Distribuire ASA 9.X Dynamic Access Policies (DAP)

Sommario

Introduzione

In questo documento vengono descritte la distribuzione, le funzionalità e l'utilizzo delle policy di accesso dinamico (DAP) di ASA 9.x.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Gateway VPN (Virtual Private Network)
- Criteri di accesso dinamico (DAP)

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

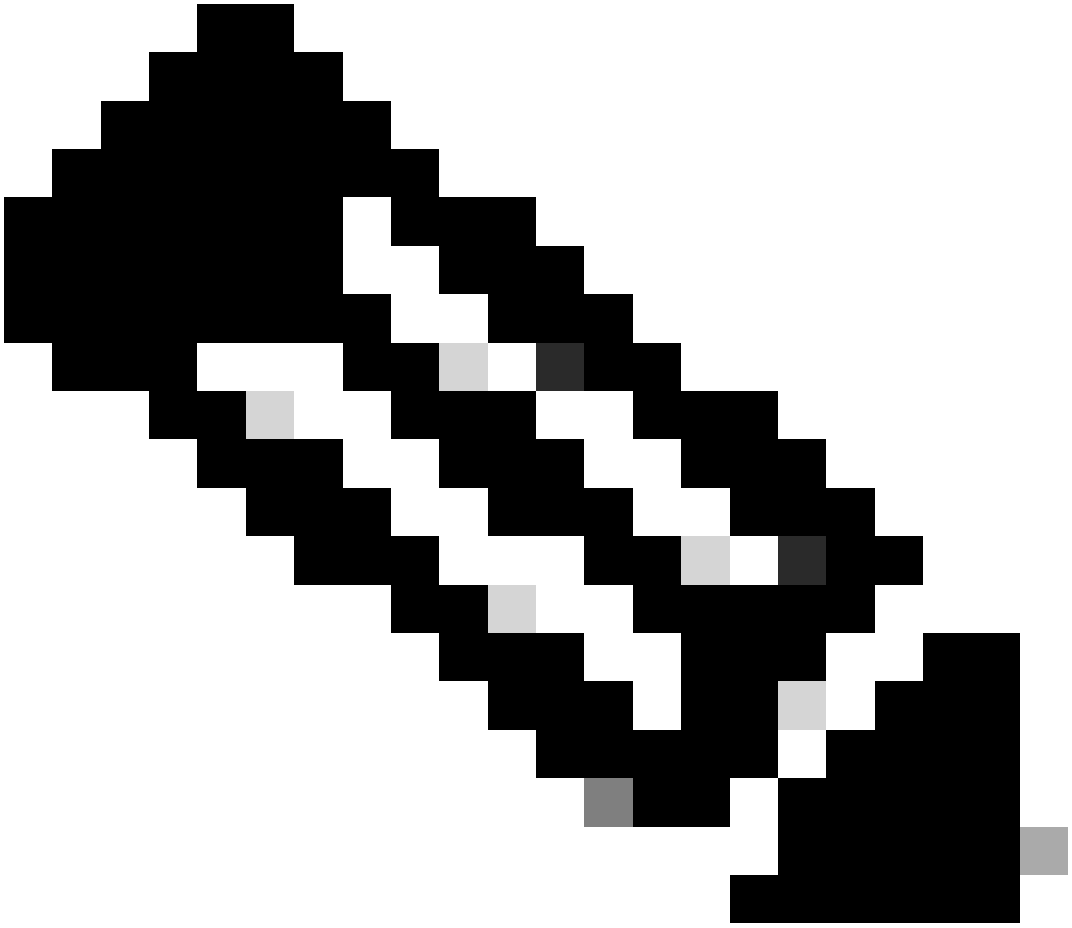
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

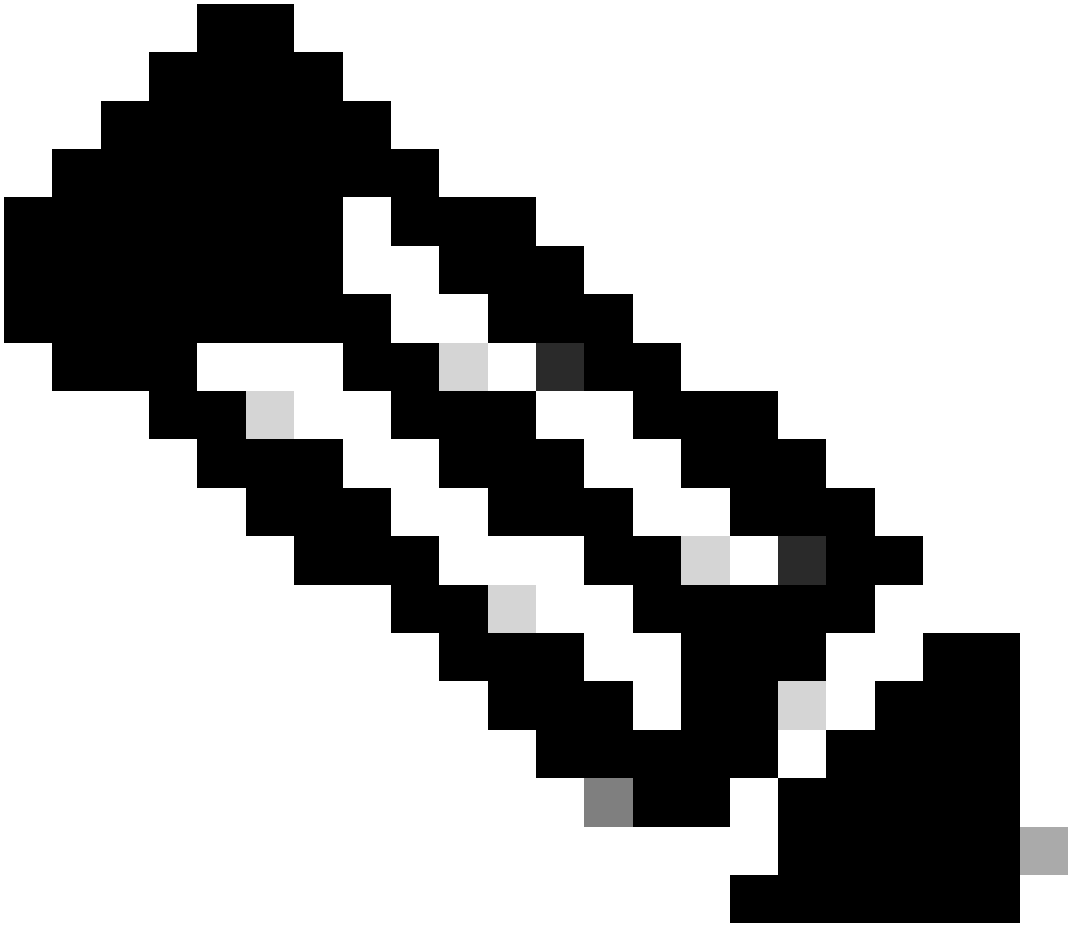
I gateway VPN (Virtual Private Network) funzionano in ambienti dinamici. Più variabili possono influire su ogni connessione VPN; ad esempio, le configurazioni Intranet che cambiano di frequente, i vari ruoli che ogni utente può ricoprire all'interno di un'organizzazione e gli accessi da siti di accesso remoto con configurazioni e livelli di sicurezza diversi. La procedura di autorizzazione degli utenti è molto più complessa in un ambiente VPN dinamico rispetto a una rete con configurazione statica.

I criteri di accesso dinamico (DAP, Dynamic Access Policies) sono una funzionalità che consente di configurare l'autorizzazione in base alle dinamiche degli ambienti VPN. I criteri di accesso dinamico vengono creati impostando un insieme di attributi di controllo di accesso associati a una sessione o a un tunnel utente specifico. Questi attributi consentono di risolvere i problemi relativi all'appartenenza a più gruppi e alla sicurezza degli endpoint.

L'appliance di sicurezza, ad esempio, concede l'accesso a un utente specifico per una determinata sessione in base ai criteri definiti. Genera un DAP durante l'autenticazione dell'utente selezionando e/o aggregando gli attributi da uno o più record DAP. Seleziona questi record DAP in base alle informazioni di sicurezza dell'endpoint del dispositivo remoto e/o alle informazioni di autorizzazione AAA per l'utente autenticato. Il record DAP viene quindi applicato al tunnel o alla sessione utente.



Nota: il file dap.xml, che contiene gli attributi di selezione dei criteri DAP, viene memorizzato nel flash ASA. Benché sia possibile esportare il file dap.xml all'esterno della casella, modificarlo (se si conosce la sintassi XML) e reimportarlo, prestare la massima attenzione in quanto, in caso di configurazione errata di un elemento, ASDM potrebbe interrompere l'elaborazione dei record DAP. Non è disponibile una CLI per modificare questa parte della configurazione.



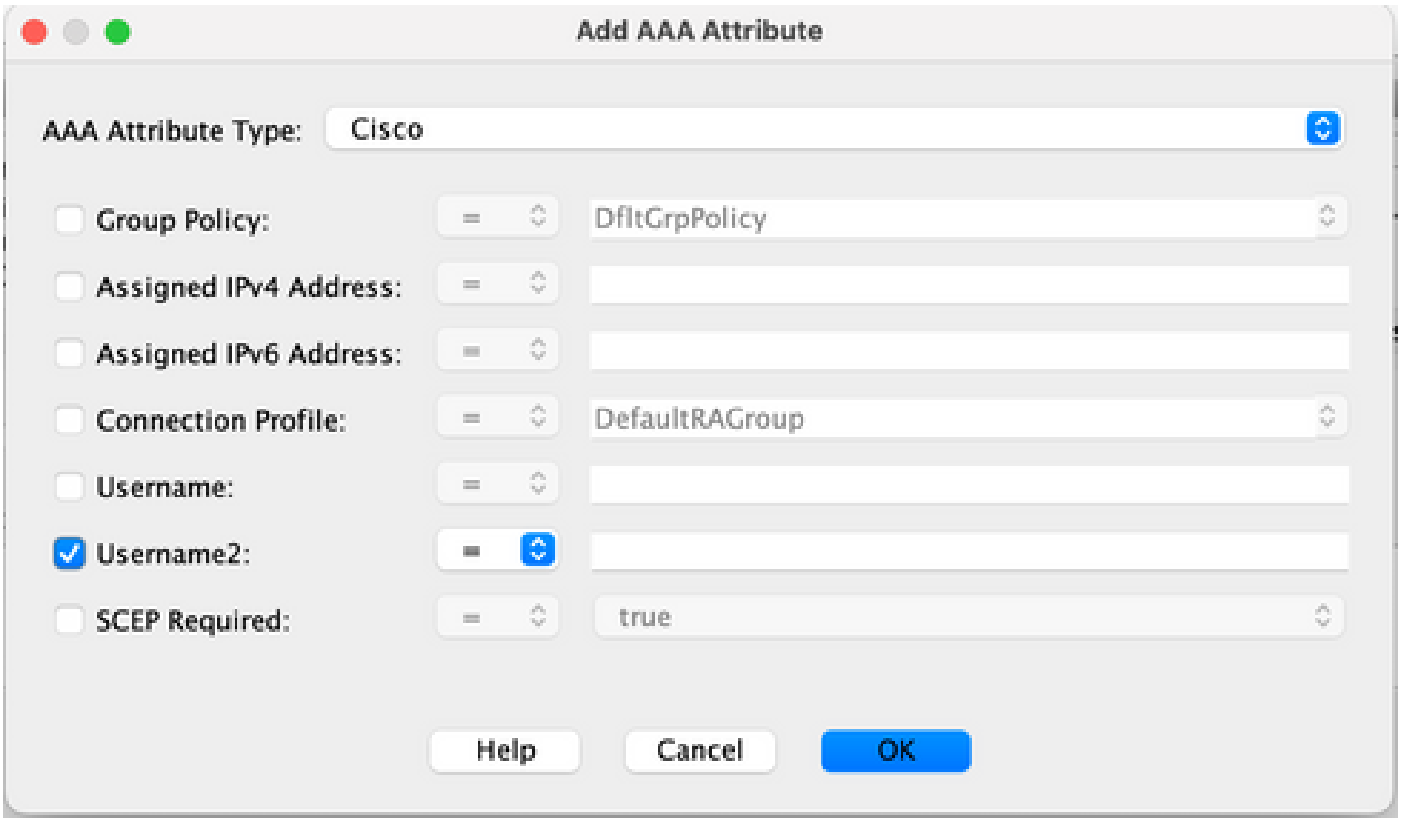
Nota: il tentativo di configurare i parametri di accesso a Dynamic-Access-Policy-Record tramite la CLI può impedire il funzionamento del protocollo DAP, anche se ASDM lo gestirebbe correttamente. Evitare la CLI e utilizzare sempre ASDM per gestire le policy DAP.

Attributi DAP e AAA

DAP integra i servizi AAA e fornisce una serie limitata di attributi di autorizzazione che possono sostituire gli attributi forniti da AAA. L'appliance di sicurezza può selezionare i record DAP in base alle informazioni di autorizzazione AAA per l'utente. L'accessorio di protezione può selezionare più record DAP in base a queste informazioni, che vengono quindi aggregati per assegnare gli attributi di autorizzazione DAP.

È possibile specificare gli attributi AAA dalla gerarchia degli attributi Cisco AAA o dall'insieme completo degli attributi di risposta che l'appliance di sicurezza riceve da un server RADIUS o LDAP, come mostrato nella Figura 1.

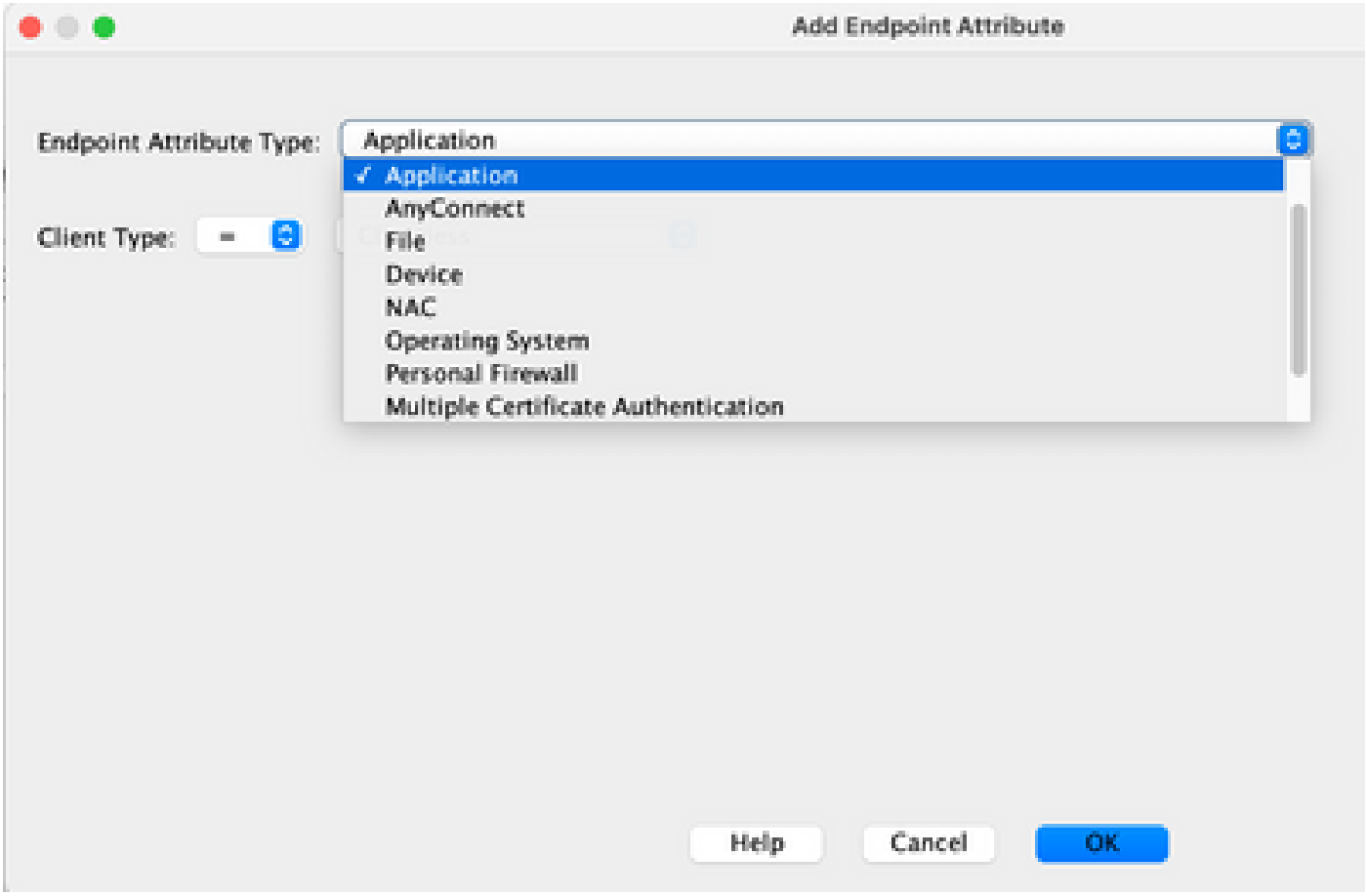
Figura 1. GUI attributo DAP AAA



Attributi DAP e di sicurezza degli endpoint

Oltre agli attributi AAA, l'appliance di sicurezza può ottenere gli attributi di sicurezza dell'endpoint utilizzando i metodi di valutazione della postura configurati dall'utente. tra cui Scan host di base, Secure Desktop, Standard/Advanced Endpoint Assessment e NAC, come mostrato nella Figura 2. Gli attributi di valutazione dell'endpoint vengono ottenuti e inviati all'appliance di sicurezza prima dell'autenticazione dell'utente. Tuttavia, gli attributi AAA, incluso il record DAP complessivo, vengono convalidati durante l'autenticazione dell'utente.

