

Bereitstellung von ASA DAP zur Identifizierung der MAC-Adresse für AnyConnect

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfiguration in ASA](#)

[Konfiguration in ASDM](#)

[Überprüfung](#)

[Szenario 1. Es wird nur ein DAP zugeordnet](#)

[Szenario 2. Standard-DAP zugeordnet](#)

[Szenario 3. Mehrere DAPs \(Aktion: Fortfahren\) werden zugeordnet](#)

[Szenario 4. Mehrere DAPs \(Aktion: Terminieren\) werden zugeordnet](#)

[Allgemeine Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Dynamic Access Policies (DAP) über ASDM konfiguriert werden, um die MAC-Adresse des Geräts zu überprüfen, das für AnyConnect-Verbindungen verwendet wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:
Konfiguration von Cisco AnyConnect und HostScan

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

ASAv 9.18 (4)

ASDM 7,20 (1)

AnyConnect 4.10.07073

Hostscan 4.10.07073

Windows 10

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

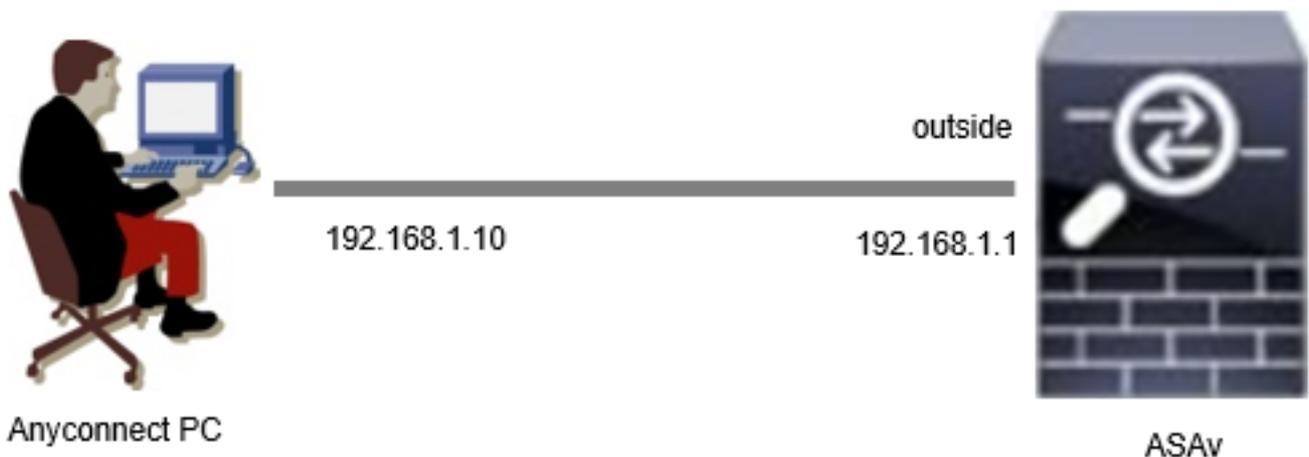
Hintergrundinformationen

HostScan ist ein Softwaremodul, mit dem der AnyConnect Secure Mobility Client Sicherheitsrichtlinien im Netzwerk durchsetzen kann. Während des Hostscan werden verschiedene Details über das Client-Gerät erfasst und an die Adaptive Security Appliance (ASA) zurückgemeldet. Zu diesen Details gehören das Betriebssystem des Geräts, Antivirus-Software, Firewall-Software, MAC-Adresse und mehr. Mit der Funktion "Dynamic Access Policies (DAP)" können Netzwerkadministratoren Sicherheitsrichtlinien auf Benutzerbasis konfigurieren. Das Attribut `endpoint.device.MAC` im DAP kann verwendet werden, um die MAC-Adresse des Client-Geräts mit vordefinierten Richtlinien abzugleichen oder zu überprüfen.

Konfigurieren

Netzwerkdiagramm

Dieses Bild zeigt die Topologie, die für das Beispiel dieses Dokuments verwendet wird.



