Configure DAP Policies on Secure Firewall

Contents

Introduction

This document describes how to perform and configure Dynamic Access Policies on an Secure Firewall device based on the RAVPN client.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Register the Secure Firewall with FMC and have them synchronized and up to date with latest version of the configuration file.
- Preconfigure Remote Access Virtual Private Network (RAVPN) policy on the Secure Firewall registered.
- Download Hostscan package (.pkg) with its equivalent version of Anyconnect Security Mobility Client.

- Basic konwledge on RAVPN solutions.
- General concepts on DAP feature.
- Secure Firewall Management Center administration and configuration knowledge.

Components Used

The information in this document is based on these software and hardware versions:

- FMC 7.0.0 version or later
- Secure Firewall 7.0.0 version or later
- MAC/Windows machine with Cisco Secure Client Anyconnect software 4.10 or later
- Hostscan package 4.10 or later
- Active Directory for AAA authentication.

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This documents describes a step by step guide on how to perform and configure Dynamic Access Policies on an Secure Firewall device based on RAVPN client machine attributes. HostScan is used to gather client information and DAP applies different policies to Mac OS and Windows users respectively.

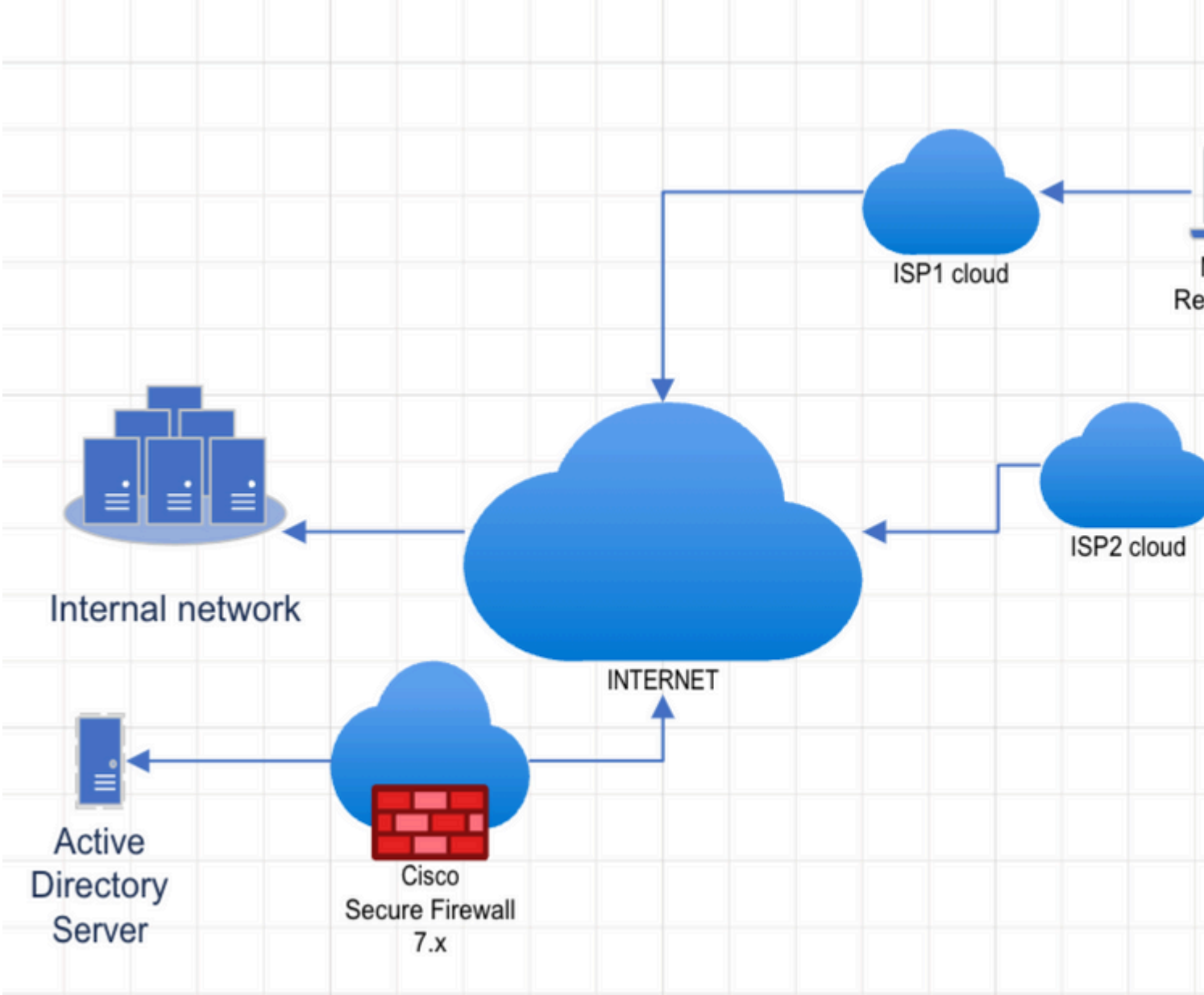
RAVPN designs run in different and dynamic scenarios that can not be controlled by network administrators. Usually there are several connections that land on the same VPN Gateway which based on multiple variables (i.e username, organizaiton, hardware device, operative system and so on) can determine how each connection can be threated, some of them can require priviledged user roles, access to programs and applications, different IP Address assignment or subnet filter rules.

Dynamic access policies (DAP), is a new feature introduced in software release 7.0.0 of the Cisco Secure Firewall Threat Defense, that allows the network administrators to apply different policies to different users that run over these dynamic environments mentioned above, based on a collection of attributes from the RAVPN clients from Cisco Secure Client (Anyconnect) equivalent with one or multiple criteria (DAP criteria).

Anyconnect software provides the RAVPN client features and Posture module the ability to identify attributes like OS, anti-virus, anti-spyware and firewall software installed on the host and the HostScan application gathers this information .

