部署ASA 9.X動態訪問策略(DAP)

目錄

簡介

必要條件

- 需求
- 採用元件

背景資訊

DAP和AAA屬性

DAP和終端安全屬性

預設動態訪問策略

配置動態訪問策略

聚合多個動態訪問策略

DAP實現

結論

相關資訊

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。

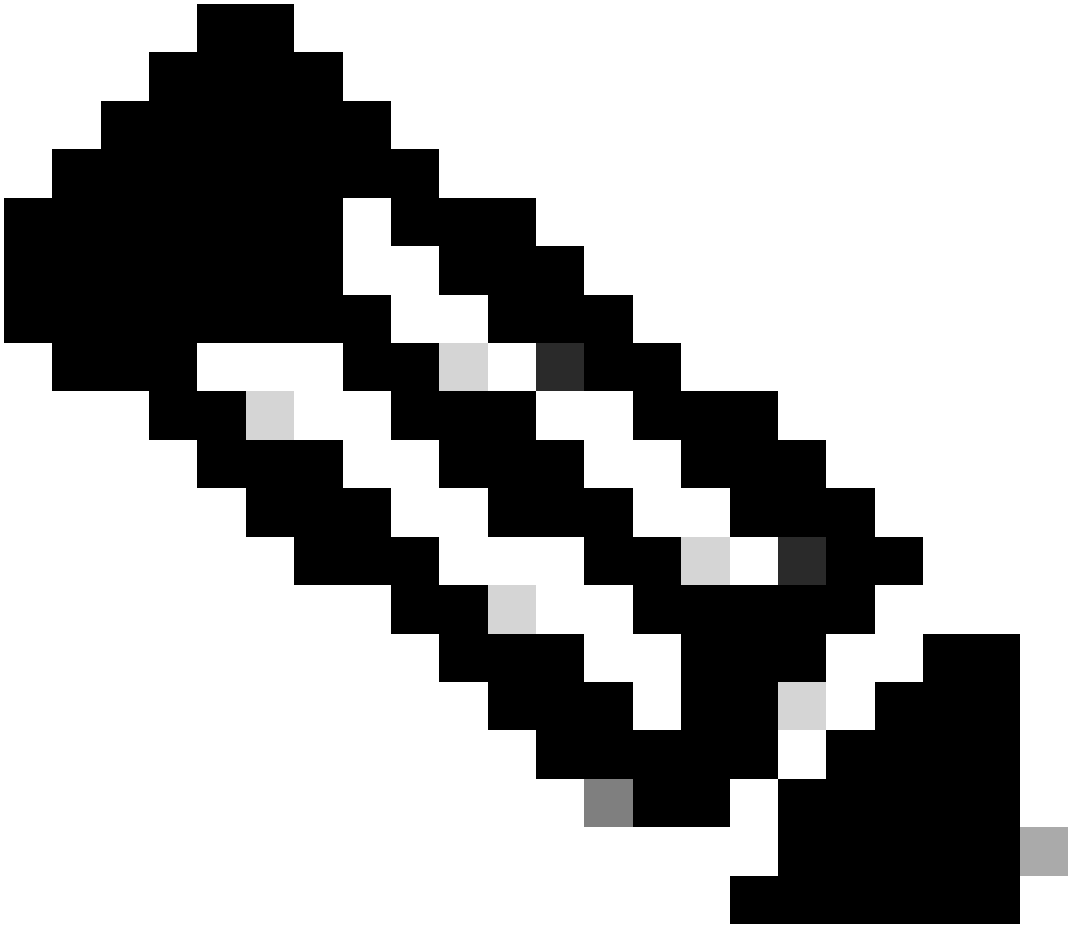
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

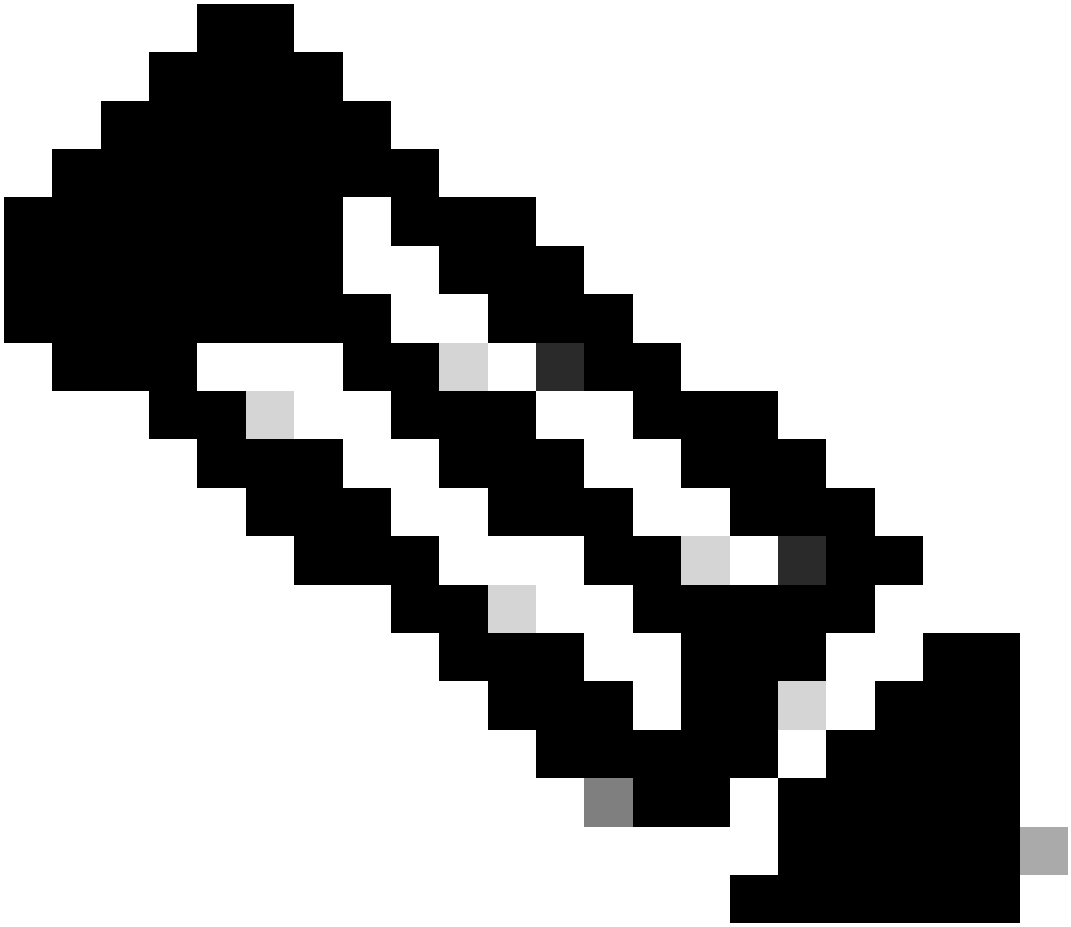
虛擬專用網路(VPN)網關在動態環境中運行。多個變數會影響每個VPN連線；例如，經常更改的內部網配置、每個使用者在一個組織內可以使用的各種角色，以及從具有不同配置和安全級別的遠端訪問站點的登入。在動態VPN環境中，授權使用者的任務要比在靜態配置的網路中複雜得多。

動態訪問策略(DAP)是一種功能，可用於配置滿足VPN環境動態性的授權。通過設定與特定使用者隧道或會話關聯的訪問控制屬性集合來建立動態訪問策略。這些屬性可解決多個組成員身份和端點安全問題。

例如，安全裝置會根據您定義的策略授予特定使用者訪問特定會話的許可權。它通過從一個或多個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，它將DAP記錄應用到使用者隧道或會話。



附註：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檔案匯出到機箱外，對其進行編輯（如果您知道XML語法），然後重新將其匯入，但請非常小心，因為如果配置有誤，可能會導致ASDM停止處理DAP記錄。沒有CLI來操作配置的這一部分。



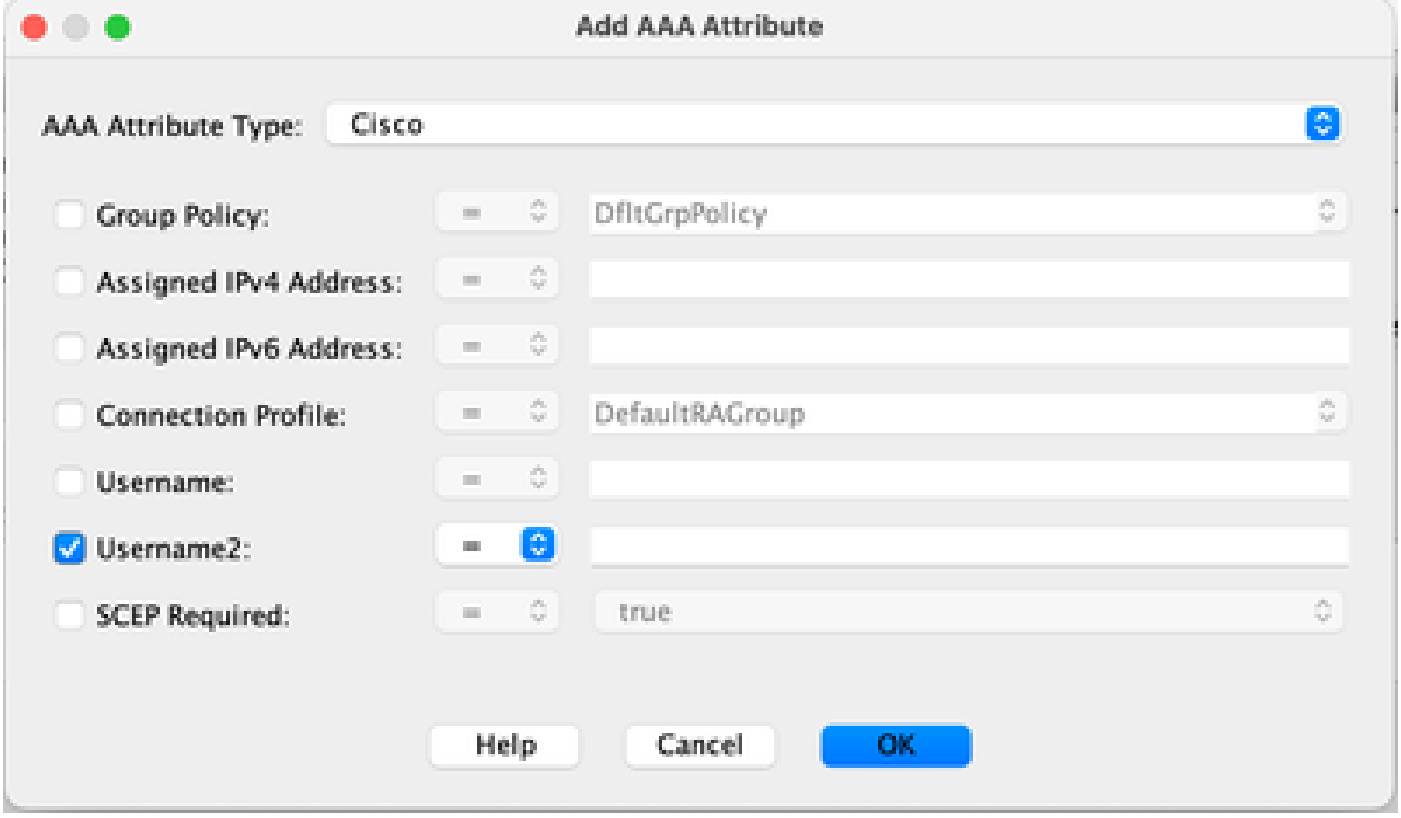
附註：嘗試通過CLI配置dynamic-access-policy-record訪問引數可能會導致DAP停止工作，儘管ASDM會正確管理這些引數。避免CLI，並始終使用ASDM管理DAP策略。

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，然後將其聚合以分配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。

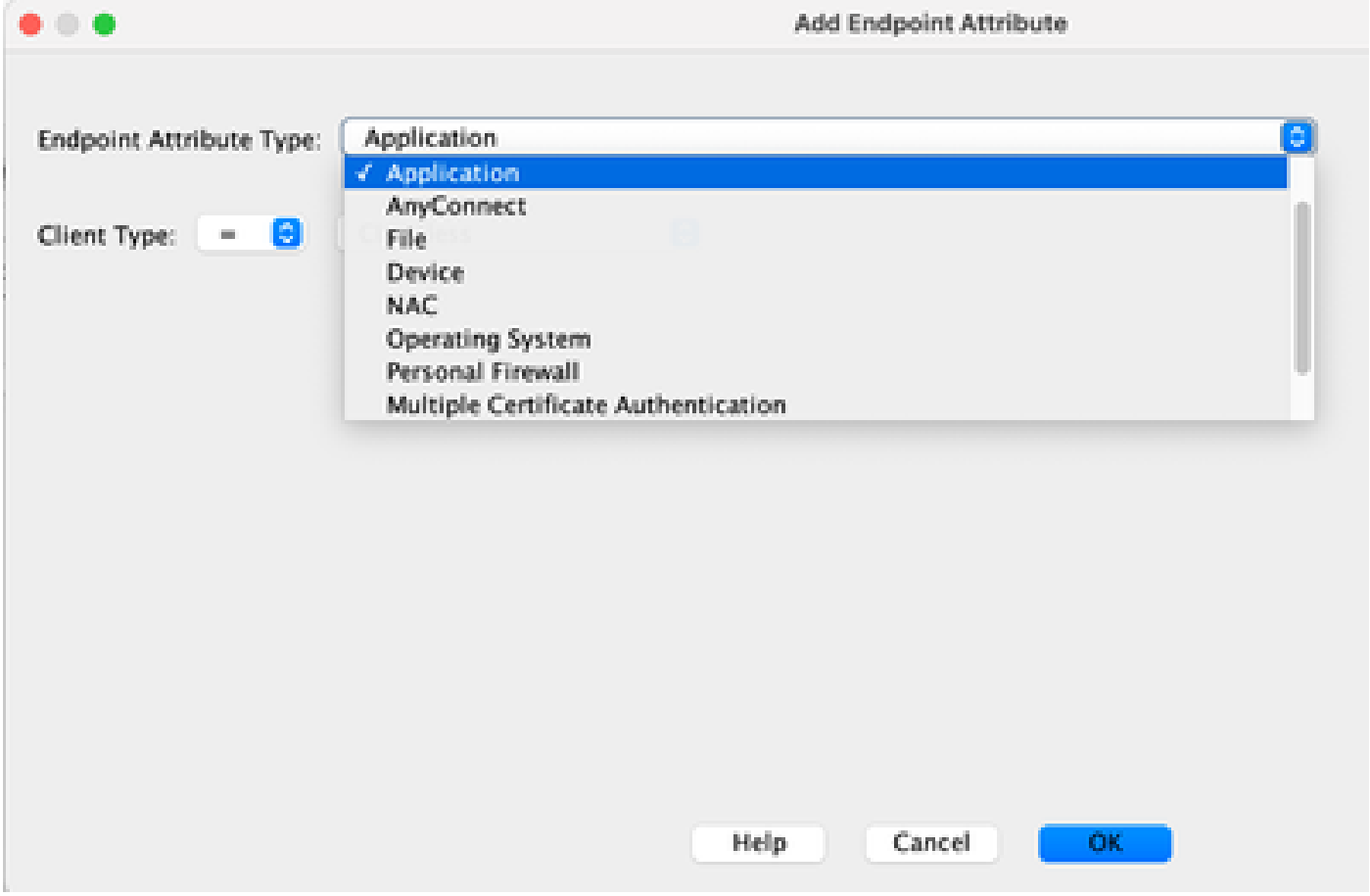
圖1. DAP AAA屬性GUI



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/高級端點評估和NAC。在使用者身份驗證之前，獲取端點評估屬性並將其傳送到安全裝置。但是，AAA屬性（包括總體DAP記錄）會在使用者身份驗證期間進行驗證。

