Dynamic Access Policy

DAP(Dynamic Access Policy)를 사용하면 VPN 환경의 역동성을 해결하는 권한 부여를 구성할 수 있습니다. 특정 사용자 터널 또는 세션과 연계되는 액세스 제어 특성 모음을 설정하여 Dynamic Access Policy를 만들 수 있습니다. 이러한 특성은 여러 그룹 멤버십 및 엔드포인트 보안 문제를 처리합니다.

Secure Firewall Threat Defense Dynamic Access Policy 정보

VPN 게이트웨이는 동적 환경에서 작동합니다. 여러 변수가 각 VPN 연결에 영향을 줄 수 있습니다. 예를 들어, 자주 변경되는 인트라넷 구성, 각 사용자가 조직 내에서 담당할 수 있는 여러 역할, 구성 및 보안 수준의 원격 액세스 사이트에서 로그인 시도 등이 있습니다. VPN 환경은 정적 구성의 네트워크보다 사용자 인증 작업이 훨씬 복잡합니다.

특정 사용자 터널 또는 세션과 연계되는 액세스 제어 특성 모음을 설정하여 Dynamic Access Policy를 만들 수 있습니다. 이러한 속성은 여러 그룹 멤버십 및 엔드포인트 보안 문제를 처리합니다. threat defense에서는 정의한 정책에 따라 특정 사용자에게 특정 세션에 대한 액세스 권한을 부여합니다. threat defense 디바이스는 사용자 인증 중에 하나 이상의 DAP 레코드에서 속성을 선택하거나 집계하여 DAP를 생성합니다. 또한 디바이스는 원격 디바이스의 엔드포인트 보안 정보 및 인증된 사용자에 대한 AAA 권한 부여 정보를 기반으로 이러한 DAP 레코드를 선택합니다. 그런 다음 DAP 레코드를 사용자 터널 또는 세션에 적용합니다.

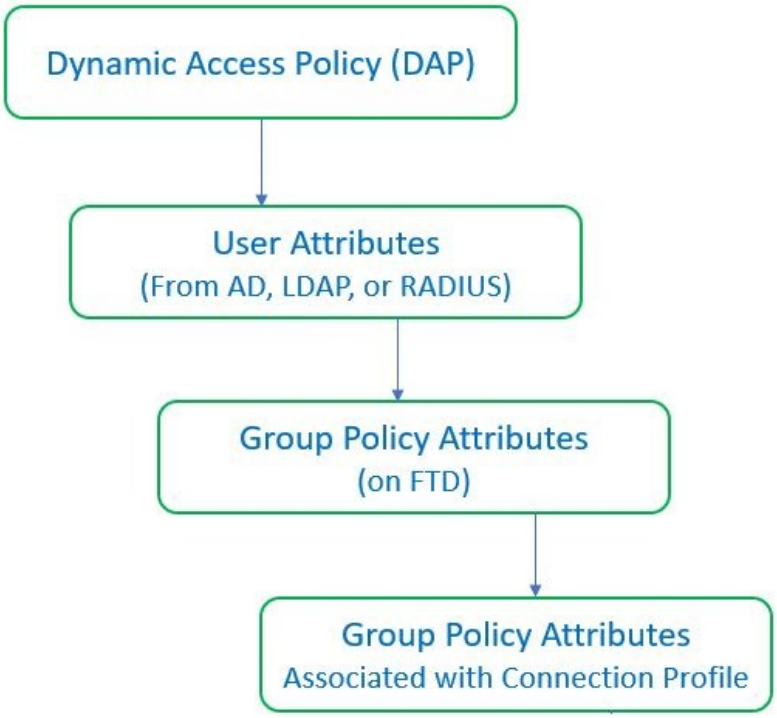
Threat Defense에서 권한 및 속성 정책 시행 계층 구조

threat defense 디바이스는 VPN 연결에 사용자 권한 부여 특성(사용자 권한 또는 허가라고도 함)을 적용할 수 있습니다. 특성은 threat defense, 외부 인증 서버 및/또는 권한 부여 AAA 서버(RADIUS)의 DAP 또는 threat defense 디바이스의 그룹 정책에서 적용됩니다.

threat defense 디바이스가 모든 소스에서 속성을 수신하면 디바이스에서 평가, 병합 및 사용자 정책에 속성을 적용합니다. DAP, AAA 서버 또는 그룹 정책에서 제공하는 특성 간에 충돌이 있는 경우 DAP의 속성이 항상 우선적으로 적용됩니다.

threat defense 디바이스에서는 다음 순서로 속성을 적용합니다.

