Cisco Secure Firewall Threat Defense Dynamic Access Policy Use Cases

First Published: 2021-07-08

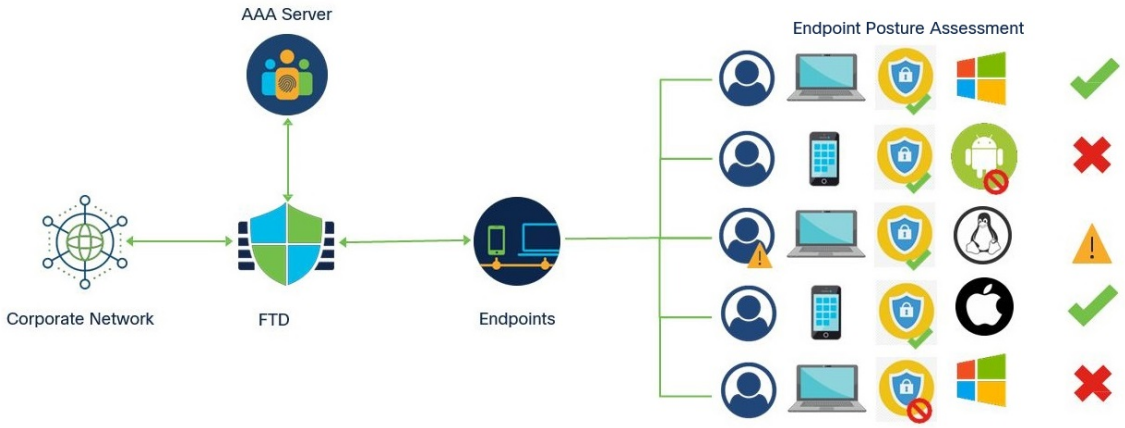
Last Modified: 2023-11-14

Cisco Secure Firewall Threat Defense Dynamic Access Policy

A Dynamic Access Policy (DAP) on Secure Firewall Threat Defense (formerly Firepower Threat Defense) allows you to configure authorization to address the dynamics of VPN environments. You can use the Secure Firewall Management Center (formerly Firepower Management Center) web interface to create a DAP by configuring a collection of access control attributes. You can associate the attributes with a specific user tunnel or session. These attributes address issues of multiple group memberships and endpoint security.

The threat defense grants VPN access to a particular user session based on your DAP configuration. threat defense selects and aggregates the attributes from one or more DAP records, and then generates a DAP during user authentication. threat defense selects the DAP records based on the endpoint security information of the remote device and AAA information. The threat defense then applies the DAP record to the user tunnel or session.

Figure 1: Dynamic Access Policy Example



Components of a DAP Configuration

A new DAP configuration requires creating a DAP policy, DAP record, and DAP criteria attributes:

- **Dynamic Access Policy**—A DAP configuration consists of records.
- **DAP Record**—A DAP record consists of criteria endpoint assessment and user authorization (AAA) attributes. If the record matches, DAP defines actions to be applied on the VPN session.
- **DAP Criteria and Attributes**—AAA Criteria, Endpoint Criteria, and Advanced criteria contain granular configuration attributes for network access.

For detailed configuration steps, see Configure a Dynamic Access Policy, on page 4.

How the Threat Defense Remote Access VPN Works with DAP

1. A remote user attempts VPN connection using the Secure Client from an endpoint device.
2. Threat Defense performs posture assessment on endpoints.
3. Threat Defense authenticates the user via the Authentication Authorization Accounting (AAA) server. The AAA server also returns authorization attributes for the user.
4. Threat Defense applies AAA authorization attributes to the session and establishes the VPN tunnel.
5. The threat defense selects DAP records based on the user AAA authorization information and posture assessment information.
6. Threat Defense aggregates DAP attributes from the selected DAP records and creates the DAP policy.
7. Threat Defense applies the DAP policy to the remote access VPN session.

Why Implement DAP?

You can configure DAP attributes to identify a connecting endpoint and authorize user access to various network resources. You can create a DAP for the following scenarios and can do more with DAP attributes to protect your endpoints and network resources:

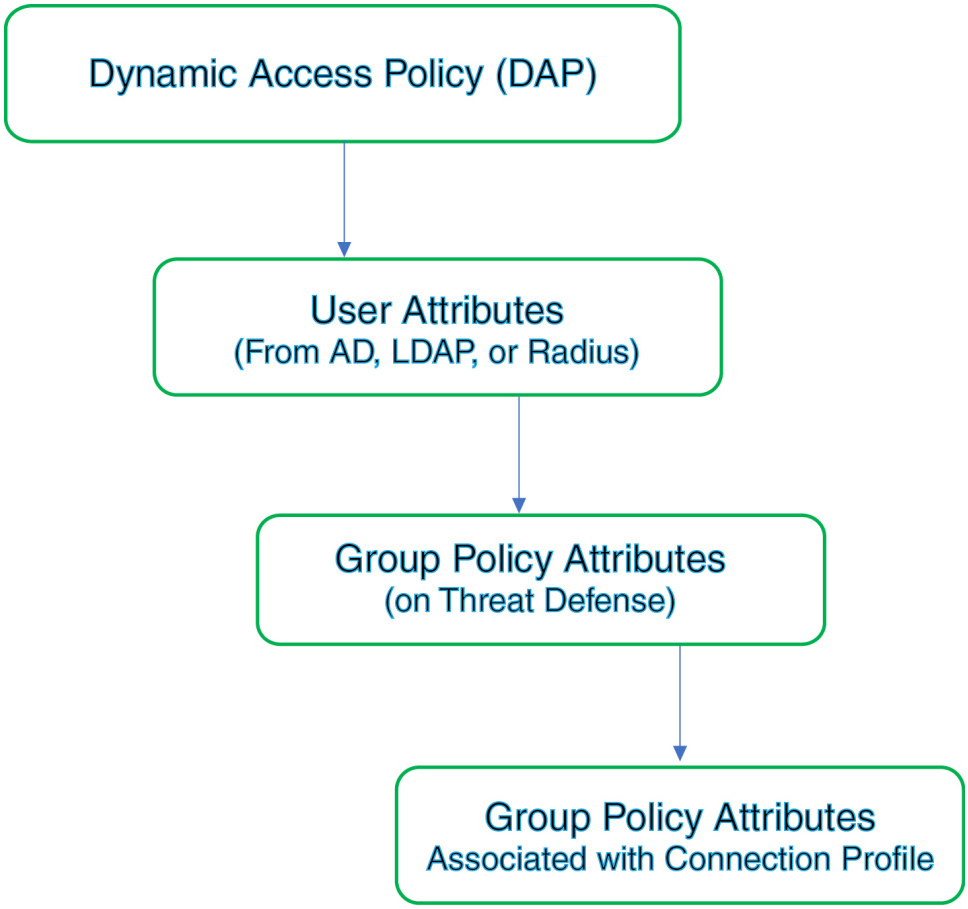
- Ensure that the endpoints connecting to the VPN comply with security policies of an organization, irrespective of the endpoint device or platform.
- Identify operating systems, various security software running on the endpoint, registry settings, file versions, and potential keystroke loggers running on the endpoints.
- Detect and enforce availability and update of the applications on company-managed endpoints. For example, anti-virus software
- Determine the network resources that the authorized users can access.

