

# Distribuire ASA DAP per identificare l'indirizzo MAC per AnyConnect

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione in ASA](#)

[Configurazione in ASDM](#)

[Verifica](#)

[Scenario1. Corrispondenza di un solo DAP](#)

[Scenario2. Corrispondenza DAP predefinito](#)

[Scenario 3. Corrispondenza di più punti di accesso al database \(Azione : Continua\)](#)

[Scenario 4. Corrispondenza di più punti di accesso dati \(Azione: Termina\)](#)

[Risoluzione dei problemi generali](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come configurare i criteri di accesso dinamico (DAP) tramite ASDM per controllare l'indirizzo Mac del dispositivo usato per la connessione AnyConnect.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:  
Configurazione di Cisco Anyconnect e Hostscan

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

ASA v 9.18 (4)

ASDM 7.20 (1)

Anyconnect 4.10.07073

Hostscan 4.10.07073

## Windows 10

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

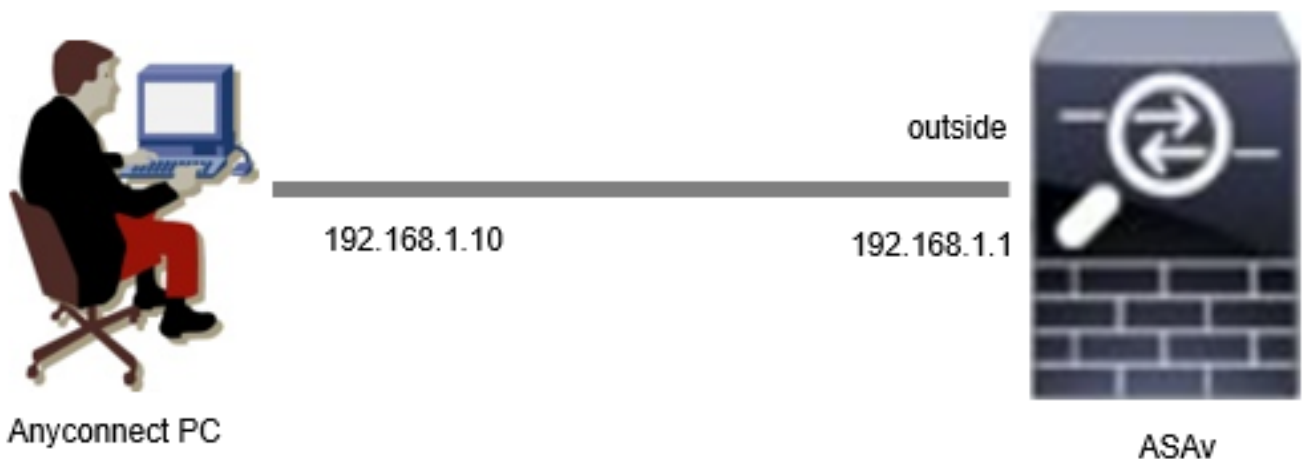
## Premesse

HostScan è un modulo software che consente a AnyConnect Secure Mobility Client di applicare i criteri di sicurezza sulla rete. Durante il processo di Hostscan, vengono raccolti vari dettagli sul dispositivo client e segnalati all'appliance ASA (Adaptive Security Appliance). Questi dettagli includono il sistema operativo del dispositivo, il software antivirus, il software firewall, l'indirizzo MAC e altro. La funzionalità DAP (Dynamic Access Policies) consente agli amministratori di rete di configurare i criteri di sicurezza per singoli utenti. È possibile utilizzare l'attributo `endpoint.device.MAC` in DAP per verificare la corrispondenza o controllare l'indirizzo MAC del dispositivo client rispetto ai criteri predefiniti.

## Configurazione

### Esempio di rete

Nell'immagine è illustrata la topologia utilizzata per l'esempio del documento.



Diagramma

### Configurazione in ASA

Questa è la configurazione minima nella CLI di ASA.

```
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
```

## Configurazione in ASDM

In questa sezione viene descritto come configurare il record DAP in ASDM. In questo esempio, impostare 3 record DAP che utilizzano l'attributo endpoint.device.MAC come condizione.

```
·01_dap_test:endpoint.device.MAC=0050.5698.e608
```

```
·02_dap_test:endpoint.device.MAC=0050.5698.e605 = indirizzo MAC dell'endpoint Anyconnect
```

```
·03_dap_test:endpoint.device.MAC=0050.5698.e609
```

1. Configurare il primo DAP denominato 01\_dap\_test.

Selezionare Configurazione > VPN Accesso remoto > Accesso di rete (client) > Criteri di accesso dinamico. Fare clic su Aggiungi e impostare Nome criterio, Attributo AAA, Attributi endpoint, Azione, Messaggio utente, come mostrato nell'immagine:

**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:  Continue  Quarantine  Terminate

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

User Message: **01\_dap\_test**

OK Cancel Help

Configura primo DAP

Configurare Criteri di gruppo per l'attributo AAA.

