

ASA Remote Access VPN IKE/SSL - Kennwortablauf und -änderung für RADIUS, TACACS und LDAP - Konfigurationsbeispiel

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[ASA mit lokaler Authentifizierung](#)

[ACS und lokale Benutzer](#)

[ACS- und Active Directory-Benutzer](#)

[ASA mit ACS über RADIUS](#)

[ASA mit ACS über TACACS+](#)

[ASA mit LDAP](#)

[Microsoft LDAP für SSL](#)

[LDAP und Warnung vor Ablauf](#)

[ASA und L2TP](#)

[ASA SSL VPN-Client](#)

[ASA SSL-Webportal](#)

[ACS-Benutzerkennwort ändern](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument werden die Funktionen zum Kennwortablauf und zur Kennwortänderung in einem VPN-Tunnel mit Remote-Zugriff beschrieben, der auf einer Cisco Adaptive Security Appliance (ASA) terminiert wird. Gegenstand des Dokuments:

- Verschiedene Clients: Cisco VPN-Client und Cisco AnyConnect Secure Mobility
- Verschiedene Protokolle: TACACS, RADIUS und Lightweight Directory Access Protocol (LDAP)
- Verschiedene Geschäfte im Cisco Secure Access Control System (ACS): Lokales und Active Directory (AD)

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnisse der ASA-Konfiguration über die Kommandozeile (CLI)
- Grundkenntnisse der VPN-Konfiguration auf einer ASA
- Grundkenntnisse des Cisco Secure ACS

Verwendete Komponenten

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

- Cisco Adaptive Security Appliance, Version 8.4 und höher
- Microsoft Windows Server 2003 SP1
- Cisco Secure Access Control System, Version 5.4 oder höher
- Cisco AnyConnect Secure Mobility, Version 3.1
- Cisco VPN Client, Version 5

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.

Konfigurieren

Hinweise:

Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Weitere Informationen [zu Debug-Befehlen](#) vor der Verwendung von **Debug**-Befehlen finden Sie unter [Wichtige Informationen](#).

ASA mit lokaler Authentifizierung

Eine ASA mit lokal definierten Benutzern lässt die Verwendung von Funktionen zum Ablauf von Kennwörtern oder zur Kennwortänderung nicht zu. Es ist ein externer Server wie RADIUS, TACACS, LDAP oder Windows NT erforderlich.

ACS und lokale Benutzer

ACS unterstützt sowohl Kennwortablauf als auch Kennwortänderung für lokal definierte Benutzer.

Sie können beispielsweise neu erstellte Benutzer zwingen, ihr Kennwort bei der nächsten Anmeldung zu ändern, oder Sie können ein Konto an einem bestimmten Datum deaktivieren:

Users and Identity Stores > Internal Identity Stores > Users > Create

General

Name: Status:

Description:

Identity Group:

Account Disable

Disable Account if Date Exceeds: (yyyy-Mmm-dd)

Password Information

Password must:

- Contain 4 - 32 characters

Password Type:

Password:

Confirm Password:

Change password on next login

User Information


There are no additional identity attributes defined for user records

Sie können eine Kennwortrichtlinie für alle Benutzer konfigurieren. Nach Ablauf eines Kennworts können Sie beispielsweise das Benutzerkonto deaktivieren (ohne Anmelde­möglichkeit blockieren) oder die Option zum Ändern des Kennworts anbieten:

Password Complexity

Advanced

Account Disable

- Never
- Disable account if:
 - Date Exceeds:  (yyyy-Mmm-dd)
 - Days Exceed:
 - Failed Attempts Exceed:
 - Reset current failed attempts count on submit

Password History

Password must be different from the previous versions

Password Lifetime

Users can be required to periodically change password

- If password not changed after days :
 - Disable user account
 - Expire the password
- Display reminder after days

Benutzerspezifische Einstellungen haben Vorrang vor globalen Einstellungen.

ACS-RESERVED-Never-Expired ist ein internes Attribut für die Benutzeridentität.

System Administration > Configuration > Dictionaries > Identity > Internal Users > Edit: "ACS-RESERVED-Never-Expired"

My Workspace

- Network Resources
- Users and Identity Stores
- Policy Elements
- Access Policies
- Monitoring and Reports
- System Administration**
 - Administrators
 - Accounts
 - Roles
 - Settings
 - Administrative Access Control
 - Users
 - Authentication Settings
 - Max User Session Global Settings
 - Purge User Sessions
 - Operations
 - Distributed System Management
 - Software Repositories
 - Scheduled Backups
 - Local Operations
 - Configuration
 - Global System Options
 - Dictionaries
 - Protocols
 - Identity
 - Internal Users**
 - Internal Hosts

General

Attribute: ACS-RESERVED-Never-Expired

Description:

Attribute Type

Attribute Type: Boolean

Default Value: False

Attribute Configuration

Add Policy Condition

Policy Condition Display Name:

⚠ = Required fields

Dieses Attribut wird vom Benutzer aktiviert und kann verwendet werden, um die globalen Kontoablaufereinstellungen zu deaktivieren. Bei dieser Einstellung ist ein Konto nicht deaktiviert, selbst wenn die globale Richtlinie Folgendes angibt:

Users and Identity Stores > Internal Identity Stores > Users > Create

Users and Identity Stores

- Identity Groups
- Internal Identity Stores
 - Users**
 - Hosts
- External Identity Stores
 - LDAP
 - Active Directory
 - RSA SecurID Token Servers
 - RADIUS Identity Servers
 - Certificate Authorities
 - Certificate Authentication Profile
 - Identity Store Sequences
- Policy Elements
- Access Policies
- Monitoring and Reports
- System Administration

General

Name: cisco Status: Enabled

Description:

Identity Group: All Groups Select

Account Disable

Disable Account if Date Exceeds: 2013-Dec-02 (yyyy-Mmm-dd)

Password Information

Password must:

- Contain 4 - 32 characters

Password Type: Internal Users Select

Password:

Confirm Password:

Change password on next login

User Information

ACS-RESERVED-Never-Expired: True

⚠ = Required fields

ACS- und Active Directory-Benutzer

ACS kann so konfiguriert werden, dass die Benutzer in einer AD-Datenbank überprüft werden. Kennwortablauf und Kennwortänderung werden unterstützt, wenn das Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2) verwendet wird. Siehe [Benutzerhandbuch für Cisco Secure Access Control System 5.4: Authentifizierung in ACS 5.4: Authentifizierungsprotokoll- und Identitätsspeicherkompatibilität](#) für Details.

Auf einer ASA können Sie die Passwortverwaltungsfunktion verwenden, wie im nächsten Abschnitt beschrieben, um die ASA zur Verwendung von MSCHAPv2 zu zwingen.

ACS verwendet den Common Internet File System (CIFS) Distributed Computing Environment/Remote Procedure Call (DCE/RPC)-Anruf, wenn er das Verzeichnis Domain Controller (DC) kontaktiert, um das Kennwort zu ändern:

80	192.168.10.152	10.48.66.128	SAMR	324	ChangePasswordUser2	request
83	10.48.66.128	192.168.10.152	SAMR	178	ChangePasswordUser2	response
.....						
▶ Frame 80: 324 bytes on wire (2592 bits), 324 bytes captured (2592 bits)						
▶ Ethernet II, Src: CadmusCo_65:a0:ff (08:00:27:65:a0:ff), Dst: 62:9d:c3:a4:c4:c8 (62:9d:c3:a4:c4:c8)						
▶ Internet Protocol Version 4, Src: 192.168.10.152 (192.168.10.152), Dst: 10.48.66.128						
▶ Transmission Control Protocol, Src Port: 35986 (35986), Dst Port: microsoft-ds (445),						
▶ [2 Reassembled TCP Segments (806 bytes): #79(536), #80(270)]						
▶ NetBIOS Session Service						
▶ SMB (Server Message Block Protocol)						
▶ SMB Pipe Protocol						
▶ Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Request, Fragment						
▼ SAMR (pidl), ChangePasswordUser2						
Operation: ChangePasswordUser2 (55)						
[Response in frame: 83]						
Encrypted stub data (672 bytes)						

ASA kann sowohl das RADIUS- als auch das TACACS+-Protokoll verwenden, um mit dem ACS Kontakt aufzunehmen, um eine AD-Kennwortänderung vorzunehmen.

ASA mit ACS über RADIUS

Das RADIUS-Protokoll unterstützt keine native Kennwortablaufzeit oder Kennwortänderung. In der Regel wird das Password Authentication Protocol (PAP) für RADIUS verwendet. Die ASA sendet Benutzername und Kennwort als Klartext, und das Kennwort wird anschließend mithilfe des gemeinsam genutzten geheimen RADIUS-Codes verschlüsselt.

In einem typischen Szenario, in dem das Benutzerkennwort abgelaufen ist, gibt ACS eine RADIUS-Reject-Nachricht an die ASA zurück. ACS bemerkt, dass:

Authentication Summary	
Logged At:	October 2, 2013 8:24:52.446 AM
RADIUS Status:	Authentication failed : <u>24203 User need to change password</u>
NAS Failure:	
Username:	<u>cisco</u>
MAC/IP Address:	192.168.10.67
Network Device:	<u>ASA3 : 192.168.11.250 :</u>
Access Service:	<u>Default Network Access</u>
Identity Store:	Internal Users
Authorization Profiles:	
CTS Security Group:	
Authentication Method:	PAP_ASCII

Bei der ASA handelt es sich um eine einfache Radius-Reject-Nachricht, und die Authentifizierung schlägt fehl.

Um dieses Problem zu beheben, ermöglicht die ASA die Verwendung des Befehls **für die Kennwortverwaltung** unter der Tunnelgruppenkonfiguration:

```
tunnel-group RA general-attributes
 authentication-server-group ACS
 password-management
```

Der Befehl **für die Kennwortverwaltung** ändert das Verhalten, sodass die ASA in der Radius-Request MSCHAPv2 anstelle von PAP verwenden muss.

