ASA 8.x动态访问策略(DAP)部署指南

目录

简介

虚拟专用网络(VPN)网关在动态条目运行。多个变量能影响每VPN连接;例如，频繁地更改的内联网配置，每个用户可能在组织内居住的多种从远程访问站点的角色和登录用不同的配置和安全级别。就用户授权任务而言，动态 VPN 环境中的该项任务要远远复杂于拥有静态配置的网络。

动态访问策略(DAP)，用可适应安全工具(ASA)的软件版本v8.0代码介绍的新特性，使您配置寻址VPN环境Dynamics的授权。通过设置一组访问控制属性并将其与特定的用户隧道或会话相关联，您就可以创建动态访问策略。这些属性可解决有关多种组成员资格和终点安全的问题。

例如，安全设备根据您定义的策略向特定用户授予对特定会话的访问权限。它将在用户身份验证过程中通过从一个或多个 DAP 记录中选择和/或聚合多个属性来生成 DAP。它根据远程设备的终点安全信息和/或身份验证用户的 AAA 授权信息来选择这些 DAP 记录。然后，安全设备就会将这些 DAP 记录应用于用户隧道或会话。

注意： *dap.xml文件*，包含DAP策略选择属性，在ASA的闪存存储。虽然您能导出箱外dap.xml的文件，请编辑它(如果知道关于xml语法)，并且再进口它回到，非常小心，因为您能造成ASDM停止处理DAP记录，如果不正确配置某事。没有操作配置的这部分的CLI。

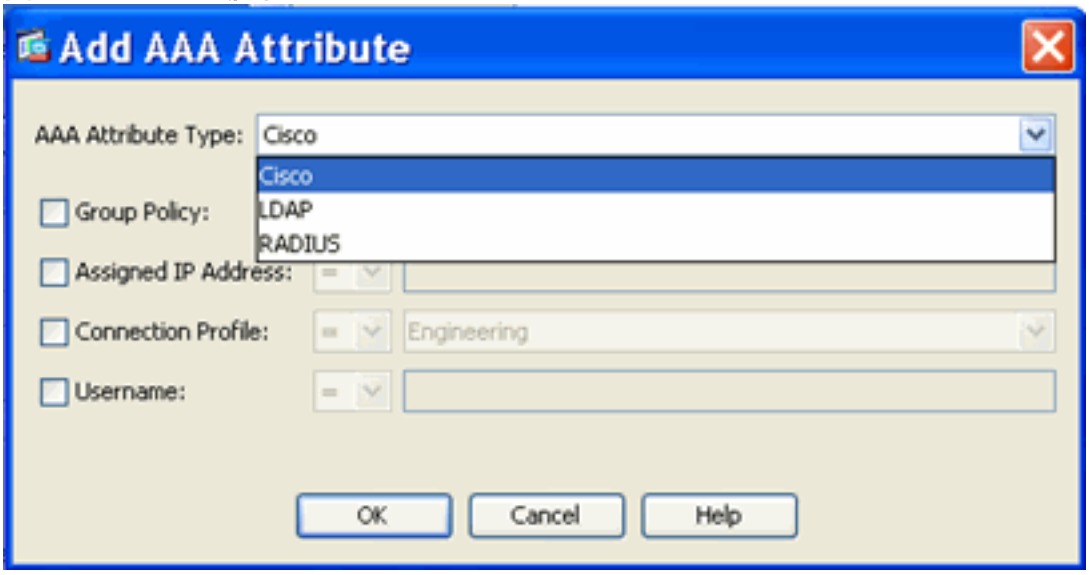
注意： 配置动态访问策略*记录访问*参数的尝试通过CLI能造成DAP停止工作，虽然ASDM将正确地管理同样。避免CLI和总是请使用ASDM管理DAP策略。

DAP 和 AAA 属性

DAP 是对 AAA 服务所做的补充，它提供了一组有限的授权属性，这些属性可以覆盖 AAA 提供的属性。安全设备可以根据用户的 AAA 授权信息选择 DAP 记录。安全设备可以根据此信息选择多个 DAP 记录，然后聚合这些记录以分配 DAP 授权属性。

您可以从 Cisco AAA 属性层次结构中指定 AAA 属性，也可以在安全设备从 RADIUS 或 LDAP 服务器接收到的全套响应属性中进行指定，如图 1 所示。

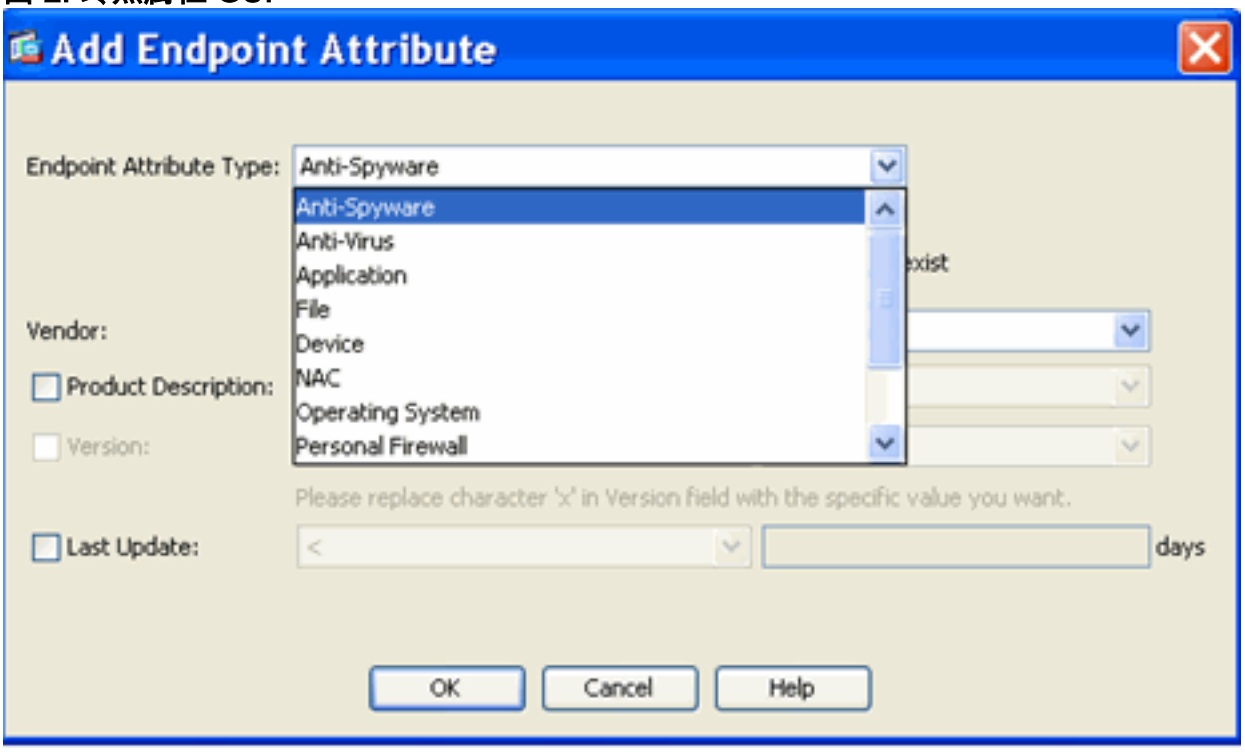
图 1. DAP AAA 属性 GUI



DAP 和终点安全属性

除 AAA 属性之外，安全设备还可以通过使用您配置的状态评估方法获取终点安全属性。这些属性包括 Basic Host Scan、Secure Desktop、Standard/Advanced Endpoint Assessment 和 NAC，如图 2 所示。终点评估属性将在用户身份验证之前获取，并发送到安全设备。但是，AAA 属性（包括整体 DAP 记录）将在用户身份验证过程中检验。

图 2. 终点属性 GUI

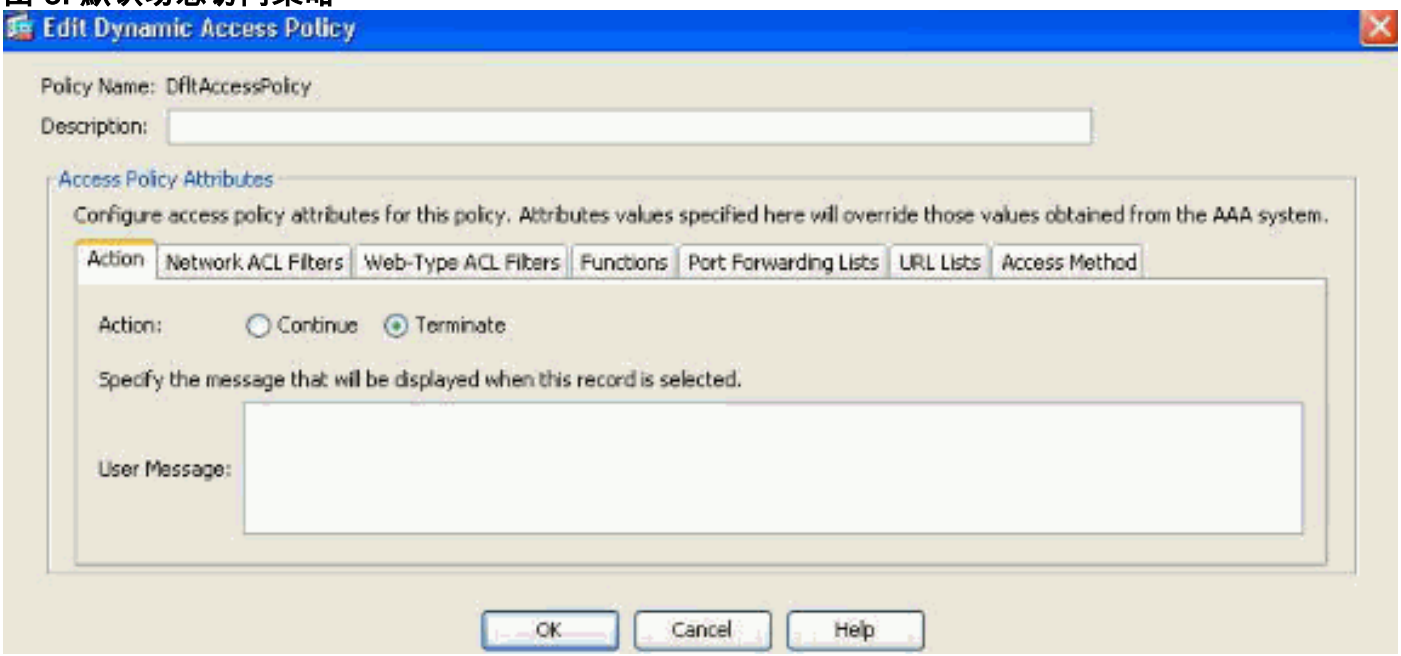


默认动态访问策略

在引入和实施 DAP 之前，会在 ASA 本地定义或者通过外部 AAA 服务器映射与特定的用户隧道或会话相关联的访问策略属性/值对（即隧道组和组策略）。然而，在 v8.0 版本中，DAP 可配置为补充或覆盖本地和外部访问策略。

默认情况下总是强制执行 DAP。然而，对于更倾向于使用传统策略执行方法的管理员，例如，通过隧道组、组策略和 AAA 强制执行访问控制但并不显式执行 DAP，这样仍然可以获得此类行为。对于传统行为，无需对 DAP 功能的配置（包括默认 DAP 记录和 DfltAccessPolicy）进行任何更改，如图 3 所示。

图 3. 默认动态访问策略



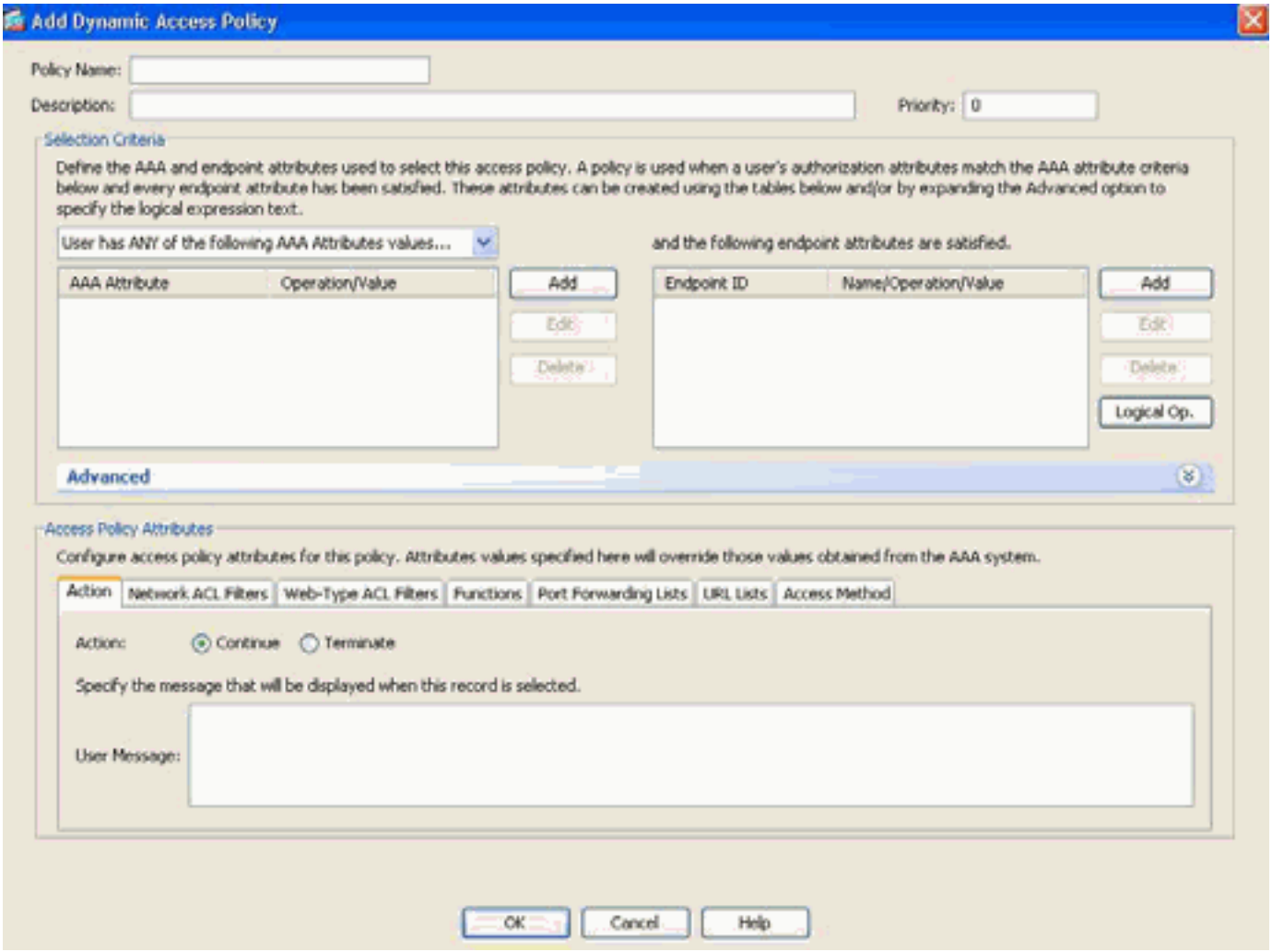
然而，如果更改了 DAP 记录中的任一默认值，例如，将 DfltAccessPolicy 中的 Action: 参数从其默认值更改为 Terminate，并且没有配置其他 DAP 记录，则默认情况下，进行身份验证的用户将匹配 DfltAccessPolicy DAP 记录，其 VPN 访问请求会遭到拒绝。

因此，将需要创建并配置一个或多个 DAP 记录，以便允许 VPN 连接并定义通过身份验证的用户有权访问哪些网络资源。这样，如果配置了 DAP，它将比传统策略优先执行。

配置动态访问策略

如果使用 DAP 定义用户有权访问的网络资源，则要考虑许多参数。例如，识别连接终点是来自受管型、非受管型还是不受信任的环境、确定必要的选择标准以识别连接终点，以及基于终点评估和/或 AAA 凭证确定连接的用户有权访问的网络资源。要完成此过程，首先需要熟悉 DAP 特性和功能，如图 4 所示。

图 4. 动态访问策略



在配置 DAP 记录时，需要考虑两个主要组成部分：

- Selection Criteria（包括 Advanced 选项）
- Access Policy Attributes

Selection Criteria 部分由管理员用于配置 AAA 和终点属性，这些属性将用于选择特定的 DAP 记录。当用户的授权属性与 AAA 属性标准相匹配、并且已满足每个终点属性时，将使用 DAP 记录。

例如，如果选择 AAA Attribute Type:LDAP (活动目录)选择，属性名称字符串是memberOf如图5a所显示，并且值字符串是承包商，正在验证用户必须是匹配AAA属性标准的活动目录组承包商的成员。

除了满足 AAA 属性标准以外，进行身份验证的用户还需要满足终点属性标准。例如，如果管理员配置Cisco Secure Desktop (CSD)确定连接的终端的状态和根据该状态评估，终端在不受管理CSD的位置安置了，管理员可能然后使用此评估信息，当终端的选择标准在图5b上归因于显示。

