ASA Remote Access VPN IKE/SSL − Password Expiry and Change for RADIUS, TACACS, and LDAP Configuration Example

TAC **Document ID: 116757**

Contributed by Michal Garcarz, Cisco TAC Engineer.
Nov 25, 2013

Contents

Introduction

This document describes the password expiry and password change features on a remote access VPN tunnel terminated on a Cisco Adaptive Security Appliance (ASA). The document covers:

- Different clients: Cisco VPN client and Cisco AnyConnect Secure Mobility
- Different protocols: TACACS, RADIUS, and Lightweight Directory Access Protocol (LDAP)
- Different stores on the Cisco Secure Access Control System (ACS): local and Active Directory (AD)

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of ASA configuration through the command−line interface (CLI)
- Basic knowledge of VPN configuration on an ASA
- Basic knowledge of the Cisco Secure ACS

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Adaptive Security Appliance, Version 8.4 and later
- Microsoft Windows Server 2003 SP1
- Cisco Secure Access Control System, Version 5.4 or later
- Cisco AnyConnect Secure Mobility, Version 3.1
- Cisco VPN Client, Release 5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Notes:

Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

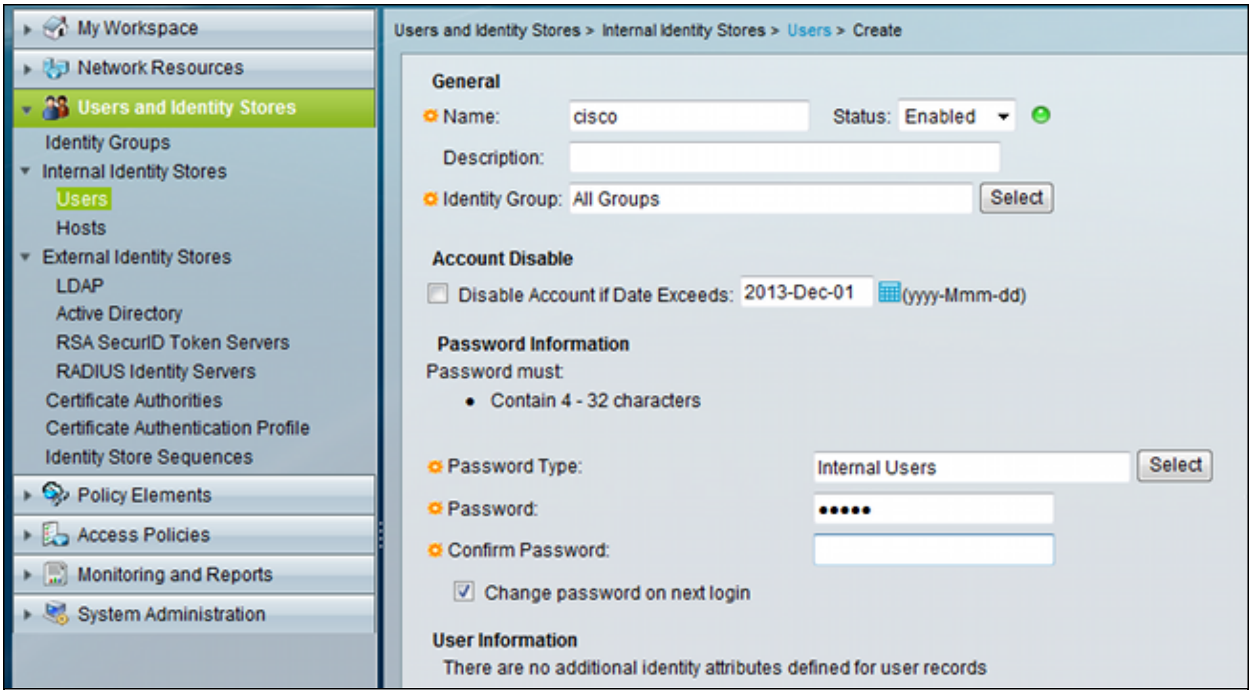
Refer to Important Information on Debug Commands before you use ***debug*** commands.

ASA with Local Authentication

An ASA with locally defined users does not allow use of password expiration or password change features. An external server, such as RADIUS, TACACS, LDAP, or Windows NT, is required.

ACS and Local Users

ACS supports both password expiry and password change for locally defined users. For example, you can force newly created users to change their password at their next login, or you can disable an account on a specific date:



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

General

Name: cisco Status: Enabled

Description:

Identity Group: All Groups

Account Disable

□ Disable Account if Date Exceeds: 2013-Dec-01 (yyyy-Mmm-dd)

Password Information

Password must:

- Contain 4 - 32 characters

Password Type: Internal Users

Password: •••••

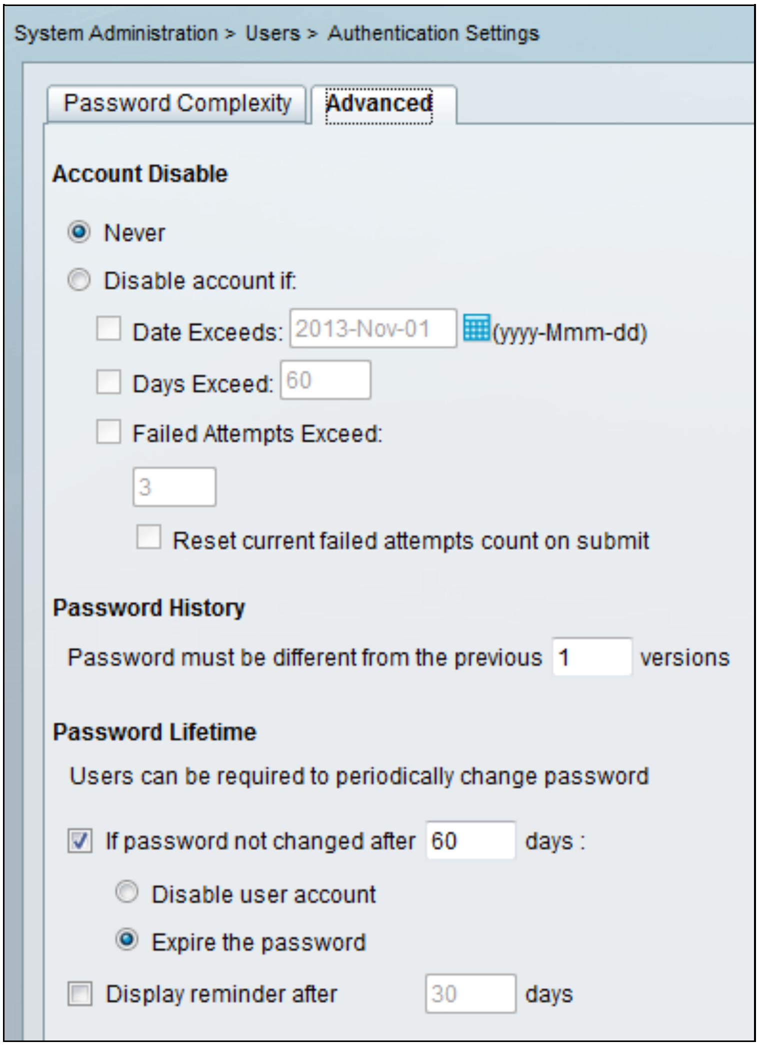
Confirm Password:

☑ Change password on next login

User Information

There are no additional identity attributes defined for user records

You can configure a password policy for all users. For example, after a password expires, you can disable the user account (block it without the ability to log in), or you can offer the option to change the password:



System Administration > Users > Authentication Settings

Account Disable

● Never

○ Disable account if:

□ Date Exceeds: 2013-Nov-01 (yyyy-Mmm-dd)

□ Days Exceed: 60

□ Failed Attempts Exceed:

3

□ Reset current failed attempts count on submit

Password History

Password must be different from the previous 1 versions

Password Lifetime

Users can be required to periodically change password

☑ If password not changed after 60 days :

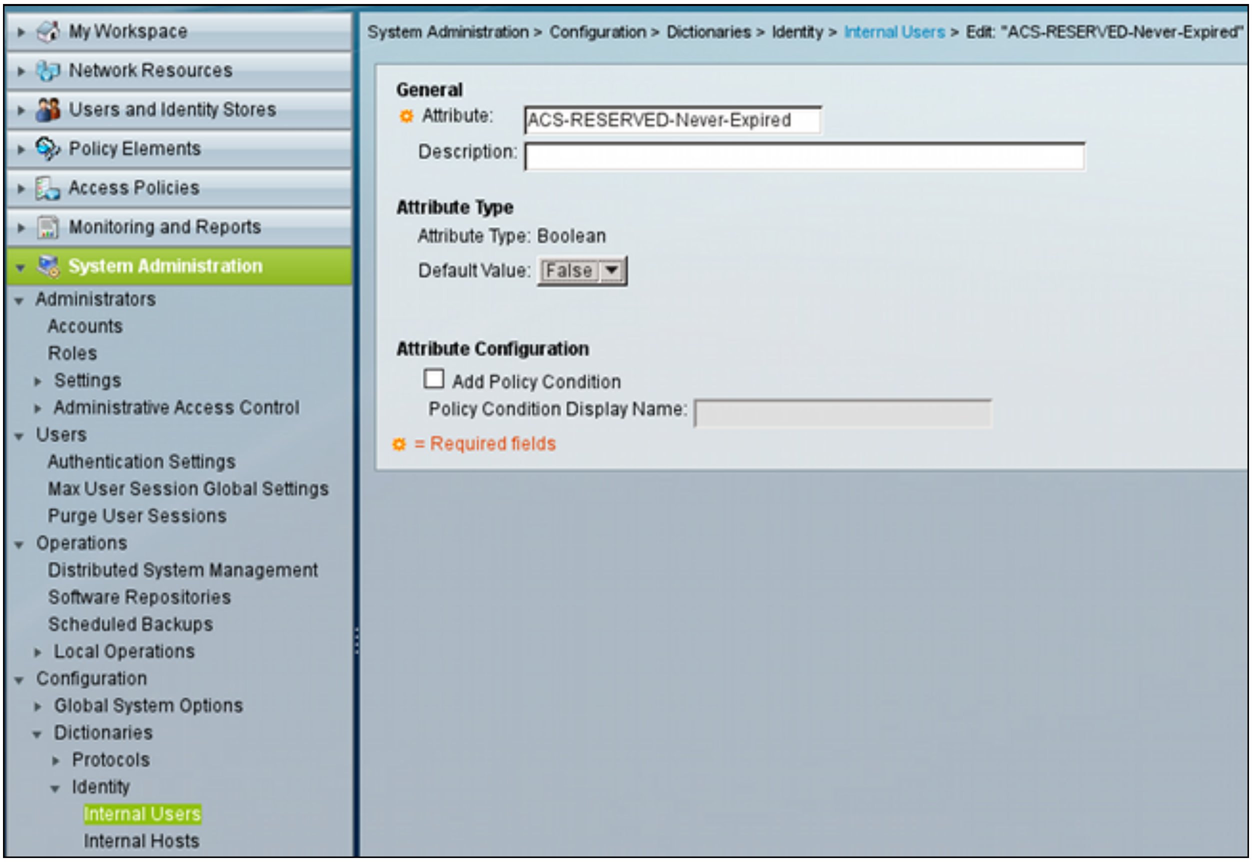
○ Disable user account

● Expire the password

□ Display reminder after 30 days

User−specific settings take precedence over global settings.

