نشر ASA DAP لتحديد عنوان MAC ل AnyConnect

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين سياسات الوصول الديناميكي (DAP) عبر ASDM، للتحقق من عنوان MAC الخاص بالجهاز المستخدم لاتصال AnyConnect.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:
تكوين Cisco AnyConnect و Hostscan

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:
ASAv 9.18 (4)
ASDM 7.20 (1)
AnyConnect 4.10.07073
Hostscan 4.10.07073
نظام التشغيل Windows 10

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

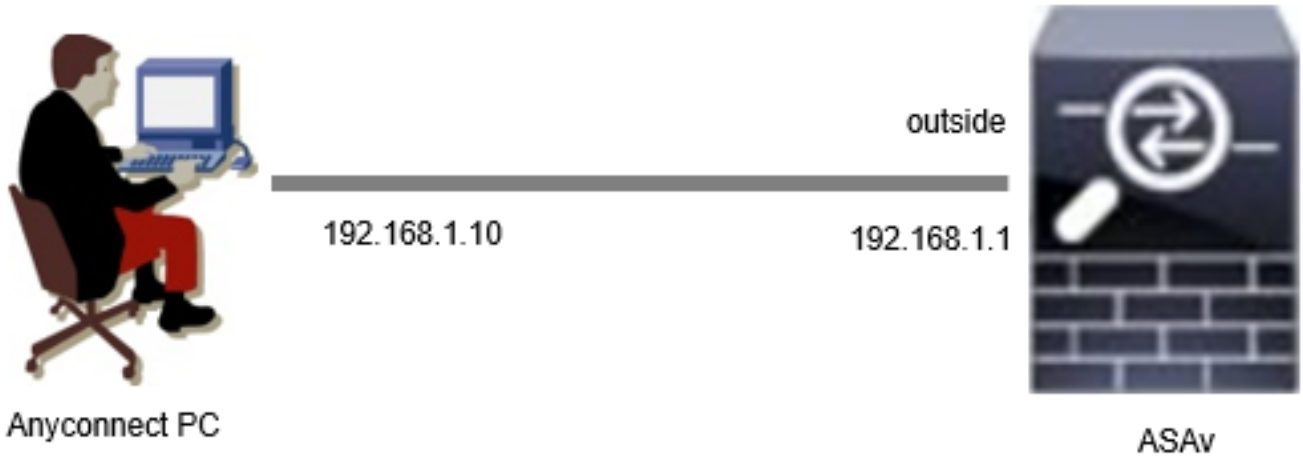
معلومات أساسية

HostScan هو وحدة برمجية توفر ل AnyConnect Secure Mobility Client القدرة على فرض سياسات الأمان على الشبكة. أو أثناء عملية Hostscan، يتم تجميع تفاصيل متنوعة حول جهاز العميل وإبلاغها مرة أخرى إلى جهاز الأمان القابل للتكيف (ASA). وتتضمن هذه التفاصيل نظام تشغيل الجهاز وبرامج مكافحة الفيروسات وبرامج جدار الحماية وعنوان MAC وغير ذلك الكثير. تتيح ميزة "سياسات الوصول الديناميكي (DAP)" لمسؤولي الشبكة تكوين سياسات الأمان على أساس كل مستخدم، ويمكن إستخدام سمة endpoint.device.mac لمطابقة عنوان MAC لجهاز العميل وأي التحقق منه مقابل السياسات المحددة مسبقا في DAP.

التكوين

الرسم التخطيطي للشبكة

تعرض هذه الصورة المخطط الذي يتم إستخدامه لمثال هذا المستند.



الرسم التخطيطي

تكوين في ASA

هذا هو الحد الأدنى للتكوين في 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
```

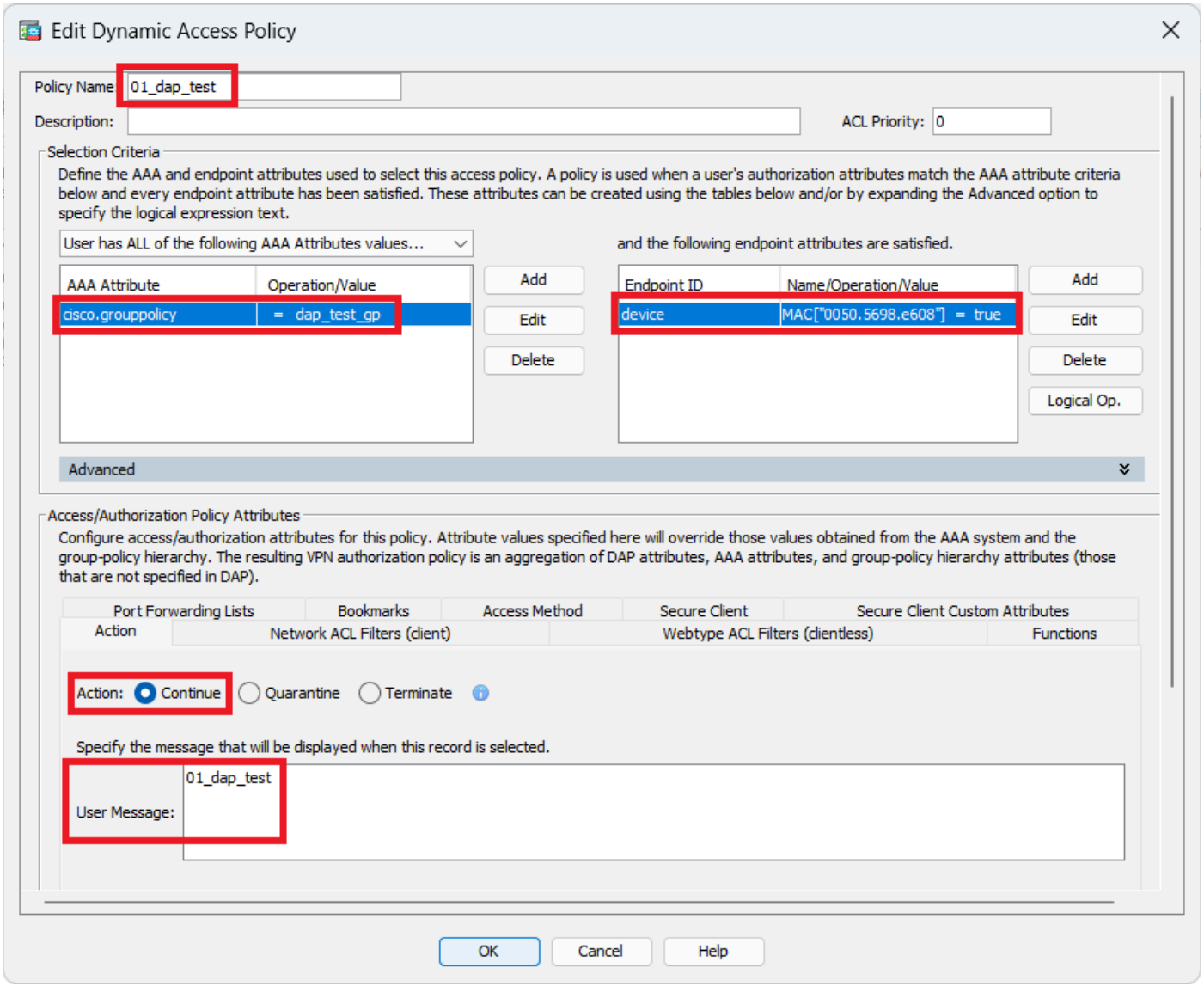
التكوين في ASDM

يصف هذا القسم كيفية تكوين سجل DAP في ASDM. في هذا المثال، قم بتعيين 3 سجلات DAP التي تستخدم سمة endpoint.device.mac كشرط.

