# Dynamic Access Policies

This chapter describes how to configure dynamic access policies.



# About Dynamic 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 ASA 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 ASA grants access to a particular user for a particular session based on the policies you define. The ASA 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 ASA uses for selecting and applying DAP records during session establishment. Stored on the ASA. You can use ASDM to modify it and upload it to the ASA 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.

Refer to the *Dynamic Access Deployment Guide* (https://supportforums.cisco.com/docs/DOC-1369) for additional information.

# DAP Support of Remote Access Protocols and Posture Assessment Tools

The ASA obtains endpoint security attributes by using posture assessment tools that you configure. These posture assessment tools include the AnyConnect posture module, the independent Host Scan package, and NAC.

The following table identifies each of the remote access protocols DAP supports, the posture assessment tools available for that method, and the information that tool provides.

| **Supported Remote Access Protocol** | **AnyConnect Posture Module**<br>**Host Scan package**<br>**Cisco Secure Desktop**<br>**(without Endpoint Assessment Host Scan Extension enabled)** | **AnyConnect Posture Module**<br>**Host Scan package**<br>**Cisco Secure Desktop**<br>**(with Endpoint Assessment Host Scan Extension enabled)** | **NAC** | **Cisco NAC Appliance** |
|---|---|---|---|---|
| | Returns file information, registry key values, running processes, operating system | Returns anti-malware and personal firewall software information | Returns NAC status | Returns VLAN Type and VLAN IDs |
| IPsec VPN | No | No | Yes | Yes |
| Cisco AnyConnect VPN | Yes | Yes | Yes | Yes |
| Clientless (browser-based) SSL VPN | Yes | Yes | No | No |
| PIX Cut-through Proxy (posture assessment not available) | No | No | No | No |

# Remote Access Connection Sequence with DAPs

The following sequence outlines a typical remote access connection establishment.

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

# Licensing for Dynamic Access Policies

**Note** This feature is not available on No Payload Encryption models.

Dynamic access policies (DAP) require one of the following licenses:

- AnyConnect Apex—To use all DAP features.
- AnyConnect Plus—For operating system and operating system/AnyConnect version checking only.

### Related Topics

Add AnyConnect Endpoint Attributes to a DAP, on page 12

# Configure Dynamic Access Policies

### Before you begin

- Other than where noted, you must install Host Scan before configuring DAP endpoint attributes.
- If upgrading from HostScan 4.3.x to HostScan 4.6.x or greater, you must migrate any existing AV/AS/FW endpoint attributes to the corresponding replacement AM/FW endpoint attributes before you upgrade. See the AnyConnect HostScan 4.3.x to 4.6.x Migration Guide for a full upgrade & migration procedure.
- Due to Java Web Start security issues, you may find that you are unable to populate Advanced Endpoint Attribute with configured values if you use webvpn based configuration on the device. To overcome this issue, either use ASDM Desktop application or add the AEA related URL(s) as the exception in the Java Security.
- Before configuring File, Process, and Registry endpoint attributes, configure File, Process, and Registry Basic Host Scan attributes. For instructions, start ASDM and choose **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan** and click **Help**.
- DAP supports only ASCII characters.

### Procedure

**Step 1** Start ASDM and choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** or **Clientless SSL VPN Access** > **Dynamic Access Policies**.

**Note** If an **Incompatible** action button is displayed below the Add, Edit and Delete action, there has been an attempt to upgrade HostScan to a version (4.6.x or later) that has had internal library updates that make it incompatible with your existing DAP policies (created when using HostScan 4.3.x or earlier). You MUST carry out a one-time migration procedure to adapt your configuration.

The appearance of the **Incompatible** action indicates that the HostScan upgrade has been initiated and you now need to migrate your configuration. Refer to the AnyConnect Hostscan 4.3.x to 4.6.x Migration Guide for detailed instructions.

**Step 2** To include certain antimalware or personal firewall endpoint attributes, click the **CSD configuration** link near the top of the pane. Then enable Cisco Secure Desktop and HostScan extensions. This link does not display if you have previously enabled both of these features.

**Step 3** View the list of previously configured DAPs.

The following fields are shown in the table:

- ACL Priority—Displays the priority of the DAP record.

  The ASA uses this value to logically sequence the ACLs when aggregating the network and web-type ACLs from multiple DAP records. The ASA 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 ACL that applies to the session.
- Web-Type ACL List—Displays the name of the SSL VPN ACL that applies to the session.
- Description—Describes the purpose of the DAP record.

**Step 4** Click **Add** or **Edit** to Add or Edit a Dynamic Access Policy, on page 5.

**Step 5** Click **Apply** to save your DAP configuration.

**Step 6** Search for a Dynamic Access Policy (DAP) by using the **Find** field.

Start typing in the field and the tool will search the beginning characters of every field of the DAP table for a match. You can use wild cards to expand your search.

For example typing **`sal`** in the **Find** field matches a DAP named `Sales` but not a DAP named `Wholesalers`. If you type **`*sal`** in the **Find** field, the search finds the first instance of either **`Sales`** or **`Wholesalers`** in the table.

**Step 7** Test Dynamic Access Policies, on page 6 to verify your configuration.

# Add or Edit a Dynamic Access Policy

**Procedure**

**Step 1** Start ASDM and choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** or **Clientless SSL VPN Access** > **Dynamic Access Policies** > **Add** or **Edit.**

**Step 2** Provide a name (required) and a description (optional) of this dynamic access policy.

- The **Policy Name** is a string of 4 through 32 characters, no spaces allowed.
- You are allowed a maximum of 80 characters in the DAP **Description** field.

**Step 3** In the **ACL 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. Values of 0 to 2147483647 are valid. The default value is 0.

**Step 4** Specify your selection criteria for this DAP:

a) In the Selection Criteria pane, use the ANY/ALL/NONE drop-down list (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, 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 ASA always selects it since all selection criteria are satisfied.

b) Click **Add** or **Edit** in the AAA Attributes field to Configure AAA Attribute Selection Criteria in a DAP, on page 7.

c) Click **Add** or **Edit** in the Endpoint Attributes area to Configure Endpoint Attribute Selection Criteria in a DAP, on page 10.

d) Click the **Advanced** field to #unique_177. This feature requires knowledge of the Lua programming language.

- 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 ASA processes it, discarding any expressions it cannot parse.

  For information about importing/exporting a *dap.xml* file, see Import and Export the DAP XML File between Two ASAs, on page 6.

**Step 5** Specify the **Access/Authorization Policy Attributes** for this DAP.

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. See Configure DAP Access and Authorization Policy Attributes, on page 27.

**Step 6** Click **OK**.

# Import and Export the DAP XML File between Two ASAs

The Dynamic Access Policies (DAP) configuration of ASA is stored in a file called *dap.xml* on the ASA's flash memory. The file contains the DAP policies selection attributes.

