

Dynamic Access Policies

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

- Firewall Threat Defense dynamic access policies, on page 1
- Prerequisites for dynamic access policy, on page 3
- Guidelines and limitations for dynamic access policies, on page 3
- Configure a Dynamic Access Policy (DAP), on page 4
- Associate dynamic access policy with remote access VPN, on page 14
- History for dynamic access policy, on page 14

Firewall Threat Defense dynamic access policies

A Secure Firewall Threat Defense dynamic access policy is a collection of access control attributes that

- addresses issues of multiple group memberships and endpoint security in VPN environments
- grants access to particular users for particular sessions according to defined policies, and
- adapts to dynamic environments with multiple variables affecting each VPN connection.

Dynamic access policy operation

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 inhabits within an organization, and log in attempts 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.

You can create a dynamic access policy by setting a collection of access control attributes that you associate with a specific user tunnel or session. The Firewall Threat Defense device generates a DAP during user authentication by selecting or aggregating attributes from one or more DAP records. The device then selects these DAP records based on the endpoint security information of the remote device and AAA authorization information for the authenticated user. Then the device applies the DAP record to the user tunnel or session.

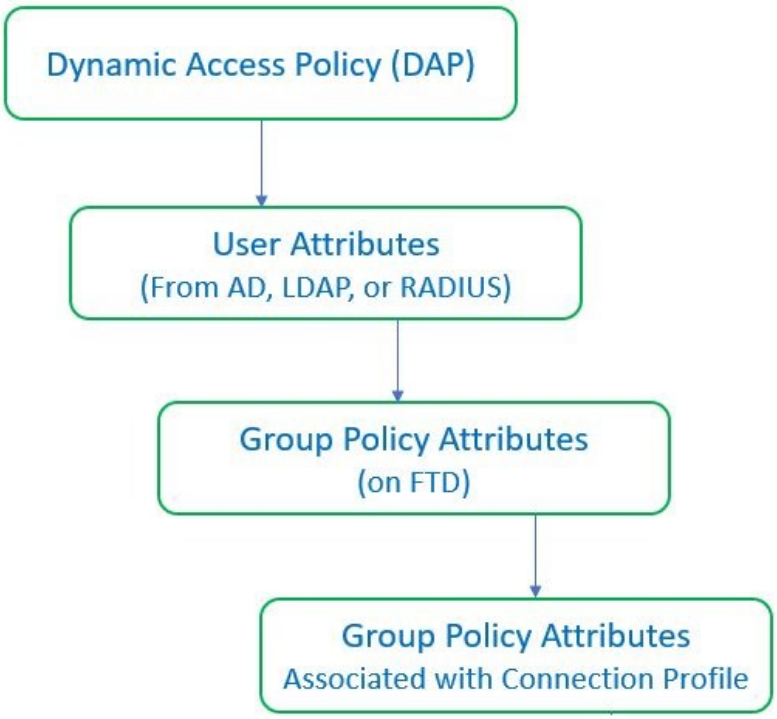
Hierarchy of policy enforcement of permissions and attributes in a Firewall Threat Defense device

The Firewall 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 Firewall Threat Defense, external authentication server and/or authorization AAA server (RADIUS) or from a group policy on the Firewall Threat Defense device.

If the Firewall Threat Defense device receives attributes from all sources, the device evaluates, merges, and applies the attributes to the user policy. If there are conflicts between attributes coming from the DAP, the AAA server, or the group policy, the attributes from the DAP always take precedence.

The Firewall Threat Defense device applies attributes in this order:

Figure 1: Policy enforcement flow



1. **DAP attributes on the FTD**—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 FTD**—If a RADIUS server returns the value of the RADIUS Class attribute IETF-Class-25 (OU= group-policy) for the user, the Firewall 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 that is applied to the user before authentication.

Note The Firewall Threat Defense device does not support inheriting system default attributes from the default group policy, *DfltGrpPolicy*. For the user session, the device uses the attributes on the group policy that you assign to the connection profile, unless the user attributes or the group policy from the AAA server overrides them.

