

ASA 8.x: AnyConnect SSL VPN CAC- Smart Cards MAC معداد عم

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [تكوين ASA من Cisco](#)
- [اعتبارات النشر](#)
- [تكوين المصادقة والتفويض والمحاسبة \(AAA\)](#)
- [تكوين خادم LDAP](#)
- [إدارة الشهادات](#)
- [إنشاء المفاتيح](#)
- [تثبيت شهادات المرجع المصدق الجذر](#)
- [تسجيل ASA وتثبيت شهادة الهوية](#)
- [تكوين AnyConnect VPN](#)
- [إنشاء تجمع عناوين IP](#)
- [إنشاء مجموعة النفق ونهج المجموعة](#)
- [واجهة مجموعة النفق وإعدادات الصورة](#)
- [قواعد مطابقة الشهادة \(إذا كان سيتم استخدام OCSP\)](#)
- [تكوين OCSP](#)
- [تكوين شهادة المستحب OCSP](#)
- [تكوين CA لاستخدام OCSP](#)
- [تكوين قواعد OCSP](#)
- [تكوين عمل AnyConnect من Cisco](#)
- [تنزيل Cisco AnyConnect VPN Client - Mac OS X](#)
- [بدء تشغيل AnyConnect VPN Client من Cisco - نظام التشغيل Mac OS X](#)
- [اتصال جديد](#)
- [بدء الوصول عن بعد](#)
- [الملحق أ - تخطيط LDAP و DAP](#)
- [السيناريو 1: تطبيق Active Directory باستخدام الطلب الهاتفي لأذن الوصول عن بعد - السماح بالوصول/رفضه](#)
- [إعداد Active Directory](#)
- [تكوين ASA](#)
- [السيناريو 2: تطبيق Active Directory باستخدام عضوية المجموعة للسماح بالوصول أو رفضه](#)
- [إعداد Active Directory](#)
- [تكوين ASA](#)
- [السيناريو 3: سياسات الوصول الديناميكي للعديد من سمات الأعضاء](#)
- [تكوين ASA](#)

[الملحق ب - تكوين ASA CLI](#)
[الملحق ج- أكتشاف الأخطاء وإصلاحها](#)
[أكتشاف أخطاء AAA و LDAP وإصلاحها](#)
[المثال 1: الاتصال المسموح به مع تعيين السمة الصحيحة](#)
[المثال 2: الاتصال المسموح به بتعيين سمة Cisco التي تم تكوينها بشكل غير منتظم](#)
[أكتشاف أخطاء DAP وإصلاحها](#)
[مثال 1: الاتصال المسموح به مع DAP](#)
[المثال 2: رفض الاتصال ب DAP](#)
[هبة شهادة أكتشاف الأخطاء وإصلاحها / OCSP](#)
[الملحق د - التحقق من كائنات LDAP في MS](#)
[عارض LDAP](#)
[محرر واجهة خدمات Active Directory](#)
[الملحق ه](#)
[معلومات ذات صلة](#)

[المقدمة](#)

يقدم هذا المستند نموذجاً لتكوين على جهاز الأمان القابل للتكيف (ASA) من Cisco للوصول عن بعد إلى AnyConnect VPN لدعم MAC باستخدام بطاقة الوصول المشترك (CAC) للمصادقة.

يغطي هذا المستند تكوين Cisco ASA باستخدام مدير أجهزة الأمان القابل للتكيف (ASDM) و Cisco AnyConnect VPN Client و (AD و Microsoft Active Directory) /بروتوكول الوصول إلى الدليل خفيف الوزن (LDAP).

يستخدم التكوين الموجود في هذا الدليل خادم Microsoft AD/LDAP. يغطي هذا المستند أيضاً الميزات المتقدمة مثل OCSP وخرائط سمات LDAP وسياسات الوصول الديناميكي (DAP).

[المتطلبات الأساسية](#)

[المتطلبات](#)

يكون الفهم الأساسي ل Cisco ASA و Cisco AnyConnect Client و Microsoft AD/LDAP وبنية المفاتيح العام (PKI) مفيداً في فهم الإعداد الكامل. تساعد الإلمام بعضوية مجموعة AD وخصائص المستخدم وكذلك كائنات LDAP في ربط عملية التحويل بين سمات الشهادة وكائنات AD/LDAP.

[المكونات المستخدمة](#)

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

- جهاز الأمان القابل للتكيف (ASA) من Cisco 5500 Series الذي يشغل الإصدار 8.0(x) من البرنامج والإصدارات الأحدث
 - Cisco Adaptive Security Device Manager (ASDM)، الإصدار x.6 ل ASA 8.x
 - Cisco AnyConnect VPN Client 2.2 مع دعم MAC
- 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.

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

تكوين ASA من Cisco

يغطي هذا القسم تكوين Cisco ASA عبر ASDM. وهو يغطي الخطوات الضرورية لنشر نفق وصول عن بعد لشبكة VPN من خلال اتصال SSL AnyConnect. يتم استخدام شهادة CAC للمصادقة، كما يتم ملء السمة User (Principal Name) (UPN) في الشهادة في Active Directory للتحويل.

اعتبارات النشر

- لا يغطي هذا الدليل التكوينات الأساسية مثل الواجهات و DNS و NTP والتوجيه والوصول إلى الجهاز والوصول إلى ASDM وما إلى ذلك. من المفترض أن مشغل الشبكة على دراية بهذه التكوينات. راجع [أجهزة الأمان متعددة الوظائف](#) للحصول على مزيد من المعلومات.
- والأقسام المبرزة في RED هي تكوينات إلزامية مطلوبة للوصول الأساسي إلى الشبكة الخاصة الظاهرية (VPN). على سبيل المثال، يمكن إعداد نفق VPN باستخدام بطاقة CAC دون إجراء فحوصات OCSP وتخطيطات LDAP وفحوصات سياسة الوصول الديناميكي (DAP). يقوم DoD بتفويض فحص OCSP ولكن يعمل النفق بدون تكوين OCSP.
- الأقسام المبرزة بالأزرق هي ميزات متقدمة يمكن تضمينها لإضافة المزيد من التأمين للتصميم.
- لا يمكن أن يستخدم ASDM و AnyConnect/SSL VPN المنافذ نفسها على الواجهة نفسها. يوصى بتغيير المنافذ على أحدها أو الآخر للحصول على حق الوصول. على سبيل المثال، استخدم المنافذ 445 ل ASDM وترك 443 ل AC/SSL VPN. تم تغيير الوصول إلى URL ل ASDM في x.8. استخدم `https://<ip_address>:<port>/admin.html`.
- صورة ASA المطلوبة هي 8.0.2.19 و 6.0.2 ASDM على الأقل.
- AnyConnect/CAC مدعوم مع Vista.
- راجع [الملحق \(أ\)](#) للحصول على أمثلة لرسم خرائط سياسة الوصول الديناميكي و LDAP لتنفيذ السياسات الإضافية.
- راجع [الملحق \(د\)](#) حول كيفية التحقق من كائنات LDAP في MS.
- راجع المعلومات ذات الصلة للحصول على قائمة بمنافذ التطبيق لتكوين جدار الحماية.

تكوين المصادقة والتفويض والمحاسبة (AAA)

تتم مصادقتك باستخدام الشهادة الموجودة في بطاقة الوصول المشترك (CAC) من خلال خادم مرجع مصدق البيانات (CA) أو خادم CA الخاص بمنظمتهم. يجب أن تكون الشهادة صالحة للوصول عن بعد إلى الشبكة. بالإضافة إلى المصادقة، يجب أن تكون مخولاً أيضاً لاستخدام كائن Microsoft Active Directory أو Lightweight Directory Access Protocol (LDAP). تتطلب وزارة الدفاع استخدام سمة اسم المستخدم الأساسي (UPN) للتحويل، والتي تعد جزءاً من قسم "الاسم البديل للموضوع (SAN)" في الشهادة. يجب أن يكون UPN أو EDI/PI بهذا التنسيق، 1234567890@mil. تظهر هذه التكوينات كيفية تكوين خادم AAA في ASA باستخدام خادم LDAP للتحويل. راجع [الملحق \(أ\)](#) للحصول على تكوين إضافي باستخدام تعيين كائن LDAP.

تكوين خادم LDAP

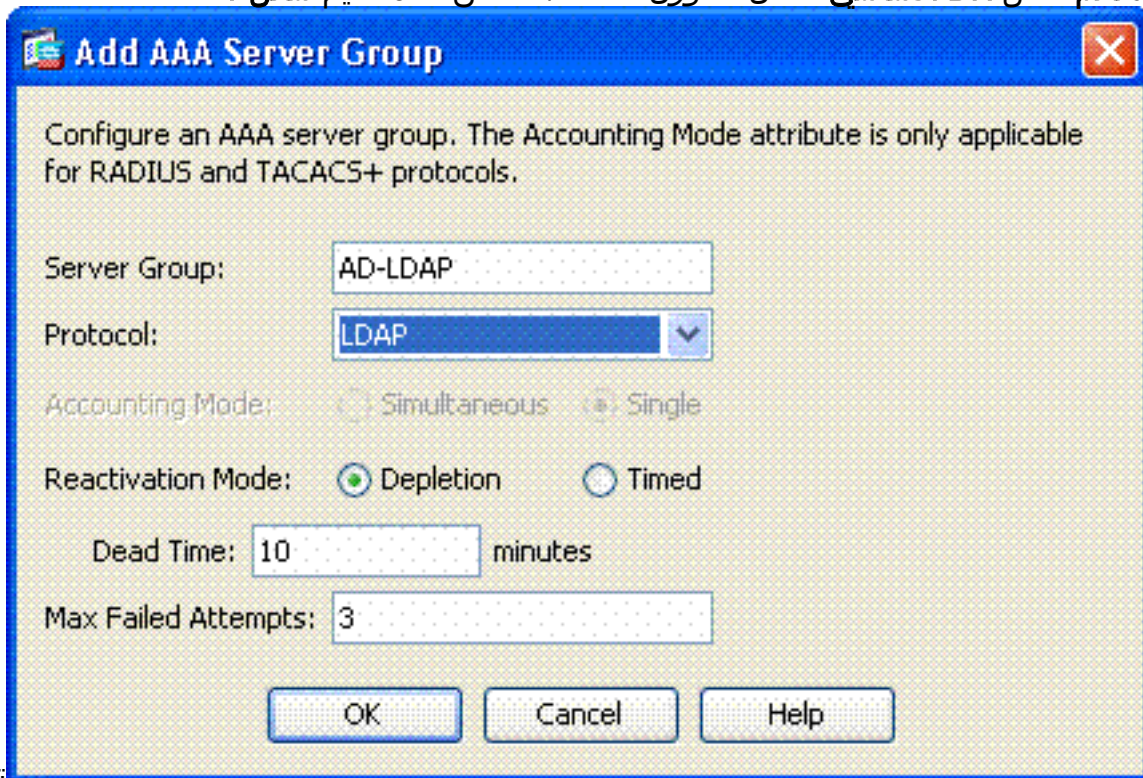
أكمل الخطوات التالية:

1. اختر Remote Access VPN (الوصول عن بعد) < إعداد AAA < مجموعة خوادم AAA.
2. في جدول مجموعات خوادم AAA، انقر فوق إضافة 3.

3. دخلت نادل مجموعة إسم واخترت LDAP في البروتوكول لاسلكي زر. راجع الشكل 1.

4. في الخوادم الموجودة في جدول المجموعة المحدد، انقر فوق إضافة. تأكد من أن الخادم الذي أنشأته مبرز في الجدول السابق.

5. في نافذة تحرير خادم AAA، أكمل الخطوات التالية. راجع الشكل 2. ملاحظة: أختار خيار تمكين LDAP عبر SSL في حالة تكوين LDAP/AD لهذا النوع من الاتصال. أخترت القارئ حيث ال LDAP يكون موقع. يظهر هذا الدليل داخل الواجهة. أدخل عنوان IP الخاص بالخادم. أدخل منفذ الخادم. التقصير LDAP ميناء 389. أختار نوع الخادم. أدخل DN الأساسي. اسأل مسؤول AD/LDAP عن هذه القيم. شكل-1



تحت خيار النطاق، أختار الإجابة المناسبة. يعتمد ذلك على DN الأساسي. اطلب المساعدة من مسؤول AD/LDAP. في سمة التسمية، أدخل userPrincipalName. هذه هي السمة المستخدمة لتحويل المستخدم في خادم AD/LDAP. دخلت في ال login DN، المسؤول DN. ملاحظة: لديك حقوق أو حقوق إدارية لعرض/البحث في بنية LDAP التي تتضمن كائنات المستخدم وعضوية المجموعة. في كلمة مرور تسجيل الدخول، أدخل كلمة مرور المسؤول. أترك سمة LDAP إلى بلا. شكل-2

Add AAA Server

Server Group: AD-LDAP

Interface Name: outside

Server Name or IP Address: 172.18.120.160

Timeout: 10 seconds

LDAP Parameters

Enable LDAP over SSL

Server Port: 389

Server Type: -- Detect Automatically/Use Generic Type --

Base DN: CN=Users,DC=gsgseclab,DC=org

Scope: One level beneath the Base DN

Naming Attribute(s): userPrincipalName

Login DN: lministrator,CN=Users,DC=gsgseclab,DC=org

Login Password: ●●●●●●●●

LDAP Attribute Map: -- None --

SASL MD5 authentication

SASL Kerberos authentication

Kerberos Server Group: _____

OK Cancel Help

ملاحظة:

يمكنك استخدام هذا الخيار لاحقاً في التكوين لإضافة كائن AD/LDAP آخر للتحويل. أختَر OK.
6. أختَر OK.

إدارة الشهادات

هناك إثنان steps in order to ركب شهادة على ال ASA. أولاً، قم بتثبيت شهادات المرجع المصدق (المرجع المصدق الأساسي والثانوي) المطلوبة. ثانياً، تسجيل مكتب المساعدة القانونية في مرجع مصدق محدد والحصول على شهادة الهوية. تستخدم وحدة PKI من DoD هذه الشهادات وشهادة ASA ID وشهادة OCSP ذات الجذر CA2 والفئة 3 و #CA متوسطة التي تم تسجيلها بها وشهادة ASA ID وشهادة OCSP. ولكن، إذا أختَر عدم استخدام OCSP، فلا يلزم تثبيت شهادة OCSP.

ملاحظة: اتصل ب POC للأمان للحصول على الشهادات الجذر بالإضافة إلى التعليمات حول كيفية التسجيل لشهادة الهوية للجهاز. يجب أن تكون شهادة SSL كافية ل ASA للوصول عن بعد. لا يلزم استخدام شهادة شبكة منطقة تخزين (SAN) مزدوجة.

ملاحظة: يجب أيضاً تثبيت سلسلة DoD CA على الجهاز المحلي. يمكن عرض الشهادات في "مخزن شهادات

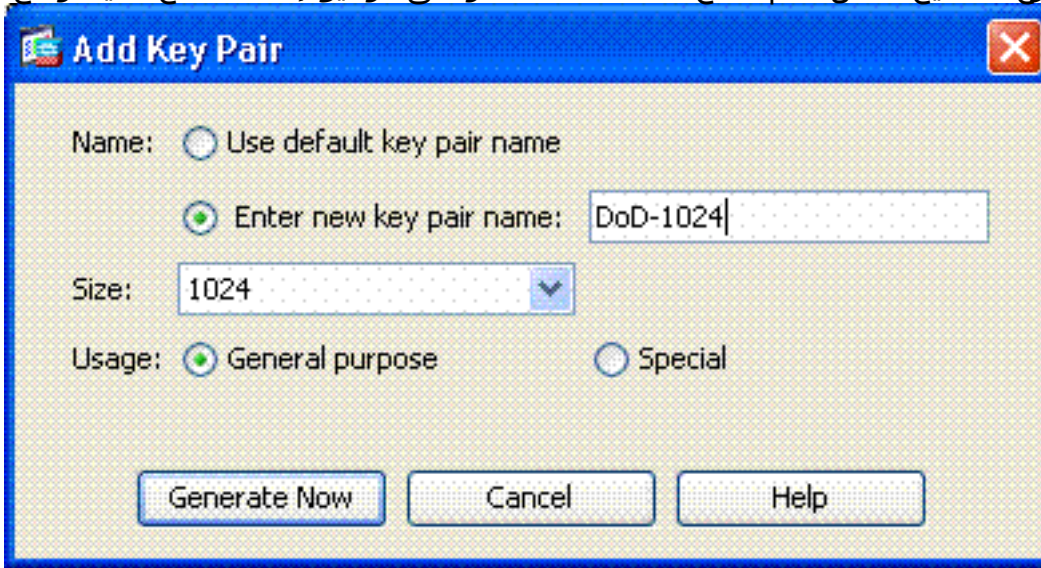
Microsoft "Internet Explorer باستخدام DoD ملف دفعة يقوم تلقائيا بإضافة كافة CAs إلى الجهاز. اطلب
PKI POC الخاص بك للحصول على مزيد من المعلومات.

ملاحظة: يجب أن يكون جذر DoD CA2 والفئة 3 وكذلك معرف ASA ومعرف CA الوسيط الذي أصدر شهادة ASA هو المرجع المصدق الوحيد المطلوب لمصادقة المستخدم. تتضمن جميع الواسطات CA الحالية تحت سلسلة جذر CA2 والفئة 3 ويتم الوثوق بها طالما تمت إضافة جذور CA2 والفئة 3.

إنشاء المفاتيح

أكمل الخطوات التالية:

1. أختَر Remote Access VPN (الوصول عن بعد) < إدارة الشهادات < شهادة الهوية < إضافة.
2. أختَر إضافة شهادة معرف جديدة ثم جديد بواسطة خيار زوج المفاتيح.
3. في نافذة إضافة زوج المفاتيح، أدخل اسم مفتاح، DoD-1024. انقر على الراديو لإضافة مفتاح جديد. راجع



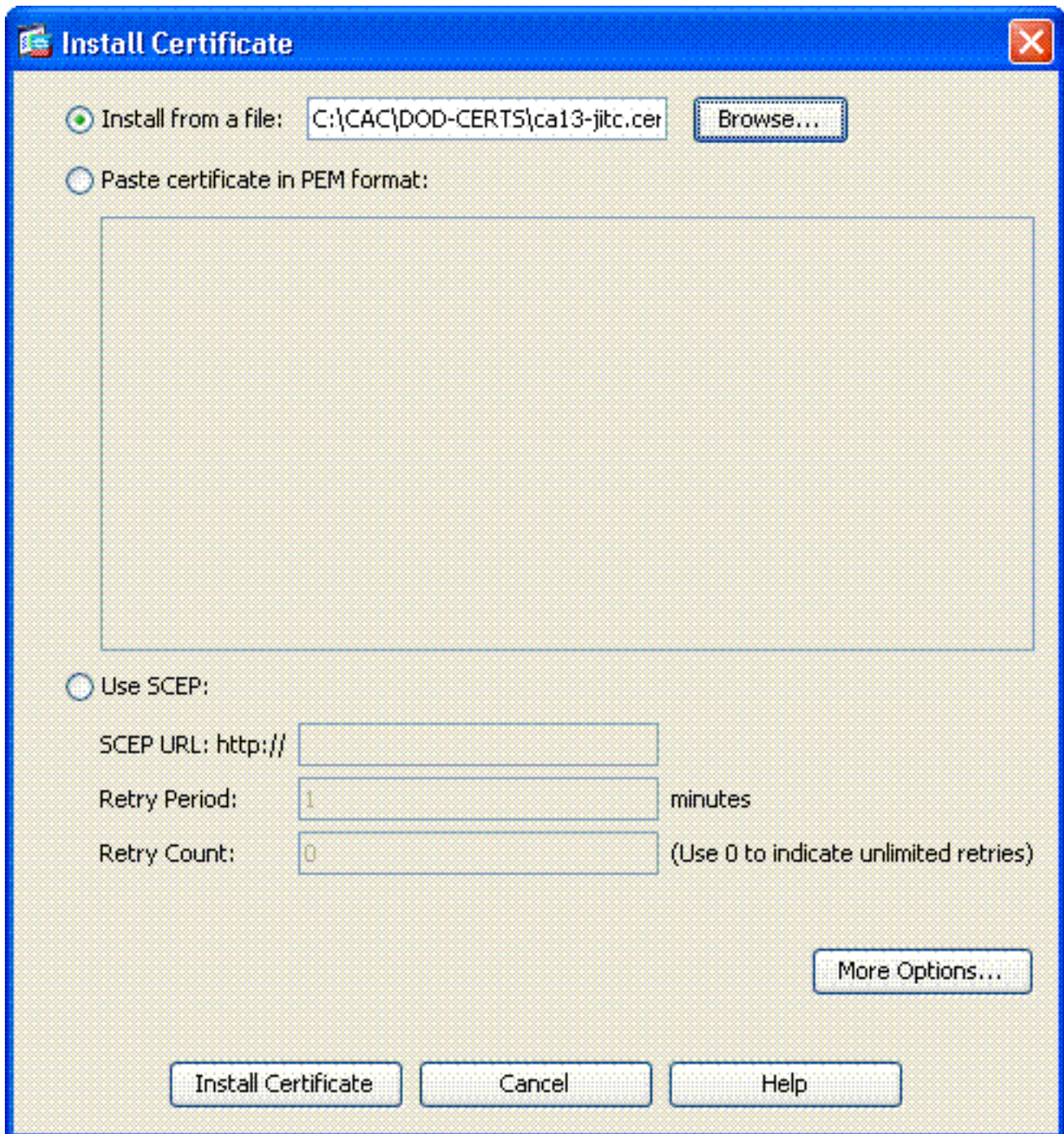
الشكل 3. الشكل 3

4. أختَر حجم المفتاح.
5. الاحتفاظ بالاستخدام للأغراض العامة.
6. انقر فوق إنشاء الآن. ملاحظة: يستخدم المرجع المصدق (CA) الجذري لـ DoD مفتاح إصدار 2048 بت. يجب إنشاء مفتاح ثانٍ يستخدم زوج مفاتيح 2048 بت ليكون قادراً على استخدام المرجع المصدق هذا. أتمت الـ steps in order to أضفت مفتاح ثاني.

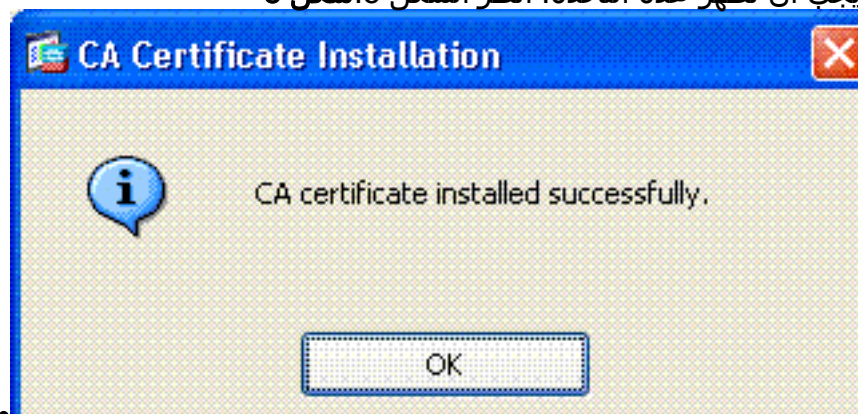
تثبيت شهادات المرجع المصدق الجذر

أكمل الخطوات التالية:

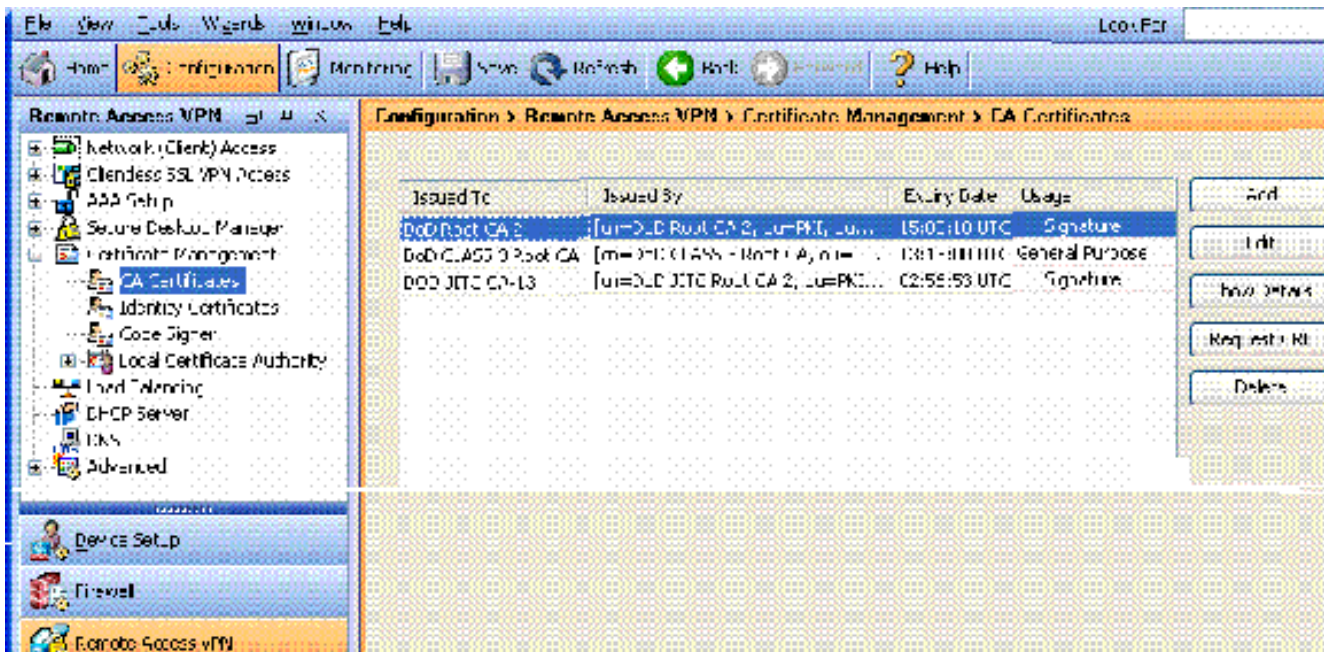
1. أختَر Remote Access VPN (الوصول عن بعد) < إدارة الشهادات < شهادة CA < إضافة.
2. أختَر تثبيت من ملف واستعرض إلى الشهادة.
3. أختَر شهادة التثبيت. الشكل 4: تثبيت الشهادة الجذر



