

Exemple de configuration de VPN d'accès à distance ASA IKE/SSL - Expiration et modification du mot de passe pour RADIUS, TACACS et LDAP

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[ASA avec authentification locale](#)

[Utilisateurs ACS et locaux](#)

[Utilisateurs ACS et Active Directory](#)

[ASA avec ACS via RADIUS](#)

[ASA avec ACS via TACACS+](#)

[ASA avec LDAP](#)

[Microsoft LDAP pour SSL](#)

[LDAP et avertissement avant expiration](#)

[ASA et L2TP](#)

[Client VPN SSL ASA](#)

[Portail Web ASA SSL](#)

[Mot de passe de modification d'utilisateur ACS](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit les fonctions d'expiration et de modification de mot de passe d'un tunnel VPN d'accès distant terminé sur un dispositif de sécurité adaptatif (ASA) Cisco. Le document couvre :

- Différents clients : Client VPN Cisco et Cisco AnyConnect Secure Mobility
- Différents protocoles : TACACS, RADIUS et LDAP (Lightweight Directory Access Protocol)
- Différents magasins du système de contrôle d'accès sécurisé Cisco (ACS) : local et Active Directory (AD)

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de la configuration ASA via l'interface de ligne de commande (CLI)
- Connaissance de base de la configuration VPN sur un ASA
- Connaissances de base de Cisco Secure ACS

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appareil de sécurité adaptatif Cisco, versions 8.4 et ultérieures
- Microsoft Windows Server 2003 SP1
- Cisco Secure Access Control System, version 5.4 ou ultérieure
- Cisco AnyConnect Secure Mobility, version 3.1
- Client VPN Cisco, version 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.

Configuration

Remarques :

Utilisez l'[Outil de recherche de commande \(clients inscrits seulement\) pour obtenir plus d'informations sur les commandes utilisées dans cette section.](#)

Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

ASA avec authentification locale

Un ASA avec des utilisateurs définis localement n'autorise pas l'utilisation de fonctions d'expiration de mot de passe ou de modification de mot de passe. Un serveur externe, tel que RADIUS, TACACS, LDAP ou Windows NT, est requis.

Utilisateurs ACS et locaux

ACS prend en charge l'expiration des mots de passe et la modification des mots de passe pour les utilisateurs définis localement. Par exemple, vous pouvez forcer les nouveaux utilisateurs à modifier leur mot de passe à leur prochaine connexion ou désactiver un compte à une date spécifique :

My Workspace
Network Resources
Users and Identity Stores
Identity Groups
Internal Identity Stores
Users
Hosts
External Identity Stores
LDAP
Active Directory
RSA SecurID Token Servers
RADIUS Identity Servers
Certificate Authorities
Certificate Authentication Profile
Identity Store Sequences
Policy Elements
Access Policies
Monitoring and Reports
System Administration

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

General
Name: cisco Status: Enabled
Description:
Identity Group: All Groups Select

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 Select
• Password: ●●●●
• Confirm Password:

Change password on next login

User Information
There are no additional identity attributes defined for user records

Vous pouvez configurer une stratégie de mot de passe pour tous les utilisateurs. Par exemple, après l'expiration d'un mot de passe, vous pouvez désactiver le compte d'utilisateur (le bloquer sans pouvoir vous connecter) ou vous pouvez proposer la possibilité de modifier le mot de passe :

Password Complexity

Advanced

Account Disable

Never

Disable account if:

Date Exceeds:  (yyyy-Mmm-dd)

Days Exceed:

Failed Attempts Exceed:

Reset current failed attempts count on submit

Password History

Password must be different from the previous versions

Password Lifetime

Users can be required to periodically change password

If password not changed after days :

Disable user account

Expire the password

Display reminder after days

Les paramètres spécifiques à l'utilisateur ont préséance sur les paramètres globaux.

ACS-RESERVED-Never-Expired est un attribut interne pour l'identité de l'utilisateur.

System Administration > Configuration > Dictionaries > Identity > Internal Users > Edit: "ACS-RESERVED-Never-Expired"

My Workspace

- Network Resources
- Users and Identity Stores
- Policy Elements
- Access Policies
- Monitoring and Reports
- System Administration**
 - Administrators
 - Accounts
 - Roles
 - Settings
 - Administrative Access Control
 - Users
 - Authentication Settings
 - Max User Session Global Settings
 - Purge User Sessions
 - Operations
 - Distributed System Management
 - Software Repositories
 - Scheduled Backups
 - Local Operations
 - Configuration
 - Global System Options
 - Dictionaries
 - Protocols
 - Identity
 - Internal Users**
 - Internal Hosts

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

Cet attribut est activé par l'utilisateur et peut être utilisé afin de désactiver les paramètres globaux d'expiration du compte. Avec ce paramètre, un compte n'est pas désactivé même si la stratégie globale indique qu'il doit être :

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

Users and Identity Stores

- Identity Groups
- Internal Identity Stores
 - Users**
 - Hosts
- External Identity Stores
 - LDAP
 - Active Directory
 - RSA SecurID Token Servers
 - RADIUS Identity Servers
 - Certificate Authorities
 - Certificate Authentication Profile
 - Identity Store Sequences
- Policy Elements
- Access Policies
- Monitoring and Reports
- System Administration

General

Name: cisco Status: Enabled

Description:

Identity Group: All Groups Select

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 Select

Password:

Confirm Password:

Change password on next login

User Information

ACS-RESERVED-Never-Expired: True

⚠ = Required fields

Utilisateurs ACS et Active Directory

ACS peut être configuré pour vérifier les utilisateurs dans une base de données AD. L'expiration et la modification du mot de passe sont prises en charge lorsque Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2) est utilisé ; voir [Guide de l'utilisateur de Cisco Secure Access Control System 5.4 : Authentification dans ACS 5.4 : Protocole d'authentification et compatibilité du magasin d'identités](#) pour plus de détails.

Sur un ASA, vous pouvez utiliser la fonctionnalité de gestion des mots de passe, comme décrit dans la section suivante, afin de forcer l'ASA à utiliser MSCHAPv2.

ACS utilise l'appel DCE/RPC (Distributed Computing Environment/Remote Procedure Call) du système de fichiers Internet commun (CIFS) lorsqu'il contacte le répertoire du contrôleur de domaine (DC) afin de modifier le mot de passe :

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 (62:9d:c3:a4:c4:c8)						
▸ 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 peut utiliser à la fois les protocoles RADIUS et TACACS+ afin de contacter ACS pour une modification de mot de passe AD.

ASA avec ACS via RADIUS

Le protocole RADIUS ne prend pas en charge nativement l'expiration du mot de passe ou la modification du mot de passe. Généralement, le protocole PAP (Password Authentication Protocol) est utilisé pour RADIUS. L'ASA envoie le nom d'utilisateur et le mot de passe en clair, et le mot de passe est ensuite chiffré via l'utilisation du secret partagé RADIUS.

Dans un scénario type, lorsque le mot de passe utilisateur a expiré, ACS renvoie un message Radius-Reject à l'ASA. ACS remarque que :

Authentication Summary	
Logged At:	October 2, 2013 8:24:52.446 AM
RADIUS Status:	Authentication failed : <u>24203 User need to change password</u>
NAS Failure:	
Username:	<u>cisco</u>
MAC/IP Address:	192.168.10.67
Network Device:	<u>ASA3 : 192.168.11.250 :</u>
Access Service:	<u>Default Network Access</u>
Identity Store:	Internal Users
Authorization Profiles:	
CTS Security Group:	
Authentication Method:	PAP_ASCII

Pour l'ASA, il s'agit d'un simple message Radius-Reject et l'authentification échoue.

Pour résoudre ce problème, l'ASA autorise l'utilisation de la commande **password-management** sous la configuration tunnel-group :

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

La commande **password-management** modifie le comportement de sorte que l'ASA soit forcé d'utiliser MSCHAPv2, plutôt que PAP, dans Radius-Request.