ACS−RESERVED−Never−Expired is an internal attribute for user identity.



General

✲ Attribute: ACS-RESERVED-Never-Expired

Description:

Attribute Type

Attribute Type: Boolean

Default Value: False

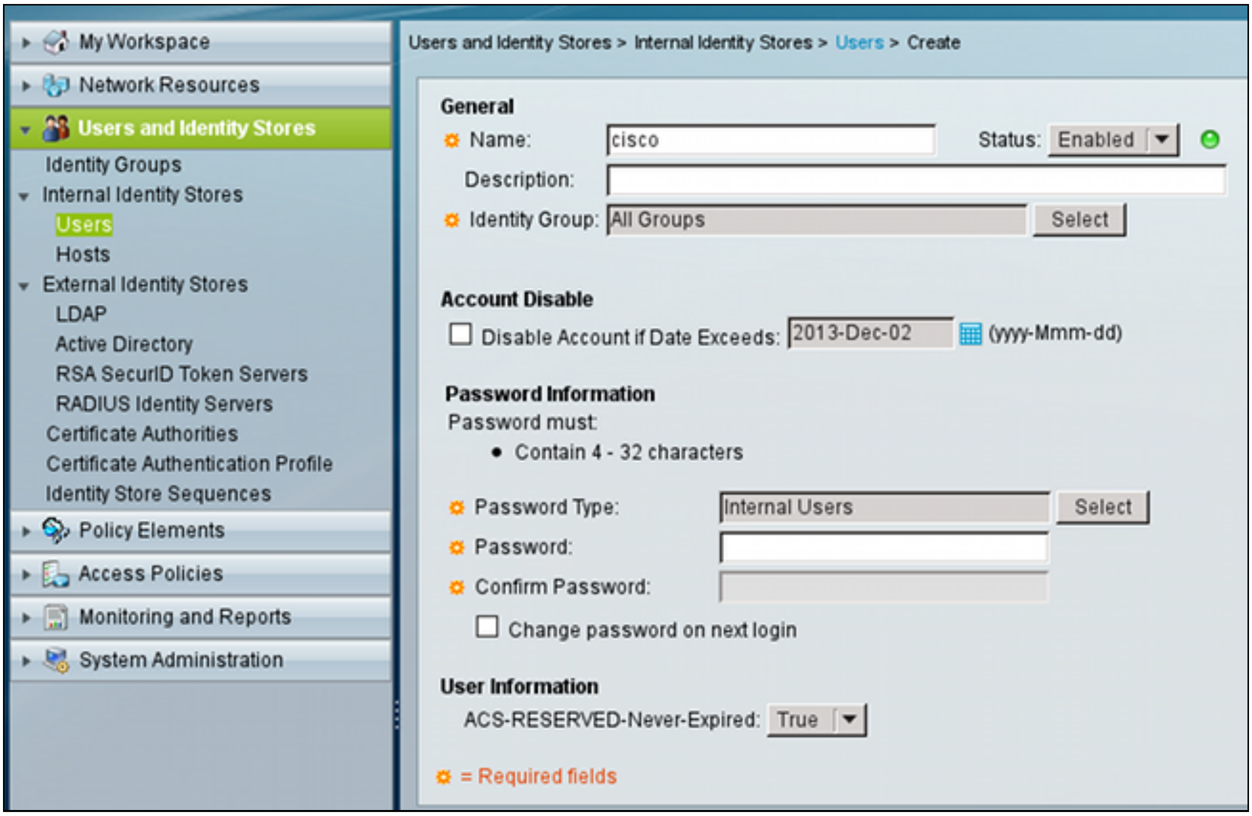
Attribute Configuration

□ Add Policy Condition

Policy Condition Display Name:

✲ = Required fields

This attribute is enabled by user and can be used in order to disable global account expiry settings. With this setting, an account is not disabled even if the global policy indicates it should be:



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

General

✲ Name: cisco   Status: Enabled ▾ ●

Description:

✲ Identity Group: All Groups

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

✲ Password:

✲ Confirm Password:

□ Change password on next login

User Information

ACS-RESERVED-Never-Expired: True ▾

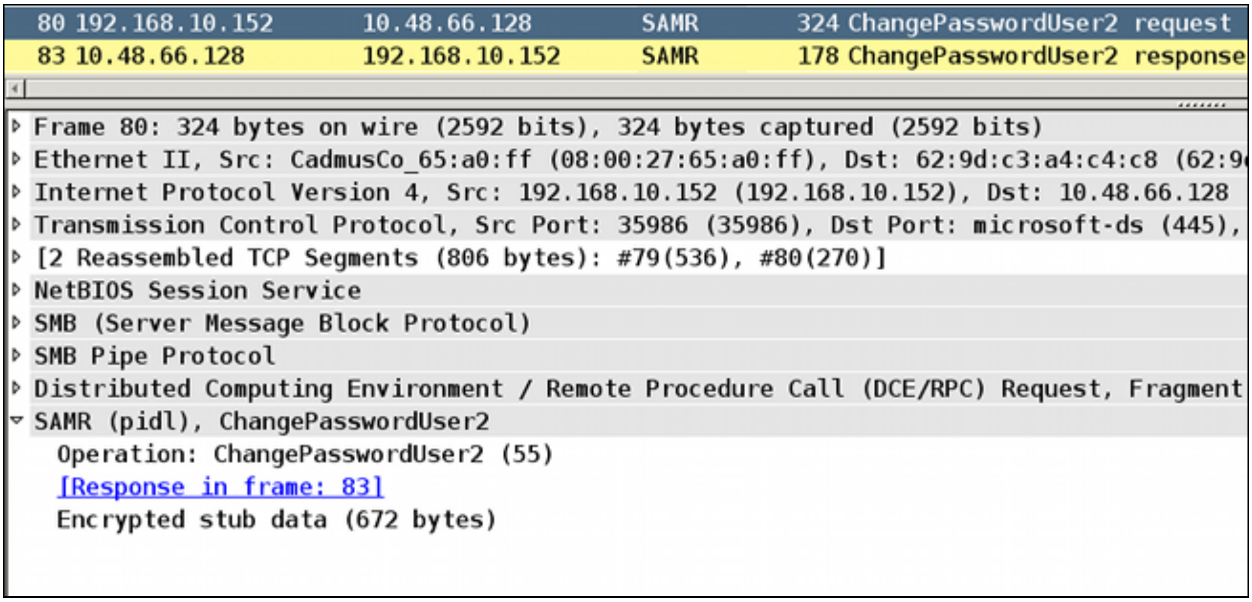
✲ = Required fields

ACS and Active Directory Users

ACS can be configured to check the users in an AD database. Password expiry and change is supported when Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2) is used; see User Guide for Cisco Secure Access Control System 5.4: Authentication in ACS 5.4: Authentication Protocol and Identity Store Compatibility for details.

On an ASA, you can use the password management feature, as described in the next section, in order to force the ASA to use MSCHAPv2.

ACS uses the Common Internet File System (CIFS) Distributed Computing Environment/Remote Procedure Call (DCE/RPC) call when it contacts the Domain Controller (DC) directory in order to change the password:



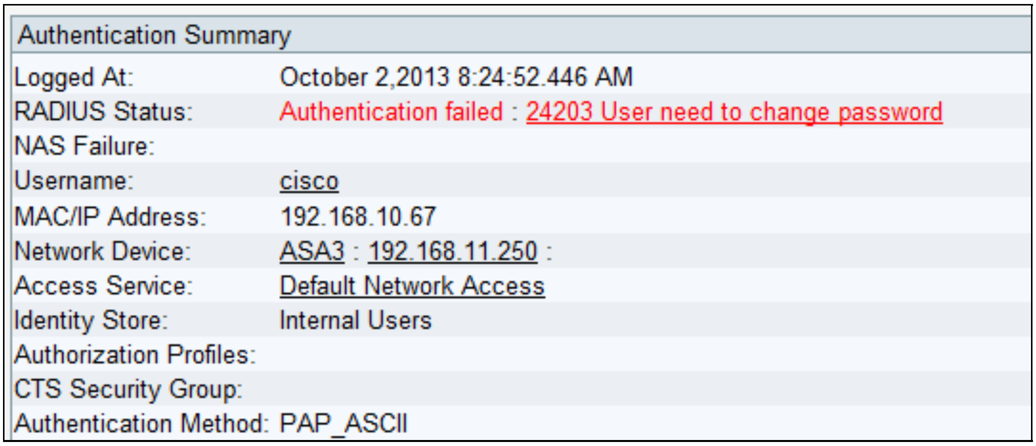
```
 80 192.168.10.152        10.48.66.128        SAMR      324 ChangePasswordUser2  request
 83 10.48.66.128          192.168.10.152      SAMR      178 ChangePasswordUser2  response

▷ 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 (62:9
▷ 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 can use both the RADIUS and TACACS+ protocols in order to contact with the ACS for an AD password change**.**

ASA with ACS via RADIUS

The RADIUS protocol does not natively support password expiry or password change. Typically, the Password Authentication Protocol (PAP) is used for RADIUS. The ASA sends the username and password in plain text, and the password is then encrypted through use of the RADIUS shared secret.

In a typical scenario when the user password has expired, ACS returns a Radius−Reject message to the ASA. ACS notices that:



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

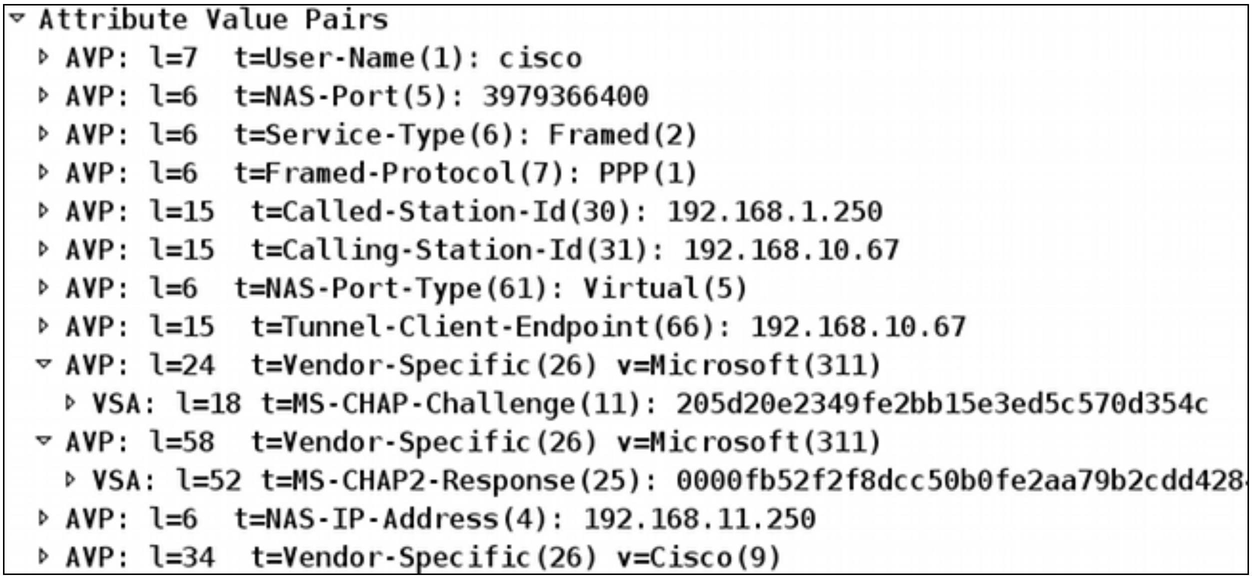
For the ASA, it is a simple Radius−Reject message, and authentication fails.

To solve this problem, the ASA allows use of the ***password−management*** command under the tunnel−group configuration:

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

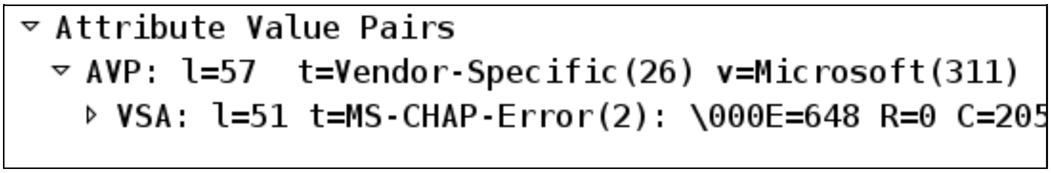
The ***password−management*** command changes the behavior so that the ASA is forced to use MSCHAPv2, rather than PAP, in the Radius−Request.

The MSCHAPv2 protocol supports password expiry and password change. So, if a VPN user has landed in that specific tunnel−group during the Xauth phase, the Radius−Request from ASA now includes an 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)
```

