ASA 8.x: AnyConnect SSL VPN CAC-SmartCards-Konfiguration für Windows

Inhalt

Einleitung

Dieses Dokument enthält eine Beispielkonfiguration auf der Cisco Adaptive Security Appliance (ASA) für den AnyConnect VPN-Remote-Zugriff unter Windows mit der Common Access Card (CAC) für die Authentifizierung.

In diesem Dokument wird die Konfiguration der Cisco ASA mit Adaptive Security Device Manager (ASDM), Cisco AnyConnect VPN Client und Microsoft Active Directory (AD)/Lightweight Directory Access Protocol (LDAP) behandelt.

Für die Konfiguration in diesem Leitfaden wird der Microsoft AD/LDAP-Server verwendet. Darüber hinaus werden in diesem Dokument erweiterte Funktionen wie OCSP, LDAP-Attributzuordnungen und Dynamic Access Polices (DAP) behandelt.

Voraussetzungen

Anforderungen

Grundlegende Kenntnisse der Cisco ASA, des Cisco AnyConnect Client, von Microsoft AD/LDAP und der Public Key Infrastructure (PKI) sind für das Verständnis der vollständigen Einrichtung von Vorteil. Die Kenntnis der AD-Gruppenmitgliedschaft, der Benutzereigenschaften sowie der LDAP-Objekte hilft bei der Korrelation des Autorisierungsprozesses zwischen Zertifikatattributen und AD/LDAP-Objekten.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Adaptive Security Appliance (ASA) der Serie 5500 mit Softwareversion 8.0(x) oder höher

- Cisco Adaptive Security Device Manager (ASDM) Version 6.x für ASA 8.x
- Cisco AnyConnect VPN-Client für Windows

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Cisco ASA-Konfiguration

In diesem Abschnitt wird die Konfiguration der Cisco ASA über ASDM beschrieben. Es beschreibt die erforderlichen Schritte zur Bereitstellung eines VPN-Remote-Zugriffstunnels über eine SSL AnyConnect-Verbindung. Das CAC-Zertifikat wird für die Authentifizierung verwendet, und das UPN-Attribut (User Principal Name) des Zertifikats wird zur Autorisierung in Active Directory eingefügt.

Überlegungen zur Bereitstellung

- Grundlegende Konfigurationen wie Schnittstellen, DNS, NTP, Routing, Gerätezugriff, ASDM-Zugriff usw. werden in diesem Leitfaden NICHT behandelt. Es wird davon ausgegangen, dass der Netzwerkbetreiber mit diesen Konfigurationen vertraut ist.

  Weitere Informationen finden Sie unter Multifunction Security Appliances.

- Die ROT hervorgehobenen Abschnitte stellen obligatorische Konfigurationen für den grundlegenden VPN-Zugriff dar. So kann beispielsweise ein VPN-Tunnel mit der CAC-Karte eingerichtet werden, ohne dass OCSP-Prüfungen, LDAP-Zuordnungen und Dynamic Access Policy (DAP)-Prüfungen durchgeführt werden müssen. DoD erfordert OCSP-Prüfung, der Tunnel funktioniert jedoch ohne konfigurierten OCSP.
- Bei den blau hervorgehobenen Abschnitten handelt es sich um erweiterte Funktionen, die hinzugefügt werden können, um das Design sicherer zu machen.
- ASDM und AnyConnect/SSL VPN können nicht dieselben Ports auf derselben Schnittstelle verwenden. Es wird empfohlen, die Ports auf dem einen oder anderen Port zu ändern, um Zugriff zu erhalten. Verwenden Sie beispielsweise Port 445 für ASDM und 443 für AC/SSL VPN. Der ASDM-URL-Zugriff hat sich in 8.x geändert. Verwenden Sie `https://<ip_address>:<port>/admin.html`.
- Erforderliches ASA-Image ist mindestens 8.0.2.19 und ASDM 6.0.2.
- AnyConnect/CAC wird von Vista unterstützt.
- In Anhang A finden Sie Beispiele für die Zuordnung von LDAP- und dynamischen Zugriffsrichtlinien für eine zusätzliche Richtliniendurchsetzung.
- Wie LDAP-Objekte in MS geprüft werden, wird in Anhang D beschrieben.

- Eine Liste der Anwendungsports für die Firewall-Konfiguration finden Sie unter Zugehörige Informationen.

Konfiguration für Authentifizierung, Autorisierung, Abrechnung (AAA)

Sie werden mit der Verwendung des Zertifikats in ihrer Common Access Card (CAC) über den DISACertificate Authority (CA) Server oder den CA Server ihrer eigenen Organisation authentifiziert. Das Zertifikat muss für den Remote-Zugriff auf das Netzwerk gültig sein. Neben der Authentifizierung müssen Sie auch zur Verwendung eines Microsoft Active Directory- oder Lightweight Directory Access Protocol (LDAP)-Objekts autorisiert sein. Für das US-Verteidigungsministerium (DoD) ist die Verwendung des UPN-Attributs (User Principal Name) zur Autorisierung erforderlich, das Teil des SAN-Abschnitts (Subject Alternative Name) des Zertifikats ist. UPN oder EDI/PI muss das folgende Format haben: 1234567890@mil. Diese Konfigurationen zeigen, wie ein AAA-Server auf dem ASA-Gerät mit einem LDAP-Server für die Autorisierung konfiguriert wird. Weitere Informationen zur Konfiguration der LDAP-Objektzuordnung finden Sie in Anhang A.

LDAP-Server konfigurieren

Führen Sie diese Schritte aus:

1. Wählen Sie Remote Access VPN > AAA Setup > AAA Server Group.
2. Klicken Sie in der Tabelle "AAA-Servergruppen" auf Hinzufügen 3.
3. Geben Sie den Namen der Servergruppe ein, und wählen Sie im Protokoll-Optionsfeld LDAP aus. Siehe Abbildung 1.
4. Klicken Sie in der ausgewählten Gruppentabelle unter Server auf Hinzufügen. Stellen Sie sicher, dass der von Ihnen erstellte Server in der vorherigen Tabelle hervorgehoben ist.
5. Führen Sie im Fenster "AAA-Server bearbeiten" die folgenden Schritte aus. Siehe Abbildung 2.

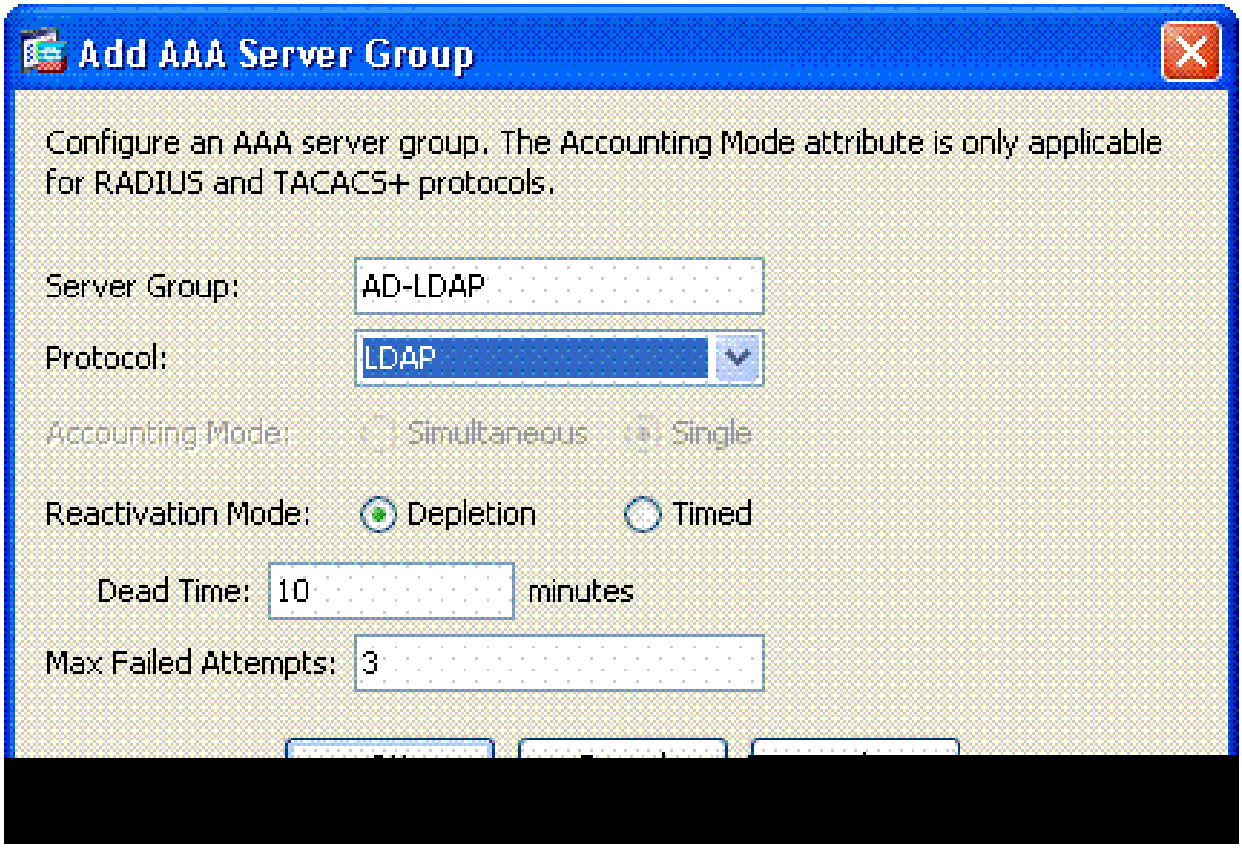
Hinweis: Wählen Sie die Option LDAP über SSL aktivieren, wenn Ihr LDAP/AD für diesen Verbindungstyp konfiguriert ist.

---

   a. Wählen Sie die Schnittstelle aus, in der sich das LDAP befindet. Dieses Handbuch wird in der Benutzeroberfläche angezeigt.
   b. Geben Sie die IP-Adresse des Servers ein.
   c. Geben Sie den Serverport ein. Der standardmäßige LDAP-Port ist 389.
   d. Wählen Sie den Servertyp aus.

e. Geben Sie die Basis-DN ein. Fragen Sie Ihren AD/LDAP-Administrator nach diesen Werten.

Abbildung 1



f. Wählen Sie unter der Bereichsoption die entsprechende Antwort aus. Dies hängt von der Basis-DN ab. Wenden Sie sich an Ihren AD/LDAP-Administrator.

g. Geben Sie im naming-Attribut userPrincipalName ein. Dies ist das Attribut, das für die Benutzerautorisierung im AD/LDAP-Server verwendet wird.

h. Geben Sie in den Anmelde-DN den Administrator-DN ein.

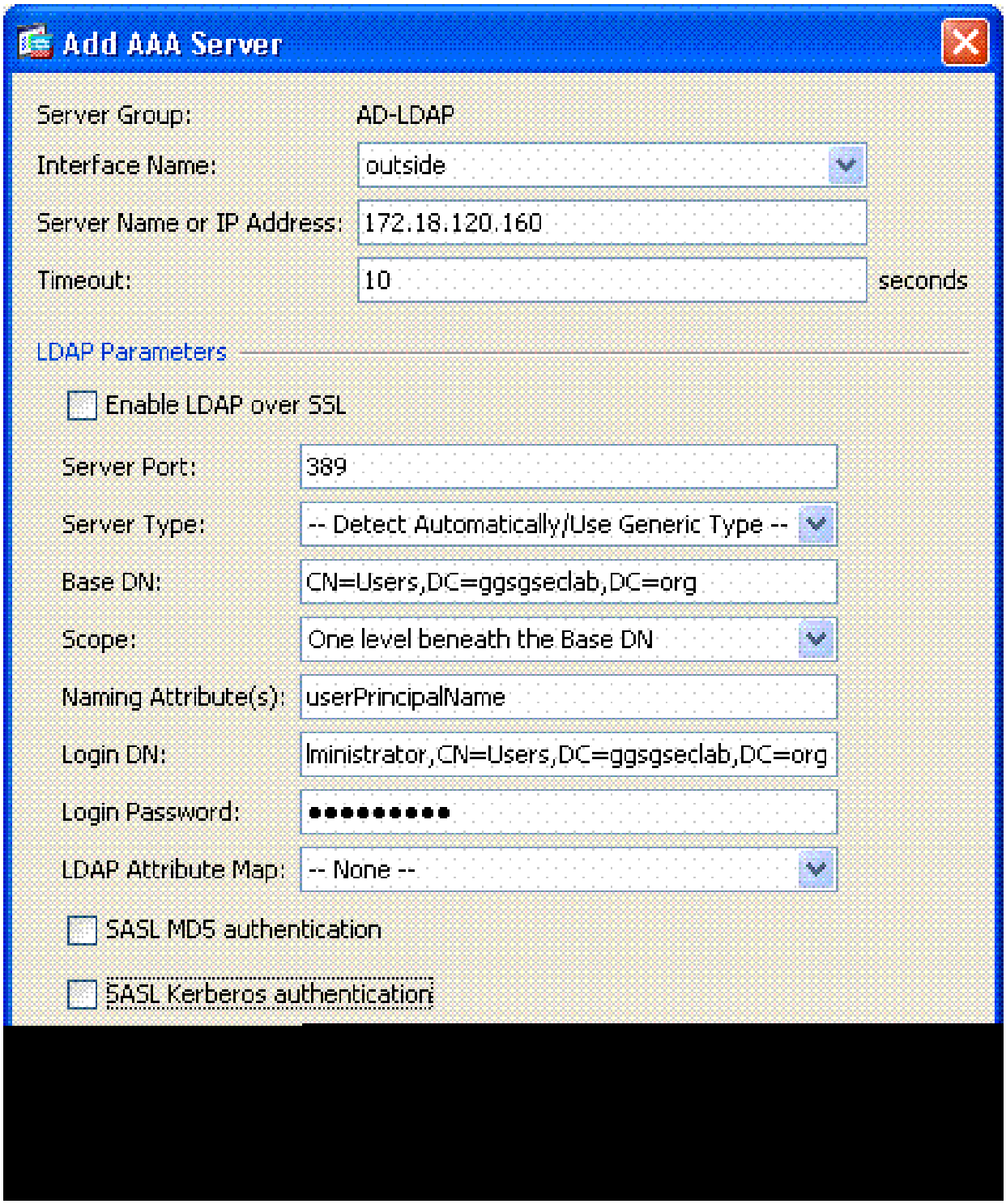
Hinweis: Sie verfügen über administrative Rechte oder Rechte zum Anzeigen/Durchsuchen der LDAP-Struktur, die Benutzerobjekte und Gruppenmitgliedschaften enthält.

---

i. Geben Sie im Feld Login Password (Anmeldungskennwort) das Kennwort des Administrators ein.

j. Lassen Sie das LDAP-Attribut auf none (kein).

Abbildung 2



> Hinweis: Sie verwenden diese Option später in der Konfiguration, um weitere AD/LDAP-Objekte zur Autorisierung hinzuzufügen.

k. Wählen Sie OK.

6. Wählen Sie OK.

Verwalten von Zertifikaten

Es gibt zwei Schritte, um Zertifikate auf der ASA zu installieren. Installieren Sie zunächst die

erforderlichen Zertifizierungsstellenzertifikate (Stamm- und untergeordnete Zertifizierungsstelle). Anschließend registrieren Sie die ASA bei einer bestimmten Zertifizierungsstelle und erhalten das Identitätszertifikat. Die DoD PKI nutzt diese Zertifikate, Root CA2, Class 3 Root, CA##, Intermediate, bei denen die ASA registriert ist, ASA ID-Zertifikat und OCSP-Zertifikat. Wenn Sie OCSP jedoch nicht verwenden, muss das OCSP-Zertifikat nicht installiert werden.

Hinweis: Wenden Sie sich an Ihren Sicherheits-POC, um Stammzertifikate sowie Anweisungen zur Anmeldung für ein Identitätszertifikat für ein Gerät zu erhalten. Ein SSL-Zertifikat sollte für die ASA für den Remote-Zugriff ausreichen. Ein Dual-SAN-Zertifikat ist nicht erforderlich.

Hinweis: Auf dem lokalen Computer muss auch die DoD-CA-Kette installiert sein. Die Zertifikate können im Microsoft Zertifikatspeicher mit Internet Explorer angezeigt werden. DoD hat eine Batch-Datei erstellt, die automatisch alle CAs zum Computer hinzufügt. Fragen Sie Ihren PKI POC nach weiteren Informationen.

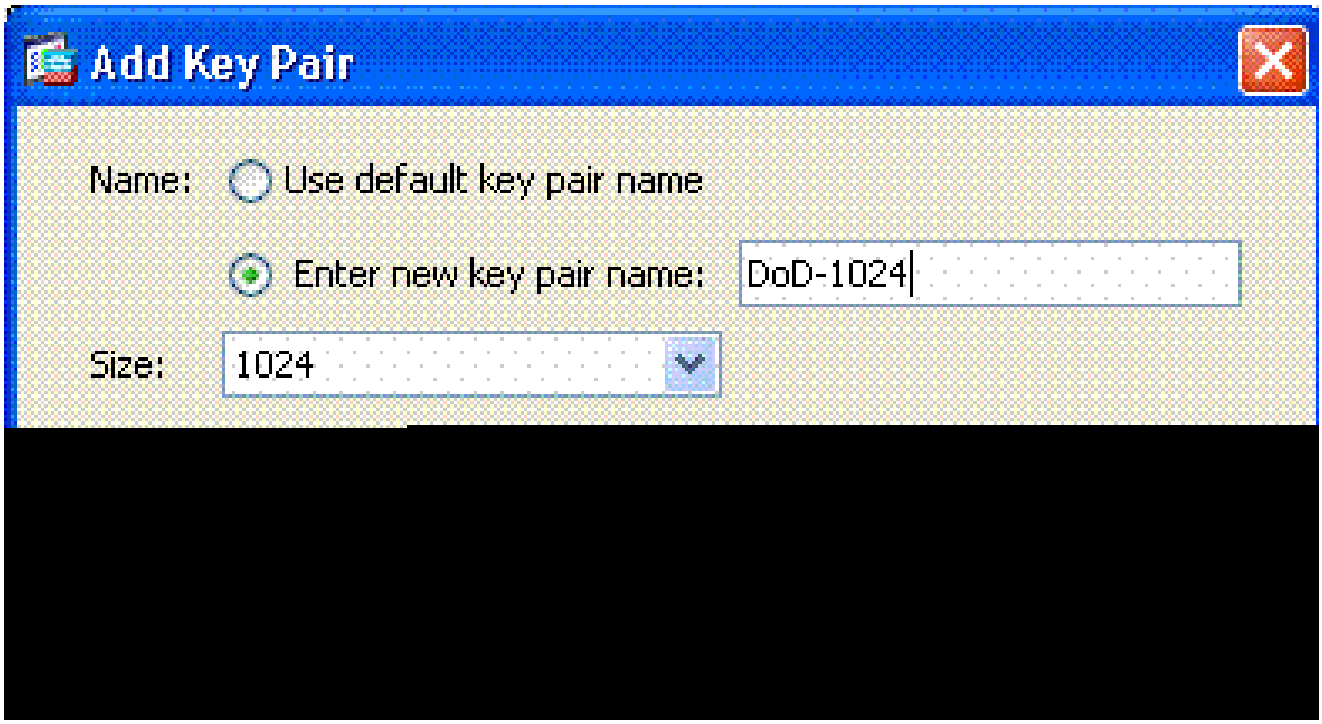
Hinweis: CA2- und Class 3-Root für das DoD sowie die ASA-ID und das CA Intermediate, die das ASA-Zertifikat ausgestellt haben, sollten die einzigen CAs sein, die für die Benutzerauthentifizierung benötigt werden. Alle aktuellen CA-Zwischenprodukte fallen in die CA2- und Class 3-Root-Kette und gelten als vertrauenswürdig, solange CA2- und Class 3-Roots hinzugefügt werden.

Schlüssel generieren

Führen Sie diese Schritte aus:

1. Wählen Sie Remote Access VPN > Certificate Management > Identity Certificate > Add.
2. Wählen Sie Add a new id certificate (Neues ID-Zertifikat hinzufügen) und dann New by the key pair option (Neu durch Schlüsselpaar) aus.
3. Geben Sie im Fenster Schlüsselpaar hinzufügen den Schlüsselnamen DoD-1024 ein. Klicken Sie auf das Radio, um einen neuen Schlüssel hinzuzufügen. Siehe Abbildung 3.

   Abbildung 3



4. Wählen Sie die Größe des Schlüssels.
5. Halten Sie die Nutzung auf General Purpose.
6. Klicken Sie auf Jetzt generieren.

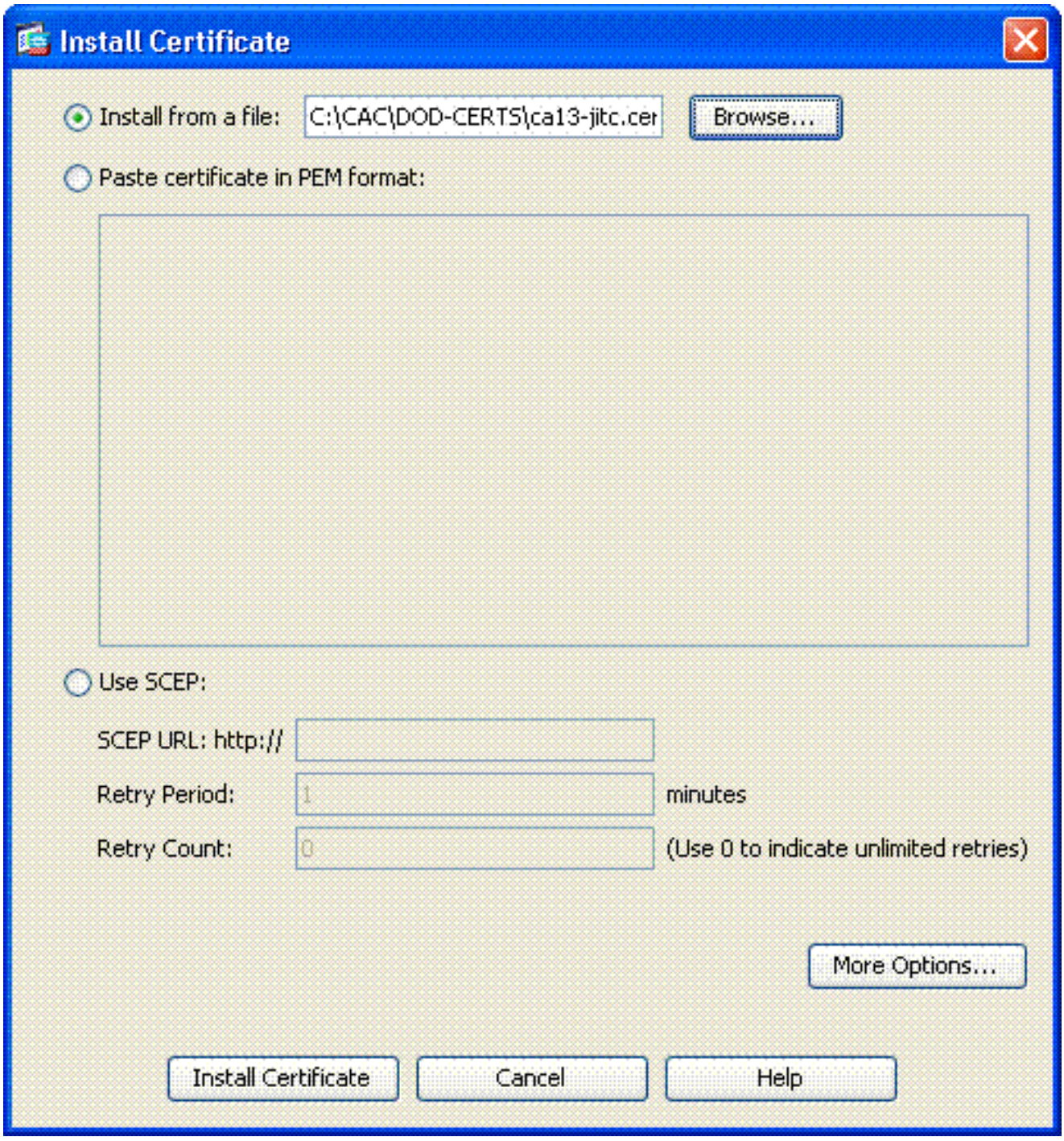
Hinweis: Die DoD-Root-CA 2 verwendet einen 2048-Bit-Schlüssel. Ein zweiter Schlüssel, der ein 2048-Bit-Schlüsselpaar verwendet, sollte generiert werden, um diese CA verwenden zu können. Führen Sie die oben genannten Schritte aus, um einen zweiten Schlüssel hinzuzufügen.

