Déployer ASA DAP pour identifier l'adresse MAC pour AnyConnect

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Diagramme du réseau
  - Configuration dans ASA
  - Configuration dans ASDM
- Vérifier
  - Scénario1. Un seul DAP correspond
  - Scénario 2. Le DAP par défaut correspond
  - Scénario 3. Plusieurs DAP (Action : Continuer) correspondent à
  - Scénario4. Plusieurs DAP (Action : Terminate) sont mis en correspondance
- Dépannage général
- Informations connexes

Introduction

Ce document décrit comment configurer des politiques d'accès dynamique (DAP) via ASDM, pour vérifier l'adresse Mac du périphérique utilisé pour la connexion AnyConnect.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :
Configuration de Cisco Anyconnect et Hostscan

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :
ASAv 9.18 (4)
ASDM 7.20 (1)
Anyconnect 4.10.07073
Hostscan 4.10.07073

Windows 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

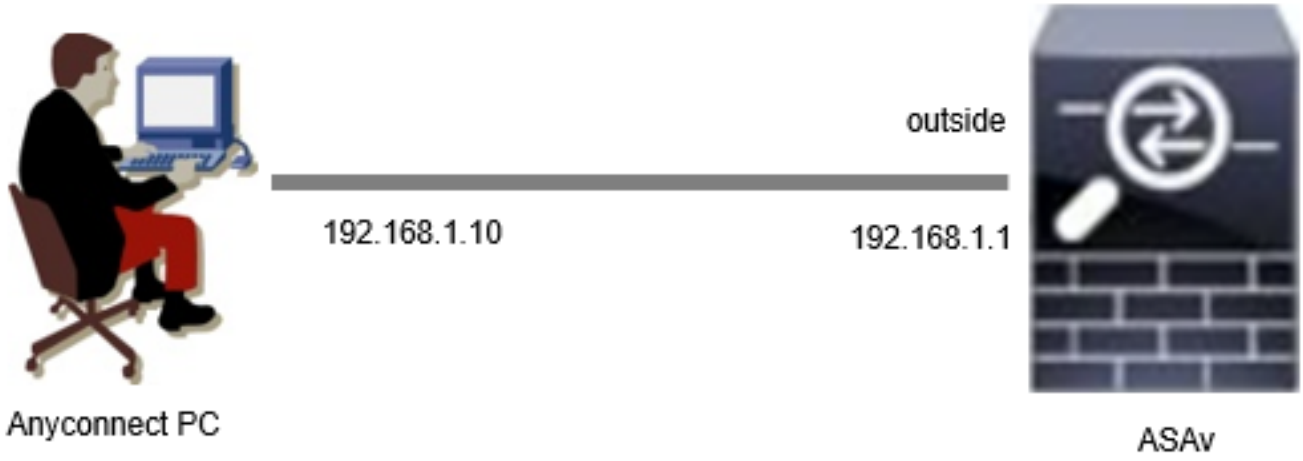
Informations générales

HostScan est un module logiciel qui permet au client AnyConnect Secure Mobility d’appliquer des stratégies de sécurité sur le réseau. Au cours du processus de Hostscan, divers détails sur le périphérique client sont rassemblés et signalés à l'appliance de sécurité adaptative (ASA). Ces détails incluent le système d'exploitation du périphérique, le logiciel antivirus, le logiciel de pare-feu, l'adresse MAC, etc. La fonctionnalité Dynamic Access Policies (DAP) permet aux administrateurs réseau de configurer des stratégies de sécurité par utilisateur. L'attribut endpoint.device.MAC de DAP peut être utilisé pour comparer ou vérifier l'adresse MAC du périphérique client par rapport à des stratégies prédéfinies.

Configurer

Diagramme du réseau

Cette image présente la topologie utilisée pour l'exemple de ce document.



Diagramme

Configuration dans ASA

Il s'agit de la configuration minimale de l'interface CLI 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
```

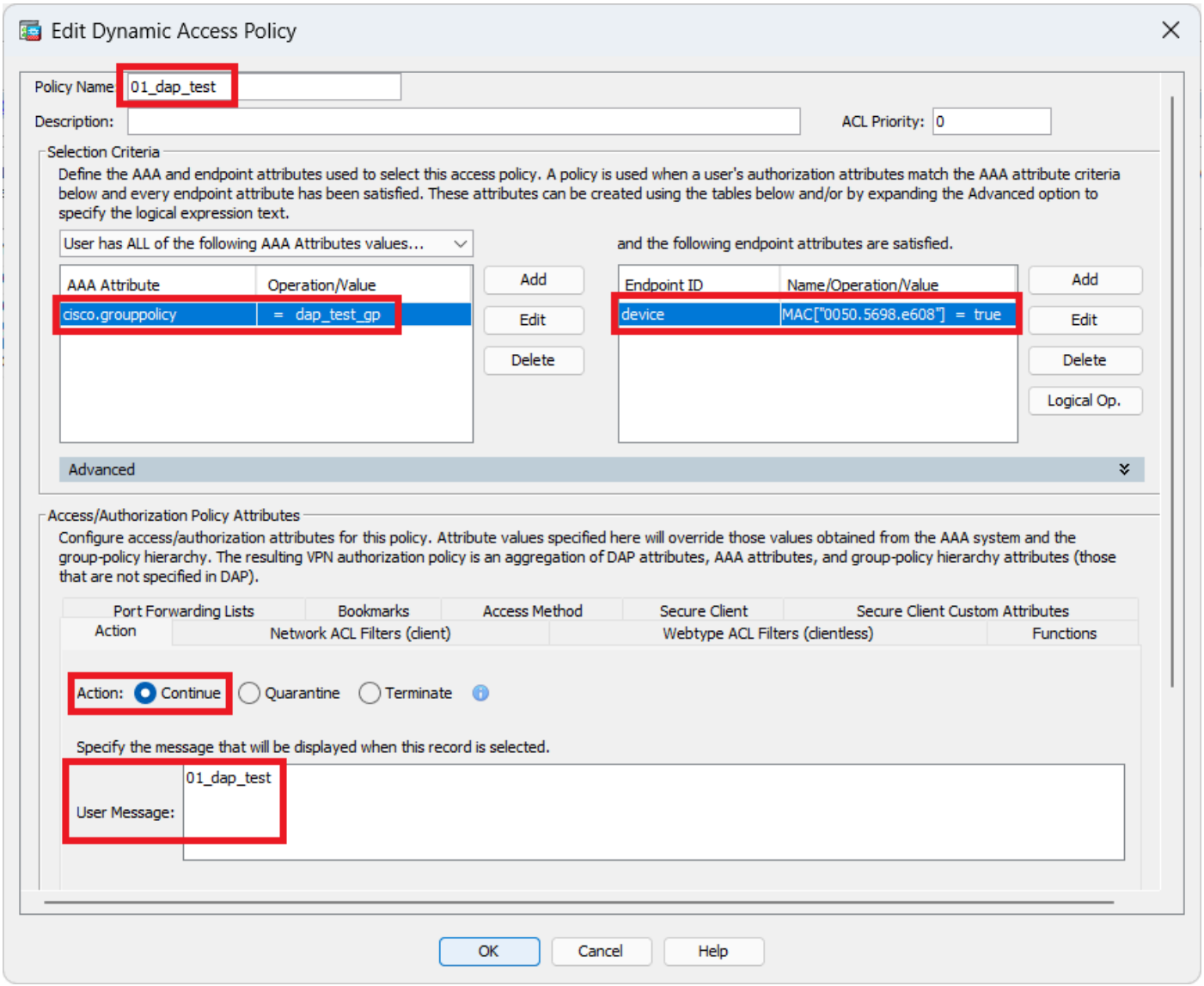
Configuration dans ASDM

Cette section décrit comment configurer l'enregistrement LDAP dans ASDM. Dans cet exemple, définissez 3 enregistrements DAP qui utilisent l'attribut endpoint.device.MAC comme condition.