If ACS notices that the user needs to change the password, it returns a Radius−Reject message with MSCHAPv2 error 648.

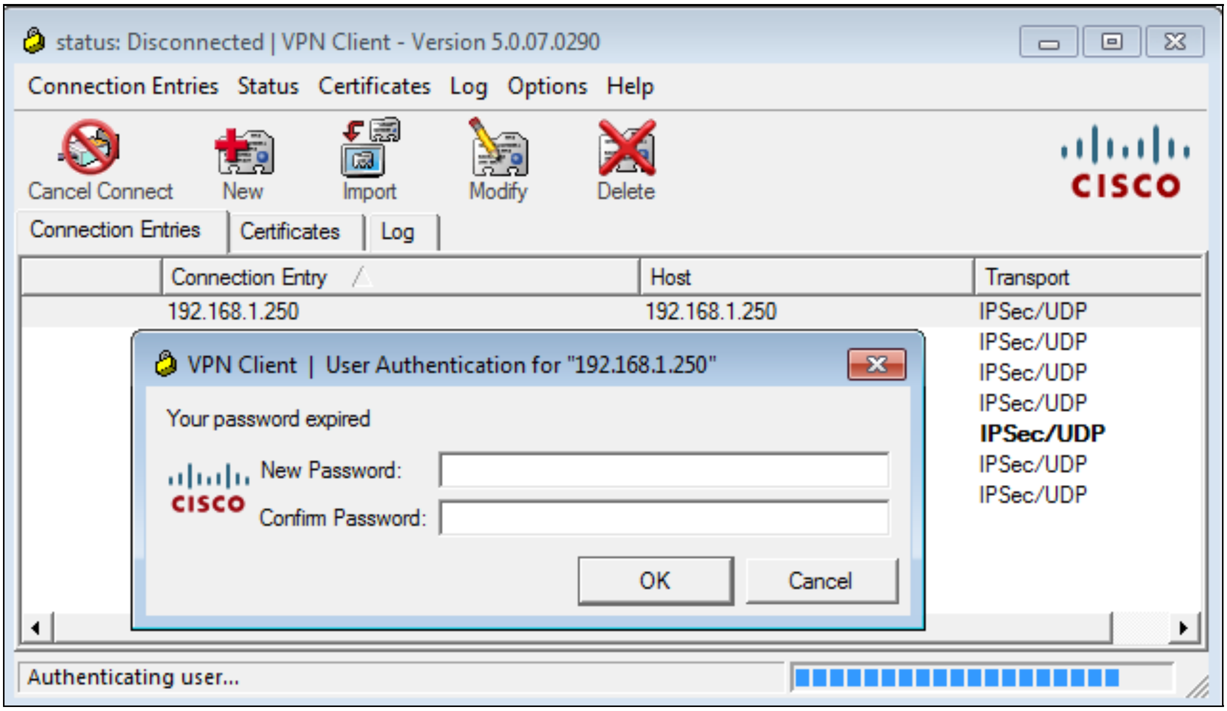


```
▽ Attribute Value Pairs
  ▽ AVP: l=57  t=Vendor-Specific(26) v=Microsoft(311)
    ▷ VSA: l=51 t=MS-CHAP-Error(2): \000E=648 R=0 C=205
```

The ASA understands that message and uses MODE_CFG in order to request the new password from the Cisco VPN client:

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

The Cisco VPN client presents a dialog box that prompts for a new password:



Connection Entry	Host	Transport
192.168.1.250	192.168.1.250	IPSec/UDP
		IPSec/UDP
		IPSec/UDP
		IPSec/UDP
		IPSec/UDP
		IPSec/UDP
		IPSec/UDP

VPN Client | User Authentication for "192.168.1.250"

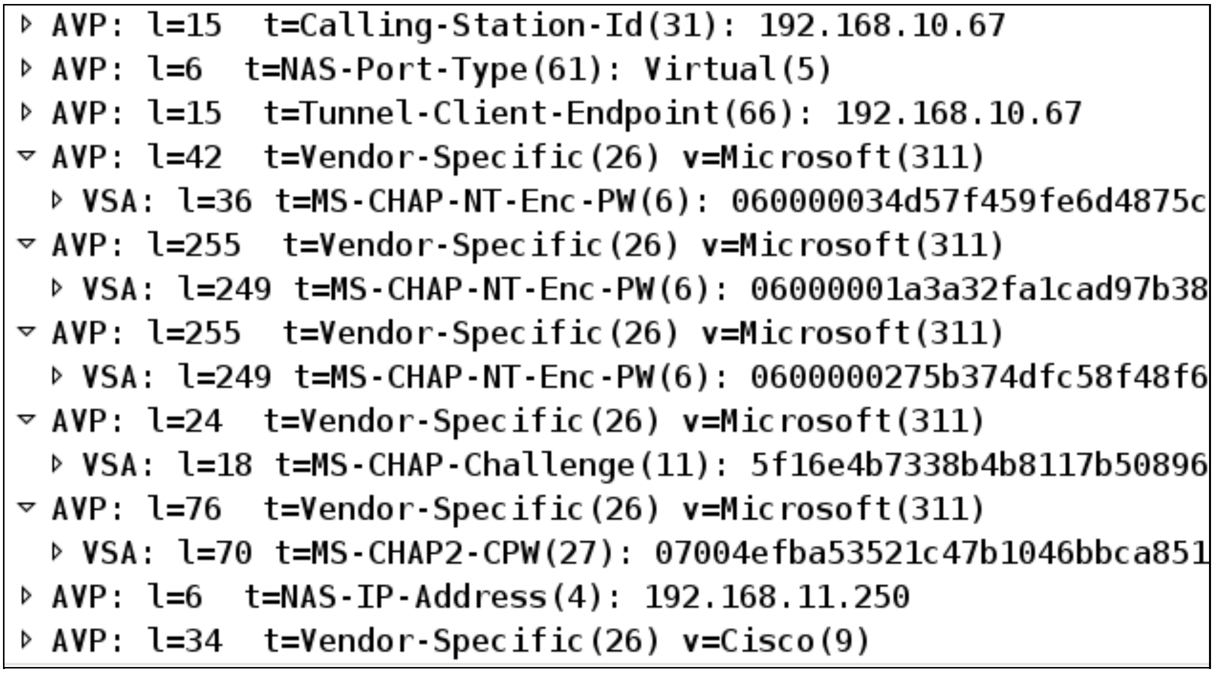
Your password expired

New Password:

Confirm Password:

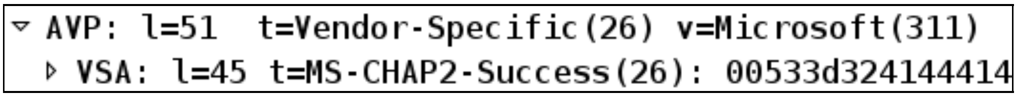
Authenticating user...

The ASA sends another Radius−Request with an MS−CHAP−CPW and MS−CHAP−NT−Enc−PW payload (the new password):



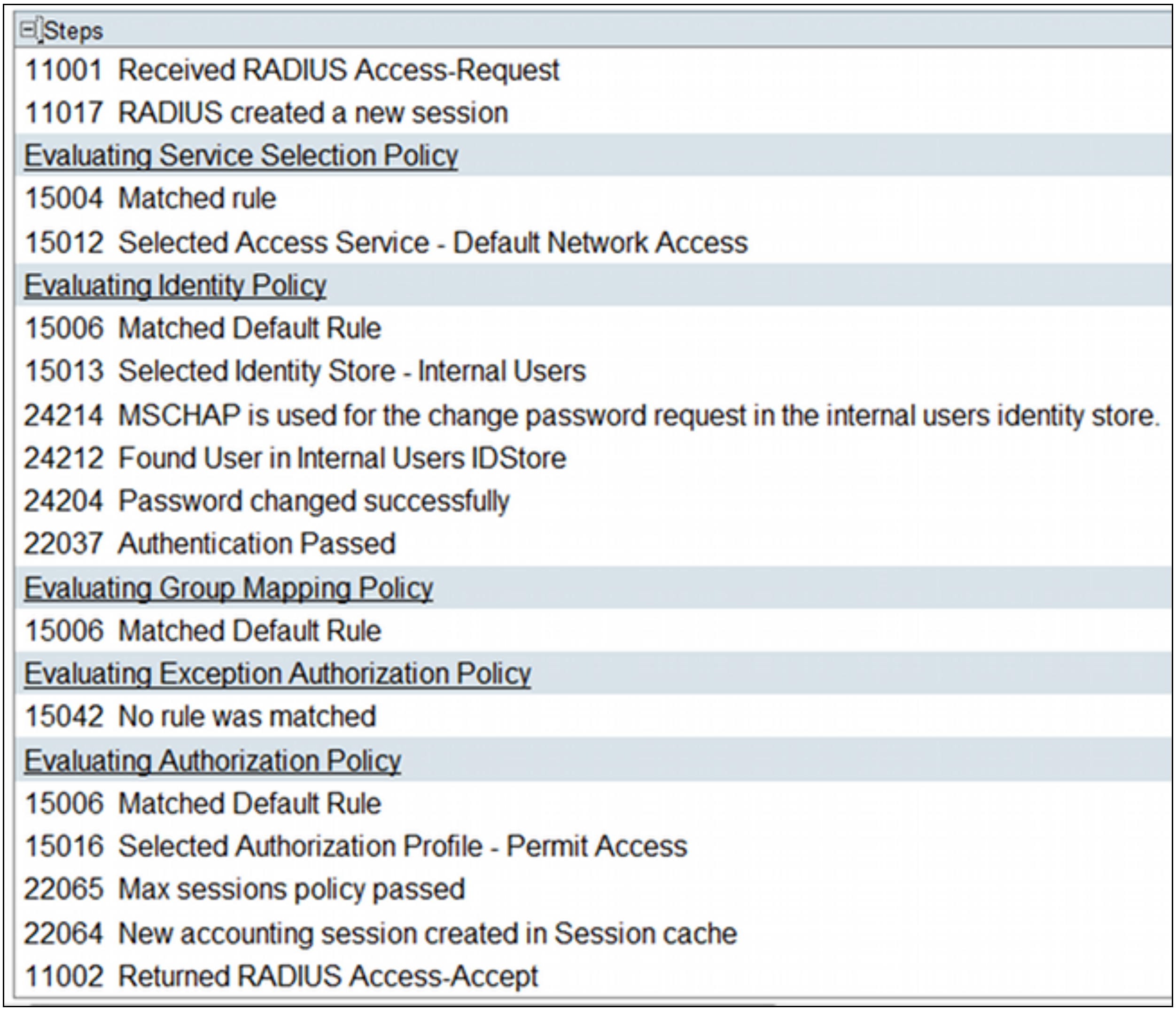
```
▷ AVP: l=15  t=Calling-Station-Id(31): 192.168.10.67
▷ AVP: l=6  t=NAS-Port-Type(61): Virtual(5)
▷ AVP: l=15  t=Tunnel-Client-Endpoint(66): 192.168.10.67
▽ AVP: l=42  t=Vendor-Specific(26) v=Microsoft(311)
  ▷ VSA: l=36 t=MS-CHAP-NT-Enc-PW(6): 060000034d57f459fe6d4875c
▽ AVP: l=255  t=Vendor-Specific(26) 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)
```

