ASA 9.X DAP(Dynamic Access Policy) 구축

목차

소개

이 문서에서는 ASA 9.x DAP(Dynamic Access Policy)의 구축, 기능 및 사용법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- VPN(Virtual Private Network) 게이트웨이
- DAP(동적 액세스 정책)

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

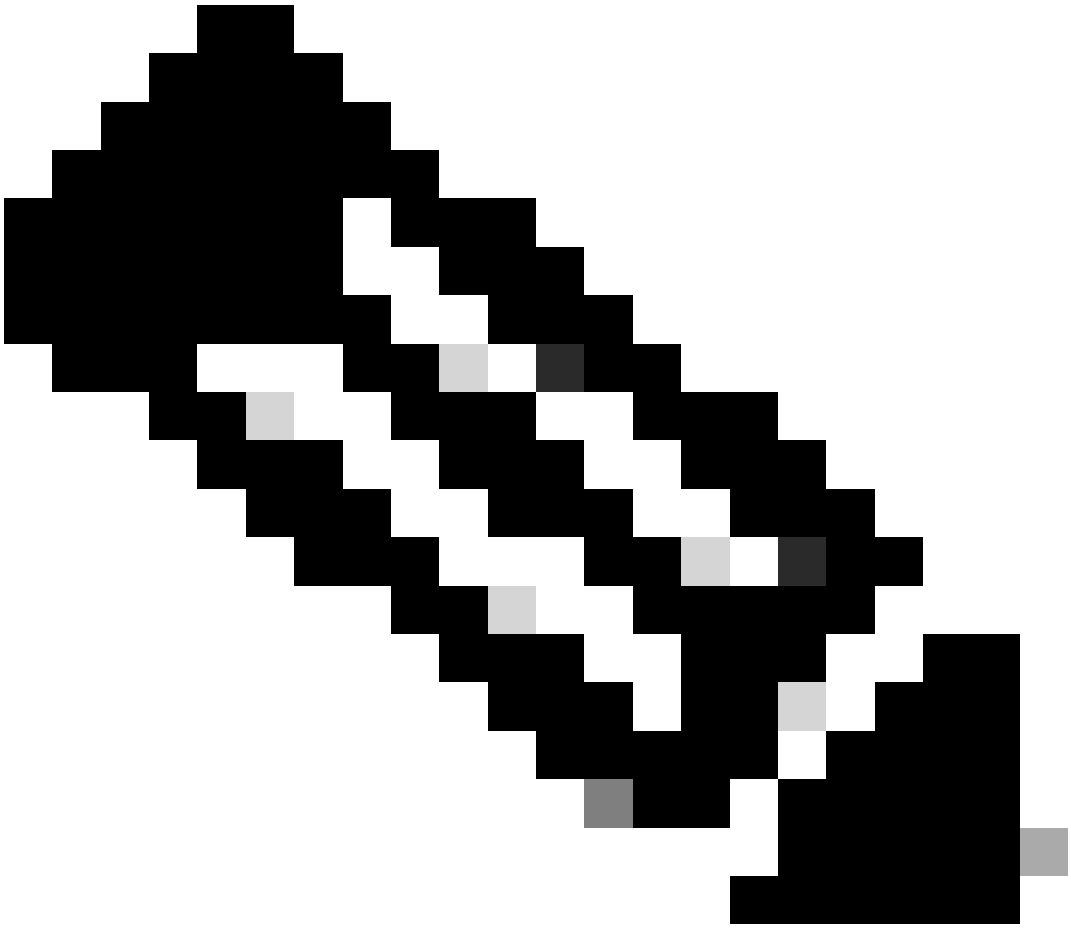
배경 정보

VPN(Virtual Private Network) 게이트웨이는 동적 환경에서 작동합니다. 여러 변수가 각 VPN 연결에 영향을 미칠 수 있습니다. 예를 들어 자주 변경되는 인트라넷 구성, 각 사용자가 조직 내에서 사

용할 수 있는 다양한 역할, 서로 다른 구성과 보안 수준을 가진 원격 액세스 사이트의 로그인 등에 영향을 줄 수 있습니다. 동적 VPN 환경에서는 정적 컨피그레이션이 있는 네트워크보다 사용자 인증 작업이 훨씬 복잡합니다.

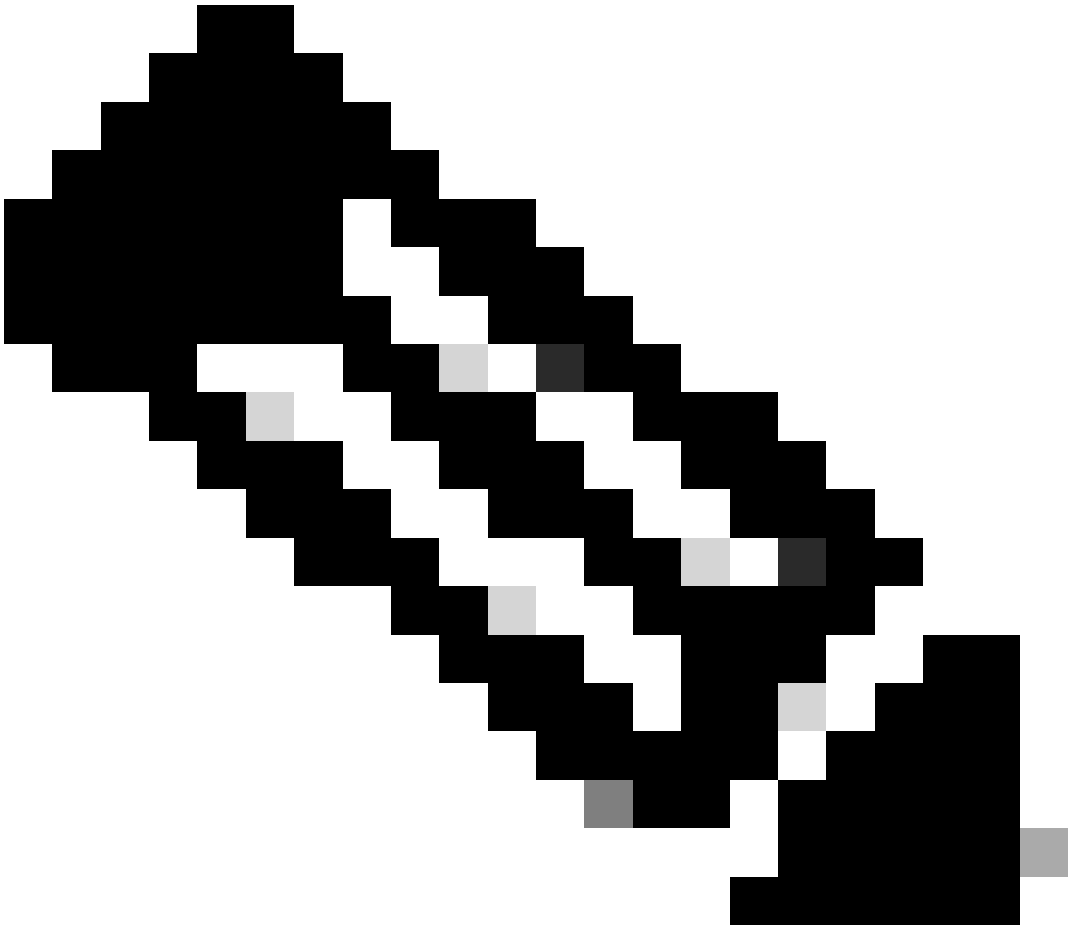
DAP(Dynamic Access Policy)는 VPN 환경의 동적 특성을 처리하는 권한 부여를 구성할 수 있는 기능입니다. 특정 사용자 터널 또는 세션과 연결하는 액세스 제어 특성 모음을 설정하여 동적 액세스 정책을 생성할 수 있습니다. 이러한 특성은 여러 그룹 멤버십 및 엔드포인트 보안의 문제를 해결합니다.

예를 들어, 보안 어플라이언스는 사용자가 정의한 정책에 따라 특정 세션에 대해 특정 사용자에게 액세스 권한을 부여합니다. 하나 이상의 DAP 레코드에서 특성을 선택 및/또는 집계하여 사용자 인증 전반에 걸쳐 DAP를 생성합니다. 원격 디바이스의 엔드포인트 보안 정보 및/또는 인증된 사용자에 대한 AAA 권한 부여 정보를 기반으로 이러한 DAP 레코드를 선택합니다. 그런 다음 DAP 레코드를 사용자 터널 또는 세션에 적용합니다.



참고: DAP 정책 선택 특성이 포함된 dap.xml 파일은 ASA 플래시에 저장됩니다. dap.xml 파일을 오프박스로 내보내고, 편집한 다음(XML 구문을 알고 있는 경우) 다시 가져올 수 있지만, 잘못 구성한 경우 ASDM에서 DAP 레코드 처리를 중지할 수 있으므로 주의하십시오. 컨

피그레이션의 이 부분을 조작할 CLI는 없습니다.



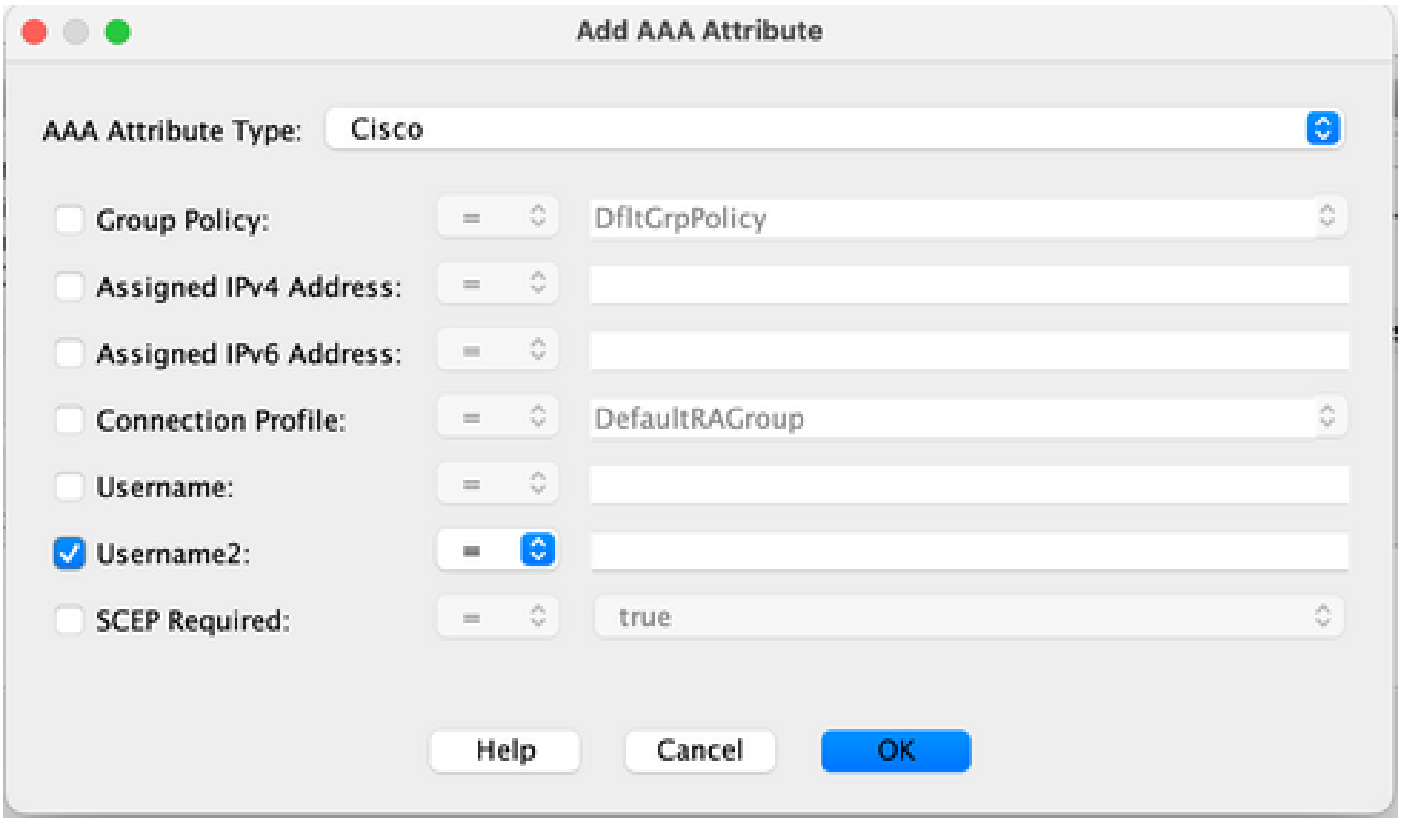
참고: CLI를 통해 dynamic-access-policy-record 액세스 매개변수를 구성하려고 하면 ASDM에서 올바르게 관리하더라도 DAP의 작동이 중지될 수 있습니다. CLI를 사용하지 않고 항상 ASDM을 사용하여 DAP 정책을 관리합니다.

DAP 및 AAA 특성

DAP는 AAA 서비스를 보완하며 AAA가 제공하는 특성을 재정의할 수 있는 제한된 권한 부여 특성 집합을 제공합니다. 보안 어플라이언스는 사용자에 대한 AAA 권한 부여 정보를 기반으로 DAP 레코드를 선택할 수 있습니다. 보안 어플라이언스는 이 정보에 따라 여러 DAP 레코드를 선택한 다음 이를 집계하여 DAP 권한 부여 특성을 할당할 수 있습니다.

그림 1과 같이 Cisco AAA 특성 계층 또는 보안 어플라이언스가 RADIUS 또는 LDAP 서버에서 수신하는 전체 응답 특성 집합에서 AAA 특성을 지정할 수 있습니다.

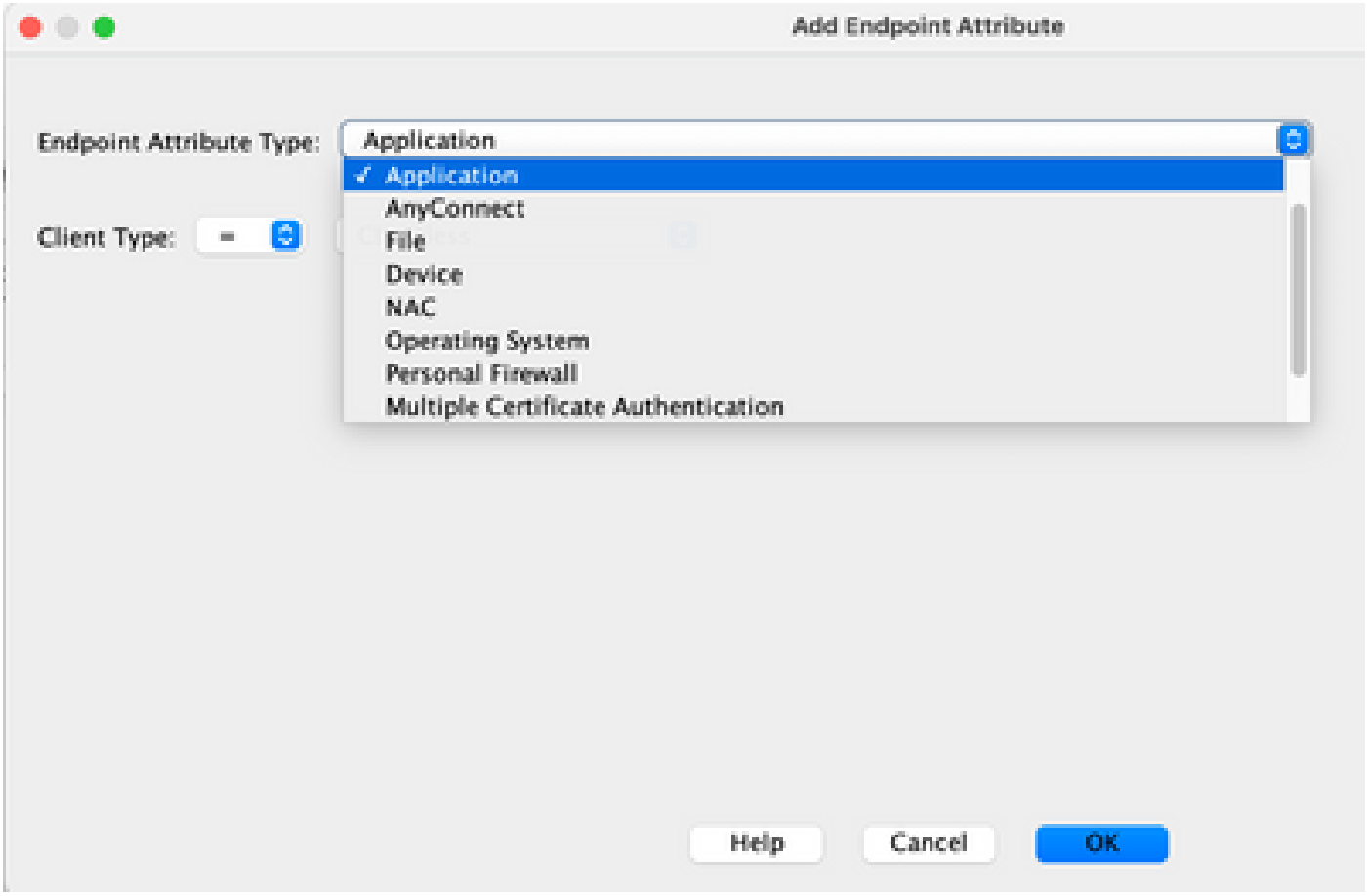
그림 1. DAP AAA 특성 GUI



DAP 및 엔드포인트 보안 특성

보안 어플라이언스는 AAA 특성 외에도 사용자가 구성한 포스처 평가 방법을 사용하여 엔드포인트 보안 특성을 가져올 수도 있습니다. 여기에는 그림 2와 같이 기본 Host Scan, Secure Desktop, Standard/Advanced Endpoint Assessment, NAC가 포함됩니다. 엔드포인트 평가 특성을 가져와 사용자 인증 전에 보안 어플라이언스로 전송합니다. 그러나 전체 DAP 레코드를 비롯한 AAA 특성은 사용자 인증 중에 검증됩니다.