Policy Enforcement of Permissions and Attributes in Threat Defense

The threat defense device supports applying user authorization attributes (also called user entitlements or permissions) to VPN connections. The attributes are applied from a DAP on the 457903threat defense, external authentication server and/or authorization AAA server (RADIUS) or from a group policy on the threat defense device.

If the threat defense device receives attributes from all sources, threat defense evaluates, merges, and applies to the user policy. If conflicts occur among attributes coming from the DAP, the AAA server, or the group policy, the attributes obtained from the DAP always take precedence.

Figure 2: Policy Enforcement Flow



1. **DAP attributes on the** Threat Defense—The DAP attributes take precedence over all others.
2. **User attributes on the external AAA server**—The server returns these attributes after successful user authentication and/or authorization.
3. **Group policy configured on the** Threat Defense —If a RADIUS server returns the value of the RADIUS Class attribute IETF-Class-25 (OU= group-policy) for the user, the threat defense device places the user in the group policy of the same name and enforces any attributes in the group policy that are not returned by the server.
4. **Group policy assigned by the Connection Profile (also known as Tunnel Group)**—The Connection Profile has the preliminary settings for the connection, and includes a default group policy applied to the user before authentication.

Note The threat defense device does not support inheriting system default attributes from the default group policy, *DfltGrpPolicy*. The group policy attributes assigned from the connection profile are used for the user session, if they are not overridden by user attributes or the group policy from the AAA server.

Licensing for Dynamic Access Policies

The threat defense must have one of the AnyConnect licenses that supports remote access VPN:

- Secure Client Premier
- Secure Client Advantage
- Secure Client VPN Only

The management center must have export-controlled features enabled.

For information about threat defense licenses, see the *Licensing the Firepower System* chapter of the *Cisco Secure Firewall Management Center Configuration Guide*.

Configure a Dynamic Access Policy

A dynamic access policy (DAP) can contain multiple DAP records, where you configure user and endpoint attributes. You can prioritize the DAP records so that the required criteria is applied when a user attempts a VPN connection.

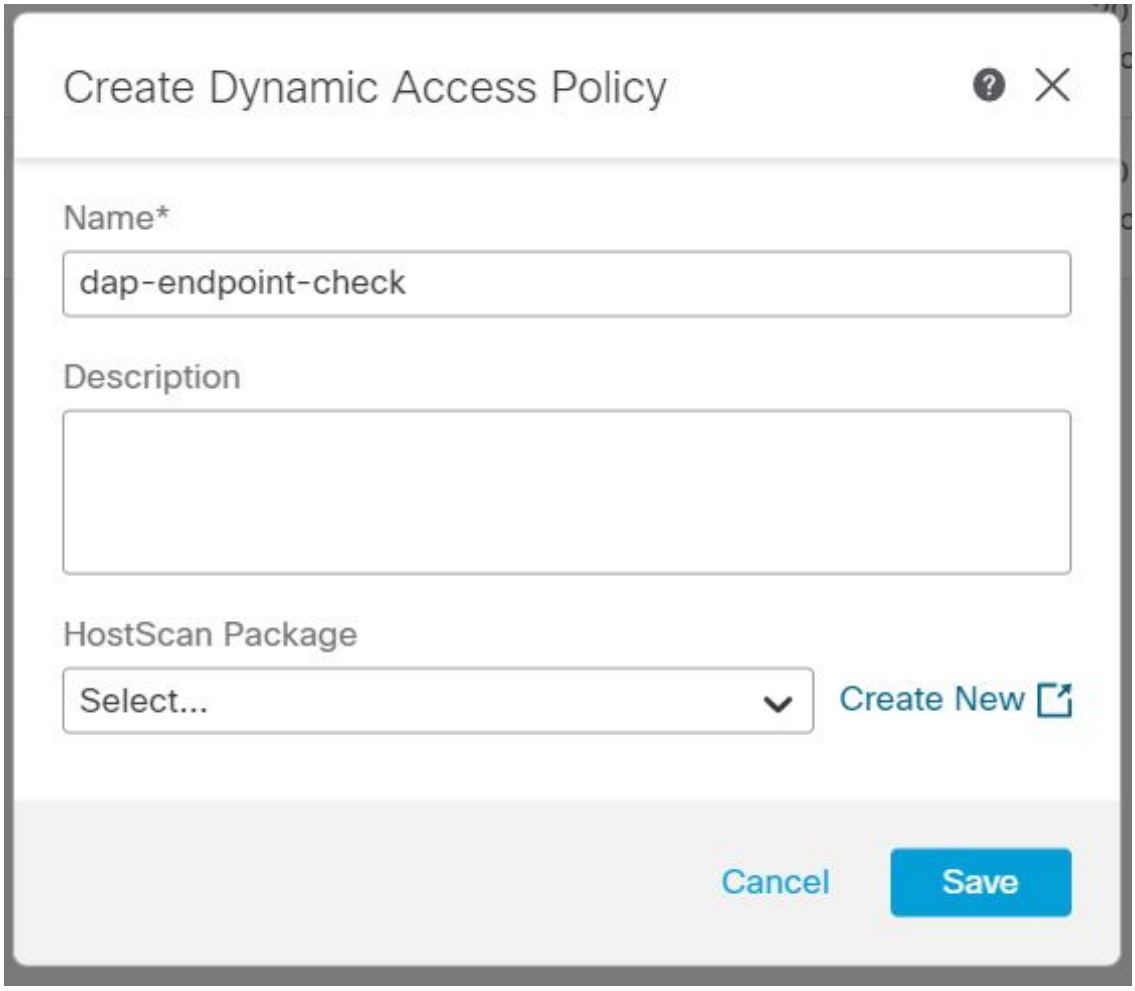
Before you begin

Ensure that you configure the required applications and settings before creating a dynamic access policy (DAP):

