Deploy ASA 9.X Dynamic Access Policies (DAP)

Contents

Introduction

This document describes the deployment, features, and usage of ASA 9.x Dynamic access policies (DAP).

Prerequisites

Requirements

Cisco recommends that you know these topics:

- Virtual Private Network (VPN) gateways
- Dynamic access policies (DAP)

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Virtual Private Network (VPN) gateways operate in dynamic environments. Multiple variables can affect each VPN connection; for example, intranet configurations that frequently change, the various roles each user can inhabit within an organization, and logins from remote access sites with different configurations and levels of security. The task of authorizing users is much more complicated in a dynamic VPN environment than it is in a network with a static configuration.

Dynamic access policies (DAP), are a feature that enables you to configure authorization that addresses the dynamics of VPN environments. You create a dynamic access policy by setting a collection of access control attributes that you associate with a specific user tunnel or session. These attributes address issues of multiple group membership and endpoint security.

For example, the security appliance grants access to a particular user for a particular session based on the policies you define. It generates a DAP throughout user authentication by selecting and/or aggregating attributes from one or more DAP records. It selects these DAP records based on the endpoint security information of the remote device and/or AAA authorization information for the authenticated user. It then applies the DAP record to the user tunnel or session.

Note: The dap.xml file, which contains the DAP policies selection attributes, is stored in the ASA flash. Although you can export the dap.xml file off-box, edit it (if you know about XML syntax), and re-import it back, be very careful because you can cause ASDM to stop processing DAP records if you have misconfigured something. There is no CLI to manipulate this part of the configuration.

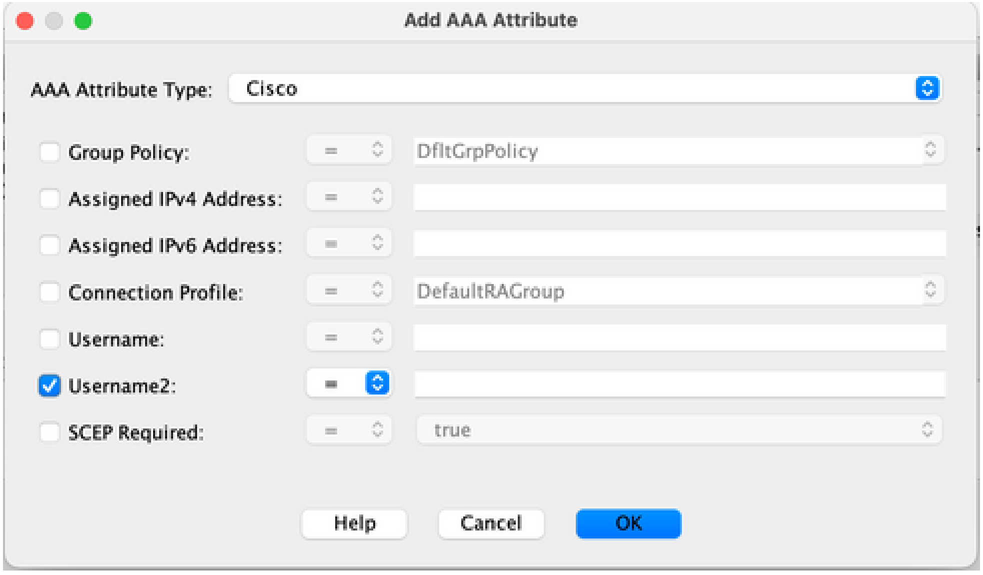
Note: Trying to configure the dynamic-access-policy-record access parameters via the CLI can cause DAP to stop working although ASDM would correctly manage the same. Avoid the CLI, and always use ASDM to manage DAP policies.

DAP and AAA Attributes

DAP complements AAA services and provides a limited set of authorization attributes that can override attributes that AAA provides. The security appliance can select DAP records based on the AAA authorization information for the user. The security appliance can select multiple DAP records depending on this information, which it then aggregates to assign DAP authorization attributes.

You can specify AAA attributes from the Cisco AAA attribute hierarchy, or from the full set of response attributes that the security appliance receives from a RADIUS or LDAP server as shown in Figure 1.

Figure 1. DAP AAA Attribute GUI



Add AAA Attribute

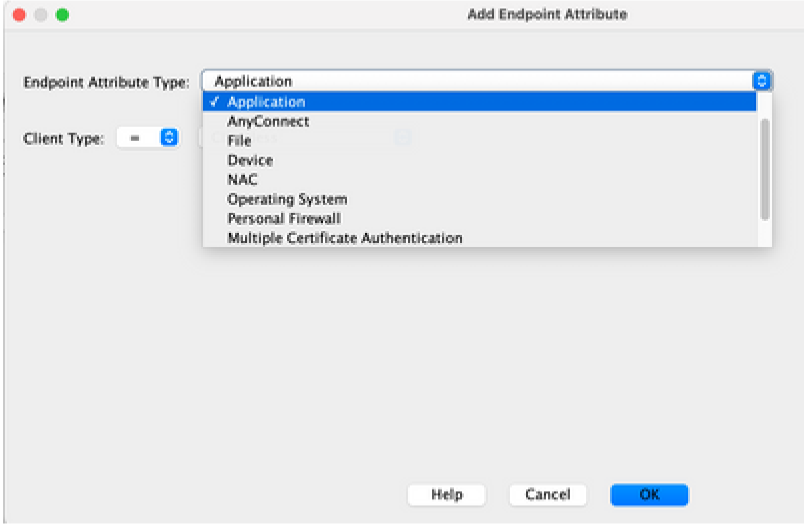
AAA Attribute Type: Cisco

□ Group Policy: = DfltGrpPolicy
□ Assigned IPv4 Address: =
□ Assigned IPv6 Address: =
□ Connection Profile: = DefaultRAGroup
□ Username: =
☑ Username2: =
□ SCEP Required: = true

DAP and Endpoint Security Attributes

In addition to AAA attributes, the security appliance can also obtain endpoint security attributes by using the posture assessment methods that you configure. These include Basic Host Scan, Secure Desktop, Standard/Advanced Endpoint Assessment, and NAC as shown in Figure 2. Endpoint Assessment Attributes are obtained and sent to the security appliance before user authentication. However, AAA Attributes, including the overall DAP record, are validated during user authentication.

Figure 2. Endpoint Attribute GUI



Endpoint Attribute Type: Application

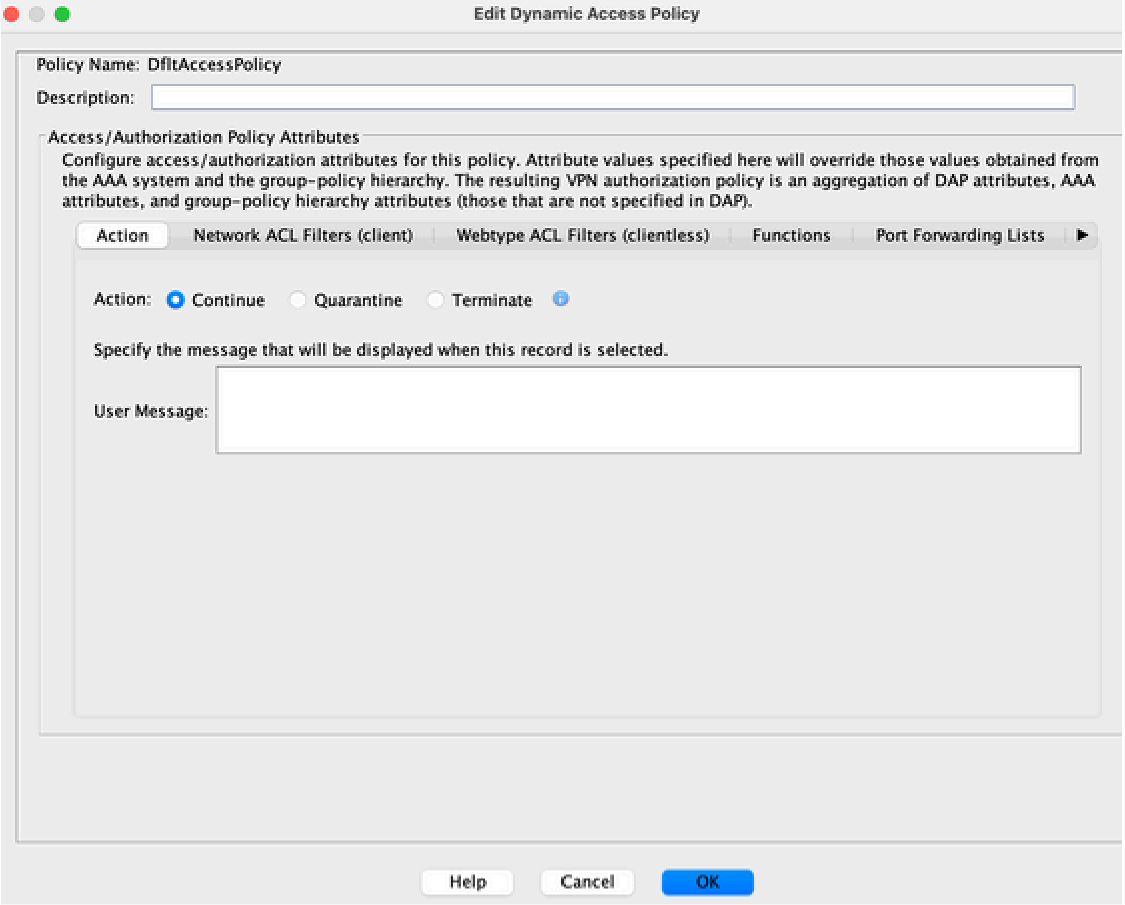
Client Type: =

Default Dynamic Access Policy

Before the introduction and implementation of DAP, access policy attribute/value pairs that were associated with a specific user tunnel or session were defined either locally on the ASA, (that is, Tunnel Groups and Group Policies) or mapped via external AAA servers.

DAP is always enforced by default. For example, enforcing access control via Tunnel Groups, Group Policies, and AAA without the explicit enforcement of DAP can still obtain this behavior. For legacy behavior, no configuration changes to the DAP feature, including the default DAP record, **DfltAccessPolicy**, are required as shown in Figure 3.

Figure 3. Default Dynamic Access Policy


Edit Dynamic Access Policy

Policy Name: DfltAccessPolicy

Description:

Access/Authorization Policy Attributes

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Action
Network ACL Filters (client)
Webtype ACL Filters (clientless)
Functions
Port Forwarding Lists

Action: ● Continue ○ Quarantine ○ Terminate

Specify the message that will be displayed when this record is selected.

User Message:

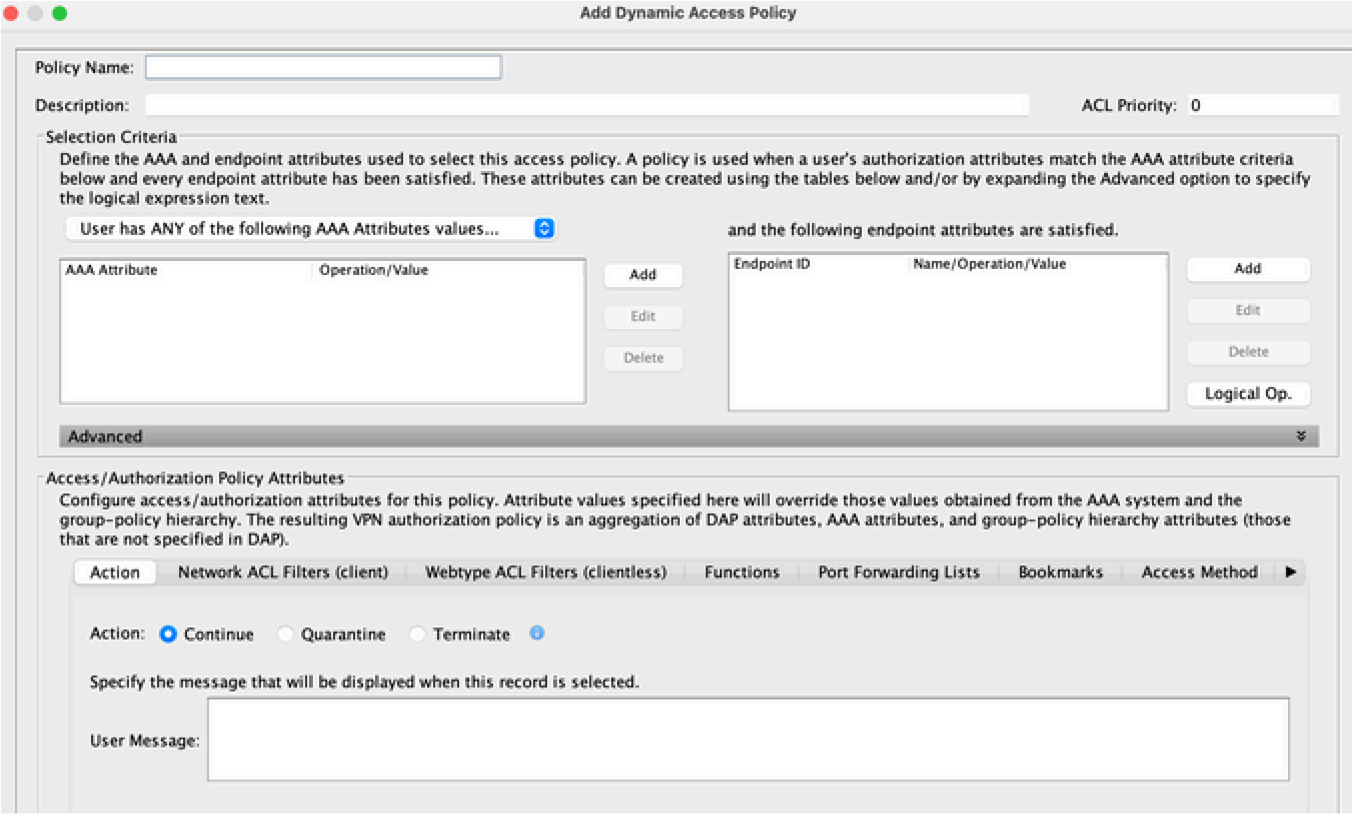
Nevertheless, if any of the default values in a DAP record are changed, for example, the **Action:** parameter in the **DfltAccessPolicy** is changed from its default value to Terminate and additional DAP records are not configured, authenticated users can, by default, match the **DfltAccessPolicy** DAP record and can be denied VPN access.

Consequently, one or more DAP records need to be created and configured to authorize VPN connectivity and define which network resources an authenticated user is authorized to access. Thus, DAP, if configured, can take precedence over legacy policy enforcement.

