## ASA 8.x: Konfiguration von AnyConnect SSL VPN CAC-SmartCards mit MAC-Unterstützung

### Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen **Cisco ASA-Konfiguration** Überlegungen zur Bereitstellung Konfiguration von Authentifizierung, Autorisierung, Abrechnung (AAA) LDAP-Server konfigurieren Zertifikate verwalten Schlüssel generieren Installation der Zertifizierungsstellenzertifikate ASA registrieren und Identitätszertifikat installieren **AnyConnect VPN-Konfiguration** Erstellen eines IP-Adresspools Erstellen von Tunnelgruppen- und Gruppenrichtlinien Tunnelgruppenschnittstelle und Bildeinstellungen Übereinstimmungsregeln für Zertifikate (wenn OCSP verwendet wird) Konfigurieren von OCSP Konfigurieren des OCSP-Responder-Zertifikats Konfiguration der CA zur Verwendung von OCSP Konfigurieren der OCSP-Regeln **Cisco AnyConnect Client-Konfiguration** Herunterladen des Cisco AnyConnect VPN-Clients - Mac OS X Starten Sie den Cisco AnyConnect VPN-Client - Mac OS X. Neue Verbindung Remote-Zugriff starten Anhang A: LDAP-Zuordnung und DAP Szenario 1: Active Directory-Durchsetzung mit Remote Access Permission Dial-in - Zugriff zulassen/verweigern Active Directory-Einrichtung **ASA-Konfiguration** Szenario 2: Active Directory-Durchsetzung durch Gruppenmitgliedschaft zum Zulassen/Verweigern des Zugriffs Active Directory-Einrichtung **ASA-Konfiguration** 

Szenario 3: Dynamische Zugriffsrichtlinien für mehrere Member von Attributen **ASA-Konfiguration** Anhang B: ASA CLI-Konfiguration Anhang C: Fehlerbehebung Fehlerbehebung AAA und LDAP Beispiel 1: Zulässige Verbindung mit korrekter Attributzuordnung Beispiel 2: Zulässige Verbindung mit falsch konfigurierter Cisco Attributzuordnung Fehlerbehebung DAP Beispiel 1: Zulässige Verbindung mit DAP Beispiel 2: Verbindung mit DAP verweigert Fehlerbehebung Zertifizierungsstelle/OCSP Anhang D: Überprüfen von LDAP-Objekten in MS LDAP-Viewer Active Directory Services-Schnittstelleneditor Anhang E Zugehörige Informationen

### **Einführung**

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

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

Die Konfiguration in diesem Handbuch verwendet Microsoft AD/LDAP-Server. Dieses Dokument behandelt außerdem erweiterte Funktionen wie OCSP, LDAP-Attributzuordnungen und Dynamic Access Polices (DAP).

### **Voraussetzungen**

#### Anforderungen

Ein grundlegendes Verständnis von Cisco ASA, Cisco AnyConnect Client, Microsoft AD/LDAP und Public Key Infrastructure (PKI) ist für das Verständnis der kompletten Einrichtung von Vorteil. Die Vertrautheit mit der AD-Gruppenzugehörigkeit, den Benutzereigenschaften und den LDAP-Objekten hilft bei der Korrelation des Autorisierungsprozesses zwischen Zertifikatattributen und AD/LDAP-Objekten.

#### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

• Cisco Adaptive Security Appliance (ASA) der Serie 5500 mit Softwareversion 8.0(x) und höher

- Cisco Adaptive Security Device Manager (ASDM) Version 6.x für ASA 8.x
- Cisco AnyConnect VPN Client 2.2 mit MAC-Unterstützung

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

#### **Konventionen**

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

### **Cisco ASA-Konfiguration**

Dieser Abschnitt behandelt die Konfiguration der Cisco ASA über ASDM. 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 User Principal Name (UPN)-Attribut im Zertifikat wird zur Autorisierung in das aktive Verzeichnis eingetragen.

#### Überlegungen zur Bereitstellung

- In diesem Leitfaden werden KEINE Basiskonfigurationen wie Schnittstellen, DNS, NTP, Routing, Gerätezugriff, ASDM-Zugriff usw. behandelt. Es wird davon ausgegangen, dass der Netzwerkbetreiber mit diesen Konfigurationen vertraut ist.Weitere Informationen finden Sie unter <u>Multifunktions-Sicherheitslösungen</u>.
- Bei den ROT hervorgehobenen Abschnitten handelt es sich um obligatorische Konfigurationen für den grundlegenden VPN-Zugriff. Beispielsweise kann ein VPN-Tunnel mit der CAC-Karte eingerichtet werden, ohne OCSP-Prüfungen, LDAP-Zuordnungen und Dynamische Zugriffsrichtlinien (DAP)-Prüfungen durchzuführen. Der DoD erfordert eine OCSP-Überprüfung, aber der Tunnel funktioniert ohne OCSP-Konfiguration.
- Die in BLAU hervorgehobenen Abschnitte sind erweiterte Funktionen, die integriert werden können, um dem Design mehr Sicherheit zu bieten.
- 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 belassen Sie 443 für AC/SSL VPN. Der ASDM-URL-Zugriff wurde in 8.x geändert. Verwenden Sie https://<ip\_address>:<port>/admin.html.
- Das erforderliche ASA-Image ist mindestens 8.0.2.19 und ASDM 6.0.2.
- AnyConnect/CAC wird von Vista unterstützt.
- Weitere Beispiele für die Richtliniendurchsetzung finden Sie in Anhang A.
- Siehe <u>Anhang D</u> zur Überprüfung von LDAP-Objekten in MS.
- Eine Liste der Anwendungsports für die Firewall-Konfiguration finden Sie unter Zugehörige Informationen.

# Konfiguration von Authentifizierung, Autorisierung, Abrechnung (AAA)

Sie werden mithilfe des Zertifikats in ihrer Common Access Card (CAC) über den DISAC Certification 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 autorisiert sein, ein Microsoft Active Directory- oder Lightweight Directory Access Protocol (LDAP)-Objekt zu verwenden. US-Verteidigungsministerium (DoD) benötigt zur Autorisierung das User Principal Name (UPN)-Attribut, das Teil des Abschnitts "Subject Alternative Name (SAN)" des Zertifikats ist. UPN oder EDI/PI müssen dieses Format haben: 1234567890@mil. Diese Konfigurationen zeigen, wie AAA-Server in der ASA mit einem LDAP-Server für die Autorisierung konfiguriert werden. Weitere Konfigurationen mit der LDAP-Objektzuordnung finden Sie <u>in Anhang A</u>.

#### **LDAP-Server konfigurieren**

Gehen Sie wie folgt vor:

- 1. Wählen Sie Remote Access VPN > AAA Setup > AAA Server Group aus.
- 2. Klicken Sie in der Tabelle "AAA-Servergruppen" auf Hinzufügen 3.
- 3. Geben Sie den Namen der Servergruppe ein, und wählen Sie im Optionsfeld Protokoll die Option LDAP aus. Siehe Abbildung 1.
- 4. Klicken Sie in der ausgewählten Gruppentabelle 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 LDAP/AD für diesen Verbindungstyp konfiguriert ist. Wählen Sie die Schnittstelle aus, auf der sich das LDAP befindet. Dieses Handbuch wird in der Schnittstelle angezeigt. Geben Sie die IP-Adresse des Servers ein. Geben Sie den Serverport ein. Der Standard-LDAP-Port ist 389. Wählen Sie Servertyp aus. Geben Sie Basis-DN ein. Fragen Sie Ihren AD/LDAP-Administrator nach diesen Werten. Abbildung 1

🗟 Add AAA Server Group 🛛 🛛 🔀			
Configure an AAA se for RADIUS and TAC	rver group. The Accounting Mode attribute is only applicable ACS+ protocols.		
Server Group:	AD-LDAP		
Protocol:	LDAP		
Accounting Mode:	💮 Simultaneous 🔘 Single		
Reactivation Mode:	<ul> <li>Depletion</li> <li>Timed</li> </ul>		
Dead Time: 10	initial minutes		
Max Failed Attempts:	3		
OK Cancel Help			

Wählen Sie

unter der Option Scope (Geltungsbereich) die entsprechende Antwort aus. Dies hängt von der Basis-DN ab. Fragen Sie Ihren AD/LDAP-Administrator um Hilfe.Geben Sie im Naming-

Attribut **userPrincipalName ein**. Dies ist das Attribut, das für die Benutzerautorisierung auf dem AD/LDAP-Server verwendet wird.Geben Sie in der Anmelde-DN den Administrator-DN ein.**Hinweis:** Sie haben Administratorrechte oder -rechte, um die LDAP-Struktur anzuzeigen/zu durchsuchen, die Benutzerobjekte und Gruppenmitgliedschaften umfasst.Geben Sie im Kennwort für die Anmeldung das Kennwort des Administrators ein.Lassen Sie das LDAP-Attribut **none.Abbildung 2** 

🚰 Add AAA Server				
Server Group:		AD-LDAP		
Interface Name:		outside		
Server Name or IP Addr	ess: 172.18.120.160			
Timeout:		10	seconds	
LDAP Parameters				
Enable LDAP over	SSL			
Server Port:	389			
Server Type:	De	etect Automatically/Use Generic Type 🔽		
Base DN:	CN=Users,DC=ggsgseclab,DC=org			
Scope:	One level beneath the Base DN			
Naming Attribute(s):	userPrincipalName			
Login DN:	lministrator, CN=Users, DC=ggsgseclab, DC=org			
Login Password:		•••••		
LDAP Attribute Map:	None			
SASL MD5 auther	iticati	on		
5ASL Kerberos au	ithent	ication		
Kerberos Server (	Group	:		
	OK	Cancel Help		

Sie verwenden diese Option später in der Konfiguration, um andere AD/LDAP-Objekte zur Autorisierung hinzuzufügen.Wählen Sie **OK aus**.