**Add AAA Attribute** ✕

AAA Attribute Type: Cisco

Group Policy: = dap\_test\_gp

Assigned IPv4 Address: =

Assigned IPv6 Address: =

Connection Profile: = DefaultRAGroup

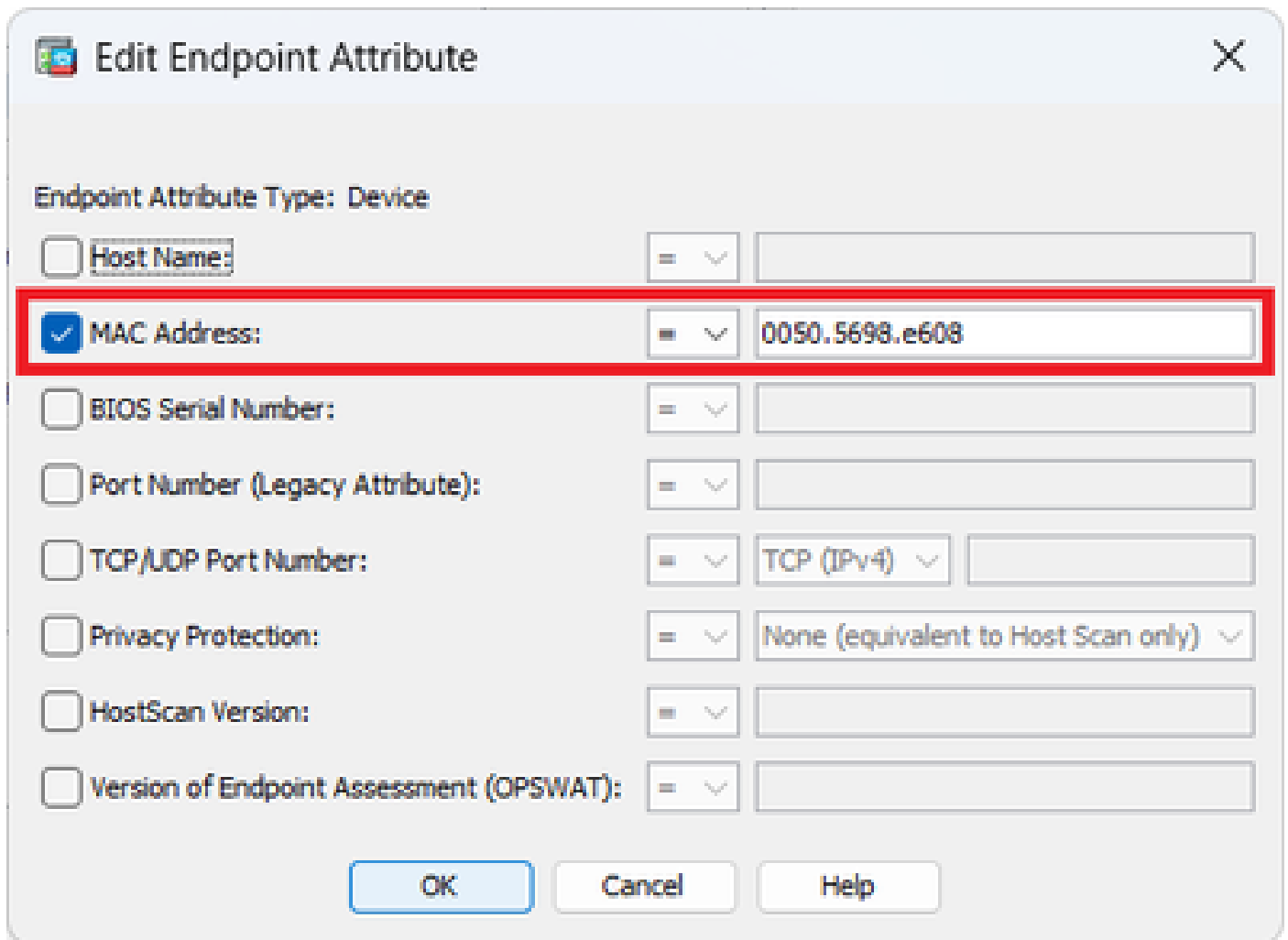
Username: =

Username2: =

SCEP Required: = true

Configura Criteri di gruppo per record DAP

Configurare Indirizzo MAC per Attributo endpoint.

