ASA 8.x ダイナミック アクセス ポリシー（DAP）導入ガイド

目次

概要

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。 個々の VPN 接続には、複数の変数が影響す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設定、組織内の各ユーザが持つさまざまなロール、および設定とセキュリティ レベルが異なるリモート アクセス サイトからのログインなどが影響する可能性があります。 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、適応型セキュリティ アプライアンス（ASA）のソフトウェア リリース v8.0 コードで導入された新機能です。DAP により、VPN 環境の動的特性に対応できるように認可を設定できます。 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。 ユーザ認証中に 1 つ以上の DAP レコードから属性を選択または集約して、DAP が生成されます。 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 のフラッシュに保管されます。 dap.xml ファイルをオフボックスでエクスポートし、（XML 構文を理解している場合には）このファイルを編集し、再インポートできますが、設定を誤ると ASDM によって DAP レコードの処理が停止されることがあるため、注意してください。 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 access** パラメータを設定しようとすると、

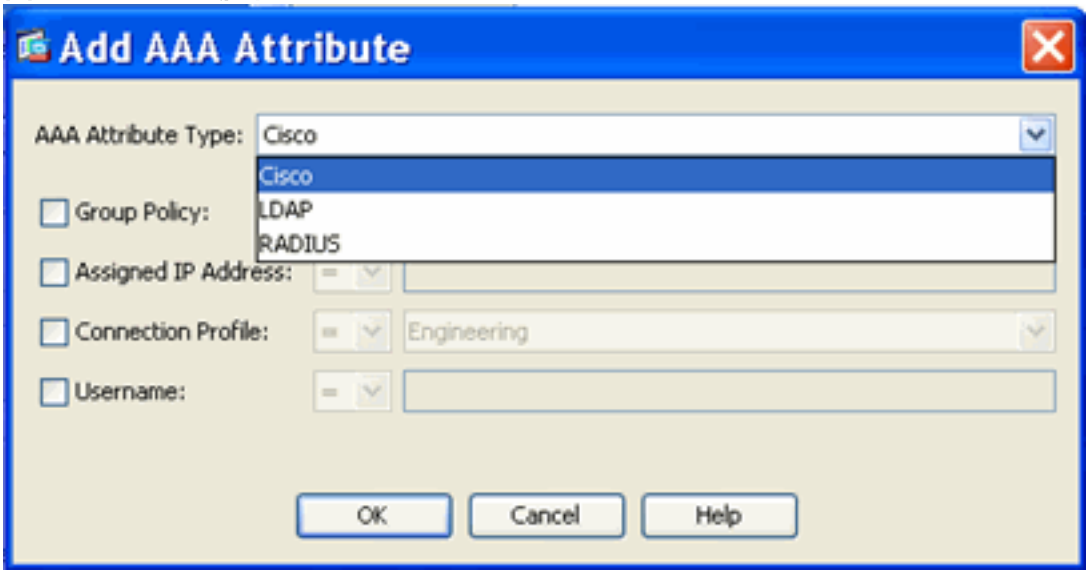
DAP により処理が停止されることがあります。ただし ASDM ではこれは適切に管理されます。DAP ポリシーを管理する際には CLI を使用せず、常に ASDM を使用してください。

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）。

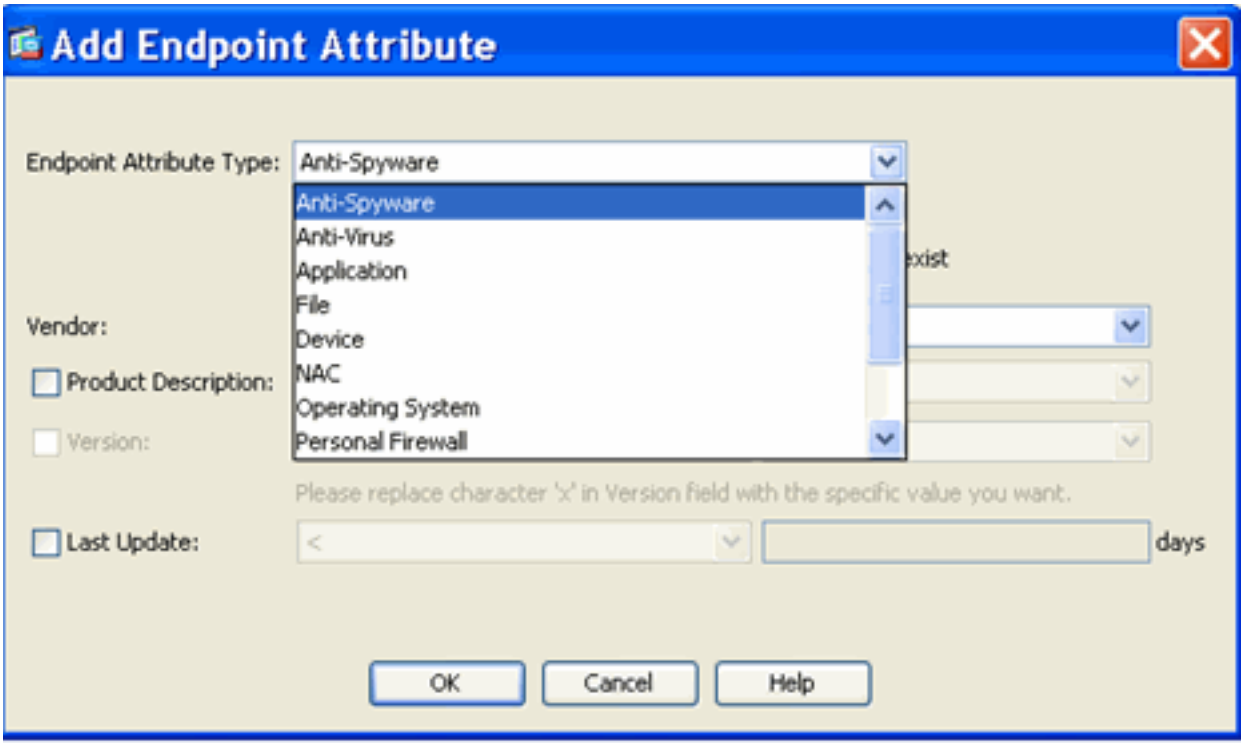
図 1.DAP AAA 属性 GUI



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 属性の他に、設定されているポスチャ評価方式を使用してエンドポイント セキュリティ属性も取得できます。 これには Basic Host Scan、Secure Desktop、Standard/Advanced Endpoint Assessment、NAC などが含まれます（図 2 を参照）。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

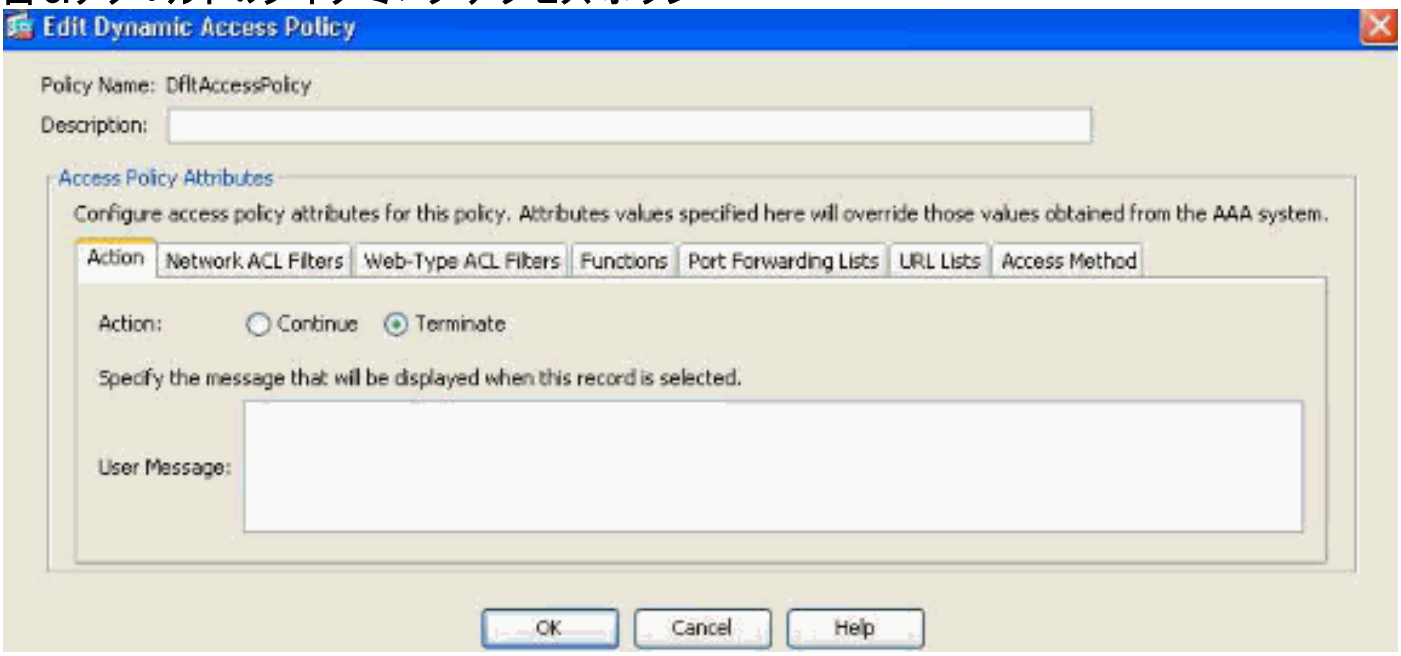


デフォルトのダイナミック アクセス ポリシー

DAP の導入および実装前には、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ていたアクセス ポリシー属性と値のペアが、ASA 上でローカルに定義されるか（トンネル グループおよびグループ ポリシー）、または外部 AAA サーバを介してマップされていました。 v8.0 リリースでは、DAP がローカル アクセス ポリシーと外部アクセス ポリシーの両方を補完または上書きするように設定できます。

デフォルトでは常に DAP が適用されます。 ただし、管理者が従来のポリシー適用方法（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、AAA などによってアクセス コントロールを施行する方法など）を使用する場合でも、この動作を実現できます。 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



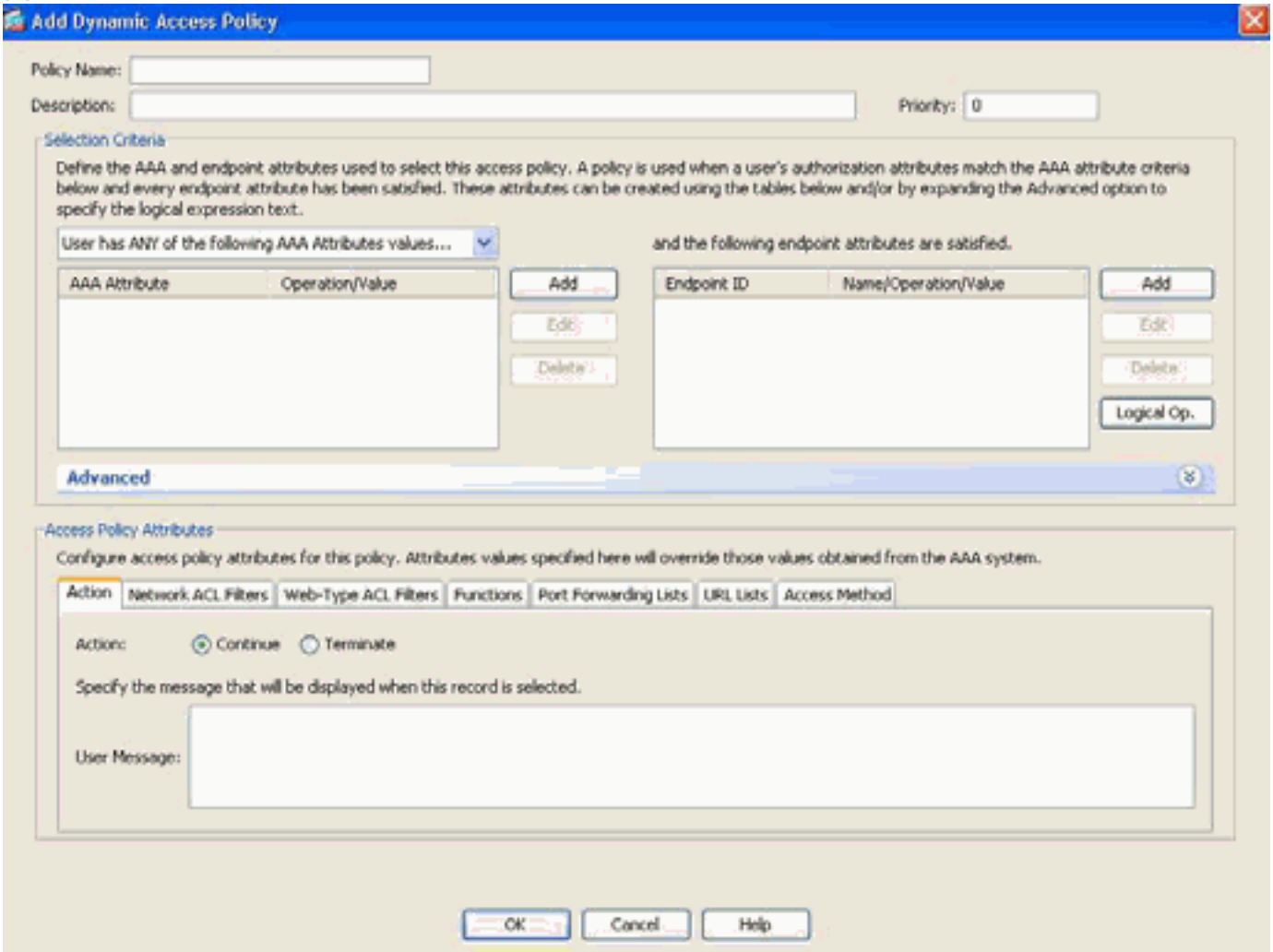
ただし、DAP レコードのデフォルト値が 1 つでも変更された場合、たとえば DfltAccessPolicy の [Action:] パラメータの値がデフォルト値から [Terminate] に変更され、追加 DAP レコードが設定されていない場合、デフォルトでは認証ユーザは DfltAccessPolicy DAP レコードに一致し、この認証ユーザの VPN アクセスが拒否されます。

その結果、VPN 接続を認可するために 1 つ以上の DAP レコードを作成して設定し、認証ユーザに対してアクセスを認可するネットワーク リソースを定義する必要が生じます。 DAP が設定されている場合は、従来のポリシー適用よりも DAP が優先されます。

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に検討すべきパラメータが多数あります。 たとえば接続エンドポイントが管理対象の環境、管理対象外の環境、信頼できない環境のいずれからであるかを確認し、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、Endpoint Assessment と AAA クレデンシャルに基づいて接続ユーザに対しアクセスを認可するネットワーク リソースを決定することなどです。 このためには、まず図 4 に示す DAP 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際には主に次の 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。

たとえば図 5a に示すように [AAA Attribute Type:] で [LDAP]（Active Directory）が選択されており、[Attribute Name] のストリングが [memberOf]、[Value] のストリングが [Contractors] である場合、AAA 属性基準に一致するには、認証対象ユーザは Active Directory グループ「Contractors」のメンバーでなければなりません。

認証対象ユーザは AAA 属性の基準だけでなく、エンドポイント属性の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 Cisco Secure Desktop（CSD）を設定しており、そのポスチャ評価に基づいてエンドポイントが CSD の Unmanaged というロケーションに配置される場合、管理者はエンドポイント属性の選択基準としてこの評価情報を使用できます（図 5b を参照）。

