



## CHAPTER 36

# Configuring Dynamic Access Policies

---

This chapter describes how to configure dynamic access policies. It includes the following sections.

- [Understanding VPN Access Policies](#)
- [Add/Edit Dynamic Access Policies](#)
- [Add/Edit AAA Attributes](#)
- [Retrieve AD Groups from selected AD Server Group](#)
- [Add/Edit Endpoint Attributes](#)
- [Operator for Endpoint Category](#)
- [DAP Examples](#)

## Understanding VPN Access Policies

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 VPN environment than it is in a network with a static configuration.

Dynamic access policies (DAP) on the security appliance let you configure authorization that addresses these many variables. 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. That is, the security appliance grants access to a particular user for a particular session based on the policies you define. It generates a DAP at the time the user connects 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 the AAA authorization information for the authenticated user. It then applies the DAP record to the user tunnel or session.

The DAP system includes the following components that require your attention:

- **DAP Selection Configuration File**—A text file containing criteria that the security appliance uses for selecting and applying DAP records during session establishment. Stored on the security appliance. You can use ASDM to modify it and upload it to the security appliance in XML data format. DAP selection configuration files include all of the attributes that you configure. These can include AAA attributes, endpoint attributes, and access policies as configured in network and web-type ACL filter, port forwarding and URL lists,

- **DfltAccess Policy**—Always the last entry in the DAP summary table, always with a priority of 0. You can configure Access Policy attributes for the default access policy, but it does not contain—and you cannot configure—AAA or endpoint attributes. You cannot delete the DfltAccessPolicy, and it must be the last entry in the summary table.

For more information about Dynamic Access Policies, click the following links:

- [DAP Support for Remote Access Connection Types](#)
- [DAP and AAA](#)
- [DAP and Endpoint Security](#)
- [DAP Connection Sequence](#)
- [Test Dynamic Access Policies](#)
- [DAP Examples](#)

## Configuring Dynamic Access Policies

To configure dynamic access policies, in the Configuration > Remote Access VPN > Network (Client) Access or Clientless SSL VPN Access > Dynamic Access Policies pane in ASDM, perform the following steps:

- 
- Step 1** To include certain antivirus, antispam, or personal firewall endpoint attributes, click the [CSD configuration](#) link near the top of the pane. Then enable Cisco Secure Desktop *and* Host Scan extensions. This link does not display if you have previously enabled both of these features.
- If you enable Cisco Secure Desktop, but do not enable Host Scan extensions, when you apply your changes ASDM includes a link to enable [Host Scan configuration](#).
- Step 2** To create a new dynamic access policy, click **Add**. To modify an existing policy, click **Edit**.
- Step 3** To test already configured policies, click **Test Dynamic Access Policies**.
- 

### Fields

- **Priority**—Displays the priority of the DAP record. 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. Higher numbers have a higher priority, that is 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.
- **Name**—Displays the name of the DAP record.
- **Network ACL List**—Displays the name of the firewall access list that applies to the session.
- **Web-Type ACL List**—Displays the name of the SSL VPN access list that applies to the session.
- **Description**—Describes the purpose of the DAP record.
- **Test Dynamic Access Policies button**—Click to test already configured DAP records.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

## DAP Support for Remote Access Connection Types

The DAP system supports the following remote access methods:

- IPsec VPN
- Clientless (browser-based) SSLVPN
- Cisco AnyConnect SSL VPN
- PIX cut-through proxy (posture assessment not available)

## DAP and AAA

DAP complements AAA services. It provides a limited set of authorization attributes that can override those AAA provides. The security appliance selects DAP records based on the AAA authorization information for the user and posture assessment information for the session. The security appliance can select multiple DAP records depending on this information, which it then aggregates to create 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. For more information about DAP and AAA, see the section, [Add/Edit AAA Attributes](#).

### AAA Attribute Definitions

[Table 36-1](#) defines the AAA selection attribute names that are available for DAP use. The Attribute Name field shows you how to enter each attribute name in a Lua logical expression, which you might do in the Advanced section of the Add/Edit Dynamic Access Policy pane.

**Table 36-1** AAA Selection Attributes for DAP Use

Attribute Type	Attribute Name	Source	Value	Max String Length	Description
Cisco	aaa.cisco.class	AAA	string	64	Group policy name on the security appliance or sent from a Radius/LDAP server as the IETF-Class (25) attribute
	aaa.cisco.ipaddress	AAA	number	-	Assigned IP address for full tunnel VPN clients (IPsec, L2TP/IPsec, SSL VPN AnyConnect)
	aaa.cisco.tunnelgroup	AAA	string	64	Connection profile (tunnel group) name
	aaa.cisco.username	AAA	string	64	Name of the authenticated user (applies if using Local authentication/authorization)

**Table 36-1** AAA Selection Attributes for DAP Use (continued)

LDAP	aaa ldap.<label>	LDAP	string	128	LDAP attribute value pair
RADIUS	aaa radius.<number>	RADIUS	string	128	Radius attribute value pair

Refer to [Security Appliance Supported RADIUS Attributes and Values](#) for a table that lists RADIUS attributes that the security appliance supports.

## DAP and Endpoint Security

The security appliance obtains endpoint security attributes by using posture assessment methods that you configure. These include Cisco Secure Desktop and NAC. For details, see the Cisco Secure Desktop section of ASDM. [Table 36-2](#) identifies each of the remote access protocols DAP supports, the posture assessment tools available for that method, and the information that tool provides.