·01_dap_test:endpoint.device.MAC=0050.5698.e608
·02_dap_test:endpoint.device.MAC=0050.5698.e605 = MAC du point de terminaison Anyconnect
·03_dap_test:endpoint.device.MAC=0050.5698.e609

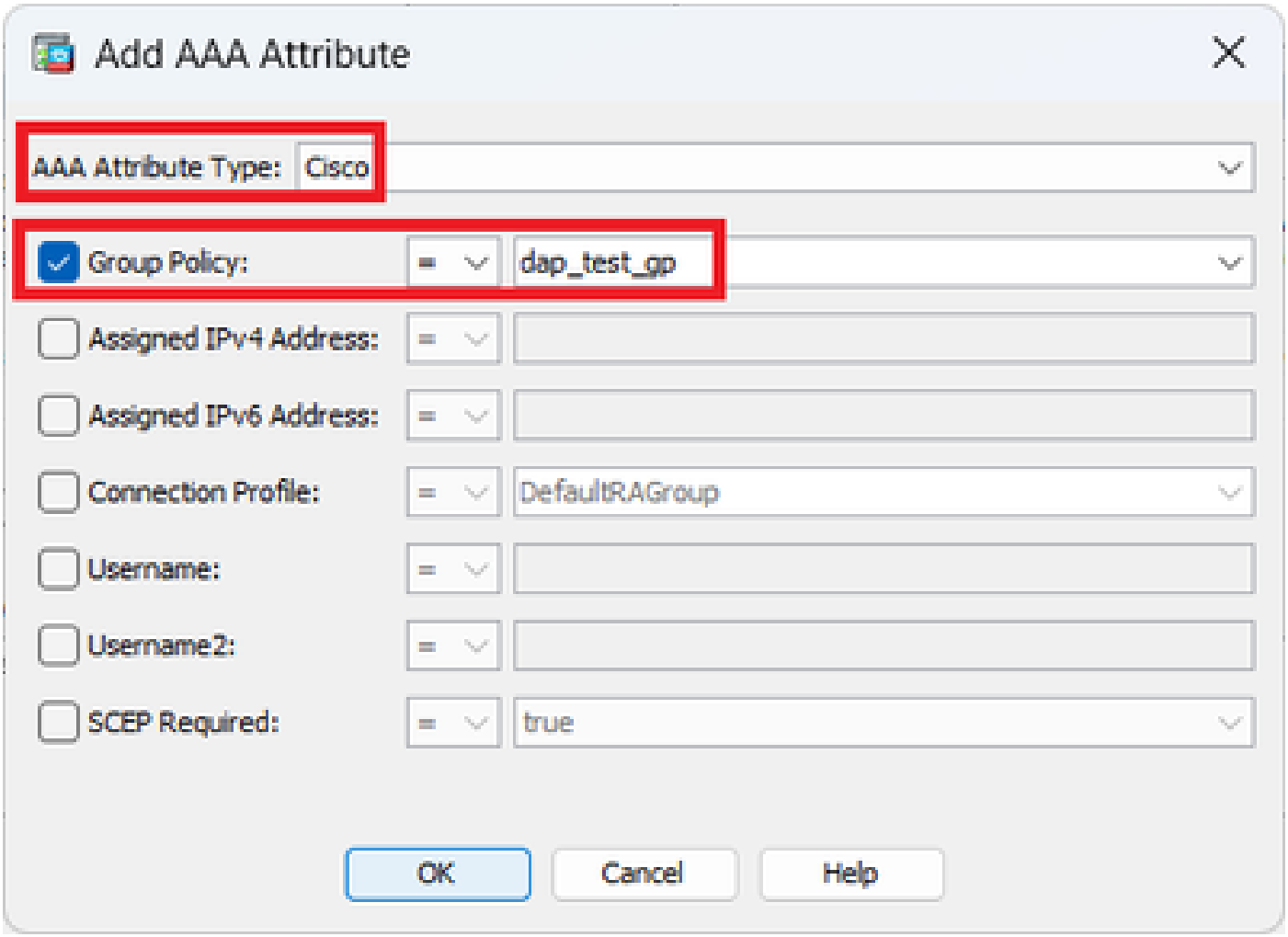
1. Configurez le premier DAP nommé 01_dap_test.

Accédez à Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies. Cliquez sur Ajouter et définissez le nom de la stratégie, l'attribut AAA, les attributs de point de terminaison, l'action, le message utilisateur, comme illustré dans l'image :



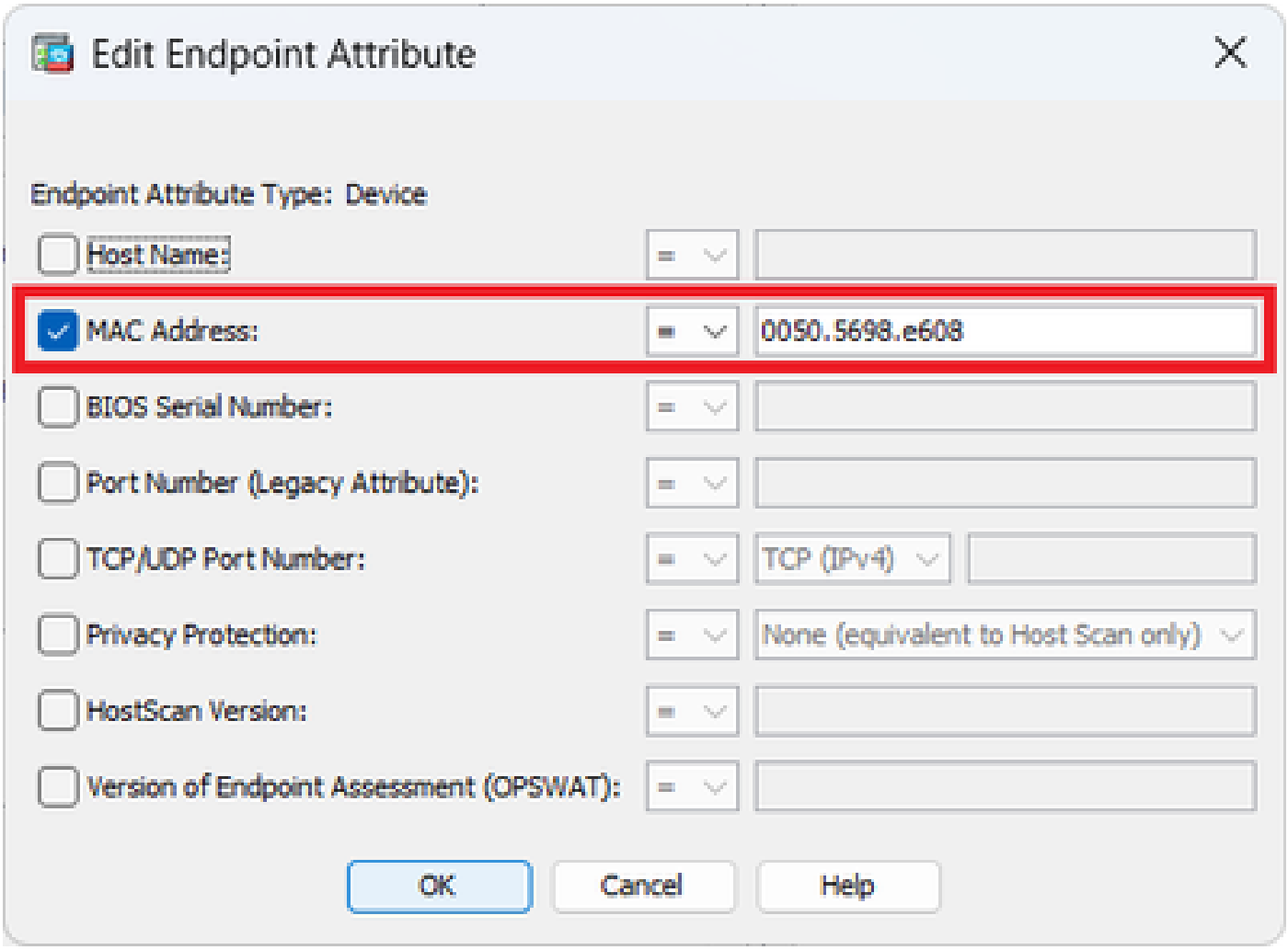
Configuration du premier DAP

Configurez la stratégie de groupe pour l'attribut AAA.



