

# آاهانا - ASA Remote Access VPN IKE/SSL ناوكت لانا مل اهرنا نغنا و رورم لانا ةم لك ةنا نال ص RADIUS و TACACS و LDAP

## المأناوات

- [المأناة](#)
- [الماأناااا الأناااا](#)
- [الماأناااا](#)
- [الماأناااا المأناة](#)
- [الماأناااا](#)
- [ASA مع المأناة المأناة](#)
- [ACS والمأنااااا المأناااا](#)
- [مأناااا ACS و Active Directory](#)
- [ASA مع ACS عنا RADIUS](#)
- [ASA مع ACS عنا TACACS+](#)
- [ASA مع LDAP](#)
- [LDAP ل Microsoft SSL](#)
- [LDAP والننااا قبل اناااا الصلاأناة](#)
- [ASA و L2TP](#)
- [ASA SSL VPN عمل](#)
- [بواأنا الونا ASA SSL](#)
- [كلمة مرور ناأنااا المأناااا ل ACS](#)
- [النأنااا من الصأناة](#)
- [اأناااا الأأنااا واصلأنااا](#)
- [معلومااا نااا صلة](#)

## المأناة

ناأنا هذا المأنااا مناااا انااااا صلاأناة كلمة المرور وناأنااا كلمة المرور على نأنا VPN للواصول عن باءااا نأناااا  
على أناااا الأنااا القابل للناأنااا (ASA) من Cisco. وناأنااا الوأناااا:

- العملاا المأنااااا: عمل Cisco VPN و Cisco AnyConnect Secure Mobility
- البروااااااا المأناااا: بروااااااا الوصول إلى الالناأنا أأنااا (LDAP) و TACACS و RADIUS
- مناااا مأنااااا على نأنااااا الأناااا (ACS) من Cisco: أأنااا (AD) المأنااااا  
والنأناااا

## الماأناااا الأنااااا

## المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة تكوين ASA من خلال واجهة سطر الأوامر (CLI)
- معرفة أساسية بتكوين VPN على ASA
- معرفة أساسية ب Cisco Secure ACS

## المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- جهاز Cisco Adaptive Security Appliance، الإصدار 8.4 والإصدارات الأحدث
  - نظام التشغيل Microsoft Windows Server 2003 SP1
  - نظام التحكم بالوصول الآمن من Cisco، الإصدار 5.4 أو إصدار أحدث
  - Cisco AnyConnect Secure Mobility، الإصدار 3.1
  - عميل شبكة VPN من Cisco، الإصدار 5
- تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين مسموح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## التكوين

ملاحظات:

استخدم [أداة بحث الأوامر \(للعلماء المسجلين فقط\)](#) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

ارجع إلى [معلومات مهمة عن أوامر تصحيح الأخطاء قبل أن تستخدم أوامر debug](#).

## ASA مع المصادقة المحلية

لا يسمح ASA مع المستخدمين المحددين محليا باستخدام ميزات انتهاء صلاحية كلمة المرور أو تغيير كلمة المرور. يلزم وجود خادم خارجي، مثل RADIUS أو TACACS أو LDAP أو Windows NT.

## ACS والمستخدمون المحليون

يدعم ACS كل من انتهاء صلاحية كلمة المرور وتغيير كلمة المرور للمستخدمين المحددين محليا. على سبيل المثال، يمكنك إجبار المستخدمين الذين تم إنشاؤهم حديثا على تغيير كلمة المرور الخاصة بهم عند تسجيل دخولهم التالي، أو يمكنك تعطيل حساب في تاريخ معين:

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:  Status:

Description:

Identity Group:

**Account Disable**

Disable Account if Date Exceeds:   (yyyy-Mmm-dd)

**Password Information**

Password must:

- Contain 4 - 32 characters

Password Type:

Password:

Confirm Password:

Change password on next login

**User Information**

There are no additional identity attributes defined for user records

يمكنك تكوين نهج كلمة المرور لكافة المستخدمين. على سبيل المثال، بعد انتهاء صلاحية كلمة المرور، يمكنك تعطيل حساب المستخدم (منعه بدون إمكانية تسجيل الدخول)، أو يمكنك تقديم الخيار لتغيير كلمة المرور:

System Administration > Users > Authentication Settings

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

الإعدادات الخاصة بالمستخدم لها الأولوية على الإعدادات العامة.  
ACS-RESERVED-Never-Expired سمة داخلية لهوية المستخدم.

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

**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

تم تمكين هذه السمة من قبل المستخدم ويمكن استخدامها لتعطيل إعدادات انتهاء صلاحية الحساب العمومي. باستخدام هذا الإعداد، لا يتم تعطيل الحساب حتى إذا كان النهج العام يشير إلى أنه يجب أن يكون:

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-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

## مستخدمو ACS و Active Directory

يمكن تكوين ACS لفحص المستخدمين في قاعدة بيانات AD. يتم دعم انتهاء صلاحية كلمة المرور وتغييرها عند استخدام بروتوكول المصادقة لتأكيد الاتصال بقيمة التحدي ل Microsoft الإصدار 2 (MSCHAPv2)؛ راجع [دليل المستخدم لنظام التحكم بالوصول الآمن من Cisco 5.4: المصادقة في ACS 5.4](#): توافق بروتوكول المصادقة ومخزن الهوية للحصول على تفاصيل.

على ASA، يمكنك استخدام ميزة إدارة كلمة المرور، كما هو موضح في القسم التالي، لإجبار ASA على استخدام MSCHAPv2.

يستخدم ACS استدعاء بيئة الحوسبة الموزعة/الإجراء البعيد (DCE/RPC) لنظام ملفات الإنترنت العام (CIFS) عند اتصاله بدليل وحدة التحكم بالمجال (DC) لتغيير كلمة المرور:

| 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)   |                |                |      |     |                              |

يمكن أن يستخدم ASA كلا من بروتوكولات RADIUS و TACACS+ للاتصال ب ACS لتغيير كلمة مرور AD.

## ASA مع ACS عبر RADIUS

لا يدعم بروتوكول RADIUS بطبيعتها انتهاء صلاحية كلمة المرور أو تغيير كلمة المرور. نموذجياً، يتم استخدام بروتوكول مصادقة كلمة المرور (PAP) ل RADIUS. يرسل ال ASA ال username وكلمة في نص عادي، وبعد ذلك يشفر الكلمة من خلال إستعمال من ال RADIUS يشارك سر.

في سيناريو نموذجي عند انتهاء صلاحية كلمة مرور المستخدم، يرجع ACS رسالة رفض RADIUS إلى ASA. يشير إلى ACS:

| 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   |

بالنسبة إلى ASA، فإنها رسالة رفض RADIUS بسيطة، وتفشل المصادقة.

لحل هذه المشكلة، يسمح ASA باستخدام الأمر `password-management` ضمن تكوين مجموعة النفق:

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

يقوم الأمر `password-management` بتغيير السلوك بحيث يتم فرض ASA لاستخدام MSCHAPv2، بدلا من PAP، في طلب Radius.

يدعم بروتوكول MSCHAPv2 انتهاء صلاحية كلمة المرور وتغيير كلمة المرور. لذلك، إذا هبط مستخدم شبكة VPN في مجموعة النفق المحددة أثناء مرحلة Xauth، فإن طلب Radius من ASA يتضمن الآن تحديا 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)                            |