Das MSCHAPv2-Protokoll unterstützt Kennwortablauf und Kennwortänderung. Wenn also ein VPN-Benutzer während der Xauth-Phase in diese spezifische Tunnelgruppe gelandet ist, beinhaltet die Radius-Request von ASA jetzt eine MS-CHAP-Challenge:

```

Attribute Value Pairs
  ▶ AVP: l=7 t=User-Name(1): cisco
  ▶ AVP: l=6 t=NAS-Port(5): 3979366400
  ▶ AVP: l=6 t=Service-Type(6): Framed(2)
  ▶ AVP: l=6 t=Framed-Protocol(7): PPP(1)
  ▶ AVP: l=15 t=Called-Station-Id(30): 192.168.1.250
  ▶ AVP: l=15 t=Calling-Station-Id(31): 192.168.10.67
  ▶ AVP: l=6 t=NAS-Port-Type(61): Virtual(5)
  ▶ AVP: l=15 t=Tunnel-Client-Endpoint(66): 192.168.10.67
  ▼ AVP: l=24 t=Vendor-Specific(26) v=Microsoft(311)
    ▶ VSA: l=18 t=MS-CHAP-Challenge(11): 205d20e2349fe2bb15e3ed5c570d354c
  ▼ AVP: l=58 t=Vendor-Specific(26) v=Microsoft(311)
    ▶ VSA: l=52 t=MS-CHAP2-Response(25): 0000fb52f2f8dcc50b0fe2aa79b2cdd428
  ▶ AVP: l=6 t=NAS-IP-Address(4): 192.168.11.250
  ▶ AVP: l=34 t=Vendor-Specific(26) v=Cisco(9)

```

Wenn der ACS bemerkt, dass der Benutzer das Kennwort ändern muss, gibt er eine Radius-Reject-Nachricht mit dem MSCHAPv2-Fehler 648 zurück.

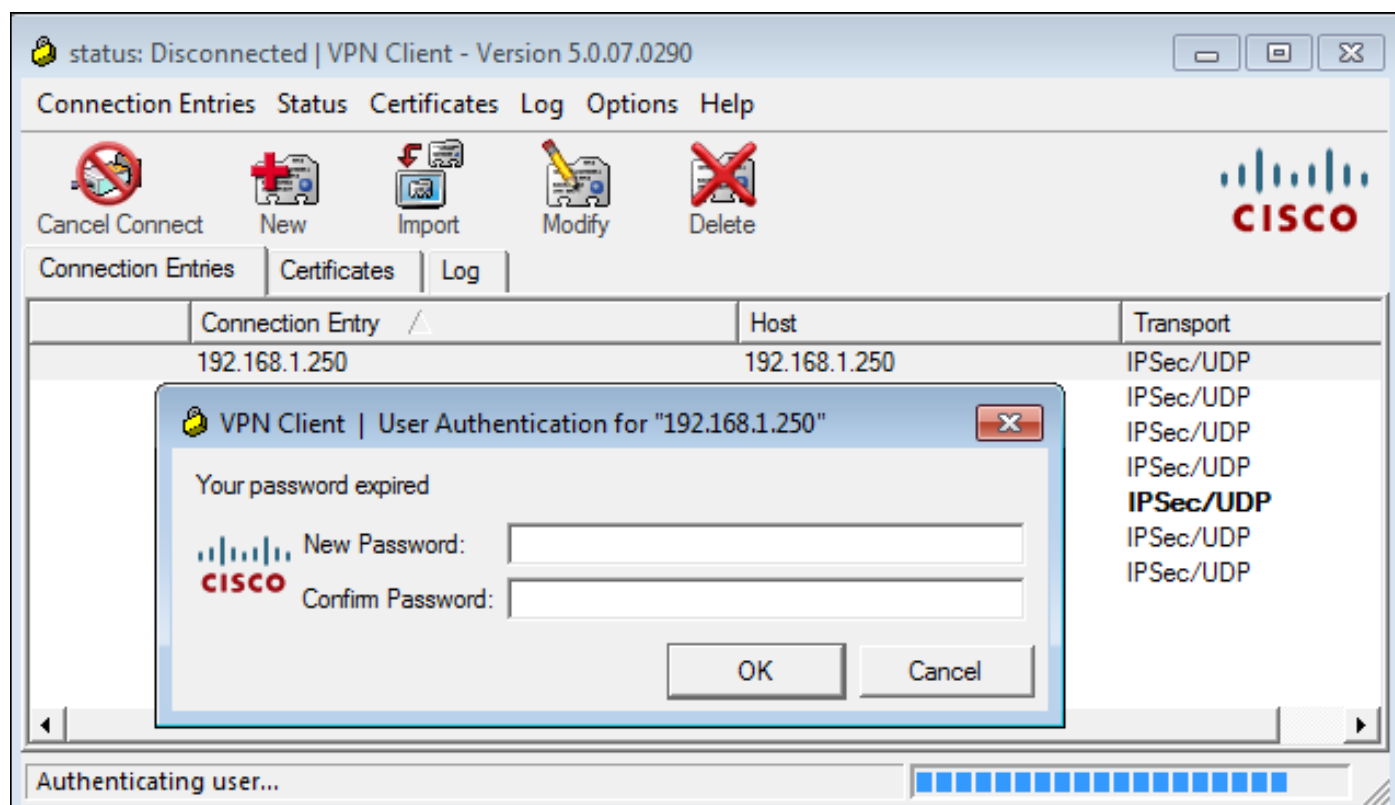
Attribute Value Pairs

- AVP: l=57 t=Vendor-Specific(26) v=Microsoft(311)
 - VSA: l=51 t=MS-CHAP-Error(2): \000E=648 R=0 C=205

Die ASA versteht diese Nachricht und verwendet MODE_CFG, um das neue Kennwort vom Cisco VPN-Client anzufordern:

```
Oct 02 06:22:26 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,  
Received Password Expiration from Auth server!
```

Der Cisco VPN-Client zeigt ein Dialogfeld an, in dem Sie zur Eingabe eines neuen Kennworts aufgefordert werden:



Die ASA sendet eine weitere Radius-Request mit MS-CHAP-CPW und MS-CHAP-NT-Enc-PW-Payload (dem neuen Kennwort):


```
▶ AVP: l=15 t=Calling-Station-Id(31): 192.168.10.67
▶ AVP: l=6 t=NAS-Port-Type(61): Virtual(5)
▶ AVP: l=15 t=Tunnel-Client-Endpoint(66): 192.168.10.67
▼ AVP: l=42 t=Vendor-Specific(26) v=Microsoft(311)
  ▶ VSA: l=36 t=MS-CHAP-NT-Enc-PW(6): 060000034d57f459fe6d4875c
▼ AVP: l=255 t=Vendor-Specific(26) v=Microsoft(311)
  ▶ VSA: l=249 t=MS-CHAP-NT-Enc-PW(6): 06000001a3a32falcad97b38
▼ AVP: l=255 t=Vendor-Specific(26) v=Microsoft(311)
  ▶ VSA: l=249 t=MS-CHAP-NT-Enc-PW(6): 0600000275b374dfc58f48f6
▼ AVP: l=24 t=Vendor-Specific(26) v=Microsoft(311)
  ▶ VSA: l=18 t=MS-CHAP-Challenge(11): 5f16e4b7338b4b8117b50896
▼ AVP: l=76 t=Vendor-Specific(26) v=Microsoft(311)
  ▶ VSA: l=70 t=MS-CHAP2-CPW(27): 07004efba53521c47b1046bbca851
▶ AVP: l=6 t=NAS-IP-Address(4): 192.168.11.250
▶ AVP: l=34 t=Vendor-Specific(26) v=Cisco(9)
```

Der ACS bestätigt die Anforderung und gibt einen Radius-Accept mit MS-CHAP2-Success zurück:

```
▼ AVP: l=51 t=Vendor-Specific(26) v=Microsoft(311)
  ▶ VSA: l=45 t=MS-CHAP2-Success(26): 00533d324144414
```

Dies kann im ACS überprüft werden, der die Meldung '24204 Password has successfully' (Kennwort erfolgreich geändert 24204) meldet:

Steps
11001 Received RADIUS Access-Request
11017 RADIUS created a new session
<u>Evaluating Service Selection Policy</u>
15004 Matched rule
15012 Selected Access Service - Default Network Access
<u>Evaluating Identity Policy</u>
15006 Matched Default Rule
15013 Selected Identity Store - Internal Users
24214 MSCHAP is used for the change password request in the internal users identity store.
24212 Found User in Internal Users IDStore
24204 Password changed successfully
22037 Authentication Passed
<u>Evaluating Group Mapping Policy</u>
15006 Matched Default Rule
<u>Evaluating Exception Authorization Policy</u>
15042 No rule was matched
<u>Evaluating Authorization Policy</u>
15006 Matched Default Rule
15016 Selected Authorization Profile - Permit Access
22065 Max sessions policy passed
22064 New accounting session created in Session cache
11002 Returned RADIUS Access-Accept

Die ASA meldet dann eine erfolgreiche Authentifizierung und fährt mit dem Quick Mode (QM)-Prozess fort:

```
Oct 02 06:22:28 [IKEv1]Group = RA, Username = cisco, IP = 192.168.10.67,
User (cisco) authenticated.
```

