ASA 8.x: Configurazione AnyConnect SSL VPN CAC-SmartCard con supporto MAC

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio su Cisco Adaptive Security Appliance (ASA) per l'accesso remoto VPN AnyConnect per il supporto MAC con scheda CAC (Common Access Card) per l'autenticazione.

Lo scopo di questo documento è coprire la configurazione di Cisco ASA con Adaptive Security Device Manager (ASDM), Cisco AnyConnect VPN Client e Microsoft Active Directory (AD)/Lightweight Directory Access Protocol (LDAP).

La configurazione di questa guida utilizza il server AD/LDAP Microsoft. Nel documento vengono inoltre descritte alcune funzionalità avanzate, ad esempio OCSP, mappe di attributi LDAP e DAP (Dynamic Access Policy).

Prerequisiti

Requisiti

Una conoscenza di base di Cisco ASA, Cisco AnyConnect Client, Microsoft AD/LDAP e Public Key Infrastructure (PKI) è utile per comprendere l'installazione completa. La familiarità con l'appartenenza ai gruppi AD, con le proprietà utente e con gli oggetti LDAP facilita la correlazione del processo di autorizzazione tra gli attributi dei certificati e gli oggetti AD/LDAP.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 5500 Adaptive Security Appliance (ASA) con software versione 8.0(x) e successive

- Cisco Adaptive Security Device Manager (ASDM) versione 6.x per ASA 8.x
- Cisco AnyConnect VPN Client 2.2 con supporto MAC

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.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione di Cisco ASA

In questa sezione viene descritta la configurazione di Cisco ASA tramite ASDM. Illustra la procedura necessaria per distribuire un tunnel di accesso remoto VPN tramite una connessione AnyConnect SSL. Il certificato CAC viene utilizzato per l'autenticazione e l'attributo UPN (User Principal Name) nel certificato viene compilato in Active Directory per l'autorizzazione.

Considerazioni sulla distribuzione

- Questa guida NON riguarda le configurazioni di base come interfacce, DNS, NTP, routing, accesso ai dispositivi, accesso ASDM e così via. Si presume che l'operatore di rete abbia familiarità con queste configurazioni.per ulteriori informazioni, fare riferimento a Appliance di sicurezza multifunzione.
- Le sezioni evidenziate in ROSSO sono configurazioni obbligatorie necessarie per l'accesso VPN di base. Ad esempio, è possibile configurare un tunnel VPN con la scheda CAC senza eseguire controlli OCSP, mapping LDAP e controlli DAP (Dynamic Access Policy). Il DoD impone il controllo OCSP, ma il tunnel funziona senza OCSP configurato.
- Le sezioni evidenziate in BLU sono caratteristiche avanzate che possono essere incluse per aumentare la protezione del progetto.
- ASDM e AnyConnect/SSL VPN non possono utilizzare le stesse porte sulla stessa interfaccia. Per ottenere l'accesso, si consiglia di modificare le porte su una di esse. Ad esempio, usare la porta 445 per ASDM e lasciare la porta 443 per la VPN AC/SSL. L'accesso all'URL ASDM è stato modificato in 8.x. Utilizzare `https://<indirizzo_ip>:<porta>/admin.html`.
- L'immagine ASA richiesta è almeno 8.0.2.19 e ASDM 6.0.2.
- AnyConnect/CAC è supportato con Vista.
- Vedere Appendice A per esempi di mappatura dei criteri di accesso dinamico e LDAP per un'ulteriore applicazione dei criteri.
- Vedere Appendice D su come controllare gli oggetti LDAP in MS.
- Per un elenco delle porte dell'applicazione per la configurazione del firewall, vedere Informazioni correlate.

Configurazione di autenticazione, autorizzazione e accounting (AAA)

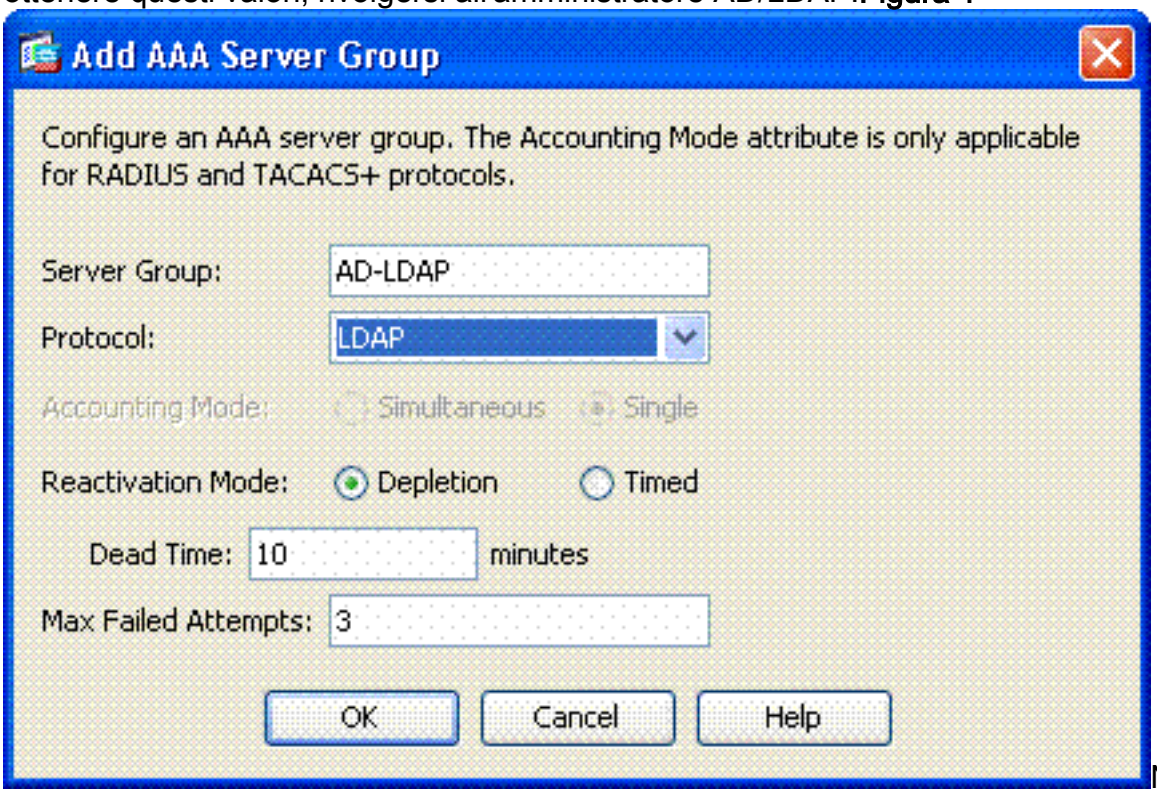
L'utente viene autenticato con l'utilizzo del certificato nella scheda di accesso comune (CAC)

tramite il server DISACertificate Authority (CA) o il server CA della propria organizzazione. Il certificato deve essere valido per l'accesso remoto alla rete. Oltre all'autenticazione, è necessario essere autorizzati a utilizzare un oggetto Microsoft Active Directory o LDAP (Lightweight Directory Access Protocol). Il Dipartimento della Difesa (DoD) richiede l'utilizzo dell'attributo UPN (User Principal Name) per l'autorizzazione, che fa parte della sezione Nome alternativo soggetto (SAN) del certificato. L'UPN o EDI/PI deve essere nel formato 1234567890@mil. Queste configurazioni mostrano come configurare il server AAA nell'appliance ASA con un server LDAP per l'autorizzazione. Vedere Appendice A per ulteriori informazioni sulla configurazione della mappatura degli oggetti LDAP.

Configura server LDAP

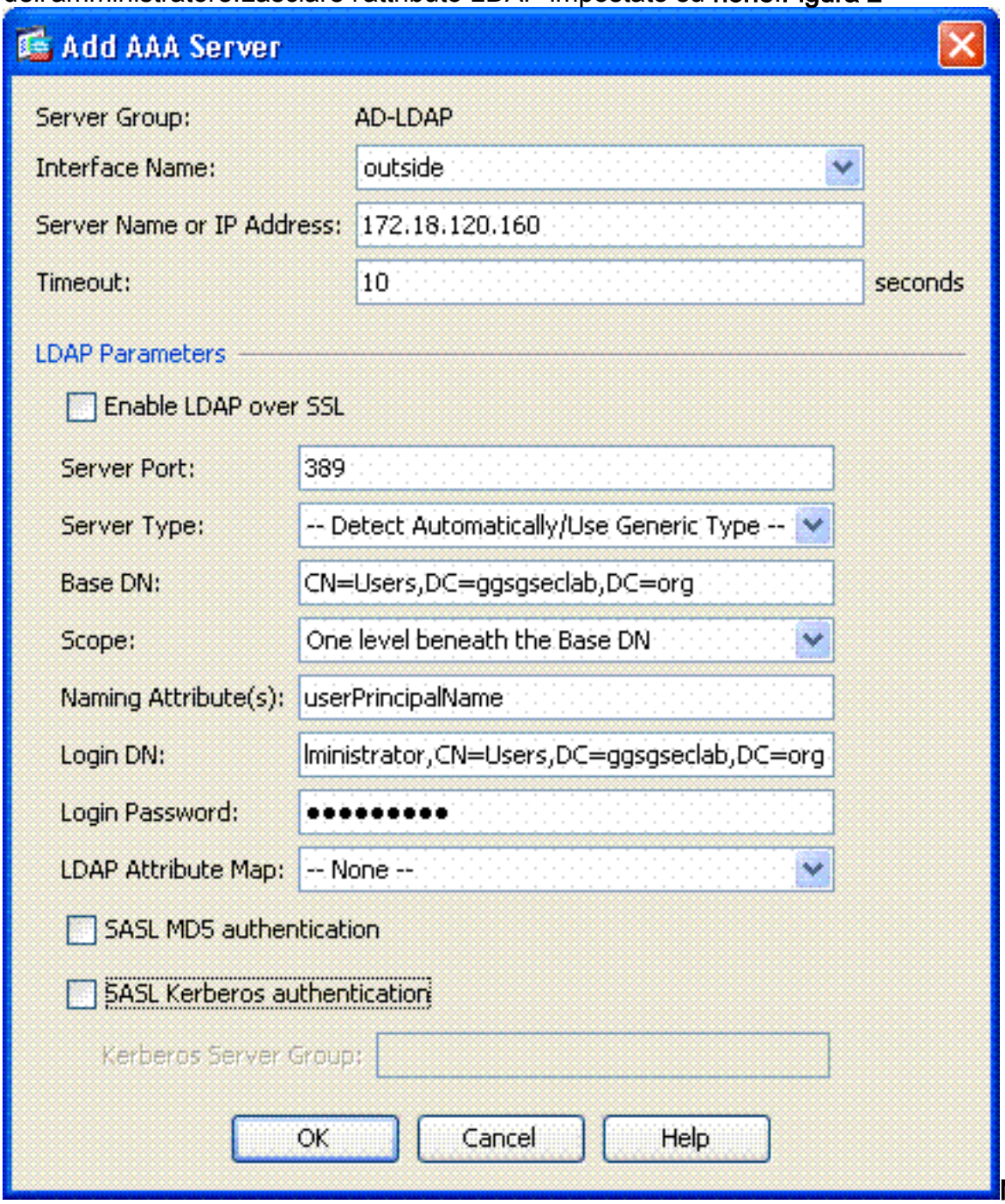
Attenersi alla seguente procedura:

1. Scegliere **VPN ad accesso remoto > Configurazione AAA > Gruppo server AAA.**
2. Nella tabella dei gruppi di server AAA, fare clic su **Add 3**.
3. Immettere il nome del gruppo di server e scegliere **LDAP** dal pulsante di opzione del protocollo. Vedere la Figura 1.
4. In Server nella tabella dei gruppi selezionata fare clic su **Aggiungi**. Assicurarsi che il server creato sia evidenziato nella tabella precedente.
5. Nella finestra Modifica server AAA, effettuare le seguenti operazioni. Vedere la Figura 2.**Nota:** scegliere l'opzione **Abilita LDAP su SSL** se per questo tipo di connessione è configurato LDAP/AD.Scegliere l'interfaccia in cui si trova LDAP. Questa guida viene mostrata all'interno dell'interfaccia.Immettere l'indirizzo IP del server.Immettere la **porta del server**. La porta LDAP predefinita è 389.Scegliere **Tipo server**.Immettere il **DN di base**. Per ottenere questi valori, rivolgersi all'amministratore AD/LDAP.**Figura 1**



Nell'ambito dell'opzione scegliere la risposta appropriata. Dipende dal DN di base. Per assistenza, rivolgersi all'amministratore AD/LDAP.Nell'attributo di denominazione, immettere **userPrincipalName**. Attributo utilizzato per l'autorizzazione utente nel server AD/LDAP.Nel DN di accesso, immettere il DN dell'amministratore.**Nota:** si dispone dei diritti amministrativi o

di accesso per visualizzare/ricercare la struttura LDAP che include gli oggetti utente e l'appartenenza ai gruppi.In Password di accesso, immettere la password dell'amministratore.Lasciare l'attributo LDAP impostato su **none**.**Figura 2**



Nota: utilizzare questa opzione in seguito nella configurazione per aggiungere altri oggetti AD/LDAP per l'autorizzazione.Scegliere **OK**.

6. Scegliere **OK**.

Gestisci certificati

Per installare i certificati sull'appliance ASA, è necessario eseguire due passaggi. Installare innanzitutto i certificati CA necessari (Autorità di certificazione principale e subordinata). In secondo luogo, registrare l'ASA su una CA specifica e ottenere il certificato di identità. DoD PKI utilizza questi certificati, Root CA2, Class 3 Root, CA## Intermediate con cui è registrata l'ASA, certificato ID ASA e certificato OCSP. Se tuttavia si sceglie di non utilizzare OCSP, *non è* necessario installare il certificato.

Nota: contattare il punto di controllo di sicurezza per ottenere i certificati radice e le istruzioni su come registrare un certificato di identità per un dispositivo. Un certificato SSL deve essere sufficiente per consentire all'appliance ASA di accedere in modalità remota. *Non* è richiesto un certificato SAN doppio.

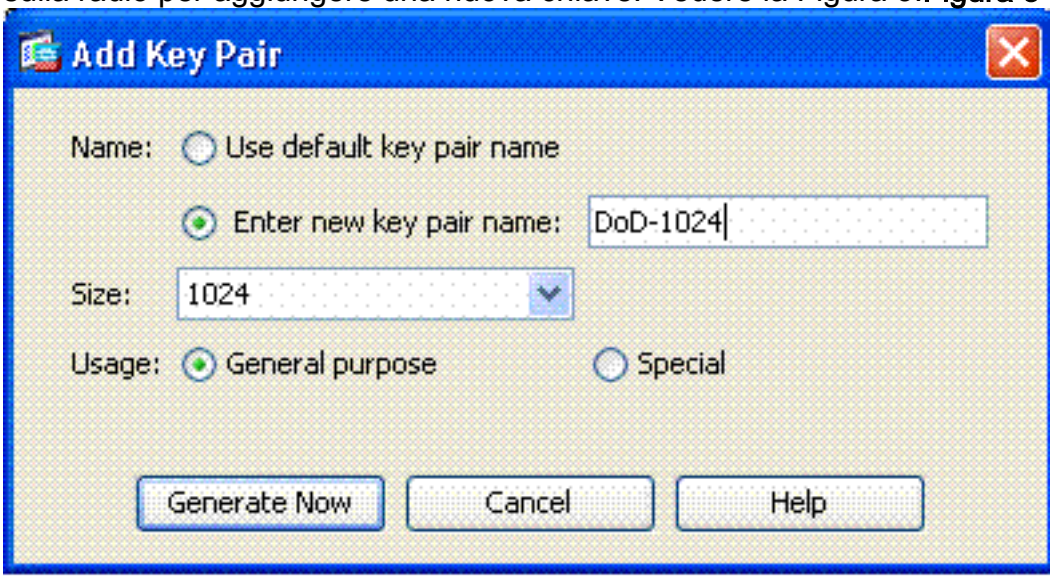
Nota: sul computer locale deve essere installata anche la catena DoD CA. I certificati possono essere visualizzati nell'archivio certificati Microsoft con Internet Explorer. Il DoD ha generato un file batch che aggiunge automaticamente tutte le CA al computer. Per ulteriori informazioni, contattare il POC PKI.

Nota: la radice DoD CA2 e Class 3, nonché l'ID ASA e il intermedio CA che hanno rilasciato il certificato ASA, devono essere le uniche CA necessarie per l'autenticazione dell'utente. Tutti gli intermedi CA correnti rientrano nella catena radice CA2 e classe 3 e sono considerati attendibili se vengono aggiunte le directory radice CA2 e classe 3.

Genera chiavi

Attenersi alla seguente procedura:

1. Scegliere **VPN ad accesso remoto > Gestione certificati > Certificato di identità > Aggiungi**.
2. Selezionare **Add a new id certificate** (Aggiungi **un nuovo certificato ID)**, quindi **New** (Nuovo) tramite l'opzione della coppia di chiavi.
3. Nella finestra Aggiungi coppia di chiavi, immettere il nome di una chiave, **DoD-1024**. Fare clic sulla radio per aggiungere una nuova chiave. Vedere la Figura 3.**Figura 3**



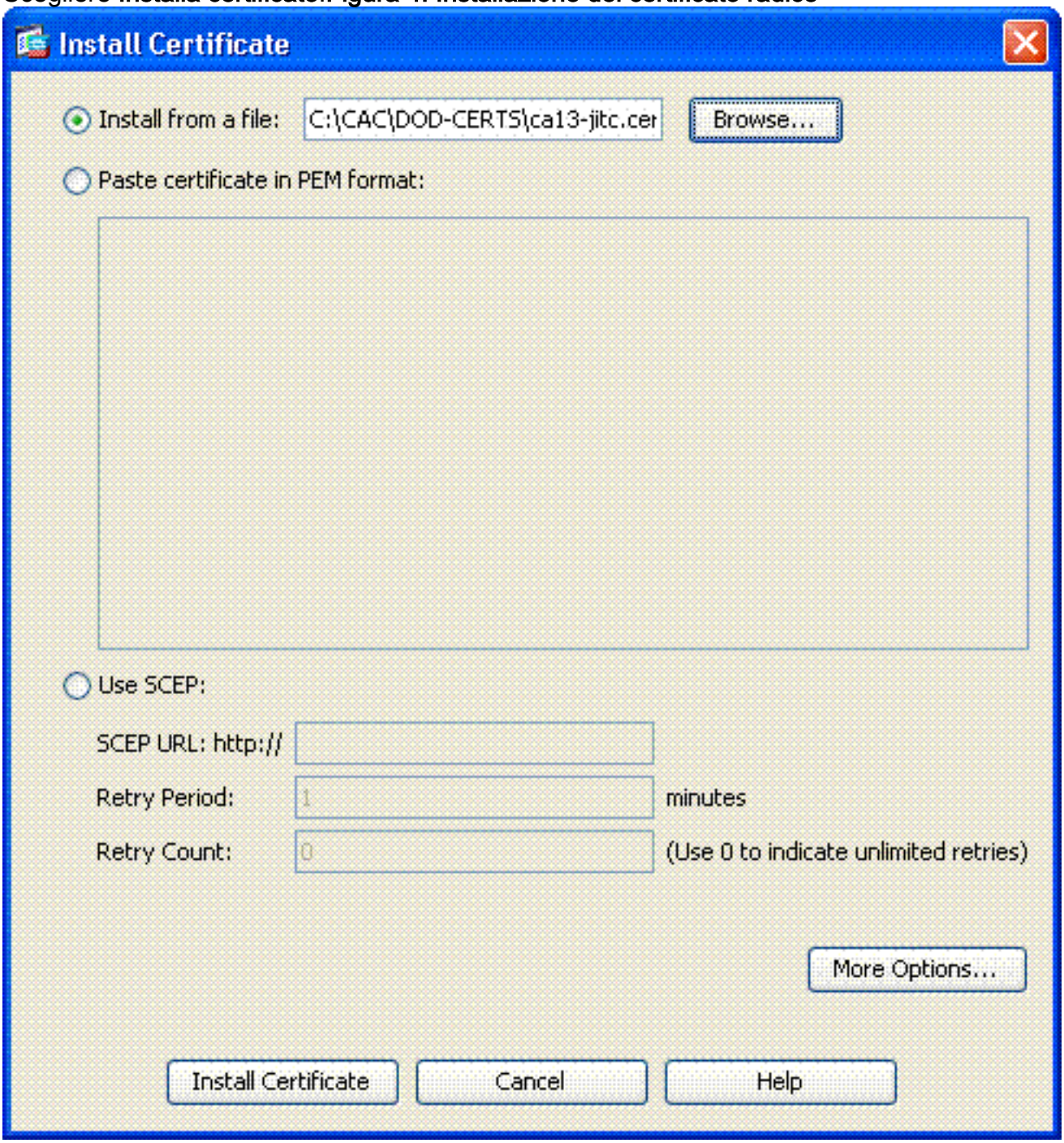
4. Scegliere le dimensioni della chiave.
5. Utilizzo per **scopi generici**.
6. Fare clic su **Genera**.**Nota: la** CA radice DoD 2 utilizza una chiave a 2048 bit. Per poter utilizzare questa CA, è necessario generare una seconda chiave che utilizza una coppia di chiavi a 2048 bit. Per aggiungere una seconda chiave, completare i passaggi precedenti.

Installa certificati CA radice

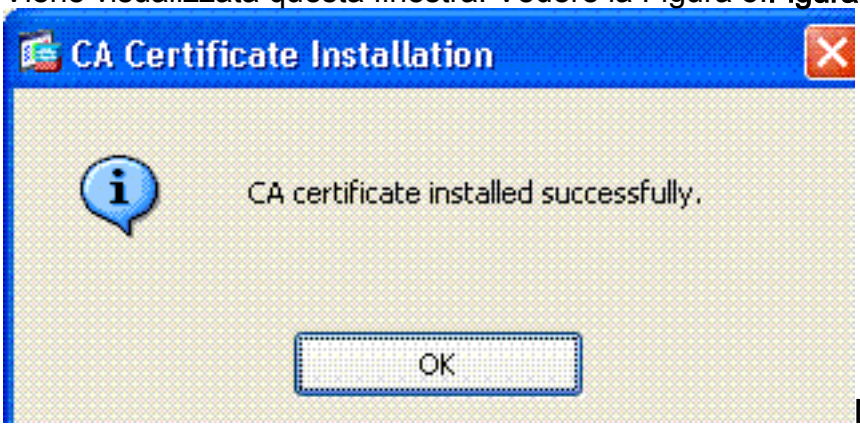
Attenersi alla seguente procedura:

1. Scegliere **VPN ad accesso remoto > Gestione certificati > Certificato CA > Aggiungi**.
2. Scegliere **Installa da file** e individuare il certificato.