4. يجب أن تظهر هذه النافذة. انظر الشكل 5. شكل 5

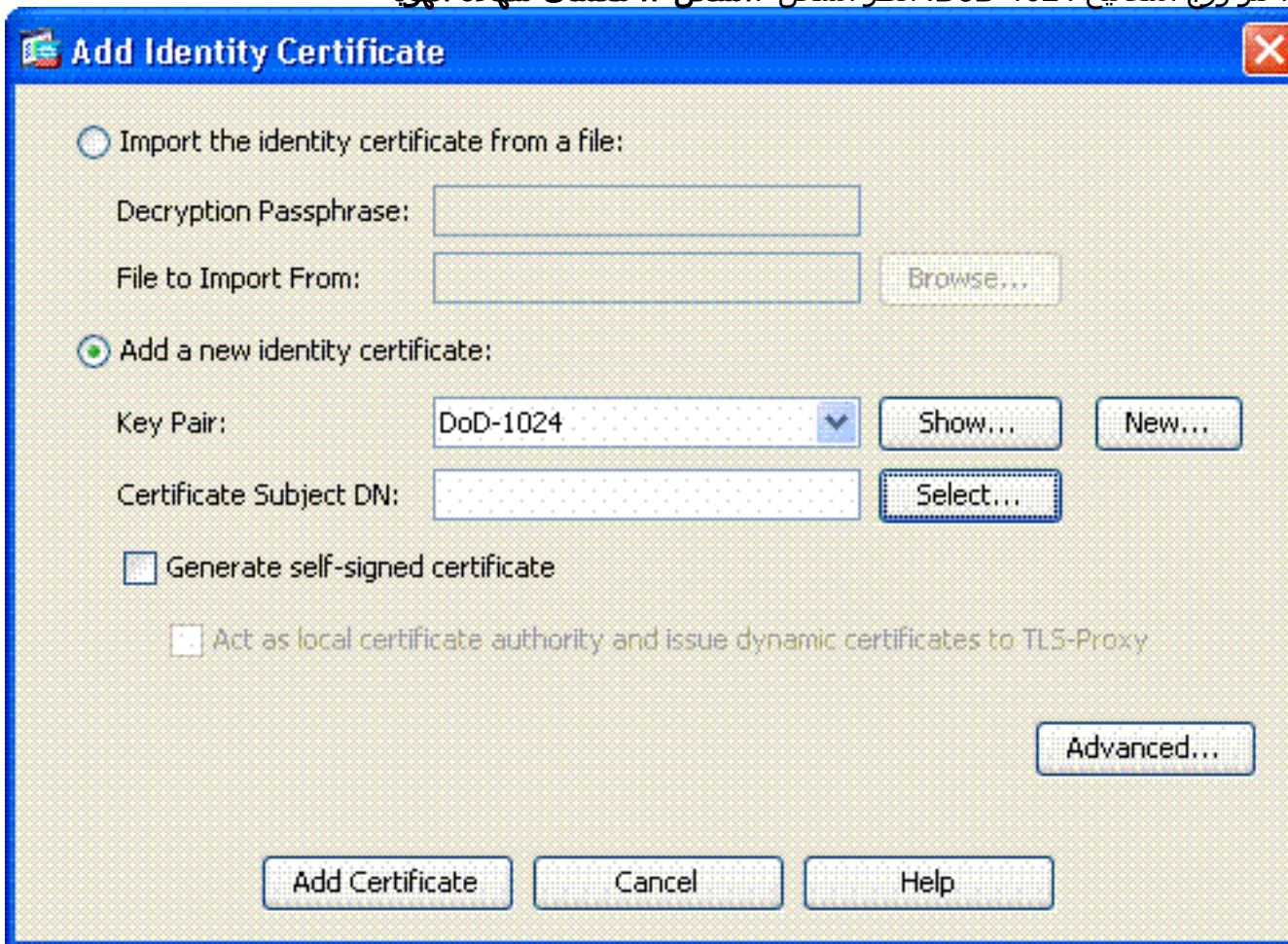


ملاحظة: كرر الخطوات من 1 إلى 3 لكل شهادة تريد تثبيتها. يتطلب DoD PKI شهادة لكل مما يلي: جذر 2 CA، جذر الفئة 3، CA # متوسط، معرف ASA وخادم OCSP. لا تكون شهادة OCSP مطلوبة إذا لم تستخدم OCSP. الشكل 6: تثبيت الشهادة الجذر

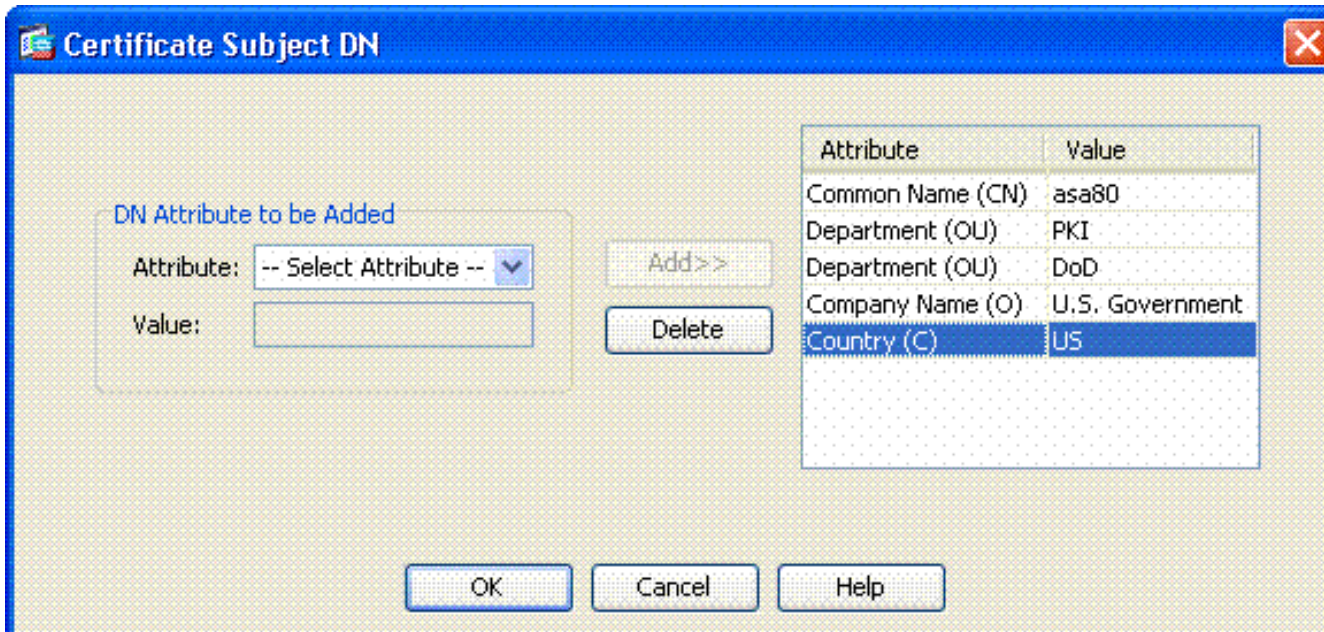


تسجيل ASA وثبت شهادة الهوية

1. أختَر Remote Access VPN (الوصول عن بعد) < إدارة الشهادات < شهادة الهوية < إضافة.
2. أختَر إضافة شهادة معرف جديدة.
3. أختَر زوج المفاتيح DoD-1024. انظر الشكل 7 الشكل 7: معلمات شهادة الهوية



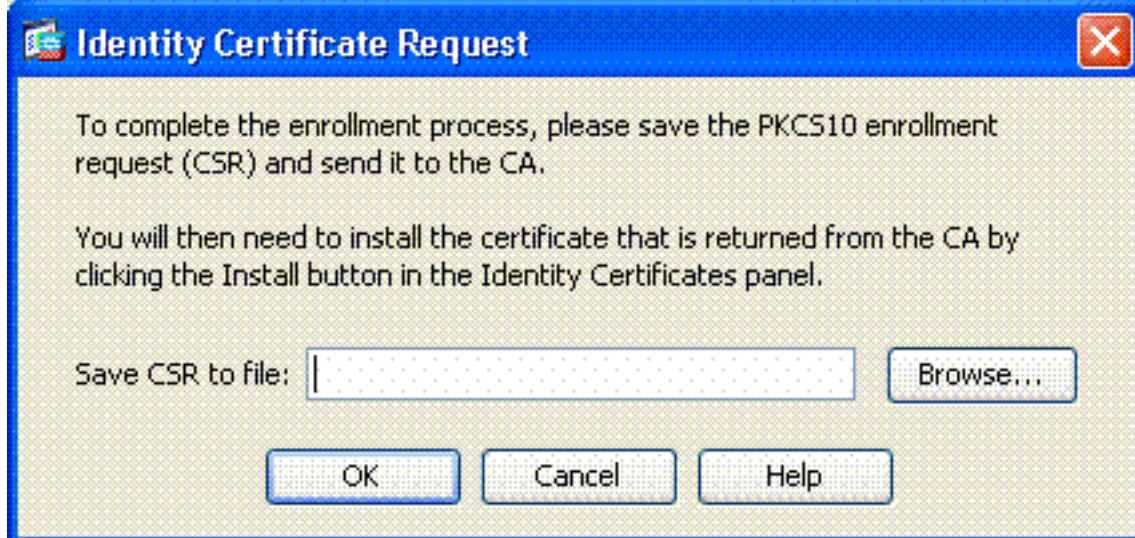
4. انتقل إلى مربع DN لموضوع الشهادة وانقر فوق تحديد.
5. في نافذة DN موضوع الشهادة، أدخل معلومات الجهاز. راجع الشكل 8 على سبيل المثال. شكل 8: تحرير DN



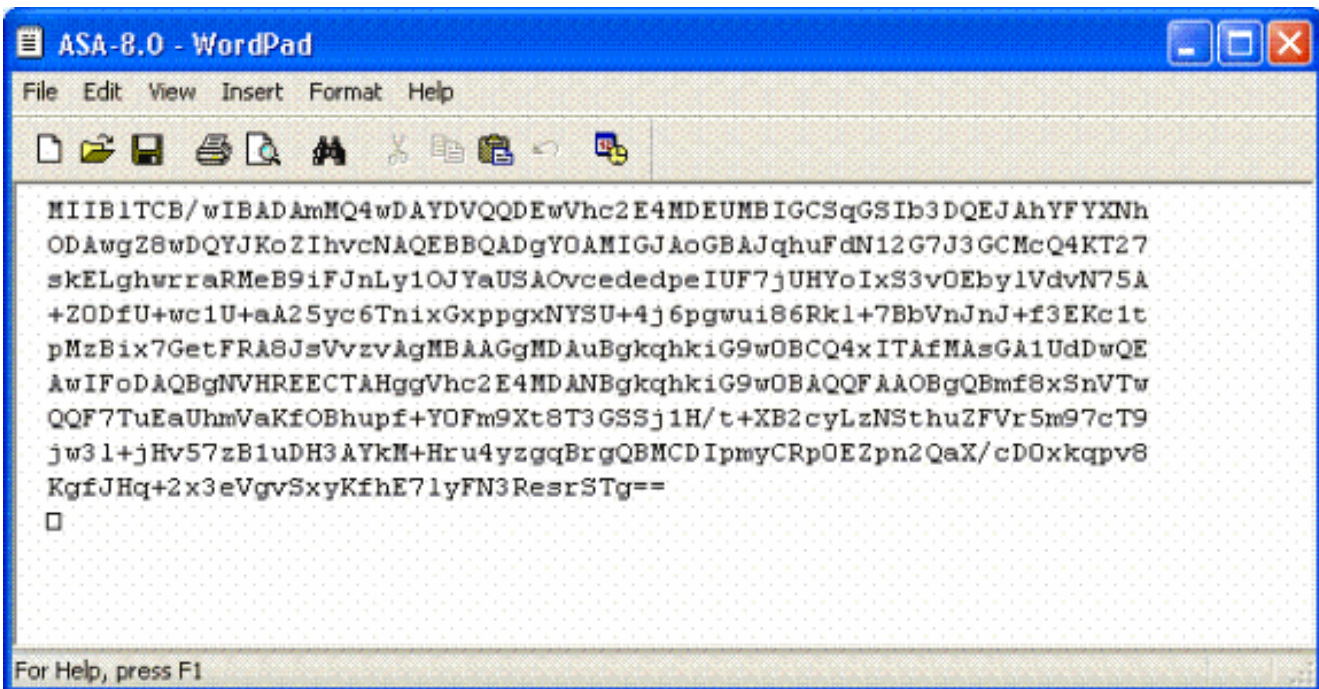
6. أختَر OK. ملاحظة: تأكد من استخدام اسم المضيف للجهاز الذي تم تكوينه في نظامك عند إضافة اسم المضيف DN للموضوع. يمكن أن يخبرك PKI POC بالحقول الإلزامية المطلوبة.

7. أختَر إضافة شهادة.

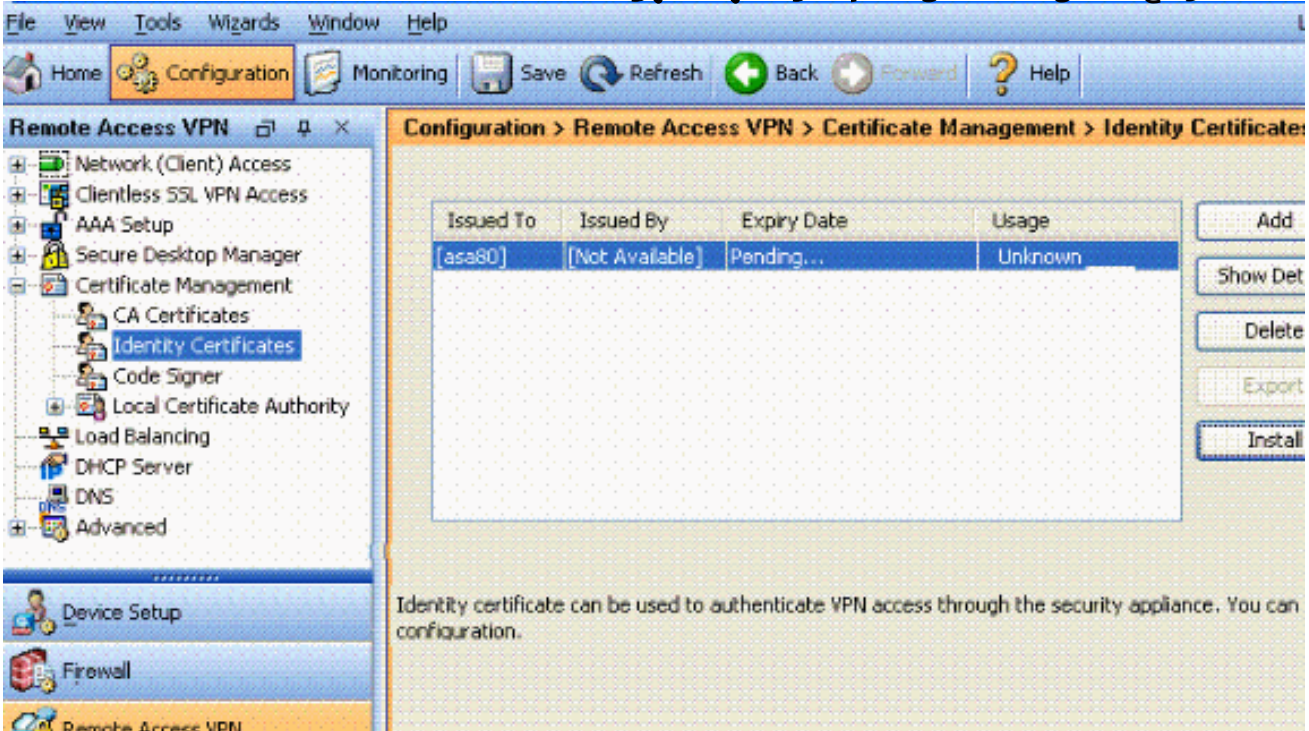
8. انقر فوق إستعراض لتحديد الدليل الذي تريد حفظ الطلب فيه. راجع الشكل 9. شكل 9 طلب شهادة



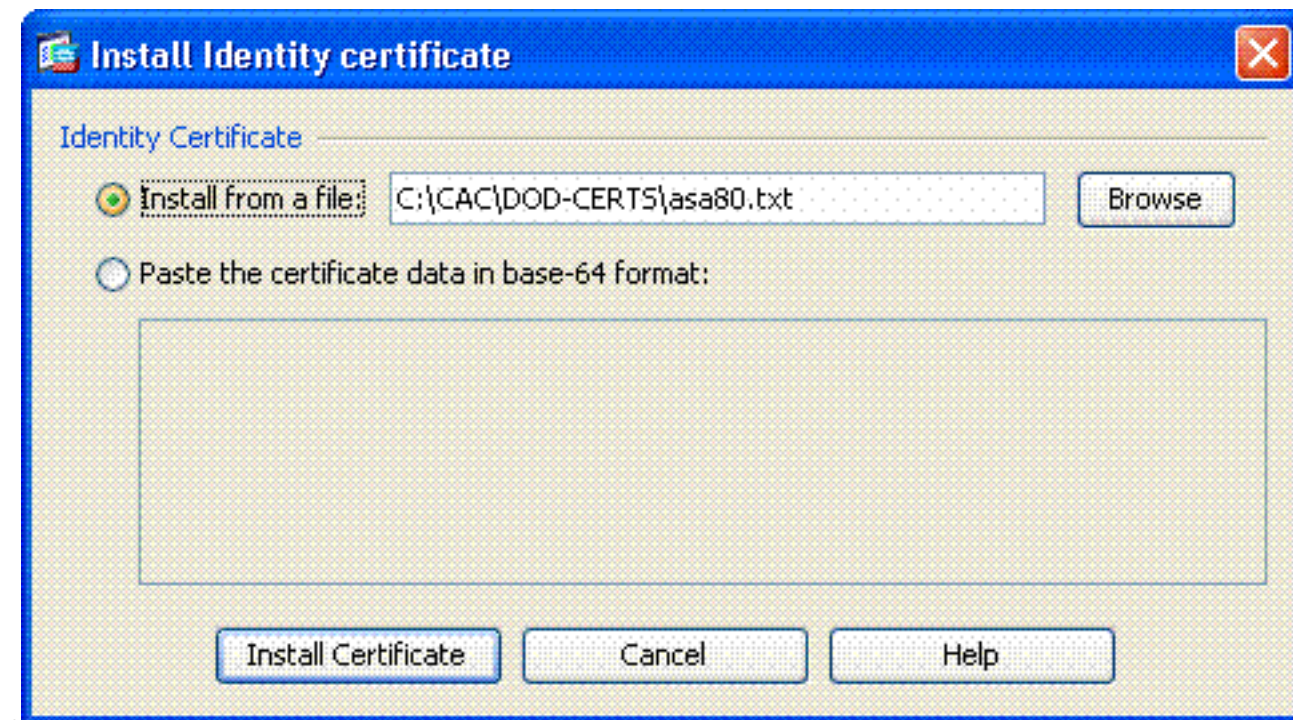
9. افتح الملف باستخدام WordPad، وانسخ الطلب إلى الوثائق المناسبة ثم قم بإرساله إلى PKI POC. راجع الشكل 10. الشكل 10: طلب التسجيل



10. ما إن يستلم أنت الشهادة من ال CA مدير، اختر Remote Access VPN < إدارة الشهادة < شهادة المعرف < تثبيت. راجع الشكل 11. الشكل 11: إستيراد شهادة الهوية



11. في نافذة "تثبيت شهادة"، استعرض للوصول إلى شهادة المعرف واختر تثبيت الشهادة. راجع الشكل 12 على سبيل المثال. الشكل 12: تثبيت شهادة الهوية



ملاحظة: يوصى بتصدير Id Certificate TrustPoint لحفظ أزواج الشهادات والمفتاح الصادرة. وهذا يسمح لمسؤول ASA باستيراد أزواج الشهادات والمفتاح إلى ASA جديد في حالة حدوث عطل في RMA أو في الجهاز. راجع [تصدير نقاط الثقة واستيرادها](#) للحصول على مزيد من المعلومات. ملاحظة: انقر فوق حفظ لحفظ التكوين في ذاكرة Flash المؤقتة).

تكوين AnyConnect VPN

هناك خياران لتكوين معلمات VPN في ASDM. الخيار الأول هو استخدام معالج SSL VPN. هذه أداة سهلة الاستخدام للمستخدمين الجدد في تكوين VPN. الخيار الثاني هو أن تفعل ذلك يدويا وتمضي خلال كل خيار. يستخدم دليل التكوين هذا الطريقة اليدوية.

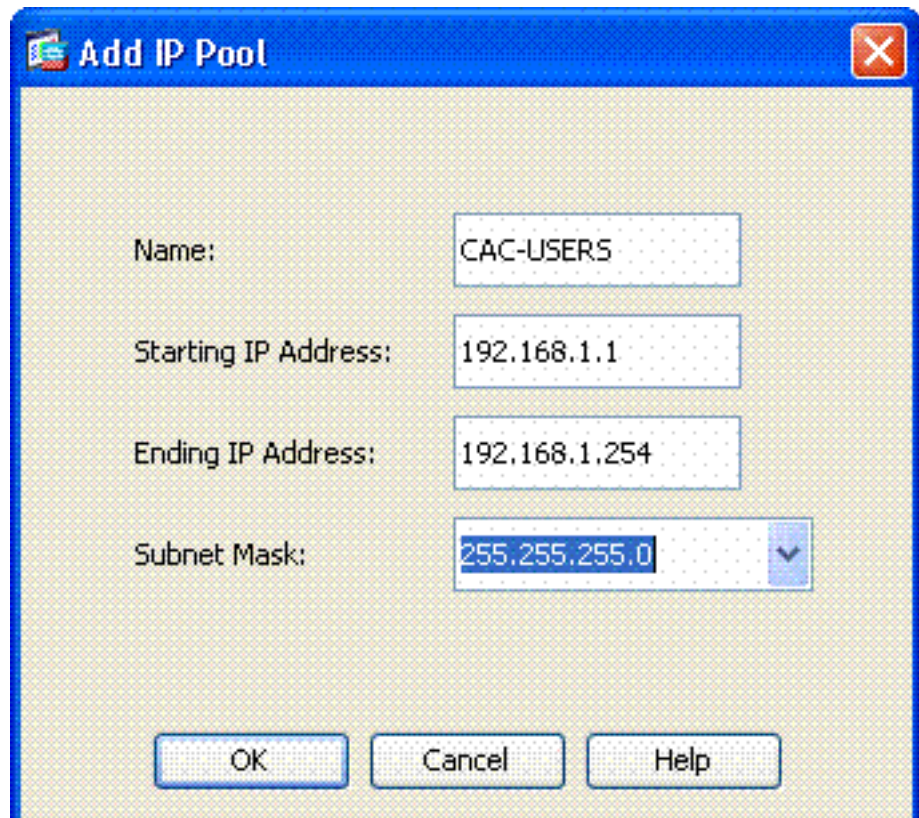
ملاحظة: هناك طريقتان لإيصال عميل AC إلى المستخدم:

1. يمكنك تنزيل العميل من موقع Cisco على الويب وتثبيته على الجهاز الخاص به.
 2. يمكن للمستخدم الوصول إلى ASA عبر مستعرض ويب ويمكن تنزيل العميل.
- ملاحظة:** على سبيل المثال، <https://asa.test.com>. يستخدم هذا الدليل الطريقة الثانية. بمجرد تثبيت عميل AC على جهاز العميل بشكل دائم، فما عليك سوى تشغيل عميل AC من التطبيق.

إنشاء تجمع عناوين IP

هذا اختياري إذا كنت تستخدم طريقة أخرى مثل DHCP.

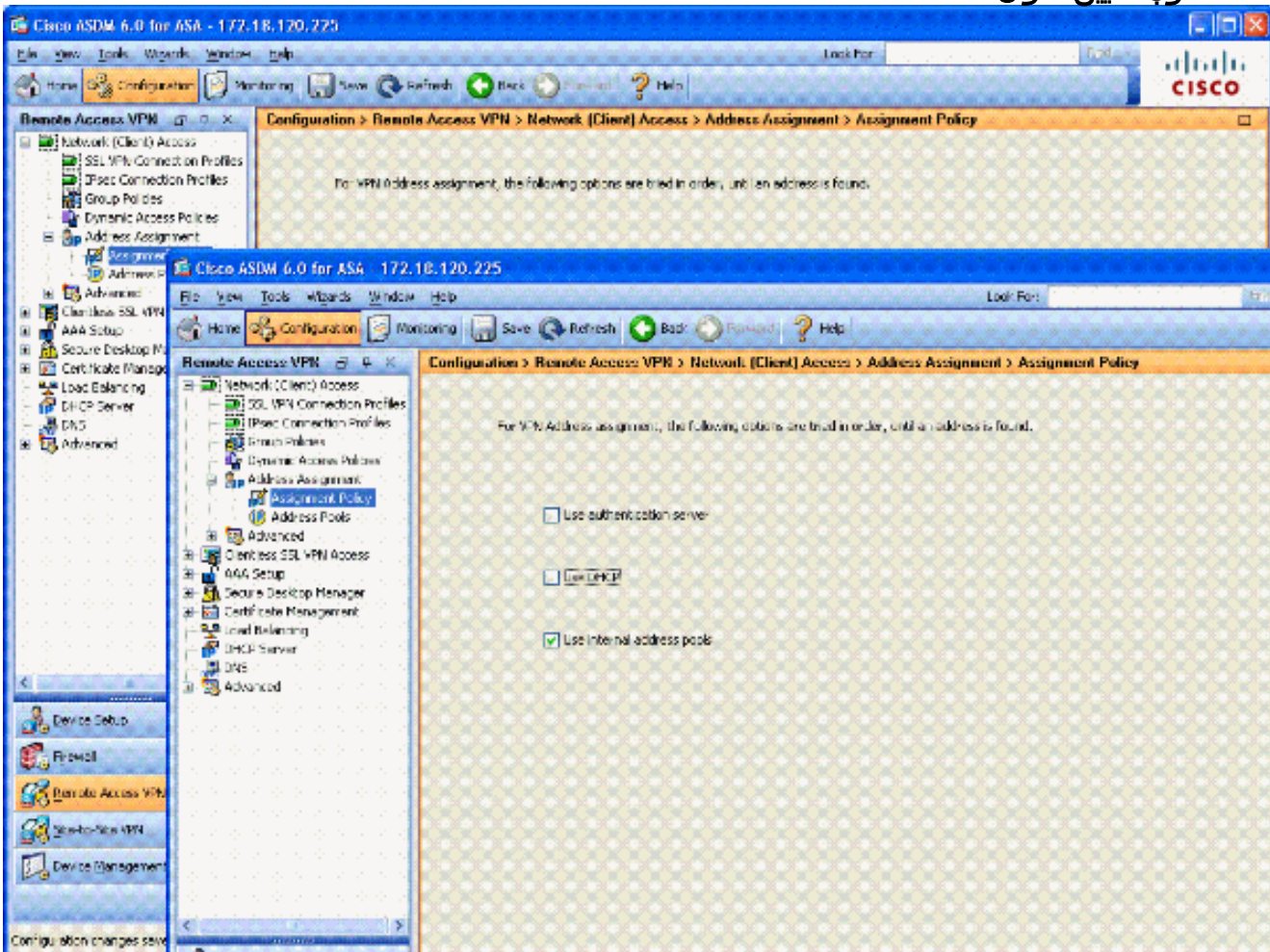
1. اختر Remote Access VPN (الشبكة الخاصة الظاهرية) > Network (VPN (العميل) > Address (العميل) > Access > Assignment (تعيين العناوين) > مجموعات العناوين.
2. انقر فوق إضافة (Add).
3. في نافذة إضافة تجمع IP، أدخل اسم تجمع IP، حيث تقوم بتشغيل عنوان IP ونهايته واختر قناع شبكة فرعية. انظر الشكل 13. الشكل 13: إضافة تجمع IP



4. أختار موافق.

