ASA远程访问VPN IKE/SSL - RADIUS、TACACS和LDAP的密码到期和更改配置示例

目录

简介

本文档介绍在思科自适应安全设备(ASA)上终止的远程访问VPN隧道上的密码到期和密码更改功能。 本文档涵盖：

- 不同的客户端：Cisco VPN客户端和Cisco AnyConnect安全移动
- 不同协议：TACACS、RADIUS和轻量目录访问协议(LDAP)
- 思科安全访问控制系统(ACS)上的不同商店：本地和Active Directory(AD)

先决条件

要求

Cisco 建议您了解以下主题：

- 通过命令行界面(CLI)了解ASA配置
- ASA上VPN配置的基本知识
- 思科安全ACS的基本知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科自适应安全设备8.4版及更高版本
- Microsoft Windows Server 2003 SP1
- 思科安全访问控制系统5.4版或更高版本
- Cisco AnyConnect安全移动，版本3.1
- Cisco VPN客户端，版本5

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

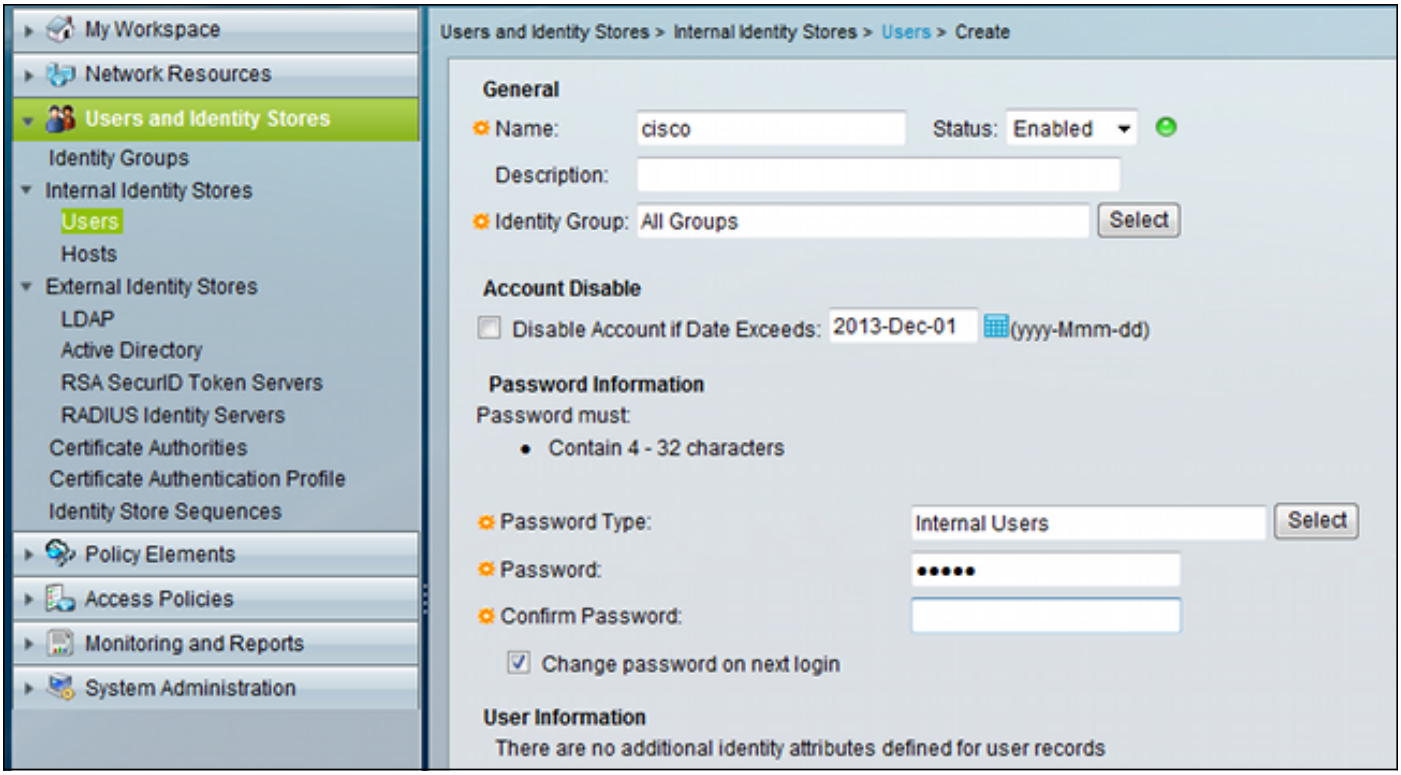
> **注意：**
>
> 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。
>
> 使用 **debug 命令之前，请参阅**有关 Debug 命令的重要信息。

具有本地身份验证的ASA

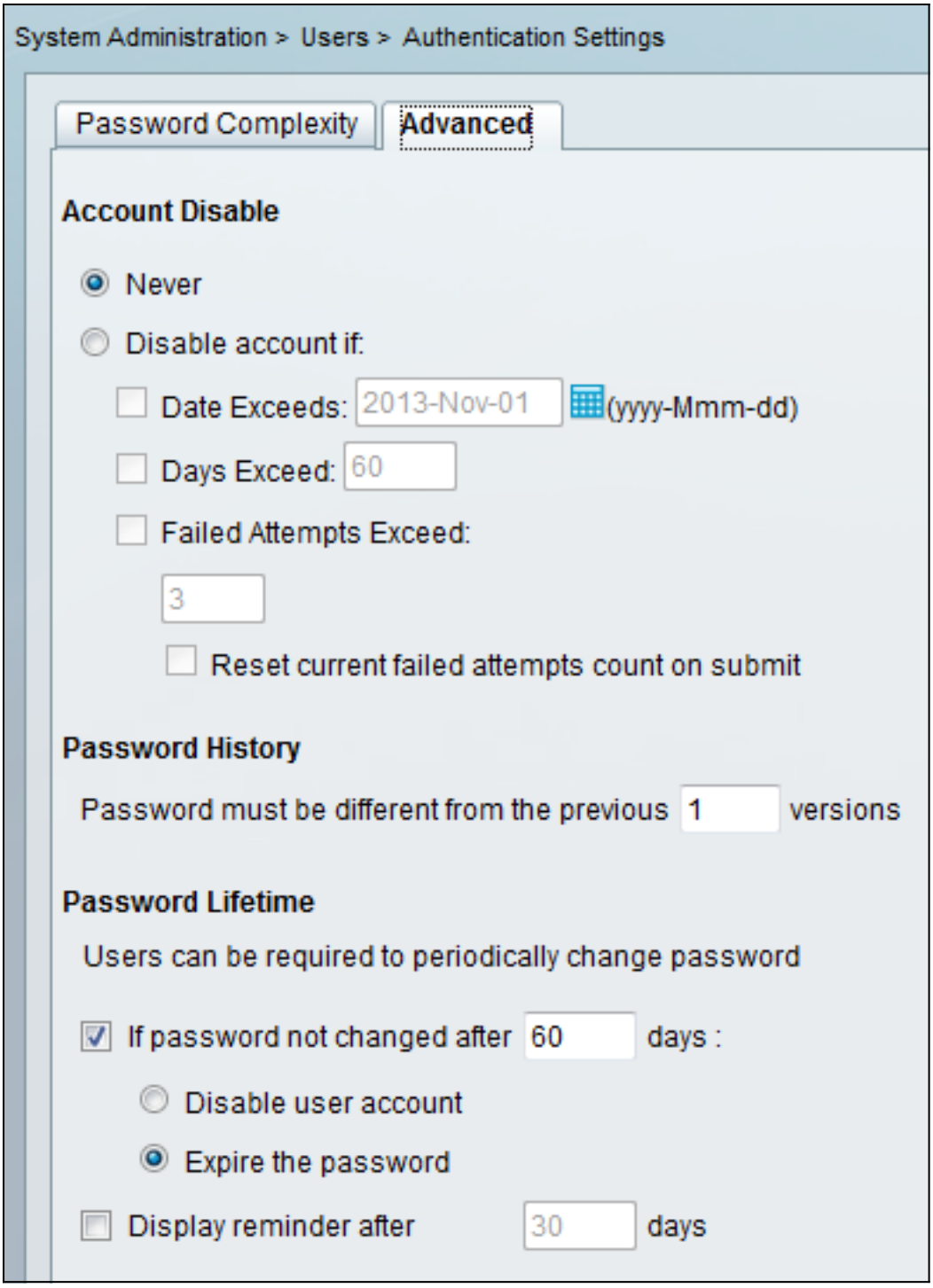
具有本地定义用户的ASA不允许使用密码到期或密码更改功能。需要外部服务器，如RADIUS、TACACS、LDAP或Windows NT。