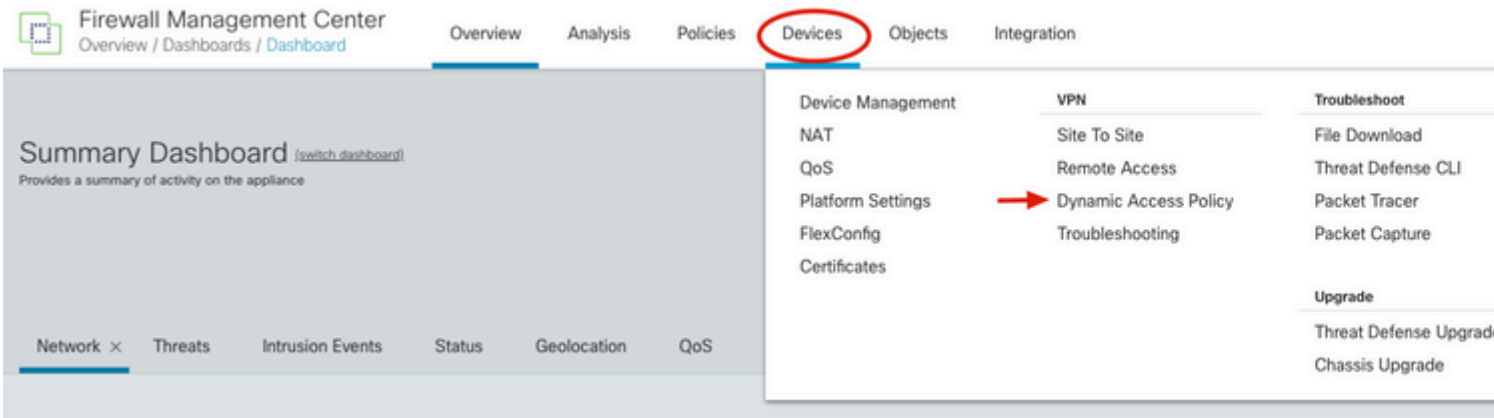
Configure

Network Diagram

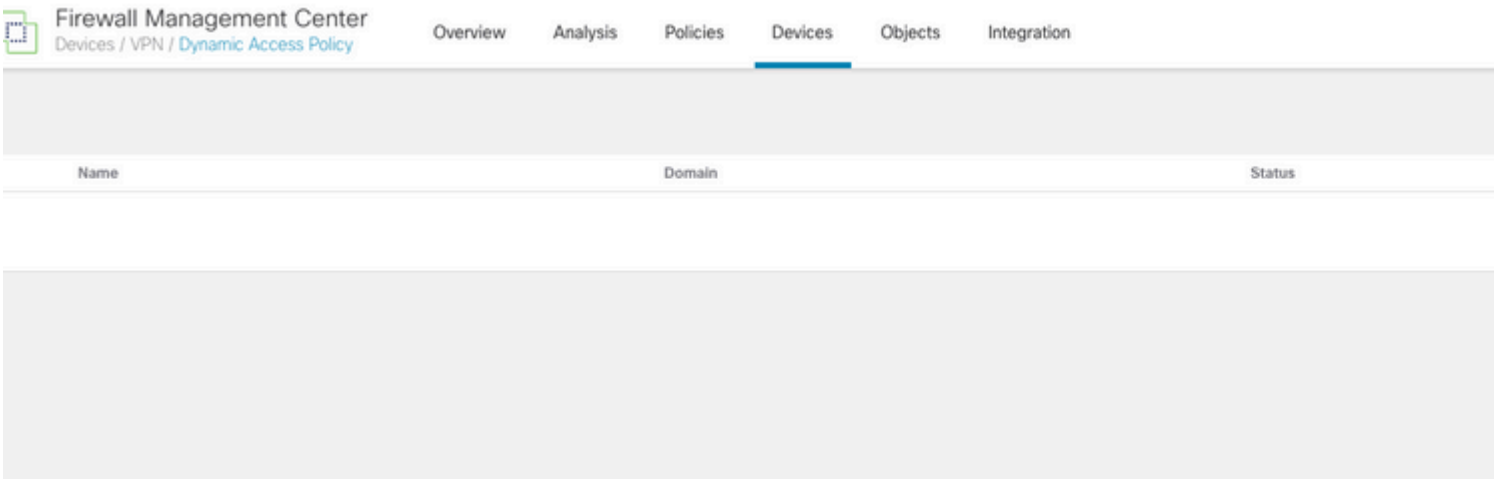


Configurations

1. Log in into FMC GUI with administrator credentials and from the home dashboard view click on **Devices** and select **Dynamic Access Policy** from the expanded menu.

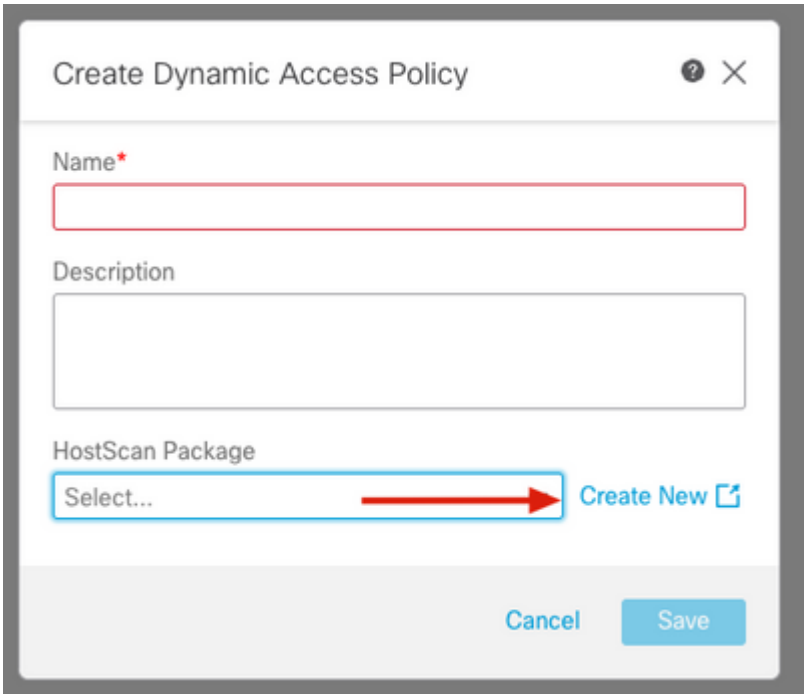


2. From the Dynamic Access Policy view click on **Create Dynamic Access Policy**.

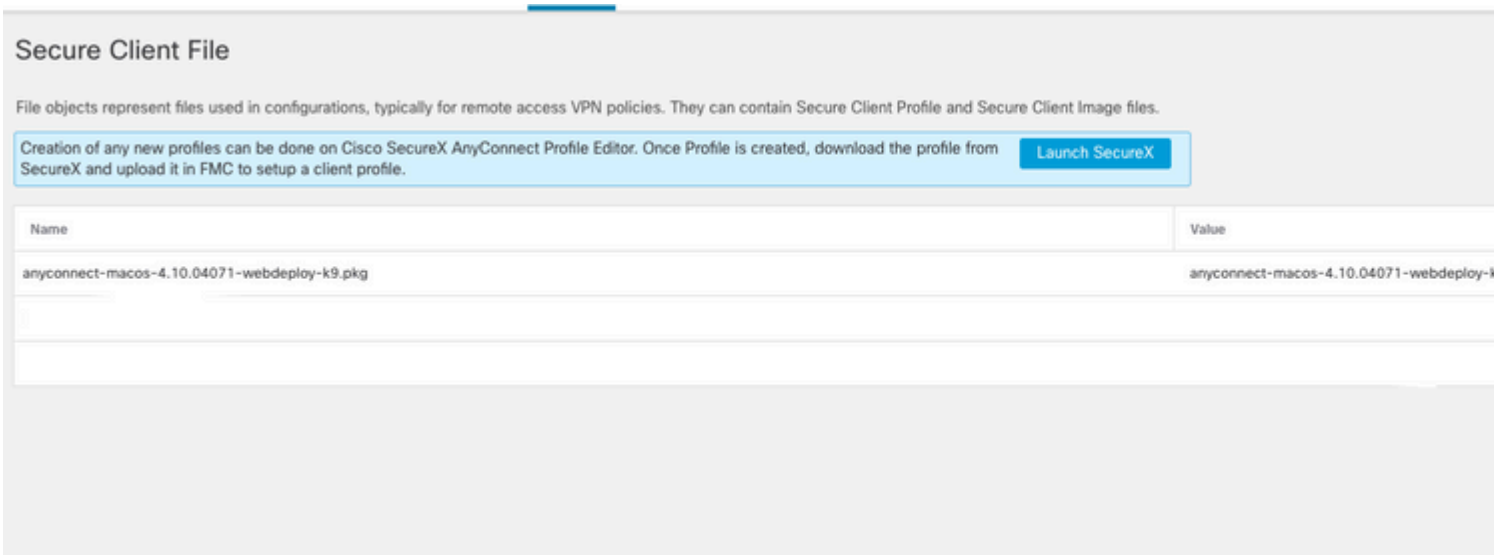


3. Specify a name for the DAP policy and selec t **Create new** next to the **HostScan package** dropdown menu (this action can open a new browser tab with the **Object manager** section).