Prerequisites for dynamic access policy

This reference provides the licensing prerequisites that must be met before configuring Dynamic Access Policy features.

Licensing prerequisites

- Firewall Threat Defense must have at least one of these AnyConnect Client licenses:
  - AnyConnect Apex
  - AnyConnect Plus
  - AnyConnect VPN Only
- The Firewall Threat Defense Base license must allow export-controlled functionality.

General prerequisite

Ensure that you have the Secure Firewall Posture package before you configure the dynamic access policy. You can add the Secure Firewall Posture file at **Objects** > **Object Management** > **VPN** > **AnyConnect File**.

Guidelines and limitations for dynamic access policies

Consider these guidelines and limitations when implementing Dynamic Access Policies:

- Matching of AAA attributes in a DAP will work only if a AAA server is configured to return the correct attributes when authenticating or authorizing a remote access VPN session.
- Minimum AnyConnect and Secure Firewall Posture package version supported for DAP is 4.6. But it is highly recommended to use the latest version of AnyConnect.
- DAP does not support clustering or multi-instance mode.
- DAP condition with an assigned IPv4 or IPv6 address does not work for local authentication.

Configure a Dynamic Access Policy (DAP)

Create a dynamic access policy

Create a dynamic access policy to enable conditional access control for VPN users based on their endpoint security posture and compliance status.

Dynamic access policies evaluate endpoint attributes and security posture to determine appropriate access permissions for VPN users. These policies work in conjunction with posture assessment packages to enforce security compliance.

Before you begin

Ensure that you have the Secure Firewall Posture package before you configure the dynamic access policy. You can add the Secure Firewall Posture file at **Objects** > **Object Management** > **VPN** > **AnyConnect File**.

Procedure

Step 1 Choose **Devices** > **VPN** > **Dynamic Access Policy**, and click **Create Dynamic Access Policy**.

Step 2 Specify the **Name** for the DAP policy and an optional **Description**.

Step 3 Choose the **HostScan Package** from the drop-down list.

Step 4 Click **Save**.

What to do next

To configure DAP record, see Create Dynamic Access Policy Record

Create a dynamic access policy record

A dynamic access policy (DAP) can contain multiple DAP records, where you configure user and endpoint attributes. You can prioritize the DAP records within a DAP so that the Firewall Threat Defense device can select and sequence the required criteria when a user attempts VPN connection.

Procedure

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

Step 2 Edit an existing dynamic access policy or click **Create Dynamic Access Policy** to create a new one and then edit the policy.

Step 3 Click **Create DAP Record**.

Step 4 Click the **General** tab.

Step 5 Specify the **Name** for the DAP record.

Step 6 Enter the **Priority** for the DAP record.

The lower the number, the higher the priority.

Step 7 Select one of these actions to take when a DAP record matches:

- **Continue**—Applies access policy attributes to the session. If any, the next DAP record (next policy line with less priority) is then evaluated.
- **Terminate**—Terminates the session.
- **Quarantine**—Quarantines the connection.

Step 8 Check the **Display User Message on Criterion Match** check-box and add the user message.

The Firewall Threat Defense displays this message to the user when the DAP record matches.

Step 9 Check the **Apply a Network ACL on Traffic** check box and select the access control list from the drop-down.

Step 10 Check the **Apply one or more AnyConnect Custom Attributes** check box and select the custom attributes object from the drop-down.

Step 11 Click **Save**.

Configure AAA criteria settings for a DAP record

Configure AAA criteria settings to specify the conditions under which DAP records are selected and applied to user sessions based on AAA authorization and posture assessment information.

DAP complements AAA services by providing a limited set of authorization attributes that can override the attributes that AAA provides. The Firewall Threat Defense device selects DAP records based on the AAA authorization information for the user and posture assessment information for the session. The Firewall Threat Defense device can choose multiple DAP records depending on this information, which it then aggregates to create DAP authorization attributes.

Procedure

Step 1 Choose **Devices** > **VPN** > **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 criteria.
- None—Matches none of the set criteria.

