Bereitstellung von dynamischen ASA 9.x-Zugriffsrichtlinien (DAP)

Inhalt

Einleitung

In diesem Dokument werden die Bereitstellung, die Funktionen und die Nutzung von dynamischen Zugriffsrichtlinien (Dynamic Access Policies, DAP) der ASA 9.x beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie folgende Themen kennen:

- VPN-Gateways (Virtual Private Network)
- Dynamic Access Policies (DAP)

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

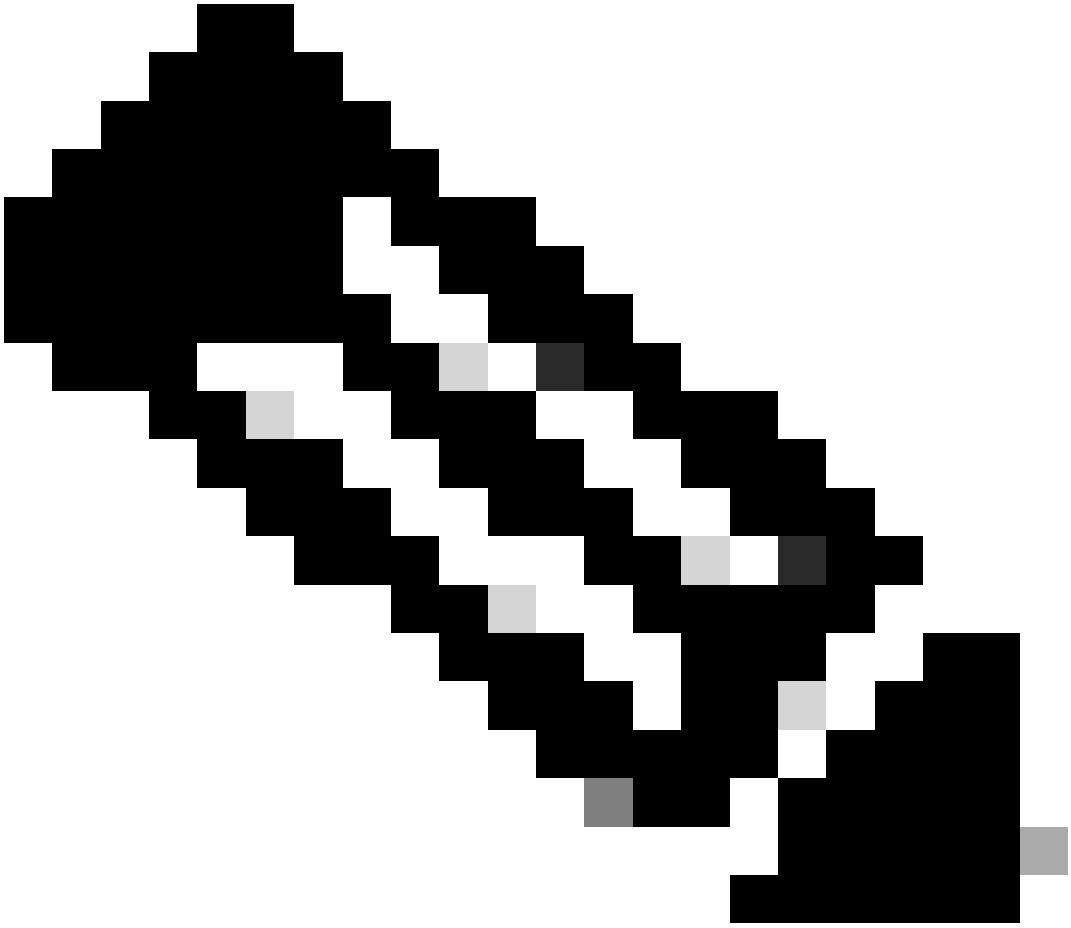
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

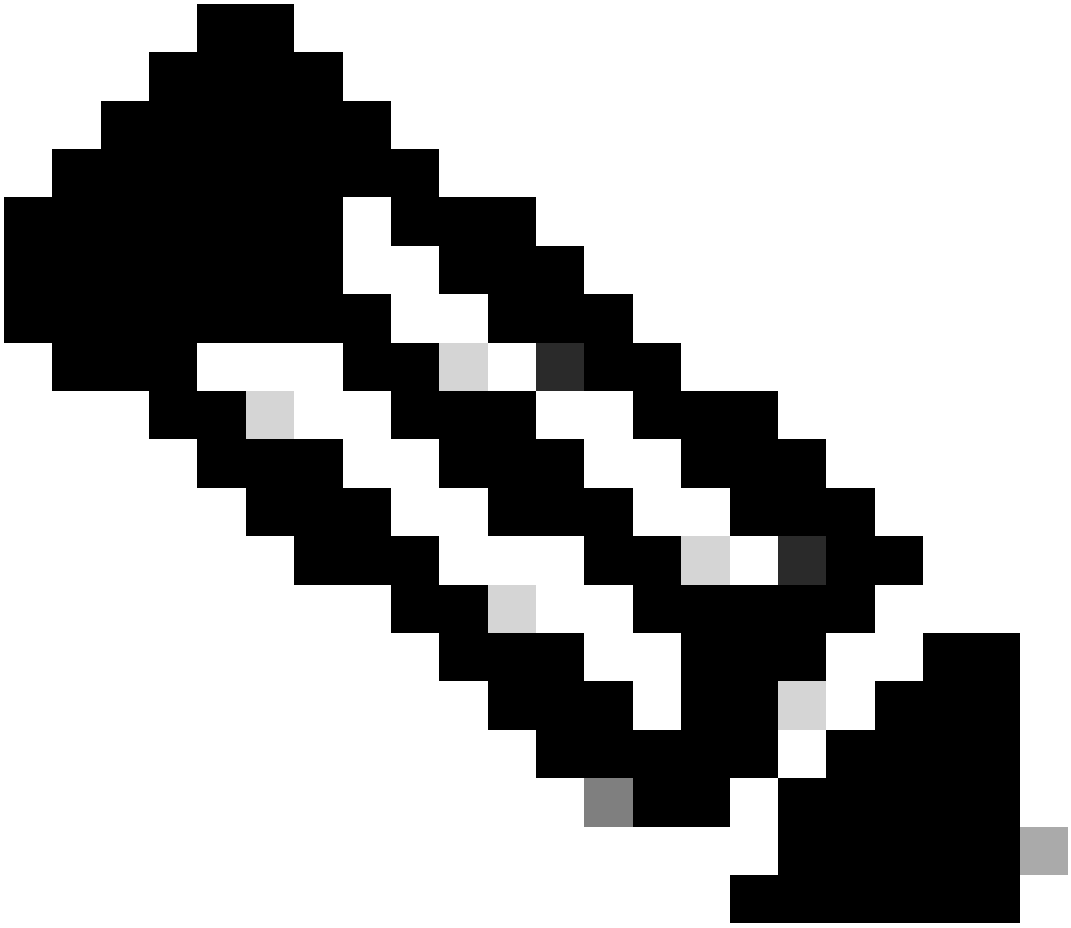
VPN-Gateways (Virtual Private Network) werden in dynamischen Umgebungen eingesetzt. Mehrere Variablen können jede VPN-Verbindung beeinflussen, z. B. Intranet-Konfigurationen, die sich häufig ändern, die verschiedenen Rollen, die jeder Benutzer innerhalb einer Organisation einnehmen kann, und Anmeldungen von Remote-Access-Standorten mit unterschiedlichen Konfigurationen und Sicherheitsstufen. Die Benutzerautorisierung ist in einer dynamischen VPN-Umgebung weitaus komplizierter als in einem Netzwerk mit statischer Konfiguration.

Dynamic Access Policies (DAP) sind eine Funktion, mit der Sie Autorisierungen für die Dynamik von VPN-Umgebungen konfigurieren können. Sie erstellen eine dynamische Zugriffsrichtlinie, indem Sie eine Auflistung von Zugriffssteuerungsattributen festlegen, die Sie einem bestimmten Benutzertunnel oder einer bestimmten Sitzung zuordnen. Diese Attribute behandeln Probleme mit mehreren Gruppenmitgliedschaften und Endpunktsicherheit.

Beispielsweise gewährt die Sicherheits-Appliance einem bestimmten Benutzer Zugriff für eine bestimmte Sitzung, basierend auf den von Ihnen definierten Richtlinien. Er generiert während der gesamten Benutzerauthentifizierung ein DAP, indem Attribute aus einem oder mehreren DAP-Datensätzen ausgewählt und/oder aggregiert werden. Diese DAP-Datensätze werden auf Basis der Endpunkt-Sicherheitsinformationen des Remote-Geräts und/oder der AAA-Autorisierungsinformationen des authentifizierten Benutzers ausgewählt. Anschließend wird der DAP-Datensatz auf den Tunnel oder die Sitzung des Benutzers angewendet.



Hinweis: Die Datei dap.xml, die die Auswahlattribute der DAP-Richtlinien enthält, wird im ASA-Flash gespeichert. Obwohl Sie die dap.xml-Datei extern exportieren, bearbeiten (wenn Sie über die XML-Syntax Bescheid wissen) und wieder importieren können, sollten Sie sehr vorsichtig sein, da Sie ASDM dazu veranlassen können, die Verarbeitung von DAP-Datensätzen zu beenden, wenn Sie etwas falsch konfiguriert haben. Es gibt keine CLI zum Bearbeiten dieses Teils der Konfiguration.



Hinweis: Der Versuch, die Zugriffsparameter für dynamische Zugriffsrichtlinien und Datensätze über die CLI zu konfigurieren, kann dazu führen, dass das DAP nicht mehr funktioniert. Dasselbe würde jedoch vom ASDM ordnungsgemäß verwaltet. Vermeiden Sie die Kommandozeile, und verwenden Sie stets ASDM zur Verwaltung von DAP-Richtlinien.

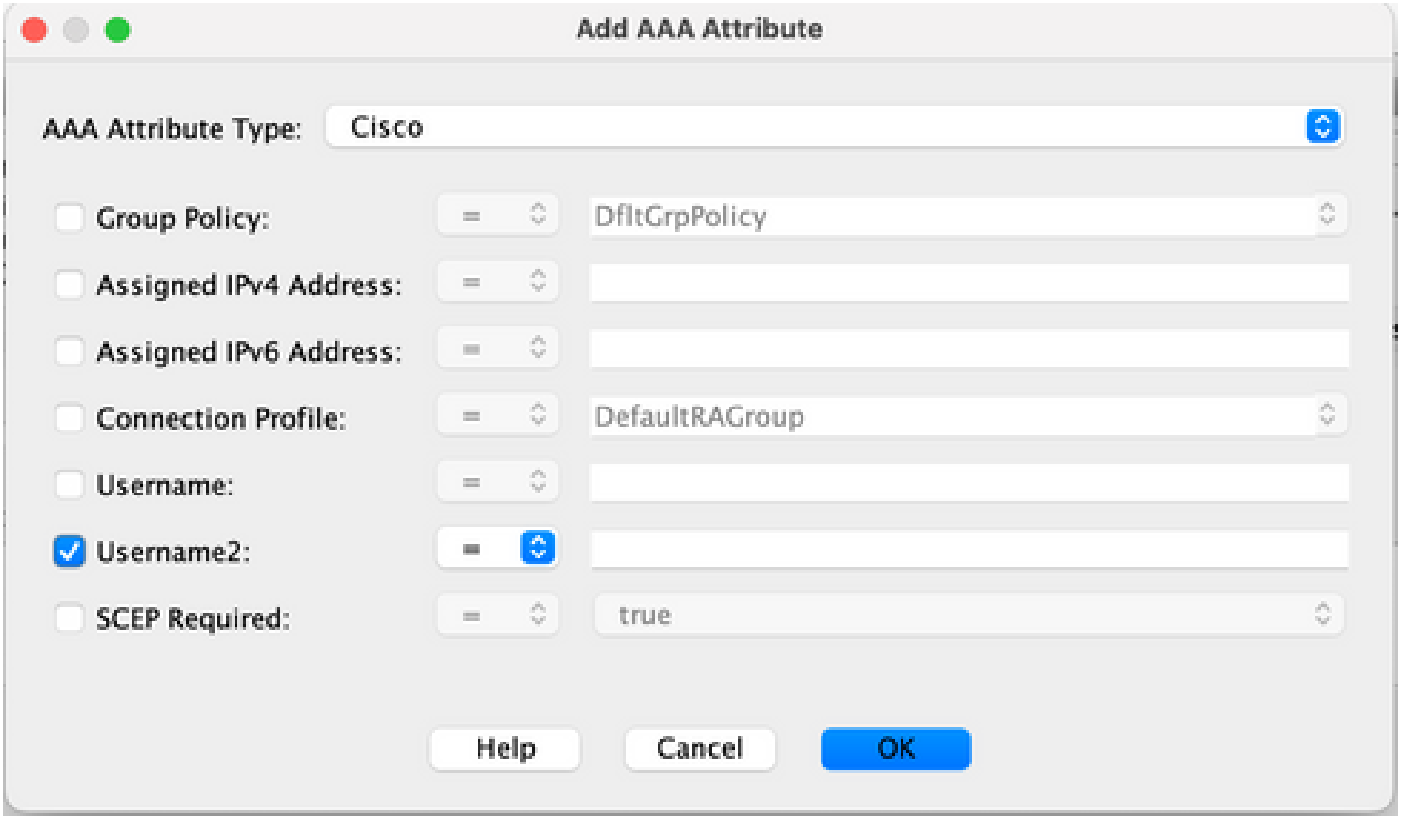
DAP- und AAA-Attribute

DAP ergänzt AAA-Services und bietet eine begrenzte Anzahl von Autorisierungsattributen, die AAA-Attribute überschreiben können. Die Sicherheits-Appliance kann DAP-Datensätze auf Basis der AAA-Autorisierungsinformationen für den Benutzer auswählen. Die Sicherheits-Appliance kann abhängig von diesen Informationen mehrere DAP-Datensätze auswählen, die dann aggregiert werden, um DAP-Autorisierungsattribute zuzuweisen.

Sie können AAA-Attribute aus der Cisco AAA-Attributhierarchie oder aus dem vollständigen Satz von Antwortattributen angeben, die die Sicherheits-Appliance von einem RADIUS- oder LDAP-

Server empfängt (siehe Abbildung 1).

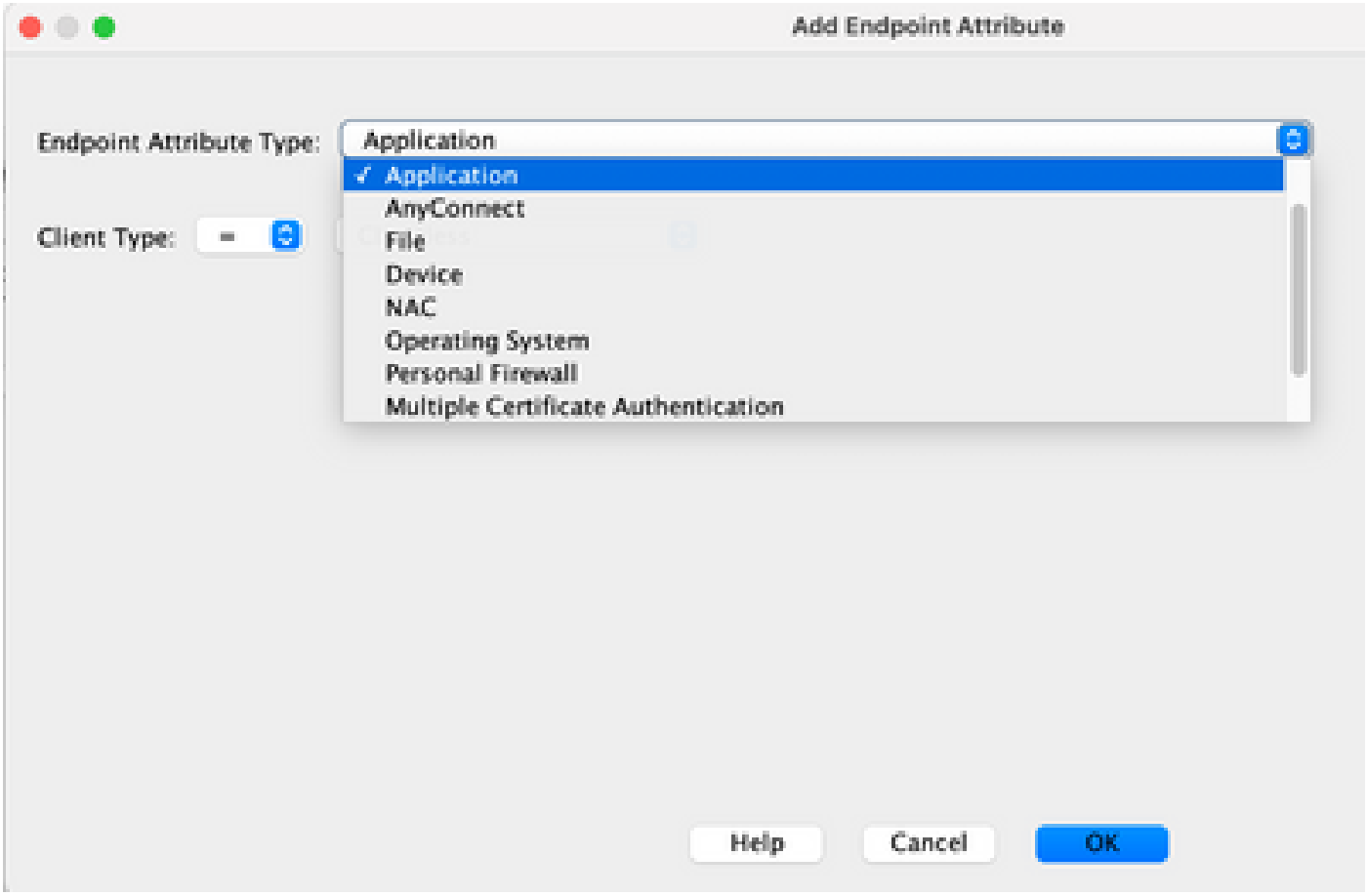
Abbildung 1. GUI für DAP-AAA-Attribut



DAP- und Endpunkt-Sicherheitsattribute

Zusätzlich zu den AAA-Attributen kann die Sicherheits-Appliance mithilfe der von Ihnen konfigurierten Statusüberprüfungsmethoden auch die Sicherheitsattribute der Endgeräte abrufen. Dazu gehören der grundlegende Host-Scan, Secure Desktop, Standard-/erweiterte Endpunktanalyse und NAC (siehe Abbildung 2). Die Attribute der Endpunktbewertung werden abgerufen und vor der Benutzerauthentifizierung an die Sicherheits-Appliance gesendet. AAA-Attribute, einschließlich des gesamten DAP-Datensatzes, werden jedoch während der Benutzerauthentifizierung validiert.