The image shows a dialog box titled "Edit Endpoint Attribute" with a close button (X) in the top right corner. The dialog is for configuring endpoint attributes for a device. The "Endpoint Attribute Type" is set to "Device". There are seven attribute rows, 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 and has its checkbox checked and its value set to "0050.5698.e608".

Endpoint Attribute Type: Device

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

OK Cancel Help

Configura condizione MAC per DAP

2. Configurare il secondo DAP denominato 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... and the following endpoint attributes are satisfied.

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

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:	02_dap_test			

OK Cancel Help

Configura secondo DAP

3. Configurare il terzo DAP denominato 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	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

Configura terzo DAP

#### 4. Utilizzare il `more flash:/dap.xml` comando per confermare l'impostazione dei record DAP nel file dap.xml.

I dettagli dei record DAP impostati su ASDM vengono salvati nella memoria flash ASA come dap.xml. Al termine di queste impostazioni, in dap.xml vengono generati tre record DAP. È possibile confermare i dettagli di ogni record DAP in dap.xml.





**Nota:** l'ordine in cui viene eseguito il confronto con DAP è l'ordine di visualizzazione in dap.xml. Ultima corrispondenza per il DAP predefinito (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

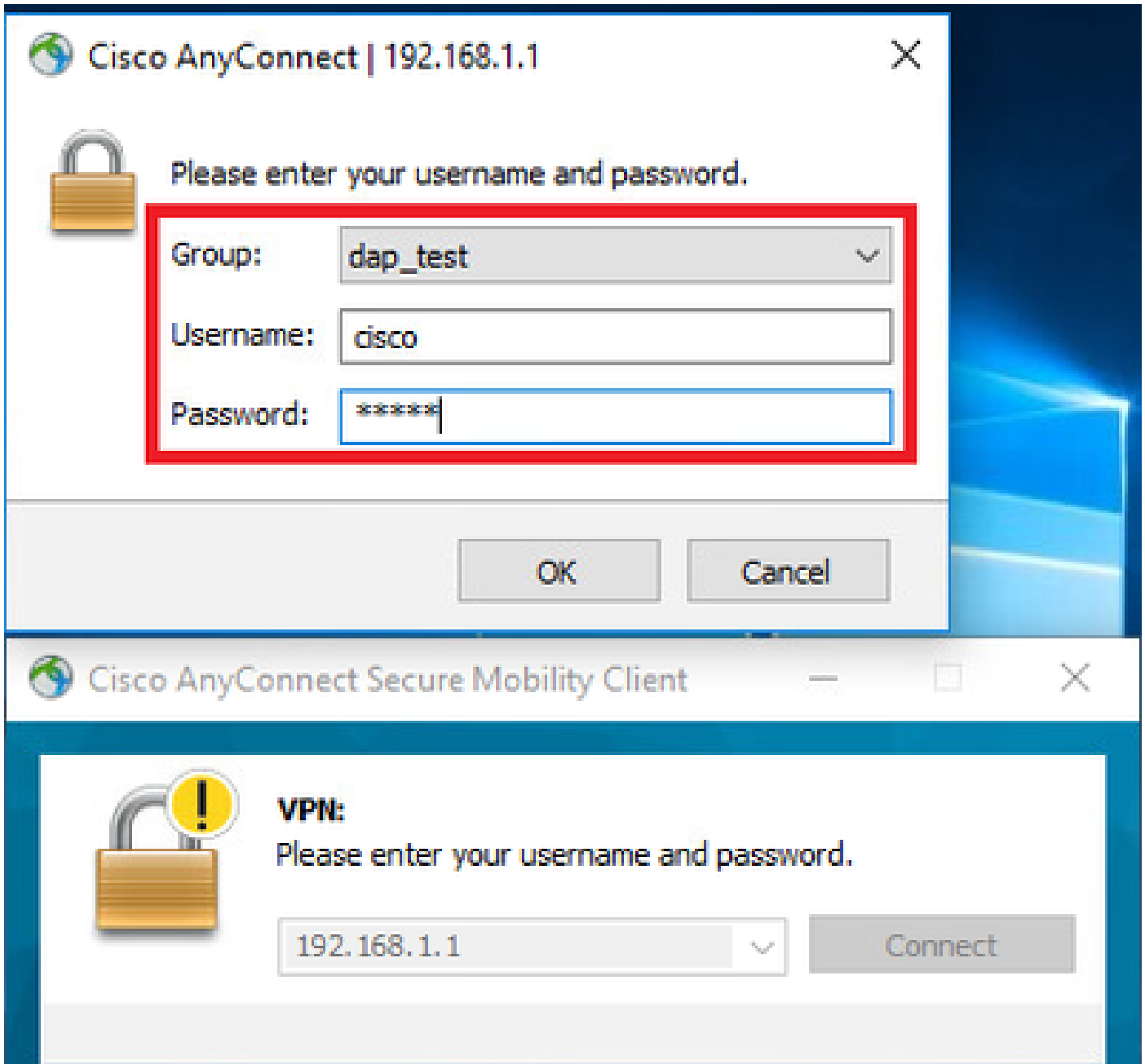
```
</value> <--- 3rd DAP group policy <operation>EQ</operation> <type>caseless</type> </attr> </dapSelecti  
endpoint.device.MAC["0050.5698.e609"]
```

```
</name> <--- 3rd DAP MAC Address condition <value>>true</value> <type>caseless</type> <operation>EQ</ope
```