Figura 2. GUI attributo endpoint

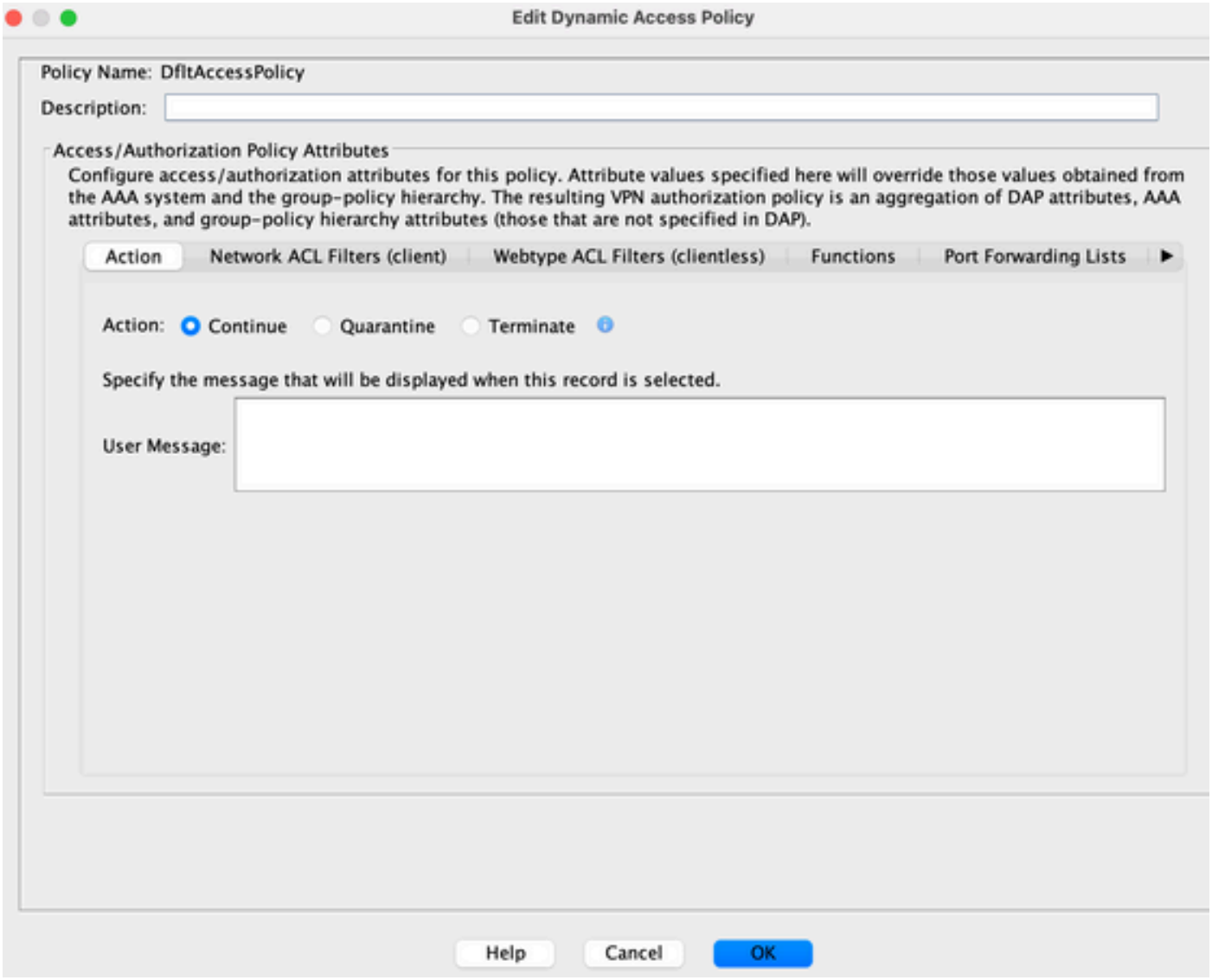


Criterio di accesso dinamico predefinito

Prima dell'introduzione e dell'implementazione del protocollo DAP, le coppie attributo/valore dei criteri di accesso associate a una sessione o a un tunnel utente specifico erano definite localmente sull'appliance ASA (ovvero gruppi di tunnel e criteri di gruppo) o mappate tramite server AAA esterni.

DAP è sempre applicato per impostazione predefinita. Ad esempio, l'applicazione del controllo di accesso tramite gruppi di tunnel, criteri di gruppo e AAA senza l'applicazione esplicita di DAP può ancora ottenere questo comportamento. Per il comportamento legacy, non è necessaria alcuna modifica alla configurazione della funzionalità DAP, incluso il record DAP predefinito, DfltAccessPolicy, come mostrato nella Figura 3.

Figura 3. Criterio di accesso dinamico predefinito



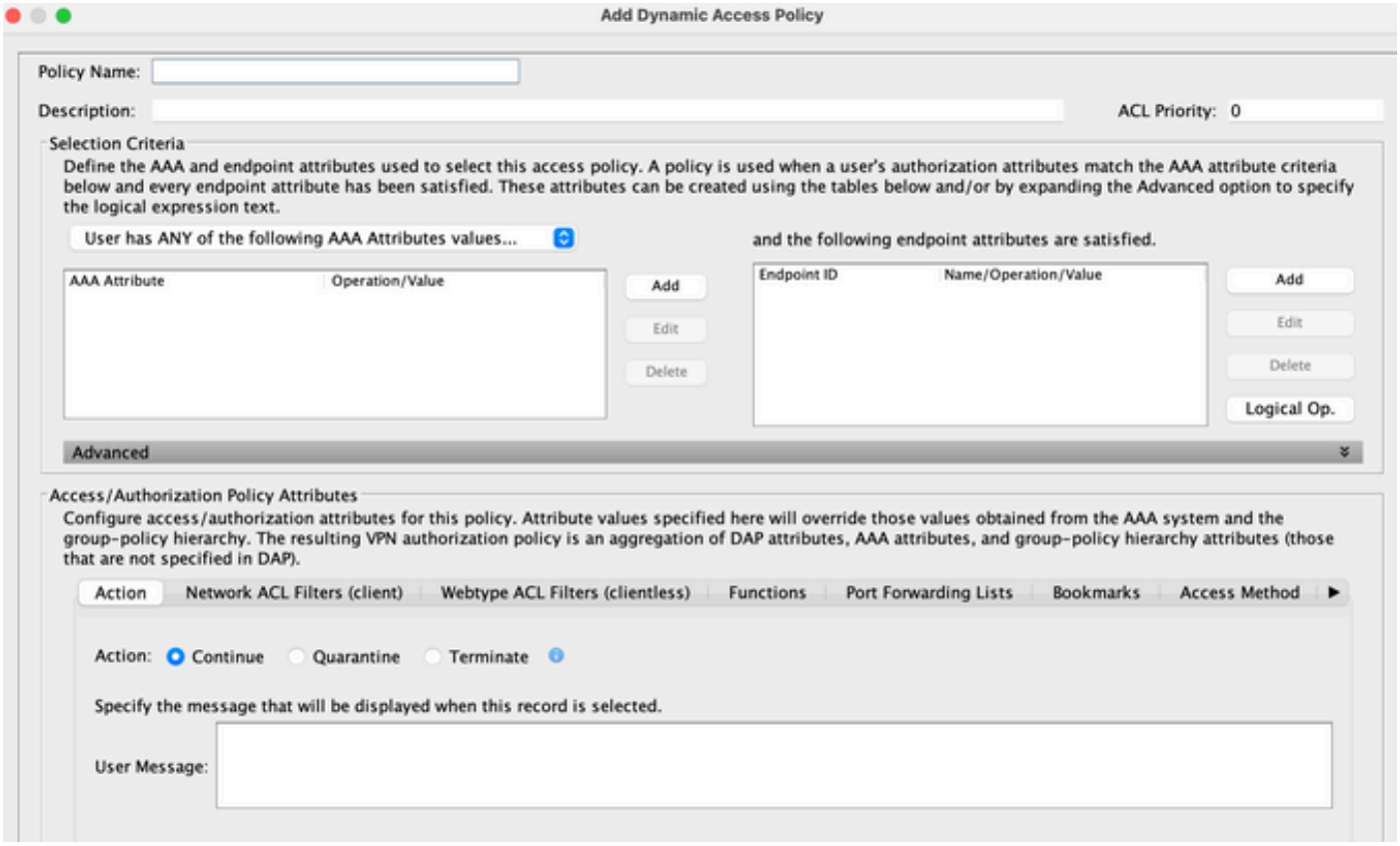
Tuttavia, se uno qualsiasi dei valori predefiniti in un record DAP viene modificato, ad esempio, il parametro Action: in DfltAccessPolicy viene modificato dal valore predefinito in Terminate e non vengono configurati ulteriori record DAP, gli utenti autenticati possono, per impostazione predefinita, corrispondere al record DAP DfltAccessPolicy e l'accesso VPN può essere negato.

Di conseguenza, è necessario creare e configurare uno o più record DAP per autorizzare la connettività VPN e definire quali risorse di rete un utente autenticato è autorizzato ad accedere. Pertanto, se configurato, il protocollo DAP può avere la precedenza sull'applicazione dei criteri legacy.

Configura criteri di accesso dinamico

Quando si utilizza il protocollo DAP per definire le risorse di rete a cui un utente ha accesso, è necessario considerare numerosi parametri. Ad esempio, se si identifica se l'endpoint di connessione proviene da un ambiente gestito, non gestito o non attendibile, determinare i criteri di selezione necessari per identificare l'endpoint di connessione e, in base alla valutazione dell'endpoint e/o alle credenziali AAA, quali risorse di rete l'utente che si connette è autorizzato ad accedere. A tale scopo, è necessario acquisire familiarità con le funzioni e le caratteristiche del punto di accesso dinamico, come illustrato nella Figura 4.

Figura 4. Criterio di accesso dinamico



Quando si configura un record DAP, è necessario considerare due componenti principali:

- Criteri di selezione, incluse le opzioni avanzate
- Attributi dei criteri di accesso

Nella sezione Criteri di selezione un amministratore configura gli attributi AAA e Endpoint utilizzati per selezionare un record DAP specifico. Un record DAP viene utilizzato quando gli attributi di autorizzazione di un utente corrispondono ai criteri degli attributi AAA e ogni attributo dell'endpoint è stato soddisfatto.

Ad esempio, se è selezionato il tipo di attributo AAA LDAP (Active Directory), la stringa Nome attributo è memberOf e la stringa Valore è Contractors, come mostrato nella Figura 5a, l'utente che esegue l'autenticazione deve essere un membro del gruppo di Active Directory Contractors per corrispondere ai criteri dell'attributo AAA.

Oltre a soddisfare i criteri degli attributi AAA, all'utente che esegue l'autenticazione può essere richiesto anche di soddisfare i criteri degli attributi dell'endpoint. Ad esempio, se l'amministratore è configurato per determinare la postura dell'endpoint di connessione e in base a tale valutazione della postura, può utilizzare queste informazioni di valutazione come criteri di selezione per l'attributo dell'endpoint mostrato nella Figura 5b.