Abbildung 2. Endgeräteattribut-GUI

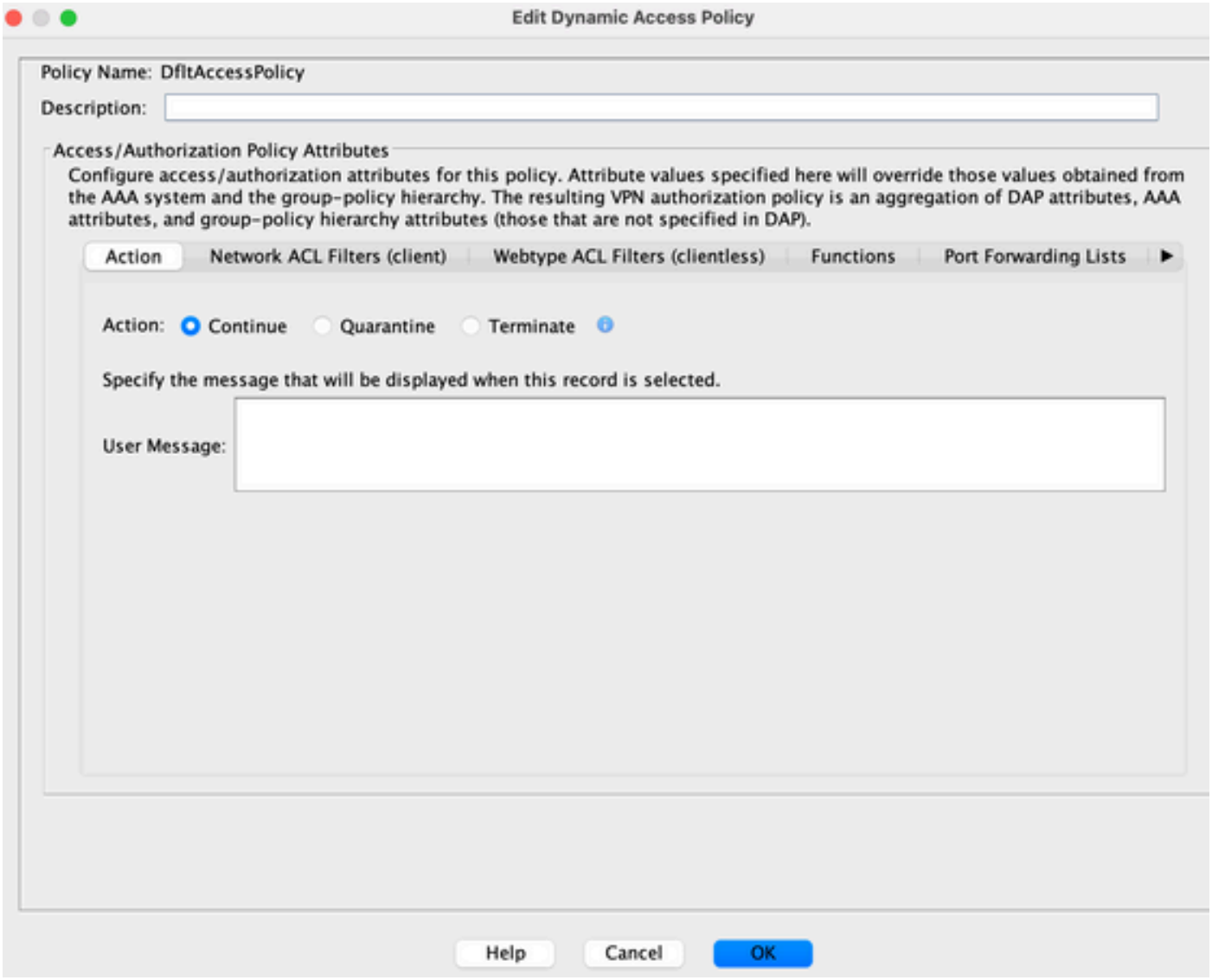


Dynamische Standardzugriffsrichtlinie

Vor der Einführung und Implementierung von DAP wurden Zugriffsrichtlinien-Attribut/Wert-Paare, die einem bestimmten Benutzertunnel oder einer Sitzung zugeordnet waren, entweder lokal auf der ASA definiert (d. h. Tunnelgruppen und Gruppenrichtlinien) oder über externe AAA-Server zugeordnet.

DAP wird standardmäßig immer erzwungen. Eine Zugriffskontrolle über Tunnelgruppen, Gruppenrichtlinien und AAA ohne die explizite Durchsetzung von DAP kann dieses Verhalten dennoch ermöglichen. Für das Legacy-Verhalten sind keine Konfigurationsänderungen an der DAP-Funktion, einschließlich des DAP-Standarddatensatzes DfltAccessPolicy, erforderlich (siehe Abbildung 3).

Abbildung 3: Dynamische Standardzugriffsrichtlinie



Wenn jedoch einer der Standardwerte in einem DAP-Datensatz geändert wird, z. B. der Parameter Action: in der DfltAccessPolicy von seinem Standardwert in Terminate geändert wird und keine zusätzlichen DAP-Datensätze konfiguriert sind, können authentifizierte Benutzer standardmäßig mit dem DfltAccessPolicy-DAP-Datensatz übereinstimmen und den VPN-Zugriff ablehnen.

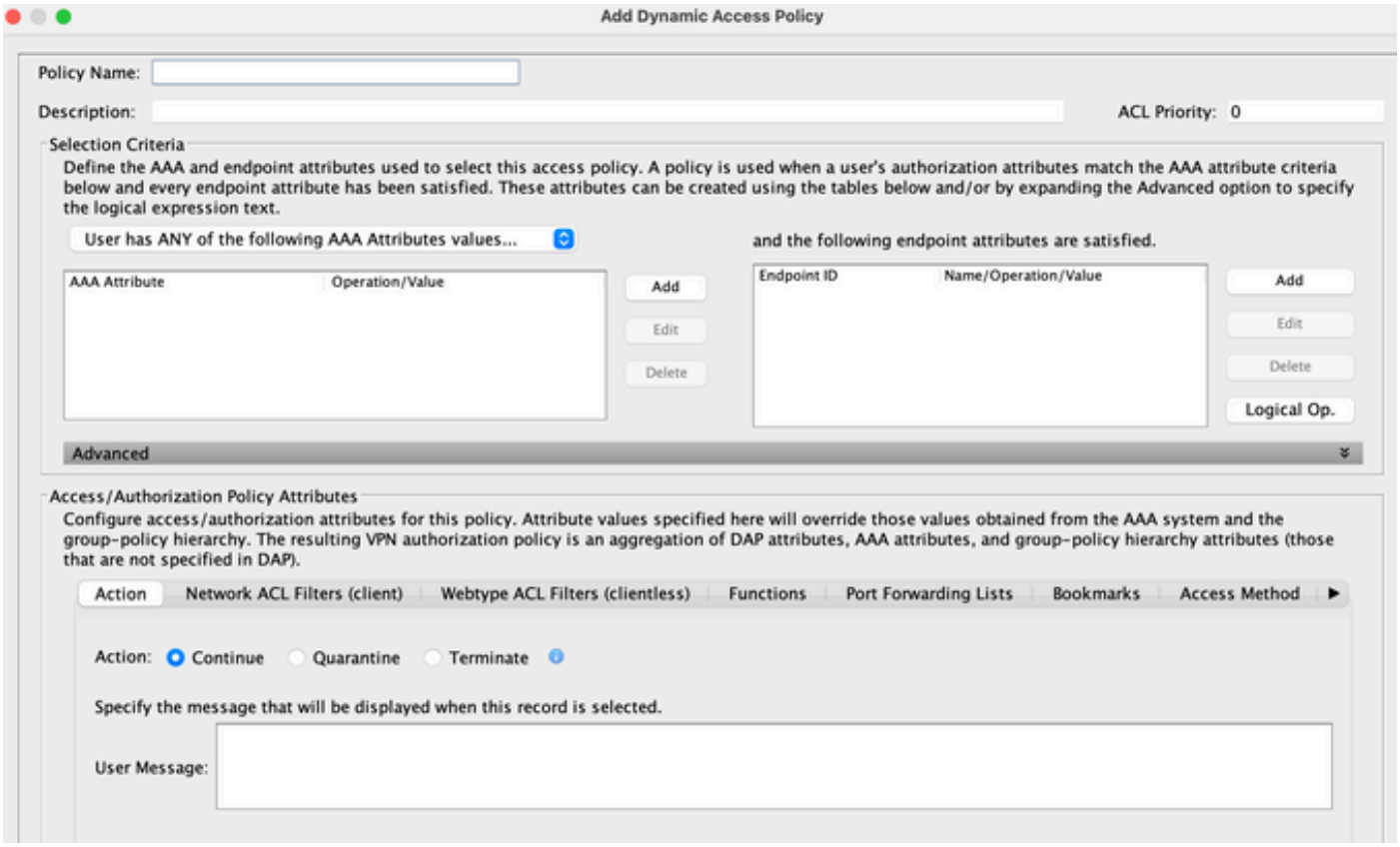
Daher müssen ein oder mehrere DAP-Datensätze erstellt und konfiguriert werden, um die VPN-Verbindung zu autorisieren und zu definieren, auf welche Netzwerkressourcen ein authentifizierter Benutzer zugreifen darf. Daher kann DAP bei entsprechender Konfiguration Vorrang vor der Durchsetzung älterer Richtlinien haben.

Konfigurieren dynamischer Zugriffsrichtlinien

Wenn Sie mithilfe von DAP definieren, auf welche Netzwerkressourcen ein Benutzer Zugriff hat, sind viele Parameter zu berücksichtigen. Wenn Sie z. B. feststellen, ob der verbindende Endpunkt aus einer verwalteten, nicht verwalteten oder nicht vertrauenswürdigen Umgebung stammt, bestimmen Sie die Auswahlkriterien, die zur Identifizierung des verbindenden Endpunkts erforderlich sind, und legen Sie anhand der Endpunktbewertung und/oder der AAA-Anmeldeinformationen fest, auf welche Netzwerkressourcen der Benutzer, der die Verbindung

herstellt, zugreifen darf. Hierzu müssen Sie sich zunächst mit den Funktionen und Merkmalen von DAP vertraut machen, wie in Abbildung 4 dargestellt.

Abbildung 4: Dynamische Zugriffsrichtlinie



Beim Konfigurieren eines DAP-Datensatzes sind zwei Hauptkomponenten zu berücksichtigen:

- Auswahlkriterien einschließlich erweiterter Optionen
- Zugriffsrichtlinien-Attribute

Im Abschnitt "Auswahlkriterien" kann ein Administrator AAA- und Endpunktattribute konfigurieren, mit denen ein bestimmter DAP-Datensatz ausgewählt wird. Ein DAP-Datensatz wird verwendet, wenn die Autorisierungsattribute eines Benutzers mit den AAA-Attributkriterien übereinstimmen und alle Endpunktattribute erfüllt wurden.

Wenn z. B. der AAA-Attributtyp LDAP (Active Directory) ausgewählt ist, die Attributnamenszeichenfolge memberOf lautet und die Wertezeichenfolge Contractors lautet, wie in Abbildung 5a dargestellt, muss der authentifizierende Benutzer Mitglied der Active Directory-Gruppe Contractors sein, um die AAA-Attributkriterien zu erfüllen.

Zusätzlich zur Erfüllung der AAA-Attributkriterien kann der authentifizierende Benutzer auch dazu verpflichtet werden, die Endpunktattributkriterien zu erfüllen. Wenn der Administrator beispielsweise den Status des verbindenden Endpunkts anhand dieser Statusüberprüfung ermittelt hat, kann der Administrator diese Informationen als Auswahlkriterien für das Endpunktattribut verwenden, das in Abbildung 5b dargestellt ist.

