# 部署ASA 9.X動態訪問策略(DAP)

## 目錄



## 簡介

本文檔介紹ASA 9.x動態訪問策略(DAP)的部署、功能和用法。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 虛擬私人網路(VPN)閘道
- 動態存取原則(DAP)

### 採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

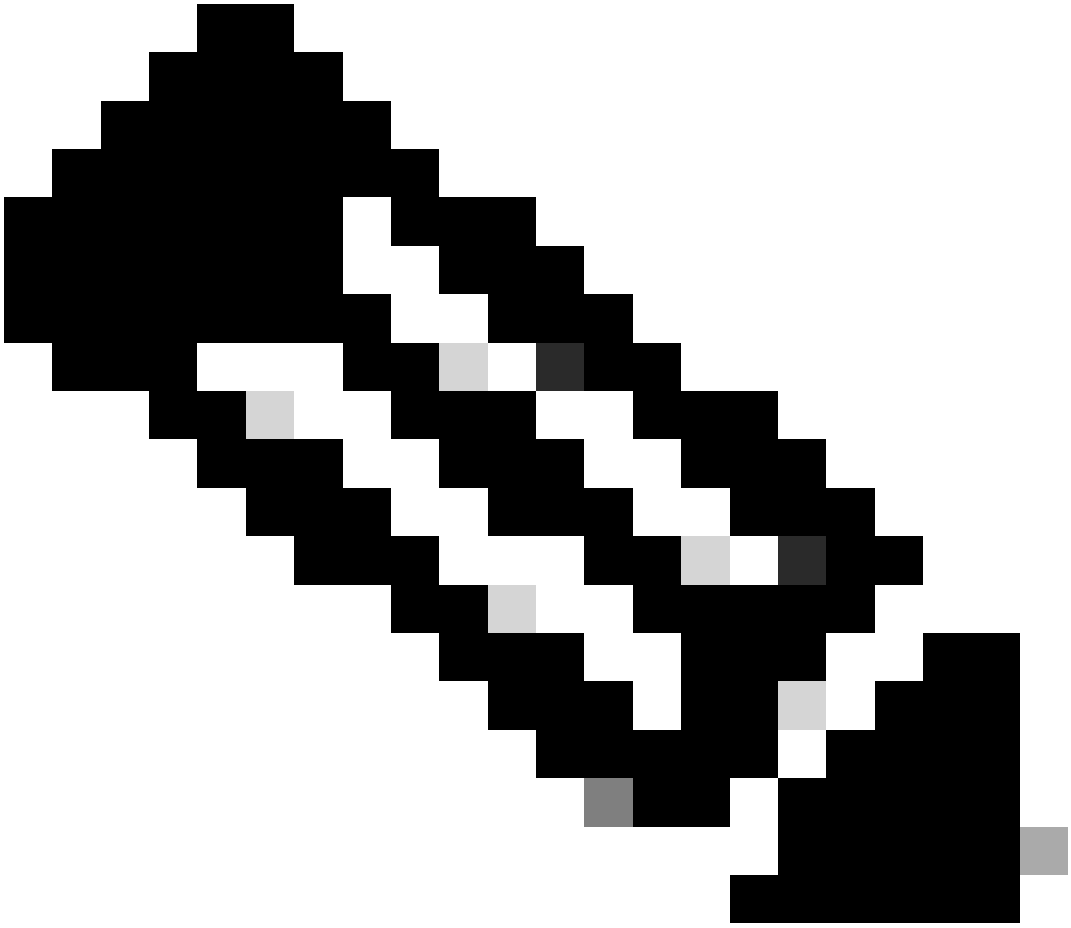
## 背景資訊

虛擬私人網路(VPN)閘道可在動態環境中運作。多個變數會影響每個VPN連線；例如，經常更改的內部網配置、每個使用者在一個組織內可以使用的各種角色，以及從具有不同配置和安全級別的遠端訪問站點登入。在動態VPN環境中，授權使用者的任務比在靜態配置網路中要複雜得多。

動態訪問策略(DAP)是一種功能，可讓您配置可解決VPN環境動態變化的授權。透過設定與特定使用者隧道或會話相關聯的訪問控制屬性集合，可以建立動態訪問策略。這些屬性可解決多個組成員身份和終端安全問題。

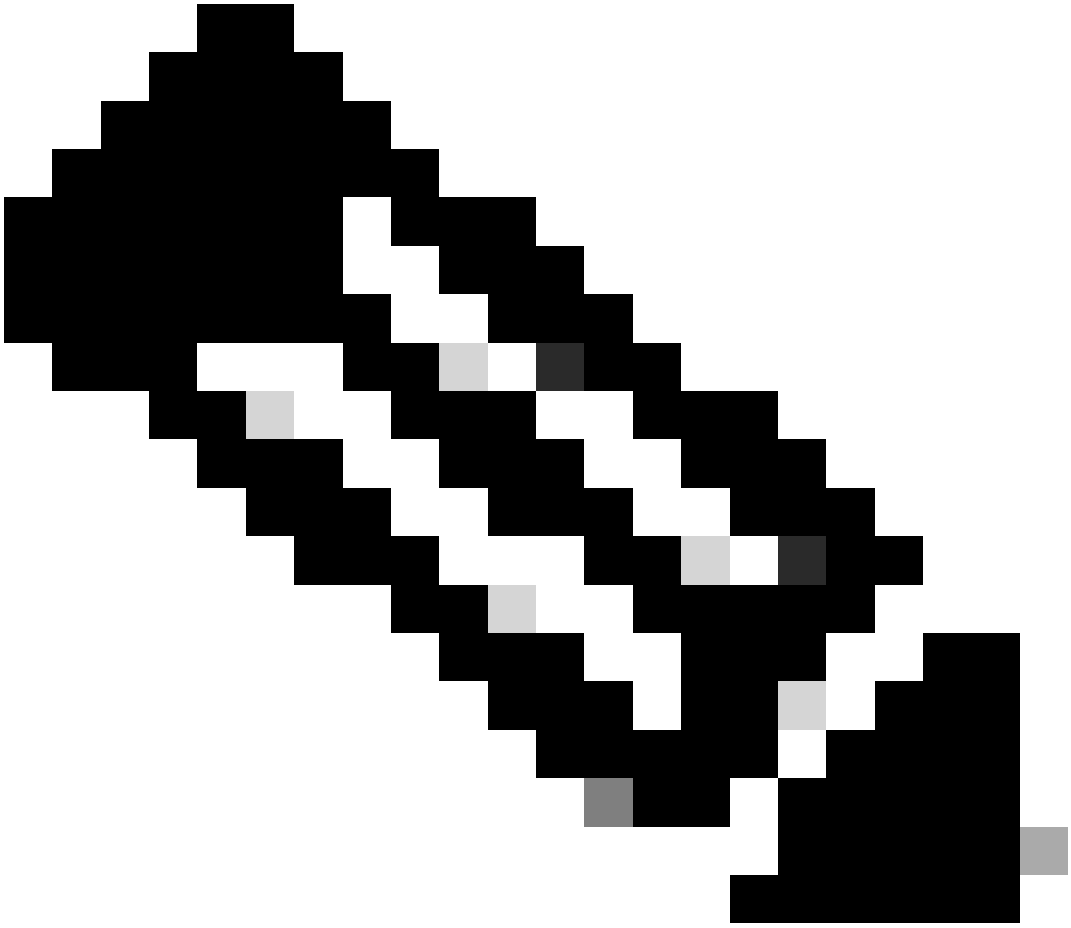
例如，安全裝置會根據您定義的策略，將特定會話的訪問權授予特定使用者。它透過從一個或多個DAP記錄中選擇和/或聚合屬性來生成整個使用者身份驗證的DAP。它基於遠端裝置的終端安全資訊和/或認證使用者的AAA授權資訊選擇這些DAP記錄。然後將DAP記錄應用到使用者隧道或會話。

---



注意：包含DAP策略選擇屬性的dap.xml檔案儲存在ASA快閃記憶體中。雖然您可以將dap.xml檔案導出到裝置外，對其進行編輯（如果您知道XML語法），然後重新將其導入，但請務必小心，因為如果配置有誤，可能會導致ASDM停止處理DAP記錄。沒有CLI可以處理此部分的配置。

---



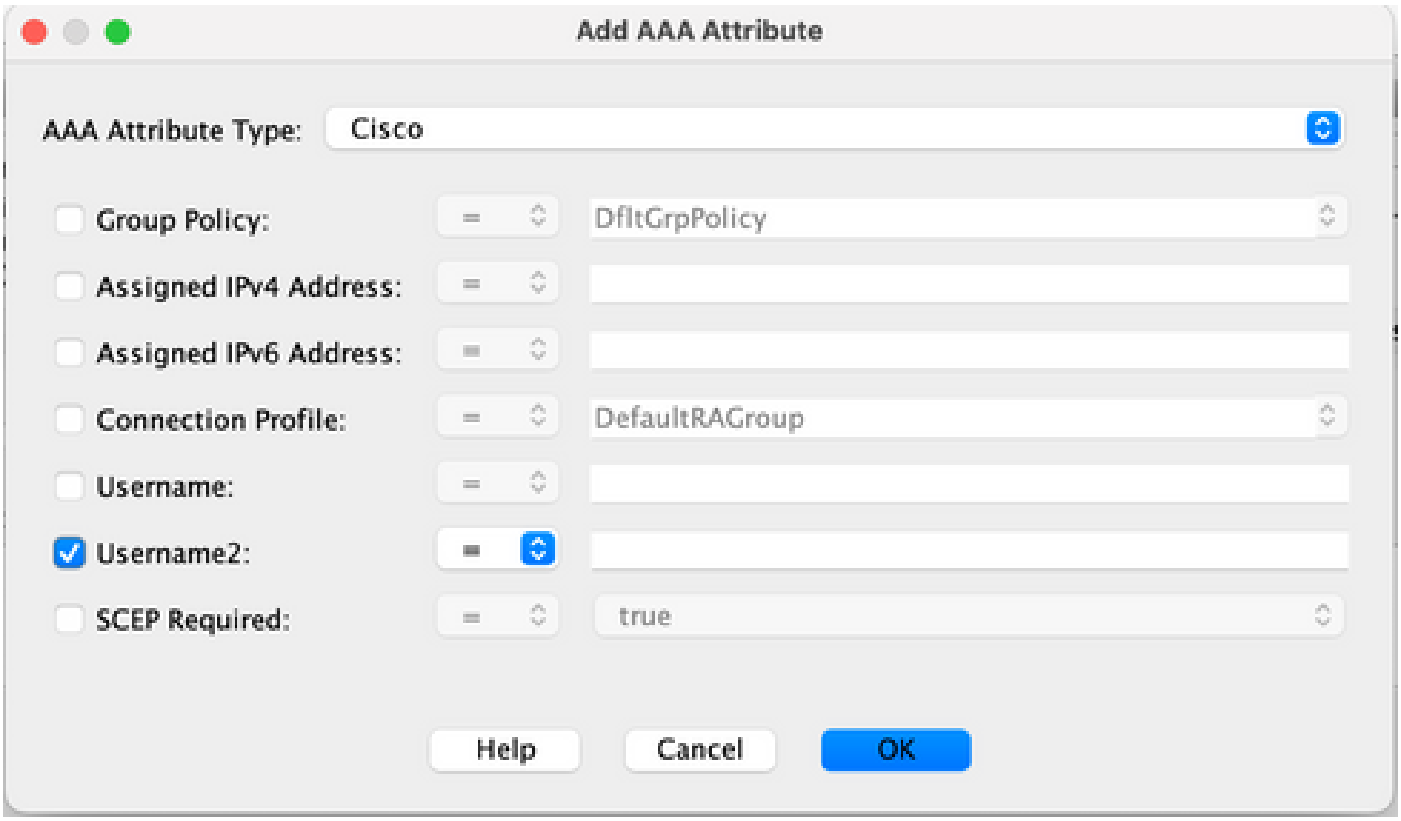
注意：嘗試透過CLI配置dynamic-access-policy-record訪問引數會導致DAP停止工作，儘管ASDM可正確管理這些引數。避免CLI，並始終使用ASDM管理DAP策略。

## DAP和AAA屬性

DAP補充了AAA服務，並提供一組有限的授權屬性，這些屬性可以覆蓋AAA提供的屬性。安全裝置可以根據使用者的AAA授權資訊選擇DAP記錄。安全裝置可根據此資訊選擇多個DAP記錄，然後聚合這些記錄以分配DAP授權屬性。