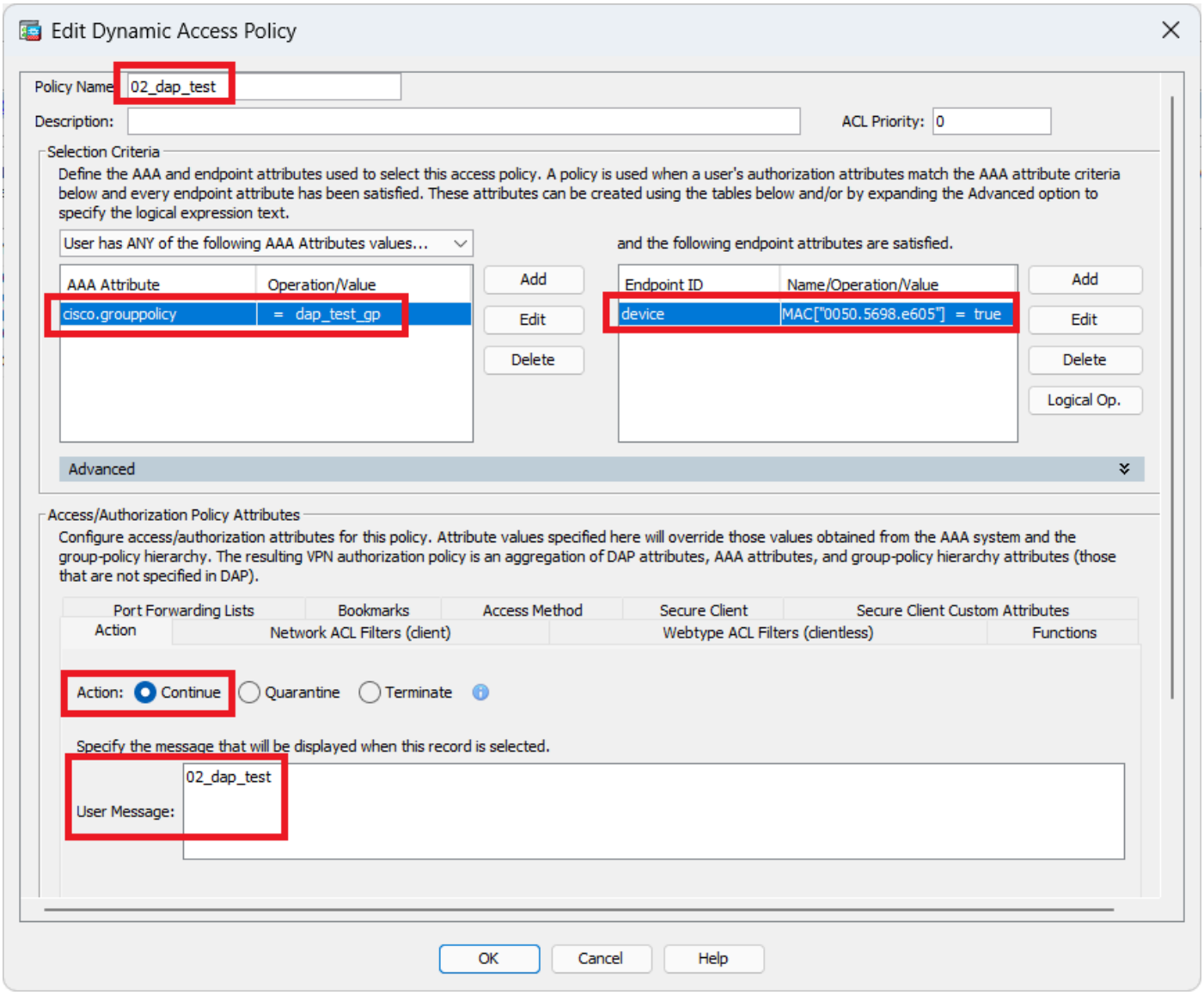
Configurer La Stratégie De Groupe Pour L'Enregistrement LDAP

Configurez l'adresse MAC pour l'attribut Endpoint.



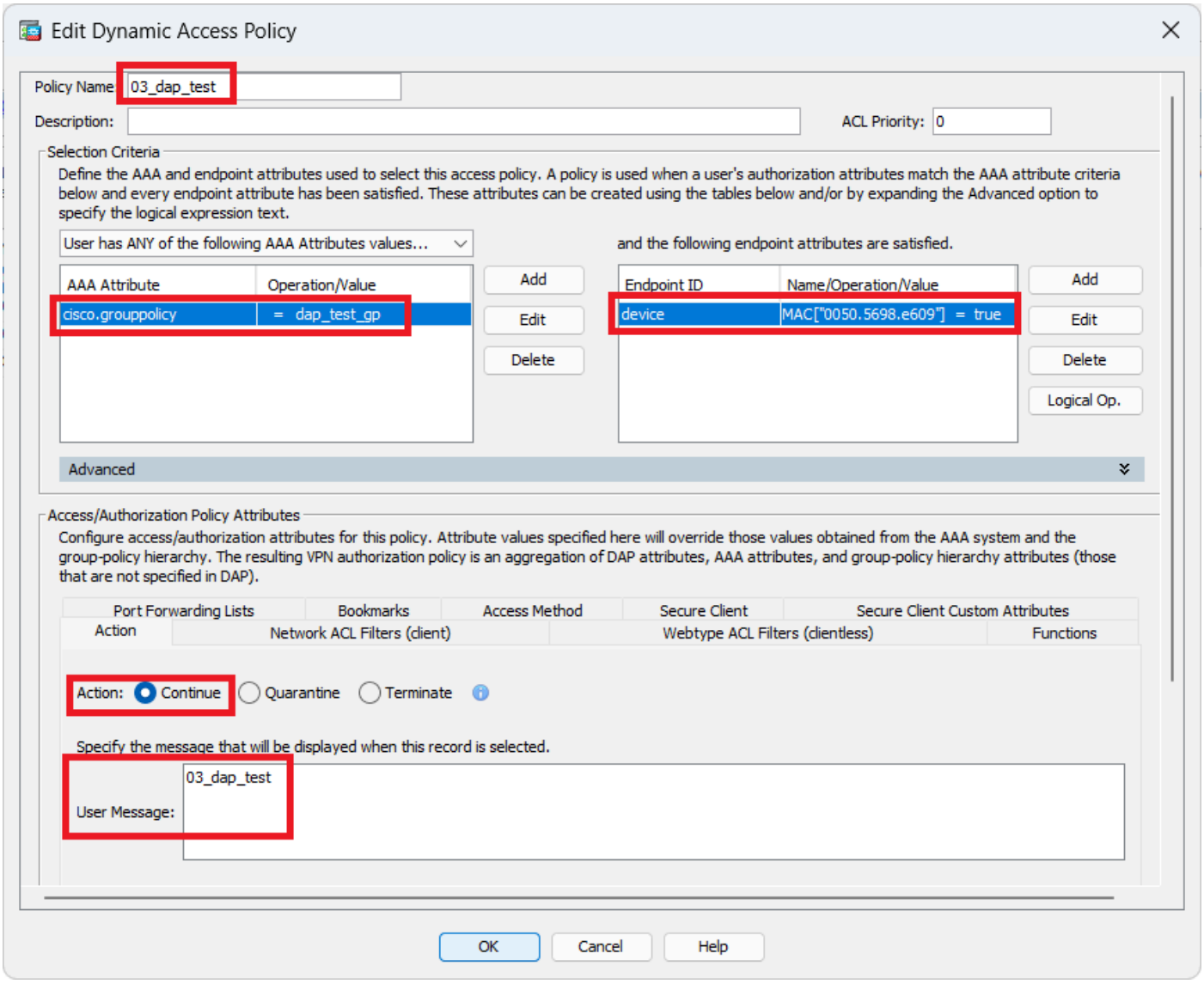
Configuration de la condition MAC pour DAP