図 5a. AAA 属性基準

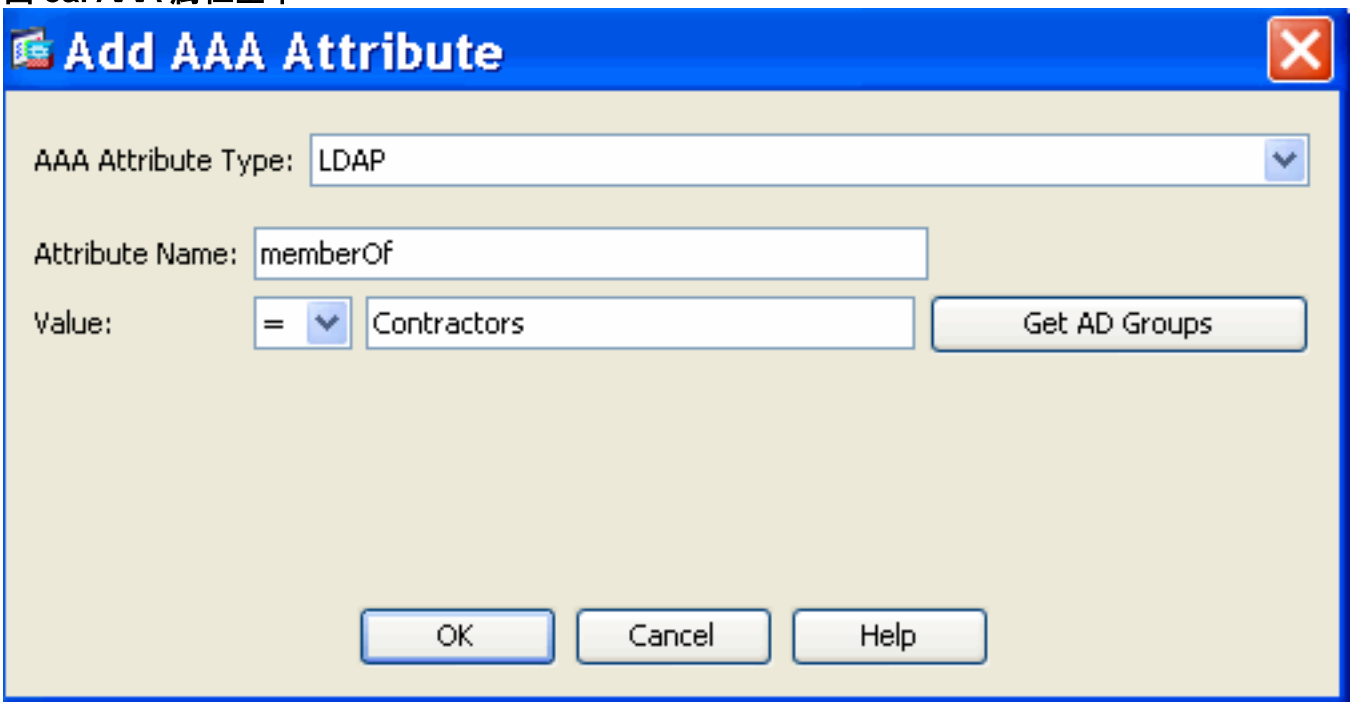
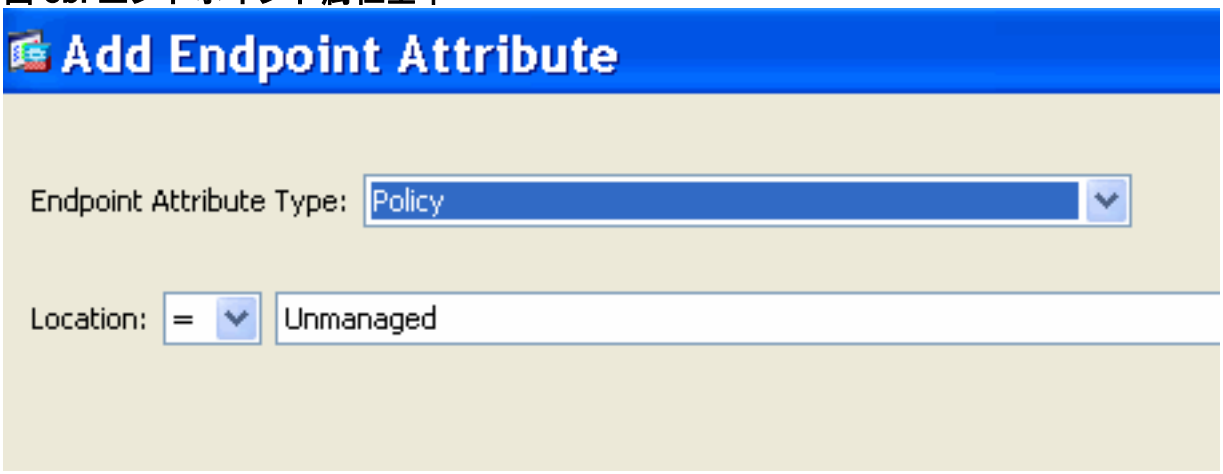
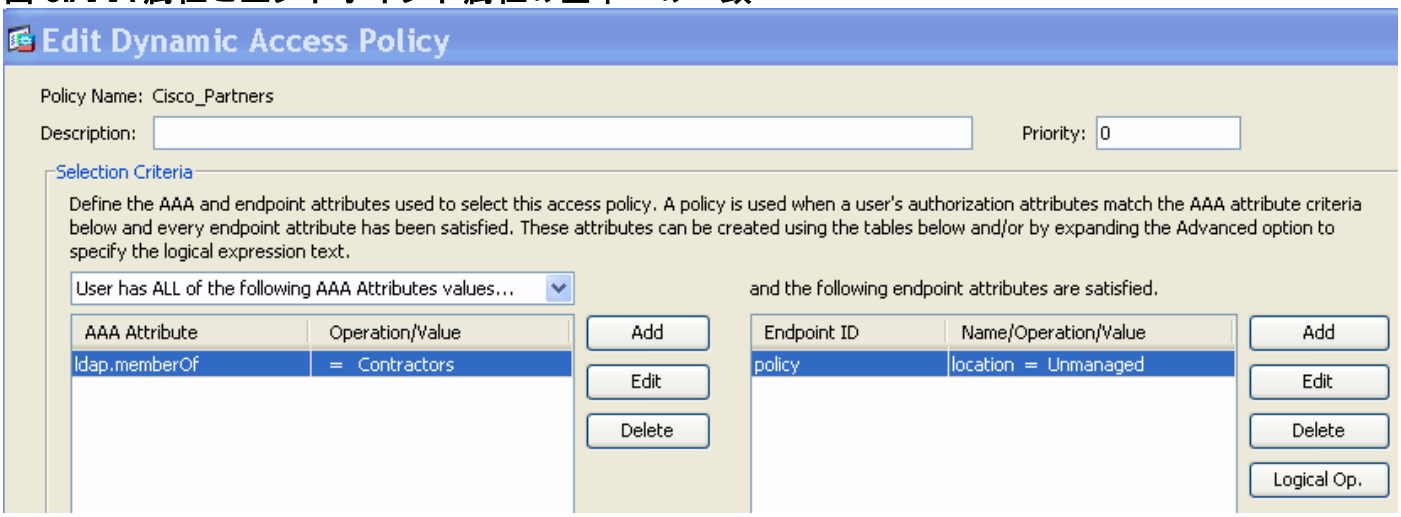


図 5b. エンドポイント属性基準



したがって、図 6 に示すように DAP レコードを基準に一致させ、DAP レコードが割り当てられるようにするには、認証対象ユーザが Active Directory グループ「Contractors」のメンバーであり、その接続エンドポイントが CSD ポリシー値「Unchanged」を満たしている必要があります。

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。 現時点では、論理式には AAA およびエンドポイントの選択論理演算を表現する EVAL 関数が使用されます。 たとえば [EVAL (endpoint.av.McAfeeAV.exists,"EQ","true","string") and EVAL (endpoint.av.McAfeeAV.description,"EQ","McAfee VirusScan Enterprise","string")] となります。

論理式は、上の説明にある AAA およびエンドポイントの属性領域で指定可能な基準以外の選択基準を追加する場合に有効です。 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、あるいはいずれも満たさない 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。エンドポイント属性は累積的で、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

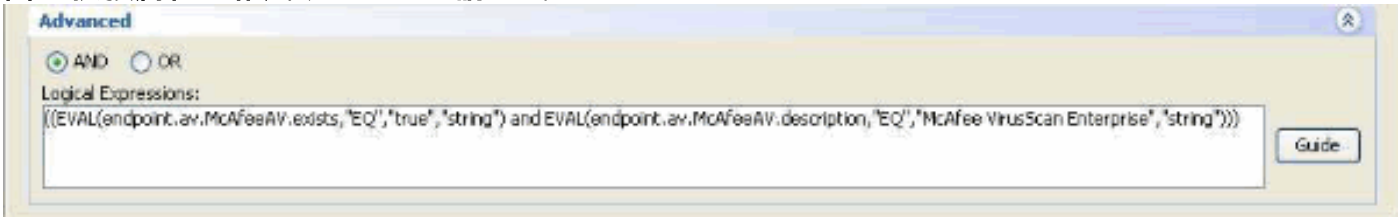
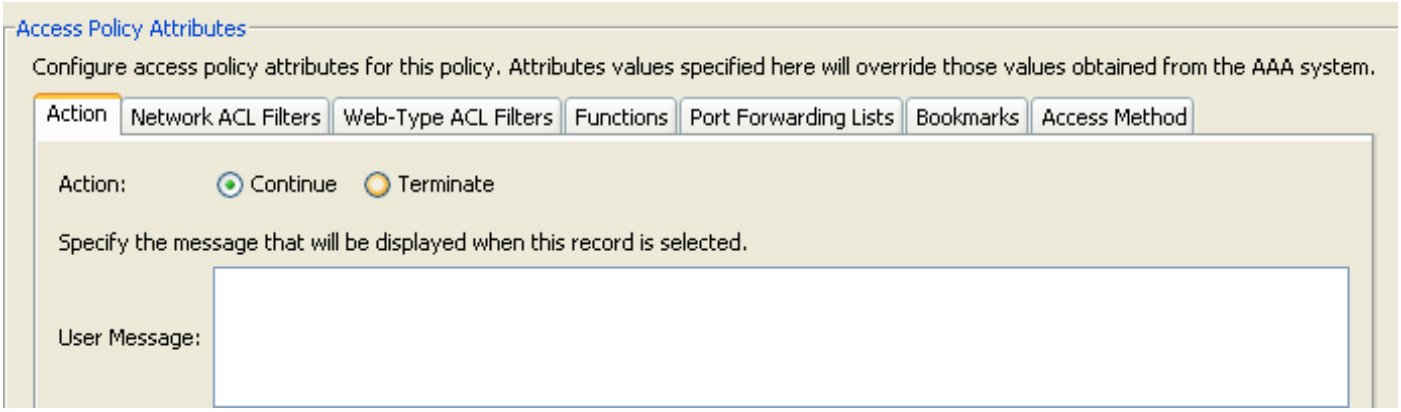


図 8 に示す [Access Policy Attributes] セクションでは、管理者が特定の DAP レコードの VPN アクセス属性を設定します。 ユーザの認可属性が AAA、エンドポイント、または論理式の基準と一致する場合は、 このセクションで設定されているアクセス ポリシー属性値が適用されます。 ここで指定する属性値は、AAA システムから取得される値（既存のユーザ、グループ、トンネル グループ、およびデフォルト グループ レコードの値など）を上書きします。

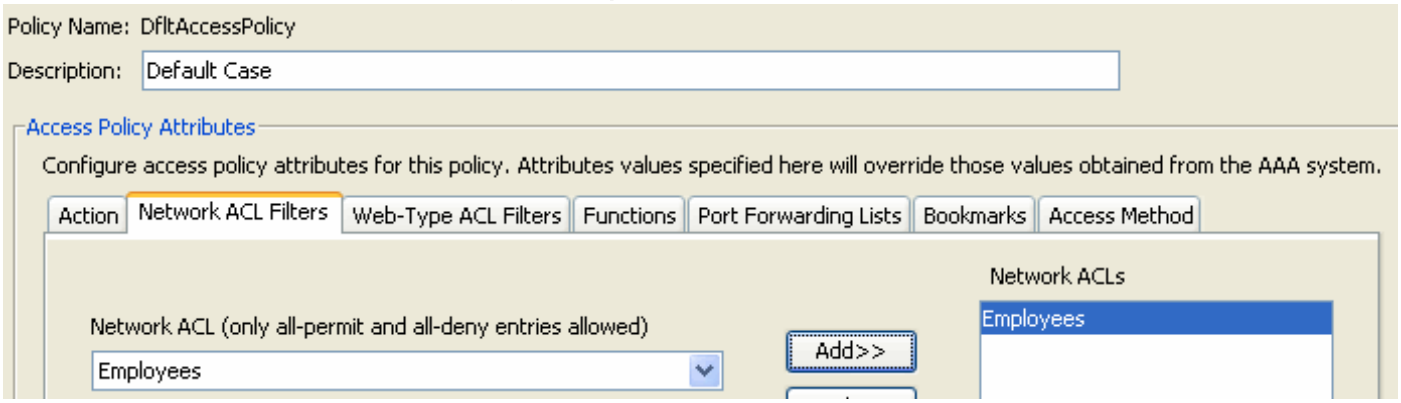
DAP レコードには、設定可能な属性値がいくつかあります。 これらの値は図 8 から図 14 に示す次のタブに表示されます。

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。



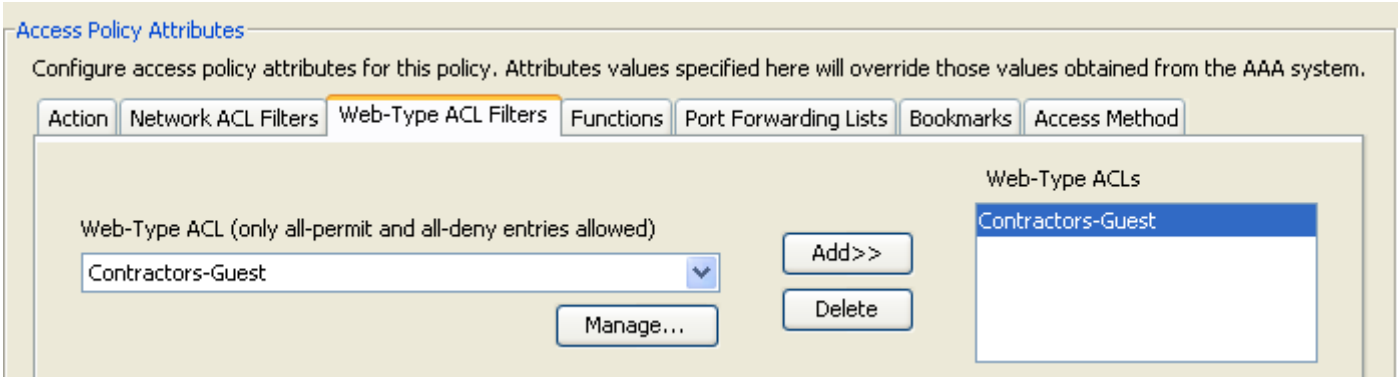
- [Continue]：（デフォルト）クリックするとセッションにアクセス ポリシー属性が適用されます。
- [Terminate]：クリックするとセッションが終了します。
- [User Message]：この DAP レコードが選択されるときに、ポータル ページに表示するテキスト メッセージを入力します。 最大 128 文字を入力できます。 ユーザ メッセージは、黄色のオーブとして表示されます。 ユーザがログインすると、メッセージは 3 回点滅してから静止します。 数件の DAP レコードが選択され、それぞれにユーザ メッセージがある場合は、ユーザ メッセージがすべて表示されます。 このよ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]：この DAP レコードに適用するネットワーク ACL を選択および設定します。 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。