5. أختار Remote Access VPN (الوصول عن بعد) < Network (العميل) Address Assignment > Access > Assignment Policy (تعيين العنوان).

6. حدد أسلوب تعيين عنوان IP المناسب. يستخدم هذا الدليل تجمعات العناوين الداخلية. انظر الشكل 14. الشكل 14: أسلوب تعيين عنوان IP

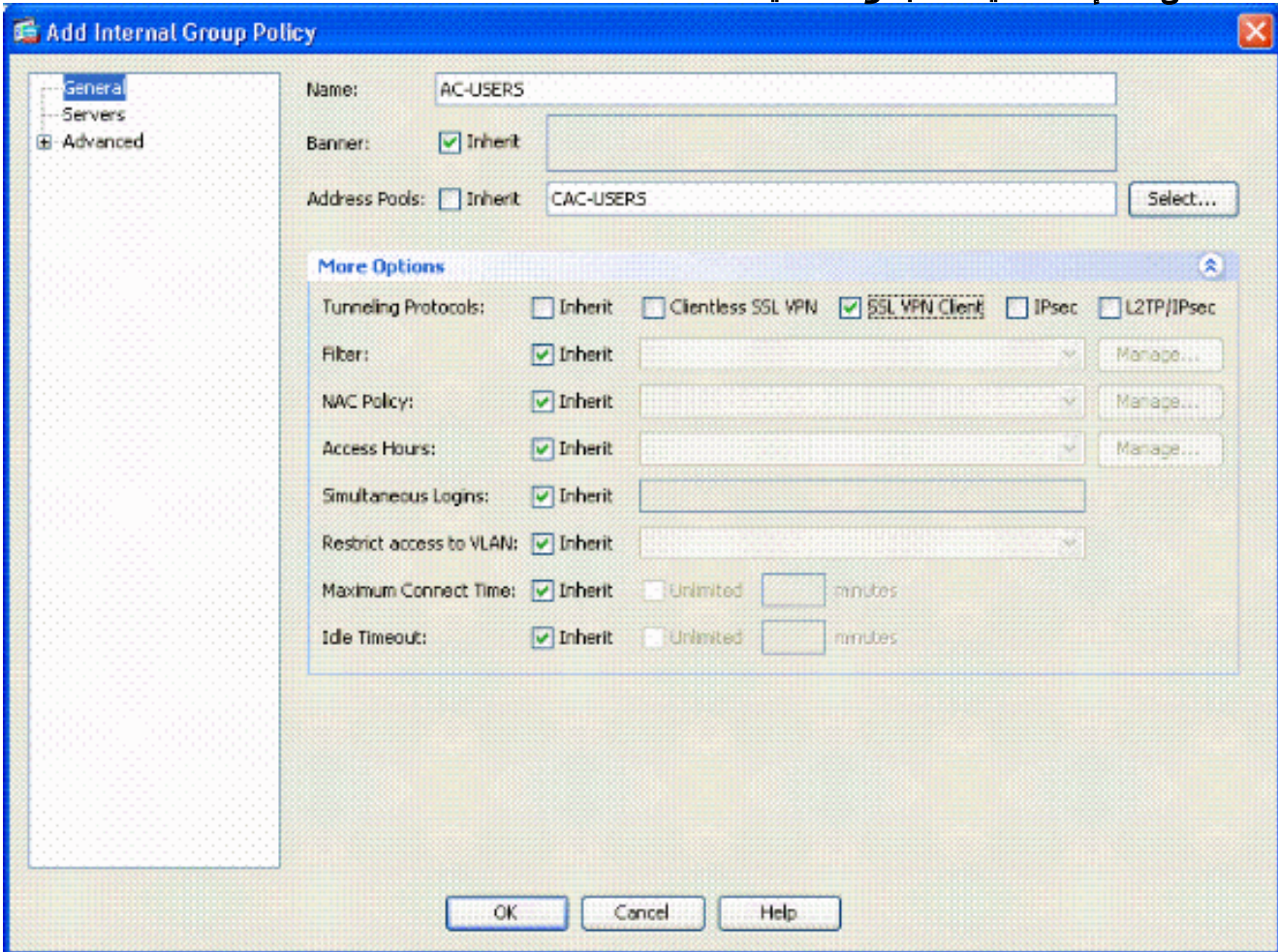


إنشاء مجموعة النفق ونهج المجموعة

نهج المجموعة

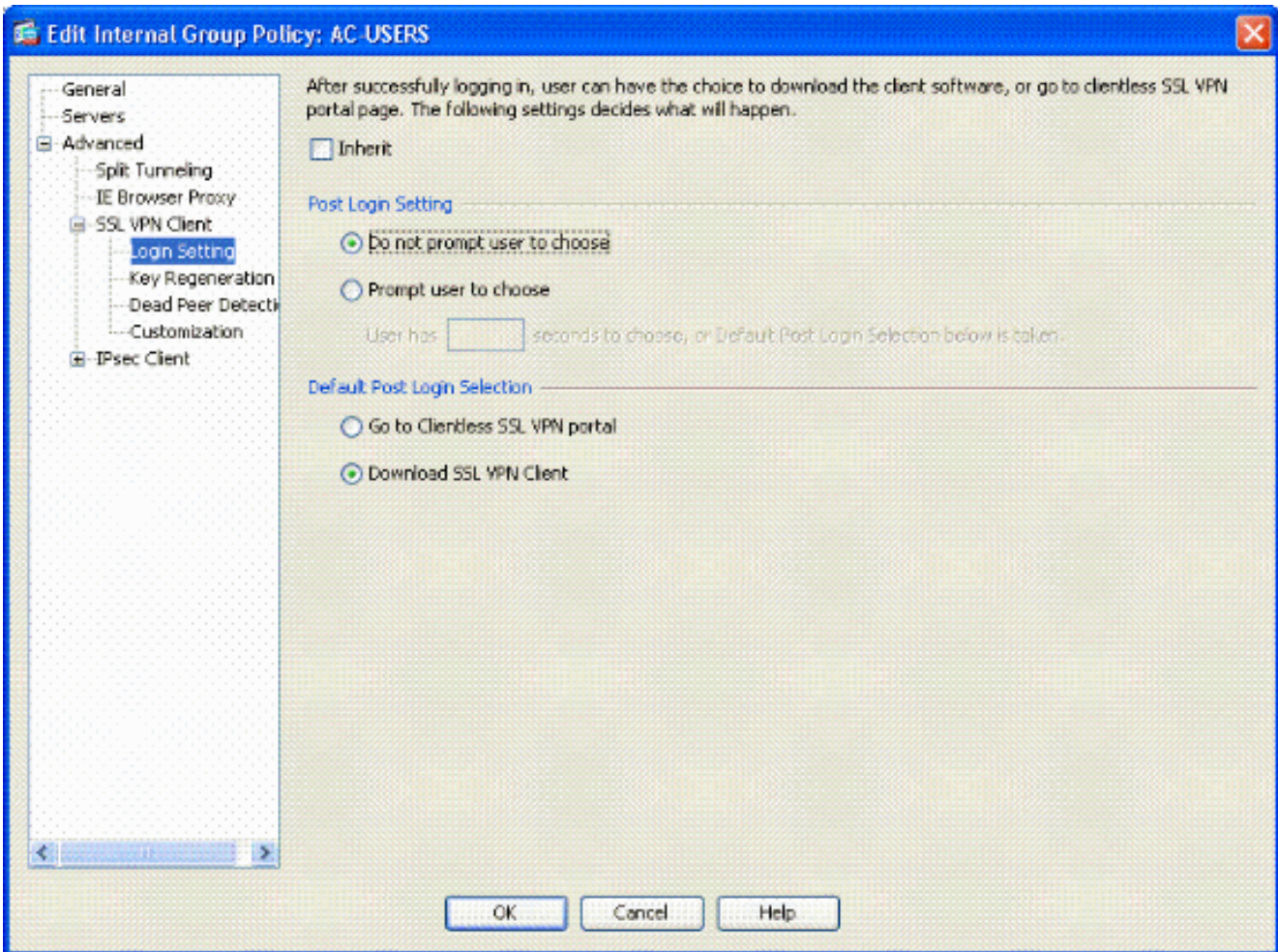
ملاحظة: إذا لم تكن ترغب في إنشاء نهج جديد، يمكنك استخدام النهج الافتراضي المضمن في المجموعة.

1. أختار الوصول عن بعد إلى VPN -> الوصول إلى الشبكة (العميل) -> نهج المجموعة.
2. انقر فوق إضافة واختر نهج المجموعة الداخلي.
3. في نافذة "إضافة نهج مجموعة داخلي"، أدخل اسم "نهج المجموعة" في مربع النص "الاسم". راجع الشكل 15. الشكل 15: إضافة سياسة مجموعة داخلية



في علامة التبويب "عام"، أختار **SSL VPN Client** في خيار بروتوكولات الاتصال النفقي، إلا إذا كنت تستخدم بروتوكولات أخرى مثل SSL بدون عميل. في قسم الخوادم، قم بإلغاء تحديد خانة الاختيار **Inherit** وأدخل عنوان IP الخاص بخوادم DNS و WINS. أدخل نطاق DHCP إذا كان ذلك ممكناً. في قسم الخوادم، قم بإلغاء تحديد خانة الاختيار **توريث** في المجال الافتراضي وأدخل اسم المجال المناسب. في علامة التبويب "عام"، قم بإلغاء تحديد خانة الاختيار **وراثه** في قسم تجمع العناوين وأضف تجمع العناوين الذي تم إنشاؤه في الخطوة السابقة. إذا كنت تستخدم طريقة أخرى لتعيين عنوان IP، فاترك هذه الطريقة للوراثه وقم بإجراء التغيير المناسب. تترك كل علامات تبويب التكوين الأخرى للإعدادات الافتراضية. ملاحظة: هناك طريقتان لنقل عميل AC إلى المستخدمين النهائيين. تتمثل أولاهما في الانتقال إلى Cisco.com وتنزيل عميل AC. الطريقة الثانية هي أن يقوم ASA بتنزيل العميل إلى المستخدم عندما يحاول المستخدم الاتصال. يوضح هذا المثال الأسلوب الأخير.

4. بعد ذلك، أختار **متقدم < SSL VPN Client > إعدادات تسجيل الدخول**. انظر الشكل 16. الشكل 16: إضافة سياسة مجموعة داخلية

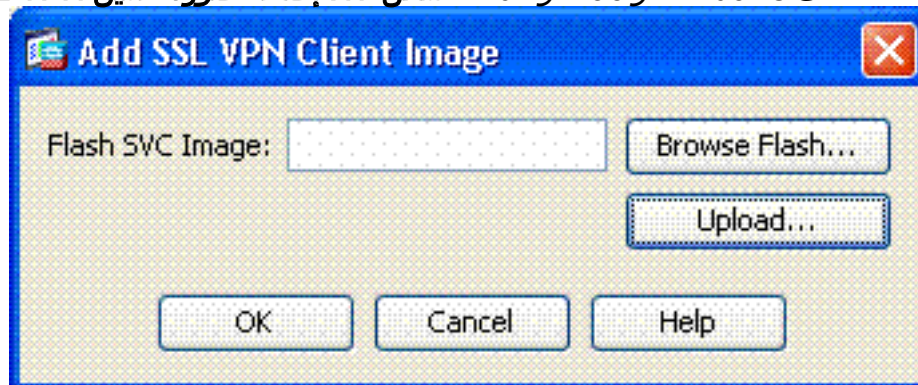


قم بإلغاء تحديد خانة الاختيار **توريث**. أختار الإعداد المناسب لـ Post Login (تسجيل الدخول إلى الموقع) الذي يناسب بيئتك. أختار تحديد مادة النشر الافتراضي المناسب الذي يناسب بيئتك. أختار **OK**.

واجهة مجموعة النفق وإعدادات الصورة

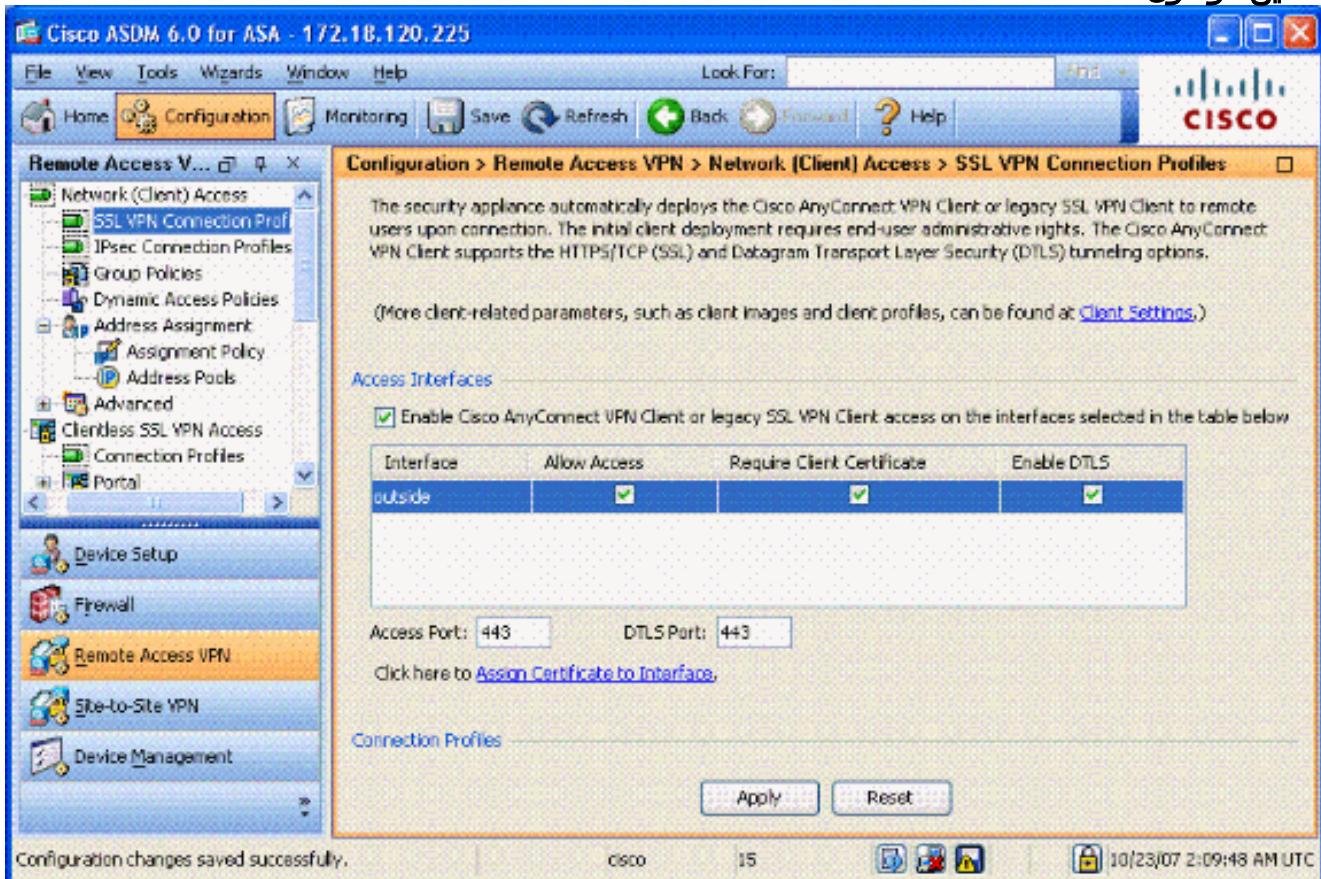
ملاحظة: إذا كنت لا تريد إنشاء مجموعة جديدة، يمكنك استخدام المجموعة المدمجة الافتراضية.

1. أختار Remote Access VPN (الوصول عن بعد) < Network (العميل) Access < ملف تعريف اتصال VPN لـ SSL.
2. أختار تمكين عميل Cisco AnyConnect
3. يظهر مربع حوار مع السؤال svc
4. أختار نعم.
5. إذا كان هناك صورة بالفعل، أختار الصورة التي تريد استخدامها مع تصفح Flash. إذا لم تكن الصورة متوفرة، أختار تحميل واستعرض الملف على الكمبيوتر المحلي. انظر الشكل 17. يمكن تنزيل الملفات من Cisco.com، هناك ملف Windows و Mac و Linux. شكل 17: إضافة صورة عميل SSL VPN



6. التمكين التالي يسمح بالوصول، يتطلب شهادة عميل وتمكين DTLS إختياريا. انظر الشكل 18. الشكل 18:

تمكين الوصول



7. طقطقة يطبق.

8. بعد ذلك، قم بإنشاء ملف تعريف اتصال/مجموعة نفق. أختَر Remote Access VPN (الوصول عن بعد) < Network (العميل) Access < ملف تعريف اتصال VPN ل SSL.

9. في قسم توصيفات التوصليل، انقر على إضافة.شكل 19: إضافة ملف تعريف الاتصال

Add SSL VPN Connection Profile

Basic
Advanced

Name: AC-USERS
Aliases:

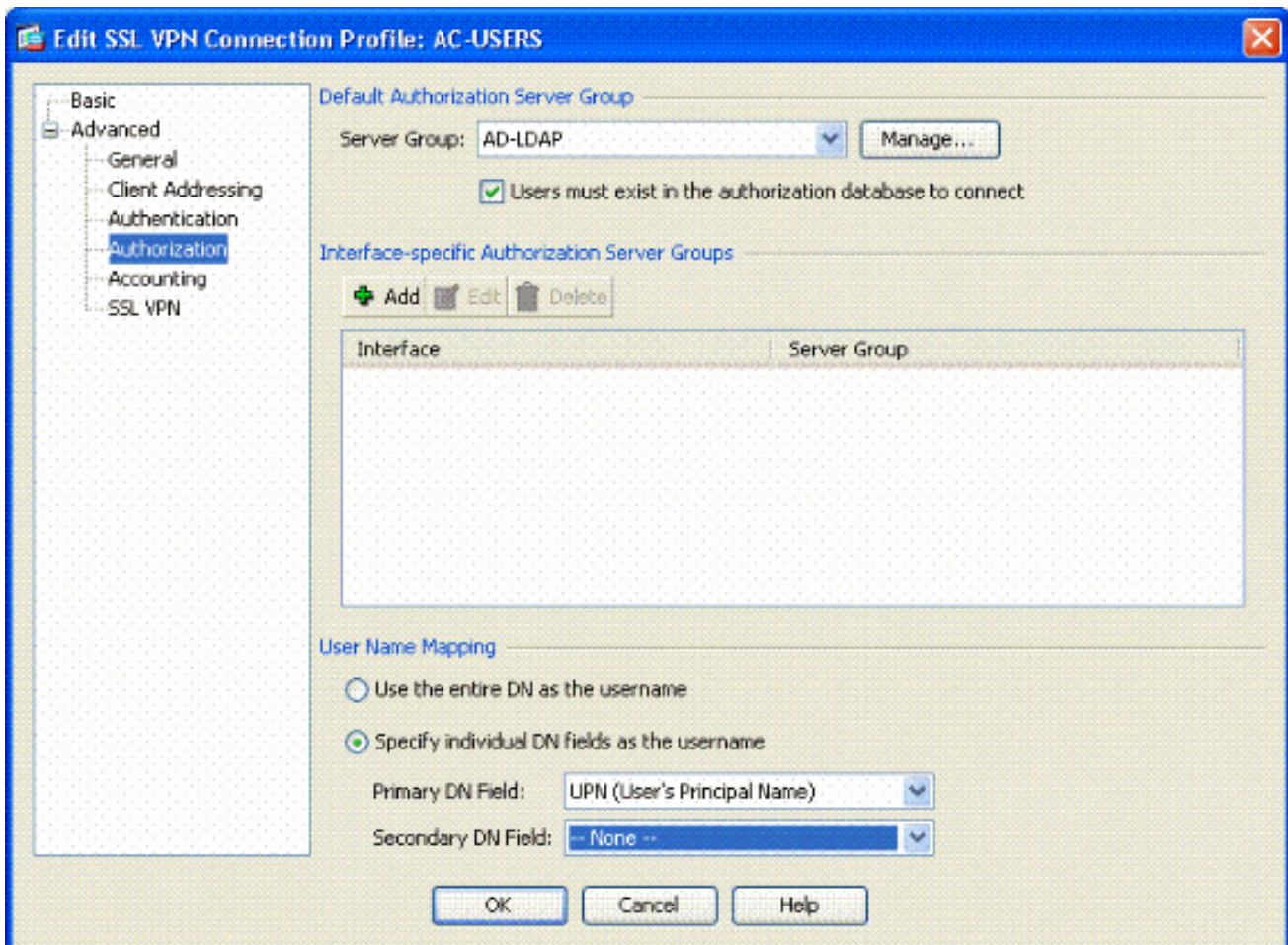
Authentication
Method: AAA Certificate Both
AAA Server Group: LOCAL Manage...
 Use LOCAL if Server Group Fails

Client Address Assignment
DHCP Servers:
Client Address Pools: Select...

Default Group Policy
Group Policy: AC-USERS Manage...
SSL VPN Client Protocol: Enabled

OK Cancel Help

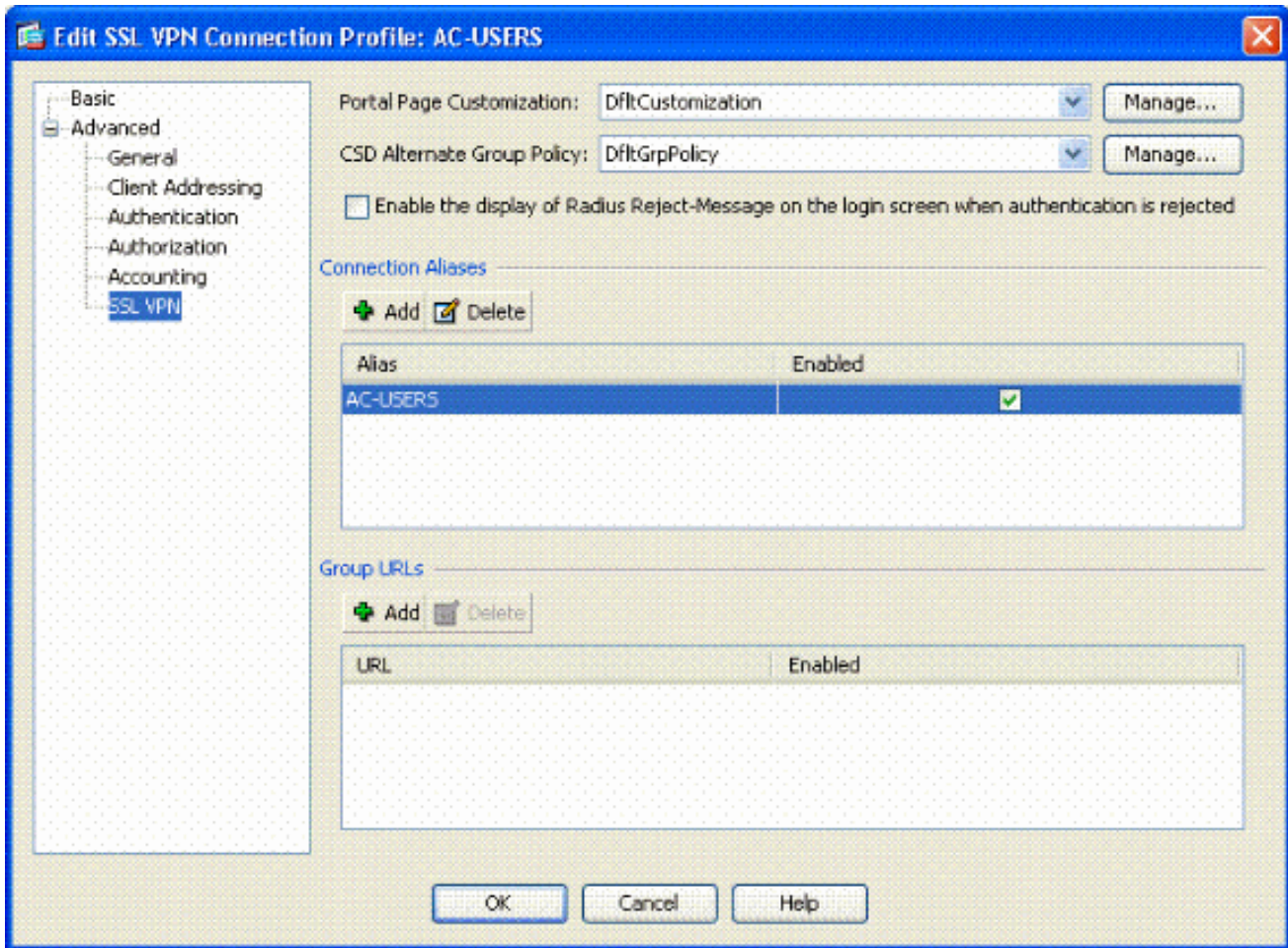
قم بتسمية المجموعة. اختر شهادة في طريقة المصادقة. اختر نهج المجموعة الذي تم إنشاؤه مسبقاً. تأكد من تمكين SSL VPN Client. أترك الخيارات الأخرى كافتراضي.
10. بعد ذلك، اختر متقدم < التحويل. راجع الشكل 20 الشكل 20: الترخيص



أختر مجموعة AD-LDAP التي تم إنشاؤها مسبقاً. تحقق من أنه يجب وجود المستخدمين... للاتصال. في حقول التعيين، اختر UPN للأساسي وnone للثانوي.