Figura 5a. Criteri degli attributi AAA

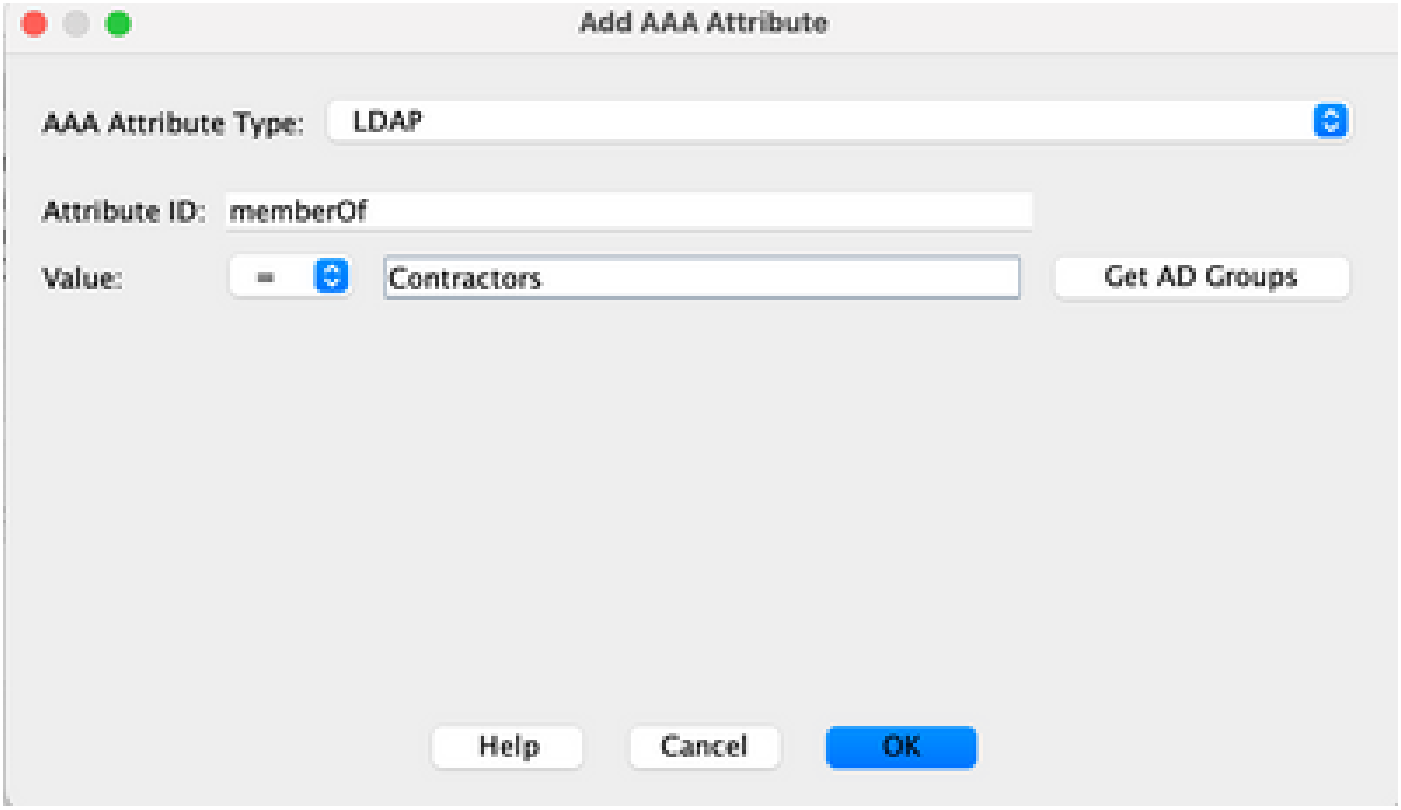


Figura 5b. Criteri degli attributi degli endpoint

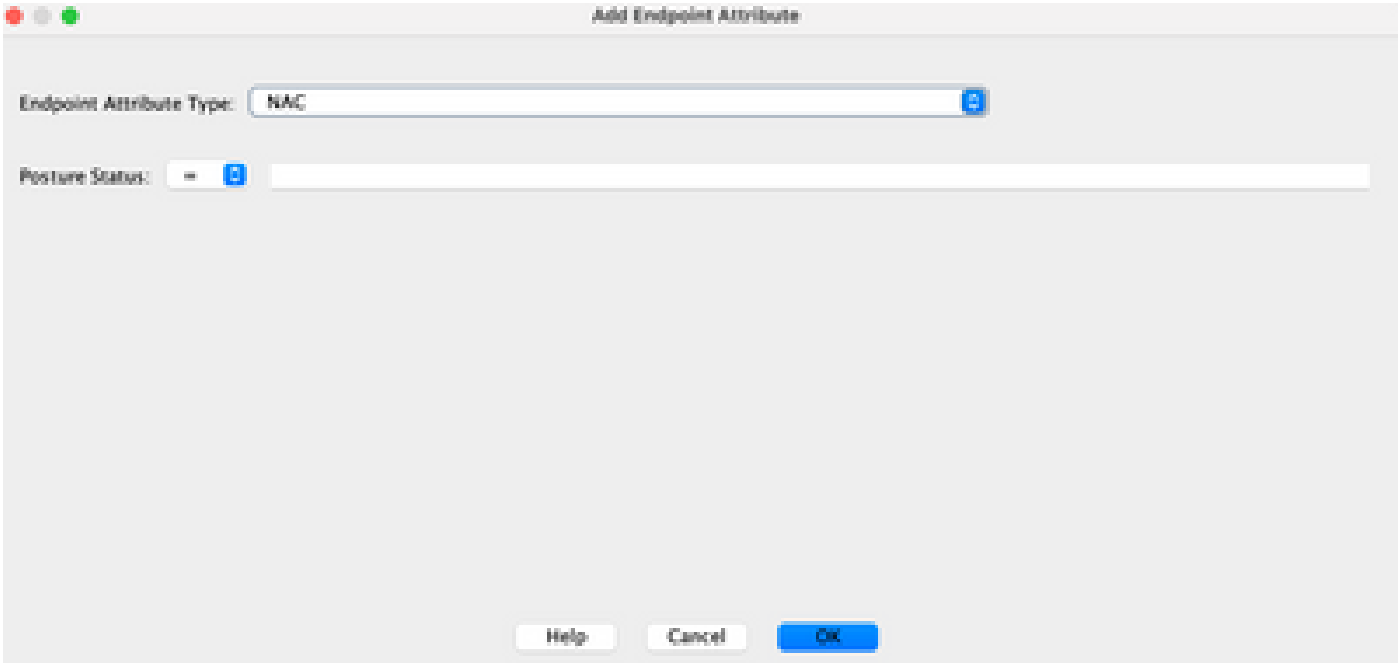
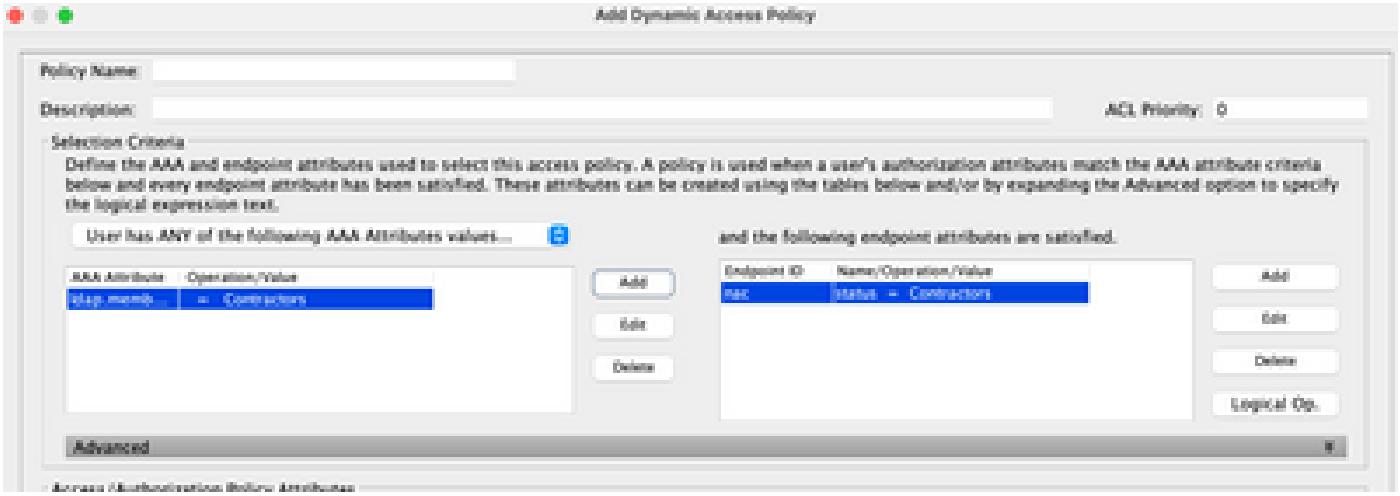


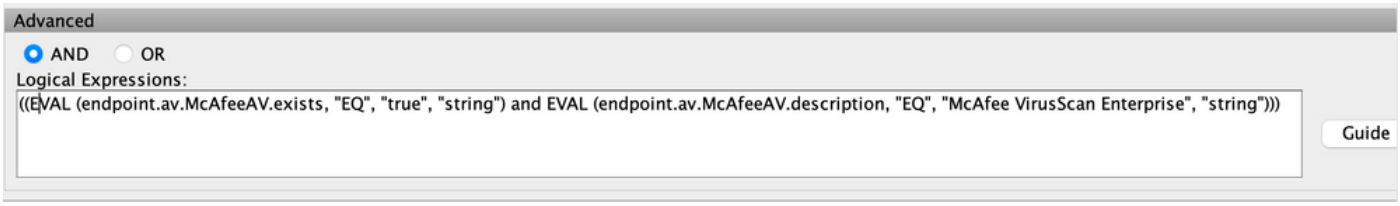
Figura 6. Corrispondenza criteri attributi AAA e endpoint



Gli attributi AAA e Endpoint possono essere creati utilizzando le tabelle descritte nella Figura 6 e/o espandendo l'opzione Advanced per specificare un'espressione logica, come mostrato nella Figura 7. Attualmente, l'espressione logica è costruita con funzioni EVAL, ad esempio EVAL (endpoint.av.McAfeeAV.exist, "EQ", "true", "string") e EVAL (endpoint.av.McAfeeAV.description, "EQ", "McAfee VirusScan Enterprise", "string"), che rappresentano operazioni logiche di selezione di endpoint e/o AAA.

Le espressioni logiche sono utili se è necessario aggiungere criteri di selezione diversi da quelli possibili nelle aree degli attributi AAA ed endpoint, come mostrato in precedenza. Ad esempio, mentre è possibile configurare le appliance di sicurezza in modo che utilizzino attributi AAA che soddisfino uno, tutti o nessuno dei criteri specificati, gli attributi dell'endpoint sono cumulativi e devono essere tutti soddisfatti. Per consentire all'accessorio di protezione di utilizzare un attributo endpoint o un altro attributo, è necessario creare le espressioni logiche appropriate nella sezione Avanzate del record DAP.

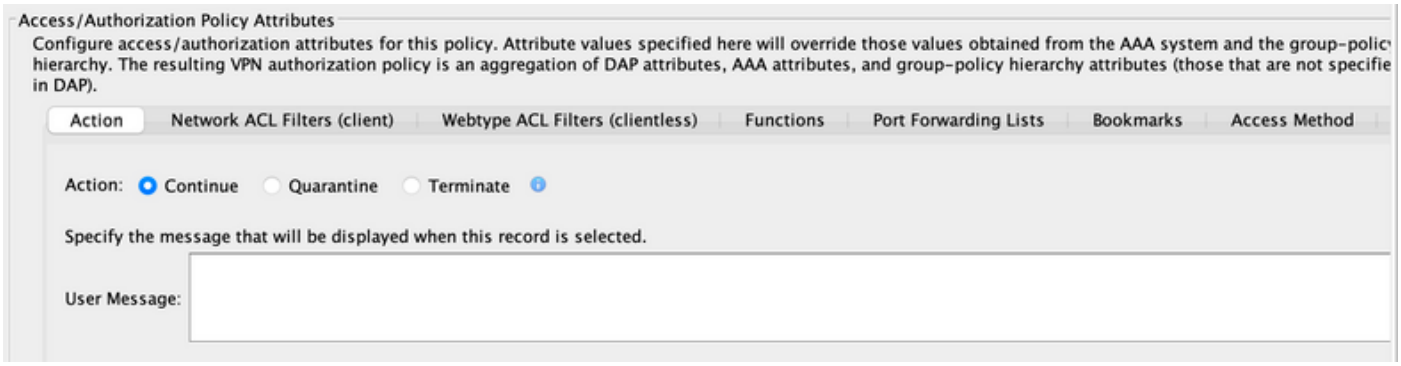
Figura 7. GUI dell'espressione logica per la creazione avanzata di attributi



Nella sezione Attributi dei criteri di accesso, come mostrato nella Figura 8, un amministratore configura gli attributi di accesso VPN per un record DAP specifico. Quando gli attributi di autorizzazione utente corrispondono ai criteri AAA, Endpoint e/o Espressione logica, è possibile applicare i valori degli attributi dei criteri di accesso configurati in questa sezione. I valori degli attributi specificati in questo campo possono sostituire i valori ottenuti dal sistema AAA, inclusi quelli nei record esistenti di utenti, gruppi, gruppi di tunnel e gruppi predefiniti.

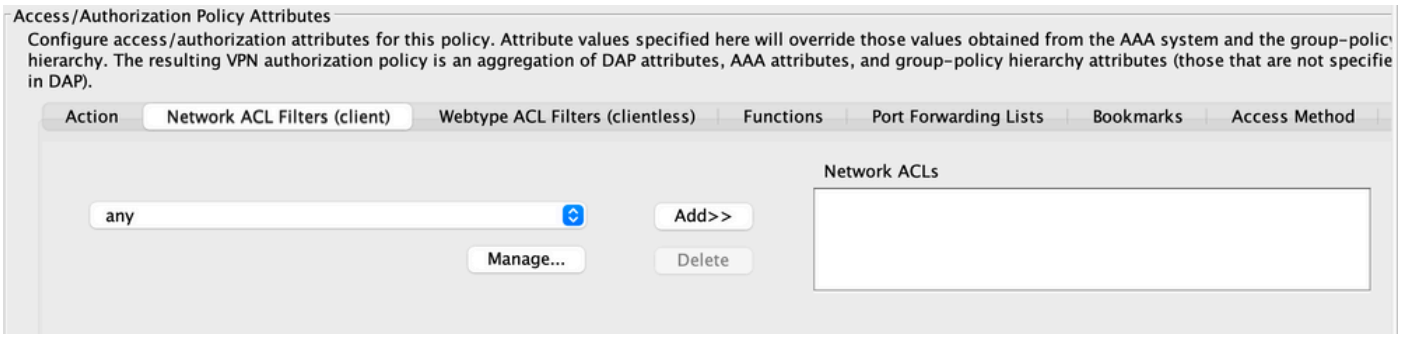
Un record DAP dispone di un set limitato di valori di attributo che è possibile configurare. Questi valori rientrano nelle schede come mostrato nelle figure da 8 a 14:

Figura 8. Azione - specifica l'elaborazione speciale da applicare a una connessione o sessione specifica.



- Continua: (impostazione predefinita) fare clic per applicare gli attributi dei criteri di accesso alla sessione.
- Termina (Terminate) - Fate clic su per terminare la sessione.
- Messaggio utente: immettere un messaggio di testo da visualizzare nella pagina del portale quando viene selezionato questo record DAP. Massimo 128 caratteri. Un messaggio utente viene visualizzato come sfera gialla. Quando un utente accede al sistema, lampeggia tre volte per attirare l'attenzione, e lo rimane. Se sono selezionati più record DAP e ognuno di essi dispone di un messaggio utente, verranno visualizzati tutti i messaggi utente. È inoltre possibile includere in tali messaggi URL o altro testo incorporato, che richiedono l'utilizzo dei tag HTML corretti.

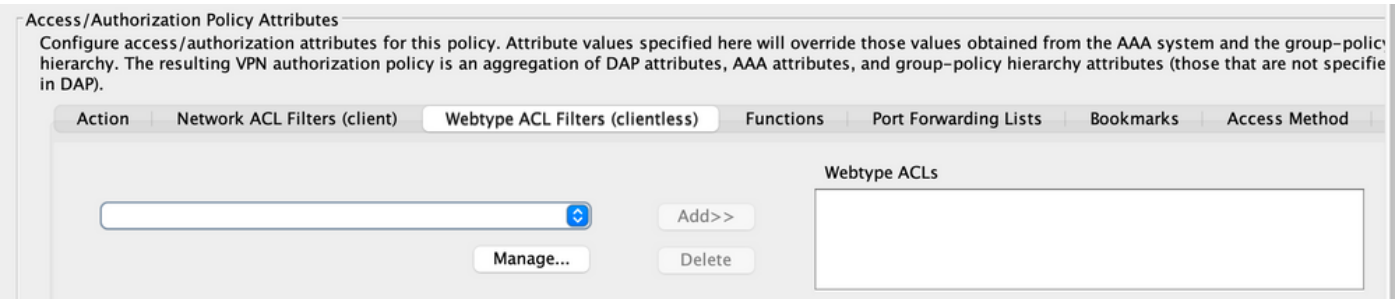
Figura 9. Scheda Filtri ACL di rete - Consente di selezionare e configurare gli ACL di rete da applicare al record DAP. Un ACL per DAP può contenere regole di autorizzazione o di negazione, ma non entrambe. Se un ACL contiene sia regole di autorizzazione che regole di negazione, l'appliance di sicurezza rifiuta la configurazione dell'ACL.



- Casella a discesa ACL di rete: ACL di rete già configurati da aggiungere al record DAP. Sono idonei solo gli ACL con tutte le regole di autorizzazione o rifiuto, e questi sono gli unici ACL che vengono visualizzati qui.
- Gestisci: fare clic per aggiungere, modificare ed eliminare ACL di rete.
- Nell'ACL di rete sono elencati gli ACL di rete per questo record DAP.
- Aggiungi: fare clic per aggiungere l'ACL di rete selezionato dalla casella di riepilogo a discesa all'elenco ACL di rete a destra.
- Elimina: fare clic per eliminare un ACL di rete evidenziato dall'elenco ACL di rete. Non è

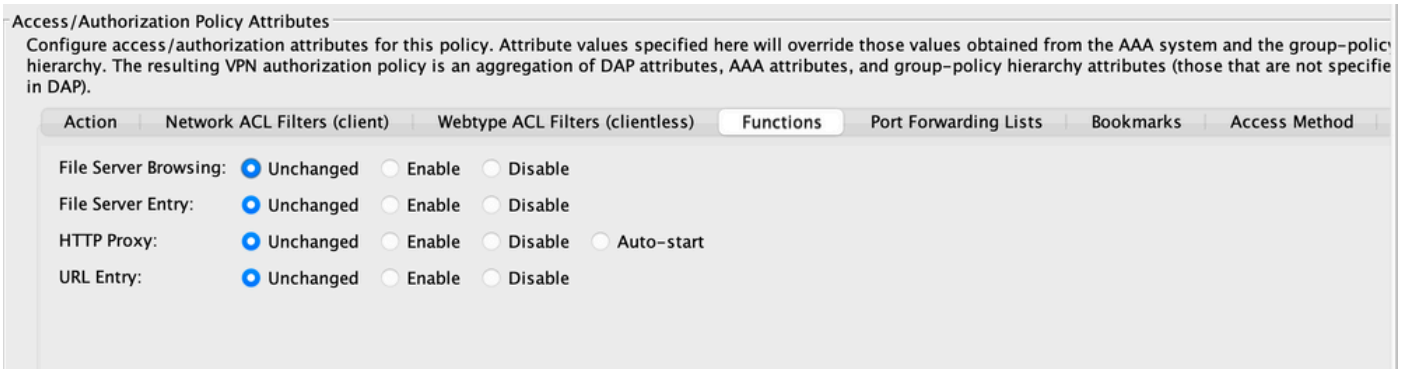
possibile eliminare un ACL se è assegnato a un record DAP o di altro tipo.

Figura 10. Scheda Filtri ACL di tipo Web: consente di selezionare e configurare ACL di tipo Web da applicare al record DAP. Un ACL per DAP può contenere solo regole di autorizzazione o di negazione. Se un ACL contiene sia regole di autorizzazione che regole di negazione, l'appliance di sicurezza rifiuta la configurazione dell'ACL.



- Casella a discesa ACL di tipo Web: selezionare gli ACL di tipo Web già configurati da aggiungere al record DAP. Sono idonei solo gli ACL con tutte le regole di autorizzazione o di negazione, e questi sono gli unici ACL visualizzati qui.
- Gestisci...: fare clic per aggiungere, modificare ed eliminare ACL di tipo Web.
- Elenco ACL di tipo Web: visualizza gli ACL di tipo Web per questo record DAP.
- Aggiungi - Fare clic per aggiungere l'ACL di tipo Web selezionato dalla casella di riepilogo a discesa all'elenco ACL di tipo Web a destra.
- Elimina - Fare clic per eliminare un ACL di tipo Web dall'elenco degli ACL di tipo Web. Non è possibile eliminare un ACL se è assegnato a un record DAP o di altro tipo.

