Ejemplo de Configuración de ASA Remote Access VPN IKE/SSL - Caducidad y Cambio de Contraseña para RADIUS, TACACS y LDAP

Contenido

Introducción

Este documento describe las funciones de caducidad de contraseña y cambio de contraseña en un túnel VPN de acceso remoto finalizado en un Cisco Adaptive Security Appliance (ASA). El documento abarca:

- Clientes diferentes: Cisco VPN Client y Cisco AnyConnect Secure Mobility
- Diferentes protocolos: TACACS, RADIUS y protocolo ligero de acceso a directorios (LDAP)
- Diferentes almacenes en Cisco Secure Access Control System (ACS): Directorio local y Active Directory (AD)

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de la configuración de ASA a través de la interfaz de línea de comandos (CLI)
- Conocimiento básico de la configuración de VPN en un ASA
- Conocimiento básico de Cisco Secure ACS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Adaptive Security Appliance, versión 8.4 y posteriores
- Microsoft Windows Server 2003 SP1
- Cisco Secure Access Control System, versión 5.4 o posterior
- Cisco AnyConnect Secure Mobility, versión 3.1
- Cisco VPN Client, versión 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.

Configurar

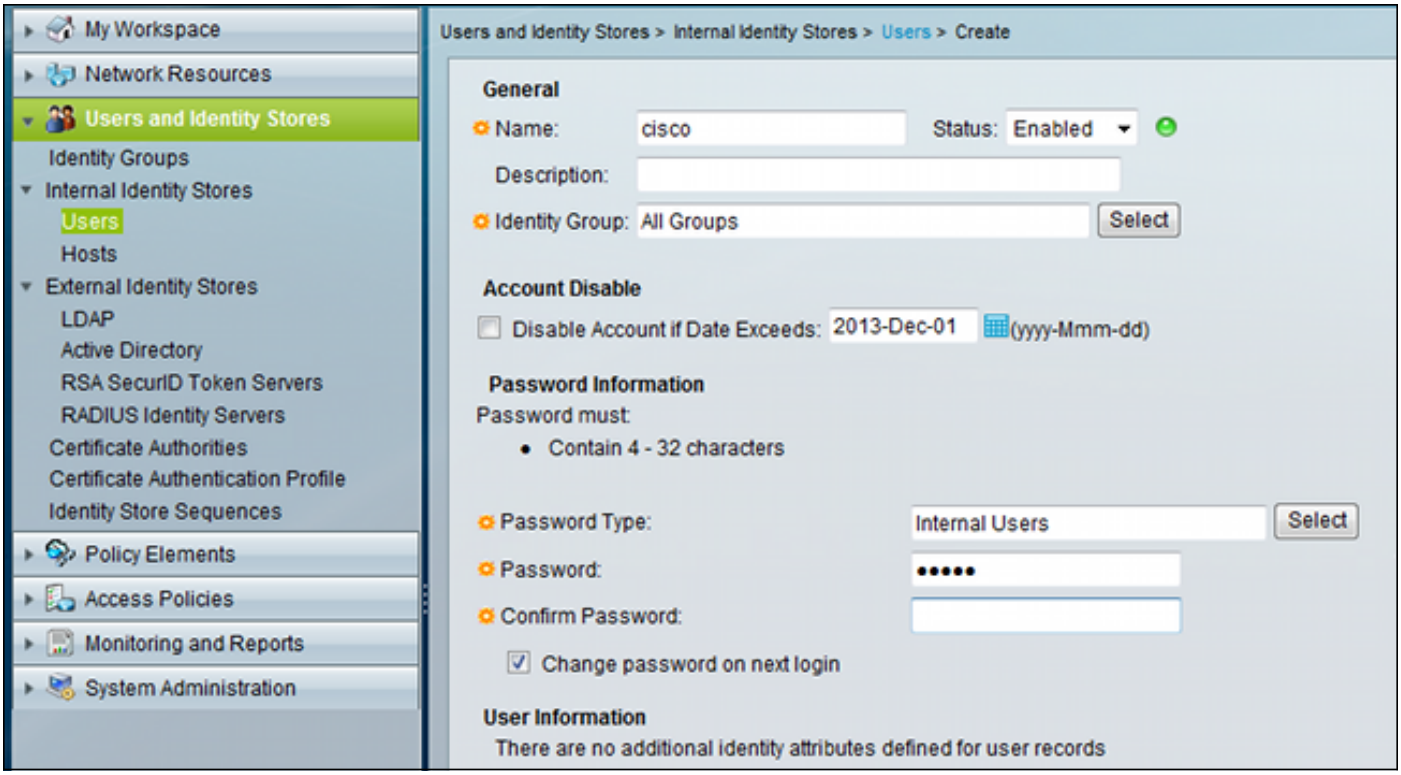
> **Notas:**
>
> Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.
>
> Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

ASA con autenticación local

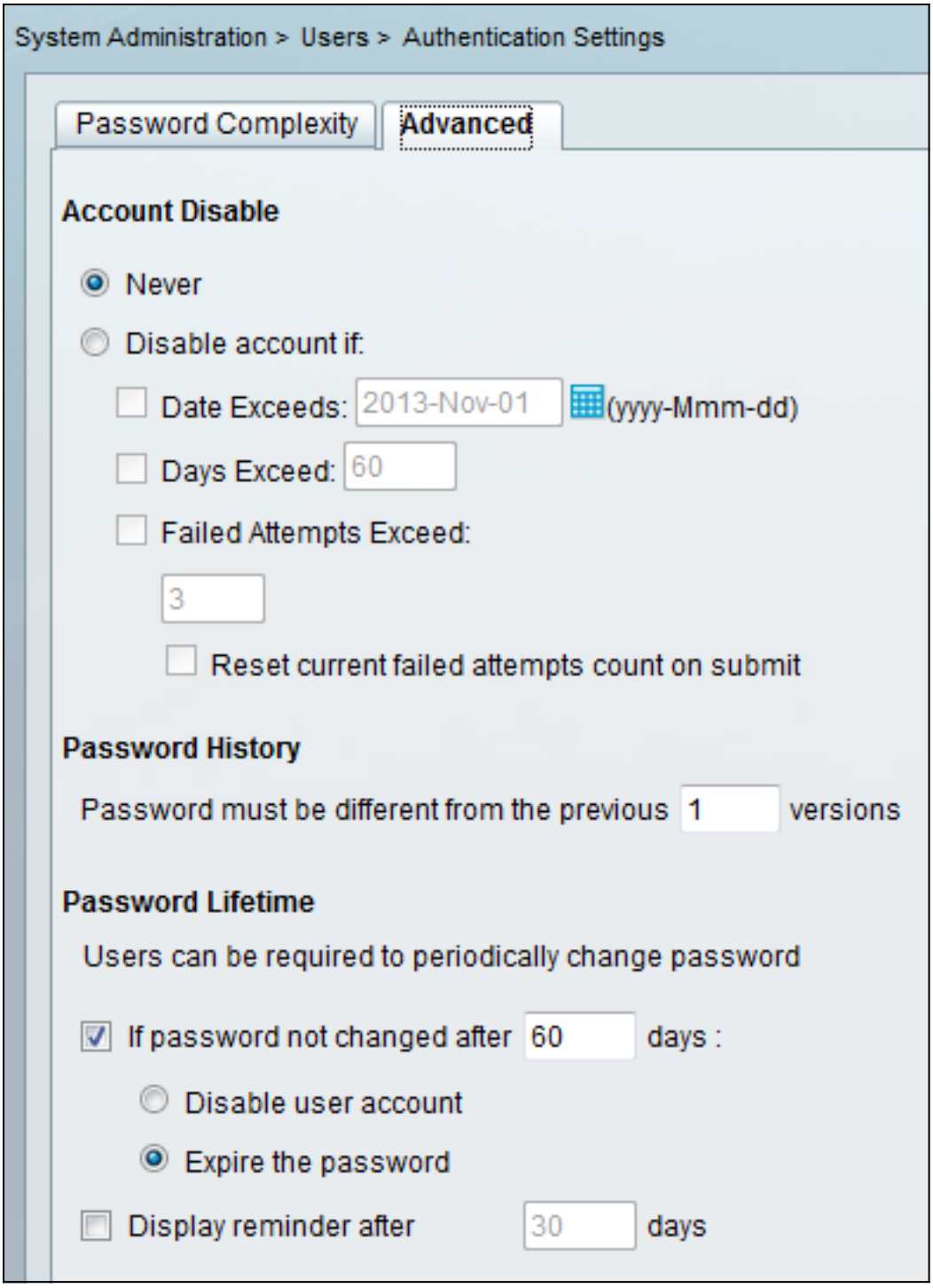
Un ASA con usuarios definidos localmente no permite el uso de funciones de caducidad de contraseña o cambio de contraseña. Se requiere un servidor externo, como RADIUS, TACACS, LDAP o Windows NT.

ACS y usuarios locales

ACS admite el vencimiento de la contraseña y el cambio de la contraseña para los usuarios definidos localmente. Por ejemplo, puede obligar a los usuarios recién creados a cambiar su contraseña en el siguiente inicio de sesión, o puede inhabilitar una cuenta en una fecha específica:

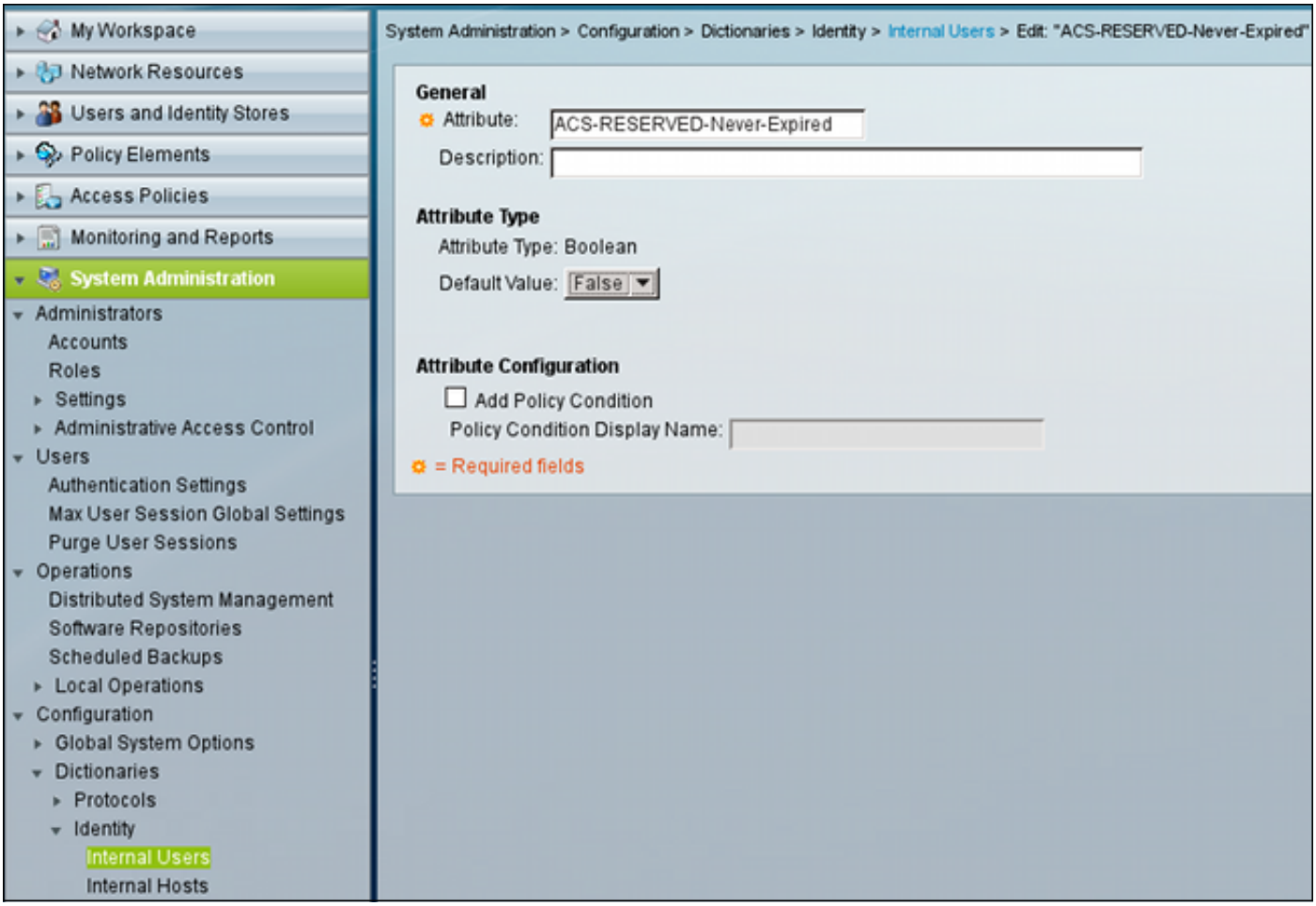


Puede configurar una política de contraseñas para todos los usuarios. Por ejemplo, después de que caduque una contraseña, puede desactivar la cuenta de usuario (bloquearla sin tener que iniciar sesión) o puede ofrecer la opción de cambiar la contraseña:

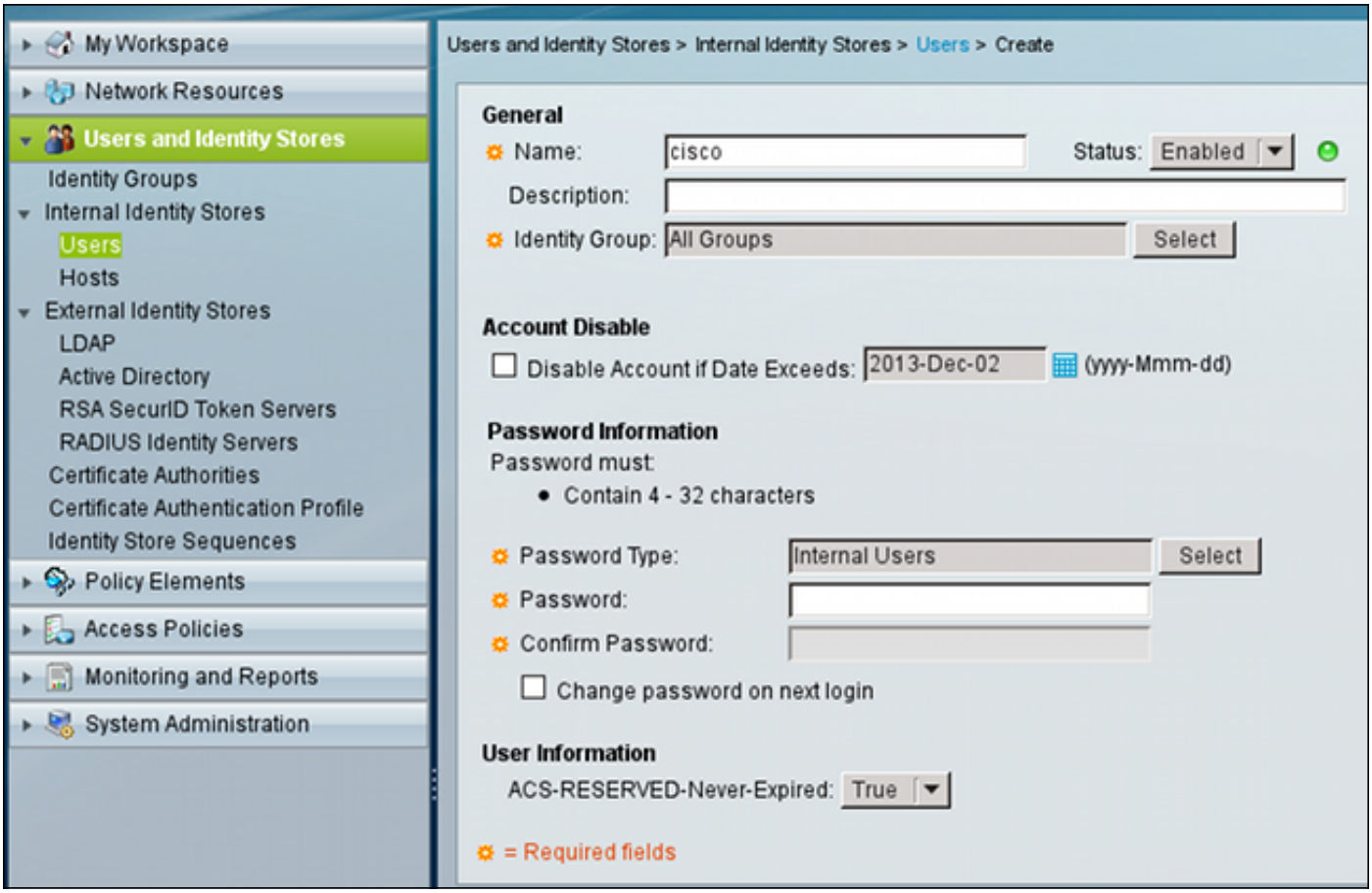


La configuración específica del usuario tiene prioridad sobre la configuración global.

ACS-RESERVED-Never-Expired es un atributo interno para la identidad del usuario.



Este atributo lo habilita el usuario y se puede utilizar para inhabilitar la configuración de vencimiento de la cuenta global. Con esta configuración, una cuenta no se inhabilita incluso si la política global indica que debe ser:

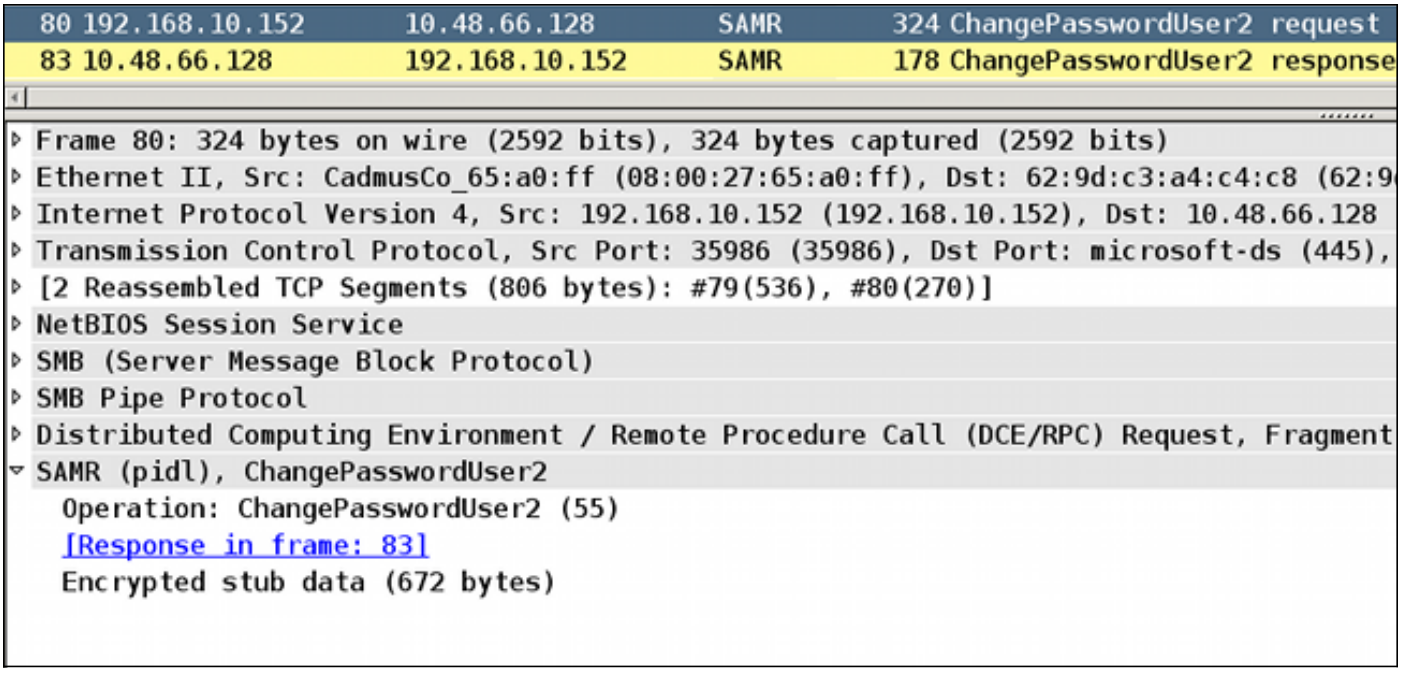


Usuarios de ACS y Active Directory

ACS se puede configurar para verificar los usuarios en una base de datos AD. La caducidad y el cambio de la contraseña se admiten cuando se utiliza Microsoft Challenge Handshake Authentication Protocol versión 2 (MSCHAPv2); consulte la guía del usuario de Cisco Secure Access Control System 5.4: Autenticación en ACS 5.4: Compatibilidad del protocolo de autenticación y del almacén de identidad para obtener más información.

En un ASA, puede utilizar la función de administración de contraseñas, como se describe en la siguiente sección, para forzar al ASA a utilizar MSCHAPv2.

ACS utiliza la llamada del entorno informático distribuido (CIFS) del sistema de archivos de Internet común/llamada de procedimiento remoto (DCE/RPC) cuando se pone en contacto con el directorio del controlador de dominio (DC) para cambiar la contraseña:



ASA puede utilizar los protocolos RADIUS y TACACS+ para contactar con el ACS para un cambio de contraseña AD.

ASA con ACS a través de RADIUS

El protocolo RADIUS no soporta nativamente la caducidad de la contraseña o el cambio de la contraseña. Normalmente, el protocolo de autenticación de contraseña (PAP) se utiliza para RADIUS. El ASA envía el nombre de usuario y la contraseña en texto sin formato, y la contraseña se cifra a continuación mediante el uso del secreto compartido RADIUS.

En un escenario típico cuando la contraseña de usuario ha caducado, ACS devuelve un mensaje de Rechazo de RADIUS al ASA. ACS observa que:

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

Para el ASA, se trata de un mensaje simple de rechazo de RADIUS y la autenticación falla.

Para resolver este problema, el ASA permite el uso del comando **password-management** bajo la configuración tunnel-group:

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

El comando **password-management** cambia el comportamiento de modo que el ASA se vea obligado a utilizar MSCHAPv2, en lugar de PAP, en la Radius-Request.