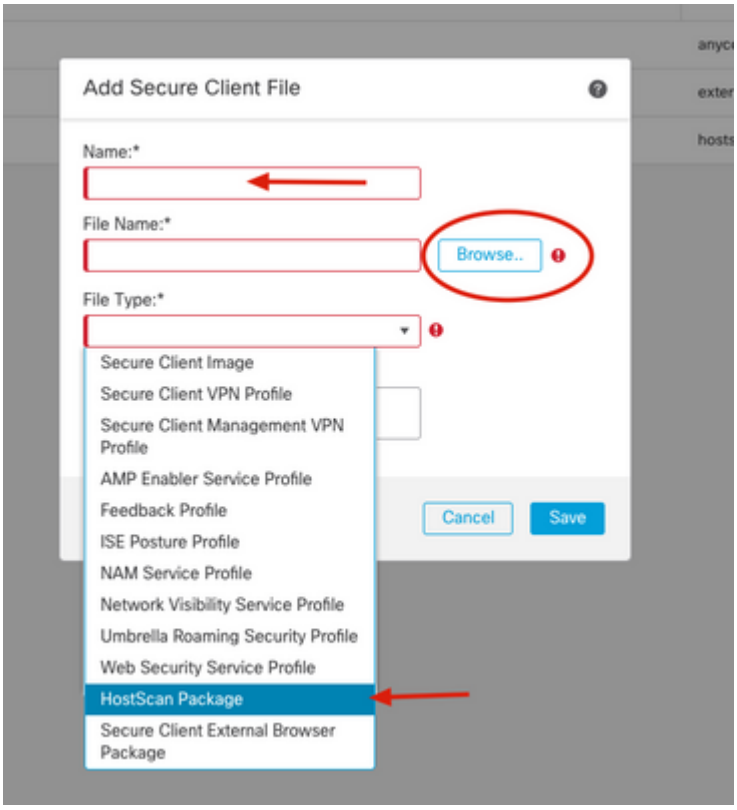
> **Note**:If a HostScan image has already been uploaded, select it from the dropdown menu, click on **Save** and skip to step 6.



4. In the **Object** tab view go to **Add Secure Client File**" to upload the HostScan package.

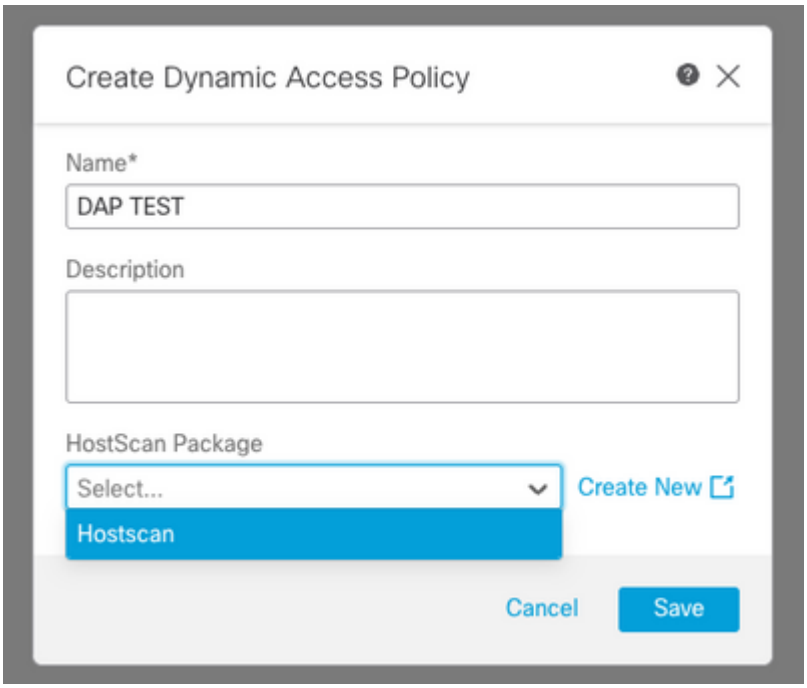


5. Specify the name of the file, click on **Browse** to upload the HostScan package (.pkg) from your local files and select **HostScan package** from the **File type** dropdown menu and then click on **Save**.



6. Go back to the **Create Dynamic Access Policy** tab from step 3.

Specify the name of the Dynamic Access Policy and this time you can see your new HostScan package on the dropdown menu and click on **Save**.



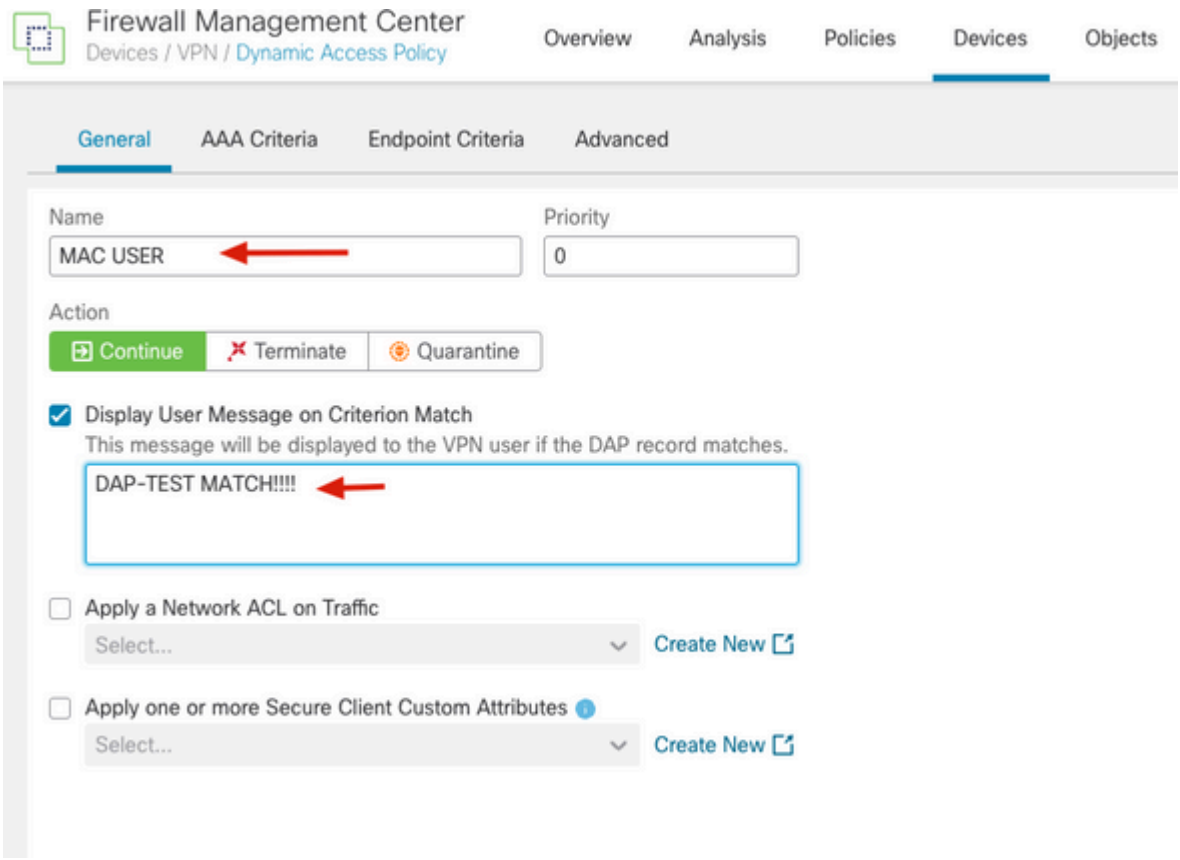
7. You can be redirected to the new DAP editor window, click on **Create DAP Record** to generate a new entry.

