Déployer des politiques d'accès dynamique (DAP) ASA 9.X

Table des matières

Introduction

Ce document décrit le déploiement, les fonctionnalités et l'utilisation des politiques d'accès dynamique (DAP) ASA 9.x.

Conditions préalables

Exigences

Cisco vous recommande de connaître les sujets suivants :

- Passerelles de réseau privé virtuel (VPN)
- Politiques d'accès dynamiques (DAP)

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

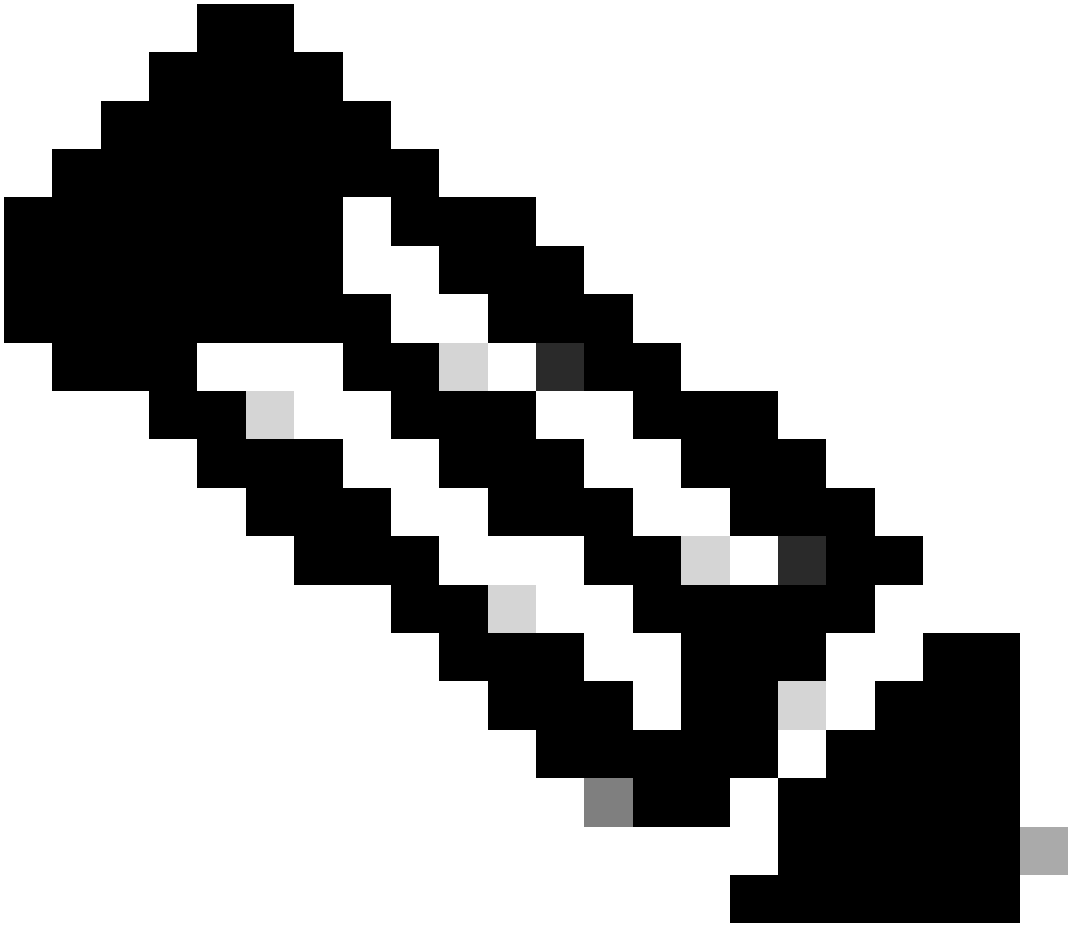
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

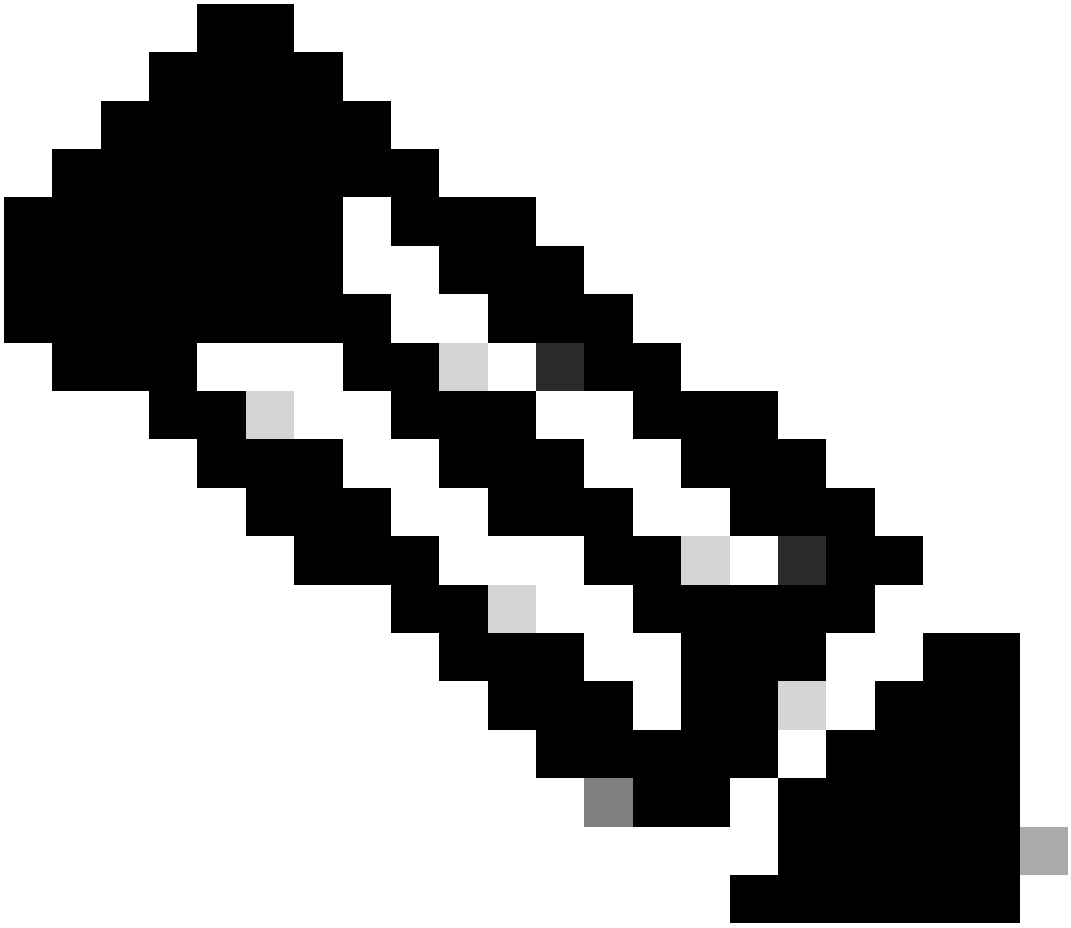
Les passerelles VPN (Virtual Private Network) fonctionnent dans des environnements dynamiques. Plusieurs variables peuvent affecter chaque connexion VPN ; par exemple, les configurations d'intranet qui changent fréquemment, les différents rôles que chaque utilisateur peut occuper au sein d'une organisation et les connexions à partir de sites d'accès à distance avec différentes configurations et différents niveaux de sécurité. La tâche d'autorisation des utilisateurs est beaucoup plus compliquée dans un environnement VPN dynamique que dans un réseau à configuration statique.

Les politiques d'accès dynamique (DAP) sont une fonctionnalité qui vous permet de configurer une autorisation qui répond à la dynamique des environnements VPN. Vous créez une stratégie d'accès dynamique en définissant une collection d'attributs de contrôle d'accès que vous associez à un tunnel ou une session utilisateur spécifique. Ces attributs permettent de résoudre les problèmes d'appartenance à plusieurs groupes et de sécurité des terminaux.

Par exemple, l'appliance de sécurité accorde l'accès à un utilisateur particulier pour une session particulière en fonction des stratégies que vous définissez. Il génère un DAP tout au long de l'authentification des utilisateurs en sélectionnant et/ou en agrégeant des attributs à partir d'un ou plusieurs enregistrements DAP. Il sélectionne ces enregistrements DAP en fonction des informations de sécurité du terminal du périphérique distant et/ou des informations d'autorisation AAA pour l'utilisateur authentifié. Il applique ensuite l'enregistrement DAP au tunnel ou à la session utilisateur.



Remarque : le fichier dap.xml, qui contient les attributs de sélection des stratégies DAP, est stocké dans la mémoire flash ASA. Bien que vous puissiez exporter le fichier dap.xml hors boîte, le modifier (si vous connaissez la syntaxe XML) et le réimporter, soyez très prudent car vous pouvez faire en sorte qu'ASDM arrête le traitement des enregistrements DAP si vous avez mal configuré quelque chose. Il n'existe pas d'interface de ligne de commande pour manipuler cette partie de la configuration.



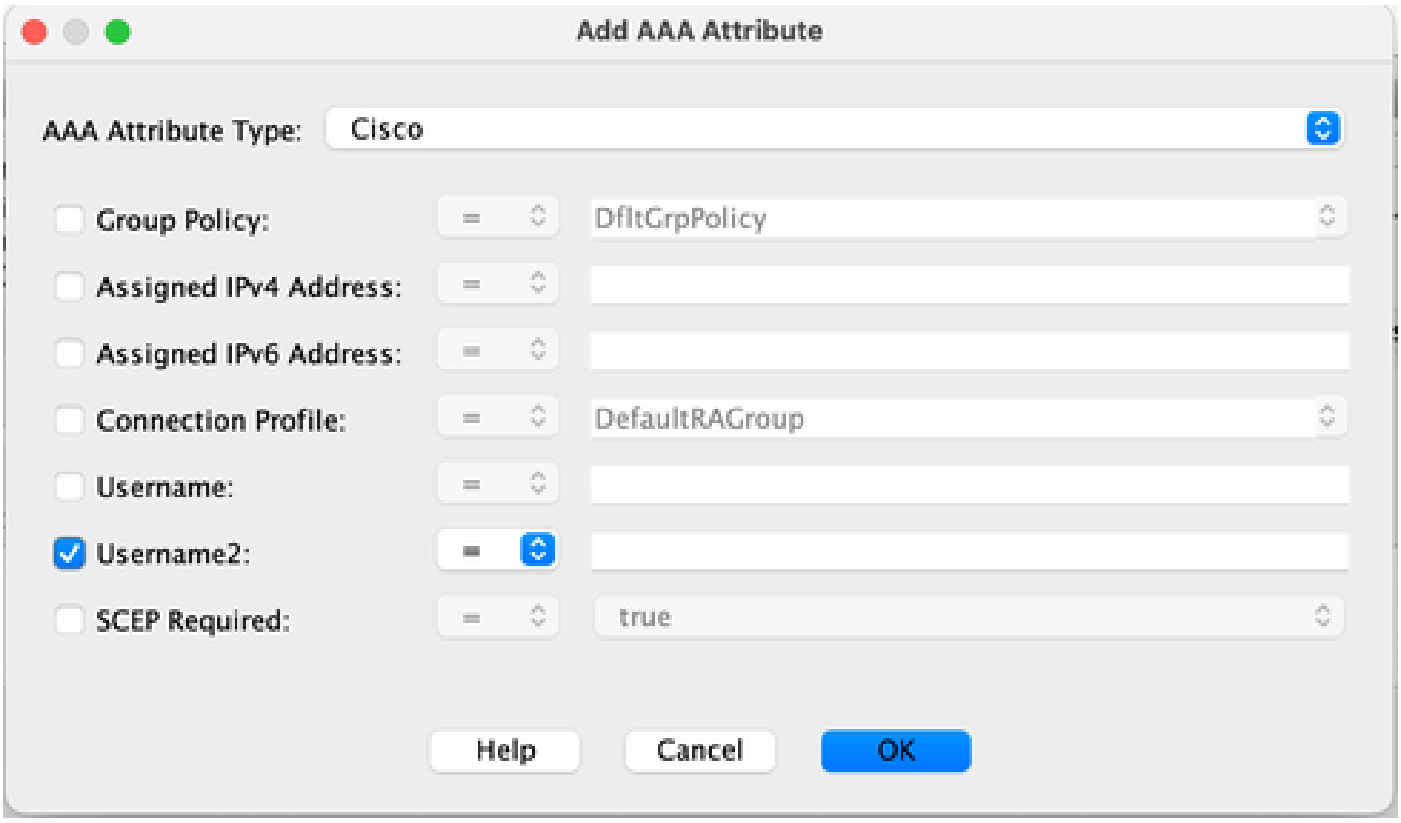
Remarque : si vous essayez de configurer les paramètres d'accès dynamic-access-policy-record via l'interface de ligne de commande, le DAP risque de ne plus fonctionner, bien que l'ASDM puisse gérer correctement ces paramètres. Évitez l'interface de ligne de commande et utilisez toujours l'ASDM pour gérer les politiques DAP.

Attributs DAP et AAA

DAP complète les services AAA et fournit un ensemble limité d'attributs d'autorisation qui peuvent remplacer les attributs fournis par AAA. L'appliance de sécurité peut sélectionner des enregistrements LDAP en fonction des informations d'autorisation AAA de l'utilisateur. L'appliance de sécurité peut sélectionner plusieurs enregistrements DAP en fonction de ces informations, qu'elle regroupe ensuite pour attribuer des attributs d'autorisation DAP.

Vous pouvez spécifier des attributs AAA à partir de la hiérarchie d'attributs AAA de Cisco ou de l'ensemble complet d'attributs de réponse que l'appliance de sécurité reçoit d'un serveur RADIUS ou LDAP, comme illustré à la Figure 1.

