

ASA 8.x Dynamic Access Policies (DAP) Deployment Guide

Contents

[Introduction](#)

[DAP and AAA Attributes](#)

[DAP and Endpoint Security Attributes](#)

[Default Dynamic Access Policy](#)

[Configuring Dynamic Access Policies](#)

[Aggregating Multiple Dynamic Access Policies](#)

[DAP Implementation](#)

[Conclusion](#)

[NetPro Discussion Forums - Featured Conversations](#)

[Related Information](#)

Introduction

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 may 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), a new feature introduced in software release v8.0 code of the Adaptive Security Appliance (ASA), enable 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.

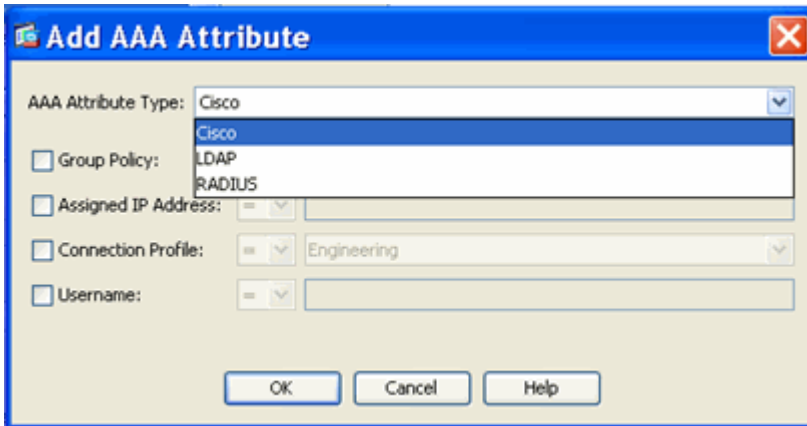
For example, the security appliance grants access to a particular user for a particular session based on the policies you define. It generates a DAP during user authentication by selecting and/or aggregating attributes from one or more DAP records. It selects these DAP records based on the endpoint security 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.

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.

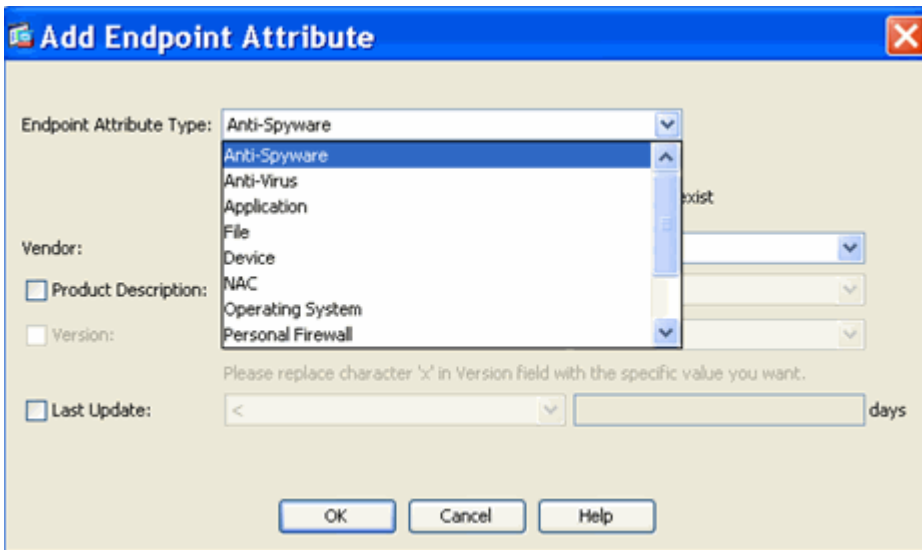
Figure 1. DAP AAA Attribute GUI



DAP and Endpoint Security Attributes

In addition to AAA attributes, the security appliance can also obtain endpoint security attributes by using 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 prior to user authentication. However, AAA Attributes, including the overall DAP record, are validated during user authentication.

Figure 2. Endpoint Attribute GUI



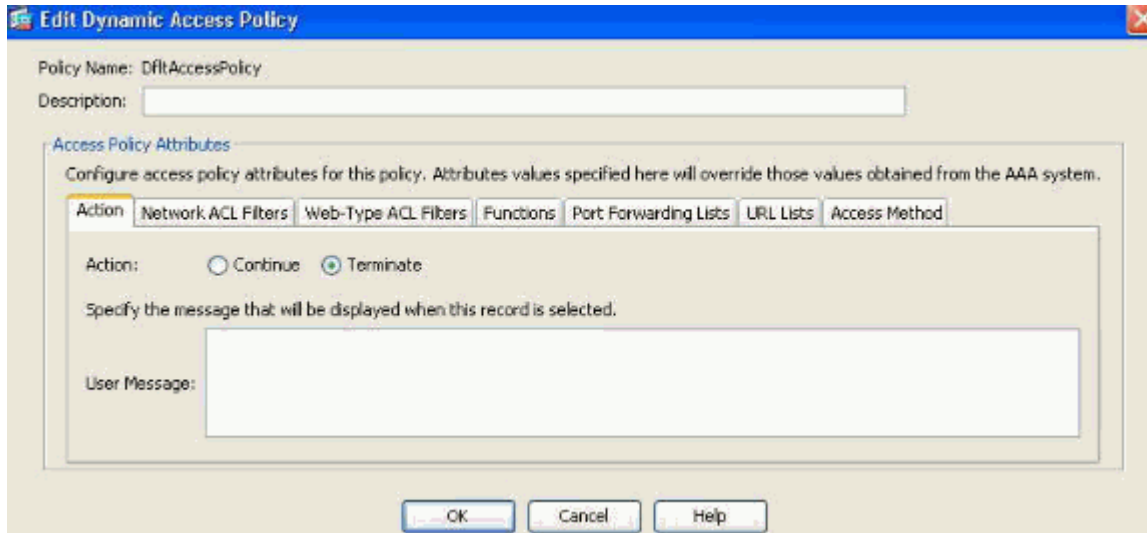
Default Dynamic Access Policy

Prior to 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, i.e., (Tunnel

Groups and Group Policies) or mapped via external AAA servers. However, in the v8.0 release, DAP can be configured to complement or override both local and external access policies.

DAP is always enforced by default. However, for administrators who prefer the legacy policy enforcement method, 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



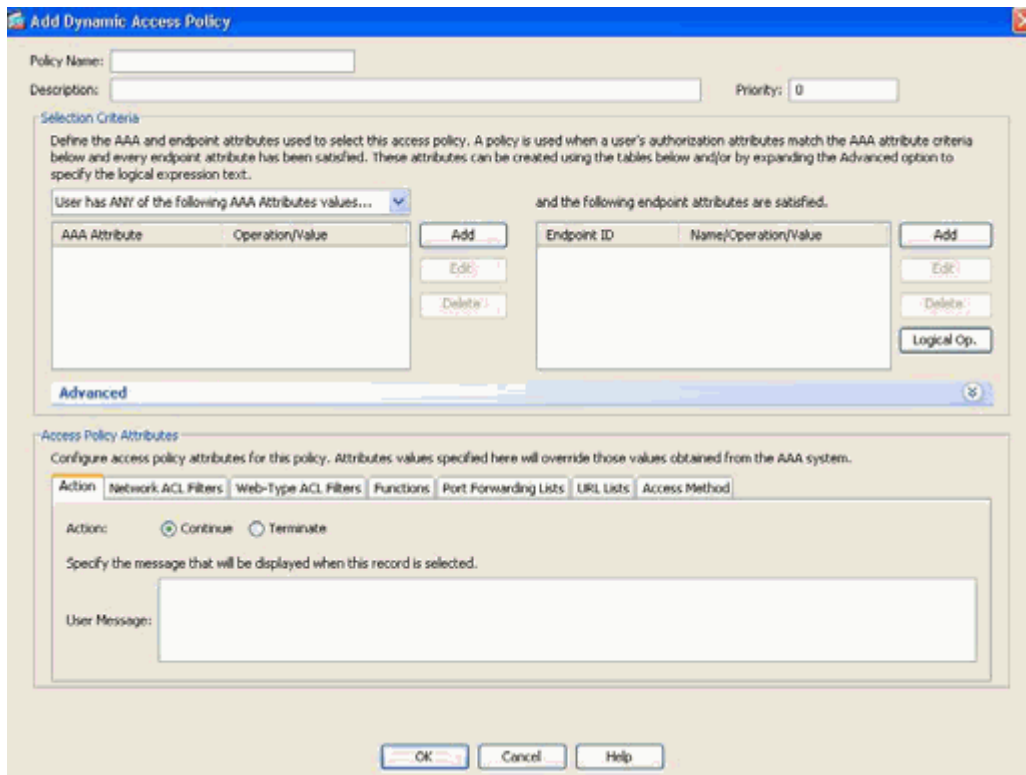
Nevertheless, if any of the default values in a DAP record are changed, for example, the Action: parameter in the DfltAccessPolicy is changed from its default value to Terminate and additional DAP records are not configured, authenticated users will, by default, match the DfltAccessPolicy DAP record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

Consequently, one or more DAP records will 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, will take precedence over legacy policy enforcement.

Configuring Dynamic Access Policies

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

Figure 4. Dynamic Access Policy



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 user'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 ID 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 will also be required to satisfy the endpoint attribute criteria. For example, if the administrator configured Cisco Secure Desktop (CSD) to determine the posture of the connecting endpoint and based on that posture assessment, the endpoint was placed in the CSD Location Unmanaged, the administrator could then use this assessment information as selection criteria for the endpoint attribute shown in Figure 5b.