Configure Dynamic Access Policies

When you use DAP to define which network resources a user has access to, there are many parameters to consider. For example, if you identify whether the connecting endpoint is from a managed, unmanaged, or untrusted environment, determine the selection criteria necessary to identify the connecting endpoint, and based on endpoint assessment and/or AAA credentials, which network resources the user who connects is authorized to access. To accomplish this, you must first become familiar with DAP features and functions as shown in Figure 4.

Figure 4. Dynamic Access Policy


Add Dynamic Access Policy

Policy Name:

Description:

ACL Priority: 0

Selection Criteria

Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ANY of the following AAA Attributes values...

and the following endpoint attributes are satisfied.

AAA Attribute	Operation/Value

Endpoint ID	Name/Operation/Value

Access/Authorization Policy Attributes

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Action
Network ACL Filters (client)
Webtype ACL Filters (clientless)
Functions
Port Forwarding Lists
Bookmarks
Access Method

Action: ● Continue ○ Quarantine ○ Terminate

Specify the message that will be displayed when this record is selected.

User Message:

When configuring a DAP record, there are two major components to consider:

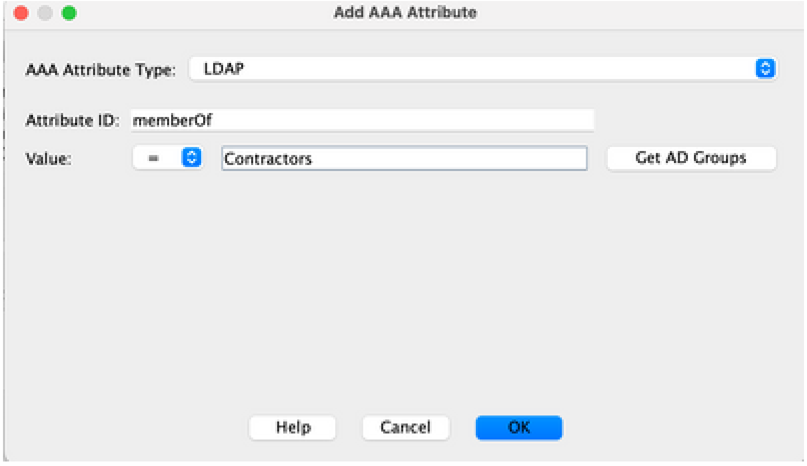
- Selection Criteria including Advanced Options
- Access Policy Attributes

The Selection Criteria section is where an administrator would configure AAA and Endpoint attributes used to select a specific DAP record. A DAP record is used when a userâ€™s authorization attributes match the AAA attribute criteria and every endpoint attribute has been satisfied.

For example, if the AAA Attribute Type LDAP (Active Directory) is selected, the Attribute Name string is **memberOf** and the Value string is Contractors, as shown in Figure 5a, the authenticating user must be a member of the Active Directory group Contractors to match the AAA attribute criteria.

In addition to satisfying the AAA attribute criteria, the authenticating user can also be required to satisfy the endpoint attribute criteria. For example, if the administrator configured to determine the posture of the connecting endpoint and based on that posture assessment, the administrator could then use this assessment information as selection criteria for the endpoint attribute shown in Figure 5b.

Figure 5a. AAA Attribute Criteria

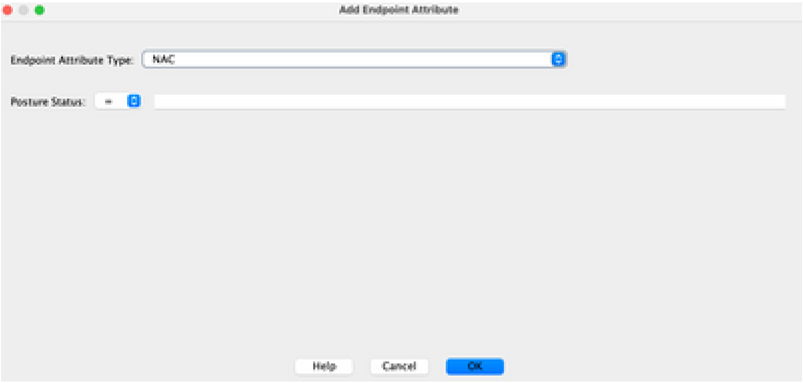


AAA Attribute Type: LDAP

Attribute ID: memberOf

Value: = Contractors

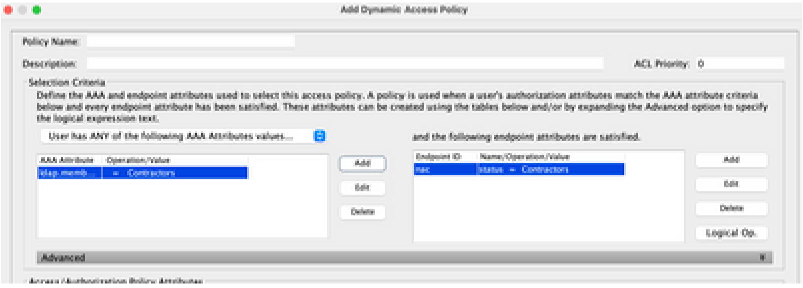
Figure 5b. Endpoint Attribute Criteria



Endpoint Attribute Type: NAC

Posture Status: =

Figure 6. AAA and Endpoint Attribute Criteria Match



Policy Name:

Description:

ACL Priority: 0

Selection Criteria

Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ANY of the following AAA Attributes values...

AAA Attribute	Operation/Value
ldap.memb...	= Contractors

and the following endpoint attributes are satisfied.

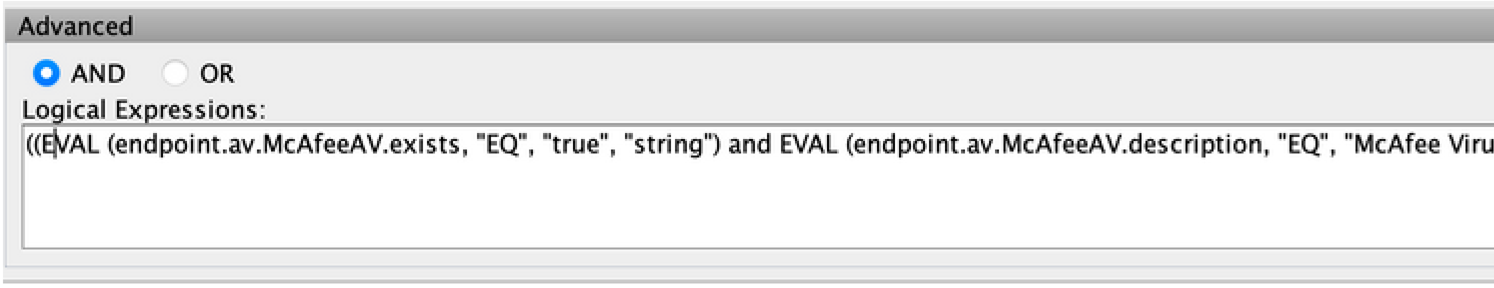
Endpoint ID	Name/Operation/Value
nac	status = Contractors

Access/Authorization Policy Attributes

AAA and Endpoint attributes can be created using the tables as described in Figure 6 and/or by expanding the Advanced option to specify a logical expression as shown in Figure 7. Currently, the logical expression is constructed with EVAL functions, for example, EVAL (endpoint.av.McAfeeAV.exists, "EQ", "true", "string") and EVAL (endpoint.av.McAfeeAV.description, "EQ", "McAfee VirusScan Enterprise", "string"), that represent AAA and/or endpoint selection logical operations.

Logical Expressions are useful if you need to add selection criteria other than what is possible in the AAA and endpoint attribute areas as shown previously. For example, while you can configure the security appliances to use AAA attributes that satisfy any, all, or none of the specified criteria, endpoint attributes are cumulative, and must all be satisfied. To let the security appliance employ one endpoint attribute or another, you need to create appropriate logical expressions under the Advanced section of the DAP record.

Figure 7. Logical Expression GUI for Advanced Attribute creation



Advanced

● AND ○ OR

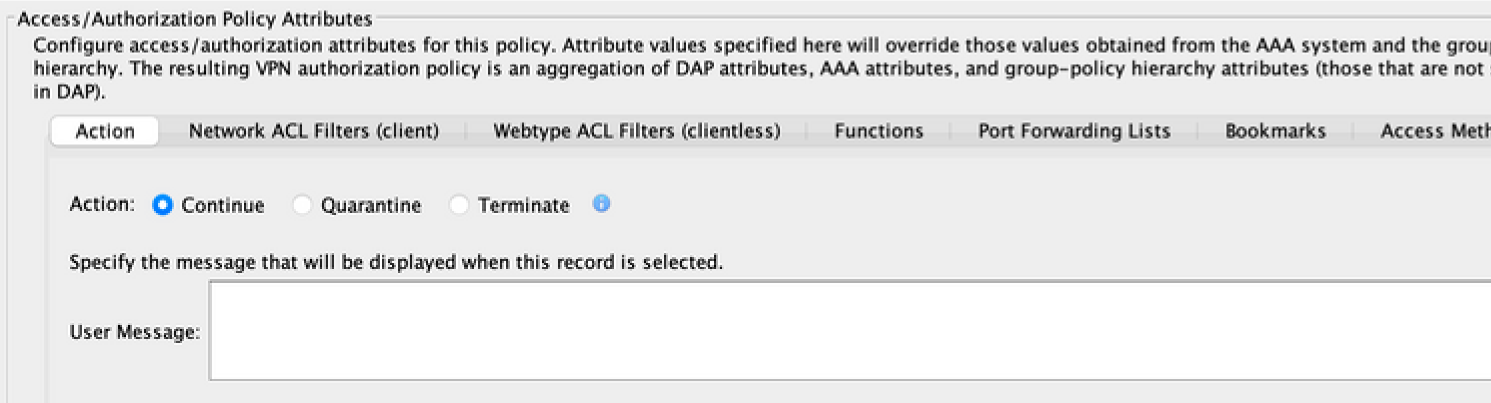
Logical Expressions:

```
((EVAL (endpoint.av.McAfeeAV.exists, "EQ", "true", "string") and EVAL (endpoint.av.McAfeeAV.description, "EQ", "McAfee Viru
```

The Access Policy Attributes section as shown in Figure 8 is where an administrator would configure VPN access attributes for a specific DAP record. When a user authorization attributes match the AAA, Endpoint, and/or Logical Expression criteria; the configured access policy attribute values in this section can be enforced. Attribute values specified here can override those values obtained from the AAA system, including those in existing user, group, tunnel group, and default group records.

A DAP record has a limited set of attribute values that can be configured. These values fall under the tabs as shown in Figures 8 through 14:

Figure 8. Action â€" Specifies special processing to apply to a specific connection or session.



Access/Authorization Policy Attributes

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the grou hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not in DAP).

Action
Network ACL Filters (client)
Webtype ACL Filters (clientless)
Functions
Port Forwarding Lists
Bookmarks
Access Meth

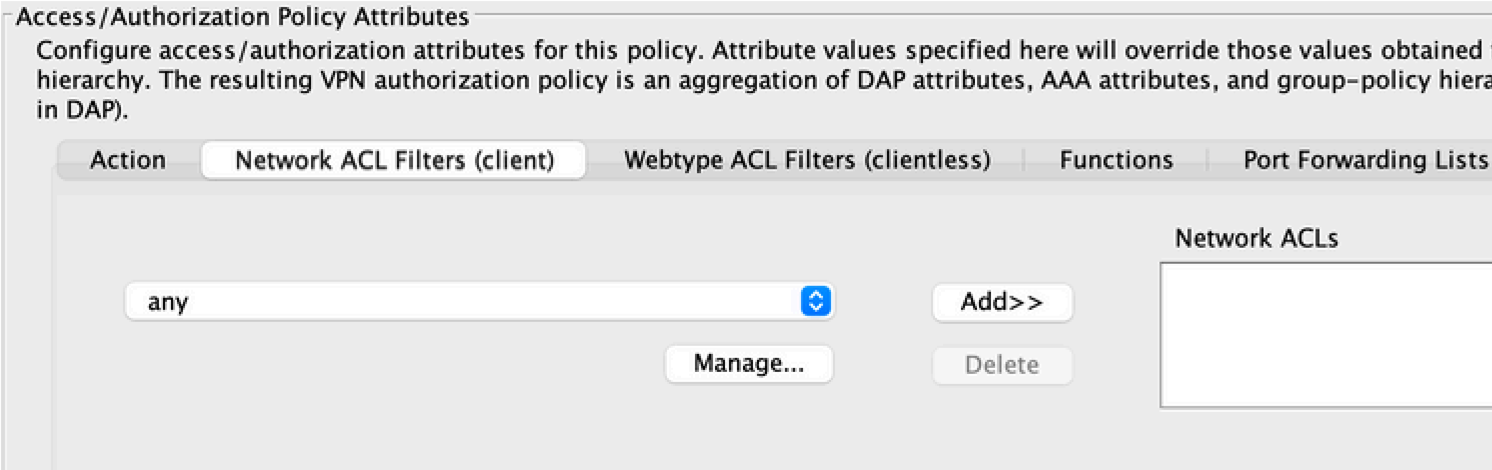
Action: ● Continue ○ Quarantine ○ Terminate

Specify the message that will be displayed when this record is selected.

User Message:

- **Continueâ€"**(default) Click to apply access policy attributes to the session.
- **Terminateâ€"Click** to terminate the session.
- **User Messageâ€"Enter** a text message to display on the portal page when this DAP record is selected. Maximum 128 characters. A user message displays as a yellow orb. When a user logs on, it blinks three times to attract attention, and then it is still. If several DAP records are selected, and each of them has a user message, all of the user messages display. Additionally, you can include in such messages URLs or other embedded text, which require that you use the correct HTML tags.

Figure 9. Network ACL Filters Tab â€" This lets you select and configure network ACLs to apply to this DAP record. An ACL for DAP can contain permit or deny rules, but not both. If an ACL contains both permit and deny rules, the security appliance rejects the ACL configuration.



Access/Authorization Policy Attributes

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hiera in DAP).

- **Network ACL drop-down box** already configured network ACLs to add to this DAP record. Only ACLs that have all permit or deny rules are eligible, and these are the only ACLs that display here.