您可以從Cisco AAA屬性層次結構或從安全裝置從RADIUS或LDAP伺服器接收的完整響應屬性集中指定AAA屬性，如圖1所示。

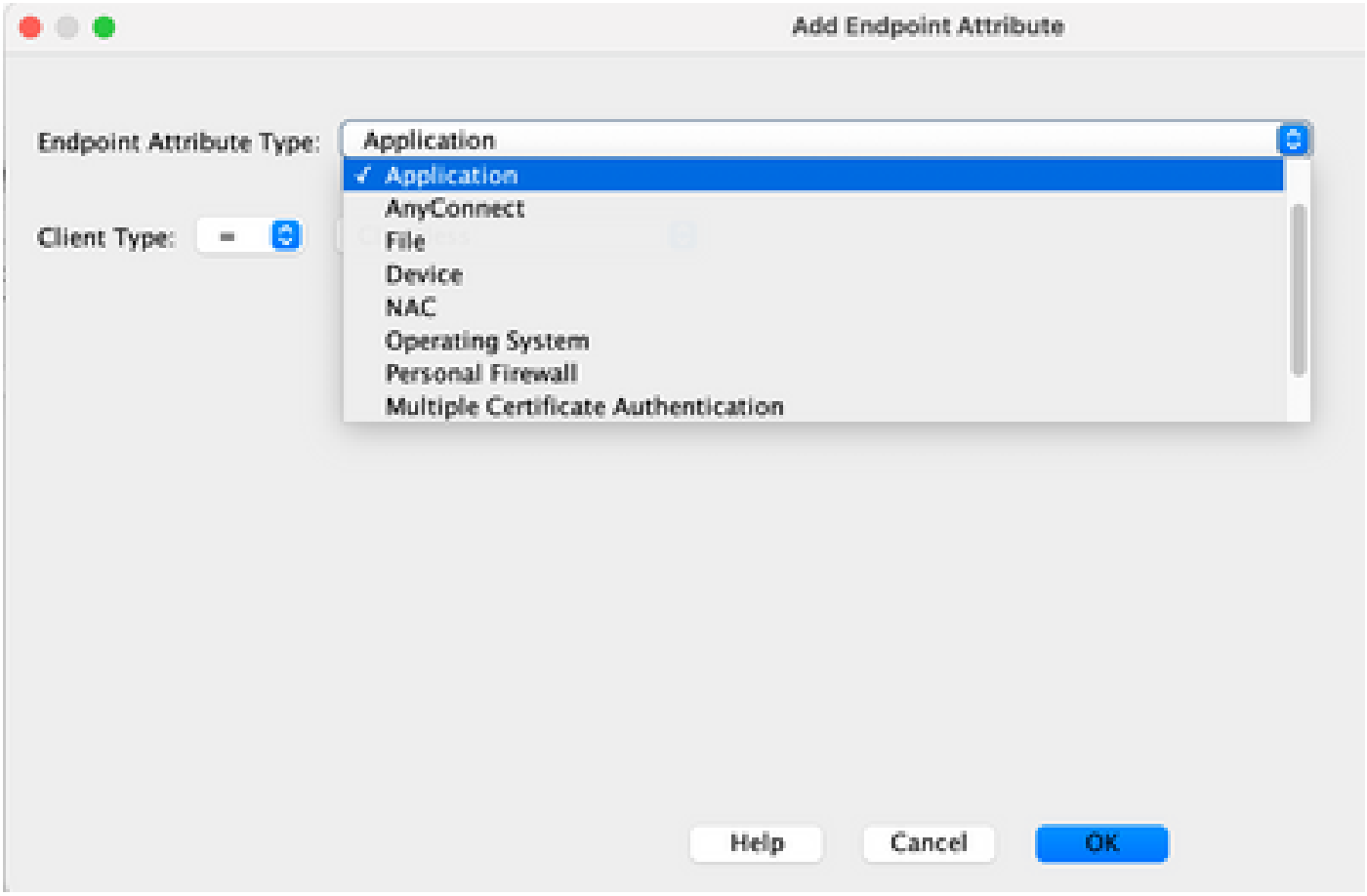
圖1.DAP AAA屬性GUI




## DAP和終端安全屬性

除AAA屬性外，安全裝置還可以使用您配置的狀態評估方法獲取終端安全屬性。如圖2所示，其中包括基本主機掃描、安全案頭、標準/高級終端評估和NAC。獲取終端評估屬性，並在使用者身份驗證之前將其傳送到安全裝置。但是，AAA屬性（包括整體DAP記錄）在使用者身份驗證期間會進行驗證。

圖2.終端屬性GUI

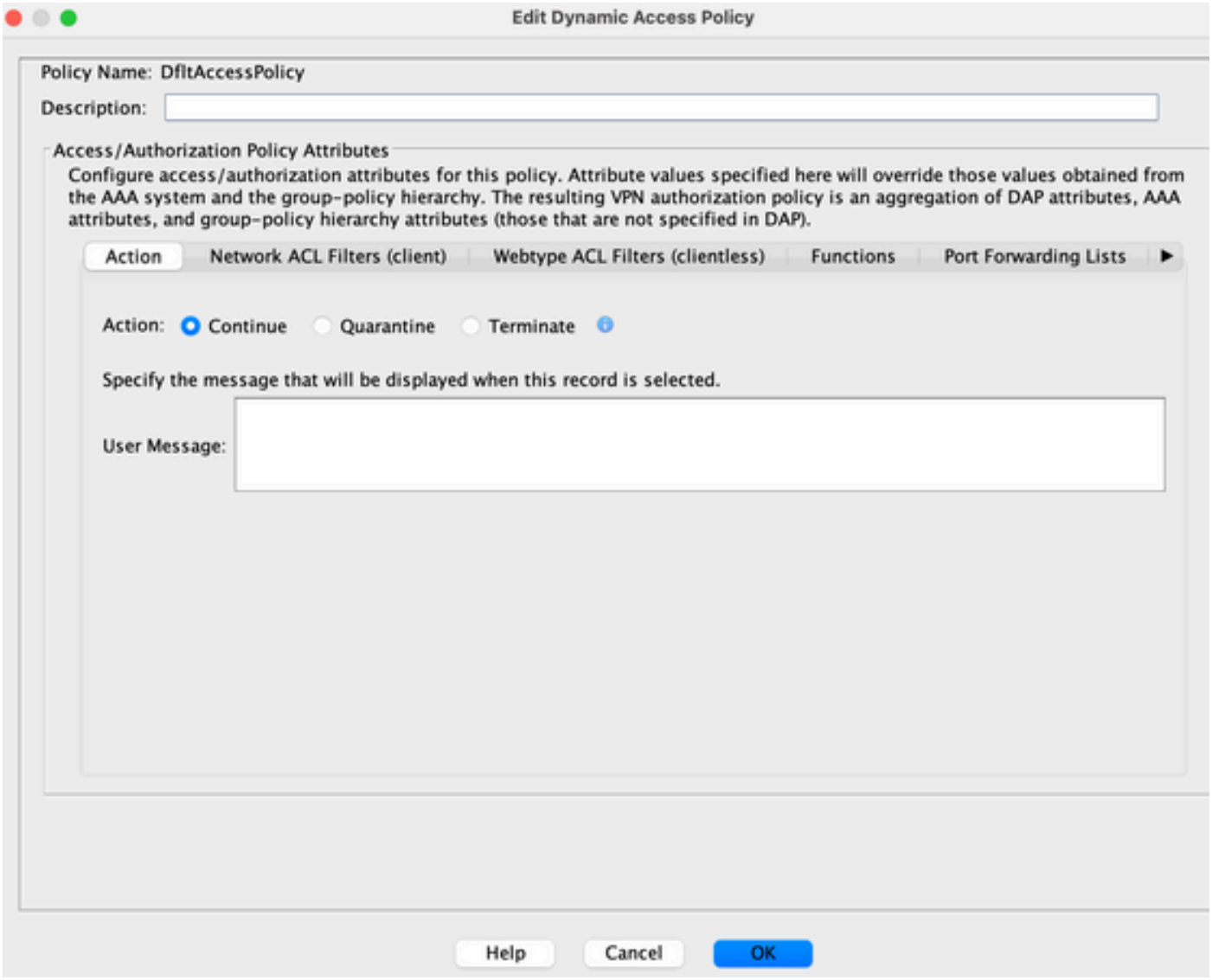



## 預設動態訪問策略

在引入和實施DAP之前，與特定使用者隧道或會話相關聯的訪問策略屬性/值對在ASA本地定義（即，隧道組和組策略）或透過外部AAA伺服器進行對映。

預設情況下，DAP始終被強制執行。例如，透過隧道組、組策略和AAA實施訪問控制而不明確實施DAP仍可獲得此行為。對於舊版行為，DAP功能(包括預設DAP記錄DfltAccessPolicy)的配置無需更改，如圖3所示。

圖3.預設動態訪問策略



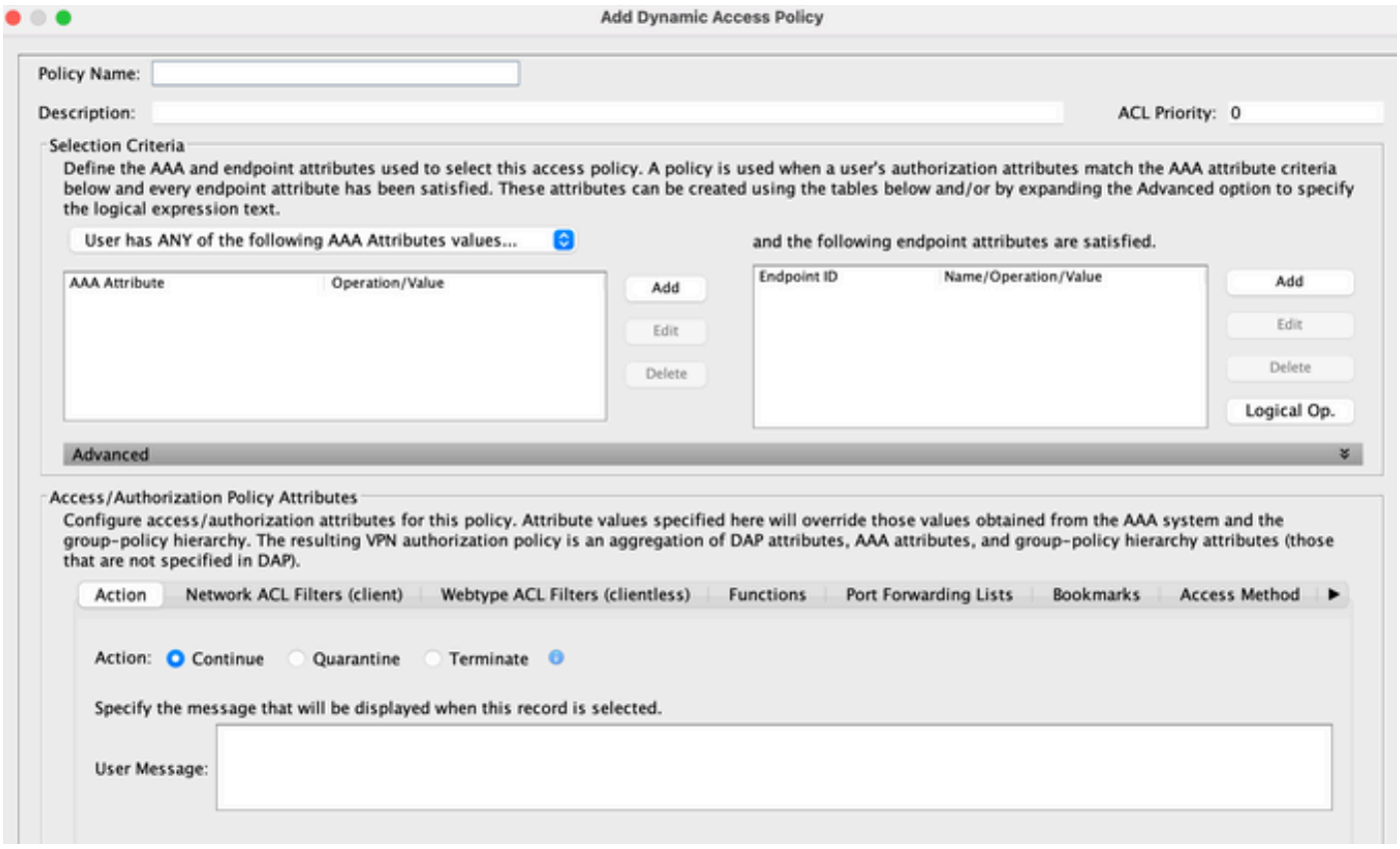

但是，如果DAP記錄中的任何預設值已更改，例如，DfltAccessPolicy中的Action：引數已從預設值更改為「Terminate」，並且未配置其他DAP記錄，則預設情況下，經過身份驗證的使用者可以匹配DfltAccessPolicy DAP記錄，並且可以拒絕VPN訪問。

因此，需要建立並配置一個或多個DAP記錄，以授權VPN連線並定義已驗證使用者有權訪問的網路資源。因此，DAP（如果已配置）可以優先於傳統策略實施。

## 配置動態訪問策略

使用DAP定義使用者有權訪問的網路資源時，需要考慮許多引數。例如，如果您確定連線端點是否來自託管、非託管或不受信任的環境，則確定辨識連線端點所需的選擇標準，並根據端點評估和/或AAA憑證（連線使用者有權訪問哪些網路資源）。為此，您必須首先熟悉DAP的特性和功能，如圖4所示。

圖4.動態訪問策略




配置DAP記錄時，需要考慮兩個主要組成部分：

- 包含進階選項的選取條件
- 存取原則屬性

選擇條件部分是管理員配置用於選擇特定DAP記錄的AAA和終端屬性的部分。當使用者的授權屬性與AAA屬性條件匹配，並且每個終端屬性都得到滿足時，使用DAP記錄。

例如，如果選擇AAA Attribute Type LDAP (Active Directory)，則Attribute Name字串是memberOf，Value字串是Contractors（如圖5a所示），則驗證使用者必須是Active Directory組Contractors的成員，才能匹配AAA屬性條件。

除滿足AAA屬性條件外，身份驗證使用者還需要滿足終端屬性條件。例如，如果管理員配置為確定連線終端的終端安全評估並基於該終端安全評估結果，則管理員可將此評估資訊用作圖5b所示終端屬性的選擇標準。