그림 *1:* 정책 시행 흐름



1. **FTD**의 **DAP** 속성 — DAP 속성은 다른 모든 속성보다 우선적으로 적용됩니다.
2. **AAA** 서버의 사용자 속성 - 사용자 인증 및/또는 권한 부여가 성공적으로 수행되면 서버에서 이러한 특성을 반환합니다.
3. **FTD** 에 구성된 그룹 정책 - RADIUS 서버에서 사용자에 대해 RADIUS 클래스 속성 IETF-Class-25(OU=group-policy) 값을 반환하면 threat defense 디바이스에서는 해당 사용자를 이름이 같은 그룹 정책에 배치하고 서버에서 반환하지 않은 그룹 정책의 모든 속성을 적용합니다.
4. 연결 프로파일에서 할당한 그룹 정책**(**터널 그룹으로 알려짐**)** - 연결 프로파일에는 연결을 위한 예비 설정이 있으며 인증 전에 사용자에게 적용되는 기본 그룹 정책을 포함합니다.

참고 threat defense 디바이스는 기본 그룹 정책인 *DfltGrpPolicy*에서 시스템 기본 속성 상속을 지원하지 않습니다. 사용자 세션의 경우 사용자 속성 또는 AAA 서버의 그룹 정책이 속성을 재정의하지 않는 한 디바이스는 사용자가 연결 프로파일에 할당한 그룹 정책의 속성을 사용합니다.

Dynamic Access Policy에 대한 라이센싱

Threat Defense에는 다음 AnyConnect Client 라이선스 중 하나 이상이 있어야 합니다.

- AnyConnect Apex
- AnyConnect Plus
- AnyConnect VPN Only

Base 라이선스는 내보내기 제어 기능을 허용해야 합니다.

Dynamic Access Policy에 대한 사전 요건

표 *1:*

사전 요건 유형	설명

라이선싱	• Threat Defense에는 다음 AnyConnect Client 라이선스 중 하나 이상이 있어야 합니다.
	  • AnyConnect Apex
	  • AnyConnect Plus
	  • AnyConnect VPN Only
	• threat defense Base 라이선스는 내보내기 제어 기능을 허용해야 합니다.

컨피그레이션	DAP의 사전 요건에 대한 자세한 내용은 *Firepower Management Center 구성 가이드*의 *Secure Firewall Threat DefenseDynamic Access Policy* 섹션을 참조하십시오. 원격 액세스 VPN 사전 요건 및 구성에 대한 자세한 내용은 *Firepower Management Center 구성 가이드*의 *Secure Firewall Threat Defense* 원격 액세스 *VPN* 섹션을 참조하십시오.

Dynamic Access Policy에 대한 지침 및 제한 사항

- DAP에서 AAA 특성 일치는 원격 액세스 VPN 세션을 인증하거나 권한 부여할 때 AAA 서버가 올바른 특성을 반환하도록 구성된 경우에만 작동합니다.

- DAP에 대해 지원되는 최소 AnyConnect 및 HostScan 패키지 버전은 4.6입니다. 그러나 최신 버전의 AnyConnect를 사용하는 것이 좋습니다.

DAP(Dynamic Access Policy) 구성

Dynamic Access Policy 생성

시작하기 전에

Dynamic Access Policy를 구성하기 전에 HostScan 패키지가 있는지 확인합니다. **Objects(**개체**)** > **Object Management(**개체 관리**)** > **VPN** > **AnyConnect File(AnyConnect** 파일**)**에서 HostScan 파일을 추가할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Dynamic Access Policy** > **Create Dynamic Access Policy(Dynamic Access Policy** 생성**)**를 선택합니다.

단계 **2** DAP 정책의 **Name(**이름**)**을 지정하고 선택 사항인 **Description(**설명**)**을 지정합니다.

단계 **3** 목록에서 **HostScan** 패키지를 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

DAP 레코드를 구성하려면 Dynamic Access Policy 레코드 생성을 참조하십시오.