圖2.端點屬性GUI

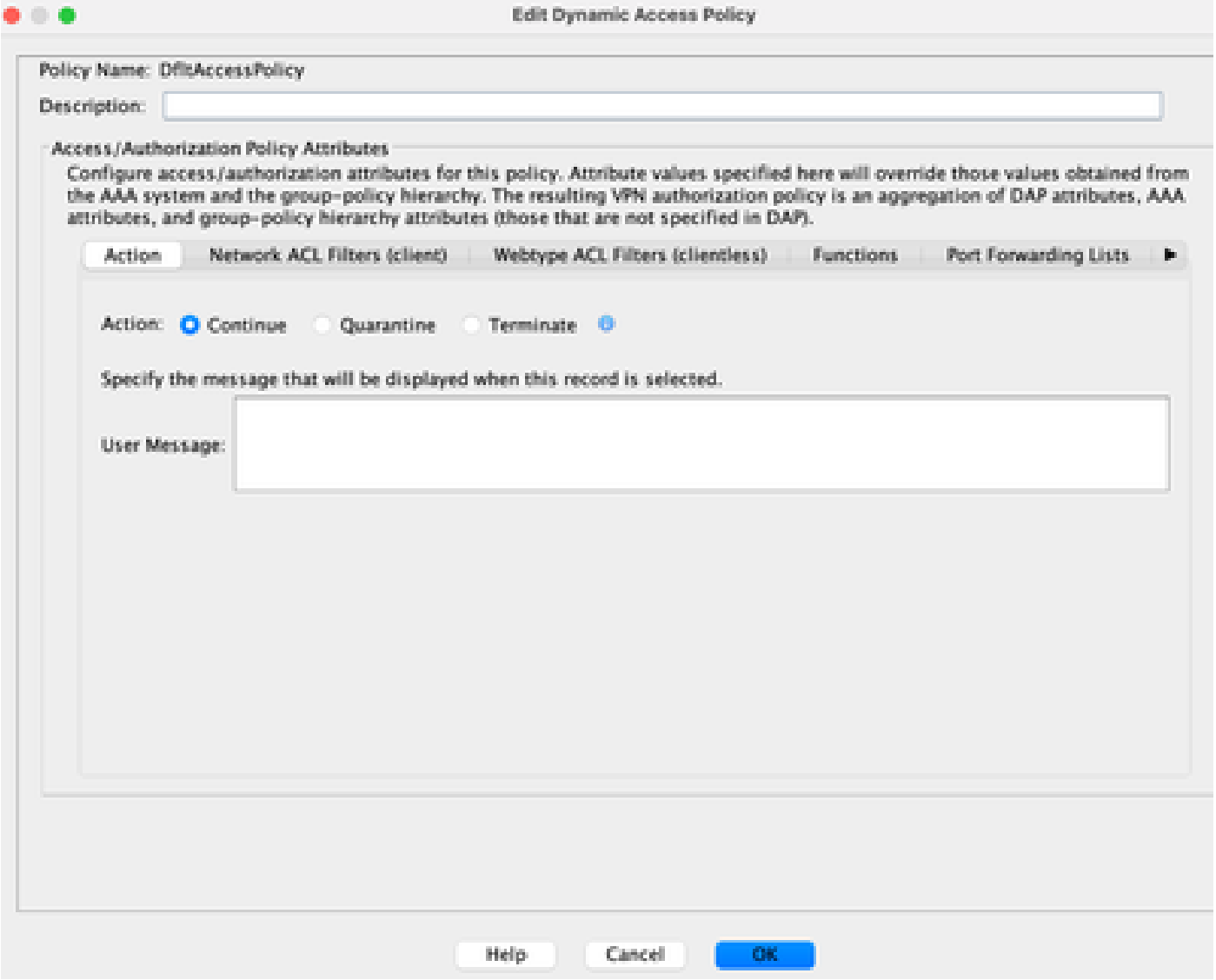


預設動態訪問策略

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）或通過外部AAA伺服器對映。

預設情況下始終實施DAP。例如，通過隧道組、組策略和AAA實施訪問控制，而不顯式實施DAP，仍然可以獲得此行為。如圖3所示，對於傳統行為，無需對DAP功能(包括預設DAP記錄DfltAccessPolicy)進行配置更改。

圖3.預設動態訪問策略



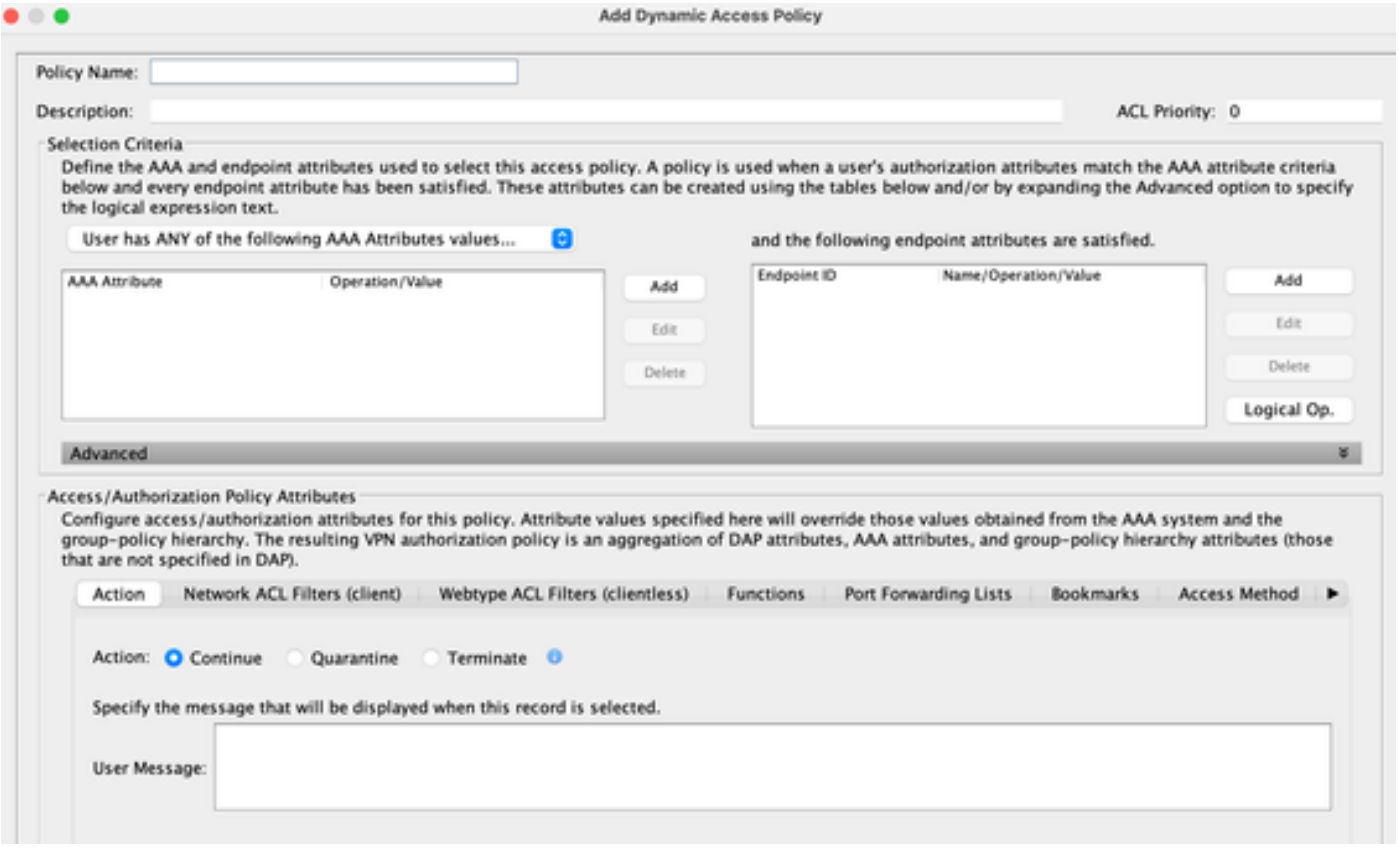
但是，如果更改了DAP記錄中的任何預設值，例如Action: DfltAccessPolicy中的引數從預設值更改為Terminate，並且未配置其他DAP記錄，預設情況下，經過身份驗證的使用者可以匹配DfltAccessPolicy DAP記錄，並且可能被拒絕VPN訪問。

因此，需要建立並配置一個或多個DAP記錄以授權VPN連線並定義經身份驗證的使用者有權訪問哪些網路資源。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，請確定識別連線端點所需的選擇標準，並根據端點評估和/或AAA認證（連線使用者有權訪問哪些網路資源）來確定連線端點。為此，您必須首先熟悉DAP特性和功能，如圖4所示。

圖4.動態訪問策略



配置DAP記錄時，需要考慮兩個主要元件：

- 包括高級選項的選擇標準
- 訪問策略屬性

在選擇標準部分，管理員可以配置用於選擇特定DAP記錄的AAA和終端屬性。當使用者的授權屬性與AAA屬性條件匹配且每個端點屬性均滿足時，使用DAP記錄。

例如，如果選擇了AAA屬性型別LDAP(Active Directory)，則屬性名稱字串為memberOf，值字串為Contractors（如圖5a所示），驗證使用者必須是Active Directory組Contractors的成員才能匹配AAA屬性條件。

除了滿足AAA屬性標準之外，還可以要求身份驗證使用者滿足終端屬性標準。例如，如果管理員配置為確定連線的端點的終端安全評估並基於該終端安全評估，則管理員可以使用此評估資訊作為圖5b所示的終端屬性的選擇標準。