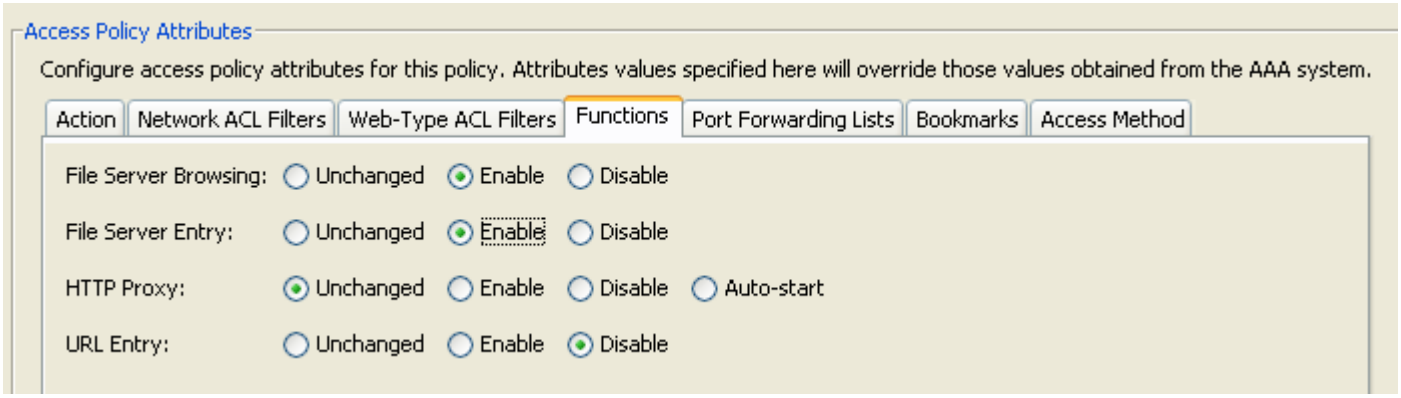
- [Network ACL] ドロップダウン ボックス：この DAP レコードに追加する、すでに設定済みのネットワーク ACL を選択します。 すべての許可ルールまたはすべての拒否ルールを含む ACL だけが適格とされ、これらの適格な ACL だけがここに表示されます。
- [Manage]：ネットワーク ACL を追加、編集、および削除します。
- [Network ACL] リスト：この DAP レコードのネットワーク ACL を表示します。
- [Add]：ドロップダウン ボックスから選択したネットワーク ACL を右側の [Network ACLs] リストに追加します。
- [Delete]：[Network 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 を選択および設定できます。 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。

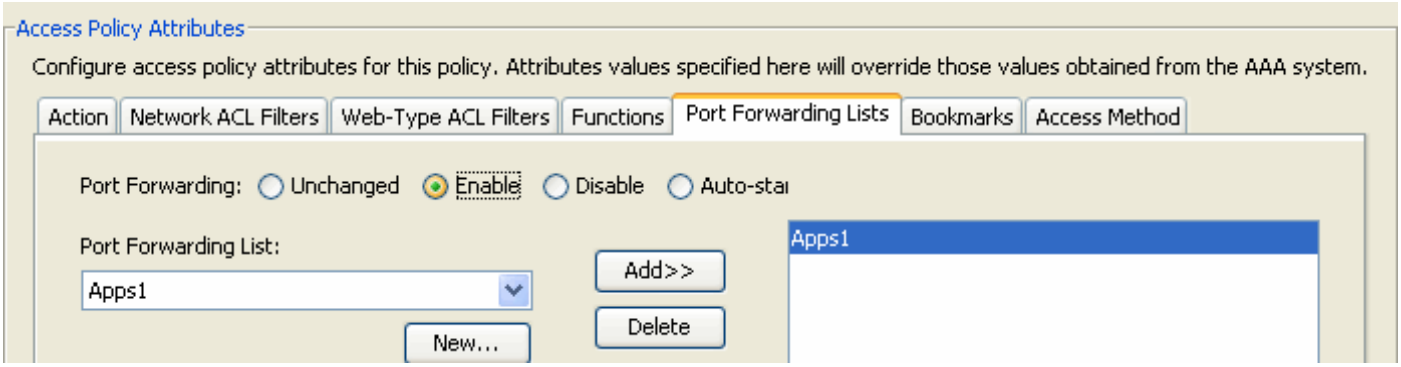
図 11.[Functions] タブ：DAP レコードのファイル サーバ入力とブラウジング、HTTP プロキシ、および URL 入力を設定できます。



- [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 エントリのドローアが配置されます。 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。 ネットワークの要件によっては、ユーザがファイルへのアクセス前に認証を受ける必要があることもあります。
- [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。 このプロキシによって、セキュリティ アプライアンスの使用を継続しながら、マングリングおよび再作成を回避できます。 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

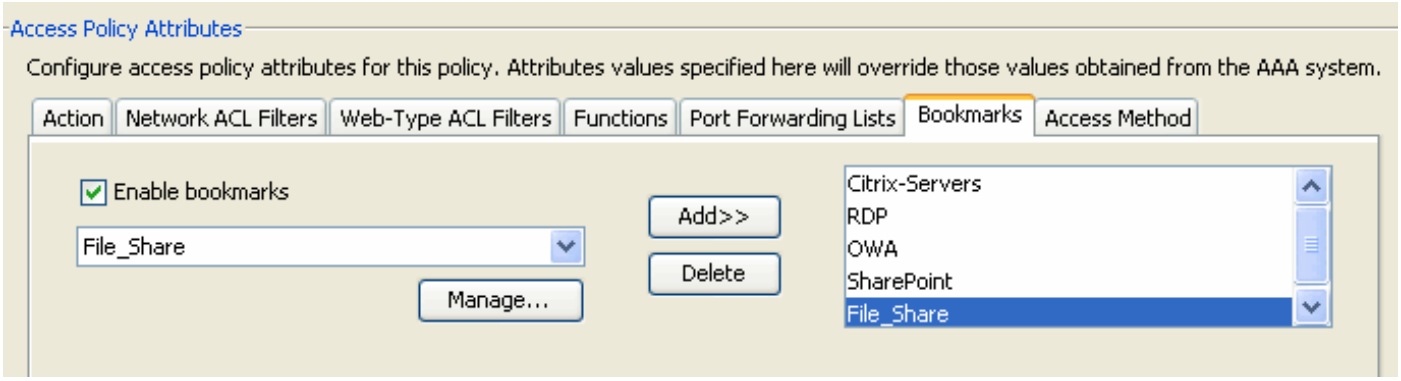
どすべてのクライアント側テクノロジーがサポートされています。 サポートされているブラウザは、Microsoft Internet Explorer だけです。
- [URL Entry]：ポータル ページでユーザが HTTP/HTTPS URL を入力できるようにするか、または入力できないようにします。 この機能がイネーブルになっている場合、ユーザは URL 入力ボックスに Web アドレスを入力できます。また、クライアントレス SSL VPN を使用して、これらの Web サイトにアクセスできます。
- [Unchanged]：（デフォルト）このセッションに適用されるグループ ポリシーの値を使用します。
- [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：ユーザ セッションでのポート転送リストを選択して設定できます。



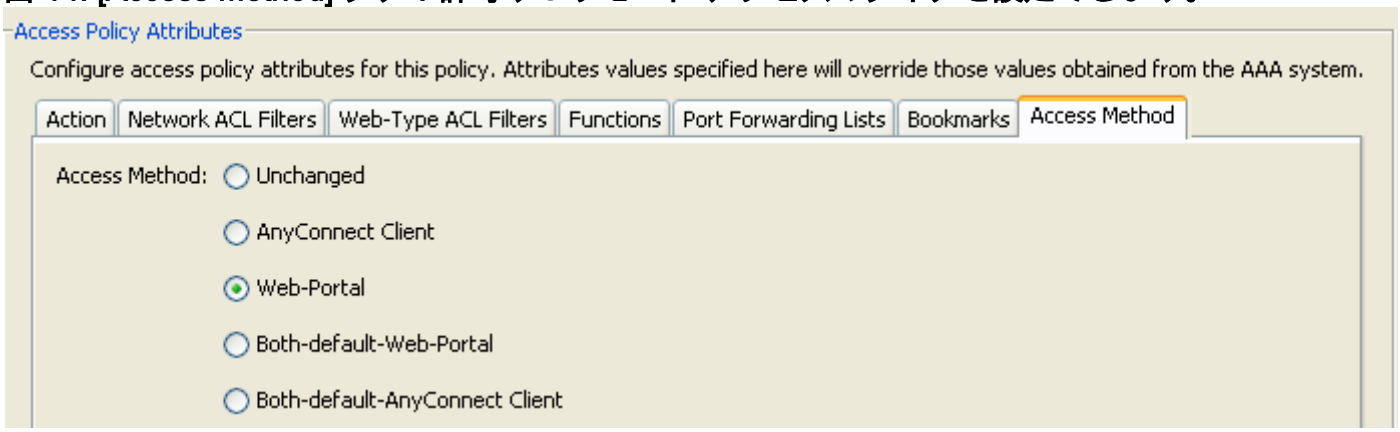
- [Port Forwarding]：この DAP レコードに適用されるポート転送リストのオプションを選択します。 このフィールドのその他の属性は、[Port Forwarding] を [Enable] または [Auto-start] に設定した場合にだけイネーブルになります。
- [Unchanged]：このセッションに適用されるグループ ポリシーの値を使用します。
- [Enable]/[Disable]：ポート転送をイネーブルまたはディセーブルにします。
- [Auto-start]：ポート転送をイネーブルにし、DAP レコードに、そのポート転送リストに関連付けられたポート転送アプ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。
- [Delete]：選択したポート転送リストをポート転送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. [Bookmarks] タブ：ユーザ セッションのブックマーク/URL リストを選択して設定できます。



- [Enable bookmarks]：ブックマークをイネーブルにします。 このボックスが選択されていない場合は、接続のポータル ページにブックマーク 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. [Access 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行リモート アクセス方式を引き続き使用します。
- [AnyConnect Client]：Cisco AnyConnect VPN Client を使用して接続します。
- [Web-Portal]：クライアントレス VPN によって接続します。
- [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。

前述したように、DAP レコードにはいくつかのデフォルト属性値があります。これらの値が変更されている場合にだけ、これらの値は既存の 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。 DAP 範囲外の属性値（Split Tunneling Lists、Banners、Smart Tunnels、Portal Customizations など）を追加する必要がある場合は、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 レコードによりその属性値を適用する必要があります。 この場合、その特定の属性値は DAP を補完するものであり、DAP を上書きしません。 したがって、ユーザはすべてのレコードの属性値が累積されます。

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。 このため、認証対象ユーザが複数の 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。 これにより、これらのポリシー全体でアクセス ポリシー属性が一貫しているか、または矛盾する結果となります。 この場合、認可ユーザに対し、一致するすべての DAP レコードの属性が累積されます。

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。 アクセス ポリシー属性の組み合わせの例を以下の表に示します。 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。 選択されている DAP レコードのいずれかで値 Terminate が設定されている場合、集約属性値は Terminate です。選択されているすべての DAP レコードで値 Continue が設定されている場合、集約属性値は Continue です。

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)	Terminate	continue	continue	terminate

表 2 に、ストリング値を含むユーザ メッセージ属性を示します。 集約属性値は、選択されている DAP レコードの属性値を連結し、改行 (16 進数値 0x0A) で個々の値を区切ったストリングになります。 連結ストリング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

クライアントレス機能をイネーブルにする属性 (関数) を表 3 に示します。これらの属性の値は Auto-start、Enable、Disable です。 選択されている DAP レコードのいずれかで Auto-start 値が設定されている場合、集約属性値は Auto-start になります。

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、1 つ以上の DAP レコードで Enable 値が設定されている場合、集約属性値は Enable になります。

選択されているどの DAP レコードでも「Auto-start」値と「Enable」値が設定されておらず、1 つ以上の DAP レコードで「Disable」値が設定されている場合、集約属性値は「Disable」になります。

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	disable		enable
file-browsing	disable	enable	disable	enable
file-entry			disable	disable

http-proxy	disable	auto-start	disable	auto-start
url-entry	disable		enable	enable

表 4 の url-list 属性と port-forward 属性の値は、ストリングまたはカンマで区切ったストリングです。 集約属性値は、選択されている DAP レコードの属性値を連結し、カンマで個々の値を区切ったストリングになります。 連結ストリング内で重複する属性値はすべて削除されます。 連結ストリングでの属性値の順序は特に重要ではありません。

表 4URL 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

アクセス方式属性は、SSL VPN 接続で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 アクセス方式は、AnyConnect Client アクセスのみ、Web-Portal アクセスのみ、AnyConnect Client アクセスまたは Web-Portal アクセス (デフォルトは Web-Portal アクセス)、AnyConnect Client アクセスまたは Web-Portal アクセス (デフォルトは AnyConnect Client アクセス) のいずれかです。 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

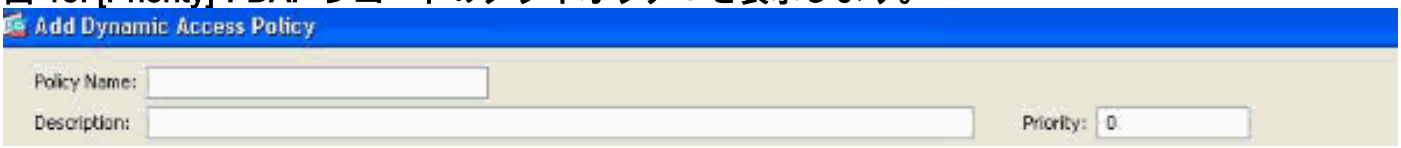
選択される属性値				集約結果
AnyConnect Client	Web-Portal	Both-default-Web-Portal	Both-default-AnyConnect Client	
			X	Both-default-AnyConnect Client
		X		Both-default-Web-Portal
		X	X	Both-default-Web-Portal
	X			Web-Portal
	X		X	Both-default-AnyConnect Client
	X	X		Both-default-Web-Portal
	X	X	X	Both-default-Web-Portal
X				AnyConnect Client
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

ネットワーク（ファイアウォール）ACL フィルタ属性および Web-type（クライアントレス）ACL フィルタ属性の集約時に考慮すべき主な 2 つのコンポーネントは、DAP プライオリティと DAP ACL です。

図 15 に示す Priority 属性は集約されません。 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 を集約するときに、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、最上位のプライオリティ番号から最下位のプライオリティ番号の順にレコードを並べ、最下位のプライオリティをテーブルの一番下に配置します。 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。

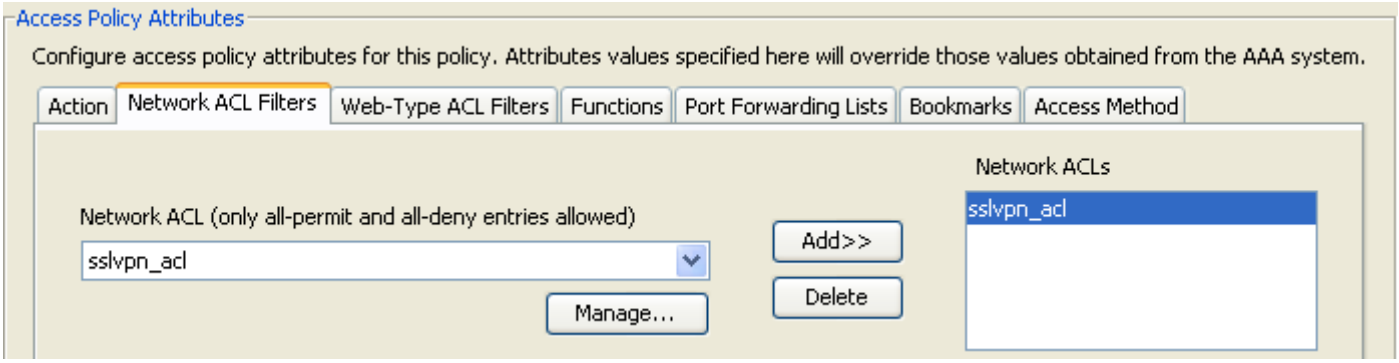
図 15. [Priority]：DAP レコードのプライオリティを表示します。



- [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 属性では、厳密な「ホワイト リスト」または「ブラック リスト」ACL モデルのいずれかに準拠するアクセス リストだけがサポートされます。 「ホワイト リスト」ACL モデルでは、アクセス リスト エントリで、指定されているネットワークまたはホストへのアクセスを「許可」するルールを指定します。 「ブラック リスト」ACL モデルでは、アクセス リスト エントリで、指定されている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るアクセス リストは非準拠アクセス リストです。 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と設定エラーとして拒否されます。 DAP レコードに対して準拠アクセス リストが割り当てられており、このアクセス リストの ACL モデルへの準拠性を変える変更が行われる場合、その変更は設定エラーとして拒否されます。