Abbildung 5a. AAA-Attributkriterien

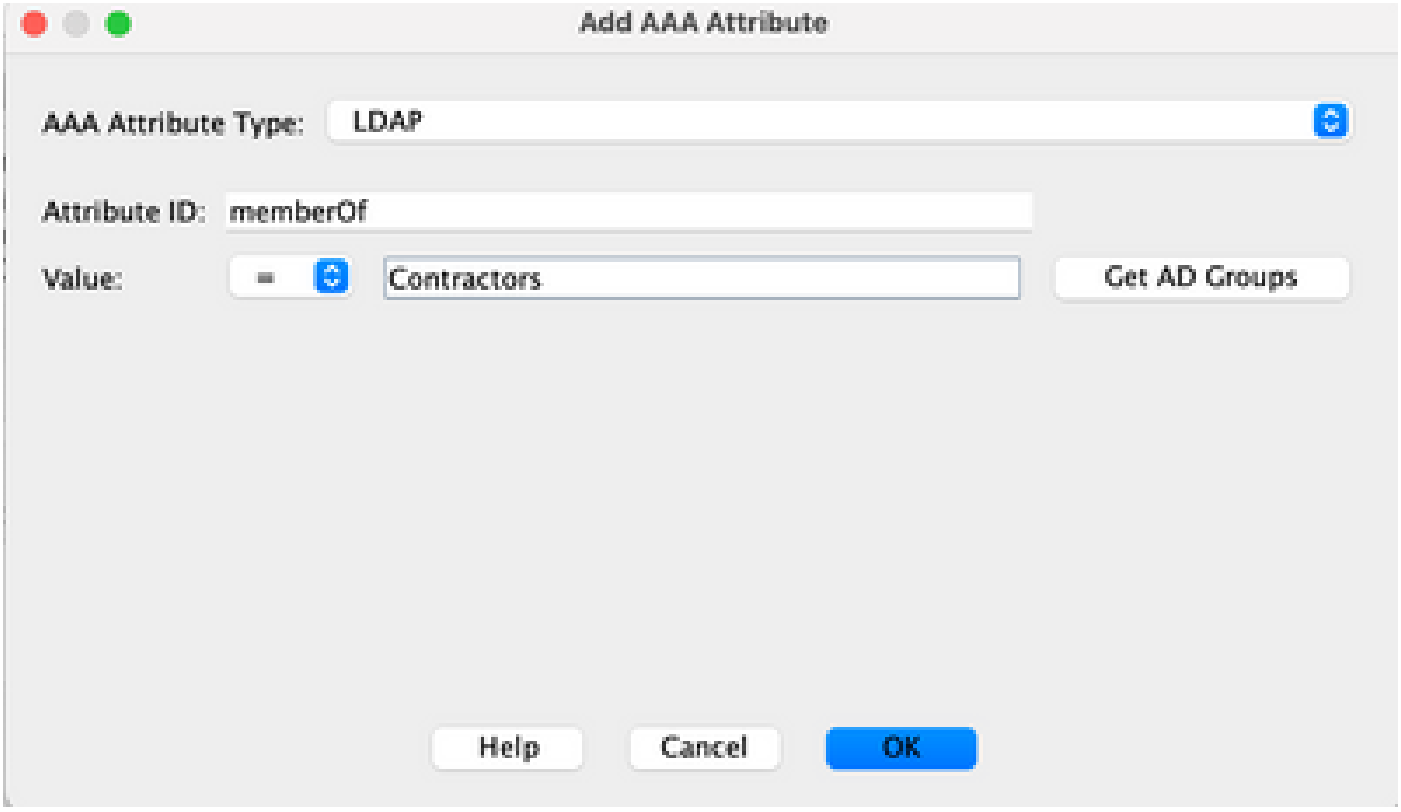


Abbildung 5b. Kriterien für Endgeräteattribute

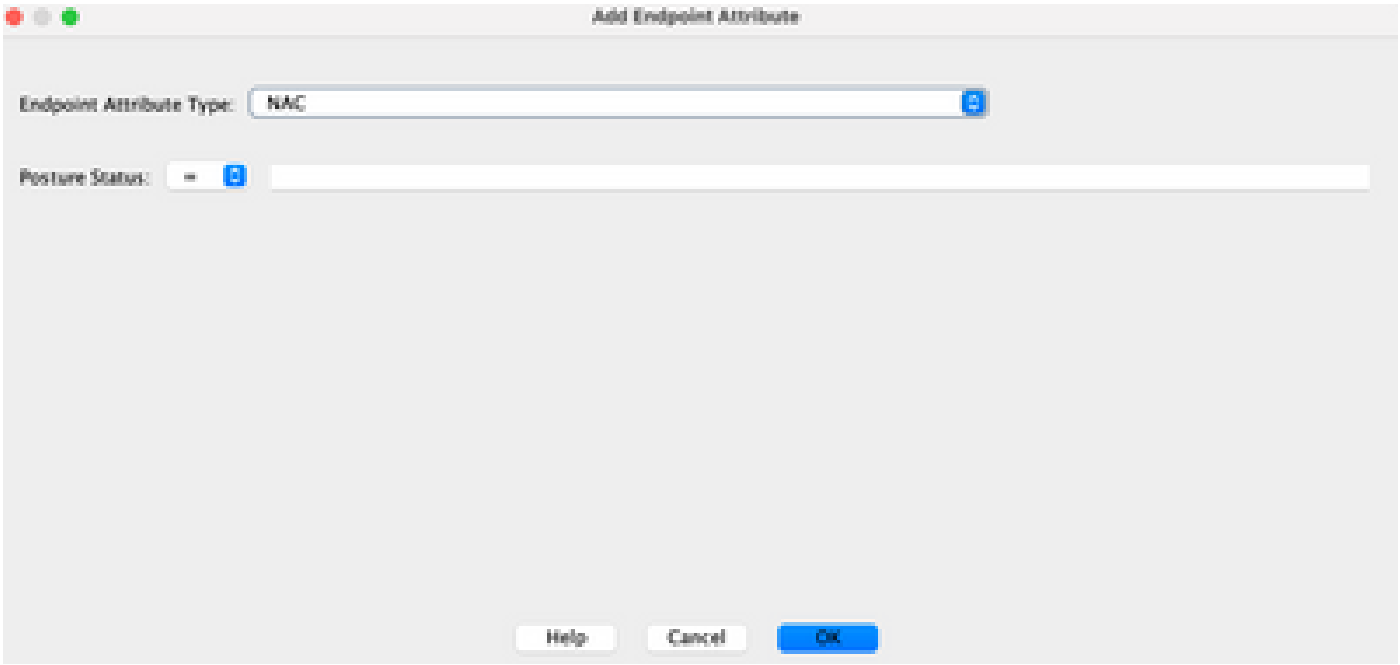
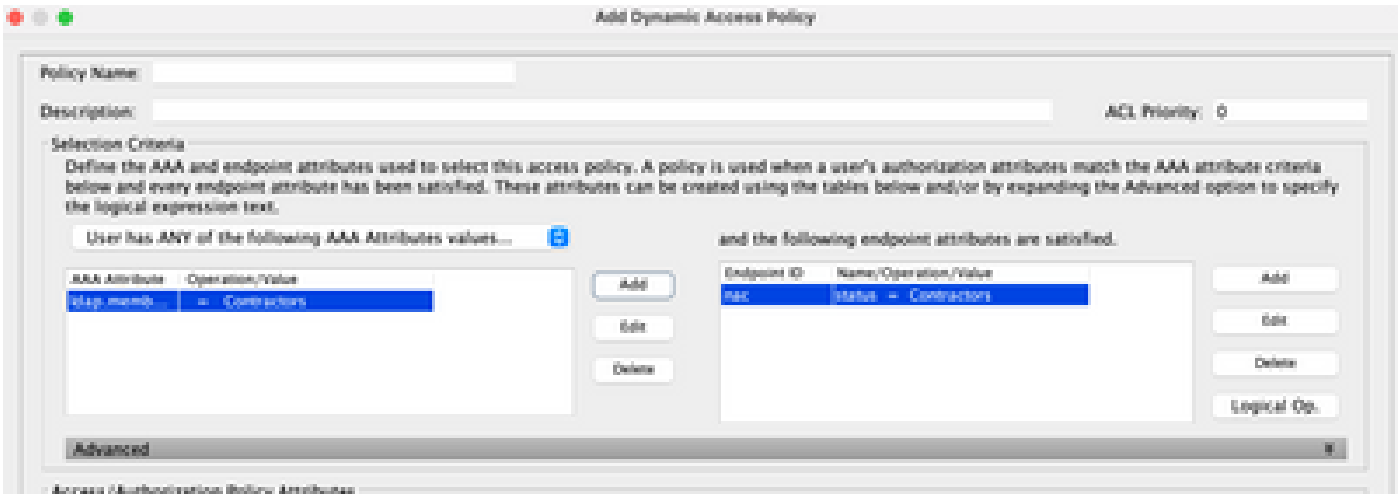


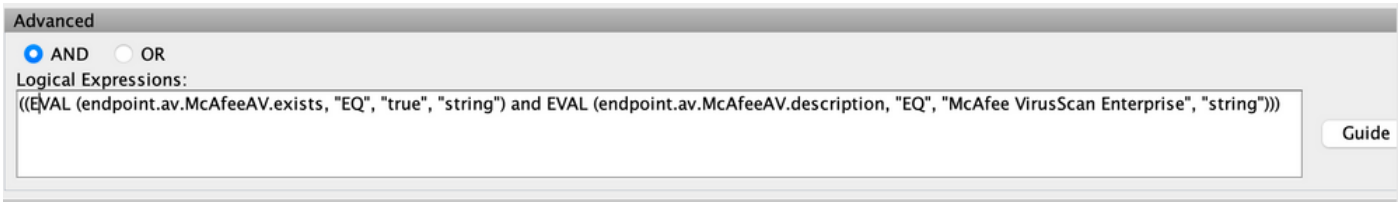
Abbildung 6: AAA- und Endpunkt-Attributkriterium-Übereinstimmung



AAA- und Endpunktattribute können mithilfe der Tabellen wie in Abbildung 6 beschrieben und/oder durch Erweitern der Option Erweitert erstellt werden, um einen logischen Ausdruck anzugeben, wie in Abbildung 7 dargestellt. Derzeit wird der logische Ausdruck mit EVAL-Funktionen erstellt, z. B. EVAL (endpoint.av.McAfeeAV.exist, "EQ", "true", "string") und EVAL (endpoint.av.McAfeeAV.description, "EQ", "McAfee VirusScan Enterprise", "string"), die logische AAA- und/oder Endpunktauswahlvorgänge darstellen.

Logische Ausdrücke sind nützlich, wenn Sie andere Auswahlkriterien als die in den Attributbereichen AAA und Endpunkt möglichen hinzufügen müssen, wie oben gezeigt. Sie können die Sicherheits-Appliances zwar für die Verwendung von AAA-Attributen konfigurieren, die alle, alle oder keines der angegebenen Kriterien erfüllen, aber die Endgeräteattribute sind kumulativ und müssen alle erfüllt sein. Damit die Sicherheits-Appliance das eine oder andere Endpunktattribut verwenden kann, müssen Sie im Abschnitt "Erweitert" des DAP-Datensatzes entsprechende logische Ausdrücke erstellen.

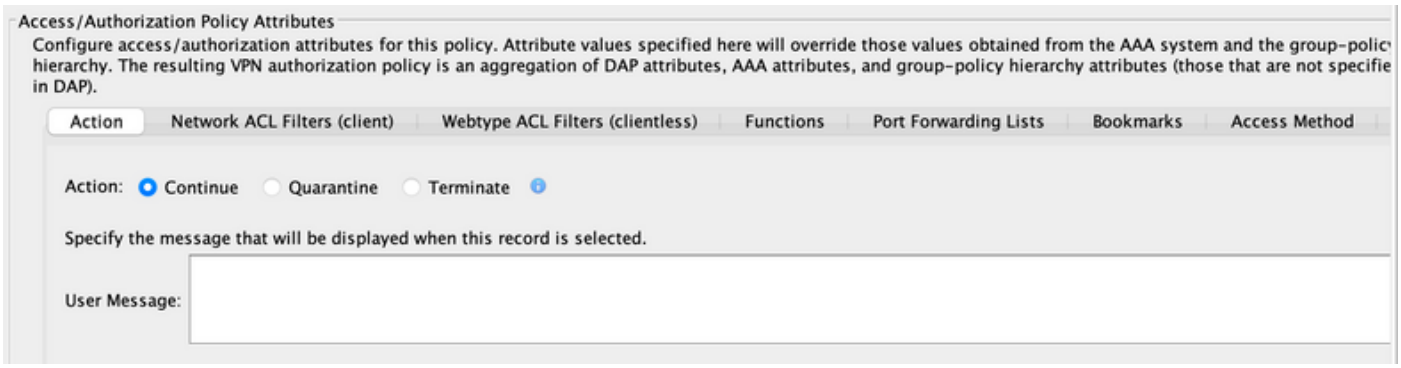
Abbildung 7: Benutzeroberfläche für logische Ausdrücke für die erweiterte Attributerstellung



Im Abschnitt "Access Policy Attributes" (Zugriffsrichtlinienattribute), wie in Abbildung 8 dargestellt, kann ein Administrator VPN-Zugriffsattribute für einen bestimmten DAP-Datensatz konfigurieren. Wenn Benutzerautorisierungsattribute den Kriterien AAA, Endpoint und/oder Logical Expression entsprechen, können die konfigurierten Attributwerte der Zugriffsrichtlinie in diesem Abschnitt erzwungen werden. Die hier angegebenen Attributwerte können diese Werte überschreiben, die vom AAA-System abgerufen werden, einschließlich der Werte in vorhandenen Benutzer-, Gruppen-, Tunnelgruppen- und Standardgruppendatensätzen.

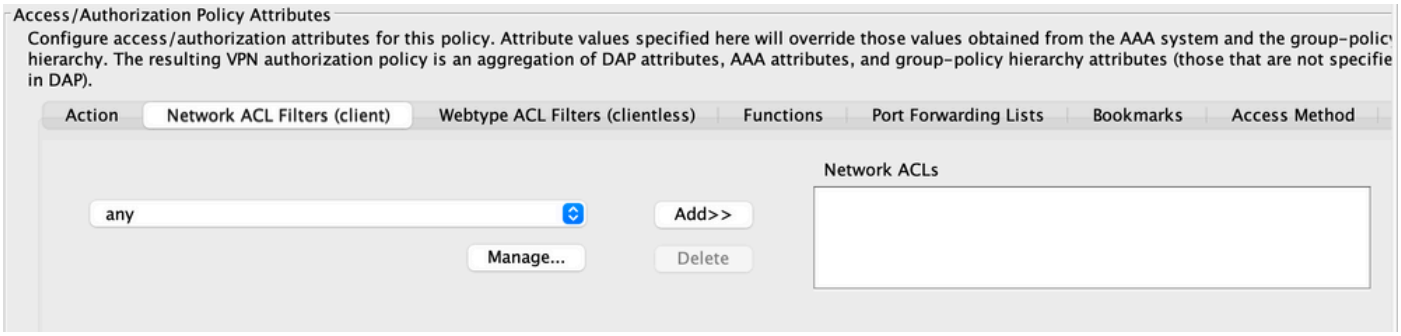
Ein DAP-Datensatz verfügt über eine begrenzte Anzahl von Attributwerten, die konfiguriert werden können. Diese Werte befinden sich unter den Registerkarten, wie in den Abbildungen 8 bis 14 gezeigt:

Abbildung 8: Aktion - Gibt die spezielle Verarbeitung an, die auf eine bestimmte Verbindung oder Sitzung angewendet werden soll.



- Continue (Fortfahren): (Standard) Klicken Sie, um Zugriffsrichtlinienattribute auf die Sitzung anzuwenden.
- Terminate (Beenden): Klicken Sie auf , um die Sitzung zu beenden.
- User Message (Benutzermeldung): Geben Sie eine Textmeldung ein, die auf der Portalseite angezeigt werden soll, wenn dieser DAP-Datensatz ausgewählt ist. Maximal 128 Zeichen. Eine Benutzermeldung wird als gelbe Kugel angezeigt. Wenn sich ein Benutzer anmeldet, blinkt er dreimal, um Aufmerksamkeit zu erregen, und bleibt dann aktiv. Wenn mehrere DAP-Datensätze ausgewählt sind und jeder von ihnen eine Benutzermeldung enthält, werden alle Benutzermeldungen angezeigt. Zusätzlich können Sie in solche Nachrichten URLs oder anderen eingebetteten Text einschließen, die erfordern, dass Sie die richtigen HTML-Tags verwenden.

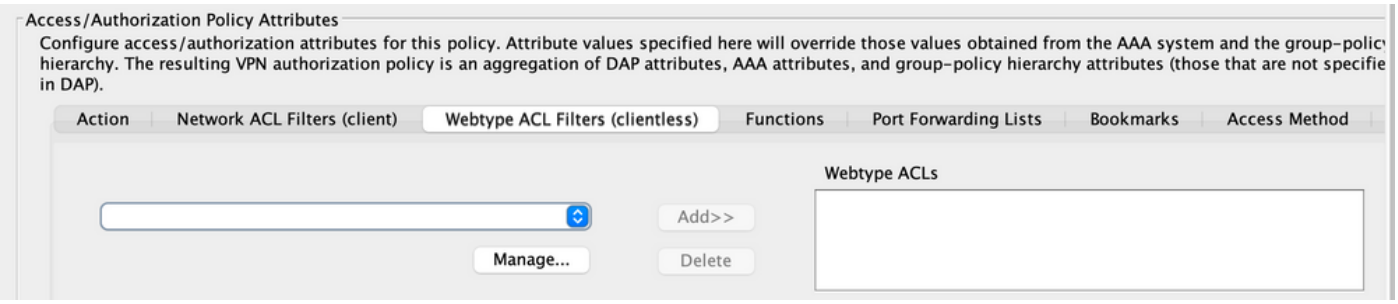
Abbildung 9: Registerkarte "Netzwerk-ACL-Filter": Auf dieser Registerkarte können Sie Netzwerk-ACLs für diesen DAP-Datensatz auswählen und konfigurieren. Eine ACL für DAP kann Zulassen- oder Ablehnungsregeln enthalten, jedoch nicht beides. Wenn eine ACL sowohl Zulassen- als auch Ablehnungsregeln enthält, lehnt die Security Appliance die ACL-Konfiguration ab.



- Das Dropdown-Feld "Network ACL" hat bereits Netzwerk-ACLs konfiguriert, die zu diesem DAP-Datensatz hinzugefügt werden sollen. Berechtigt sind nur ACLs, die über alle Zulassen- oder Ablehnungsregeln verfügen. Dies sind die einzigen ACLs, die hier angezeigt werden.
- Verwalten - Klicken Sie auf diese Schaltfläche, um Netzwerk-ACLs hinzuzufügen, zu bearbeiten und zu löschen.
- Die Netzwerk-ACL listet die Netzwerk-ACLs für diesen DAP-Datensatz auf.

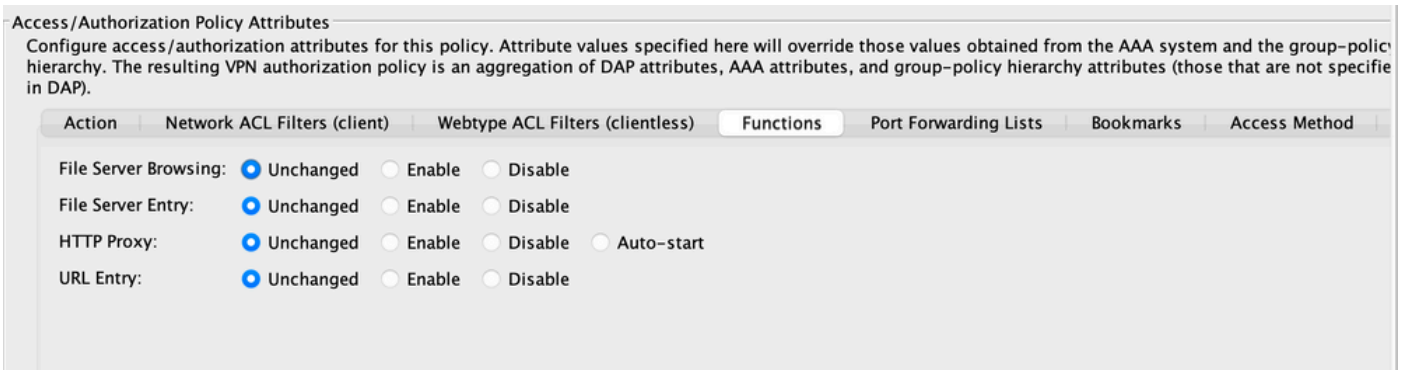
- Add (Hinzufügen): Klicken Sie auf diese Schaltfläche, um die ausgewählte Netzwerk-ACL aus dem Dropdown-Feld zur Liste der Netzwerk-ACLs rechts hinzuzufügen.
- Delete (Löschen) - Klicken Sie auf diese Option, um eine hervorgehobene Netzwerk-ACL aus der Liste der Netzwerk-ACLs zu löschen. Sie können eine ACL nicht löschen, wenn sie einem DAP oder einem anderen Datensatz zugewiesen ist.

Abbildung 10: Registerkarte Web-Type ACL Filters (Webtyp-ACL-Filter): Auf dieser Registerkarte können Sie Webtyp-ACLs für diesen DAP-Datensatz auswählen und konfigurieren. Eine ACL für DAP kann nur Zulassen- oder Ablehnungsregeln enthalten. Wenn eine ACL sowohl Zulassen- als auch Ablehnungsregeln enthält, lehnt die Security Appliance die ACL-Konfiguration ab.