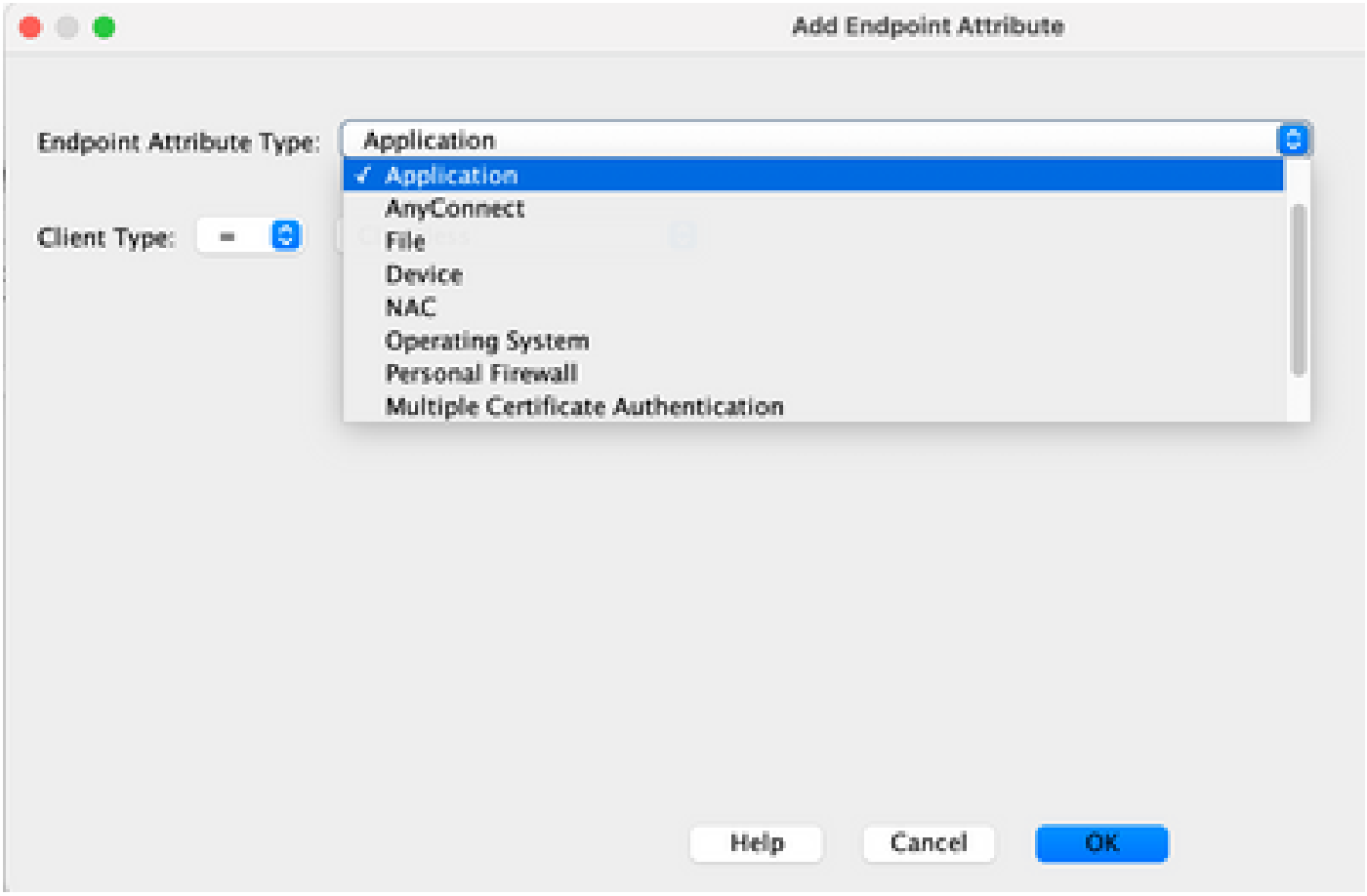
Figure 1. GUI d'attribut AAA DAP



Attributs de sécurité LDAP et des terminaux

Outre les attributs AAA, l'appliance de sécurité peut également obtenir des attributs de sécurité de point de terminaison en utilisant les méthodes d'évaluation de la position que vous configurez. Il s'agit notamment de Basic Host Scan, Secure Desktop, Standard/Advanced Endpoint Assessment et NAC, comme illustré à la Figure 2. Les attributs d'évaluation des terminaux sont obtenus et envoyés au dispositif de sécurité avant l'authentification de l'utilisateur. Cependant, les attributs AAA, y compris l'enregistrement LDAP global, sont validés lors de l'authentification de l'utilisateur.

Figure 2. Interface utilisateur graphique des attributs de terminal

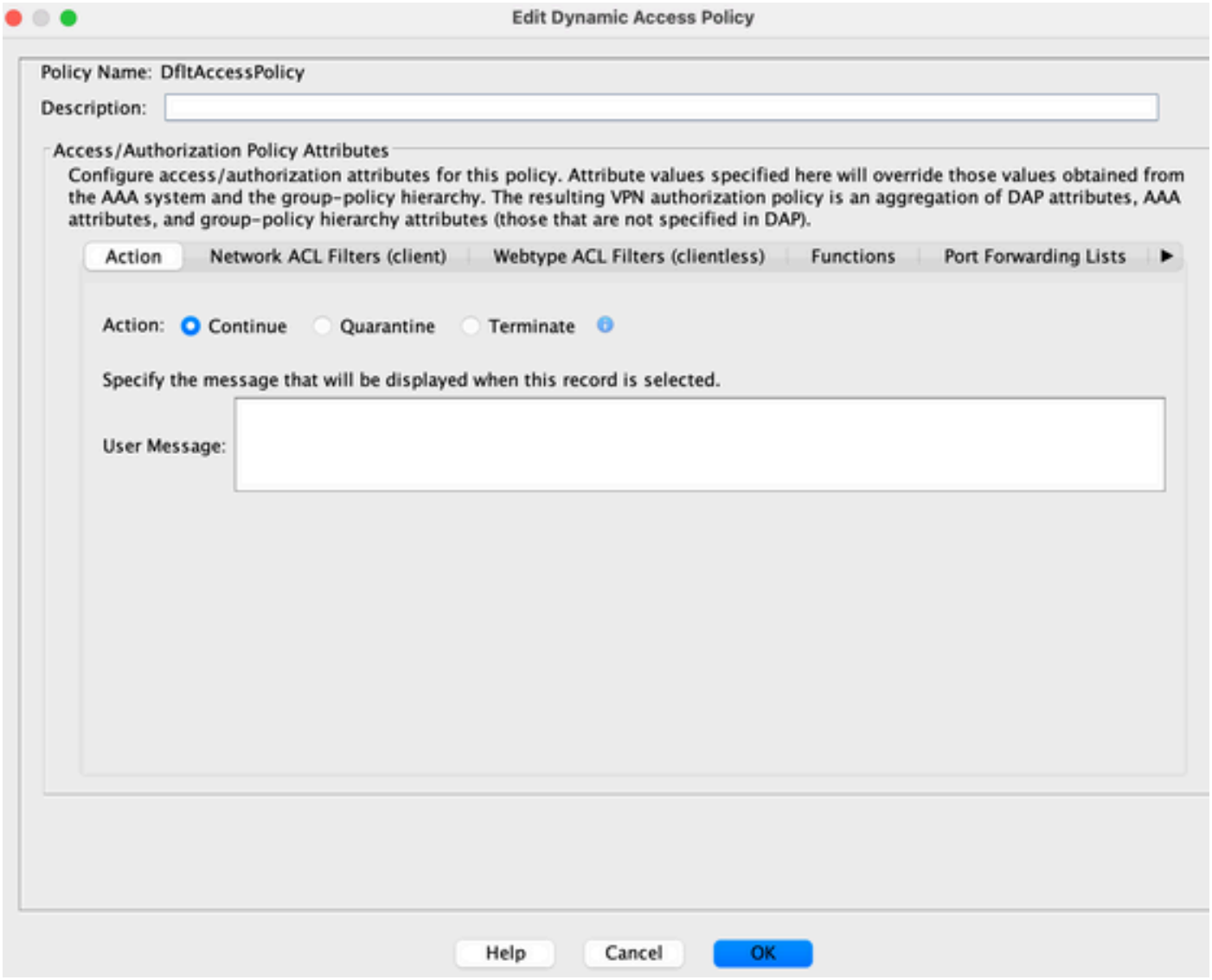


Stratégie d'accès dynamique par défaut

Avant l'introduction et l'implémentation de DAP, les paires attribut/valeur de stratégie d'accès qui étaient associées à un tunnel ou une session utilisateur spécifique étaient définies localement sur l'ASA (c'est-à-dire, les groupes de tunnels et les stratégies de groupe) ou mappées via des serveurs AAA externes.

DAP est toujours appliqué par défaut. Par exemple, l'application du contrôle d'accès via les groupes de tunnels, les stratégies de groupe et AAA sans l'application explicite de DAP peut encore obtenir ce comportement. Pour le comportement hérité, aucune modification de configuration de la fonctionnalité DAP, y compris l'enregistrement DAP par défaut, DfltAccessPolicy, n'est requise, comme illustré à la Figure 3.

Figure 3. Stratégie d'accès dynamique par défaut



Néanmoins, si l'une des valeurs par défaut d'un enregistrement DAP est modifiée, par exemple, le paramètre Action : dans DfltAccessPolicy est modifié de sa valeur par défaut à Terminate et des enregistrements DAP supplémentaires ne sont pas configurés, les utilisateurs authentifiés peuvent, par défaut, correspondre à l'enregistrement DAP DfltAccessPolicy et peuvent se voir refuser l'accès VPN.

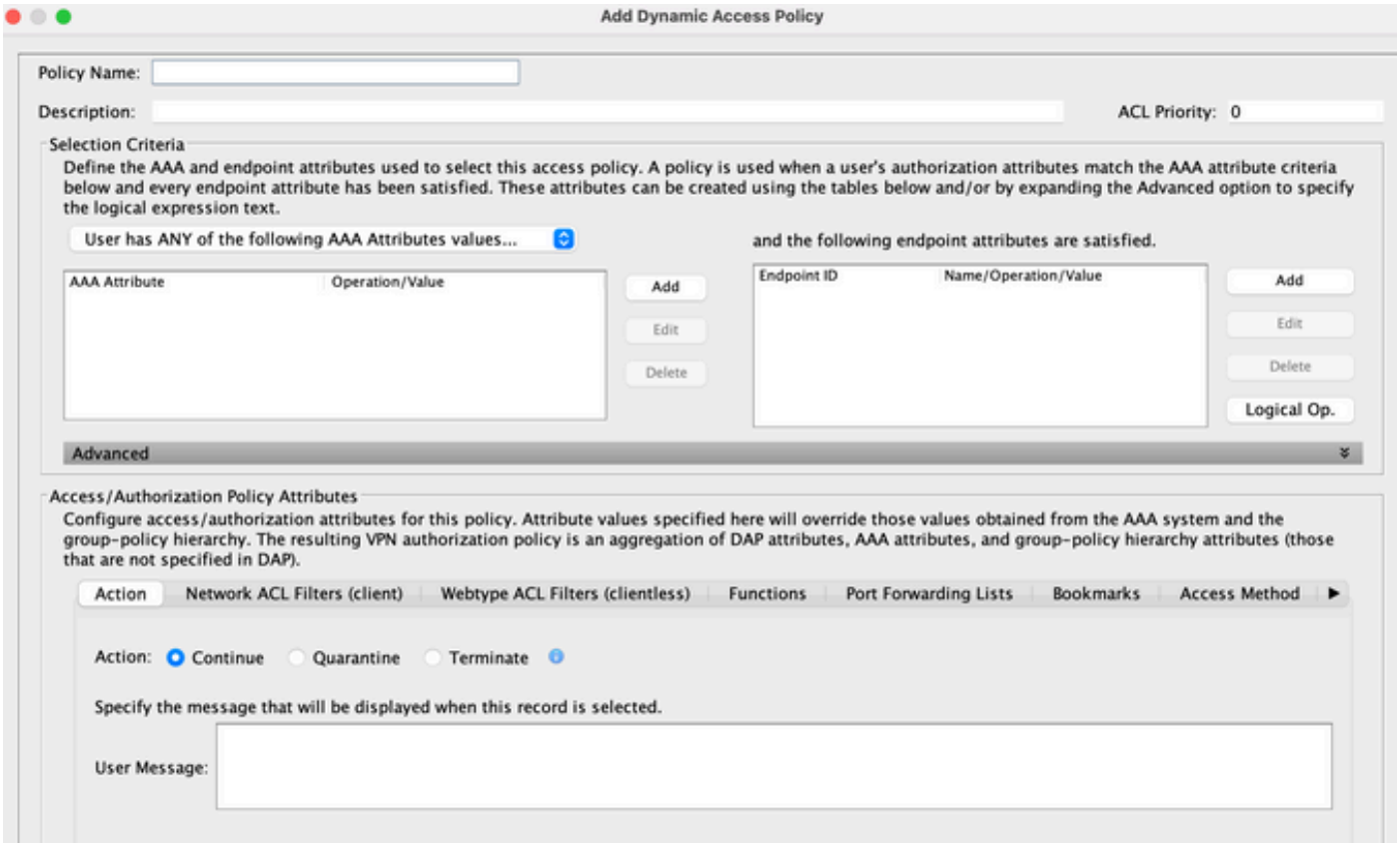
Par conséquent, un ou plusieurs enregistrements DAP doivent être créés et configurés pour autoriser la connectivité VPN et définir les ressources réseau auxquelles un utilisateur authentifié est autorisé à accéder. Ainsi, le protocole DAP, s'il est configuré, peut avoir la priorité sur l'application des politiques héritées.

Configurer les stratégies d'accès dynamique

Lorsque vous utilisez DAP pour définir les ressources réseau auxquelles un utilisateur a accès, il y a de nombreux paramètres à prendre en compte. Par exemple, si vous déterminez si le point d'extrémité de connexion provient d'un environnement géré, non géré ou non approuvé, déterminez les critères de sélection nécessaires pour identifier le point d'extrémité de connexion et, en fonction de l'évaluation du point d'extrémité et/ou des informations d'identification AAA, quelles ressources réseau l'utilisateur qui se connecte est autorisé à accéder. Pour ce faire, vous

devez d'abord vous familiariser avec les fonctionnalités et les fonctions LDAP, comme illustré à la Figure 4.

Figure 4. Politique d'accès dynamique



Lors de la configuration d'un enregistrement DAP, deux composants principaux doivent être pris en compte :

- Critères de sélection, y compris options avancées
- Attributs de stratégie d'accès

La section Critères de sélection permet à un administrateur de configurer les attributs AAA et Endpoint utilisés pour sélectionner un enregistrement DAP spécifique. Un enregistrement DAP est utilisé lorsque les attributs d'autorisation d'un utilisateur correspondent aux critères d'attribut AAA et que chaque attribut de point de terminaison a été satisfait.

Par exemple, si le type d'attribut AAA LDAP (Active Directory) est sélectionné, la chaîne Nom d'attribut est memberOf et la chaîne Valeur est Contractors, comme illustré dans la Figure 5a, l'utilisateur authentifiant doit être membre du groupe Active Directory Contractors pour correspondre aux critères d'attribut AAA.

En plus de satisfaire aux critères d'attribut AAA, l'utilisateur authentifiant peut également être tenu de satisfaire aux critères d'attribut de point d'extrémité. Par exemple, si l'administrateur a configuré pour déterminer la position du point d'extrémité de connexion et sur la base de cette évaluation de la position, il peut alors utiliser ces informations d'évaluation comme critères de sélection pour l'attribut de point d'extrémité illustré à la Figure 5b.