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ている場合、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 リスト属性が集計され、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。 次の例に、ダイナミック DAP ファイアウォール アクセス リストの作成方法を示します。 ダイナミック DAP クライアントレス アクセス リストも同じ方法で作成されます。

最初に ASA により DAP Network-ACL の固有名が動的に作成されます（表 6 を参照）。

表 6ダイナミック DAP Network-ACL 名

DAP Network-ACL 名
DAP-Network-ACL-X（X は固有名を作成するための増分整数値）

2 番目に、ASA により選択されている DAP レコードから Network-ACL 属性が取得されます（表 7 を参照）。

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 により DAP レコードのプライオリティ番号に基づいて Network-ACL の順序が並べ替えられ、次に、選択されている 2 つ以上の DAP レコードの Priority 値が同一の場合は、最初にブラックリストに基づいてネットワーク ACL の順序が並べ替えられます。 その後、ASA は各 Network-ACL から Network-ACL エントリを取得します（表 8 を参照）。

表 8DAP 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 Network-ACL エントリを 1 つのダイナミック生成 Network-ACL にマージし、このダイナミック 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-Network-ACL-1	DDDD DDD PPPP PPP DDDD PPPP

DAP 実装

管理者は、さまざまな理由で DAP の実装を検討します。 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。 次に示す例では、接続エンドポイントを識別し、各種ネットワーク リソースへのアクセスをユーザに認可するように DAP とそのコンポーネントを設定します。

テスト ケース：次の VPN アクセス要件で概念実証を顧客から依頼されました。

- 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できること。 —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。
- 従業員の管理対象エンドポイントで実行アプリケーション（McAfee AntiVirus など）を検出および適用できること。 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、認可ユーザがアクセスできるネットワーク リソースを決定できること。 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」ベースの接続で接続している場合、ネットワーク リソース（ネットワーク ファクスやプリンタなど）へのローカル LAN アクセスを許可できること。

- 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クライアントレス アクセスを付与する必要があります。また、従業員に比べ、契約作業員のアプリケーションへのポータル アクセスを制限する必要があります。

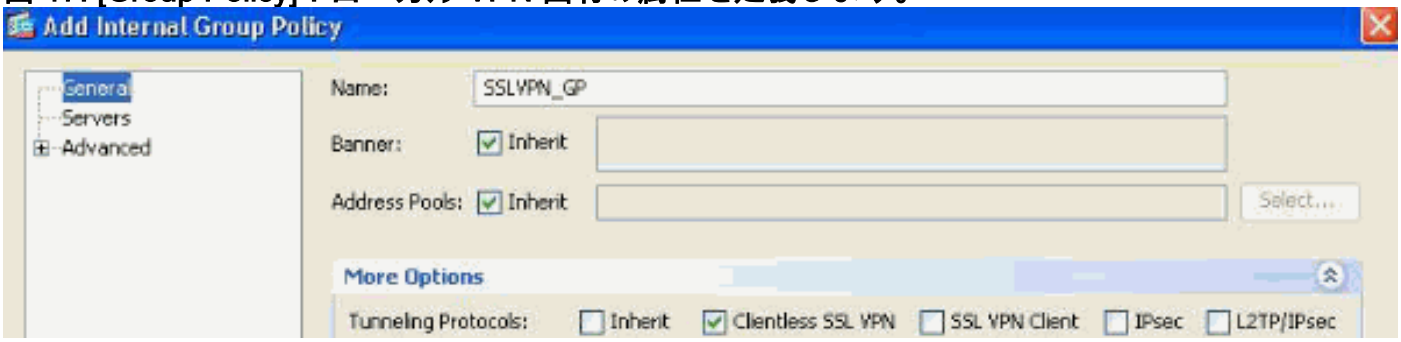
この例では、顧客の VPN アクセス要件に対応するため一連の設定ステップを実行します。 必要であるが DAP には直接関連しない設定ステップと、DAP に直接関連する設定ステップがあります。 ASA は非常に動的であり、多くのネットワーク環境に適応できます。 このため、VPN ソリューションをさまざまな方法で定義できます。場合によっては、最終的なソリューションが同一になることがあります。 ただし、実際にとられる方法は顧客のニーズと環境に基づいて決まります。

このドキュメントの本質と、定義される顧客の要件に基づき、Adaptive Security Device Manager（ASDM）6.0(x) を使用し、DAP を中心とした設定に重点を置いて説明します。 ただし、DAP によるローカル ポリシーの補完および上書きについて説明するため、ローカル グループ ポリシー属性の設定も行います。 このテスト ケースの基盤として、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、基本 IP 接続（IP プール、DefaultDNS サーバ グループなど）を事前に定義できます。

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、クライアントレスおよびクライアント ベースの属性を定義する際にも使用されます）

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] に移動し、次の手順に従って内部グループ ポリシーを追加します。

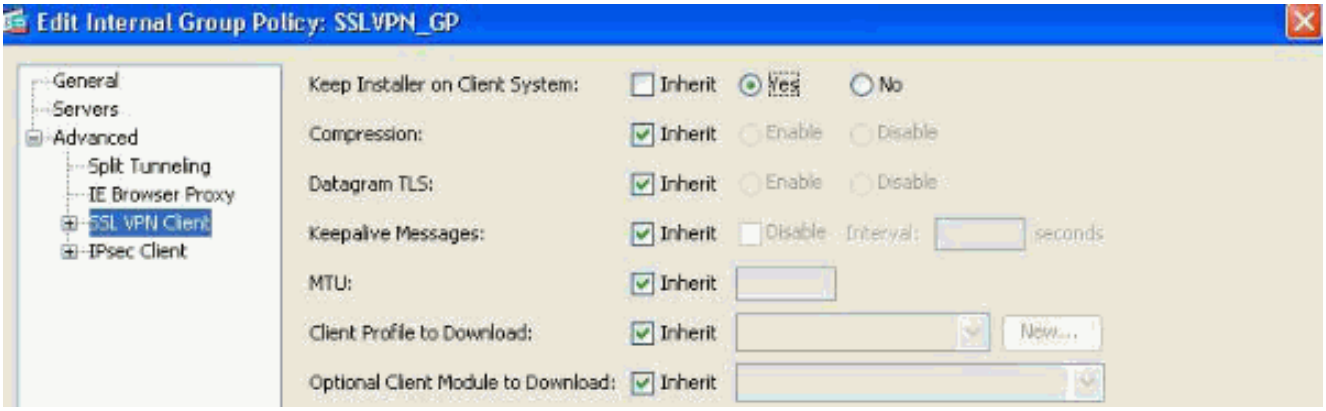
図 17. [Group Policy]：ローカル VPN 固有の属性を定義します。



1. [General] リンクの下で、グループ ポリシーに **SSLVPN_GP** という名前を設定します。
2. [General] リンクの下で [More Options] をクリックし、[Tunneling Protocol:] で [Clientless SSLVPN] だけを設定します（アクセス方式を上書きおよび管理するように DAP を設定します）。
3. [Advanced] > [Split Tunneling] リンクの下で、以下の項目を設定します。**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。**

[Policy]： [Inherit] のチェックマークを外し、[Exclude Network List Below] を選択します。
[Network List]： [Inherit] のチェックマークを外し、リスト名 [Local_Lan_Access] を選択します（事前に設定されていることを前提としています）。

4. [Advanced] > [SSL VPN Client] リンクの下で、以下の項目を設定します。**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。**

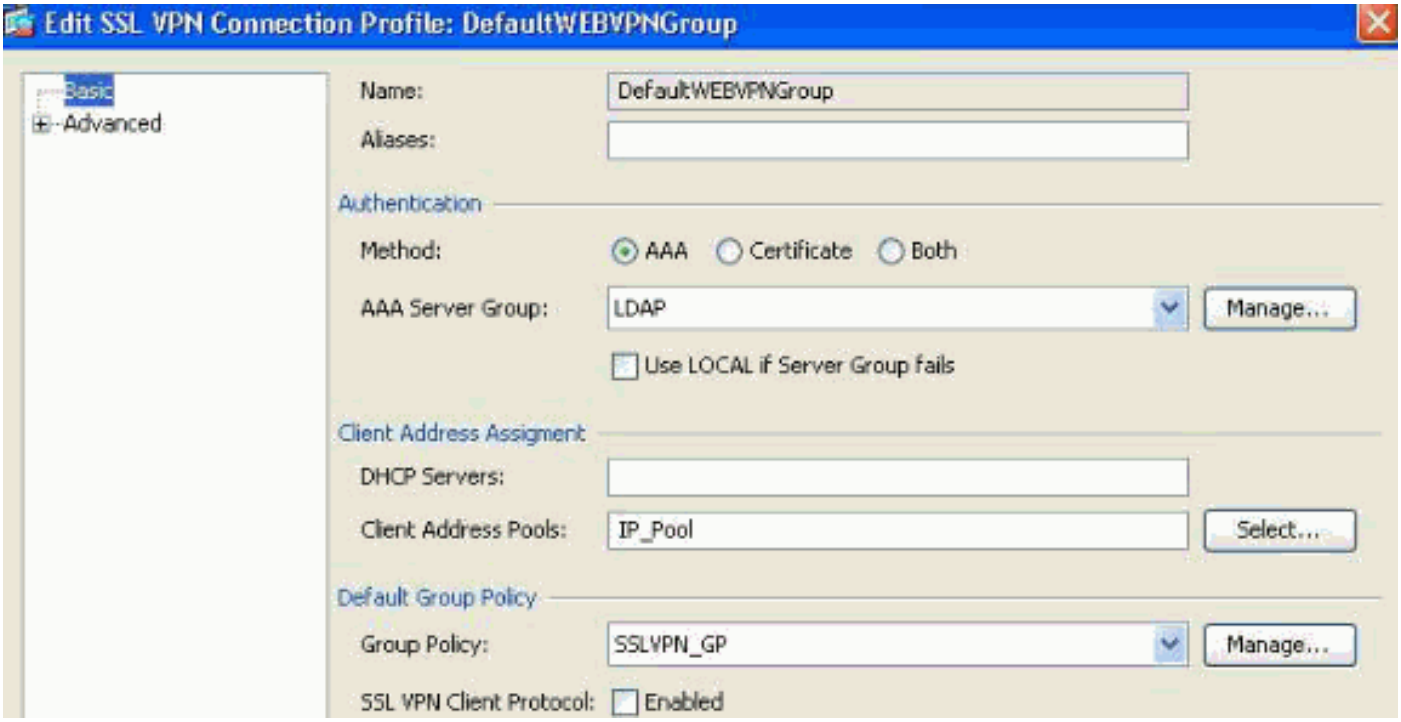


5. [Keep Installer on Client System]： [Inherit] のチェックマークを外し、[Yes] を選択します。
6. [OK] をクリックし、次に [Apply] をクリックします。
7. 設定変更を適用します。

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、以前に設定されていたグループ 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 ポリシーで定義される属性の対象になります（（このプロファイルは、クライアントレスおよびクライアント ベースの属性を定義する際にも使用されます）。

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [SSL VPN Connection Profiles] に移動し、次の項目を設定します。

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。

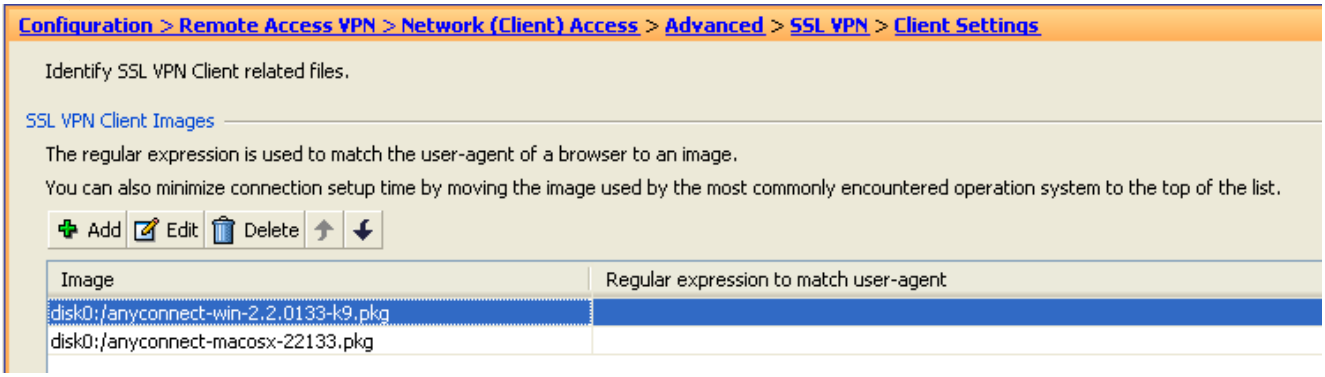


1. [Connection Profiles] セクションで DefaultWEBVPNGroup を編集し、[Basic] リンクの下で次の項目を設定します。[Authentication]：[Method]： [AAA][Authentication]：[AAA Server Group]： [LDAP]（LDAP が事前に設定されていることを前提とします）[Client Address Assignment]：[Client Address Pools]： [IP_Pool]（IP_Pool が事前に定義されていることを前提とします）[Default Group Policy]：[Group Policy]： [SSLVPN_GP] を選択します。
2. 設定変更を適用します。

SSL VPN 接続の IP インターフェイスの定義：この設定は、指定され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 アクセスをイネーブルにする前に、SSL VPN クライアント イメージを最初に定義する必要があります。

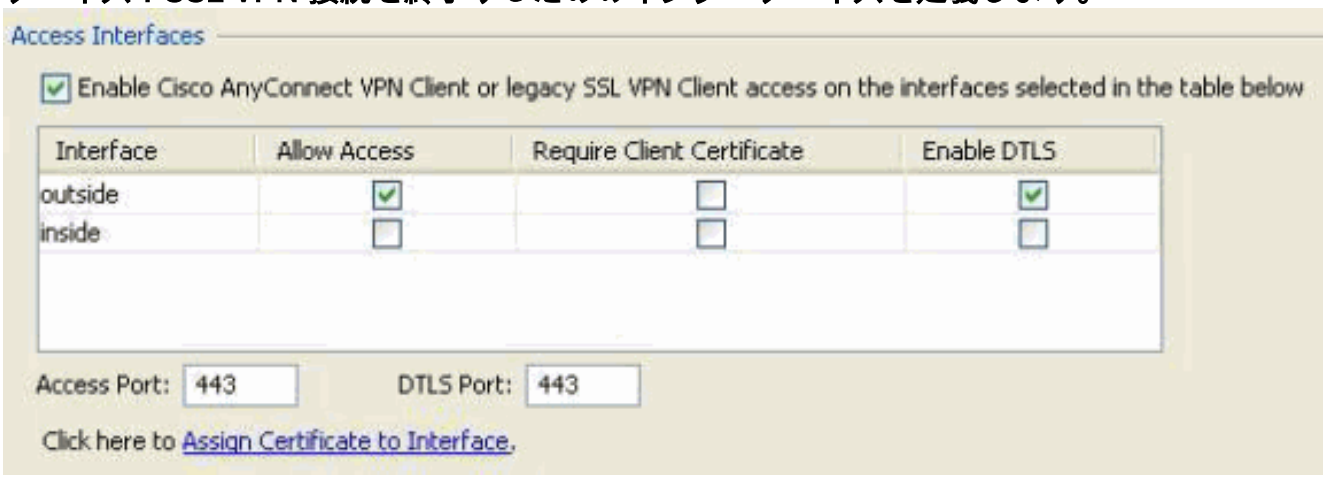
1. [Configuration] > [Remote Access VPN] > [Network (Client)Access] > [Advanced] > [SSL VPN] > [Client Settings] に移動し、ASA フラッシュ ファイル システムの次の SSL VPN クライアント イメージを追加します（このイメージは CCO、www.cisco.com からダウンロードできます）**図 21. SSL VPN クライアント イメージのインストール**
：SSLVPN（AnyConnect）クライアント イメージを接続エンドポイントにプッシュするように定義します。



anyconnect-win-2.x.xxx-k9.pkg[OK]、もう一度 [OK]、そして [Apply] の順にクリックします。

2. [Configuration] > [Remote Access VPN] > [Network (Client)Access] > [SSL VPN Connection Profiles] に移動し、以下の項目をイネーブルにします。**図 22. SSL VPN アクセス インター**