- **HostScan Package**—Download the HostScan Package version 4.6 or above.
- **AAA Server**—Configure the required AAA servers to return the correct attributes while authenticating or authorizing VPN sessions.
- **Secure Client Package**—Download the latest version of the Cisco Secure Client and add it to your remote access VPN configuration.
- **Remote Access VPN**—Configure the settings for your remote access VPN using the Remote Access VPN configuration wizard under **Devices** > **VPN** > **Remote Access**.
- Upload the HostScan package at **Objects** > **Object Management** > **VPN** > **AnyConnect File**.

1. Configure a new dynamic policy if you have not done already.
   a) Choose **Devices** > **Dynamic Access Policy** > **Create Dynamic Access Policy**.

Figure 3: Creating a Dynamic Access Policy



b) Specify a **Name** for the DAP policy and an optional **Description**.

c) Select the **HostScan Package** from the drop-down; or click **Create New** to add a HostScan package file.
A dynamic access policy contains a default DAP record. You can start adding DAP records with required attributes under AAA Criteria, Endpoint Criteria, and Advanced criteria using the Lua script.

d) Click **Save**.

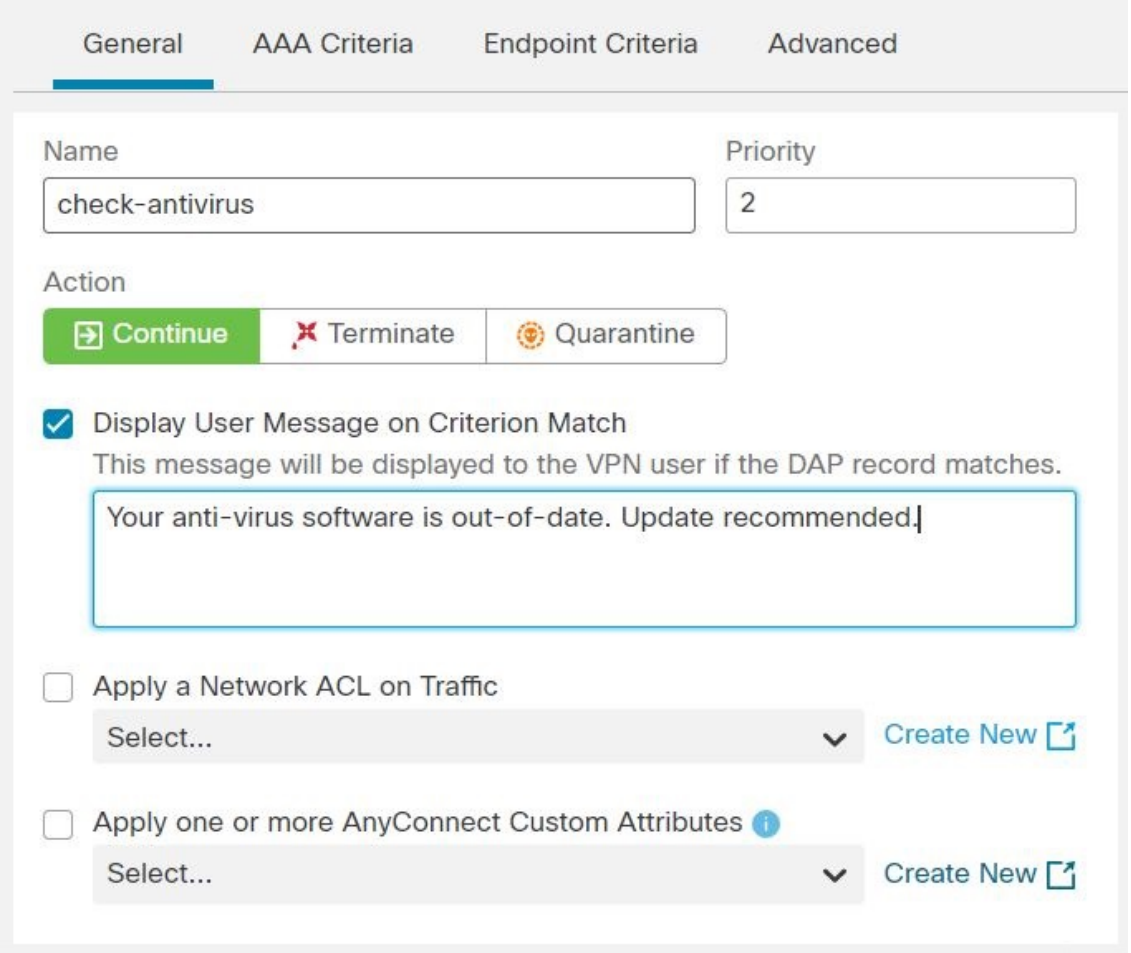
2. Create a DAP record, and assign a priority number.

A DAP record contains the attributes for matching when a VPN user attempts a VPN connection to threat defense VPN gateway. You can use the DAP record settings to grant, deny, or restrict VPN access based on the selected criteria attributes.

The **Priority** number indicates the order in which a record matches. threat defense uses the priority number of a DAP record to sequence and select the record. The lower the number the higher the priority.

Note If you do not configure a DAP record for a DAP, the **default DAP** record is applied. The default DAP record does not have a priority.

a) Choose **Devices** > **Dynamic Access Policy**.
b) Edit an existing DAP policy or create a new one.
c) Click **Create DAP Record**.



d) Specify the **Name** for the DAP record.
e) Enter the **Priority** number for the DAP record.
f) Select an **Action** to take if DAP record matches:

- **Continue**—Click to apply access policy attributes to the session and permit the user.
- **Terminate**—Select to terminate the session.
- **Quarantine**—Select to quarantine the connection.

g) Select **Display User Message on Criterion Match** and add the message in the box.