Note: In this example we can configure a DAP record to gather OS information from RAVPN Anyconnect client and allow the connection if host machine runs Mac OS.

---

8. Specify the name of the DAP record, check the **Display User Message on Criterion Match** and type a prompt message so that we let the user know that connection landed into a DAP based on the OS. Select **Continue** to allow connection under the **Action** field.

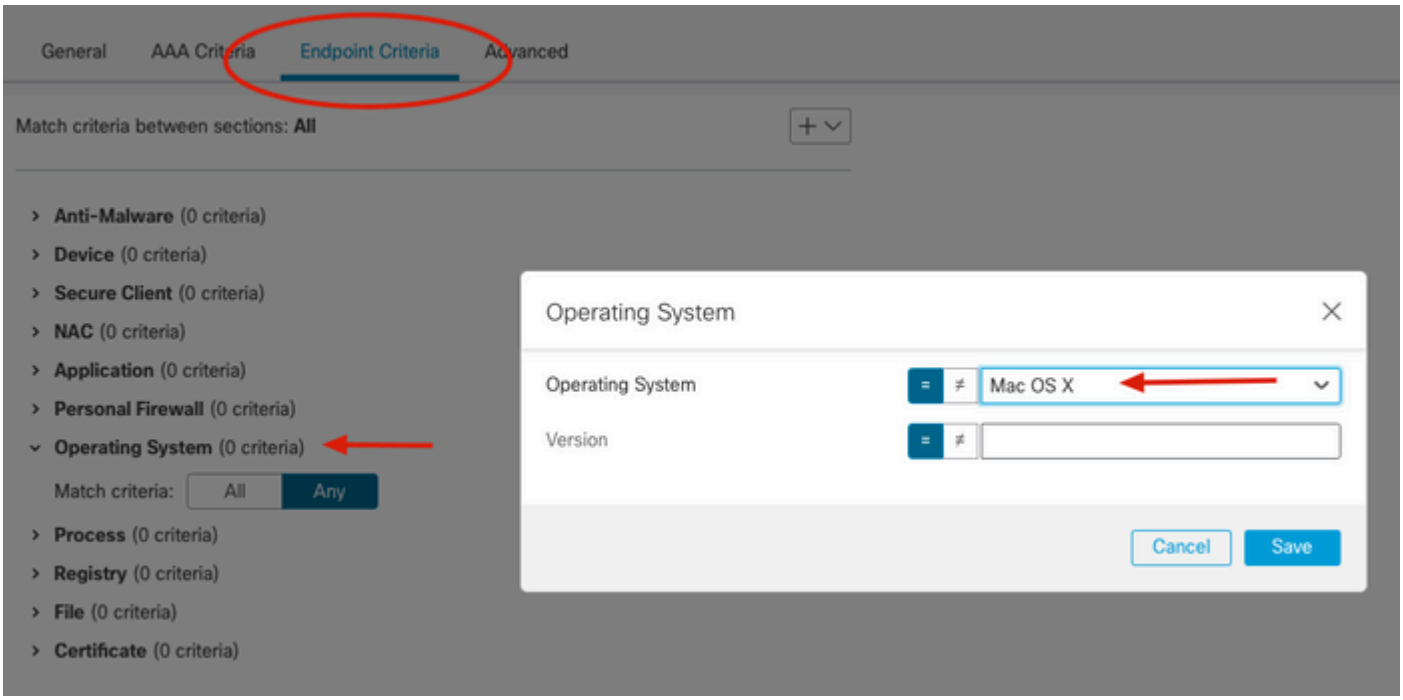
Note: You can either select **Terminate** or **Quarantine** as the action to apply based on your case.



Note: You can also apply a network ACL or Secure Client attributes as per your network requirements.

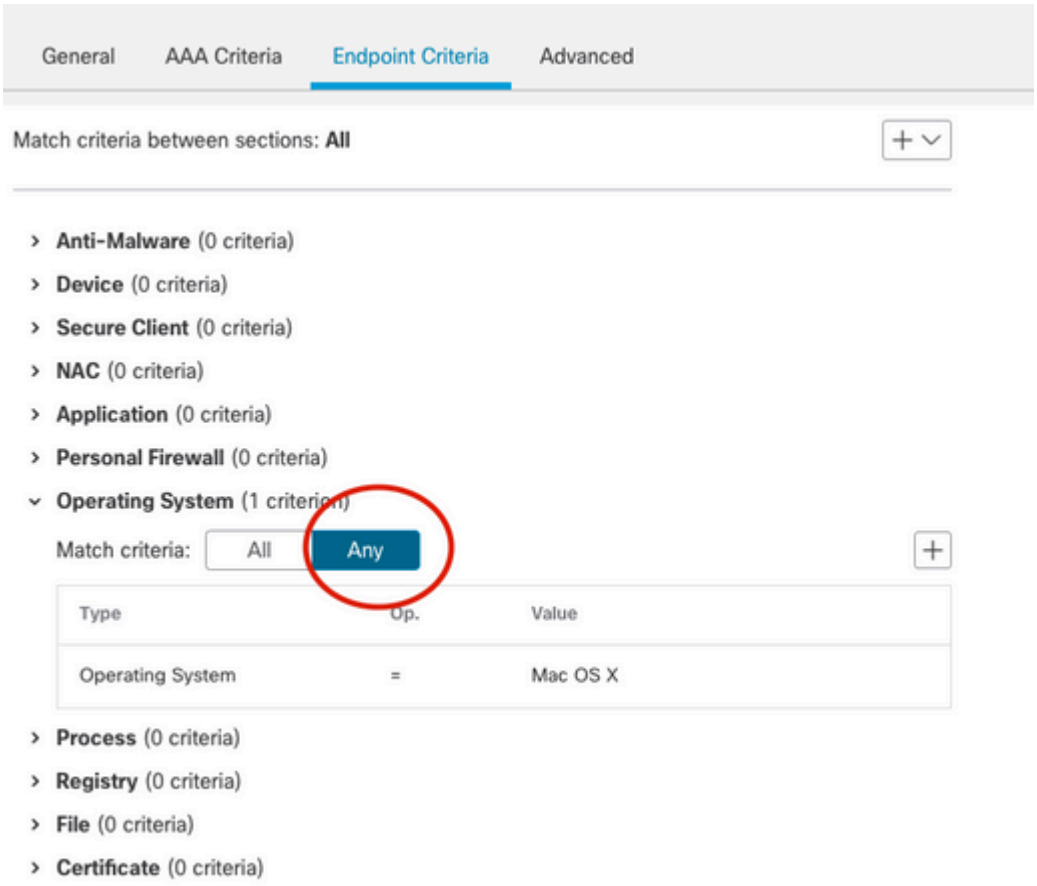
9. Go to **Endpoint Criteria** tab, select **OS system** and specify **equals Mac OS X**, leave **Version** dropdown empty as this example intention is to detect Mac OS regardless the version and click on **Save.**

Note: In this article **Endpoint Criteria** attributes are used but you can use AAA Criteria for LDAP or RADIUS attributes match.