Le protocole MSCHAPv2 prend en charge l'expiration du mot de passe et la modification du mot de passe. Ainsi, si un utilisateur VPN a atterri dans ce groupe de tunnels spécifique pendant la phase Xauth, la requête Radius de l'ASA inclut maintenant un 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)

Si ACS remarque que l'utilisateur doit modifier le mot de passe, il renvoie un message Radius-Reject avec l'erreur MSCHAPv2 648.

Attribute Value Pairs

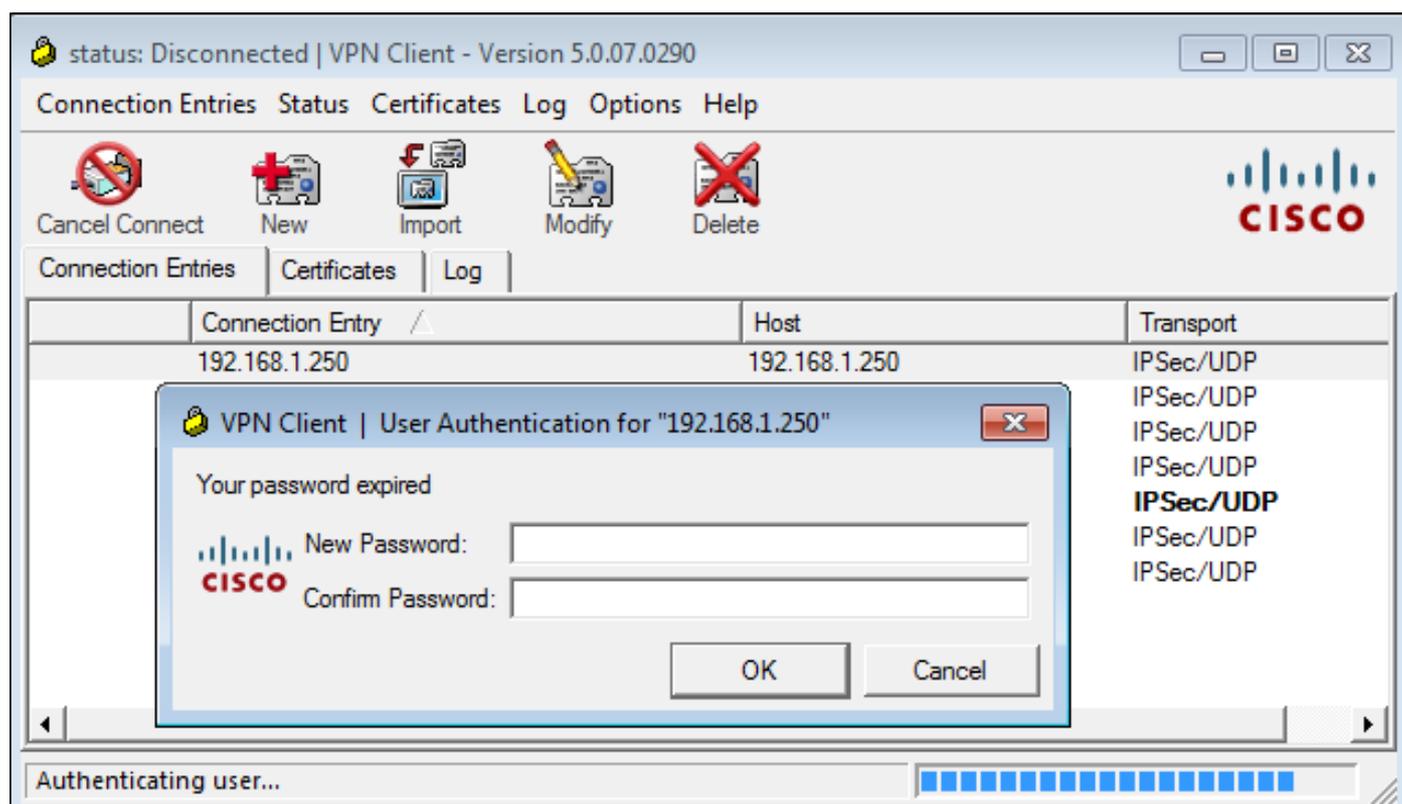
AVP: l=57 t=Vendor-Specific(26) v=Microsoft(311)

VSA: l=51 t=MS-CHAP-Error(2): \000E=648 R=0 C=205

L'ASA comprend ce message et utilise MODE_CFG afin de demander le nouveau mot de passe au 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!

Le client VPN Cisco présente une boîte de dialogue qui demande un nouveau mot de passe :



L'ASA envoie une autre requête Radius avec une charge utile MS-CHAP-CPW et MS-CHAP-NT-Enc-PW (le nouveau mot de passe) :

```
▷ 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): 06000001a3a32falcad97b38
▽ 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)
```

L'ACS confirme la demande et renvoie un Radius-Accept avec MS-CHAP2-Success :

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

Ceci peut être vérifié sur ACS, qui signale une modification réussie du mot de passe 24204 :

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

L'ASA signale ensuite une authentification réussie et poursuit le processus Quick Mode (QM) :

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

ASA avec ACS via TACACS+

De même, TACACS+ peut être utilisé pour l'expiration et la modification des mots de passe. La fonctionnalité de gestion des mots de passe n'est pas nécessaire, car l'ASA utilise toujours TACACS+ avec un type d'authentification ASCII au lieu de MSCHAPv2.

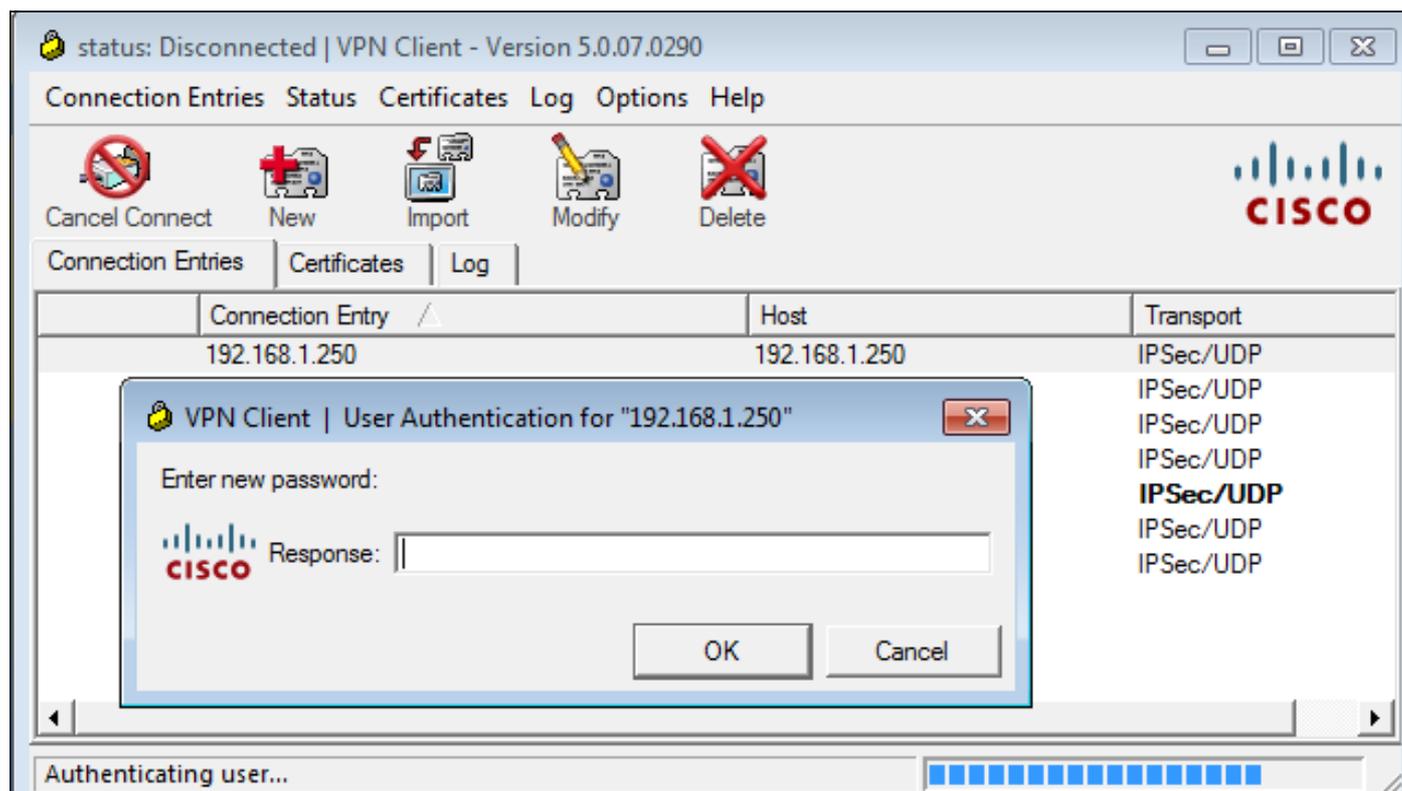
Plusieurs paquets sont échangés et ACS demande un nouveau mot de passe :

```

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