11. اخترت ال SSL VPN قسم من القائمة.

12. في قسم الأسماء المستعارة للاتصال، أكمل الخطوات التالية: الشكل 21: الأسماء المستعارة للاتصال



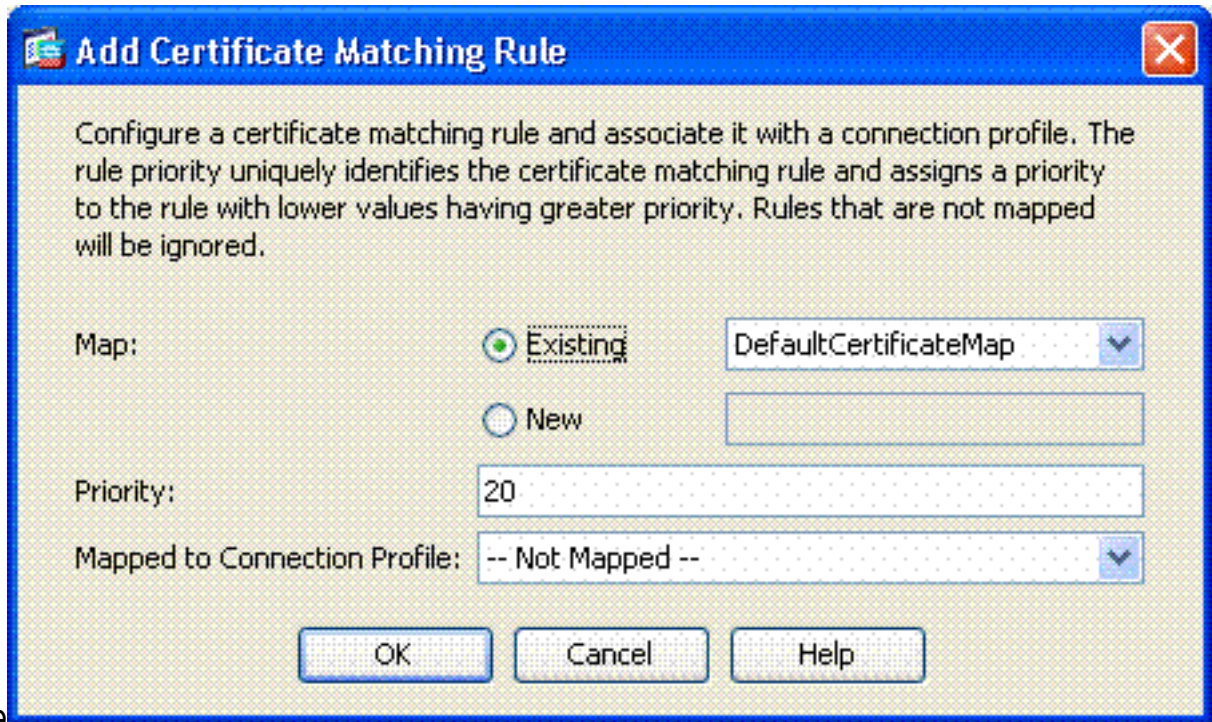
أختر إضافة. أدخل الاسم المستعار للمجموعة التي تريد إستخدامها. تأكد من أن ممكن يكون محددًا. انظر الشكل 21.

13. وانقر فوق OK.

ملاحظة: انقر فوق حفظ لحفظ التكوين في ذاكرة Flash (الذاكرة المؤقتة).

قواعد مطابقة الشهادة (إذا كان سيتم إستخدام OCSP)

1. أخترت Remote Access VPN < متقدم > شهادة إلى SSL VPN توصيل خرائط. انظر الشكل 22. أختر إضافة في قسم خرائط توصيفات التوصيل. يمكنك الاحتفاظ بالخريطة الموجودة كخريطة DefaultCertificateMap في قسم الخريطة أو إنشاء خريطة جديدة إذا كنت تستخدم بالفعل خرائط الثقة ل IPsec. حافظ على أولوية القاعدة. تحت مجموعة معينة، أترك باسم — غير معين —. انظر الشكل 22. الشكل 22: إضافة قاعدة مطابقة الشهادات

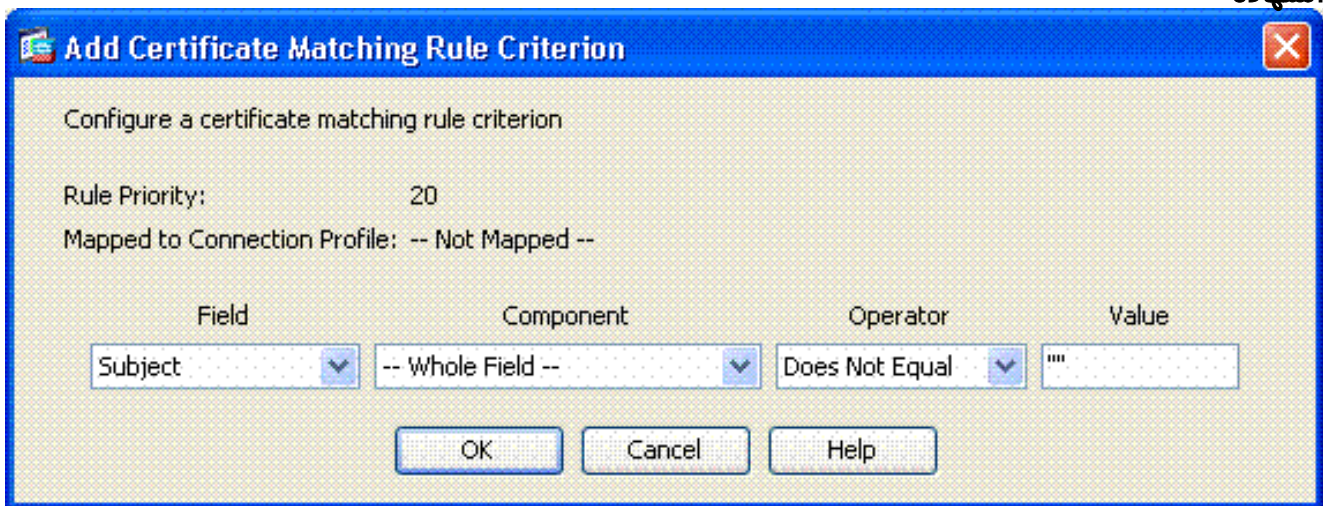


وانقر

فوق OK.

2. انقر فوق إضافة في الجدول السفلي.

3. في نافذة "معيار إضافة قاعدة مطابقة الشهادة"، أكمل الخطوات التالية: الشكل 23: معيار قاعدة مطابقة الشهادة



الاحتفاظ بعمود الحقل إلى الموضوع. الاحتفاظ بعمود المكون في الحقل بأكمله. قم بتغيير عمود عامل التشغيل إلى لا يساوي. في عمود القيمة، أدخل علامتي اقتباس ". طقطقة ok ويطبق. راجع الشكل 23 على سبيل المثال.

[تكوين OCSP](#)

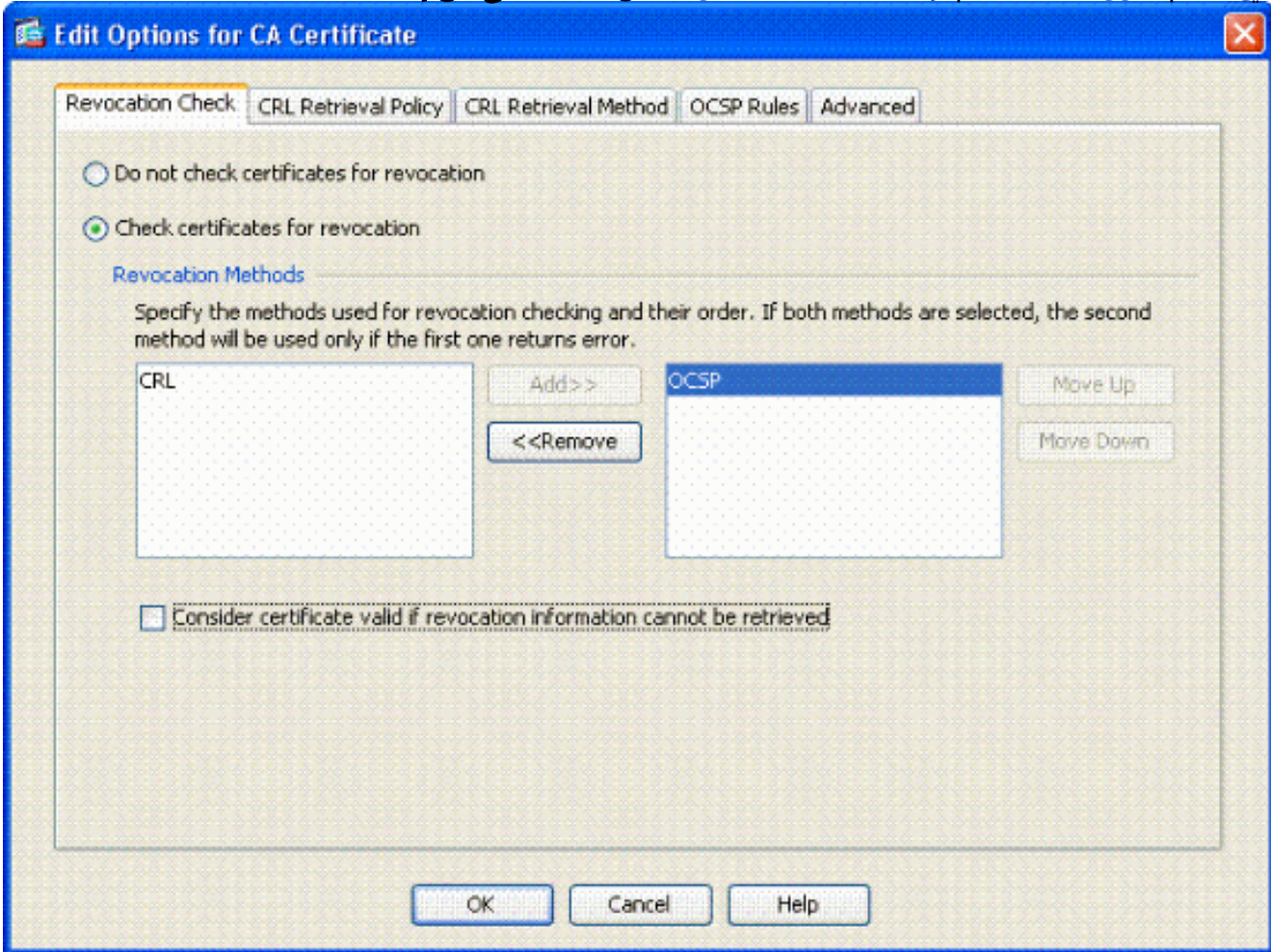
يمكن أن يختلف تكوين OCSP ويتوقف على مورد مستجيب OCSP. اقرأ دليل المبرشرين لمزيد من المعلومات.

[تكوين شهادة المستجيب OCSP](#)

1. الحصول على شهادة تم إنشاؤها ذاتيا من المستجيب OCSP.
2. أكمل الإجراءات المذكورة سابقا وقم بتثبيت شهادة لخاص OCSP. ملاحظة: تأكد من تحديد عدم التحقق من شهادات الإلغاء لنقطة الثقة لشهادة OCSP.

[تكوين CA لاستخدام OCSP](#)

1. أختار إدارة شهادات الوصول عن بعد < شهادات CA.
2. ركزت OCSP in order to أخترت CA أن يشكل أن يستعمل OCSP.
3. انقر فوق تحرير.
4. تأكد من التحقق من شهادة الإبطال.
5. في قسم طرق الإبطال، قم بإضافة OCSP. انظر الشكل 24.التحقق من إبطال OCSP



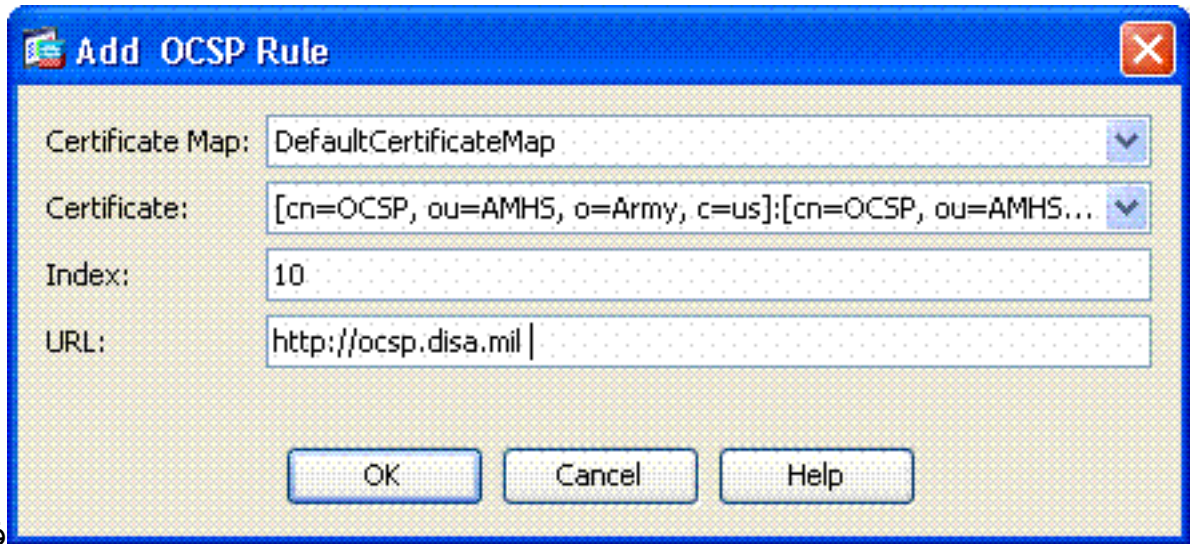
6. تأكد من أن إعتبار الشهادة صالحة... لا يمكن إستردادها إذا كنت تريد اتباع فحص OCSP الصارم. ملاحظة: تكوين/تحرير جميع خادم CA الذي يستخدم OCSP للإبطال.

تكوين قواعد OCSP

ملاحظة: تحقق من إنشاء نهج مطابقة لمجموعة الشهادات ومن تكوين المستجيب OCSP قبل إكمال هذه الخطوات.

ملاحظة: في بعض عمليات تنفيذ OCSP، قد تكون هناك حاجة إلى سجل DNS A و PTR لمكتب خدمات الدعم التقني. يتم إجراء هذا التحقق للتحقق من أن ASA من موقع mil.

1. أخترت Remote Access VPN < شهادة إدارة < شهادة CA 2.
2. ركزت OCSP in order to أخترت CA أن يشكل أن يستعمل OCSP.
3. أختار تحرير.
4. انقر فوق علامة التبويب قاعدة OCSP.
5. انقر فوق إضافة (Add).
6. في نافذة إضافة قاعدة OCSP، أكمل الخطوات التالية. راجع الشكل 25. الشكل 25: إضافة قواعد OCSP



في خيار

خريطة الشهادة، أختار DefaultCertificateMap أو خريطة تم إنشاؤها مسبقاً. في خيار الشهادة، أختار المستجيب OCSP. في خيار الفهرس، قم بإدخال 10. في خيار عنوان الربط، أدخل عنوان IP أو اسم المضيف الخاص بالمستجيب OCSP. إذا كنت تستخدم اسم المضيف، فتأكد من تكوين خادم DNS على ASA. وانقر فوق OK. طقطقة يطبق.

تكوين عميل AnyConnect من Cisco

يغطي هذا القسم تكوين عميل Cisco AnyConnect VPN.

الافتراضات — تم تثبيت عميل AnyConnect VPN من Cisco وتطبيق Middleware بالفعل في الكمبيوتر المضيف. تم اختبار ActiveClient و ActiveCard Gold.

ملاحظة: يستخدم هذا الدليل أسلوب URL المجموعة للتثبيت الأولي لعميل AC فقط. بمجرد تثبيت عميل AC، تقوم بتشغيل تطبيق AC تماماً مثل عميل IPsec.

ملاحظة: يلزم تثبيت سلسلة شهادات DoD على الجهاز المحلي. ارجع إلى PKI POC للحصول على ملف الشهادات/الدفع.

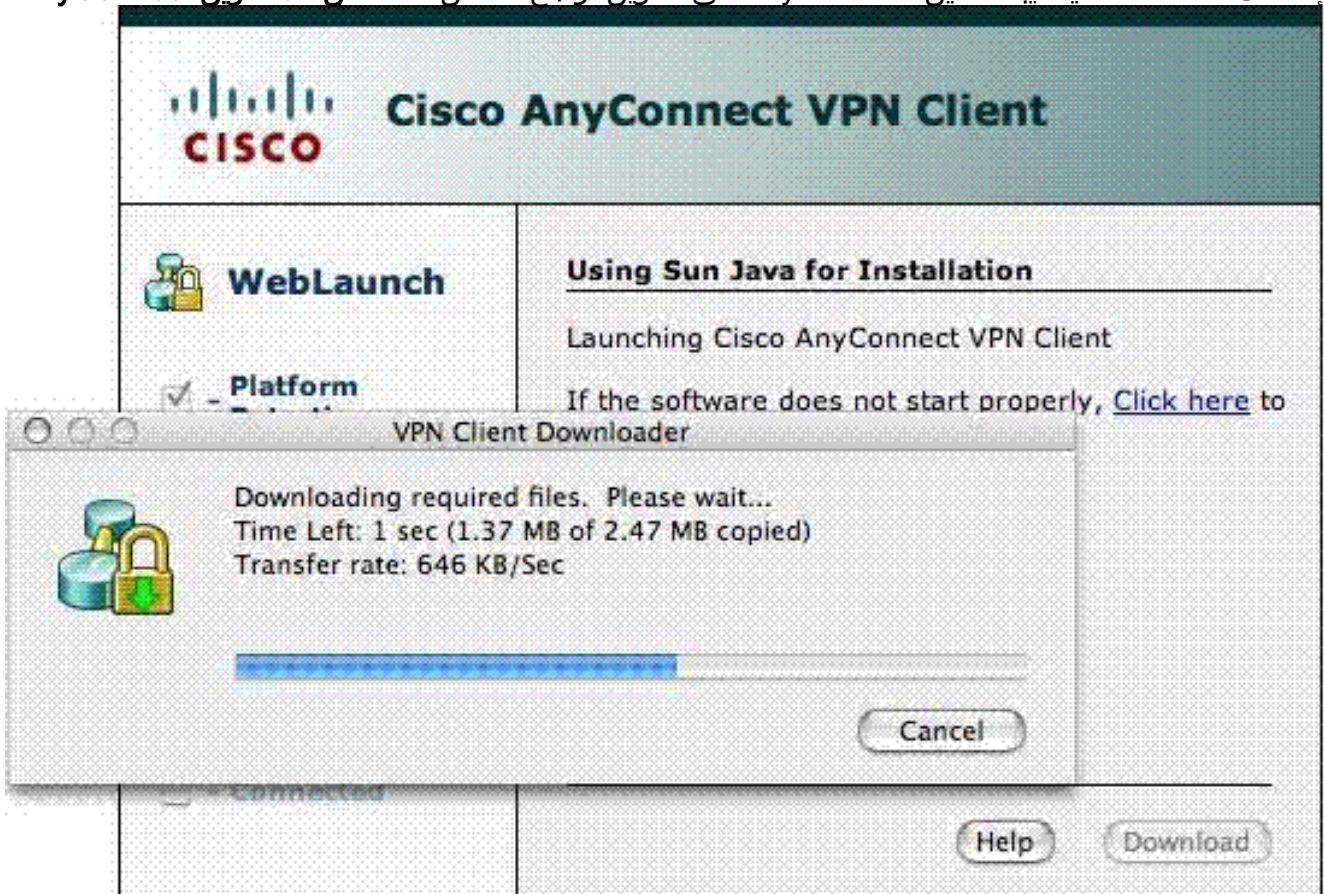
ملاحظة: برنامج تشغيل قارئ البطاقة لـ Mac OS X مثبت بالفعل ومتوافق مع إصدار نظام التشغيل الحالي الذي تستخدمه.

تنزيل Cisco AnyConnect VPN Client - Mac OS X

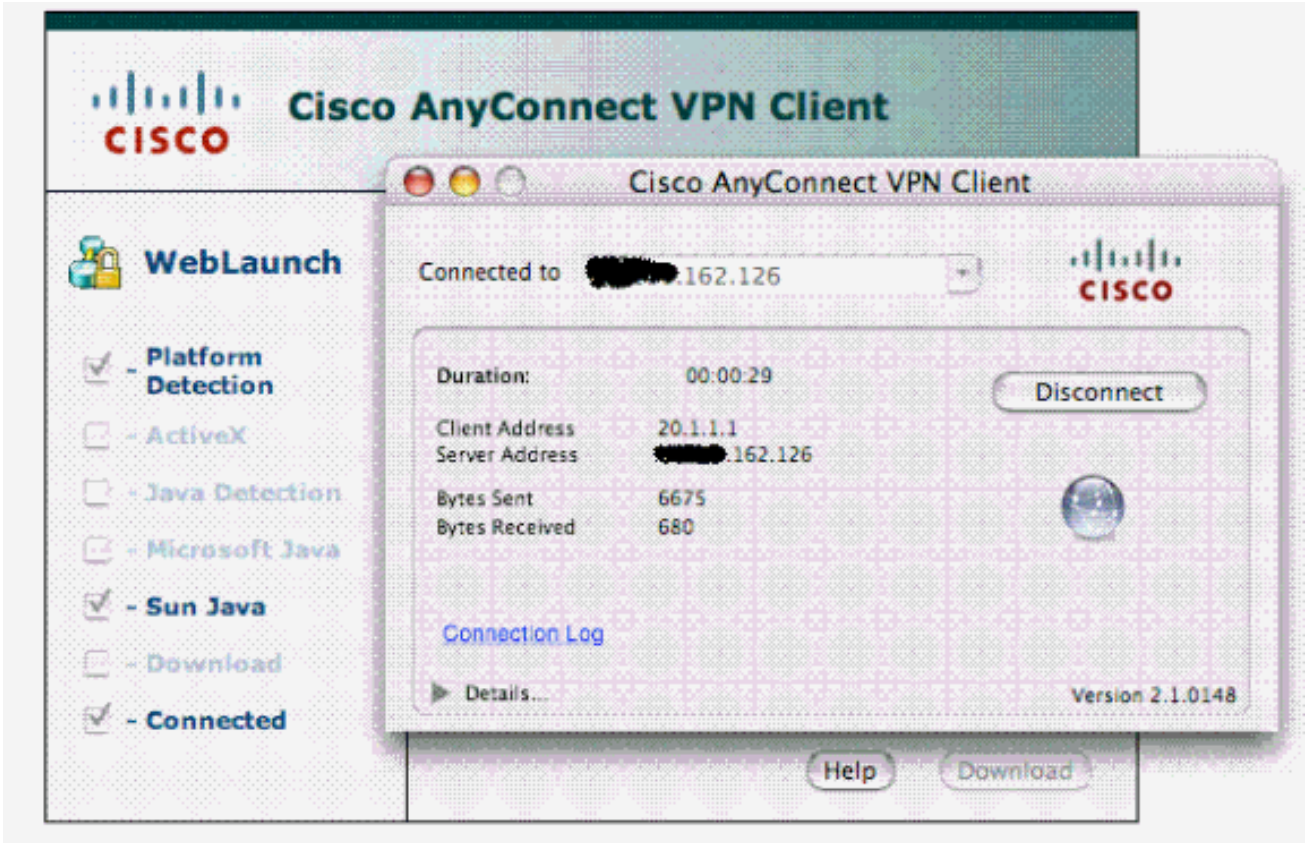
1. إطلاق موقع جلسة إلى الـ ASA من خلال Safari. ينبغي أن يكون العنوان على شكل <https://Outside-Interface.https://172.18.120.225>.
2. إطار منبثق يطلب التحقق من شهادة ASA. انقر فوق متابعة.
3. يظهر نافذة منبثقة أخرى لإلغاء تأمين سلسلة مفاتيح CAC. أدخل رقم التعريف الشخصي (PIN). راجع الشكل 31. شكل 31: أدخل رمز PIN



4. بعد أن تظهر صفحة ويب SSL VPN-service، انقر فوق متابعة.
5. بعد إلغاء تأمين سلسلة المفاتيح، يطالبك المستعرض إذا كنت تشق في الشهادة من ASA. انقر فوق الثقة.
6. أدخل كلمة مرور الجذر لإلغاء تأمين سلسلة المفاتيح لإنشاء اتصال آمن، ثم انقر على موافق.
7. أخطر الشهادة التي تريد استخدامها لمصادقة العميل، ثم انقر على موافق.
8. ثم يطلب المستعرض كلمة مرور الجذر/المستخدم للسماح بتنزيل عملاء AnyConnect.
9. إذا تمت المصادقة عليه، يبدأ عميل AnyConnect في التنزيل. راجع الشكل 32. شكل 32: تنزيل AnyConnect



10. بعد تنزيل التطبيق، يطالبك المستعرض بقبول شهادة ASA. انقر فوق قبول.
11. تم تأسيس الاتصال. شكل 33. شكل 33: AnyConnect متصل



بدء تشغيل Cisco AnyConnect VPN Client من Cisco - نظام التشغيل Mac OS X

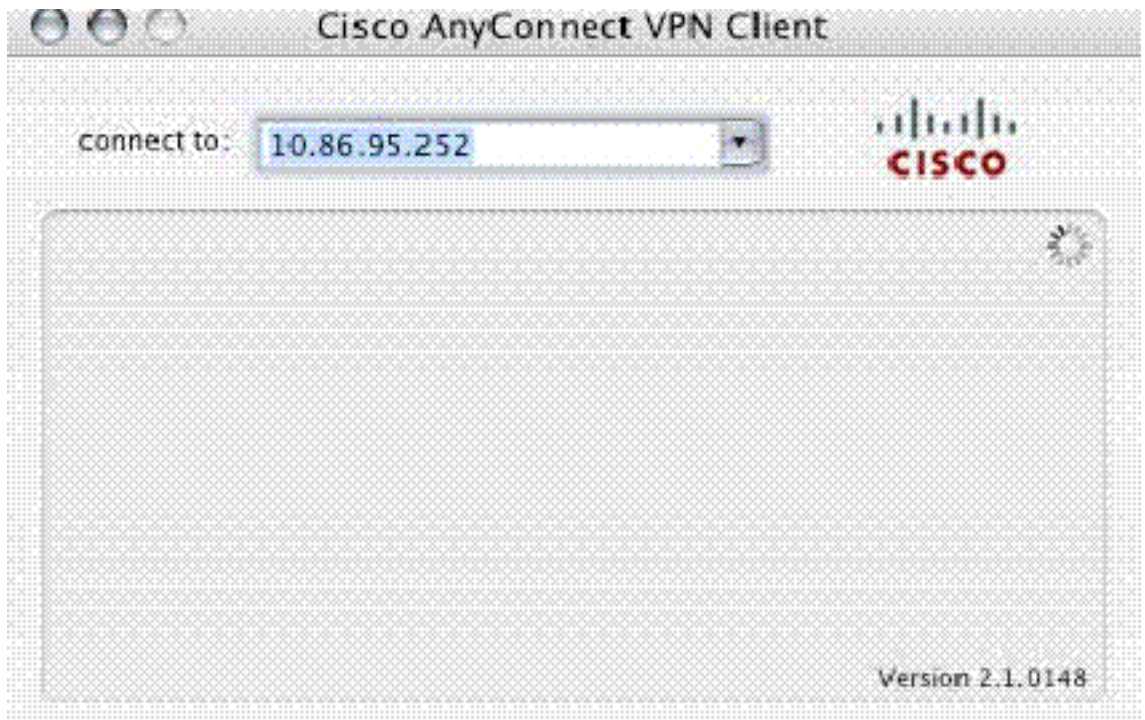
من Cisco AnyConnect VPN عميل < Finder—Applications

ملاحظة: راجع الملحق (هـ) للحصول على تكوين ملف تعريف عميل AnyConnect الاختياري.