10. From the **Endpoint Criteria** tab, you can see the new OS System criteria, followed by the **Match criteria** option.

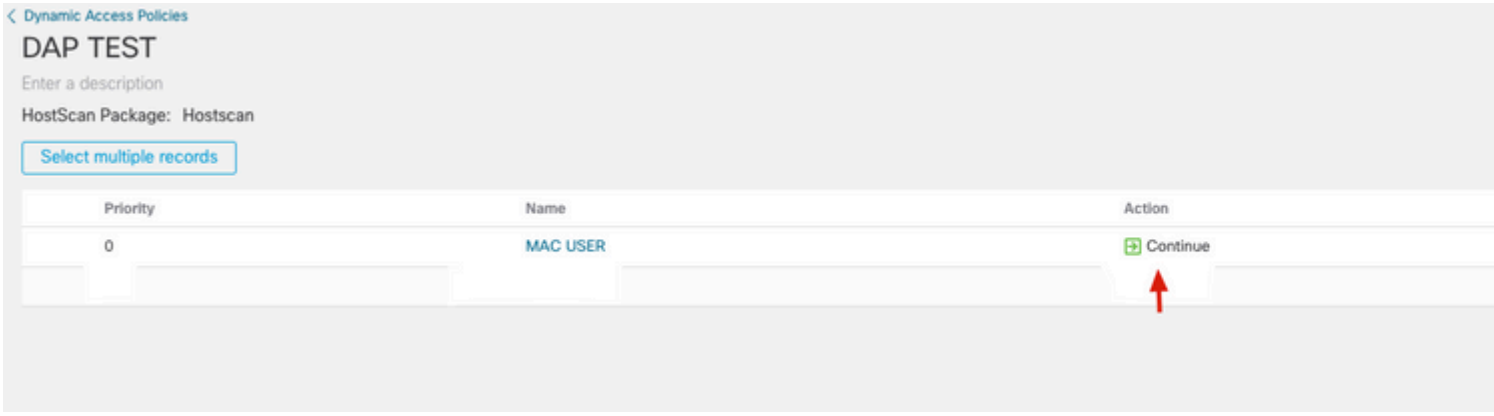
Select **Any**.



Note: You can create multiple criteria entries and select **Match All** or **Match any** as per your requirements.

---

11. Go to the right bottom of the page and click on **Save**.

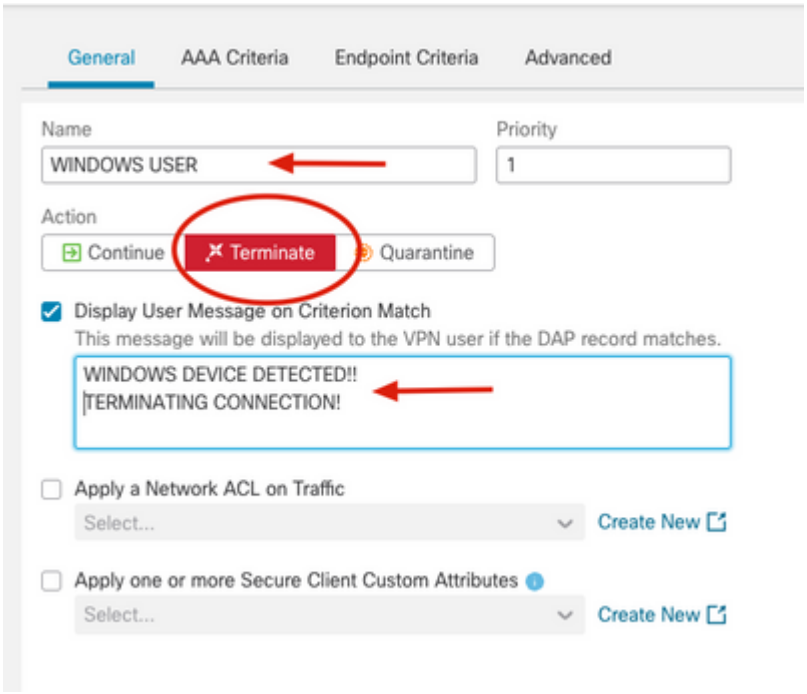


11. New Mac OS DAP record can be display with its configuration parameters, confirm they are correct and click on **Create DAP Record** to create a new record for Windows OS detection.

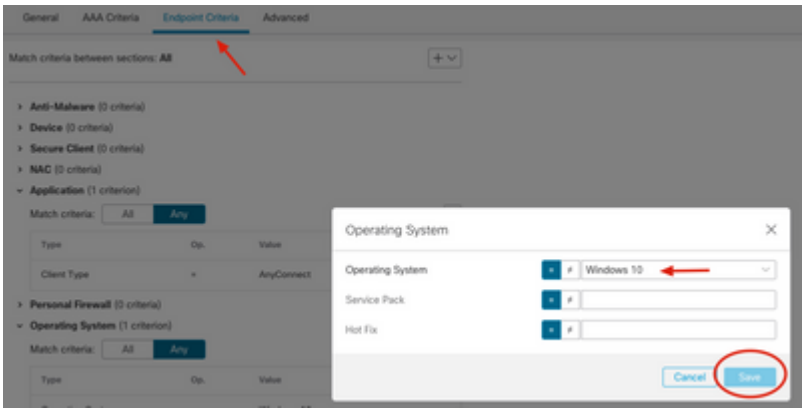
> **Note**: In this example the intention is to block Windows clients and allow only Mac OS for RAVPN connections.

---

12. Specify the name of the DAP Record, select **Terminate** under the **Action** field and type the warning message prompt to be sent to the user.

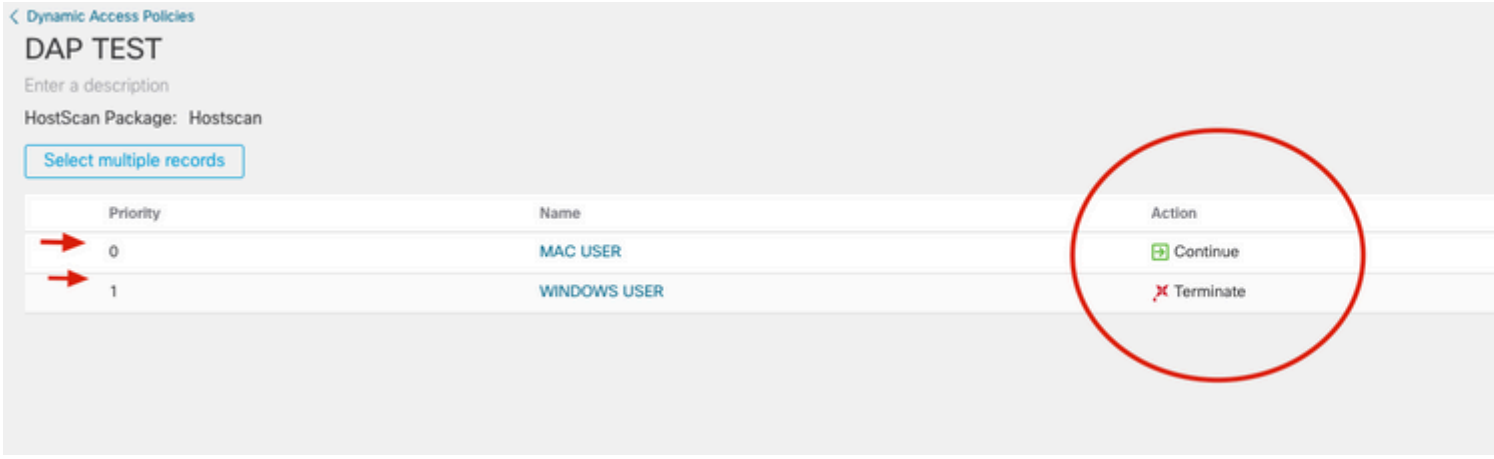


13. Go to **Endpoint Criteria** tab and create a new equivalent criteria under **Operative System** section, select **Windows 10** as the equivalent OS and click on **Save** then select **Match Any**.