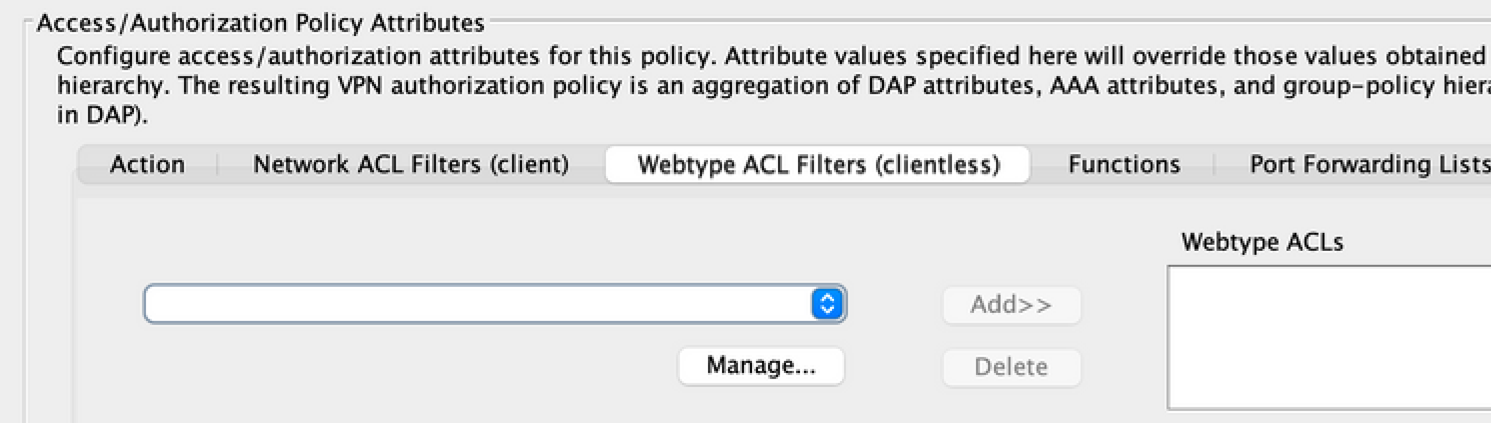
- **Manageâ€”Click** to add, edit, and delete network ACLs.

- **Network ACL lists** the network ACLs for this DAP record.

- **Addâ€”Click t**o add the selected network ACL from the drop-down box to the Network ACLs list on the right.

- **Deleteâ€”Click t**o delete a highlighted network ACL from the Network ACLs list. You cannot delete an ACL if it is assigned to a DAP or other record.

Figure 10. Web-Type ACL Filters Tab â€” This lets you select and configure web-type ACLs to apply to this DAP record. An ACL for DAP can contain only permit or deny rules. If an ACL contains both permit and deny rules, the security appliance rejects the ACL configuration.



Access/Authorization Policy Attributes

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hiera in DAP).

- **Web-Type ACL drop-down box** â€” Select already configured web-type ACLs to add to this DAP record. Only ACLs having all permit or all deny rules are eligible, and these are the only ACLs that display here.

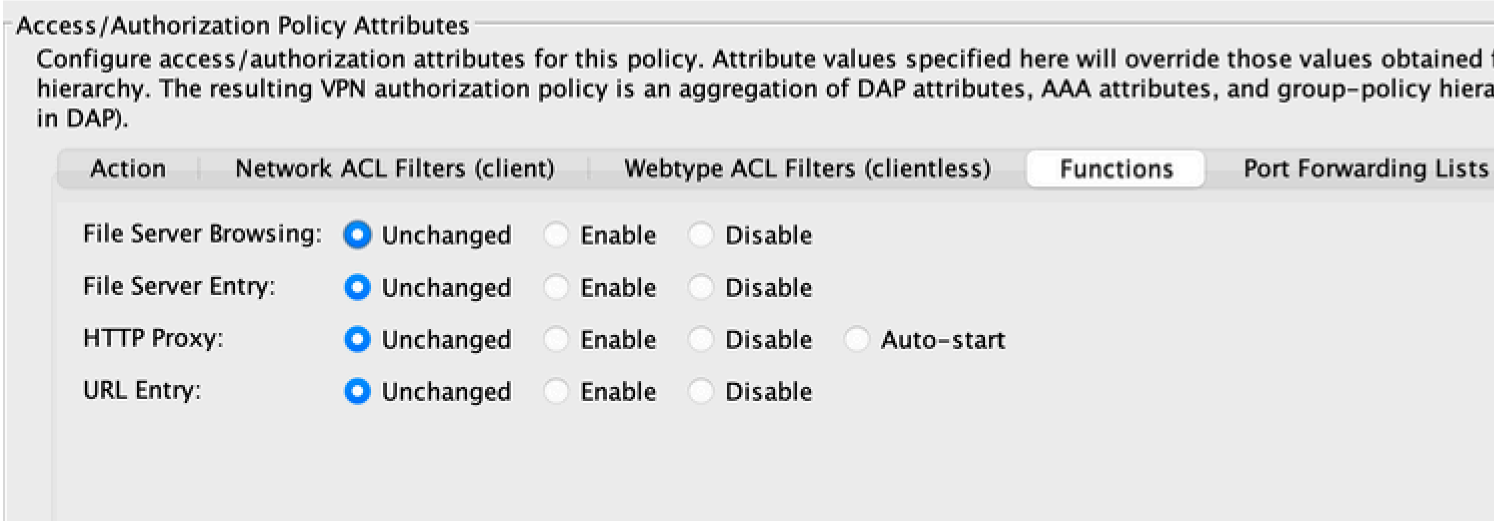
- **Manage...** â€” Click to add, edit, and delete web-type ACLs.

- **Web-Type ACL list** â€”Displays the web-type ACLs for this DAP record.

- Add â€—Click to add the selected web-type ACL from the drop-down box to the Web-Type ACLs list on the right.

- Delete â€”Click to delete a web-type ACL from the Web-Type ACLs list. You cannot delete an ACL if it is assigned to a DAP or other record.

Figure 11. Functions Tab â€” This lets you configure file server entry and browsing, HTTP proxy, and URL entry for the DAP record.



Access/Authorization Policy Attributes

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained f hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hiera in DAP).

Action
Network ACL Filters (client)
Webtype ACL Filters (clientless)
Functions
Port Forwarding Lists

File Server Browsing: ● Unchanged ○ Enable ○ Disable

File Server Entry: ● Unchanged ○ Enable ○ Disable

HTTP Proxy: ● Unchanged ○ Enable ○ Disable ○ Auto-start

URL Entry: ● Unchanged ○ Enable ○ Disable

- File Server Browsingâ€”Enables or disables CIFS browsing for file servers or share features.

- File Server Entryâ€”Allows or denies a user from entering file server paths and names on the portal page. When enabled, places the file server entry drawer on the portal page. Users can enter pathnames to Windows files directly. They can download, edit, delete, rename, and move files. They can also add files and folders. Shares must also be configured for user access on the applicable Microsoft Windows servers. Users can be required to authenticate before accessing files, depending on network requirements.

- HTTP Proxyâ€”Affects the forwarding of an HTTP applet proxy to the client. The proxy is useful for technologies that interfere with proper content transformation, such as Java, ActiveX, and Flash. It bypasses the mangling/rewriting process while ensuring the continued use of the security appliance. The forwarded proxy modifies the browserâ€™s old proxy configuration automatically and redirects all HTTP and HTTPS requests to the new proxy configuration. It supports virtually all client-side technologies, including HTML, CSS, JavaScript, VBScript, ActiveX, and Java. The only browser it supports is Microsoft Internet Explorer.

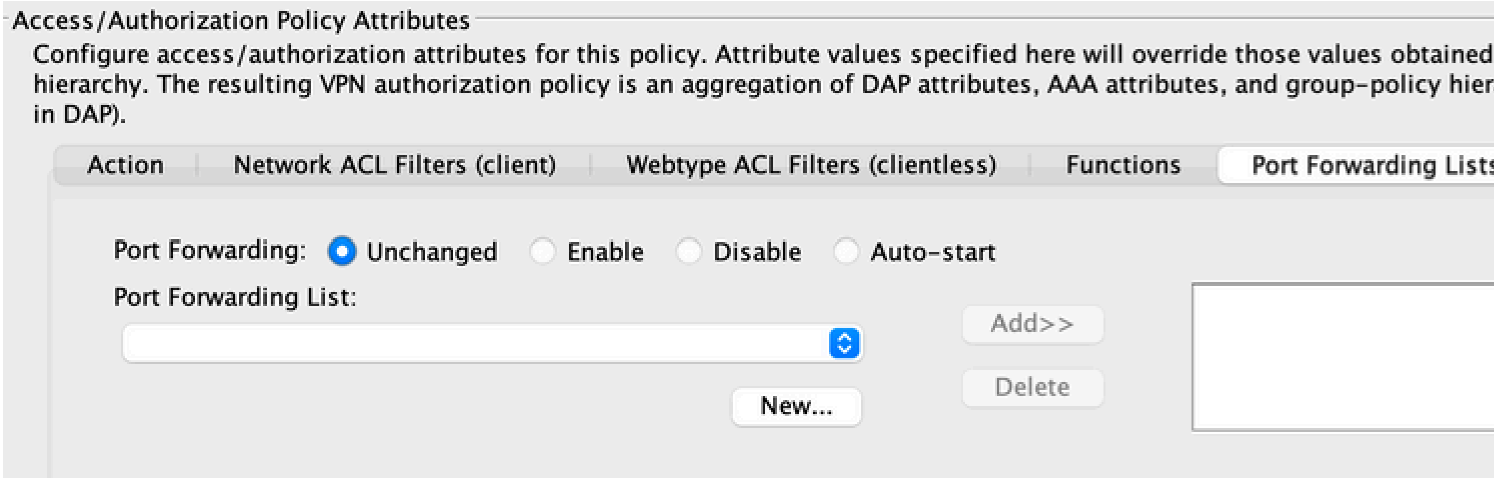
- URL Entryâ€”Allows or prevents a user from entering HTTP/HTTPS URLs on the portal page. If this feature is enabled, users can enter web addresses in the URL entry box, and use clientless SSL VPN to access those websites.

- Unchangedâ€”(default) Click to use values from the group policy that applies to this session.

- Enable/Disableâ€”Click to enable or disable the feature.

- Auto-startâ€”Click to enable HTTP proxy and to have the DAP record automatically start the applets associated with these features.

Figure 12. Port Forwarding Lists Tab â€” This lets you select and configure port forwarding lists for user sessions.



Access/Authorization Policy Attributes

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hier in DAP).

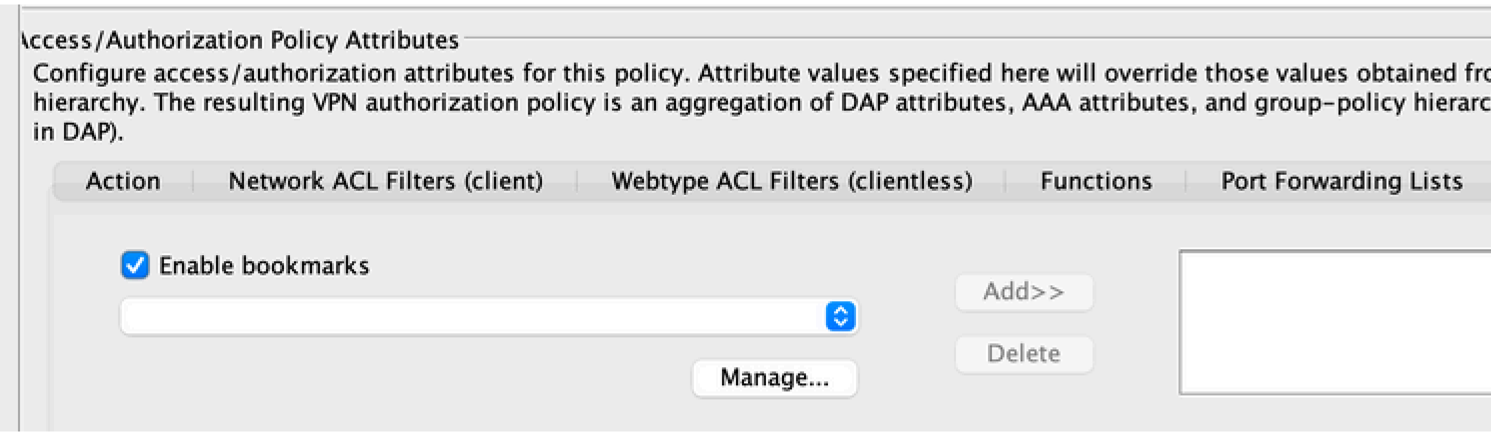
Action
Network ACL Filters (client)
Webtype ACL Filters (clientless)
Functions
Port Forwarding Lists

Port Forwarding: ● Unchanged ○ Enable ○ Disable ○ Auto-start

Port Forwarding List:

- Port Forwardingâ€”Select an option for the port forwarding lists that apply to this DAP record. The other attributes in this field are enabled only when you set Port Forwarding to Enable or Auto-start.
- Unchangedâ€” Click to use values from the group policy that applies to this session.
- Enable/Disableâ€”Click to enable or disable port forwarding.
- Auto-startâ€—Click to enable port forwarding, and to have the DAP record automatically start the port forwarding applets associated with its port forwarding lists.
- Port Forwarding List drop-down boxâ€—Select already configured port forwarding lists to add to the DAP record.
- Newâ€—Click to configure new port forwarding lists.
- Port Forwarding Listsâ€—Displays the port forwarding list for the DAP record.
- Addâ€—Click to add the selected port forwarding list from the drop-down box to the Port Forwarding list on the right.
- Deleteâ€—Click to delete the selected port forwarding list from the Port Forwarding list. You cannot delete an ACL if it is assigned to a DAP or other record.

Figure 13. Bookmarks tab â€” allows you to select and configure bookmarks/URL lists for user sessions.



\ccess/Authorization Policy Attributes

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained fr hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierar in DAP).