Dynamic Access Policy 레코드 생성

DAP(Dynamic Access Policy)는 사용자 및 엔드포인트 특성을 구성하는 여러 DAP 레코드를 포함할 수 있습니다. 사용자가 VPN 연결을 시도할 때 threat defense가 필수 기준을 선택하고 순서를 지정할 수 있도록 DAP 내 DAP 레코드의 우선 순위를 지정할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Dynamic Access Policy**를 선택합니다.

단계 **2** 기존 Dynamic Access Policy를 편집하거나 새 정책을 생성한 다음 편집합니다.

단계 **3** DAP 레코드의 **Name(**이름**)**을 지정합니다.

단계 **4** DAP 레코드의 우선순위를 입력합니다.

번호가 낮을수록 우선 순위가 높습니다.

단계 **5** DAP 레코드가 일치할 때 수행할 다음 작업 중 하나를 선택합니다.

- **Continue(**계속**)** - 액세스 정책 특성을 세션에 적용하려면 클릭합니다.
- **Terminate(**종료**)** - 세션을 종료하려면 선택합니다.
- **Quarantine(**격리**)** - 연결을 격리하려면 선택합니다.

단계 **6** **Display User Message on Criterion Match(**조건 일치 시 사용자 메시지 표시**)** 확인란을 선택하고 사용자 메시지를 추가합니다.

threat defense는 DAP 레코드가 일치할 때 사용자에게 이 메시지를 표시합니다.

단계 **7** **Apply a Network ACL on Traffic(**트래픽에 네트워크 **ACL** 적용**)** 확인란을 선택하고 드롭다운에서 액세스 제어 목록을 선택합니다.

단계 **8** **Apply one or more AnyConnect Custom Attributes(**하나 이상의 **AnyConnect** 사용자 지정 속성 적용**)** 확인란을 선택하고 드롭다운에서 사용자 지정 속성 개체를 선택합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

DAP에 대한 AAA 기준 설정 구성

DAP는 AAA에서 제공하는 특성을 재정의할 수 있는 제한된 권한 부여 특성 집합을 제공하여 AAA 서비스를 보완합니다. threat defense에서는 사용자에 대한 AAA 권한 부여 정보 및 세션에 대한 상태 진단 정보를 기반으로 DAP 레코드를 선택합니다. threat defense에서는 이 정보에 따라 여러 DAP 레코드를 선택한 다음 이를 집계하여 DAP 권한 부여 특성을 만들 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Dynamic Access Policy**를 선택합니다.

단계 **2** 기존 DAP 정책을 편집하거나 새 정책을 생성한 다음 편집합니다.

단계 **3** DAP 레코드를 선택하거나 새 레코드를 생성하고 DAP 레코드를 수정합니다.

단계 **4** **AAA Criteria(AAA** 기준**)**를 클릭합니다.

단계 **5** 다음의 **Match criteria between sections(**섹션 간 일치 기준**)** 중에서 하나를 선택합니다.

- Any(임의) - 다음 조건 중 하나와 일치
- All(모두) - 모든 기준과 일치
- None(없음) - 설정된 기준과 일치하지 않음

단계 **6** **Add(**추가**)**를 클릭하여 필요한 **Cisco VPN Criteria(Cisco VPN** 기준**)**를 추가합니다.

Cisco VPN 기준에는 그룹 정책, 할당된 IPv4 주소, 할당된 IPv6 주소, 연결 프로파일, 사용자 이름, 사용자 이름 2 및 필수 SCEP에 대한 속성이 포함됩니다.

a) 속성을 선택하고 **Value(**값**)**를 지정합니다.

b) 기준을 더 추가하려면 **Add another criteria(**다른 기준 추가**)**를 클릭합니다.
c) **Save(**저장**)**를 클릭합니다.

SCEP 필수

단계 **7** **LDAP Criteria(LDAP** 기준**)**, **RADIUS Criteria(RADIUS** 기준**)** 또는 **SAML Criteria(SAML** 기준**)**를 선택하고 **Attribute ID(**속성 **ID)** 및 **Value(**값**)**를 지정합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

DAP에서 엔드포인트 속성 선택 조건 구성

엔드포인트 속성은 엔드포인트 시스템 환경, 상태 진단 결과 및 애플리케이션에 대한 정보를 포함합니다. threat defense에서는 세션을 설정하는 동안 엔드포인트 속성 모음을 생성하고 이러한 속성을 해당 세션과 연계된 데이터베이스에 저장합니다. 각 DAP 레코드는 threat defense에서 세션에 대해 선택하기 위해 충족해야 하는 엔드포인트 선택 특성을 지정합니다. threat defense에서는 구성된 모든 조건을 충족하는 DAP 레코드만 선택합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Dynamic Access Policy** > **Create Dynamic Access Policy(Dynamic Access Policy** 생성**)**를 선택합니다.