**Note** Although you can export the *dap.xml* file, edit it (if you know about xml syntax), and re-import it back, be very careful, because you can cause ASDM to stop processing DAP records if you have misconfigured something. There is no CLI to manipulate this part of the configuration.

Use these steps to import and export the *dap.xml* file between two ASAs.

The procedure uses the example of exporting a *dap.xml* file from ASA#1 and importing in on ASA#2.

For information about handling files on ASA using the ASDM, see the *Managing Files* section of the *Cisco ASA Series General Operations ASDM Configuration Guide*.

### Procedure

**Step 1** Clear the *dap.xml* file on the ASA#2.

a) Save the ASA#2 configuration and *dap.xml* externally to a tftp or an ftp server.
b) Exit the ASDM for ASA#2.

**Note** You can also use the **ASDM** > **Tools** > **BackUp Configurations** > **DAP Configurations** option to save the *dap.xml* file.

You can also rename or delete the *dap.xml* file on the ASA#2 flash memory.

**Step 2** On the ASA#2 command prompt, enter the **clear configure dynamic-access-policy-record** command to remove the DAP record configurations.

**Step 3** Export the *dap.xml* file from ASA#1 flash and import it on the ASA#2 flash.

**Step 4** Use the **dynamic-access-policy-record** command to configure the DAP record entries from ASA#1 on ASA#2.

**Step 5** On ASA#2 enable DAP using the **dynamic-access-policy-config activate** command.

**Note** You can also relaunch the ASDM for ASA#2 to activate the DAP configuration.

**Step 6** Relaunch the ASDM on ASA#2.
The new DAP policies are configured in ASA#2.

# 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.

**Procedure**

**Step 1** Use the Add/Edit buttons associated with the AAA Attribute and Endpoint Attribute tables to specify attribute value pairs.

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.

**Step 2** 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** area.

# Configure AAA Attribute Selection Criteria in a DAP

DAP complements AAA services by providing a limited set of authorization attributes that can override the attributes that AAA provides. You can specify AAA attributes from the Cisco AAA attribute hierarchy, or from the full set of response attributes that the ASA receives from a RADIUS or LDAP server. The ASA selects DAP records based on the AAA authorization information for the user and posture assessment information for the session. The ASA can choose multiple DAP records depending on this information, which it then aggregates to create DAP authorization attributes.

**Procedure**

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, on page 9.

AAA Attributes Type—Use the drop-down list to choose 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 VPN user session. Can be set locally on the security appliance or sent from a RADIUS/LDAP server as the IETF-Class (25) attribute. Maximum 64 characters.
  - Assigned IP Address—Enter the IPv4 address you want to specify for the policy. 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.
  - Assigned IPv6 Address—Enter the IPv6 address you want to specify for the policy.
  - 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, RADIUS, LDAP authentication/authorization or any other authentication type (for example, RSA/SDI), NT Domain, etc).

- =/!=—Equal to/Not equal to.

- LDAP—The LDAP client (security appliance) 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.

  In the case where the VPN remote access session to an LDAP authentication/authorization server returns the following three Active directory groups (memberOf enumerations):

  cn=Engineering,ou=People,dc=company,dc=com

  cn=Employees,ou=People,dc=company,dc=com

  cn=EastCoastast,ou=People,dc=company,dc=com

  the ASA processes three Active Directory groups: Engineering, Employees, and EastCoast which could be used in any combination as aaa.ldap selection criteria.

  LDAP attributes consist of an attribute name and attribute value pair in the DAP record. The LDAP attribute name is syntax/case sensitive. If for example you specify LDAP attribute Department instead of what the AD server returns as department, the DAP record will not match based on this attribute setting.

  **Note** To enter multiple values in the Value field, use the semicolon (;) as the delimiter. For example:

  eng;sale; cn=Audgen VPN,ou=USERS,o=OAG

- 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.

  **Note** For RADIUS attributes, DAP defines the Attribute ID = 4096 + 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).

  To enter multiple values in the Value field, use the semicolon (;) as the delimiter. For example:
  `eng;sale; cn=Audgen VPN,ou=USERS,o=OAG`
- =/!=—Equal to/Not equal to.

- LDAP includes the Get AD Groups button. See Retrieve Active Directory Groups, on page 9.

# Retrieve Active Directory Groups

You can query an Active Directory server for available AD groups in this pane. This feature applies only to Active Directory servers using LDAP. This button queries the Active Directory LDAP server for the list of groups the user belong to (memberOf enumerations). Use the group information to specify dynamic access policy AAA selection criteria.

AD groups are retrieved from the LDAP server using the CLI s**how-ad-groups** command in the background. The default time that the ASA 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.

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 pane. You can also change the time that the ASA waits for a response from the server in the window. To configure these features, choose **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 (or the output of the **show ad-groups** command) 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.

**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.

# AAA Attribute Definitions

The following table 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.

| Attribute Type | Attribute Name | Source | Value | Max String Length | Description |
|---|---|---|---|---|---|
| Cisco | aaa.cisco.grouppolicy | AAA | string | 64 | Group policy name on the ASA 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) |
| LDAP | aaa.ldap.<*label*> | LDAP | string | 128 | LDAP attribute value pair |
| RADIUS | aaa.radius.<number> | RADIUS | string | 128 | Radius attribute value pair |

# Configure Endpoint Attribute Selection Criteria in a DAP

Endpoint attributes contain information about the endpoint system environment, posture assessment results, and applications. The ASA dynamically generates a collection of endpoint attributes during session establishment and stores these attributes in a database associated with the session. Each DAP record specifies the endpoint selection attributes that must be satisfied for the ASA to choose it for a session. The ASA selects only DAP records that satisfy every condition configured.

### Before you begin

- Configuring endpoint attributes as selection criteria for DAP records is part of a larger process to Configure Dynamic Access Policies, on page 3. Review this procedure before configuring endpoint attributes as selection criteria for DAPs.
- For detailed information about Endpoint attributes, see Endpoint Attribute Definitions, on page 18.
- 
- For detailed information on how Host Scan checks for anti-malware and personal firewall programs that are memory-resident, see DAP and Antimalware and Personal Firewall Programs, on page 18.

### Procedure

**Step 1** Click **Add** or **Edit** and add any of the following endpoint attributes as selection criteria.

You can create multiple instances of each type of endpoint attribute. There is no limit for the number of endpoint attributes for each DAP record.