Verifica

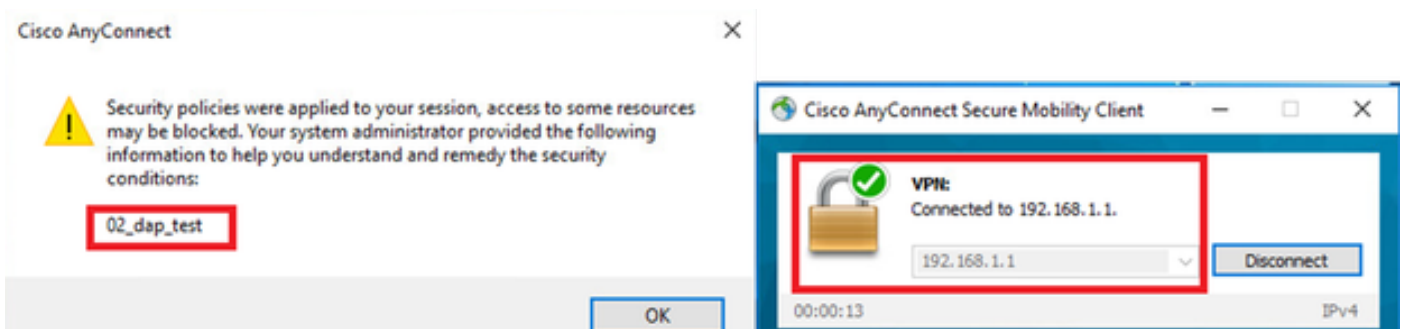
Scenario1. Corrispondenza di un solo DAP

1. Verificare che l'indirizzo MAC dell'endpoint sia 0050.5698.e605 corrispondente alla condizione MAC in 02\_dap\_test.
2. Sull'endpoint, eseguire la connessione Anyconnect e immettere nome utente e password.