Diagramm

Konfiguration in ASA

Dies ist die minimale Konfiguration in der 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
```

Konfiguration in ASDM

In diesem Abschnitt wird beschrieben, wie Sie DAP-Datensätze im ASDM konfigurieren. Legen Sie in diesem Beispiel drei DAP-Datensätze fest, die das Attribut `endpoint.device.MAC` als Bedingung verwenden.

- 01_dap_test:endpoint.device.MAC=0050.5698.e608
- 02_dap_test:endpoint.device.MAC=0050.5698.e605 = MAC von AnyConnect-Endgeräten
- 03_dap_test:endpoint.device.MAC=0050.5698.e609

1. Konfigurieren Sie den ersten DAP mit dem Namen 01_dap_test.

Navigieren Sie zu Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies. Klicken Sie auf Hinzufügen, und legen Sie den Richtliniennamen, AAA-Attribut, Endpunkteigenschaften, die Aktion, die Benutzernachricht fest, wie im folgenden Bild dargestellt:

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) | Webype 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

Erstes DAP konfigurieren

Konfigurieren der Gruppenrichtlinie für das AAA-Attribut

Add AAA Attribute ✕

AAA Attribute Type: Cisco

Group Policy: = dap_test_gp

Assigned IPv4 Address: =

Assigned IPv6 Address: =

Connection Profile: = DefaultRAGroup

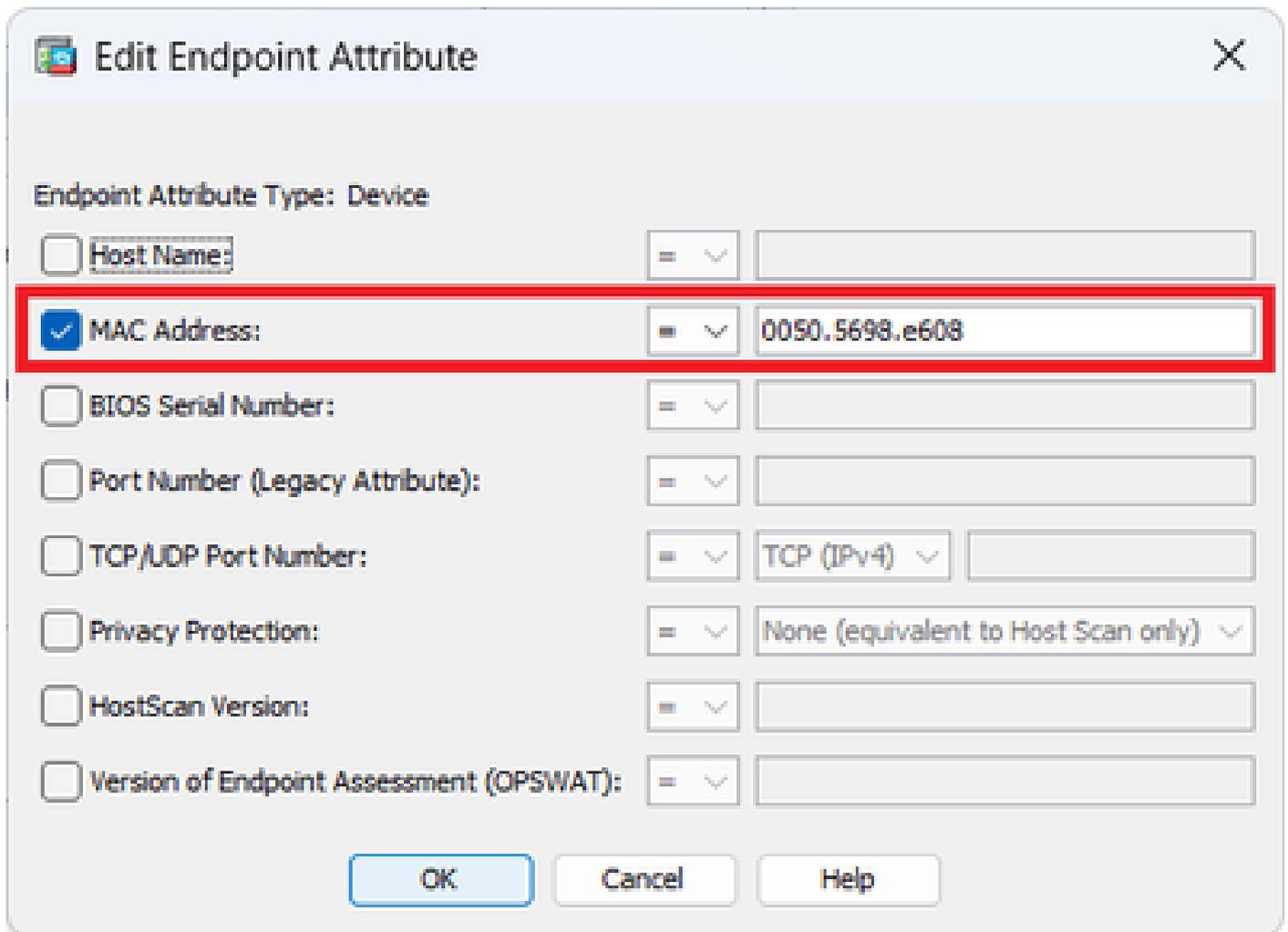
Username: =

Username2: =

SCEP Required: = true

Gruppenrichtlinie für DAP-Datensatz konfigurieren

Konfigurieren der MAC-Adresse für das Endpunktattribut

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". The other rows have their checkboxes unchecked and their values empty. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

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

MAC-Bedingung für DAP konfigurieren

2. Konfigurieren Sie das zweite DAP mit dem Namen 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
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: <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

Zweites DAP konfigurieren

3. Konfigurieren Sie den dritten DAP mit dem Namen 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: <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: **03_dap_test**

OK Cancel Help

Konfigurieren des dritten DAP

4. Verwenden Sie den **more flash:/dap.xml** Befehl, um die Einstellung von DAP-Datensätzen in dap.xml zu bestätigen.

Details der auf dem ASDM gespeicherten DAP-Datensätze werden im ASA-Flash als dap.xml gespeichert. Nach Abschluss dieser Einstellungen werden drei DAP-Datensätze in dap.xml generiert. Sie können die Details jedes DAP-Datensatzes in dap.xml bestätigen.



Hinweis: Die Reihenfolge, in der das DAP zugeordnet wird, ist die Anzeigereihenfolge in dap.xml. Der Standard-DAP (DfltAccessPolicy) wird zuletzt zugeordnet.