2. Configurez le deuxième DAP nommé 02_dap_test.



Configurer le deuxième DAP

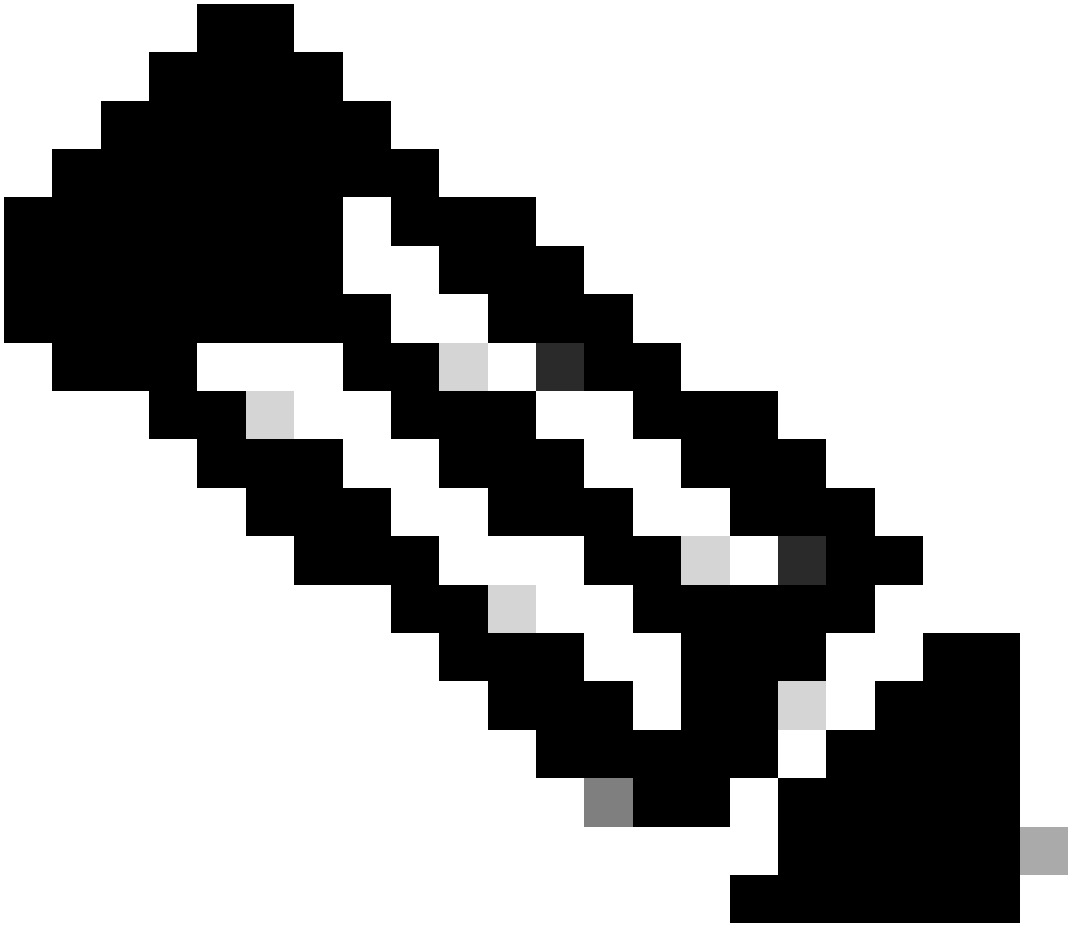
3. Configurez le troisième DAP nommé 03_dap_test.



Configuration du troisième DAP

4. Utilisez cette **more flash:/dap.xml** commande pour confirmer le paramétrage des enregistrements DAP dans dap.xml.

Les détails des enregistrements DAP définis sur ASDM sont enregistrés dans la mémoire flash ASA sous le nom dap.xml. Une fois ces paramètres définis, trois enregistrements DAP sont générés dans dap.xml. Vous pouvez confirmer les détails de chaque enregistrement DAP dans dap.xml.



Remarque : L'ordre dans lequel le DAP est mis en correspondance est l'ordre d'affichage dans dap.xml. Le DAP par défaut (DfltAccessPolicy) est mis en correspondance en dernier.

