ASA Remote Access VPN IKE/SSL - Scadenza e modifica della password per esempio di configurazione RADIUS, TACACS e LDAP

Sommario

Introduzione

In questo documento vengono descritte le funzionalità di scadenza e modifica della password su un tunnel VPN ad accesso remoto terminato su una appliance Cisco Adaptive Security (ASA). Il documento riguarda:

- Client diversi: Cisco VPN client e Cisco AnyConnect Secure Mobility
- Protocolli diversi: TACACS, RADIUS e Lightweight Directory Access Protocol (LDAP)
- Diversi archivi sul Cisco Secure Access Control System (ACS): locale e Active Directory (AD)

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza della configurazione ASA dall'interfaccia della riga di comando (CLI)
- Conoscenze base di configurazione VPN su un'appliance ASA
- Conoscenze base di Cisco Secure ACS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Adaptive Security Appliance, versione 8.4 e successive
- Microsoft Windows Server 2003 SP1
- Cisco Secure Access Control System versione 5.4 o successive
- Cisco AnyConnect Secure Mobility, versione 3.1
- Cisco VPN Client, release 5

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

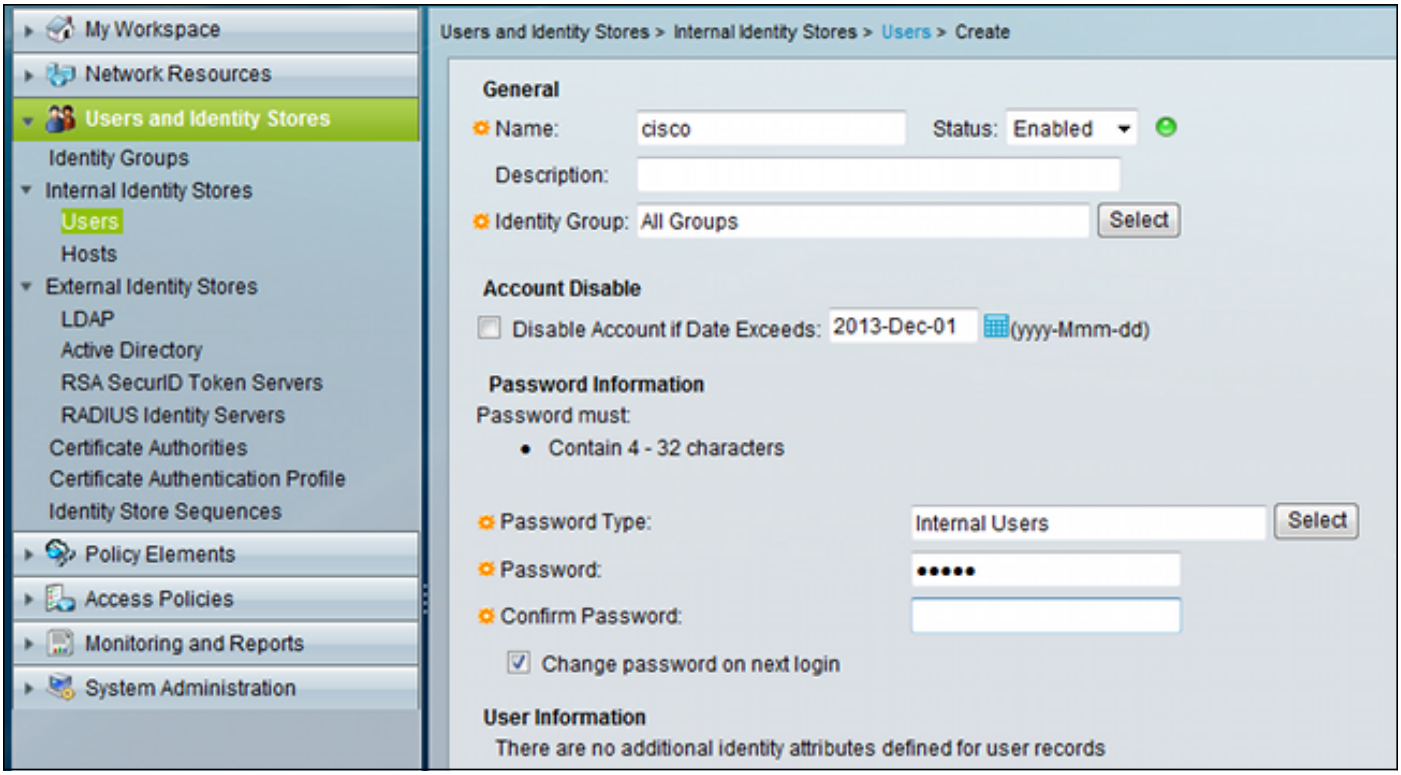
> **Note:**
>
> per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).
>
> consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug.**

ASA con autenticazione locale

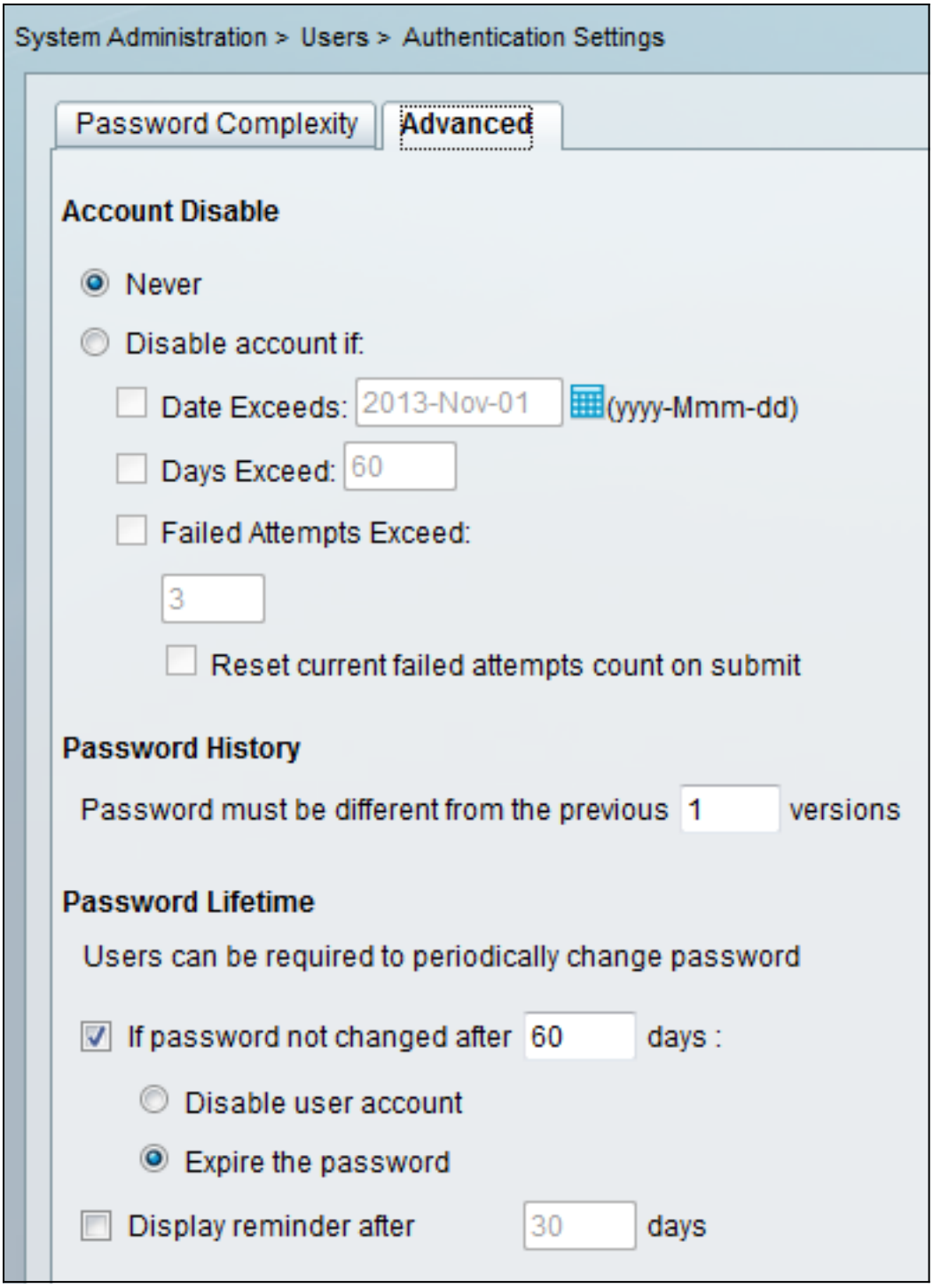
Le appliance ASA con utenti definiti localmente non possono usare le funzionalità di scadenza o modifica delle password. È necessario un server esterno, ad esempio RADIUS, TACACS, LDAP o Windows NT.

ACS e utenti locali

ACS supporta sia la scadenza che la modifica della password per gli utenti definiti localmente. Ad esempio, è possibile forzare gli utenti appena creati a modificare la password al successivo accesso oppure disabilitare un account in una data specifica:

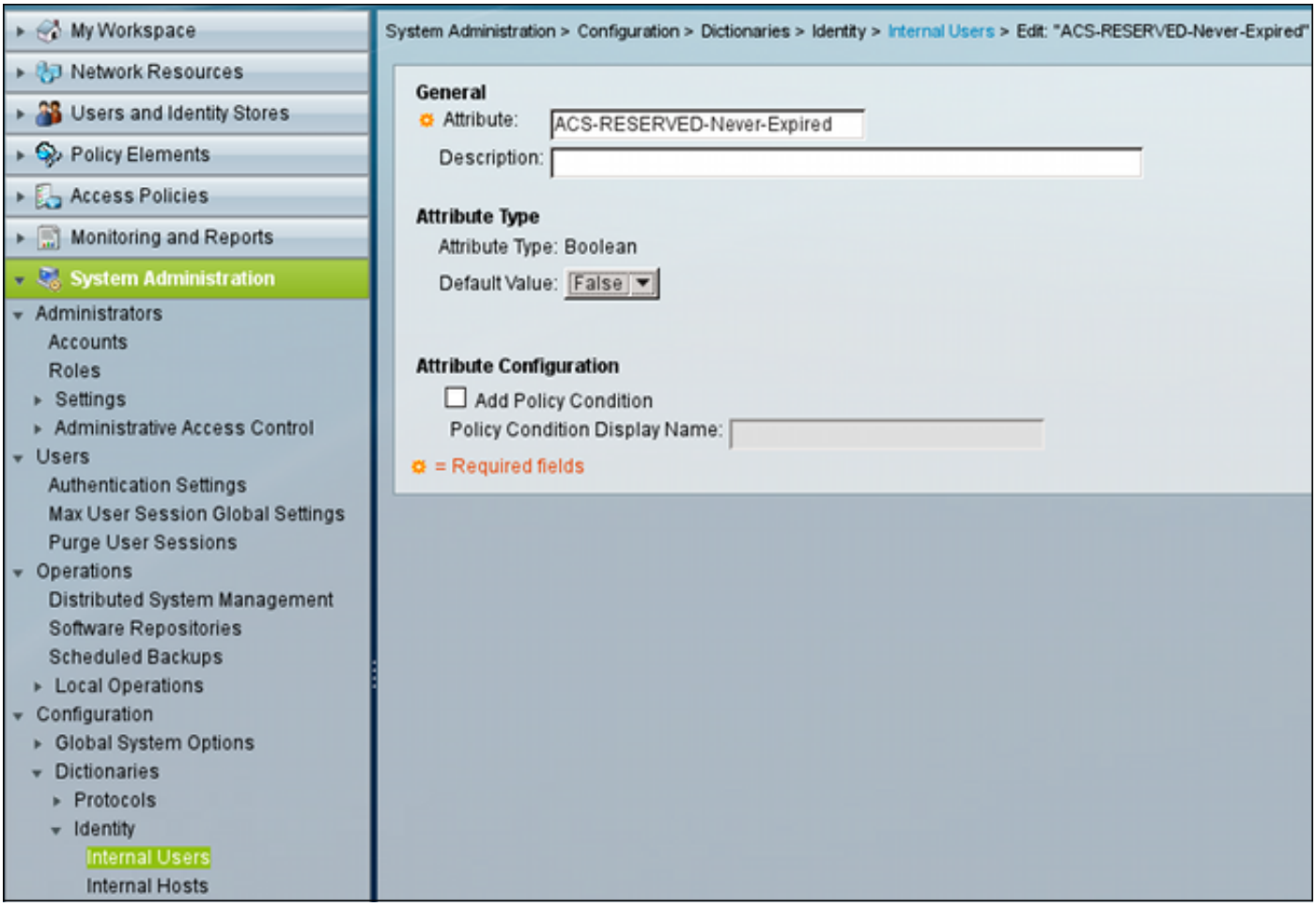


Èpossibile configurare un criterio password per tutti gli utenti. Ad esempio, dopo la scadenza di una password, è possibile disabilitare l'account utente (bloccarlo senza la possibilità di accedere) oppure offrire l'opzione per modificare la password:

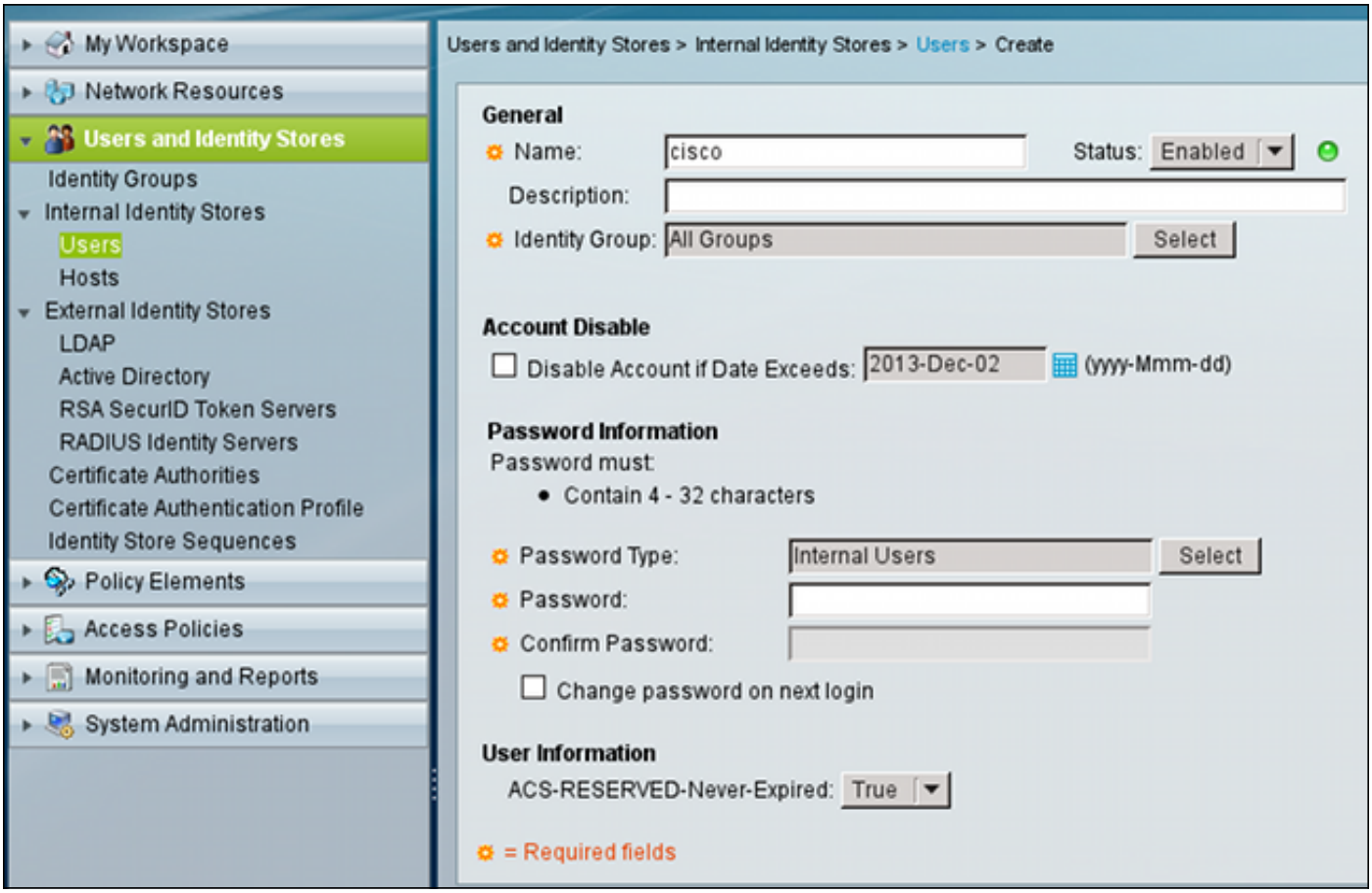


Le impostazioni specifiche dell'utente hanno la precedenza sulle impostazioni globali.

ACS-RESERVED-Never-Expired è un attributo interno per l'identità dell'utente.



Questo attributo è abilitato dall'utente e può essere usato per disabilitare le impostazioni di scadenza dell'account globale. Con questa impostazione, un account non viene disabilitato anche se il criterio globale indica che deve essere:

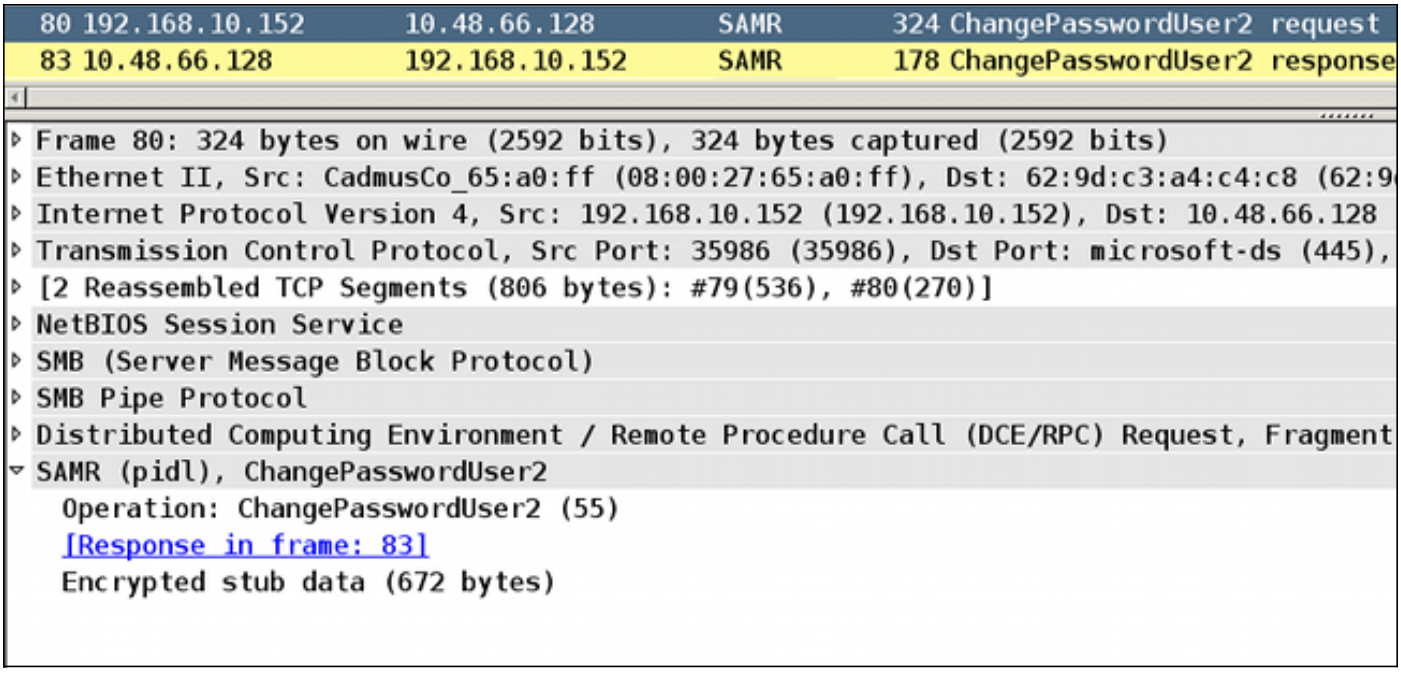


Utenti ACS e Active Directory

Èpossibile configurare ACS per controllare gli utenti in un database di Active Directory. La scadenza e la modifica della password sono supportate quando si utilizza MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol versione 2). vedere la Guida per l'utente di Cisco Secure Access Control System 5.4: Autenticazione in ACS 5.4: Per ulteriori informazioni, vedere Compatibilità tra il protocollo di autenticazione e l'archivio identità.

Su un'ASA, è possibile usare la funzione di gestione delle password, come descritto nella sezione successiva, per forzare l'appliance a usare MSCHAPv2.

ACS utilizza la chiamata DCE/RPC (Common Internet File System) (CIFS) Distributed Computing Environment/Remote Procedure Call quando contatta la directory del controller di dominio per modificare la password:



L'ASA può usare sia il protocollo RADIUS che TACACS+ per contattare l'ACS e richiedere la modifica della password di un AD.

ASA con ACS tramite RADIUS

Il protocollo RADIUS non supporta in modo nativo la scadenza o la modifica della password. In genere, per RADIUS viene utilizzato il protocollo PAP (Password Authentication Protocol). L'appliance ASA invia il nome utente e la password in formato testo normale e la password viene quindi crittografata tramite il segreto condiviso RADIUS.

In uno scenario tipico in cui la password dell'utente è scaduta, ACS restituisce un messaggio di rifiuto del raggio all'appliance ASA. ACS osserva che:

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

Per l'appliance ASA, si tratta di un semplice messaggio di rifiuto del raggio e l'autenticazione non riesce.

Per risolvere questo problema, l'ASA consente di usare il comando **password-management** nella configurazione del gruppo di tunnel:

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

Il comando **password-management** modifica il comportamento in modo che l'ASA sia costretta a utilizzare MSCHAPv2, anziché PAP, nella richiesta Radius.