Installieren von Zertifikaten der Stammzertifizierungsstelle

Führen Sie diese Schritte aus:

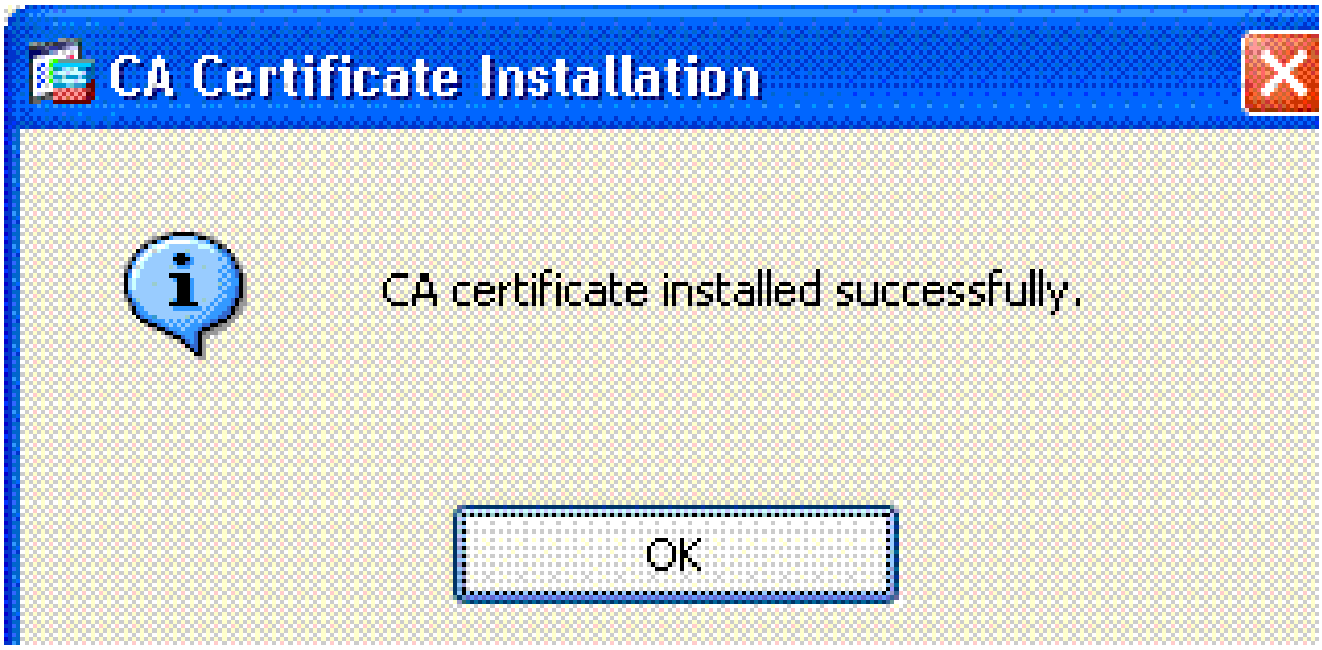
1. Wählen Sie Remote Access VPN > Certificate Management > CA Certificate > Add aus.
2. Wählen Sie Install from File (Von Datei installieren) aus, und navigieren Sie zum Zertifikat.
3. Wählen Sie Zertifikat installieren aus.

Abbildung 4: Installieren des Stammzertifikats



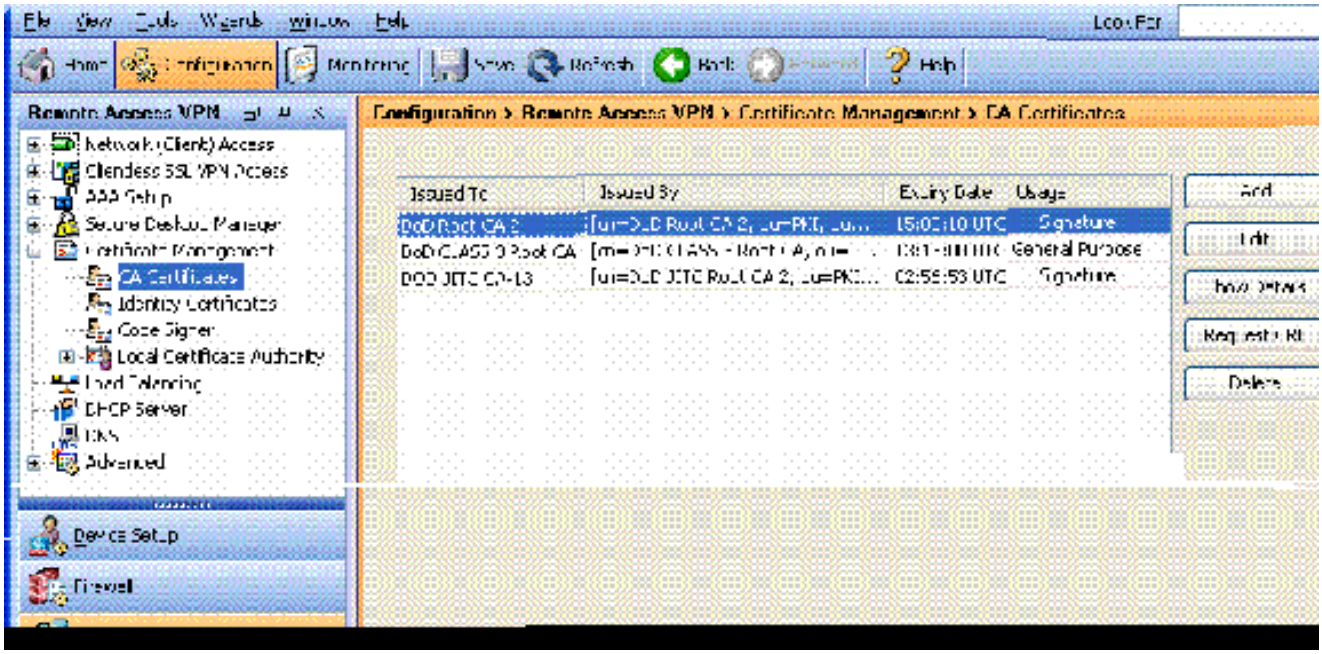
4. Dieses Fenster sollte angezeigt werden. Siehe Abbildung 5.

Abbildung 5



Hinweis: Wiederholen Sie die Schritte 1 bis 3 für jedes Zertifikat, das Sie installieren möchten. Für die DoD PKI ist jeweils ein Zertifikat erforderlich: Root CA 2, Class 3 Root, CA## Intermediate, ASA ID und OCSP-Server. Das OCSP-Zertifikat wird nicht benötigt, wenn Sie OCSP nicht verwenden.

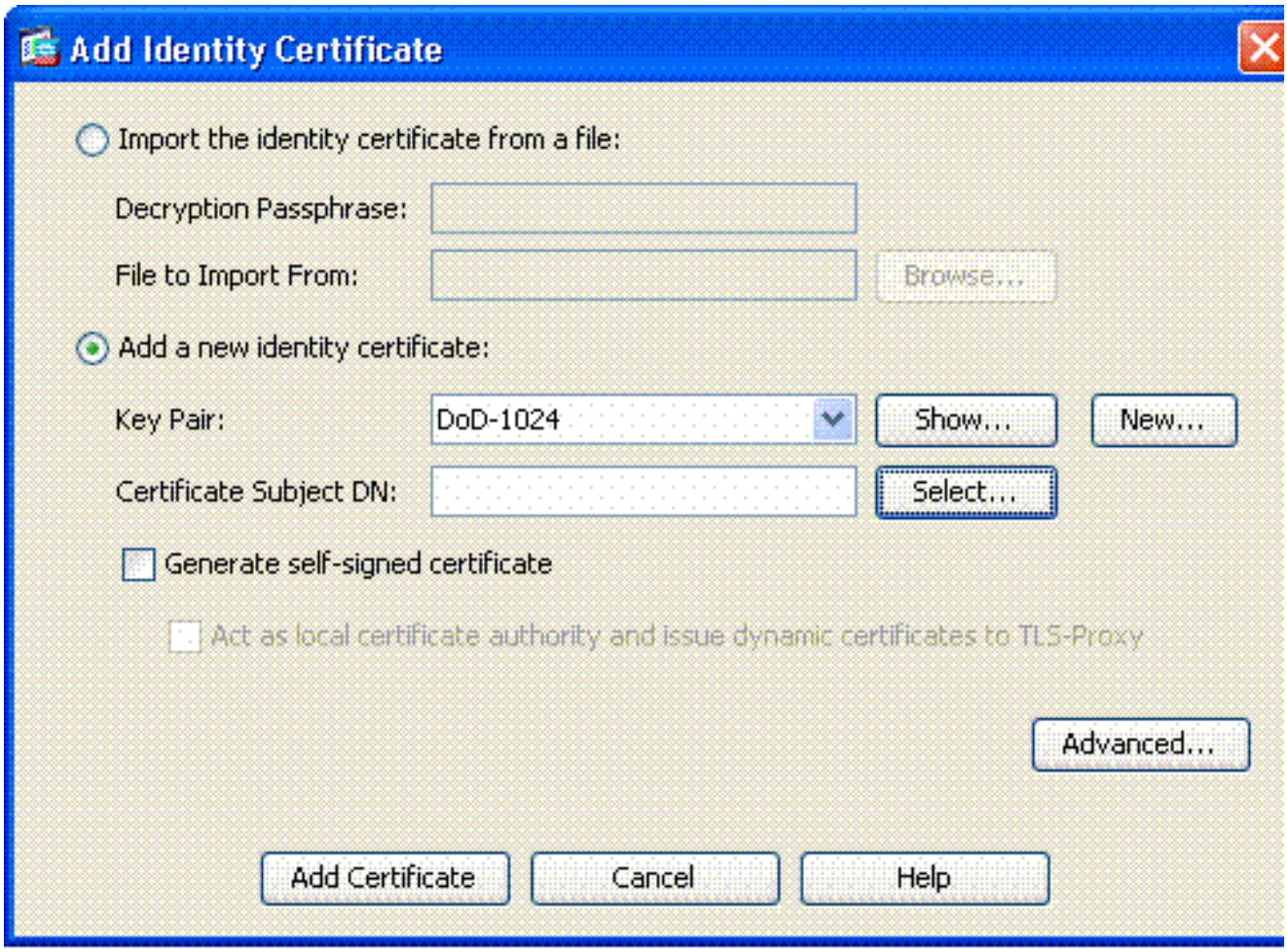
Abbildung 6: Installieren des Stammzertifikats



ASA registrieren und Identitätszertifikat installieren

1. Wählen Sie Remote Access VPN > Certificate Management > Identity Certificate > Add.
2. Wählen Sie Neues ID-Zertifikat hinzufügen aus.
3. Wählen Sie das DoD-1024 Schlüsselpaar aus. Siehe Abbildung 7

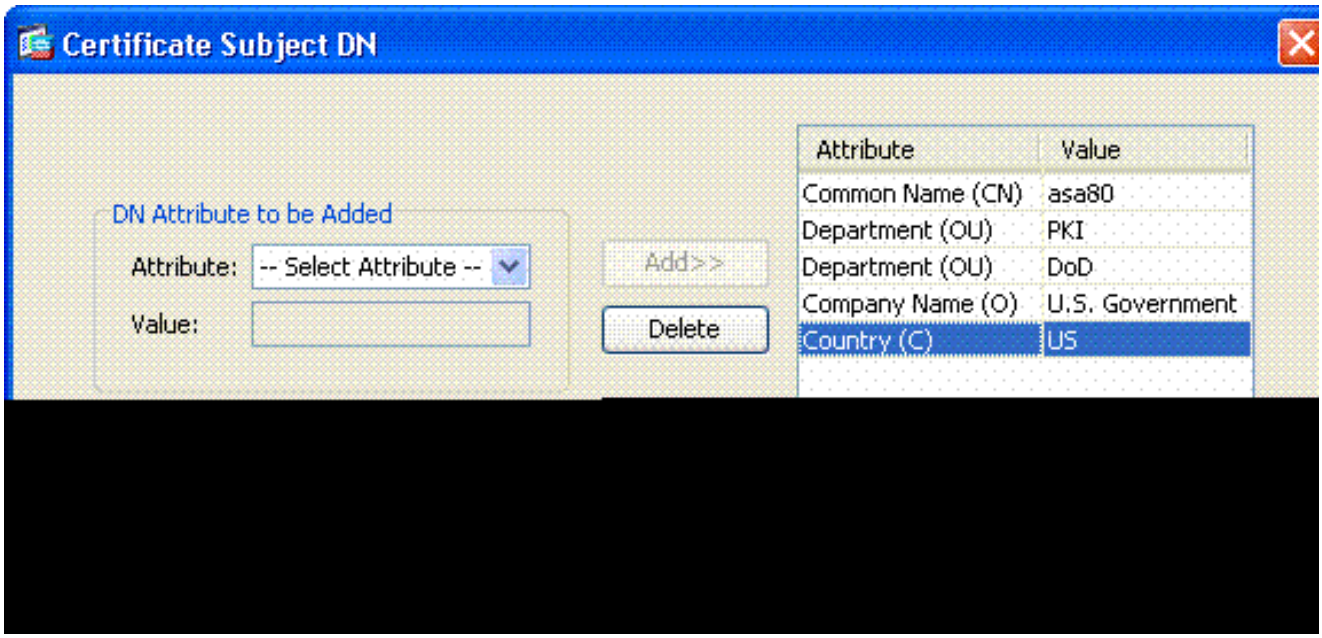
Abbildung 7: Identitätszertifikatparameter



4. Wechseln Sie zum Feld Zertifikatantragsteller-DN, und klicken Sie auf Auswählen.

5. Geben Sie im Fenster Zertifikatantragsteller-DN die Informationen zum Gerät ein. Siehe zum Beispiel Abbildung 8.

Abbildung 8: DN bearbeiten



6. Wählen Sie OK.

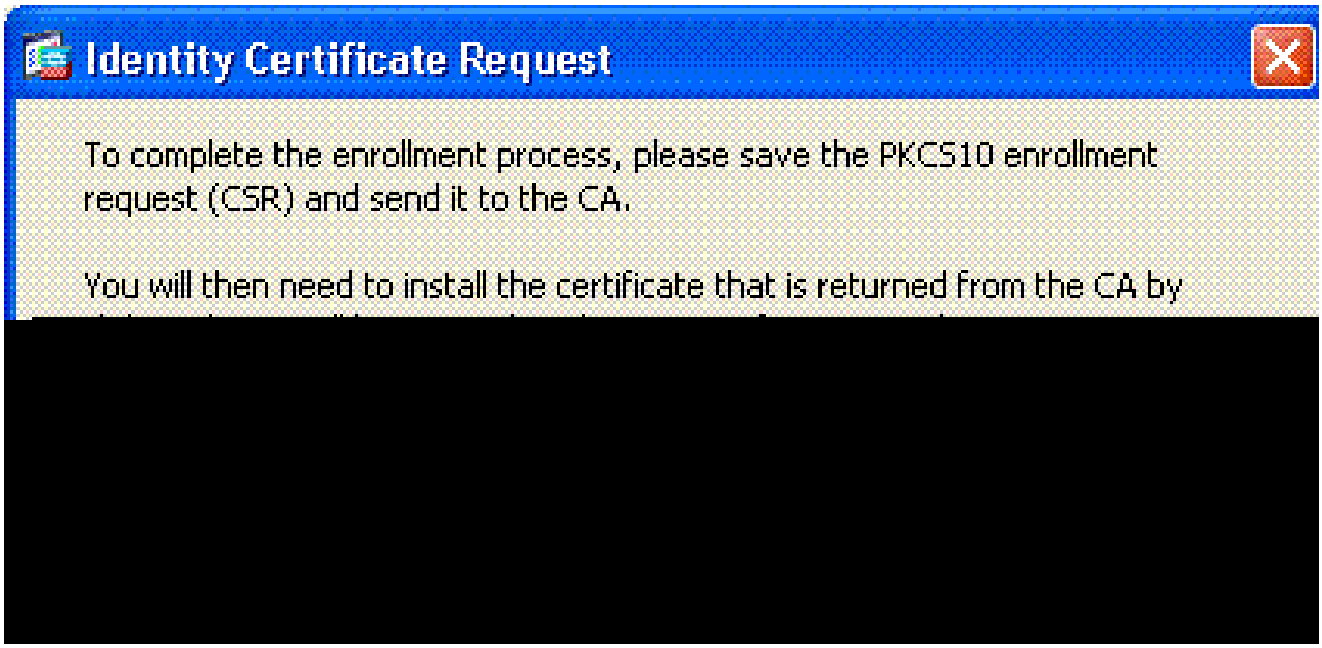
Hinweis: Achten Sie darauf, dass Sie den Hostnamen des Geräts verwenden, das in Ihrem System konfiguriert ist, wenn Sie die Betreff-DN hinzufügen. Der PKI-Verbindungspunkt zeigt Ihnen die erforderlichen Pflichtfelder an.

---

7. Wählen Sie Zertifikat hinzufügen aus.

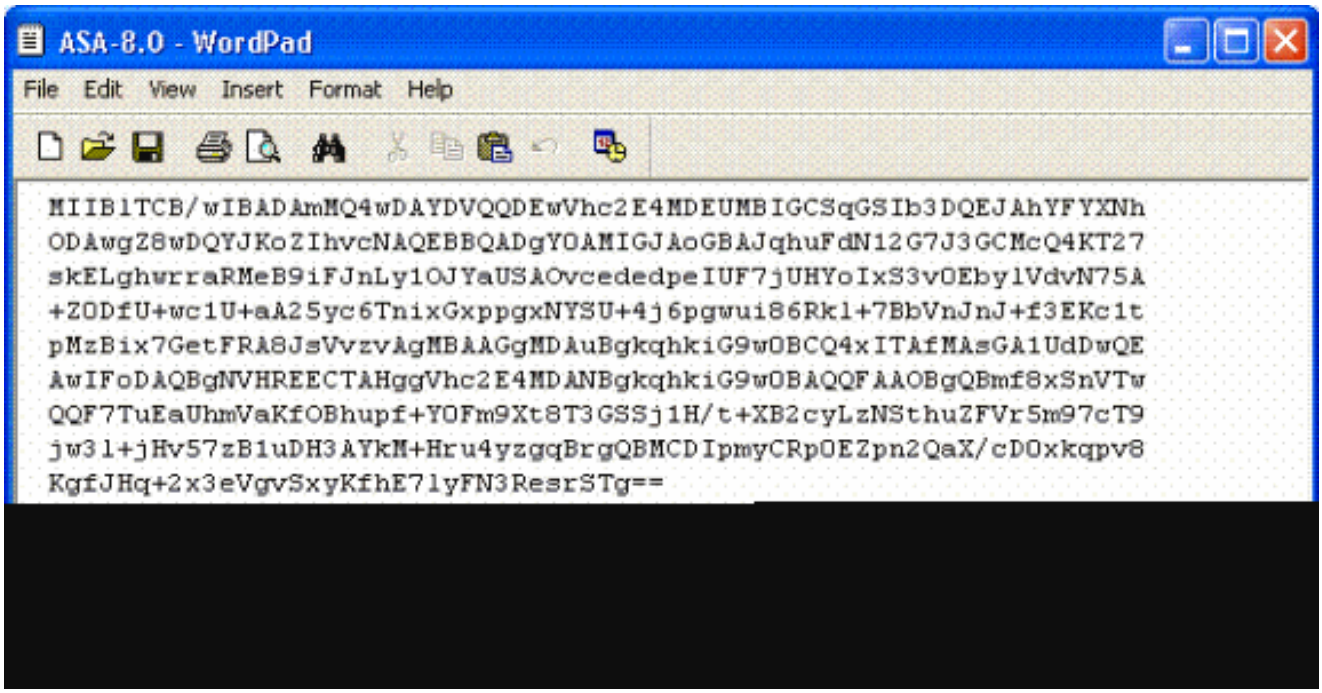
8. Klicken Sie auf Durchsuchen, um das Verzeichnis auszuwählen, in dem Sie die Anforderung speichern möchten. Siehe Abbildung 9.

   Abbildung 9: Zertifikatanforderung



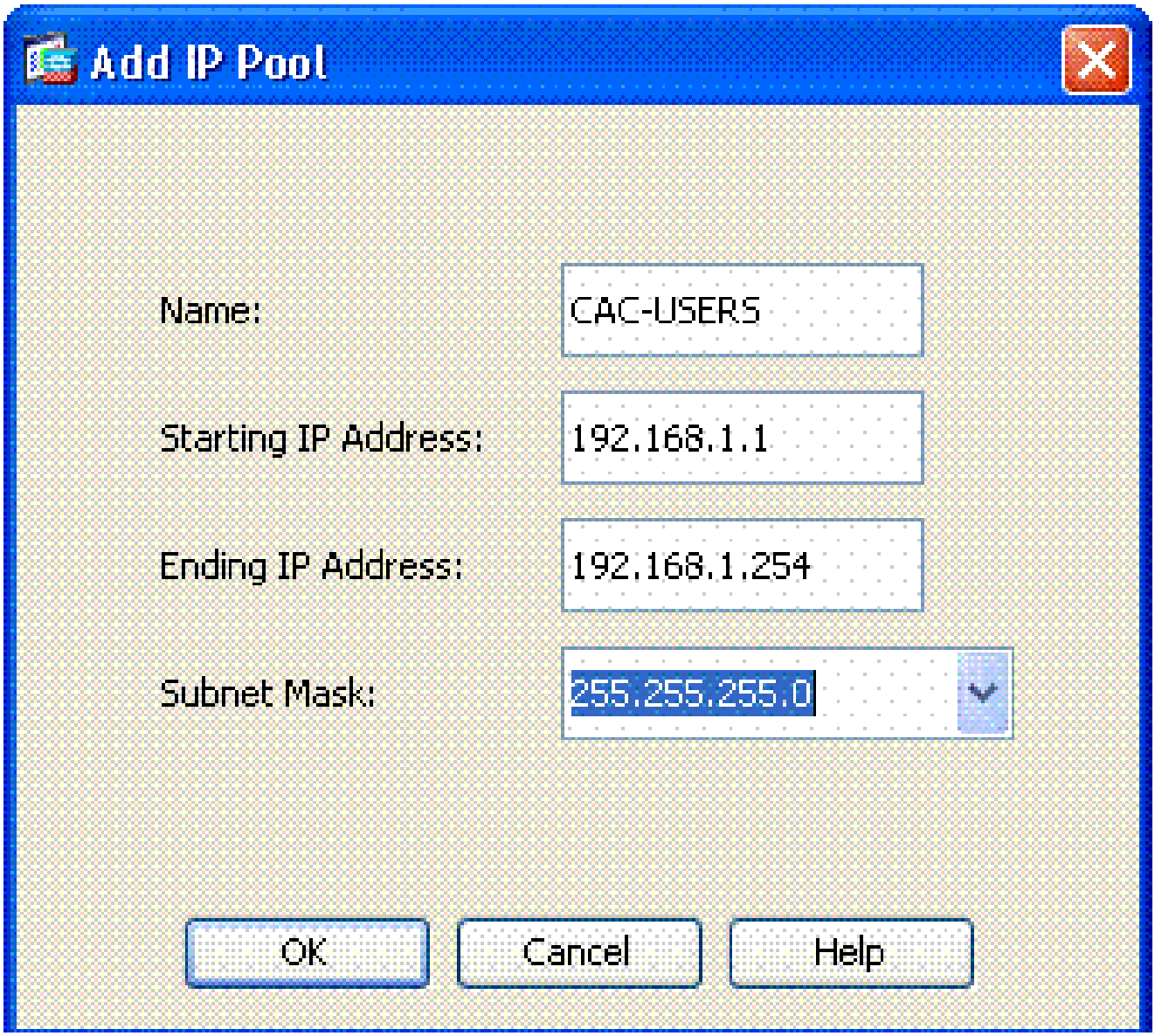
9. Öffnen Sie die Datei mit WordPad, kopieren Sie die Anforderung in die entsprechende Dokumentation, und senden Sie sie an Ihren PKI POC. Siehe Abbildung 10.

   Abbildung 10: Anmeldeantrag



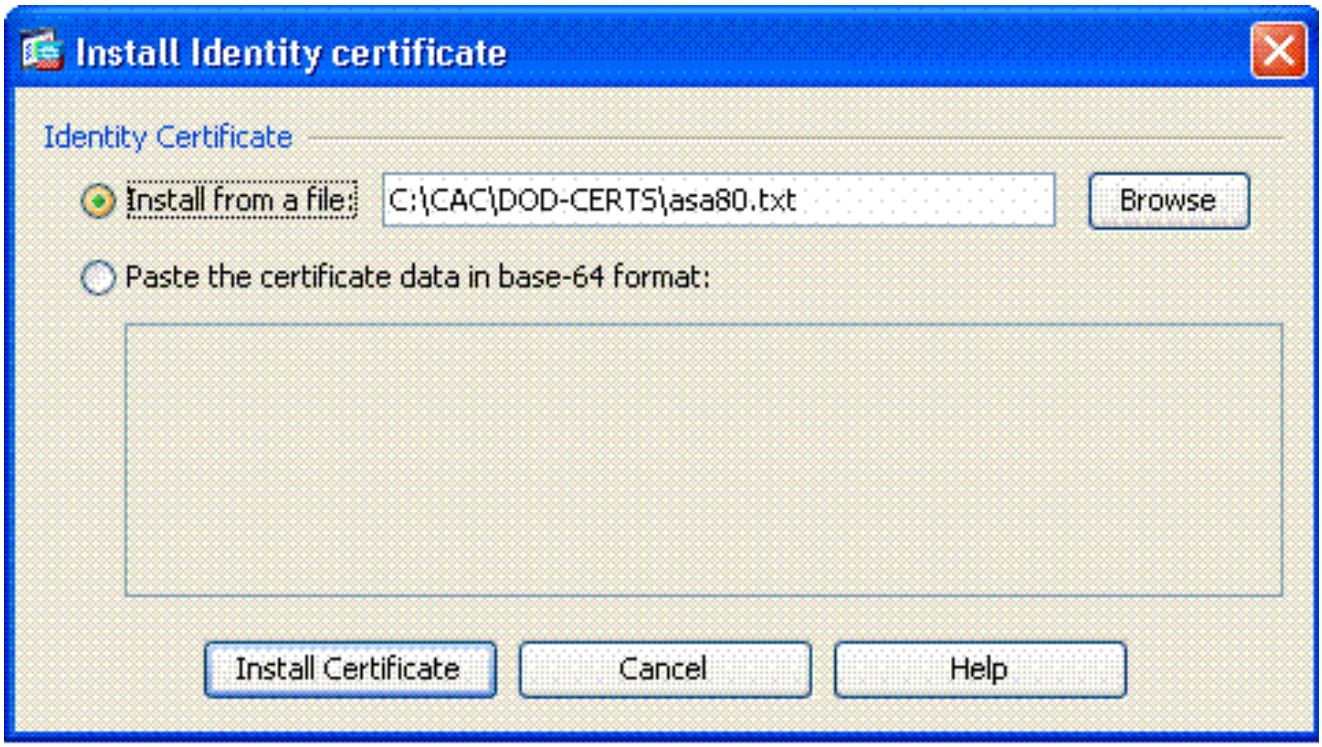
10. Wenn Sie das Zertifikat vom CA-Administrator erhalten haben, wählen Sie Remote Access VPN > Certificate Management > ID Certificate > Install aus. Siehe Abbildung 11.

    Abbildung 11: Importieren des Identitätszertifikats



11. Navigieren Sie im Fenster Zertifikat installieren zum ID-Zertifikat, und wählen Sie Zertifikat installieren aus. Siehe zum Beispiel Abbildung 12.