**Table 36-2** DAP Posture Assessment

Remote Access Protocol	Cisco Secure Desktop	Host Scan	NAC	Cisco NAC Appliance
	Returns files information, registry key values, running processes, operating system	Returns antivirus, antispyware, and personal firewall software information	Returns NAC status	Returns VLAN Type and VLAN IDs
IPsec VPN	— <sup>1</sup>	—	X	X
Cisco AnyConnect VPN	X	X	X	X
Clientless VPN	X	X	—	—
PIX Cut-through Proxy	—	—	—	—

1. — indicates no; X indicates yes

### Endpoint Attribute Definitions

[Table 36-3](#) defines the endpoint selection attribute names that are available for DAP use. The Attribute Name field shows you how to enter each attribute name in a Lua logical expression, which you might do in the Advanced area in the Add/Edit Dynamic Access Policy pane. The *label* variable identifies the application, filename, process, or registry entry.

**Table 36-3** Endpoint Attribute Definitions

Attribute Type	Attribute Name	Source	Value	Max String Length	Description
Antispyware (Requires Cisco Secure Desktop)	endpoint.as. <i>label</i> .exists	Host Scan	true	—	Antispyware program exists
	endpoint.as. <i>label</i> .version		string	32	Version
	endpoint.as. <i>label</i> .description		string	128	Antispyware description
	endpoint.as. <i>label</i> .lastupdate		integer	—	Seconds since update of antispyware definitions

Table 36-3 Endpoint Attribute Definitions (continued)

Attribute Type	Attribute Name	Source	Value	Max String Length	Description
Antivirus (Requires Cisco Secure Desktop)	endpoint.av.label.exists	Host Scan	true	—	Antivirus program exists
	endpoint.av.label.version		string	32	Version
	endpoint.av.label.description		string	128	Antivirus description
	endpoint.av.label.lastupdate		integer	—	Seconds since update of antivirus definitions
Application	endpoint.application.clienttype	Application	string	—	Client type: CLIENTLESS ANYCONNECT IPSEC L2TP
File	endpoint.file.label.exists	Secure Desktop	true	—	The files exists
	endpoint.file.label.lastmodified		integer	—	Seconds since file was last modified
	endpoint.file.label.crc.32		integer	—	CRC32 hash of the file
NAC	endpoint.nac.status	NAC	string	—	User defined status string
Operating System	endpoint.os.version	Secure Desktop	string	32	Operating system
	endpoint.os.servicepack		integer	—	Service pack for Windows
Personal firewall (Requires Secure Desktop)	endpoint.fw.label.exists	Host Scan	true	—	The personal firewall exists
	endpoint.fw.label.version		string	32	Version
	endpoint.fw.label.description		string	128	Personal firewall description
Policy	endpoint.policy.location	Secure Desktop	string	64	Location value from Cisco Secure Desktop
Process	endpoint.process.label.exists	Secure Desktop	true	—	The process exists
	endpoint.process.label.path		string	255	Full path of the process
Registry	endpoint.registry.label.type	Secure Desktop	<i>dword string</i>	—	dword
	endpoint.registry.label.value		string	255	Value of the registry entry
VLAN	endoint.vlan.type	CNA	string	—	VLAN type: ACCESS AUTH ERROR GUEST QUARANTINE ERROR STATIC TIMEOUT

## DAP and Anti-Virus, Anti-Spyware, and Personal Firewall Programs

The security appliance uses a DAP policy when the user attributes matches the configured AAA and endpoint attributes. The Prelogin Assessment and Host Scan modules of Cisco Secure Desktop return information to the security appliance about the configured endpoint attributes, and the DAP subsystem uses that information to select a DAP record that matches the values of those attributes.

Most, but not all, anti-virus, anti-spyware, and personal firewall programs support active scan, which means that the programs are memory-resident, and therefore always running. Host Scan checks to see if an endpoint has a program installed, and if it is memory-resident as follows:

- If the installed program does not support active scan, Host Scan reports the presence of the software. The DAP system selects DAP records that specify the program.
- If the installed program does support active scan, and active scan is enabled for the program, Host Scan reports the presence of the software. Again the security appliance selects DAP records that specify the program.
- If the installed program does support active scan and active scan is disabled for the program, Host Scan ignores the presence of the software. The security appliance does not select DAP records that specify the program. Further, the output of the **debug trace** command, which includes a lot of information about DAP, does not indicate the program presence, even though it is installed.

## DAP Connection Sequence

The following sequence outlines a typical remote access connection establishment.

1. A remote client attempts a VPN connection.
2. The security appliance performs posture assessment, using configured NAC and Cisco Secure Desktop Host Scan values.
3. The security appliance authenticates the user via AAA. The AAA server also returns authorization attributes for the user.
4. The security appliance applies AAA authorization attributes to the session, and establishes the VPN tunnel.
5. The security appliance selects DAP records based on the user AAA authorization information and the session posture assessment information.
6. The security appliance aggregates DAP attributes from the selected DAP records, and they become the DAP policy.
7. The security appliance applies the DAP policy to the session.

## Test Dynamic Access Policies

This pane lets you test the retrieval of the set of DAP records configured on the device by specifying authorization attribute value pairs. To specify these pairs, use the Add/Edit buttons associated with the AAA Attribute and Endpoint Attribute tables. The dialogs that display when you click these Add/Edit buttons are similar to those in the Add/Edit AAA Attributes and Add/Edit Endpoint Attributes dialog boxes.