그림 2. 엔드포인트 특성 GUI

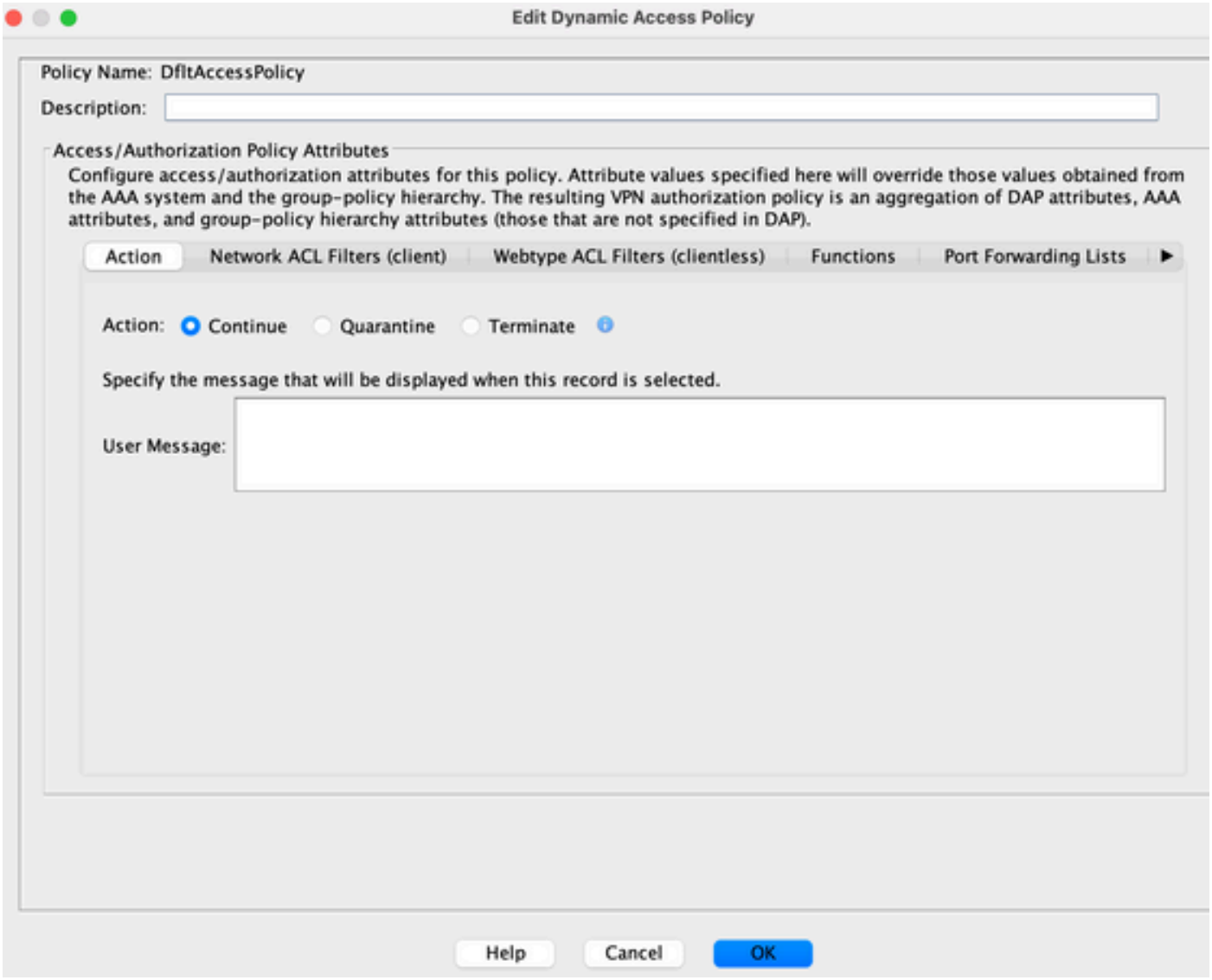


기본 동적 액세스 정책

DAP를 도입하고 구현하기 전에 특정 사용자 터널 또는 세션과 연결된 액세스 정책 특성/값 쌍이 ASA에서 로컬로 정의되었거나(즉, 터널 그룹 및 그룹 정책) 외부 AAA 서버를 통해 매핑되었습니다.

DAP는 항상 기본적으로 적용됩니다. 예를 들어, DAP를 명시적으로 적용하지 않고 터널 그룹, 그룹 정책 및 AAA를 통해 액세스 제어를 시행해도 이러한 동작이 발생할 수 있습니다. 레거시 동작의 경우 그림 3과 같이 기본 DAP 레코드인 DfltAccessPolicy를 포함하여 DAP 기능에 대한 컨피그레이션 변경이 필요하지 않습니다.

그림 3. 기본 동적 액세스 정책



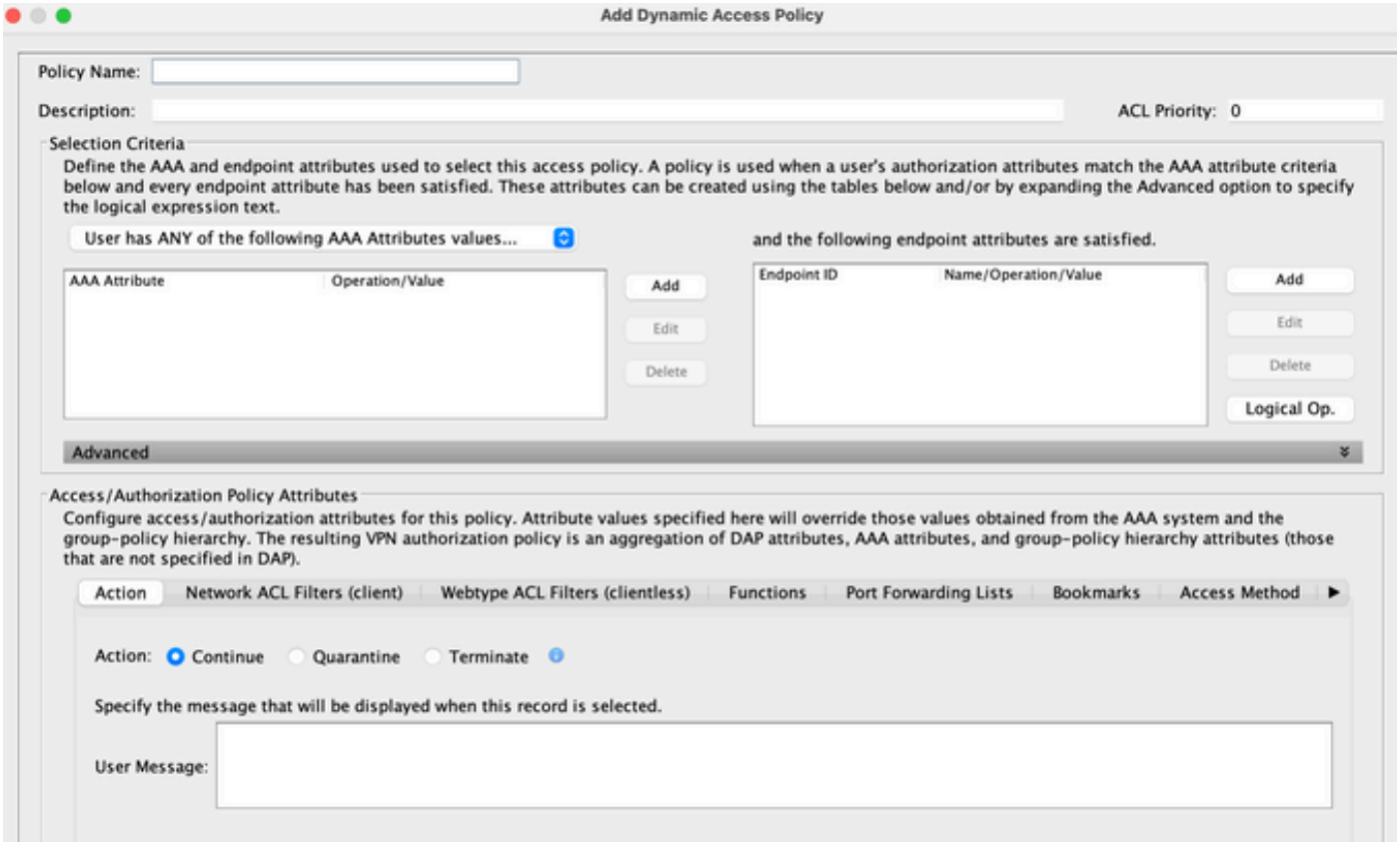
그러나 DAP 레코드의 기본값 중 하나가 변경된 경우(예: DfltAccessPolicy의 Action: 매개 변수가 기본값에서 Terminate로 변경되고 추가 DAP 레코드가 구성되지 않은 경우), 인증된 사용자는 기본적으로 DfltAccessPolicy DAP 레코드와 일치할 수 있으며 VPN 액세스가 거부될 수 있습니다.

따라서 VPN 연결을 인증하고 인증된 사용자가 액세스할 수 있는 네트워크 리소스를 정의하기 위해 하나 이상의 DAP 레코드를 만들고 구성해야 합니다. 따라서 구성된 경우 DAP가 레거시 정책 시행보다 우선할 수 있습니다.

동적 액세스 정책 구성

DAP를 사용하여 사용자가 액세스할 수 있는 네트워크 리소스를 정의할 때 고려해야 할 매개 변수가 많습니다. 예를 들어, 연결 엔드포인트가 관리 환경, 관리되지 않음 환경 또는 신뢰할 수 없는 환경에서 온 것인지 식별하는 경우 연결 엔드포인트를 식별하는 데 필요한 선택 기준을 결정하고, 엔드포인트 평가 및/또는 AAA 자격 증명을 기반으로 연결하는 사용자가 액세스할 수 있는 네트워크 리소스를 결정합니다. 이를 위해서는 먼저 그림 4와 같이 DAP의 기능과 특징을 숙지해야 합니다.

그림 4. 동적 액세스 정책



DAP 레코드를 구성할 때 고려해야 할 두 가지 주요 구성 요소가 있습니다.

- 고급 옵션을 포함한 선택 기준
- 액세스 정책 특성

Selection Criteria(선택 조건) 섹션에서는 관리자가 특정 DAP 레코드를 선택하는 데 사용되는 AAA 및 엔드포인트 특성을 구성합니다. DAP 레코드는 사용자의 권한 부여 특성이 AAA 특성 기준과 일치하고 모든 엔드포인트 특성이 충족된 경우에 사용됩니다.

예를 들어, AAA Attribute Type LDAP(Active Directory)(AAA 특성 유형 LDAP(Active Directory))를 선택하고 Attribute Name(특성 이름) 문자열은 memberOf(멤버)이며 Value(값) 문자열은 Contractors(계약자)인 경우, 인증 사용자는 AAA 특성 기준에 일치하려면 Active Directory 그룹 Contractors(계약자)의 멤버여야 합니다.

인증 사용자는 AAA 특성 기준을 충족하는 것 외에도 엔드포인트 특성 기준을 충족해야 할 수 있습니다. 예를 들어, 연결 엔드 포인트의 상태를 결정 하고 그 상태 평가에 따라 관리자가 구성 된 경우, 관리자는 그림 5b에 표시 된 엔드 포인트 특성에 대한 선택 기준으로 이 평가 정보를 사용 할 수 있습니다.