圖5a.AAA屬性條件

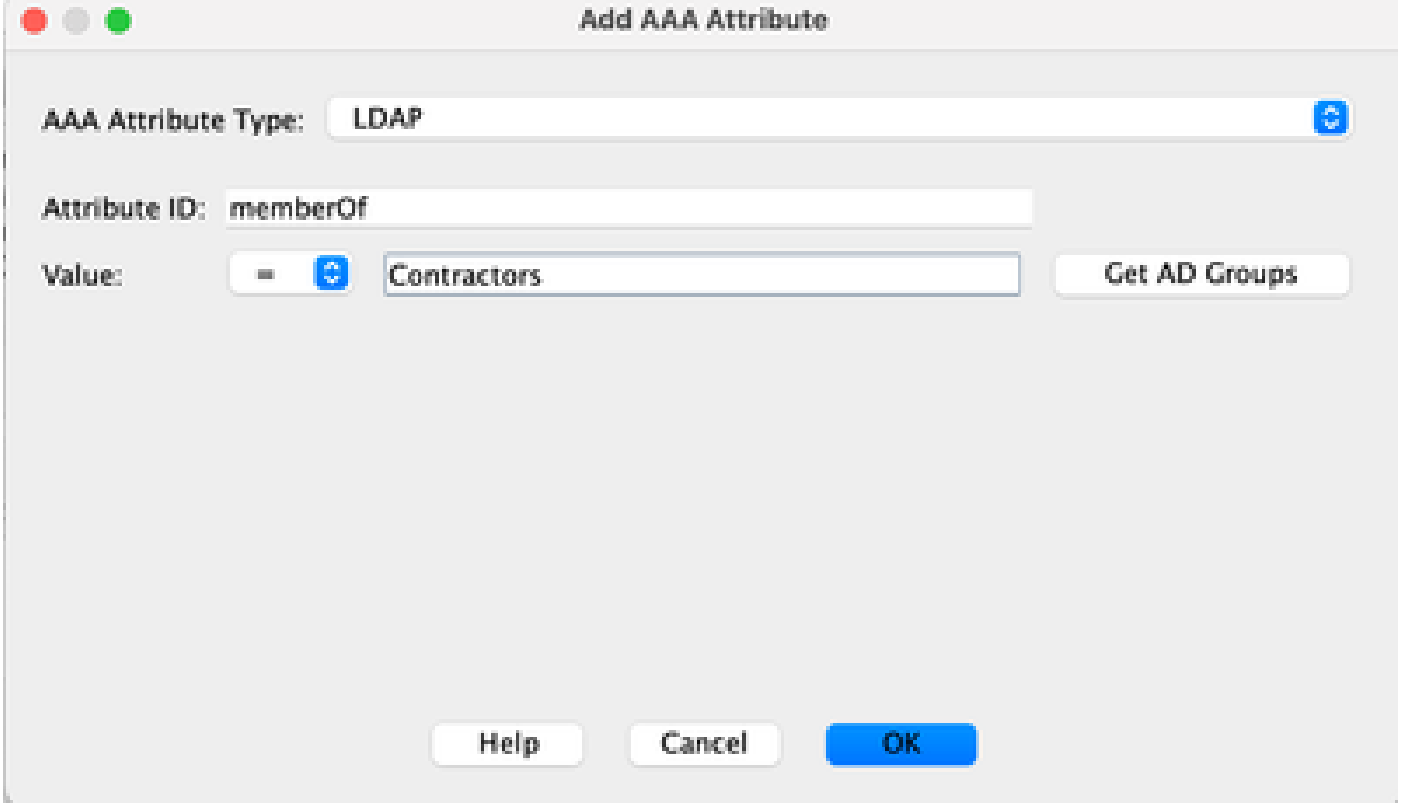


圖5b.端點屬性條件

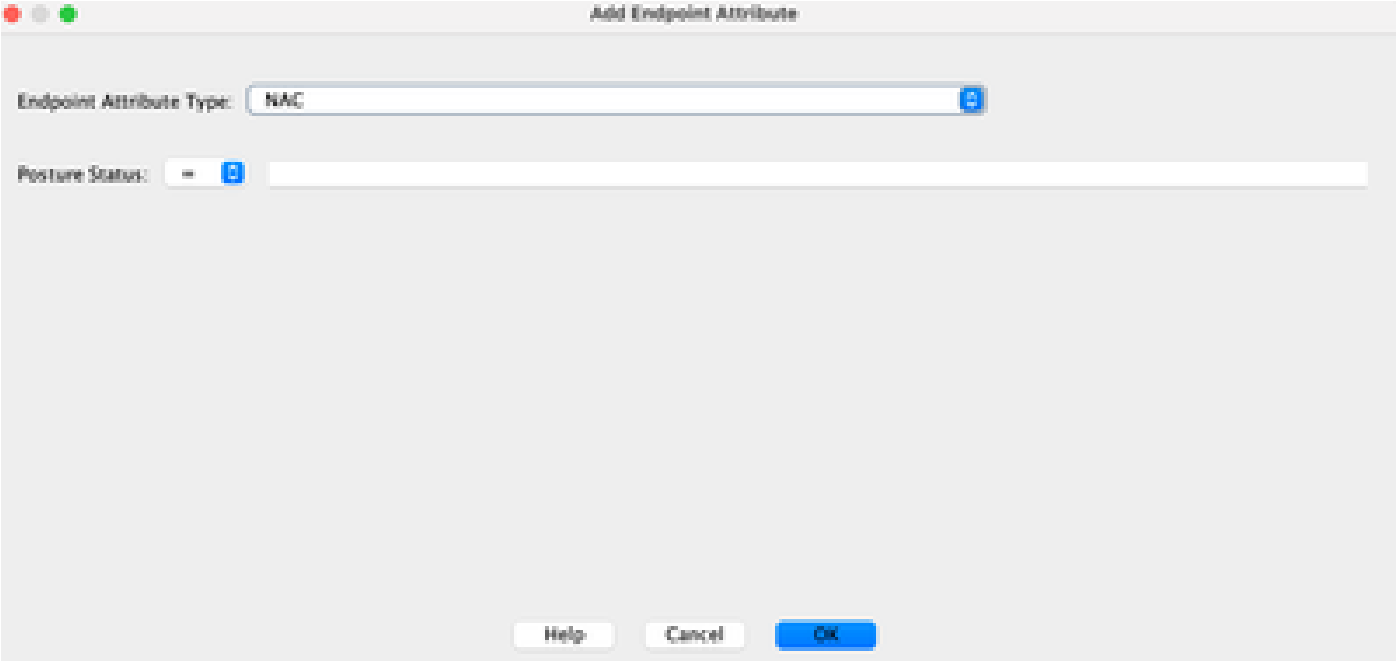
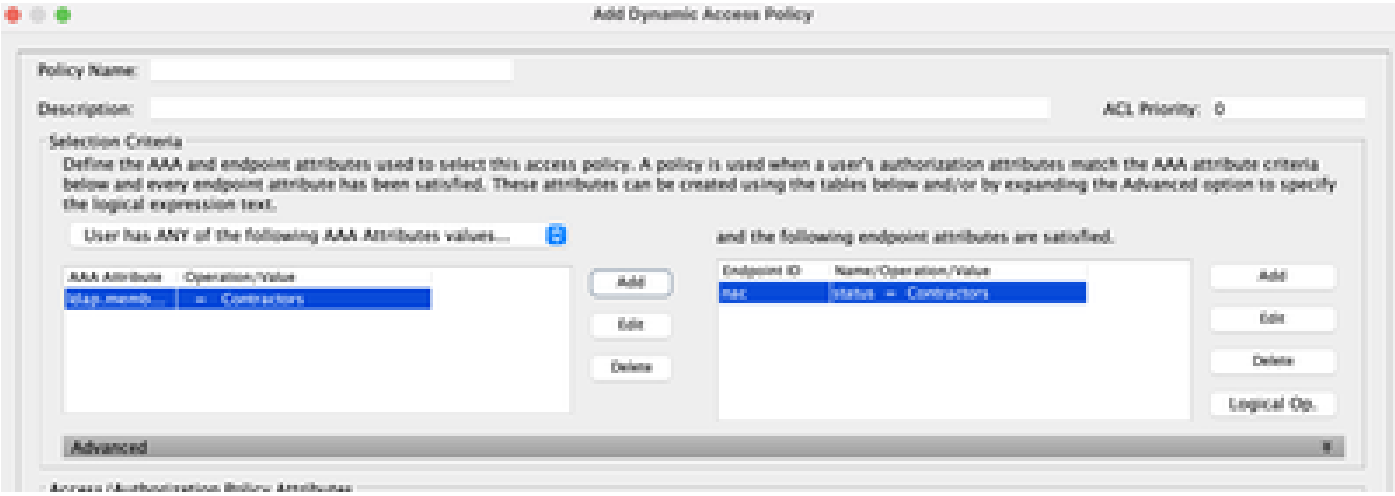


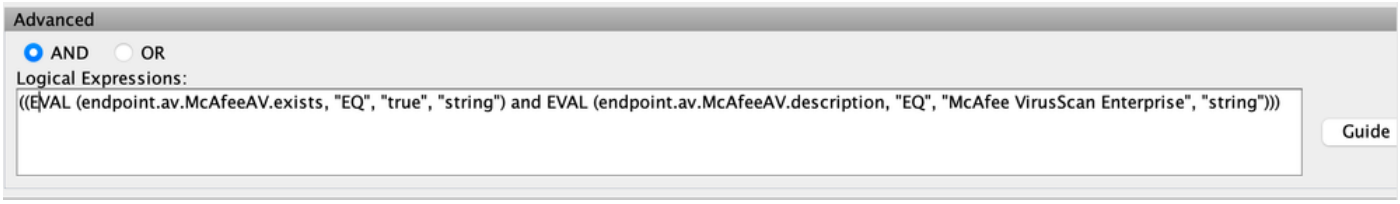
圖6. AAA和終端屬性條件匹配



可以使用圖6中所述的表和/或展開Advanced選項以指定邏輯表達式（如圖7所示）來建立AAA和終端屬性。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/或終端邏輯選擇操作。

如果您需要在AAA和端點屬性區域中新增選擇標準（如前所示）以外的選擇標準，邏輯表達式將非常有用。例如，雖然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標準的AAA屬性，但終端屬性是累積的，必須滿足所有屬性。要使安全裝置採用一個或另一個端點屬性，您需要在DAP記錄的「高級」部分下建立適當的邏輯表達式。

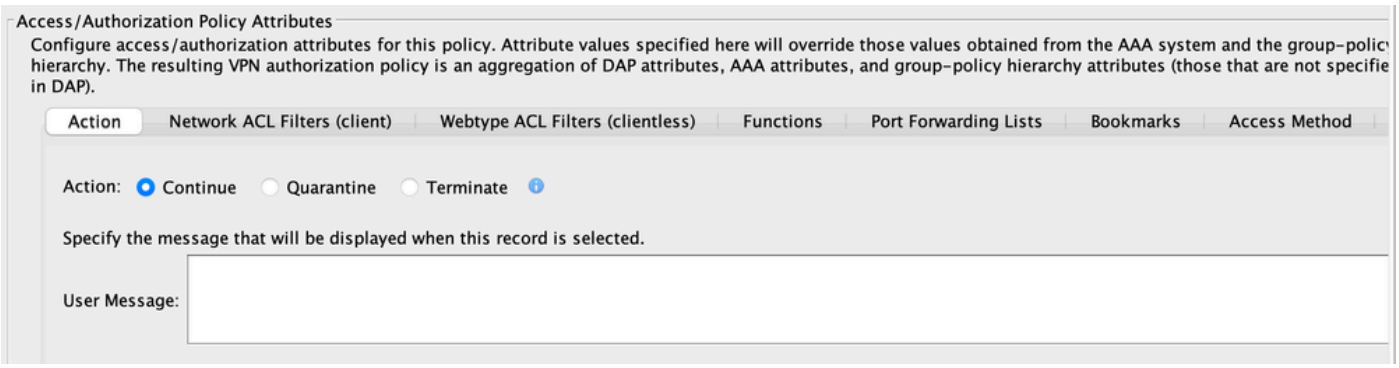
圖7.用於建立高級屬性的邏輯表達式GUI



如圖8所示，「Access Policy Attributes（訪問策略屬性）」部分是管理員為特定DAP記錄配置VPN訪問屬性的位置。使用者授權屬性與AAA、端點和/或邏輯表達式條件匹配時；可以實施本節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。

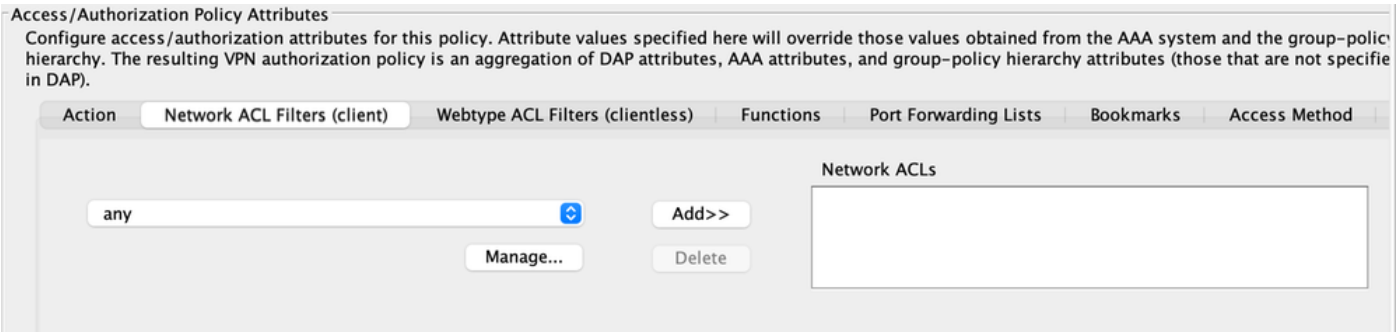
DAP記錄具有一組可以配置的有限屬性值。這些值位於如圖8至圖14所示的頁籤下面：

圖8.操作 — 指定要應用於特定連線或會話的特殊處理。



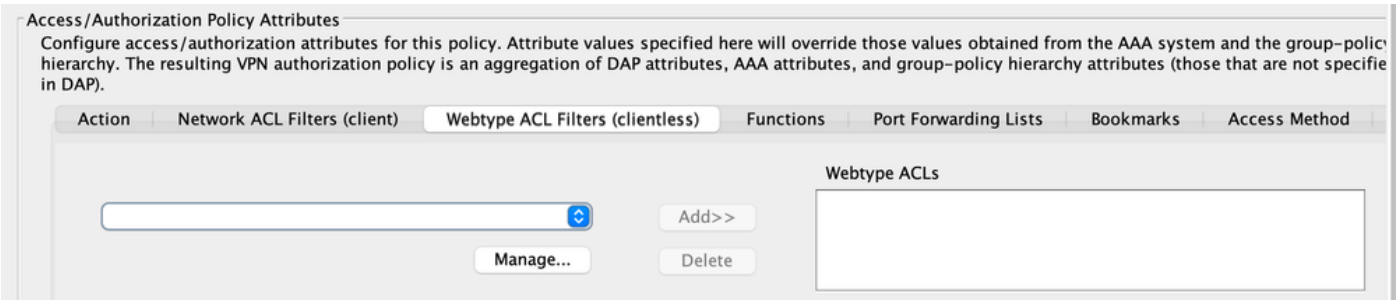
- 繼續(Continue) — （預設）按一下可將訪問策略屬性應用於會話。
- 終止(Terminate) — 單擊以終止會話。
- 使用者消息 — 輸入當選擇此DAP記錄時要在門戶頁面上顯示的文本消息。最多128個字元。使用者消息顯示為黃色球體。當使用者登入時，它會閃爍三次以吸引注意，然後就靜止。如果選擇了多個DAP記錄，並且每個記錄都有一個使用者消息，則顯示所有使用者消息。此外，您可以在此類郵件中包含URL或其他嵌入文本，它們要求您使用正確的HTML標籤。

圖9.網路ACL過濾器頁籤 — 通過此頁籤，可以選擇並配置要應用到此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permit和deny規則，則安全裝置將拒絕ACL配置。



- 網路ACL下拉框已配置網路ACL，以便新增到此DAP記錄。只有具有所有允許或拒絕規則的ACL才符合條件，並且只有此處顯示的ACL符合條件。
- 管理 — 單擊以新增、編輯和刪除網路ACL。
- 網路ACL 列了此DAP記錄的網路ACL。
- Add — 單擊將下拉框中的所選網路ACL新增到右側的Network ACL清單中。
- Delete — 按一下從Network ACLs清單中刪除突出顯示的網路ACL。如果某個ACL已分配給DAP或其他記錄，則不能將其刪除。

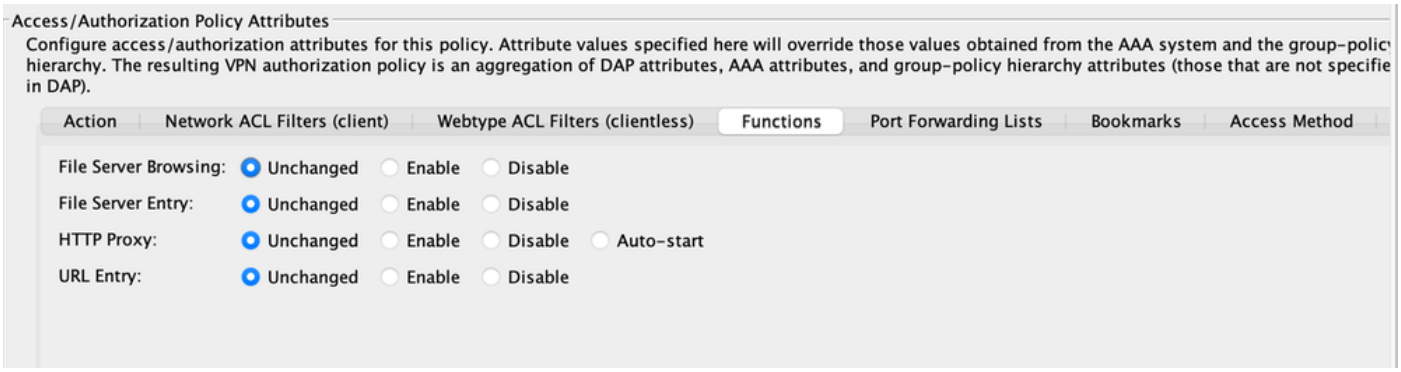
圖10. Web-Type ACL Filters頁籤 — 通過此頁籤，可以選擇並配置要應用到此DAP記錄的Web-type ACL。DAP的ACL只能包含允許或拒絕規則。如果ACL同時包含permit和deny規則，則安全裝置將拒絕ACL配置。



- Web-Type ACL下拉框 — 選擇已配置的Web-type ACL以新增到此DAP記錄。只有具有所有permit或all deny規則的ACL才符合條件，並且只有此處顯示的ACL符合條件。

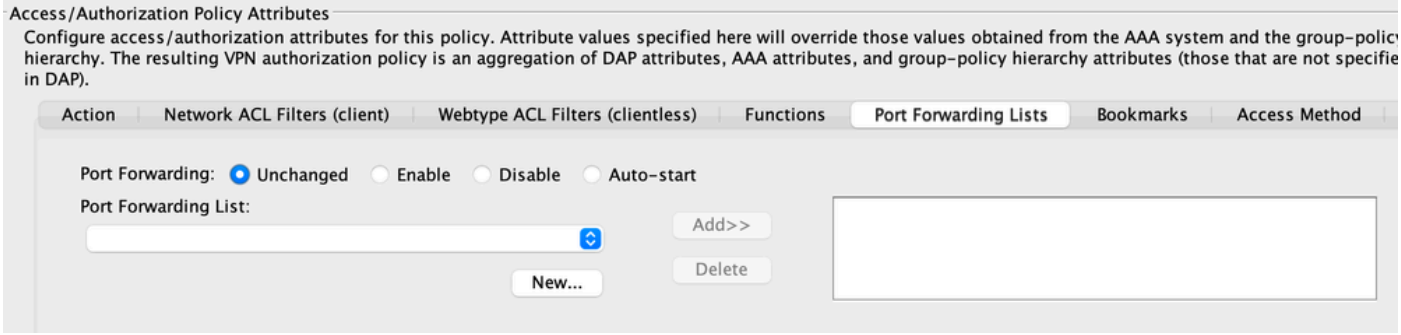
- 管理…… — 按一下可新增、編輯和刪除Web型別ACL。
- Web-Type ACL list — 顯示此DAP記錄的Web型別ACL。
- Add — 按一下將下拉框中的所選Web型別ACL新增到右側的Web型別ACL清單中。
- Delete — 按一下從Web型別ACL清單中刪除Web型別ACL。如果某個ACL已分配給DAP或其他記錄，則不能將其刪除。