圖5a.AAA屬性條件

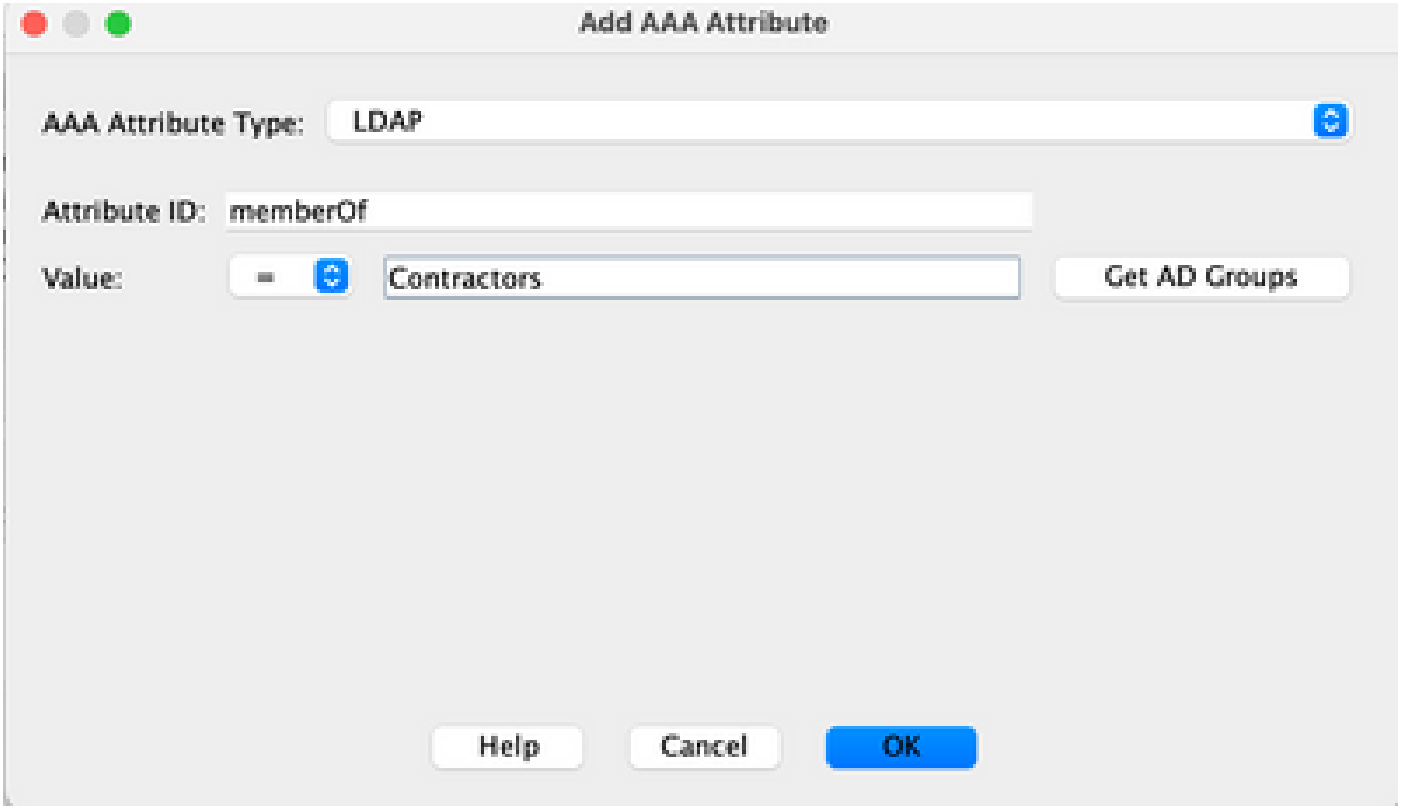



圖5b.端點屬性條件

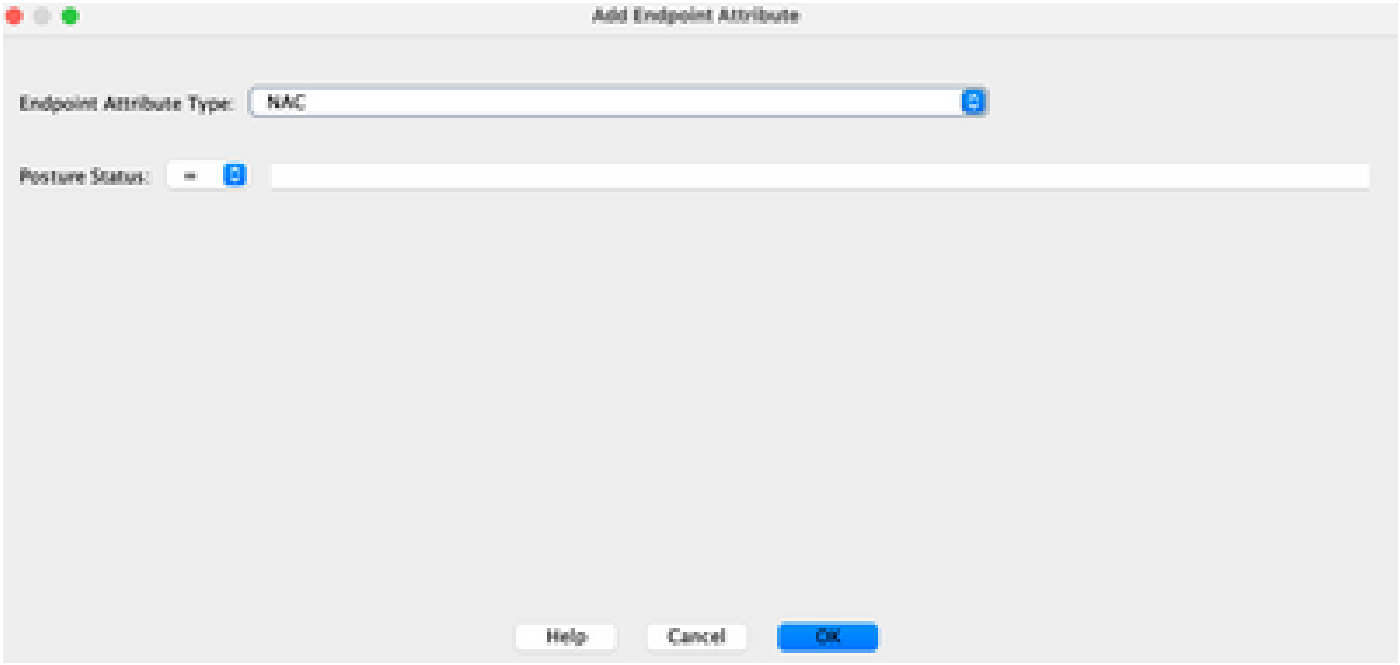
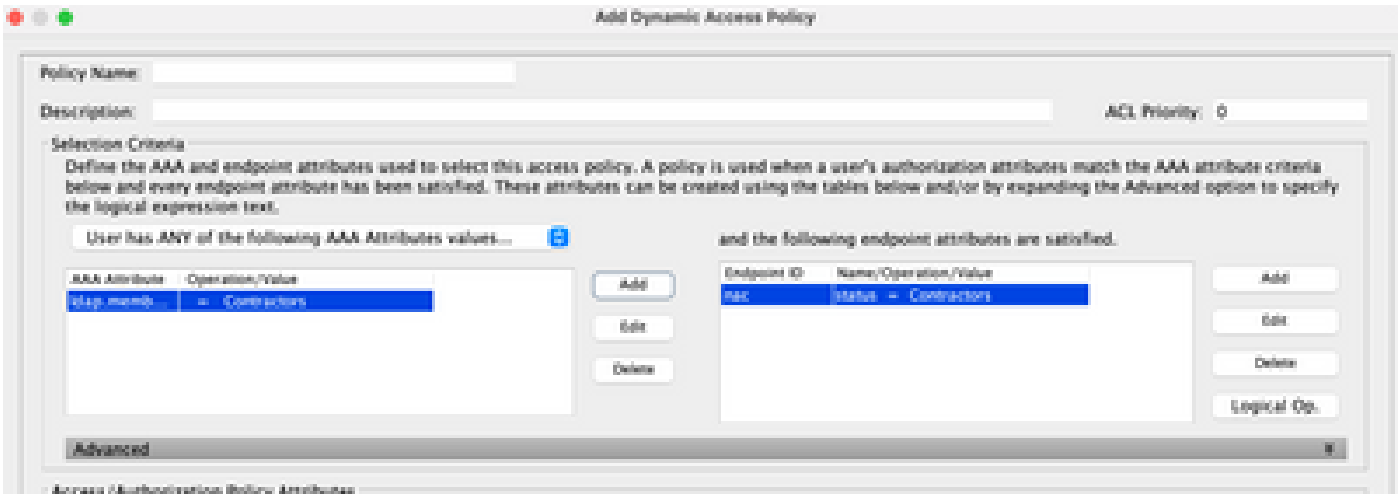


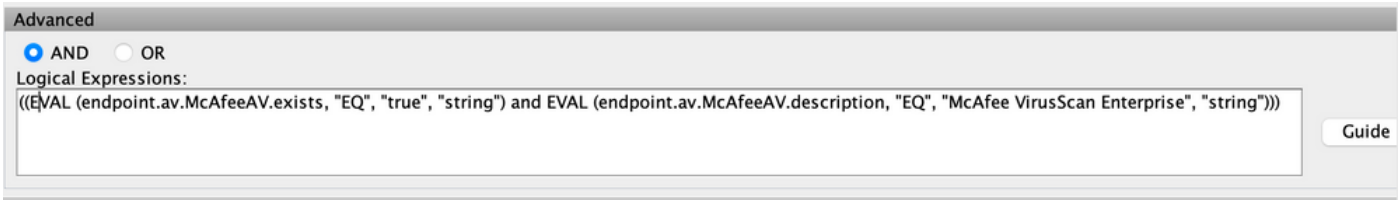

圖6.AAA和端點屬性條件匹配




AAA和終端屬性可以使用圖6中所述的表和/或透過展開Advanced選項以指定如圖7所示的邏輯表達式來建立。目前，邏輯表達式是使用EVAL函式構建的，例如EVAL (endpoint.av.McAfeeAV.exists， "EQ"， "true"， "string")和EVAL (endpoint.av.McAfeeAV.description， "EQ"， "McAfee VirusScan Enterprise"， "string")，這些函式表示AAA和/或終端選擇邏輯操作。

如果您需要增加AAA和終端屬性區域以外的選擇標準（如前所示），邏輯表達式非常有用。例如，雖然您可以將安全裝置配置為使用滿足任意、全部或不滿足任何指定條件的AAA屬性，但終端屬性是累積的，必須滿足全部屬性。要使安全裝置使用一個或另一個終端屬性，您需要在DAP記錄的Advanced部分下建立相應的邏輯表達式。

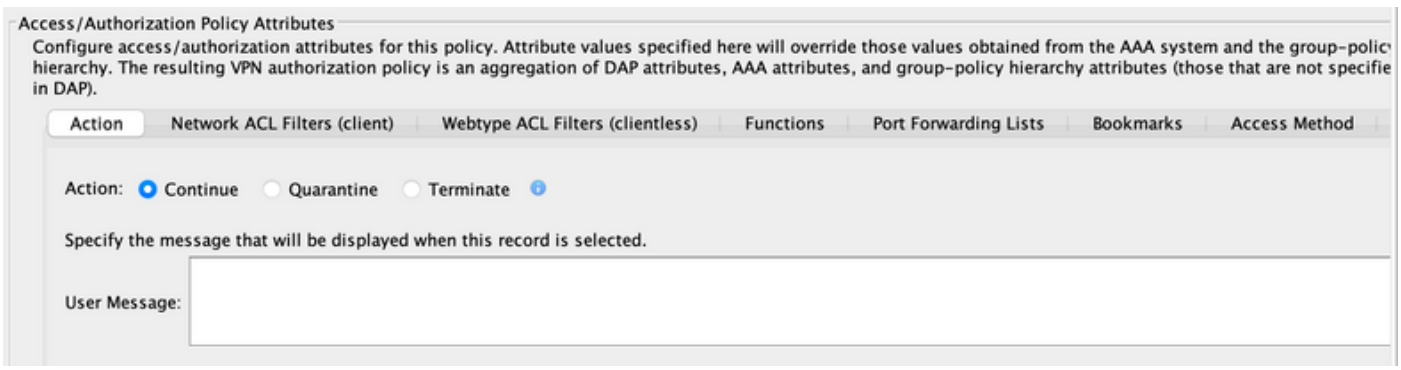
圖7.用於建立進階屬性的邏輯運算式GUI




如圖8所示，訪問策略屬性部分是管理員為特定DAP記錄配置VPN訪問屬性的部分。當使用者授權屬性與AAA、終端和/或邏輯表達式條件匹配時，可以實施此部分中配置的訪問策略屬性值。此處指定的屬性值可以覆蓋從AAA系統獲得的值，包括現有使用者、組、隧道組和預設組記錄中的值。