6. Wählen Sie OK aus.

### Zertifikate verwalten

Es gibt zwei Schritte, um Zertifikate auf der ASA zu installieren. Installieren Sie zunächst die erforderlichen CA-Zertifikate (Root and Subordinate Certificate Authority). Zweitens müssen Sie die ASA bei einer bestimmten Zertifizierungsstelle registrieren und das Identitätszertifikat abrufen.

Die DoD-PKI verwendet folgende Zertifikate: Root CA2, Class 3 Root, CA# Intermediate, bei dem die ASA angemeldet ist, ASA-ID-Zertifikat und OCSP-Zertifikat. Wenn Sie jedoch OCSP nicht verwenden möchten, muss das OCSP-Zertifikat *nicht* installiert werden.

**Hinweis:** Wenden Sie sich an Ihren Sicherheits-POC, um Root-Zertifikate zu erhalten, sowie an Anweisungen zur Anmeldung für ein Identitätszertifikat für ein Gerät. 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 mit Internet Explorer im Microsoft Certificate Store angezeigt werden. DoD hat eine Batch-Datei erstellt, die automatisch alle CAs zum Rechner hinzufügt. Fragen Sie Ihren PKI POC nach weiteren Informationen.

**Hinweis:** Der DoD CA2- und Class 3-Root sowie das ASA ID- und CA-Intermediär, das die ASA-Zertifizierung ausgestellt hat, sollten die einzigen CAs sein, die für die Benutzerauthentifizierung erforderlich sind. Alle aktuellen CA-Zwischenprodukte fallen unter die Root-Kette CA2 und Class 3 und sind vertrauenswürdig, solange die CA2- und Class 3-Roots hinzugefügt werden.

#### Schlüssel generieren

Gehen Sie wie folgt vor:

- 1. Wählen Sie Remote Access VPN > Certificate Management > Identity Certificate > Add aus.
- 2. Wählen Sie Neues ID-Zertifikat hinzufügen und dann Neu durch die Option Schlüsselpaar.
- 3. Geben Sie im Fenster Schlüsselpaar hinzufügen den Schlüsselnamen **DoD-1024 ein**. Klicken Sie auf das Optionsfeld, um einen neuen Schlüssel hinzuzufügen. Siehe Abbildung

	Enter new key pair pa	me: DoD-1024
ize:	1024	× •
lsage:	💿 General purpose	🚫 Special

#### 3.Abbildung 3

- 4. Wählen Sie die Größe des Schlüssels aus.
- 5. Halten Sie die Verwendung für allgemeine Zwecke.
- 6. Klicken Sie auf Jetzt generieren. Hinweis: DoD Root CA 2 verwendet einen 2048-Bit-Schlüssel. Ein zweiter Schlüssel, der ein 2048-Bit-Schlüsselpaar verwendet, sollte generiert werden, damit diese CA verwendet werden kann. Gehen Sie wie oben beschrieben vor, um eine zweite Taste hinzuzufügen.

Installation der Zertifizierungsstellenzertifikate

Gehen Sie wie folgt vor:

- 1. Wählen Sie Remote Access VPN > Certificate Management > CA Certificate > Add aus.
- 2. Wählen Sie Von Datei installieren, und wechseln Sie zum Zertifikat.
- 3. Wählen Sie Zertifikat installieren aus Abbildung 4: Installieren des Stammzertifikats

🕵 Install Certificate		
<ol> <li>Install from a file:</li> </ol>	C:\CAC\DOD-CERTS\ca13-jitc.cer	Browse
🔘 Paste certificate in	PEM format:	
O Use SCEP:		
SCEP URL: http://		
Retry Period:	1	minutes
Retry Count:	0	(Use 0 to indicate unlimited retries)
		More Options
Install Cer	tificate Cancel	Help

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

Schritte 1 bis 3 für jedes Zertifikat, das Sie installieren möchten. Für die DoD-PKI ist ein

Zertifikat für jedes der folgenden Elemente 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

Ele giew Couls Wigerus wincow	Felt		LcovEcr	
🕤 Home 🥵 Centigueation 💽 Mer	uteine 🔛 styp 🚱 R	ofinsh 🕜 Katik 💮 Krimens	🤣 нор	
Remote Access VPNK	Configuration > Report	e Access VPN ): Certificate Man	agement > CA Certificates	
🗟 🏧 Network (Client) Access 🗟 🌃 Cliendess SSL VPN Access				l (
E 🚽 222 Setup	ISSUED TO	150120 57	Example Usage	
🖶 🚰 Ferne Ferror Manade.	DoD CLASS 3 Pool CA	[m=0100485 - Rott ( A) ore	Den-ammer General Purpose	l dt
A Calificates	DOD JEC CA-13	Jun=DLC JITC ROLLCA 2; Lu=PKI	C2:55:53.UTC high/fure	how perais
				Reg est i Rt
- Here I alencing				Delete
High EFCP Server R DAN Server Server Server				
A Device Set_p				
Firevel				
CA Econote Access vPN				

#### ASA registrieren und Identitätszertifikat installieren

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

Add Identity Certification Management The Identity Certification	te icate from a file:	
Decryption Passphrase:		]
File to Import From:		Browse,
<ul> <li>Add a new identity certil</li> </ul>	icate:	
Key Pair:	DoD-1024	Show New
Certificate Subject DN:		Select
C Generate self-signed	l certificate	
Act as local certil	icate authority and issue dynamic (	certificates to TLS-Proxy
		Advanced
Add Certif	icate Cancel	Help

- 4. Wechseln Sie zum Feld DN des Zertifikats, und klicken Sie auf Auswählen.
- 5. Geben Sie im Fenster Certificate Subject DN (Zertifikatsfach-DN) die Informationen für das Gerät ein. Siehe Abbildung 8. Abbildung 8: DN bearbeiten

		Attribute	Value
- DN Allebute to be Added		Common Name (CN)	asa80
DN Attribute to be Added		Department (OU)	PKI
Attribute: Select Attribute 💙	Add>>	Department (OU)	DoD
Value	E CONTRACTOR OFFICE	Company Name (O)	U.S. Governmer
value;	Delete	Country (C)	US

- 6. Wählen Sie **OK aus.Hinweis:** Stellen Sie sicher, dass Sie den Hostnamen des Geräts verwenden, das in Ihrem System konfiguriert ist, wenn Sie die Betreffnummer hinzufügen. Der PKI POC kann Ihnen die erforderlichen Pflichtfelder mitteilen.
- 7. Wählen Sie Zertifikat hinzufügen aus.
- 8. Klicken Sie auf **Durchsuchen**, um das Verzeichnis auszuwählen, in dem die Anforderung gespeichert werden soll. Siehe Abbildung 9. **Abbildung 9 Zertifikatsanforderung**

🛸 Identity Certificate Request	
To complete the enrollment process, please save request (CSR) and send it to the CA.	e the PKCS10 enrollment
You will then need to install the certificate that is clicking the Install button in the Identity Certifica	returned from the CA by stes panel.
Save CSR to file:	Browse
OK Cancel	Help

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

🖹 ASA-8.0 - WordPad	
File Edit View Insert Format Help	
D 🚅 🖬 🎒 🗛 🐰 🖻 🛍 🗢 🦳	
MIIB1TCB/wIBADAmMQ4wDAYDVQQDEwVhc2E4MDEUMBIGCSqGSIb3DQEJAhYF ODAwg28wDQYJKoZIhvcNAQEBBQADgYOAMIGJAoGBAJqhuFdN12G7J3GCMcQ40 skELghwrraRMeB9iFJnLy10JYaUSAOvcededpeIUF7jUHYoIxS3v0Eby1VdvI +Z0DfU+wc1U+aA25yc6TnixGxppgxNYSU+4j6pgwui86Rk1+7BbVnJnJ+f3E) pMzBix7GetFRA8JsVvzvAgMBAAGgMDAuBgkqhkiG9w0BCQ4xITAfMAsGA1Ud) AwIFoDAQBgNVHREECTAHggVhc2E4MDANBgkqhkiG9w0BAQQFAA0BgQBmf8xS) QQF7TuEaUhmVaKfOBhupf+Y0Fm9Xt8T3GSSj1H/t+XB2cyLzNSthuZFVr5m9 jw31+jHv57zB1uDH3AYkM+Hru4yzgqBrgQBMCDIpmyCRp0E2pn2QaX/cD0xkd KgfJHq+2x3eVgvSxyKfhE71yFN3ResrSTg==	YXNh KT27 N75A Kclt DwQE nVTw 7cT9 qpv8
For Help, press F1	A state for the set of the

 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: Identitätszertifikat importieren

<u>File View Tools Wizards Window</u>	Help				ι
🐇 Home 🦓 Configuration 📴 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🔘 Excivered 🦻 Help					
Remote Access VPN 🗗 🕂 🗡	Configuration	> Remote Acc	ess VPN > Certifical	e Management > Iden	tity Certificate:
AAA Setup	Issued To	Issued By	Expiry Date	Usage	Add
Secure Desktop Manager	[asa80]	[[Not Available]	Pending	Unknown	Show Det
CA Certificates					
					Delete
Code Signer					Export
Local Certificate Authority	a da a da a d				( North of the second s
DHCP Server					Install
	le forterio				
🗄 🐻 Advanced					<u></u>
A Device Setup	Identity certificat configuration.	e can be used to	authenticate VPN acce	ss through the security ap	pliance. You can
Frowall					
CR Remote Access VPN					

11. Navigieren Sie im Fenster Zertifikat installieren zum ID-Zertifikat, und wählen SieZertifikat installieren aus. Siehe Abbildung 12. Abbildung 12: Installieren des Identitätszertifikats

🖆 Install Identity certif	ïicate	
Identity Certificate	\CAC\DOD-CERTS\asa80.txt	Browse
<ul> <li>Paste the certificate d</li> </ul>	ata in base-64 format:	
Install Certific	ate Cancel	Help

**Hinweis:** Es wird empfohlen, den ID-ZertifikatsTrustpoint zu exportieren, um die ausgestellten Zertifikatpaare und Schlüsselpaare zu speichern. Auf diese Weise kann der ASA-Administrator das Zertifikat und die Schlüsselpaare im Falle eines RMA- oder Hardwareausfalls in eine neue ASA importieren. Weitere Informationen finden Sie unter Exportieren und Importieren von Trustpoints.Hinweis: Klicken Sie auf **SPEICHERN**, um die Konfiguration im Flash-Speicher zu speichern.

