ASA Remote Access VPN IKE/SSL - Exemplo de configuração de expiração e alteração de senha para RADIUS, TACACS e LDAP

Contents

Introduction

Este documento descreve os recursos de expiração de senha e alteração de senha em um túnel VPN de acesso remoto encerrado em um Cisco Adaptive Security Appliance (ASA). O documento abrange:

- Clientes diferentes: Cisco VPN Client e Cisco AnyConnect Secure Mobility
- Protocolos diferentes: TACACS, RADIUS e Lightweight Diretory Access Protocol (LDAP)
- Diferentes lojas no Cisco Secure Access Control System (ACS): Diretório local e ativo (AD)

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento da configuração do ASA através da interface da linha de comando (CLI)
- Conhecimento básico da configuração de VPN em um ASA
- Conhecimento básico do Cisco Secure ACS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Adaptive Security Appliance, versão 8.4 e posterior
- Microsoft Windows Server 2003 SP1
- Cisco Secure Access Control System, versão 5.4 ou posterior
- Cisco AnyConnect Secure Mobility, versão 3.1
- Cisco VPN Client, versão 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

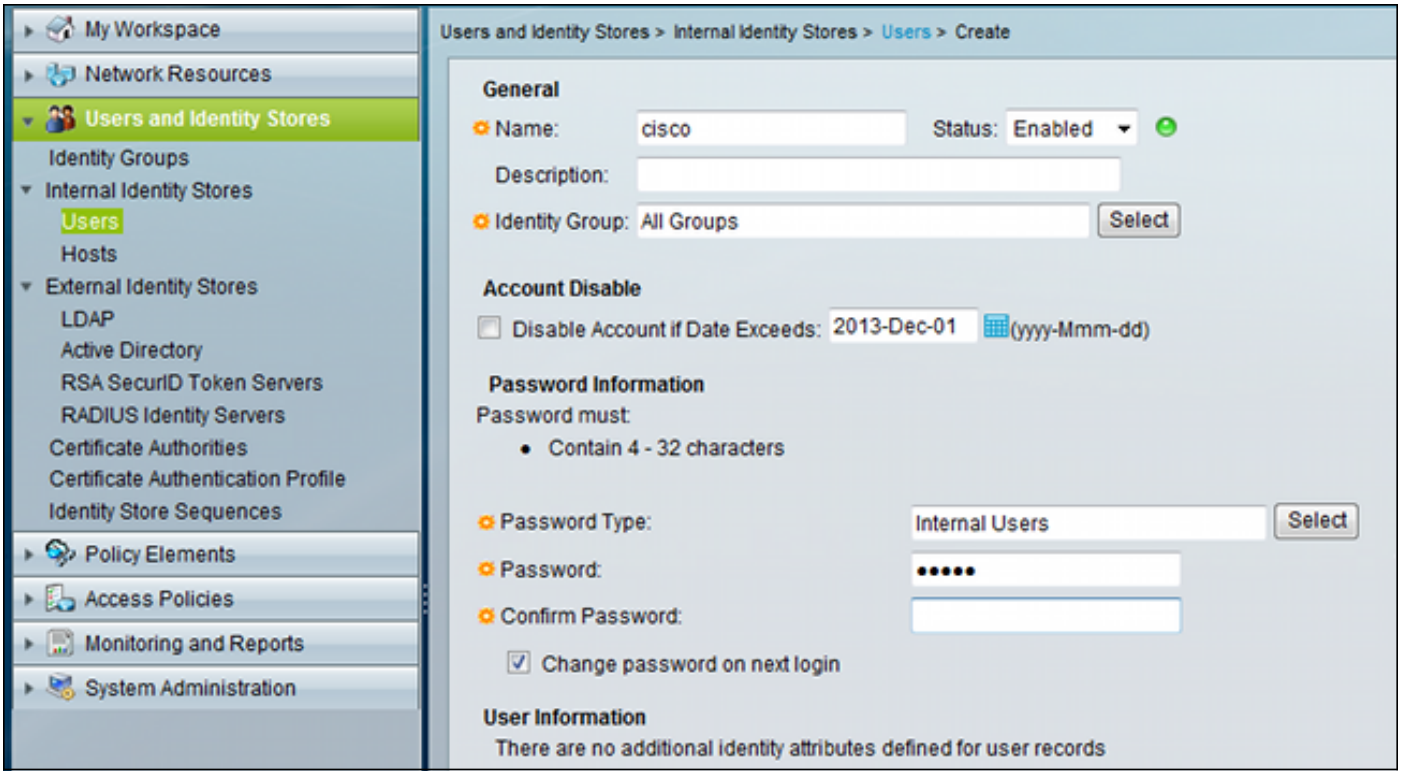
> **Notas:**
>
> Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.
>
> Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug.**

ASA com autenticação local

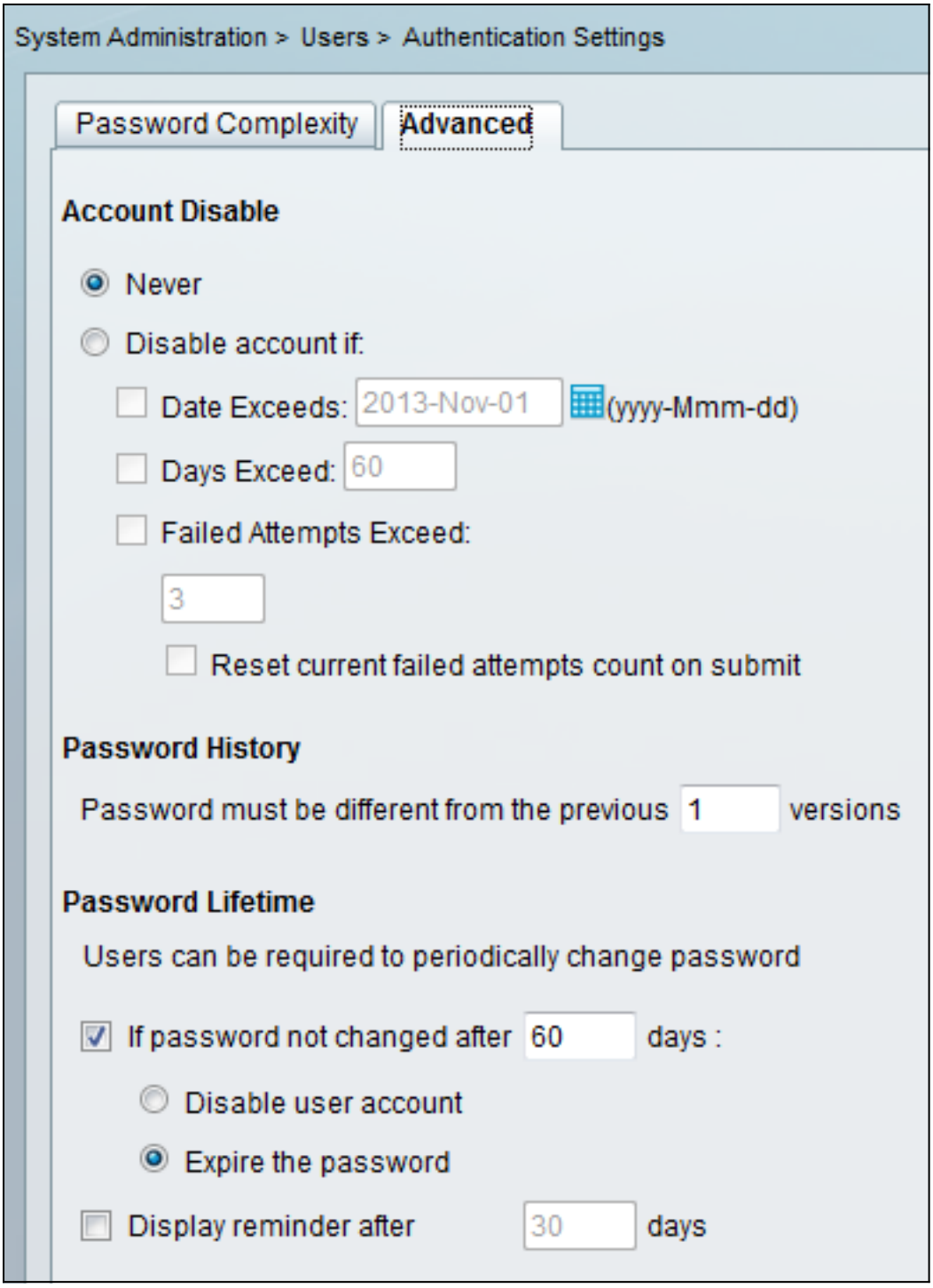
Um ASA com usuários definidos localmente não permite o uso de recursos de expiração de senha ou alteração de senha. Um servidor externo, como RADIUS, TACACS, LDAP ou Windows NT, é necessário.

ACS e usuários locais

O ACS suporta a expiração de senha e a alteração de senha para usuários definidos localmente. Por exemplo, você pode forçar usuários recém-criados a alterar sua senha no próximo login ou pode desabilitar uma conta em uma data específica:

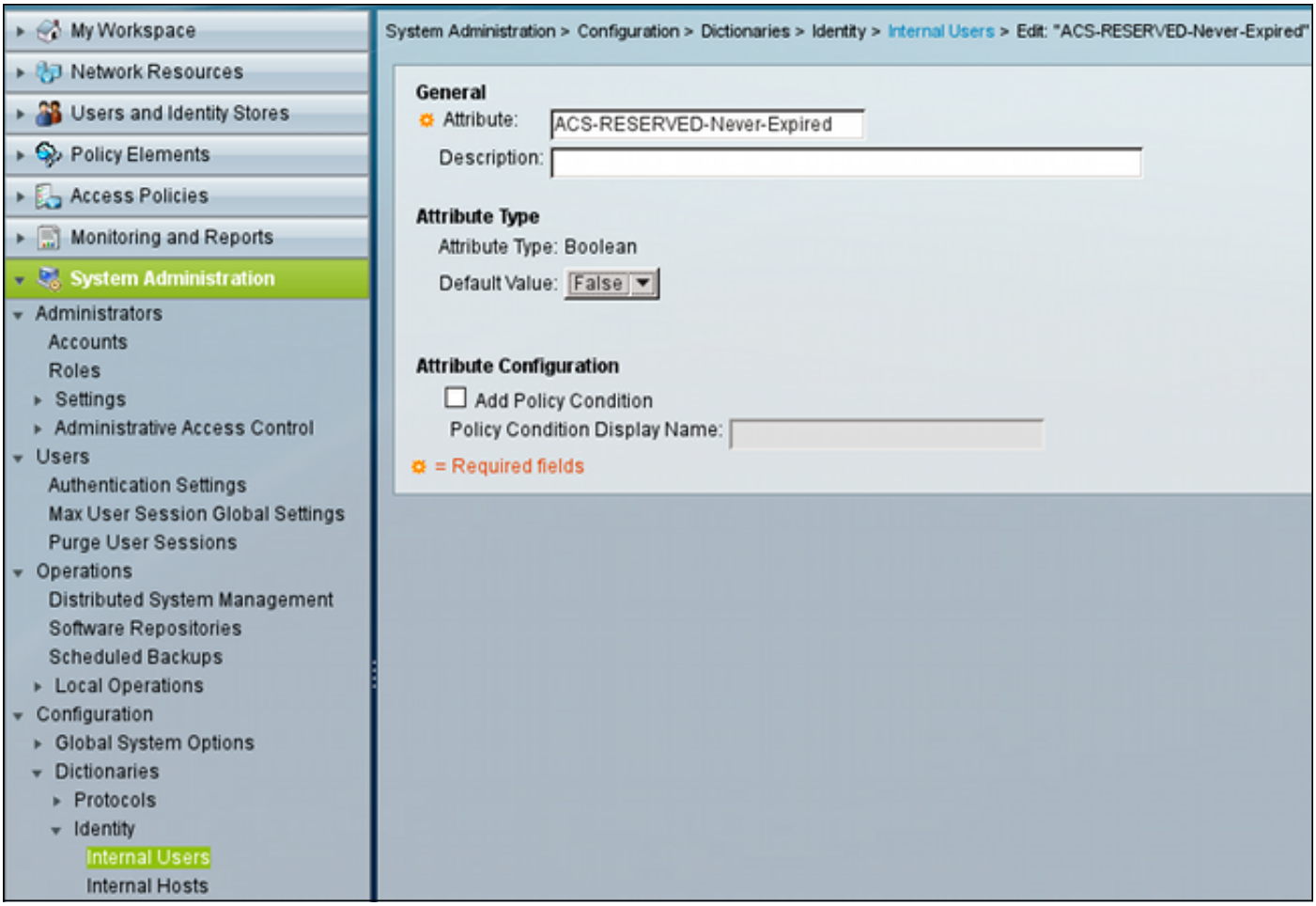


Você pode configurar uma política de senha para todos os usuários. Por exemplo, depois que uma senha expira, você pode desativar a conta de usuário (bloqueá-la sem a capacidade de fazer login) ou pode oferecer a opção de alterar a senha:

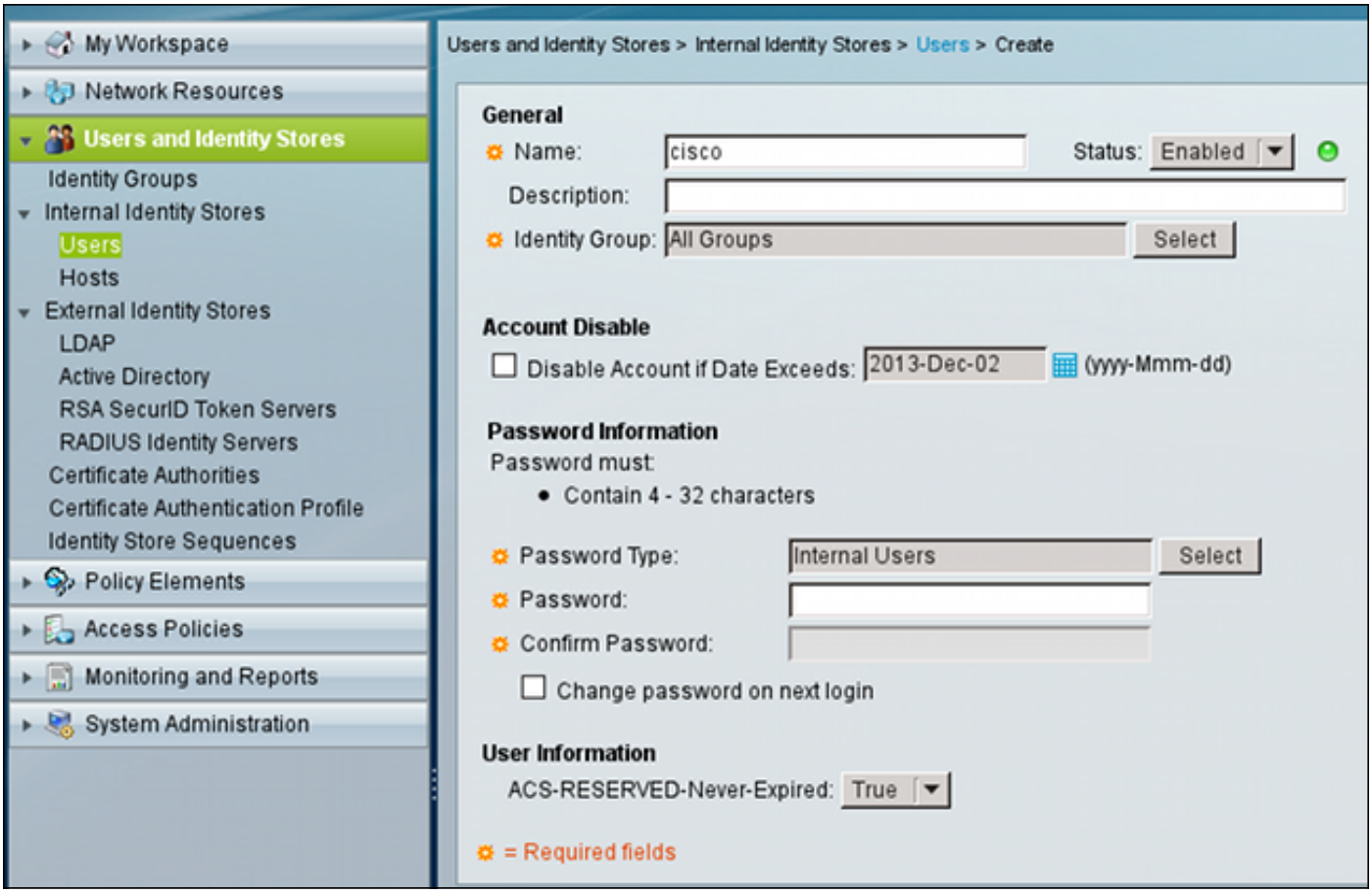


As configurações específicas do usuário têm precedência sobre as configurações globais.

ACS-RESERVED-Nunca-Expired é um atributo interno para a identidade do usuário.



Este atributo é ativado pelo usuário e pode ser usado para desativar as configurações globais de expiração de conta. Com essa configuração, uma conta não é desabilitada mesmo que a política global indique que ela deve ser:

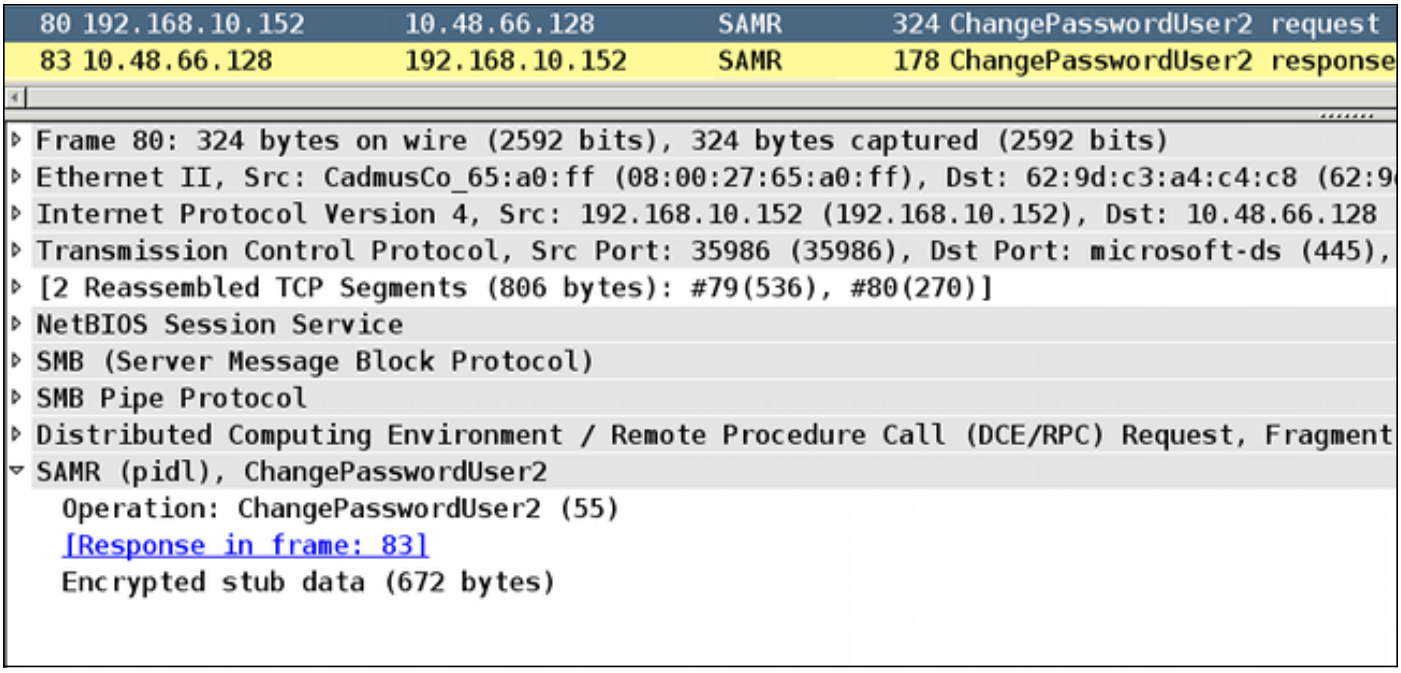


Usuários do ACS e do Ative Diretory

O ACS pode ser configurado para verificar os usuários em um banco de dados do AD. A expiração e a alteração da senha são suportadas quando o Microsoft Challenge Handshake Authentication Protocol versão 2 (MSCHAPv2) é usado; consulte o Guia do usuário do Cisco Secure Access Control System 5.4: Autenticação no ACS 5.4: Authentication Protocol e Identity Store Compatibility para detalhes.

Em um ASA, você pode usar o recurso de gerenciamento de senha, conforme descrito na próxima seção, para forçar o ASA a usar o MSCHAPv2.

O ACS usa a chamada DCE/RPC (Common Internet File System, sistema de arquivos de Internet comum) quando entra em contato com o diretório do controlador de domínio (DC) para alterar a senha:



O ASA pode usar os protocolos RADIUS e TACACS+ para entrar em contato com o ACS para uma alteração de senha do AD.

ASA com ACS via RADIUS

O protocolo RADIUS não oferece suporte nativo à expiração de senha ou à alteração de senha. Geralmente, o PAP (Password Authentication Protocol) é usado para RADIUS. O ASA envia o nome de usuário e a senha em texto simples, e a senha é criptografada por meio do uso do segredo compartilhado RADIUS.

Em um cenário típico quando a senha do usuário expirou, o ACS retorna uma mensagem de RADIUS Reject para o ASA. O ACS percebe 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 o ASA, é uma mensagem RADIUS-Reject simples e a autenticação falha.

Para resolver esse problema, o ASA permite o uso do comando **password-management** na configuração do grupo de túneis:

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

O comando **password-management** altera o comportamento para que o ASA seja forçado a usar MSCHAPv2, em vez de PAP, na solicitação de RADIUS.