- Add an Anti-Malware Endpoint Attribute to a DAP, on page 11
- Add an Application Attribute to a DAP, on page 12
- Add AnyConnect Endpoint Attributes to a DAP, on page 12
- Add a File Endpoint Attribute to a DAP, on page 14
- Add a Device Endpoint Attribute to a DAP, on page 14
- Add a NAC Endpoint Attribute to a DAP, on page 15
- Add an Operating System Endpoint Attribute to a DAP, on page 15
- Add a Personal Firewall Endpoint Attribute to a DAP, on page 15
- Add a Policy Endpoint Attribute to a DAP, on page 16
- Add a Process Endpoint Attribute to a DAP, on page 16
- Add a Registry Endpoint Attribute to a DAP, on page 17
- Add Multiple Certificate Authentication Attributes to DAP, on page 17

**Step 2** Specify the DAP policy matching criteria.

For each of these endpoint attribute types, decide whether the DAP policy should require that the user have all instances of a type (Match all = AND, default) or only one of them (Match Any = OR).

a) Click **Logical Op.**
b) Choose **Match Any** (default) or **Match All** for each type of endpoint attribute.
c) Click **OK**.

**Step 3** Return to Add or Edit a Dynamic Access Policy, on page 5.

# Add an Anti-Malware Endpoint Attribute to a DAP

### Before you begin

If upgrading from HostScan 4.3.x to HostScan 4.6.x or greater, you must migrate any existing AV/AS/FW endpoint attributes to the corresponding replacement AM/FW endpoint attributes before you upgrade. See the AnyConnect HostScan 4.3.x to 4.6.x Migration Guide for a full upgrade & migration procedure.

### Procedure

**Step 1** In the **Endpoint Attribute Type** list box, choose **Anti-Malware**.

**Step 2** Click the appropriate **Installed or Not Installed** button to indicate whether the selected endpoint attribute and its accompanying qualifiers (fields below the Name/Operation/Value column) are installed or not installed.

**Step 3** Determine if you want realtime scanning enabled or disabled.

**Step 4** From the **Vendor** list box, choose the name of the anti-malware vendor you are testing for.

**Step 5** Check the **Product Description** check box and choose from the list box the vendor's product name you are testing for.

**Step 6** Check the **Version** checkbox and set the operation field to equal to (=), not equal (!=), less than (<), greater than (>), less that or equal to (<=), or greater than or equal to (>=) the product version number you choose from the **Version** list box.

If the choice in the version list box has an x, such as 3.x, replace the x with a specific release number, for example, 3.5.

**Step 7** Check the **Last Update** check box. 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.

**Step 8** Click **OK**.

# Add an Application Attribute to a DAP

### Procedure

**Step 1** In the **Endpoint Attribute Type** list box, choose **Application**.

**Step 2** In the Client Type operation field, choose equals (=) or does not eaqual (!=).

**Step 3** In the Client type list box, indicate the type of remote access connection you are testing for.

**Step 4** Click **OK**.

# Add AnyConnect Endpoint Attributes to a DAP

AnyConnect Endpoint Attributes, also known as Mobile Posture or AnyConnect Identity Extensions (ACIDex), are used by the AnyConnect VPN client to communicate posture information to the ASA. Dynamic Access Polices use these endpoint attributes to authorize users.

These mobile posture attributes can be included in a dynamic access policy and enforced without installing Host Scan or Cisco Secure Desktop on the endpoint.

Some mobile posture attributes are relevant to the AnyConnect client running on mobile devices only. Some mobile posture attributes are relevant to both AnyConnect clients running on mobile devices and AnyConnect desktop clients.

### Before you begin

Mobile posture requires an AnyConnect Mobile license and an AnyConnect Premium license installed on the ASA. Enterprises that install these licenses will be able to enforce DAP policies on supported mobile devices based on DAP attributes and other existing endpoint attributes. This includes allowing or denying remote access from a mobile device.

### Procedure

**Step 1** In the **Endpoint Attribute Type** list box, choose **AnyConnect**.

**Step 2** Check the **Client Version** check box and set the operation field to be equal to (=), not equal to (!=), less than (<), greater than (>), less than or equal to (<=), or greater than or equal to (>=) the AnyConnect client version number you then specify in the **Client Version** field.

You can use this field to evaluate the client version on mobile devices, such as mobile phones and tablets, or desktop and laptop devices.

**Step 3** Check the **Platform** check box and set the operation field to be equal to (=), or not equal to (!=) the operating system you then choose from the **Platform** list box.

You can use this field to evaluate the operating system on mobile devices, such as mobile phones and tablets, as well as the operating system on desktop and laptop devices. Selecting a platform activates the additional attribute fields for Device Type and Device Unique ID.

**Step 4** Check the **Platform Version** check box and set the operation field to be equal to (=), not equal to (!=), less than (<), greater than (>), less than or equal to (<=), or greater than or equal to (>=) the operating system version number you then specify in the **Platform Version** field.

If you want to create a DAP record that contains this attribute, be sure to also specify a Platform in the previous step.

**Step 5** If you selected the Platform checkbox you can check the **Device Type** checkbox. Set the operation field to be equal to (=) or not equal to (!=) the device you then choose or enter in the **Device Type** field.

If you have a supported device which is not listed in the Device Type field, you can enter it in the Device Type field. The most reliable way to obtain the device type information is to install the AnyConnect client on the endpoint, connect to the ASA, and perform a DAP Trace. In the DAP trace results, look for the value of **endpoint.anyconnect.devicetype**. That is the value that you need to enter in the Device Type field.

**Step 6** If you selected the Platform checkbox you can check the **Device Unique ID** checkbox. Set the operation field to be equal to (=) or not equal to (!=) the device's unique ID you then specify in the **Device Unique ID** field.

The Device Unique ID distinguishes individual devices allowing you to set policies for a particular mobile device. To obtain a device's unique ID you need the device to connect to the ASA and perform a DAP trace, look for the value of **endpoint.anyconnect.deviceuniqueid**. That is the value that you need to enter in the Device Unique ID field.

**Step 7** If you selected a Platform, you can add MAC addresses to the **MAC Addresses Pool** field. Set the operation field to be equal to (=) or not equal to (!=) the specified MAC addresses. Each MAC address must be in the format xx-xx-xx-xx-xx-xx, where 'x' is a valid hexadecimal character (0-9, A-F, or a-f). MAC addresses should be separated by at least one blank space.

The MAC address distinguishes individual systems allowing you to set policies for a particular device. To obtain a system's MAC address, you will need the device to connect to the ASA and perform a DAP trace, look for the value of **endpoint.anyconnect.macaddress**. That is the value that you need to enter in the MAC Address Pool field.

**Step 8** Click **OK**.

# Add a File Endpoint Attribute to a DAP

### Before you begin

Before configuring a File endpoint attribute, define the file for which you want to scan in the Host Scan window for Cisco Secure Desktop. In ASDM choose **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan**. Click **Help** on that page for more information.

### Procedure

**Step 1** In the **Endpoint Attribute Type** list box, choose **File**.

**Step 2** Select the appropriate **Exists** or **Does not exist** radio 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.

**Step 3** In the **Endpoint ID** list box, choose from the drop-down list the endpoint ID that equates to the file entry for which you want to scan.