그림 5a. AAA 특성 기준

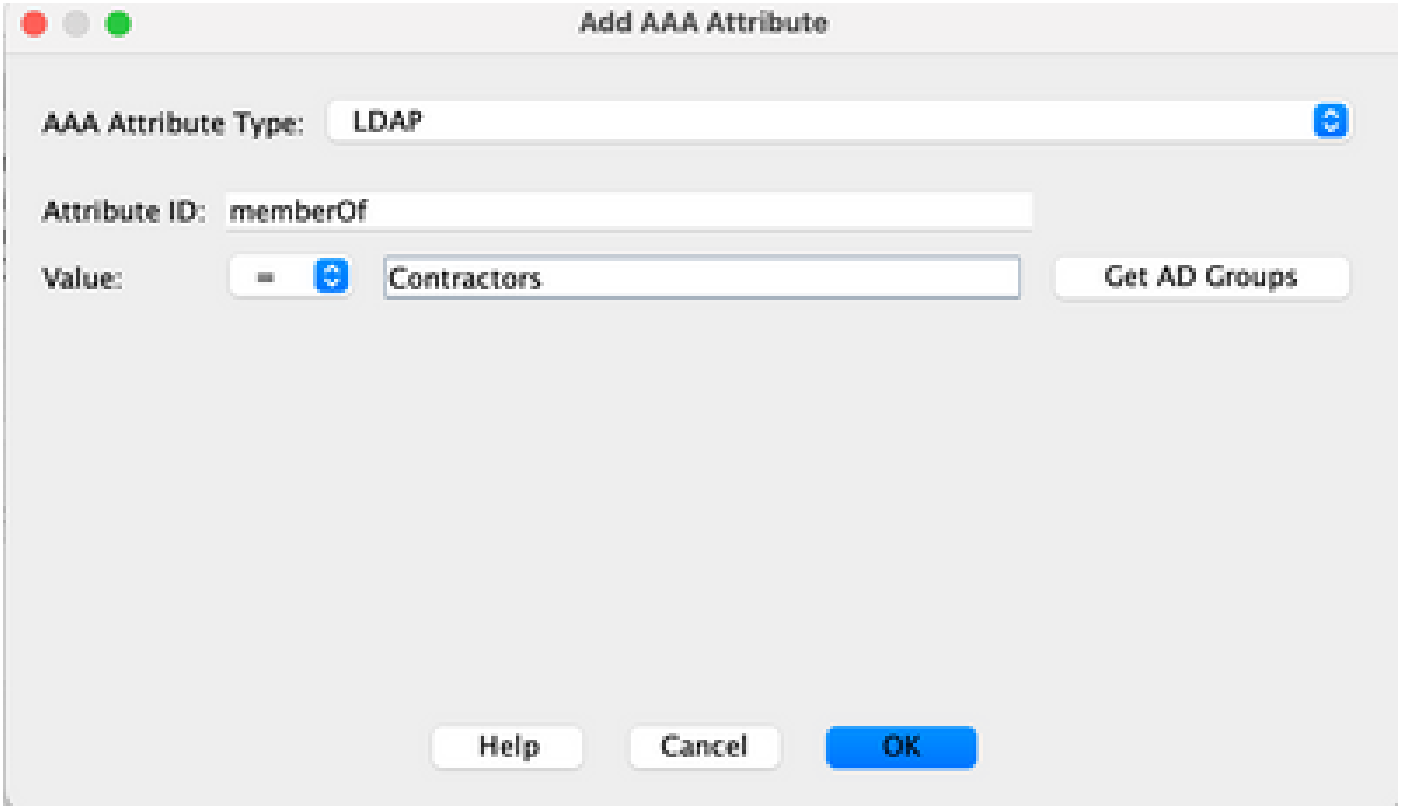


그림 5b. 엔드포인트 특성 기준

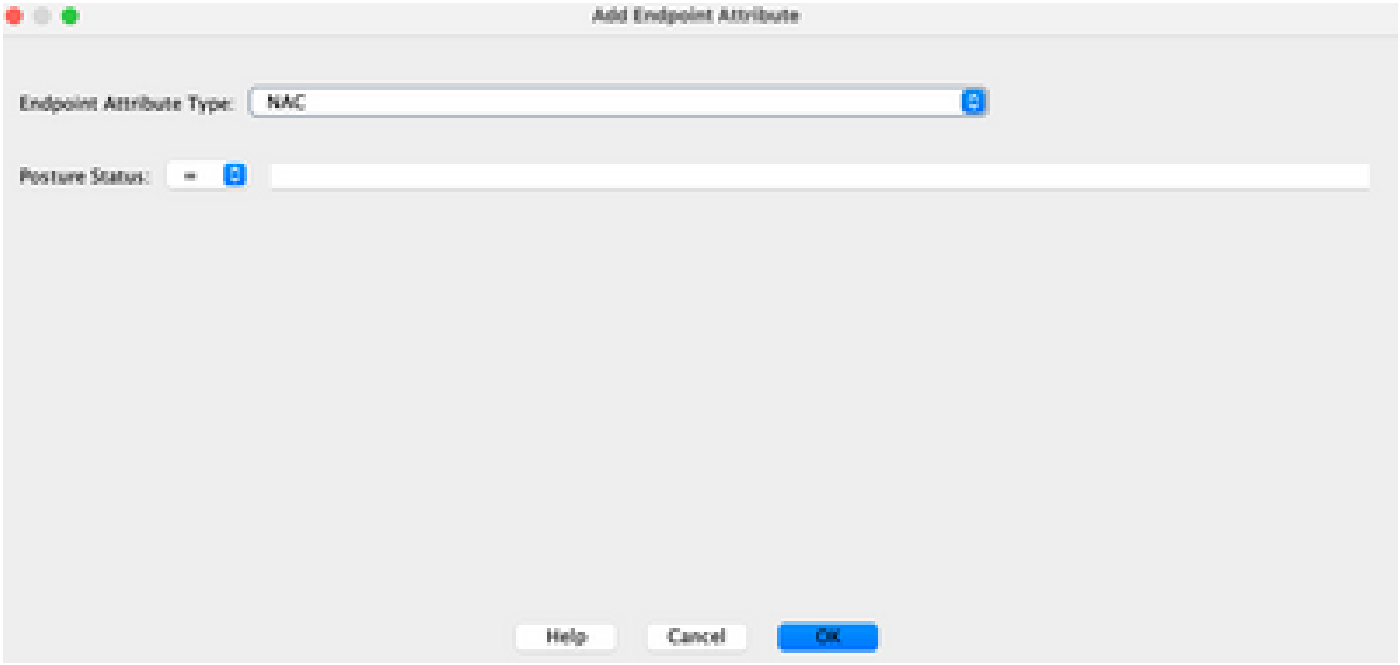
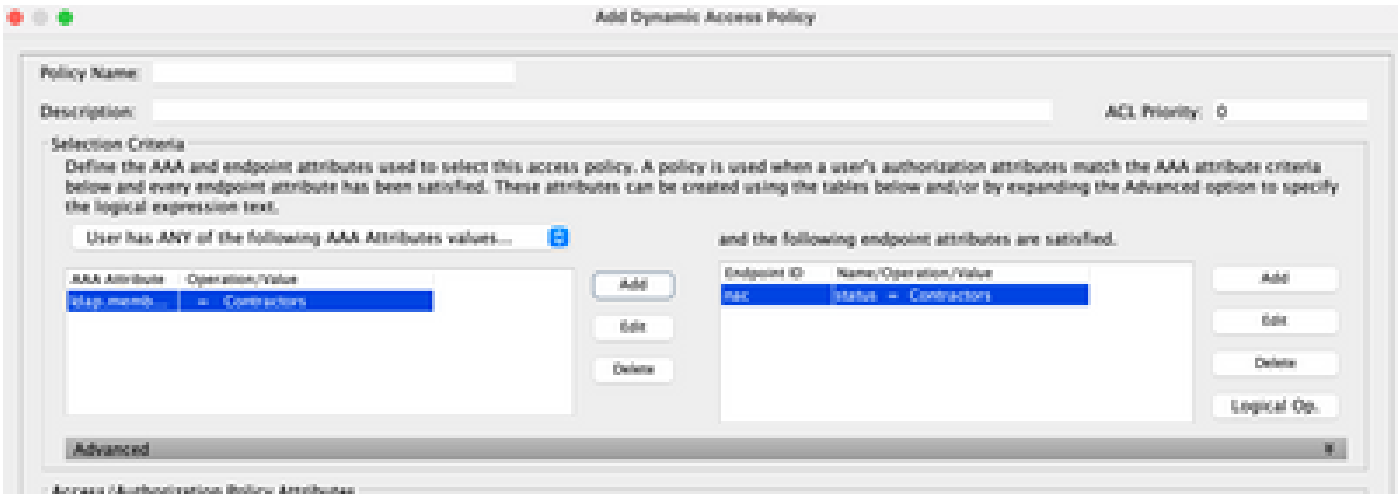


그림 6. AAA 및 엔드포인트 특성 기준 일치



AAA 및 엔드포인트 특성은 그림 6에 설명된 대로 테이블을 사용하거나 그림 7과 같이 Advanced(고급) 옵션을 확장하여 논리 식을 지정하여 생성할 수 있습니다. 현재 논리 식은 AAA 및/또는 엔드포인트 선택 논리 연산을 나타내는 EVAL(endpoint.av.McAfeeAV.exists, "EQ", "true", "string") 및 EVAL(endpoint.av.McAfeeAV.description, "EQ", "McAfee VirusScan Enterprise", "string") 등의 EVAL 함수로 구성됩니다.

논리 식은 이전에 표시된 대로 AAA 및 엔드포인트 특성 영역에서 사용할 수 없는 선택 기준을 추가해야 하는 경우 유용합니다. 예를 들어, 지정된 기준을 모두 충족하거나 하나도 충족하지 않는 AAA 특성을 사용하도록 보안 어플라이언스를 구성할 수 있지만 엔드포인트 특성은 누적되므로 모두 충족해야 합니다. 보안 어플라이언스에서 하나의 엔드포인트 특성 또는 다른 특성을 사용하게 하려면 DAP 레코드의 Advanced(고급) 섹션에서 적절한 논리 식을 만들어야 합니다.

그림 7. 고급 특성 생성을 위한 논리 식 GUI

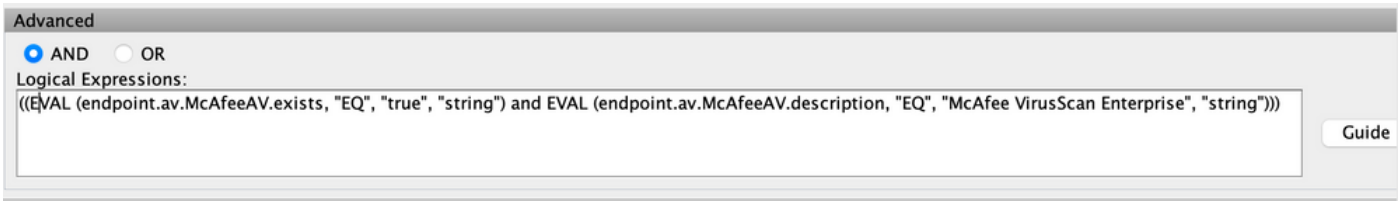
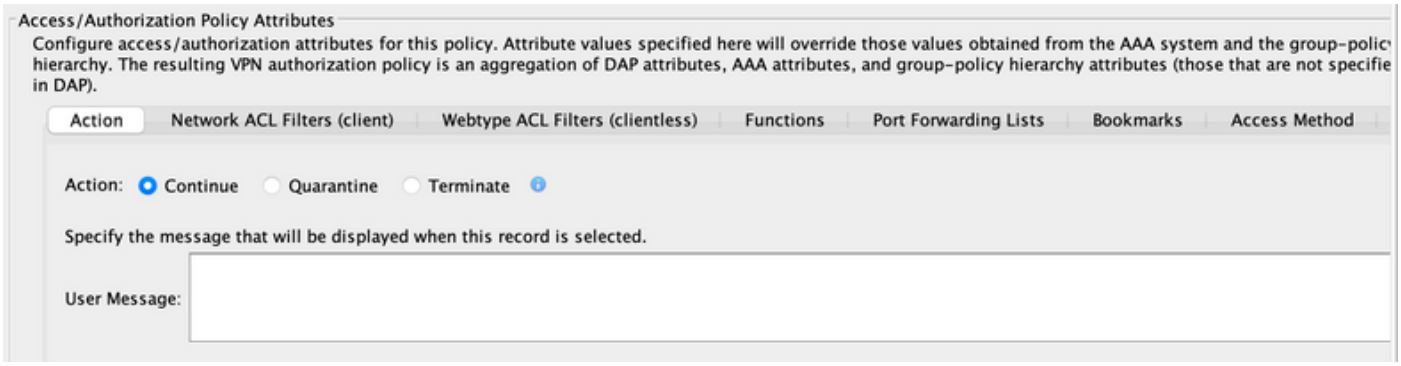


그림 8과 같은 Access Policy Attributes 섹션에서는 관리자가 특정 DAP 레코드에 대한 VPN 액세스 특성을 구성합니다. 사용자 권한 부여 특성이 AAA, 엔드포인트 및/또는 논리 식 기준과 일치하는 경우, 이 섹션에서 구성된 액세스 정책 특성 값을 적용할 수 있습니다. 여기에 지정된 특성 값은 기존 사용자, 그룹, 터널 그룹 및 기본 그룹 레코드의 특성 값을 포함하여 AAA 시스템에서 얻은 값을 재정의할 수 있습니다.

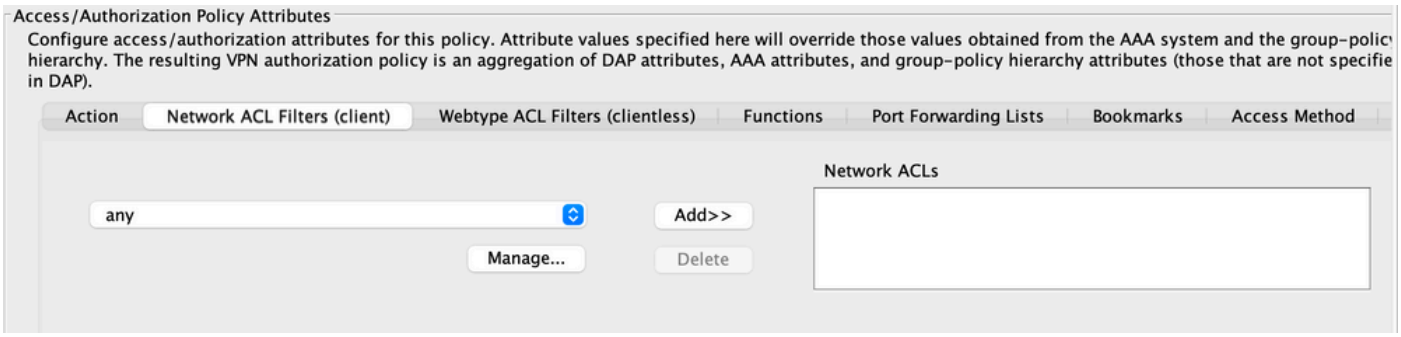
DAP 레코드에는 구성 가능한 제한된 특성 값 집합이 있습니다. 이러한 값은 그림 8~14와 같은 탭에 해당됩니다.

그림 8. 작업 — 특정 연결 또는 세션에 적용할 특수 처리를 지정합니다.



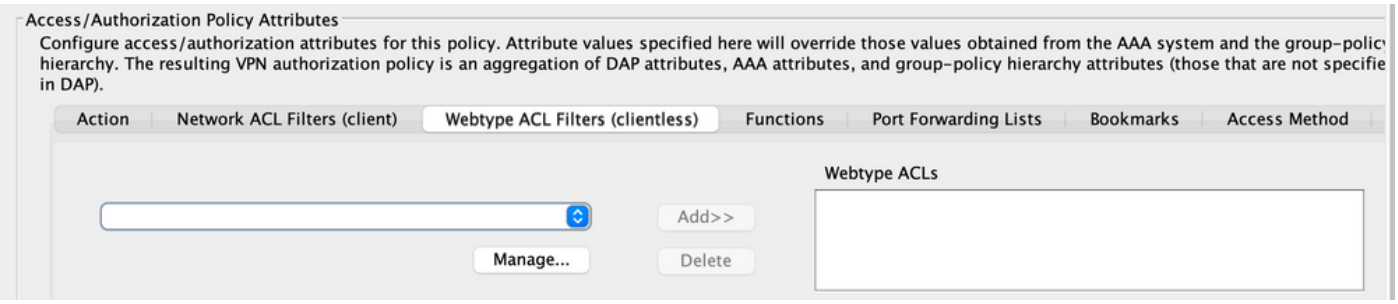
- Continue(계속) - (기본값) 액세스 정책 특성을 세션에 적용하려면 클릭합니다.
- Terminate(종료) - 세션을 종료하려면 클릭합니다.
- User Message(사용자 메시지) - 이 DAP 레코드를 선택한 경우 포털 페이지에 표시할 텍스트 메시지를 입력합니다. 최대 128자입니다. 사용자 메시지가 노란색 구형으로 표시됩니다. 사용자가 로그온하면 관심을 끌기 위해 세 번 깜박인 다음 계속 깜박입니다. 여러 DAP 레코드를 선택한 경우 각 레코드에 사용자 메시지가 있으면 모든 사용자 메시지가 표시됩니다. 또한 이러한 메시지에 올바른 HTML 태그를 사용해야 하는 URL 또는 기타 포함 텍스트를 포함할 수 있습니다.

그림 9. Network ACL Filters(네트워크 ACL 필터) 탭 — 이 DAP 레코드에 적용할 네트워크 ACL을 선택하고 구성할 수 있습니다. DAP에 대한 ACL에는 허용 규칙과 거부 규칙이 모두 포함될 수 있지만 둘 다 포함될 수는 없습니다. ACL에 허용 규칙과 거부 규칙이 모두 포함된 경우 보안 어플라이언스는 ACL 컨피그레이션을 거부합니다.



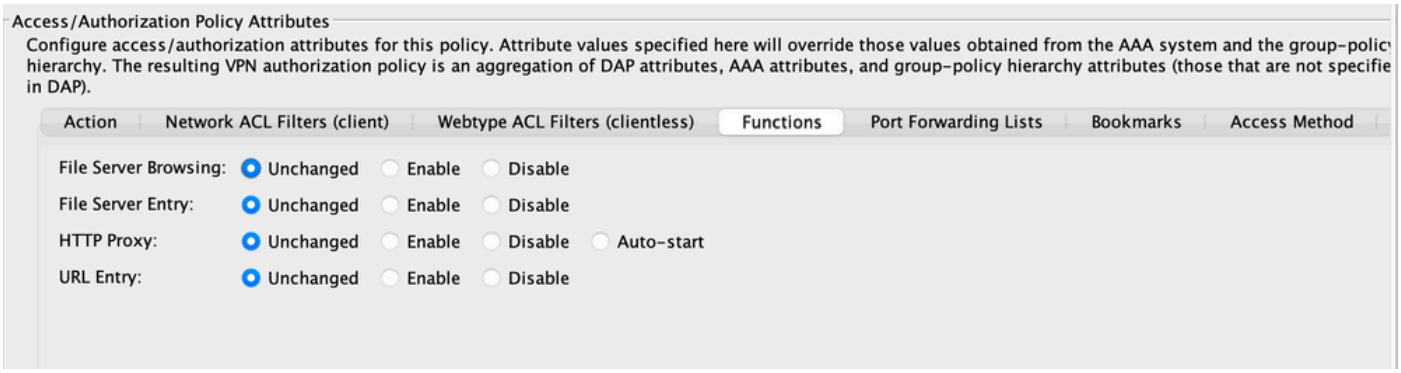
- Network ACL(네트워크 ACL) 드롭다운 상자가 이 DAP 레코드에 추가할 네트워크 ACL을 이미 구성했습니다. 모든 허용 또는 거부 규칙이 있는 ACL만 사용할 수 있으며, 여기에는 이러한 ACL만 표시됩니다.
- Manage(관리) - 네트워크 ACL을 추가, 수정 및 삭제하려면 클릭합니다.
- 네트워크 ACL은 이 DAP 레코드에 대한 네트워크 ACL을 나열합니다.
- Add(추가) - 드롭다운 상자에서 선택한 네트워크 ACL을 오른쪽에 있는 Network ACLs(네트워크 ACL) 목록에 추가하려면 클릭합니다.
- Delete(삭제) - 강조 표시된 네트워크 ACL을 Network ACLs(네트워크 ACL) 목록에서 삭제하려면 클릭합니다. ACL이 DAP 또는 다른 레코드에 할당된 경우에는 ACL을 삭제할 수 없습니다.

그림 10. Web-Type ACL Filters(웹 형식 ACL 필터) 탭 — 이 DAP 레코드에 적용할 웹 형식 ACL을 선택하고 구성할 수 있습니다. DAP에 대한 ACL은 허용 또는 거부 규칙만 포함할 수 있습니다. ACL에 허용 규칙과 거부 규칙이 모두 포함된 경우 보안 어플라이언스는 ACL 컨피그레이션을 거부합니다.



- Web-Type ACL(웹 형식 ACL) 드롭다운 상자 - 이 DAP 레코드에 추가할 이미 구성된 웹 형식 ACL을 선택합니다. 모든 허용 또는 모든 거부 규칙이 있는 ACL만 사용할 수 있으며, 여기에 표시되는 ACL은 이것뿐입니다.
- 관리... — 웹 형식 ACL을 추가, 수정 및 삭제하려면 클릭합니다.
- Web-Type ACL list - 이 DAP 레코드에 대한 웹 형식 ACL을 표시합니다.
- Add(추가) - 드롭다운 상자에서 선택한 웹 형식 ACL을 오른쪽에 있는 Web-Type ACLs(웹 형식 ACL) 목록에 추가하려면 클릭합니다.
- Delete(삭제) - Web-Type ACLs(웹 형식 ACL) 목록에서 웹 형식 ACL을 삭제하려면 클릭합니다. ACL이 DAP 또는 다른 레코드에 할당된 경우에는 ACL을 삭제할 수 없습니다.