The ACS confirms the request and returns a 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
```

This can be verified on ACS, which reports a '24204 Password changed successfully':



```
Steps
11001  Received RADIUS Access-Request
11017  RADIUS created a new session
Evaluating Service Selection Policy
15004  Matched rule
15012  Selected Access Service - Default Network Access
Evaluating Identity Policy
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
Evaluating Group Mapping Policy
15006  Matched Default Rule
Evaluating Exception Authorization Policy
15042  No rule was matched
Evaluating Authorization Policy
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
```

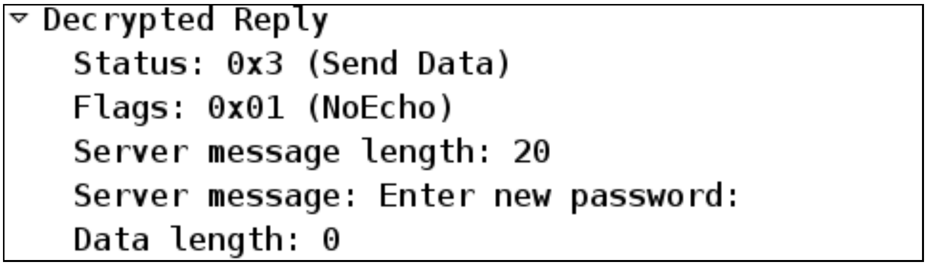
The ASA then reports successful authentication and continues with the Quick Mode (QM) process:

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

ASA with ACS via TACACS+

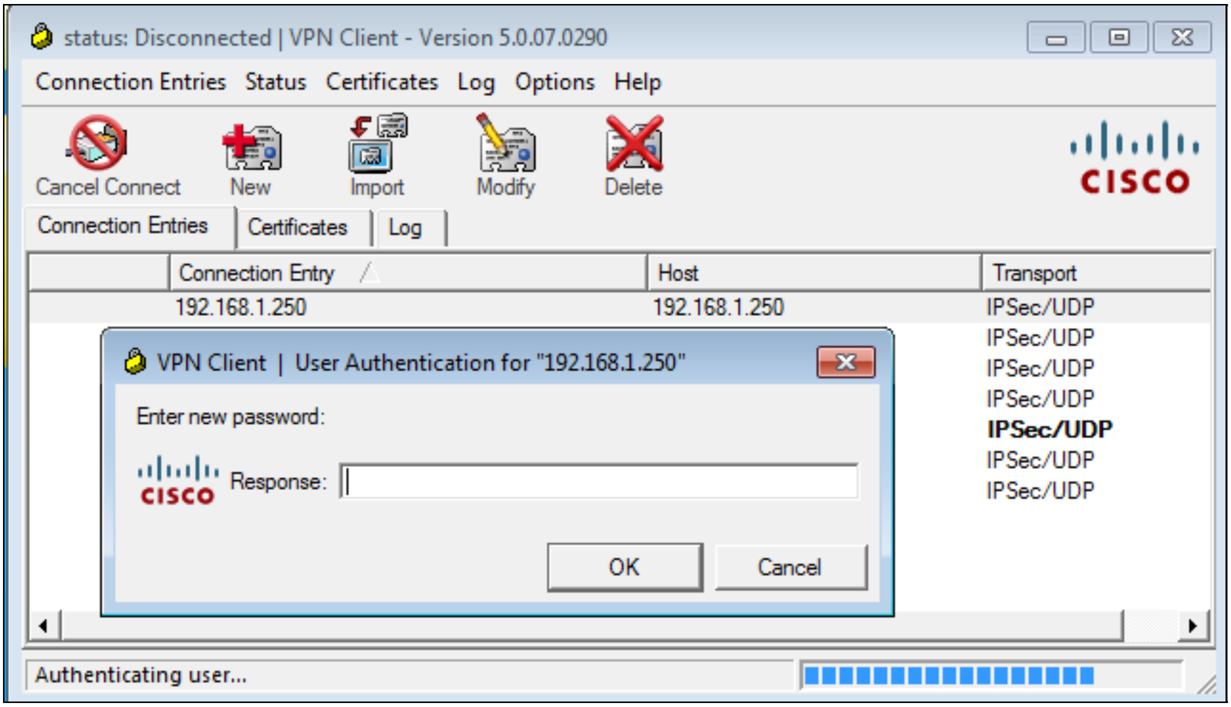
Similarly, TACACS+ can be used for password expiry and change. The password−management feature is not needed, because the ASA still uses TACACS+ with an authentication type of ASCII instead of MSCHAPv2.

Multiple packets are exchanged, and ACS asks for a new password:



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

The Cisco VPN client presents a dialog box (which differs from the dialog used by RADIUS) that prompts for a new password:



status: Disconnected | VPN Client - Version 5.0.07.0290

Connection Entry	Host	Transport
192.168.1.250	192.168.1.250	IPSec/UDP
		IPSec/UDP
		IPSec/UDP
		IPSec/UDP
		IPSec/UDP
		IPSec/UDP
		IPSec/UDP

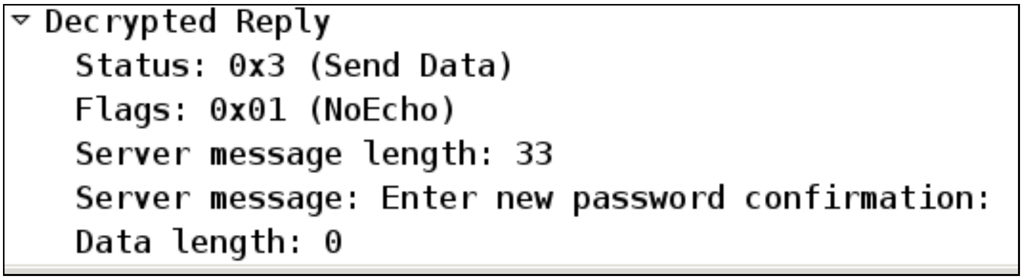
VPN Client | User Authentication for "192.168.1.250"

Enter new password:

Response:

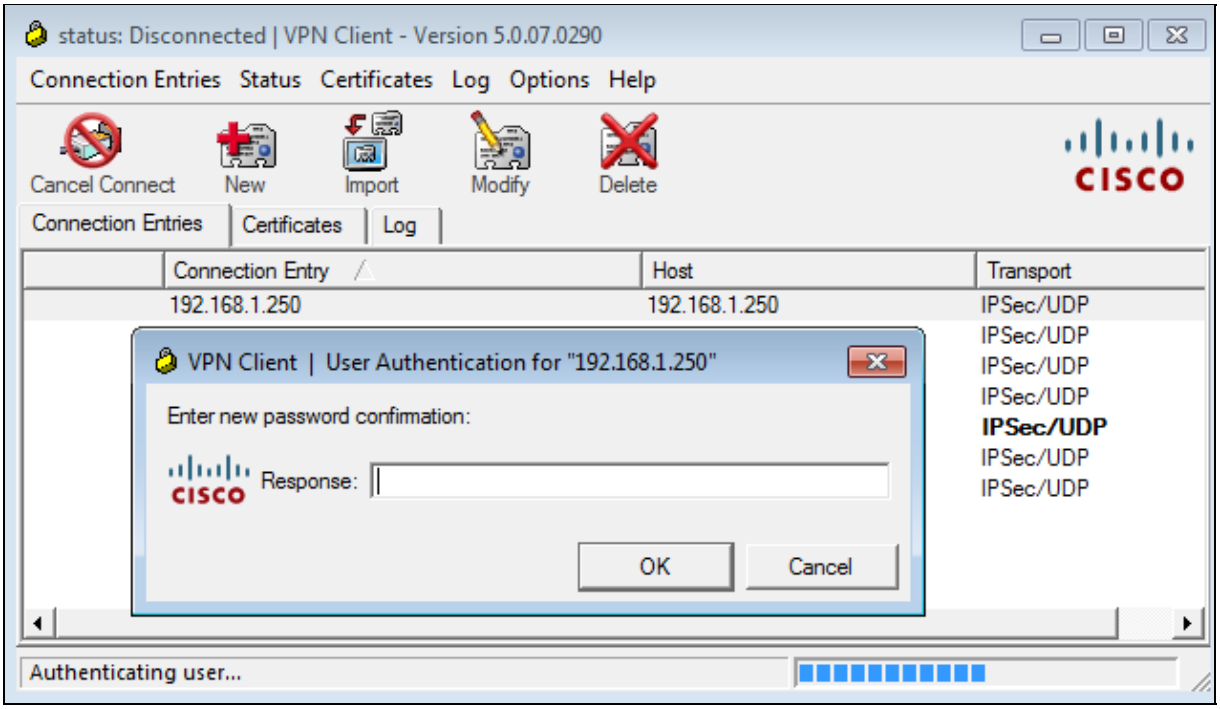
Authenticating user...

ACS requests confirmation of the new password:



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

The Cisco VPN client present a confirmation box:



status: Disconnected | VPN Client - Version 5.0.07.0290

Connection Entry	Host	Transport
192.168.1.250	192.168.1.250	IPSec/UDP
		IPSec/UDP
		IPSec/UDP
		IPSec/UDP
		IPSec/UDP
		IPSec/UDP
		IPSec/UDP

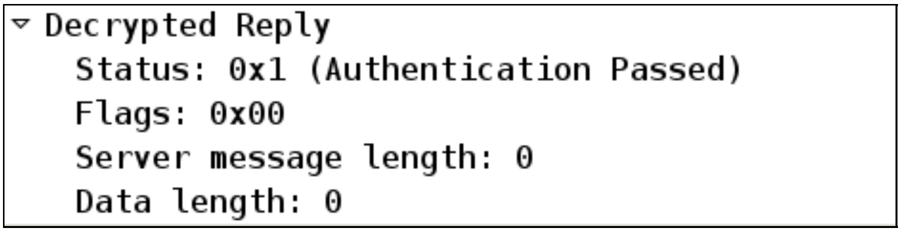
VPN Client | User Authentication for "192.168.1.250"

Enter new password confirmation:

Response:

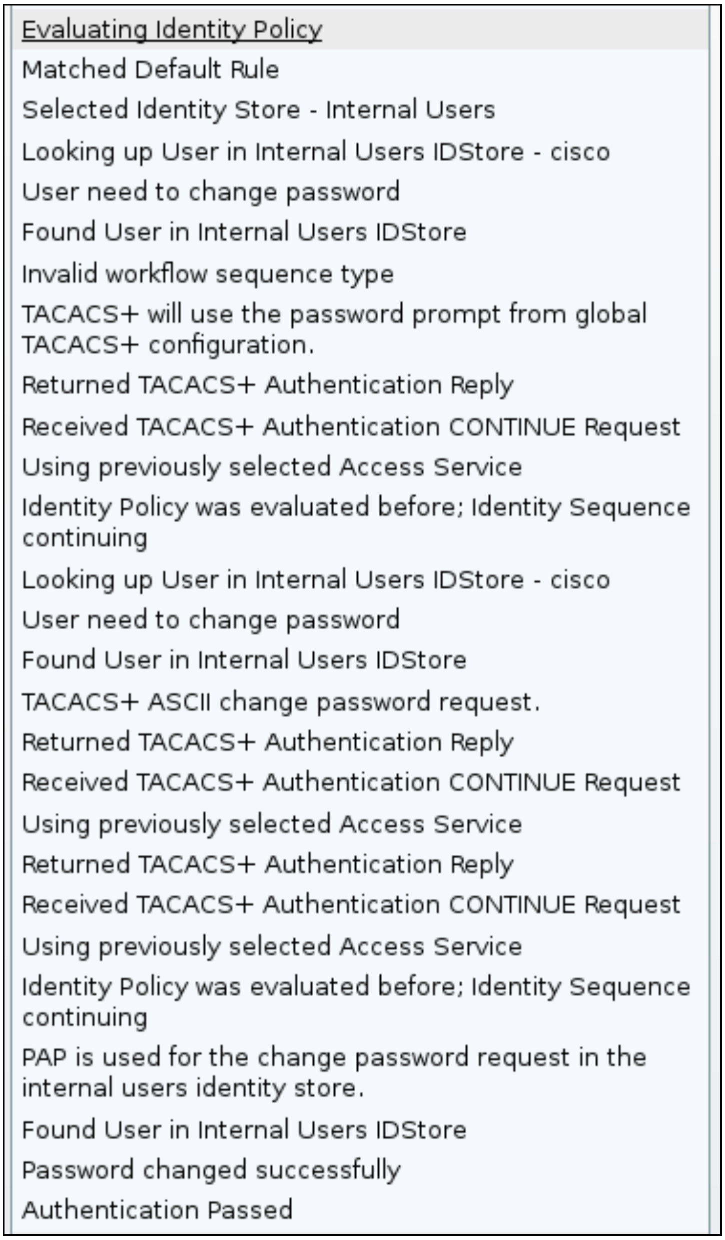
Authenticating user...

If the confirmation is correct, ACS reports a successful authentication:



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

ACS then logs an event that the password has been changed successfully:



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

The ASA debugs show the entire process of exchange and successful authentication:

```
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.
```

That password change is completely transparent for ASA. It is just a bit longer the TACACS+ session with more request and reply packets, which are parsed by the VPN client and presented to the user who is changing the password.

ASA with LDAP

Password expiry and change are fully supported by the Microsoft AD and Sun LDAP server schema.

For a password change, the servers return 'bindresponse = invalidCredentials' with 'error = 773.' This error indicates that the user must reset the password. Typical error codes include:

Error Code	Error
525	User not found
52e	Invalid credentials
530	Not permitted to logon at this time
531	Not permitted to logon at this workstation
532	Password expired
533	Account disabled
701	Account expired
773	User must reset password
775	User account locked

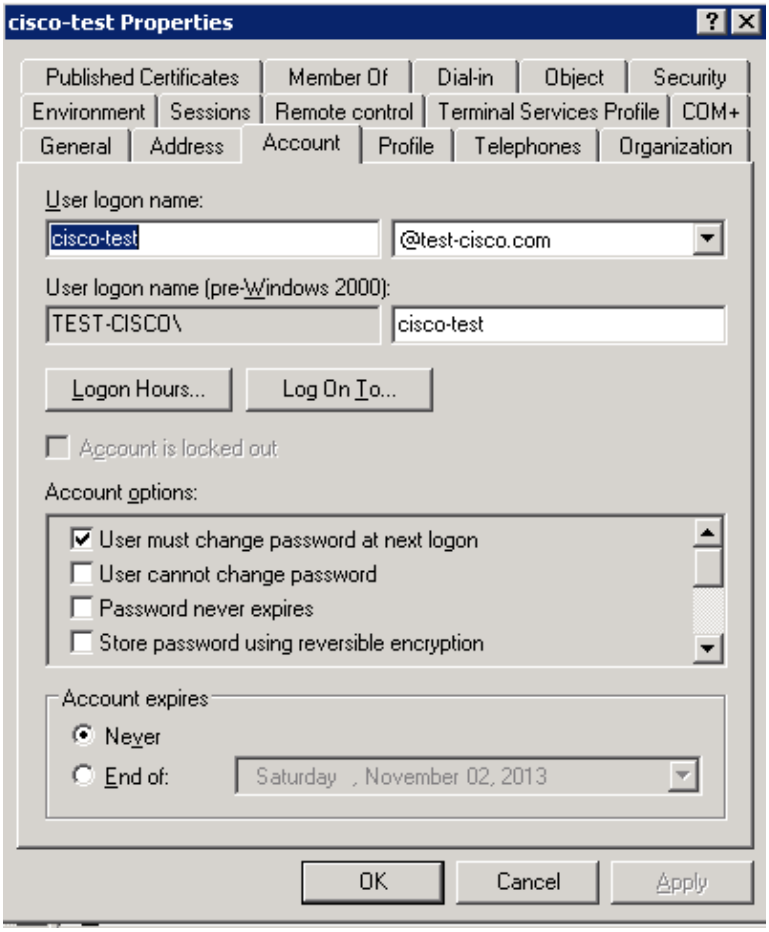
Configure the LDAP server:

```
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
```

Use that configuration for the tunnel−group and the password−management feature:

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

Configure the AD user so a password change is required:



User logon name: cisco-test @test-cisco.com

User logon name (pre-Windows 2000): TEST-CISCO\ cisco-test

□ Account is locked out

Account options:

☑ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Store password using reversible encryption

Account expires

● Never
○ End of: Saturday , November 02, 2013

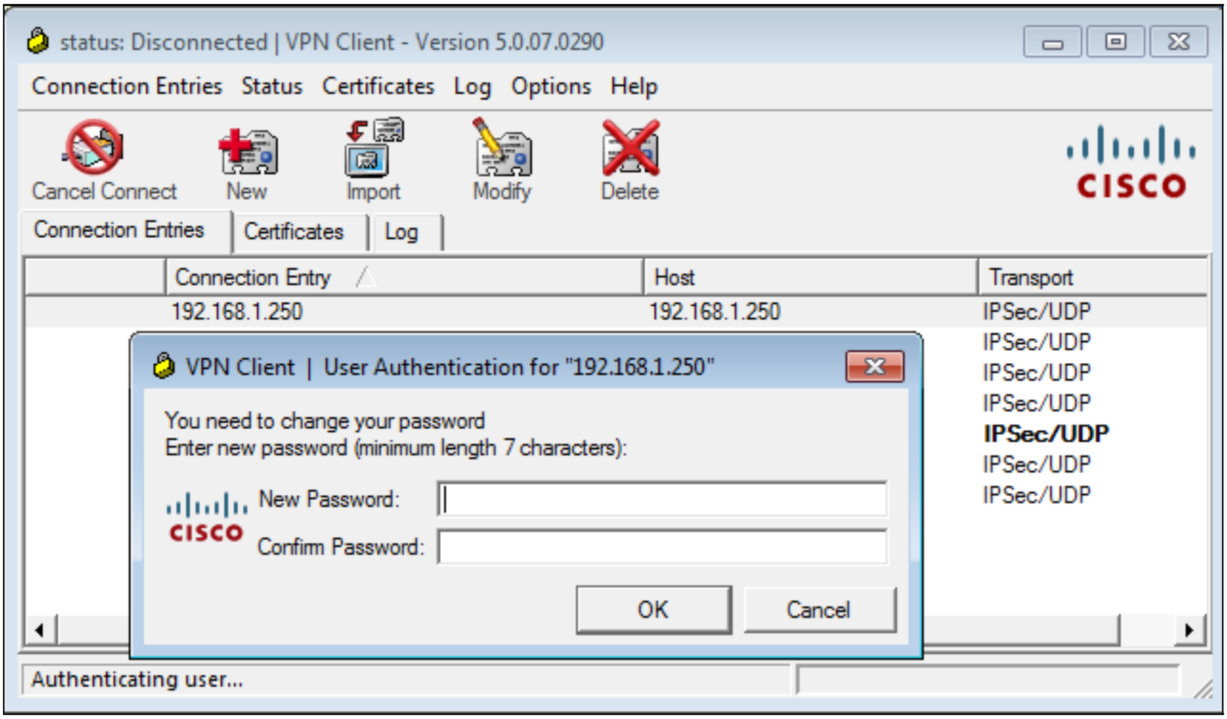
When the user tries to use the Cisco VPN client, the ASA reports an invalid password:

```
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
```

If the credentials are invalid, the 52e error appears:

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

The Cisco VPN client then asks for a password change:



	Connection Entry	Host	Transport
	192.168.1.250	192.168.1.250	IPSec/UDP
			IPSec/UDP
			IPSec/UDP
			IPSec/UDP
			IPSec/UDP
			IPSec/UDP
			IPSec/UDP

You need to change your password
Enter new password (minimum length 7 characters):

New Password:

Confirm Password:

Authenticating user...

This dialog box differs from the dialog used by TACACS or RADIUS because it displays the policy. In this example, the policy is a minimum password length of seven characters.

Once the user changes the password, the ASA might get this failure message from the LDAP server:

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

Microsoft policy requires use of the Secure Sockets Layer (SSL) for password modification. Change the configuration:

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

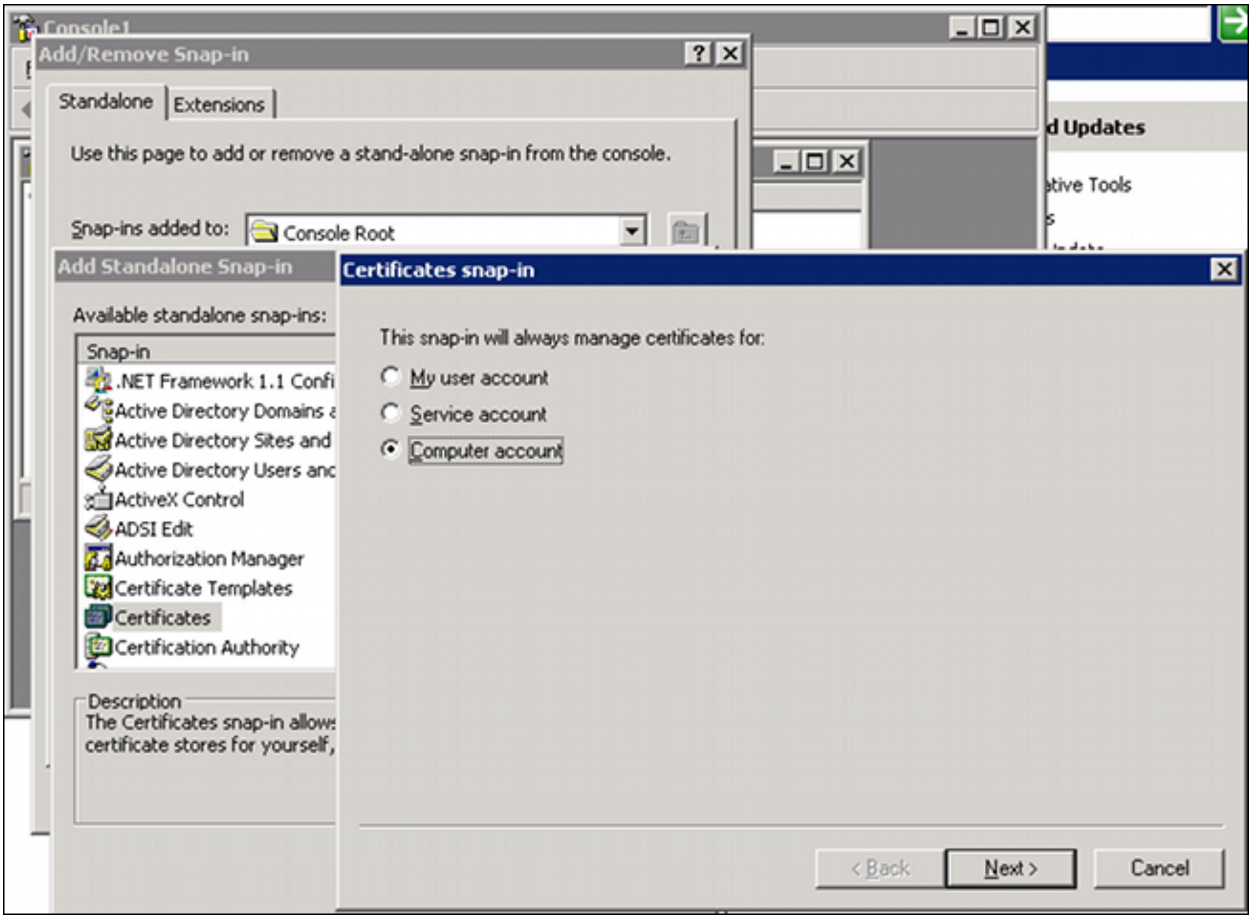
Microsoft LDAP for SSL

By default, Microsoft LDAP over SSL does not work. In order to enable this function, you must install the certificate for the computer account with the correct key extension. See How to enable LDAP over SSL with a third−party certification authority for more details.

The certificate can even be a self−signed certificate because the ASA does not verify the LDAP certificate. See Cisco Bug ID CSCui40212, "Allow ASA to validate certificate from LDAPS server," for a related enhancement request.

Note: ACS verifies the LDAP certificate in Version 5.5 and later.

To install the certificate, open the mmc console, select ***Add/Remove Snap−in***, add the certificate, and choose ***Computer account***:



Use this page to add or remove a stand-alone snap-in from the console.

Snap-ins added to: Console Root

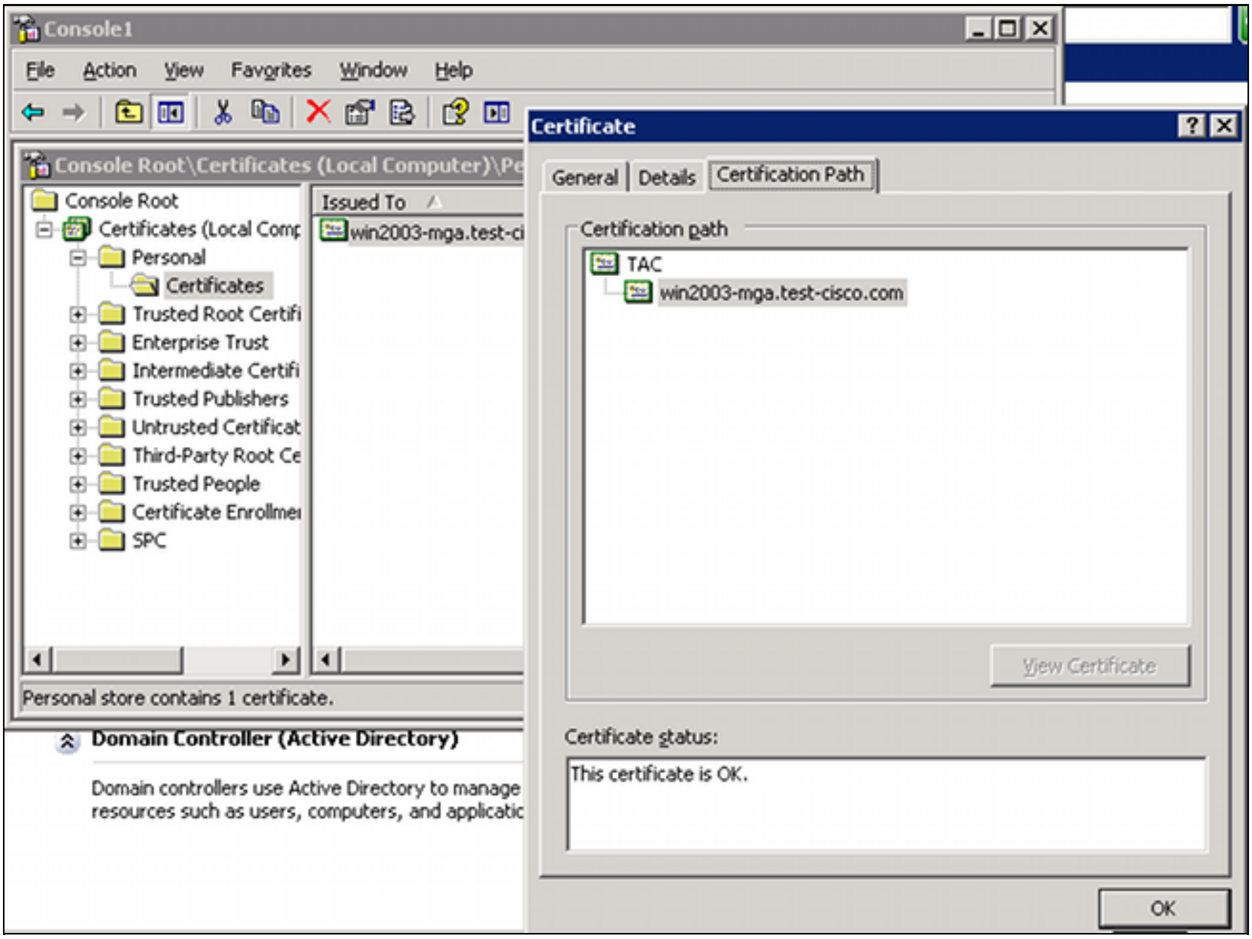
Available standalone snap-ins:

Description
The Certificates snap-in allow
certificate stores for yourself,

This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

Select ***Local computer***, import the certificate to the personal store, and move the associated Certificate Authority (CA) certificate to the trusted store. Verify that the certificate is trusted:



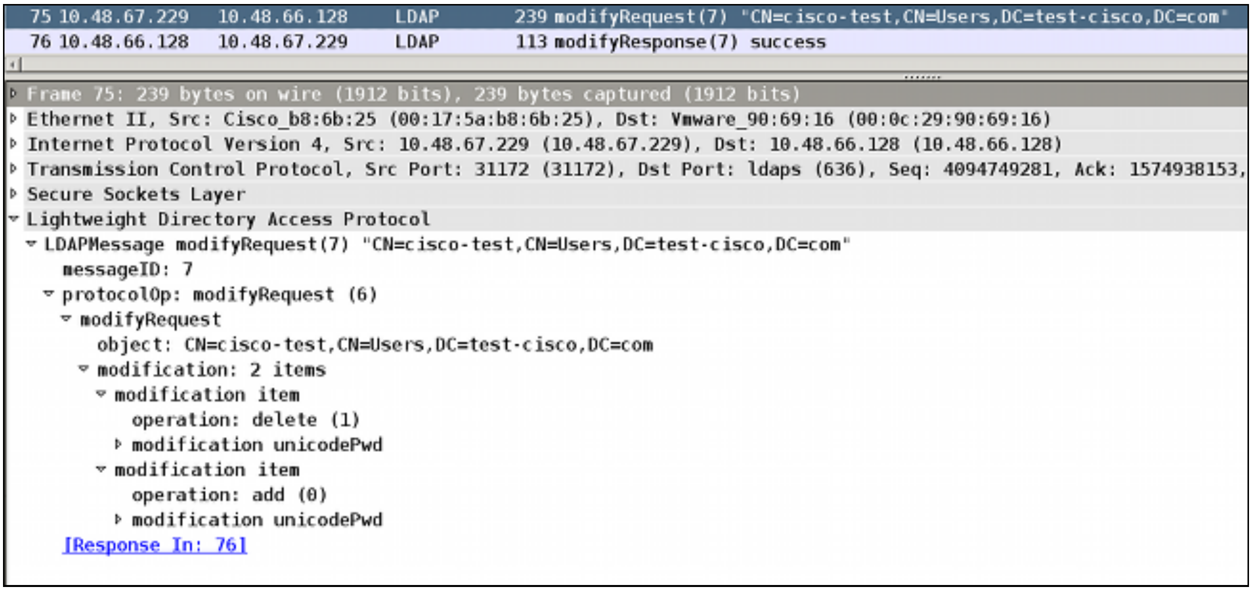
There is a bug in ASA Version 8.4.2, where this error might be returned when you are trying to use LDAP over SSL:

```
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 works correctly with the same configuration. There are two LDAP sessions. The first session returns a failure with the code 773 (password expired), while the second session is used for the password change:

```
[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)
```

To verify the password change, look at the packets. The private key of the LDAP server can be used by Wireshark in order to decrypt SSL traffic:



```
 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]
```

Internet Key Exchange (IKE)/Authentication, Authorization, and Accounting (AAA) debugs on the ASA are very similar to those presented in the RADIUS authentication scenario.