When you enter attribute value pairs and click the “Test” button, the DAP subsystem on the device references these values when evaluating the AAA and endpoint selection attributes for each record. The results display in the “Test Results” text area.

**Fields**

- Selection Criteria—Determine the AAA and endpoint attributes to test for dynamic access policy retrieval.
- AAA Attributes
  - AAA Attribute—Identifies the AAA attribute.
  - Operation Value—Identifies the attribute as  $\neq$  to the given value.
  - Add/Edit—Click to add or edit a AAA attribute.
- Endpoint Attributes—Identifies the endpoint attribute.
  - Endpoint ID—Provides the endpoint attribute ID.
  - Name/Operation/Value—
  - Add/Edit/Delete—Click to add, edit or delete and endpoint attribute.
- Test Result—Displays the result of the test.
- Test—Click to test the retrieval of the policies you have set.
- Close—Click to close the pane.

**Modes**

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

## Add/Edit Dynamic Access Policies

To add or edit a dynamic access policy, perform the following steps:

- 
- Step 1** At the top of the **Add/Edit Dynamic Access Policy** pane, provide a name (required) and a description (optional) of this dynamic access policy.
  - Step 2** In the **Priority** field, set a priority for the dynamic access policy. The security appliance applies access policies in the order you set here, highest number having the highest priority. In the case of DAP records with the same priority setting and conflicting ACL rules, the most restrictive rule applies.
  - Step 3** In the **Add/Edit AAA Attributes** field, use the ANY/ALL/NONE drop-down box (unlabeled) to choose whether a user must have any, all, or none of the AAA attribute values you configure to use this dynamic access policy.
  - Step 4** To Set AAA attributes, click **Add/Edit** in the AAA Attributes field.
  - Step 5** Before you set endpoint attributes, configure CSD Host Scan.
  - Step 6** To set endpoint security attributes, click **Add/Edit** in the Endpoint ID field.
  - Step 7** You can create multiple instances of each type of endpoint attribute. For each of these types, you need to decide whether the DAP policy should require that the user have all instances of a type (Match all = AND) or only one of them (Match Any = OR). To set this value for each of the end point attributes, click the **Logical Op.** button.

- Step 8** In the **Advanced** field you can enter one or more logical expressions to set AAA or endpoint attributes other than what is possible in the AAA and Endpoint areas above.
- Step 9** To configure network and webtype ACLs, file browsing, file server entry, HTTP proxy, URL entry, port forwarding lists and URL lists, set values in the **Access Policy Attributes** fields.

---

### Fields

- Policy Name—A string of 4 through 32 characters, no spaces allowed.
- Description—(Optional) Describes the purpose of the DAP record. Maximum 80 characters.
- Priority—Sets the priority of the DAP. The security appliance applies access policies in the order you set here, highest number having the highest priority. Values of 0 to 2147483647 are valid. Default = 0.
- ANY/ALL/NONE drop-down box—Set to require that user authorization attributes match any, all, or none of the values in the AAA attributes you are configuring, as well as satisfying every endpoint attribute. Duplicate entries are not allowed. If you configure a DAP record with no AAA or endpoint attributes, the security appliance always selects it since all selection criteria are satisfied.
- AAA Attributes—Displays the configured AAA attributes.
  - Attribute—Displays the name of the AAA attribute.
  - Operation/Value—= !=
  - Add/Edit/Delete —Click to add, edit, or delete the highlighted AAA attribute.
- Endpoint Attributes—Displays the configured endpoint attributes
  - Endpoint ID—Identifies endpoint attributes.
  - Name/Operation/Value—Summarizes configured values for each endpoint attribute.
  - Add/Edit/Delete—Click to add, edit, or delete the highlighted endpoint attribute.



### Note

Cisco Secure Desktop provides the security appliance with all endpoint attributes except Application and NAC. To configure all other endpoint attributes, you must first enable Cisco Secure Desktop, and configure the relevant endpoint attributes there as well.

- Logical Op.—You can create multiple instances of each type of endpoint attribute. Click to configure whether the DAP policy should require that the user have all instances of a type (Match all = AND) or only one of them (Match Any = OR). Be aware that for some endpoint attributes, for example OS, it can never happen that a user would have more than one instance of the attribute.
- Advanced—Click to set additional attributes for the dynamic access policy. Be aware that this is an advanced feature that requires knowledge of Lua.
- AND/OR—Click to define the relationship between the basic selection rules and the logical expressions you enter here, that is, whether the new attributes add to or substitute for the AAA and endpoint attributes already set. The default is AND.
- Logical Expressions—You can configure multiple instances of each type of endpoint attribute. Enter free-form Lua text that defines new AAA and/or endpoint selection attributes. ASDM does not validate text that you enter here; it just copies this text to the DAP XML file, and the security appliance processes it, discarding any expressions it cannot parse.
- Guide—Click to display online help for creating these logical operations.

- Access Policy Attributes—These tabs let you set attributes for network and webtype ACL filters, file access, HTTP proxy, URL entry and lists, port forwarding, and clientless SSL VPN access methods. Attribute values that you configure here override authorization values in the AAA system, including those in existing user, group, tunnel group, and default group records.
- Action Tab
  - 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.