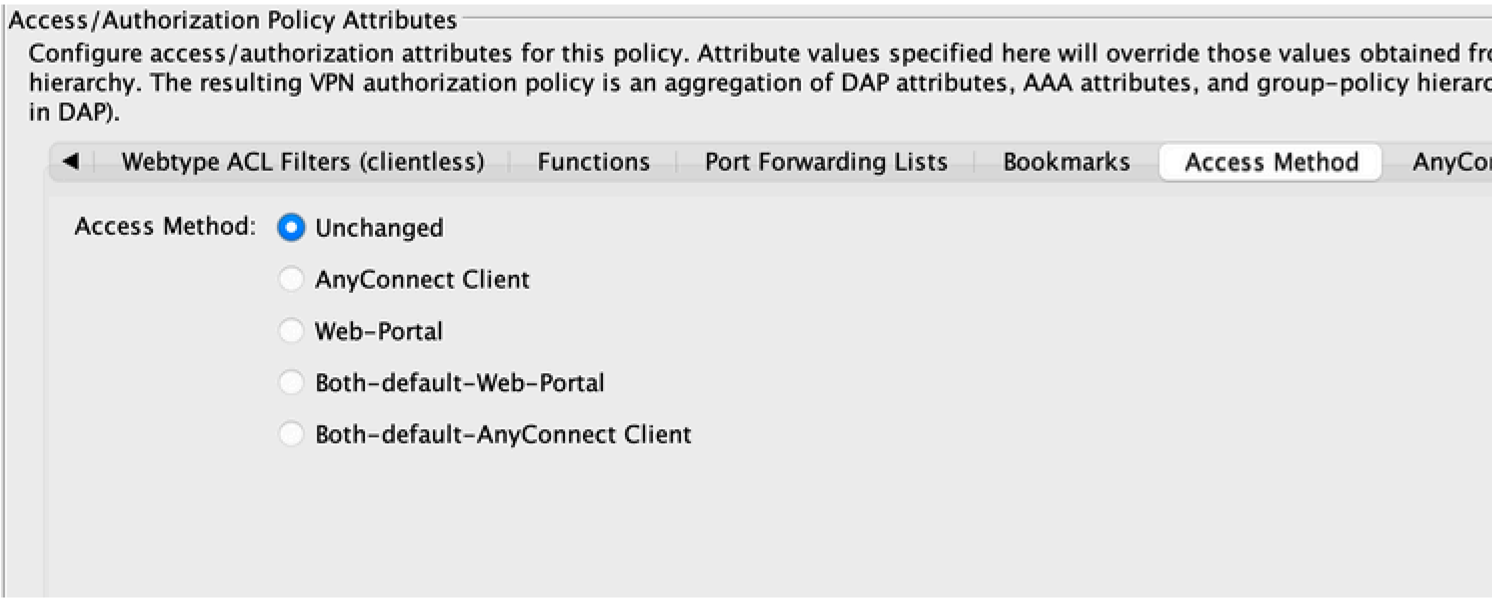
Action
Network ACL Filters (client)
Webtype ACL Filters (clientless)
Functions
Port Forwarding Lists

☑ Enable bookmarks

- Enable bookmarksâ€—Click to enable. when this box is not selected, no Bookmark lists display on the portal page for the connection

- Manageâ€”Click to add, import, export, and delete Bookmark lists.
- Bookmarks Lists (Drop-down) â€”Displays the bookmark lists for the DAP record.
- Addâ€”Click to add the selected bookmark list from the drop-down box to the bookmark list box on the right.
- Deleteâ€”Click to delete the selected bookmark list from the bookmark list box. You cannot delete a bookmark list from the security appliance unless you first delete it from DAP records.

Figure 14. Method Tab â€” Allows you to configure the type of remote access permitted.



Access/Authorization Policy Attributes

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained fr hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarc in DAP).

Access Method:
● Unchanged
○ AnyConnect Client
○ Web-Portal
○ Both-default-Web-Portal
○ Both-default-AnyConnect Client

- Unchangedâ€”Continue with the current remote access method set in the group policy for the session.
- AnyConnect Clientâ€”Connect using the Cisco AnyConnect VPN Client.
- Web Portalâ€—Connect with a clientless VPN.
- Both-default-Web-Portalâ€—Connect via either clientless or the AnyConnect client, with a default of clientless.
- Both-default-AnyConnect Clientâ€—Connect via either clientless or the AnyConnect client, with a default of AnyConnect.

As mentioned previously, a DAP record has a limited set of default attribute values, only if they are modified do they take precedence over current AAA, user, group, tunnel group, and default group records. If additional attribute values outside the scope of DAP are required, for example, Split Tunneling Lists, Banners, Smart Tunnels, Portal Customizations, and so on, then they need to be enforced via AAA, user, group, tunnel group, and default group records. In this case, those specific attribute values can complement DAP and can not be overridden. Thus, the user gets a cumulative set of attribute values across all records.

Aggregate Multiple Dynamic Access Policies

An administrator can configure multiple DAP records to address many variables. As a result, an authenticating user can satisfy the AAA and Endpoint attribute criteria of multiple DAP records. In consequence, Access Policy Attributes can either be consistent or conflict throughout these policies. In this case, the authorized user can get the cumulative result across all matched DAP records.

This also includes unique attribute values enforced via authentication, authorization, user, group, tunnel group, and default group records. The cumulative result of Access Policy Attributes creates the Dynamic Access Policy. Examples of combined Access Policy Attributes are listed in the next Tables. These examples depict the results of 3 combined DAP records.

The action attribute shown in Table 1 has a value that is either Terminate or Continue. The aggregated attribute value is Terminate if the Terminate value is configured in any of the selected DAP records and is Continue if the Continue value is configured in all of the selected DAP records.

Table 1. Action Attribute

Attribute Name	DAP#1	DAP#2	DAP#3	DAP
Action (Example 1)	continue	continue	continue	continue
Action (Example 2)	Terminate	continue	continue	terminate

The user-message attribute shown in Table 2 contains a string value. The aggregated attribute value can be a line-feed (hex value 0x0A) separated string created by linking together the attribute values from the selected DAP records. The ordering of the attribute values in the combined string is insignificant.

Table 2. User-Message Attribute

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

The **Clientless** feature enabling attributes (Functions) shown in Table 3 contain values that are **Auto-start**, **Enable**, or **Disable**. The aggregated attribute value can be Auto-start if the **Auto-Start** value is configured in any of the selected DAP records.

The aggregated attribute value can be Enabled if there is no Auto-start value configured in any of the selected DAP records, and the **Enable** value is configured in at least one of the selected DAP records.

The aggregated attribute value can be disabled if there is no **Auto-start** or **Enable** value configured in any of the selected DAP records, and the â€œdisableâ€� value is configured in at least one of the selected DAP records.

Table 3. Clientless Feature Enabling Attributes (Functions)

Attribute Name	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

The **URL list** and **port-forward** attributes shown in Table 4 contain a value that is either a string or a comma-separated string. The aggregated attribute value can be a comma-separated string created by when you link together the attribute values from the selected DAP records. Any duplicate attribute value in the combined string can be removed. How the attribute values are ordered in the combined string is insignificant.

Table 4. URL List and Port Forward List Attribute

Attribute Name	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

The **Access Method** attributes specify the client access method allowed for SSL VPN connections. The client access method can be AnyConnect Client access only, Web-Portal access only, AnyConnect Client or Web-Portal access with Web-Portal access as the default, or AnyConnect Client or Web-Portal access with AnyConnect Client access as the default. The aggregated attribute value is summarized in Table 5.

Table 5. Access Method Attributes

Attribute Values Selected				Aggregation result
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

When you combine **Network (Firewall)** and **Web-Type (Clientless) ACL Filter** attributes, the **DAP Priority** and **DAP ACL** are two major components to consider.

The **Priority** tribute as shown in Figure 15 is not aggregated. The security appliance uses this value to logically sequence the access lists when aggregating the **Network** and **Web-Type ACLs** from multiple DAP records. The security appliance orders the records from highest to lowest priority number, with the lowest at the bottom of the table. For instance, a **DAP** record with a value of 4 has a higher priority than a record with a value of 2. You cannot manually sort them.

Figure 15. Priority â€”Displays the priority of the DAP record.

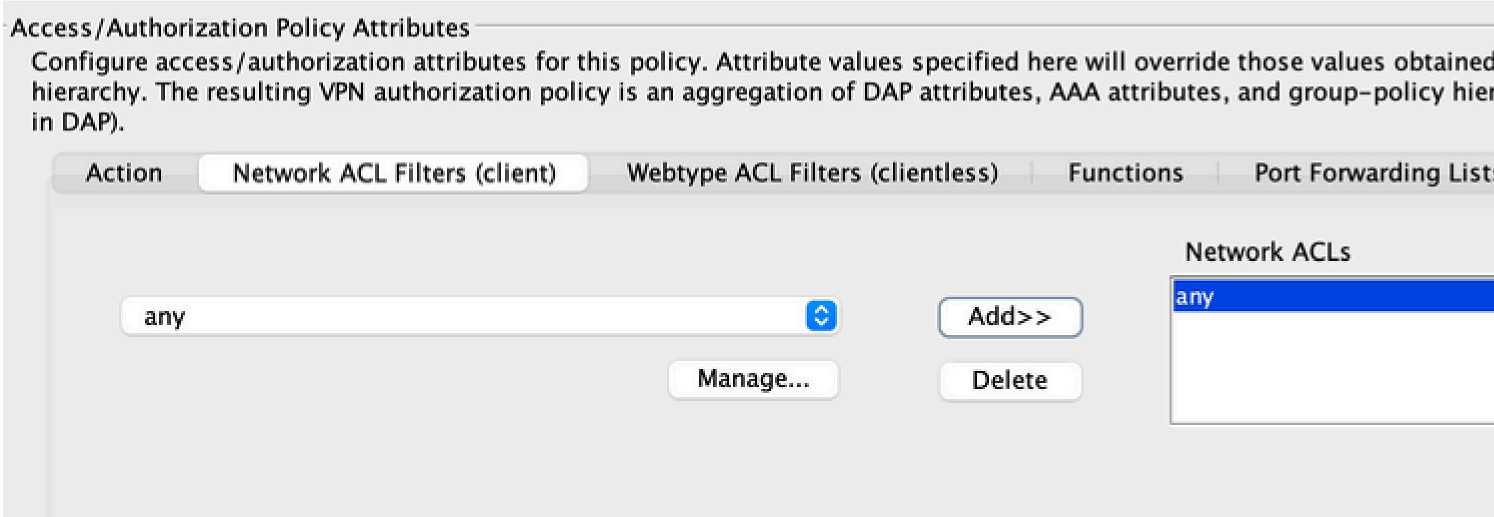
Policy Name:

Description:

- Policy Nameâ€”Displays the name of the **DAP** record.
- Descriptionâ€”Describes the purpose of the **DAP** record.

The DAP ACL attribute only supports access lists that conform to either a strict **Allow-List** or strict **Block-List** ACL model. In an **Allow-List** ACL model, the access-list entries specify rules that â€œPermitâ€� access to specified networks or hosts. In a **Block-List** ACL mode, the access-list entries specify rules that **deny** access to specified networks or hosts. A non-conforming access list contains access-list entries with a mixture of **permit** and **deny** rules. If a nonconforming access list is configured for a DAP record, it can be rejected as a configuration error when the administrator tries to add the record. If an access list that conforms is assigned to a DAP record, then any modification to the access list that changes the conformance characteristic can be rejected as a configuration error.

Figure 16. DAP ACLâ€” This lets you select and configure network ACLs to apply to this DAP record.



Access/Authorization Policy Attributes

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hier in DAP).

When multiple DAP records are selected, the access-lists attributes specified in the Network (Firewall) ACL are aggregated to create a **Dynamic Access List** for the **DAP Firewall ACL**. In the same way, the access-lists attributes specified in the **Web-Type (Clientless) ACL** are aggregated to create a Dynamic Access List for the DAP Clientless ACL. The next example focuses on how a dynamic DAP Firewall Access-List is created specifically. However, a dynamic DAP Clientless Access List also can do the same process.

First, the ASA dynamically creates a unique name for the **DAP Network-ACL** as shown in Table 6.

Table 6. Dynamic DAP Network-ACL Name

DAP Network-ACL Name
DAP-Network-ACL-X (where X is an integer that can increment to ensure uniqueness)

Second, the ASA retrieves the **Network-ACL** attribute from the selected DAP records as shown in Table 7.

Table 7. Network ACLs

Selected DAP Records	Priority	Network-ACLs	Network-ACL Entries
DAP 1	1	101 and 102	ACL 101 has 4 Deny Rules and ACL 102 has 4 Permit Rules
DAP 2	2	201 and 202	ACL 201 has 3 Permit Rules and ACL 202 has 3 Deny Rules
DAP 3	2	101 and 102	ACL 101 has 4 Deny Rules and ACL 102 has 4 Permit Rules

Third, the ASA reorders the **Network-ACL** first by the DAP record Priority number, and then by **Block-List** first if the Priority value for 2 or more selected DAP records is the same. After this, the ASA can then retrieve the Network-ACL entries from each Network-ACL as shown in Table 8.

Table 8. DAP Record Priority

Network-ACLs	Priority	White/Black Access-List Model	Network-ACL Entries
101	2	Black-List	4 Deny Rules (DDDD)
202	2	Black-List	3 Deny Rules (DDD)
102	2	White-List	4 Permit Rules (PPPP)
202	2	White-List	3 Permit Rules (PPP)
101	1	Black-List	4 Deny Rules (DDDD)
102	1	White-List	4 Permit Rules (PPPP)

Lastly, the ASA merges the **Network-ACL** entries into the dynamically generated **Network-ACL** and then returns the name of the dynamic **Network-ACL** as the new **Network-ACL** to be enforced as shown in Table 9.

Table 9. Dynamic DAP Network-ACL

DAP Network-ACL Name	Network-ACL Entry
DAP-Network-ACL-1	DDDD DDD PPPP PPP DDDD PPP

DAP Implementation

There are a host of reasons why an administrator must consider implementing DAP. Some underlying reasons are when posture assessment on an endpoint is to be enforced, and/or when more granular AAA or policy attributes are to be considered when authorizing user access to network resources. In the next example, you can configure DAP and its components to identify a connecting endpoint and authorize user access to various network resources.

Test Case â€“ A client has requested a Proof-of-Concept with these VPN Access requirements:

- The ability to detect and identify an employee endpoint as Managed or Unmanaged. â€”If the endpoint is identified as managed (work PC) but fails the posture requirements, that endpoint must then be denied access. On the other hand, if the employeeâ€™s endpoint is identified as unmanaged (home PC), that endpoint must then be granted clientless access.
- The ability to invoke cleanup of session cookies and cache when a clientless connection terminates.
- The ability to detect and enforce running applications on managed employee endpoints, such as McAfee AntiVirus. If the application does not exist, that endpoint must then be denied Access.

- The ability to use AAA authentication to determine what network resources authorized users must have access to. The Security Appliance must support Native MS LDAP authentication and support multiple LDAP group membership roles.
- The ability to allow local LAN access to network resources such as network faxes and printers when connected via a client/network-based connection.
- The ability to provide authorized guest access to contractors. Contractors and their endpoints must get clientless access, and their portal access to applications must limit in comparison to employee access.