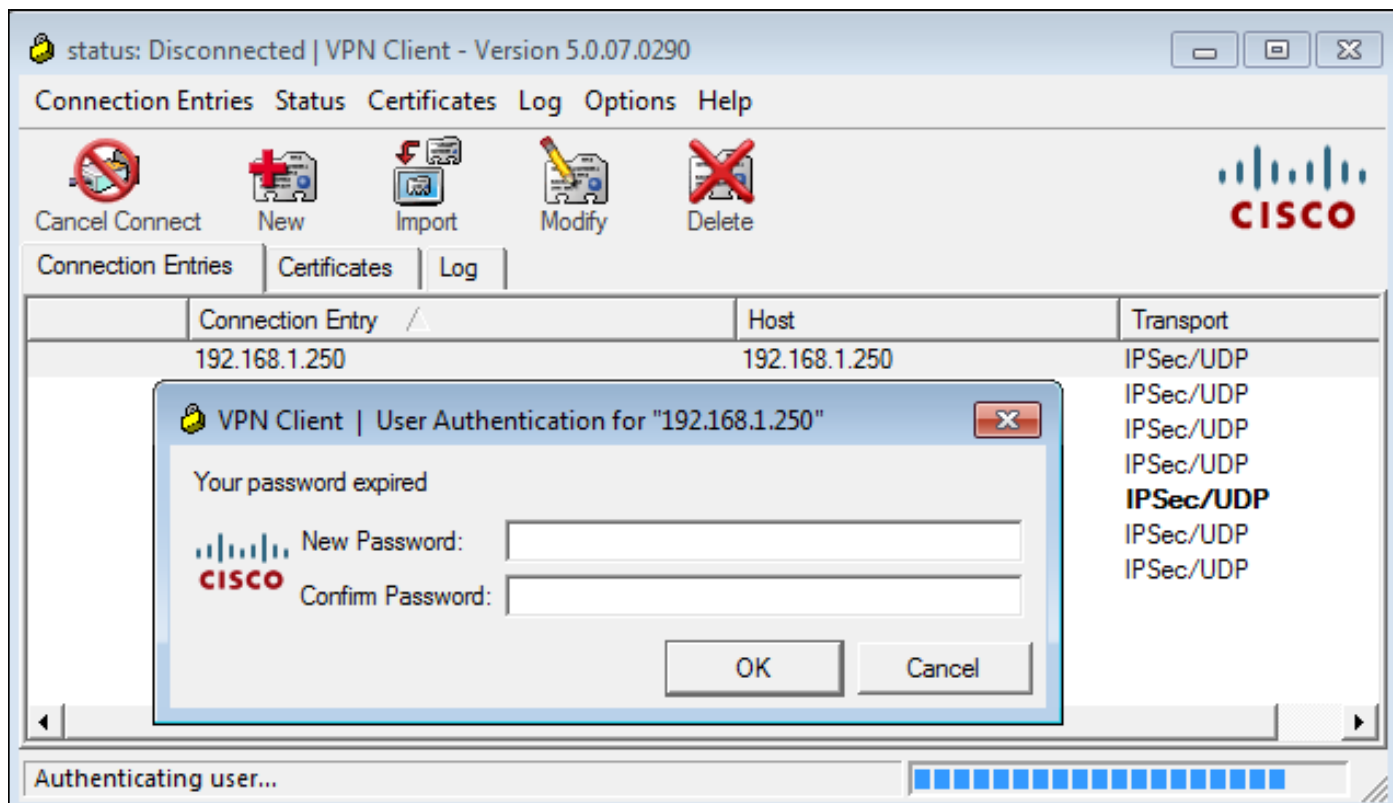
إذا لاحظ ACS أن المستخدم يحتاج إلى تغيير كلمة المرور، فإنه يرجع رسالة رفض Radius مع خطأ MSCHAPv2.648

## 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

يفهم ال ASA أن رسالة ويستعمل MODE\_CFG طلبت الكلمة جديد من ال VPN cisco زبون:

```
,Oct 02 06:22:26 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67  
!Received Password Expiration from Auth server  
يقدم عميل Cisco VPN حوار يطلب كلمة مرور جديدة:
```



يرسل ASA طلب Radius آخر مع MS-CHAP-CPW و MS-CHAP-NT-ENC-PW حمولة (كلمة المرور الجديدة):



```
▷ 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)
```

تؤكد ACS الطلب وتعيد قبول RADIUS مع MS-CHAP2-SUCCESS:

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

يمكن التحقق من هذا الإجراء على ACS، الذي يشير إلى "تغيير كلمة المرور 24204 بنجاح":

| 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  |

يبلغ ASA بعد ذلك عن المصادقة الناجحة ويواصل عملية الوضع السريع (QM):

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

## ASA مع ACS عبر TACACS+

وبالمثل، يمكن استخدام TACACS+ لانهاء صلاحية كلمة المرور وتغييرها. لا يلزم وجود ميزة إدارة كلمة المرور، لأن ASA لا يزال يستخدم TACACS+ مع نوع مصادقة ASCII بدلا من MSCHAPv2.

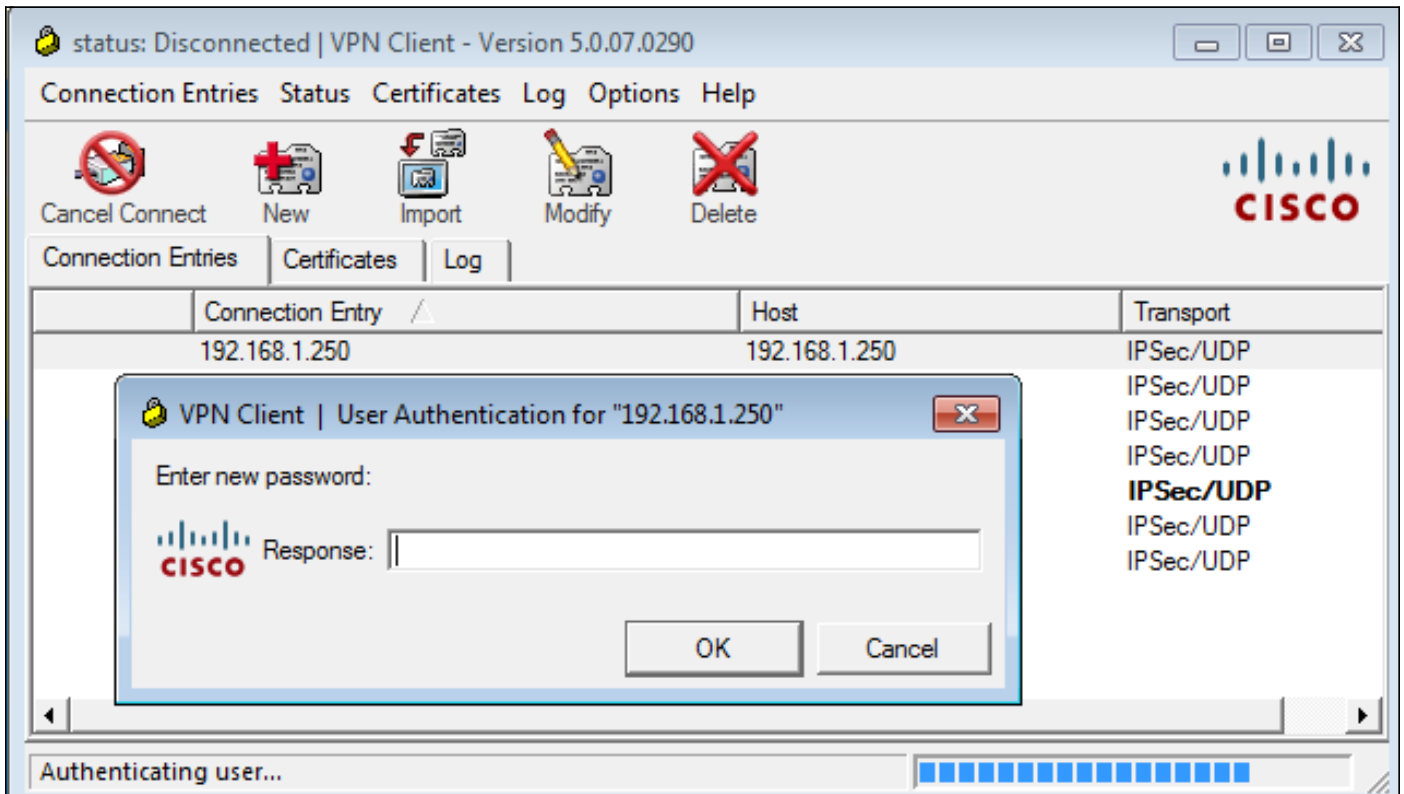
يتم تبادل حزم متعددة، ويطلب ACS كلمة مرور جديدة:

```

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

```

يقدم عميل شبكة VPN من Cisco مربع حوار (يختلف عن الحوار المستخدم بواسطة RADIUS) يطلب كلمة مرور جديدة:



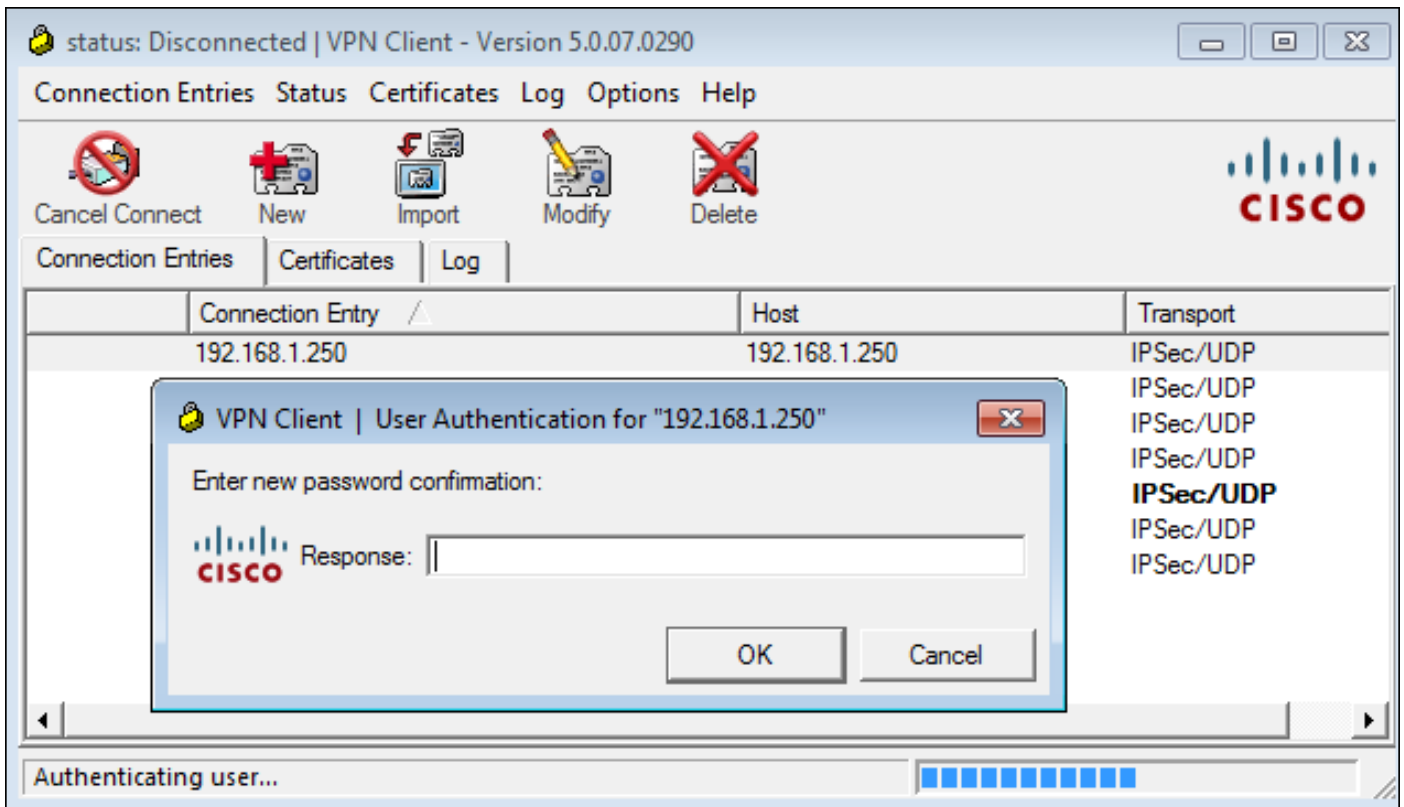
يطلب ACS تأكيد كلمة المرور الجديدة:

```

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

```

يقدم عميل Cisco VPN مربع تأكيد:



إذا كان التأكيد صحيحا، يبلغ ACS عن مصادقة ناجحة:

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

يقوم ACS بعد ذلك بتسجيل حدث تم فيه تغيير كلمة المرور بنجاح:

## 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

تظهر تصحيح أخطاء ASA عملية الاستبدال بالكامل والمصادقة الناجحة:

```
,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

```

تغيير كلمة المرور هذا شفاف تماما ل ASA. أطول قليلا من جلسة TACACS+ مع المزيد من حزم الطلب والرد، والتي يتم تحليلها بواسطة عميل VPN ويتم تقديمها إلى المستخدم الذي يقوم بتغيير كلمة المرور.

## LDAP مع ASA

تم دعم انتهاء صلاحية كلمة المرور وتغييرها بالكامل بواسطة مخطط خادم Microsoft AD و Sun LDAP.

لتغيير كلمة المرور، ترجع الخوادم 'bindResponse = invalidCredentials' مع 'error = 773'. يشير هذا الخطأ إلى أنه يجب على المستخدم إعادة تعيين كلمة المرور. تتضمن رموز الأخطاء النموذجية:

| الخطأ   | رمز الخطأ |
|---|-----------|
| لم يتم العثور على المستخدم  | 525       |
| بيانات الاعتماد غير الصالحة   | 52 اس     |
| مسموح بتسجيل الدخول في هذا الوقت غير مسموح بتسجيل الدخول في محطة العمل هذه انتهت صلاحية كلمة المرور | 530       |
| تم تعطيل الحساب انتهت صلاحية الحساب يجب على المستخدم إعادة تعيين كلمة                               | 531       |
| الخطأ   | 532       |
| الخطأ   | 533       |
| الخطأ   | 701       |
| الخطأ   | 773       |

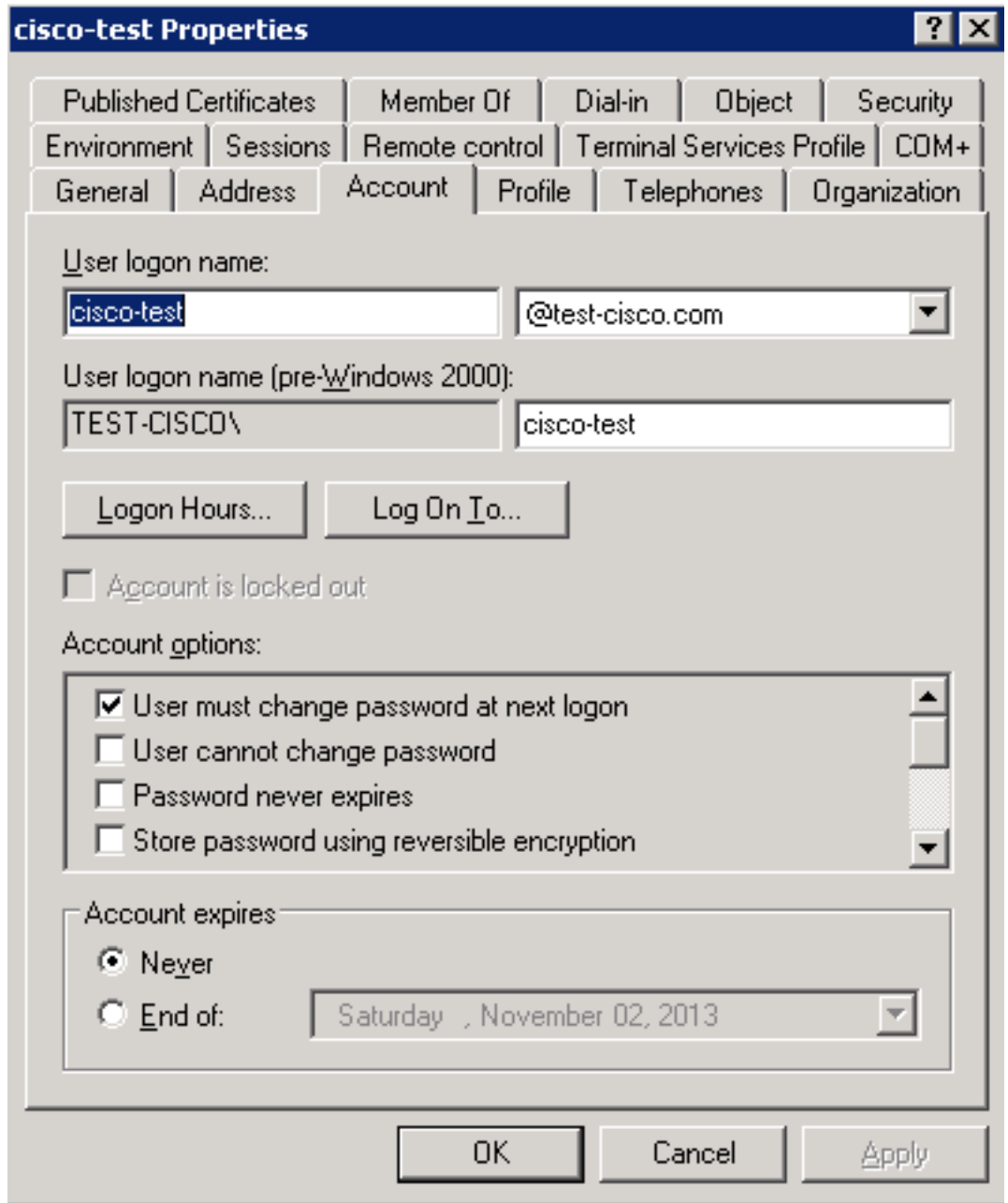
قم بتكوين خادم LDAP:

```
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
```

