ASA遠端訪問VPN IKE/SSL - RADIUS、TACACS和LDAP的密碼到期和更改配置示例

目錄

簡介

本文檔介紹在思科自適應安全裝置(ASA)上終止的遠端訪問VPN隧道中的密碼到期和密碼更改功能。 本文檔涵蓋：

- 不同使用者端：Cisco VPN客戶端和Cisco AnyConnect Security Mobility
- 不同的通訊協定：TACACS、RADIUS和輕量型目錄存取通訊協定(LDAP)
- 思科安全存取控制系統(ACS)上的不同儲存區：本地和Active Directory(AD)

必要條件

需求

思科建議您瞭解以下主題：

- 通過命令列介面(CLI)瞭解ASA配置
- ASA上VPN配置的基本知識
- Cisco Secure ACS基礎知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科自適應安全裝置8.4版及更高版本
- Microsoft Windows Server 2003 SP1
- 思科安全存取控制系統5.4版或更高版本
- Cisco AnyConnect安全行動化版本3.1
- Cisco VPN使用者端，版本5

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

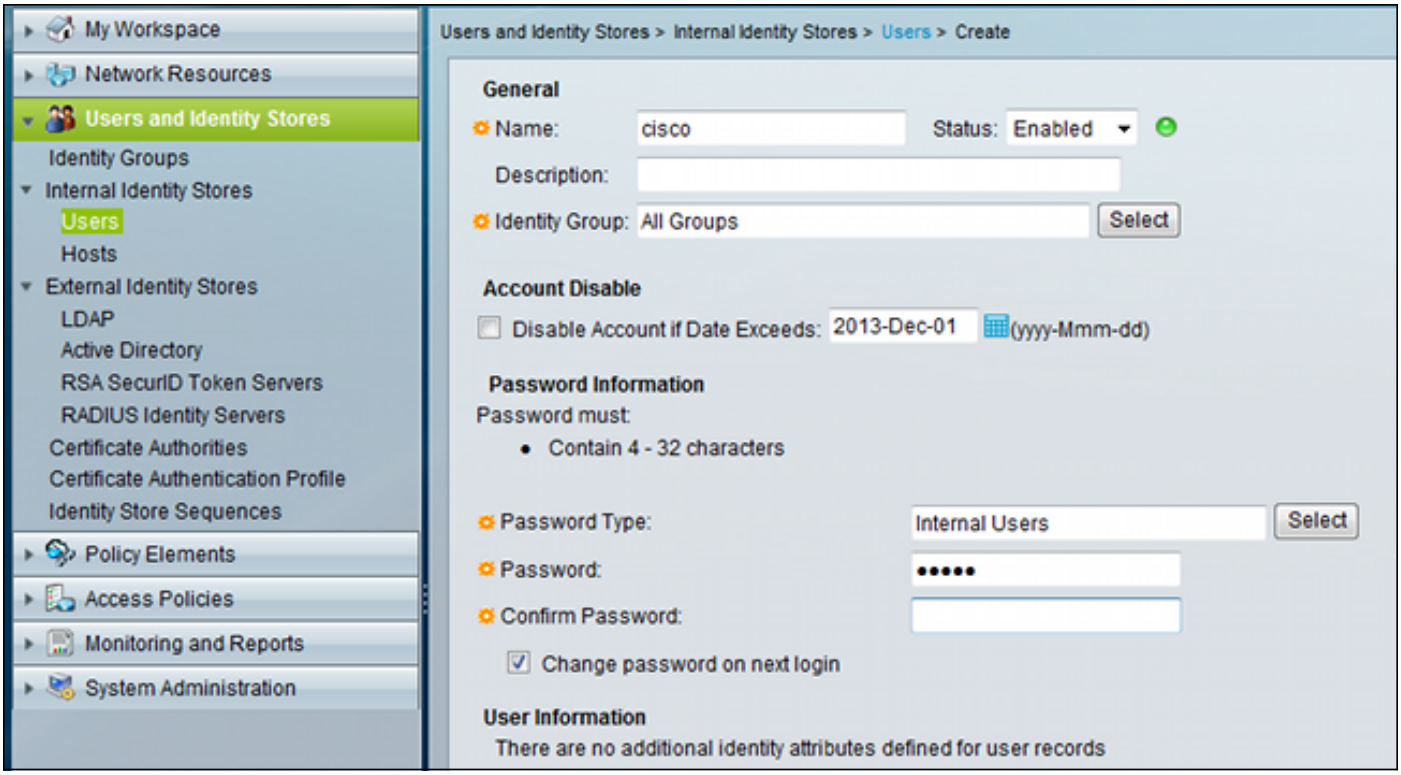
> **附註**：
>
> 使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。
>
> 使用 **debug 指令之前，請先參閱**有關 Debug 指令的重要資訊。

具有本地身份驗證的ASA

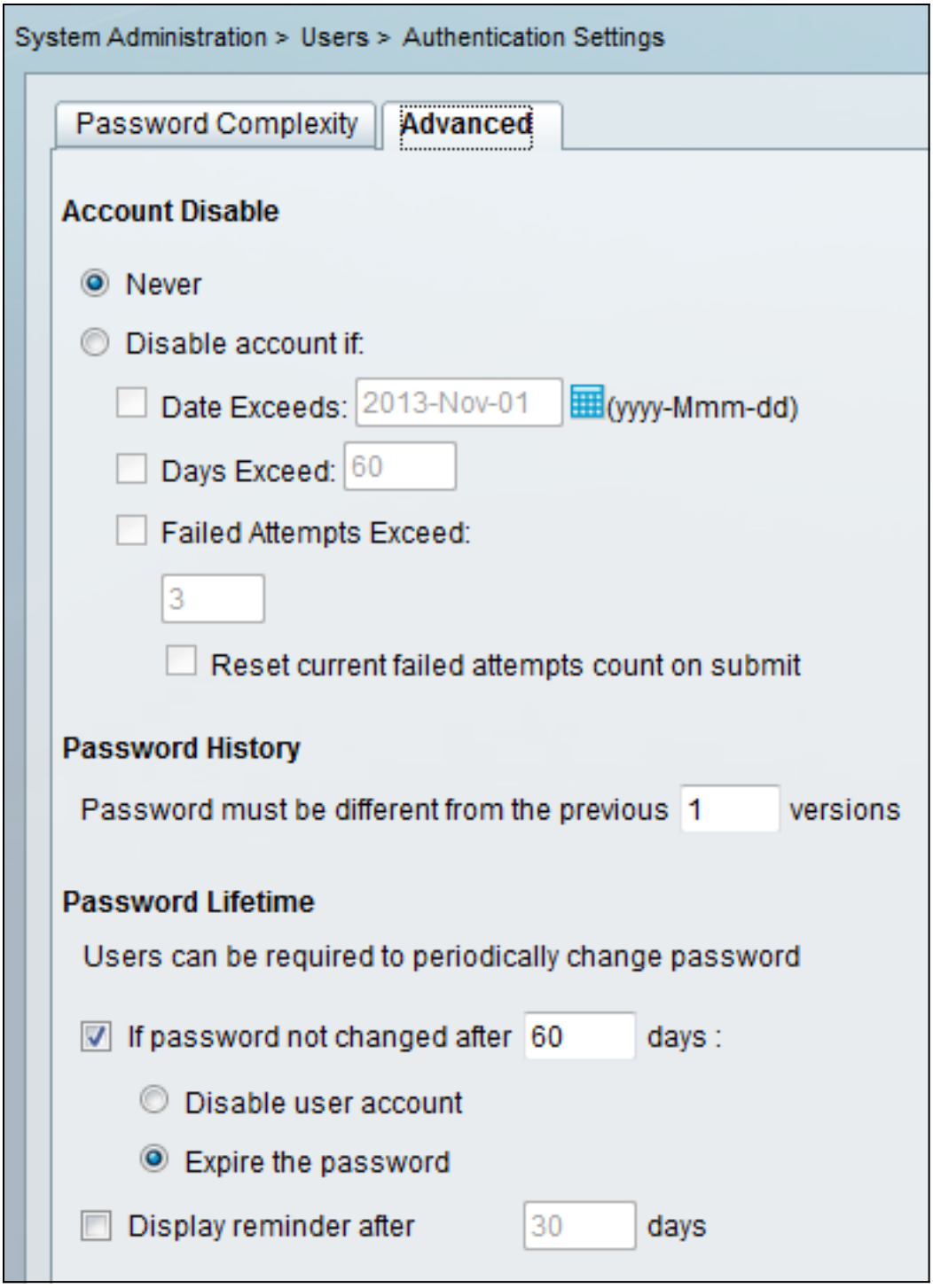
具有本地定義使用者的ASA不允許使用密碼過期或密碼更改功能。需要外部伺服器，例如RADIUS、TACACS、LDAP或Windows NT。