·01_dap_test:endpoint.device.mac=0050.5698.e608
·02_dap_test:endpoint.device.mac=0050.5698.e605 = MAC لنقطة نهاية AnyConnect
·03_dap_test:endpoint.device.mac=0050.5698.e609

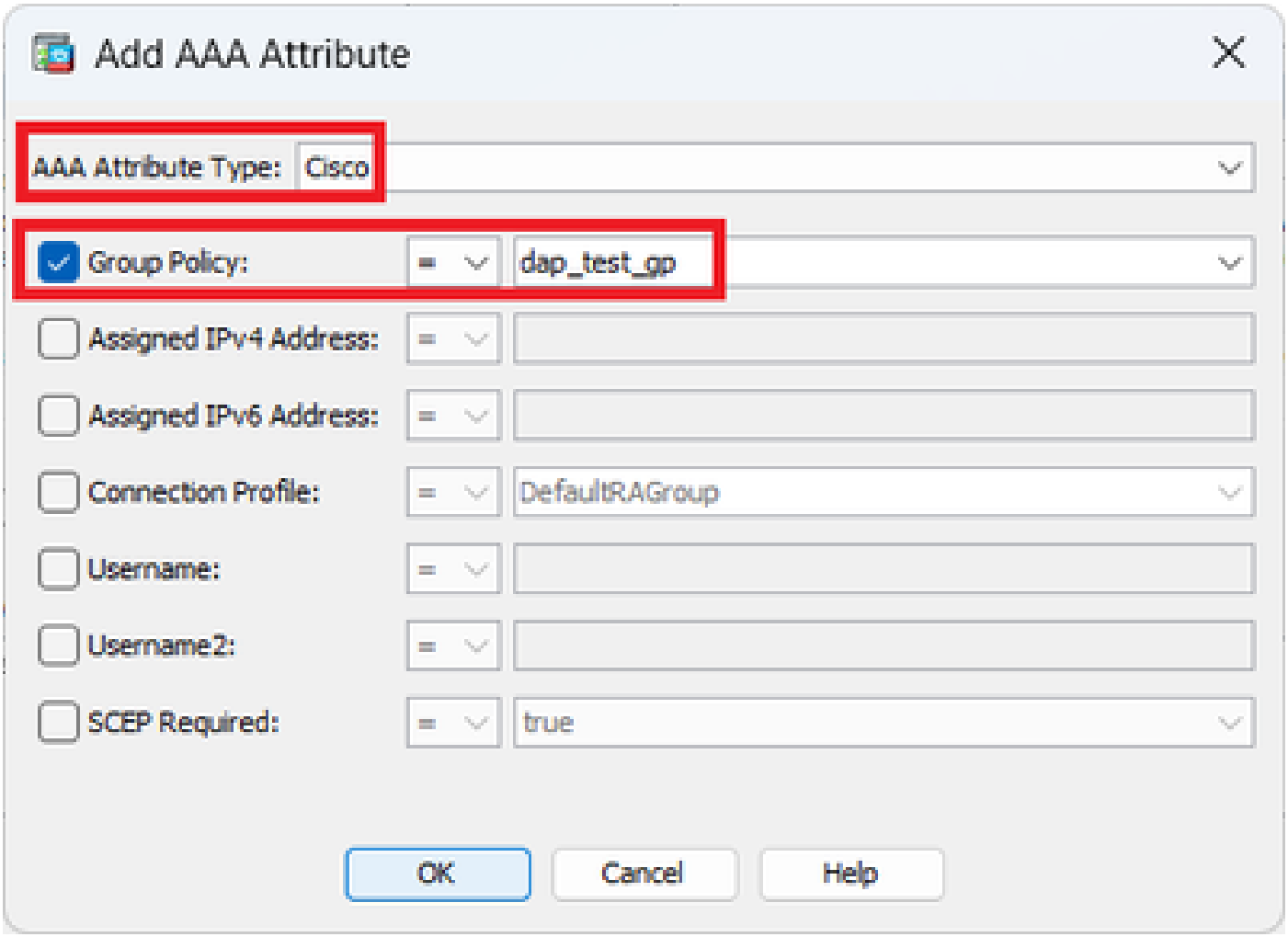
1. قم بتكوين DAP الأول المسمى 01_dap_test.

انتقل إلى التكوين>Remote Access VPN للوصول عن بعد>الوصول إلى الشبكة (العميل)>سياسات الوصول الديناميكية. انقر فوق إضافة ، وقم بتعيين اسم النهج وسمة AAA و سمات نقطة النهاية والإجراء ورسالة المستخدم، كما هو موضح في الصورة:



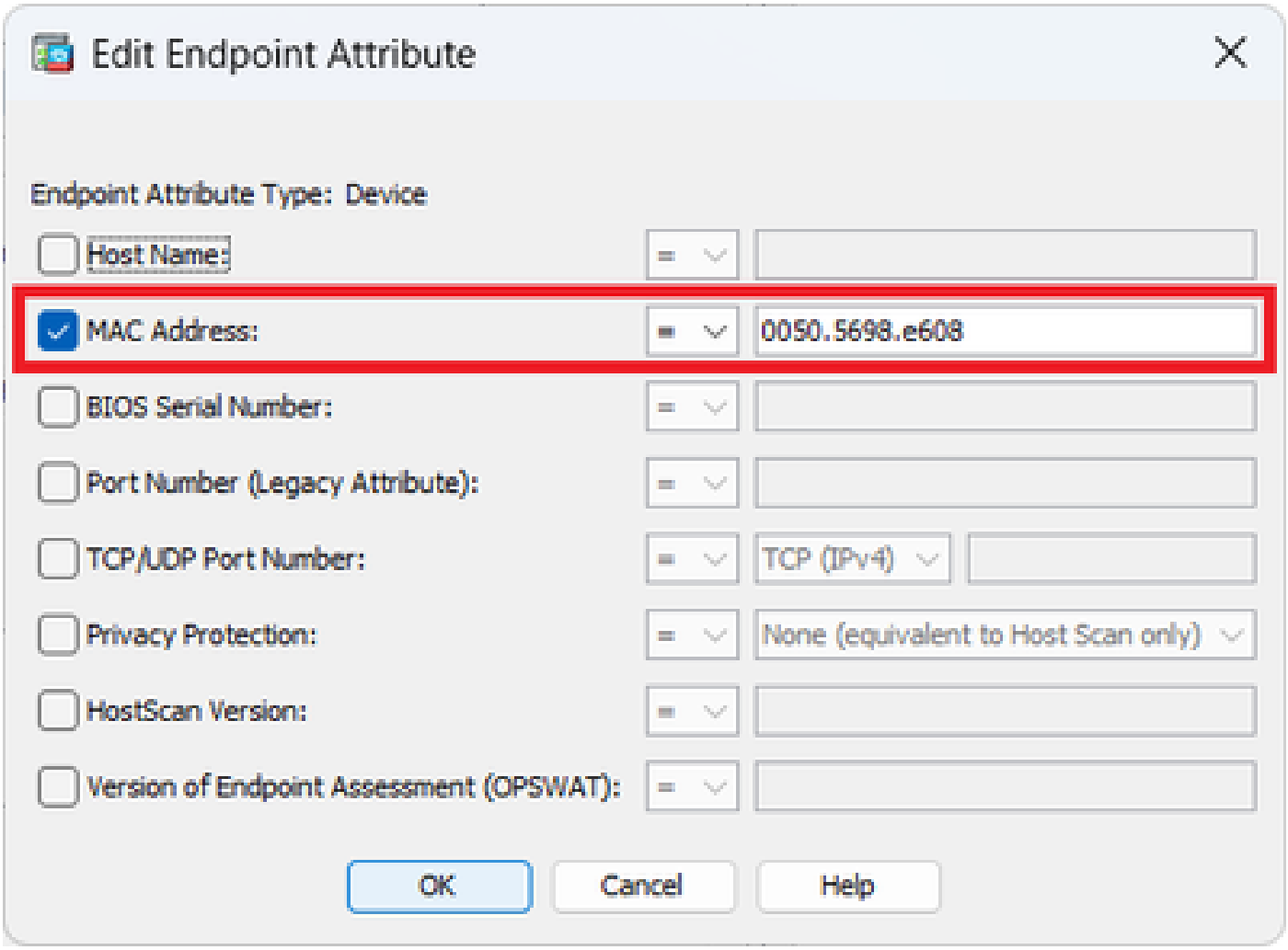
تكوين DAP الأول

تكوين نهج المجموعة لسمة AAA.