```
<#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

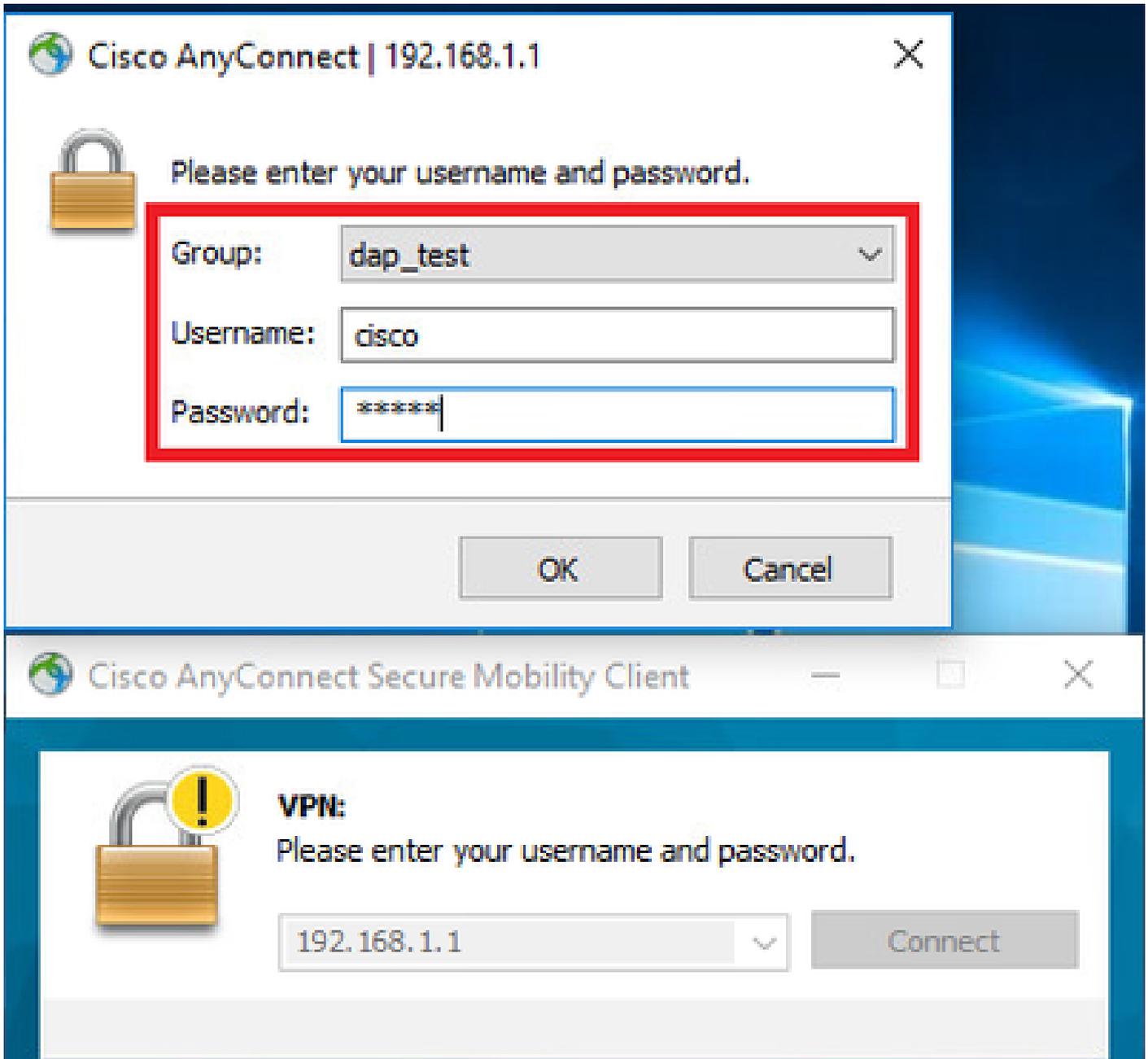
```
</value> <--- 3rd DAP group policy <operation>EQ</operation> <type>caseless</type> </attr> </dapSelecti  
endpoint.device.MAC["0050.5698.e609"]
```

