

ASA 9.Xダイナミックアクセスポリシー(DAP)の導入

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[DAPとAAA属性](#)

[DAPとエンドポイントセキュリティ属性](#)

[デフォルトのダイナミックアクセスポリシー](#)

[ダイナミックアクセスポリシーの設定](#)

[複数のダイナミックアクセスポリシーの集約](#)

[DAP実装](#)

[結論](#)

[関連情報](#)

はじめに

このドキュメントでは、ASA 9.xダイナミックアクセスポリシー(DAP)の導入、機能、および使用方法について説明します。

前提条件

要件

次の項目について理解しておくことをお勧めします。

- バーチャルプライベートネットワーク(VPN)ゲートウェイ
- ダイナミックアクセスポリシー(DAP)

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

バーチャルプライベート ネットワーク (VPN) ゲートウェイは、動的な環境で動作します。複数の変数が各VPN接続に影響を与える可能性があります。たとえば、頻繁に変更されるイントラネット構成、組織内の各ユーザーが持つさまざまな役割、リモートアクセスサイトからのログインなど、構成やセキュリティレベルが異なる場合があります。動的 VPN 環境でのユーザ認可のタスクは、静的設定のネットワークでの認可タスクよりもかなり複雑です。

ダイナミックアクセスポリシー(DAP)は、VPN環境のダイナミクスに対応する認可を設定できる機能です。ダイナミック アクセス ポリシーは、特定のユーザトンネルまたはユーザ セッションに関連付ける一連のアクセス コントロール属性を設定して作成します。これらの属性により、複数のグループ メンバーシップやエンドポイント セキュリティの問題に対処します。

たとえば、セキュリティ アプライアンスは、定義されるポリシーに基づいて、特定のセッションで特定のユーザにアクセス権を付与します。1つ以上のDAPレコードから属性を選択または集約することにより、ユーザ認証全体を通じてDAPを生成します。DAP レコードは、リモート デバイスのエンドポイント セキュリティ情報および認証ユーザの AAA 認可情報に基づいて選択されます。選択された DAP レコードは、ユーザ トンネルまたはセッションに適用されます。



注:DAPポリシー選択属性が含まれているdap.xmlファイルはASAフラッシュに保存されま
す。dap.xmlファイルをオフボックスでエクスポートし、編集して (XML構文を理解して
いる場合)、再インポートできますが、設定に誤りがあるとASDMでDAPレコードの処理
が停止する可能性があるため、注意が必要です。この設定を操作できる CLI はありませ
ん。



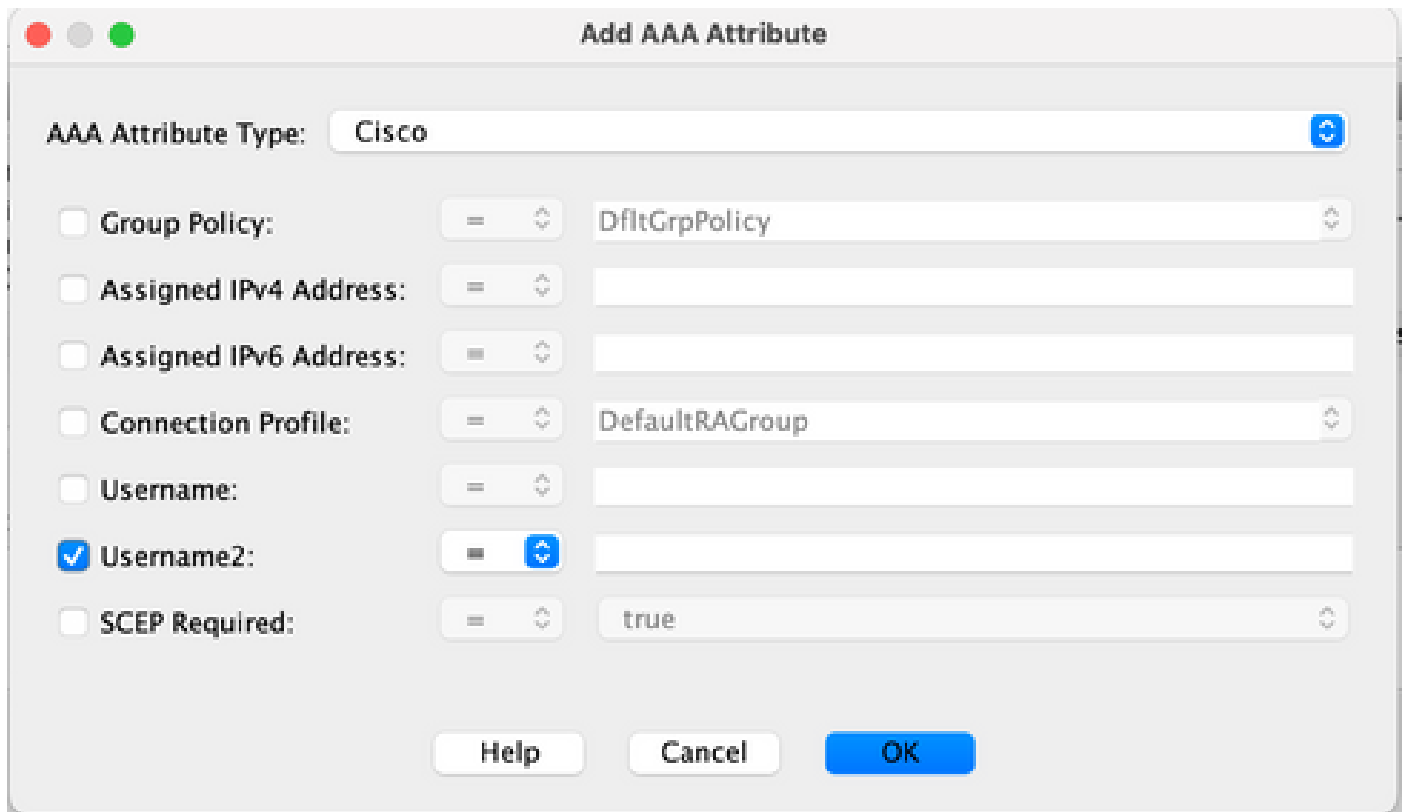
注：CLIを使用してdynamic-access-policy-recordアクセスパラメータを設定しようとする
と、DAPにより処理が停止されることがあります。ただしASDMではこれは適切に管理さ
れます。DAP ポリシーを管理する際には CLI を使用せず、常に ASDM を使用してくださ
い。

DAP と AAA 属性

DAP は AAA サービスを補完し、DAP の認可属性により、AAA が提供する属性を上書きできます
。セキュリティ アプライアンスは、ユーザの AAA 認可情報に基づいて DAP レコードを選択でき
ます。セキュリティ アプライアンスは、この情報に基づいて複数の DAP レコードを選択し、次
に選択したレコードを集約して DAP 認可属性を割り当てます。

AAA 属性は、Cisco AAA 属性階層から、またはセキュリティ アプライアンスが RADIUS サーバ
または LDAP サーバから受信するフル セットの応答属性から指定できます (図 1 を参照) 。

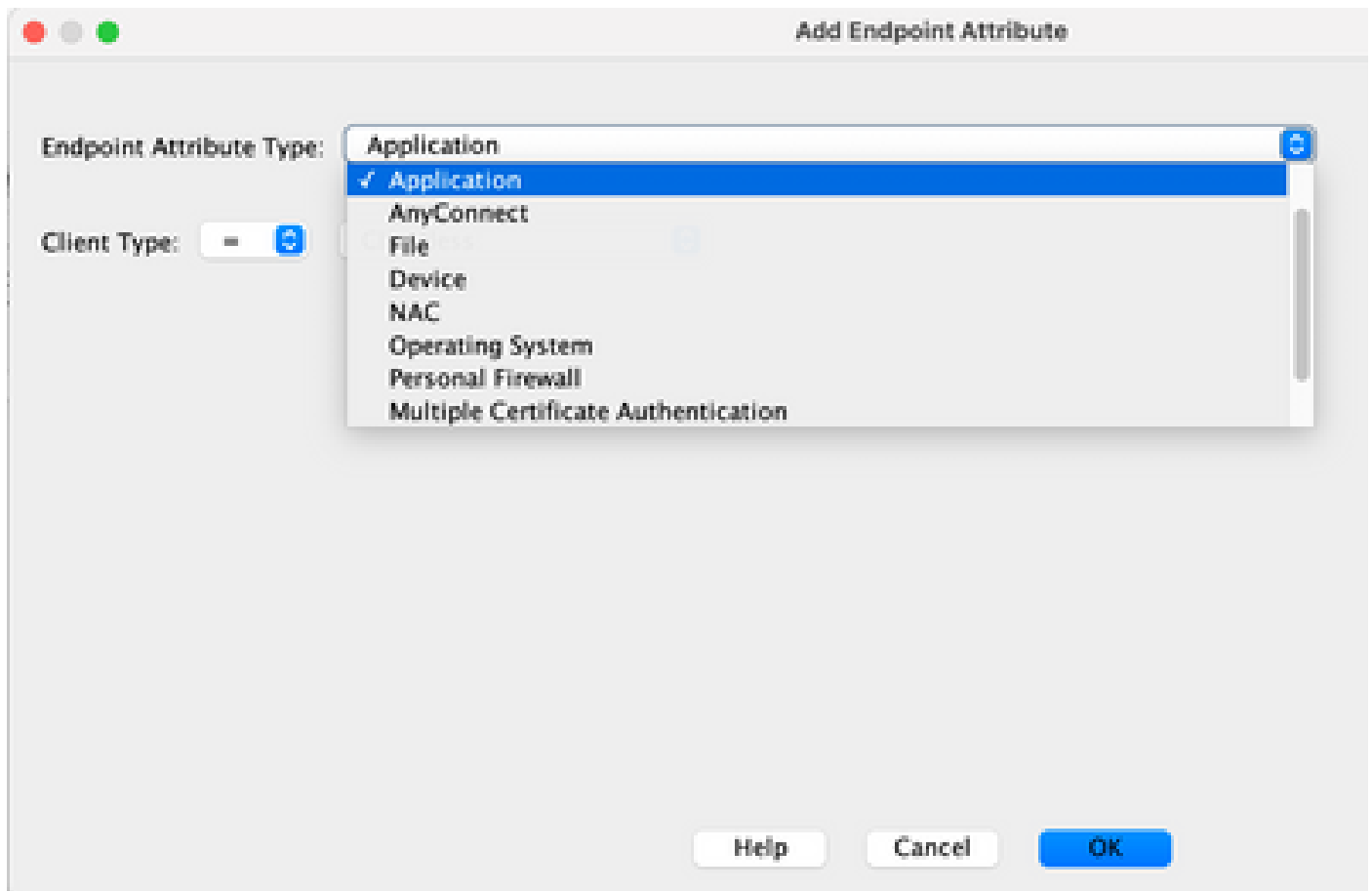
図 1.DAP AAA属性GUI



DAP とエンドポイント セキュリティ属性

セキュリティアプライアンスは、AAA属性に加えて、設定したポスチャ評価方式を使用してエンドポイントセキュリティ属性を取得することもできます。これには、図2に示すように、Basic Host Scan、Secure Desktop、Standard/Advanced Endpoint Assessment、NACが含まれます。Endpoint Assessment属性が取得され、ユーザ認証の前にセキュリティアプライアンスに送信されます。ただし DAP レコード全体を含む AAA 属性は、ユーザ認証中に検証されます。