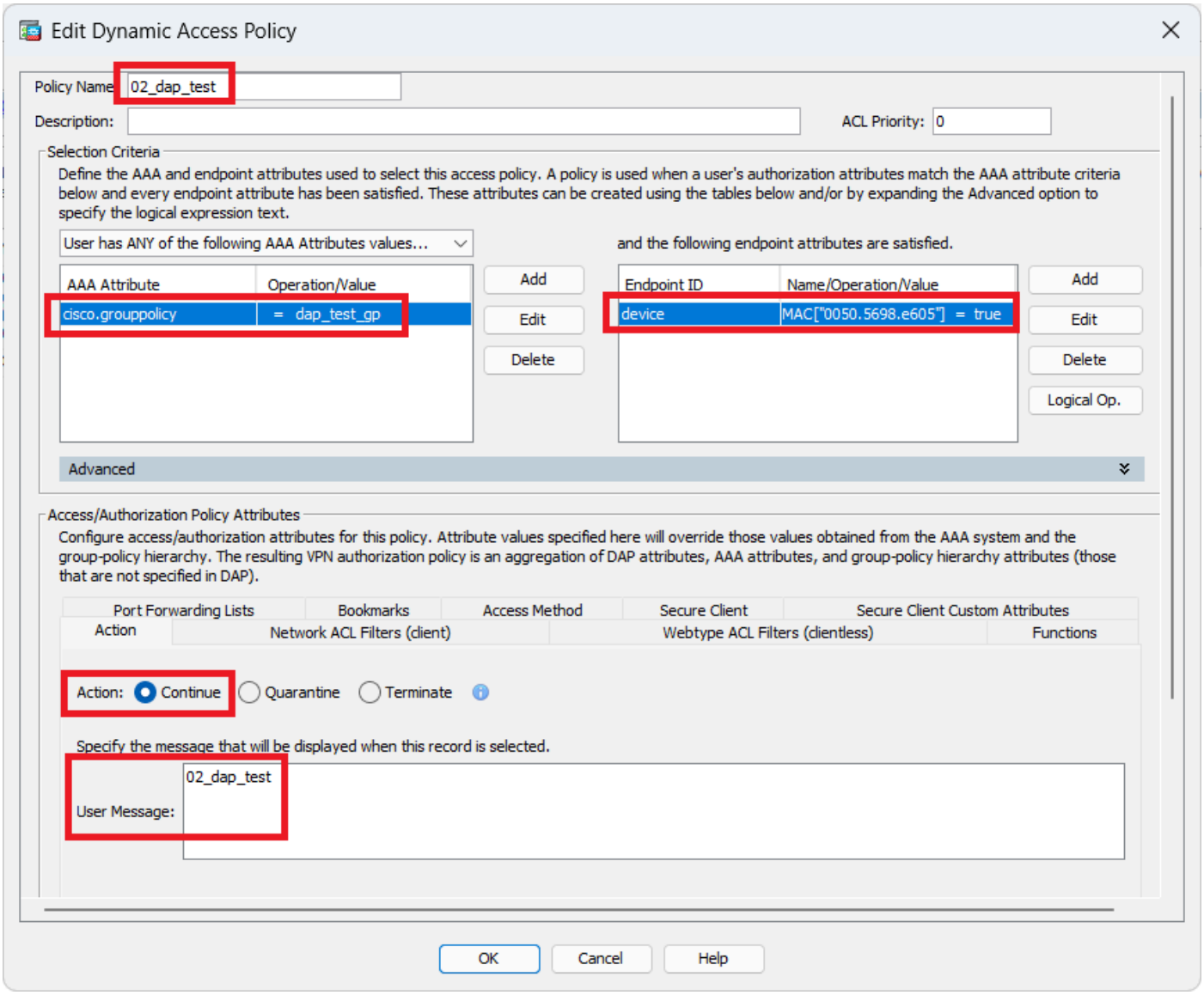
تكوين نهج المجموعة لسجل DAP

تكوين عنوان MAC لسمة نقطة النهاية.