3. Scegliere **Installa certificato.Figura 4: Installazione del certificato radice**

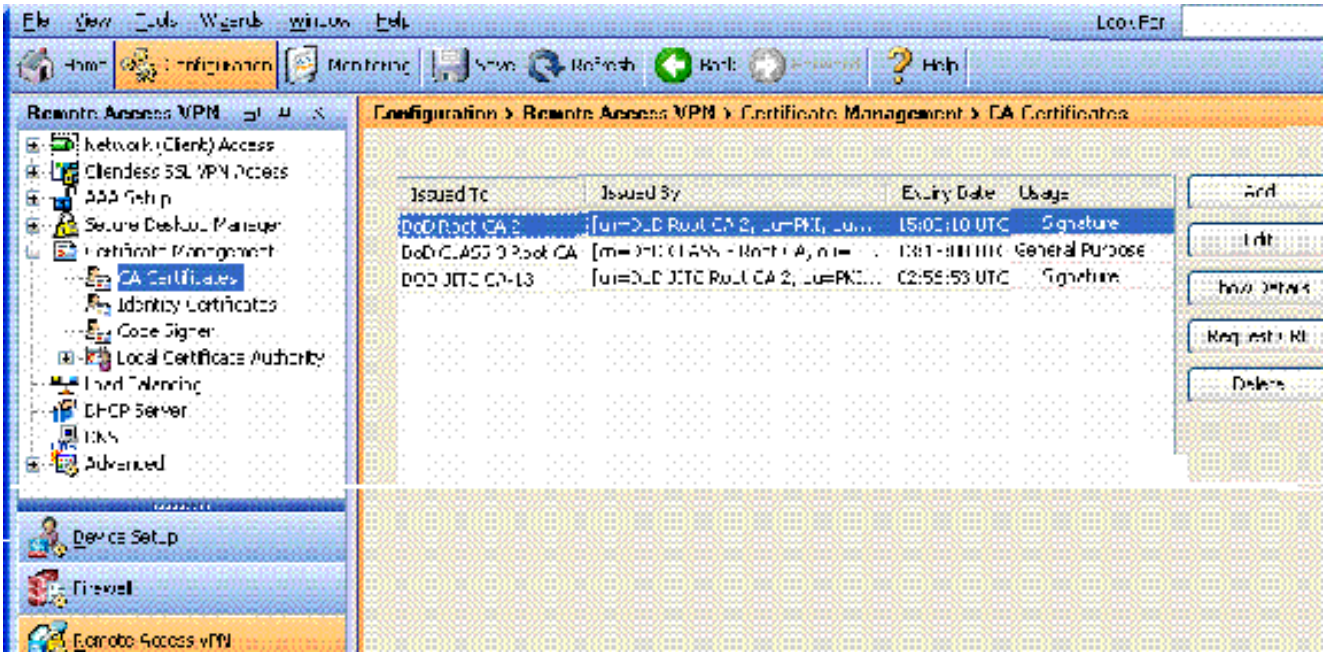


4. Viene visualizzata questa finestra. Vedere la Figura 5.**Figura 5**



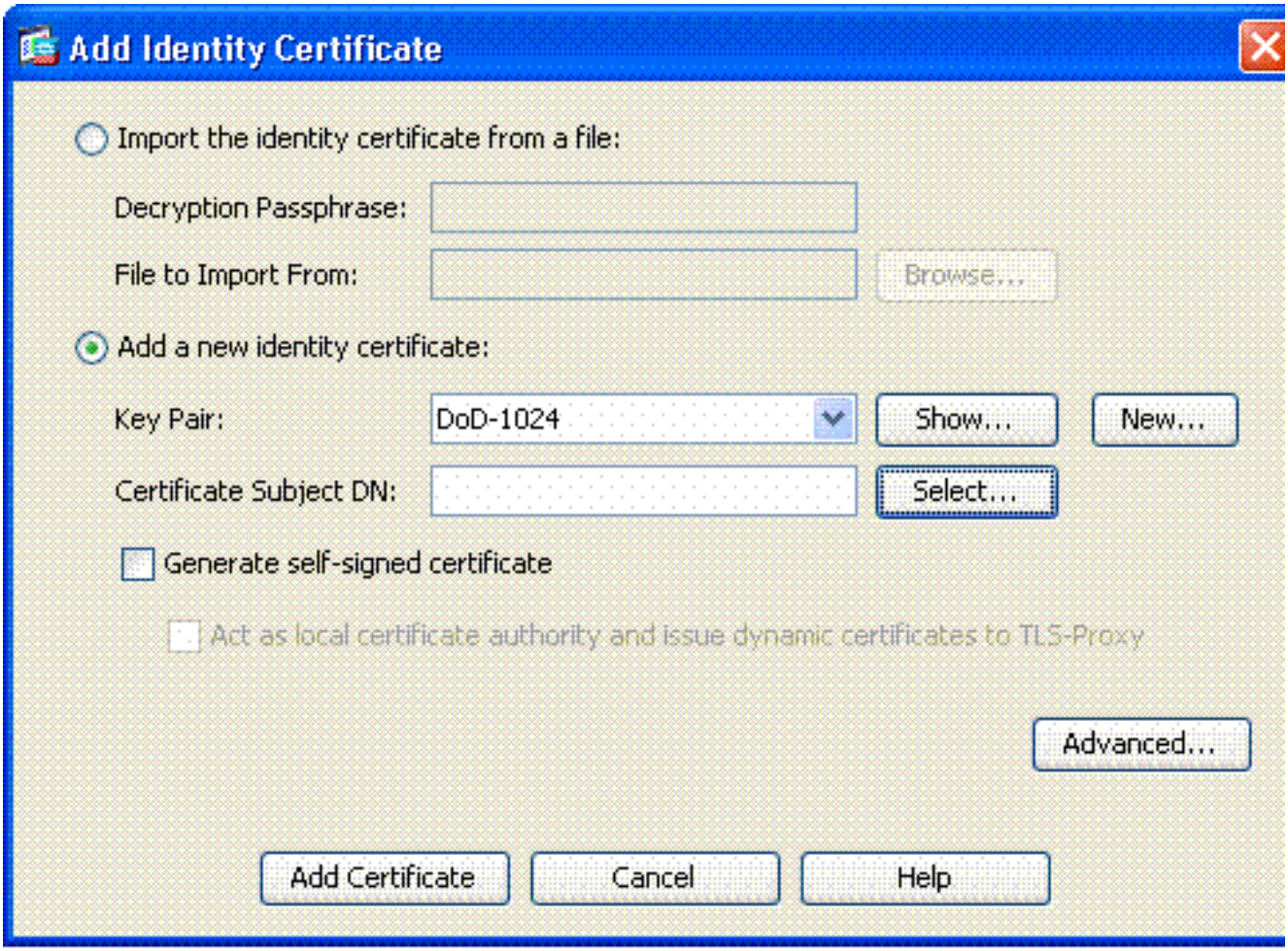
Nota: ripetere i passaggi da 1 a 3 per ogni certificato che si desidera installare. DoD PKI richiede un certificato per ognuno dei seguenti elementi: CA radice 2, radice classe 3, CA## Intermedio, ID ASA e server OCSP. Il certificato OCSP non è necessario se non si utilizza OCSP.**Figura 6: Installazione**

del certificato radice



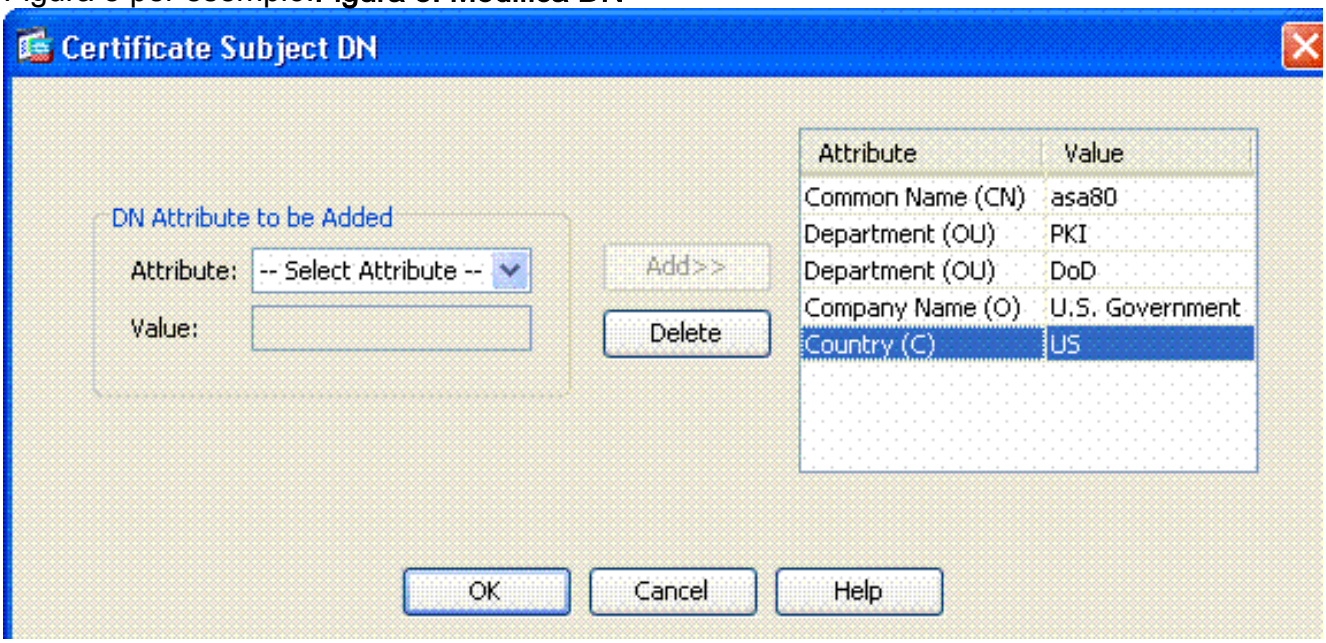
Registra ASA e installa certificato di identità

1. Scegliere **VPN ad accesso remoto > Gestione certificati > Certificato di identità > Aggiungi**.
2. Scegliere **Aggiungi nuovo certificato ID**.
3. Scegliere la coppia di tasti **DoD-1024**. Vedere la figura 7**Figura 7: Parametri del certificato di identità**

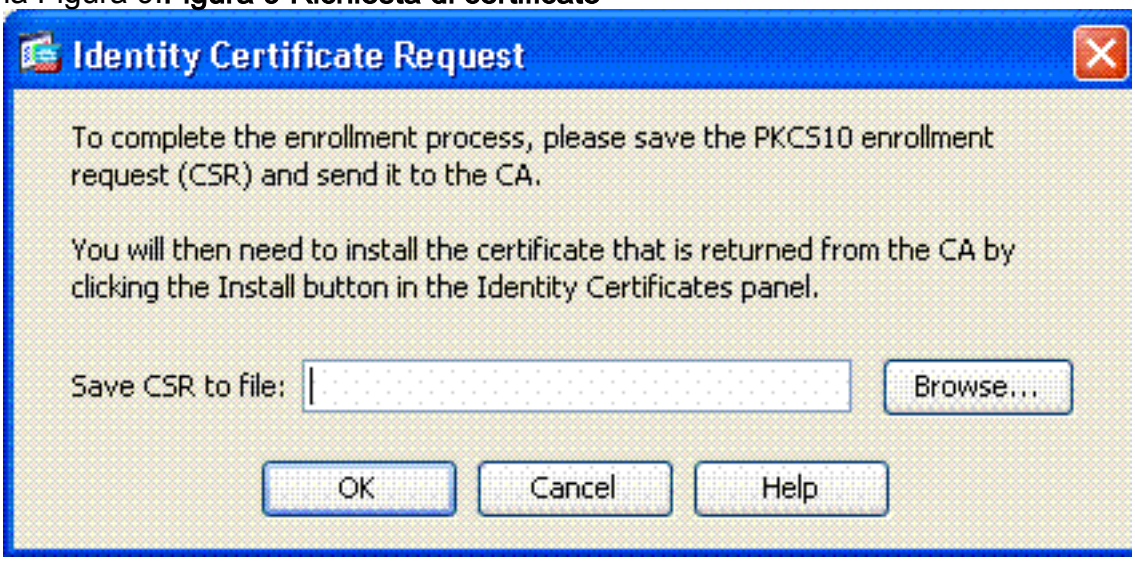


4. Selezionare la casella DN oggetto certificato e fare clic su **Seleziona**.

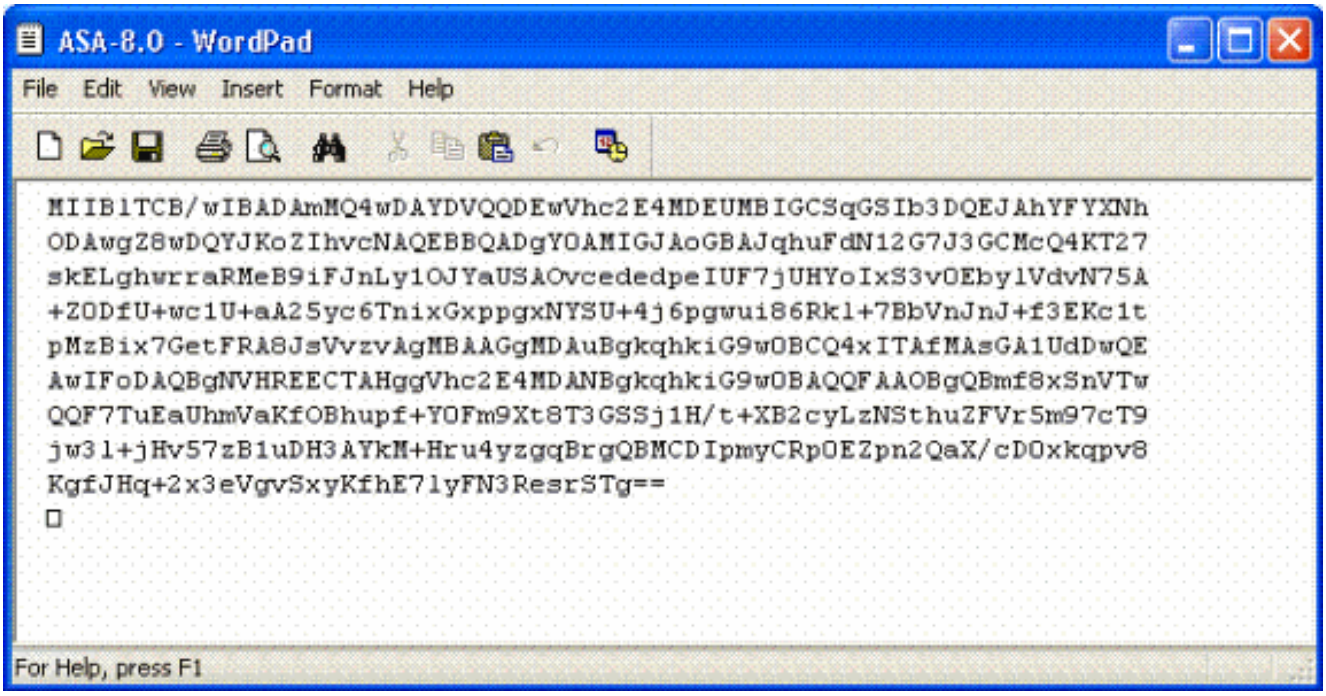
5. Nella finestra DN soggetto certificato immettere le informazioni sulla periferica. Vedere la Figura 8 per esempio.**Figura 8: Modifica DN**



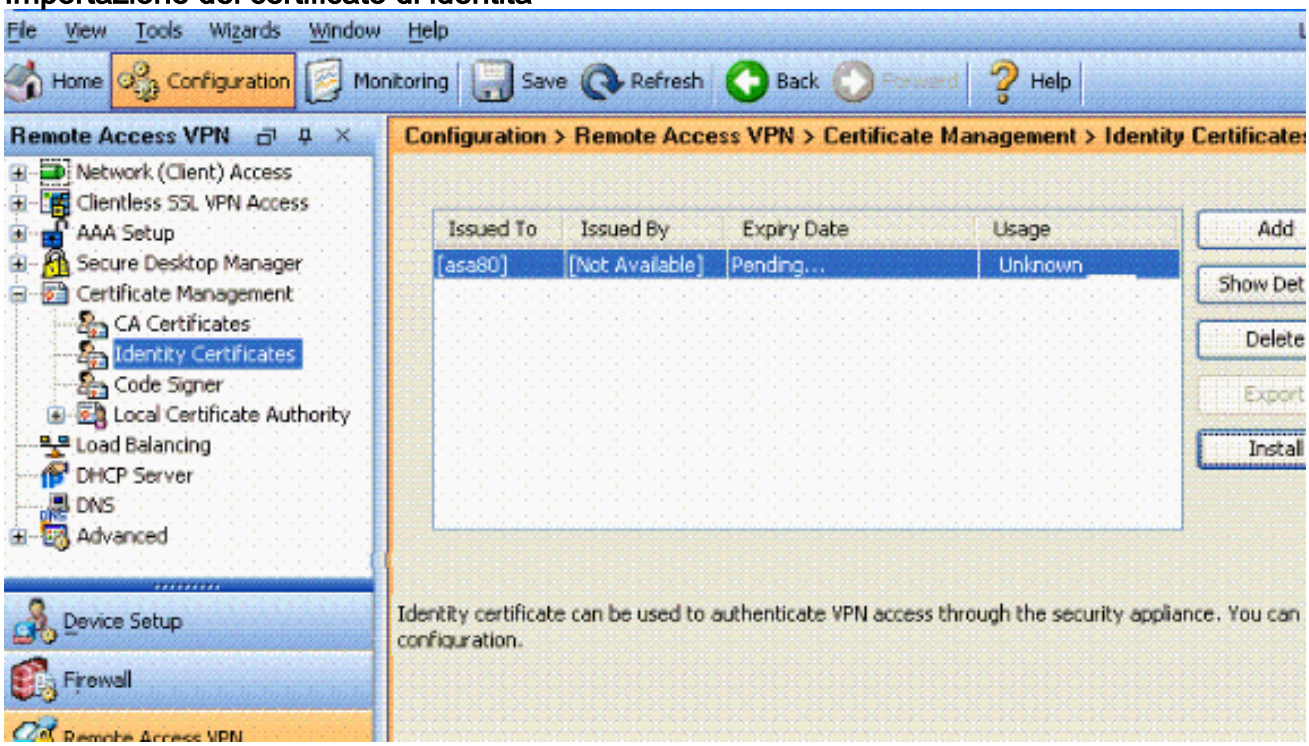
6. Scegliere **OK**.**Nota:** assicurarsi di utilizzare il nome host del dispositivo configurato nel sistema quando si aggiunge il DN dell'oggetto. Il POC PKI può indicare i campi obbligatori obbligatori obbligatori.
7. Scegliere **Aggiungi certificato**.
8. Fare clic su **Sfoglia** per selezionare la directory in cui si desidera salvare la richiesta. Vedere la Figura 9.**Figura 9 Richiesta di certificato**



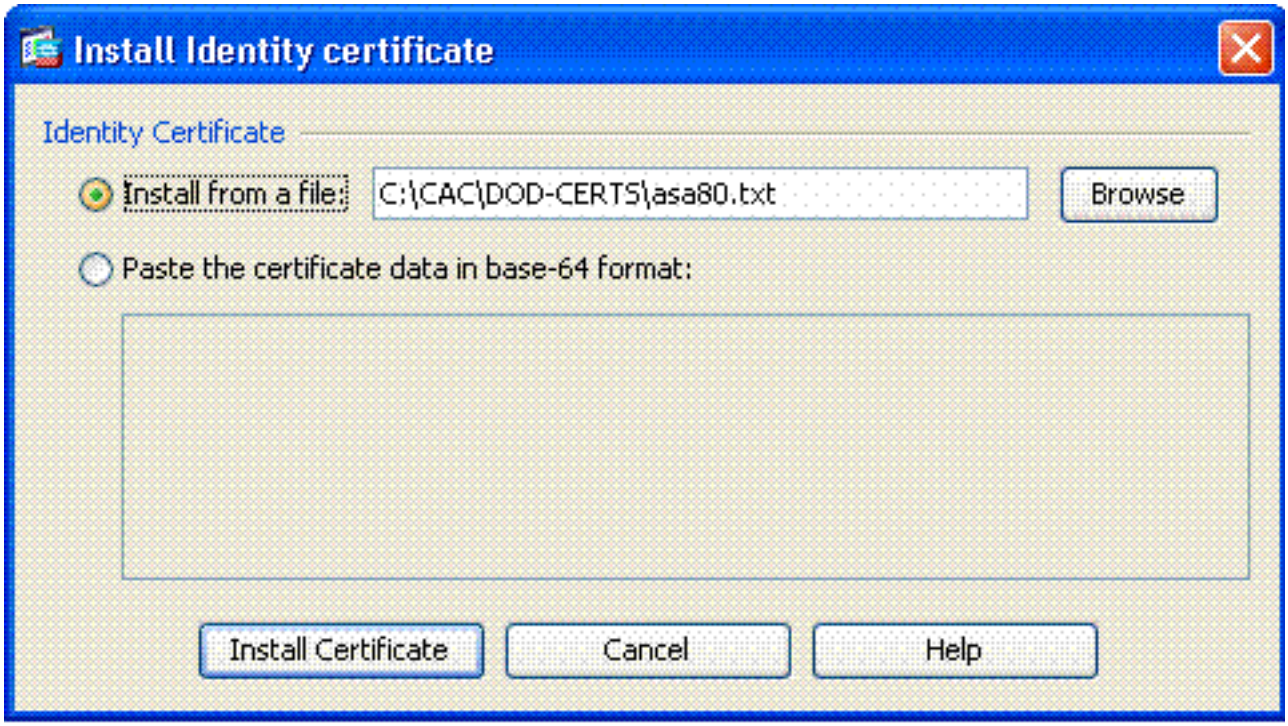
9. Aprire il file con WordPad, copiare la richiesta nella documentazione appropriata e inviarla al POC PKI. Vedere la Figura 10.**Figura 10: Richiesta di registrazione**



10. Dopo aver ricevuto il certificato dall'amministratore della CA, scegliere **VPN ad accesso remoto > Gestione certificati > Certificato ID > Installa**. Vedere la Figura 11.**Figura 11: Importazione del certificato di identità**



11. Nella finestra Installa certificato individuare il certificato ID e **scegliere Installa certificato**. Vedere la Figura 12 per esempio.**Figura 12: Installazione del certificato di identità**



Nota: si consiglia di esportare il trust point del certificato ID per salvare il certificato emesso e le coppie di chiavi. In questo modo, l'amministratore ASA può importare le coppie di certificati e chiavi in una nuova appliance ASA in caso di autorizzazione al reso (RMA) o di errore hardware. Per ulteriori informazioni, fare riferimento a Esportazione e importazione di trust.**Nota:** per salvare la configurazione nella memoria flash, fare clic su **SAVE**.

Configurazione VPN AnyConnect

Per configurare i parametri VPN in ASDM, è possibile procedere in due modi. La prima opzione consiste nell'utilizzare la procedura guidata SSL VPN. Si tratta di uno strumento facile da utilizzare per gli utenti che non conoscono la configurazione VPN. La seconda opzione consiste nel farlo manualmente e nel passare attraverso ciascuna opzione. Questa guida alla configurazione utilizza il metodo manuale.

Nota: per ottenere il client AC dall'utente, è possibile procedere in due modi:

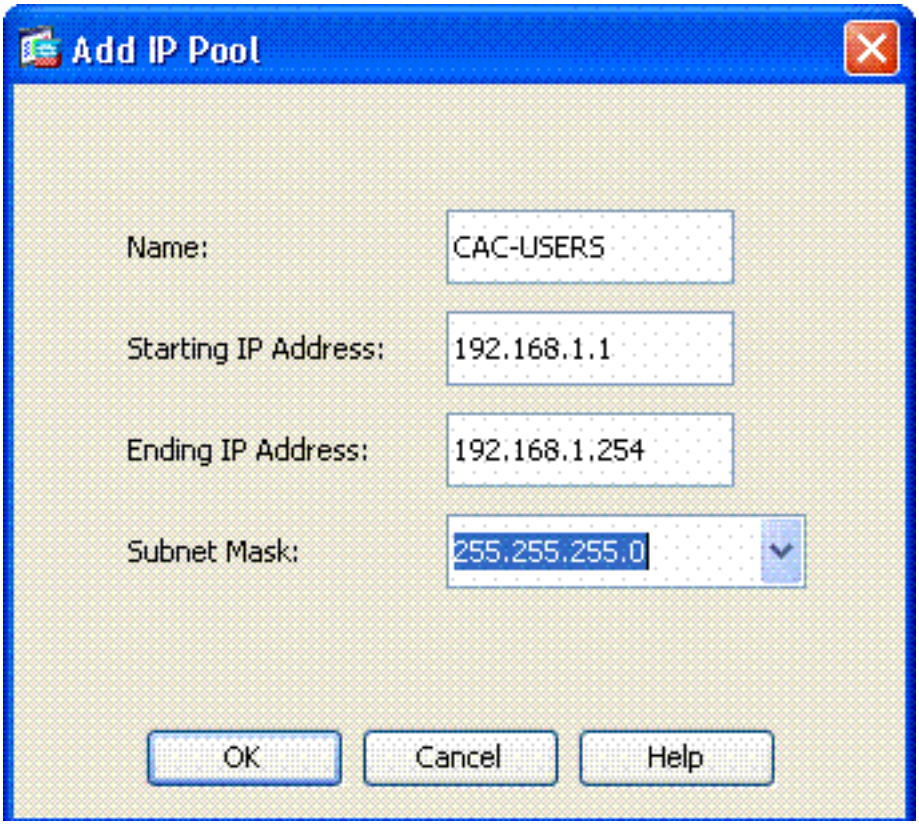
1. Èpossibile scaricare il client dal sito Web di Cisco e installarlo sul suo computer.
2. L'utente può accedere all'ASA tramite un browser Web e il client può essere scaricato.

Nota: Ad esempio, https://asa.test.com. In questa guida viene utilizzato il secondo metodo. Una volta installato il client AC sul computer client in modo permanente, è sufficiente avviare il client AC dall'applicazione.