図 2 : エンドポイント属性 GUI

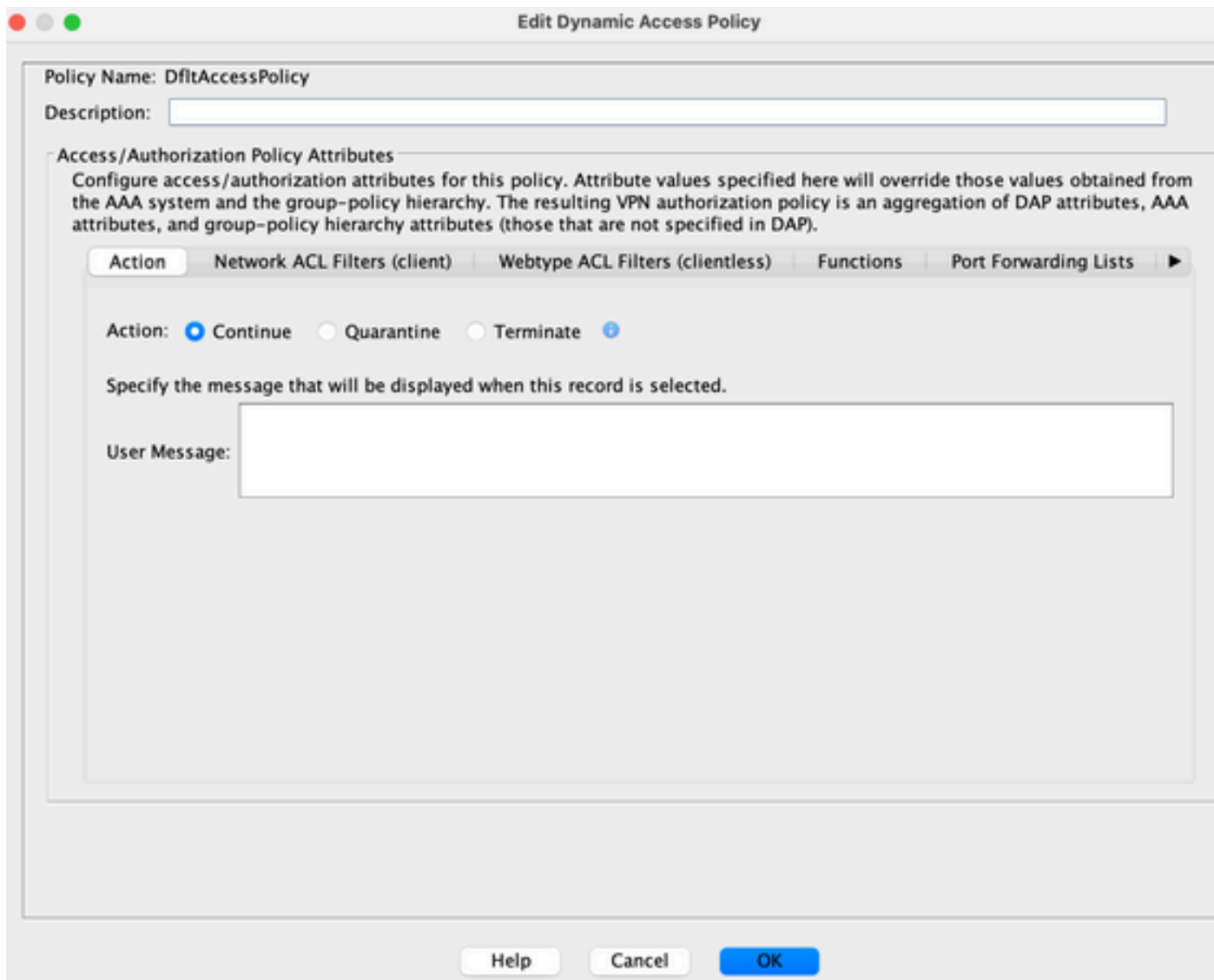


デフォルトのダイナミック アクセス ポリシー

DAPの導入と実装の前は、特定のユーザトンネルまたはセッションに関連付けられたアクセスポリシーの属性と値のペアは、ASAでローカルに（つまり、トンネルグループとグループポリシーで）定義されたか、外部のAAAサーバを介してマッピングされていました。

デフォルトでは常に DAP が適用されます。たとえば、DAPを明示的に適用せずに、トンネルグループ、グループポリシー、およびAAAを介してアクセスコントロールを適用すると、この動作が引き続き発生する可能性があります。従来の動作の場合は DAP 機能（デフォルト DAP レコード DfltAccessPolicy を含む）の設定変更は不要です（図 3 を参照）。

図 3 : デフォルトのダイナミック アクセス ポリシー



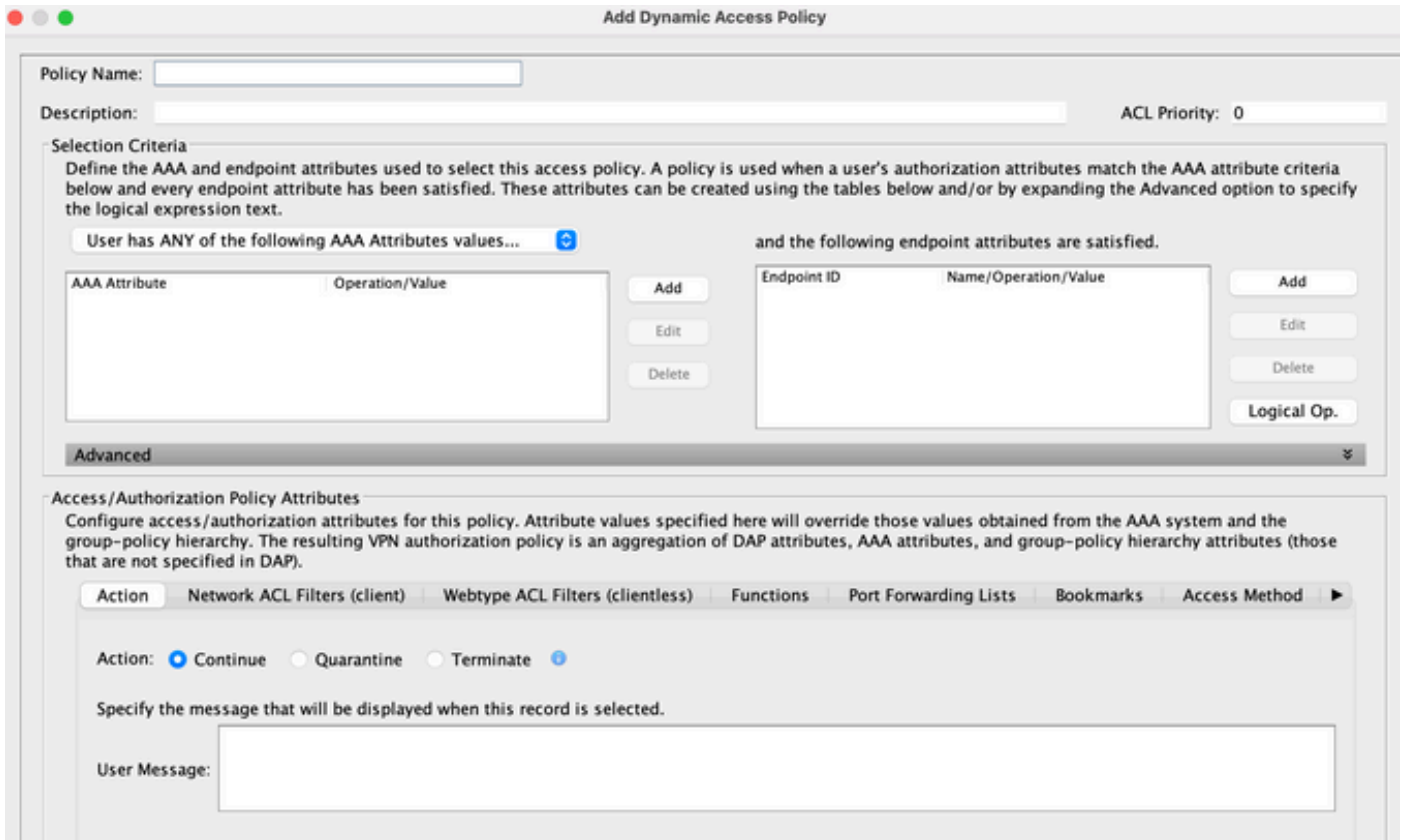
ただし、DAPレコードのいずれかのデフォルト値(たとえば、DfltAccessPolicyのAction:パラメータ)がデフォルト値のTerminateから変更され、追加のDAPレコードが設定されていない場合でも、認証されたユーザはデフォルトでDfltAccessPolicy DAPレコードと照合してVPNアクセスを拒否できます。

その結果、VPN接続を許可し、認証されたユーザがアクセスを許可されるネットワークリソースを定義するために、1つ以上のDAPレコードを作成して設定する必要があります。したがって、DAPが設定されている場合は、レガシーポリシーの適用よりも優先されます。

ダイナミックアクセスポリシーの設定

DAPを使用してユーザがアクセスできるネットワークリソースを定義する場合、考慮すべきパラメータが数多くあります。たとえば、接続エンドポイントが管理対象、管理対象外、非信頼のいずれの環境からのものかを特定する場合は、接続エンドポイントを特定するために必要な選択基準を決定し、エンドポイント評価とAAAクレデンシャルに基づいて、接続ユーザがアクセスを許可されているネットワークリソースを決定します。これを実現するには、まず図4に示すように、DAPの機能を理解する必要があります。

図4：ダイナミックアクセスポリシー



DAP レコードを設定するには主に次の2つの点について検討する必要があります。

- 選択基準 ([Advanced] のオプションを含む)
- アクセス ポリシー属性

[Selection Criteria] セクションでは、特定の DAP レコードを選択するために使用される AAA 属性とエンドポイント属性を管理者が設定します。DAP レコードが使用されるのは、ユーザの認可属性が AAA 属性基準に一致しており、すべてのエンドポイント属性の基準が満たされている場合です。

たとえば、AAA属性タイプLDAP(Active Directory)を選択し、属性名にmemberOf、値文字列にContractorsを指定した場合 (図5aを参照)、AAA属性基準を満たすには、認証を行うユーザがActive DirectoryグループContractorsのメンバーである必要があります。

認証ユーザは、AAA属性基準を満たすだけでなく、エンドポイント属性基準も満たす必要があります。たとえば、管理者が接続エンドポイントのポスチャを判別するように設定し、そのポスチャ評価に基づいて、この評価情報を図5bに示すエンドポイント属性の選択基準として使用できます。