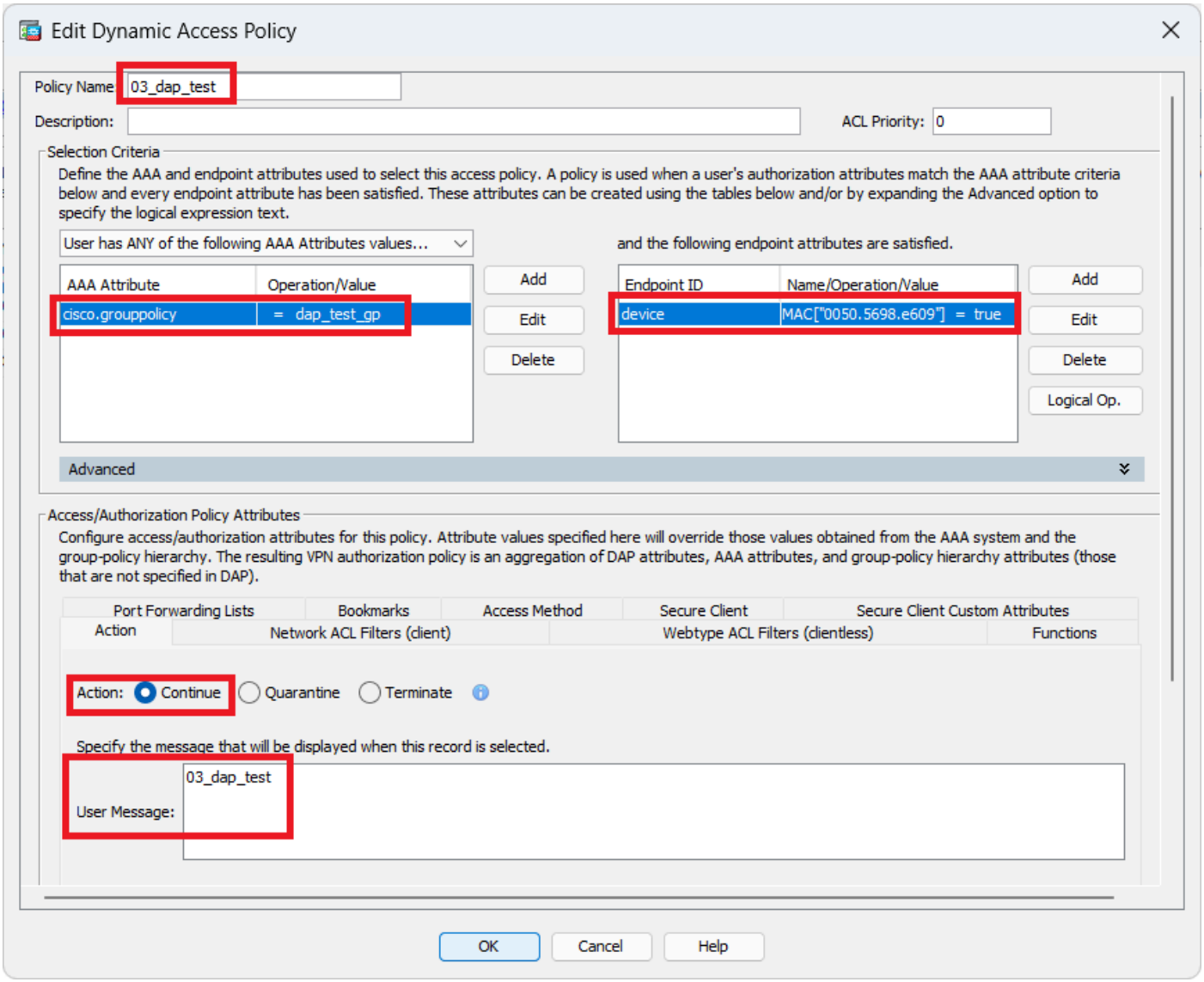
تكوين شرط MAC ل DAP

2. قم بتكوين DAP الثاني المسمى 02_dap_test.



تكوين DAP الثاني

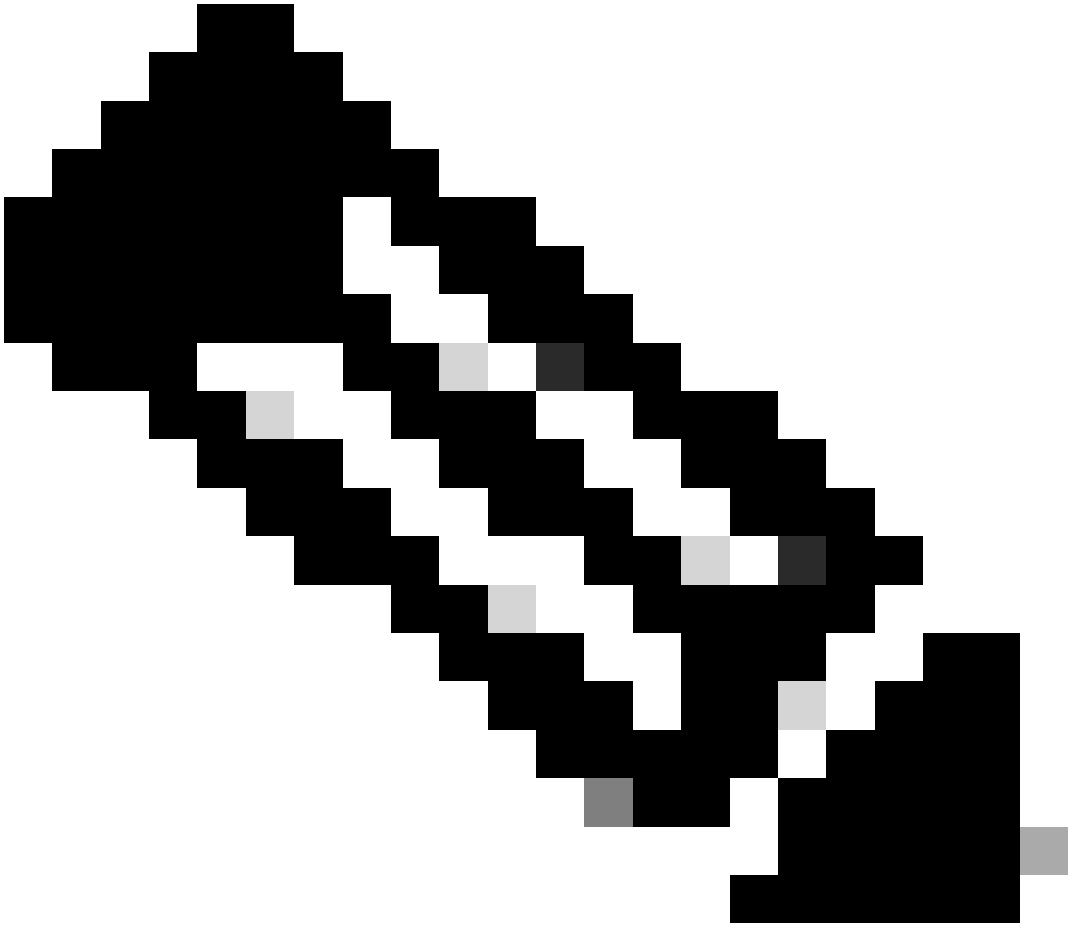
3. قم بتكوين DAP الثالث المسمى 03_dap_test.



تكوين DAP الثالث

4. أستخدم **more flash:/dap.xml** الأمر لتأكيد إعداد سجلات DAP في dap.xml.

يتم حفظ تفاصيل سجلات DAP المعينة على ASDM في ذاكرة ASA المؤقتة على هيئة dap.xml. بعد اكتمال هذه الإعدادات، يتم إنشاء ثلاثة سجلات DAP في dap.xml. يمكنك تأكيد تفاصيل كل سجل DAP في dap.xml.



ةظحالم: ترتيب مطابقة DAP هو ترتيب العرض في dap.xml. DAP الافتراضي (DfltAccessPolicy) مطابق لآخر رمز.