ACS和本地用户

ACS支持本地定义用户的密码到期和密码更改。例如，您可以强制新创建的用户在下次登录时更改其密码，或在特定日期禁用帐户：

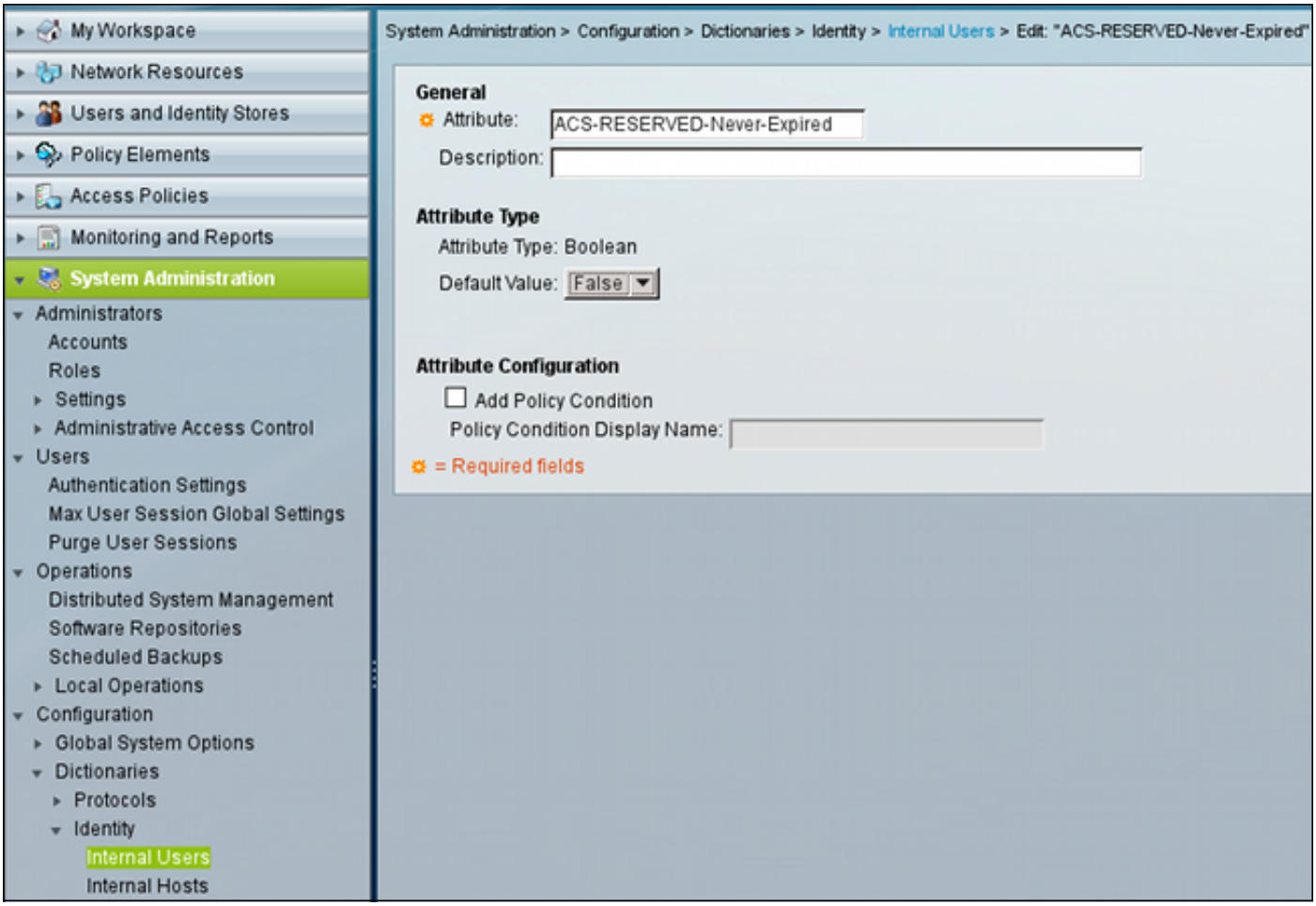


您可以为所有用户配置密码策略。例如，密码到期后，您可以禁用用户帐户（阻止它而不能登录），也可以提供更改密码的选项：

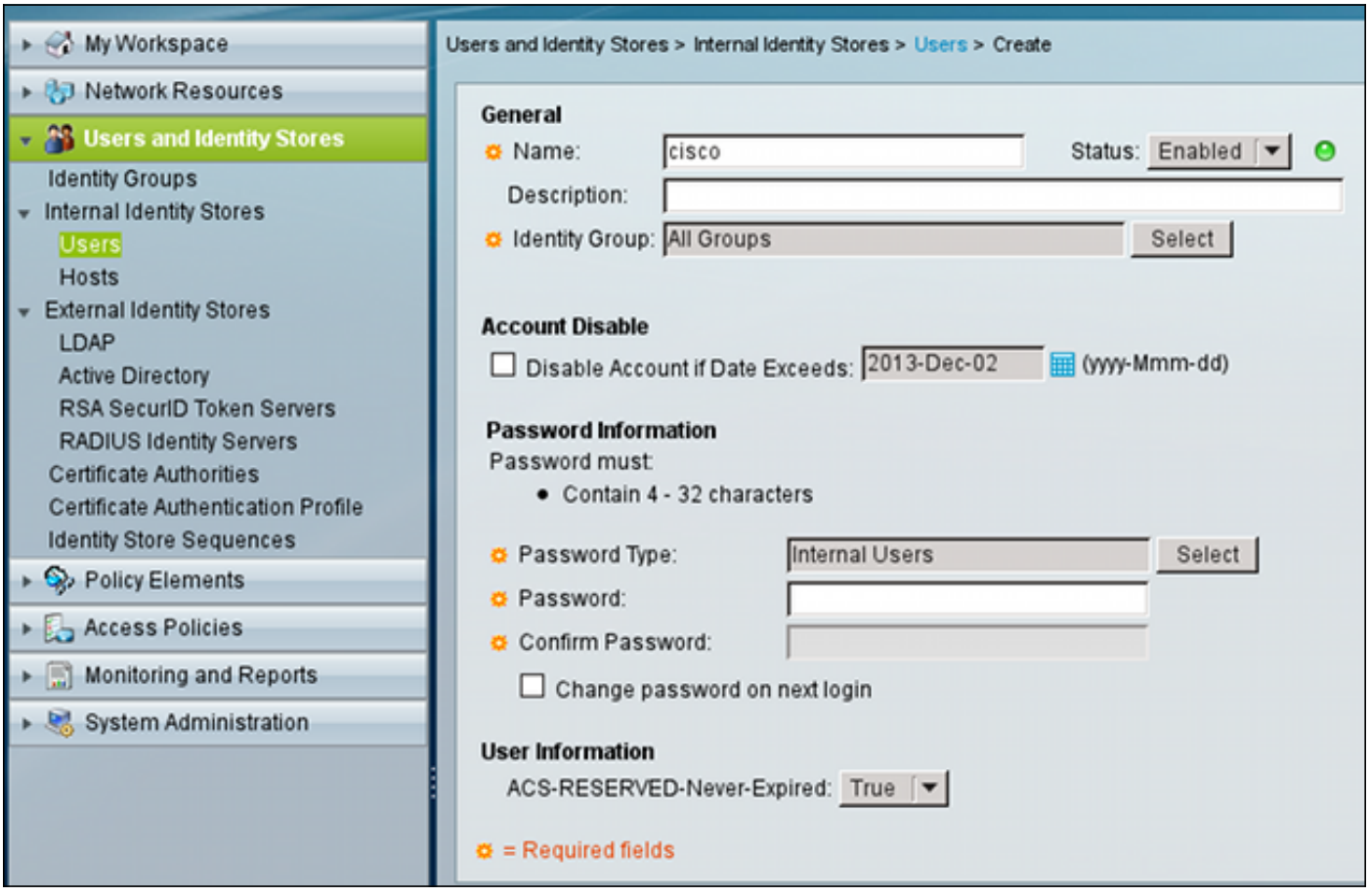


用户特定设置优先于全局设置。

ACS-RESERVED-Never-Expired是用户身份的内部属性。



此属性由用户启用，可用于禁用全局帐户到期设置。使用此设置时，即使全局策略指示帐户应为：

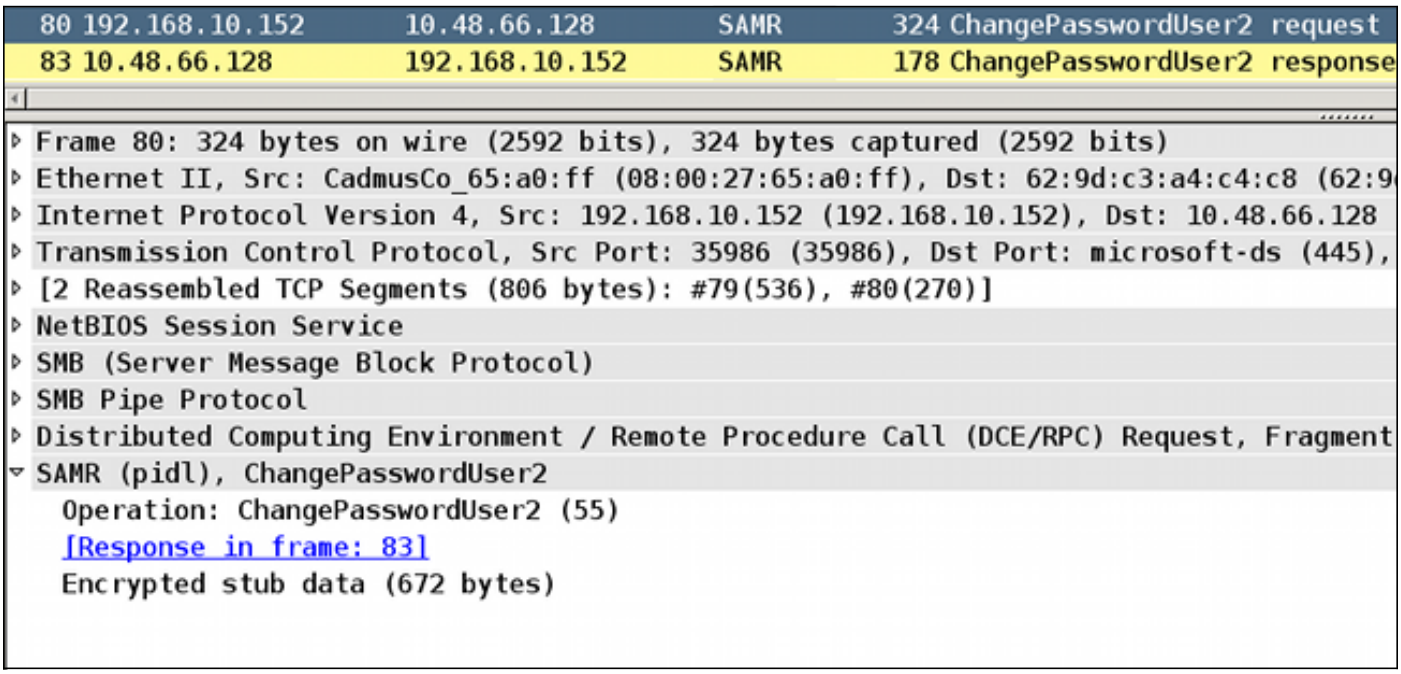


ACS和Active Directory用户

ACS可配置为检查AD数据库中的用户。使用Microsoft质询握手身份验证协议第2版(MSCHAPv2)时，支持密码到期和更改；请参阅《思科安全访问控制系统5.4用户指南》：ACS 5.4中的身份验证：身份验证协议和身份库兼容性(了解详细信息)。

在ASA上，您可以使用密码管理功能（如下一节所述），以强制ASA使用MSCHAPv2。

当ACS与域控制器(DC)目录联系时，它使用通用互联网文件系统(CIFS)分布式计算环境/远程过程调用(DCE/RPC)调用来更改密码：



ASA可以同时使用RADIUS和TACACS+协议，以便与ACS联系以更改AD密码。

通过RADIUS的带ACS的ASA

RADIUS协议本地不支持密码到期或密码更改。通常，RADIUS使用密码身份验证协议(PAP)。ASA以明文形式发送用户名和密码，然后使用RADIUS共享密钥加密密码。