### **AnyConnect VPN-Konfiguration**

Es gibt zwei Optionen zum Konfigurieren der VPN-Parameter im ASDM. Die erste Option ist die Verwendung des SSL VPN-Assistenten. Dies ist ein benutzerfreundliches Tool für Benutzer, die

noch keine VPN-Konfiguration haben. Die zweite Option besteht darin, dies manuell zu tun und jede Option zu durchlaufen. In diesem Konfigurationsleitfaden wird die manuelle Methode verwendet.

Hinweis: Es gibt zwei Methoden, um den AC-Client für den Benutzer bereitzustellen:

- 1. Sie können den Client von der Cisco Website herunterladen und auf dem Computer des Kunden 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 Handbuch wird die zweite Methode verwendet. Sobald der AC-Client dauerhaft auf dem Client-Rechner installiert ist, starten Sie den AC-Client einfach von der Anwendung aus.

#### 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 ein, starten und beenden Sie die IP-Adresse, und wählen Sie eine Subnetzmaske aus. Siehe Abbildung 13. Abbildung 13: Hinzufügen von IP-Pool

🖆 Add IP Pool	
Name:	CAC-USERS
Starting IP Address:	192.168.1.1
Ending IP Address:	192,168,1,254
Subnet Mask:	255.255.255.0
ок	Cancel Help

- 4. Wählen Sie OK.
- 5. Wählen Sie Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy (Remote-Zugriffs-VPN > Netzwerkzugriff (Client) > Adressenzuweisung > Zuweisungsrichtlinie.
- 6. Wählen Sie die entsprechende Methode für die IP-Adresszuweisung aus. In diesem

Leitfaden werden die internen Adresspools verwendet. Siehe Abbildung 14. Abbildung 14: IP-Adressenzuweisungsmethode



7. Klicken Sie auf Übernehmen.

#### Erstellen von Tunnelgruppen- und Gruppenrichtlinien

#### Gruppenrichtlinie

**Hinweis:** Wenn Sie keine neue Richtlinie erstellen möchten, können Sie die standardmäßig integrierte Gruppenrichtlinie verwenden.

- 1. Wählen Sie Remote Access VPN -> Network (Client) Access -> Group Policies (Remote-Zugriffs-VPN -> Netzwerkzugriff -> Gruppenrichtlinien aus.
- 2. Klicken Sie auf Hinzufügen, und wählen Sie Interne Gruppenrichtlinie aus.
- Geben Sie im Fenster Richtlinie f
  ür interne Gruppen hinzuf
  ügen im Textfeld Name den Namen f
  ür die Gruppenrichtlinie ein. Siehe Abbildung 15. Abbildung 15: Hinzuf
  ügen von Richtlinien f
  ür interne Gruppen

5	Add Internal Group Poli	cy							×
	General	Name:	AC-USERS						
		Banner:	🔽 Inherit						
		Address Pools:	🗌 Inherit	CAC-USE	RS			Select	
		More Option	s					۲	
		Tunneling Pro	tocols:	🗌 Inherit	Clientless SSL VPN	SSL VPN Client	IPsec	L2TP/IPsec	
		Filter:		🔽 Inherit				Manage	
		NAC Policy:		🔽 Inherit				Manage	
		Access Hours:		🔽 Inherit				Manage	
		Simultaneous	Logins:	🕑 Inherit					
		Restrict acces	s to VLAN:	🖌 Inherit					
		Maximum Con	nect Time:	🖌 Inherit	Unimited	mnutes			
		Idle Timeout:		🔽 Inherit	Unimited	mnutes			
	la de la della d		ОК		ancel Help				

Wählen Sie auf der Registerkarte Allgemein die Option **SSL VPN Client in Tunneling Protocols** aus, es sei denn, Sie verwenden andere Protokolle wie Clientless SSL.Deaktivieren Sie im Abschnitt Servers das Kontrollkästchen **Erben** und geben Sie die IP-Adresse der DNS- und WINS-Server ein. Geben Sie ggf. den DHCP-Bereich ein.Deaktivieren Sie im Abschnitt Server das Kontrollkästchen **Erben** in der Standarddomäne, und geben Sie den entsprechenden Domänennamen ein.Deaktivieren Sie auf der Registerkarte Allgemein das Kontrollkästchen **Erben** im Adresspoolbereich, und fügen Sie den im vorherigen Schritt erstellten Adresspool hinzu. Wenn Sie eine andere Methode der IP-Adresszuweisung verwenden, lassen Sie diese zu erben und nehmen Sie die entsprechende Änderung vor.Auf allen anderen Konfigurationsregisterkarten werden die Standardeinstellungen beibehalten.**Hinweis:** Es gibt zwei Methoden, um den AC-Client für Endbenutzer bereitzustellen. Eine Möglichkeit ist, den AC-Client auf Cisco.com herunterzuladen. Die zweite Methode besteht darin, dass die ASA den Client zum Benutzer herunterlädt, wenn der Benutzer versucht, eine Verbindung herzustellen. In diesem Beispiel wird die letztgenannte Methode veranschaulicht.

4. Wählen Sie anschließend Erweitert > SSL VPN Client > Login Settings aus. Siehe Abbildung 16. Abbildung 16: Hinzufügen von Richtlinien für interne Gruppen

🐔 Edit Internal Group Pol	icy: AC-USERS
General Servers Advanced Split Tunneling IE Browser Proxy SSL VPN Client Cogn Setting Key Regeneration Dead Peer Detecti Customization TPsec Client	After successfully logging in, user can have the choice to download the clent software, or go to clentless SSL VPN prival page. The following settings decides what will happen.         Inherit         Post Logn Setting <ul> <li>Do not prompt user to choose</li> <li>Prompt user to choose</li> <li>Default Post Logn Selecton</li> </ul> <ul> <li>On to Clentless SSL VPN portal</li> <li>Download SSL VPN Clent</li> </ul>
	OK Cancel Help

Deaktivieren Sie das Kontrollkästchen **Erben**.Wählen Sie die für Ihre Umgebung geeigneten Einstellungen nach der Anmeldung aus.Wählen Sie die für Ihre Umgebung passende Standard-Post-Login-Auswahl aus.Wählen Sie **OK aus**.

#### Tunnelgruppenschnittstelle und Bildeinstellungen

Hinweis: Wenn Sie keine neue Gruppe erstellen möchten, können Sie die standardmäßig integrierte Gruppe 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-Image festlegen?
- 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 Upload (Hochladen) und suchen Sie nach der Datei auf dem lokalen Computer. Siehe Abbildung 17. Die Dateien können von Cisco.com heruntergeladen werden. Es gibt eine Windows-, MAC- und Linux-Datei.Abbildung 17: SSL VPN-Client-Image hinzufügen

🚰 Add SSL VPN Client Image	
Flash SVC Image:	Browse Flash
	Upload
OK Cance	Help

6. Aktivieren Sie anschließend Zugriff zulassen, Client-Zertifizierung erforderlich und optional DTLS aktivieren. Siehe Abbildung 18. Abbildung 18: Aktivieren des Zugriffs

📫 Cisco ASDM 6.0 for ASA - 173	2.18.120.225				
Ele Yew Iools Wigards Windo	w Help fonitoring 🔛 Save	Refresh	Look For: Back OForward ? Help	n in the second se	ahaha cisco
Remote Access V 🗇 🗘 ×	Configuration > R	emote Access VPN	> Network (Client) Access >	SSL VPN Connection	on Profiles 🛛
Network (Client) Access	The security appli users upon come VPN Client suppor (More client-relat Access Interfaces IV Enable Cisco -	ance automatically dep action. The initial client of ts the HTTP5/TCP (SSL red parameters, such a AnyConnect VPN Client	loys the Cisco AnyConnect VPN C leployment requires end-user adr ) and Datagram Transport Layer : s client images and client profiles, or legecy SSL VPN Client access o	Tent or legacy SSL VPN ministrative rights. The C Security (DTLS) tunnelin , can be found at <u>client</u> ) on the interfaces selecte	Client to remote Jisco AnyConnect g aptions. Settings.) d in the table below
Connection Profiles	Interface	Allow Access	Require Client Certificate	Enable DTLS	
A Device Setup	outside				
🚮 Firewall	in <u>deste dest</u>				<u>1995</u>
Remote Access VPN           Ste-to-Site VPN	Access Port: 443 Click here to Ass	DTLS Po	rt: 443		
Device <u>M</u> anagement	Connection Profiles		Apply Reset	)	
Configuration changes saved successful	Y	CISCO	15 🕠 😼	01 🔂	23/07 2:09:48 AM UTC

- 7. Klicken Sie auf Übernehmen.
- 8. Erstellen Sie anschließend ein Verbindungsprofil/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

E	Add SSL VPN Connecti	on Profile		<b>X</b>
	Basic H-Advapred	Name:	AC-USER5	
		Aliases:		
		Authentication		
		Method:	○ AAA ④ Certificate ○ Both	
		AAA Server Group:		Manage
			Use LOCAL If Server Group Fels	
		Client Address Assignent		
		DHCP Servers:		
		Client Address Pools:		Select
		Default Group Policy		
		Group Policy:	AC-USERS 🗸	Manage
		SSL VPN Client Protocol:	C Enabled	
		OK	Cancel Help	

Geben Sie der Gruppe einen Namen.Wählen Sie Certificate in der

Authentifizierungsmethode aus.Wählen Sie die zuvor erstellte Gruppenrichtlinie aus.Stellen Sie sicher, dass der **SSL VPN-Client** aktiviert ist.Lassen Sie andere Optionen als Standard.

