



# ダイナミック アクセス ポリシー

ダイナミック アクセス ポリシー (DAP) を使用すると、VPN 環境のダイナミクスに対応する許可を設定できます。ダイナミック アクセス ポリシーは、特定のユーザー トンネルまたはユーザー セッションに関連付ける一連のアクセス コントロール属性を設定して作成します。これらの属性により、複数のグループ メンバーシップやエンドポイント セキュリティの問題に対処します。

- [Secure Firewall Threat Defense ダイナミック アクセス ポリシーについて \(1 ページ\)](#)
- [ダイナミック アクセス ポリシーの前提条件 \(3 ページ\)](#)
- [ダイナミック アクセス ポリシーに関する注意事項と制限事項 \(3 ページ\)](#)
- [ダイナミック アクセス ポリシー \(DAP\) の設定 \(4 ページ\)](#)
- [ダイナミック アクセス ポリシーとリモートアクセス VPN の関連付け \(15 ページ\)](#)
- [ダイナミック アクセス ポリシーの履歴 \(16 ページ\)](#)

## Secure Firewall Threat Defense ダイナミック アクセス ポリシーについて

VPN ゲートウェイは動的な環境で動作します。個々の VPN 接続には、複数の変数が影響を与える可能性があります。たとえば、頻繁に変更されるイントラネット設定、組織内の各ユーザーが持つさまざまなロール、および設定とセキュリティレベルが異なるリモートアクセスサイトからのログイン試行などです。VPN 環境でのユーザー認可のタスクは、スタティックな設定のネットワークでの認可タスクよりもかなり複雑です。

ダイナミック アクセス ポリシーは、特定のユーザー トンネルまたはユーザー セッションに関連付ける一連のアクセス コントロール属性を設定して作成できます。これらの属性により、複数のグループ メンバーシップやエンドポイント セキュリティの問題に対処します。Firewall Threat Defense では、定義したポリシーに基づき、特定のセッションへのアクセス権が特定のユーザーに付与されます。Firewall Threat Defense デバイスは、ユーザーの認証中に、DAP レコードからの属性を選択または集約することによって DAP を生成します。次に、リモートデバイスのエンドポイントセキュリティ情報および認証されたユーザーの AAA 認可情報に基づいて DAP レコードを選択します。その後、デバイスは選択した DAP レコードをユーザー トンネルまたはセッションに適用します。

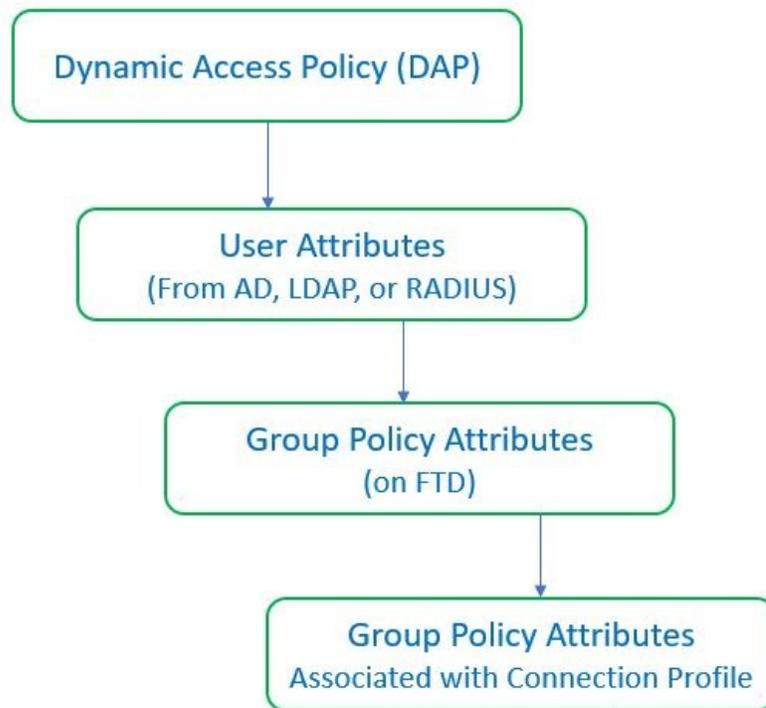
## Firewall Threat Defense での権限および属性のポリシー適用階層