図 5a. AAA 属性基準

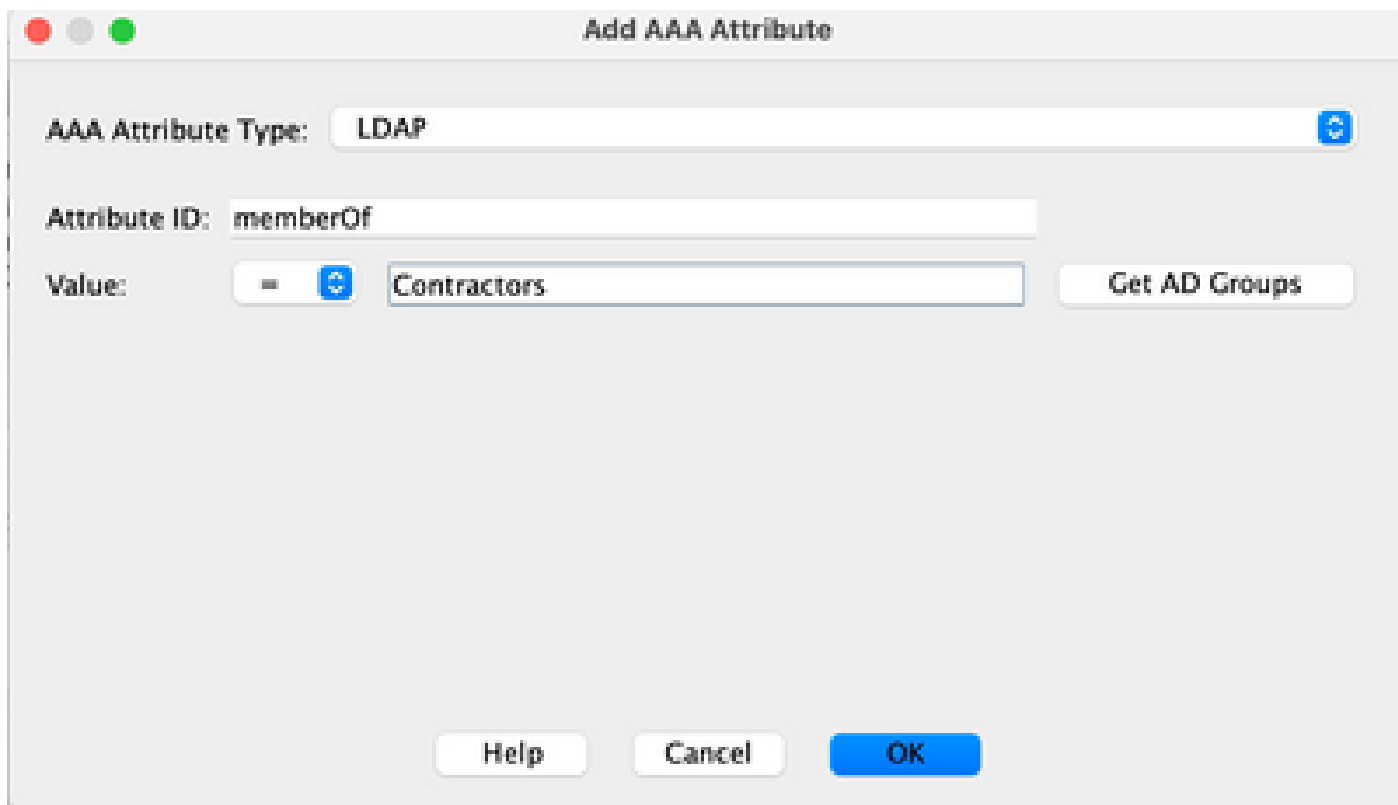


図 5b. エンドポイント属性基準

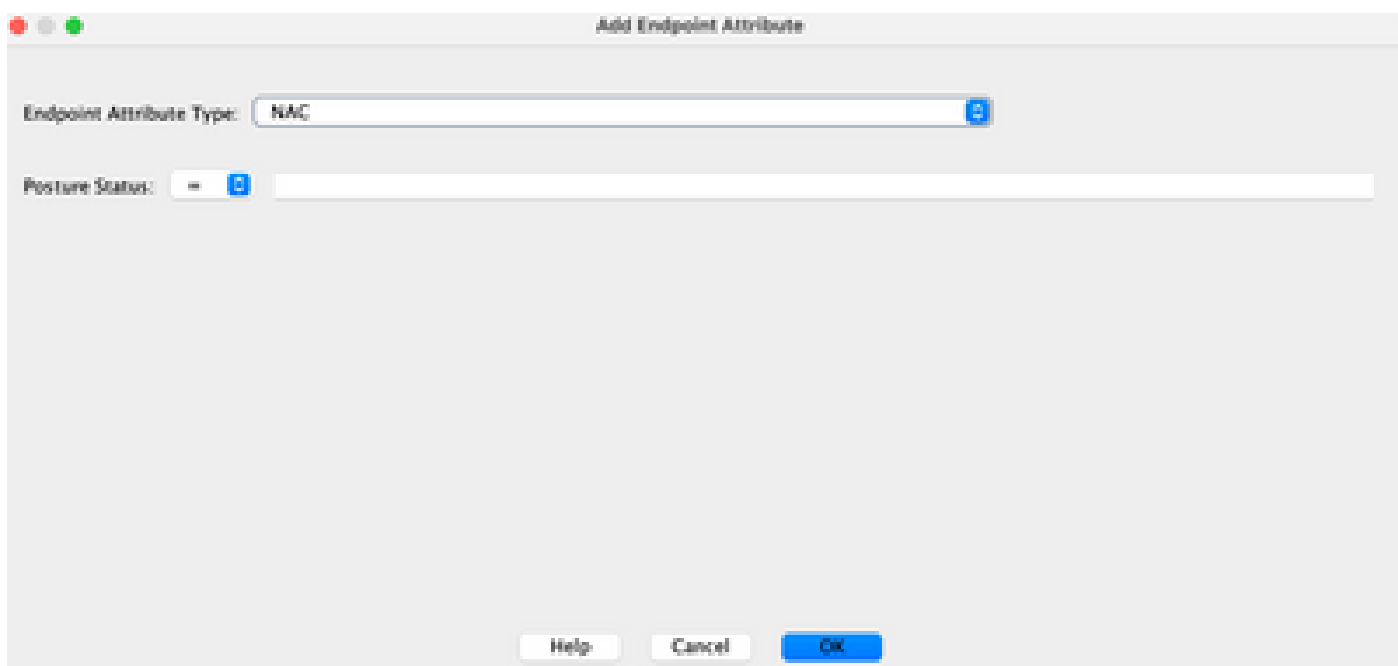
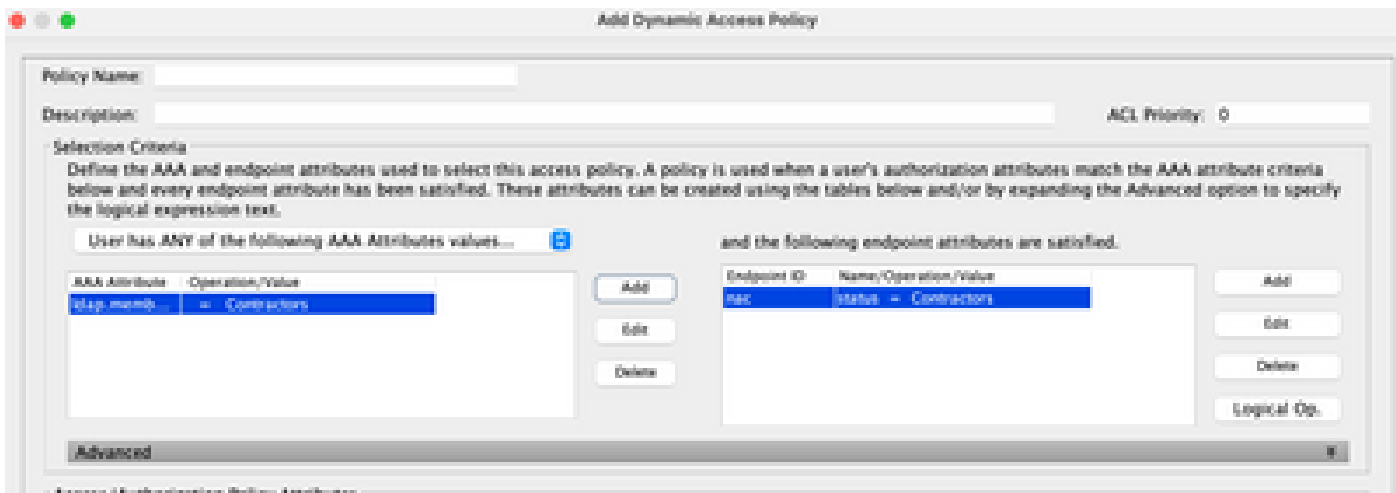


図 6.AAA 属性とエンドポイント属性の基準への一致



AAA 属性とエンドポイント属性を作成するには、図 6 に示されているテーブルを使用するか、または図 7 に示すように [Advanced] オプションを展開して論理式を指定します。現在、論理式は EVAL 関数で構成されています。たとえば、AAA やエンドポイント選択論理操作を表す EVAL (endpoint.av.McAfeeAV.exists, "EQ", "true", "string") や EVAL (endpoint.av.McAfeeAV.description, "EQ", "McAfee VirusScan Enterprise", "string") です。

論理式は、前述のように AAA およびエンドポイント属性領域で可能な選択条件とは異なる選択基準を追加する必要がある場合に便利です。たとえば、指定された基準のいずれか、またはすべてを満たす、あるいはすべてを満たさない AAA 属性を使用するようにセキュリティアプライアンスを設定できますが、エンドポイント属性は累積されるため、すべてを満たす必要があります。セキュリティアプライアンスが特定のエンドポイント属性を使用するようにするには、DAP レコードの [Advanced] セクションで該当する論理式を作成する必要があります。

図 7 拡張属性を作成するための論理式 GUI

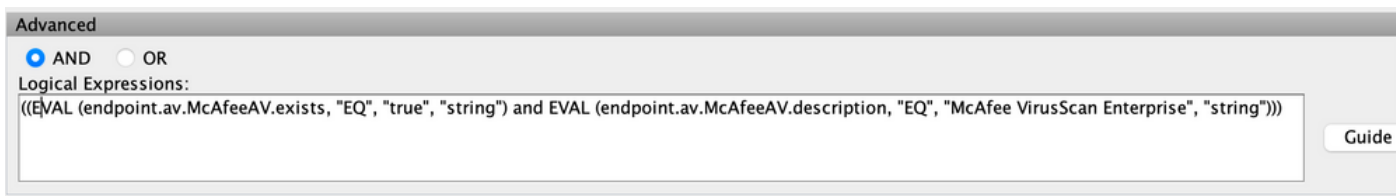
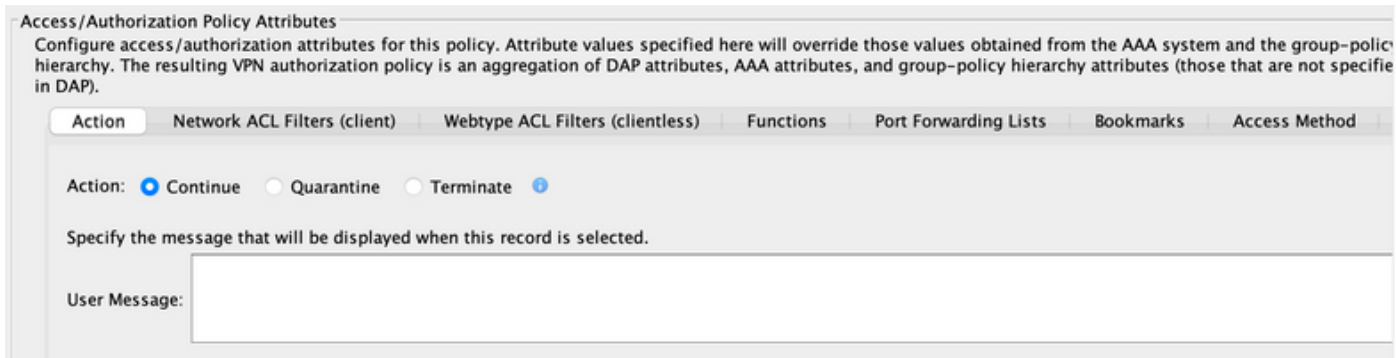


図 8 に示す [Access Policy Attributes] セクションでは、管理者が特定の DAP レコードの VPN アクセス属性を設定します。ユーザ認可属性が AAA、エンドポイント、論理式の基準に一致する場合、このセクションで設定したアクセスポリシー属性値を適用できます。ここで指定する属性値は、既存のユーザ、グループ、トンネルグループ、およびデフォルトグループレコードの値など、AAA システムから取得した値を上書きできます。

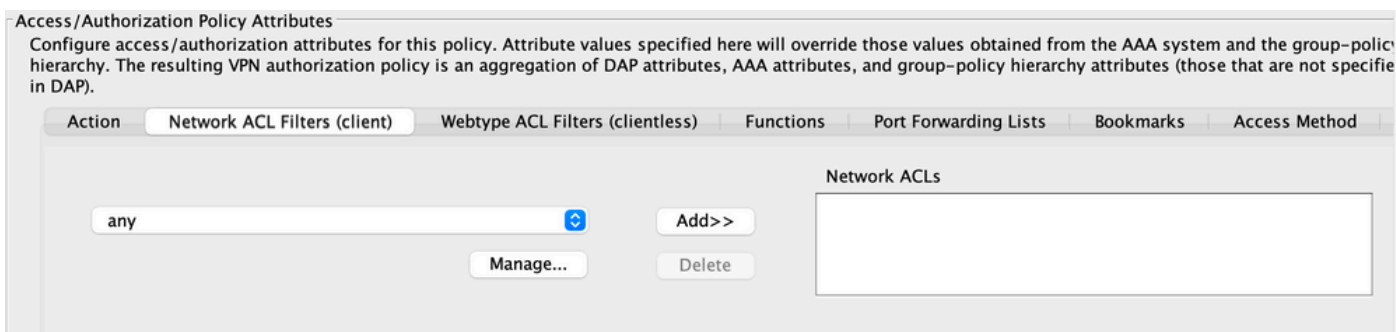
DAP レコードには、設定可能な属性値がいくつかあります。これらの値は、図 8 ~ 14 に示すタブに分類されます。

図 8.[Action] : 特定の接続またはセッションに適用される特別な処理を指定します。



- [Continue] : (デフォルト) クリックするとセッションにアクセス ポリシー属性が適用されます。
- [Terminate] : クリックするとセッションが終了します。
- [User Message] : この DAP レコードが選択されるときに、ポータル ページに表示するテキスト メッセージを入力します。最大 128 文字を入力できます。ユーザ メッセージは、黄色のオーブとして表示されます。ユーザがログインすると、メッセージは 3 回点滅してから静止します。数件の DAP レコードが選択され、それぞれにユーザ メッセージがある場合は、ユーザ メッセージがすべて表示されます。このようなメッセージには、URL やその他の埋め込みテキストを含めることができます。この場合は、正しい HTML タグを使用する必要があります。

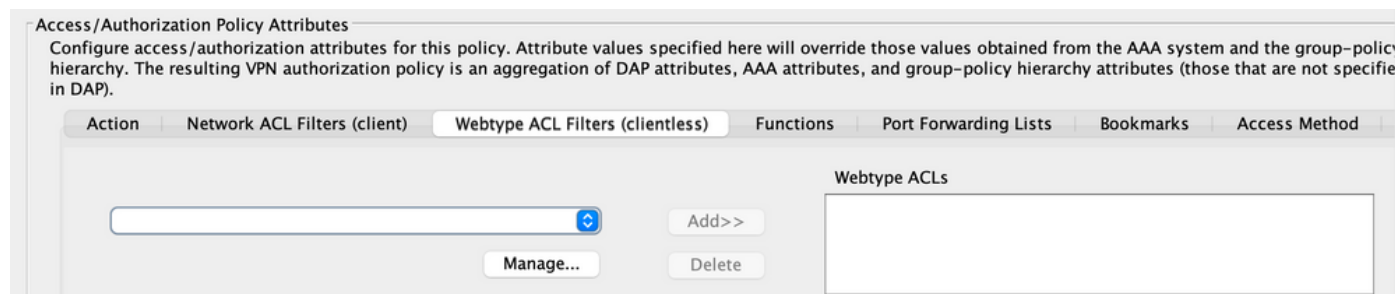
図 9. Network ACL Filters タブ : この DAP レコードに適用するネットワーク ACL を選択して設定できます。DAP の ACL には許可ルールまたは拒否ルールのいずれかを含めることができますが、両方を含めることはできません。ACL に許可ルールと拒否ルールの両方が含まれる場合は、セキュリティ アプライアンスで ACL 設定が拒否されます。



- Network ACL ドロップダウンボックスは、この DAP レコードに追加するためにすでに設定されているネットワーク ACL です。すべての許可ルールまたは拒否ルールを持つ ACL のみが適格で、これらがここに表示される唯一の ACL です。
- [Manage] : ネットワーク ACL を追加、編集、および削除します。
- ネットワーク ACL : この DAP レコードのネットワーク ACL のリスト。
- [Add] : ドロップダウン ボックスから選択したネットワーク ACL を右側の [Network ACLs] リストに追加します。
- [Delete] : [Network ACLs] リストから、選択したネットワーク ACL を削除します。DAP レ

