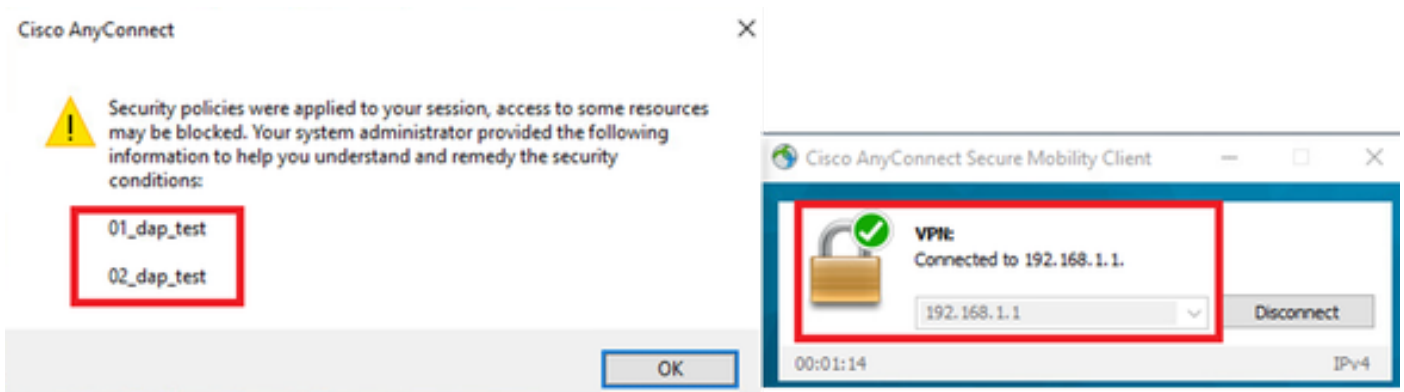
· 刪除03_dap_test DAP記錄

2. 在終端上，運行Anyconnect連線並輸入使用者名稱和密碼。

3. 在Anyconnect UI中，確認所有2個DAP都匹配



注意：如果連線與多個DAP匹配，則多個DAP的使用者消息將整合在一起並顯示在Anyconnect UI中。



在UI中確認使用者訊息

4. 在ASA syslog中，確認所有2個DAP都匹配。

<#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

案例4.匹配多個DAP (Action : Terminate)

1. 變更01_dap_test的作業。

·01_dap_test :

dapSelection (MAC地址) = endpoint.device.MAC[0050.5698.e605] = Anyconnect終端的MAC

操作=終止

·02_dap_test :

dapSelection (主機名) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Anyconnect終端的主機名

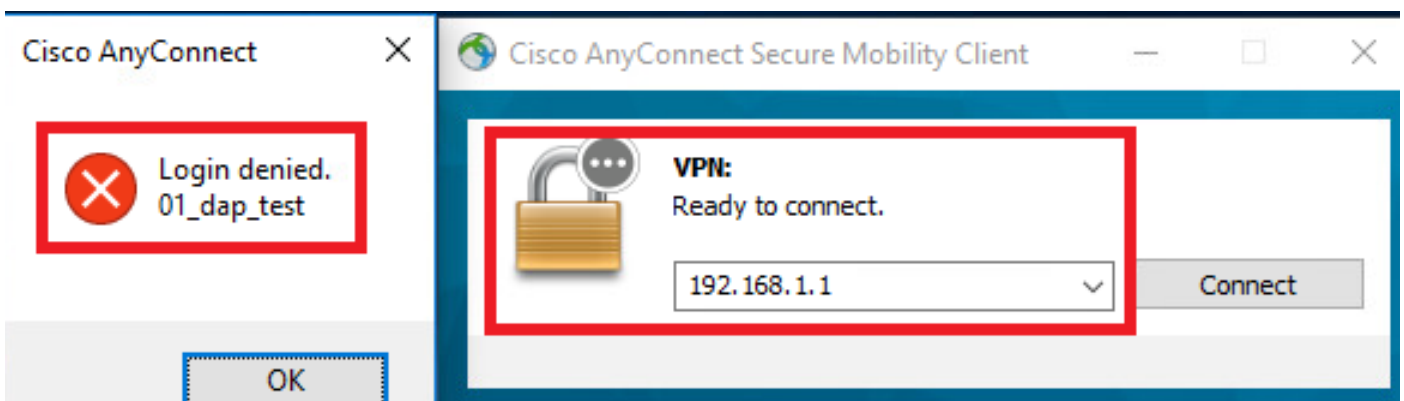
操作=繼續

2. 在終端上，運行Anyconnect連線並輸入使用者名稱和密碼。

3. 在Anyconnect UI中，確認僅匹配01_dap_test。



註：一個連線與已設定為終止操作的DAP記錄匹配。終止操作後不再匹配後續記錄。



在UI中確認使用者訊息

4. 在ASA syslog中，確認僅匹配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: I
```

一般疑難排解

這些調試日誌可幫助您確認DAP在ASA中的詳細行為。

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-
```

相關資訊

<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>

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。