    Abbildung 12: Installieren des Identitätszertifikats



Hinweis: Es wird empfohlen, den ID-Zertifikat-Vertrauenspunkt zu exportieren, um das ausgestellte Zertifikat und die Schlüsselpaare zu speichern. Auf diese Weise kann der ASA-Administrator das Zertifikat und die Schlüsselpaare im Falle einer RMA oder eines Hardwarefehlers in eine neue ASA importieren. Weitere Informationen finden Sie unter Exportieren und Importieren von Vertrauenspunkten.

Hinweis: Klicken Sie auf SPEICHERN, um die Konfiguration im Flash-Speicher zu speichern.

AnyConnect VPN-Konfiguration

Zur Konfiguration der VPN-Parameter in ASDM stehen zwei Optionen zur Verfügung. Die erste Option ist der SSL VPN-Assistent. Dies ist ein benutzerfreundliches Tool für Benutzer, die noch nicht mit der VPN-Konfiguration vertraut sind. Die zweite Option besteht darin, dies manuell zu tun und jede Option einzeln durchzugehen. In diesem Konfigurationsleitfaden wird die manuelle Methode verwendet.

Hinweis: Es gibt zwei Methoden, um den AC-Client an den Benutzer zu senden:

1. Sie können den Client von der Cisco Website herunterladen und auf dem Computer installieren.
2. Der Benutzer kann über einen Webbrowser auf die ASA zugreifen, und der Client kann heruntergeladen werden.

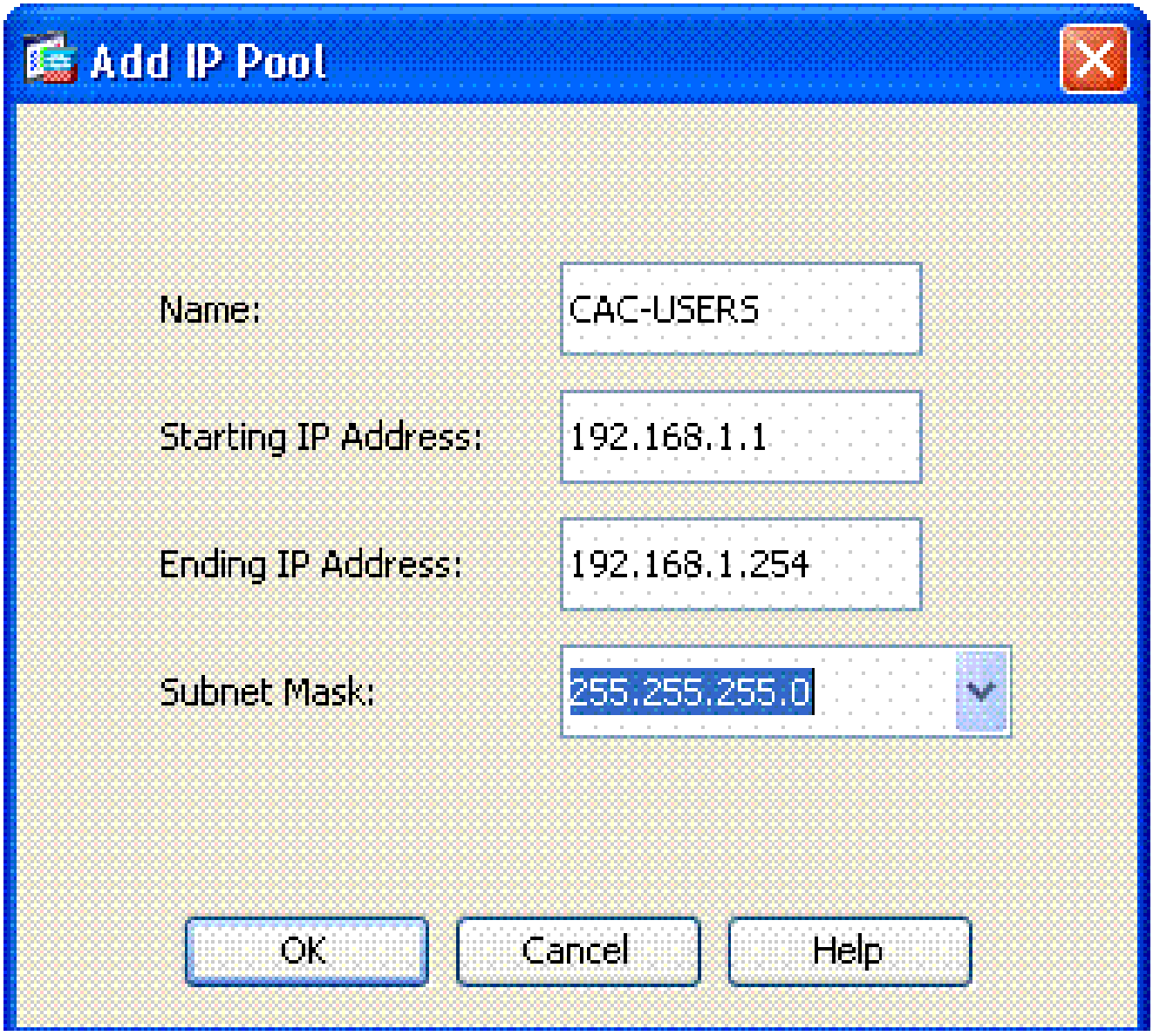
Hinweis: Beispiel: https://asa.test.com. In diesem Leitfaden wird die zweite Methode verwendet. Sobald der AC-Client dauerhaft auf dem Client-Computer installiert ist, starten Sie den AC-Client einfach über die Anwendung.

Erstellen eines IP-Adresspools

Dies ist optional, wenn Sie eine andere Methode wie DHCP verwenden.

1. Wählen Sie Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools aus.
2. Klicken Sie auf Hinzufügen.
3. Geben Sie im Fenster Add IP Pool (IP-Pool hinzufügen) den Namen des IP-Pools sowie die Start- und End-IP-Adresse ein, und wählen Sie eine Subnetzmaske. Siehe Abbildung 13.

   Abbildung 13: Hinzufügen eines IP-Pools

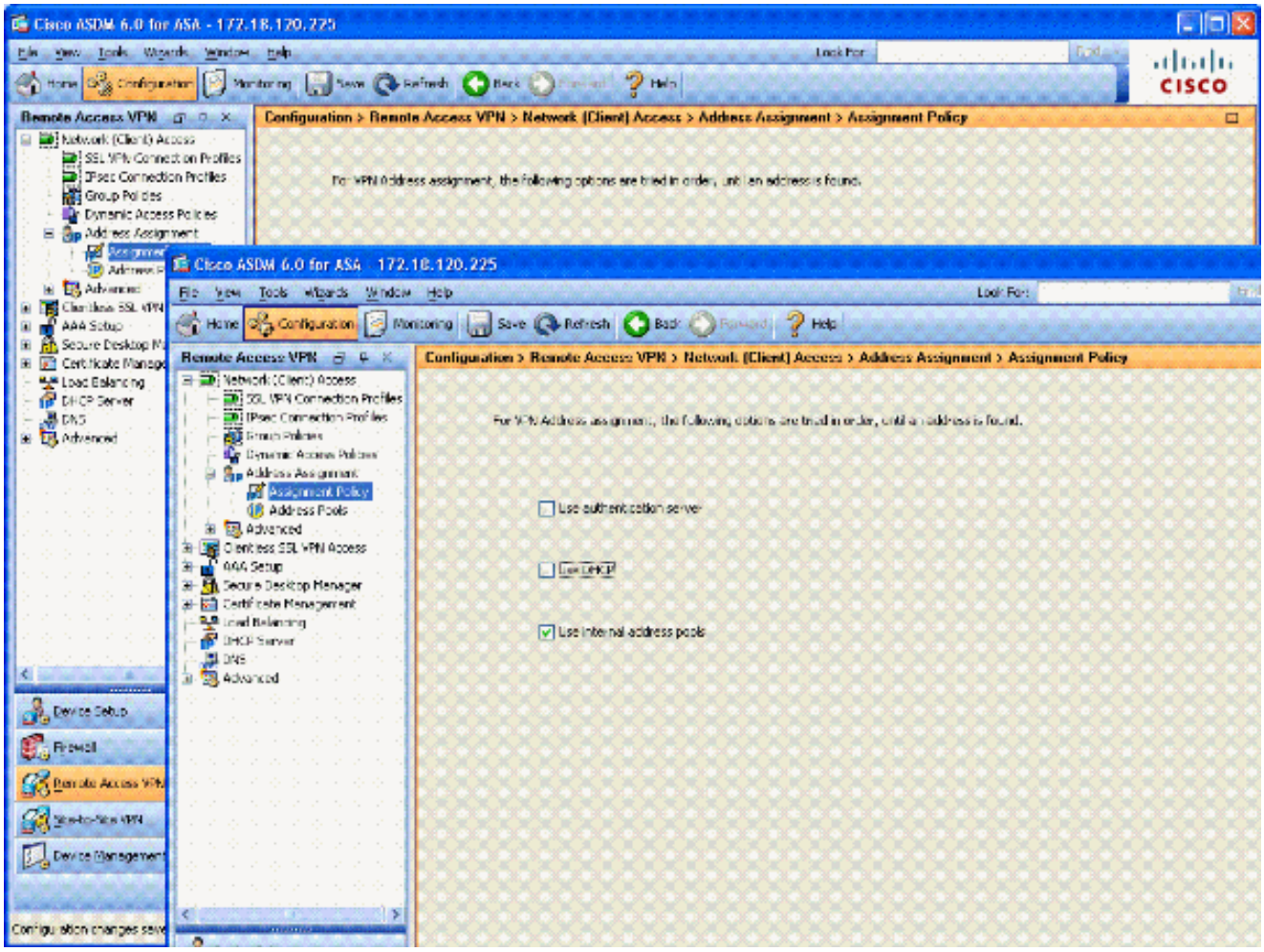


4. Wählen Sie OK aus.

5. Wählen Sie Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy aus.

6. Wählen Sie die entsprechende IP-Adresszuweisungsmethode aus. In diesem Leitfaden werden die internen Adresspools verwendet. Siehe Abbildung 14.

   Abbildung 14: Zuweisungsmethode für IP-Adressen



7. Klicken Sie auf Apply (Anwenden).

Erstellen einer Tunnelgruppen- und Gruppenrichtlinie

Gruppenrichtlinie

Hinweis: Wenn Sie keine neue Richtlinie erstellen möchten, können Sie die integrierte Standardrichtlinie für Gruppen verwenden.

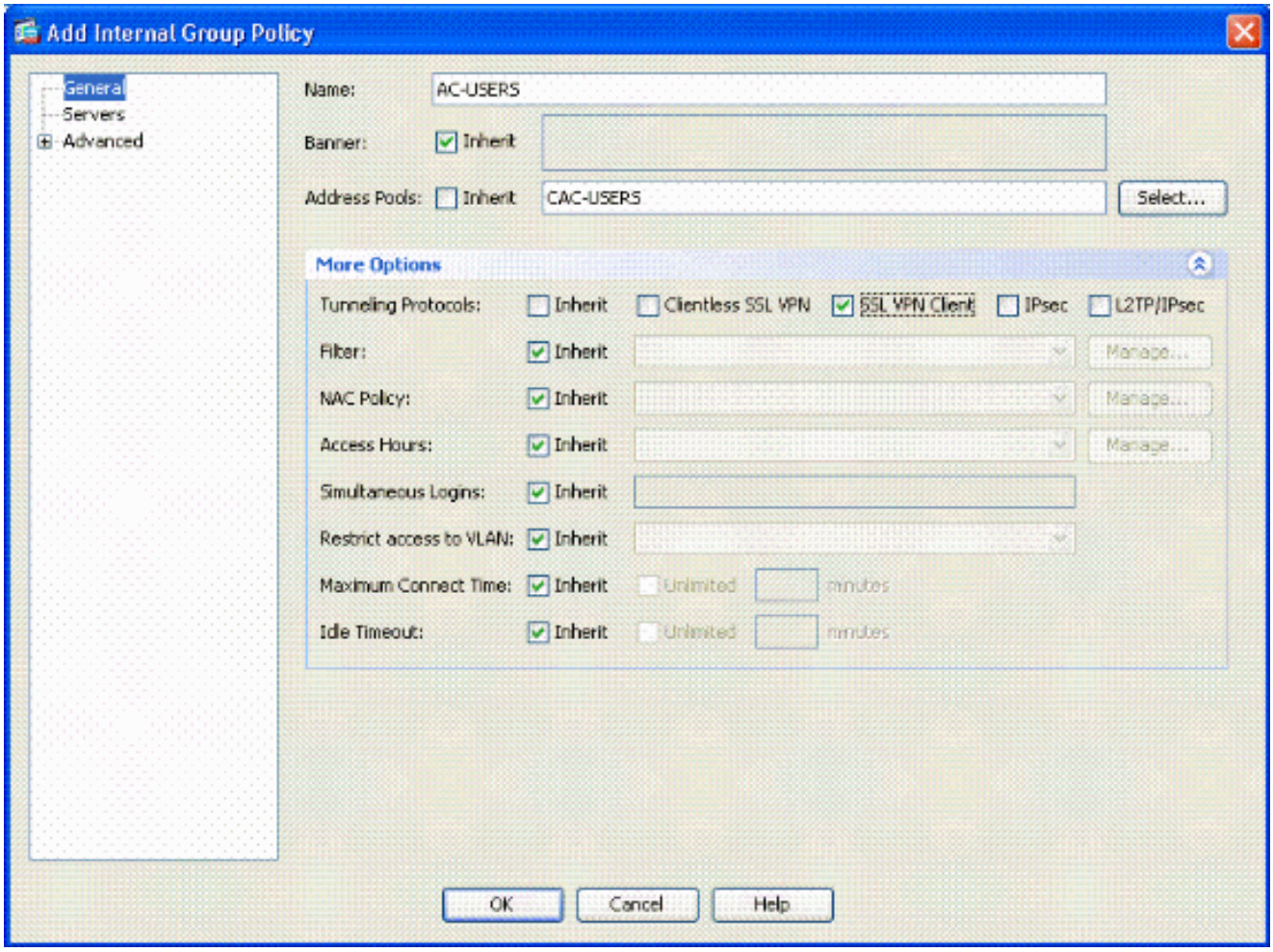
---

1. Wählen Sie Remote Access VPN -> Network (Client) Access -> Group Policies (Remote-Zugriffs-VPN -> Netzwerkzugriff (Client) -> Gruppenrichtlinien aus.

2. Klicken Sie auf Hinzufügen, und wählen Sie Interne Gruppenrichtlinie aus.

3. Geben Sie im Fenster Interne Gruppenrichtlinie hinzufügen den Namen für die Gruppenrichtlinie in das Textfeld Name ein. Siehe Abbildung 15.

   Abbildung 15: Hinzufügen einer internen Gruppenrichtlinie



   a. Wählen Sie auf der Registerkarte General (Allgemein) in der Option Tunneling Protocols (Tunneling-Protokolle) den SSL VPN Client aus, es sei denn, Sie verwenden andere Protokolle wie Clientless SSL.

   b. Deaktivieren Sie im Abschnitt Servers das Kontrollkästchen inherit (vererben), und geben Sie die IP-Adresse der DNS- und WINS-Server ein. Geben Sie ggf. den DHCP-Bereich ein.

   c. Deaktivieren Sie im Abschnitt Servers das Kontrollkästchen inherit in der Standarddomäne, und geben Sie den entsprechenden Domänennamen ein.

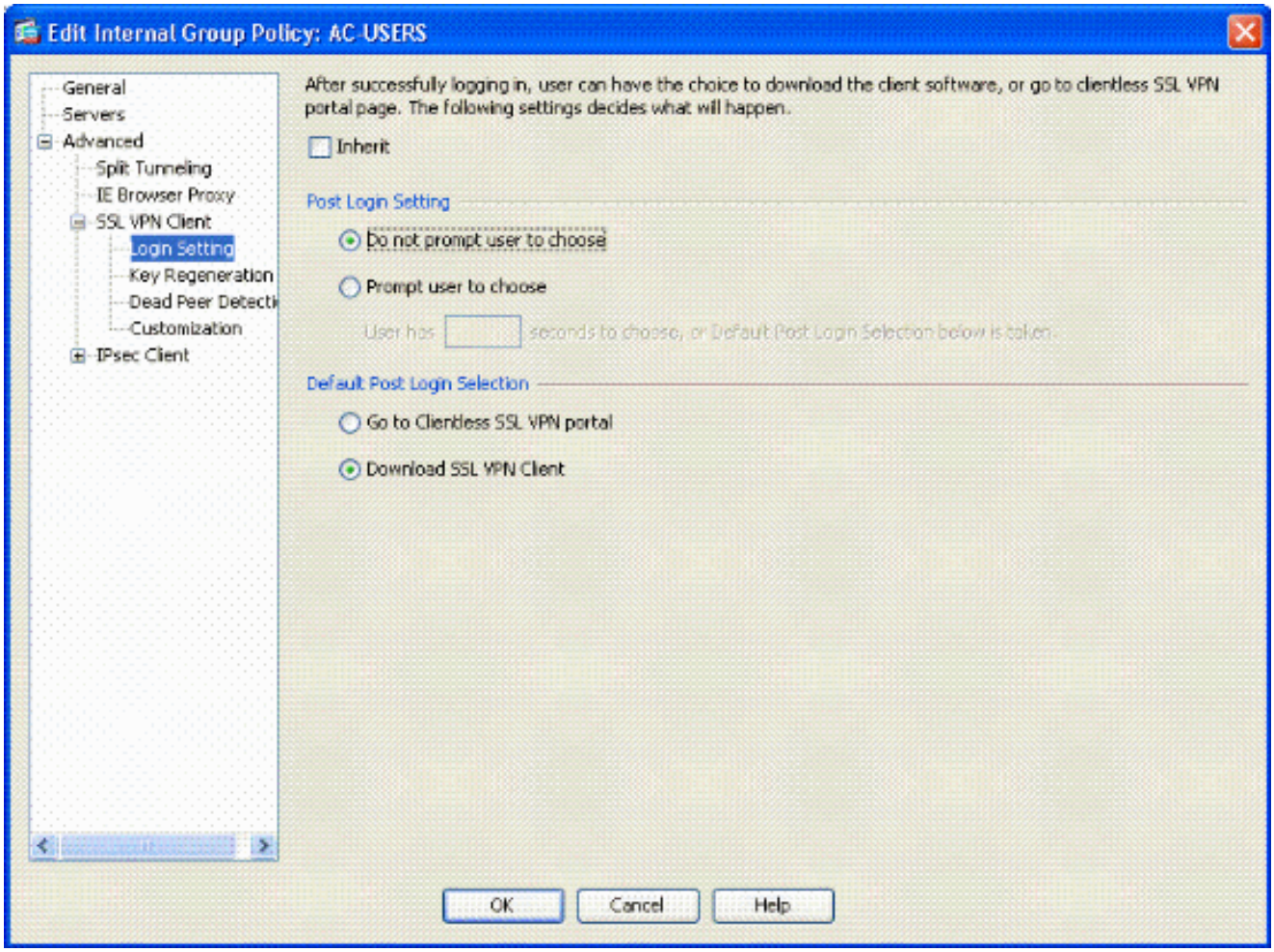
   d. Deaktivieren Sie auf der Registerkarte Allgemein das Kontrollkästchen Vererbung im Adresspoolbereich, und fügen Sie den im vorherigen Schritt erstellten Adresspool hinzu. Wenn Sie eine andere Methode der IP-Adresszuweisung verwenden, überlassen Sie dies dem Erben, und nehmen Sie die entsprechende Änderung vor.

   e. Auf allen anderen Konfigurationsregistern werden die Standardeinstellungen übernommen.

> Hinweis: Es gibt zwei Methoden, um den AC-Client an die Endbenutzer zu senden. Eine Möglichkeit besteht darin, den AC-Client unter Cisco.com herunterzuladen. Die zweite Methode besteht darin, dass die ASA den Client für den Benutzer herunterlädt, wenn der Benutzer versucht, eine Verbindung herzustellen. Dieses Beispiel zeigt die zweite Methode.

4. Wählen Sie anschließend Erweitert > SSL VPN-Client > Anmeldeeinstellungen aus. Siehe Abbildung 16.

   Abbildung 16: Hinzufügen einer internen Gruppenrichtlinie



   a. Deaktivieren Sie das Kontrollkästchen Vererben.

   b. Wählen Sie die für Ihre Umgebung passende Einstellung nach der Anmeldung aus.

   c. Wählen Sie die für Ihre Umgebung passende Standardauswahl für die Postanmeldung aus.

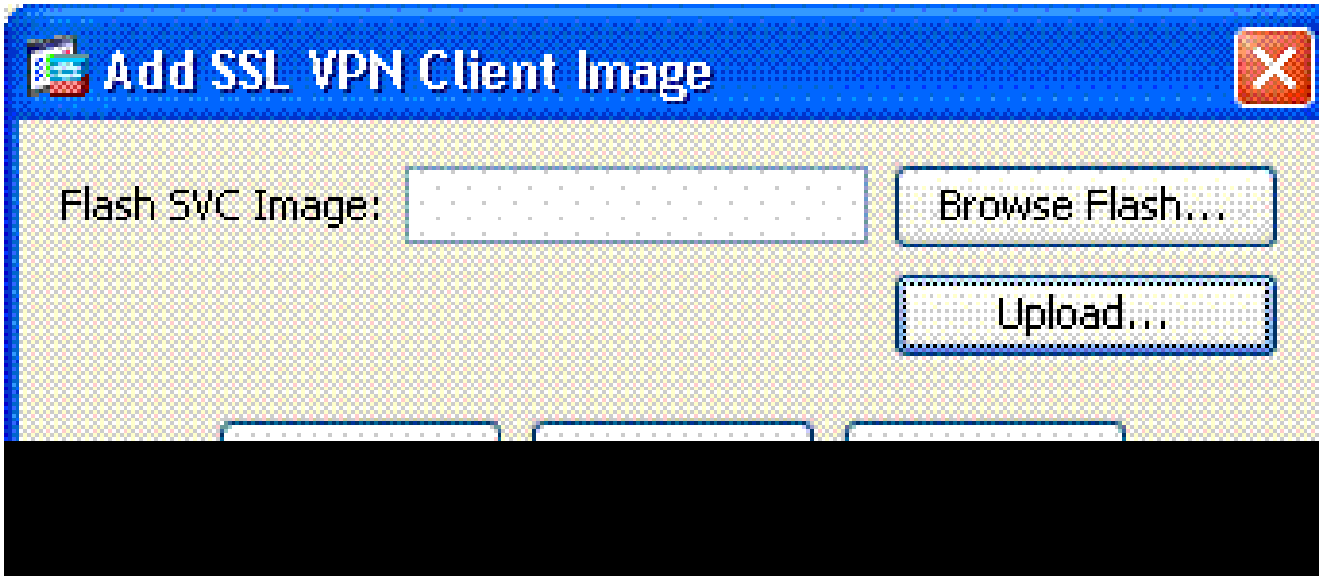
   d. Wählen Sie OK.

Tunnelgruppen-Schnittstelle und Image-Einstellungen

Hinweis: Wenn Sie keine neue Gruppe erstellen möchten, können Sie die integrierte Standardgruppe verwenden.

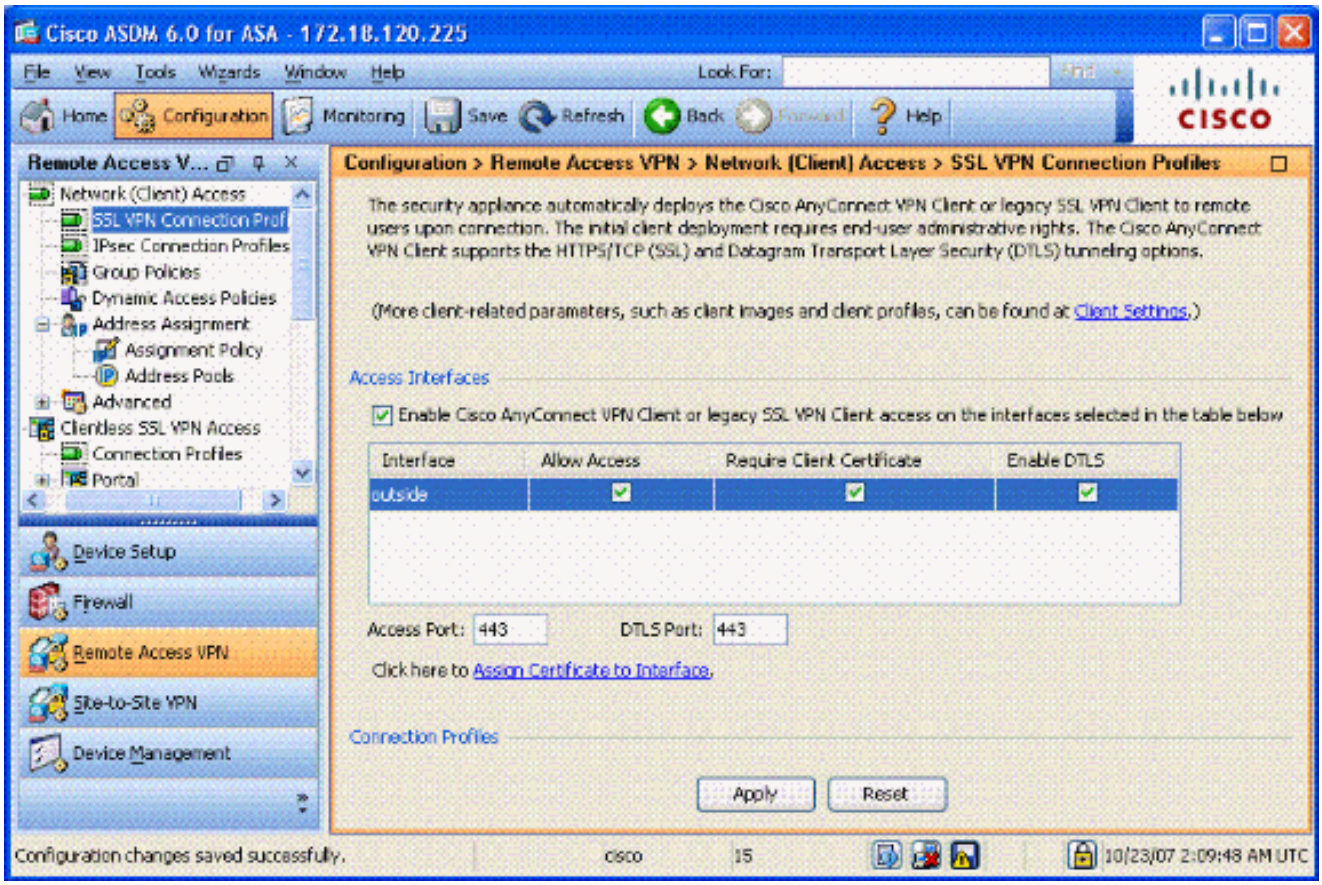
1. Wählen Sie Remote Access VPN > Network (Client) Access > SSL VPN Connection Profile aus.
2. Wählen Sie Cisco AnyConnect Client aktivieren.....
3. Es erscheint ein Dialogfeld mit der Frage `Möchten Sie ein SVC-Bild zuweisen?`
4. Wählen Sie Ja aus.
5. Wenn bereits ein Bild vorhanden ist, wählen Sie das Bild aus, das mit Flash durchsuchen verwendet werden soll. Wenn das Bild nicht verfügbar ist, wählen Sie Hochladen, und suchen Sie auf dem lokalen Computer nach der Datei. Siehe Abbildung 17. Die Dateien können von Cisco.com heruntergeladen werden; es gibt eine Windows-, MAC- und Linux-Datei.