Figure 5a. AAA Attribute Criteria

Add AAA Attribute

AAA Attribute Type: LDAP

Attribute Name: memberOf

Value: = Contractors

Figure 5b. Endpoint Attribute Criteria

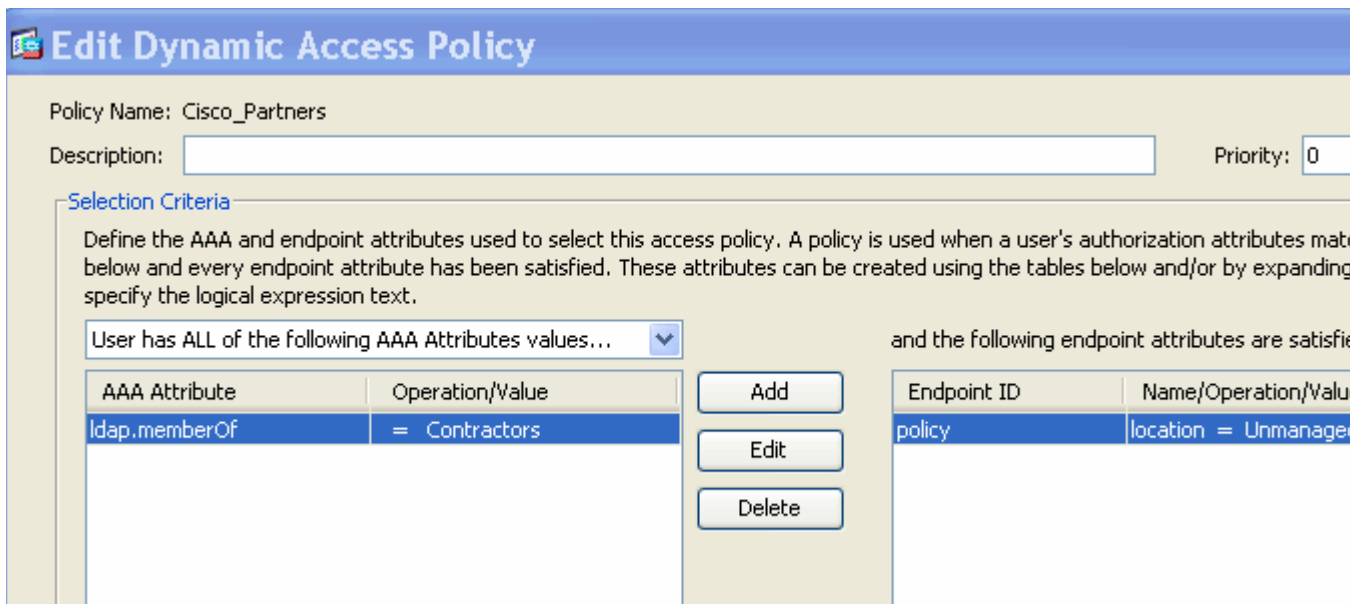
Add Endpoint Attribute

Endpoint Attribute Type: Policy

Location: = Unmanaged

Thus, to match the DAP record shown in Figure 6, the authenticating user must be a member of the Contractors Active Directory group and its connecting endpoint must satisfy the CSD policy value “Unchanged,” to be assigned the DAP record.

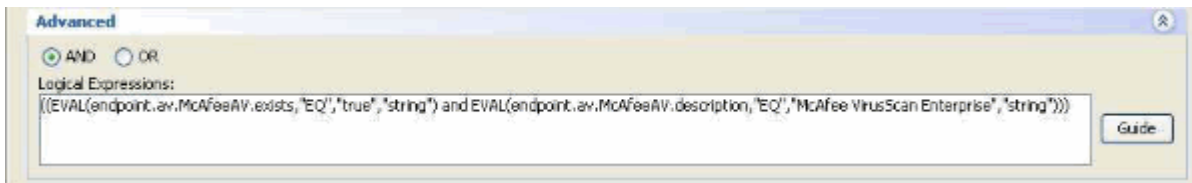
Figure 6. AAA and Endpoint Attribute Criteria Match



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 for adding selection criteria other than what is possible in the AAA and endpoint attribute areas above. 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.

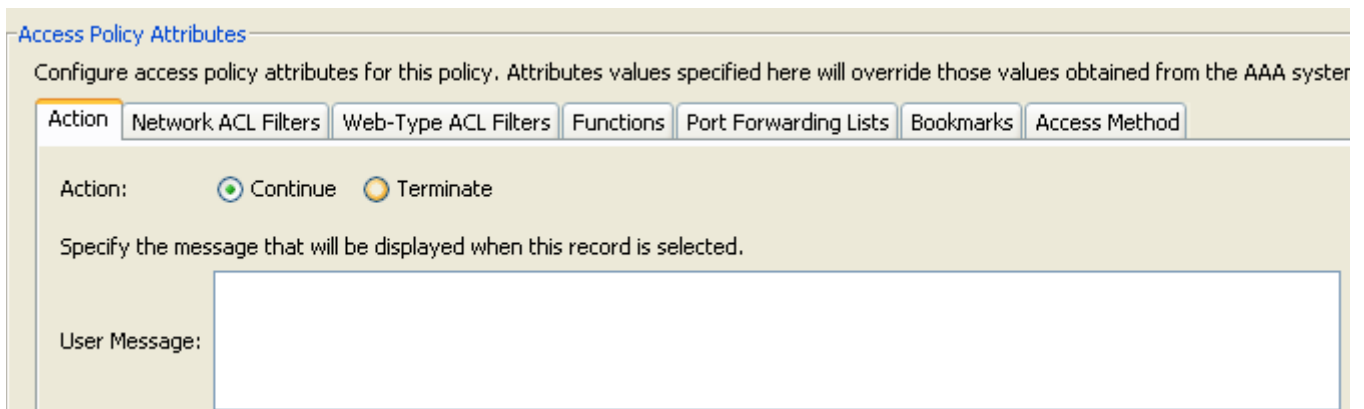
Figure 7. Logical Expression GUI for Advanced Attribute creation



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's authorization attributes match the AAA, Endpoint and/or Logical Expression criteria; the configured access policy attribute values in this section will be enforced. Attribute values specified here will override those values obtained from the AAA system, including those in existing user, group, tunnel group, and default group records.

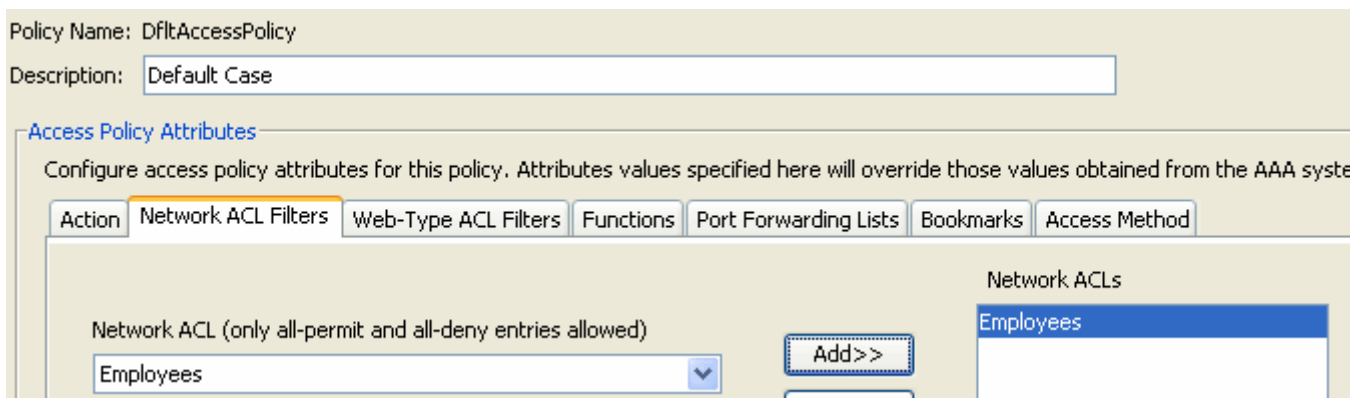
A DAP record has a limited set of attribute values that can be configured. These values fall under the following tabs as shown in the Figures 8 through 14:

Figure 8. Action —Specifies special processing to apply to a specific connection or session.



- Continue—(default) Click to apply access policy attributes to the session.
- Terminate—Click to terminate the session.
- User Message—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.

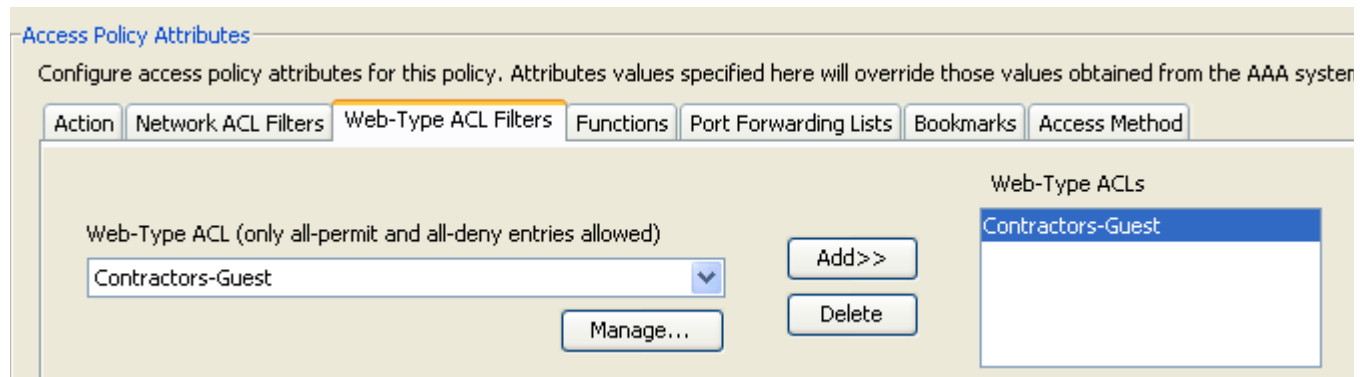
Figure 9. Network ACL Filters Tab—Lets you select and configure network ACLs to apply to this DAP record. An ACL for DAP can contain permit or deny rules, but not both. If an ACL contains both permit and deny rules, the security appliance rejects the ACL configuration.



- Network ACL drop-down box—Select already configured network 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—Click to add, edit, and delete network ACLs.
- Network ACL list—Displays the network ACLs for this DAP record.
- Add—Click to add the selected network ACL from the drop-down box to the Network ACLs list on the right.

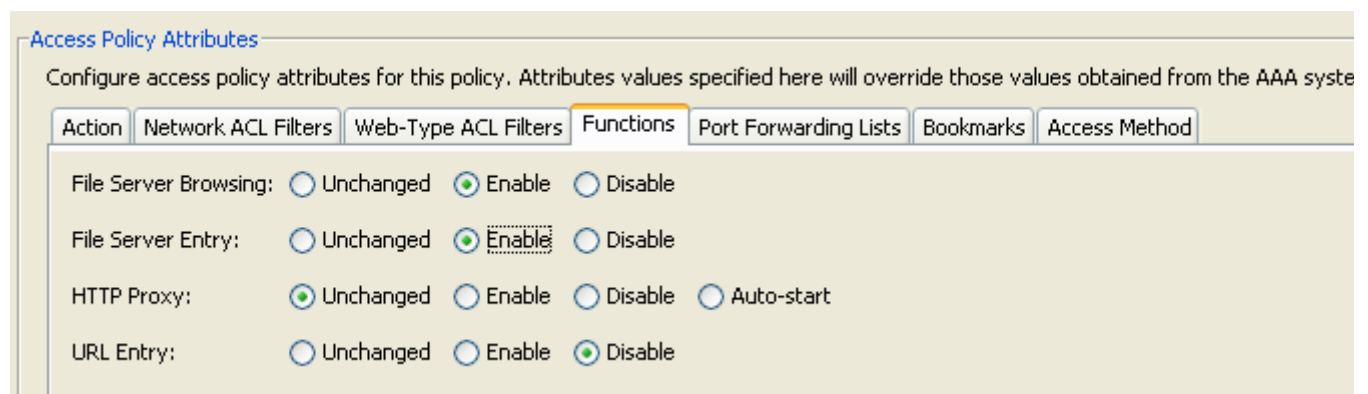
- Delete—Click to delete a highlighted network ACL from the Network ACLs list. You cannot delete an ACL if it is assigned to a DAP or other record.