10. Wählen Sie anschließend Erweitert > Autorisierung aus. Siehe Abbildung 20Abbildung 20: Autorisierung

🖆 Edit SSL VPN Connecti	on Profile: AC-	USERS			E Contraction (Contraction)	<
Basic	Default Authoriza	ition Server Group				
-Advanced	Server Group:	AD-LDAP		Manage		
Client Addressing Authentication		Users must exist in	in the authoriz	ation database to conne	t	
Accounting	Interface-specific	Authorization Server	Groups			
SSL VPN	🗣 Add 🏢	dt Delete				
	Interface			Server Group		
	User Name Mappi	ng				
	🔿 Use the en	tire DN as the usernam	ne			
	<ul> <li>Specify ind</li> </ul>	ividual DN fields as the	e username			
	Primary DN	Field: UPN (User's	s Principal Nam	ne)		
	Secondary	DN Field: None		<b>~</b>		
		OK Cance	ы	lelp		

Wählen Sie die zuvor erstellte AD-LDAP-Gruppe aus. Überprüfen Sie, **ob Benutzer vorhanden sein müssen...um eine Verbindung herzustellen.** Wählen Sie in den Zuordnungsfeldern **UPN** für den primären und **keinen** für den sekundären Modus aus.

- 11. Wählen Sie im Menü den Abschnitt SSL VPN aus.
- 12. Gehen Sie im Abschnitt VerbindungsAliase wie folgt vor: Abbildung 21: VerbindungsAliase

🚰 Edit SSL VPN Connection	Profile: AC-USERS		
-Basic	Portal Page Customization:	DfltCustomization	Manage
General	CSD Alternate Group Policy:	DfltGrpPolicy	Manage
Client Addressing Authentication	Enable the display of Rad	dius Reject-Message on the login screen when authent	cation is rejected
Accounting	onnection Aliases		
SSL VPN	💠 Add 📝 Delete		
	Alias	Enabled	
	AC-USERS	<b>∀</b>	
	roun I PL c		
	Add Colete		
		Fachlad	
	URL	Enabled	
			00000000000
· · · · · · · · · · · · · · · · · · ·			
	OK	Cancel Help	

Wählen Sie **Hinzufügen aus**.Geben Sie den zu verwendenden Gruppenalias ein.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.

#### Übereinstimmungsregeln für Zertifikate (wenn OCSP verwendet wird)

 Wählen Sie Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps aus. Siehe Abbildung 22.Wählen Sie Add im Abschnitt Certificate to Connection Profile Maps (Zertifikat zu Verbindungsprofilzuordnungen hinzufügen) aus.Sie können die vorhandene Map als DefaultCertificateMap im Map-Abschnitt beibehalten oder eine neue erstellen, wenn Sie bereits Zertifizierungen für IPsec verwenden.Behalten Sie die Regelpriorität bei.Gehen Sie unter Zugeordneter Gruppe als — Nicht zugeordnet — fort. Siehe Abbildung 22.Abbildung 22: Hinzufügen einer Regel für die Zertifikatszuordnung

Configure a certificate Matchi Configure a certificate match rule priority uniquely identifie to the rule with lower values will be ignored.	ng Rule ing rule and associa s the certificate ma having greater prio	te it with a connection profile. The tching rule and assigns a priority rity. Rules that are not mapped
Map:	<ul> <li>Existing</li> </ul>	DefaultCertificateMap
	🚫 New	
Priority:	20	
Mapped to Connection Profile	: Not Mapped	
CHILLI OK IN	Cancel	

Sie auf OK.

- 2. Klicken Sie in der unteren Tabelle auf Hinzufügen.
- 3. Gehen Sie wie folgt vor, um im Fenster Zertifikat-Matching-Regelkriterien hinzufügen zu verfahren: Abbildung 23: Regelkriterien für Übereinstimmung mit Zertifikaten

Add Certificate	Matching Rule Criterion		
Configure a certific	ate matching rule criterion		
Rule Priority:	20		
Mapped to Connect	tion Profile: Not Mapped		
Field	Component	Operator	Value
The second s	and states to a		imi statistististististist
Subject		Does Not Equal	

Behalten Sie die Spalte Feld in **Betreff**.Behalten Sie die Spalte Komponente im **Feld Gesamtes Feld**.Ändern Sie die Spalte Operator in **Nicht gleich**.Geben Sie in der Spalte Wert zwei doppelte Anführungszeichen ein "".Klicken Sie auf **OK** und **Übernehmen**. Siehe Abbildung 23.

### Konfigurieren von OCSP

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

#### Konfigurieren des OCSP-Responder-Zertifikats

- 1. Erhalten Sie ein selbst erstelltes Zertifikat vom OCSP-Responder.
- 2. Führen Sie die zuvor genannten Verfahren aus, und installieren Sie ein Zertifikat für den

OSCP-Server.**Hinweis:** Stellen Sie sicher, dass **Zertifikate nicht auf Widerruf überprüft** werden, für den Vertrauensbereich des OCSP-Zertifikats ausgewählt ist.

#### Konfiguration der CA zur Verwendung von OCSP

- 1. Wählen Sie Remote Access VPN > Certificate Management > CA Certificates aus.
- 2. Markieren Sie einen OCSP, um eine CA auszuwählen, die für die Verwendung von OCSP konfiguriert werden soll.
- 3. Klicken Sie auf Bearbeiten.
- 4. Stellen Sie sicher, dass Check certificate for revocation aktiviert ist.
- 5. Fügen Sie im Abschnitt Widerrufsmethoden OCSP hinzu. Siehe Abbildung 24.OCSP-Widerrufsprüfung

	CRL Retrieval Policy	CRL Retrieval Method	OCSP Rules	Advanced	
Do not check     Oneck certification	certificates for revoca ates for revocation	tion			
Revocation Me	athods				
Specify the method will	methods used for revi be used only if the firs	ocation checking and the t one returns error.	ir order. If bo	th methods are sel	ected, the second
CRL		Add>>	DCSP		Move Up
		< <remove< td=""><td></td><td></td><td>Move Down</td></remove<>			Move Down
Cooside	r cortificato valid é roj	ocation information can	not be retrieve	a	
		ocadori ni chinacion can	not be retrieve	24	

6. Stellen Sie sicher, dass **Consider Certificate gültig ist...kann nicht abgerufen werden**, deaktiviert ist, wenn Sie eine strenge OCSP-Prüfung befolgen möchten.

Hinweis: Konfigurieren/Bearbeiten aller CA-Server, die OCSP für den Widerruf verwenden.

#### Konfigurieren der OCSP-Regeln

**Hinweis:** Überprüfen Sie, ob eine Richtlinie für die Übereinstimmung von Zertifikatsgruppen erstellt und der OCSP-Responder konfiguriert wurde, bevor Sie diese Schritte ausführen.

**Hinweis:** In einigen OCSP-Implementierungen kann ein DNS A- und ein PTR-Datensatz für die ASA benötigt werden. Diese Überprüfung wird durchgeführt, um zu überprüfen, 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 auszuwählen, die für die Verwendung von OCSP konfiguriert werden soll.
- 3. Wählen Sie Bearbeiten.
- 4. Klicken Sie auf die Registerkarte OCSP-Regel.
- 5. Klicken Sie auf Hinzufügen.
- 6. Führen Sie im Fenster OCSP-Regel hinzufügen die folgenden Schritte aus. Siehe Abbildung 25. Abbildung 25: Hinzufügen von OCSP-Regeln

Certificate Map:	DefaultCertificateMap 😽 😽
Certificate:	[cn=OCSP, ou=AMHS, o=Army, c=us]:[cn=OCSP, ou=AMHS ⊻
Index:	10
URL:	http://ocsp.disa.mil

Sie in der Option Certificate Map (Zertifikatszuordnung) die Option **DefaultCertificateMap** oder eine zuvor erstellte Zuordnung aus.Wählen Sie in der Option Zertifikat die Option **OCSP Responder aus**.Geben Sie in die Indexoption **10 ein**.Geben Sie in die 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 ASA konfiguriert ist.Klicken Sie auf **OK**.Klicken Sie auf **Übernehmen**.

### **Cisco AnyConnect Client-Konfiguration**

Dieser Abschnitt behandelt die Konfiguration des Cisco AnyConnect VPN-Clients.

**Annahmen**: 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 erstmalige Installation des 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.

**Hinweis:** Der Kartenlesertreiber für MAC OSX ist bereits installiert und kompatibel mit der aktuellen Betriebssystemversion, die Sie verwenden.

#### Herunterladen des Cisco AnyConnect VPN-Clients - Mac OS X

1. Starten Sie eine Websitzung mit der ASA über Safari. Die Adresse sollte das Format

https://Outside-Interface haben. Beispiel: https://172.18.120.225.