*Immettere nome utente e password*

3. Nell'interfaccia utente di Anyconnect, confermare che il valore di 02\_dap\_test sia corrispondente.



*Conferma messaggio utente nell'interfaccia utente*

4. Nel syslog dell'ASA, confermare la corrispondenza di 02\_dap\_test.

---

**Nota:** verificare che la traccia del dap di debug sia abilitata nell'appliance 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
```

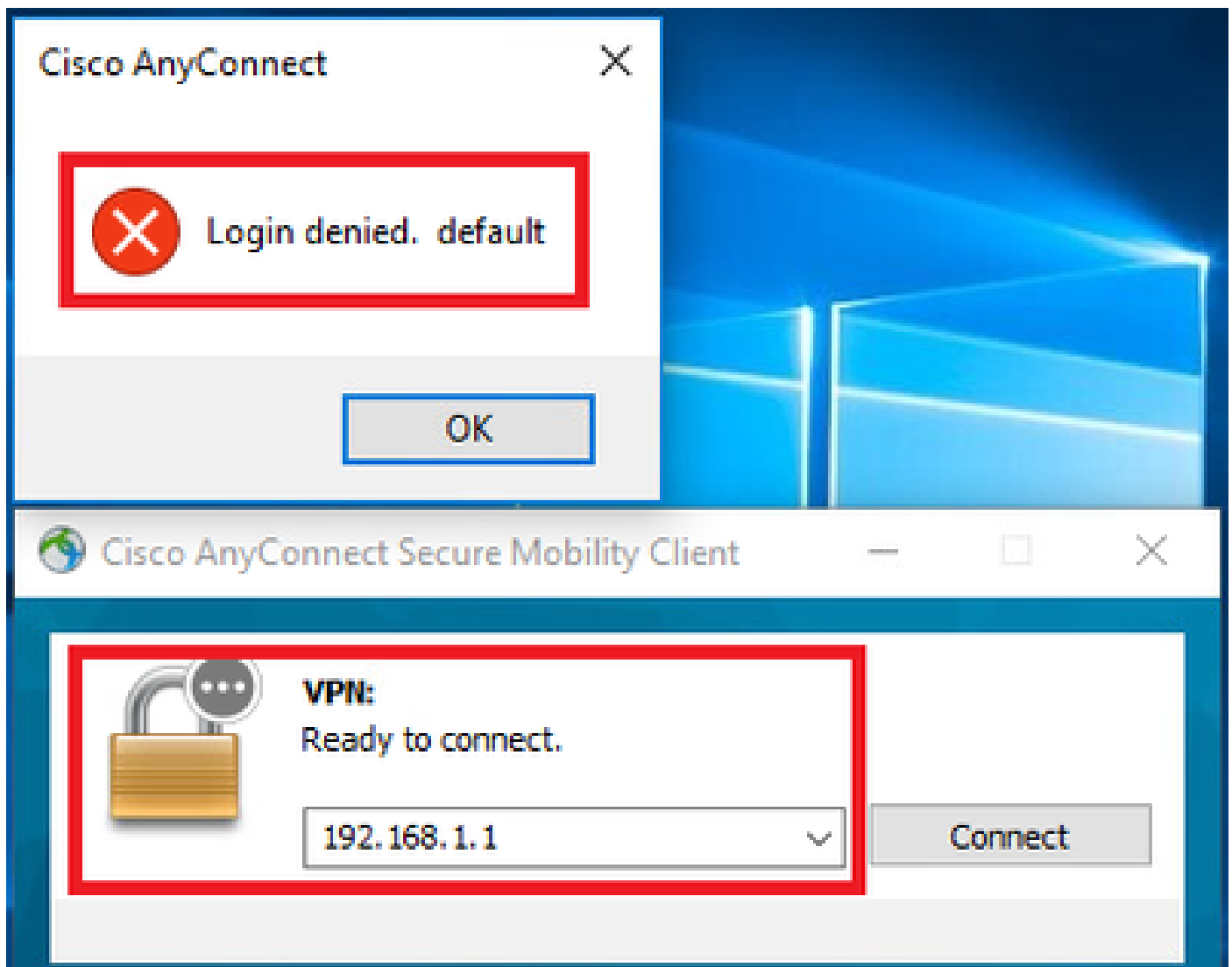
```
Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 11:46:11: %ASA-4-711001: I
```

Scenario2. Corrispondenza DAP predefinito

1. Modificare il valore di endpoint.device.MAC in 02\_dap\_test in 0050.5698.e607 che non corrisponde al valore MAC dell'endpoint.

2. Sull'endpoint, eseguire la connessione Anyconnect e immettere nome utente e password.

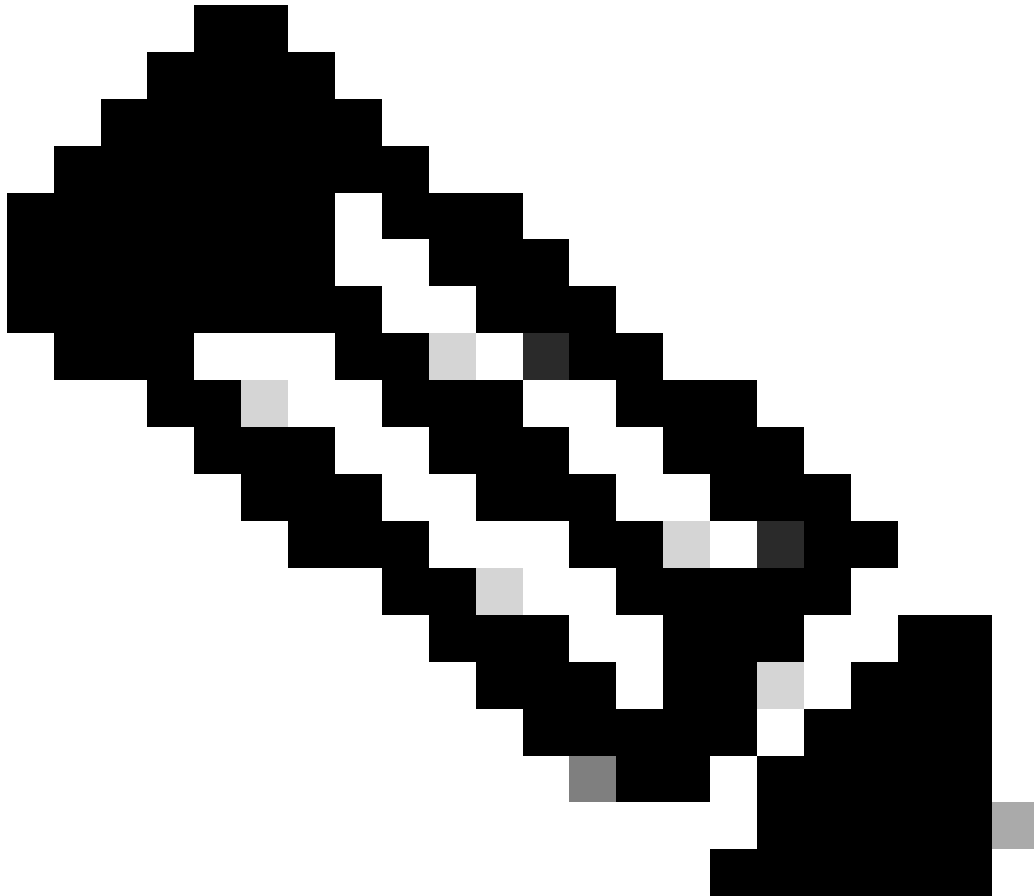
3. Confermare che la connessione Anyconnect è stata negata.



