ASA Remote Access VPN IKE/SSL - RADIUS, TACACS 및 LDAP 컨피그레이션에 대한 비밀번호 만료 및 변경 예

목차

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance)에서 종료된 원격 액세스 VPN 터널의 비밀번호 만료 및 비밀번호 변경 기능에 대해 설명합니다. 이 문서에는 다음이 포함됩니다.

- 다른 클라이언트:Cisco VPN 클라이언트 및 Cisco AnyConnect Secure Mobility
- 다른 프로토콜:TACACS, RADIUS 및 LDAP(Lightweight Directory Access Protocol)
- Cisco ACS(Secure Access Control System)의 다른 저장소:로컬 및 AD(Active Directory)

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CLI(Command Line Interface)를 통한 ASA 컨피그레이션 지식
- ASA에서 VPN 컨피그레이션에 대한 기본적인 지식
- Cisco Secure ACS에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Adaptive Security Appliance, 버전 8.4 이상
- Microsoft Windows Server 2003 SP1
- Cisco Secure Access Control System, 버전 5.4 이상
- Cisco AnyConnect Secure Mobility, 버전 3.1
- Cisco VPN Client, 릴리스 5

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

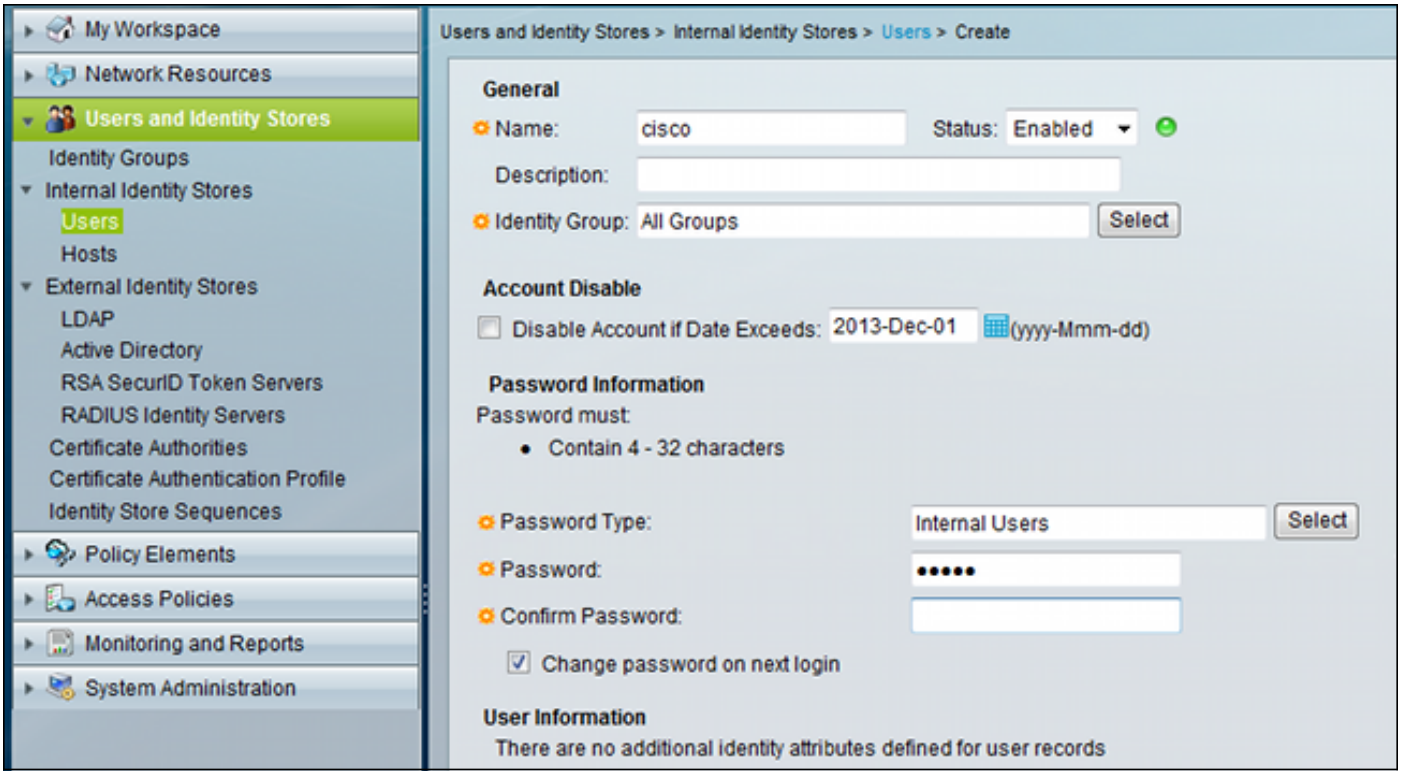
> **참고:**
>
> 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.
>
> **debug** 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

로컬 인증과 함께 ASA

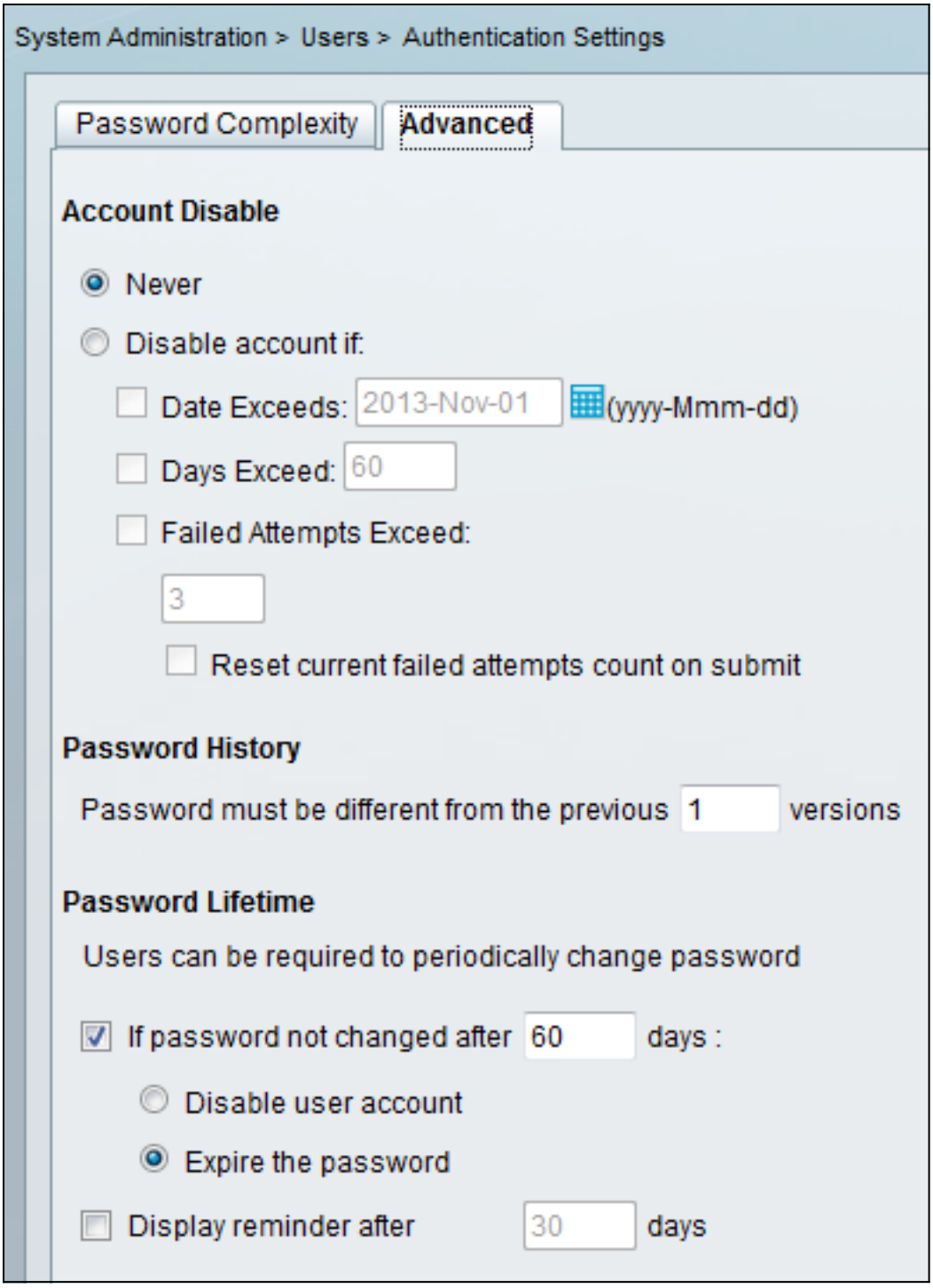
로컬로 정의된 사용자가 있는 ASA에서는 비밀번호 만료 또는 비밀번호 변경 기능을 사용할 수 없습니다.RADIUS, TACACS, LDAP 또는 Windows NT와 같은 외부 서버가 필요합니다.

ACS 및 로컬 사용자

ACS는 로컬로 정의된 사용자에 대해 비밀번호 만료 및 비밀번호 변경을 모두 지원합니다.예를 들어 새로 만든 사용자가 다음 로그인 시 비밀번호를 변경하도록 강제할 수 있으며, 특정 날짜에 계정을 비활성화할 수도 있습니다.