Figura 11. Scheda Funzioni - consente di configurare la voce e l'esplorazione del file server, il proxy HTTP e la voce URL per il record DAP.

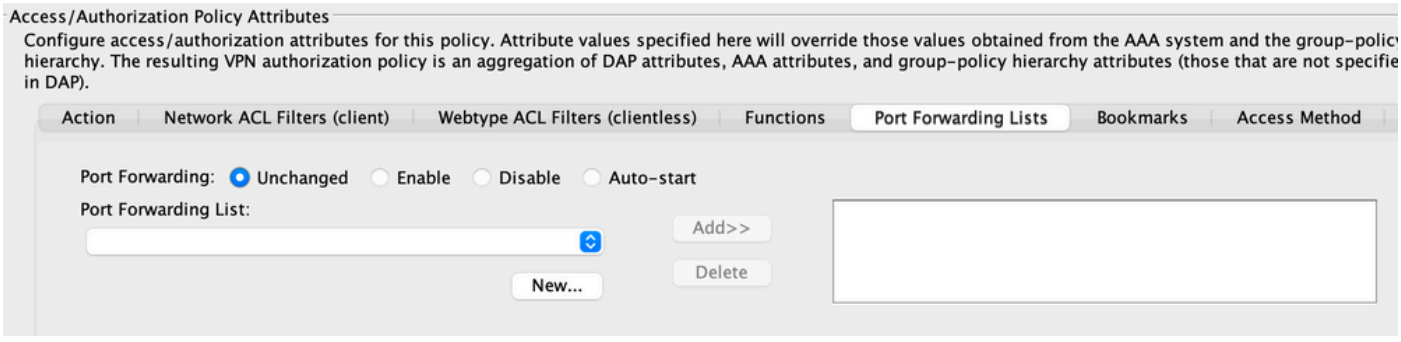


- Esplorazione file server - Abilita o disabilita la ricerca di file server o funzionalità di condivisione CIFS.
- Voce file server (File Server Entry) - Consente o impedisce a un utente di immettere percorsi e nomi di file server nella pagina del portale. Quando è attivata, posiziona il cassetto delle voci del file server nella pagina del portale. Gli utenti possono immettere direttamente i percorsi dei file di Windows. Possono scaricare, modificare, eliminare, rinominare e spostare

i file. Possono inoltre aggiungere file e cartelle. Le condivisioni devono inoltre essere configurate per l'accesso degli utenti ai server Microsoft Windows applicabili. È possibile richiedere agli utenti di eseguire l'autenticazione prima di accedere ai file, a seconda dei requisiti di rete.

- Proxy HTTP: influisce sull'inoltro di un proxy di applet HTTP al client. Il proxy è utile per le tecnologie che interferiscono con la corretta trasformazione dei contenuti, ad esempio Java, ActiveX e Flash. Ignora il processo di modifica/riscrittura garantendo al contempo l'uso continuato dell'appliance di sicurezza. Il proxy inoltrato modifica automaticamente la configurazione del proxy precedente del browser e reindirizza tutte le richieste HTTP e HTTPS alla nuova configurazione del proxy. Supporta praticamente tutte le tecnologie sul lato client, tra cui HTML, CSS, JavaScript, VBScript, ActiveX e Java. L'unico browser supportato è Microsoft Internet Explorer.
- Voce URL: consente o impedisce a un utente di immettere URL HTTP/HTTPS nella pagina del portale. Se questa funzionalità è abilitata, gli utenti possono immettere indirizzi Web nella casella di immissione URL e utilizzare VPN SSL senza client per accedere a tali siti Web.
- Non modificato - (impostazione predefinita) Fare clic per utilizzare i valori dei Criteri di gruppo validi per questa sessione.
- Attiva/Disattiva (Enable/Disable) - Fate clic su per attivare o disattivare la feature.
- Avvio automatico: fare clic per abilitare il proxy HTTP e fare in modo che il record DAP avvii automaticamente le applet associate a queste funzionalità.

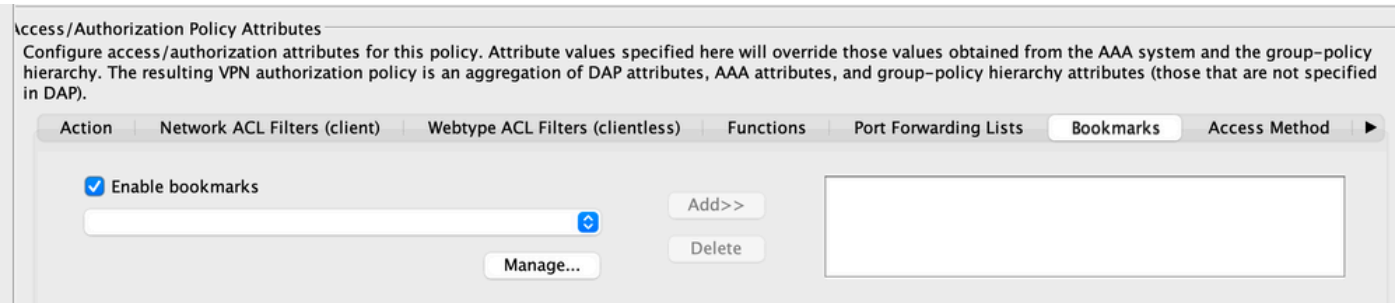
Figura 12. Scheda Elenchi inoltro porte - consente di selezionare e configurare gli elenchi di inoltro porte per le sessioni utente.



- Inoltro porta: selezionare un'opzione per gli elenchi di inoltro delle porte validi per questo record DAP. Gli altri attributi in questo campo vengono abilitati solo quando si imposta Port Forwarding su Enable o Auto-start.
- Non modificato: fare clic per utilizzare i valori dei Criteri di gruppo validi per questa sessione.
- Abilita/Disabilita: fare clic per abilitare o disabilitare l'inoltro delle porte.
- Avvio automatico: fare clic per attivare l'inoltro delle porte e fare in modo che il record DAP avvii automaticamente le applet di inoltro delle porte associate ai relativi elenchi di inoltro delle porte.

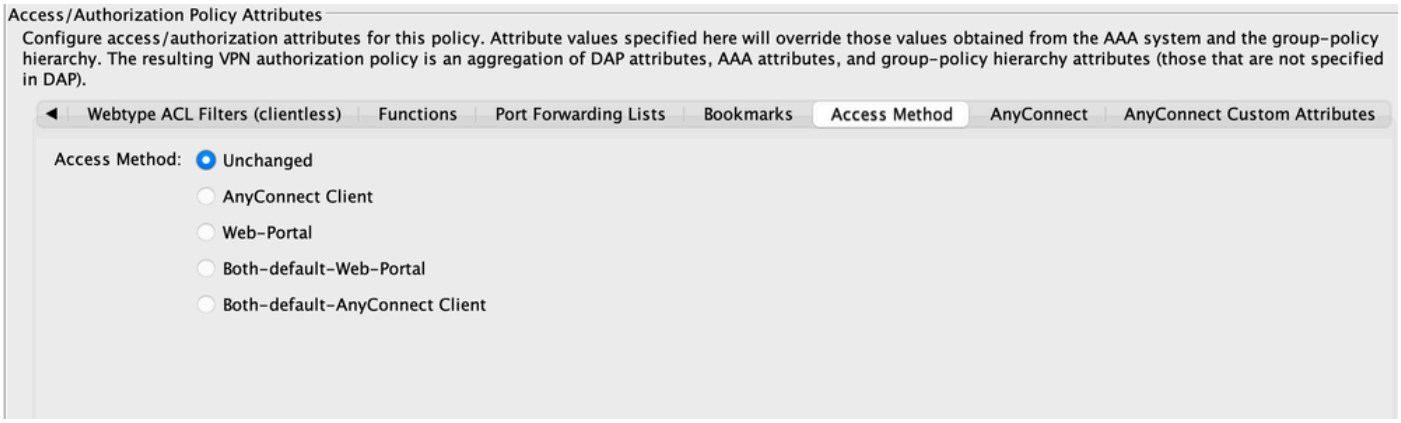
- Casella a discesa Elenco inoltro porta: selezionare gli elenchi di inoltro delle porte già configurati da aggiungere al record DAP.
- Nuovo: fare clic per configurare nuovi elenchi di inoltro porte.
- Elenchi inoltro porte: visualizza l'elenco di inoltro delle porte per il record DAP.
- Aggiungi: fare clic per aggiungere l'elenco di inoltro delle porte selezionato dalla casella a discesa all'elenco di inoltro delle porte a destra.
- Elimina: fare clic per eliminare l'elenco di inoltro delle porte selezionato dall'elenco Inoltro porte. Non è possibile eliminare un ACL se è assegnato a un record DAP o di altro tipo.

Figura 13. Scheda Segnalibri — consente di selezionare e configurare segnalibri/elenchi URL per le sessioni utente.



- Abilita segnalibri: fare clic per abilitare. se questa casella non è selezionata, nella pagina del portale per la connessione non verrà visualizzato alcun elenco di segnalibri.
- Gestisci: fare clic per aggiungere, importare, esportare ed eliminare elenchi di segnalibri.
- Elenchi segnalibri (elenco a discesa) - Visualizza gli elenchi dei segnalibri per il record DAP.
- Aggiungi: fare clic per aggiungere l'elenco di segnalibri selezionato dalla casella di riepilogo a discesa alla casella di riepilogo a destra.
- Elimina (Delete) - Fate clic su per eliminare l'elenco di segnalibri selezionato dalla casella di riepilogo. Non è possibile eliminare un elenco di segnalibri dall'accessorio di protezione se non è stato prima eliminato dai record DAP.

Figura 14. Scheda Metodo — consente di configurare il tipo di accesso remoto consentito.



- Unchanged - Continua con il metodo di accesso remoto corrente impostato nei Criteri di gruppo per la sessione.
- AnyConnect Client: connessione tramite il client VPN Cisco AnyConnect.
- Portale Web: connessione con una VPN senza client.
- Both-default-Web-Portal: per la connessione si utilizza un client senza client o AnyConnect, con il valore predefinito senza client.
- Both-default-AnyConnect Client: connessione senza client o tramite il client AnyConnect, per impostazione predefinita è AnyConnect.

Come accennato in precedenza, un record DAP dispone di un set limitato di valori di attributi predefiniti, solo se modificati hanno la precedenza sui record AAA, utente, gruppo, gruppo di tunnel e gruppo predefinito correnti. Se sono necessari valori di attributi aggiuntivi esterni all'ambito del protocollo DAP, ad esempio elenchi di tunneling suddivisi, banner, smart tunnel, personalizzazioni del portale e così via, è necessario applicarli tramite record AAA, utente, gruppo, gruppo di tunnel e gruppo predefinito. In questo caso, i valori di tali attributi specifici possono essere complementari a DAP e non possono essere sostituiti. In questo modo, l'utente ottiene un insieme cumulativo di valori di attributo in tutti i record.

Aggregazione di più criteri di accesso dinamico

Un amministratore può configurare più record DAP in modo da gestire più variabili. Di conseguenza, un utente che esegue l'autenticazione può soddisfare i criteri degli attributi AAA ed Endpoint di più record DAP. Di conseguenza, gli attributi dei criteri di accesso possono essere coerenti o in conflitto in tutti i criteri. In questo caso, l'utente autorizzato può ottenere il risultato cumulativo per tutti i record DAP corrispondenti.

Sono inoltre inclusi i valori di attributo univoci imposti tramite i record di autenticazione, autorizzazione, utente, gruppo, gruppo tunnel e gruppo predefinito. Il risultato cumulativo degli attributi dei criteri di accesso crea i criteri di accesso dinamico. Nelle tabelle seguenti sono riportati alcuni esempi di attributi dei criteri di accesso combinati. In questi esempi vengono illustrati i risultati di 3 record DAP combinati.

Il valore dell'attributo action mostrato nella Tabella 1 è Termina o Continua. Il valore dell'attributo

aggregato è Termina se il valore Termina è configurato in uno dei record DAP selezionati ed è Continua se il valore Continua è configurato in tutti i record DAP selezionati.

Tabella 1. Attributo Action

Nome attributo	DAP n. 1	DAP n. 2	DAP n. 3	DAP
Azione (esempio 1)	continua	continua	continua	continua
Azione (esempio 2)	Termina	continua	continua	terminare

L'attributo user-message mostrato nella Tabella 2 contiene un valore string. Il valore dell'attributo aggregato può essere una stringa di avanzamento riga (valore esadecimale 0x0A) separata creata collegando i valori dell'attributo dai record DAP selezionati. L'ordinamento dei valori degli attributi nella stringa combinata è insignificante.

Tabella 2. Attributo User-Message

Nome attributo	DAP n. 1	DAP n. 2	DAP n. 3	DAP
messaggio-utente	il rapido	volpe marrone	Salta	la rapida<LF>volpe marrone<LF>passa

La funzione Client che abilita gli attributi (Funzioni) mostrati nella Tabella 3 contiene valori quali Auto-start, Enable o Disable (Avvio automatico, Abilita o Disabilita). Il valore dell'attributo aggregato può essere Avvio automatico se il valore di Avvio automatico è configurato in uno dei record DAP selezionati.

Il valore dell'attributo aggregato può essere Abilitato se non è stato configurato alcun valore di avvio automatico in uno dei record DAP selezionati e il valore Abilita è configurato in almeno uno dei record DAP selezionati.

Il valore dell'attributo aggregato può essere disabilitato se non è stato configurato alcun valore di avvio automatico o abilitazione in nessuno dei record DAP selezionati e se il valore "disable" è stato configurato in almeno uno dei record DAP selezionati.

Tabella 3. Attributi di abilitazione delle funzionalità senza client (funzioni)

Nome attributo	DAP n. 1	DAP n. 2	DAP n. 3	DAP
port-forward	attivare	disabilitare		attivare
esplorazione dei file	disabilitare	attivare	disabilitare	attivare
immissione di file			disabilitare	disabilitare
Proxy HTTP	disabilitare	avvio automatico	disabilitare	avvio automatico
URL-entry	disabilitare		attivare	attivare

L'elenco URL e gli attributi port-forward mostrati nella Tabella 4 contengono un valore che può essere una stringa o una stringa separata da virgole. Il valore dell'attributo aggregato può essere una stringa separata da virgole creata da quando si collegano i valori degli attributi dai record DAP selezionati. Qualsiasi valore attributo duplicato nella stringa combinata può essere rimosso. Il

modo in cui i valori degli attributi vengono ordinati nella stringa combinata è insignificante.

Tabella 4. Elenco URL e attributo elenco di inoltro porte

Nome attributo	DAP n. 1	DAP n. 3	DAP n. 3	DAP
url-list	a	b,c	a	a, b, c
port-forward		d,e	e,f	d,e,f

Gli attributi Access Method specificano il metodo di accesso client consentito per le connessioni VPN SSL. Il metodo di accesso client può essere AnyConnect Client (solo accesso), AnyConnect Portal (solo accesso al portale Web), AnyConnect Client o Web-Portal (accesso al portale Web) con accesso al portale Web come impostazione predefinita oppure AnyConnect Client o Web-Portal (accesso al portale Web) con accesso al client AnyConnect come impostazione predefinita. Il valore dell'attributo aggregato è riepilogato nella Tabella 5.

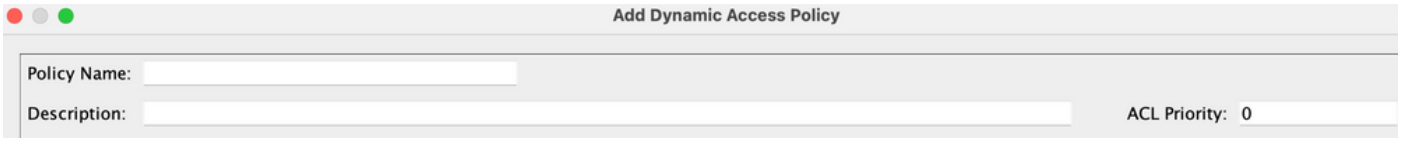
Tabella 5. Attributi dei metodi di accesso

Valori attributo selezionati				Risultato aggregazione
Client AnyConnect	Portale Web	Both-default-Web-Portal	Both-default-AnyConnect Client	
			X	Both-default-AnyConnect Client
		X		Both-default-Web-Portal
		X	X	Both-default-Web-Portal
	X			Portale Web
	X		X	Both-default-AnyConnect Client
	X	X		Both-default-Web-Portal
	X	X	X	Both-default-Web-Portal
X				Client AnyConnect
X			X	Both-default-AnyConnect Client
X		X		Both-default-Web-Portal
X		X	X	Both-default-Web-Portal
X	X			Both-default-Web-Portal
X	X		X	Both-default-AnyConnect Client
X	X	X		Both-default-Web-Portal
X	X	X	X	Both-default-Web-Portal

Quando si combinano gli attributi Network (Firewall) e Web-Type (Clientless) ACL Filter, DAP Priority e DAP ACL sono due componenti principali da prendere in considerazione.