<#root>

ciscoasa#

more flash:/dap.xml

01_dap_test

<--- 1st DAP name

and

match-all

aaa.cisco.grouppolicy

dap_test_gp

<--- 1st DAP group policy

EQ

caseless

match-any

match-all

endpoint.device.MAC["0050.5698.e608"]

<--- 1st DAP MAC Address condition

true

caseless

EQ

02_dap_test

<--- 2nd DAP name

and

match-any

aaa.cisco.grouppolicy

dap_test_gp

<--- 2nd DAP group policy

EQ

caseless

match-any

match-all

endpoint.device.MAC["0050.5698.e605"]

<--- 2nd DAP MAC Address condition

true

caseless

EQ

03_dap_test

<--- 3rd DAP name

and

match-any

aaa.cisco.grouppolicy

dap_test_gp

<--- 3rd DAP group policy

EQ

caseless

match-any

match-all

endpoint.device.MAC["0050.5698.e609"]

<--- 3rd DAP MAC Address condition

true

caseless

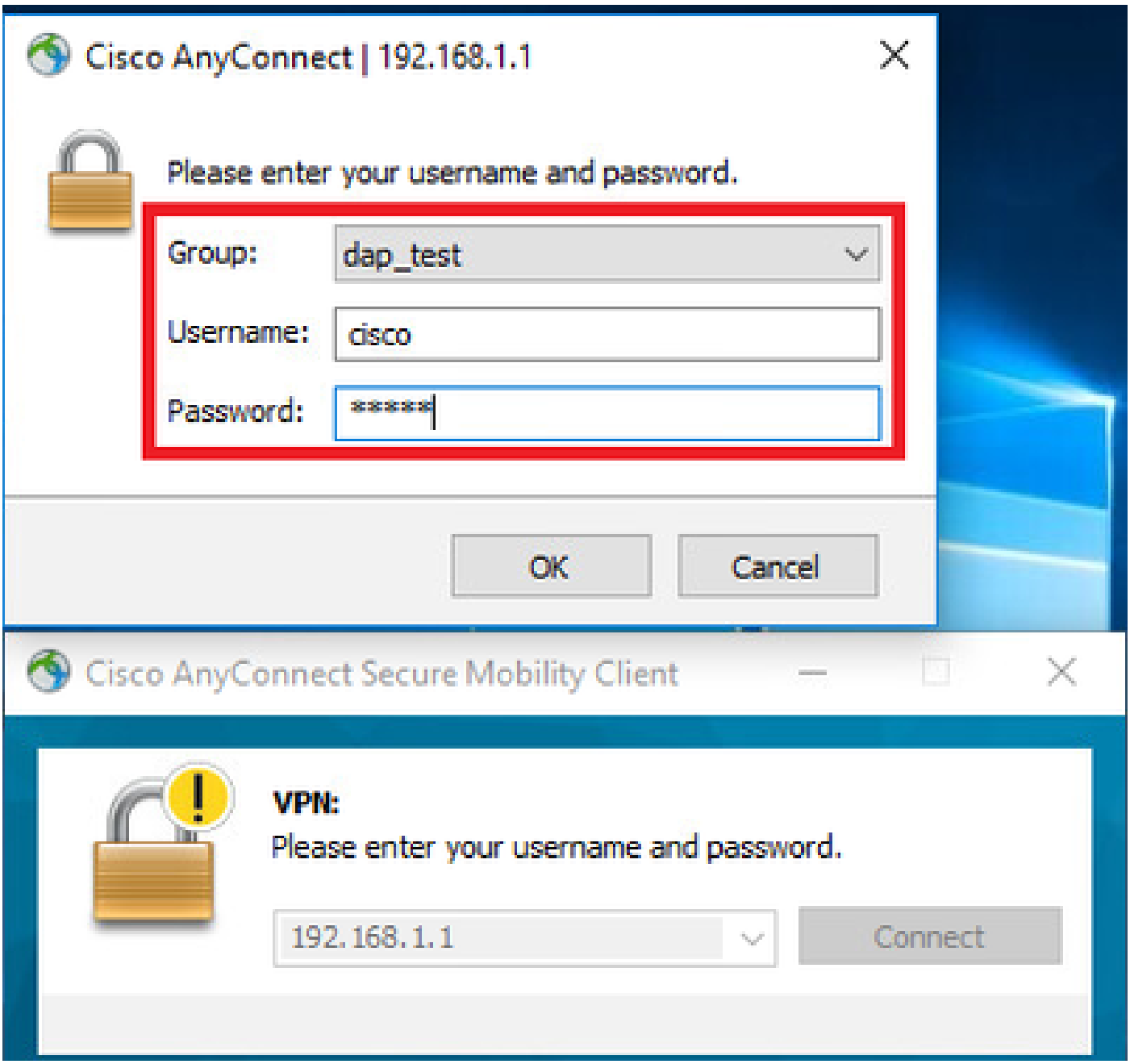
EQ

Vérifier

Scénario1. Un seul DAP correspond

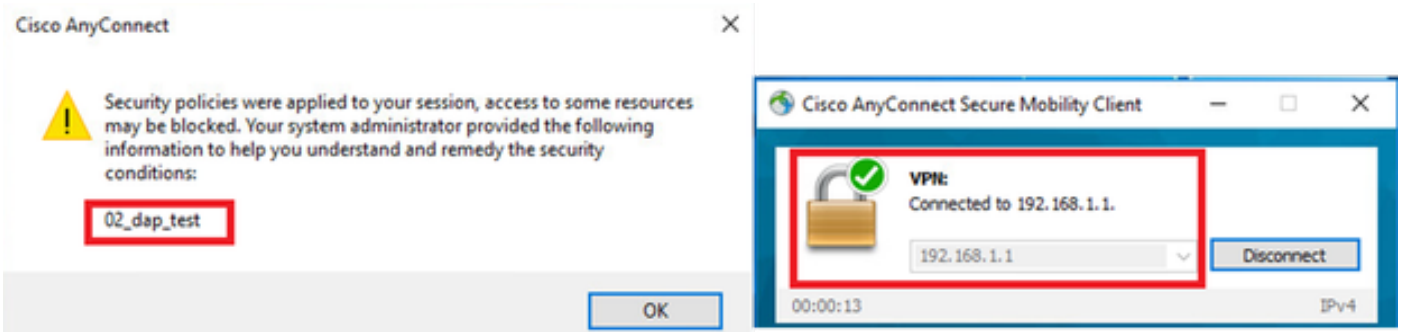
1. Assurez-vous que l'adresse MAC du point de terminaison est 0050.5698.e605, ce qui correspond à la condition MAC dans 02_dap_test.

2. Sur le terminal, exécutez Anyconnect connection et entrez le nom d'utilisateur et le mot de passe.



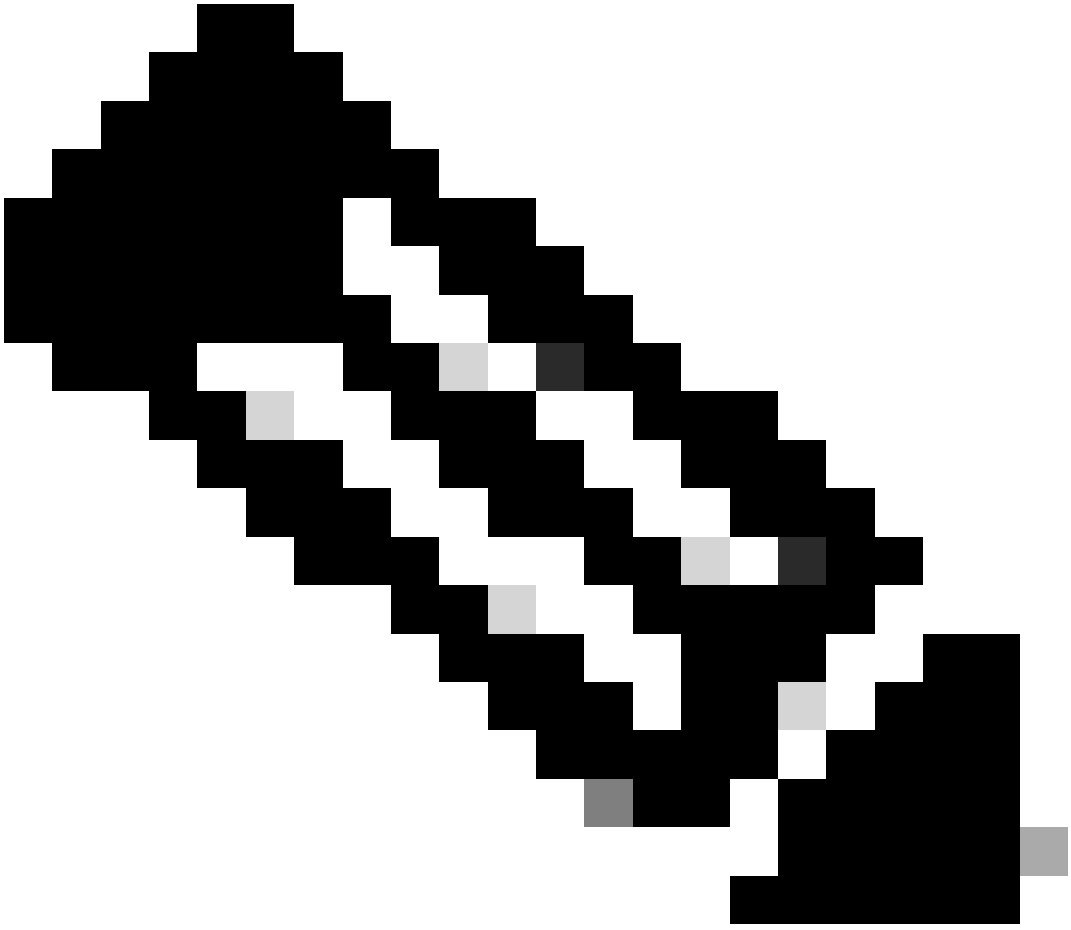
Entrez le nom d'utilisateur et le mot de passe