Firewall Threat Defense デバイスは、ユーザー認可属性（ユーザー権利またはユーザー権限とも呼ばれる）の VPN 接続への適用をサポートしています。属性は、Firewall Threat Defense の DAP、外部認証サーバー、または認可 AAA サーバー（RADIUS）（あるいはこれらのすべて）、または Firewall Threat Defense デバイスのグループポリシーから適用されます。

Firewall Threat Defense デバイスは、すべてのソースから属性を受信すると、その属性を評価し、集約してユーザーポリシーに適用します。DAP、AAA サーバー、またはグループポリシーから取得した属性の間で衝突がある場合、DAP から取得した属性が常に優先されます。

Firewall Threat Defense デバイスは次の順序で属性を適用します。

図 1: ポリシー実施フロー



1. **FTD 上の DAP 属性** : DAP 属性は、他のすべての属性よりも優先されます。
2. **外部 AAA サーバー上のユーザー属性** : ユーザー認証や認可が成功すると、サーバーからこの属性が返されます。
3. **FTD で設定されているグループポリシー** : RADIUS サーバーからユーザーの RADIUS Class 属性 IETF-Class-25 (OU=group-policy) の値が返された場合、Firewall Threat Defense デバイスはそのユーザーを同じ名前前のグループポリシーに入れて、そのグループポリシーの属性のうち、サーバーから返されないものを適用します。

4. 接続プロファイル（トンネルグループと呼ばれる）で割り当てられたグループポリシー：接続プロファイルには、接続の事前設定と、認証前にユーザーに適用されるデフォルトのグループポリシーが含まれています。



(注) Firewall Threat Defense デバイスは、デフォルトのグループポリシー *DfltGrpPolicy* から継承したシステム デフォルト属性をサポートしていません。ユーザー属性または AAA サーバーのグループポリシーによって上書きされない場合、デバイスは、接続プロファイルに割り当てられたグループポリシーの属性をユーザーセッションに使用します。

## ダイナミック アクセス ポリシーの前提条件

ライセンス：

- Firewall Threat Defense には次の Secure Client ライセンスの少なくとも 1 つが必要です。
  - Secure Client Premier
  - Secure Client Advantage
  - Secure Client VPN Only
- Firewall Threat Defense Essentials ライセンスにより輸出規制機能が許可される必要があります。

## ダイナミック アクセス ポリシーに関する注意事項と制限事項

- DAP での AAA 属性の照合は、リモートアクセス VPN セッションを認証または認可するときに正しい属性を返すように AAA サーバーが設定されている場合にのみ機能します。
- DAP でサポートされる Secure Client および Secure Firewall Posture パッケージの最小バージョンは 4.6 です。ただし、最新バージョンの Secure Client を使用することを強くお勧めします。
- DAP はクラスタリングまたはマルチインスタンスモードをサポートしていません。
- IPv4 または IPv6 アドレスが割り当てられた DAP 条件は、ローカル認証では機能しません。

# ダイナミック アクセス ポリシー (DAP) の設定

## ダイナミック アクセス ポリシーの作成

### 始める前に

ダイナミック アクセス ポリシーを設定する前に、Secure Firewall Posture パッケージがあることを確認してください。Secure Firewall Posture ファイルは、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] > [VPN] > [Secure Client ファイル (Secure Client File)] で追加できます。

### 手順

- ステップ 1 [デバイス (Devices)] > [ダイナミックアクセスポリシー (Dynamic Access Policy)] > [ダイナミックアクセスポリシーの作成 (Create Dynamic Access Policy)] を選択します。
- ステップ 2 DAP ポリシーの[名前 (Name)] を指定し、必要に応じて[説明 (Description)] を指定します。
- ステップ 3 ドロップダウンリストから [Secure Firewall ポスチャ パッケージ (Secure Firewall Posture Package)] を選択します。
- ステップ 4 [保存 (Save)] をクリックします。

### 次のタスク

DAP レコードを設定するには、「[ダイナミック アクセス ポリシー レコードの作成](#)」を参照してください。

## ダイナミック アクセス ポリシー レコードの作成

ダイナミック アクセス ポリシー (DAP) には、ユーザーとエンドポイントの属性を構成する複数の DAP レコードを含めることができます。ユーザーが VPN 接続を試みるときに必要な基準を Firewall Threat Defense が選択および順序付けできるように、DAP 内の DAP レコードに優先順位を付けることができます。