L'attributo Priority, illustrato nella Figura 15, non è aggregato. Questo valore viene utilizzato dall'appliance di sicurezza per definire la sequenza logica degli elenchi degli accessi durante l'aggregazione degli ACL di rete e di tipo Web da più record DAP. L'accessorio di protezione ordina i record dal numero di priorità più alto a quello più basso, con il numero più basso nella parte inferiore della tabella. Ad esempio, un record DAP con valore 4 ha una priorità più alta rispetto a un record con valore 2. Non è possibile ordinarli manualmente.

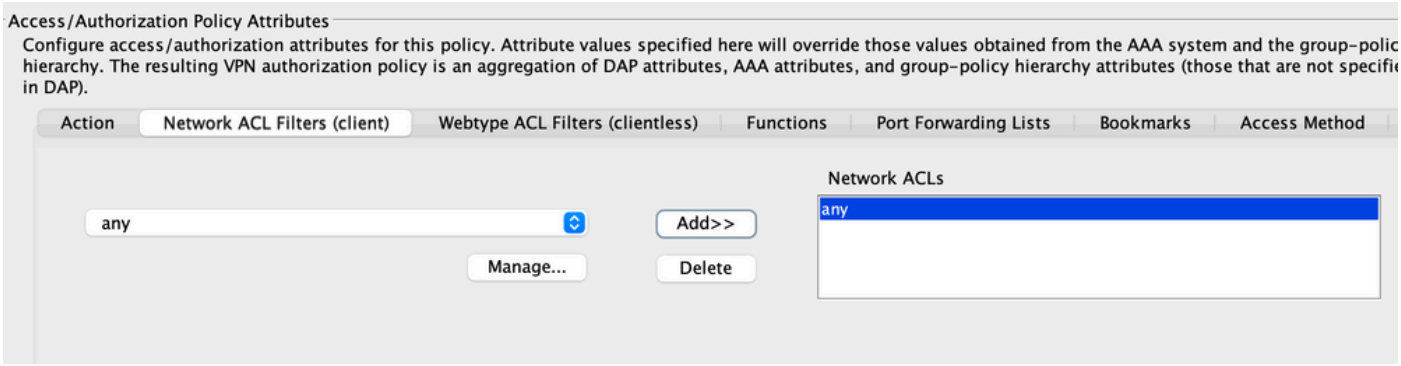
Figura 15. Priorità - Visualizza la priorità del record DAP.



- Nome criterio: visualizza il nome del record DAP.
- Descrizione: descrive lo scopo del record DAP.

L'attributo ACL DAP supporta solo elenchi degli accessi conformi a un modello rigoroso Allow-List o Block-List ACL. In un modello ACL Allow-List, le voci dell'elenco degli accessi specificano le regole che "permettono" l'accesso a reti o host specifici. In modalità ACL block-list, le voci dell'elenco degli accessi specificano le regole che negano l'accesso a reti o host specifici. Un elenco degli accessi non conforme contiene voci dell'elenco degli accessi con una combinazione di regole di autorizzazione e di rifiuto. Se per un record DAP è configurato un elenco di accesso non conforme, è possibile rifiutarlo come errore di configurazione quando l'amministratore tenta di aggiungere il record. Se un elenco di accesso conforme viene assegnato a un record DAP, qualsiasi modifica apportata all'elenco di accesso che modifichi la caratteristica di conformità può essere rifiutata come errore di configurazione.

Figura 16. ACL DAP: consente di selezionare e configurare ACL di rete da applicare al record DAP.



Quando si selezionano più record DAP, gli attributi degli elenchi degli accessi specificati nell'ACL di rete (firewall) vengono aggregati per creare un elenco degli accessi dinamici per l'ACL del firewall DAP. Allo stesso modo, gli attributi degli elenchi degli accessi specificati nell'ACL di tipo Web (senza client) vengono aggregati per creare un elenco degli accessi dinamici per l'ACL senza client DAP. Nell'esempio seguente viene illustrato come creare specificamente un elenco degli accessi al firewall DAP dinamico. Tuttavia, un elenco DAP accesso senza client dinamico può eseguire lo stesso processo.

In primo luogo, l'ASA crea dinamicamente un nome univoco per l'ACL di rete DAP, come mostrato nella Tabella 6.

Tabella 6. Nome ACL di rete DAP dinamico

Nome ACL di rete DAP
DAP-Network-ACL-X (dove X è un numero intero incrementabile per garantire l'univocità)

In secondo luogo, l'ASA recupera l'attributo Network-ACL dai record DAP selezionati, come mostrato nella Tabella 7.

Tabella 7. ACL di rete

Record DAP selezionati	Priority	ACL di rete	Voci ACL di rete
DAP 1	1	101 e 102	ACL 101 ha 4 regole di negazione e ACL 102 ne ha 4
DAP 2	2	201 e 202	ACL 201 ha 3 regole di autorizzazione e ACL 202 ne ha 3
DAP 3	2	101 e 102	ACL 101 ha 4 regole di negazione e ACL 102 ne ha 4

In terzo luogo, l'ASA riordina l'ACL di rete prima in base al numero di priorità del record DAP, quindi in base all'elenco di blocchi prima se il valore di priorità per 2 o più record DAP selezionati è lo stesso. Quindi, l'ASA può recuperare le voci Network-ACL da ciascun ACL, come mostrato nella Tabella 8.

Tabella 8. Priorità record DAP

ACL di rete	Priority	Modello Access-List Bianco/Nero	Voci ACL di rete
101	2	Lista nera	4 Regole di rifiuto (DDDD)
202	2	Lista nera	3 Regole di rifiuto (DDD)
102	2	Lista bianca	4 Regole di autorizzazione (PPP)
202	2	Lista bianca	3 Regole di autorizzazione (PPP)
101	1	Lista nera	4 Regole di rifiuto (DDDD)
102	1	Lista bianca	4 Regole di autorizzazione (PPP)

Infine, l'ASA unisce le voci Network-ACL nell'ACL di rete generato in modo dinamico e restituisce il nome dell'ACL di rete dinamico come nuovo ACL di rete da applicare, come mostrato nella Tabella 9.

Tabella 9. ACL di rete DAP dinamico

Nome ACL di rete DAP	Voce Network-ACL
DAP-Network-ACL-1	DDDD DDD PPP PPP DDDD PPP

Implementazione DAP

Esistono numerosi motivi per cui un amministratore deve prendere in considerazione l'implementazione di DAP. Alcuni dei motivi sottostanti sono quando la valutazione della postura su un endpoint deve essere applicata e/o quando si devono prendere in considerazione attributi AAA o di policy più granulari quando si autorizza l'accesso degli utenti alle risorse di rete. Nell'esempio successivo è possibile configurare DAP e i relativi componenti per identificare un endpoint di connessione e autorizzare l'accesso degli utenti a diverse risorse di rete.

Test case: un client ha richiesto una prova di concetto con i seguenti requisiti di accesso VPN:

- La capacità di rilevare e identificare un endpoint dipendente come gestito o non gestito. - Se l'endpoint viene identificato come gestito (PC di lavoro) ma non soddisfa i requisiti di postura, l'accesso a tale endpoint deve essere negato. Se invece l'endpoint del dipendente è identificato come non gestito (PC di casa), a tale endpoint deve essere concesso l'accesso senza client.
- Possibilità di richiamare la pulizia dei cookie di sessione e della cache al termine di una connessione senza client.
- La capacità di rilevare e applicare le applicazioni in esecuzione sugli endpoint dei dipendenti gestiti, ad esempio McAfee AntiVirus. Se l'applicazione non esiste, all'endpoint deve essere negato l'accesso.
- Possibilità di utilizzare l'autenticazione AAA per determinare a quali risorse di rete devono avere accesso gli utenti autorizzati. L'appliance di sicurezza deve supportare l'autenticazione LDAP MS nativa e più ruoli di appartenenza ai gruppi LDAP.
- Possibilità di consentire l'accesso LAN locale alle risorse di rete, ad esempio fax e stampanti di rete, se connessi tramite una connessione client/di rete.
- La capacità di fornire agli utenti guest autorizzati l'accesso ai collaboratori esterni. Gli appaltatori e i relativi endpoint devono poter accedere alle applicazioni senza client e l'accesso alle applicazioni tramite portale deve essere limitato rispetto all'accesso per i dipendenti.

In questo esempio, è possibile eseguire una serie di passaggi di configurazione per soddisfare i requisiti di accesso VPN del client. Possono essere necessari dei passaggi di configurazione, ma non direttamente correlati al DAP, mentre altre configurazioni possono essere direttamente correlate al DAP. L'ASA è molto dinamica e può adattarsi a molti ambienti di rete. Di conseguenza, le soluzioni VPN possono essere definite in diversi modi e in alcuni casi fornire la stessa soluzione finale. Tuttavia, l'approccio adottato dipende dalle esigenze dei client e dai relativi ambienti.

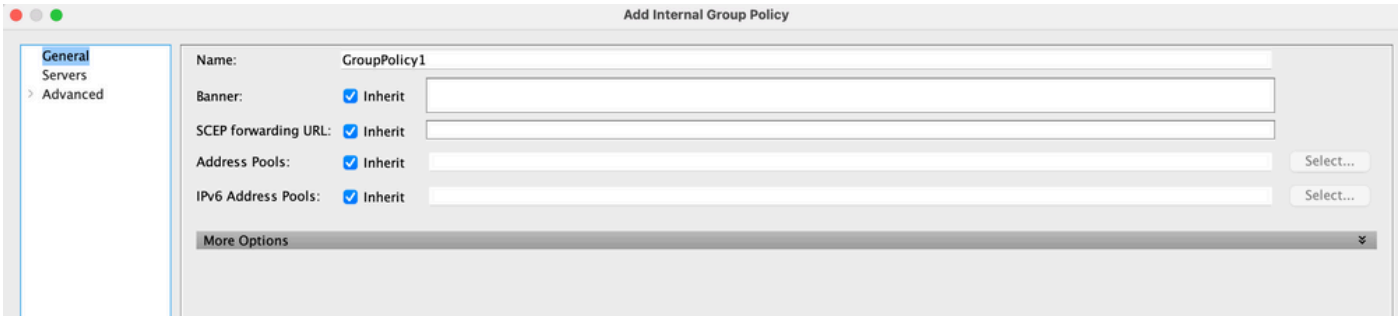
In base alla natura di questo documento e ai requisiti del client definiti, è possibile utilizzare Adaptive Security Device Manager (ASDM) e concentrare la maggior parte delle configurazioni su DAP. È tuttavia possibile anche configurare Criteri di gruppo locali per mostrare in che modo il punto di accesso locale può integrare e/o ignorare gli attributi dei criteri locali. Sulla base di questo

test case, è possibile presupporre che un gruppo di server LDAP, un elenco delle reti di tunneling suddivise e la connettività IP di base, inclusi i pool IP e il gruppo di server DNS predefinito, siano preconfigurati.

Definizione di Criteri di gruppo: questa configurazione è necessaria per definire gli attributi dei criteri locali. Alcuni attributi definiti qui non sono configurabili in DAP (ad esempio, Accesso LAN locale). (Questo criterio può essere utilizzato anche per definire attributi senza client e basati su client).

Passare a Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Criteri di gruppo, quindi aggiungere un criterio di gruppo interno come illustrato di seguito:

Figura 17. Criteri di gruppo - Definisce gli attributi specifici della VPN locale.

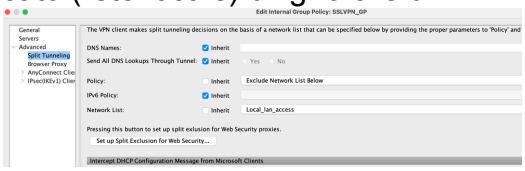


a. Nel collegamento Generale configurare il nome SSLVPN_GP per Criteri di gruppo.

b. Inoltre, nel collegamento Generale, fare clic su Altre opzionie configurare solo il protocollo di tunneling SSLVPN senza client (è possibile configurare il protocollo DAP in modo che esegua l'override e gestisca il metodo di accesso).

c. Nel collegamento Avanzate > Tunneling ripartito, configurare la procedura seguente:

Figura 18. Tunneling ripartito: consente al traffico specificato (rete locale) di ignorare un tunnel non crittografato durante una connessione client.

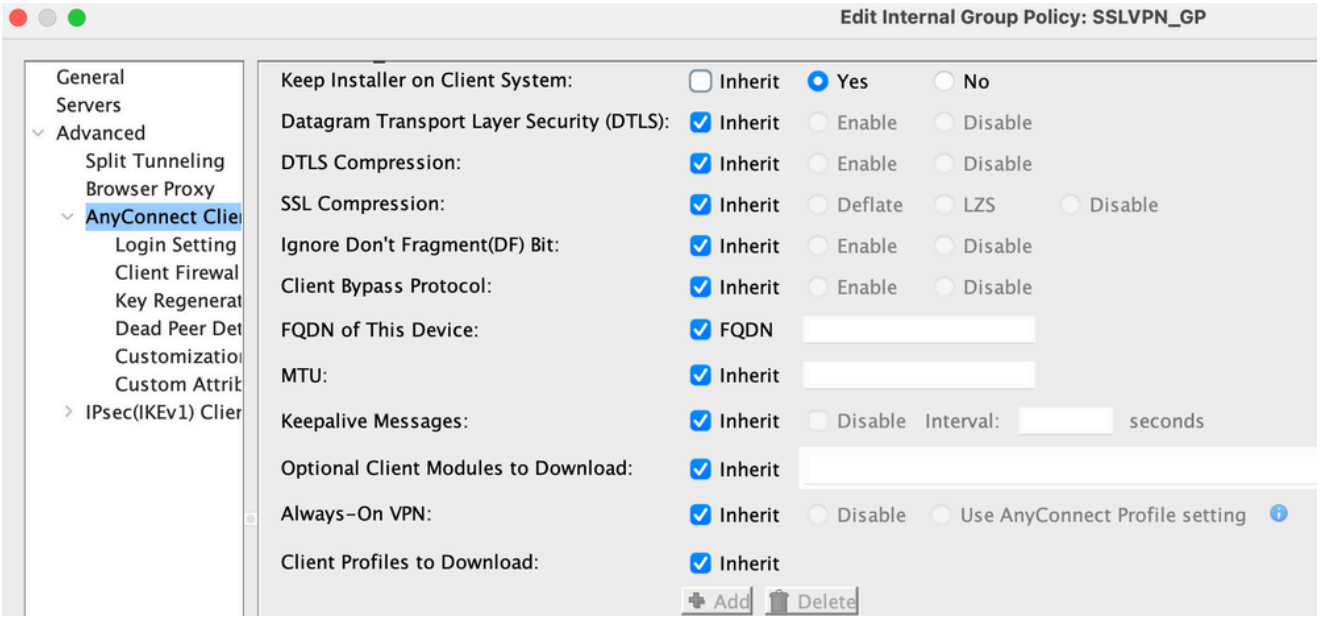


a. Criterio: UncheckInheritand selectExclude Network List.

b. Elenco reti: deselezionareEredita e selezionare il nome dell'elenco Local_Lan_Access. (si presume che sia preconfigurato).

d. Nel collegamento Advanced > ANYCONNECT Client, configurare i seguenti passaggi:

Figura 19. SSL VPN Client Installer: dopo la terminazione della VPN, il client SSL può rimanere sull'endpoint o essere disinstallato.



e. Mantieni programma di installazione sul sistema client: Deselezionare Eredita, quindi selezionare Sì.