- 2. In einem Popup-Fenster werden Sie aufgefordert, das Zertifikat der ASA zu überprüfen. Klicken Sie auf **Weiter**.
- 3. Ein weiteres Popup-Fenster wird angezeigt, um die CAC-Schlüsselkette zu entsperren. Geben Sie Ihre PIN-Nummer ein. Siehe Abbildung 31.**Abbildung 31: PIN eingeben**

	Unlock	Keychain
0	Please enter your	keychain password.
	Safari wants to use k "CAC-2050-5000-10	eychain 028-0004-5279".
	Password:	
▶ Details		
?		Cancel OK

- 4. Wenn die Webseite für den SSL VPN-Service angezeigt wird, klicken Sie auf Weiter.
- 5. Nachdem Sie die Schlüsselkette entsperrt haben, werden Sie vom Browser gefragt, ob Sie dem Zertifikat von der ASA vertrauen. Klicken Sie auf **Vertrauenswürdig**.
- 6. Geben Sie das Root-Kennwort ein, um die Schlüsselkette zu entsperren, um eine sichere Verbindung herzustellen, und klicken Sie dann auf **OK**.
- 7. Wählen Sie das für die Client-Authentifizierung zu verwendende Zertifikat aus, und klicken Sie dann auf **OK**.
- 8. Anschließend fragt der Browser das Root-/Benutzerkennwort ab, um das Herunterladen von AnyConnect-Clients zu ermöglichen.
- 9. Wenn authentifiziert, lädt der AnyConnect-Client den Computer herunter. Siehe Abbildung 32. Abbildung 32: AnyConnect-Download

HebLaunch	Using Sun Java for Installation
Platform	Launching Cisco AnyConnect VPN Client If the software does not start properly, <u>Click he</u> nt Downloader
Downloading require Time Left: 1 sec (1.3) Transfer rate: 646 KB	d files. Please wait 7 MB of 2.47 MB copied) I/Sec

- 10. Nachdem die Anwendung heruntergeladen wurde, werden Sie vom Browser aufgefordert, das ASA-Zertifikat zu akzeptieren. Klicken Sie auf **Akzeptieren**.
- 11. Verbindung hergestellt. Abbildung 33: Abbildung 33: AnyConnect-Verbindung

	000	Cisco AnyConnect	VPN Client	L
WebLaunch	Connected to	162.126	Ð	diada cisco
✓ - Platform Detection	Duration:	00:00:29	6	Disconnect
- ActiveX	Client Address Server Address	20.1.1.1		
<ul> <li>Java Detection</li> <li>Microsoft Java</li> </ul>	Bytes Sent Bytes Received	6675 680		0
🖉 - Sun Java	Connection Log			
- Dutrinoau	► Details			Version 2.1.0148

Starten Sie den Cisco AnyConnect VPN-Client - Mac OS X.

Von Finder: Anwendungen > Cisco AnyConnect VPN-Client

**Hinweis:** Informationen zur optionalen AnyConnect-Client-Profilkonfiguration finden Sie im Anhang E.

#### Neue Verbindung

Das Wechselstrom-Fenster wird angezeigt. Siehe Abbildung 37.

Abbildung	37.	Νοιιο		erhindung	
Appliquing	<b>J</b> <i>I</i> .	INCUC	V F IN-V	erbindung	J

000	Cisco AnyConnect VPN Client			
connect to:	10.86.95.252		cisco	
			0	
			Version 2.1.0148	

- 1. Wählen Sie den geeigneten Host aus, wenn die Verbindung nicht automatisch vom AC-Gerät versucht wird.
- 2. Geben Sie bei Aufforderung Ihre PIN ein. Siehe Abbildung 38. Abbildung 38: PIN eingeben Unlock Keychain

a	Please enter you	r keychain password.
	Cisco AnyConnect V "CAC-4090-0029-	/PN Client wants to use keychain 8400-0005-60C1".
	Password:	
▶ Details		
?		(Cancel) (OK)

#### **Remote-Zugriff starten**

- 1. Wählen Sie die Gruppe und den Host aus, mit der Sie eine Verbindung herstellen möchten.
- Da Zertifikate verwendet werden, wählen Sie Connect aus, um das VPN einzurichten. Siehe Abbildung 39. Hinweis: Da die Verbindung Zertifikate verwendet, müssen Sie keinen Benutzernamen und kein Kennwort eingeben. Abbildung 39: Verbindung

Connect to:	10.86.95.252		cisco
/PN session ende	6		
Group:	SVC	•	
Username:	CACUSER		
Password:			
		Get Cer	tificate
			Version 2.1.0148
******			

Informationen zur optionalen AnyConnect-Client-Profilkonfiguration 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. Dadurch entfällt die Notwendigkeit einer LDAP-Schemaänderung. Für die CAC-Authentifizierungsimplementierung kann dies die zusätzliche Durchsetzung von Richtlinien für Remotezugriffsverbindungen 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. DAP kann in Zusammenarbeit mit CAC mehrere AD-Gruppen sowie Push-Richtlinien, ACLs usw. prüfen.

#### Szenario 1: Active Directory-Durchsetzung mit Remote Access Permission Dial-in -Zugriff zulassen/verweigern

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

• Der AD-Attributwert: TRUE = Allow; FALSE = Verweigern

• Cisco Attributwert: 1 = FALSE, 4 (IPSec) oder 20 (4 IPSEC + 16 WebVPN) = TRUE,

Für die ZULASSUNGSBedingung wird Folgendes zugeordnet:

• TRUE = 20

Für die DENY-Einwahlbedingung ordnen Sie Folgendes zu:

• FALSCH = 1

**Hinweis:** Stellen Sie sicher, dass TRUE und FALSE in allen Kapiteln enthalten sind. Weitere Informationen finden Sie unter <u>Konfigurieren eines externen Servers für die Benutzerautorisierung</u> <u>der Sicherheitsappliance</u>.

#### Active Directory-Einrichtung

- 1. Klicken Sie im Active Directory-Server auf **Start > Ausführen**.
- 2. Geben Sie im Textfeld Öffnen **dsa.msc ein** und klicken Sie auf **OK**. Dadurch wird die Active Directory-Managementkonsole gestartet.
- 3. Klicken Sie in der Active Directory-Verwaltungskonsole auf das Pluszeichen, um die 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 Sie alle Benutzer im Ordner Benutzer zugewiesen haben, erweitern Sie diesen Ordner, um ihn anzuzeigen. Siehe Abbildung A1. Abbildung A1: Active Directory-Verwaltungskonsole

habrat - [Console Root\Active Dir	ectory Users and Computers	[Ciscojax-2k3.labrat.com]\l	abrat.com\MIL]	_ 🗆 🗵
🚡 Ele Action Yew Favorites Y	<u>M</u> indow <u>H</u> elp			_5×
🗢 🔿 💽 💽 🎼 🗳 🗔	8 2000	ð		
Console Root Console Root Console Root Console Root Compatibility Comparised Computers Compu	Vame Clark Kent Ethan Hunt Peter Parker	User User User	Description	
<u>•</u>	1			<u> </u>

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 auf Zulassen oder Ablehnen. Siehe Abbildung A2.Abbildung A2: Benutzereigenschaften

rk Kent Properties	1
Environment   Sessions   Remote control   1 General   Address   Account   Profile Published Certificates   Member 01	Ferminal Services Profile   CO   Telephones   Organizatio Dial-in   Object   Securi
Remote Access Permission (Dial-in or VPN)	
Allow access	
C Deny access	
C Control access through Remote Access	Policy
☐ Verity Caller ID:	
Callback Options	
C Set by Caller (Routing and Remote Acc	ess Service only)
C Always Callback to:	
Assign a Static IP Address	
Apply State Boutes	·
Define routes to enable for this Dial-in connection.	Static Roytes
OK	Cancel Apply

7. Klicken Sie anschließend 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 der LDAP-Attributzuordnung

Add LDAP Attribute Map				X
Mep Name   Map Value   Customer Name: msNPAllowDialm Claco Name: Tunneling-Protocols	Add >>	Customar Name	Cisco Name	
	CK Cancel	Help		

Geben Sie im Textfeld Name einen Namen ein.Geben Sie auf der Registerkarte Name der Karte **msNPAllowDialin** im Textfeld Kundenname ein.Wählen Sie auf der Registerkarte Map Name (Name zuordnen) **Tunneling-Protokolle** im Dropdown-Menü in Cisco Name aus.Klicken Sie auf **Hinzufügen**.Wählen Sie die Registerkarte **Kartenwert aus**.Klicken Sie auf **Hinzufügen**.Geben Sie im Fenster Add Attribute LDAP Map Value (Wert hinzufügen) **TRUE** in das Textfeld Kundenname ein, und geben Sie **20** in das Textfeld Cisco Value ein.Klicken Sie auf **Hinzufügen**.Geben Sie **FALSE** in das Textfeld Kundenname ein, und geben Sie **1** in das Textfeld Cisco Value ein. Siehe Abbildung

		Customer Value	Cisco Value	
	-	FALSE	1	
			2U	
Customer Value:				
	Add >>			
Cisco Value:	<< Remove			
[]				

Klicken Sie auf **OK**.Klicken Sie auf **OK**.Klicken Sie auf **ANWENDEN**.Die Konfiguration sollte wie in Abbildung A5 aussehen.**Abbildung A5: Konfiguration der LDAP-Attributzuordnung** 

📬 Cisco ASDM 6.0 for ASA - 172	2.18.120.225		
<u>File View Tools Wizards Windo</u>	w Help	Look For: Find +	alulu
Home 🖧 Configuration 🖉 M	fonitoring 🔚 Save 🌘	🗞 Refresh 🔇 Back 🚫 Forward 🧳 Help	CISCO
Remote Access V d P ×	Configuration > Rem	ote Access VPN > AAA Setup > LDAP Attribute Map	
Network (Client) Access     Image: Access SS, VPN Access			
AAA Setup	Add and configure a	attribute map used by LDAP server.	
LDAP Attribute Map	Name	Attribute Map Name	
a 🔏 Secure Desktop Manager 👱	msNPAlowDialn	msNPAllowDiain – Tunneing-Protocols	
			t
Device Setup			D D
🖏 Firewall			
Remote Access VPN			
Site-to-Site VPN			
Device Management			
».		Apply Reset	
Device configuration loaded	cisc	o 15 😡 🛃 🔥 7/	17/07 1:56:07 PM UTC