أستخدم هذا التكوين لمجموعة النفق وميزة إدارة كلمة المرور:

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

قم بتكوين مستخدم AD لذلك يلزم تغيير كلمة المرور:



عندما يحاول المستخدم استخدام عميل Cisco VPN، يبلغ ASA عن كلمة مرور غير صحيحة:

```

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

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 [111]
[Base DN = [CN=USers,DC=test-cisco,DC=com
[Filter = [sAMAccountName=cisco-test
[Scope = [SUBTREE
[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 [111]

```



```

DC=test-cisco,DC=com
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 [111]
credentials
:Message (cisco-test): 80090308: LdapErr: DSID-0C090334, comment [111]
AcceptSecurityContext error, data 773, vece
Invalid password for cisco-test [111]

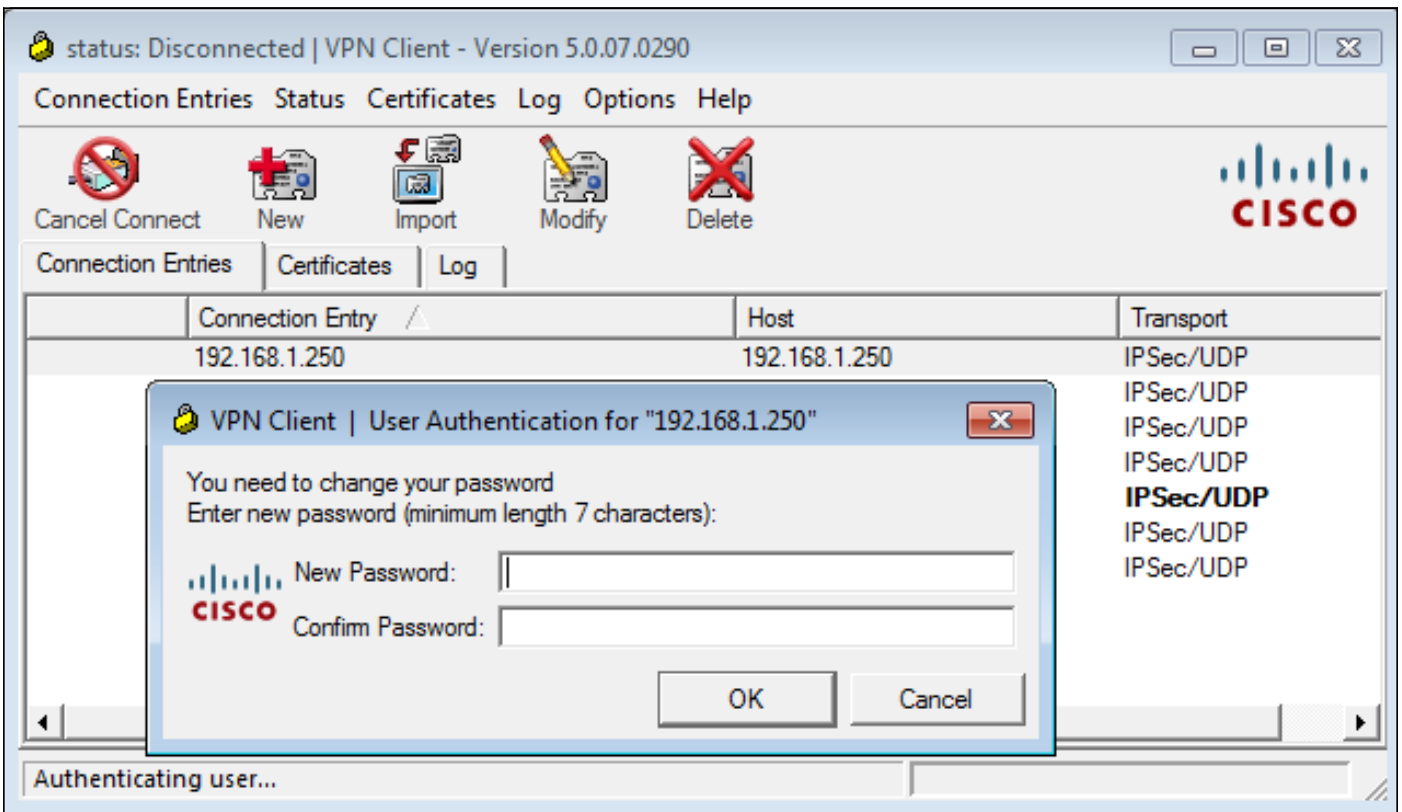
```

إذا كانت بيانات الاعتماد غير صحيحة، يظهر الخطأ 52e:

```

:Message (cisco-test): 80090308: LdapErr: DSID-0C090334, comment [110]
AcceptSecurityContext error, data 52e, vece
يطلب عميل Cisco VPN بعد ذلك تغيير كلمة المرور:

```



تختلف شاشة العرض هذه عن مربع الحوار المستخدم من قبل TACACS أو RADIUS لأنها تعرض السياسة. في هذا مثال، السياسة حد أدنى لطول كلمة المرور سبعة رمز.

ما إن يغير المستعمل الكلمة، ال ASA يمكن إستلمت هذا إخفاق رسالة من ال LDAP نادل:

```

Modify Password for cisco-test successfully converted password to unicode [113]
modify failed, no SSL enabled on connection [113]
يتطلب نهج Microsoft استخدام طبقة مأخذ التوصيل الآمنة (SSL) لتعديل كلمة المرور. غيرت التشكيل:

```

```

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

```

## SSL J Microsoft LDAP

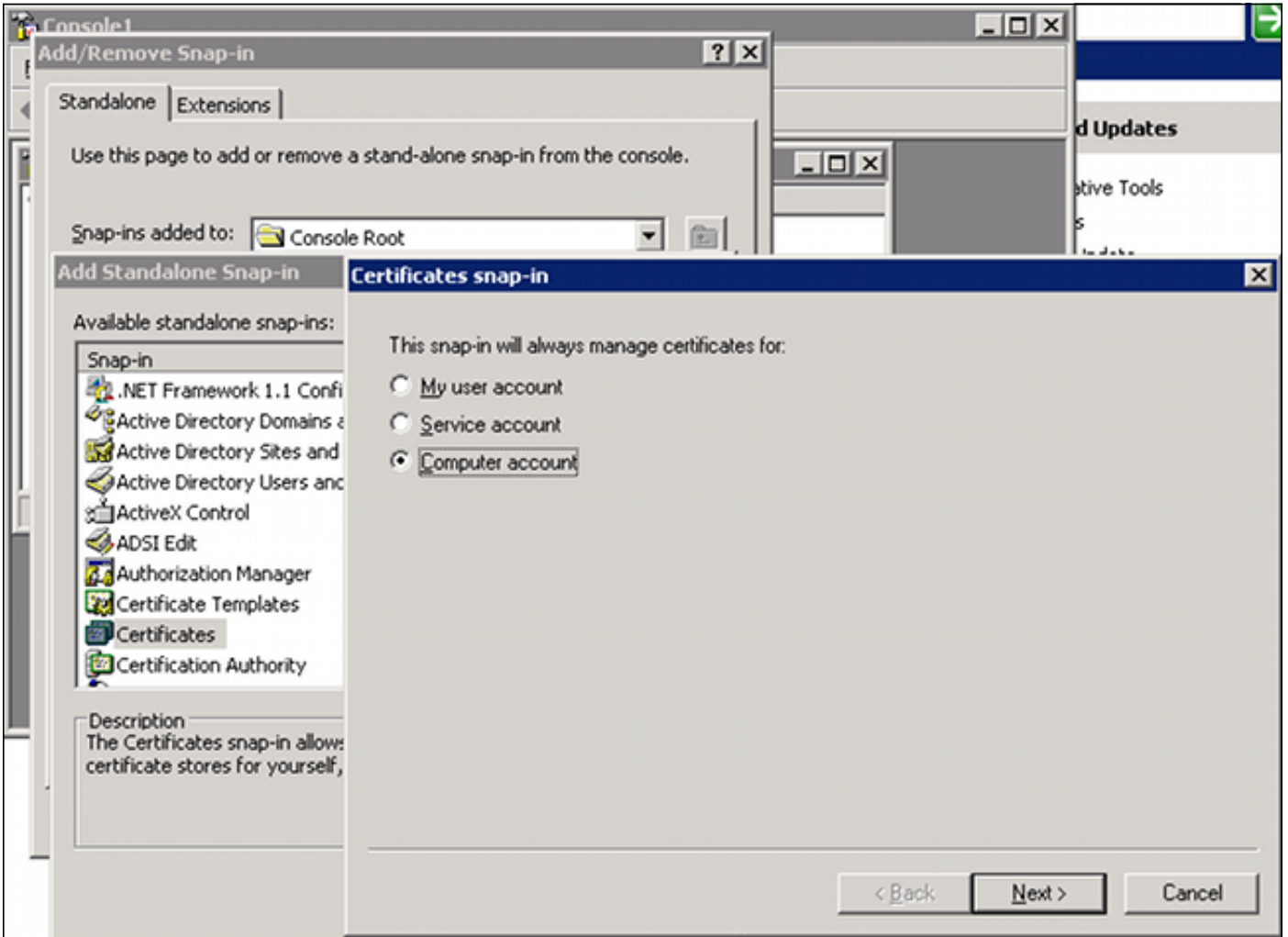
بشكل افتراضي، لا يعمل Microsoft LDAP عبر SSL. لتمكين هذه الوظيفة، يجب تثبيت شهادة حساب الكمبيوتر

بملحق المفتاح الصحيح. راجع كيفية تمكين LDAP عبر SSL باستخدام مرجع مصدق تابع لجهة خارجية للحصول على مزيد من التفاصيل.

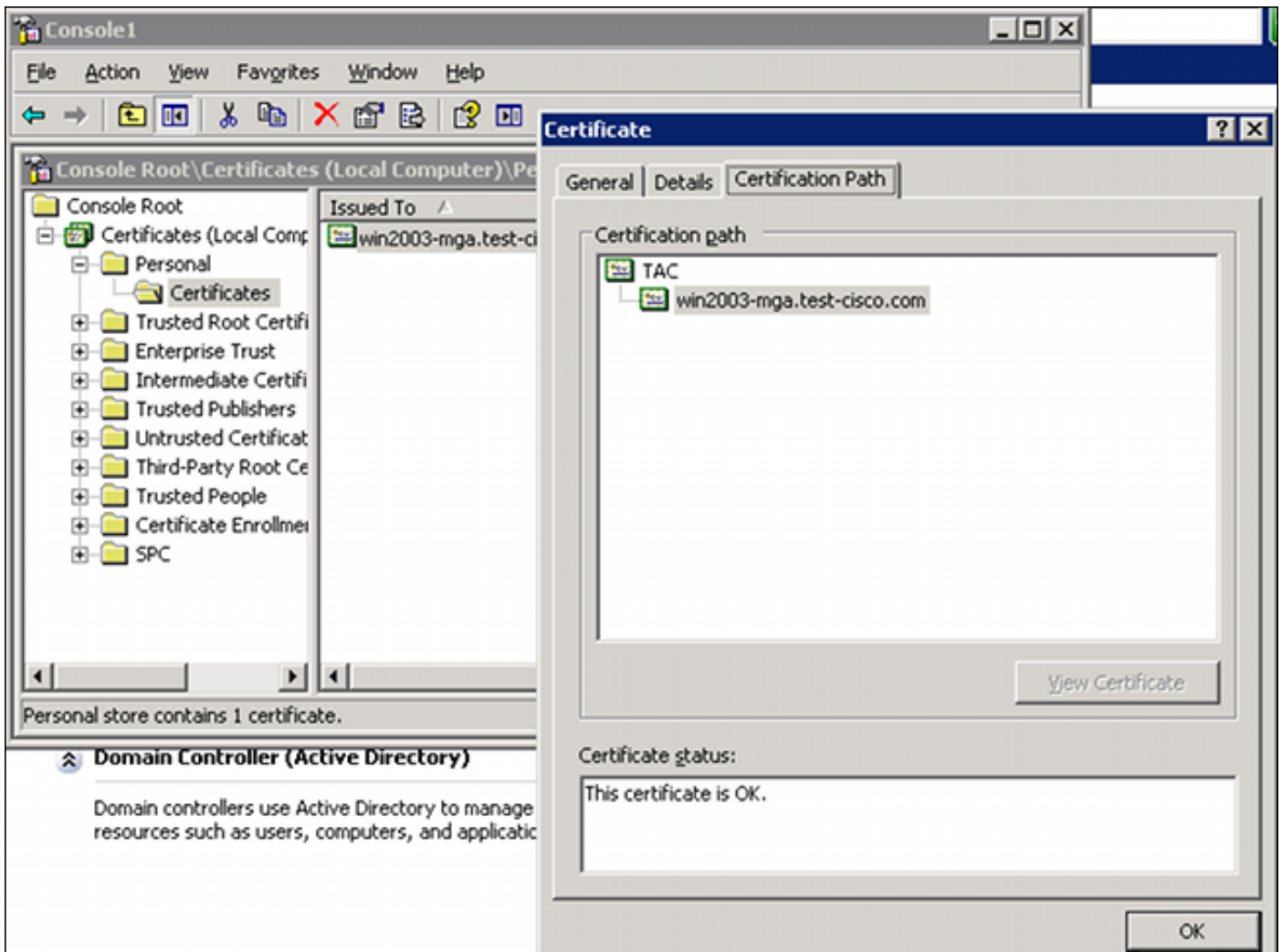
يمكن أن تكون الشهادة موقعة ذاتيا لأن ASA لا يتحقق من شهادة LDAP. راجع معرف تصحيح الأخطاء من Cisco [CSCui40212](#)، "السماح ASA بالتحقق من صحة الشهادة من خادم LDAP"، للحصول على طلب تحسين ذي صلة.

ملاحظة: يتحقق ACS من شهادة LDAP في الإصدار 5.5 والإصدارات اللاحقة.

لتثبيت الشهادة، افتح وحدة تحكم MMC، وحدد إضافة/إزالة الأداة الإضافية، وقم بإضافة الشهادة، واختر حساب الكمبيوتر:



حدد كمبيوتر محلي، وقم باستيراد الشهادة إلى المخزن الشخصي، ثم قم بنقل شهادة المرجع المصدق المقترن (CA) إلى المخزن الموثوق به. تحقق من أن الشهادة موثوق بها:



هناك خطأ في إصدار ASA 8.4.2، حيث قد يتم إرجاع هذا الخطأ عندما تحاول استخدام LDAP عبر SSL:

```
ASA(config)# debug ldap 255
```

```
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 [142]
[Base DN = [CN=Users,DC=test-cisco,DC=com
[Filter = [sAMAccountName=Administrator
[Scope = [SUBTREE
Request for Administrator returned code (-1) Can't contact LDAP server [142]
```

يعمل الإصدار 9.1.3 من ASA بشكل صحيح مع التكوين نفسه. هناك إثبات LDAP جلسة. ترجع الجلسة الأولى فشل مع الرمز 773 (كلمة منتهية الصلاحية)، بينما يتم استخدام الجلسة الثانية لتغيير كلمة المرور:

```
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 [53]
```

```

[Base DN = [CN=Users,DC=test-cisco,DC=com
[Filter = [sAMAccountName=cisco-test
[Scope = [SUBTREE
[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 [53]
DC=test-cisco,DC=com
Read bad password count 0 [53]
Change Password for cisco-test successfully converted old password to [53]
unicode
Change Password for cisco-test successfully converted new password to [53]
unicode
Password for cisco-test successfully changed [53]
:Retrieved User Attributes [53]