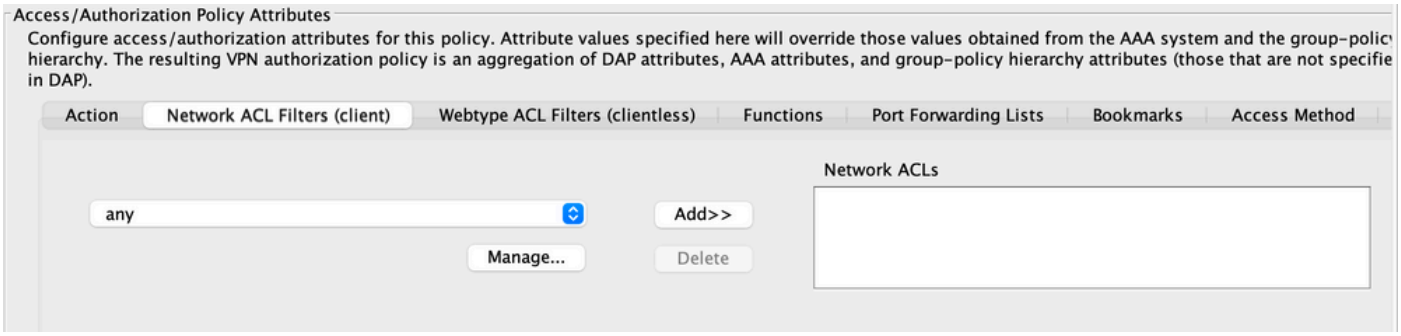
DAP記錄具有一組可配置的有限屬性值。這些值位於圖8至圖14所示的頁籤下：

圖8.動作—指定要套用至特定連線或作業階段的特殊處理。



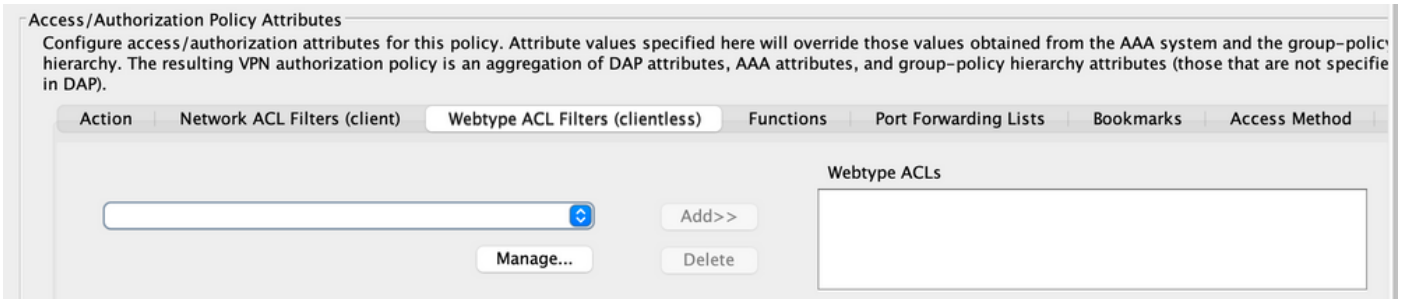
- 繼續(Continue) - （預設）按一下可將訪問策略屬性應用於會話。
- 終止- 按一下終止會話。
- User Message —輸入在選擇此DAP記錄時要顯示在門戶頁上的文本消息。最多128個字元。使用者訊息會顯示為黃色orb。當使用者登入時，它會閃爍三次以吸引注意，然後就靜止。如果選擇了多個DAP記錄，並且每條記錄都有一個使用者消息，則將顯示所有使用者消息。此外，您可以在此類訊息中包含URL或其他內嵌文字，這些內容需要您使用正確的HTML標籤。

圖9.網路ACL過濾器頁籤—用於選擇和配置要應用於此DAP記錄的網路ACL。DAP的ACL可以包含允許或拒絕規則，但不能同時包含兩者。如果ACL同時包含允許和拒絕規則，安全裝置將拒絕ACL配置。




- 網路ACL下拉選單框中已配置要增加到此DAP記錄的網路ACL。只有具有所有permit或deny規則的ACL才符合條件，並且只有此處顯示的ACL符合條件。
- Manage —按一下以增加、編輯和刪除網路ACL。
- 網路ACL列出此DAP記錄的網路ACL。
- Add - 點選將下拉框中的所選網路ACL增加到右側的網路ACL清單中。
- Delete — 按一下以從網路ACL清單中刪除突出顯示的網路ACL。如果ACL已分配給DAP或其他記錄，則不能將其刪除。

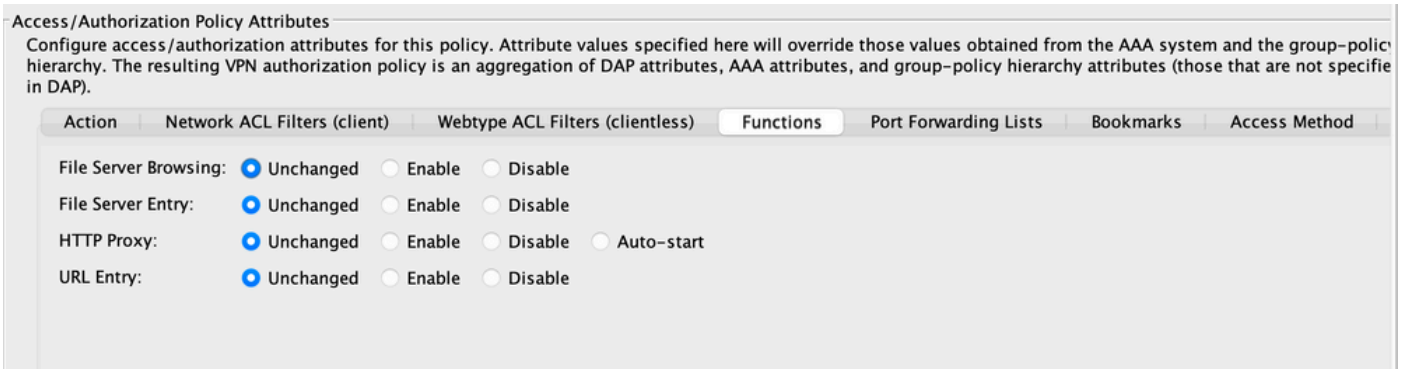
圖10.Web-Type ACL Filters頁籤—用於選擇和配置要應用於此DAP記錄的Web-type ACL。DAP的ACL只能包含允許或拒絕規則。如果ACL同時包含允許和拒絕規則，安全裝置將拒絕ACL配置。




- Web-Type ACL下拉框 —選擇已配置的Web-type ACL以增加到此DAP記錄。只有具有所有允許或所有拒絕規則的ACL才符合條件，並且此處僅顯示這些ACL。
- 管理…… —按一下可增加、編輯和刪除Web型別ACL。

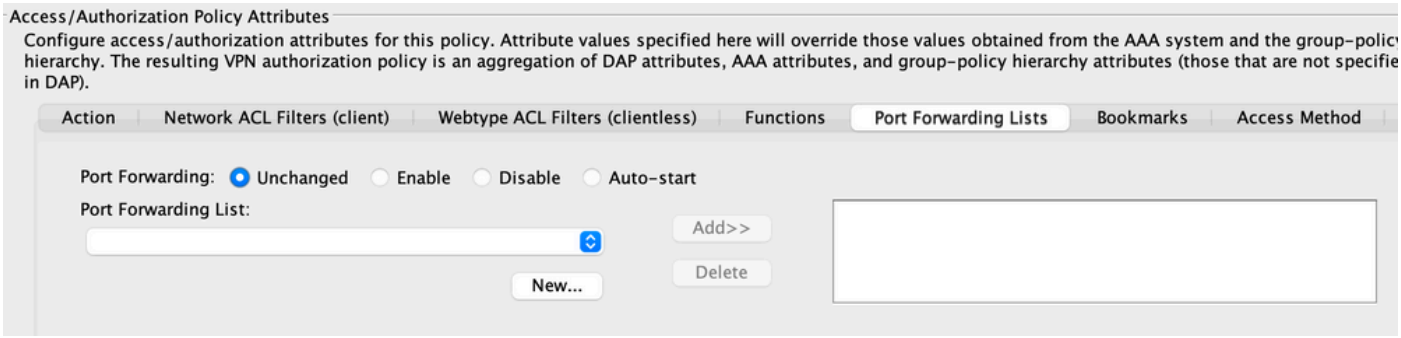
- Web-Type ACL list —顯示此DAP記錄的Web型別ACL。
- Add -點選以將下拉框中選擇的Web型別ACL增加到右側的Web型別ACL清單中。
- Delete -點選以從Web型別ACL清單中刪除Web型別ACL。如果ACL已分配給DAP或其他記錄，則不能將其刪除。

圖11.功能標籤—可讓您設定DAP記錄的檔案伺服器專案與瀏覽、HTTP代理和URL專案。



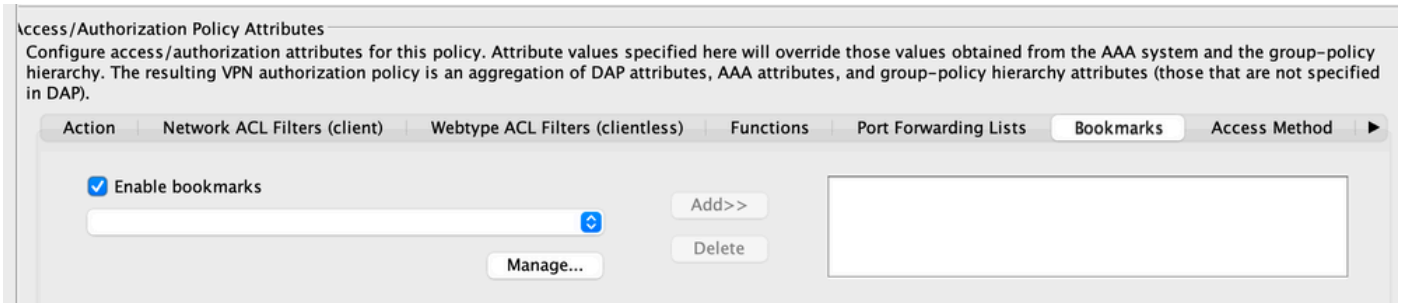

- File Server Browsing -啟用或停用檔案伺服器或共用功能的CIFS瀏覽。
- File Server Entry -允許或拒絕使用者在門戶頁上輸入檔案伺服器路徑和名稱。啟用時，將檔案伺服器專案抽屜放在入口頁面上。使用者可以直接輸入Windows檔案的路徑名稱。他們可以下載、編輯、刪除、重新命名和移動檔案。他們還可以增加檔案和資料夾。還必須配置共用，以便使用者在適用的Microsoft Windows伺服器上進行訪問。使用者在存取檔案前可能需要進行驗證，視網路需求而定。
- HTTP Proxy -影響HTTP applet Proxy向客戶端的轉發。代理對於干擾正確內容轉換的技術（如Java、ActiveX和Flash）非常有用。它繞過修剪/重寫過程，同時確保安全裝置的持續使用。轉發的代理會自動修改瀏覽器的舊代理配置，並將所有HTTP和HTTPS請求重定向到新的代理配置。它支援幾乎所有客戶端技術，包括HTML、CSS、JavaScript、VBScript、ActiveX和Java。它支援的唯一瀏覽器是Microsoft Internet Explorer。
- URL Entry -允許或阻止使用者在門戶頁面上輸入HTTP/HTTPS URL。如果啟用此功能，則使用者可以在URL條目框中輸入Web地址，並使用無客戶端SSL VPN訪問這些網站。
- Unchanged -（預設）按一下以使用套用至此階段作業的群組原則值。
- Enable/Disable -按一下以啟用或停用特徵。
- Auto-start -按一下以啟用HTTP代理，並使DAP記錄自動啟動與這些功能相關聯的Applet。

圖 12.Port Forwarding Lists頁籤—用於為使用者會話選擇和配置埠轉發清單。



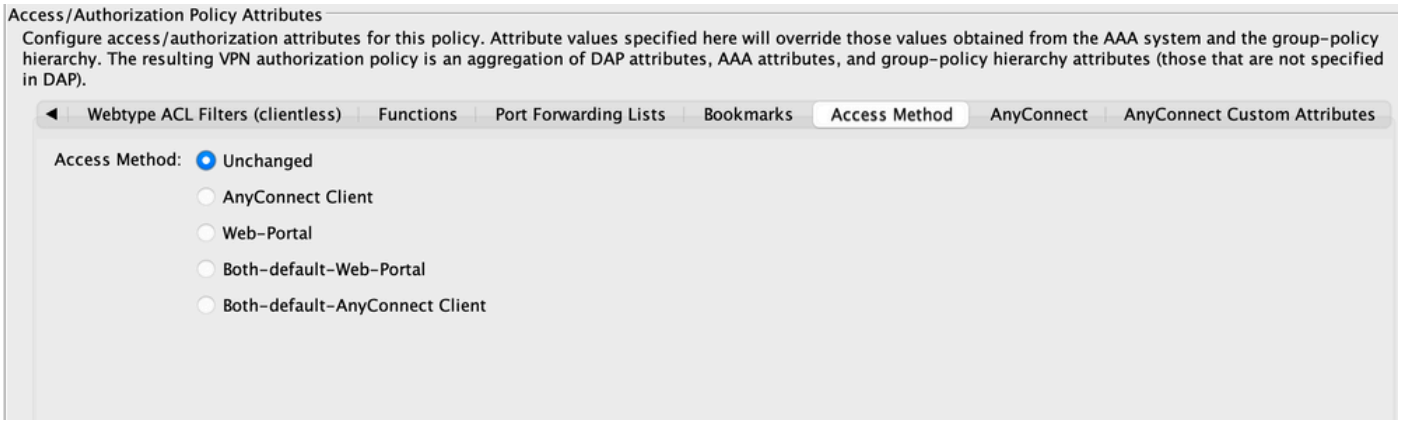

- Port Forwarding -為應用於此DAP記錄的埠轉發清單選擇一個選項。此欄位中的其他屬性僅在將Port Forwarding設定為Enable或Auto-start時啟用。
- 未變更—按一下以使用套用至此階段作業的群組原則值。
- Enable/Disable -點選以啟用或停用埠轉發。
- Auto-start -點選以啟用埠轉發，並使DAP記錄自動啟動與其埠轉發清單關聯的埠轉發applet。
- Port Forwarding List下拉框-選擇已配置的埠轉發清單以增加到DAP記錄。
- New -點選以配置新的埠轉發清單。
- Port Forwarding Lists -顯示DAP記錄的埠轉發清單。
- Add -點選以將下拉框中的所選埠轉發清單增加到右側的Port Forwarding清單。
- Delete -點選以從Port Forwarding清單中刪除所選埠轉發清單。如果ACL已分配給DAP或其他記錄，則不能將其刪除。