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

Überprüfung

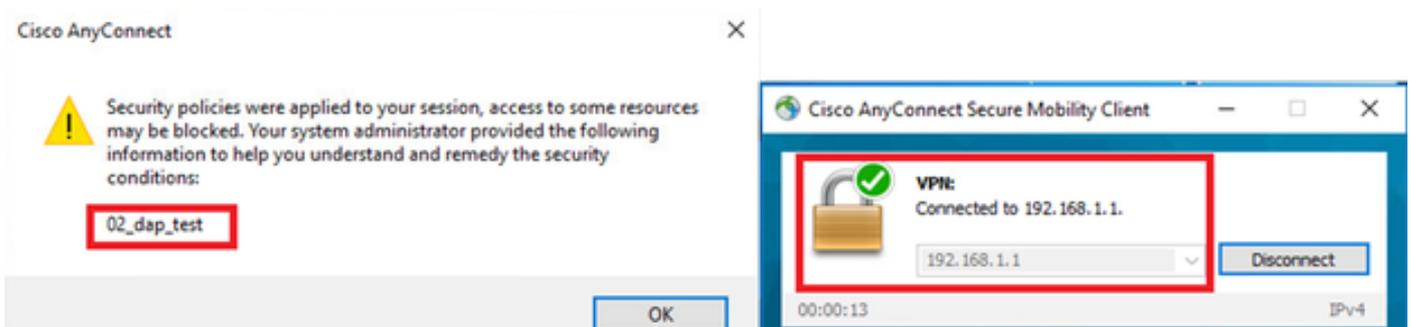
Szenario 1. Es wird nur ein DAP zugeordnet

1. Stellen Sie sicher, dass die MAC-Adresse des Endpunkts 0050.5698.e605 lautet, was der MAC-Bedingung in 02_dap_test entspricht.
2. Führen Sie auf dem Endpunkt AnyConnect-Verbindung aus, und geben Sie Benutzername und Kennwort ein.



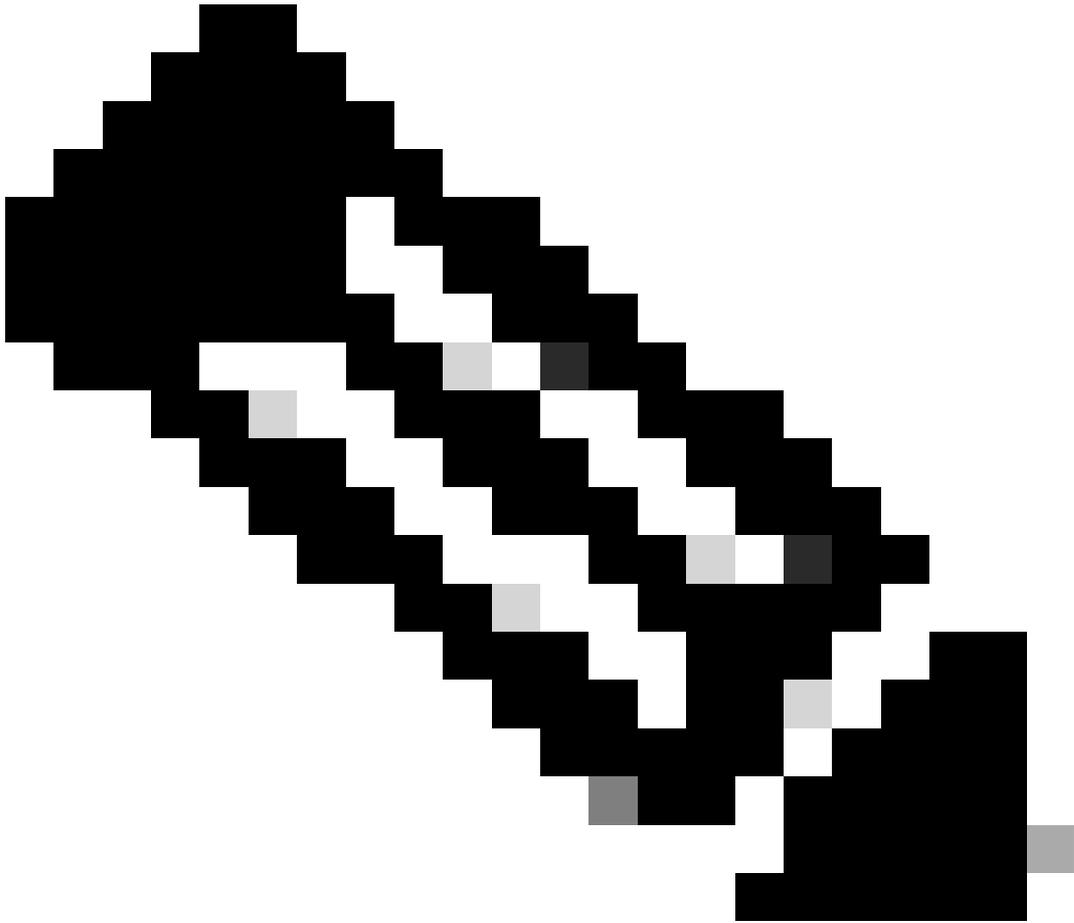
Benutzername und Kennwort eingeben

3. Bestätigen Sie in der AnyConnect-Benutzeroberfläche, dass 02_dap_test zugeordnet ist.



Benutzernachricht in der Benutzeroberfläche bestätigen

4. Bestätigen Sie im ASA-Syslog, dass 02_dap_test zugeordnet ist.



Hinweis: Stellen Sie sicher, dass die Debug-Dap-Verfolgung in ASA aktiviert ist.