ACS和本地使用者

ACS支援本地定義使用者的密碼到期和密碼更改。例如，您可以強制新建立的使用者在下次登入時更改密碼，或者可以在特定日期禁用帳戶：

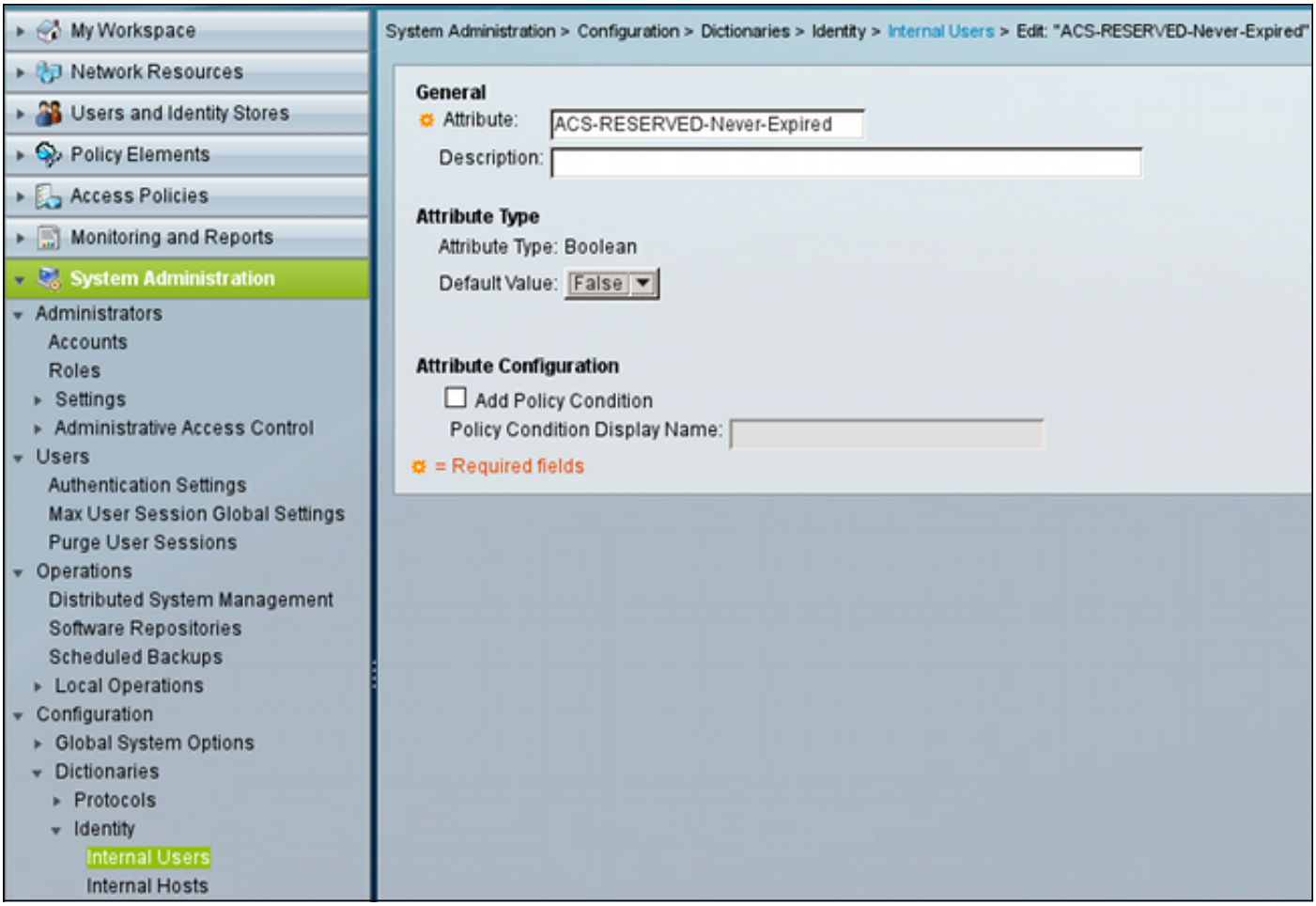


您可以為所有使用者配置密碼策略。例如，密碼到期後，您可以禁用使用者帳戶（阻止它而不能夠登入），或者提供更改密碼的選項：

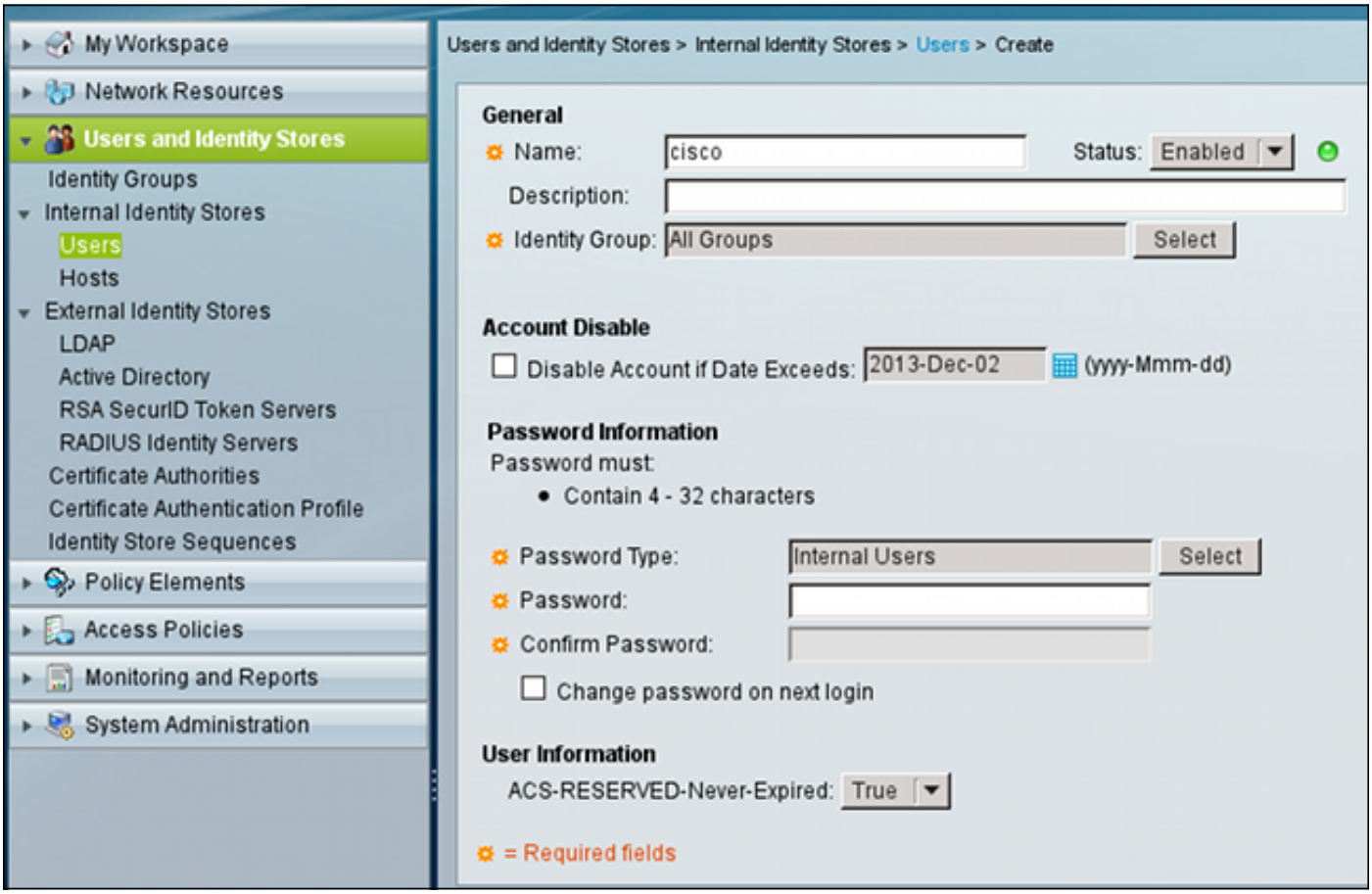


特定於使用者的設定優先於全域性設定。

ACS-RESERVED-Never-Expired是使用者身份的內部屬性。



此屬性由使用者啟用，可用於禁用全域性帳戶到期設定。使用此設定，即使全域性策略指示帳戶應該處於以下狀態，該帳戶也未被禁用：

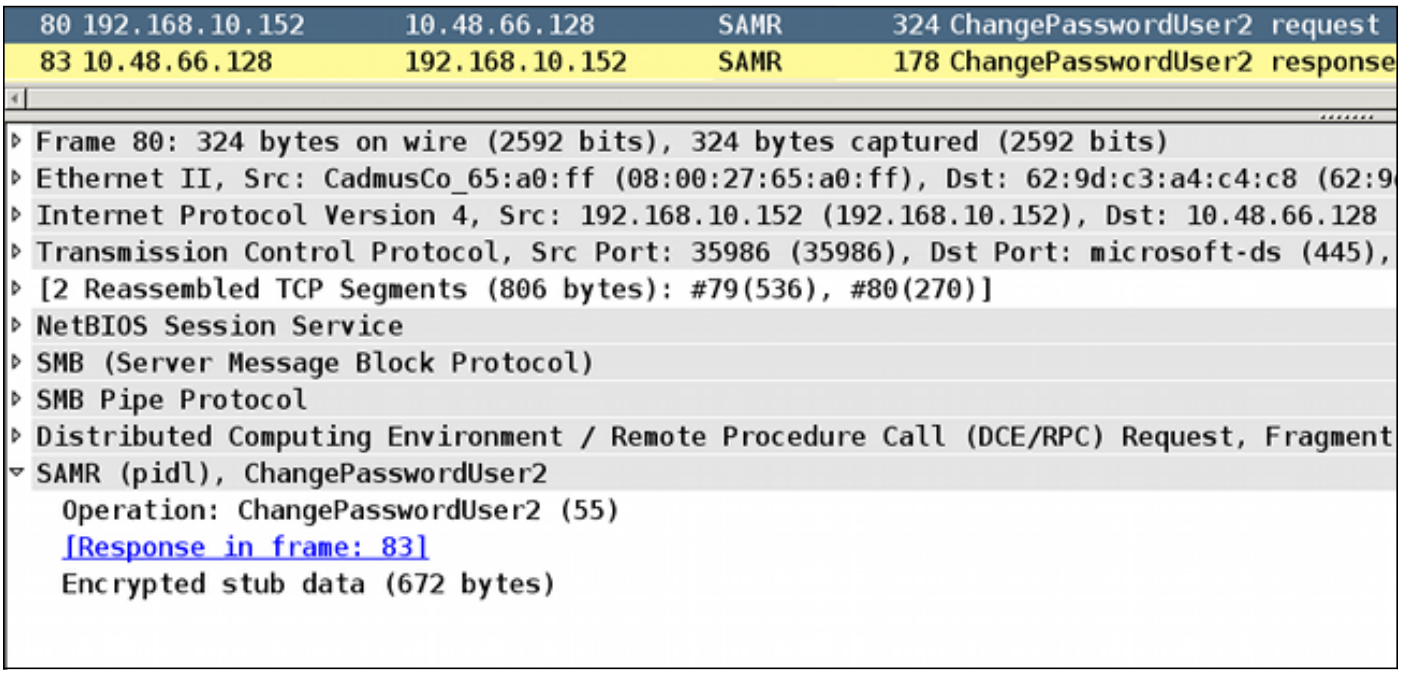


ACS和Active Directory使用者

可以將ACS配置為檢查AD資料庫中的使用者。使用Microsoft Challenge Handshake身份驗證協定第2版(MSCHAPv2)時支援密碼到期和更改；請參閱思科安全存取控制系統5.4使用手冊：ACS 5.4中的身份驗證：身份驗證協定和身份庫相容性以瞭解詳細資訊。

在ASA上，您可以使用密碼管理功能（如下一節所述），以強制ASA使用MSCHAPv2。

ACS在與域控制器(DC)目錄聯絡時使用通用網際網路檔案系統(CIFS)分散式計算環境/遠端過程呼叫(DCE/RPC)呼叫以更改密碼：



ASA可以使用RADIUS和TACACS+協定與ACS聯絡以更改AD密碼。

通過RADIUS使用ACS的ASA

RADIUS通訊協定本身不支援密碼到期或密碼變更。通常，密碼驗證通訊協定(PAP)用於RADIUS。ASA以明文傳送使用者名稱和密碼，然後使用RADIUS共用金鑰加密密碼。