圖 13.書籤標籤—可讓您選取和設定使用者工作階段的書籤/URL清單。




- 啟用書籤—按一下以啟用。如果未選取此方塊，連線的入口頁面上不會顯示書籤清單
- 管理—按一下以新增、匯入、匯出及刪除「書籤」清單。
- 書籤清單(Bookmarks Lists)（下拉選單）-顯示DAP記錄的書籤清單。
- 新增—按一下以將下拉式方塊中的所選書籤清單新增至右邊的書籤清單方塊。
- 已刪除-按一下以從書籤清單方塊中刪除所選書籤清單。您不能從安全裝置中刪除書籤清單，除非您首先從DAP記錄中刪除該書籤清單。

圖14.[Method]標籤—可讓您設定允許的遠端存取型別。




- Unchanged -繼續會話組策略中設定的當前遠端訪問方法。
- AnyConnect Client -使用Cisco AnyConnect VPN客戶端連線。
- Web Portal -使用無客戶端VPN連線。
- Both-default-Web-Portal -透過無客戶端或AnyConnect客戶端進行連線，預設情況下為無客戶端。
- Both-default-AnyConnect Client -透過無客戶端或AnyConnect客戶端進行連線，預設值為AnyConnect。

如前所述，DAP記錄具有一組有限的預設屬性值，只有在修改後，這些值的優先順序才會高於當前AAA、使用者、組、隧道組和預設組記錄。如果需要在DAP範圍之外的其他屬性值，例如，分割隧道清單、標語、智慧隧道、門戶自定義等，則需要透過AAA、使用者、組、隧道組和預設組記錄來實施這些值。在這種情況下，這些特定屬性值可以補充DAP，並且不能被覆蓋。因此，使用者會取得所有記錄的屬性值累積集。

# 聚合多個動態訪問策略

管理員可以配置多個DAP記錄以解決許多變數問題。因此，身份驗證使用者可以滿足多個DAP記錄的AAA和終端屬性條件。因此，訪問策略屬性在這些策略中可能一致或衝突。在這種情況下，授權使用者可以獲得所有匹配DAP記錄的累計結果。

這還包括透過身份驗證、授權、使用者、組、隧道組和預設組記錄實施的唯一屬性值。訪問策略屬性的累積結果將建立動態訪問策略。下表列出了組合訪問策略屬性的示例。這些示例描述了3個組合DAP記錄的結果。

表1中顯示的操作屬性的值為「終止」或「繼續」。如果在任何選定的DAP記錄中配置了Terminate值，則聚合屬性值為Terminate；如果在所有選定的DAP記錄中配置了Continue值，則聚合屬性值為Continue。

表 1.動作屬性

| 屬性名稱 | DAP#1 | DAP#2 | DAP#3 | DAP |
|---|---|---|---|---|
| 動作（範例1） | 繼續 | 繼續 | 繼續 | 繼續 |

| | | | | |
|---|---|---|---|---|
| 動作（範例2） | 終止 | 繼續 | 繼續 | 終止 |

表2中顯示的user-message屬性包含一個字串值。聚合屬性值可以是行進式（十六進位制值0x0A）分隔的字串，該字串透過將選定DAP記錄的屬性值連結在一起而建立。組合字串中屬性值的順序無關緊要。

表2.User-Message屬性

| 屬性名稱 | DAP#1 | DAP#2 | DAP#3 | DAP |
|---|---|---|---|---|
| user-message | 快速 | 褐狐狸 | 跳過 | 快速狐狸<LF>跳過 |

表3中所示的無客戶端啟用屬性（功能）的功能包含Auto-start、Enable或Disable值。如果在任何選定的DAP記錄中配置了Auto-Start值，則聚合屬性值可以是Auto-start。

如果在任何所選DAP記錄中沒有配置自動啟動值，並且在至少一個所選DAP記錄中配置了Enable值，則可以啟用聚合屬性值。

如果在任何所選DAP記錄中未配置Auto-start或Enable值，並且至少在一個所選DAP記錄中配置了「disable」值，則可以停用聚合屬性值。

表3.無客戶端功能啟用屬性（功能）

| 屬性名稱 | DAP#1 | DAP#2 | DAP#3 | DAP |
|---|---|---|---|---|
| port-forward | 啟用 | 停用 | | 啟用 |
| 檔案瀏覽 | 停用 | 啟用 | 停用 | 啟用 |
| file-entry | | | 停用 | 停用 |
| HTTP代理 | 停用 | 自動啟動 | 停用 | 自動啟動 |
| URL條目 | 停用 | | 啟用 | 啟用 |

表4中顯示的URL list和port-forward屬性包含一個值，該值可以是字串或者逗號分隔字串。聚合屬性值可以是當您從所選DAP記錄中將屬性值連結在一起時所建立的逗號分隔字串。可以移除組合字串中的任何重複屬性值。屬性值在組合字串中的排序方式並不重要。

表4.URL清單和埠轉發清單屬性

| 屬性名稱 | DAP#1 | DAP#3 | DAP#3 | DAP |
|---|---|---|---|---|
| url-list | 答 | b，c | 答 | a、b、c |
| port-forward | | d，e | e，f | d、e、f |

Access Method屬性指定SSL VPN連線允許的客戶端訪問方法。客戶端訪問方法可以是僅AnyConnect客戶端訪問、僅Web門戶訪問、將Web門戶訪問用作預設訪問的AnyConnect客戶端或Web門戶訪問，或將AnyConnect客戶端訪問用作預設訪問的AnyConnect客戶端或Web門戶訪問。彙總的屬性值彙總於表5。

表5.存取方法屬性

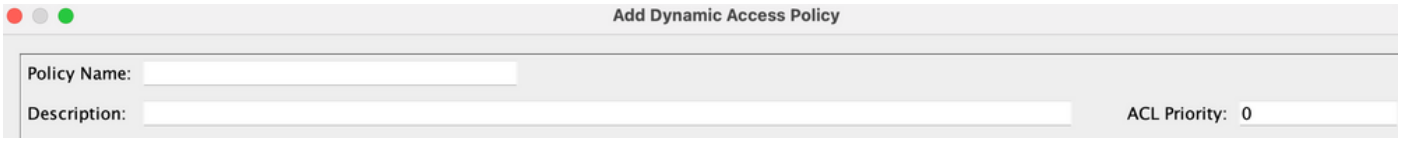
| 選取的屬性值 | 彙總結果 |
|---|---|

| AnyConnect客戶端 | Web門戶 | Both-default-Web-門戶 | Both-default-AnyConnect客戶端 | |
|---|---|---|---|---|
| | | | X | Both-default-AnyConnect客戶端 |
| | | X | | Both-default-Web-Portal |
| | | X | X | Both-default-Web-Portal |
| | X | | | Web門戶 |
| | X | | X | Both-default-AnyConnect客戶端 |
| | X | X | | Both-default-Web-Portal |
| | X | X | X | Both-default-Web-Portal |
| X | | | | AnyConnect客戶端 |
| X | | | X | Both-default-AnyConnect客戶端 |
| X | | X | | Both-default-Web-Portal |
| X | | X | X | Both-default-Web-Portal |
| X | X | | | Both-default-Web-Portal |
| X | X | | X | Both-default-AnyConnect客戶端 |
| X | X | X | | Both-default-Web-Portal |
| X | X | X | X | Both-default-Web-Portal |

如果結合使用網路（防火牆）和Web型別（無客戶端）ACL過濾器屬性，DAP優先順序和DAP ACL是需要考慮的兩個主要元件。

圖15所示的Priority屬性未經聚合。在從多個DAP記錄聚合網路和Web型別ACL時，安全裝置將使用此值對訪問清單進行邏輯排序。安全裝置從優先順序最高到最低對記錄進行排序，優先順序最低在表底部。例如，值為4的DAP記錄的優先順序高於值為2的記錄。您無法手動將它們排序。

圖15.優先順序-顯示DAP記錄的優先順序。

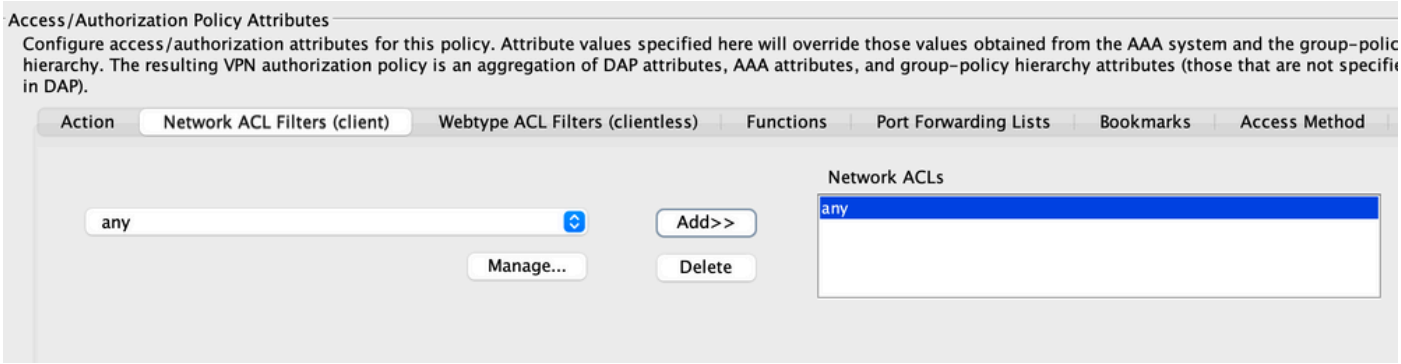



- Policy Name -顯示DAP記錄的名稱。
- 說明-說明DAP記錄的用途。

DAP ACL屬性僅支援符合嚴格Allow-List或嚴格Block-List ACL模型的訪問清單。在Allow-List ACL模型中，訪問清單條目指定規則「允許」對指定網路或主機的訪問。在阻止清單 ACL模式下，訪問清單條目會指定規則，以便拒絕對指定網路或主機的訪問。不合格訪問清單包含混合了permit和deny規則的訪問清單條目。如果為DAP記錄配置了不符合條件的訪問清單，則當管理員嘗試增加記錄時，該訪問清單可能會因配置錯誤而被拒絕。如果符合條件的訪問清單被分配給DAP記

錄，則對訪問清單所做的任何更改都會因配置錯誤而被拒絕。

圖16.DAP ACL -用於選擇和配置網路ACL以應用於此DAP記錄。




當選擇多個DAP記錄時，網路（防火牆）ACL中指定的訪問清單屬性將被聚合以建立DAP防火牆ACL的動態訪問清單。同樣，Web型別（無客戶端）ACL中指定的訪問清單屬性將被聚合以建立DAP無客戶端ACL的動態訪問清單。下一個示例重點介紹如何專門建立動態DAP防火牆訪問清單。但是，動態DAP無客戶端訪問清單也可以執行相同的過程。

首先，ASA會為DAP Network-ACL 動態建立唯一名稱，如表6所示。

表6.動態DAP網路ACL名稱

| DAP網路ACL名稱 |
| --- |
| DAP-Network-ACL-X（其中X是一個整數，可以遞增以確保唯一性） |

第二，ASA從所選DAP記錄中檢索Network-ACL屬性，如表7所示。

表7.網路ACL

| 選取的DAP記錄 | 優先順序機制 | 網路ACL | 網路ACL條目 |
| --- | --- | --- | --- |
| DAP 1 | 1 | 101和102 | ACL 101有4條拒絕規則，ACL 102有4條允許規則 |
| DAP 2 | 2 | 201和202 | ACL 201有3條允許規則，ACL 202有3條拒絕規則 |
| DAP 3 | 2 | 101和102 | ACL 101有4條拒絕規則，ACL 102有4條允許規則 |

第三，如果2條或更多所選DAP記錄的優先順序值相同，則ASA會首先透過DAP記錄優先順序編號對網路-ACL進行重新排序，然後透過Block-List進行重新排序。之後，ASA可以從每個網路ACL中檢索網路ACL條目，如表8所示。

表8.DAP記錄優先順序

| 網路ACL | 優先順序機制 | 白/黑存取清單模型 | 網路ACL條目 |
| --- | --- | --- | --- |
| 101 | 2 | 黑名單 | 4拒絕規則(DDDD) |
| 202 | 2 | 黑名單 | 3拒絕規則(DDD) |
| 102 | 2 | 白名單 | 4允許規則(PPPP) |
| 202 | 2 | 白名單 | 3允許規則(PPP) |

| | | | |
|---|---|---|---|
| 101 | 1 | 黑名單 | 4拒絕規則(DDDD) |
| 102 | 1 | 白名單 | 4允許規則(PPPP) |