Il protocollo MSCHAPv2 supporta la scadenza e la modifica della password. Quindi, se un utente VPN è atterrato in quello specifico gruppo di tunnel durante la fase Xauth, la richiesta Radius dall'ASA include ora una richiesta 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)
```

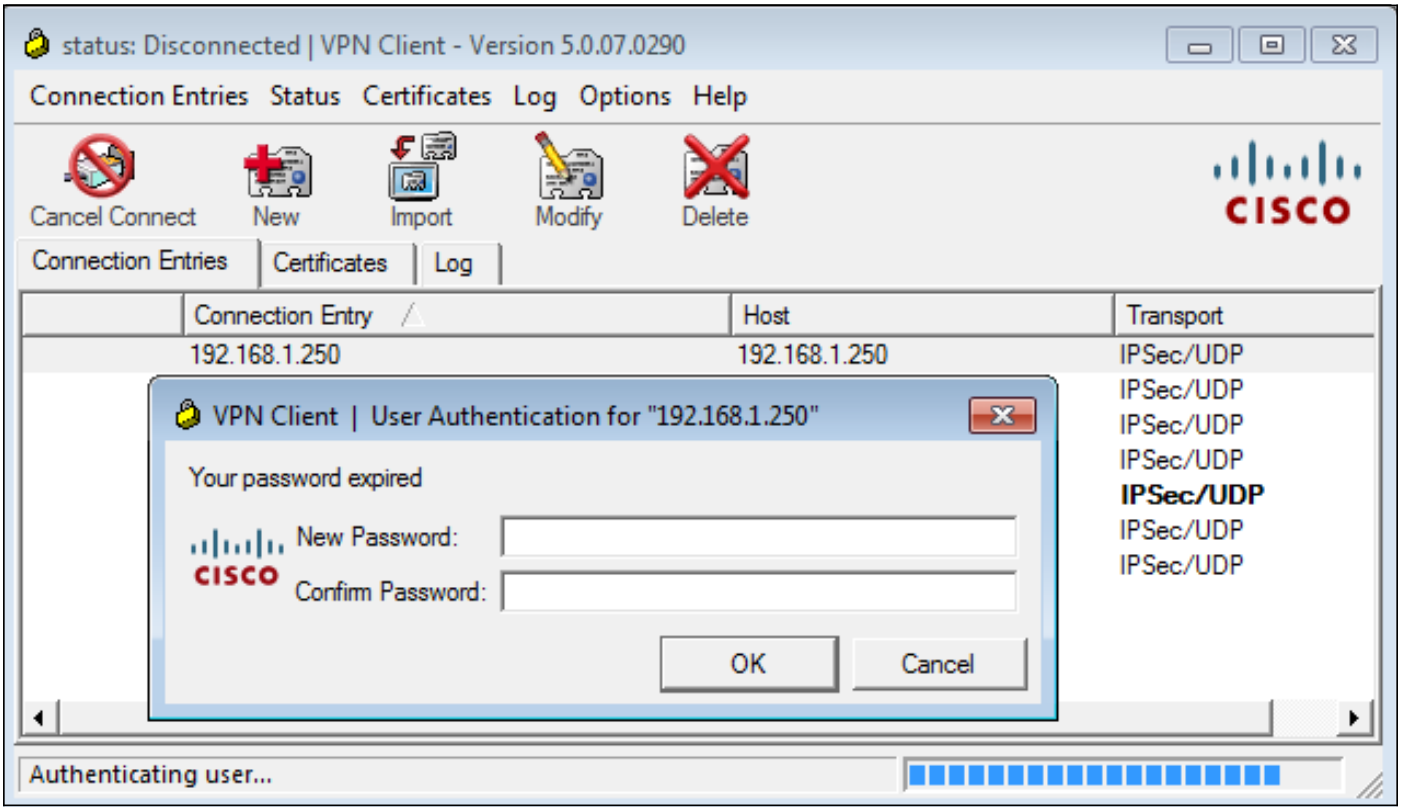
Se ACS rileva la necessità di modificare la password, restituisce un messaggio Radius-Reject con errore MSCHAPv2 648.