Figure 10. Web-Type ACL Filters Tab—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.



- Web-Type ACL drop-down box —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... —Click to add, edit, and delete web-type ACLs.
- Web-Type ACL list —Displays the web-type ACLs for this DAP record.
- Add —Click to add the selected web-type ACL from the drop-down box to the Web-Type ACLs list on the right.
- Delete —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.

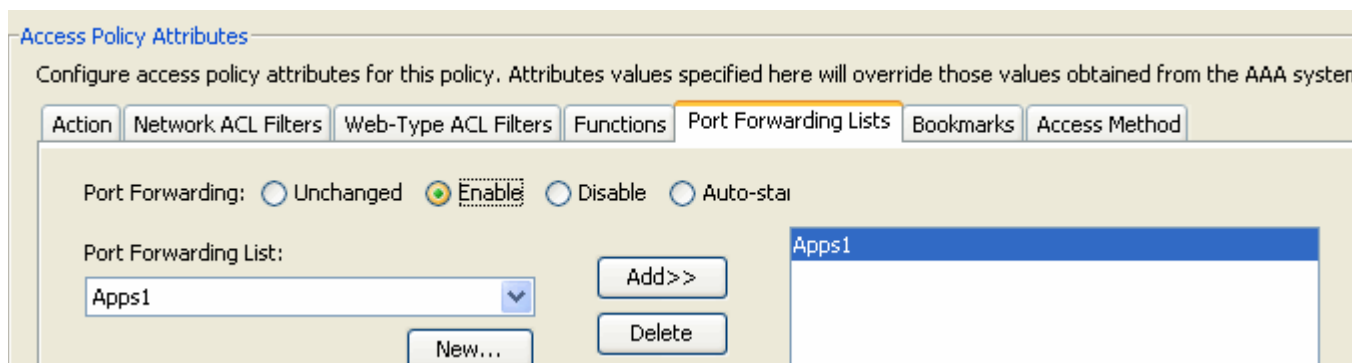
Figure 11. Functions Tab—Lets you configure file server entry and browsing, HTTP proxy, and URL entry for the DAP record.



- File Server Browsing—Enables or disables CIFS browsing for file servers or share features.

- File Server Entry—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 might have to be authenticated before accessing files, depending on network requirements.
- HTTP Proxy—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 mangling/rewriting process while ensuring the continued use of the security appliance. The forwarded proxy modifies the browser’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 Entry—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.
- Unchanged—(default) Click to use values from the group policy that applies to this session.
- Enable/Disable—Click to enable or disable the feature.
- Auto-start—Click to enable HTTP proxy and to have the DAP record automatically start the applets associated with these features.

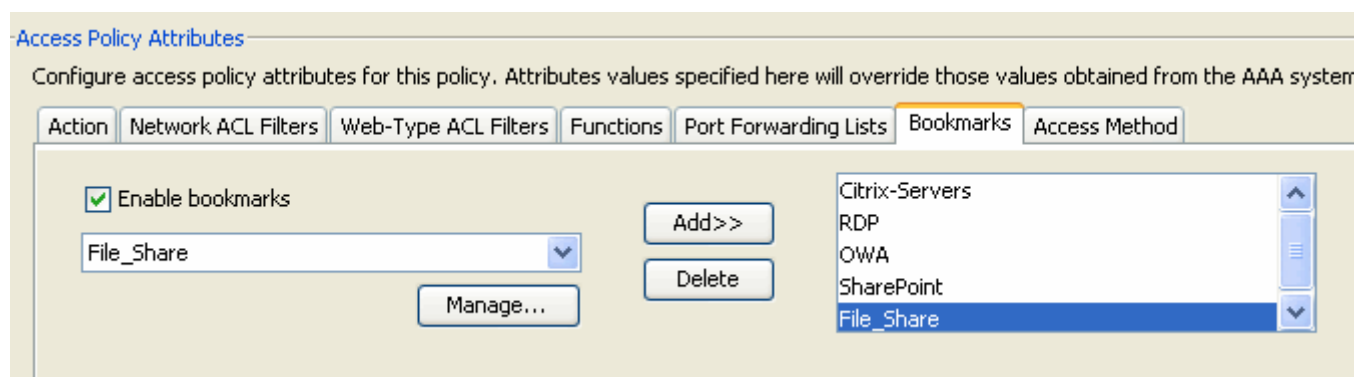
Figure 12. Port Forwarding Lists Tab —Lets you select and configure port forwarding lists for user sessions.



- Port Forwarding—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.
- Unchanged— Click to use values from the group policy that applies to this session.
- Enable/Disable—Click to enable or disable port forwarding.
- Auto-start—Click to enable port forwarding, and to have the DAP record automatically start the port forwarding applets associated with its port forwarding lists.

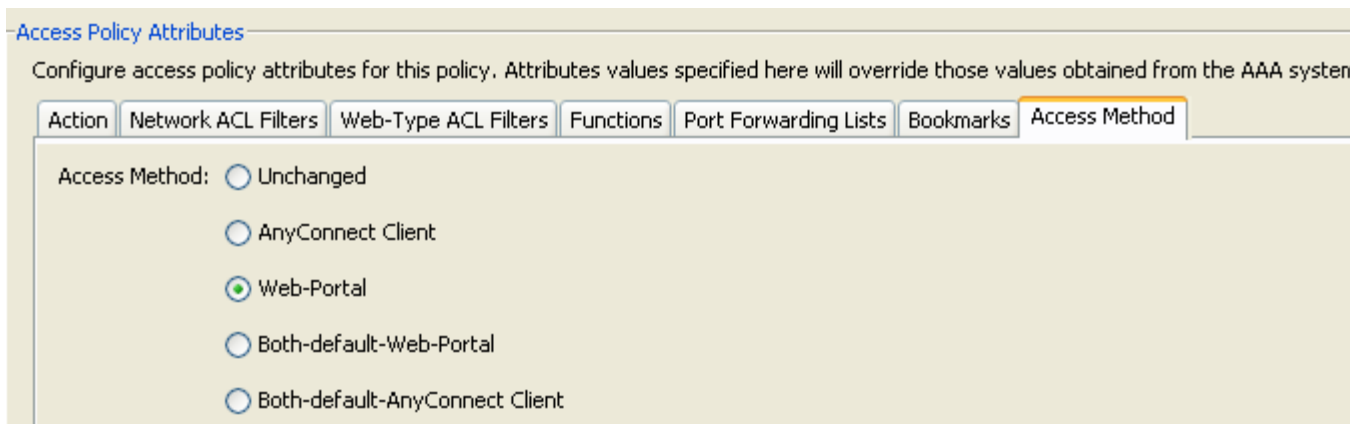
- Port Forwarding List drop-down box—Select already configured port forwarding lists to add to the DAP record.
- New—Click to configure new port forwarding lists.
- Port Forwarding Lists—Displays the port forwarding list for the DAP record.
- Add—Click to add the selected port forwarding list from the drop-down box to the Port Forwarding list on the right.
- Delete—Click to delete 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—Lets you select and configure bookmarks/URL lists for user sessions.



- Enable bookmarks—Click to enable. when this box is not selected, no Bookmark lists display on the portal page for the connection
- Manage—Click to add, import, export, and delete Bookmark lists.
- Bookmarks Lists (Drop-down) —Displays the bookmark lists for the DAP record.
- Add—Click to add the selected bookmark list from the drop-down box to the bookmark list box on the right.
- Delete—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—Lets you configure the type of remote access permitted.



- Unchanged—Continue with the current remote access method set in the group-policy for the session.
- AnyConnect Client—Connect using the Cisco AnyConnect VPN Client.
- Web-Portal—Connect with clientless VPN.
- Both-default-Web-Portal—Connect via either clientless or the AnyConnect client, with a default of clientless.
- Both-default-AnyConnect Client—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 will they take precedence over existing AAA, user, group, tunnel group, and default group records. If additional attribute values outside the scope of DAP is required, for example, Split Tunneling Lists, Banners, Smart Tunnels, Portal Customizations, ...etc, will then need to be enforced via AAA, user, group, tunnel group, and default group records. In this case, those specific attribute values will complement DAP and will not be overriding. Thus, the user will get a cumulative set of attribute values across all records.

Aggregating Multiple Dynamic Access Policies

An administrator can configure multiple DAP records to address many variables. As a result, it is possible for an authenticating user to satisfy the AAA and Endpoint attribute criteria of multiple DAP records. In consequence, Access Policy Attributes will either be consistent or conflict throughout these policies. In this case, the authorized user will 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 Tables below. 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 will be Terminate if the Terminate value is configured in any of the selected DAP records and 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 will 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 will be Auto-start if the Auto-Start value is configured in any of the selected DAP records.

The aggregated attribute value will be Enable 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 will be Disable if there is no Auto-start or Enable value configured in any of the selected DAP records, and the “disable” 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 will be a comma separated string created by linking together the attribute values from the selected DAP records. Any duplicate attribute value in the combined string will be removed. The ordering of the attributes values in the combined string is insignificant.

Table 4. URL List and Port Forward List Attribute

Attribute Name	DAP#1	DAP#2	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 specifies 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 aggregating Network (Firewall) and Web-Type (Clientless) ACL Filter attributes, the DAP Priority and DAP ACL are two major components to consider.

The Priority attribute 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 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 —Displays the priority of the DAP record.