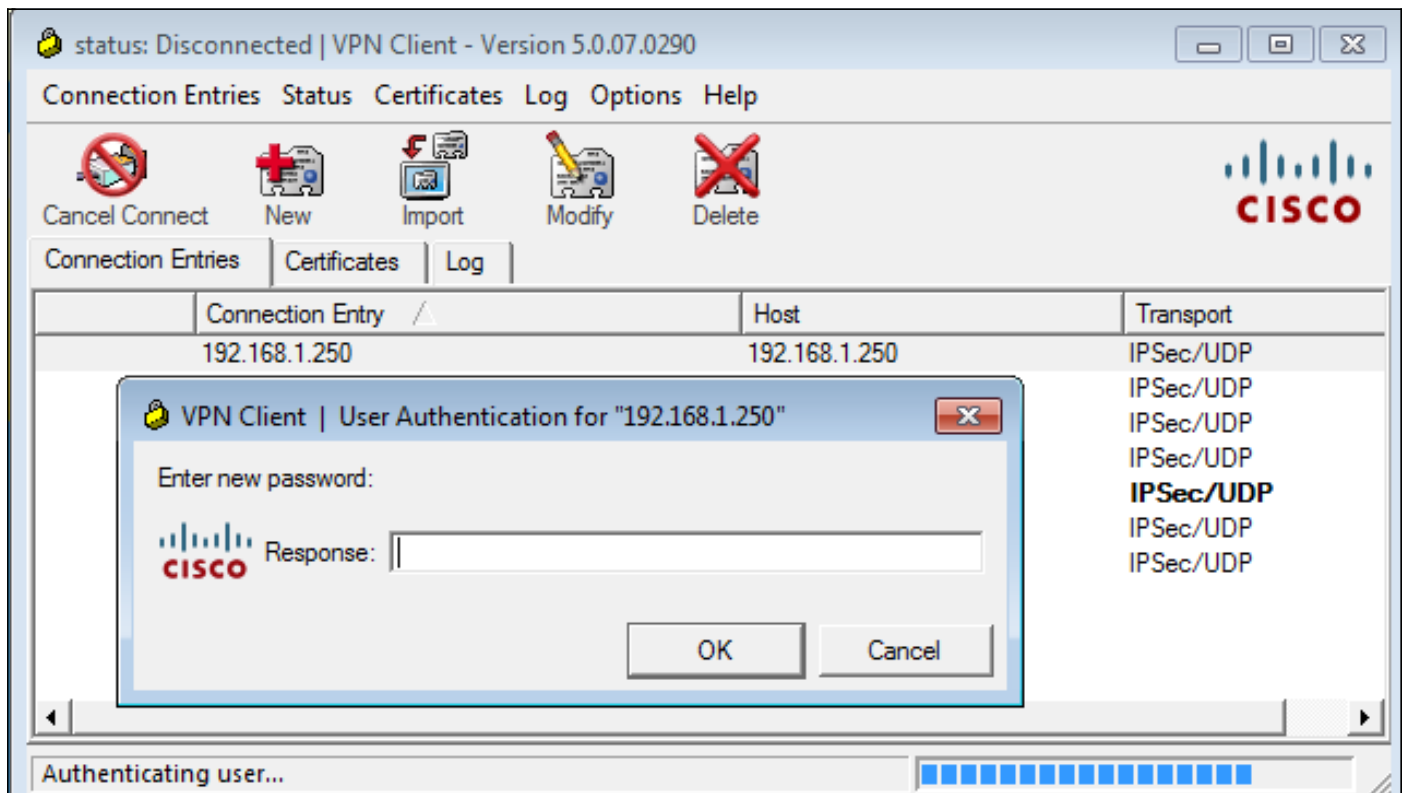
ASA mit ACS über TACACS+

Ebenso kann TACACS+ für das Ablaufdatum und die Änderung von Kennwörtern verwendet werden. Die Funktion zur Kennwortverwaltung ist nicht erforderlich, da die ASA noch immer TACACS+ mit einem Authentifizierungstyp von ASCII anstelle von MSCHAPv2 verwendet.

Mehrere Pakete werden ausgetauscht, und ACS fordert ein neues Kennwort an:

```
▼ Decrypted Reply
  Status: 0x3 (Send Data)
  Flags: 0x01 (NoEcho)
  Server message length: 20
  Server message: Enter new password:
  Data length: 0
```

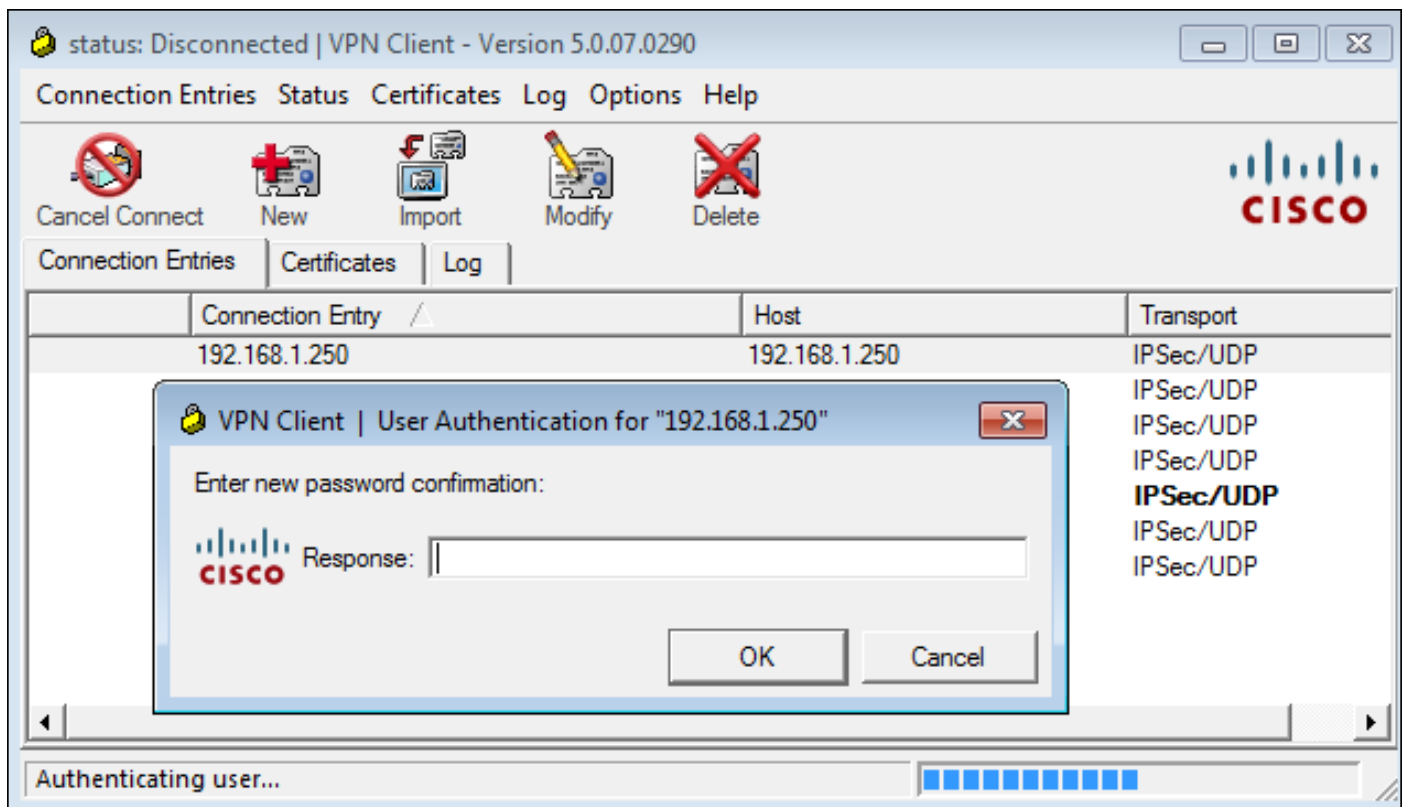
Der Cisco VPN-Client zeigt ein Dialogfeld an (das sich von dem von RADIUS verwendeten Dialogfeld unterscheidet), in dem Sie zur Eingabe eines neuen Kennworts aufgefordert werden:



ACS fordert Bestätigung des neuen Kennworts an:

```
▼ Decrypted Reply
  Status: 0x3 (Send Data)
  Flags: 0x01 (NoEcho)
  Server message length: 33
  Server message: Enter new password confirmation:
  Data length: 0
```

Der Cisco VPN-Client stellt ein Bestätigungsfeld bereit:



Wenn die Bestätigung richtig ist, meldet der ACS eine erfolgreiche Authentifizierung:

```
▼ Decrypted Reply
  Status: 0x1 (Authentication Passed)
  Flags: 0x00
  Server message length: 0
  Data length: 0
```

ACS protokolliert dann ein Ereignis, dass das Kennwort erfolgreich geändert wurde:

Evaluating Identity Policy

Matched Default Rule

Selected Identity Store - Internal Users

Looking up User in Internal Users IDStore - cisco

User need to change password

Found User in Internal Users IDStore

Invalid workflow sequence type

TACACS+ will use the password prompt from global TACACS+ configuration.

Returned TACACS+ Authentication Reply

Received TACACS+ Authentication CONTINUE Request

Using previously selected Access Service

Identity Policy was evaluated before; Identity Sequence continuing

Looking up User in Internal Users IDStore - cisco

User need to change password

Found User in Internal Users IDStore

TACACS+ ASCII change password request.

Returned TACACS+ Authentication Reply

Received TACACS+ Authentication CONTINUE Request

Using previously selected Access Service

Returned TACACS+ Authentication Reply

Received TACACS+ Authentication CONTINUE Request

Using previously selected Access Service

Identity Policy was evaluated before; Identity Sequence continuing

PAP is used for the change password request in the internal users identity store.

Found User in Internal Users IDStore

Password changed successfully

Authentication Passed

Die ASA-Debugger zeigen den gesamten Austauschprozess und die erfolgreiche Authentifizierung an:

```
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,  
Received challenge status!  
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,  
process_attr(): Enter!
```

```
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Processing MODE_CFG Reply attributes
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
    Received challenge status!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
process_attr(): Enter!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Processing MODE_CFG Reply attributes.
Oct 02 07:44:41 [IKEv1]Group = RA, Username = cisco, IP = 192.168.10.67,
User (cisco) authenticated.
```

Diese Kennwortänderung ist für ASA vollkommen transparent. Die TACACS+-Sitzung mit mehr Anforderungs- und Antwortpaketen, die vom VPN-Client analysiert und dem Benutzer angezeigt werden, der das Kennwort ändert, ist etwas länger.

ASA mit LDAP

Kennwortablauf und Kennwortänderungen werden vollständig vom Microsoft AD- und Sun LDAP-Serverschema unterstützt.