3. Dans l'interface utilisateur Anyconnect, vérifiez que 02_dap_test correspond.



Confirmer le message utilisateur dans l'interface utilisateur

4. Dans le syslog ASA, vérifiez que 02_dap_test correspond.



Remarque : Assurez-vous que debug dap trace est activé dans 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

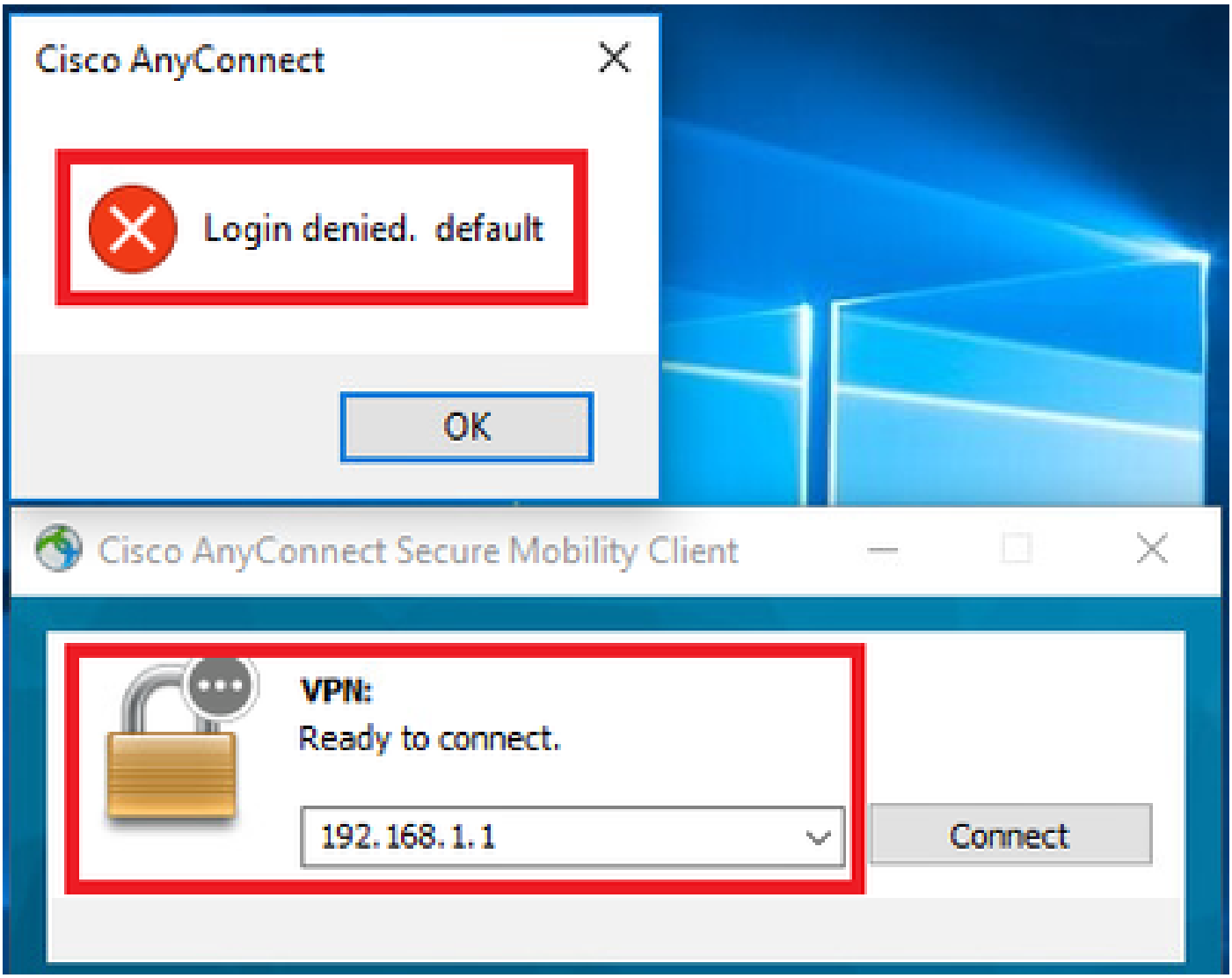
Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 11:46:11: %ASA-4-711001: DA

Scénario 2. Le DAP par défaut correspond

1. Modifiez la valeur de endpoint.device.MAC dans 02_dap_test en 0050.5698.e607, qui ne correspond pas à l'adresse MAC du point de terminaison.