在使用者密碼已到期的典型情況下，ACS會向ASA返回Radius-Reject消息。ACS注意到：

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

對於ASA，這是簡單的Radius-Reject消息，身份驗證失敗。

要解決此問題，ASA允許在隧道組配置下使用**password-management**命令：

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

password-management命令更改行為，從而強制在Radius-Request中使用MSCHAPv2，而不是PAP。

MSCHAPv2協定支援密碼到期和密碼更改。因此，如果VPN使用者在Xauth階段到達特定隧道組，則來自ASA的Radius-Request現在包括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)
```

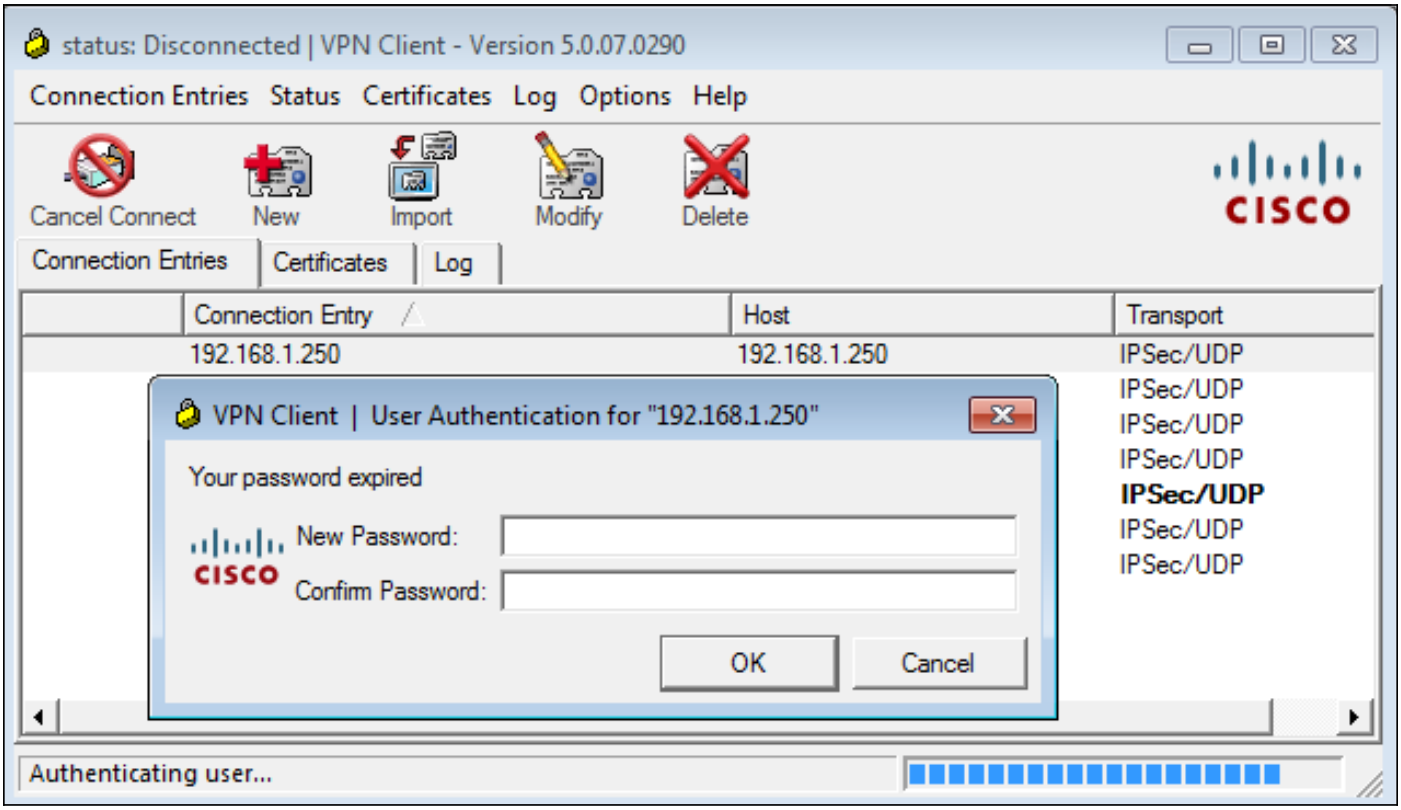
如果ACS注意到使用者需要更改密碼，則會返回一則Radius-Reject消息，其中包含MSCHAPv2錯誤648。

```
▽ 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
```

ASA瞭解該消息並使用MODE_CFG從Cisco VPN客戶端請求新密碼：

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

Cisco VPN客戶端將顯示提示輸入新密碼的對話方塊：



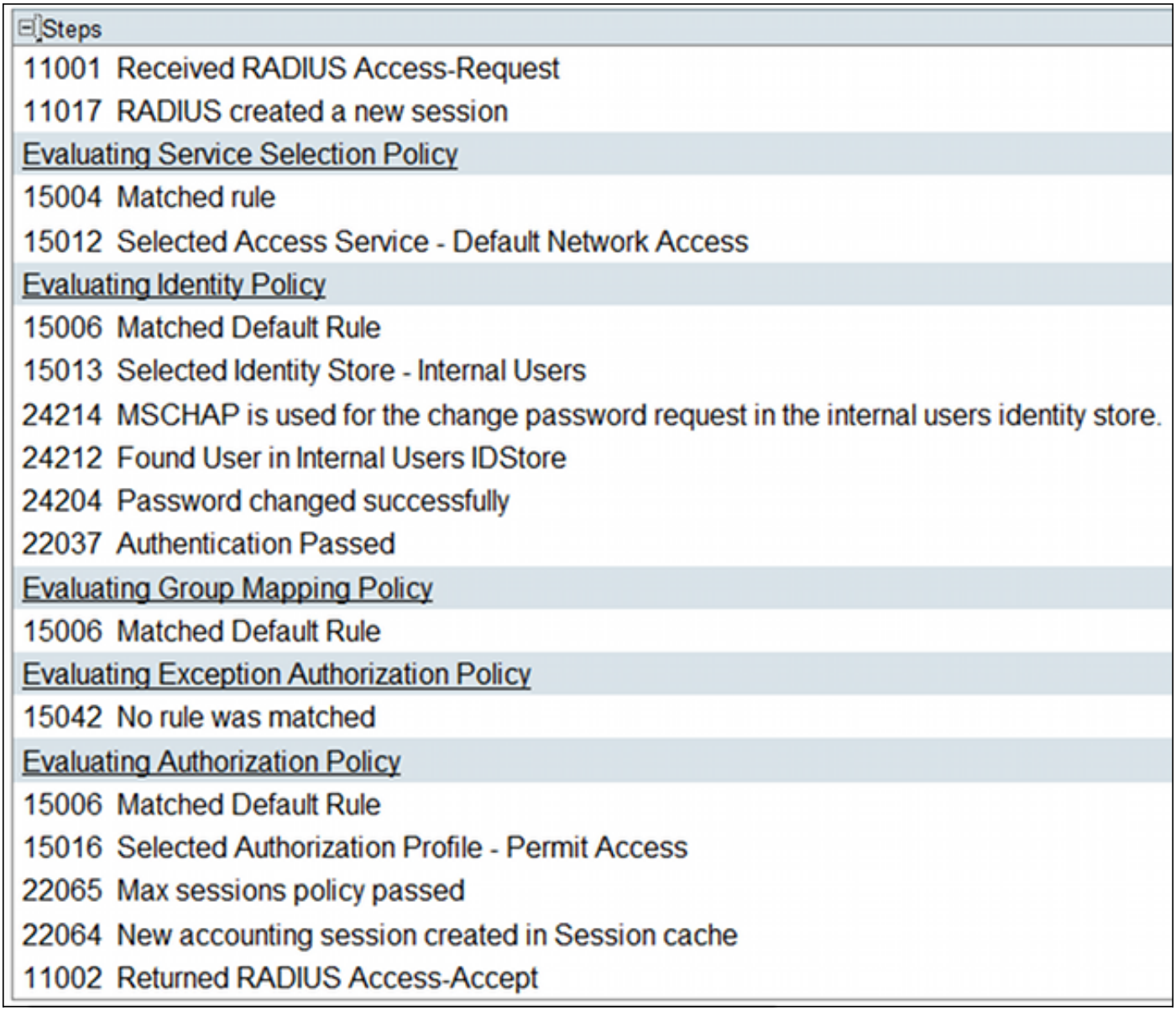
ASA傳送另一個具有MS-CHAP-CPW和MS-CHAP-NT-Enc-PW負載（新密碼）的Radius-Request：