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

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

a) Select an attribute and specify the **Value**.
b) Click **Add another criteria** to add more criteria.
c) Click **Save**.

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

Step 8 Click **Save**.

Configure endpoint attribute selection criteria in DAP

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

Note When using remote Access VPN with DAP or Secure Firewall Posture (formerly HostScan) and change of authorization (CoA), endpoint attribute checks differ between initial authentication and CoA-triggered authorization.

Procedure

Step 1 Choose **Devices** > **VPN** > **Dynamic Access Policy**, and click **Create Dynamic Access Policy**.

Step 2 Create or edit a DAP record.

Step 3 Click **Endpoint Criteria** and configure attributes such as anti-malware, device, AnyConnect, NAC, application, personal firewall, operating system, process, registry, file, and certificate authentication.

Note
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.

Step 4 Click **Save**.

Add an anti-malware endpoint attribute to a DAP record

Add anti-malware endpoint attributes to a DAP to control access based on the presence and configuration of anti-malware software on client devices.

Anti-malware endpoint attributes allow you to create access policies that verify client devices have appropriate anti-malware protection before granting network access.

Before you begin

Follow these steps to add an anti-malware endpoint attribute to a DAP:

Procedure

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

Step 2 Create or edit a DAP policy and a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **Anti-Malware**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click + to add the anti-malware attributes.

In the **Anti-Malware** dialog box, configure these parameters:

a) Check the **Installed** check box to indicate whether the selected endpoint attribute and its accompanying qualifiers are installed or not installed.
b) In **Real Time Scanning**, choose **Enabled** or **Disabled** to activate or deactivate real-time malware scanning.
c) Choose the anti-malware vendor from the **Vendor** drop-down list.
d) Choose the anti-malware description from the **Product Description** drop-down list.
e) Choose the **Version** of the anti-malware product.
f) Specify the number of days since the **Last Update**.

You can indicate that an anti-malware update must occur in less than (<) or more than (>) the number of days you specify.

g) Click **Save**.

Add a device endpoint attribute to a DAP record

Add device endpoint attributes to a DAP to control access based on specific device characteristics such as hostname, MAC address, BIOS serial number, or port configuration.

Device endpoint attributes allow you to create policies that evaluate device-specific criteria to determine access permissions. These attributes help enforce security policies based on device identity and configuration.

Before you begin

Follow these steps to add a device endpoint attribute to a DAP:

Procedure

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

Step 2 Create or edit a DAP policy and a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **Device**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click + to add application attributes.

In the **Device** dialog box, configure these parameters:

Select the = or ≠ operator to check the attribute to be equal to or not equal to the value you enter for these attributes:

- **Host Name**—Hostname of the device. Use the computer's host name only, not the fully qualified domain name (FQDN).
- **MAC Address**—MAC address of the network interface card you are testing for. The address must be in the format xxxx.xxxx.xxxx where x is a hexadecimal character.
- **BIOS Serial Number**—BIOS serial number value of the device you are testing for. The number format is manufacturer-specific.
- **Port Number**—Listening port number of the device.
- **Secure Desktop Version**—Version of the Secure Firewall Posture image running on the endpoint.
- **OPSWAT Version**—The OPSWAT client version.
- **Privacy Protection**—None, Cache cleaner, Secure Desktop.
- **TCP/UDP Port Number**—TCP or UDP port in the listening state.

Step 6 Click **Save**.

Add AnyConnect endpoint attributes to a DAP record

Add specific endpoint attributes to a Dynamic Access Policy (DAP) record to control client access based on AnyConnect characteristics such as client version, platform, and device identifiers.

Procedure

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

Step 2 Create or edit a DAP policy and a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **AnyConnect**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click **+** to add the attributes.

In the **AnyConnect** dialog box, configure these parameters:

Select the **=** or **≠** operator to check the attribute to be equal to or not equal to the value you enter.

a) Specify the **Client Version**.
b) Choose the platform from the **Platform** drop-down list.
c) Choose the platform version from the **Platform Version** drop-down list.
d) Specify the **Device Type** and **Device Unique ID**.
e) Add the **MAC Addresses**.