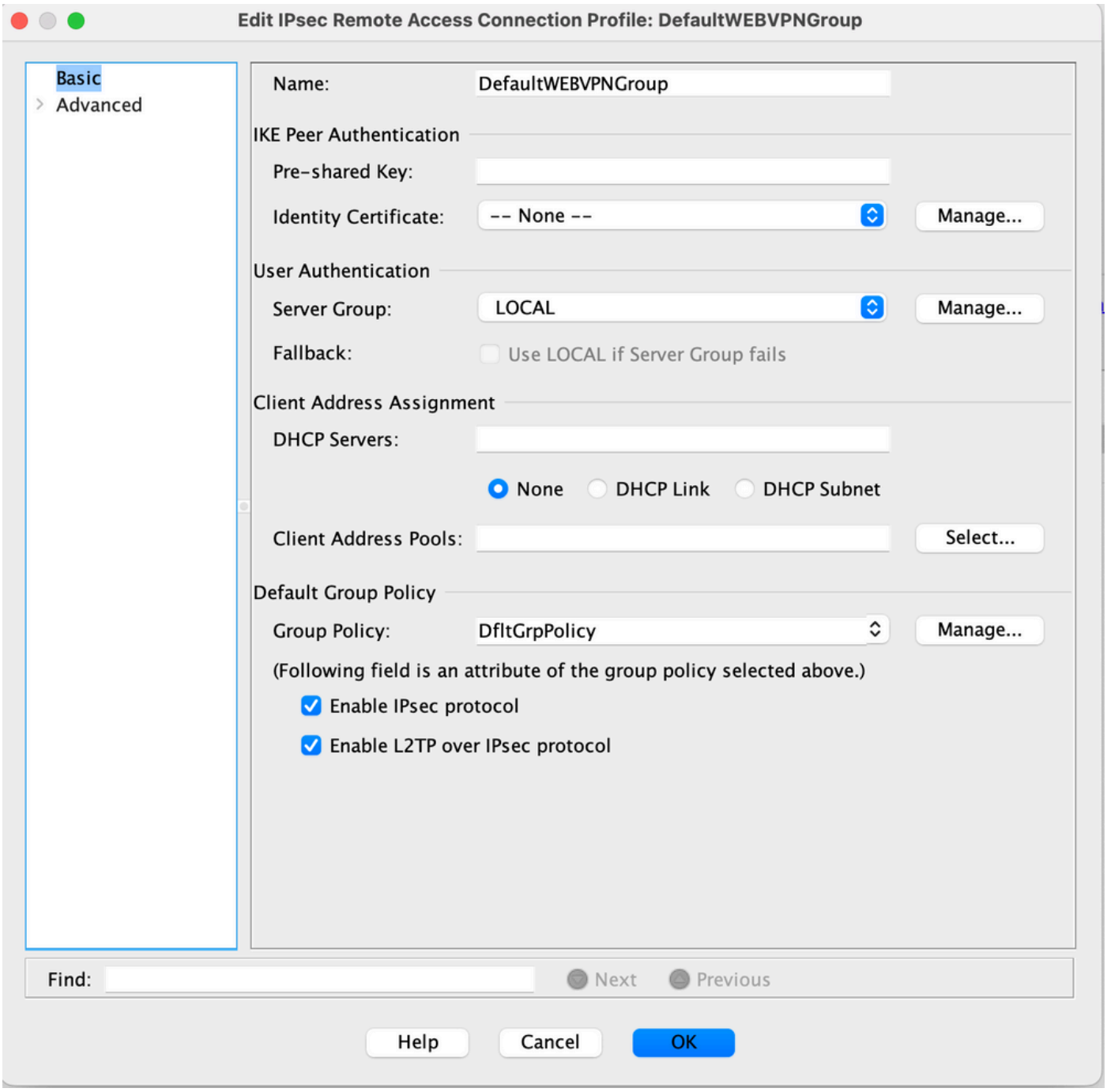
f. Fare clic su OK, quindi su Applica.

g. Applicare le modifiche alla configurazione.

Definizione di un profilo di connessione: questa configurazione è necessaria per definire il metodo di autenticazione AAA, ad esempio LDAP, e applicare i Criteri di gruppo (SSLVPN_GP) configurati in precedenza a questo profilo di connessione. Gli utenti che si connettono tramite questo profilo di connessione possono essere soggetti agli attributi definiti qui e agli attributi definiti in SSLVPN_GP Group Policy. (Questo profilo può essere utilizzato anche per definire gli attributi senza client e basati su client).

Selezionare Configurazione > VPN ad accesso remoto > Profilo connessione di rete (client) >Accesso remoto IPsec e configurare:

Figura 20. Profilo connessione - Definisce gli attributi specifici della VPN locale.



a. Nella sezione Profili di connessione modificare DefaultWEBVPNGroup e configurare la procedura seguente nel collegamento Base:

   a. Autenticazione—Metodo:AAA

   b. Autenticazione—Gruppo server AAA:LDAP(preconfigurata)

   c. Assegnazione indirizzo client - Pool di indirizzi client:IP_Pool (preconfigurato)

   d. Criteri di gruppo predefiniti - Criteri di gruppo: SelectSSLVPN_GP

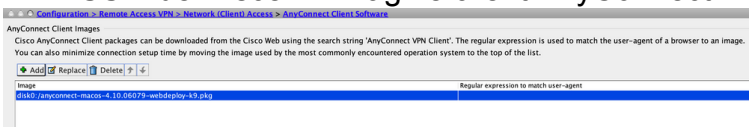
b. Applicare le modifiche alla configurazione.

Definire un'interfaccia IP per la connettività VPN SSL: questa configurazione è necessaria per terminare le connessioni SSL client e senza client su un'interfaccia specificata.

Prima di abilitare l'accesso client/di rete su un'interfaccia, è necessario definire un'immagine client VPN SSL.

1. Selezionare Configuration > Remote Access VPN > Network (Client)Access > Anyconnect Client Software, quindi aggiungere l'immagine successiva, ossia l'immagine SSL VPN Client Image, dal file system Flash ASA: (questa immagine può essere scaricata da CCO, https://www.cisco.com)

   Figura 21. Installazione immagine client VPN SSL: definisce l'immagine client AnyConnect da inviare agli endpoint di connessione.

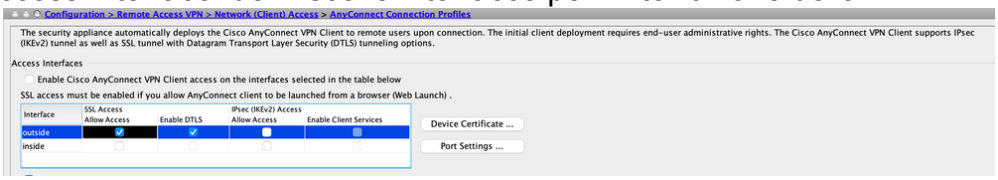
   

   a. anyconnect-mac-4.x.xxx-k9.pkg

   b. Fare clic su OK, nuovamente su OK e quindi su Applica.

2. Selezionare Configurazione > VPN ad accesso remoto > Accesso di rete (client), quindi Profili di connessione AnyConnect e procedere come segue per abilitare questa funzionalità:

   Figura 22. SSL VPN Access Interface: definisce le interfacce per l'interruzione della connettività SSL VPN.

   a. Nella sezione Access Interface, abilitare:Enable Cisco AnyConnect VPN Client o l'accesso ai client VPN SSL legacy sulle interfacce selezionate nella tabella seguente.

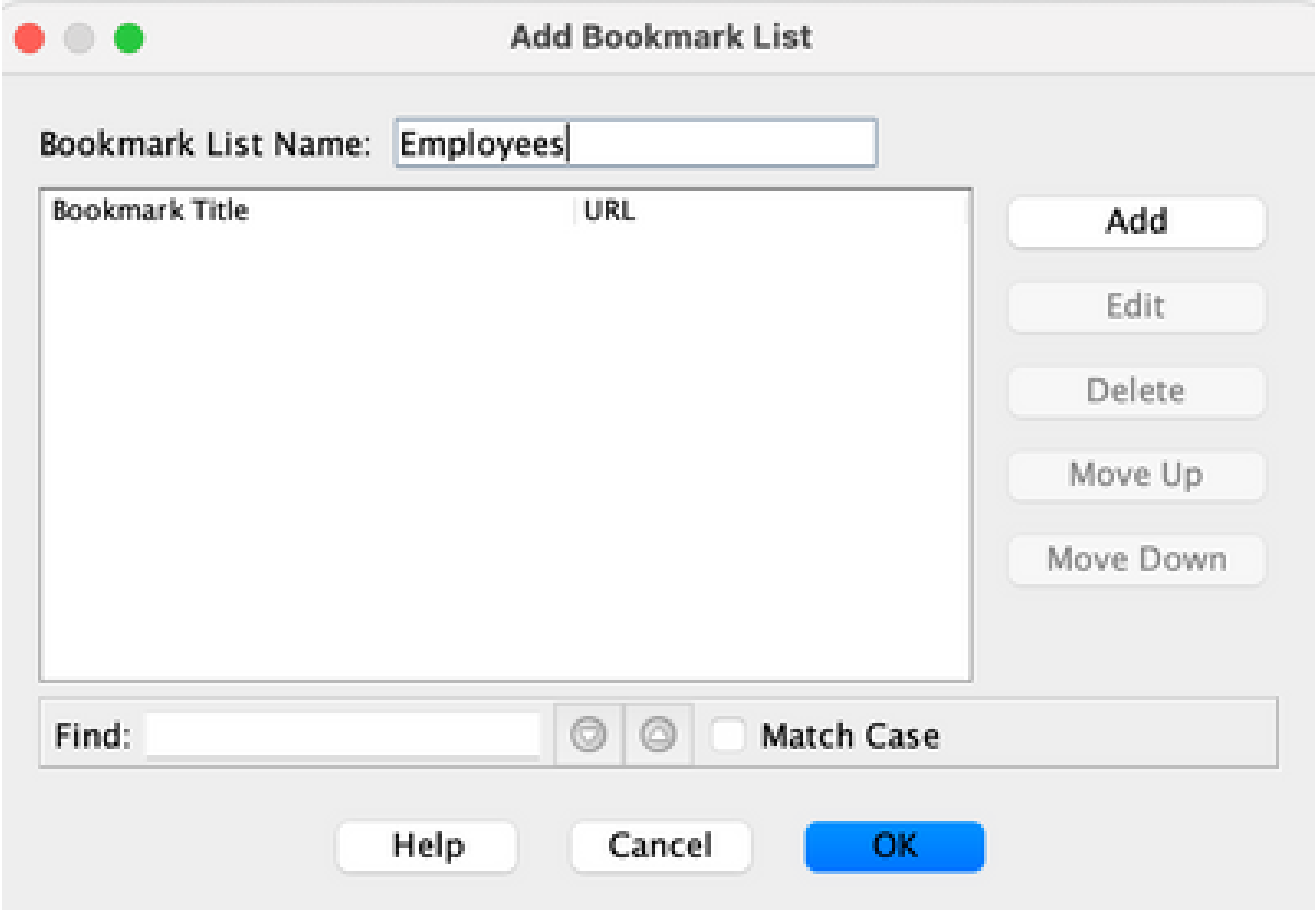
   b. Inoltre, nella sezione Interfacce di accesso, selezionare Consenti accesso sull'interfaccia esterna. (Questa configurazione può anche abilitare l'accesso SSL VPN senza client sull'interfaccia esterna.)

   c. Fare clic su Applica.

Definizione di elenchi segnalibri (elenchi URL) per l'accesso senza client: questa configurazione è necessaria per definire un'applicazione basata sul Web da pubblicare sul portale. È possibile definire due elenchi URL, uno per i dipendenti e l'altro per i collaboratori esterni.

1. Selezionare Configurazione > VPN ad accesso remoto > Accesso VPN SSL senza client > Portale > Segnalibri, fare clic su + Aggiungi e configurare la procedura seguente:

   Figura 23. Elenco segnalibri: definisce gli URL da pubblicare e a cui accedere dal portale Web. (Personalizzato per l'accesso dei dipendenti).



a. Nome elenco segnalibri:Dipendenti, quindi fare clic su Aggiungi.

b. Titolo segnalibro:Intranet aziendale

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

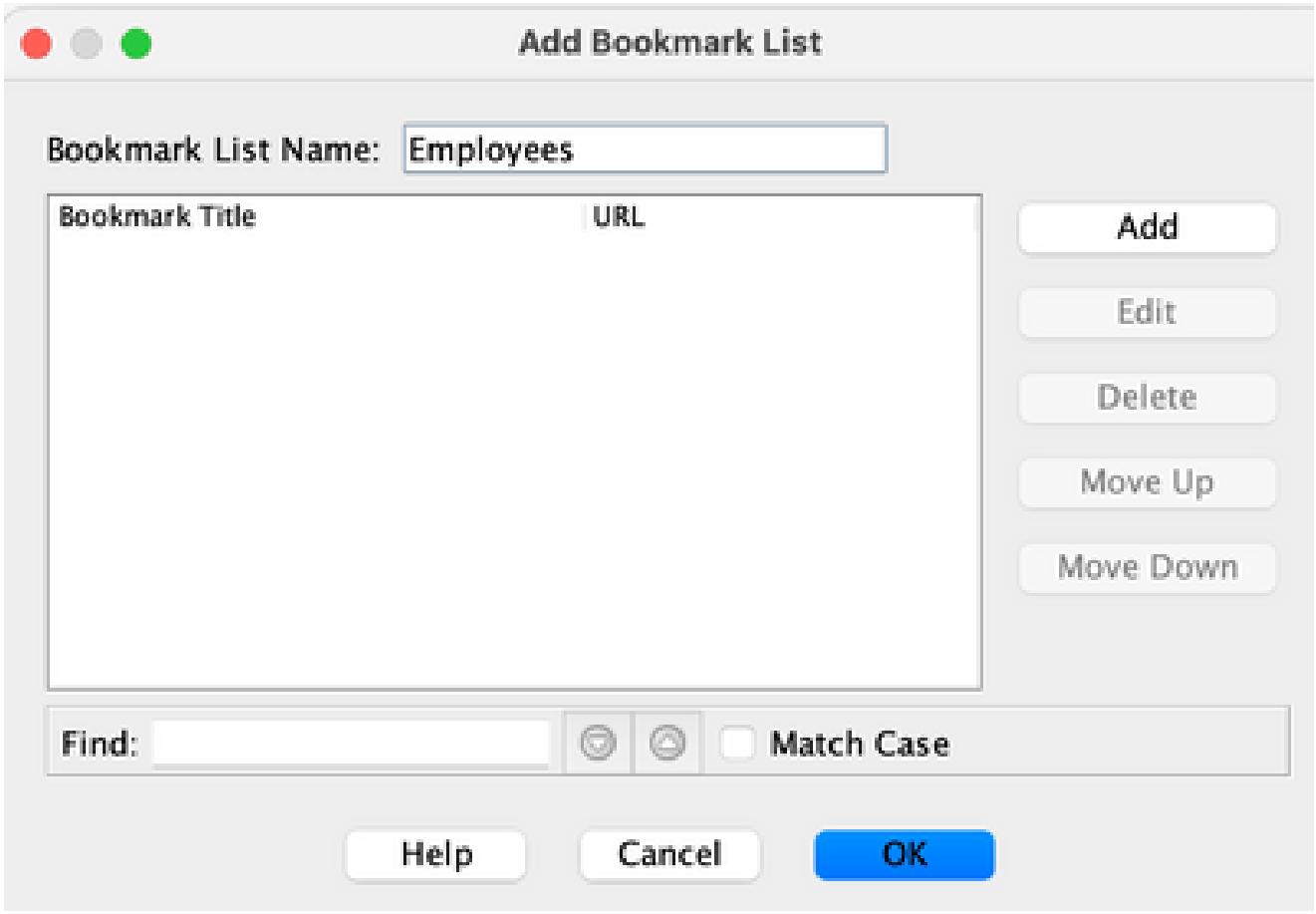
-

Fare clic su OK, quindi di nuovo su OK.

-

Fare clic su + Aggiungi e configurare un secondo elenco segnalibri (elenco URL) come indicato di seguito:

Figura 24. Elenco segnalibri - Personalizzato per l'accesso come Guest.



a.

Nome elenco segnalibri:**Appaltatori**, quindi **fare clic su Aggiungi**.

b.

Titolo Segnalibro:**Accesso Guest**

c.

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

-

Fare clic su OK, quindi di nuovo su OK.

-

Fare clic su Applica.

Configurare Hostscan:

- Passare **a Configurazione > VPN ad accesso remoto > Secure Desktop Manager > Immagine di HostScan** e configurare la procedura seguente:

Figura 25. HostScan Image Install: definisce l'immagine HostScan da inserire negli endpoint di connessione. 

a. Installare **il disco0:/hostscan_4.xx.xxxxx-k9.**pkgimage dal file system Flash ASA.

b. **Selezionare Abilita HostScan**.

c. **Fare clic su Applica**.

Criteri di accesso dinamico: questa configurazione è necessaria per convalidare la connessione degli utenti e dei loro endpoint in base a criteri di valutazione AAA e/o endpoint definiti. Se i criteri definiti di un record DAP sono soddisfatti, è possibile concedere agli utenti che si connettono l'accesso alle risorse di rete associate al record o ai record DAP. L'autorizzazione DAP viene eseguita durante il processo di autenticazione.