   Abbildung 17: Hinzufügen eines SSL VPN-Client-Images



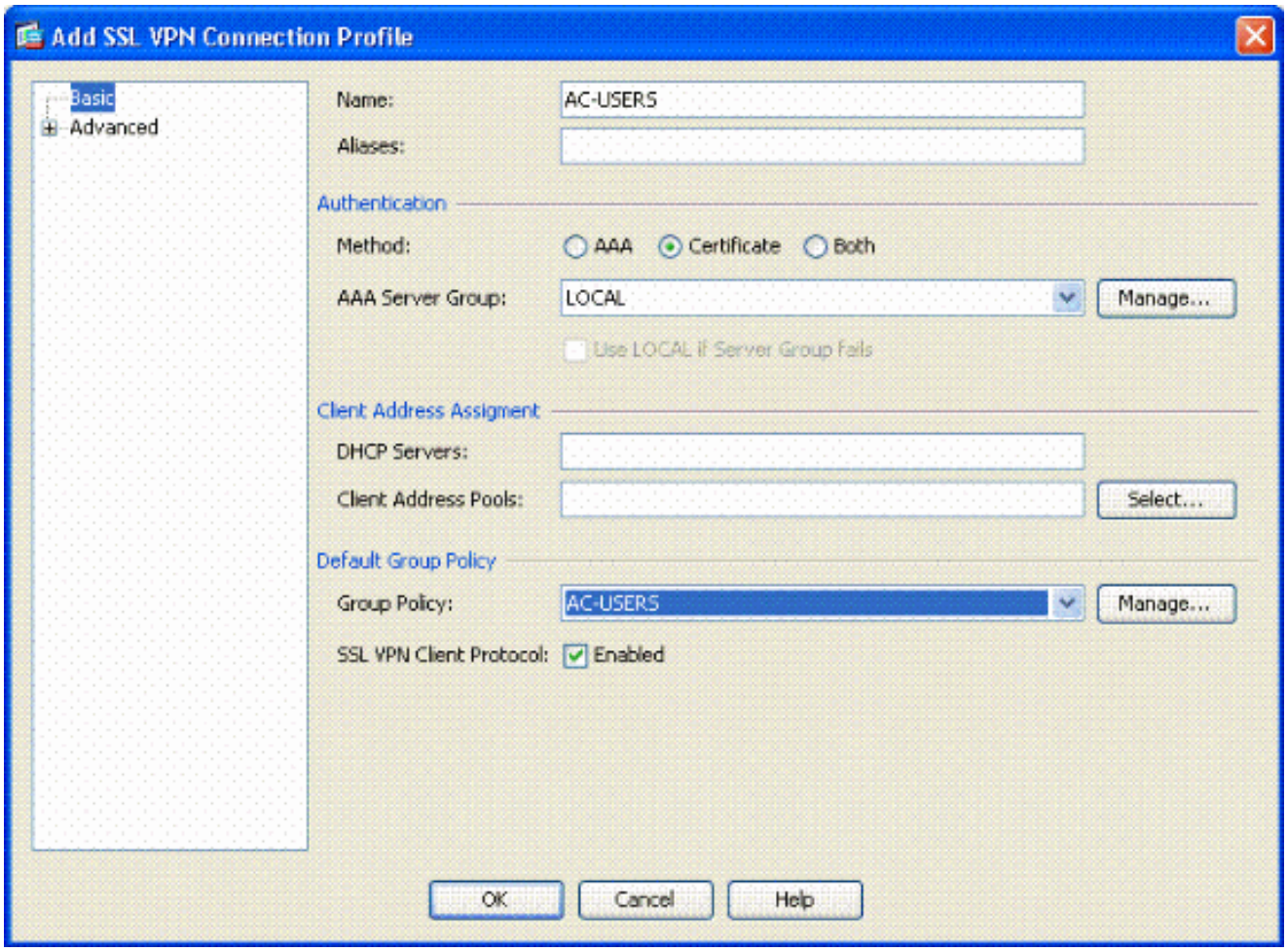
6. Aktivieren Sie als Nächstes Zugriff zulassen, Clientzertifikat anfordern und optional DTLS aktivieren. Siehe Abbildung 18.

   Abbildung 18: Aktivieren des Zugriffs



7. Klicken Sie auf Apply (Anwenden).
8. Erstellen Sie anschließend ein Verbindungsprofil bzw. eine Tunnelgruppe. Wählen Sie Remote Access VPN > Network (Client) Access > SSL VPN Connection Profile aus.
9. Klicken Sie im Abschnitt "Verbindungsprofile" auf Hinzufügen.

   Abbildung 19: Hinzufügen eines Verbindungsprofils



a. Nennen Sie die Gruppe.

b. Wählen Sie in der Authentifizierungsmethode Zertifikat aus.

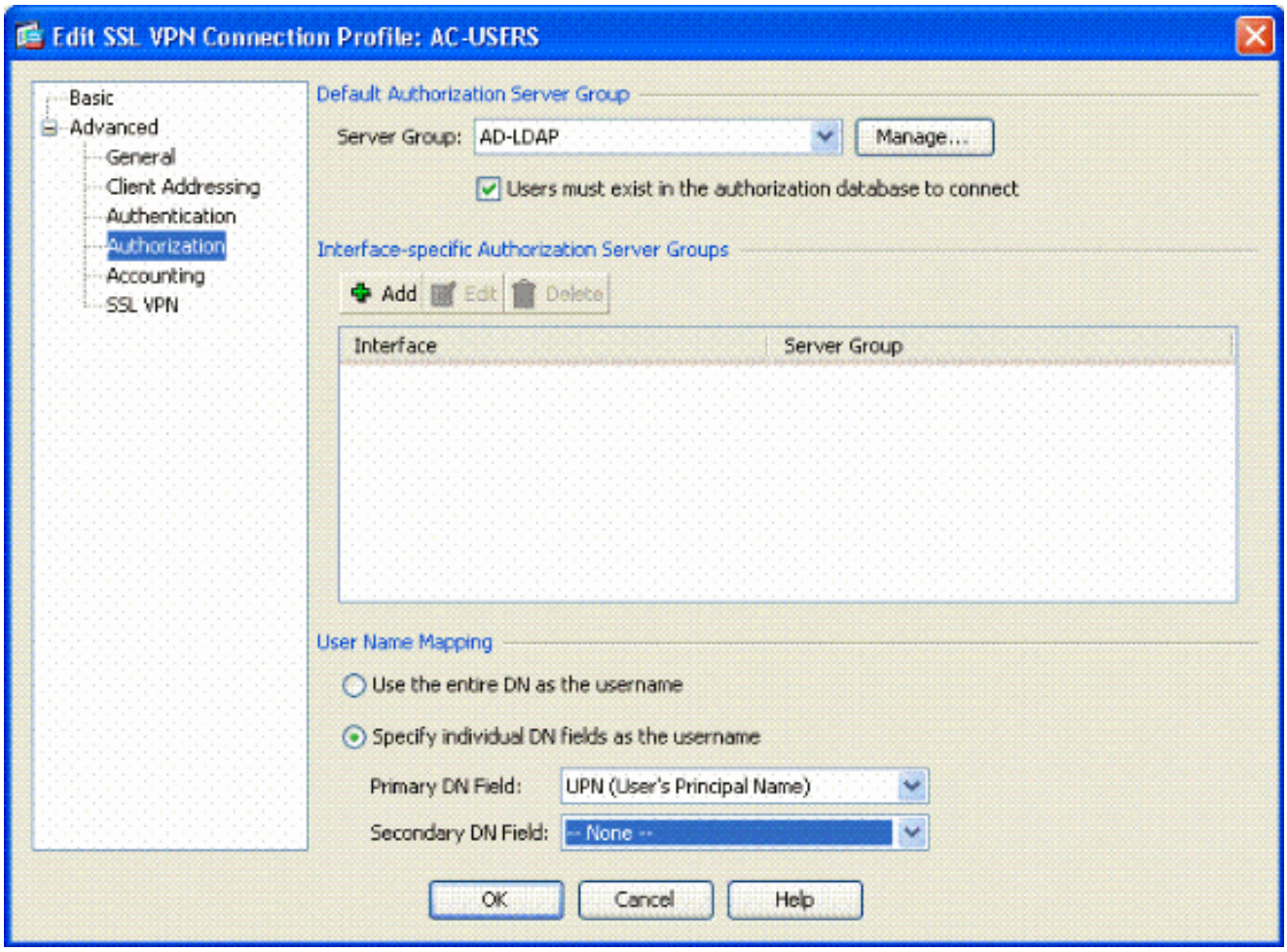
c. Wählen Sie die zuvor erstellte Gruppenrichtlinie aus.

d. Stellen Sie sicher, dass der SSL VPN-Client aktiviert ist.

e. Belassen Sie andere Optionen als Standard.

10. Wählen Sie anschließend Advanced > Authorization (Erweitert > Autorisierung). Siehe Abbildung 20

Abbildung 20: Autorisierung



a. Wählen Sie die zuvor erstellte AD-LDAP-Gruppe aus.

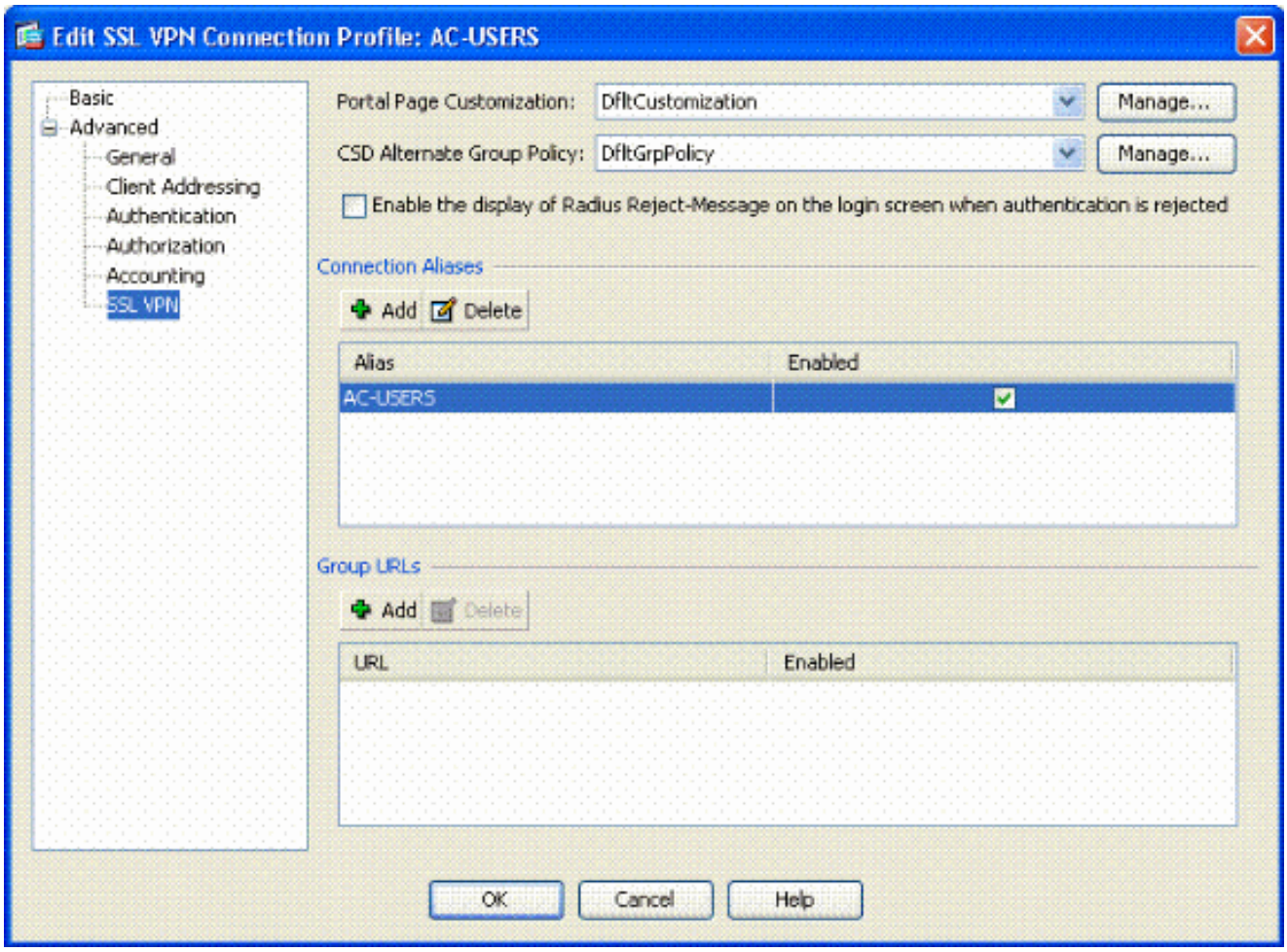
b. Aktivieren Sie Benutzer müssen vorhanden sein...um eine Verbindung herzustellen.

c. Wählen Sie in den Zuordnungsfeldern UPN als primäres und kein UPN als sekundäres aus.

11. Wählen Sie im Menü den Abschnitt SSL VPN aus.

12. Führen Sie im Abschnitt Verbindungsaliase die folgenden Schritte aus:

Abbildung 21: Verbindungsaliase



a. Wählen Sie Hinzufügen aus.

b. Geben Sie den Gruppenalias ein, den Sie verwenden möchten.

c. Stellen Sie sicher, dass Aktiviert aktiviert ist. Siehe Abbildung 21.

13. Klicken Sie auf OK.

Hinweis: Klicken Sie auf Speichern, um die Konfiguration im Flash-Speicher zu speichern.

Zertifikatzuordnungsregeln (wenn OCSP verwendet wird)

1. Wählen Sie Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps aus. Siehe Abbildung 22.

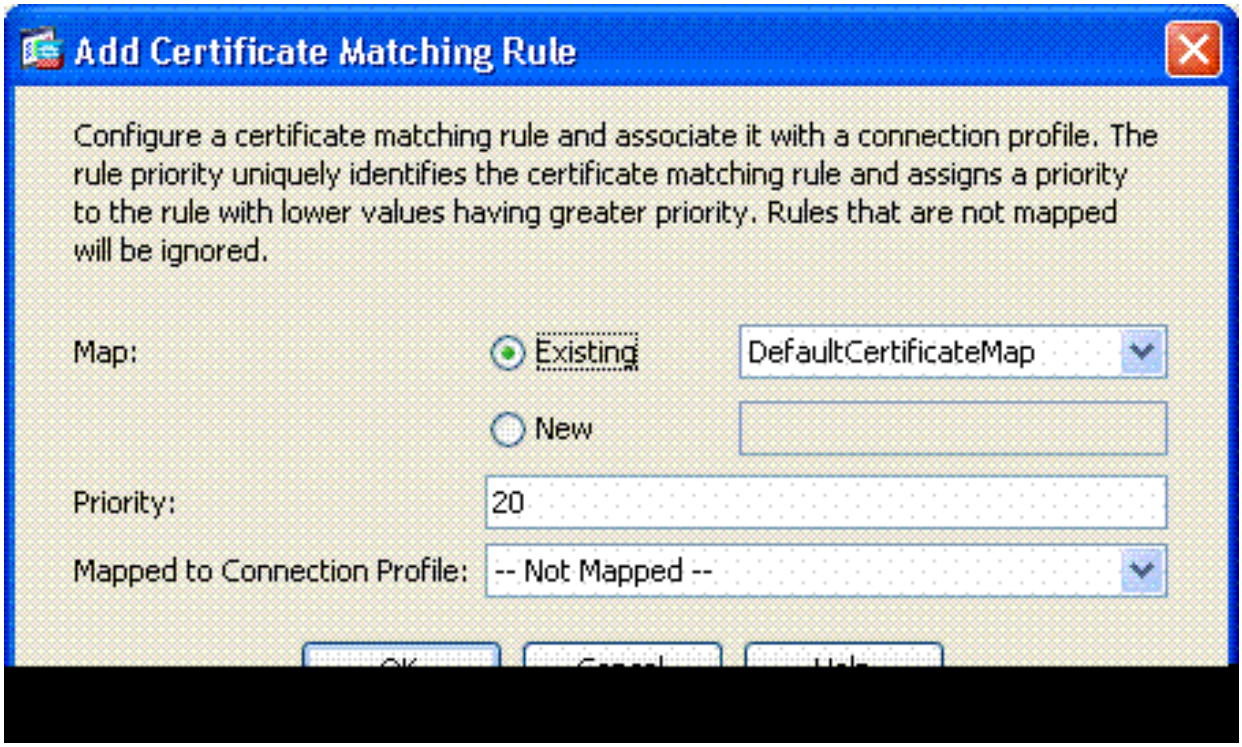
   a. Wählen Sie im Abschnitt Zertifikat zu Verbindungsprofilzuordnungen hinzufügen aus.

   b. Sie können die vorhandene Zuordnung im Zuordnungsabschnitt als DefaultCertificateMap beibehalten oder eine neue erstellen, wenn Sie bereits Zertifikatzuordnungen für IPsec verwenden.

   c. Behalten Sie die Regelpriorität bei.

d. Belassen Sie unter Zugeordnete Gruppe den Wert — Nicht Zugeordnet —. Siehe Abbildung 22.

Abbildung 22: Hinzufügen einer Zertifikatzuordnungsregel

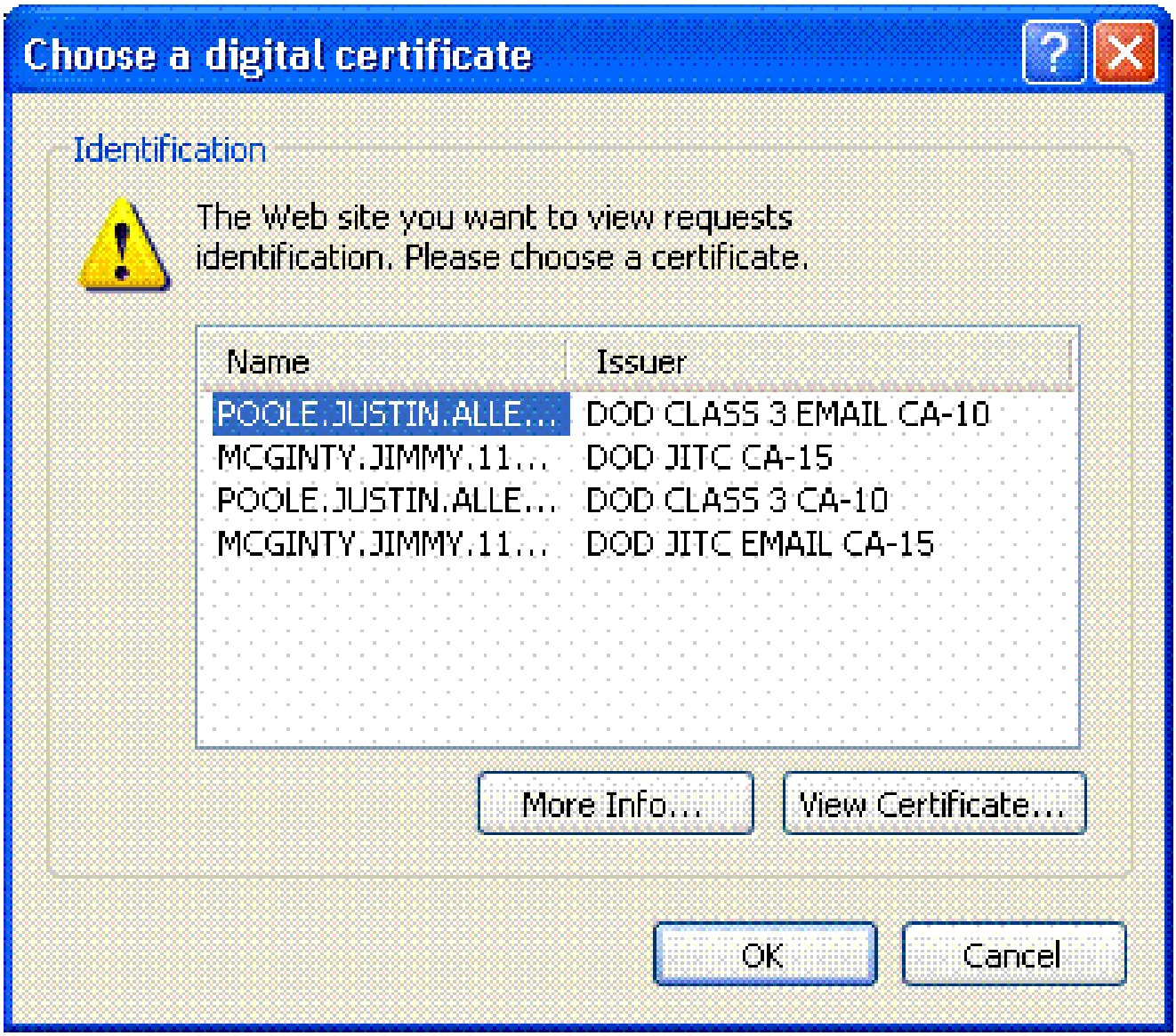


e. Klicken Sie auf OK.

2. Klicken Sie in der unteren Tabelle auf Hinzufügen.

3. Führen Sie im Fenster "Zertifikatzuordnungsregelkriterium hinzufügen" die folgenden Schritte aus:

Abbildung 23: Kriterium für die Zertifikatzuordnungsregel



a. Behalten Sie in der Spalte Feld den Wert Betreff bei.

b. Behalten Sie in der Spalte Komponente den Wert Volles Feld bei.

c. Ändern Sie die Spalte Operator in Does Not Equal.

d. Geben Sie in der Spalte Wert zwei doppelte Anführungszeichen "" ein

e. Klicken Sie auf OK und Apply. Siehe zum Beispiel Abbildung 23.

OCSP konfigurieren

Die Konfiguration eines OCSP kann variieren und hängt vom Anbieter des OCSP-Ansprechpartners ab. Weitere Informationen finden Sie im Handbuch des Anbieters.

OCSP-Responder-Zertifikat konfigurieren

1. Holen Sie sich ein selbst generiertes Zertifikat vom OCSP-Responder.

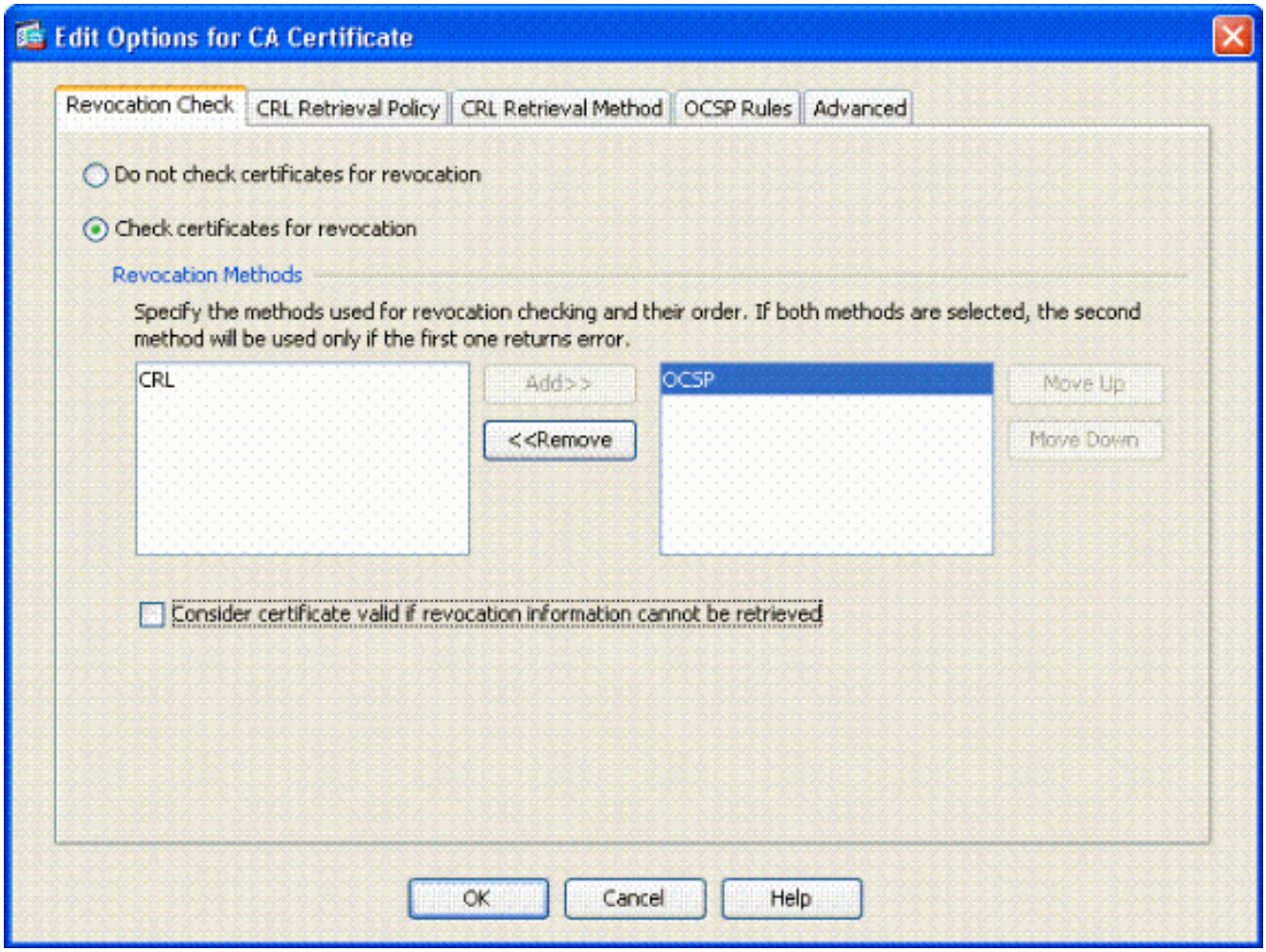
2. Führen Sie die zuvor genannten Schritte aus, und installieren Sie ein Zertifikat für den OSCP-Server.