最後，ASA會將網路-ACL條目合併到動態生成的網路-ACL中，然後返回動態網路-ACL的名稱作為要實施的新網路-ACL，如表9所示。

表9.動態DAP網路ACL

| DAP網路ACL名稱 | 網路ACL條目 |
|---|---|
| DAP-Network-ACL-1 | DDDD DDD PPPP PPP DDDD PPP |

# DAP實施

有許多原因促使管理員必須考慮實施DAP。一些根本原因是在終端上實施狀態評估和/或在授權使用者訪問網路資源時考慮更精細的AAA或策略屬性時。在下一個示例中，您可以配置DAP及其元件以標識連線終端並授權使用者訪問各種網路資源。

測試案例-客戶端請求了具有以下VPN訪問要求的概念驗證：

- 檢測員工終端並將其標識為「託管」或「非託管」的能力。— 如果終端被辨識為受管（工作PC）但無法滿足安全評估要求，則必須拒絕該終端訪問。另一方面，如果員工的終端標識為非託管（家庭PC），則必須向該終端授予無客戶端訪問許可權。
- 無客戶端連線終止時呼叫會話cookie和快取清理的功能。
- 在受管理的員工終端（如McAfee AntiVirus）上檢測並強制執行正在運行的應用程式的能力。如果應用不存在，則必須拒絕該終端訪問。
- 能夠使用AAA身份驗證確定授權使用者必須訪問的網路資源。安全裝置必須支援本地MS LDAP身份驗證並支援多個LDAP組成員角色。
- 透過使用者端/網路連線時，允許本機LAN存取網路資源，例如網路傳真與印表機。
- 為承包商提供授權訪客訪問許可權的能力。承包商及其終端必須獲得無客戶端訪問，而且與員工訪問相比，他們對應用程式的門戶訪問必須受到限制。

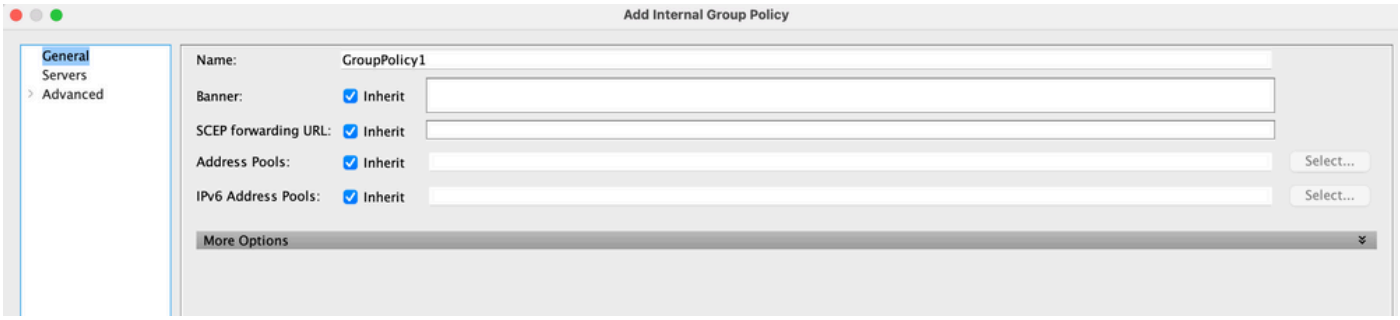
在本示例中，您可以執行一系列配置步驟以滿足客戶端的VPN訪問要求。可能有必要的配置步驟，但不直接與DAP相關，而其他配置則直接與DAP相關。ASA非常動態，能夠適應許多網路環境。因此，VPN解決方案可以透過多種方式定義，並且在某些情況下提供相同的終端解決方案。但是，所採用的方法是由客戶需求及其環境所驅動的。

根據本文的性質和定義的客戶端要求，您可以使用自適應安全裝置管理器(ASDM)，並將大多數配置集中在DAP上。但是，您也可以配置本地組策略，以顯示DAP如何補充和/或覆蓋本地策略屬性。在此測試案例的基礎上，您可以假設LDAP伺服器組、分割隧道網路清單和基本IP連線（包括IP池和DefaultDNS伺服器組）已預先配置。

定義組策略-此配置對於定義本地策略屬性是必需的。此處定義的某些屬性在DAP中不可配置（例如，本地LAN訪問）。（此策略也可用於定義無客戶端屬性和基於客戶端的屬性）。

導航到Configuration > Remote Access VPN > Network (Client) Access > Group Policies，然後增加一個內部組策略，如下所示：

圖17.組策略-定義本地VPN特定屬性。




a. 在General連結下，為組策略配置nameSSLVPN_GP。

b. 還是在General連結下，按一下More選項並僅配置Tunneling Protocol：Clientless SSLVPN。（您可以配置DAP以覆蓋和管理訪問方法。）

c. 在Advanced > Split Tunneling連結下，配置以下步驟：

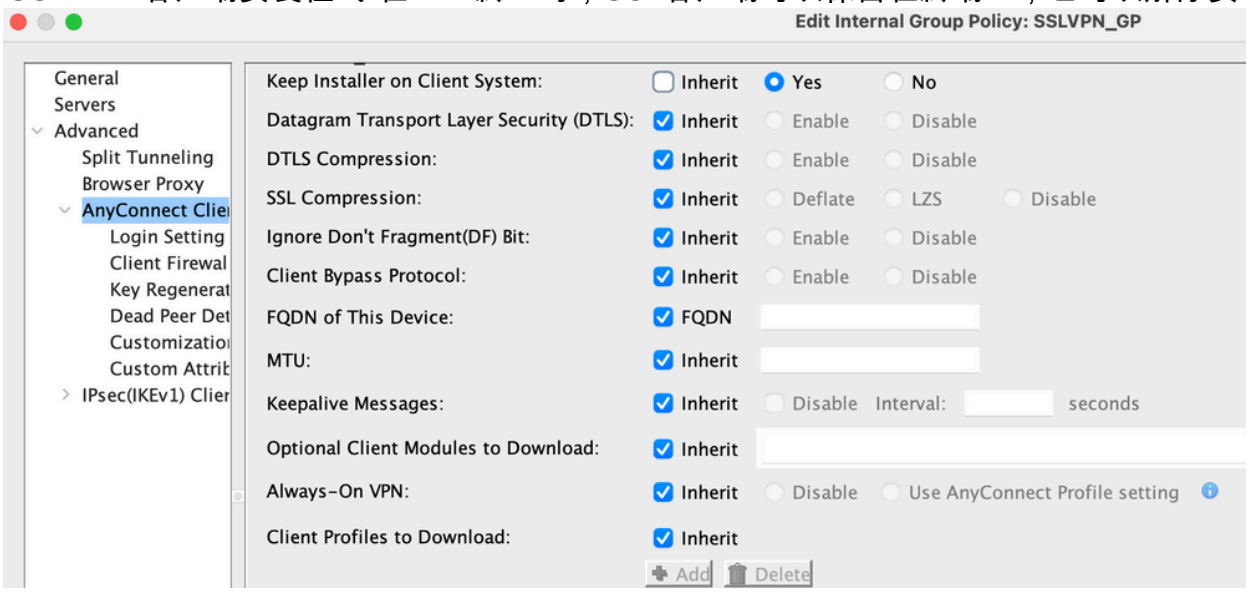
圖18.Split Tunneling -允許指定的流量（本地網路）在客戶端連線期間繞過未加密的隧道。

a. 策略：取消選中Inheritand selectExclude Network List。

b. 網路清單：取消核取繼承，然後選取清單nameLocal_Lan_Access。（假設已預配置。）

d. 在高級> ANYCONNECT客戶端連結下，配置以下這些後續步驟：

圖19.SSL VPN客戶端安裝程式-在VPN終止時，SSL客戶端可以保留在終端上，也可以解除安裝。




e. 保留客戶端系統上的安裝程式：取消選中Inheritand，然後選擇Yes。

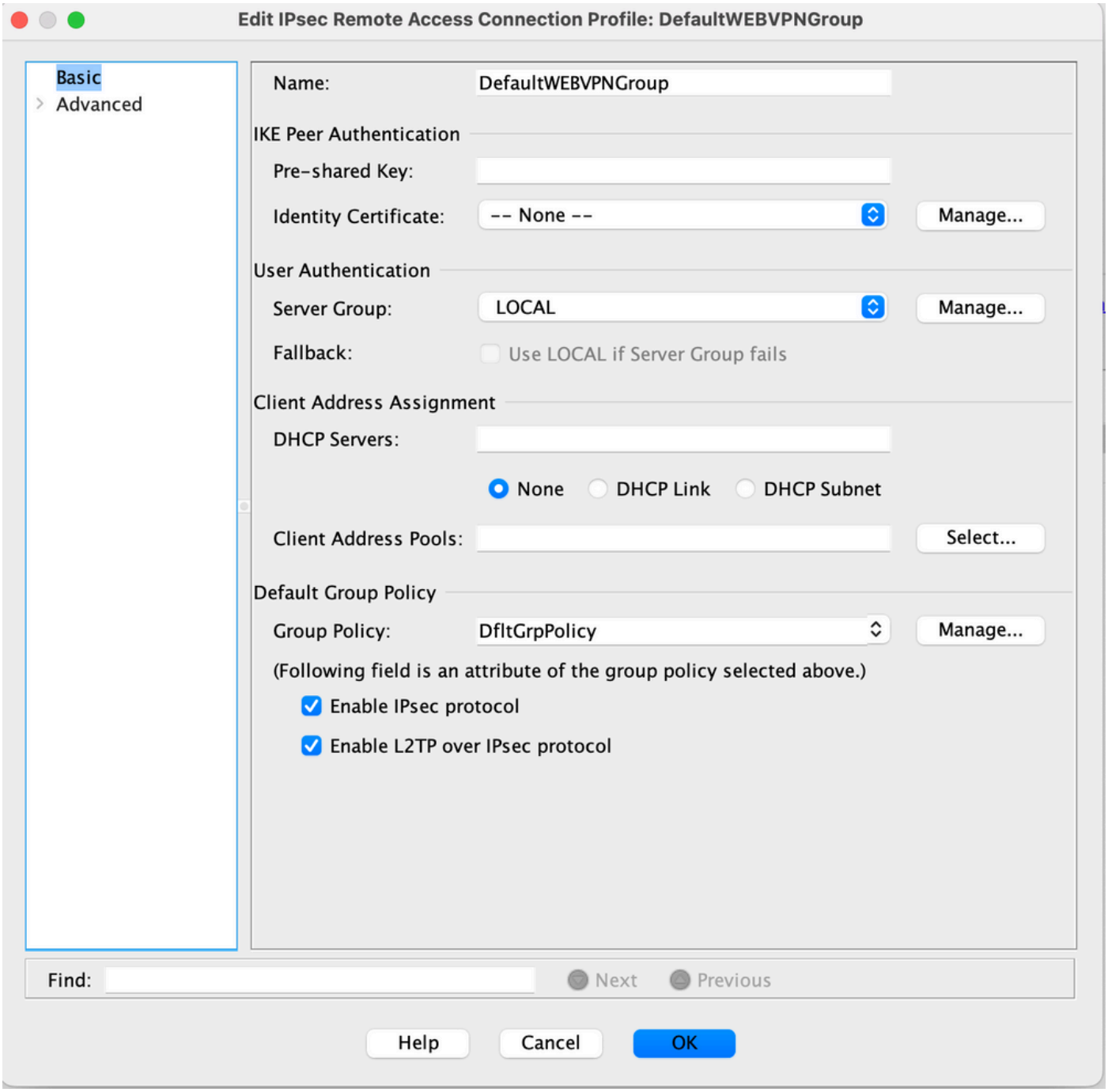
f. 按一下「確定」「應用」。

g. 應用您的配置更改。

Defining a Connection Profile -此配置對於定義AAA身份驗證方法（例如LDAP）以及將先前配置的組策略(SSLVPN_GP)應用於此連線配置檔案是必需的。透過此連線配置檔案進行連線的使用者可使用此處定義的屬性以及SSLVPN_GP組策略中定義的屬性。（此配置檔案還可用於定義無客戶端屬性和基於客戶端的屬性）。

導航到Configuration > Remote Access VPN > Network (Client) Access > IPsec Remote Access Connection Profile，然後配置：

圖20.連線配置檔案-定義本地VPN特定屬性。




a. 在Connection Profiles部分下，編輯DefaultWEBVPNGroup，並在Basic連結下配置以下步驟：

a. 身份驗證—方法：AAA

b. Authentication - AAA Server Group：LDAP（假定已預配置）

c. Client Address Assignment—客戶端地址池：IP_Pool（假設已預配置）

d. 預設組策略-組策略：SelectSSLVPN_GP

b. 應用您的配置更改。

為SSL VPN連線定義IP介面— 在指定介面上終止客戶端和無客戶端SSL連線需要此配置。

在介面上啟用客戶端/網路訪問之前，必須先定義SSL VPN客戶端映像。

1. 導航到Configuration > Remote Access VPN > Network (Client)Access > Anyconnect Client Software，然後從ASA快閃記憶體檔案系統中增加下一個映像（SSL VPN客戶端映像）：(此映像可以從CCO，https://www.cisco.com下載)

   圖21.SSL VPN Client Image Install -定義要推送到連線終端的AnyConnect客戶端映像。 

   a. anyconnect-mac-4.x.xxx-k9.pkg

   b. 按一下「確定」、「確定」，然後按一下「套用」。

2. 導航到Configuration > Remote Access VPN > Network (Client)Access > AnyConnect Connection Profiles，然後按照以下步驟啟用此功能：