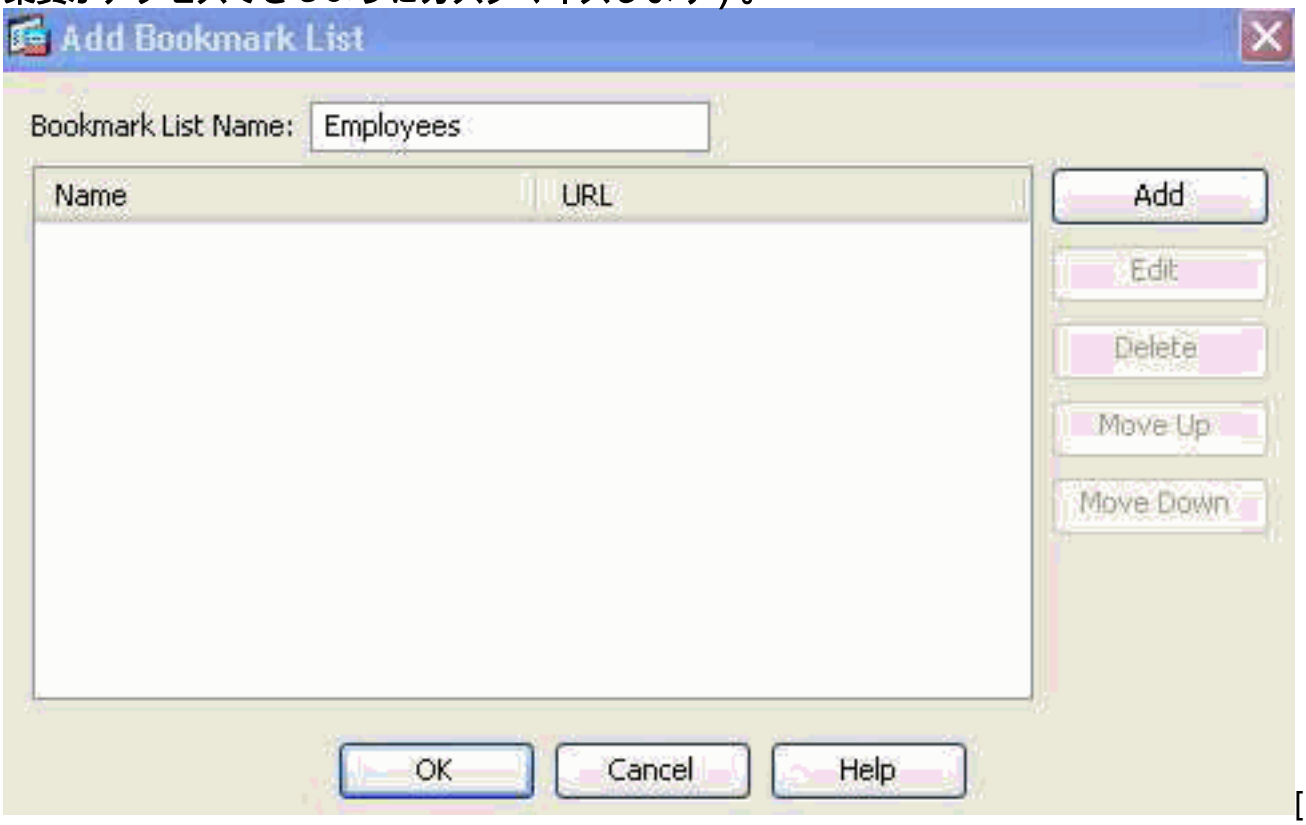
フェイス：SSL VPN 接続を終了するためのインターフェイスを定義します。



[Access Interface] セクションで、 **“[Enable Cisco AnyConnect VPN Client or legacy SSL VPN client access on the interfaces selected in the table below] を有効にします。**また、[Access Interfaces] セクションの下で、外部インターフェイスの [Allow Access] を選択します（この設定により、外部インターフェイスでの SSL VPN クライアントレス アクセスがイネーブルにされます）。[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 アプリケーションを定義するために必要です。 従業員（Employee）用と契約作業員（Contractor）用の 2 つの URL リストを定義します。

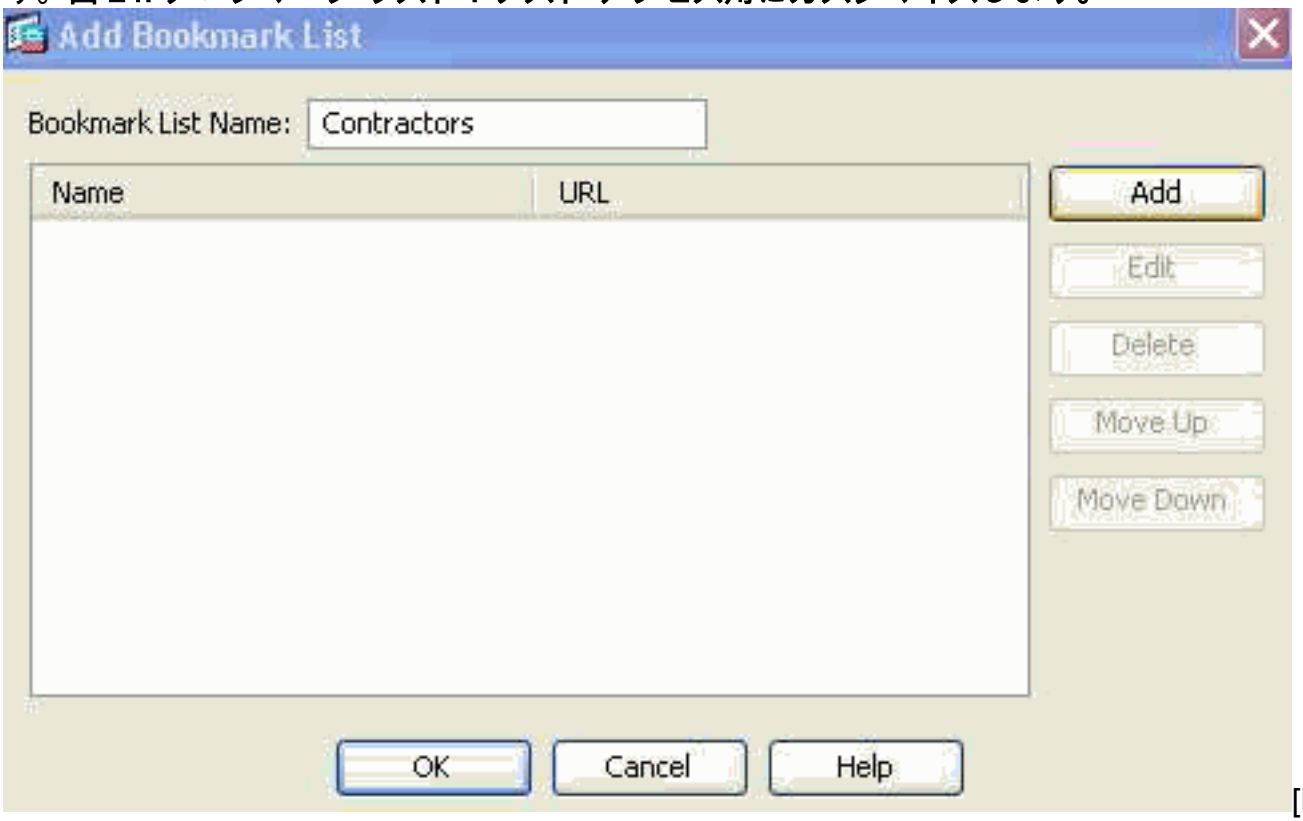
1. [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Bookmarks] に移動し、[+ Add] をクリックして以下の項目を設定します。**図 23. ブックマーク リスト：Web ポータルで公開し、アクセスできるようにする URL を定義します（（従業員がアクセスできるようにカスタマイズします）。**



[Bookmark List Name]： 「Employees」と入力し、[Add] をクリックします。[Bookmark Title]： **Company Intranet**[URL Value]： **http://company.resource.com**[OK] をクリックし、さらに [OK] をクリックします。

2. [+ Add] をクリックし、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。**

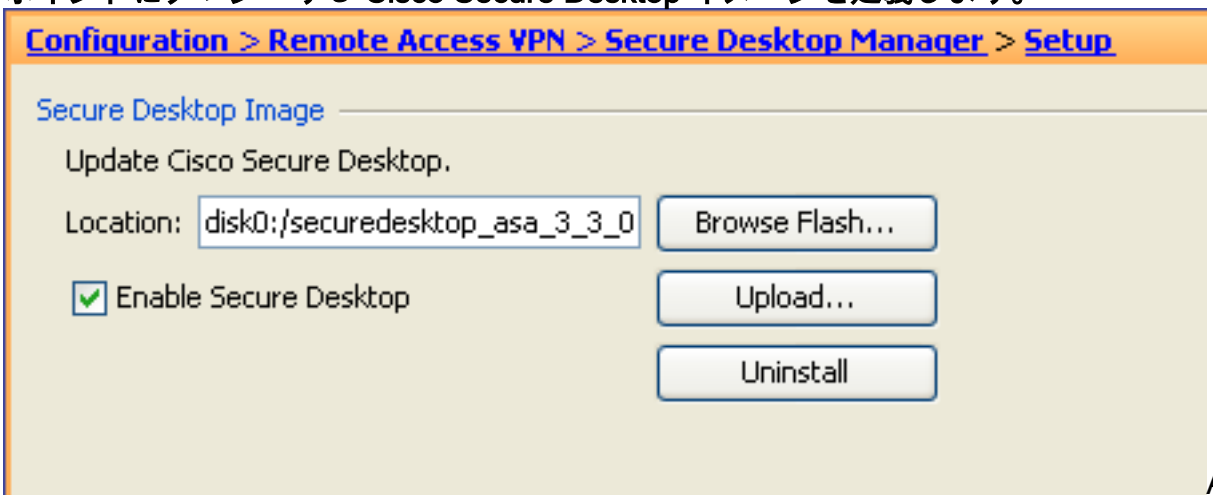


[Bookmark List Name]：「Contractors」と入力し、[Add] をクリックします。[Bookmark Title]：**ゲスト アクセス**[URL Value]：**http://company.contractors.com**[OK] をクリックし、さらに [OK] をクリックします。[Apply] をクリックします。

Cisco Secure Desktop：この設定は、Endpoint Assessment 属性を定義するために必要です。 満たす必要がある基準に基づいて、接続エンドポイントは管理対象と管理対象外に分類されます。 認証プロセスの前に Cisco Secure Desktop 評価が実施されます。

Windows ロケーションの Cisco Secure Desktop とログイン前決定ツリーの設定：

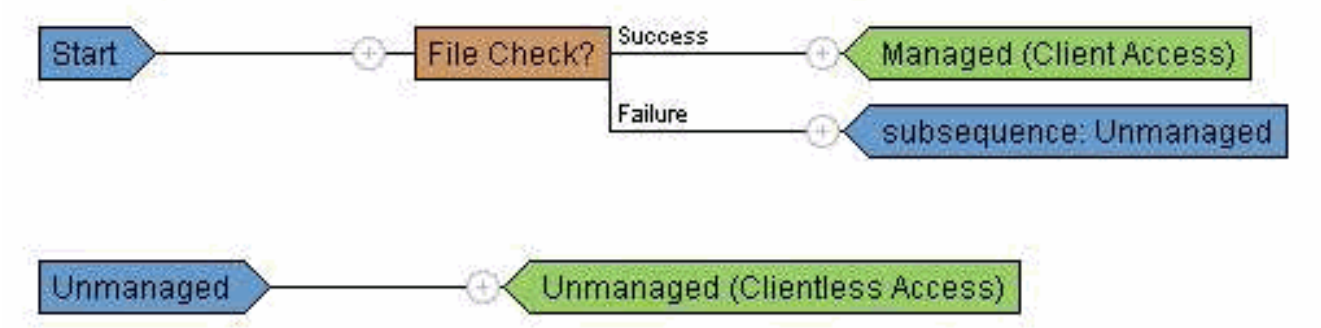
1. [Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Setup] に移動し、以下の項目を設定します。**図 25. Cisco Secure Desktop イメージのインストール：接続エンドポイントにプッシュする Cisco Secure Desktop イメージを定義します。**



ASA フラッシュ ファイル システムから **disk0:/securedesktop-asa-3.3.-xxx-k9.pkg** イメージをインストールします。[Enable Secure Desktop] にチェックマークを付けます。[Apply] をクリックします。

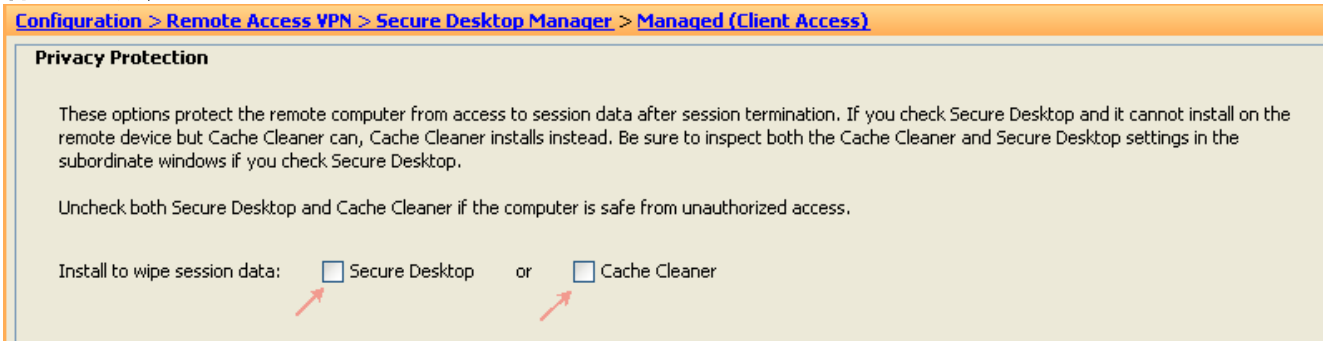
2. [Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Prelogin Policy] に移動し、以下の項目を設定します。**図 26. ログオン前決定ツリー：[File Check] を使用し、管**

理対象エンドポイントと管理対象外エンドポイントを区別するようにカスタマイズします。



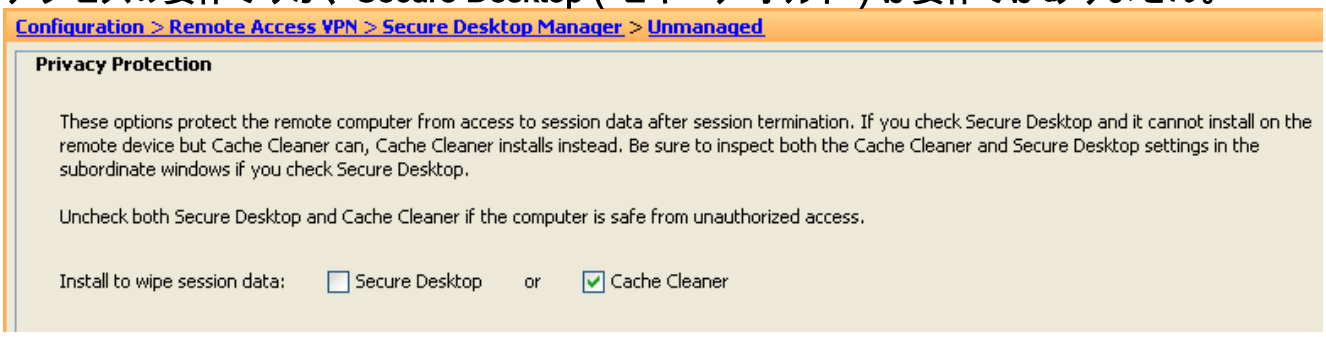
[Default] ノードをクリックし、ラベルの名前を [Managed (Client Access)] に変更し、[Update] をクリックします。[Managed] ノードの先頭にある「+」記号をクリックします。チェックとして、挿入する [File Check] を選択して追加します。「exists」の [File Path] に「**C:\managed.txt**」と入力し、[Update] をクリックします。[Login Denied] ノードをクリックし、[Subsequence] を選択します。ラベルとして「**Unmanaged**」を入力し、[Update] をクリックします。[Login Denied] ノードをクリックし、[Location] を選択します。ラベルとして「**Unmanaged (Clientless Access)**」を入力し、[Update] をクリックします。[Apply All] をクリックします。