O protocolo MSCHAPv2 suporta a expiração de senha e alteração de senha. Portanto, se um usuário de VPN tiver entrado nesse grupo de túneis específico durante a fase Xauth, a solicitação de RADIUS do ASA agora inclui um 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)
```

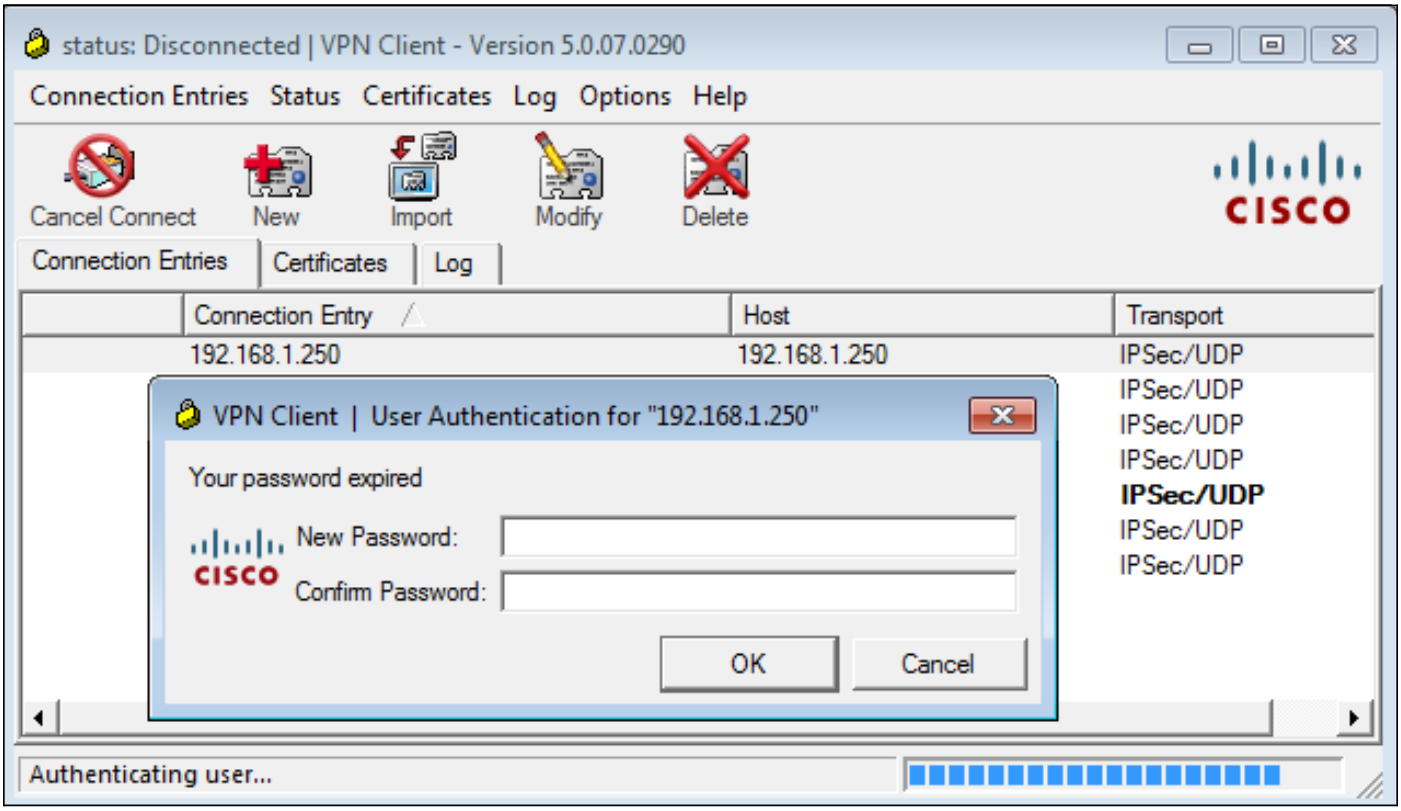
Se o ACS perceber que o usuário precisa alterar a senha, ele retorna uma mensagem Radius-Reject com o erro MSCHAPv2 648.