在用户密码过期的典型场景中，ACS会向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

对于ASA，它是简单的Radius-Reject消息，身份验证失败。

要解决此问题，ASA允许在隧道组配置下使用**password-management**命令：

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

password-management命令更改行为，以便ASA在Radius-Request中强制使用MSCHAPv2，而不是PAP。

MSCHAPv2协议支持密码到期和密码更改。因此，如果VPN用户在扩展身份验证阶段登录到该特定隧道组，则来自ASA的Radius请求现在包括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)
```

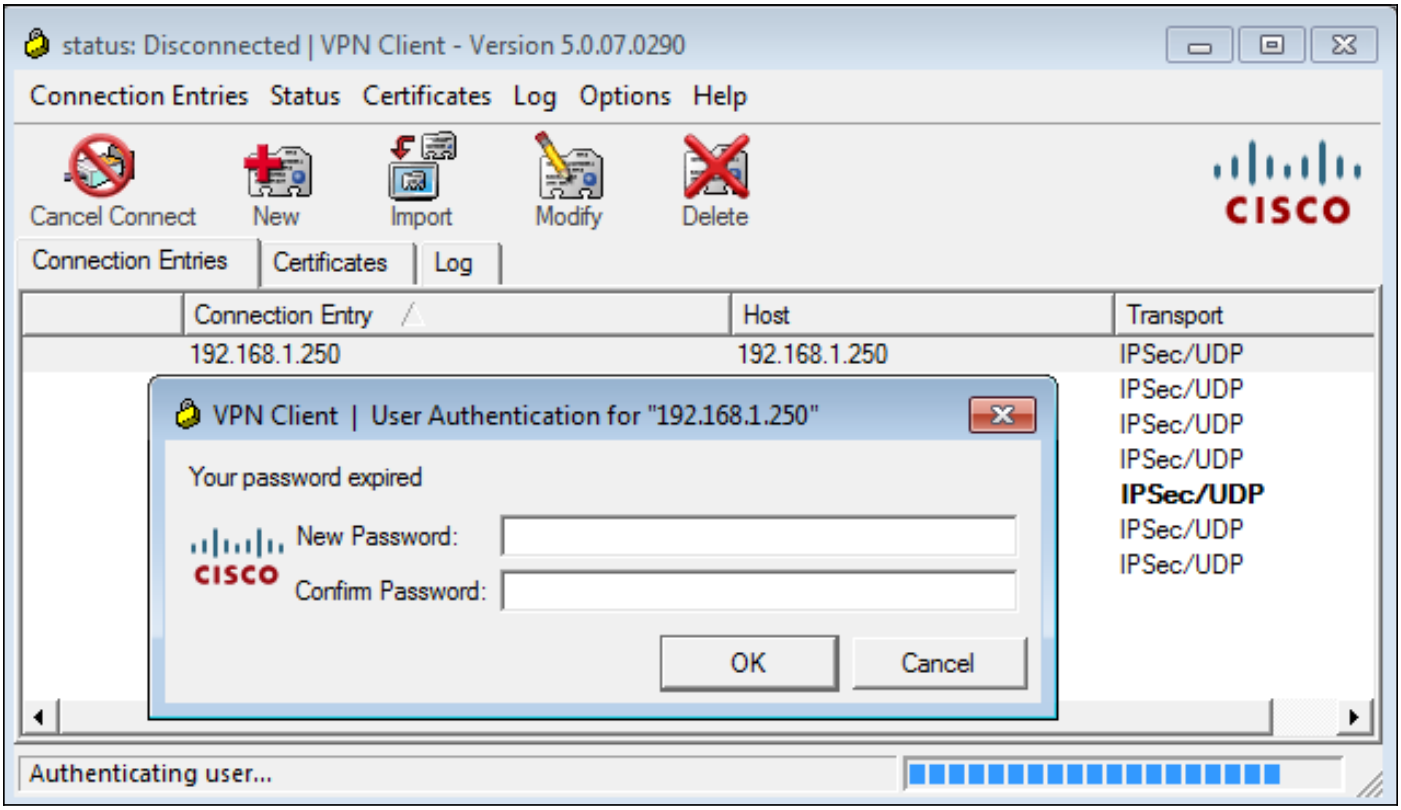
如果ACS发现用户需要更改密码，它会返回Radius-Reject消息，并返回MSCHAPv2错误648。