Figure 5a. Critères d'attribut AAA

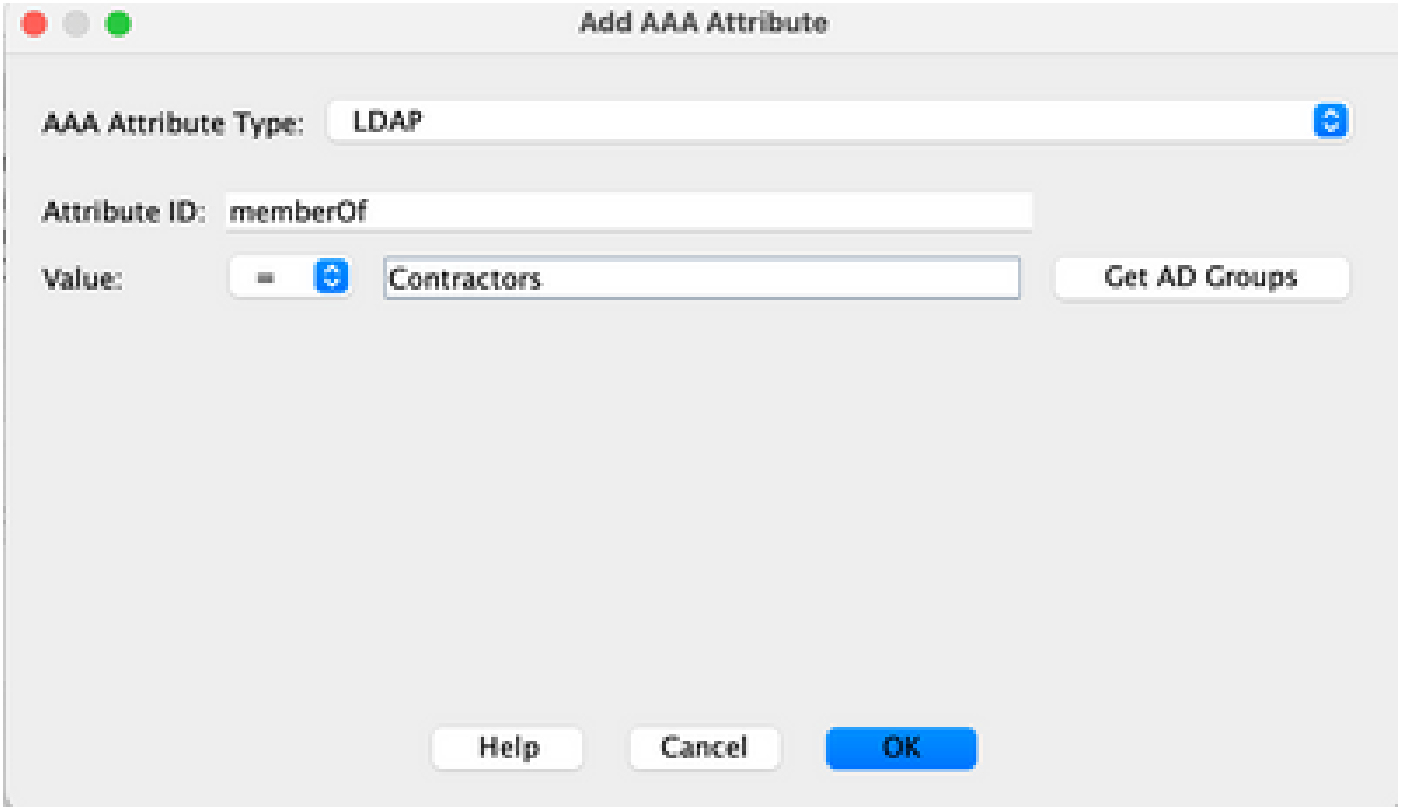


Figure 5b. Critères d'attribut Endpoint

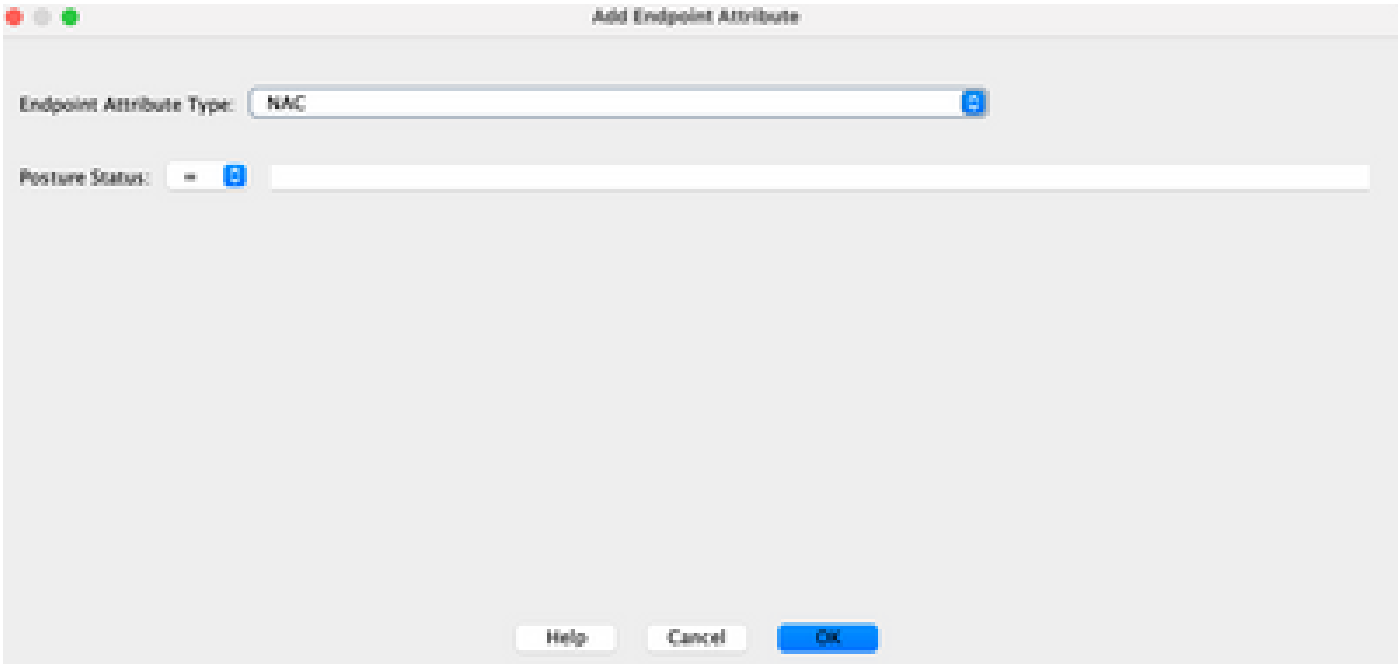
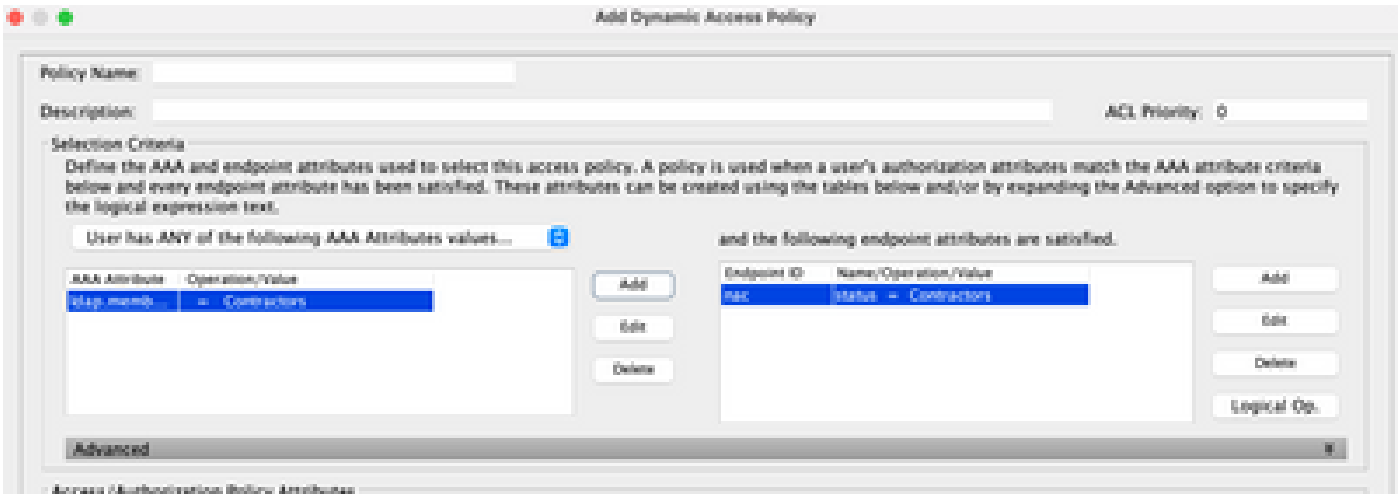


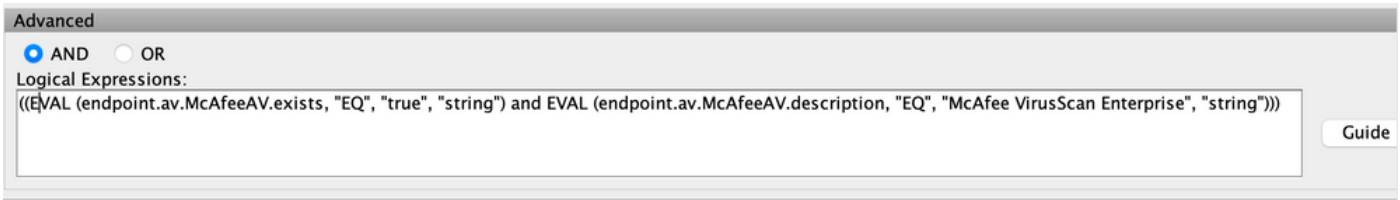
Figure 6. Les critères d'attribut AAA et Endpoint correspondent



Les attributs AAA et Endpoint peuvent être créés à l'aide des tables décrites dans la Figure 6 et/ou en développant l'option Avancé pour spécifier une expression logique, comme illustré dans la Figure 7. Actuellement, l'expression logique est construite avec des fonctions EVAL, par exemple, EVAL (endpoint.av.McAfeeAV.exists, "EQ", "true", "string") et EVAL (endpoint.av.McAfeeAV.description, "EQ", "McAfee VirusScan Enterprise", "string"), qui représentent des opérations logiques de sélection AAA et/ou de point d'extrémité.

Les expressions logiques sont utiles si vous devez ajouter des critères de sélection autres que ce qui est possible dans les zones d'attributs AAA et de point de terminaison, comme indiqué précédemment. Par exemple, bien que vous puissiez configurer les appliances de sécurité pour qu'elles utilisent des attributs AAA qui répondent à n'importe quel critère, à tous les critères ou à aucun des critères spécifiés, les attributs des points de terminaison sont cumulatifs et doivent tous être satisfaits. Pour permettre à l'appliance de sécurité d'utiliser un attribut de point de terminaison ou un autre, vous devez créer des expressions logiques appropriées sous la section Advanced de l'enregistrement DAP.

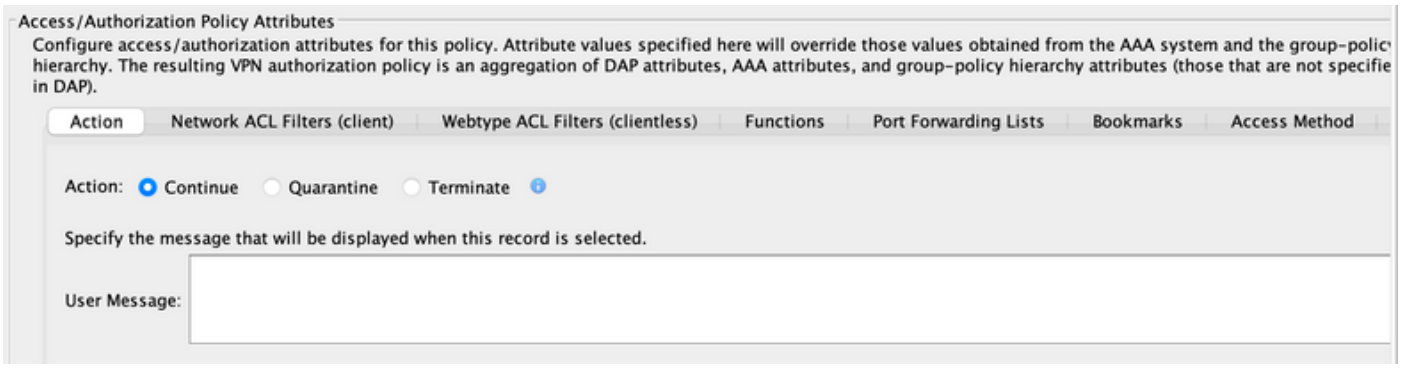
Figure 7. Interface utilisateur graphique Expression logique pour la création d'attributs avancés



La section Access Policy Attributes (Attributs de stratégie d'accès), illustrée à la Figure 8, permet à un administrateur de configurer les attributs d'accès VPN pour un enregistrement DAP spécifique. Lorsqu'un attribut d'autorisation d'utilisateur correspond aux critères AAA, Endpoint et/ou Expression logique, les valeurs d'attribut de stratégie d'accès configurées dans cette section peuvent être appliquées. Les valeurs d'attribut spécifiées ici peuvent remplacer les valeurs obtenues à partir du système AAA, y compris celles des enregistrements d'utilisateur, de groupe, de groupe de tunnel et de groupe par défaut existants.

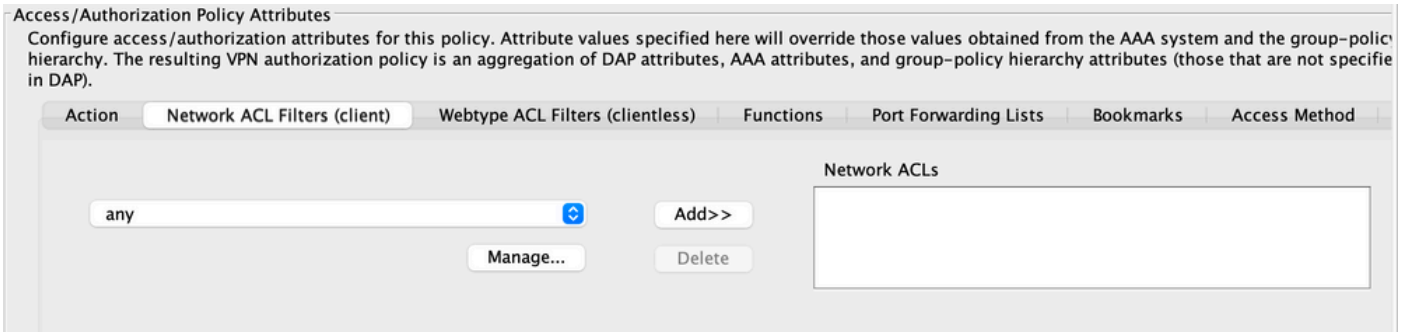
Un enregistrement DAP possède un ensemble limité de valeurs d'attribut qui peuvent être configurées. Ces valeurs se trouvent sous les onglets, comme illustré aux figures 8 à 14 :

Figure 8. Action : spécifie le traitement spécial à appliquer à une connexion ou une session spécifique.



- Continuer : (par défaut) cliquez sur ce bouton pour appliquer les attributs de stratégie d'accès à la session.
- Terminate : cliquez sur ce bouton pour terminer la session.
- User Message : saisissez un message texte à afficher sur la page du portail lorsque cet enregistrement DAP est sélectionné. 128 caractères maximum. Un message utilisateur s'affiche sous forme d'orbe jaune. Lorsqu'un utilisateur se connecte, il clignote trois fois pour attirer l'attention, puis il reste immobile. Si plusieurs enregistrements DAP sont sélectionnés et que chacun d'eux comporte un message utilisateur, tous les messages utilisateur s'affichent. En outre, vous pouvez inclure dans ces messages des URL ou d'autres textes incorporés, qui exigent que vous utilisiez les balises HTML correctes.

Figure 9. Onglet Network ACL Filters : permet de sélectionner et de configurer les listes de contrôle d'accès réseau à appliquer à cet enregistrement LDAP. Une liste de contrôle d’accès pour DAP peut contenir des règles d’autorisation ou de refus, mais pas les deux. Si une liste de contrôle d’accès contient des règles d’autorisation et de refus, l’appliance de sécurité rejette la configuration de la liste.

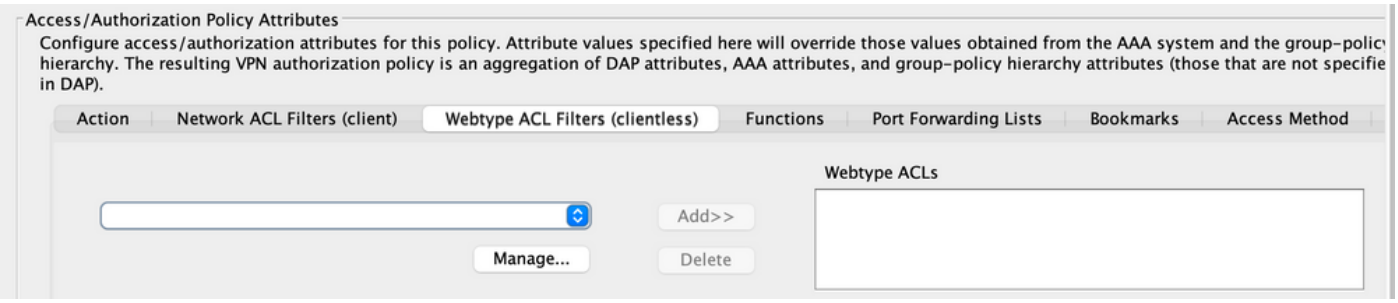


- La zone déroulante ACL réseau contient les ACL réseau déjà configurées à ajouter à cet enregistrement DAP. Seules les listes de contrôle d’accès qui ont toutes les règles d’autorisation ou de refus sont éligibles, et ce sont les seules listes qui s’affichent ici.
- Manage : cliquez sur ce bouton pour ajouter, modifier et supprimer des listes de contrôle d'accès réseau.
- La liste de contrôle d'accès réseau répertorie les listes de contrôle d'accès réseau pour cet

enregistrement DAP.