Hinweis: Stellen Sie sicher, dass für den OCSP-Zertifikatvertrauenspunkt "Zertifikate nicht auf Widerruf prüfen" ausgewählt ist.

Konfigurieren der Zertifizierungsstelle zur Verwendung von OCSP

1. Wählen Sie Remote Access VPN > Certificate Management > CA Certificates aus.
2. Markieren Sie einen OCSP, um eine CA für die Verwendung von OCSP auszuwählen.
3. Klicken Sie auf Bearbeiten.
4. Stellen Sie sicher, dass Zertifikat auf Widerruf überprüfen aktiviert ist.
5. Fügen Sie im Abschnitt "Revocation Methods" (Sperrmethoden) OCSP hinzu. Siehe Abbildung 24.

   OCSP-Sperrprüfung



6. Stellen Sie sicher, dass Zertifikat als gültig betrachten...kann nicht abgerufen werden deaktiviert ist, wenn Sie eine strenge OCSP-Prüfung befolgen möchten.

Hinweis: Konfigurieren/bearbeiten Sie alle CA-Server, die OCSP für den Widerruf verwenden.

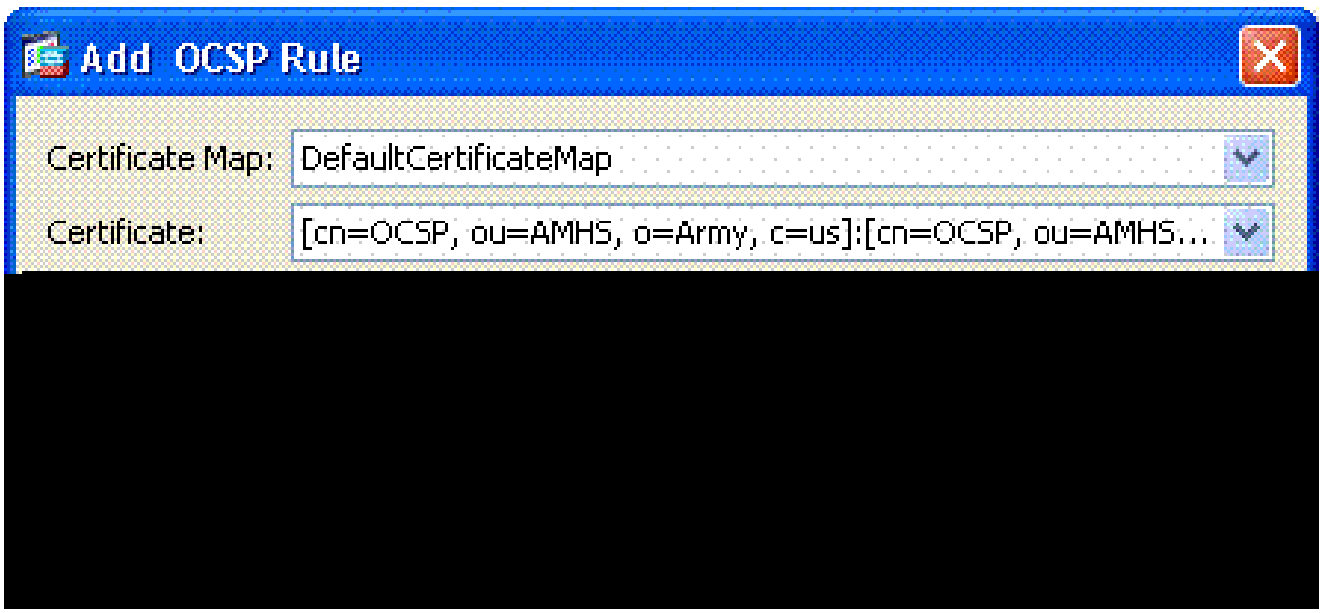
OCSP-Regeln konfigurieren

Hinweis: Überprüfen Sie, ob eine Richtlinie für den Zertifikatgruppenabgleich erstellt und der OCSP-Responder konfiguriert wurde, bevor Sie diese Schritte ausführen.

Hinweis: In einigen OCSP-Implementierungen können ein DNS A- und ein PTR-Datensatz für die ASA erforderlich sein. Mit dieser Prüfung wird überprüft, ob die ASA von einer MIL-Site stammt.

1. Wählen Sie Remote Access VPN > Certificate Management > CA Certificates 2 aus.
2. Markieren Sie einen OCSP, um eine CA für die Verwendung von OCSP auszuwählen.
3. Wählen Sie Bearbeiten aus.
4. Klicken Sie auf die Registerkarte OCSP Rule (OCSP-Regel).
5. Klicken Sie auf Hinzufügen.
6. Führen Sie im Fenster "Add OCSP Rule" (OCSP-Regel hinzufügen) diese Schritte aus. Siehe Abbildung 25.

   Abbildung 25: Hinzufügen von OCSP-Regeln



   a. Wählen Sie in der Option Zertifikatzuordnung die Option DefaultCertificateMap oder eine zuvor erstellte Zuordnung aus.

   b. Wählen Sie unter Certificate (Zertifikat) die Option OCSP responder (OCSP-

Responder).

c. Geben Sie in der Indexoption 10 ein.

d. Geben Sie in der URL-Option die IP-Adresse oder den Hostnamen des OCSP-Responders ein. Wenn Sie den Hostnamen verwenden, stellen Sie sicher, dass der DNS-Server auf der ASA konfiguriert ist.

e. Klicken Sie auf OK.

f. Klicken Sie auf Apply (Anwenden).

Konfiguration des Cisco AnyConnect-Clients

In diesem Abschnitt wird die Konfiguration des Cisco AnyConnect VPN-Clients beschrieben.

Annahmen - Der Cisco AnyConnect VPN Client und die Middleware-Anwendung sind bereits auf dem Host-PC installiert. ActivCard Gold und ActivClient wurden getestet.

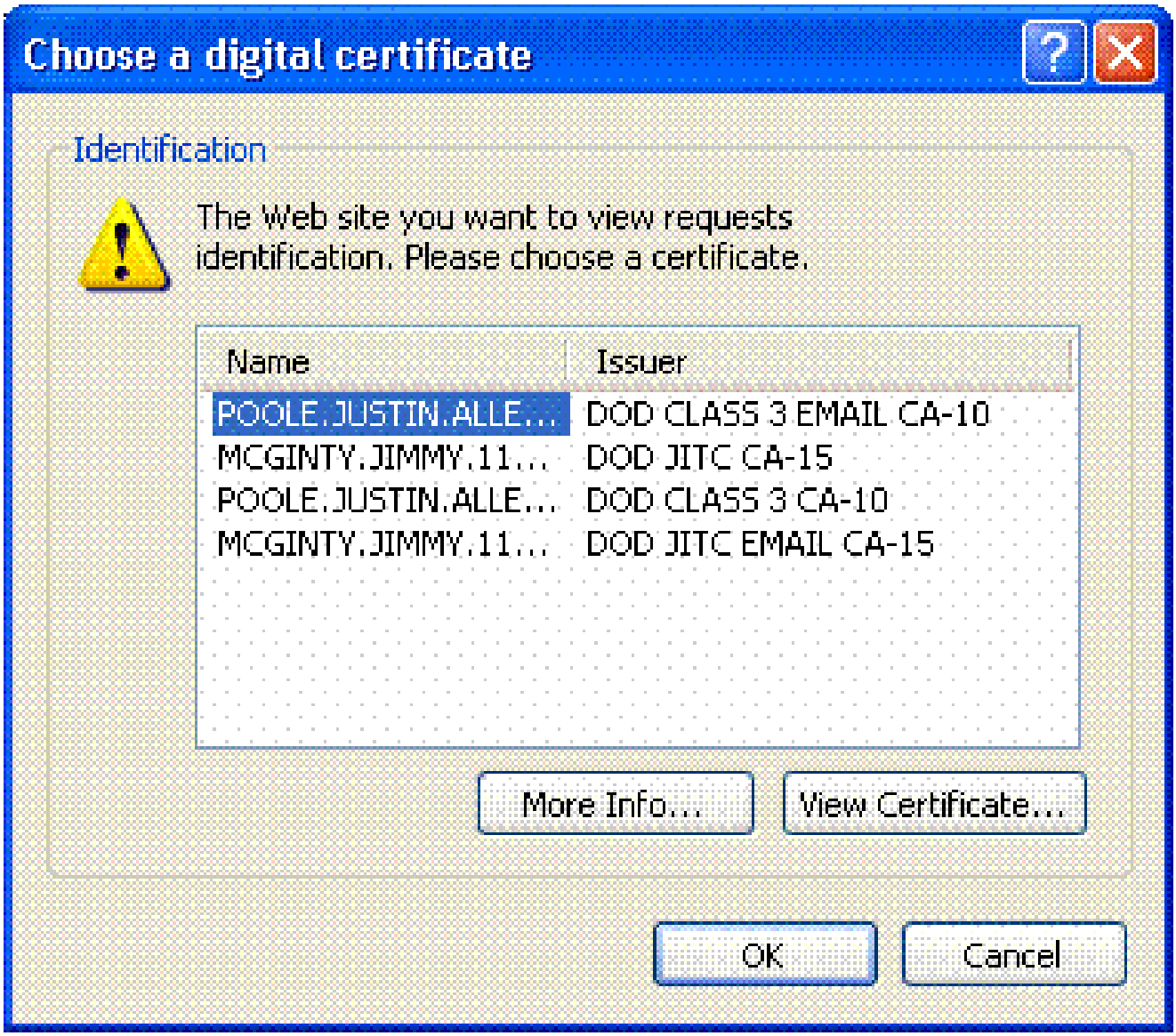
Hinweis: In diesem Handbuch wird die group-url-Methode nur für die Erstinstallation eines AC-Clients verwendet. Sobald der AC-Client installiert ist, starten Sie die AC-Anwendung genau wie den IPsec-Client.

Hinweis: Die DoD-Zertifikatskette muss auf dem lokalen Computer installiert werden. Wenden Sie sich an den PKI POC, um die Zertifikate-/Batch-Datei zu erhalten.

Herunterladen des Cisco AnyConnect VPN Client - Windows

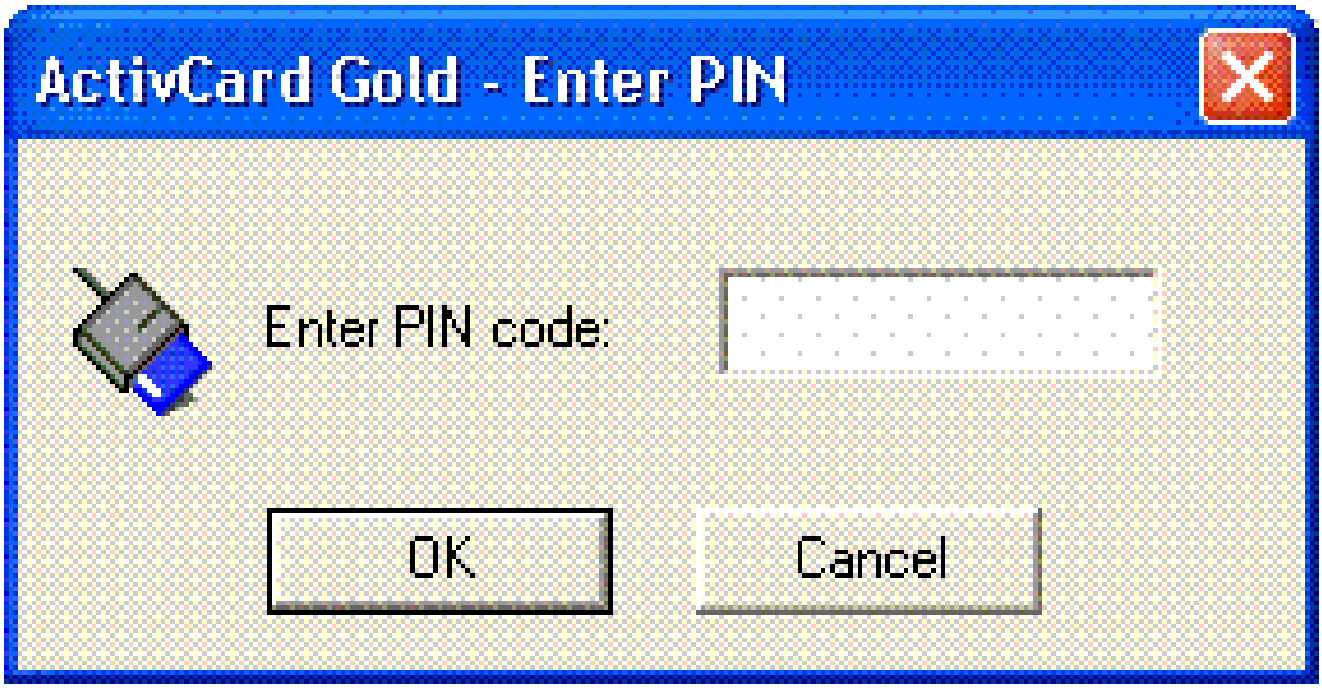
1. Starten Sie über Internet Explorer eine Websitzung mit der ASA. Die Adresse muss das Format https://Outside-Interface haben. Beispiel: https://172.18.120.225.
2. Wählen Sie das Signaturzertifikat aus, das für den Zugriff verwendet werden soll. Siehe Abbildung 26.

   Abbildung 26: Auswählen des richtigen Zertifikats



3. Geben Sie Ihre PIN ein, wenn Sie dazu aufgefordert werden.

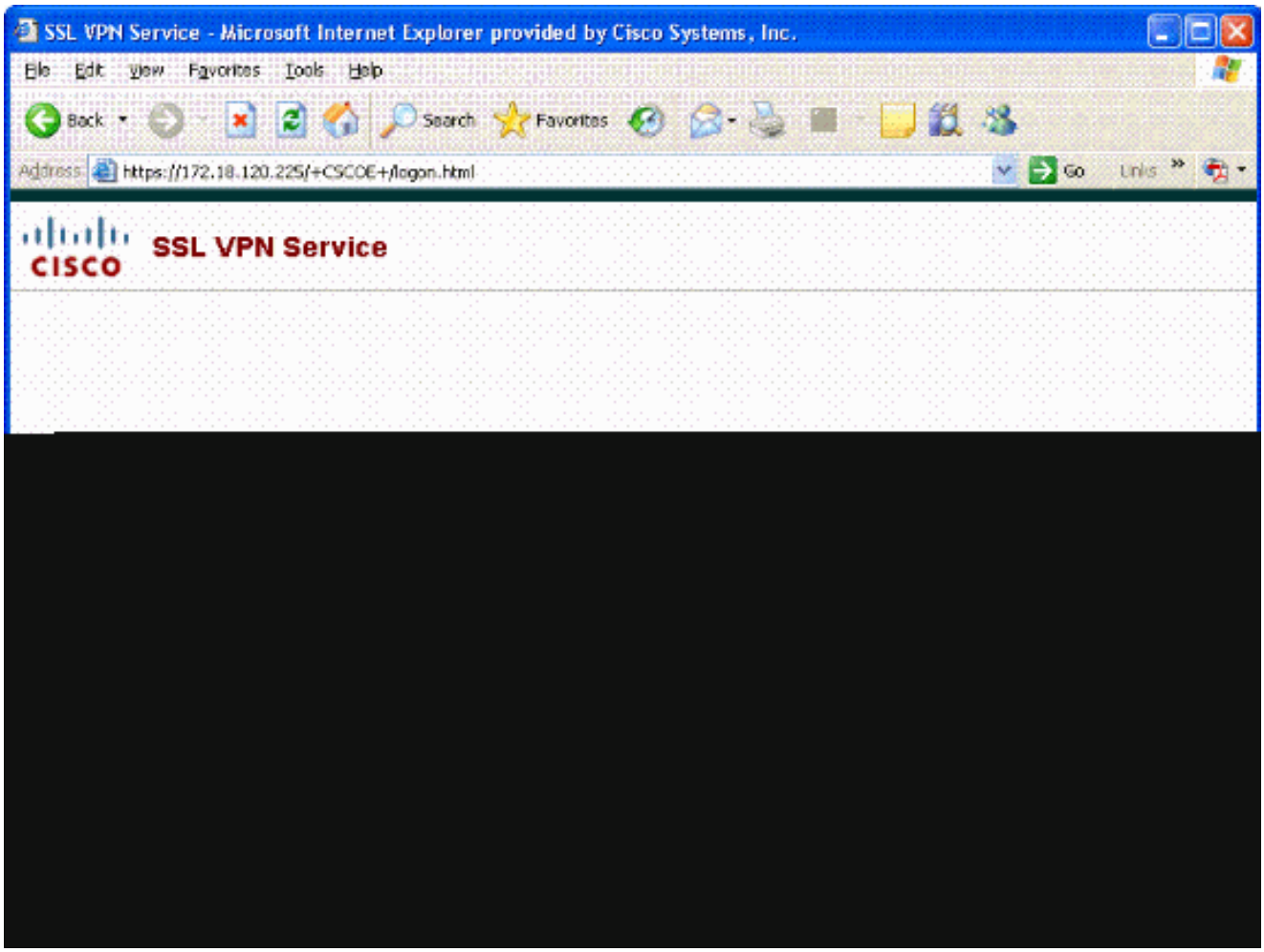
Abbildung 27: PIN eingeben



4. Wählen Sie Ja, um die Sicherheitswarnung zu akzeptieren.

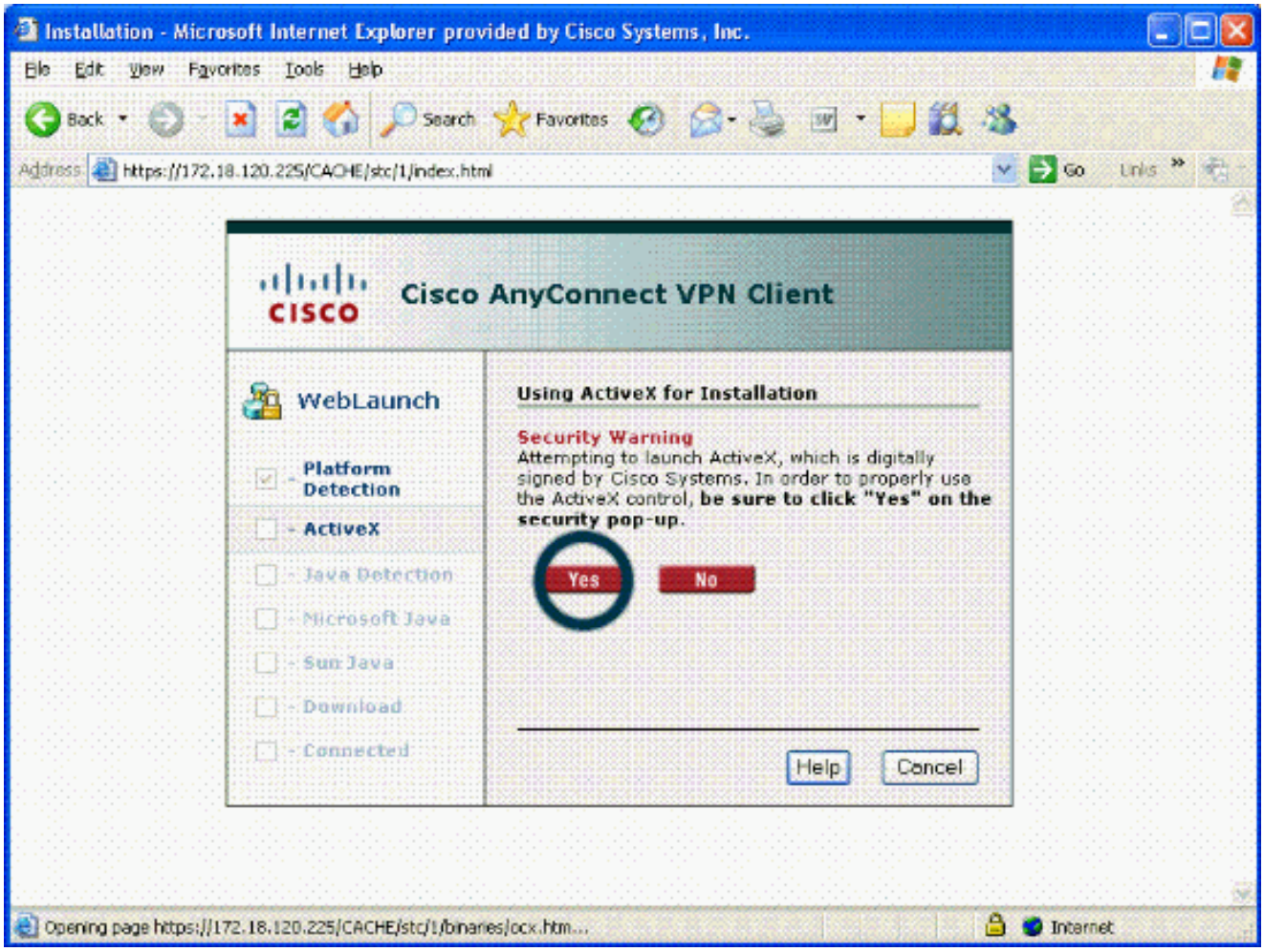
5. Sobald Sie sich auf der SSL-Anmeldeseite angemeldet haben, wählen Sie Anmelden. Das Client-Zertifikat wird für die Anmeldung verwendet. Siehe Abbildung 28.

   Abbildung 28: SSL-Anmeldung



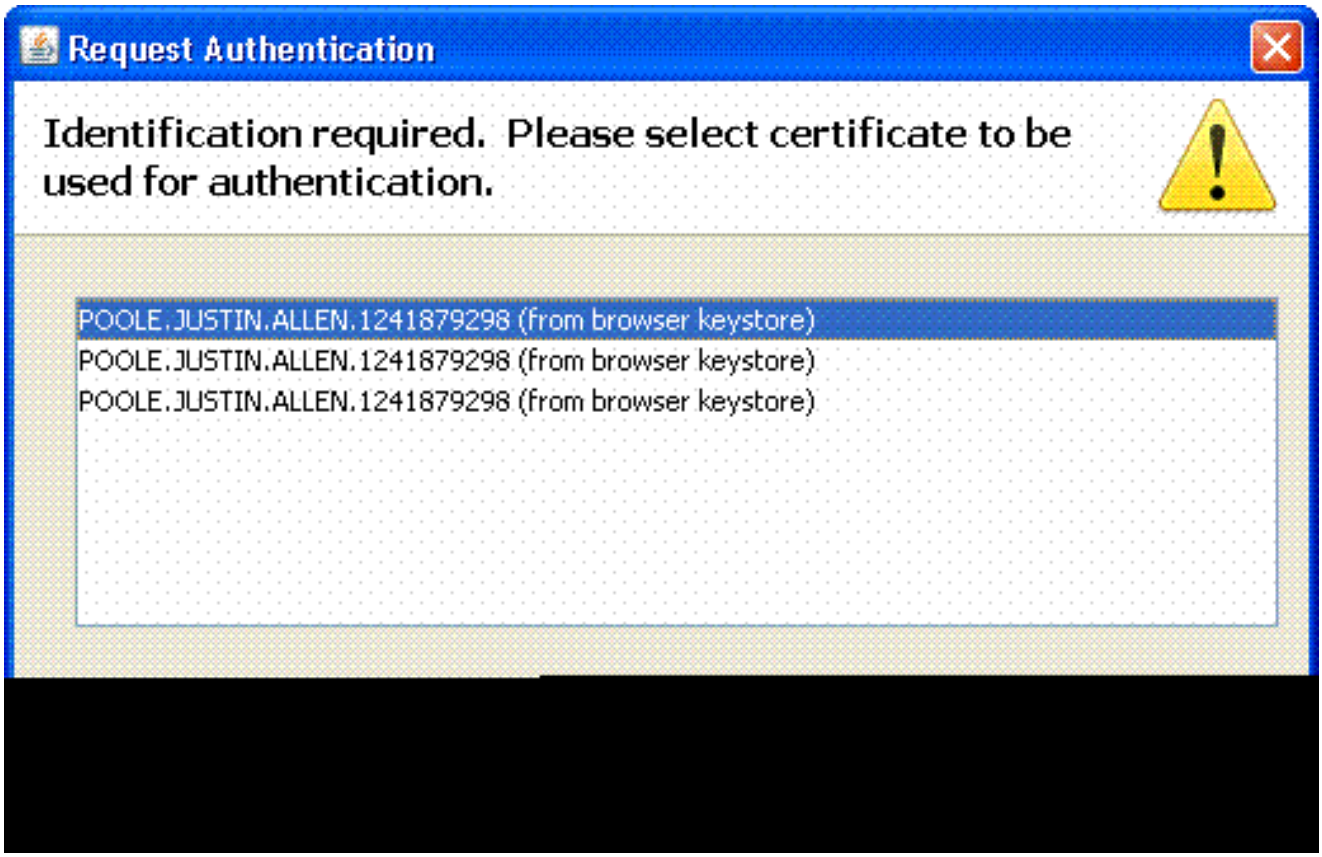
6. AnyConnect beginnt mit dem Herunterladen des Clients. Siehe Abbildung 29.