```
▽ 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
```

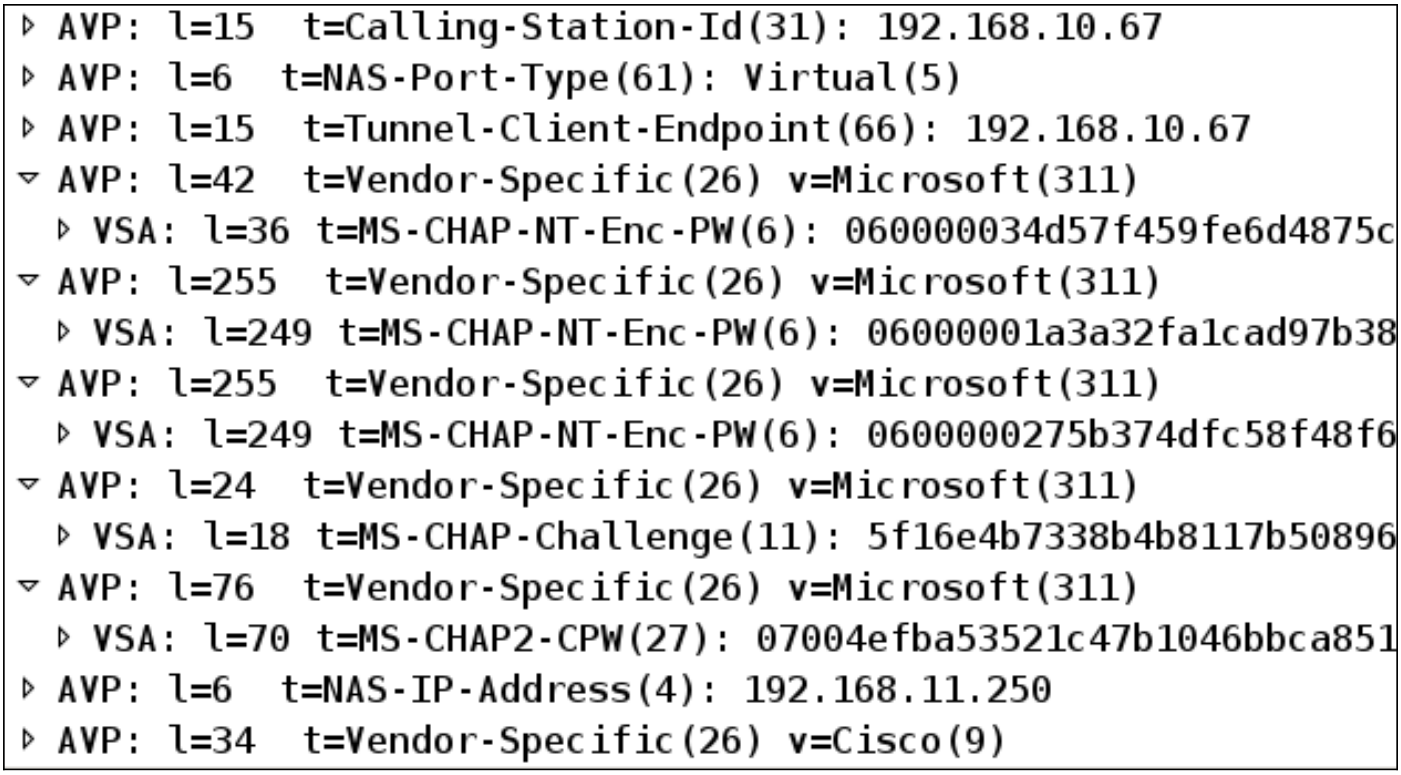
L'ASA comprende il messaggio e usa MODE_CFG per richiedere la nuova password al client VPN Cisco:

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

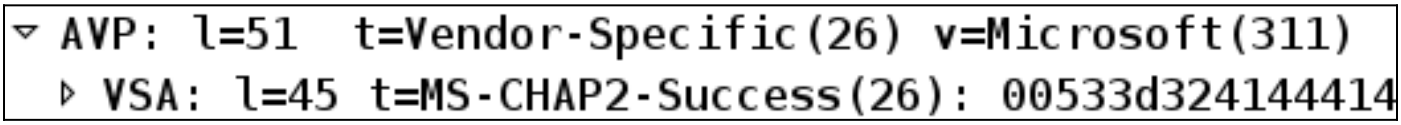
Il client VPN Cisco visualizza una finestra di dialogo che richiede una nuova password:



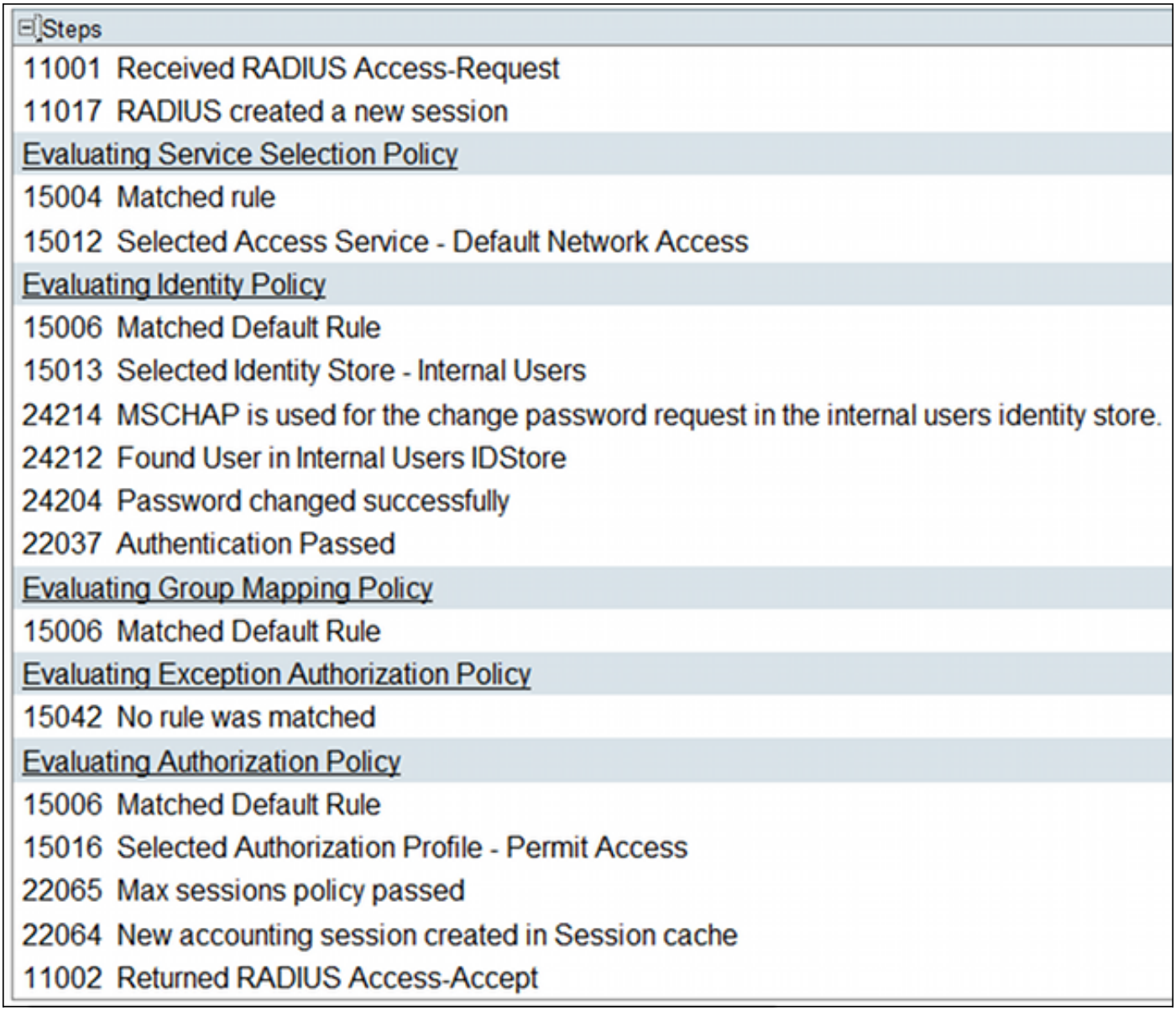
L'ASA invia un'altra richiesta Radius con un payload MS-CHAP-CPW e MS-CHAP-NT-Enc-PW (la nuova password):



ACS conferma la richiesta e restituisce un valore Radius-Accept con MS-CHAP2-Success:



Èpossibile verificare questa condizione su ACS, che indica che la password 24204 è stata modificata correttamente:



L'ASA segnala quindi la riuscita dell'autenticazione e continua con il processo in modalità rapida (QM):

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

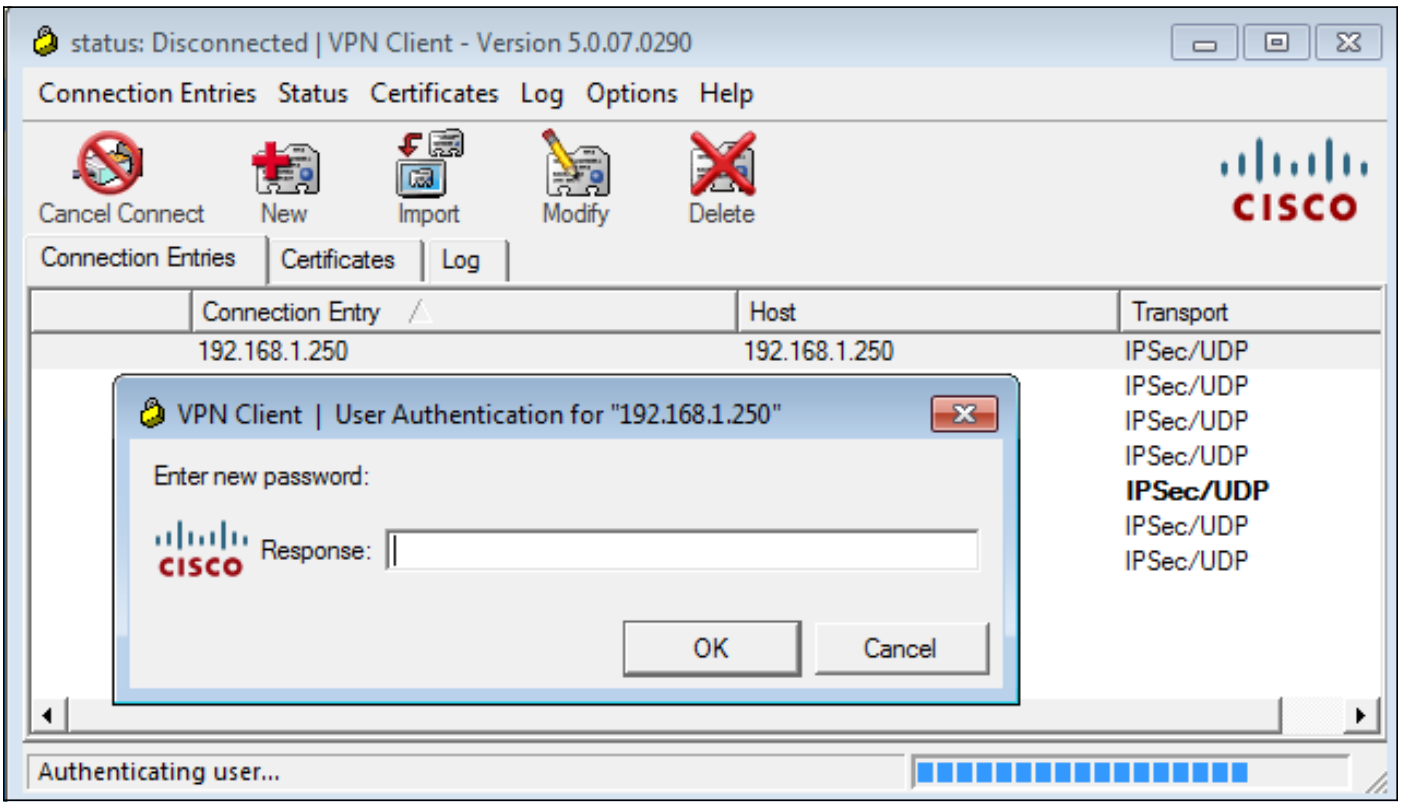
ASA con ACS tramite TACACS+

Analogamente, TACACS+ può essere utilizzato per la scadenza e la modifica della password. La funzione di gestione delle password non è necessaria, in quanto l'ASA usa ancora TACACS+ con un tipo di autenticazione ASCII anziché MSCHAPv2.

Vengono scambiati più pacchetti e ACS chiede una nuova password:

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

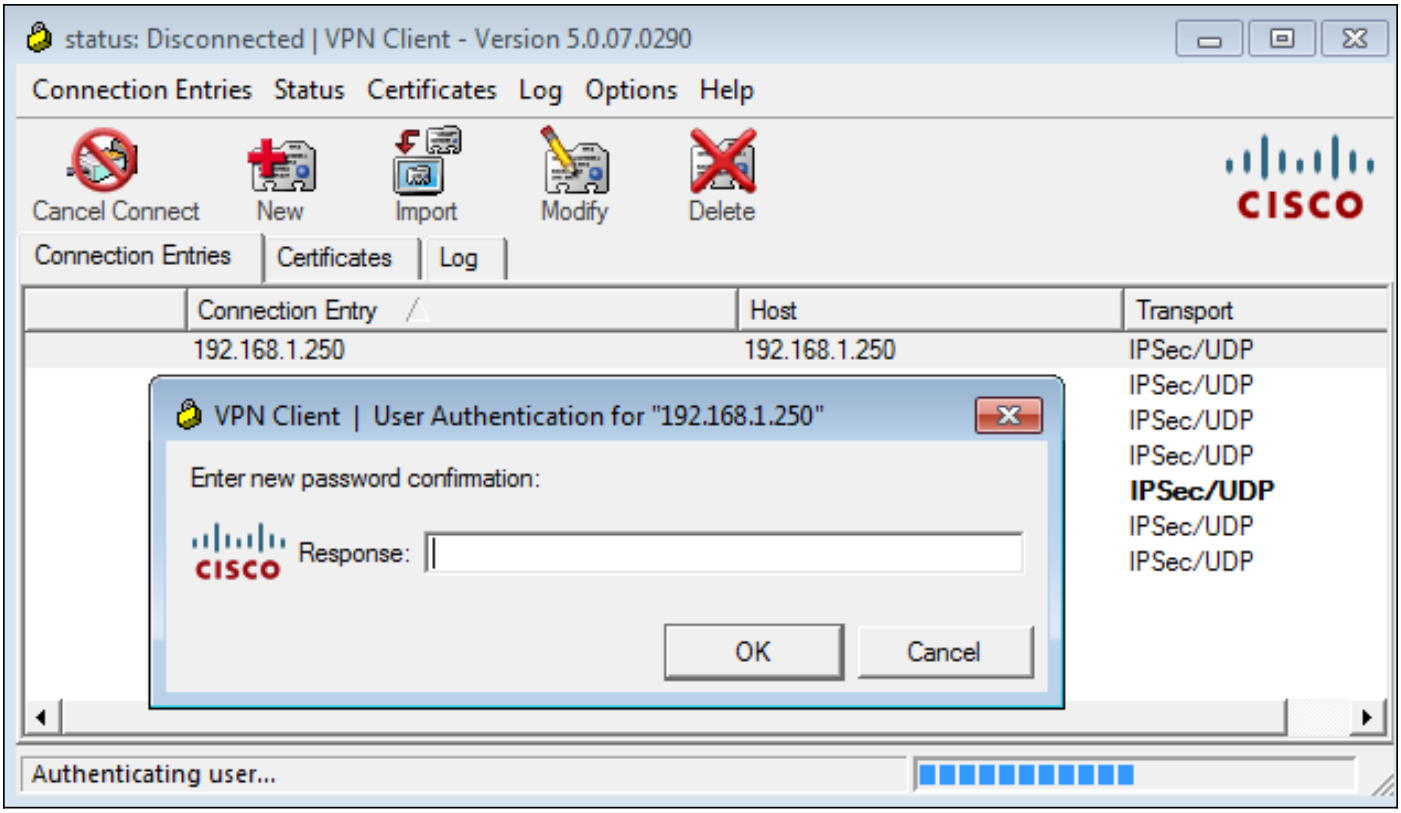
Il client VPN Cisco visualizza una finestra di dialogo (diversa da quella utilizzata da RADIUS) che richiede una nuova password:



ACS richiede la conferma della nuova password:

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

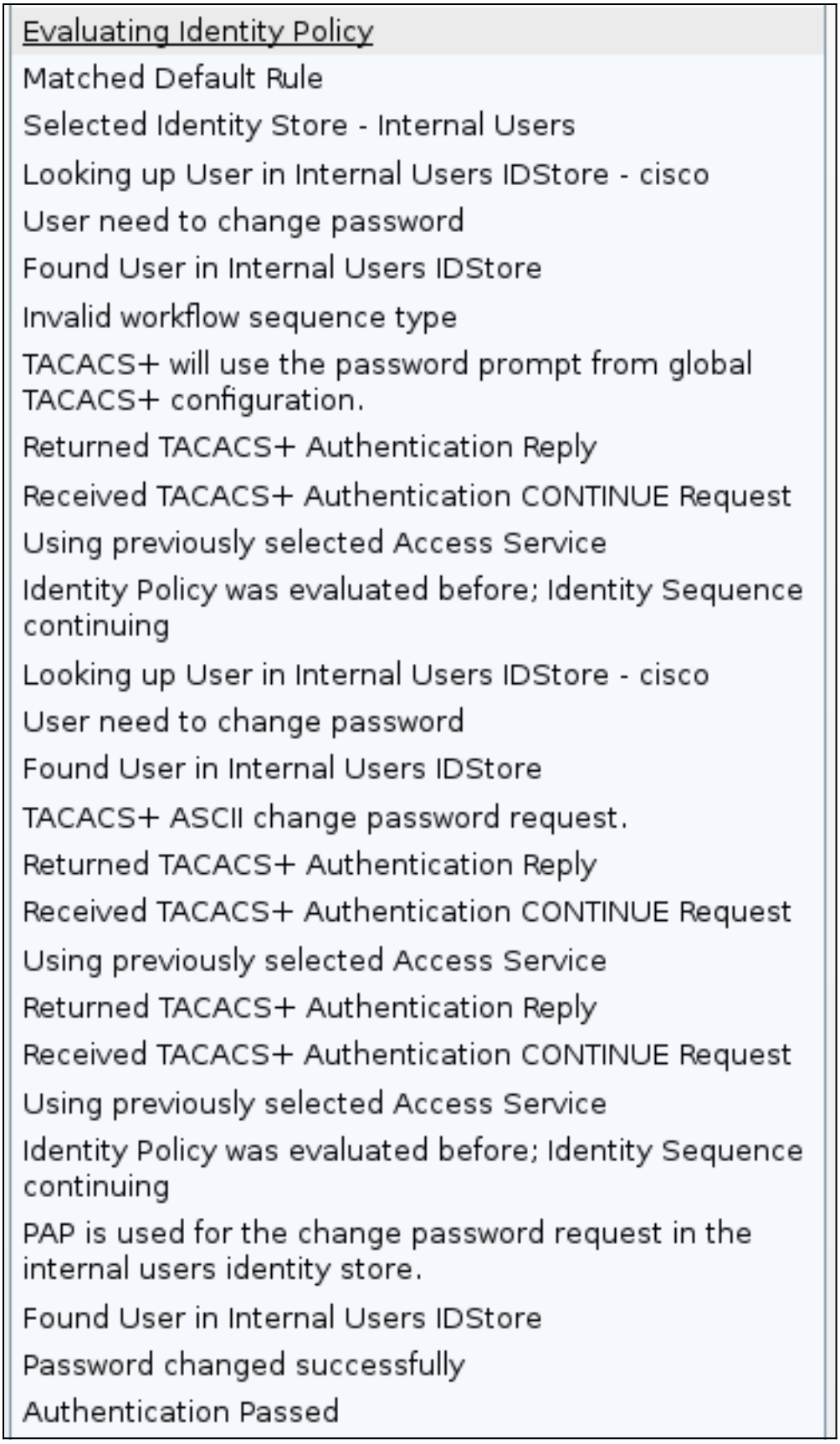
Il client VPN Cisco presenta una finestra di conferma:



Se la conferma è corretta, ACS segnala un'autenticazione riuscita:

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

ACS registra quindi un evento per il quale la password è stata modificata correttamente:



I debug ASA mostrano l'intero processo di scambio e la riuscita dell'autenticazione:

```
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.
```

La modifica della password è completamente trasparente per l'ASA. È solo un po' più lunga la sessione TACACS+ con altri pacchetti di richiesta e risposta, che vengono analizzati dal client VPN e presentati all'utente che sta cambiando la password.

ASA con LDAP

La scadenza e la modifica delle password sono completamente supportate dallo schema del server LDAP Microsoft AD e Sun.

Per la modifica della password, i server restituiscono 'bindresponse = invalidCredentials' con 'error = 773.' Questo errore indica che l'utente deve reimpostare la password. I codici di errore tipici includono:

Codice errore	Errore
525	Utente non trovato
52 sexies	Invalid Credentials (Credenziali non valide)
530	Accesso non consentito in questo momento
531	Accesso alla workstation non consentito
532	Password scaduta
533	Account disabilitato
701	Account scaduto
773	L'utente deve reimpostare la password
775	Account utente bloccato

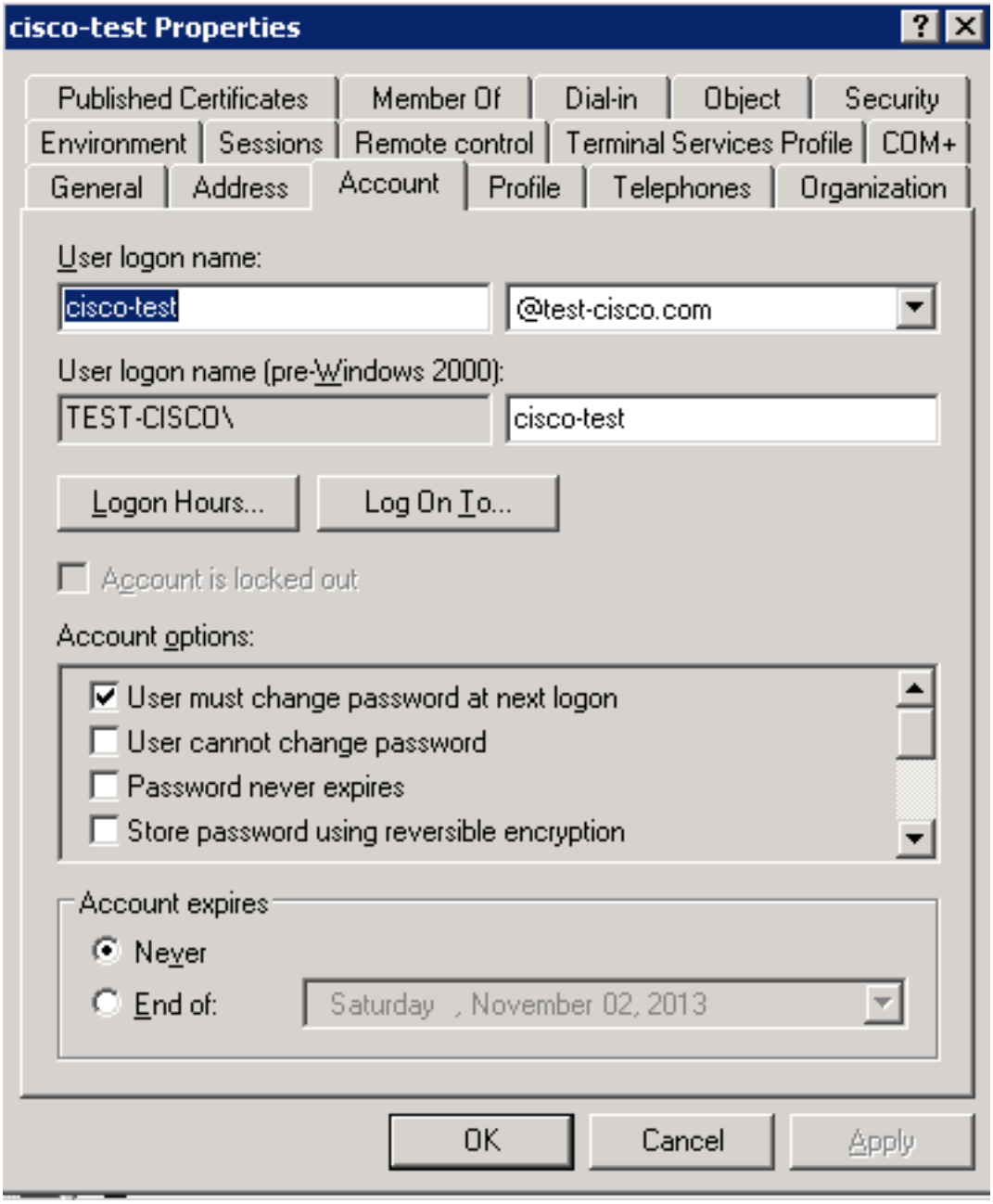
Configurare il server LDAP:

```
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
```

Utilizzare questa configurazione per il gruppo di tunnel e la funzione di gestione delle password:

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

Configurare l'utente AD in modo che sia necessario modificare la password:



Quando l'utente tenta di utilizzare il client VPN Cisco, l'ASA segnala una password non valida:

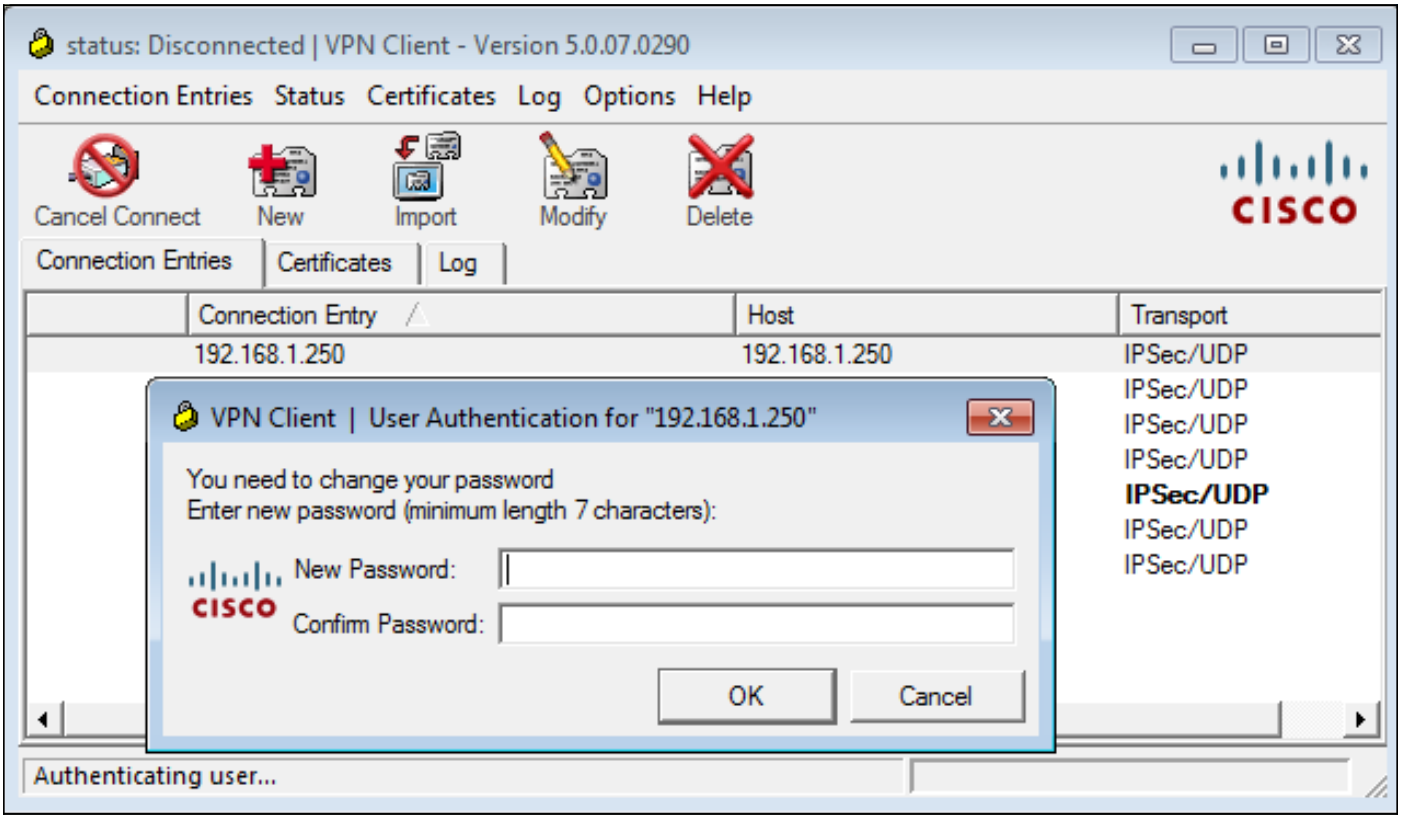
```
ASA(config-tunnel-general)# debug ldap 255
<some output ommited for clarity>