El protocolo MSCHAPv2 admite el vencimiento de la contraseña y el cambio de la contraseña. Por lo tanto, si un usuario de VPN ha aterrizado en ese grupo de túnel específico durante la fase Xauth, la Radius-Request de ASA ahora incluye un Desafío MS-CHAP:

```
▼ 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)
```

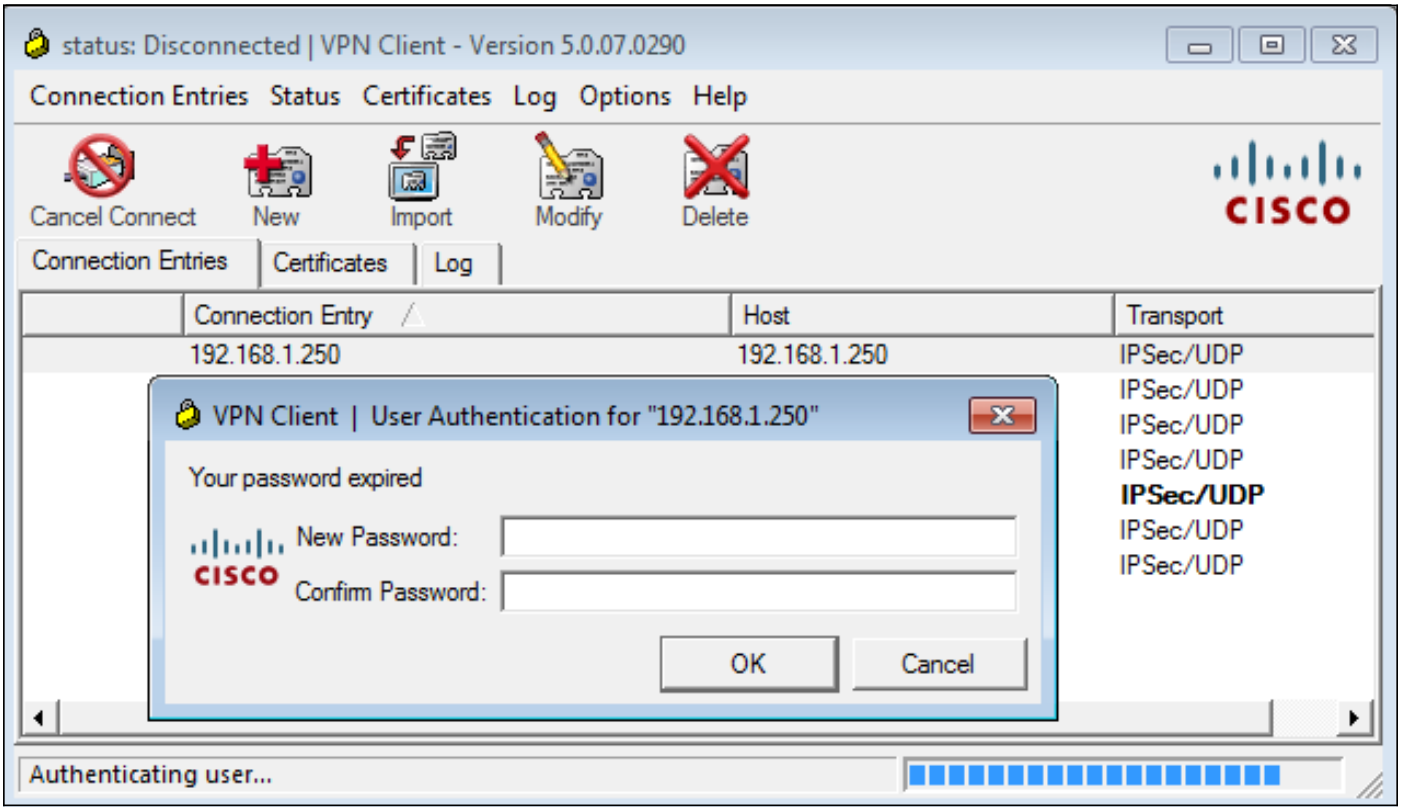
Si el ACS nota que el usuario necesita cambiar la contraseña, devuelve un mensaje Radius-Reject con el error MSCHAPv2 648.

```
▽ 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
```

El ASA entiende ese mensaje y utiliza MODE_CFG para solicitar la nueva contraseña del cliente VPN de Cisco:

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

El cliente Cisco VPN presenta un cuadro de diálogo que solicita una nueva contraseña:



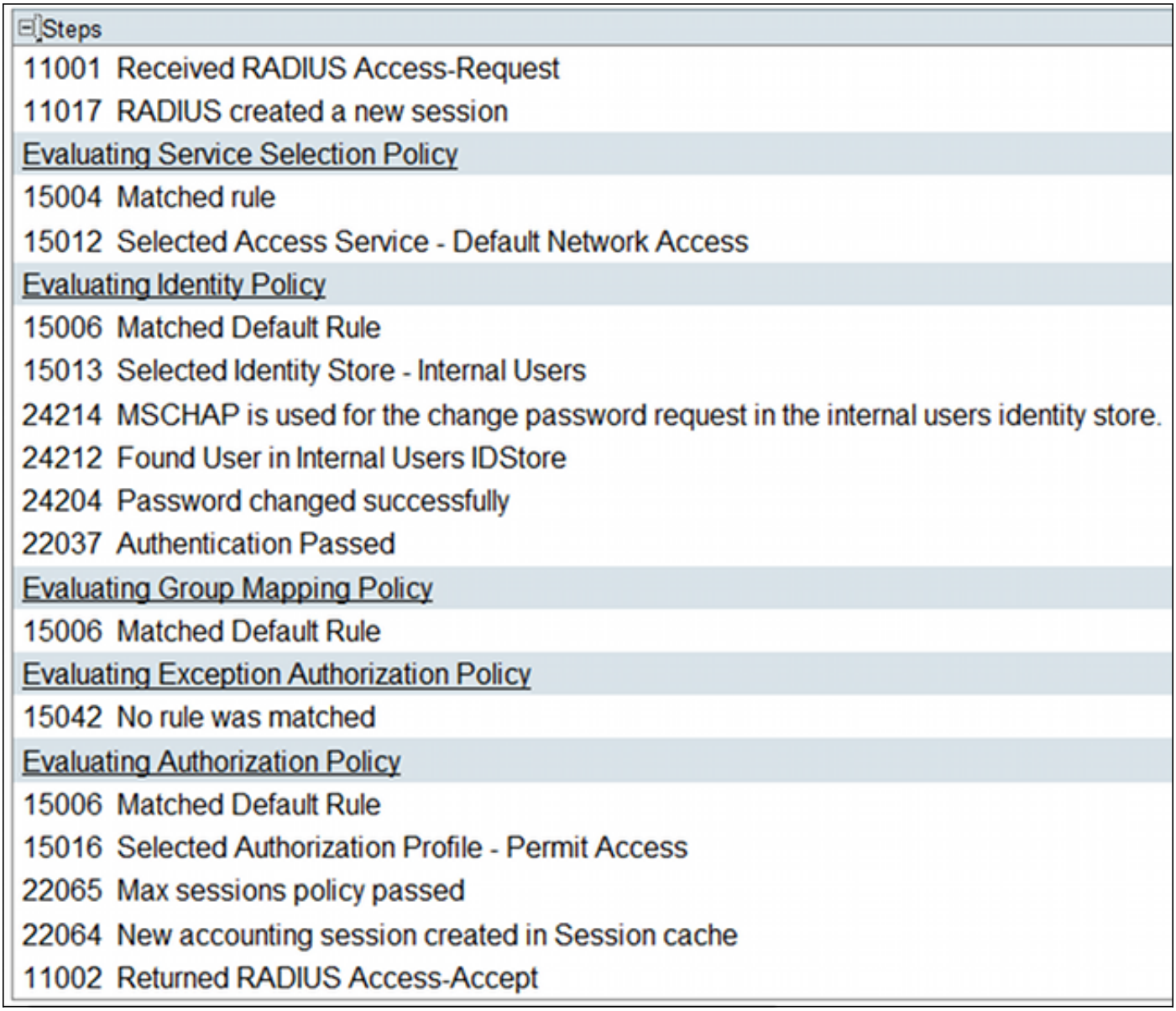
El ASA envía otra solicitud de radio con una carga útil MS-CHAP-CPW y MS-CHAP-NT-Enc-PW (la nueva contraseña):

```
▷ 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)
```

El ACS confirma la solicitud y devuelve un Radius-Accept con MS-CHAP2-Success:

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

Esto se puede verificar en ACS, que informa que la '24204 Password ha cambiado correctamente':



A continuación, ASA informa de que la autenticación se ha realizado correctamente y continúa con el proceso de modo rápido (QM):

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

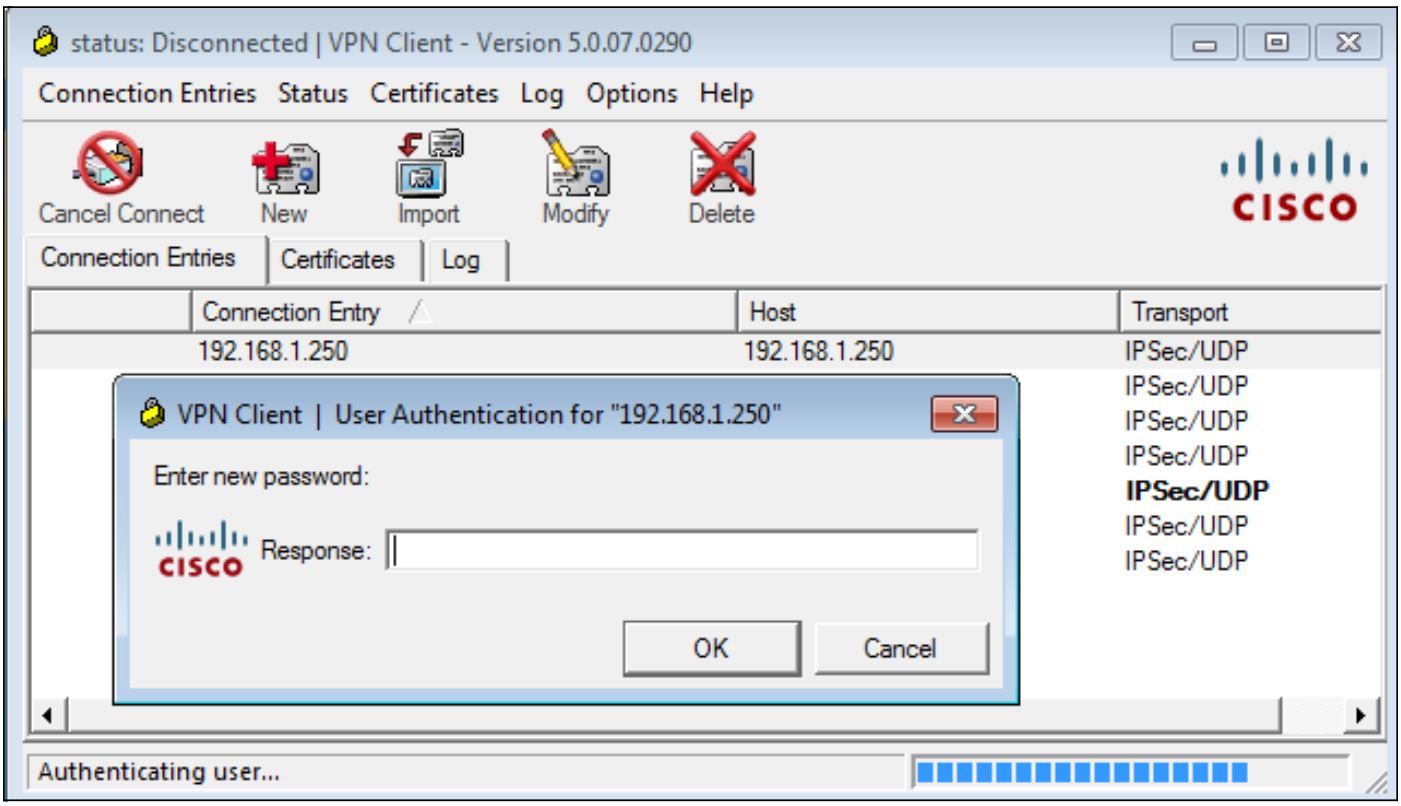
ASA con ACS a través de TACACS+

Asimismo, TACACS+ puede utilizarse para la caducidad y el cambio de la contraseña. La función de administración de contraseñas no es necesaria, ya que ASA todavía utiliza TACACS+ con un tipo de autenticación de ASCII en lugar de MSCHAPv2.