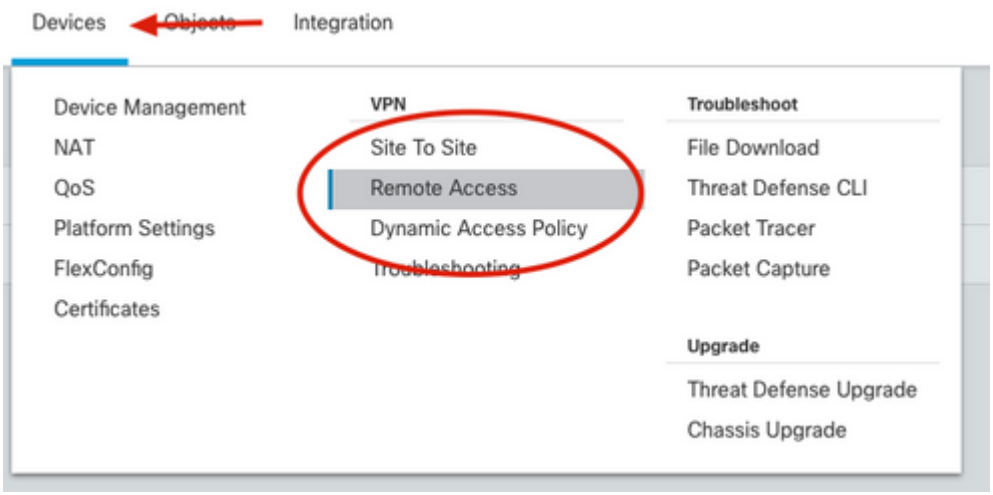


14. Go to the right bottom and click on **Save**.

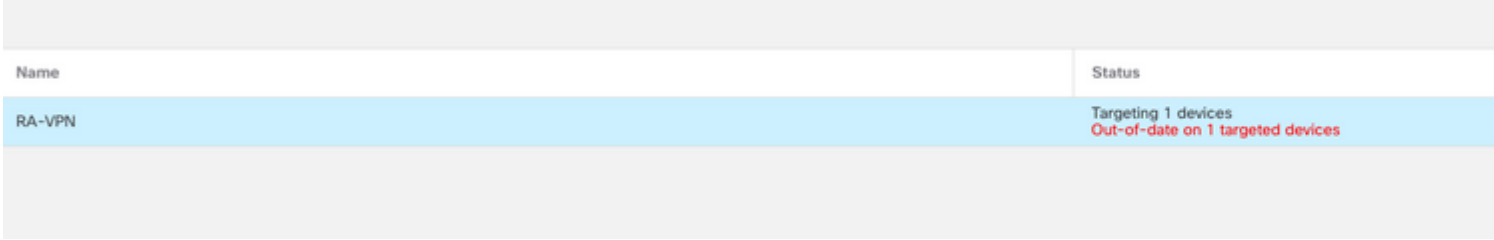
15. On the DAP menu confirm there are two new entries with the new configuration.



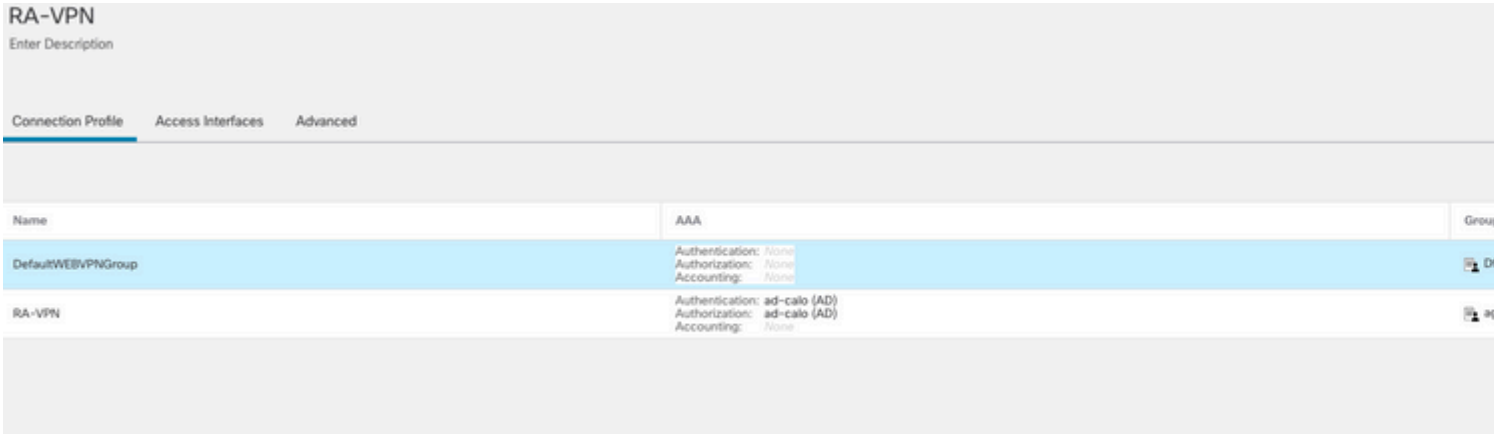
16. Dynamic Access Policy has been created, in order to apply it to the RAVPN set up, go to **Devices** tab from FMC GUI and click on **Remote Access**.



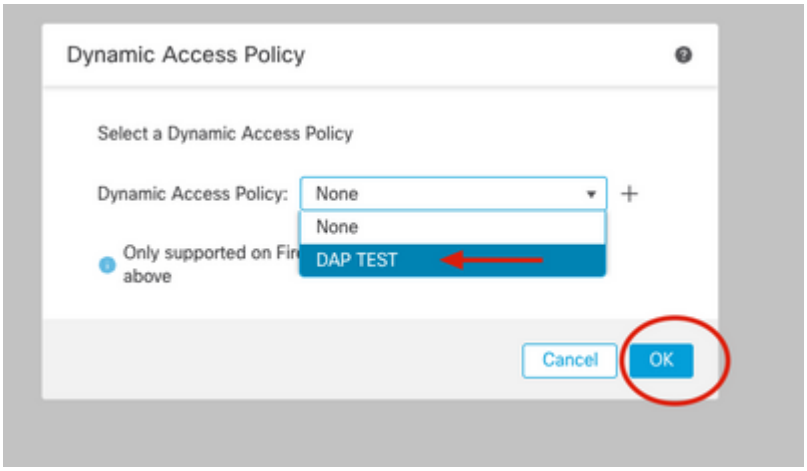
17. Select your pre configured RAVPN policy and click on the edit butoon (pencil icon).