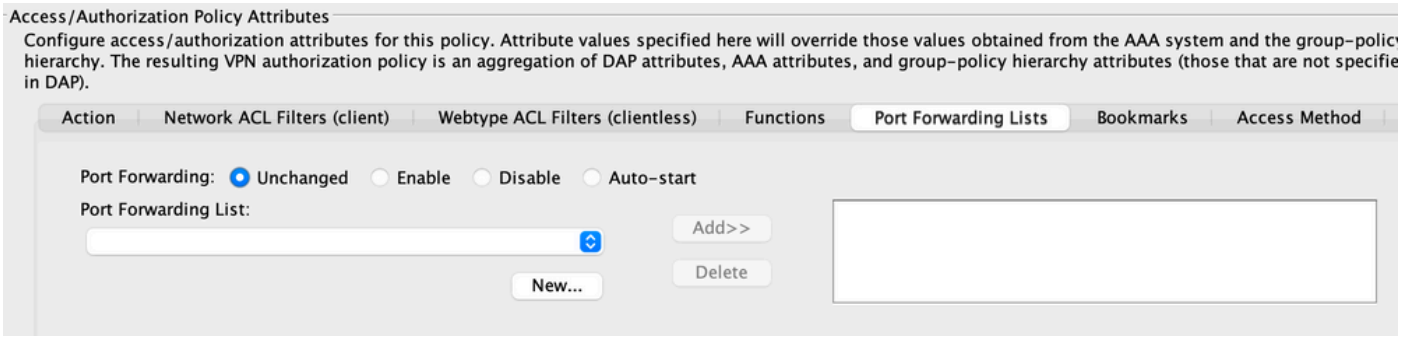
- Web-Type ACL-Dropdown-Feld — Wählen Sie bereits konfigurierte Web-Type ACLs aus, die diesem DAP-Datensatz hinzugefügt werden sollen. Nur ACLs mit allen Zulassen- oder Ablehnungsregeln sind zulässig. Dies sind die einzigen ACLs, die hier angezeigt werden.
- Verwalten... — Klicken Sie auf diese Option, um webbasierte Zugriffskontrolllisten hinzuzufügen, zu bearbeiten und zu löschen.
- Web-Type ACL list (Webtyp-ACL-Liste): Zeigt die Webtyp-ACLs für diesen DAP-Datensatz an.
- Hinzufügen - Klicken Sie auf diese Schaltfläche, um die ausgewählte Web-Typ-ACL aus dem Dropdown-Feld zur Liste Web-Typ-ACLs rechts hinzuzufügen.
- Löschen - Klicken Sie auf diese Option, um eine Web-Typ-ACL aus der Liste Web-Typ-ACLs zu löschen. Sie können eine ACL nicht löschen, wenn sie einem DAP oder einem anderen Datensatz zugewiesen ist.

Abbildung 11: Registerkarte Funktionen - Hier können Sie die Dateiservereingabe und -suche, den HTTP-Proxy und den URL-Eintrag für den DAP-Datensatz konfigurieren.



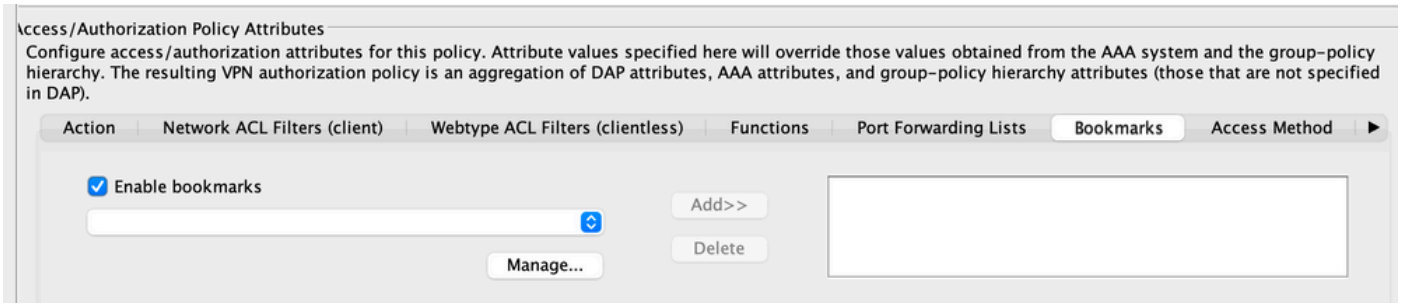
- File Server Browsing - Aktiviert oder deaktiviert die CIFS-Suche nach Dateiservern oder Freigabefunktionen.
- File Server Entry (Dateiservereintrag) - Ermöglicht oder verweigert einem Benutzer die Eingabe von Dateiserverpfaden und -namen auf der Portalseite. Wenn diese Option aktiviert ist, wird die Mappe für den Dateiserver-Eintrag auf der Portalseite platziert. Benutzer können Pfadnamen zu Windows-Dateien direkt eingeben. Sie können Dateien herunterladen, bearbeiten, löschen, umbenennen und verschieben. Sie können auch Dateien und Ordner hinzufügen. Freigaben müssen außerdem für den Benutzerzugriff auf den entsprechenden Microsoft Windows-Servern konfiguriert werden. Abhängig von den Netzwerkanforderungen kann von den Benutzern verlangt werden, dass sie sich authentifizieren, bevor sie auf Dateien zugreifen.
- HTTP Proxy (HTTP-Proxy): Betrifft die Weiterleitung eines HTTP-Applet-Proxys an den Client. Der Proxy eignet sich für Technologien, die eine ordnungsgemäße Content-Transformation behindern, z. B. Java, ActiveX und Flash. Sie umgeht den Prozess des Umschreibens und Umschreibens und stellt gleichzeitig sicher, dass die Sicherheits-Appliance weiterhin verwendet wird. Der weitergeleitete Proxy ändert die alte Proxykonfiguration des Browsers automatisch und leitet alle HTTP- und HTTPS-Anfragen an die neue Proxykonfiguration um. Es unterstützt praktisch alle Client-seitigen Technologien, einschließlich HTML, CSS, JavaScript, VBScript, ActiveX und Java. Microsoft Internet Explorer wird als einziger Browser unterstützt.
- URL Entry (URL-Eingabe): Ermöglicht oder verhindert die Eingabe von HTTP-/HTTPS-URLs auf der Portalseite durch einen Benutzer. Wenn diese Funktion aktiviert ist, können Benutzer Webadressen in das URL-Eingabefeld eingeben und über SSL VPN ohne Client auf diese Websites zugreifen.
- Unverändert - (Standard) Klicken Sie hier, um Werte aus der Gruppenrichtlinie zu verwenden, die für diese Sitzung gilt.
- Enable/Disable (Aktivieren/Deaktivieren): Klicken Sie, um die Funktion zu aktivieren oder zu deaktivieren.
- Auto-start (Automatisch starten): Klicken Sie auf diese Schaltfläche, um den HTTP-Proxy zu aktivieren und den DAP-Datensatz automatisch die Applets starten zu lassen, die diesen Funktionen zugeordnet sind.

Abbildung 12: Registerkarte Port Forwarding Lists (Port-Weiterleitungslisten): Auf dieser Registerkarte können Sie Port Forwarding-Listen für Benutzersitzungen auswählen und konfigurieren.



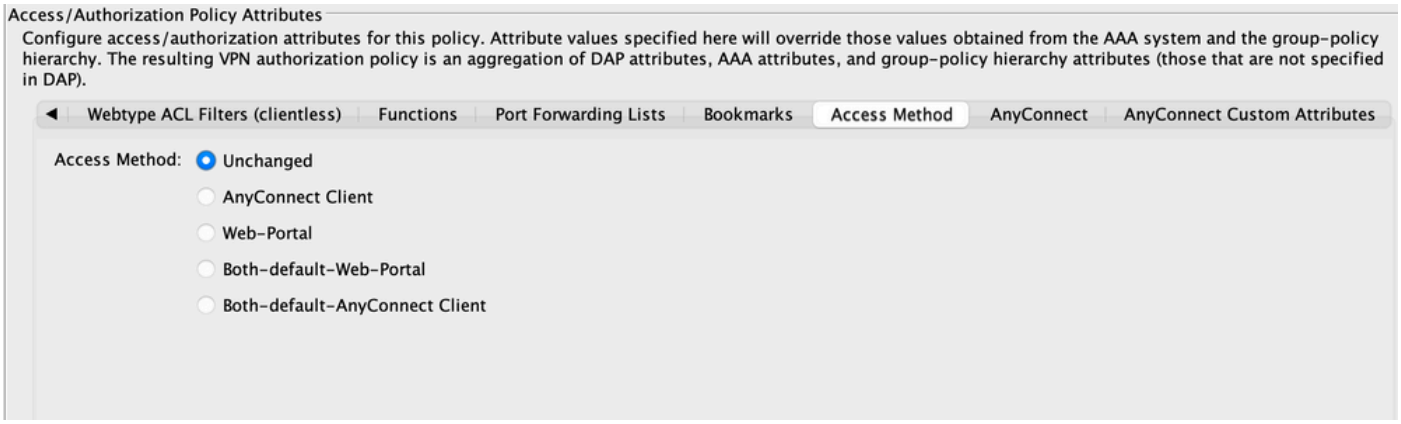
- Port Forwarding (Port-Weiterleitung) - Wählen Sie eine Option für die Port-Weiterleitungslisten aus, die für diesen DAP-Datensatz gelten. Die anderen Attribute in diesem Feld sind nur aktiviert, wenn Sie Port Forwarding auf Enable (Aktivieren) oder Auto-start (Automatisch starten) festlegen.
- Unverändert - Klicken Sie hier, um Werte aus der Gruppenrichtlinie zu verwenden, die für diese Sitzung gilt.
- Enable/Disable (Aktivieren/Deaktivieren): Klicken Sie, um die Port-Weiterleitung zu aktivieren oder zu deaktivieren.
- Auto-start (Automatisch starten): Klicken Sie auf diese Schaltfläche, um die Port-Weiterleitung zu aktivieren, und um den DAP-Datensatz automatisch die Port-Weiterleitungs-Applets starten zu lassen, die den Port-Weiterleitungslisten zugeordnet sind.
- Port Forwarding List (Port-Weiterleitungsliste) - Wählen Sie bereits konfigurierte Port Forwarding-Listen aus, die dem DAP-Datensatz hinzugefügt werden sollen.
- New (Neu): Klicken Sie auf , um neue Port Forwarding-Listen zu konfigurieren.
- Port Forwarding Lists (Portweiterleitungslisten): Zeigt die Portweiterleitungsliste für den DAP-Datensatz an.
- Add (Hinzufügen): Klicken Sie auf diese Schaltfläche, um die im Dropdown-Feld ausgewählte Port Forwarding-Liste rechts hinzuzufügen.
- Delete (Löschen) - Klicken Sie auf diese Option, um die ausgewählte Portweiterleitungsliste aus der Portweiterleitungsliste zu löschen. Sie können eine ACL nicht löschen, wenn sie einem DAP oder einem anderen Datensatz zugewiesen ist.

Abbildung 13: Lesezeichen: Auf dieser Registerkarte können Sie Lesezeichen/URL-Listen für Benutzersitzungen auswählen und konfigurieren.



- Lesezeichen aktivieren - Klicken Sie auf diese Option, um sie zu aktivieren. Wenn dieses Kontrollkästchen nicht aktiviert ist, werden auf der Portalseite keine Lesezeichenlisten für die Verbindung angezeigt.
- Verwalten - Zum Hinzufügen, Importieren, Exportieren und Löschen von Lesezeichenlisten klicken.
- Lesezeichenlisten (Dropdown-Liste) - Zeigt die Lesezeichenlisten für den DAP-Datensatz an.
- Hinzufügen - Klicken Sie auf diese Schaltfläche, um die ausgewählte Lesezeichenliste aus dem Dropdown-Feld rechts zum Listenfeld hinzuzufügen.
- Löschen (Delete) - Klicken Sie auf diese Option, um die ausgewählte Lesezeichenliste aus dem Listenfeld zu löschen. Sie können eine Lesezeichenliste nur dann aus der Sicherheits-Appliance löschen, wenn Sie sie zuvor aus DAP-Datensätzen löschen.

Abbildung 14: Registerkarte "Methode" - Ermöglicht Ihnen die Konfiguration des zulässigen Remotezugriffstyps.



- Unchanged (Nicht geändert): Fahren Sie mit der aktuellen Remote-Zugriffsmethode fort, die in der Gruppenrichtlinie für die Sitzung festgelegt wurde.
- AnyConnect Client - Verbindung über den Cisco AnyConnect VPN Client
- Web Portal: Herstellen einer Verbindung mit einem Client-losen VPN
- Both-default-Web-Portal (Beides - Standard-Webportal): Stellt eine Verbindung entweder über clientless oder den AnyConnect-Client her, wobei der Standardwert clientless lautet.
- Both-default-AnyConnect Client - Verbinden Sie sich entweder über den Client-losen oder den AnyConnect-Client, wobei der Standardwert AnyConnect ist.

Wie bereits erwähnt, verfügt ein DAP-Datensatz nur über einen begrenzten Satz von Standardattributwerten. Nur wenn diese geändert werden, haben sie Vorrang vor aktuellen AAA-, Benutzer-, Gruppen-, Tunnelgruppen- und Standardgruppendatensätzen. Wenn zusätzliche Attributwerte außerhalb des DAP-Bereichs erforderlich sind, z. B. Split Tunneling Lists, Banner, Smart Tunnels, Portal Customizations usw., dann müssen sie über AAA-, Benutzer-, Gruppen-, Tunnelgruppen- und Standardgruppendatensätze durchgesetzt werden. In diesem Fall können

diese spezifischen Attributwerte das DAP ergänzen und nicht überschrieben werden. Somit erhält der Benutzer einen kumulativen Satz von Attributwerten für alle Datensätze.

Aggregieren mehrerer dynamischer Zugriffsrichtlinien

Ein Administrator kann mehrere DAP-Datensätze konfigurieren, um viele Variablen zu adressieren. Dadurch kann ein authentifizierender Benutzer die AAA- und Endpoint-Attributkriterien mehrerer DAP-Datensätze erfüllen. Folglich können Zugriffsrichtlinienattribute entweder konsistent sein oder in allen Richtlinien in Konflikt zueinander stehen. In diesem Fall kann der autorisierte Benutzer das Gesamtergebnis für alle zugeordneten DAP-Datensätze abrufen.

Dazu gehören auch eindeutige Attributwerte, die über Authentifizierungs-, Autorisierungs-, Benutzer-, Gruppen-, Tunnelgruppen- und Standardgruppendatensätze erzwungen werden. Durch das kumulative Ergebnis der Zugriffsrichtlinienattribute wird die dynamische Zugriffsrichtlinie erstellt. Beispiele für kombinierte Zugriffsrichtlinien-Attribute sind in den folgenden Tabellen aufgeführt. Diese Beispiele zeigen die Ergebnisse von 3 kombinierten DAP-Datensätzen.

Das Aktionsattribut in Tabelle 1 hat den Wert "Beenden" oder "Weiter". Der aggregierte Attributwert ist "Beenden", wenn der Wert "Beenden" in einem der ausgewählten DAP-Datensätze konfiguriert ist, und "Fortfahren", wenn der Wert "Fortfahren" in allen ausgewählten DAP-Datensätzen konfiguriert ist.

Tabelle 1. Aktionsattribut

Attributname	DAP 1	DAP 2	DAP 3	DAP
Aktion (Beispiel 1)	fortfahren	fortfahren	fortfahren	fortfahren
Aktion (Beispiel 2)	Beenden	fortfahren	fortfahren	beenden

Das in Tabelle 2 dargestellte Attribut "user-message" enthält einen Zeichenfolgenwert. Bei dem aggregierten Attributwert kann es sich um eine durch Zeilenvorschub (Hexadezimalwert 0x0A) getrennte Zeichenfolge handeln, die durch Verknüpfung der Attributwerte aus den ausgewählten DAP-Datensätzen erstellt wird. Die Reihenfolge der Attributwerte in der kombinierten Zeichenfolge ist unbedeutend.

Tabelle 2. Benutzernachrichten-Attribut

Attributname	DAP 1	DAP 2	DAP 3	DAP
Benutzernachricht	schnell	Braunfuchs	Springt über	der schnelle<LF>braune Fuchs<LF>springt über

Die in Tabelle 3 aufgeführten Attribute zur Aktivierung der Clientless-Funktion (Funktionen) enthalten Werte, die Auto-start, Enable oder Disable lauten. Der aggregierte Attributwert kann Auto-start sein, wenn der Auto-Start-Wert in einem der ausgewählten DAP-Datensätze konfiguriert ist.

Der aggregierte Attributwert kann aktiviert werden, wenn in keinem der ausgewählten DAP-Datensätze ein Auto-Start-Wert konfiguriert ist und der Enable-Wert in mindestens einem der ausgewählten DAP-Datensätze konfiguriert ist.

Der aggregierte Attributwert kann deaktiviert werden, wenn in einem der ausgewählten DAP-Datensätze kein Auto-Start- oder Aktivierungswert konfiguriert ist und der Deaktivierungswert in mindestens einem der ausgewählten DAP-Datensätze konfiguriert ist.

Tabelle 3. Attribute zur Aktivierung von Clientless-Funktionen (Funktionen)

Attributname	DAP 1	DAP 2	DAP 3	DAP
Port-Forward	aktivieren	abschalten		aktivieren
Durchsuchen von Dateien	abschalten	aktivieren	abschalten	aktivieren
Dateieintrag			abschalten	abschalten
HTTP-Proxy	abschalten	Autostart	abschalten	Autostart
URL-Eintrag	abschalten		aktivieren	aktivieren

Die in Tabelle 4 aufgeführten Attribute für die URL-Liste und den Port-Forward enthalten einen Wert, der entweder eine Zeichenfolge oder eine kommagetrennte Zeichenfolge ist. Der aggregierte Attributwert kann eine kommagetrennte Zeichenfolge sein, die erstellt wird, wenn Sie die Attributwerte aus den ausgewählten DAP-Datensätzen miteinander verknüpfen. Alle doppelten Attributwerte in der kombinierten Zeichenfolge können entfernt werden. Die Reihenfolge der Attributwerte in der kombinierten Zeichenfolge ist unerheblich.