### 手順

- ステップ 1 [デバイス (Devices)] > [ダイナミック アクセス ポリシー (Dynamic Access Policy)] を選択します。 >

- ステップ 2** 既存のダイナミック アクセス ポリシーを編集するか、[ダイナミック アクセス ポリシーの作成 (Create Dynamic Access Policy)] をクリックして新しいポリシーを作成してからポリシーを編集します。
- ステップ 3** [DAPレコードの作成 (Create DAP Record)] をクリックします。
- ステップ 4** [全般 (General)] タブをクリックします。
- ステップ 5** DAP レコードの [名前 (Name)] を指定します。
- ステップ 6** DAP レコードの [優先順位 (Priority)] を入力します。  
値が小さいほど、プライオリティが高くなります。
- ステップ 7** DAP レコードが一致した場合に実行するアクションを次から 1 つ選択します。
- [続行 (Continue)] : セッションにアクセス ポリシー属性を適用します。存在する場合は、次の DAP レコード (優先順位の低い、次のポリシー行) が評価されます。
  - [強制終了 (Terminate)] : エンドユーザーセッションを強制終了します。
  - [検疫 (Quarantine)] : 接続を隔離します。
- ステップ 8** [基準に一致したときユーザーメッセージを表示 (Display User Message on Criterion Match)] チェックボックスをオンにして、ユーザーメッセージを追加します。  
Firewall Threat Defense で、DAP レコードが一致する場合に、このメッセージがユーザーに表示されます。
- ステップ 9** [トラフィックにネットワーク ACL を適用する (Apply a Network ACL on Traffic)] チェックボックスをオンにして、ドロップダウンからアクセス制御リストを選択します。
- ステップ 10** [1つまたは複数のセキュア クライアント カスタム属性を適用する (Apply one or more Secure Client Custom Attributes)] チェックボックスをオンにして、ドロップダウンからカスタム属性オブジェクトを選択します。
- ステップ 11** [保存 (Save)] をクリックします。

## ポスチャアセスメント基準の設定

DAP ポリシーの場合、一意のエンドポイント ID を使用してファイル、プロセス、またはレジストリのエンドポイント属性を設定できます。これらの ID は、DAP レコードを設定するための Lua スクリプトでエンドポイント基準として使用できます。

### 手順

- ステップ 1** [デバイス (Devices)] > [ダイナミック アクセス ポリシー (Dynamic Access Policy)] を選択します。 >
- ステップ 2** [ダイナミック アクセス ポリシーの作成 (Create Dynamic Access Policy)] をクリックして、新しい DAP ポリシーを作成してからポリシーを編集します。

**ステップ3** DAP ポリシーの横にある編集アイコンをクリックします。

**ステップ4** [ポスチャアセスメント基準の追加 (Add Posture Assessment Criteria) ] をクリックします。

**ステップ5** 次のいずれかを実行します。

- ファイルエンドポイント属性を設定します。
  1. [ファイル (File) ] オプションボタンをクリックします。
  2. [エンドポイント識別子 (EndpointID) ] フィールドに、ファイルの一意の識別子を入力します。文字列または数値を指定できます。
  3. [ファイルパス (File Path) ] フィールドに、ファイルパスを指定します。
- レジストリのエンドポイント属性を設定します。
  1. [レジストリ (Registry) ] オプションボタンをクリックします。
  2. [エンドポイント識別子 (EndpointID) ] フィールドに、レジストリの一意の識別子を入力します。文字列または数値を指定できます。
  3. [エントリパス (Entry Path) ] フィールドに、ファイルパスを指定します。
- プロセスのエンドポイント属性を設定します。
  1. [プロセス (Process) ] オプションボタンをクリックします。
  2. [エンドポイント識別子 (EndpointID) ] フィールドに、プロセスの一意の識別子を入力します。文字列または数値を指定できます。
  3. [プロセス名 (Process Name) ] フィールドに、プロセス名を指定します。

(注)  
保存後は、エンドポイント識別子を編集できません。

**ステップ6** [保存 (Save) ] をクリックします。

---

#### 次のタスク

エンドポイント識別子を使用して、Lua スクリプトを使用した高度なポスチャアセスメント基準を設定できます。詳細については、「[DAP の詳細設定の設定 \(14 ページ\)](#)」を参照してください。

## DAP の AAA 基準設定を構成する

DAP は AAA サービスを補完します。用意されている認可属性のセットは限られていますが、それらの属性によって AAA で提供される認可属性を無効にできます。Firewall Threat Defense は、ユーザーの AAA 認可情報とセッションのポスチャ評価情報に基づいて DAP レコードを選