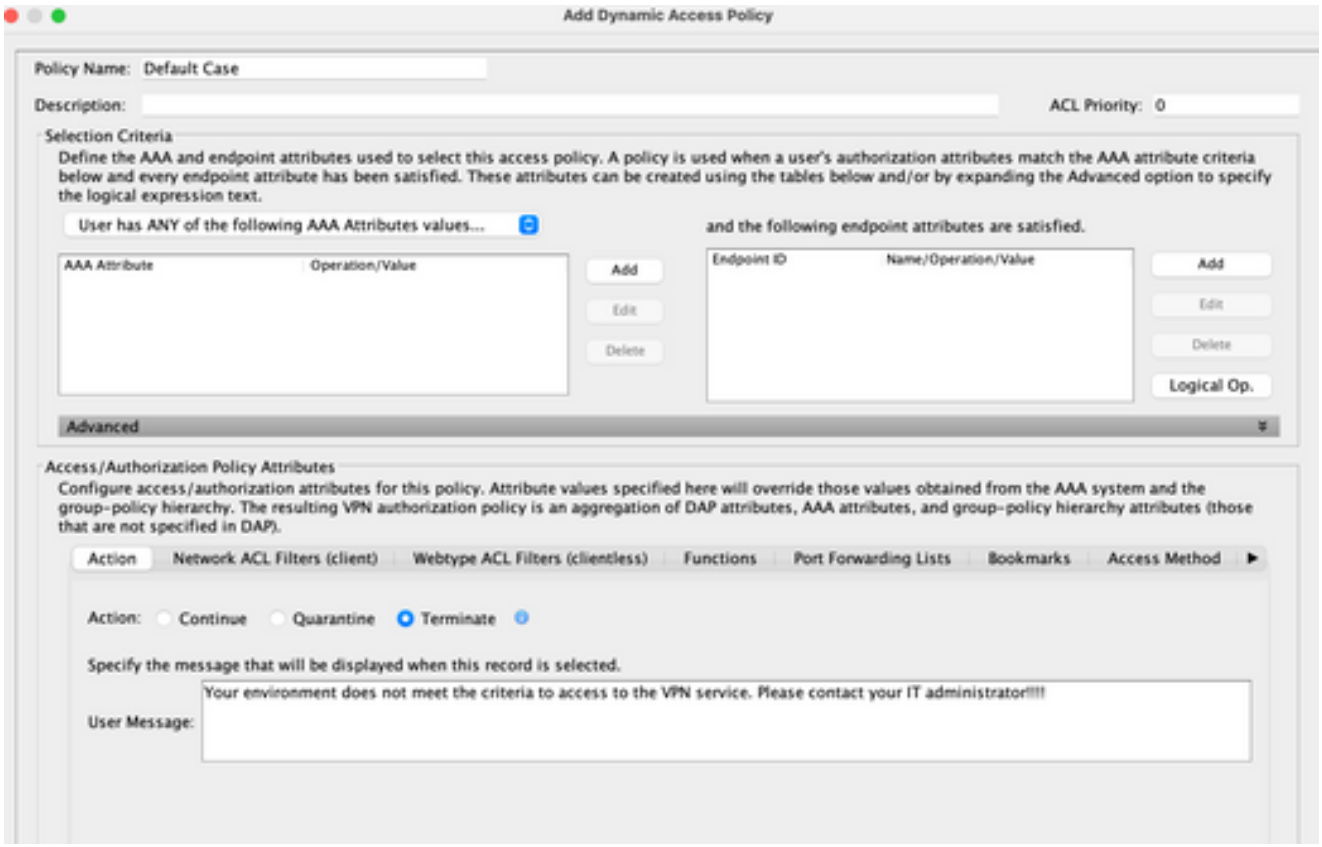
Per assicurarsi che una connessione VPN SSL possa terminare nel caso predefinito, ad esempio quando l'endpoint non corrisponde ad alcun criterio di accesso dinamico configurato, è possibile configurarlo eseguendo la procedura seguente:

Nota: quando si configurano i criteri di accesso dinamico per la prima volta, viene visualizzato un messaggio di errore DAP.xml che indica che non esiste un file di configurazione DAP (DAP.XML). Una volta modificata e salvata la configurazione DAP iniziale, il messaggio non può più essere visualizzato.

-

Passare **a Configurazione > VPN ad accesso remoto > Accesso VPN SSL senza client > Criteri di accesso dinamico** e configurare la procedura seguente:

Figura 30. Criterio di accesso dinamico predefinito: se non viene trovata una corrispondenza con alcun record DAP predefinito, è possibile applicare tale record. Pertanto, l'accesso VPN SSL può essere negato.



a.

Modificare la proprietà DfltAccessPolicy e impostare l'azione **su Termina**.

b.

Fare clic su OK.

•

Aggiungere un nuovo criterio di accesso dinamico **denominato Managed_Endpoints**, come indicato di seguito:

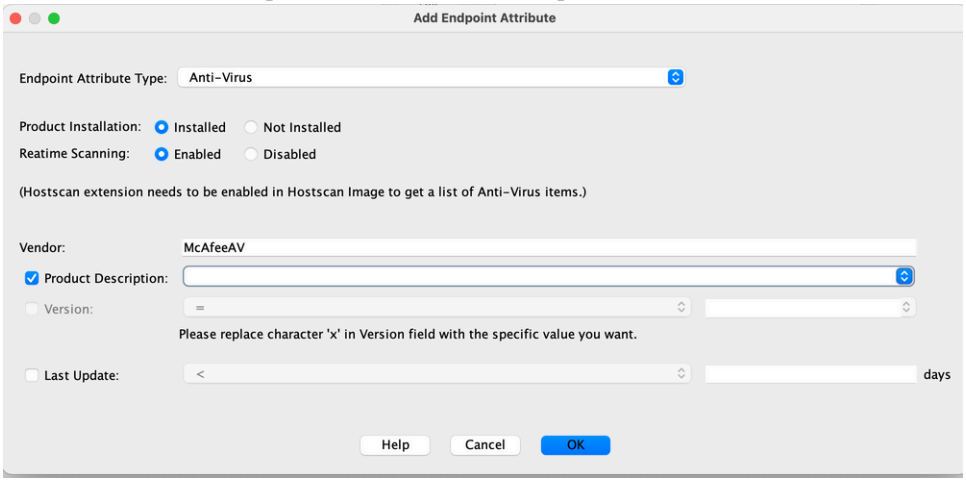
a.

Descrizione:**Employee Client Access**

b.

Aggiungere un tipo di attributo dell'endpoint (antivirus) come mostrato nella Figura 31. Al termine, fate clic su OK.

Figura 31. Attributo endpoint DAP - Advanced Endpoint Assessment AntiVirus può essere utilizzato come criterio DAP per l'accesso client/di rete.



c.

Come mostrato nell'immagine precedente, dall'elenco a discesa della sezione Attributo AAA selezionare User has ALL of the following AAA Attributes Values.

•

Aggiungere (a destra della casella Attributo AAA) un tipo di attributo AAA (LDAP), come mostrato nelle figure 33 e 34. Al termine, fate clic su OK.

Figura 33. Attributo DAP AAA: l'appartenenza al gruppo AAA può essere utilizzata come criterio DAP per identificare un dipendente.

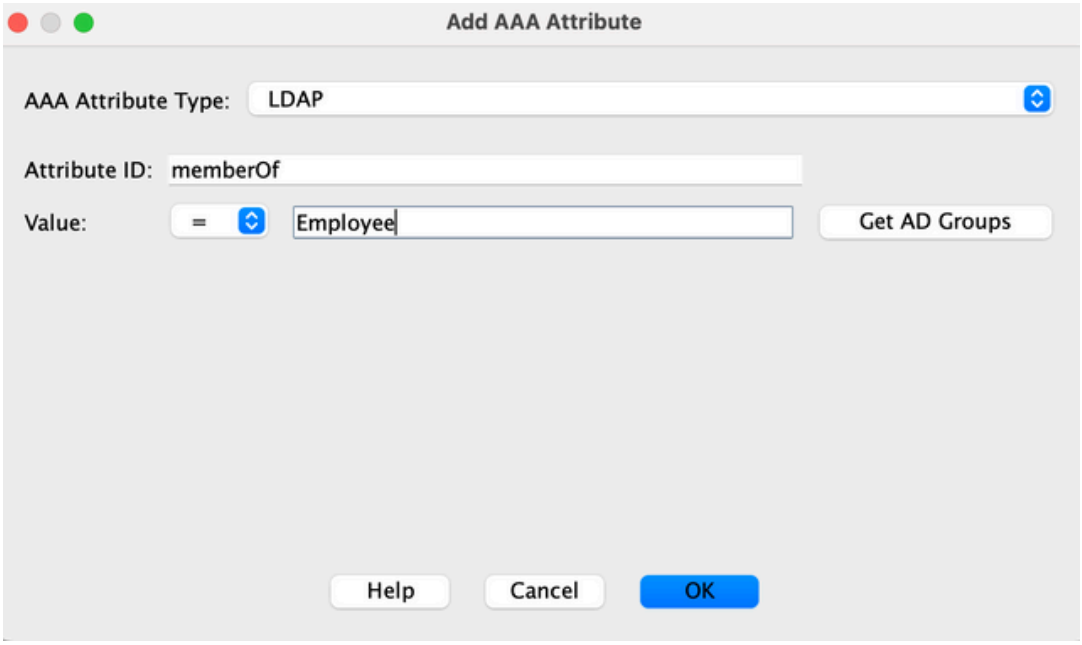
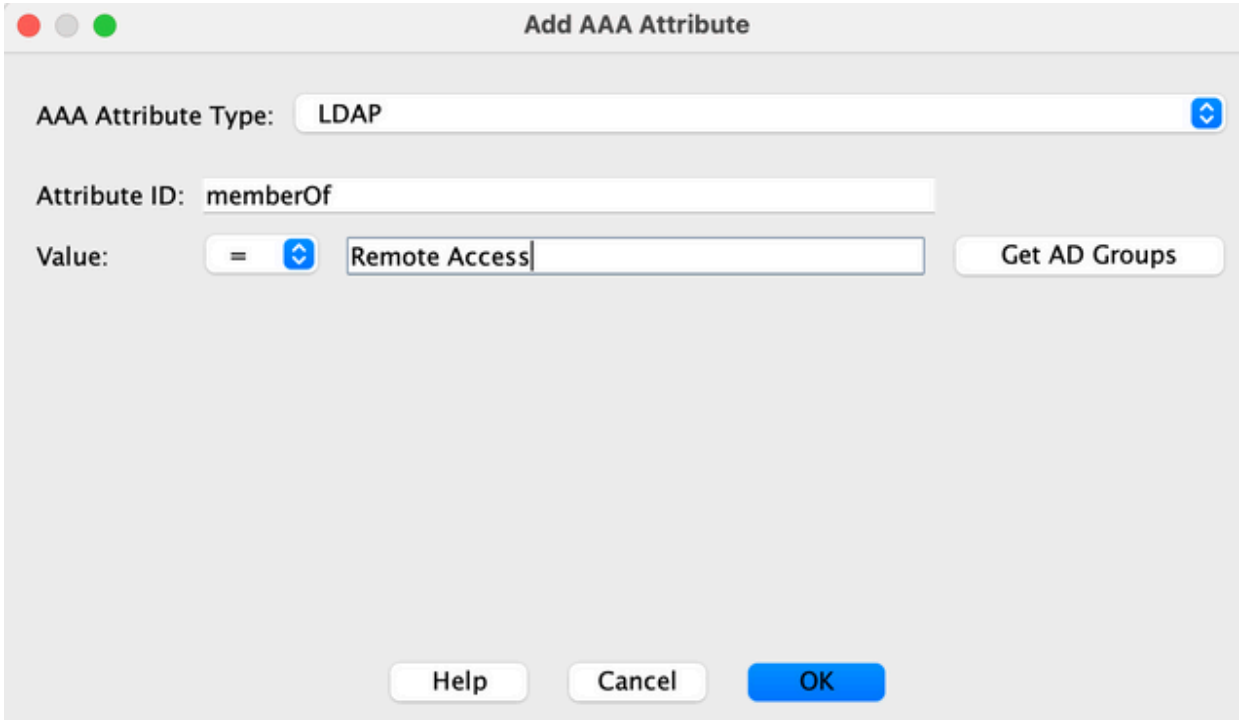


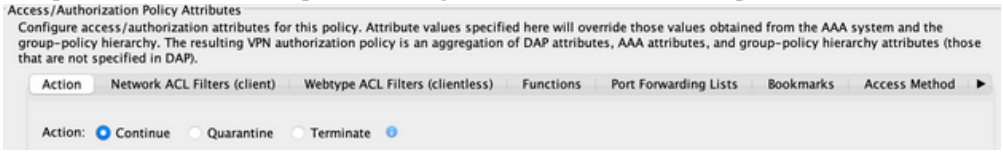
Figura 34. Attributo DAP AAA: è possibile utilizzare l'appartenenza al gruppo AAA come criterio DAP per consentire le funzionalità di Accesso remoto.



-

Nella scheda Azione verificare che l'opzione Azione sia impostata **su Continua**, come mostrato nella Figura 35.

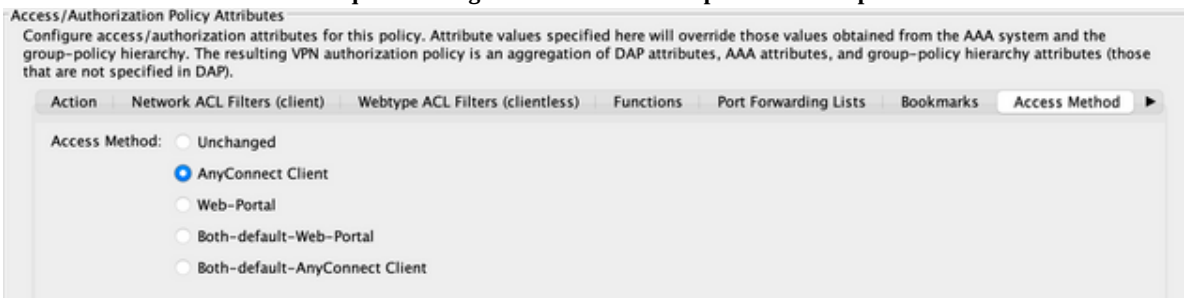
Figura 35. Scheda Azione (Action) - Questa configurazione è necessaria per definire un'elaborazione speciale per una connessione o una sessione specifica. L'accesso VPN può essere negato se un record DAP corrisponde e l'azione è impostata su Termina.



-

Nella scheda Access Method (Metodo di accesso), selezionare Access **MethodAnyConnect Client**, come mostrato nella Figura 36.

Figura 36. Scheda Metodo di accesso: questa configurazione è necessaria per definire i tipi di connessione client VPN SSL.



-

Fare clic su OK, quindi su Applica.

-

Aggiungere un secondo criterio di accesso dinamico **denominato Unmanaged_Endpoints**, come descritto:

a.

Descrizione:**Employee Clientless Access**.

b.

Dall'elenco a discesa nell'immagine precedente della sezione degli attributi AAA, selezionare User has ALL of the following AAA Attributes Values .

-

Aggiungere (a destra del tipo di attributo AAA) un tipo di attributo AAA (LDAP), come mostrato nelle figure 38 e 39. Al termine, fate clic su OK.

Figura 38. Attributo DAP AAA: l'appartenenza al gruppo AAA può essere utilizzata come criterio DAP per identificare un dipendente.