Note
The MAC Address must be in the format XX-XX-XX-XX-XX-XX, where each X is a hexadecimal character. You can click **Add another MAC Address** to add more addresses.

f) Click **Save**.

Add NAC endpoint attributes to a DAP record

You can configure Network Access Control (NAC) endpoint attributes within a DAP (Dynamic Access Policy) record to evaluate endpoint posture status based on a defined criteria.

NAC endpoint attributes in DAP records help determine access permissions based on endpoint posture compliance. You can specify whether endpoints must match all criteria or any criteria, and define specific posture token strings for evaluation.

Procedure

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

Step 2 Create or edit a DAP policy and a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **NAC**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click + to add NAC attributes.

Step 6 In the **NAC** dialog box, set the operator to be equal to = or not equal to ≠ the posture status.

Step 7 Choose one of these options from the **Posture Status** drop-down list:

- Compliant
- Non-Compliant
- Unknown

Step 8 Click **Save**.

Add an application attribute to a DAP record

This task allows you to define application-specific criteria within a DAP record to control access based on the type of remote access client.

Application attributes in DAP records help determine access policies by evaluating the client application type used for remote connections. You can configure these attributes to match all or any specified criteria.

Procedure

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

Step 2 Create or edit a DAP policy and a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **Application**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click + to add application attributes.

Step 6 In the **Application** dialog box, choose equals (=) or does not equal (≠) and specify the **Client Type** to indicate the type of remote access connection. Choose from one of these options:

- Clientless

- Cut-Through-Proxy
- Secure Client
- IPsec
- L2TP
- IPsec-IKEv2-Generic-RA

Step 7 Click **Save**.

Add a personal firewall endpoint attribute to a DAP record

Adding personal firewall endpoint attributes to a DAP allows you to control network access based on whether client devices have specific firewall software installed, enabled, and meeting version requirements.

Personal firewall endpoint attributes help enforce security policies by ensuring that connecting devices meet firewall protection standards before granting network access.

Procedure

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

Step 2 Create or edit a DAP policy and a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **Personal Firewall**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click + to add personal firewall attributes.

In the **Personal Firewall** dialog box, configure these parameters:

a) Click **Installed** to indicate whether the personal firewall endpoint attribute and its accompanying qualifiers (fields below the Name/Operation/Value column) are installed or not installed.
b) Select **Enabled** or **Disabled** to activate or deactivate firewall protection.
c) Choose the name of the firewall vendor from the **Vendor** drop-down list.
d) Choose the firewall description from the **Product Description** drop-down list.
e) Select the equals (=) or does not equal (≠) operator and choose the **Version** of the personal firewall product.
f) Click **Save**.

Add an operating system endpoint attribute to a DAP record

Operating system endpoint attributes help create granular access policies by identifying and filtering client devices based on their operating system characteristics. This is useful for implementing different access levels or restrictions based on device types.

Procedure

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

Step 2 Create or edit a DAP policy and a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **Operating System**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click + to add endpoint attributes.

In the **Operating System** dialog box, configure these parameters:

a) Select the equals (=) or does not equal (≠) operator and then choose the operating system from the **Operating System** drop-down list.
b) Select the equals (=) or does not equal (≠) operator and then specify the operating system version in the **Version** field.
c) Click **Save**.

Add a process endpoint attribute to a DAP

Configure process endpoint attributes to define specific criteria for device access policy enforcement based on running processes.

Process endpoint attributes allow you to create device access policies based on specific processes running on endpoints. This helps ensure that only devices with approved processes can access network resources.

Procedure

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

Step 2 Create or edit a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **Process**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click + to add process attributes.

In the **Process** dialog box, configure these parameters:

a) Select **Exists** or **Does not exist**.
b) Specify the **Process Name**.
c) Click **Save**.

Add a registry endpoint attribute to a DAP record

Registry endpoint attributes allow you to define specific registry keys that the system scans during posture assessment to determine endpoint compliance status.

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 Secure Firewall Posture window for Cisco Secure Desktop.