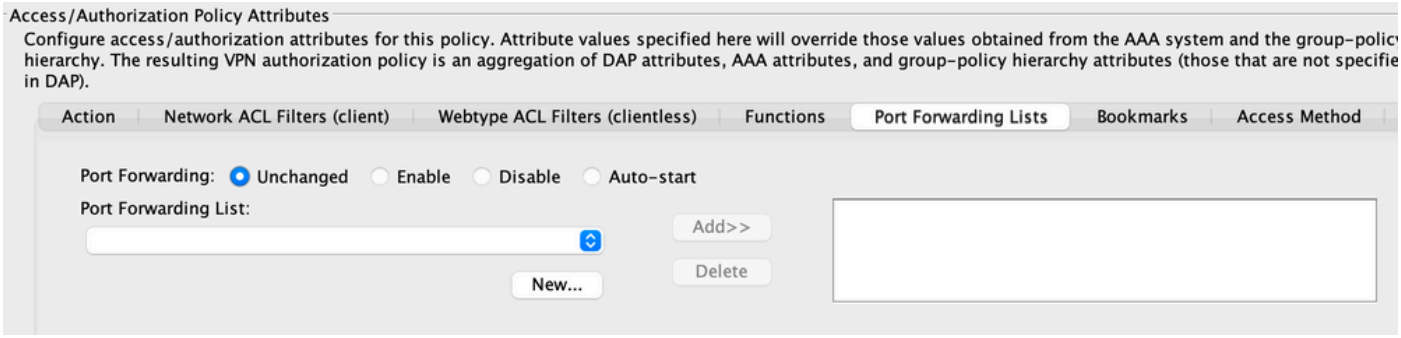
그림 11. 함수 탭 — DAP 레코드에 대한 파일 서버 항목 및 찾아보기, HTTP 프록시, URL 항목을 구성할 수 있습니다.



- File Server Browsing(파일 서버 찾아보기) - 파일 서버 또는 공유 기능에 대한 CIFS 찾아보기를 활성화하거나 비활성화합니다.
- File Server Entry(파일 서버 항목) - 사용자가 포털 페이지에서 파일 서버 경로 및 이름을 입력하는 것을 허용하거나 거부합니다. 활성화하면 포털 페이지에 파일 서버 입력란이 배치됩니다. 사용자는 Windows 파일에 대한 경로 이름을 직접 입력할 수 있습니다. 파일을 다운로드, 편집, 삭제, 이름 변경 및 이동할 수 있습니다. 또한 파일과 폴더를 추가할 수도 있습니다. 해당되는 Microsoft Windows 서버에서 사용자 액세스에 대한 공유도 구성해야 합니다. 사용자는 네트워크 요구 사항에 따라 파일에 액세스하기 전에 인증해야 할 수 있습니다.

- HTTP Proxy(HTTP 프록시) - HTTP 애플릿 프록시를 클라이언트로 전달하는 데 영향을 줍니다. 이 프록시는 Java, ActiveX, Flash와 같이 적절한 콘텐츠 변환을 방해하는 기술에 유용합니다. 보안 어플라이언스의 지속적인 사용을 보장하면서 맹글링/재작성 프로세스를 우회합니다. 전달된 프록시는 브라우저의 이전 프록시 컨피그레이션을 자동으로 수정하고 모든 HTTP 및 HTTPS 요청을 새 프록시 컨피그레이션으로 리디렉션합니다. HTML, CSS, JavaScript, VBScript, ActiveX 및 Java를 비롯한 거의 모든 클라이언트측 기술을 지원합니다. 지원하는 유일한 브라우저는 Microsoft Internet Explorer입니다.
- URL Entry(URL 입력) - 사용자가 포털 페이지에서 HTTP/HTTPS URL을 입력하는 것을 허용하거나 금지합니다. 이 기능이 활성화된 경우 사용자는 URL 입력 상자에 웹 주소를 입력하고 클라이언트리스 SSL VPN을 사용하여 해당 웹 사이트에 액세스할 수 있습니다.
- Unchanged(변경되지 않음) - (기본값) 이 세션에 적용되는 그룹 정책의 값을 사용하려면 클릭합니다.
- Enable/Disable(활성화/비활성화) - 기능을 활성화하거나 비활성화하려면 클릭합니다.
- Auto-start(자동 시작) - HTTP 프록시를 활성화하고 DAP 레코드가 이러한 기능과 연결된 애플릿을 자동으로 시작하도록 하려면 클릭합니다.

그림 12. 포트 전달 목록 탭 — 사용자 세션에 대한 포트 전달 목록을 선택하고 구성할 수 있습니다.

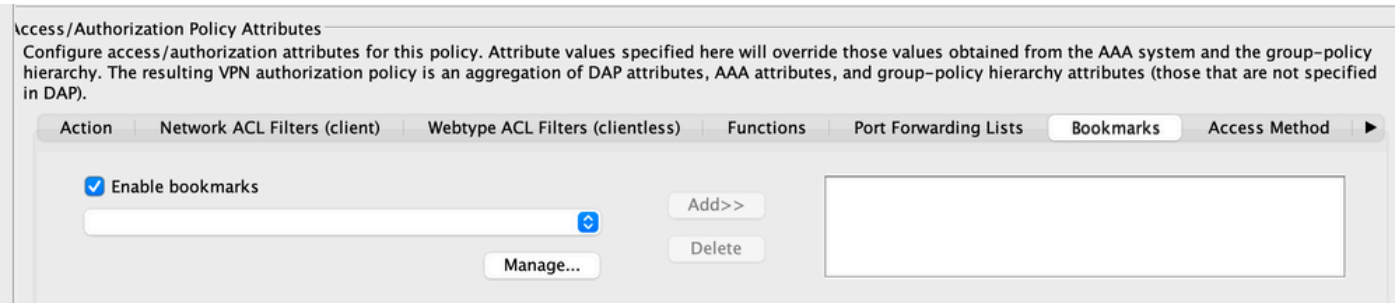


- Port Forwarding(포트 전달) - 이 DAP 레코드에 적용되는 포트 전달 목록에 대한 옵션을 선택합니다. 이 필드의 다른 특성은 Port Forwarding(포트 전달)을 Enable(활성화) 또는 Auto-start(자동 시작)로 설정한 경우에만 활성화됩니다.
- Unchanged(변경되지 않음) - 이 세션에 적용되는 그룹 정책의 값을 사용하려면 클릭합니다.
- Enable/Disable(활성화/비활성화) - 포트 전달을 활성화하거나 비활성화하려면 클릭합니다.
- Auto-start(자동 시작) - 포트 전달을 활성화하고 DAP 레코드가 해당 포트 전달 목록과 연결된 포트 전달 애플릿을 자동으로 시작하도록 하려면 클릭합니다.
- Port Forwarding List(포트 전달 목록) 드롭다운 상자 - DAP 레코드에 추가할 이미 구성된 포트 전달 목록을 선택합니다.
- New(새로 만들기) - 새 포트 전달 목록을 구성하려면 클릭합니다.
- Port Forwarding Lists(포트 전달 목록) - DAP 레코드에 대한 포트 전달 목록을 표시합니다.
- Add(추가) - 드롭다운 상자에서 선택한 포트 전달 목록을 오른쪽에 있는 Port Forwarding(포트

전달) 목록에 추가하려면 클릭합니다.

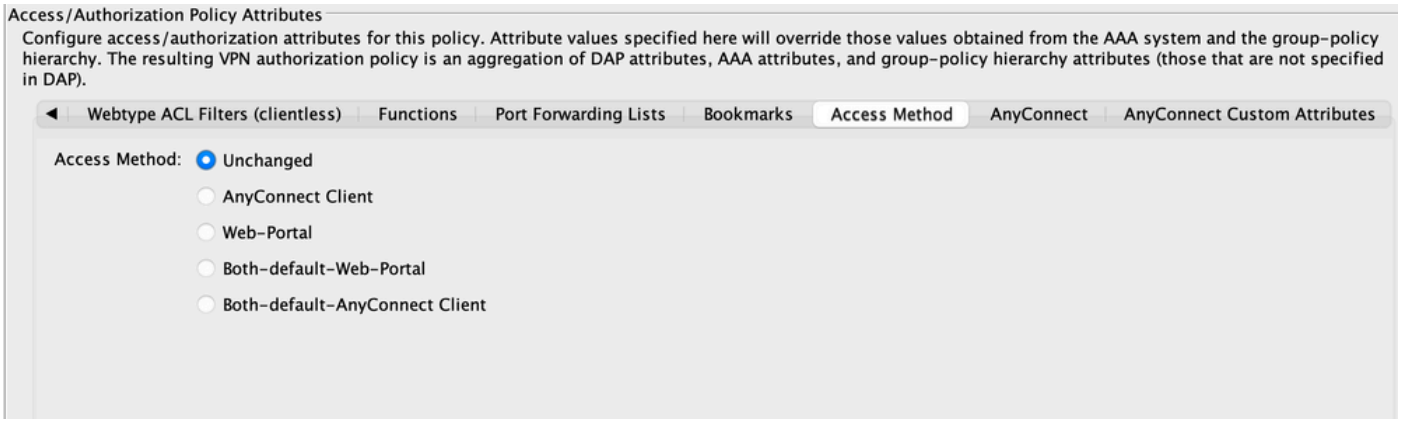
- Delete(삭제) - 선택한 포트 전달 목록을 포트 전달 목록에서 삭제하려면 클릭합니다. ACL이 DAP 또는 다른 레코드에 할당된 경우에는 ACL을 삭제할 수 없습니다.

그림 13. Bookmarks(책갈피) 탭 — 사용자 세션에 대한 책갈피/URL 목록을 선택하고 구성할 수 있습니다.



- 책갈피 사용 - 활성화하려면 누릅니다. 이 상자를 선택하지 않으면 연결에 대한 포털 페이지에 책갈피 목록이 표시되지 않습니다
- Manage(관리) - 책갈피 목록을 추가, 가져오기, 내보내기 및 삭제하려면 클릭합니다.
- Bookmarks Lists(책갈피 목록)(드롭다운) - DAP 레코드에 대한 책갈피 목록을 표시합니다.
- Add(추가) - 드롭다운 상자에서 선택한 책갈피 목록을 오른쪽에 있는 책갈피 목록 상자에 추가하려면 클릭합니다.
- 삭제(Delete) - 책갈피 목록 상자에서 선택한 책갈피 목록을 삭제하려면 클릭합니다. DAP 레코드에서 책갈피 목록을 먼저 삭제하지 않는 한 보안 어플라이언스에서 책갈피 목록을 삭제할 수 없습니다.

그림 14. Method(방법) 탭 — 허용되는 원격 액세스 유형을 구성할 수 있습니다.



- Unchanged(변경되지 않음) - 세션에 대한 그룹 정책에 설정된 현재 원격 액세스 방법을 계속 사용합니다.
- AnyConnect Client(AnyConnect 클라이언트) - Cisco AnyConnect VPN 클라이언트를 사용하여 연결합니다.

- Web Portal(웹 포털) - 클라이언트리스 VPN에 연결합니다.
- Both-default-Web-Portal(기본 웹 포털 둘 다) - 클라이언트리스 또는 AnyConnect 클라이언트를 통해 연결합니다(기본값: clientless).
- Both-default-AnyConnect Client(둘 다 기본값-AnyConnect 클라이언트) - 클라이언트리스 또는 AnyConnect 클라이언트(기본값: AnyConnect)를 통해 연결합니다.

앞에서 언급한 대로 DAP 레코드에는 제한된 기본 특성 값 집합이 있으며, 이를 수정한 경우에만 현재 AAA, 사용자, 그룹, 터널 그룹 및 기본 그룹 레코드보다 우선합니다. 스플릿 터널링 목록, 배너, 스마트 터널, 포털 사용자 지정 등과 같이 DAP 범위를 벗어나는 추가 특성 값이 필요한 경우 AAA, 사용자, 그룹, 터널 그룹 및 기본 그룹 레코드를 통해 이를 적용해야 합니다. 이 경우 이러한 특정 특성 값은 DAP를 보완할 수 있으며 재정의할 수 없습니다. 따라서 사용자는 모든 레코드에서 누적 특성 값 집합을 가져옵니다.

여러 동적 액세스 정책 집계

관리자는 여러 변수를 처리하도록 여러 DAP 레코드를 구성할 수 있습니다. 따라서 인증 사용자는 여러 DAP 레코드의 AAA 및 엔드포인트 특성 기준을 충족할 수 있습니다. 결과적으로 액세스 정책 특성은 이러한 정책 전체에서 일관되거나 충돌할 수 있습니다. 이 경우 인증된 사용자는 모든 일치하는 DAP 레코드에서 누적 결과를 얻을 수 있습니다.

여기에는 인증, 권한 부여, 사용자, 그룹, 터널 그룹 및 기본 그룹 레코드를 통해 적용되는 고유한 특성 값도 포함됩니다. 액세스 정책 특성의 누적 결과는 동적 액세스 정책을 생성합니다. 결합된 액세스 정책 특성의 예는 다음 표에 나와 있습니다. 다음 예에서는 3개의 결합된 DAP 레코드의 결과를 보여 줍니다.

표 1에 나와 있는 action 속성의 값은 Terminate 또는 Continue입니다. 선택한 DAP 레코드에 Terminate 값이 구성되어 있으면 집계된 특성 값은 Terminate이고, 선택한 모든 DAP 레코드에 Continue 값이 구성되어 있으면 Continue입니다.

표 1. 작업 특성

속성 이름	DAP#1	DAP#2	DAP#3	DAP
Action(예 1)	계속	계속	계속	계속
Action(예 2)	종료	계속	계속	종료

표 2에 나와 있는 user-message 속성은 문자열 값을 포함합니다. 집계된 특성 값은 선택한 DAP 레코드의 특성 값을 함께 연결하여 만든 라인 피드(16진수 값 0x0A)로 구분된 문자열일 수 있습니다. 결합된 문자열에서 특성 값의 순서는 중요하지 않습니다.

표 2. 사용자 메시지 특성

속성 이름	DAP#1	DAP#2	DAP#3	DAP
사용자 메시지	빠름	갈색여우	뛰어넘기	재빠른 여우가 뛰어넘다

표 3에 나와 있는 클라이언트리스 기능 활성화 특성(함수)에는 자동 시작, 활성화 또는 비활성화 값

이 포함됩니다. 선택한 DAP 레코드에 자동 시작 값이 구성된 경우 집계된 특성 값은 자동 시작이 될 수 있습니다.

집계된 특성 값은 선택한 DAP 레코드에 구성된 자동 시작 값이 없고 선택한 DAP 레코드 중 하나 이상에 Enable 값이 구성된 경우 Enabled가 될 수 있습니다.

선택한 DAP 레코드 중 하나에 자동 시작 또는 활성화 값이 구성되어 있지 않고 선택한 DAP 레코드 중 하나 이상에서 "disable" 값이 구성되어 있으면 집계된 특성 값을 비활성화할 수 있습니다.

표 3. 클라이언트리스 기능 특성 활성화(기능)

속성 이름	DAP#1	DAP#2	DAP#3	DAP
포트 포워드	사용	비활성화		사용
파일 브라우징	비활성화	사용	비활성화	사용
파일 엔트리			비활성화	비활성화
HTTP 프록시	비활성화	자동 시작	비활성화	자동 시작
URL 입력	비활성화		사용	사용

표 4에 표시된 URL 목록 및 포트 전달 특성에는 문자열 또는 쉼표로 구분된 문자열인 값이 포함됩니다. 집계된 특성 값은 선택한 DAP 레코드의 특성 값을 함께 링크할 때 생성되는 쉼표로 구분된 문자열일 수 있습니다. 결합된 문자열의 중복 특성 값은 제거할 수 있습니다. 결합된 문자열에서 특성 값이 정렬되는 방식은 중요하지 않습니다.

표 4. URL 목록 및 포트 전달 목록 특성

속성 이름	DAP#1	DAP#3	DAP#3	DAP
URL 목록	a	b,c	a	a,b,c
포트 포워드		d,e	e,f	d,e,f

Access Method 특성은 SSL VPN 연결에 허용되는 클라이언트 액세스 방법을 지정합니다. 클라이언트 액세스 방법은 AnyConnect 클라이언트 액세스 전용, 웹 포털 액세스 전용, 웹 포털 액세스를 기본값으로 하는 AnyConnect 클라이언트 또는 웹 포털 액세스 또는 AnyConnect 클라이언트 액세스를 기본값으로 하는 AnyConnect 클라이언트 또는 웹 포털 액세스일 수 있습니다. 집계된 속성 값은 표 5에 요약되어 있습니다.