```
▽ 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
```

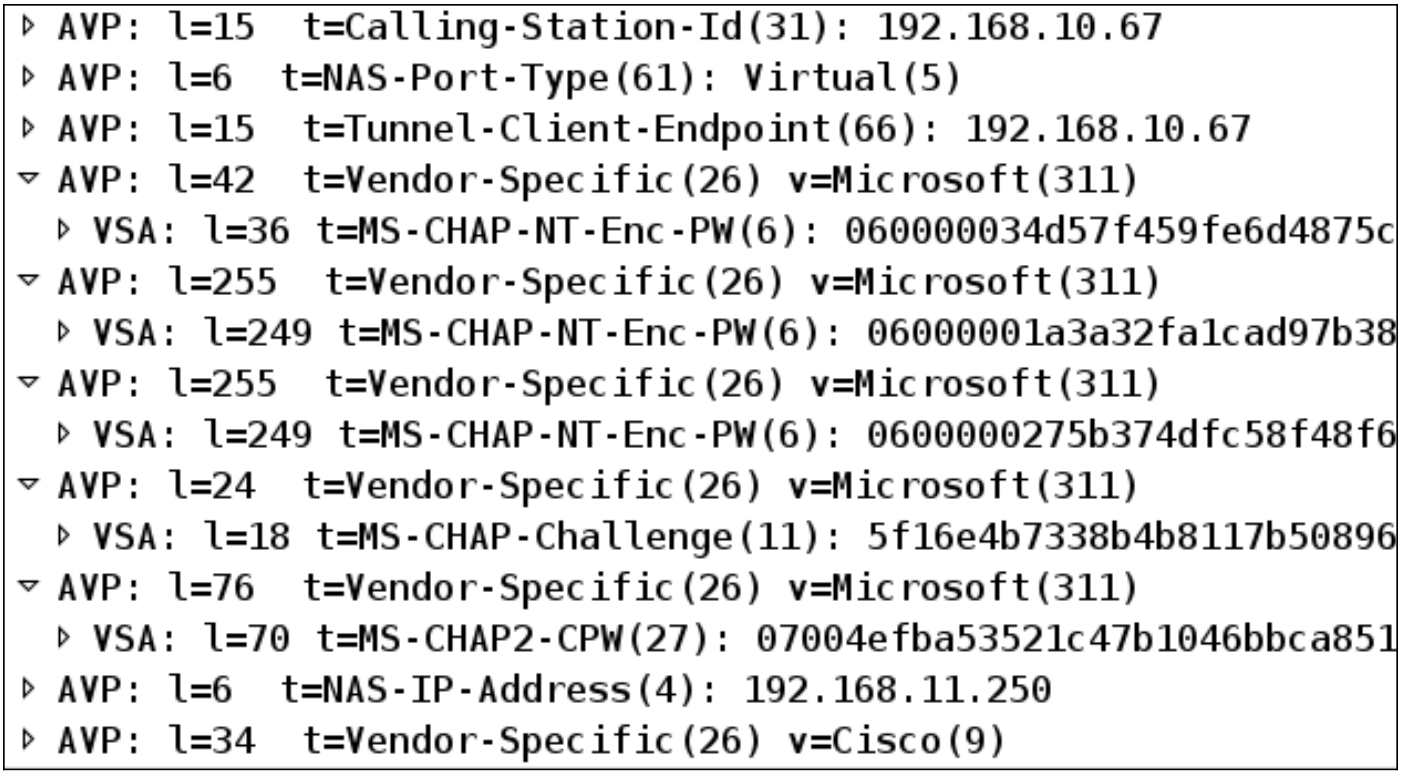
O ASA entende essa mensagem e usa MODE_CFG para solicitar a nova senha ao cliente Cisco VPN:

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

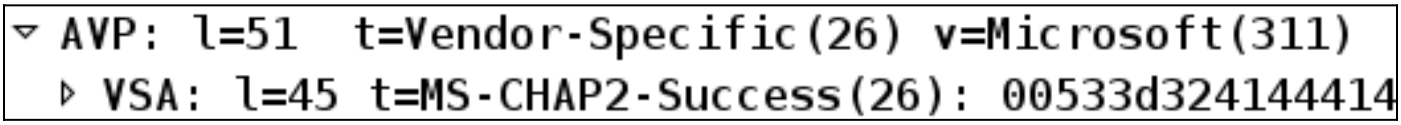
O Cisco VPN Client apresenta uma caixa de diálogo que solicita uma nova senha:



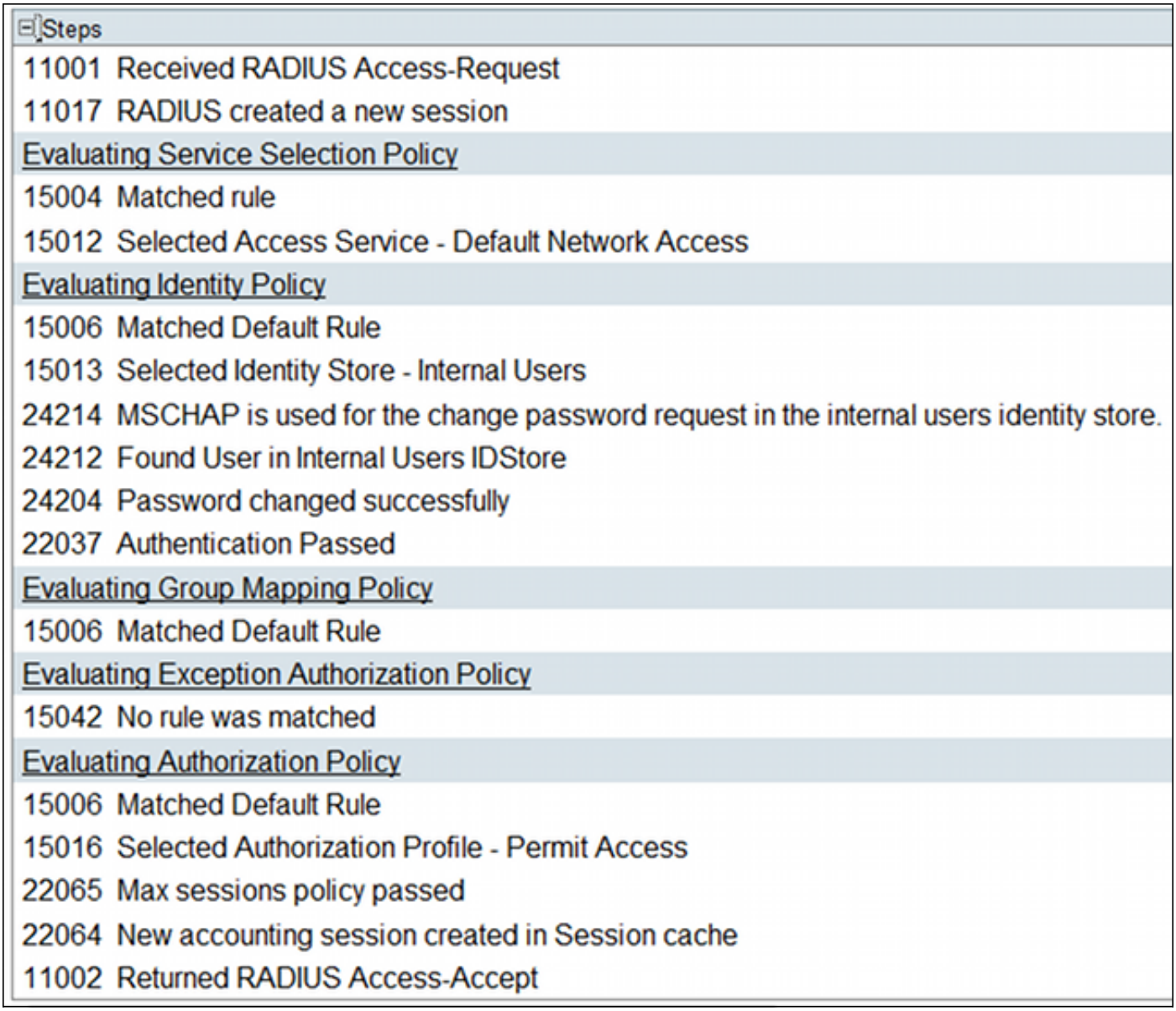
O ASA envia outra solicitação Radius com um payload MS-CHAP-CPW e MS-CHAP-NT-Enc-PW (a nova senha):



O ACS confirma a solicitação e retorna um RADIUS-Accept com MS-CHAP2-Success:



Isso pode ser verificado no ACS, que relata uma 'Senha 24204 alterada com êxito':



Em seguida, o ASA relata a autenticação bem-sucedida e continua com o processo de Modo Rápido (QM):

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

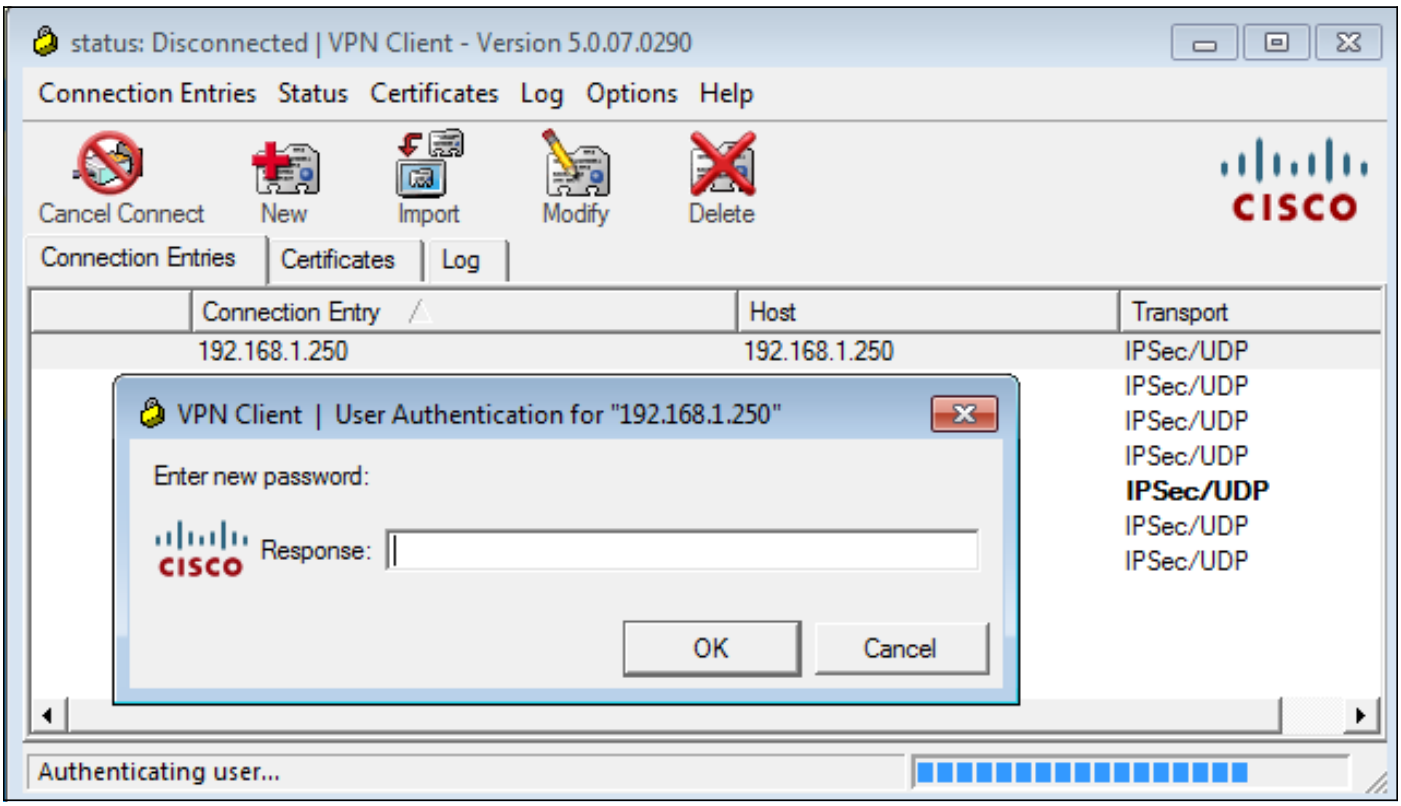
ASA com ACS via TACACS+

Da mesma forma, TACACS+ pode ser usado para a expiração e alteração de senha. O recurso de gerenciamento de senha não é necessário, pois o ASA ainda usa TACACS+ com um tipo de autenticação ASCII em vez de MSCHAPv2.

Vários pacotes são trocados e o ACS solicita uma nova senha:

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

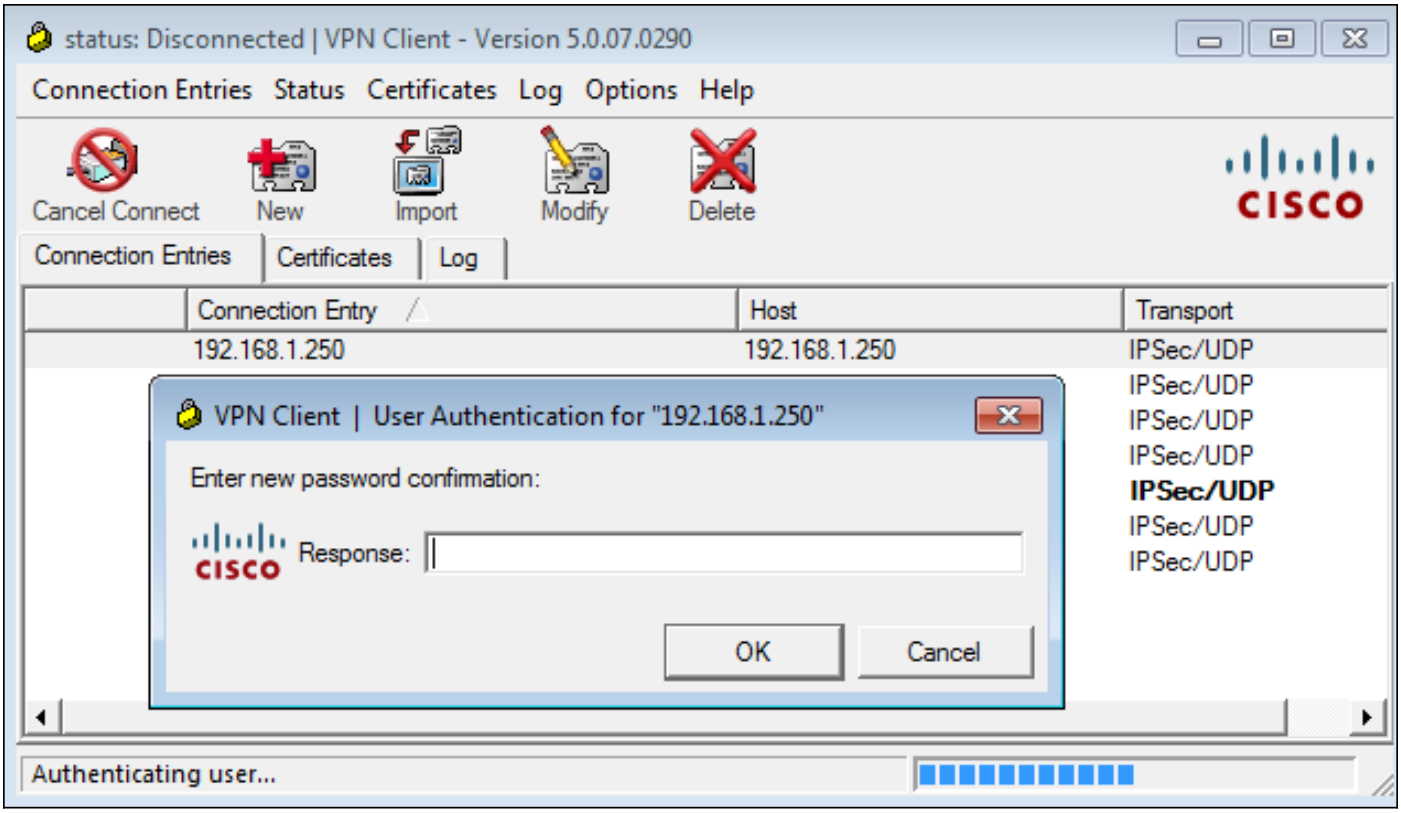
O Cisco VPN Client apresenta uma caixa de diálogo (diferente da usada pelo RADIUS) que solicita uma nova senha:



O ACS solicita a confirmação da nova senha:

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

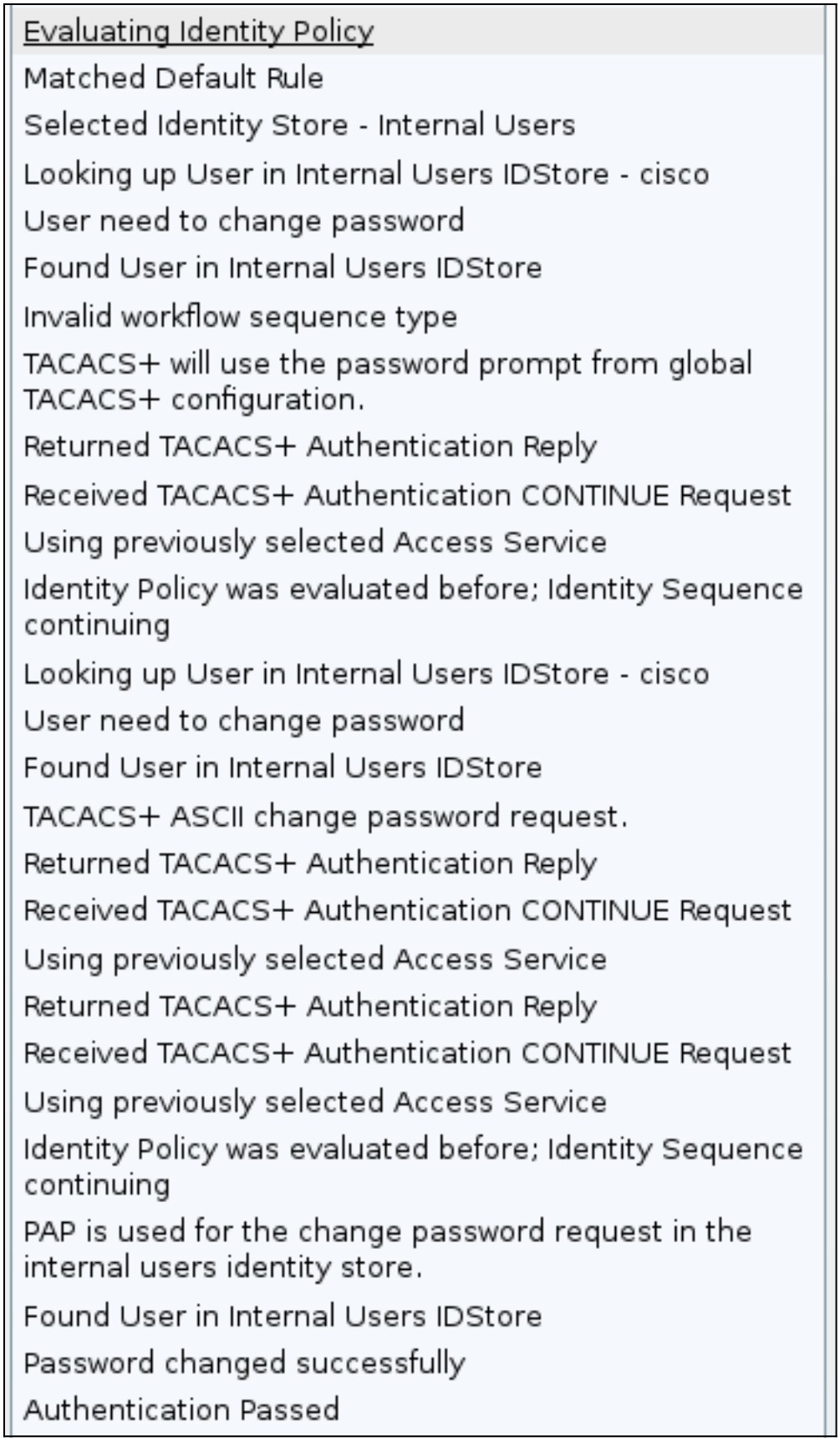
O cliente VPN Cisco apresenta uma caixa de confirmação:



Se a confirmação estiver correta, o ACS relata uma autenticação bem-sucedida:

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

Em seguida, o ACS registra um evento no qual a senha foi alterada com êxito:



As depurações do ASA mostram todo o processo de troca e autenticação bem-sucedida:

```
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.
```

Essa alteração de senha é completamente transparente para o ASA. É apenas um pouco mais longa a sessão TACACS+ com mais pacotes de solicitação e resposta, que são analisados pelo cliente VPN e apresentados ao usuário que está alterando a senha.

ASA com LDAP

A expiração e alteração de senha são totalmente suportadas pelo esquema do servidor Microsoft AD e Sun LDAP.

Para uma alteração de senha, os servidores retornam 'bindresponse = invalidCredentials' com 'error = 773'. Esse erro indica que o usuário deve redefinir a senha. Os códigos de erro típicos incluem:

Código de erro	Erro
525	Usuário não encontrado
52.º-E	Credenciais inválidas
530	Não é permitido fazer logon no momento
531	Não é permitido fazer logon nesta estação de trabalho
532	Senha expirada
533	Conta desabilitada
701	Conta expirada
773	O usuário deve redefinir a senha
775	Conta de usuário bloqueada

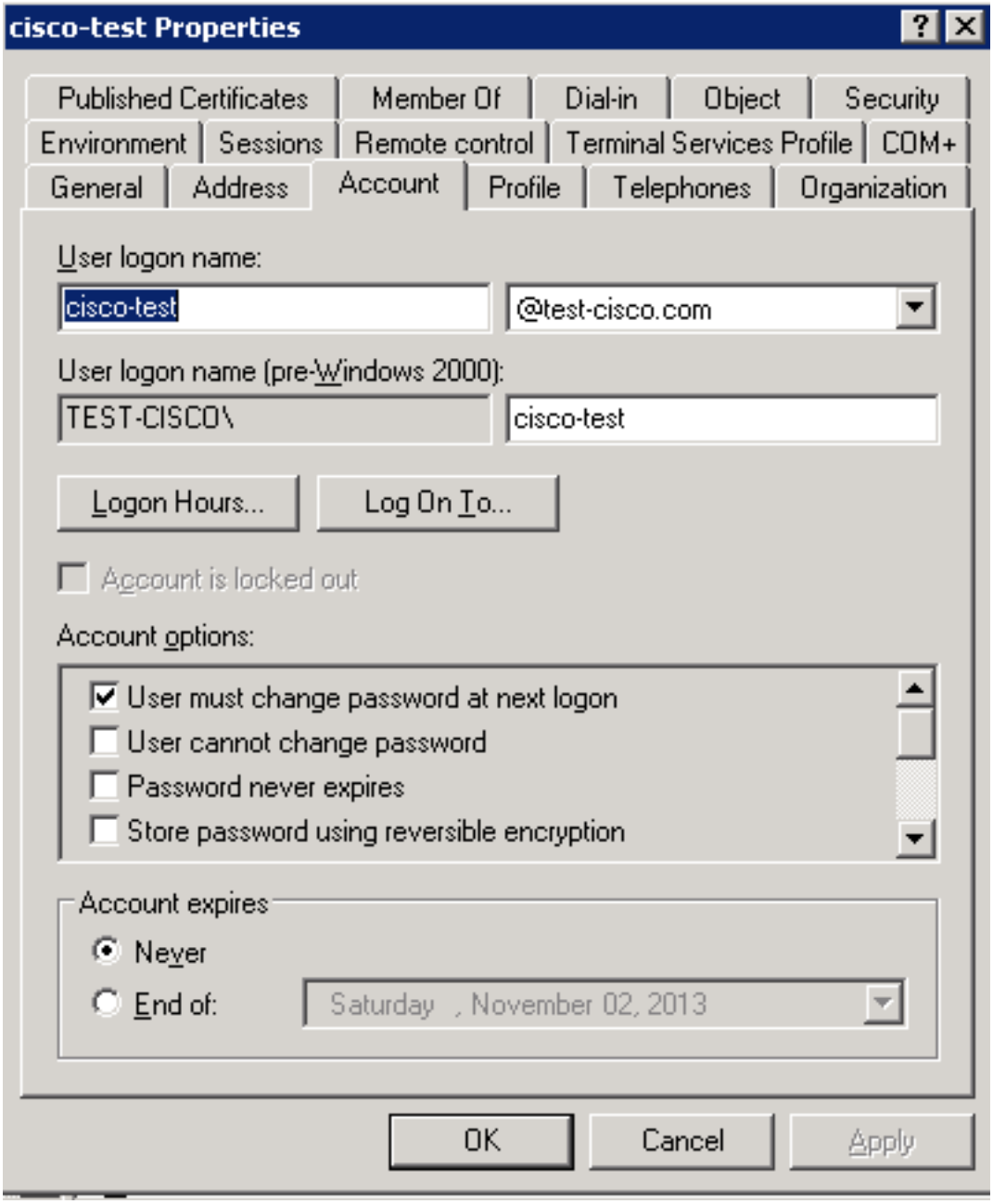
Configurar o servidor LDAP:

```
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
```

Use essa configuração para o grupo de túneis e o recurso de gerenciamento de senha:

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

Configure o usuário do AD para que uma alteração de senha seja necessária:



Quando o usuário tenta usar o cliente Cisco VPN, o ASA relata uma senha inválida:

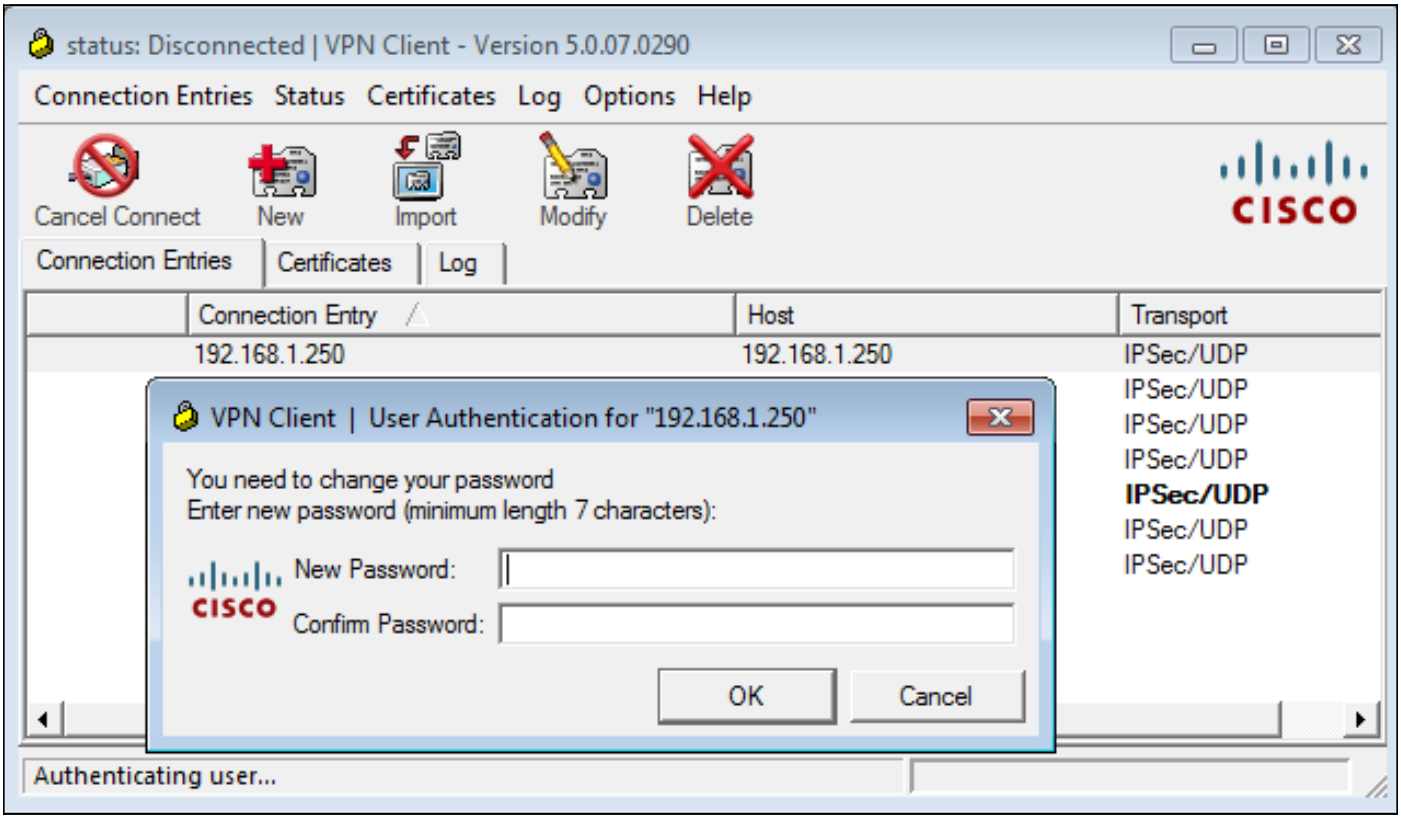
```
ASA(config-tunnel-general)# debug ldap 255
<some output ommited for clarity>

[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 as credenciais forem inválidas, o erro 52e será exibido:

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

O cliente VPN Cisco pede uma alteração de senha:



Essa caixa de diálogo difere do diálogo usado por TACACS ou RADIUS porque exibe a política. Neste exemplo, a política tem um comprimento mínimo de senha de sete caracteres.

Quando o usuário alterar a senha, o ASA poderá receber esta mensagem de falha do servidor LDAP:

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

A política da Microsoft exige o uso de SSL (Secure Sockets Layer) para a modificação de senha. Alterar a configuração:

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

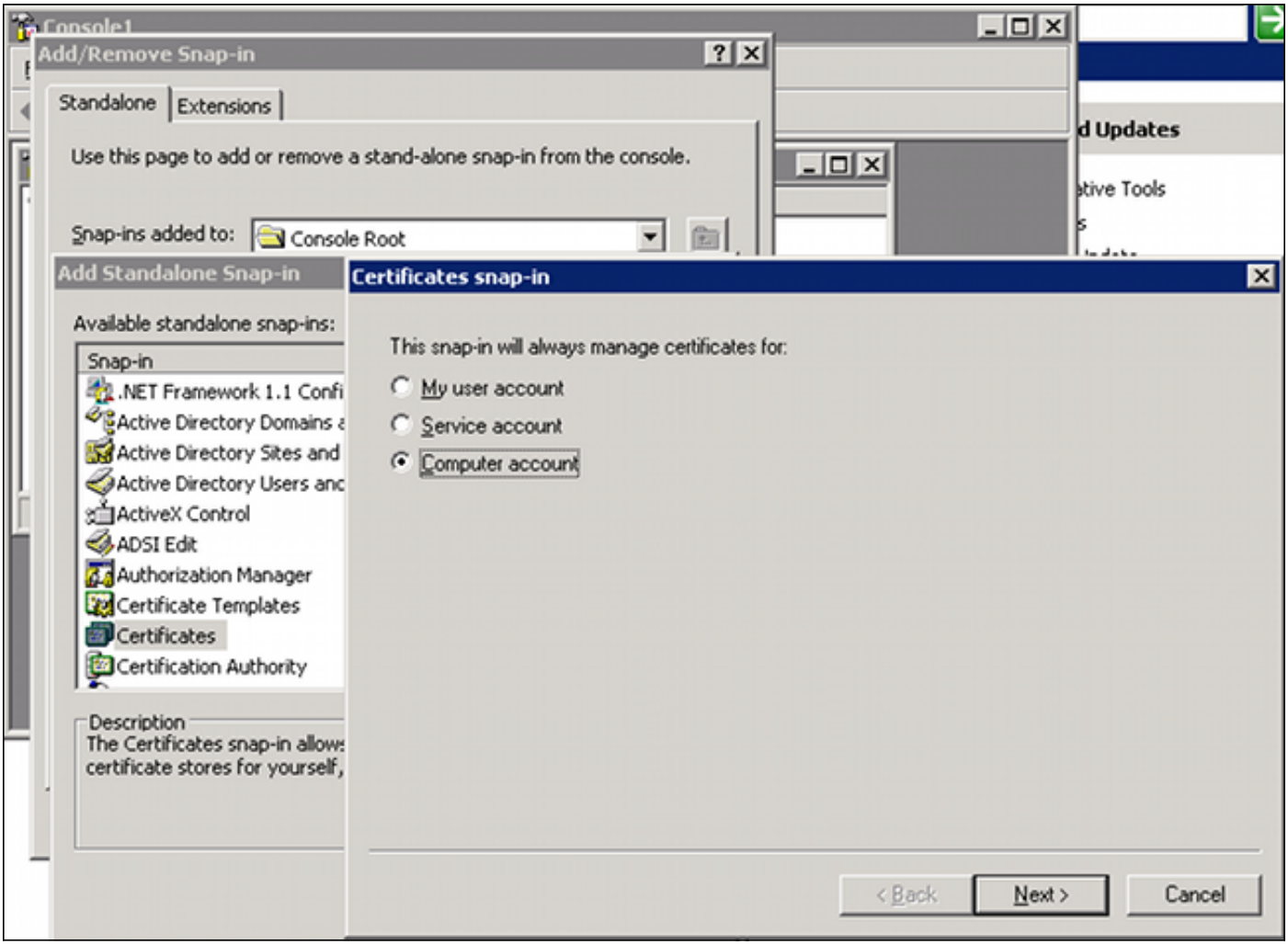
Microsoft LDAP para SSL

Por padrão, o Microsoft LDAP sobre SSL não funciona. Para habilitar essa função, você deve instalar o certificado para a conta do computador com o ramal de chave correto. Consulte Como habilitar o LDAP sobre SSL com uma autoridade de certificação de terceiros para obter mais detalhes.

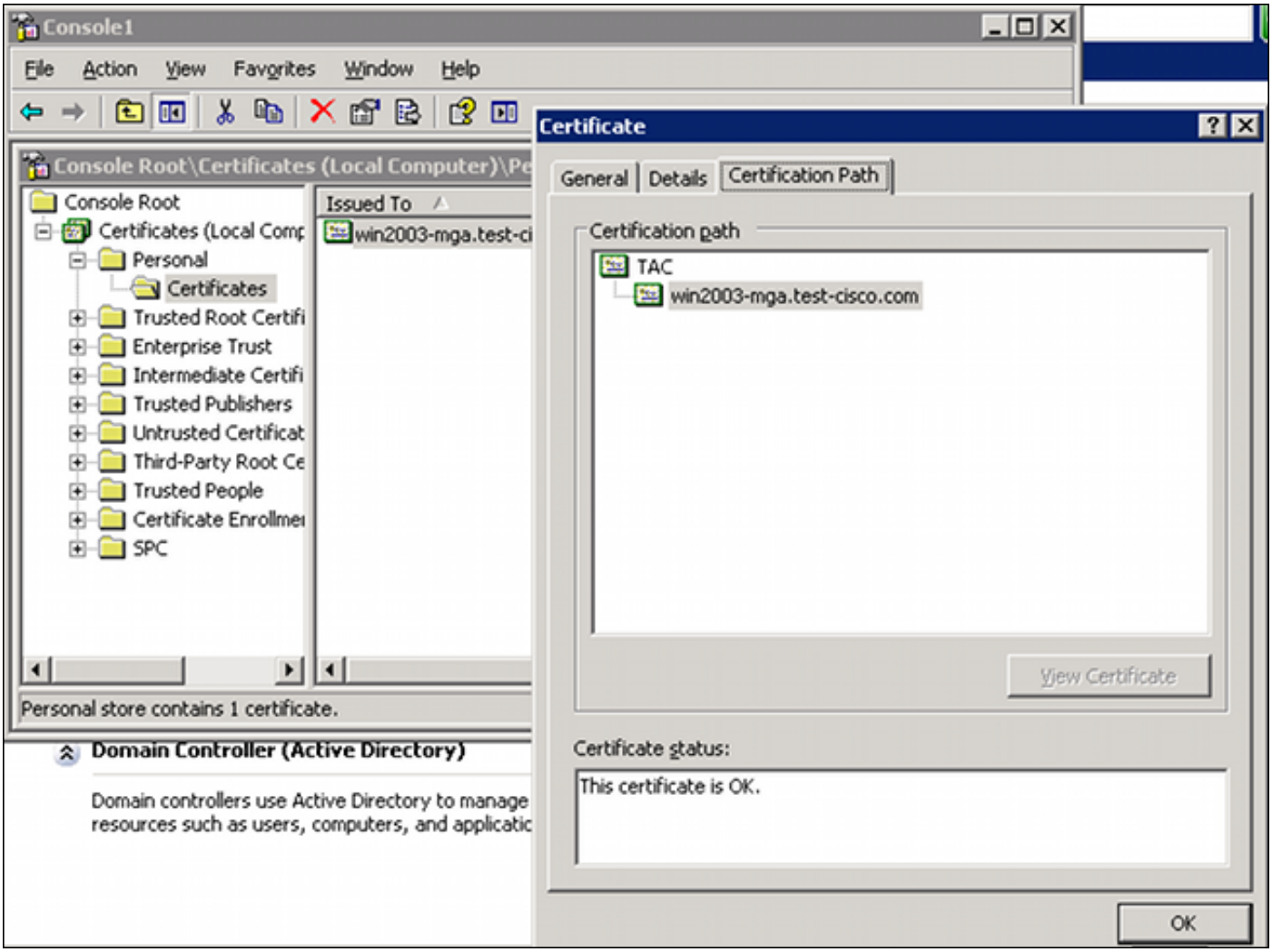
O certificado pode até ser um certificado autoassinado porque o ASA não verifica o certificado LDAP. Consulte Cisco Bug ID CSCui40212, "Permitir que o ASA valide o certificado do servidor LDAPS", para obter uma solicitação de aprimoramento relacionada.

> **Note**: O ACS verifica o certificado LDAP na versão 5.5 e posterior.

Para instalar o certificado, abra o console mmc, selecione **Adicionar/remover snap-in**, adicione o certificado e escolha **Conta do computador**:



Selecione **Computador local**, importe o certificado para o arquivo pessoal e mova o certificado da Autoridade de Certificação (AC) associado para o arquivo confiável. Verifique se o certificado é confiável:



Há um erro no ASA versão 8.4.2, em que esse erro pode ser retornado quando você está tentando usar LDAP sobre SSL:

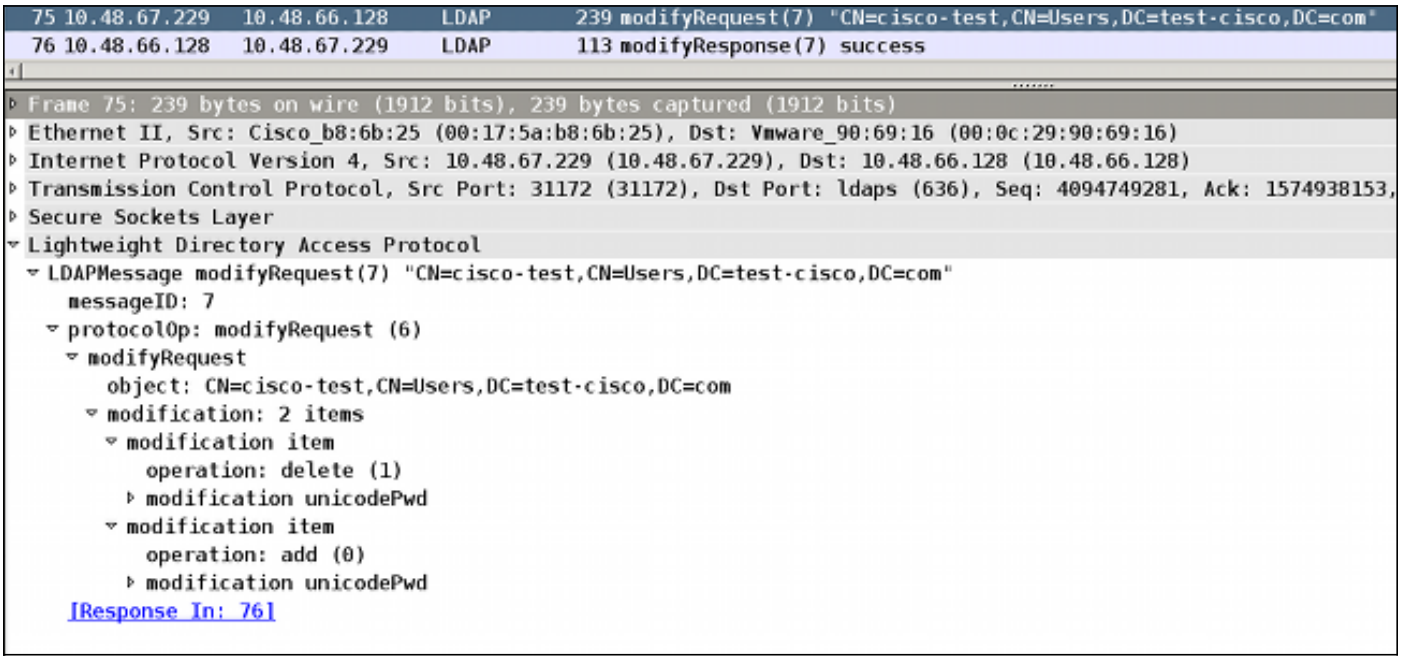
```
ASA(config)# debug ldap 255

[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
```