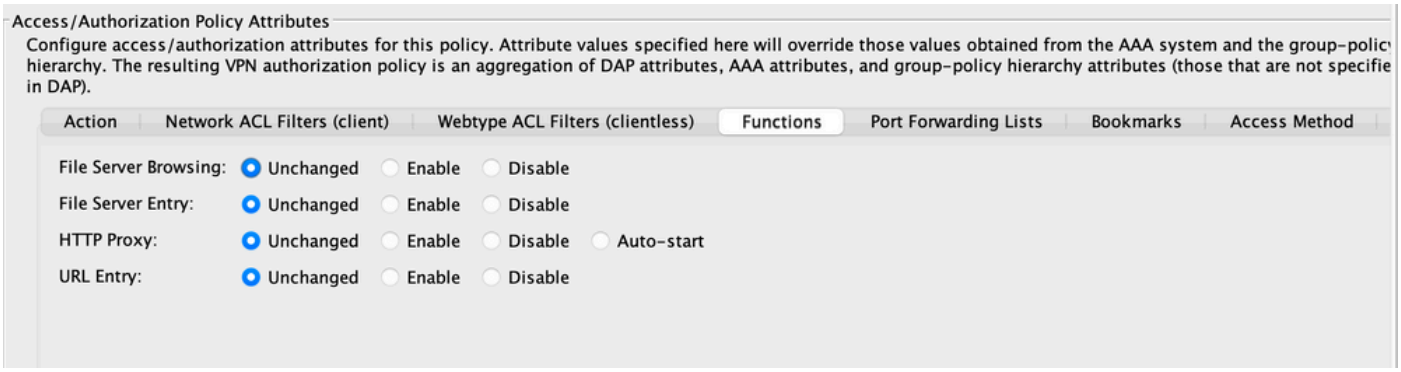
- Add : cliquez sur ce bouton pour ajouter la liste de contrôle d'accès réseau sélectionnée dans la liste déroulante de droite.
- Delete : cliquez sur ce bouton pour supprimer une liste de contrôle d'accès réseau mise en surbrillance de la liste ACL réseau. Vous ne pouvez pas supprimer une liste de contrôle d'accès si elle est attribuée à un DAP ou à un autre enregistrement.

Figure 10. Onglet Web-Type ACL Filters - Permet de sélectionner et de configurer des listes de contrôle d'accès de type Web à appliquer à cet enregistrement DAP. Une liste de contrôle d’accès pour DAP ne peut contenir que des règles d’autorisation ou de refus. Si une liste de contrôle d’accès contient des règles d’autorisation et de refus, l’appliance de sécurité rejette la configuration de la liste.



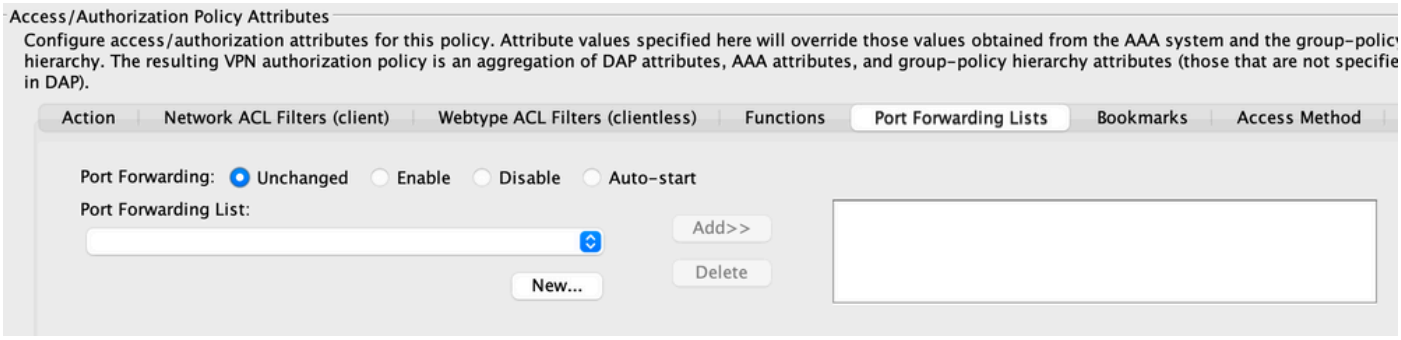
- Liste déroulante ACL de type Web : sélectionnez les ACL de type Web déjà configurées à ajouter à cet enregistrement DAP. Seules les listes de contrôle d’accès comportant toutes les règles d’autorisation ou de refus sont éligibles, et ce sont les seules listes qui s’affichent ici.
- Manage... — Cliquez pour ajouter, modifier et supprimer des listes de contrôle d'accès de type Web.
- Web-Type ACL list : affiche les listes de contrôle d'accès de type Web pour cet enregistrement DAP.
- Ajouter : cliquez sur ce bouton pour ajouter la liste de contrôle d'accès de type Web sélectionnée dans la liste déroulante à droite.
- Delete : cliquez sur ce bouton pour supprimer une liste de contrôle d'accès de type Web de la liste des listes de contrôle d'accès de type Web. Vous ne pouvez pas supprimer une liste de contrôle d'accès si elle est attribuée à un DAP ou à un autre enregistrement.

Figure 11. Onglet Fonctions : permet de configurer l'entrée et la navigation sur le serveur de fichiers, le proxy HTTP et l'entrée d'URL pour l'enregistrement DAP.



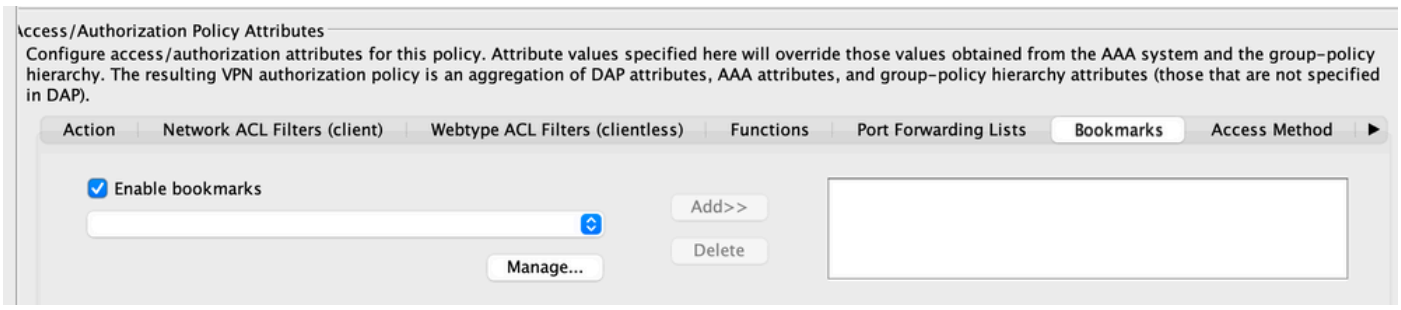
- File Server Browsing : active ou désactive la navigation CIFS pour les serveurs de fichiers ou les fonctionnalités de partage.
- File Server Entry : autorise ou interdit à un utilisateur d'entrer les chemins d'accès et les noms des serveurs de fichiers sur la page du portail. Lorsque cette option est activée, place le tiroir d'entrées du serveur de fichiers sur la page du portail. Les utilisateurs peuvent entrer directement les chemins d'accès aux fichiers Windows. Ils peuvent télécharger, modifier, supprimer, renommer et déplacer des fichiers. Ils peuvent également ajouter des fichiers et des dossiers. Les partages doivent également être configurés pour l'accès utilisateur sur les serveurs Microsoft Windows applicables. Les utilisateurs peuvent être obligés de s'authentifier avant d'accéder aux fichiers, selon les besoins du réseau.
- Proxy HTTP : affecte le transfert d'un proxy d'applet HTTP au client. Le proxy est utile pour les technologies qui interfèrent avec la transformation de contenu appropriée, telles que Java, ActiveX et Flash. Il contourne le processus de manipulation/réécriture tout en assurant l'utilisation continue de l'appliance de sécurité. Le proxy transféré modifie automatiquement l'ancienne configuration de proxy du navigateur et redirige toutes les requêtes HTTP et HTTPS vers la nouvelle configuration de proxy. Il prend en charge pratiquement toutes les technologies côté client, notamment HTML, CSS, JavaScript, VBScript, ActiveX et Java. Le seul navigateur pris en charge est Microsoft Internet Explorer.
- Entrée d'URL : permet ou empêche un utilisateur d'entrer des URL HTTP/HTTPS sur la page du portail. Si cette fonctionnalité est activée, les utilisateurs peuvent entrer des adresses Web dans la zone de saisie d'URL et utiliser le VPN SSL sans client pour accéder à ces sites Web.
- Unchanged : (valeur par défaut) cliquez sur cette option pour utiliser les valeurs de la stratégie de groupe qui s'applique à cette session.
- Enable/Disable : cliquez sur ce bouton pour activer ou désactiver la fonction.
- Auto-start : cliquez sur cette option pour activer le proxy HTTP et faire en sorte que l'enregistrement DAP lance automatiquement les applets associés à ces fonctionnalités.

Figure 12. Onglet Listes de transfert de connexion — Permet de sélectionner et de configurer des listes de transfert de connexion pour les sessions utilisateur.



- Port Forwarding : sélectionnez une option pour les listes de transfert de port qui s'appliquent à cet enregistrement DAP. Les autres attributs de ce champ sont activés uniquement lorsque vous définissez le transfert de port sur Activer ou Démarrage automatique.
- Unchanged : cliquez sur ce bouton pour utiliser les valeurs de la stratégie de groupe qui s'applique à cette session.
- Enable/Disable : cliquez sur ce bouton pour activer ou désactiver le transfert de port.
- Auto-start : cliquez sur ce bouton pour activer le transfert de port et pour que l'enregistrement DAP lance automatiquement les applets de transfert de port associés à ses listes de transfert de port.
- Zone déroulante Port Forwarding List : sélectionnez les listes de transfert de port déjà configurées à ajouter à l'enregistrement DAP.
- New : cliquez sur ce bouton pour configurer de nouvelles listes de transfert de port.
- Port Forwarding Lists : affiche la liste de transfert de port pour l'enregistrement DAP.
- Add : cliquez sur ce bouton pour ajouter la liste de transfert de port sélectionnée de la liste déroulante à la liste de transfert de port de droite.
- Delete : cliquez sur ce bouton pour supprimer la liste de transfert de port sélectionnée de la liste de transfert de port. Vous ne pouvez pas supprimer une liste de contrôle d'accès si elle est attribuée à un DAP ou à un autre enregistrement.

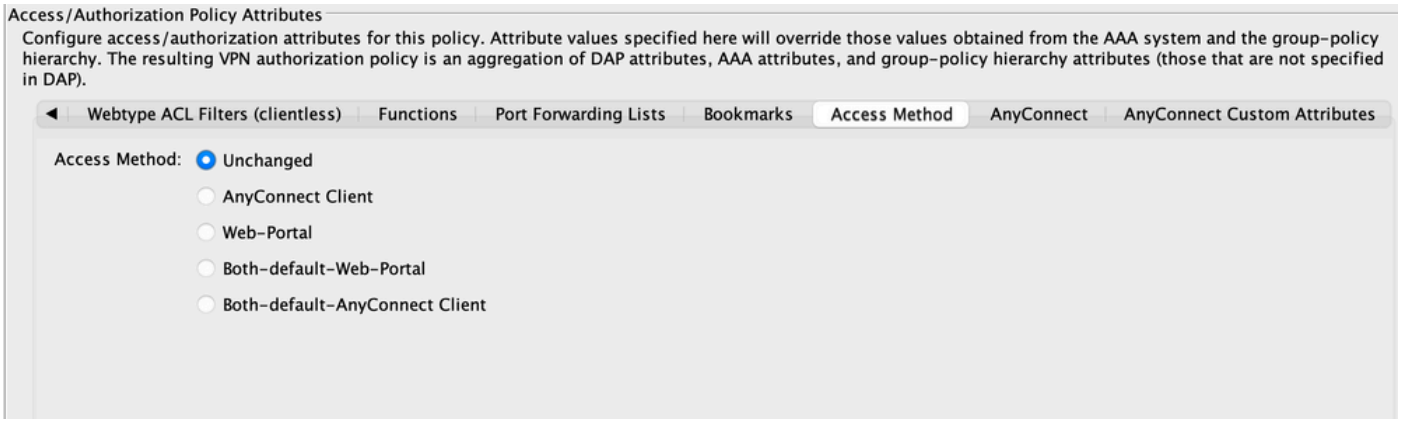
Figure 13. Onglet Signets : vous permet de sélectionner et de configurer des signets/listes d'URL pour les sessions utilisateur.



- Activer les signets : cliquez sur cette option pour l'activer. Lorsque cette case n'est pas cochée, aucune liste de signets ne s'affiche sur la page du portail pour la connexion

- Gérer : cliquez sur ce bouton pour ajouter, importer, exporter et supprimer des listes de signets.
- Bookmarks Lists (Liste déroulante) : affiche les listes de signets pour l'enregistrement DAP.
- Ajouter : cliquez sur ce bouton pour ajouter la liste de signets sélectionnée de la zone de liste déroulante à la zone de liste de signets de droite.
- Supprimer : cliquez sur ce bouton pour supprimer la liste de signets sélectionnée de la zone de liste de signets. Vous ne pouvez pas supprimer une liste de signets de l'appliance de sécurité à moins de la supprimer d'abord des enregistrements DAP.

Figure 14. Onglet Method : permet de configurer le type d'accès à distance autorisé.



- Unchanged : poursuivez avec la méthode d'accès à distance actuelle définie dans la stratégie de groupe pour la session.
- AnyConnect Client : connectez-vous à l'aide du client VPN Cisco AnyConnect.
- Portail Web : connexion à un VPN sans client.
- Both-default-Web-Portal : connectez-vous via le client sans client ou AnyConnect, avec la valeur par défaut clientless.
- Both-default-AnyConnect Client : connectez-vous via le client AnyConnect ou via le client AnyConnect, avec la valeur par défaut AnyConnect.

Comme mentionné précédemment, un enregistrement DAP possède un jeu limité de valeurs d'attribut par défaut, mais seulement si elles sont modifiées, elles ont priorité sur les enregistrements AAA, utilisateur, groupe, groupe de tunnels et groupe par défaut actuels. Si des valeurs d'attribut supplémentaires en dehors de la portée de DAP sont requises, par exemple, Split Tunneling Lists, Banners, Smart Tunnels, Portal Customizations, etc., elles doivent être appliquées via AAA, les enregistrements d'utilisateur, de groupe, de groupe de tunnel et de groupe par défaut. Dans ce cas, ces valeurs d'attribut spécifiques peuvent compléter DAP et ne peuvent pas être remplacées. Ainsi, l'utilisateur obtient un ensemble cumulatif de valeurs d'attribut dans tous les enregistrements.

Agréger plusieurs stratégies d'accès dynamique

Un administrateur peut configurer plusieurs enregistrements LDAP pour traiter de nombreuses variables. Par conséquent, un utilisateur authentifiant peut satisfaire aux critères d'attribut AAA et Endpoint de plusieurs enregistrements DAP. Par conséquent, les attributs de la politique d'accès peuvent être cohérents ou conflictuels dans l'ensemble de ces politiques. Dans ce cas, l'utilisateur autorisé peut obtenir le résultat cumulé pour tous les enregistrements DAP correspondants.