표 5. 액세스 방법 속성

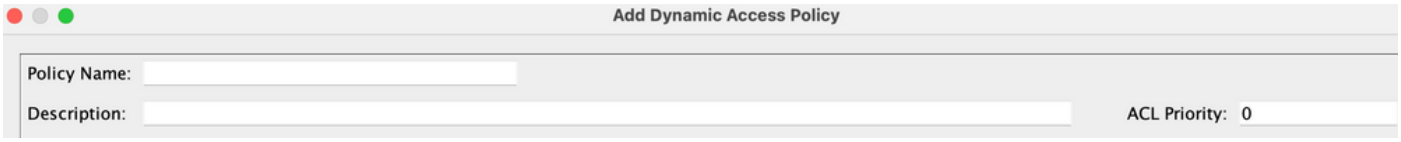
선택한 특성 값				집계 결과
AnyConnect 클라이언트	웹 포털	Both-default-Web- 포털	Both-default-AnyConnect 클라이언트	
			X	Both-default-AnyConnect 클라이언트
		X		Both-default-웹 포털
		X	X	Both-default-웹 포털
	X			웹 포털

	X		X	Both-default-AnyConnect 클라이언트
	X	X		Both-default-웹 포털
	X	X	X	Both-default-웹 포털
X				AnyConnect 클라이언트
X			X	Both-default-AnyConnect 클라이언트
X		X		Both-default-웹 포털
X		X	X	Both-default-웹 포털
X	X			Both-default-웹 포털
X	X		X	Both-default-AnyConnect 클라이언트
X	X	X		Both-default-웹 포털
X	X	X	X	Both-default-웹 포털

네트워크(방화벽) 및 웹 유형(클라이언트리스) ACL 필터 특성을 결합할 때 DAP 우선순위 및 DAP ACL은 고려해야 할 두 가지 주요 구성 요소입니다.

그림 15와 같은 Priority Attribute는 집계되지 않습니다. 보안 어플라이언스는 여러 DAP 레코드에서 네트워크 및 웹 유형 ACL을 집계할 때 이 값을 사용하여 액세스 목록을 논리적으로 시퀀싱합니다. 보안 어플라이언스는 가장 높은 우선순위 번호부터 가장 낮은 우선순위 번호까지 레코드를 정렬하며, 가장 낮은 우선순위 번호는 테이블 맨 아래에 있습니다. 예를 들어 값이 4인 DAP 레코드는 값이 2인 레코드보다 우선순위가 더 높습니다. 수동으로 정렬할 수 없습니다.

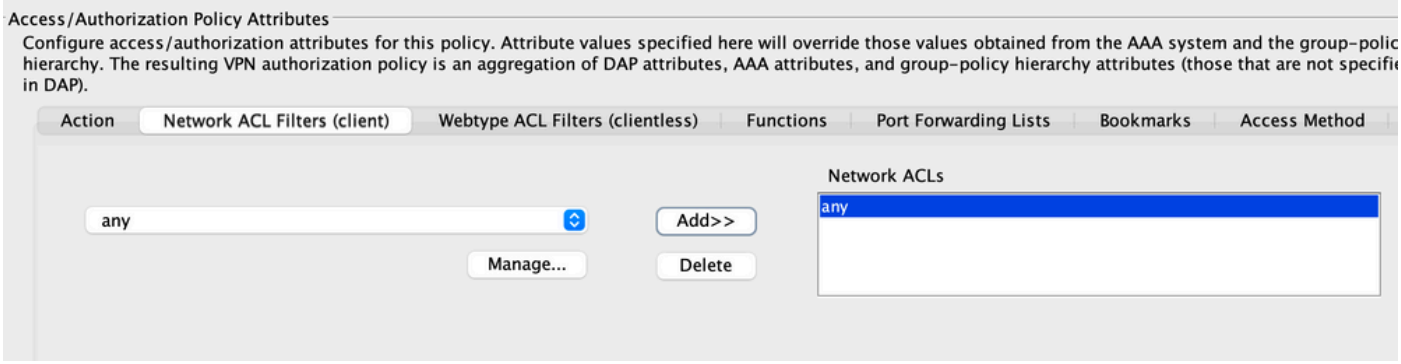
그림 15. Priority(우선순위) - DAP 레코드의 우선순위를 표시합니다.



- Policy Name(정책 이름) - DAP 레코드의 이름을 표시합니다.
- Description(설명) - DAP 레코드의 용도를 설명합니다.

DAP ACL 특성은 엄격한 허용 목록 또는 엄격한 차단 목록 ACL 모델을 준수하는 액세스 목록만 지원합니다. Allow-List ACL 모델에서 access-list 항목은 지정된 네트워크 또는 호스트에 대한 액세스를 "허용"하는 규칙을 지정합니다. Block-List ACL 모드에서 access-list 항목은 지정된 네트워크 또는 호스트에 대한 액세스를 거부하는 규칙을 지정합니다. 비준수 액세스 목록에는 허용 규칙과 거부 규칙이 혼합된 access-list 항목이 포함됩니다. 일치하지 않는 액세스 목록이 DAP 레코드에 대해 구성된 경우 관리자가 레코드를 추가하려고 할 때 구성 오류로 거부될 수 있습니다. 준수하는 액세스 목록이 DAP 레코드에 할당된 경우, 적합성 특성을 변경하는 액세스 목록 수정은 컨피그레이션 오류로 거부될 수 있습니다.

그림 16. DAP ACL - 이 DAP 레코드에 적용할 네트워크 ACL을 선택하고 구성할 수 있습니다.



여러 DAP 레코드를 선택하면 네트워크(방화벽) ACL에 지정된 액세스 목록 특성이 집계되어 DAP 방화벽 ACL에 대한 동적 액세스 목록을 생성합니다. 같은 방식으로 웹 형식(클라이언트리스) ACL에 지정된 액세스 목록 특성이 집계되어 DAP 클라이언트리스 ACL에 대한 동적 액세스 목록을 생성합니다. 다음 예에서는 특히 동적 DAP 방화벽 액세스 목록을 생성하는 방법에 중점을 둡니다. 그러나 동적 DAP 클라이언트리스 액세스 목록에서도 동일한 프로세스를 수행할 수 있습니다.

먼저 ASA는 표 6에 나와 있는 것처럼 DAP Network-ACL에 고유한 이름을 동적으로 생성합니다.

표 6. 동적 DAP 네트워크 ACL 이름

DAP 네트워크 ACL 이름
DAP-Network-ACL-X(여기서 X는 고유성을 보장하기 위해 증가할 수 있는 정수)

둘째, ASA는 표 7과 같이 선택된 DAP 레코드에서 Network-ACL 특성을 검색합니다.

표 7. 네트워크 ACL

선택한 DAP 레코드	우선순위	네트워크 ACL	네트워크 ACL 항목
DAP 1	1	101 및 102	ACL 101에는 4개의 거부 규칙이 있고 ACL 102에는 4개의 허용 규칙이 있습니다
DAP 2	2	201 및 202	ACL 201에는 3개의 허용 규칙이 있고 ACL 202에는 3개의 거부 규칙이 있습니다
DAP 3	2	101 및 102	ACL 101에는 4개의 거부 규칙이 있고 ACL 102에는 4개의 허용 규칙이 있습니다

셋째, ASA는 먼저 DAP 레코드 우선 순위 번호로 네트워크 ACL을 재정렬한 다음 2개 이상의 선택한 DAP 레코드의 우선 순위 값이 동일하면 차단 목록으로 먼저 재정렬합니다. 그런 다음 ASA는 표 8에 나와 있는 것처럼 각 Network-ACL에서 Network-ACL 엔트리를 검색할 수 있습니다.

표 8. DAP 레코드 우선 순위

네트워크 ACL	우선순위	White/Black Access-List 모델	네트워크 ACL 항목
101	2	블랙리스트	4개의 거부 규칙(DDDD)
202	2	블랙리스트	3 거부 규칙(DDD)
102	2	화이트리스트	4 허용 규칙(PPPP)

202	2	화이트리스트	3 허용 규칙(PPP)
101	1	블랙리스트	4개의 거부 규칙(DDDD)
102	1	화이트리스트	4 허용 규칙(PPPP)

마지막으로, ASA는 Network-ACL 엔트리를 동적으로 생성된 Network-ACL에 병합한 다음 표9와 같이 적용할 새 Network-ACL로 동적 Network-ACL의 이름을 반환합니다.

표 9. 동적 DAP 네트워크 ACL

DAP 네트워크 ACL 이름	네트워크 ACL 항목
DAP 네트워크 ACL-1	DDD DDD PPPP PPP DDD PPP

DAP 구현

관리자가 DAP 구현을 고려해야 하는 이유에는 여러 가지가 있습니다. 몇 가지 근본적인 이유는 엔드포인트에 대한 상태 평가가 시행될 때 및/또는 네트워크 리소스에 대한 사용자 액세스 권한을 부여할 때 보다 세부적인 AAA 또는 정책 특성을 고려해야 할 때입니다. 다음 예에서는 DAP 및 해당 구성 요소를 구성하여 연결 엔드포인트를 식별하고 다양한 네트워크 리소스에 대한 사용자 액세스를 인증할 수 있습니다.

테스트 사례 - 클라이언트가 다음과 같은 VPN 액세스 요구 사항에 대한 개념 증명을 요청했습니다.

- 직원 엔드포인트를 Managed(관리됨) 또는 Unmanaged(관리되지 않음)로 탐지하고 식별하는 기능. - 엔드포인트가 관리 대상(작업 PC)으로 식별되었지만 포스처 요건이 충족되지 않는 경우 해당 엔드포인트에 대한 액세스를 거부해야 합니다. 반면, 직원의 엔드포인트가 관리되지 않는(가정용 PC)으로 식별되면 해당 엔드포인트에 클라이언트리스 액세스 권한이 부여되어야 합니다.
- 클라이언트리스 연결이 종료될 때 세션 쿠키 및 캐시의 정리를 호출하는 기능.
- McAfee AntiVirus와 같이 관리되는 직원 엔드포인트에서 실행 중인 애플리케이션을 탐지하고 시행하는 기능. 애플리케이션이 존재하지 않는 경우, 해당 엔드포인트는 액세스가 거부되어야 합니다.
- AAA 인증을 사용하여 인증된 사용자가 액세스해야 하는 네트워크 리소스를 결정하는 기능. 보안 어플라이언스는 기본 MS LDAP 인증을 지원하고 여러 LDAP 그룹 멤버십 역할을 지원해야 합니다.
- 클라이언트/네트워크 기반 연결을 통해 연결된 경우 로컬 LAN에서 네트워크 팩스 및 프린터와 같은 네트워크 리소스에 액세스하도록 허용하는 기능.
- 계약자에게 승인된 게스트 액세스를 제공하는 기능. 계약자와 그 엔드포인트는 클라이언트리스 액세스를 받아야 하며, 애플리케이션에 대한 포털 액세스는 직원 액세스에 비해 제한되어야 합니다.

이 예에서는 클라이언트의 VPN 액세스 요구 사항을 충족하기 위해 일련의 컨피그레이션 단계를 실행할 수 있습니다. 필요한 컨피그레이션 단계가 있지만 DAP와 직접 관련이 없는 반면 다른 컨피그

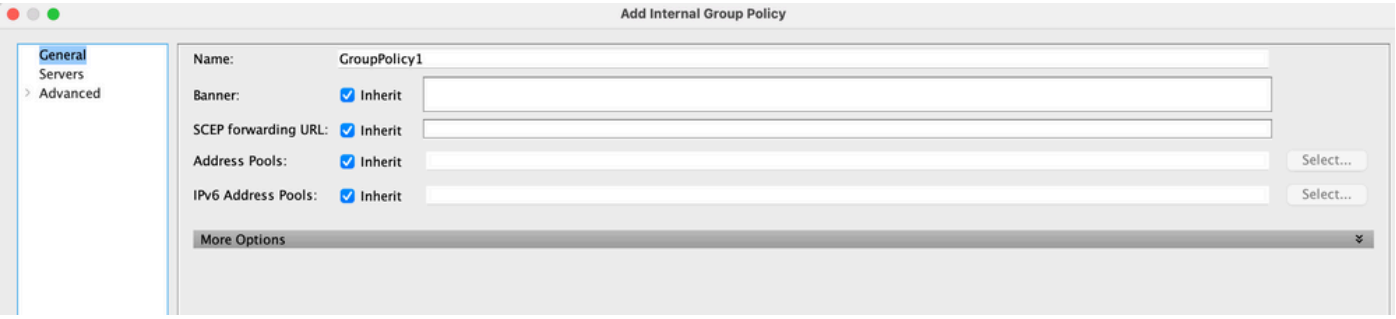
레이션은 DAP와 직접 관련이 있을 수 있습니다. ASA는 매우 동적이며 많은 네트워크 환경에 적응할 수 있습니다. 따라서 VPN 솔루션은 다양한 방법으로 정의할 수 있으며 경우에 따라 동일한 최종 솔루션을 제공합니다. 그러나 이 접근 방식은 고객의 요구와 환경에 의해 좌우됩니다.

이 문서의 특성과 정의된 클라이언트 요구 사항에 따라 ASDM(Adaptive Security Device Manager)을 사용하고 대부분의 컨피그레이션을 DAP에 집중할 수 있습니다. 그러나 DAP가 로컬 정책 특성을 보완 및/또는 재정의할 수 있는 방법을 표시하도록 로컬 그룹 정책을 구성할 수도 있습니다. 이 테스트 사례를 기반으로 LDAP 서버 그룹, 스플릿 터널링 네트워크 목록, 기본 IP 연결(IP 풀 및 DefaultDNS 서버 그룹 포함)이 미리 구성되어 있다고 가정할 수 있습니다.

그룹 정책 정의 - 이 컨피그레이션은 로컬 정책 특성을 정의하는 데 필요합니다. 여기에 정의된 일부 특성은 DAP에서 구성할 수 없습니다(예: 로컬 LAN 액세스). (이 정책은 클라이언트리스 및 클라이언트 기반 특성을 정의하는 데에도 사용할 수 있습니다.)

Configuration(컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Group Policies(그룹 정책)로 이동하고 다음과 같이 내부 그룹 정책을 추가합니다.

그림 17. Group Policy(그룹 정책) - 로컬 VPN 관련 특성을 정의합니다.

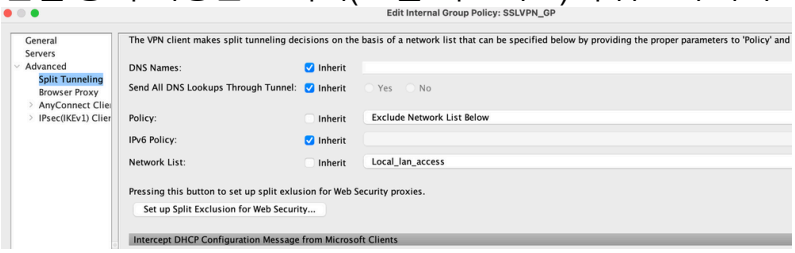


a. General(일반) 링크에서 그룹 정책의 이름SSLVPN_GP를 구성합니다.

b. 또한 General(일반) 링크에서 More Options(추가 옵션)를 클릭하고 Tunneling Protocol:Clientless SSLVPN(터널링 프로토콜:클라이언트리스 SSLVPN)만 구성합니다. 액세스 방법을 재정의하고 관리하도록 DAP를 구성할 수 있습니다.

c. Advanced(고급) > Split Tunneling(스플릿 터널링) 링크 아래에서 다음 단계를 구성합니다.

그림 18. 스플릿 터널링 - 클라이언트 연결 중에 지정된 트래픽(로컬 네트워크)이 암호화되지 않은 터널을 우회하도록 허용합니다.



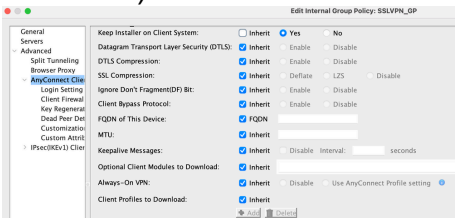
a. 정책: Inheritand(상속)의 선택을 취소하고 Exclude Network List(네트워크 목록 제외)를 선택합니다.

b. 네트워크 목록: 상속을 취소하고 목록 이름 Local_Lan_Access를 선택합니다. (사전 구

성되어 있다고 가정합니다.)

d. Advanced(고급) > ANYCONNECT Client(ANYCONNECT 클라이언트) 링크에서 다음 단계를 구성합니다.

그림 19. SSL VPN Client Installer(SSL VPN 클라이언트 설치 프로그램) - VPN 종료 시 SSL 클라이언트를 엔드포인트에 유지하거나 제거할 수 있습니다.



e. Keep Installer on Client System(클라이언트 시스템에서 설치 프로그램 유지): Inheritt(상속)의 선택을 취소한 다음 Yes(예)를 선택합니다.