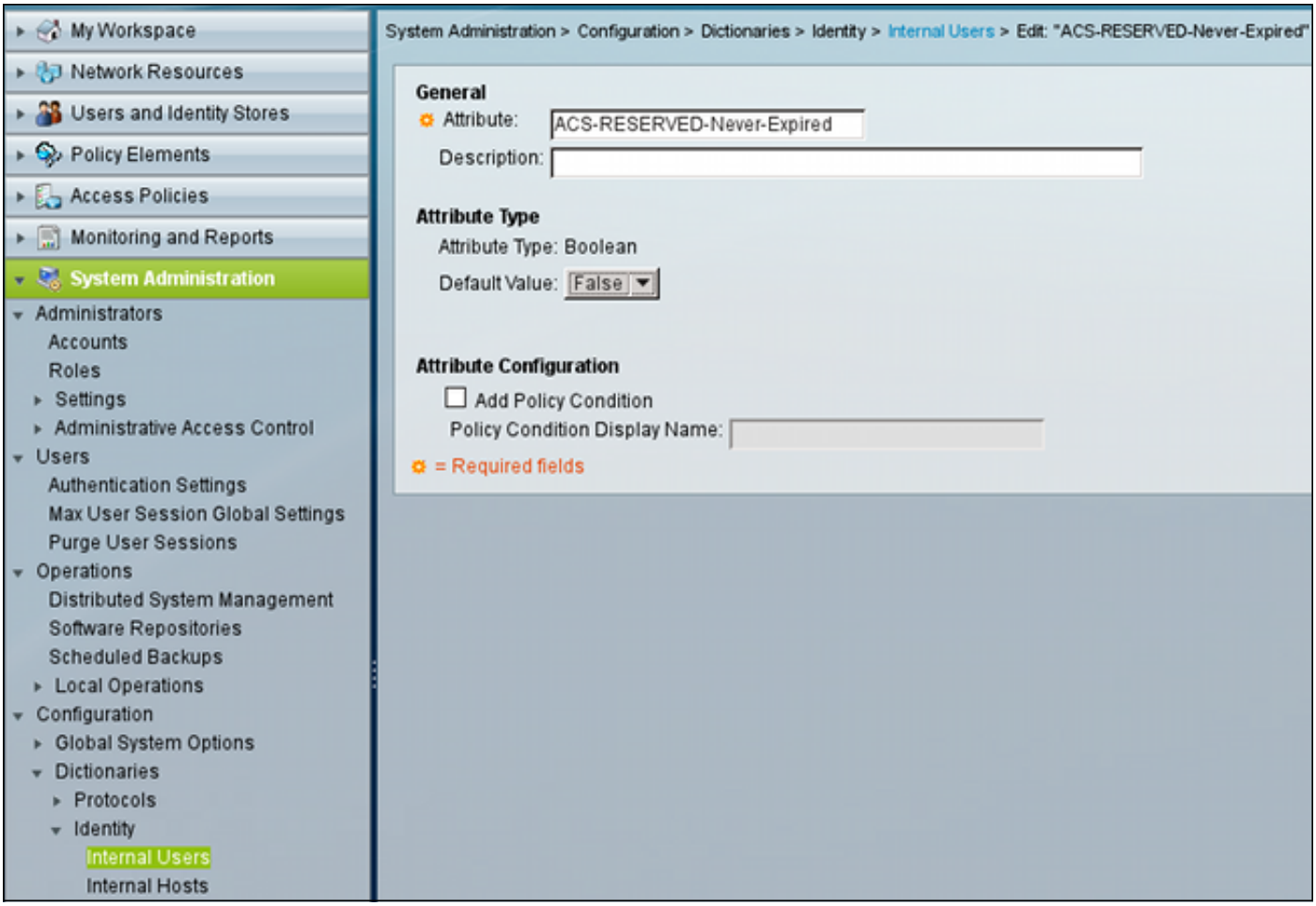


모든 사용자에 대한 비밀번호 정책을 구성할 수 있습니다.예를 들어, 비밀번호가 만료된 후 사용자 계정을 비활성화(로그인 기능 없이 차단)하거나 비밀번호를 변경하는 옵션을 제공할 수 있습니다.

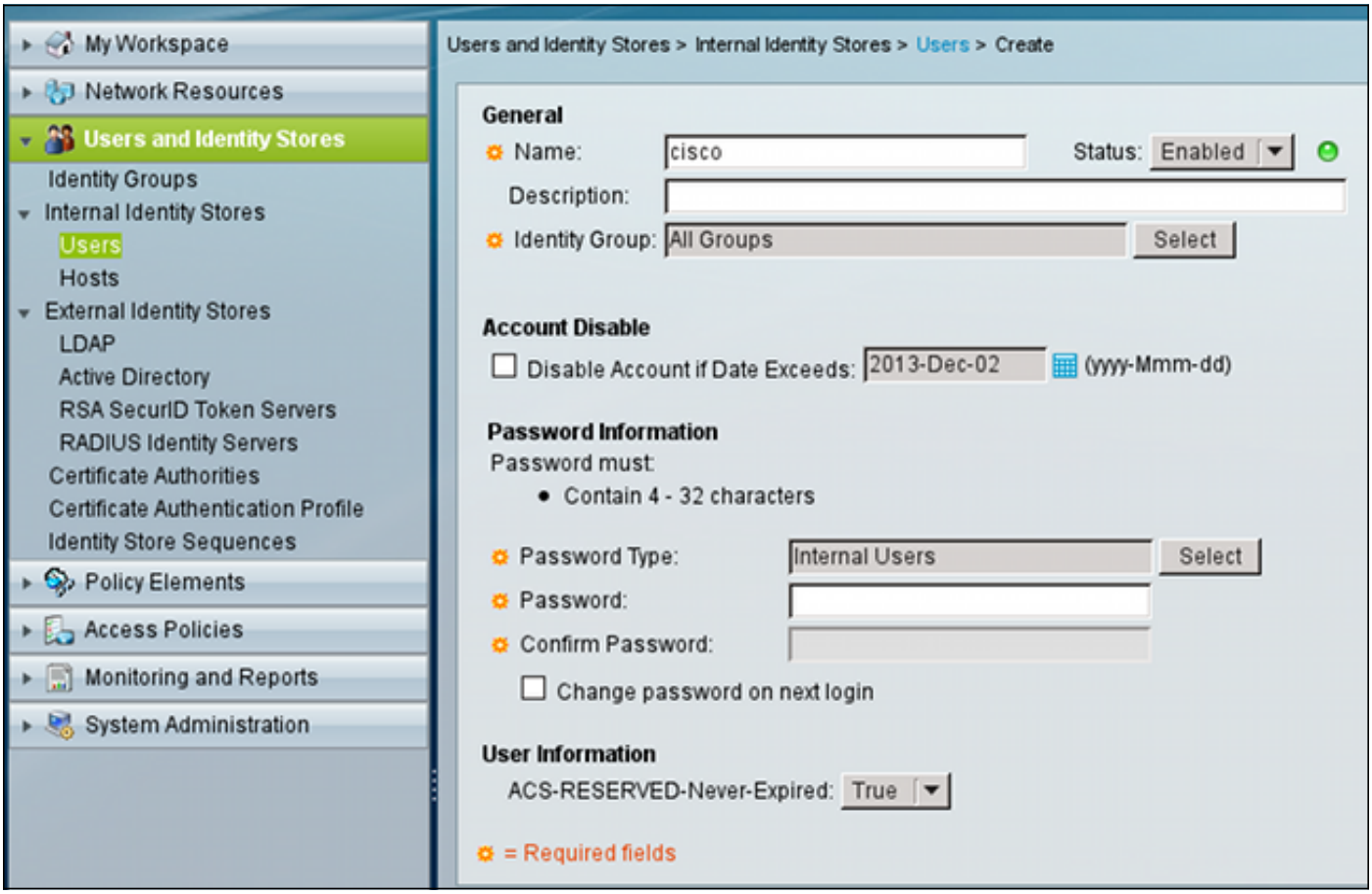


사용자별 설정이 전역 설정에 우선합니다.

ACS-RESERVED-Never-Expired는 사용자 ID의 내부 특성입니다.



이 특성은 사용자에 의해 활성화되며 전역 계정 만료 설정을 비활성화하기 위해 사용할 수 있습니다.이 설정을 사용하면 글로벌 정책에서 다음을 나타나도 계정이 비활성화되지 않습니다.

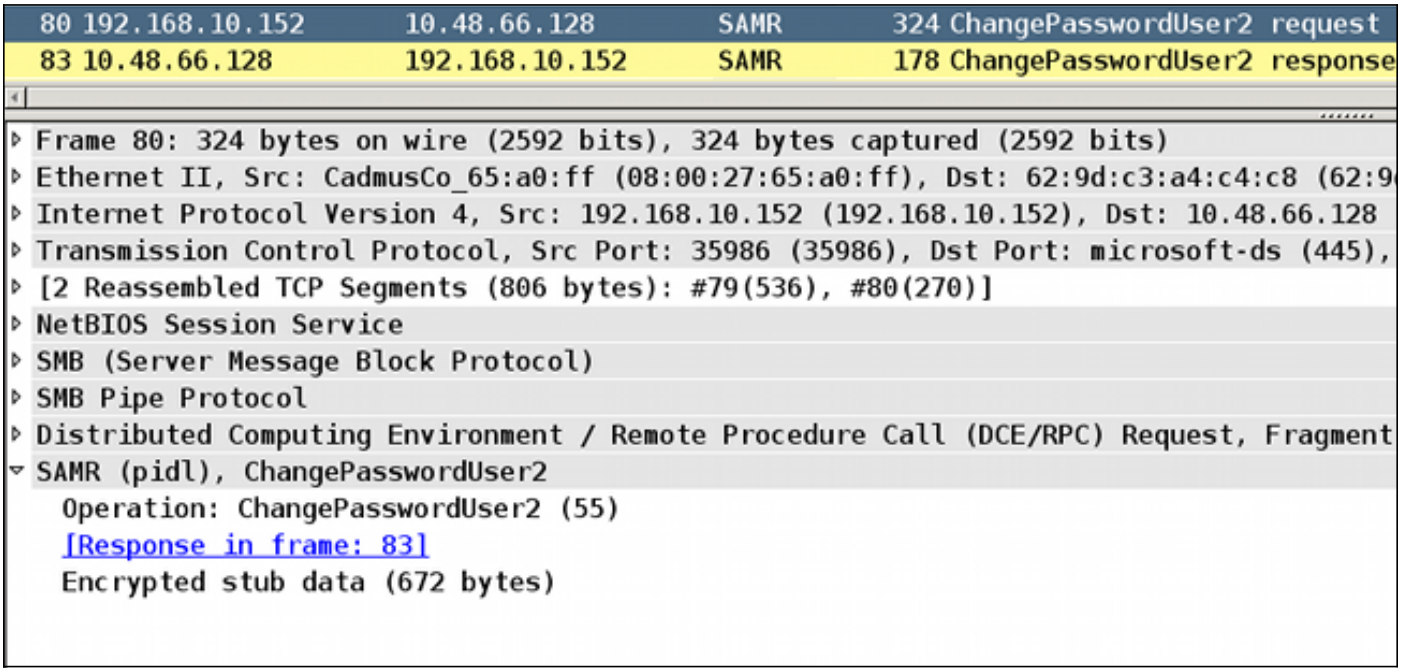


ACS 및 Active Directory 사용자

AD 데이터베이스에서 사용자를 확인하도록 ACS를 구성할 수 있습니다.비밀번호 만료 및 변경은 MSCHAPv2(Microsoft Challenge Handshake Authentication Protocol version 2)를 사용할 때 지원됩니다.Cisco Secure Access Control System 5.4 사용 설명서 참조:ACS 5.4의 인증:자세한 내용은 인증 프로토콜 및 ID 저장소 호환성을 참조하십시오.

ASA에서 다음 섹션에 설명된 대로 비밀번호 관리 기능을 사용하여 ASA가 MSCHAPv2를 사용하도록 강제할 수 있습니다.

ACS는 비밀번호를 변경하기 위해 DC(Domain Controller) 디렉터리에 연결할 때 CIFS(Common Internet File System) DCE/RPC(Distributed Computing Environment/Remote Procedure Call) 호출을 사용합니다.



ASA는 RADIUS 및 TACACS+ 프로토콜을 모두 사용하여 AD 비밀번호 변경을 위해 ACS와 연결할 수 있습니다.

RADIUS를 통해 ACS를 사용하는 ASA

RADIUS 프로토콜은 기본적으로 비밀번호 만료 또는 비밀번호 변경을 지원하지 않습니다.일반적으로 PAP(Password Authentication Protocol)는 RADIUS에 사용됩니다.ASA는 일반 텍스트로 사용자 이름과 비밀번호를 전송하고, 비밀번호는 RADIUS 공유 비밀번호를 사용하여 암호화됩니다.

사용자 비밀번호가 만료된 일반적인 시나리오에서 ACS는 ASA에 Radius-Reject 메시지를 반환합니다.ACS는 다음 사항을 확인합니다.

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

ASA의 경우 단순 Radius-Reject 메시지이며 인증이 실패합니다.

이 문제를 해결하기 위해 ASA에서는 tunnel-group 컨피그레이션에서 password-**management** 명령을 사용할 수 있습니다.

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

password-**management** 명령은 ASA가 Radius-Request에서 PAP가 아닌 MSCHAPv2를 강제로 사용하도록 동작을 변경합니다.