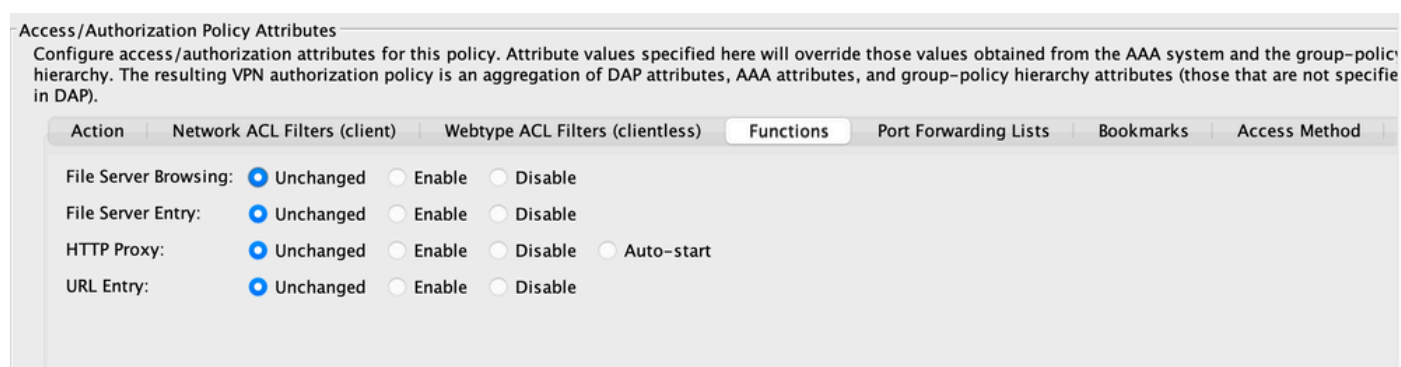
コードまたはその他のレコードに割り当てられている ACL は削除できません。

図 10 Web-Type ACL Filters タブ：この DAP レコードに適用する Web-type ACL を選択して設定できません。DAP の ACL には、許可ルールだけまたは拒否ルールだけを含めることができます。ACL に許可ルールと拒否ルールの両方が含まれる場合は、セキュリティ アプライアンスで ACL 設定が拒否されます。



- [Web-Type ACL] ドロップダウン ボックス：この DAP レコードに追加する、すでに設定済みの Web-type ACL を選択します。すべての許可ルールまたはすべての拒否ルールを含む ACL だけが適格とされ、これらの適格な ACL だけがここに表示されます。
- Manage...: Web-type ACL を追加、編集、および削除します。
- [Web-Type ACL] リスト：この DAP レコードの Web-type ACL を表示します。
- [Add]：ドロップダウン ボックスから選択した Web-type ACL を右側の [Web-Type ACLs] リストに追加します。
- [Delete]：[Web-Type ACLs] リストから Web-type ACL を削除します。DAP レコードまたはその他のレコードに割り当てられている ACL は削除できません。

図 11 [Functions] タブ：このタブでは、DAP レコードのファイルサーバエントリとブラウジング、HTTP プロキシ、および URL エントリを設定できます。

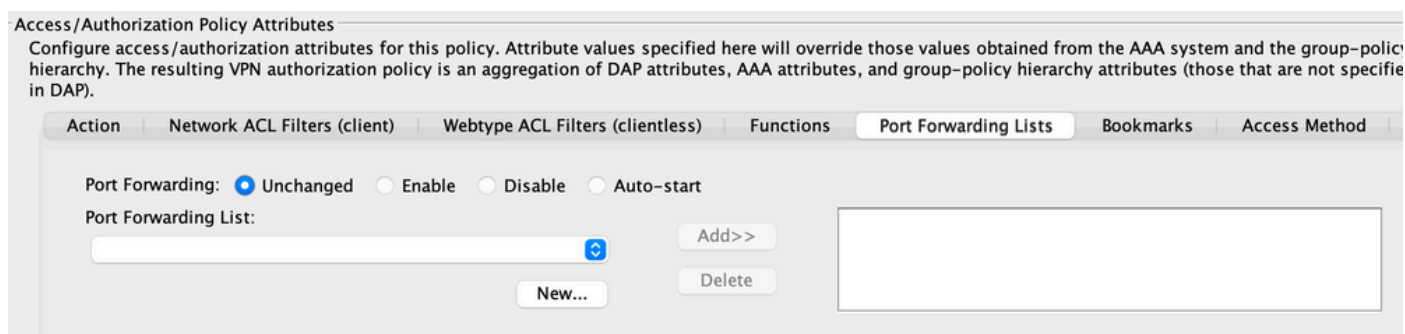


- [File Server Browsing]：ファイル サーバまたは共有機能の CIFS ブラウジングをイネーブルまたはディセーブルにします。
- [File Server Entry]：ポータル ページでユーザがファイル サーバのパスおよび名前を入力できるようにするか、または入力するのを禁止します。イネーブルになっている場合、ポータル ページにファイル サーバ エントリのドロアが配置されます。ユーザは Windows ファイルのパス名を直接入力できます。ユーザは、ファイルをダウンロード、編集、削除、名前

変更、および移動できます。また、ファイルとフォルダを追加することもできます。該当する Windows サーバでユーザ アクセスに対して共有を設定する必要もあります。ネットワーク要件によっては、ファイルにアクセスする前にユーザの認証が必要になる場合があります。

- [HTTP Proxy] : クライアントへの HTTP アプレット プロキシの転送に影響します。このプロキシは、適切なコンテンツ変換に干渉するテクノロジー (Java、ActiveX、Flash など) に対して有用です。セキュリティアプライアンスの継続的な使用を保証しながら、マングリング/書き換えプロセスをバイパスします。転送されたプロキシは、自動的にブラウザの古いプロキシ設定を変更して、すべての HTTP および HTTPS 要求を新しいプロキシ設定にリダイレクトします。HTML、CSS、JavaScript、VBScript、ActiveX、Javaなど、ほとんどすべてのクライアント側テクノロジーをサポートしています。サポートされているブラウザは、Microsoft Internet Explorer だけです。
- [URL Entry] : ポータル ページでユーザが HTTP/HTTPS URL を入力できるようにするか、または入力できないようにします。この機能がイネーブルになっている場合、ユーザは URL 入力ボックスに Web アドレスを入力できます。また、クライアントレス SSL VPN を使用して、これらの Web サイトにアクセスできます。
- [Unchanged] : (デフォルト) このセッションに適用されるグループ ポリシーの値を使用します。
- [Enable]/[Disable] : 機能をイネーブルまたはディセーブルにします。
- [Auto-start] : HTTP プロキシをイネーブルにし、DAP レコードにより、これらの機能に関連付けられたアプレットを自動的に起動させます。

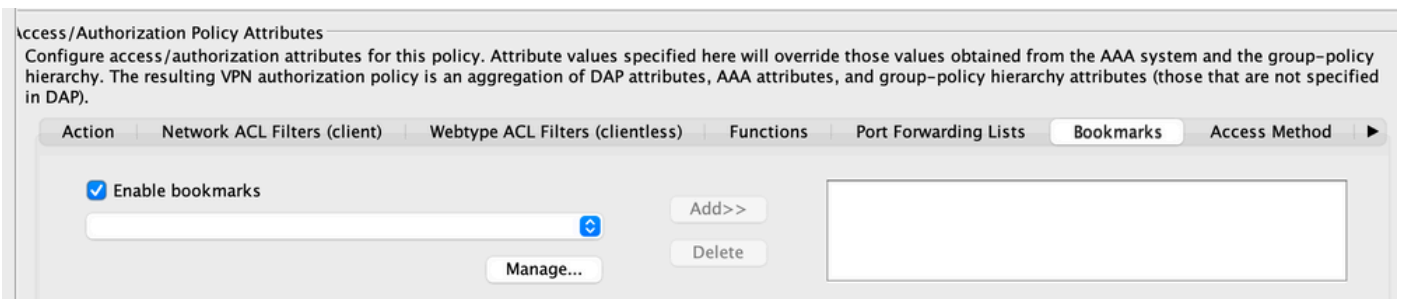
図 12. Port Forwarding Lists タブ : このタブでは、ユーザセッションのポート転送リストを選択および設定できます。



- [Port Forwarding] : この DAP レコードに適用されるポート転送リストのオプションを選択します。このフィールドのその他の属性は、[Port Forwarding] を [Enable] または [Auto-start] に設定した場合にだけイネーブルになります。
- [Unchanged] : このセッションに適用されるグループ ポリシーの値を使用します。
- [Enable]/[Disable] : ポート転送をイネーブルまたはディセーブルにします。
- [Auto-start] : ポート転送をイネーブルにし、DAP レコードに、そのポート転送リストに関連付けられたポート転送アプレットを自動的に起動させます。

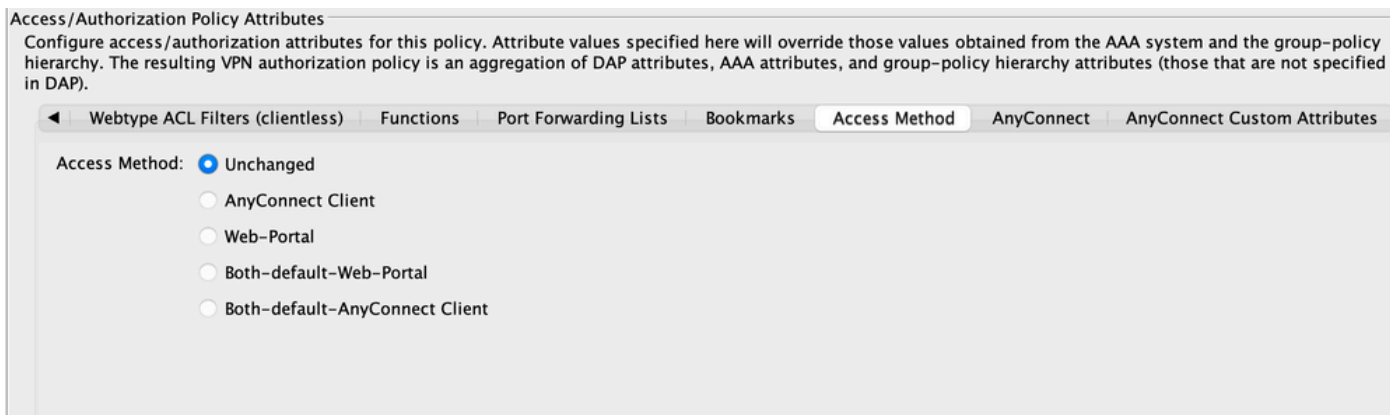
- [Port Forwarding List] ドロップダウン ボックス : DAP レコードに追加する、すでに設定済みのポート転送リストを選択します。
- [New] : 新しいポート転送リストを設定します。
- [Port Forwarding Lists] : DAP レコードのポート転送リストを表示します。
- [Add] : ドロップダウン ボックスから選択したポート転送リストを右側のポート転送リストに追加します。
- 削除 : 選択したポートフォワーディングリストをポートフォワーディングリストから削除します。DAP レコードまたはその他のレコードに割り当てられている ACL は削除できません。

図 13.[ブックマーク]タブ : ユーザー・セッションのブックマーク/URLリストを選択および構成できます。



- ブックマークを使用可能にする : クリックすると使用可能になります。このボックスが選択されていない場合、接続のポータル・ページにはブックマーク・リストが表示されません
- [Manage] : ブックマーク リストを追加、インポート、エクスポート、削除します。
- [Bookmarks Lists] (ドロップダウン) : DAP レコードのブックマーク リストを表示します。
- [Add] : ドロップダウン ボックスから選択したブックマーク リストを右側のブックマーク リスト ボックスに追加します。
- [Delete] : ブックマーク リスト ボックスから選択したブックマークリストを削除します。セキュリティ アプライアンスからブックマーク リストを削除するには、まず DAP レコードからそのリストを削除する必要があります。

図 14.Methodタブ : 許可するリモートアクセスのタイプを設定できます。



- Unchanged : セッションのグループポリシーで設定されている現在のリモートアクセス方式で続行します。
- [AnyConnect Client] : Cisco AnyConnect VPN Client を使用して接続します。
- Webポータル : クライアントレスVPNに接続します。
- [Both-default-Web-Portal] : クライアントレスまたは AnyConnect Client のいずれかによって接続します。デフォルトはクライアントレスです。
- [Both-default-AnyConnect Client] : クライアントレスまたは AnyConnect Client のいずれかによって接続します。デフォルトは AnyConnect です。

前述のように、DAPレコードには限られたデフォルト属性値があります。これらの値は、変更されている場合にだけ、現在のAAA、ユーザ、グループ、トンネルグループ、およびデフォルトグループレコードよりも優先されます。スプリットトンネリングリスト、バナー、スマートトンネル、ポータルカスタマイズなど、DAPの範囲外の属性値が追加が必要な場合は、AAA、ユーザ、グループ、トンネルグループ、およびデフォルトグループレコードを使用して適用する必要があります。この場合、これらの特定の属性値はDAPを補完し、上書きすることはできません。したがって、ユーザはすべてのレコードにわたって属性値の累積セットを取得します。