```

<most attributes details omitted for clarity...>

```

accountExpires: value = 130256568000000000 <----- 100ns intervals since
(January 1, 1601 (UTC

```

للتحقق من تغيير كلمة المرور، راجع الحزم. يمكن استخدام المفتاح الخاص لخادم LDAP من قبل Wireshark لفك تشفير حركة مرور SSL:

| Time | Source       | Destination  | Protocol | Length | Info   |
|------|--------------|--------------|----------|--------|--|
| 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]

```

تتمثل أخطاء تبادل مفتاح الإنترنت (IKE)/المصادقة والتفويض والمحاسبة (AAA) على ASA إلى حد كبير مع تلك المقدمة في سيناريو مصادقة RADIUS.

## LDAP والتنبيه قبل انتهاء الصلاحية

ل LDAP، أنت تستطيع استعملت سمة أن يرسل تحذير قبل كلمة مرور ينتهي. يقوم ASA بتحذير المستخدم قبل انتهاء صلاحية كلمة المرور ب 90 يوما باستخدام هذا الإعداد:

```

tunnel-group RA general-attributes
password-management password-expire-in-days 90
هنا تنتهي كلمة السر في 42 يوم، والمستعمل يحاول أن يدون:

```

```

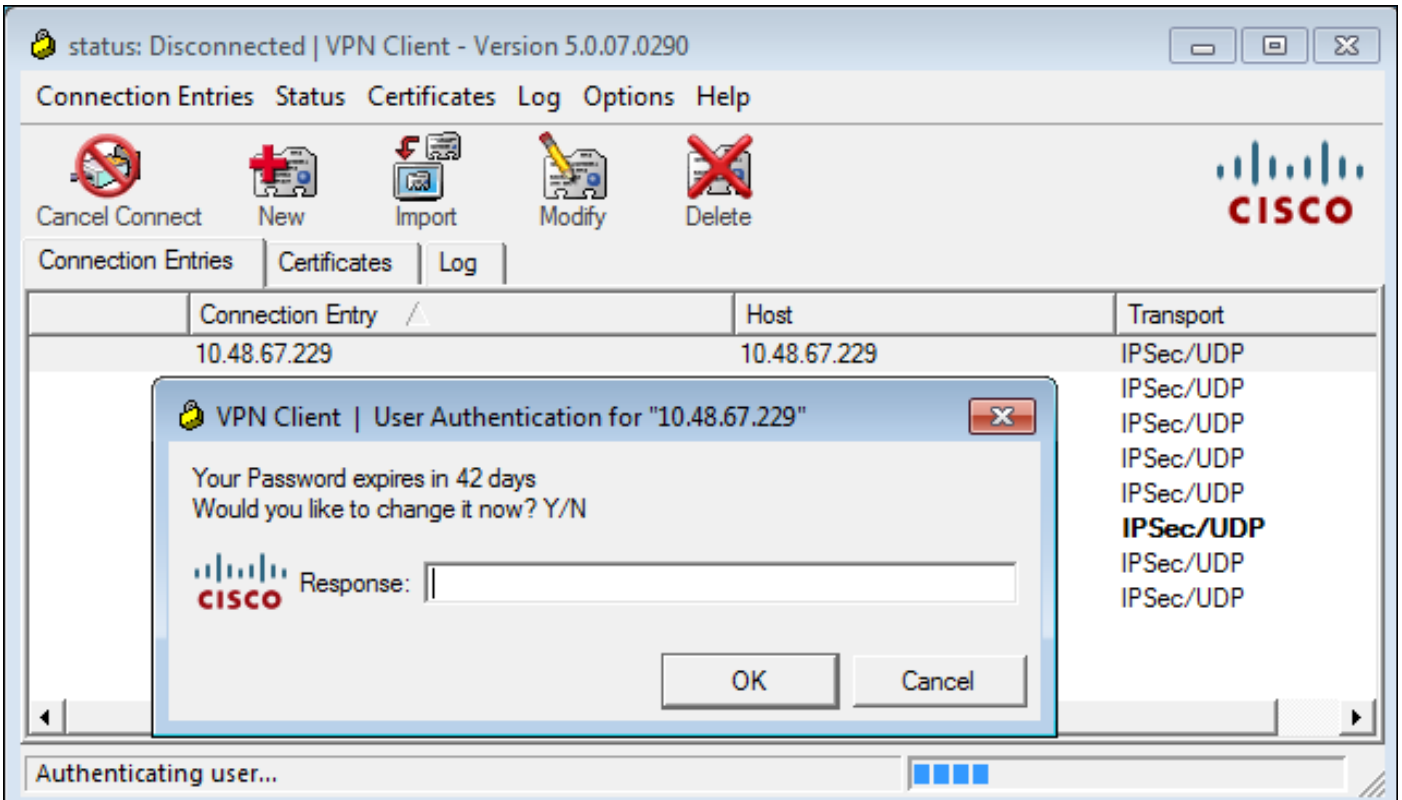
ASA# debug ldap 255
<some outputs removed for clarity>

```

```

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 [84]
GMT, delta=2072, maxage=1244139139 secs
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 [84]
يرسل ال ASA تحذير ويقدم الخيار ل كلمة تغيير:

```



إن يختار المستعمل أن يغير الكلمة، هناك رسالة حث لكلمة جديد، ويبدأ الإجراء عادي كلمة تغيير.

## L2TP و ASA

قدمت الأمثلة السابقة الإصدار 1 من IKE (IKEv1) وشبكة VPN من IPSec.

بالنسبة لبروتوكول الاتصال النفقي للطبقة 2 (L2TP) و IPSec، يتم استخدام PPP كنقل للمصادقة. يلزم وجود MSCHAPv2 بدلا من PAP حتى يعمل تغيير كلمة المرور:

```

ciscoasa(config-tunnel-general)# tunnel-group DefaultRAGroup ppp-attributes
ciscoasa(config-ppp)# authentication ms-chap-v2
لمصادقة الموسعة في L2TP داخل جلسة PPP، يتم التفاوض حول MSCHAPv2:

```

```

> 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

```

عند انتهاء صلاحية كلمة مرور المستخدم، يتم إرجاع فشل بالرمز 648:

```

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

```

ثم يلزم تغيير كلمة المرور. أما بقية العملية فهي مماثلة جدا لسيناريو RADIUS باستخدام MSCHAPv2.

راجع [L2TP عبر IPsec بين Windows 2000/XP PC و PIX/ASA 7.2 باستخدام مثال تكوين مفتاح مشترك مسبقا](#) للحصول على تفاصيل إضافية حول كيفية تكوين L2TP.

## عمل ASA SSL VPN

أشارت الأمثلة السابقة إلى IKEv1 وعمل Cisco VPN، وهو نهاية العمر (EOL).

الحل الموصى به لشبكة VPN للوصول عن بعد هو Cisco AnyConnect Secure Mobility، والذي يستخدم الإصدار 2 من IKE (IKEv2) وبروتوكولات SSL. تعمل ميزات تغيير كلمة المرور وانتهاء الصلاحية بنفس الطريقة تماما ل Cisco AnyConnect كما فعلت لعمل Cisco VPN.

بالنسبة ل IKEv1، تم تبادل بيانات تغيير كلمة المرور وانتهاء الصلاحية بين ASA وعمل VPN في المرحلة 1.5 (Xauth/mode config).

بالنسبة ل IKEv2، هو مماثل؛ يستخدم وضع config حزم CFG\_REQUEST/CFG\_REPLY.

بالنسبة ل SSL، تكون البيانات في جلسة عمل "أمان طبقة النقل في مخطط بيانات التحكم" (DTLS).

التشكيل هو نفسه ل ال ASA.

هذا مثال على التكوين باستخدام بروتوكول Cisco AnyConnect و SSL باستخدام خادم LDAP عبر 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

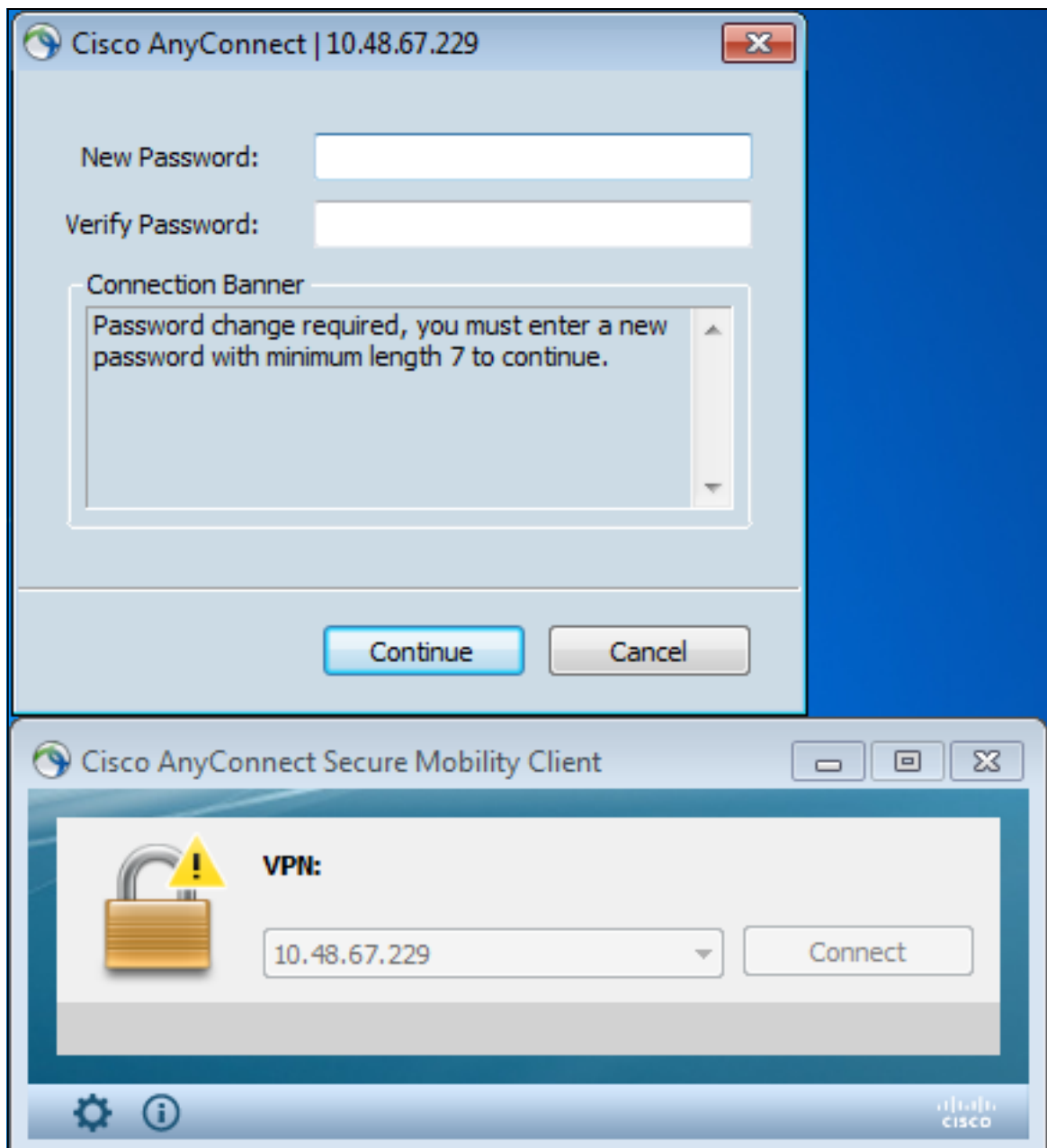
                                webvpn
                                enable outside
anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
                                anyconnect enable
                                tunnel-group-list enable

                                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

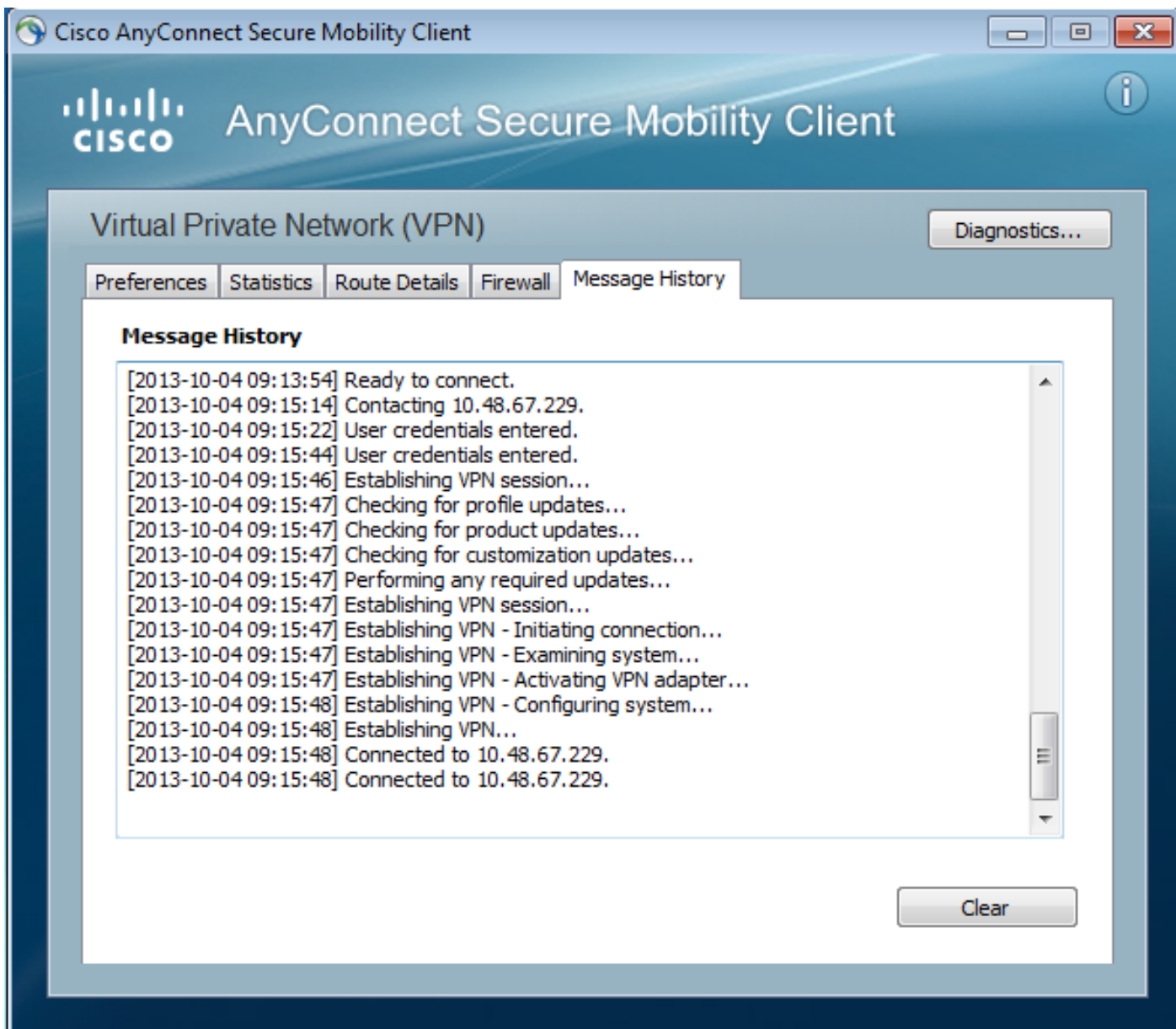
ip local pool POOL 192.168.11.100-192.168.11.105 mask 255.255.255.0
```

بمجرد توفير كلمة المرور الصحيحة (التي انتهت صلاحيتها)، يحاول Cisco AnyConnect الاتصال ويطلب كلمة مرور جديدة:



تشير السجلات إلى إدخال بيانات اعتماد المستخدم مرتين:

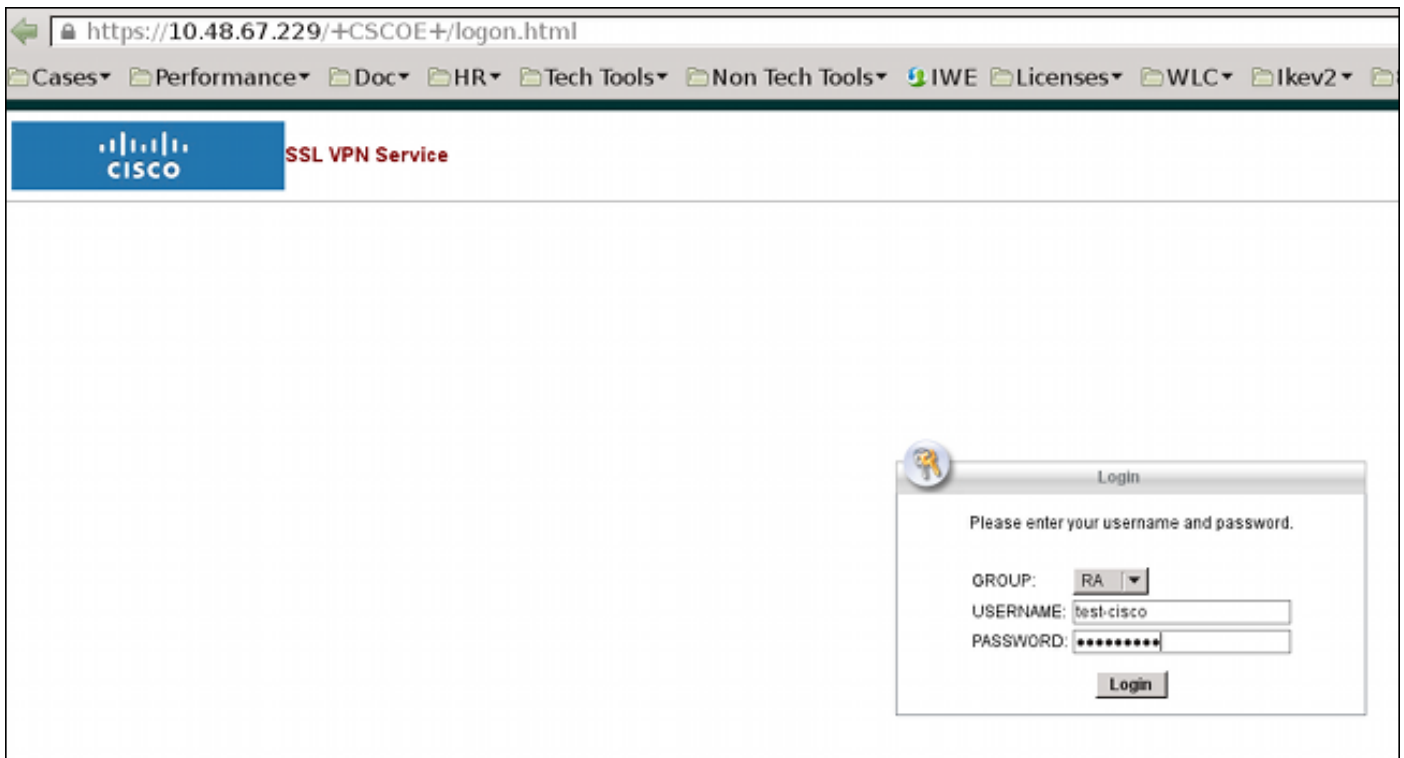




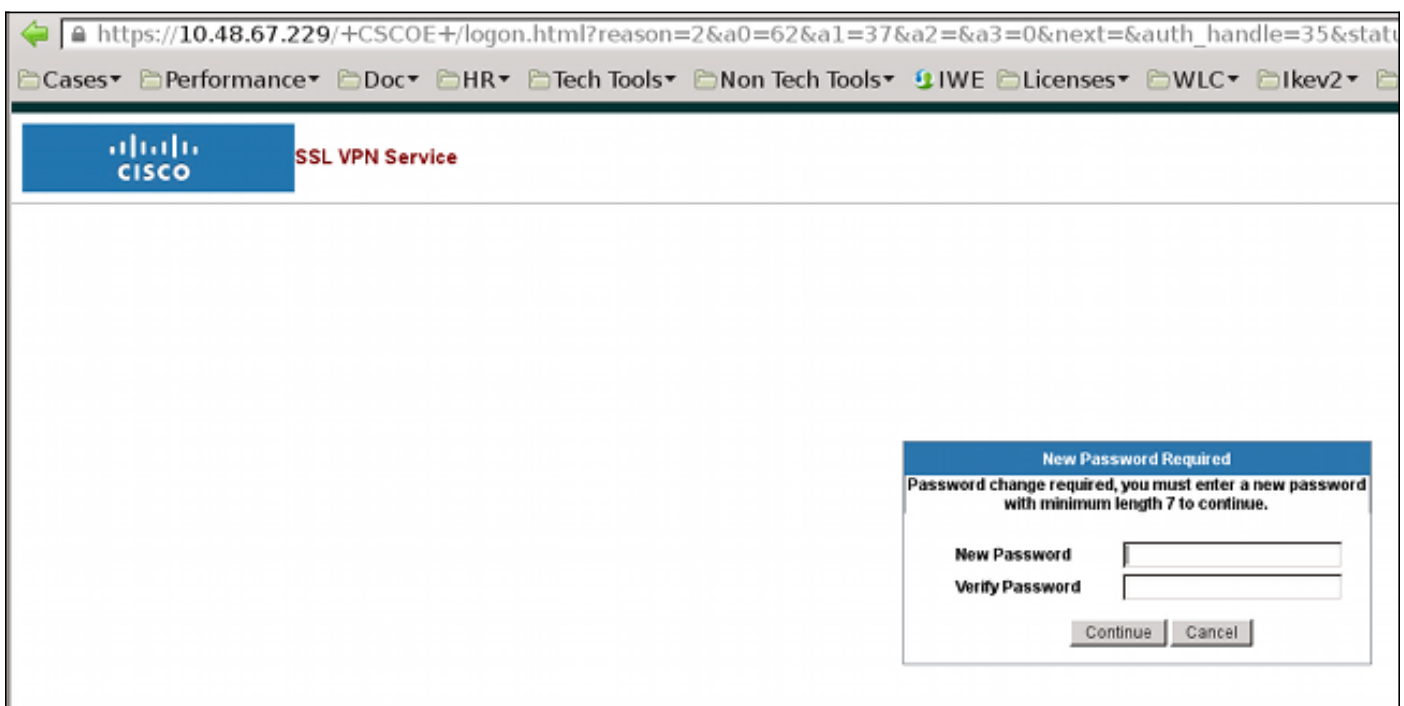
تتوفر سجلات أكثر تفصيلا في أداة تقارير AnyConnect التشخيصية (DART).

## بوابة الويب ASA SSL

تحدث نفس عملية تسجيل الدخول في بوابة الويب:



تحديث نفس عملية انتهاء صلاحية كلمة المرور والتغيير:



## كلمة مرور تغيير المستخدم ل ACS

إن لا يمكن أن يغير الكلمة على ال VPN، أنت تستطيع استعملت ال ACS مستعمل يغير كلمة (UCP) كرسن موقع خدمة. انظر دليل مطور البرامج لنظام التحكم بالوصول الآمن من Cisco 5.4: استخدام خدمات ويب UCP.

## التحقق من الصحة

لا يوجد حالياً إجراء للتحقق من صحة هذا التكوين.

# استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

## معلومات ذات صلة

- [دليل تكوين سلسلة Cisco ASA 5500 باستخدام 8.4، CLI، و 8.6: تكوين خادم خارجي لتفويض مستخدم جهاز الأمان](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومجم مادختساب دن تسمل اذ Cisco تچرت  
ملاعلاء انءم ةم ةم ةم ةم ةم ةم ةم ةم ةم ةم ةم ةم ةم ةم ةم ةم  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال م ةم ةم ةم ةم  
Cisco ةلخت . فرتجم مچرت م ةم ةم ةم ةم ةم ةم ةم ةم ةم ةم  
ىل إأمءاد ةوچرلاب ةصؤت و تامچرتل هذه ةقءن ةم ةم ةم ةم  
(رفوتم طبارل) ةلصلأل ةم ةم ةم ةم ةم ةم ةم ةم ةم ةم ةم ةم