The file information is displayed below the Endpoint ID list box.

**Step 4** Check the **Last Update** check box and set the operation field to be less than (<) or greater than (>) a certain number of days old. Enter the number of days old in the **days** field.

**Step 5** Check the **Checksum** checkbox and set the operation field to be equal to (=) or not equal to (!=) the checksum value of the file you are testing for.

**Step 6** Click **Compute CRC32 Checksum** to determine the checksum value of the file you are testing for.

**Step 7** Click **OK**.

# Add a Device Endpoint Attribute to a DAP

### Procedure

**Step 1** In the **Endpoint Attribute Type** list box, choose **Device**.

**Step 2** Check the **Host Name** checkbox and set the operation field to be equal to (=) or not equal to (!=) the host name of the device you are testing for. Use the computer's host name only, not the fully qualified domain name (FQDN).

**Step 3** Check the **MAC address** checkbox and set the operation field to be equal to (=) or not equal to (!=) the MAC address of the network interface card you are testing for. Only one MAC address per entry. The address must be in the format xxxx.xxxx.xxxx where x is a hexadecimal character.

**Step 4** Check the **BIOS Serial Number** checkbox and set the operation field to be equal to (=) or not equal to (!=) the BIOS serial number value of the device you are testing for. The number format is manufacturer-specific. There is no format requirement.

**Step 5** Check the **TCP/UDP Port Number** checkbox and set the operation field to be equal to (=) or not equal to (!=) the TCP or UDP port in listening state that you are testing for.

In the TCP/UDP combo box, choose the kind of port you are testing for: TCP (IPv4), UDP(IPv4), TCP (IPv6), or UDP (IPv6). If you are testing for more than one port, make several individual endpoint attribute rules in the DAP and specify one port in each.

**Step 6** Check the **Version of Secure Desktop (CSD)** checkbox and set the operation field to be equal to (=) or not equal to (!=) the version of the Host Scan image running on the endpoint.

**Step 7** Check the **Version of Endpoint Assessment** checkbox and set the operation field to be equal to (=) or not equal to (!=) the version of endpoint assessment (OPSWAT) you are testing for.

**Step 8** Click **OK**.

# Add a NAC Endpoint Attribute to a DAP

### Procedure

**Step 1** In the **Endpoint Attribute Type** list box, choose **NAC**.

**Step 2** Check the **Posture Status** checkbox and set the operation field to be equal to (=) or not equal to (!=) the posture token string received by ACS. Enter the posture token string in the Posture Status text box.

**Step 3** Click **OK**.

# Add an Operating System Endpoint Attribute to a DAP

### Procedure

**Step 1** In the **Endpoint Attribute Type** list box, choose **Operating System**.

**Step 2** Check the **OS Version** checkbox and set the operation field to be equal to (=) or not equal to (!=) the Windows, Mac, or Linux operating system you set in the **OS Version** list box.

**Step 3** Check the **OS Update** checkbox and set the operation field to be equal to (=) or not equal to (!=) the Windows, Mac, or Linux service pack for the operating system you enter in the **OS Update** text box.

**Step 4** Click **OK**.

# Add a Personal Firewall Endpoint Attribute to a DAP

### Before you begin

If upgrading from HostScan 4.3.x to HostScan 4.6.x or greater, you must migrate any existing AV/AS/FW endpoint attributes to the corresponding replacement AM/FW endpoint attributes before you upgrade. See the AnyConnect HostScan 4.3.x to 4.6.x Migration Guide for a full upgrade & migration procedure.

### Procedure

**Step 1** In the **Endpoint Attribute Type** list box, choose **Operating System**.

**Step 2** Click the appropriate **Installed or Not Installed** button to indicate whether the selected endpoint attribute and its accompanying qualifiers (fields below the Name/Operation/Valud column) are installed or not installed.

**Step 3** From the **Vendor** list box, click the name of the personal firewall vendor you are testing for.

**Step 4** Check the **Product Description** check box and choose from the list box the vendor's product name you are testing for.

**Step 5** Check the **Version** checkbox and set the operation field to equal to (=), not equal (!=), less than (<), greater than (>), less that or equal to (<=), or greater than or equal to (>=) the product version number you choose from the **Version** list box.

If the choice in the **Version** list box has an x, such as 3.x, replace the x with a specific release number, for example, 3.5.

**Step 6** Check the **Last Update** check box. 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.

**Step 7** Click **OK.**

# Add a Policy Endpoint Attribute to a DAP

### Procedure

**Step 1** In the **Endpoint Attribute Type** list box, choose **Policy**.

**Step 2** Check the **Location** checkbox and set the operation field to be equal to (=) or not equal to (!=) the Cisco Secure Desktop Microsoft Windows location profile. Enter the Cisco Secure Desktop Microsoft Windows location profile string in the **Location** text box.

**Step 3** Click **OK**.

# Add a Process Endpoint Attribute to a DAP

### Before you begin

Before configuring a Process endpoint attribute, define the process for which you want to scan in the Host Scan window for Cisco Secure Desktop. In ASDM choose **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan**. Click **Help** on that page for more information.

### Procedure

**Step 1** In the **Endpoint Attribute Type** list box, choose **Process**.

**Step 2** Click the appropriate **Exists or Does not exist** button to indicate whether the selected endpoint attribute and its accompanying qualifiers (fields below the Exists and Does not exist buttons) should be present or not.

**Step 3** In the **Endpoint ID** list box, choose from the drop-down list the endpoint ID for which you want to scan.

The endpoint ID process information is displayed below the list box.

**Step 4** Click **OK**.

# Add a Registry Endpoint Attribute to a DAP

Scanning for registry endpoint attributes applies to Windows operating systems only.

### Before you begin

Before configuring a Registry endpoint attribute, define the registry key for which you want to scan in the Host Scan window for Cisco Secure Desktop. In ASDM choose **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan**. Click **Help** on that page for more information.

### Procedure

**Step 1** In the **Endpoint Attribute Type** list box, choose **Registry**.

**Step 2** Click the appropriate **Exists or Does not exist** button to indicate whether the **Registry** endpoint attribute and its accompanying qualifiers (fields below the Exists and Does not exist buttons) should be present or not.

**Step 3** In the **Endpoint ID** list box, choose from the drop-down list the endpoint ID that equates to the registry entry for which you want to scan.

The registry information is displayed below the Endpoint ID list box.

**Step 4** Check the **Value** checkbox and set the operation field to be equal to (=) or not equal to (!=).

**Step 5** In the first **Value** list box, identify the registry key as a dword or a string.

**Step 6** In the second Value operation list box, enter the value of the registry key you are scanning for.

**Step 7** If you want to disregard the case of the registry entry when scanning, click the checkbox. If you want the search to be case-sensitive, do not check the check box.