複数のダイナミックアクセスポリシーの集約

管理者は複数の DAP レコードを設定することで複数の変数に対応できます。その結果、認証を行うユーザは、複数のDAPレコードのAAA属性とエンドポイント属性の基準を満たすことができます。その結果、アクセスポリシー属性は、これらのポリシー全体で一貫しているか、または競合している可能性があります。この場合、認可ユーザは、一致したすべてのDAPレコードの累積結果を取得できます。

これには、認証、認可、ユーザ、グループ、トンネルグループ、およびデフォルトグループレコードによって適用される固有の属性値も含まれます。アクセスポリシー属性が累積された結果として、ダイナミックアクセスポリシーが作成されます。組み合わせられたアクセスポリシー属性の例を次の表に示します。これらの例には、3つのDAPレコードを組み合わせられた結果が示されています。

表 1 に示すアクション属性の値は Terminate と Continue です。集約属性値は、選択されているいずれかのDAPレコードでTerminate値が設定されている場合はTerminateとなり、選択されてい

るすべてのDAPレコードでContinue値が設定されている場合はContinueとなります。

表 1.アクション属性

属性名	DAP#1	DAP#2	DAP#3	DAP
Action (例 1)	continue	continue	continue	continue
Action (例 2)	終了	continue	continue	terminate

表 2 に、文字列値を含むユーザメッセージ属性を示します。集約属性値は、選択されたDAPレコードの属性値をリンクして作成された改行 (16進数値0x0A) 区切りの文字列にすることができます。連結文字列での属性値の順序は特に重要ではありません。

表 2 ユーザメッセージ属性

属性名	DAP#1	DAP#2	DAP#3	DAP
user-message	the quick	brown fox	Jumps over	the quick<LF>brown fox<LF>jumps over

表3に示すクライアントレス機能をイネーブルにする属性 (関数) には、Auto-start、Enable、またはDisableの値が含まれています。選択されているいずれかのDAPレコードでAuto-Start値が設定されている場合、集約属性値はAuto-startになる可能性があります。

選択されているどのDAPレコードでもAuto-start値が設定されておらず、少なくとも1つのDAPレコードでEnable値が設定されている場合は、集約属性値をEnabledにできます。

選択されているどのDAPレコードにもAuto-start値またはEnable 値が設定されておらず、選択されているDAPレコードの少なくとも1つに「disable」値が設定されている場合は、集約属性値を無効にできます。

表 3 クライアントレス機能イネーブル属性 (関数)

属性名	DAP#1	DAP#2	DAP#3	DAP
port-forward	enable	無効化		enable
file-browsing	無効化	enable	無効化	enable
file-entry			無効化	無効化
http-proxy	無効化	auto-start	無効化	auto-start
url-entry	無効化		enable	enable

表4に、URLリスト属性とport-forward属性を示します。これらの属性には、文字列またはカンマで区切られた文字列のいずれかの値が含まれます。集約属性値は、選択したDAPレコードの属性値をリンクするとき作成される、カンマで区切られた文字列にすることができます。結合文字列内の重複する属性値は削除できます。結合文字列内の属性値の順序は重要ではありません。

表 4 URL リスト属性とポート転送リスト属性

属性名	DAP#1	DAP#3	DAP#3	DAP
-----	-------	-------	-------	-----

url-list	a	b,c	a	a,b,c
port-forward		d,e	e,f	d,e,f

Access Method属性では、SSL VPN接続に許可されるクライアントアクセス方式を指定します。クライアントアクセス方式には、AnyConnectクライアントアクセスのみ、Webポータルアクセスのみ、AnyConnectクライアントまたはWebポータルアクセス（デフォルトはWebポータルアクセス）、AnyConnectクライアントまたはWebポータルアクセス（デフォルトはAnyConnectクライアントアクセス）があります。集約属性値の要約を表5に示します。

表5 アクセス方式属性

選択される属性値				集約結果
AnyConnect Client	Web ポータル	Both-default-Web- Portal	Both-default-AnyConnect Client	
			X	Both-default-AnyConnect Client
		X		両方 - デフォルト - Web - ポータル
		X	X	両方 - デフォルト - Web - ポータル
	X			Web-Portal
	X		X	Both-default-AnyConnect Client
	X	X		両方 - デフォルト - Web - ポータル
	X	X	X	両方 - デフォルト - Web - ポータル
X				AnyConnect Client
X			X	Both-default-AnyConnect Client
X		X		両方 - デフォルト - Web - ポータル
X		X	X	両方 - デフォルト - Web - ポータル
X	X			両方 - デフォルト - Web - ポータル
X	X		X	Both-default-AnyConnect Client
X	X	X		両方 - デフォルト - Web - ポータル
X	X	X	X	両方 - デフォルト - Web - ポータル

ネットワーク (ファイアウォール) 属性とWeb-Type (クライアントレス) ACLフィルタ属性を組み合わせる場合、DAPプライオリティとDAP ACLの2つの主要コンポーネントを考慮する必要があります。

図15に示すPriorityトリビュートは集約されません。セキュリティ アプライアンスは、複数のDAP レコードからネットワーク ACL と Web-type ACL を集約するとき、この値を使用してアクセス リストを論理的に順序付けします。セキュリティアプライアンスは、プライオリティ番号の高い順にレコードを並べます。プライオリティ番号の低い順がテーブルの一番下に表示されます。たとえば、値が 4 の DAP レコードは、値が 2 のレコードよりもプライオリティが高くなります。プライオリティは、手動での並べ替えはできません。

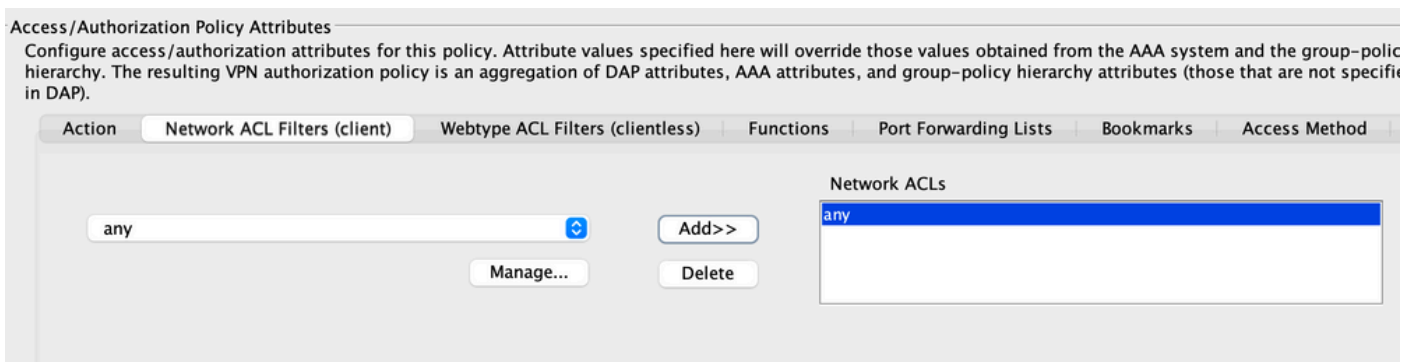
図 15.[Priority] : DAP レコードのプライオリティを表示します。



- [Policy Name] : DAP レコードの名前を表示します。
- [Description] : DAP レコードの目的を説明します。

DAP ACL属性は、厳密なAllow-List ACLモデルまたはBlock-List ACLモデルのいずれかに準拠するアクセスリストのみをサポートします。Allow-List ACLモデルでは、アクセスリストエントリによって、指定されたネットワークまたはホストへのアクセスを「許可」するルールが指定されます。ブロックリスト ACLモードでは、アクセスリストエントリによって、指定されたネットワークまたはホストへのアクセスを拒否するルールが指定されます。非準拠アクセスリストには、許可ルールと拒否ルールが混在したアクセスリストエントリが含まれています。DAPレコードに対して非準拠アクセスリストが設定されている場合、管理者がレコードを追加しようとする、設定エラーとして拒否される可能性があります。準拠するアクセスリストがDAPレコードに割り当てられている場合、準拠の特性を変更するアクセスリストの変更は、設定エラーとして拒否される可能性があります。

図 16.DAP ACL : このDAPレコードに適用するネットワークACLを選択して設定できます。



複数のDAPレコードが選択されると、ネットワーク (ファイアウォール) ACLに指定されているアクセスリスト属性が集約され、DAPファイアウォールACLのダイナミックアクセスリストが作成されます。同様に、Web-Type (クライアントレス) ACLに指定されているアクセスリスト属性が集約され、DAPクライアントレスACLのダイナミックアクセスリストが作成されます。次の例

では、ダイナミックDAPファイアウォールアクセスリストがどのように特別に作成されるかについて説明します。ただし、ダイナミックDAPクライアントレスアクセスリスト(ACL)も同じプロセスを実行できます。

まず、ASAは表6に示すように、DAP Network-ACLの一意の名前を動的に作成します。

表 6 ダイナミック DAP Network-ACL 名

DAP Network-ACL 名
DAP-Network-ACL-X (Xは、一意性を保証するために増分できる整数)

2番目に、ASAは表7に示すように、選択されたDAPレコードからNetwork-ACL属性を取得します。

表 7 ネットワーク ACL

選択される DAP レコード	Priority	Network-ACL	Network-ACL エントリ
DAP 1	1	101 および 102	ACL 101 には 4 つの拒否ルールがあり、ACL 102 には 4 つの許可ルールがある
DAP 2	2	201 および 202	ACL 201 には 3 つの許可ルールがあり、ACL 202 には 3 つの拒否ルールがある
DAP 3	2	101 および 102	ACL 101 には 4 つの拒否ルールがあり、ACL 102 には 4 つの許可ルールがある

3番目に、ASAはDAPレコードのプライオリティ番号によってNetwork-ACLを並べ替え、次に、選択した2つ以上のDAPレコードのプライオリティ値が同じ場合はBlock-List によって並べ替えます。その後、ASAは表8に示すように、各Network-ACLからNetwork-ACLエントリを取得できます。

表 8 DAP レコードの Priority

Network-ACL	Priority	ホワイト/ブラック アクセス リスト モデル	Network-ACL エントリ
101	2	ブラックリスト	4 つの拒否ルール (DDDD)
202	2	ブラックリスト	3 つの拒否ルール (DDD)
102	2	ホワイトリスト	4 つの許可ルール (PPPP)
202	2	ホワイトリスト	3 つの許可ルール (PPP)
101	1	ブラックリスト	4 つの拒否ルール (DDDD)
102	1	ホワイトリスト	4 つの許可ルール (PPPP)

最後に、ASAはダイナミックに生成されたNetwork-ACLにNetwork-ACLエントリをマージし、ダイナミックNetwork-ACLの名前を、適用する新しいNetwork-ACLとして返します (表9を参照)。

表 9 ダイナミック DAP Network-ACL

DAP Network-ACL 名	Network-ACL エントリ
-------------------	------------------

DAP 実装

管理者がDAPの実装を検討する必要がある理由は数多くあります。このような理由としては、エンドポイントのポスチャ評価を適用する場合や、認可対象ユーザがネットワークリソースにアクセスするときにより細かなAAA属性またはポリシー属性を検討する場合などがあります。次の例では、DAPとそのコンポーネントを設定して、接続エンドポイントを特定し、さまざまなネットワークリソースへのユーザアクセスを許可できます。

テストケース：クライアントから次のVPNアクセス要件を持つ概念実証が要求されました。

- 従業員のエンドポイントを検出し、管理対象または管理対象外として識別する機能。—エンドポイントが管理対象（ワークPC）と識別されたが、ポスチャ要件を満たしていない場合、そのエンドポイントのアクセスを拒否する必要があります。一方、従業員のエンドポイントが管理対象外（ホームPC）と識別された場合、そのエンドポイントに対してクライアントレスアクセスを付与する必要があります。
- クライアントレス接続の終了時にセッションのcookieとキャッシュのクリーンアップを実行できること。
- McAfee AntiVirusなど、管理対象の従業員エンドポイントで実行中のアプリケーションを検出して適用する機能。アプリケーションが存在しない場合、エンドポイントのアクセスを拒否する必要があります。
- AAA認証を使用して、認可されたユーザがアクセスする必要があるネットワークリソースを判別する機能。セキュリティアプライアンスではネイティブMS LDAP認証と複数のLDAPグループメンバーシップロールがサポートされている必要があります。
- クライアント/ネットワークベースの接続を介して接続したときに、ネットワークリソース（ネットワークFAXやプリンタなど）へのローカルLANアクセスを許可する機能。
- 契約作業員にゲストアクセスを認可できること。契約作業員とそのエンドポイントにはクライアントレスアクセスが必要であり、アプリケーションへのポータルアクセスは従業員アクセスに比べて制限が必要です。

この例では、クライアントのVPNアクセス要件を満たすために、一連の設定手順を実行できます。必要な設定手順はあっても、DAPに直接関連していない設定がある場合と、DAPに直接関連している設定がある場合があります。ASAは非常に動的で、多くのネットワーク環境に適応できます。このため、VPNソリューションをさまざまな方法で定義できます。場合によっては、最終的なソリューションが同一になることがあります。ただし、実行されるアプローチは、クライアントのニーズと環境によって決まります。