[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
```

Se le credenziali non sono valide, viene visualizzato l'errore 52e:

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

Il client VPN Cisco chiede quindi di modificare la password:



Questa finestra di dialogo è diversa da quella utilizzata da TACACS o RADIUS perché visualizza il criterio. In questo esempio il criterio prevede una lunghezza minima della password di sette caratteri.

Una volta modificata la password, l'ASA potrebbe ricevere questo messaggio di errore dal server LDAP:

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

I criteri Microsoft richiedono l'utilizzo di SSL (Secure Sockets Layer) per la modifica della password. Modificare la configurazione:

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

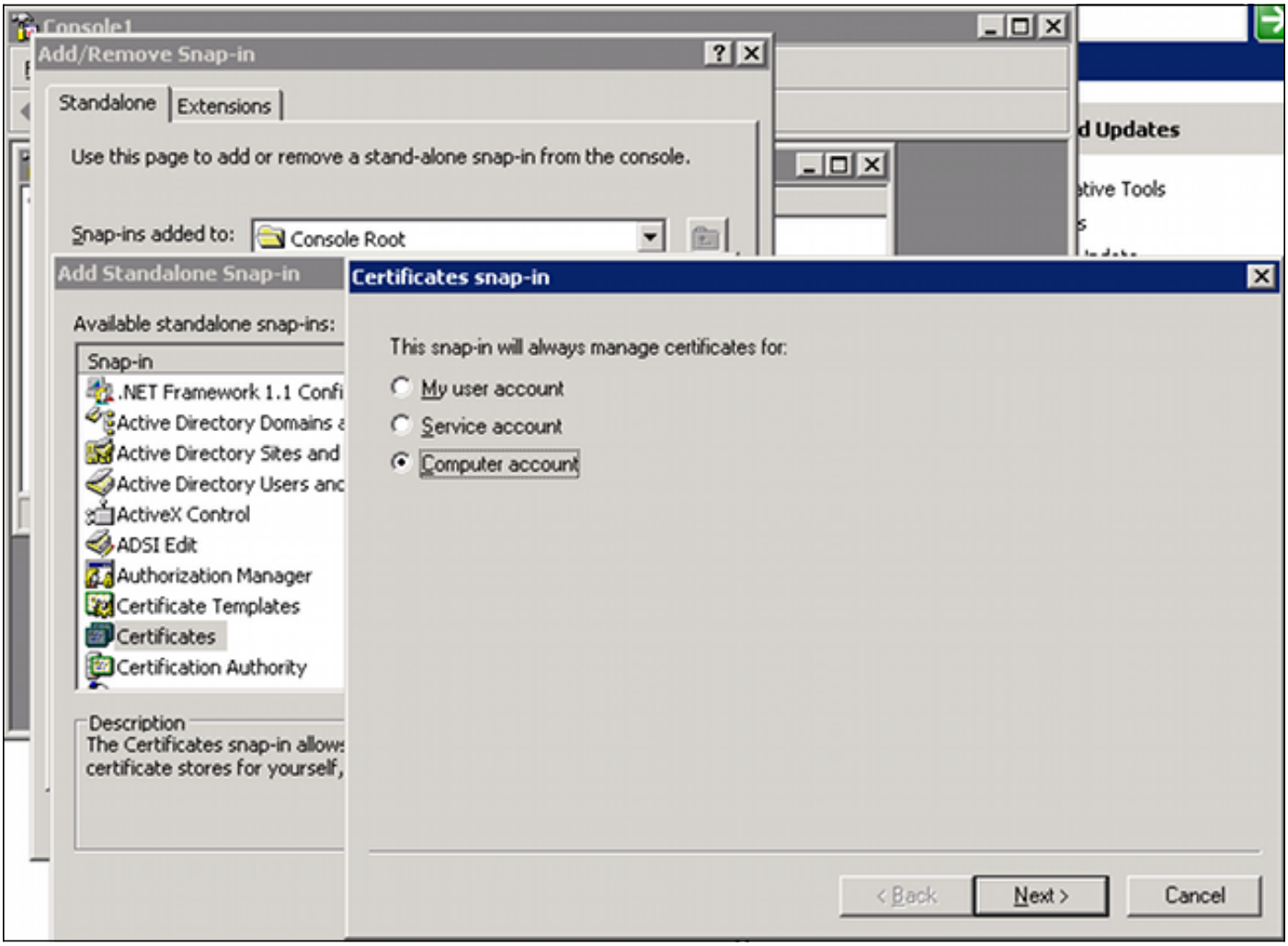
LDAP Microsoft per SSL

Per impostazione predefinita, Microsoft LDAP su SSL non funziona. Per abilitare questa funzione, è necessario installare il certificato per l'account computer con l'estensione della chiave corretta. Per ulteriori informazioni, vedere Come abilitare LDAP su SSL con un'autorità di certificazione di terze parti.

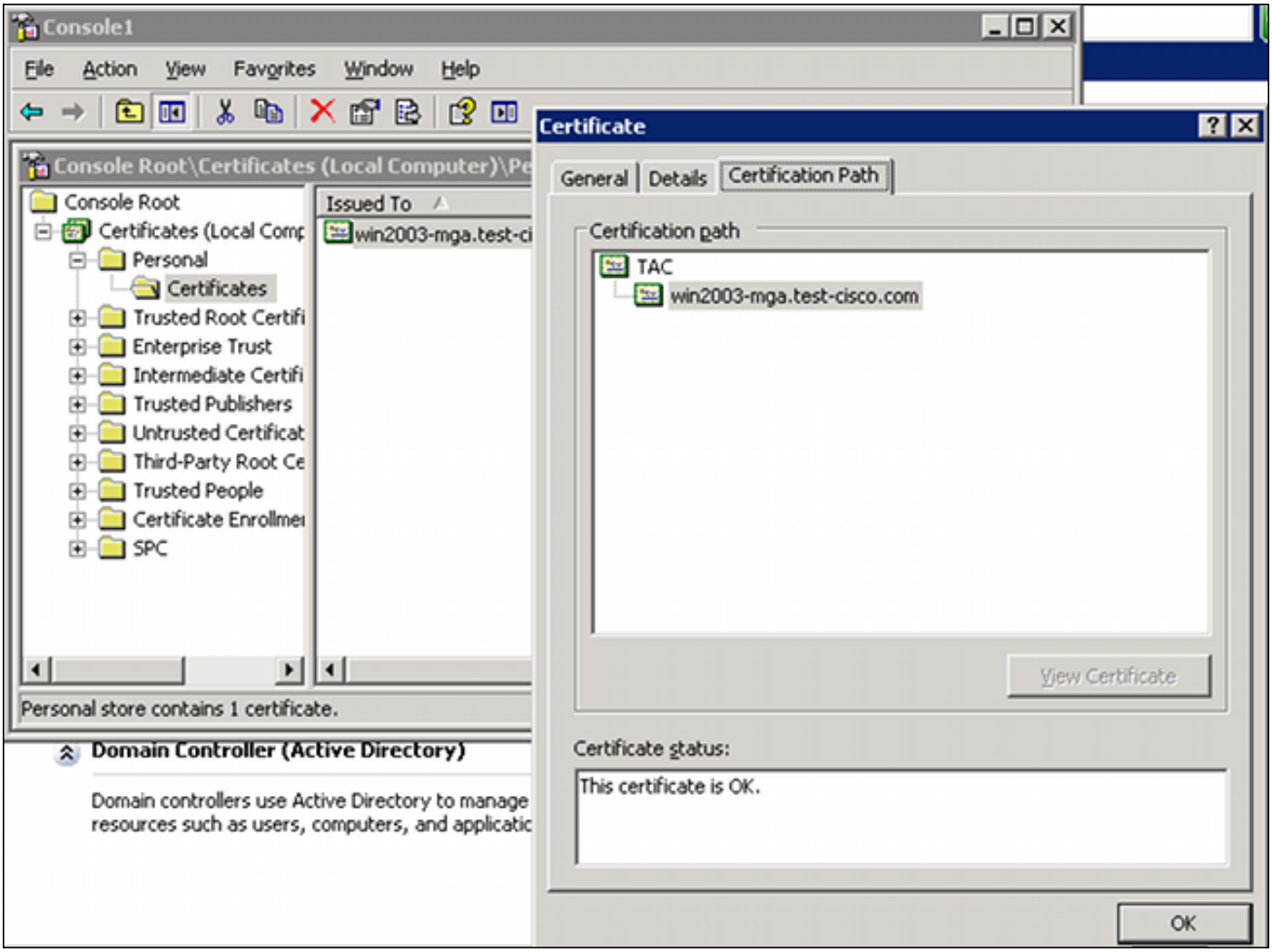
Il certificato può anche essere autofirmato perché l'ASA non verifica il certificato LDAP. Per una richiesta di miglioramento correlata, vedere l'ID bug Cisco CSCui40212, "Allow ASA to validate certificate from LDAPS server" (Consenti all'ASA di convalidare il certificato dal server LDAPS).

> **Nota:** ACS verifica il certificato LDAP nella versione 5.5 e successive.

Per installare il certificato, aprire la console mmc, selezionare **Aggiungi/Rimuovi snap-in**, aggiungere il certificato e scegliere **Account computer**:



Selezionare **Computer locale**, importare il certificato nell'archivio personale e spostare il certificato CA associato nell'archivio attendibile. Verificare che il certificato sia attendibile:



Si è verificato un bug in ASA versione 8.4.2, dove questo errore potrebbe essere restituito quando si cerca di usare LDAP su SSL:

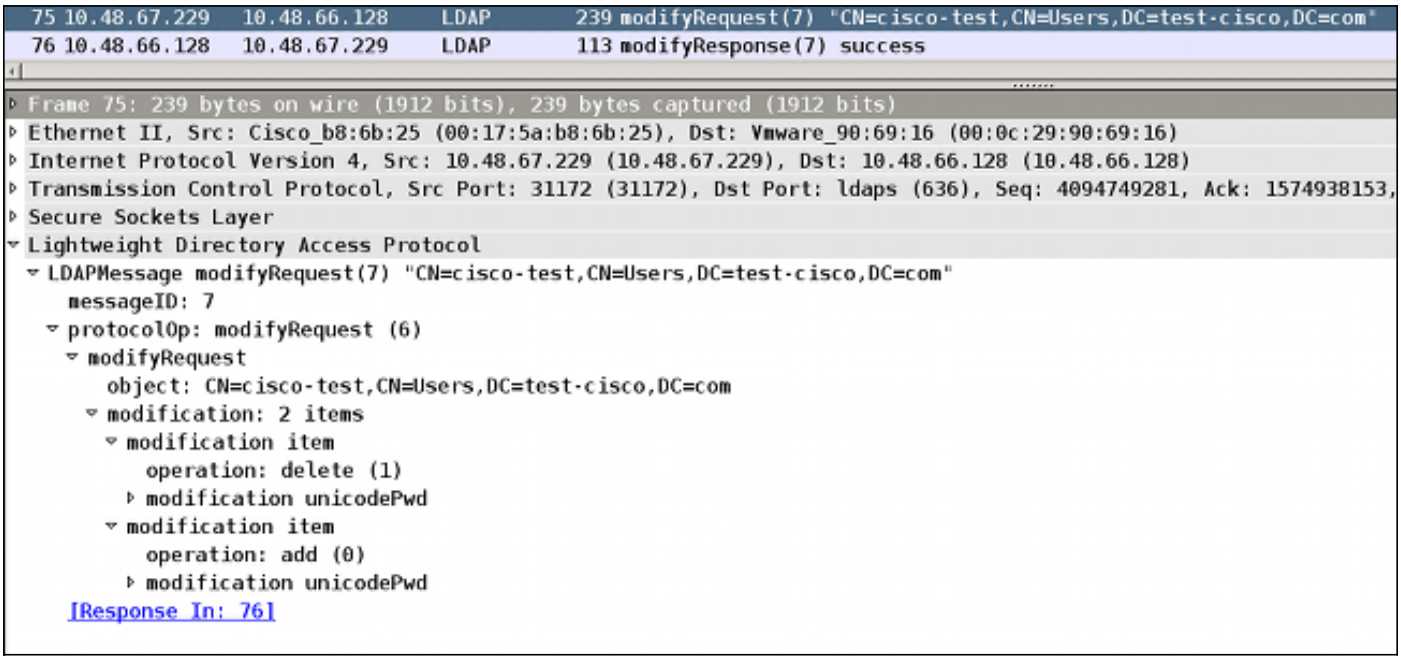
```
ASA(config)# debug ldap 255

[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 versione 9.1.3 funziona correttamente con la stessa configurazione. Esistono due sessioni LDAP. La prima sessione restituisce un errore con il codice 773 (password scaduta), mentre la seconda sessione viene utilizzata per la modifica della password:

```
[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)
```

Per verificare il cambiamento della password, esaminare i pacchetti. La chiave privata del server LDAP può essere utilizzata da Wireshark per decrittografare il traffico SSL:



I debug IKE (Internet Key Exchange)/Authentication, Authorization, and Accounting (AAA) sull'appliance ASA sono molto simili a quelli riportati nello scenario di autenticazione RADIUS.