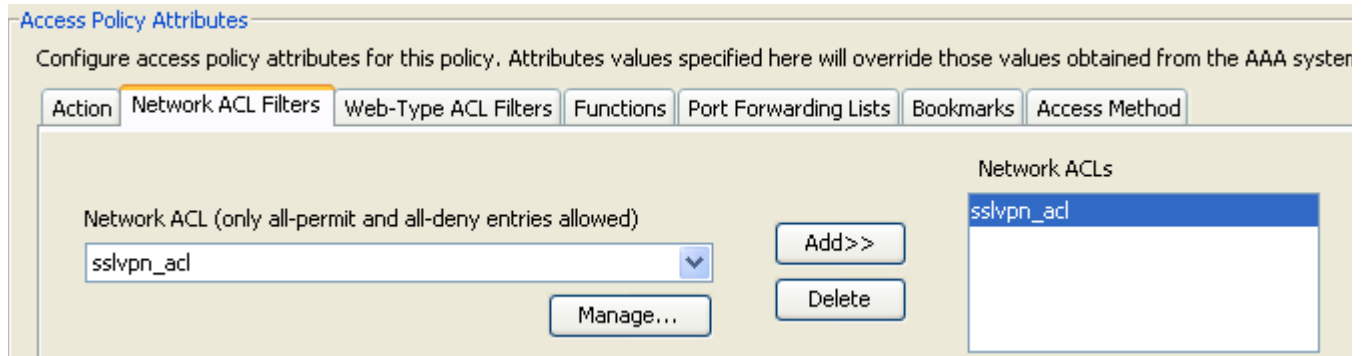
The screenshot shows a configuration window titled "Add Dynamic Access Policy". It contains three input fields: "Policy Name" (empty), "Description" (empty), and "Priority" (set to 0).

- Policy Name—Displays the name of the DAP record.
- Description—Describes the purpose of the DAP record.

The DAP ACL attribute only supports access-lists that conform to either a strict “White-List” or strict “Black-List” ACL model. In a “White-List” ACL model, the access-list entries specify rules that “Permit” access to specified networks or hosts. In a “Black-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 will be rejected as a configuration error when the administrator tries to

add the record. If a conforming access-list is assigned to a DAP record, then any modification to the access-list that changes the conformance characteristic will be rejected as a configuration error.

Figure 16. DAP ACL— Lets you select and configure network ACLs to apply to this DAP record.



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 example below will focus on how a dynamic DAP Firewall Access-List is created specifically. However, a dynamic DAP Clientless Access-List will follow the same process.

First, the ASA will dynamically create 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 will increment to ensure uniqueness)

Second, the ASA will retrieve 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 will reorder the Network-ACLs first by the DAP record Priority number, and then by Black-List first if the Priority value for 2 or more selected DAP records are the same. Following this, the ASA will 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 will merge the Network-ACL entries into the dynamically generated Network-ACL and then return 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 PPPP

DAP Implementation

There are a host of reasons why an administrator should 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 example below, we will configure DAP and its components to identify a connecting endpoint and authorize user access to various network resources.

Test Case – A customer has requested a Proof-of-Concept with the following VPN Access requirements:

- The ability to detect and identify an employees’ endpoint as Managed or Unmanaged. —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 employee’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 employees' 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 should 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 be limited in comparison to an employee's.

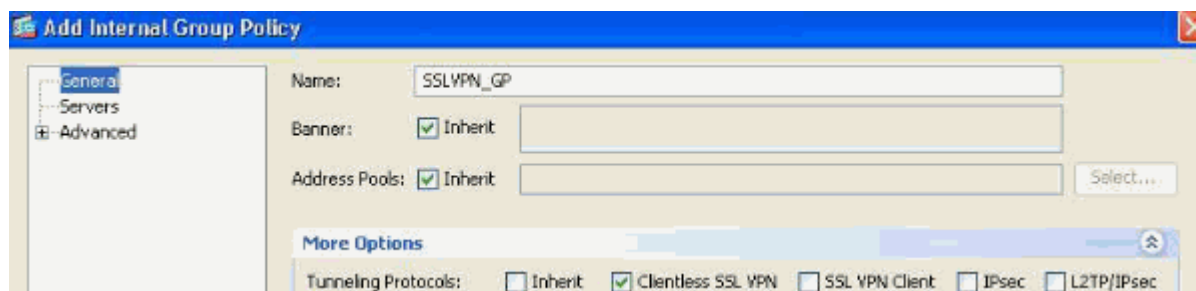
In this example, we will execute a series of configuration steps in an effort to meet the customer's VPN access requirements. There will be configuration steps that are necessary but not directly related to DAP while other configurations will be directly related to DAP. The ASA is very dynamic and can adapt in 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 customers' needs and their environments.

Based on the nature of this paper and the customer's requirements defined, we will use Adaptive Security Device Manager (ASDM) 6.0(x) and focus most of our configurations around DAP. However, we will also configure local Group Policies to show how DAP can complement and/or override local policy attributes. For the basis of this test case, we will 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 Policy— 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 will 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 by doing the following:

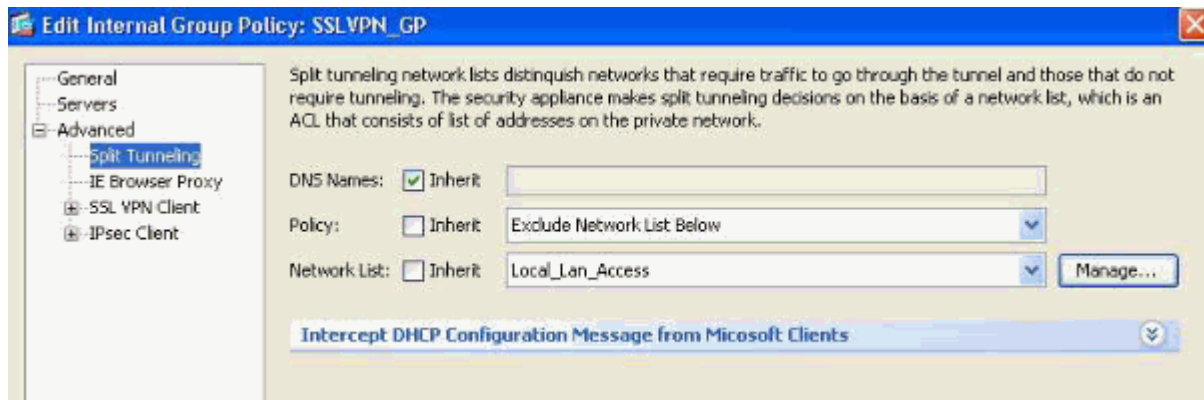
Figure 17. Group Policy —Defines Local VPN Specific Attributes.



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

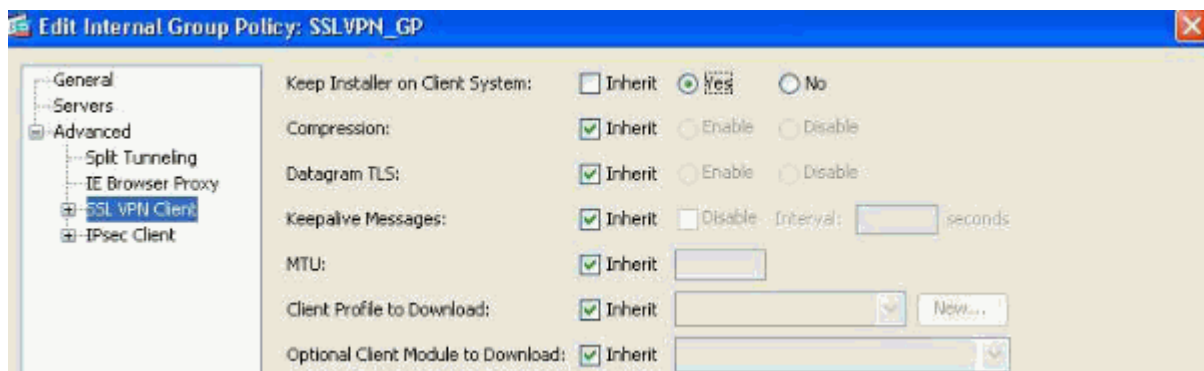
- b. Also under the General link, click **More Options** and configure only the Tunneling Protocol: **Clientless SSLVPN**. (We will configure DAP to override and manage the Access Method.)
- c. Under the Advanced > Split Tunneling link, configure the following:

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



- a. Policy: Uncheck **Inherit** and select **Exclude Network List Below**.
- b. Network List: Uncheck **Inherit** and select the list name **Local_Lan_Access**. (Assumed preconfigured.)
- d. Under the Advanced > SSL VPN Client link, configure the following:

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



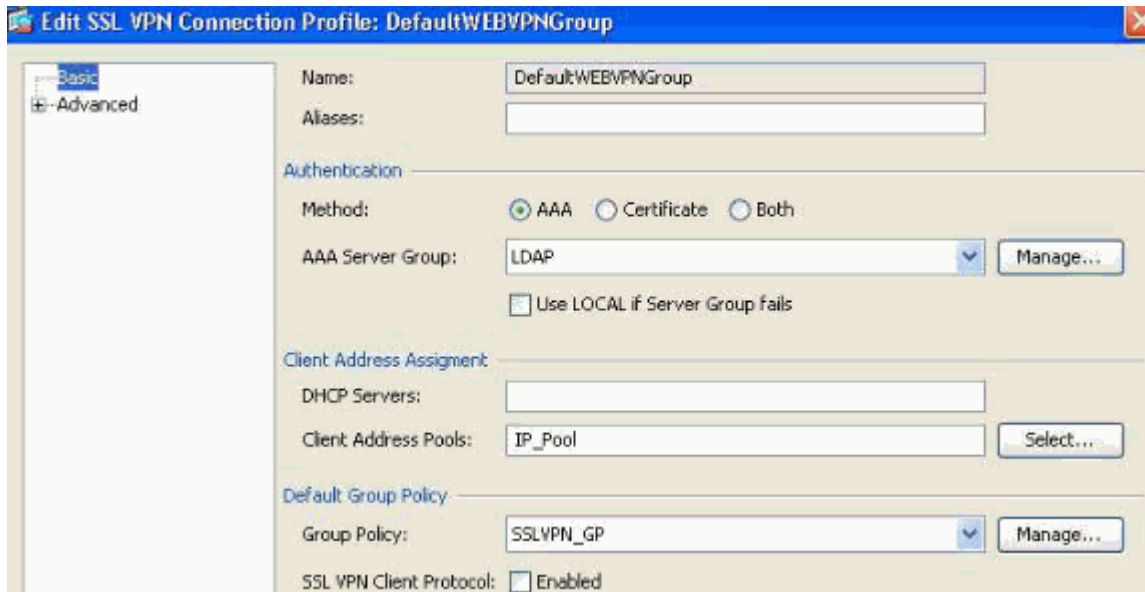
- e. Keep Installer on Client System: Uncheck **Inherit** and then select **Yes**.
- f. Click **OK** then **Apply**.
- g. Apply your configuration changes.

Defining a Connection Profile—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 will be subjected to the attributes defined here as well as attributes defined in the SSLVPN_GP Group Policy. (This Profile will also be used to define both Clientless and Client based attributes).

Navigate to **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** and configure the following:

Figure 20. Connection Profile —Defines Local VPN Specific Attributes.