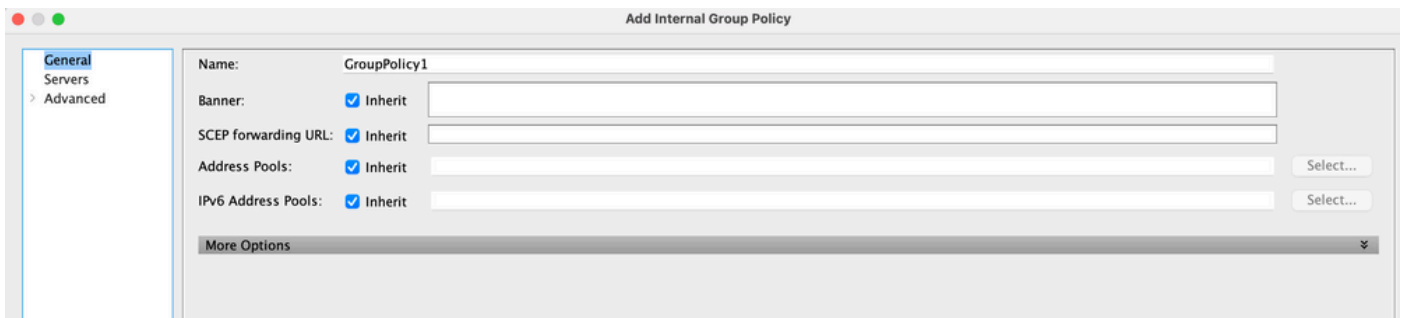
この文書の性質と定義されているクライアント要件に基づいて、Adaptive Security Device Manager(ASDM)を使用し、DAPに関する設定の大部分に焦点を当てることができます。ただし、ローカルグループポリシーを設定して、DAPがローカルポリシー属性をどのように補完または上書きできるかを示すこともできます。このテストケースでは、LDAPサーバグループ、スプリットトンネリングネットワークリスト、および基本的なIP接続（IPプール、DefaultDNSサーバグル

ープなど)が事前に設定されているものとします。

グループポリシーの定義：ローカルポリシー属性の定義に必要な設定です。ここで定義する属性の一部は、DAPでは設定できません(例：Local LAN Access)。(このポリシーは、クライアントレス属性とクライアントベース属性の定義にも使用できます)。

Configuration > Remote Access VPN > Network (Client) Access > Group Policiesの順に移動し、次に示すようにInternal Group Policyを追加します。

図 17.[Group Policy]：ローカルVPN固有の属性を定義します。



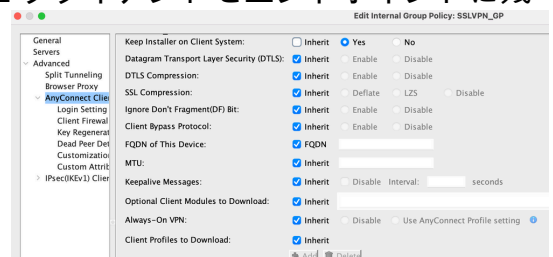
- Generalリンクの下で、グループポリシーのnameSSLVPN_GPを設定します。
- また、GeneralリンクでMore Optionsをクリックし、Tunneling Protocol:Clientless SSLVPNのみを設定します(アクセス方式を上書きして管理するようにDAPを設定できます)。
- Advanced > Split Tunnelingリンクの下で、次の手順を設定します。

図 18.[Split Tunneling]：クライアント接続時に、指定したトラフィック(ローカルネットワーク)が暗号化されていないトンネルをバイパスできるようにします。



- ポリシー：UncheckInheritand selectExclude Network List.
 - ネットワークリスト：継承のチェックを外し、リストnameLocal_Lan_Accessを選択します。(事前設定されているものと仮定します)。
- Advanced > ANYCONNECT Clientリンクの下で、次の手順を設定します。

図 19.[SSL VPN Client Installer]：VPN終了時に、SSLクライアントをエンドポイントに残



すか、またはアンインストールすることができます。

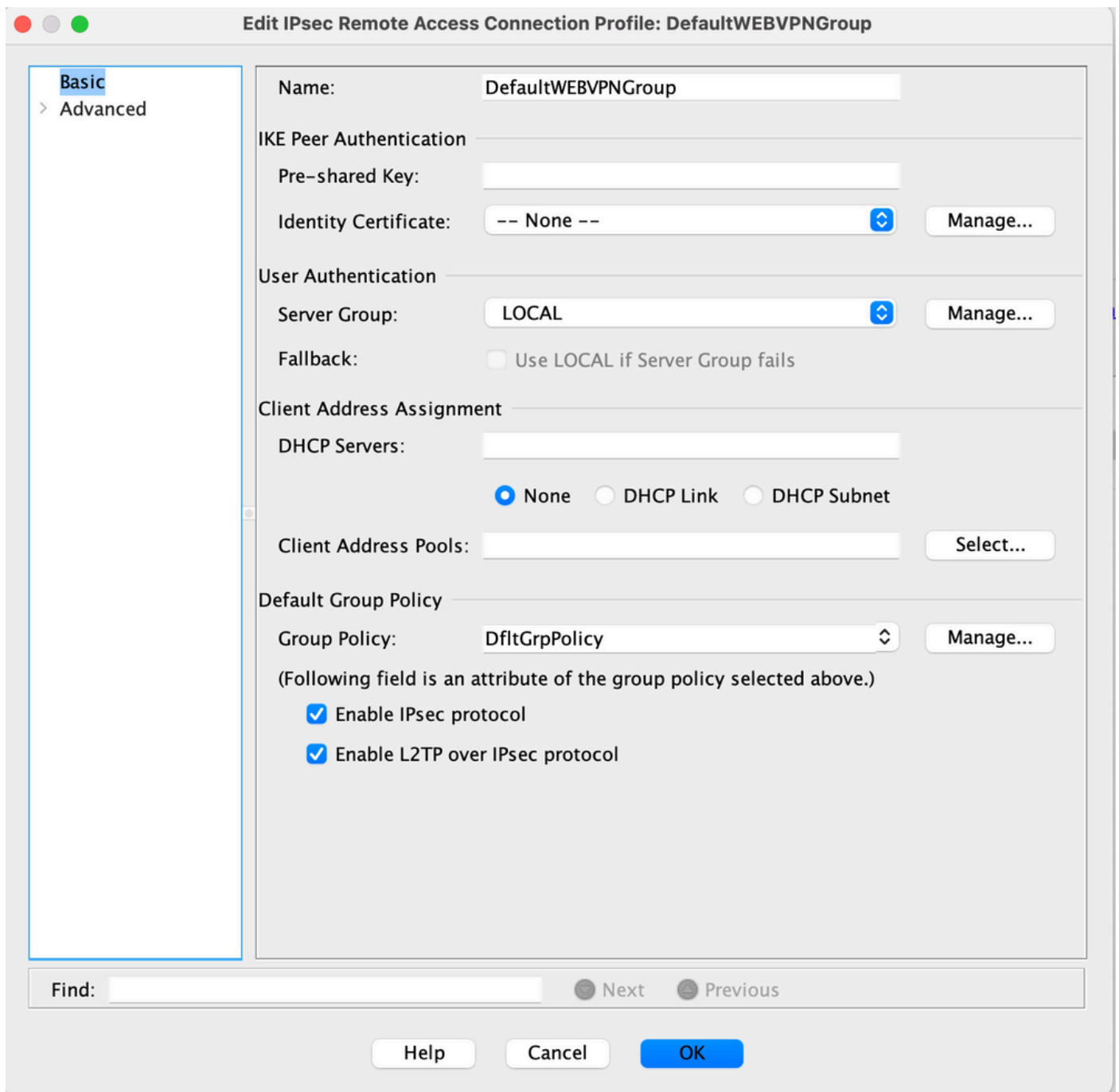
- クライアントシステムにインストーラを保持する：UncheckInheritand then selectYes.
- OKthenApplyをクリックします。

g. 設定変更を適用します。

接続プロファイルの定義：この設定は、AAA認証方式（LDAPなど）を定義し、以前に設定したグループポリシー(SSLVPN_GP)をこの接続プロファイルに適用するために必要です。この接続プロファイルを使用して接続するユーザは、ここで定義する属性と、SSLVPN_GPグループポリシーで定義する属性の対象になります。（このプロファイルは、クライアントレス属性とクライアントベース属性の両方の定義にも使用できます）。

Configuration > Remote Access VPN > Network (Client) Access > IPsec Remote Access Connection Profileの順に移動し、次のように設定します。

図 20.接続プロファイル：ローカルVPN固有の属性を定義します。



a. Connection ProfilesセクションでDefaultWEBVPNGroupを編集し、Basicリンクで次の手順

を設定します。

- a. 認証：方式：AAA
- b. 認証：AAAサーバグループ：LDAP (事前設定されていると想定)
- c. クライアントアドレスの割り当て：Client Address Pools:IP_Pool (事前に設定されていると想定)
- d. デフォルトのグループポリシー：グループポリシー：SelectSSLVPN_GP

b. 設定変更を適用します。

SSL VPN接続用のIPインターフェイスの定義：この設定は、指定したインターフェイスでクライアント/クライアントレスSSL接続を終了するために必要です。

インターフェイスでクライアント/ネットワークアクセスを有効にする前に、SSL VPNクライアントイメージを定義する必要があります。

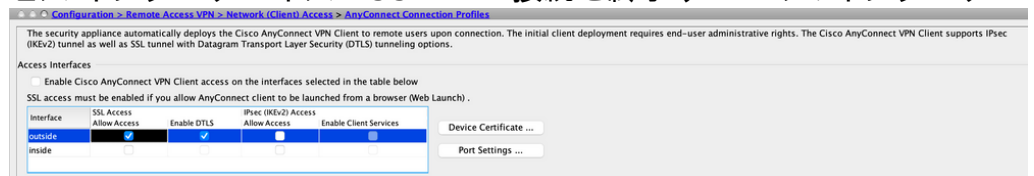
1. Configuration > Remote Access VPN > Network (Client)Access > Anyconnect Client Softwareの順に選択し、次のイメージである、ASAフラッシュファイルシステムからのSSL VPN Client Image:(このイメージはCCO、<https://www.cisco.com>からダウンロードできます)を追加します。

図 21.SSL VPNクライアントイメージのインストール：エンドポイントに接続するためにブッシュするAnyConnectクライアントイメージを定義します。

- a. anyconnect-mac-4.x.xxx-k9.pkg (入手可能)
- b. OK、OK、続いてApplyの順にクリックします。

2. Configuration > Remote Access VPN > Network (Client)Access > AnyConnect Connection Profilesの順に移動し、次の手順を使用してこれを有効にします。

図 22.SSL VPN アクセス インターフェイス：SSL VPN 接続を終了するためのインターフェイスを定義します。



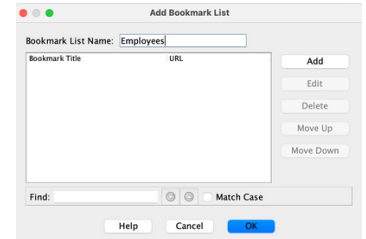
イスを定義します。

- a. Access Interfaceセクションで、Enable:Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the table below.
- b. また、「アクセスインターフェイス」セクションで、外部インターフェイスのAllow Accessをチェックします。(この設定により、外部インターフェイスでSSL VPNクライアントレスアクセスを有効にすることもできます)。
- c. [適用 (Apply)] をクリックします。

クライアントレスアクセスのブックマークリスト (URLリスト) の定義 : この設定は、ポータルで公開するWebベースのアプリケーションを定義するために必要です。従業員と契約作業員の2つのURLリストを定義できます。

1. Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarksの順に移動し、+ をクリックして、次の手順を設定します。

図 23.ブックマーク リスト : Web ポータルで公開し、アクセスできるようにする URL を定



義します (従業員がアクセスできるようにカスタマイズします) 。

- a. Bookmark List Name:Employeesと入力し、Addをクリックします。
- b. ブックマークタイトル : 企業イントラネット
- c. [URL Value] : <https://company.resource.com>

•

OKをクリックし、再度OKをクリックします。

•

+をクリックして追加し、2番目のブックマークリスト (URLリスト) を次のように設定します。

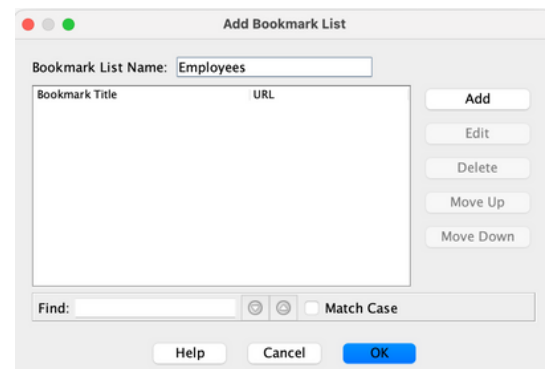


図 24.ブックマーク リスト : ゲスト アクセス用にカスタマイズします。

a.

Bookmark List Name:Contractorsと入力して、Addをクリックします。

b.

ブックマークタイトル：ゲストアクセス

c.