단계 **2** DAP 정책을 수정한 다음 DAP 레코드를 수정합니다.

참고 아직 수행하지 않은 경우 DAP 정책 및 DAP 레코드를 생성합니다.

단계 **3** **Endpoint Criteria(**엔드포인트 기준**)**를 클릭하고 다음 엔드포인트 기준 특성을 구성합니다.

참고 각 엔드포인트 특성 유형의 여러 인스턴스를 만들 수 있습니다. 각 DAP 레코드의 엔드포인트 특성 수에 대한 제한은 없습니다.

- DAP에 안티맬웨어 엔드포인트 특성 추가
- DAP에 디바이스 엔드포인트 특성 추가
- DAP에 AnyConnect 엔드포인트 특성 추가, 8 페이지
- DAP에 NAC 엔드포인트 특성 추가
- DAP에 애플리케이션 특성 추가
- DAP에 개인 방화벽 엔드포인트 특성 추가
- DAP에 운영 체제 엔드포인트 특성 추가
- DAP에 프로세스 엔드포인트 특성 추가
- DAP에 레지스트리 엔드포인트 특성 추가

- DAP에 파일 엔드포인트 특성 추가
- DAP에 인증서 인증 속성 추가

단계 **4** **Save(**저장**)**를 클릭합니다.

DAP에 안티맬웨어 엔드포인트 특성 추가

프로시저

단계 **1** DAP 레코드를 편집하고 **Endpoint Criteria(**엔드포인트 기준**)** > **Anti-Malware(**악성코드 차단**)**를 선택합니다.

단계 **2** Match Criteria(일치 기준)으로 **All(**모두**)** 또는 **Any(**임의**)**를 선택합니다.

단계 **3** **Add(**추가**)**를 클릭하여 악성코드 차단 속성을 추가합니다.

단계 **4** **Installed(**설치됨**)**을 클릭하여 선택한 엔드포인트 속성과 해당 한정자가 설치되어 있는지 또는 설치되어 있지 않은지 표시합니다.

단계 **5** 실시간 악성코드 검사를 활성화하거나 비활성화하려면 **Enabled(**활성화**)** 또는 **Disabled(**비활성화**)**를 선택합니다.

단계 **6** 목록에서 악성코드 차단 **Vendor(**벤더**)**의 이름을 선택합니다.

단계 **7** 악성코드 차단 제품 설명을 선택합니다.

단계 **8** 악성코드 차단 제품의 버전을 선택합니다.

단계 **9** **Last Update(**마지막 업데이트**)**에는 마지막 업데이트 이후로 경과한 일 수를 지정합니다.

악성코드 차단 업데이트가 지정한 일 수보다 짧거나(<) 더 많이(>) 발생하도록 지정할 수 있습니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

DAP에 디바이스 엔드포인트 특성 추가

프로시저

단계 **1** DAP 레코드를 편집하고 **Endpoint Criteria(**엔드포인트 기준**)** > **Device(**디바이스**)**를 선택합니다.

단계 **2** Match Criteria(일치 기준)으로 **All(**모두**)** 또는 **Any(**임의**)**를 선택합니다.

단계 **3** **Add(**추가**)**를 클릭하고 = 또는 ≠ 연산자를 선택하여 속성이 다음 속성에 대해 입력한 값과 같거나 같지 않은지 확인합니다.

- **Host Name(**호스트 이름**)** — 테스트할 디바이스의 호스트 이름입니다. 컴퓨터의 FQDN(정규화된 도메인 이름)이 아니라 호스트 이름만 사용합니다.