O ASA versão 9.1.3 funciona corretamente com a mesma configuração. Há duas sessões LDAP. A primeira sessão retorna uma falha com o código 773 (senha expirada), enquanto a segunda sessão é usada para a alteração de senha:

```
[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 a alteração de senha, examine os pacotes. A chave privada do servidor LDAP pode ser usada pelo Wireshark para descriptografar o tráfego SSL:



As depurações de Internet Key Exchange (IKE)/Authentication, Authorization, and Accounting (AAA) no ASA são muito semelhantes às apresentadas no cenário de autenticação RADIUS.

LDAP e aviso antes do vencimento

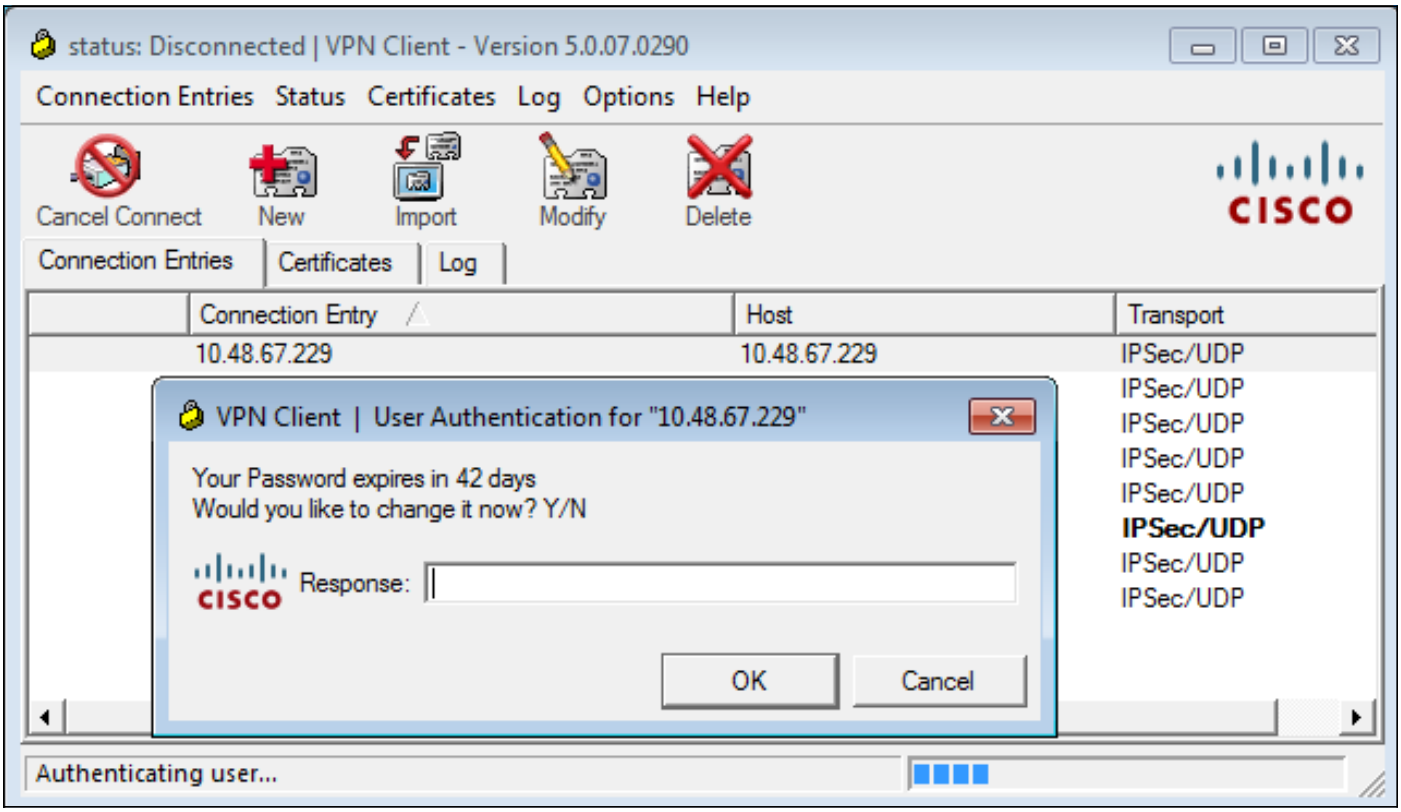
Para LDAP, você pode usar um recurso que envia um aviso antes de uma senha expirar. O ASA avisa ao usuário 90 dias antes da expiração da senha com esta configuração:

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

Aqui a senha expira em 42 dias e o usuário tenta fazer login:

```
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
```

O ASA envia um aviso e oferece a opção de alteração de senha:



Se o usuário optar por alterar a senha, haverá um prompt para uma nova senha e o procedimento normal de alteração de senha será iniciado.

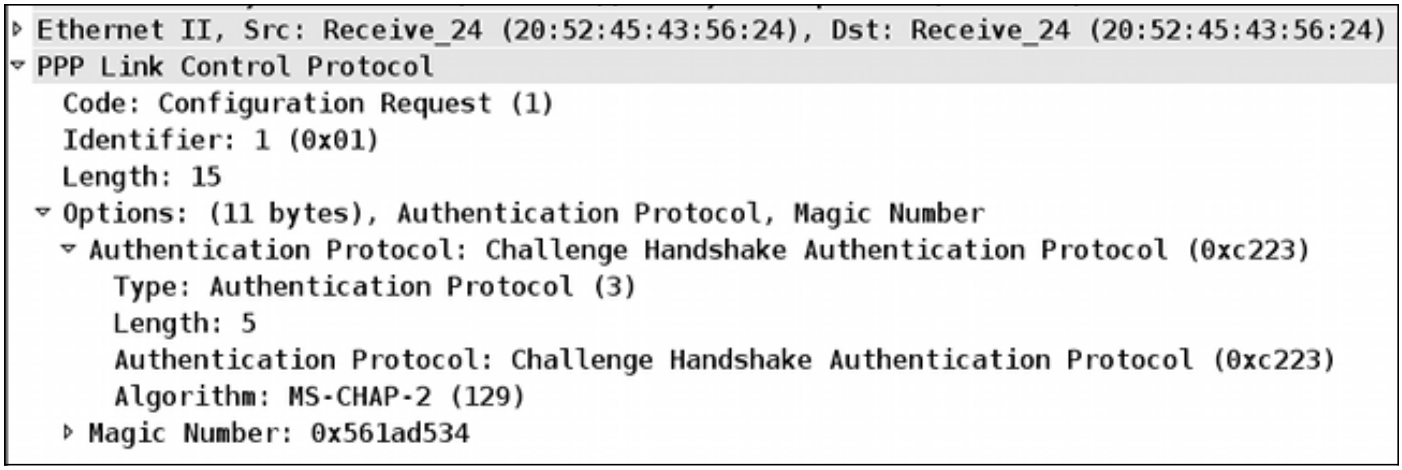
ASA e L2TP

Os exemplos anteriores apresentavam IKE versão 1 (IKEv1) e IPSec VPN.

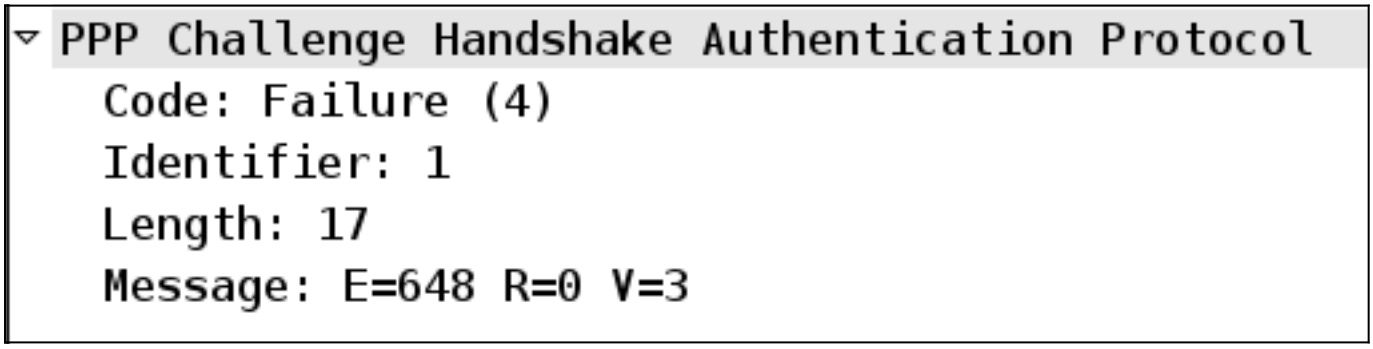
Para o L2TP (Layer 2 Tunneling Protocol) e IPSec, o PPP é usado como um transporte para autenticação. MSCHAPv2 é necessário em vez de PAP para que uma alteração de senha funcione:

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

Para Autenticação Estendida em L2TP dentro da sessão PPP, o MSCHAPv2 é negociado:



Quando a senha do usuário expirou, uma falha com o código 648 é retornada:



Uma alteração de senha é necessária. O restante do processo é muito semelhante ao cenário para RADIUS com MSCHAPv2.

Consulte L2TP sobre IPsec entre o PC Windows 2000/XP e o PIX/ASA 7.2 usando o exemplo de configuração de chave pré-compartilhada para obter detalhes adicionais sobre como configurar o L2TP.

Cliente VPN SSL ASA

Os exemplos anteriores se referiam ao IKEv1 e ao cliente VPN da Cisco, que é o fim da vida útil (EOL).

A solução recomendada para uma VPN de acesso remoto é o Cisco AnyConnect Secure Mobility, que usa os protocolos IKE versão 2 (IKEv2) e SSL. Os recursos de alteração e expiração de senha funcionam exatamente da mesma forma para o Cisco AnyConnect que para o Cisco VPN Client.

Para IKEv1, os dados de alteração e expiração de senha foram trocados entre o ASA e o cliente VPN na fase 1.5 (configuração Xauth/mode).

Para IKEv2, é semelhante; o modo de configuração usa pacotes CFG_REQUEST/CFG_REPLY.

Para SSL, os dados estão na sessão Control Datagram Transport Layer Security (DTLS).

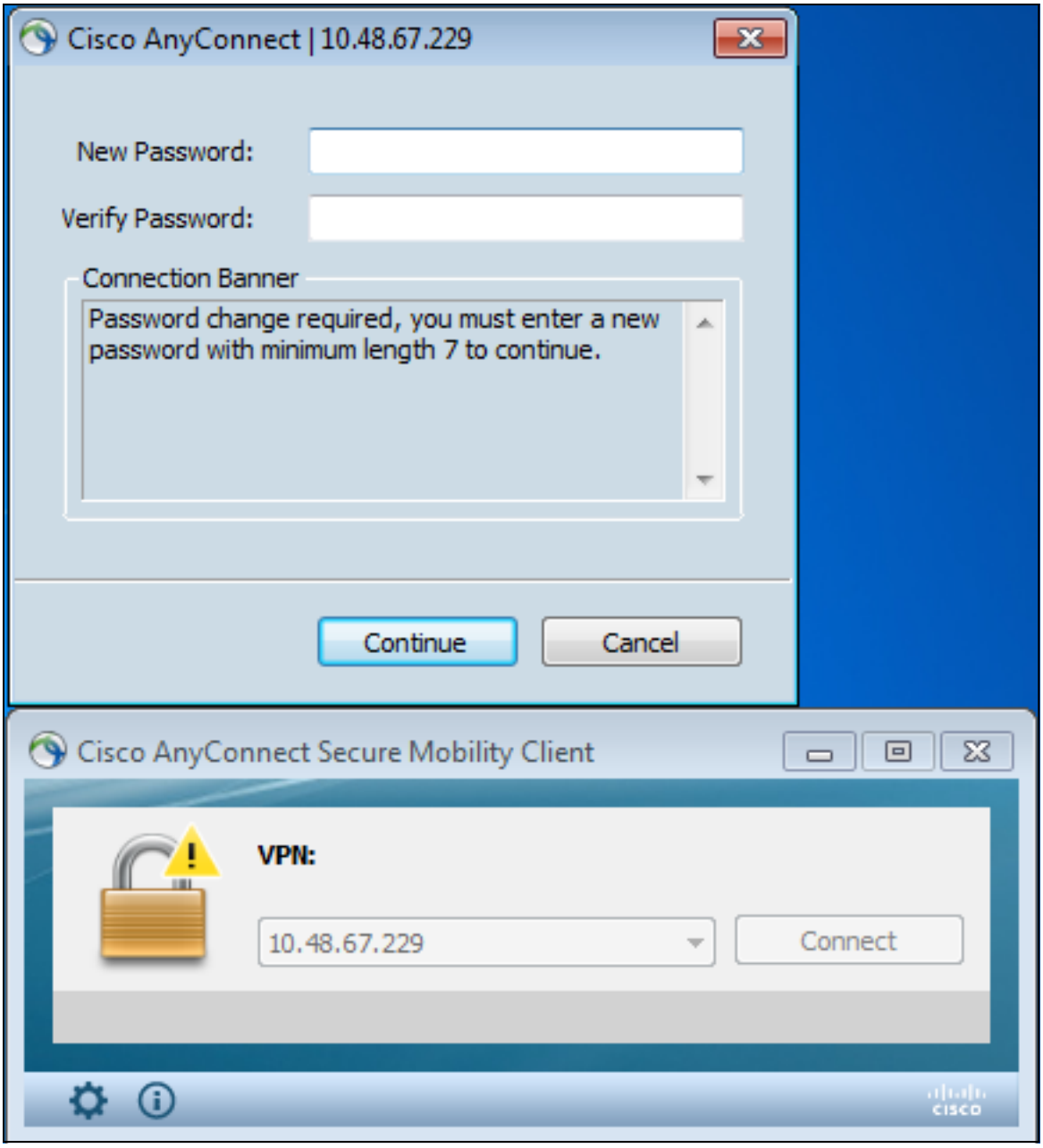
A configuração é a mesma para o ASA.

Este é um exemplo de configuração com o Cisco AnyConnect e o protocolo SSL com um servidor

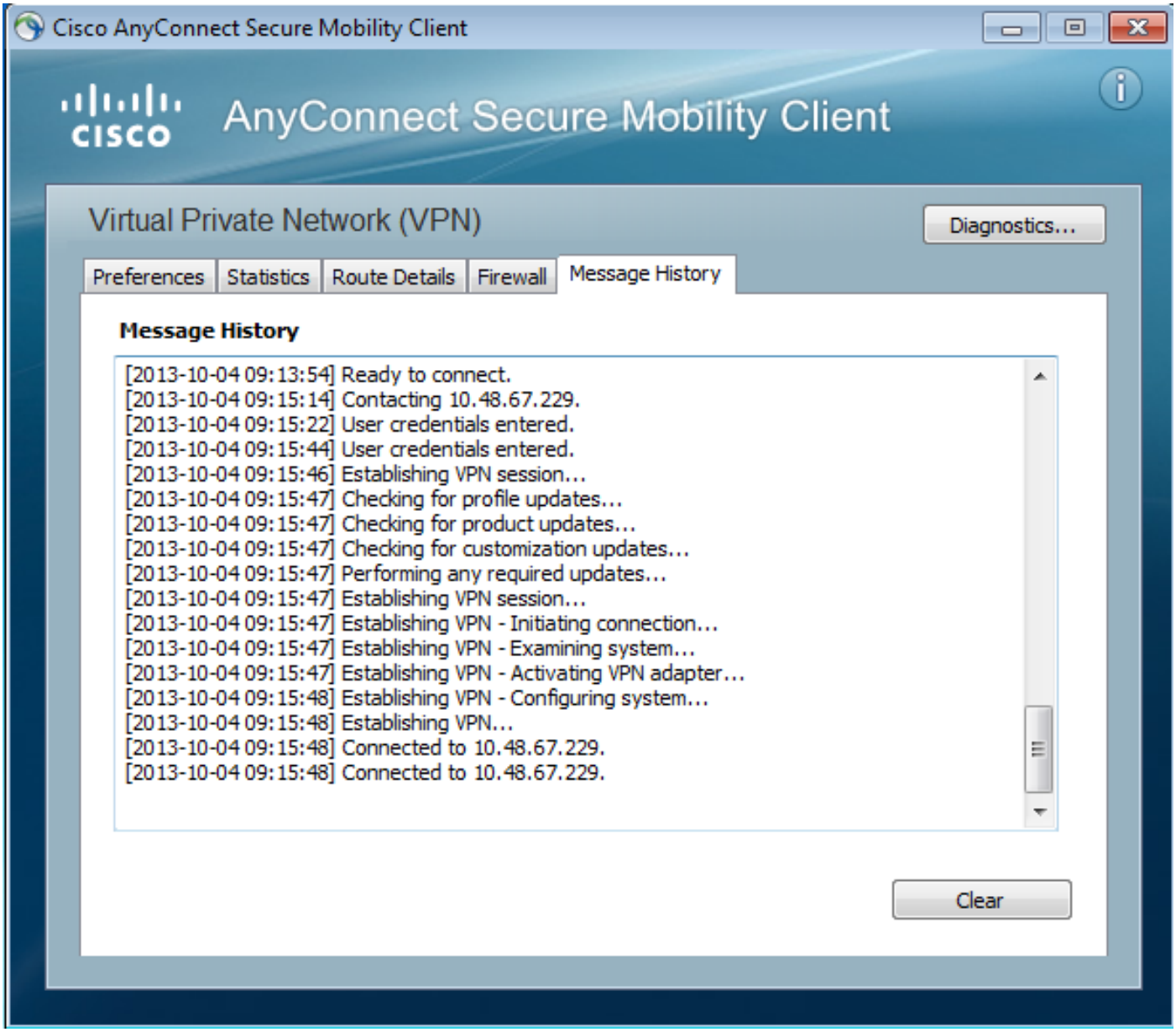
LDAP sobre SSL:

```
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
```

Depois que a senha correta (que expirou) é fornecida, o Cisco AnyConnect tenta se conectar e solicita uma nova senha:



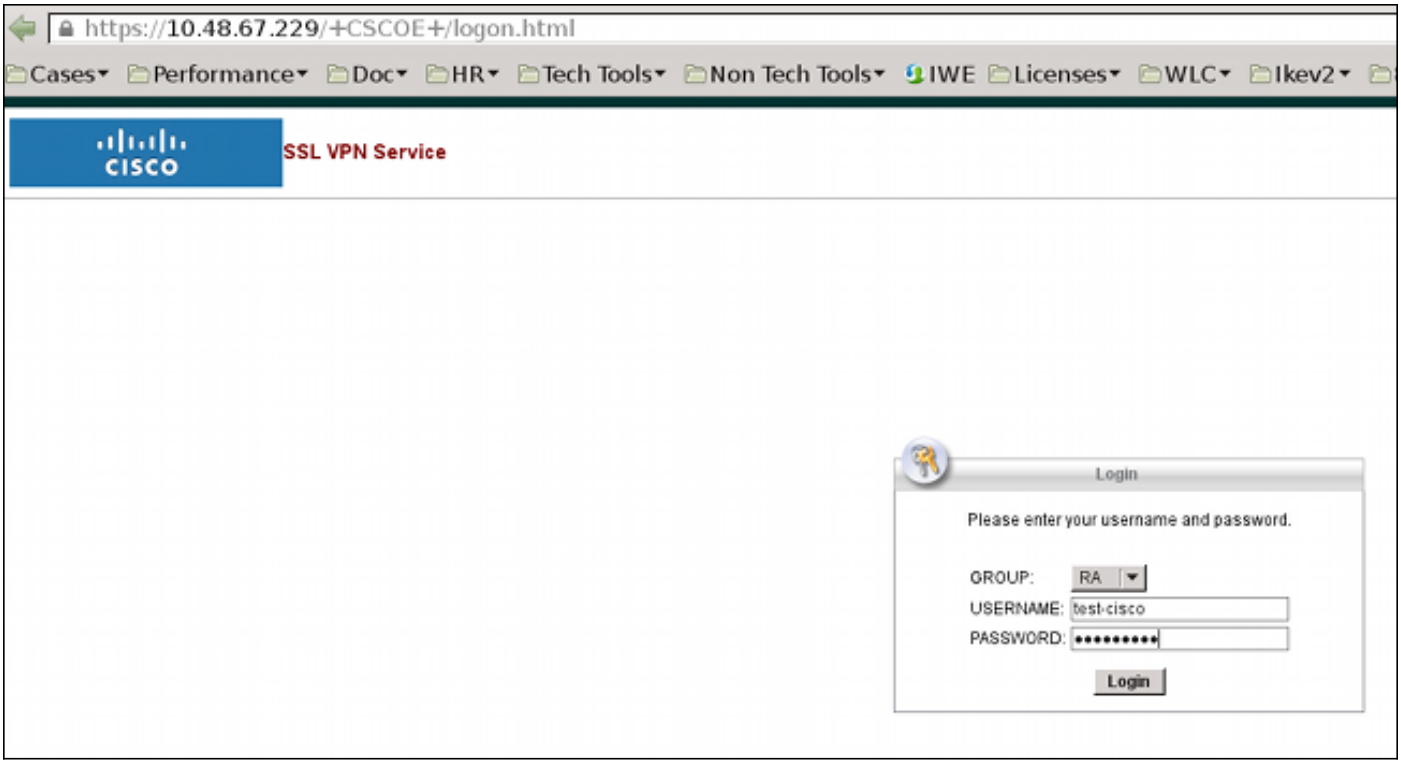
Os registros indicam que as credenciais de usuário foram inseridas duas vezes:



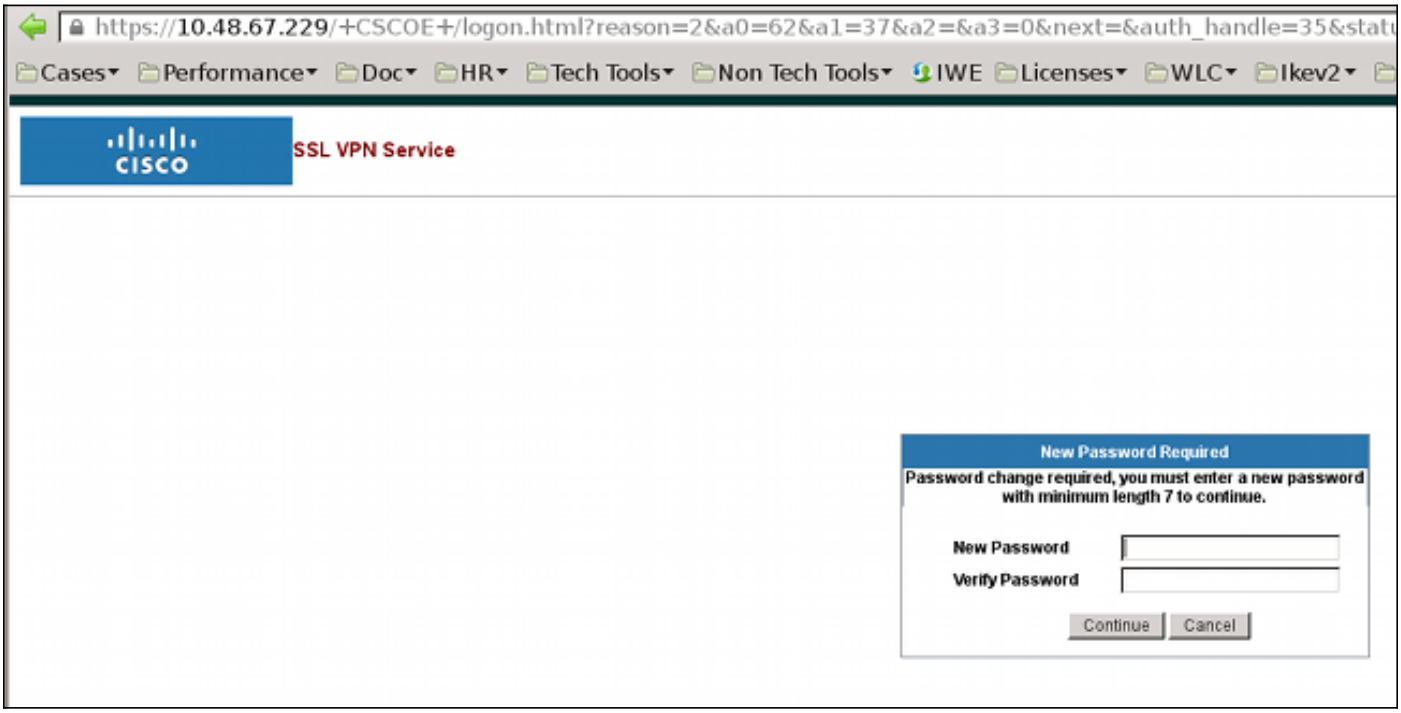
Registros mais detalhados estão disponíveis na Diagnostic AnyConnect Reporting Tool (DART).

Portal da Web ASA SSL

O mesmo processo de login ocorre no portal da Web:



O mesmo processo de expiração e alteração de senha ocorre:



Senha de alteração de usuário ACS

Se não for possível alterar a senha sobre a VPN, você pode usar o serviço da Web dedicado UCP (User Change Password, Senha de alteração de usuário do ACS). Consulte o Guia do desenvolvedor de software do Cisco Secure Access Control System 5.4: Usando os Serviços Web UCP.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Guia de configuração do Cisco ASA 5500 Series usando CLI, 8.4 e 8.6: Como configurar um servidor externo para autorização de usuário de dispositivo de segurança
- Suporte Técnico e Documentação - Cisco Systems