圖11.功能頁籤 — 用於為DAP記錄配置檔案伺服器條目和瀏覽、HTTP代理和URL條目。



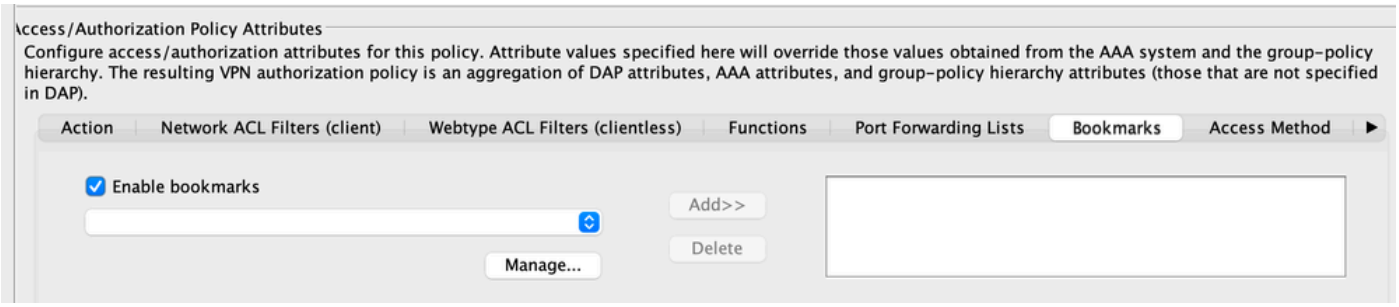
- File Server Browsing — 啟用或禁用檔案伺服器或共用功能的CIFS瀏覽。
- File Server Entry — 允許或拒絕使用者在門戶頁面上輸入檔案伺服器路徑和名稱。啟用時，將檔案伺服器條目抽屜放在門戶頁面上。使用者可以直接輸入Windows檔案的路徑名。他們可以下載、編輯、刪除、重新命名和移動檔案。他們還可以新增檔案和資料夾。還必須配置共用，以便使用者在適用的Microsoft Windows伺服器上訪問。根據網路要求，使用者可能需要在訪問檔案之前進行身份驗證。
- HTTP Proxy — 影響HTTP applet Proxy向客戶端的轉發。代理對於干擾正確內容轉換的技術（例如Java、ActiveX和Flash）非常有用。它可繞過修剪/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輸入框中輸入網址，並使用無客戶端SSL VPN訪問這些網站。
- Unchanged —（預設）按一下以使用適用於此會話的組策略中的值。
- Enable/Disable — 單擊啟用或禁用該功能。
- 自動啟動 — 單擊以啟用HTTP代理，並使DAP記錄自動啟動與這些功能關聯的小程式。

圖12.埠轉發清單頁籤 — 用於為使用者會話選擇和配置埠轉發清單。



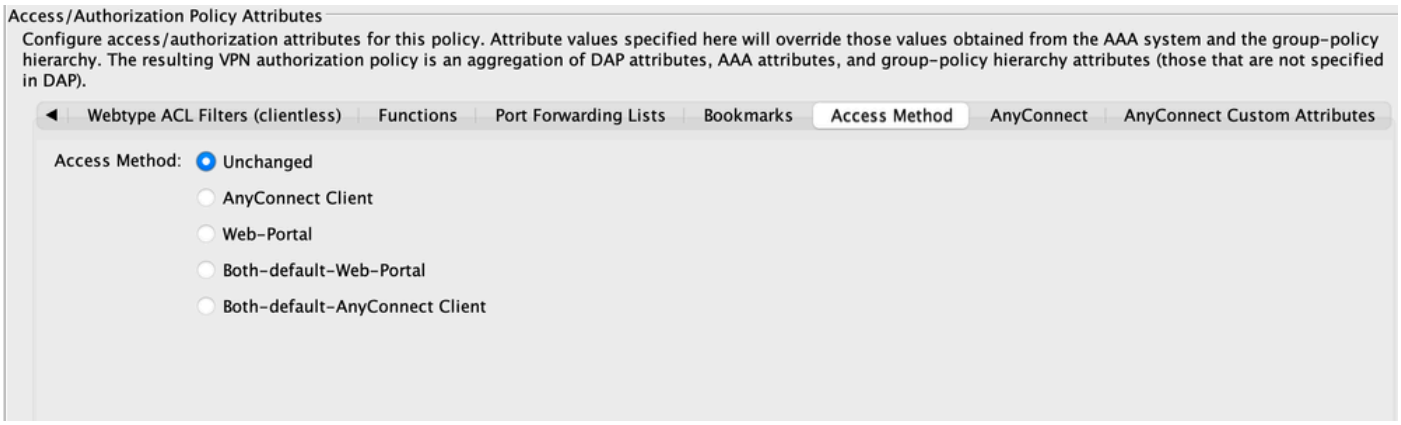
- Port Forwarding — 為適用於此DAP記錄的埠轉發清單選擇一個選項。僅當將Port Forwarding設定為Enable或Auto-start時，才會啟用此欄位中的其他屬性。
- Unchanged — 按一下以使用應用於此會話的組策略中的值。
- Enable/Disable — 按一下以啟用或禁用埠轉發。
- Auto-start — 按一下以啟用埠轉發，並使DAP記錄自動啟動與其埠轉發清單關聯的埠轉發小程式。
- Port Forwarding List下拉框 — 選擇已配置的埠轉發清單，以新增到DAP記錄。
- New — 按一下以配置新的埠轉發清單。
- Port Forwarding Lists — 顯示DAP記錄的埠轉發清單。
- Add — 點選將下拉框中的所選埠轉發清單新增到右側的Port Forwarding清單。
- Delete — 按一下以從Port Forwarding清單中刪除選定的埠轉發清單。如果某個ACL已分配給DAP或其他記錄，則不能將其刪除。

圖13.書籤頁籤 — 允許您為使用者會話選擇和配置書籤/URL清單。



- 啟用書籤 — 按一下以啟用。如果未選擇此框，則連線的門戶頁面上不會顯示書籤清單
- 管理 — 按一下以新增、匯入、匯出和刪除書籤清單。
- 書籤列表(Bookmarks Lists)（下拉選單） — 顯示DAP記錄的書籤清單。
- Add -按一下將下拉框中的所選書籤清單新增到右側的書籤清單框中。
- Delete — 按一下以從書籤清單框中刪除選定的書籤清單。您不能從安全裝置中刪除書籤清單，除非您首先從DAP記錄中刪除該清單。

圖14.方法頁籤 — 允許您配置允許的遠端訪問型別。



- Unchanged -繼續使用在會話的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 — 通過無客戶端或AnyConnect客戶端進行連線，預設情況下為無客戶端。
- Both-default-AnyConnect Client — 通過無客戶端或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，僅當修改它們時，它們優先於當前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，拆分隧道清單、橫幅、智慧隧道、門戶自定義設定等，則需要通過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，這些特定的屬性值可以補充DAP，並且不能被覆蓋。因此，使用者將獲得所有記錄的屬性值的累積集合。

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和終端屬性標準。因此，訪問策略屬性可以在這些策略中保持一致或衝突。在這種情況下，授權使用者可以獲取所有匹配的DAP記錄的累積結果。

這還包括通過身份驗證、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中所示的action屬性的值為Terminate或Continue。如果在任何選定的DAP記錄中配置了「終止」值，則聚合屬性值為「終止」；如果在所有選定的DAP記錄中配置了「繼續」值，則聚合屬性值為「繼續」。

表1.行動屬性

屬性名稱	DAP#1	DAP#2	DAP#3	DAP
Action（示例1）	繼續	繼續	繼續	繼續

Action（示例2）	終止	繼續	繼續	終止

表2中顯示的user-message屬性包含字串值。聚合的屬性值可以是通過將所選DAP記錄的屬性值連結在一起而建立的行饋送（十六進位制值0x0A）分隔的字串。組合字串中屬性值的排序無關緊要。

表2.使用者消息屬性

屬性名稱	DAP#1	DAP#2	DAP#3	DAP
user-message	快速	棕狐	跳過	快速的<LF>棕狐<LF>跳過

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

如果在任何選定的DAP記錄中沒有配置Auto-start或Enable值，並且至少在一個選定的DAP記錄中配置了「disable」值，則可以禁用聚合屬性值。

表3.啟用屬性的無客戶端功能（函式）

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

表4中顯示的URL清單和port-forward屬性包含一個值，該值可以是字串或逗號分隔字串。聚合的屬性值可以是將選定DAP記錄的屬性值連結在一起時建立的逗號分隔字串。可以刪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、AnyConnect客戶端或Web門戶訪問（預設情況下使用Web門戶訪問），或預設情況下使用AnyConnect客戶端訪問的AnyConnect客戶端或Web門戶訪問。彙總的屬性值彙總於表5。

表5.訪問方法屬性

已選擇屬性值				聚合結果
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

當結合網路（防火牆）和Web型別（無客戶端）ACL過濾器屬性時，要考慮的兩大元件是DAP Priority和DAP ACL。

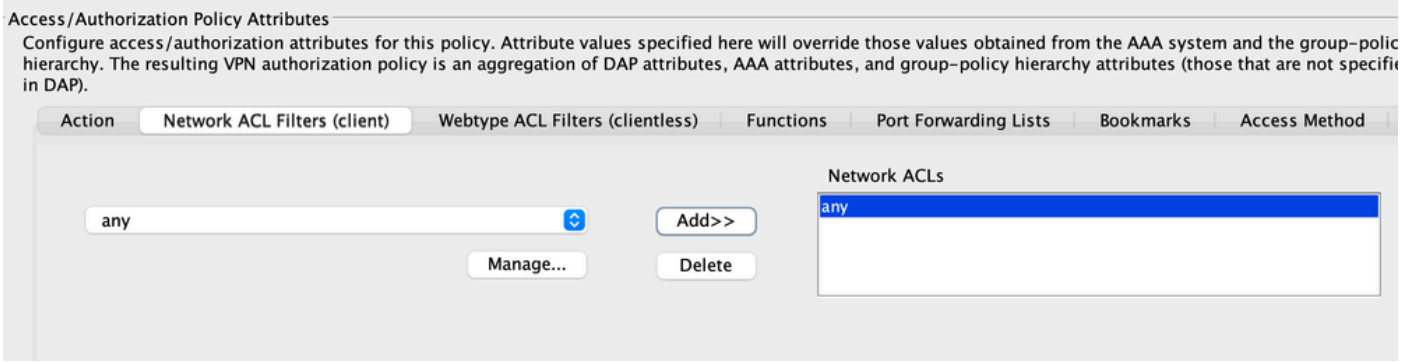
圖15中所示的Priority屬性不進行聚合。在從多個DAP記錄中聚合Network和Web-Type ACL時，安全裝置使用此值對訪問清單進行邏輯排序。安全裝置按優先順序從高到低的順序對記錄進行排序，優先順序最低的在表底部。例如，值為4的DAP記錄的優先順序高於值為2的記錄。您無法手動對其進行排序。

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。
- Description -描述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模型的訪問列表。在Allow-List ACL模型中，訪問清單條目指定「允許」訪問指定網路或主機的規則。在Block-List ACL模式下，access-list條目指定拒絕對指定網路或主機的訪問的規則。不一致的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，則當管理員嘗試新增該記錄時，可能會因為配置錯誤而拒絕該清單。如果符合的訪問清單被分配給DAP記錄，則對訪問清單進行的任何更改符合性特徵的修改都會被拒絕為配置錯誤。

圖16. DAP ACL — 用於選擇和配置網路ACL以應用於此DAP記錄。



選擇多個DAP記錄時，將聚合網路（防火牆）ACL中指定的訪問清單屬性，以建立DAP防火牆ACL的動態訪問清單。 同樣地，會將Web-Type(Clientless)ACL中指定的存取清單屬性聚集，以便為DAP無使用者端ACL建立動態存取清單。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從選定的DAP記錄中檢索Network-ACL屬性，如表7所示。

表7.網路ACL

選定的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具有4個拒絕規則，ACL 102具有4個允許規則
DAP 2	2	201和202	ACL 201具有3個允許規則，ACL 202具有3個拒絕規則
DAP 3	2	101和102	ACL 101具有4個拒絕規則，ACL 102具有4個允許規則

第三，如果2個或更多選定的DAP記錄的優先順序值相同，則ASA首先按DAP記錄優先順序編號對Network-ACL重新排序，然後按Block-List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	白色/黑色存取清單型號	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許可規則(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許可規則(PPPP)

最後，ASA將Network-ACL條目合併到動態生成的Network-ACL中，然後返回動態Network-ACL的名稱，作為要強制實施的新Network-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 PPP PPP DDDD PPP

DAP實現

管理員必須考慮實施DAP的原因有很多。一些根本原因是在終端上實施狀況評估，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。在下一個示例中，可以配置DAP及其元件以標識連線端點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「受管」或「非受管」的能力。 — 如果端點被識別為受管（工作PC）但狀態要求失敗，則必須拒絕該端點的訪問。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。
- 在無客戶端連線終止時呼叫會話cookie和快取清理的功能。
- 能夠檢測並強制在受管理的員工端點（如McAfee AntiVirus）上運行應用程式。如果應用程式不存在，則必須拒絕該終結點訪問。
- 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。
- 通過客戶端/基於網路的連線進行連線時，允許本地LAN訪問網路資源，如網路傳真和印表機。
- 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，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。

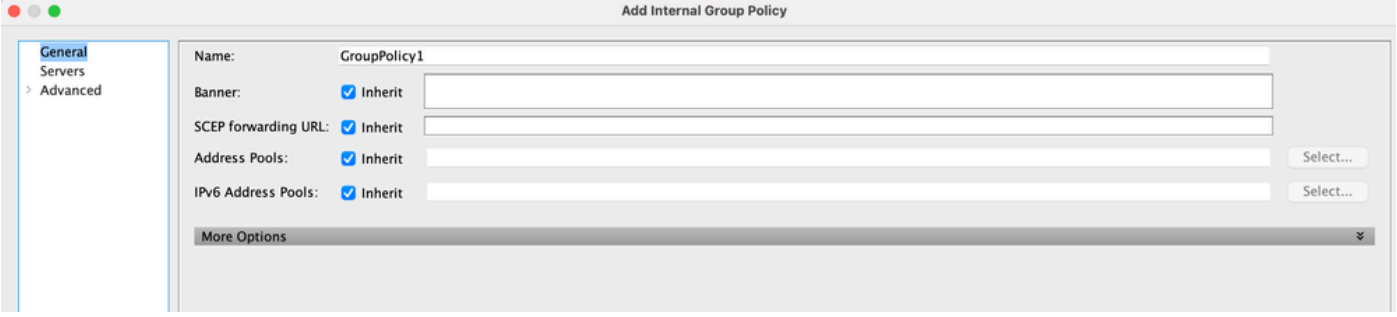
在本示例中，您可以執行一系列配置步驟以滿足客戶端的VPN訪問要求。可能存在必要的配置步驟，但與DAP不直接相關，而其它配置可能直接與DAP相關。ASA非常動態，可以適應許多網路環境。因此，可以通過各種方式定義VPN解決方案，並在某些情況下提供相同的最終解決方案。但是，所採用的方法受客戶需求及其環境的驅動。

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，您還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池和預設DNS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和基於客戶端的屬性）。

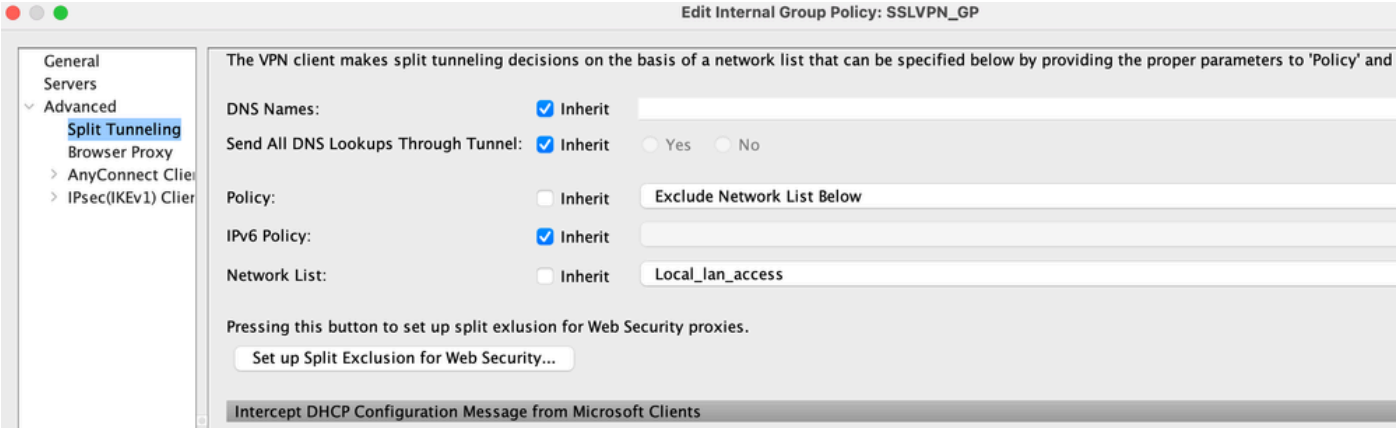
導覽至Configuration > Remote Access VPN > Network(Client)Access > Group Policies，然後新增內部組策略，如下所示：