```
▽ 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
```

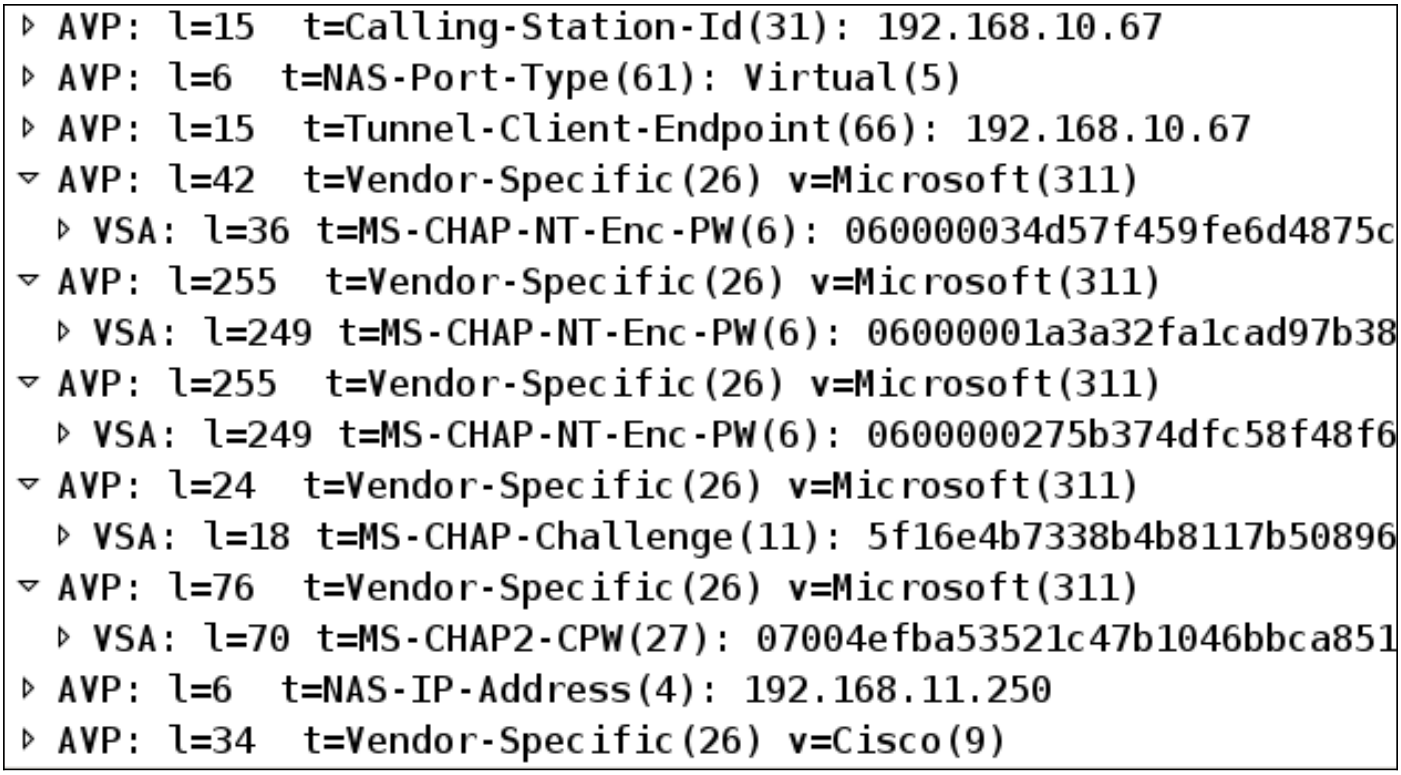
ASA了解该消息并使用MODE_CFG从Cisco VPN客户端请求新密码：

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

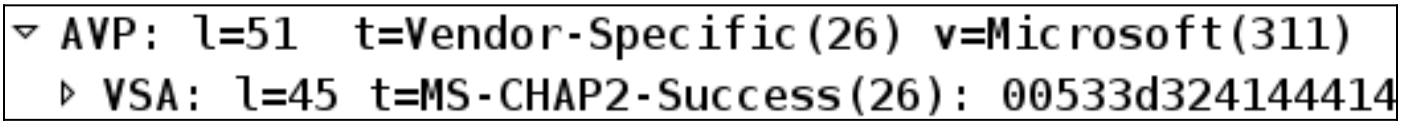
Cisco VPN客户端显示一个对话框，提示输入新密码：



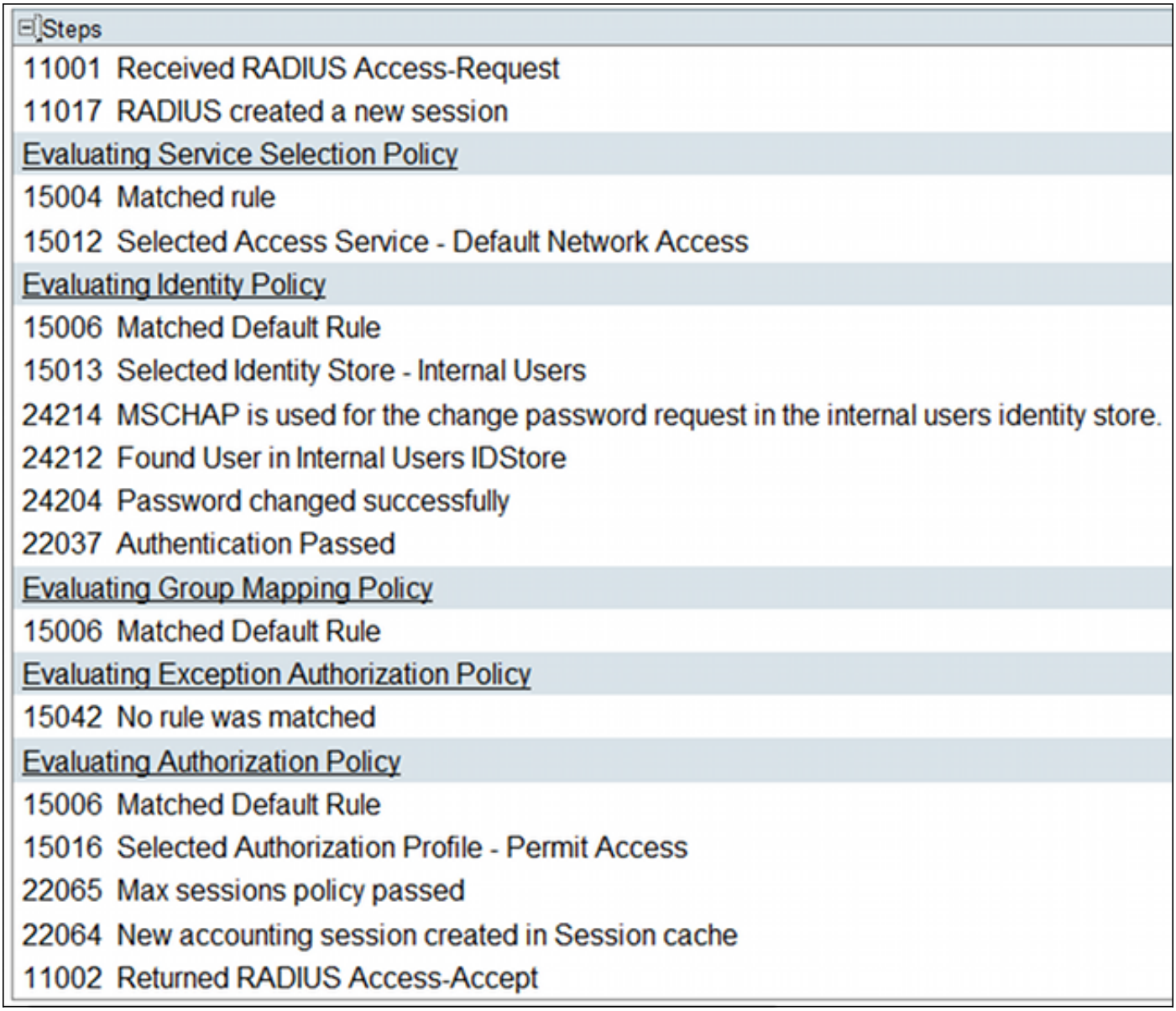
ASA发送另一个带有MS-CHAP-CPW和MS-CHAP-NT-Enc-PW负载（新密码）的Radius请求：



ACS确认请求并返回带MS-CHAP2-Success的Radius-Accept:



这可以在报告“24204密码已成功更改”的ACS上验证：



然后，ASA报告身份验证成功并继续执行快速模式(QM)过程：

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

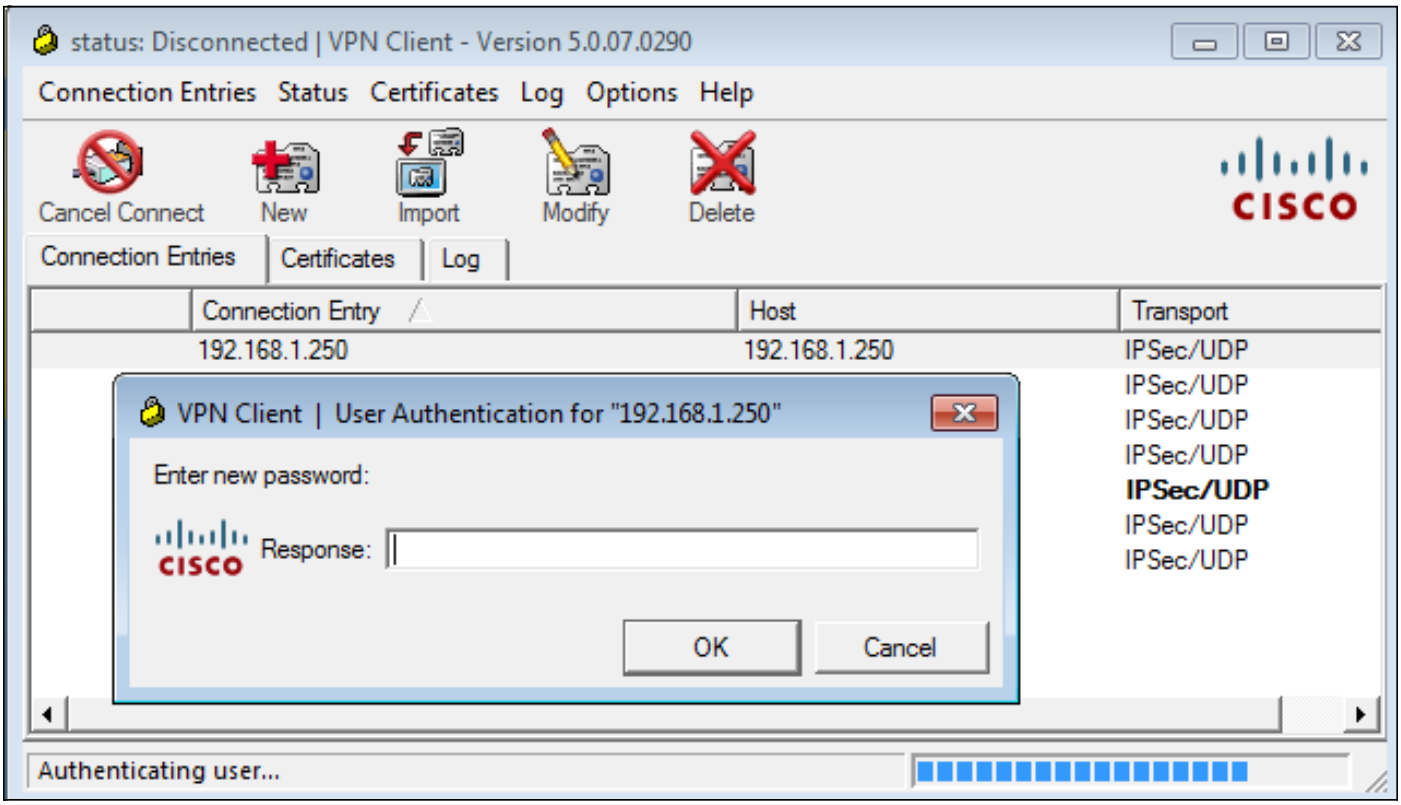
通过TACACS+实现ASA与ACS

同样，TACACS+可用于密码到期和更改。不需要密码管理功能，因为ASA仍使用身份验证类型为ASCII的TACACS+而不是MSCHAPv2。

交换多个数据包，ACS要求输入新密码：

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

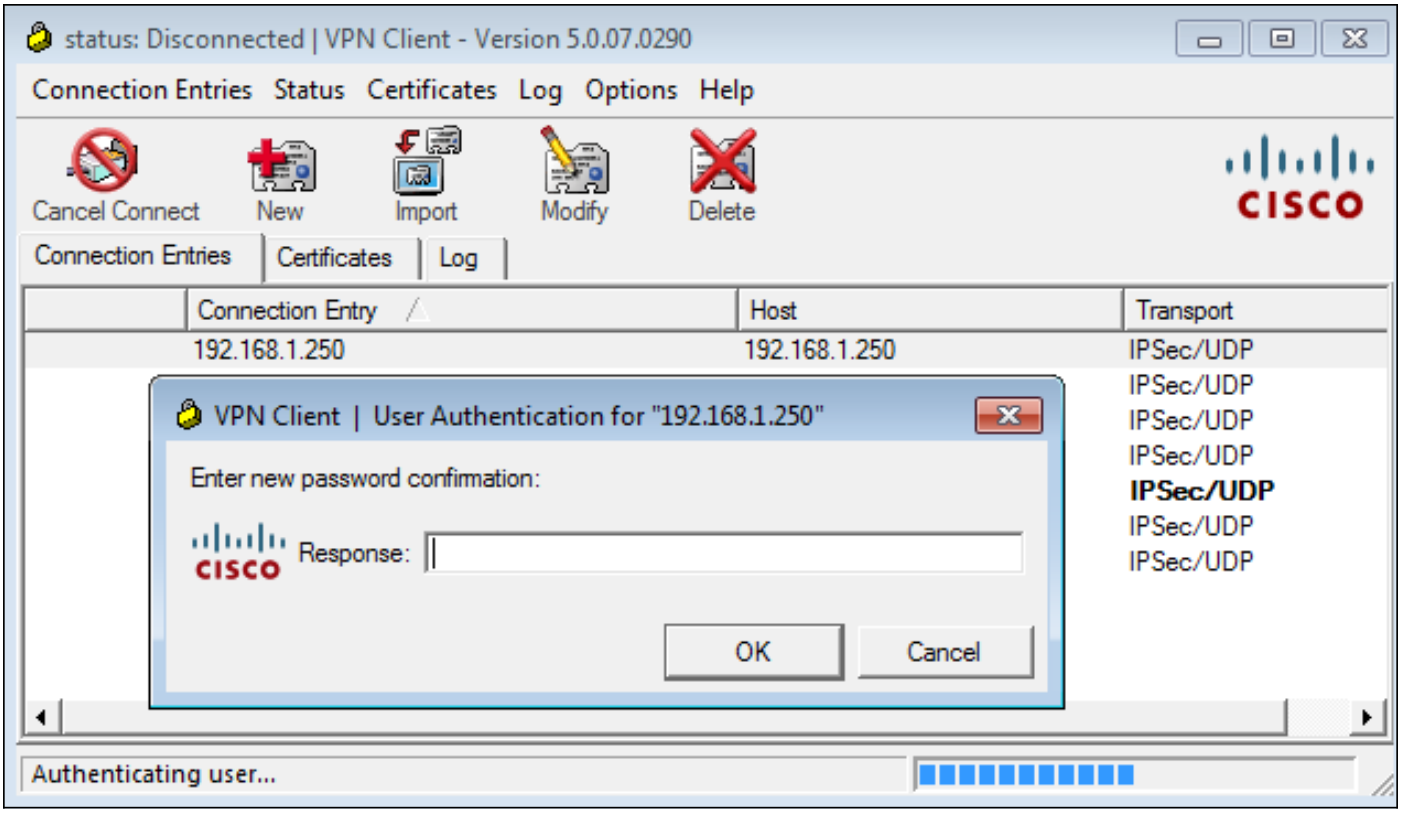
Cisco VPN客户端显示一个对话框（与RADIUS使用的对话框不同），提示输入新密码：



ACS请求确认新密码：

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

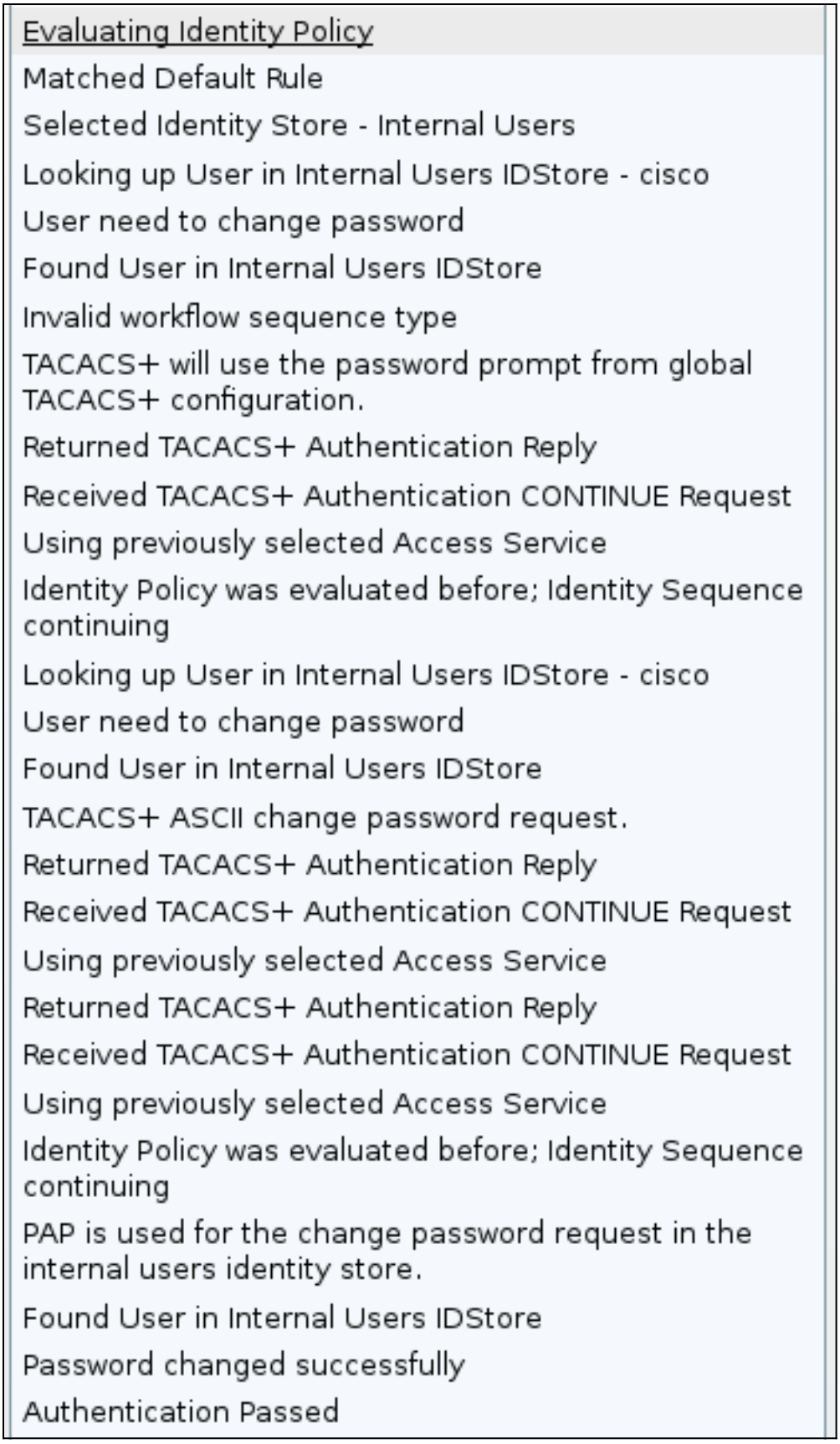
Cisco VPN客户端提供确认框：



如果确认正确，ACS报告身份验证成功：

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

然后，ACS记录密码已成功更改的事件：



ASA调试显示交换和成功身份验证的整个过程：