[URL Value] : <https://company.contractors.com>

•

OKをクリックし、再度OKをクリックします。

•

[適用 (Apply)] をクリックします。

ホストスキャンを設定します。

•

Configuration > Remote Access VPN > Secure Desktop Manager > HostScan Imageの順に移動し、次の手順を設定します。

図 25.HostScanイメージのインストール：エンドポイントを接続するためにプッシュするHostScanイメージを定義します

Use this panel to install HostScan.

HostScan configuration can be performed by going to Secure Desktop Manager/HostScan. If 'HostScan' is not visible under 'Secure Desktop Manager', you will need to restart ASDM.

Location:

Enable HostScan

•

a.

disk0:/hostscan_4.xx.xxxxx-k9.pkgimageをASAフラッシュファイルシステムからインストールします。

b.

CheckEnable HostScanを使用します。

c.

[**適用 (Apply)**] をクリックします。

ダイナミック アクセス ポリシー : この設定は、接続ユーザとそのエンドポイントを、定義されている **AAA 基準** と **Endpoint Assessment 基準** に照合して検証するために必要です。DAPレコードで定義されている基準を満たす場合、接続ユーザに対して、そのDAPレコードに関連付けられているネットワークリソースへのアクセス権を付与できます。DAP 認可は認証プロセスで実行されます。

SSL VPN接続がデフォルトケース(たとえば、エンドポイントが設定済みのダイナミックアクセスポリシー(DAP)に一致しない場合)で確実に終了するには、次の手順で設定します。

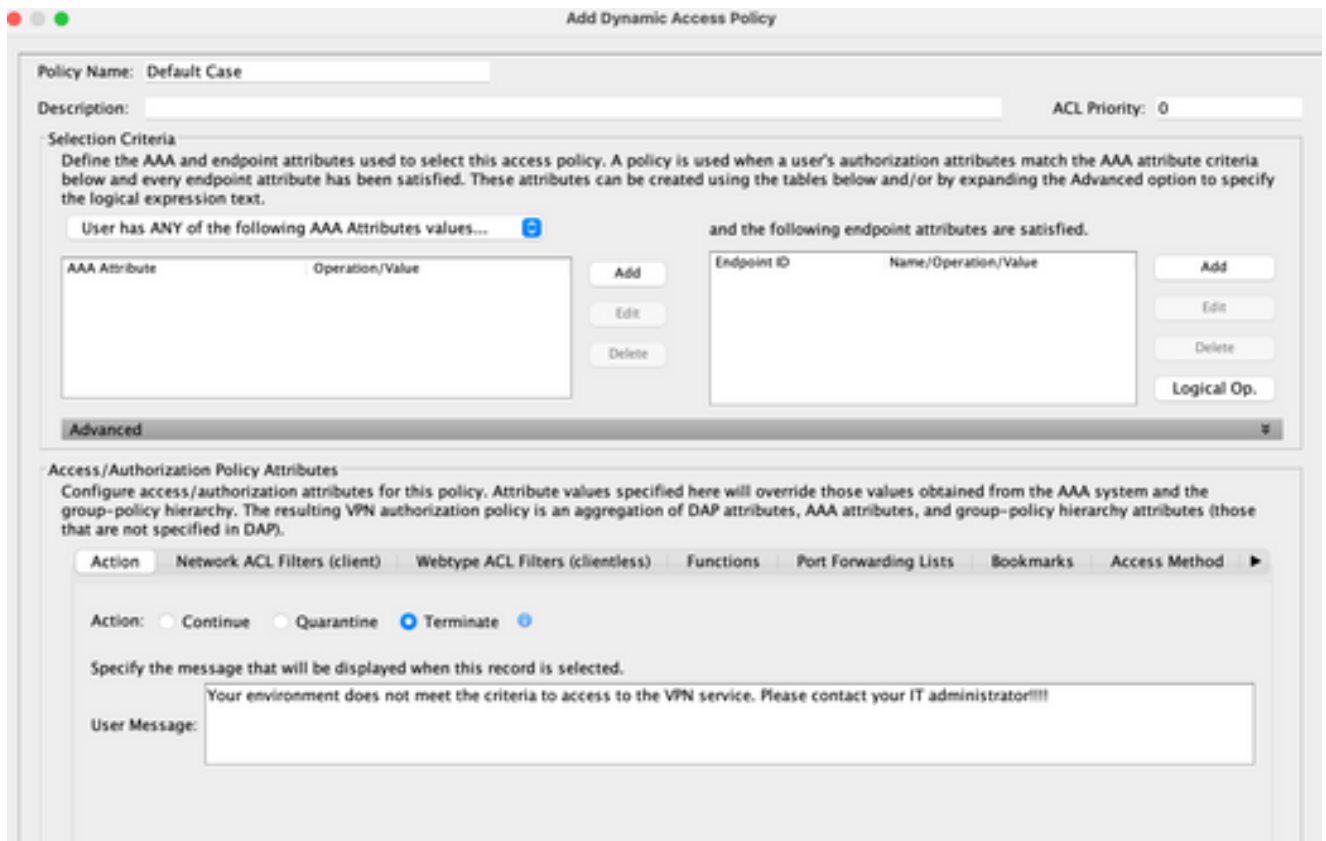


注：ダイナミックアクセスポリシー(DAP)を初めて設定するときには、DAPコンフィギュレーションファイル(DAP.XML)が存在しないことを示すDAP.xmlエラーメッセージが表示されます。初期DAP設定を変更して保存すると、このメッセージは表示されなくなります。

•

Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policiesの順に移動し、次の手順を設定します。

図 30.デフォルトのダイナミックアクセスポリシー(DAP)：事前に定義されたDAPレコードが一致しない場合、このDAPレコードを適用できます。したがって、SSL VPNアクセスを拒否できます。



a.

DfltAccessPolicyを編集し、Actionを**Terminate**に設定します。

b.

[OK] をクリックします。

•
Managed_Endpointsという名前の新しいダイナミックアクセスポリシーを次のように追加します。

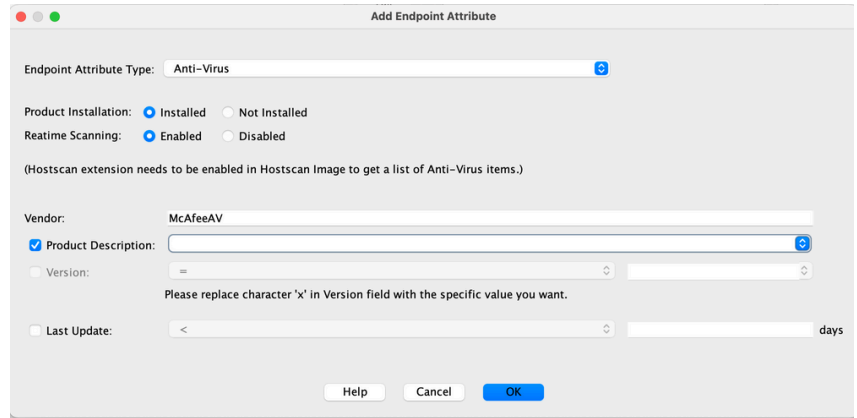
a.

説明：従業員のクライアントアクセス

b.

図31に示すように、エンドポイント属性タイプ (アンチウイルス) を追加します。完了したら、「OK」をクリックします。

図 31.DAPエンドポイント属性 : **Advanced Endpoint Assessment AntiVirus**は、クライアント/ネットワークアクセ



スのDAP基準として使用できます。

C.

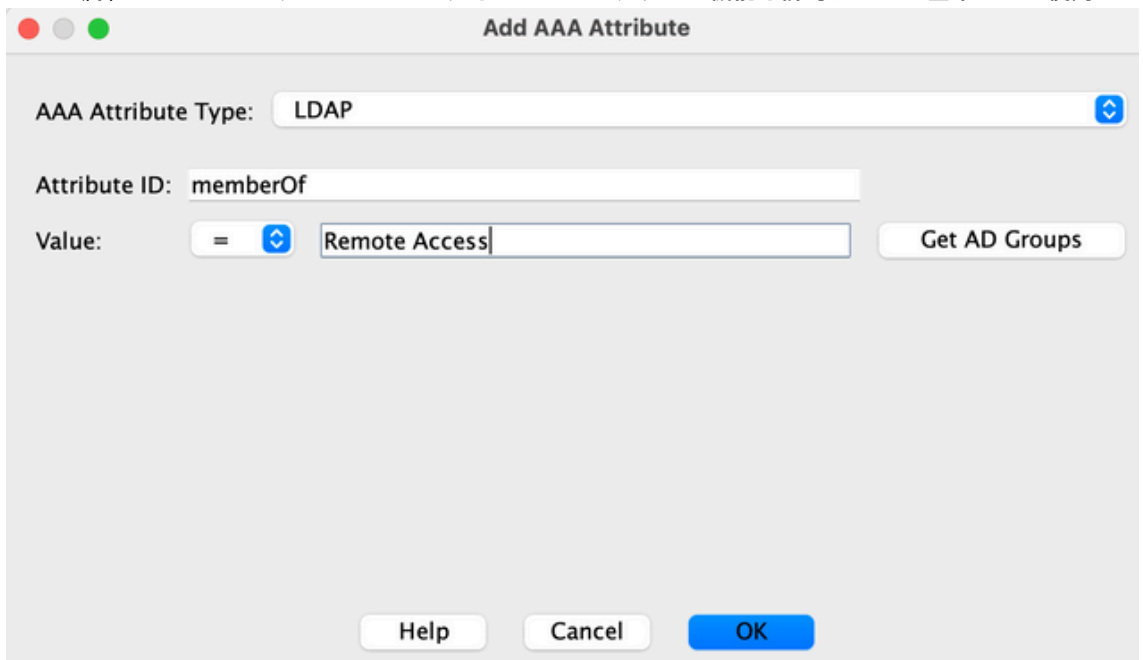
前の図に示すように、ドロップダウンリストのAAA Attributeセクションで、User has ALL of the following AAA Attributes Valuesを選択します。

•

図33および34に示すように、AAA属性タイプ(LDAP)を追加します (AAA属性ボックスの右側)。完了したら、「OK」をクリックします。

図 33.DAP AAA属性 : AAAグループメンバーシップを、従業員を識別するDAP基準として使用できます。

図 34.DAP AAA属性 : AAAグループメンバーシップを、リモートアクセス機能を許可するDAP基準として使用で



きます。

•

図35に示すように、Actionタブで、ActionがContinueに設定されていることを確認します。

図 35.[Action] タブ：この設定は、特定の接続またはセッションの特殊処理を定義するために必要です。DAPレコードが一致し、ActionがTerminateに設定されている場合は、VPNアクセスを拒否できます。



•

図36に示すように、Access MethodタブでAccess MethodAnyConnect Clientを選択します。

図 36.[Access Method] タブ：この設定は、SSL VPN クライアント接続タイプを定義するために必要です。



•

OK、Applyの順にクリックします。

•

「Unmanaged_Endpoints」という名前の2番目のダイナミックアクセスポリシーを次のように追加します。

a.

説明：従業員のクライアントレスアクセス。

b.

AAA属性セクションの上記の図に示されているドロップダウンリストから、User has ALL of the following AAA Attributes Valuesを選択します。