<#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"]

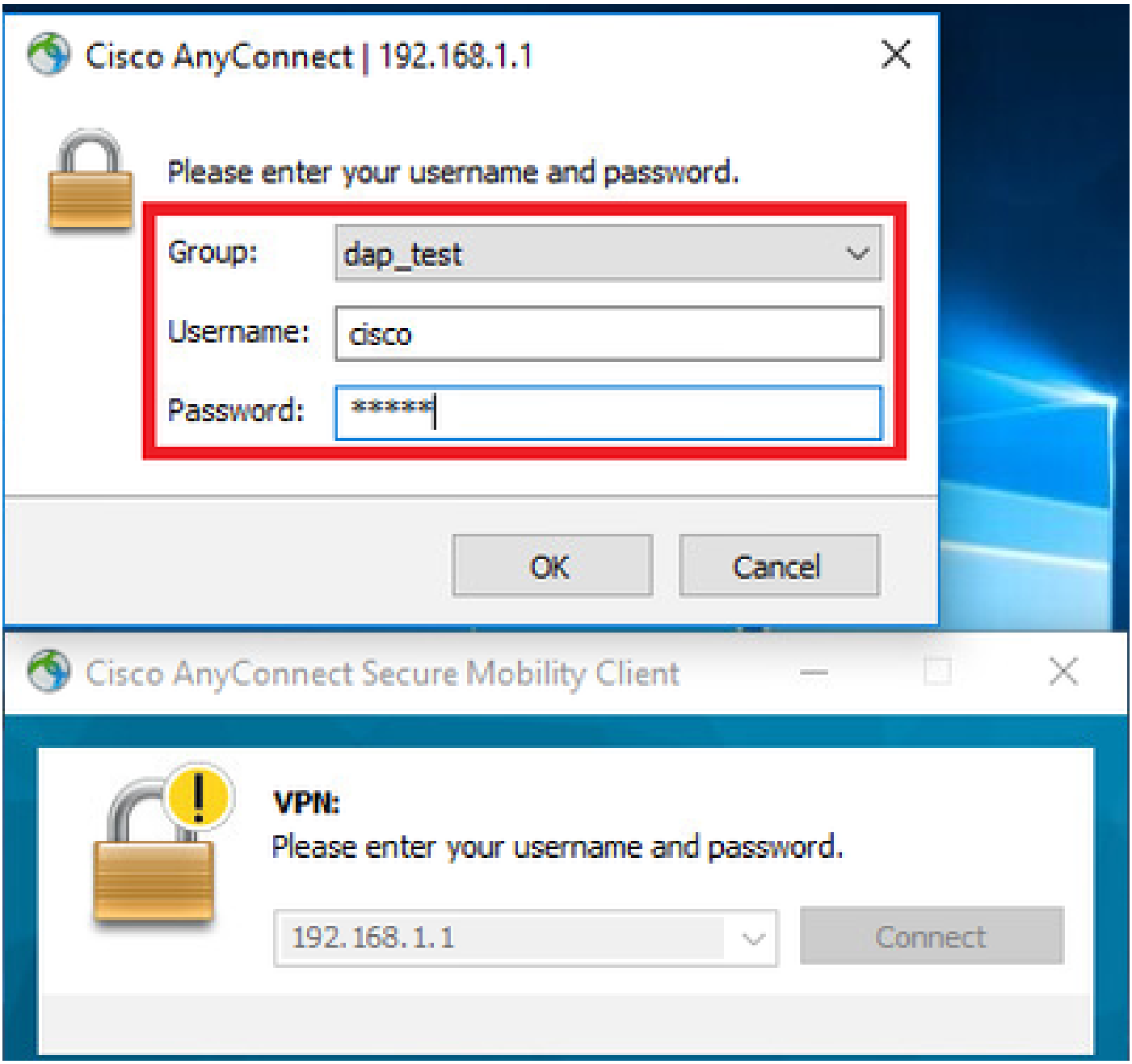
</name> <--- 3rd DAP MAC Address condition <value>true</value> <type>caseless</type> <operation>EQ</ope

التحقق من الصحة

السيناريو 1. تم مطابقة DAP واحد فقط

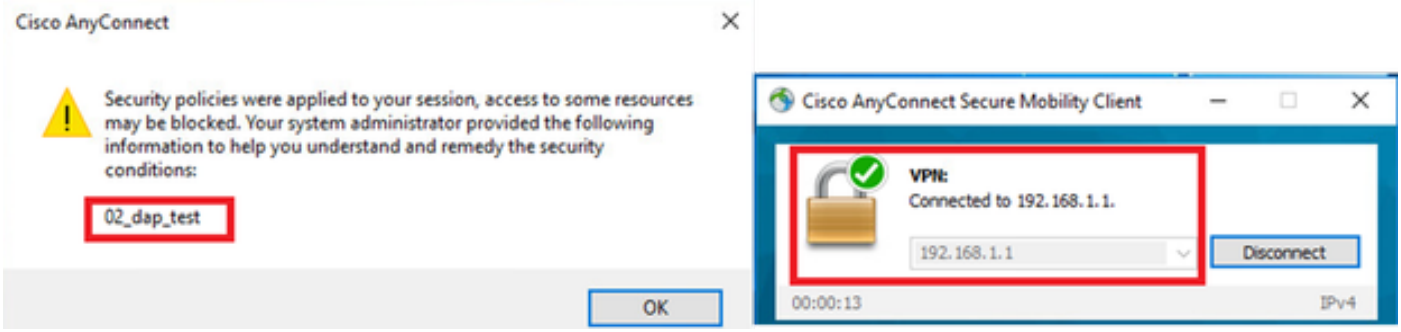
1. تأكد من أن MAC الخاص بنقطة النهاية 0050.5698.e605 وهو طرش قباطي MAC في 02_dap_test.

2. على نقطة النهاية، قم بتشغيل اتصال AnyConnect واستخدم اسم المستخدم وكلمة المرور الداخل.



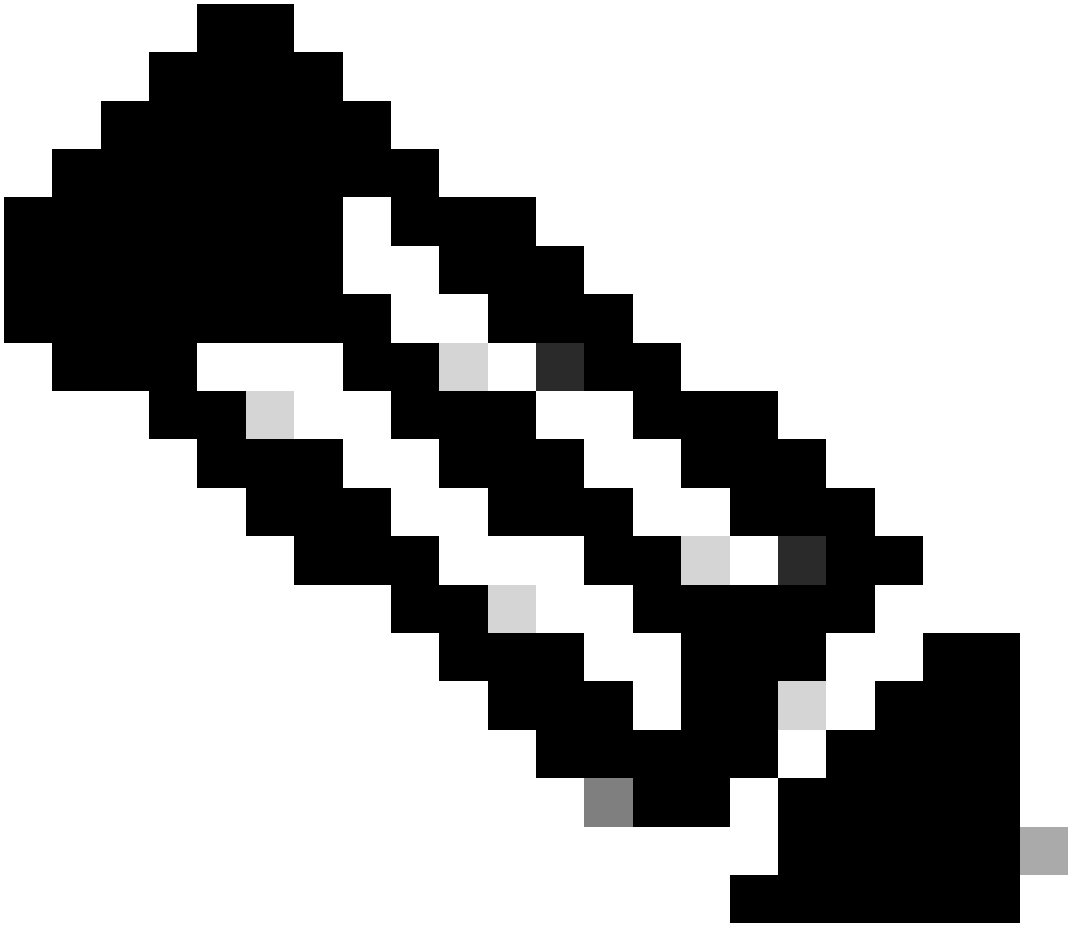
ادخال اسم المستخدم وكلمة المرور

3. في واجهة مستخدم AnyConnect، تأكد من مطابقة 02_dap_test.