Bei einer Kennwortänderung geben die Server 'bindresponse = invalidCredentials' mit 'error = 773' zurück. Dieser Fehler weist darauf hin, dass der Benutzer das Kennwort zurücksetzen muss. Typische Fehlercodes sind:

Fehlercode Fehler

525	Benutzer nicht gefunden
52 e	Ungültige Anmeldeinformationen
530	Derzeit ist die Anmeldung nicht gestattet.
531	Anmeldung an dieser Workstation nicht gestattet
532	Kennwort abgelaufen
533	Konto deaktiviert
701	Konto abgelaufen
773	Benutzer muss Kennwort zurücksetzen
775	Benutzerkonto gesperrt

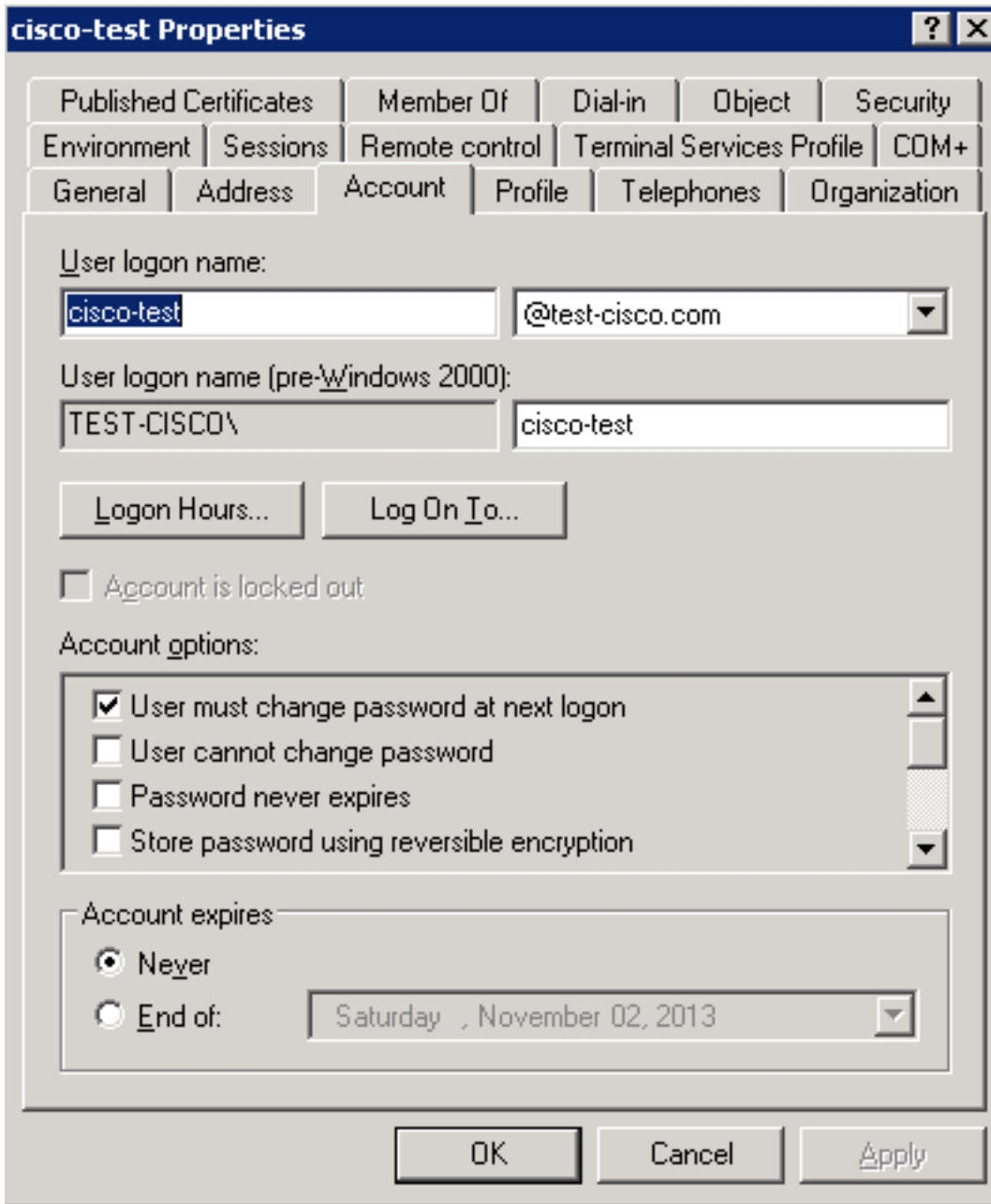
Konfigurieren Sie den LDAP-Server:

```
aaa-server LDAP protocol ldap
aaa-server LDAP (outside) host 10.48.66.128
  ldap-base-dn CN=USers,DC=test-cisco,DC=com
  ldap-scope subtree
  ldap-naming-attribute sAMAccountName
  ldap-login-password *****
  ldap-login-dn CN=Administrator,CN=users,DC=test-cisco,DC=com
  server-type microsoft
```

Verwenden Sie diese Konfiguration für die Tunnelgruppe und die Kennwortverwaltungsfunktion:

```
tunnel-group RA general-attributes
  address-pool POOL
  authentication-server-group LDAP
  default-group-policy MY
password-management
```

Konfigurieren Sie den AD-Benutzer so, dass eine Kennwortänderung erforderlich ist:



Wenn der Benutzer versucht, den Cisco VPN-Client zu verwenden, meldet die ASA ein ungültiges Kennwort:

```
ASA(config-tunnel-general)# debug ldap 255
<some output ommited for clarity>
```

```
[111] Session Start
[111] New request Session, context 0xbd835c10, reqType = Authentication
[111] Fiber started
[111] Creating LDAP context with uri=ldap://10.48.66.128:389
[111] Connect to LDAP server: ldap://10.48.66.128:389, status = Successful
[111] supportedLDAPVersion: value = 3
[111] supportedLDAPVersion: value = 2
[111] Binding as Administrator
[111] Performing Simple authentication for Administrator to 10.48.66.128
[111] LDAP Search:
      Base DN = [CN=USers,DC=test-cisco,DC=com]
      Filter  = [sAMAccountName=cisco-test]
      Scope   = [SUBTREE]
[111] User DN = [CN=cisco-test,CN=Users,DC=test-cisco,DC=com]
```

```

[111] Talking to Active Directory server 10.48.66.128
[111] Reading password policy for cisco-test, dn:CN=cisco-test,CN=Users,
DC=test-cisco,DC=com
[111] Read bad password count 2
[111] Binding as cisco-test
[111] Performing Simple authentication for cisco-test to 10.48.66.128
[111] Simple authentication for cisco-test returned code (49) Invalid
credentials
[111] Message (cisco-test): 80090308: LdapErr: DSID-0C090334, comment:
AcceptSecurityContext error, data 773, vece
[111] Invalid password for cisco-test

```

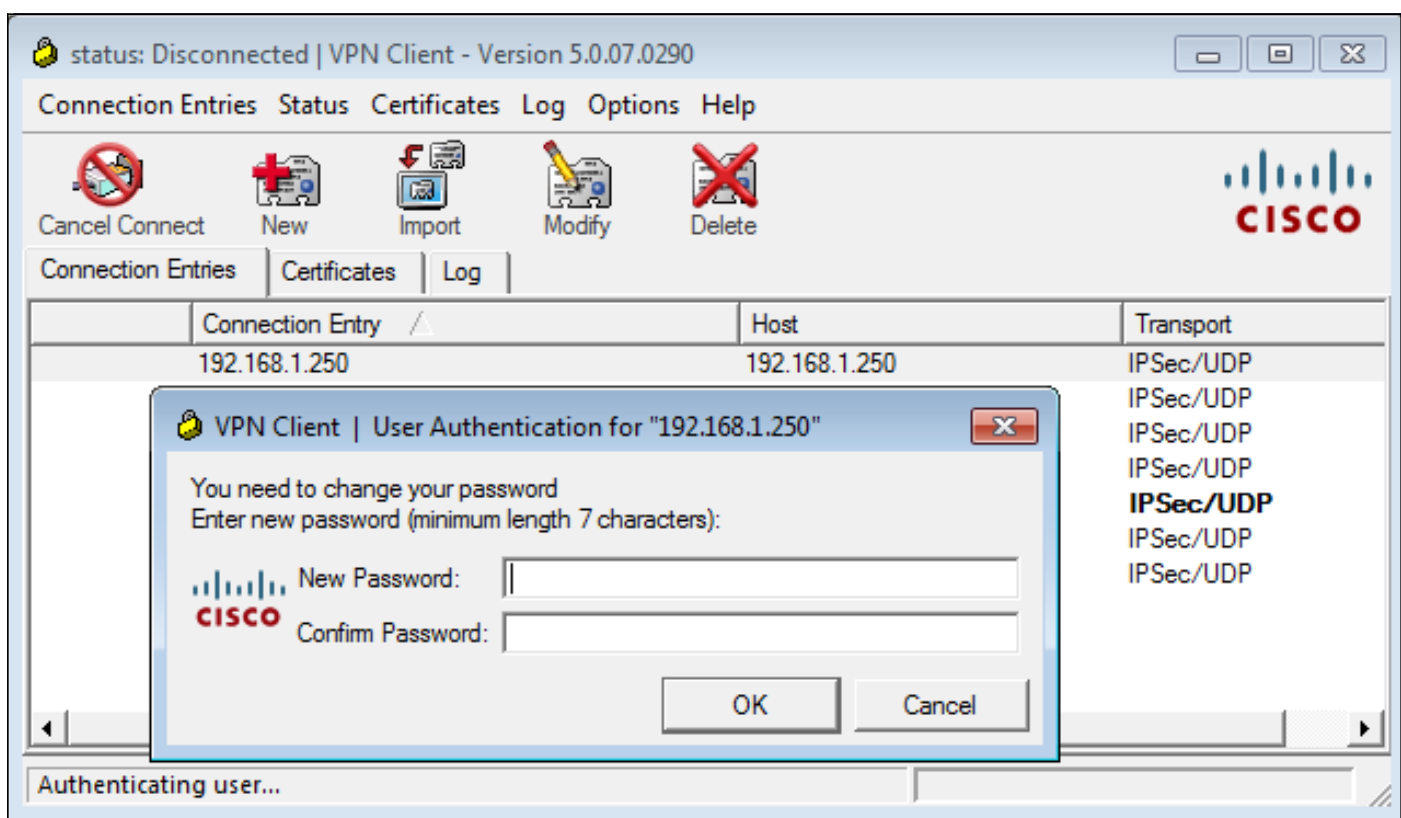
Wenn die Anmeldeinformationen ungültig sind, wird der Fehler 52e angezeigt:

```

[110] Message (cisco-test): 80090308: LdapErr: DSID-0C090334, comment:
AcceptSecurityContext error, data 52e, vece

```

Anschließend fordert der Cisco VPN-Client eine Kennwortänderung an:



Dieses Dialogfeld unterscheidet sich vom Dialogfeld, das von TACACS oder RADIUS verwendet wird, da die Richtlinie angezeigt wird. In diesem Beispiel ist die Richtlinie eine Kennwortlänge von mindestens sieben Zeichen.