<#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

: ,

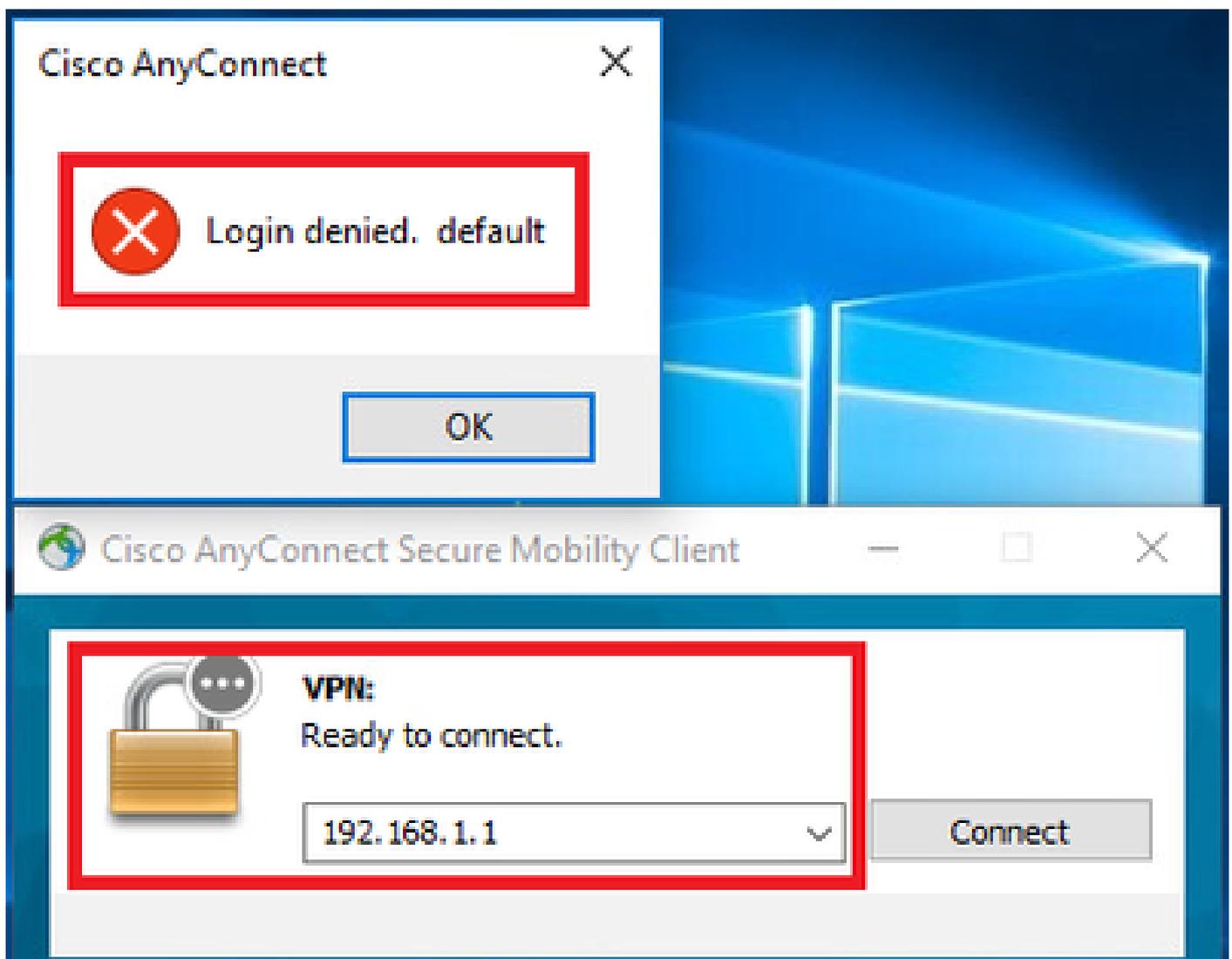
02_dap_test

```
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
```