Se intercambian varios paquetes y ACS pide una nueva contraseña:

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

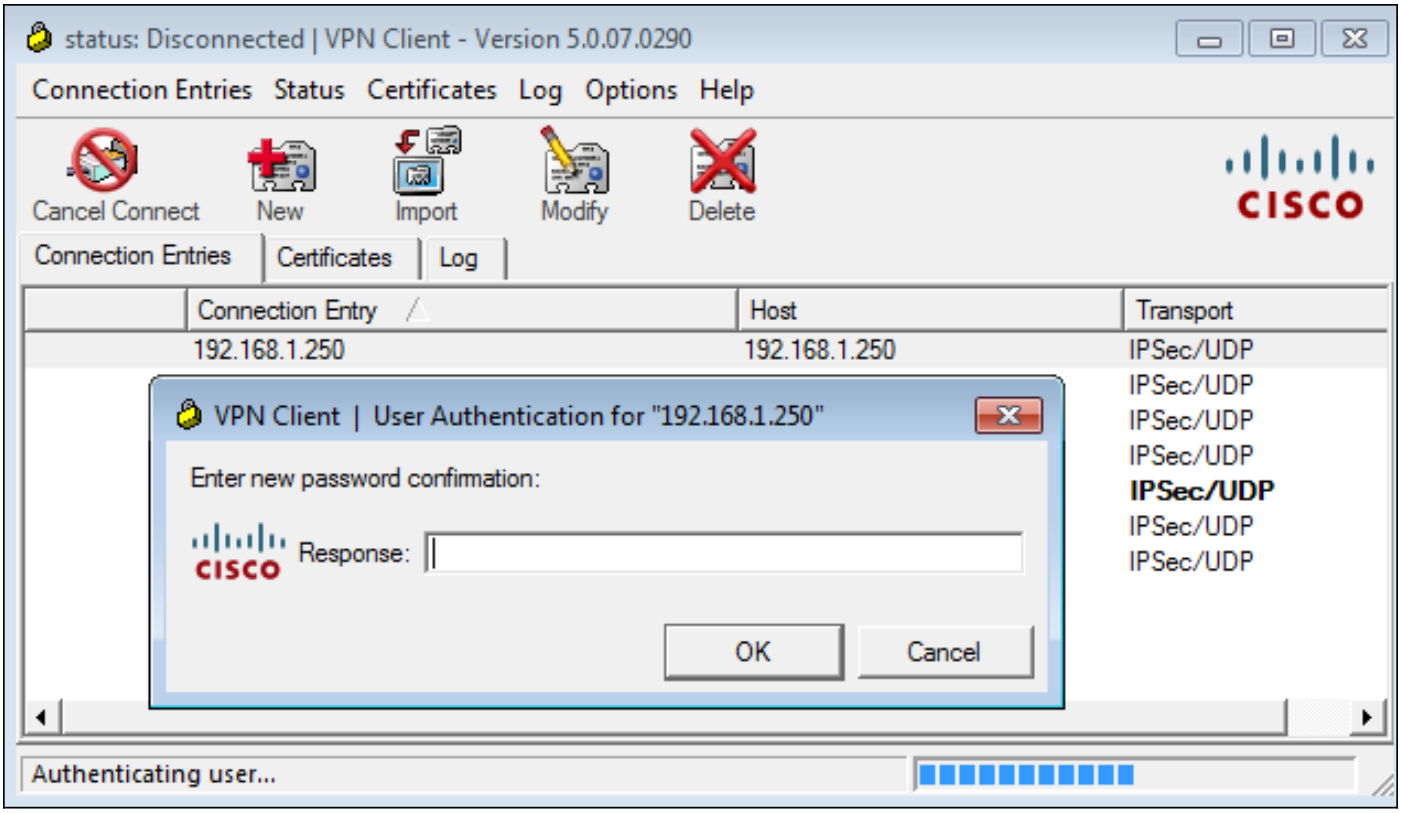
El cliente Cisco VPN presenta un cuadro de diálogo (que difiere del diálogo utilizado por RADIUS) que solicita una nueva contraseña:



ACS solicita confirmación de la nueva contraseña:

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

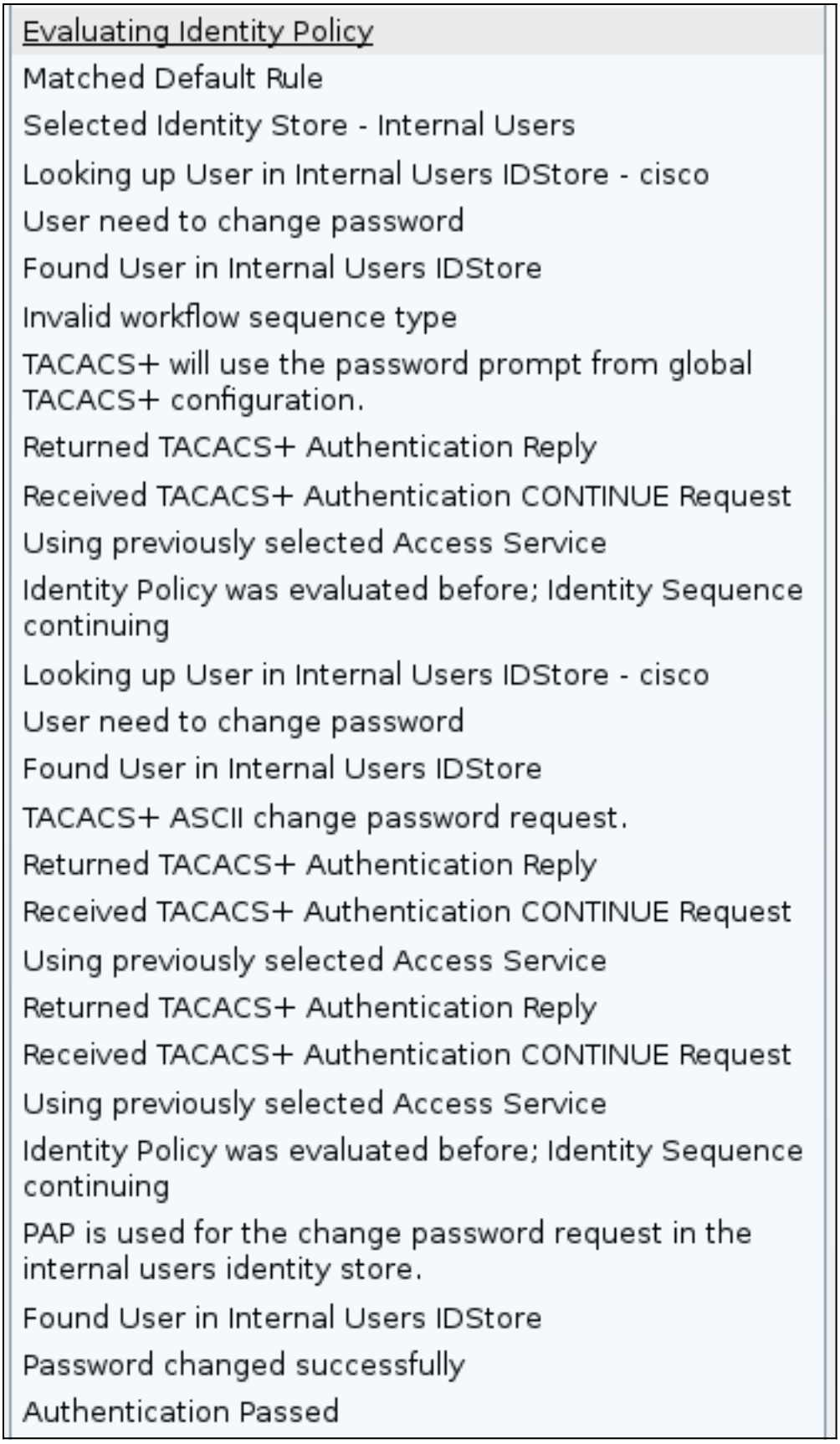
El cliente Cisco VPN presenta una caja de confirmación:



Si la confirmación es correcta, ACS informa una autenticación exitosa:

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

ACS luego registra un evento que la contraseña se ha cambiado correctamente:



Las depuraciones de ASA muestran todo el proceso de intercambio y autenticación exitosa:

```
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.
```

Ese cambio de contraseña es completamente transparente para ASA. Es un poco más larga la sesión TACACS+ con más paquetes de solicitud y respuesta, los cuales son analizados por el cliente VPN y presentados al usuario que está cambiando la contraseña.

ASA con LDAP

La caducidad y el cambio de la contraseña son totalmente compatibles con el esquema del servidor LDAP de Microsoft AD y Sun.

Para un cambio de contraseña, los servidores devuelven 'bindresponse = invalidCredentials' con 'error = 773'. Este error indica que el usuario debe restablecer la contraseña. Los códigos de error típicos incluyen:

Código de error	Error
525	Usuario no encontrado
52 sexies	Credenciales no válidas
530	No se permite el inicio de sesión en este momento
531	No se permite iniciar sesión en esta estación de trabajo
532	La contraseña ha caducado
533	Cuenta desactivada
701	La cuenta ha caducado
773	El usuario debe restablecer la contraseña
775	Cuenta de usuario bloqueada