**Note**

You can include in such messages URLs or other embedded text, which require that you use the correct HTML tags.

For example: All contractors please read `<a href='http://wwwin.abc.com/procedure.html'>Instructions</a>` for the procedure to upgrade your antivirus software.

- 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 it.
  - 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 from the security appliance unless you first delete it from DAP records.
- 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 it.
  - 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 from the security appliance unless you first delete it from DAP records.
- 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 shared features.




---

**Note** Browsing requires NBNS (Master Browser or WINS). If that fails or is not configured, we use DNS.

---




---

**Note** The CIFS browse feature does not support internationalization.

---

- File Server Entry—Lets or prohibits 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 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 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.

Using SSL VPN does not ensure that communication with every site is secure. SSL VPN ensures the security of data transmission between the remote user's PC or workstation and the security appliance on the corporate network. If a user then accesses a non-HTTPS web resource (located on the Internet or on the internal network), the communication from the corporate security appliance to the destination web server is not secured.

In a clientless VPN connection, the security appliance acts as a proxy between the end user web browser and target web servers. When a user connects to an SSL-enabled web server, the security appliance establishes a secure connection and validates the server SSL certificate. The end user browser never receives the presented certificate, so therefore cannot examine and validate the certificate. The current implementation of SSL VPN does not permit communication with sites that present expired certificates. Neither does the security appliance perform trusted CA certificate validation. Therefore, users cannot analyze the certificate an SSL-enabled web-server presents before communicating with it.

To limit Internet access for users, select Disable for the URL Entry field. This prevents SSL VPN users from surfing the Web during a clientless VPN connection.

- 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.
- Port Forwarding Lists Tab—Lets you select and configure port forwarding lists for user sessions. Port Forwarding provides access for remote users in the group to client/server applications that communicate over known, fixed TCP/IP ports. Remote users can use client applications that are installed on their local PC and securely access a remote server that supports that application. Cisco

has tested the following applications: Windows Terminal Services, Telnet, Secure FTP (FTP over SSH), Perforce, Outlook Express, and Lotus Notes. Other TCP-based applications may also work, but Cisco has not tested them.



**Note** Port Forwarding does not work with some SSL/TLS versions.



**Caution**

Make sure Sun Microsystems Java™ Runtime Environment (JRE) 1.4+ is installed on the remote computers to support port forwarding (application access) and digital certificates.

- 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 remove the attributes from the running configuration.
- 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 (unlabeled)—Displays the port forwarding lists 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 a port forwarding list from the security appliance unless you first delete it from DAP records.
- URL Lists Tab—Lets you select and configure URL lists for user sessions.
  - Enable URL Lists—Click to enable. When this box is not selected, no URL lists display on the portal page for the connection.
  - URL List drop-down box—select already configured URL lists to add to the DAP record.
  - Manage...—Click to add, import, export, and delete URL lists.
  - URL Lists (unlabeled)—Displays the URL lists for the DAP record.
  - Add—Click to add the selected URL list from the drop-down box to the URL list box on the right.
  - Delete—Click to delete the selected URL list from the URL list box. You cannot delete a URL list from the security appliance unless you first delete it from DAP records.
- Access Method Tab—Lets you configure the type of remote access permitted.
  - Unchanged—Continue with the current remote access method.
  - 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.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

## Add/Edit AAA Attributes

To configure AAA attributes as selection criteria for DAP records, in the **Add/Edit AAA Attributes** dialog box, set the Cisco, LDAP, or RADIUS attributes that you want to use. You can set these attributes either to = or != the value you enter. There is no limit for the number of AAA attributes for each DAP record. For detailed information about AAA attributes, see [AAA Attribute Definitions](#).

### Fields

AAA Attributes Type—Use the drop down box to select Cisco, LDAP or RADIUS attributes:

- Cisco—Refers to user authorization attributes that are stored in the AAA hierarchical model. You can specify a small subset of these attributes for the AAA selection attributes in the DAP record. These include:
  - Group Policy —The group policy name associated with the user on the security appliance or sent from a Radius/LDAP server as the IETF-Class (25) attribute. Maximum 64 characters.
  - IP Address—The assigned IP address for full tunnel VPN clients (IPsec, L2TP/IPsec, SSL VPN AnyConnect). Does not apply to Clientless SSL VPN, since there is no address assignment for clientless sessions.
  - Connection Profile—The connection or tunnel group name. Maximum 64 characters.
  - Username—The username of the authenticated user. Maximum 64 characters. Applies if you are using Local authentication/authorization.
  - =/!=—Equal to/Not equal to
- LDAP—The LDAP client stores all native LDAP response attribute value pairs in a database associated with the AAA session for the user. The LDAP client writes the response attributes to the database in the order in which it receives them. It discards all subsequent attributes with that name. This scenario might occur when a user record and a group record are both read from the LDAP server. The user record attributes are read first, and always have priority over group record attributes.

To support Active Directory group membership, the AAA LDAP client provides special handling of the LDAP memberOf response attribute. The AD memberOf attribute specifies the DN string of a group record in AD. The name of the group is the first CN value in the DN string. The LDAP client extracts the group name from the DN string and stores it as the AAA memberOf attribute, and in the response attribute database as the LDAP memberOf attribute. If there are additional memberOf attributes in the LDAP response message, then the group name is extracted from those attributes and is combined with the earlier AAA memberOf attribute to form a comma separated string of group names, also updated in the response attribute database.