圖17.組策略 — 定義本地VPN特定屬性。



1. 在General連結下，為組策略配置名稱SSLVPN_GP。
2. 此外，在General連結下，按一下More選項並僅配置隧道協定：Clientless SSLVPN。（可以配置DAP以覆蓋和管理訪問方法。）
3. 在Advanced > Split Tunneling連結下，配置後續步驟：

圖18.分割通道 — 允許指定流量（本地網路）在客戶端連線期間繞過未加密的通道。

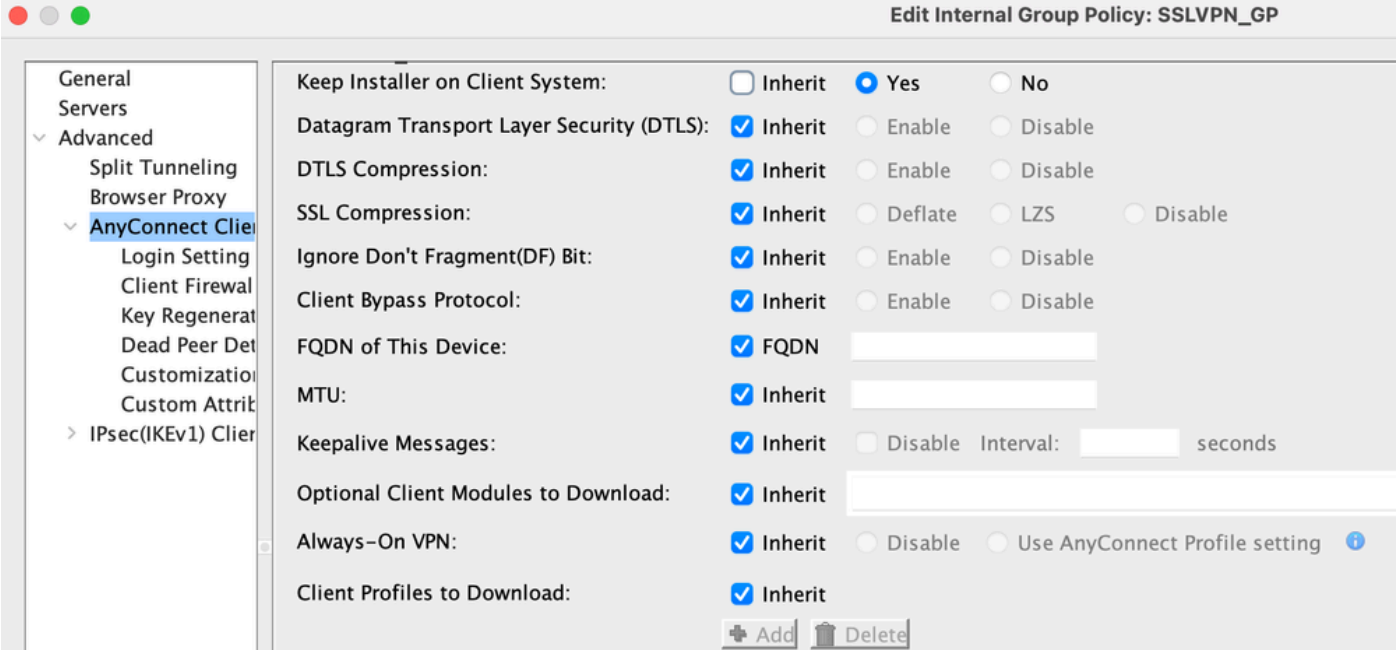


原則：取消選中Inheritand selectExclude Network List。

網路清單：取消選中Inheritand並選擇清單nameLocal_Lan_Access。（假設已預配置。）

在Advanced > ANYCONNECT Client連結下，配置以下後續步驟：

圖19. SSL VPN客戶端安裝程式 — 在VPN終止時，SSL客戶端可以保留在端點上或者可以解除安裝。



a. 在客戶端系統上保留安裝程式：取消選中Inheritand，然後選擇Yes。

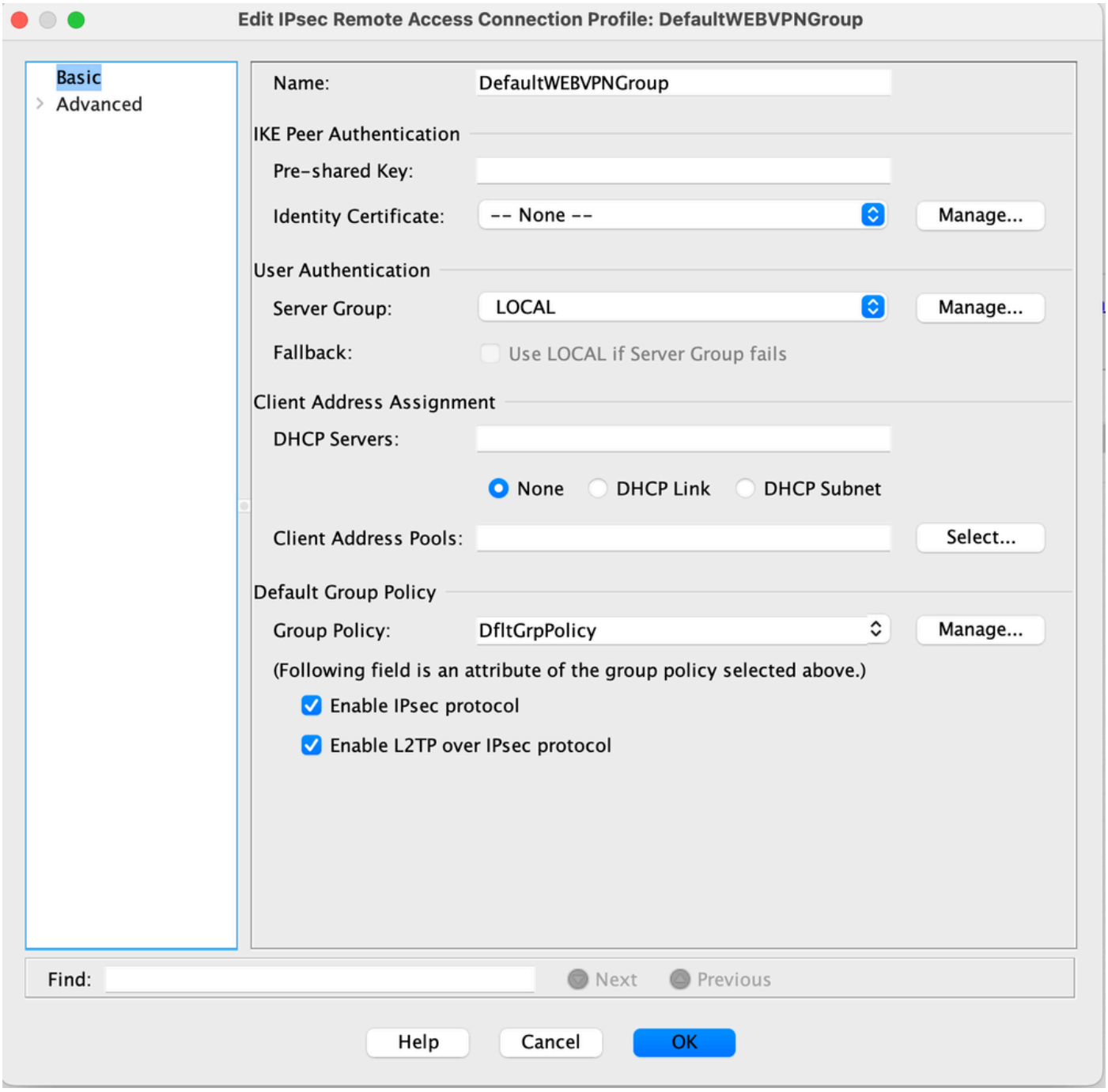
b. 按一下「確定」(OK)>「應用」(Apply)。

c. 應用您的配置更改。

定義連線配置檔案 — 此配置對於定義AAA身份驗證方法（例如LDAP）以及將以前配置的組策略(SSLVPN_GP)應用到此連線配置檔案是必需的。通過此連線配置檔案進行連線的使用者可採用此處定義的屬性以及在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和基於客戶端的屬性）。

導覽至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。



1. 在Connection Profiles部分下，編輯DefaultWEBVPNGroup，並在Basic連結下配置後續步驟：
    1. 身份驗證 — 方法：AAA
    2. 身份驗證 — AAA伺服器組:LDAP（假設預配置）
    3. Client Address Assignment — 客戶端地址池:IP_Pool（假設預配置）
    4. 預設組策略 — 組策略：SelectSSLVPN_GP
2. 應用您的配置更改。

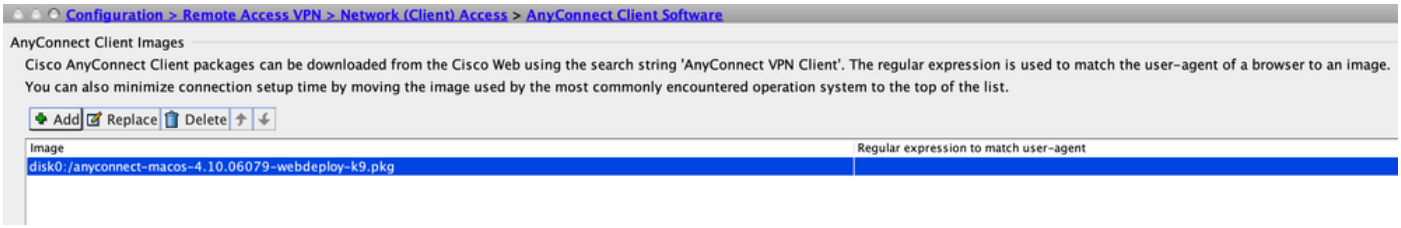
為SSL VPN連線定義IP介面 — 在指定介面上終止客戶端和無客戶端SSL連線需要此配置。

在介面上啟用客戶端/網路訪問之前，必須首先定義SSL VPN客戶端映像。

1. 導覽至Configuration > Remote Access VPN > Network(Client)Access > Anyconnect Client Software，然後從ASA Flash檔案系統新增下一個映像SSL VPN Client Image:(此影象可從

CCO(https://www.cisco.com)下載)

圖21. SSL VPN客戶端映像安裝 — 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. 依次按一下OK、OK和Apply。

1. 導航到Configuration > Remote Access VPN > Network(Client)Access > AnyConnect Connection Profiles，然後使用後續步驟啟用此功能：

圖22. SSL VPN訪問介面 — 定義用於終止SSL VPN連線的介面。

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

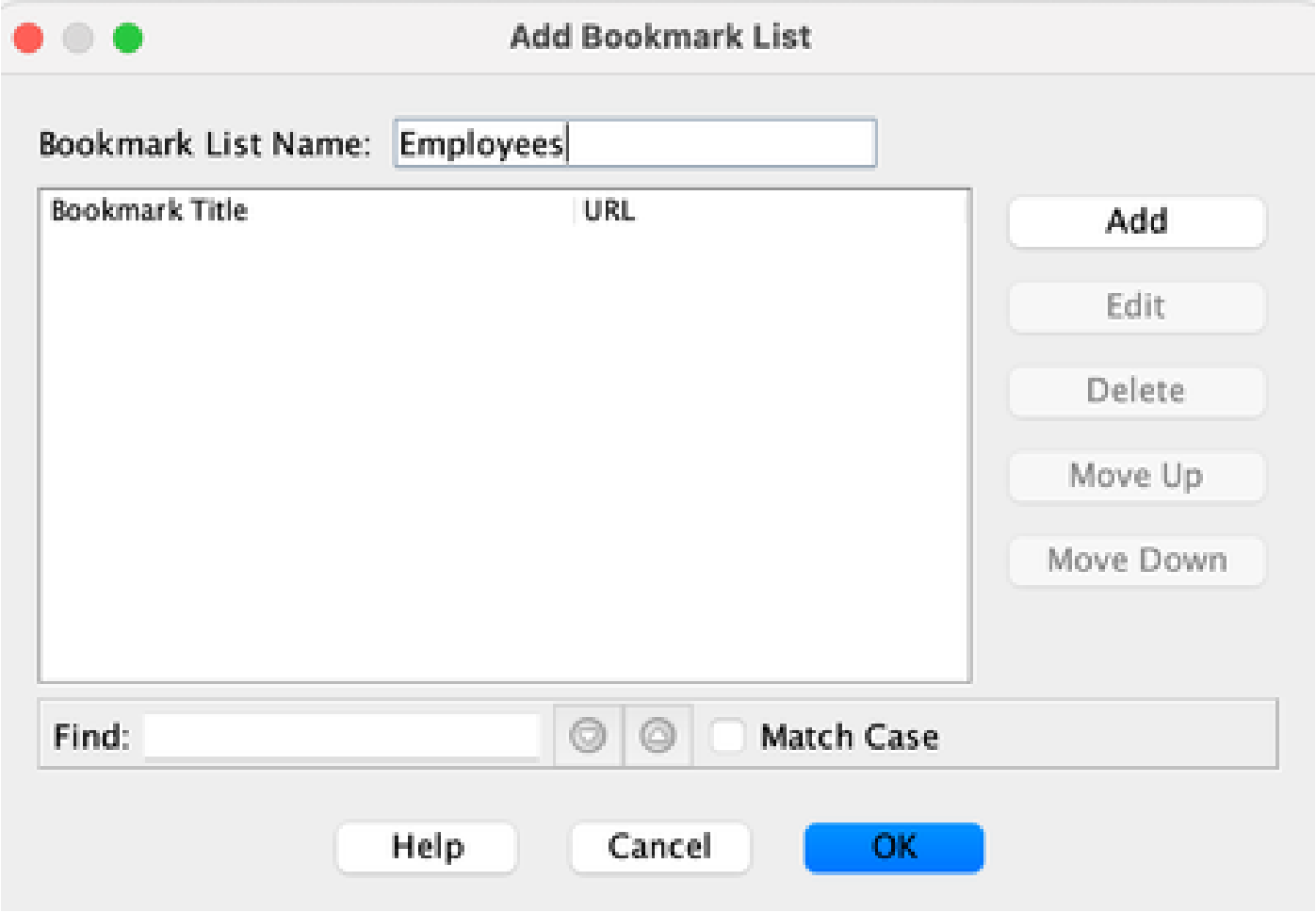
b. 此外，在Access Interfaces部分下，選中Allow Access外部介面。（此配置也可以在外部介面上啟用SSL VPN無客戶端訪問。）

c. 按一下「Apply」。

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的應用程式是必需的。您可以定義2個URL清單，一個用於員工，另一個用於承包商。

1. 導覽至Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks，然後點選+ Addition並配置後續步驟：