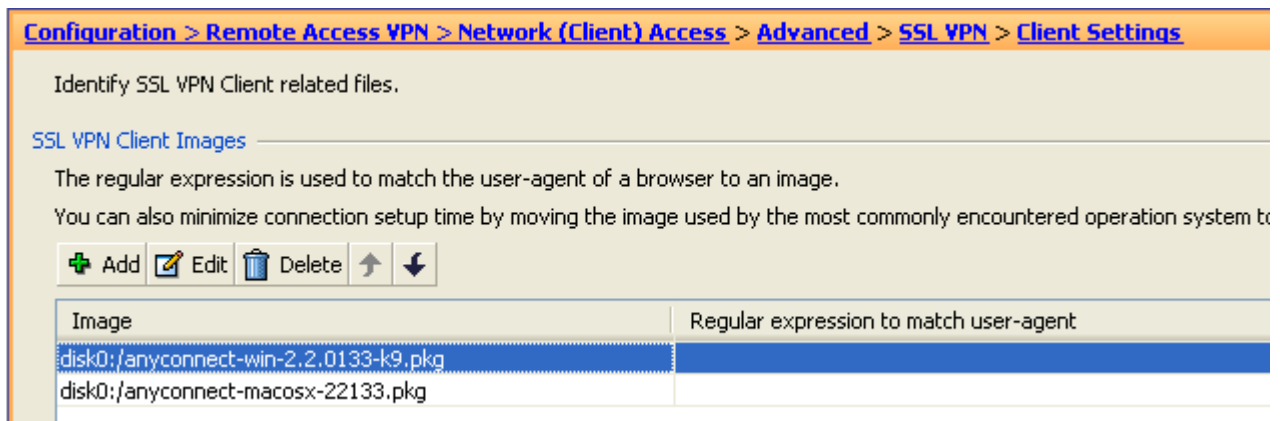
- a. Under the Connection Profiles section, Edit the DefaultWEBVPNGroup and under the Basic link configure the following:
 - a. Authentication—Method: **AAA**
 - b. Authentication—AAA Server Group: **LDAP** (Assumed preconfigured)
 - c. Client Address Assignment—Client Address Pools: **IP_Pool** (Assumed preconfigured)
 - d. Default Group Policy—Group Policy: Select **SSLVPN_GP**
- b. Apply your configurations changes.

Defining an IP interface for SSL VPN connectivity—This configuration is necessary for terminating Client and Clientless SSL connections on a specified interface.

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

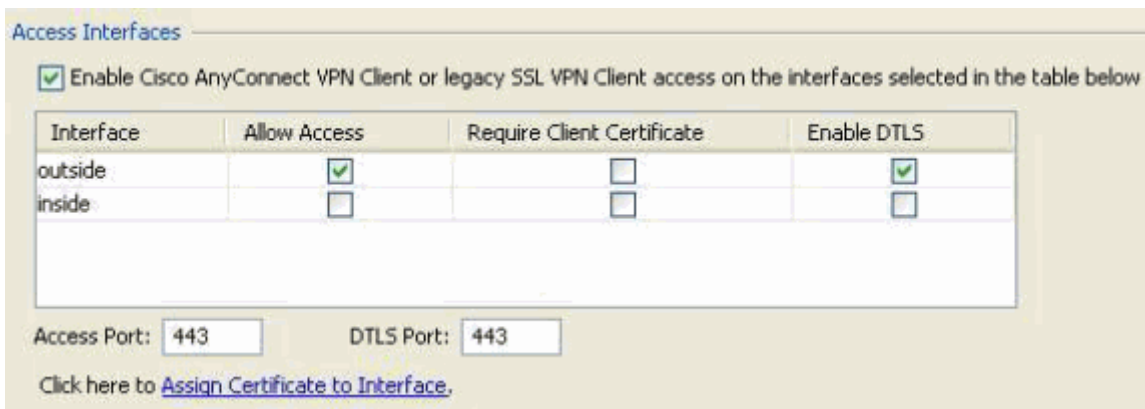
1. Navigate to **Configuration > Remote Access VPN > Network (Client)Access > Advanced > SSL VPN > Client Settings**, and Add the following SSL VPN Client Image from the ASA Flash file system: (This image can be downloaded from CCO, www.cisco.com)

Figure 21. SSL VPN Client Image Install—Defines the SSLVPN (AnyConnect) Client image to be pushed to connecting endpoints.



- a. **anyconnect-win-2.x.xxx-k9.pkg**
 - b. Click **OK**, **OK** again, and then **Apply**.
2. **Navigate to Configuration > Remote Access VPN > Network (Client)Access > SSL VPN Connection Profiles**, and enable the following:

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

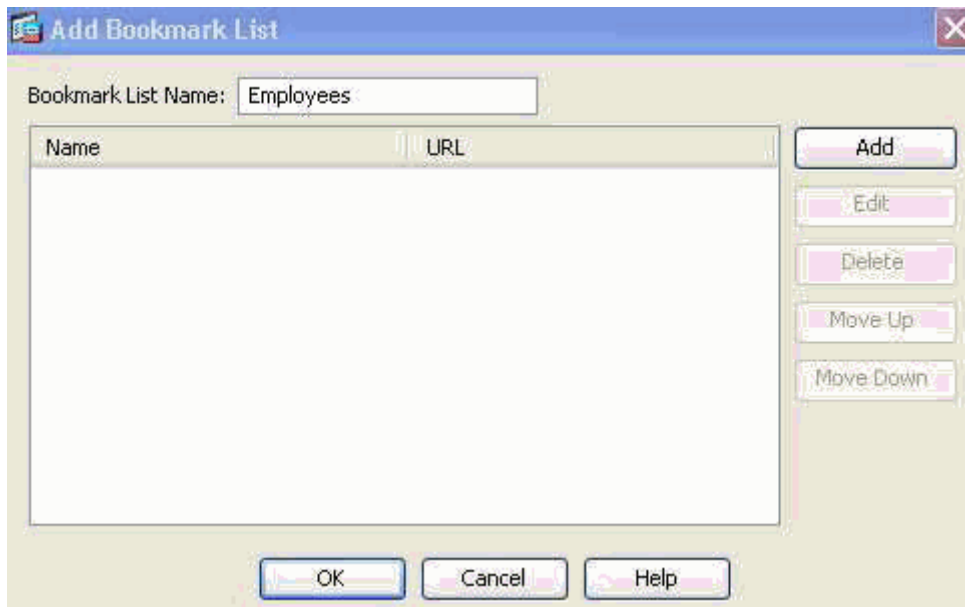


- a. Under the Access Interface section, enable: **“Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the table below.”**
- b. Also under the Access Interfaces section, check **Allow Access** on the outside interface. (This configuration will also enable SSL VPN Clientless access on the outside interface.)
- c. Click **Apply**.

Defining Bookmark Lists (URL Lists) for Clientless Access—This configuration is necessary for defining a web based application to be published on the Portal. We will define 2 URL Lists, one for Employees and the other for Contractors.

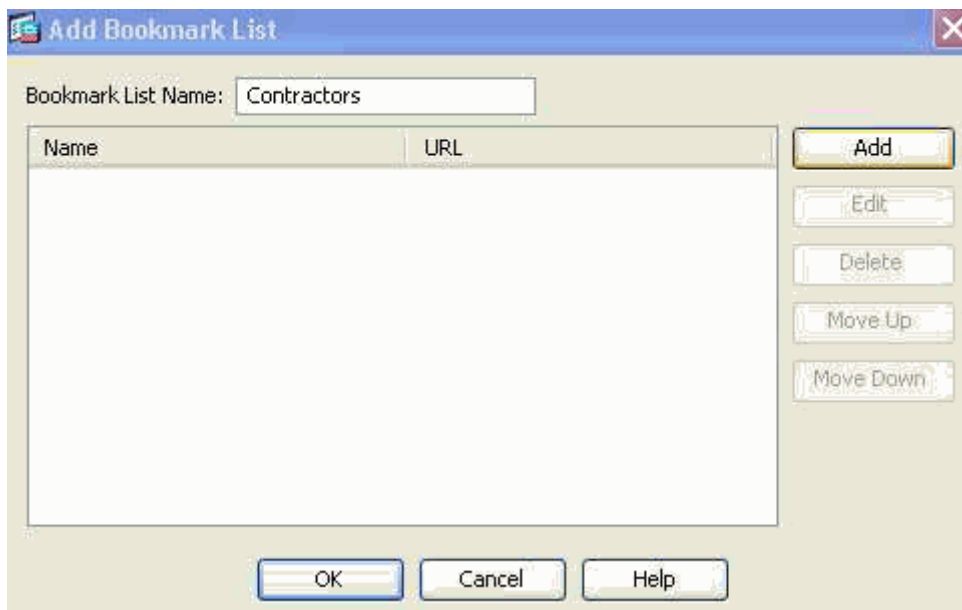
1. Navigate to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks**, click + **Add** and configure the following:

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



- a. Bookmark List Name: **Employees**, then click **Add**.
 - b. Bookmark Title: **Company Intranet**
 - c. URL Value: **http://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 —Customized for Guest access.



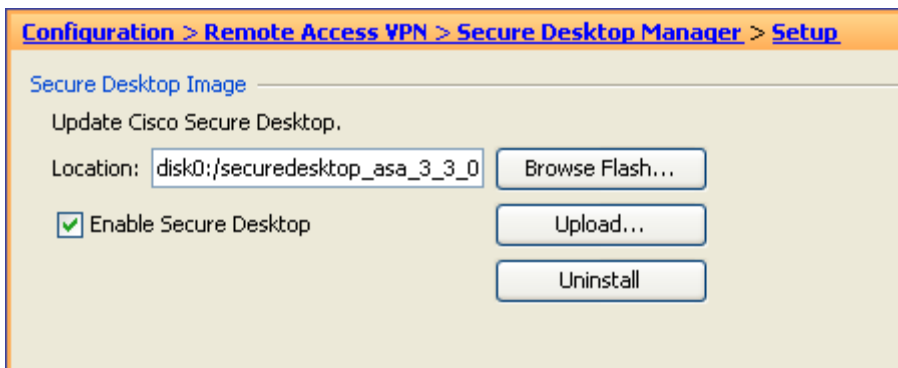
- a. Bookmark List Name: **Contractors**, then click **Add**.
- b. Bookmark Title: **Guest Access**
- c. URL Value: **http://company.contractors.com**
- d. Click **OK** and then **OK** again.
- e. Click **Apply**.

Cisco Secure Desktop —this configuration is necessary for defining Endpoint Assessment attributes. Based on the criteria to be satisfied, connecting endpoints will be classified as Managed or Unmanaged. Cisco Secure Desktop assessments are executed prior to the authentication process.