```
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.
```

该密码更改对ASA完全透明。TACACS+会话只比TACACS+会话长一点，请求和应答数据包更多，由VPN客户端解析并呈现给更改密码的用户。

带LDAP的ASA

Microsoft AD和Sun LDAP服务器架构完全支持密码到期和更改。

对于密码更改，服务器返回“bindresponse = invalidCredentials”，返回“error = 773”。 此错误表示用户必须重置密码。典型错误代码包括：

错误代码	Error
525	找不到用户
52e	凭据无效
530	此时不允许登录
531	不允许登录此工作站
532	密码过期
533	帐户已禁用
701	帐户已过期
773	用户必须重置密码
775	用户帐户已锁定

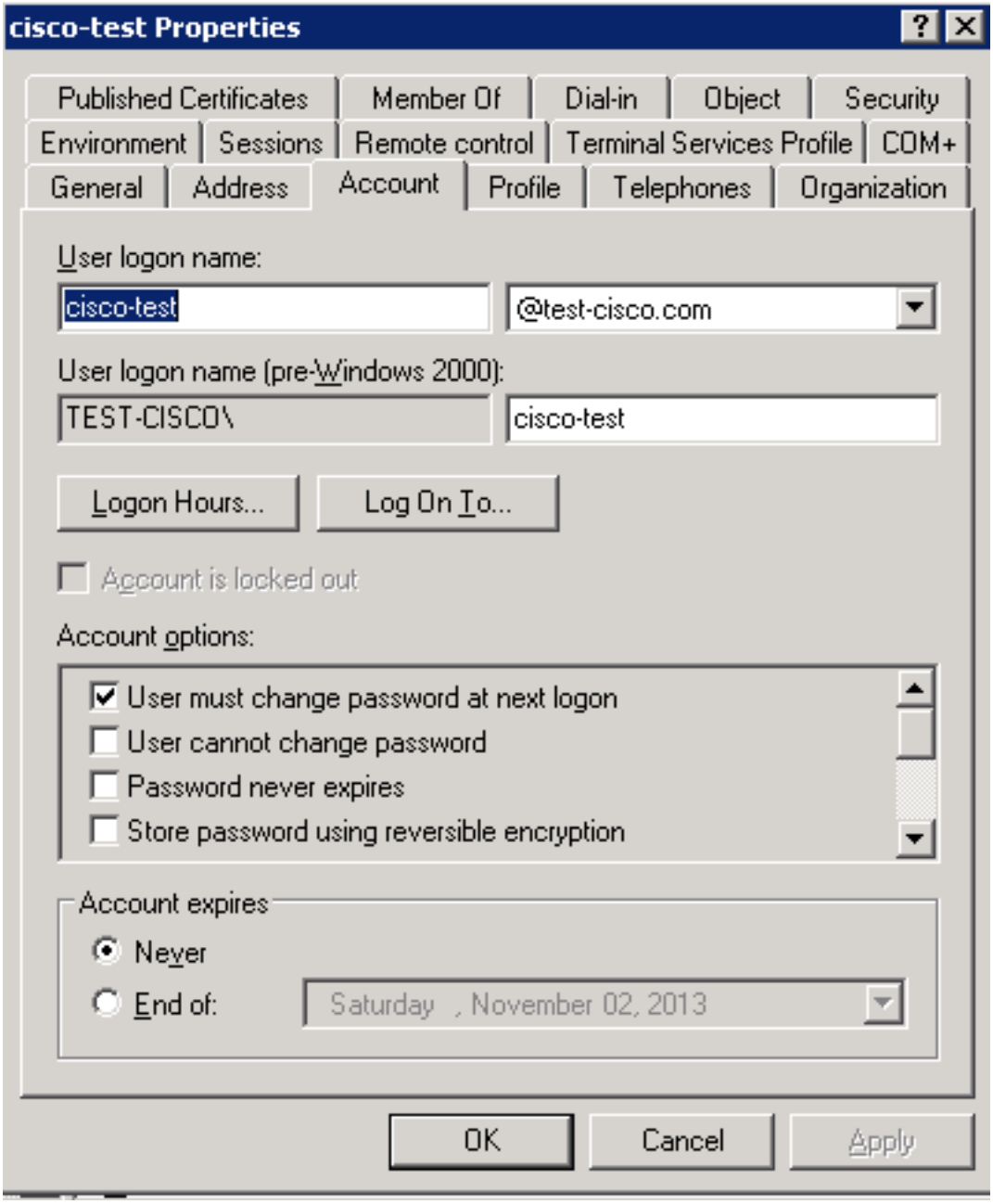
配置 LDAP 服务器:

```
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
```

将该配置用于隧道组和密码管理功能：

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

配置AD用户，以便需要更改密码：



当用户尝试使用Cisco VPN客户端时，ASA报告无效密码：

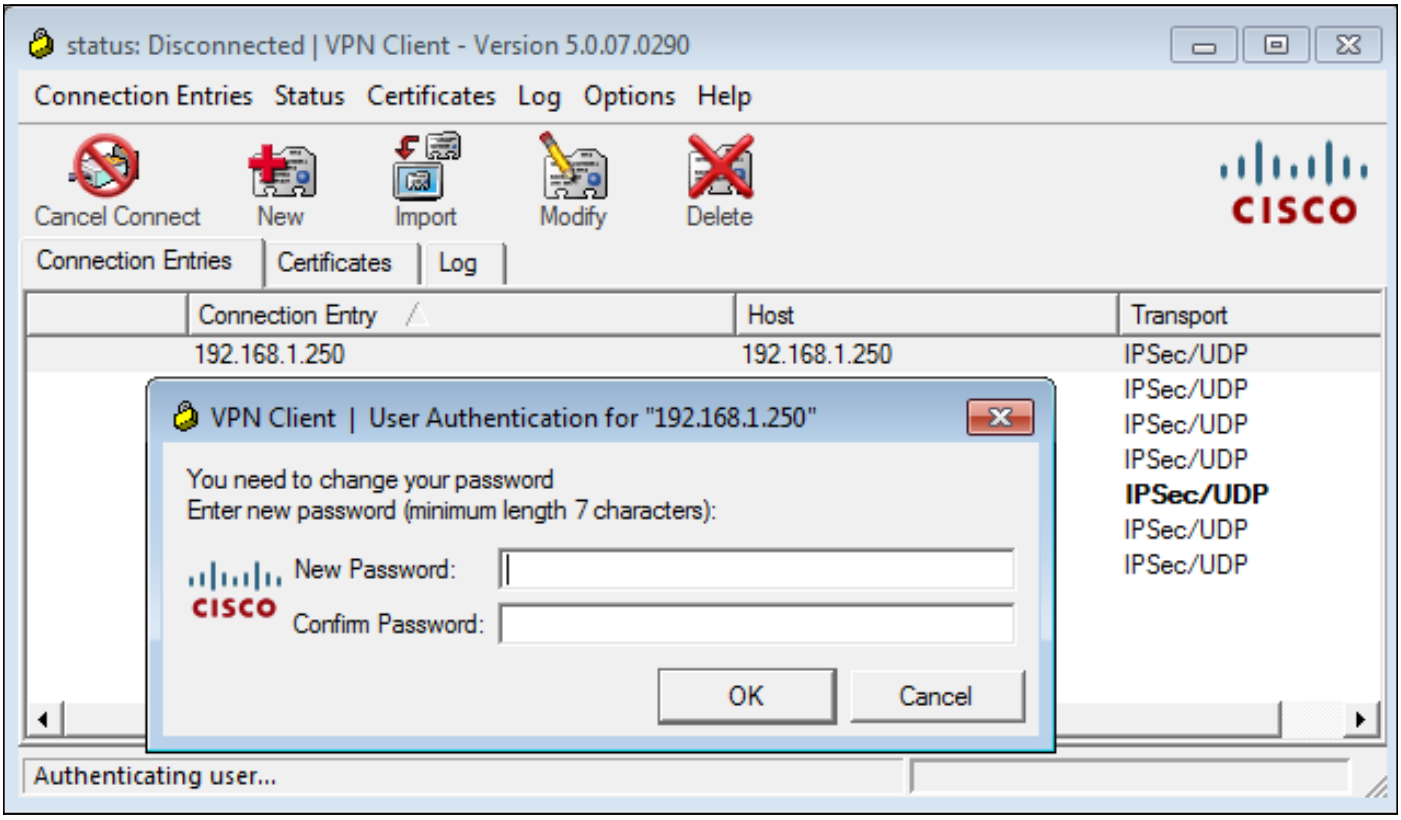
```
ASA(config-tunnel-general)# debug ldap 255
<some output ommited for clarity>