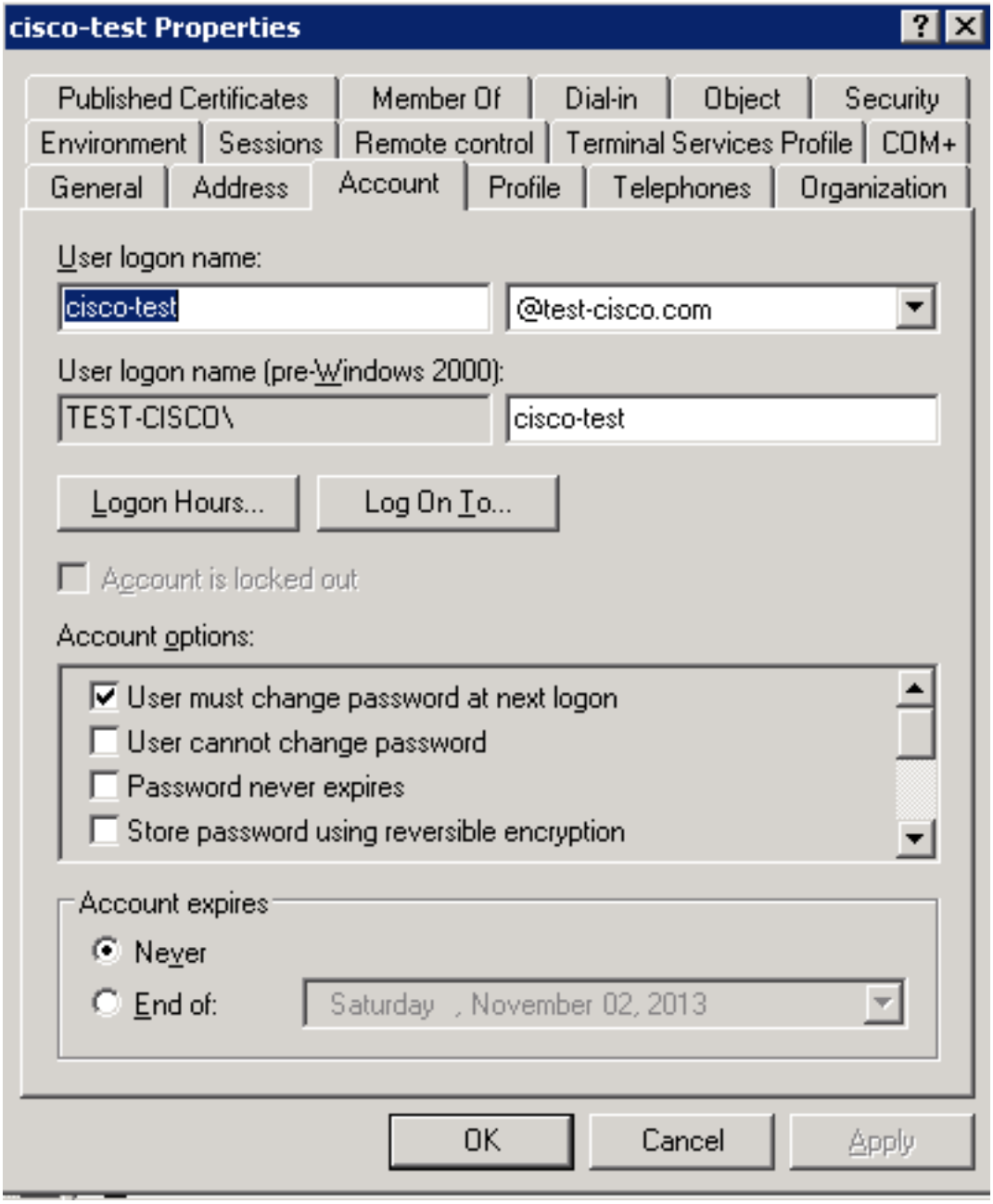
Configure el servidor LDAP:

```
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
```

Utilice esa configuración para el grupo de túnel y la función de administración de contraseñas:

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

Configure el usuario de AD para que se requiera un cambio de contraseña:



Cuando el usuario intenta utilizar el cliente Cisco VPN, ASA informa una contraseña no válida:

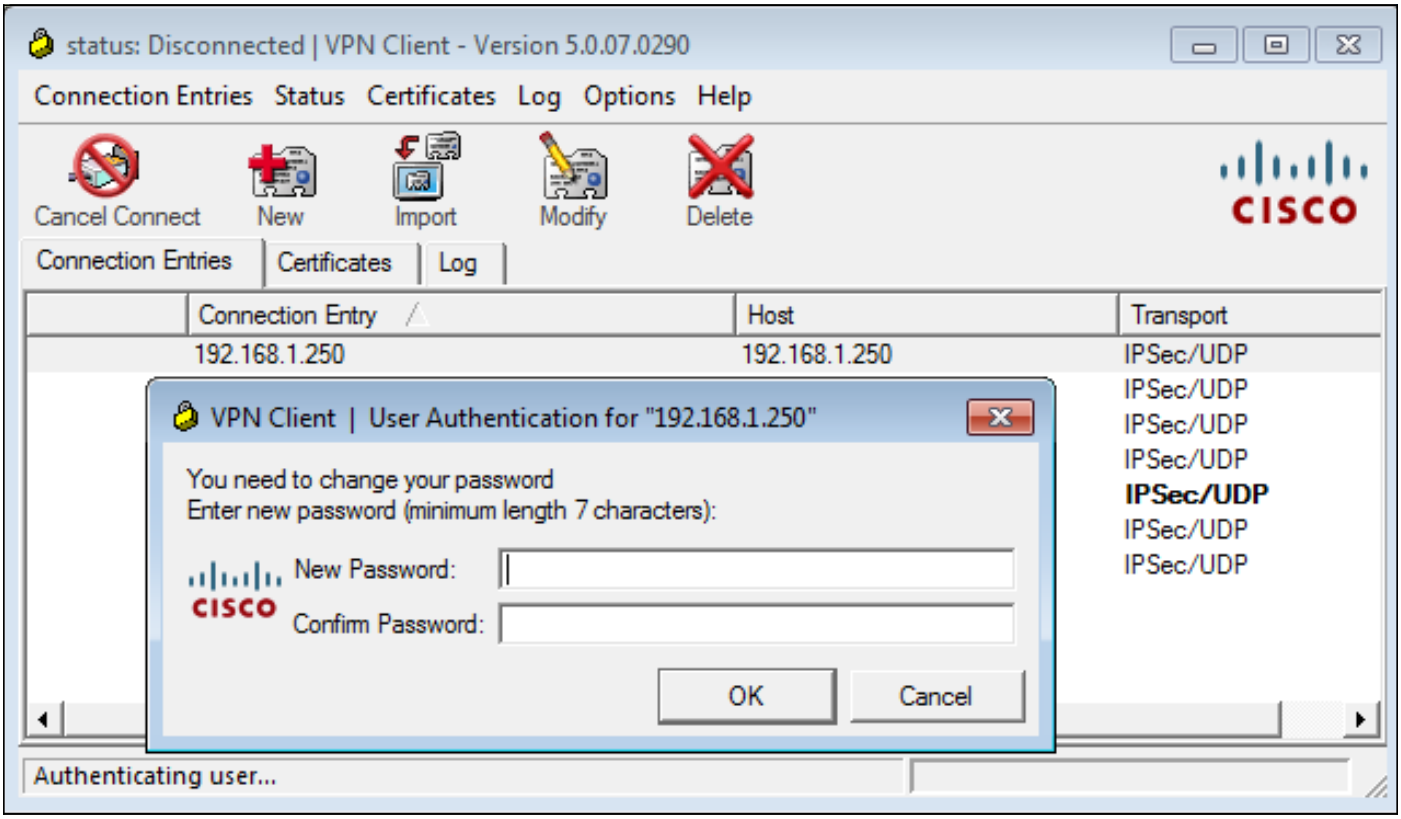
```
ASA(config-tunnel-general)# debug ldap 255
<some output ommited for clarity>

[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
```

Si las credenciales no son válidas, aparece el error 52e:

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

A continuación, el cliente VPN de Cisco solicita un cambio de contraseña:



Este cuadro de diálogo difiere del diálogo utilizado por TACACS o RADIUS porque muestra la política. En este ejemplo, la política es una longitud mínima de contraseña de siete caracteres.

Una vez que el usuario cambia la contraseña, el ASA podría obtener este mensaje de error del servidor LDAP:

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

La política de Microsoft requiere el uso de Secure Sockets Layer (SSL) para la modificación de la contraseña. Cambie la configuración:

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

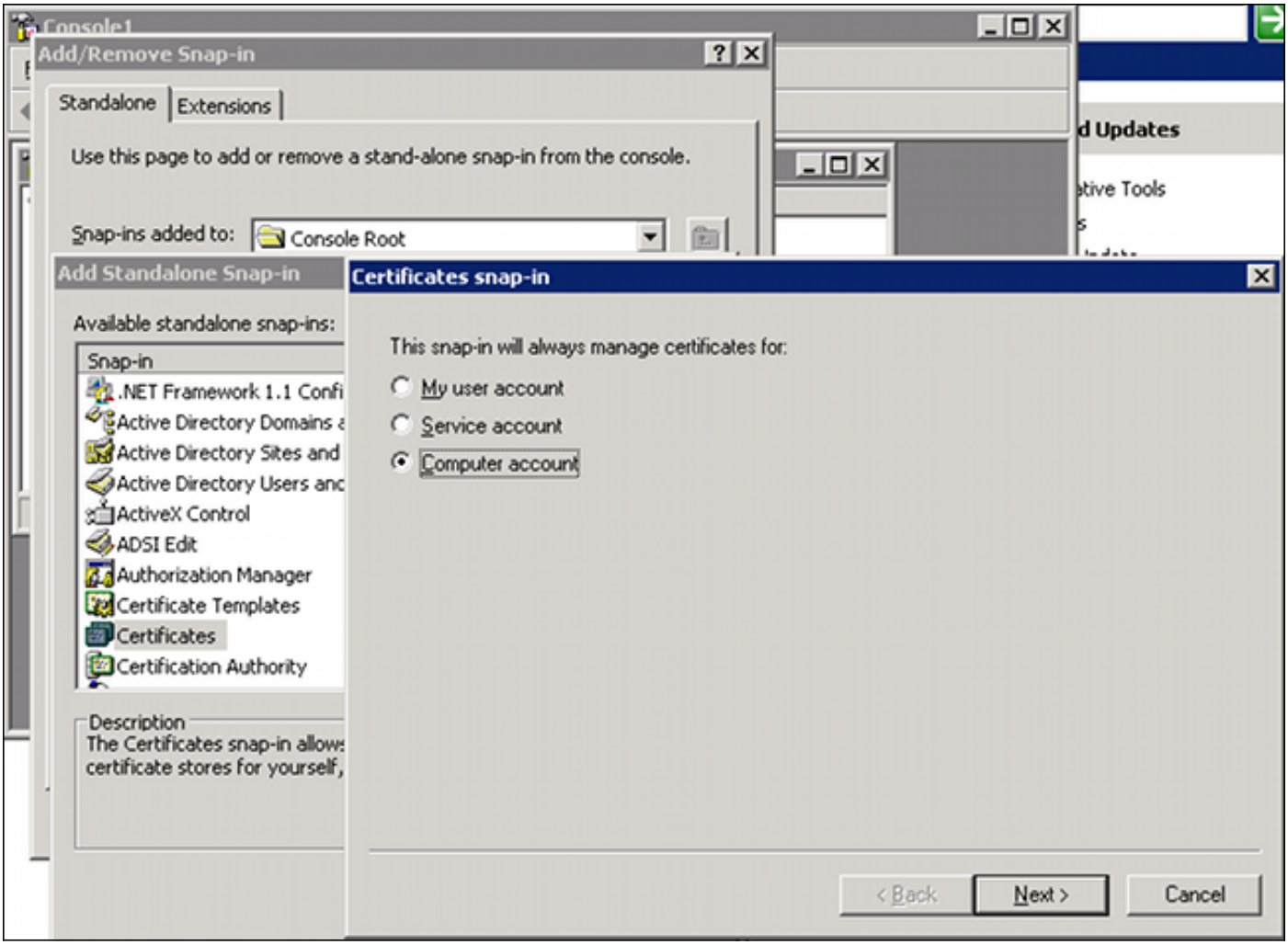
Microsoft LDAP para SSL

De forma predeterminada, Microsoft LDAP sobre SSL no funciona. Para habilitar esta función, debe instalar el certificado para la cuenta del equipo con la extensión de clave correcta. Consulte Cómo habilitar LDAP sobre SSL con una entidad de certificación de terceros para obtener más detalles.