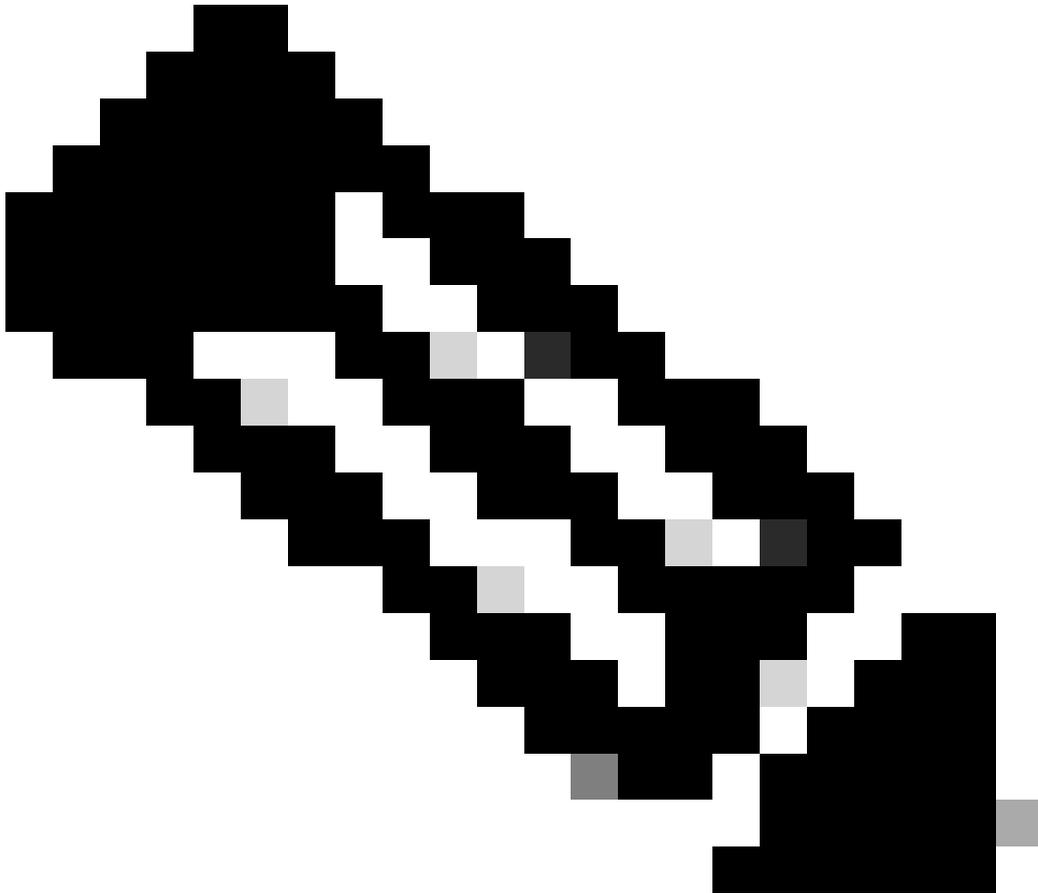
Szenario 2. Standard-DAP zugeordnet

1. Ändern Sie den Wert von endpoint.device.MAC in 02_dap_test in 0050.5698.e607, der nicht mit der MAC des Endpunkts übereinstimmt.
2. Führen Sie auf dem Endpunkt AnyConnect-Verbindung aus, und geben Sie Benutzername und Kennwort ein.
3. Bestätigen Sie, dass die AnyConnect-Verbindung abgelehnt wurde.



Benutzernachricht in der Benutzeroberfläche bestätigen

4. Überprüfen Sie im ASA-Syslog, ob die DfltAccessPolicy zugeordnet ist.



Hinweis: Standardmäßig lautet die Aktion von DfltAccessPolicy 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

Szenario 3. Mehrere DAPs (Aktion: Fortfahren) werden zugeordnet

1. Ändern Sie die Aktion und das Attribut in jedem DAP.

- 01_dap_test :
dapSelection (MAC-Adresse) = endpoint.device.MAC[0050.5698.e605] = MAC of AnyConnect Endpoint
Aktion = **Fortfahren**
- 02_dap_test :

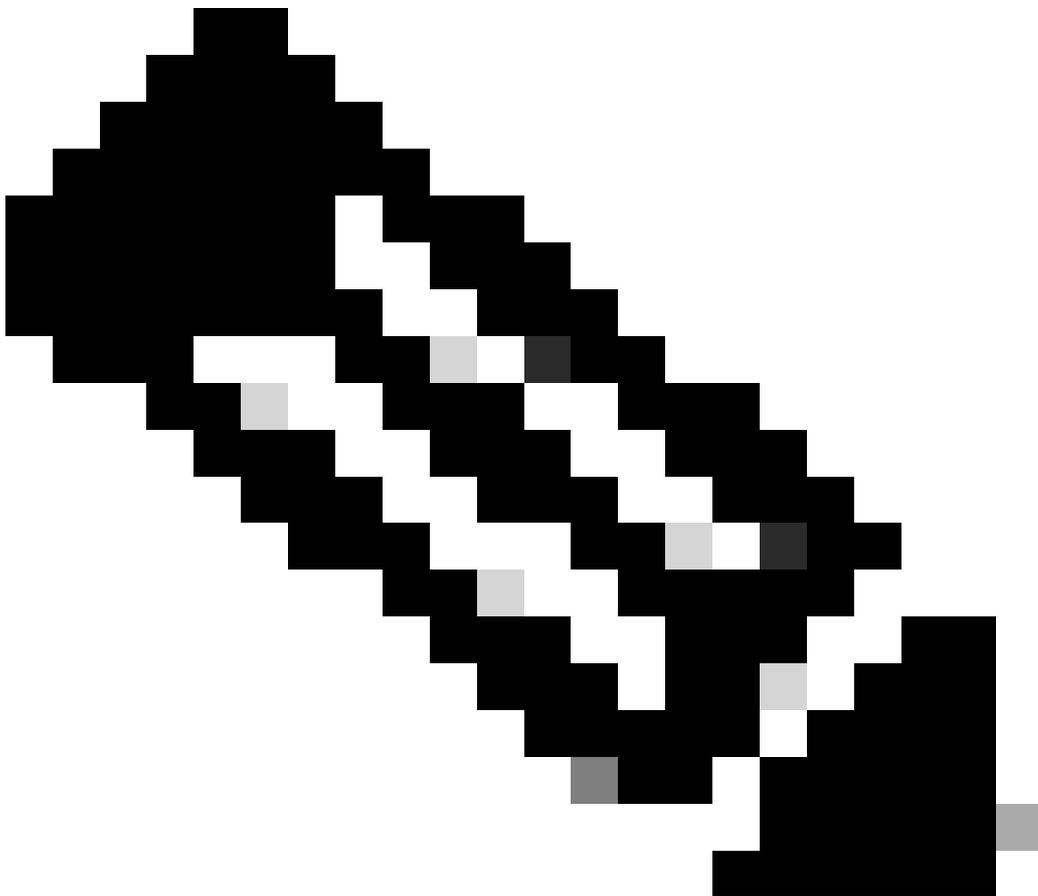
dapSelection (Hostname) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Hostname des AnyConnect-Endpunkts