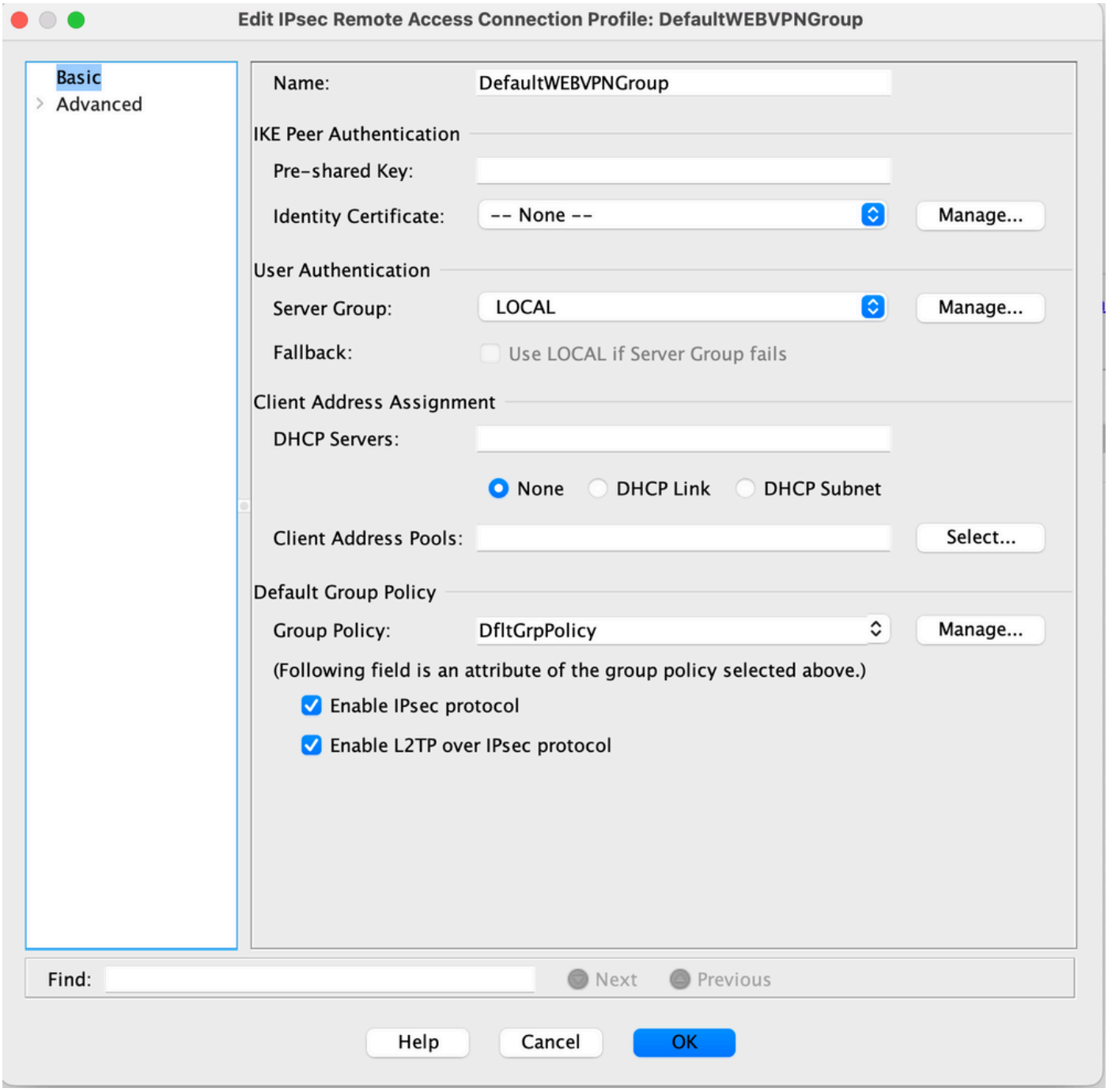
f. 확인 후 적용을 클릭합니다.

g. 컨피그레이션 변경 사항을 적용합니다.

연결 프로파일 정의 - 이 컨피그레이션은 AAA 인증 방법(예: LDAP)을 정의하고 이 연결 프로파일에 이전에 구성된 그룹 정책(SSLVPN_GP)을 적용하는 데 필요합니다. 이 연결 프로파일을 통해 연결하는 사용자는 여기에 정의된 특성뿐만 아니라 SSLVPN_GP 그룹 정책에 정의된 특성도 적용 받을 수 있습니다. 이 프로파일은 클라이언트리스 및 클라이언트 기반 특성을 모두 정의하는 데에도 사용할 수 있습니다.

Configuration(컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) >IPsec Remote Access Connection Profile(IPsec 원격 액세스 연결 프로파일)로 이동하여 다음을 구성합니다.

그림 20. 연결 프로파일 — 로컬 VPN 관련 특성을 정의합니다.



a. Connection Profiles(연결 프로파일) 섹션에서 DefaultWEBVPNGroup을 편집하고 Basic(기본) 링크에서 다음 단계를 구성합니다.

   a. 인증—방법:AAA

   b. Authentication(인증) - AAA 서버 그룹:LDAP(미리 구성된 것으로 가정)

   c. Client Address Assignment(클라이언트 주소 할당) - 클라이언트 주소 풀:IP_Pool(미리 구성된 것으로 가정)

   d. 기본 그룹 정책 - 그룹 정책: SelectSSLVPN_GP

b. 컨피그레이션 변경 사항을 적용합니다.

SSL VPN 연결을 위한 IP 인터페이스 정의 - 이 컨피그레이션은 지정된 인터페이스에서 클라이언트

및 클라이언트리스 SSL 연결을 종료하는 데 필요합니다.

인터페이스에서 클라이언트/네트워크 액세스를 활성화하기 전에 먼저 SSL VPN 클라이언트 이미지를 정의해야 합니다.

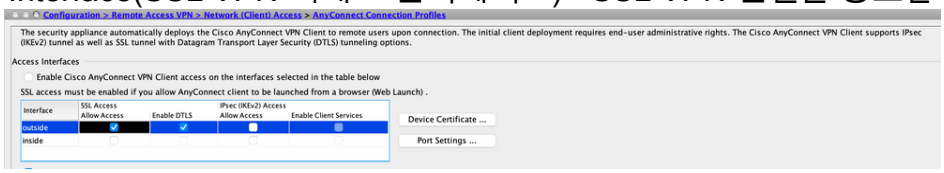
1. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client)Access(네트워크(클라이언트)액세스) > Anyconnect Client Software(Anyconnect 클라이언트 소프트웨어)로 이동하고 다음 이미지인 ASA Flash 파일 시스템의 SSL VPN 클라이언트 이미지를 추가합니다. (이 이미지는 CCO에서 다운로드할 수 있습니다. https://www.cisco.com)

   그림 21. SSL VPN Client Image Install(SSL VPN 클라이언트 이미지 설치) - 엔드포인트를 연결하기 위해 푸시할 AnyConnect 클라이언트 이미지를 정의합니다. 

   a. anyconnect mac-4.x.xxx-k9.pkg

   b. OK,OK다시, Apply를 차례로 클릭합니다.

2. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트)액세스) > AnyConnect Connection Profiles(AnyConnect 연결 프로파일)로 이동하고 다음 단계를 사용하여 이 기능을 활성화합니다.

   그림 22. SSL VPN Access Interface(SSL VPN 액세스 인터페이스) - SSL VPN 연결을 종료할 인터페이스를 정의합니다. 

   a. Access Interface(액세스 인터페이스) 섹션에서 아래 표에 선택된 인터페이스에서 Cisco AnyConnect VPN Client 또는 레거시 SSL VPN Client 액세스를 활성화합니다.

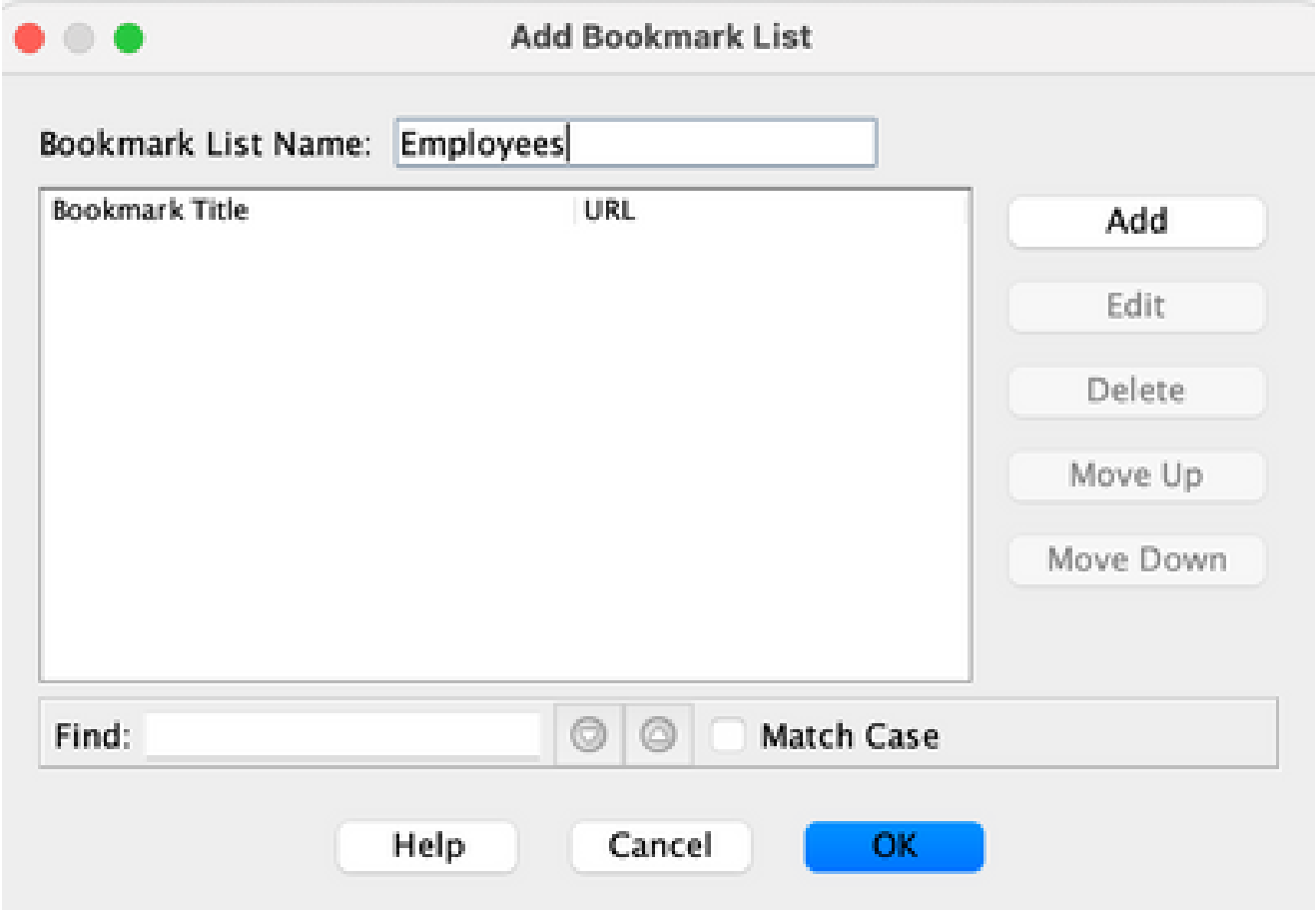
   b. 또한 Access Interfaces(액세스 인터페이스) 섹션에서 외부 인터페이스의 Allow Access(액세스 허용)를 선택합니다. 이 컨피그레이션은 외부 인터페이스에서 SSL VPN 클라이언트리스 액세스를 활성화할 수도 있습니다.

   c. 적용을 클릭합니다.

클라이언트리스 액세스에 대한 책갈피 목록(URL 목록) 정의 - 이 구성은 포털에 게시할 웹 기반 응용 프로그램을 정의하는 데 필요합니다. 직원용 URL 목록과 계약자용 URL 목록을 2개 정의할 수 있습니다.

1. Configuration(컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Portal(포털) > Bookmarks(책갈피)로 이동하여+ Add(추가)를 클릭하고 다음 단계를 구성합니다.

   그림 23. Bookmark List(책갈피 목록) - 웹 포털에서 게시하고 액세스할 URL을 정의합니다. (직원 액세스를 위해 사용자 지정됨).



a. Bookmark List Name(책갈피 목록 이름):Employees(직원)를 클릭한 다음 Add(추가)를 클릭합니다.

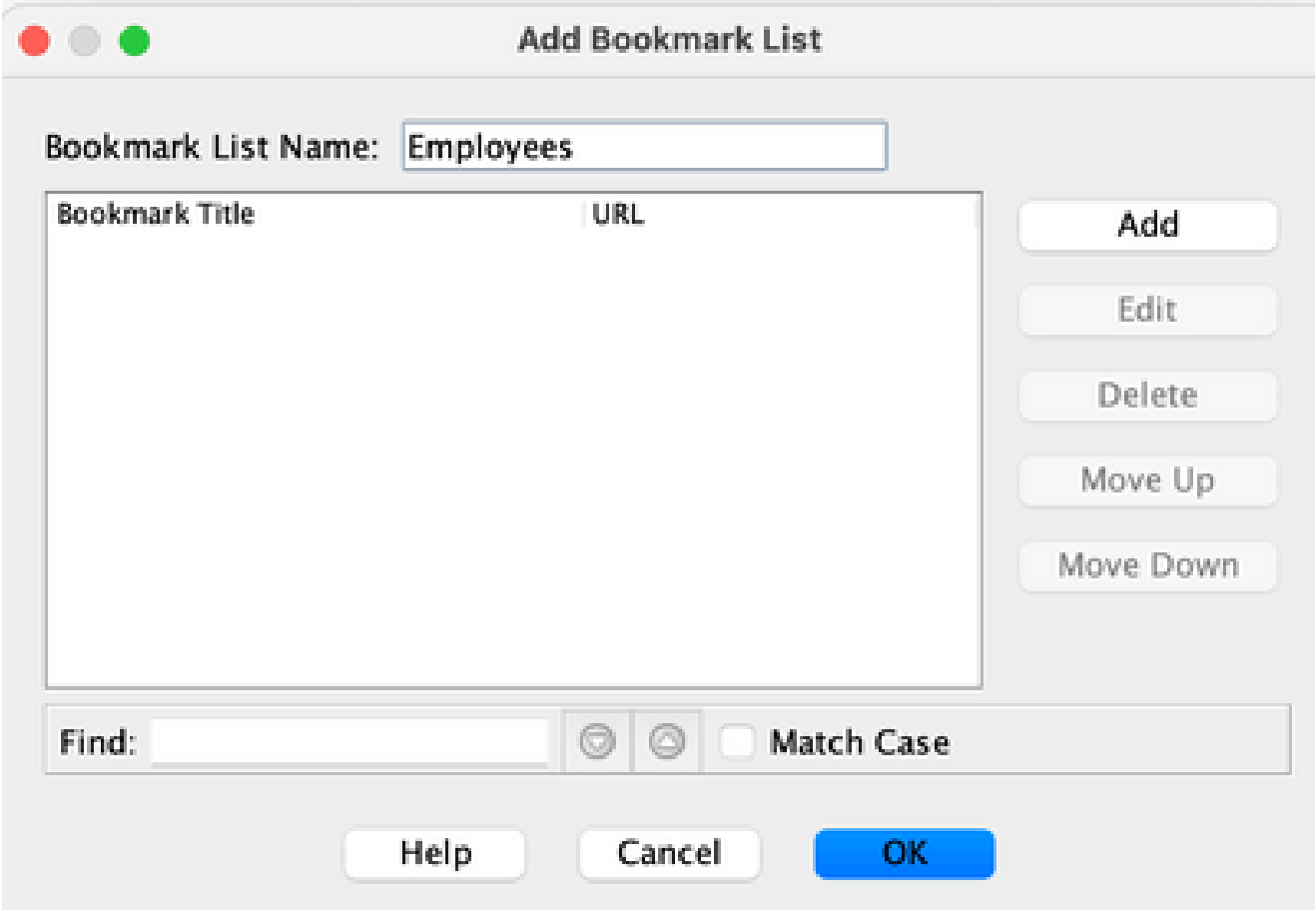
b. 책갈피 제목:회사 인트라넷

c. URL 값: https://company.resource.com

- OK(확인)를 클릭한 다음 OK(확인)를 다시 클릭합니다.

- Add**(추가)**를 클릭하고 다음과 같이 두 번째 책갈피 목록(URL 목록)을 구성합니다.

그림 24. Bookmark List(책갈피 목록) - 게스트 액세스를 위해 사용자 지정됩니다.



a.

Bookmark List Name:Contractors(책갈피 목록 이름:**계약업체)**를 선택한 다음 Add(추가)**를 클릭합니다**.

b.

책갈피 제목:**게스트 액세스**

c.

URL 값: https://company.contractors.com

-

OK(확인)를 클릭한 다음 OK(확인)를 다시 클릭합니다.