圖23.書籤清單 — 定義要從Web門戶發佈和訪問的URL。（為員工訪問而定製）。



a. 將清單名稱：Employees書籤，然後按一下Add。

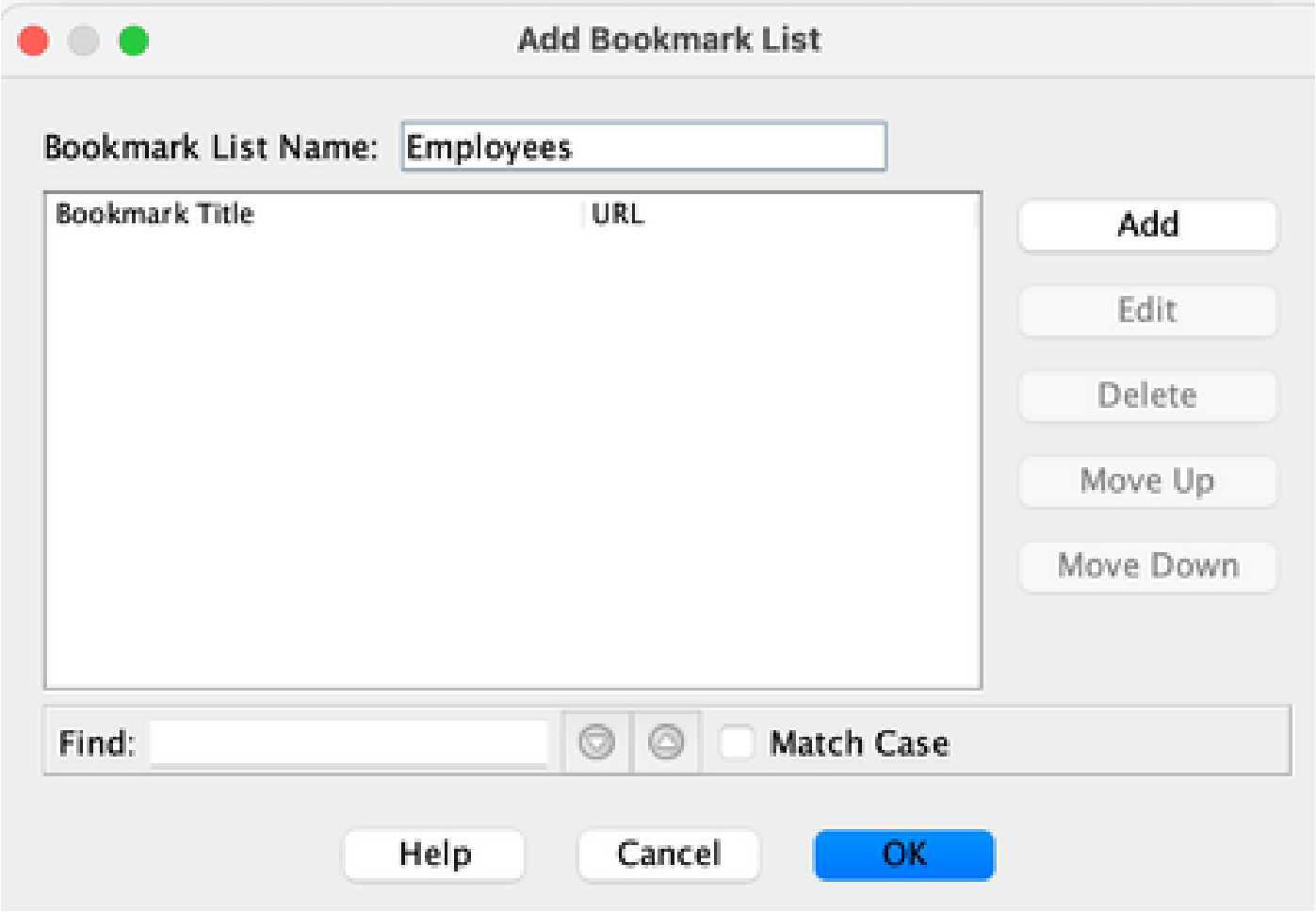
b. 書籤標題：公司內部網

c. URL值： https://company.resource.com

d. 按一下「確定」(OK)，然後再次按一下「確定」(OK)。

1. 按一下「+ 」，然後設定第二個書籤清單（URL清單），如下所示：

圖24.書籤清單 — 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

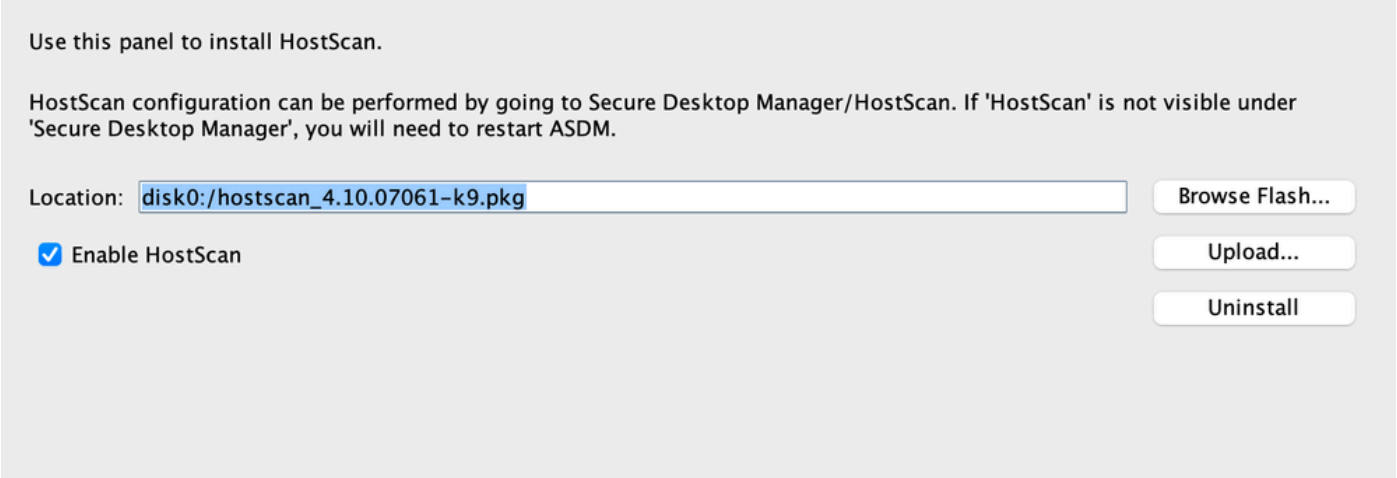
d. 按一下「確定」(OK)，然後再次按一下「確定」(OK)。

e. 按一下「Apply」。

配置Hostscan:

1. 導覽至Configuration > Remote Access VPN > Secure Desktop Manager > HostScan Image，然後配置後續步驟：

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



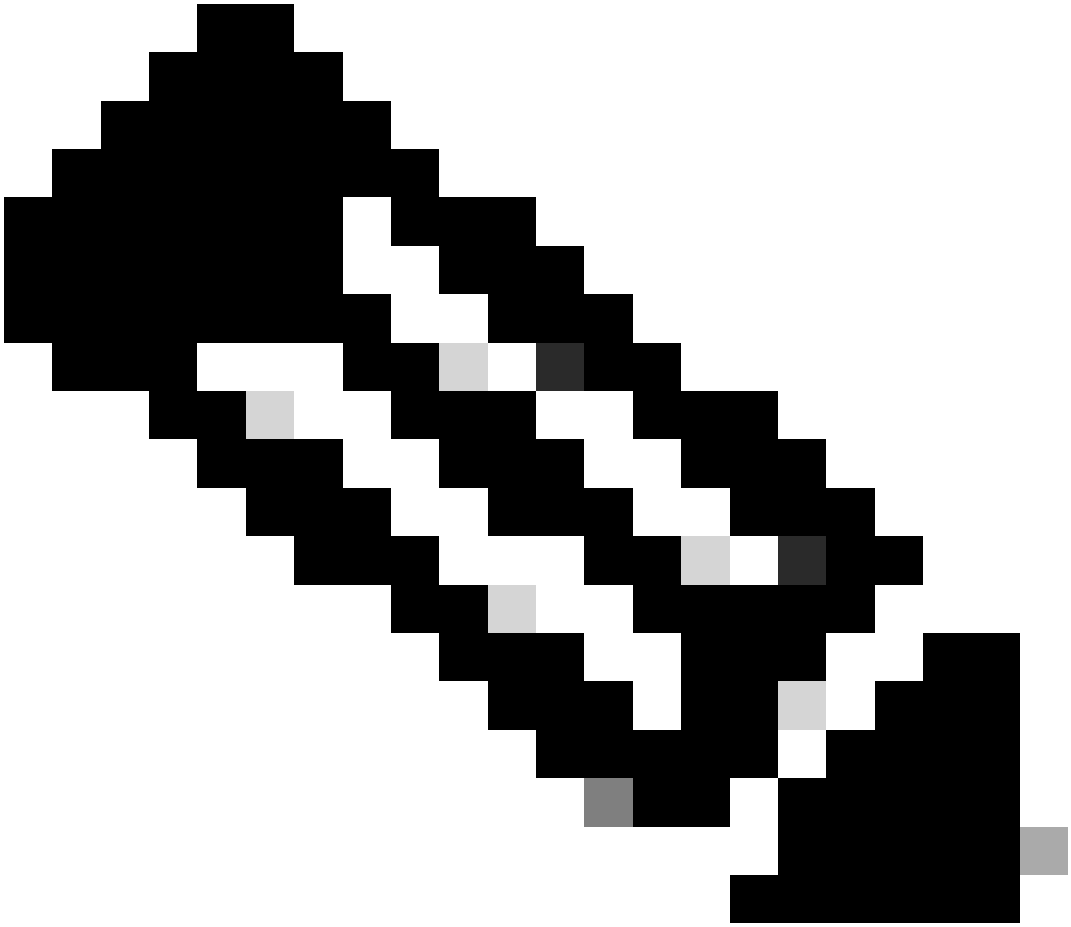
a. 從ASA快閃記憶體檔案系統安裝disk0:/hostscan_4.xx.xxxxx-k9.pkg映像。

b. CheckEnable HostScan。

c. 按一下「Apply」。

動態訪問策略 — 根據定義的AAA和/或終端評估標準，驗證連線使用者及其終端時，必須使用此配置。如果滿足DAP記錄的所定義的標準，那麼可以將與該DAP記錄相關聯的網路資源授予連線使用者訪問許可權。在身份驗證過程中執行DAP授權。

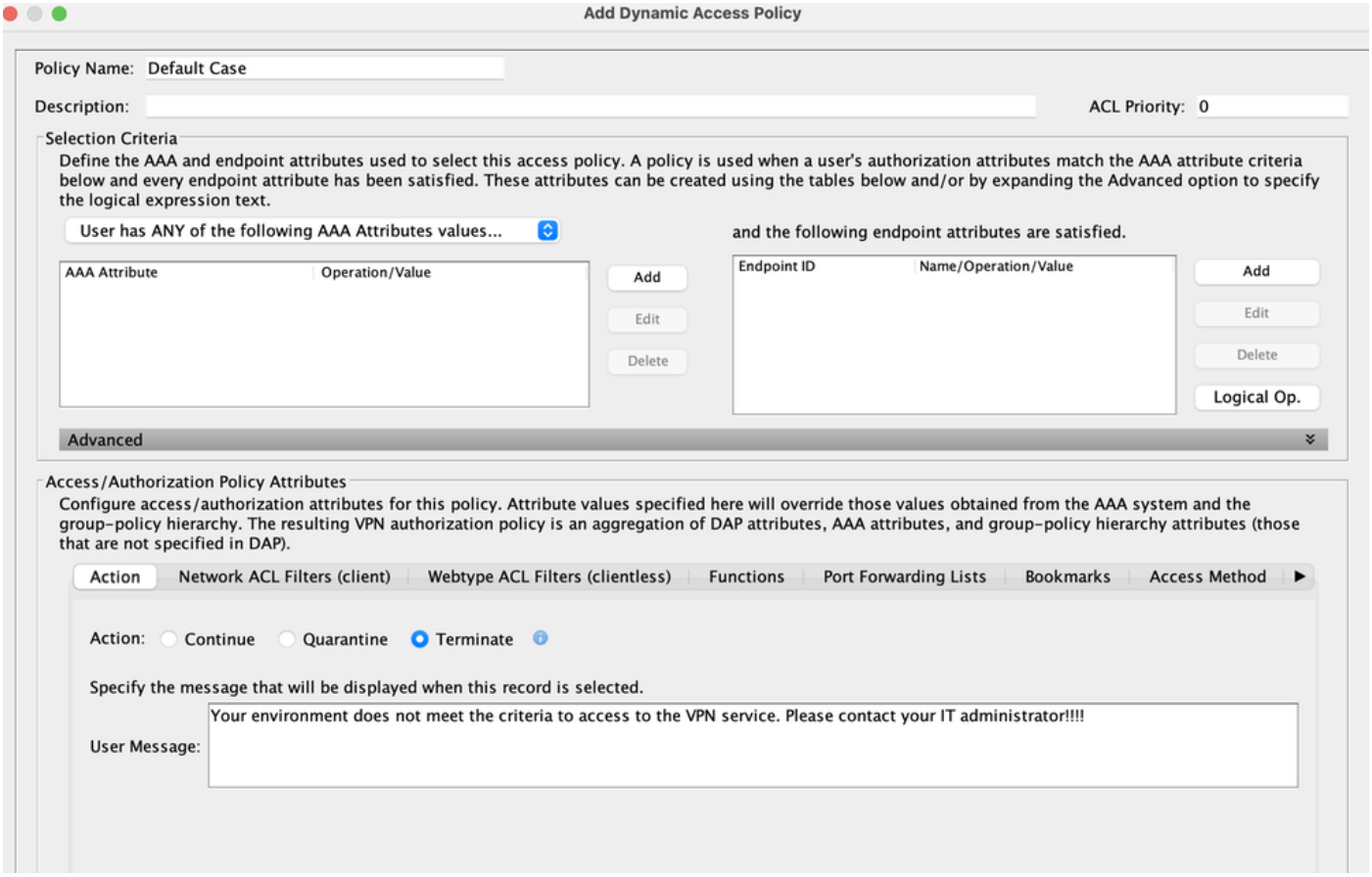
要確保SSL VPN連線可以在預設情況下終止（例如，當終端與任何已配置的動態訪問策略都不匹配時），可以使用以下步驟進行配置：