**Step 8** Click **OK**.

# Add Multiple Certificate Authentication Attributes to DAP

You can index each certificate so that any of the received certificates can be referenced by the configured rules. Based on these certificate fields, you can configure DAP rules to allow or disallow connection attempts.

### Procedure

**Step 1** Browse to **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add Endpoint Attribute**.

**Step 2** Choose **Multiple Certificate Authentication** as the Endpoint Attribute Type in the drop-down menu.

**Step 3** Configure one or all of the following, depending on what your preference is:

- Subject Name
- Issuer Name

- Subject Alternate Name
- Serial Number

**Step 4** Leave the Certificate Store at the default of None to allow certificates from either store or choose which to allow, only user or only machine. If you choose User or Machine, you must enter the store that the certificate came from. This information is sent by the client in the protocol.

# DAP and Antimalware 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 HostScan modules return information to the security appliance about the configured endpoint attributes, and the DAP subsystem uses that information to choose a DAP record that matches the values of those attributes.

Most, but not all, antimalware and personal firewall programs support active scan, which means that the programs are memory-resident, and therefore always running. HostScan 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, HostScan 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, HostScan 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, HostScan ignores the presence of the software. The security appliance does not choose 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.

**Note** If upgrading from HostScan 4.3.x to HostScan 4.6.x or greater, you must migrate any existing AV/AS/FW endpoint attributes to the corresponding replacement AM/FW endpoint attributes before you upgrade. See the AnyConnect HostScan 4.3.x to 4.6.x Migration Guide for a full upgrade & migration procedure.

# Endpoint Attribute Definitions

The following endpoint selection attributes are available for DAP use.The Attribute Name field shows you how to enter each attribute name in a LUA logical expression, used in the Advanced area in Dynamic Access Policy Selection Criteria pane. The *label* variable identifies the application, filename, process, or registry entry.

| Attribute Type | Attribute Name | Source | Value | Max String Length | Description |
|---|---|---|---|---|---|
| Antimalware<br>(Requires Cisco Secure Desktop) | endpoint.am["*label*"].exists | Host Scan | true | — | Antimalware program exists |
| | endpoint.am["*label*"].version | | string | 32 | Version |
| | endpoint.am["*label*"].description | | string | 128 | Antimalware description |
| | endpoint.am["*label*"].lastupdate | | integer | — | Seconds since update of antimalware definitions |
| Personal firewall<br>(Requires Secure Desktop) | endpoint.pfw["*label*"].exists | Host Scan | true | — | The personal firewall exists |
| | endpoint.pfw["*label*"].version | | string | string | Version |
| | endpoint.pfw["*label*"].description | | string | 128 | Personal firewall description |
| AnyConnect<br>(Does not require Cisco Secure Desktop or Host Scan) | endpoint.anyconnect.clientversion | Endpoint | version | — | AnyConnect client version |
| | endpoint.anyconnect.platform | | string | — | Operating system on which AnyConnect client is installed |
| | endpoint.anyconnect.platformversion | | version | 64 | Version of operating system on which AnyConnect client is installed |
| | endpoint.anyconnect.devicetype | | string | 64 | Mobile device type on which AnyConnect client is installed |
| | endpoint.anyconnect.deviceuniqueid | | | 64 | Unique ID of mobile device on which AnyConnect client is installed |
| | endpoint.anyconnect.macaddress | | string | — | MAC Address of device on which AnyConnect client is installed<br>Must be in the format xx-xx-xx-xx-xx-xx, where 'x' is a valid hexadecimal character |

| Attribute Type | Attribute Name | Source | Value | Max String Length | Description |
|---|---|---|---|---|---|
| Application | endpoint.application. clienttype | Application | string | — | Client type:<br>CLIENTLESS<br>ANYCONNECT<br>IPSEC<br>L2TP |
| Device | endpoint.device. hostname | Endpoint | string | 64 | Host Name only. Not FQDN |
| | endpoint.device.MAC | | string | — | Mac Address for a network interface card. Only one Mac address per entry<br>Must be in the format xxxx.xxxx.xxxx where x is a hexadecimal character. |
| | endpoint.device.id | | string | 64 | BIOS Serial Number. The number format is manufacturer-specific. There is no format requirement |
| | endpoint.device.port | | string | — | TCP port in listening state<br>You can define a single port per line<br>An integer between 1 and 65535 |
| | endpoint.device. protection_version | | string | 64 | Version of Host Scan image they are running |
| | endpoint.device. protection_extension | | string | 64 | Version of Endpoint Assessment (OPSWAT) |
| File | endpoint.file["*label*"].exists | Secure Desktop | true | — | The files exists |
| | endpoint.file[“label”]. endpointid | | | | |
| | endpoint.file["*label*"]. lastmodified | | integer | — | Seconds since file was last modified |
| | endpoint.file["*label*"]. crc.32 | | integer | — | CRC32 hash of the file |

| Attribute Type | Attribute Name | Source | Value | Max String Length | Description |
|---|---|---|---|---|---|
| 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 |
| 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 | *dword string* | — | dword |
| | endpoint. registry["*label*"].value | | string | 255 | Value of the registry entry |
| VLAN | endoint.vlan.type | CNA | string | — | VLAN type:<br>ACCESS AUTH ERROR GUEST QUARANTINE ERROR STATIC TIMEOUT |

# Create Additional DAP Selection Criteria in DAP Using LUA

This section provides information about constructing logical expressions for AAA or endpoint attributes. Be aware that doing so requires sophisticated knowledge of LUA. You can find detailed LUA programming information at http://www.lua.org/manual/5.1/manual.html.

In the Advanced field 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 ASA 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 ASA 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 in LUA and enter them here.

The following sections provide detailed explanations of creating LUA EVAL expressions, as well as examples.

• Syntax for Creating LUA EVAL Expressions, on page 22

• Examples of DAP EVAL Expressions, on page 26
• Additional LUA Functions, on page 23

# Syntax for Creating LUA EVAL Expressions

**Note** If you must use Advanced mode, 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 Endpoint Attribute Definitions, on page 18 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 |
| | “” | 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 |

# LUA Procedures for HostScan 4.6 and Later

# LUA Script for 'ANY' Antimalware (endpoint.am) with Last Update

Use the following LUA script to check for 'ANY' antimalware product/vendor (endpoint.am). Modifications may apply to accommodate a different Last Update interval. The following example shows how a Last Update must have been performed in <30 days (noted as 2592000 seconds).

```
assert(function()
  for k,v in pairs(endpoint.am) do
    if(EVAL(v.activescan, "EQ", "ok", "string")and EVAL (v.lastupdate, "LT", "2592000",
"integer"))
     then
              return true
         end
  end
  return false
end)()
```

# LUA Script for 'ANY' Personal Firewall

Use the following LUA script to check for 'ANY' firewall product/vendor (endpoint.pfw):

```
assert(function()
    for k,v in pairs(endpoint.pfw) do
         if (EVAL(v.enabled, "EQ", "ok", "string")) then
              return true
         end
    end
    return false
end)()
```

# Additional LUA Functions

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

- CheckAndMsg is a LUA function that you can configure DAP to call. It generates a user message based on a condition.
- Organizational Unit (OU) or other level of the hierarchy for the user object.
- Group names that follow a naming convention with many possible matches might require the ability to use a wildcard.