3. [Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Managed (Client Access)] に移動し、[Location Settings] セクションで以下の項目を設定します。**図 27. ロケーション/プライバシー保護設定：[Secure Desktop] (セキュア ボルト) と [Cache Cleaner] (ブラウザ クリーンアップ) は、クライアント/ネットワーク ベース アクセスの要件ではありません。**



ロケーション モジュール： [Secure Desktop] と [Cache Cleaner] がイネーブルになっている場合は、両方ともチェックマークを外してください。必要に応じて [Apply All] をクリックします。

4. [Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Unmanaged (Clientless Access)] に移動し、[Location Settings] セクションで以下の項目を設定します。**図 28. ロケーション設定：Cache Cleaner (ブラウザ クリーナ) はクライアントレス ベース アクセスの要件ですが、Secure Desktop (セキュア ボルト) は要件ではありません。**

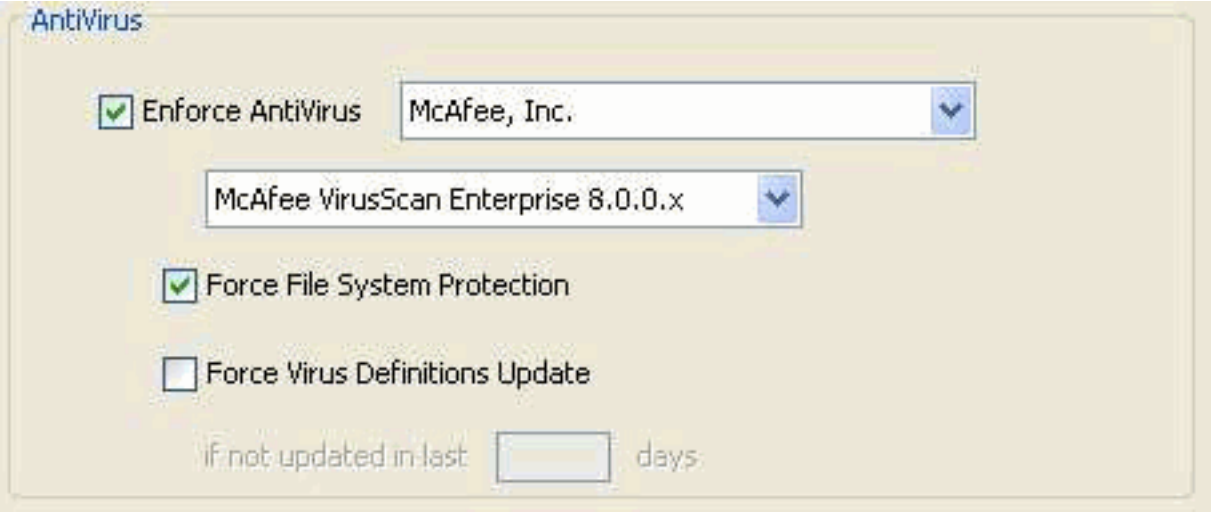


ロケーション モジュール： [Secure Desktop] のチェックマークを外し、[Cache Cleaner] にチェックマークを付けます。[Apply All] をクリックします。

Advanced Endpoint Assessment：この設定は、エンドポイントにアンチウイルス、アンチスパイウェア、パーソナル ファイアウォールを適用するために必要です。 たとえば、この評価では接続エンドポイントで McAfee が実行されているかどうかが検証されます（（Advanced Endpoint Assessment はライセンス済み機能であり、Cisco Secure Desktop 機能がディセーブルになっている場合は設定できません）。

[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Host Scan] に移動し、[Host Scan Extensions] セクションで以下の項目を設定します。

図 29. アンチウイルスの適用：クライアント/ネットワーク ベース アクセスに合わせてカスタマイズします。



[Host Scan Extensions] セクションで以下の項目を設定します。

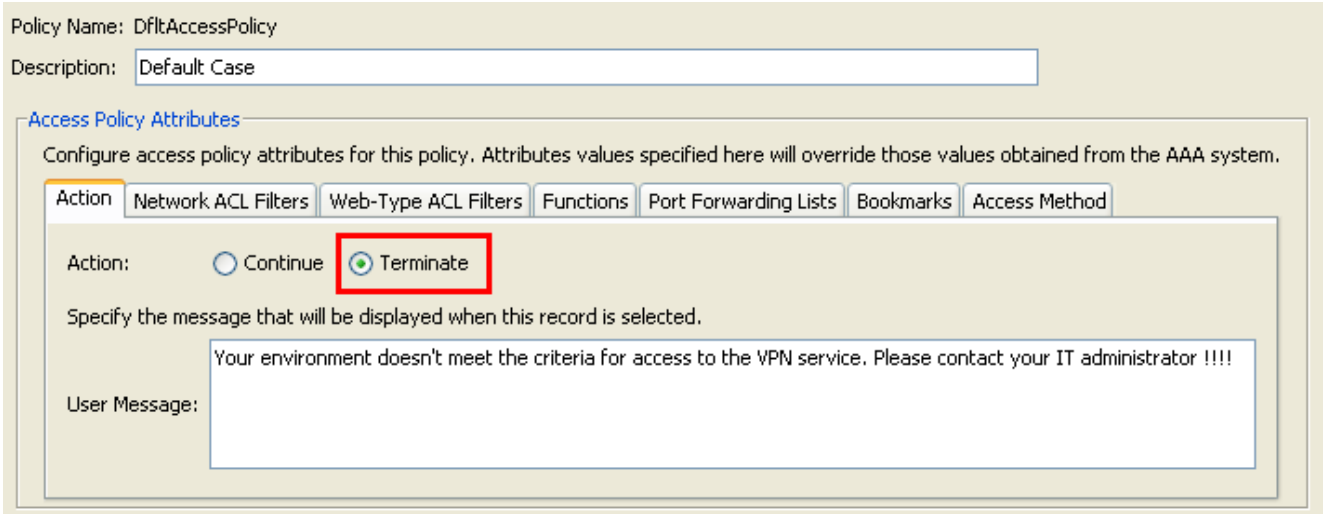
1. [Advanced Endpoint Assessment ver 2.3.3.1] を選択し、次に [Configure] を選択します。
2. [Enforce AntiVirus] を選択します。
3. [Enforce AntiVirus] ドロップダウン リストから [McAfee, Inc] を選択します。
4. [AntiVirus Version] ドロップダウン リストから [McAfee VirusScan Enterprise 8.0.0.x] を選択します。
5. [Force File System Protection] を選択して、[Apply All] をクリックします。

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、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が付与されます。 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、つまり設定されているダイナミック アクセス ポリシーのいずれにもエンドポイントが一致しない場合に終了するようにするため、以下の項目を設定します。

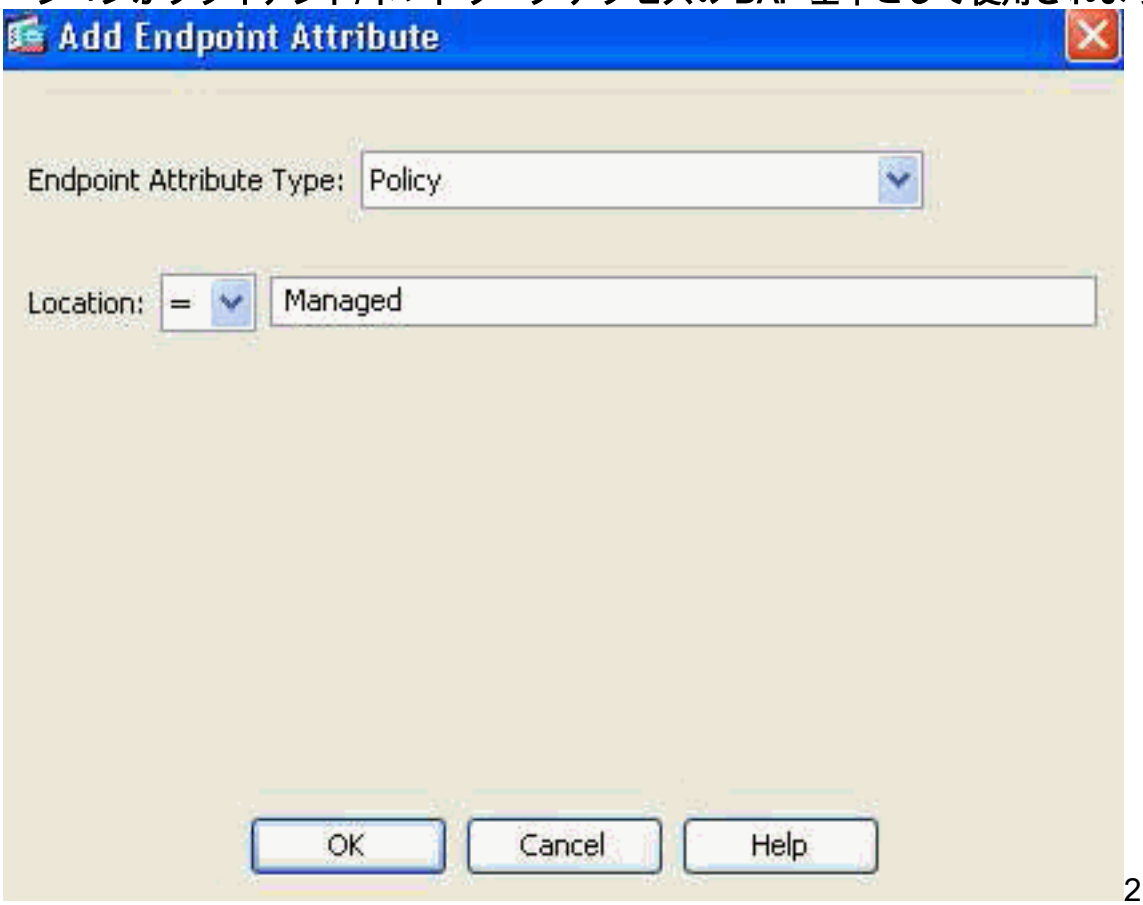
注: ダイナミック アクセス ポリシーを初めて設定するときに、DAP コンフィギュレーション ファイル（DAP.XML）が存在しないという DAP.xml エラー メッセージが表示されます。 初期 DAP 設定が変更および保存されると、このメッセージは表示されなくなります。

1. [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Dynamic Access Policies] に移動し、以下の項目を設定します。**図 30. デフォルトのダイナミック アクセス ポリシー：事前に定義されている DAP レコードが一致しない場合、この DAP レコードが適用されます。 このため、SSL VPN アクセスは拒否されます。**

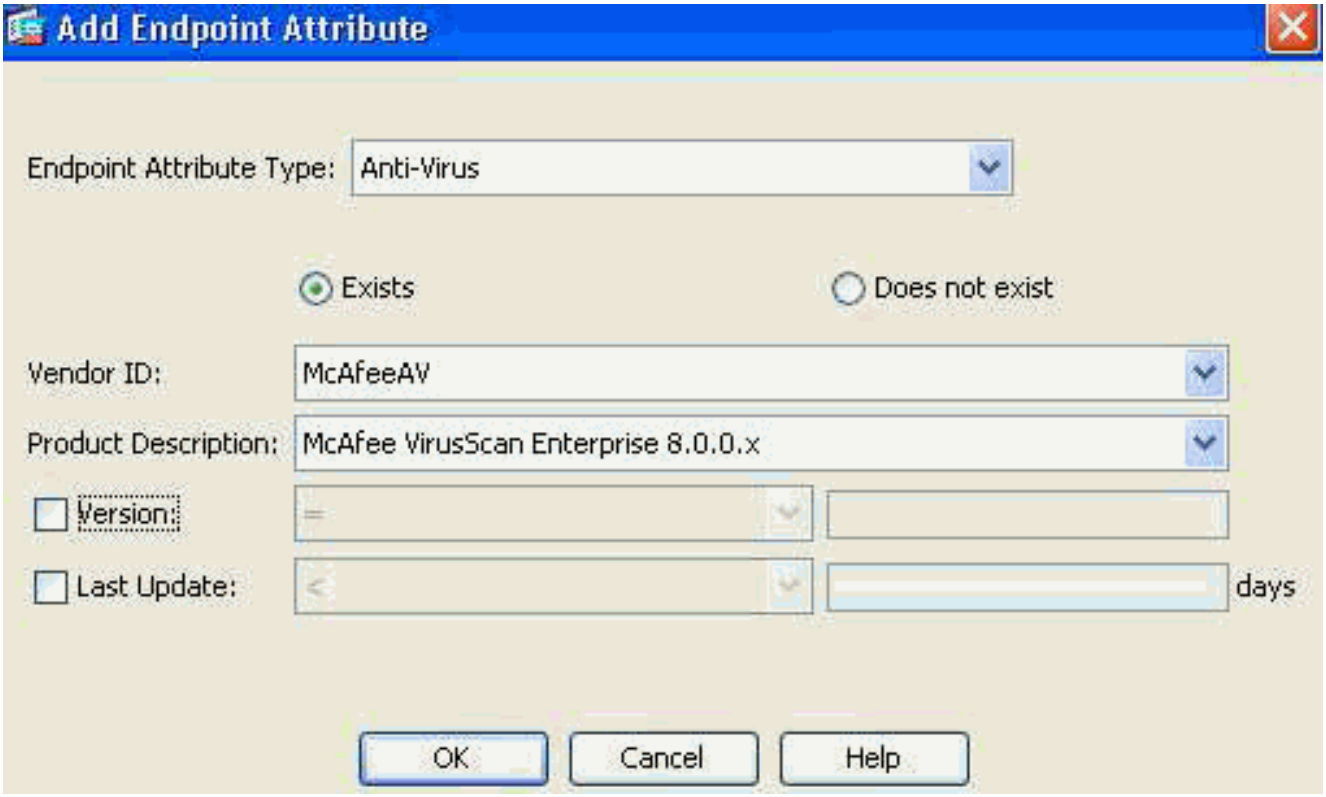


「**DfltAccessPolicy**」を編集し、[Action] に [Terminate] を設定します。[OK] をクリックします。

2. 「**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。[Description]： **Employee Client Access**図 31 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 31. DAP エンドポイント属性：Cisco Secure Desktop ロケーションがクライアント/ネットワーク アクセスの DAP 基準として使用されます。**



2 番目のエンドポイント属性タイプ（Anti-Virus）を、図 32 に示すように追加します。 完了したら、[OK] をクリックします。**図 32. DAP エンドポイント属性：Advanced Endpoint Assessment AntiVirus がクライアント/ネットワーク アクセスの DAP 基準として使用されます。**



[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 33 と 34 に示すように、AAA 属性タイプ（LDAP）を追加します（[AAA Attribute Type] 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 メンバーシップが、従業員を識別する DAP 基準として使用されます。**