```
▷ 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): 06000001a3a32fa1cad97b38
▽ 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)
```

ACS確認該請求並返回Radius-Accept with MS-CHAP2-Success:

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

這可以在ACS上驗證，ACS報告「24204 Password changed successfully」：



然後，ASA報告身份驗證成功，並繼續執行快速模式(QM)流程：

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

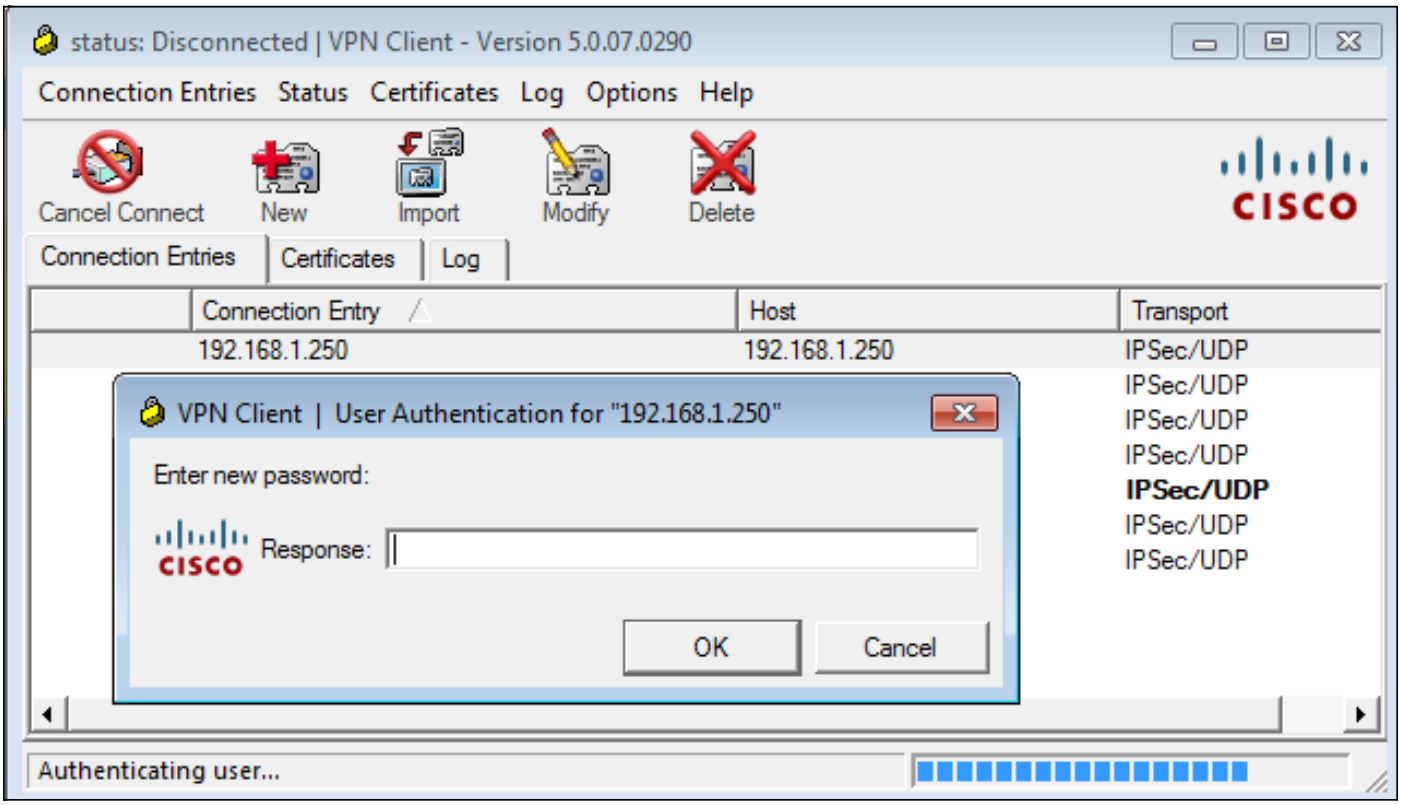
通過TACACS+使用ACS的ASA

同樣，TACACS+也可用於密碼到期和更改。不需要密碼管理功能，因為ASA仍使用身份驗證型別為ASCII而不是MSCHAPv2的TACACS+。

交換多個資料包，ACS要求輸入新密碼：

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

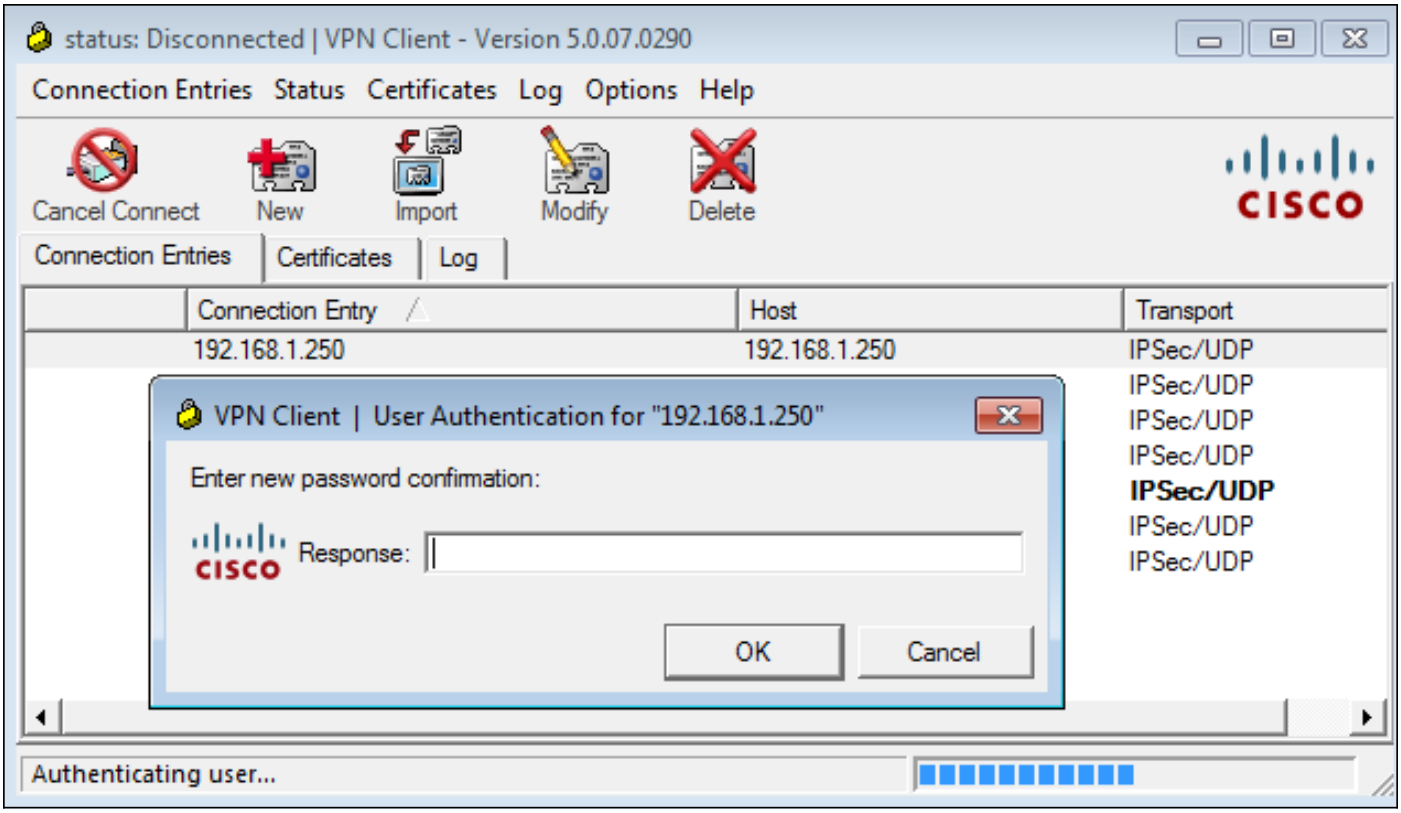
Cisco VPN客戶端顯示提示輸入新密碼的對話方塊（不同於RADIUS使用的對話方塊）：



ACS請求確認新密碼：

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

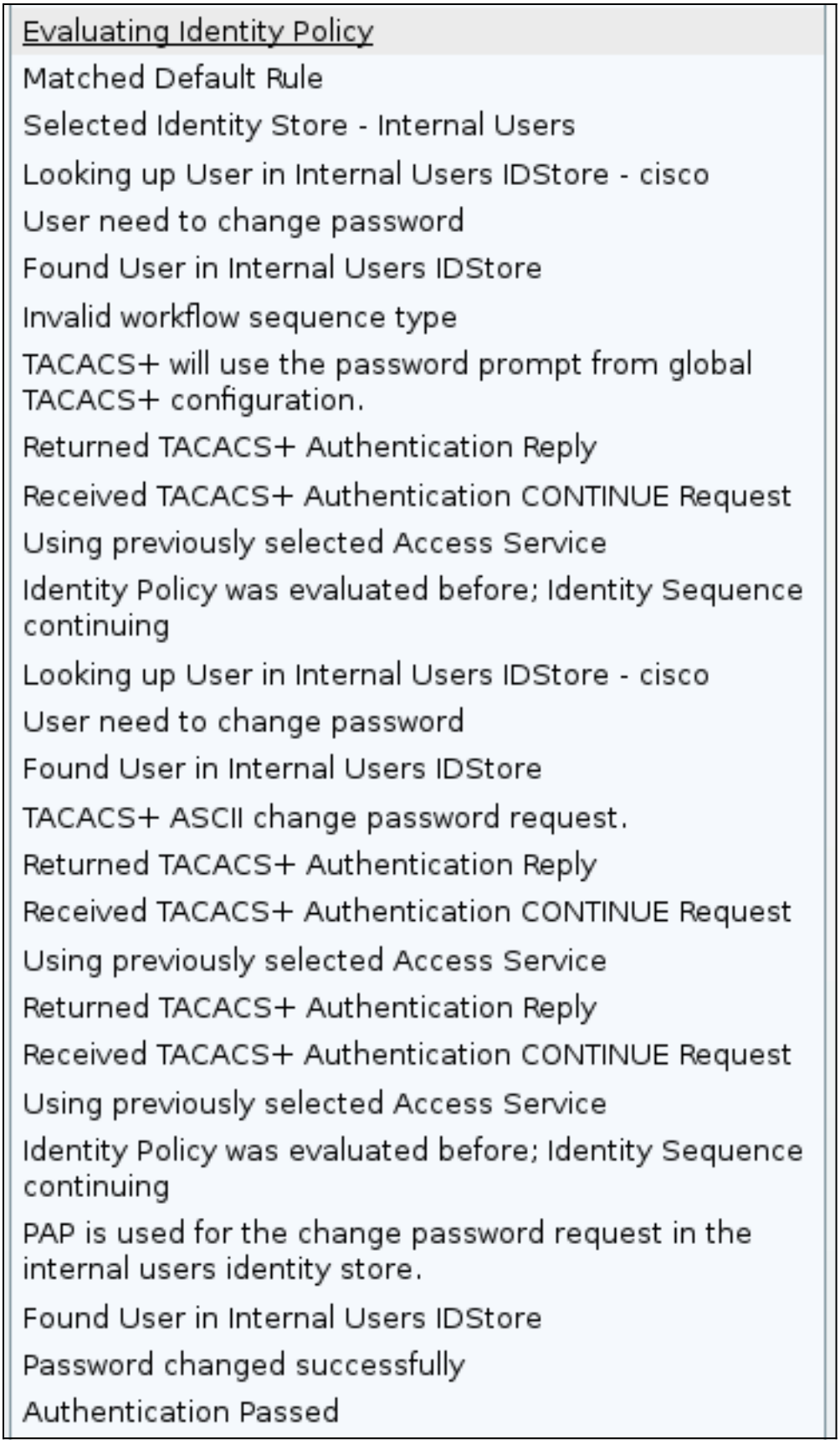
Cisco VPN客戶端顯示一個確認框：



如果確認正確，ACS報告身份驗證成功：

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

然後，ACS記錄已成功更改密碼的事件：



ASA調試顯示交換和成功身份驗證的整個過程：