Sobald der Benutzer das Kennwort ändert, erhält die ASA möglicherweise die folgende Fehlermeldung vom LDAP-Server:

```

[113] Modify Password for cisco-test successfully converted password to unicode
[113] modify failed, no SSL enabled on connection

```

Microsoft-Richtlinien erfordern die Verwendung von SSL (Secure Sockets Layer) zur Kennwortänderung. Ändern Sie die Konfiguration:

```

aaa-server LDAP (outside) host 10.48.66.128
  ldap-over-ssl enable

```

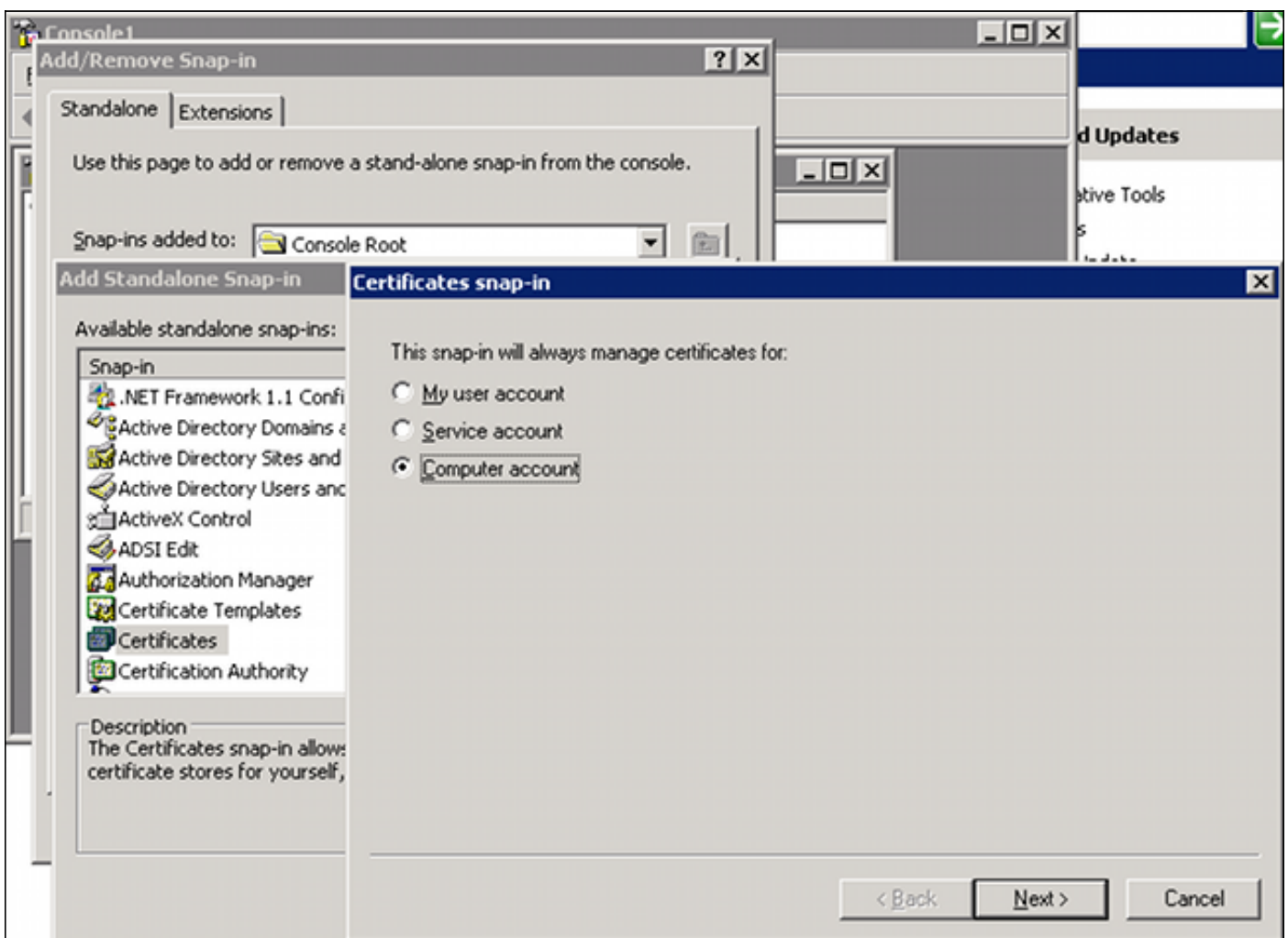

Microsoft LDAP für SSL

Standardmäßig funktioniert Microsoft LDAP über SSL nicht. Um diese Funktion zu aktivieren, müssen Sie das Zertifikat für das Computerkonto mit der richtigen Schlüsselerweiterung installieren. Weitere Informationen [finden Sie unter Aktivieren von LDAP über SSL bei einer Zertifizierungsstelle eines Drittanbieters](#).

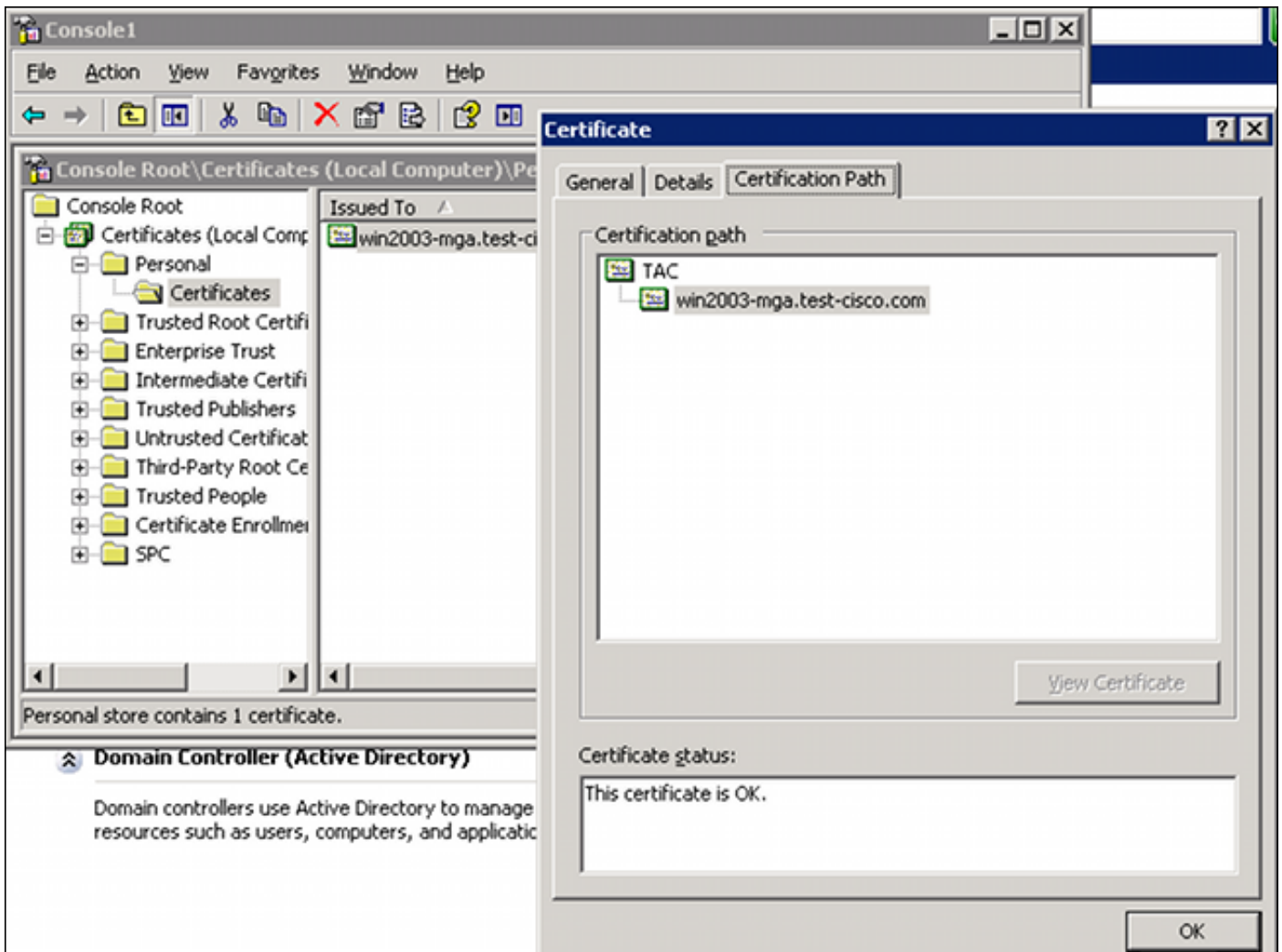
Das Zertifikat kann auch ein selbstsigniertes Zertifikat sein, da die ASA das LDAP-Zertifikat nicht prüft. Eine entsprechende Erweiterungsanforderung finden Sie unter Cisco Bug ID [CSCui40212](#), "Allow ASA to validate certificate from LDAPS server".