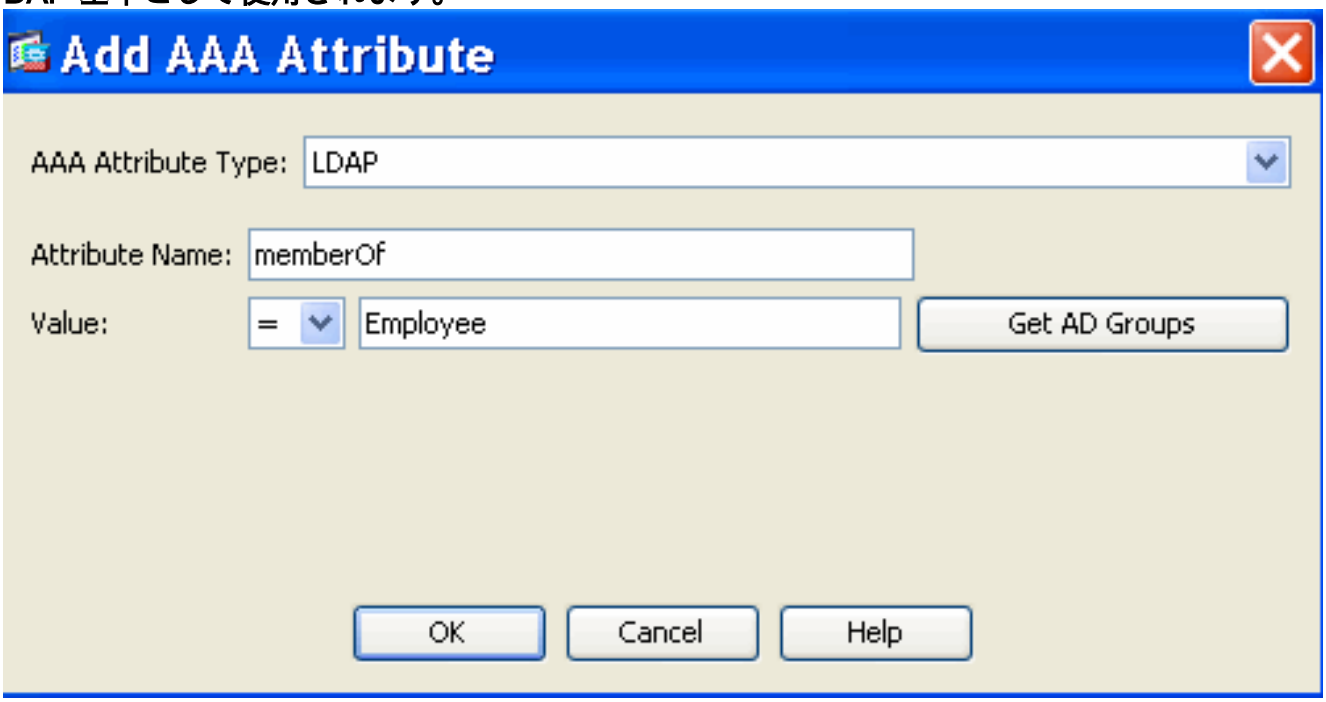
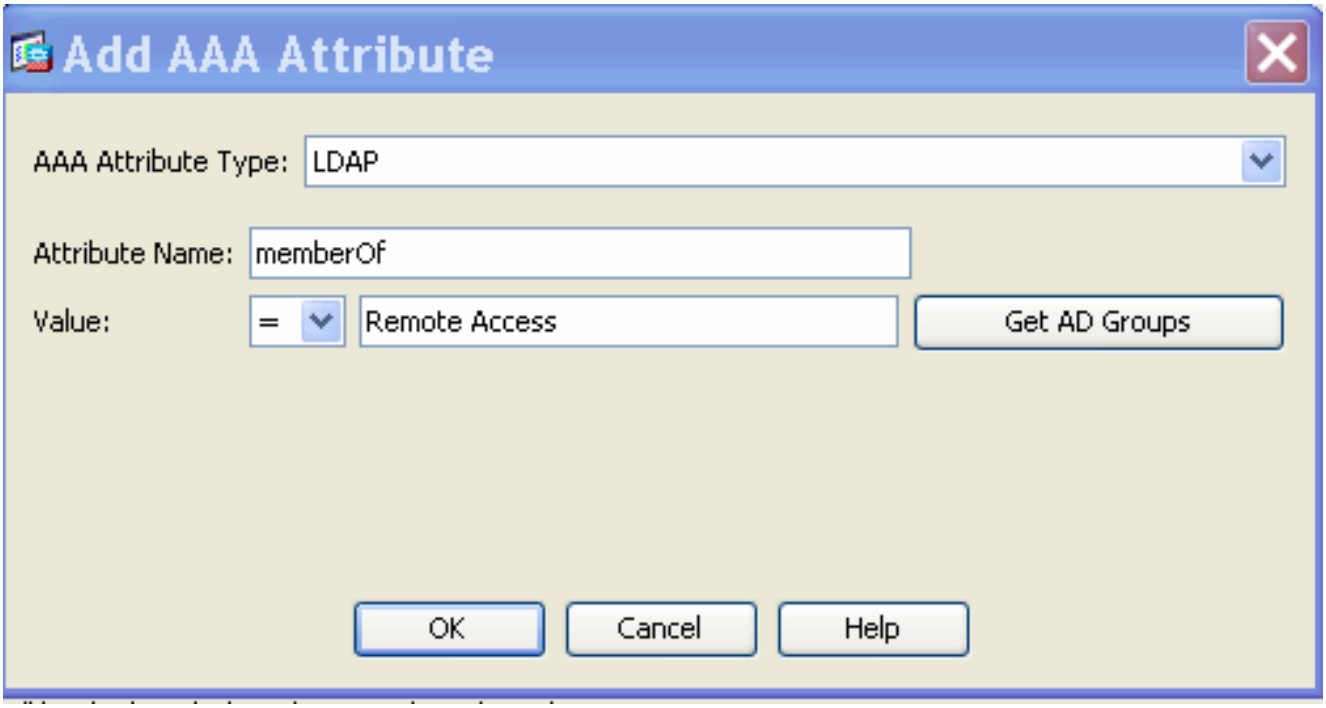
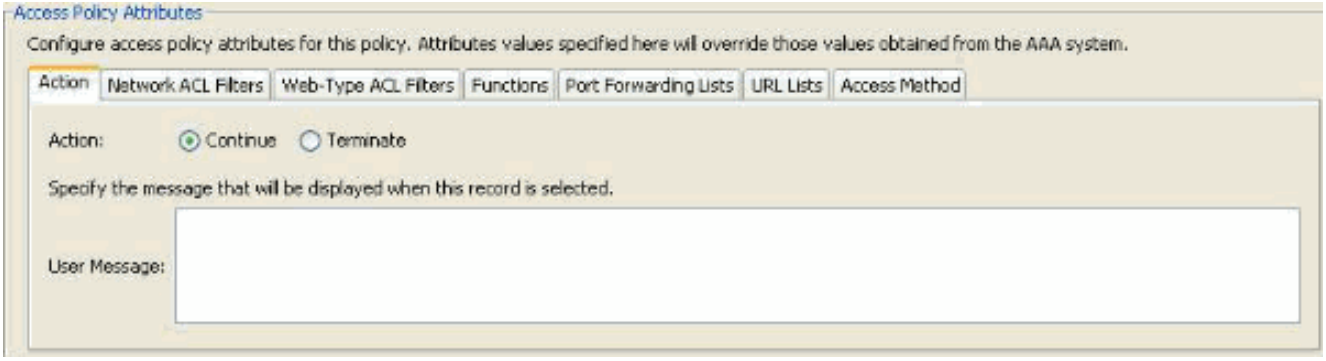


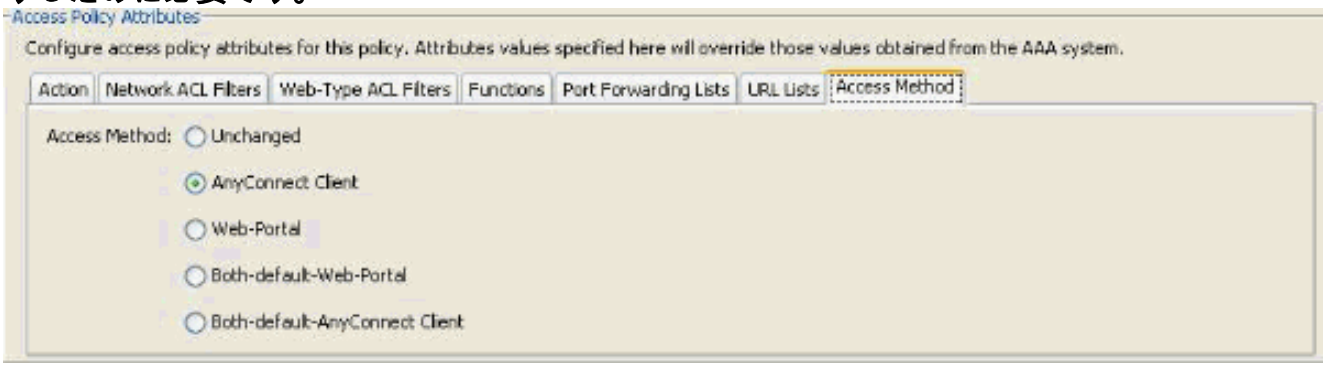
図 34. DAP AAA 属性：AAA グループ メンバーシップが、リモート アクセス機能を許可する DAP 基準として使用されます。



[Action] タブで [Action] に [Continue] を設定します（図 35 を参照）。**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] に [Terminate] が設定されている場合、VPN アクセスが拒否されます。**



[Access Method] タブの [Access Method] で [AnyConnect Client] を選択します（図 36 を参照）。**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] をクリックし、次に [Apply] をクリックします。

3. 「**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。[Description]： Employee Clientless Access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 37. DAP エンドポイント属性：Cisco Secure Desktop ロケーションがクライアントレス アクセスの DAP 基準として使用されます。**

[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 38 と 39 に示すように、AAA 属性タイプ（LDAP）を追加します（[AAA Attribute Type] ボックスの右側）。 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 メンバーシップが、従業員を識別する DAP 基準として使用されます。**

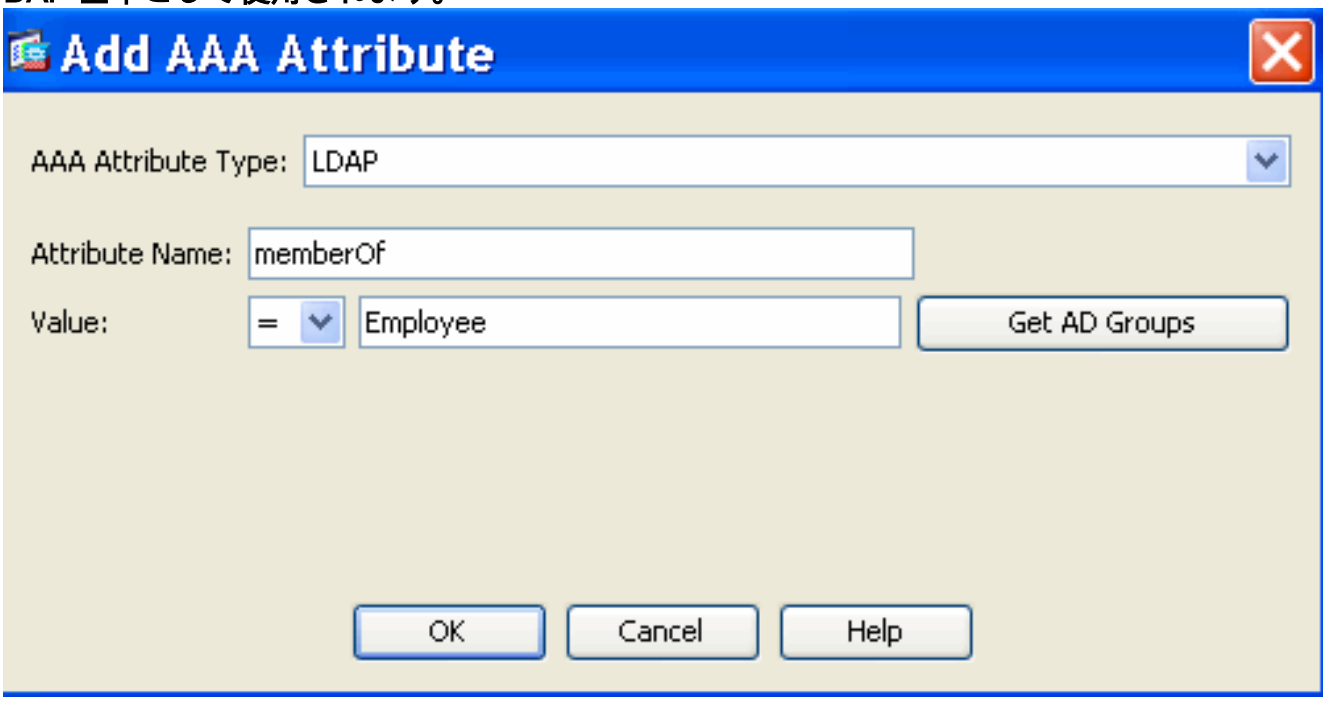
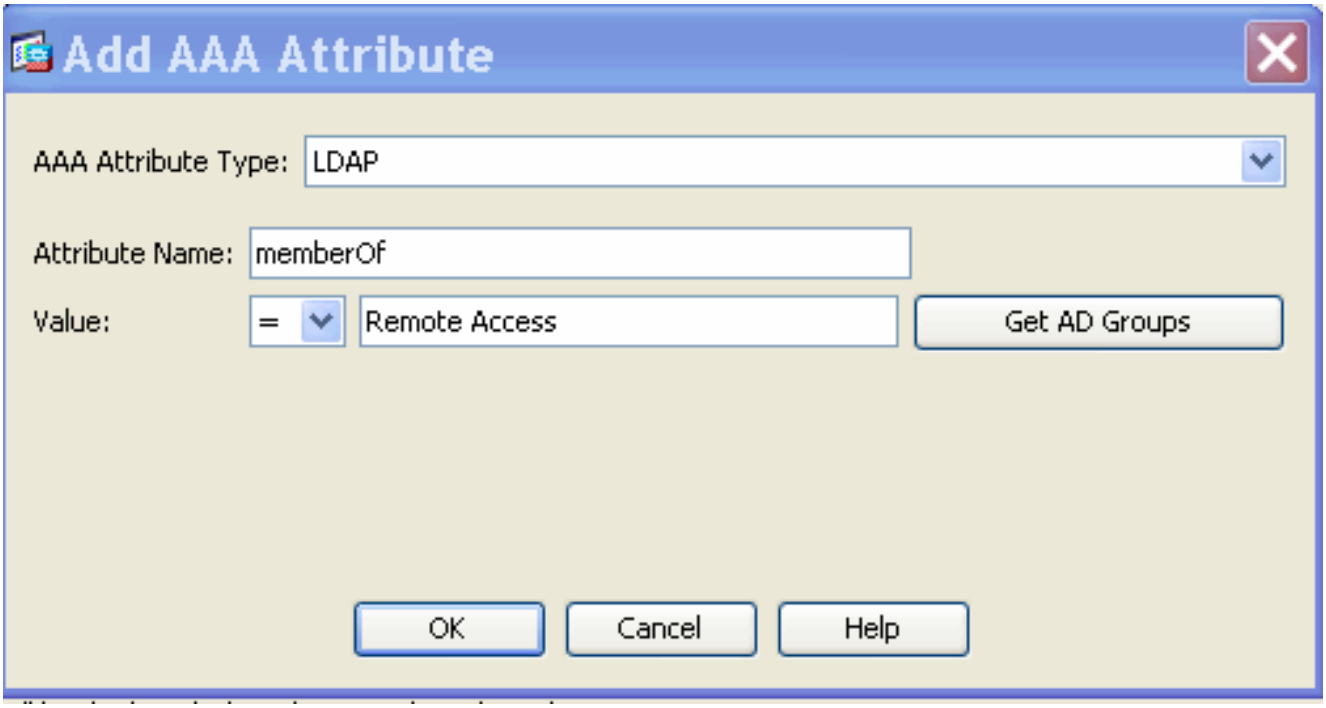
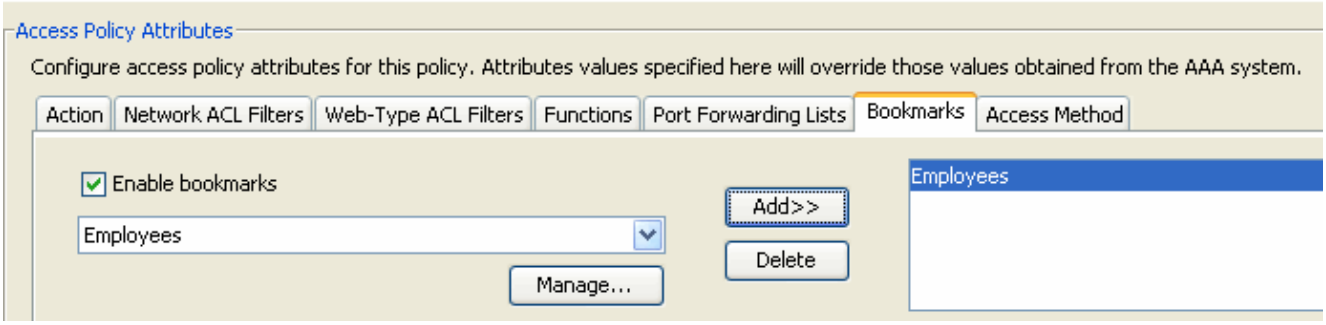