Tabelle 4. Attribut für URL-Liste und Portweiterleitungsliste

Attributname	DAP 1	DAP 3	DAP 3	DAP
URL-Liste	a	b,c	a	a,b,c
Port-Forward		d,e	e,f	d,e,f

Die Attribute der Zugriffsmethode geben die Clientzugriffsmethode an, die für SSL VPN-Verbindungen zulässig ist. Die Clientzugriffsmethode kann AnyConnect Client Access Only, Web-Portal Access Only, AnyConnect Client oder Web-Portal Access mit Web-Portal-Zugriff als Standard oder AnyConnect Client oder Web-Portal Access mit AnyConnect Client Access als Standard sein. Der aggregierte Attributwert ist in Tabelle 5 zusammengefasst.

Tabelle 5. Attribute der Zugriffsmethode

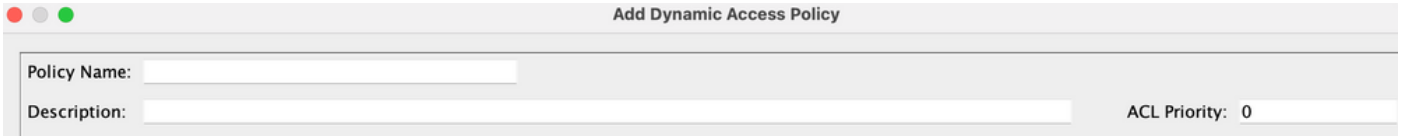
Ausgewählte Attributwerte				Aggregationsergebnis
AnyConnect-Client	Web-Portal	Beide Standard-Webportale	Beide Standard-AnyConnect-Clients	
			X	Beide Standard-AnyConnect-Clients
		X		Beide Standardwebportale
		X	X	Beide Standardwebportale

	X			Webportal
	X		X	Beide Standard-AnyConnect-Clients
	X	X		Beide Standardwebportale
	X	X	X	Beide Standardwebportale
X				AnyConnect-Client
X			X	Beide Standard-AnyConnect-Clients
X		X		Beide Standardwebportale
X		X	X	Beide Standardwebportale
X	X			Beide Standardwebportale
X	X		X	Beide Standard-AnyConnect-Clients
X	X	X		Beide Standardwebportale
X	X	X	X	Beide Standardwebportale

Wenn Sie die Attribute Netzwerk- (Firewall) und Webtyp- (Clientless-)ACL-Filter kombinieren, sind die DAP-Priorität und die DAP-ACL zwei wichtige zu berücksichtigende Komponenten.

Das Tribut Priority (Priorität), wie in Abbildung 15 dargestellt, ist nicht aggregiert. Die Sicherheits-Appliance verwendet diesen Wert, um die Zugriffslisten beim Aggregieren der Netzwerk- und Webtyp-ACLs aus mehreren DAP-Datensätzen logisch zu sequenzieren. Die Sicherheits-Appliance ordnet die Datensätze von der höchsten zur niedrigsten Prioritätsnummer, wobei sich die niedrigste in der Tabelle unten befindet. Ein DAP-Datensatz mit dem Wert 4 hat beispielsweise eine höhere Priorität als ein Datensatz mit dem Wert 2. Sie können sie nicht manuell sortieren.

Abbildung 15: Priorität - Zeigt die Priorität des DAP-Datensatzes an.

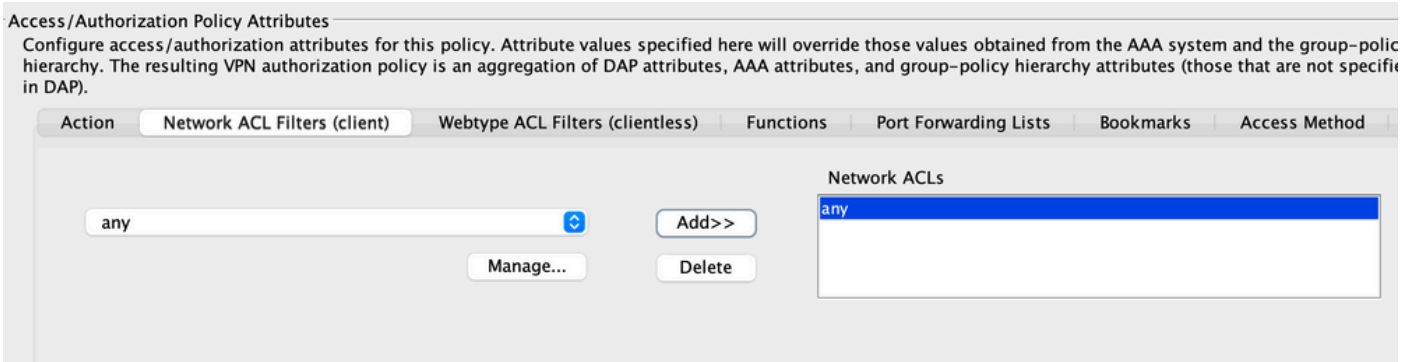


- Policy Name (Richtlinienname): Zeigt den Namen des DAP-Datensatzes an.
- Description (Beschreibung): Beschreibt den Zweck des DAP-Datensatzes.

Das DAP ACL-Attribut unterstützt nur Zugriffslisten, die entweder einem strengen Modell der Zulassungsliste oder dem strengen Modell der Sperrliste entsprechen. In einem ACL-Modell mit Zulassungsliste geben die Zugriffslisteneinträge Regeln an, die den Zugriff auf bestimmte Netzwerke oder Hosts zulassen. In einem Block-List-ACL-Modus geben die Zugriffslisteneinträge Regeln an, die den Zugriff auf bestimmte Netzwerke oder Hosts verweigern. Eine nicht konforme Zugriffsliste enthält Zugriffslisteneinträge mit einer Mischung aus Zulassen- und Ablehnungsregeln. Wenn eine nicht konforme Zugriffsliste für einen DAP-Datensatz konfiguriert ist, kann sie als Konfigurationsfehler zurückgewiesen werden, wenn der Administrator versucht, den Datensatz hinzuzufügen. Wenn eine konforme Zugriffsliste einem DAP-Datensatz zugewiesen

wird, kann jede Änderung an der Zugriffsliste, die das Konformitätsmerkmal ändert, als Konfigurationsfehler zurückgewiesen werden.

Abbildung 16: DAP ACL (DAP-ACL): Hiermit können Sie Netzwerk-ACLs für diesen DAP-Datensatz auswählen und konfigurieren.



Wenn mehrere DAP-Datensätze ausgewählt sind, werden die in der Netzwerk-(Firewall-)ACL angegebenen Attribute der Zugriffslisten zusammengefasst, um eine dynamische Zugriffsliste für die DAP-Firewall-ACL zu erstellen. Auf die gleiche Weise werden die in der Webtyp-ACL (Clientless) angegebenen Attribute der Zugriffslisten zusammengefasst, um eine dynamische Zugriffsliste für die DAP Clientless-ACL zu erstellen. Im nächsten Beispiel geht es darum, wie eine dynamische DAP Firewall Access-List speziell erstellt wird. Eine dynamische clientlose DAP-Zugriffsliste kann jedoch den gleichen Prozess ausführen.

Zunächst erstellt die ASA dynamisch einen eindeutigen Namen für die DAP-Netzwerk-ACL, wie in Tabelle 6 gezeigt.

Tabelle 6. Dynamischer DAP-Netzwerk-ACL-Name

DAP-Netzwerk-ACL-Name
DAP-Network-ACL-X (wobei X eine ganze Zahl ist, die inkrementiert werden kann, um Eindeutigkeit zu gewährleisten)

Anschließend ruft die ASA das Attribut Network-ACL aus den ausgewählten DAP-Datensätzen ab (siehe Tabelle 7).

Tabelle 7. Netzwerk-ACLs

Ausgewählte DAP-Datensätze	Priorität	Netzwerk-ACLs	Netzwerk-ACL-Einträge
DAP 1	1	101 und 102	ACL 101 verfügt über 4 Regeln zur Ablehnung und ACL 102 über 4 Regeln zur Genehmigung
DAP 2	2	201 und 202	ACL 201 verfügt über 3 Berechtigungsregeln und ACL 202 über 3 Ablehnungsregeln
DAP 3	2	101 und 102	ACL 101 verfügt über 4 Regeln zur Ablehnung und ACL 102 über 4 Regeln zur Genehmigung

Drittens ordnet die ASA die Netzwerk-ACL zuerst nach der Prioritätsnummer des DAP-Datensatzes und dann zuerst nach der Sperrliste neu, wenn der Prioritätswert für zwei oder mehr ausgewählte DAP-Datensätze gleich ist. Anschließend kann die ASA die Einträge für die Netzwerk-ACLs aus jeder Netzwerk-ACL abrufen, wie in Tabelle 8 gezeigt.

Tabelle 8. DAP-Datensatzpriorität

Netzwerk-ACLs	Priorität	Weißes/schwarzes Zugriffslistenmodell	Netzwerk-ACL-Einträge
101	2	Blacklist	4 Regeln verweigern (DDD)
202	2	Blacklist	3 Regeln verweigern (DD)
102	2	Whitelist	4 Genehmigungsregeln (PPPP)
202	2	Whitelist	3 Zulässigkeitsregeln (PPP)
101	1	Blacklist	4 Regeln verweigern (DDD)
102	1	Whitelist	4 Genehmigungsregeln (PPPP)

Zuletzt führt die ASA die Einträge der Netzwerk-ACL in die dynamisch generierte Netzwerk-ACL zusammen und gibt dann den Namen der dynamischen Netzwerk-ACL als neue Netzwerk-ACL zurück, die wie in Tabelle 9 gezeigt durchgesetzt werden muss.

Tabelle 9. Dynamische DAP-Netzwerk-ACL

DAP-Netzwerk-ACL-Name	Netzwerk-ACL-Eintrag
DAP-Netzwerk-ACL-1	DDDD DDD PPPP PPP DDDD PPP

DAP-Implementierung

Es gibt eine Vielzahl von Gründen, warum ein Administrator die Implementierung von DAP in Betracht ziehen muss. Zu den Gründen gehört, wann eine Statusüberprüfung eines Endpunkts durchgesetzt werden soll und/oder wann bei der Autorisierung des Benutzerzugriffs auf Netzwerkressourcen detailliertere AAA- oder Richtlinienattribute zu berücksichtigen sind. Im nächsten Beispiel können Sie DAP und seine Komponenten konfigurieren, um einen verbundenen Endpunkt zu identifizieren und den Benutzerzugriff auf verschiedene Netzwerkressourcen zu autorisieren.

Testfall: Ein Kunde hat eine Machbarkeitsstudie mit folgenden VPN-Zugriffsanforderungen angefordert:

- Die Fähigkeit, ein Mitarbeiterendgerät als verwaltet oder nicht verwaltet zu erkennen. - Wenn der Endpunkt als verwalteter (Arbeits-PC) identifiziert wird, aber die Statusanforderungen nicht erfüllt, muss diesem Endpunkt der Zugriff verweigert werden. Wenn dagegen das Endgerät des Mitarbeiters als nicht verwaltet (Heim-PC) identifiziert wird, muss diesem Endgerät der Client-lose Zugriff gewährt werden.
- Die Möglichkeit, die Bereinigung von Sitzungscookies und den Cache aufzurufen, wenn eine clientlose Verbindung beendet wird.

- Erkennen und Durchsetzen von laufenden Anwendungen auf verwalteten Mitarbeiterendpunkten wie McAfee AntiVirus. Wenn die Anwendung nicht vorhanden ist, muss diesem Endpunkt der Zugriff verweigert werden.
- Möglichkeit zur AAA-Authentifizierung zur Bestimmung der Netzwerkressourcen, auf die autorisierte Benutzer Zugriff haben müssen Die Sicherheits-Appliance muss die native MS LDAP-Authentifizierung und mehrere LDAP-Gruppenmitgliedschaftsrollen unterstützen.
- Die Möglichkeit, lokalen LAN-Zugriff auf Netzwerkressourcen wie Netzwerkfaxe und Drucker zuzulassen, wenn die Verbindung über eine Client-/Netzwerkverbindung erfolgt.
- Möglichkeit zur Bereitstellung von autorisiertem Gastzugriff für Auftragnehmer Auftragnehmer und ihre Endgeräte müssen clientlosen Zugriff erhalten, und ihr Portalzugriff auf Anwendungen muss im Vergleich zum Mitarbeiterzugriff eingeschränkt werden.

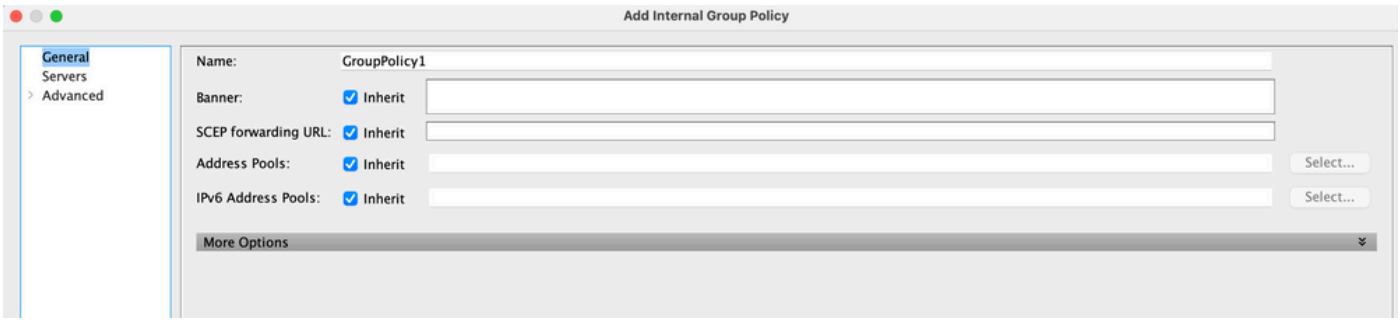
In diesem Beispiel können Sie eine Reihe von Konfigurationsschritten ausführen, um die VPN-Zugriffsanforderungen des Clients zu erfüllen. Möglicherweise sind Konfigurationsschritte erforderlich, die jedoch nicht direkt mit dem DAP in Zusammenhang stehen, während andere Konfigurationen direkt mit dem DAP in Verbindung stehen können. Die ASA ist sehr dynamisch und kann sich an viele Netzwerkumgebungen anpassen. Dadurch können VPN-Lösungen auf verschiedene Weise definiert werden und stellen in einigen Fällen dieselbe Endlösung bereit. Der gewählte Ansatz hängt jedoch von den Kundenanforderungen und deren Umgebungen ab.

Basierend auf der in diesem Whitepaper vorgestellten Struktur und den definierten Client-Anforderungen können Sie den Adaptive Security Device Manager (ASDM) verwenden und die meisten unserer Konfigurationen auf das DAP konzentrieren. Sie können jedoch auch lokale Gruppenrichtlinien konfigurieren, um anzuzeigen, wie das DAP lokale Richtlinienattribute ergänzen und/oder überschreiben kann. Für diesen Testfall können Sie davon ausgehen, dass eine LDAP-Servergruppe, eine Split Tunneling-Netzwerkliste und grundlegende IP-Verbindungen, einschließlich IP-Pools und die DefaultDNS-Servergruppe, vorkonfiguriert sind.

Definieren einer Gruppenrichtlinie - Diese Konfiguration ist zum Definieren von Attributen für lokale Richtlinien erforderlich. Einige der hier definierten Attribute (z. B. lokaler LAN-Zugang) können in DAP nicht konfiguriert werden. (Diese Richtlinie kann auch zum Definieren von clientlosen und clientbasierten Attributen verwendet werden.)

Navigieren Sie zuConfiguration > Remote Access VPN > Network (Client) Access > Group Policies, und fügen Sie eine interne Gruppenrichtlinie wie folgt hinzu:

Abbildung 17: Gruppenrichtlinie - Definition lokaler VPN-spezifischer Attribute.



a. Konfigurieren Sie unter dem Link General (Allgemein) den Namen SSLVPN_GP für die Gruppenrichtlinie.

b. Klicken Sie außerdem unter dem Link Allgemein auf Weitere Optionen, und konfigurieren Sie nur das Tunneling-Protokoll:Clientless SSL VPN. (Sie können DAP so konfigurieren, dass die Zugriffsmethode überschrieben und verwaltet wird.)

c. Konfigurieren Sie unter dem Link Advanced > Split Tunneling die folgenden Schritte:

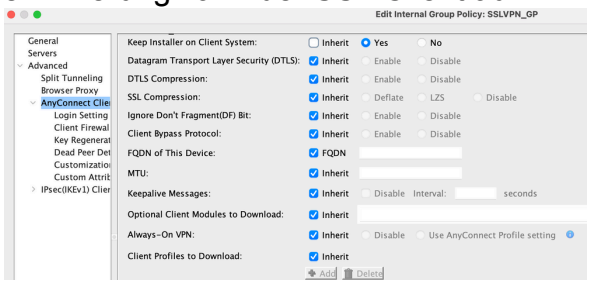
   Abbildung 18: Split-Tunneling - Ermöglicht die Umgehung eines unverschlüsselten Tunnels durch den angegebenen Datenverkehr (lokales Netzwerk) während einer Client-Verbindung.

   a. Richtlinie: Deaktivieren Sie Vererbung, und wählen Sie Netzwerkliste ausschließen aus.

   b. Netzwerkliste: Deaktivieren Sie Vererbung, und wählen Sie den Listennamen Local_LAN_Access aus. (Vorausgesetzt, sie ist vorkonfiguriert.)

d. Konfigurieren Sie unter dem Link Erweitert > ANYCONNECT Client die folgenden Schritte:

   Abbildung 19: SSL VPN Client Installer - Bei VPN-Terminierung kann der SSL Client auf dem Endgerät verbleiben oder deinstalliert werden.



e. Installationsprogramm auf Client-System beibehalten: Deaktivieren Sie Vererbung, und wählen Sie dann Ja aus.