LDAP and Warning Before Expiration

For LDAP, you can use a feature that sends a warning before a password expires. The ASA warns the user 90 days before password expiration with this setting:

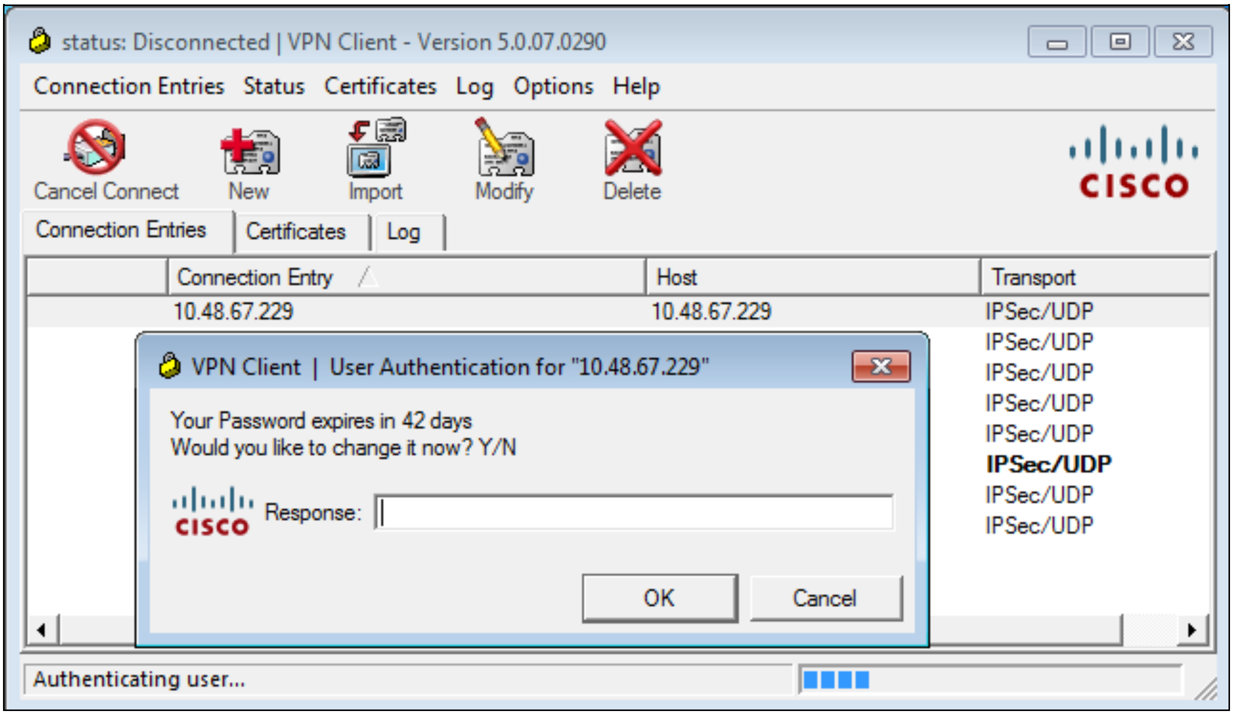
```
tunnel-group RA general-attributes
 password-management password-expire-in-days 90
```

Here the password is expiring in 42 days, and the user tries to log in:

```
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
```

The ASA sends a warning and offers the option for a password change:



status: Disconnected | VPN Client - Version 5.0.07.0290

Connection Entry	Host	Transport
10.48.67.229	10.48.67.229	IPSec/UDP
		IPSec/UDP
		IPSec/UDP
		IPSec/UDP
		IPSec/UDP
		IPSec/UDP
		IPSec/UDP
		IPSec/UDP

VPN Client | User Authentication for "10.48.67.229"

Your Password expires in 42 days
Would you like to change it now? Y/N

Response:

Authenticating user...

If the user chooses to change the password, there is a prompt for a new password, and the normal password change procedure begins.

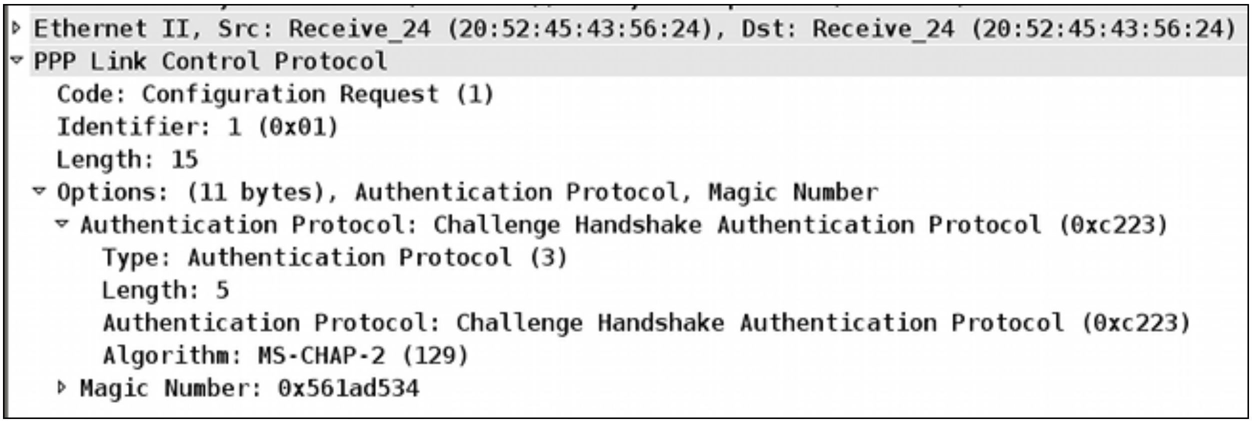
ASA and L2TP

The previous examples presented IKE version 1 (IKEv1) and an IPSec VPN.

For the Layer 2 Tunneling Protocol (L2TP) and IPSec, PPP is used as a transport for authentication. MSCHAPv2 is required instead of PAP for a password change to work:

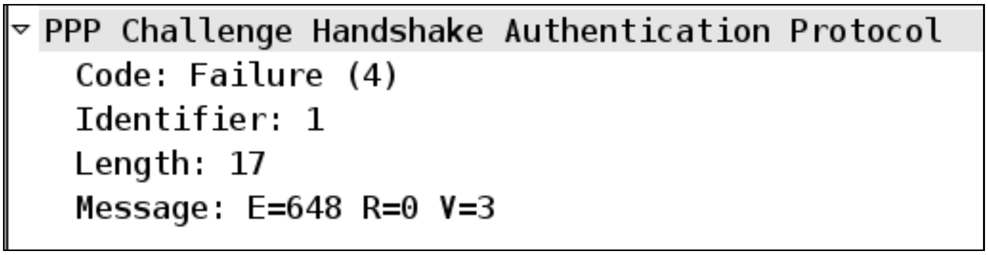
```
ciscoasa(config-tunnel-general)# tunnel-group DefaultRAGroup ppp-attributes
ciscoasa(config-ppp)# authentication ms-chap-v2
```

For Extended Authentication in L2TP inside the PPP session, MSCHAPv2 is negotiated:



```
▷ 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
```

When the user password has expired, a failure with the code 648 is returned:



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

A password change is then needed. The rest of the process is very similar to the scenario for RADIUS with MSCHAPv2.

See L2TP Over IPsec Between Windows 2000/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

The previous examples referred to IKEv1 and the Cisco VPN client, which is end−of−life (EOL).

The recommended solution for a remote access VPN is Cisco AnyConnect Secure Mobility, which uses the IKE version 2 (IKEv2) and SSL protocols. The password change and expiry features work exactly the same for Cisco AnyConnect as they did for the Cisco VPN client.

For IKEv1, the password change and expiry data was exchanged between the ASA and the VPN client in phase 1.5 (Xauth/mode config).

For IKEv2, it is similar; the config mode uses CFG_REQUEST/CFG_REPLY packets.

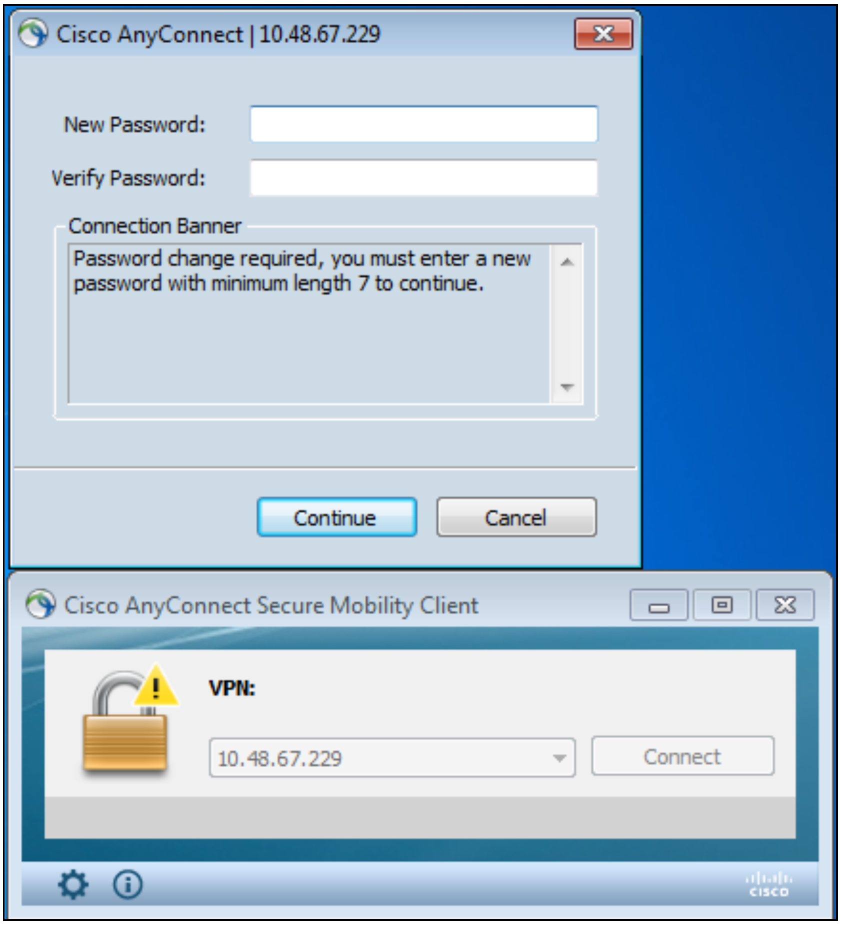
For SSL, the data is in the control Datagram Transport Layer Security (DTLS) session.

The configuration is the same for the ASA.