Note VPN users get the message when the DAP record matches.

h) Select the **Apply a Network ACL on Traffic** check box and select the ACL from the list. You can also create a new ACL and then select it.

The Network ACL is applied to the VPN session when this DAP record matches.

i) Select **Apply one or more AnyConnect Custom Attributes** and select the custom attributes object from the drop-down.

j) Click **Save**.

For information about Network ACL and AnyConnect Custom Attributes, see the latest Secure Firewall Management Center Configuration Guide.

k) Configure the DAP attributes to check when users and endpoints connect to the VPN.

- Configure AAA Criteria Settings for a DAP, on page 7
- Configure Endpoint Attribute Selection Criteria in a DAP, on page 9
- Configure Advanced Settings for a DAP, on page 11

3. Link the DAP with a remote access VPN configuration.

You must associate a DAP with a remote access VPN policy for the DAP attributes to match during VPN session authentication or authorization.

a) On the Secure Firewall Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

b) Select and edit the remote access policy where you want to add a DAP.

a) Click the Dynamic Access Policy association link.

b) Select a **Dynamic Access Policy** from the list.

c) Click **Ok**.

Once you associate a DAP to a remote access VPN, the threat defense checks the configured DAP records and attributes when a user attempts a VPN connection. The threat defense creates a DAP based on the matching and takes the appropriate action on the VPN session.

4. Deploy the remote access VPN on the threat defense devices.

a) On the management center menu bar, click **Deploy** and then select **Deployment**.

You can view the list of all the out-of-date configurations pending deployment on the threat defense devices.

b) Identify and choose the devices on which you want to deploy the remote access VPN and other configuration changes.

c) Click **Deploy**.

Note Rectify any errors before deploying the configuration.

Configure AAA Criteria Settings for a DAP

Threat Defense uses the AAA attributes attached to a VPN session by the AAA server to match a user or a user group.

DAP complements AAA services by providing a limited set of authorization attributes that can override the attributes that AAA provides. Threat Defense selects DAP records based on the AAA authorization information

and posture assessment information for a VPN session. The threat defense can choose multiple DAP records depending on the assessment, and then aggregate to create DAP authorization attributes.

Before you begin

Ensure that you have configured the required AAA servers for VPN user authentication, authorization, and accounting. The AAA servers must be reachable from the threat defense device, where you want to deploy your remote access VPN.

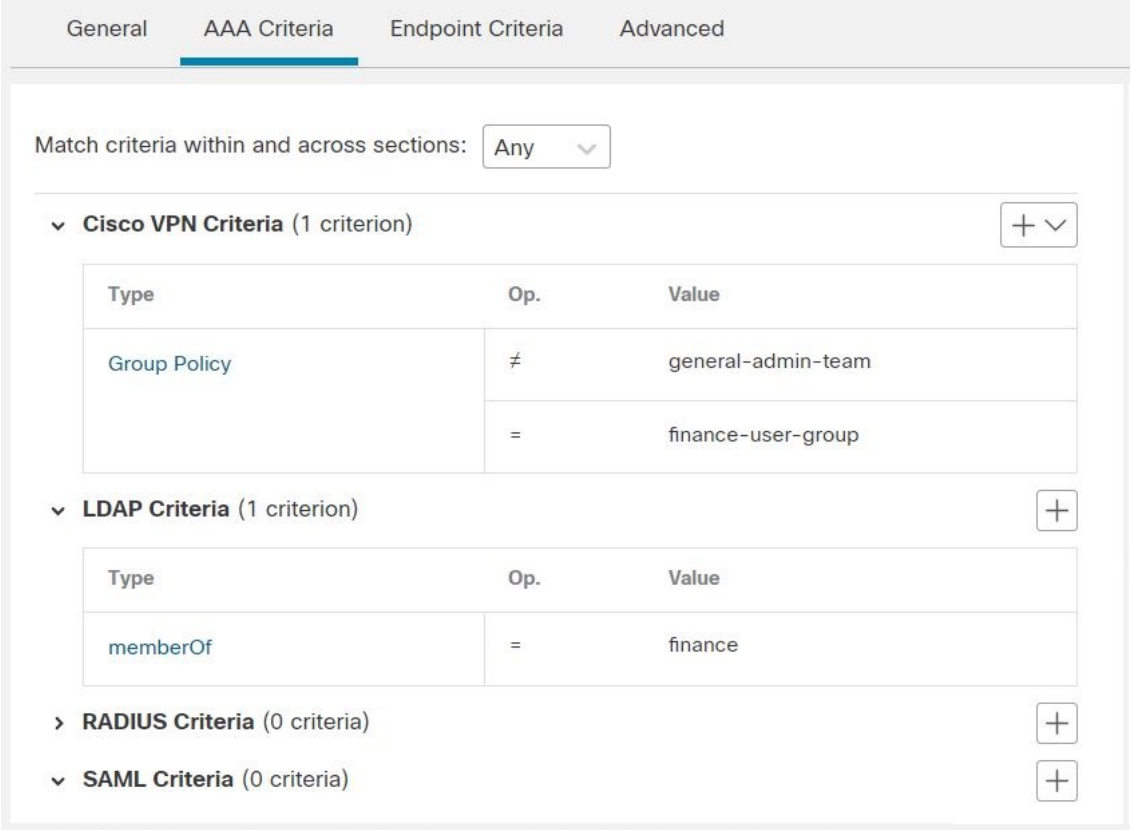
Procedure

Step 1 Choose **Devices** > **Dynamic Access Policy**.

Step 2 Edit an existing DAP policy or create a new one and then edit the policy.

Step 3 Select a DAP record or create a new one, and edit the DAP record.

Step 4 Click **AAA Criteria**.



Step 5 Select one of the **Match criteria between sections**:

- **Any**—matches any of the criteria.
- **All**—matches all the set criteria.
- **None**—matches none of the set criteria.

Step 6 Click **Add** to add the required **Cisco VPN Criteria**.

Cisco VPN Criteria include predefined attributes for group policy, assigned IPv4 address, assigned IPv6 address, connection profile, username, username 2, and SCEP required.

a) Select an **Attribute ID** and operator, and then specify **Value** to match.
b) Click **Add another criteria** to add more AAA criteria.
c) Click **Save**.