Cela inclut également les valeurs d'attribut uniques appliquées via les enregistrements d'authentification, d'autorisation, d'utilisateur, de groupe, de groupe de tunnels et de groupe par défaut. Le résultat cumulé des attributs de stratégie d'accès crée la stratégie d'accès dynamique. Des exemples d'attributs de stratégie d'accès combinés sont répertoriés dans les tableaux suivants. Ces exemples décrivent les résultats de 3 enregistrements DAP combinés.

La valeur de l'attribut action du tableau 1 est Terminate ou Continue. La valeur de l'attribut agrégé est Terminer si la valeur Terminer est configurée dans l'un des enregistrements DAP sélectionnés et est Continuer si la valeur Continuer est configurée dans tous les enregistrements DAP sélectionnés.

Tableau 1 . Attribut Action

Nom d'attribut	DAP n° 1	DAP n° 2	DAP n° 3	DAP
Action (exemple 1)	continuer	continuer	continuer	continuer
Action (exemple 2)	Résilier	continuer	continuer	terminer

L'attribut user-message présenté dans le tableau 2 contient une valeur de chaîne. La valeur d'attribut agrégée peut être une chaîne séparée par un saut de ligne (valeur hexadécimale 0x0A) créée en liant ensemble les valeurs d'attribut des enregistrements DAP sélectionnés. L'ordre des valeurs d'attribut dans la chaîne combinée est insignifiant.

Tableau 2 . Attribut de message utilisateur

Nom d'attribut	DAP n° 1	DAP n° 2	DAP n° 3	DAP
message-utilisateur	le rapide	renard brun	Saute par dessus	le rapide<LF>renard brun<LF>saute par dessus

Les attributs d'activation de la fonctionnalité Clientless (Fonctions) présentés dans le Tableau 3 contiennent des valeurs qui sont Auto-start, Enable, ou Disable. La valeur de l'attribut agrégé peut être Démarrage automatique si la valeur Démarrage automatique est configurée dans l'un des enregistrements DAP sélectionnés.

La valeur d'attribut agrégée peut être activée si aucune valeur de démarrage automatique n'est configurée dans l'un des enregistrements DAP sélectionnés, et la valeur Enable est configurée dans au moins un des enregistrements DAP sélectionnés.

La valeur d'attribut agrégée peut être désactivée si aucune valeur Auto-start ou Enable n'est configurée dans l'un des enregistrements DAP sélectionnés, et la valeur « disable » est configurée dans au moins l'un des enregistrements DAP sélectionnés.

Tableau 3 . Attributs d'activation des fonctionnalités sans client (fonctions)

Nom d'attribut	DAP n° 1	DAP n° 2	DAP n° 3	DAP
port-forward	activer	désactiver		activer
exploration d'un fichier	désactiver	activer	désactiver	activer
entrée de fichier			désactiver	désactiver
HTTP-proxy	désactiver	démarrage automatique	désactiver	démarrage automatique
entrée d'URL	désactiver		activer	activer

Les attributs URL list et port-forward indiqués dans le tableau 4 contiennent une valeur qui est soit une chaîne, soit une chaîne séparée par des virgules. La valeur d'attribut agrégée peut être une chaîne séparée par des virgules créée par lorsque vous liez ensemble les valeurs d'attribut des enregistrements DAP sélectionnés. Toute valeur d'attribut dupliquée dans la chaîne combinée peut être supprimée. L'ordre des valeurs d'attribut dans la chaîne combinée est insignifiant.

Tableau 4 . Liste d'URL et attribut de liste de transfert de port

Nom d'attribut	DAP n° 1	DAP n° 3	DAP n° 3	DAP
url-list	a	b, c	a	a, b, c
port-forward		D, E	e, f	D, E, F

Les attributs Access Method spécifient la méthode d'accès client autorisée pour les connexions VPN SSL. La méthode d'accès client peut être AnyConnect Client access only, Web-Portal access only, AnyConnect Client ou Web-Portal avec accès Web-Portal par défaut, ou AnyConnect Client ou Web-Portal avec accès AnyConnect Client par défaut. La valeur de l'attribut agrégé est résumée dans le tableau 5.

Tableau 5 . Attributs de méthode Access

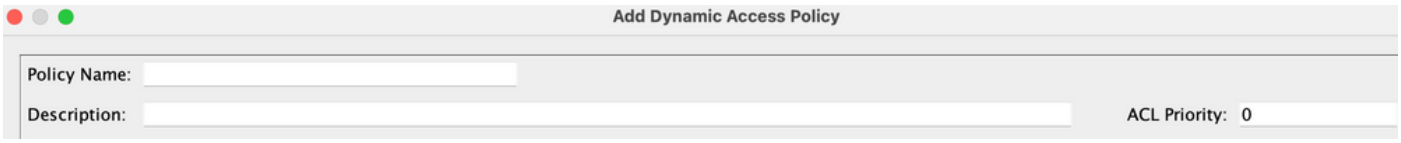
Valeurs d'attribut sélectionnées				Résultat d'agrégation
Client AnyConnect	Portail Web	Both-default-Web-Portal	Both-default-AnyConnect Client	
			X	Both-default-AnyConnect Client
		X		Both-default-Web-Portal
		X	X	Both-default-Web-Portal
	X			Portail Web
	X		X	Both-default-AnyConnect Client
	X	X		Both-default-Web-Portal

	X	X	X	Both-default-Web-Portal
X				Client AnyConnect
X			X	Both-default-AnyConnect Client
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 Client
X	X	X		Both-default-Web-Portal
X	X	X	X	Both-default-Web-Portal

Lorsque vous combinez les attributs Network (Firewall) et Web-Type (Clientless) ACL Filter, la priorité DAP et la liste de contrôle d'accès DAP sont deux composants majeurs à prendre en compte.

L'attribut Priority, tel qu'illustré à la Figure 15, n'est pas agrégé. L'appliance de sécurité utilise cette valeur pour séquencer logiquement les listes d'accès lors de l'agrégation des listes de contrôle d'accès réseau et de type Web à partir de plusieurs enregistrements DAP. L'appliance de sécurité classe les enregistrements du numéro de priorité le plus élevé au numéro de priorité le plus faible, le plus faible étant placé au bas du tableau. Par exemple, un enregistrement DAP avec une valeur de 4 a une priorité plus élevée qu'un enregistrement avec une valeur de 2. Vous ne pouvez pas les trier manuellement.

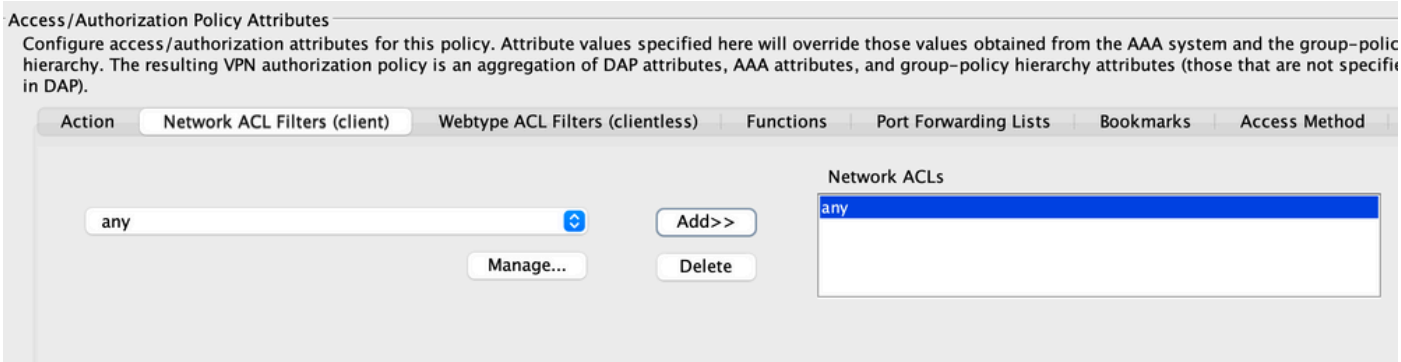
Figure 15. Priority : affiche la priorité de l'enregistrement DAP.



- Policy Name : affiche le nom de l'enregistrement DAP.
- Description : décrit l'objectif de l'enregistrement DAP.

L'attribut ACL DAP prend uniquement en charge les listes d'accès conformes à un modèle ACL Allow-List ou Block-List strict. Dans un modèle de liste de contrôle d'accès Allow-List, les entrées de la liste de contrôle d'accès spécifient des règles qui « autorisent » l'accès aux réseaux ou hôtes spécifiés. En mode Liste de blocage ACL, les entrées de la liste de contrôle d'accès spécifient des règles qui refusent l'accès à des réseaux ou hôtes spécifiés. Une liste de contrôle d'accès non conforme contient des entrées de liste de contrôle d'accès avec un mélange de règles permit et deny. Si une liste d'accès non conforme est configurée pour un enregistrement LDAP, elle peut être rejetée comme erreur de configuration lorsque l'administrateur tente d'ajouter l'enregistrement. Si une liste d'accès conforme est attribuée à un enregistrement DAP, toute modification apportée à la liste d'accès qui modifie la caractéristique de conformité peut être rejetée en tant qu'erreur de configuration.

Figure 16. ACL DAP : permet de sélectionner et de configurer les ACL réseau à appliquer à cet enregistrement DAP.



Lorsque plusieurs enregistrements DAP sont sélectionnés, les attributs de listes d'accès spécifiés dans la liste de contrôle d'accès Réseau (Pare-feu) sont agrégés pour créer une liste d'accès dynamique pour la liste de contrôle d'accès Pare-feu DAP. De la même manière, les attributs de listes d'accès spécifiés dans la liste de contrôle d'accès Web-Type (sans client) sont agrégés pour créer une liste d'accès dynamique pour la liste de contrôle d'accès sans client DAP. L'exemple suivant porte sur la création spécifique d'une liste d'accès de pare-feu LDAP dynamique. Cependant, une liste d'accès sans client LDAP dynamique peut également effectuer le même processus.

Tout d'abord, l'ASA crée dynamiquement un nom unique pour la liste de contrôle d'accès réseau DAP comme indiqué dans le tableau 6.

Tableau 6 . Nom ACL-réseau LDAP dynamique

Nom de la liste de contrôle d'accès réseau LDAP
DAP-Network-ACL-X (où X est un entier qui peut être incrémenté pour garantir l'unicité)

Deuxièmement, l'ASA récupère l'attribut Network-ACL à partir des enregistrements DAP sélectionnés comme indiqué dans le tableau 7.

Tableau 7 . ACL réseau

Enregistrements LDAP sélectionnés	Priorité	ACL-réseau	Entrées de liste de contrôle d'accès réseau
DAP 1	1	101 et 102	La liste de contrôle d’accès 101 comporte 4 règles de refus et la liste 102 4 règles d’autorisation
DAP 2	2	201 et 202	ACL 201 a 3 règles d'autorisation et ACL 202 a 3 règles de refus
DAP 3	2	101 et 102	La liste de contrôle d’accès 101 comporte 4 règles de refus et la liste 102 4 règles d’autorisation

Troisièmement, l'ASA réorganise la liste de contrôle d'accès réseau d'abord par le numéro de priorité de l'enregistrement DAP, puis par liste de blocage d'abord si la valeur de priorité pour 2 enregistrements DAP sélectionnés ou plus est la même. Ensuite, l'ASA peut récupérer les entrées

de la liste de contrôle d'accès réseau à partir de chaque liste de contrôle d'accès réseau, comme indiqué dans le tableau 8.

Tableau 8 . Priorité d'enregistrement LDAP

ACL-réseau	Priorité	Modèle de liste d'accès blanc/noir	Entrées de liste de contrôle d'accès réseau
101	2	Liste Noire	4 Règles de refus (DDDD)
202	2	Liste Noire	3 Règles de refus (DDD)
102	2	Liste Blanche	4 Règles de permis (PPPP)
202	2	Liste Blanche	3 Règles d'autorisation (PPP)
101	1	Liste Noire	4 Règles de refus (DDDD)
102	1	Liste Blanche	4 Règles de permis (PPPP)

Enfin, l'ASA fusionne les entrées Network-ACL dans la Network-ACL générée dynamiquement et retourne ensuite le nom de la Network-ACL dynamique en tant que la nouvelle liste de contrôle d'accès Network-ACL à appliquer, comme indiqué dans le tableau 9.

Tableau 9 . ACL-réseau LDAP dynamique

Nom de la liste de contrôle d'accès réseau LDAP	Entrée ACL-réseau
DAP-Network-ACL-1	DDDD DDD PPP PPP PPP DDD PPP

Implémentation DAP

Il existe de nombreuses raisons pour lesquelles un administrateur doit envisager de mettre en oeuvre le protocole DAP. Certaines raisons sous-jacentes sont liées à l'application de l'évaluation de la position sur un terminal et/ou à la prise en compte d'attributs AAA ou de politiques plus granulaires lors de l'autorisation d'accès des utilisateurs aux ressources réseau. Dans l'exemple suivant, vous pouvez configurer DAP et ses composants pour identifier un point d'extrémité de connexion et autoriser l'accès utilisateur à diverses ressources réseau.

Cas de test : un client a demandé une preuve de concept avec les conditions d'accès VPN suivantes :

- Capacité à détecter et à identifier un terminal d'employé comme étant géré ou non géré. : si le terminal est identifié comme géré (PC de travail) mais ne répond pas aux exigences de posture, l'accès à ce terminal doit lui être refusé. D'autre part, si le terminal de l'employé est identifié comme non géré (PC domestique), ce terminal doit alors bénéficier d'un accès sans client.
- Possibilité d'appeler le nettoyage des cookies de session et du cache lorsqu'une connexion sans client se termine.
- La capacité à détecter et à appliquer des applications en cours d'exécution sur les terminaux

gérés des employés, tels que McAfee AntiVirus. Si l'application n'existe pas, ce point de terminaison doit se voir refuser l'accès.

- Possibilité d'utiliser l'authentification AAA pour déterminer les ressources réseau auxquelles les utilisateurs autorisés doivent avoir accès. L'appliance de sécurité doit prendre en charge l'authentification MS LDAP native et prendre en charge plusieurs rôles d'appartenance à un groupe LDAP.
- Possibilité d'autoriser l'accès local au réseau local aux ressources réseau telles que les télécopieurs et les imprimantes réseau lorsqu'ils sont connectés via une connexion client/réseau.
- Possibilité de fournir un accès invité autorisé aux sous-traitants. Les sous-traitants et leurs terminaux doivent bénéficier d'un accès sans client et leur accès au portail des applications doit être limité par rapport à l'accès des employés.

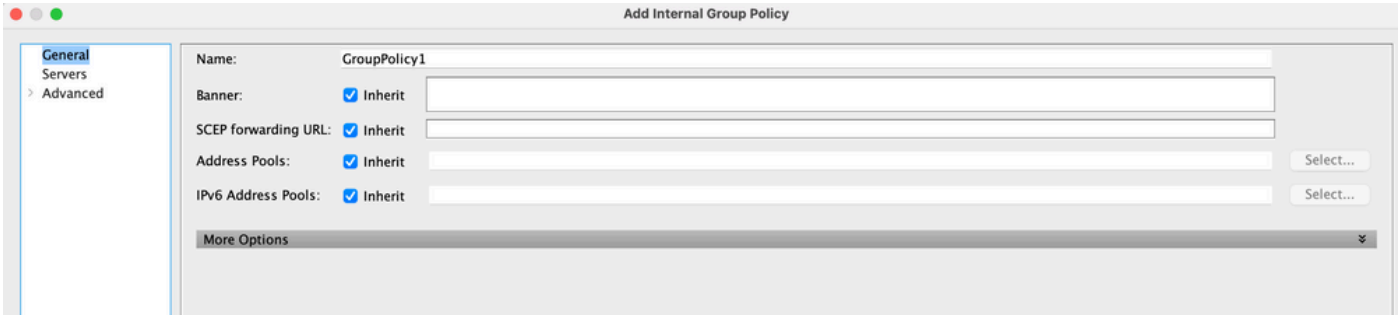
Dans cet exemple, vous pouvez exécuter une série d'étapes de configuration pour répondre aux exigences d'accès VPN du client. Il peut y avoir des étapes de configuration nécessaires, mais pas directement liées à DAP, alors que d'autres configurations peuvent être directement liées à DAP. L'ASA est très dynamique et peut s'adapter à de nombreux environnements réseau. Par conséquent, les solutions VPN peuvent être définies de différentes manières et, dans certains cas, fournir la même solution finale. L'approche adoptée est toutefois dictée par les besoins des clients et leur environnement.