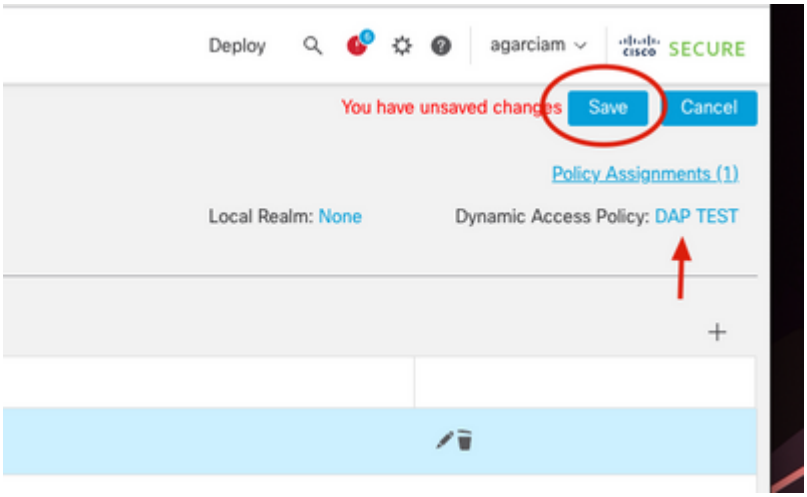
18. On the top right corner click on **None** next to the **Dynamic Access Policy** text label.



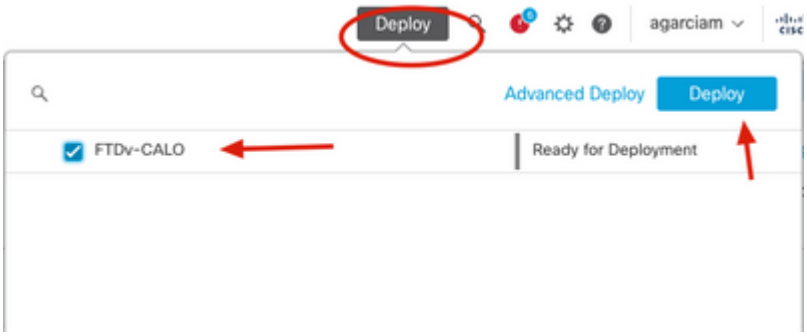
19. On the Dynamic Access Policy window, select the DAP policy we just created and click **OK.**



20. On the top right corner confirm DAP is applied next to the Dynamic Access Policy text label and click on **Save.**



Deploy changes, click **Deploy** tab from FMC GUI, select the FTD Device and click **Deploy** button.



Verify

1. Go Command Line Interface (CLI) from the Secure Firewall, confirm HostScan configuration has been applied:

```
firepower# sh run webvpn

webvpn
enable OUTSIDE
enable
hostscan image disk0:/csm/hostscan_4.10.06083-k9.pkg
hostscan enable
anyconnect image disk0:/csm/anyconnect-macos-4.10.04071-webdeploy-k9.pkg 1 regex "Mac OS"
anyconnect enable
.
.

firepower# sh run all dynamic-access-policy-record

dynamic-access-policy-record DfltAccessPolicy
 user-message "nDID NOT MEET THE CRITERIA! TERMINATING"
 action terminate
dynamic-access-policy-record "MAC USER"
 user-message "DAP-TEST MATCH!!!!MAC USER DETECTED"
 action continue
 priority 0
dynamic-access-policy-record "WINDOWS USER"
 user-message "WINDOWS DEVICE DETECTED!!TERMINATING CONNECTION!"
 action terminate
 priority 1
```

2. Confirm dap.xml file has been generated and stored in flash:

```
firepower# sh flash:
--#-- --length-- -----date/time------ path
76 4096 Feb 03 2023 19:01:10 log
222 1293 Feb 09 2023 17:32:16 dap.xml
```

3. Display dap.xml content

```
firepower# more flash:dap.xml
<?xml version="1.0" encoding="UTF-8"?>
<dapRecordList>
<dapRecord>
<dapName>
<value>MAC USER</value>
</dapName>
<dapViewsRelation>
<value>and</value>
</dapViewsRelation>
<dapBasicView>
<dapSelection>
<dapPolicy>
<value>match-any</value>
</dapPolicy>
<dapSubSelection>
<dapPolicy>
<value>match-all</value>
</dapPolicy>
<attr>
<name>endpoint.os.version</name>
<operation>EQ</operation>
<value>Mac OS X</value>
</attr>
</dapSubSelection>
</dapSelection>
</dapBasicView>
</dapRecord>
<dapRecord>
<dapName>
<value>WINDOWS USER</value>
</dapName>
<dapViewsRelation>
<value>and</value>
</dapViewsRelation>
<dapBasicView>
<dapSelection>
<dapPolicy>
<value>match-any</value>
</dapPolicy>
<dapSubSelection>
<dapPolicy>
<value>match-all</value>
</dapPolicy>
<attr>
<name>endpoint.os.version</name>
<operation>EQ</operation>
<value>Windows 10</value>
</attr>
</dapSubSelection>
</dapSelection>
</dapBasicView>
</dapRecord>
</dapRecordList>
```

Troubleshoot

This section provides the information you can use in order to troubleshoot and confirm how DAP process is

performed and works as expected.

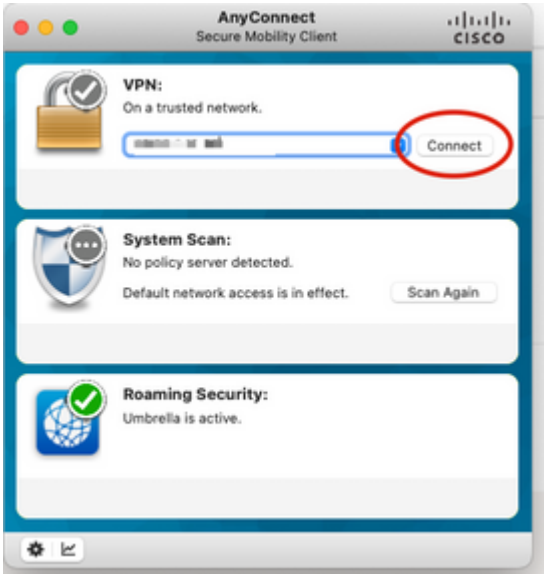
> **Note**: On the Secure Firewall, you can set various debug levels; by default, level 1 is used. If you change the debug level, the verbosity of the debugs can increase. Do this with caution, especially in production environments.

Test with Mac OS.

Enable DAP debugs while user tries to connect from one Mac OS device.

```
firepower# debug dap trace 127
debug dap trace enabled at level 127
firepower# debug dap errors
debug dap errors enabled at level 1
```

Initiate Mac OS device and run Anyconnect application, connect to the IP Address/hostname/FQDN and click **Connect** login with the requested authentication method.