LDAP attributes consist of an attribute name and attribute value pair in the DAP record.

- **RADIUS**—The RADIUS client stores all native RADIUS response attribute value pairs in a database associated with the AAA session for the user. The RADIUS client writes the response attributes to the database in the order in which it receives them. It discards all subsequent attributes with that name. This scenario might occur when a user record and a group record are both read from the RADIUS server. The user record attributes are read first, and always have priority over group record attributes.

RADIUS attributes consist of an attribute number and attribute value pair in the DAP record. Refer to [Security Appliance Supported RADIUS Attributes and Values](#) for a table that lists RADIUS attributes that the security appliance supports.



**Note** For RADIUS attributes, DAP defines the Attribute ID = 409 + RADIUS ID.

For example:

The RADIUS attribute "Access Hours" has a Radius ID = 1, therefore DAP attribute value = 4096 + 1 = 4097.

The RADIUS attribute "Member Of" has a Radius ID = 146, therefore DAP attribute value = 4096 + 146 = 4242.

- LDAP and RADIUS attributes include:
  - Attribute ID—Names/numbers the attribute. Maximum 64 characters.
  - Value— the attribute name (LDAP) or number (RADIUS).
  - =/!=—Equal to/Not equal to
- LDAP includes the Get AD Groups button. This button queries the LDAP server

The **show ad-groups** command applies only to Active Directory servers using LDAP. Use this command to display AD groups that you can use for dynamic access policy AAA selection criteria.

The default time that the security appliance waits for a response from the server is 10 seconds. You can adjust this time using the **group-search-timeout** command in aaa-server host configuration mode.



**Note**

If the Active Directory server has a large number of groups, the output of the **show ad-groups** command might be truncated based on limitations to the amount of data the server can fit into a response packet. To avoid this problem, use the **filter** option to reduce the number of groups reported by the server.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

## Retrieve AD Groups from selected AD Server Group

You can query an Active Directory server for available AD groups in this window. This feature applies only to Active Directory servers using LDAP. Use the group information to specify dynamic access policy AAA selection criteria.

You can change the level in the Active Directory hierarchy where the search begins by changing the Group Base DN in the Edit AAA Server window. You can also change the time that the security appliance waits for a response from the server in the window. To configure these features, go to: Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups > Edit AAA Server.



### Note

If the Active Directory server has a large number of groups, the list of AD groups retrieved may be truncated based on limitations of the amount of data the server can fit into a response packet. To avoid this problem, use the filter feature to reduce the number of groups reported by the server.

### Fields

AD Server Group—The name of the AAA server group to retrieve AD groups.

Filter By—Specify a group or the partial name of a group to reduce the groups displayed.

Group Name—A list of AD groups retrieved from the server.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

## Add/Edit Endpoint Attributes

Endpoint attributes contain information about the endpoint system environment, posture assessment results, and applications. The security appliance dynamically generates a collection of endpoint attributes during session establishment, and stores these attributes in a database associated with the session. There is no limit for the number of endpoint attributes for each DAP record.

Each DAP record specifies the endpoint selection attributes that must be satisfied for the security appliance to select it. The security appliance selects only DAP records that satisfy every condition configured.

For detailed information about Endpoint attributes, click the following link:

- [Endpoint Attribute Definitions](#)

To configure endpoint attributes as selection criteria for DAP records, in the **Add/Edit Endpoint Attribute** dialog box, set components. These components change according to the attribute type you select.

**Fields**

- **Endpoint Attribute Type**—Select from the drop-down list the endpoint attribute you want to set. Options include Antispyware, Antivirus, Application, File, NAC, Operating System, Personal Firewall, Process, Registry, VLAN, and Priority.

Endpoint attributes include these components, but not all attributes include all components. The following descriptions show (in parentheses) the attributes to which each component applies.

- **Exists/Does not exist buttons** (Antispyware, Antivirus, Application, File, NAC, Operating System, Personal Firewall, Process, Registry, VLAN, Priority)—Click the appropriate button to indicate whether the selected endpoint attribute and its accompanying qualifiers (fields below the Exists/Does not exist buttons) should be present or not.
- **Vendor ID** (Antispyware, Antivirus, Personal Firewall)—Identify the application vendor.
- **Vendor Description** (Antispyware, Antivirus, Personal Firewall)—Provide text that describes the application vendor.
- **Version** (Antispyware, Antivirus, Personal Firewall)—Identify the version of the application, and specify whether you want the endpoint attribute to be equal to/not equal to that version.
- **Last Update** (Antispyware, Antivirus, File)—Specify the number of days since the last update. You might want to indicate that an update should occur in less than (<) or more than (>) the number of days you enter here.
- **Client Type** (Application)—Indicate the type of remote access connection, AnyConnect, Clientless, Cut-through Proxy, IPsec, or L2TP.
- **Checksum** (File)—Select the file and click the Compute Checksum button to arrive at this value.
- **Compute CRC32 Checksum** (File)—Use this calculator to determine the checksum value of a file.
- **Posture Status** (NAC)—Contains the posture token string received from ACS.
- **OS Version** (Operating System)—Windows (various), MAC, Linux, Pocket PC.
- **Service Pack** (Operating System)—Identify the service pack for the operating system.
- **Endpoint ID** (File, Process, Registry)—A string that identifies an endpoint for files, processes or registry entries. DAP uses this ID to match Cisco Secure Desktop host scan attributes for DAP selection. You must configure Host Scan before you configure this attribute. When you configure Host Scan, the configuration displays in this pane, so you can select it, reducing the possibility of errors in typing or syntax.
- **Path** (Process, Policy)—Configure Host Scan before you configure this attribute. When you configure Host Scan, the configuration displays in this pane, so you can select it, reducing the possibility of errors in typing or syntax.
- **Value** (Registry)—dword or string
- **Caseless** (Registry)—Select to disregard case in registry entries.
- **VLAN ID** (VLAN)—A valid 802.1q number ranging from 1 to 4094
- **VLAN Type** (VLAN)—Possible values include the following:

ACCESS	Posture assessment passed
STATIC	No posture assessment applied
TIMEOUT	Posture assessment failed due to no response
AUTH	Posture assessment still active
GUEST	Posture assessment passed, switch to guest VLAN

QUARANTINE	Posture assessment failed, switch to quarantine VLAN
ERROR	Posture assessment failed due to fatal error

- Policy (Location)—Enter the Cisco Secure Desktop Microsoft Windows location profile, case sensitive.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

### Guide

This section provides information about constructing logical expressions for AAA or Endpoint attributes. Be aware that doing so requires sophisticated knowledge of Lua ([www.lua.org](http://www.lua.org)).

In the text box you enter free-form Lua text that represents AAA and/or endpoint selection logical operations. ASDM does not validate text that you enter here; it just copies this text to the DAP policy file, and the security appliance processes it, discarding any expressions it cannot parse.

This option is 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 appliance 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 j

appropriate logical expressions in Lua and enter them here.

- For a list of AAA Selection attributes, including proper name syntax for creating logical expressions, see [Table 36-1](#).
- For a list of endpoint selection attributes, including proper name syntax for creating logical expressions, see [Table 36-3](#).

### Syntax for Creating Lua EVAL Expressions

This section provides information about the syntax for creating Lua EVAL expressions.



#### Note

We recommend that you use EVAL expressions whenever possible for reasons of clarity, which makes verifying the program straightforward.

EVAL(<attribute> , <comparison>, {<value> | <attribute>}, {<type>})

<attribute>	AAA attribute or an attribute returned from Cisco Secure Desktop, see <a href="#">Table 36-1</a> and <a href="#">Table 36-3</a> for attribute definitions
<comparison>	One of the following strings (quotation marks required)

	“EQ”	equal
	“NE”	not equal
	“LT”	less than
	“GT”	greater than
	“LE”	less than or equal
	“GE”	greater than or equal
<value>	A string in quotation marks that contains the value to compare the attribute against	
<type>	One of the following strings (quotation marks required)	
	“string”	case-sensitive string comparison
	“caseless”	case-insensitive string comparison
	“integer”	number comparison, converts string values to numbers
	“hex”	number comparison using hexadecimal values, converts hex string to hex numbers
	“version”	compares versions of the form X.Y.Z. where X, Y, and Z are numbers

**Example:**

```
EVAL(endpoint.os.version, "EQ", "Windows XP", "string")
```

**Constructing DAP Logical Expressions**

Study these examples for help in creating logical expressions in Lua.

- This AAA Lua expression tests for a match on usernames that begin with "b". It uses the string library and a regular expression:

```
(string.find(aaa.cisco.username, "^b") ~= nil)
```



**Note** The *string.find* expression does not work with multivalued attributes. See the [Group Membership Example](#) for an example that uses a multivalued attribute.

- This endpoint expression tests for a match on CLIENTLESS OR CVC client types:

```
(EVAL(endpoint.application.clienttype, "EQ", "CLIENTLESS") or  
EVAL(endpoint.application.clienttype, "EQ", "CVC"))
```

- This endpoint expression tests for Norton Antivirus versions 10.x but excludes 10.5.x:

```
(EVAL(endpoint.av["NortonAV"].version, "GE", "10", "version") and  
(EVAL(endpoint.av["NortonAV"].version, "LT", "10.5", "version") or  
EVAL(endpoint.av["NortonAV"].version, "GE", "10.6", "version")))
```

**The DAP CheckAndMsg Function**

CheckAndMsg is a Lua function that you can configure DAP to call. It generates a user message based on a condition.

You use ASDM to configure CheckAndMsg through the Advanced field in DAP. The security appliance displays the message to the user only when the DAP record containing the LUA CheckAndMsg function is selected and results in a clientless SSL VPN or AnyConnect termination.

The syntax of the CheckAndMsg function follows:

```
CheckAndMsg(value, "<message string if value is true>", "<message string if value if false>")
```

Be aware of the following when creating CheckAndMsg functions:

- CheckAndMsg returns the value passed in as its first argument.
- Use the EVAL function as the first argument if you do not want to use string comparison. For example,

```
(CheckAndMsg((EVAL(...)) , "true msg", "false msg"))
```

CheckAndMsg returns the result of the EVAL function and the security appliances uses it to determine whether to select the DAP record. If the record is selected and results in termination, the security appliance displays the appropriate message.