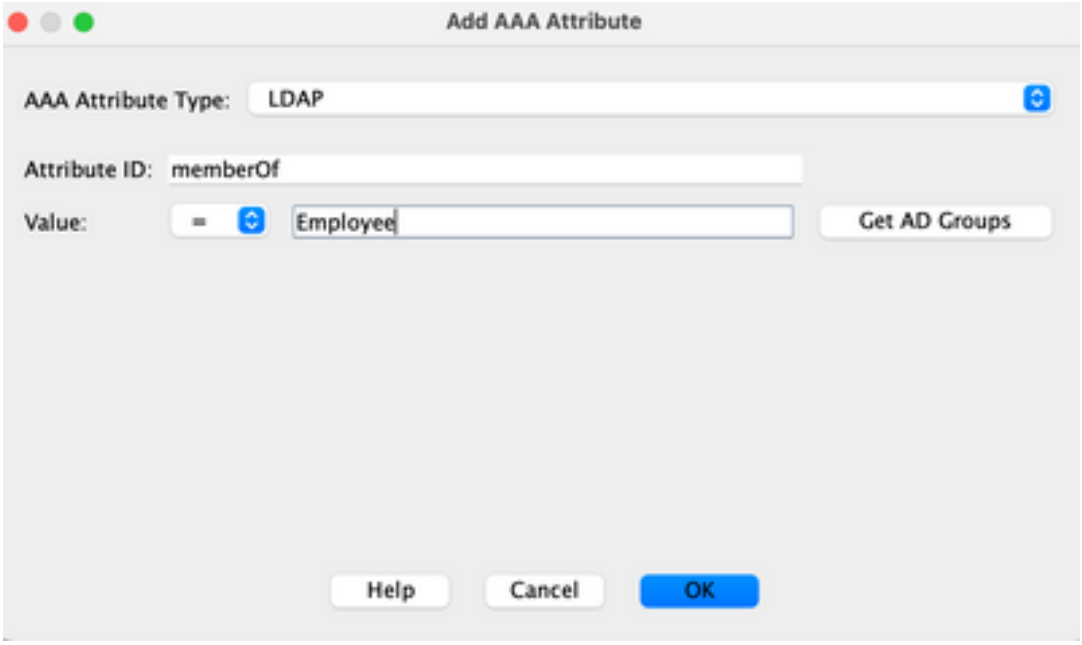
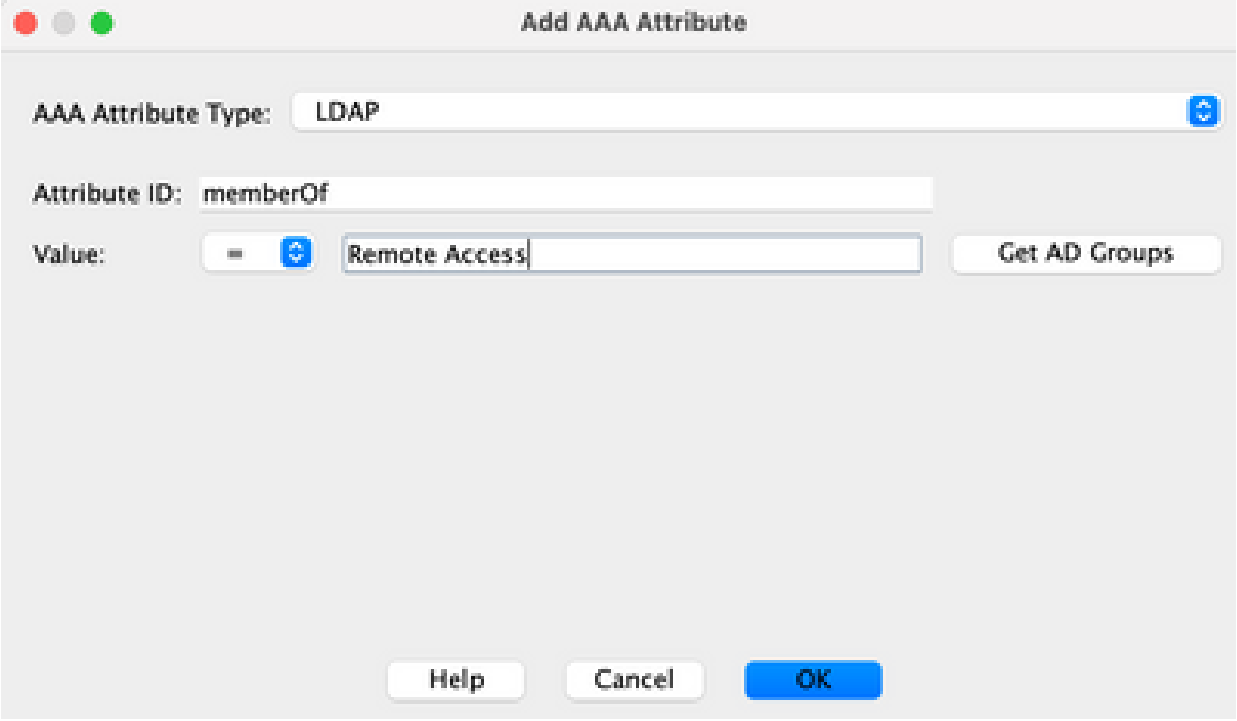


Figura 39. Attributo DAP AAA: è possibile utilizzare l'appartenenza al gruppo AAA come criterio DAP per consentire le funzionalità di Accesso remoto.



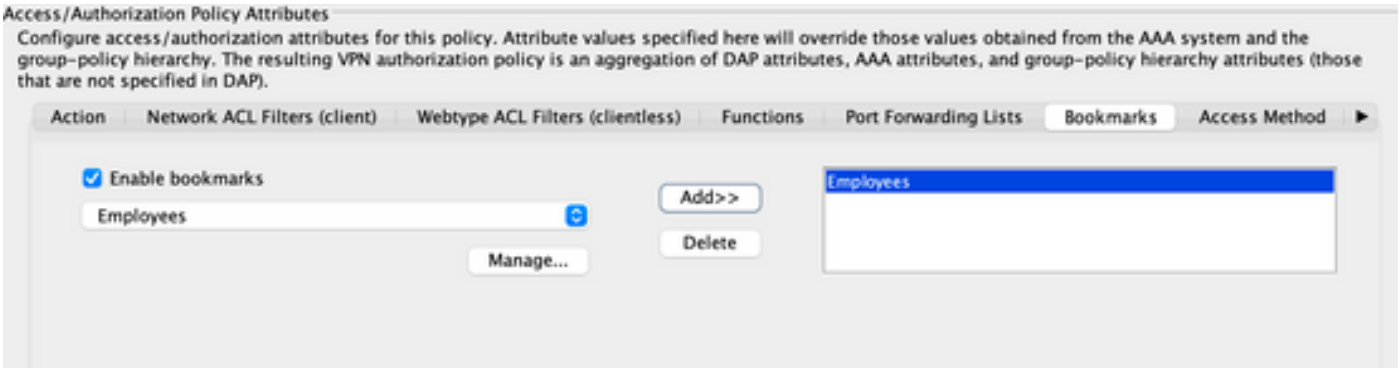
-

Nella scheda Azione verificare che l'opzione Azione sia impostata **su Continua**. (Figura 35)

-

Nella scheda Segnalibri selezionare il nome elenco Dipendenti dall'elenco a discesa e quindi **fare clic su Aggiungi**. Verificare inoltre che i segnalibri Enable siano selezionati, come mostrato nella Figura 40.

Figura 40. Scheda Segnalibri: consente di selezionare e configurare gli elenchi URL per le sessioni utente.



-

a.

Nella scheda Metodo di accesso selezionare il **portale Web** Metodo di accesso. (Figura 36)

- **Fare clic su OK**, **quindi su Applica**.

1. I fornitori possono essere identificati solo tramite gli attributi DAP AAA. Di conseguenza, non è possibile configurare il tipo di attributi dell'endpoint: (Criterio) nel passo 4. Questo approccio è stato concepito esclusivamente per mostrare la versatilità di DAP.

3. Aggiungere un terzo criterio di accesso dinamico **denominato Guest_Access** con le informazioni seguenti:

•

Descrizione:**Guest Clientless Access**.

•

Aggiungere (a destra della casella Attributo endpoint) un tipo di attributo dell'endpoint (criterio), come mostrato nella Figura 37. Al termine, fate clic su OK.

•

Nella Figura 40, dall'elenco a discesa nella sezione Attributo AAA, selezionare User has ALL of the following AAA Attributes Values.

•

Aggiungere (a destra della casella Attributo AAA) un tipo di attributo AAA (LDAP), come mostrato nelle figure 41 e 42. Al termine, fate clic su OK.

Figura 41. È possibile utilizzare Attributo AAA DAP - Appartenenza al gruppo AAA come criterio DAP per identificare un collaboratore esterno

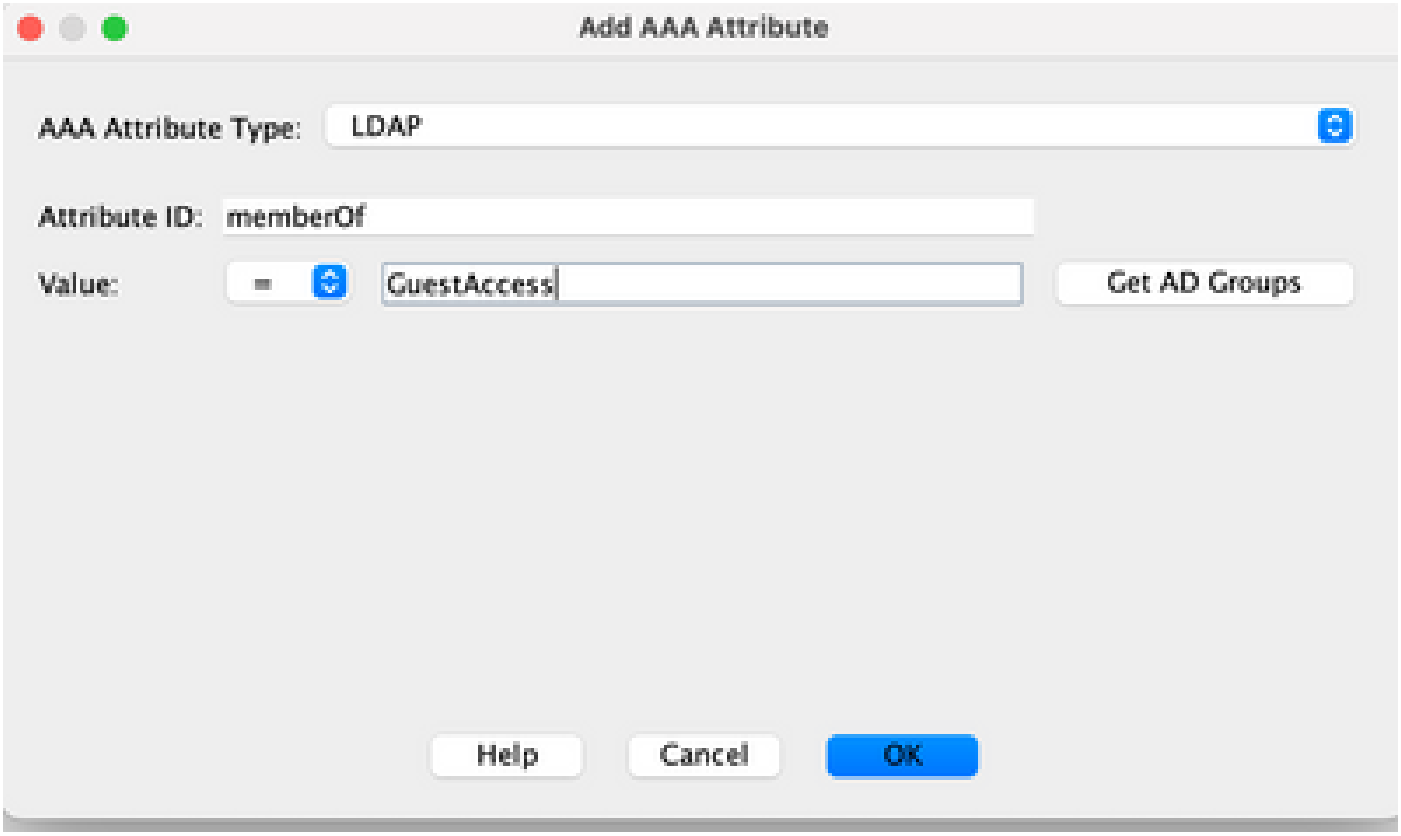
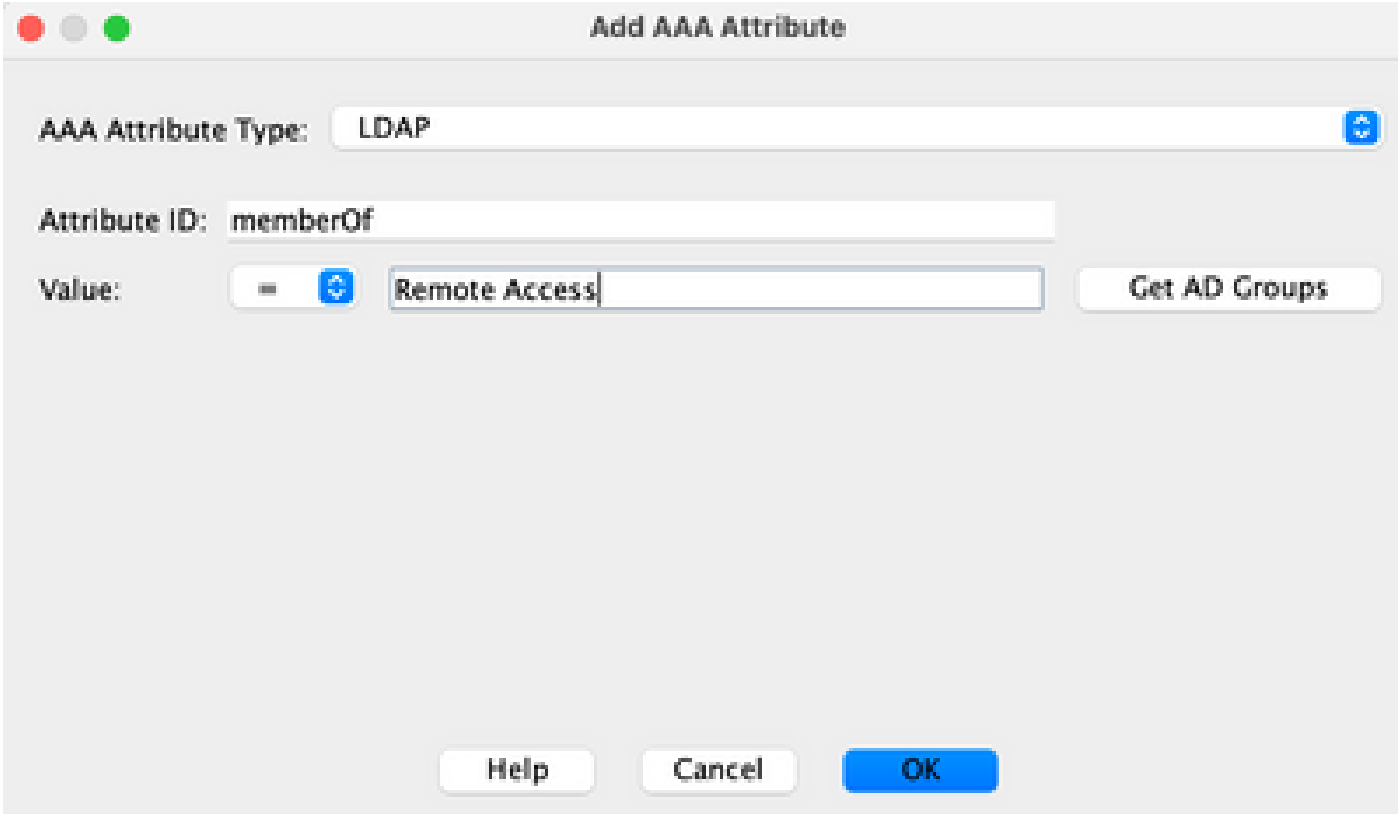


Figura 42. Attributo DAP AAA: è possibile utilizzare l'appartenenza ai gruppi AAA come criterio DAP per consentire le funzionalità di accesso remoto



-

a.

Nella scheda Azione verificare che l'opzione Azione sia impostata su **Continua**. (Figura 35)

b.

Nella scheda Segnalibri selezionare il nome dell'elenco **Appaltatori** dall'elenco a discesa e quindi fare clic su Aggiungi. Verificare inoltre che l'opzione **Abilita segnalibri** sia selezionata. (Figura 40.)

c.

Nella scheda Metodo di accesso selezionare il portale Web Metodo di accesso. (Figura 36)

d.

Fare clic su **OK**, quindi su **Applica**.

Conclusioni

In base ai requisiti SSL VPN di Accesso remoto del client indicati in questo esempio, questa soluzione soddisfa i requisiti VPN di Accesso remoto del client.

Con gli ambienti VPN dinamici in evoluzione nella fase di unione, Dynamic Access Policies è in grado di adattarsi e adattarsi alle frequenti modifiche della configurazione di Internet, ai vari ruoli che ogni utente può ricoprire all'interno di un'organizzazione e agli accessi da siti di accesso remoto gestiti e non gestiti con configurazioni e livelli di sicurezza diversi.

Le policy di accesso dinamico sono integrate da tecnologie legacy nuove e collaudate, tra cui Advanced Endpoint Assessment, Host Scan, Secure Desktop, AAA e Local Access Policies. Di conseguenza, le organizzazioni possono garantire un accesso VPN sicuro a qualsiasi risorsa di rete da qualsiasi luogo.

Informazioni correlate

- **Supporto tecnico Cisco e download**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).