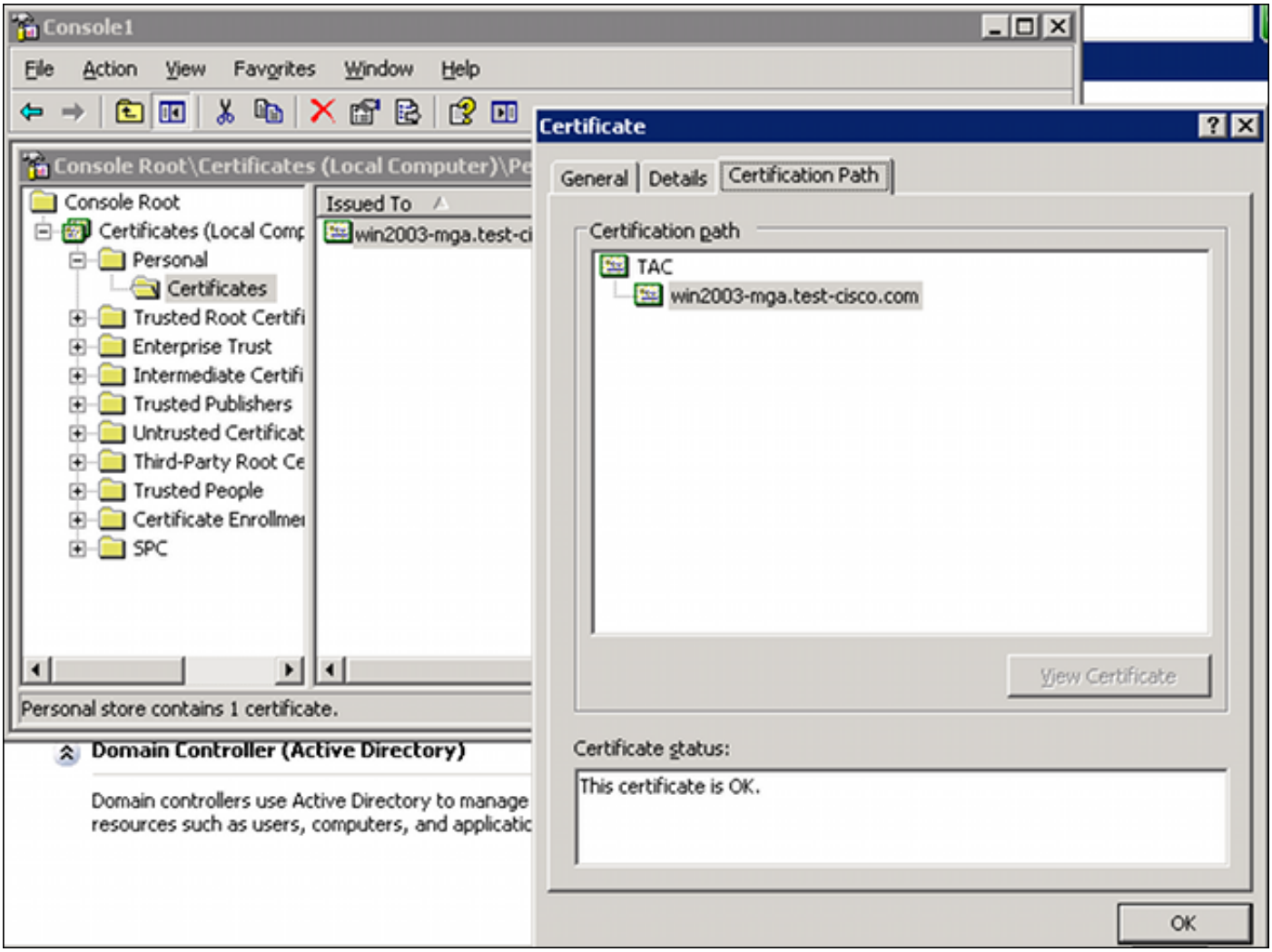
El certificado puede incluso ser un certificado autofirmado porque el ASA no verifica el certificado LDAP. Consulte Cisco Bug ID CSCui40212, "Permitir que ASA valide el certificado del servidor LDAPS" para obtener una solicitud de mejora relacionada.

> **Nota:** ACS verifica el certificado LDAP en la versión 5.5 y posteriores.

Para instalar el certificado, abra la consola mmc, seleccione **Agregar/Quitar complemento**, agregue el certificado y elija **Cuenta de equipo**:



Seleccione **Equipo local**, importe el certificado al almacén personal y mueva el certificado de autoridad certificadora (CA) asociado al almacén de confianza. Verifique que el certificado sea de confianza:



Hay un error en la versión 8.4.2 de ASA, donde este error puede ser devuelto cuando intenta utilizar LDAP sobre SSL:

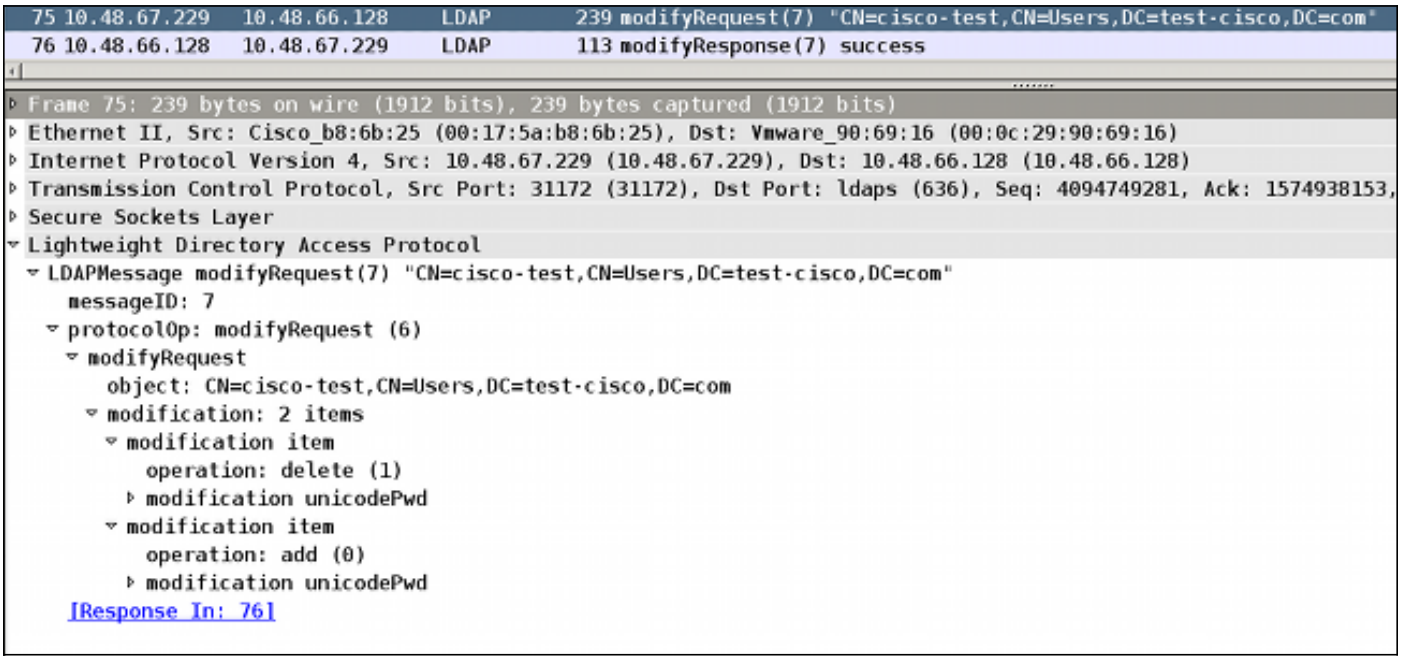
```
ASA(config)# debug ldap 255

[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
```

La versión 9.1.3 de ASA funciona correctamente con la misma configuración. Hay dos sesiones LDAP. La primera sesión devuelve un error con el código 773 (la contraseña venció), mientras que la segunda sesión se utiliza para el cambio de contraseña:

```
[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)
```

Para verificar el cambio de contraseña, observe los paquetes. Wireshark puede utilizar la clave privada del servidor LDAP para descifrar el tráfico SSL:



Las depuraciones de Intercambio de claves de Internet (IKE)/Autenticación, Autorización y Contabilización (AAA) en ASA son muy similares a las presentadas en el escenario de autenticación RADIUS.

LDAP y advertencia antes del vencimiento

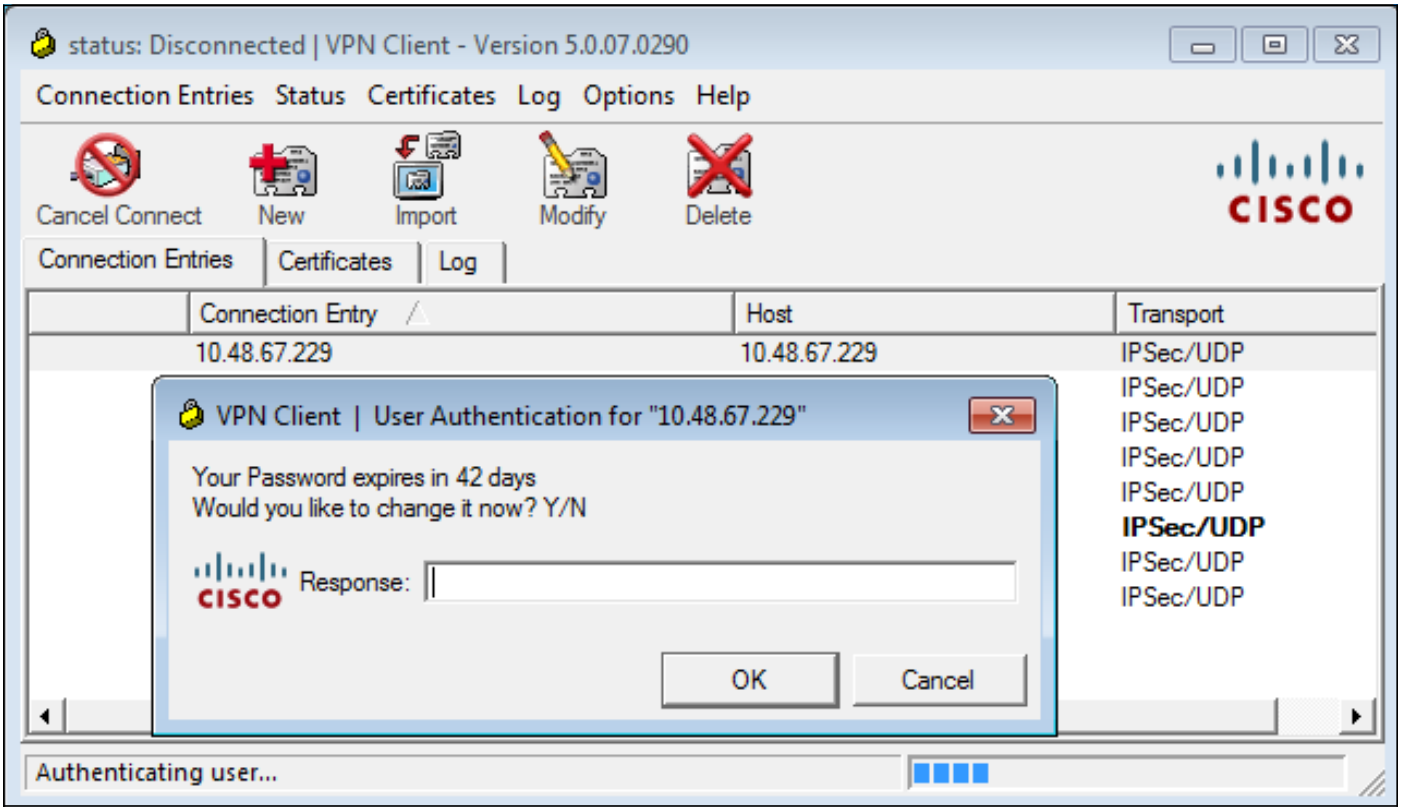
Para LDAP, puede utilizar una función que envía una advertencia antes de que caduque una contraseña. El ASA advierte al usuario 90 días antes del vencimiento de la contraseña con esta configuración:

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

Aquí la contraseña caduca en 42 días y el usuario intenta iniciar sesión:

```
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
```

El ASA envía una advertencia y ofrece la opción de un cambio de contraseña:



Si el usuario decide cambiar la contraseña, se le solicita una nueva contraseña y se inicia el procedimiento normal de cambio de contraseña.