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

🕵 Cisco ASDM 6.0 for ASA - 17	2.18.120.225				
Ele Yew Tools Wigards Winds	w Help Yonitoring 🔛 Save (	Look For:	Back 🚫 Forward	Find -	uhuhu cisco
Remote Access V 🗗 🕈 ×	Configuration > Re	mote Access VP	N > AAA Setup > AA	A Server Groups	
Image: Network (Client) Access	AAA Server Groups -				
AAA Setup	Server Group	Protocol	Accounting Mode	Reactivation M	Add
AAA Server Groups	AD-LDAP LOCAL	LDAP		Depletion	Edit
🖶 🚮 Local Users 🗟 🕂 Secure Desktop Manager 👱	<	U)		>	Delete
< <u>0</u>	Servers in the Selecte	d Group			
A Device Setup	Server Name or IF	Address	Interface	Timeout	Add
Firewall	172.18.120.160		outside	10	Edit
Remote Access VPN				(	Delete
Site-to-Site VPN					Move Up
Device Management					Move Down
÷			Apply Reset		
Device configuration loaded	d	sco  15	6	R 🔒 7/17	7/07 1:59:07 PM UTC

- 5. Klicken Sie auf die Servergruppe, die Sie bearbeiten möchten. Wählen Sie im Bereich Server im Abschnitt Ausgewählte Gruppe die Server-IP-Adresse oder den Hostnamen 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. Siehe Abbildung A7Abbildung A7: Hinzufügen der LDAP-Attributzuordnung

6 C . H		Com	
	11111	<b>MH</b>	<b>VH</b>
			<b>1 1 1 1</b>

E COIT AAA SERVER							
Server Group:	,	AD-LDAP					
Interface Name:		outside	~				
Server Name or IP Addr	ess:	172.18.120.160					
Timeout:		10		seconds			
LDAP Parameters							
Enable LDAP over	SSL						
Server Port:	389						
Server Type:	De	tect Automatically/Use Generic Type		I			
Base DN:	CN=Users,DC=ggsgseclab,DC=org						
Scope:	One level beneath the Base DN						
Naming Attribute(s):	userPrincipalName						
Login DN:	CN=Administrator,CN=Users,DC=ggsgseclab,DC=o						
Login Password:	•••••						
LDAP Attribute Map:	msNPAllowDialin						
SASL MD5 authentication							
SASL Kerberos authentication							
Kerberos Server Group:							
OK Cancel Help							

7. Klicken Sie auf OK.

Hinweis: Aktivieren Sie beim Testen 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 durch Gruppenmitgliedschaft zum Zulassen/Verweigern des Zugriffs

In diesem Beispiel wird der LDAP-AttributmemberOf dem Tunneling Protocol-Attribut zugeordnet, um eine Gruppenmitgliedschaft als Bedingung einzurichten. Damit diese Richtlinie funktioniert, müssen folgende Bedingungen erfüllt sein:

- Verwenden Sie eine bereits vorhandene Gruppe, oder erstellen Sie eine neue Gruppe f
  ür ASA VPN-Benutzer, um Mitglied von für ALLOW-Bedingungen zu sein.
- Verwenden Sie eine Gruppe, die bereits vorhanden ist, oder erstellen Sie eine neue Gruppe

für Nicht-ASA-Benutzer, um Mitglied für DENY-Bedingungen zu sein.

• Überprüfen Sie im LDAP Viewer, ob Sie die richtige DN für die Gruppe haben. Siehe Anhang D. Wenn die DN falsch ist, funktioniert die Zuordnung nicht ordnungsgemäß.

**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 spezielles Zeichen vor den Namen zu setzen, da AD Sonderzeichen zuerst betrachtet. Um dieses Problem zu umgehen, verwenden Sie DAP in 8.x-Software, um sich mehrere Gruppen anzusehen.

**Hinweis:** Stellen Sie sicher, dass ein Benutzer Teil der Deny-Gruppe oder mindestens einer anderen Gruppe ist, sodass das MitgliedOf immer an die ASA zurückgesendet wird. Sie müssen die FALSE-deny-Bedingung 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 DAP kann die ASA mehrere Gruppen im memberOf-Attribut und die Basislizenzautorisierung der Gruppen betrachten. Siehe Abschnitt DAP.

#### ZUORDNUNG

- Der AD-Attributwert:memberOf CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=orgmemberOf CN=TelnetClients,CN=Users,DC=labrat,DC=com
- Cisco Attributwert: 1 = FALSE, 20 = TRUE,

Für ALLOW Bedingung müssen Sie Folgendes zuordnen:

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

Für DENY-Bedingung kartieren Sie:

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

**Hinweis:** In zukünftigen Versionen gibt es ein Cisco-Attribut, um die Verbindung zuzulassen und zu verweigern. Weitere Informationen zu <u>Cisco Attributen</u> finden Sie unter <u>Konfigurieren eines</u> <u>externen Servers für die Benutzerautorisierung der Sicherheitsappliance</u>.

#### Active Directory-Einrichtung

- 1. Wählen Sie im Active Directory-Server **Start > Ausführen aus**.
- 2. Geben Sie im Textfeld Öffnen **dsa.msc ein** und klicken Sie dann auf **OK**. Dadurch wird die Active Directory-Managementkonsole gestartet.
- 3. Klicken Sie in der Active Directory-Verwaltungskonsole auf das Pluszeichen, um die Active Directory-Benutzer und -Computer zu erweitern. Siehe Abbildung A8Abbildung A8: Active Directory-Gruppen

Elle Action View Window Help					
► → 🗈 🗷 👗 🗙 📽 🖳 😚 💆 🕍 🏹	4 E				
Active Directory Users and Computer Users 23 objects					
Saved Queries Name	Туре	Description	1		
🖻 🗊 labrat.com	User	Built-in account for administering the co			
🖲 🛄 Builtin 🖸 artperez	User				
Computers	Security Group	VPN Remote Access Users	- Contract		
Onan Controlers     Of Cert Publishers	Security Group	Members of this group are permitted to			
CERTSVC_DCOM_ACC	ESS Security Group				
DisAdmins	Security Group	DNS Administrators Group			
DrisUpdateProxy	Security Group	DNS clients who are permitted to perfor			
🔂 Domain Admins	Security Group	Designated administrators of the domain			
Domain Computers	Security Group	All workstations and servers joined to th			
Domain Controllers	Security Group	All domain controllers in the domain			
🚮 Domain Guests	Security Group	All domain guests			
Domain Users	Security Group	All domain users			
Enterprise Admins	Security Group	Designated administrators of the enterp	<u>i de tete</u>		
Group Policy Creator O	whers Security Group	Members in this group can modify group .			
Guest	User	Built-in account for guest access to the			
4 HelpServicesGroup	Security Group	Group for the Help and Support Center			
TIS_WPG	Security Group	IIS Worker Process Group			
IUSR_CISCOJAX-2K3	User	Built-in account for anonymous access t			
IWAM_CISCOJAX-2K3	User	Built-in account for Internet Information			
TRAS and IAS Servers	Security Group	Servers in this group can access remote			
Schema Admins	Security Group	Designated administrators of the schema			
5upport_388945a0	User	This is a vendor's account for the Help a			
TelnetClients	Security Group	Members of this group have access to T	- 61-1-1-		

- 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**.
- 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 soeben erstellte Gruppe.
- 9. Wählen Sie die Registerkarte Mitglieder, 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.Geben Sie im Textfeld Name einen Namen ein.Geben Sie auf der Registerkarte "Map Name" im Textfeld Kundenname den MemberOf ein.Wählen Sie auf der Registerkarte Map Name (Name zuordnen) Tunneling-Protokolle im Dropdown-Menü in Cisco Name aus.Wählen Sie Hinzufügen aus.Klicken Sie auf die Registerkarte Kartenwert.Wählen Sie Hinzufügen aus.Geben Sie im Fenster Add Attribute LDAP Map Value (Wert hinzufügen) CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org im Textfeld Kundenname ein, und geben Sie 20 in das Textfeld Cisco Value ein.Klicken Sie auf Hinzufügen.Geben Sie CN=TelnetClients,CN=Users,DC=ggsgseclab,DC=org im Textfeld Kundenname ein, und geben Sie 1 in das Textfeld Cisco Value ein. Siehe Abbildung A4.Klicken Sie auf OK.Klicken Sie auf OK.Klicken Sie auf Übernehmen.Die Konfiguration

sollte wie in Abbildung A9 aussehen. Abbildung A9 LDAP-Attributzuordnung

1 Cisco ASDM 6.0 for ASA - 17	2.18.120.225			
<u>File View Tools Wizards Windo</u>	w <u>H</u> elp	Look For:	(1996) And -	ahah
Home 🖧 Configuration 🚺 N	fonitoring 🔛 Save	🔇 Refresh 🔇 Back 🔘 F	criverid 🧳 Help	CISCO
Remote Access V 🗗 🕂 🗡	Configuration > R	emote Access VPN > AAA Set	up > LDAP Attribute Map	
Network (Client) Access     Clientless SSL VPN Access     AAA Setup     AAA Setup     AAA Server Groups	Add and configu	re attribute map used by LDAP serv	<del>थ</del> ा.	
LDAP Attribute Map	Name	Attribute Map Name		
E 🔏 Secure Desktop Manager ⊻	memberOf	memberOf=Tunneing-Proto	cols	
Cevice Setup				
Frewall				
Remote Access VPN				
Site-to-Site VPN				
Device Management				1999 - 1999 1999 - 1999 1999 - 1999
10 T		ерру (	Keset	
Configuration changes say		cisco 15	D 🗒 🔝 🛛 🔂 7	/17/07 2:14:47 PM UTC

- 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 Bereich Server im Abschnitt Ausgewählte Gruppe die Server-IP-Adresse oder den Hostnamen aus, und klicken Sie dann auf

lame: memberOf		
p Name Map Value		
Customer Name	Customer to Gsco Map Value	DDA DOA
memberOf	CN=TeinetOients, CN=Users, DC=ggsgsedab, DC=org=1 CN=ASAUsers, CN=Users, DC=ggsgsedab, DC=org=20	
		Edit
		Delete
		2.2.2.2.2.2.2.2.2.2

- 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 beim Testen das LDAP-Debugging, um zu überprüfen, ob die LDAP-

Bindungen und Attributzuordnungen ordnungsgemäß funktionieren. Befehle zur Fehlerbehebung finden Sie in Anhang C.