- **MAC Address(MAC** 주소**)** — 테스트할 네트워크 인터페이스 카드의 MAC 주소입니다. 주소는 xxxx.xxxx.xxxx 형식(여기서 x는 유효한 16진수 문자)이어야 합니다.
- **BIOS Serial Number(BIOS** 일련 번호**)** — 테스트할 디바이스의 BIOS 일련 번호 값입니다. 번호 형식은 제조업체별로 다릅니다.
- **Port Number(**포트 번호**)** — 디바이스의 수신 대기 포트 번호입니다.
- **Secure Desktop Version(Secure Desktop** 버전**) -** 엔드포인트에서 실행 중인 Host Scan 이미지의 버전입니다.
- **OPSWAT Version(OPSWAT** 버전**)** — OPSWAT 클라이언트 버전입니다.
- **Privacy Protection(**개인정보 보호**)** — None(없음), Cache Cleaner(캐시 클리너), Secure Desktop(보안 데스크톱).
- **TCP/UDP Port Number(TCP/UDP** 포트 번호**) -** 테스트 중인 수신 대기 상태의 TCP 또는 UDP 포트입니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

DAP에 AnyConnect 엔드포인트 특성 추가

프로시저

단계 **1** DAP 레코드를 편집하고 **Endpoint Criteria(**엔드포인트 기준**)** > **AnyConnect**를 선택합니다.

단계 **2** Match Criteria(일치 기준)으로 **All(**모두**)** 또는 **Any(**임의**)**를 선택합니다.

단계 **3** 속성이 입력한 값과 같거나 같지 않은지 확인하려면 **Add(**추가**)**를 클릭하고 = 또는 ≠ 연산자를 선택합니다.

단계 **4** **Client Version(**클라이언트 버전**)** 및 **Platform(**플랫폼**)**을 선택합니다.

단계 **5** **Platform Version(**플랫폼 버전**)**을 선택하고 **Device Type(**디바이스 유형**)** 및 **Device Unique ID(**디바이스 고유 **ID)**를 지정합니다.

단계 **6** **MAC** 주소를 MAC 주소 풀에 추가합니다.

참고 MAC 주소는 XX-XX-XX-XX-XX-XX 형식(여기서 X는 16진수 문자)이어야 합니다. **Add another MAC Address(**다른 **MAC** 주소 추가**)**를 클릭하여 주소를 더 추가할 수 있습니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

DAP에 NAC 엔드포인트 속성 추가

프로시저

단계 **1** DAP 레코드를 편집하고 **Endpoint Criteria(**엔드포인트 기준**)** > **NAC**를 선택합니다.

단계 **2** Match Criteria(일치 기준)으로 **All(**모두**)** 또는 **Any(**임의**)**를 선택합니다.

단계 **3** **Add(**추가**)**를 클릭하여 NAC 속성을 추가합니다.

단계 **4** 연산자를 같음 = 또는 같지 않음 ≠ 상태 토큰 문자열로 설정합니다. **Posture Status(**포스처 상태**)** 상자에 상태 토큰 문자열을 입력합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

DAP에 애플리케이션 특성 추가

프로시저

단계 **1** DAP 레코드를 편집하고 **Endpoint Criteria(**엔드포인트 기준**)** > **Application(**애플리케이션**)**을 선택합니다.

단계 **2** Match Criteria(일치 기준)으로 **All(**모두**)** 또는 **Any(**임의**)**를 선택합니다.

단계 **3** **Add(**추가**)**를 클릭하여 애플리케이션 속성을 추가합니다.

단계 **4** 같음(=) 또는 같지 않음(≠)을 선택하고 원격 액세스 연결의 유형을 나타내는 **Client Type(**클라이언트 유형**)**을 지정합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

DAP에 개인 방화벽 엔드포인트 특성 추가

프로시저

단계 **1** DAP 레코드를 편집하고 **Endpoint Criteria(**엔드포인트 기준**)** > **Personal Firewall(**개인 방화벽**)**을 선택합니다.

단계 **2** Match Criteria(일치 기준)으로 **All(**모두**)** 또는 **Any(**임의**)**를 선택합니다.

단계 **3** **Add(**추가**)**를 클릭하여 개인 방화벽 속성을 추가합니다.

단계 **4** **Installed(**설치됨**)**을 클릭하여 개인 방화벽 엔드포인트 속성과 해당 한정자(Name/Operation/Value(이름/작업/값) 열 아래의 필드)가 설치되어 있는지 또는 설치되어 있지 않은지 표시합니다.