Procedure

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

Step 2 Create or edit a DAP policy and a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **Registry**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click **+** to add registry attributes.

In the **Registry** dialog box, configure these parameters:

a) Select the **Entry Path** for the registry and specify the path.
b) Choose the existence of the registry, **Exists** or **Does not exist**.
c) Select the registry **Type** from the list.
d) Select the equals (=) or does not equal (≠) operator and enter the **Value** of the registry key.
e) Select **Case insensitive** to disregard the case of the registry entry while scanning.
f) Click **Save**.

Add a file endpoint attribute to a DAP record

You can configure file endpoint criteria within a DAP (Device Access Policy) record to specify file attributes used for posture assessment and device authorization.

Procedure

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

Step 2 Create or edit a DAP policy and a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **File**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click **+** to add file attributes.

In the **File** dialog box, configure these parameters:

a) Specify the **File Path**.
b) Select **Exists** or **Does not exist** to indicate the presence of the file.
c) Select less than (<) or greater than (>) and specify the **Last Modified** days for the file.
d) Select the equal to (=) or not equal to ≠ operator and enter the **Checksum**.
e) Click **Save**.

Add certificate authentication attributes to a DAP record

Adding certificate authentication attributes to a DAP allows you to control access based on specific certificate fields such as subject, issuer, and serial number.

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



Note This configuration is applicable only for certificates used with multiple certificate authentication. It does not apply for single client certificate authentication.

Procedure

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

Step 2 Create or edit a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **Multiple Certificate Authentication**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click **+** to add certification authentication criteria.

In the **Multiple Certificate Authentication Criteria** dialog box, configure these parameters:

a) Select **Cert1** or **Cert2** certificate.
b) Select the **Subject** and specify the subject value.
c) Select the **Issuer** and specify the issuer value.
d) Select the **Subject Alternate Name** and specify the subject value.
e) Specify the **Serial Number**.
f) Choose the **Certificate Store** as **None**, **Machine**, or **User**.

The VPN client sends the certificate store information.

g) Click **Save**.

Configure advanced settings for DAP

This task allows you to configure selection criteria for DAP records using Lua scripts when the standard AAA AND endpoint attribute areas are insufficient for your requirements.

You can use the **Advanced** tab for adding selection criteria other than what is possible in the AAA AND endpoint attribute areas. For example, while you can configure the Firewall Threat Defense to use AAA attributes that satisfy any, all, OR none of the specified criteria, the endpoint attributes are cumulative, AND must satisfy all. To let the security appliance employ one endpoint attribute OR another, you must create appropriate logical expressions in Lua AND enter them here.

Procedure

Step 1 Choose **Devices** > **VPN** > **Dynamic Access Policy**.
Step 2 Create or edit a DAP record.
Step 3 Click the **Advanced** tab.
Step 4 Select **AND** OR **OR** as the match criteria to use in the DAP configuration.
Step 5 Add the Lua script in the **Lua script for advanced attribute matching** field.
Step 6 Click **Save**.

Associate dynamic access policy with remote access VPN

You can associate Dynamic Access Policy (DAP) with remote access VPN policy for the dynamic access policy attributes to match during VPN session authentication and authorization. You can then deploy the remote access VPN on the Firewall Threat Defense.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.
Step 2 Click **Edit** next to the remote access VPN policy to which you want to associate dynamic access policy.
Step 3 Click the link in remote access VPN to select the dynamic access policy.
Step 4 Select the policy from the **Dynamic Access Policy** drop-down or click **Create a new Dynamic Access Policy** to configure a new dynamic access policy.
Step 5 Click **OK**.
Step 6 Click **Save** to save the remote access VPN policy.

When the remote access VPN user tries to connect, the VPN checks the configured dynamic access policy records and attributes. VPN creates a dynamic access policy based on the matching dynamic access policy records and takes appropriate action on the VPN session.

History for dynamic access policy

This reference provides the version history for dynamic access policy features, including when they were introduced and what changes were made in each release.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Dynamic Access Policy	7.0	Any	The feature was introduced.