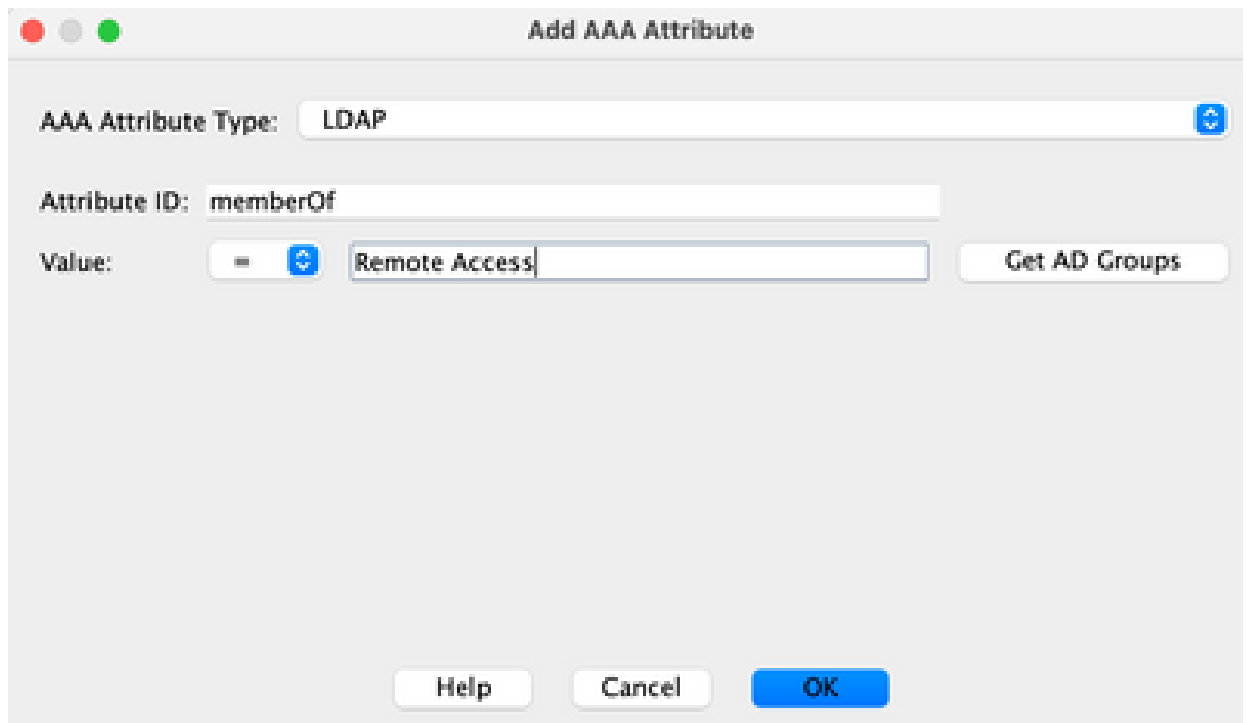
•

図38および39に示すように、AAA属性タイプ(LDAP)の右側に配置されたAAA属性タイプを追加します。完了したら、「OK」をクリックします。

図 38.DAP AAA属性：AAAグループメンバーシップを、従業員を識別するDAP基準として使用できます。



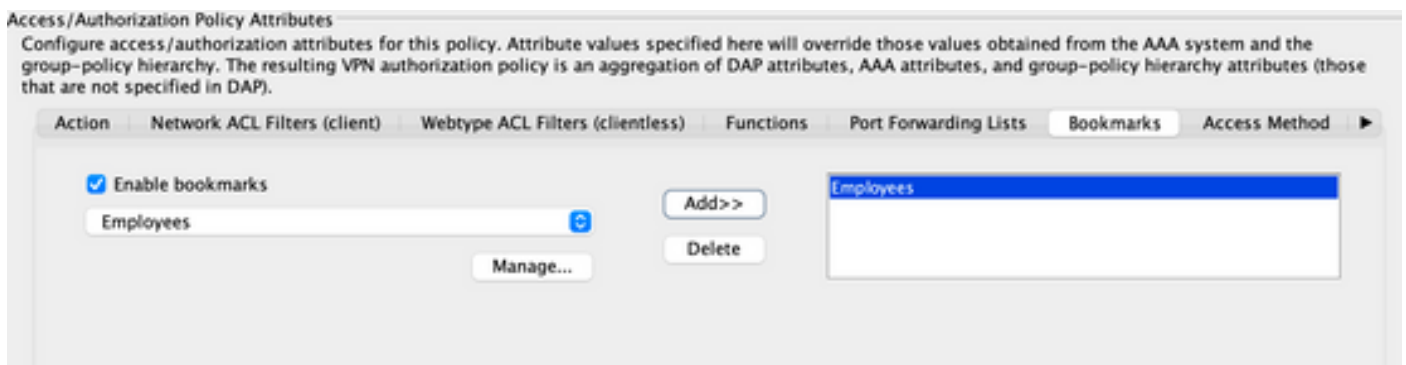
図 39.DAP AAA属性：AAAグループメンバーシップを、リモートアクセス機能を許可するDAP基準として使用できます。



•
Actionタブで、Actionが**Continue**に設定されていることを確認します。(図 35)。

•
[ブックマーク]タブで、ドロップダウンからリストnameEmployeesを選択し、[追加]をクリックします。また、図 40に示すように、Enable bookmarksにチェックマークが付いていることも確認します。

図 40.[ブックマーク]タブ：このタブでは、ユーザセッションのURLリストを選択および設定できます。



a.

Access Methodタブで、Access Method **Web Portal**を選択します。(図 36)。

- **OK、Apply**の順にクリックします。

1. 契約作業員は、DAP AAA属性でのみ識別できます。その結果、エンドポイント属性タイプ：(ポリシー) は手順 4で設定できません。これは、DAP 内の多様性を示すことだけを目的としています。

3.3番目のダイナミックアクセスポリシー**Guest_Access**を追加し、以下の項目を設定します。

-

説明：ゲストクライアントレスアクセス。

-

図 37 に示すように、エンドポイント属性タイプ (Policy) を追加します ([Endpoint Attribute Type] ボックスの右側)。完了したら、「OK」をクリックします。

-

図40では、AAA Attributeセクションのドロップダウンリストから、User has ALL of the following AAA Attributes Valuesを選択します。

-

図41および図42に示すように、AAA属性タイプ(LDAP)を追加します (AAA属性ボックスの右側)。完了したら、「OK」をクリックします。

図 41.DAP AAA属性：AAAグループメンバーシップをDAP基準として使用して契約作業員を識別できます

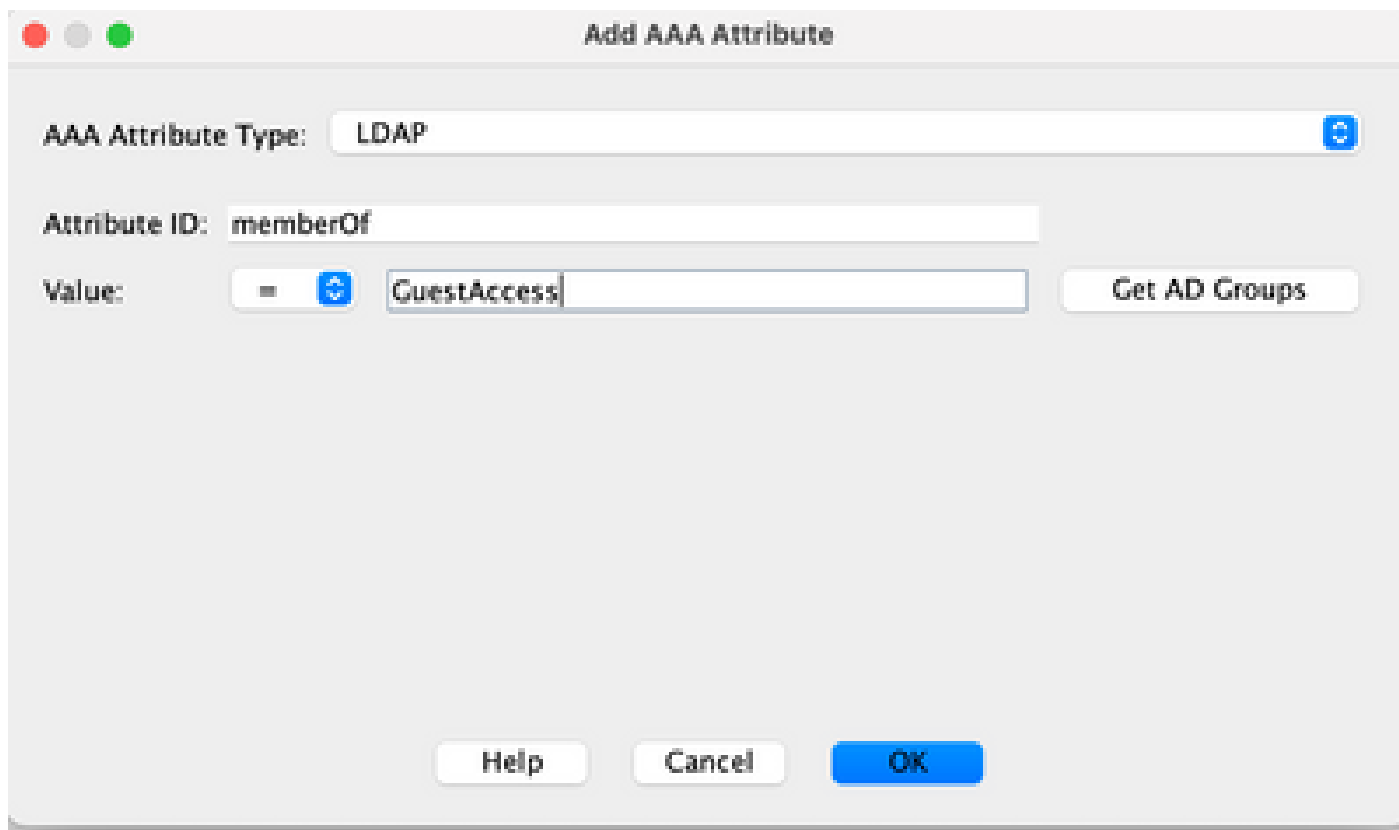
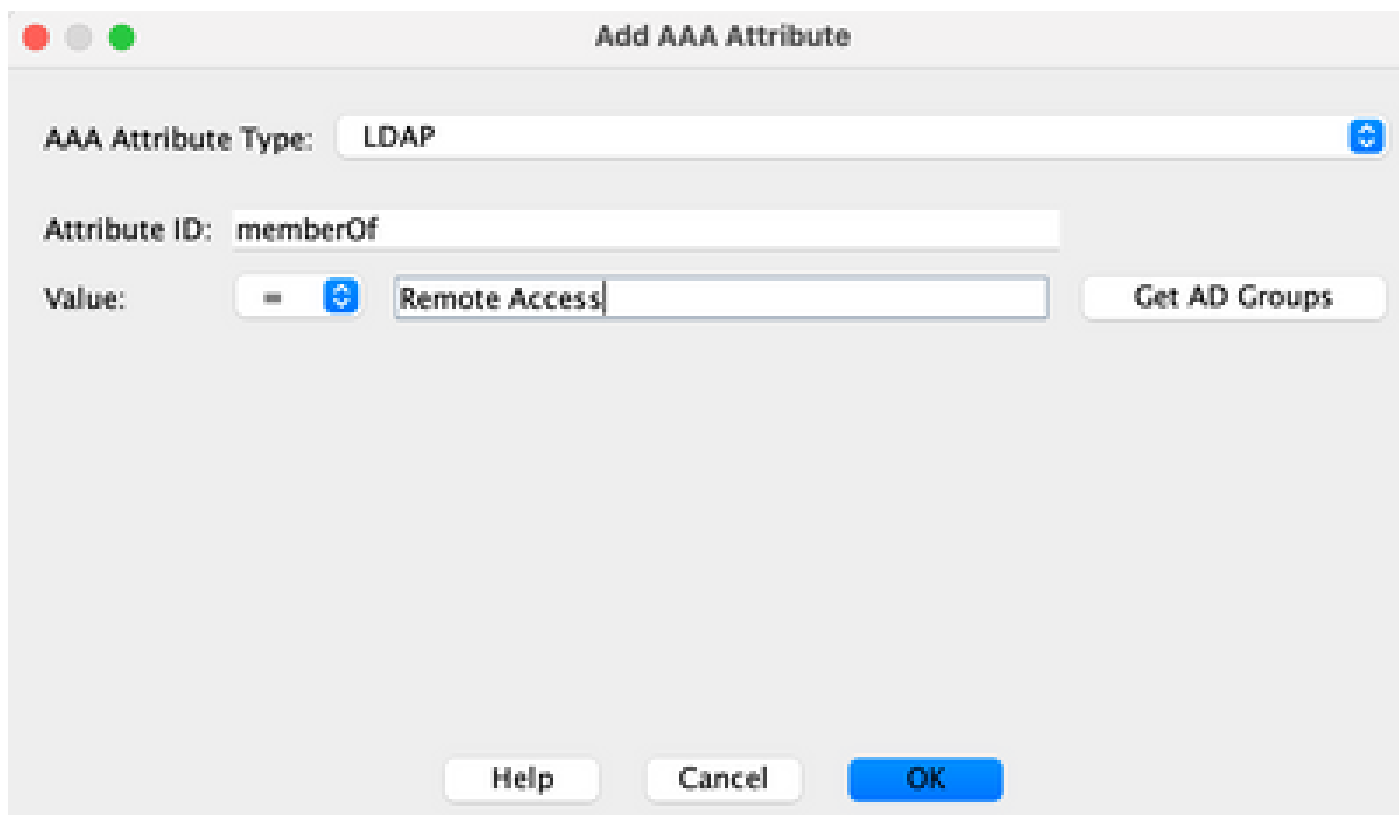


図 42.DAP AAA属性 : AAAグループメンバーシップをDAP基準として使用し、リモートアクセス機能を許可できます



a.

[Action] タブで、[Action] に [Continue] が設定されていることを確認します (図 35)。

b.

[Bookmarks] タブで、ドロップダウンから「Contractors」というリスト名を選択し、[Add] をクリックします。また、**Enable bookmarks**にチェックマークが付いていることも確認します。(図 40 を参照)。

c.

「アクセス方法」タブで、「アクセス方法Webポータル」を選択します。(図 36)。

d.

[OK] をクリックし、次に [Apply] をクリックします。

結論

この例に記載されているクライアントのリモートアクセスSSL VPN要件に基づき、このソリューションはクライアントのリモートアクセスVPN要件を満たします。

この統合によって進化するダイナミックVPN環境により、ダイナミックアクセスポリシーは、頻繁なインターネット設定の変更、組織内の各ユーザが持つさまざまなルール、および設定とセキュリティレベルが異なるマネージド/アンマネージドリモートアクセスサイトからのログインに適応し、拡張することができます。

ダイナミックアクセスポリシーは、Advanced Endpoint Assessment、ホストスキャン、Secure Desktop、AAA、ローカルアクセスポリシーなどの新しい実績あるレガシーテクノロジーによって補完されます。その結果、組織はあらゆるロケーションからあらゆるネットワーク リソースへのセキュア VPN アクセスを確実に実現できます。

関連情報

- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。