MSCHAPv2 프로토콜은 비밀번호 만료 및 비밀번호 변경을 지원합니다.따라서 VPN 사용자가 Xauth 단계 동안 특정 터널 그룹에 도달하면 ASA의 Radius-Request에 MS-CHAP-Challenge가 포함됩니다.

```
▼ 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)
```

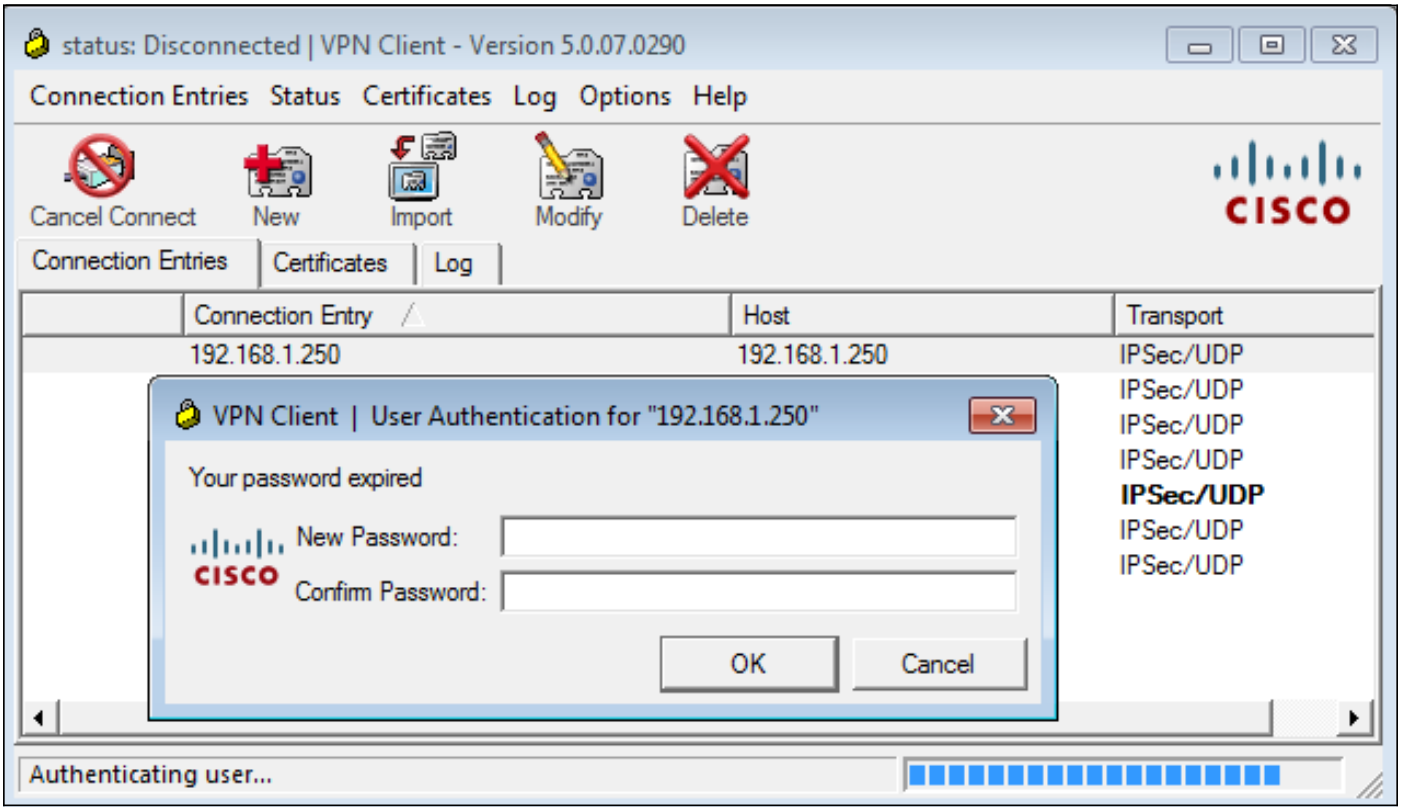
ACS에서 사용자가 비밀번호를 변경해야 한다는 것을 알리면 MSCHAPv2 오류 648과 함께 Radius-Reject 메시지를 반환합니다.

```
▽ 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
```

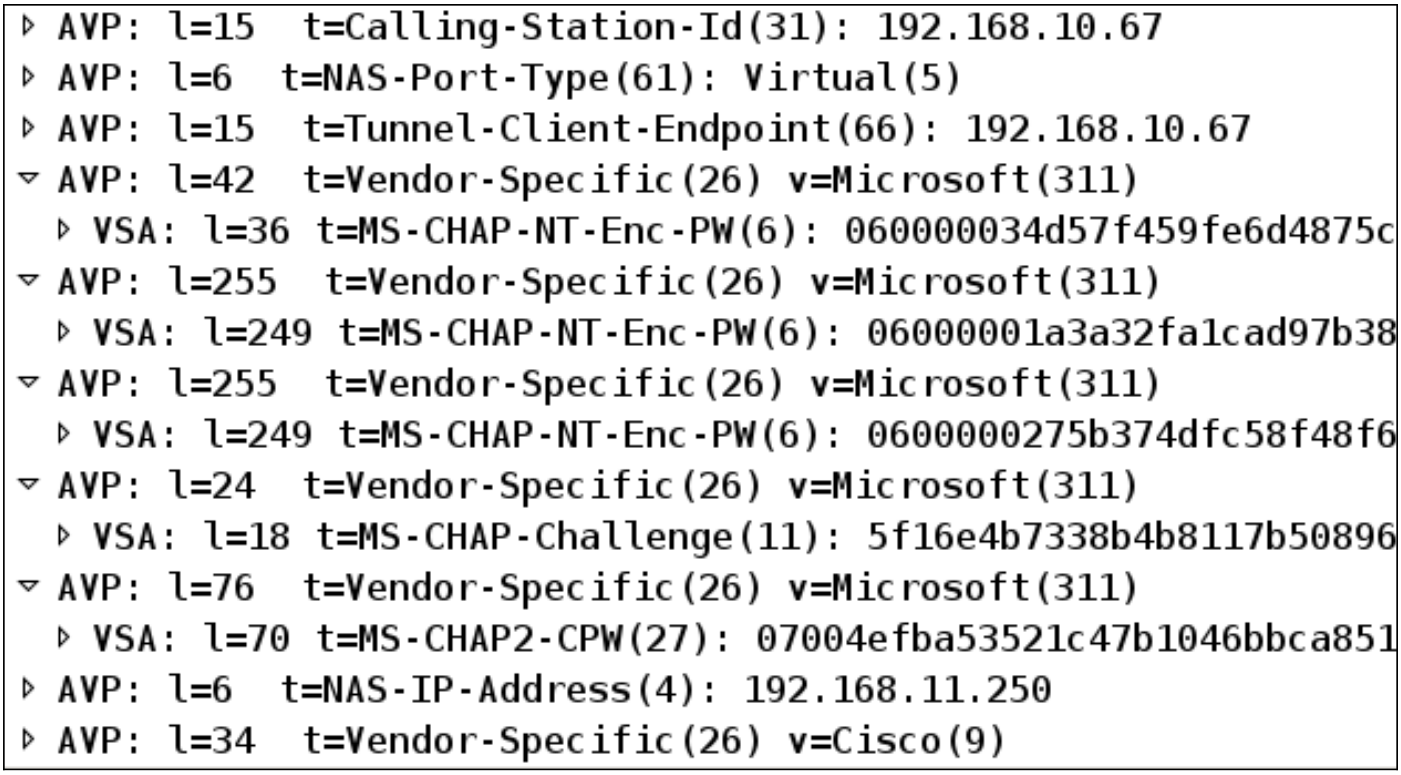
ASA는 이 메시지를 이해하고 MODE_CFG를 사용하여 Cisco VPN 클라이언트에서 새 비밀번호를 요청합니다.

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

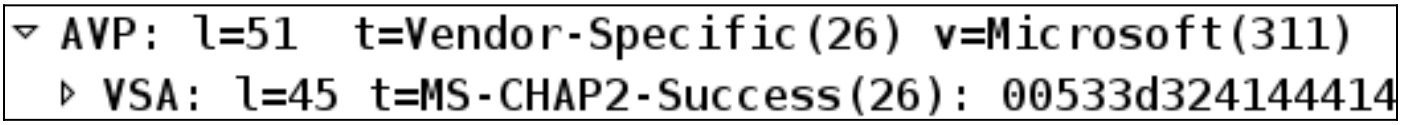
Cisco VPN 클라이언트는 새 비밀번호를 묻는 대화 상자를 표시합니다.



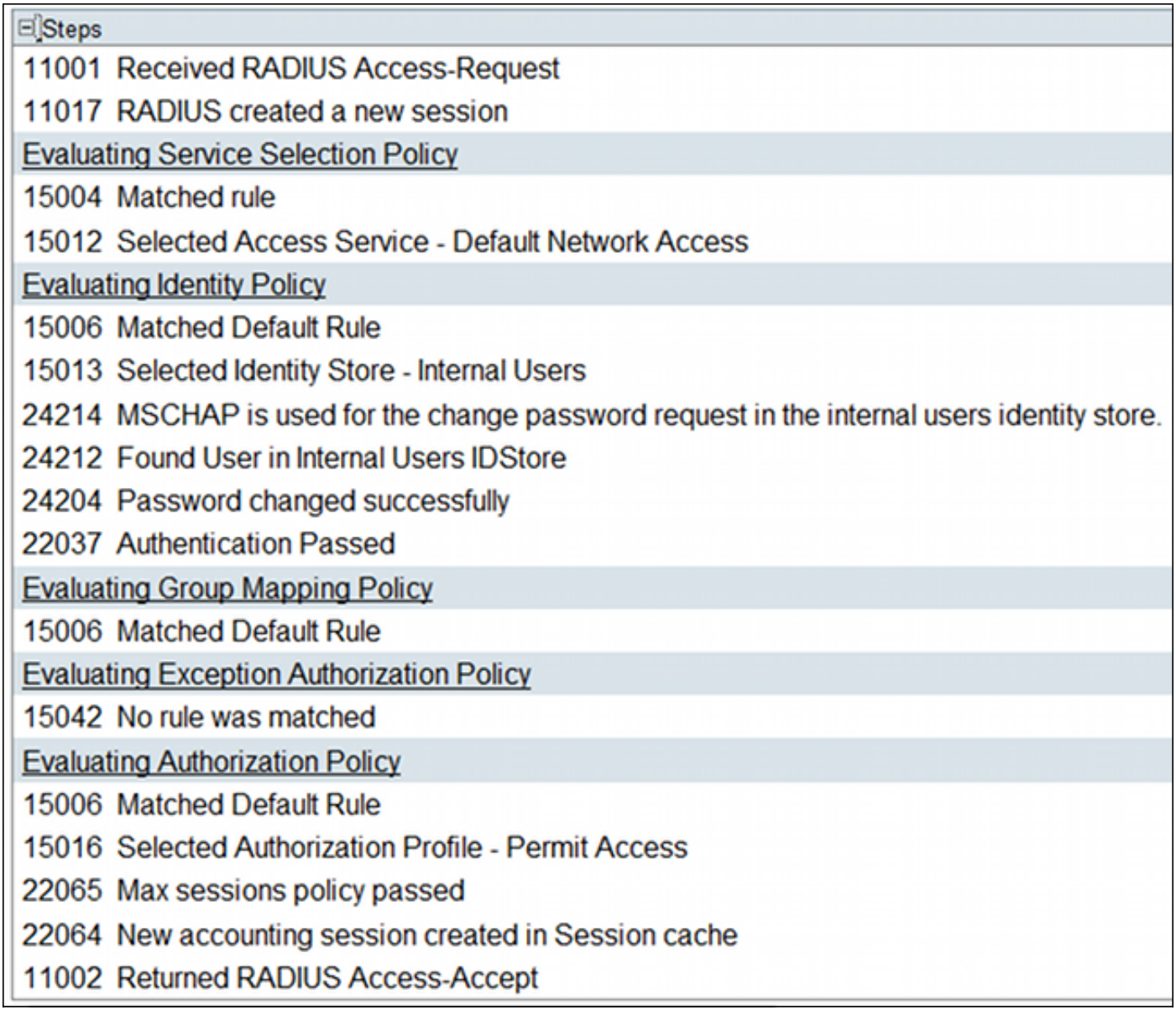
ASA는 MS-CHAP-CPW 및 MS-CHAP-NT-Enc-PW 페이로드와 함께 다른 Radius-Request(새 비밀번호)를 전송합니다.