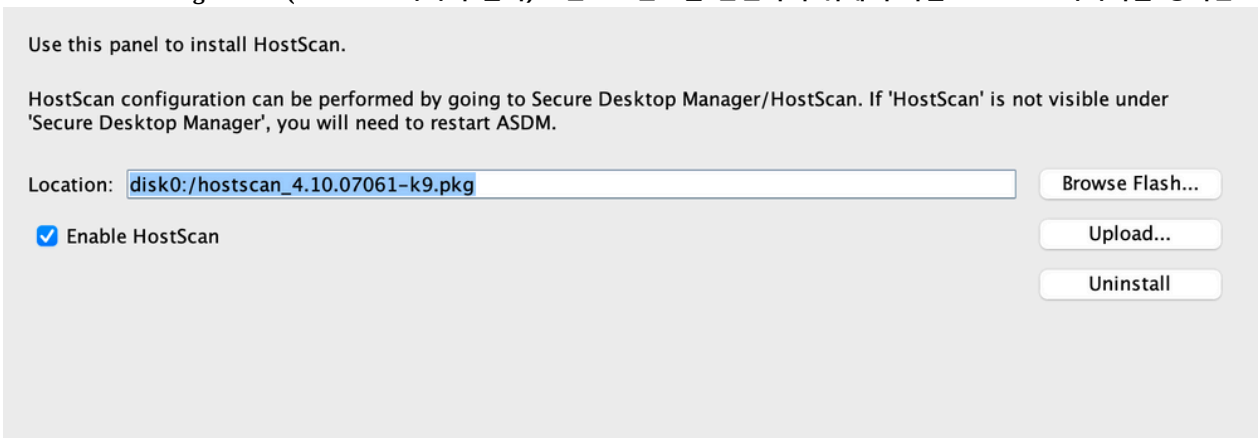
-

적용을 클릭합니다.

Hostscan 구성:

- Configuration(**컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > Secure Desktop Manager(Secure Desktop 관리자) > HostScan Image(HostScan 이미지)**로 이동하고 다음 단계를 구성합니다.

그림 25. HostScan Image Install(HostScan 이미지 설치) - 엔드포인트를 연결하기 위해 푸시할 HostScan 이미지를 정의합니다.



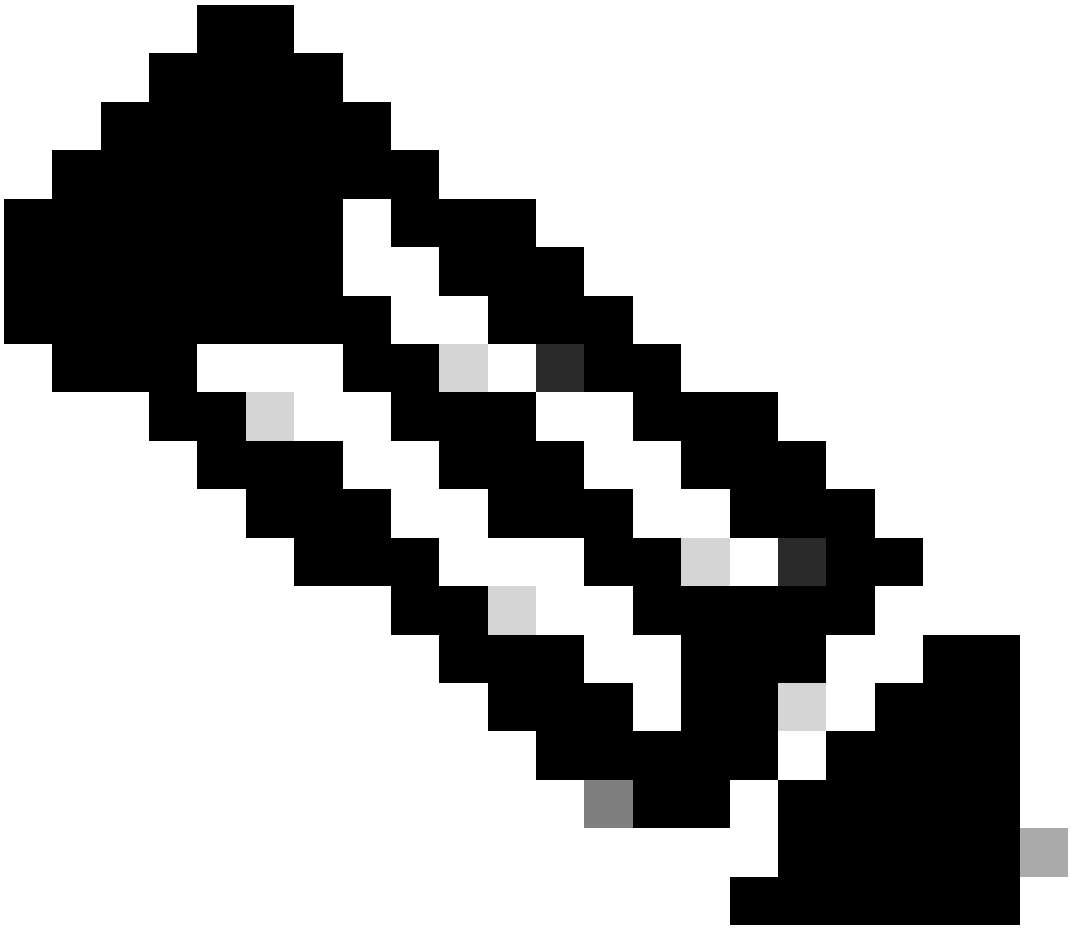
a. ASA 플래시 파일 시스템에서 **disk0:/hostscan_4.xx.xxxxx-k9.**pkgimage를 설치합니다.

b. **Enable HostScan을 선택합니다**.

c. **적용을 클릭합니다**.

동적 액세스 정책 — 이 컨피그레이션은 정의된 AAA 및/또는 엔드포인트 평가 기준에 따라 연결된 사용자 및 엔드포인트를 검증하는 데 필요합니다. DAP 레코드의 정의된 조건이 충족되면 연결 사용자에게 해당 DAP 레코드 또는 레코드와 연결된 네트워크 리소스에 대한 액세스 권한을 부여할 수 있습니다. 인증 프로세스 중에 DAP 권한 부여가 실행됩니다.

엔드포인트가 구성된 동적 액세스 정책과 일치하지 않는 경우와 같이 SSL VPN 연결이 기본 경우에 종료될 수 있도록 하려면 다음 단계를 통해 이를 구성할 수 있습니다.

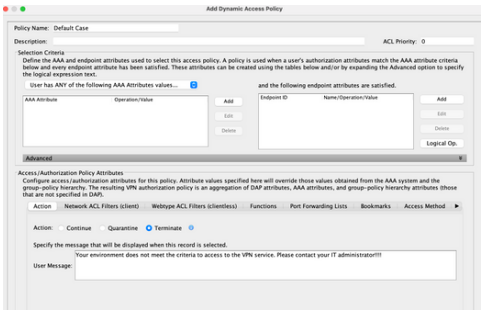


참고: 처음 동적 액세스 정책을 구성할 때 DAP 구성 파일(DAP.XML)이 없음을 나타내는 DAP.xml 오류 메시지가 표시됩니다. 초기 DAP 컨피그레이션을 수정한 후 저장하면 이 메시지가 더 이상 표시되지 않습니다.

•

Configuration(**컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Dynamic Access Policies(동적 액세스 정책)**로 이동하고 다음 단계를 구성합니다.

그림 30. Default Dynamic Access Policy(기본 동적 액세스 정책) - 일치하는 사전 정의된 DAP 레코드가 없는 경우 이 DAP



레코드를 적용할 수 있습니다. 따라서 SSL VPN 액세스를 거부할 수 있습니다.

a.

DfltAccessPolicy를 편집하고 Action을 Terminate**로 설정합니다**.

b.

확인을 클릭합니다.

•

다음과 같이 이름이 Managed_**Endpoints인** 새 동적 액세스 정책을 추가합니다.

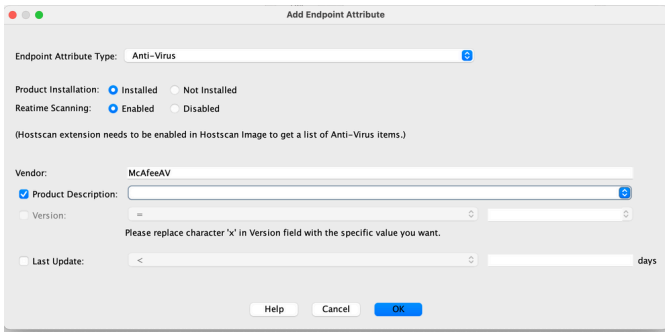
a.

설명:**직원 클라이언트 액세스**

b.

그림 31과 같이 엔드포인트 특성 유형(Anti-Virus)을 추가합니다. 완료되면 확인을 클릭합니다.

그림 31. DAP Endpoint Attribute(DAP 엔드포인트 특성) - 고급 엔드포인트 평가 AntiVirus를 클라이언트/네트워



크 액세스에 대한 DAP 기준으로 사용할 수 있습니다.

c.

이전 이미지에 표시된 대로 드롭다운 목록의 AAA Attribute 섹션에서 을 선택합니다User has ALL of the following AAA Attributes Values.

-

그림 33 및 34와 같이 AAA Attribute Type(LDAP)을 추가합니다(AAA Attribute(AAA 특성) 상자 오른쪽에 위치). 완료되면 확인을 클릭합니다.

그림 33. DAP AAA Attribute(DAP AAA 특성) - AAA 그룹 멤버십을 DAP 기준으로 사용하여 직원을 식별할 수 있습니다.

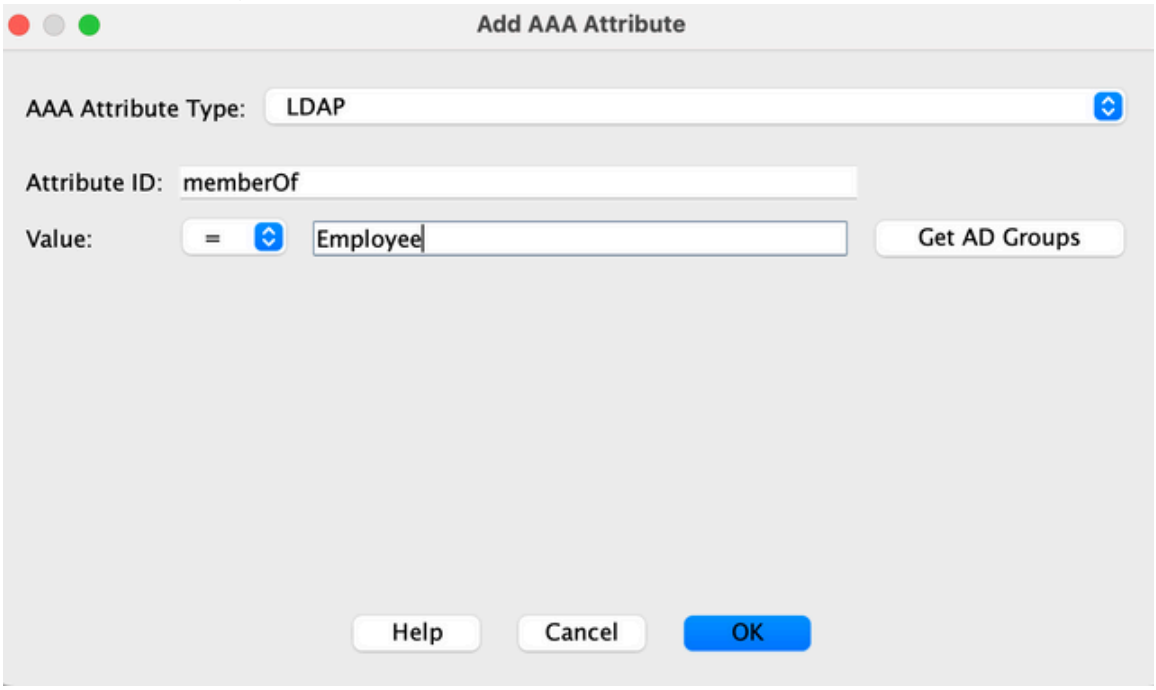
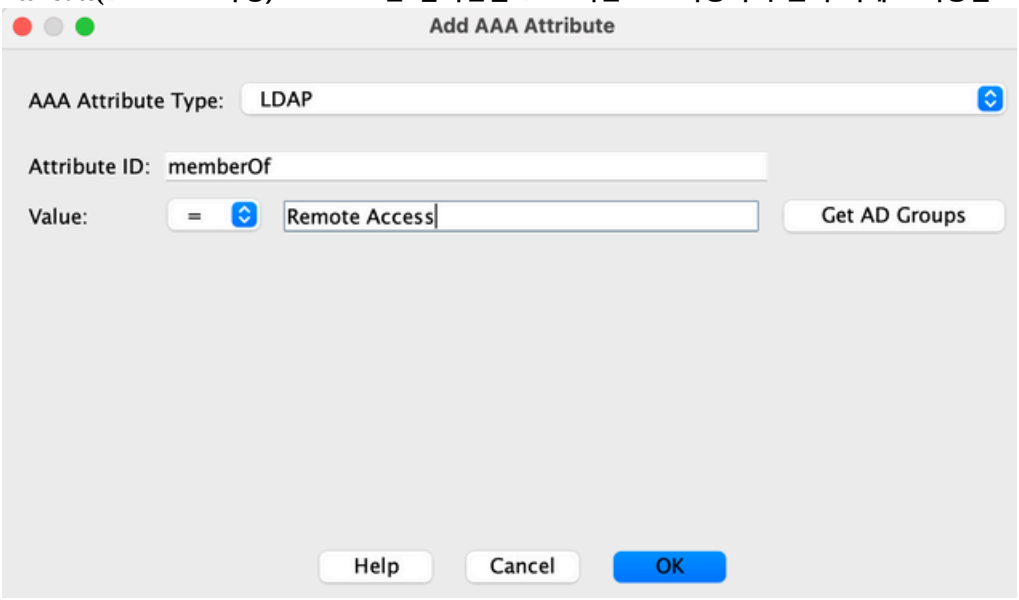


그림 34. DAP AAA Attribute(DAP AAA 특성) - AAA 그룹 멤버십을 DAP 기준으로 사용하여 원격 액세스 기능을 허용할 수 있습니다.



-

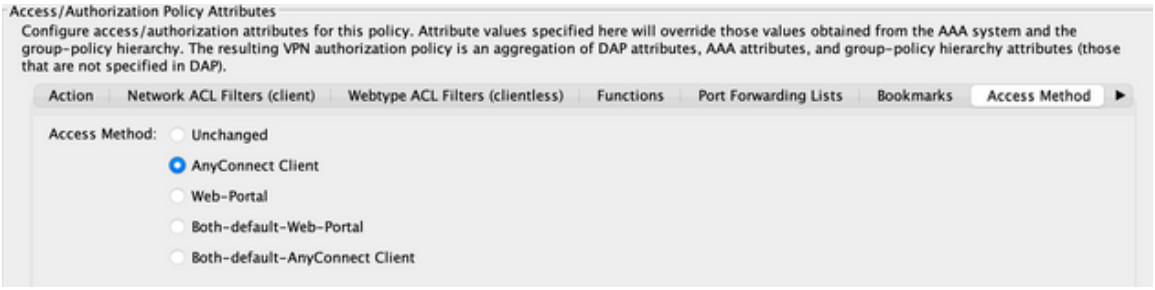
그림 35와 같이 Action(작업) 탭에서 Action(작업)이 **Continue(계속)**로 설정되어 있는지 확인합니다.

그림 35. Action(작업) 탭 - 이 컨피그레이션은 특정 연결 또는 세션에 대한 특수 처리를 정의하는 데 필요합니다.

DAP 레코드가 일치하고 Action(작업)이 Terminate(종료)로 설정된 경우 VPN 액세스가 거부될 수 있습니다.

- 그림 36과 같이 Access Method(액세스 방법) 탭에서 Access **Method(액세스 방법)**AnyConnect Client(AnyConnect 클라이언트)를 선택합니다.

그림 36. Access Method(액세스 방법) 탭 - 이 컨피그레이션은 SSL VPN 클라이언트 연결 유형을 정의하는 데 필요합니다.



- **확인**을 **클릭한 다음 적용**을 **클릭합니다**.

- 다음과 같이 이름이 Unmanaged_**Endpoints인** 두 번째 동적 액세스 정책을 추가합니다.

a. 설명: **직원 클라이언트리스 액세스**.

b. AAA Attribute Section(AAA 특성 섹션)의 이전 이미지 드롭다운 목록에서 을 선택합니다User has ALL of the following AAA Attributes Values.

- 그림 38 및 39와 같이 AAA 특성 유형(LDAP)을 추가합니다(AAA 특성 유형 오른쪽에 위치). 완료되면 확인을 클릭합니다.

그림 38. DAP AAA Attribute(DAP AAA 특성) - AAA 그룹 멤버십을 DAP 기준으로 사용하여 직원을 식별할 수 있습니다.