### Checking for a Single Antivirus Program

This example checks if a single antivirus program, in this case McAfee, is installed on the user PC, and displays a message if it is not.

```
(CheckAndMsg(EVAL(endpoint.av.McAfeeAV.exists,"NE","true"),"McAfee AV was not found on your computer", nil))
```

### Checking for Antivirus Definitions Within the Last 10 Days

This example checks antivirus definitions within the last 10 days (864000 sec), in particular the last update of the McAfee AV dat file, and displays a message to a user lacking the appropriate update that they need an antivirus update:

```
((CheckAndMsg(EVAL(endpoint.av.McAfeeAV.lastupdate,"GT","864000","integer"),"AV Update needed! Please wait for the McAfee AV till it loads the latest dat file.",nil) ))
```

### Checking for a Hotfix on the User PC

This example checks for a specific hotfix. If a user does not have the hotfix on their PC, a message that it is not installed displays.

```
(not CheckAndMsg(EVAL(endpoint.os.windows.hotfix["KB923414"],"EQ","true"),nil,"The required hotfix is not installed on your PC."))
```

or you could define it this way (which makes more sense):

```
(CheckAndMsg(EVAL(endpoint.os.windows.hotfix["KB923414"],"NE","true"),"The required hotfix is not installed on your PC.",nil))
```

You can build the expression in this example because the debug dap trace returns:

```
endpoint.os.windows.hotfix["KB923414"] = "true";
```

### Checking for Antivirus Programs

You can configure messages so that the end user is aware of and able to fix problems with missing or not running AVs. As a result, if access is denied, the security appliance collects all messages for the DAP that caused the "terminate" condition and displays them in the browser on the logon page. If access is allowed, the security appliance displays all messages generated in the process of DAP evaluation on the portal page.

The following instructions show how to use this feature to check on the Norton Antivirus program.

- 
- Step 1** Copy and paste the following Lua expression into the Advanced field of the Add/Edit Dynamic Access Policy pane (click the double arrow on the far right to expand the field).

```
(CheckAndMsg(EVAL(endpoint.av.NortonAV.exists, "EQ", "false"), "Your Norton AV was found but the active component of it was not enabled", nil) or
CheckAndMsg(EVAL(endpoint.av.NortonAV.exists, "NE", "true"), "Norton AV was not found on your computer", nil) )
```

- Step 2** In that same Advanced field, select the **OR** button.
- Step 3** In the Access Attributes section below, set the leftmost tab, **Action**, to **Terminate**.
- Step 4** Connect from a PC that does not have or has disabled Norton Antivirus.
- The expected result is that the connection is not allowed *and* the message appears as a blinking ! point.
- Step 5** Click the blinking ! to see the message.
- 

### Checking for Antivirus Programs *and* Definitions Older than 1 1/2 Days

This example checks for the presence of the Norton and McAfee antivirus programs, and whether the virus definitions are older than 1 1/2 days (10,000 seconds). If the definitions are older than 1 1/2 days, the security appliance terminates the session with a message and links for remediation.

- 
- Step 1** Copy and paste the following Lua expression into the Advanced field of the Add/Edit Dynamic Access Policy pane (click the double arrow on the far right to expand the field).

```
((EVAL(endpoint.av.NortonAV.esists, "EQ", "true", "string") and
CheckAndMsg(EVAL(endpoint.av.NortonAV.lastupdate, "GT", "10000", integer), To
remediate <a href='http://www.symantec.com'>Click this link </a>", nil)) or
(EVAL(endpoint.av.McAfeeAV.esists, "EQ", "true", "string") and
CheckAndMsg(EVAL(endpoint.av.McAfeeAV.lastupdate, "GT", "10000", integer), To
remediate <a href='http://www.mcafee.com'>Click this link</a>", nil))
```

- Step 2** In that same Advanced field, select the **AND** button.
- Step 3** In the Access Attributes section below, set the leftmost tab, **Action**, to **Terminate**.
- Step 4** Connect from a PC that has Norton and McAfee antivirus programs with versions that are older than 1 1/2 days.

The expected result is that the connection is not allowed *and* the message appears as a blinking ! point.

**Step 5** Click the blinking ! to see the message and links for remediation.

---

## Advanced Lua Functions

When working with dynamic access policies for clientless SSL VPN, you might need additional flexibility of match criteria. For example, you might want to apply a different DAP based on the following:

- Organizational Unit (OU) or other level of the hierarchy for the user object
- Group Name that follows a naming convention but has many possible matches— you might require the ability to use a wildcard on group names.

You can accomplish this flexibility by creating a Lua logical expression in the Advanced section of the DAP pane in ASDM.

## OU-Based Match

DAP can use many attributes returned from an LDAP server in a logical expression. See the DAP trace section for example output of this, or run a debug dap trace.

The LDAP server returns the user Distinguished Name (DN). This implicitly identifies where in the directory the user object is located. For example, if the user DN is CN=Example User,OU=Admins,dc=cisco,dc=com this user is located in OU=Admins,dc=cisco,dc=com. If all administrators are in this OU (or any container below this level) you can use a logical expression to match on this criteria as follows:

```
(string.find(aaa.ldap.distinguishedName, "OU=Admins,dc=cisco,dc=com$" ~= nil)
```

In this example, the string.find function allows for a regular expression. Use the \$ at the end of the string to anchor this string to the end of the distinguishedName field.

## Group Membership Example

You can create a basic logical expression for pattern matching of AD group membership. Because users can be members of multiple groups, DAP parses the response from the LDAP server into separate entries in a table. You need an advanced function to accomplish the following:

- Compare the memberOf field as a string (in the event the user belongs to only one group).
- Iterate through each returned memberOf field if the returned data is of type "table".