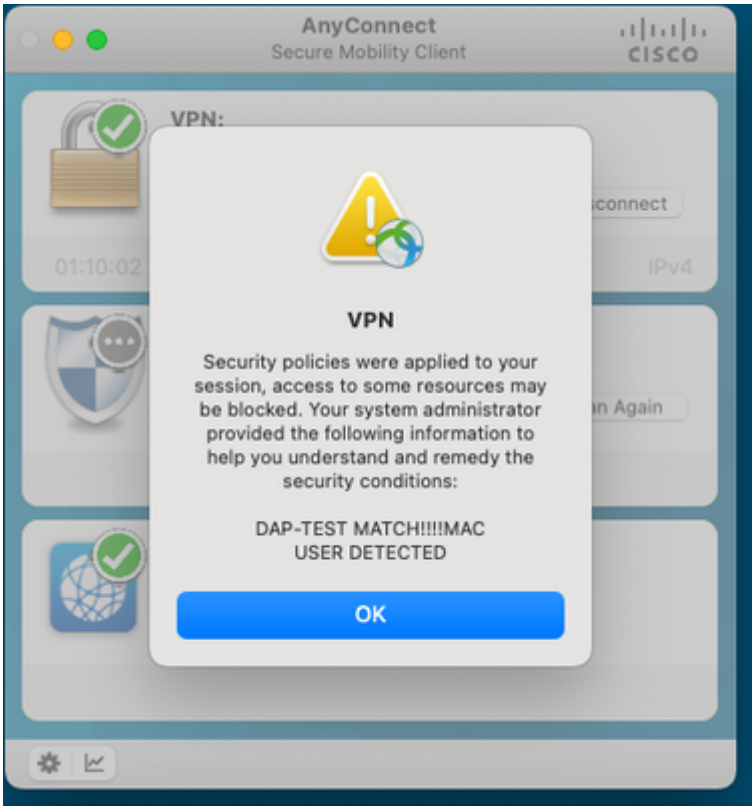


Debugs output on Secure Firewall CLI

```
firepower#
firepower# DAP_TRACE: DAP_open: New DAP Request: 9
DAP_TRACE[5]: Username: ad1, DAP_add_AC:
endpoint.anyconnect.clientversion = "4.10.06079";
endpoint.anyconnect.platform = "mac-intel";
endpoint.anyconnect.devicetype = "MacBookPro17,1";
endpoint.anyconnect.platformversion = "13.1.0";
.
.
.
DAP_TRACE: aaa["ldap"]["displayName"] = "ad1"
DAP_TRACE: aaa["ldap"]["memberOf"] = "AD-USERS-ONLY"
DAP_TRACE: aaa["ldap"]["name"] = "ad1"
.
```

```
.
.
DAP_TRACE: aaa["cisco"]["tunnelgroup"] = "RA-VPN"
DAP_TRACE: endpoint["application"]["clienttype"] = "AnyConnect"
DAP_TRACE: endpoint.os.version = "Mac OS X"
DAP_TRACE: endpoint.os.servicepack = "13.1"
.
.
.
DAP_TRACE: Username: ad1, Selected DAPs: ,MAC USER
DAP_TRACE: dap_process_selected_daps: selected 1 records
DAP_TRACE: Username: ad1, dap_concat_fcn: [DAP-TEST MATCH!!!!MAC USER DETECTED] 35 490
DAP_TRACE: Username: ad1, DAP_close: 9
```

Mac OS client prompt.

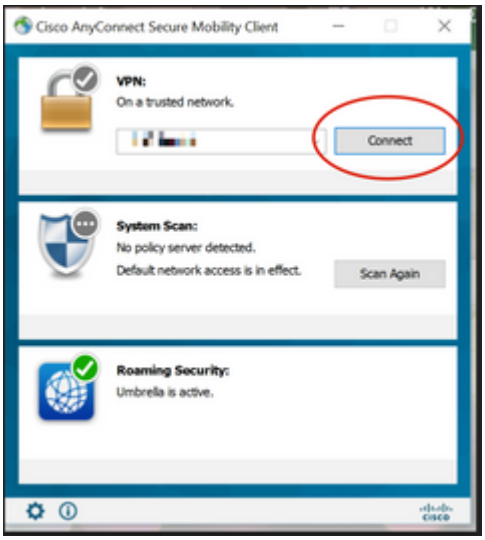


Test with Windows 10 device.

Run DAP debugs and try to connect from one Windows 10 device.

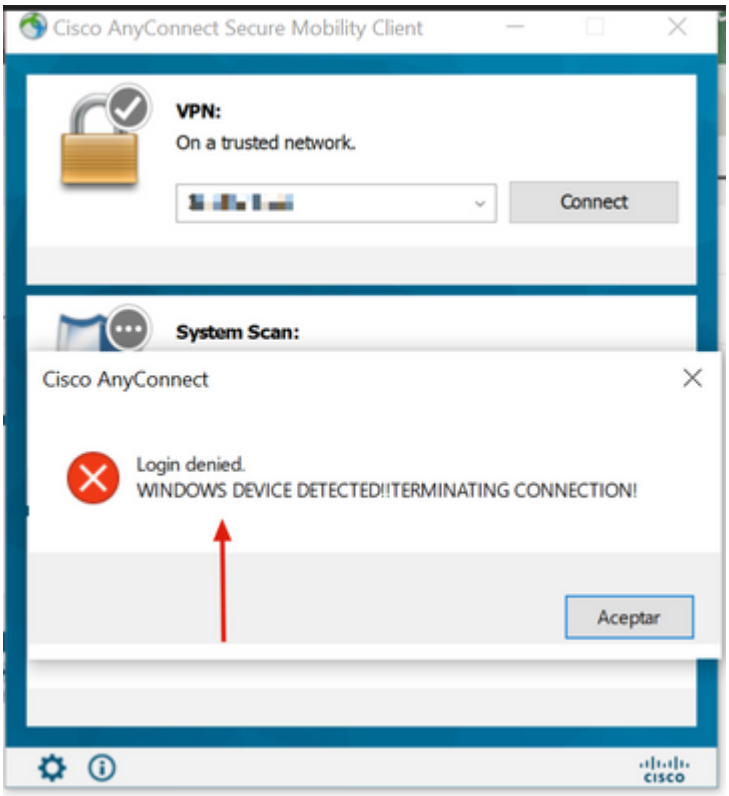
```
firepower# debug dap trace 127
debug dap trace enabled at level 127
firepower# debug dap errors
debug dap errors enabled at level 1
```

Initiate Windows 10 device and run Anyconnect appliation, connect to the IP Address/hostname/FQDN and click **Connect** login with the requested authentication method.




```
firepower#
firepower# DAP_TRACE: DAP_open: New DAP Request: A
DAP_TRACE[5]: Username: ad1, DAP_add_AC:
endpoint.anyconnect.clientversion = "4.10.05111";
endpoint.anyconnect.platform = "win";
endpoint.anyconnect.devicetype = "LENOVO";
endpoint.anyconnect.useragent = "AnyConnect Windows 4.10.05111";
.
.
.
AP_TRACE: aaa["cisco"]["grouppolicy"] = "agarciam"
DAP_TRACE: aaa["cisco"]["username"] = "ad1"
DAP_TRACE: aaa["cisco"]["tunnelgroup"] = "RA-VPN"
DAP_TRACE: endpoint["application"]["clienttype"] = "AnyConnect"
DAP_TRACE: endpoint.os.version = "Windows 10"
.
.
.
DAP_TRACE: Username: ad1, Selected DAPs: ,WINDOWS USER
DAP_TRACE: dap_process_selected_daps: selected 1 records
DAP_TRACE: Username: ad1, dap_concat_fcn: [WINDOWS DEVICE DETECTED!!TERMINATING CONNECTION!] 48 490
DAP_TRACE: Username: ad1, DAP_close: A
```

Windows 10 user promtp.


Cisco AnyConnect Secure Mobility Client
VPN:
On a trusted network.
Connect
System Scan:
Cisco AnyConnect
Login denied.
WINDOWS DEVICE DETECTED!!TERMINATING CONNECTION!
Aceptar
cisco