```

Le client VPN Cisco présente une boîte de dialogue (différente de celle utilisée par RADIUS) qui demande un nouveau mot de passe :



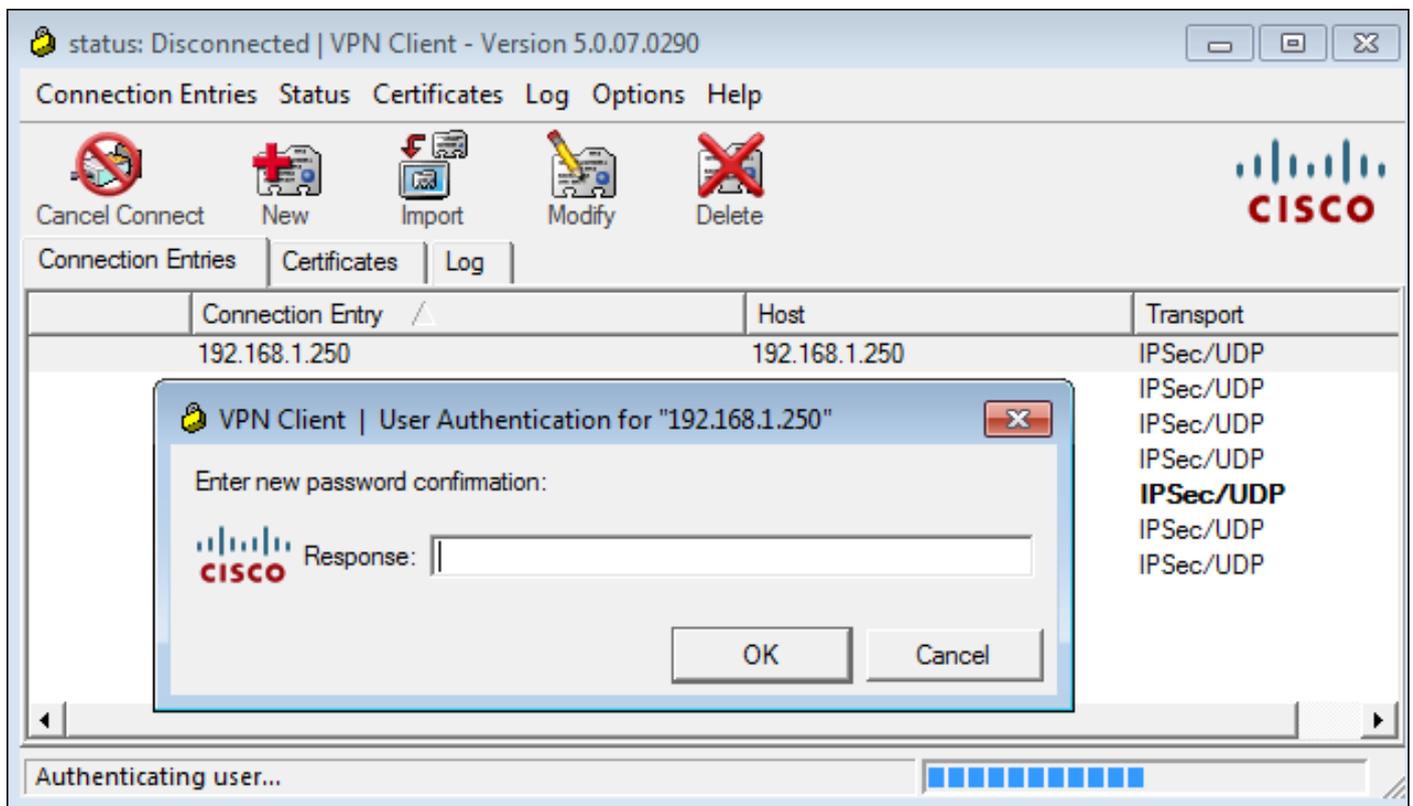
ACS demande la confirmation du nouveau mot de passe :

```

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

```

Le client VPN Cisco présente une boîte de confirmation :



Si la confirmation est correcte, ACS signale une authentification réussie :

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

ACS enregistre ensuite un événement dont le mot de passe a été modifié avec succès :

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

Les débogages ASA montrent l'ensemble du processus d'échange et d'authentification réussie :

```
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.
```

Ce changement de mot de passe est totalement transparent pour ASA. La session TACACS+ est juste un peu plus longue avec plus de paquets de requête et de réponse, qui sont analysés par le client VPN et présentés à l'utilisateur qui change le mot de passe.

ASA avec LDAP

L'expiration et la modification du mot de passe sont entièrement prises en charge par le schéma du serveur Microsoft AD et Sun LDAP.

Pour une modification de mot de passe, les serveurs retournent 'bindresponse = InvalidCredential' avec 'error = 773.' Cette erreur indique que l'utilisateur doit réinitialiser le mot de passe. Les codes d'erreur typiques sont les suivants :

« Error Code Erreur

525	Utilisateur introuvable
52e	Informations d'identification non valides
530	Non autorisé à se connecter pour le moment
531	Impossible d'ouvrir une session sur cette station de travail
532	Mot de passe expiré
533	Compte désactivé
701	Compte expiré
773	L'utilisateur doit réinitialiser le mot de passe
775	Compte utilisateur verrouillé