Aktion = **Fortfahren**

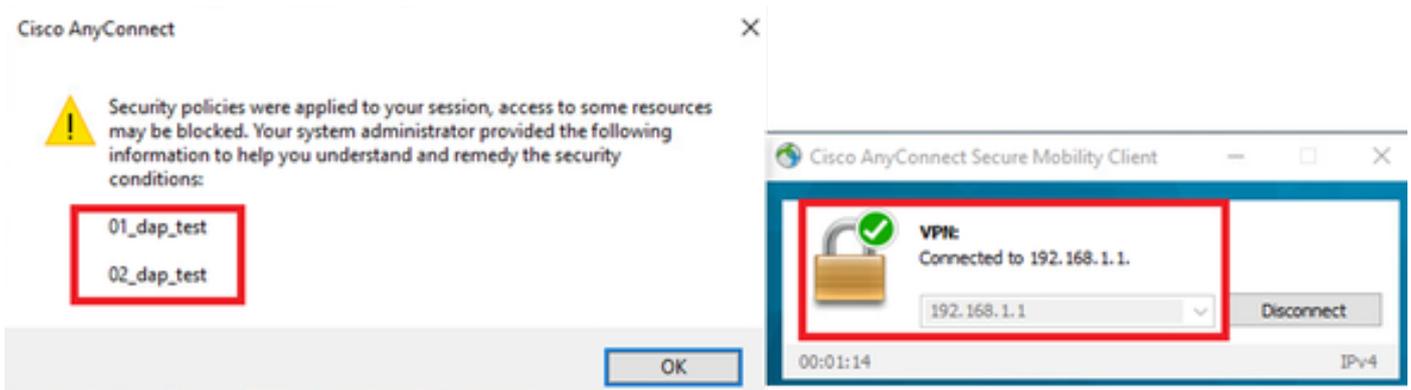
- 03_dap_test DAP-Eintrag löschen

2. Führen Sie auf dem Endpunkt AnyConnect-Verbindung aus, und geben Sie Benutzername und Kennwort ein.

3. Überprüfen Sie in der AnyConnect-Benutzeroberfläche, ob alle 2 DAPs übereinstimmen.



Hinweis: Wenn eine Verbindung mit mehreren DAPs übereinstimmt, werden die Benutzermeldungen mehrerer DAPs in der AnyConnect-Benutzeroberfläche integriert und zusammen angezeigt.