This is an example configuration with Cisco AnyConnect and the SSL protocol with an LDAP server over 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
```

Once the correct password (which has expired) is provided, Cisco AnyConnect tries to connect and asks for a new password:



Cisco AnyConnect | 10.48.67.229

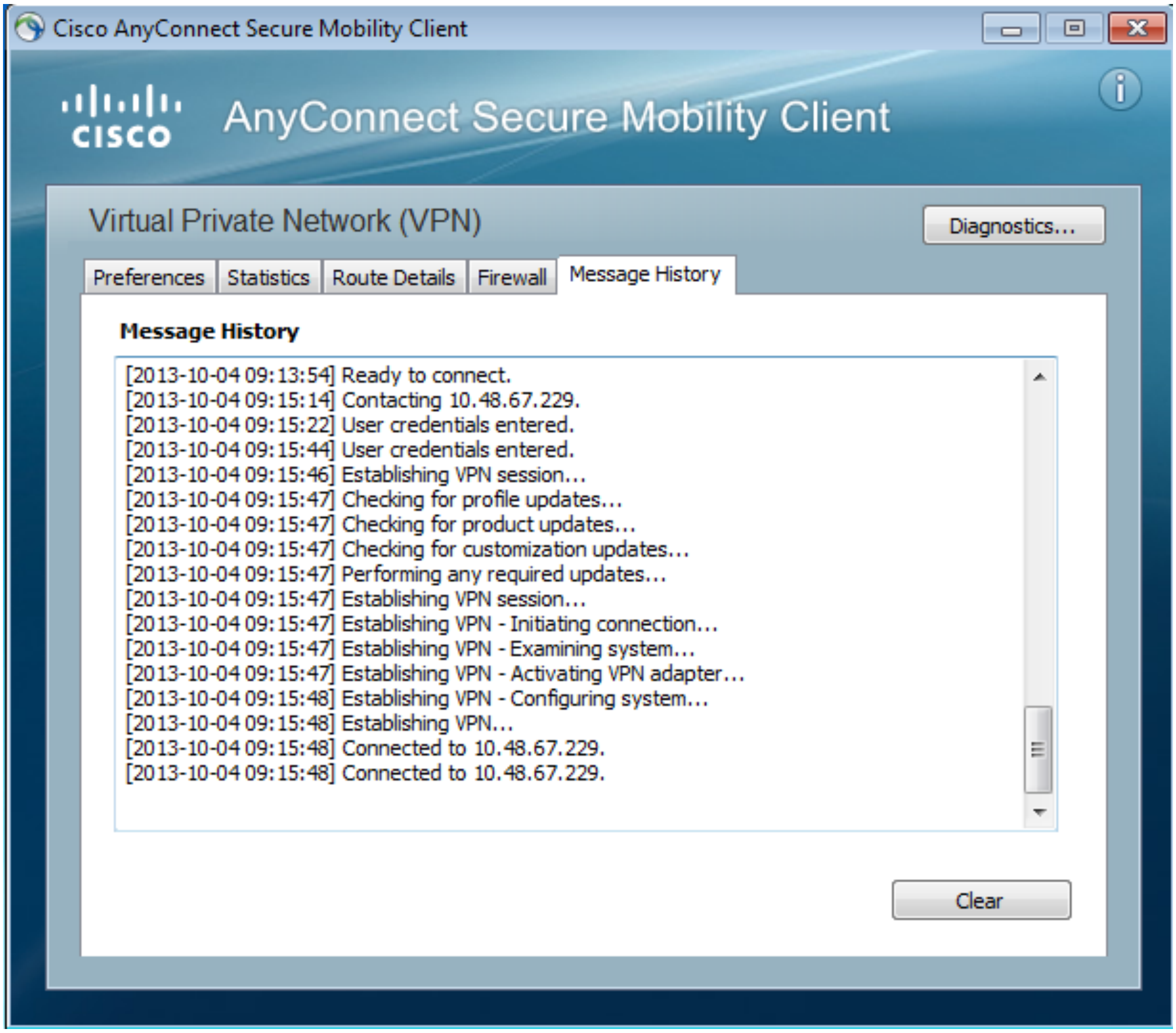
New Password:

Verify Password:

Connection Banner

Password change required, you must enter a new password with minimum length 7 to continue.

The logs indicate that user credentials were entered twice:



Cisco AnyConnect Secure Mobility Client
cisco
AnyConnect Secure Mobility Client
Virtual Private Network (VPN)
Diagnostics...
Preferences
Statistics
Route Details
Firewall
Message History
Clear

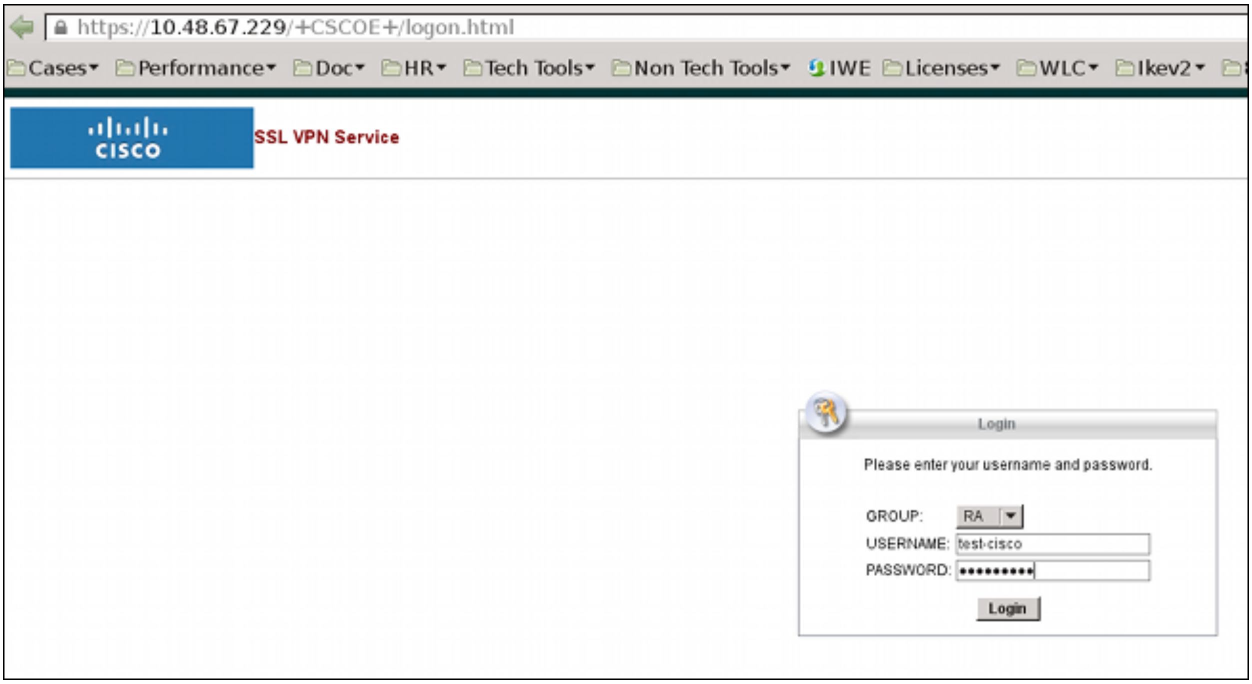
Message History

```
[2013-10-04 09:13:54] Ready to connect.
[2013-10-04 09:15:14] Contacting 10.48.67.229.
[2013-10-04 09:15:22] User credentials entered.
[2013-10-04 09:15:44] User credentials entered.
[2013-10-04 09:15:46] Establishing VPN session...
[2013-10-04 09:15:47] Checking for profile updates...
[2013-10-04 09:15:47] Checking for product updates...
[2013-10-04 09:15:47] Checking for customization updates...
[2013-10-04 09:15:47] Performing any required updates...
[2013-10-04 09:15:47] Establishing VPN session...
[2013-10-04 09:15:47] Establishing VPN - Initiating connection...
[2013-10-04 09:15:47] Establishing VPN - Examining system...
[2013-10-04 09:15:47] Establishing VPN - Activating VPN adapter...
[2013-10-04 09:15:48] Establishing VPN - Configuring system...
[2013-10-04 09:15:48] Establishing VPN...
[2013-10-04 09:15:48] Connected to 10.48.67.229.
[2013-10-04 09:15:48] Connected to 10.48.67.229.
```

More detailed logs are available in the Diagnostic AnyConnect Reporting Tool (DART).

ASA SSL Web Portal

The same login process occurs in the web portal:



https://10.48.67.229/+CSCOE+/logon.html

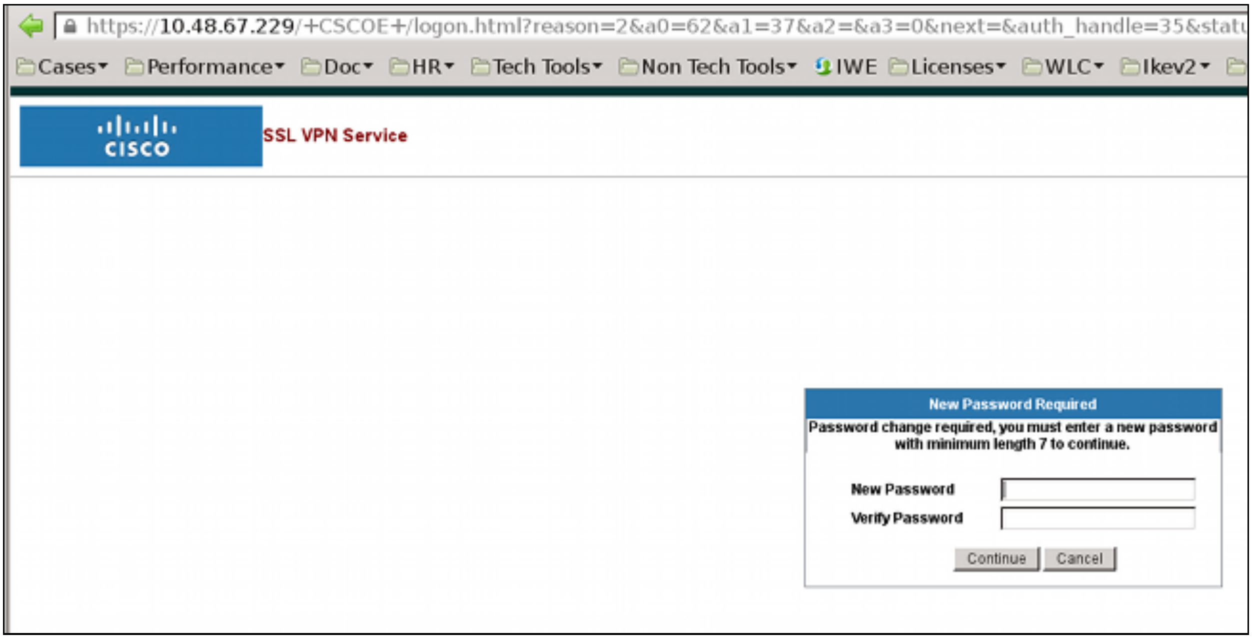
Please enter your username and password.

GROUP: RA

USERNAME: test-cisco

PASSWORD: •••••••••

The same password expiration and change process occurs:



https://10.48.67.229/+CSCOE+/logon.html?reason=2&a0=62&a1=37&a2=&a3=0&next=&auth_handle=35&statu

Password change required, you must enter a new password with minimum length 7 to continue.

New Password

Verify Password

ACS User Change Password

If it is not possible to change the password over the VPN, you can use the ACS User Change Password (UCP) dedicated web service. See Software Developer's Guide for Cisco Secure Access Control System 5.4: Using the UCP Web Services.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- ***Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6: Configuring an External Server for Security Appliance User Authorization***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Nov 25, 2013 Document ID: 116757