图 5a.AAA 属性标准

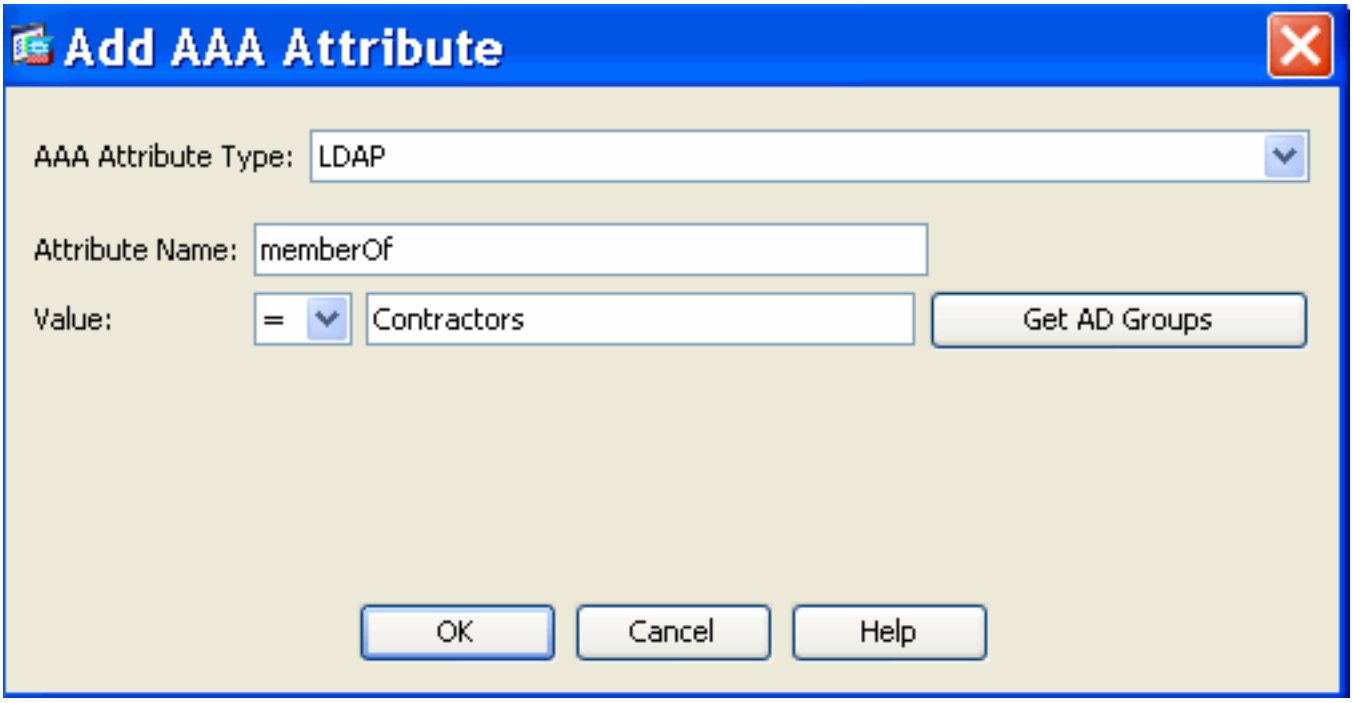
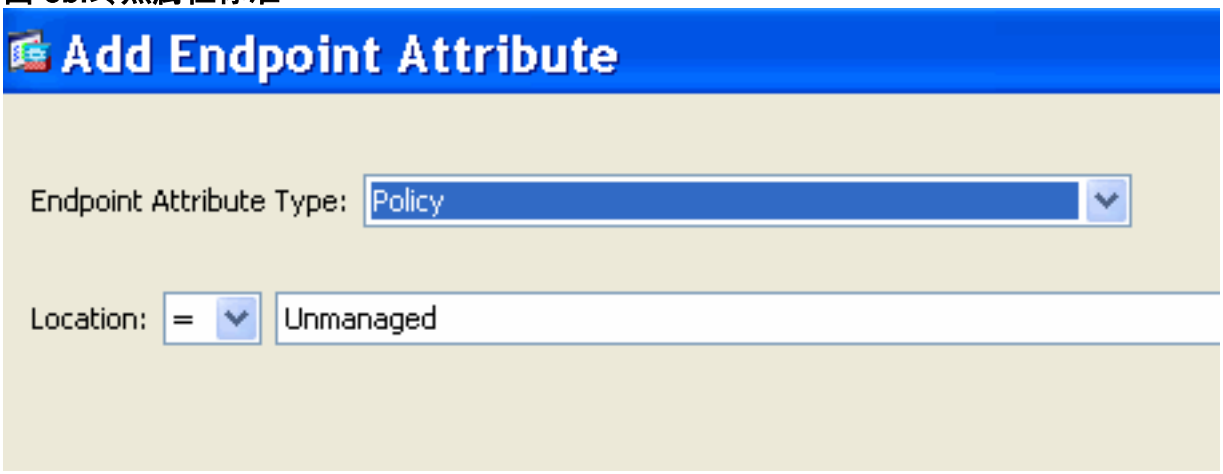
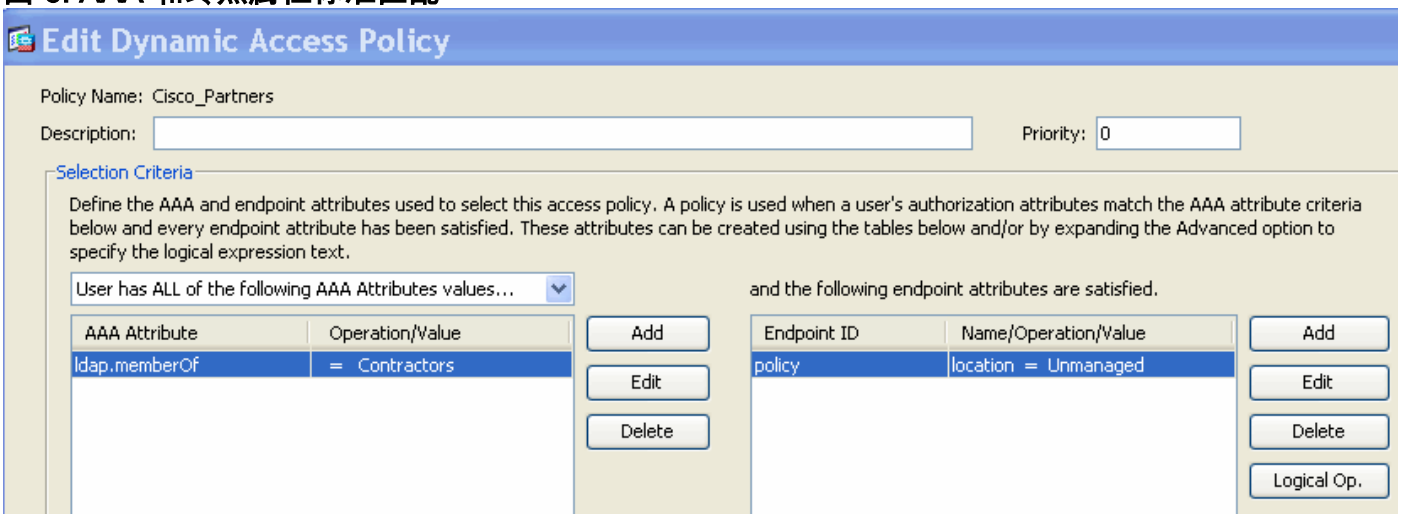


图 5b.终点属性标准



因此，要匹配图 6 所示的 DAP 记录，进行身份验证的用户必须是 Contractors Active Directory 组的成员，并且其连接终点必须满足 CSD 策略值“Unchanged”，这样才能对其分配 DAP 记录。

图 6. AAA 和终点属性标准匹配



如图 6 所示使用表格和/或如图 7 所示展开 Advanced 选项以指定逻辑表达式，可创建 AAA 和终点属性。目前，逻辑表达式通过 EVAL 函数而构建，例如，EVAL

(endpoint.av.McAfeeAV.exists,"EQ","true","string") 和 EVAL (endpoint.av.McAfeeAV.description,"EQ","McAfee VirusScan Enterprise","string")，表示 AAA 和/或终点选择逻辑运算。

逻辑表达式对于添加上述 AAA 和终点属性区域中无法添加的选择标准非常有用。例如，您可以配置安全设备使用满足任何或所有指定标准或者不满足任何指定标准的 AAA 属性，但终点属性是累加性的，必须全部满足。要让安全设备使用一个或另一个终点属性，需要在 DAP 记录的 Advanced 部分下创建适当的逻辑表达式。

图 7. 用于创建高级属性的逻辑表达式 GUI

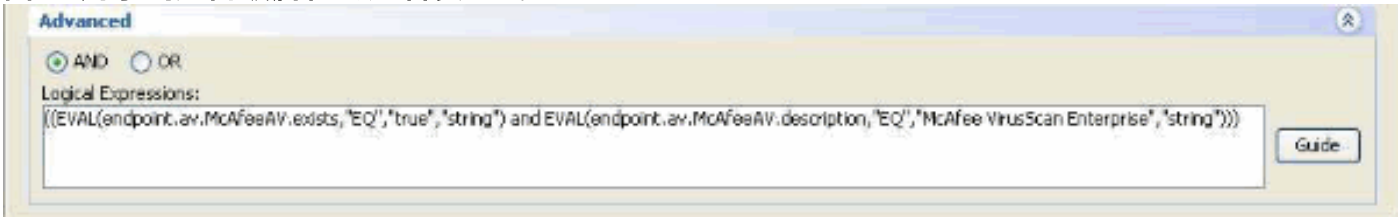
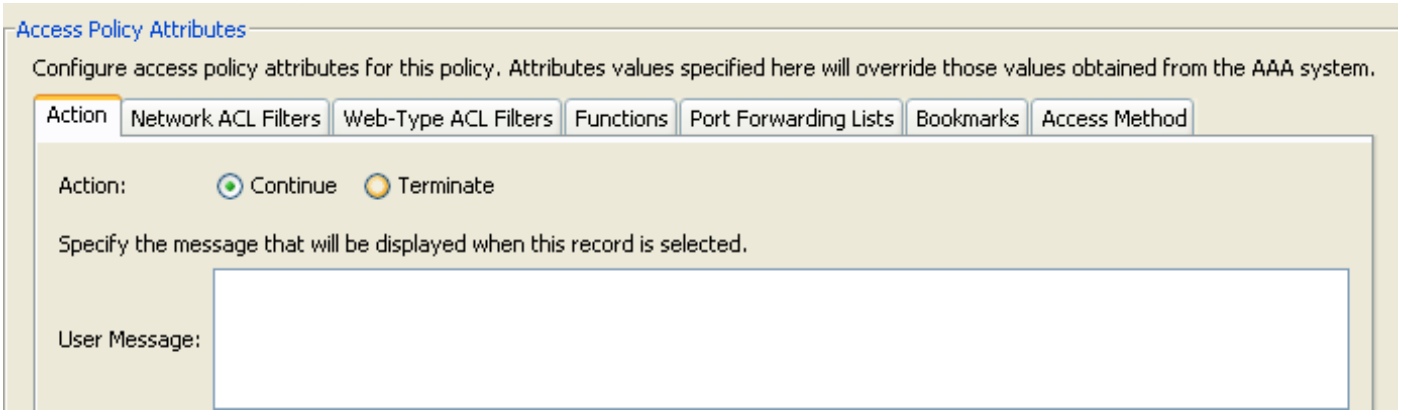


图 8 所示的 Access Policy Attributes 部分由管理员用于针对特定的 DAP 记录配置 VPN 访问属性。当用户的授权属性匹配 AAA、终点和/或逻辑表达式标准时，将强制执行此部分中配置的访问策略属性值。此处指定的属性值将覆盖从 AAA 系统获取的值，包括现有的用户、组、隧道组和默认组记录中的值。

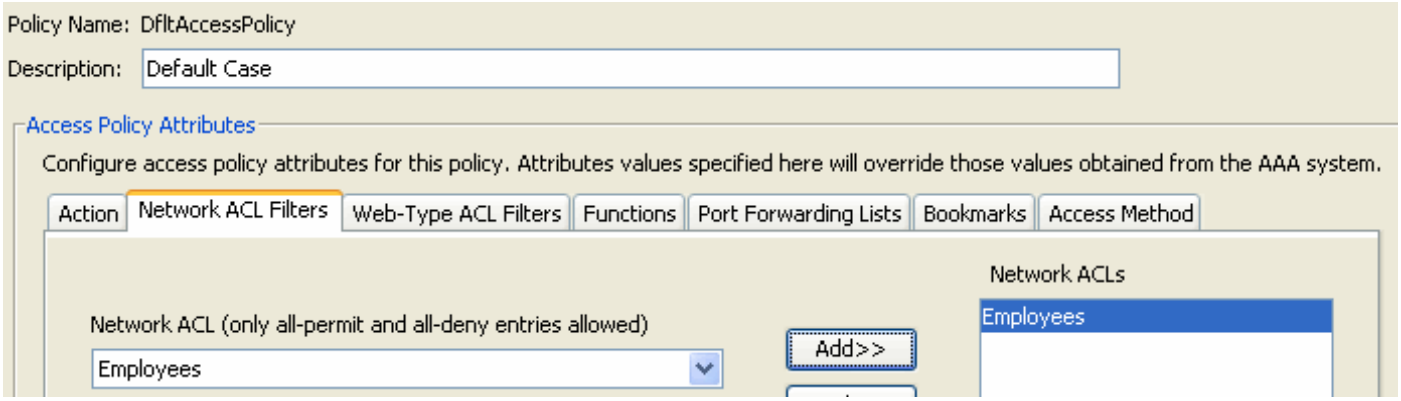
DAP 记录具有一组有限的、可配置的属性值。这些值出现在以下选项卡中，如图 8 至 14 所示：

图 8. Action - 指定应用于特定连接或会话的特殊处理。



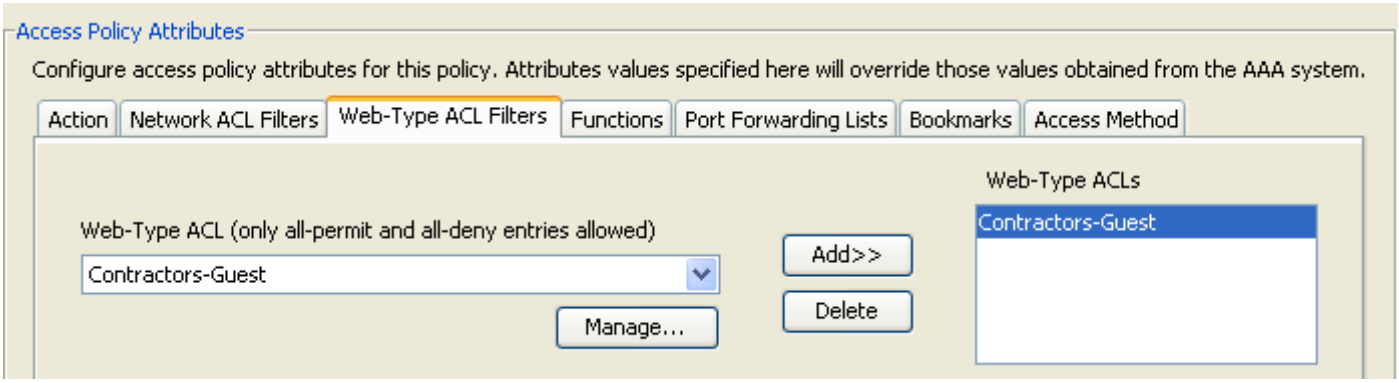
- Continue - (默认值) 单击此值可将访问策略属性应用于会话。
- Terminate - 单击此值可终止会话。
- User Message - 输入一段文本消息，选择此 DAP 记录时，将在门户页上显示该消息。最多可输入 128 个字符。用户消息显示为黄色球体。当用户登录时，该球体将闪烁三次以引起注意，然后就会静止。如果选择了多个 DAP 记录，并且每个记录都具有用户消息，则将显示所有用户消息。另外，可以在此类消息中加入 URL 或其他嵌入式文本，但要求使用正确的 HTML 标记。

图 9. Network ACL Filters 选项卡 - 用于选择和配置要应用于此 DAP 记录的网络 ACL。DAP 的 ACL 可以包含允许或拒绝规则，但不能同时包含二者。如果 ACL 同时包含允许和拒绝规则，安全设备将拒绝该 ACL 配置。