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

### The DAP CheckAndMsg Function

The ASA displays the message to the user only when the DAP record containing the LUA CheckAndMsg function is selected and results in a connection 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 appliance uses it to determine whether to choose the DAP record. If the record is selected and results in termination, the security appliance displays the appropriate message.

### OU-Based Match Example

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 this criteria as follows:

```
assert(function()
   if ( (type(aaa.ldap.distinguishedName) == "string") and
        (string.find(aaa.ldap.distinguishedName, "OU=Admins,dc=cisco,dc=com$") ~= nil) )
then
       return true
   end
   return false
end)()
```

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()
   local pattern = "-stu$"
   local attribute = aaa.ldap.memberOf
   if ((type(attribute) == "string") and
       (string.find(attribute, pattern) ~= nil)) then
```

```
        return true
    elseif (type(attribute) == "table") then
        local k, v
        for k, v in pairs(attribute) do
            if (string.find(v, pattern) ~= nil) then
                return true
            end
        end
    end
    return false
end)()
```

### Deny Access Example

You can use the following function to deny access in the absence of an antimalware program. Use it with a DAP that has Action set to terminate.

```
assert(
    function()
for k,v in pairs(endpoint.am) do

        if (EVAL(v.exists, "EQ", "true", "string")) then

            return false

        end
    end
    return CheckAndMsg(true, "Please install antimalware software before connecting.", nil)
end)()
```

If a user lacking an antimalware program attempts to log in, DAP displays the following message:

```
Please install antimalware software before connecting.
```

### Multiple Certificate Authentication Example

You can definite a wildcard issuer CN with Multiple Certificate Authentication in DAP rules.

If you have configured two certificates issued to two different machines by two different certificate authorities (for example abc.cisco.com and xyz.cisco.com), then the DAP rule must have a condition for multiple certificate authentication where the issuer CN is be *.cisco.com or cisco.com.

You can use the following function to define a DAP rule for certificate with wildcard issuer_cn cisco.com for user and machine certificates:

```
assert(
 function()
  if ((string.find(endpoint.cert[1].issuer.cn[0], "cisco.com") ~= nil) and
   (string.find(endpoint.cert[2].issuer.cn[0], "cisco.com") ~= nil)) then
     return true;
 end
 return false;
end)()
```

# Examples of DAP EVAL Expressions

Study these examples for help in creating logical expressions in LUA:

| Description | Example |
|---|---|
| Endpoint LUA checks for Windows 10 | `(EVAL(endpoint.os.version,"EQ","Windows 10","string"))` |
| Endpoint LUA checks for a match on CLIENTLESS OR CVC client types. | `(EVAL(endpoint.application.clienttype,”EQ”,"CLIENTLESS") or EVAL(endpoint.application.clienttype, “EQ”,"CVC"))` |
| Endpoint LUA checks if a single Antimalware program Symantec Enterprise Protection is installed on the user PC, displays a message if it is not. | `(CheckAndMsg(EVAL(endpoint.am["538"].description,"NE","Symantec Endpoint Protection","string"),"Symantec Endpoint Protection was not found on your computer", nil))` |
| Endpoint LUA checks for McAfee Endpoint Protection versions 10 to 10.5.3 and versions above 10.6. | `(EVAL(endpoint.am["1637"].version,"GE","10","version") and EVAL(endpoint.am["1637"].version,"LT","10.5.4","version") or EVAL(endpoint.am["1637"].version,"GE","10.6","version"))` |
| Endpoint LUA checks if McAfee Antimalware definitions have been updated within the last 10 days(864000 sec) and displays a message if an update is needed. | `(CheckAndMsg(EVAL(endpoint.am["1637"].lastupdate,"GT","864000","integer"),"Update needed! Please wait for McAfee to load the latest dat file.", nil))` |
| Check for a specific hotfix after debug dap trace returns: `endpoint.os.windows.hotfix["KB923414"] = "true";` | `(CheckAndMsg(EVAL(endpoint.os.windows.hotfix["KB923414"],"NE","true"), "The required hotfix is not installed on your PC.",nil))` |

### Check for Antimalware Programs and Provide Messages

You can configure messages so that the end users are aware of and able to fix problems with their antimalware software. If access is allowed, the ASA displays all messages generated in the process of DAP evaluation on the portal page. If access is denied, the ASA collects all messages for the DAP that caused the "terminate" condition and displays them in the browser on the logon page.

The following example shows how to use this feature to check on the status of Symantec Endpoint Protection.

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.am["538"].description,"EQ","Symantec Endpoint
   Protection","string") and EVAL(endpoint.am["538"].activescan,"NE","ok","string") "Symantec
    Endpoint Protection is disabled. You must enable before being granted access", nil))
   ```

2. In that same Advanced field, click the **OR** button.
3. In the Access Attributes section below, in the leftmost tab, Action**,** click **Terminate**.

4. Connect from a PC that has Symantec Endpoint Protection installed, but has Symantec Endpoint Protection disabled. The expected result is that the connection is not allowed and that the user will be presented the message "Symantec Endpoint Protection is disabled. You must enable before being granted access."

### Check for Antimalware Programs and Definitions Older than 2 Days

This example checks for the presence of the Symantec and McAfee antimalware programs, and whether the virus definitions are older than 2 days (172,800 seconds). If the definitions are older than 2 days, the ASA terminates the session with a message and links for remediation. To accomplish this task, perform the following steps.

1. Copy and paste the following LUA expression into the Advanced field of the Add/Edit Dynamic Access Policy pane:

```
(CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint
Protection","string") and EVAL(endpoint.am["538"].lastupdate,"GT","172800","integer"),
"Symantec Endpoint Protection Virus Definitions are Out of Date. You must run LiveUpdate
 before being granted access", nil)) or
(CheckAndMsg(EVAL(endpoint.am["1637"].description,"EQ","McAfee Endpoint
Security","string") and EVAL(endpoint.am["1637"].lastupdate,"GT","172800","integer"),
"McAfee Endpoint Security Virus Definitions are Out of Date. You must update your McAfee
 Virus Definitions before being granted access", nil))
```

2. In that same Advanced field, click **AND**.
3. In the Access Attributes section below, in leftmost tab Action, click **Terminate**.
4. Connect from a PC that has Symantec and McAfee antimalware programs with versions that are older than 2 days.

   The expected result is that the connection is not allowed and that the user is presented a message that the virus definitions are out of date.