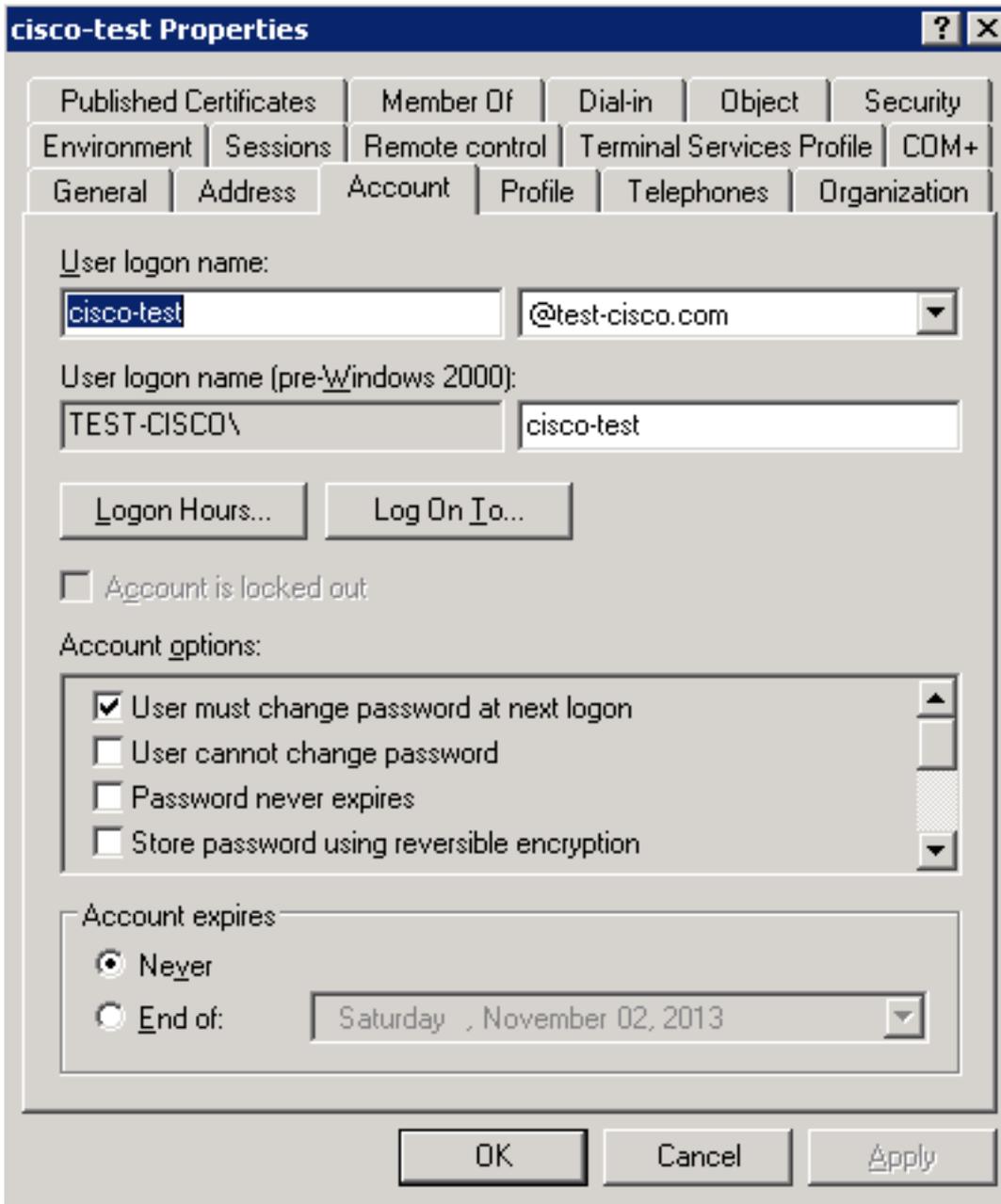
Configurez le serveur LDAP :

```
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
```

Utilisez cette configuration pour le groupe de tunnels et la fonction de gestion des mots de passe :

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

Configurez l'utilisateur AD de sorte qu'une modification du mot de passe soit requise :



Lorsque l'utilisateur tente d'utiliser le client VPN Cisco, l'ASA signale un mot de passe non valide :

```
ASA(config-tunnel-general)# debug ldap 255
<some output omitted 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

```

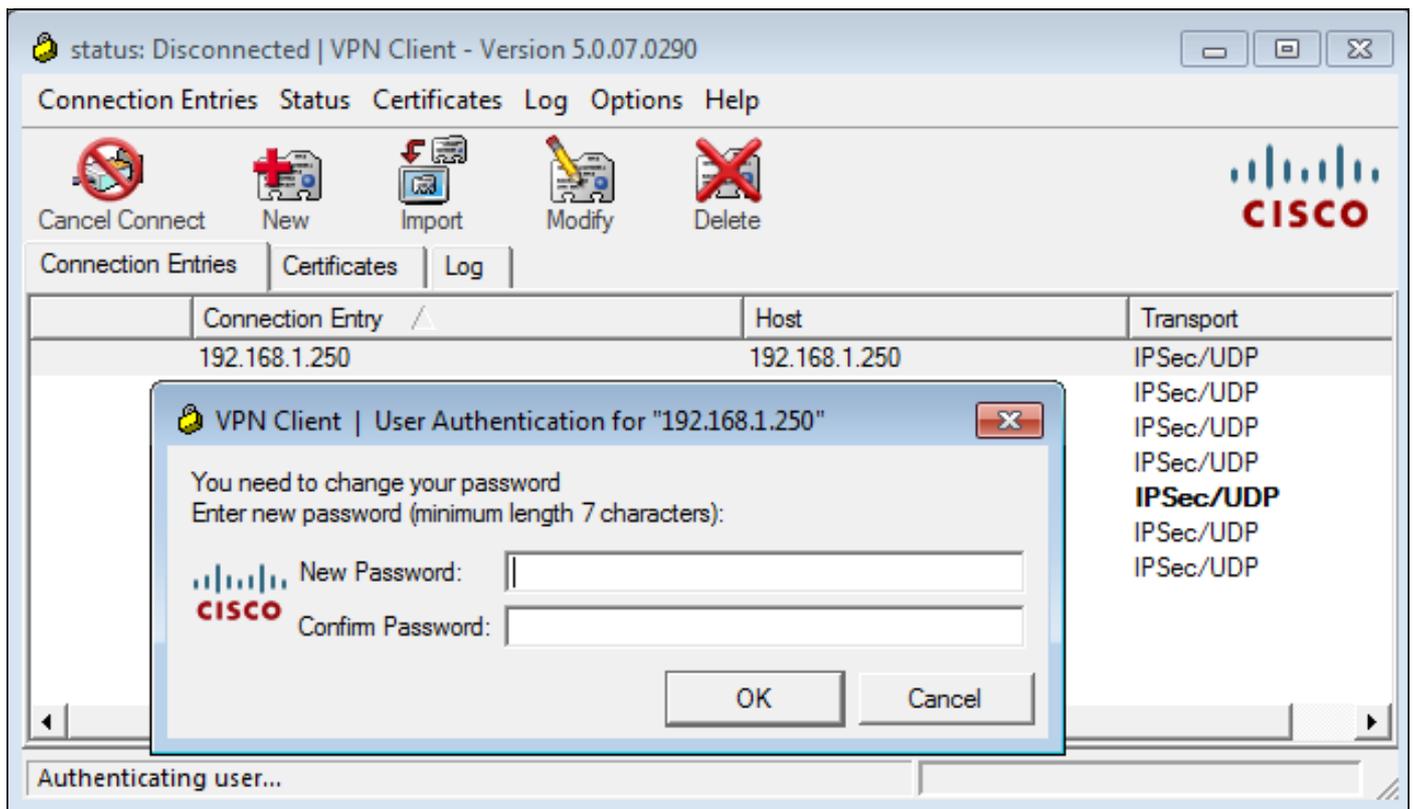
Si les informations d'identification ne sont pas valides, l'erreur 52e apparaît :

```

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

```

Le client VPN Cisco demande ensuite un changement de mot de passe :



Cette boîte de dialogue diffère de la boîte de dialogue utilisée par TACACS ou RADIUS car elle affiche la stratégie. Dans cet exemple, la stratégie comporte une longueur de mot de passe minimale de sept caractères.