Step 7 Select **LDAP Criteria**, **RADIUS Criteria**, or **SAML Criteria**. Specify the **Attribute ID** and **Value**.

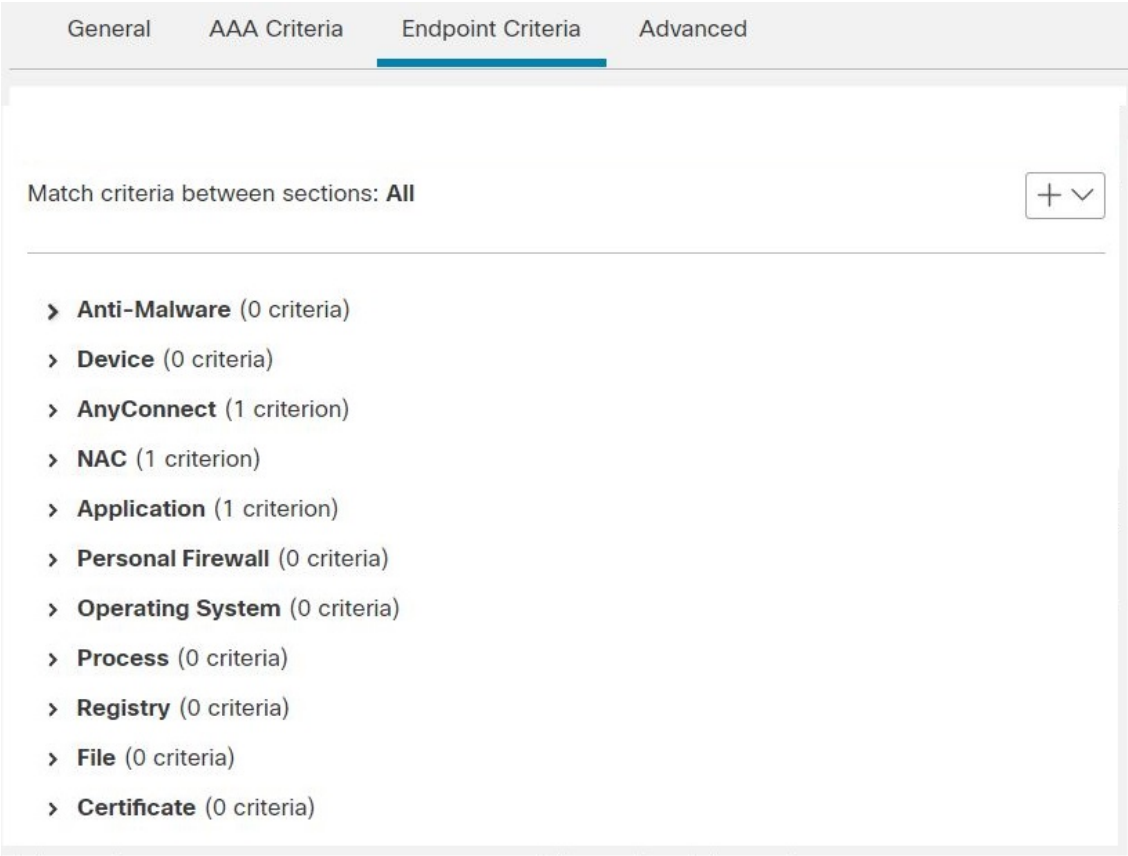
You can set these attributes either to = or ≠ the value you enter. You can add any number of AAA attributes for each DAP record.

Step 8 Click **Save**.

Configure Endpoint Attribute Selection Criteria in a DAP

Endpoint attributes contain information about the endpoint system environment, posture assessment results, and applications. The threat defense 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 satisfy for the threat defense to choose it for a session. The threat defense selects only DAP records that satisfy every condition configured.

Figure 4: DAP Endpoint Attributes



Procedure

Step 1 Choose **Devices** > **Dynamic Access Policy** > **Create Dynamic Access Policy**.

Step 2 Edit a DAP policy and then DAP record.

Note Create a DAP policy and DAP record if not done already.

Step 3 Click **Endpoint Criteria** and configure the required endpoint criteria attributes from the following attribute types:

- Anti-Malware
- Device
- Secure Client
- NAC
- Application
- Firewall
- Operating System

- Process
- Registry
- File
- Certificate

Note You can create multiple instances of each type of endpoint attribute. You can also add any number of endpoint attributes for each DAP record.

Step 4 Click **Save**.

Configure Advanced Settings for a DAP

You can use the Advanced tab for adding selection criteria other than what is possible in the AAA and endpoint attribute areas.

Create appropriate logical expressions in Lua and enter them here. You can use an assert function in the Lua script. This function returns the argument as true or a condition of the code; otherwise it displays the assert error message. For more information about assert functions and Lua scripts, see the Lua Reference Manual.

Procedure

Step 1 Choose **Devices** > **Dynamic Access Policy**.

Step 2 Edit a DAP policy and then edit a DAP record.

Note Create a DAP policy and DAP record if not done already.