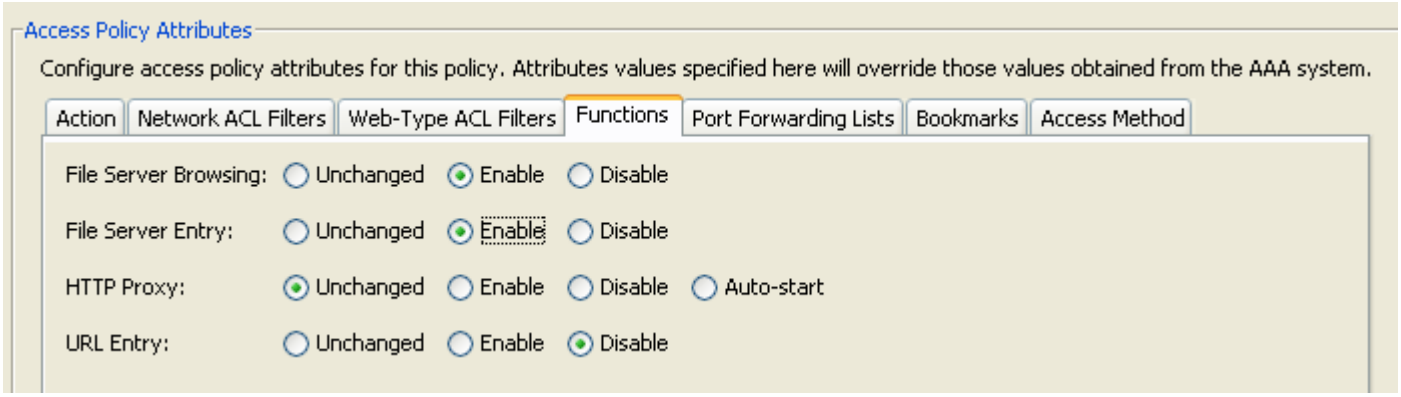
- Network ACL 下拉框 - 选择已配置的网络 ACL 以便添加到此 DAP 记录中。只有包含的规则全部都是允许规则或全部都是拒绝规则的 ACL 才符合规定，并且此处也只会显示这一类 ACL。
- Manage - 单击此按钮可添加、编辑和删除网络 ACL。
- Network ACLs 列表 - 显示此 DAP 记录的网络 ACL。
- Add - 单击此按钮可将下拉框中所选的网络 ACL 添加到右边的 Network ACLs 列表。
- Delete - 单击此按钮可从 Network ACLs 列表中删除突出显示的网络 ACL。如果某个 ACL 已分配到 DAP 或其他记录，则不能删除。

图 10. Web-Type ACL Filters 选项卡 - 用于选择和配置要应用于此 DAP 记录的 Web 型 ACL。DAP 的 ACL 可以仅包含允许规则或仅包含拒绝规则。如果 ACL 同时包含允许和拒绝规则，安全设备将拒绝该 ACL 配置。



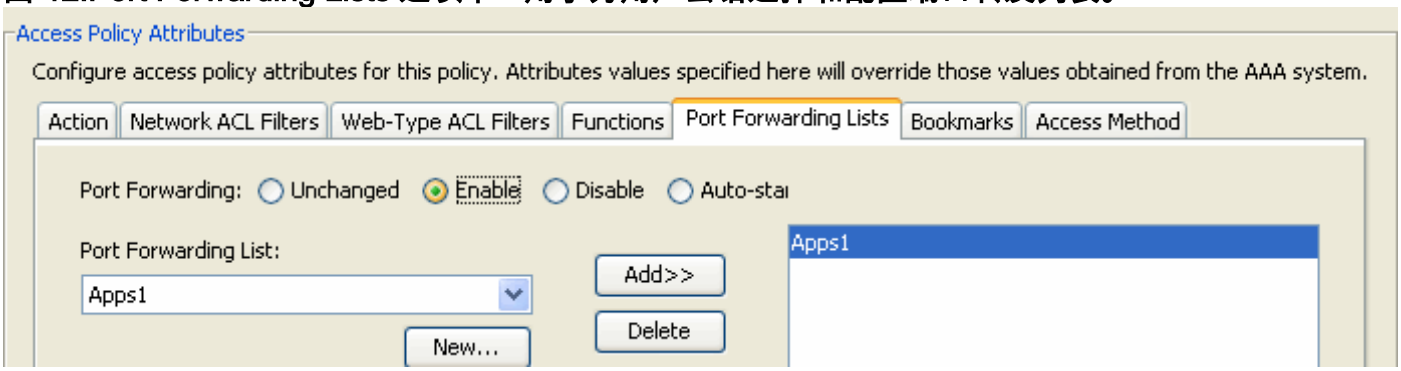
- Web-Type ACL 下拉框 - 选择已配置的 Web 型 ACL 以便添加到此 DAP 记录中。只有包含的规则全部都是允许规则或全部都是拒绝规则的 ACL 才符合规定，并且此处也只会显示这一类 ACL。
- 管理...- 单击此按钮可添加、编辑和删除 Web 型 ACL。
- Web-Type ACLs 列表 - 显示此 DAP 记录的 Web 型 ACL。
- Add - 单击此按钮可将下拉框中所选的 Web 型 ACL 添加到右边的 Web-Type ACLs 列表。
- Delete - 单击此按钮可从 Web-Type ACLs 列表中删除 Web 型 ACL。如果某个 ACL 已分配到 DAP 或其他记录，则不能删除。

图 11. Functions 选项卡 - 用于配置 DAP 记录的文件服务器输入和浏览、HTTP 代理以及 URL 输入。



- File Server Browsing - 启用或禁用文件服务器的 CIFS 浏览或者共享功能。
- File Server Entry - 允许或拒绝用户在门户页上输入文件服务器路径和名称。启用时，会将文件服务器输入抽屉置于门户页上。用户可以直接输入 Windows 文件的路径名称，也可以下载、编辑、删除、重命名和移动文件，同时还可以添加文件和文件夹。还必须配置共享，以便用户在适用的 Microsoft Windows 服务器上进行访问。用户可能必须通过身份验证才能访问文件，具体取决于网络要求。
- HTTP Proxy - 影响 HTTP 小程序代理到客户端的转发。代理对于会干扰正确内容转换的技术（如 Java、ActiveX 和 Flash）非常有用。在确保安全设备持续工作的同时，它会绕过破坏/重写进程。转发的代理会自动地修改浏览器的旧代理配置，并将所有 HTTP 和 HTTPS 请求重定向到新代理配置。它几乎可以支持所有客户端技术，包括 HTML、CSS、JavaScript、VBScript、ActiveX 和 Java。它唯一支持的浏览器是 Microsoft Internet Explorer。
- URL Entry - 允许或阻止用户在门户页上输入 HTTP/HTTPS URL。如果启用此功能，则用户可在 URL 输入框中输入 Web 地址，并且可使用无客户端 SSL VPN 访问这些网站。
- Unchanged -（默认值）单击以使用应用于此会话的组策略中的值。
- Enable/Disable - 单击以启用或禁用该功能。
- Auto-start - 单击以启用 HTTP 代理，并使 DAP 记录自动启动与这些功能关联的小程序。

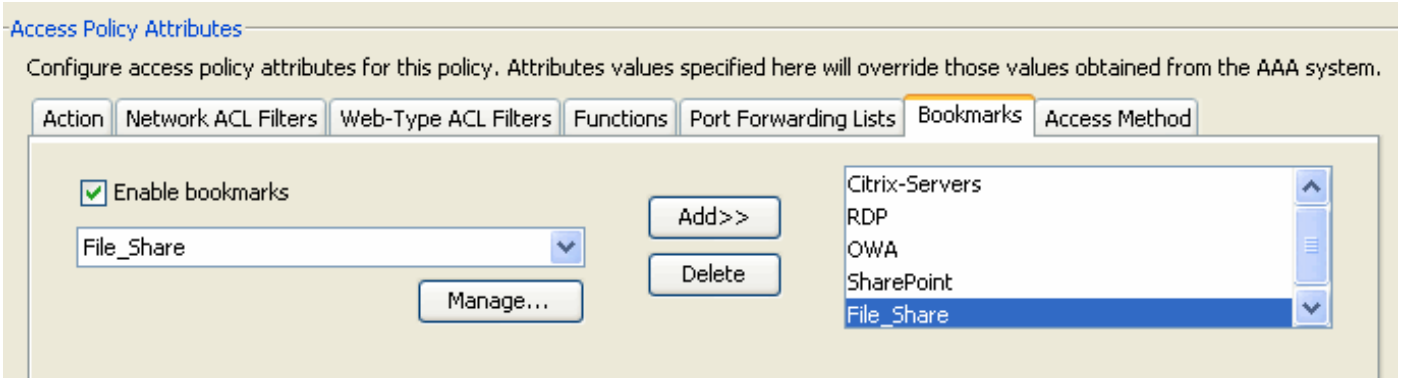
图 12.Port Forwarding Lists 选项卡 - 用于为用户会话选择和配置端口转发列表。



- Port Forwarding - 为应用于此 DAP 记录的端口转发列表选择一个选项。只有将 Port Forwarding 设置为 Enable 或 Auto-start 时，此字段中的其他属性才会启用。
- Unchanged - 单击以使用应用于此会话的组策略中的值。
- Enable/Disable - 单击以启用或禁用端口转发。
- Auto-start - 单击以启用端口转发，并使 DAP 记录自动启动与其端口转发列表关联的端口转发小程序。
- Port Forwarding List 下拉框 - 选择已配置的端口转发列表以便添加到 DAP 记录中。
- 新请单击配置新建的端口转发列表。
- Port Forwarding Lists - 显示 DAP 记录的端口转发列表。
- Add - 单击此按钮将下拉框中所选的端口转发列表添加到右边的 Port Forwarding Lists。
- Delete - 单击此按钮可从 Port Forwarding Lists 中删除所选的端口转发列表。如果某个 ACL 已

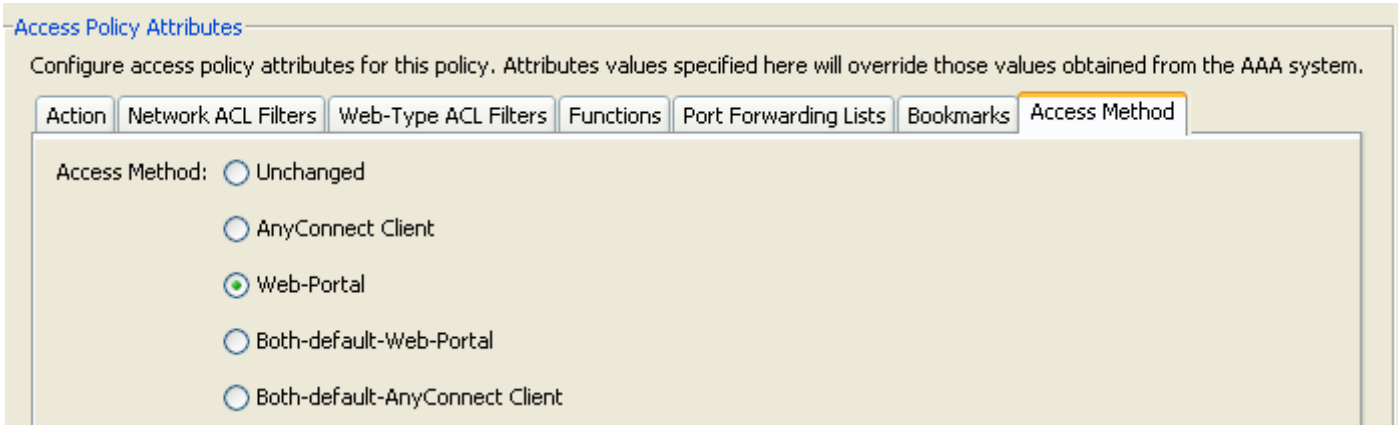
分配到 DAP 或其他记录，则不能删除。

图 13.Bookmarks 选项卡 - 用于为用户会话选择和配置书签/URL 列表。



- Enable bookmarks - 单击以启用。如果未选中此框，则连接的门户页上将不显示书签列表
- Manage - 单击以添加、导入、导出和删除书签列表。
- Bookmarks Lists（下拉式）- 显示 DAP 记录的书签列表。
- Add - 单击此按钮将下拉框中所选的书签列表添加到右边的书签列表框中。
- 删除 - 单击此按钮可从书签列表框中删除所选的书签列表。除非首先从 DAP 记录中删除，否则无法从安全设备上删除书签列表。

图 14.Access Method 选项卡 - 用于配置允许的远程访问类型。



- Unchanged - 继续使用会话组策略中设置的当前远程访问方法。
- AnyConnect Client - 使用 Cisco AnyConnect VPN 客户端进行连接。
- Web-Portal - 使用无客户端 VPN 进行连接。
- Both-default-Web-Portal - 通过无客户端或 AnyConnect 客户端进行连接，其中无客户端为默认值。
- Both-default-AnyConnect Client - 通过无客户端或 AnyConnect 客户端进行连接，其中 AnyConnect 为默认值。

如前文所述，DAP 记录具有一组有限的默认属性值，只有在修改后，这些属性值才会优先于现有的 AAA、用户、组、隧道组和默认组记录。如果需要 DAP 范围之外的其他属性值，例如，Split Tunneling Lists、Banners、Smart Tunnels、Portal Customizations 等，则需要通过 AAA、用户、组、隧道组和默认组记录来强制执行。在这种情况下，这些特定的属性值将补充 DAP 并且不会被覆盖。因此，用户将获得在所有记录间累加的一组属性值。

聚合多个动态访问策略

管理员可以配置多个 DAP 记录，以应对各种各样的可变因素。这样，进行身份验证的用户就有可能满足多个 DAP 记录的 AAA 和终点属性标准。如此一来，这些策略中的访问策略属性要么一致

，要么互相冲突。在这种情况下，授权用户将获得在所有匹配的 DAP 记录间累加的结果。

这还包括通过身份验证、授权、用户、组、隧道组和默认组记录强制执行的唯一属性值。访问策略属性的累加结果将形成动态访问策略。下面的一些表列出了组合访问策略属性示例。这些示例描述了 3 个组合 DAP 记录的结果。

表 1 中显示的 Action 属性的值可为 Terminate 或 Continue。如果所选的任何 DAP 记录配置了 Terminate 值，则聚合属性值为 Terminate；如果所选的所有 DAP 记录都配置了 Continue 值，则聚合属性值为 Continue。

表 1. Action 属性

属性名称	DAP#1	DAP#2	DAP#3	DAP
Action（示例 1）	继续	继续	继续	继续
Action（示例 2）	终止	继续	继续	终止

表 2 中显示的 user-message 属性包含一个字符串值。聚合属性值将为换行（十六进制值 0x0A）分隔的字符串，该字符串通过将所选 DAP 记录的属性值链接起来而创建。组合字符串中属性值的顺序无关紧要。

表 2. User-Message 属性

属性名称	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 中显示的无客户端功能启用属性 (Functions) 包含的值为 Auto-start、Enable 或 Disable。如果所选的任何 DAP 记录配置了 Auto-start 值，则聚合属性值为 Auto-start。

如果所选的 DAP 记录中均未配置 Auto-start 值，且所选的 DAP 记录中至少有一个配置了 Enable 值，则聚合属性值为 Enable。

如果所选的 DAP 记录中既未配置 Auto-start 值，也未配置 Enable 值，且所选的 DAP 记录中至少有一个配置了 Disable 值，则聚合属性值为 Disable。

表 3. 无客户端功能启用属性 (Functions)

属性名称	DAP#1	DAP#2	DAP#3	DAP
port-forward	enable (event)	禁用		enable (event)
file-browsing	禁用	enable (event)	禁用	enable (event)
file-entry			禁用	禁用
http-proxy	禁用	auto-start	禁用	auto-start
url-entry	禁用		enable (event)	enable (event)

表 4 中显示的 url-list 和 port-forward 属性包含的值为字符串或逗号分隔的字符串。聚合属性值将为逗号分隔的字符串，该字符串通过将所选 DAP 记录的属性值链接起来而创建。组合字符串中任何重复的属性值都将被删除。组合字符串中属性值的顺序无关紧要。

表 4. URL List 和 Port Forward List 属性

属性名称	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 属性指定针对 SSL VPN 连接所允许的客户端访问方法。客户端访问方法可以为仅允许 AnyConnect 客户端访问、仅允许 Web 门户访问、允许 AnyConnect 客户端或 Web 门户访问但将 Web 门户访问作为默认值或者允许 AnyConnect 客户端或 Web 门户访问但将 AnyConnect 客户端访问作为默认值。表 5 中汇总了聚合属性值。

表 5. Access Method 属性

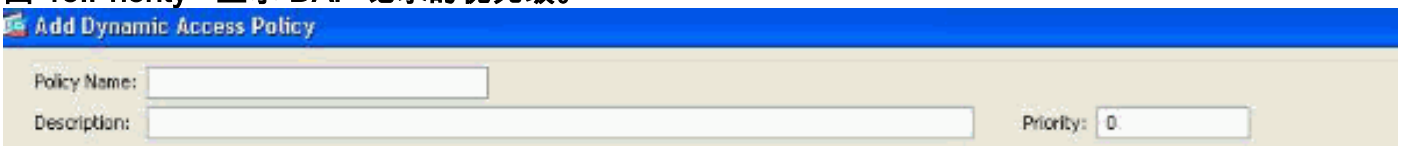
所选的属性值				聚合结果
AnyConnect Client	Web-Portal	Both-default-Web-Portal	Both-default-AnyConnect Client	
			X	Both-default-AnyConnect Client
		X		Both-default-Web-Portal
		X	X	Both-default-Web-Portal
	X			Web-Portal
	X		X	Both-default-AnyConnect Client
	X	X		Both-default-Web-Portal
	X	X	X	Both-default-Web-Portal
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

聚合网络（防火墙）ACL 过滤器和 Web 型（无客户端）ACL 过滤器属性时，DAP Priority 和 DAP ACL 是要考虑的两个主要组成部分。

图 15 所示的 Priority 属性尚未聚合。聚合多个 DAP 记录中的网络和 Web 型 ACL 时，安全设备将使用此值对访问列表进行逻辑排序。安全设备按优先级编号从最高到最低对记录进行排序，优先级最低的排在表格底部。例如，值为 4 的 DAP 记录优先级高于值为 2 的记录。不能手动进行排序。