   Abbildung 29: Installation von AnyConnect



7. Wählen Sie das entsprechende Zertifikat aus. Siehe Abbildung 30. Die Installation von AnyConnect wird fortgesetzt. Der ASA-Administrator kann dem Client die permanente Installation oder Installation auf jeder ASA-Verbindung gestatten.

   Abbildung 30: Zertifikat



Starten des Cisco AnyConnect VPN Clients - Windows

Wählen Sie auf dem Host-PC Start > Alle Programme > Cisco > AnyConnect VPN Client aus.

Hinweis: Informationen zur optionalen Konfiguration des AnyConnect-Clientprofils finden Sie im Anhang E.

Neue Verbindung

1. Das Fenster Wechselstrom wird angezeigt. Siehe Abbildung 34.

   Abbildung 34: Neue VPN-Verbindung

2. Wählen Sie den geeigneten Host aus, wenn AC die Verbindung nicht automatisch versucht.

3. Geben Sie bei Aufforderung Ihre PIN ein. Siehe Abbildung 35.

Abbildung 35: PIN eingeben

Remote-Zugriff starten

Wählen Sie die Gruppe und den Host aus, mit der Sie eine Verbindung herstellen möchten.

Da Zertifikate verwendet werden, wählen Sie Verbinden, um das VPN einzurichten. Siehe Abbildung 36.

Abbildung 36: Anschließen


Cisco AnyConnect VPN Client
Connection
Statistics
About
CISCO
Connect to:
172.18.120.225
Group:
AC-USERS
Username:
Password:
Connect
Please enter your username and password.

Hinweis: Da für die Verbindung Zertifikate verwendet werden, müssen Sie keinen Benutzernamen und kein Kennwort eingeben.

Hinweis: Informationen zur optionalen Konfiguration des AnyConnect-Clientprofils finden Sie im Anhang E.

Anhang A: LDAP-Zuordnung und DAP

In ASA/PIX Version 7.1(x) und höher wurde eine Funktion namens LDAP-Zuordnung eingeführt. Dies ist eine leistungsstarke Funktion, die eine Zuordnung zwischen einem Cisco-Attribut und LDAP-Objekten/Attributen ermöglicht, sodass keine LDAP-Schemaänderungen erforderlich sind. Bei der Implementierung der CAC-Authentifizierung kann dies die Durchsetzung zusätzlicher Richtlinien für die RAS-Verbindung unterstützen. Dies sind Beispiele für die LDAP-Zuordnung. Beachten Sie, dass Sie Administratorrechte benötigen, um Änderungen am AD/LDAP-Server vorzunehmen. In der ASA 8.x-Software wurde die Funktion "Dynamic Access Policy (DAP)" eingeführt. Das DAP kann in Verbindung mit der CAC mehrere AD-Gruppen sowie Push-Richtlinien, ACLs usw. untersuchen.

Szenario 1: Active Directory-Durchsetzung mit Einwahl für Remote-Zugriffsberechtigungen - Zugriff zulassen/verweigern

In diesem Beispiel wird das AD-Attribut msNPAllowDailin dem Cisco-Attribut cVPN3000-Tunneling-Protocol zugeordnet.

- Der AD-Attributwert: TRUE = Allow; FALSE = Deny
- Cisco Attributwert: 1 = FALSE, 4 (IPSec) oder 20 (4 IPSEC + 16 WebVPN) = TRUE,

Für die Bedingung ZULÄSSIG ordnen Sie Folgendes zu:

- TRUE = 20

Für die DENY-Einwahlbedingung bestimmen Sie Folgendes:

- FALSCH = 1

Hinweis: Vergewissern Sie sich, dass TRUE und FALSE in Großbuchstaben angegeben sind. Weitere Informationen finden Sie unter Configuring an External Server for Security Appliance User Authorization (Konfigurieren eines externen Servers für die Sicherheitsappliance-Benutzerautorisierung).

Active Directory-Setup

1. Klicken Sie im Active Directory-Server auf Start > Ausführen.

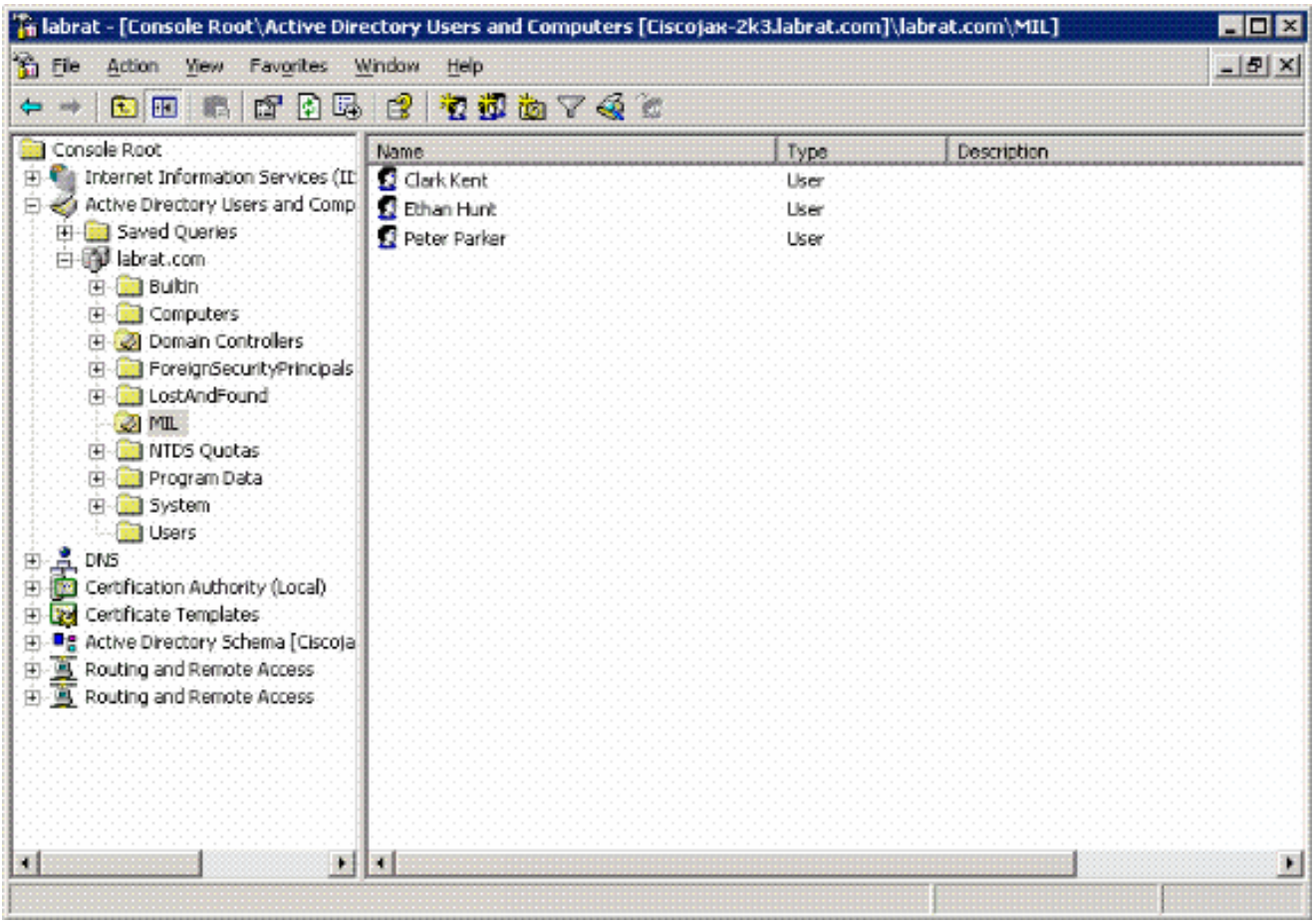
2. Geben Sie in das Textfeld Öffnen den Text dsa.msc ein, und klicken Sie dann auf OK. Dadurch wird die Active Directory-Verwaltungskonsole gestartet.

3. Klicken Sie in der Active Directory-Verwaltungskonsole auf das Pluszeichen, um Active Directory-Benutzer und -Computer zu erweitern.

4. Klicken Sie auf das Pluszeichen, um den Domänennamen zu erweitern.

5. Wenn Sie eine OU für Ihre Benutzer erstellt haben, erweitern Sie die OU, um alle Benutzer anzuzeigen. Wenn alle Benutzer dem Ordner Benutzer zugewiesen sind, erweitern Sie diesen Ordner, um sie anzuzeigen. Siehe Abbildung A1.

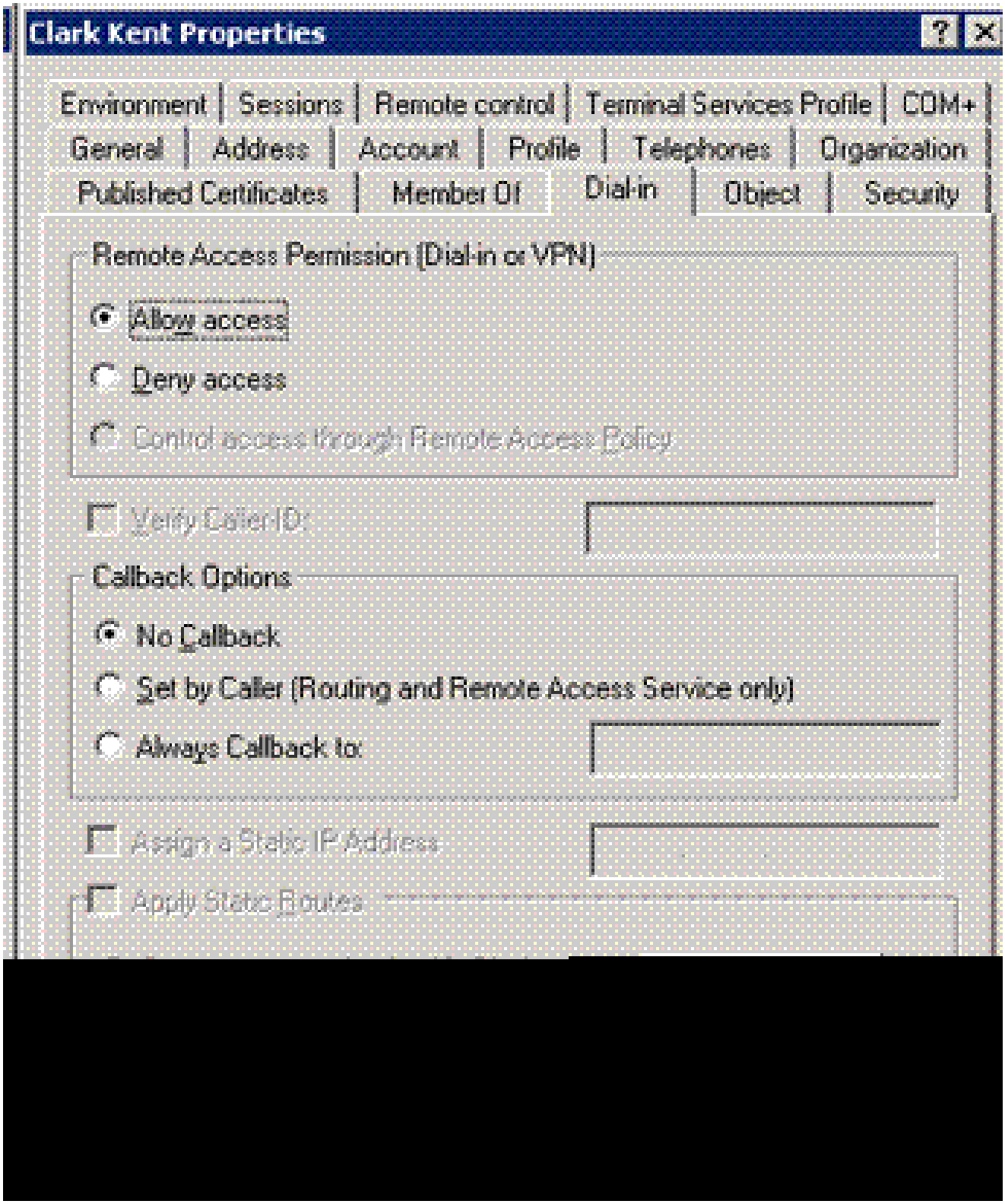
   Abbildung A1: Active Directory-Verwaltungskonsole



6. Doppelklicken Sie auf den Benutzer, den Sie bearbeiten möchten.

   Klicken Sie auf der Seite mit den Benutzereigenschaften auf die Registerkarte Einwählen, und klicken Sie dann auf Zulassen oder Verweigern. Siehe Abbildung A2.

   Abbildung A2: Benutzereigenschaften



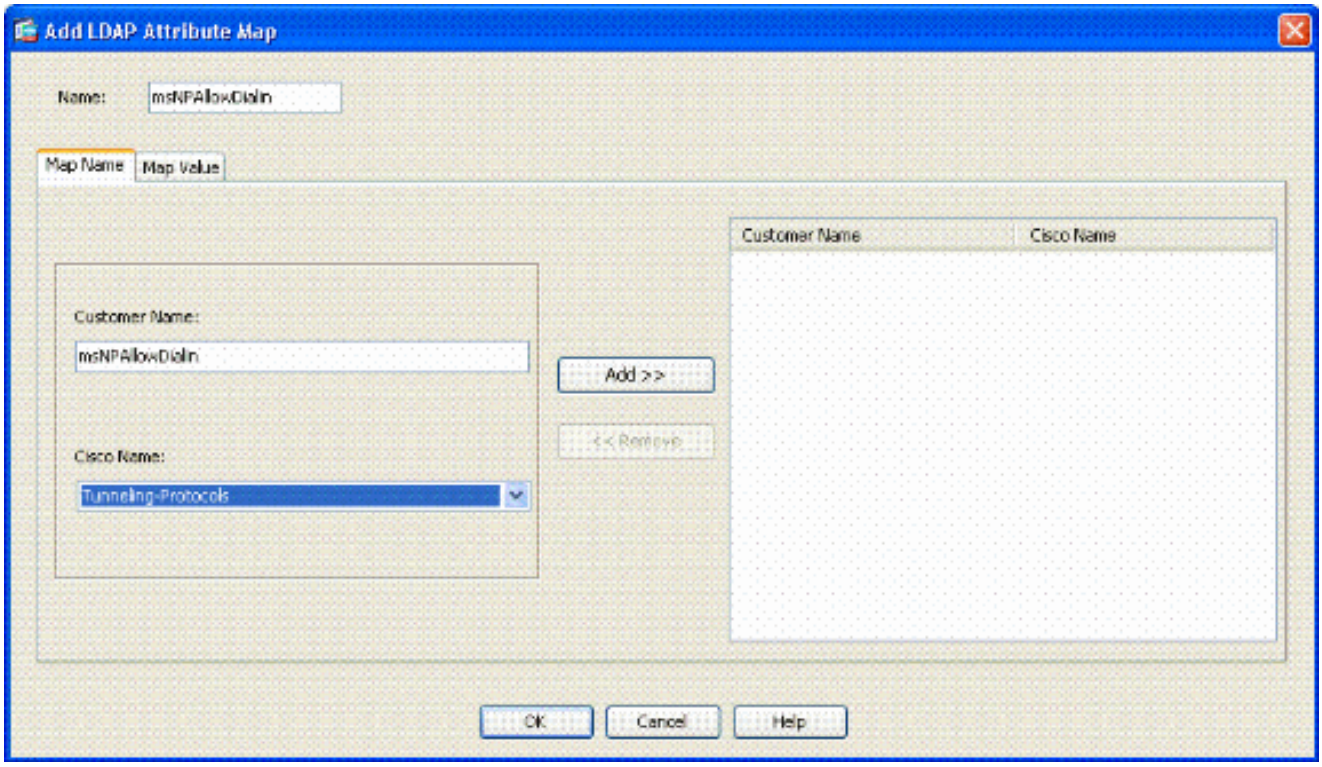
7. Klicken Sie dann auf OK.

ASA-Konfiguration

1. Wählen Sie im ASDM Remote Access VPN > AAA Setup > LDAP Attribute Map aus.
2. Klicken Sie auf Hinzufügen.
3. Führen Sie im Fenster LDAP-Attributzuordnung hinzufügen die folgenden Schritte aus.

Siehe Abbildung A3.

Abbildung A3: Hinzufügen einer LDAP-Attributzuordnung



a. Geben Sie einen Namen in das Textfeld Name ein.

b. Geben Sie auf der Registerkarte Zuordnungsname im Textfeld Kundenname msNPAllowDialin ein.

c. Wählen Sie auf der Registerkarte Map Name (Name der Zuordnung) Tunneling-Protocols aus der Dropdown-Option unter Cisco Name aus.

d. Klicken Sie auf Hinzufügen.

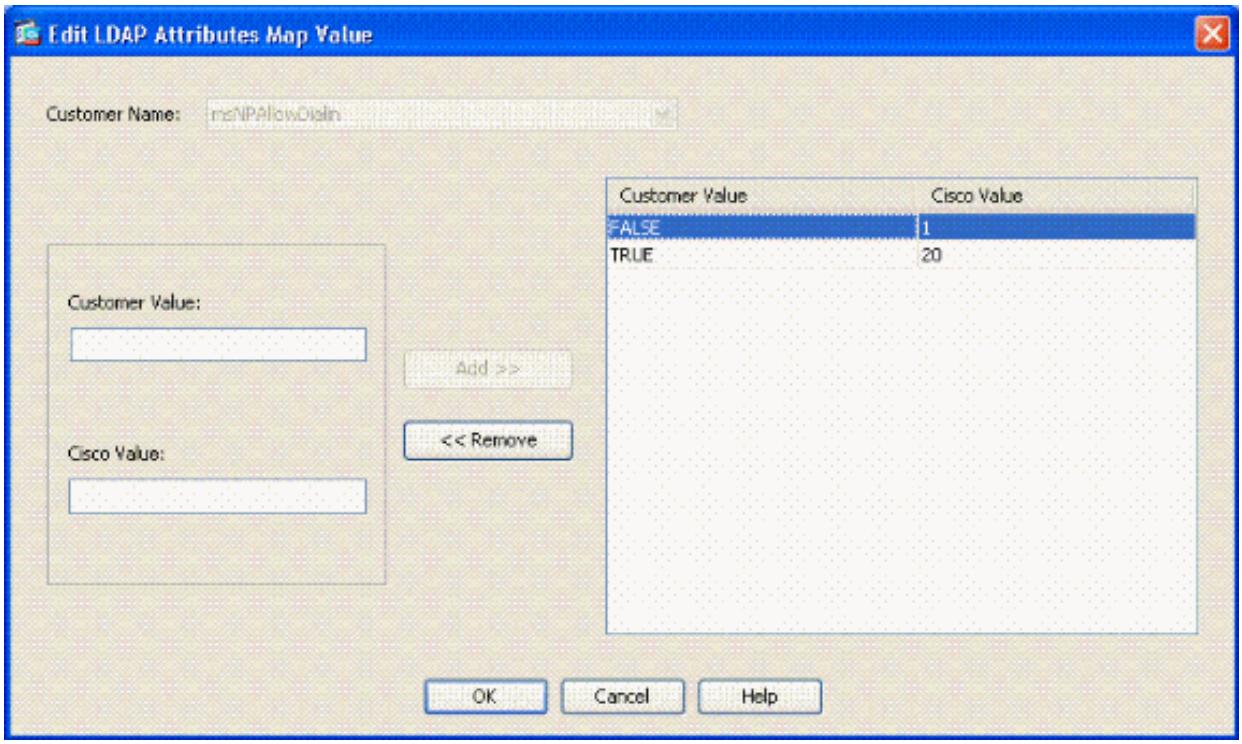
e. Wählen Sie die Registerkarte Map Value aus.

f. Klicken Sie auf Hinzufügen.

g. Geben Sie im Fenster Add Attribute LDAP Map Value (Wert der LDAP-Attributzuordnung hinzufügen) TRUE in das Textfeld Customer Name ein, und geben Sie 20 in das Textfeld Cisco Value ein.

h. Klicken Sie auf Hinzufügen.

i. Geben Sie FALSE in das Textfeld Kundenname ein, und geben Sie 1 in das Textfeld Cisco Wert ein. Siehe Abbildung A4.



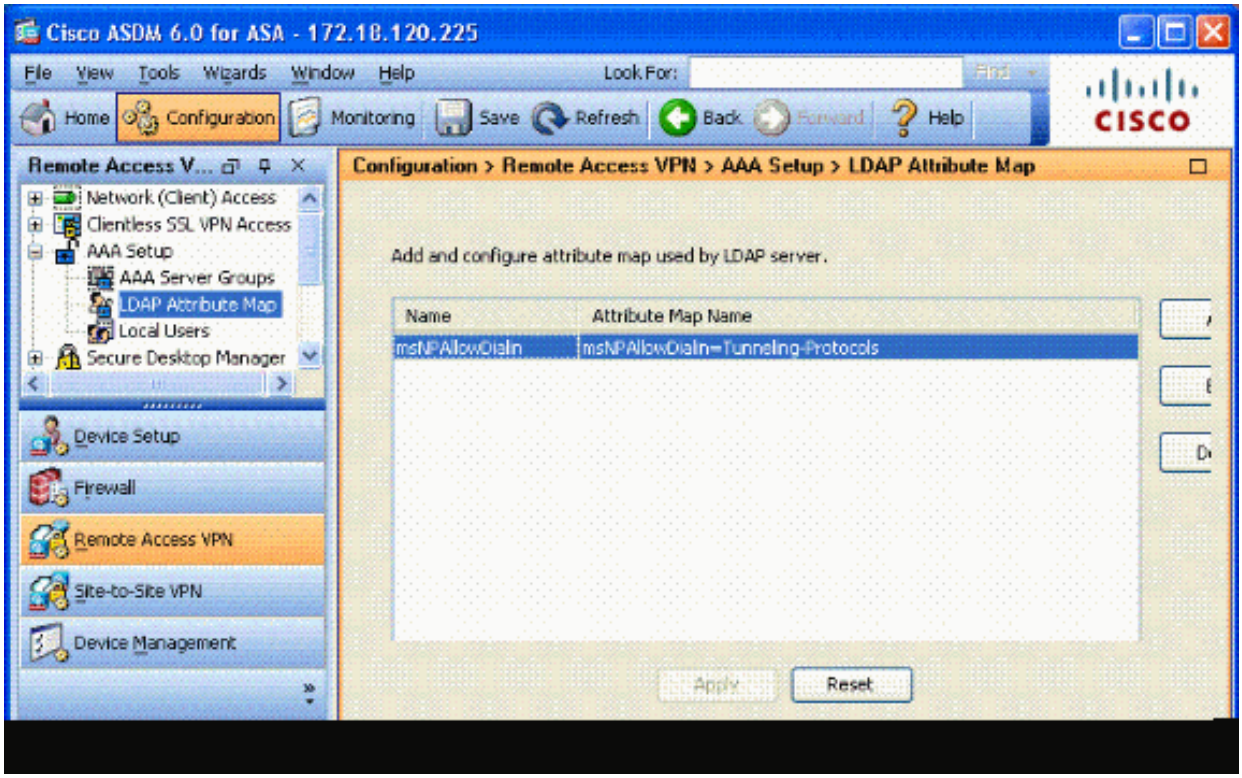
j. Klicken Sie auf OK.

k. Klicken Sie auf OK.

l. Klicken Sie auf Apply (Anwenden).

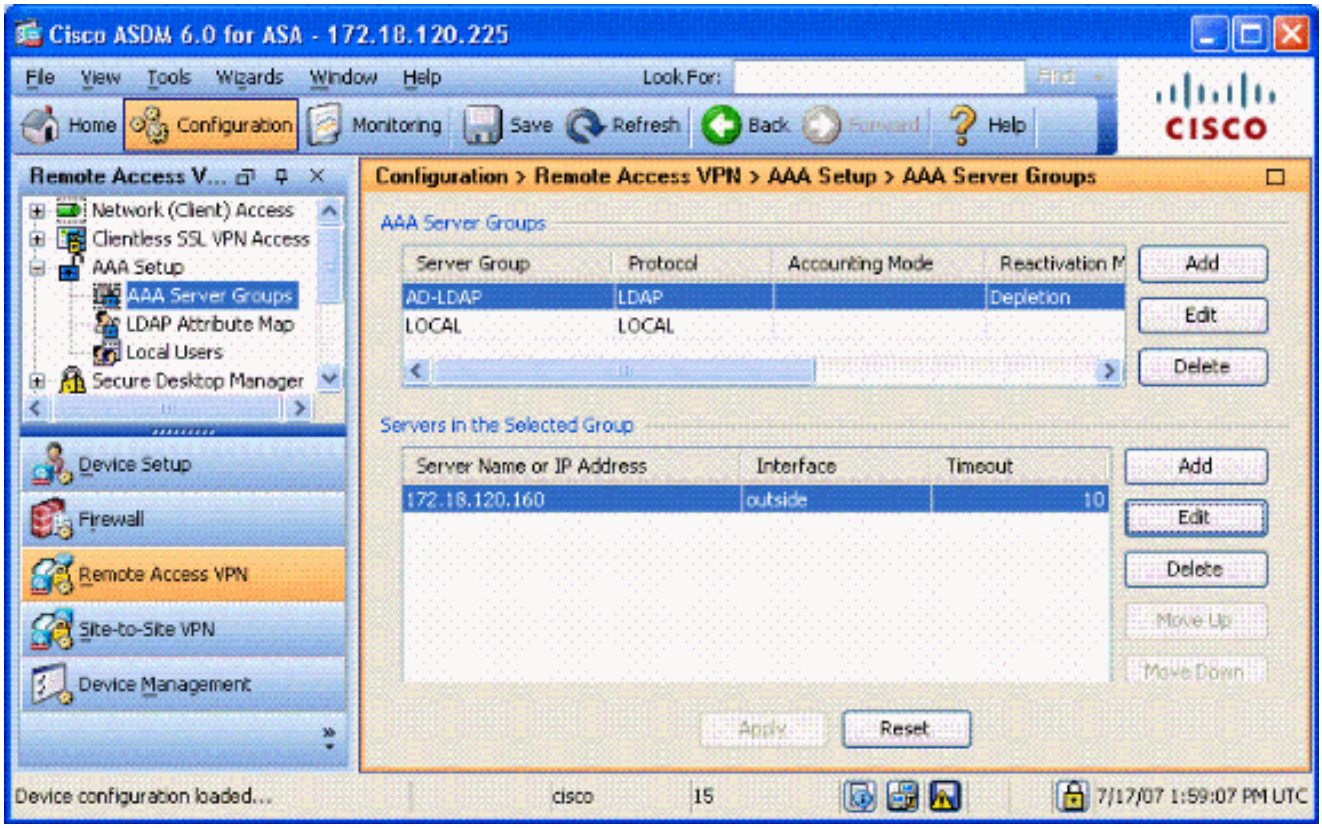
m. Die Konfiguration sollte wie in Abbildung A5 aussehen.