択します。Firewall Threat Defense は、この情報に基づいて複数の DAP レコードを選択でき、それらのレコードを集約して DAP 認可属性を作成します。

## 手順

**ステップ 1** **Devices > VPN > Dynamic Access Policy** を選択します。

**ステップ 2** 既存の DAP ポリシーを編集するか、新しい DAP ポリシーを作成してからポリシーを編集します。

**ステップ 3** DAP レコードを選択するか新しいレコードを作成して、DAP レコードを編集します。

**ステップ 4** [AAA 基準 (AAA Criteria) ] をクリックします。

**ステップ 5** 次の [セクション間の一致基準 (Match criteria between sections) ] のいずれかを選択します。

- [任意 (Any) ] : いずれかの基準に一致する。
- [すべて (All) ] : すべての基準に一致する。
- [なし (None) ] : 設定された基準のいずれにも一致しない。

**ステップ 6** [追加 (Add) ] をクリックして、必要な **Cisco VPN 基準** を追加します。

Cisco VPN 基準には、グループポリシー、割り当てられた IPv4 アドレス、割り当てられた IPv6 アドレス、接続プロファイル、ユーザー名、ユーザー名 2、必要な SCEP の属性が含まれます。

- a) 属性を選択し、**値** を指定します。
- b) [別の条件を追加 (Add another criteria) ] をクリックして、さらに条件を追加します。
- c) [保存 (Save) ] をクリックします。

必要な SCEP

**ステップ 7** [LDAP 基準 (LDAP Criteria) ]、[RADIUS 基準 (RADIUS Criteria) ]、[SAML 基準 (SAML Criteria) ] を選択し、[属性 ID (Attribute ID) ] と [値 (Value) ] を指定します。

**ステップ 8** [保存 (Save) ] をクリックします。

## DAP のエンドポイント属性選択基準の設定

エンドポイント属性には、エンドポイントシステム環境、ポストチャ評価結果、およびアプリケーションに関する情報が含まれています。Firewall Threat Defense は、エンドポイント属性の集合をセッション確立時に動的に生成し、セッションに関連付けられたデータベースにその属性を保存します。各 DAP レコードには、Firewall Threat Defense がセッションの DAP レコードを選択するために満たす必要があるエンドポイント選択属性が指定されます。Firewall Threat Defense は、設定されたすべての条件を満たす DAP レコードだけを選択します。

## 手順

---

**ステップ 1** [デバイス (Devices) ]>[ダイナミックアクセスポリシー (Dynamic Access Policy) ]>[ダイナミックアクセスポリシーの作成 (Create Dynamic Access Policy) ]を選択します。

**ステップ 2** DAP ポリシーを編集してから、DAP レコードを編集します。

(注)

DAP ポリシーと DAP レコードをまだ作成していない場合は作成します。

**ステップ 3** [エンドポイント基準 (Endpoint Criteria) ]をクリックし、次のエンドポイント基準属性を設定します。

(注)

各タイプのエンドポイント属性のインスタンスを複数作成できます。各 DAP レコードに設定可能なエンドポイント属性の数に制限はありません。

- [DAP へのマルウェア対策エンドポイント属性の追加](#)
- [DAP へのデバイス エンドポイント属性の追加](#)
- [DAP への Secure Client エンドポイント属性の追加 \(10 ページ\)](#)
- [DAP への NAC エンドポイント属性の追加](#)
- [DAP へのアプリケーション属性の追加](#)
- [DAP へのパーソナルファイアウォール エンドポイント属性の追加](#)
- [DAP へのオペレーティング システム エンドポイント属性の追加](#)
- [DAP へのプロセス エンドポイント属性の追加](#)
- [DAP へのレジストリ エンドポイント属性の追加](#)
- [DAP へのファイル エンドポイント属性の追加](#)
- [DAP への複数証明書認証属性の追加](#)