```
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.
```

該密碼更改對ASA完全透明。具有更多請求和應答資料包的TACACS+會話稍長一點，這些請求和應答資料包由VPN客戶端解析並呈現給更改密碼的使用者。

具備LDAP的ASA

Microsoft AD和Sun LDAP伺服器架構完全支援密碼到期和更改。

對於密碼更改，伺服器返回「bindresponse = invalidCredentials」，並顯示「error = 773」。 此錯誤表示使用者必須重設密碼。典型的錯誤代碼包括：

錯誤代碼	錯誤
525	未找到使用者
52e	憑據無效
530	此時不允許登入
531	不允許在此工作站登入
532	密碼已過期
533	帳戶已禁用
701	帳戶已過期
773	使用者必須重置密碼
775	使用者帳戶已鎖定

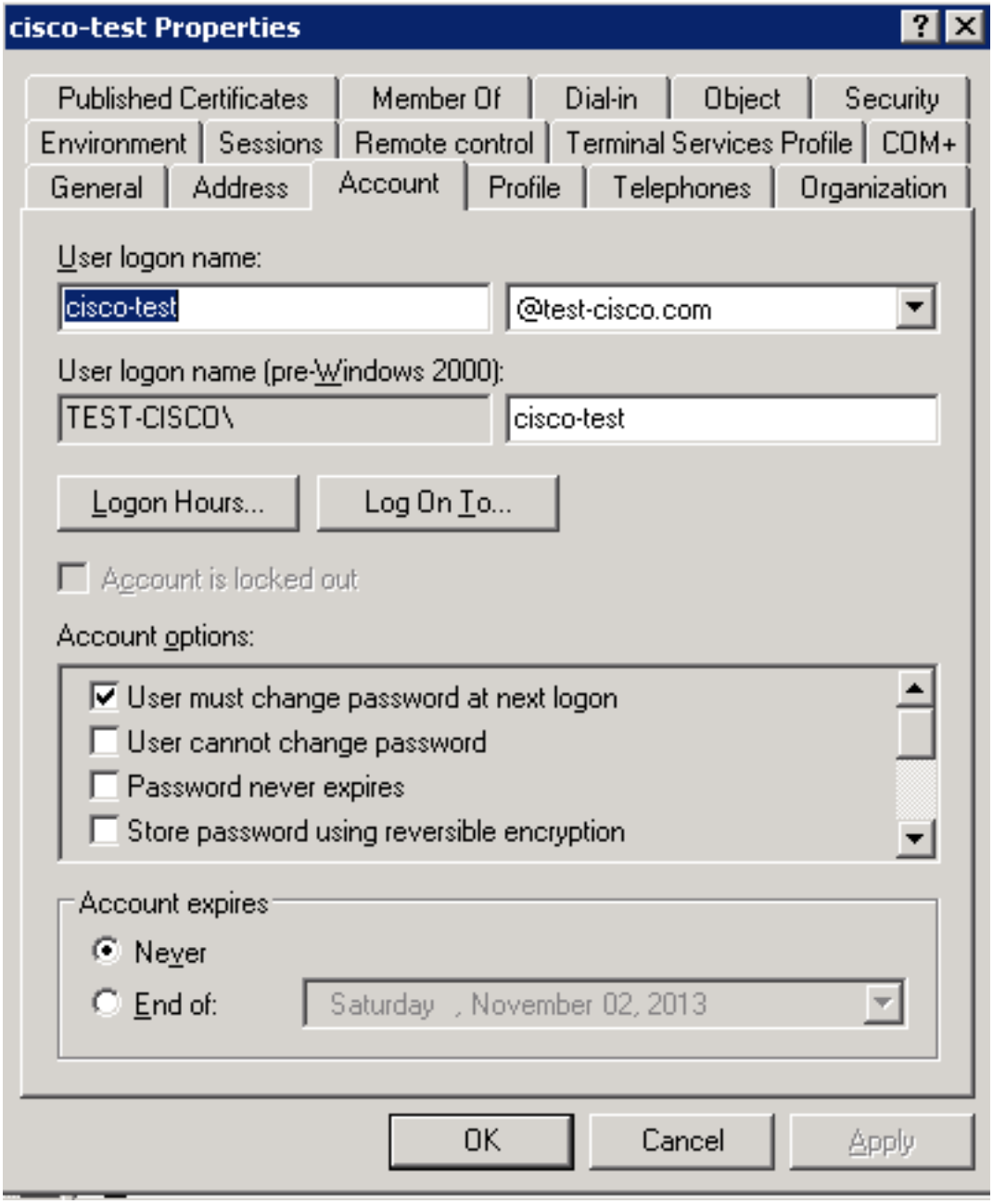
配置LDAP伺服器：

```
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
```

將該配置用於隧道組和密碼管理功能：

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

配置AD使用者，以便需要更改密碼：



當使用者嘗試使用Cisco VPN客戶端時，ASA報告無效密碼：

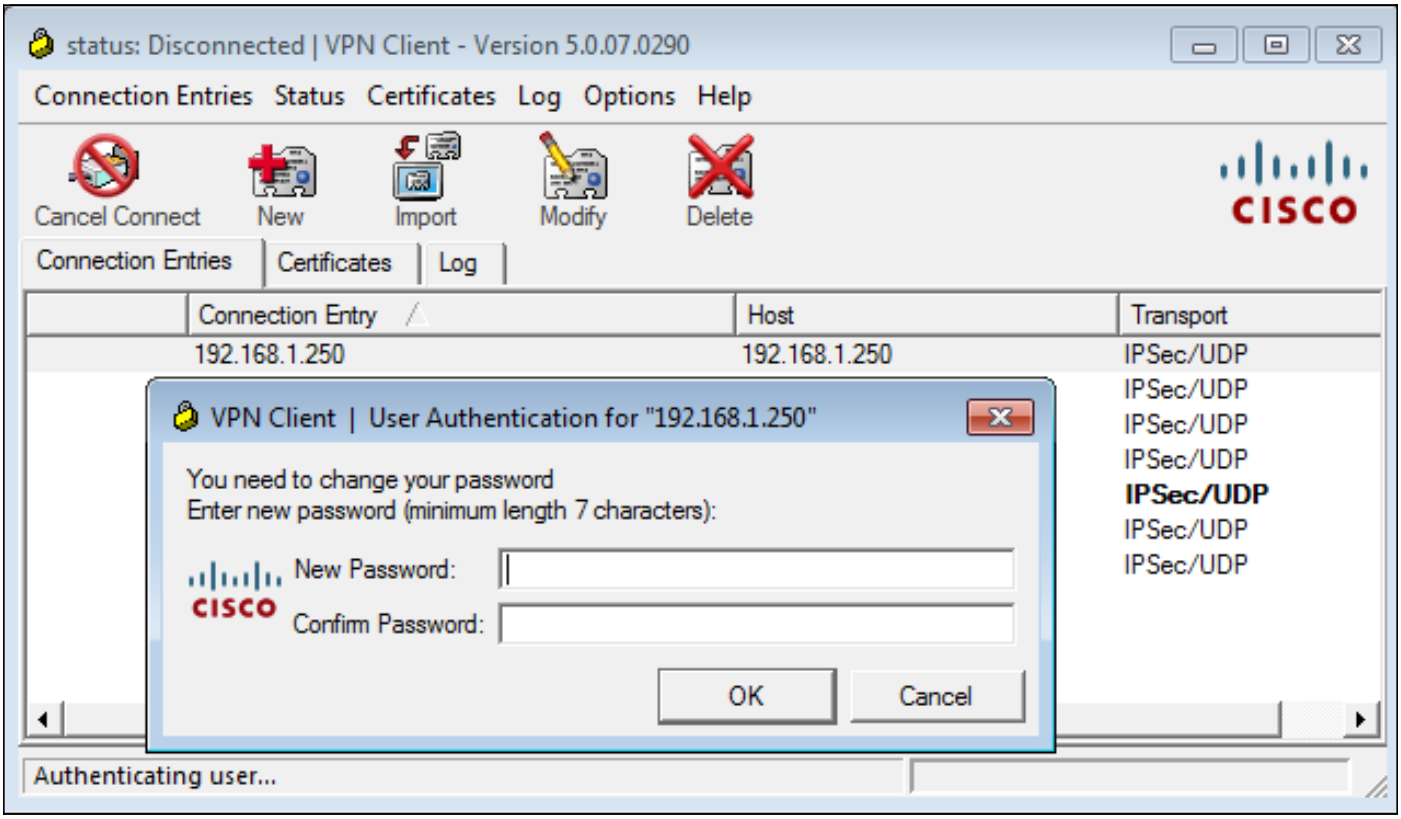
```
ASA(config-tunnel-general)# debug ldap 255
<some output ommited for clarity>