Hinweis: ACS überprüft das LDAP-Zertifikat in Version 5.5 und höher.

Um das Zertifikat zu installieren, öffnen Sie die MMC-Konsole, wählen Sie **Snap-In hinzufügen/entfernen**, fügen Sie das Zertifikat hinzu, und wählen Sie **Computerkonto**:



Wählen Sie **Lokaler Computer** aus, importieren Sie das Zertifikat in den persönlichen Speicher, und verschieben Sie das entsprechende Zertifikat der Zertifizierungsstelle (Certificate Authority, CA) in den vertrauenswürdigen Speicher. Überprüfen Sie, ob das Zertifikat vertrauenswürdig ist:



In ASA Version 8.4.2 gibt es einen Fehler, der bei der Verwendung von LDAP über SSL zurückgegeben werden kann:

```
ASA(config)# debug ldap 255
```

```
[142] Connect to LDAP server: ldaps://10.48.66.128:636, status = Successful
[142] supportedLDAPVersion: value = 3
[142] supportedLDAPVersion: value = 2
[142] Binding as Administrator
[142] Performing Simple authentication for Administrator to 10.48.66.128
[142] LDAP Search:
      Base DN = [CN=Users,DC=test-cisco,DC=com]
      Filter  = [sAMAccountName=Administrator]
      Scope   = [SUBTREE]
[142] Request for Administrator returned code (-1) Can't contact LDAP server
```

ASA Version 9.1.3 funktioniert mit derselben Konfiguration ordnungsgemäß. Es gibt zwei LDAP-Sitzungen. Die erste Sitzung gibt einen Fehler mit dem Code 773 (Kennwort abgelaufen) zurück, während die zweite Sitzung für die Kennwortänderung verwendet wird:

```
[53] Session Start
[53] New request Session, context 0xadebe3d4, reqType = Modify Password
[53] Fiber started
[53] Creating LDAP context with uri=ldaps://10.48.66.128:636
[53] Connect to LDAP server: ldaps://10.48.66.128:636, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
```

```

[53] Binding as Administrator
[53] Performing Simple authentication for Administrator to 10.48.66.128
[53] LDAP Search:
      Base DN = [CN=Users,DC=test-cisco,DC=com]
      Filter  = [sAMAccountName=cisco-test]
      Scope   = [SUBTREE]
[53] User DN = [CN=cisco-test,CN=Users,DC=test-cisco,DC=com]
[53] Talking to Active Directory server 10.48.66.128
[53] Reading password policy for cisco-test, dn:CN=cisco-test,CN=Users,
DC=test-cisco,DC=com
[53] Read bad password count 0
[53] Change Password for cisco-test successfully converted old password to
unicode
[53] Change Password for cisco-test successfully converted new password to
unicode
[53] Password for cisco-test successfully changed
[53] Retrieved User Attributes:

```

```

<...most attributes details omitted for clarity>
accountExpires: value = 13025656800000000 <----- 100ns intervals since
January 1, 1601 (UTC)

```

Überprüfen Sie die Pakete, um die Kennwortänderung zu überprüfen. Der private Schlüssel des LDAP-Servers kann von Wireshark zum Entschlüsseln von SSL-Datenverkehr verwendet werden:

75	10.48.67.229	10.48.66.128	LDAP	239	modifyRequest(7)	"CN=cisco-test,CN=Users,DC=test-cisco,DC=com"
76	10.48.66.128	10.48.67.229	LDAP	113	modifyResponse(7)	success

Frame 75: 239 bytes on wire (1912 bits), 239 bytes captured (1912 bits)

- ▶ Ethernet II, Src: Cisco_b8:6b:25 (00:17:5a:b8:6b:25), Dst: Vmware_90:69:16 (00:0c:29:90:69:16)
- ▶ Internet Protocol Version 4, Src: 10.48.67.229 (10.48.67.229), Dst: 10.48.66.128 (10.48.66.128)
- ▶ Transmission Control Protocol, Src Port: 31172 (31172), Dst Port: ldaps (636), Seq: 4094749281, Ack: 1574938153,
- ▶ Secure Sockets Layer
- ▼ Lightweight Directory Access Protocol
 - ▼ LDAPMessage modifyRequest(7) "CN=cisco-test,CN=Users,DC=test-cisco,DC=com"
 - messageID: 7
 - ▼ protocolOp: modifyRequest (6)
 - ▼ modifyRequest
 - object: CN=cisco-test,CN=Users,DC=test-cisco,DC=com
 - ▼ modification: 2 items
 - ▼ modification item
 - operation: delete (1)
 - ▶ modification unicodePwd
 - ▼ modification item
 - operation: add (0)
 - ▶ modification unicodePwd

[\[Response In: 76\]](#)

Die Debug-Fehler für Internet Key Exchange (IKE)/Authentifizierung, Autorisierung und Abrechnung (AAA) auf der ASA ähneln denen im RADIUS-Authentifizierungsszenario.

LDAP und Warnung vor Ablauf

Für LDAP können Sie eine Funktion verwenden, die eine Warnung sendet, bevor ein Kennwort abläuft. Die ASA warnt den Benutzer 90 Tage vor Ablauf des Kennworts mit der folgenden Einstellung:

```

tunnel-group RA general-attributes
  password-management password-expire-in-days 90

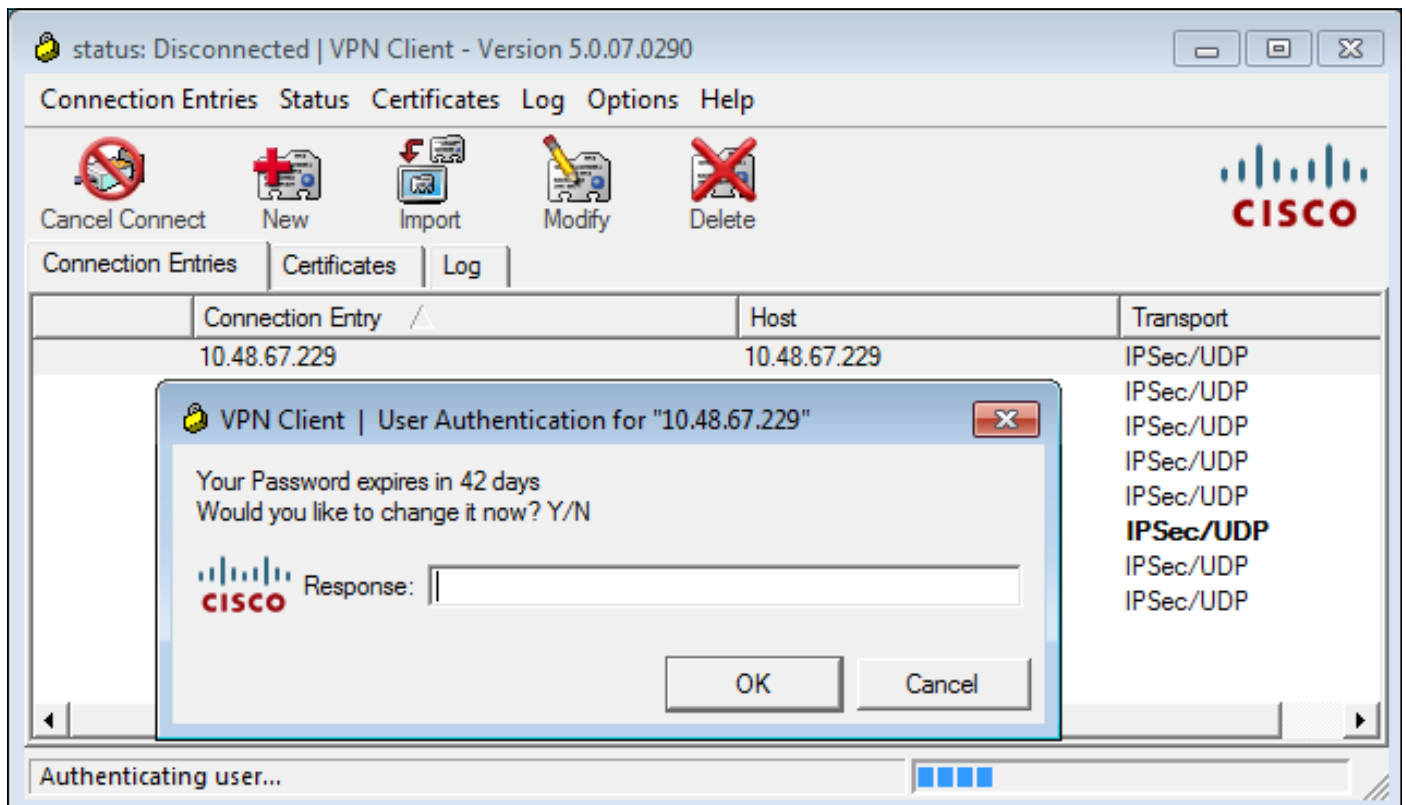
```

In diesem Fall läuft das Kennwort in 42 Tagen ab und der Benutzer versucht, sich anzumelden:

```
ASA# debug ldap 255
<some outputs removed for clarity>
```

```
[84] Binding as test-cisco
[84] Performing Simple authentication for test-cisco to 10.48.66.128
[84] Processing LDAP response for user test-cisco
[84] Message (test-cisco):
[84] Checking password policy
[84] Authentication successful for test-cisco to 10.48.66.128
[84] now: Fri, 04 Oct 2013 09:41:55 GMT, lastset: Fri, 04 Oct 2013 09:07:23
GMT, delta=2072, maxage=1244139139 secs
[84] expire in: 3708780 secs, 42 days
[84] Password expires Sat, 16 Nov 2013 07:54:55 GMT
[84] Password expiring in 42 day(s), threshold 90 days
```

Die ASA sendet eine Warnung und bietet die Möglichkeit einer Kennwortänderung:



Wenn der Benutzer das Kennwort ändern möchte, wird eine Aufforderung zur Eingabe eines neuen Kennworts angezeigt, und die normale Kennwortänderung wird gestartet.