附註：首次配置動態訪問策略時，將顯示DAP.xml錯誤消息，指示DAP配置檔案(DAP.XML)不存在。修改初始DAP配置並儲存後，此消息將不再顯示。

1. 導覽至Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies，然後配置後續步驟：

圖30.預設動態訪問策略 — 如果未匹配預定義的DAP記錄，則可以強制實施此DAP記錄。因此，可以拒絕SSL VPN訪問。



a. 編輯DfltAccessPolicy並將Action設置為Terminate。

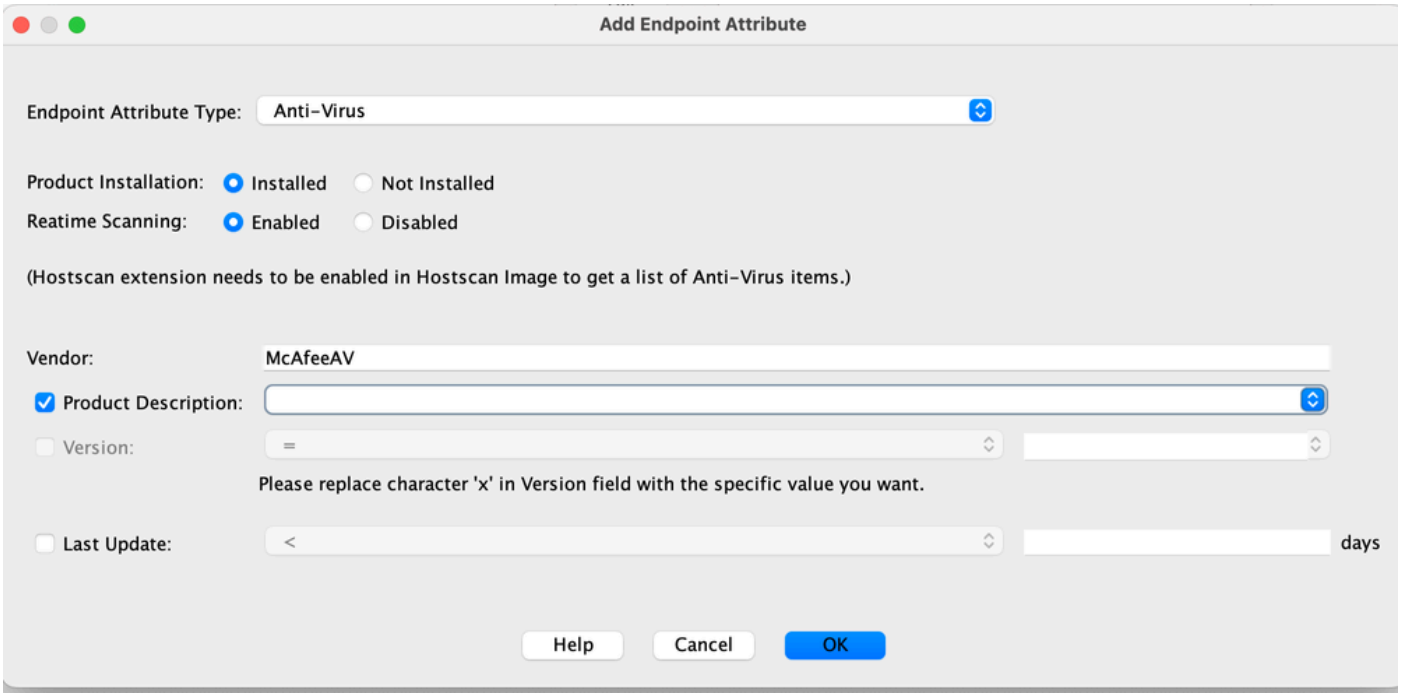
b. 按一下「確定」。

1. 新增名為Managed_Endpoints的新動態訪問策略，如下所示：

    a. 說明：員工客戶端訪問

    b. 如圖31所示新增端點屬性型別（防病毒）。完成時按一下OK。

圖31. DAP端點屬性 — 高級端點評估防病毒可以用作客戶端/網路訪問的DAP標準。



a. 如上一圖所示，從下拉選單AAA Attribute部分中選擇User has ALL of the following AAA Attributes Values。

b. 如圖33和34所示，新增（位於AAA屬性框的右側）AAA屬性型別(LDAP)。完成時按一下確定。

圖33. DAP AAA屬性 — AAA組成員身份可以作為DAP標準來標識員工。

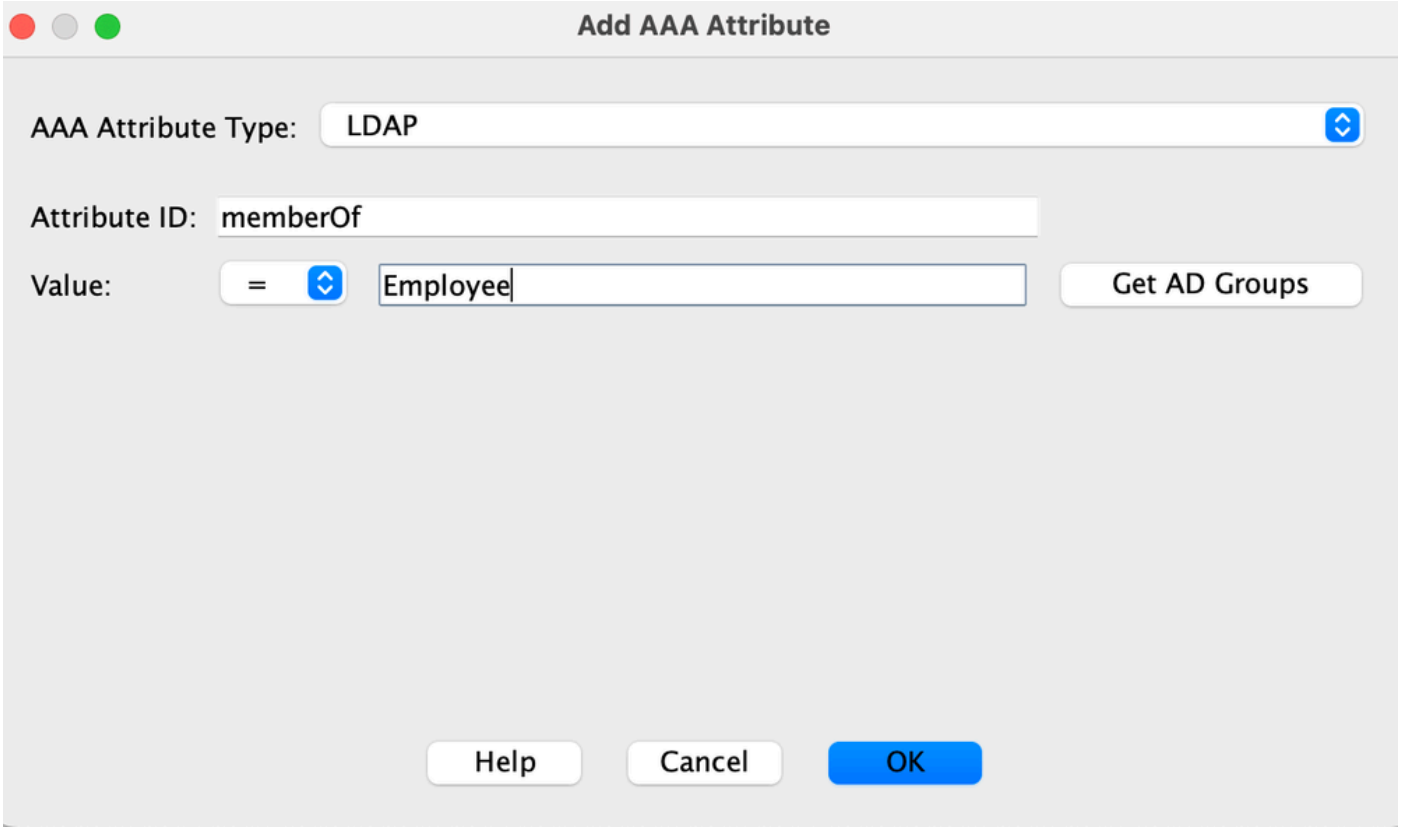
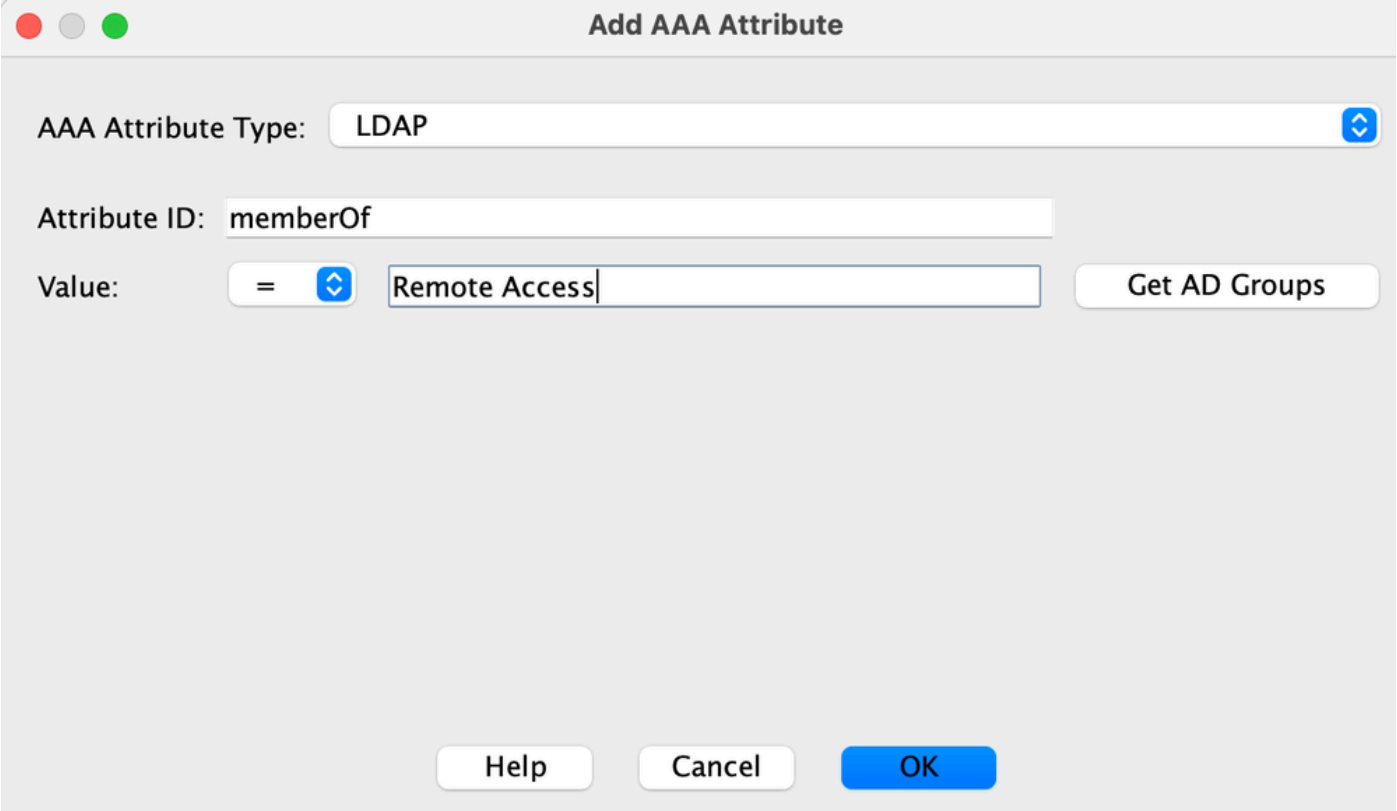
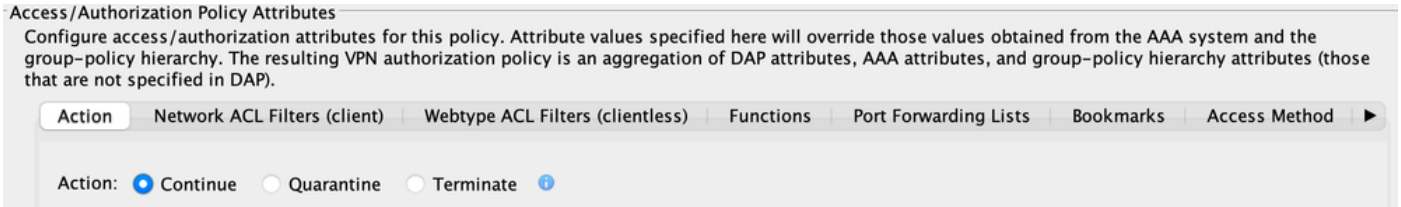


圖34. DAP AAA屬性 — AAA組成員身份可以作為DAP標準以允許遠端訪問功能。



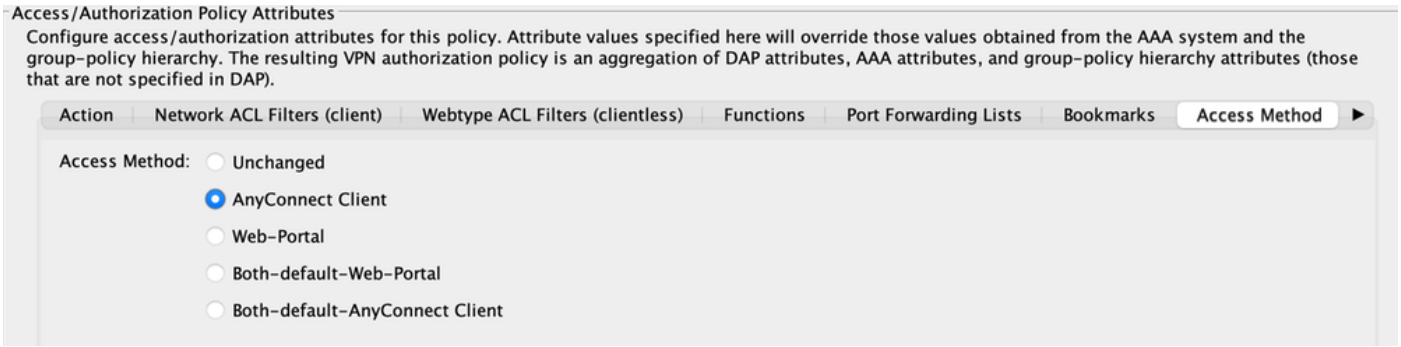
a. 在「Action（操作）」頁籤下，驗證「Action（操作）」是否設定為Continue，如圖35所示。

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。如果匹配了DAP記錄並且操作設定為Terminate ，則可能會拒絕VPN訪問。