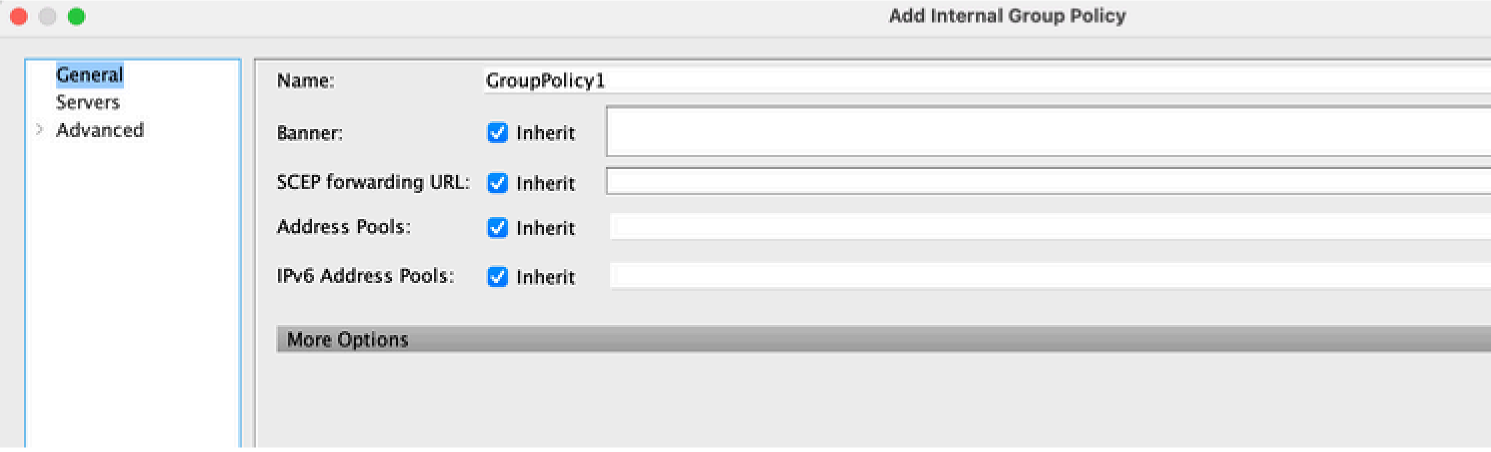
In this example, you can execute a series of configuration steps to meet the clientâ€™s VPN access requirements. There can be necessary configuration steps but not directly related to DAP while other configurations can be directly related to DAP. The ASA is very dynamic and can adapt to many network environments. As a result, VPN solutions can be defined in various ways and in some cases provide the same end solution. The approach taken however is driven by client needs and their environments.

Based on the nature of this paper and the client requirements defined, you can use Adaptive Security Device Manager (ASDM) and focus most of our configurations around DAP. However, you can also configure local Group Policies to show how DAP can complement and/or override local policy attributes. For the basis of this test case, you can assume an LDAP Server Group, Split Tunneling Network List, and basic IP connectivity, including IP Pools and the DefaultDNS Server Group, are preconfigured.

Defining a Group Policyâ€” this configuration is necessary for defining Local Policy Attributes. Some attributes defined here are not configurable in DAP for (example, Local LAN Access). (This Policy can also be used to define Clientless and Client based attributes).

Navigate to**Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**, and add an Internal Group Policy as shown:

Figure 17. Group Policy â€”Defines Local VPN Specific Attributes.



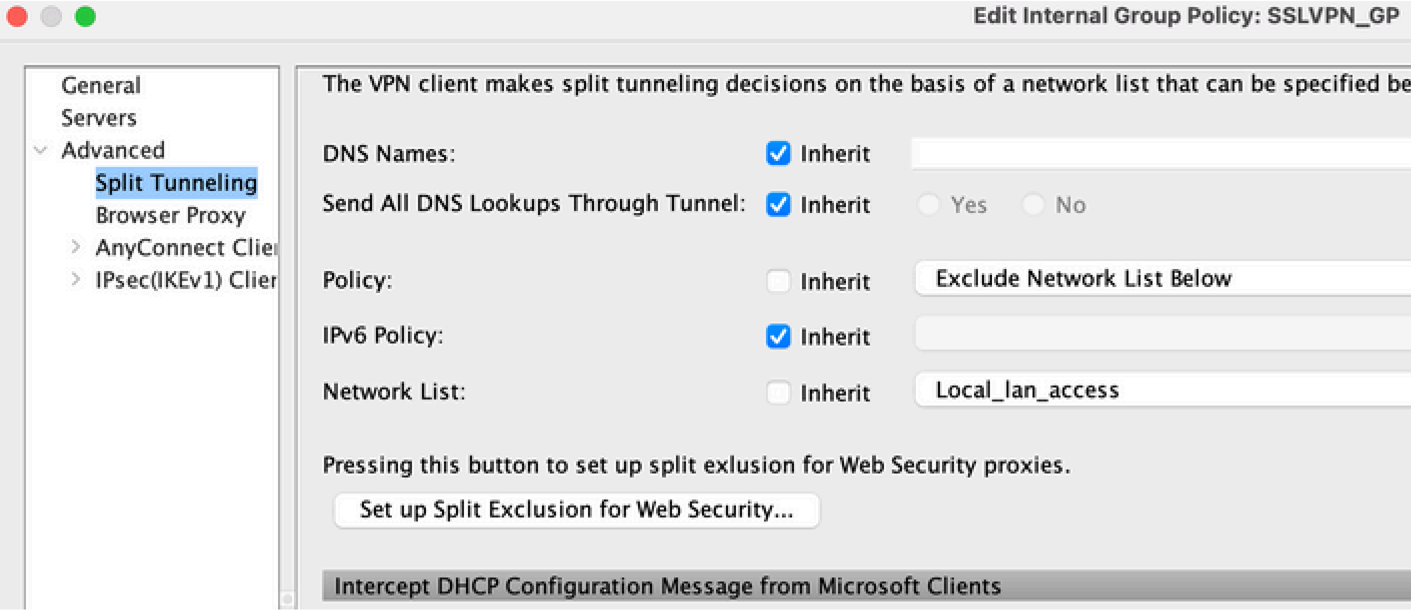
Name: GroupPolicy1
Banner: ☑ Inherit
SCEP forwarding URL: ☑ Inherit
Address Pools: ☑ Inherit
IPv6 Address Pools: ☑ Inherit

a. Under the General link, configure the name**SSLVPN_GP**for the Group Policy.

b. Also under the General link, click**More Options**and configure only the Tunneling Protocol:**Clientless SSLVPN**. (You can configure DAP to override and manage the Access Method.)

c. Under the **Advanced** > **Split Tunneling** link, configure the next steps:

Figure 18. Split Tunneling â€”Allows specified traffic (Local Network) to bypass an unencrypted tunnel during a Client connection.



Edit Internal Group Policy: SSLVPN_GP

The VPN client makes split tunneling decisions on the basis of a network list that can be specified be

DNS Names: ☑ Inherit

Send All DNS Lookups Through Tunnel: ☑ Inherit ○ Yes ○ No

Policy: □ Inherit Exclude Network List Below

IPv6 Policy: ☑ Inherit

Network List: □ Inherit Local_lan_access

Pressing this button to set up split exlusion for Web Security proxies.

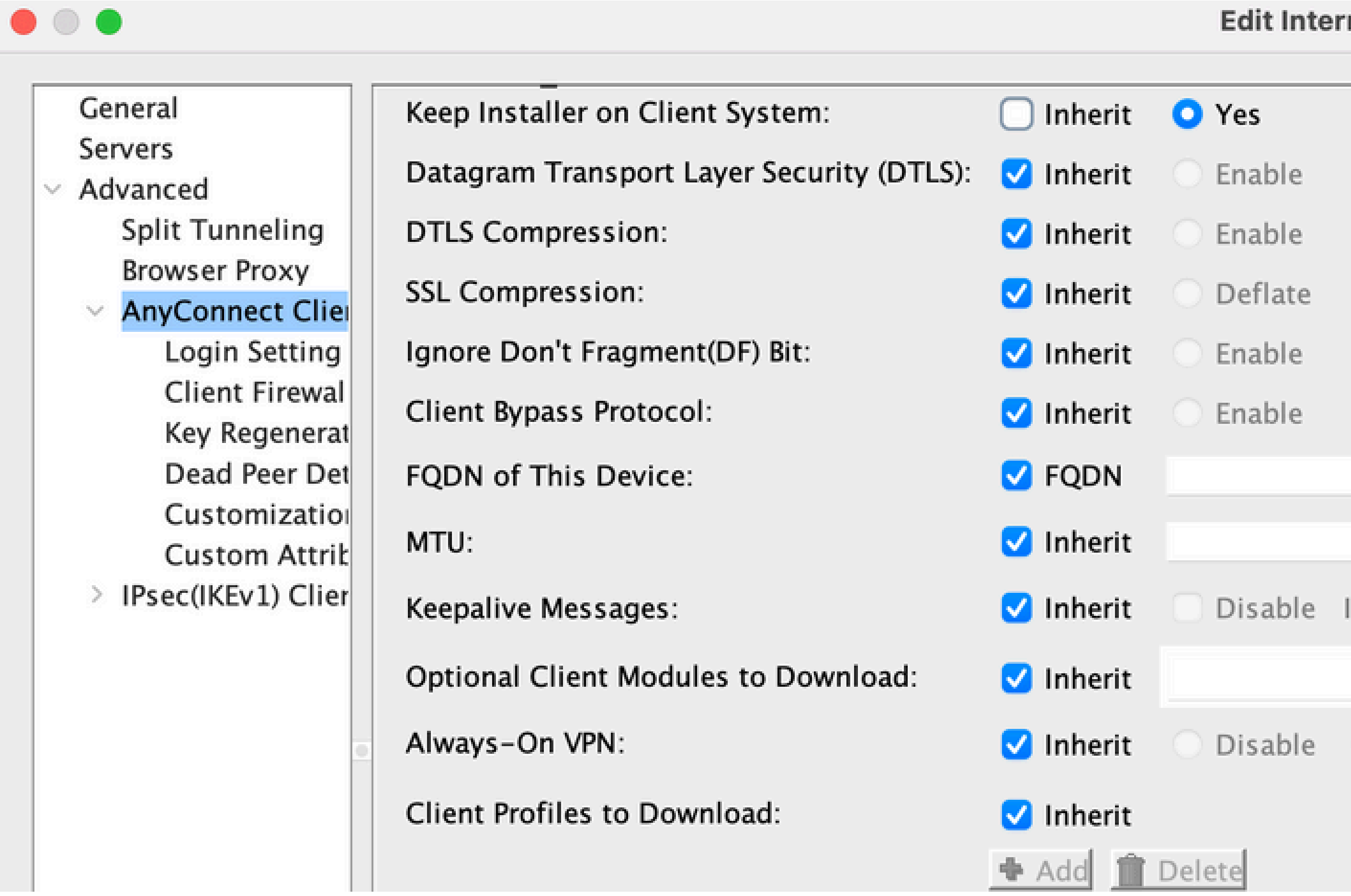
Set up Split Exclusion for Web Security...
Intercept DHCP Configuration Message from Microsoft Clients

a. Policy: Uncheck**Inherit**and select**Exclude Network List**.

b. Network List: Uncheck**Inherit**and select the list name**Local_Lan_Access**. (Assumed that it is preconfigured.)

d. Under the **Advanced** > **ANYCONNECT Client** link, configure these next steps:

Figure 19. SSL VPN Client Installer â€”Upon VPN termination, the SSL Client can remain on the endpoint or be uninstalled.



Edit Interı

Keep Installer on Client System: □ Inherit ● Yes

Datagram Transport Layer Security (DTLS): ☑ Inherit ○ Enable

DTLS Compression: ☑ Inherit ○ Enable

SSL Compression: ☑ Inherit ○ Deflate

Ignore Don't Fragment(DF) Bit: ☑ Inherit ○ Enable

Client Bypass Protocol: ☑ Inherit ○ Enable

FQDN of This Device: ☑ FQDN

MTU: ☑ Inherit

Keepalive Messages: ☑ Inherit □ Disable

Optional Client Modules to Download: ☑ Inherit

Always-On VPN: ☑ Inherit ○ Disable

Client Profiles to Download: ☑ Inherit

e. Keep Installer on Client System: Uncheck**Inherit**and then select**Yes**.

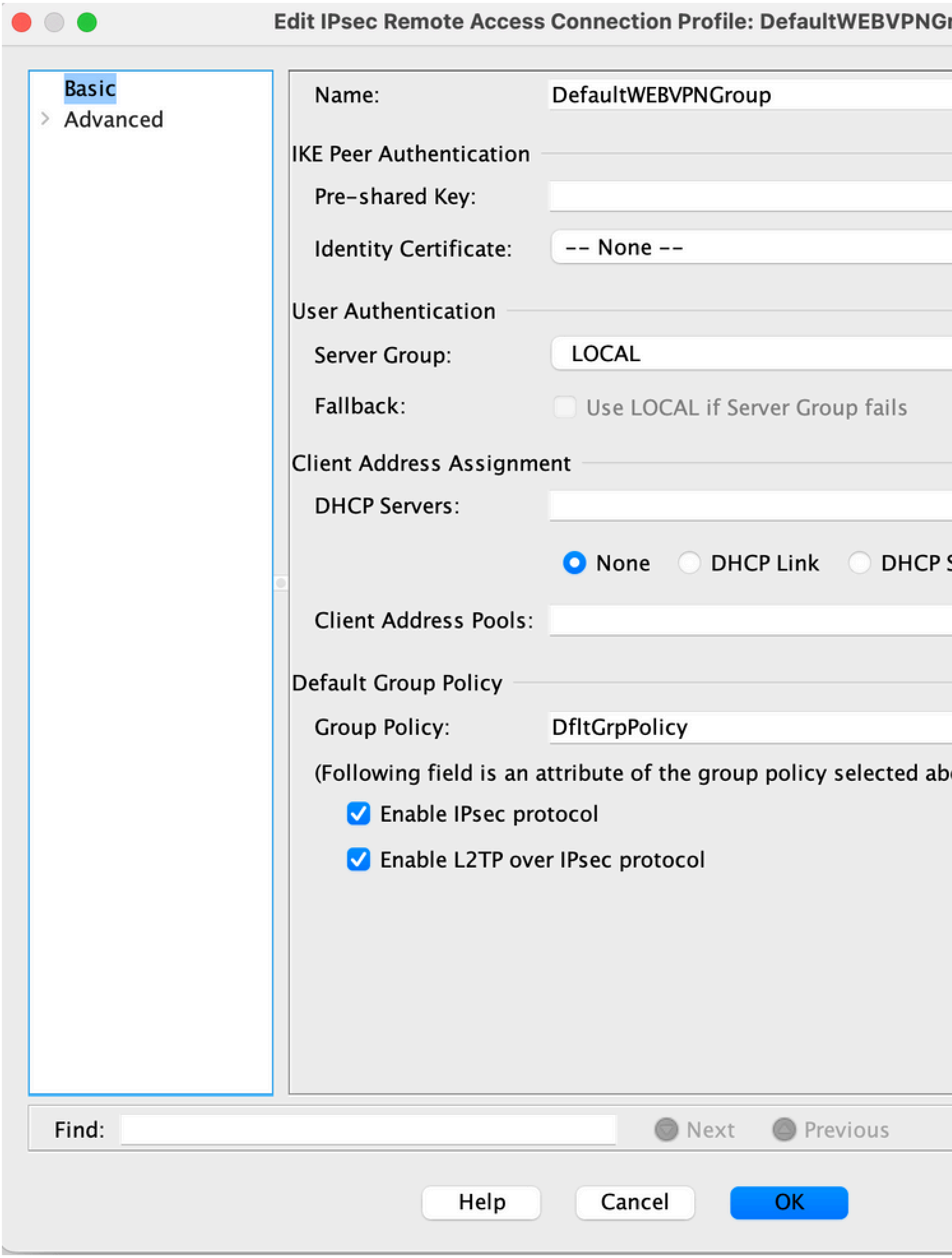
f. ClickOKthenApply.

g. Apply your configuration changes.