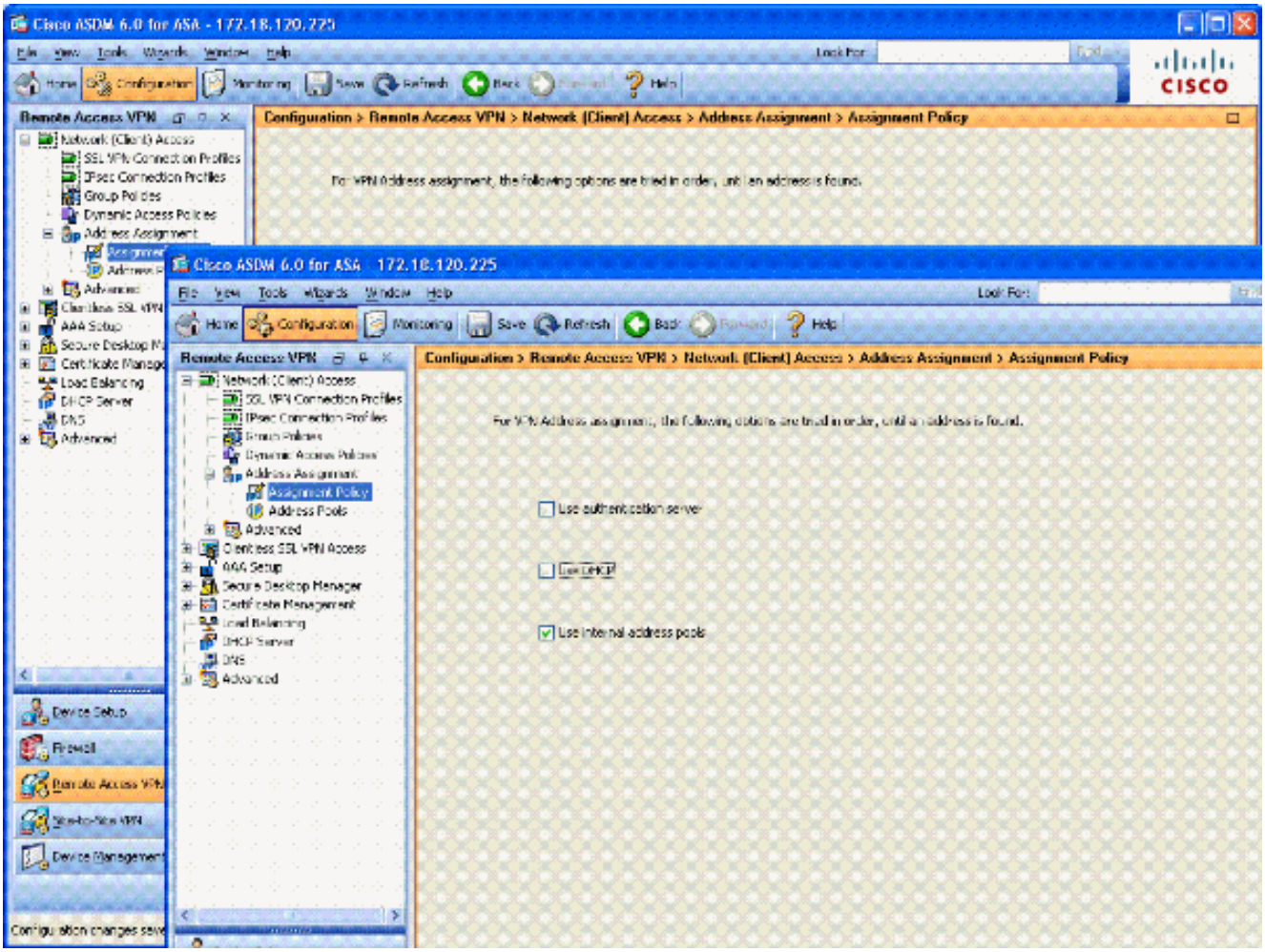
Crea pool di indirizzi IP

Questa operazione è facoltativa se si utilizza un altro metodo, ad esempio DHCP.

1. Scegliere **VPN ad accesso remoto > Accesso di rete (client) > Assegnazione indirizzi > Pool di indirizzi**.
2. Fare clic su **Add**.
3. Nella finestra Aggiungi pool IP, immettere il nome del pool IP, l'indirizzo IP iniziale e finale e scegliere una subnet mask. Vedere la Figura 13.**Figura 13: Aggiunta del pool IP**



4. Scegliere **OK**.
5. Scegliere **VPN ad accesso remoto > Accesso di rete (client) > Assegnazione indirizzi > Criteri di assegnazione**.
6. Selezionare il metodo di assegnazione dell'indirizzo IP appropriato. In questa guida vengono utilizzati i pool di indirizzi interni. Vedere la Figura 14.**Figura 14: Metodo di assegnazione dell'indirizzo IP**



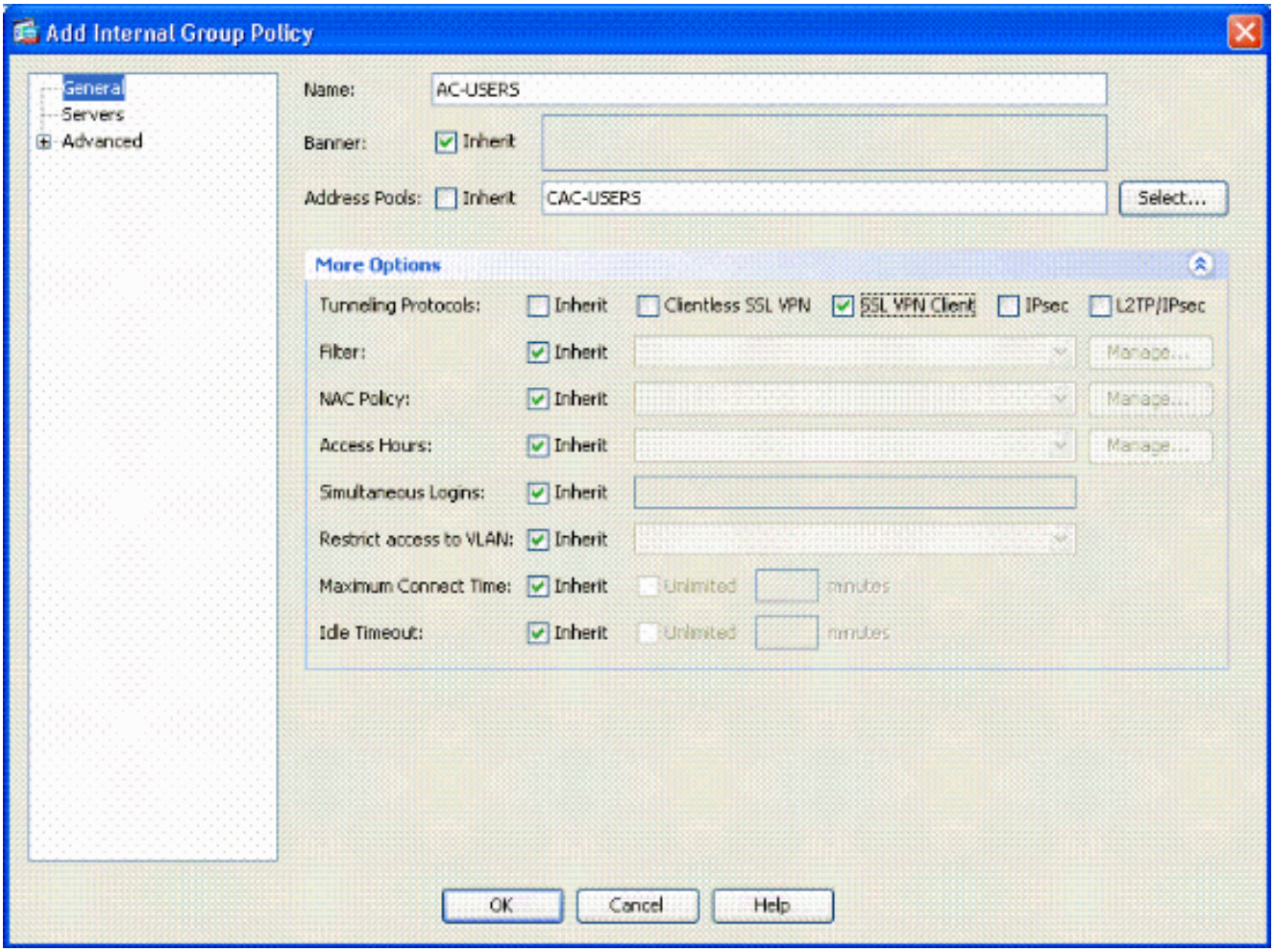
7. Fare clic su **Apply** (Applica).

Crea gruppo tunnel e Criteri di gruppo

Criteri di gruppo

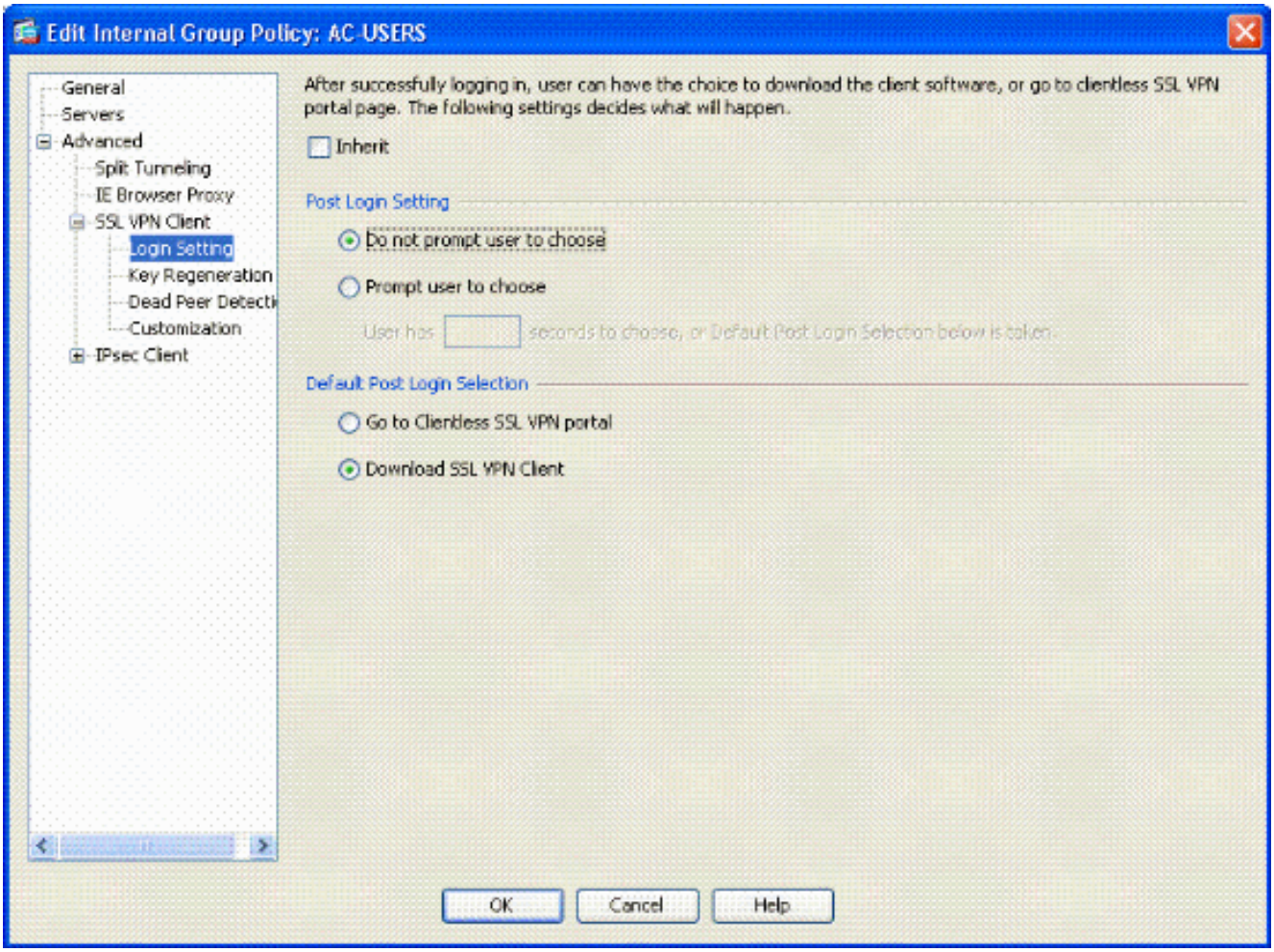
Nota: se non si desidera creare un nuovo criterio, è possibile utilizzare il criterio di gruppo predefinito.

1. Scegliere **VPN ad accesso remoto -> Accesso di rete (client) -> Criteri di gruppo**.
2. Fare clic su **Aggiungi** e scegliere **Criteri di gruppo interni**.
3. Nella finestra Aggiungi Criteri di gruppo interni immettere il nome dei Criteri di gruppo nella casella di testo Nome. Vedere la Figura 15.**Figura 15: Aggiunta di Criteri di gruppo interni**



Nella scheda Generale scegliere l'opzione **SSL VPN Client in Protocolli di tunneling**, a meno che non si utilizzino altri protocolli, ad esempio SSL senza client.Nella sezione Server deselezionare la casella di controllo **eredita** e immettere l'indirizzo IP dei server DNS e WINS. Immettere l'ambito DHCP, se applicabile.Nella sezione Server deselezionare la casella di controllo **inherit** nel dominio predefinito e immettere il nome di dominio appropriato.Nella scheda Generale deselezionare la casella di controllo **eredita** nella sezione pool di indirizzi e aggiungere il pool di indirizzi creato nel passaggio precedente. Se si utilizza un altro metodo di assegnazione degli indirizzi IP, lasciare che erediti e apportare le modifiche appropriate.Tutte le altre schede di configurazione vengono lasciate alle impostazioni predefinite.**Nota:** esistono due metodi per ottenere il client AC per gli utenti finali. Uno dei metodi consiste nell'andare all'indirizzo Cisco.com e scaricare il client AC. Il secondo metodo consiste nel fare in modo che l'appliance ASA scarichi il client quando l'utente tenta di connettersi. In questo esempio viene illustrato il secondo metodo.

4. Quindi, scegliere **Avanzate > SSL VPN Client > Impostazioni di accesso**. Vedere la Figura 16.**Figura 16: Aggiunta di Criteri di gruppo interni**

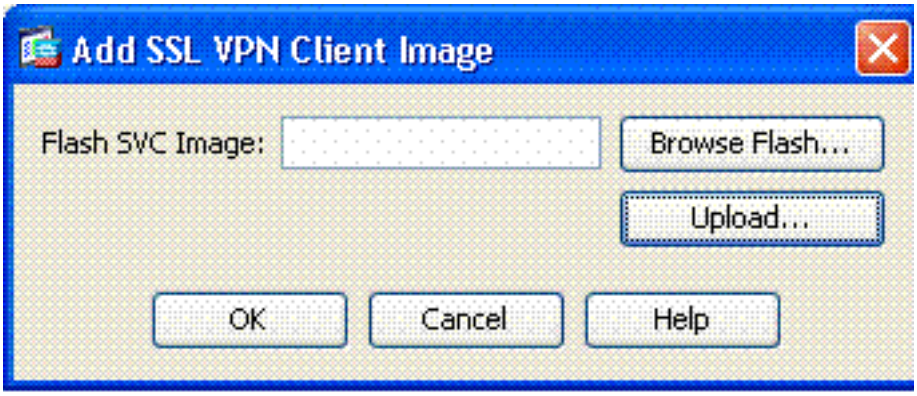


Deselezionare la casella di controllo **Eredita**.Scegliere l'impostazione post-login appropriata per l'ambiente in uso.Scegliere la selezione post-login predefinita appropriata per l'ambiente in uso.Scegliere **OK**.

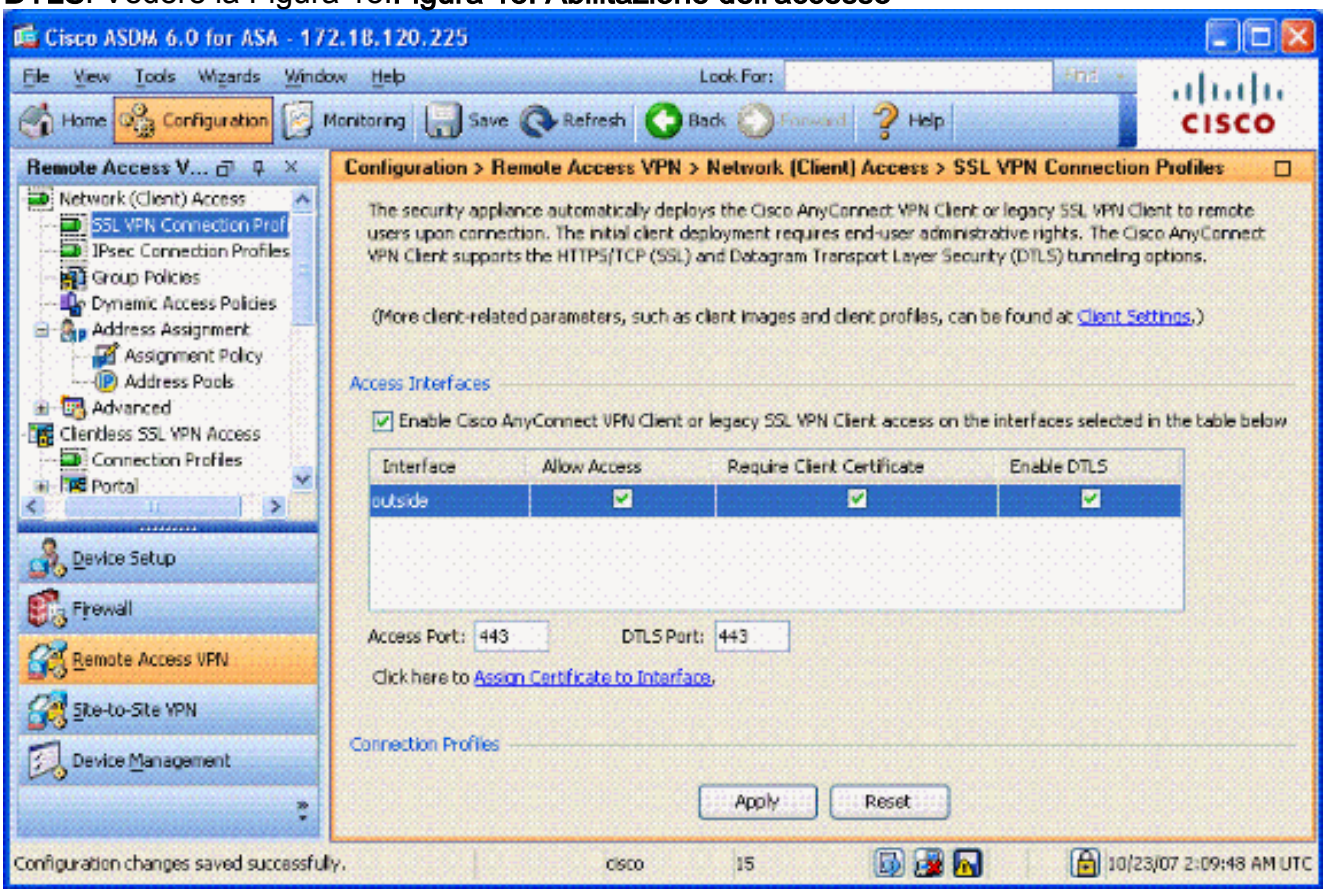
Impostazioni interfaccia e immagine tunnel Group

Nota: se non si desidera creare un nuovo gruppo, è possibile utilizzare il gruppo predefinito.

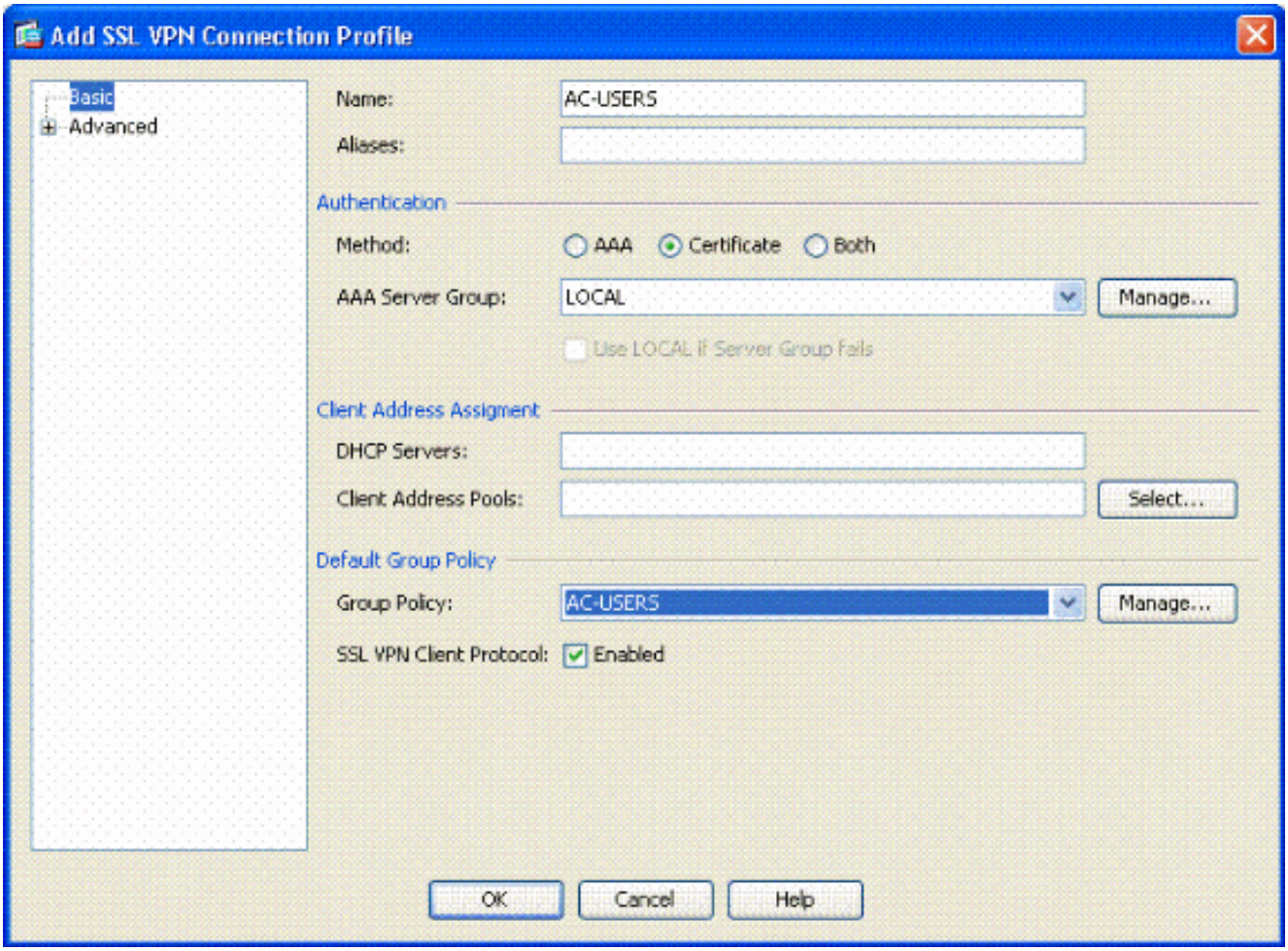
1. Scegliere **VPN ad accesso remoto > Accesso di rete (client) > Profilo connessione VPN SSL**.
2. Scegliere **Abilita client Cisco AnyConnect.....**.
3. Viene visualizzata una finestra di dialogo con la domanda `Designare un'immagine SVC?`
4. Scegliere **Sì**.
5. Se è già presente un'immagine, scegliete l'immagine da utilizzare con Browse Flash. Se l'immagine non è disponibile, scegliere **Upload** e cercare il file nel computer locale. Vedere la Figura 17. I file possono essere scaricati da Cisco.com; esiste un file Windows, MAC e Linux.**Figura 17: Aggiungi immagine client VPN SSL**



6. Quindi abilitare **Consenti accesso**, **Richiedi certificato client** e facoltativamente **Abilitare DTLS**. Vedere la Figura 18.**Figura 18: Abilitazione dell'accesso**

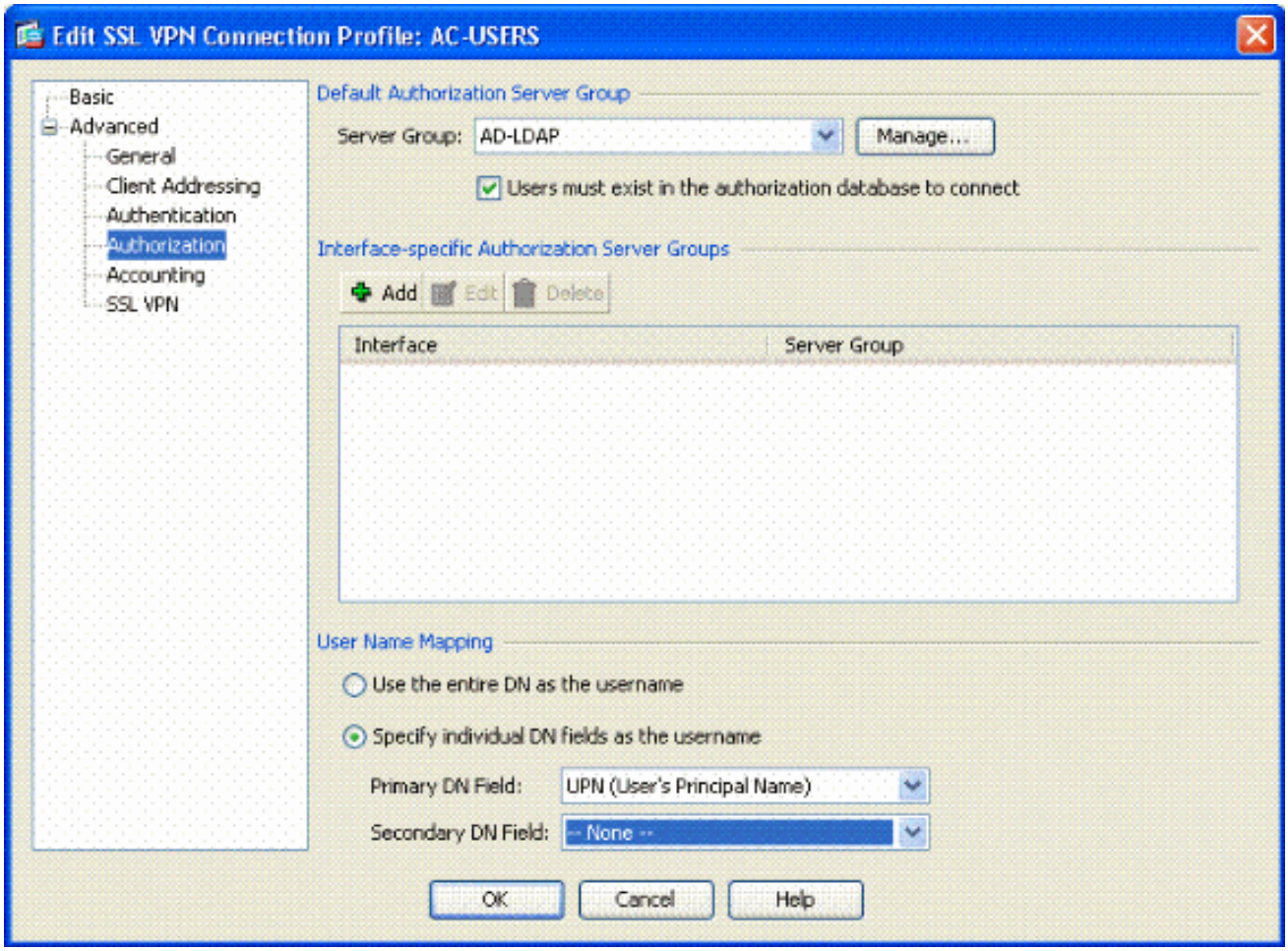


7. Fare clic su **Apply** (Applica).
8. Creare quindi un profilo di connessione/gruppo di tunnel. Scegliere **VPN ad accesso remoto > Accesso di rete (client) > Profilo connessione VPN SSL**.
9. Nella sezione Profili di connessione fare clic su **Aggiungi**.**Figura 19: Aggiunta del profilo di connessione**