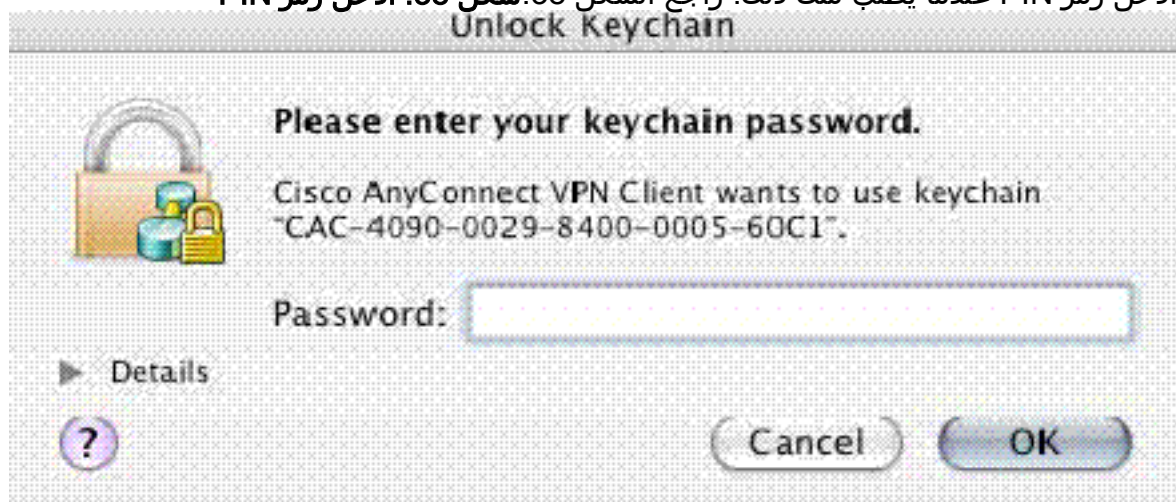
اتصال جديد

تظهر نافذة التيار المتردد. انظر الشكل 37.

شكل 37: اتصال VPN جديد

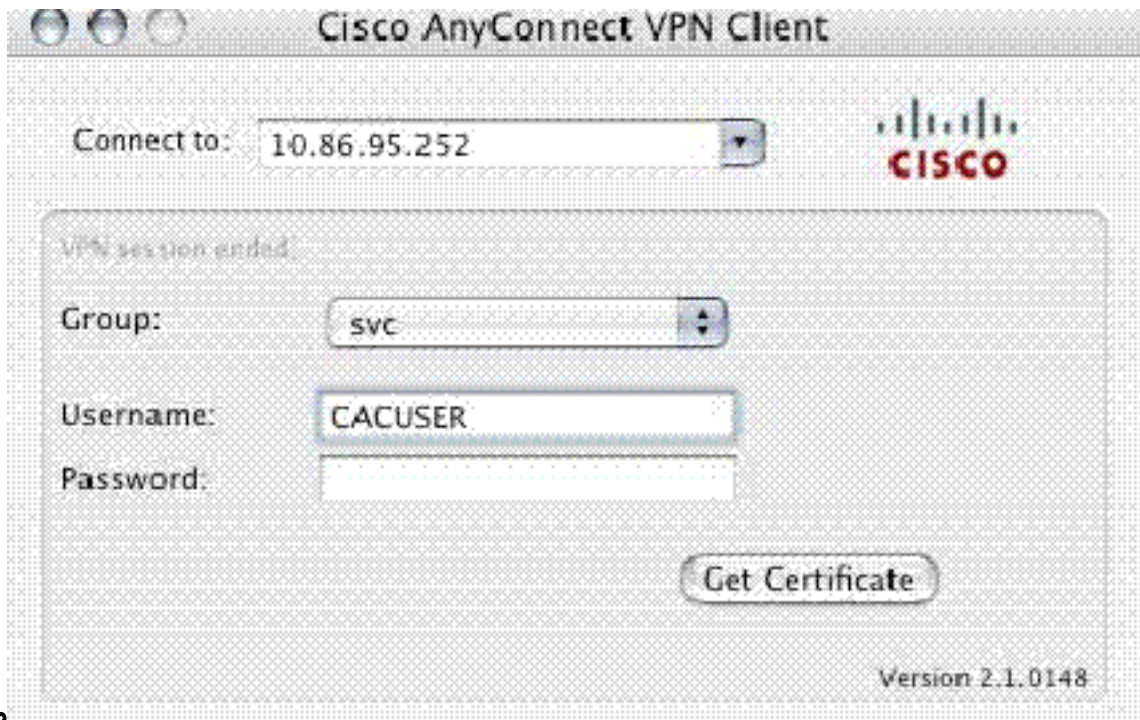


1. أختار المضيف المناسب إذا لم يحاول AC الاتصال تلقائياً.
2. أدخل رمز PIN عندما يطلب منك ذلك. راجع الشكل 38. شكل 38: أدخل رمز PIN



بدء الوصول عن بعد

1. أختار المجموعة والمضيف اللذين تريد الاتصال بهما.
2. أخترت بما أن شهادات استعملت، يربط in order to أسست ال VPN. راجع الشكل 39. ملاحظة: نظراً لأن الاتصال يستخدم الشهادات، فلا حاجة لإدخال اسم مستخدم وكلمة مرور. شكل 39: التوصيل



ملاحظة: راجع

الملحق (ه) للحصول على تكوين ملف تعريف عميل AnyConnect الاختياري.

الملحق أ - تخطيط LDAP و DAP

في الإصدار 7.1(x) من ASA/PIX والإصدارات الأحدث، تم تقديم ميزة تسمى تخطيط LDAP. هذه ميزة قوية توفر تعيين بين سمة Cisco وكائنات/سمة LDAP، مما ينفي الحاجة إلى تغيير مخطط LDAP. لتنفيذ مصادقة CAC، يمكن أن يدعم هذا فرض سياسات إضافية على اتصال الوصول عن بعد. هذا مثال من LDAP يخطط. اعلم أنك تحتاج إلى حقوق المسؤول لإجراء تغييرات في خادم AD/LDAP. في برنامج ASA 8.x، تم تقديم ميزة سياسة الوصول الديناميكي (DAP). يمكن أن يعمل بروتوكول DAP بالاقتران مع CAC للنظر في مجموعات AD متعددة بالإضافة إلى سياسات الدفع وقوائم التحكم في الوصول وما إلى ذلك.

السيناريو 1: تطبيق Active Directory باستخدام الطلب الهاتفي لأذن الوصول عن بعد - السماح بالوصول/رفضه

يخطط هذا المثال سمة AD msNPAllowDailin إلى سمة Cisco cVPN3000-tunneling - البروتوكول.

- قيمة سمة AD: صواب = السماح؛ خطأ = رفض
- قيمة سمة (IPSec = 4، Cisco: 1 = false، أو 20) (IPSec + 16 WebVPN) = true 4
- للشروط "السماح"، قم بتعيين:

- صحيح = 20
- لرفض الطلب الهاتفي، تقوم بتعيين:

- خطأ = 1

ملاحظة: تأكد من أن TRUE و FALSE في كل الحروف كبيرة. راجع تكوين خادم خارجي لتفويض مستخدم جهاز الأمان للحصول على مزيد من المعلومات.

إعداد Active Directory

1. في خادم Active Directory، انقر فوق ابدأ < تشغيل.
2. في مربع النص المفتوح، اكتب dsa.msc ثم انقر موافق. يقوم هذا بتشغيل وحدة تحكم إدارة Active

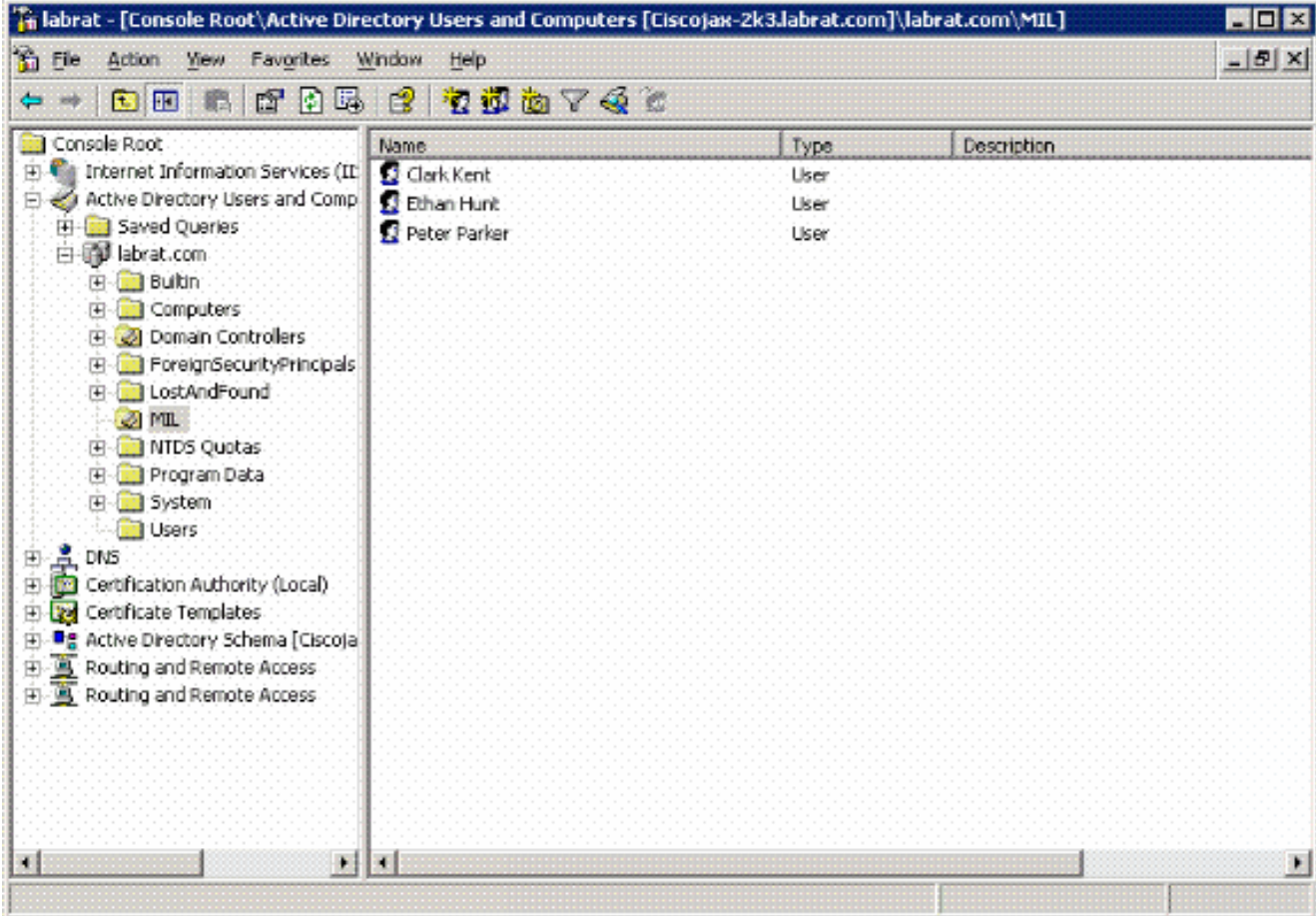
.Directory

3. في وحدة تحكم إدارة Active Directory، انقر فوق علامة الجمع لتوسيع Active Directory Users and Computers.

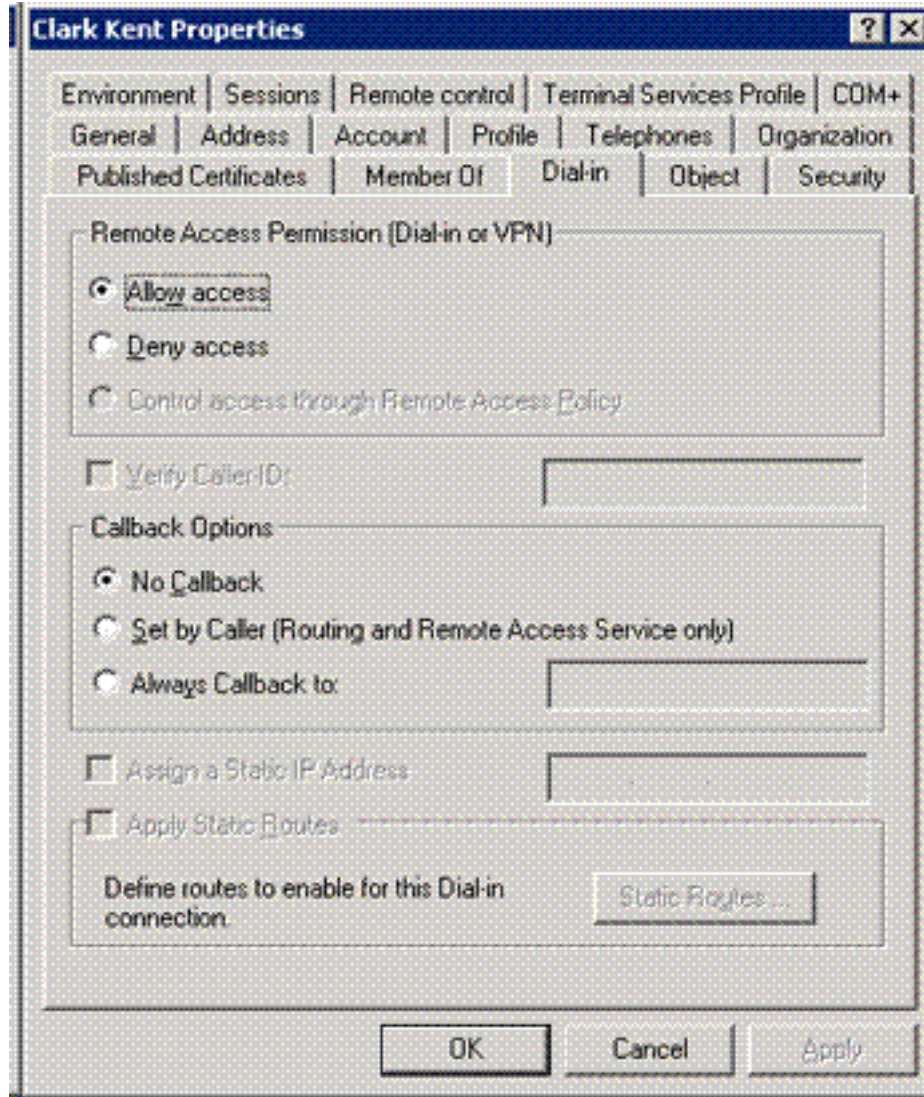
4. انقر فوق علامة الجمع لتوسيع اسم المجال.

5. إذا كان لديك وحدة تخزين تم إنشاؤها للمستخدمين، فقم بتوسيع وحدة التحكم لعرض كافة المستخدمين، وإذا كان لديك كافة المستخدمين الذين تم تعيينهم في مجلد المستخدمين، فقم بتوسيع هذا المجلد لعرضهم. راجع

الشكل A1. الشكل A1: وحدة تحكم إدارة Active Directory



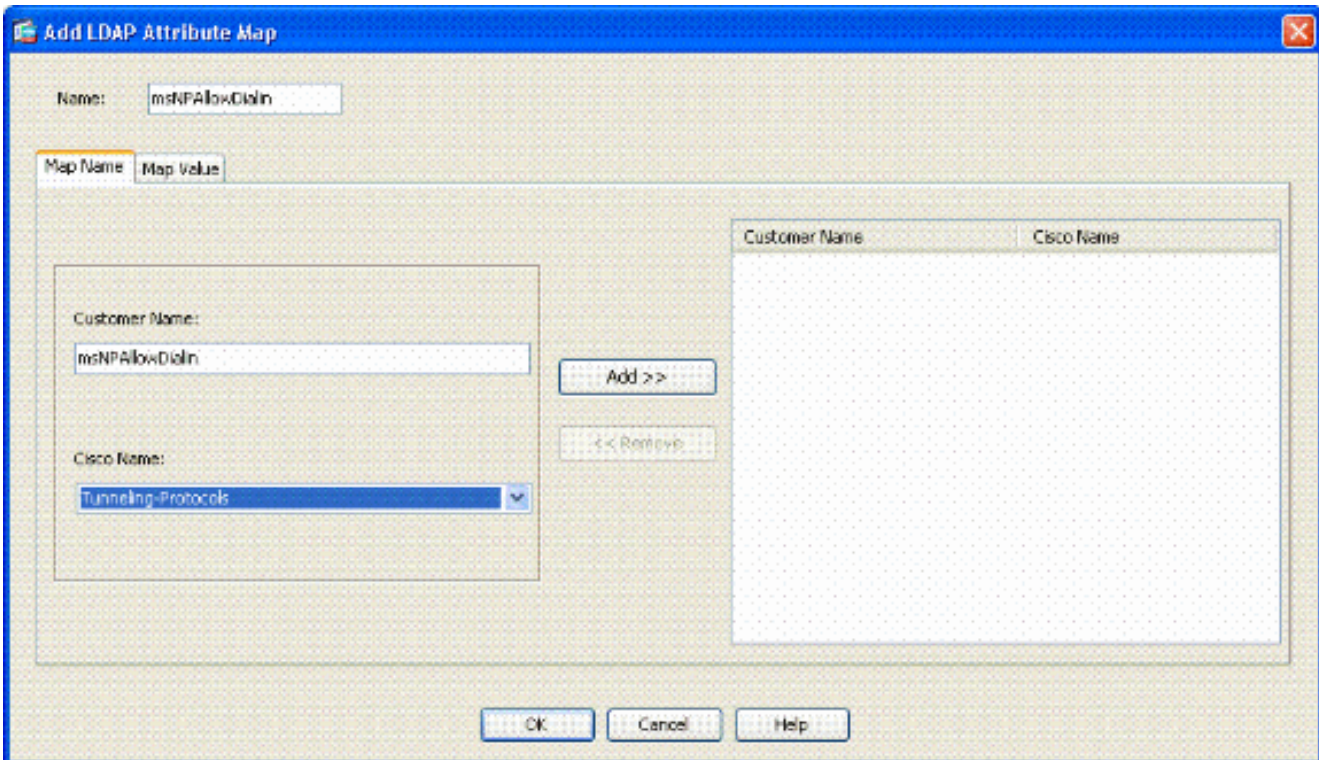
6. انقر نقرًا مزدوجًا فوق المستخدم الذي تريد تحريره. انقر فوق علامة التبويب "الطلب الهاتفي" في صفحة خصائص المستخدم وانقر فوق السماح أو الرفض. راجع الشكل أ 2. الشكل أ 2: خصائص المستخدم



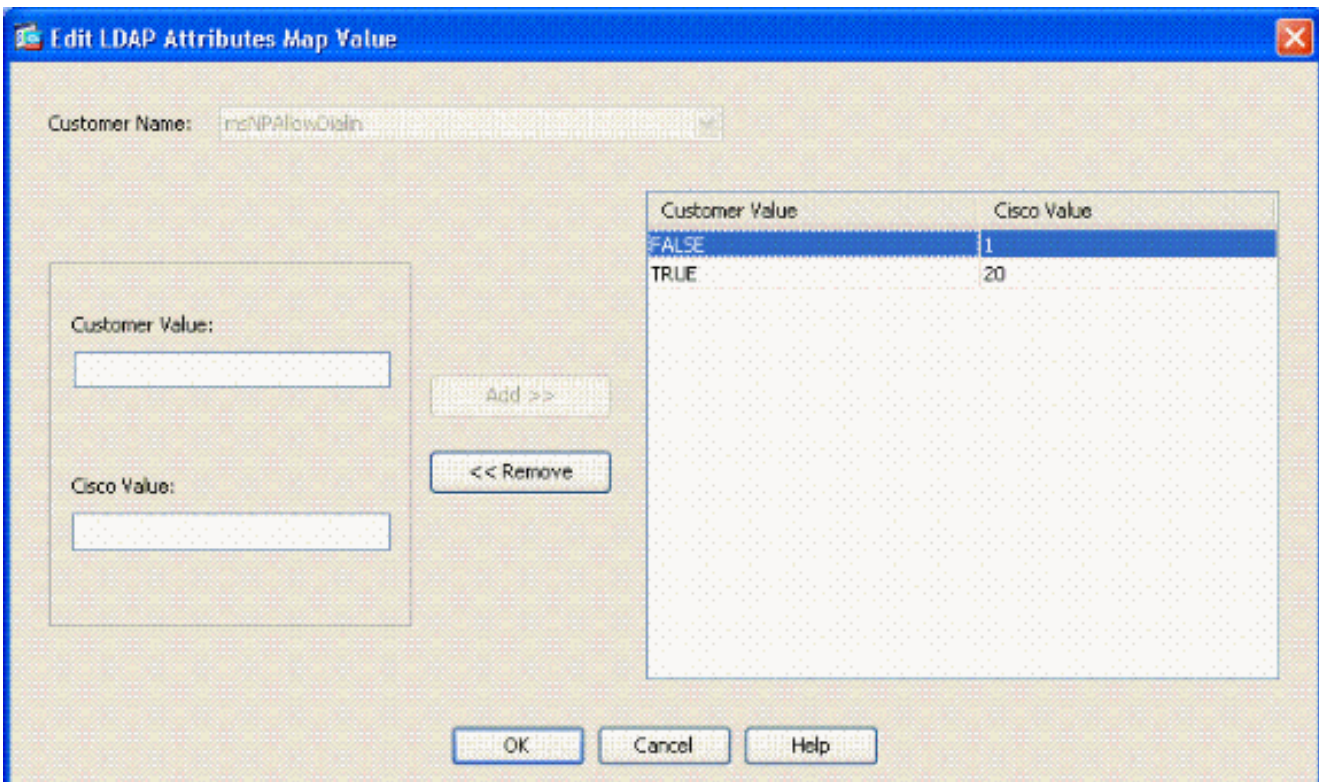
7. ثم انقر فوق OK.