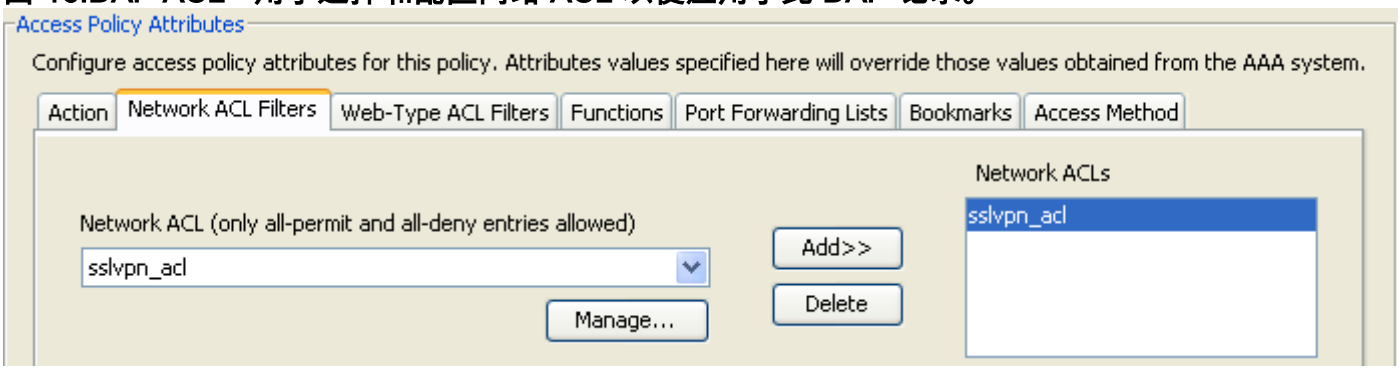
图 15.Priority - 显示 DAP 记录的优先级。



- Policy Name - 显示 DAP 记录的名称。
- Description - 描述 DAP 记录的用途。

DAP ACL 属性只支持符合严格的“白名单”或严格的“黑名单”ACL 模式的访问列表。在“白名单”ACL 模式中，访问列表条目指定“允许”访问指定网络或主机的规则。在“黑名单”ACL 模式中，访问列表条目指定“拒绝”访问指定网络或主机的规则。在不符合规定的访问列表中，访问列表条目既包含“允许”规则也包含“拒绝”规则。如果为 DAP 记录配置了不符合规定的访问列表，那么当管理员尝试添加此记录时，该列表将作为配置错误遭到拒绝。如果为 DAP 记录分配了符合规定的访问列表，那么对该访问列表所做的任何修改如果更改了合规性特征，就会作为配置错误遭到拒绝。

图 16.DAP ACL - 用于选择和配置网络 ACL 以便应用于此 DAP 记录。



选择了多个 DAP 记录时，将聚合网络（防火墙）ACL 中指定的访问列表属性，以便为 DAP 防火墙 ACL 创建动态访问列表。同样地，聚合 Web 型（无客户端）ACL 中指定的访问列表属性可以为 DAP 无客户端 ACL 创建动态访问列表。以下示例将详细介绍如何创建动态 DAP 防火墙访问列表。但是，动态 DAP 无客户端访问列表的创建过程也同样如此。

首先，ASA 将动态地为 DAP 网络 ACL 创建唯一名称，如表 6 所示。

表 6. 动态 DAP 网络 ACL 名称

DAP 网络 ACL 名称
DAP-Network-ACL-X（其中 X 是递增的整数以保证唯一性）

第二步，ASA 从所选的 DAP 记录中检索网络 ACL 属性，如表 7 所示。

表 7. 网络 ACL

所选的 DAP 记录	优先级	网络 ACL	网络 ACL 条目
DAP 1	1	101 和 102	ACL 101 具有 4 个拒绝规则，而 ACL 102 具有 4 个允许规则
DAP 2	2	201 和 202	ACL 201 具有 3 个允许规则，而 ACL 202 具有 3 个拒绝规则
DAP 3	2	101 和 102	ACL 101 具有 4 个拒绝规则，而 ACL 102 具有 4 个允许规则

第三步，ASA 将首先按 DAP 记录 Priority 编号对网络 ACL 重新排序，如果有两个或更多所选 DAP 记录的 Priority 值相同，那么接下来首先按黑名单排序。然后，ASA 将从每个网络 ACL 中检索网络 ACL 条目，如表 8 所示。

表 8. DAP 记录优先级

网络 ACL	优先级	白名单/黑名单访问列表模式	网络 ACL 条目
101	2	黑名单	4 个拒绝规则 (DDDD)
202	2	黑名单	3 个拒绝规则 (DDD)
102	2	白名单	4 个允许规则 (PPPP)
202	2	白名单	3 个允许规则 (PPP)
101	1	黑名单	4 个拒绝规则 (DDDD)
102	1	白名单	4 个允许规则 (PPPP)

最后，ASA 将网络 ACL 条目合并到动态生成的网络 ACL 中，然后返回动态网络 ACL 的名称作为要强制执行的新网络 ACL，如表 9 所示。

表 9. 动态 DAP 网络 ACL

DAP 网络 ACL 名称	网络 ACL 条目
DAP-Network-ACL-1	DDDD DDD PPPP PPP DDDD PPPP

DAP 实施

有许多原因促使管理员应该考虑实施 DAP。一些深层次的原因就存在于要强制执行终点状态评估的情况下，和/或授权用户访问网络资源时要考虑更多细粒度 AAA 或策略属性的情况下。在下面的示例中，我们将配置 DAP 及其组成部分，以识别连接终点并为用户授予对各种网络资源的访问权限。

测试案例 - 客户请求具有以下 VPN 访问要求的概念验证：

- 检测和识别员工终点是受管型还是非受管型的能力。如果确定某终点为受管型（工作 PC），但是不满足状态要求，则必须拒绝该终点的访问。另一方面，如果确定员工的终点为非受管型（家庭 PC），则必须为该终点授予无客户端访问权限。
- 在无客户端连接终止时调用会话 cookie 和缓存清理的能力。
- 在受管型员工终点上检测和强制执行运行应用程序（例如 McAfee 防病毒软件）的能力。如果没有此类应用程序，则必须拒绝该终点的访问。
- 使用 AAA 身份验证来确定授权用户应该有权访问哪些网络资源的能力。安全设备必须支持本地 MS LDAP 身份验证并支持多个 LDAP 组成员角色。
- 通过基于“客户端/网络”的连接方式进行连接时允许对网络资源（例如网络传真和打印机）进行本地 LAN 访问的能力。
- 对承包商提供授权访客访问的能力。承包商及其终点必须获得无客户端访问权限，并且与员工相比，他们对应用程序的门户访问权限必须是有限的。

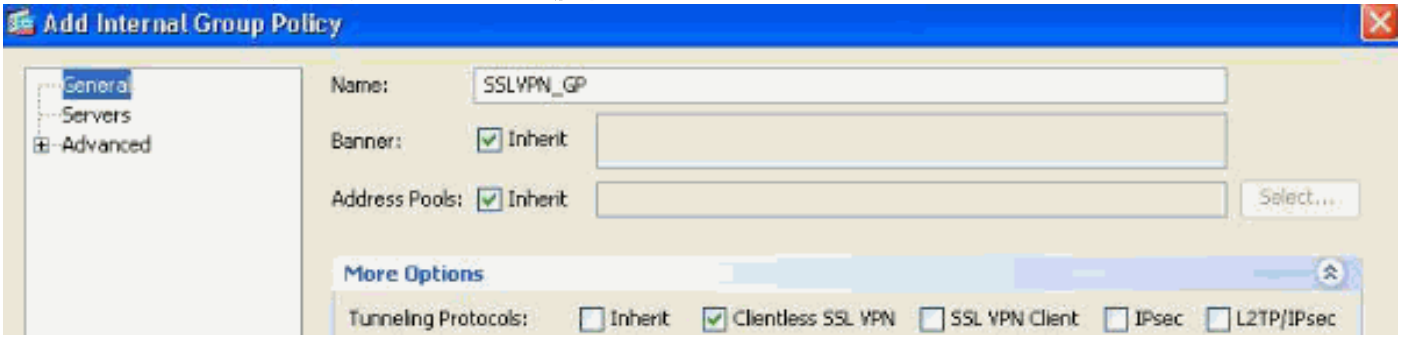
在本例中，我们将完成一系列的配置步骤，以满足客户的 VPN 访问要求。有些配置步骤是必需的，但是并不直接与 DAP 相关，而其他一些配置则直接与 DAP 相关。ASA 的动态性很强，可以适应许多网络环境。因此，可以通过多种方式定义 VPN 解决方案，并且在某些情况下会提供相同的最终解决方案。然而，实际采取的方法由用户需求及其环境决定。

基于定义的本文和用户要求的本质，我们将使用可适应安全设备管理器(ASDM) 6.0(x)并且在DAP附近集中大多我们的配置。但是，我们还将配置本地组策略，以展示 DAP 如何补充和/或覆盖本地策略属性。对于此测试案例的基础，我们假定已预先配置 LDAP Server Group、Split Tunneling Network List 和基本 IP 连接，包括 IP Pools 和 DefaultDNS Server Group。

定义组策略 - 要定义本地策略属性，必须进行此配置。此处定义的部分属性在 DAP 中是无法配置的（例如，Local LAN Access）。（此策略还将用于定义无客户端和基于客户端的属性。）

导航到 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**，然后通过执行以下操作添加一个内部组策略：

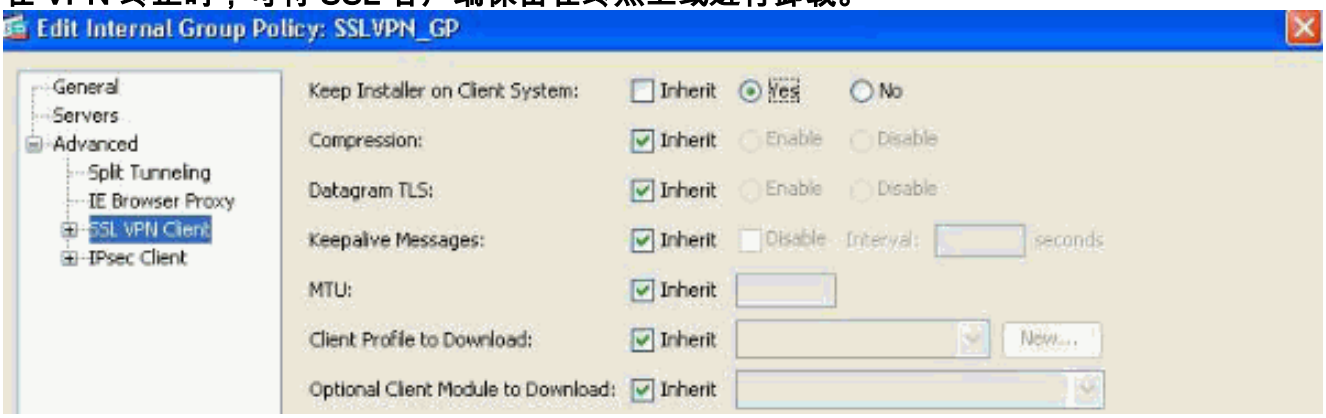
图 17.组策略 - 定义特定于本地 VPN 的属性。



1. 在 General 链接下，为组策略配置名称 **SSLVPN_GP**。
2. 还是在 General 链接下，单击 **More Options**，然后仅配置 Tunneling Protocol:**Clientless SSLVPN**。（我们将配置 DAP 以覆盖并管理访问方法。）
3. 在 Advanced > Split Tunneling 链接下，进行以下配置：**图 18.Split Tunneling - 允许指定的数据流（本地网络）在客户端连接过程中绕过未加密的隧道。**

策略：取消选中 **Inherit** 并选择 Exclude Network List Below。Network List：取消选中 **Inherit** 并选择列表名 Local_Lan_Access。（假定已预先配置。）

4. 在 Advanced > SSL VPN Client 链接下，进行以下配置：**图 19.SSL VPN 客户端安装程序 - 在 VPN 终止时，可将 SSL 客户端保留在终点上或进行卸载。**

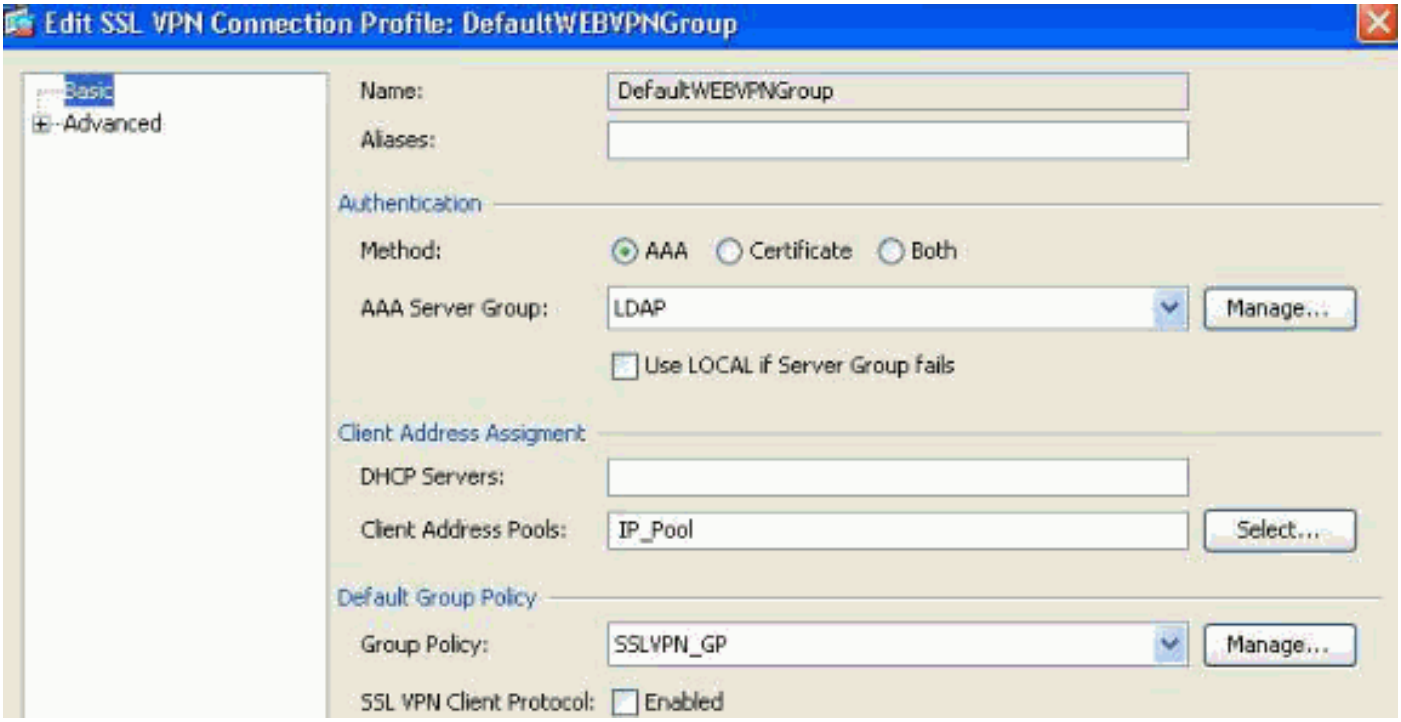


5. Keep Installer on Client System：取消选中 **Inherit**，然后选择 Yes。
6. 单击 **OK**，然后单击 Apply。
7. 应用您所做的配置更改。

定义连接配置文件 - 要定义 AAA 身份验证方法（例如 LDAP）并将之前配置的组策略 (SSLVPN_GP) 应用于此连接配置文件，必须进行此配置。通过此连接配置文件连接的用户将遵从此处定义的属性，以及在 SSLVPN_GP 组策略中定义的属性。（此配置文件还将用于定义无客户端和基于客户端的属性。）

导航到 **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles**，然后进行以下配置：

图 20.连接配置文件 - 定义特定于本地 VPN 的属性。

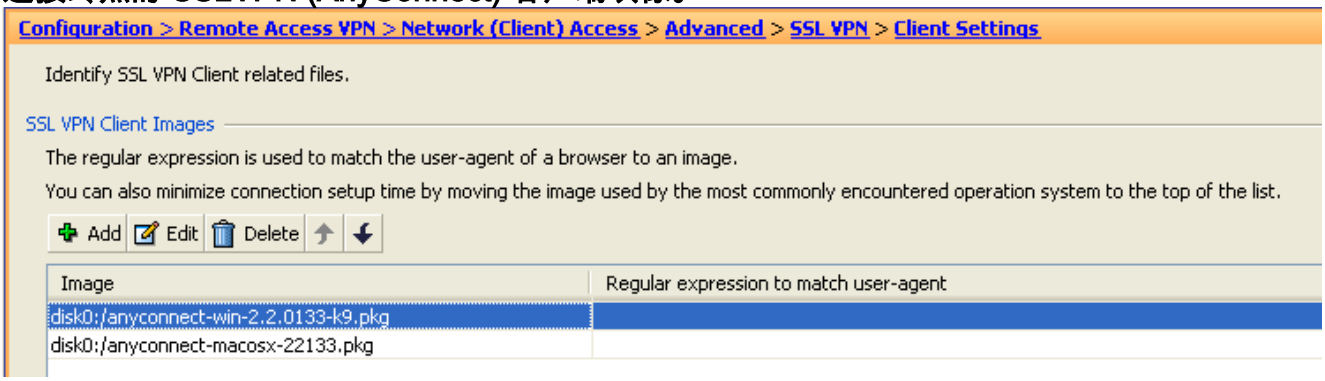


1. 在 Connection Profiles 部分下编辑 DefaultWebVPNGroup，并在 Basic 链接下进行以下配置：Authentication - Method：**AAA**Authentication - AAA Server Group：**LDAP**（假定已预先配置）Client Address Assignment - Client Address Pools：**IP_Pool**（假定已预先配置）Default Group Policy - Group Policy：选择 **SSLVPN_GP**
2. 应用您所做的配置更改。