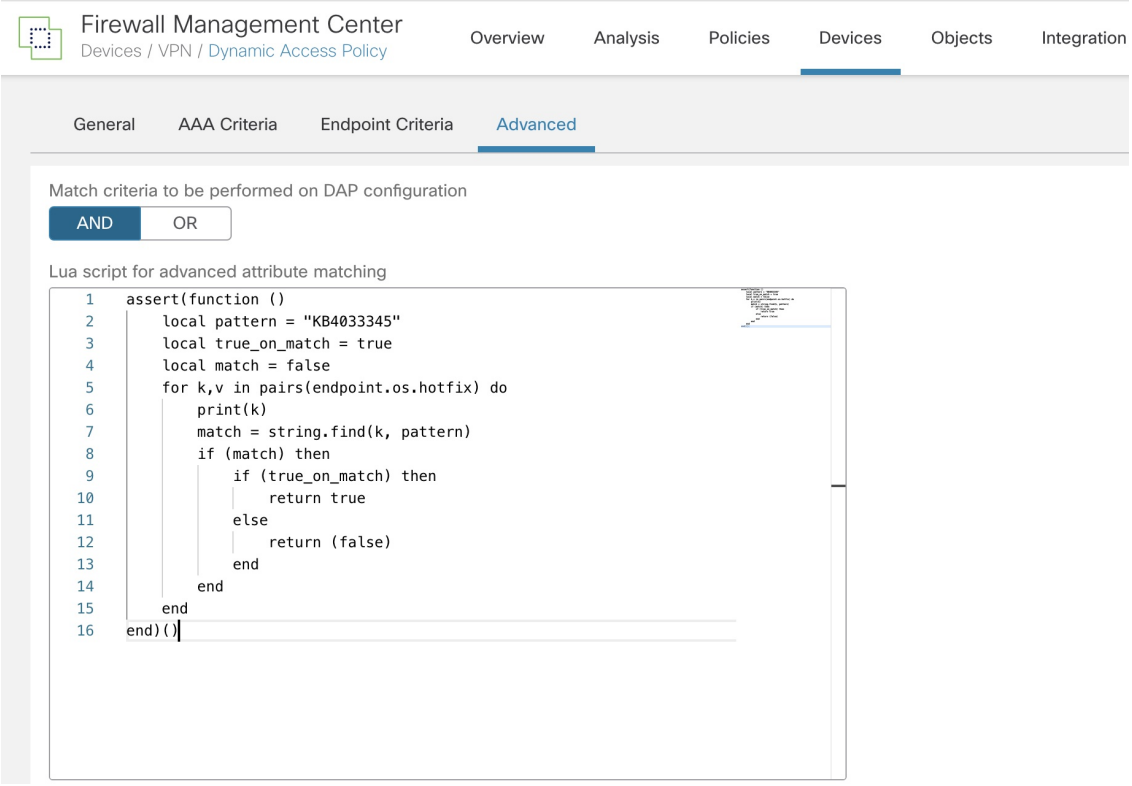
Step 3 Click the **Advanced** tab.

Step 4 Select **AND** or **OR** as the match criteria to match on DAP configuration.

Step 5 Add the lua script in the **Lua script for advanced attribute matching** field.

The script below checks for a particular hotfix in the client's OS (where Secure Client is installed), and returns true or false.

Figure 5: Advanced Criteria Matching Using Lua Script



Step 6 Click **Save**.

Troubleshooting Dynamic Access Policies

Before troubleshooting DAP issues:

- Enable VPN syslog in the Platform Settings policy.
- Check the DAP-related logs under **Devices** > **VPN** > **Troubleshooting** > **.**

Problem 1: Unable to save the DAP configuration

Solution

If you're not able to save the DAP configuration from the management center web interface, check the appropriate logs to find the reason for the failure:

- `/var/opt/CSCOpx/MDC/log/operation/vmssharedsvcs.log.*`
- `/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log.*`

You can use the keyword `vpn` or `sso` to filter related logs.

Problem 2: DAP deployment fails

Solution:

If the DAP deployment fails, check the deployment transcript details, and then check the log file `/var/opt/CSCOpx/MDC/log/operation/vmsbesvcs.log.*`

Examples for Dynamic Access Policy

This section provides example dynamic access policy (DAP) configurations to allow or block VPN access for VPN users and their endpoints.

Note The instructions provided in this document are example configurations. You can use various DAP settings to configure a single DAP record or multiple DAP records based on your requirements. The DAP settings include attributes under the AAA Criteria, Endpoint Criteria, and Advanced setting using the Lua script.

Based on your security requirements, you can configure a single DAP record for multiple criteria matching, or create multiple DAP records and prioritize them as required.

Allow or Block VPN Access Based on the Operating System

You can decide on the VPN access for endpoints based on the operating system. Use the example here to block endpoints running Windows operating system version 7 and not using the service pack SP1 Convenience Rollup.

Procedure

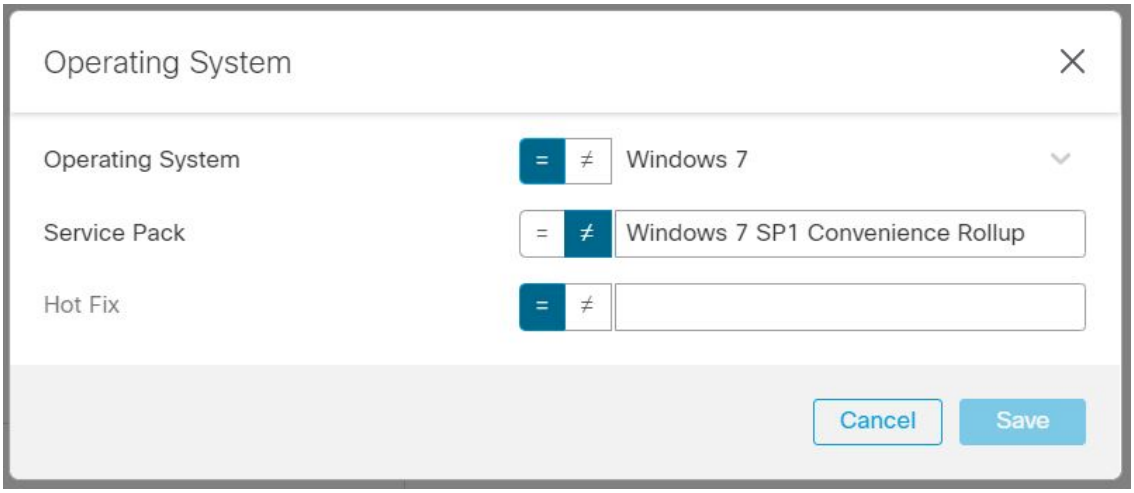
Step 1 Create a DAP record or edit and existing one with the **Terminate** action.

Step 2 Choose **Endpoint Criteria** > **Operating System** .

Step 3 Select the match criteria **All** to select criteria only when all the configured attributes match.

Step 4 Click **Add** to add operating system attributes.

Figure 6: DAP Operating System Endpoint Criteria



Step 5 Select the **Operating System**equals (=) operator, and then select *Windows 7*.

Step 6 Select the **Service Pack** not equals (≠) operator, and then specify *SP1 Convenience Rollup*.

Step 7 Click **Save**.