Abbildung A5: Konfiguration der LDAP-Attributzuordnung



4. Wählen Sie Remote Access VPN > AAA Setup > AAA Server Groups aus. Siehe Abbildung A6.

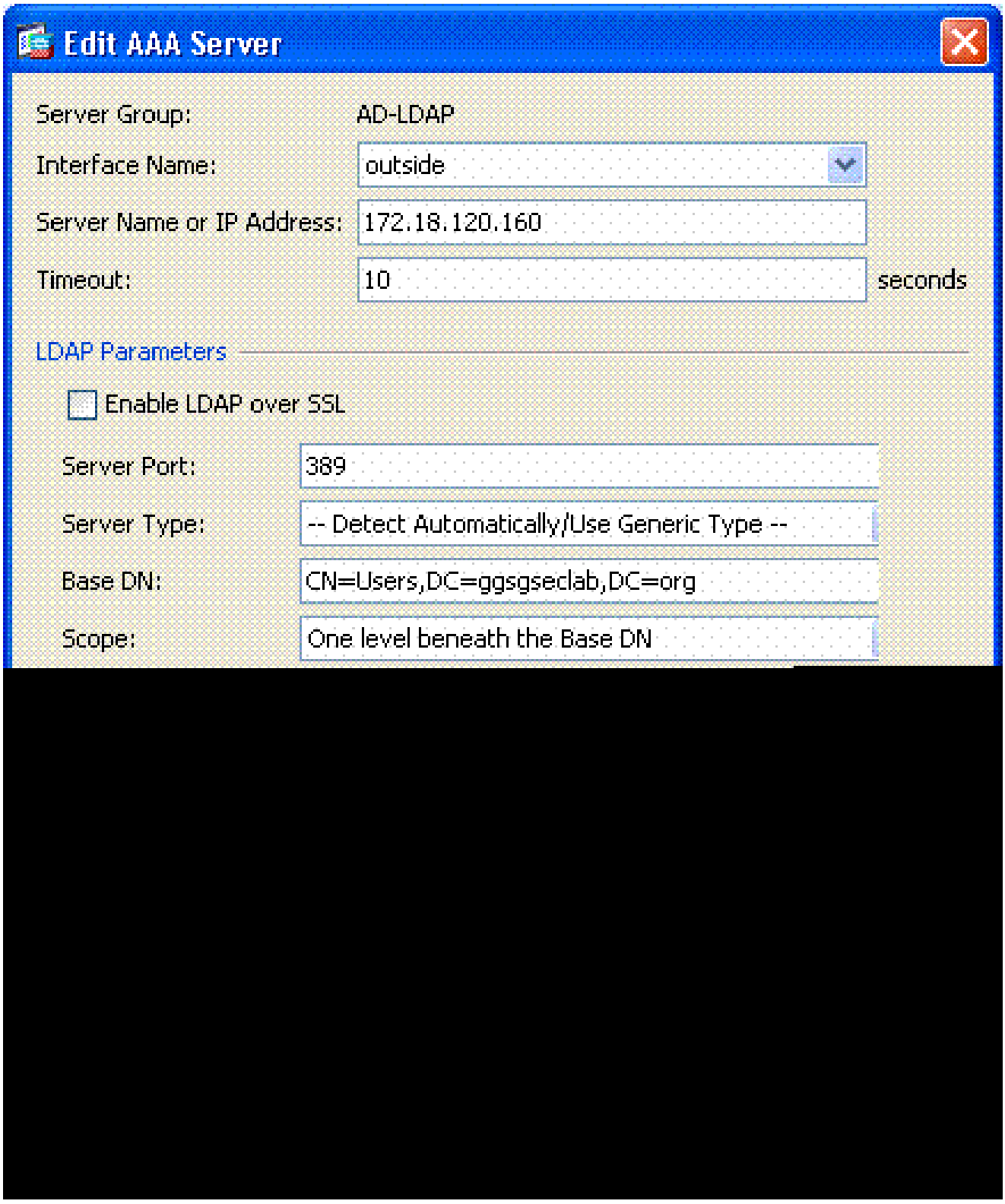
   Abbildung A6: AAA-Servergruppen



5. Klicken Sie auf die Servergruppe, die Sie bearbeiten möchten. Wählen Sie im Abschnitt "Servers in the Selected Group" (Server in der ausgewählten Gruppe) die IP-Adresse oder den Hostnamen des Servers aus, und klicken Sie dann auf Edit.

6. Wählen Sie im Fenster "AAA-Server bearbeiten" im Textfeld LDAP-Attributzuordnung die im Dropdown-Menü erstellte LDAP-Attributzuordnung aus. Siehe Abbildung A7

   Abbildung A7: Hinzufügen der LDAP-Attributzuordnung



7. Klicken Sie auf OK.

Hinweis: Aktivieren Sie während des Tests das LDAP-Debugging, um zu überprüfen, ob die LDAP-Bindung und die Attributzuordnung ordnungsgemäß funktionieren. Befehle zur Fehlerbehebung finden Sie in Anhang C.

Szenario 2: Active Directory-Durchsetzung mithilfe der Gruppenmitgliedschaft, um

den Zugriff zu erlauben/zu verweigern

In diesem Beispiel wird das LDAP-Attribut memberOf verwendet, um dem Tunneling Protocol-Attribut eine Gruppenmitgliedschaft als Bedingung zuzuordnen. Damit diese Richtlinie funktioniert, müssen folgende Bedingungen erfüllt sein:

- Verwenden Sie eine bereits vorhandene Gruppe, oder erstellen Sie eine neue Gruppe für ASA VPN-Benutzer, um Mitglied von für ALLOW-Bedingungen zu sein.
- Verwenden Sie eine bereits vorhandene Gruppe, oder erstellen Sie eine neue Gruppe für Nicht-ASA-Benutzer, um Mitglied für DENY-Bedingungen zu werden.
- Stellen Sie sicher, dass Sie im LDAP-Viewer die richtige DN für die Gruppe angegeben haben. Siehe Anhang D. Wenn der DN falsch ist, funktioniert die Zuordnung nicht richtig.

Hinweis: Beachten Sie, dass die ASA nur die erste Zeichenfolge des memberOf-Attributs in dieser Version lesen kann. Stellen Sie sicher, dass die neu erstellte Gruppe ganz oben in der Liste steht. Die andere Option besteht darin, ein Sonderzeichen vor den Namen zu setzen, da AD zuerst Sonderzeichen betrachtet. Um diese Einschränkung zu umgehen, verwenden Sie DAP in 8.x-Software, um mehrere Gruppen anzuzeigen.

Hinweis: Stellen Sie sicher, dass ein Benutzer der deny-Gruppe oder mindestens einer anderen Gruppe angehört, sodass memberOf immer an die ASA zurückgesendet wird. Sie müssen die Bedingung FALSE deny nicht angeben. Dies ist jedoch die beste Vorgehensweise. Wenn der vorhandene Gruppenname oder der Gruppenname ein Leerzeichen enthält, geben Sie das Attribut folgendermaßen ein:

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

Hinweis: Mit dem DAP kann die ASA mehrere Gruppen im memberOf-Attribut und die Basisautorisierung der Gruppen untersuchen. Siehe DAP-Abschnitt.

ZUORDNUNG

- Der AD-Attributwert:
    - memberOf CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
    - memberOf CN=TelnetClients,CN=Users,DC=labrat,DC=com
- Cisco Attributwert: 1 = FALSCH, 20 = WAHR,

Für den Zustand ZULÄSSIG ordnen Sie Folgendes zu:

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

Für den DENY-Zustand erstellen Sie eine Karte:

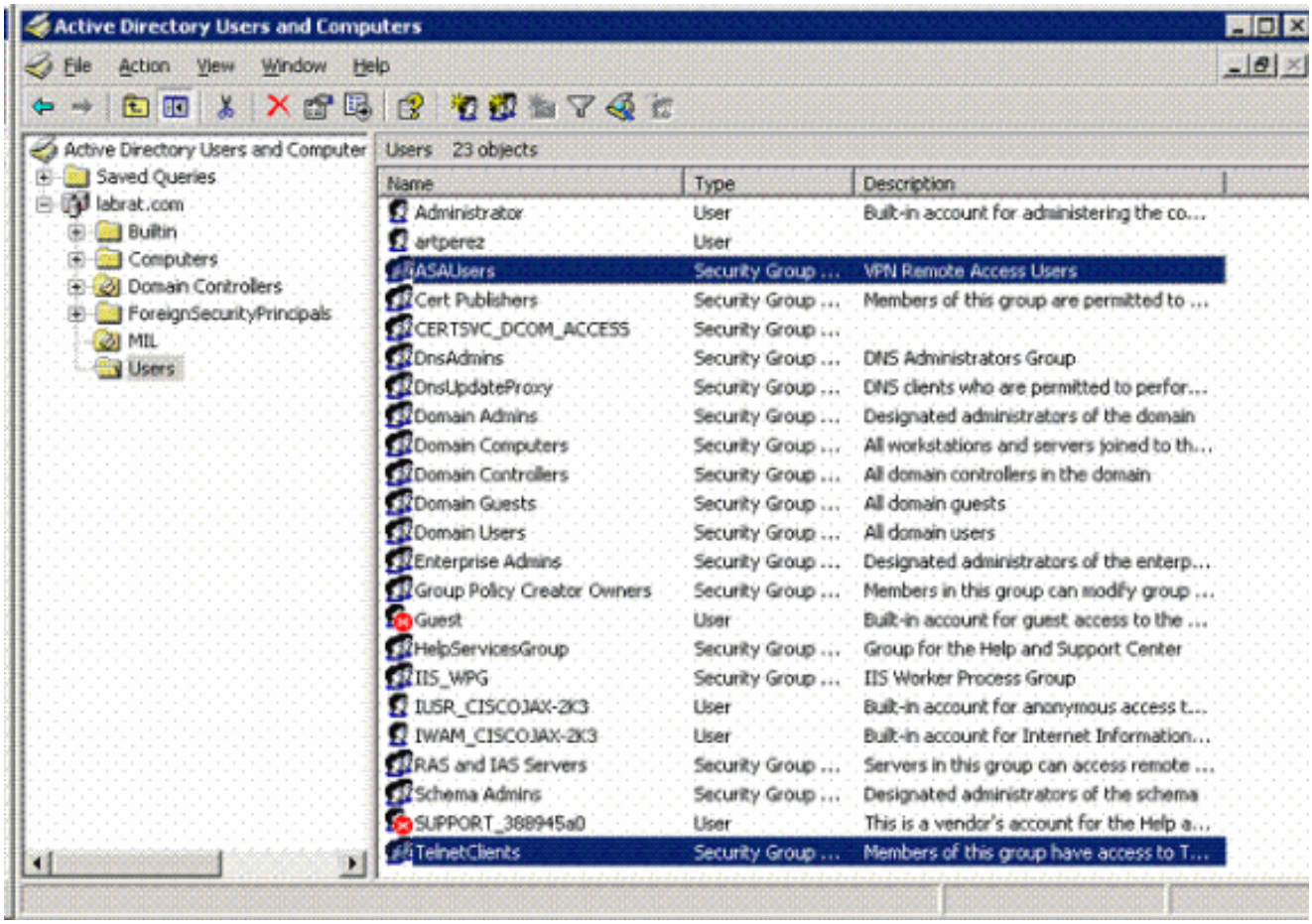
- memberOf CN=TelnetClients,CN=Users,DC=ggsgseclab,DC=org = 1

Hinweis: In einer zukünftigen Version gibt es ein Cisco-Attribut, um die Verbindung zu erlauben und zu verweigern. Weitere Informationen zu Cisco Attributen finden Sie unter Configuring an External Server for Security Appliance User Authorization.

Active Directory-Setup

1. Wählen Sie im Active Directory-Server Start > Ausführen aus.
2. Geben Sie in das Textfeld Öffnen den Text dsa.msc ein, und klicken Sie dann auf OK. Dadurch wird die Active Directory-Verwaltungskonsole gestartet.
3. Klicken Sie in der Active Directory-Verwaltungskonsole auf das Pluszeichen, um Active Directory-Benutzer und -Computer zu erweitern. Siehe Abbildung A8

   Abbildung A8: Active Directory-Gruppen



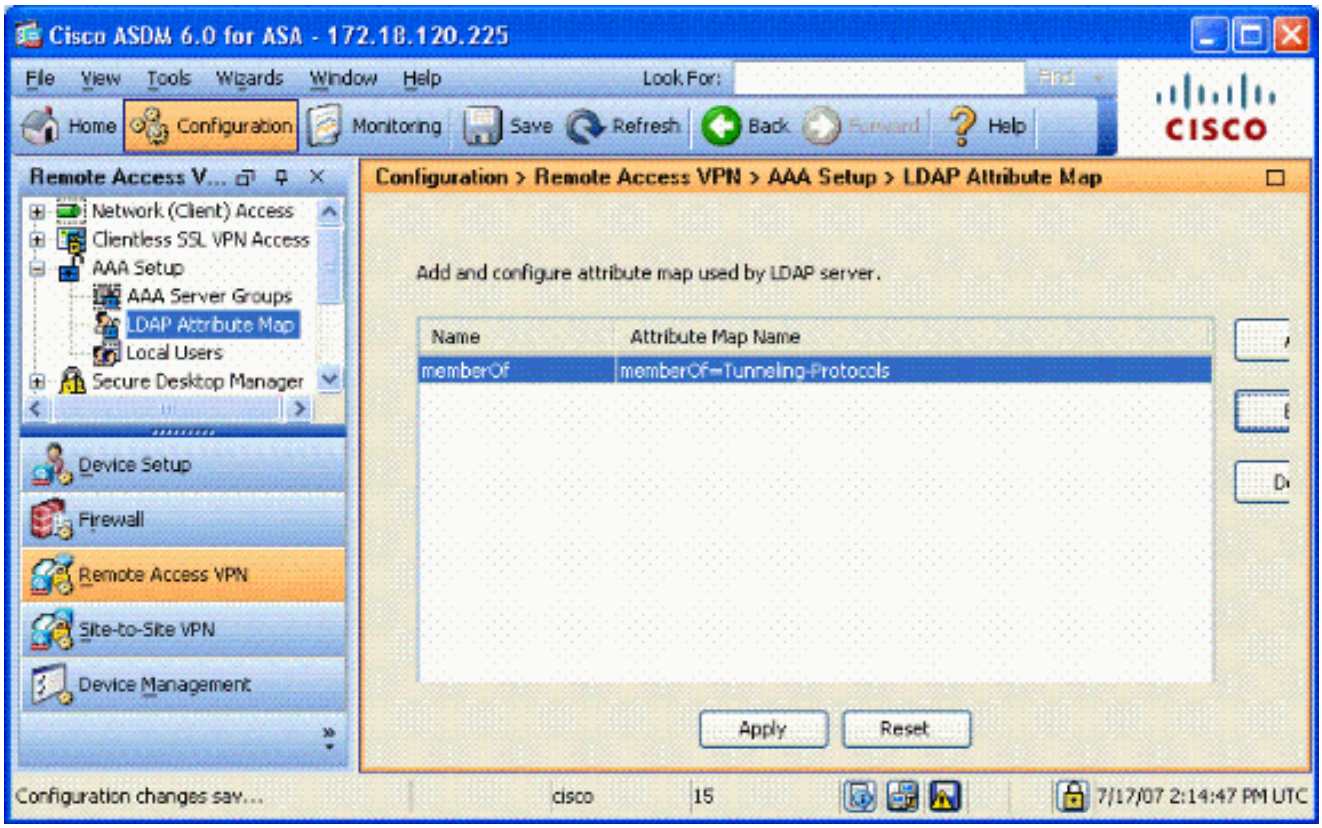
4. Klicken Sie auf das Pluszeichen, um den Domänennamen zu erweitern.
5. Klicken Sie mit der rechten Maustaste auf den Ordner Benutzer, und wählen Sie Neu > Gruppe aus.
6. Geben Sie einen Gruppennamen ein. Beispiel: ASAUsers.

7. Klicken Sie auf OK.
8. Klicken Sie auf den Ordner Benutzer und doppelklicken Sie dann auf die Gruppe, die Sie gerade erstellt haben.
9. Wählen Sie die Registerkarte Member aus, und klicken Sie dann auf Hinzufügen.
10. Geben Sie den Namen des Benutzers ein, den Sie hinzufügen möchten, und klicken Sie dann auf OK.

ASA-Konfiguration

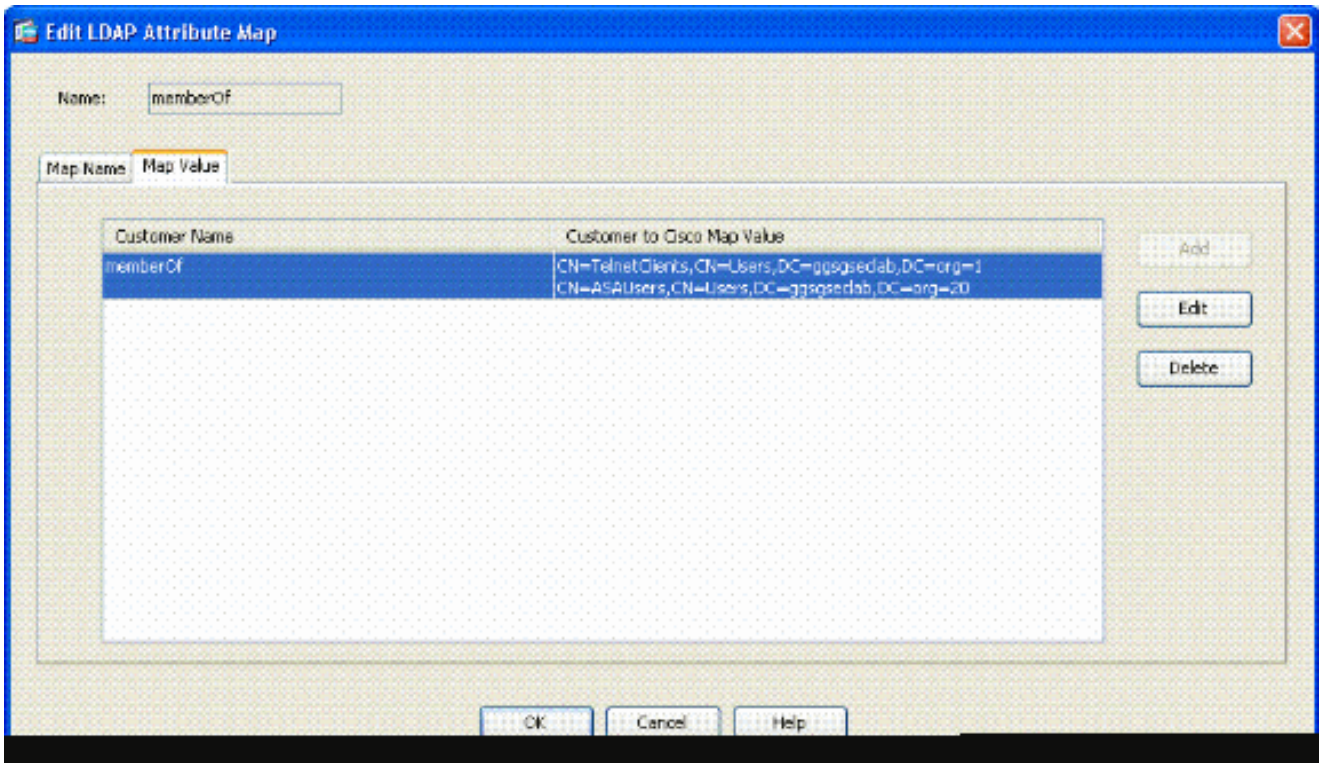
1. Wählen Sie im ASDM Remote Access VPN > AAA Setup > LDAP Attribute Map aus.
2. Klicken Sie auf Hinzufügen.
3. Führen Sie im Fenster LDAP-Attributzuordnung hinzufügen die folgenden Schritte aus. Siehe Abbildung A3.
    a. Geben Sie einen Namen in das Textfeld Name ein.
    b. Geben Sie auf der Registerkarte Zuordnungsname memberOf in das Textfeld Kundenname c ein.
    c. Wählen Sie auf der Registerkarte Map Name (Name der Zuordnung) Tunneling-Protocols aus der Dropdown-Option unter Cisco Name aus.
    d. Wählen Sie Hinzufügen aus.
    e. Klicken Sie auf die Registerkarte Kartenwert.
    f. Wählen Sie Hinzufügen aus.
    g. Geben Sie im Fenster Add Attribute LDAP Map Value (Wert für LDAP-Zuordnung hinzufügen) CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org in das Textfeld Customer Name ein, und geben Sie 20 in das Textfeld Cisco Value ein.
    h. Klicken Sie auf Hinzufügen.
    i. Geben Sie CN=TelnetClients,CN=Users,DC=ggsgseclab,DC=org in das Textfeld Kundenname ein, und geben Sie 1 in das Textfeld Cisco Wert ein. Siehe Abbildung A4.
    j. Klicken Sie auf OK.
    k. Klicken Sie auf OK.
    l. Klicken Sie auf Apply (Anwenden).
    m. Die Konfiguration sollte wie in Abbildung A9 aussehen.

Abbildung A9 LDAP-Attributzuordnung



4. Wählen Sie Remote Access VPN > AAA Setup > AAA Server Groups aus.

5. Klicken Sie auf die Servergruppe, die Sie bearbeiten möchten. Wählen Sie im Abschnitt "Server in der ausgewählten Gruppe" die IP-Adresse oder den Hostnamen des Servers aus, und klicken Sie dann auf Bearbeiten



6. Wählen Sie im Fenster "AAA-Server bearbeiten" im Textfeld LDAP-Attributzuordnung die im Dropdown-Menü erstellte LDAP-Attributzuordnung aus.

7. Klicken Sie auf OK.

Hinweis: Aktivieren Sie während des Tests das LDAP-Debugging, um zu überprüfen, ob die LDAP-Bindung und die Attributzuordnungen ordnungsgemäß funktionieren. Befehle zur Fehlerbehebung finden Sie in Anhang C.

Szenario 3: Dynamische Zugriffsrichtlinien für mehrere Attributelemente

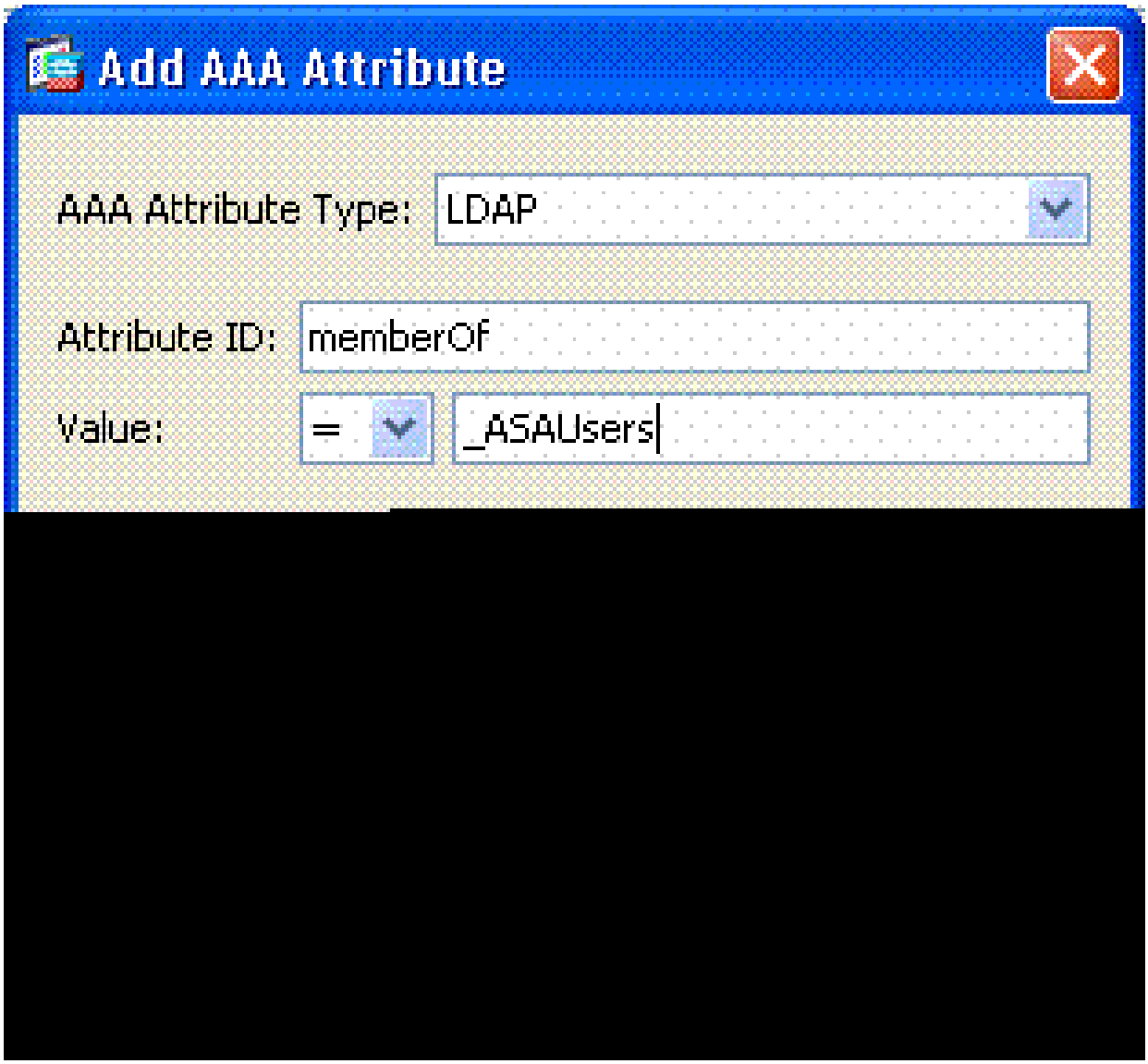
In diesem Beispiel wird DAP verwendet, um mehrere memberOf-Attribute zu überprüfen, um den Zugriff basierend auf der Active Directory-Gruppenmitgliedschaft zu ermöglichen. Vor 8.x hat die ASA nur das erste memberOf-Attribut gelesen. Mit 8.x und höheren Versionen kann die ASA alle memberOf-Attribute überprüfen.