Benutzernachricht in der Benutzeroberfläche bestätigen

4. Stellen Sie im ASA-Syslog sicher, dass alle beiden DAPs übereinstimmen.

<#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

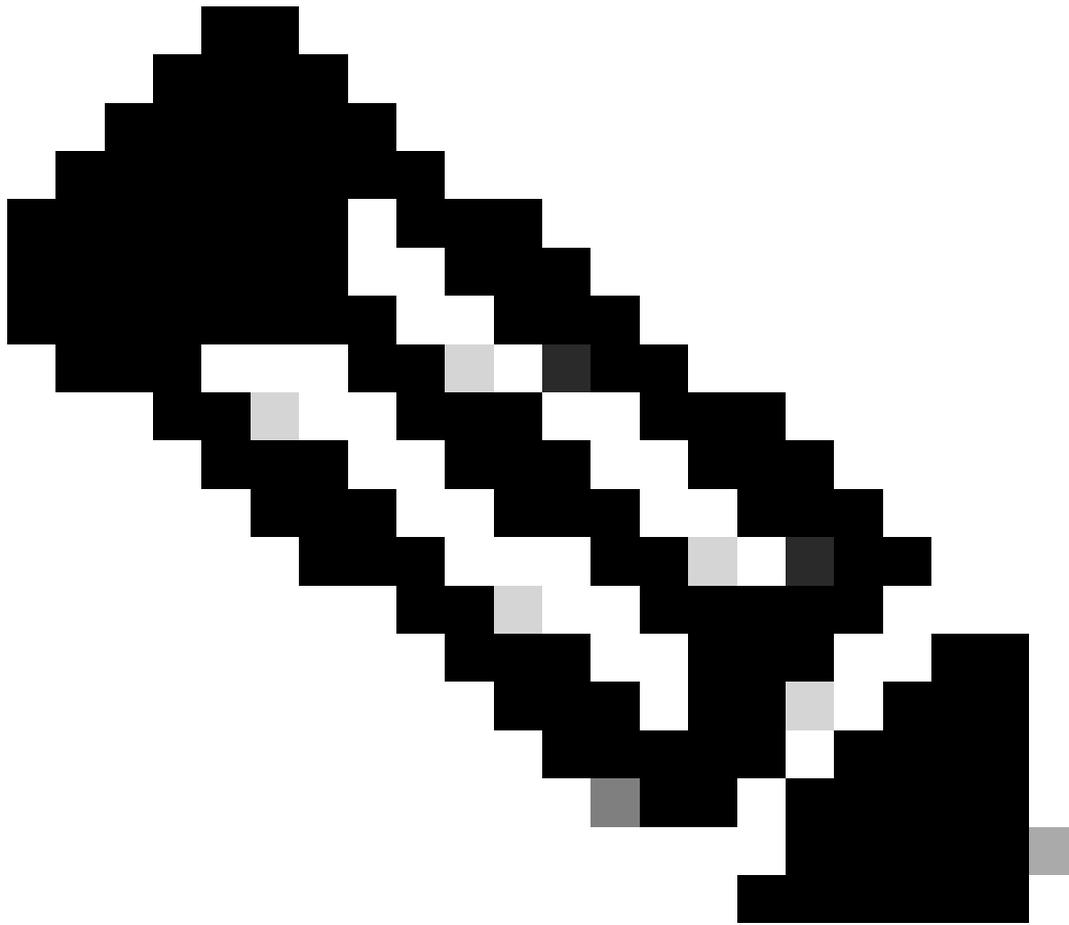
Szenario 4. Mehrere DAPs (Aktion :Beenden) werden zugeordnet

1. Ändern Sie die Aktion von 01_dap_test.

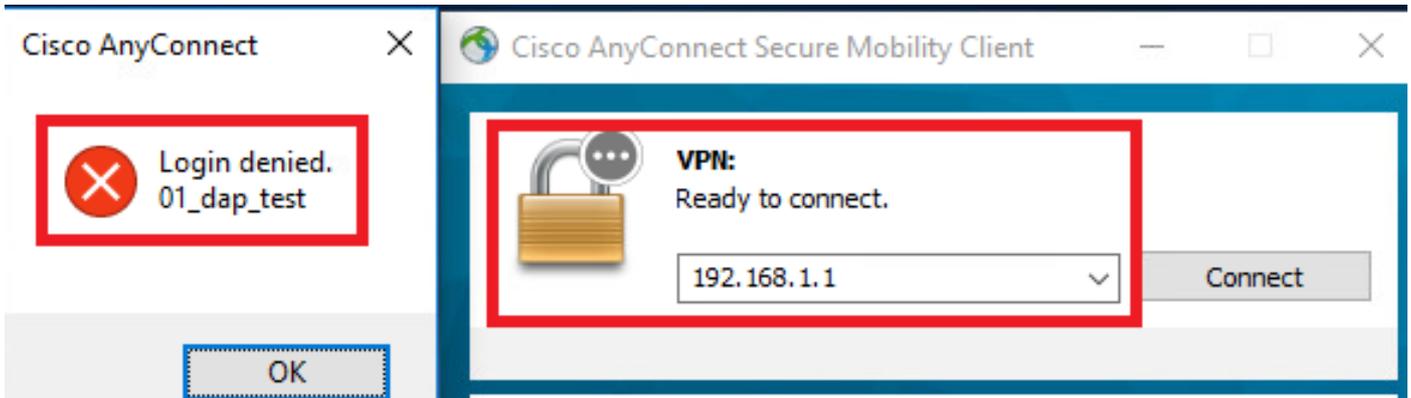
- 01_dap_test :
dapSelection (MAC-Adresse) = endpoint.device.MAC[0050.5698.e605] = MAC of AnyConnect Endpoint
Aktion = **Beenden**
- 02_dap_test :
dapSelection (Hostname) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Hostname des AnyConnect-Endpunkts
Aktion = **Fortfahren**

2. Führen Sie auf dem Endpunkt AnyConnect-Verbindung aus, und geben Sie Benutzername und Kennwort ein.

3. Überprüfen Sie in der AnyConnect-Benutzeroberfläche, ob nur **01_dap_test** übereinstimmt.



Hinweis: Eine Verbindung wird dem DAP-Datensatz zugeordnet, der so eingestellt wurde, dass die Aktion beendet wird. Nachfolgende Datensätze werden nach der Terminierungsaktion nicht mehr abgeglichen.



Benutzernachricht in der Benutzeroberfläche bestätigen

4. Bestätigen Sie im ASA-Syslog, dass nur "01_dap_test" zugeordnet ist.

<#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
```

Allgemeine Fehlerbehebung

Diese Debug-Protokolle helfen Ihnen, das detaillierte Verhalten von DAP in ASA zu bestätigen.

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-
```

Zugehörige Informationen

<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>

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.