図 39. DAP AAA 属性：AAA グループ メンバーシップが、リモート アクセス機能を許可する DAP 基準として使用されます。



[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 を参照）。[Bookmarks] タブで、ドロップダウンから「**Employees**」というリスト名を選択し、[Add] 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を確認します。**図 40. [Bookmarks] タブ：ユーザ セッションの URL リストを選択して設定できます。**



[Access Method] タブでアクセス方式として [Web-Portal] を選択します（図 36 を参照）。[OK] をクリックし、次に [Apply] をクリックします。契約作業員の識別には DAP AAA 属性だけが使用されます。 このため、ステップ 4 で [Endpoint Attributes Type:] に（Policy）が設定されません。 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。

4. 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。[Description]： Guest Clientless Access。前述の図 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。[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 と 42 に示すように、AAA 属性タイプ（LDAP）を追加します（[AAA Attribute Type] 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 メンバーシップが、契約作業員を識別する DAP 基準として使用されます。**

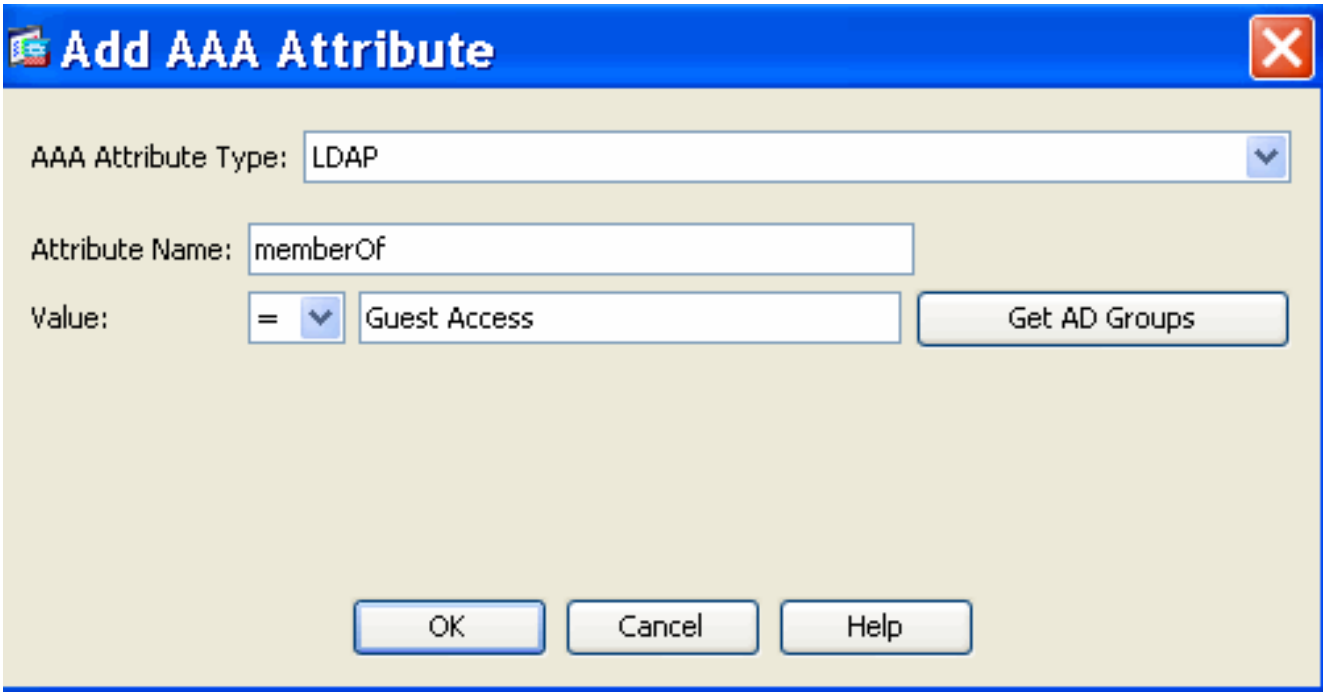


図 42. DAP AAA 属性：AAA グループ メンバーシップが、リモート アクセス機能を許可する DAP 基準として使用されます。

[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 を参照）。[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を確認します（図 40 を参照）。[Access Method] タブでアクセス方式として [Web-Portal] を選択します（図 36 を参照）。[OK] をクリックし、次に [Apply] をクリックします。

DAP 選択基準：上記の DAP 設定手順に基づいて定義される 4 つの DAP ポリシーの選択基準は、図 43、44、45、および 46 と一致しています。

図 43. 管理対象エンドポイント：この DAP レコードの基準が満たされると、従業員（Employee）に対し、クライアント/ネットワーク（AnyConnect Client）接続を介した社内リソースへのアクセスが許可されます。

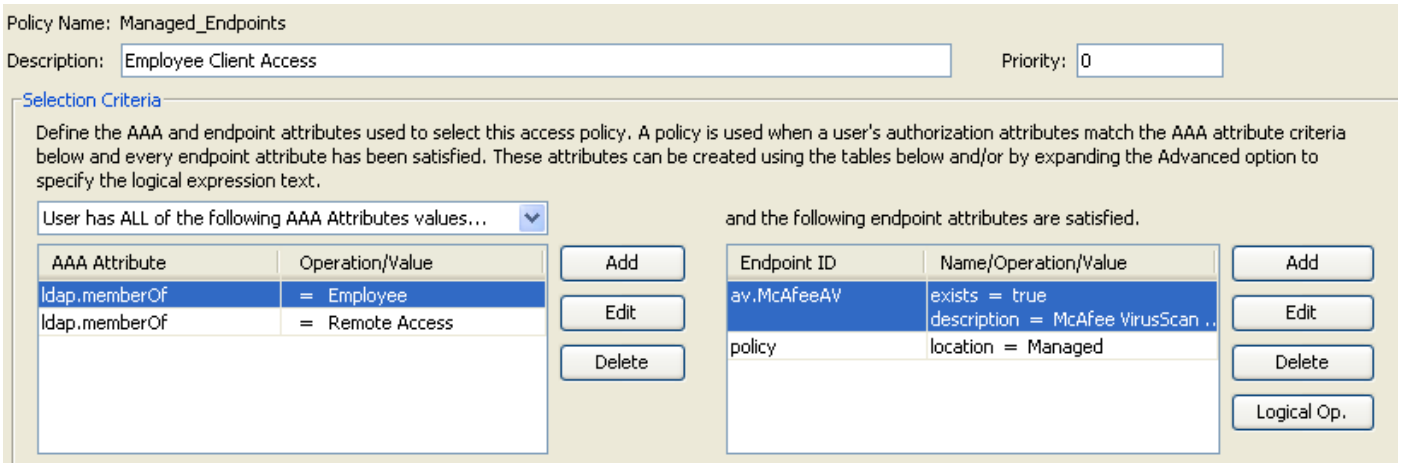


図 44. 管理対象外エンドポイント：この DAP レコードの基準が満たされると、従業員（Employee）に対し、クライアントレス（ポータル）接続を介した社内リソースへのアクセスが許可されます。 従業員の URL リストもこのポリシーに適用されます。

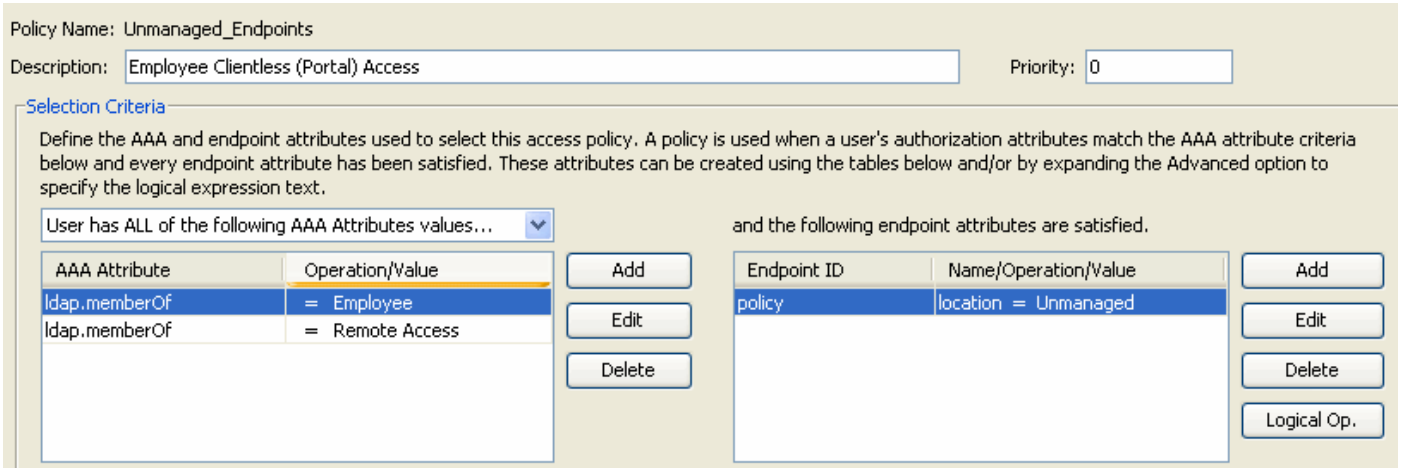


図 45. ゲスト アクセス：この DAP レコードの基準が満たされると、契約作業員に対し、クライアントレス（ポータル）接続を介した社内リソースへのアクセスが許可されます。 契約作業員の URL リストもこのポリシーに適用されます。

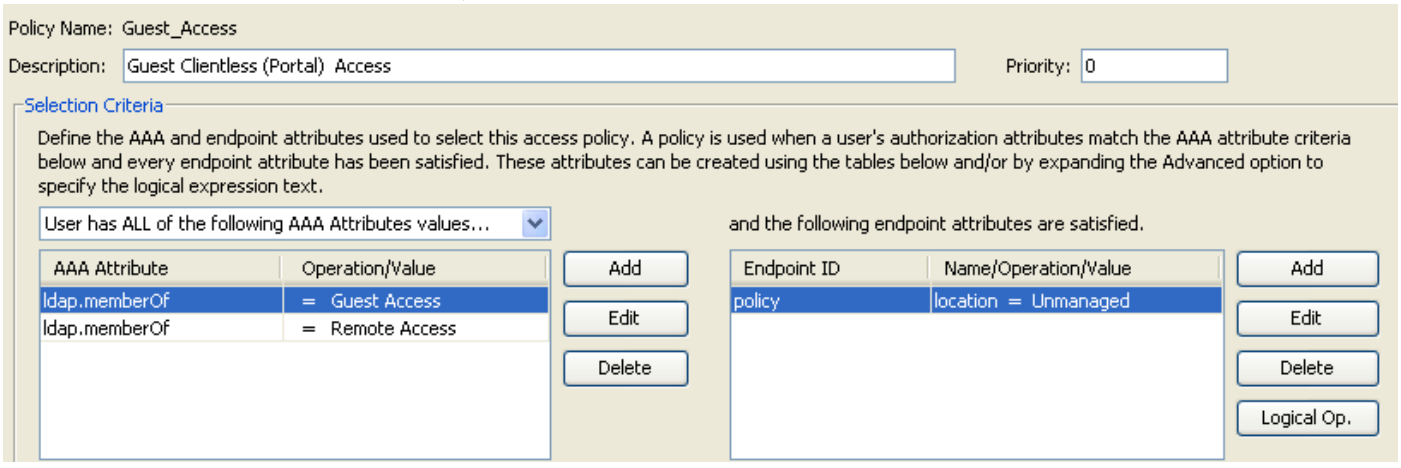
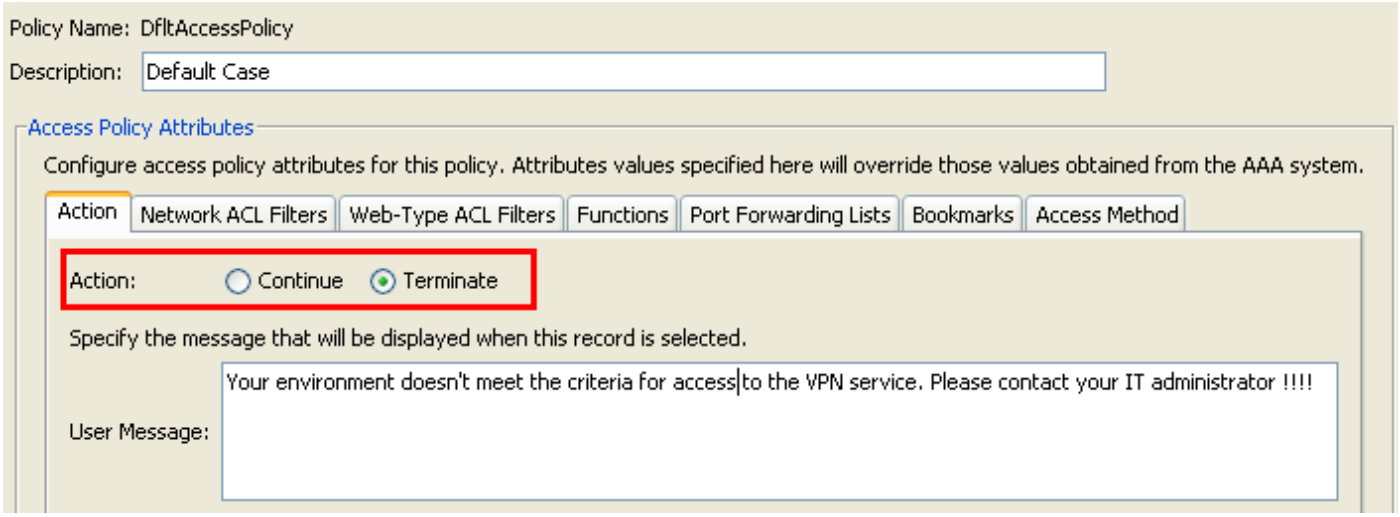


図 46. デフォルト DAP ポリシー：前述のすべての DAP レコード基準が満たされない場合、デフォルトで従業員と契約作業員に対しアクセスが拒否されます。



結論

この例に示す顧客のリモート アクセス SSL VPN 要件に基づき、このソリューションはリモート アクセス VPN 要件を満たします。

変化するダイナミックな VPN 環境により、ダイナミック アクセス ポリシーは、頻繁に変更されるイントラネット設定、組織内の各ユーザが持つさまざまなロール、および設定とセキュリティ レベルが異なる管理/管理対象外リモート アクセス サイトからのログインなどに適応して拡大できます。

ダイナミック アクセス ポリシーは、新たな技術と定評ある従来の技術（Advanced Endpoint Assessment、Host Scan、Secure Desktop、AAA、ローカル アクセス ポリシーなど）により補完されます。 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

- テクニカルサポートとドキュメント - Cisco Systems