#### Szenario 3: Dynamische Zugriffsrichtlinien für mehrere Member von Attributen

In diesem Beispiel wird DAP verwendet, um mehrere memberOf-Attribute anzuzeigen, um den Zugriff basierend auf der Active Directory-Gruppenmitgliedschaft zuzulassen. Vor 8.x liest die ASA nur das erste memberOf-Attribut. Mit 8.x und höher kann die ASA alle MemberOf-Attribute anzeigen.

- Verwenden Sie eine bereits vorhandene Gruppe, oder erstellen Sie eine neue Gruppe (oder mehrere Gruppen), bei der ASA VPN-Benutzer für ALLOW-Bedingungen Mitglied sein sollen.
- Verwenden Sie eine Gruppe, die bereits vorhanden ist, oder erstellen Sie eine neue Gruppe für Nicht-ASA-Benutzer, um Mitglied für DENY-Bedingungen zu sein.
- Überprüfen Sie im LDAP Viewer, ob Sie die richtige DN für die Gruppe haben. Siehe Anhang D. Wenn die DN falsch ist, funktioniert die Zuordnung nicht ordnungsgemäß.

#### **ASA-Konfiguration**

- 1. Wählen Sie im ASDM Remote Access VPN > Network (Client) Access > Dynamic Access Policies (Remote-Access-VPN > Netzwerkzugriff > dynamische Zugriffsrichtlinien aus.
- 2. Klicken Sie auf Hinzufügen.
- 3. Gehen Sie in der Registerkarte Add Dynamic Access Policy (Dynamische Zugriffsrichtlinie hinzufügen) wie folgt vor:Geben Sie im Textfeld b. einen Namen ein.Geben Sie im Abschnitt "Priorität" 1 oder eine Zahl größer als 0 ein.Klicken Sie in den Auswahlkriterien auf Hinzufügen.Wählen Sie im Feld AAA-Attribut hinzufügen die Option LDAP.Geben Sie im Abschnitt Attribut-ID memberOf ein.Wählen Sie im Wertebereich = und geben Sie den AD-Gruppennamen ein. Wiederholen Sie diesen Schritt für jede Gruppe, auf die Sie verweisen möchten. Siehe Abbildung A10.Abbildung A10 AAA-Attributübersicht

📬 Add AAA	Attribute 🛛 🛛 🔀	
AAA Attribute	Type: LDAP	
Attribute ID:	memberOf	
Value:		
	Cancel Help	

Klicken Sie auf OK.Wählen Sie im

Abschnitt Access Policy Attributes (Zugriffsrichtlinienattribute) Weiter aus. Siehe Abbildung

#### A11. Abbildung A11 Dynamische Richtlinie hinzufügen

				and a second	
Multi-Group Membership Check				Priority: 1	
tere					
<ul> <li>AAA and endpoint attributes used to select th i every endpoint attribute has been satisfied. T a logical expression text.</li> </ul>	is acces hese at	s policy. A policy tributes can be c	is used when a user's reated using the tables	authorization attributes match the AJ s below and/or by expanding the Adv	AA attribute oriteria anced option to
ANY of the following AAA Attributes values	~		and the following er	idpoint attributes are satisfied.	
vibute Operation/Value	1	Add	Endpoint ID	Name/Operation/Value	Add
berOf = _ASAUsers	1	Frit			Edd
LerOf - MPNUsers					
	l	Delete			Delete
					Logical Op.
			1		
y Attributes access policy attributes for this policy. Attribut Network ACL Filters Web-Type ACL Filters    F	tes value Function	es specified here s Port Forward	will override those valuing Lists   A	ues obtained from the AAA system. ccass Mathod	
💽 Continue 🔵 Terminate					
the message that will be displayed when this m	ecord is	selected,			
essage:					
	Multi-Group Membership Check  Perie  AAA and endpoint attributes used to select th every endpoint attributes used to select th every endpoint attributes has been satisfied. Ta logical expression text.  ANY of the following AAA Attributes values  rbute Operation/Value berOf = _ACAAUsers berOf =	Multi-Group Membership Check  Ferie  AAA and endpoint attributes used to select this acces every endpoint attributes used to select this acces every endpoint attribute has been satisfied. These atta logical expression text.  ANY of the following AAA Attributes values  rbute Operation/Value berOf = _ASAUsers berOf	Multi-Group Membership Check  Fere  AAA and endpoint attributes used to select this access policy. A policy every endpoint attributes has been satisfied. These attributes can be o a logical expression text.  ANY of the following AAA Attributes values  rbute Operation/Value Add BerOf Add BerOf Add BerOf Continue Co	Multi-Group Membership Check  Fore  AAAA and endpoint attributes used to select this access policy. A policy is used when a user's every endpoint attributes has been satisfied. These attributes can be created using the tablet a logical expression text.  ANY of the following AAA Attributes values  The of the following AAA Attributes values  ANY of the following AAA Attributes values attributes values attributes values attributes the values attributes at the values of the	Multi-Group Membership Check       Printly: 1         Printly:       AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AV a logical expression text.         ANN of the following AAA Attributes values <ul> <li>and the following endpoint attributes are satisfied. These attributes can be created using the tables below and/or by expanding the Adv a logical expression text.</li> </ul> ANN of the following AAA Attributes values <ul> <li>and the following endpoint attributes are satisfied.</li> <li>Endpoint 1D</li> <li>Name/Operation/Value</li> <li>Endpoint 1D</li> <li>Name/Operation/Value</li> <li>Endpoint 1D</li> <li>Name/Operation/Value</li> <li>Endpoint 1D</li> <li>Name/Operation/Value</li> </ul> end <ul> <li>YMUters</li> <li>Continue</li> <li>Terminate</li> <li>Functions</li> <li>Port Forwarding LBts</li> <li>URL Lists</li> <li>Access Method</li> </ul> @ Continue     Terminate

- 4. Wählen Sie im ASDM Remote Access VPN > Network (Client) Access > Dynamic Access Policies (Remote-Access-VPN > Netzwerkzugriff > dynamische Zugriffsrichtlinien aus.
- 5. Wählen Sie Standard Access Policy (Standardzugriffsrichtlinie) aus, und wählen Sie Edit (Bearbeiten) aus.
- 6. Die Standardaktion sollte auf **Terminate** gesetzt werden. Siehe Abbildung A12. **Abbildung** A12 Dynamische Richtlinie bearbeiten

📬 Edi	t Dyna	nic Access Policy	,					Note
Polic	y Name:	DfltAccessPolicy						
Des	cription:							
Ac	cess Pol	cy Attributes access policy attribut	tes for this policy. Attrib	utes values	specified here will over	ride those v	values obtained from th	e AAA system.
	Action	Network ACL Filters	Web-Type ACL Filters	Functions	Port Forwarding Lists	URL Lists	Access Method	
	Specifi User M	v the message that will lessage:	I be displayed when this	racord is s	elected.			
			ОК		Cancel Help			

7. Klicken Sie auf OK.

Hinweis: Wenn Terminate nicht ausgewählt ist, sind Sie auch in Gruppen zugelassen, wenn nicht,

### Anhang B: ASA CLI-Konfiguration

ASA 5510 ciscoasa#show running-config : Saved ASA Version 8.0(2) 1 hostname asa80 domain-name army.mil enable password 8Ry2YjIyt7RRXU24 encrypted names 1 interface GigabitEthernet0/0 nameif outside security-level 0 ip address x.x.x.x 255.255.255.128 1 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 1 -----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
1
-----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 1 -----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 ! 1 class-map inspection\_default match default-inspection-traffic 1 policy-map type inspect dns preset\_dns\_map parameters message-length maximum 512 policy-map global\_policy class inspection\_default inspect dns preset\_dns\_map inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp

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

### Anhang C: Fehlerbehebung

#### Fehlerbehebung AAA und LDAP

- debug Idap 255 Zeigt LDAP-Austauschprogramme an
- debug aaa common 10 Zeigt AAA-Austauschvorgänge an

#### Beispiel 1: Zulässige Verbindung mit korrekter Attributzuordnung

Dieses Beispiel zeigt die Ausgabe von **debug Idap** und **debug, die** bei einer erfolgreichen Verbindung mit dem in Anhang A gezeigten Szenario 2 **häufig** auftritt.

Abbildung C1: LDAP debug und Debugging a common output - richtige 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 = ....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.....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

In diesem Beispiel wird die Ausgabe von **debug Idap** und **debug** veranschaulicht, die bei einer zulässigen Verbindung mit Szenario 2 in Anhang A **üblich** ist.

Abbildung C2: LDAP debug und Debugging a common output - 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 0x26flc44, 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 =
....com1.0....
&...,d...
[82] userCertificate: value =
....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.....q.....mY...
[82] accountExpires: value = 9223372036854775807
[82] logonCount: value = 25
[82] sAMAccountName: value = 1234567890
[82] sAMAccountType: value = 805306368
[82] userPrincipalName: value = 1234567890@mil
[82] objectCategory: value =
CN=Person, CN=Schema, CN=Configuration, DC=ggsgseclab, DC=or
q
[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

In diesem Beispiel wird die Ausgabe von **Debug-Dap-Fehlern** und **Debug-Dap-Trace** während einer erfolgreichen Verbindung mit Szenario 3 in Anhang A veranschaulicht. Beachten Sie mehrere MemberOf-Attribute. Sie können sowohl \_ASAUsers als auch VPNUsers angehören, oder Sie können einer der beiden Gruppen angehören, was von der ASA-Konfiguration abhängt.