# Configure DAP Access and Authorization Policy Attributes

Click each of the tabs and configure the contained fields.

### Procedure

**Step 1** Select the **Action** tab to specify special processing to apply to a specific connection or session.

- Continue—(Default) Click to apply access policy attributes to the session.
- Quarantine—Through the use of quarantine, you can restrict a particular client who already has an established tunnel through a VPN. ASA applies restricted ACLs to a session to form a restricted group, based on the selected DAP record. When an endpoint is not compliant with an administratively defined policy, the user can still access services for remediation, but restrictions are placed upon the user. After the remediation occurs, the user can reconnect, which invokes a new posture assessment. If this assessment passes, the user connects. This parameter requires an AnyConnect release that supports AnyConnect Secure Mobility features.
- 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 490 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.

  You can include URLs or other embedded text, which require that you use the correct HTML tags. For example: All contractors read <a href='http://wwwin.example.com/procedure.html'> Instructions</a> for the procedure to upgrade your anti-malware software.

**Step 2** Select the **Network ACL Filters** tab to 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 ASA rejects it.

- Network ACL drop-down list—Select already configured network ACLs to add to this DAP record. The ACLs may be any combination of permit and deny rules. This field supports unified ACLs which can define access rules for IPv4 and IPv6 network traffic.
- **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 list 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 ASA unless you first delete it from DAP records.

**Step 3** Select the **Web-Type ACL Filters (clientless)** tab to 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 ASA rejects it.

- **Web-Type ACL** drop-down list—Select already configured web-type ACLs to add to this DAP record. The ACLs may be any combination of permit and deny rules.
- **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 list 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 ASA unless you first delete it from DAP records.

**Step 4** Select the **Functions** tab to 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.

  Browsing requires NBNS (Master Browser or WINS). If that fails or is not configured, we use DNS. 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 PC or workstation and the ASA 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 ASA to the destination web server is not secured.

In a clientless VPN connection, the ASA 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 ASA 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 ASA 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, choose 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.

**Step 5** Select the **Port Forwarding Lists** tab to 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) 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 list—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 list 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 ASA unless you first delete it from DAP records.

**Step 6** Select the **Bookmarks** tab to configure bookmarks for certain user session URLs.

- **Enable bookmarks**—Click to enable. When unchecked, no bookmarks display in the portal page for the connection.
- **Bookmark** drop-down list—Choose already configured bookmarks to add to the DAP record.
- **Manage...**—Click to add, import, export, and delete bookmarks.
- **Bookmarks (unlabeled)**—Displays the URL lists for the DAP record.
- **Add>>**—Click to add the selected bookmark from the drop-down list to the URL area on the right.
- **Delete**—Click to delete the selected bookmark from the URL list area. You cannot delete a bookmark from the ASA unless you first delete it from DAP records.

**Step 7** Select the **Access Method** tab to 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.

**Step 8** Select the **AnyConnect** tab to choose the status of the Always-on VPN flag.

- Always-On VPN for AnyConnect client—Determine if the always-on VPN flag setting in the AnyConnect service profile is unchanged, disabled, or if the AnyConnect profile setting should be used.

  This parameter requires a release of the Cisco Web Security appliance that provides Secure Mobility Solution licensing support for the Cisco AnyConnect VPN client. It also requires an AnyConnect release that supports “Secure Mobility Solution” features. Refer to the *Cisco AnyConnect VPN Client Administrator Guide* for additional information.

**Step 9** Select the **AnyConnect Custom Attributes** tab to view and associate previously defined custom attributes to this policy. You can also define custom attributes and then associate them with this policy.

Custom attributes are sent to and used by the AnyConnect client to configure features such as Deferred Upgrade. A custom attribute has a type and a named value. The type of the attribute is defined first, then one or more named values of this type can be defined. For details about the specific custom attributes to configure for a feature, see the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for the AnyConnect release you are using.

Custom attributes can be predefined in **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes** and **AnyConnect Custom Attribute Names**. Predefined custom attributes are used by both Dynamic Access Policies and Group Policies.

# Configure SAML Authorization Using DAP

You can configure SAML authorization and group policy selections using DAP, without having to rely on an external server (RADIUS or LDAP) to retrieve authorization attributes.

The SAML Identity Provider can be configured to send authorization attributes in addition to the authentication assertions. The SAML Service Provider component in ASA interprets the SAML assertions and makes authorization or group policy selections based on the received assertions. The assertion attributes are processed using DAP rules configured by ASDM.

The Group Policy attribute must use the attribute name **cisco_group_policy**. This attribute is not dependent on DAP being configured. However, if a DAP is configured, it can be used as part of the DAP policy.

**Group Policy Selection**

If an attribute with the name **cisco_group_policy** is received, the corresponding value is used to select the connection group-policy.

When a connection is made, group-policy information can be taken from multiple sources and combined to form an effective group-policy that is applied to the connection.

The following scenarios are possible while combining the group-policy information received:

**Group-policy received in SAML authentication, authorization NOT configured**

In this scenario, the effective group-policy is determined as follows in order of decreasing priority:

1. Group-policy specified in SAML attribute.
2. Group-policy specified in the tunnel-group.
3. Default group-policy.

**Group-policy received in SAML authentication, authorization configured**

In this scenario, the effective group-policy is determined as follows in order of decreasing priority:

1. Group-policy specified in authorization attributes.
2. User group-policy: use value returned from authorization server if present.
3. User group-policy: use the value returned in SAML attribute.

4. Group-policy specified in the tunnel-group.
5. Default group-policy.

**Procedure**

**Step 1** In ASDM, select **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Dynamic Access Policies** > **Add/Edit Dynamic Access Policy** .

**Step 2** In the AAA attributes selection area, click **Add**.

a) From the **AAA Attribute Type** drop down, select SAML.
b) Specify *memberOf* as the **Attribute ID**.
c) Enter the *memberOf* attribute **Value** or click **Get AD Group** if the AD server groups are configured.

To configure additional AD Server Groups go to **Configuration** > **Remote Access VPN** > **AAA/Local Users** > **AAA Server Groups**.

To configure group-policy selection attributes, select the following settings in the same DAP policy or in another DAP policy as required:

- **AAA Attribute Type**: SAML
- **Attribute ID**: cisco_group_policy
- **Value**: Name of the group policy

**Step 3** Click **OK**.

**Step 4** Click **OK** to save the DAP policy.

# Perform a DAP Trace

A DAP trace displays the DAP endpoint attributes for all connected devices.

**Procedure**

**Step 1** Log on to the ASA from an SSH terminal and enter Privileged Exec mode.

In Privileged Exec mode, the ASA prompts: `hostname#`.