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

圖36. Access Method頁籤 — 此配置是定義SSL VPN客戶端連線型別所必需的。



a. 按一下「確定」，然後「應用」。

1. 新增第二個名為Unmanaged_Endpoints的動態訪問策略，如下所述：

a. 描述：員工無客戶端訪問。

b. 在AAA屬性部分上一映像的下拉選單中，選擇User has ALL of the following AAA Attributes Values。

c. 如圖38和39所示，新增（位於AAA屬性型別右側）AAA屬性型別(LDAP)。完成時按一下OK。

圖38. DAP AAA屬性 — AAA組成員身份可用作DAP標準來標識員工。

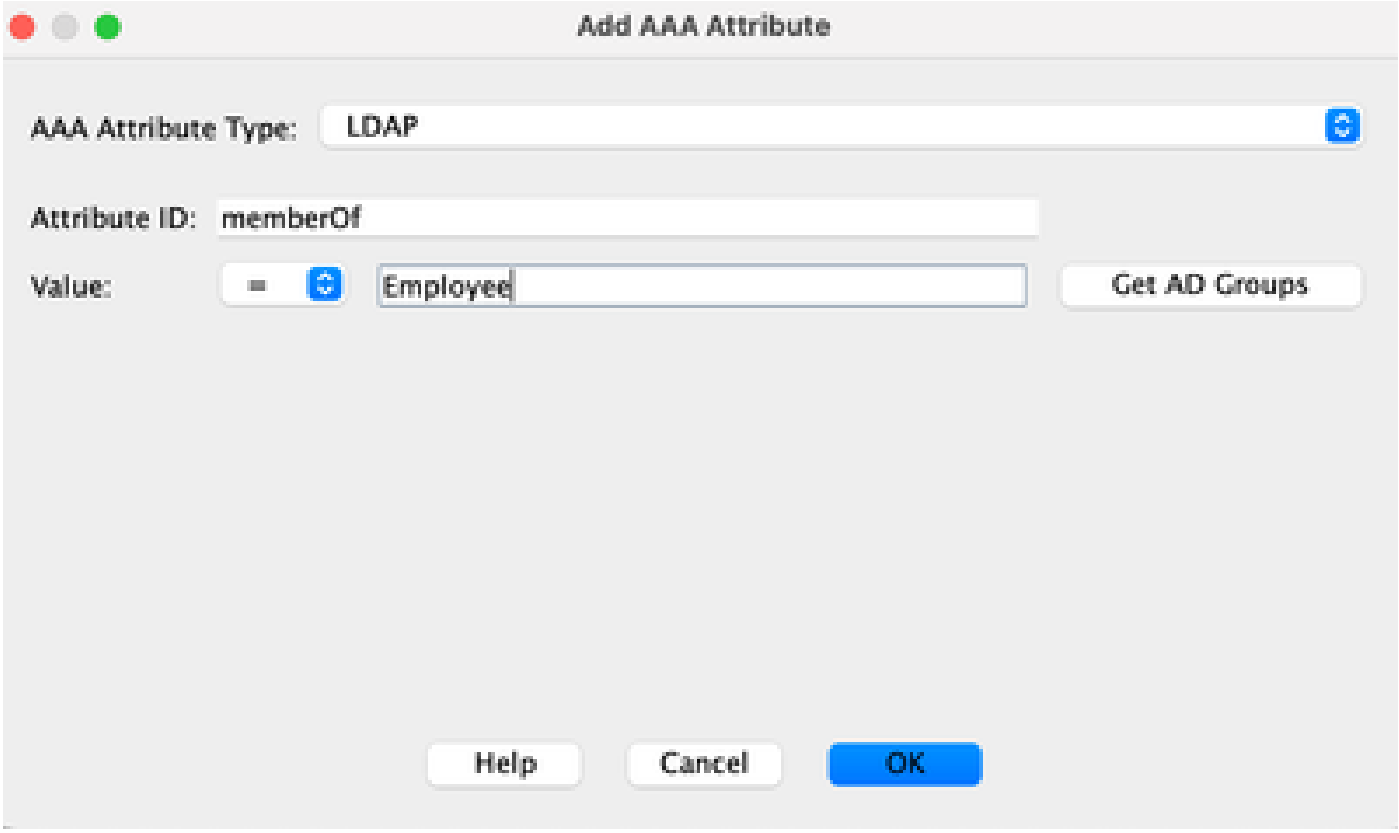
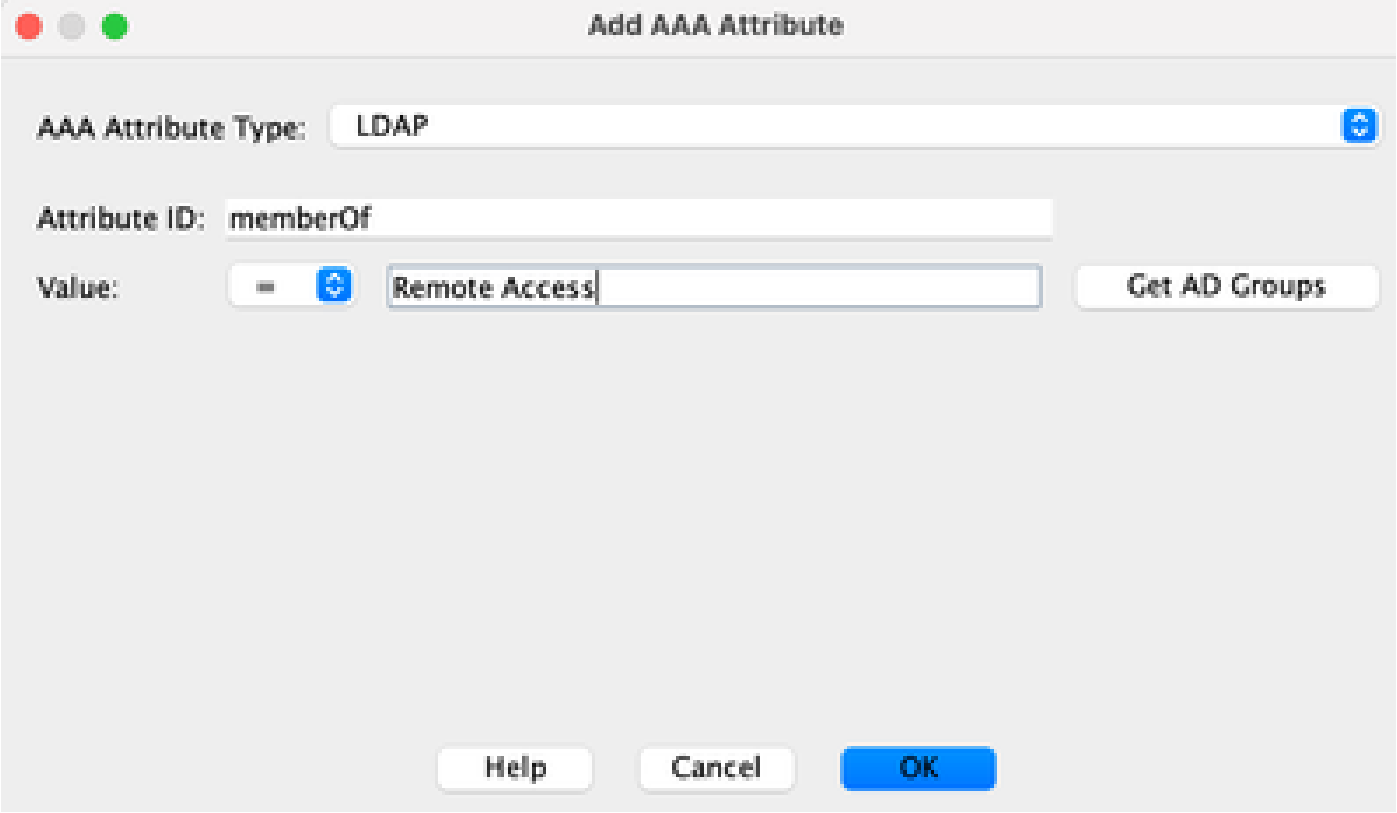


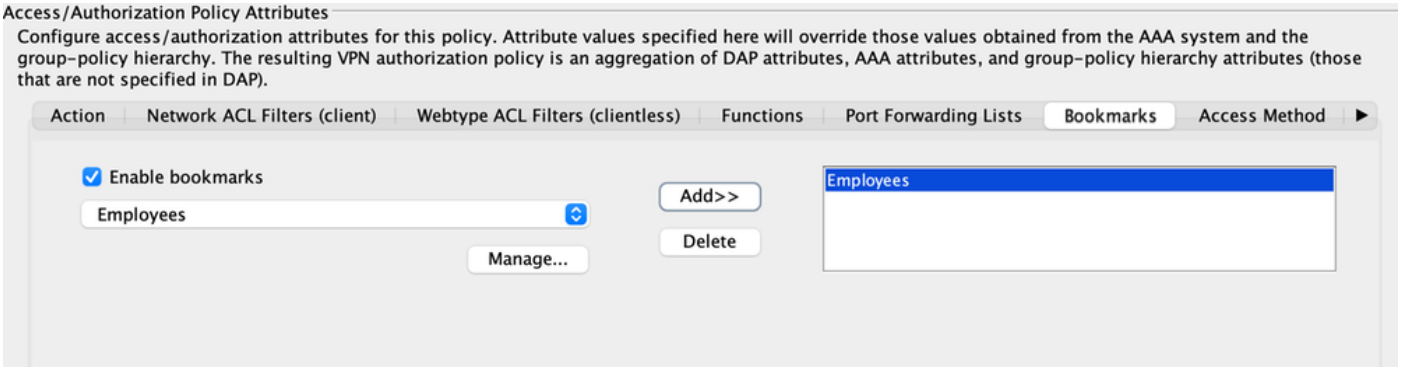
圖39. DAP AAA屬性 — AAA組成員身份可以作為DAP標準以允許遠端訪問功能。



a. 在Action頁籤下，驗證Action是否設定為Continue。(圖 35)

b. 在「書籤」頁籤下，從下拉選單中選擇nameEmployees，然後單擊Add。此外，驗證是否已選中Enable書籤，如圖40所示。

圖40. Bookmarks Tab — 此選項可讓您為使用者會話選擇和配置URL清單。



a. 在「訪問方法」頁籤下，選擇訪問方法Web門戶。(圖 36)

2. 按一下「確定」，然後「應用」。
   1. 承包商只能通過DAP AAA屬性進行識別。因此，端點屬性型別：（策略）無法在步驟4中配置。此方法僅用於顯示DAP中的通用性。

3.新增第三個名為Guest_Access的動態訪問策略，其內容如下：

a. 描述：訪客無客戶端訪問。

b. 如圖37所示，在「端點屬性」(Endpoint Attribute)框的右邊新增端點屬性型別（策略）。完成

時按一下「確定」(OK)。

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

d. 如圖41和42所示，新增（位於AAA屬性框的右側）AAA屬性型別(LDAP)。完成時按一下確定。

圖41.可以使用DAP AAA屬性 — AAA組成員身份作為DAP標準來標識承包商

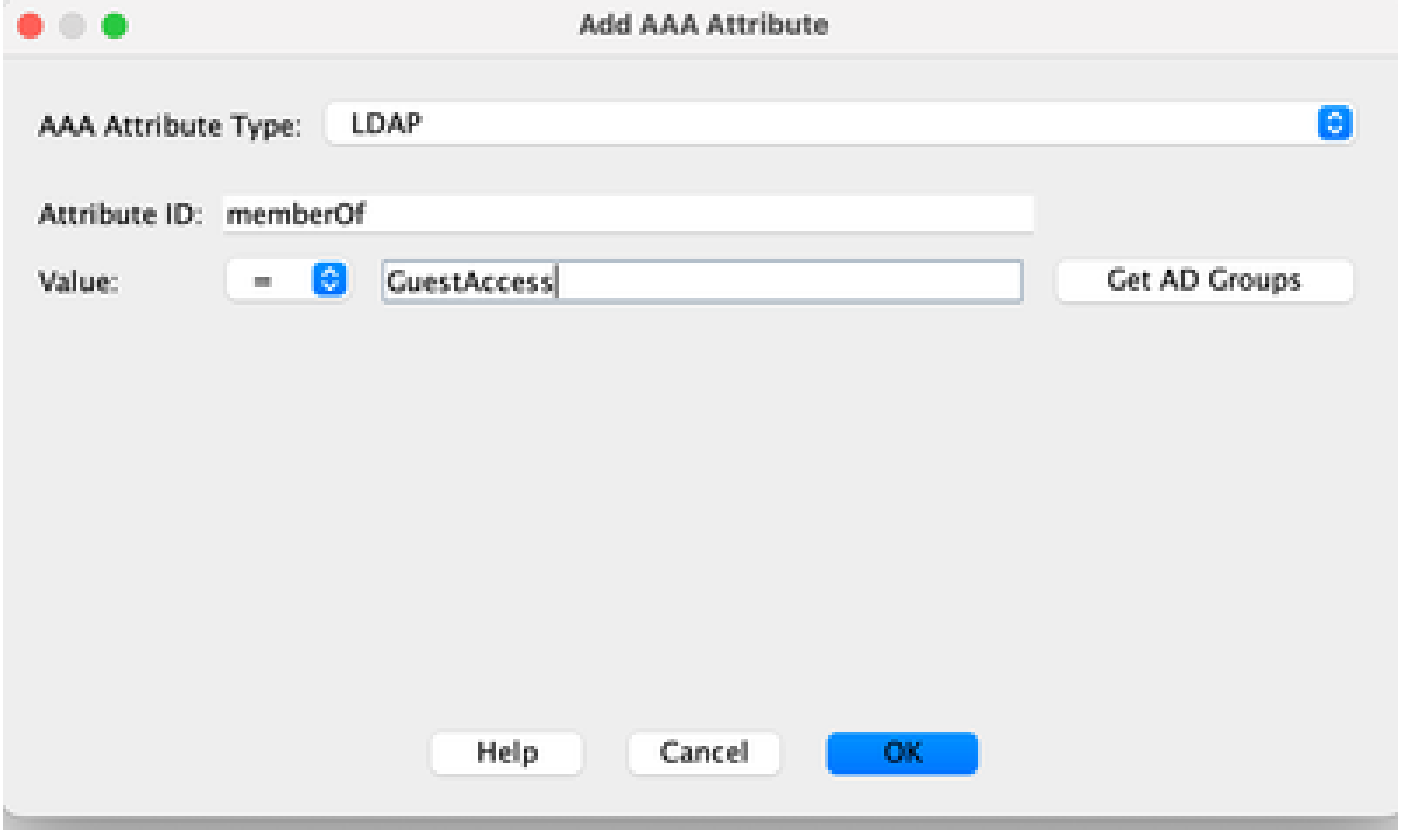
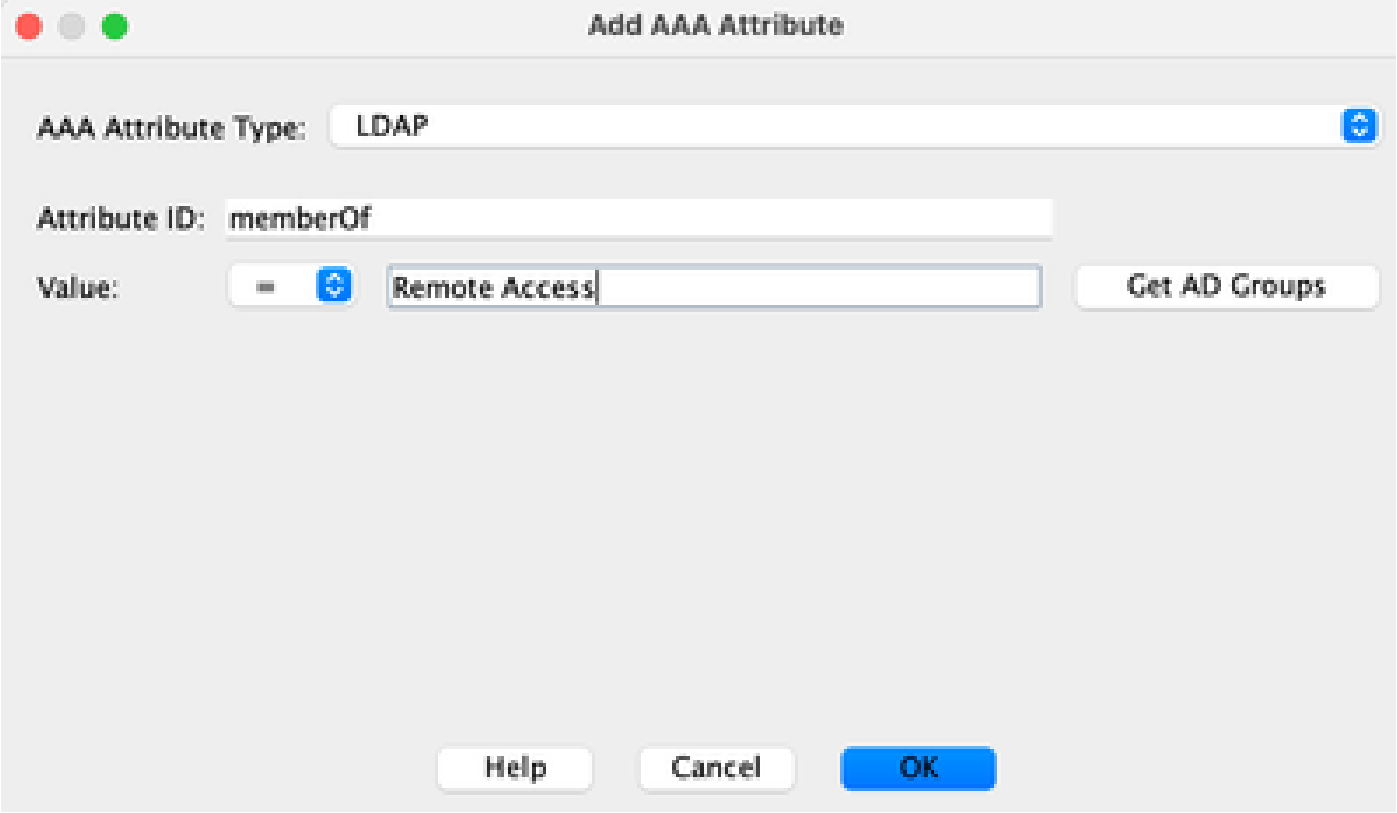


圖42. DAP AAA屬性 — 可以將AAA組成員身份用作DAP標準，以允許遠端訪問功能



a. 在Action頁籤下，驗證Action是否設定為Continue。(圖 35)

b. 在「書籤」頁籤下，從下拉選單中選擇清單名稱Contractors，然後按一下「新增」。此外，驗證Enable書籤是否已選中。（請參見圖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「Apply」。

結論

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

隨著不斷發展變化的動態VPN環境的合併，動態訪問策略可以適應頻繁的Internet配置更改、每個使用者可以在組織內擔任各種角色，以及從具有不同配置和安全級別的託管和非託管遠端訪問站點登入。

動態訪問策略由新的成熟傳統技術作為補充，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為任何網路資源提供安全的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）。