定义用于 SSL VPN 连接的 IP 接口 - 要在指定接口上终止客户端和无客户端 SSL 连接，必须进行此配置。

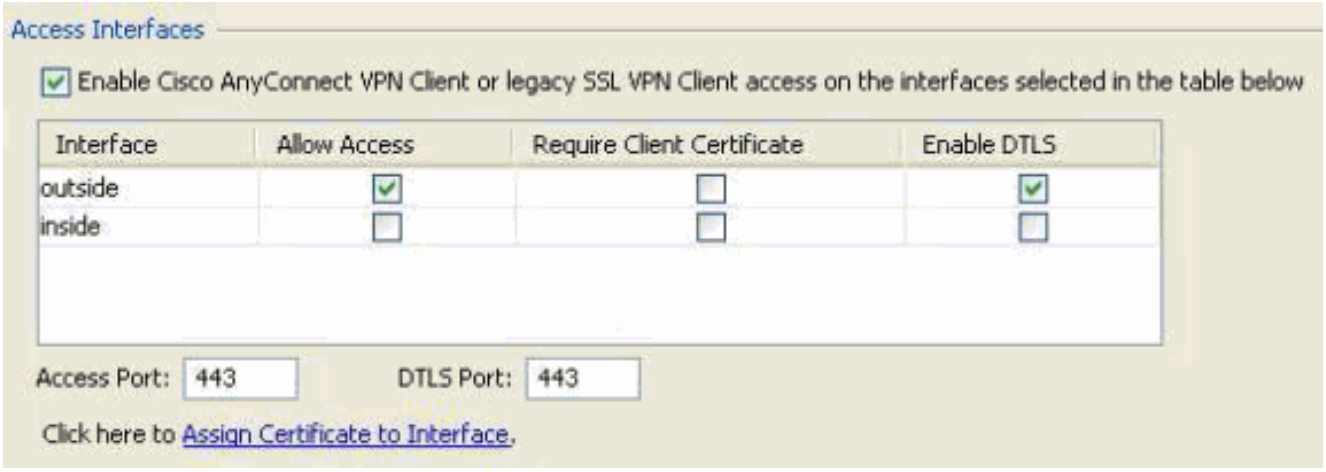
在接口上启用客户端/网络访问之前，必须先定义 SSL VPN 客户端映像。

1. 导航到 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings**，然后从 ASA 闪存文件系统中添加以下 SSL VPN 客户端映像：（可从 CCO 下载此映像，网址为 www.cisco.com）**图 21.SSL VPN 客户端映像安装 - 定义将推送到连接终点的 SSLVPN (AnyConnect) 客户端映像。**



anyconnect-win-2.x.xxx-k9.pkg单击 **OK**，接着再次单击 OK，然后单击 Apply。

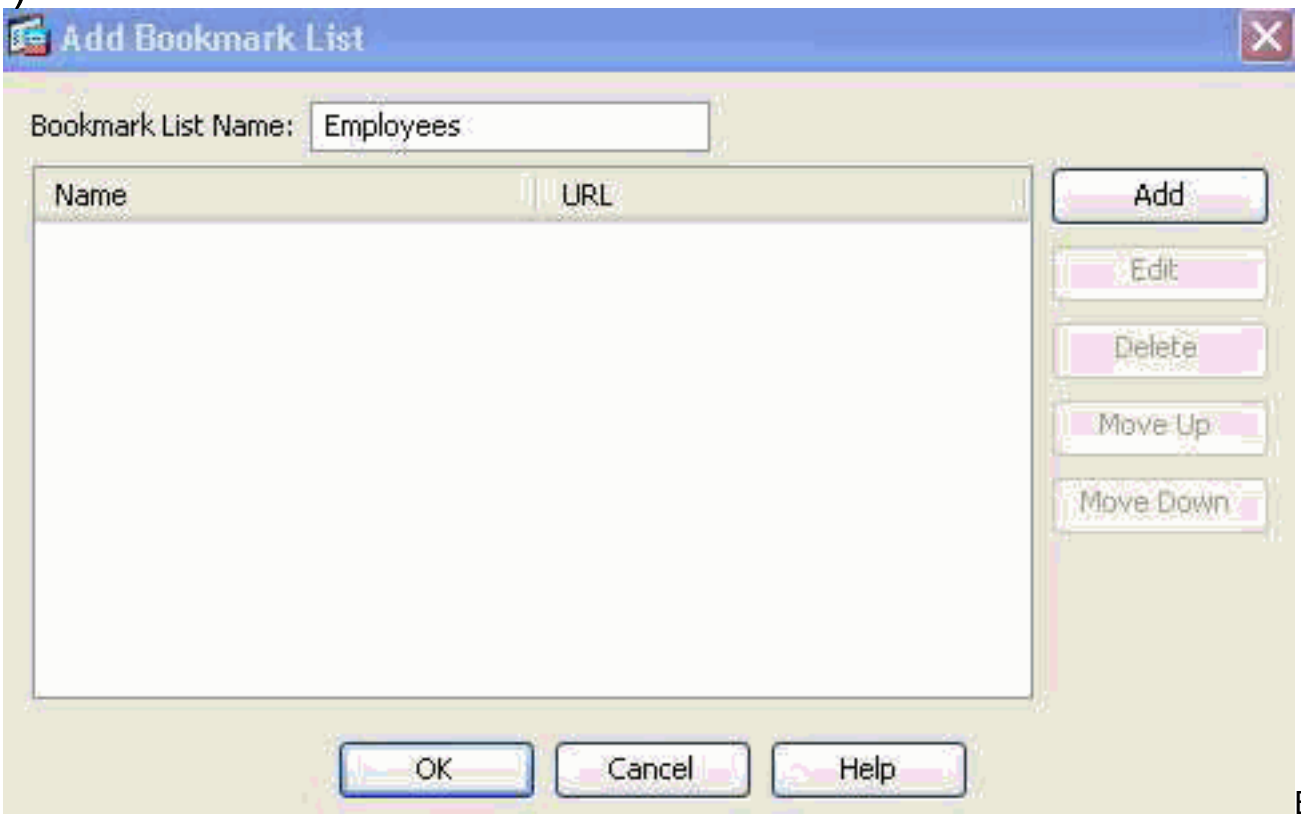
2. **导航到 Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles**，然后启用以下选项：**图 22.SSL VPN访问接口—定义了终止的SSL VPN连接接口。**



在 Access Interface 部分下，启用：**“Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the table below”**。还是在 Access Interfaces 部分下，选中外部接口上的 **Allow Access**。（此配置还将启用外部接口上的 SSL VPN 无客户端访问。)单击 **Apply**。

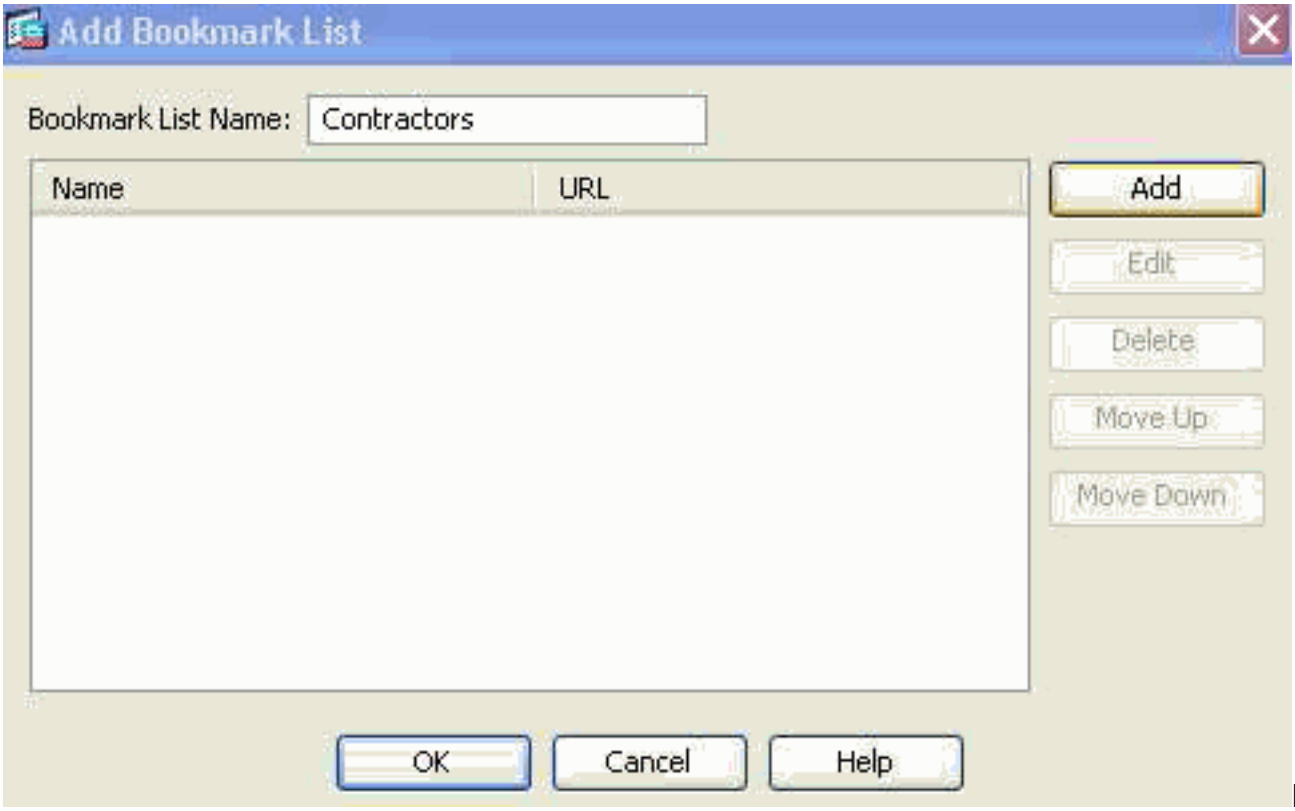
定义无客户端访问的书签列表（URL 列表）- 要定义将在门户上发布的基于 Web 的应用程序，必须进行此配置。我们将定义两个 URL 列表，一个用于员工，另一个用于承包商。

1. 导航到 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks**，单击 + Add 并进行以下配置：**图 23.书签列表 - 定义将发布在 Web 门户上供用户访问的 URL。（专为员工访问而定制。**
   ）



B
ookmark List Name：**Employees**，然后单击 Add。书签标题：**Company Intranet**URL 值：**http://company.resource.com**单击 **OK**，然后再次单击 OK。

2. 单击 **+ Add** 并配置第二个书签列表（URL 列表），如下所示：**图 24.书签列表 - 专为访客访问而定制。**

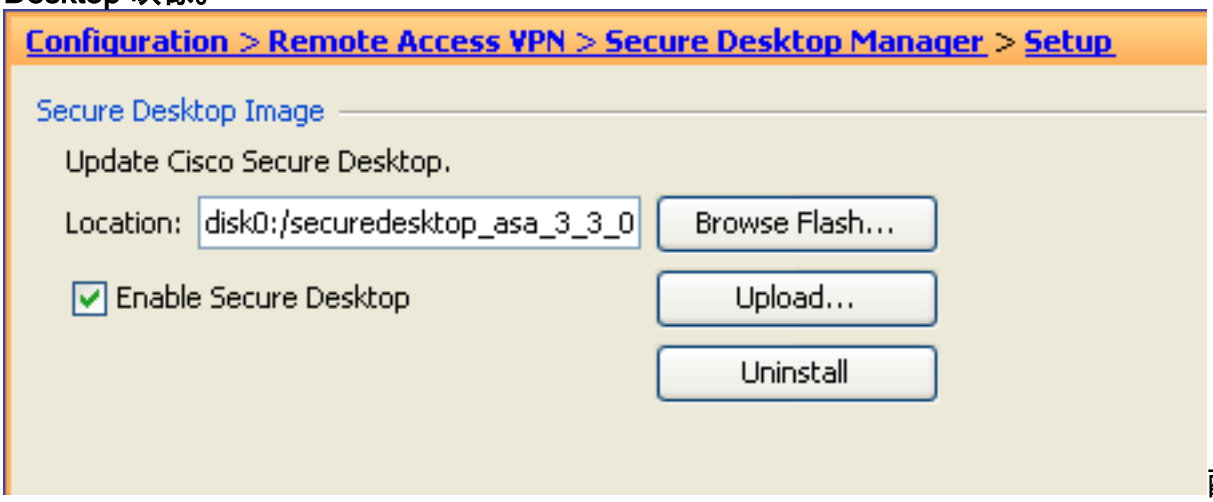


Bookmark List Name：**Contractors**，然后单击 Add。书签标题：**访客权限**URL 值：**http://company.contractors.com**单击 **OK**，然后再次单击 OK。单击 **Apply**。

Cisco Secure Desktop - 要定义终点评估属性，必须进行此配置。基于要满足的标准，连接终点将分为受管型或非受管型。Cisco Secure Desktop 评估将在身份验证过程之前执行。

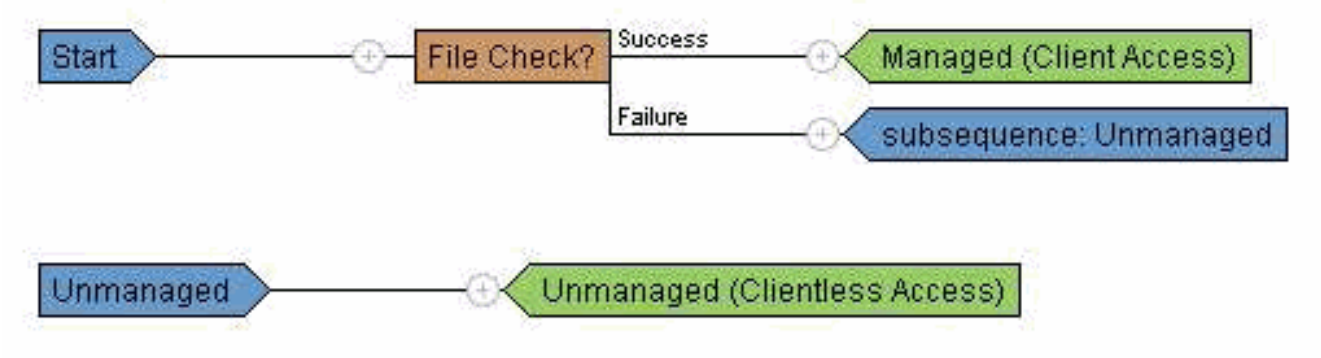
配置 Cisco Secure Desktop 和 Windows 位置的登录前决策树：

1. 导航到 **Configuration > Remote Access VPN > Secure Desktop Manager > Setup**，然后进行以下配置：**图 25.Cisco Secure Desktop 映像安装 - 定义将推送至连接终点的 Cisco Secure Desktop 映像。**



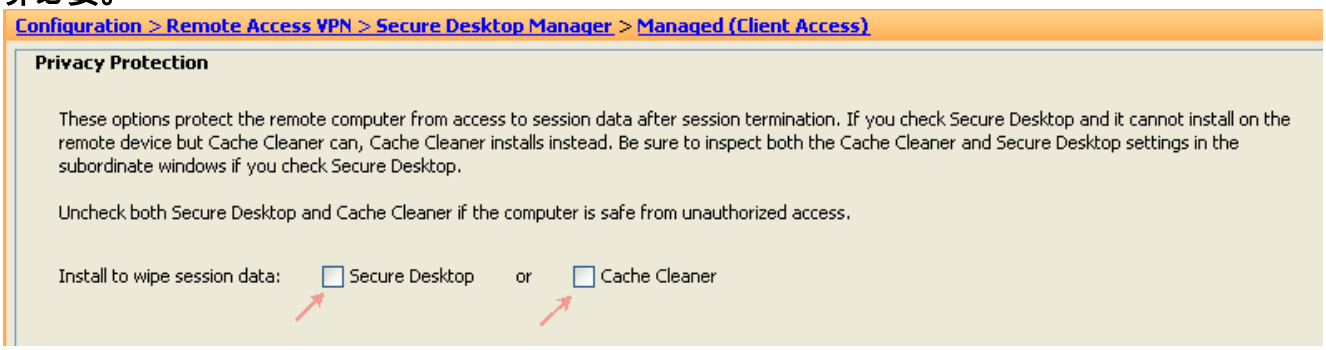
配置从 ASA闪存文件系统的**disk0:/securedesktop-asa-3.3.-xxx-k9.pkg**镜像。选中 **Enable Secure Desktop**。单击 **Apply**。

2. 导航到 **Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy**，然后进行以下配置：**图 26.登录前决策树 - 通过 File Check 进行定制，以区分受管型终点和非受管型终点。**