ACS는 요청을 확인하고 MS-CHAP2-Success와 함께 Radius-Accept를 반환합니다.



이는 '24204 비밀번호가 성공적으로 변경되었다고 보고하는 ACS에서 확인할 수 있습니다.



그런 다음 ASA는 성공적인 인증을 보고하고 QM(Quick Mode) 프로세스를 계속합니다.

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

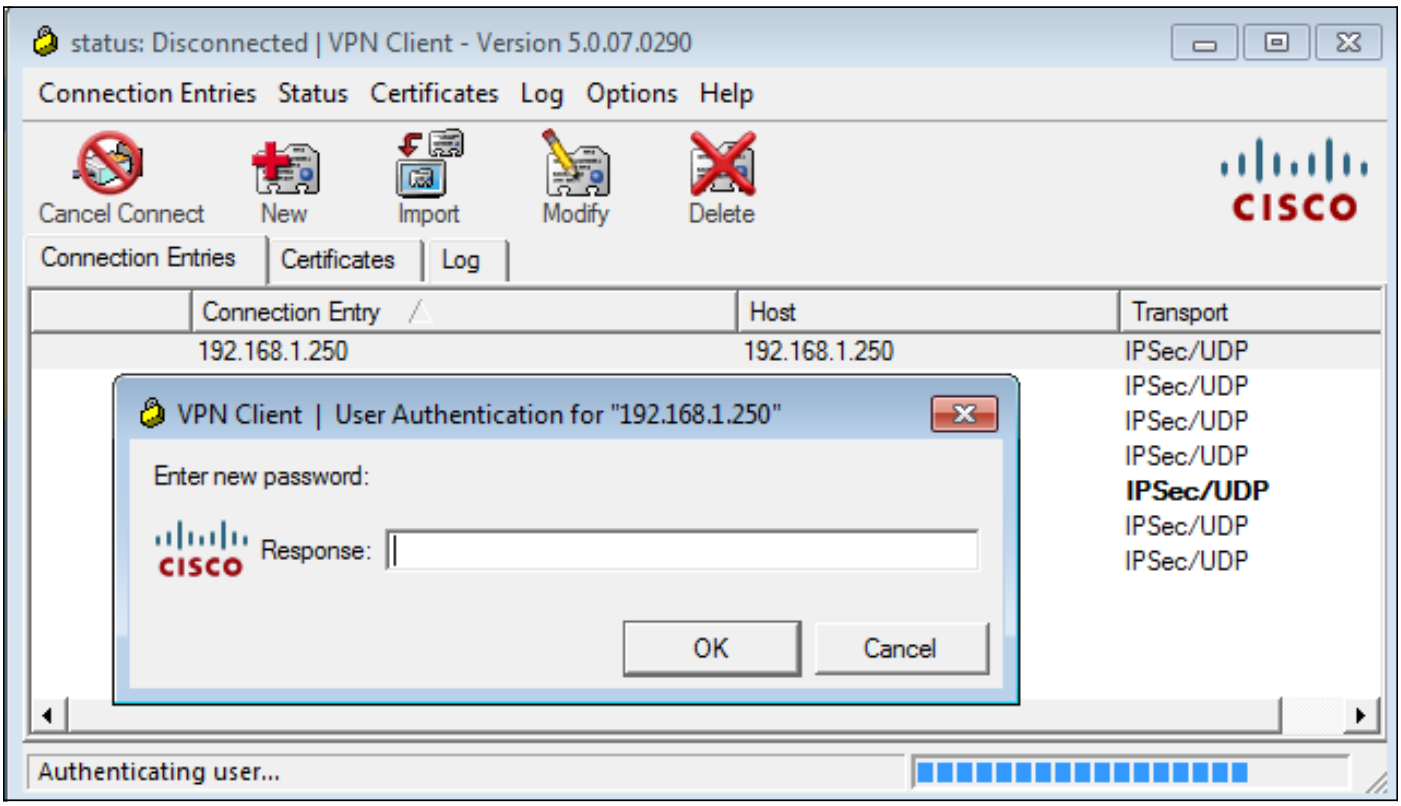
TACACS+를 통한 ACS가 포함된 ASA

마찬가지로, TACACS+는 비밀번호 만료 및 변경에 사용할 수 있습니다.ASA는 MSCHAPv2 대신 인증 유형이 ASCII인 TACACS+를 계속 사용하므로 비밀번호 관리 기능이 필요하지 않습니다.

여러 패킷이 교환되고 ACS에서 새 비밀번호를 요청합니다.

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

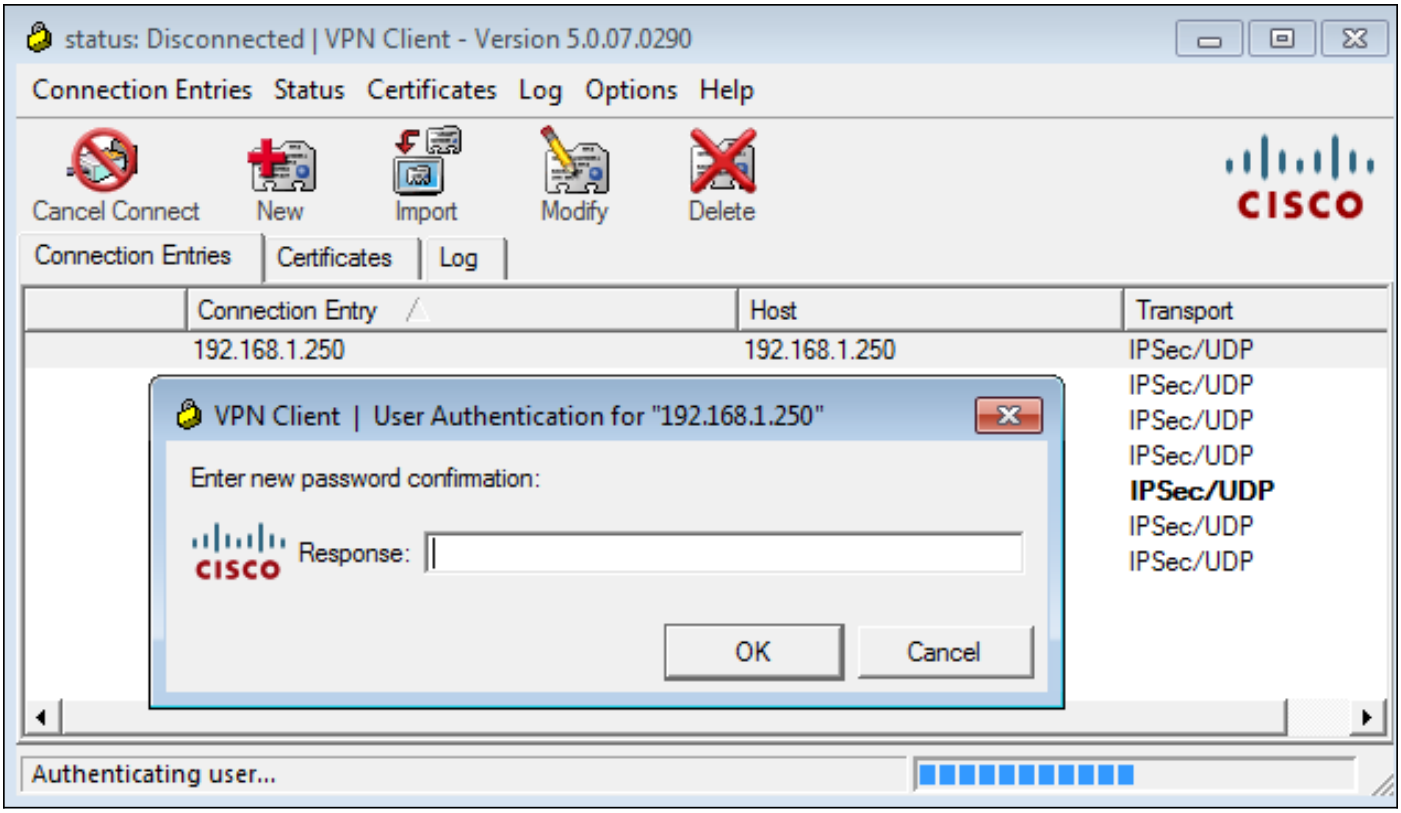
Cisco VPN 클라이언트는 새 비밀번호를 묻는 대화 상자(RADIUS에서 사용하는 대화 상자와 다름)를 표시합니다.



ACS에서 새 비밀번호 확인을 요청합니다.

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

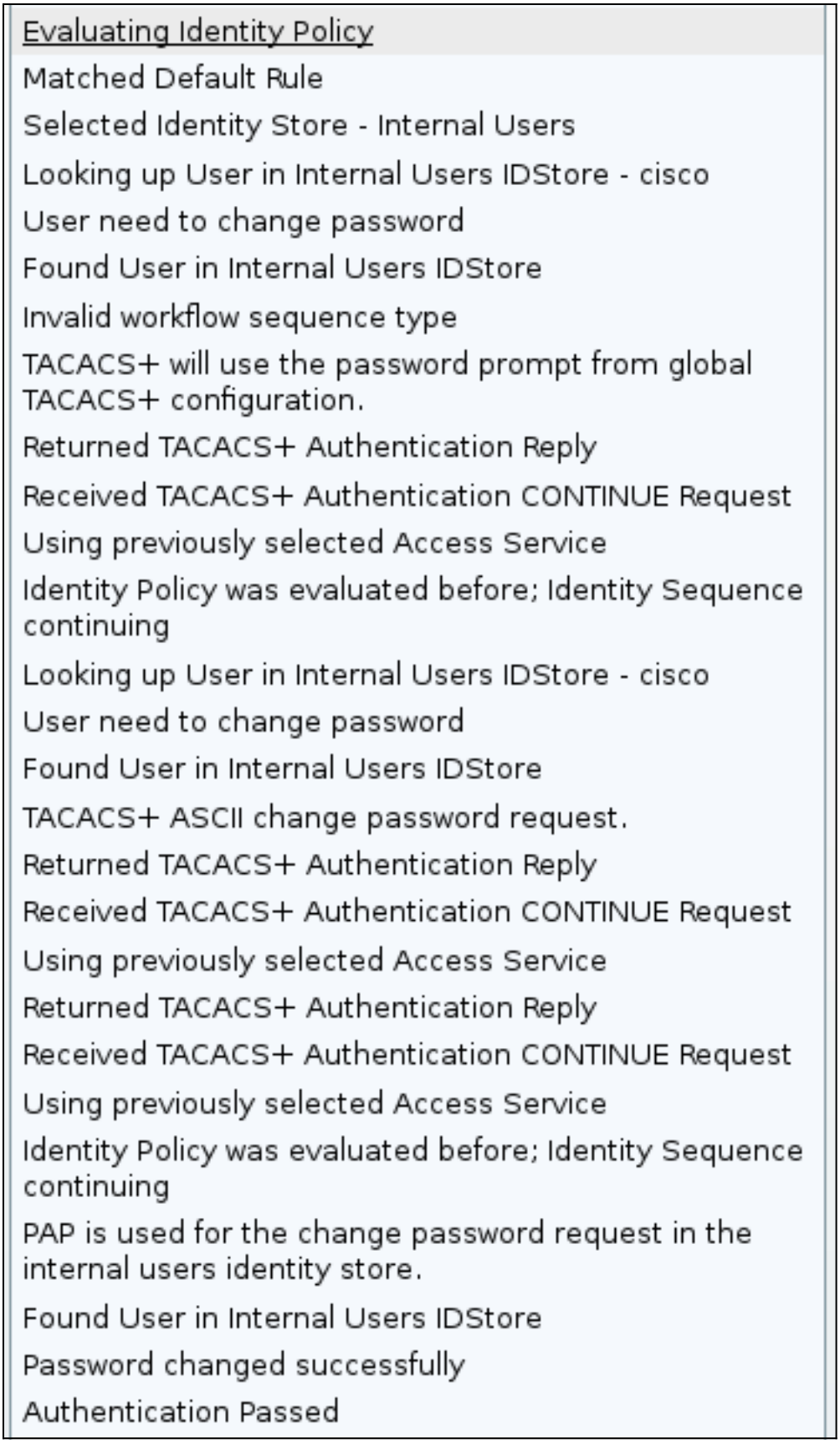
Cisco VPN 클라이언트에는 확인 상자가 표시됩니다.