Une fois le mot de passe modifié, l'ASA peut recevoir ce message d'échec du serveur LDAP :

```

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

```

La stratégie Microsoft nécessite l'utilisation du protocole SSL (Secure Sockets Layer) pour la modification du mot de passe. Modifier la configuration :

```

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

```

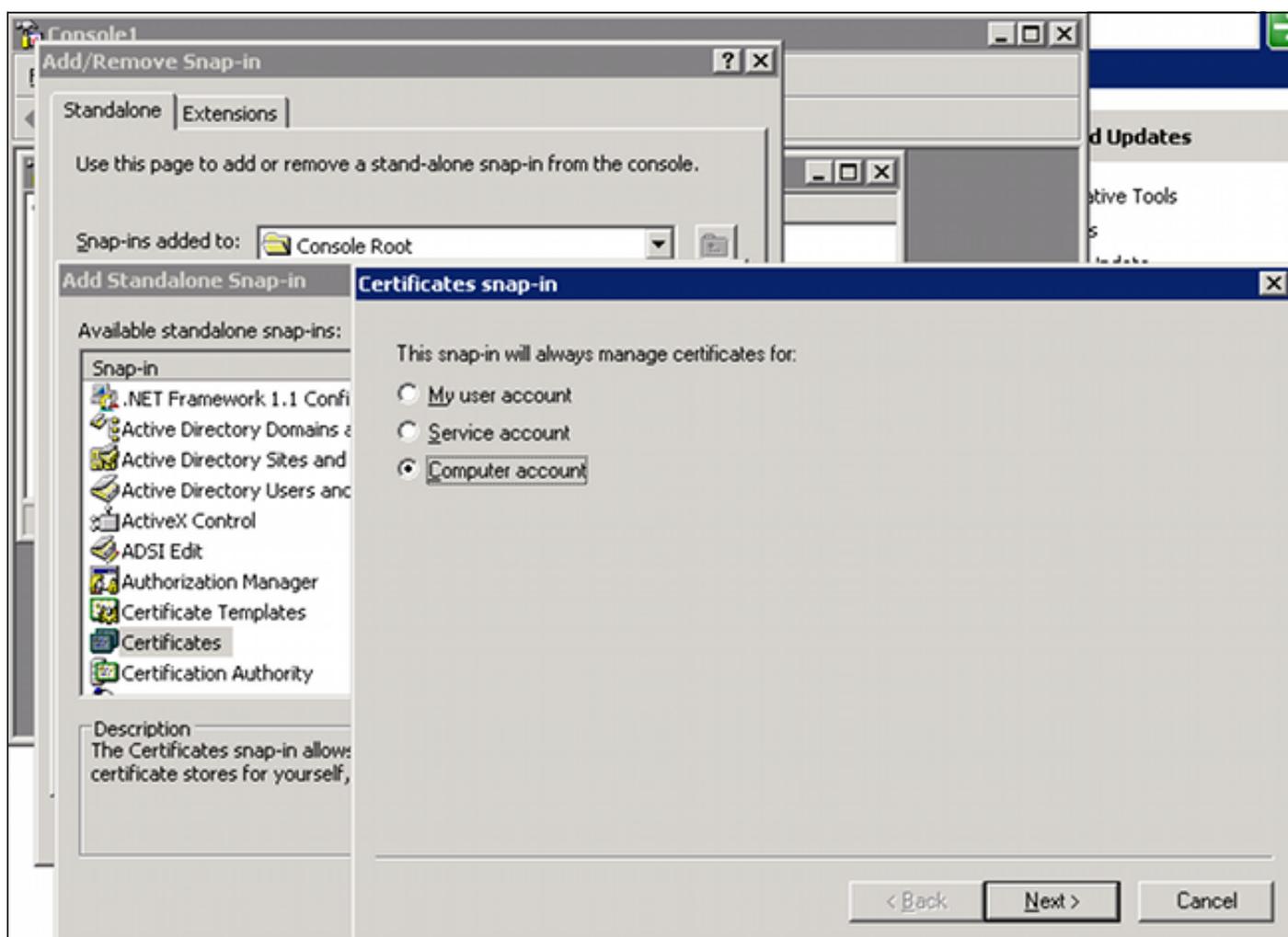
Microsoft LDAP pour SSL

Par défaut, Microsoft LDAP sur SSL ne fonctionne pas. Pour activer cette fonction, vous devez installer le certificat du compte d'ordinateur avec le poste de clé approprié. Reportez-vous à [Comment activer LDAP sur SSL avec une autorité de certification tierce](#) pour plus de détails.

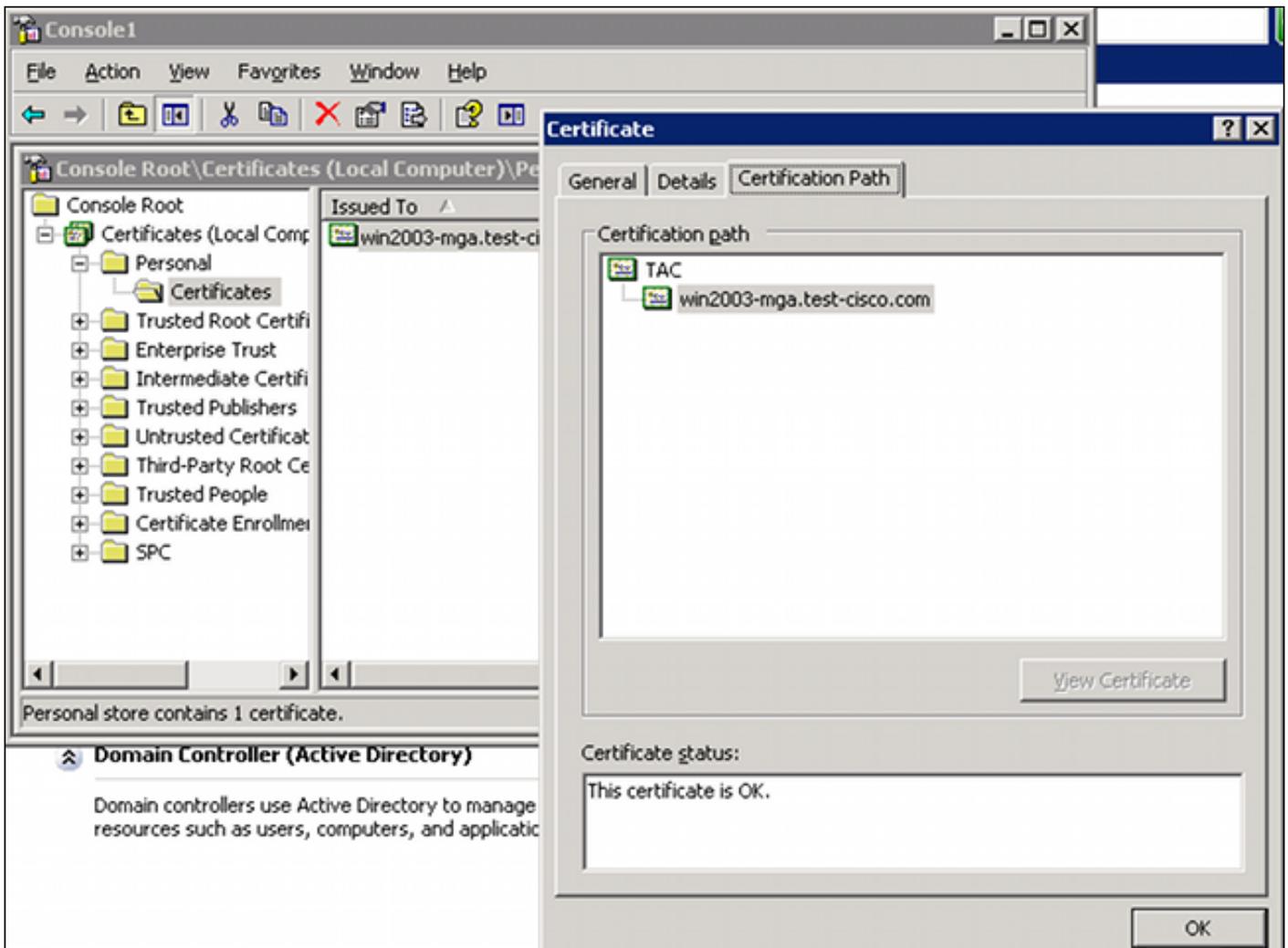
Le certificat peut même être un certificat auto-signé, car l'ASA ne vérifie pas le certificat LDAP. Reportez-vous à l'ID de bogue Cisco [CSCui40212](#), « Autoriser ASA à valider le certificat du serveur LDAPS », pour obtenir une demande d'amélioration associée.

Note: ACS vérifie le certificat LDAP dans les versions 5.5 et ultérieures.