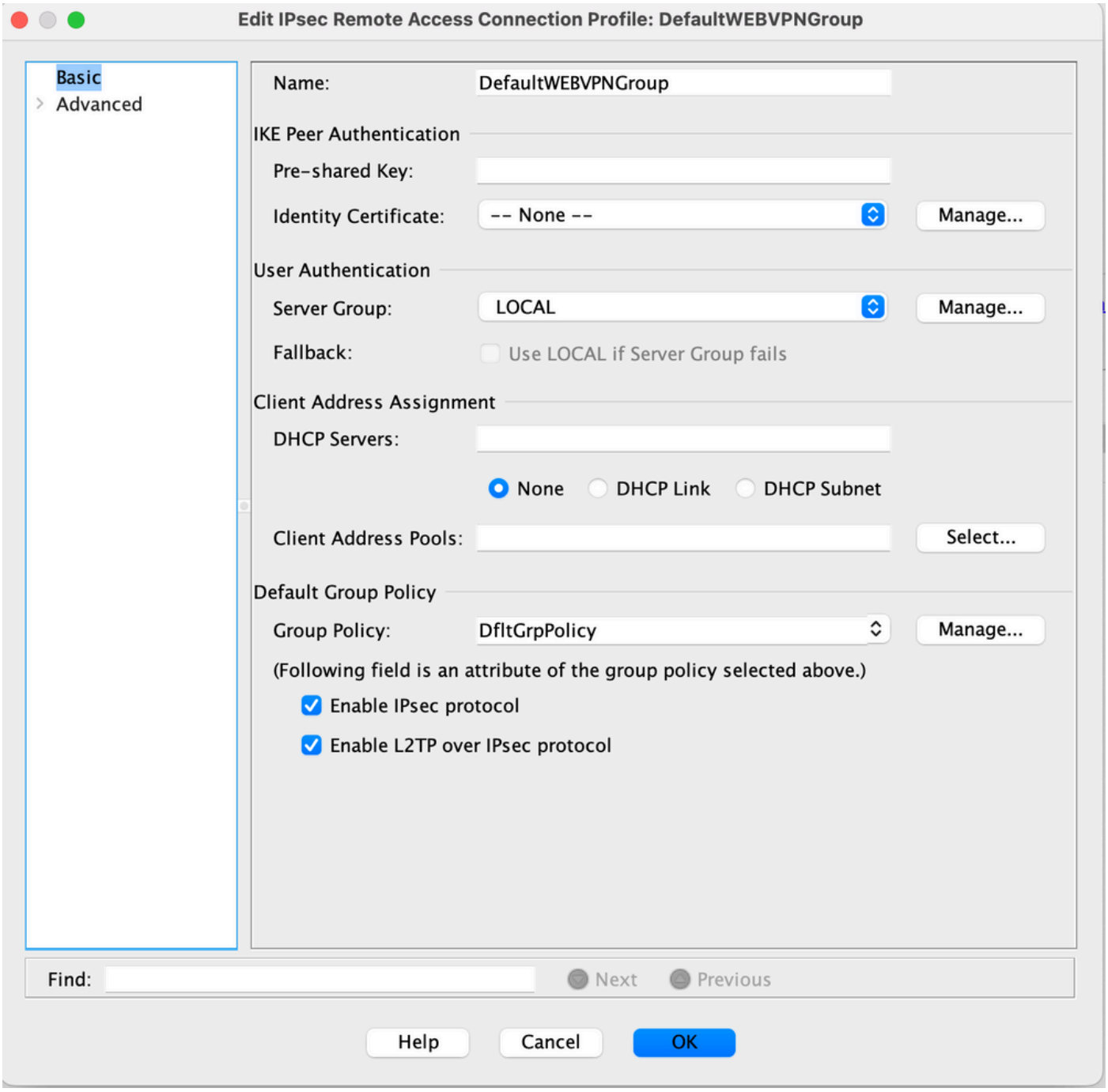
f. Klicken Sie auf OK und dann auf Übernehmen.

g. Wenden Sie Ihre Konfigurationsänderungen an.

Definieren eines Verbindungsprofils - Diese Konfiguration ist erforderlich, um unsere AAA-Authentifizierungsmethode, z. B. LDAP, zu definieren und die zuvor konfigurierte Gruppenrichtlinie (SSL VPN_GP) auf dieses Verbindungsprofil anzuwenden. Benutzer, die über dieses Verbindungsprofil eine Verbindung herstellen, können die hier definierten Attribute sowie die in der SSL VPN_GP-Gruppenrichtlinie definierten Attribute verwenden. (Dieses Profil kann auch verwendet werden, um clientlose und clientbasierte Attribute zu definieren.)

Navigieren Sie zuConfiguration > Remote Access VPN > Network (Client) Access > IPsec Remote Access Connection Profile, und konfigurieren Sie:

Abbildung 20: Verbindungsprofil - Definiert lokale VPN-spezifische Attribute.



a. Bearbeiten Sie im Abschnitt "Connection Profiles" (Verbindungsprofile) die DefaultWEBVPNGroup (Standard-WEBVPN-Gruppe), und konfigurieren Sie unter dem Link Basic (Grundlegend) die folgenden Schritte:

   a. Authentication (Authentifizierung) - Methode: AAA

   b. Authentication - AAA-Servergruppe:LDAP(vorausgesetzt, vorkonfiguriert)

   c. Client-Adressenzuweisung - Client-Adresspools:IP_Pool(vermutlich vorkonfiguriert)

   d. Standard-Gruppenrichtlinie - Gruppenrichtlinie: Wählen Sie SSL VPN_GP aus.

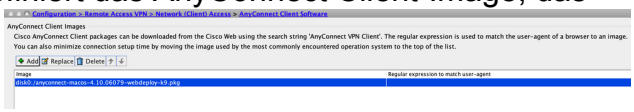
b. Wenden Sie Ihre Konfigurationsänderungen an.

Definieren einer IP-Schnittstelle für SSL-VPN-Verbindungen - Diese Konfiguration ist erforderlich,

um Client- und Clientless-SSL-Verbindungen an einer angegebenen Schnittstelle zu terminieren.

Bevor Sie den Client/Network-Zugriff auf einer Schnittstelle aktivieren, müssen Sie zunächst ein SSL VPN Client-Image definieren.

1. Navigieren Sie zuConfiguration > Remote Access VPN > Network (Client)Access > AnyConnect Client Software, und fügen Sie das nächste Image, das SSL VPN Client-Image, aus dem ASA Flash-Dateisystem hinzu: (Dieses Image kann von CCO heruntergeladen werden, https://www.cisco.com)

   Abbildung 21: SSL VPN Client Image Install - Definiert das AnyConnect Client-Image, das per Push an die Endgeräte angeschlossen wird. 

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

   b. Klicken Sie auf OK, erneut auf OK und dann auf Anwenden.

2. Navigieren Sie zu Configuration > Remote Access VPN > Network (Client)Access > AnyConnect Connection Profiles, und aktivieren Sie mit den folgenden Schritten:

   Abbildung 22: SSL VPN Access Interface (SSL-VPN-Zugriffsschnittstelle) - Definiert die Schnittstelle(en) zum Terminieren der SSL VPN-Verbindung. 

   a. Aktivieren Sie im Abschnitt "Access Interface" (Zugriffsoberfläche) den Zugriff des Cisco AnyConnect VPN Clients oder des älteren SSL VPN Clients auf die in der Tabelle unten ausgewählten Schnittstellen.

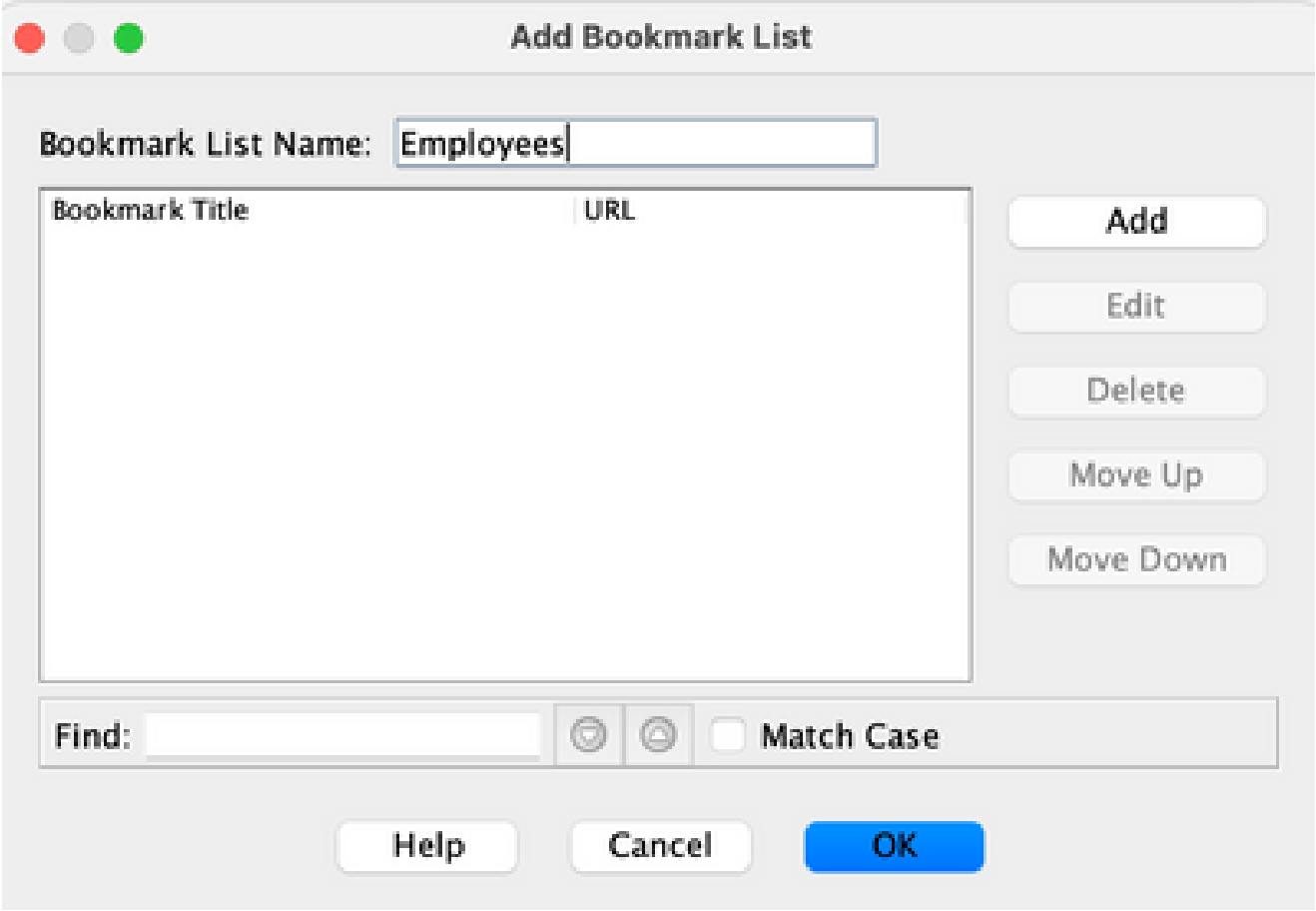
   b. Aktivieren Sie außerdem im Abschnitt "Access Interfaces" das Kontrollkästchen Allow Access on the outside interface. (Mit dieser Konfiguration kann auch der SSL VPN Clientless-Zugriff auf der externen Schnittstelle aktiviert werden.)

   c. Klicken Sie auf Anwenden.

Definieren von Lesezeichenlisten (URL-Listen) für Clientless Access - Diese Konfiguration ist erforderlich, um eine webbasierte Anwendung zu definieren, die im Portal veröffentlicht werden soll. Sie können zwei URL-Listen definieren, eine für Mitarbeiter und die andere für Auftragnehmer.

1. Navigieren Sie zuConfiguration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks, klicken Sie auf + Hinzufügen, und konfigurieren Sie die folgenden Schritte:

   Abbildung 23: Bookmark List (Lesezeichenliste): Definiert URLs, die veröffentlicht werden und auf die vom Webportal aus zugegriffen werden kann. (Benutzerdefiniert für Mitarbeiterzugriff).



a. Lesezeichen-Listenname:Mitarbeiter, und klicken Sie dann auf Hinzufügen.

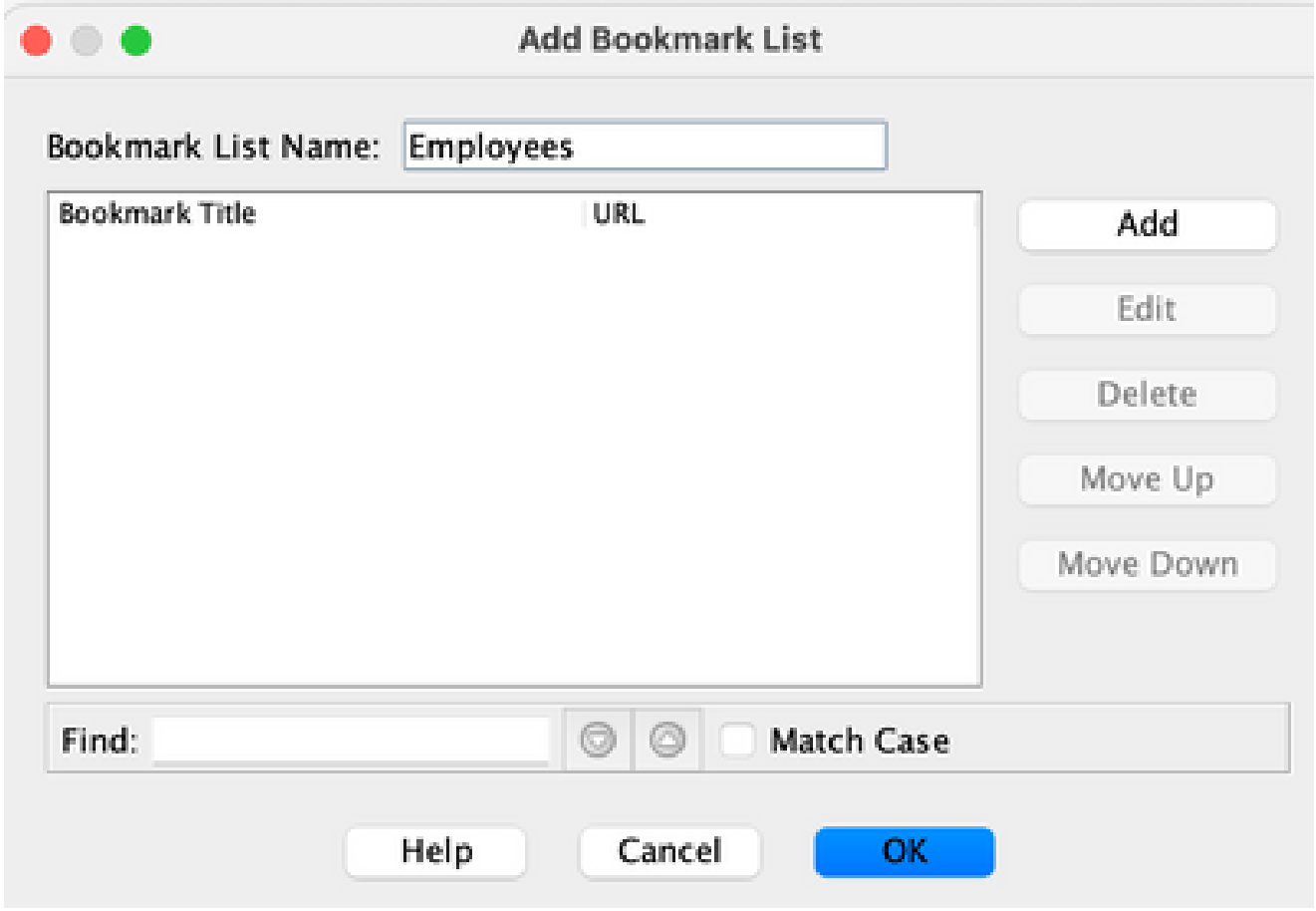
b. Lesezeichen-Titel:Unternehmens-Intranet

c. URL-Wert: https://company.resource.com

- Klicken Sie auf OK und dann erneut auf OK.

- Klicken Sie auf + Hinzufügen, und konfigurieren Sie eine zweite Lesezeichenliste (URL-Liste) wie folgt:

Abbildung 24: Lesezeichenliste - Für Gastzugriff angepasst.



a.

Lesezeichen-Listenname:**Auftragnehmer**, und **klicken Sie** dann **auf Hinzufügen**.

b.

Lesezeichentitel: **Gastzugriff**

c.