LDAP e avviso prima della scadenza

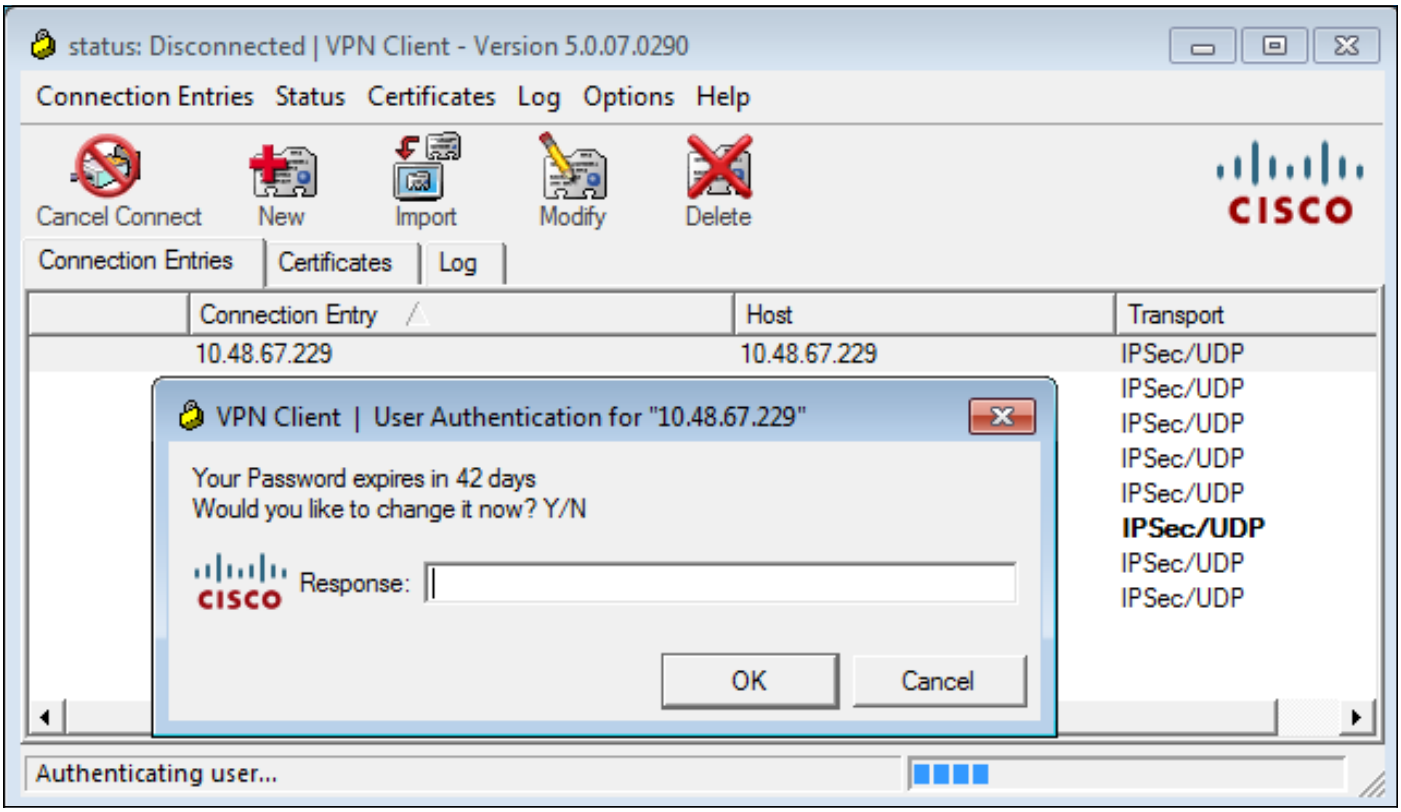
Per LDAP, è possibile utilizzare una funzione che invia un avviso prima della scadenza di una password. L'ASA avvisa l'utente 90 giorni prima della scadenza della password con questa impostazione:

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

La password scade tra 42 giorni e l'utente tenta di eseguire l'accesso:

```
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
```

L'appliance ASA invia un avviso offrendo la possibilità di modificare la password:



Se l'utente sceglie di modificare la password, viene richiesto di immettere una nuova password e viene avviata la normale procedura di modifica della password.

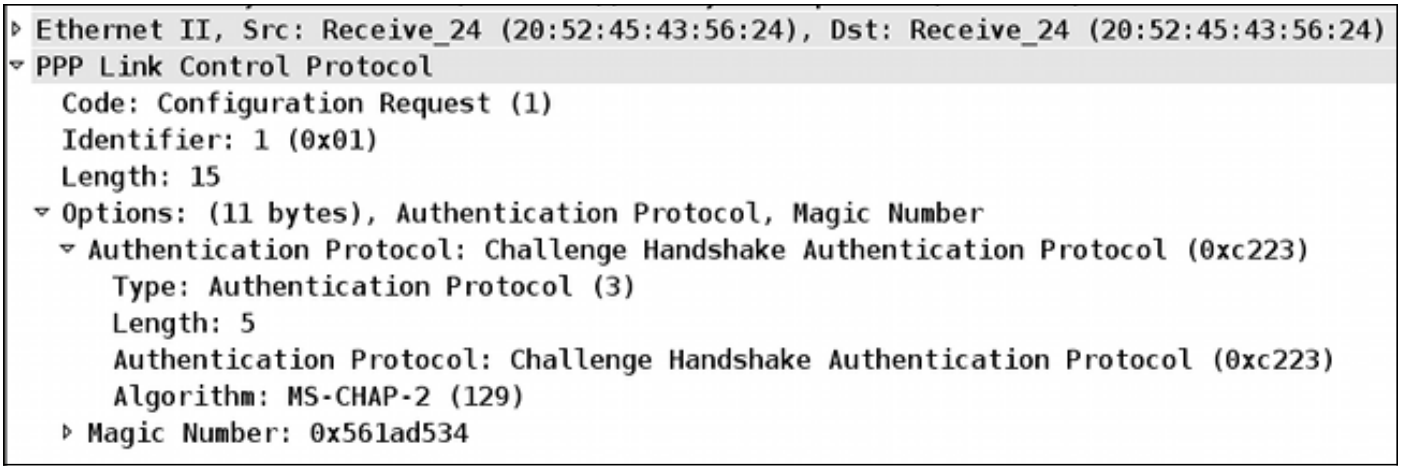
ASA e L2TP

Negli esempi precedenti sono stati presentati IKE versione 1 (IKEv1) e una VPN IPSec.

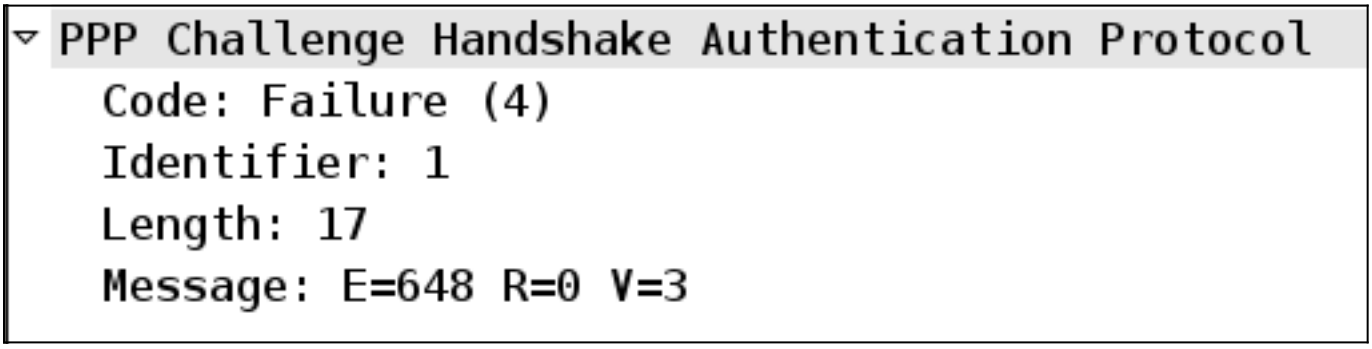
Per il protocollo L2TP (Layer 2 Tunneling Protocol) e IPSec, il protocollo PPP viene utilizzato come trasporto per l'autenticazione. Per il corretto funzionamento di una modifica della password, è necessario MSCHAPv2 anziché PAP:

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

Per l'autenticazione estesa in L2TP all'interno della sessione PPP, viene negoziato MSCHAPv2:



Quando la password utente è scaduta, viene restituito un errore con il codice 648:



Ènecessario modificare la password. Il resto del processo è molto simile allo scenario per RADIUS con MSCHAPv2.

Per ulteriori informazioni su come configurare L2TP, vedere L2TP over IPsec tra Windows 2000/XP PC e PIX/ASA 7.2 Using Pre-shared Key Configuration Example.

ASA SSLVPN Client

Gli esempi precedenti fanno riferimento a IKEv1 e al client VPN Cisco, che non è più commercializzato (EOL).

La soluzione consigliata per una VPN ad accesso remoto è Cisco AnyConnect Secure Mobility, che utilizza i protocolli IKE versione 2 (IKEv2) e SSL. Le funzionalità di modifica della password e di scadenza sono identiche per Cisco AnyConnect e per il client VPN Cisco.

Per IKEv1, la modifica della password e i dati sulla scadenza sono stati scambiati tra l'ASA e il client VPN nella fase 1.5 (Xauth/mode config).

Per IKEv2, è simile. la modalità di configurazione utilizza i pacchetti CFG_REQUEST/CFG_REPLY.

Per SSL, i dati si trovano nella sessione DTLS (Transport Layer Security) del datagramma di controllo.

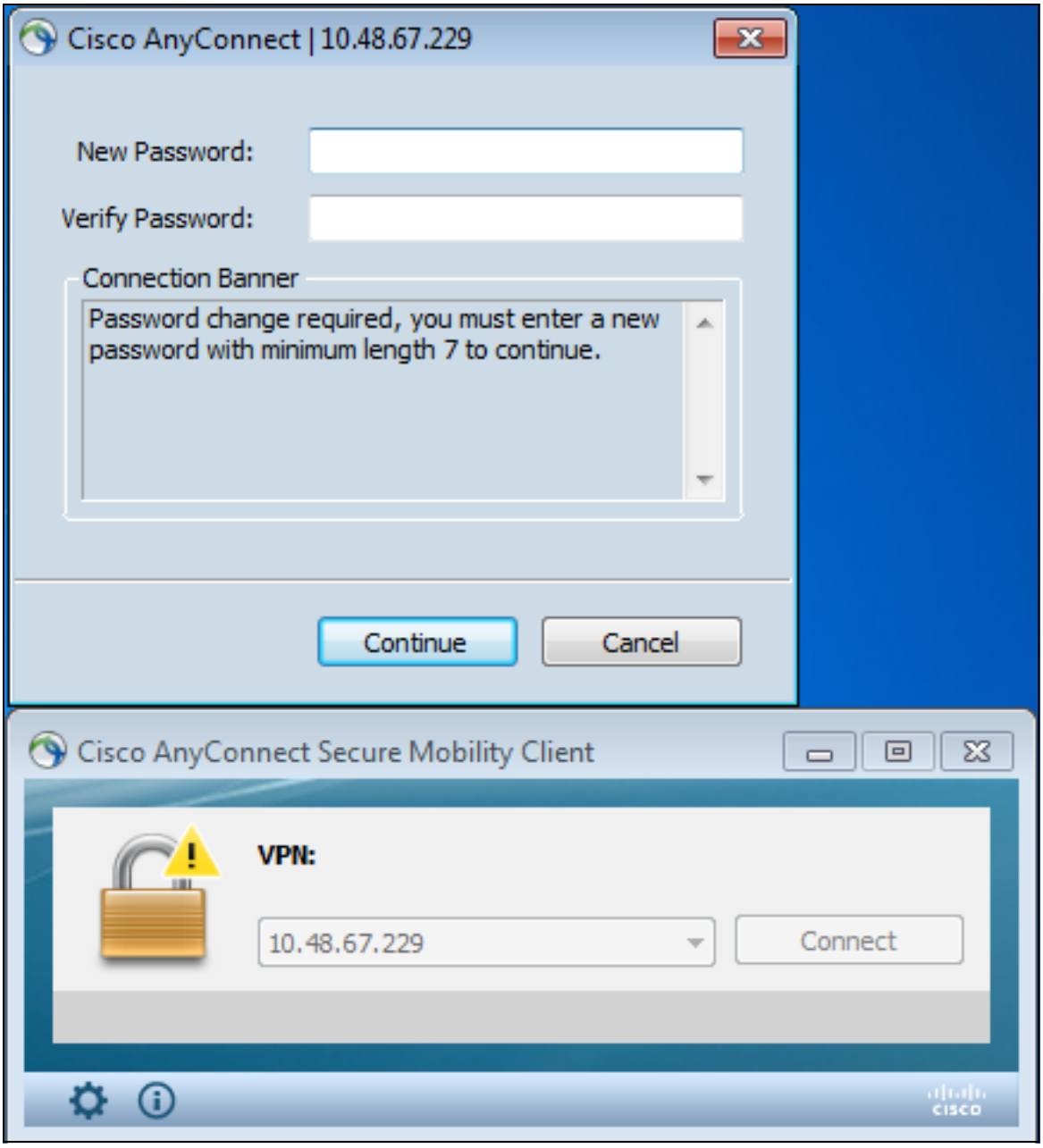
La configurazione è la stessa per l'appliance ASA.