확인이 올바르면 ACS에서 성공적인 인증을 보고합니다.

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

그런 다음 ACS는 비밀번호가 성공적으로 변경되었다는 이벤트를 기록합니다.



ASA 디버그에는 Exchange 및 성공적인 인증의 전체 프로세스가 표시됩니다.

```
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.
```

해당 비밀번호 변경은 ASA에 대해 완전히 투명합니다.더 많은 요청 및 응답 패킷이 포함된 TACACS+ 세션의 시간이 조금 더 길어 VPN 클라이언트에서 구문 분석되고 비밀번호를 변경하는 사용자에게 표시됩니다.

LDAP를 사용하는 ASA

비밀번호 만료 및 변경은 Microsoft AD 및 Sun LDAP 서버 스키마에서 완벽하게 지원됩니다.

암호 변경 시 서버는 'error = 773'과 함께 'bindresponse = invalidCredentials'를 반환합니다. 이 오류는 사용자가 비밀번호를 재설정해야 함을 나타냅니다.일반적인 오류 코드는 다음과 같습니다.

오류 코드	오류
525	사용자를 찾을 수 없음
52e	잘못된 자격 증명
530	현재 로그온할 수 없음
531	이 워크스테이션에서 로그온할 수 없음
532	비밀번호 만료
533	계정 사용 안 함
701	계정 만료
773	사용자가 비밀번호를 재설정해야 함
775	사용자 계정 잠김

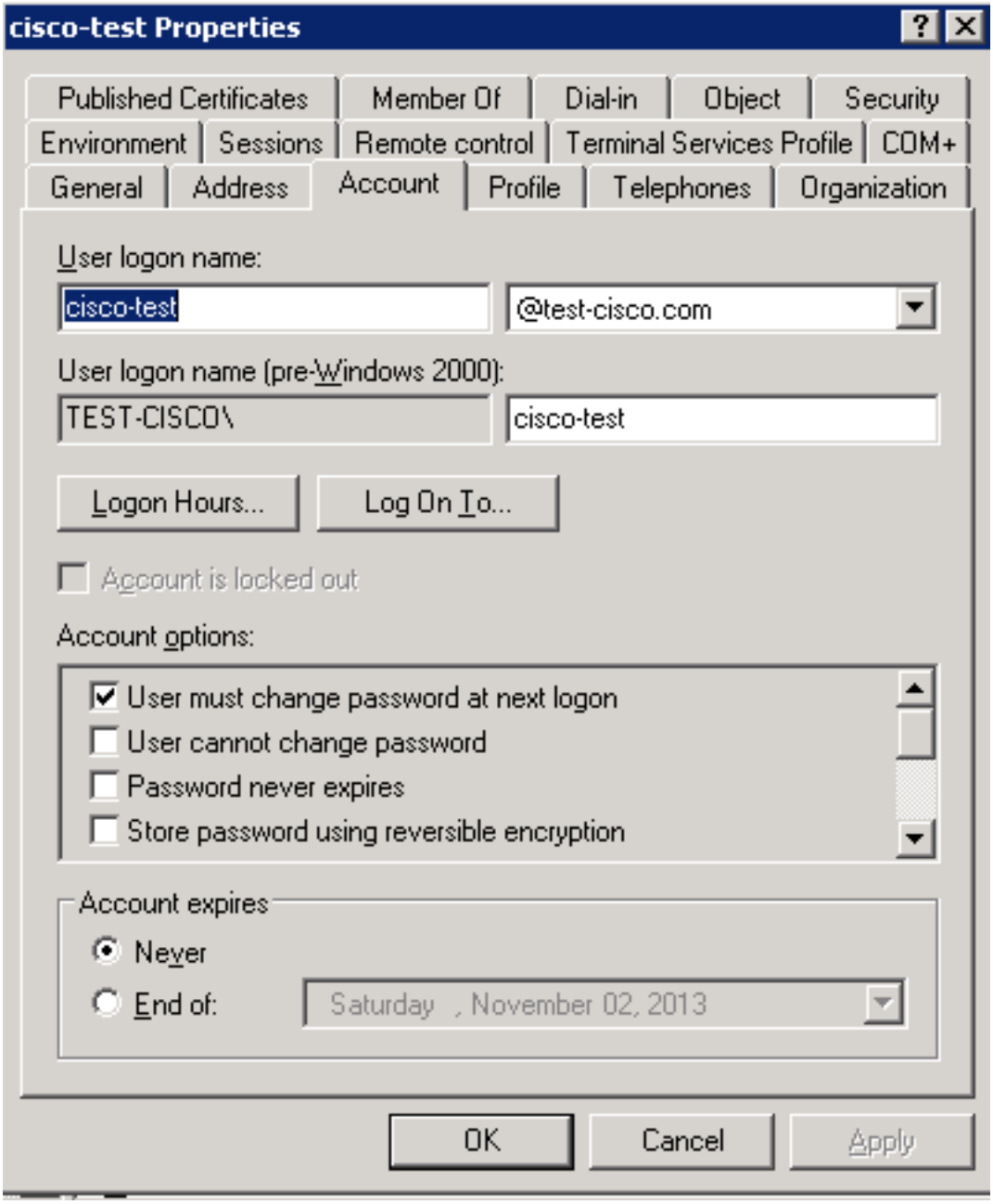
LDAP 서버를 구성합니다.

```
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
```

터널 그룹 및 비밀번호 관리 기능에 대해 이 컨피그레이션을 사용합니다.

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

비밀번호를 변경해야 하도록 AD 사용자를 구성합니다.



사용자가 Cisco VPN 클라이언트를 사용하려고 하면 ASA에서 잘못된 비밀번호를 보고합니다.

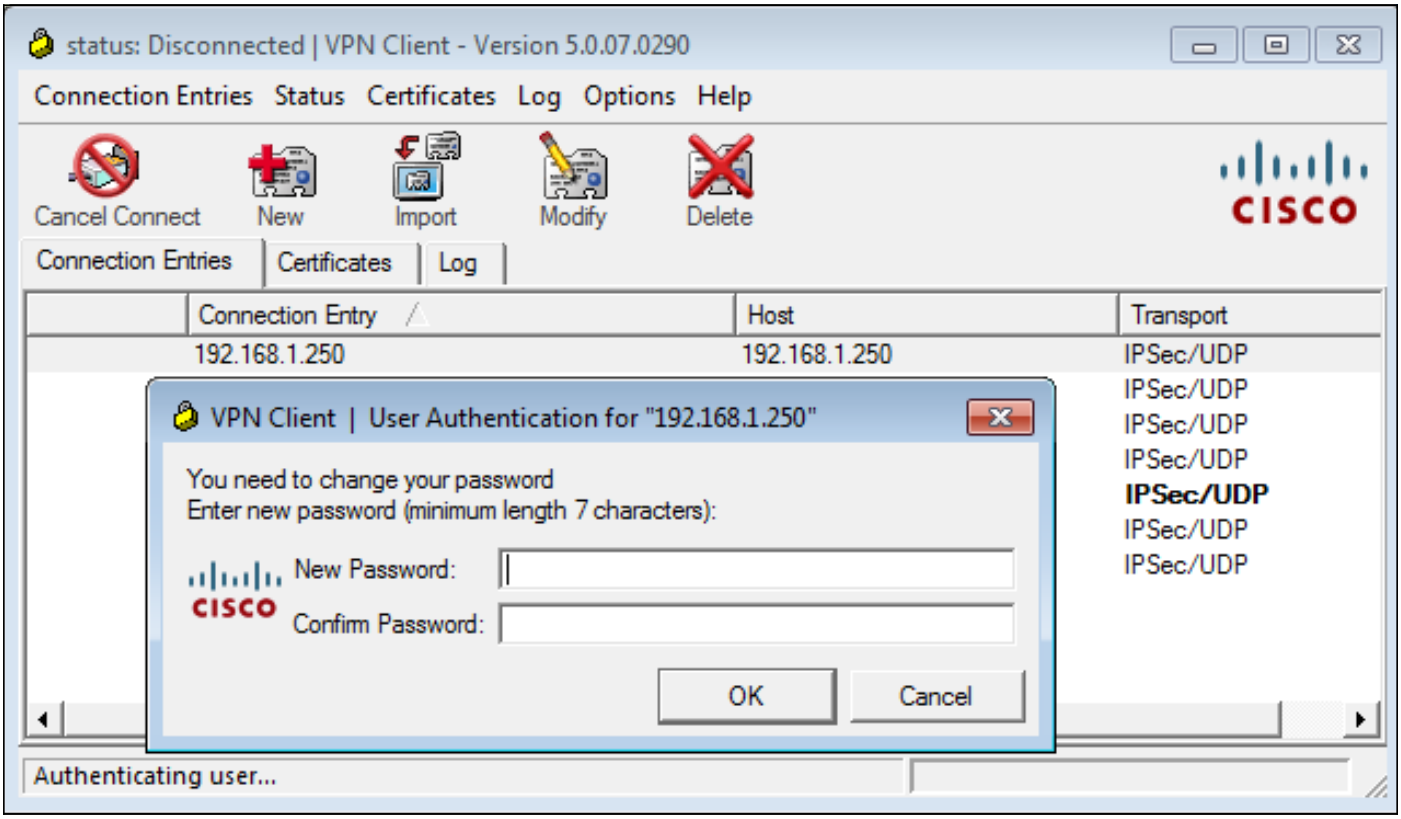
```
ASA(config-tunnel-general)# debug ldap 255
<some output ommited for clarity>

[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
```

자격 증명이 유효하지 않으면 52e 오류가 나타납니다.

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

그런 다음 Cisco VPN 클라이언트에서 비밀번호 변경을 요청합니다.



이 대화 상자는 정책을 표시하므로 TACACS 또는 RADIUS에서 사용하는 대화 상자와는 다릅니다 .이 예에서 정책은 최소 비밀번호 길이 7자입니다.

사용자가 비밀번호를 변경하면 ASA에서 LDAP 서버에서 이 오류 메시지를 받을 수 있습니다.

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

Microsoft 정책에서는 비밀번호를 수정하려면 SSL(Secure Sockets Layer)을 사용해야 합니다.구성을 변경합니다.