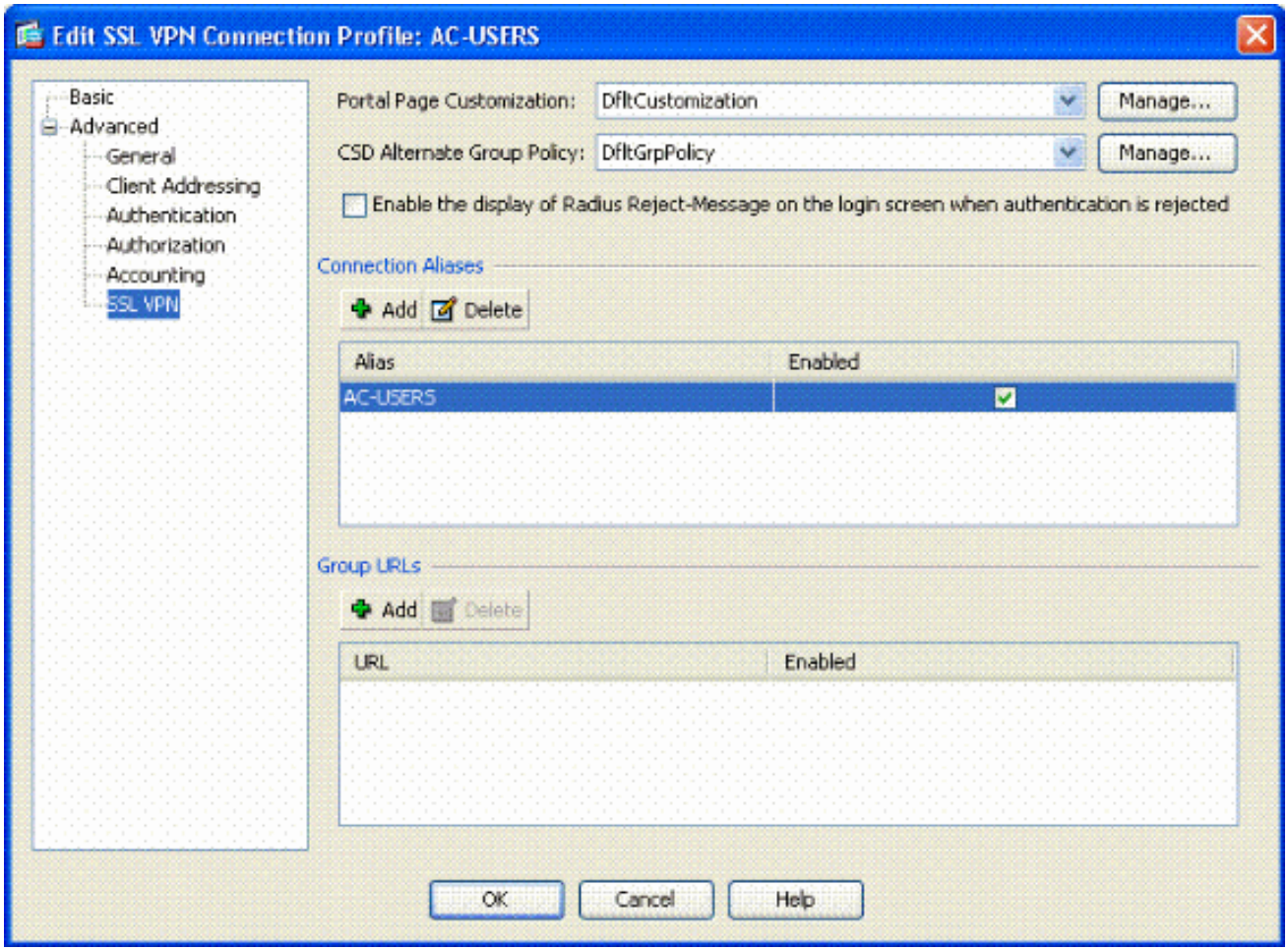
Assegnare un nome al gruppo.Scegliere **Certificato** nel metodo di autenticazione.Scegliere i Criteri di gruppo creati in precedenza.Verificare che il **client VPN SSL** sia abilitato.Accettate le altre opzioni come predefinite.

10. Quindi, **scegliere Avanzate > Autorizzazione**. Vedere la Figura 20**Figura 20: Authorization**



Scegliere il gruppo AD-LDAP creato in precedenza.Selezionare **Gli utenti devono esistere... per connettersi.**Nei campi di mapping, scegliere **UPN** per il database primario e **none** per il database secondario.

11. Scegliere la sezione **SSL VPN** del menu.
12. Nella sezione Alias di connessione eseguire la procedura seguente:**Figura 21: Alias di connessione**



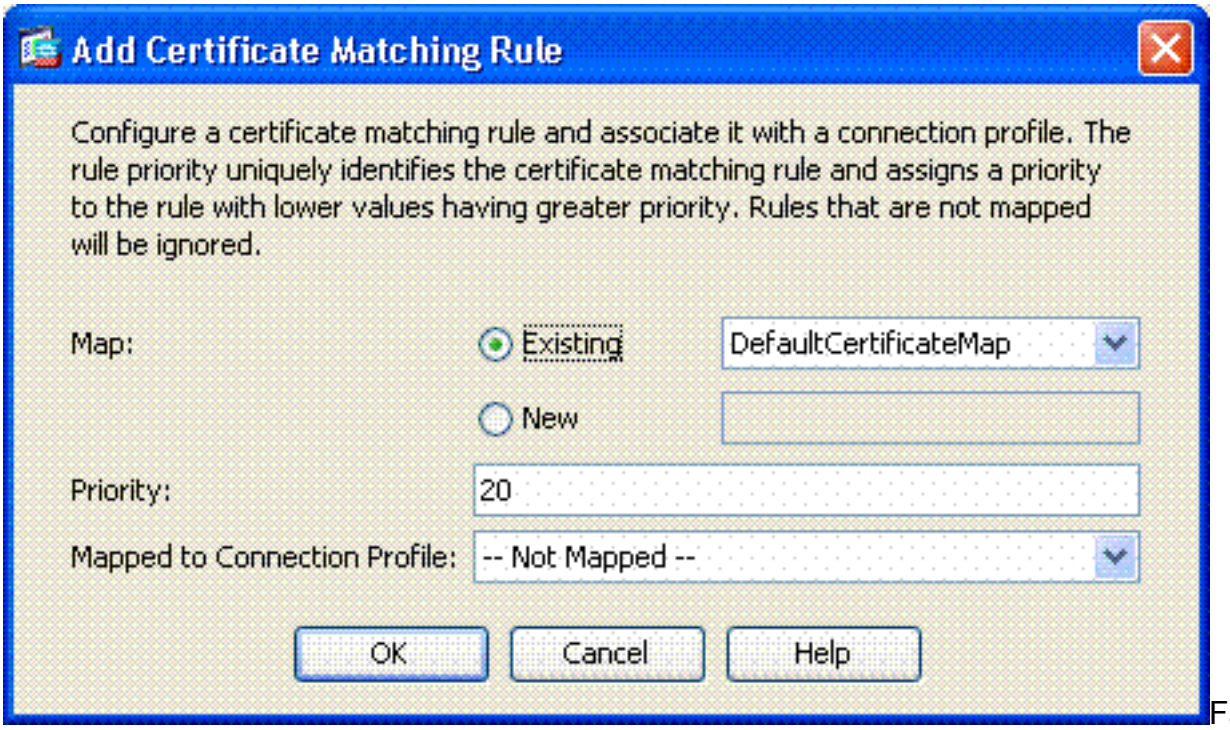
Scegliere **Aggiungi**.Immettere l'alias del gruppo che si desidera utilizzare.Verificare che l'opzione **Enabled** sia selezionata. Vedere la Figura 21.

13. Fare clic su **OK**.

Nota: per salvare la configurazione nella memoria flash, fare clic su **Save** (Salva).

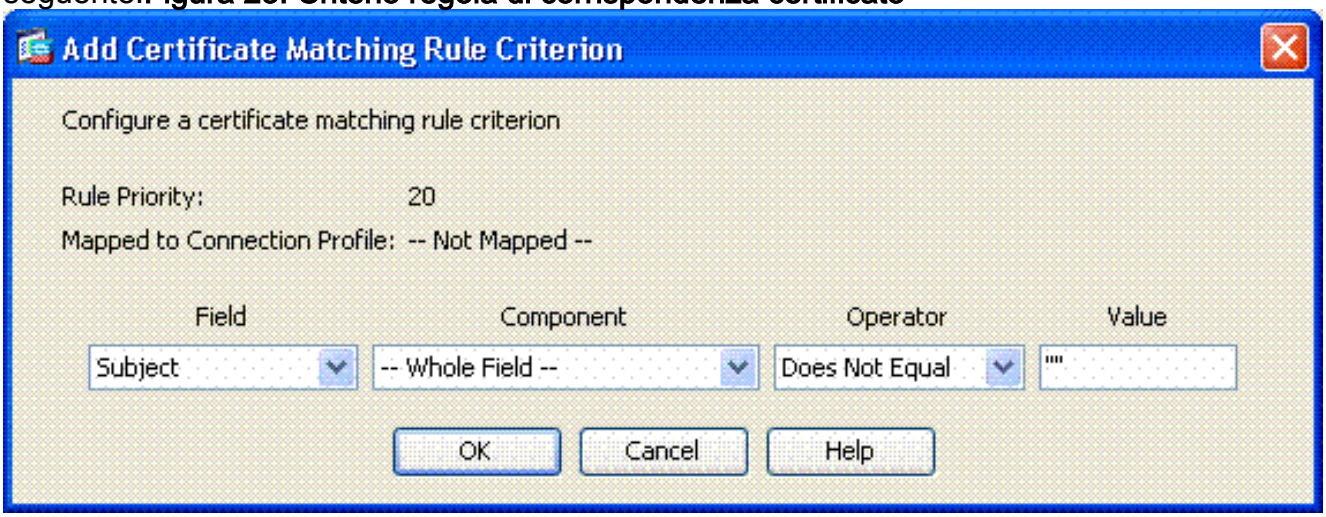
Regole di corrispondenza certificato (se verrà utilizzato OCSP)

1. Scegliere **VPN ad accesso remoto > Avanzate > Mappe profilo connessione VPN da certificato a SSL**. Vedere la Figura 22.Scegliere **Aggiungi** nella sezione Mappe profilo certificato-connessione.Èpossibile mantenere la mappa esistente come DefaultCertificateMap nella sezione della mappa oppure crearne una nuova se si utilizzano già le mappe certificati per IPSec.Mantenere la priorità della regola.In Gruppo mappato lasciare come **— Non mappato —**. Vedere la Figura 22.**Figura 22: Aggiunta della regola di corrispondenza certificato**



Fare clic su **OK**.

2. Fare clic su **Add** nella tabella inferiore.
3. Nella finestra Aggiungi criterio regola di corrispondenza certificato eseguire la procedura seguente:**Figura 23: Criterio regola di corrispondenza certificato**



Mantenere la colonna Campo su **Oggetto**.Mantenere la colonna Componente su **Campo intero**.Modificare la colonna Operatore in **Diverso da**.Nella colonna Valore immettere due virgolette doppie **""**.Fare clic su **Ok** e su **Applica**. Vedere la Figura 23 per esempio.

Configura OCSP

La configurazione di un OCSP può variare e dipende dal fornitore del risponditore OCSP. Per ulteriori informazioni, leggere il manuale del fornitore.

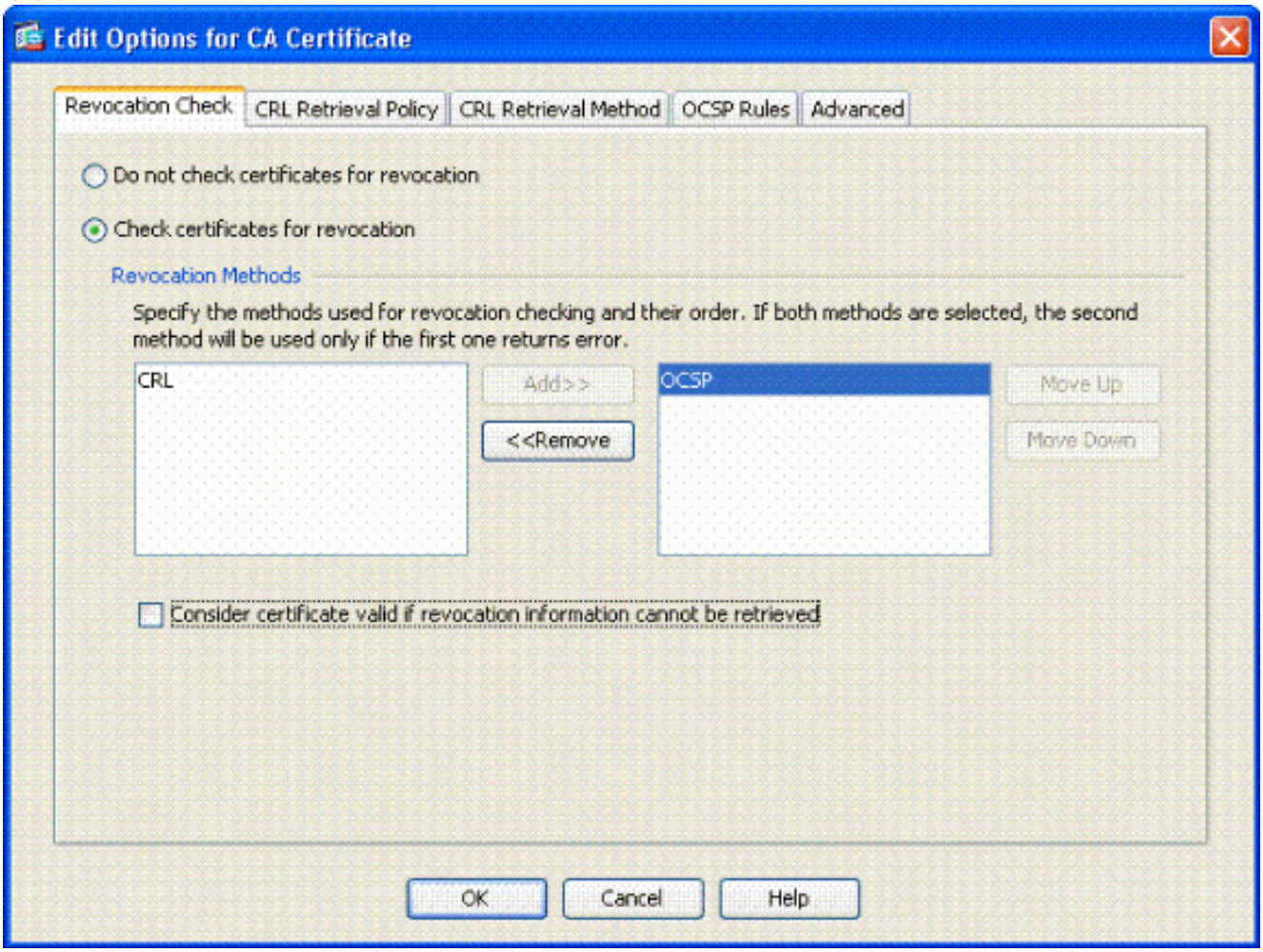
Configura certificato risponditore OCSP

1. Ottenere un certificato generato automaticamente dal risponditore OCSP.
2. Completare le procedure descritte in precedenza e installare un certificato per il server OSCP.**Nota:** verificare che l'opzione **Non controllare certificati per la revoca** sia selezionata

per il trust certificati OCSP.

Configura CA per l'utilizzo di OCSP

1. Scegliere **VPN Accesso remoto> Gestione certificati > Certificati CA**.
2. Evidenziare un OCSP per scegliere una CA da configurare per l'utilizzo di OCSP.
3. Fare clic su **Modifica**.
4. Verificare che **Controllo certificato per revoca** sia selezionato.
5. Nella sezione Metodi di revoca aggiungere **OCSP**. Vedere la Figura 24.**Controllo revoca OCSP**



6. Assicurarsi che l'opzione **Considera certificato valido...non recuperabile** sia deselezionata se si desidera eseguire una rigorosa verifica OCSP.

Nota: configurare/modificare tutti i server CA che utilizzano OCSP per la revoca.

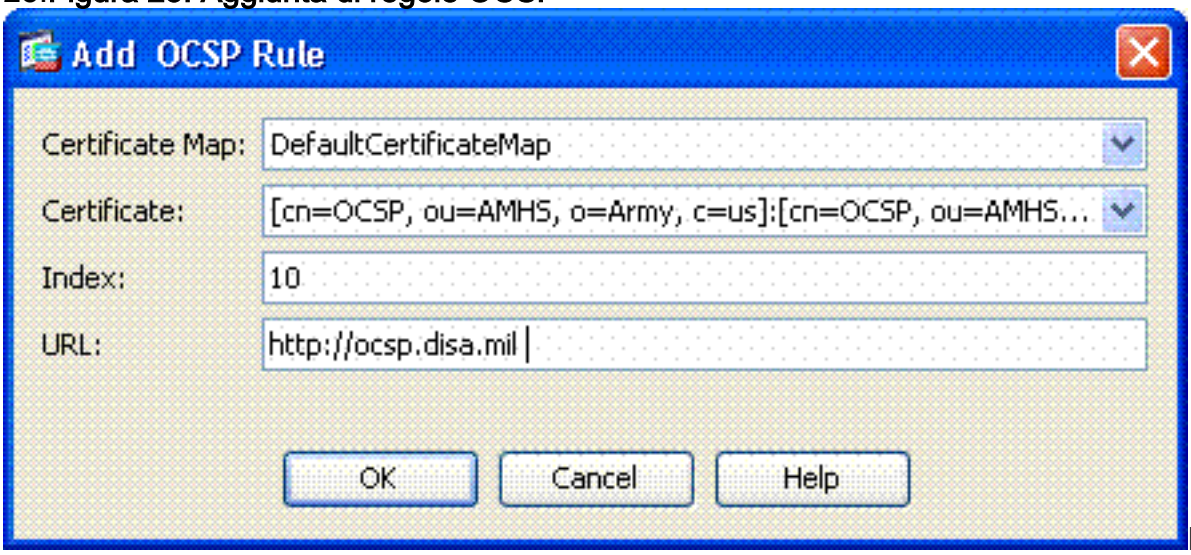
Configura regole OCSP

Nota: prima di completare questa procedura, verificare che sia stato creato un criterio di corrispondenza del gruppo di certificati e che il risponditore OCSP sia configurato.

Nota: In alcune implementazioni OCSP può essere necessario un record A e PTR DNS per l'ASA. Questo controllo viene eseguito per verificare che l'appliance ASA provenga da un sito .mil.

1. Scegliere **VPN Accesso remoto> Gestione certificati > Certificati CA 2**.
2. Evidenziare un OCSP per scegliere una CA da configurare per l'utilizzo di OCSP.
3. Scegliere **Modifica**.

4. Fare clic sulla scheda **Regola OCSP**.
5. Fare clic su **Add.**
6. Nella finestra Aggiungi regola OCSP effettuare le seguenti operazioni. Vedere la Figura 25.**Figura 25: Aggiunta di regole OCSP**



Nell'opzione Mappa certificati scegliere **DefaultCertificateMap** oppure una mappa creata in precedenza.Nell'opzione Certificato scegliere **Risponditore OCSP**.Nell'opzione Indice, immettere **10**.Nell'opzione URL, immettere l'indirizzo IP o il nome host del risponditore OCSP. Se si utilizza il nome host, verificare che il server DNS sia configurato sull'appliance ASA.Fare clic su **OK**.Fare clic su **Apply** (Applica).

Configurazione client Cisco AnyConnect

In questa sezione viene descritta la configurazione del client VPN Cisco AnyConnect.

Presupposti: Cisco AnyConnect VPN Client e l'applicazione middleware sono già installati nel PC host. ActivCard Gold e ActivClient sono stati testati.

Nota: questa guida utilizza il metodo group-url solo per l'installazione iniziale del client CA. Una volta installato il client AC, l'applicazione AC viene avviata come il client IPsec.

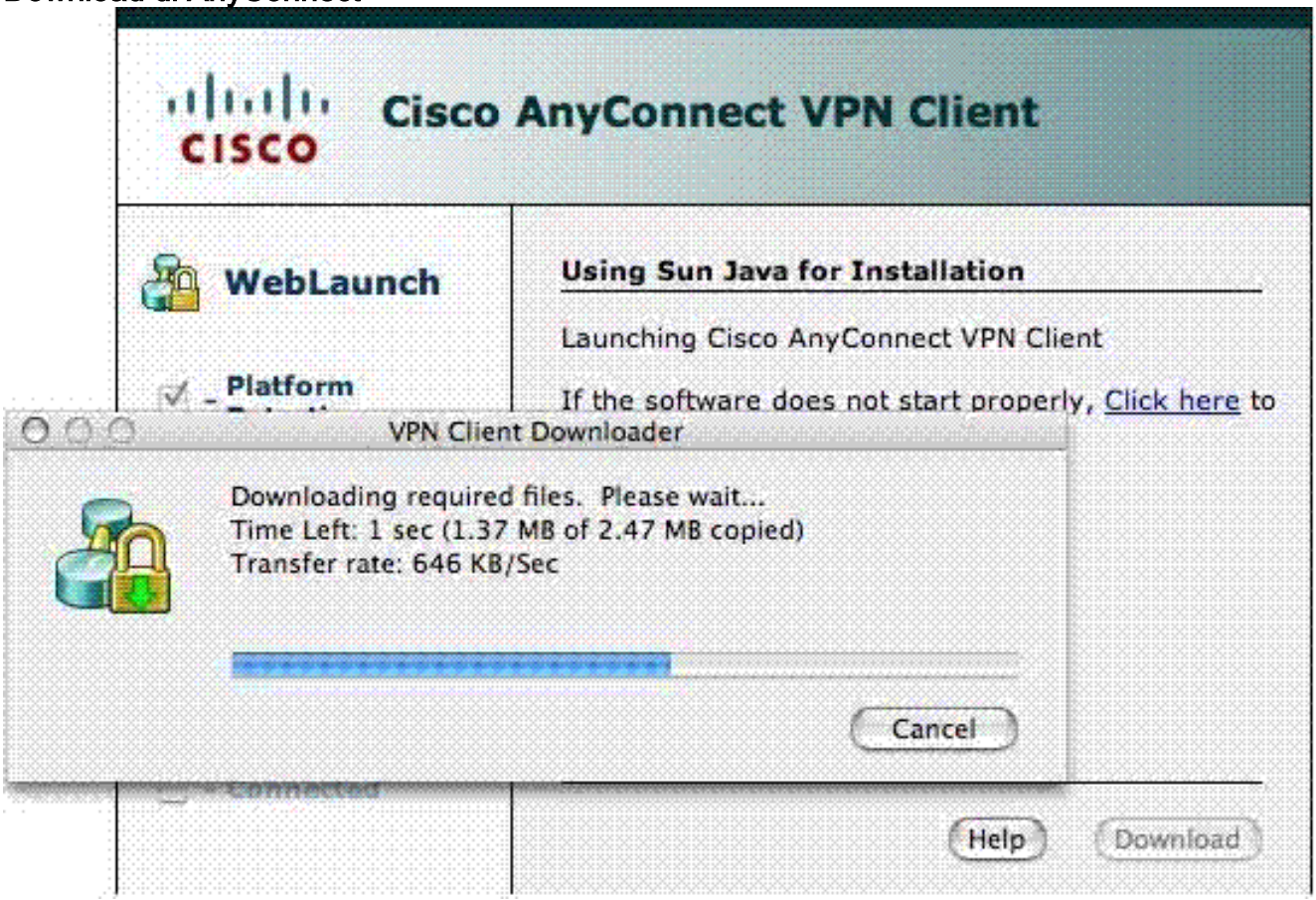
Nota: è necessario installare la catena di certificati DoD nel computer locale. Verificare con il POC PKI per ottenere i certificati/file batch.

Nota: il driver del lettore di schede per MAC OSX è già installato e compatibile con la versione corrente del sistema operativo in uso.