Questa è una configurazione di esempio con Cisco AnyConnect e il protocollo SSL con un server

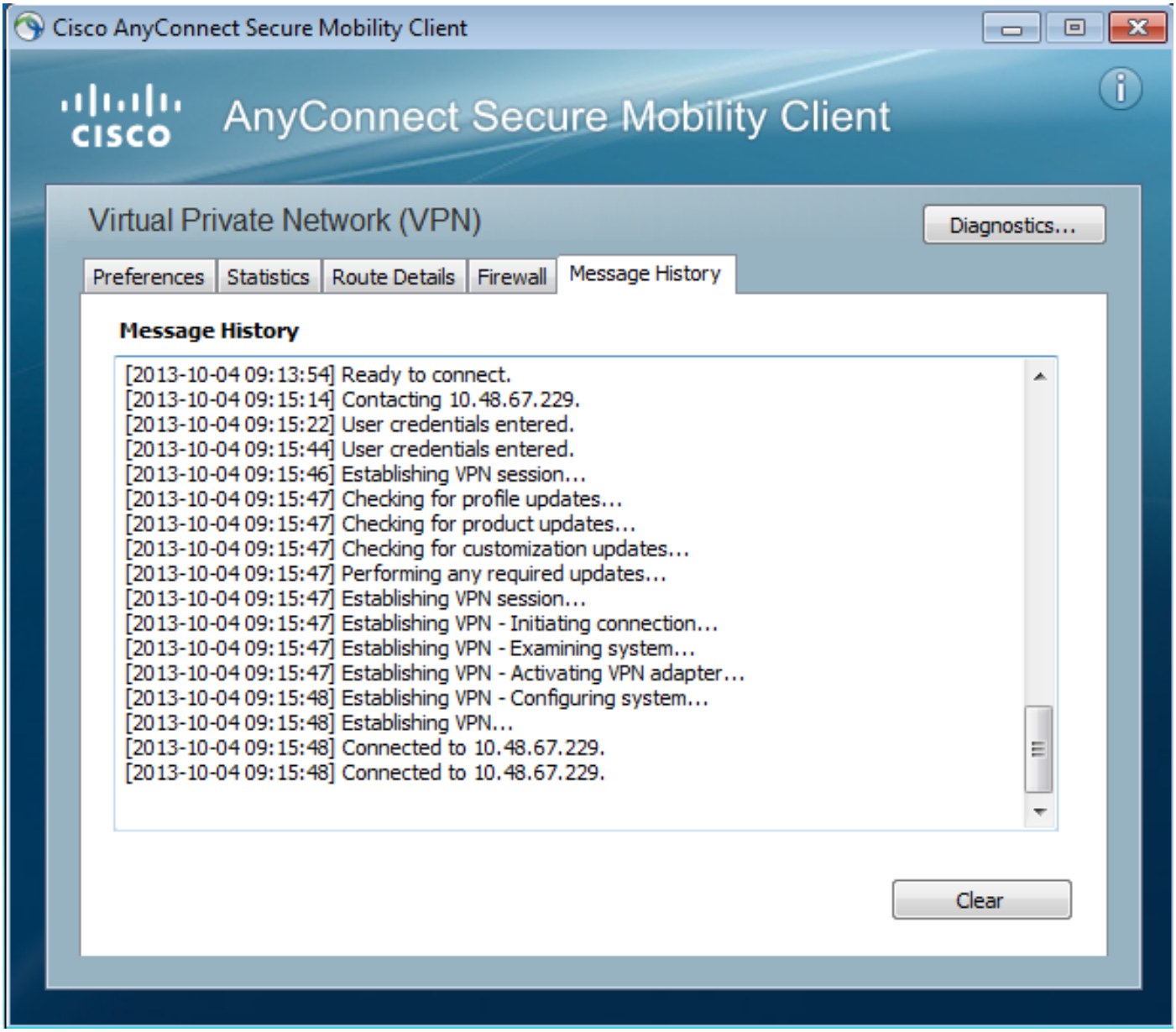
LDAP su SSL:

```
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
```

Dopo aver fornito la password corretta (scaduta), Cisco AnyConnect tenta di connettersi e chiede una nuova password:



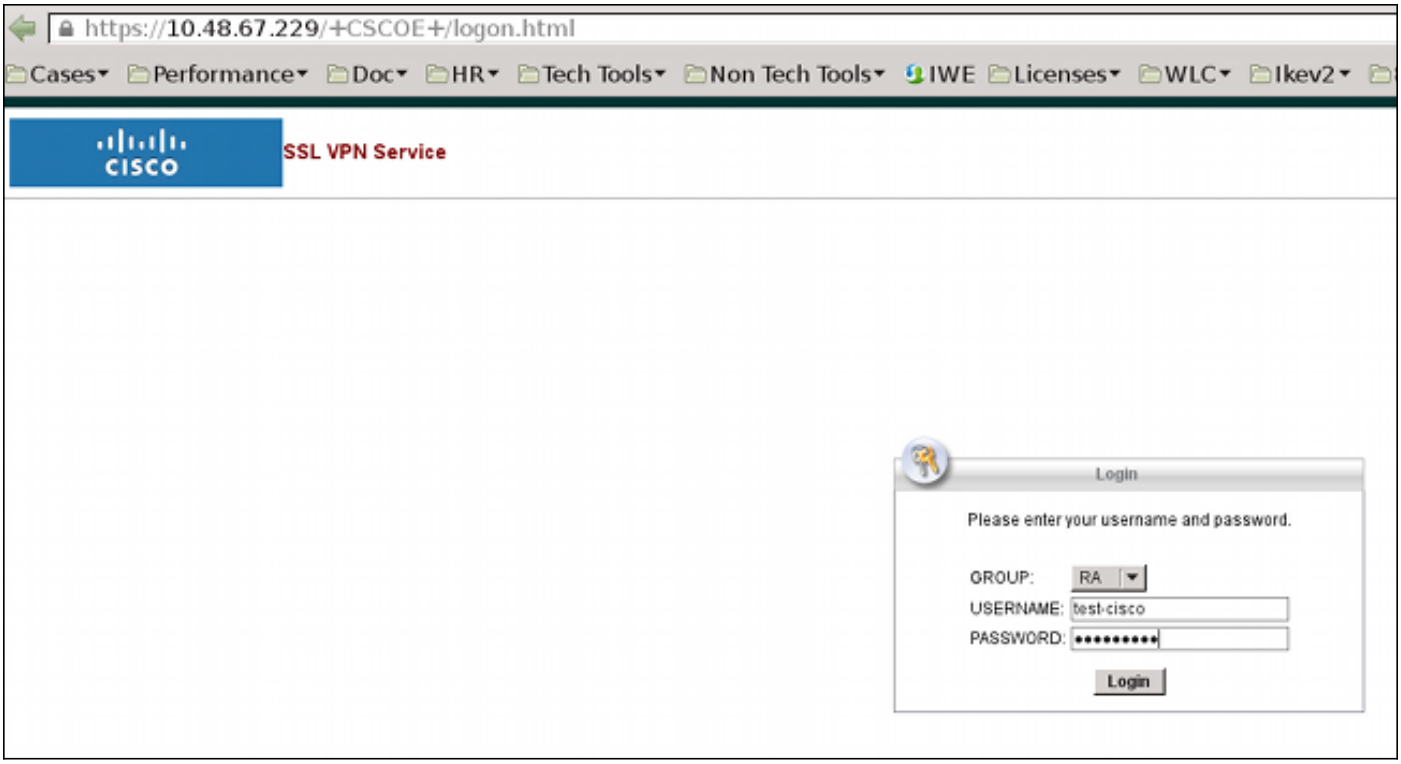
I registri indicano che le credenziali utente sono state immesse due volte:



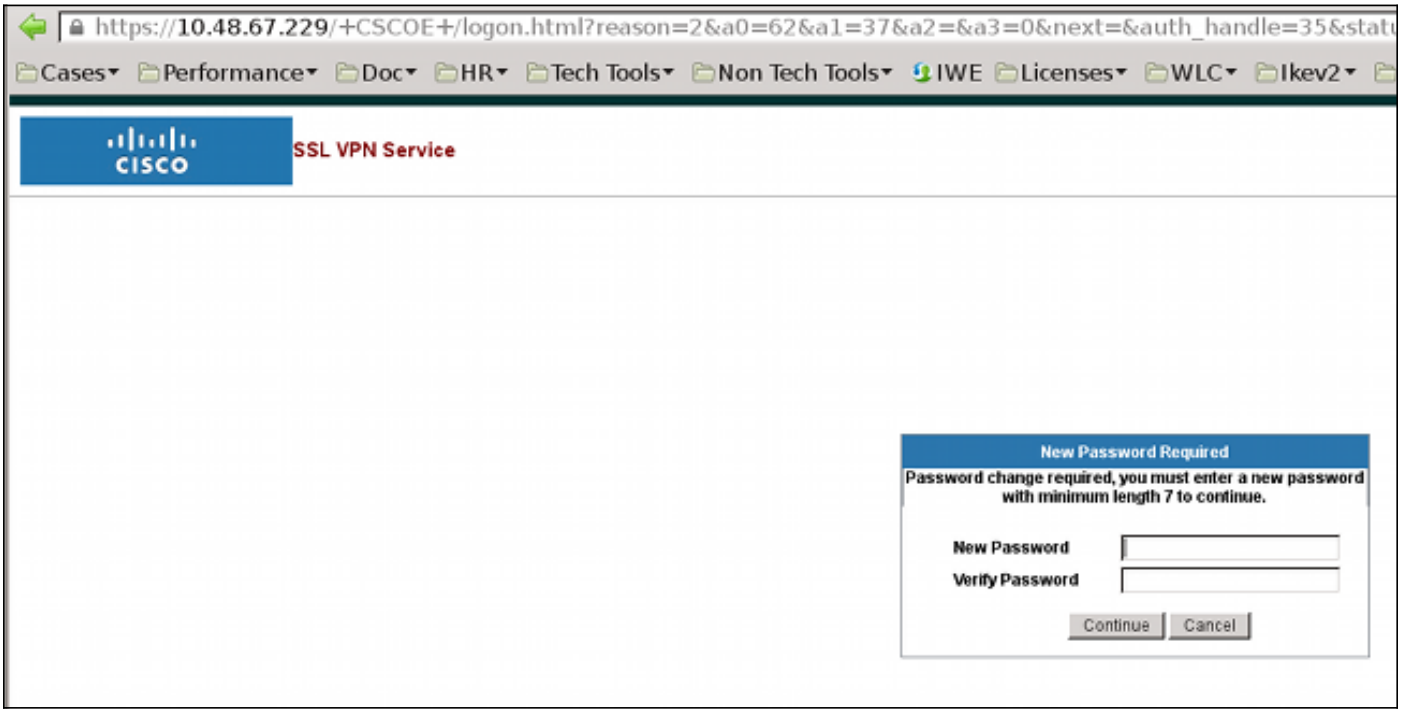
Log più dettagliati sono disponibili nello strumento di report AnyConnect (DART) per la diagnostica.

Portale Web ASA SSL

Lo stesso processo di accesso viene eseguito nel portale Web:



La scadenza e il processo di modifica della password sono gli stessi:



Cambia password utente ACS

Se non è possibile modificare la password sulla VPN, è possibile utilizzare il servizio Web dedicato ACS User Change Password (UCP). Vedere [la guida dello sviluppatore di software per Cisco Secure Access Control System 5.4: Utilizzo dei servizi Web UCP].

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Guida alla configurazione di Cisco ASA serie 5500 dall'interfaccia CLI, 8.4 e 8.6: Configurazione di un server esterno per l'autorizzazione utente di Security Appliance
- Documentazione e supporto tecnico – Cisco Systems