**ステップ 4** [保存 (Save) ]をクリックします。

---

## DAP へのマルウェア対策エンドポイント属性の追加

## 手順

---

**ステップ 1** DAP レコードを編集し、[エンドポイント基準 (Endpoint Criteria) ]>[マルウェア対策 (Anti-Malware) ]を選択します。

- ステップ 2** 一致基準 [すべて (All) ] または [任意 (Any) ] を選択します。
- ステップ 3** [追加 (Add) ] をクリックして、属性を追加します。
- ステップ 4** [インストール済み (Installed) ] をクリックして、選択したエンドポイント属性と付随する修飾子をインストールするか、インストールしないかを指定します。
- ステップ 5** [有効 (Enabled) ] または [無効 (Disabled) ] を選択して、リアルタイムのマルウェアスキャンをアクティブまたは非アクティブにします。
- ステップ 6** [ベンダー (Vendor) ] のリストからマルウェア対策ベンダーの名前を選択します。
- ステップ 7** マルウェア対策製品の [製品の説明 (Product Description) ] を選択します。
- ステップ 8** マルウェア対策製品の [バージョン (Version) ] を選択します。
- ステップ 9** [最終更新 (Last Update) ] からの日数を指定します。  
マルウェア対策製品の更新を、指定した日数よりも早く ([<]) 実行するか、遅く ([>]) 実行するかを指定できます。
- ステップ 10** [保存 (Save) ] をクリックします。

## DAP へのデバイス エンドポイント属性の追加

### 手順

- ステップ 1** DAP レコードを編集し、[エンドポイント基準 (Endpoint Criteria) ] > [デバイス (Device) ] を選択します。
- ステップ 2** 一致基準 [すべて (All) ] または [任意 (Any) ] を選択します。
- ステップ 3** [追加 (Add) ] をクリックし、[=] または [≠] 演算子を選択して、次の属性に入力した値と属性が等しいか等しくないかを確認します。
- [ホスト名 (Host Name) ] : テスト対象のデバイスのホスト名。完全修飾ドメイン名 (FQDN) ではなく、コンピュータのホスト名のみを使用します。
  - [MAC アドレス (MAC Address) ] : テスト対象のネットワークインターフェイスカードの MAC アドレス。アドレスのフォーマットは xxxx.xxxx.xxxx であることが必要です。x は 16 進数文字です。
  - [BIOS シリアル番号 (BIOS Serial Number) ] : テスト対象のデバイスの BIOS シリアル番号の値。数値フォーマットは、製造業者固有です。
  - [ポート番号 (Port Number) ] : デバイスのリスンポート番号。
  - [Secure Desktop バージョン (Secure Desktop Version) ] : エンドポイントで実行されているホストスキャンイメージのバージョン。
  - [OPSWAT バージョン (OPSWAT Version) ] : OPSWAT クライアントのバージョン。
  - [プライバシー保護 (Privacy Protection) ] : なし、Cache Cleaner、Secure Desktop。

- [TCP/UDPポート番号 (TCP/UDP Port Number) ] : テスト対象のリスニング状態の TCP または UDP ポート。

ステップ4 [保存 (Save) ] をクリックします。

---

## DAP への Secure Client エンドポイント属性の追加

### 手順

---

- ステップ1 DAP レコードを編集し、[エンドポイントの基準 (Endpoint Criteria) ] > [Secure Client] を選択します。
- ステップ2 一致基準 [すべて (All) ] または [任意 (Any) ] を選択します。
- ステップ3 [追加 (Add) ] をクリックし、[=] または [≠] 演算子を選択して、入力した値と属性が等しいか等しくないかを確認します。
- ステップ4 [クライアントバージョン (Client Version) ] と [プラットフォーム (Platform) ] を選択します。
- ステップ5 [プラットフォームバージョン (Platform Version) ] を選択し、[デバイスタイプ (Device Type) ] と [デバイスの固有ID (Device Unique ID) ] を指定します。
- ステップ6 [MACアドレス (MAC Addresses) ] を MAC アドレスプールに追加します。

(注)

MACアドレスは XX-XX-XX-XX-XX-XX 形式である必要があります。各 X は 16 進数文字です。[別のMACアドレスを追加 (Add another MAC Address) ] をクリックして、さらにアドレスを追加できます。

ステップ7 [保存 (Save) ] をクリックします。

---

## DAP への NAC エンドポイント属性の追加

### 手順

---

- ステップ1 DAP レコードを編集し、[エンドポイント基準 (Endpoint Criteria) ] > [NAC] を選択します。
- ステップ2 一致基準 [すべて (All) ] または [任意 (Any) ] を選択します。
- ステップ3 [追加 (Add) ] をクリックして、NAC 属性を追加します。
- ステップ4 演算子を、ポスチャトークン文字列に等しい (=) または等しくない (≠) に設定します。ポスチャトークン文字列を [ポスチャステータス (Posture Status) ] ボックスに入力します。
- ステップ5 [保存 (Save) ] をクリックします。
-