단계 **5** **Enabled(**활성화**)** 또는 **Disabled(**비활성화**)**를 선택하여 방화벽 보호를 활성화하거나 비활성화합니다.

단계 **6** 목록에서 방화벽 벤더의 이름을 선택합니다.

단계 **7** 방화벽 제품 설명을 선택합니다.

단계 **8** 같음(=) 또는 같지 않음(≠) 연산자를 선택하고 개인 방화벽 제품의 버전을 선택합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

DAP에 운영 체제 엔드포인트 특성 추가

프로시저

단계 **1** DAP 레코드를 편집하고 **Endpoint Criteria(**엔드포인트 기준**)** > **Operating System(**운영 체제**)**을 선택합니다.

단계 **2** Match Criteria(일치 기준)으로 **All(**모두**)** 또는 **Any(**임의**)**를 선택합니다.

단계 **3** **Add(**추가**)**를 클릭하여 엔드포인트 속성을 추가합니다.

단계 **4** 같음(=) 또는 같지 않음(≠) 연산자를 선택한 다음 **Operating System(**운영 체제**)**을 선택합니다.

단계 **5** 같음(=) 또는 같지 않음(≠) 연산자를 선택한 다음 운영 체제 **Version(**버전**)**을 지정합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

DAP에 프로세스 엔드포인트 특성 추가

프로시저

단계 **1** DAP 레코드를 편집하고 **Endpoint Criteria(**엔드포인트 기준**)** > **Process(**프로세스**)**를 선택합니다.

단계 **2** Match Criteria(일치 기준)으로 **All(**모두**)** 또는 **Any(**임의**)**를 선택합니다.

단계 **3** **Add(**추가**)**를 클릭하여 프로세스 속성을 추가합니다.

단계 **4** **Exists(**있음**)** 또는 **Does not exist(**없음**)**를 선택합니다.

단계 **5** **Process Name(**프로세스 이름**)**을 지정합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

DAP에 레지스트리 엔드포인트 특성 추가

레지스트리 엔드포인트 특성 검사는 Windows 운영 체제에만 적용됩니다.

시작하기 전에

레지스트리 엔드포인트 특성을 구성하기 전에 Cisco Secure Desktop Host Scan 창에서 검사할 레지스트리 키를 정의합니다.

프로시저

단계 **1** DAP 레코드를 편집하고 **Endpoint Criteria(**엔드포인트 기준**)** > **Registry(**레지스트리**)**를 선택합니다.
단계 **2** Match Criteria(일치 기준)으로 **All(**모두**)** 또는 **Any(**임의**)**를 선택합니다.
단계 **3** **Add(**추가**)**를 클릭하여 레지스트리 속성을 추가합니다.
단계 **4** 레지스트리의 **Entry Path(**항목 경로**)**를 선택하고 경로를 지정합니다.
단계 **5** 레지스트리의 존재 여부를 **Exists(**있음**)** 또는 **Does not Exist(**존재하지 않음**)** 중에서 선택합니다.
단계 **6** 목록에서 레지스트리 유형을 선택합니다.
단계 **7** 같음(=) 또는 같지 않음(≠) 연산자를 선택하고 레지스트리 키의 **Value(**값**)**를 입력합니다.
단계 **8** 검사하는 동안 레지스트리 항목의 대/소문자를 무시하려면 **Case insensitive(**대/소문자 구분 안 함**)**를 선택합니다.
단계 **9** **Save(**저장**)**를 클릭합니다.

DAP에 파일 엔드포인트 특성 추가

프로시저

단계 **1** DAP 레코드를 편집하고 **Endpoint Criteria(**엔드포인트 기준**)** > **File(**파일**)**을 선택합니다.
단계 **2** Match Criteria(일치 기준)으로 **All(**모두**)** 또는 **Any(**임의**)**를 선택합니다.
단계 **3** **Add(**추가**)**를 클릭하여 파일 속성을 추가합니다.
단계 **4** **File Path(**파일 경로**)**를 지정합니다.
단계 **5** **Exists(**있음**)** 또는 **Does not exist(**없음**)**를 선택하여 파일의 존재 여부를 나타냅니다.
단계 **6** 보다 작음(<) 또는 보다 큼(>)을 선택하고 파일의 **Last Modified(**마지막 수정일를 지정합니다.
단계 **7** 같음(=) 또는 같지 않음(≠) 연산자를 선택하고 체크섬을 입력합니다.
단계 **8** **Save(**저장**)**를 클릭합니다.