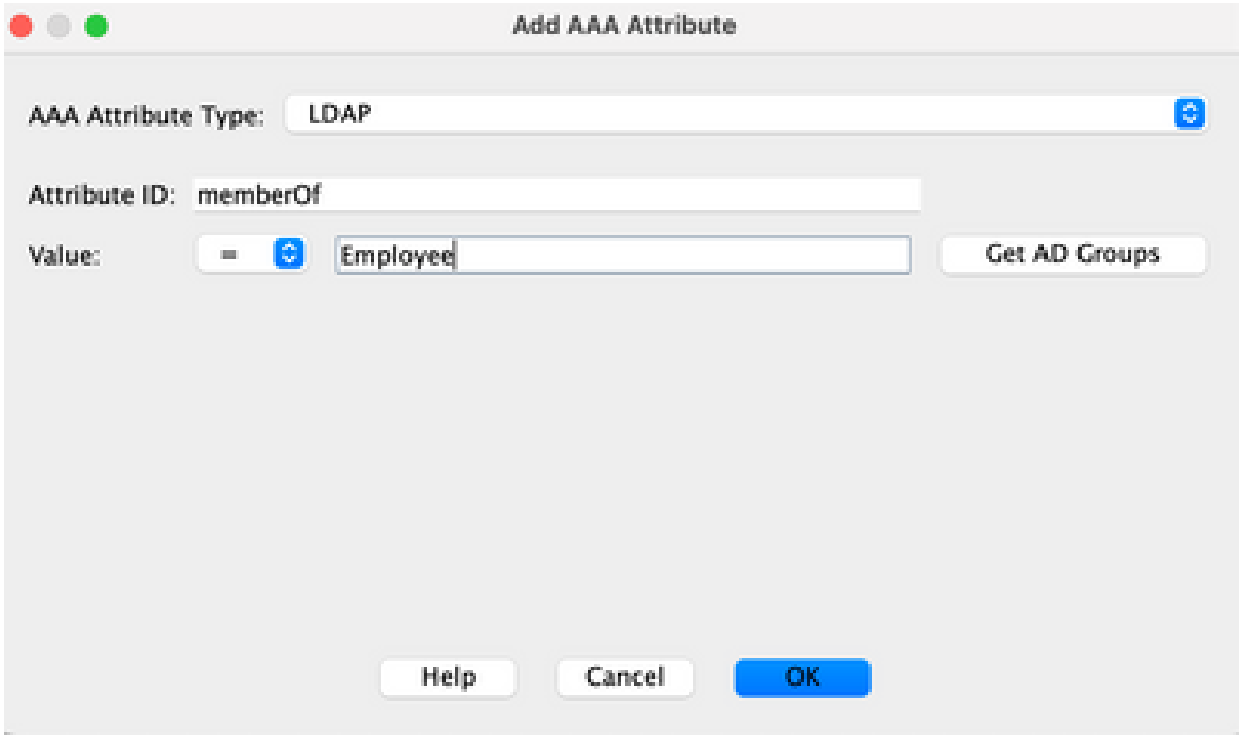
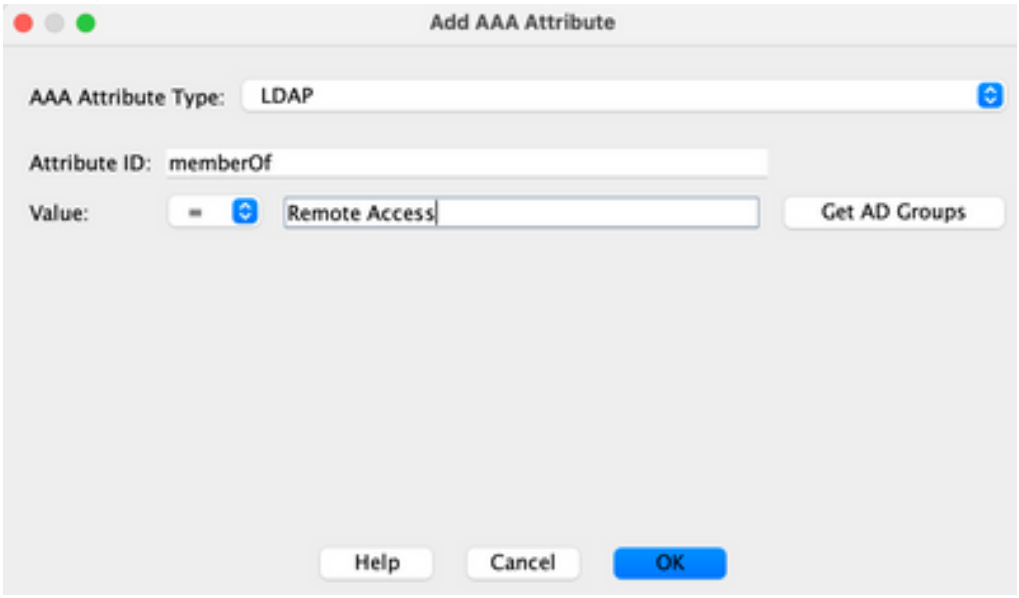


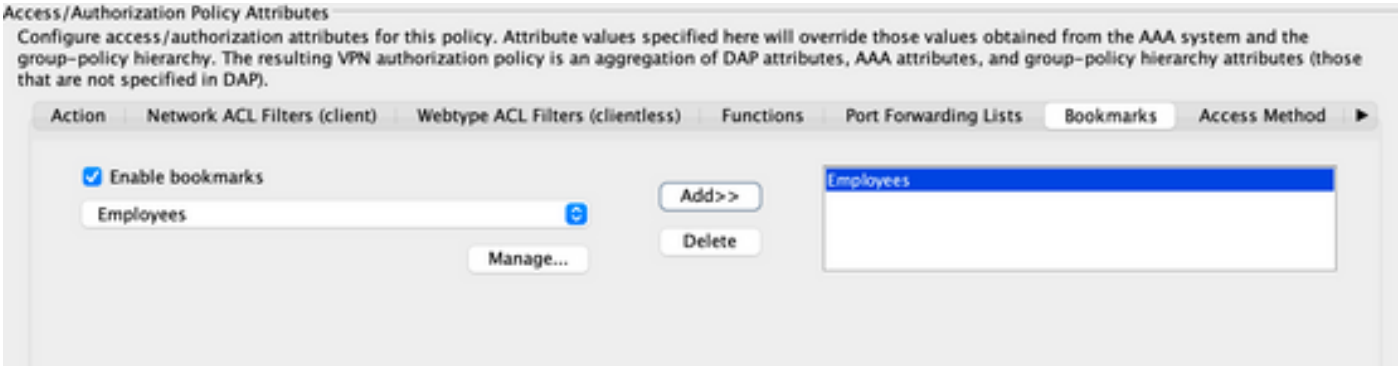
그림 39. DAP AAA Attribute(DAP AAA 특성) - AAA 그룹 멤버십을 DAP 기준으로 사용하여 원격 액세스 기능을 허용할 수 있습니다.



- Action(작업) 탭에서 Action(작업)이 Continue(계속)**로 설정되어 있는지 확인합니다.** (그림 35)

- Bookmarks(책갈피) 탭의 드롭다운 목록에서 name(직원)Employees(직원)를 선택한 다음 Add(추가)**를 클릭합니다.** 또한 그림 40과 같이 Enable bookmarks(책갈피 활성화)가 선택되어 있는지 확인합니다.

그림 40. Bookmarks(책갈피) 탭 - 사용자 세션에 대한 URL 목록을 선택하고 구성할 수 있습니다.



-

  a.

  Access Method(액세스 방법) 탭에서 Access Method Web Portal(액세스 방법 **웹 포털)을 선택합니다**. (그림 36)

- **확인**을 **클릭한 다음 적용**을 **클릭합니다**.

1. 계약자는 DAP AAA 특성에서만 식별할 수 있습니다. 따라서 4단계에서 엔드포인트 특성 유형(정책)을 구성할 수 없습니다. 이 접근 방식은 DAP 내에서 다기능성을 보여주는 데 그칩니다.

3. 다음을 사용하여 세 번째 동적 액세스 정책인 **Guest_Access**를 추가합니다.

-

  설명: **게스트 클라이언트리스 액세스**.

-

  Endpoint Attribute(엔드포인트 특성) 상자의 오른쪽에 있는 Endpoint Attribute Type(Policy)을 그림 37과 같이 추가합니다. 완료되면 확인을 클릭합니다.

-

  그림 40의 AAA Attribute(AAA 특성) 섹션에 있는 드롭다운 목록에서 을 선택합니다User has ALL of the following AAA Attributes Values.

-

그림 41 및 42와 같이 AAA Attribute Type(LDAP)을 추가합니다(AAA Attribute(AAA 특성) 상자 오른쪽에 위치). 완료되면 확인을 클릭합니다.

그림 41. DAP AAA 특성 - AAA 그룹 멤버십을 DAP 기준으로 사용하여 계약자를 식별할 수 있습니다

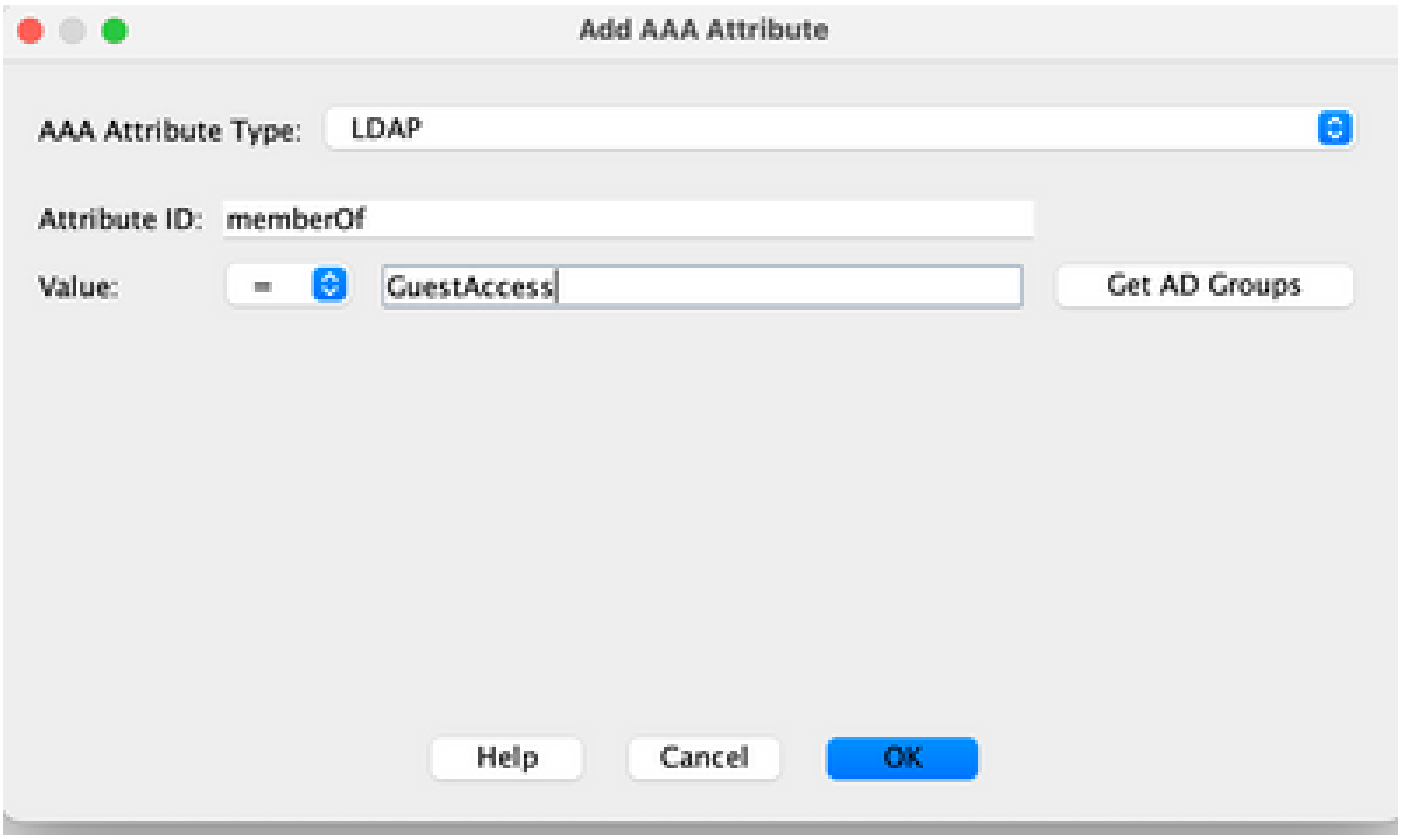
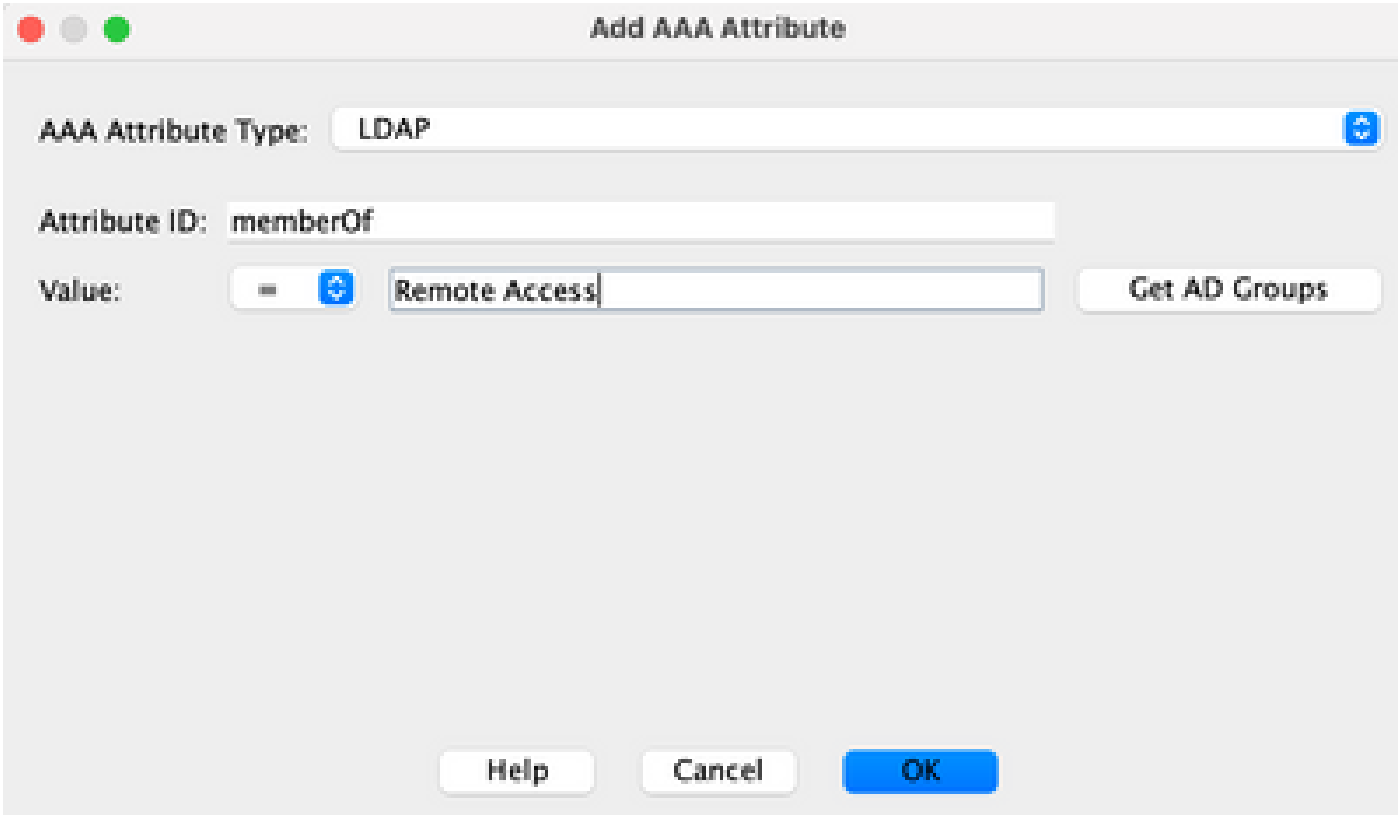


그림 42. DAP AAA Attribute(DAP AAA 특성) - AAA 그룹 멤버십을 DAP 기준으로 사용하여 원격 액세스 기능을 허용할 수 있습니다



-

  a.

  Action(작업) 탭에서 Action(작업)이 Continue(계속)로 설정되어 있는지 **확인합니다**. (그림 35)

  b.

  Bookmarks(책갈피) 탭의 드롭다운에서 **Contractors**(계약자)라는 목록 이름을 선택한 다음 Add(추가)를 클릭합니다. 또한 Enable bookmarks(책갈피 활성화)**가** 선택되어 있는지 확인합니다. (그림 40 참조)

  c.

  Access Method(액세스 방법) 탭에서 Access Method Web Portal(액세스 방법 웹 포털)을 선택합니다. (그림 36)

  d.

  OK(**확인**)를 클릭한 다음 Apply(**적용)를 클릭합니다**.

결론

이 예에서 언급한 클라이언트 원격 액세스 SSL VPN 요구 사항에 따라 이 솔루션은 클라이언트 원격 액세스 VPN 요구 사항을 충족합니다.

통합의 진화하고 동적인 VPN 환경을 통해 동적 액세스 정책은 자주 변경되는 인터넷 구성, 각 사용자가 조직 내에서 사용할 수 있는 다양한 역할, 서로 다른 구성 및 보안 수준을 가진 관리되고 관리되지 않는 원격 액세스 사이트의 로그인에 맞게 조정 및 확장될 수 있습니다.

동적 액세스 정책은 Advanced Endpoint Assessment, Host Scan, Secure Desktop, AAA 및 Local Access Policies와 같은 검증되고 새로운 레거시 기술로 보완됩니다. 따라서 조직은 모든 위치에서 모든 네트워크 리소스에 대한 보안 VPN 액세스를 자신 있게 제공할 수 있습니다.

관련 정보

- **Cisco 기술 지원 및 다운로드**

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.