[تكوين ASA](#)

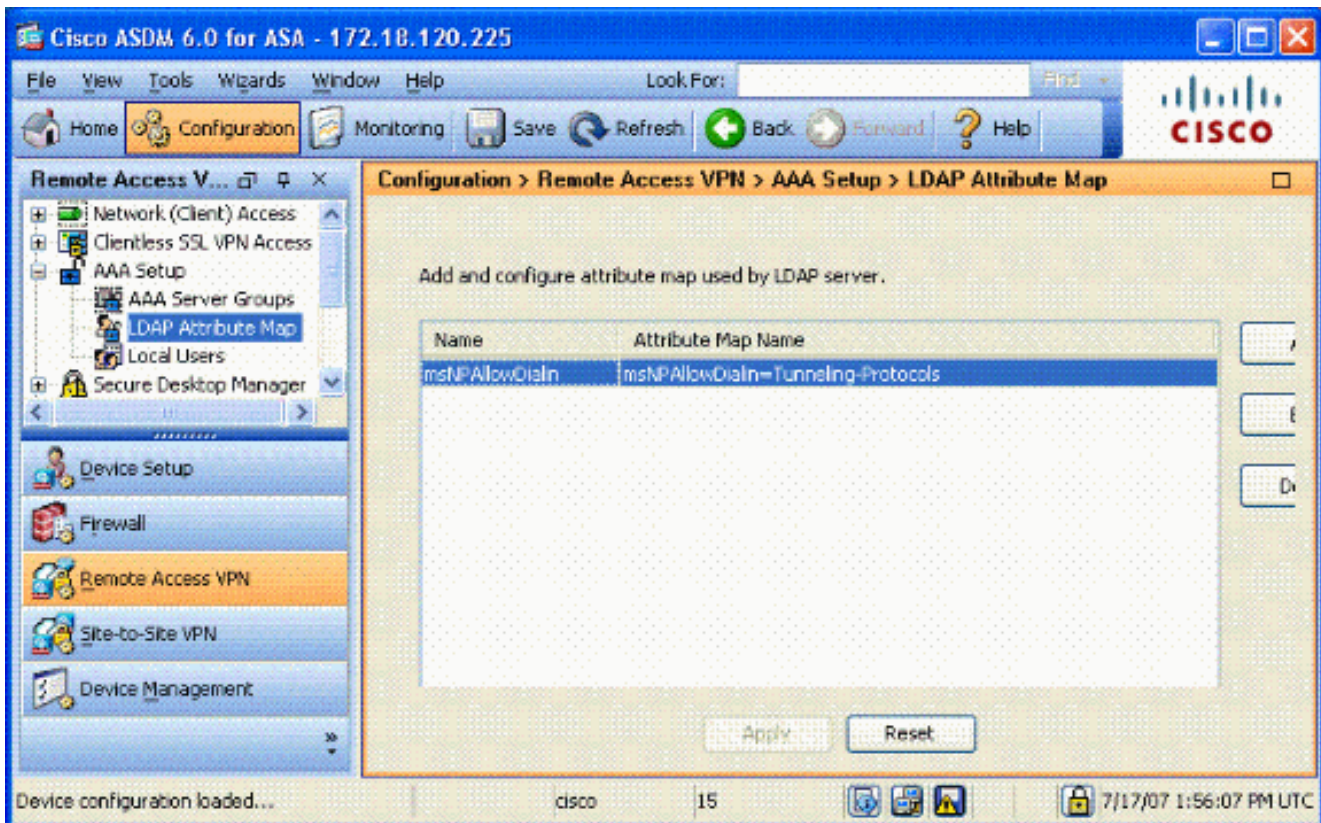
1. في ASDM، اختر إعداد AAA للوصول عن بعد VPN < خريطة سمة LDAP.
2. انقر فوق إضافة (Add).
3. في نافذة خريطة إضافة سمة LDAP، أكمل الخطوات التالية. انظر الشكل أ 3. الشكل A3: إضافة تعيين سمة LDAP



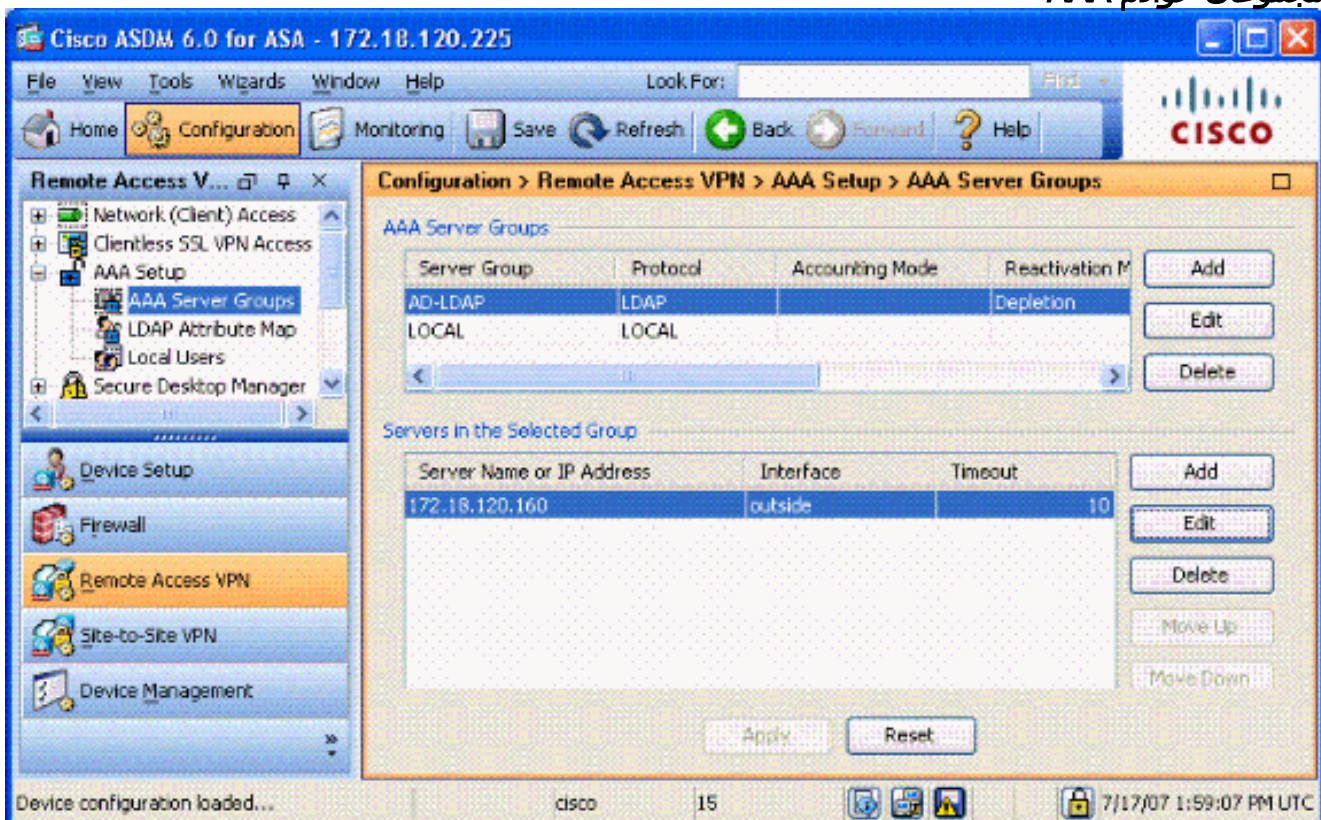
أدخل اسما في مربع نص الاسم. في علامة التبويب "اسم الخريطة"، اكتب msNPAllowDialin في مربع النص "اسم العميل". في علامة التبويب اسم الخريطة، اختر بروتوكولات الاتصال النفقي في الخيار المنسدل في اسم Cisco. انقر فوق إضافة (Add). اختر علامة التبويب تعيين قيمة. انقر فوق إضافة (Add). في نافذة قيمة خريطة LDAP للسمة المضافة، اكتب TRUE في مربع النص اسم العميل واكتب 20 في مربع النص قيمة Cisco. انقر فوق إضافة (Add). اكتب FALSE في مربع نص اسم العميل واكتب 1 في مربع نص قيمة Cisco. راجع الشكل 4.



وانقر فوق OK. وانقر فوق OK. طقطقة يطبق. يجب أن يبدو التكوين مثل الشكل A5. الشكل A5: تكوين تعيين سمة LDAP



4. أختار إعداد AAA للوصول عن بعد VPN < مجموعات خوادم AAA. انظر الشكل ألف 6. الشكل A6:



5. انقر فوق مجموعة الخوادم التي تريد تحريرها. في الخوادم الموجودة في قسم المجموعة المحددة، أختار عنوان IP الخاص بالخادم أو اسم المضيف، ثم انقر فوق تحرير.

6. في نافذة Edit AAA Server، في مربع نص خريطة سمة LDAP، أختار خريطة سمة LDAP التي تم إنشاؤها في القائمة المنسدلة. راجع الشكل A7 الشكل A7: إضافة تعيين سمة LDAP

7. وانقر فوق OK.

ملاحظة: قم بتشغيل تصحيح LDAP بينما تقوم بالاختبار للتحقق من عمل ربط LDAP وتخطيط السمات بشكل صحيح. راجع الملحق (ج) للحصول على أوامر استكشاف الأخطاء وإصلاحها.

السيناريو 2: تطبيق Active Directory باستخدام عضوية المجموعة للسماح بالوصول أو رفضه

يستخدم هذا المثال تعيين عضو سمة LDAP لسمة بروتوكول الاتصال النفقي لإنشاء عضوية مجموعة كشرط. لكي تنجح هذه السياسة، يجب أن تتوفر لديك هذه الشروط:

- استخدم مجموعة موجودة بالفعل أو قم بإنشاء مجموعة جديدة لمستخدمي ASA VPN ليكونوا عضوا في شروط السماح.
- استخدم مجموعة موجودة بالفعل أو قم بإنشاء مجموعة جديدة لمستخدمي غير ASA لتكون عضوا في شروط الرفض.
- تأكد من إيداع عارض LDAP الذي يتوفر لديك DN الصحيح للمجموعة. انظر الملحق د. إن يكون ال DN خطأ، ال يخطط لا يعمل بشكل صحيح.

ملاحظة: اعلم أنه يمكن ل ASA قراءة السلسلة الأولى من السمة memberOf فقط في هذا الإصدار. تأكد من أن المجموعة الجديدة التي تم إنشاؤها موجودة في أعلى القائمة. الخيار الآخر هو أن تضع حرف خاص أمام الاسم عندما ينظر AD إلى الحروف الخاصة أولاً. للعمل حول هذا التحذير، استخدم DAP في برنامج x.8 للنظر في مجموعات متعددة.

ملاحظة: تأكد من أن المستخدم جزء من مجموعة الرفض أو على الأقل مجموعة أخرى بحيث يتم إرسال العضو مرة أخرى إلى ASA دائماً. لا يتوجب عليك تحديد شرط الرفض الكاذب ولكن أفضل ممارسة هي القيام بذلك. إذا كان اسم المجموعة الموجود أو اسم المجموعة يحتوي على مسافة، فأدخل السمة بهذه الطريقة:

CN=Backup Operators,CN=Builtin,DC=gsgseclab,DC=org

ملاحظة: يسمح DAP لمكتب المحاسبة المستقل بالنظر إلى مجموعات متعددة في السمة memberOf والتفويض الأساسي لهذه المجموعات. راجع قسم DAP.

رسم الخرائط

- قيمة سمة AD: عضو CN=AsauSers.CN=Users.DC=gsgseclab.DC=org
- قيمة سمة 1: Cisco = خطأ، 20 = true،
- من أجل شرط السماح، تقوم بالتعيين:

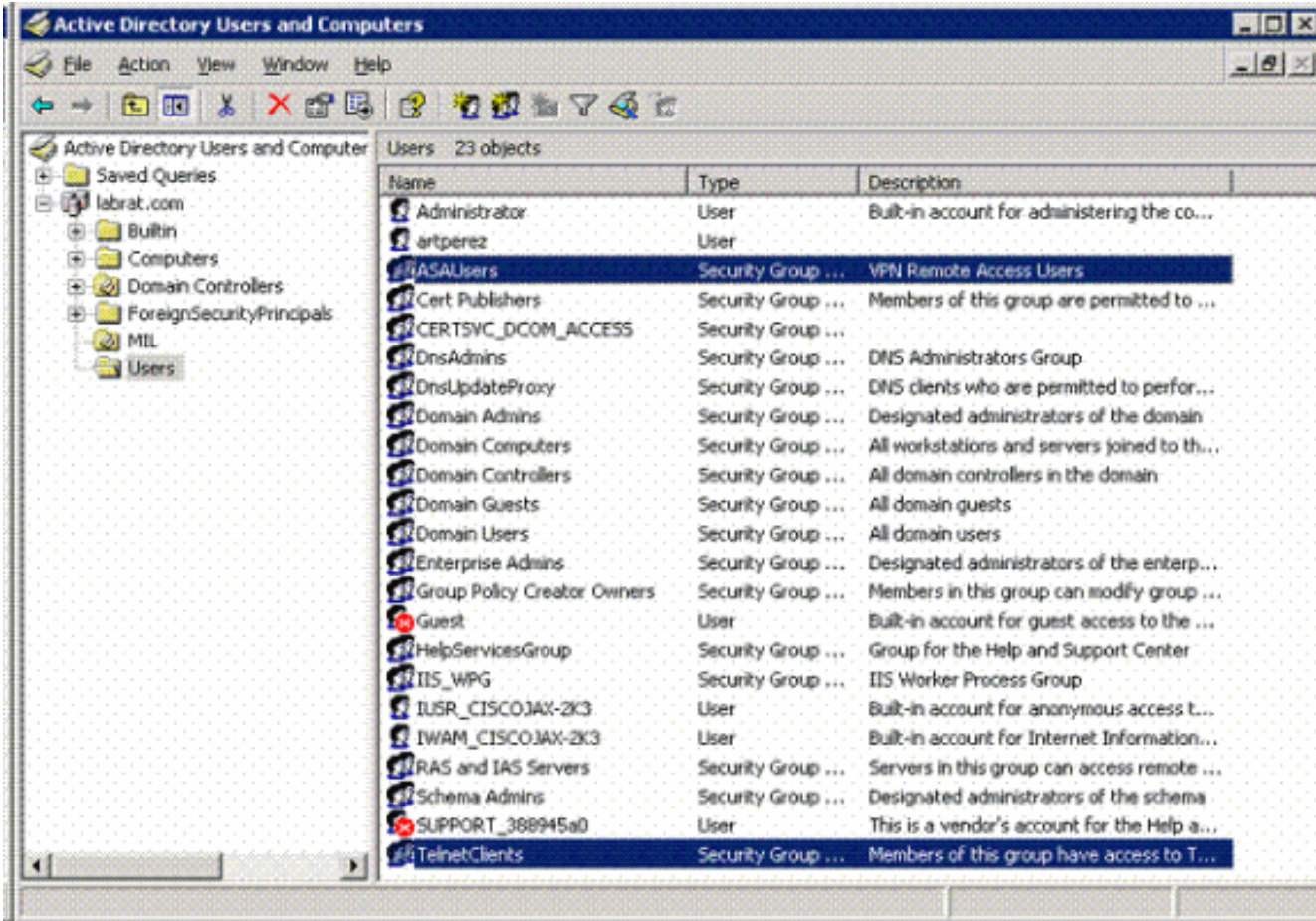
- عضو 20 = CN=AsauSers.CN=Users.DC=gsgseclab.DC=org
- بالنسبة لشرط الرفض، تقوم بتعيين:

- عضو 1 = CN=TelnetClient.CN=Users.DC=gsgseclab.DC=org

ملاحظة: في الإصدار المستقبلي، هناك سمة Cisco للسماح بالاتصال ورفضه. راجع [تكوين خادم خارجي لتفويض مستخدم جهاز الأمان](#) للحصول على مزيد من المعلومات حول سمات Cisco.

إعداد Active Directory

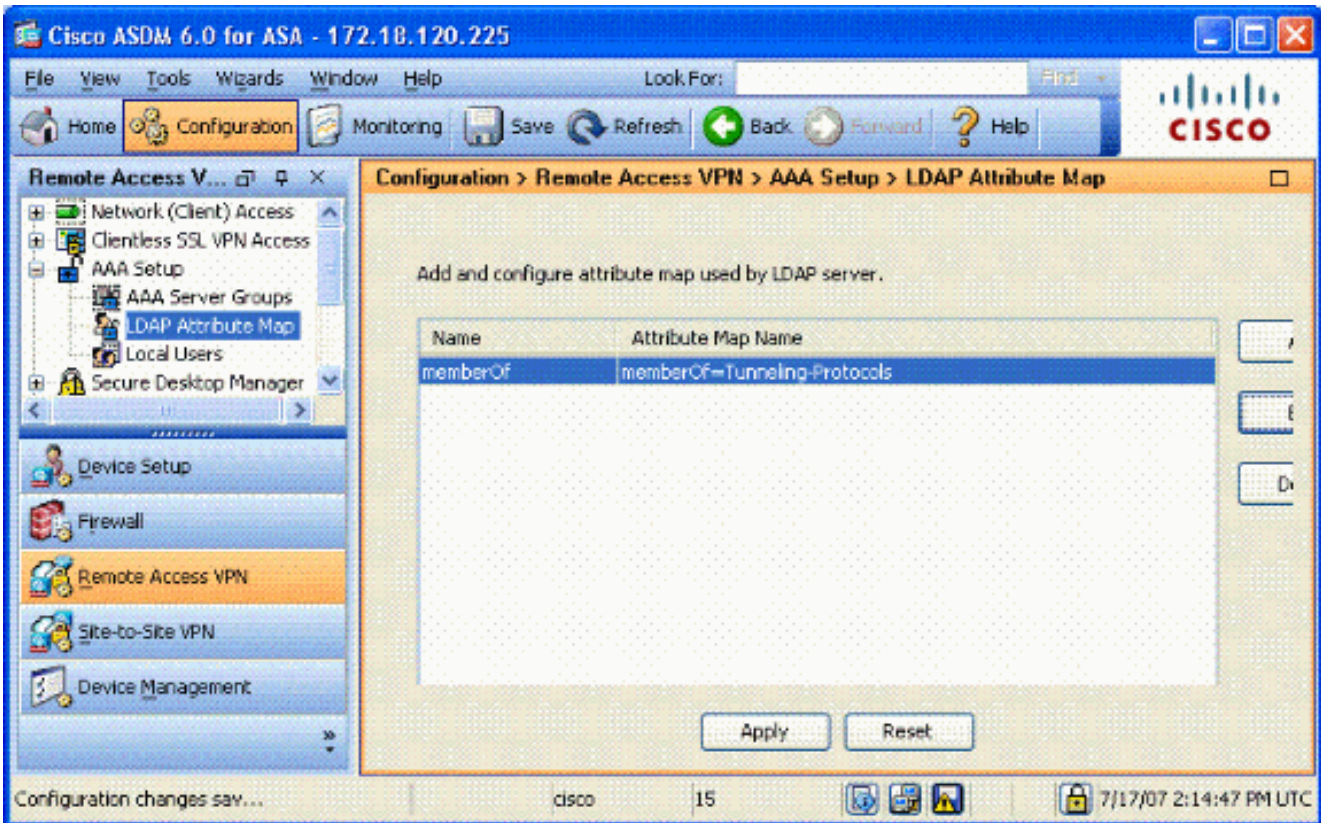
1. في خادم Active Directory، اختر ابدأ < تشغيل.
2. في مربع النص المفتوح، اكتب dsa.msc، ثم انقر موافق. يقوم هذا بتشغيل وحدة تحكم إدارة Active Directory.
3. في وحدة تحكم إدارة Active Directory، انقر فوق علامة الجمع لتوسيع Active Directory Users and Computers. انظر الشكل 8 أ الشكل 8A: مجموعات Active Directory



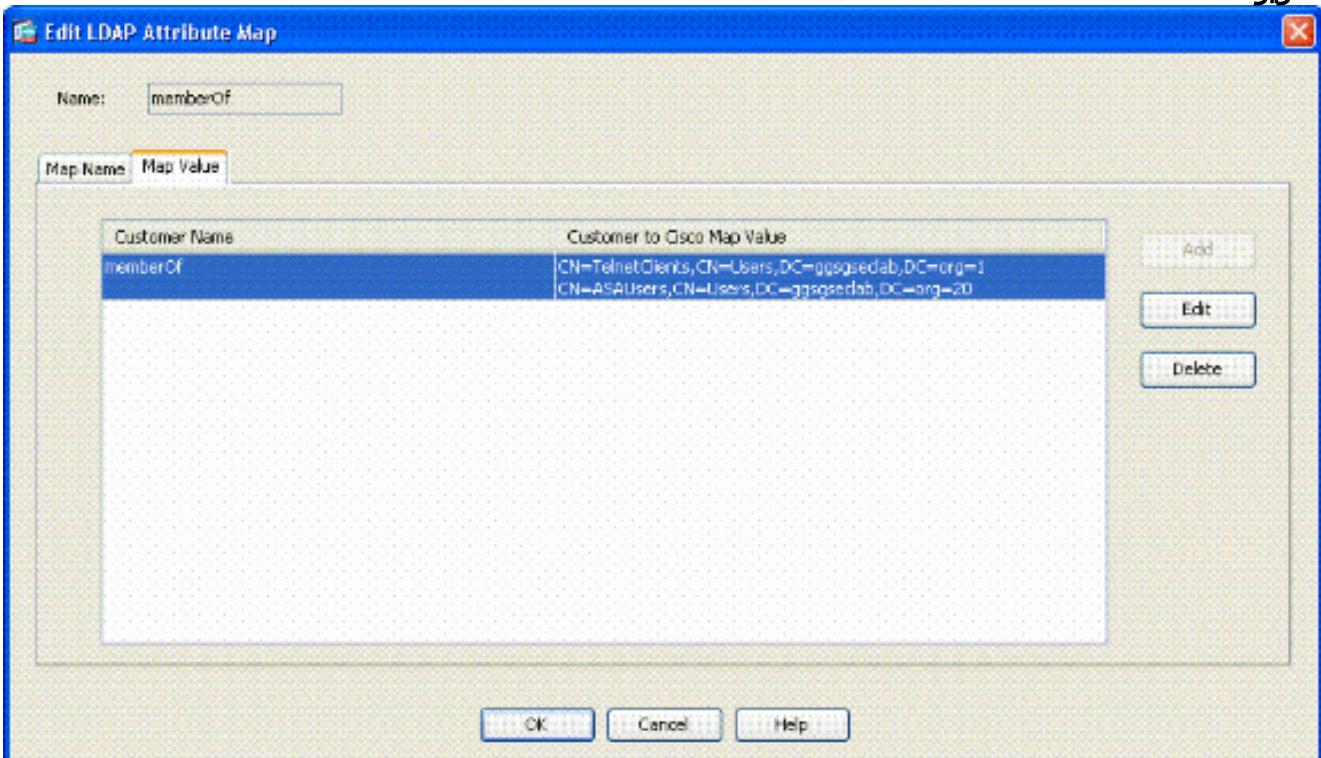
4. انقر فوق علامة الجمع لتوسيع اسم المجال.
5. انقر بزر الماوس الأيمن فوق المجلد **المستخدمون** واختر **جديد > مجموعة**.
6. أدخل اسم مجموعة. على سبيل المثال: **AsauSers**.
7. وانقر فوق **OK**.
8. انقر فوق المجلد **المستخدمون**، ثم انقر نقرا مزدوجا فوق المجموعة التي أنشأتها للتو.
9. أختار علامة التبويب **أعضاء**، ثم انقر فوق **إضافة**.
10. اكتب اسم المستخدم الذي تريد إضافته، ثم انقر فوق **موافق**.

تكوين ASA

1. في ASDM، أختار **Remote Access VPN (الوصول عن بعد) < إعداد AAA < خريطة سمة LDAP**.
2. انقر فوق **إضافة (Add)**.
3. في نافذة خريطة إضافة سمة LDAP، أكمل الخطوات التالية. انظر الشكل أ 3. أدخل اسما في مربع نص الاسم. في علامة التبويب "اسم الخريطة"، اكتب **عضو** في مربع النص "ج" الخاص ب "اسم العميل". في علامة التبويب اسم الخريطة، أختار **بروتوكولات الاتصال النقي** في الخيار المنسدل في اسم Cisco. أختار **إضافة**. انقر فوق علامة التبويب **تعيين قيمة**. أختار **إضافة**. في نافذة قيمة خريطة LDAP لسمة الإضافة، اكتب **cn=asauSers,cn=Users,dc=gsgseclab,dc=org** في مربع النص العميل و اكتب 20 في مربع نص قيمة Cisco. انقر فوق **إضافة (Add)**. اكتب **cn=telnetClient,cn=Users,dc=gsgseclab,dc=org** في مربع نص اسم العميل و اكتب 1 في مربع نص قيمة Cisco. راجع الشكل أ 4. وانقر فوق **OK**. وانقر فوق **OK**. طقطقة **يطبق**. يجب أن يبدو التكوين مثل الشكل A9. شكل A9 LDAP سمة **تعيين**



4. أختبر إعداد AAA للوصول عن بعد VPN < مجموعات خوادم AAA.
5. انقر فوق مجموعة الخوادم التي تريد تحريرها. في الخوادم الموجودة في قسم المجموعة المحددة، حدد عنوان IP الخاص بالخادم أو اسم المضيف، ثم انقر فوق تحرير



6. في نافذة Edit AAA Server، في مربع نص خريطة سمات LDAP، حدد خريطة سمات LDAP التي تم إنشاؤها في القائمة المنسدلة.
7. وانقر فوق OK.

ملاحظة: قم بتشغيل تصحيح LDAP بينما تقوم بالاختبار للتحقق من أن ربط LDAP وتعيينات السمات تعمل بشكل صحيح. راجع الملحق (ج) للحصول على أوامر استكشاف الأخطاء وإصلاحها.

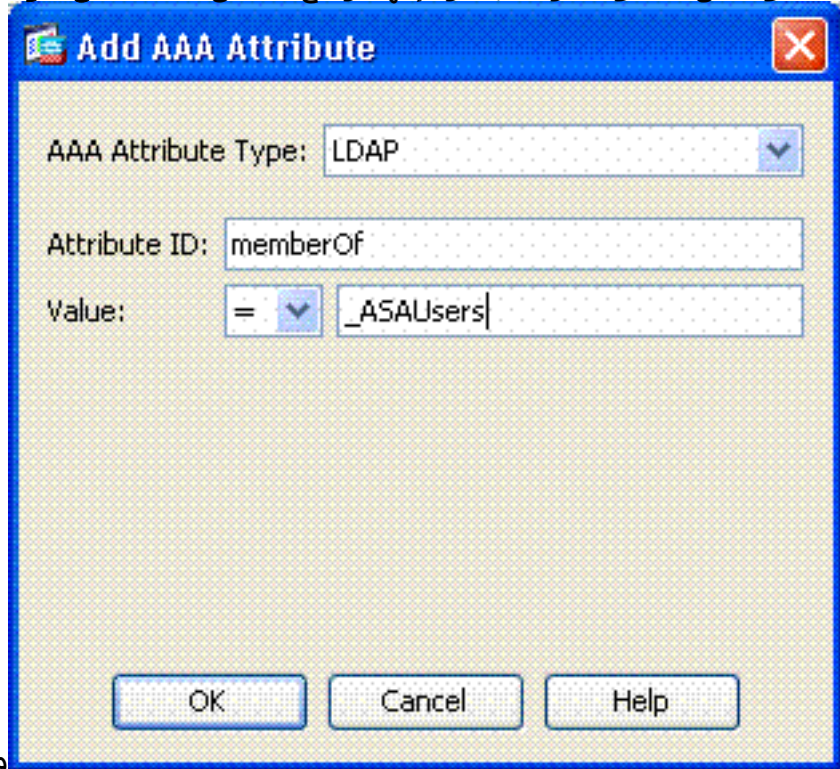
السيناريو 3: سياسات الوصول الديناميكي للعديد من سمات الأعضاء

يستخدم هذا المثال DAP للنظر في سمات أعضاء متعددين للسماح بالوصول بناء على عضوية مجموعة Active Directory. قبل x.8، كان ASA يقرأ أول سمة عضو فقط. مع x.8 والإصدارات الأحدث، يمكن أن يقوم ASA بالنظر إلى جميع سمات أعضاء Of.

- أستخدم مجموعة موجودة بالفعل أو قم بإنشاء مجموعة جديدة (أو مجموعات متعددة) لمستخدمي ASA VPN ليكونوا أعضاء في شروط السماح.
- أستخدم مجموعة موجودة بالفعل أو قم بإنشاء مجموعة جديدة لمستخدمي غير ASA لتكون عضوا في شروط الرفض.
- تأكد من إيداع عارض LDAP الذي يتوفر لديك DN الصحيح للمجموعة. انظر الملحق د. إن يكون ال DN خطأ، ال يخطط لا يعمل بشكل صحيح.