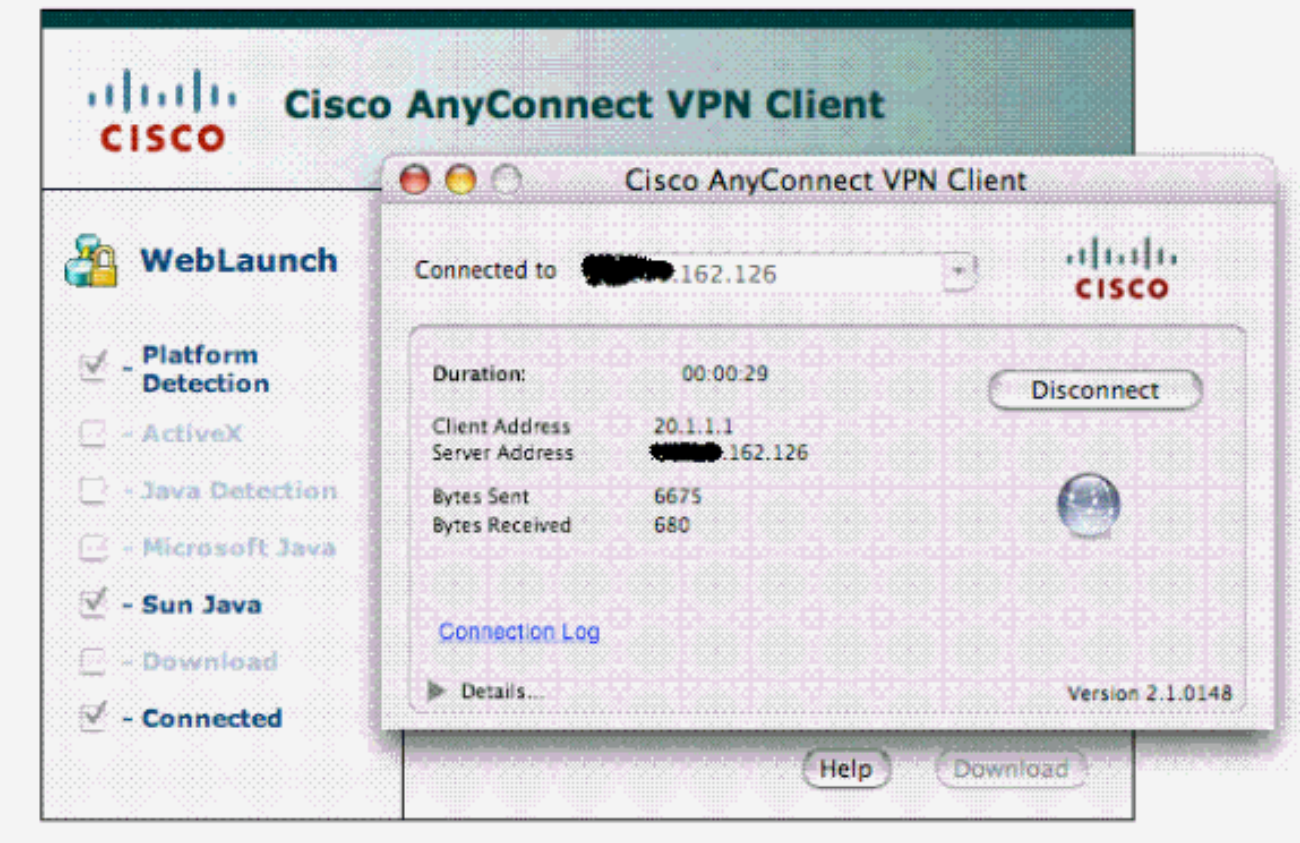
Download del client VPN Cisco Anyconnect - Mac OS X

1. Avviare una sessione Web sull'appliance ASA tramite Safari. L'indirizzo deve essere nel formato https://Outside-Interface. Ad esempio, https://172.18.120.225.
2. Una finestra pop-up chiede di verificare il certificato dell'ASA. Fare clic su **Continue** (Continua).
3. Viene visualizzata un'altra finestra popup per sbloccare il portachiavi CAC. Immettere il numero di pin. Vedere la Figura 31.**Figura 31: Immettere il PIN**

4. Dopo la visualizzazione della pagina Web SSL VPN-service, fare clic su **Continue** (Continua).
5. Dopo aver sbloccato il portachiavi, il browser chiede se si considera attendibile il certificato emesso dall'appliance ASA. Fare clic su **trust**.
6. Immettere la password di root per sbloccare il portachiavi per stabilire una connessione sicura, quindi fare clic su **OK**.
7. Scegliere il certificato da utilizzare per l'autenticazione client e quindi fare clic su **OK**.
8. Il browser chiede quindi la password root/user per consentire il download dei client AnyConnect.
9. Se il client AnyConnect è autenticato, inizia il download. Vedere la Figura 32.**Figura 32: Download di AnyConnect**



10. Dopo aver scaricato l'applicazione, il browser chiede di accettare il certificato ASA. Fare clic su **Accetta**.
11. Connessione stabilita. Figura 33.**Figura 33:AnyConnect Connected**



Avvio di Cisco AnyConnect VPN Client - Mac OS X

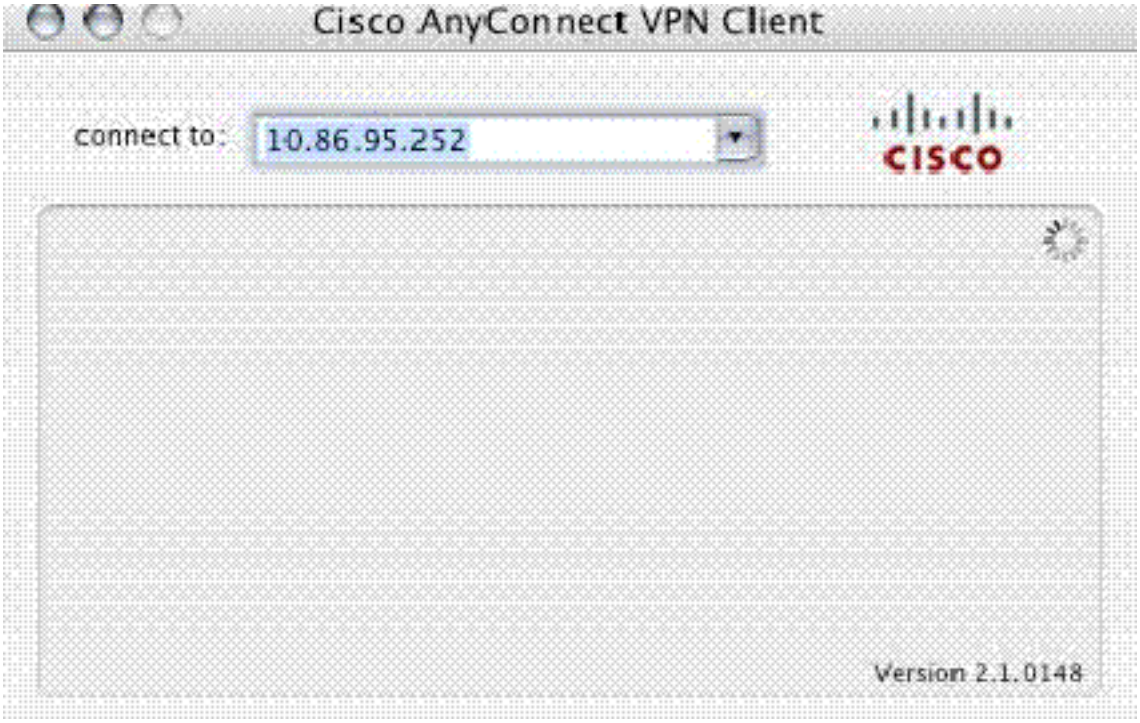
Da Finder—**Applicazioni > Cisco AnyConnect VPN Client**

Nota: vedere l'Appendice E per la configurazione opzionale del profilo del client AnyConnect.

Nuova connessione

Viene visualizzata la finestra AC. Vedere la Figura 37.

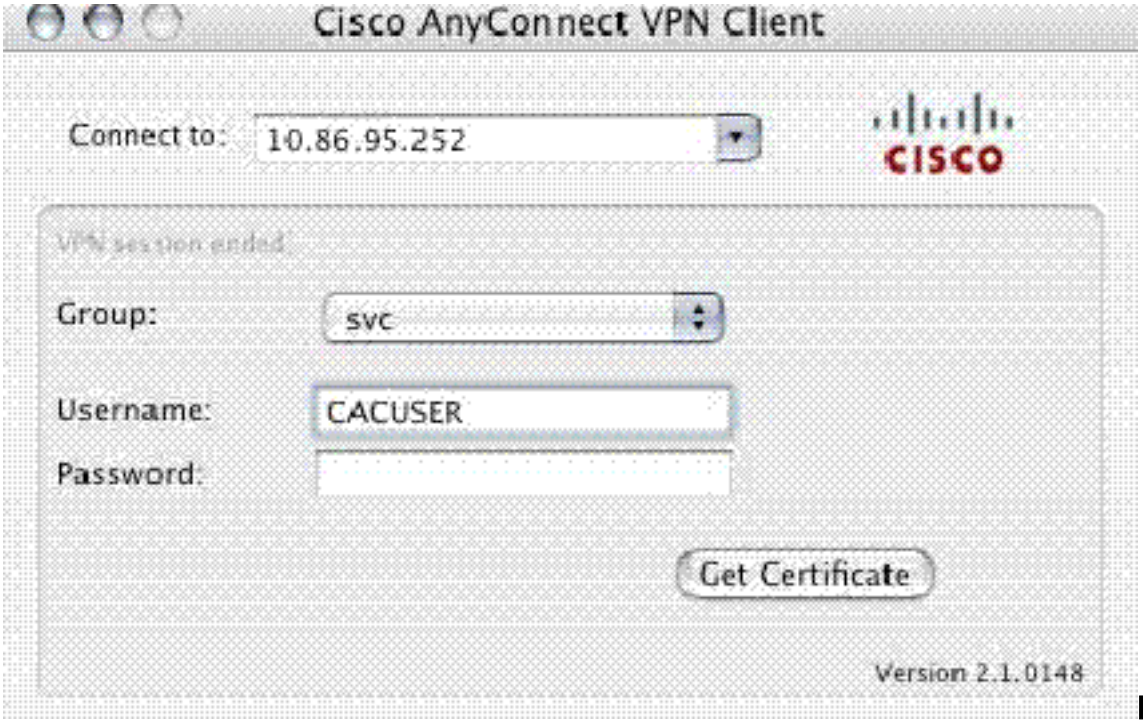
Figura 37: Nuova connessione VPN



1. Scegliere l'host appropriato se l'applicazione non tenta automaticamente la connessione.
2. Quando richiesto, immettere il PIN. Vedere la Figura 38.**Figura 38: Immettere il PIN**

Avvia accesso remoto

1. Scegliere il gruppo e l'host a cui connettersi.
2. Poiché vengono utilizzati i certificati, scegliere **Connetti** per stabilire la VPN. Vedere la Figura 39.**Nota:** poiché la connessione utilizza certificati, non è necessario immettere un nome utente e una password.**Figura 39: Connessione**



Nota: vedere l'Appendice E per la configurazione opzionale del profilo del client AnyConnect.

Appendice A - Mappatura LDAP e DAP

In ASA/PIX versione 7.1(x) e successive, è stata introdotta una funzione chiamata mappatura LDAP. Si tratta di una potente funzione che fornisce un mapping tra un attributo Cisco e oggetti/attributi LDAP, che elimina la necessità di modificare lo schema LDAP. Per l'implementazione dell'autenticazione CAC, è possibile supportare l'applicazione di ulteriori criteri sulla connessione di accesso remoto. Questi sono esempi di mapping LDAP. Per apportare modifiche nel server AD/LDAP sono necessari diritti di amministratore. Nel software ASA 8.x è stata introdotta la funzionalità DAP (Dynamic Access Policy). DAP può lavorare in combinazione con CAC per esaminare più gruppi AD, nonché i criteri push, gli ACL e così via.

Scenario 1: Imposizione di Active Directory tramite l'autorizzazione Accesso remoto Accesso remoto - Consenti/Nega accesso

In questo esempio viene eseguito il mapping dell'attributo di Active Directory msNPAllowDailin all'attributo di Cisco cVPN3000-Tunneling-Protocol.

- Il valore dell'attributo di Active Directory: TRUE = Consenti; FALSO = Nega
- Valore attributo Cisco: 1 = FALSE, 4 (IPSec) o 20 (4 IPSEC + 16 WebVPN) = TRUE,

Per la condizione ALLOW è possibile mappare:

- VERO = 20

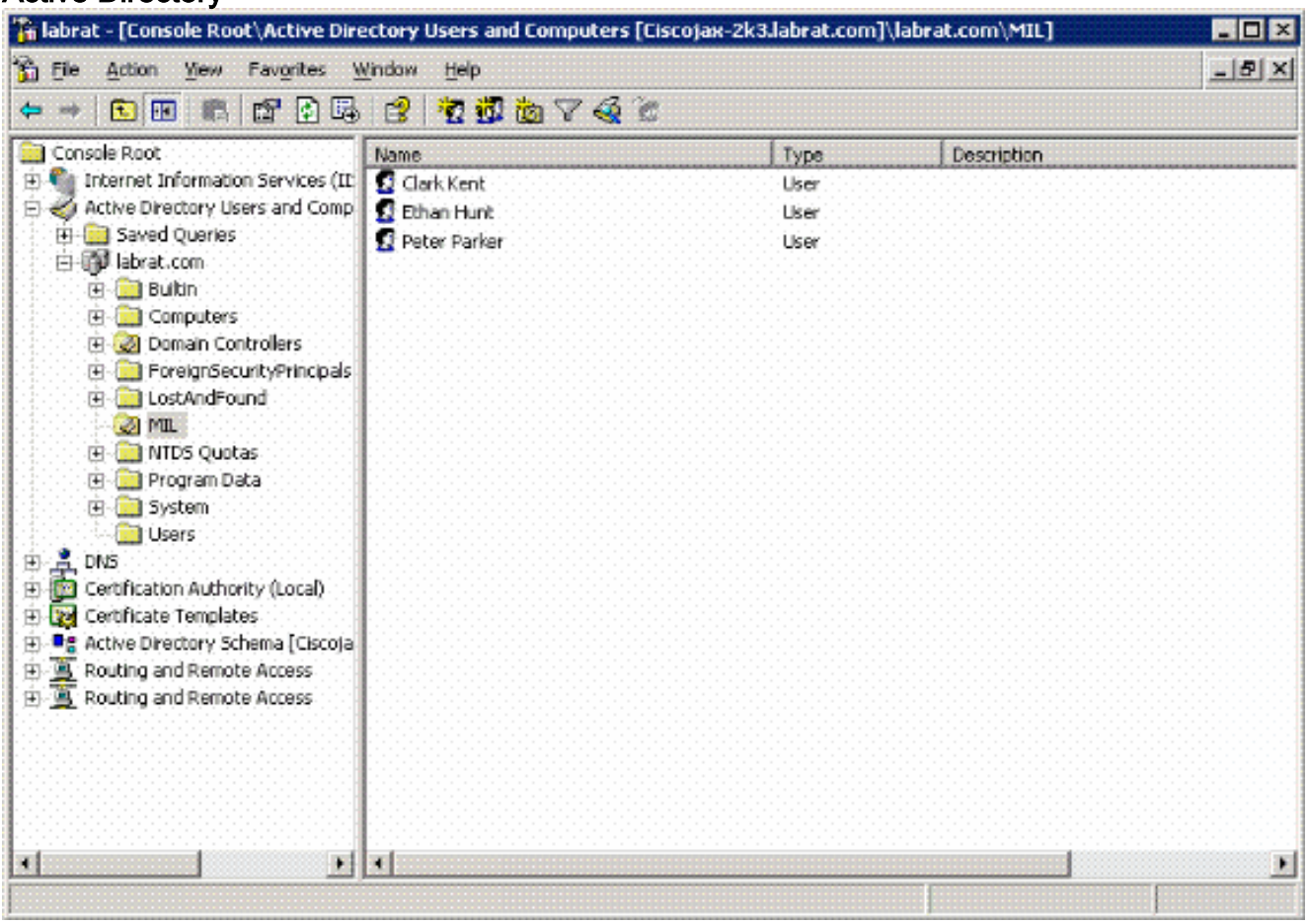
Per la condizione di connessione negata, è possibile mappare:

- FALSO = 1

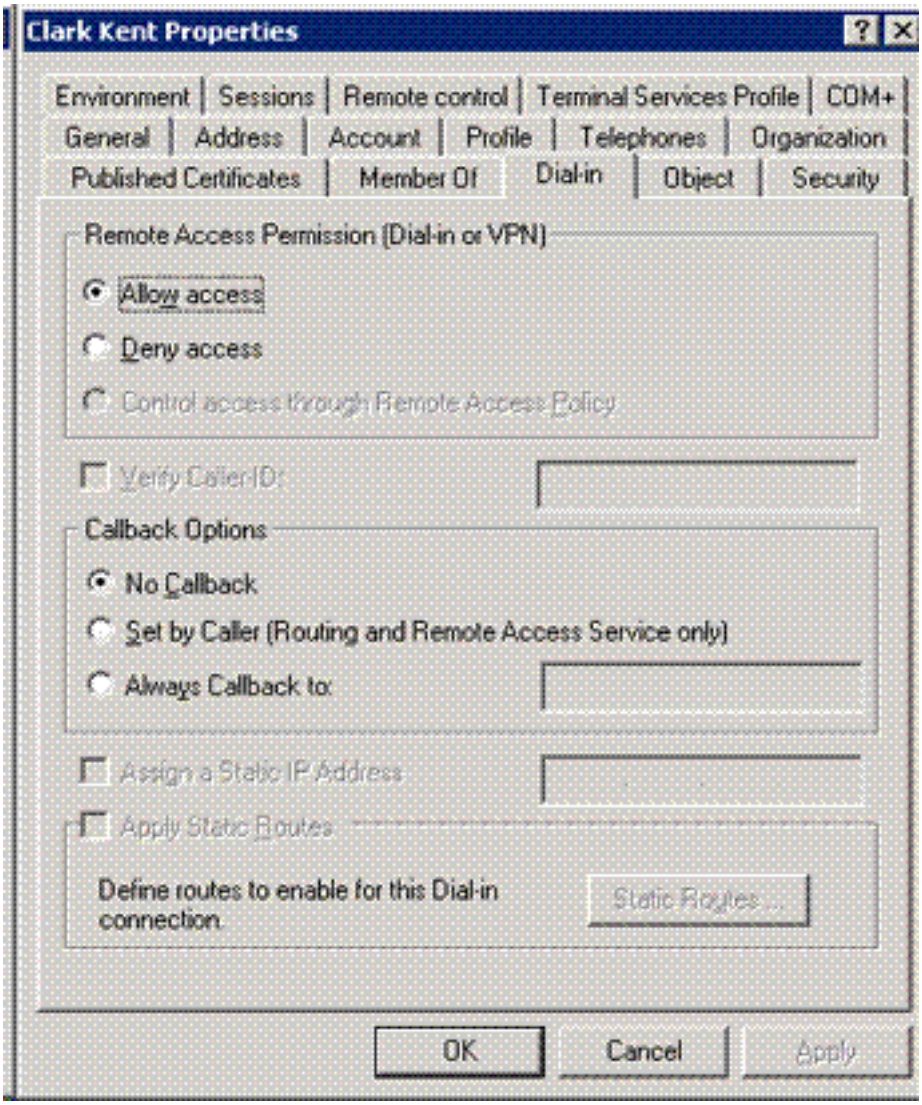
Nota: assicurarsi che VERO e FALSO siano in maiuscolo. per ulteriori informazioni, fare riferimento a Configurazione di un server esterno per l'autorizzazione utente di Security Appliance.

Installazione di Active Directory

1. Nel server Active Directory fare clic su **Start > Esegui**.
2. Nella casella di testo Apri digitare **dsa.msc** quindi fare clic su **OK**. Verrà avviata la console di gestione di Active Directory.
3. Nella console di gestione di Active Directory fare clic sul segno più per espandere Utenti e computer di Active Directory.
4. Fare clic sul segno più per espandere il nome del dominio.
5. Se è stata creata un'unità organizzativa per gli utenti, espandere l'unità organizzativa per visualizzare tutti gli utenti. se nella cartella Utenti sono stati assegnati tutti gli utenti, espandere tale cartella per visualizzarli. Vedere la Figura A1.**Figura A1: Console di gestione Active Directory**



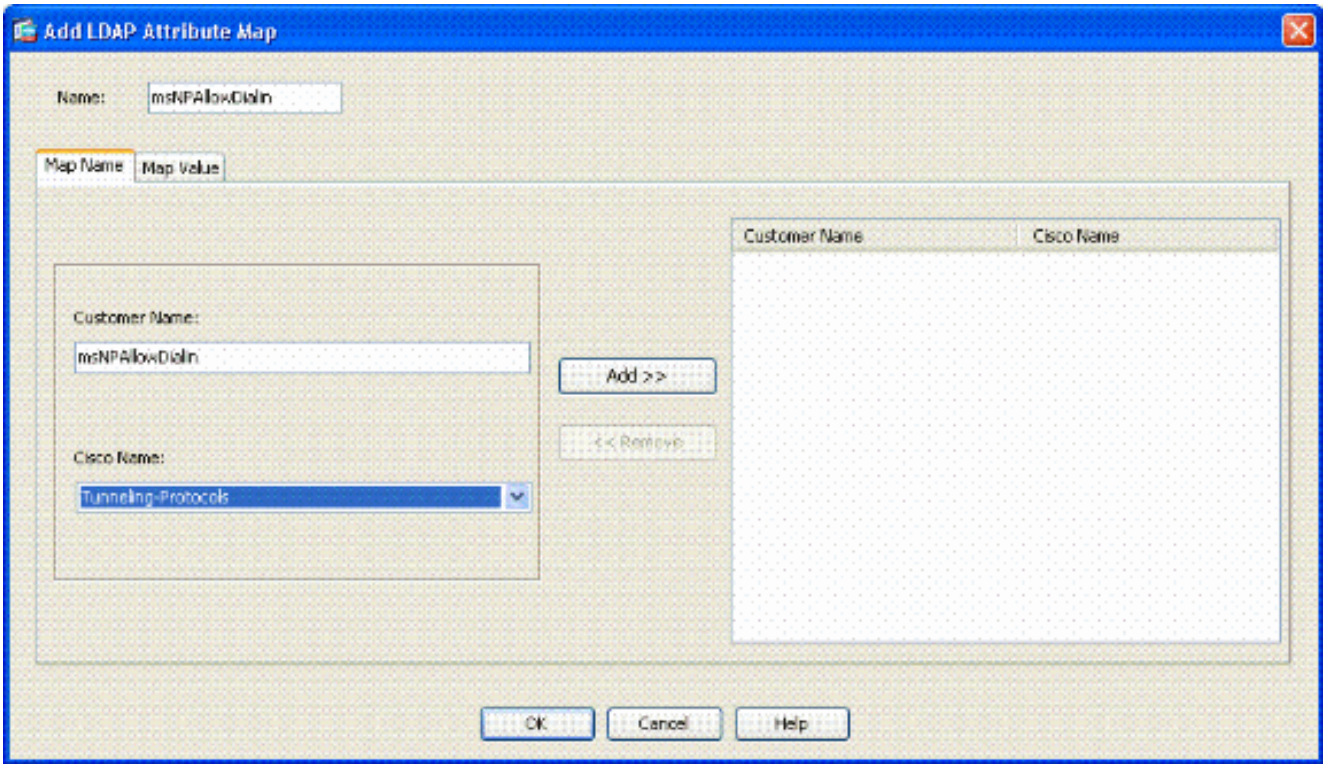
6. Fare doppio clic sull'utente che si desidera modificare.Fare clic sulla scheda Chiamate in ingresso nella pagina delle proprietà dell'utente e fare clic su **Consenti** o **Nega**. Vedere la Figura A2.**Figura A2: Proprietà utente**



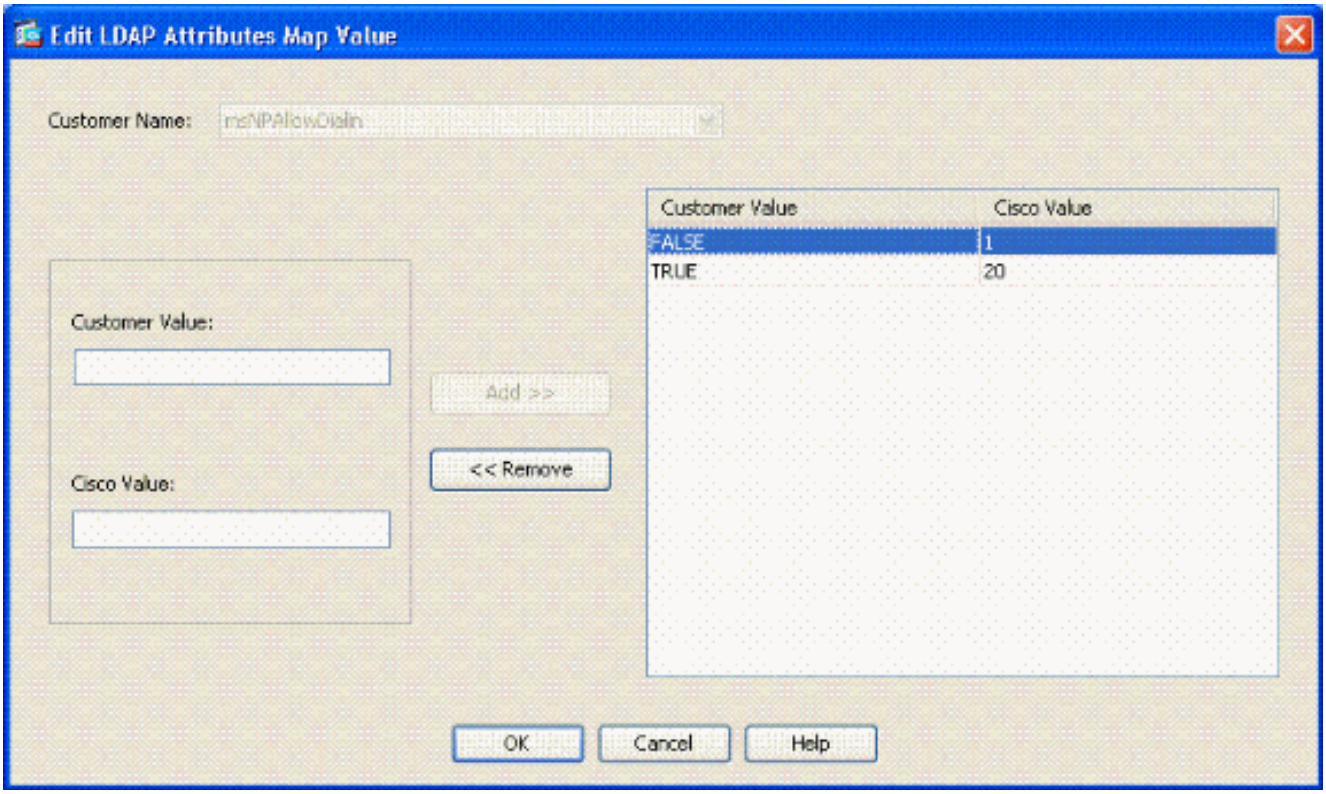
7. Quindi fare clic su **Ok**.