تأكيد رسالة المستخدم في واجهة المستخدم

4. في ASA syslog، تأكد من تطابق 02_dap_test.



ةظحالم: تأكد من تمكين تتبع DAP لتتبع تصحيح الأخطاء في 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

: ,

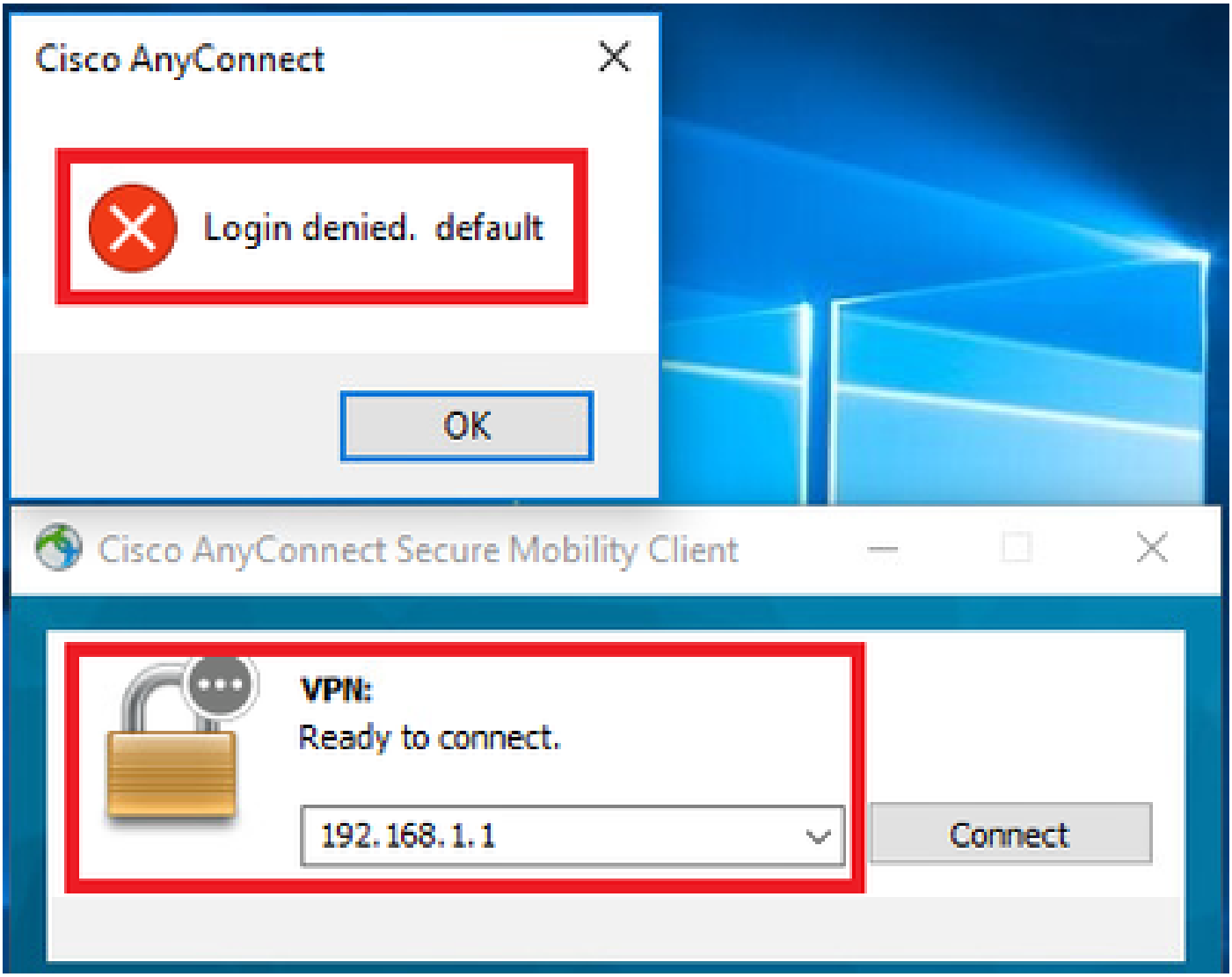
```
02_dap_test
 Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Dec 30 2023 11:46:11: %ASA-4-711001: dap_process_selec
selected 1 records
 Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 11:46:11: %ASA-4-711001:
```

السيناريو 2. DAP الافتراضي مطابق

1. قم بتغيير قيمة endpoint.device.mac في 02_dap_test إلى 0050.5698.e607 والتي تطابق MAC الخاص بنقطة النهاية.

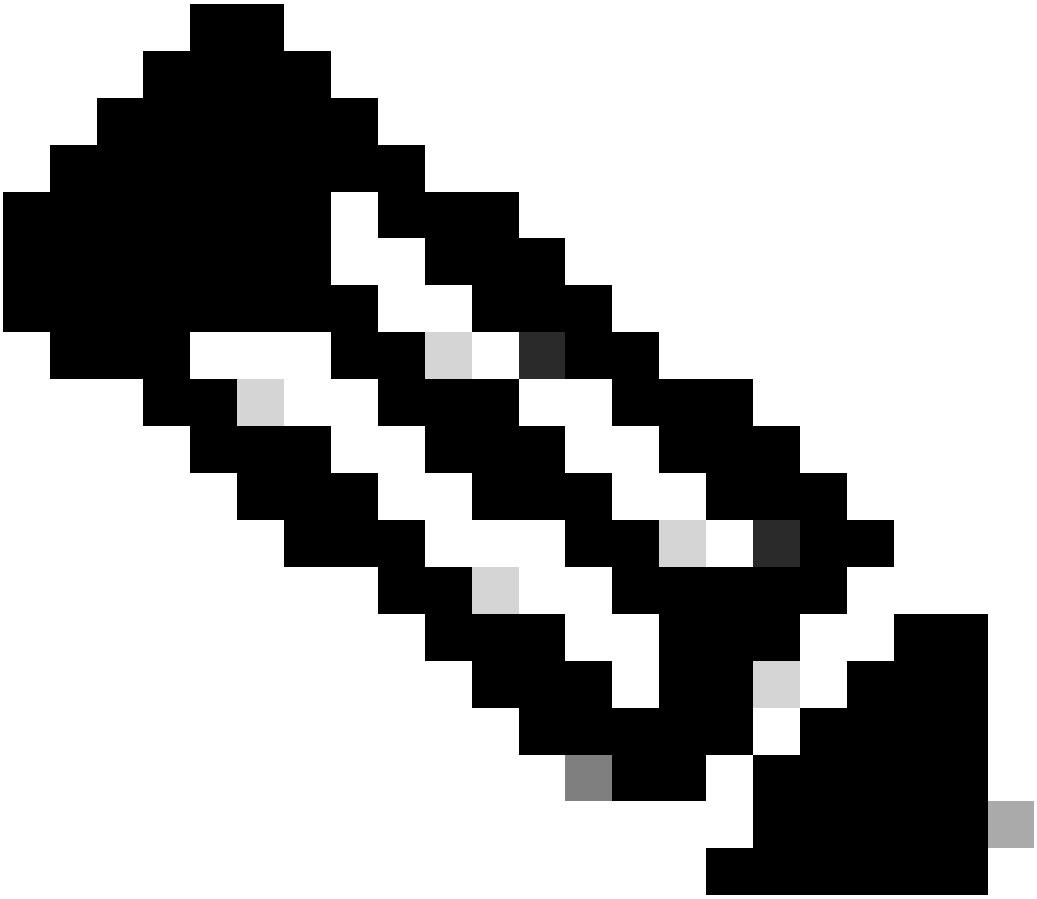
2. على نقطة النهاية، قم بتشغيل اتصال AnyConnect واسم مستخدم وكلمة مرور الإدخال.