Block Traffic Based on Anti-Malware Attributes on Endpoints

The steps listed here allow you to configure anti-malware attributes to check when an endpoint tries to connect to the VPN. You can use the DAP record attributes to check,

- Whether the endpoint has Cisco Secure Endpoint installed and real-time scanning is enabled.
- If the Cisco Secure Endpoint version is greater than 1.1 and the anti-malware is updated within 15 days.

See Configure a Dynamic Access Policy, on page 4 for detailed instructions to configure a DAP on threat defense.

Procedure

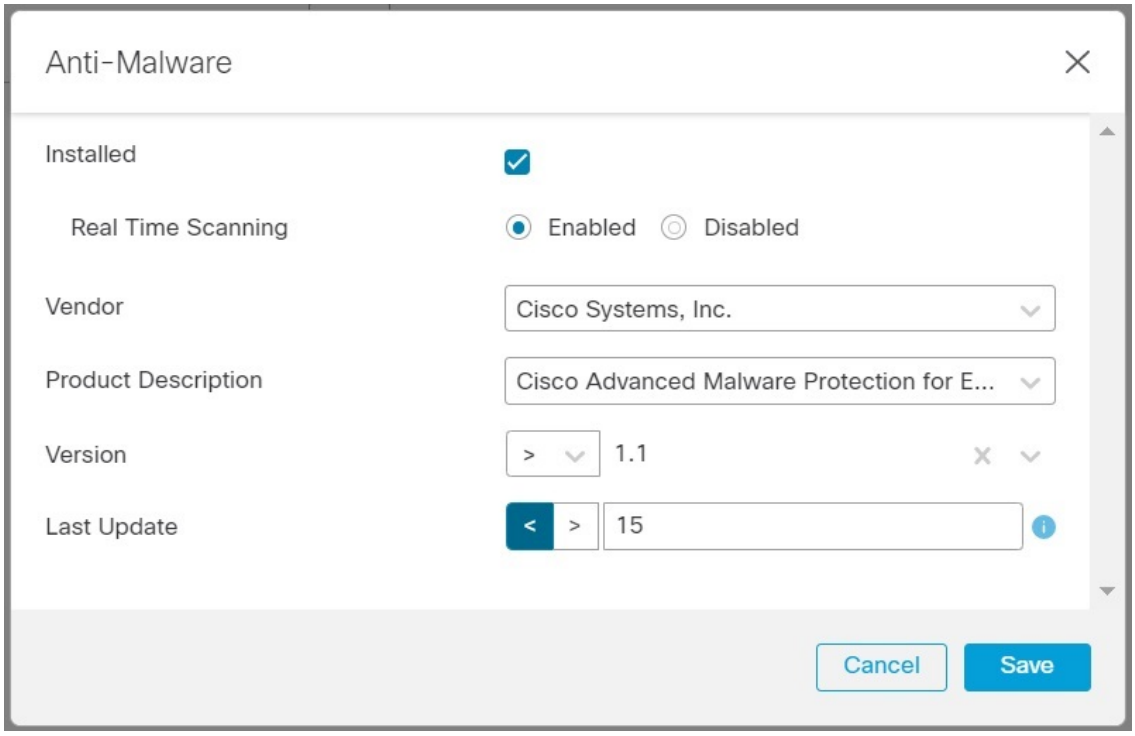
Step 1 Create a DAP record with **Terminate** action or edit an existing DAP record.

Step 2 Choose **Endpoint Criteria** > **Anti-Malware** in the DAP record.

Step 3 Select the match criteria **All** to select criteria only when all the configured attributes match or **Any** to any of the attributes.

Step 4 Click **Add** to add anti-malware attributes.

Figure 7: DAP Anti-Malware Endpoint Criteria



Step 5 Click **Installed** to indicate whether the anti-malware product is installed.

Step 6 Choose **Enabled** to check whether real-time malware scanning is active.

Step 7 Select the name of the anti-malware **Vendor** from the list.

For this example, select *Cisco Systems, Inc.* as the vendor for Cisco Secure Endpoint. Select the Vendor of your choice.

Step 8 Select the anti-malware **Product Description**, *Cisco Secure Endpoint*.

Note Select another vendor and product of your choice based the anti-malware product running on the endpoints connecting to your VPN.

Step 9 Choose the **Version** of the anti-malware product to be greater than 1.1.

Step 10 Specify the number of days since the **Last Update**.

Indicate that an anti-malware update must be less than (<) 15 days old.

Step 11 Click **Save**.

Allow or Block VPN Access for a Remote Access Application

To check the type of remote access connection to permit or deny VPN access for users, use the application endpoint criteria in a DAP record.

Procedure

Step 1 Create a DAP record or edit an existing one with the **Continue** or **Terminate** action as required.

Step 2 Choose **Endpoint Criteria** > **Application**.

Step 3 Select the match criteria **All** to select criteria only when all the configured attributes match or **Any** to any of the attributes.

Step 4 Click **Add** to add operating system attributes.

Figure 8: DAP Application Endpoint Criteria

Note You can use the example to allow or block the VPN users connecting using the Secure Client application.

You can select only the items that you want to check, and enter the required values. You can also choose to combine the Device check with another DAP record with multiple Endpoint or AAA criteria.

Step 5 Select the equals (=) or the not equals (≠) operator, and select the remote access **Client Type**.

The client types listed are Clientless, Cut-Through-Proxy, Secure Client, IPsec, L2TP, and IPsec-IKEv2-Generic-RA.

Step 6 Click **Save**.

Check the Endpoint Device to Allow or Block VPN Access

You can create a DAP criteria to allow or block VPN access for a specific device. Configure the device details to check for when a use attempts VPN connection.