Configurazione ASA

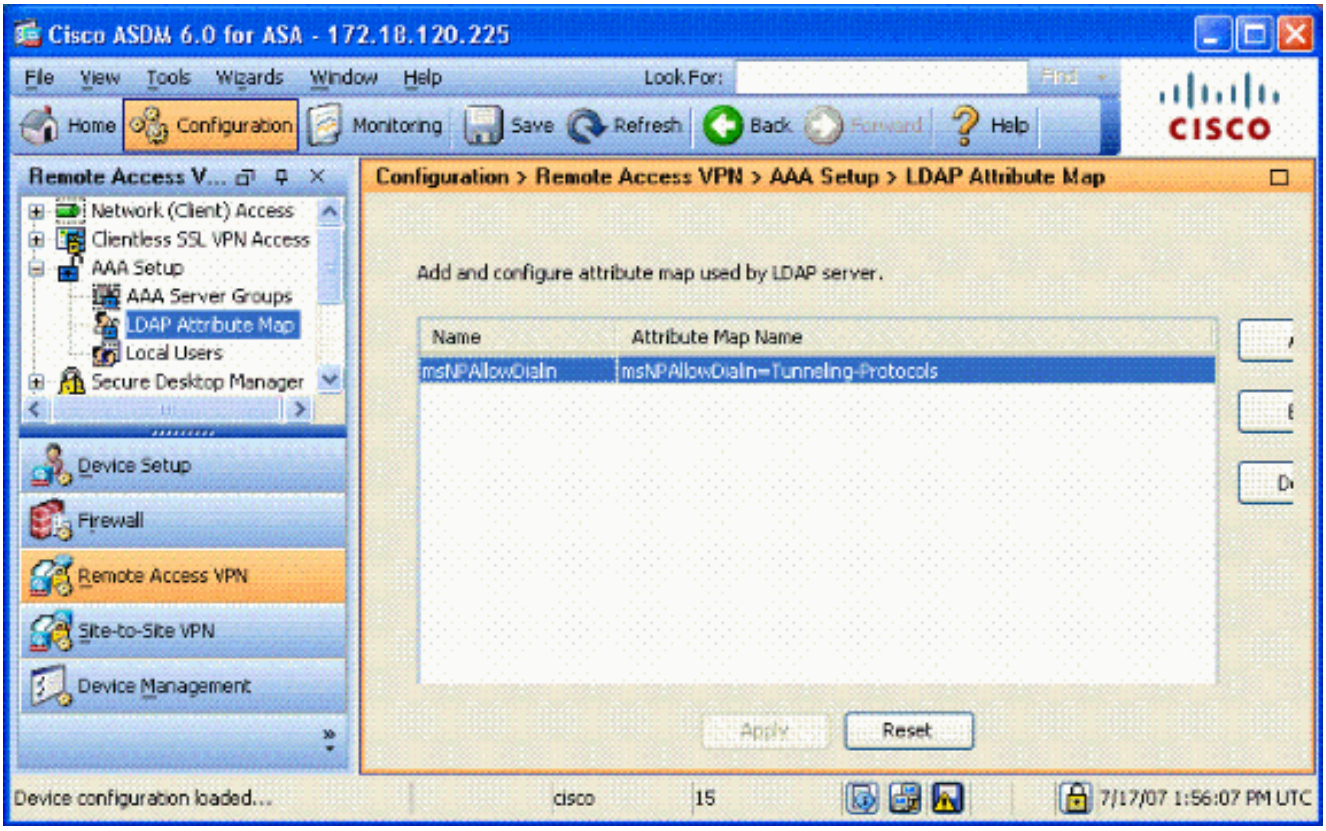
1. In ASDM, scegliere **VPN ad accesso remoto> Impostazione AAA > Mappa attributi LDAP**.
2. Fare clic su **Add**.
3. Nella finestra Aggiungi mappa attributi LDAP, effettuare le seguenti operazioni. Vedere la Figura A3.**Figura A3: Aggiunta della mappa degli attributi LDAP**



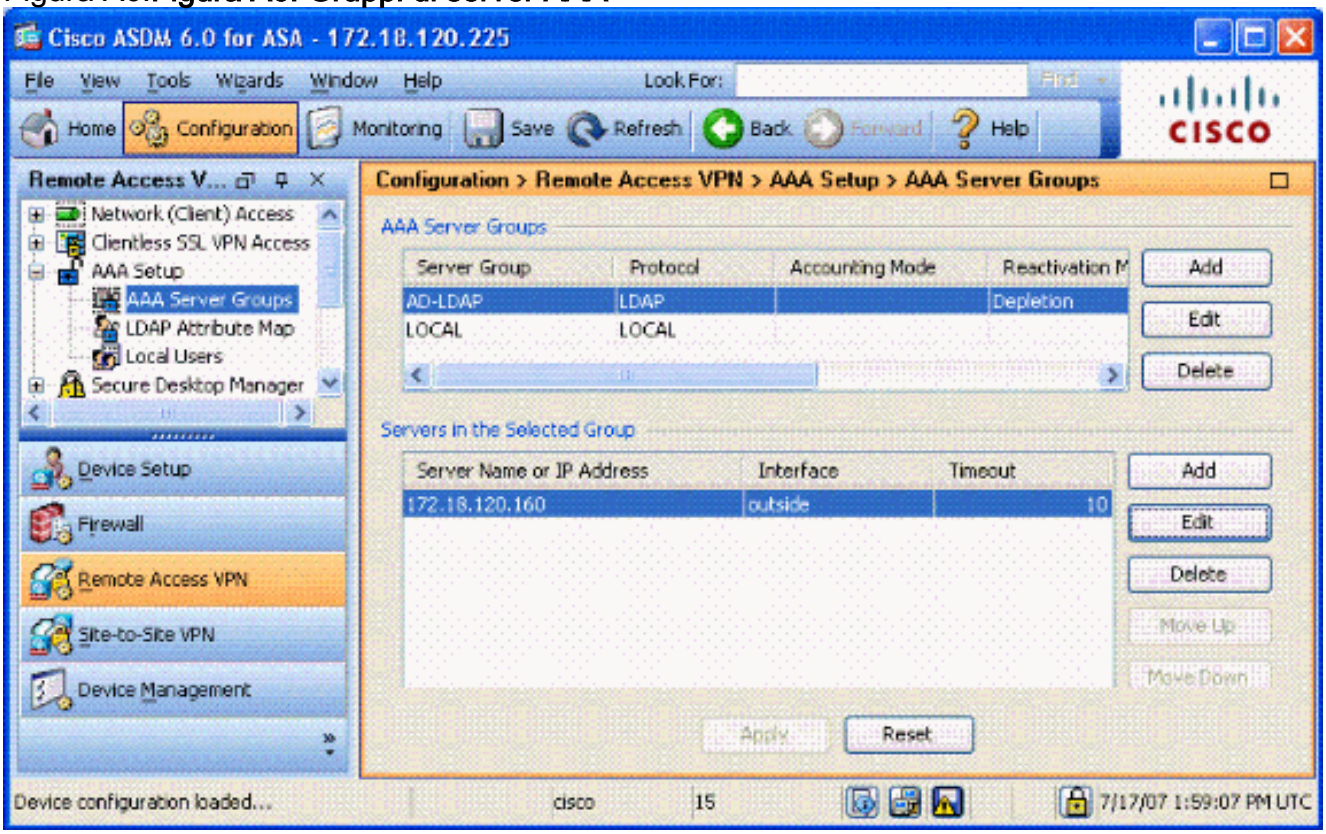
Immettere un nome nella casella di testo Nome.Nella scheda Nome corrispondenza digitare **msNPAllowDialin** nella casella di testo Nome cliente.Nella scheda Map Name (Nome mappa), selezionare **Tunneling-Protocols** (Protocolli di tunneling) nell'opzione a discesa in Cisco Name (Nome Cisco).Fare clic su **Add**.Scegliere la scheda **Valore mappa**.Fare clic su **Add**.Nella finestra Aggiungi valore mappa LDAP dell'attributo, digitare **TRUE** nella casella di testo Nome cliente e digitare **20** nella casella di testo Valore Cisco.Fare clic su **Add**.Digitare **FALSE** nella casella di testo Nome cliente e digitare **1** nella casella di testo Valore Cisco. Vedere la Figura
A4.



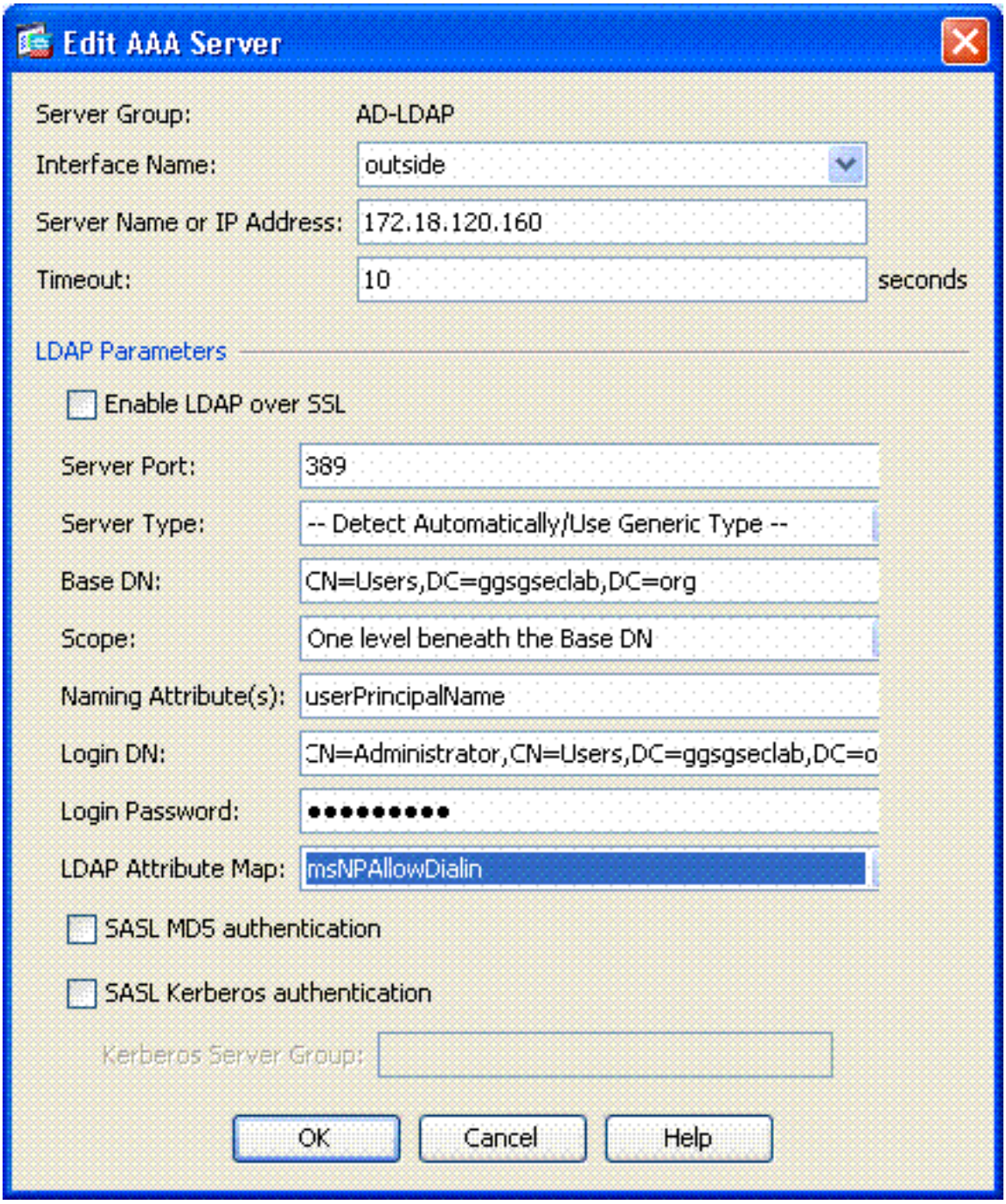
Fare clic su **OK**.Fare clic su **OK**.Fare clic su **Apply** (Applica).La configurazione deve essere simile a quella della Figura A5.**Figura A5: Configurazione mappa attributi LDAP**



4. Scegliere **VPN Accesso remoto> Configurazione AAA > Gruppi di server AAA**. Vedere la Figura A6.**Figura A6: Gruppi di server AAA**



5. Fare clic sul gruppo di server che si desidera modificare. Nella sezione Server del gruppo selezionato scegliere l'indirizzo IP o il nome host del server e quindi fare clic su **Modifica**.
6. Nella finestra Modifica server AAA, nella casella di testo Mappa attributi LDAP, scegliere la mappa degli attributi LDAP creata nel menu a discesa. Vedere la Figura A7**Figura A7: Aggiunta della mappa degli attributi LDAP**



7. Fare clic su **OK**.

Nota: attivare il debug LDAP durante il test per verificare se l'associazione LDAP e il mapping degli attributi funzionano correttamente. Vedere Appendice C per i comandi di risoluzione dei problemi.

Scenario 2: Applicazione di Active Directory tramite l'appartenenza ai gruppi per consentire/negare l'accesso

In questo esempio viene utilizzato l'attributo LDAP memberOf per eseguire il mapping all'attributo Tunneling Protocol al fine di stabilire l'appartenenza a un gruppo come condizione. Affinché questo criterio funzioni, è necessario che siano soddisfatte le seguenti condizioni:

- Usare un gruppo già esistente o crearne uno nuovo a cui gli utenti VPN ASA possano appartenere per le condizioni ALLOW.
- Utilizzare un gruppo già esistente o creare un nuovo gruppo per gli utenti non ASA a cui

appartenere per le condizioni DENY.
- Assicurarsi di verificare nel visualizzatore LDAP che si disponga del DN corretto per il gruppo. Vedere Appendice D. Se il DN è errato, il mapping non funziona correttamente.

Nota: in questa release, l'appliance ASA può leggere solo la prima stringa dell'attributo memberOf. Assicurarsi che il nuovo gruppo creato sia all'inizio dell'elenco. L'altra opzione consiste nell'inserire un carattere speciale davanti al nome, in quanto AD cerca prima i caratteri speciali. Per risolvere questo problema, utilizzare DAP nel software 8.x per esaminare più gruppi.

Nota: verificare che un utente appartenga al gruppo di negazione o ad almeno un altro gruppo, in modo che memberOf venga sempre rimandato all'appliance ASA. Non è necessario specificare la condizione di rifiuto FALSE, ma è buona norma farlo. Se il nome del gruppo esistente o il nome del gruppo contiene uno spazio, immettere l'attributo nel modo seguente:

```
CN=Backup Operators,CN=Builtin,DC=ggsgseclab,DC=org
```

Nota: il protocollo DAP consente all'appliance ASA di esaminare più gruppi nell'attributo memberOf e nell'autorizzazione di base dei gruppi. Vedere la sezione DAP.

MAPPING

- Il valore dell'attributo di Active Directory:memberOf CN=ASAUsers,CN=Users,DC=gsgseclab,DC=orgmemberOf CN=TelnetClients,CN=Users,DC=labrat,DC=com
- Valore attributo Cisco: 1 = FALSO, 20 = VERO,

Per la condizione **ALLOW**, è possibile mappare:

- memberOf CN=ASAUsers,CN=Users,DC=gsgseclab,DC=org= 20

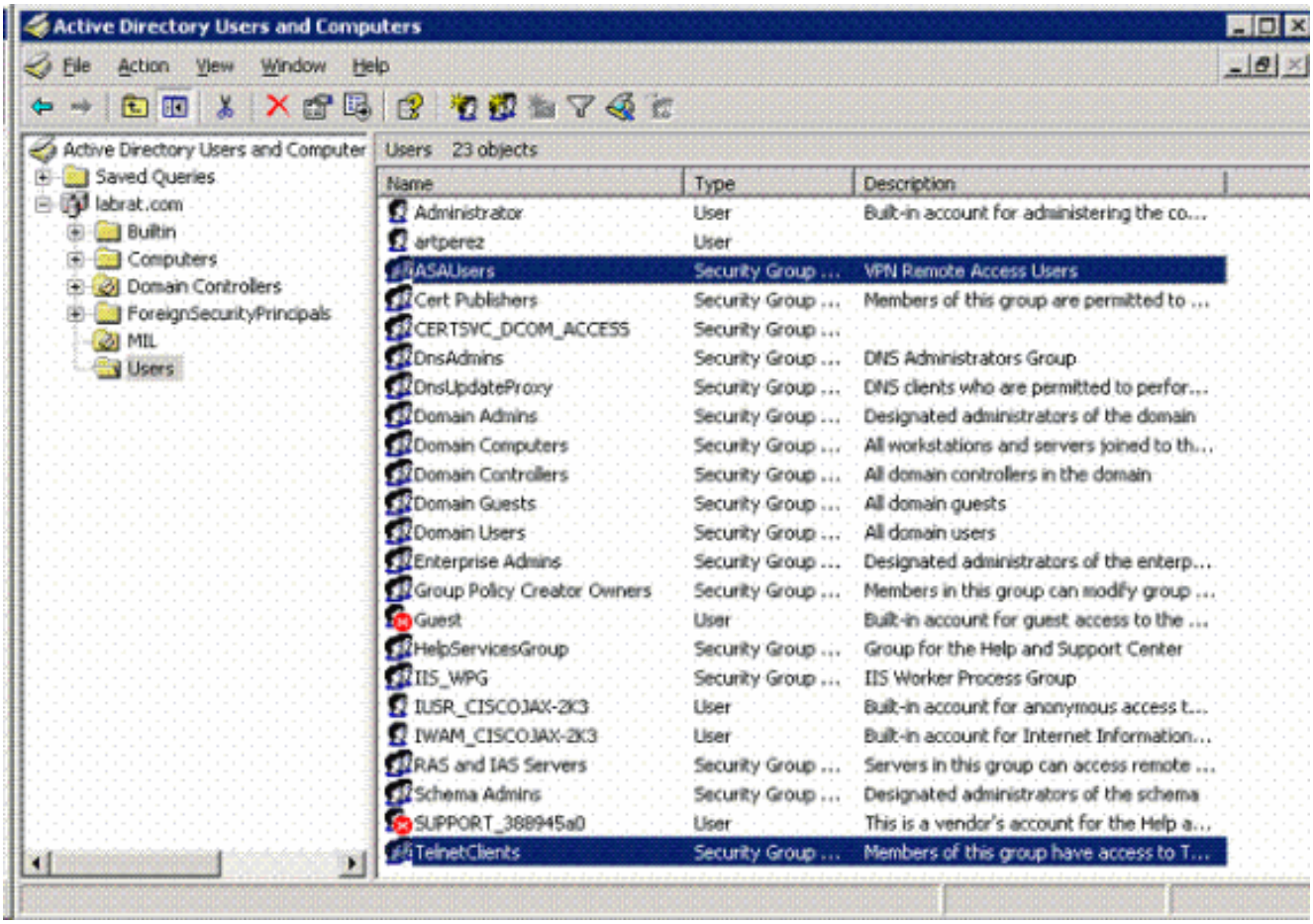
Per la condizione **DENY**, è possibile mappare:

- memberOf CN=TelnetClients,CN=Users,DC=gsgseclab,DC=org = 1

Nota: nelle versioni future, è presente un attributo Cisco che permette e nega la connessione. per ulteriori informazioni sugli attributi Cisco, fare riferimento a Configurazione di un server esterno per l'autorizzazione degli utenti di Security Appliance.

Installazione di Active Directory

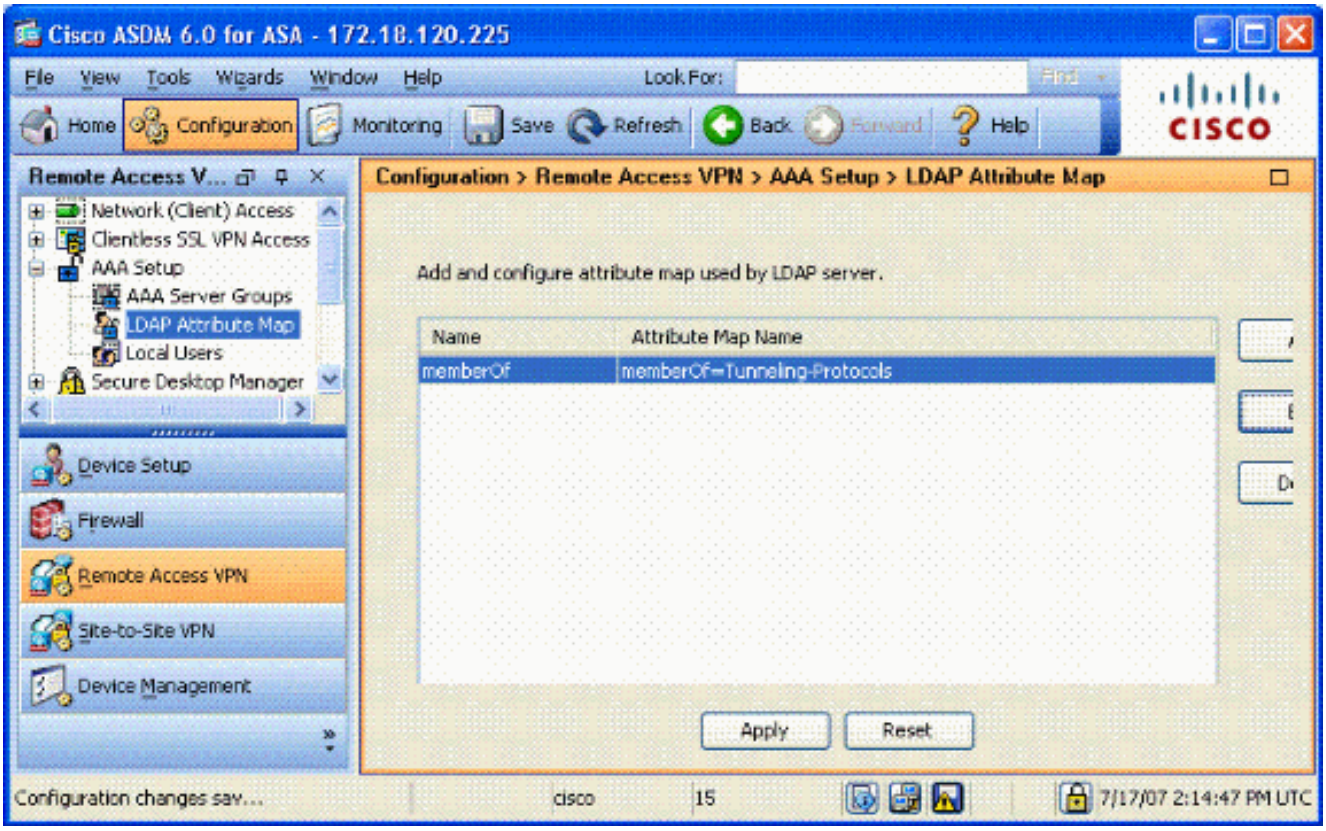
1. Nel server Active Directory scegliere **Start > Esegui**.
2. Nella casella di testo Apri digitare **dsa.msc** e quindi fare clic su **OK**. Verrà avviata la console di gestione di Active Directory.
3. Nella console di gestione di Active Directory fare clic sul segno più per espandere Utenti e computer di Active Directory. Vedere la Figura A8**Figura A8: Gruppi di Active Directory**



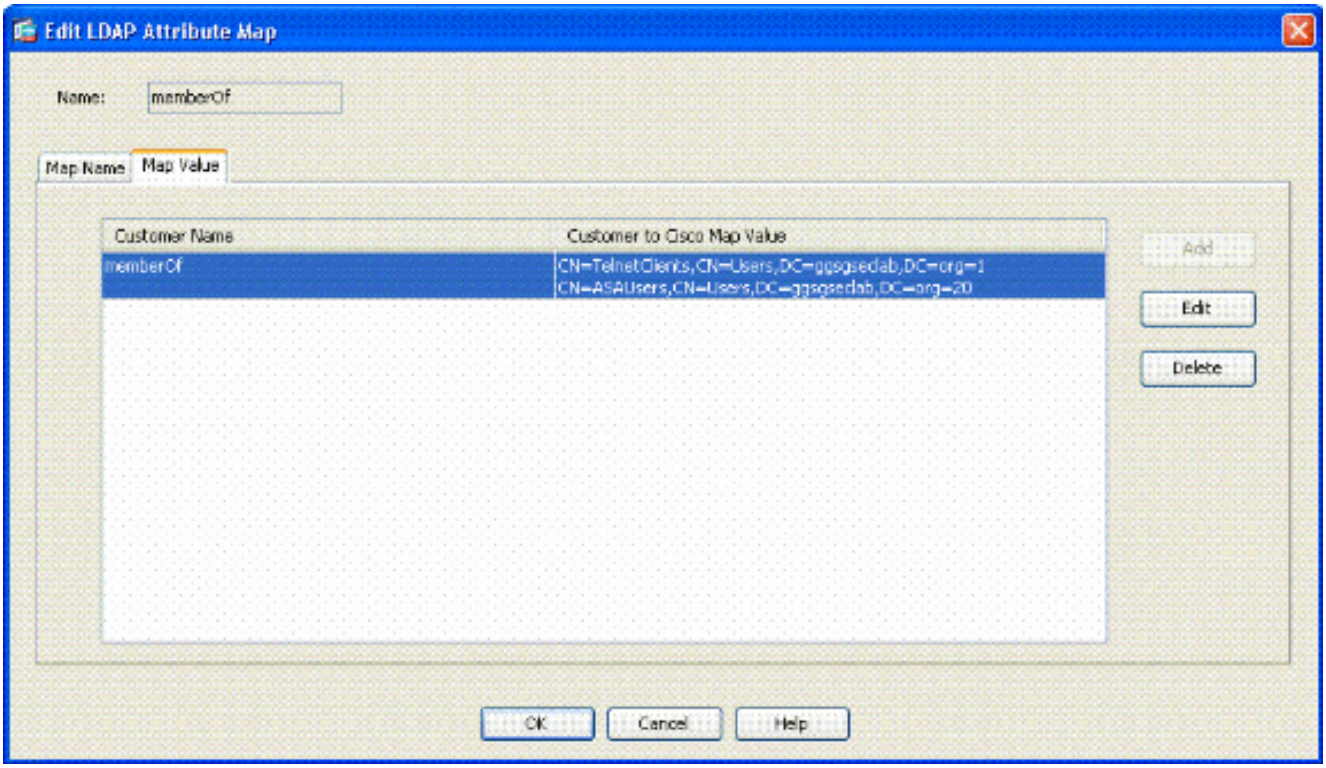
4. Fare clic sul segno più per espandere il nome del dominio.
5. Fare clic con il pulsante destro del mouse sulla cartella **Utenti** e scegliere **Nuovo > Gruppo**.
6. Immettere un nome per il gruppo. Ad esempio: Utenti ASAU.
7. Fare clic su **OK**.
8. Fare clic sulla cartella **Utenti**, quindi fare doppio clic sul gruppo appena creato.
9. Scegliere la scheda **Membri** e quindi fare clic su **Aggiungi**.
10. Digitare il nome dell'utente che si desidera aggiungere e quindi fare clic su **OK**.