[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
```

如果凭证无效，则显示52e错误：

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

然后，Cisco VPN客户端要求更改密码：



此对话框与TACACS或RADIUS使用的对话框不同，因为它显示策略。在本例中，策略的最小密码长度为7个字符。

用户更改密码后，ASA可能会从LDAP服务器获取以下失败消息：

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

Microsoft策略要求使用安全套接字层(SSL)修改密码。更改配置：

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

用于SSL的Microsoft LDAP

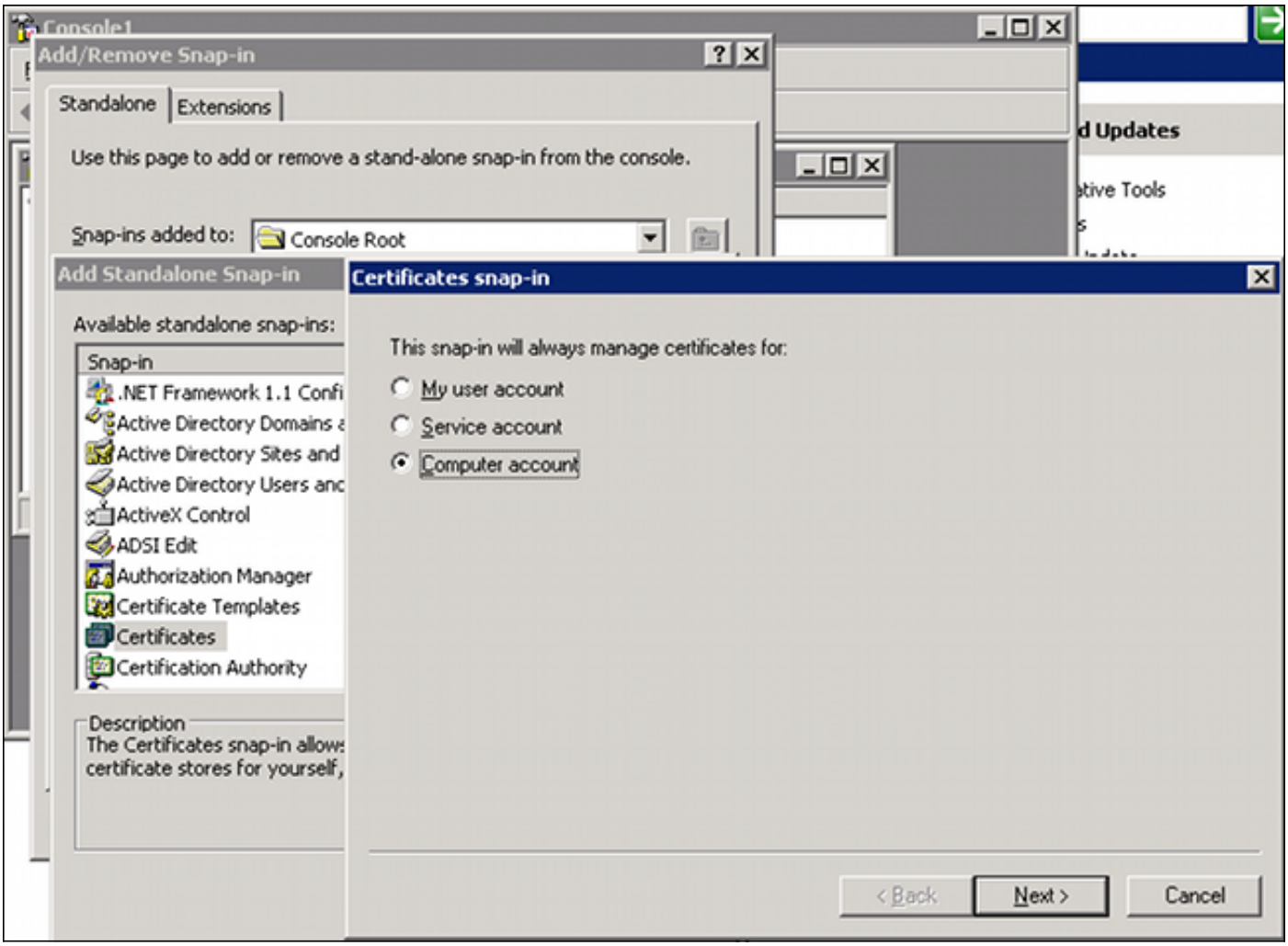
默认情况下，基于SSL的Microsoft LDAP不起作用。要启用此功能，您必须为具有正确密钥扩展名

的计算机帐户安装证书。有关详细信息，请参阅如何通过第三方证书颁发机构启用SSL上的LDAP。

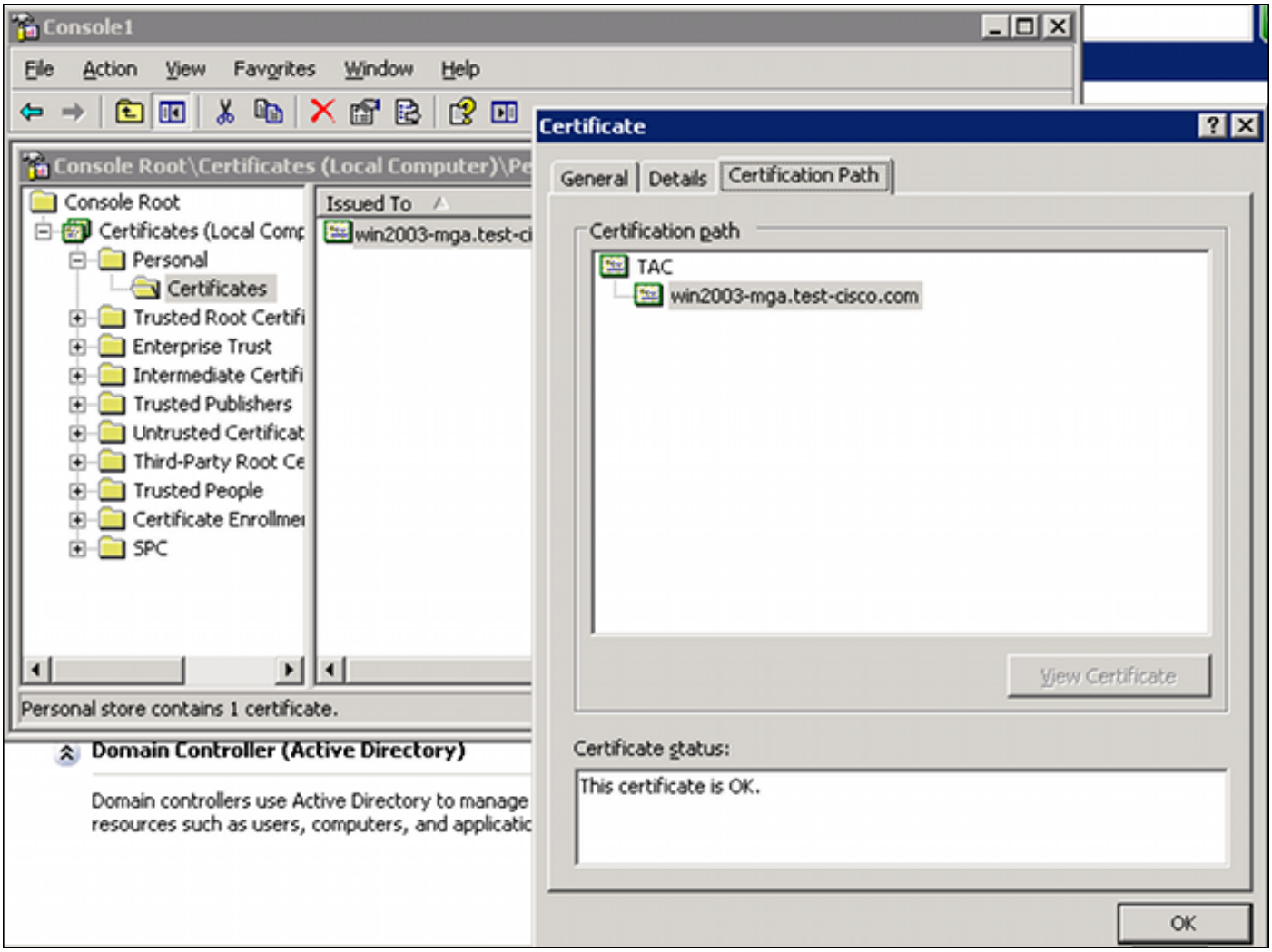
证书甚至可以是自签名证书，因为ASA不验证LDAP证书。有关相关增强请求，请参阅Cisco Bug ID CSCui40212，“Allow ASA to validate certificate from LDAPS server”。

注意：ACS验证5.5版及更高版本中的LDAP证书。

要安装证书，请打开mmc控制台，选择“添**加/删除管理单元”**，添加证书，然后选择“计算**机帐户**:



选择**Local computer**，将证书导入到个人存储，并将关联的证书颁发机构(CA)证书移到受信任存储。验证证书是否受信任：



ASA 8.4.2版中存在错误，当您尝试使用LDAP over SSL时，可能会返回此错误：

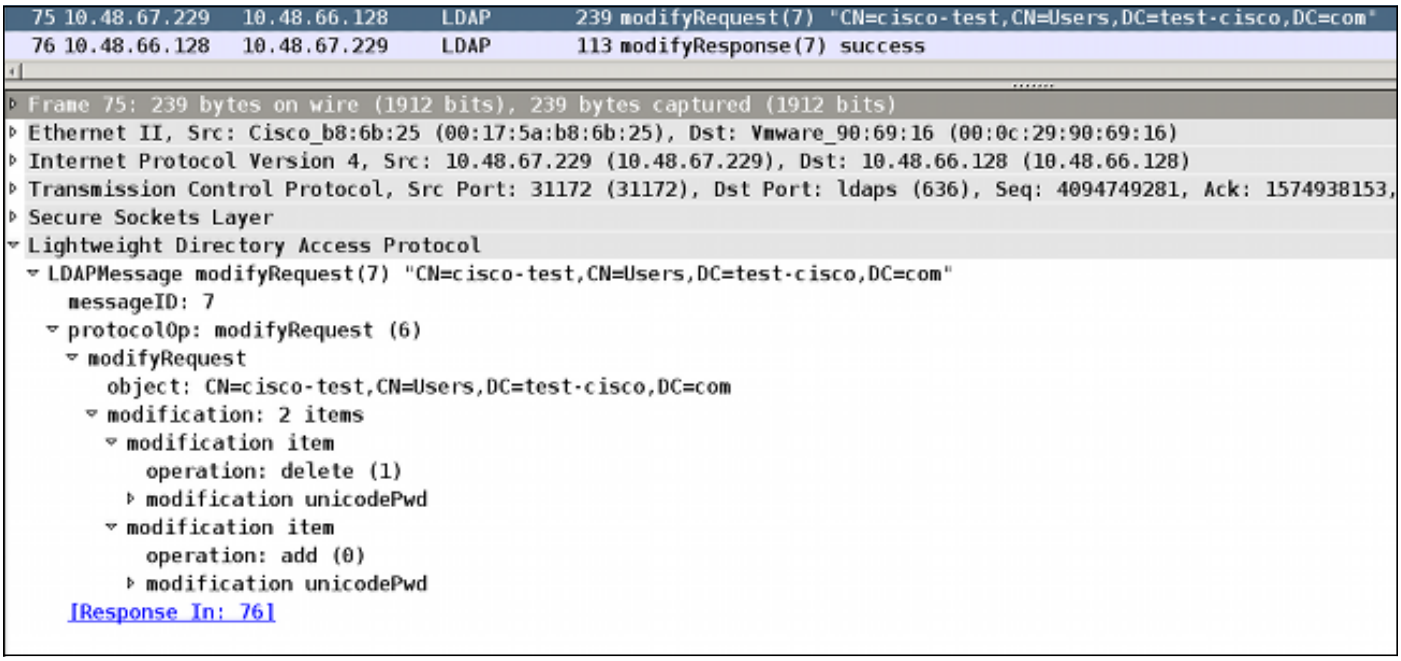
```
ASA(config)# debug ldap 255

[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。有两个LDAP会话。第一个会话返回代码为773（密码已过期）的故障，而第二个会话用于密码更改：

```
[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)
```