[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
```

如果憑證無效，將出現52e錯誤：

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

然後，Cisco VPN客戶端要求更改密碼：



此對話方塊與TACACS或RADIUS使用的對話方塊不同，因為它顯示策略。在本示例中，策略的最小密碼長度為七個字元。

使用者更改密碼後，ASA可能會從LDAP伺服器收到此失敗消息：

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

Microsoft策略需要使用安全套接字層(SSL)來修改密碼。變更設定：

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

適用於SSL的Microsoft LDAP

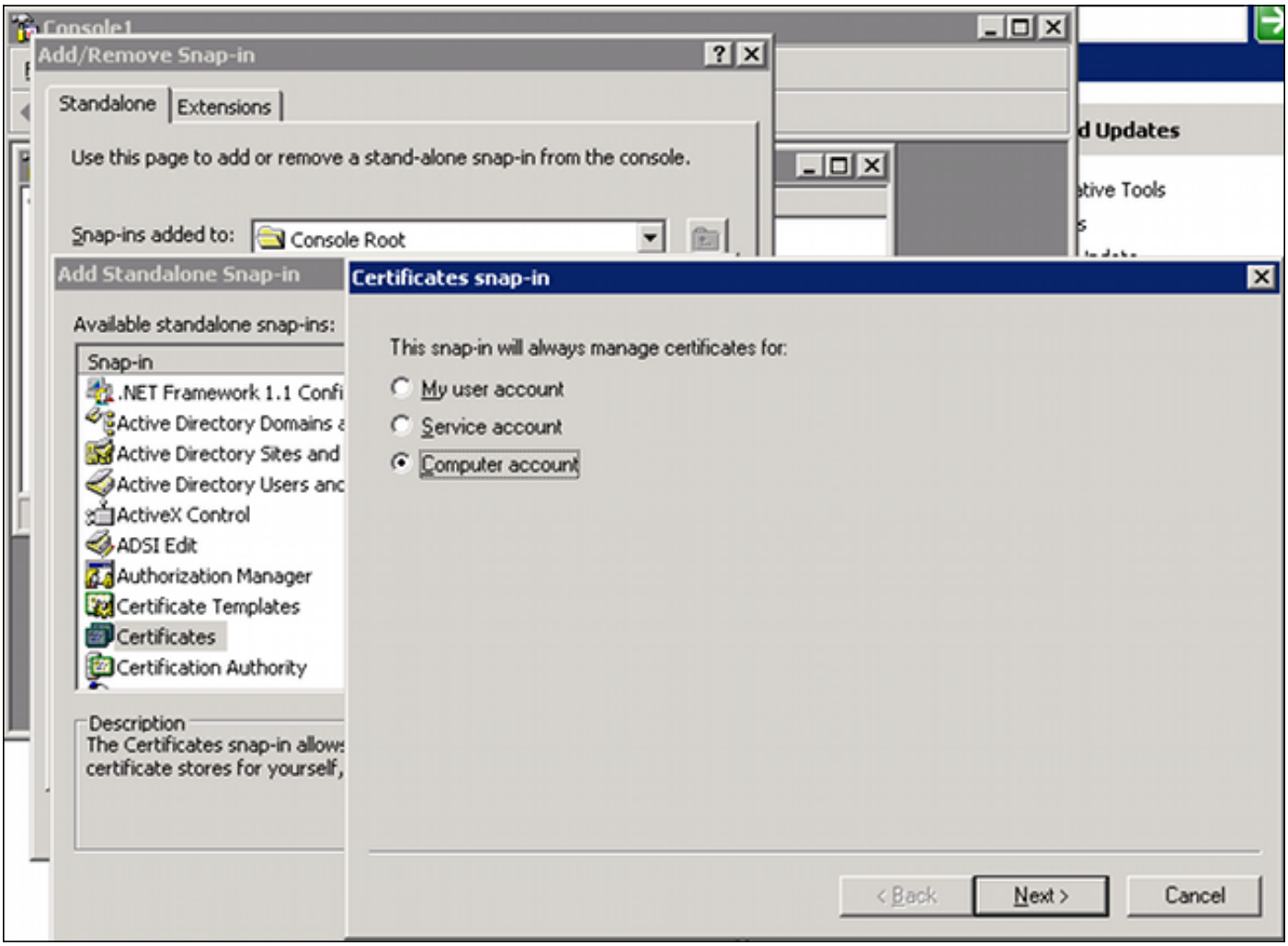
預設情況下，Microsoft LDAP over SSL不起作用。若要啟用此功能，您必須使用正確的金鑰擴展為

電腦帳戶安裝證書。有關更多詳細資訊，請參閱如何通過第三方證書頒發機構啟用SSL。

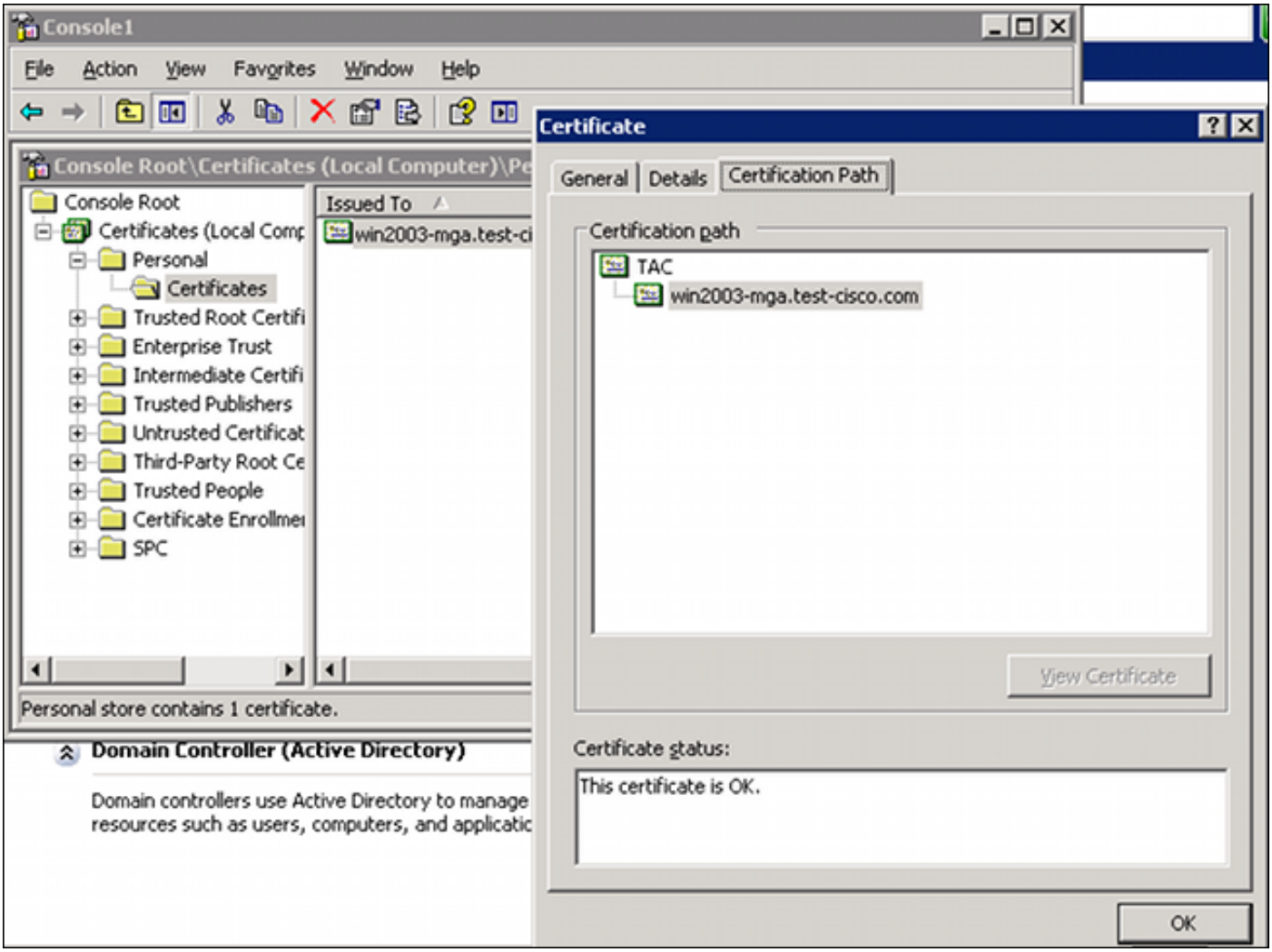
證書甚至可以是自簽名證書，因為ASA不驗證LDAP證書。如需相關增強要求，請參閱Cisco錯誤ID CSCui40212，「Allow ASA to validate certificate from LDAPS server」。

附註：ACS驗證5.5及更新版本中的LDAP證書。

要安裝證書，請開啟mmc控制檯，選擇**Add/Remove Snap-in**，新增證書，然後選擇**Computer account**:



選擇**本地電腦**，將證書匯入到個人儲存，然後將關聯的證書頒發機構(CA)證書移動到受信任的儲存中。驗證憑證是否受信任：



ASA 8.4.2版中存在錯誤，當您嘗試通過SSL使用LDAP時，可能會返回此錯誤：

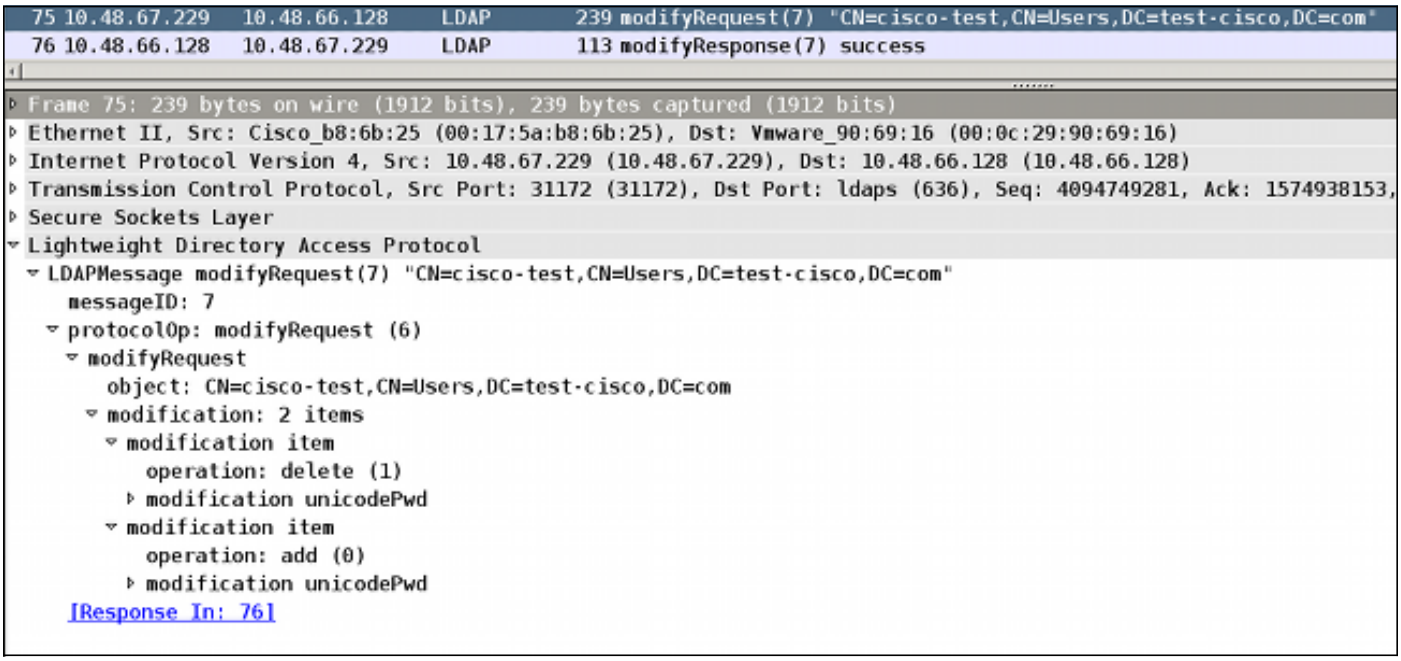
```
ASA(config)# debug ldap 255

[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 9.1.3版在相同配置下工作正常。有兩個LDAP會話。第一個會話返回失敗，代碼為773（密碼已過期），而第二個會話用於密碼更改：

```
[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 ommitted for clarity>
accountExpires: value = 130256568000000000 <----- 100ns intervals since
January 1, 1601 (UTC)
```