Configuring Cisco Secure Desktop and a Pre Login Decision Tree for Windows Locations:

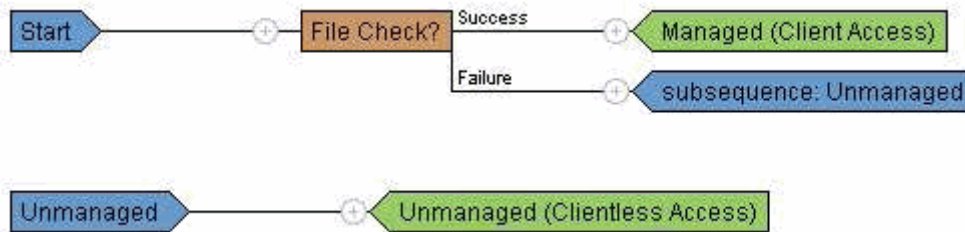
1. Navigate to **Configuration > Remote Access VPN > Secure Desktop Manager > Setup**, and configure the following:

Figure 25. Cisco Secure Desktop Image Install—Defines the Cisco Secure Desktop image to be pushed to connecting endpoints.



- a. Install the **disk0:/securedesktop-asa-3.3.-xxx-k9.pkg** image from the ASA Flash file system.
 - b. Check **Enable Secure Desktop**.
 - c. Click **Apply**.
2. Navigate to **Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy**, and configure the following:

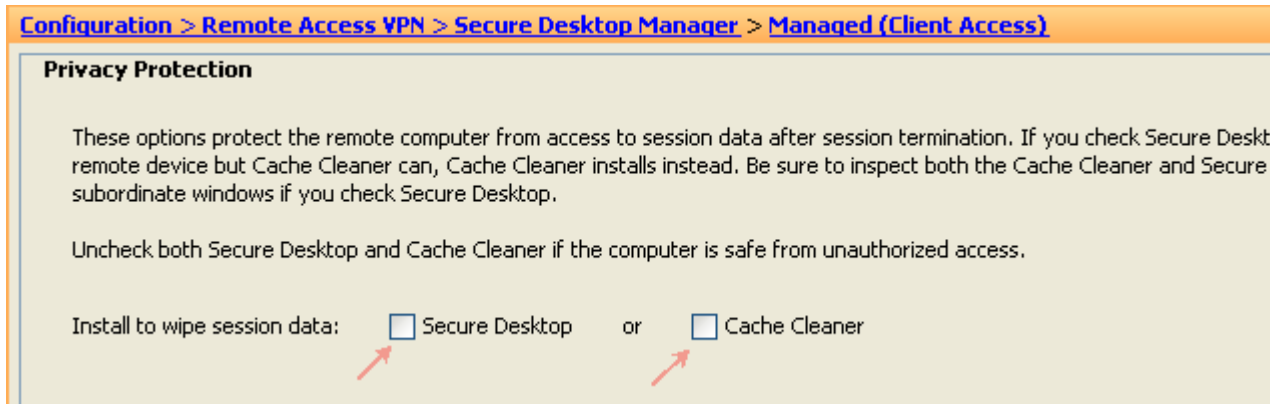
Figure 26. Pre-logout Decision Tree—Customized via File Check to distinguish between a managed endpoint and an unmanaged endpoint.



- a. Click the **Default** node and rename the label **Managed (Client Access)** and then click **Update**.
- b. Click the “+” symbol at the beginning of the **Managed** node.
- c. For the Check, select and Add **File Check** to be inserted.
- d. Enter **C:\managed.txt** for the File Path to “exists” and click **Update**.
- e. Click the **Login Denied** node and then select **Subsequence**.
- f. Enter **Unmanaged** for the label and then click **Update**.
- g. Click the **Login Denied** node and then select **Location**.
- h. Enter **Unmanaged (Clientless Access)** for the label and then click **Update**.

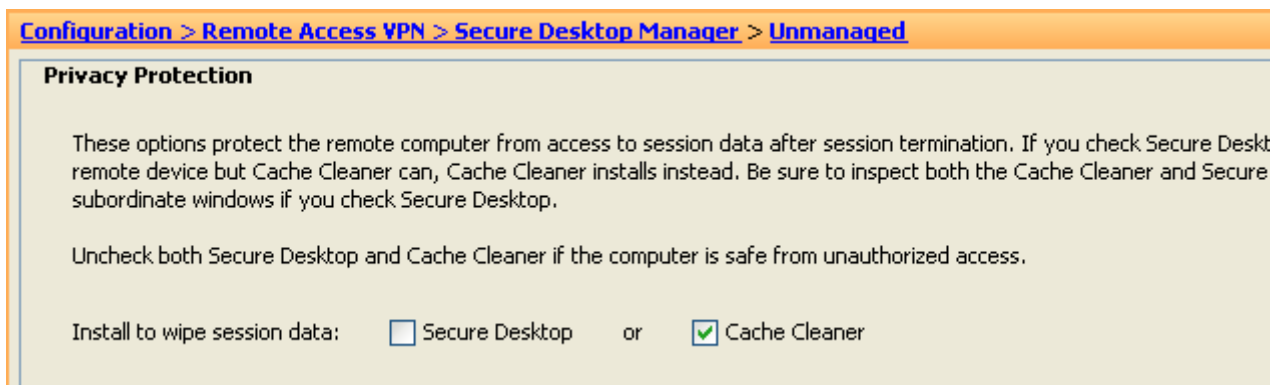
- i. Click **Apply All**.
3. Navigate to **Configuration > Remote Access VPN > Secure Desktop Manager > Managed (Client Access)**, and configure the following under the Location Settings section:

Figure 27. Location/Privacy Protection settings—Secure Desktop (secure vault) and Cache Cleaner (browser cleanup) is not a requirement for Client/Network based access.



- a. Location Module: Uncheck both **Secure Desktop** and **Cache Cleaner** if enabled.
- b. Click **Apply All** if needed.
4. Navigate to **Configuration > Remote Access VPN > Secure Desktop Manager > Unmanaged (Clientless Access)**, and configure the following under the Location Settings section:

Figure 28. Location Settings—The Cache Cleaner (browser cleanup) is a requirement for Clientless based access, however, Secure Desktop (secure vault) is not.

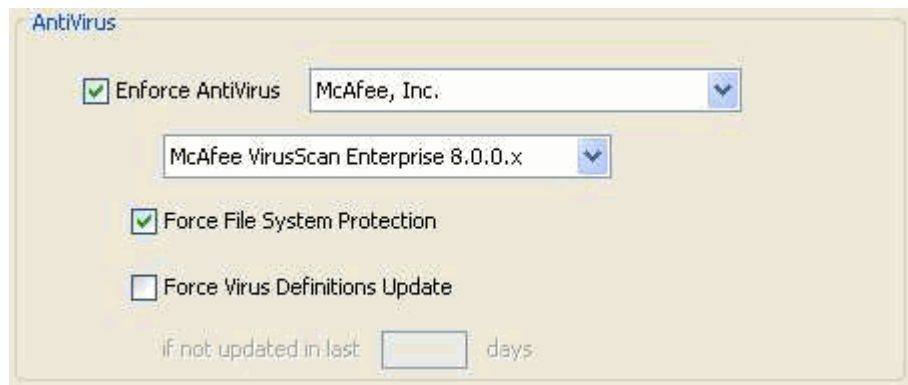


- a. Location Module: Uncheck **Secure Desktop** and check **Cache Cleaner**.
- b. Click **Apply All**.

Advanced Endpoint Assessment—This configuration is necessary for enforcing AntiVirus, AntiSpyware and Personal Firewall on an Endpoint. For example, this assessment will verify if McAfee is running on the connecting endpoint. (Advanced endpoint Assessment is a licensed feature and is not configurable if the Cisco Secure Desktop feature is disabled).

Navigate to **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan**, and configure the following under the Host Scan Extensions section:

Figure 29. AntiVirus Enforcement—Customized for Client/Network based access.



Under the Host Scan Extensions section, configure the following:

- a. Select **Advanced Endpoint Assessment ver 2.3.3.1** and then **Configure**.
- b. Select **Enforce AntiVirus**.
- c. From the Enforce AntiVirus drop down list, select **McAfee, Inc**.
- d. From the AntiVirus Version drop down list select **McAfee VirusScan Enterprise 8.0.0.x**.
- e. Select **Force File System Protection** and then click **Apply All**.

Dynamic Access Policies—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 will 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 will terminate in the default case, e.g. when the endpoint does not match any configured Dynamic Access policies), we will configure the following:

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 will no longer appear.

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

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

Policy Name: DfltAccessPolicy

Description:

Access Policy Attributes

Configure access policy attributes for this policy. Attributes values specified here will override those values obtained from the A

Action: Continue Terminate

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

User Message:

- 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 (located to the right of the Endpoint Attribute box) an Endpoint Attribute Type (Policy) as shown in Figure 31. Click **OK** when complete.

Figure 31. DAP Endpoint Attribute—Cisco Secure Desktop Location will be used as a DAP criterion for Client/Network access.

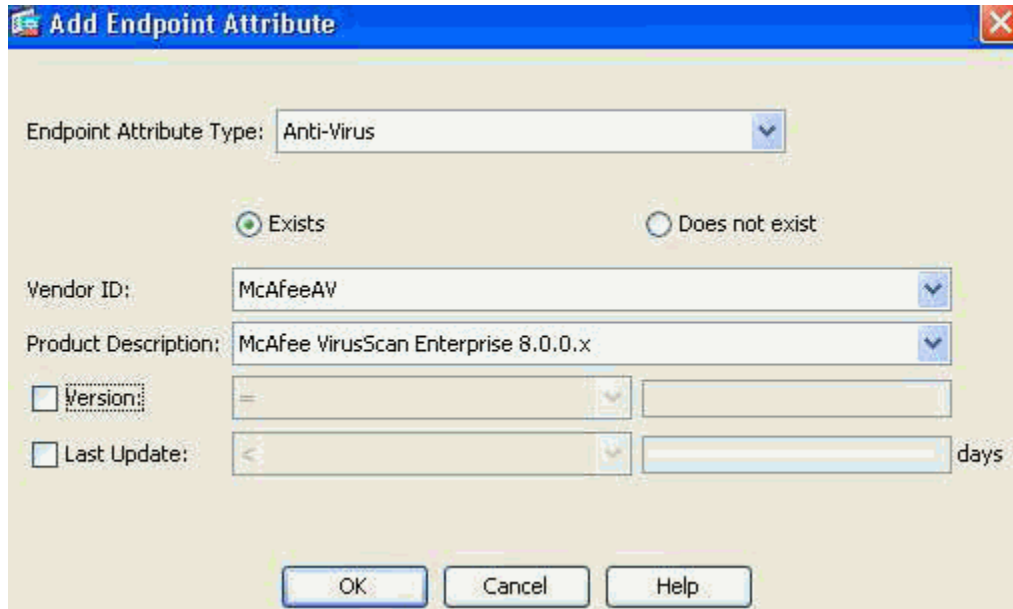
Add Endpoint Attribute

Endpoint Attribute Type:

Location:

- c. Add a second Endpoint Attribute Type (Anti-Virus) as shown in Figure 32. Click **OK** when complete.