## DAP へのアプリケーション属性の追加

### 手順

- 
- ステップ 1** DAP レコードを編集し、[エンドポイント基準 (Endpoint Criteria)] > [アプリケーション (Application)] を選択します。
  - ステップ 2** 一致基準 [すべて (All)] または [任意 (Any)] を選択します。
  - ステップ 3** [追加 (Add)] をクリックして、アプリケーション属性を追加します。
  - ステップ 4** 等しい ([=]) または等しくない ([≠]) を選択し、[クライアントタイプ (Client Type)] を指定して、リモートアクセス接続のタイプを示します。
  - ステップ 5** [保存 (Save)] をクリックします。
- 

## DAP へのパーソナル ファイアウォール エンドポイント属性の追加

### 手順

- 
- ステップ 1** DAP レコードを編集し、[エンドポイント基準 (Endpoint Criteria)] > [パーソナルファイアウォール (Personal Firewall)] を選択します。
  - ステップ 2** 一致基準 [すべて (All)] または [任意 (Any)] を選択します。
  - ステップ 3** [追加 (Add)] をクリックして、パーソナルファイアウォール属性を追加します。
  - ステップ 4** [インストール済み (Installed)] をクリックして、パーソナルファイアウォールのエンドポイント属性と付随する修飾子 ([名前 (Name)]/[操作 (Operation)]/[値 (Value)] 列の下のフィールド) をインストールするか、インストールしないかを指定します。
  - ステップ 5** [有効 (Enabled)] または [無効 (Disabled)] を選択して、ファイアウォール保護をアクティブまたは非アクティブにします。
  - ステップ 6** リストからファイアウォール [ベンダー (Vendor)] の名前を選択します。
  - ステップ 7** ファイアウォールの [製品説明 (Product Description)] を選択します。
  - ステップ 8** 等しい ([=]) または等しくない ([≠]) 演算子を選択し、パーソナルファイアウォール製品の [バージョン (Version)] を選択します。
  - ステップ 9** [保存 (Save)] をクリックします。
-

## DAP へのオペレーティング システム エンドポイント属性の追加

### 手順

- 
- ステップ 1 DAP レコードを編集し、[エンドポイント基準 (Endpoint Criteria)] > [オペレーティング システム (Operating System)] を選択します。
  - ステップ 2 一致基準 [すべて (All)] または [任意 (Any)] を選択します。
  - ステップ 3 [追加 (Add)] をクリックして、エンドポイント属性を追加します。
  - ステップ 4 等しい (=) または等しくない (≠) 演算子を選択し、[オペレーティング システム (Operating System)] を選択します。
  - ステップ 5 等しい (=) または等しくない (≠) 演算子を選択し、オペレーティング システムの [バージョン (Version)] を指定します。
  - ステップ 6 [保存 (Save)] をクリックします。
- 

## DAP へのプロセス エンドポイント属性の追加

### 手順

- 
- ステップ 1 DAP レコードを編集します。
  - ステップ 2 [エンドポイント基準 (Endpoint Criteria)] タブをクリックします。
  - ステップ 3 [プロセス (Process)] をクリックします。
  - ステップ 4 [一致基準 (Match Criteria)] に [すべて (All)] または [任意 (Any)] を選択します。
  - ステップ 5 [+] をクリックして、プロセス属性を追加します。
  - ステップ 6 [存在する (Exists)] または [存在しない (Does not exist)] を選択します。
  - ステップ 7 [プロセス名 (Process Name)] を指定します。
  - ステップ 8 [エンドポイント識別子 (Endpoint ID)] ドロップダウンリストから、プロセスの識別子を選択するか、[+] をクリックしてプロセスのポストチャアセスメント基準を設定します。詳細については、「[ポストチャアセスメント基準の設定 \(5 ページ\)](#)」を参照してください。
  - ステップ 9 [存在する (Exists)] または [存在しない (Does not exist)] をクリックします。
  - ステップ 10 [保存 (Save)] をクリックします。
- 

## DAP へのレジストリ エンドポイント属性の追加

レジストリ エンドポイント属性のスキャンは Windows オペレーティング システムにのみ適用されます。

### 始める前に

レジストリ エンドポイント属性を設定する前に、どのレジストリ キーをスキャンするかを Cisco Secure Desktop の [Host Scan] ウィンドウで定義します。