- Verwenden Sie eine Gruppe, die bereits vorhanden ist, oder erstellen Sie eine neue Gruppe (oder mehrere Gruppen) für ASA VPN-Benutzer, um Mitglied von für ALLOW-Bedingungen zu sein.
- Verwenden Sie eine bereits vorhandene Gruppe, oder erstellen Sie eine neue Gruppe für Nicht-ASA-Benutzer, um Mitglied für DENY-Bedingungen zu werden.
- Stellen Sie sicher, dass Sie im LDAP-Viewer die richtige DN für die Gruppe angegeben haben. Siehe Anhang D. Wenn der DN falsch ist, funktioniert die Zuordnung nicht richtig.

ASA-Konfiguration

1. Wählen Sie im ASDM Remote Access VPN > Network (Client) Access > Dynamic Access Policies (Remote-Zugriffs-VPN > Netzwerkzugriff (Client) > Dynamic Access Policies (Dynamische Zugriffsrichtlinien) aus.
2. Klicken Sie auf Hinzufügen.
3. Führen Sie unter "Add Dynamic Access Policy" (Dynamische Zugriffsrichtlinie hinzufügen) die folgenden Schritte aus:
    a. Geben Sie einen Namen in das Textfeld Name b ein.
    b. Geben Sie im Prioritätsabschnitt 1 oder eine Zahl größer als 0 ein.
    c. Klicken Sie unter "Auswahlkriterien" auf Hinzufügen.
    d. Wählen Sie unter AAA-Attribut hinzufügen die Option LDAP aus.
    e. Geben Sie im Abschnitt "Attribut-ID" memberOf ein.
    f. Wählen Sie im Wertabschnitt die Option =, und geben Sie den AD-Gruppennamen ein. Wiederholen Sie diesen Schritt für jede Gruppe, auf die Sie verweisen möchten. Siehe Abbildung A10.

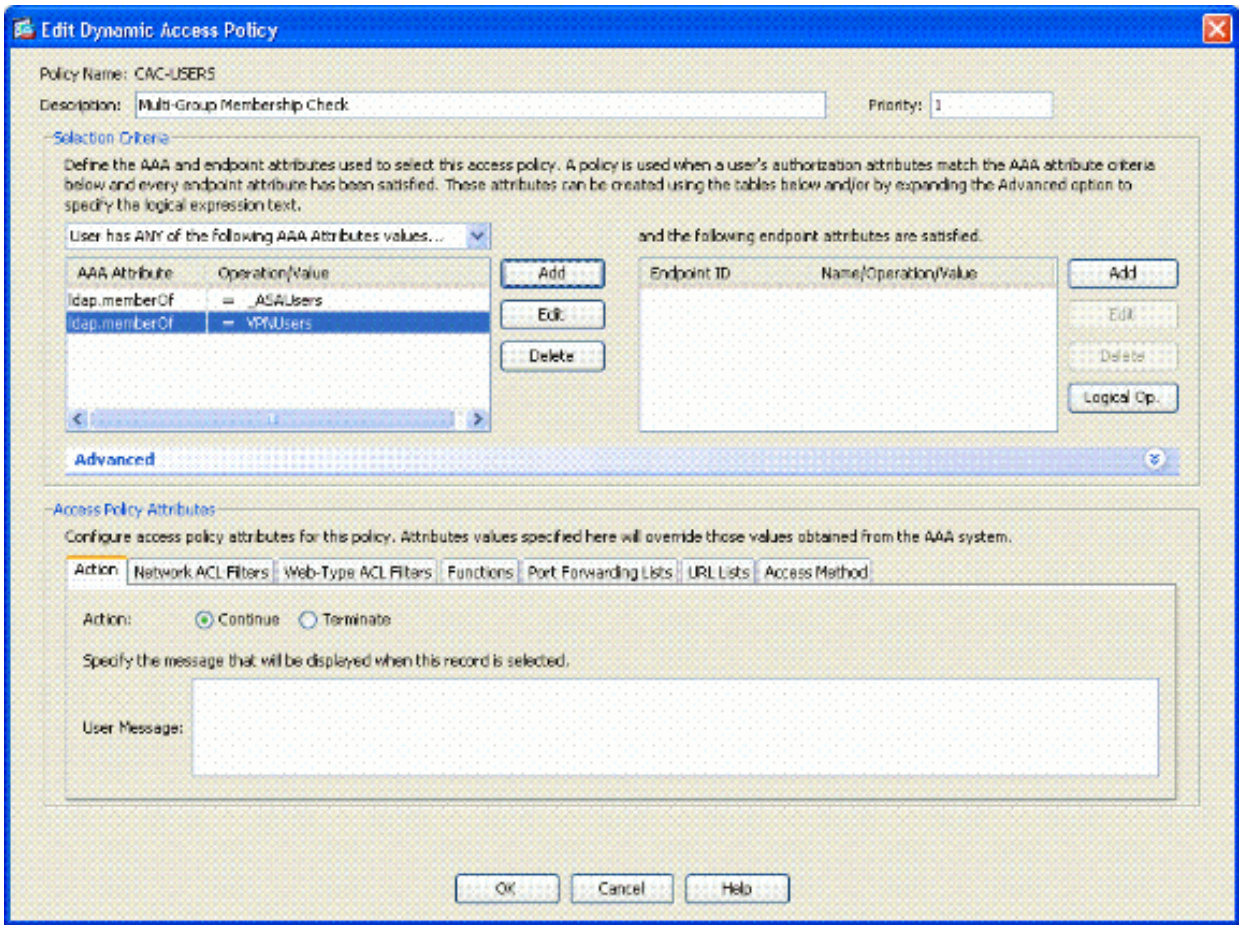
Abbildung AAA-Attributzuordnung A10



g. Klicken Sie auf OK.

h. Wählen Sie im Abschnitt "Access Policy Attributes" (Zugriffsrichtlinienattribute) die Option Continue (Weiter). Siehe Abbildung A11.

Abbildung A11 Hinzufügen einer dynamischen Richtlinie

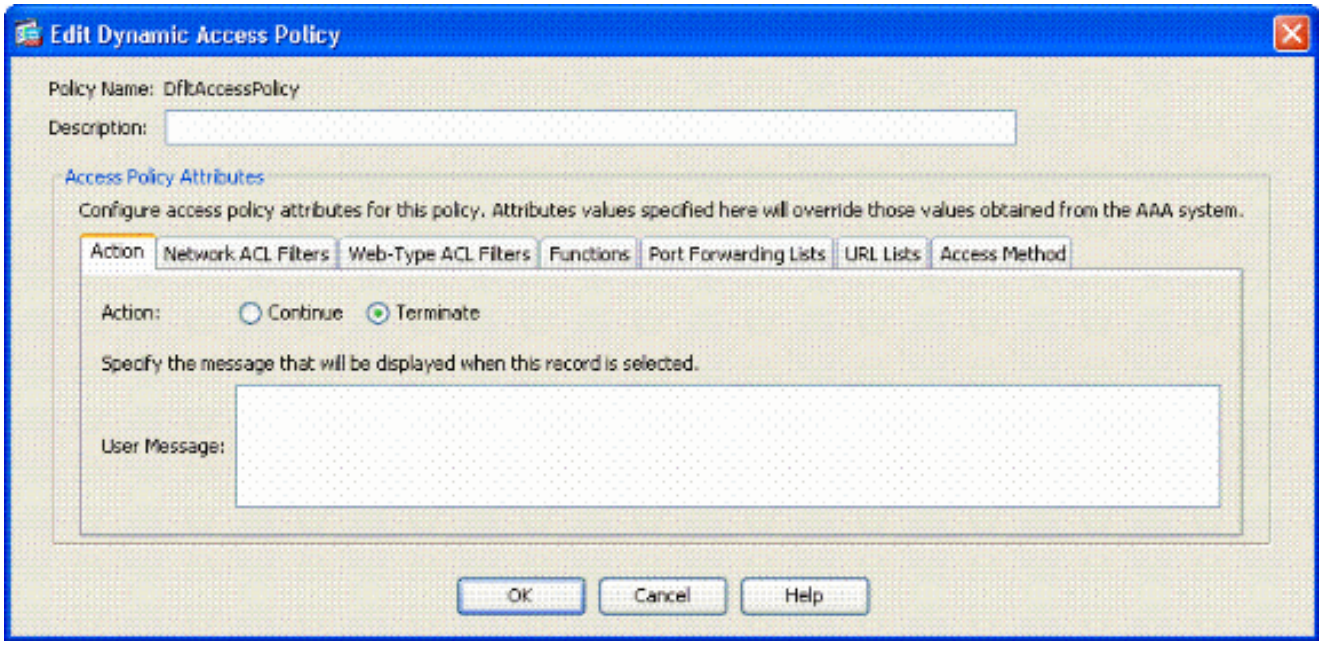


4. Wählen Sie im ASDM Remote Access VPN > Network (Client) Access > Dynamic Access Policies (Remote-Zugriffs-VPN > Netzwerkzugriff (Client) > Dynamic Access Policies (Dynamische Zugriffsrichtlinien) aus.

5. Wählen Sie Standard-Zugriffsrichtlinie aus, und wählen Sie Bearbeiten aus.

6. Die Standardaktion sollte auf "Beenden" gesetzt werden. Siehe Abbildung A12.

   Abbildung A12: Dynamische Richtlinie bearbeiten



7. Klicken Sie auf OK.

Hinweis: Wenn Beenden nicht ausgewählt ist, können Sie auch in anderen Gruppen teilnehmen, wenn diese nicht aktiviert sind, da der Standardwert Weiter lautet.

Anhang B: ASA CLI-Konfiguration

ASA 5510

```
<#root>

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-windows-----------------------------------
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-windows-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-windows-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
```

Anhang C: Fehlerbehebung

Fehlerbehebung: AAA und LDAP

- debug ldap 255: Zeigt LDAP-Austauschvorgänge an
- debug aaa common 10: Zeigt AAA-Austauschvorgänge an

Beispiel 1: Zulässige Verbindung mit korrekter Attributzuordnung

Dieses Beispiel zeigt die Ausgabe von debug ldap und debug aaa gemeinsam während einer erfolgreichen Verbindung mit Szenario 2 in Anhang A.

Abbildung C1: Debuggen von LDAP und Debuggen einer allgemeinen Ausgabe - korrekte Zuordnung

```
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#
```

Beispiel 2: Zulässige Verbindung mit falsch konfigurierter Cisco Attributzuordnung

Dieses Beispiel zeigt die Ausgabe von debug ldap und debug aaa common während einer zulässigen Verbindung mit Szenario 2 in Anhang A.

Abbildung C2: Debuggen von LDAP und Debuggen einer allgemeinen Ausgabe - falsche Zuordnung

```
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=org
[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
```

Fehlerbehebung - DAP

- debug dap errors: Zeigt DAP-Fehler an.
- debug dap trace: Zeigt die Ablaufverfolgung der DAP-Funktion an.

Beispiel 1: Zulässige Verbindung mit DAP

Dieses Beispiel zeigt die Ausgabe von debug dap-Fehlern und debug dap trace während einer erfolgreichen Verbindung mit Szenario 3 in Anhang A. Beachten Sie mehrere memberOf-Attribute. Sie können sowohl _ASAUsers als auch VPNUsers angehören, oder Sie können eine der beiden Gruppen wählen, je nach ASA-Konfiguration.

Abbildung C3: DAP debuggen

```
<#root>

#

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=org
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"]["physicalDeliveryOfficeName"] =
"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=org";
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.
```

Beispiel 2: Verweigerte Verbindung mit DAP

Dieses Beispiel zeigt die Ausgabe von debug dap errors und debug dap trace während einer nicht erfolgreichen Verbindung mit Szenario 3 in Anhang A.

Abbildung C4: DAP debuggen

```
<#root>
```

```
#

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=org
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"]["physicalDeliveryOfficeName"] =
"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=org";
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
```

Fehlerbehebung: Zertifizierungsstelle/OCSP

- debuggen crypto ca 3
- Im Konfigurationsmodus - logging class ca console(or buffer) debugging

Diese Beispiele zeigen eine erfolgreiche Zertifikatsvalidierung mit dem OCSP-Responder und eine fehlgeschlagene Zertifikatgruppen-Zuordnungsrichtlinie.

Abbildung C3 zeigt die Debugausgabe mit einem validierten Zertifikat und einer Arbeitszertifikatgruppe, die mit Policy übereinstimmt.

Abbildung C4 zeigt die Debugausgabe einer falsch konfigurierten Zertifikatgruppen-Zuordnungsrichtlinie.

Abbildung C5 zeigt die Debug-Ausgabe eines Benutzers mit einem gesperrten Zertifikat.

Abbildung C5: OCSP-Debugging - erfolgreiche Zertifikatsvalidierung

```
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
```

Abbildung C5: Ausgabe einer fehlerhaften Zertifikatgruppen-Zuordnungsrichtlinie

Abbildung C5: Ausgabe eines widerrufenen Zertifikats

```
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
```

Anhang D - Überprüfen von LDAP-Objekten in MS

Auf der Microsoft Server 2003-CD können zusätzliche Tools installiert werden, um die LDAP-Struktur sowie die LDAP-Objekte/Attribute anzuzeigen. Um diese Tools zu installieren, gehen Sie zum Verzeichnis Support auf der CD und dann zu Tools. Installieren Sie SUPTOOLS.MSI.

LDAP-Viewer

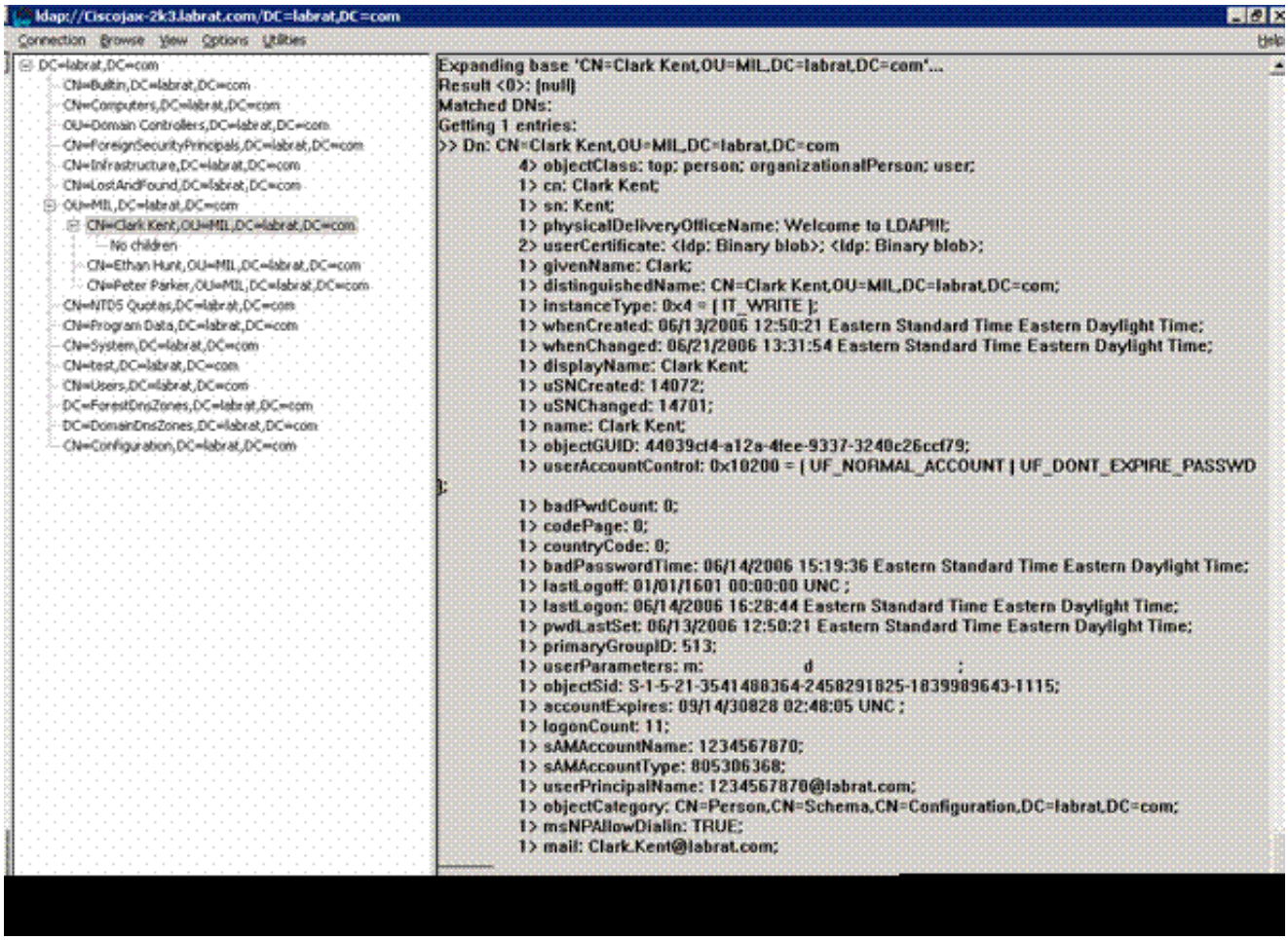
1. Wählen Sie nach der Installation Start > Ausführen.
2. Geben Sie ldp ein, und klicken Sie dann auf OK. Dadurch wird der LDAP-Viewer gestartet.
3. Wählen Sie Verbindung > Verbinden aus.
4. Geben Sie den Servernamen ein, und klicken Sie dann auf OK.
5. Wählen Sie Verbindung > Binden aus.
6. Geben Sie einen Benutzernamen und ein Kennwort ein.

   Hinweis: Sie benötigen Administratorrechte.

   ---

7. Klicken Sie auf OK.
8. Zeigt LDAP-Objekte an. Siehe Abbildung D1.

   Abbildung D1: LDAP-Viewer

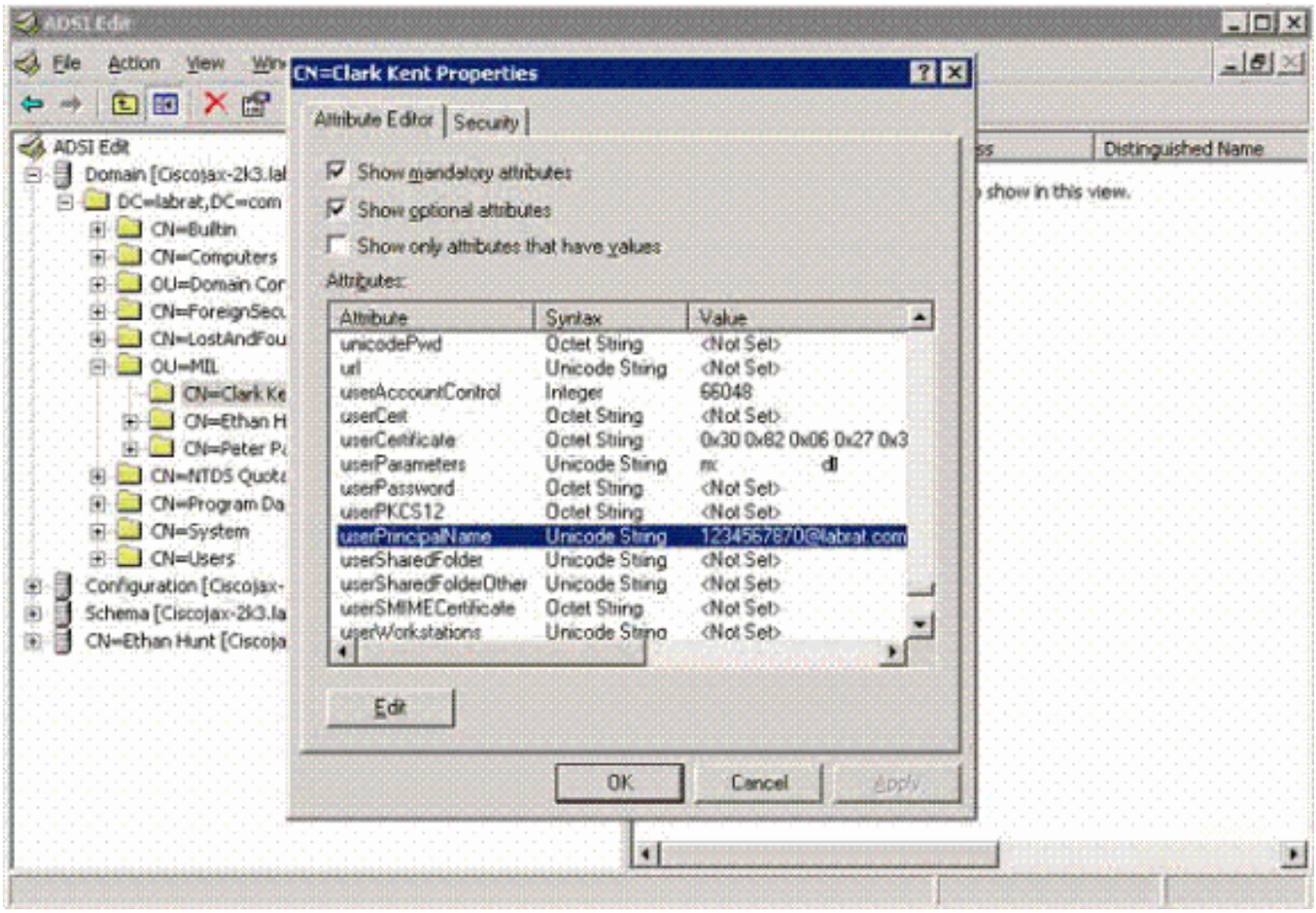


Active Directory Services-Schnittstellen-Editor

- Wählen Sie im Active Directory-Server Start > Ausführen aus.
- Geben Sie adsiedit.msc ein. Damit wird der Editor gestartet.
- Klicken Sie mit der rechten Maustaste auf ein Objekt, und klicken Sie auf Eigenschaften.

Dieses Tool zeigt alle Attribute für bestimmte Objekte an. Siehe Abbildung D2.

Abbildung D2: ADSI-Bearbeitung



Anhang E

Ein AnyConnect-Profil kann erstellt und einer Workstation hinzugefügt werden. Das Profil kann auf verschiedene Werte verweisen, z. B. ASA-Hosts oder Parameter für die Zertifikatzuordnung, z. B. Distinguished Name oder Issuer. Das Profil wird als XML-Datei gespeichert und kann mit Notepad bearbeitet werden. Die Datei kann jedem Client manuell hinzugefügt oder per Push über eine Gruppenrichtlinie von der ASA weitergeleitet werden. Die Datei wird gespeichert in:

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

Führen Sie diese Schritte aus:

1. Wählen Sie AnyConnectProfile.tmpl aus, und öffnen Sie die Datei im Editor.
2. Nehmen Sie entsprechende Änderungen an der Datei vor, z. B. am Aussteller oder an der Host-IP. Siehe zum Beispiel Abbildung F1.
3. Speichern Sie die Datei anschließend als XML.

Informationen zur Profilverwaltung finden Sie in der Dokumentation zu Cisco AnyConnect. Kurz

gesagt:

- Ein Profil muss eindeutig nach Ihrem Unternehmen benannt sein. Beispiel: CiscoProfile.xml
- Der Profilname muss gleich sein, auch wenn er für einzelne Gruppen innerhalb des Unternehmens unterschiedlich ist.

Diese Datei ist für die Verwaltung durch einen Secure Gateway-Administrator und die anschließende Verteilung an die Client-Software vorgesehen. Das auf dieser XML basierende Profil kann jederzeit an die Clients verteilt werden. Die unterstützten Verteilungsmechanismen werden als gebündelte Datei mit der Softwareverteilung oder als Teil des automatischen Downloadmechanismus bereitgestellt. Der automatische Downloadmechanismus ist nur bei bestimmten Cisco Secure Gateway-Produkten verfügbar.

> Hinweis: Administratoren wird dringend empfohlen, das von ihnen erstellte XML-Profil mit einem Online-Validierungstool oder über die Profilimport-Funktion in ASDM zu validieren. Die Validierung kann mit AnyConnectProfile.xsd durchgeführt werden, das sich in diesem Verzeichnis befindet. AnyConnectProfile ist das Stammelement, das das AnyConnect-Clientprofil darstellt.

Dies ist ein Beispiel für eine XML-Profildatei für den Cisco AnyConnect VPN Client.

```
<#root>

xml version="1.0" encoding="UTF-8"
- - <AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">


!--- The ClientInitialization section represents global settings !--- for the client. In some cases, fo
!--

-->
-
 <ClientInitialization>


!--- The Start Before Logon feature can be used to activate !--- the VPN as part of the logon sequence.


-->

<UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon>


!--- This control enables an administrator to have a one time !--- message displayed prior to a users t
```

```
<ShowPreConnectMessage>false</ShowPreConnectMessage>

!-- This section enables the definition of various attributes !--- that can be used to refine client ce


-->
-
<CertificateMatch>

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


- <DistinguishedName>
- <DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled">
<Name>ISSUER-CN</Name>
<Pattern>DoD-Issuer-ABC</Pattern>
</DistinguishedNameDefinition>
</DistinguishedName>
</CertificateMatch>
</ClientInitialization>

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

-
<ServerList>



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

-->
-
<HostEntry>
<HostName>host-02</HostName>
<HostAddress>host-02.dod.gov</HostAddress>
</HostEntry>
- <HostEntry>
<HostName>host-01</HostName>
<HostAddress>192.168.1.1</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

Zugehörige Informationen

- Zertifikate und Zertifikatsperrlisten gemäß X.509 und RFC 3280
- OCSP spezifiziert durch RFC 2560
- Einführung in Public Key-Infrastrukturen
- "Lightweight OCSP", profiliert nach Standardentwurf
- SSL/TLS gemäß RFC 2246

- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

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