En fonction de la nature de ce document et des exigences client définies, vous pouvez utiliser Adaptive Security Device Manager (ASDM) et concentrer la plupart de nos configurations sur DAP. Cependant, vous pouvez également configurer des stratégies de groupe locales pour montrer comment DAP peut compléter et/ou remplacer les attributs de stratégie locale. Sur la base de ce cas de test, vous pouvez supposer qu'un groupe de serveurs LDAP, une liste de réseaux de tunnellisation partagée et une connectivité IP de base, y compris des pools d'adresses IP et le groupe de serveurs DNS par défaut, sont préconfigurés.

Définition d'une stratégie de groupe : cette configuration est nécessaire pour définir les attributs de stratégie locale. Certains attributs définis ici ne sont pas configurables dans DAP (par exemple, Accès LAN local). (Cette stratégie peut également être utilisée pour définir des attributs sans client et basés sur le client).

Accédez à Configuration > Remote Access VPN > Network (Client) Access > Group Policies, et ajoutez une stratégie de groupe interne comme indiqué :

Figure 17. Stratégie de groupe : définit les attributs spécifiques au VPN local.

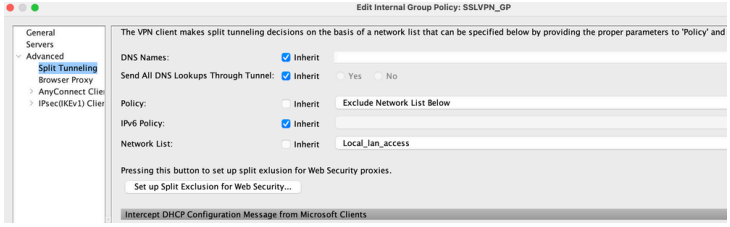


a. Sous le lien Général, configurez le nomSSLVPN_GPpour la stratégie de groupe.

b. Également sous le lien General, cliquez sur More Options et configurez seulement le Tunneling Protocol : Clientless SSLVPN. (Vous pouvez configurer DAP pour remplacer et gérer la méthode d'accès.)

c. Sous le lien Advanced > Split Tunneling, configurez les étapes suivantes :

Figure 18. Split Tunneling : permet au trafic spécifié (réseau local) de contourner un tunnel non chiffré pendant une connexion client.

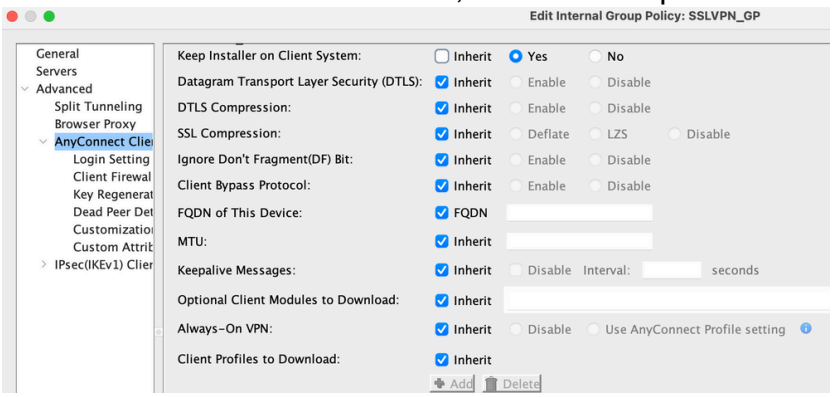


a. Stratégie : désactivez Hériter et sélectionnezExclure la liste de réseaux.

b. Network List : désactivez la case à cocher Inherit et sélectionnez le nom de liste Local_Lan_Access. (Supposons qu'il soit préconfiguré.)

d. Sous le lien Advanced > ANYCONNECT Client, configurez les étapes suivantes :

Figure 19. Installation du client VPN SSL : une fois le VPN terminé, le client SSL peut rester sur le terminal ou être désinstallé.



e. Conserver le programme d'installation sur le système client : DécochezHériter, puis sélectionnezOui.

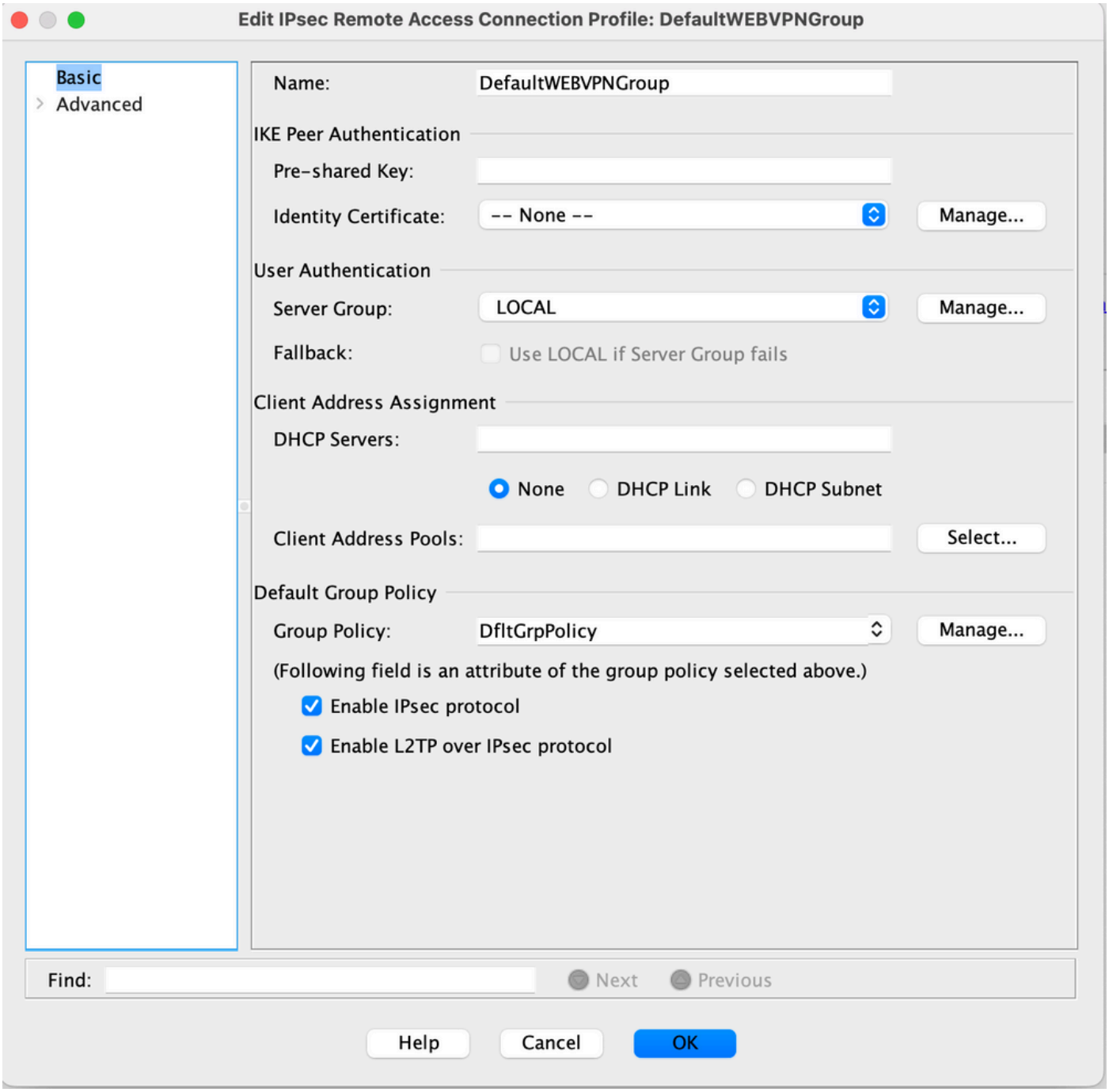
f. Cliquez sur OKpuis sur Appliquer.

g. Appliquez vos modifications de configuration.

Définition d'un profil de connexion : cette configuration est nécessaire pour définir notre méthode d'authentification AAA, par exemple LDAP, et pour appliquer la stratégie de groupe précédemment configurée (SSLVPN_GP) à ce profil de connexion. Les utilisateurs se connectant via ce profil de connexion peuvent être soumis aux attributs définis ici ainsi qu'aux attributs définis dans la stratégie de groupe SSLVPN_GP. (Ce profil peut également être utilisé pour définir les attributs sans client et basés sur le client).

Accédez à Configuration > Remote Access VPN > Network (Client) Access > IPsec Remote Access Connection Profile et configurez :

Figure 20. Connection Profile : définit les attributs spécifiques au VPN local.



a. Dans la section Profils de connexion, modifiez le groupe DefaultWEBVPNGroup et, sous le lien Basic, configurez les étapes suivantes :

a. Authentification : méthode : AAA

b. Authentification - Groupe de serveurs AAA : LDAP (préconfiguré supposé)

c. Attribution d'adresses client : pools d'adresses client :IP_Pool(préconfiguré supposé)

d. Stratégie de groupe par défaut - Stratégie de groupe : SelectSSLVPN_GP

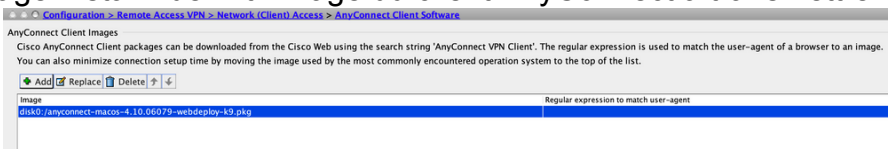
b. Appliquez vos modifications de configuration.

Définir une interface IP pour la connectivité VPN SSL - Cette configuration est nécessaire pour mettre fin aux connexions SSL client et sans client sur une interface spécifiée.

Avant d'activer l'accès client/réseau sur une interface, vous devez d'abord définir une image de client VPN SSL.

1. Accédez à Configuration > Remote Access VPN > Network (Client)Access > Anyconnect Client Software, et ajoutez l'image suivante, l'image du client VPN SSL à partir du système de fichiers Flash ASA : (Cette image peut être téléchargée à partir de CCO, https://www.cisco.com)

   Figure 21. SSL VPN Client Image Install : définit l'image du client AnyConnect à transmettre pour connecter les terminaux.



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

   b. Cliquez sur OK, OKà nouveau, puis sur Appliquer.

2. Accédez à Configuration > Remote Access VPN > Network (Client)Access > AnyConnect Connection Profiles, et suivez les étapes suivantes pour activer ceci :

   Figure 22. SSL VPN Access Interface : définit la ou les interfaces permettant de mettre fin à la connectivité VPN SSL.

   a. Dans la section Interface d'accès, activez l'option : Activer l'accès au client VPN Cisco AnyConnect ou au client VPN SSL hérité sur les interfaces sélectionnées dans le tableau ci-dessous.

   b. Également sous la section Access Interfaces, cochez Allow Access sur l'interface externe. (Cette configuration peut également activer l'accès sans client VPN SSL sur l'interface externe.)

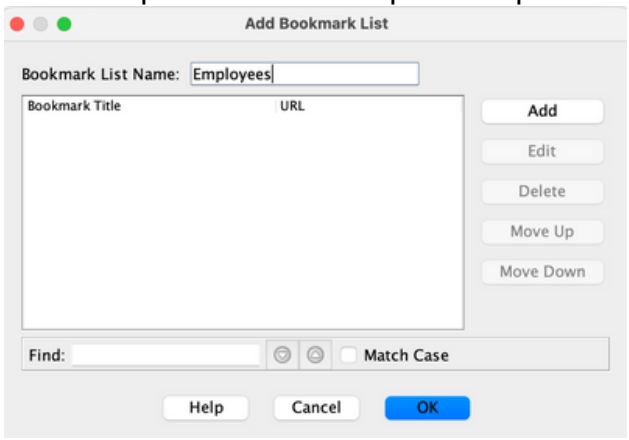
   c. Cliquez sur Appliquer.

Définition de listes de signets (listes d'URL) pour l'accès sans client : cette configuration est

nécessaire pour définir une application Web à publier sur le portail. vous pouvez définir 2 listes d'URL, l'une pour les employés et l'autre pour les sous-traitants.

1. Accédez à Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks, cliquez sur + Add et configurez les étapes suivantes :

   Figure 23. Bookmark List : définit les URL à publier et auxquelles accéder à partir du portail Web. (Personnalisé pour l'accès des employés).



   a. Nom de la liste de signets : Employés, puis cliquez sur Ajouter.

   b. Titre du signet : Intranet de la société

   c. Valeur d'URL : https://company.resource.com

   •

   Cliquez sur OK, puis de nouveau sur OK.

•

Cliquez sur + Ajouter et configurez une deuxième liste de signets (liste d'URL) comme suit :

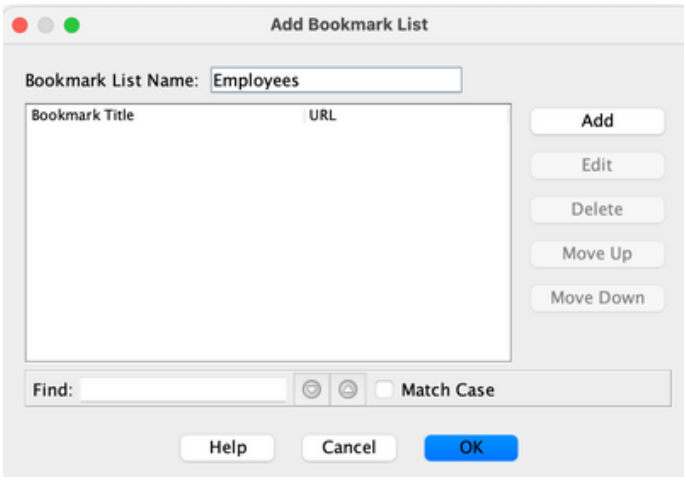


Figure 24. Liste de signets : personnalisée pour l'accès invité.

a.

Nom de la liste de signets : **Entrepreneurs**, puis **cliquez sur Ajouter**.

b.

Titre du signet : **Accès invité**

c.

Valeur d'URL : https://company.contractors.com

- Cliquez sur OK, puis de nouveau sur OK.

- **Cliquez sur Appliquer**.

Configurer Hostscan :

- Accédez **à Configuration > Remote Access VPN > Secure Desktop Manager > HostScan Image**, et configurez les étapes suivantes :

Figure 25. HostScan Image Install : définit l'image HostScan à diffuser pour connecter les terminaux. 

a.

Installez **l'image disk0:/hostscan_4.xx.xxxxx-k9.**pkgimage à partir du système de fichiers Flash ASA.

b.