Defining a Connection Profileâ€”this configuration is necessary for defining our AAA authentication method, for example, LDAP, and applying the previously configured Group Policy (SSLVPN_GP) to this Connection Profile. Users connecting via this Connection Profile can be subjected to the attributes defined here as well as attributes defined in the SSLVPN_GP Group Policy. (This Profile can also be used to define both Clientless and Client based attributes).

Navigate to**Configuration > Remote Access VPN > Network (Client) Access >IPsec Remote Access Connection Profile** and configure:

Figure 20. Connection Profile â€” Defines Locally VPN Specific Attributes.



Edit IPsec Remote Access Connection Profile: DefaultWEBVPNGr

Name: DefaultWEBVPNGroup

IKE Peer Authentication

Pre-shared Key:

Identity Certificate: -- None --

User Authentication

Server Group: LOCAL

Fallback: □ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP S

Client Address Pools:

Default Group Policy

Group Policy: DfltGrpPolicy

(Following field is an attribute of the group policy selected ab

☑ Enable IPsec protocol

☑ Enable L2TP over IPsec protocol

a. Under the Connection Profiles section, Edit the DefaultWEBVPNGroup and under the Basic link configure the next steps:

   a. Authenticationâ€”Method:**AAA**

   b. Authenticationâ€”AAA Server Group:**LDAP**(Assumed preconfigured)

   c. Client Address Assignmentâ€—Client Address Pools:**IP_Pool**(Assumed preconfigured)

   d. Default Group Policyâ€—Group Policy: Select**SSLVPN_GP**

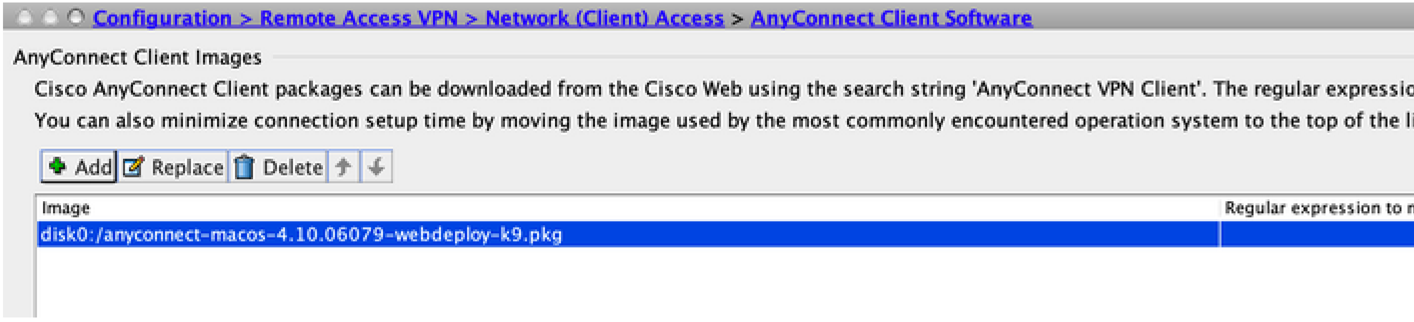
b. Apply your configuration changes.

Define an IP interface for SSL VPN connectivity â€” This configuration is necessary for terminating Client and Clientless SSL connections on a specified interface.

Before enabling Client/Network access on an interface, you must first define an SSL VPN Client image.

1. Navigate to**Configuration > Remote Access VPN > Network (Client)Access > Anyconnect Client Software**, and Add the next image, the SSL VPN Client Image from the ASA Flash file system: (This image can be downloaded from CCO, https://www.cisco.com)

   Figure 21. SSL VPN Client Image Installâ€”Defines the AnyConnect Client image to be pushed to connect endpoints.



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Software

AnyConnect Client Images

Cisco AnyConnect Client packages can be downloaded from the Cisco Web using the search string 'AnyConnect VPN Client'. The regular expressio

You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the li

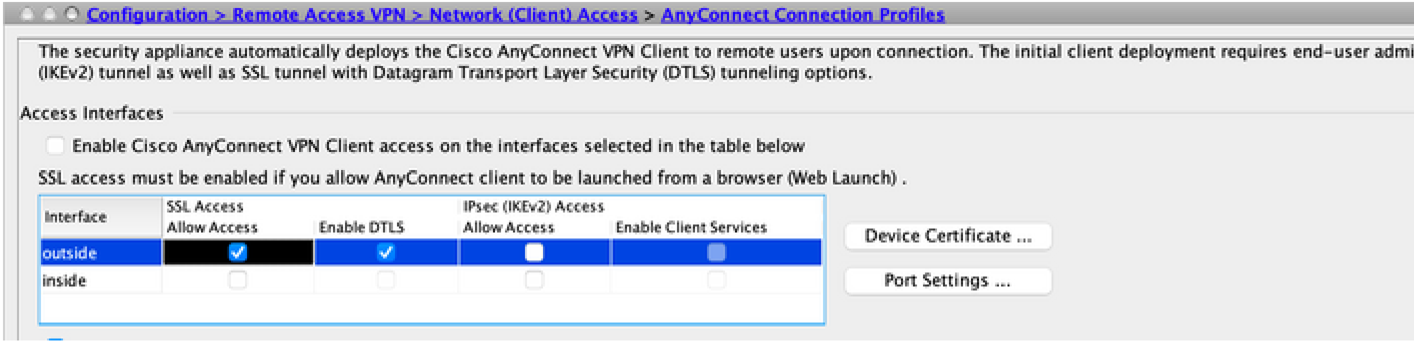
Image	Regular expression to r
disk0:/anyconnect-macos-4.10.06079-webdeploy-k9.pkg	

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

   b. Click**OK**,**OK**again, and then**Apply**.

2. **Navigate to Configuration > Remote Access VPN > Network (Client)Access > AnyConnect Connection Profiles**, and use the next steps to enable this:

   Figure 22. SSL VPN Access Interfaceâ€—Defines the interface(s) for terminating SSL VPN connectivity.



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user admi (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

Access Interfaces

□ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access Allow Access	Enable DTLS	IPsec (IKEv2) Access Allow Access	Enable Client Services
outside	☑	☑	□	□
inside	□	□	□	□

   a. Under the Access Interface section, enable:**Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the table below.**

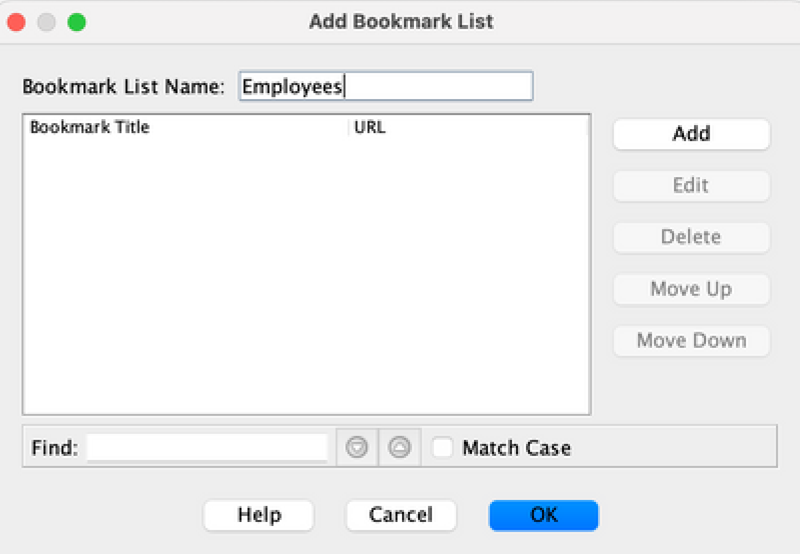
b. Also under the Access Interfaces section, check**Allow Access**on the outside interface. (This configuration can also enable SSL VPN Clientless access on the outside interface.)

c. Click**Apply**.

Defining Bookmark Lists (URL Lists) for Clientless Accessâ€"This configuration is necessary for defining a web-based application to be published on the Portal. you can define 2 URL Lists, one for Employees and the other for Contractors.

1. Navigate to**Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Portal** > **Bookmarks**, click**+ Add**and configure the next steps:

Figure 23. Bookmark Listâ€"Defines URLs to be published and accessed from the Web Portal. (Customized for Employee access).



Add Bookmark List

Bookmark List Name: Employees

Bookmark Title	URL

a. Bookmark List Name:**Employees**, then click**Add**.

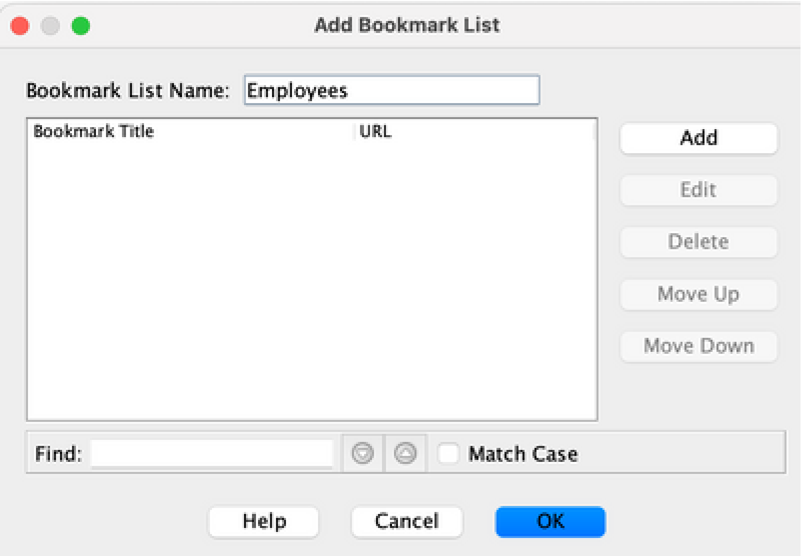
b. Bookmark Title:**Company Intranet**

c. URL Value: https://company.resource.com

d. Click**OK**and then**OK**again.

2. Click**+ Add**and configure a second Bookmark List (URL List) as follows:

Figure 24. Bookmark List â€"Customized for Guest access.


Add Bookmark List

Bookmark List Name: Employees

a. Bookmark List Name:**Contractors**, then click**Add**.

b. Bookmark Title:**Guest Access**

c. URL Value: https://company.contractors.com

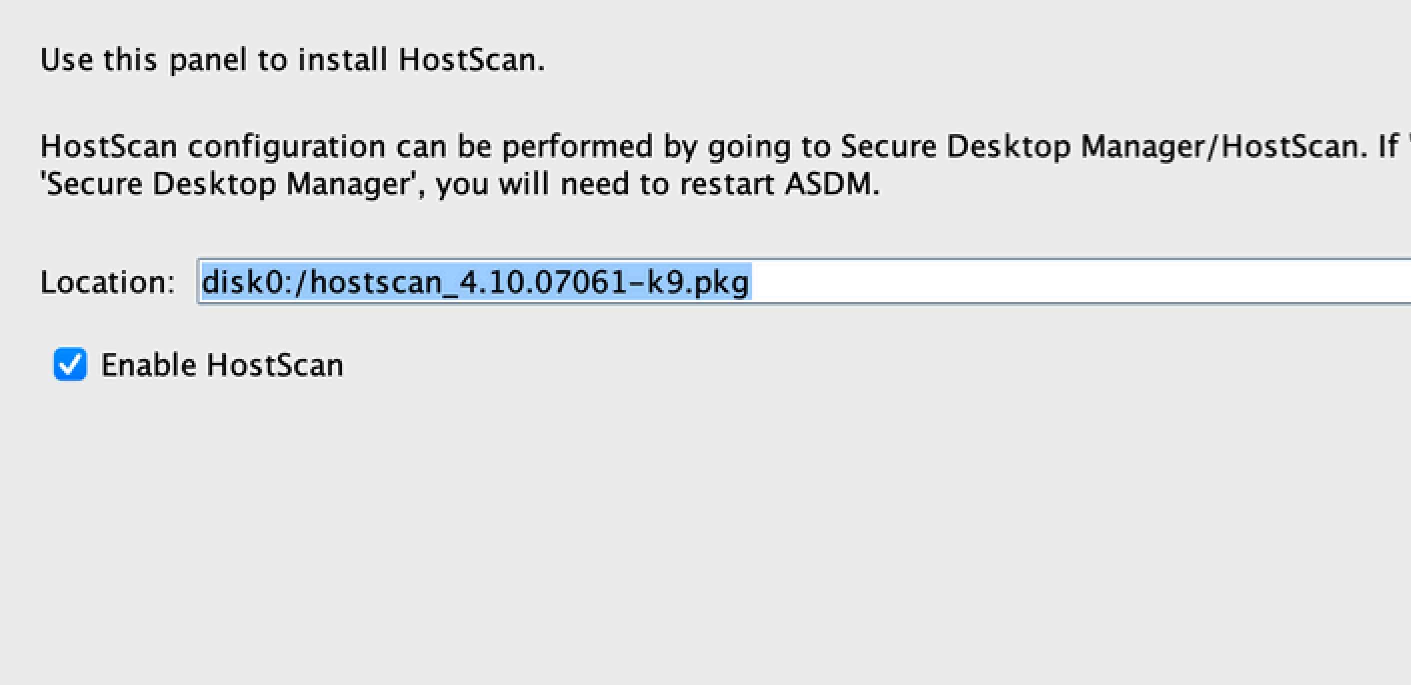
d. Click**OK**and then**OK**again.

e. Click**Apply**.