Configurazione ASA

1. In ASDM, scegliere **VPN ad accesso remoto > Impostazione AAA > Mappa attributi LDAP**.
2. Fare clic su **Add**.
3. Nella finestra Aggiungi mappa attributi LDAP, effettuare le seguenti operazioni. Vedere la Figura A3.Immettere un nome nella casella di testo Nome.Nella scheda Nome corrispondenza digitare **memberOf** nella casella di testo Nome cliente c.Nella scheda Map Name (Nome mappa), selezionare **Tunneling-Protocols** (Protocolli di tunneling) nell'opzione a discesa in Cisco Name (Nome Cisco).Scegliere **Aggiungi**.Fare clic sulla scheda **Valore mappa**.Scegliere **Aggiungi**.Nella finestra Aggiungi valore mappa LDAP dell'attributo, digitare **CN=ASAUsers,CN=Users,DC=gsgseclab,DC=org** nella casella di testo Nome cliente e digitare **20** nella casella di testo Valore Cisco.Fare clic su **Add**.Digitare **CN=TelnetClients,CN=Users,DC=gsgseclab,DC=org** nella casella di testo Nome cliente e digitare **1** nella casella di testo Valore Cisco. Vedere la Figura A4.Fare clic su **OK**.Fare clic su **OK**.Fare clic su **Apply** (Applica).La configurazione deve essere simile a quella della Figura A9.**Figura A9: mappa degli attributi LDAP**



4. Scegliere **VPN Accesso remoto> Configurazione AAA > Gruppi di server AAA**.
5. Fare clic sul gruppo di server che si desidera modificare. Nella sezione Server del gruppo selezionato selezionare l'indirizzo IP o il nome host del server e quindi fare clic su **Modifica**



6. Nella finestra Modifica server AAA, nella casella di testo Mappa attributi LDAP, selezionare la mappa attributi LDAP creata nel menu a discesa.
7. Fare clic su **OK**.

Nota: attivare il debug LDAP durante il test per verificare il corretto funzionamento dell'associazione LDAP e dei mapping di attributi. Vedere Appendice C per i comandi di risoluzione dei problemi.

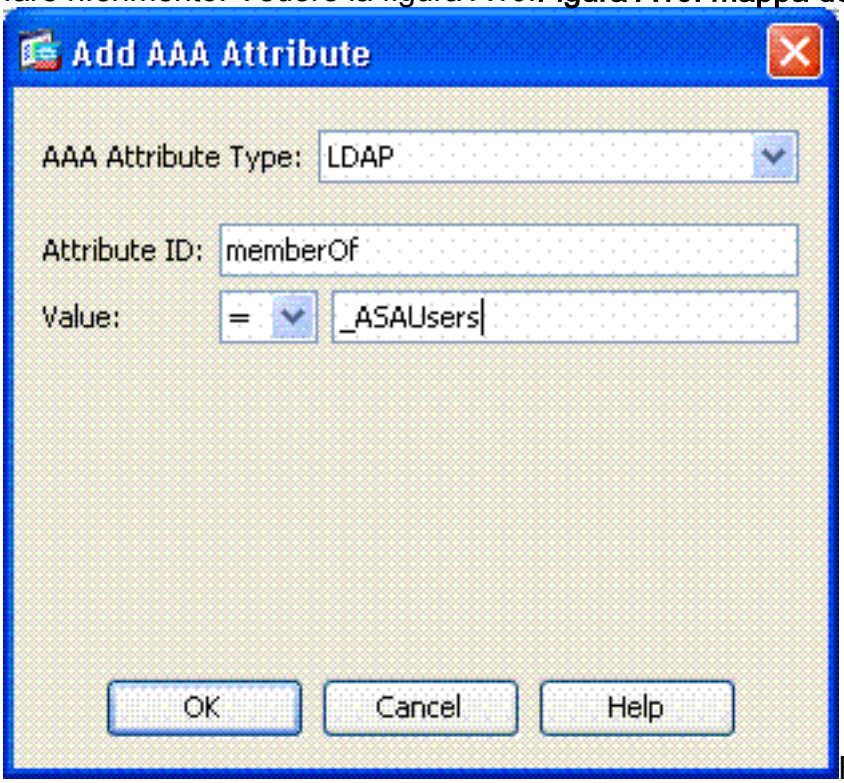
Scenario 3: Criteri di accesso dinamico per più attributi memberOf

In questo esempio viene utilizzato il protocollo DAP per esaminare più attributi memberOf e consentire l'accesso in base all'appartenenza ai gruppi di Active Directory. Nelle versioni precedenti alla 8.x, l'ASA ha letto solo il primo attributo memberOf. Con la versione 8.x e successive, l'ASA può esaminare tutti gli attributi memberOf.

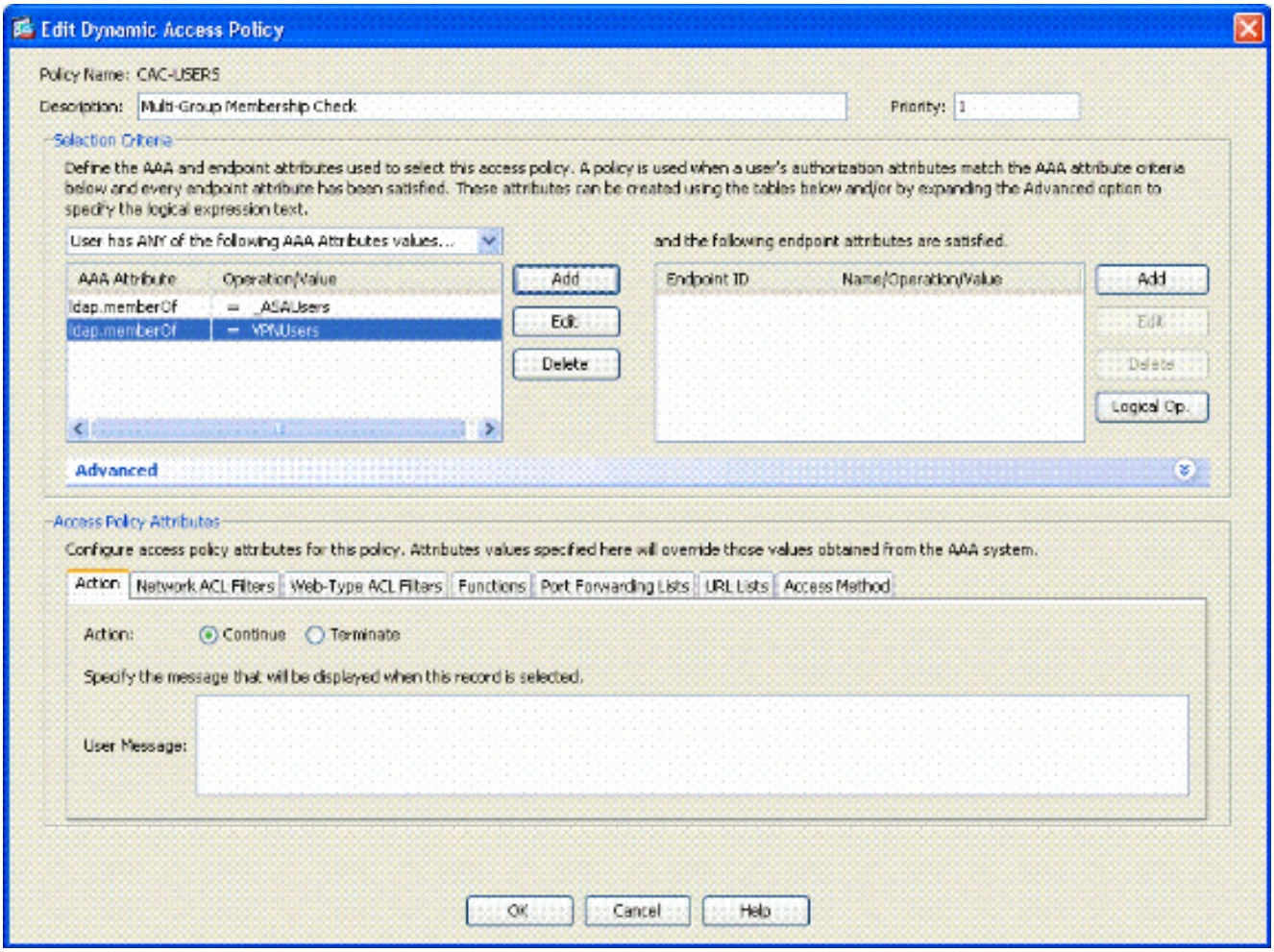
- Usare un gruppo già esistente o creare un nuovo gruppo (o più gruppi) di cui gli utenti VPN ASA devono essere membri per le condizioni ALLOW.
- Utilizzare un gruppo già esistente o creare un nuovo gruppo per gli utenti non ASA a cui appartenere per le condizioni DENY.
- Assicurarsi di verificare nel visualizzatore LDAP che si disponga del DN corretto per il gruppo. Vedere Appendice D. Se il DN è errato, il mapping non funziona correttamente.

Configurazione ASA

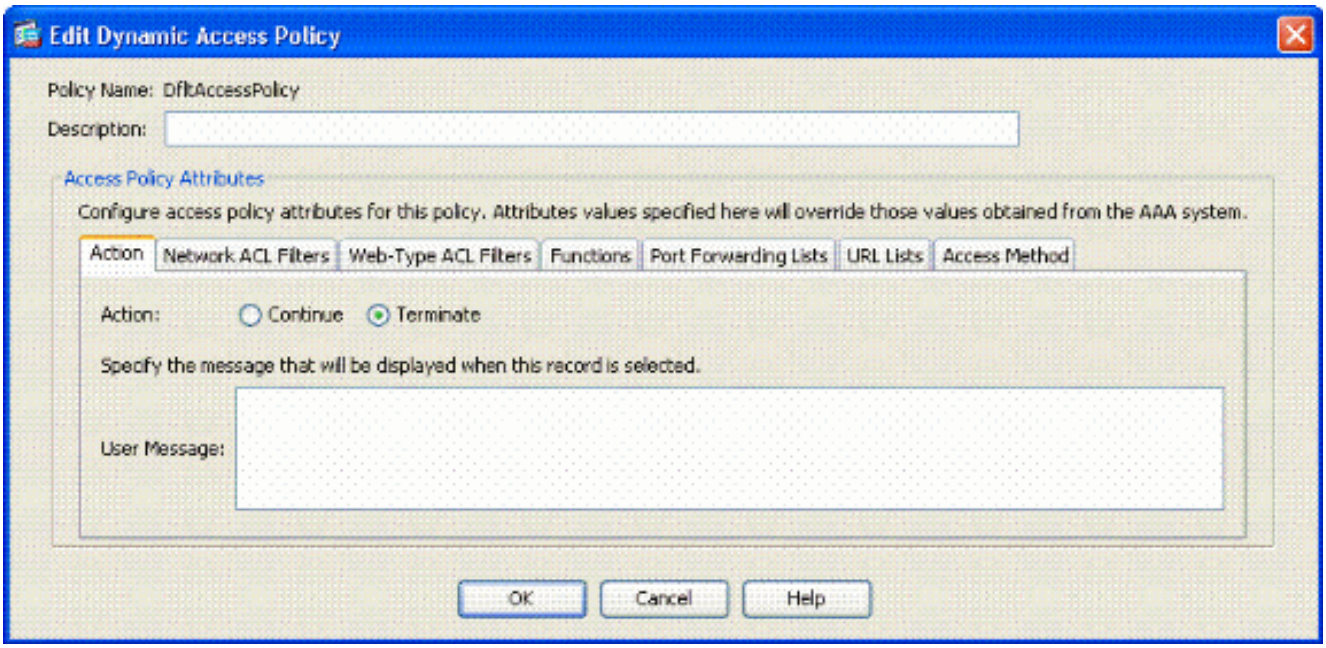
1. In ASDM, scegliere **VPN ad accesso remoto > Accesso di rete (client) > Criteri di accesso dinamico**.
2. Fare clic su **Add**.
3. In Aggiungi criterio di accesso dinamico eseguire la procedura seguente:Immettere un nome nella casella di testo Nome b.Nella sezione Priorità immettere **1** o un numero maggiore di 0.Nel campo Criteri di selezione fare clic su **Aggiungi**.In Aggiungi attributo AAA, scegliere **LDAP**.Nella sezione ID attributo immettere **memberOf**.Nella sezione Valore, scegliere **=** e immettere il nome del gruppo AD. Ripetete questo passo per ogni gruppo a cui desiderate fare riferimento. Vedere la figura A10.**Figura A10: mappa degli attributi AAA**



Fare clic su **OK**.Nella sezione Attributi dei criteri di accesso **scegliere Continua**. Vedere la figura A11.**Figura A11 Aggiunta di un criterio dinamico**



4. In ASDM, scegliere **VPN ad accesso remoto > Accesso di rete (client) > Criteri di accesso dinamico**.
5. Scegliere **Criterio di accesso predefinito**, quindi **Modifica**.
6. L'azione predefinita deve essere impostata su **Termina**. Vedere la figura A12.**Figura A12 Modifica criterio dinamico**



7. Fare clic su **OK**.

Nota: se l'opzione **Termina** non è selezionata, è possibile eseguire l'operazione anche se non in alcun gruppo, in quanto per impostazione predefinita viene selezionata l'opzione Continua.

Appendice B - Configurazione ASA CLI

ASA 5510

```
ciscoasa#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname asa80
domain-name army.mil
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address x.x.x.x 255.255.255.128
!
interface GigabitEthernet0/1
nameif inside
security-level 100
no ip address
!
boot system disk0:/asa802-k8.bin
ftp mode passive
dns server-group DefaultDNS
domain-name army.mil
!
--------------ACL's---------------------------------
------------
access-list out extended permit ip any any
------------------------------------------------------
------------
pager lines 24
logging console debugging
mtu outside 1500
!
---------------VPN Pool---------------------------------
------------
ip local pool CAC-USERS 192.168.1.1-192.168.1.254 mask
255.255.255.0
------------------------------------------------------
------------
!
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400
access-group out in interface outside
route outside 0.0.0.0 0.0.0.0 172.18.120.129 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect
0:02:00
```

```
timeout uauth 0:05:00 absolute
!
-------------------------LDAP Maps & DAP---------------
------------
ldap attribute-map memberOf
map-name memberOf Tunneling-Protocols
March 11, 2008 ASA – CAC Authentication for AnyConnect
VPN Access
Company Confidential. A printed copy of this document is
considered uncontrolled.
49
map-value memberOf
CN=_ASAUsers,CN=Users,DC=ggsgseclab,DC=org 20
ldap attribute-map msNPAllowDialin
map-name msNPAllowDialin Tunneling-Protocols
map-value msNPAllowDialin FALSE 1
map-value msNPAllowDialin TRUE 20
dynamic-access-policy-record CAC-USERS
description "Multi-Group Membership Check"
priority 1
dynamic-access-policy-record DfltAccessPolicy
action terminate
------------------------------------------------------
------------
!
--------------------LDAP Server-------------------------
------------
aaa-server AD-LDAP protocol ldap
aaa-server AD-LDAP (outside) host 172.18.120.160
ldap-base-dn CN=Users,DC=ggsgseclab,DC=org
ldap-scope onelevel
ldap-naming-attribute userPrincipalName
ldap-login-password *
ldap-login-dn
CN=Administrator,CN=Users,DC=ggsgseclab,DC=org
------------------------------------------------------
------------
!
aaa authentication http console LOCAL
http server enable 445
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
!
----------------CA Trustpoints---------------------------
------------
crypto ca trustpoint ASDM_TrustPoint0
revocation-check ocsp
enrollment terminal
keypair DoD-1024
match certificate DefaultCertificateMap override ocsp
trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
crl configure
crypto ca trustpoint ASDM_TrustPoint1
revocation-check ocsp
enrollment terminal
fqdn asa80
subject-name CN=asa80,OU=PKI,OU=DoD,O=U.S.
Government,C=US
keypair DoD-1024
match certificate DefaultCertificateMap override ocsp
```

```
trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
no client-types
crl configure
crypto ca trustpoint ASDM_TrustPoint2
revocation-check ocsp
enrollment terminal
keypair DoD-2048
match certificate DefaultCertificateMap override ocsp
trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
no client-types
crl configure
crypto ca trustpoint ASDM_TrustPoint3
revocation-check ocsp none
enrollment terminal
crl configure
!
------------------Certificate Map----------------------
---------
crypto ca certificate map DefaultCertificateMap 10
subject-name ne ""
--------------------CA Certificates (Partial Cert is
Shown)------------
crypto ca certificate chain ASDM_TrustPoint0
certificate ca 37
3082044c 30820334 a0030201 02020137 300d0609 2a864886
f70d0101
05050030
60310b30 09060355 04061302 55533118 30160603 55040a13
0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c
300a0603
55040b13
03504b49 311b3019 06035504 03131244 6f44204a 49544320
526f6f74
crypto ca certificate chain ASDM_TrustPoint1
certificate 319e
30820411 3082037a a0030201 02020231 9e300d06 092a8648
86f70d01
01050500
305c310b 30090603 55040613 02555331 18301606 0355040a
130f552e
532e2047
6f766572 6e6d656e 74310c30 0a060355 040b1303 446f4431
0c300a06
0355040b
crypto ca certificate chain ASDM_TrustPoint2
certificate ca 37
3082044c 30820334 a0030201 02020137 300d0609 2a864886
f70d0101
05050030
60310b30 09060355 04061302 55533118 30160603 55040a13
0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c
300a0603
55040b13
f766e045 f15ddb43 9549d1e9 a0ea6814 b64bcece 089e1b6e
1be959a5
6fc20a76
crypto ca certificate chain ASDM_TrustPoint3
certificate ca 05
```

```
30820370 30820258 a0030201 02020105 300d0609 2a864886
f70d0101
05050030
5b310b30 09060355 04061302 55533118 30160603 55040a13
0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c
300a0603
55040b13
03504b49 31163014 06035504 03130d44 6f442052 6f6f7420
43412032
301e170d
30343132 31333135 30303130 5a170d32 39313230 35313530
3031305a
305b310b
30090603 55040613 02555331 18301606 0355040a 130f552e
532e2047
6f766572
6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06
0355040b
1303504b
49311630 14060355 0403130d 446f4420 526f6f74 20434120
32308201
crypto ca certificate chain ASDM_TrustPoint4
certificate ca 04
30820267 308201d0 a0030201 02020104 300d0609 2a864886
f70d0101
05050030
61310b30 09060355 04061302 55533118 30160603 55040a13
0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c
300a0603
55040b13
03504b49 311c301a 06035504 03131344 6f442043 4c415353
20332052
6f6f7420
!
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
```

```
!
------------------------SSL/WEBVPN---------------------
---------------
ssl certificate-authentication interface outside port
443
webvpn
enable outside
svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1
svc enable
tunnel-group-list enable
-----------------------------------------------------
------------
-----------------------VPN Group/Tunnel Policy----------
----------
group-policy CAC-USERS internal
ggroup-policy AC-USERS internal
group-policy AC-USERS attributes
vpn-tunnel-protocol svc
address-pools value CAC-USERS
webvpn
svc ask none default svc
tunnel-group AC-USERS type remote-access
tunnel-group AC-USERS general-attributes
authorization-server-group AD-LDAP
default-group-policy AC-USERS
authorization-required
authorization-dn-attributes UPN
tunnel-group AC-USERS webvpn-attributes
authentication certificate
group-alias AC-USERS enable
tunnel-group-map enable rules
no tunnel-group-map enable ou
no tunnel-group-map enable ike-id
no tunnel-group-map enable peer-ip
-----------------------------------------------------
------------
prompt hostname context
```

Appendice C - Risoluzione dei problemi

Risoluzione dei problemi relativi a AAA e LDAP

- **debug ldap 255**: visualizza gli scambi LDAP
- **debug aaa common 10**: visualizza gli scambi AAA

Esempio 1: Connessione consentita con mapping di attributi corretto

Nell'esempio viene mostrato l'output dei comandi **debug ldap** e **debug aaa common** durante una connessione riuscita allo scenario 2 mostrato nell'Appendice A.

Figura C1: output comune debug LDAP e debug aaa - mapping corretto

```
AAA API: In aaa_open
AAA session opened: handle = 39
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
```

```
AAA task: aaa_process_msg(1a87a64) received message type
0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
-------------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[78] Session Start
[78] New request Session, context 0x26f1c44, reqType = 0
[78] Fiber started
[78] Creating LDAP context with uri=ldap://
172.18.120.160:389
[78] Binding as administrator
[78] Performing Simple authentication for Administrator
to
172.18.120.160
[78] Connect to LDAP server: ldap:// 172.18.120.160,
status =
Successful
[78] LDAP Search:
Base DN = [CN=Users,DC=ggsgseclab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
[78] Retrieved Attributes:
[78] objectClass: value = top
[78] objectClass: value = person
[78] objectClass: value = organizationalPerson
[78] objectClass: value = user
[78] cn: value = Ethan Hunt
[78] sn: value = Hunt
[78] userCertificate: value =
0..50........../........60...*.H........0@1.0.....&...,d
....com1.0.....
&...,d...
[78] userCertificate: value =
0..'0........../..t.....50...*.H........0@1.0.....&...,d
....com1.0.....
&...,d...
[78] givenName: value = Ethan
[78] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[78] instanceType: value = 4
[78] whenCreated: value = 20060613151033.0Z
[78] whenChanged: value = 20060622185924.0Z
[78] displayName: value = Ethan Hunt
[78] uSNCreated: value = 14050
[78] memberOf: value =
CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[78] mapped to cVPN3000-Tunneling-Protocols: value = 20
[78] uSNChanged: value = 14855
[78] name: value = Ethan Hunt
[78] objectGUID: value = ..9...NJ..GU..z.
[78] userAccountControl: value = 66048
[78] badPwdCount: value = 0
[78] codePage: value = 0
[78] countryCode: value = 0
[78] badPasswordTime: value = 127954717631875000
[78] lastLogoff: value = 0
[78] lastLogon: value = 127954849209218750
```

```
[78] pwdLastSet: value = 127946850340781250
[78] primaryGroupID: value = 513
[78] objectSid: value = ................q......mY...
[78] accountExpires: value = 9223372036854775807
[78] logonCount: value = 25
[78] sAMAccountName: value = 1234567890
[78] sAMAccountType: value = 805306368
[78] userPrincipalName: value = 1234567890@mil
[78] objectCategory: value =
[78] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
[78] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[78] Session End
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE,
auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-
LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state =
IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(CAC-USERS)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp:
GROUP_POLICY_DB)
-------------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
User: CAC-USER
Pasw:
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a870b4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY,
auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-
LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user
1234567890@mil
AAA FSM: In AAA_Callback
```

```
user attributes:
1 Tunnelling-Protocol(4107) 20 20
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunnelling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "ggsgseclab.org"
5 List of address pools to assign addresses from(4313)
10
"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type
3
In aaai_close_session (39)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
CAC-Test#
```

Esempio 2: Connessione consentita con mapping di attributi Cisco non configurati correttamente

Nell'esempio viene mostrato l'output dei comandi **debug ldap** e **debug aaa common** durante una connessione consentita allo scenario 2 mostrato nell'Appendice A.