3. تأكد من رفض اتصال AnyConnect.



تأكيد رسالة المستخدم في واجهة المستخدم

4. في ASA syslog، تأكد من تطابق DfltAccessPolicy.



ملاحظة: بشكل افتراضي، يتم إنهاء الإجراء DfltAccessPolicy.

<#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

السيناريو 3. DAPs متعددة (الإجراء: إستمرار) متطابقة

1. تغيير الإجراء والسمة في كل DAP.

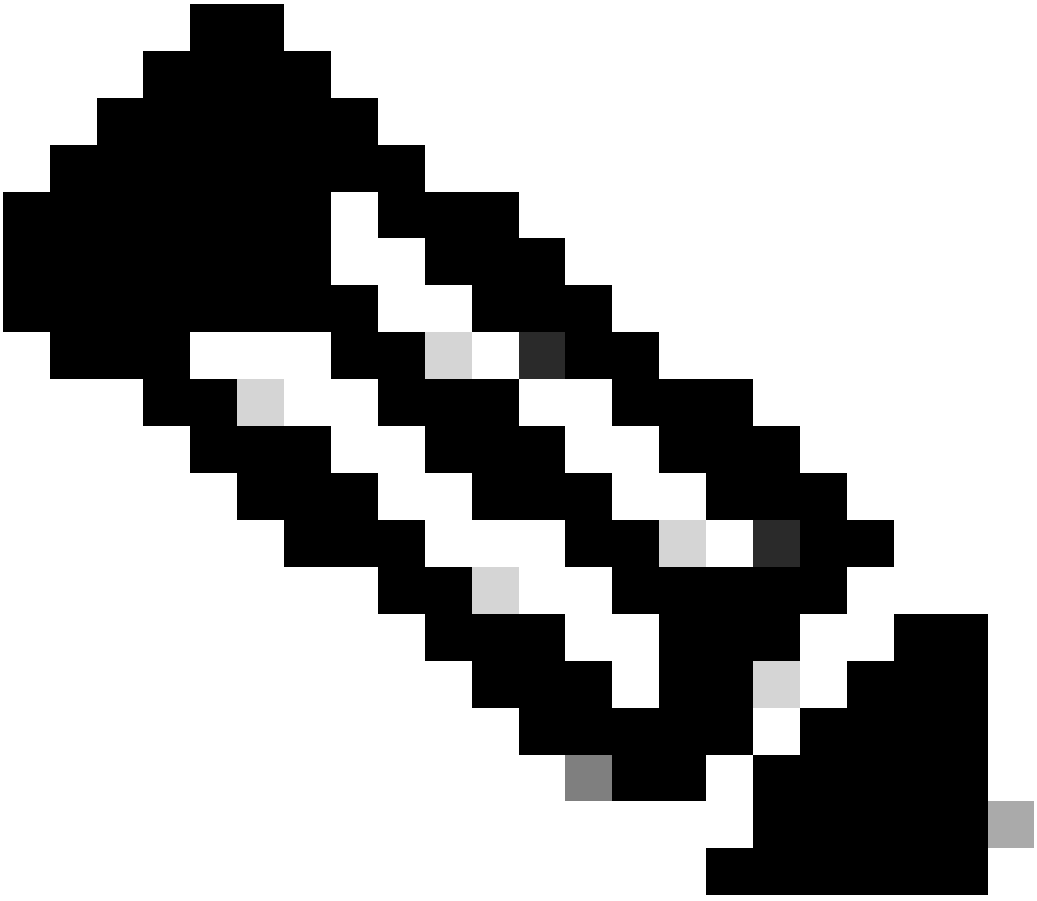
·01_dap_test :
dapSelection (عنوان MAC) = endpoint.device.mac[0050.5698.e605] = MAC من AnyConnect Endpoint
الإجراء = متابعة
·02_dap_test :

dapSelection (اسم المضيف) = endpoint.device.hostname[desktop-vckhrg1] = اسم المضيف لنقطة نهاية AnyConnect
متابعة = الإجراء

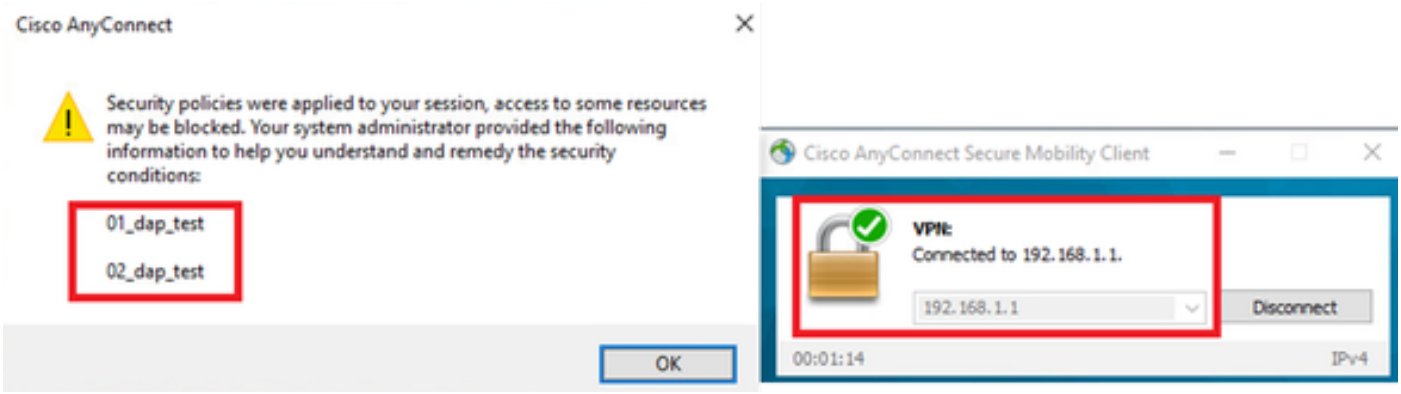
حذف سجل DAP الخاص بـ 03_dap_test.