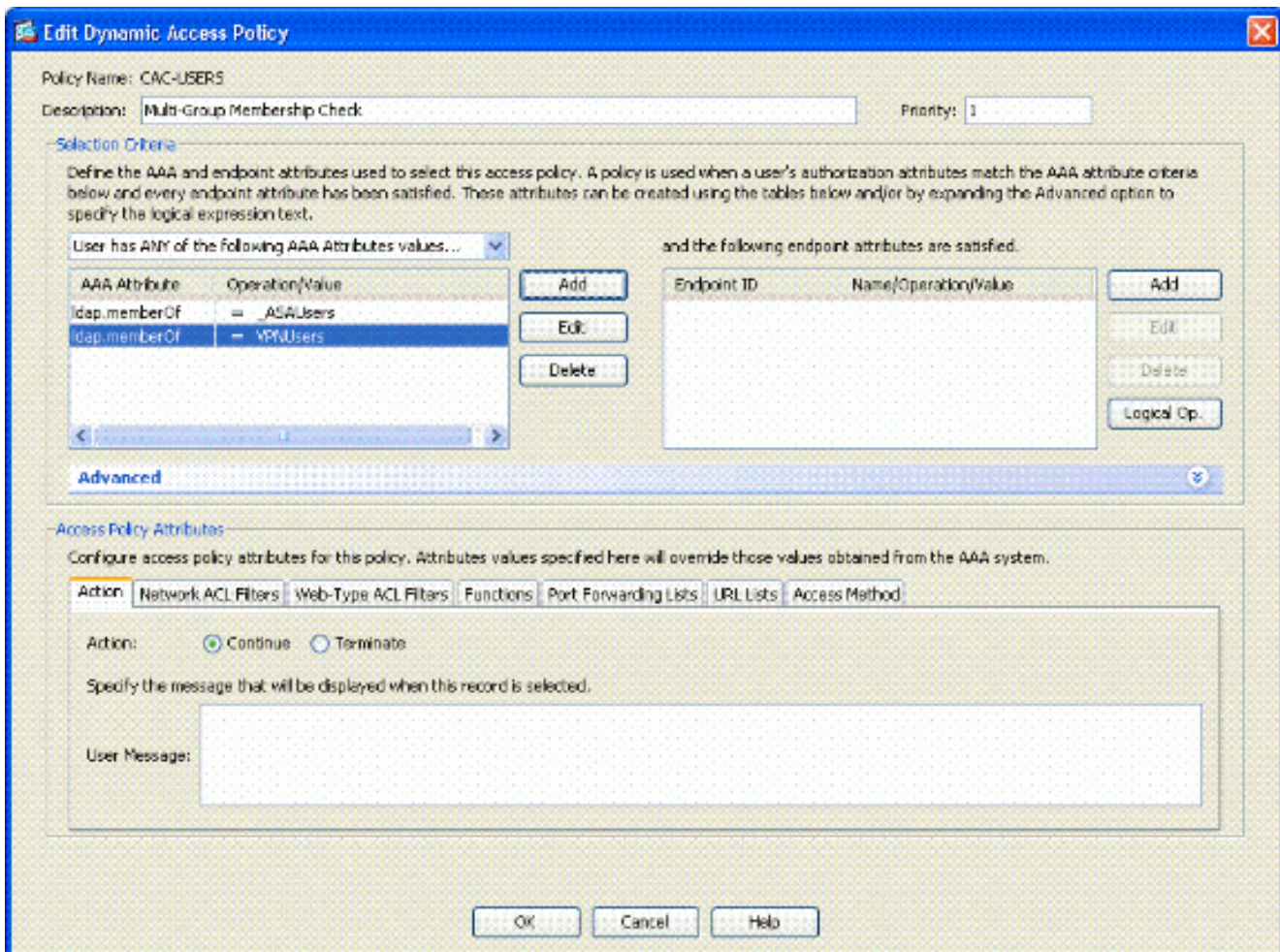
تكوين ASA

1. في ASDM، أختار الوصول عن بعد إلى شبكة VPN <(العميل) < سياسات الوصول الديناميكية.
2. انقر فوق إضافة (Add).
3. في نهج إضافة الوصول الديناميكي، أكمل الخطوات التالية: أدخل اسما في مربع نص الاسم ب. في قسم الأولوية، أدخل 1، أو رقم أكبر من 0. في فئة التحديد، انقر فوق إضافة. في سمة إضافة AAA، أختار LDAP. في قسم معرف السمة، أدخل memberOf. في قسم القيمة، أختار = وأدخل اسم مجموعة الإعلان. كرر هذه الخطوة لكل مجموعة تريد الإشارة إليها. راجع الشكل A10. شكل خريطة سمة AAA10



وانقر فوق OK. في قسم سمات نهج

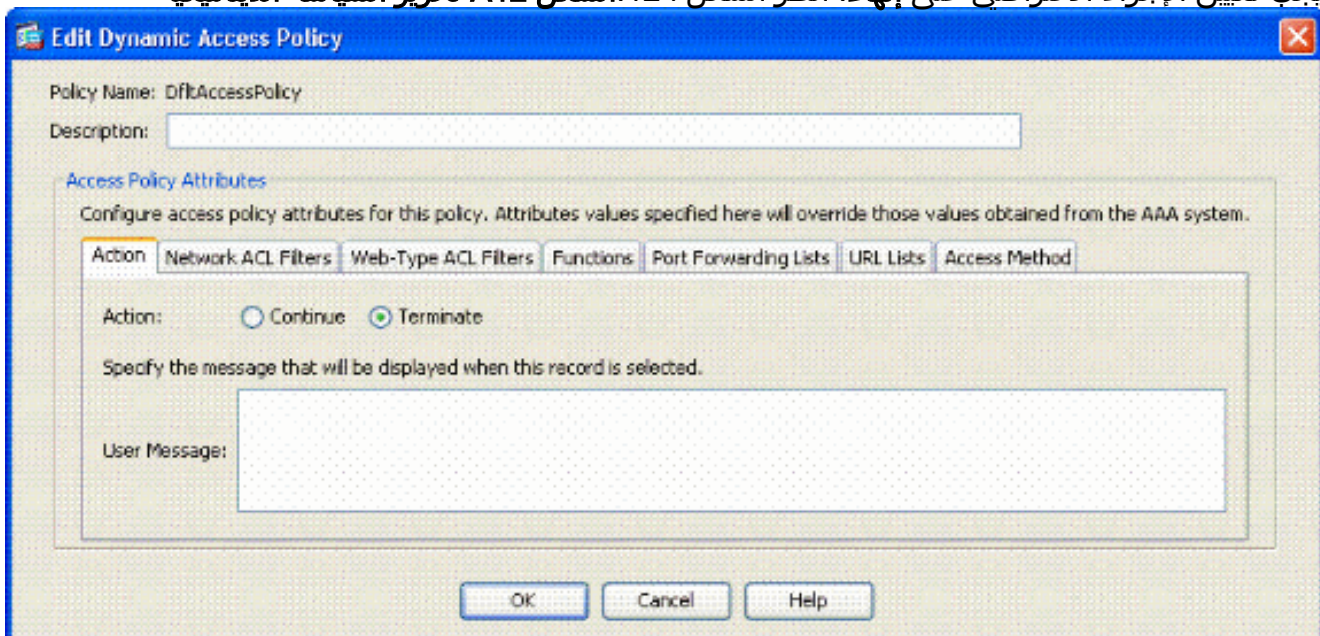
الوصول، أختار إستمرار. انظر الشكل أ 11. الشكل A11 إضافة سياسة ديناميكية



4. في ASDM، أختَر الوصول عن بعد إلى شبكة VPN <(العميل) < سياسات الوصول الديناميكية.

5. أختَر نهج الوصول الافتراضي واختر Edit (تحرير).

6. يجب تعيين الإجراء الافتراضي على إنهاء. انظر الشكل أ 12. الشكل A12 تحرير السياسة الديناميكية



7. وانقر فوق OK.

ملاحظة: إذا لم يتم تحديد إنهاء، يتم السماح لك بالدخول حتى إذا لم تكن في أي مجموعات لأن الافتراضي هو المتابعة.

[الملحق ب - تكوين ASA CLI](#)


```
ciscoasa#show running-config
Saved :
:
(ASA Version 8.0(2)
!
hostname asa80
domain-name army.mil
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address x.x.x.x 255.255.255.128
!
interface GigabitEthernet0/1
nameif inside
security-level 100
no ip address
!
boot system disk0:/asa802-k8.bin
ftp mode passive
dns server-group DefaultDNS
domain-name army.mil
!
-----ACL's-----
-----
access-list out extended permit ip any any
-----
-----
pager lines 24
logging console debugging
mtu outside 1500
!
-----VPN Pool-----
-----
ip local pool CAC-USERS 192.168.1.1-192.168.1.254 mask
255.255.255.0
-----
!
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400
access-group out in interface outside
route outside 0.0.0.0 0.0.0.0 172.18.120.129 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect
0:02:00
timeout uauth 0:05:00 absolute
!
-----LDAP Maps & DAP-----
-----
```

```

        ldap attribute-map memberOf
        map-name memberOf Tunneling-Protocols
March 11, 2008 ASA - CAC Authentication for AnyConnect
        VPN Access
Company Confidential. A printed copy of this document is
        .considered uncontrolled
        49
        map-value memberOf
CN=_ASAUsers,CN=Users,DC=gsgseclab,DC=org 20
        ldap attribute-map msNPAllowDialin
        map-name msNPAllowDialin Tunneling-Protocols
        map-value msNPAllowDialin FALSE 1
        map-value msNPAllowDialin TRUE 20
        dynamic-access-policy-record CAC-USERS
        "description "Multi-Group Membership Check
        priority 1
        dynamic-access-policy-record DfltAccessPolicy
        action terminate
-----
!
-----LDAP Server-----
-----
        aaa-server AD-LDAP protocol ldap
aaa-server AD-LDAP (outside) host 172.18.120.160
        ldap-base-dn CN=Users,DC=gsgseclab,DC=org
        ldap-scope onelevel
        ldap-naming-attribute userPrincipalName
        * ldap-login-password
        ldap-login-dn
CN=Administrator,CN=Users,DC=gsgseclab,DC=org
-----
!
        aaa authentication http console LOCAL
        http server enable 445
        http 0.0.0.0 0.0.0.0 outside
        no snmp-server location
        no snmp-server contact
snmp-server enable traps snmp authentication linkup
        linkdown coldstart
!
-----CA Trustpoints-----
-----
        crypto ca trustpoint ASDM_TrustPoint0
        revocation-check ocs
        enrollment terminal
        keypair DoD-1024
match certificate DefaultCertificateMap override ocs
        trustpoint
ASDM_TrustPoint5 10 url http://ocs.disa.mil
        crl configure
        crypto ca trustpoint ASDM_TrustPoint1
        revocation-check ocs
        enrollment terminal
        fqdn asa80
        subject-name CN=asa80,OU=PKI,OU=DoD,O=U.S.
        Government,C=US
        keypair DoD-1024
match certificate DefaultCertificateMap override ocs
        trustpoint
ASDM_TrustPoint5 10 url http://ocs.disa.mil
        no client-types
        crl configure

```

```
crypto ca trustpoint ASDM_TrustPoint2
    revocation-check oosp
    enrollment terminal
    keypair DoD-2048
match certificate DefaultCertificateMap override oosp
    trustpoint
    ASDM_TrustPoint5 10 url http://oosp.disa.mil
    no client-types
    crl configure
crypto ca trustpoint ASDM_TrustPoint3
    revocation-check oosp none
    enrollment terminal
    crl configure
!
```

-----Certificate Map-----

```
crypto ca certificate map DefaultCertificateMap 10
    " subject-name ne
CA Certificates (Partial Cert is-----
------(Shown
crypto ca certificate chain ASDM_TrustPoint0
    certificate ca 37
3082044c 30820334 a0030201 02020137 300d0609 2a864886
    f70d0101
    05050030
60310b30 09060355 04061302 55533118 30160603 55040a13
    0f552e53
    2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c
    300a0603
    55040b13
03504b49 311b3019 06035504 03131244 6f44204a 49544320
    526f6f74
crypto ca certificate chain ASDM_TrustPoint1
    certificate 319e
3082037a a0030201 02020231 9e300d06 092a8648 30820411
    86f70d01
    01050500
305c310b 30090603 55040613 02555331 18301606 0355040a
    130f552e
    532e2047
6f766572 6e6d656e 74310c30 0a060355 040b1303 446f4431
    0c300a06
    0355040b
crypto ca certificate chain ASDM_TrustPoint2
    certificate ca 37
3082044c 30820334 a0030201 02020137 300d0609 2a864886
    f70d0101
    05050030
60310b30 09060355 04061302 55533118 30160603 55040a13
    0f552e53
    2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c
    300a0603
    55040b13
f766e045 f15ddb43 9549d1e9 a0ea6814 b64bcece 089e1b6e
    1be959a5
    6fc20a76
crypto ca certificate chain ASDM_TrustPoint3
    certificate ca 05
a0030201 02020105 300d0609 2a864886 30820258 30820370
    f70d0101
    05050030
5b310b30 09060355 04061302 55533118 30160603 55040a13
```



```

0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c
300a0603
55040b13
03504b49 31163014 06035504 03130d44 6f442052 6f6f7420
43412032
301e170d
5a170d32 39313230 35313530 30303130 31333135 30343132
3031305a
305b310b
0355040a 130f552e 18301606 02555331 55040613 30090603
532e2047
6f766572
6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06
0355040b
1303504b
0403130d 446f4420 526f6f74 20434120 14060355 49311630
32308201
crypto ca certificate chain ASDM_TrustPoint4
certificate ca 04
308201d0 a0030201 02020104 300d0609 2a864886 30820267
f70d0101
05050030
61310b30 09060355 04061302 55533118 30160603 55040a13
0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c
300a0603
55040b13
03504b49 311c301a 06035504 03131344 6f442043 4c415353
20332052
6f6f7420
!
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
!
-----SSL/WEBVPN-----
-----
ssl certificate-authentication interface outside port

```

```

443
webvpn
enable outside
svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1
svc enable
tunnel-group-list enable
-----
-----VPN Group/Tunnel Policy-----
-----
group-policy CAC-USERS internal
ggroup-policy AC-USERS internal
group-policy AC-USERS attributes
vpn-tunnel-protocol svc
address-pools value CAC-USERS
webvpn
svc ask none default svc
tunnel-group AC-USERS type remote-access
tunnel-group AC-USERS general-attributes
authorization-server-group AD-LDAP
default-group-policy AC-USERS
authorization-required
authorization-dn-attributes UPN
tunnel-group AC-USERS webvpn-attributes
authentication certificate
group-alias AC-USERS enable
tunnel-group-map enable rules
no tunnel-group-map enable ou
no tunnel-group-map enable ike-id
no tunnel-group-map enable peer-ip
-----
-----
prompt hostname context

```

الملحق ج- استكشاف الأخطاء وإصلاحها

استكشاف أخطاء AAA و LDAP وإصلاحها

- **debug ldap 255** — يعرض تبادلات LDAP
- **debug aaa 10** — يعرض تبادلات AAA

المثال 1: الاتصال المسموح به مع تعيين السمة الصحيحة

يوضح هذا المثال إخراج **debug ldap** و **debug aaa** شائع أثناء اتصال ناجح بالسيناريو 2 الموضح في الملحق (أ).

```

الشكل C1: تصحيح أخطاء LDAP و debug aaa إخراج مشترك -
تعيين صحيح
AAA API: In aaa_open
AAA session opened: handle = 39
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type
0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
(Initiating authorization query (Svr Grp: AD-LDAP
-----

```

```
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
:Resp
Session Start [78]
New request Session, context 0x26f1c44, reqType = 0 [78]
Fiber started [78]
Creating LDAP context with uri=ldap:// [78]
172.18.120.160:389
Binding as administrator [78]
Performing Simple authentication for Administrator [78]
to
172.18.120.160
Connect to LDAP server: ldap:// 172.18.120.160, [78]
= status
Successful
:LDAP Search [78]
[Base DN = [CN=Users,DC=gsgseclab,DC=org
[Filter = [userPrincipalName=1234567890@mil
[Scope = [SUBTREE
:Retrieved Attributes [78]
objectClass: value = top [78]
objectClass: value = person [78]
objectClass: value = organizationalPerson [78]
objectClass: value = user [78]
cn: value = Ethan Hunt [78]
sn: value = Hunt [78]
= userCertificate: value [78]
H.....0@1.0.....&....,d.*...60...../.....50..0
.....com1.0
...d,...&
= userCertificate: value [78]
t.....50...*.H.....0@1.0.....&....,d./.....0'.0
.....com1.0
...d,...&
givenName: value = Ethan [78]
distinguishedName: value = CN=Ethan [78]
Hunt,OU=MIL,DC=labrat,DC=com
instanceType: value = 4 [78]
whenCreated: value = 20060613151033.0Z [78]
whenChanged: value = 20060622185924.0Z [78]
displayName: value = Ethan Hunt [78]
uSNCreated: value = 14050 [78]
memberOf: value = [78]
CN=ASAUUsers,CN=Users,DC=gsgseclab,DC=org
mapped to cVPN3000-Tunneling-Protocols: value = 20 [78]
uSNChanged: value = 14855 [78]
name: value = Ethan Hunt [78]
.objectGUID: value = ..9...NJ..GU..z [78]
userAccountControl: value = 66048 [78]
badPwdCount: value = 0 [78]
codePage: value = 0 [78]
countryCode: value = 0 [78]
badPasswordTime: value = 127954717631875000 [78]
lastLogoff: value = 0 [78]
lastLogon: value = 127954849209218750 [78]
pwdLastSet: value = 127946850340781250 [78]
primaryGroupID: value = 513 [78]
...objectSid: value = .....q.....mY [78]
accountExpires: value = 9223372036854775807 [78]
logonCount: value = 25 [78]
sAMAccountName: value = 1234567890 [78]
```



```

sAMAccountType: value = 805306368 [78]
userPrincipalName: value = 1234567890@mil [78]
= objectCategory: value [78]
mail: value = Ethan.Hunt@labrat.com [78]
= callback_aaa_task: status = 1, msg
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
Fiber exit Tx=147 bytes Rx=4821 bytes, status=1 [78]
Session End [78]
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
:Back End response
-----
(Authorization Status: 1 (ACCEPT
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE,
auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-
= LDAP, user pol
tunn pol = CAC-USERS ,
AAA_NextFunction: New i_fsm_state =
,IFSM_TUNN_GRP_POLICY
AAA FSM: In AAA_InitTransaction
(aaai_policy_name_to_server_id(CAC-USERS
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp:
(GROUP_POLICY_DB
-----
AAA FSM: In AAA_BindServer
<AAA_BindServer: Using server: <Internal Server
AAA FSM: In AAA_SendMsg
User: CAC-USER
:Pasw
:Resp
(grp_policy_ioctl(12f1b20, 114698, 1a870b4
grp_policy_ioctl: Looking up CAC-USERS
= callback_aaa_task: status = 1, msg
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
:Back End response
-----
(Tunnel Group Policy Status: 1 (ACCEPT
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY,
= auth_status
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-
= LDAP, user pol
tunn pol = CAC-USERS ,
,AAA_NextFunction: New i_fsm_state = IFSM_DONE
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user
1234567890@mil
AAA FSM: In AAA_Callback
:user attributes
Tunnelling-Protocol(4107) 20 20 1
:user policy attributes
None
:tunnel policy attributes
Primary-DNS(4101) 4 IP: 10.0.10.100 1

```

```

Secondary-DNS(4102) 4 IP: 0.0.0.0 2
Tunnelling-Protocol(4107) 4 4 3
"Default-Domain-Name(4124) 10 "ggsgseclab.org 4
List of address pools to assign addresses from(4313) 5
10
"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type
3
(In aaai_close_session (39
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
#CAC-Test

```

المثال 2: الاتصال المسموح به بتعيين سمة Cisco التي تم تكوينها بشكل غير منتظم

يوضح هذا المثال إخراج `debug ldap` و `debug aaa` شائع أثناء اتصال مسموح به مع السيناريو 2 الموضح في الملحق (أ).

الشكل C2: تصحيح أخطاء LDAP و debug aaa إخراج مشترك - تعيين غير صحيح

```

AAA API: In aaa_open
AAA session opened: handle = 41
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type
0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
(Initiating authorization query (Svr Grp: AD-LDAP
-----
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
:Resp
Session Start [82]
New request Session, context 0x26f1c44, reqType = 0 [82]
Fiber started [82]
Creating LDAP context with [82]
uri=ldap://172.18.120.160:389
Binding as administrator [82]
Performing Simple authentication for Administrator [82]
to
172.18.120.160
Connect to LDAP server: ldap:// 172.18.120.160:389, [82]
= status
Successful
:LDAP Search [82]
[Base DN = [CN=Users,DC=ggsgseclab,DC=org
[Filter = [userPrincipalName=1234567890@mil
[Scope = [SUBTREE
:Retrieved Attributes [82]
objectClass: value = top [82]
objectClass: value = person [82]
objectClass: value = organizationalPerson [82]
objectClass: value = user [82]
cn: value = Ethan Hunt [82]

```

```

sn: value = Hunt [82]
= userCertificate: value [82]
H.....0@1.0.....&....,d.*...60...../.....50..0
.....com1.0
...d,...&
= userCertificate: value [82]
t.....50...*.H.....0@1.0.....&....,d./.....0'.0
.....com1.0
...d,...&
givenName: value = Ethan [82]
distinguishedName: value = CN=Ethan [82]
Hunt,OU=MIL,DC=labrat,DC=com
instanceType: value = 4 [82]
whenCreated: value = 20060613151033.0Z [82]
whenChanged: value = 20060622185924.0Z [82]
displayName: value = Ethan Hunt [82]
uSNCreated: value = 14050 [82]
memberOf: value = [82]
CN=ASAUUsers,CN=Users,DC=ggsgseclab,DC=org
= mapped to cVPN3000-Tunneling-Protocols: value [82]
CN=ASAUUsers,CN=Users,DC=ggsgseclab,DC=org
uSNChanged: value = 14855 [82]
name: value = Ethan Hunt [82]
.objectGUID: value = ..9...NJ..GU..z [82]
userAccountControl: value = 66048 [82]
badPwdCount: value = 0 [82]
codePage: value = 0 [82]
countryCode: value = 0 [82]
badPasswordTime: value = 127954717631875000 [82]
lastLogoff: value = 0 [82]
lastLogon: value = 127954849209218750 [82]
pwdLastSet: value = 127946850340781250 [82]
primaryGroupID: value = 513 [82]
...objectSid: value = .....q.....mY [82]
accountExpires: value = 9223372036854775807 [82]
logonCount: value = 25 [82]
sAMAccountName: value = 1234567890 [82]
sAMAccountType: value = 805306368 [82]
userPrincipalName: value = 1234567890@mil [82]
= objectCategory: value [82]
CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=org
g
mail: value = Ethan.Hunt@labrat.com [82]
= callback_aaa_task: status = 1, msg
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
Fiber exit Tx=147 bytes Rx=4821 bytes, status=1 [82]
Session End [82]
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
:Back End response
-----
(Authorization Status: 1 (ACCEPT
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE,
auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-
= LDAP, user pol
tunn pol = CAC-USERS ,
AAA_NextFunction: New i_fsm_state =
,IFSM_TUNN_GRP_POLICY
AAA FSM: In AAA_InitTransaction
(aai_policy_name_to_server_id(USAFE

```



```

Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp:
(GROUP_POLICY_DB
-----
AAA FSM: In AAA_BindServer
<AAA_BindServer: Using server: <Internal Server
AAA FSM: In AAA_SendMsg
User: CAC-USERS
:Pasw
:Resp
(grp_policy_ioctl(12f1b20, 114698, 1a870b4
grp_policy_ioctl: Looking up CAC-USERS
= callback_aaa_task: status = 1, msg
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcB = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
:Back End response
-----
(Tunnel Group Policy Status: 1 (ACCEPT
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY,
= auth_status
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-
= LDAP, user pol
tunn pol = CAC-USERS ,
,AAA_NextFunction: New i_fsm_state = IFSM_DONE
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user
1234567890@mil
AAA FSM: In AAA_Callback
:user attributes
Tunnelling-Protocol(4107) 20 0 1
:user policy attributes
None
:tunnel policy attributes
Primary-DNS(4101) 4 IP: 10.0.10.100 1
Secondary-DNS(4102) 4 IP: 0.0.0.0 2
Tunnelling-Protocol(4107) 4 4 3
"Default-Domain-Name(4124) 10 "ggsgseclab.org 4
List of address pools to assign addresses from(4313) 5
10
"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type
3
(In aaai_close_session (41
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop

```

أستكشاف أخطاء DAP وإصلاحها

- تصحيح أخطاء DAP—يعرض أخطاء DAP
- debug dap trace—يعرض تتبع وظيفة DAP

مثال 1: الاتصال المسموح به مع DAP

يوضح هذا المثال إخراج أخطاء تصحيح الأخطاء و debug dap trace أثناء اتصال ناجح بالسيناريو 3 الموضح في الملحق أ. لاحظ العديد من سمات الأعضاء. يمكنك الانضمام إلى كل من ASAUsers و VPNUsers أو tp أي من المجموعتين، والتي تعتمد على تكوين ASA.