Conferma messaggio utente nell'interfaccia utente

4. Nel syslog ASA, confermare che DfltAccessPolicy corrisponda.

---



**Nota:** per impostazione predefinita, l'azione di DfltAccessPolicy è Termina.

---

<#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

### Scenario 3. Corrispondenza di più punti di accesso al database (Azione : Continua)

1. Modificare l'azione e l'attributo in ogni punto di accesso al database.

.01\_dap\_test :

dapSelection (Indirizzo MAC) = endpoint.device.MAC[0050.5698.e605] = MAC di Anyconnect Endpoint

Action = **Continua**

.02\_dap\_test :

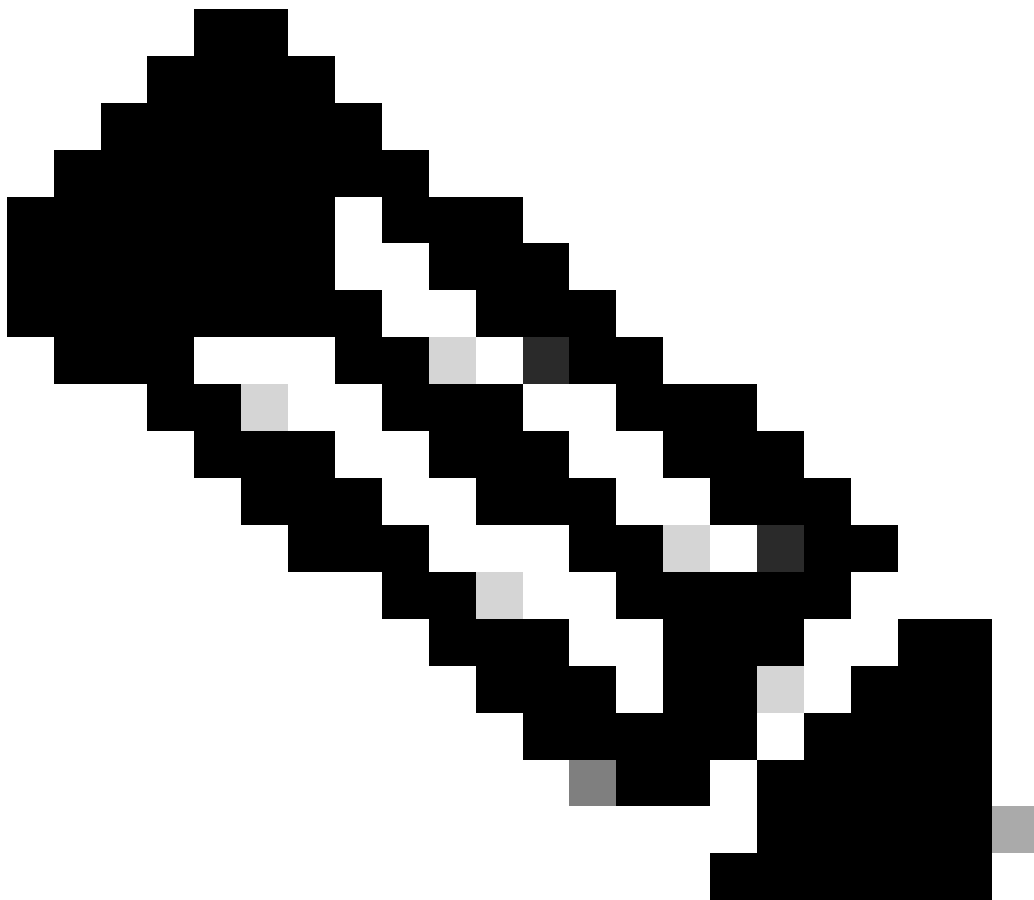
dapSelection (Nome host) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Nome host dell'endpoint Anyconnect

Action = **Continua**

·Elimina record DAP 03\_dap\_test

2. Sull'endpoint, eseguire la connessione Anyconnect e immettere nome utente e password.

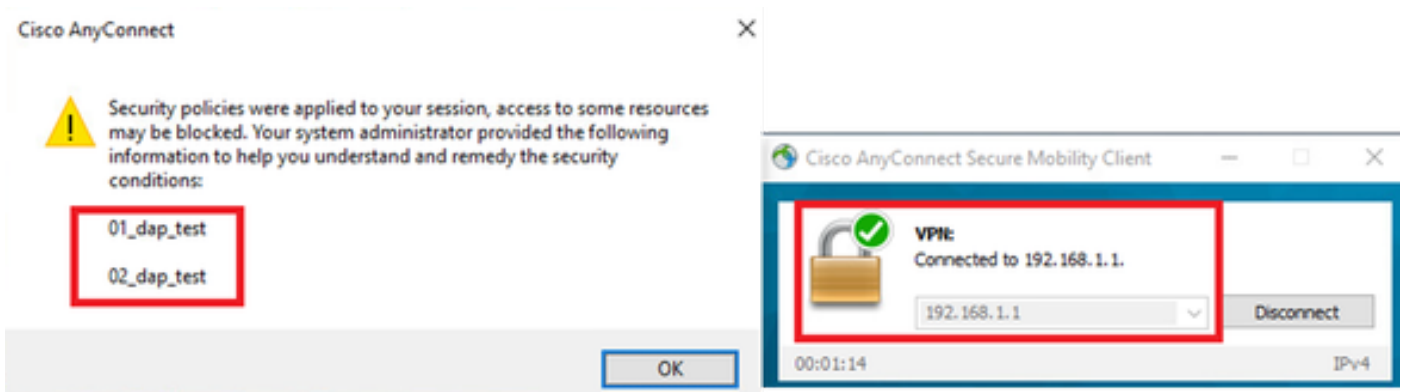