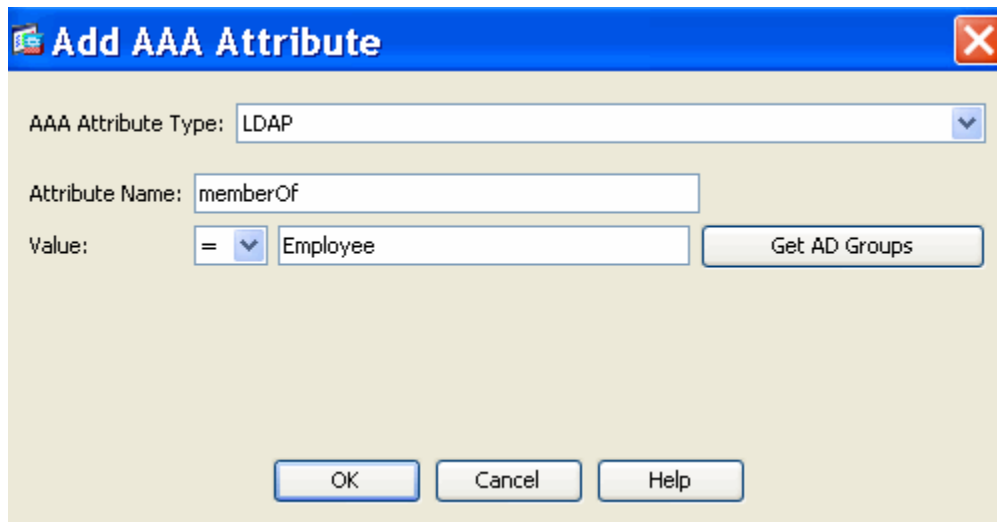
Figure 32. DAP Endpoint Attribute—Advanced Endpoint Assessment AntiVirus will be used as a DAP criterion for Client/Network access.



The screenshot shows the 'Add Endpoint Attribute' dialog box. The 'Endpoint Attribute Type' dropdown is set to 'Anti-Virus'. Below this, there are two radio buttons: 'Exists' (selected) and 'Does not exist'. The 'Vendor ID' dropdown is set to 'McAfeeAV' and the 'Product Description' dropdown is set to 'McAfee VirusScan Enterprise 8.0.0.x'. There are two checkboxes: 'Version' and 'Last Update', each with a corresponding input field. The 'Version' field contains '=' and the 'Last Update' field contains '<'. At the bottom, there are three buttons: 'OK', 'Cancel', and 'Help'.

- d. From the drop down list above the AAA Attribute section, select **User has ALL of the following AAA Attributes Values...**
- e. Add (located to the right of the AAA Attribute box) an AAA Attribute Type (LDAP) as shown in Figure 33 and 34. Click **OK** when complete.

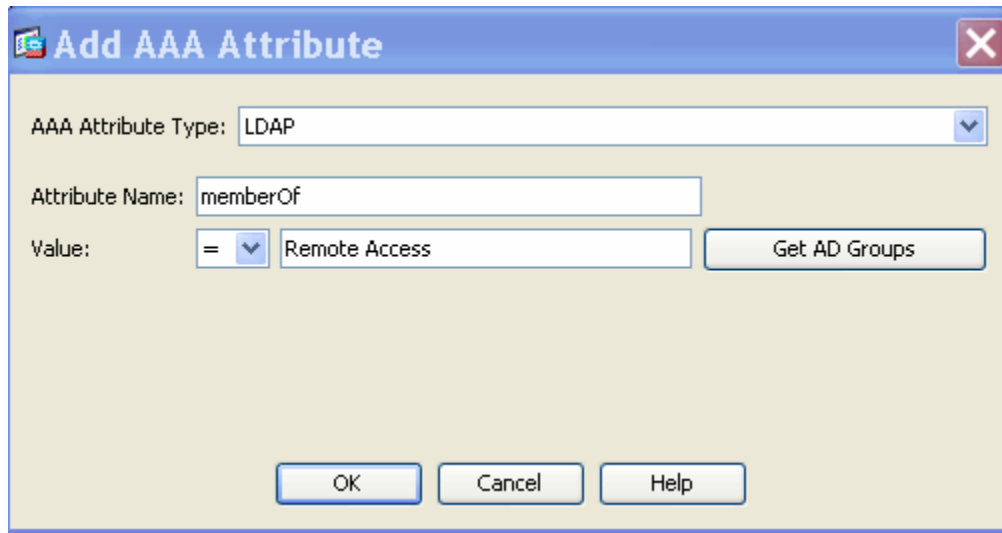
Figure 33. DAP AAA Attribute—AAA Group Membership will be used as a DAP criterion to identify an Employee.



The screenshot shows the 'Add AAA Attribute' dialog box. The 'AAA Attribute Type' dropdown is set to 'LDAP'. The 'Attribute Name' text box contains 'memberOf'. The 'Value' dropdown is set to 'Employee'. To the right of the 'Value' field is a 'Get AD Groups' button. At the bottom, there are three buttons: 'OK', 'Cancel', and 'Help'.

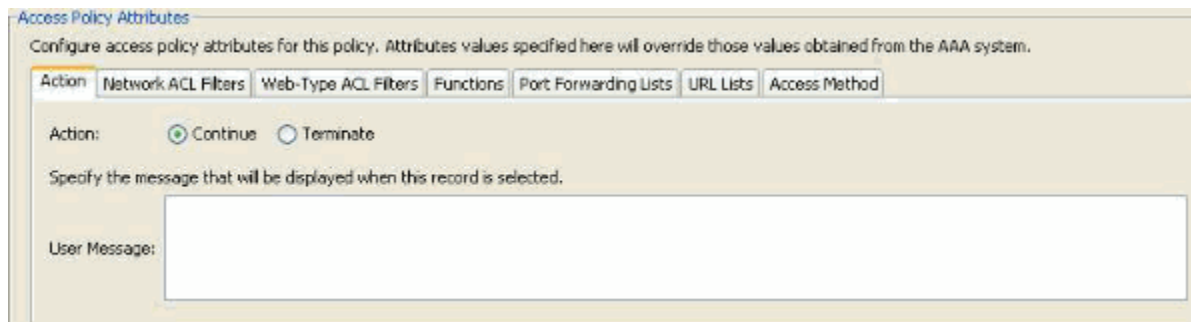
Figure 34. DAP AAA Attribute—AAA Group Membership will be used as a DAP

criteria to allow Remote Access capabilities.



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

Figure 35. Action Tab—This configuration is necessary for defining special processing for a specific connection or session. VPN access will be denied if a DAP record is match and the Action is set to Terminate.



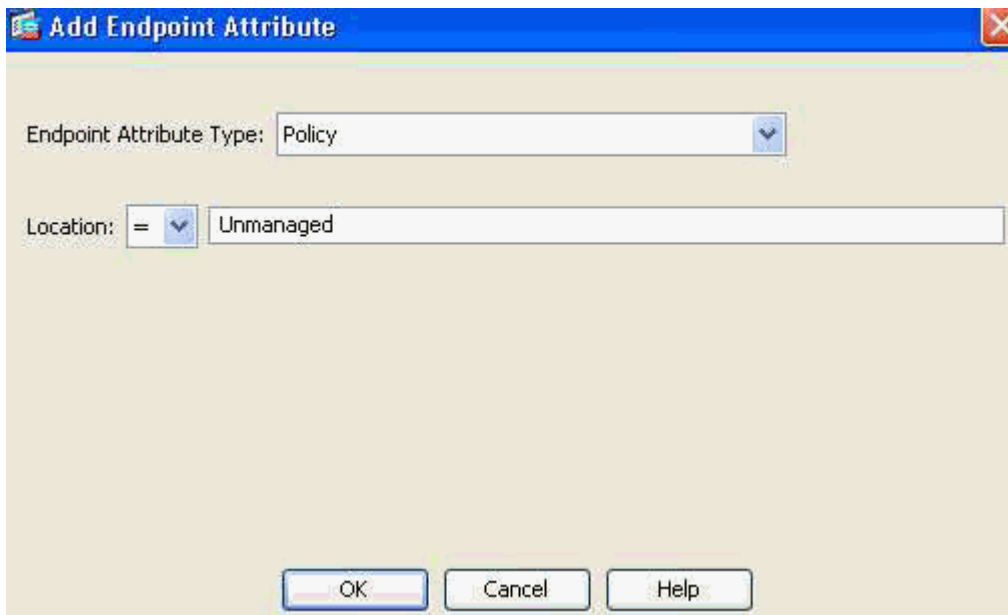
- g. Under the Access Method tab, select the Access Method **AnyConnect Client**, as shown in Figure 36.

Figure 36. Access Method Tab—This configuration is necessary for defining the SSL VPN client connection types.



- h. Click **OK**, and then **Apply**.
3. Add a second Dynamic Access Policy named **Unmanaged_Endpoints**, as follows:
 - a. Description: **Employee 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.

Figure 37. DAP Endpoint Attribute—Cisco Secure Desktop Location will be used as a DAP criteria for Clientless access.



- c. From the drop down list above 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 Figure 38 and 39. Click **OK** when complete.

Figure 38. DAP AAA Attribute—AAA Group Membership will be used as a DAP criteria to identify an Employee.