ASA y L2TP

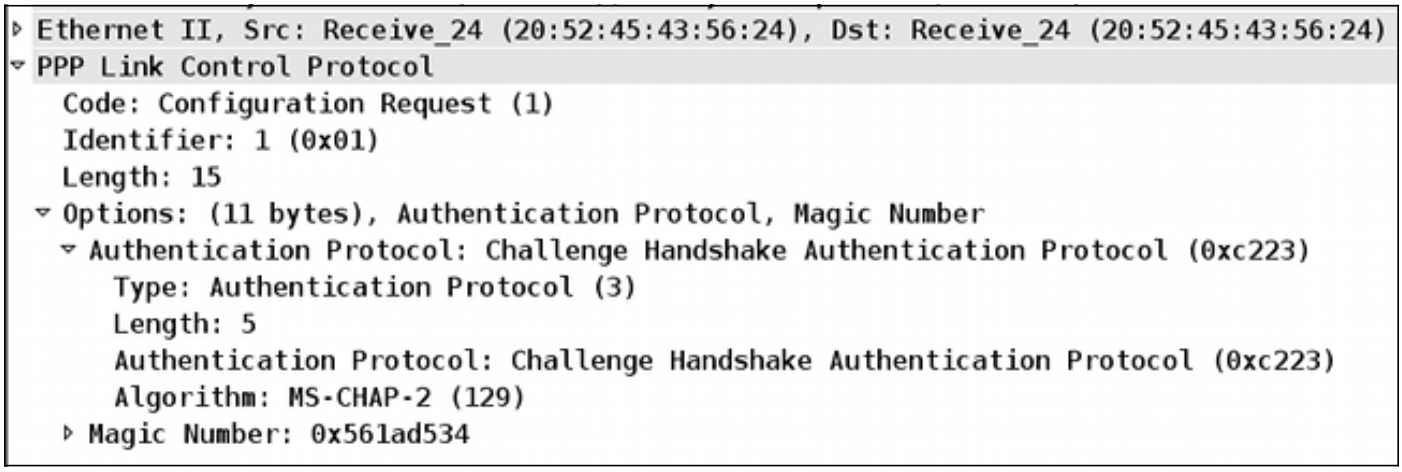
Los ejemplos anteriores presentaban IKE versión 1 (IKEv1) y una VPN IPSec.

Para el protocolo de túnel de capa 2 (L2TP) e IPSec, PPP se utiliza como transporte para la autenticación. Se requiere MSCHAPv2 en lugar de PAP para que funcione un cambio de contraseña:

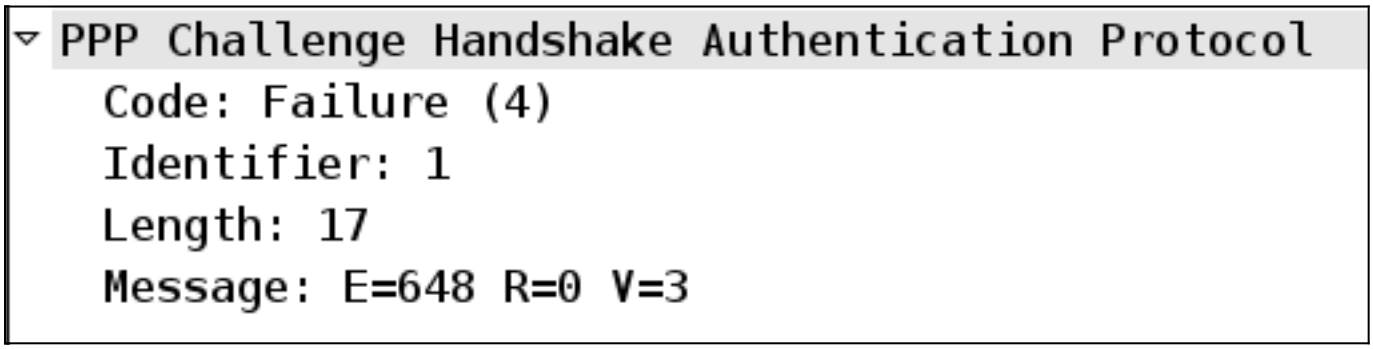
```
ciscoasa(config-tunnel-general)# tunnel-group DefaultRAGroup ppp-attributes
```

```
ciscoasa(config-ppp)# authentication ms-chap-v2
```

Para la autenticación extendida en L2TP dentro de la sesión PPP, se negocia MSCHAPv2:



Cuando la contraseña de usuario ha caducado, se devuelve un error con el código 648:



A continuación, se necesita un cambio de contraseña. El resto del proceso es muy similar al escenario para RADIUS con MSCHAPv2.

Consulte Ejemplo de Configuración de L2TP a través de IPSec entre Windows 2000/XP PC y PIX/ASA 7.2 Usando Clave Previamente Compartida para obtener detalles adicionales sobre cómo configurar L2TP.

Cliente VPN SSL ASA

Los ejemplos anteriores se referían a IKEv1 y al cliente Cisco VPN, que es el fin de vida útil (EOL).

La solución recomendada para una VPN de acceso remoto es Cisco AnyConnect Secure Mobility, que utiliza los protocolos IKE versión 2 (IKEv2) y SSL. Las funciones de cambio de contraseña y caducidad funcionan exactamente igual para Cisco AnyConnect que para el cliente Cisco VPN.

Para IKEv1, los datos de cambio y vencimiento de la contraseña se intercambiaron entre el ASA y el cliente VPN en la fase 1.5 (Xauth/mode config).

Para IKEv2, es similar; el modo de configuración utiliza paquetes CFG_REQUEST/CFG_REPLY.

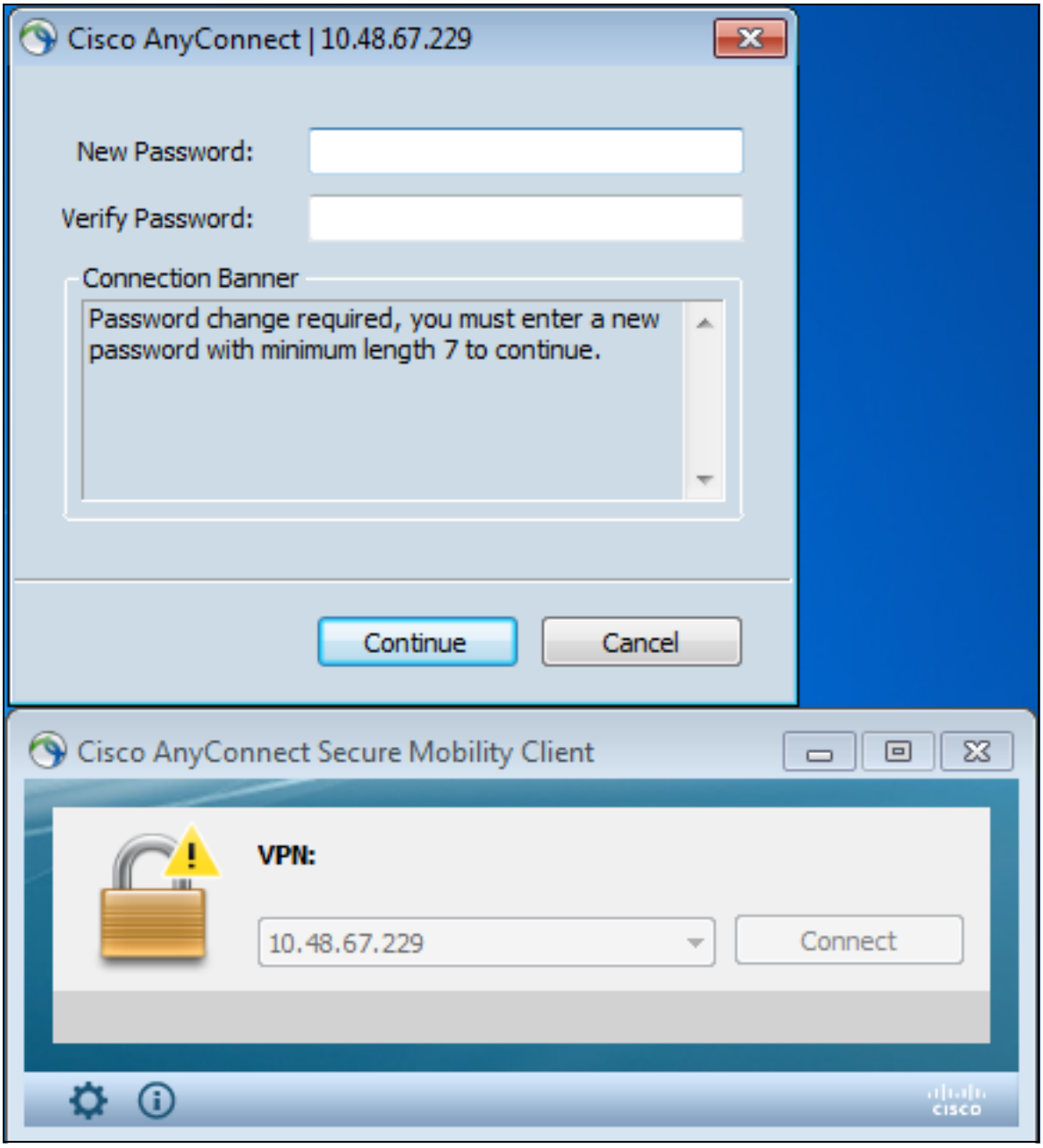
Para SSL, los datos se encuentran en la sesión de control Datagram Transport Layer Security (DTLS).

La configuración es la misma para el ASA.