要驗證密碼更改，請檢視資料包。Wireshark可以使用LDAP伺服器的私鑰對SSL流量進行解密：



ASA上的網際網路金鑰交換(IKE)/驗證、授權和計量(AAA)偵錯與RADIUS驗證場景中顯示的非常相似。

LDAP和到期前警告

對於LDAP，您可以使用在密碼到期之前傳送警告的功能。ASA在密碼到期前90天使用以下設定警告使用者：

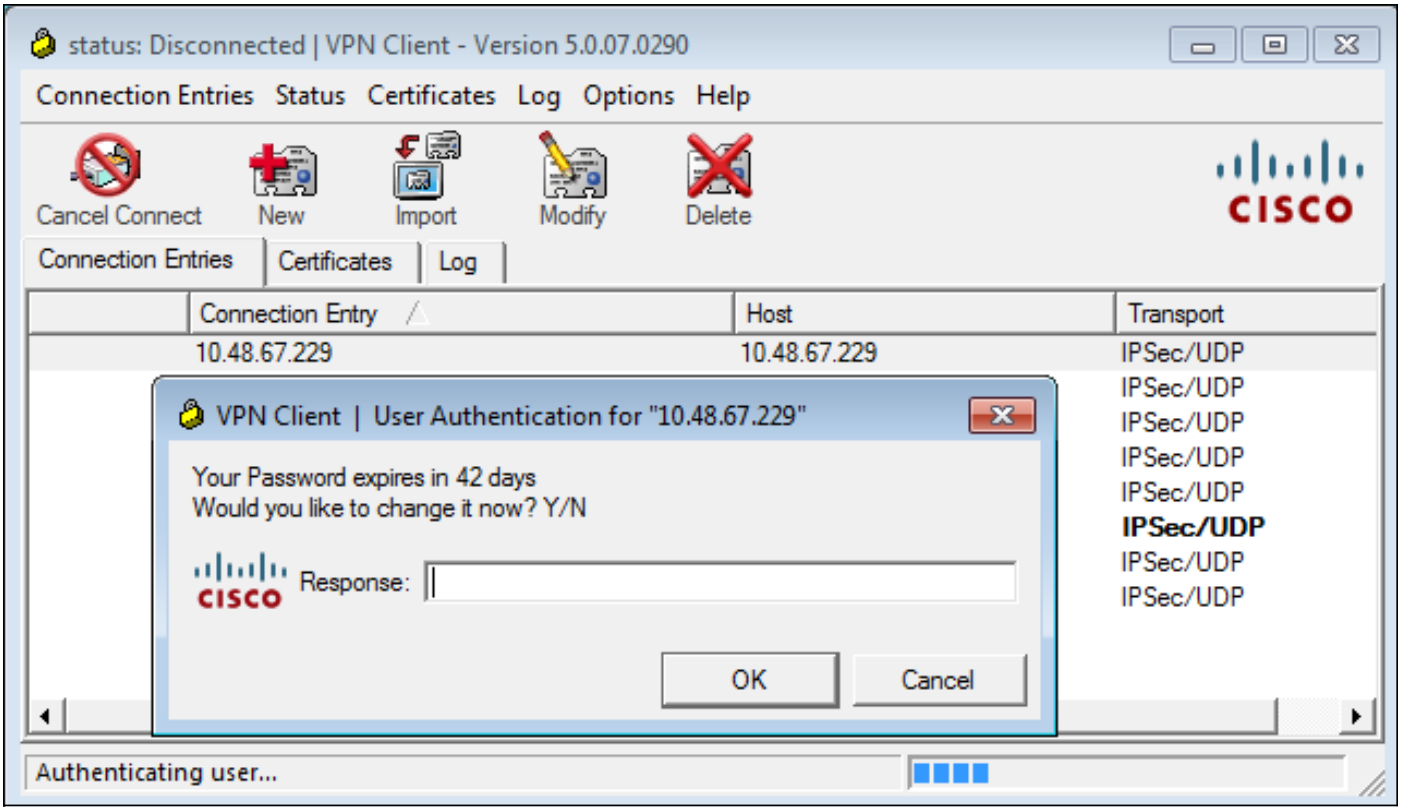
```
tunnel-group RA general-attributes
 password-management password-expire-in-days 90
```

密碼將在42天後過期，使用者嘗試登入：

```
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
```

ASA傳送警告並提供密碼更改選項：



如果使用者選擇更改密碼，系統會提示輸入新密碼，然後開始正常的密碼更改過程。

ASA和L2TP

前面的示例介紹了IKE第1版(IKEv1)和IPSec VPN。

對於第2層通道通訊協定(L2TP)和IPSec，PPP用作身份驗證的傳輸。需要使用MSCHAPv2而不是PAP才能使密碼更改生效：

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

對於PPP會話內L2TP中的擴展身份驗證，將協商MSCHAPv2:

```
▷ 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
```

使用者密碼到期後，返回代碼為648的故障：

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

然後需要更改密碼。剩餘程式非常類似使用MSCHAPv2的RADIUS案例。

有關如何配置L2TP的其他詳細資訊，請參閱Windows 2000/XP PC和PIX/ASA 7.2之間使用預共用金鑰的L2TP Over IPsec配置示例。

ASA SSL VPN客戶端

以上示例涉及IKEv1和生命週期終止(EOL)的Cisco VPN客戶端。

遠端訪問VPN的推薦解決方案是Cisco AnyConnect安全移動，它使用IKE第2版(IKEv2)和SSL協定。Cisco AnyConnect的密碼更改和到期功能與對Cisco VPN客戶端的功能完全相同。