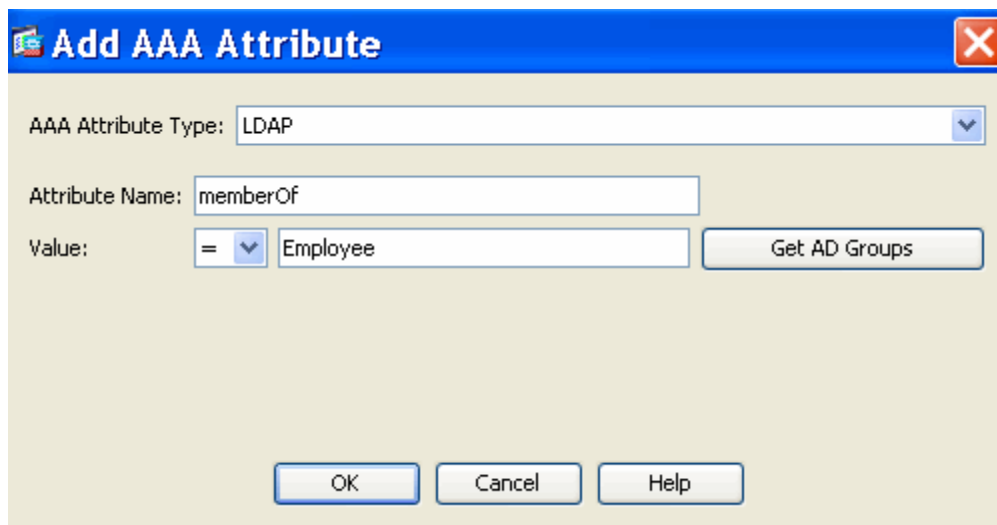
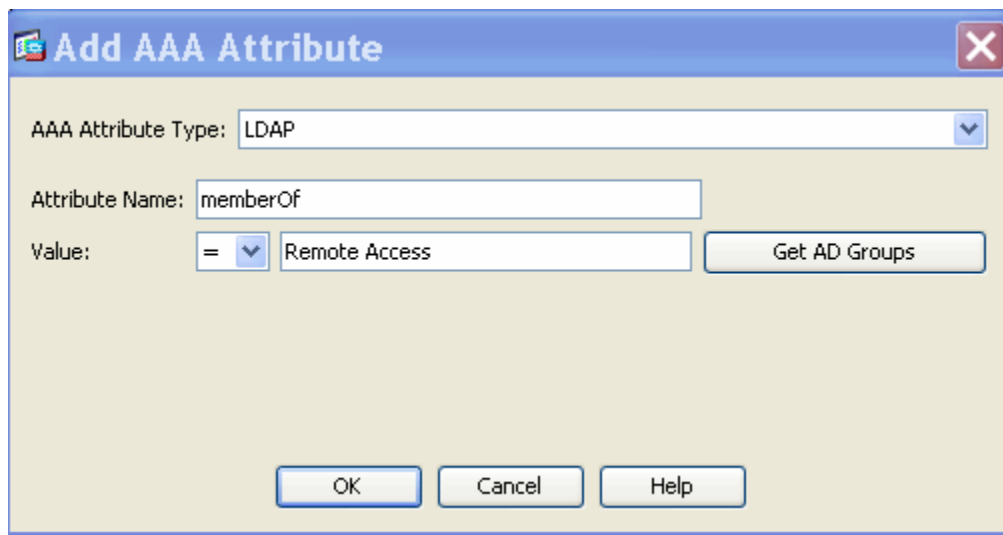
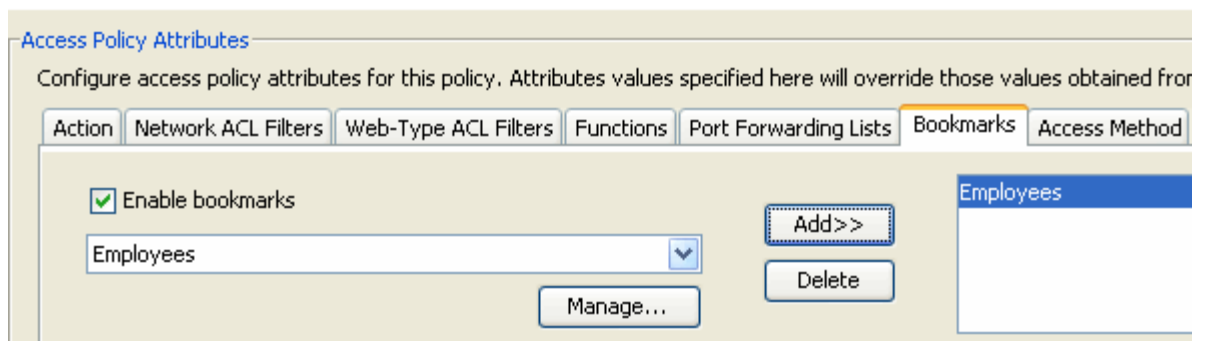


Figure 39. DAP AAA Attribute—AAA Group Membership will be used as a DAP criterion to allow Remote Access capabilities.



- e. Under the Action tab, verify that the Action is set to **Continue**. (Reference Figure 35.)
- f. Under the URL List tab, select the list name **Employees** from the drop-down and then click **Add**. Also, verify that the Enable URL lists is checked as shown in Figure 40.

Figure 40. URL Lists Tab—Lets you select and configure URL lists for user sessions.



- g. Under the Access Method tab, select the Access Method **Web-Portal**. (Reference Figure 36.)
- h. Click **OK**, and then **Apply**.

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

4. Add a third Dynamic Access Policy named **Guest_Access** and 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 above. Click **OK** when complete.
 - c. From the drop down list above 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 Figure 41 and 42. Click **OK** when complete.

Figure 41. DAP AAA Attribute—AAA Group Membership will be used as a DAP criterion to identify a contractor.

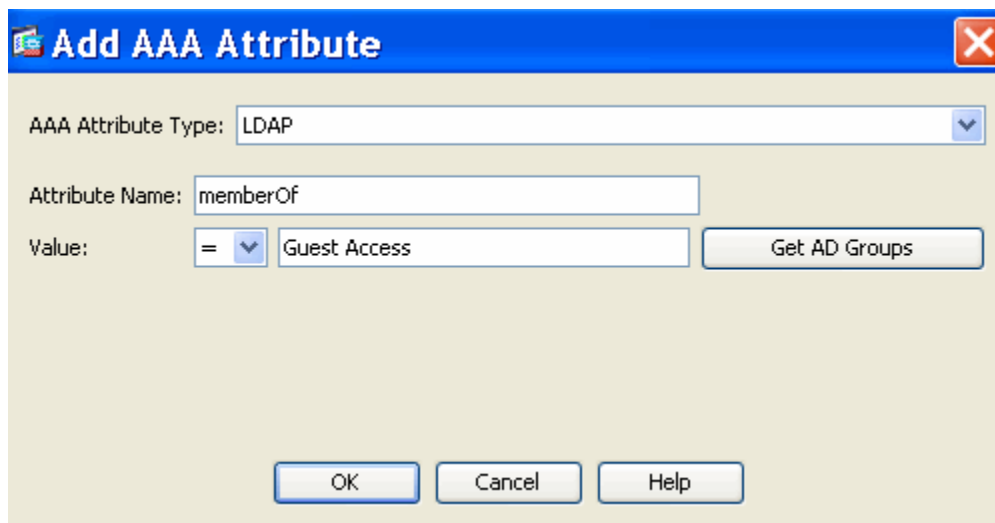


Figure 42. DAP AAA Attribute—AAA Group Membership will be used as a DAP criterion to allow remote access capabilities.



- e. Under the Action tab, verify that the Action is set to **Continue**. (Reference Figure 35.)
- f. Under the URL List tab, select the list name **Contractors** from the drop-down and then click Add. Also, verify that the **Enable URL lists** is checked. (Reference Figure 40.)
- g. Under the Access Method tab, select the Access Method **Web-Portal**. (Reference Figure 36.)
- h. Click **OK**, and then **Apply**.

DAP Selection Criteria—Based on that DAP configuration procedures above, your Selection Criteria for the 4 DAP policies defined, should be consistent with Figures 43, 44, 45 and 46.

Figure 43. Managed Endpoints—If the Criteria of this DAP record are satisfied, Employees will have access to corporate resources via a client/network (AnyConnect Client) connection.

Policy Name: Managed_Endpoints

Description: Priority:

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 below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the specify the logical expression text.

User has ALL of the following AAA Attributes values... and the following endpoint attributes are satisfied.

AAA Attribute	Operation/Value
ldap.memberOf	= Employee
ldap.memberOf	= Remote Access

Endpoint ID	Name/Operation/Value
av.McAfeeAV	exists = true description = McAfee Virus
policy	location = Managed

Figure 44. Unmanaged Endpoints—If the Criteria of this DAP record is satisfied, employees will have access to corporate resources via a clientless (portal) connection. A URL list for employees is also applied to this policy.

Policy Name: Unmanaged_Endpoints

Description: Priority:

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 below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the specify the logical expression text.

User has ALL of the following AAA Attributes values... and the following endpoint attributes are satisfied.

AAA Attribute	Operation/Value
ldap.memberOf	= Employee
ldap.memberOf	= Remote Access

Endpoint ID	Name/Operation/Value
policy	location = Unmanaged

Figure 45. Guest Access—If the criteria of this DAP record are satisfied, contractors will have access to corporate resources via a clientless (portal) connection. A URL list for contractors is also applied to this policy.

Policy Name: Guest_Access

Description: Priority:

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 below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the specify the logical expression text.

User has ALL of the following AAA Attributes values... and the following endpoint attributes are satisfied.

AAA Attribute	Operation/Value
ldap.memberOf	= Guest Access
ldap.memberOf	= Remote Access

Endpoint ID	Name/Operation/Value
policy	location = Unmanaged

Figure 46. Default DAP Policy—If the criteria for all DAP records above are not satisfied, employees and contractors will, by default, be denied access.

Policy Name: DfltAccessPolicy

Description:

Access Policy Attributes

Configure access policy attributes for this policy. Attributes values specified here will override those values obtained from the AAA system.

Action: Continue Terminate

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

User Message:

Conclusion

Based on the customer's Remote Access SSL VPN requirements noted in this example, this solution will satisfy their 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 may 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.

NetPro Discussion Forums - Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums - Featured Conversations for Security
Security: Intrusion Detection [Systems]
Cisco IME and Data Archive - Oct 7, 2008 CSM Signature Policy - Oct 7, 2008 Converting Snort Signatures to Cisco IDS/IPS - Oct 7, 2008 IOS IDS vs. ASA Module vs. ISR module vs. Blade vs. Appliance - Oct 7, 2008 IDSM2 and VACLs to capture monitored traffic - Oct 7, 2008
Security: AAA
Dial up Authentication Issues - Oct 7, 2008 Roles of the different access levels - Oct 7, 2008 en pass and en secret with AAA authentication - Oct 7, 2008 AAA configuration on switches 2960 - Oct 7, 2008 per user QoS Policy in ASA - Oct 6, 2008
Security: General
Two vinternal segments on asa - Oct 7, 2008 ASK THE EXPERT - CISCO VIRTUAL OFFICE - Oct 7, 2008 CSA and GPO machine settings - Oct 7, 2008 What is process name "68 Dispaeth Unit" on 515e 7.22? - Oct 7, 2008 SSL Reverse proxy - Oct 7, 2008
Security: Firewalling
Upgrade from Cisco/Linksys RV082 to ASA5505? - Oct 7, 2008 PIX V8.04 Update - Sqlnet Problem - Oct 7, 2008 duplicate MAC addresses on Fa0 and VLAN1 - Why? - Oct 7, 2008 ASAre-booting at random - Oct 7, 2008 ASA5520 stops passing traffic - Oct 7, 2008

Related Information

- [Technical Support & Documentation - Cisco Systems](#)

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)