#### 手順

- 
- ステップ 1 DAP レコードを編集します。
  - ステップ 2 [エンドポイント基準 (Endpoint Criteria)] タブをクリックします。
  - ステップ 3 [レジストリ (Registry)] をクリックします。
  - ステップ 4 [一致基準 (Match Criteria)] に [すべて (All)] または [任意 (Any)] を選択します。
  - ステップ 5 [+] をクリックして、レジストリ属性を追加します。
  - ステップ 6 レジストリの [エントリパス (Entry Path)] を選択し、パスを指定します。
  - ステップ 7 [エンドポイント識別子 (Endpoint ID)] ドロップダウンリストから、レジストリの識別子を選択するか、[+] をクリックしてレジストリのポスチャアセスメント基準を設定します。詳細については、「[ポスチャアセスメント基準の設定 \(5 ページ\)](#)」を参照してください。
  - ステップ 8 レジストリの有無 ([存在する (Exists)] または [存在しない (Does not Exist)]) を選択します。
  - ステップ 9 リストからレジストリの [種類 (Type)] を選択します。
  - ステップ 10 等しい (=) または等しくない (≠) 演算子を選択し、レジストリキーの [値 (Value)] を入力します。
  - ステップ 11 スキャン中にレジストリエントリの大文字と小文字を無視するには、[大文字と小文字を区別しない (Case insensitive)] を選択します。
  - ステップ 12 [保存 (Save)] をクリックします。
- 

## DAP へのファイル エンドポイント属性の追加

#### 手順

- 
- ステップ 1 DAP レコードを編集します。
  - ステップ 2 [エンドポイント基準 (Endpoint Criteria)] タブをクリックします。
  - ステップ 3 **File** をクリックします。
  - ステップ 4 一致基準 [すべて (All)] または [任意 (Any)] を選択します。
  - ステップ 5 [+] をクリックして、ファイル属性を追加します。
  - ステップ 6 [ファイルパス (File Path)] を指定します。
  - ステップ 7 [エンドポイント識別子 (Endpoint ID)] ドロップダウンリストから、ファイルの識別子を選択するか、[+] をクリックしてファイルのポスチャアセスメント基準を設定します。詳細については、「[ポスチャアセスメント基準の設定 \(5 ページ\)](#)」を参照してください。

- ステップ 8 [存在する (Exists) ]または[存在しない (Does not exist) ]を選択して、ファイルの存在を示します。
- ステップ 9 より小さい ([<]) またはより大きい ([>]) を選択し、ファイルの[最終更新 (Last Modified) ]日を指定します。
- ステップ 10 等しい ([=]) または等しくない ([≠]) 演算子を選択し、[チェックサム (Checksum) ]を入力します。
- ステップ 11 [保存 (Save) ]をクリックします。

## DAP への証明書認証属性の追加

受信した証明書のいずれかを設定されたルールで参照できるように各証明書をインデックス化できます。これらの証明書フィールドに基づいて、接続試行を許可または拒否する DAP ルールを設定できます。

### 手順

- ステップ 1 DAP レコードを編集し、[エンドポイント基準 (Endpoint Criteria) ]>[証明書 (Certificate) ]を選択します。
- ステップ 2 一致基準[すべて (All) ]または[任意 (Any) ]を選択します。
- ステップ 3 [追加 (Add) ]をクリックして、証明書属性を追加します。
- ステップ 4 証明書、[Cert1]または[Cert2]を選択します。
- ステップ 5 [サブジェクト (Subject) ]を選択し、サブジェクト値を指定します。
- ステップ 6 [発行者 (Issuer) ]を選択し、発行者名を指定します。
- ステップ 7 [サブジェクト代替名 (Subject Alternate Name) ]を選択し、サブジェクト値を指定します。
- ステップ 8 [シリアル番号 (Serial Number) ]を指定します。
- ステップ 9 [証明書ストア (Certificate Store) ]を選択します ([なし (None) ]、[マシン (Machine) ]、または[ユーザー (User) ])。  
VPN クライアントが証明書ストア情報を送信します。
- ステップ 10 [保存 (Save) ]をクリックします。

## DAP の詳細設定の設定

[詳細設定 (Advanced) ]タブを使用して、AAA およびエンドポイントの属性領域で指定可能な基準以外の選択基準を追加できます。たとえば、指定された条件のいずれかを満たす、すべてを満たす、またはいずれも満たさない AAA 属性を使用するように Firewall Threat Defense を設定できます。エンドポイント属性は累積されるため、すべてを満たす必要があります。セキュリティアプライアンスが任意のエンドポイント属性を使用できるようにするには、Lua で適切な論理式を作成し、この手順でその式を入力する必要があります。