對於IKEv1，在1.5階段(Xauth/mode config)中，ASA與VPN客戶端之間交換了密碼更改和到期資料。

IKEv2類似；配置模式使用CFG_REQUEST/CFG_REPLY資料包。

對於SSL，資料位於控制資料包傳輸層安全(DTLS)會話中。

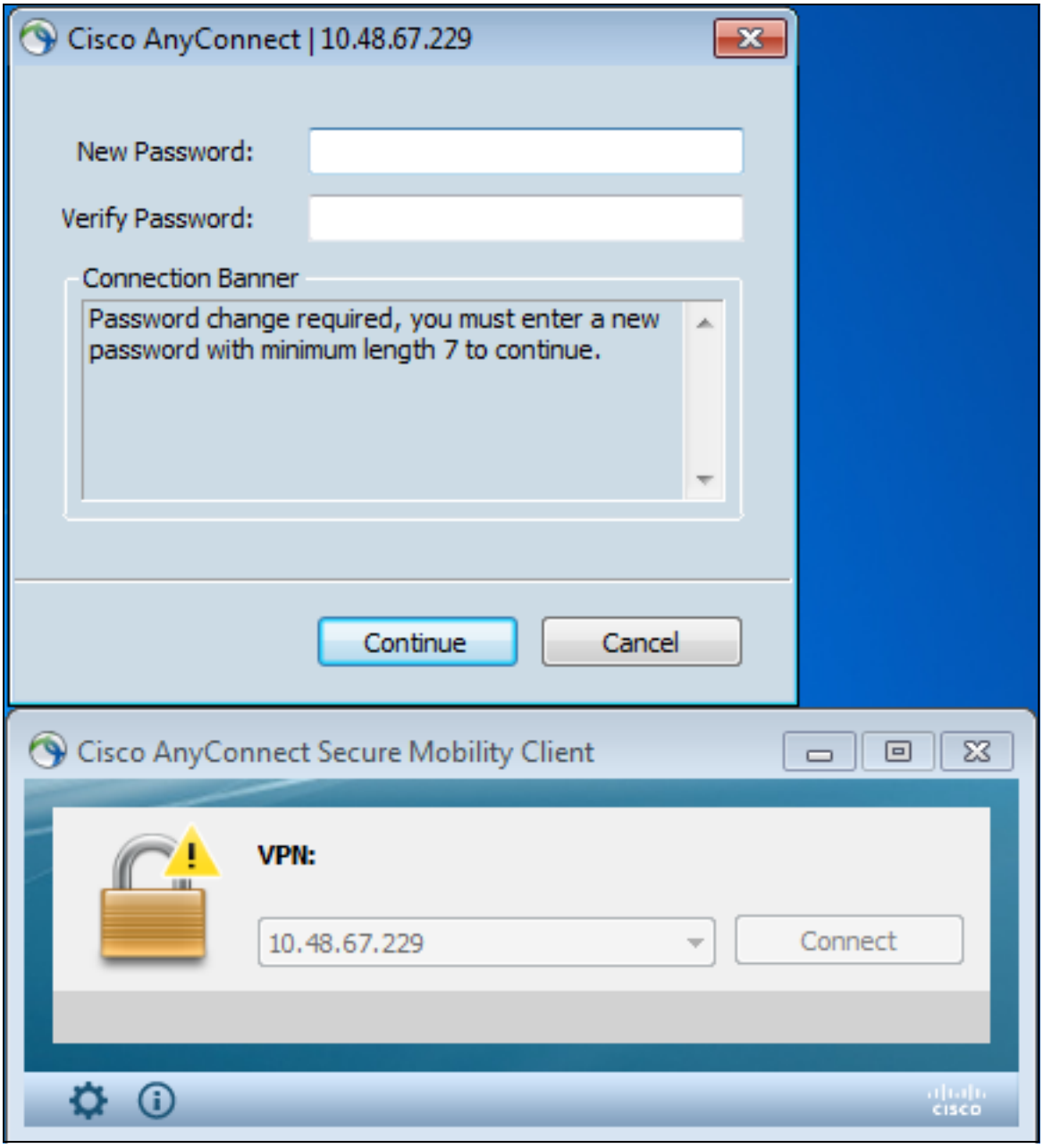
ASA的配置相同。

以下是使用Cisco AnyConnect的示例配置，以及使用SSL上的LDAP伺服器的SSL協定：

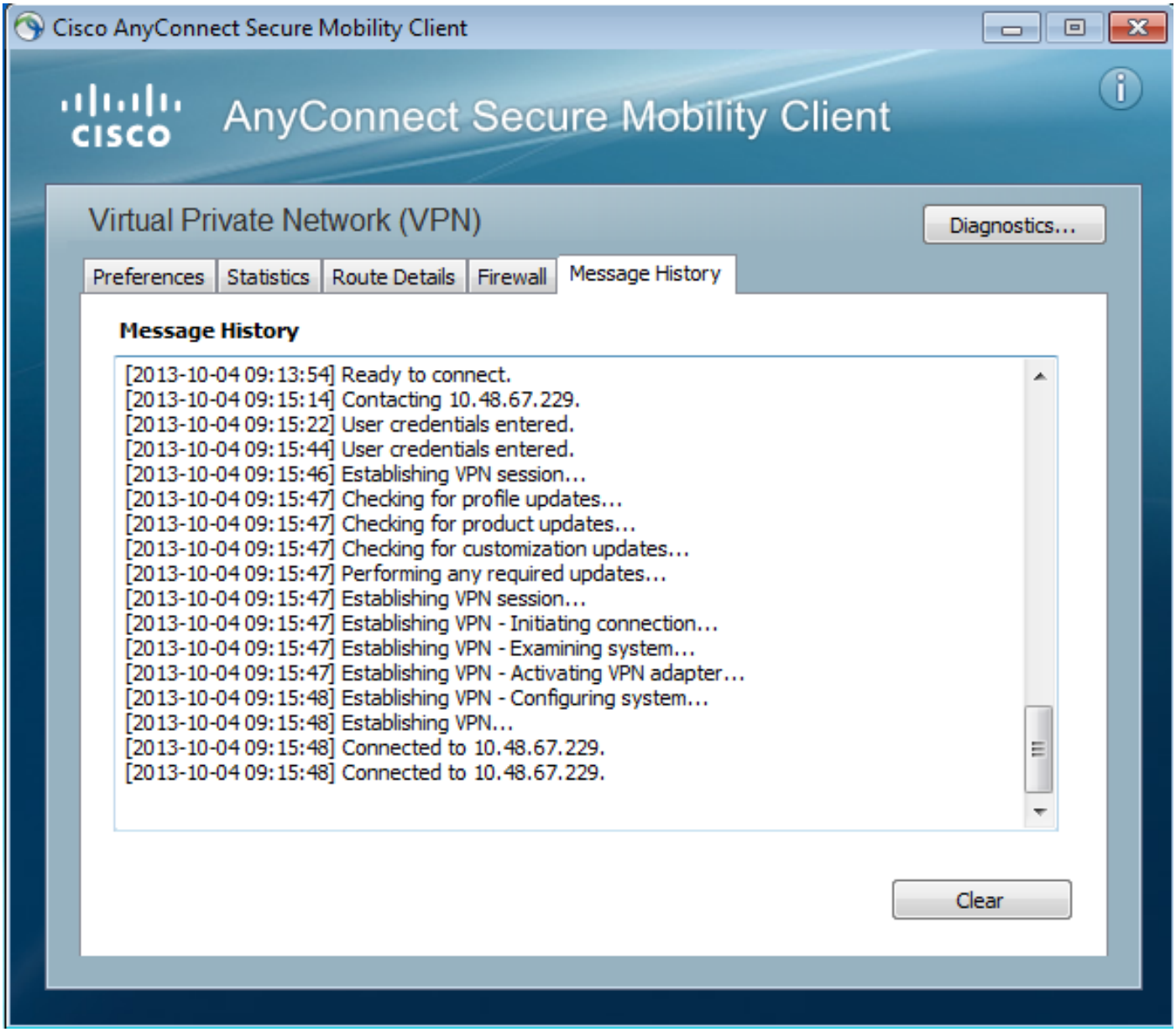
```
aaa-server LDAP protocol ldap
aaa-server LDAP (outside) host win2003-mga.test-cisco.com
 ldap-base-dn CN=Users,DC=test-cisco,DC=com
 ldap-scope subtree
```

```
 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
```

提供正確的密碼（已過期）後，Cisco AnyConnect會嘗試連線並請求輸入新密碼：



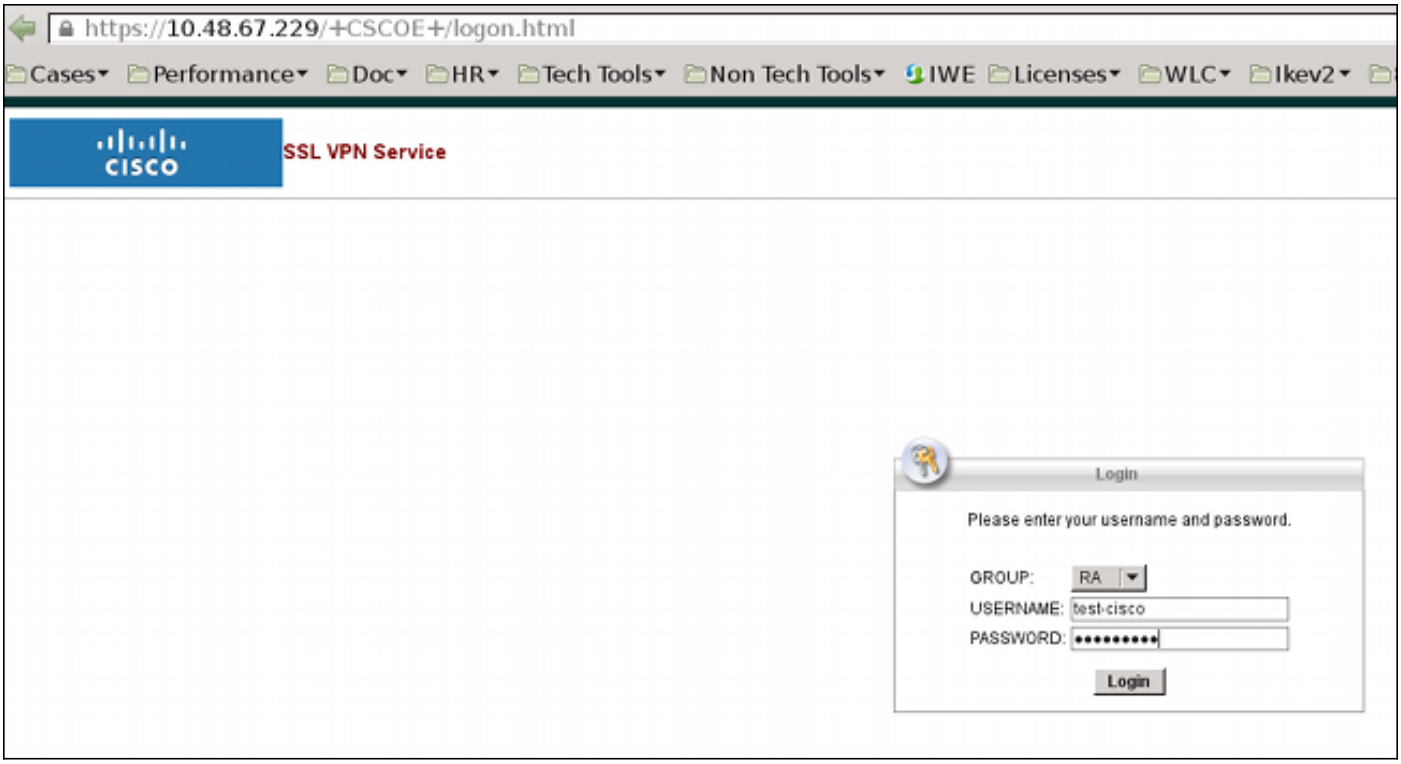
日誌表明使用者憑證輸入了兩次：



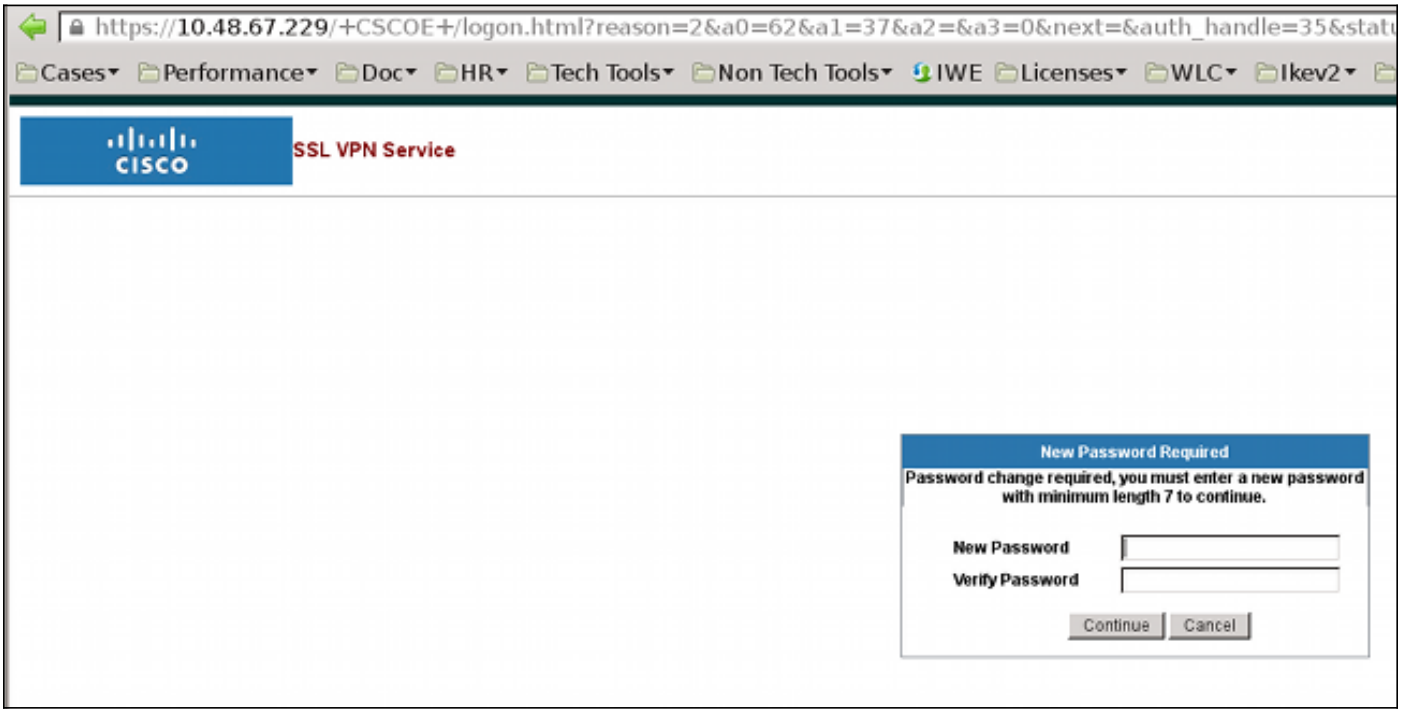
更詳細的日誌可在診斷AnyConnect報告工具(DART)中獲得。

ASA SSL Web門戶

在Web入口中會出現相同的登入過程：



密碼到期和更改過程相同：



ACS使用者更改密碼

如果無法通過VPN更改密碼，您可以使用ACS使用者更改密碼(UCP)專用Web服務。請參閱思科安全訪問控制系統5.4軟體開發人員指南：使用UCP Web服務。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 使用CLI 8.4和8.6的Cisco ASA 5500系列配置指南：配置外部伺服器以進行安全裝置使用者授權
- 技術支援與文件 - Cisco Systems