Configure Hostscan:

1. Navigate to**Configuration** > **Remote Access VPN** > **Secure Desktop Manager** > **HostScan Image**, and configure the next steps:

Figure 25. HostScan Image Installâ€”Defines the HostScan image to be pushed to connect endpoints.


Use this panel to install HostScan.

HostScan configuration can be performed by going to Secure Desktop Manager/HostScan. If '
'Secure Desktop Manager', you will need to restart ASDM.

Location: disk0:/hostscan_4.10.07061-k9.pkg

☑ Enable HostScan

a. Install the**disk0:/hostscan_4.xx.xxxxx-k9.pkg**image from the ASA Flash file system.

b. Check**Enable HostScan**.

c. Click**Apply**.

Dynamic Access Policies â€” This configuration is necessary for validating connecting users and their endpoints against defined AAA and/or endpoint assessment criteria. If the defined criteria of a DAP record are satisfied, connecting users can then be granted access to network resources that are associated with that DAP record or records. DAP authorization is executed during the authentication process.

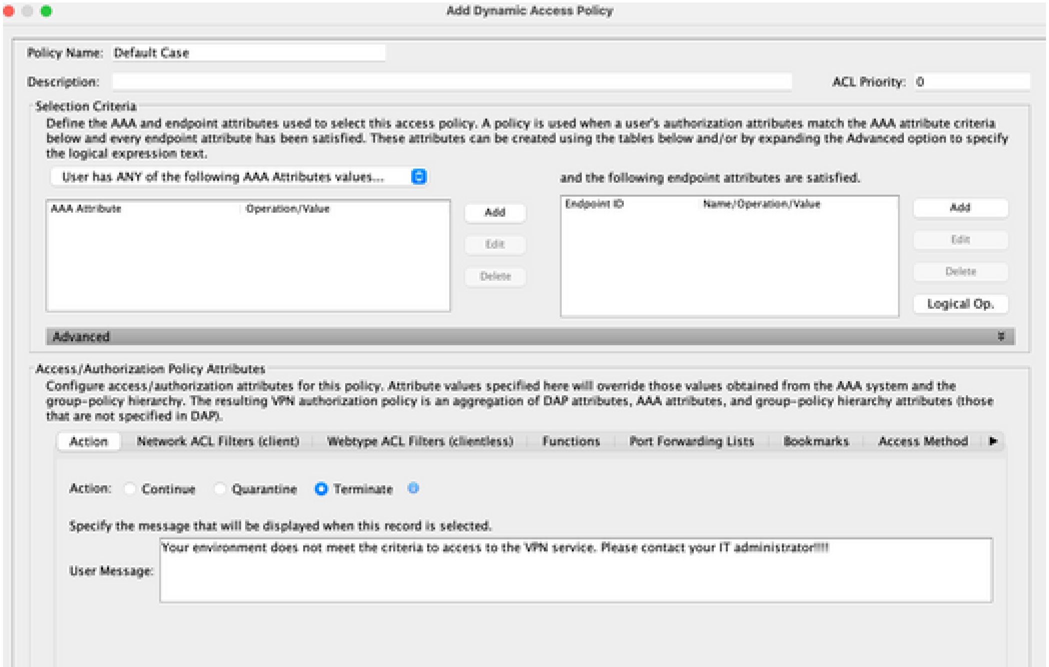
To ensure that an SSL VPN connection can terminate in the default case, for example, when the endpoint does not match any configured Dynamic Access policies), you can configure it with these steps:

> **Note**: When configuring Dynamic Access Policies for the first time, a DAP.xml error message is displayed indicating that a DAP configuration file (DAP.XML) does not exist. Once your initial DAP configuration is modified and then saved, this message can no longer appear.

---

1. Navigate to**Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies**, and configure the next steps:

   Figure 30. Default Dynamic Access Policy â€”if no predefined DAP records are matched, this DAP record can be enforced. Thus, SSL VPN access can be denied.



Add Dynamic Access Policy

Policy Name: Default Case

Description:

ACL Priority: 0

Selection Criteria

Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ANY of the following AAA Attributes values...

and the following endpoint attributes are satisfied.

AAA Attribute	Operation/Value

Endpoint ID	Name/Operation/Value

Access/Authorization Policy Attributes

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Action: ○ Continue ○ Quarantine ● Terminate

Specify the message that will be displayed when this record is selected.

User Message: Your environment does not meet the criteria to access to the VPN service. Please contact your IT administrator!!!!

a. Edit the**DfltAccessPolicy**and set the Action to**Terminate**.

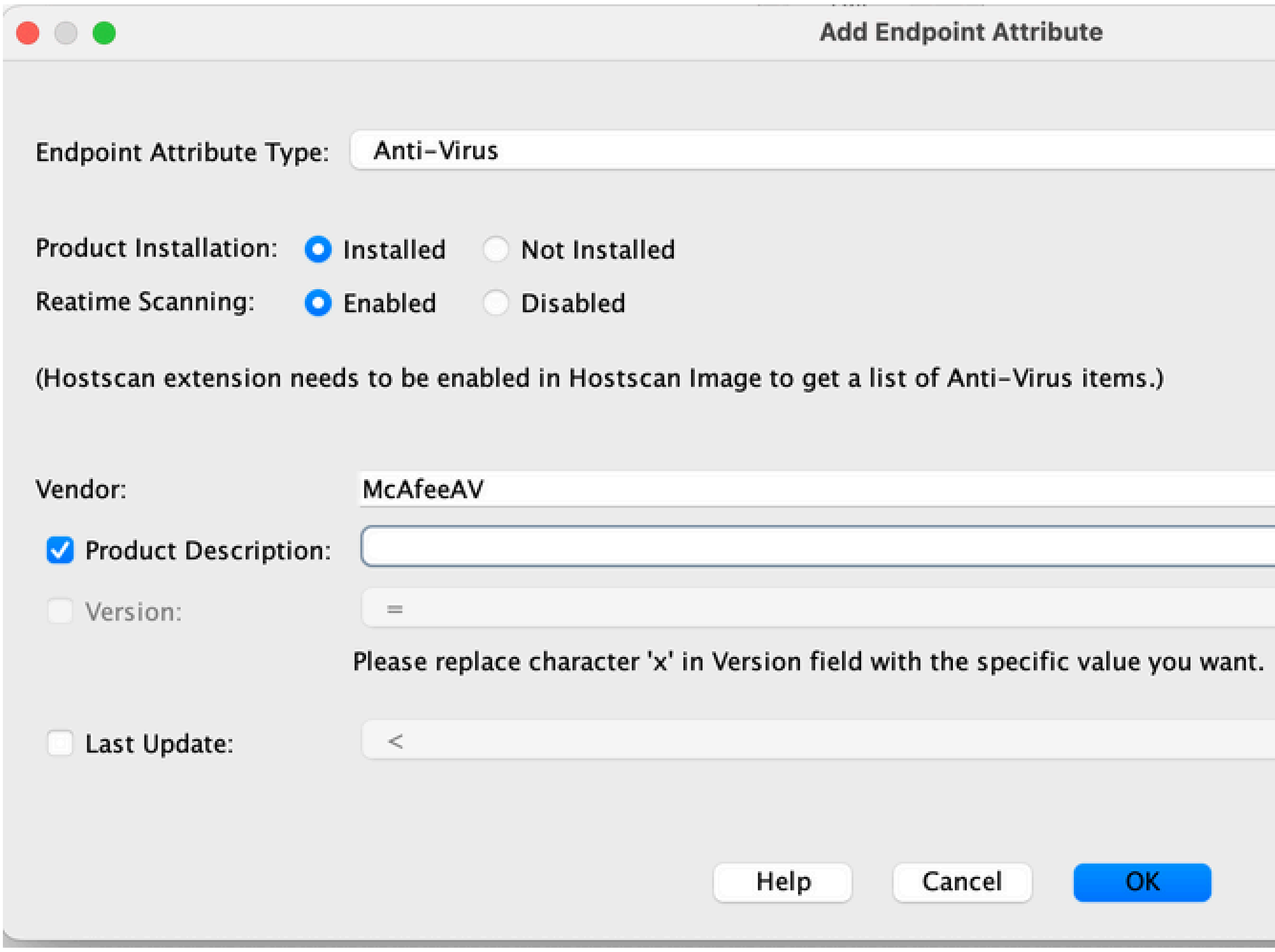
b. Click**OK**.

2. Add a new Dynamic Access Policy named**Managed_Endpoints**, as follows:

a. Description:**Employee Client Access**

b. Add an Endpoint Attribute Type (Anti-Virus) as shown in Figure 31. Click**OK**when complete.

Figure 31. DAP Endpoint Attributeâ€”Advanced Endpoint Assessment AntiVirus can be used as a DAP Criterion for Client/Network Access.



Add Endpoint Attribute

Endpoint Attribute Type: Anti-Virus

Product Installation: ● Installed ○ Not Installed

Reatime Scanning: ● Enabled ○ Disabled

(Hostscan extension needs to be enabled in Hostscan Image to get a list of Anti-Virus items.)

Vendor: McAfeeAV

☑ Product Description:

□ Version: =

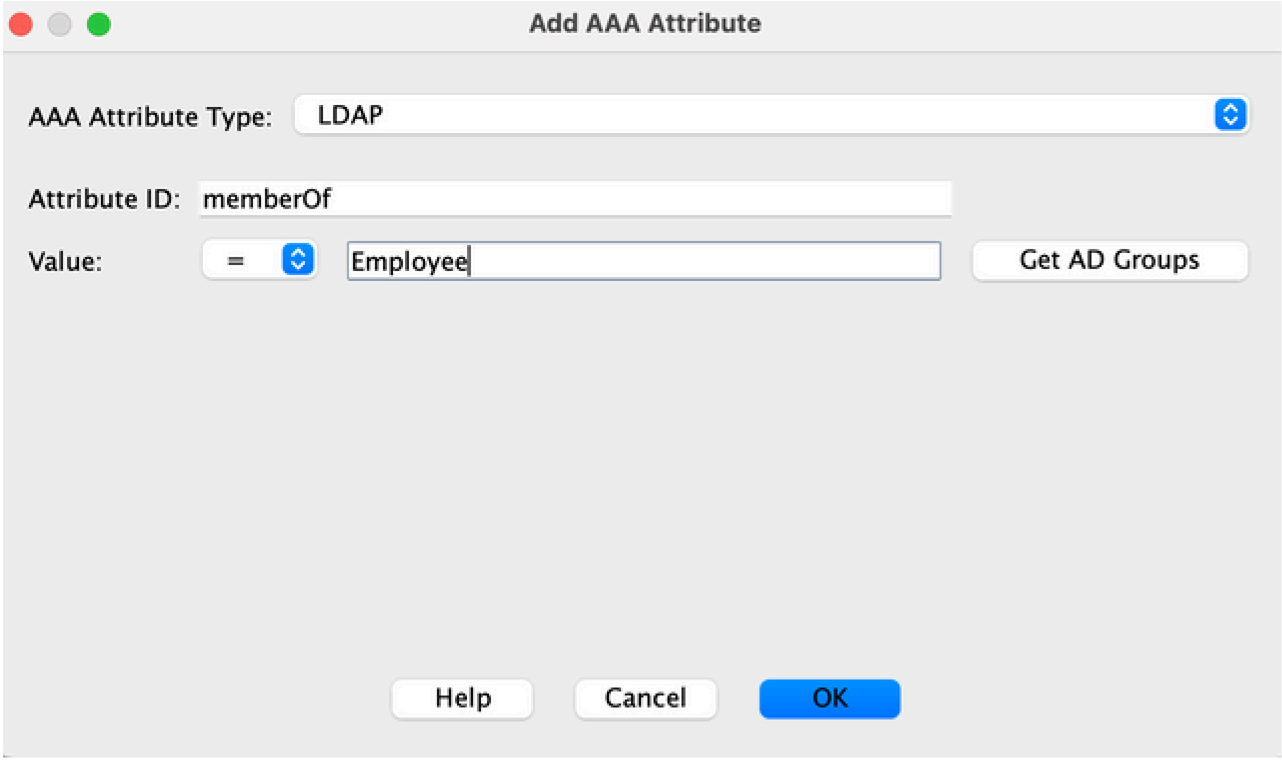
Please replace character 'x' in Version field with the specific value you want.

□ Last Update: <

c. As shown in the previous image, from the drop-down list the AAA Attribute section, select User has ALL of the following AAA Attributes Values.

d. Add (located to the right of the AAA Attribute box) an AAA Attribute Type (LDAP) as shown in Figures 33 and 34. Click**OK**when complete.

Figure 33. DAP AAA Attributeâ€”AAA Group Membership can be used as a DAP criterion to identify an Employee.



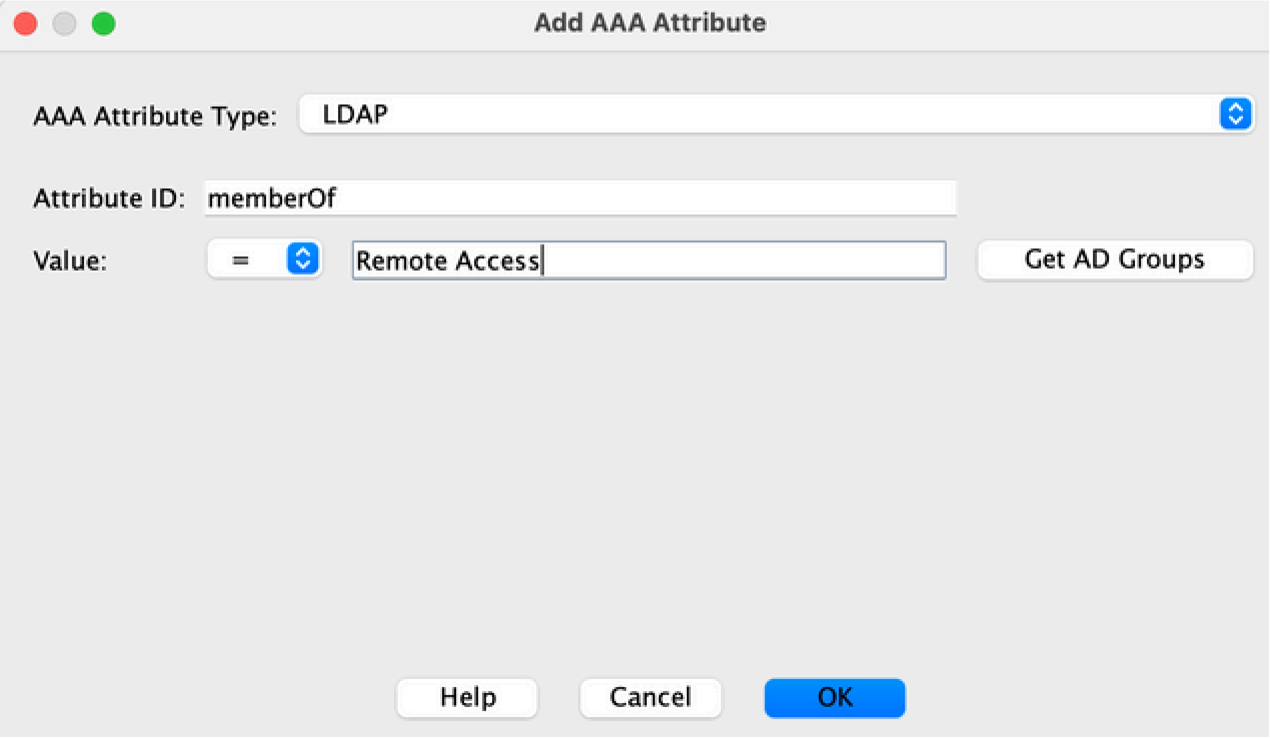
Add AAA Attribute

AAA Attribute Type: LDAP

Attribute ID: memberOf

Value: = Employee

Figure 34. DAP AAA Attributeâ€"AAA Group Membership can be used as a DAP criterion to allow Remote Access capabilities.