   圖22.SSL VPN Access Interface -定義用於終止SSL VPN連線的介面。 

   a. 在Access Interface部分下，啟用：在下表中選擇的介面上啟用Cisco AnyConnect VPN客戶端或傳統SSL VPN客戶端訪問。

   b. 還是在Access Interfaces部分下，對外部介面執行checkAllow Accesson。（此配置還可以在外部介面上啟用SSL VPN無客戶端訪問。）

   c. 按一下「應用」。

定義無客戶端訪問的書籤清單（URL清單）-此配置對於定義要在門戶上發佈的基於Web的應用程式是必要的。您可以定義兩個URL清單，一個用於員工，另一個用於承包商。

1. 導航到Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks，點選+ 並配置後續步驟：

   圖23.書籤清單-定義要從Web入口網站發佈和存取的URL。（為員工訪問而定製）。 

   a. 將清單名稱加入書籤：Employees，然後按一下新增。

   b. 書籤標題：公司內部網

   c. URL值： https://company.resource.com

- 

  按一下「確定」，然後再按一下「確定」。

- 

按一下+增加並配置第二個書籤清單（URL清單），如下所示：

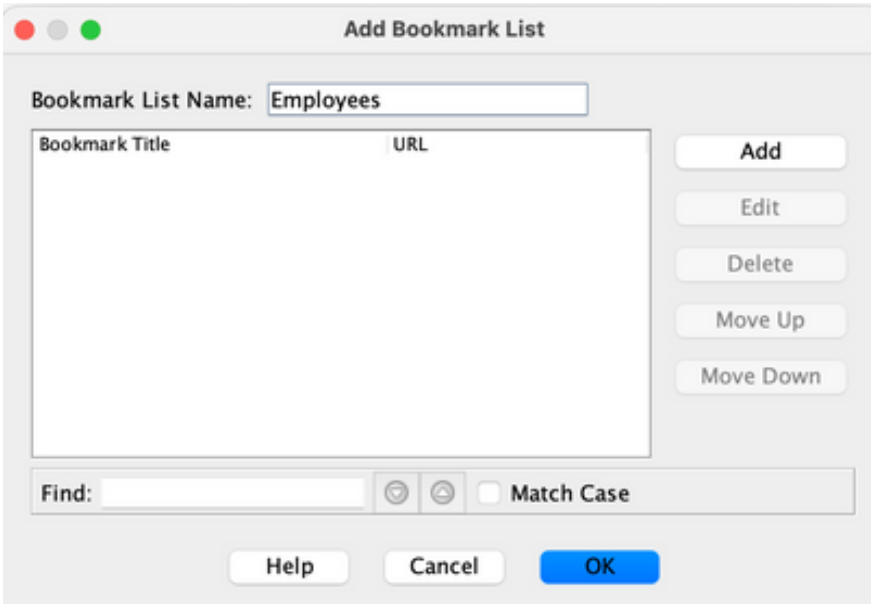



**圖24.Bookmark List —為訪客訪問定製。**

a. 

   書籤清單名稱：**Contractors**，然後**按一下Add**。

b. 

   書籤標題：**訪客訪問**

c. 

   URL值： https://company.contractors.com

- 

  按一下「確定」，然後再按一下「確定」。

- **按一下「應用」。**

配置Hostscan：

- **導航到Configuration > Remote Access VPN > Secure Desktop Manager > HostScan Image**，然後配置下一步：

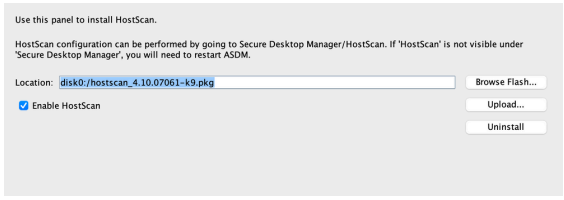



**圖25.HostScan Image Install -定義要推送到連線終端的HostScan映像。**

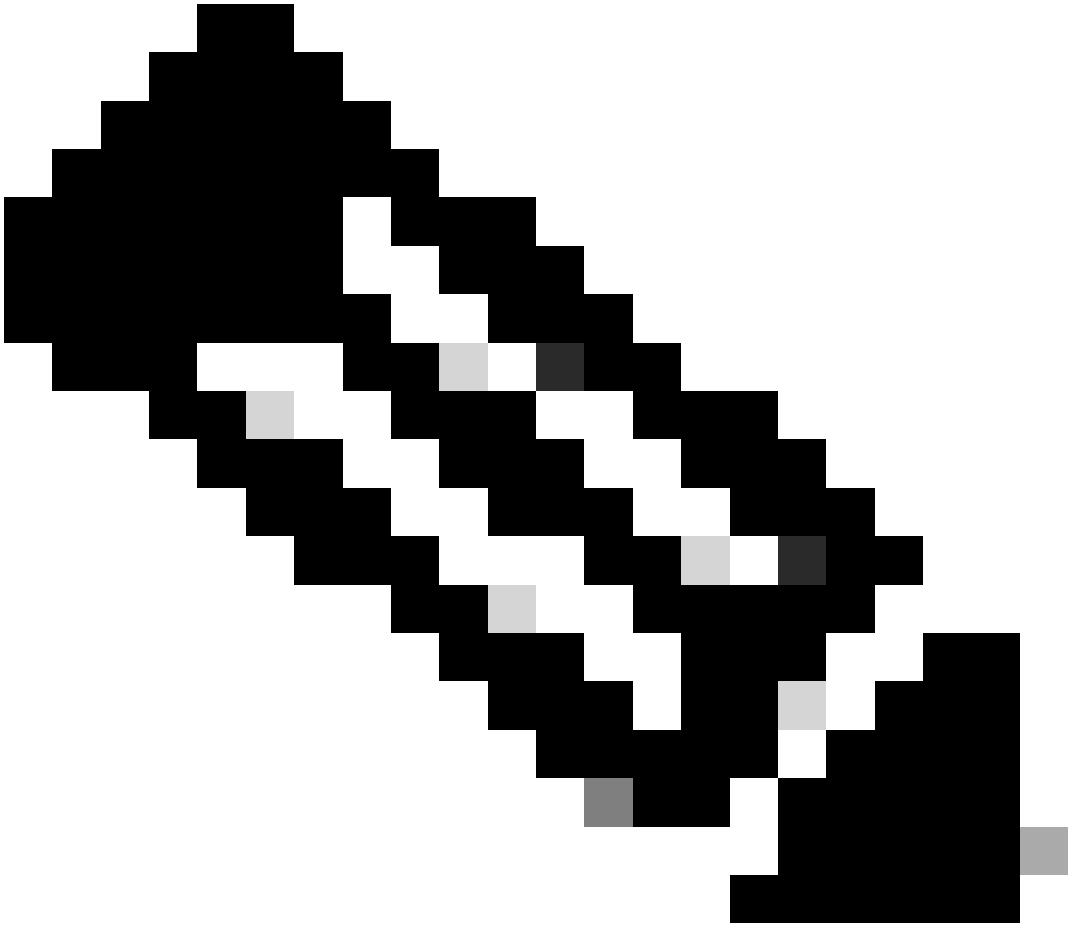
a. 從ASA快閃記憶體檔案系統安裝**disk0：/hostscan_4.xx.xxxxx-k9.**pkgimage。

b. **CheckEnable HostScan。**

c. **按一下「應用」。**

**動態訪問策略** —要根據定義的AAA和/或終端評估標準驗證連線使用者及其端點，此配置必不可少。如果滿足了DAP記錄的已定義標準，則連線使用者就可以被授予訪問與該DAP記錄相關聯的網路資源的許可權。在身份驗證過程中執行DAP授權。

要確保SSL VPN連線可以在預設情況下終止（例如，當終端與任何已配置的動態訪問策略都不匹配時），可以使用以下步驟對其進行配置：



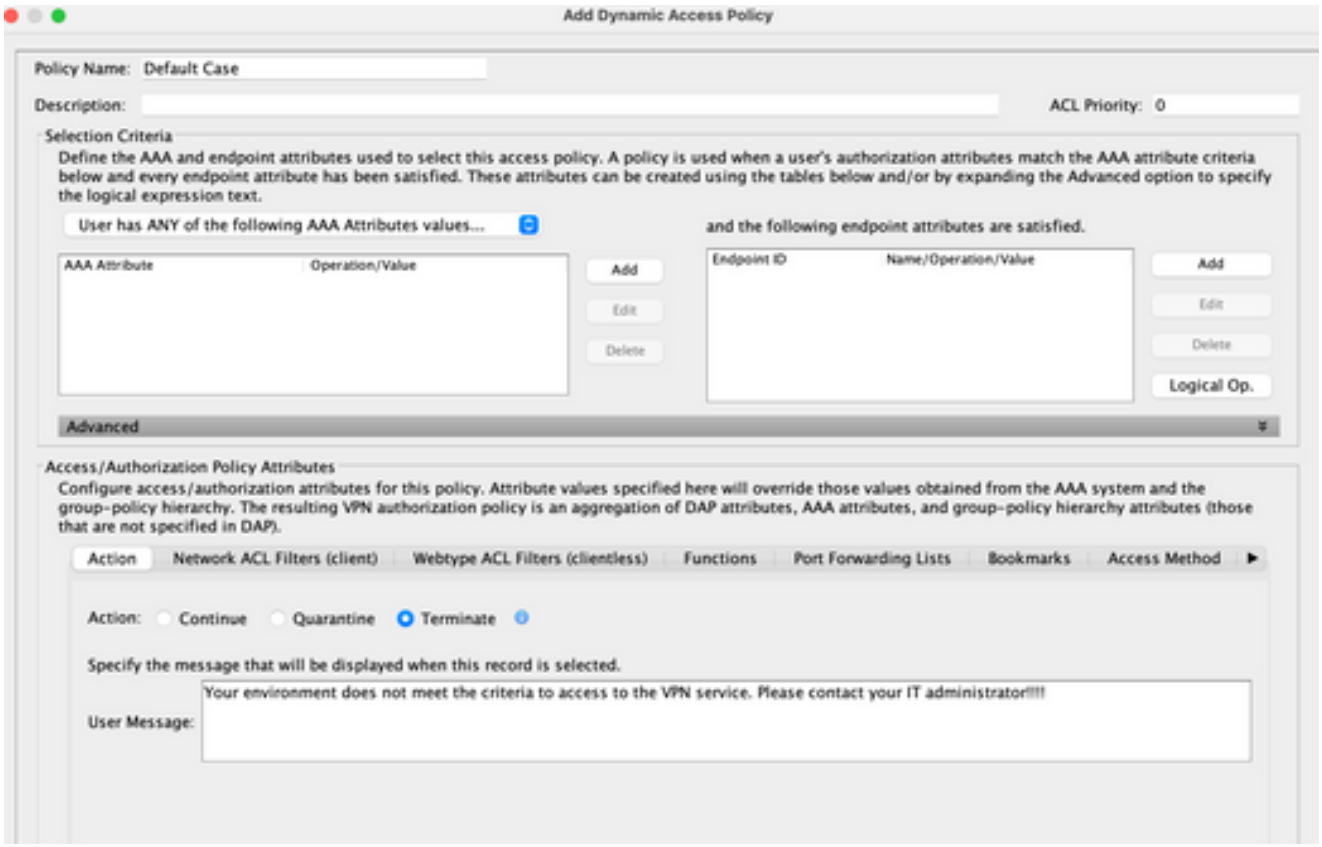
**注意**：首次配置動態訪問策略時，會顯示DAP.xml錯誤消息，指示DAP配置檔案(DAP.XML)不存在。修改您的初始DAP配置並儲存後，此消息將不再出現。

---

- 

導航到**Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies**，然後配置下一步：

**圖30.預設動態訪問策略-如果未匹配任何預定義的DAP記錄，則可以強制執行此DAP記錄。因此，可能會拒絕SSL VPN訪問**。




a.

編輯DfltAccessPolicyand set the Action **toTerminate**。

b.

**按一下「確定」**。

•

增加新的動態訪問策略**namedManaged_Endpoints**，如下所示：

a.

說明：**員工客戶端訪問**

b.

增加終端屬性型別（防病毒），如圖31所示。完成後，按一下「確定」。

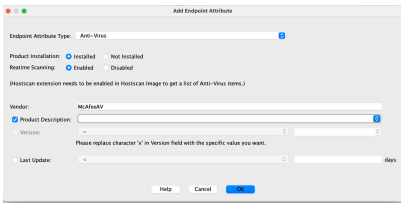



**圖31.DAP終端屬性-高級終端評估防病毒可用作客戶端/網路訪問的DAP標準。**

c.