The function we have written and tested for this purpose is shown below. In this example, if a user is a member of any group ending with "-stu" they match this DAP.

```
assert(function()
  if ((type(aaa.ldap.memberOf) == "string") and
      (string.find(aaa.ldap.memberOf, "-stu$" ~= nil)) then
    return true
  elseif (type(aaa.ldap.memberOf) == "table") then
    local k, v
    for k, v in pairs(aaa.ldap.memberOf) do
      if (string.find(v, "-stu$" ~= nil) then
        return true
      end
    end
  end
  return false
end)
```

```
end) ()
```

### Further Information on Lua

You can find detailed LUA programming information at <http://www.lua.org/manual/5.1/manual.html>.

## Operator for Endpoint Category

You can configure multiple instances of each type of endpoint. In this pane, set each type of endpoint to require only one instance of a type (Match Any = OR) or to have all instances of a type (Match All = AND).

- If you configure only one instance of an endpoint category, you do not need to set a value.
- For some endpoint attributes, it makes no sense to configure multiple instances. For example, no users have more than one running OS.
- You are configuring the Match Any/Match All operation within each endpoint type.

The security appliance evaluates each type of endpoint attribute, and then performs a logical AND operation on all of the configured endpoints. That is, each user must satisfy the conditions of ALL of the endpoints you configure, as well as the AAA attributes.

## DAP Examples

The following sections provide examples of useful dynamic access policies.

### Using DAP to Define Network Resources

This example shows how to configure dynamic access policies as a method of defining network resources for a user or group. The DAP policy named `Trusted_VPN_Access` permits clientless and AnyConnect VPN access. The policy named `Untrusted_VPN_Access` permits only clientless VPN access. [Table 36-4](#) summarizes the configuration of each of these policies.

The ASDM path is Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies > Add/Edit Dynamic Access Policy > Endpoint

**Table 36-4** A Simple DAP Configuration for Network Resources

Attribute	Trusted_VPN_Access	Untrusted_VPN_Access
Endpoint Attribute Type Policy	Trusted	Untrusted
Endpoint Attribute Process	ieexplore.exe	—
Advanced Endpoint Assessment	AntiVirus= McAfee Attribute	
CSD Location	Trusted	Untrusted
LDAP memberOf	Engineering, Managers	Vendors
ACL		Web-Type ACL
Access	AnyConnect and Web Portal	Web Portal

## Using DAP to Apply a WebVPN ACL

DAP can directly enforce a subset of access policy attributes including Network ACLs (for IPsec and AnyConnect), clientless SSL VPN Web-Type ACLs, URL lists, and Functions. It cannot directly enforce, for example, a banner or the split tunnel list, which the group policy enforces. The Access Policy Attributes tabs in the Add/Edit Dynamic Access Policy pane provide a complete menu of the attributes DAP directly enforces.

Active Directory/LDAP stores user group policy membership as the “memberOf” attribute in the user entry. You can define a DAP such that for a user in AD group (memberOf) = Engineering the security appliance applies a configured Web-Type ACL. To accomplish this task, perform the following steps:

- 
- Step 1** Navigate to the Add AAA attributes pane (Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies > Add/Edit Dynamic Access Policy > AAA Attributes section > Add AAA Attribute).
  - Step 2** For the AAA Attribute type, use the drop-down menu to select LDAP.
  - Step 3** In the Attribute ID field, enter memberOf, exactly as you see it here. Case is important.
  - Step 4** In the Value field, use the drop-down menu to select =, and in the adjacent text box enter Engineering.
  - Step 5** In the Access Policy Attributes area of the pane, click the Web-Type ACL Filters tab.
  - Step 6** Use the Web-Type ACL drop-down menu to select the ACL you want to apply to users in the AD group (memberOf) = Engineering.
- 

## Enforcing CSD Checks and Applying Policies via DAP

This example creates a DAP that checks that a user belongs to two specific AD/LDAP groups (Engineering and Employees) and a specific ASA tunnel group. It then applies an ACL to the user.

The ACLs that DAP applies control access to the resources. They override any ACLS defined the group policy on the security appliance. In addition, the security appliance applied the regular AAA group policy inheritance rules and attributes for those that DAP does not define or control, examples being split tunneling lists, banner, and DNS.

- 
- Step 1** Navigate to the Add AAA attributes pane (Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies > Add/Edit Dynamic Access Policy > AAA Attributes section > Add AAA Attribute).
  - Step 2** For the AAA Attribute type, use the drop-down menu to select LDAP.
  - Step 3** In the Attribute ID field, enter memberOf, exactly as you see it here. Case is important.
  - Step 4** In the Value field, use the drop-down menu to select =, and in the adjacent text box enter Engineering.
  - Step 5** In the Attribute ID field, enter memberOf, exactly as you see it here. Case is important.
  - Step 6** In the Value field, use the drop-down menu to select =, and in the adjacent text box enter Employees.
  - Step 7** For the AAA attribute type, use the drop-down menu to select Cisco.
  - Step 8** Check the Tunnel group box, use the drop-down menu to select =, and in the adjacent drop down box select the appropriate tunnel group (connection policy).
  - Step 9** In the Network ACL Filters tab of the Access Policy Attributes area, select the ACLs to apply to users who meet the DAP criteria defined in the previous steps.