Figura C2: output comune debug LDAP e debug aaa - mapping non corretto

```
AAA API: In aaa_open
AAA session opened: handle = 41
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type
0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
-------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[82] Session Start
[82] New request Session, context 0x26f1c44, reqType = 0
[82] Fiber started
[82] Creating LDAP context with
uri=ldap://172.18.120.160:389
[82] Binding as administrator
[82] Performing Simple authentication for Administrator
to
172.18.120.160
[82] Connect to LDAP server: ldap:// 172.18.120.160:389,
status =
Successful
[82] LDAP Search:
Base DN = [CN=Users,DC=ggsgseclab,DC=org]
```

```
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
[82] Retrieved Attributes:
[82] objectClass: value = top
[82] objectClass: value = person
[82] objectClass: value = organizationalPerson
[82] objectClass: value = user
[82] cn: value = Ethan Hunt
[82] sn: value = Hunt
[82] userCertificate: value =
0..50........./........60...*.H........0@1.0.....&...,d
....com1.0.....
&...,d...
[82] userCertificate: value =
0..'0........./..t.....50...*.H........0@1.0.....&...,d
....com1.0.....
&...,d...
[82] givenName: value = Ethan
[82] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[82] instanceType: value = 4
[82] whenCreated: value = 20060613151033.0Z
[82] whenChanged: value = 20060622185924.0Z
[82] displayName: value = Ethan Hunt
[82] uSNCreated: value = 14050
[82] memberOf: value =
CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[82] mapped to cVPN3000-Tunneling-Protocols: value =
CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[82] uSNChanged: value = 14855
[82] name: value = Ethan Hunt
[82] objectGUID: value = ..9...NJ..GU..z.
[82] userAccountControl: value = 66048
[82] badPwdCount: value = 0
[82] codePage: value = 0
[82] countryCode: value = 0
[82] badPasswordTime: value = 127954717631875000
[82] lastLogoff: value = 0
[82] lastLogon: value = 127954849209218750
[82] pwdLastSet: value = 127946850340781250
[82] primaryGroupID: value = 513
[82] objectSid: value = ................q......mY...
[82] accountExpires: value = 9223372036854775807
[82] logonCount: value = 25
[82] sAMAccountName: value = 1234567890
[82] sAMAccountType: value = 805306368
[82] userPrincipalName: value = 1234567890@mil
[82] objectCategory: value =
CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=or
g
[82] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
[82] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[82] Session End
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE,
```

```
auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-
LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state =
IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(USAFE)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp:
GROUP_POLICY_DB)
-----------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
User: CAC-USERS
Pasw:
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a870b4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY,
auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-
LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user
1234567890@mil
AAA FSM: In AAA_Callback
user attributes:
1 Tunnelling-Protocol(4107) 20 0
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunnelling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "ggsgseclab.org"
5 List of address pools to assign addresses from(4313)
10
"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type
3
In aaai_close_session (41)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
```

Risoluzione dei problemi DAP

- **debug dap errors**: visualizza gli errori DAP.
- **debug dap trace**: visualizza la traccia della funzione DAP

Esempio 1: Connessione consentita con DAP

In questo esempio viene mostrato l'output degli **errori di debug dap** e della **traccia di debug dap** durante una connessione riuscita con lo scenario 3 mostrato nell'Appendice A. Si notino più attributi memberOf. È possibile appartenere sia a _ASAUsers che a VPNUsers o a entrambi i gruppi, a seconda della configurazione ASA.

Figura C3: debug DAP

```
#debug dap errors
debug dap errors enabled at level 1
#debug dap trace
debug dap trace enabled at level 1
#
The DAP policy contains the following attributes for
user:
1241879298@mil
------------------------------------------------------------
---------------
---
1: action = continue
DAP_TRACE: DAP_open: C8EEFA10
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.2 = person
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.3 =
organizationalPerson
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.4 = user
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn =
1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName
= 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=ggsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.whenCreated =
20070626163734.0Z
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.whenChanged =
20070718151143.0Z
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.displayName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNCreated
= 33691
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.1
= VPNUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.2
= _ASAUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged
```

```
= 53274
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.department
= NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name =
1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID
=
....+..F.."5....
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userAccountControl =
328192
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage =
0
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.badPasswordTime = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff
= 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon
= 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet
=
128273494546718750
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userParameters = m:
d.
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid
= ..
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.accountExpires =
9223372036854775807
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount
= 0
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.sAMAccountName =
1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.sAMAccountType =
805306368
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userPrincipalName =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectCategory =
CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=or
g
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username
=
1241879298@mil
DAP_TRACE: Username: 1241879298@mil,
aaa.cisco.tunnelgroup = CAC-USERS
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] =
"top";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person";
```

```
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] =
"1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeN
ame"] =
"NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"]
= "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=ggsgseclab,DC=org";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"]
= "33691";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["1"] =
"VPNUsers";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["2"] =
"_ASAUsers";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"]
= "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"]
= "NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"]
contains
binary data
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] =
"0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] =
"0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"]
= "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"]
= "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"]
=
"128273494546718750";
```

```
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] =
"513";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userParameters"]
contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"]
contains binary
data
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"]
= "0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=o
rg";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] =
"TRUE";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"]
=
"1241879298@mil";
DAP_TRACE:
dap_add_to_lua_tree:aaa["cisco"]["tunnelgroup"] =
"CACUSERS";
DAP_TRACE:
dap_add_to_lua_tree:endpoint["application"]["clienttype"
] =
"IPSec";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs: CAC-
USERS
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 1 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr:
rec_count = 1
DAP_TRACE: Username: 1241879298@mil, DAP_close: C8EEFA10
d.
```

Esempio 2: Connessione negata con DAP

Nell'esempio viene mostrato l'output degli **errori** di **debug dap** e della **traccia di debug dap** durante una connessione non riuscita allo scenario 3 mostrato nell'Appendice A.

Figura C4: debug DAP

```
#debug dap errors
debug dap errors enabled at level 1
#debug dap trace
debug dap trace enabled at level 1
```

```
#
The DAP policy contains the following attributes for
user:
1241879298@mil
------------------------------------------------------
---------------
---
1: action = terminate
DAP_TRACE: DAP_open: C91154E8
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.2 = person
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.3 =
organizationalPerson
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.4 = user
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn =
1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName
= 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=ggsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.whenCreated =
20070626163734.0Z
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.whenChanged =
20070718151143.0Z
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.displayName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNCreated
= 33691
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf =
DnsAdmins
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged
= 53274
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.department
= NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name =
1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID
=
....+..F.."5....
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userAccountControl =
328192
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage =
0
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.badPasswordTime = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff
= 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon
```

```
= 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet
=
128273494546718750
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userParameters = m:
d.
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid
= ..
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.accountExpires =
9223372036854775807
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount
= 0
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.sAMAccountName =
1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.sAMAccountType =
805306368
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userPrincipalName =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectCategory =
CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=or
g
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username
=
1241879298@mil
DAP_TRACE: Username: 1241879298@mil,
aaa.cisco.tunnelgroup = CAC-USERS
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] =
"top";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] =
"1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeN
ame"] =
"NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"]
= "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=ggsgseclab,DC=org";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z";
```

```
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"]
= "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"] =
"DnsAdmins";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"]
= "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"]
= "NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"]
contains
binary data
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] =
"0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] =
"0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"]
= "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"]
= "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"]
=
"128273494546718750";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] =
"513";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userParameters"]
contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"]
contains binary
data
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"]
= "0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
```

```
"CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=o
rg";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] =
"TRUE";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"]
=
"1241879298@mil";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs:
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 0 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr:
rec_count = 1
```

Risoluzione dei problemi di Autorità di certificazione/OCSP

- **debug crypto ca 3**
- In modalità di configurazione - **debug della console o del buffer della classe di registrazione**

In questi esempi viene illustrata una convalida del certificato riuscita con il risponditore OCSP e un criterio di corrispondenza del gruppo di certificati non riuscito.

Nella Figura C3 viene illustrato l'output di debug con un certificato convalidato e un gruppo di certificati funzionante corrispondente ai criteri.

Nella Figura C4 viene illustrato l'output di debug di un criterio di corrispondenza gruppo di certificati non configurato correttamente.

Nella figura C5 viene illustrato l'output di debug di un utente con certificato revocato.

Figura C5: Debug OCSP - convalida del certificato riuscita

```
CRYPTO_PKI: Found a suitable authenticated trustpoint
ASDM_TrustPoint11.
CRYPTO_PKI: Allocated OCSP data handle 0xca2d27b8
CRYPTO_PKI: Certificate validation: Successful, status:
0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: status = 0: poll revocation status
CRYPTO_PKI: Attempting to find OCSP override for peer
cert: serial
number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
CRYPTO_PKI: Processing map rules for SSL.
CRYPTO_PKI: Processing map SSL sequence 20...
CRYPTO_PKI: Match of subject-name field to map PASSED.
Peer cert field:
=
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: SSL
sequence: 20.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://198.154.68.90, Override trustpoint:
ASDM_TrustPoint12
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
```

```
CRYPTO_PKI: Destroying OCSP data handle 0xca2d27b8
Crypto CA thread sleeps!
CRYPTO_PKI: Attempting to find tunnel group for cert
with serial
number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
CRYPTO_PKI: Processing map rules for
DefaultCertificateMap.
CRYPTO_PKI: Processing map DefaultCertificateMap
sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED.
Peer cert field:
=
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map:
DefaultCertificateMap
sequence: 10.
CRYPTO_PKI: Ignoring match on map DefaultCertificateMap,
index 10 for
WebVPN group map processing. No tunnel group is
configured.
CRYPTO_PKI: Peer cert could not be authorized with map:
DefaultCertificateMap.
CRYPTO_PKI: Processing map rules for SSL.
CRYPTO_PKI: Processing map SSL sequence 20...
CRYPTO_PKI: Match of subject-name field to map PASSED.
Peer cert field:
=
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: SSL
sequence: 20.
CRYPTO_PKI: Ignoring match on map SSL, index 20 for
WebVPN group map
```

Figura C5: Output di un criterio di corrispondenza gruppo di certificati non riuscito

Figura C5: Output di un certificato revocato

```
n %PI=X-3-7E17t02h7a Certinf icaHtue cnhta,in faioled
uvalidation=.
CMertifiIcLa,ted ccha=inl ais eibtrhaer tin,valdid cor
=noct
oamuthori,zed.
map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map:
DefaultCertificateMap
sequence: 10.
Tunnel Group Match on map DefaultCertificateMap sequence
# 10.
Group name is CAC-USERS
CRYPTO_PKI: Checking to see if an identical cert is
already in the database...
CRYPTO_PKI: looking for cert in handle=2467668, digest=
CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI: Cert not found in database.
CRYPTO_PKI: Looking for suitable trustpoints...
CRYPTO_PKI: Found a suitable authenticated trustpoint
trustpoint0.
```

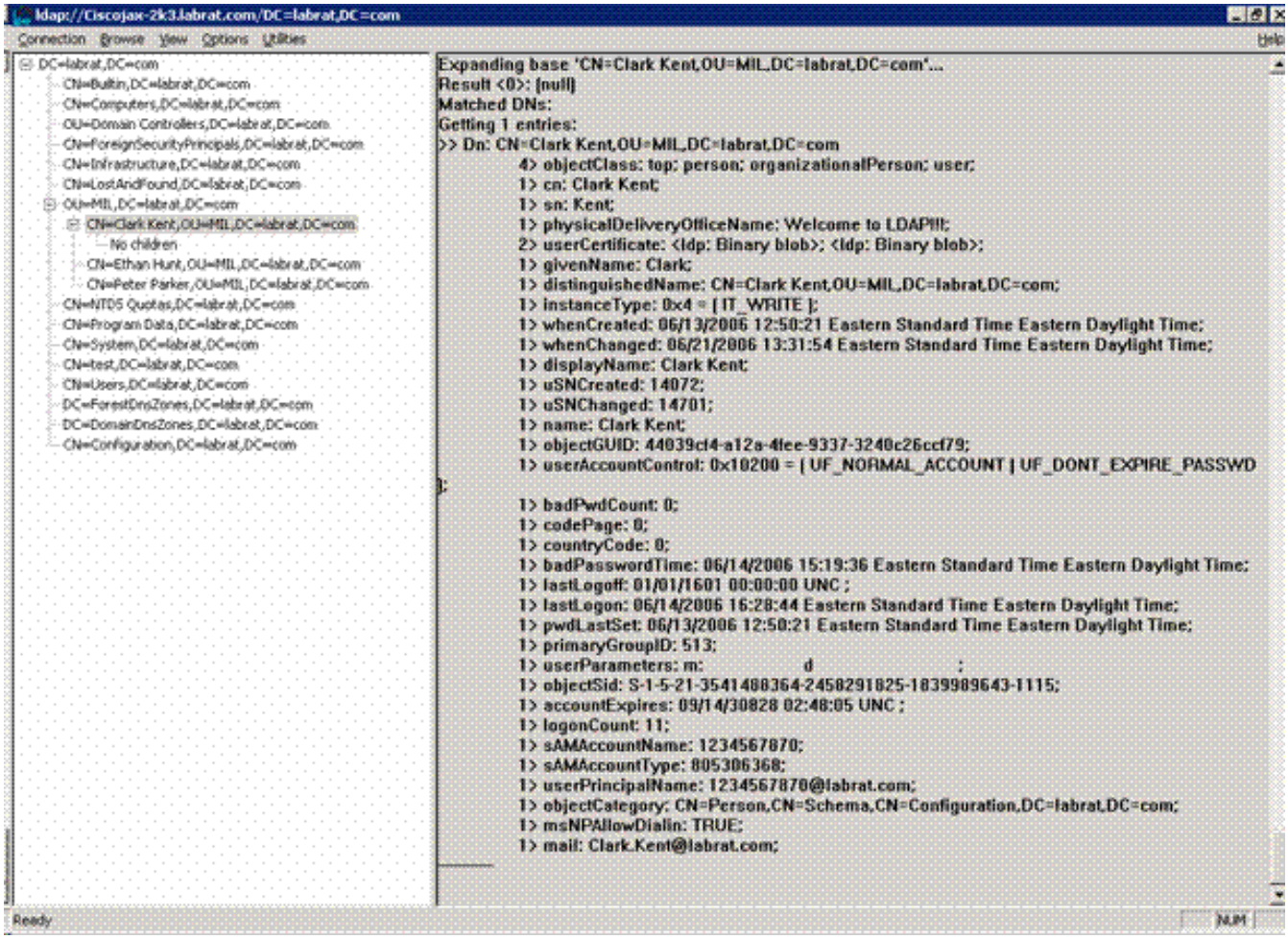
```
CRYPTO_PKI: Certificate validation: Successful, status:
0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: Attempting to find OCSP override for peer
cert: serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
Hunt,ou=MIL,dc=ggsgseclab,dc=org, issuer_name:
cn=ggsgseclab,dc=ggsgseclab,dc=org.
CRYPTO_PKI: Processing map rules for
DefaultCertificateMap.
CRYPTO_PKI: Processing map DefaultCertificateMap
sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED.
Peer cert field:
= cn=Ethan Hunt,ou=MIL,dc=ggsgseclab,dc=org, map rule:
subject-name
ne "".
CRYPTO_PKI: Peer cert has been authorized by map:
DefaultCertificateMap
sequence: 10.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://ocsp.disa.mil, Override trustpoint: OCSP
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Found a subject match
ERROR: Certificate validation failed, Certificate is
revoked, serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
Hunt,ou=MIL,dc=ggsgseclab,dc=org
CRYPTO_PKI: Certificate not validated
```

Appendice D - Verifica degli oggetti LDAP in MS

Nel CD di Microsoft Server 2003 sono disponibili strumenti aggiuntivi che è possibile installare per visualizzare la struttura LDAP nonché gli oggetti/attributi LDAP. Per installare questi strumenti, selezionare la directory **Support** nel CD, quindi **Tools** (Strumenti). Installare **SUPTOOLS.MSI**.

Visualizzatore LDAP

- Dopo l'installazione, scegliere **Start > Esegui**.
- Digitare **ldp**, quindi fare clic su **Ok**. Verrà avviato il visualizzatore LDAP.
- Scegliete **Connessione > Connetti**.
- Immettere il nome del server e fare clic su **OK**.
- Scegliete **Connessione > Binding**.
- Immettere un nome utente e una password.**Nota:** sono necessari i diritti di amministratore.
- Fare clic su **OK**.
- Visualizzare gli oggetti LDAP. Vedere la Figura D1.**Figura D1: Visualizzatore LDAP**

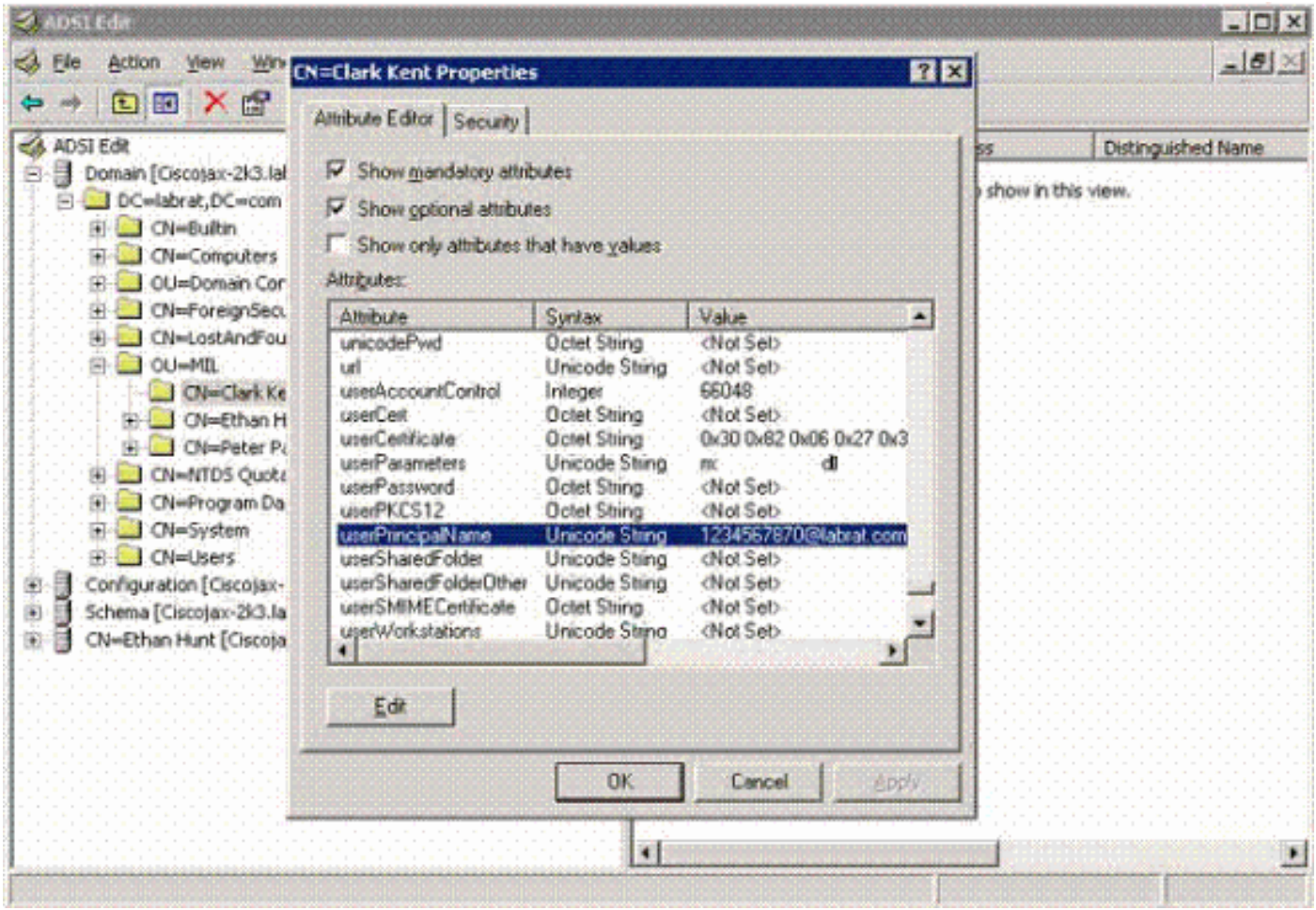


Editor interfaccia servizi Active Directory

- Nel server Active Directory scegliere **Start > Esegui**.
- Digitare **adsiedit.msc**. Verrà avviato l'editor.
- Fare clic con il pulsante destro del mouse su un oggetto e scegliere **Proprietà**.

Questo strumento mostra tutti gli attributi per oggetti specifici. Vedere la Figura D2.

Figura D2: Modifica ADSI



Appendice E

Èpossibile creare un profilo AnyConnect e aggiungerlo a una workstation. Il profilo può fare riferimento a vari valori, quali host ASA o parametri di corrispondenza certificato, ad esempio il nome distinto o l'autorità emittente. Il profilo viene archiviato come file XML e può essere modificato con Blocco note. Il file può essere aggiunto manualmente a ciascun client o inviato dall'ASA tramite un criterio di gruppo. Il file è archiviato in:

```
C:\Documents and Settings\All Users\Application Data\Cisco\Cisco
AnyConnect VPN Client\Profile
```

Attenersi alla seguente procedura:

1. Scegliere AnyConnectProfile.tmpl e aprire il file con il Blocco note.
2. Apportare le modifiche appropriate al file, ad esempio emittente o IP host. Vedere la Figura F1 per esempio.
3. Al termine, salvare il file in formato .xml.

Questo è un esempio di file XML di Cisco AnyConnect VPN Client Profile.

Per la gestione dei profili, consultare la documentazione di Cisco AnyConnect. In breve:

- Un Profilo deve avere un nome univoco per la tua Azienda. Un esempio è: CiscoProfile.xml
- Il nome del profilo deve essere lo stesso anche se diverso per ogni singolo gruppo all'interno della società.

Questo file deve essere gestito da un amministratore Secure Gateway e quindi distribuito con il software client. Il profilo basato su questo XML può essere distribuito ai client in qualsiasi

momento. I meccanismi di distribuzione supportati sono come file in bundle con la distribuzione del software o come parte del meccanismo di download automatico. Il meccanismo di download automatico è disponibile solo con alcuni prodotti Cisco Secure Gateway.

Nota: si consiglia agli amministratori di convalidare il profilo XML creato utilizzando uno strumento di convalida in linea o la funzionalità di importazione dei profili in ASDM. Per eseguire la convalida, usare il file AnyConnectProfile.xsd che si trova in questa directory. AnyConnectProfile è l'elemento radice che rappresenta AnyConnect Client Profile.

```
xml version="1.0" encoding="UTF-8"
- -




!--- The ClientInitialization section represents global
settings !--- for the client. In some cases, for
example, BackupServerList, host specific !--- overrides
are possible. !-- --> -




!--- The Start Before Logon feature can be used to
activate !--- the VPN as part of the logon sequence. !--
- UserControllable: Does the administrator of this
profile allow the user !--- to control this attribute
for their own use. Any user setting !--- associated with
this attribute is stored elsewhere. -->




!--- This control enables an administrator to have a one
time !--- message displayed prior to a users first
connection attempt. As an !--- example, the message can
be used to remind a user to insert their smart !--- card
into its reader. !--- The message to be used with this
control is localizable and can be !--- found in the
AnyConnect message catalog. !--- (default: "This is a
pre-connect reminder message.")




!-- This section enables the definition of various
attributes !--- that can be used to refine client
certificate selection. --> -




!--- Certificate Distinguished Name matching allows for
exact !--- match criteria in the choosing of acceptable
```

```
client !--- certificates. -




- !-- This section contains the list of hosts from which
!--- the user is able to select. -




!--- This is the data needed to attempt a connection to
a specific !--- host. --> -


          -
```

Informazioni correlate

- Certificati e CRL specificati da X.509 e RFC 3280
- OCSP specificato da RFC 2560
- Introduzione all'infrastruttura a chiave pubblica
- "OCSP leggero" profilato da bozza standard
- SSL/TLS specificato da RFC 2246
- Documentazione e supporto tecnico – Cisco Systems