URL-Wert: https://company.contractors.com

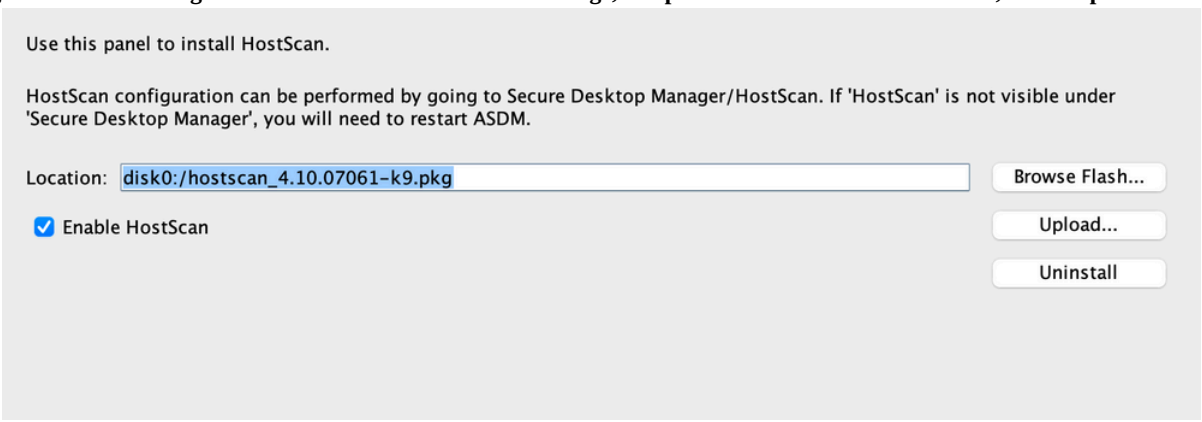
- Klicken Sie auf OK und dann erneut auf OK.

- **Klicken Sie auf Anwenden**.

Host-Scan konfigurieren:

- Navigieren Sie **zu Configuration > Remote Access VPN > Secure Desktop Manager > HostScan Image,** und konfigurieren Sie die nächsten Schritte:

Abbildung 25: HostScan Image Install - Definiert das HostScan-Image, das per Push verbunden werden soll, um Endpunkte zu verbinden.



a. Installieren Sie **disk0:/hostscan_4.xx.xxxxx-k9.**pkgimage vom ASA-Flash-Dateisystem.

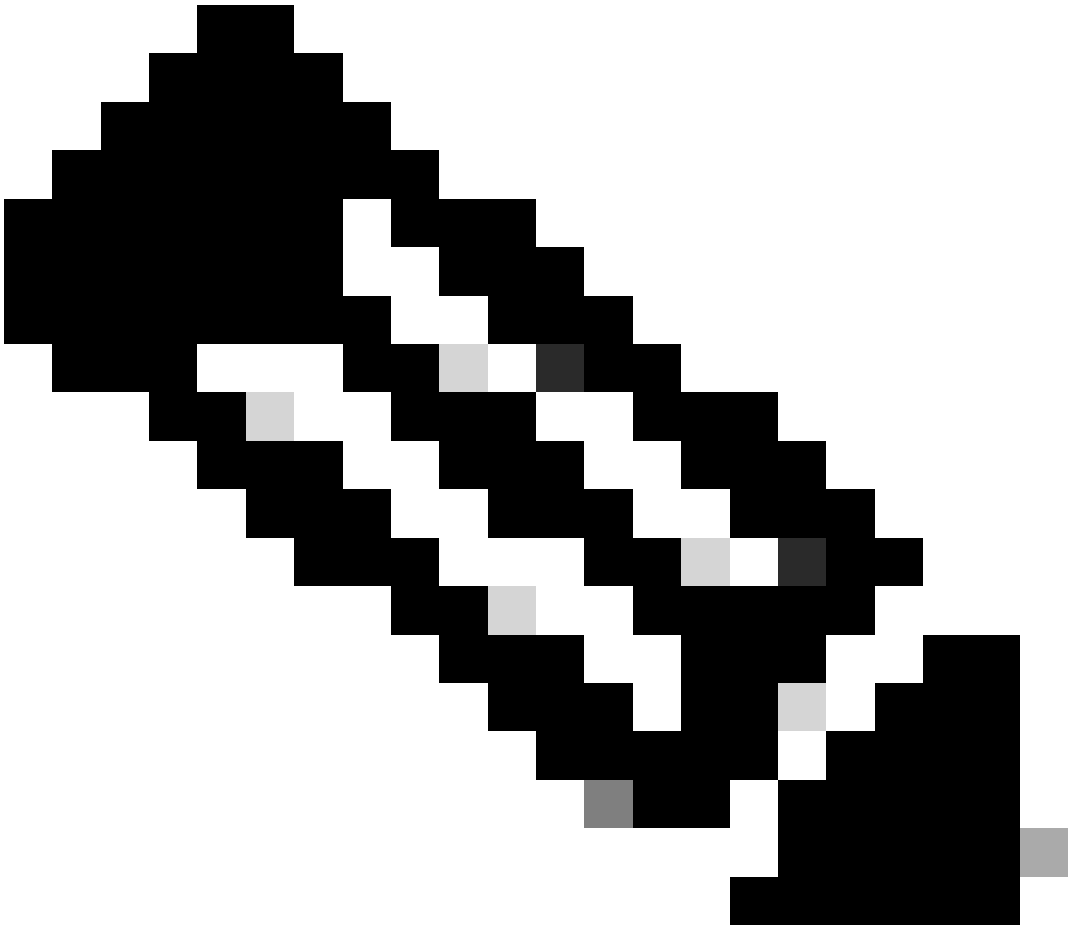
b. **AktivierenHostScan aktivieren**.

c. **Klicken Sie auf Anwenden**.

Dynamische Zugriffsrichtlinien - Diese Konfiguration ist erforderlich, um die Benutzer und ihre Endpunkte, die eine Verbindung herstellen, anhand definierter AAA- und/oder Endpunkt-Bewertungskriterien zu validieren. Wenn die definierten Kriterien eines DAP-Datensatzes erfüllt sind, können angeschlossene Benutzer auf Netzwerkressourcen zugreifen, die diesem oder diesen DAP-Datensatz zugeordnet sind. Die DAP-Autorisierung wird während des Authentifizierungsprozesses ausgeführt.

Um sicherzustellen, dass eine SSL-VPN-Verbindung im Standardfall beendet werden kann (z. B. wenn der Endpunkt nicht mit einer

konfigurierten Richtlinie für den dynamischen Zugriff übereinstimmt), können Sie sie wie folgt konfigurieren:

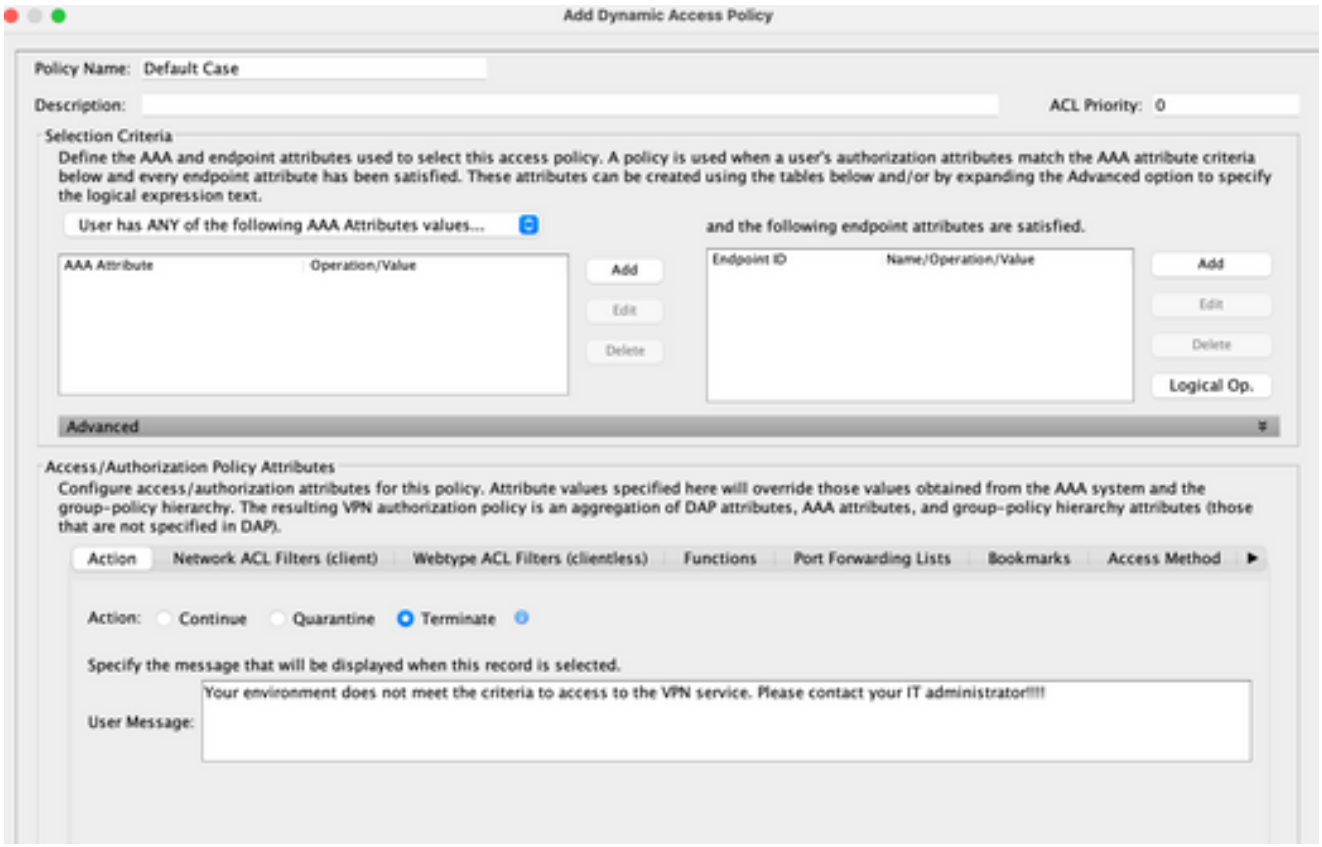


Hinweis: Bei der erstmaligen Konfiguration dynamischer Zugriffsrichtlinien wird eine DAP.xml-Fehlermeldung angezeigt, die besagt, dass keine DAP-Konfigurationsdatei (DAP.XML) vorhanden ist. Sobald die ursprüngliche DAP-Konfiguration geändert und gespeichert wurde, kann diese Meldung nicht mehr angezeigt werden.

•

Navigieren Sie **zuConfiguration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies**, und konfigurieren Sie die folgenden Schritte:

Abbildung 30: Dynamische Standard-Zugriffsrichtlinie - Wenn keine vordefinierten DAP-Datensätze zugeordnet werden, kann dieser DAP-Datensatz durchgesetzt werden. Daher kann der SSL VPN-Zugriff verweigert werden.



a.

Bearbeiten Sie die DfltAccessPolicy, und legen Sie die Action **auf Terminate fest**.

b.

Klicken Sie auf OK.

•

Fügen Sie eine neue dynamische Zugriffsrichtlinie **mit dem NamenManaged_Endpoints** hinzu:

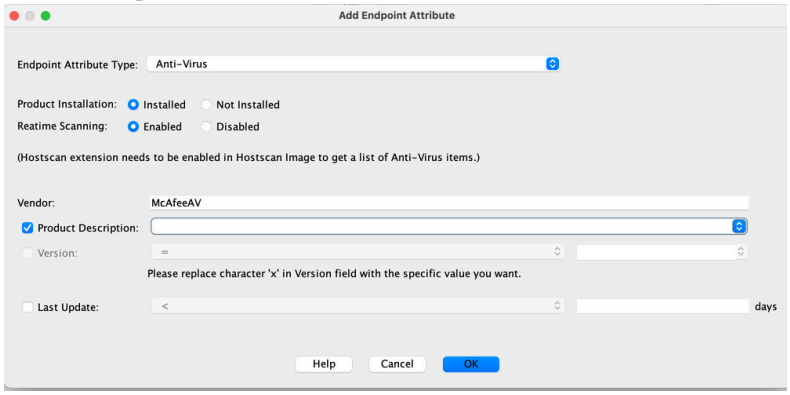
a.

Beschreibung: **Employee Client Access**

b.

Fügen Sie einen Endpunkt-Attributtyp (Anti-Virus) hinzu, wie in Abbildung 31 dargestellt. Klicken Sie abschließend auf OK.

Abbildung 31: DAP Endpoint Attribute - Advanced Endpoint Assessment AntiVirus kann als DAP-Kriterium für Client-/Netzwerkzugriff verwendet werden.



c.

Wählen Sie aus der Dropdown-Liste im Abschnitt "AAA-Attribut" die Option aus, wie im vorherigen Bild gezeigtUser has ALL of the following AAA Attributes Values.

•

Fügen Sie rechts neben dem Feld AAA-Attribut einen AAA-Attributtyp (LDAP) hinzu (siehe Abbildungen 33 und 34). Klicken Sie abschließend auf OK.

Abbildung 33: DAP AAA-Attribut - Die AAA-Gruppenmitgliedschaft kann als DAP-Kriterium zur Identifizierung eines Mitarbeiters verwendet werden.

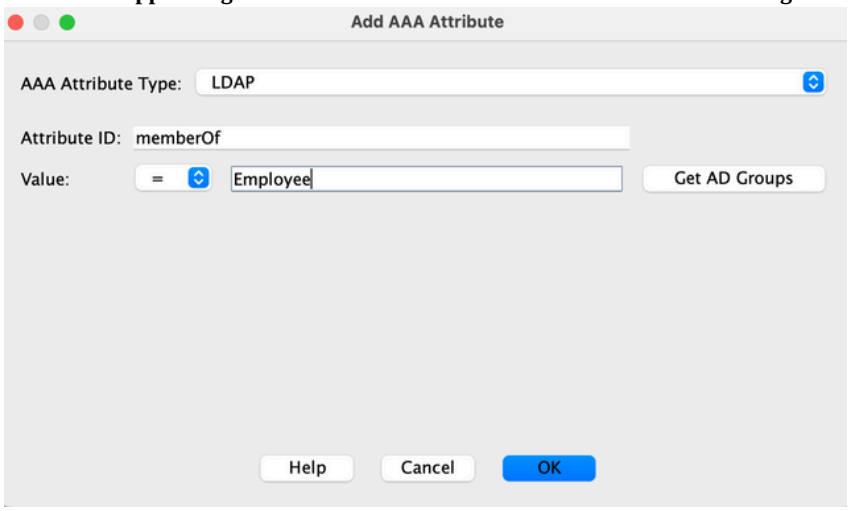
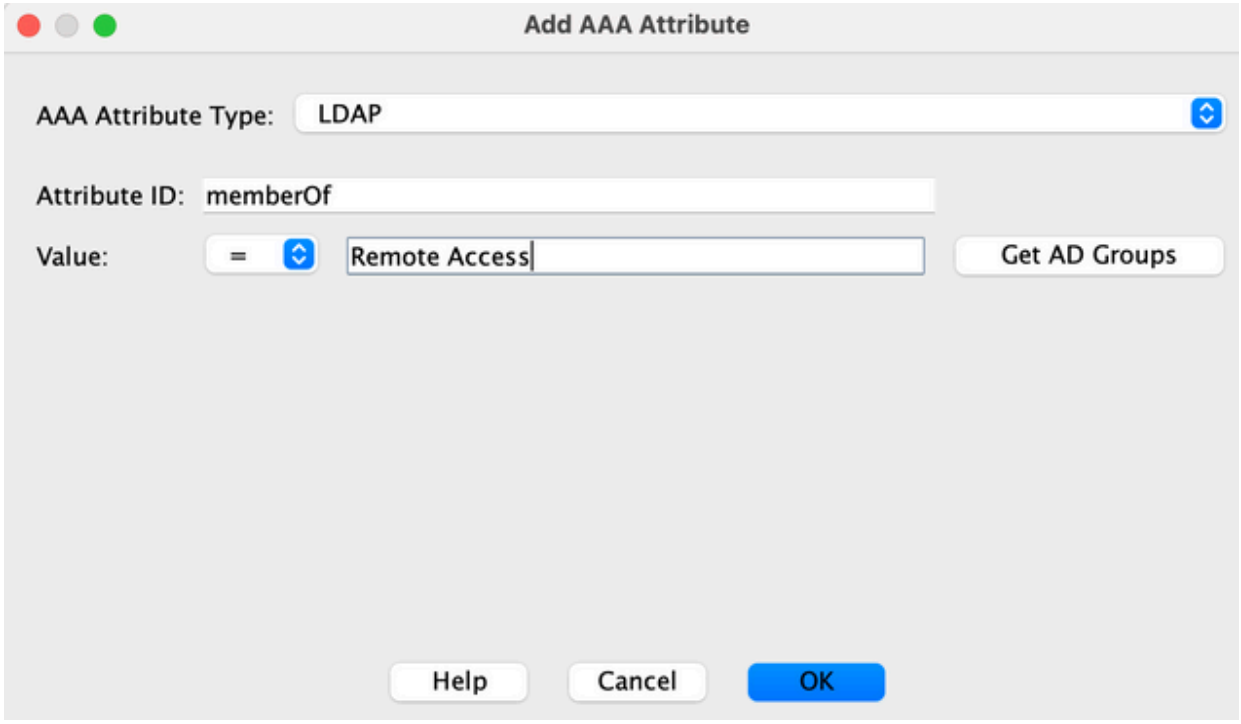


Abbildung 34: DAP AAA-Attribut - Die AAA-Gruppenmitgliedschaft kann als DAP-Kriterium verwendet werden, um Remote-Zugriffsfunktionen zuzulassen.



-

Überprüfen Sie auf der Registerkarte Action (Aktion), ob Action (Aktion) **auf Continue (Fortsetzen)** eingestellt ist, wie in Abbildung 35 dargestellt.