Pour installer le certificat, ouvrez la console mmc, sélectionnez **Ajouter/Supprimer un composant logiciel enfichable**, ajoutez le certificat et choisissez **Compte d'ordinateur** :



Sélectionnez **Ordinateur local**, importez le certificat dans le magasin personnel et déplacez le certificat d'autorité de certification associé dans le magasin approuvé. Vérifiez que le certificat est approuvé :



Il y a un bogue dans la version 8.4.2 d'ASA, où cette erreur peut être renvoyée lorsque vous essayez d'utiliser LDAP sur 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 fonctionne correctement avec la même configuration. Il existe deux sessions LDAP. La première session renvoie un échec avec le code 773 (mot de passe expiré), tandis que la deuxième session est utilisée pour la modification du mot de passe :

```
[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 omitted for clarity>
accountExpires: value = 13025656800000000 <----- 100ns intervals since
January 1, 1601 (UTC)

```

Pour vérifier la modification du mot de passe, consultez les paquets. La clé privée du serveur LDAP peut être utilisée par Wireshark afin de déchiffrer le trafic SSL :

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]

Les débogages IKE (Internet Key Exchange)/Authentication, Authorization, and Accounting (AAA) sur l'ASA sont très similaires à ceux présentés dans le scénario d'authentification RADIUS.

LDAP et avertissement avant expiration

Pour LDAP, vous pouvez utiliser une fonction qui envoie un avertissement avant l'expiration d'un mot de passe. L'ASA avertit l'utilisateur 90 jours avant l'expiration du mot de passe avec ce paramètre :

```

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

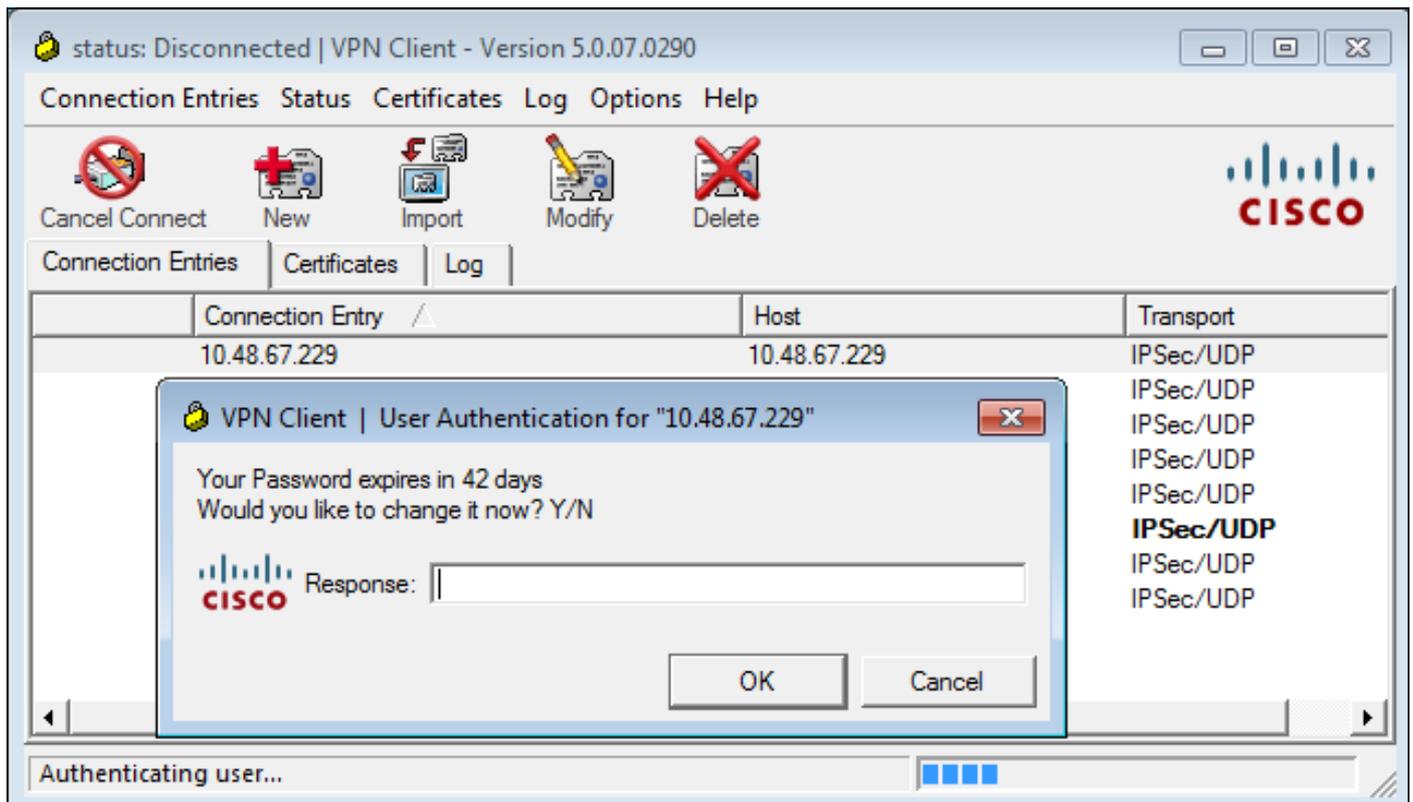
```

Ici, le mot de passe expire dans 42 jours, et l'utilisateur essaie de se connecter :

```
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'ASA envoie un avertissement et offre l'option de changement de mot de passe :



Si l'utilisateur choisit de modifier le mot de passe, une invite lui demande un nouveau mot de passe et la procédure normale de modification du mot de passe commence.

ASA et L2TP

Les exemples précédents présentaient IKE version 1 (IKEv1) et un VPN IPSec.

Pour les protocoles L2TP (Layer 2 Tunneling Protocol) et IPSec, le protocole PPP est utilisé comme transport pour l'authentification. MSCHAPv2 est requis au lieu du protocole PAP pour qu'un changement de mot de passe fonctionne :

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

Pour l'authentification étendue dans L2TP à l'intérieur de la session PPP, MSCHAPv2 est négocié