如上圖所示，從AAA Attribute部分的下拉選單中選擇User has ALL of the following AAA Attributes Values。

•

如圖33和圖34所示，增加（位於AAA Attribute框右側）AAA Attribute Type (LDAP)。完成後，按一下「確定」。

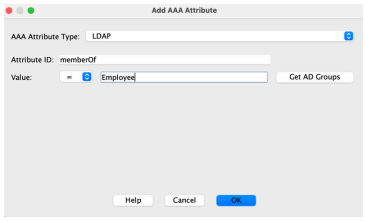



**圖33.DAP AAA Attribute - AAA Group Membership可用作辨識員工的DAP條件。**

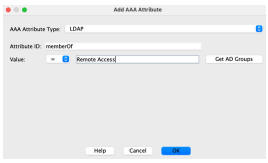



**圖34.DAP AAA Attribute - AAA Group Membership可用作允許遠端訪問功能的DAP條件。**

•

在Action頁籤下，驗證Action是否已設定為**Continue**，如圖35所示。

**圖35.操作頁籤-為特定連線或會話定義特殊處理時需要此配置。如果DAP記錄匹配，且Action設定為Terminate，則可以拒絕VPN訪問。**


•

如圖36所示，在Access Method頁籤下，選擇Access **MethodAnyConnect Client**。

**圖36.Access Method頁籤-此配置對於定義SSL VPN客戶端連線型別是必需的。**

•

**按一下「確定」，然後「套用」。**

- 

增加第二個動態訪問策略**Unmanaged_Endpoints**，如下所示：

a. 

說明：**Employee Clientless Access**。

b. 

從AAA Attribute部分上一映像的下拉選單中選擇User has ALL of the following AAA Attributes Values。

- 

如圖38和圖39所示，增加（位於AAA Attribute Type右側）AAA Attribute Type (LDAP)。完成後，按一下「確定」。

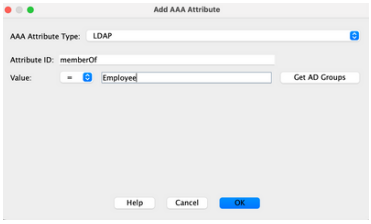



**圖38.DAP AAA Attribute - AAA Group Membership可用作辨識員工的DAP條件。**

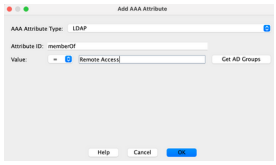



**圖39.DAP AAA Attribute - AAA Group Membership可用作允許遠端訪問功能的DAP條件。**

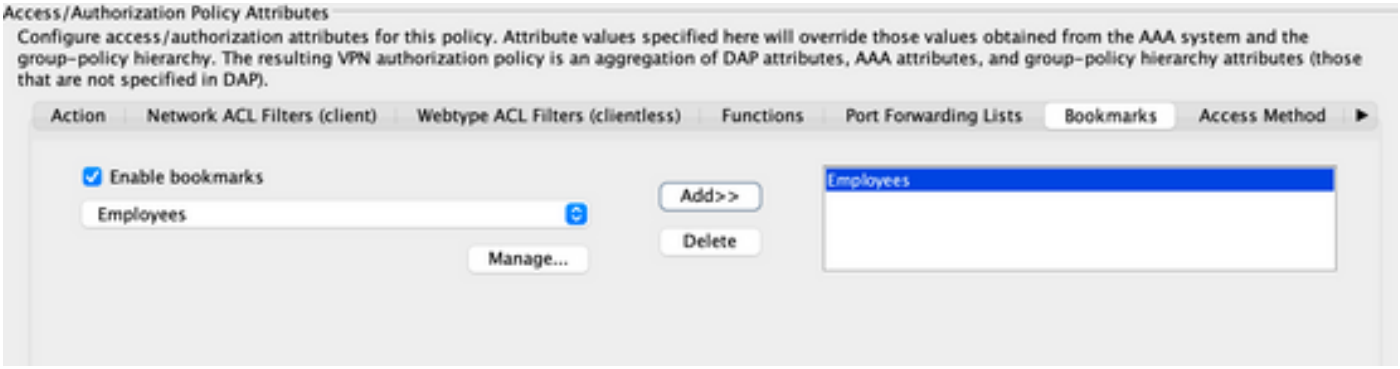
- 

在Action頁籤下，驗證Action是否已設定為**Continue**。（圖35）

- 

在Bookmarks頁籤下，從下拉選單中選擇清單nameEmployees，然後**按一下Add**。此外，請驗證是否已選中Enable書籤（如圖40所示）。

**圖40.「書籤」標籤-可讓您選取和設定使用者階段作業的URL清單。**




- 

  a. 

  在Access Method頁籤下，選擇Access Method **Web Portal**。（圖36）

- **按一下「確定」，然後「套用」。**

1. 承包商只能透過DAP AAA屬性進行標識。因此，無法在步驟4中配置終端屬性型別：（策略）。此方法僅用於顯示DAP中的多樣性。

3. 增加第三個動態訪問策略**namedGuest_Access**，策略如下：

- 

  說明：**Guest Clientless Access**。

- 

  如圖37所示，增加（位於終端屬性框右側）終端屬性型別（策略）。完成後，按一下「確定」。

- 

  在圖40中，從AAA Attribute部分的下拉選單中選擇User has ALL of the following AAA Attributes Values。

-

如圖41和圖42所示，增加（位於AAA Attribute框右側）AAA Attribute Type (LDAP)。完成後，按一下「確定」。

**圖41.您可以使用DAP AAA Attribute - AAA Group Membership作為DAP標準，以標識承包商**

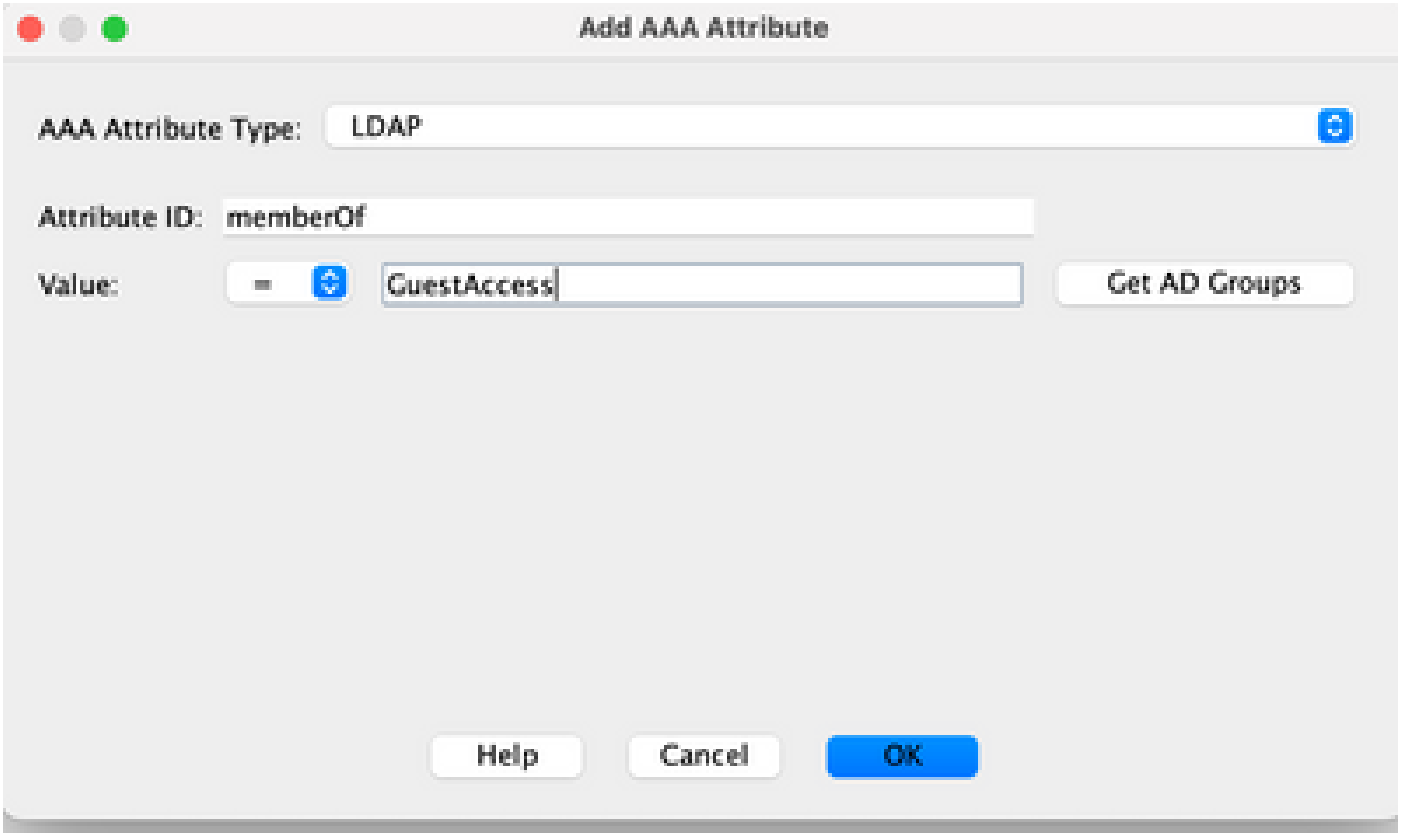
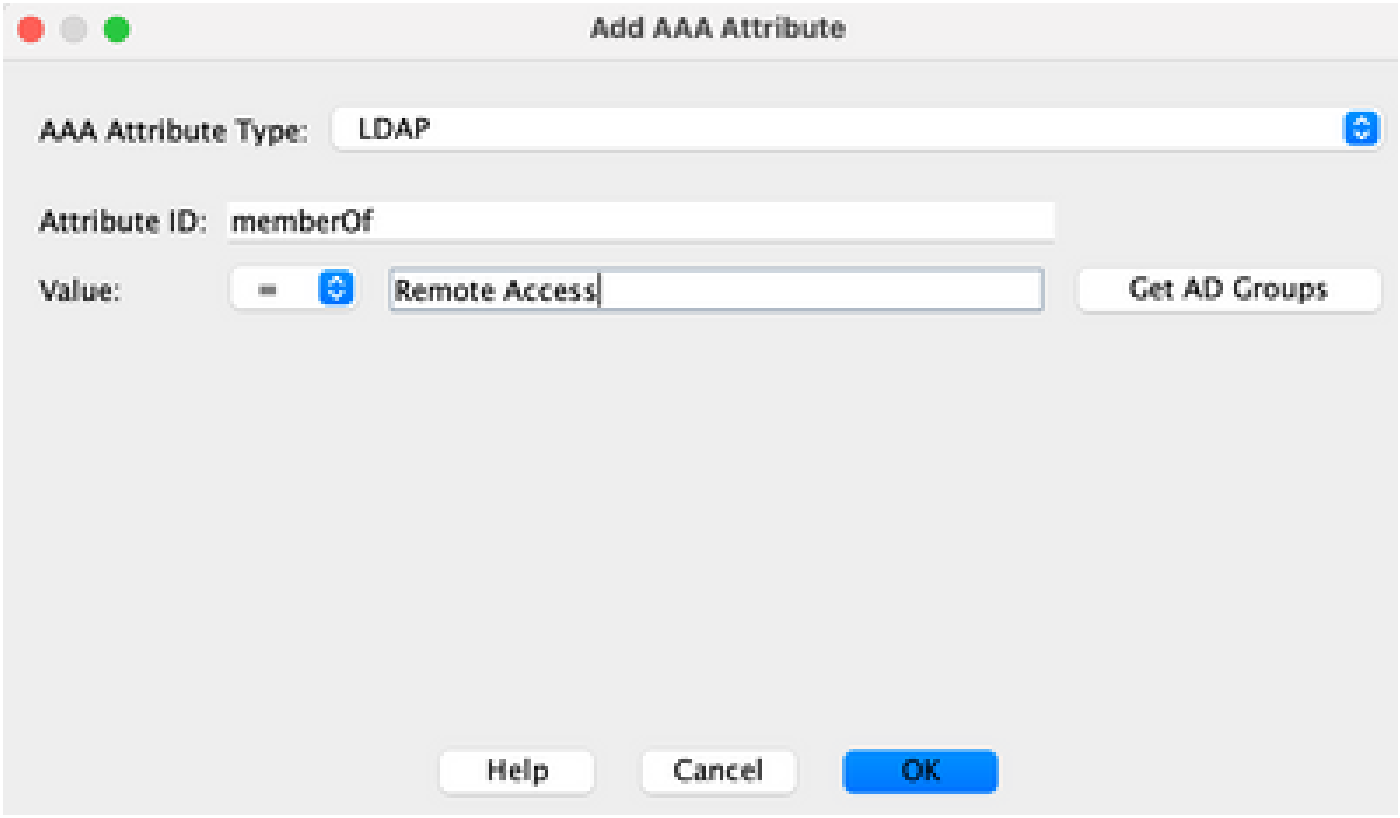



**圖42.DAP AAA Attribute— 您可以使用AAA組成員資格作為DAP條件以允許遠端訪問功能**




- 

a.

在Action頁籤下，驗證Action是否已設定為**Continue**。（圖35）

b.

在「Bookmarks」頁籤下，從下拉選單中選擇清單名**Contractors**，然後按一下「Add」。此外，請驗證是否已選中**Enable bookmarks**。（參見圖40。）

c.

在訪問方法頁籤下，選擇訪問方法Web門戶。 （圖36）

d.

按一下**OK**，然後按一下**Apply**。

## 結論

根據本示例中提到的客戶端遠端訪問SSL VPN要求，此解決方案可滿足客戶端遠端訪問VPN要求。

隨著不斷發展和動態的VPN環境不斷合併，動態訪問策略可以適應頻繁的網際網路配置更改、每個使用者可以在組織內擔任的各種角色，以及從具有不同配置和安全級別的受管和非受管遠端訪問站點進行的登入。

動態訪問策略由經過驗證的新舊技術補充，包括高級終端評估、主機掃描、安全案頭、AAA和本地訪問策略。因此，組織可以放心地從任何位置對任何網路資源進行安全的VPN訪問。

## 相關資訊

- **思科技術支援與下載**

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。