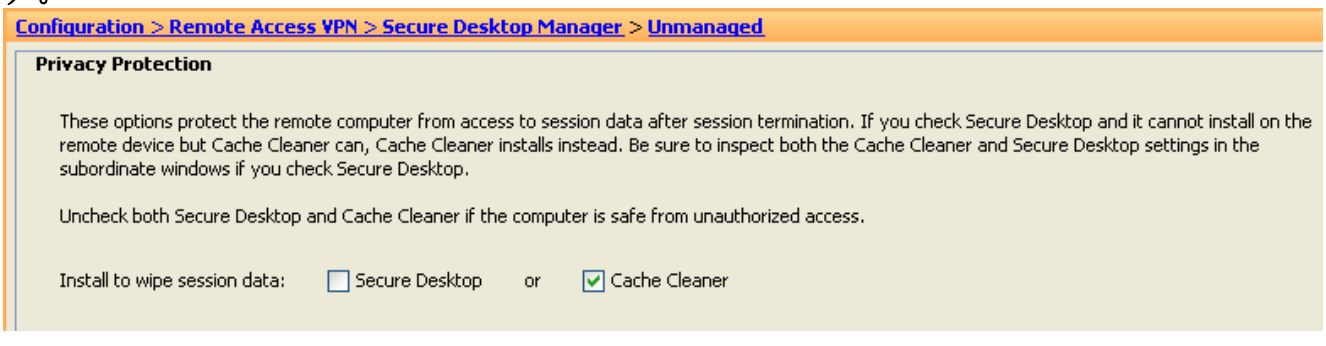
单击 **Default** 节点并将标签重命名为 Managed (Client Access)，然后单击 Update。单击 Managed 节点前面的“+”号。对于检查，请选择并添加要插入的 **File Check**。输入 **C:\managed.txt** 使文件路径存在，然后单击 Update。单击 **Login Denied** 节点，然后选择 Subsequence。为标签输入 **Unmanaged**，然后单击 Update。单击 **Login Denied** 节点，然后选择 Location。为标签输入 **Unmanaged (Clientless Access)**，然后单击 Update。单击 **Apply All**。

3. 导航到 **Configuration > Remote Access VPN > Secure Desktop Manager > Managed (Client Access)**，然后在 Location Settings 部分进行以下配置：**图 27.位置/隐私保护设置 - Secure Desktop（安全保管库）和 Cache Cleaner（浏览器清理）对基于客户端或网络的访问而言并非必要。**



位置模块：如果已启用 **Secure Desktop** 和 Cache Cleaner，请全部取消选中。如果需要，请单击 **Apply All**。

4. 导航到 **Configuration > Remote Access VPN > Secure Desktop Manager > Unmanaged (Clientless Access)**，然后在 Location Settings 部分进行以下配置：**图 28.位置设置 – 基于无客户端的访问需要缓存清理软件（浏览器清理），但不需要 Secure Desktop（安全保管库）。**

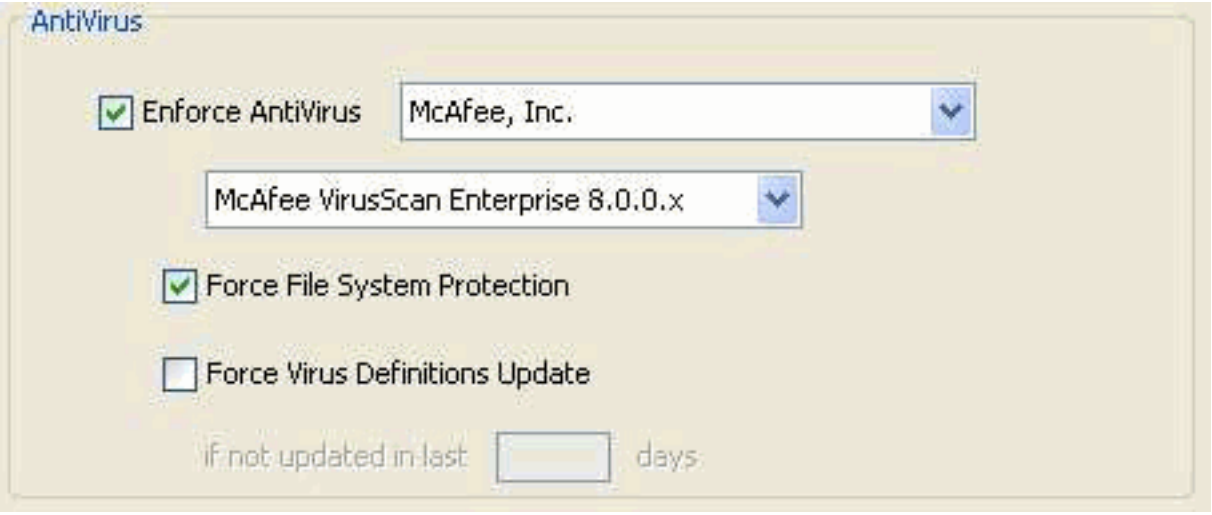


位置模块：取消选中 **Secure Desktop** 并选中 Cache Cleaner。单击 **Apply All**。

高级终点评估 - 要在终点上强制执行防病毒软件、防间谍软件和个人防火墙，必须进行此配置。例如，此评估将验证 McAfee 是否正在连接终点上运行。（高级终点评估是一项获得许可的功能，如果禁用了 Cisco Secure Desktop 功能，则无法配置该功能。）

导航到 **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan**，然后在 Host Scan Extensions 部分进行以下配置：

图 29.防病毒软件的强制执行 - 专为基于客户端或网络的访问而定制。



在 Host Scan Extensions 部分下，进行以下配置：

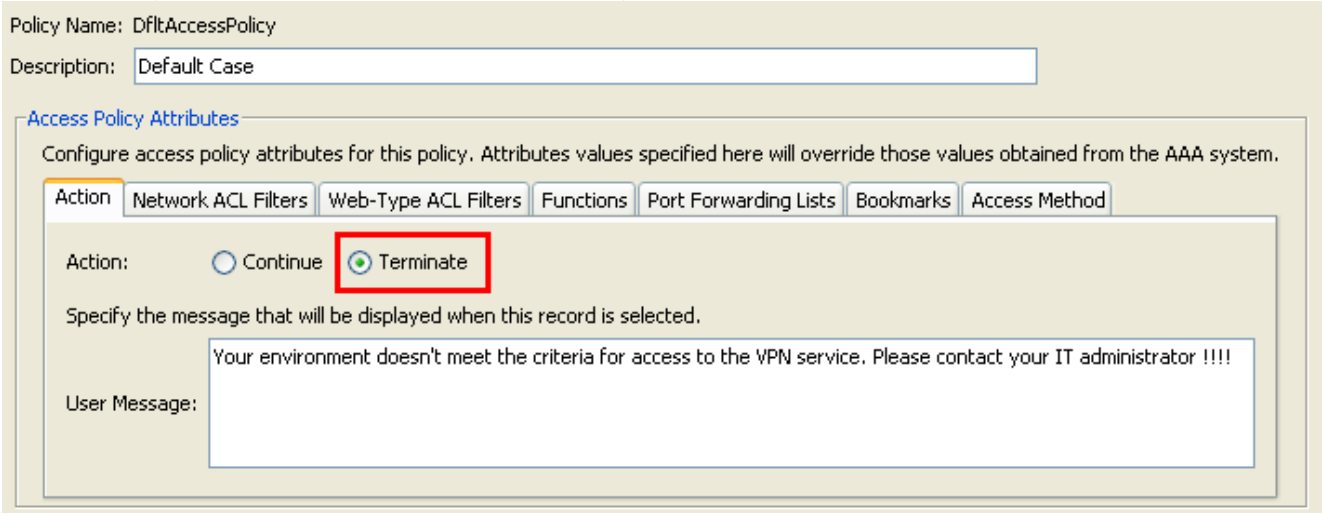
1. 选择 **Advanced Endpoint Assessment ver 2.3.3.1**，然后选择 Configure。
2. 选择 **Enforce AntiVirus**。
3. 从 Enforce AntiVirus 下拉列表中选择 **McAfee, Inc.**
4. 从 AntiVirus Version 下拉列表中选择 **McAfee VirusScan Enterprise 8.0.0.x**。
5. 选择 **Force File System Protection**，然后单击 Apply All。

动态访问策略 - 要根据定义的 AAA 和终点评估标准验证连接的用户及其终点，必须进行此配置。如果满足 DAP 记录的已定义标准，则将为连接的用户授予对 DAP 记录的关联网络资源的访问权限。DAP 授权在身份验证过程中执行。

为确保 SSL VPN 连接在默认情况下终止（例如，当终点不匹配任何配置的动态访问策略时），我们将进行以下配置：

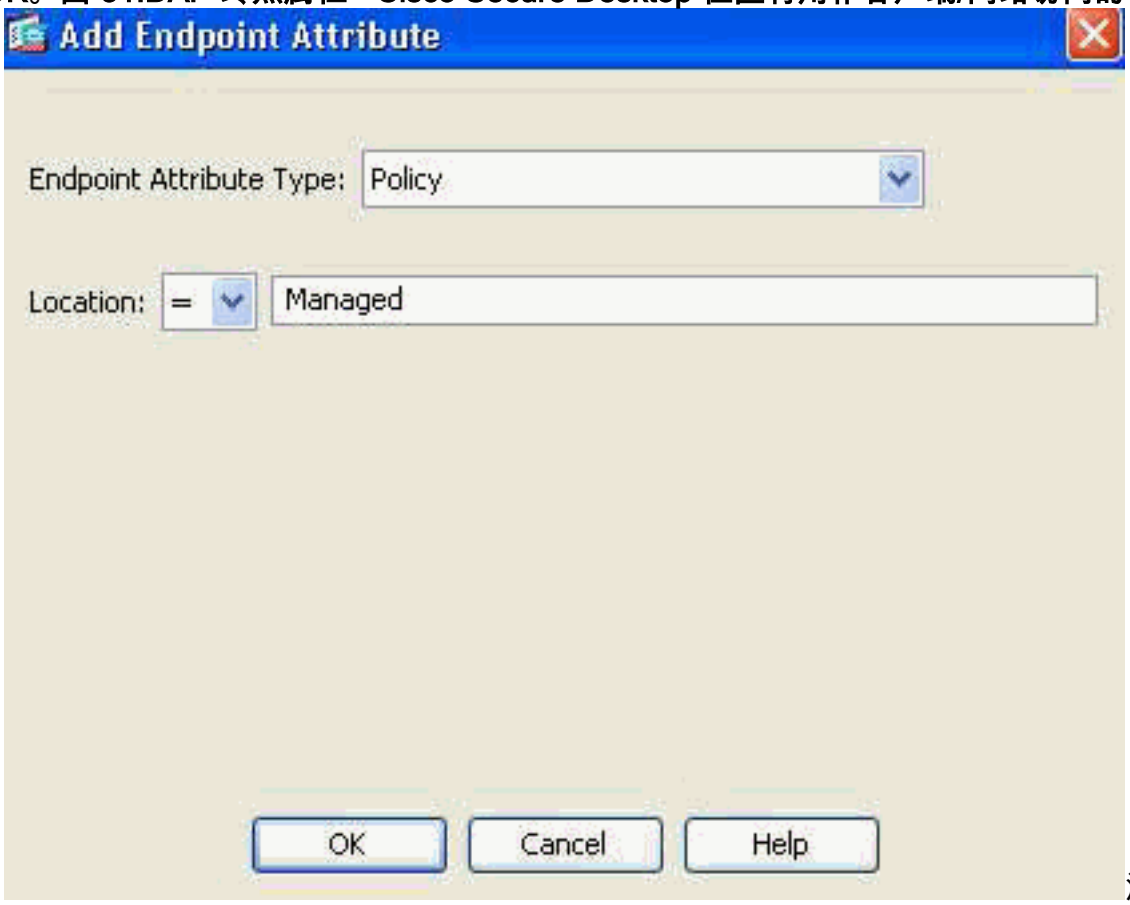
注意： 第一次配置动态访问策略时，将显示一条 DAP.xml 错误消息，指明 DAP 配置文件 (DAP.XML) 不存在。修改初始 DAP 配置并保存后，此消息将不再出现。

1. 导航到 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies**，然后进行以下配置：**图 30.默认动态访问策略 - 如果未能匹配任何预定义的 DAP 记录，则强制执行此 DAP 记录。因此，SSL VPN 访问将遭到拒绝。**

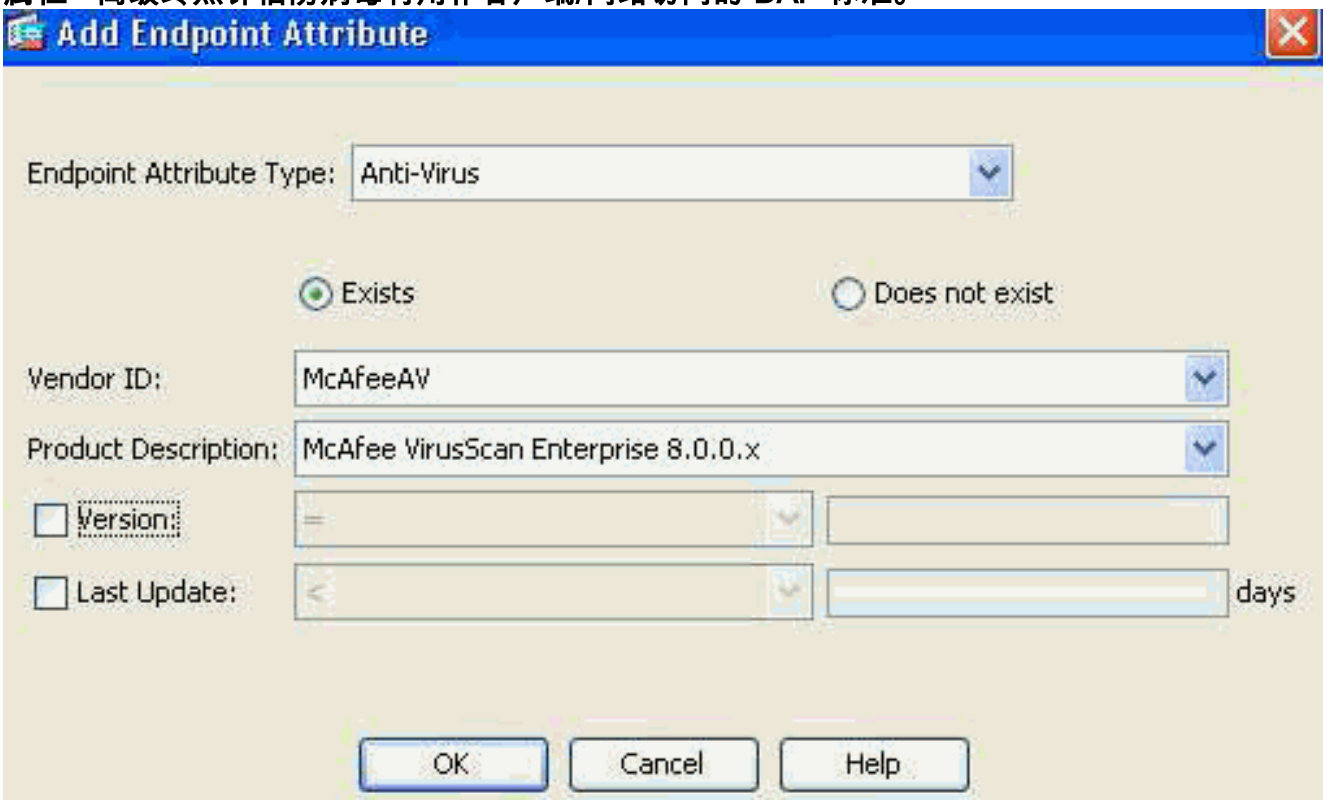


   编辑 **DfltAccessPolicy** 并将 Action 设置为 Terminate。单击 **Ok**。
2. 添加一个名为 **Managed_Endpoints** 的新动态访问策略，如下所示：说明：**Employee Client Access**添加(查找在终端Attribute type右边)一终端Attribute type (策略)如图31所显示。完成后

单击 OK。**图 31.DAP 终点属性 - Cisco Secure Desktop 位置将用作客户端/网络访问的 DAP 标准。**



添加第二个 Endpoint Attribute Type (Anti-Virus)，如图 32 所示。完成后单击 OK。**图 32.DAP 终点属性 - 高级终点评估防病毒将用作客户端/网络访问的 DAP 标准。**



从 AAA Attribute 部分上方的下拉列表中选择 **User has ALL of the following AAA Attributes Values...**添加（在 AAA Attribute 框右边）一个 AAA Attribute Type (LDAP)，如图 33 和 34 所示。完成后单击 OK。**图 33.DAP AAA 属性 - AAA 组成员资格将用作识别员工的 DAP 标准。**