3. Nell'interfaccia utente di Anyconnect, verificare che tutti e 2 i DAP siano corrispondenti



**Nota:** se una connessione corrisponde a più DAP, i messaggi utente di più DAP vengono integrati e visualizzati insieme nell'interfaccia utente di Anyconnect.

---





Conferma messaggio utente nell'interfaccia utente

4. Nel syslog dell'ASA, confermare che tutti e due i DAP siano stati associati.

<#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

#### Scenario 4. Corrispondenza di più punti di accesso dati (Azione :Termina) completata

1. Modificare l'azione di 01\_dap\_test.

·01\_dap\_test :

dapSelection (Indirizzo MAC) = endpoint.device.MAC[0050.5698.e605] = MAC di Anyconnect Endpoint

Azione = **Termina**

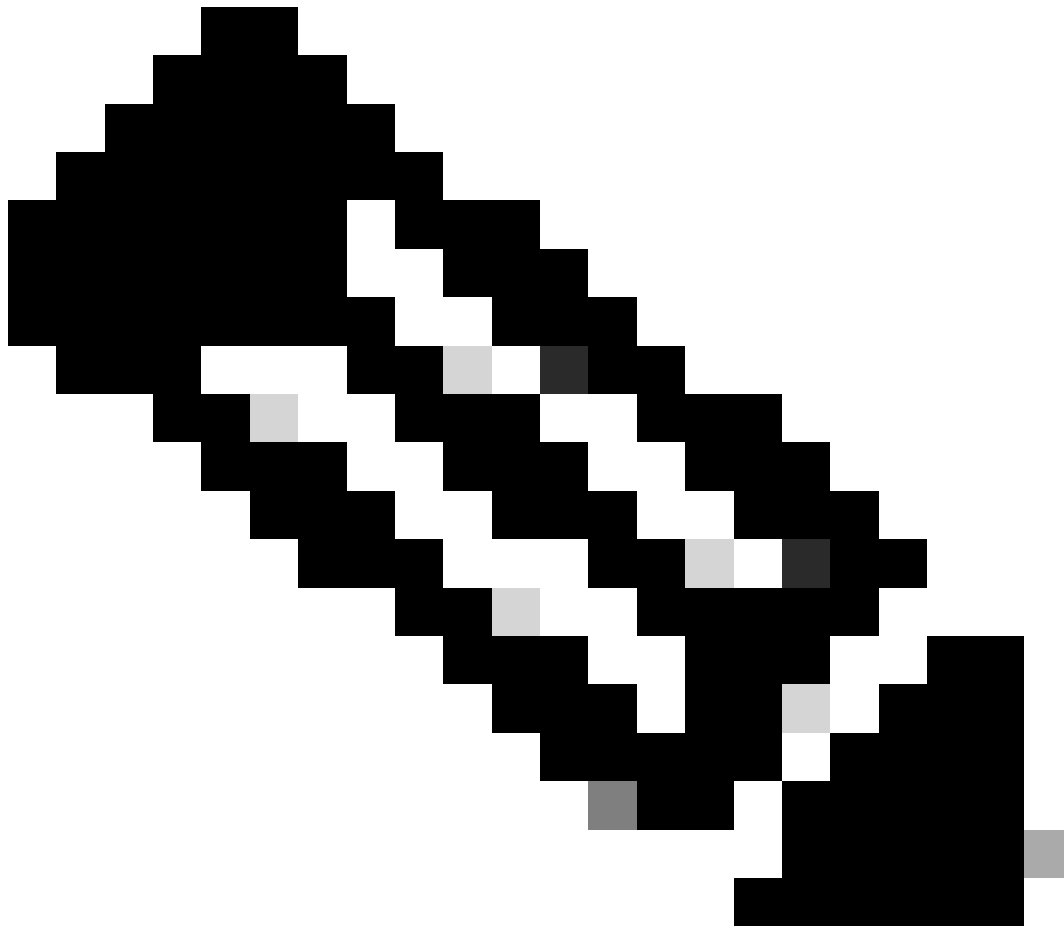
·02\_dap\_test :

dapSelection (Nome host) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Nome host dell'endpoint Anyconnect

Action = **Continua**

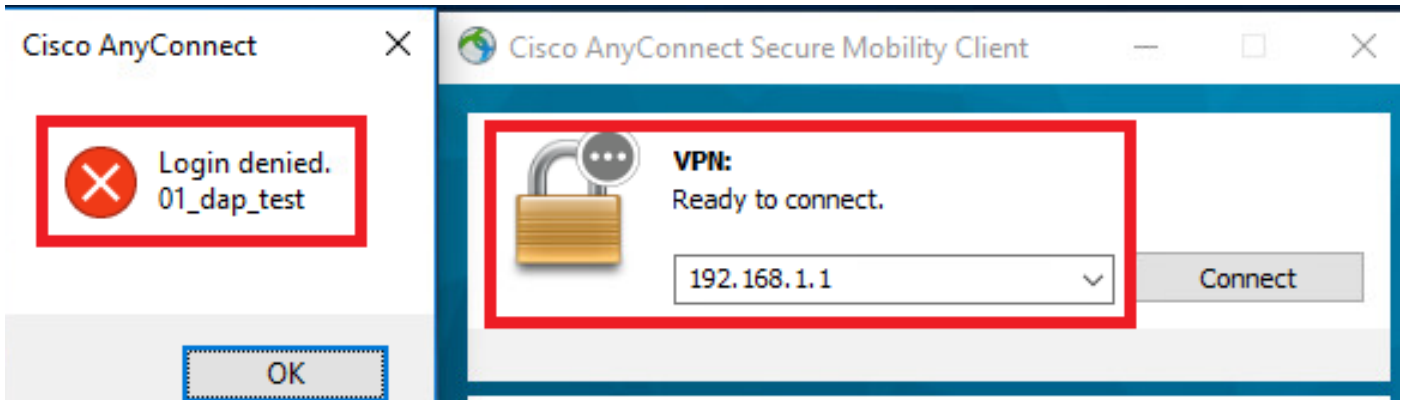
2. Sull'endpoint, eseguire la connessione Anyconnect e immettere nome utente e password.

3. Nell'interfaccia utente di Anyconnect, verificare che solo **01\_dap\_test** sia corrispondente.



**Nota:** una connessione viene associata al record DAP impostato per terminare l'azione. I record successivi non verranno più abbinati dopo l'azione di terminazione.

---



Conferma messaggio utente nell'interfaccia utente

4. Nel syslog ASA, confermare che solo 01\_dap\_test sia stato trovato.

<#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
```

Risoluzione dei problemi generali

I log di debug consentono di confermare il comportamento dettagliato di DAP nell'appliance 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
```

```
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-
```

Informazioni correlate

<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>

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).