要验证密码更改，请查看数据包。LDAP服务器的私钥可由Wireshark用于解密SSL流量：



ASA上的互联网密钥交换(IKE)/身份验证、授权和记帐(AAA)调试与RADIUS身份验证场景中的调试非常相似。

LDAP和到期前警告

对于LDAP，您可以使用在密码到期前发送警告的功能。ASA在密码到期前90天使用以下设置警告用户：

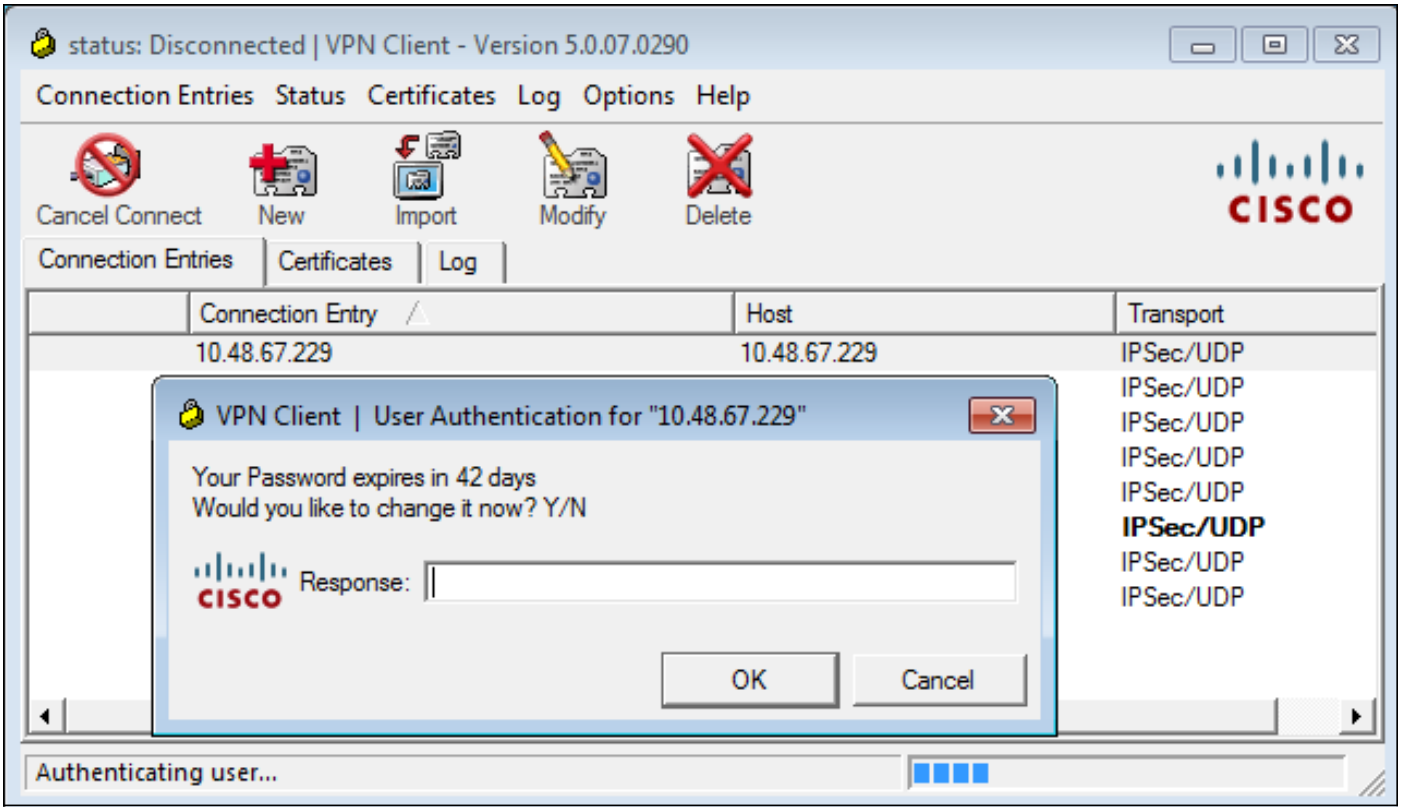
```
tunnel-group RA general-attributes
 password-management password-expire-in-days 90
```

此处密码将在42天后过期，用户尝试登录：

```
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发送警告，并提供密码更改选项：



如果用户选择更改密码，则会提示输入新密码，并开始正常的密码更改过程。

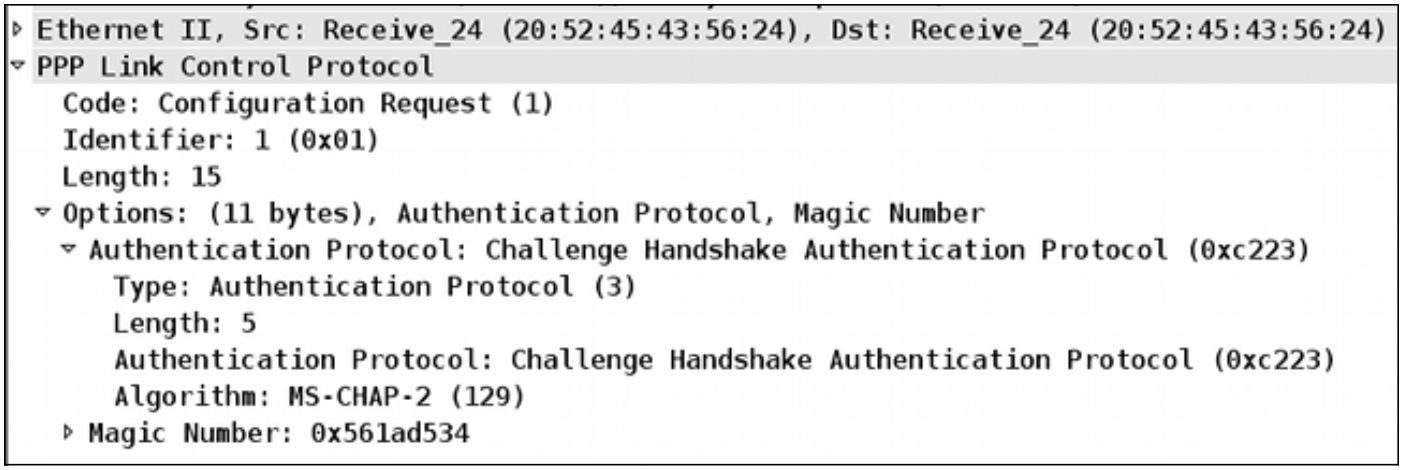
ASA和L2TP

以上示例提供IKE第1版(IKEv1)和IPSec VPN。

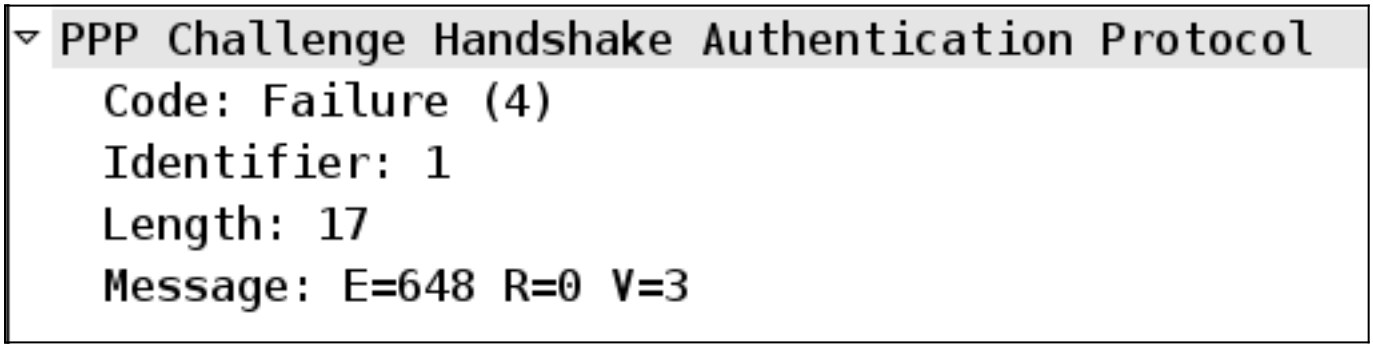
对于第2层隧道协议(L2TP)和IPSec，PPP用作身份验证的传输。要使密码更改生效，需要使用MSCHAPv2，而不是PAP:

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

对于PPP会话内L2TP中的扩展身份验证，MSCHAPv2是协商的：



当用户密码过期时，返回代码为648的故障：



然后需要更改密码。其余过程与使用MSCHAPv2的RADIUS场景非常相似。

有关如何配置L2TP的更多详细信息，请参阅Windows 2000/XP PC和PIX/ASA 7.2之间使用预共享密钥的L2TP over IPsec配置示例。

ASA SSL VPN客户端

以上示例涉及IKEv1和Cisco VPN客户端，即寿命终止(EOL)。

远程访问VPN的推荐解决方案是Cisco AnyConnect安全移动，它使用IKE第2版(IKEv2)和SSL协议。密码更改和到期功能对Cisco AnyConnect的作用与对Cisco VPN客户端的作用完全相同。

对于IKEv1，在第1.5阶段(Xauth/mode config)中，ASA和VPN客户端之间交换了密码更改和到期数据。

对于IKEv2，它类似；配置模式使用CFG_REQUEST/CFG_REPLY数据包。

对于SSL，数据处于控制数据报传输层安全(DTLS)会话中。

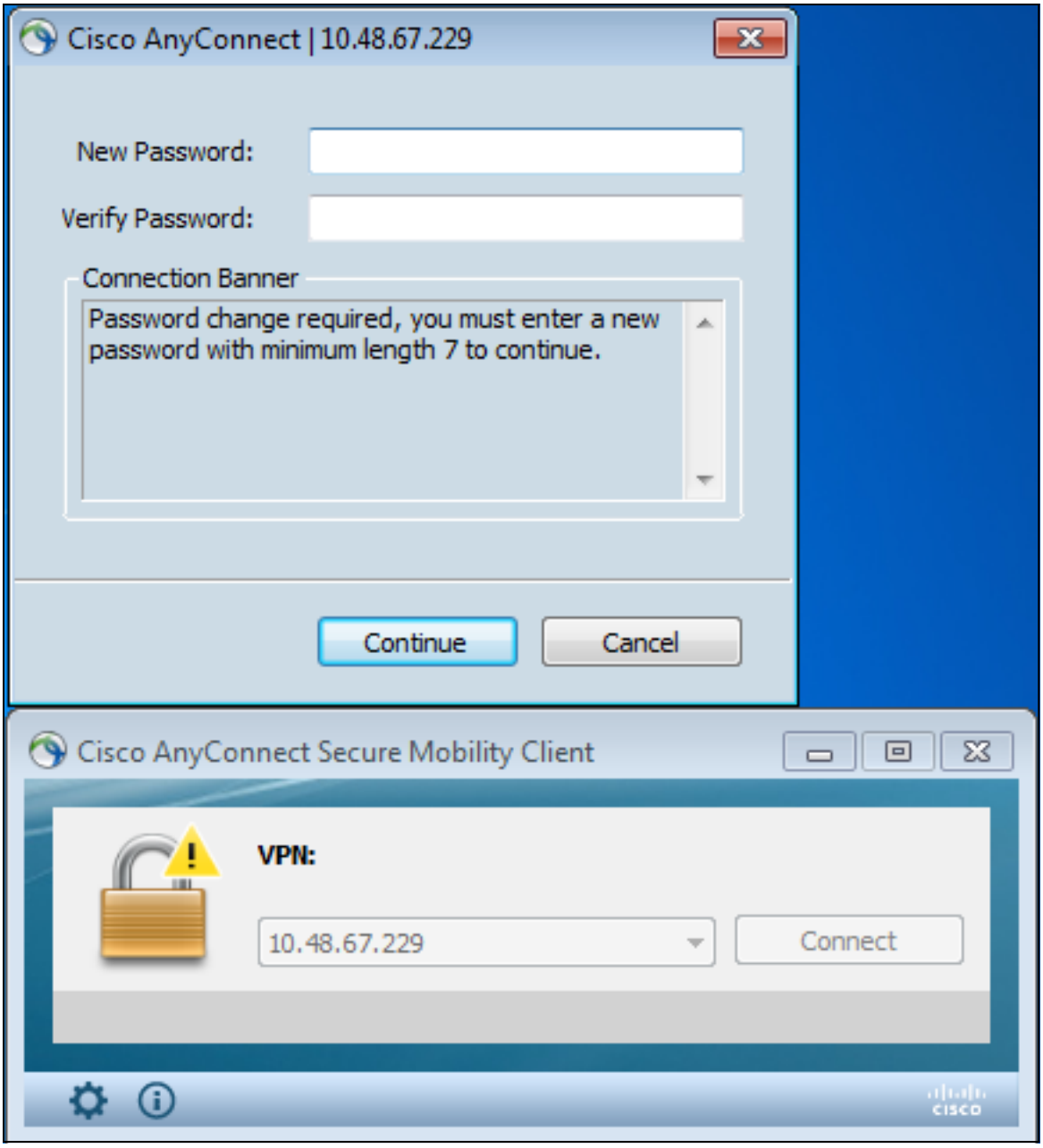
ASA的配置相同。

以下是使用Cisco AnyConnect和SSL协议通过SSL使用LDAP服务器的示例配置：

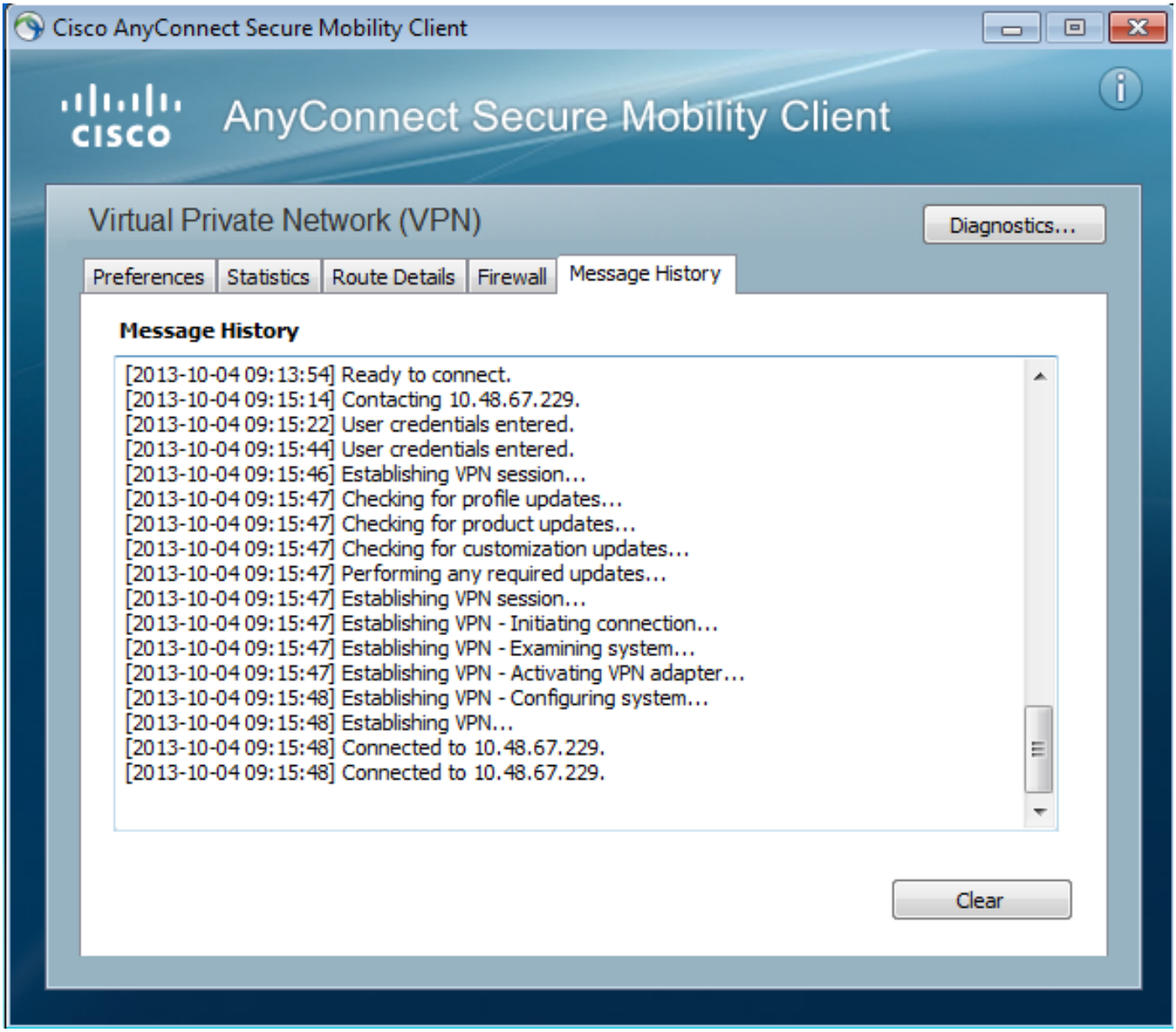
```
aaa-server LDAP protocol ldap
aaa-server LDAP (outside) host win2003-mga.test-cisco.com
 ldap-base-dn CN=Users,DC=test-cisco,DC=com
 ldap-scope subtree
```