**Step 2** Enable DAP debugs to display all DAP attributes for the session in the terminal window:

```
hostname# debug dap trace
endpoint.anyconnect.clientversion="0.16.0021";
endpoint.anyconnect.platform="apple-ios";
endpoint.anyconnect.platformversion="4.1";
endpoint.anyconnect.devicetype="iPhone1,2";
endpoint.anyconnect.deviceuniqueid="dd13ce3547f2fa1b2c3d4e5f6g7h8i9j0fa03f75";
```

**Step 3** (Optional) In order to search the output of the DAP trace, send the output of the command to a system log. To learn more about logging on the ASA see *Configure Logging* in the *Cisco ASA Series General Operations ASDM Configuration Guide*.

# Examples of DAPs



## Use 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.

### Procedure

**Step 1** In ASDM, go to **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Dynamic Access Policies** > **Add/Edit Dynamic Access Policy** > **Endpoint**.

**Step 2** Configure the following attributes for each policy:

| 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** |

## Use 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. Define a DAP such that for a user in AD group (memberOf) = Engineering the ASA applies a configured Web-Type ACL.

**Procedure**

**Step 1** In ASDM got 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 list to choose **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 list to choose =, and in the adjacent field 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 list to choose the ACL you want to apply to users in the AD group (memberOf) = Engineering.

# Enforce CSD Checks and Apply 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 ASA. In addition, the ASA 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.

**Procedure**

**Step 1** In ASDM got 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 list to choose 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 list to choose =, and in the adjacent field 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 list to choose =, and in the adjacent field enter Employees.

**Step 7** For the AAA attribute type, use the drop-down list to choose Cisco.

**Step 8** Check the Tunnel group box, use the drop-down list to choose =, and in the adjacent drop-down list choose the appropriate tunnel group (connection policy).

**Step 9** In the Network ACL Filters tab of the Access Policy Attributes area, choose the ACLs to apply to users who meet the DAP criteria defined in the previous steps.

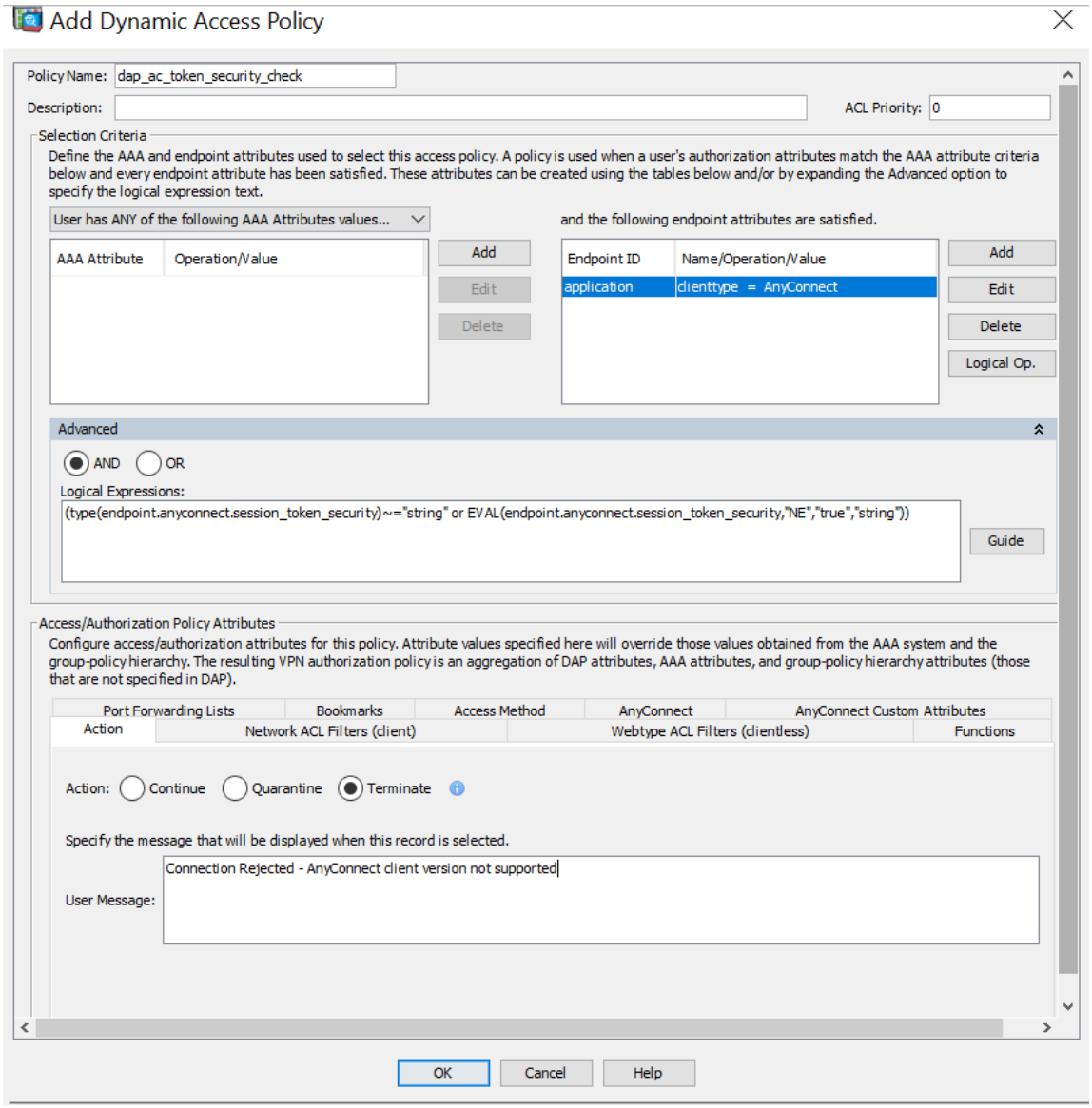
# Use DAP to Check Session Token Security

When the ASA authenticates a VPN connection request from the AnyConnect, the ASA returns a session token to the client. Starting with AnyConnect 4.9 (MR1), the ASA and AnyConnect client support a mechanism that provides enhanced security for the session token. You must configure a DAP to ensure that the AnyConnect client supports session token security.

Use the this DAP with endpoint attribute settings, and LUA script to reject connection attempts from AnyConnect versions that do not support token security.

### Procedure

**Step 1** In ASDM, select **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Dynamic Access Policies** > **Add/Edit Dynamic Access Policy** .




**Step 2** In the endpoint attributes selection area, click **Add**.

a) From the **Endpoint Attribute Type** drop down, select Application.

b) For the **Client Type**, select the equals (=) operator and then select AnyConnect from the drop-down.

c) Click **OK**.

**Step 3** Configure the **Advanced** selection criteria:

a) Select the **AND** operator.

b) Add the **Logical Expression**

```
(type(endpoint.anyconnect.session_token_security)~="string" or
EVAL(endpoint.anyconnect.session_token_security,"NE","true","string"))
```

**Step 4** In the **Action** area, select **Terminate**.

**Step 5** Add an optional User Message and click **OK**.