DAP에 인증서 인증 속성 추가

구성된 규칙에 따라 수신된 인증서를 참조할 수 있도록 각 인증서를 인덱싱할 수 있습니다. 이러한 인증서 필드를 기준으로 연결 시도를 허용하거나 거부하도록 DAP 규칙을 구성할 수 있습니다.

프로시저

단계 **1** DAP 레코드를 편집하고 **Endpoint Criteria(**엔드포인트 기준**)** > **Certificate(**인증서**)**를 선택합니다.
단계 **2** Match Criteria(일치 기준)으로 **All(**모두**)** 또는 **Any(**임의**)**를 선택합니다.
단계 **3** **Add(**추가**)**를 클릭하여 인증서 속성을 추가합니다.

단계 **4** 인증서, **Cert1** 또는 **Cert2**를 선택합니다.

단계 **5** **Subject(**제목**)**를 선택하고 제목 값을 지정합니다.

단계 **6** **Issuer(**발급자**)**를 선택하고 발급자 값을 지정합니다.

단계 **7** **Subject Alternate Name(**주체 대체 이름**)**을 선택하고 주체 값을 지정합니다.

단계 **8** 일련 번호를 지정합니다.

단계 **9** **Certificate Store(**인증서 저장소**)**: (None(없음), Machine(시스템) 또는 User(사용자))를 선택합니다.

VPN 클라이언트가 인증서 저장소 정보를 전송합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

DAP에 대한 고급 설정 구성

Advanced(고급) 탭을 사용하여 AAA 및 엔드포인트 속성 영역에서 지정할 수 없는 선택 기준을 추가할 수 있습니다. 예를 들어 지정한 조건 중 하나 이상 또는 모두를 충족하거나 지정한 조건이 없는 AAA 특성을 사용하도록 threat defense를 구성할 수 있지만 엔드포인트 특성은 누적되므로 모두 충족해야 합니다. 보안 어플라이언스에서 하나의 특정 엔드포인트 특성을 사용하도록 하려면 적절한 Lua 논리 식을 만들어 여기에 입력해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Dynamic Access Policy**를 선택합니다.

단계 **2** DAP 정책을 편집한 다음 DAP 레코드를 변경합니다.

참고 아직 수행하지 않은 경우 DAP 정책 및 DAP 레코드를 생성합니다.

단계 **3** **Advanced(**고급**)** 탭을 클릭합니다.

단계 **4** DAP 구성에서 사용할 일치 기준으로 **AND** 또는 **OR**를 선택합니다.

단계 **5** 고급 속성 일치를 위한 **Lua** 스크립트 필드에 Lua 스크립트를 추가합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

Dynamic Access Policy를 원격 액세스 VPN과 연결

Dynamic Access Policy(DAP)을 원격 액세스 VPN 정책과 연결하여 VPN 세션 인증 및 권한 부여 중에 Dynamic Access Policy 특성을 일치시킬 수 있습니다. 그런 다음 threat defense에 원격 액세스 VPN을 구축할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** Dynamic Access Policy를 연결할 원격 액세스 VPN 정책 옆에 있는 **Edit(**편집**)**를 클릭합니다.

단계 **3** 원격 액세스 VPN의 링크를 클릭하여 Dynamic Access Policy(Dynamic Access Policy)를 선택합니다.

단계 **4** **Dynamic Access Policy(Dynamic Access Policy)**드롭다운에서 정책을 선택하거나 **Create a new Dynamic Access Policy**(새 Dynamic Access Policy 생성)를 클릭하여 새 Dynamic Access Policy를 구성합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭하여 원격 액세스 VPN 정책을 저장합니다.

원격 액세스 VPN 사용자가 연결을 시도하면 VPN은 구성된 Dynamic Access Policy 레코드 및 속성을 확인합니다. VPN은 일치하는 Dynamic Access Policy 레코드를 기반으로 Dynamic Access Policy를 생성하고 VPN 세션에서 적절한 작업을 수행합니다.

Dynamic Access Policy 기록

기능	버전	세부 사항
Dynamic Access Policy	7.0	이 기능을 도입했습니다.