## 手順

**ステップ 1** [デバイス (Devices) ]>[ダイナミック アクセス ポリシー (Dynamic Access Policy) ] を選択します。 >

**ステップ 2** DAP ポリシーを編集してから、DAP レコードを編集します。

(注)

DAP ポリシーと DAP レコードをまだ作成していない場合は作成します。

**ステップ 3** [Advanced] タブをクリックします。

**ステップ 4** DAP 設定で使用する一致基準として [AND] または [OR] を選択します。

**ステップ 5** [高度な属性照合用の Lua スクリプト (Lua script for advanced attribute matching) ] フィールドに Lua スクリプトを追加します。

**ステップ 6** Lua スクリプトでエンドポイント基準識別子を使用するには、次の手順を実行します。

1. エンドポイント基準識別子を挿入する場所にカーソルを置きます。
2. [エンドポイント基準 (Endpoint Criteria) ] ドロップダウンリストから、基準 a を選択します
3. 横にあるドロップダウンリストから対応する ID を選択します。

例 :

次の例では、DAPTESTFILE、LIBAGENT、vpnagent、および DUOAGENT が Lua スクリプトに挿入されています。

```
EVAL(endpoint.file["DAPTESTFILE"].exists,"EQ","true") or  
EVAL(endpoint.file["LIBAGENT"].exists,"EQ","true") and  
EVAL(endpoint.process["vpnagent"].exists,"EQ","true") and  
EVAL(endpoint.registry["DUOAGENT"].exists,"EQ","true")
```

**ステップ 7** [保存 (Save) ] をクリックします。

## ダイナミック アクセス ポリシーとリモートアクセス VPN の関連付け

VPN セッションの認証または認可中にダイナミック アクセス ポリシー (DAP) 属性が照合されるように、DAP をリモートアクセス VPN ポリシーに関連付ける必要があります。その後、リモートアクセス VPN を Firewall Threat Defense に展開できます。

## 手順

- ステップ 1** [デバイス (Devices)] > [リモートアクセス (Remote Access)] を選択します。
- ステップ 2** ダイナミック アクセス ポリシーを関連付けるリモートアクセス VPN ポリシーの横にある [編集 (Edit)] をクリックします。
- ステップ 3** リモートアクセス VPN のリンクをクリックして、ダイナミック アクセス ポリシーを選択します。
- ステップ 4** [ダイナミック アクセス ポリシー (Dynamic Access Policy)] ドロップダウンからポリシーを選択するか、[新しいダイナミック アクセス ポリシーの作成 (Create a new Dynamic Access Policy)] をクリックして新しいダイナミック アクセス ポリシーを設定します。
- ステップ 5** [OK] をクリックします。
- ステップ 6** [保存 (Save)] をクリックして、リモートアクセス VPN ポリシーを保存します。

リモートアクセス VPN ユーザーが接続を試みると、VPN は、設定されたダイナミック アクセス ポリシーのレコードおよび属性をチェックします。VPN は、一致するダイナミック アクセス ポリシーレコードに基づいてダイナミック アクセス ポリシーを作成し、VPN セッションで適切なアクションを実行します。

## ダイナミック アクセス ポリシーの履歴

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
ダイナミック アクセス ポリシーのポスチャ評価基準の簡単な構成。	7.7	任意	<p>DAP ポリシーの場合、一意のエンドポイント ID を使用してファイル、プロセス、またはレジストリのエンドポイント属性を設定できます。これらの ID は、DAP レコードを設定するための Lua スクリプトでエンドポイント基準として使用できます。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> <li>• [デバイス (Devices)] &gt; [ダイナミック アクセス ポリシー (Dynamic Access Policy)] &gt; [ポリシーの追加/編集 (Add/Edit Policy)] &gt; [ポスチャ評価基準 (Posture Assessment Criteria)]</li> <li>• [デバイス (Devices)] &gt; [ダイナミック アクセス ポリシー (Dynamic Access Policy)] &gt; [ポリシーの追加/編集 (Add/Edit Policy)] &gt; [DAP レコードの追加/編集 (Add/Edit DAP Record)] &gt; [詳細設定 (Advanced)] &gt; [エンドポイント基準 (Endpoint Criteria)]</li> </ul>
ダイナミック アクセス ポリシー	7.0	任意 (Any)	この機能が導入されました。

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。