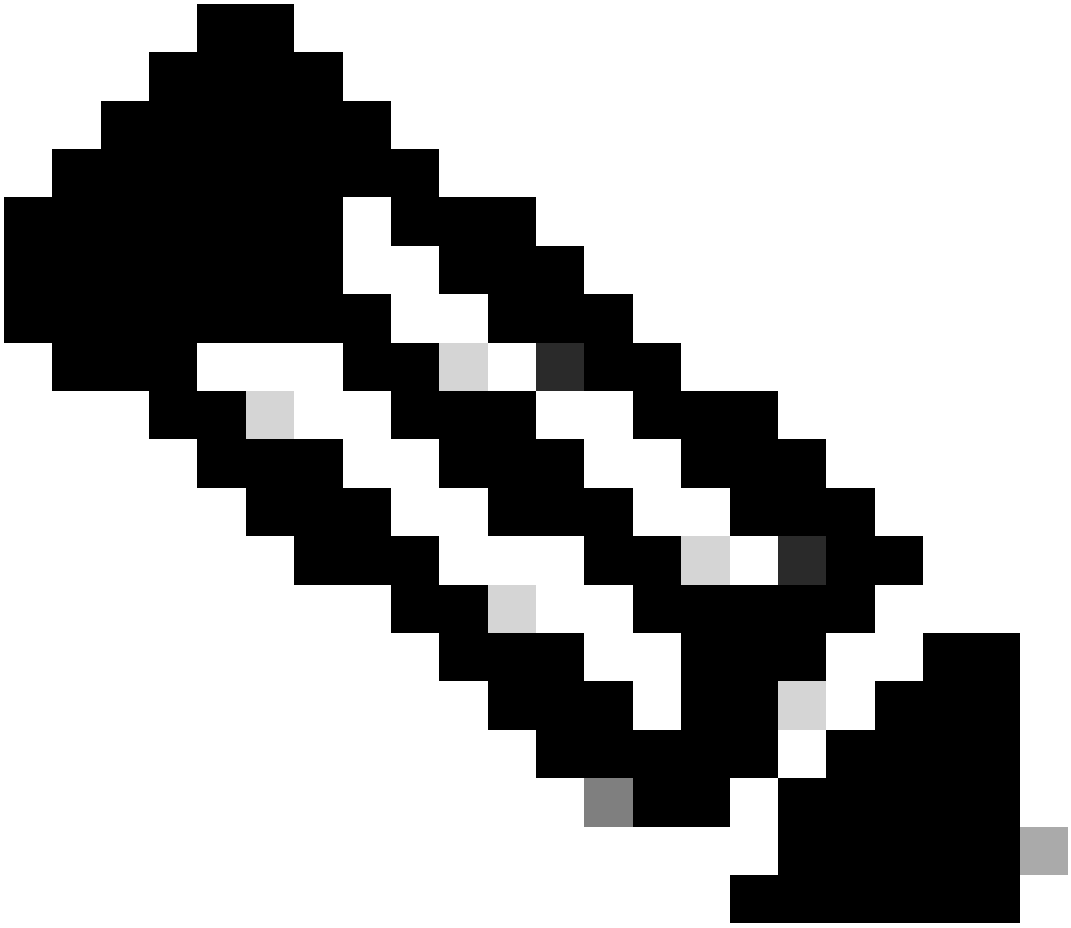
2. Sur le terminal, exécutez Anyconnect connection et entrez le nom d'utilisateur et le mot de passe.

3. Vérifiez que la connexion Anyconnect a été refusée.



Confirmer le message utilisateur dans l'interface utilisateur

4. Dans le syslog ASA, vérifiez que DfltAccessPolicy correspond.



Remarque : Par défaut , l'action de DfltAccessPolicy est 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_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

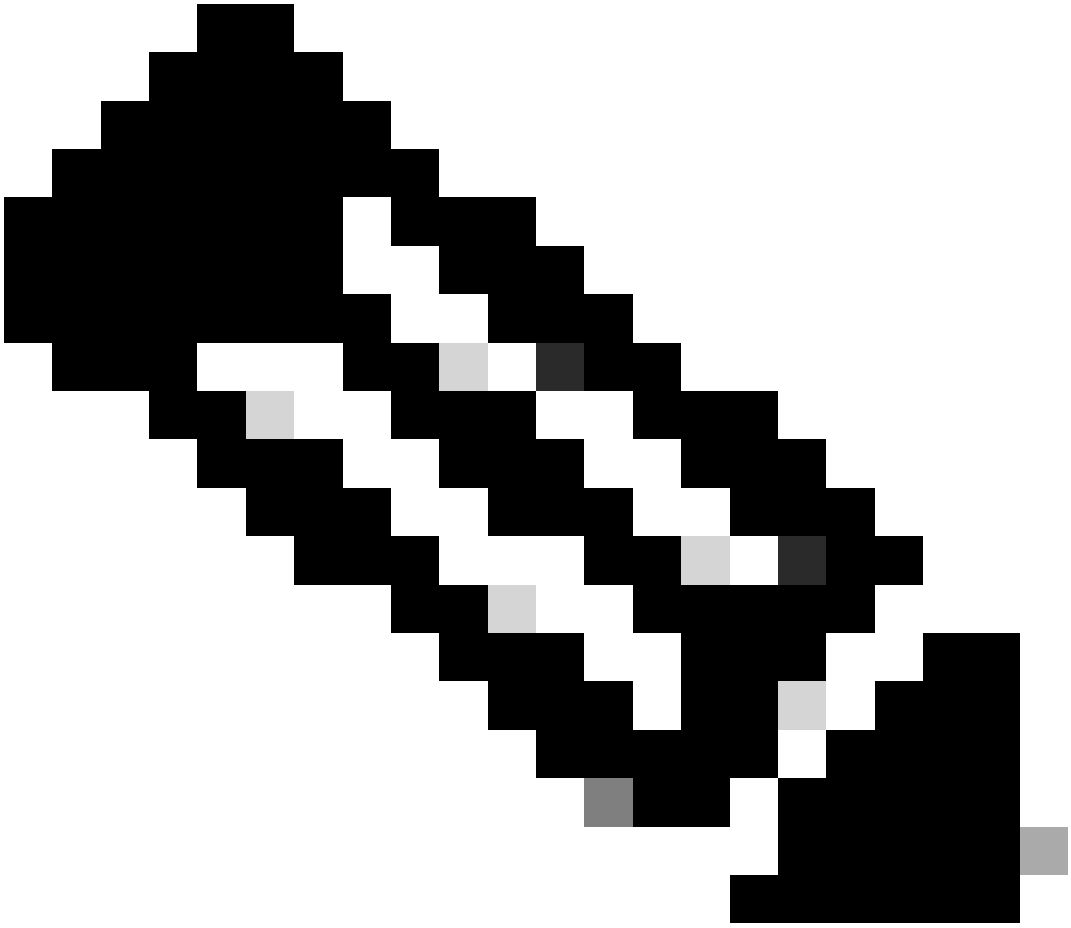
Scénario 3. Plusieurs DAP (Action : Continuer) correspondent à

1. Modifiez l'action et l'attribut dans chaque DAP.

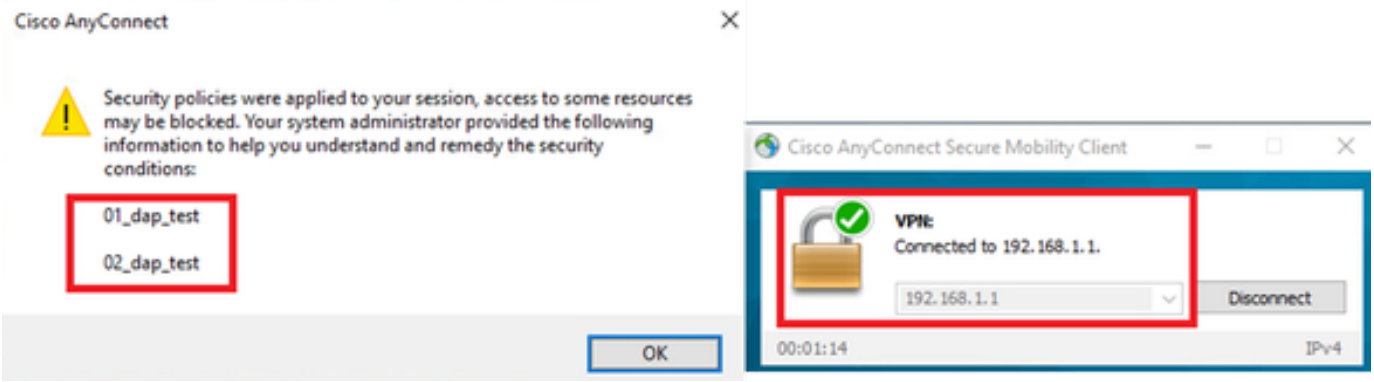
·01_dap_test :
dapSelection (adresse MAC) = endpoint.device.MAC[0050.5698.e605] = MAC du terminal Anyconnect
Action = Continuer
·02_dap_test :
dapSelection (Nom d'hôte) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Nom d'hôte du point de terminaison Anyconnect
Action = Continuer
·Supprimer l'enregistrement 03_dap_test LDAP

2. Sur le terminal, exécutez Anyconnect connection et entrez le nom d'utilisateur et le mot de passe.

3. Dans l’interface utilisateur Anyconnect, vérifiez que les 2 DAP correspondent



Remarque : Si une connexion correspond à plusieurs DAP, les messages utilisateur de plusieurs DAP sont intégrés et affichés ensemble dans l'interface utilisateur Anyconnect.