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

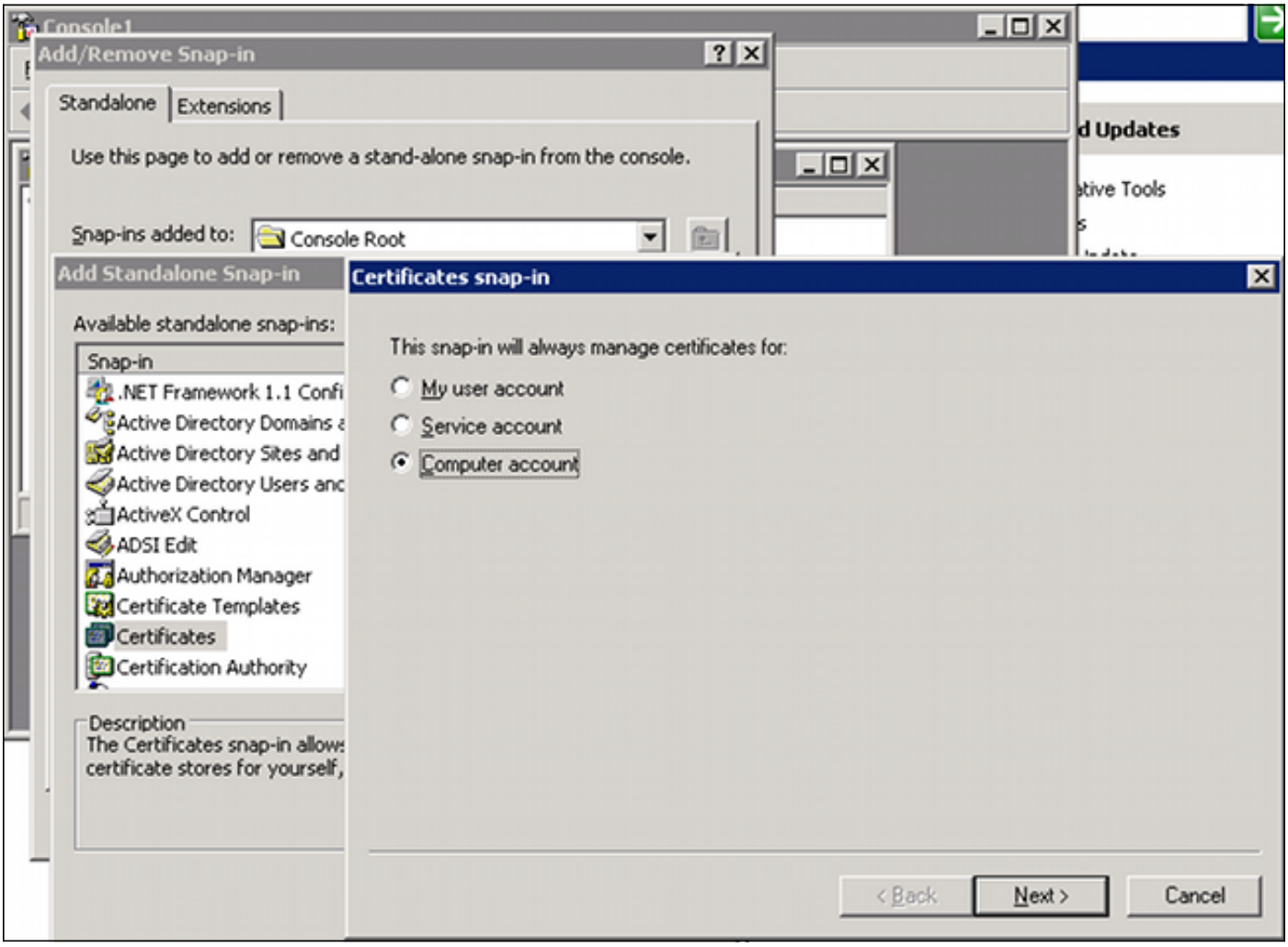
SSL용 Microsoft LDAP

기본적으로 Microsoft LDAP over SSL은 작동하지 않습니다.이 기능을 사용하려면 올바른 키 확장 명으로 컴퓨터 계정에 대한 인증서를 설치해야 합니다.자세한 내용은 서드파티 인증 기관에서 SSL을 통한 LDAP를 활성화하는 방법을 참조하십시오.

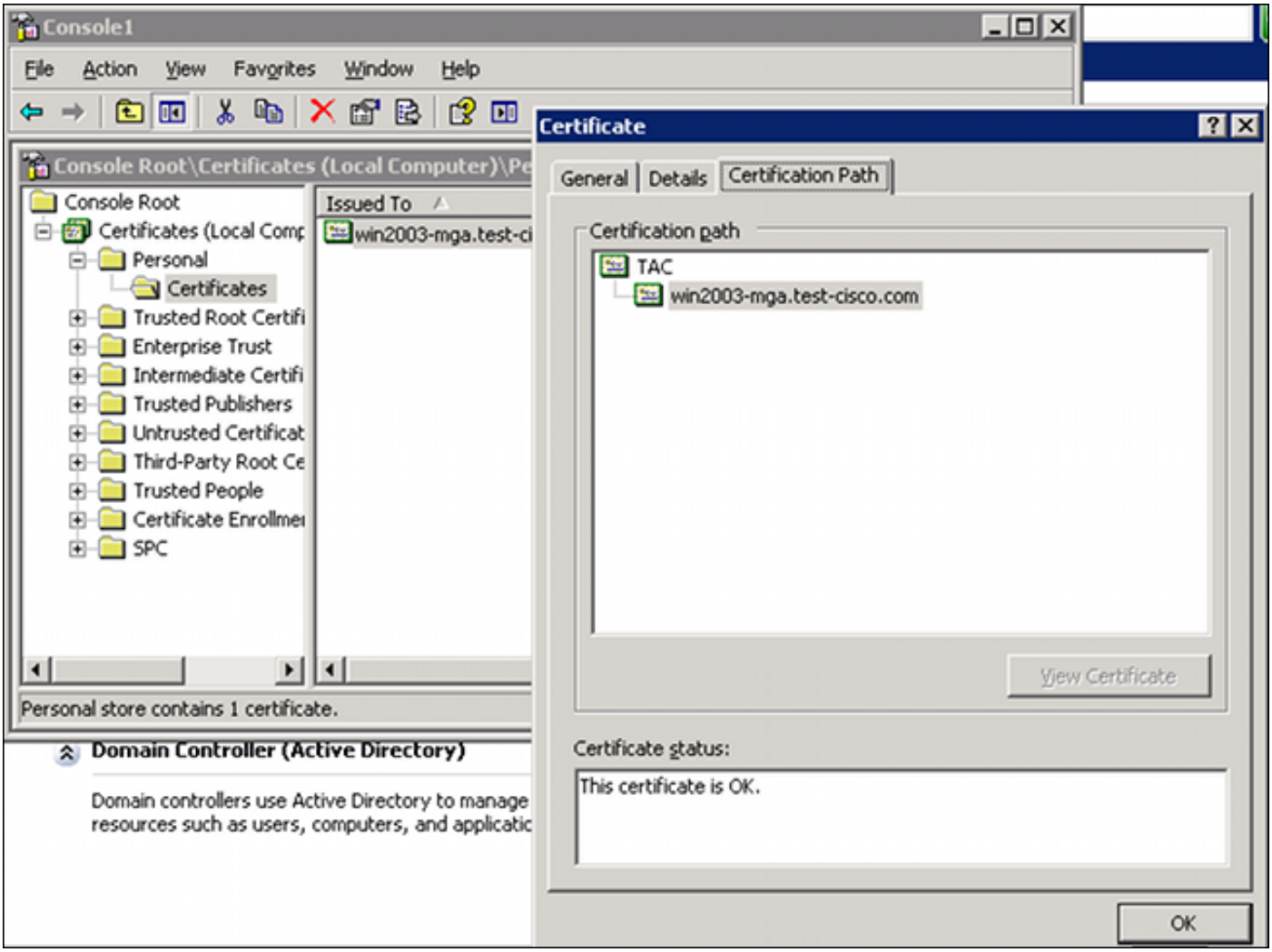
ASA에서 LDAP 인증서를 확인하지 않으므로 인증서가 자체 서명 인증서일 수도 있습니다.관련 개선 요청에 대해서는 Cisco Bug ID CSCui40212, "ASA에서 LDAPS 서버의 인증서를 검증할 수 있도록 허용"을 참조하십시오.

참고:ACS는 버전 5.5 이상에서 LDAP 인증서를 확인합니다.

인증서를 설치하려면 mmc 콘솔을 열고 스냅인 **추가/제거**를 선택하고 인증서를 추가하고 **컴퓨터 계정**을 선택합니다.



로컬 **컴퓨터**를 선택하고 인증서를 개인 저장소로 가져온 다음 연결된 CA(Certificate Authority) 인증서를 신뢰할 수 있는 저장소로 이동합니다.인증서가 신뢰되는지 확인합니다.



ASA 버전 8.4.2에 버그가 있습니다. 여기서 SSL을 통해 LDAP를 사용하려고 할 때 이 오류가 반환될 수 있습니다.

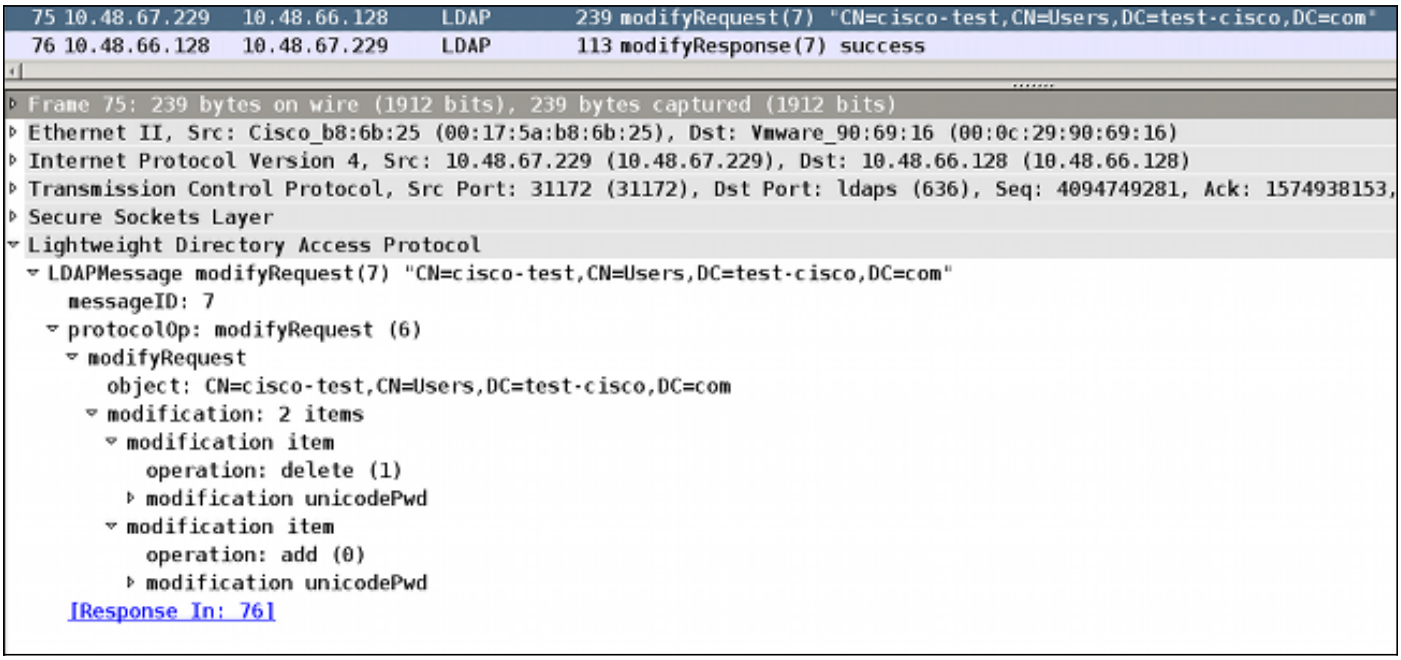
```
ASA(config)# debug ldap 255

[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 버전 9.1.3은 동일한 컨피그레이션에서 올바르게 작동합니다.두 개의 LDAP 세션이 있습니다.첫 번째 세션에서는 코드 773(비밀번호가 만료됨)의 오류를 반환하고 두 번째 세션은 비밀번호 변경에 사용됩니다.