Add AAA Attribute

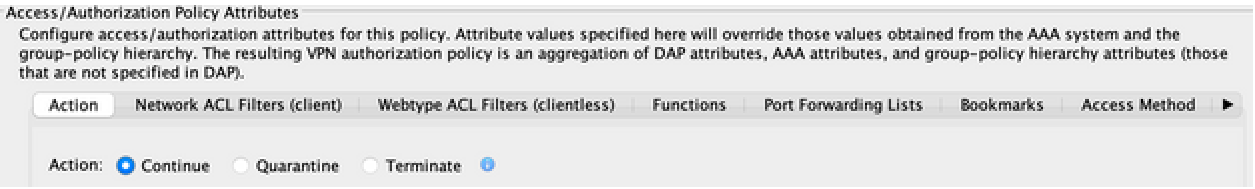
AAA Attribute Type: LDAP

Attribute ID: memberOf

Value: = Remote Access

e. Under the Action tab, verify that the Action is set to**Continue**, as shown in Figure 35.

Figure 35. Action Tabâ€"This configuration is necessary for defining special processing for a specific connection or session. VPN access can be denied if a DAP record is matched and the Action is set to Terminate.



Access/Authorization Policy Attributes

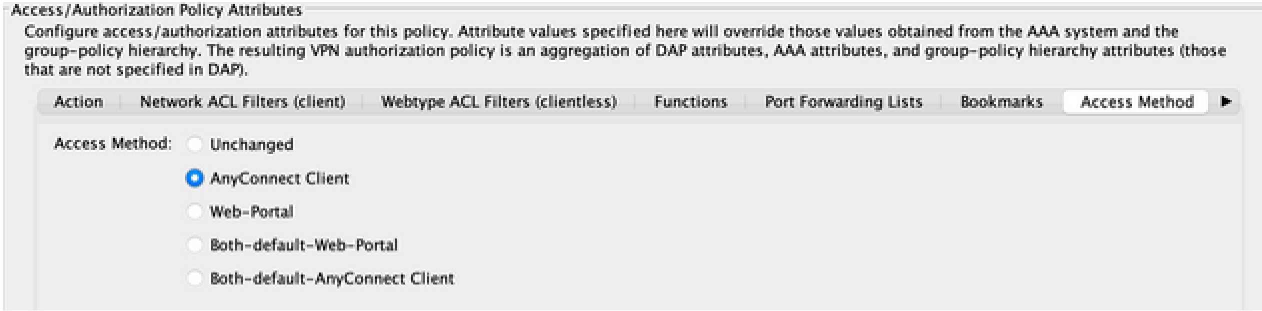
Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Action
Network ACL Filters (client)
Webtype ACL Filters (clientless)
Functions
Port Forwarding Lists
Bookmarks
Access Method
▶

Action: ● Continue ○ Quarantine ○ Terminate

f. Under the Access Method tab, select the Access Method**AnyConnect Client**, as shown in Figure 36.

Figure 36. Access Method Tabâ€"This configuration is necessary for defining the SSL VPN client connection types.



Access/Authorization Policy Attributes

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Action
Network ACL Filters (client)
Webtype ACL Filters (clientless)
Functions
Port Forwarding Lists
Bookmarks
Access Method

Access Method:
○ Unchanged
● AnyConnect Client
○ Web-Portal
○ Both-default-Web-Portal
○ Both-default-AnyConnect Client

g. Click**OK**, and then**Apply**.

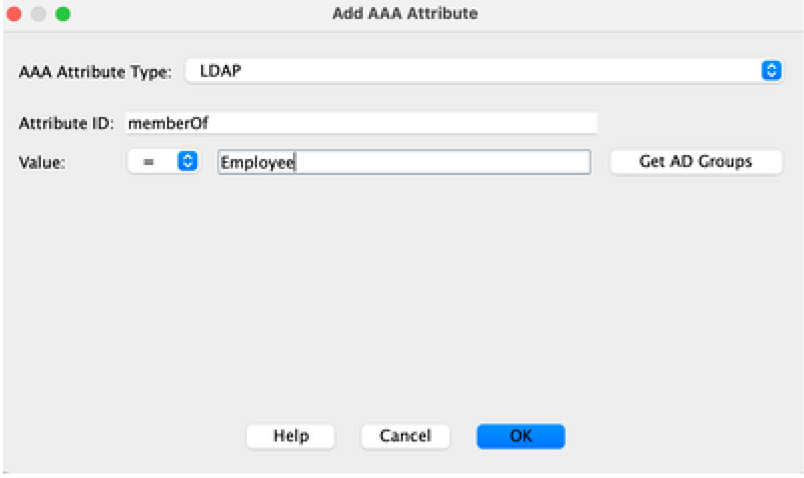
3. Add a second Dynamic Access Policy named**Unmanaged_Endpoints**, as described:

a. Description:**Employee Clientless Access**.

b. From the drop-down list in the previous image of the AAA Attribute Section, select User has ALL of the following AAA Attributes Values .

c. Add (located to the right of the AAA Attribute Type) an AAA Attribute Type (LDAP) as shown in Figures 38 and 39. Click**OK**when complete.

Figure 38. DAP AAA Attributeâ€"AAA Group Membership can be used as DAP criteria to identify an Employee.



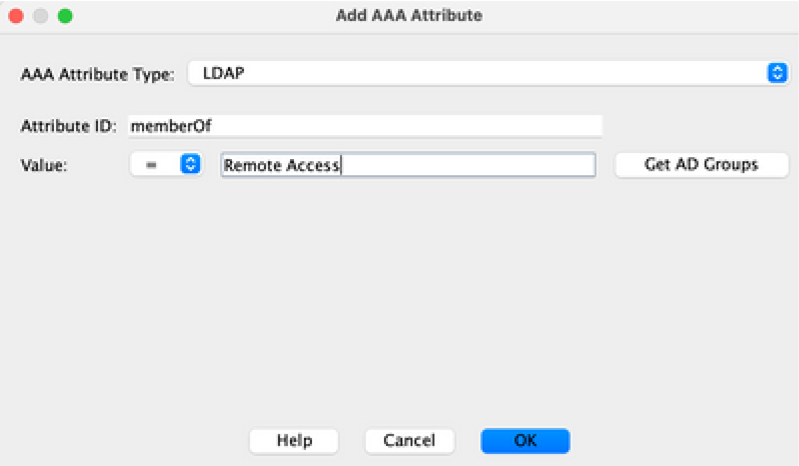
Add AAA Attribute

AAA Attribute Type: LDAP

Attribute ID: memberOf

Value: = Employee

Figure 39. DAP AAA Attributeâ€"AAA Group Membership can be used as a DAP criterion to allow Remote Access capabilities.



Add AAA Attribute

AAA Attribute Type: LDAP

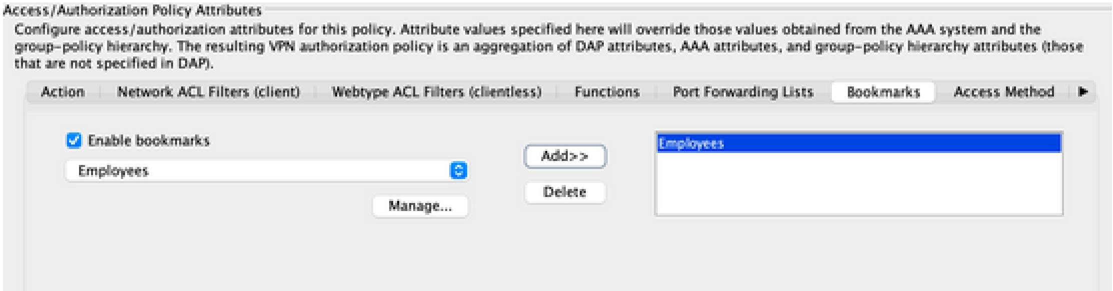
Attribute ID: memberOf

Value: = Remote Access

d. Under the Action tab, verify that the Action is set to**Continue**. (Figure 35)

e. Under the Bookmarks tab, select the list name**Employees**from the drop-down and then click**Add**. Also, verify that the Enable bookmarks are checked as shown in Figure 40.

Figure 40. Bookmarks Tabâ€”This lets you select and configure URL lists for user sessions.



Access/Authorization Policy Attributes

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

☑ Enable bookmarks

Employees

Employees

a. Under the Access Method tab, select the Access Method **Web Portal**. (Figure 36)

2. Click**OK**, and then**Apply**.

   1. Contractors can be identified by DAP AAA Attributes only. As a result, Endpoint Attributes Type: (Policy) can not be configured in Step 4. This approach is only meant to show versatility within DAP.

3. Add a third Dynamic Access Policy named**Guest_Access** with the following:

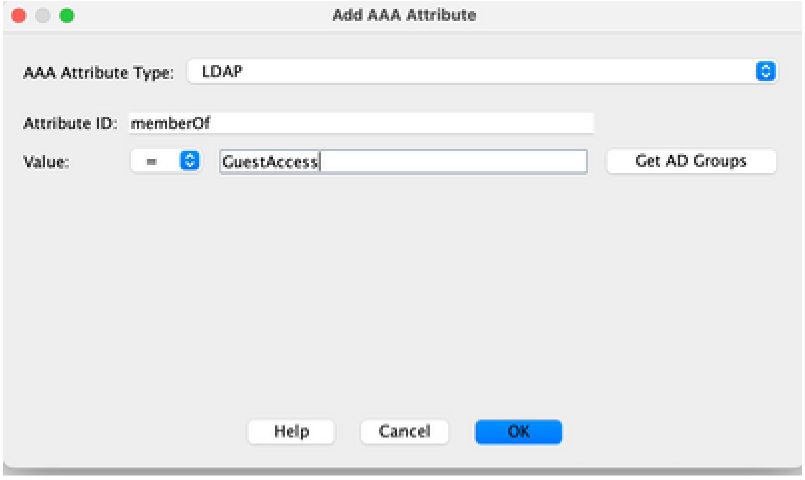
a. Description:**Guest Clientless Access**.

b. Add (located to the right of the Endpoint Attribute box) an Endpoint Attribute Type (Policy) as shown in Figure 37. Click**OK**when complete.

c. In Figure 40, from the drop-down list in the AAA Attribute Section, select User has ALL of the following AAA Attributes Values.

d. Add (located to the right of the AAA Attribute box) an AAA Attribute Type (LDAP) as shown in Figures 41 and 42. Click**OK**when complete.

Figure 41. You can use DAP AAA Attributeâ€”AAA Group Membership as a DAP Criterion to Identify a Contractor

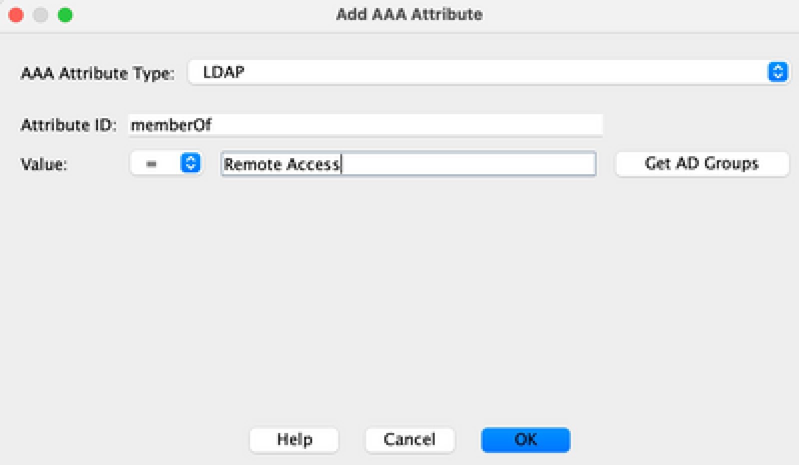


AAA Attribute Type: LDAP

Attribute ID: memberOf

Value: = GuestAccess

Figure 42. DAP AAA Attributeâ€”You can use AAA Group Membership as a DAP Criterion to Allow Remote Access Capabilities



AAA Attribute Type: LDAP

Attribute ID: memberOf

Value: = Remote Access

a. Under the Action tab, verify that the Action is set to **Continue**. (Figure 35)

b. Under the Bookmarks tab, select the list name **Contractors** from the drop-down and then click Add. Also, verify that the **Enable bookmarks** are checked. (Reference Figure 40.)

c. Under the Access Method tab, select the Access Method Web Portal. (Figure 36)

d. Click **OK**, and then **Apply**.

Conclusion

Based on the client Remote Access SSL VPN requirements noted in this example, this solution satisfies the client Remote Access VPN requirements.

With evolving and dynamic VPN environments on the merge, Dynamic Access Policies can adapt and scale to frequent internet configuration changes, various roles each user can inhabit within an organization, and logins from managed and unmanaged remote access sites with different configurations and levels of security.

Dynamic Access Policies are complemented by new and proven legacy technologies including, Advanced Endpoint Assessment, Host Scan, Secure Desktop, AAA, and Local Access Policies. As a result, organizations can confidently deliver secure VPN access to any network resource from any location.

Related Information

- **Cisco Technical Support & Downloads**