ASA und L2TP

In den vorherigen Beispielen wurden IKE-Version 1 (IKEv1) und ein IPSec-VPN vorgestellt.

Für das Layer 2 Tunneling Protocol (L2TP) und IPSec wird PPP als Transport für die Authentifizierung verwendet. MSCHAPv2 ist anstelle von PAP erforderlich, damit eine Kennwortänderung funktioniert:

```
ciscoasa(config-tunnel-general)# tunnel-group DefaultRAGroup ppp-attributes
ciscoasa(config-ppp)# authentication ms-chap-v2
```

Für erweiterte Authentifizierung in L2TP in der PPP-Sitzung wird MSCHAPv2 ausgehandelt:

```
▸ Ethernet II, Src: Receive_24 (20:52:45:43:56:24), Dst: Receive_24 (20:52:45:43:56:24)
▾ PPP Link Control Protocol
  Code: Configuration Request (1)
  Identifier: 1 (0x01)
  Length: 15
  ▾ Options: (11 bytes), Authentication Protocol, Magic Number
    ▾ Authentication Protocol: Challenge Handshake Authentication Protocol (0xc223)
      Type: Authentication Protocol (3)
      Length: 5
      Authentication Protocol: Challenge Handshake Authentication Protocol (0xc223)
      Algorithm: MS-CHAP-2 (129)
    ▸ Magic Number: 0x561ad534
```

Wenn das Benutzerkennwort abgelaufen ist, wird ein Fehler mit dem Code 648 zurückgegeben:

```
▾ PPP Challenge Handshake Authentication Protocol
  Code: Failure (4)
  Identifier: 1
  Length: 17
  Message: E=648 R=0 V=3
```

Anschließend muss das Kennwort geändert werden. Der restliche Prozess ähnelt dem Szenario für RADIUS mit MSCHAPv2.

Siehe [L2TP Over IPsec Between Windows 200/XP PC and PIX/ASA 7.2 Using Pre-shared Key Configuration Example](#) for additional details on how to configure L2TP.

ASA SSL VPN-Client

Die vorherigen Beispiele beziehen sich auf IKEv1 und den Cisco VPN-Client, der End-of-Life (EOL) ist.

Die empfohlene Lösung für ein VPN mit Remote-Zugriff ist Cisco AnyConnect Secure Mobility, die die Protokolle IKE Version 2 (IKEv2) und SSL verwendet. Die Funktionen für Kennwortänderung und Ablaufdatum sind für Cisco AnyConnect identisch mit denen für den Cisco VPN-Client.

Für IKEv1 wurden die Kennwortänderungs- und Ablaufdaten in Phase 1.5 (Xauth/Mode-Konfiguration) zwischen ASA und VPN-Client ausgetauscht.

Für IKEv2 ist dies ähnlich. Der Konfigurationsmodus verwendet CFG_REQUEST/CFG_REPLY-Pakete.

Bei SSL befinden sich die Daten in der Datagram Transport Layer Security (DTLS)-Sitzung.

Die Konfiguration ist für die ASA identisch.

Dies ist eine Beispielkonfiguration mit Cisco AnyConnect und dem SSL-Protokoll mit einem LDAP-Server über SSL:

```
aaa-server LDAP protocol ldap
aaa-server LDAP (outside) host win2003-mga.test-cisco.com
  ldap-base-dn CN=Users,DC=test-cisco,DC=com
  ldap-scope subtree
  ldap-naming-attribute sAMAccountName
  ldap-login-password *****
  ldap-login-dn CN=Administrator,CN=users,DC=test-cisco,DC=com
  ldap-over-ssl enable
  server-type microsoft

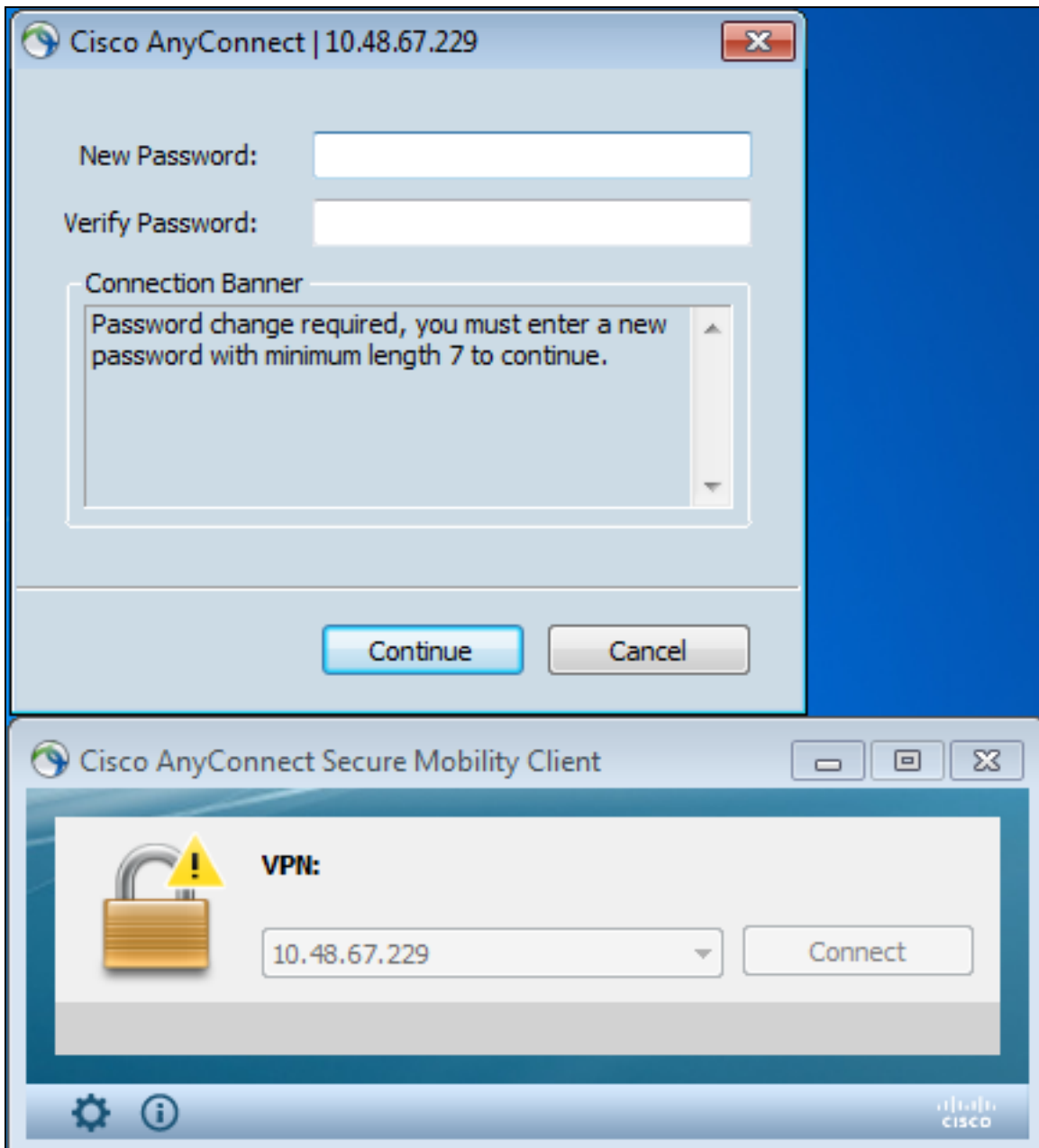
webvpn
  enable outside
  anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
  anyconnect enable
  tunnel-group-list enable

group-policy MY internal
group-policy MY attributes
  vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless

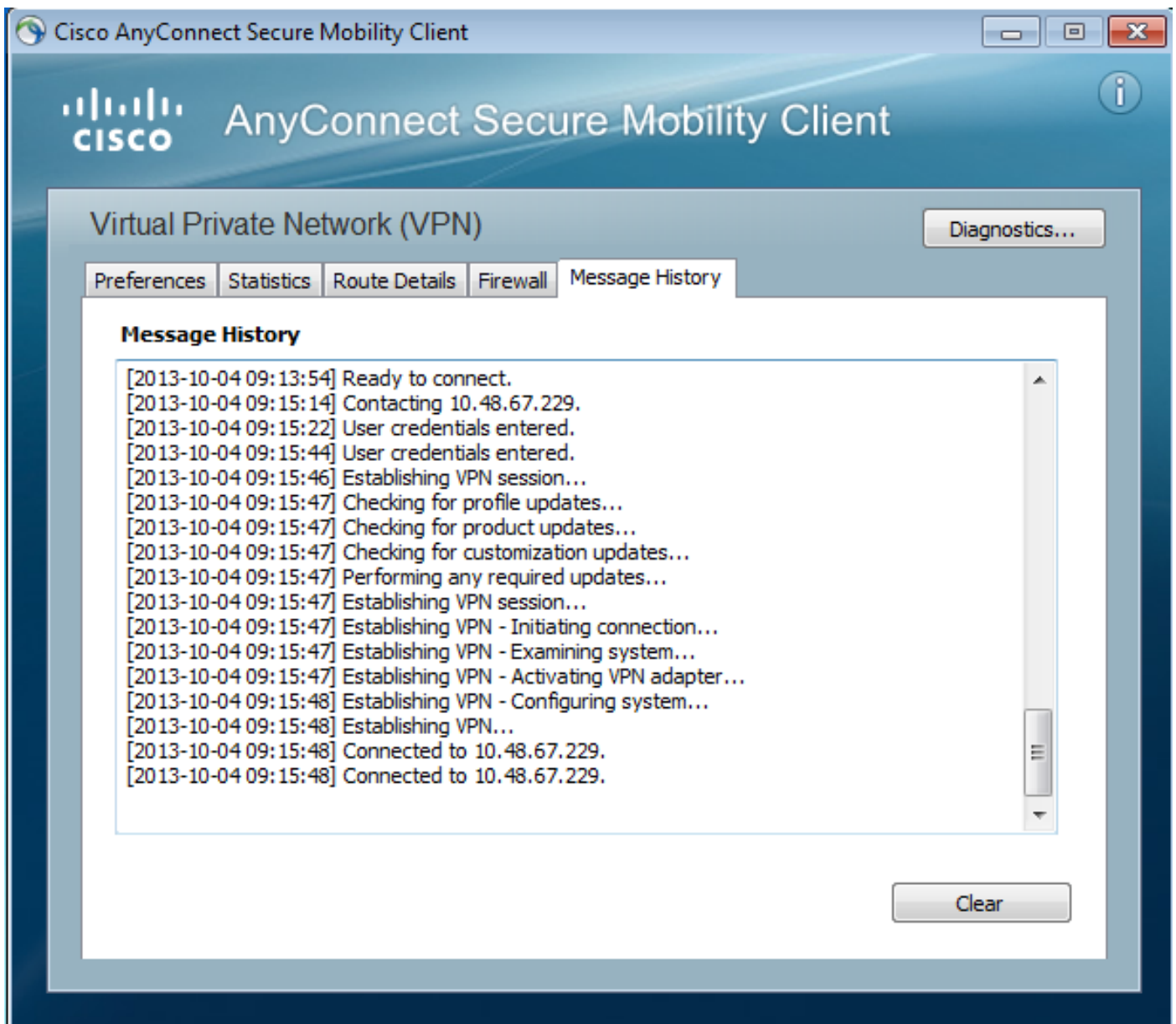
tunnel-group RA type remote-access
tunnel-group RA general-attributes
  address-pool POOL
  authentication-server-group LDAP
  default-group-policy MY
  password-management
tunnel-group RA webvpn-attributes
  group-alias RA enable
  without-csd

ip local pool POOL 192.168.11.100-192.168.11.105 mask 255.255.255.0
```