```
[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)
```

비밀번호 변경을 확인하려면 패킷을 확인합니다.Wireshark는 LDAP 서버의 개인 키를 사용하여 SSL 트래픽을 해독할 수 있습니다.



ASA의 IKE(Internet Key Exchange)/AAA(Authentication, Authorization, and Accounting) 디버그는 RADIUS 인증 시나리오에서 제공하는 것과 매우 유사합니다.

만료 전 LDAP 및 경고

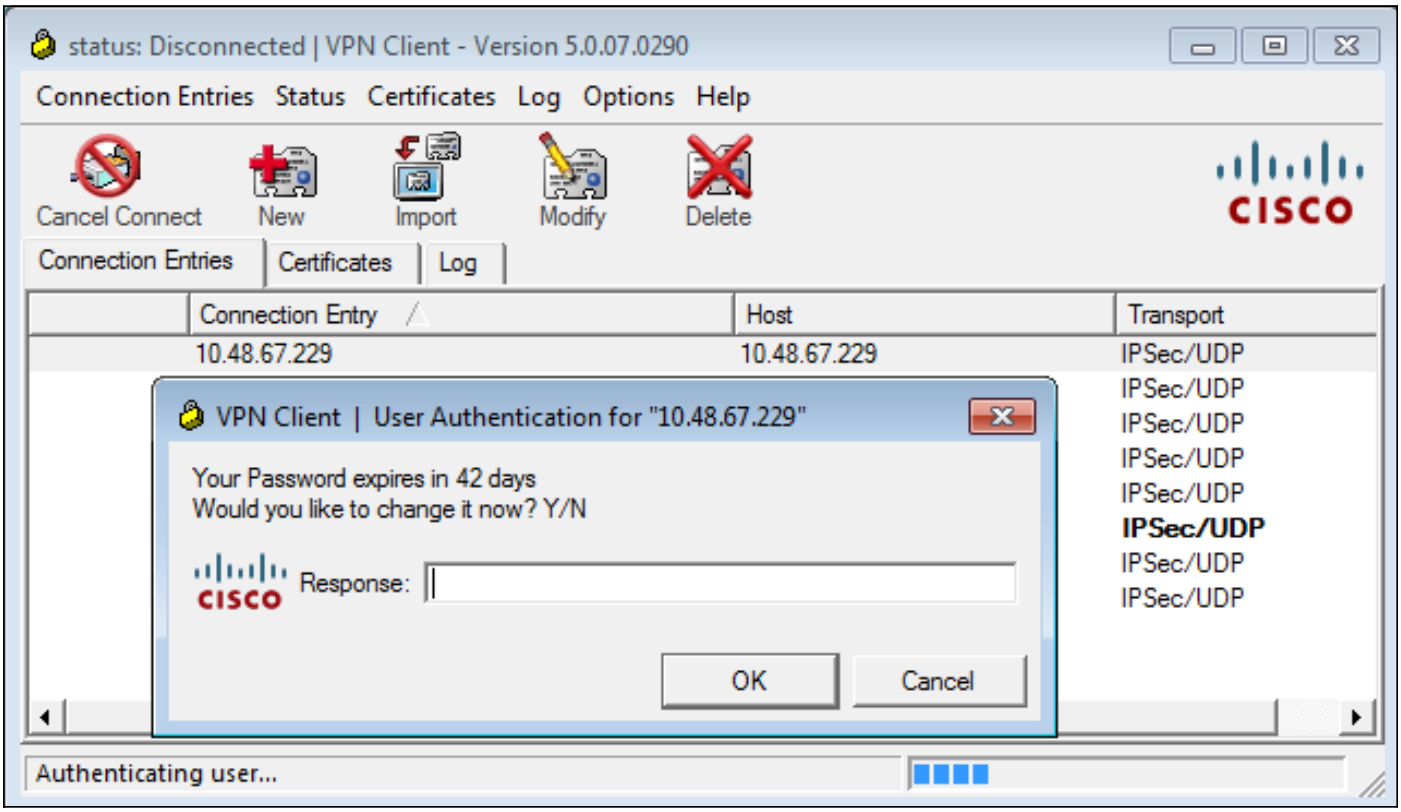
LDAP의 경우 비밀번호가 만료되기 전에 경고를 보내는 기능을 사용할 수 있습니다.ASA는 다음 설정을 사용하여 비밀번호 만료 90일 전에 사용자에게 경고합니다.

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

여기서 비밀번호는 42일 후에 만료되며 사용자가 로그인을 시도합니다.

```
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
```

ASA는 경고를 전송하고 비밀번호 변경 옵션을 제공합니다.



사용자가 비밀번호를 변경하기로 선택하면 새 비밀번호를 입력하라는 프롬프트가 표시되고 일반 비밀번호 변경 절차가 시작됩니다.

ASA 및 L2TP

이전 예에서는 IKE 버전 1(IKEv1) 및 IPSec VPN을 제시했습니다.

L2TP(Layer 2 Tunneling Protocol) 및 IPSec의 경우 PPP가 인증을 위한 전송으로 사용됩니다.비밀번호를 변경하려면 PAP 대신 MSCHAPv2가 필요합니다.

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

PPP 세션 내의 L2TP에서 확장 인증의 경우 MSCHAPv2가 협상됩니다.

```
▷ 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
```

사용자 비밀번호가 만료되면 코드 648에 오류가 반환됩니다.

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

그러면 비밀번호를 변경해야 합니다.나머지 프로세스는 MSCHAPv2를 사용하는 RADIUS의 시나리오와 매우 유사합니다.

L2TP 구성 방법에 대한 자세한 내용은 Windows 2000/XP PC와 PIX/ASA 7.2 Using Pre-shared Key Configuration Example을 참조하십시오.

ASA SSL VPN 클라이언트

이전 예제는 IKEv1 및 EOL(End-of-Life)인 Cisco VPN 클라이언트를 참조했습니다.

원격 액세스 VPN에 권장되는 솔루션은 IKE 버전 2(IKEv2) 및 SSL 프로토콜을 사용하는 Cisco AnyConnect Secure Mobility입니다.비밀번호 변경 및 만료 기능은 Cisco AnyConnect에서 Cisco VPN 클라이언트에 대해 수행한 것과 동일하게 작동합니다.

IKEv1의 경우 1.5단계(Xauth/mode config)에서 ASA와 VPN 클라이언트 간에 비밀번호 변경 및 만료 데이터가 교환되었습니다.

IKEv2의 경우 유사합니다.구성 모드는 CFG_REQUEST/CFG_REPLY 패킷을 사용합니다.

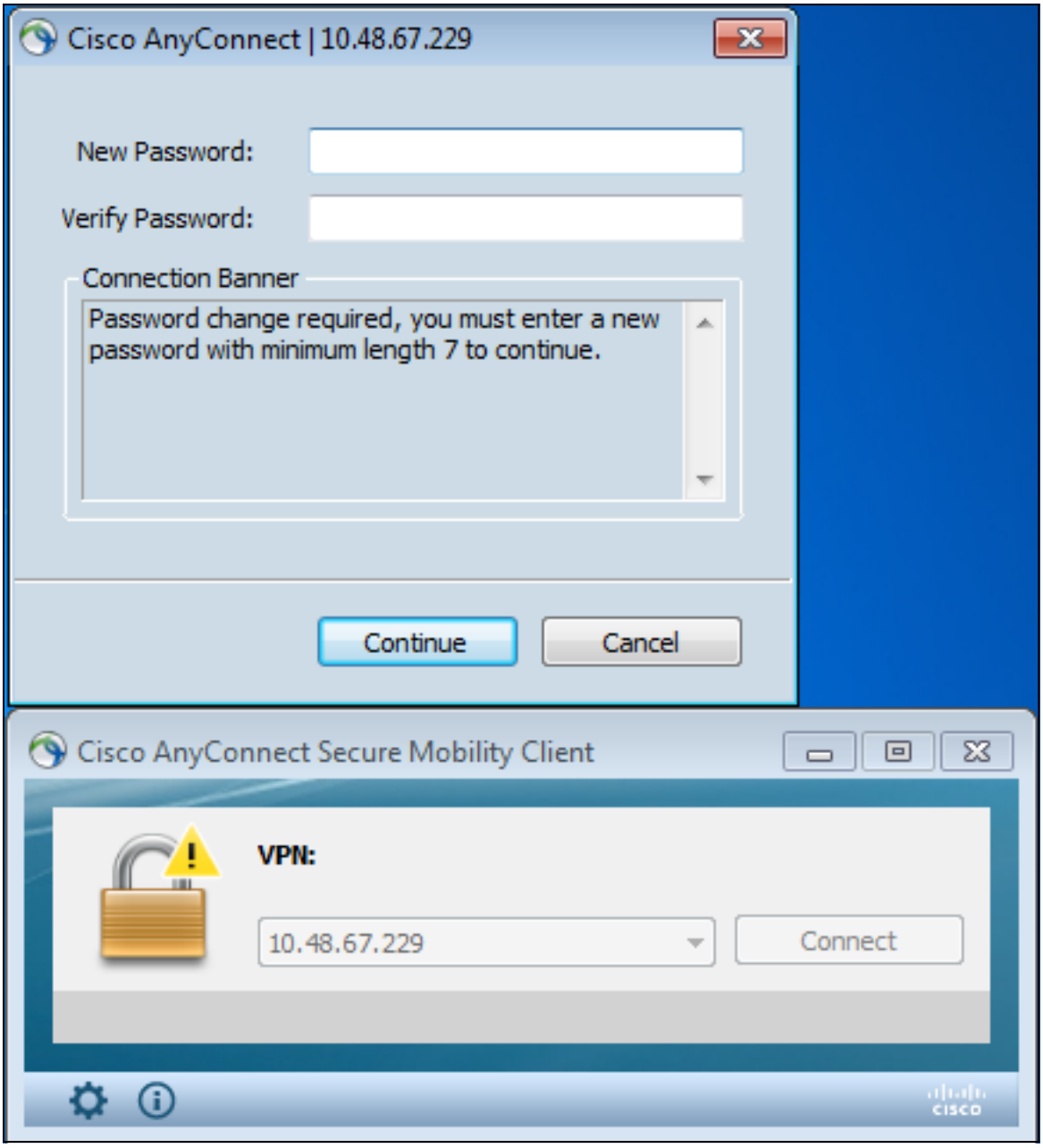
SSL의 경우 데이터는 DTLS(Datagram Transport Layer Security) 제어 세션에 있습니다.

ASA의 컨피그레이션은 동일합니다.

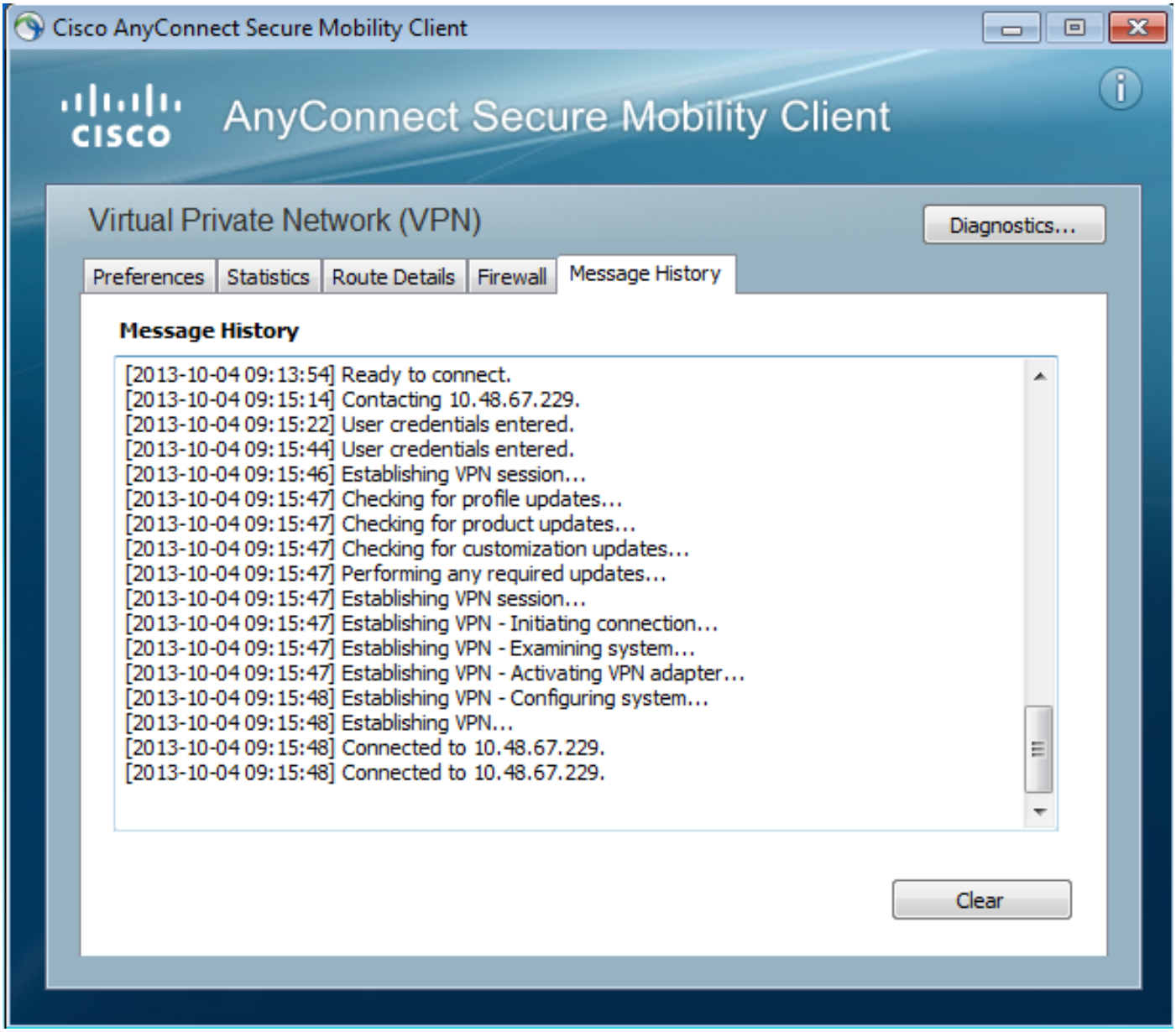
다음은 Cisco AnyConnect 및 SSL을 통한 LDAP 서버를 사용하는 SSL 프로토콜의 예제 컨피그레이션입니다.