Procedure

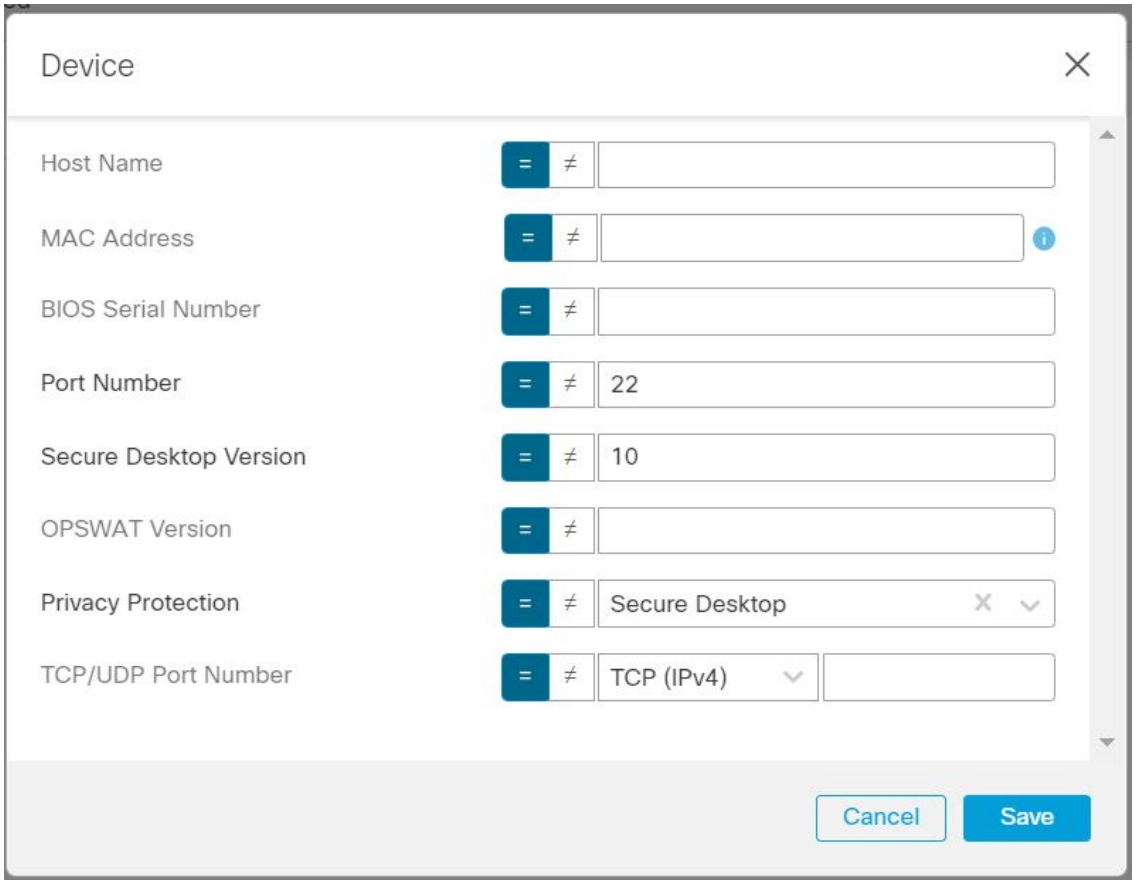
Step 1 Create a DAP record or edit an existing one with the **Continue** or **Terminate** action as required.

Step 2 Choose **Endpoint Criteria** > **Device**.

Step 3 Select the match criteria **All** to select criteria only when all the configured attributes match or **Any** to any of the attributes.

Step 4 Click **Add** to add operating system attributes.

Figure 9: DAP Device Endpoint Criteria Example



Note Use the example to allow or block endpoints connecting through port number 22, secure desktop version 10, and privacy protection Secure Desktop.

You can select only the items that you want to check and then enter the required values. You can also choose to combine the Device check with another DAP record with multiple Endpoint or AAA criteria.

Step 5 Select the equals (=) or the not equals (≠) operator and then specify the device information. Select the required fields and enter the values for the Host Name, MAC Address, BIOS Serial Number, Port Number, Secure Desktop Version, and OPSWAT Version.

Step 6 Select the equals (=) or the not equals (≠) operator, and select the Privacy Protection and TCP/UDP Port Number.

Step 7 Click **Save**.

Use the Lua Script to Check the Anti-Malware on Endpoints

The configuration example shown in this section provides the Lua script required to check the presence of an anti-malware product on endpoints.

Constructing logical expressions using the Lua script requires knowledge of LUA. You can find detailed LUA programming information at http://www.lua.org/manual/5.1/manual.html.

For more information, see the *Cisco Secure Firewall Threat Defense Dynamic Access Policies* section of the *Cisco Secure Firewall Management Center Configuration Guide*.

Procedure

Step 1 Create a DAP record or edit an existing DAP record.

Step 2 Click **Advanced** in the DAP record.

Step 3 Select the match criteria **AND** or **OR**.

Step 4 Copy the following script to the Lua script area:

```
assert(function()
local am_count = 0;
CheckAndMsg( true, "endpoint.av="..type(endpoint.am), nil)
for k,v in pairs(endpoint.am) do
am_count = am_count + 1
-- CheckAndMsg( true, "v.exists"..v.exists, nil)
-- CheckAndMsg( true, "v.description"..v.description, nil)
-- CheckAndMsg( true, "v.version"..v.version, nil)
-- CheckAndMsg( true, "v.activescan"..v.activescan, nil)
end
CheckAndMsg( true, "Your request has "..am_count.." Ams", nil)
return true
end)()
```

Step 5 Click **Save**.

AAA and Endpoint Attributes Supported in DAP

The threat defense device uses a DAP policy when the user attributes matches the configured AAA and endpoint attributes. The Host Scan modules of Cisco Secure Client return information to the device about the configured endpoint attributes. The DAP subsystem uses that information to choose a DAP record that matches the values of those attributes.

Most, but not all, antivirus, antispyware, 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 choose DAP records that specify the program.

AAA Attributes Supported in DAP

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.

Cisco VPN Criteria

The Cisco VPN criteria 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 IPv4 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).
- **Assigned IPv6 Address**—Enter the IPv6 address you want to specify for the policy.
- Connection Profile—The remote access VPN connection profile name. Maximum 64 characters.
- Username—The primary 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).
- Username2—The secondary username of the authenticated user. Maximum 64 characters.

LDAP Criteria

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 (AD) 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.

When the VPN remote access session to an LDAP authentication/authorization server returns the following three Active directory groups (memberOf enumerations), the Threat Defense Device processes three Active Directory groups:

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

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

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

These group 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 Criteria

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.

SAML Criteria

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 threat defense device 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 in the management center.

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.

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.

Endpoint Attributes Supported in DAP

For the list of antimalware and firewall vendors and applications that the HostScan application can detect and posture attributes available from those vendors that we support, see HostScan Antimalware and Firewall Support Charts.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.