Sobald das richtige Kennwort (das abgelaufen ist) eingegeben wurde, versucht Cisco AnyConnect eine Verbindung herzustellen und fordert ein neues Kennwort an:



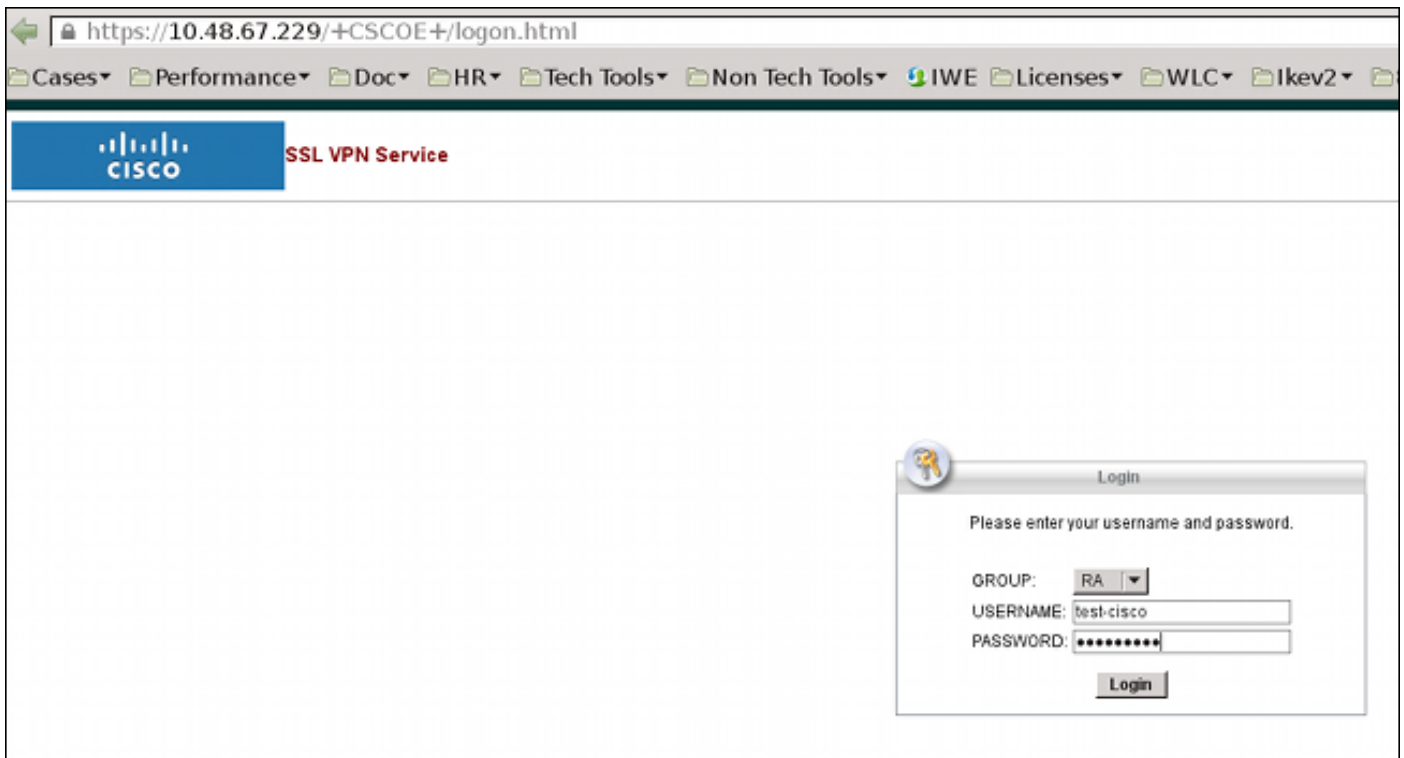
Die Protokolle zeigen an, dass die Benutzeranmeldeinformationen zweimal eingegeben wurden:



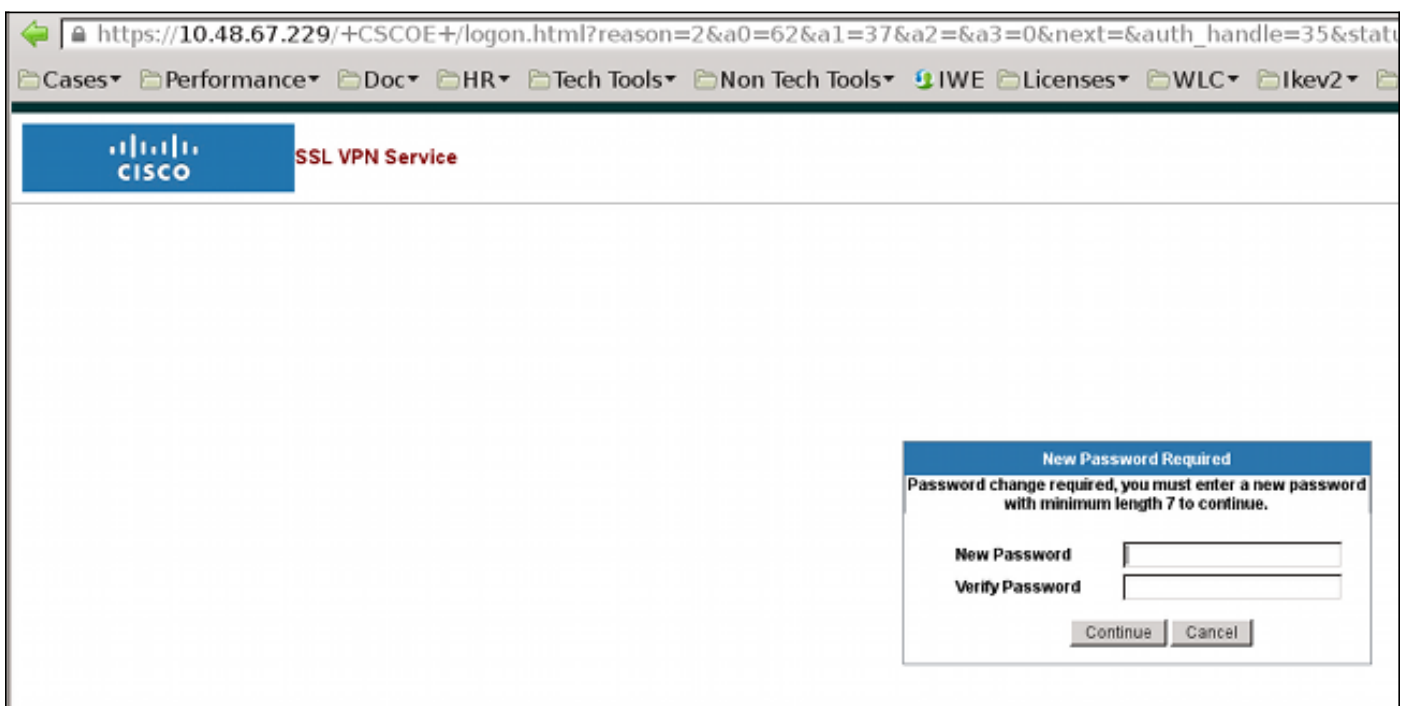
Ausführlichere Protokolle finden Sie im Diagnostic AnyConnect Reporting Tool (DART).

ASA SSL-Webportal

Der gleiche Anmeldeprozess findet im Webportal statt:



Der Kennwortablauf und der gleiche Kennwortänderungsprozess erfolgen:



ACS-Benutzerkennwort ändern

Wenn es nicht möglich ist, das Kennwort über das VPN zu ändern, können Sie den dedizierten Webservice für das ACS User Change Password (UCP) verwenden. Siehe [Software Developer's Guide for Cisco Secure Access Control System 5.4: Verwenden der UCP-Webdienste](#).

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- [Konfigurationsanleitung für die Cisco Serie ASA 5500 unter Verwendung der CLI, 8.4 und 8.6: Konfigurieren eines externen Servers für die Benutzerautorisierung der Sicherheitsappliance](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)