Abbildung C3: Debug-DAP
#debug dap errors
debug dap errors enabled at level 1
#debug dap trace
debug dap trace enabled at level 1
#
The DAP policy contains the following attributes for
user:
1241879298@mil
1: action - continue
DAD TRACE: DAD open: CREEEN10
DAP_IRACE: DAP_OPEN: COLEFAIO
DAP_IRACE. USerHame. 12410/9290@mill,
DAD_TDACE: Hackmane: 12419702000mil
DAP_IRACE: Username: 12410/9296@mill,
DAD TDAGE: Usermane: 12410702000mil
DAP_IRACE. Username. 12418/9298@mii,
aaa.ldap.objectClass.3 =
organizationalPerson
DAP_TRACE: Username: 12418/9298@mil,
aaa.ldap.objectClass.4 = user
DAP_TRACE: Username: 12418/9298@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:
Ы
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid
= ...
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.accountExpires =
9223372036854775807
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount
= 0
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.sAMAccountName =
1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.sAMAccountType =
805306368
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userPrincipalName =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectCategory =
CN=Person, CN=Schema, CN=Configuration, DC=ggsgseclab, DC=or
q
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username
1241879298@mil
DAP_TRACE: Username: 1241879298@mil,
aaa.cisco.tunnelgroup = CAC-USERS
DAP TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] =
"top";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person";
```

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

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

#### Beispiel 2: Verbindung mit DAP verweigert

Dieses Beispiel zeigt die Ausgabe von **Debug-Dap-Fehlern** und **Debug-Dap-Trace** bei einer nicht erfolgreichen Verbindung mit Szenario 3, wie in Anhang A gezeigt.

#### Abbildung C4: Debug-DAP

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

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

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

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

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

### Fehlerbehebung Zertifizierungsstelle/OCSP

- debuggen crypto ca 3
- Im Konfigurationsmodus: Protokollierungsklasse kann das Debuggen von Konsole(oder Puffer)

Diese Beispiele zeigen eine erfolgreiche Zertifikatsvalidierung mit dem OCSP-Responder und eine Richtlinie für die Übereinstimmung von Zertifikatsgruppen.

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

Abbildung C4 zeigt die Debug-Ausgabe einer falsch konfigurierten Richtlinie für die Übereinstimmung von Zertifikatsgruppen.

Abbildung C5 zeigt die Debug-Ausgabe eines Benutzers mit einem widerrufenen 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: OF192B, 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 Richtlinie für die Übereinstimmung von Zertifikatsgruppen mit fehlgeschlagenen Zertifikaten

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: 2FB5FC740000000035, 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: 2FB5FC740000000035, 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**

- Wählen Sie nach der Installation Start > Ausführen.
- Geben Sie Idp ein, und klicken Sie dann auf OK. Dadurch wird der LDAP-Viewer gestartet.
- Wählen Sie Verbindung > Verbindung aus.
- Geben Sie den Servernamen ein, und klicken Sie dann auf OK.
- Wählen Sie Verbindung > Bind aus.
- Geben Sie einen Benutzernamen und ein Kennwort ein.**Hinweis:** Sie benötigen Administratorrechte.
- Klicken Sie auf OK.
- LDAP-Objekte anzeigen Siehe Abbildung D1. Abbildung D1: LDAP-Viewer

🚰 ldap://Ciscojax-2k3.labrat.com/DC=labrat,DC=com	-0
Connection Browse Yew Options Utilities	the state of the s
<ul> <li>CN=labrat, DC=vcom</li> <li>CN=Bultin, DC=labrat, DC=vcom</li> <li>CN=Computers, DC=labrat, DC=vcom</li> <li>CN=Computers, DC=labrat, DC=vcom</li> <li>CN=Infrastructure, DC=labrat, DC=vcom</li> <li>CN=Infrastructure, DC=labrat, DC=vcom</li> <li>CN=Chabrat, DC=labrat, DC=vcom</li> <li>CN=Chabrat, CD=HMIL, DC=labrat, DC=vcom</li> <li>CN=Chabrat, NC=VHIL, DC=labrat, DC=vcom</li> <li>CN=Chabrat, NC=VHIL, DC=labrat, DC=vcom</li> <li>CN=Chabrat, DC=Vabrat, DC=vcom</li> <li>CN=Chabrat, DC=Vabrat, DC=vcom</li> <li>CN=Chabrat, DC=vlabrat, DC=vcom</li> <li>CN=Stap, DC=labrat, DC=vcom</li> <li>CN=Stap, DC=labrat, DC=vcom</li> <li>CN=Vabrat, DC=vlabrat, DC=vcom</li> <li>CN=Vabrat, DC=vcom</li> <li>C</li></ul>	Expanding base 'CN=Clark Kent,OU=MIL_DC=labraLDC=com' Result 40: [null] Matched DNs: Getting 1 entries: >> Dn: CN=Clark Kent,OU=MIL_DC=labraLDC=com 4 objectClass: top: person; organizationalPerson; user; 1> cn: Clark Kent; 1> physicalDeliveryOfficeName: Welcome to LDAPHI; 2> userCertificate: (ldp: Binary blob>; (ldp: Binary blob>; 1> givenName: Clark; 1> distinguishedName: CN=Clark Kent,OU=MIL_DC=labraLDC=com; 1> instanceType: Dx4 = ITWRITE 1; 1> whenCreated: 06/13/2006 12:50:21 Eastern Standard Time Eastern Daylight Time; 1> whenCreated: 06/21/2006 13:31:54 Eastern Standard Time Eastern Daylight Time; 1> whenCreated: 06/21/2006 13:31:54 Eastern Standard Time Eastern Daylight Time; 1> uSNCreated: 14072; 1> uSNChanged: 14072; 1> uSNChanged: 14701; 1> name: Clark Kent; 1> objectGUID: 44039dt4=12a-4fee-9337-3240c26ccf79; 1> userAccountControl: 0x10200 = [UF_NORIMAL_ACCOUNT   UF_DONT_EXPIRE_PASSWD] 3 1> badPwdCount: 0; 1> cadeFage: 0; 1> countyCode: 0; 1> badPswordTime: 06/14/2006 15:19:36 Eastern Standard Time Eastern Daylight Time; 1> hast_sport 01/01/1601 00:00:00 UNC ; 1> last_sport 01/01/1601 0
Ready	N.M.

#### Active Directory Services-Schnittstelleneditor

- Wählen Sie im Active Directory-Server Start > Ausführen.
- Geben Sie adsiedit.msc ein. Dadurch 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 zum Abgleich von Zertifikaten, wie z. B. Distinguished Name oder Herausgeber. Das Profil wird als XML-Datei gespeichert und kann mit Notepad bearbeitet werden. Die Datei kann jedem Client manuell hinzugefügt oder 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 **Gehen Sie wie folgt vor:** 

- 1. Wählen Sie AnyConnectProfile.tmpl aus, und öffnen Sie die Datei mit Notepad.
- 2. Nehmen Sie geeignete Änderungen an der Datei vor, z. B. Aussteller oder Host-IP. Siehe Abbildung F1.
- 3. Speichern Sie die Datei anschließend als XML-Datei.

Dies ist ein Beispiel für eine Cisco AnyConnect VPN Client Profile-XML-Datei.

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

- Ein Profil sollte eindeutig für Ihr Unternehmen benannt sein. Ein Beispiel: CiscoProfile.xml
- Der Profilname sollte der gleiche sein, auch wenn er für einzelne Unternehmensgruppen unterschiedlich ist.

Diese Datei soll von einem Secure Gateway-Administrator verwaltet und dann mit der Client-

Software verteilt werden. Das Profil, das auf dieser XML-Datei basiert, kann jederzeit an Clients verteilt werden. Die unterstützten Verteilungsmechanismen sind als Paketdatei mit der Softwareverteilung oder als Teil des automatischen Downloadmechanismus verfügbar. Der automatische Downloadmechanismus ist nur bei bestimmten Cisco Secure Gateway-Produkten verfügbar.

**Hinweis:** Administratoren wird dringend empfohlen, das von ihnen erstellte XML-Profil mithilfe eines Online-Validierungstools oder über die Profilimport-Funktion in ASDM zu validieren. Die Validierung kann mit dem in diesem Verzeichnis enthaltenen AnyConnectProfile.xsd durchgeführt werden. AnyConnectProfile ist das Stammelement, das das AnyConnect-Clientprofil darstellt.

xml version="1.0" encoding="UTF-8" 
<pre>! The ClientInitialization section represents global settings ! for the client. In some cases, for example, BackupServerList, host specific ! overrides are possible. !&gt; -</pre>
<pre>! The Start Before Logon feature can be used to activate ! the VPN as part of the logon sequence. ! - UserControllable: Does the administrator of this profile allow the user ! to control this attribute for their own use. Any user setting ! associated with this attribute is stored elsewhere&gt;</pre>
<pre>! This control enables an administrator to have a one time ! message displayed prior to a users first connection attempt. As an ! example, the message can be used to remind a user to insert their smart ! card into its reader. ! The message to be used with this control is localizable and can be ! found in the AnyConnect message catalog. ! (default: "This is a pre-connect reminder message.")</pre>
<pre>! This section enables the definition of various attributes ! that can be used to refine client certificate selection&gt; -</pre>

F



### Zugehörige Informationen

- Von X.509 und RFC 3280 angegebene Zertifikate und CRLs
- OCSP angegeben durch RFC 2560
- Einführung in Public Key Infrastructure
- "Lightweight OCSP" gemäß Draft Standard
- <u>SSL/TLS gemäß RFC 2246</u>
- <u>Technischer Support und Dokumentation Cisco Systems</u>