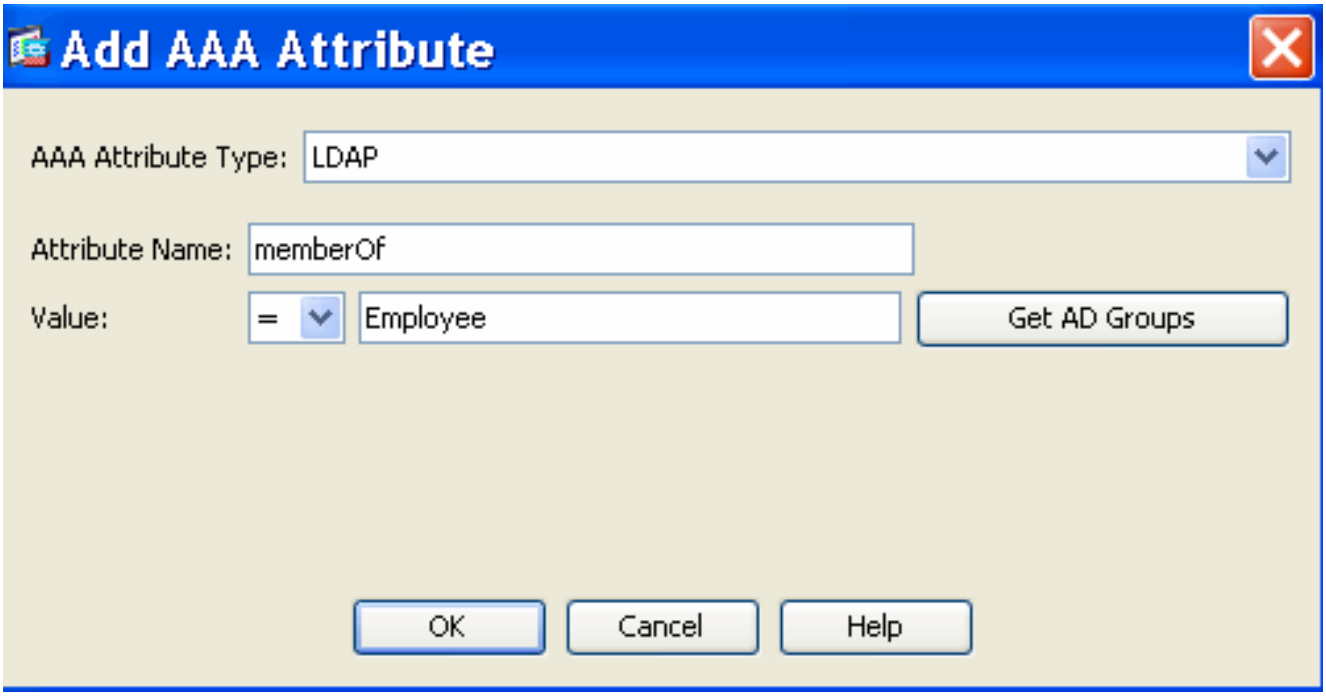
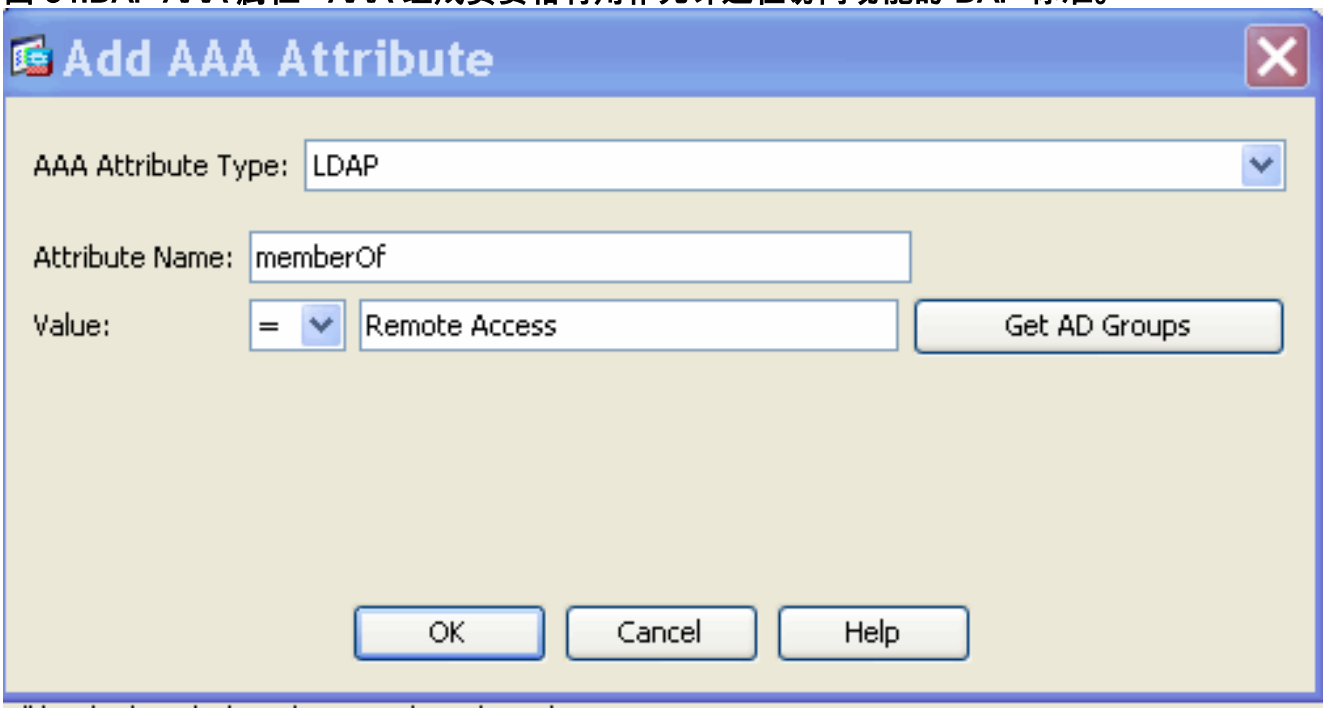
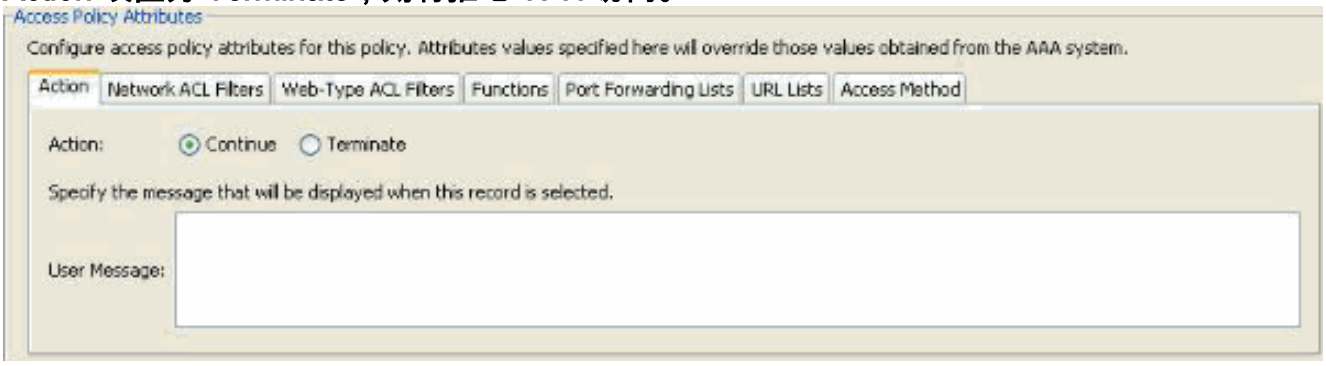


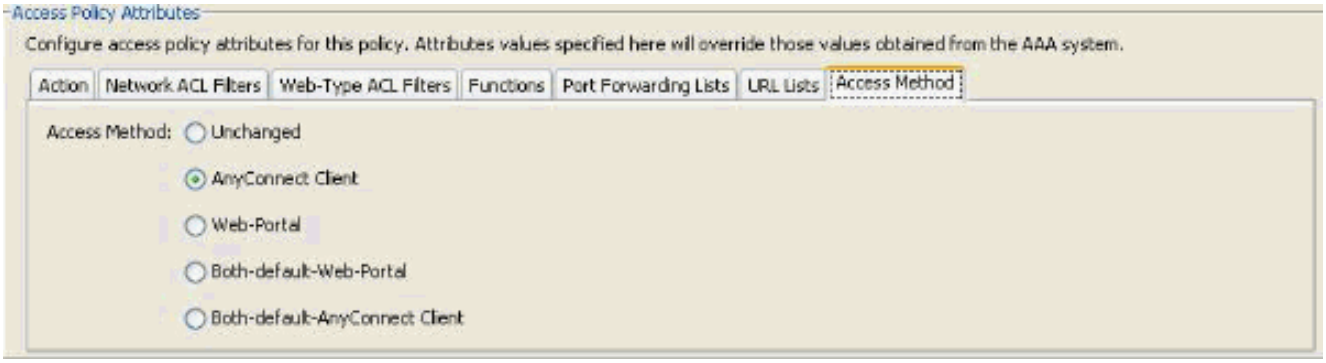
图 34.DAP AAA 属性 - AAA 组成员资格将用作允许远程访问功能的 DAP 标准。



在 Action 选项卡下，验证 Action 是否已设置为 **Continue**，如图 35 所示。**图 35.Action 选项卡 - 要为特定的连接或会话定义特殊处理，必须进行此配置。如果有匹配的 DAP 记录，并且 Action 设置为 Terminate，则将拒绝 VPN 访问。**



如图 36 所示，在 Access Method 选项卡下，选择 Access Method **AnyConnect Client**。**图 36.Access Method 选项卡 - 要定义 SSL VPN 客户端连接类型，必须进行此配置。**



单击 **OK**，然后单击 Apply

3. 添加第二个动态访问策略，名为 **Unmanaged_Endpoints**，如下所示：说明：**Employee Clientless Access**。添加（在 Endpoint Attribute 框右边）一个 Endpoint Attribute Type (Policy)，如图 37 所示。完成后单击 **OK**。**图 37.DAP 终点属性 - Cisco Secure Desktop 位置将用作无客户端访问的 DAP 标准。**

从 AAA Attribute 部分上方的下拉列表中选择 **User has ALL of the following AAA Attributes Values...**添加(查找在AAA Attribute type右边)一AAA Attribute type (LDAP)如图38和39所显示。完成后单击 **OK**。**图 38.DAP AAA 属性 - AAA 组成员资格将用作识别员工的 DAP 标准。**

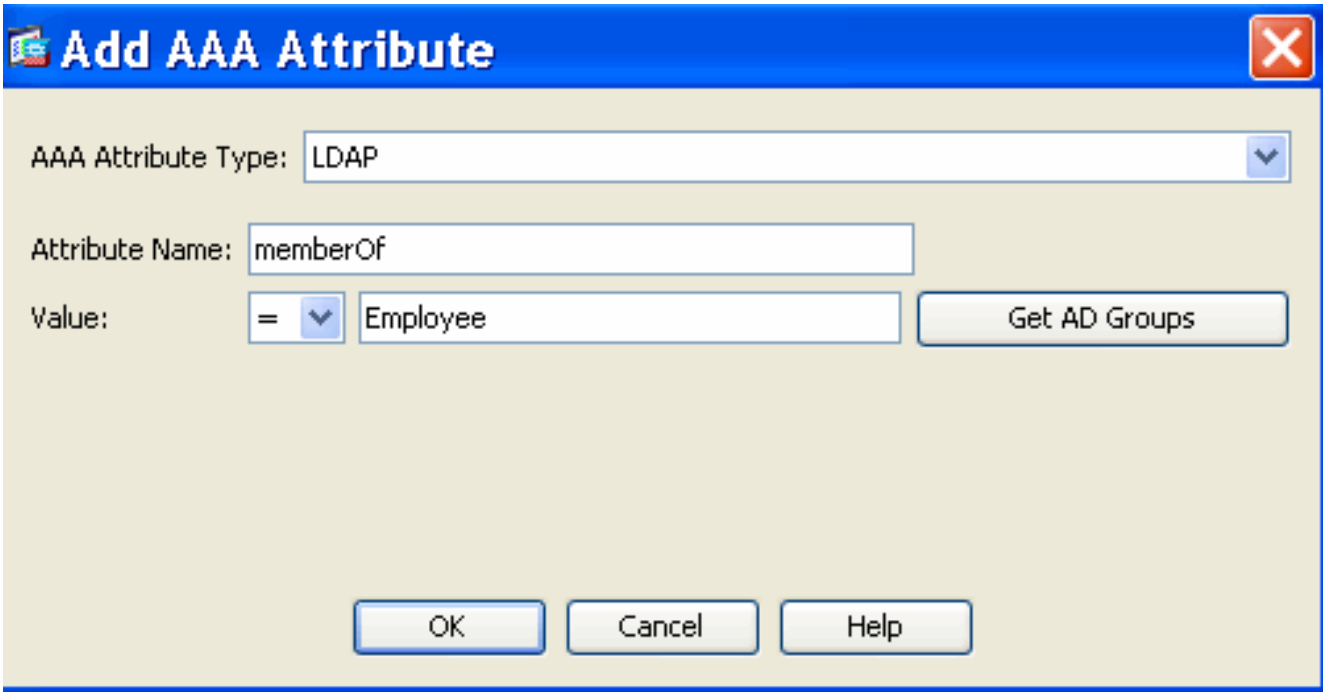
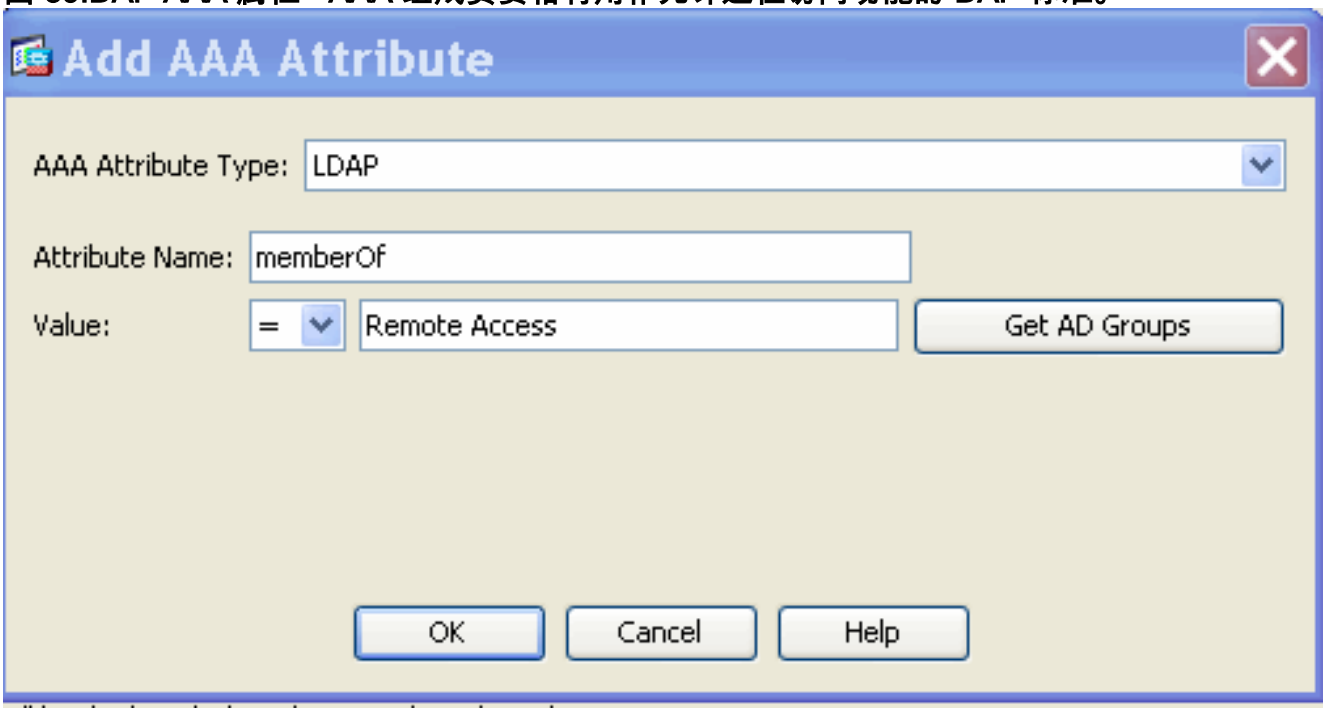
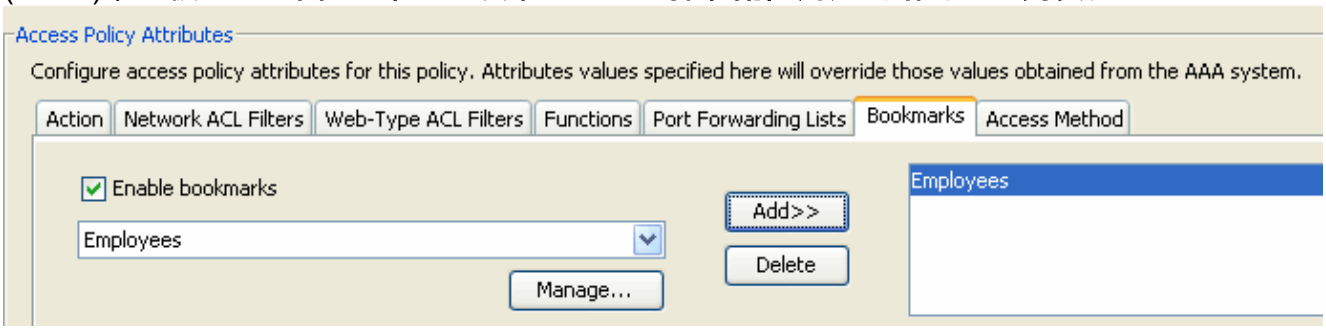