```
▶ 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
```

Lorsque le mot de passe utilisateur a expiré, une erreur avec le code 648 est renvoyée :

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

Un changement de mot de passe est alors nécessaire. Le reste du processus est très similaire au scénario pour RADIUS avec MSCHAPv2.

Reportez-vous à [L2TP sur IPsec entre un PC Windows 2000/XP et PIX/ASA 7.2 à l'aide de l'exemple de configuration de clé prépartagée](#) pour plus de détails sur la configuration de L2TP.

Client VPN SSL ASA

Les exemples précédents ont fait référence à IKEv1 et au client VPN Cisco, qui est en fin de vie (EOL).

La solution recommandée pour un VPN d'accès à distance est Cisco AnyConnect Secure Mobility, qui utilise les protocoles IKE version 2 (IKEv2) et SSL. Les fonctions de modification et d'expiration des mots de passe fonctionnent exactement de la même manière pour Cisco AnyConnect que pour le client VPN Cisco.

Pour IKEv1, les données de modification et d'expiration du mot de passe ont été échangées entre l'ASA et le client VPN au cours de la phase 1.5 (configuration Xauth/mode).

Pour IKEv2, il est similaire ; le mode de configuration utilise des paquets CFG_REQUEST/CFG_REPLY.

Pour SSL, les données se trouvent dans la session DTLS (Datagram Transport Layer Security) de contrôle.

La configuration est identique pour l'ASA.

Voici un exemple de configuration avec Cisco AnyConnect et le protocole SSL avec un serveur LDAP sur 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

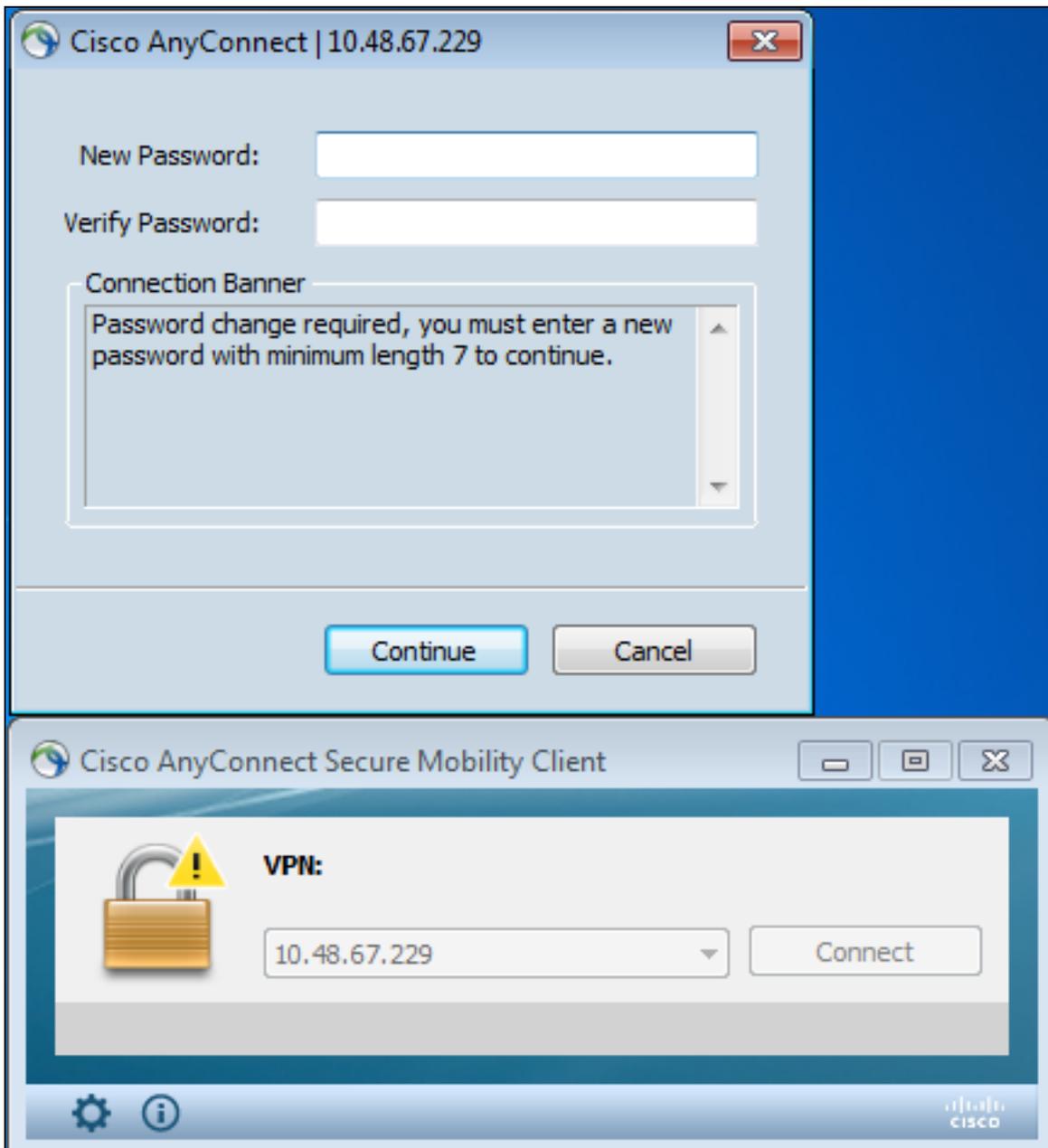
webvpn
  enable outside
  anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
  anyconnect enable
  tunnel-group-list enable

group-policy MY internal
group-policy MY attributes
  vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless

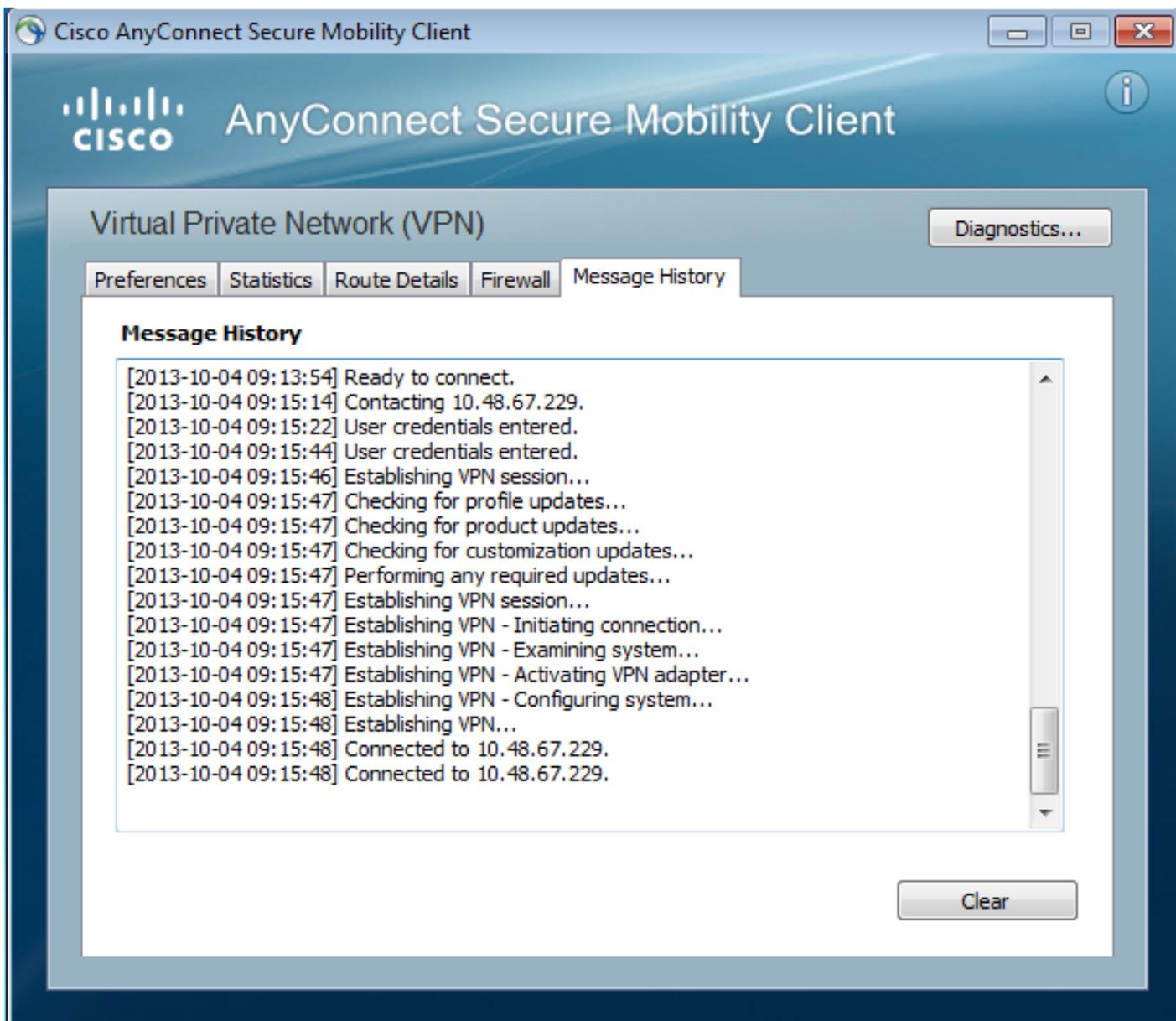
tunnel-group RA type remote-access
tunnel-group RA general-attributes
  address-pool POOL
  authentication-server-group LDAP
  default-group-policy MY
  password-management
tunnel-group RA webvpn-attributes
  group-alias RA enable
  without-csd

ip local pool POOL 192.168.11.100-192.168.11.105 mask 255.255.255.0
```