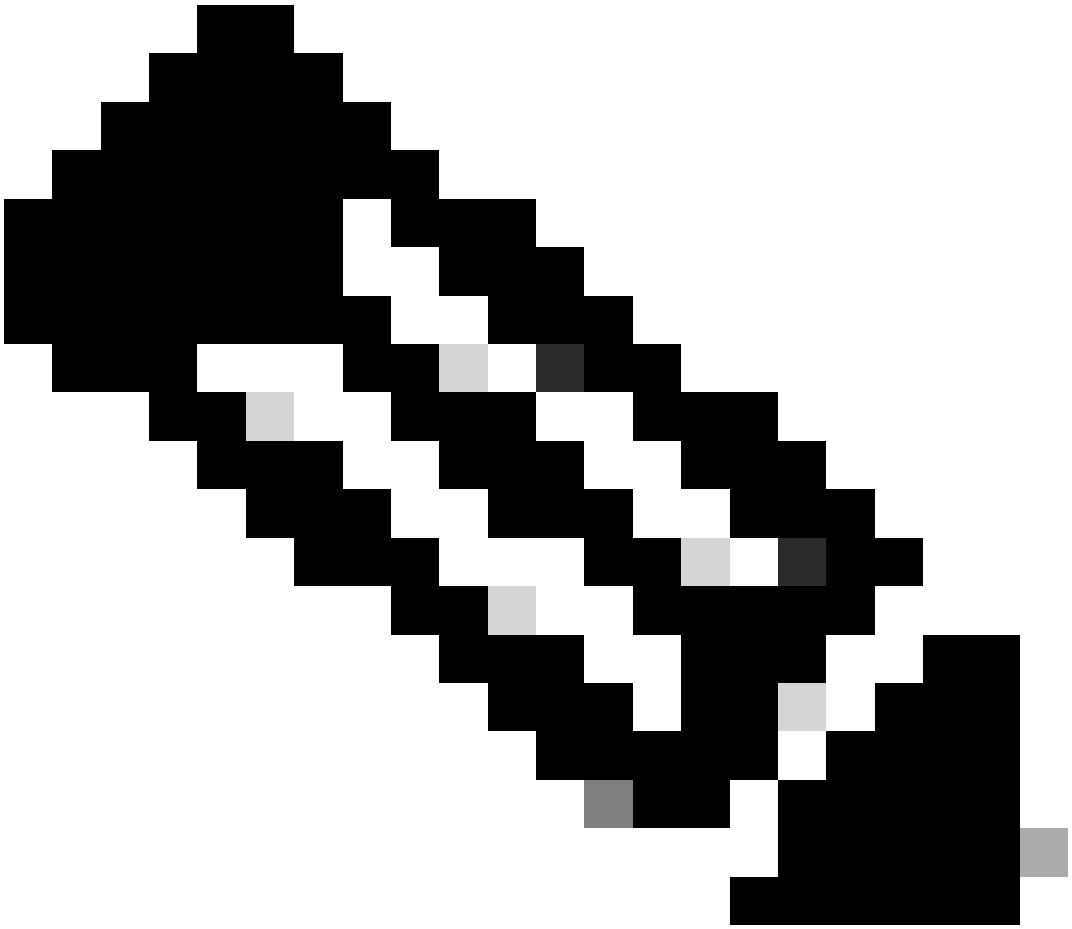
Cochez Activer HostScan.

c.

Cliquez sur Appliquer.

Stratégies d'accès dynamique - Cette configuration est nécessaire pour valider la connexion des utilisateurs et de leurs terminaux par rapport aux critères d'évaluation AAA et/ou des terminaux définis. Si les critères définis d'un enregistrement DAP sont satisfaits, les utilisateurs connectés peuvent alors accéder aux ressources réseau associées à cet enregistrement ou à ces enregistrements DAP. L'autorisation DAP est exécutée pendant le processus d'authentification.

Pour vous assurer qu'une connexion VPN SSL peut se terminer dans le cas par défaut (par exemple, lorsque le point d'extrémité ne correspond à aucune stratégie d'accès dynamique configurée), vous pouvez la configurer en procédant comme suit :

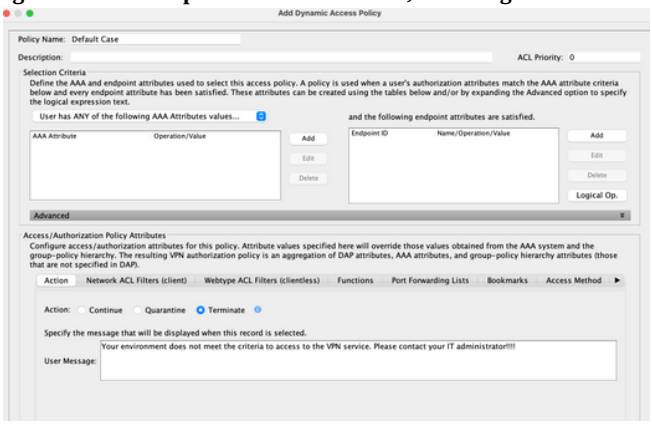


Remarque : lors de la première configuration des stratégies d'accès dynamiques, un message d'erreur DAP.xml s'affiche pour indiquer qu'aucun fichier de configuration DAP (DAP.XML) n'existe. Une fois que votre configuration DAP initiale est modifiée puis enregistrée, ce message ne peut plus s'afficher.

-

Accédez **à Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies**, et configurez les étapes suivantes :

Figure 30. Stratégie d'accès dynamique par défaut : si aucun enregistrement DAP prédéfini n'est associé, cet enregistrement DAP peut être appliqué. Ainsi, l'accès VPN SSL peut être refusé.



a.

Modifiez laDfltAccessPolicy et définissez l'action **sur Terminer**.

b.

Cliquez sur OK.

-

Ajoutez une nouvelle stratégie d'accès dynamique **nommée Managed_Endpoints**, comme suit :

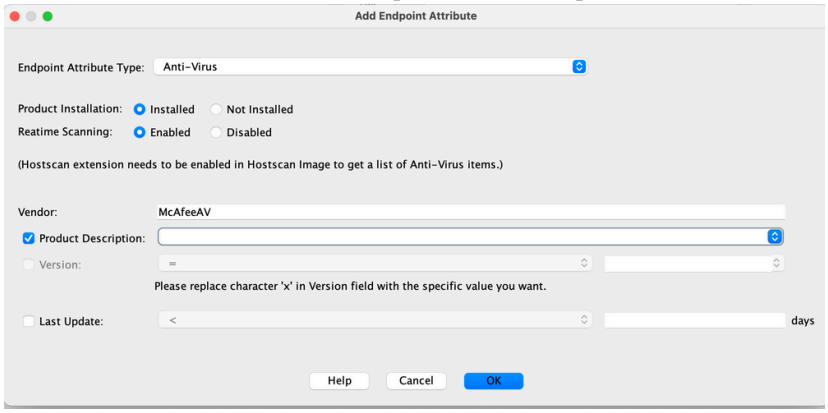
a.

Description : **Accès client employé**

b.

Ajoutez un type d'attribut de point de terminaison (antivirus), comme illustré à la Figure 31. Cliquez sur OK lorsque vous avez terminé.

Figure 31. Attribut de point de terminaison LDAP : l'antivirus Advanced Endpoint Assessment peut être utilisé comme critère LDAP pour l'accès client/réseau.



c.

Comme l'illustre l'image précédente, dans la liste déroulante de la section Attribut AAA, sélectionnez User has ALL of the following AAA Attributes Values.

•

Ajoutez (à droite de la zone Attribut AAA) un type d'attribut AAA (LDAP), comme illustré aux Figures 33 et 34. Cliquez sur OK lorsque vous avez terminé.

Figure 33. Attribut LDAP AAA : l'appartenance à un groupe AAA peut être utilisée comme critère DAP pour identifier un employé.

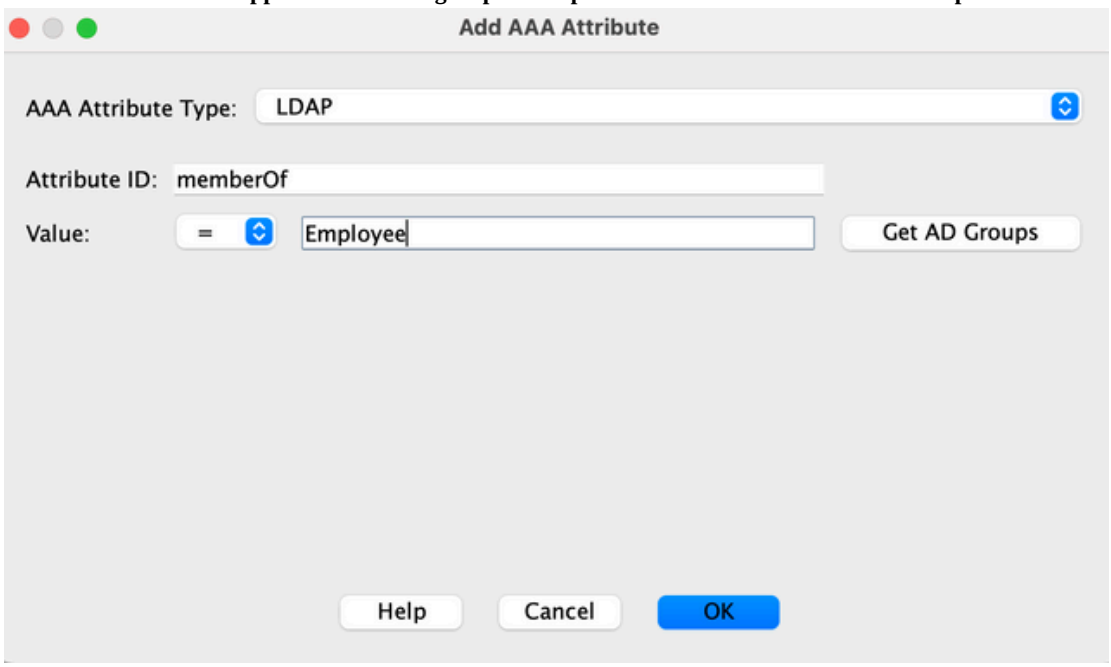
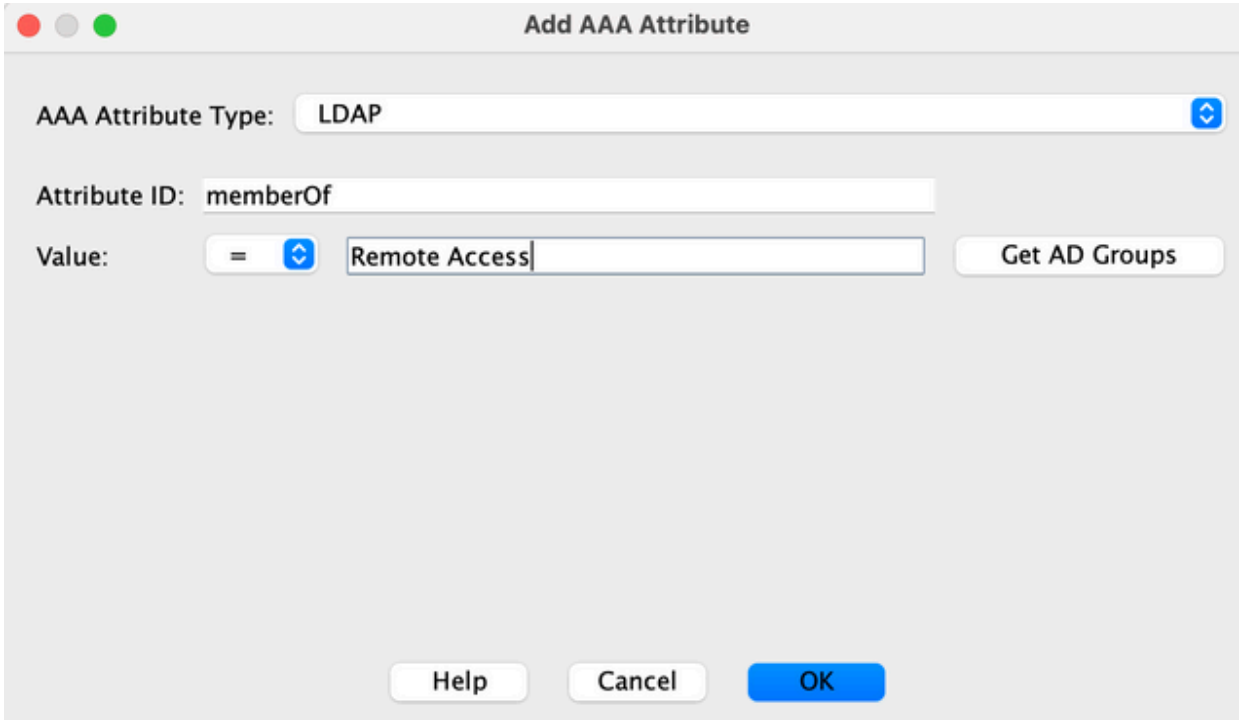


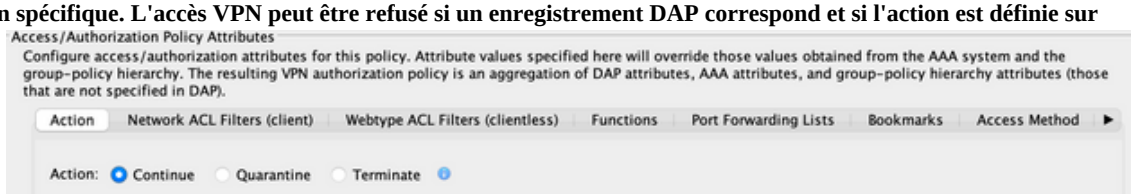
Figure 34. Attribut LDAP AAA : l'appartenance à un groupe AAA peut être utilisée comme critère LDAP pour permettre des fonctionnalités d'accès à distance.



-

Sous l'onglet Action, vérifiez que l'action est définie **sur Continue**, comme illustré à la Figure 35.

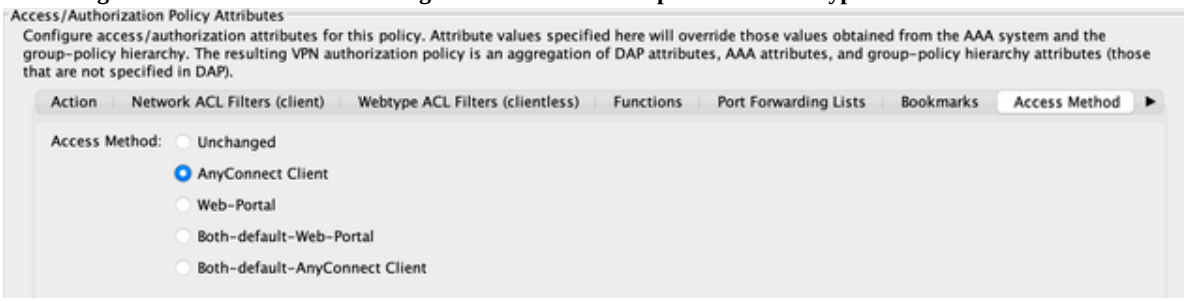
Figure 35. Onglet Action : cette configuration est nécessaire pour définir un traitement spécial pour une connexion ou une session spécifique. L'accès VPN peut être refusé si un enregistrement DAP correspond et si l'action est définie sur Terminer.



-

Sous l'onglet Access Method, sélectionnez Access **MethodAnyConnect Client**, comme illustré à la Figure 36.

Figure 36. Onglet Access Method : cette configuration est nécessaire pour définir les types de connexion des clients VPN SSL.



-

Cliquez sur OK, puis sur Appliquer.

-

Ajoutez une deuxième stratégie d'accès dynamique **nommée Unmanaged_Endpoints**, comme décrit ci-dessous :

a.

Description : **Accès sans client pour les employés**.

b.

Dans la liste déroulante de l'image précédente de la section Attribut AAA, sélectionnez User has ALL of the following AAA Attributes Values .

-

Ajoutez (à droite du type d'attribut AAA) un type d'attribut AAA (LDAP), comme illustré aux Figures 38 et 39. Cliquez sur OK lorsque vous avez terminé.

Figure 38. Attribut DAP AAA : l'appartenance à un groupe AAA peut être utilisée comme critère DAP pour identifier un employé.