图 39.DAP AAA 属性 - AAA 组成员资格将用作允许远程访问功能的 DAP 标准。



在 Action 选项卡下，验证 Action 是否已设置为 **Continue**。（参考图 35。）在书签下请选中，选择从下拉式的列表名**员工**和然后单击**添加**。并且，请验证如图40所显示， Enable (event)书签被检查。**图 40.书签选项卡—让您选择和配置用户会话的URL列表。**



在 Access Method 选项卡下，选择 Access Method **Web-Portal**。（参考图 36。）单击 **OK**，然后单击 Apply将仅按 DAP AAA 属性识别承包商。结果，在步骤 4 中将不配置 Endpoint Attributes Type:(Policy)。此方法只用于显示 DAP 内的多功能性。

4. 添加第三个动态访问策略，名为 **Guest_Access**，并且具有以下配置：说明：**Guest Clientless Access**。添加（在 Endpoint Attribute 框右边）一个 Endpoint Attribute Type (Policy)，如图 37 所示。完成后单击 **OK**。从 AAA Attribute 部分上方的下拉列表中选择 **User has ALL of the following AAA Attributes Values...**添加（在 AAA Attribute 框右边）一个 AAA Attribute Type (LDAP)，如图 41 和 42 所示。完成后单击 **OK**。**图 41.DAP AAA 属性 - AAA 组成员资格将用作识别承包商的 DAP 标准。**

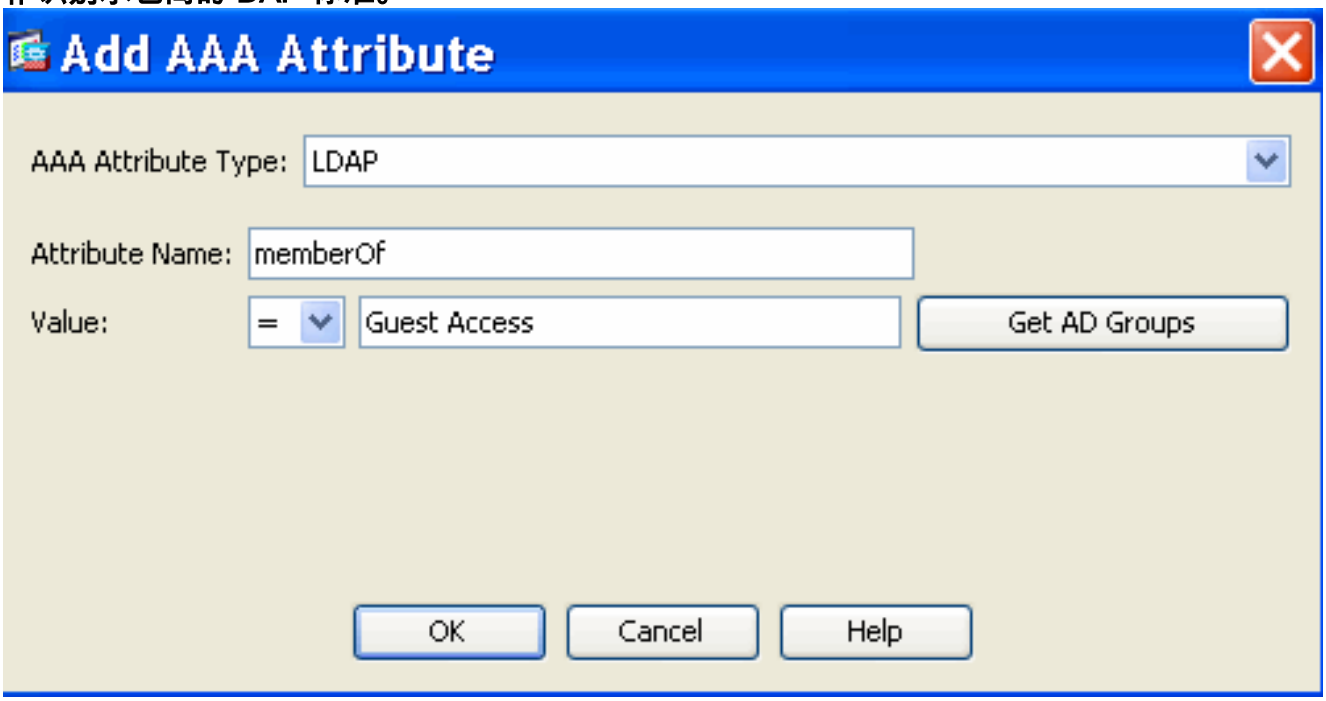
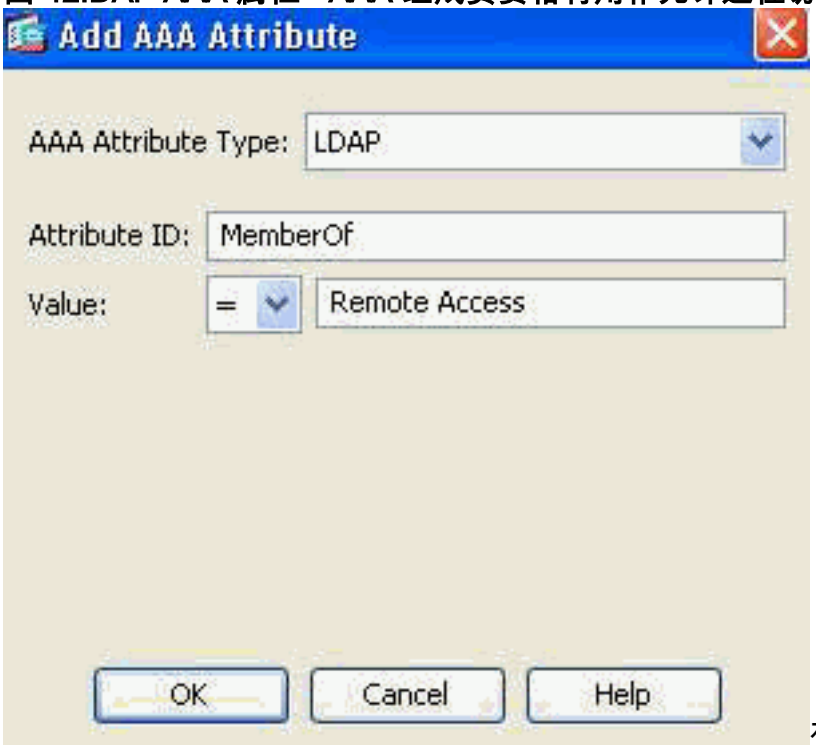


图 42.DAP AAA 属性 - AAA 组成员资格将用作允许远程访问功能的 DAP 标准。



在 Action 选项卡下，验证 Action 是否已设置为 **Continue**。（参考图 35。）在书签下请选中，选择从下拉式的列表名**承包商**和然后单击添加。并且，请验证**Enable (event)书签**被检查。（参考图 40。）在 Access Method 选项卡下，选择 Access Method **Web-Portal**。（参考图 36。）单击 **OK**，然后单击 Apply

DAP 选择标准 - 根据上述 DAP 配置步骤，所定义的 4 个 DAP 策略的 Selection Criteria 应该与图 43、44、45 和 46 一致。

图 43.受管型终点 - 如果满足此 DAP 记录的标准，员工将有权通过客户端/网络（AnyConnect 客户

端）连接访问公司资源。

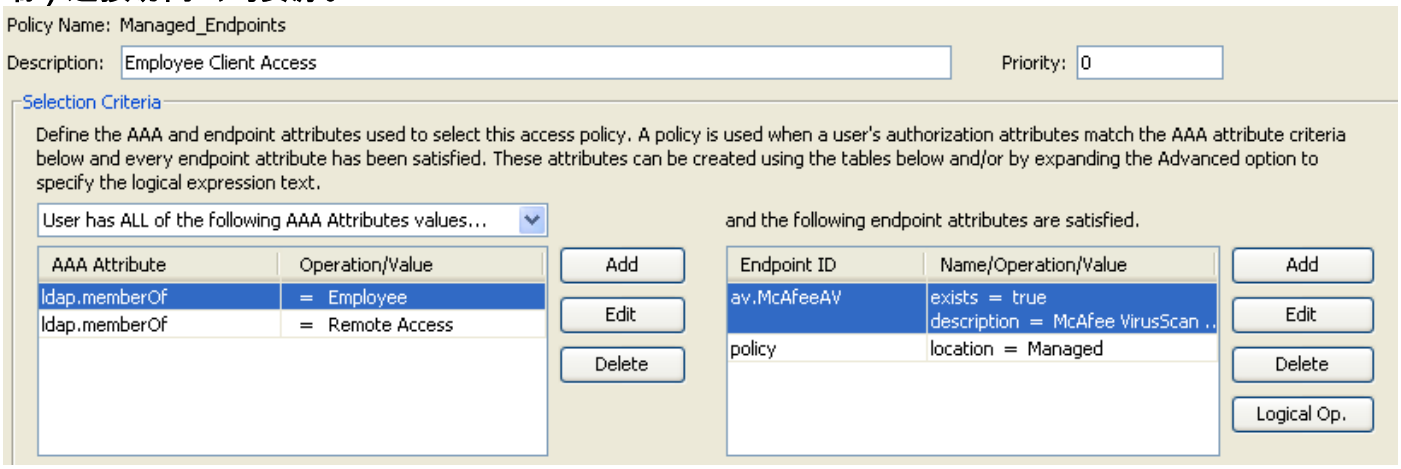


图 44.非受管型终点 - 如果满足此 DAP 记录的标准，员工将有权通过无客户端（门户）连接访问公司资源。员工的 URL 列表也适用于此策略。

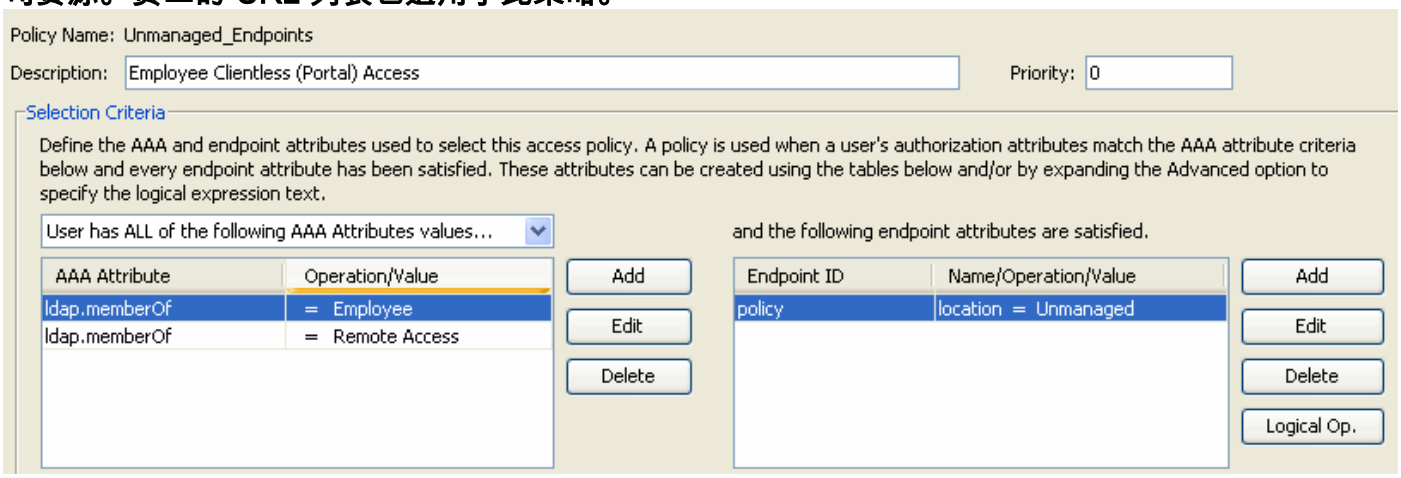


图 45.访客访问 - 如果满足此 DAP 记录的标准，承包商将有权通过无客户端（门户）连接访问公司资源。承包商的 URL 列表也适用于此策略。

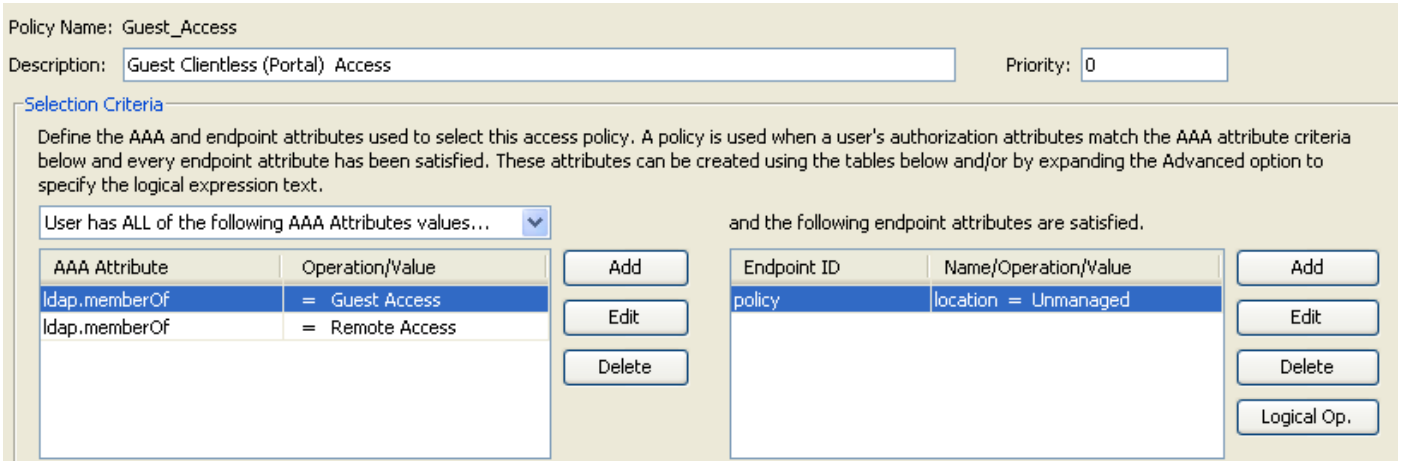
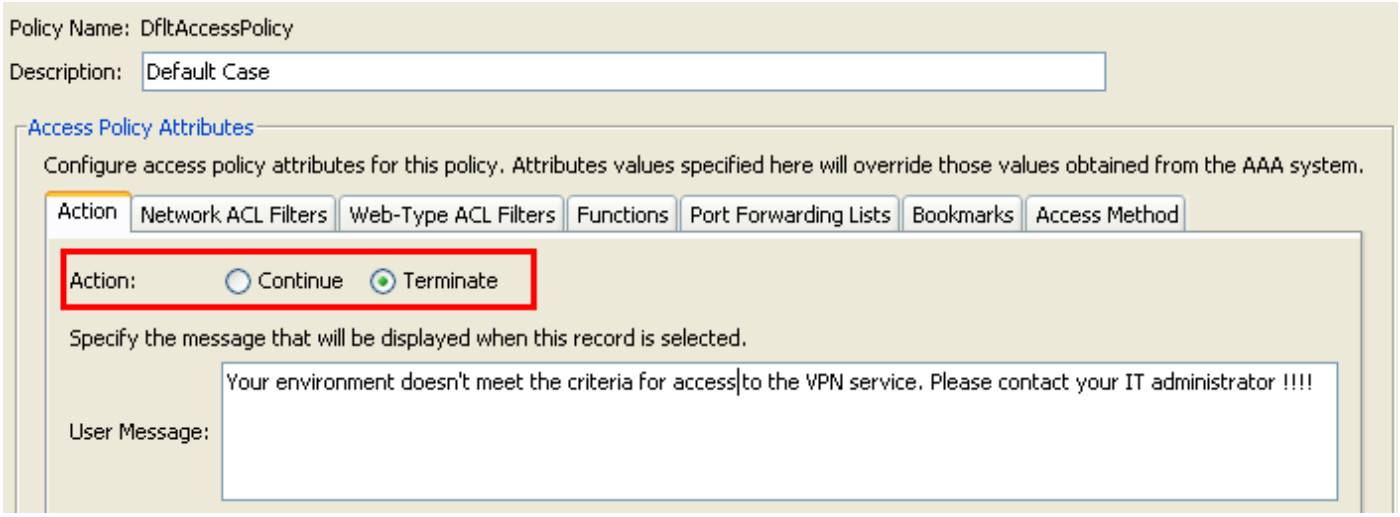


图 46.默认 DAP 策略 - 如果上述所有 DAP 记录的标准都无法满足，则默认情况下将拒绝员工和承包商的访问。



结论

根据本示例中讲述的客户的远程访问 SSL VPN 要求，此解决方案可满足其远程访问 VPN 要求。

随着不断演变的动态 VPN 环境持续合并，动态访问策略可以适应频繁的 Internet 配置更改、组织内每个用户可能具有的各种角色以及从具备不同配置和安全级别的受管型和非受管型远程访问站点发起的登录操作，并作出相应的扩展。

通过一些新技术和已得到验证的传统技术，包括高级终点评估、主机扫描、Secure Desktop、AAA 和本地访问策略，可对动态访问策略加以补充。这样，组织就可以放心地从任何位置提供对所有网络资源的安全 VPN 访问。

相关信息

- 技术支持和文档 - Cisco Systems