```
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
```

올바른 비밀번호(만료된 비밀번호)가 제공되면 Cisco AnyConnect는 연결을 시도하고 새 비밀번호를 요청합니다.



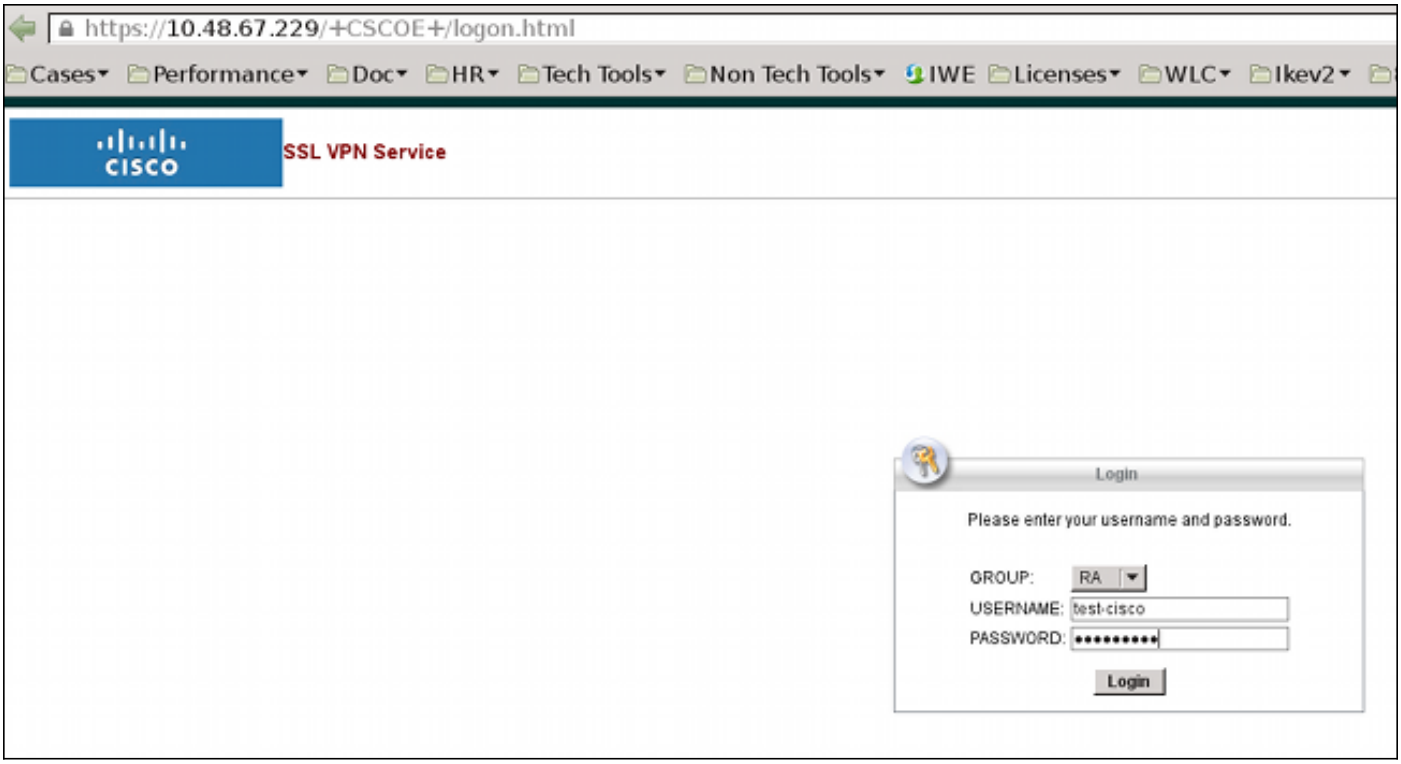
로그는 사용자 자격 증명이 두 번 입력되었음을 나타냅니다.



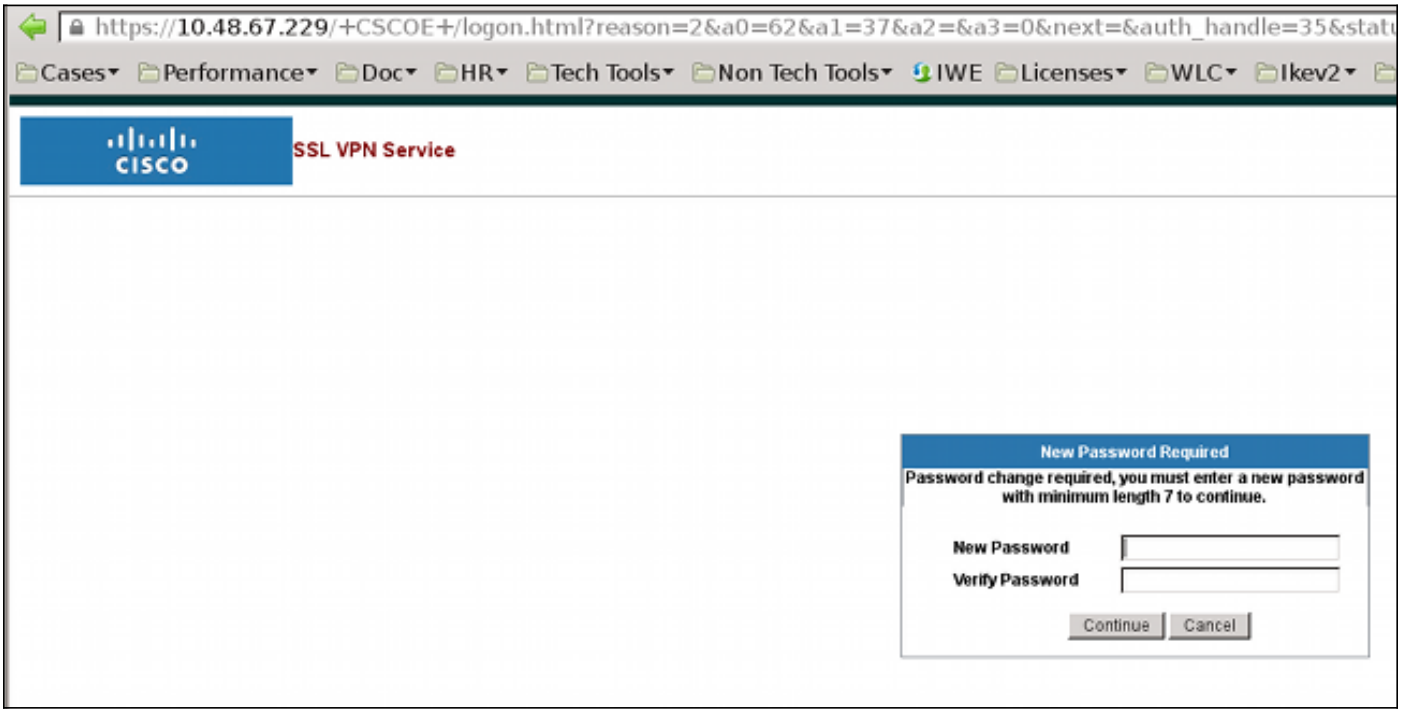
자세한 로그는 진단 DART(AnyConnect Reporting Tool)에서 확인할 수 있습니다.

ASA SSL 웹 포털

웹 포털에서 동일한 로그인 프로세스가 발생합니다.



동일한 비밀번호 만료 및 변경 프로세스가 발생합니다.



ACS 사용자 암호 변경

VPN을 통해 비밀번호를 변경할 수 없는 경우 ACS UCP(User Change Password) 전용 웹 서비스를 사용할 수 있습니다.Cisco Secure Access Control System 5.4에 대한 소프트웨어 개발자 설명서 참조:UCP 웹 서비스 사용.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- CLI를 사용하는 Cisco ASA 5500 Series 컨피그레이션 가이드, 8.4 및 8.6:보안 어플라이언스 사용자 권한 부여를 위한 외부 서버 구성
- 기술 지원 및 문서 – Cisco Systems