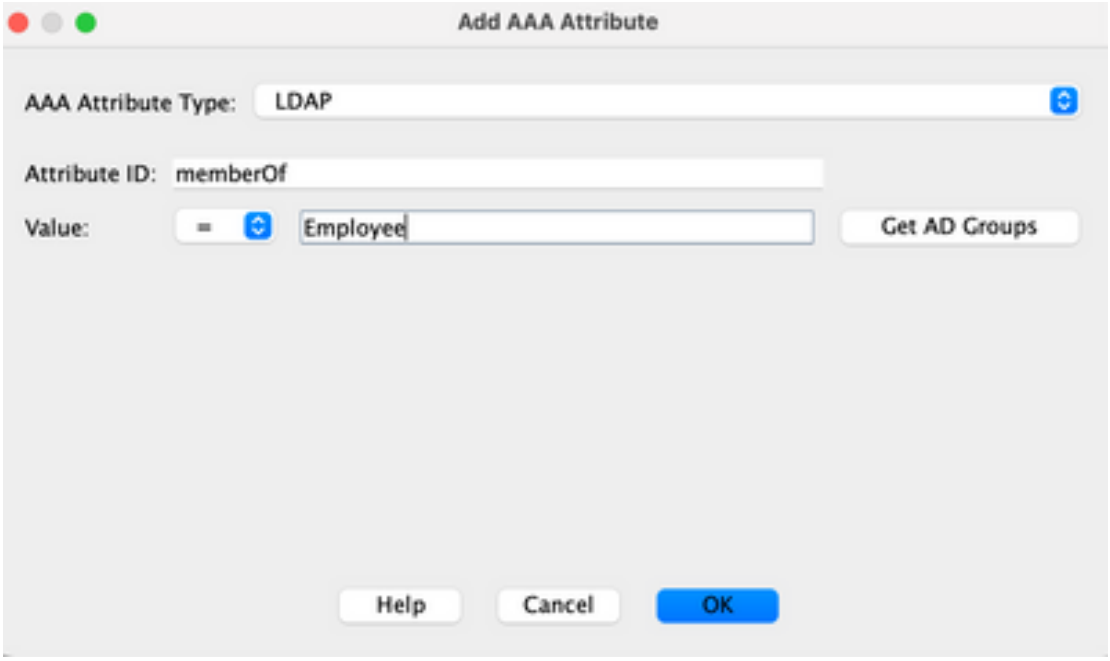
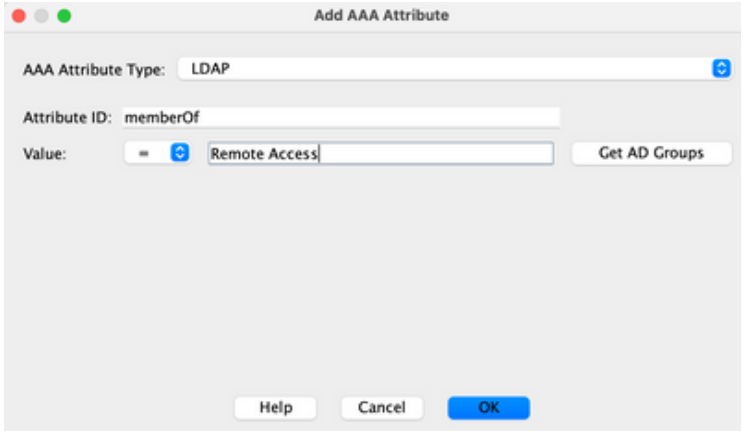


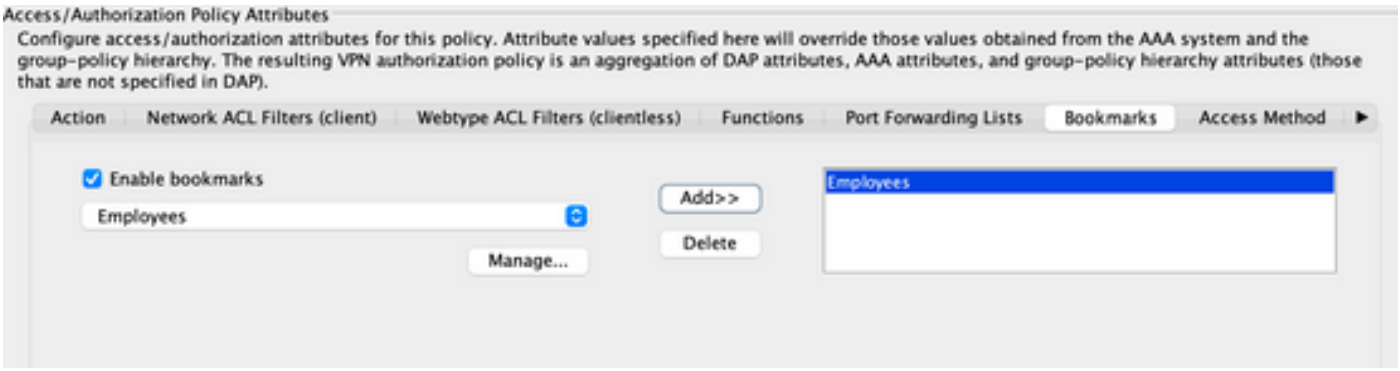
Figure 39. Attribut LDAP AAA : l'appartenance à un groupe AAA peut être utilisée comme critère LDAP pour permettre des fonctionnalités d'accès à distance.



- Sous l'onglet Action, vérifiez que l'action est définie **sur Continue**. (Figure 35)

- Sous l'onglet Signets, sélectionnez le nom de liste Employés dans la liste déroulante, puis **cliquez sur Ajouter**. Vérifiez également que la case Activer les signets est cochée, comme illustré à la Figure 40.

Figure 40. Onglet Signets : permet de sélectionner et de configurer les listes d'URL pour les sessions utilisateur.



- a. Sous l'onglet Méthode d'accès, sélectionnez le **portail Web** Méthode d'accès. (Figure 36)

- **Cliquez sur OK**, **puis sur Appliquer**.

1. Les sous-traitants ne peuvent être identifiés que par les attributs AAA LDAP. Par conséquent, le type d'attributs de point de terminaison (stratégie) ne peut pas être configuré à l'étape 4. Cette approche n'est destinée qu'à démontrer la polyvalence au sein de DAP.

3. Ajoutez une troisième stratégie d'accès dynamique **nommée Guest_Access** avec ce qui suit :

- Description : **Accès sans client invité**.

- Ajoutez (à droite de la zone Attribut de point de terminaison) un type d'attribut de point de terminaison (politique), comme illustré à la Figure 37. Cliquez sur OK lorsque vous avez terminé.

- Dans la Figure 40, dans la liste déroulante de la section Attribut AAA, sélectionnez User has ALL of the following AAA Attributes Values.

- Ajoutez (à droite de la zone Attribut AAA) un type d'attribut AAA (LDAP), comme illustré aux Figures 41 et 42. Cliquez sur OK lorsque vous avez terminé.

Figure 41. Vous pouvez utiliser l'attribut AAA DAP - Appartenance au groupe AAA comme critère DAP pour identifier un sous-traitant

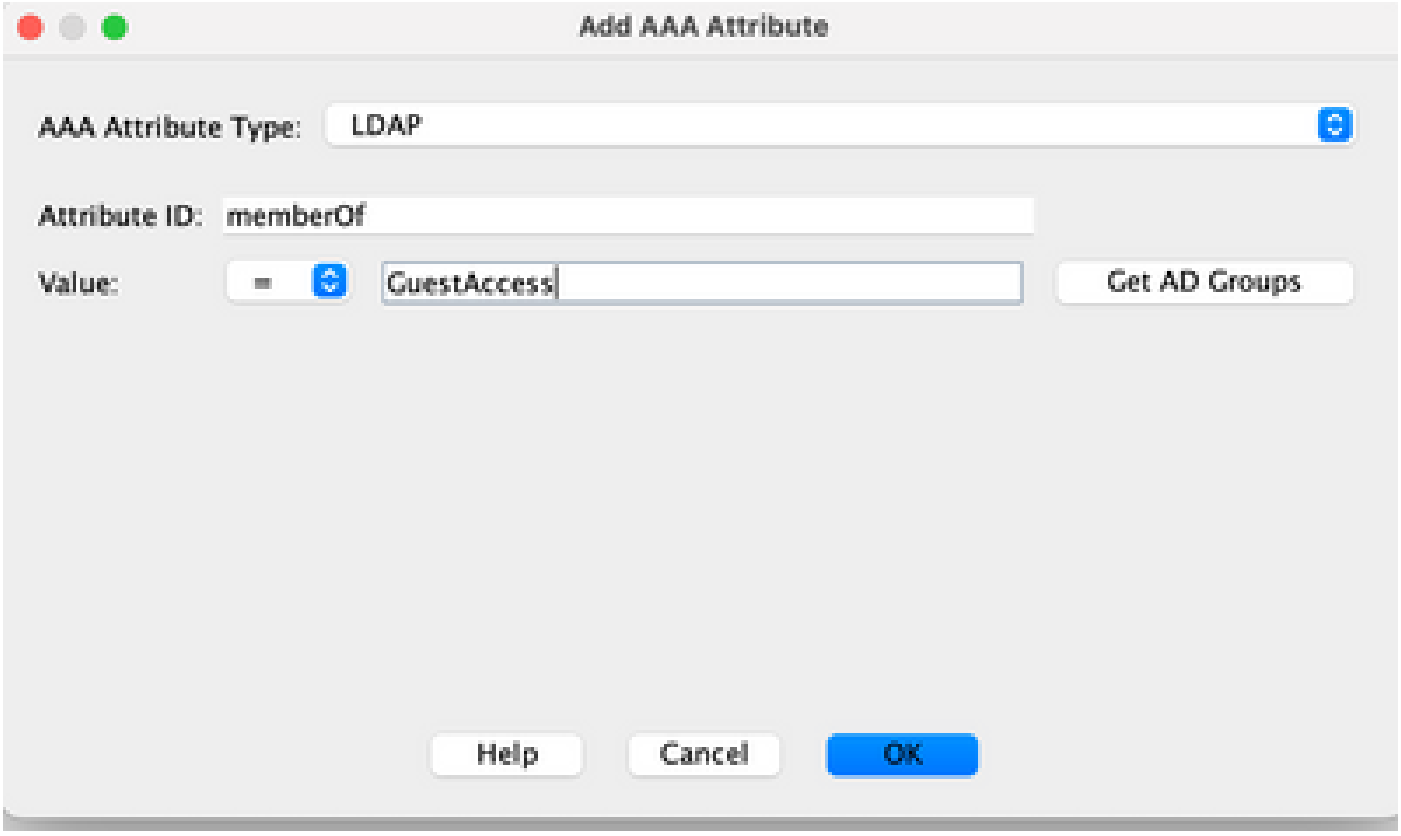
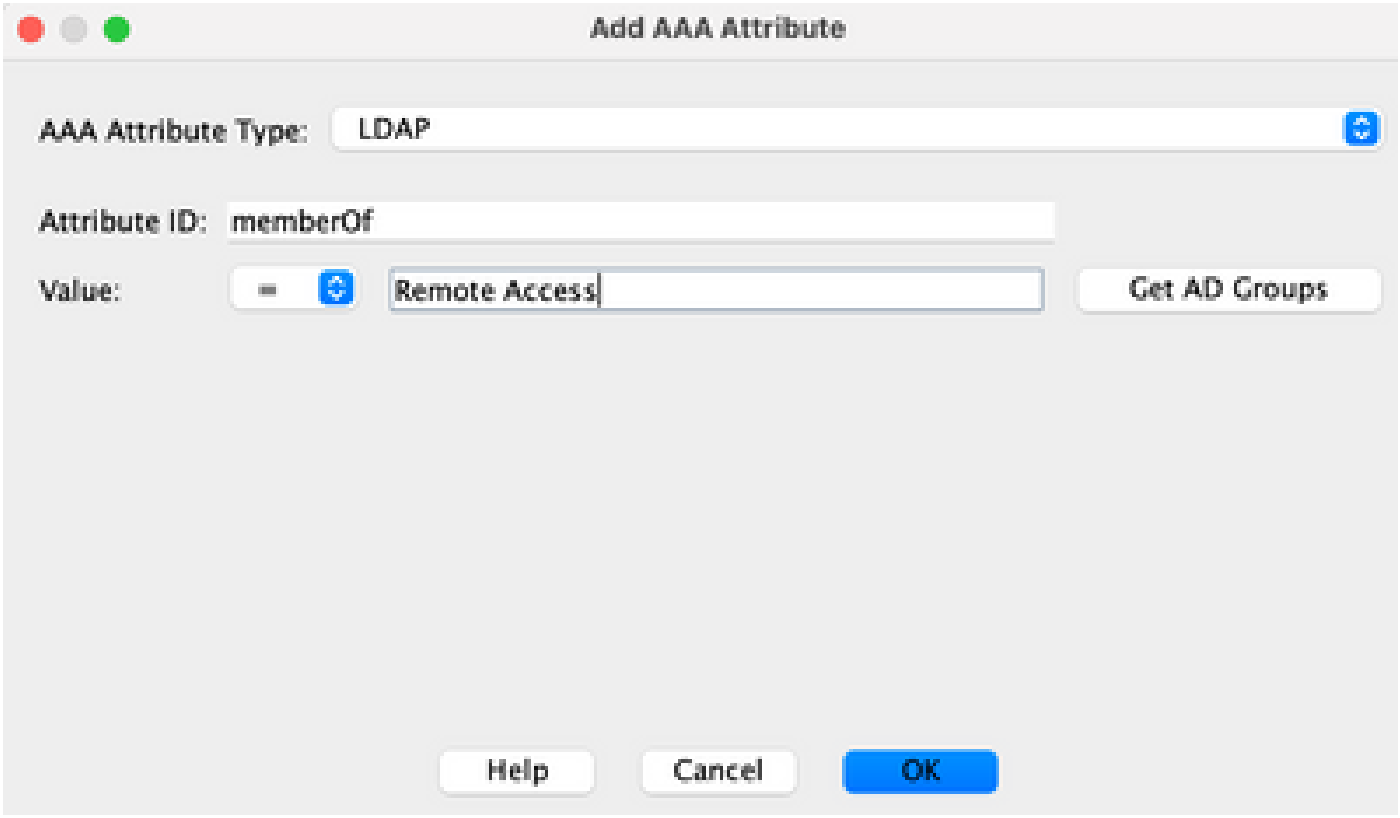


Figure 42. Attribut LDAP AAA : vous pouvez utiliser l'appartenance à un groupe AAA comme critère DAP pour autoriser les fonctionnalités d'accès à distance



-

a.

Sous l'onglet Action, vérifiez que l'action est définie sur **Continue**. (Figure 35)

b.

Sous l'onglet Signets, sélectionnez le nom de liste **Contractors** dans la liste déroulante, puis cliquez sur Ajouter. Vérifiez également que la case **Enable bookmarks** est cochée. (Voir la figure 40.)

c.

Sous l'onglet Méthode d'accès, sélectionnez le portail Web Méthode d'accès. (Figure 36)

d.

Cliquez sur **OK**, puis sur **Apply**.

Conclusion

Sur la base des exigences VPN SSL d'accès à distance du client notées dans cet exemple, cette solution répond aux exigences VPN d'accès à distance du client.

Avec des environnements VPN dynamiques et évolutifs sur la fusion, les politiques d'accès dynamiques peuvent s'adapter et évoluer en fonction des modifications fréquentes de la configuration Internet, des différents rôles que chaque utilisateur peut occuper au sein d'une organisation et des connexions à partir de sites d'accès à distance gérés et non gérés avec différentes configurations et différents niveaux de sécurité.

Les stratégies d'accès dynamique sont complétées par des technologies nouvelles et éprouvées, notamment Advanced Endpoint Assessment, Host Scan, Secure Desktop, AAA et Local Access Policies. Par conséquent, les entreprises peuvent fournir en toute confiance un accès VPN sécurisé à n'importe quelle ressource réseau, quel que soit le lieu.

Informations connexes

- **Assistance technique de Cisco et téléchargements**

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.