2. على نقطة النهاية، قم بتشغيل اتصال AnyConnect واسم مستخدم وكلمة مرور الإدخال.

3. في واجهة مستخدم AnyConnect، تأكد من تطابق كافة بروتوكولات DAP الـ 2



ملاحظة: في حالة تطابق اتصال مع العديد من بروتوكولات DAP، يتم دمج رسائل المستخدم الخاصة ببروتوكولات DAP المتعددة وعرضها معا في واجهة مستخدم AnyConnect.



تأكيد رسالة المستخدم في واجهة المستخدم

4. في ASA syslog، تأكد من أن كل 2 DAPs متطابقة.

<#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: DA

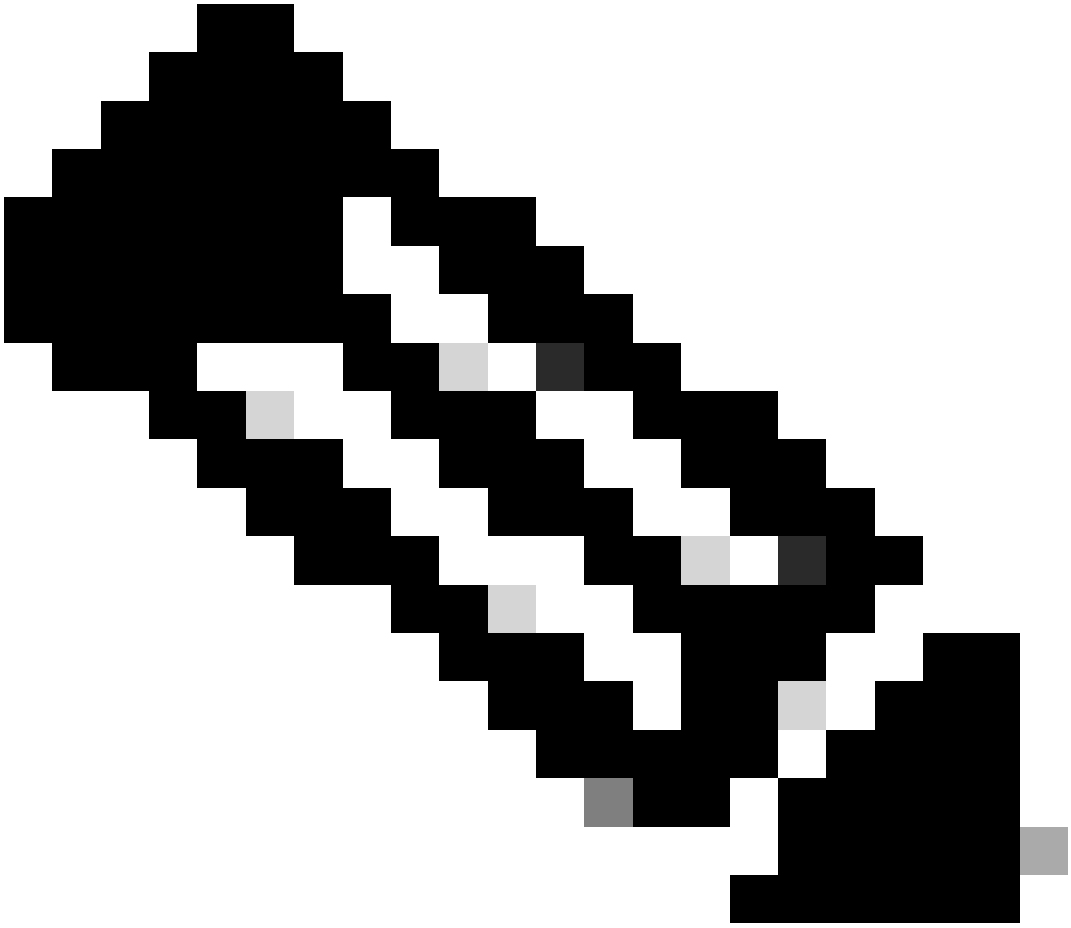
السيناريو 4. DAPs متعددة (إجراء: إنهاء) متطابقة

1. قم بتغيير الإجراء 01_dap_test.

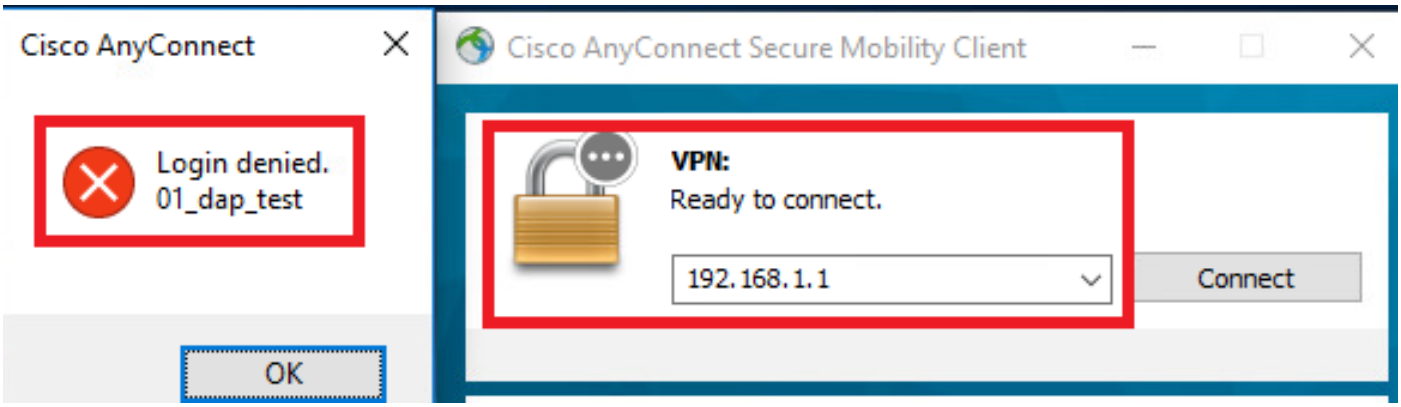
·01_dap_test :
dapSelection (عنوان MAC) = endpoint.device.mac[0050.5698.e605] = MAC من AnyConnect Endpoint
الإجراء = إنهاء
·02_dap_test :
dapSelection (اسم المضيف) = endpoint.device.hostname[desktop-vckhrg1] = اسم المضيف لنقطة نهاية AnyConnect
الإجراء = متابعة

2. على نقطة النهاية، قم بتشغيل اتصال AnyConnect واسم مستخدم وكلمة مرور الإدخال.

3. في واجهة مستخدم AnyConnect، تأكد من تطابق **01_dap_test** فقط.



ملاحظة: اتصال مطابق لسجل DAP الذي تم تعيينه لإنهاء الإجراء. لم تعد السجلات التالية متطابقة بعد إجراء الإنهاء.



تأكيد رسالة المستخدم في واجهة المستخدم

4. في ASA syslog، تأكد من مطابقة 01_dap_test فقط.

<#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:

أستكشاف الأخطاء وإصلاحها بشكل عام

تساعدك سجلات تصحيح الأخطاء هذه على تأكيد سلوك تفاصيل DAP في 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

معلومات ذات صلة

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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).