Une fois le mot de passe correct (qui a expiré) fourni, Cisco AnyConnect tente de se connecter et demande un nouveau mot de passe :



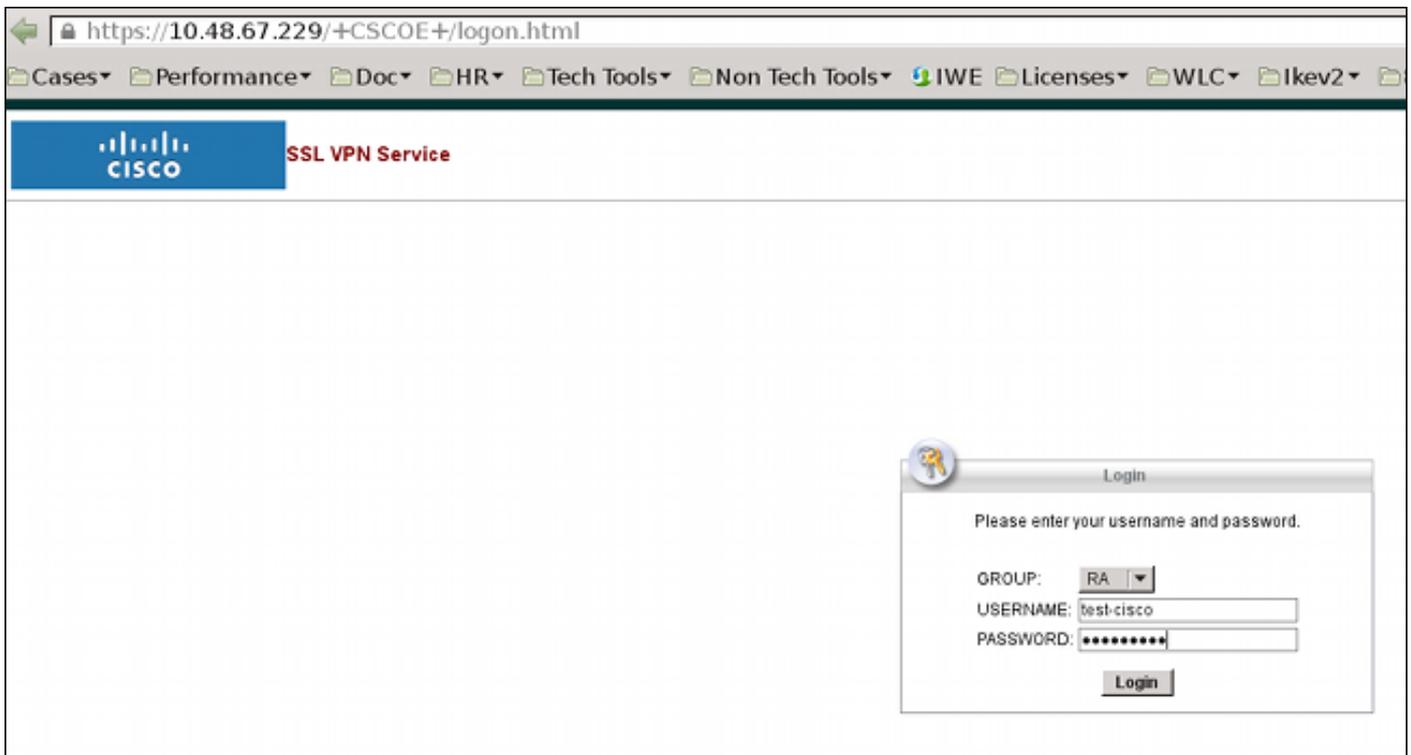
Les journaux indiquent que les informations d'identification de l'utilisateur ont été entrées deux fois :



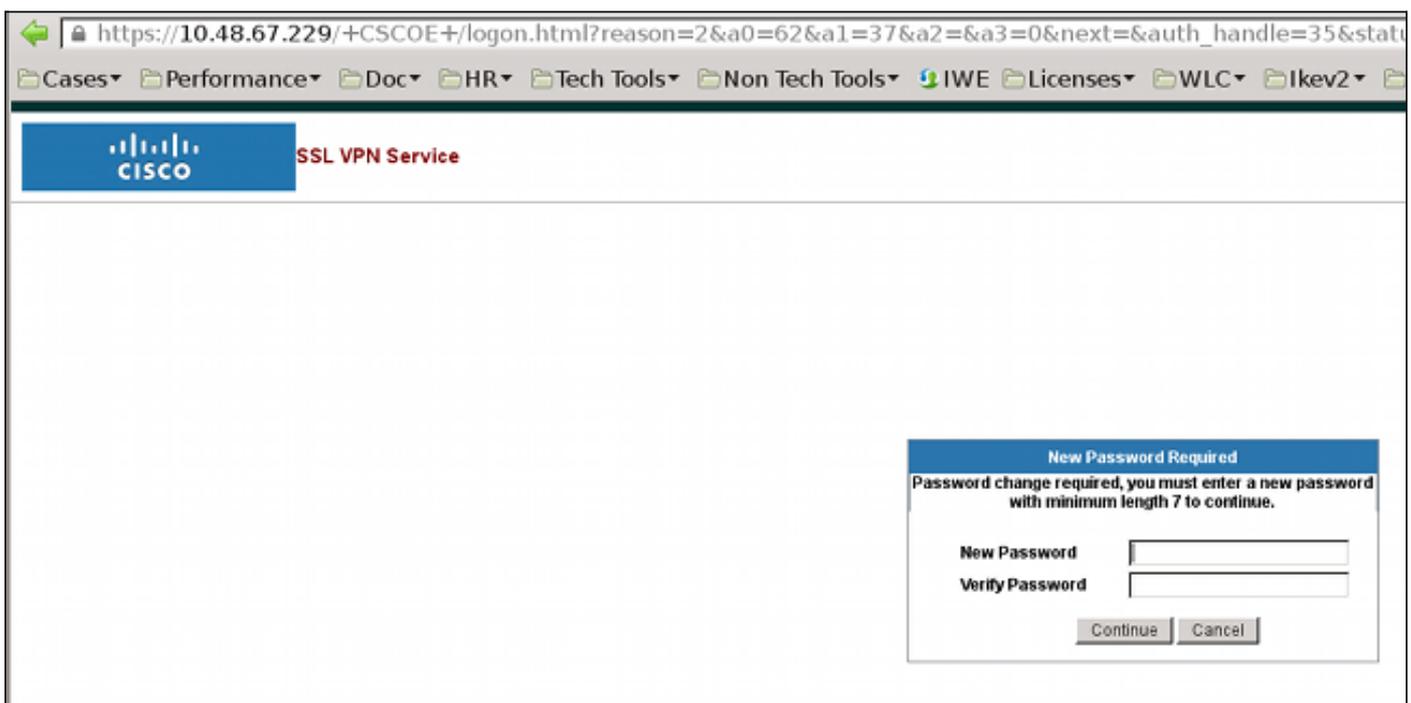
Des journaux plus détaillés sont disponibles dans l'outil de rapport Diagnostic AnyConnect (DART).

Portail Web ASA SSL

Le même processus de connexion se produit dans le portail Web :



Le même processus d'expiration et de modification de mot de passe se produit :



Mot de passe de modification d'utilisateur ACS

S'il n'est pas possible de modifier le mot de passe sur le VPN, vous pouvez utiliser le service Web dédié UCP (ACS User Change Password). Reportez-vous au [Guide du développeur de logiciels pour Cisco Secure Access Control System 5.4 : Utilisation des services Web UCP](#).

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Guide de configuration de la gamme Cisco ASA 5500 à l'aide de la CLI, 8.4 et 8.6 : Configuration d'un serveur externe pour l'autorisation de l'utilisateur de l'appareil de sécurité](#)
- [Support et documentation techniques - Cisco Systems](#)