شكل debug dap c3:

```
debug dap errors#
debug dap errors enabled at level 1
debug dap trace#
debug dap trace enabled at level 1
#
The DAP policy contains the following attributes for
:user
mil@1241879298
-----
-----
---
action = continue :1
DAP_TRACE: DAP_open: C8EEFA10
DAP_TRACE: Username: 1241879298@mil,
aaa ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil,
aaa ldap.objectClass.2 = person
DAP_TRACE: Username: 1241879298@mil,
= aaa ldap.objectClass.3
organizationalPerson
DAP_TRACE: Username: 1241879298@mil,
aaa ldap.objectClass.4 = user
DAP_TRACE: Username: 1241879298@mil, aaa ldap.cn =
1241879298
,DAP_TRACE: Username: 1241879298@mil
aaa ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa ldap.givenName
= 1241879298
DAP_TRACE: Username: 1241879298@mil,
= aaa ldap.distinguishedName
CN=1241879298,CN=Users,DC=ggsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil,
aaa ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil,
= aaa ldap.whenCreated
20070626163734.0Z
DAP_TRACE: Username: 1241879298@mil,
= aaa ldap.whenChanged
20070718151143.0Z
DAP_TRACE: Username: 1241879298@mil,
aaa ldap.displayName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa ldap.uSNCreated
= 33691
DAP_TRACE: Username: 1241879298@mil, aaa ldap.memberOf.1
= VPNUsers
DAP_TRACE: Username: 1241879298@mil, aaa ldap.memberOf.2
= _ASAUsers
DAP_TRACE: Username: 1241879298@mil, aaa ldap.uSNChanged
= 53274
DAP_TRACE: Username: 1241879298@mil, aaa ldap.department
= NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa ldap.name =
1241879298
DAP_TRACE: Username: 1241879298@mil, aaa ldap.objectGUID
=
....F..5..+....
```

```
DAP_TRACE: Username: 1241879298@mil,
           = aaa.ldap.userAccountControl
           328192
DAP_TRACE: Username: 1241879298@mil,
           aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage =
           0
DAP_TRACE: Username: 1241879298@mil,
           aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil,
           aaa.ldap.badPasswordTime = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff
           = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon
           = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet
           =
           128273494546718750
DAP_TRACE: Username: 1241879298@mil,
           aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil,
           :aaa.ldap.userParameters = m
           .d
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid
           .. =
DAP_TRACE: Username: 1241879298@mil,
           = aaa.ldap.accountExpires
           9223372036854775807
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount
           = 0
DAP_TRACE: Username: 1241879298@mil,
           = aaa.ldap.sAMAccountName
           1241879298
DAP_TRACE: Username: 1241879298@mil,
           = aaa.ldap.sAMAccountType
           805306368
DAP_TRACE: Username: 1241879298@mil,
           = aaa.ldap.userPrincipalName
           mil@1241879298
DAP_TRACE: Username: 1241879298@mil,
           = aaa.ldap.objectCategory
CN=Person,CN=Schema,CN=Configuration,DC=gsgseclab,DC=or
g
DAP_TRACE: Username: 1241879298@mil,
           aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username
           =
           mil@1241879298
DAP_TRACE: Username: 1241879298@mil,
           aaa.cisco.tunnelgroup = CAC-USERS
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] =
           ;"top"
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2
           ;"person"
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3
           ;"organizationalPerson"
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4
           ;"user"
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] =
           ;"1241879298
```



```

: DAP_TRACE
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeN
= ["ame
; "NETADMIN"
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"]
; "= "1241879298
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["distinguishedName
; "CN=1241879298,CN=Users,DC=gsgseclab,DC=org"
DAP_TRACE:
; "dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["whenCreated
; "20070626163734.0Z"
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["whenChanged
; "20070718151143.0Z"
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["displayName
; "1241879298"
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"]
; "= "33691
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["memberOf"] ["1
; "VPNUsers"
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["memberOf"] ["2
; "ASAUsers_"
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"]
; "= "53274
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"]
; "= "NETADMIN
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] =
; "1241879298
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"]
contains
binary data
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["userAccountControl
; "328192"
DAP_TRACE:
; "dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] =
; "0
DAP_TRACE:
; "dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] =
; "0
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"]
; "= "0
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"]
; "= "0
["DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet
=
; "128273494546718750"
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] =
; "513
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userParameters"]
contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"]

```

```

contains binary
data
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]]["accountExpires
; "9223372036854775807"
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"] ["logonCount"]
; "0"
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]]["sAMAccountName
; "1241879298"
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]]["sAMAccountType
; "805306368"
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]]["userPrincipalName
; "mil@1241879298"
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]]["objectCategory
CN=Person,CN=Schema,CN=Configuration,DC=gsgseclab,DC=o"
; "rg"
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"] ["msNPAllowDialin"] =
; "TRUE"
["DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]]["username
=
; "mil@1241879298"
DAP_TRACE:
dap_add_to_lua_tree:aaa["cisco"] ["tunnelgroup"] =
; "CACUSERS"
DAP_TRACE:
"dap_add_to_lua_tree:endpoint["application"] ["clienttype
= [
; "IPSec"
DAP_TRACE: Username: 1241879298@mil, Selected DAPs: CAC-
USERS
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 1 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr:
rec_count = 1
DAP_TRACE: Username: 1241879298@mil, DAP_close: C8EEFA10
.d

```

المثال 2: رفض الاتصال ب DAP

يوضح المثال التالي إخراج أخطاء DAP و debug dap trace أثناء اتصال غير ناجح بالسيناريو 3 الموضح في الملحق أ.

الشكل C4: تصحيح الأخطاء DAP

```

debug dap errors#
debug dap errors enabled at level 1
debug dap trace#
debug dap trace enabled at level 1
#
The DAP policy contains the following attributes for
:user
mil@1241879298
-----
-----
-----
action = terminate :1

```

```
DAP_TRACE: DAP_open: C91154E8
DAP_TRACE: Username: 1241879298@mil,
    aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil,
    aaa.ldap.objectClass.2 = person
DAP_TRACE: Username: 1241879298@mil,
    = aaa.ldap.objectClass.3
        organizationalPerson
DAP_TRACE: Username: 1241879298@mil,
    aaa.ldap.objectClass.4 = user
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn =
    1241879298
    ,DAP_TRACE: Username: 1241879298@mil
    aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName
    = 1241879298
DAP_TRACE: Username: 1241879298@mil,
    = aaa.ldap.distinguishedName
    CN=1241879298,CN=Users,DC=ggsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil,
    aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil,
    = aaa.ldap.whenCreated
    20070626163734.0Z
DAP_TRACE: Username: 1241879298@mil,
    = aaa.ldap.whenChanged
    20070718151143.0Z
DAP_TRACE: Username: 1241879298@mil,
    aaa.ldap.displayName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNCreated
    = 33691
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf =
    DnsAdmins
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged
    = 53274
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.department
    = NETADMIN
    DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name =
    1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID
    =
    ....F.."5..+....
DAP_TRACE: Username: 1241879298@mil,
    = aaa.ldap.userAccountControl
    328192
DAP_TRACE: Username: 1241879298@mil,
    aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage =
    0
DAP_TRACE: Username: 1241879298@mil,
    aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil,
    aaa.ldap.badPasswordTime = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff
    = 0
    DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon
    = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet
    =
    128273494546718750
DAP_TRACE: Username: 1241879298@mil,
    aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil,
    :aaa.ldap.userParameters = m
```



```
.d
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid
.. =
DAP_TRACE: Username: 1241879298@mil,
= aaa.ldap.accountExpires
9223372036854775807
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount
= 0
DAP_TRACE: Username: 1241879298@mil,
= aaa.ldap.sAMAccountName
1241879298
DAP_TRACE: Username: 1241879298@mil,
= aaa.ldap.sAMAccountType
805306368
DAP_TRACE: Username: 1241879298@mil,
= aaa.ldap.userPrincipalName
mil@1241879298
DAP_TRACE: Username: 1241879298@mil,
= aaa.ldap.objectCategory
CN=Person,CN=Schema,CN=Configuration,DC=gsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username
=
mil@1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.cisco.tunnelgroup = CAC-USERS
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] =
; "top"
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2
; "person"
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3
; "organizationalPerson"
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4
; "user"
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] =
; "1241879298
: DAP_TRACE
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeN
= [ "ame
; "NETADMIN"
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"]
; " = "1241879298
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["distinguishedName
; "CN=1241879298,CN=Users,DC=gsgseclab,DC=org"
DAP_TRACE:
; "dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["whenCreated
; "20070626163734.0Z"
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["whenChanged
; "20070718151143.0Z"
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["displayName
; "1241879298"
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"]
; " = "33691
```

```
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"] =
; "DnsAdmins"
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"]
; "= 53274"
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"]
; "= NETADMIN"
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] =
; "1241879298"
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"]
contains
binary data
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"]
; "328192"
DAP_TRACE:
; "dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0"
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] =
; "0"
DAP_TRACE:
; "dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0"
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] =
; "0"
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"]
; "= 0"
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"]
; "= 0"
["DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"]
=
; "128273494546718750"
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] =
; "513"
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userParameters"]
contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"]
contains binary
data
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["accountExpires"]
; "9223372036854775807"
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"]
; "= 0"
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"]
; "1241879298"
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"]
; "805306368"
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"]
; "mil@1241879298"
DAP_TRACE:
= ["dap_add_to_lua_tree:aaa["ldap"]["objectCategory"]
CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=o"
; "rg"
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] =
; "TRUE"
["DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"]
=
; "mil@1241879298"
```

```
:DAP_TRACE: Username: 1241879298@mil, Selected DAPs
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 0 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr:
rec_count = 1
```

هيئة شهادة أكتشاف الأخطاء وإصلاحها / OCSP

• debug crypto ca 3

• في وضع التكوين—تصحيح أخطاء وحدة تحكم CA للفتنة (أو المخزن المؤقت) للتسجيل تظهر هذه الأمثلة التحقق من صحة الشهادة بنجاح باستخدام مستجيب OCSP ونهج مطابقة مجموعة الشهادات الفاشلة.

يوضح الشكل C3 إخراج تصحيح الأخطاء الذي يحتوي على شهادة تم التحقق من صحتها ومجموعة شهادات عاملة تطابق النهج.

الشكل C4 يوضح إخراج تصحيح الأخطاء لنهج مطابقة مجموعة شهادات تم تكوينها بشكل غير صحيح.

يوضح الشكل C5 إخراج تصحيح الأخطاء لمستخدم بشهادة ملغاة.

الشكل C5: تصحيح أخطاء OCSP - التحقق من الشهادة بنجاح

```
CRYPTO_PKI: Found a suitable authenticated trustpoint
               .ASDM_TrustPoint11
CRYPTO_PKI: Allocated OCSP data handle 0xca2d27b8
CRYPTO_PKI: Certificate validation: Successful, status:
               0. Attempting
               to retrieve revocation status if necessary
CRYPTO_PKI: status = 0: poll revocation status
CRYPTO_PKI: Attempting to find OCSP override for peer
               cert: serial
               :number: 0F192B, subject name
               .cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S
               -Government,c=US, issuer_name: cn=DOD JITC EMAIL CA
               .ou=PKI,ou=DoD,o=U.S. Government,c=US,15
               .CRYPTO_PKI: Processing map rules for SSL
               ...CRYPTO_PKI: Processing map SSL sequence 20
CRYPTO_PKI: Match of subject-name field to map PASSED.
               :Peer cert field
               =
               .cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S
               ." Government,c=US, map rule: subject-name ne
CRYPTO_PKI: Peer cert has been authorized by map: SSL
               .sequence: 20
               :CRYPTO_PKI: Found OCSP override match. Override URL
               http://198.154.68.90, Override trustpoint:
               ASDM_TrustPoint12
               ()CRYPTO_PKI: crypto_pki_get_cert_record_by_subject
CRYPTO_PKI: Destroying OCSP data handle 0xca2d27b8
               !Crypto CA thread sleeps
CRYPTO_PKI: Attempting to find tunnel group for cert
               with serial
               :number: 0F192B, subject name
               .cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S
               -Government,c=US, issuer_name: cn=DOD JITC EMAIL CA
               .ou=PKI,ou=DoD,o=U.S. Government,c=US,15
               CRYPTO_PKI: Processing map rules for
               .DefaultCertificateMap
```



```

CRYPTO_PKI: Processing map DefaultCertificateMap
...sequence 10
CRYPTO_PKI: Match of subject-name field to map PASSED.
:Peer cert field
=
.cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S
." Government,c=US, map rule: subject-name ne
CRYPTO_PKI: Peer cert has been authorized by map:
DefaultCertificateMap
.sequence: 10
CRYPTO_PKI: Ignoring match on map DefaultCertificateMap,
index 10 for
WebVPN group map processing. No tunnel group is
.configured
:CRYPTO_PKI: Peer cert could not be authorized with map
.DefaultCertificateMap
.CRYPTO_PKI: Processing map rules for SSL
...CRYPTO_PKI: Processing map SSL sequence 20
CRYPTO_PKI: Match of subject-name field to map PASSED.
:Peer cert field
=
.cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S
." Government,c=US, map rule: subject-name ne
CRYPTO_PKI: Peer cert has been authorized by map: SSL
.sequence: 20
CRYPTO_PKI: Ignoring match on map SSL, index 20 for
WebVPN group map

```

الشكل C5: إخراج نهج مطابقة مجموعة الشهادات الفاشلة

الشكل جيم5: إخراج شهادة ملغاة

```

n %PI=X-3-7E17t02h7a Certinf icaHtue cnhta,in faioled
.=validation
CMertifiIcLa,ted ccha=inl ais eibtrhaer tin,validid cor
=noct
.oamuthori,zed
." map rule: subject-name ne
CRYPTO_PKI: Peer cert has been authorized by map:
DefaultCertificateMap
.sequence: 10
Tunnel Group Match on map DefaultCertificateMap sequence
.# 10
Group name is CAC-USERS
CRYPTO_PKI: Checking to see if an identical cert is
...already in the database
=CRYPTO_PKI: looking for cert in handle=2467668, digest
CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
.CRYPTO_PKI: Cert not found in database
...CRYPTO_PKI: Looking for suitable trustpoints
CRYPTO_PKI: Found a suitable authenticated trustpoint
.trustpoint0
CRYPTO_PKI: Certificate validation: Successful, status:
0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: Attempting to find OCSP override for peer
cert: serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
:Hunt,ou=MIL,dc=gsgseclab,dc=org, issuer_name
.cn=gsgseclab,dc=gsgseclab,dc=org
CRYPTO_PKI: Processing map rules for
.DefaultCertificateMap

```

```
CRYPTO_PKI: Processing map DefaultCertificateMap
...sequence 10
CRYPTO_PKI: Match of subject-name field to map PASSED.
:Peer cert field
cn=Ethan Hunt,ou=MIL,dc=gsgseclab,dc=org, map rule: =
subject-name
." ne
CRYPTO_PKI: Peer cert has been authorized by map:
DefaultCertificateMap
.sequence: 10
:CRYPTO_PKI: Found OCSP override match. Override URL
http://ocsp.disa.mil, Override trustpoint: OCSP
()CRYPTO_PKI: crypto_pki_get_cert_record_by_subject
CRYPTO_PKI: Found a subject match
ERROR: Certificate validation failed, Certificate is
revoked, serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
Hunt,ou=MIL,dc=gsgseclab,dc=org
CRYPTO_PKI: Certificate not validated
```

الملحق د - التحقق من كائنات LDAP في MS

في القرص المضغوط الخاص بـ Microsoft Server 2003، هناك أدوات إضافية يمكن تثبيتها لعرض بنية LDAP وكذلك كائنات/سمات LDAP. لتثبيت هذه الأدوات، انتقل إلى دليل الدعم في القرص المضغوط ثم الأدوات. تثبيت .SUPTOOLS.MSI

عارض LDAP

- بعد التثبيت، أختبر بدء < تشغيل.
- اكتب ldp، ثم انقر موافق. يقوم هذا بتشغيل عارض LDAP.
- أختبر توصيل < توصيل.
- أدخل اسم الخادم ثم انقر فوق موافق.
- أختبر توصيل < ربط.
- أدخل اسم مستخدم وكلمة مرور. ملاحظة: تحتاج إلى حقوق المسؤول.
- وانقر فوق OK.
- عرض كائنات LDAP. راجع الشكل D1. الشكل D1: عارض LDAP

The screenshot shows an LDAP browser window with the following content:

Left Panel (Directory Structure):

- DC=labrat,DC=com
 - CN=Builtin,DC=labrat,DC=com
 - CN=Computers,DC=labrat,DC=com
 - OU=Domain Controllers,DC=labrat,DC=com
 - CN=ForeignSecurityPrincipals,DC=labrat,DC=com
 - CN=Infrastructure,DC=labrat,DC=com
 - CN=LostAndFound,DC=labrat,DC=com
 - OU=MIL,DC=labrat,DC=com
 - CN=Clark Kent,OU=MIL,DC=labrat,DC=com
 - No children
 - CN=Ethan Hunt,OU=MIL,DC=labrat,DC=com
 - CN=Peter Parker,OU=MIL,DC=labrat,DC=com
 - CN=NTDS Quotas,DC=labrat,DC=com
 - CN=Program Data,DC=labrat,DC=com
 - CN=System,DC=labrat,DC=com
 - CN=test,DC=labrat,DC=com
 - CN=Users,DC=labrat,DC=com
 - DC=ForestDnsZones,DC=labrat,DC=com
 - DC=DomainDnsZones,DC=labrat,DC=com
 - CN=Configuration,DC=labrat,DC=com

Right Panel (User Details):

Expanding base 'CN=Clark Kent,OU=MIL,DC=labrat,DC=com'...

Result <0>: [null]

Matched DN:

Getting 1 entries:

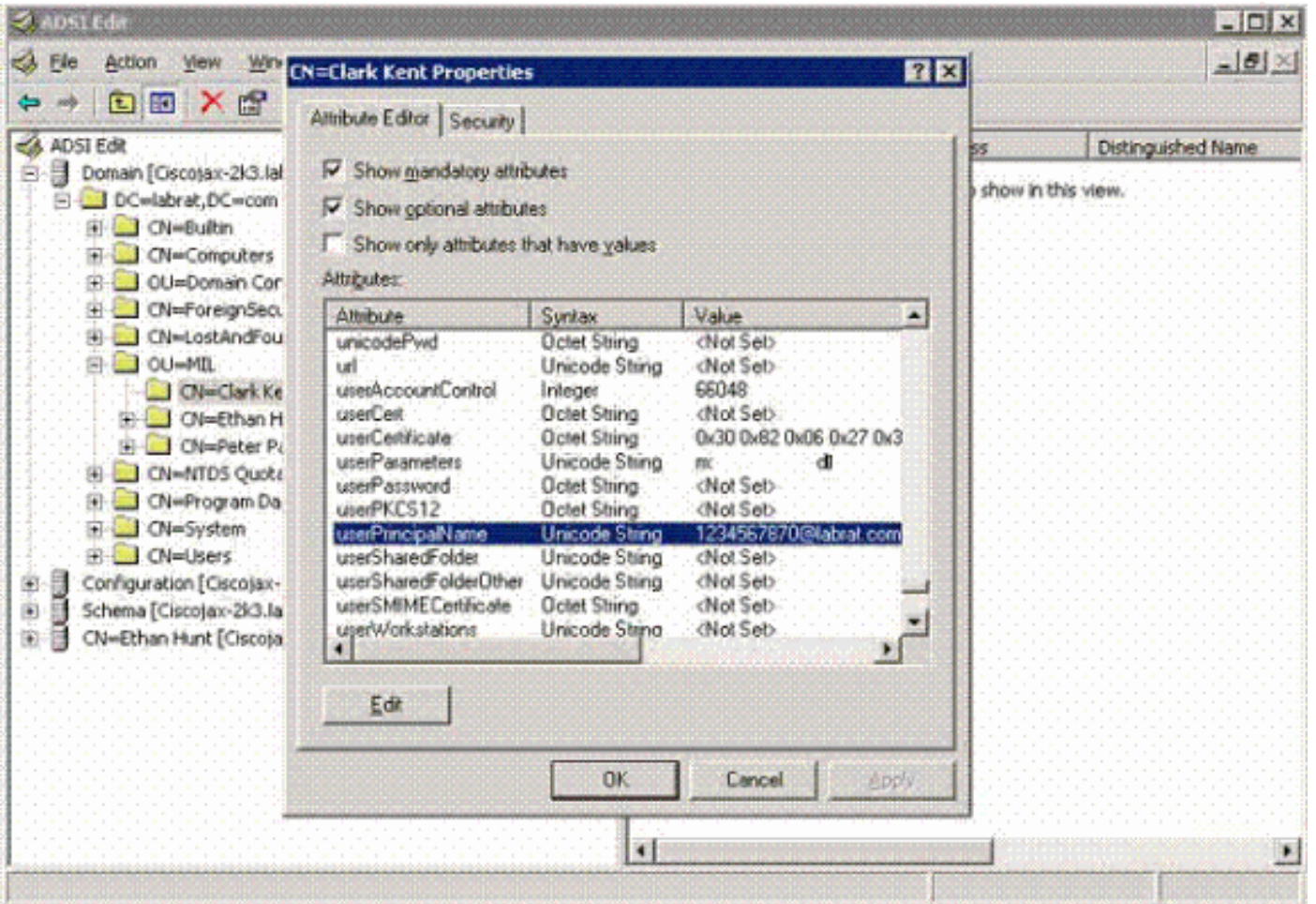
>> Dn: CN=Clark Kent,OU=MIL,DC=labrat,DC=com

- 4> objectClass: top; person; organizationalPerson; user;
- 1> cn: Clark Kent;
- 1> sn: Kent;
- 1> physicalDeliveryOfficeName: Welcome to LDAP!!!;
- 2> userCertificate: <ldap: Binary blob>; <ldap: Binary blob>;
- 1> givenName: Clark;
- 1> distinguishedName: CN=Clark Kent,OU=MIL,DC=labrat,DC=com;
- 1> instanceType: 0x4 = [IT_WRITE];
- 1> whenCreated: 06/13/2006 12:50:21 Eastern Standard Time Eastern Daylight Time;
- 1> whenChanged: 06/21/2006 13:31:54 Eastern Standard Time Eastern Daylight Time;
- 1> displayName: Clark Kent;
- 1> uSNCreated: 14072;
- 1> uSNChanged: 14701;
- 1> name: Clark Kent;
- 1> objectGUID: 44039cf4-a12a-4fee-9337-3240c26ccf79;
- 1> userAccountControl: 0x10200 = [UF_NORMAL_ACCOUNT] [UF_DONT_EXPIRE_PASSWD]
- 1> badPwdCount: 0;
- 1> codePage: 0;
- 1> countryCode: 0;
- 1> badPasswordTime: 06/14/2006 15:19:36 Eastern Standard Time Eastern Daylight Time;
- 1> lastLogoff: 01/01/1601 00:00:00 UNC ;
- 1> lastLogon: 06/14/2006 16:28:44 Eastern Standard Time Eastern Daylight Time;
- 1> pwdLastSet: 06/13/2006 12:50:21 Eastern Standard Time Eastern Daylight Time;
- 1> primaryGroupID: 513;
- 1> userParameters: m: d ;
- 1> objectSid: S-1-5-21-3541480364-2458291825-1839989643-1115;
- 1> accountExpires: 09/14/30028 02:48:05 UNC ;
- 1> logonCount: 11;
- 1> sAMAccountName: 1234567870;
- 1> sAMAccountType: 805306368;
- 1> userPrincipalName: 1234567870@labrat.com;
- 1> objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=labrat,DC=com;
- 1> msNPAllowDialin: TRUE;
- 1> mail: Clark.Kent@labrat.com;

محرر واجهة خدمات Active Directory

- في خادم Active Directory، أختار ابدأ < تشغيل.
- اكتب adsiedit.msc. هذا يبدأ المحرر.
- انقر بزر الماوس الأيمن فوق كائن وانقر فوق خصائص.
- تظهر هذه الأداة كل الخصائص لكائنات معينة. راجع الشكل D2.

الشكل D2: تحرير ADSI



الملحق هـ

يمكن إنشاء توصيف AnyConnect وإضافته إلى محطة عمل. يمكن أن يشير التوصيف إلى قيم مختلفة مثل مضيفي ASA أو معلمات مطابقة الشهادة مثل الاسم المميز أو المصدر. يتم تخزين ملف التعريف كملف xml ويمكن تحريره باستخدام Notepad. يمكن إضافة الملف إلى كل عميل يدويا أو دفعه من ال ASA من خلال نهج مجموعة. يتم تخزين الملف في:

C:\Documents and Settings\All Users\Application Data\Cisco\Cisco
AnyConnect VPN Client\Profile

أكمل الخطوات التالية:

1. أختار AnyConnectProfile.tmpl وافتح الملف باستخدام Notepad.
 2. قم بإجراء التعديلات المناسبة على الملف مثل المصدر أو عنوان IP المضيف. راجع الشكل F1 على سبيل المثال.
 3. عند الانتهاء، احفظ الملف على هيئة xml.
- هذه عينة من ملف XML لملف تعريف عميل AnyConnect VPN من Cisco.
- راجع وثائق Cisco AnyConnect فيما يتعلق بإدارة ملف التعريف. وباختصار:

- يجب تسمية ملف تعريف بشكل فريد لشركتك. مثال: CiscoProfile.xml
 - يجب أن يكون اسم ملف التعريف هو نفسه حتى ولو كان مختلفا للمجموعة الفردية داخل الشركة.
- تم تصميم هذا الملف ليتم الاحتفاظ به بواسطة مسؤول عبارة آمنة ثم يتم توزيعه مع برنامج العميل. يمكن توزيع التوصيف المستند إلى XML هذا على العملاء في أي وقت. آليات التوزيع المدعومة هي كملف مجمع مع توزيع البرامج أو كجزء من آلية التنزيل التلقائية. آلية التنزيل التلقائية متاحة فقط مع بعض منتجات عبارة الأمان من Cisco.

ملاحظة: يتم تشجيع المسؤولين بشدة على التحقق من ملف تعريف XML الذي يقومون بإنشائه باستخدام أداة تحقق من الصحة عبر الإنترنت أو من خلال وظيفة إستيراد ملف التعريف في ASDM. يمكن تحقيق التحقق من الصحة باستخدام AnyConnectProfile.xsd الموجود في هذا الدليل. AnyConnectProfile هو العنصر الجذري الذي يمثل ملف تعريف عميل AnyConnect.

```
"xml version="1.0" encoding="UTF-8
```

```
--
```

```
The ClientInitialization section represents global ---!  
settings !--- for the client. In some cases, for  
example, BackupServerList, host specific !--- overrides  
- <-- --! .are possible
```

```
The Start Before Logon feature can be used to ---!  
activate !--- the VPN as part of the logon sequence. !--  
- UserControllable: Does the administrator of this  
profile allow the user !--- to control this attribute  
for their own use. Any user setting !--- associated with  
<-- .this attribute is stored elsewhere
```

```
This control enables an administrator to have a one ---!  
time !--- message displayed prior to a users first  
connection attempt. As an !--- example, the message can  
be used to remind a user to insert their smart !--- card  
into its reader. !--- The message to be used with this  
control is localizable and can be !--- found in the  
AnyConnect message catalog. !--- (default: "This is a  
(".pre-connect reminder message
```

```
This section enables the definition of various --!  
attributes !--- that can be used to refine client  
- <-- .certificate selection
```

```
Certificate Distinguished Name matching allows for ---!  
exact !--- match criteria in the choosing of acceptable  
- .client !--- certificates
```

*This section contains the list of hosts from which --! -
- .!--- the user is able to select*

*This is the data needed to attempt a connection to ---!
- <-- .a specific !--- host*

معلومات ذات صلة

- [الشهادات و CRLs المحددة بواسطة X.509 و RFC 3280](#)
- [OCSP المحدد بواسطة RFC 2560](#)
- [تقديم البنية الأساسية للمفتاح العام](#)
- ["OCSP خفيف الوزن" موضع حسب معيار المسودة](#)
- [RFC 2246 SSL / TLS المحدد بواسطة](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة م ادخت ساب دن تسمل اذة Cisco ت مچرت
ملاعلاء انء مچ م ف ن م دخت سمل م عد ى وت م م يدقت ل ى رش ب ل و
امك ة قى قد ن وكت ن ل ة ل آل ة مچرت ل ض ف أن ة ظ حال م ى چر ى . ة ص اخل م هت ب
Cisco ى لخت . فرت م مچرت م ا م د قى ى ت ل ة ف ارت حال ة مچرت ل م لاعل و
ى ل ا م ئ اد و چر ل اب ى ص و ت و ت ا مچرت ل هذه ة قد ن ع ا هت ى ل و ئ س م
Systems (رف و تم ط بار ل ا) ى ل ص أل ا ى زى ل چ ن ل دن تسمل ا