```
 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
```

提供正确的密码（已过期）后，Cisco AnyConnect会尝试连接并要求输入新密码：



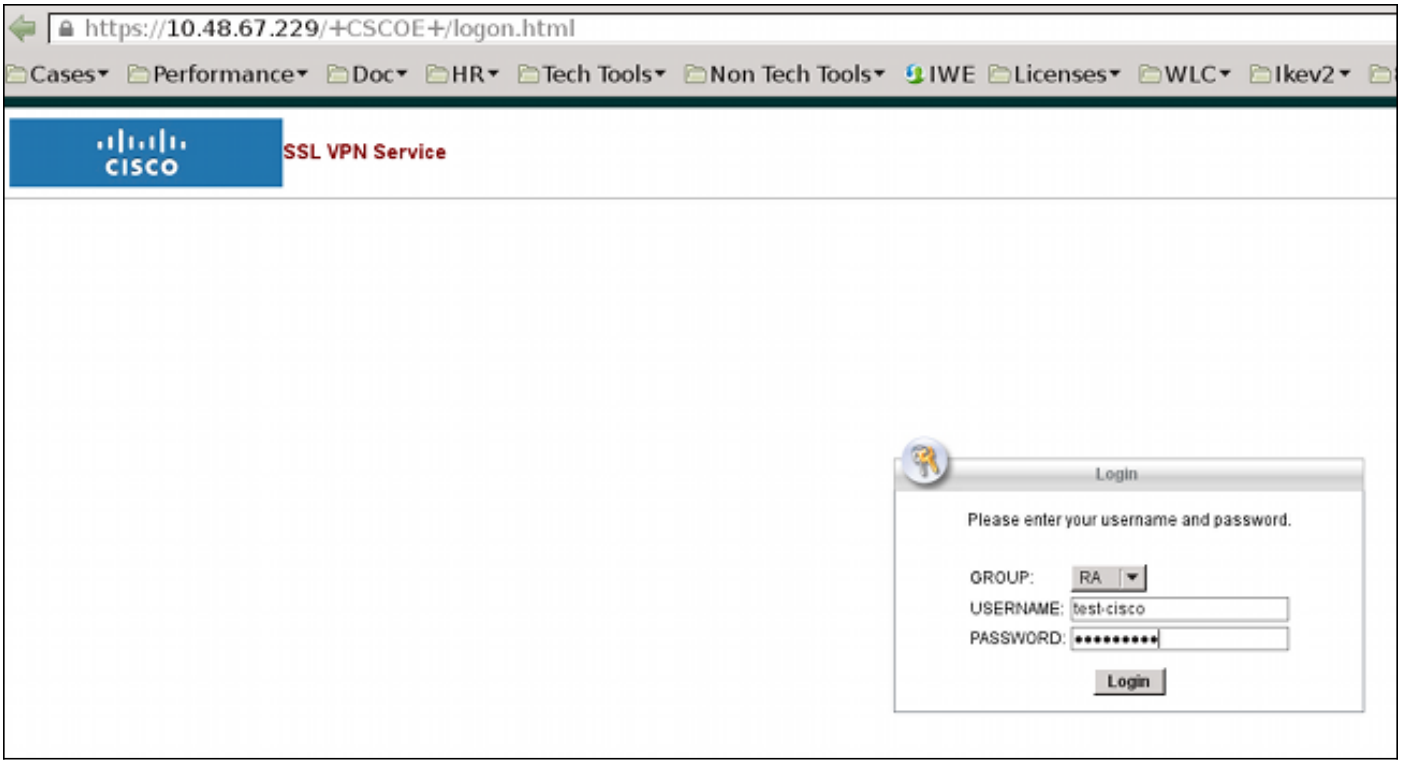
日志表明输入了两次用户凭证：



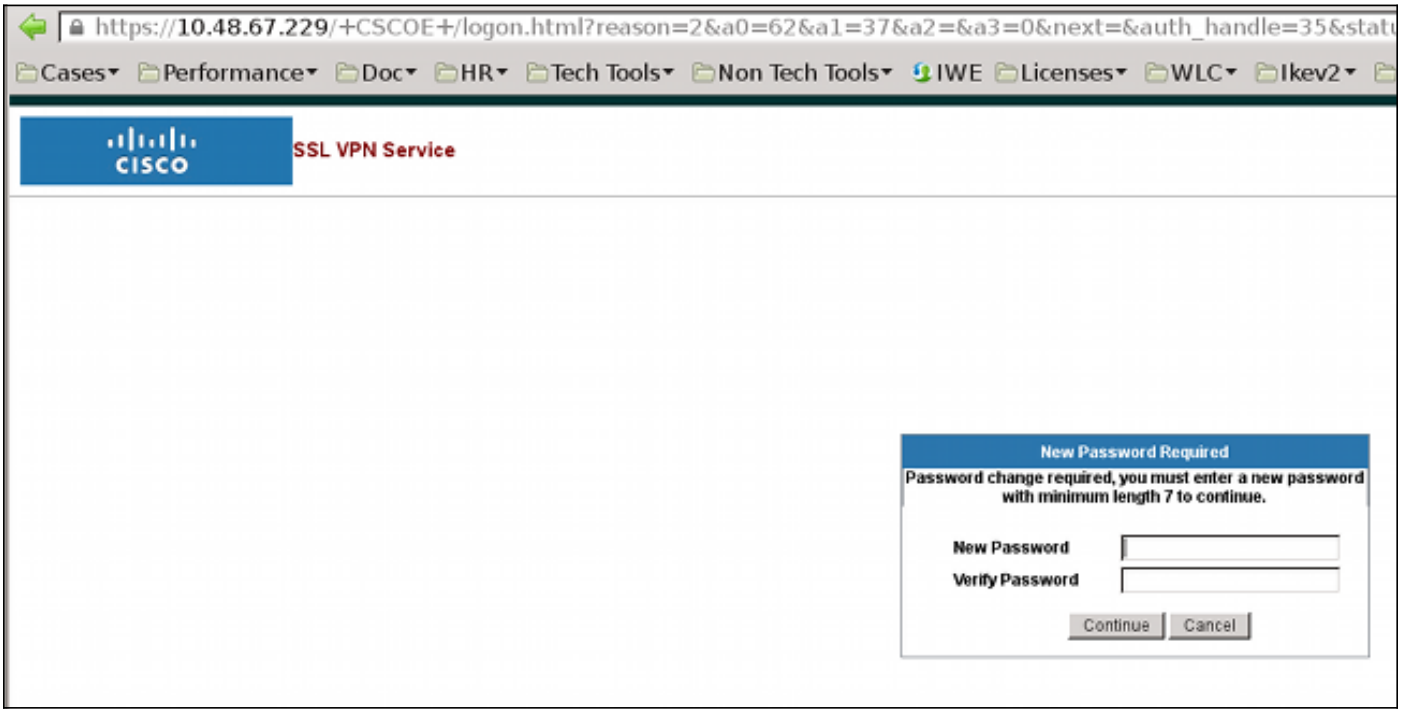
诊断AnyConnect报告工具(DART)中提供了更详细的日志。

ASA SSL Web门户

Web门户中会出现相同的登录过程：



密码到期和更改过程相同：



ACS用户更改密码

如果无法通过VPN更改密码，则可以使用ACS用户更改密码(UCP)专用Web服务。请参阅《思科安全访问控制系统5.4软件开发人员指南》：使用UCP Web服务。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 使用CLI、8.4和8.6的Cisco ASA 5500系列配置指南：为安全设备用户授权配置外部服务器
- 技术支持和文档 - Cisco Systems