Confirmer le message utilisateur dans l'interface utilisateur

4. Dans le syslog ASA, vérifiez que les 2 DAP correspondent.

<#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_selecte

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

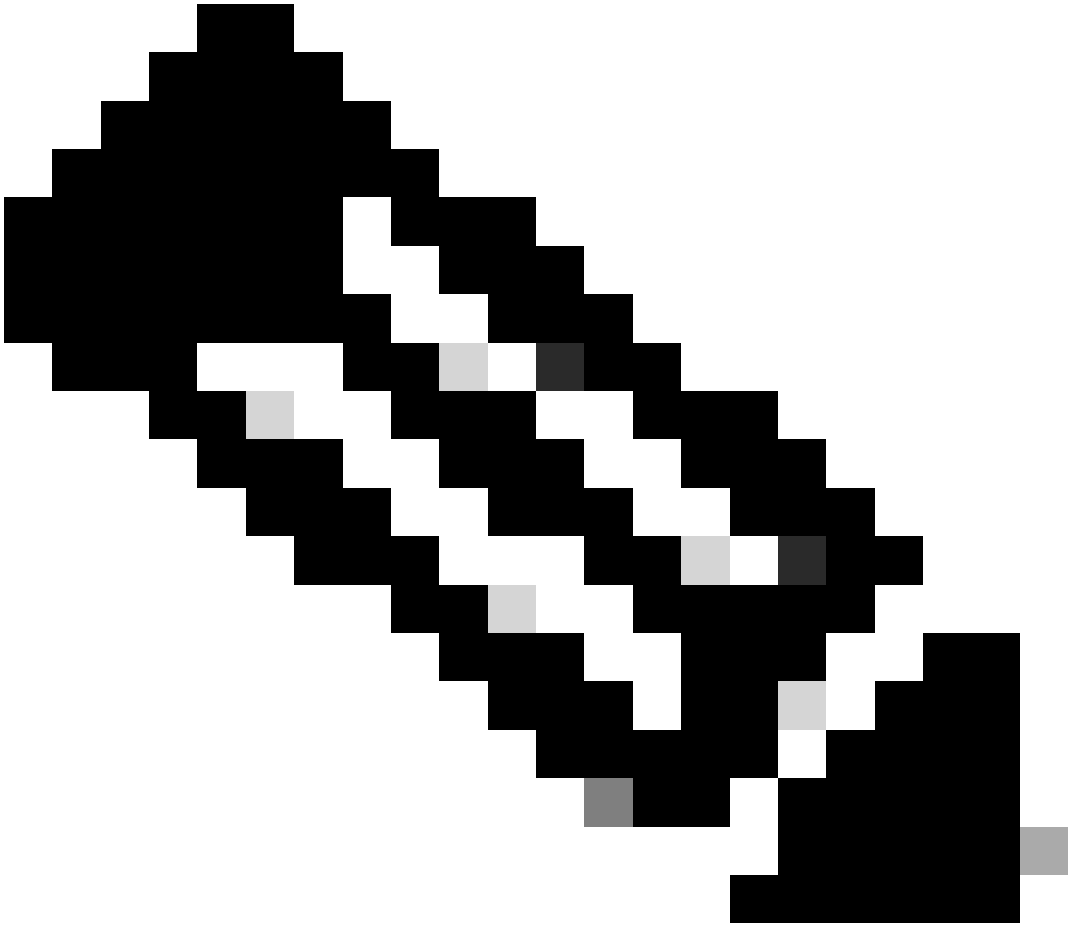
Scénario4. Plusieurs DAP (Action : Terminate) sont mis en correspondance

1. Modifiez l'action de 01_dap_test.

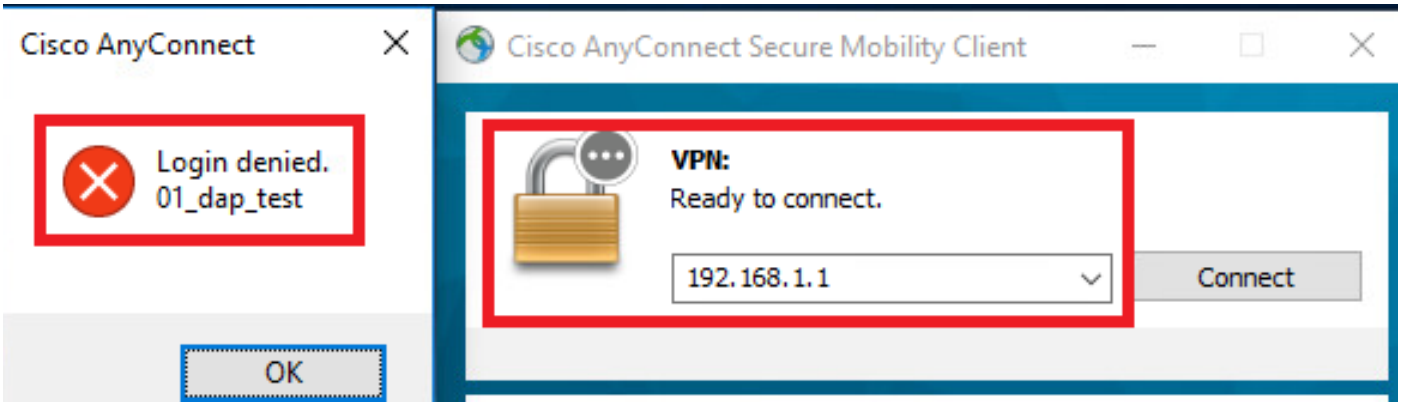
·01_dap_test :
dapSelection (adresse MAC) = endpoint.device.MAC[0050.5698.e605] = MAC du terminal Anyconnect
Action = Terminer
·02_dap_test :
dapSelection (Nom d'hôte) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Nom d'hôte du point de terminaison Anyconnect
Action = Continuer

2. Sur le terminal, exécutez Anyconnect connection et entrez le nom d'utilisateur et le mot de passe.

3. Dans l'interface utilisateur Anyconnect, vérifiez que seul 01_dap_test correspond.



Remarque : Une connexion est mise en correspondance avec l'enregistrement DAP qui a été défini pour mettre fin à l'action. Les enregistrements suivants ne sont plus mis en correspondance après l'action de fin.



Confirmer le message utilisateur dans l'interface utilisateur

4. Dans le syslog ASA, vérifiez que seul 01_dap_test correspond.

<#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: S

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_selecte

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: DA

Dépannage général

Ces journaux de débogage vous aident à confirmer le comportement détaillé de DAP dans 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 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:49:02: %ASA-4-711001: endpoint.device.hostname = "DESKTOP-VCKHRG1"

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Username: cisco, Feb 01 2024 08:49:02: %ASA-4-711001:

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-4-711001: dap_process_selecte

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Username: cisco, Feb 01 2024 08:49:02: %ASA-4-711001: DA

Informations connexes

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.