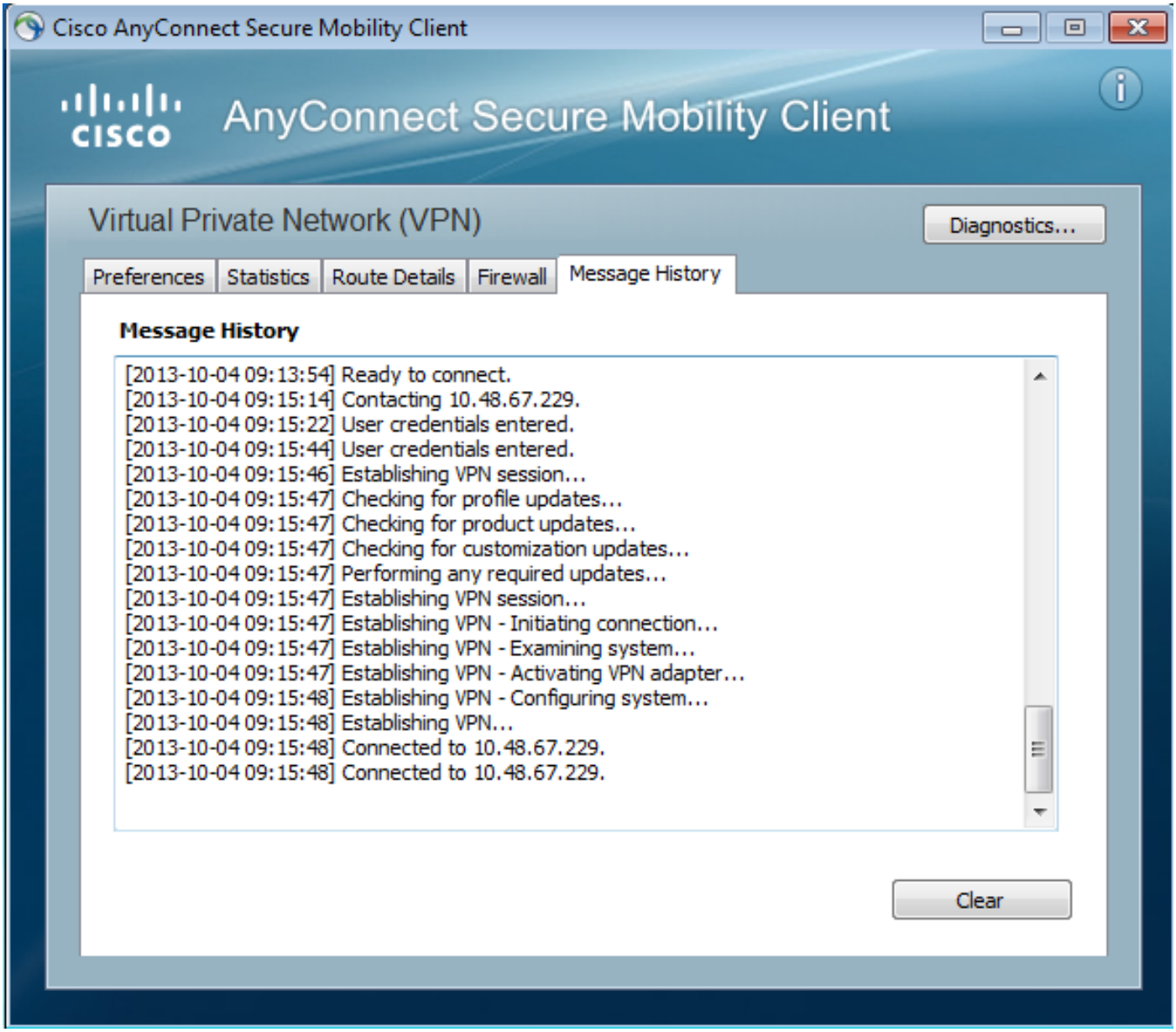
Este es un ejemplo de configuración con Cisco AnyConnect y el protocolo SSL con un servidor LDAP sobre SSL:

```
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
```

Una vez proporcionada la contraseña correcta (que ha caducado), Cisco AnyConnect intenta conectarse y solicita una nueva contraseña:



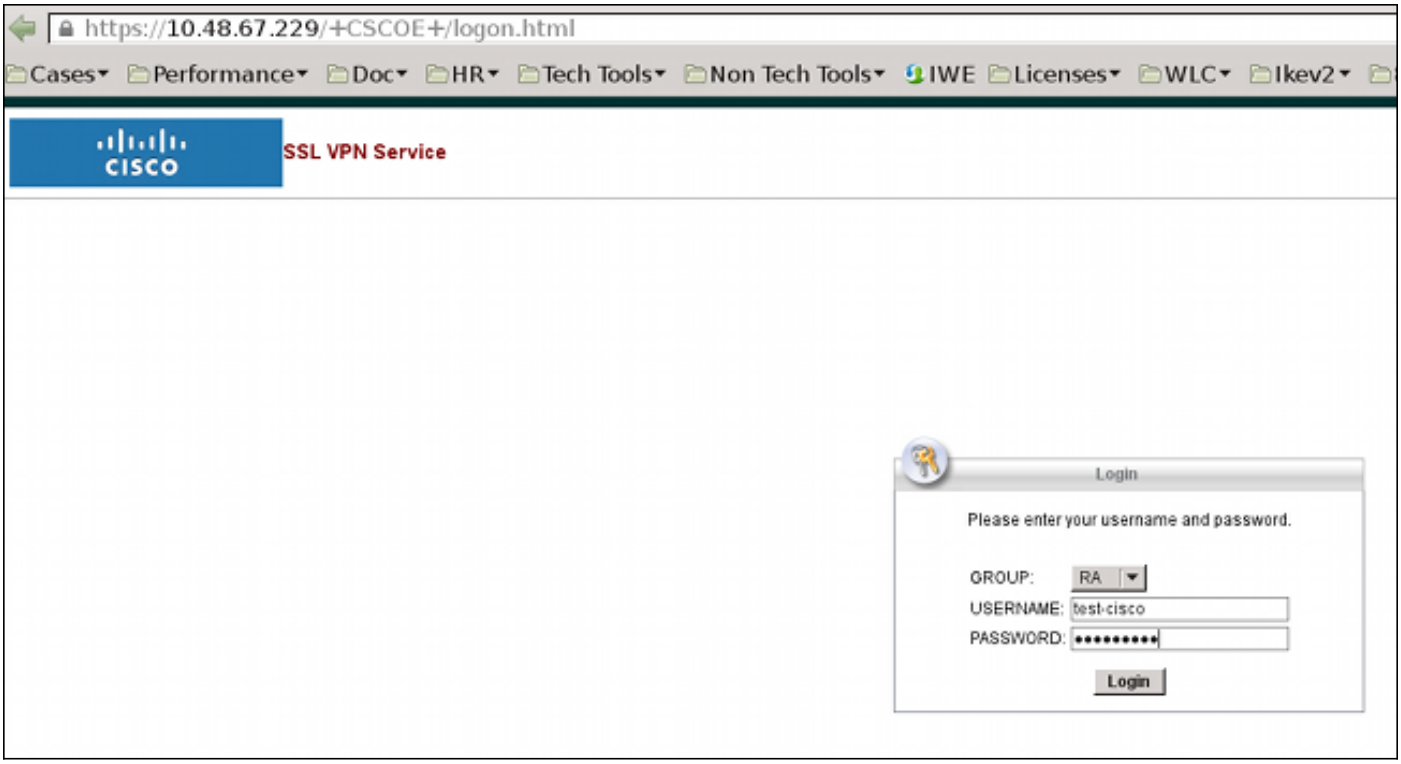
Los registros indican que las credenciales de usuario se ingresaron dos veces:



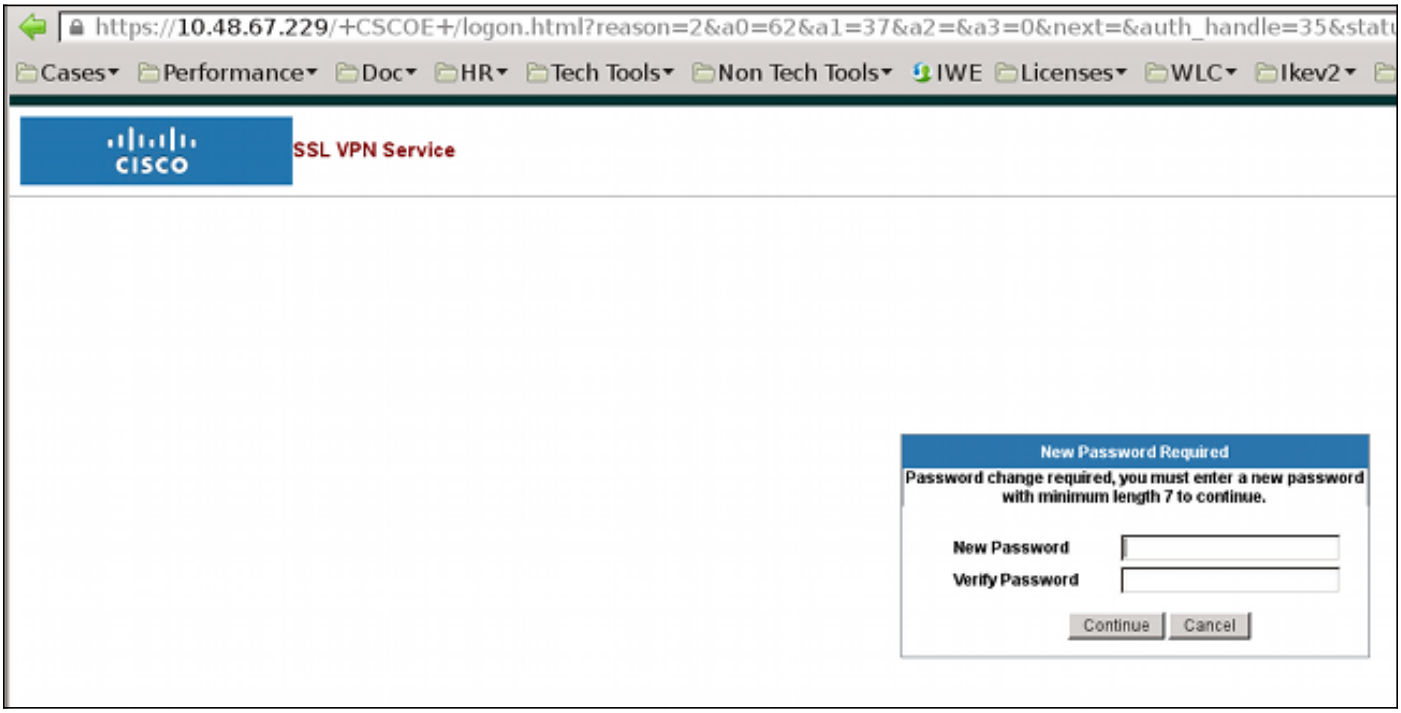
Hay registros más detallados disponibles en la herramienta Diagnostic AnyConnect Reporting Tool (DART).

Portal web de ASA SSL

El mismo proceso de inicio de sesión ocurre en el portal web:



Se produce el mismo proceso de caducidad y cambio de contraseña:



Contraseña de cambio de usuario ACS

Si no es posible cambiar la contraseña a través de la VPN, puede utilizar el servicio web dedicado de cambio de contraseña de usuario ACS (UCP). Consulte la Guía del Desarrollador de Software para Cisco Secure Access Control System 5.4: Uso de los Servicios Web UCP.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Guía de configuración de Cisco ASA serie 5500 con CLI, 8.4 y 8.6: Configuración de un servidor externo para la autorización de usuario de dispositivo de seguridad
- Soporte Técnico y Documentación - Cisco Systems