Abbildung 35: Registerkarte "Aktion" - Diese Konfiguration ist erforderlich, um die spezielle Verarbeitung für eine bestimmte Verbindung oder Sitzung festzulegen. Der VPN-Zugriff kann verweigert werden, wenn ein DAP-Datensatz zugeordnet und die Aktion auf Terminate (Beenden) festgelegt ist.

-

Wählen Sie auf der Registerkarte Access Method die Option Access **MethodAnyConnect Client aus**, wie in Abbildung 36 dargestellt.

Abbildung 36: Registerkarte Access Method (Zugriffsmethode): Diese Konfiguration ist zum Definieren der Verbindungstypen für den SSL VPN-Client erforderlich.

-

Klicken Sie auf OK und **dann auf Anwenden**.

-

Fügen Sie eine zweite dynamische Zugriffsrichtlinie **mit dem Namen Unmanaged_Endpoints** hinzu, wie folgt:

a.

Beschreibung: **Employee Clientless Access**.

b.

Wählen Sie aus der Dropdown-Liste im vorherigen Bild des Abschnitts "AAA-Attribut" die Option User has ALL of the following AAA Attributes Values aus.

-

Fügen Sie rechts neben dem Attributtyp AAA einen Attributtyp AAA (LDAP) hinzu (siehe Abbildungen 38 und 39). Klicken Sie abschließend auf OK.

Abbildung 38: DAP AAA-Attribut - Die AAA-Gruppenmitgliedschaft kann als DAP-Kriterium zur Identifizierung eines Mitarbeiters verwendet werden.

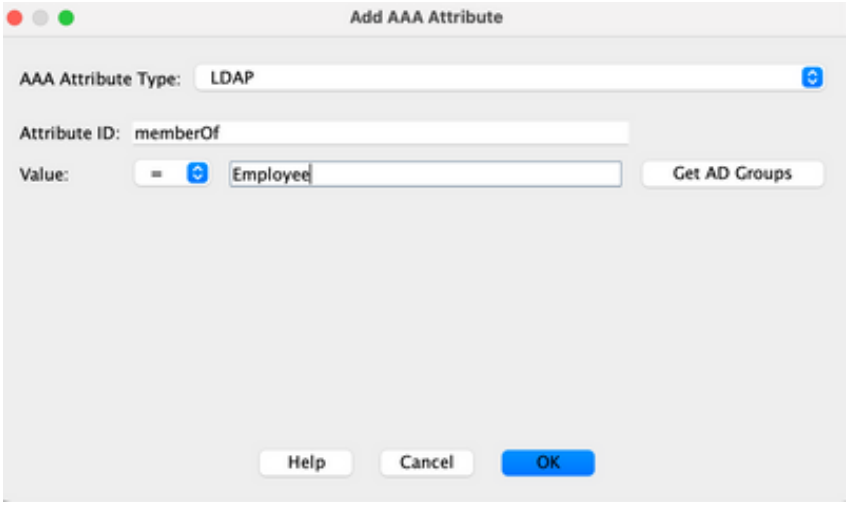
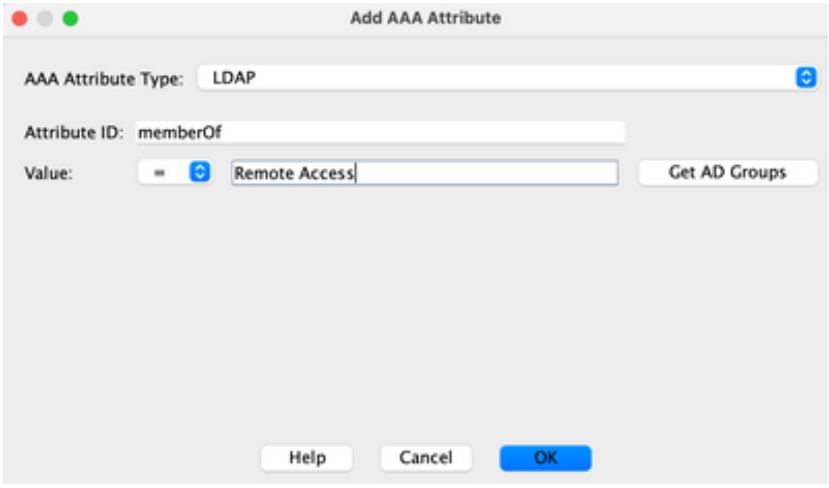


Abbildung 39: DAP AAA-Attribut - Die AAA-Gruppenmitgliedschaft kann als DAP-Kriterium verwendet werden, um Remote-Zugriffsfunktionen zuzulassen.



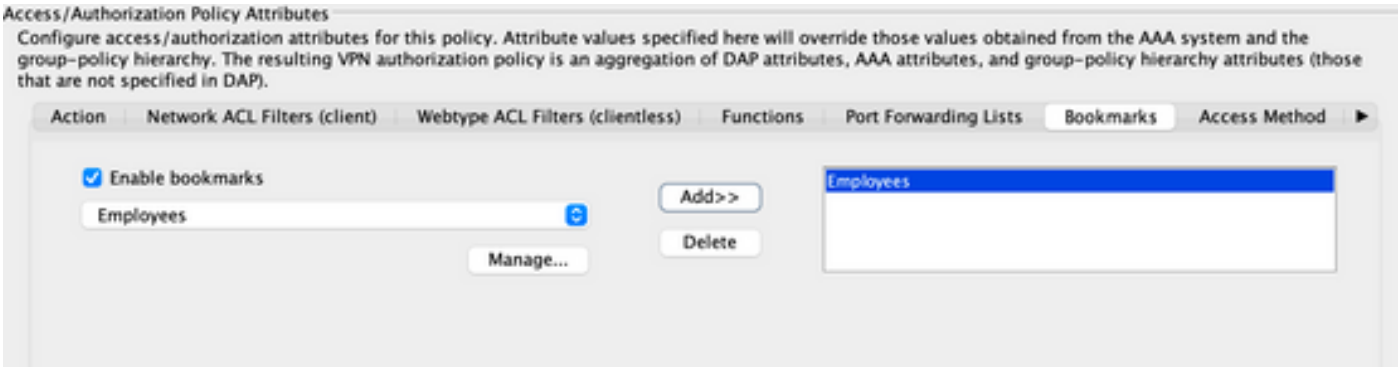
-

Überprüfen Sie auf der Registerkarte Aktion, ob Aktion **auf Weiter** eingestellt ist. (Abbildung 35)

-

Wählen Sie auf der Registerkarte Lesezeichen aus dem Dropdown-Menü den ListennamenEmployees aus, und **klicken Sie** dann **auf Hinzufügen**. Überprüfen Sie außerdem, ob Lesezeichen aktivieren aktiviert ist, wie in Abbildung 40 dargestellt.

Abbildung 40: Lesezeichen: Auf dieser Registerkarte können Sie URL-Listen für Benutzersitzungen auswählen und konfigurieren.



-

a.

Wählen Sie auf der Registerkarte Access Method die Option Access Method **Web Portal aus**. (Abbildung 36)

- **Klicken Sie auf OK** und **dann auf Anwenden**.

1. Auftragnehmer können nur durch DAP-AAA-Attribute identifiziert werden. Daher kann in Schritt 4 nicht der Attributtyp des Endpunkts (Richtlinie) konfiguriert werden. Dieser Ansatz soll nur die Vielseitigkeit innerhalb des DAP aufzeigen.

3. Fügen Sie eine dritte dynamische Zugriffsrichtlinie **mit dem Namen Guest_Access** mit folgendem Inhalt hinzu:

-

Beschreibung: **Guest Clientless Access**.

-

Fügen Sie (rechts neben dem Feld Endpoint Attribute) einen Endpoint Attribute Type (Policy) hinzu (siehe Abbildung 37). Klicken Sie

abschließend auf OK.

- Wählen Sie in Abbildung 40 aus der Dropdown-Liste im AAA-Attributabschnitt die Option User has ALL of the following AAA Attributes Values.

- Fügen Sie rechts neben dem Feld AAA-Attribut einen AAA-Attributtyp (LDAP) hinzu (siehe Abbildungen 41 und 42). Klicken Sie abschließend auf OK.

Abbildung 41: Sie können das AAA-Attribut des DAP verwenden - AAA-Gruppenmitgliedschaft als DAP-Kriterium für die Identifizierung eines Subunternehmers

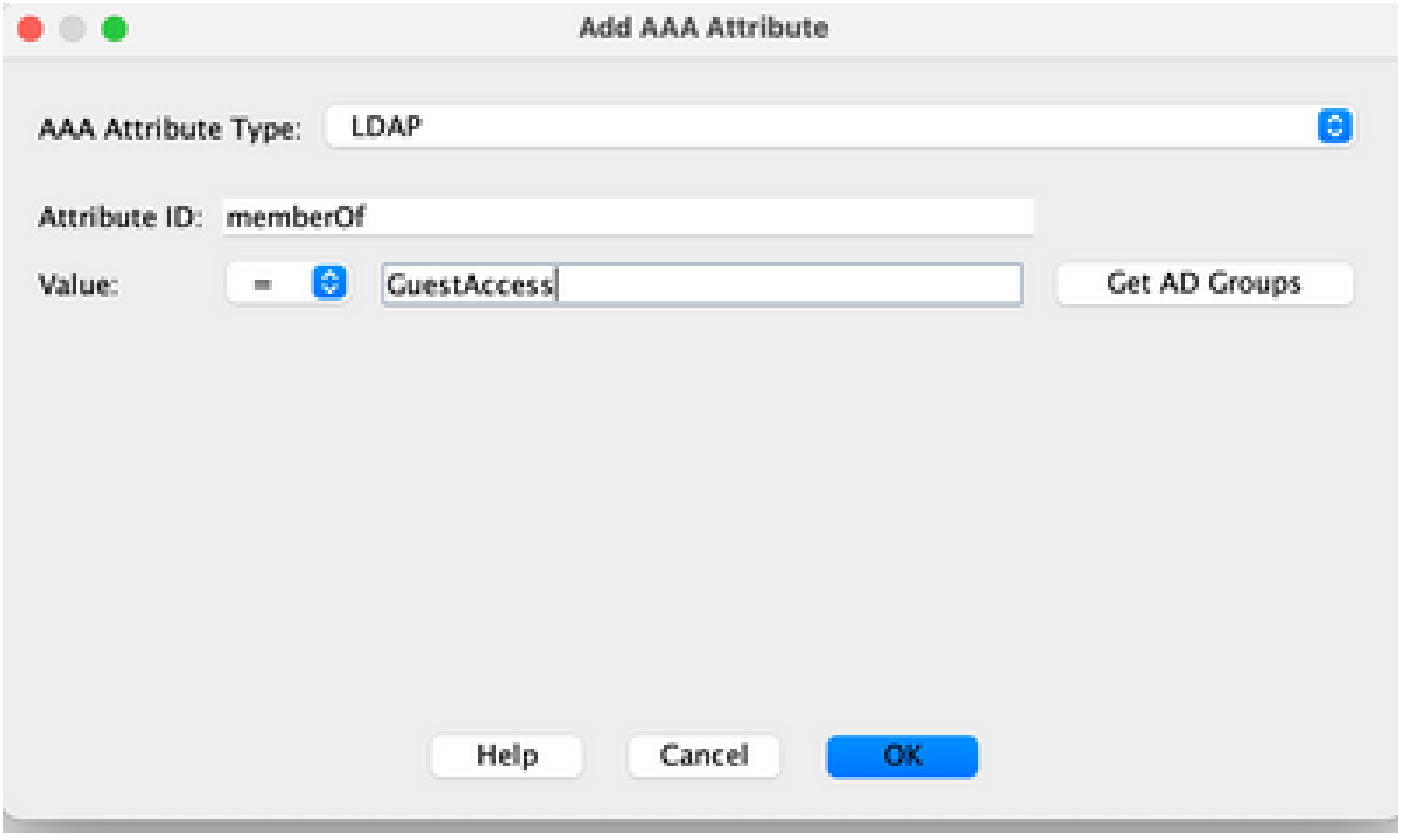
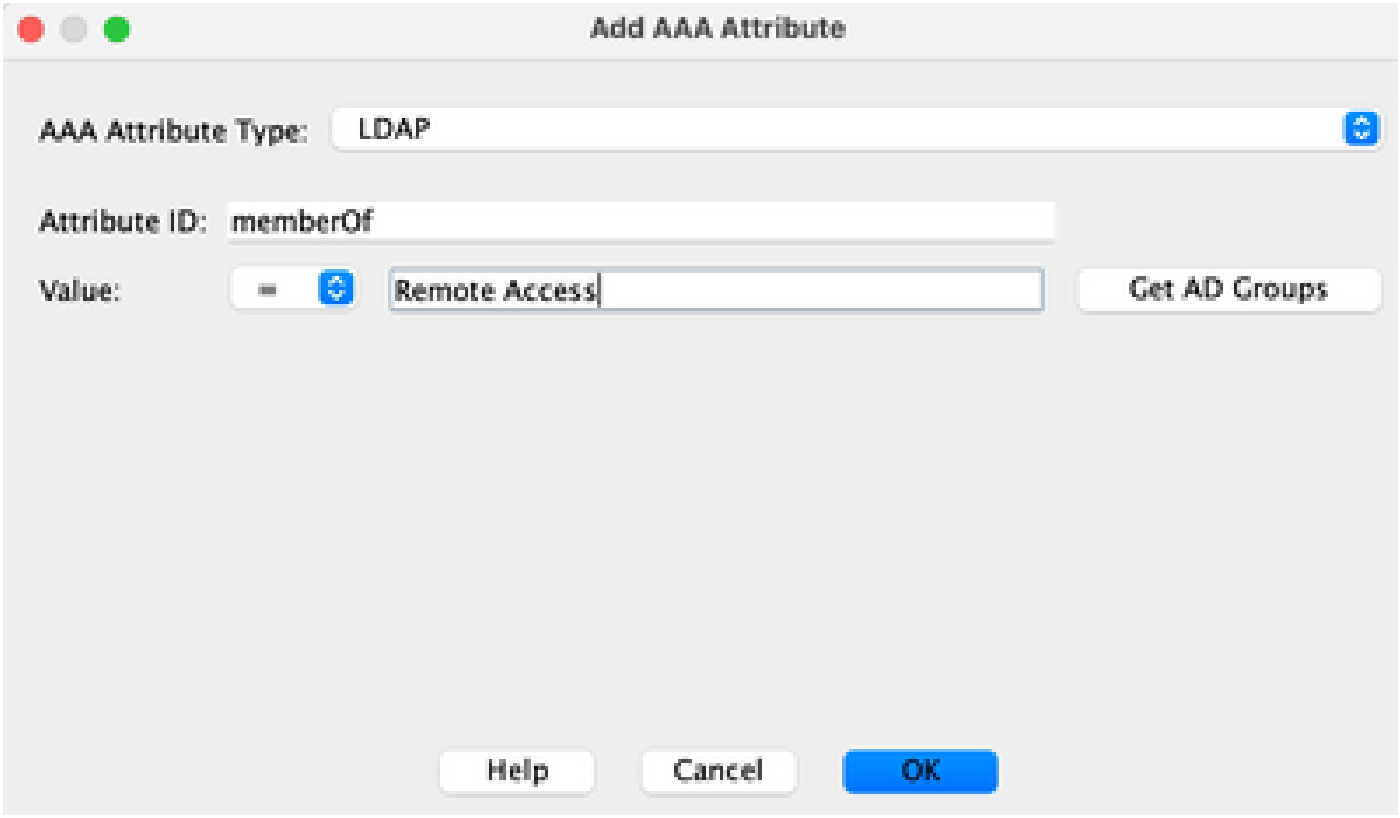


Abbildung 42: DAP AAA-Attribut - Sie können die AAA-Gruppenmitgliedschaft als DAP-Kriterium verwenden, um Remote-Zugriffsfunktionen zuzulassen.



-

a.

Überprüfen Sie auf der Registerkarte Aktion, ob Aktion auf **Weiter** eingestellt ist. (Abbildung 35)

b.

Wählen Sie auf der Registerkarte "Lesezeichen" den Listennamen **Auftragnehmer** aus dem Dropdown-Menü aus, und klicken Sie dann auf Hinzufügen. Überprüfen Sie außerdem, ob **Lesezeichen aktivieren** aktiviert ist. (Siehe Abbildung 40.)

c.

Wählen Sie auf der Registerkarte Access Method die Option Access Method Web Portal aus. (Abbildung 36)

d.

Klicken Sie auf **OK** und dann auf **Anwenden**.

Schlussfolgerung

Basierend auf den in diesem Beispiel genannten SSL-VPN-Anforderungen für den Client Remote Access erfüllt diese Lösung die VPN-Anforderungen für den Client Remote Access.

Da dynamische VPN-Umgebungen immer stärker zusammengeführt werden, können dynamische Zugriffsrichtlinien angepasst und skaliert werden, um häufigen Änderungen der Internetkonfiguration, verschiedenen Benutzerrollen innerhalb einer Organisation und Anmeldungen von verwalteten und nicht verwalteten Remote-Zugriffsstandorten mit unterschiedlichen Konfigurationen und Sicherheitsstufen Rechnung zu tragen.

Dynamische Zugriffsrichtlinien werden durch neue und bewährte Legacy-Technologien ergänzt, darunter Advanced Endpoint Assessment, Host Scan, Secure Desktop, AAA und Richtlinien für lokalen Zugriff. So können Organisationen sicheren VPN-Zugriff auf alle Netzwerkressourcen von jedem Standort aus bereitstellen.

Zugehörige Informationen

- **Technischer Support und Downloads von Cisco**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.