Cisco Secure Services Client مع لاثم عم نيوكت PEAP/GTC WPA

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين بروتوكول المصادقة المتوسع المحمي (PEAP)/بطاقة الرمز المميز العام ((GTC Wi-Fi Protected Access (WPA) على عميل Cisco Secure Services.

المتطلبات الأساسية

المكونات المستخدمة

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

- Cisco Secure Services Client، الإصدار 4.0يتوفر عميل Cisco Secure Services للتنزيل من Cisco.com Software Center (للعملاء المسجلين فقط).
- الحد الأدنى لنظام التشغيل Windows XP SP2 أو 2000 SP 4

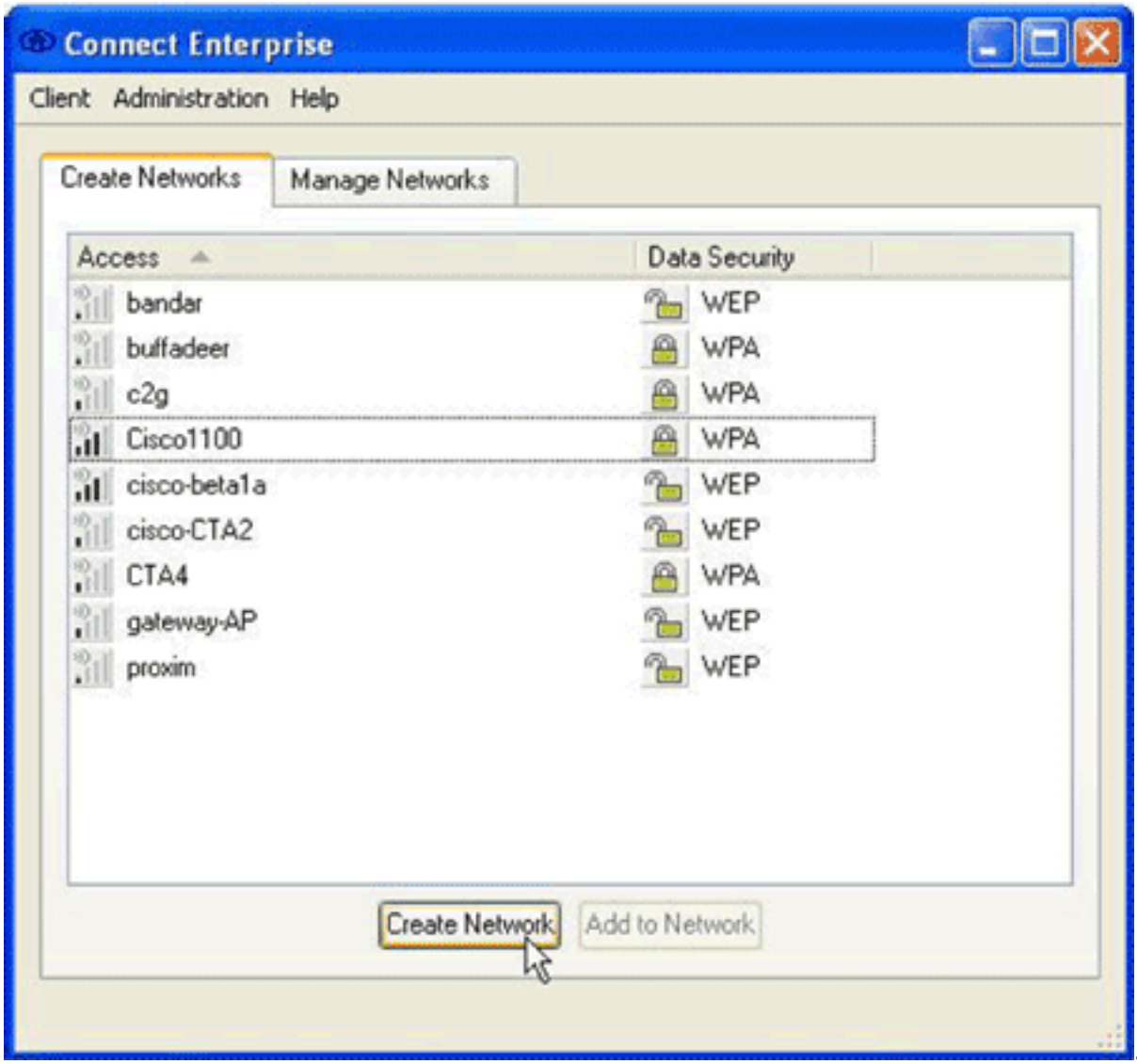
الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

تكوين Cisco Secure Services Client باستخدام PEAP/GTC WPA

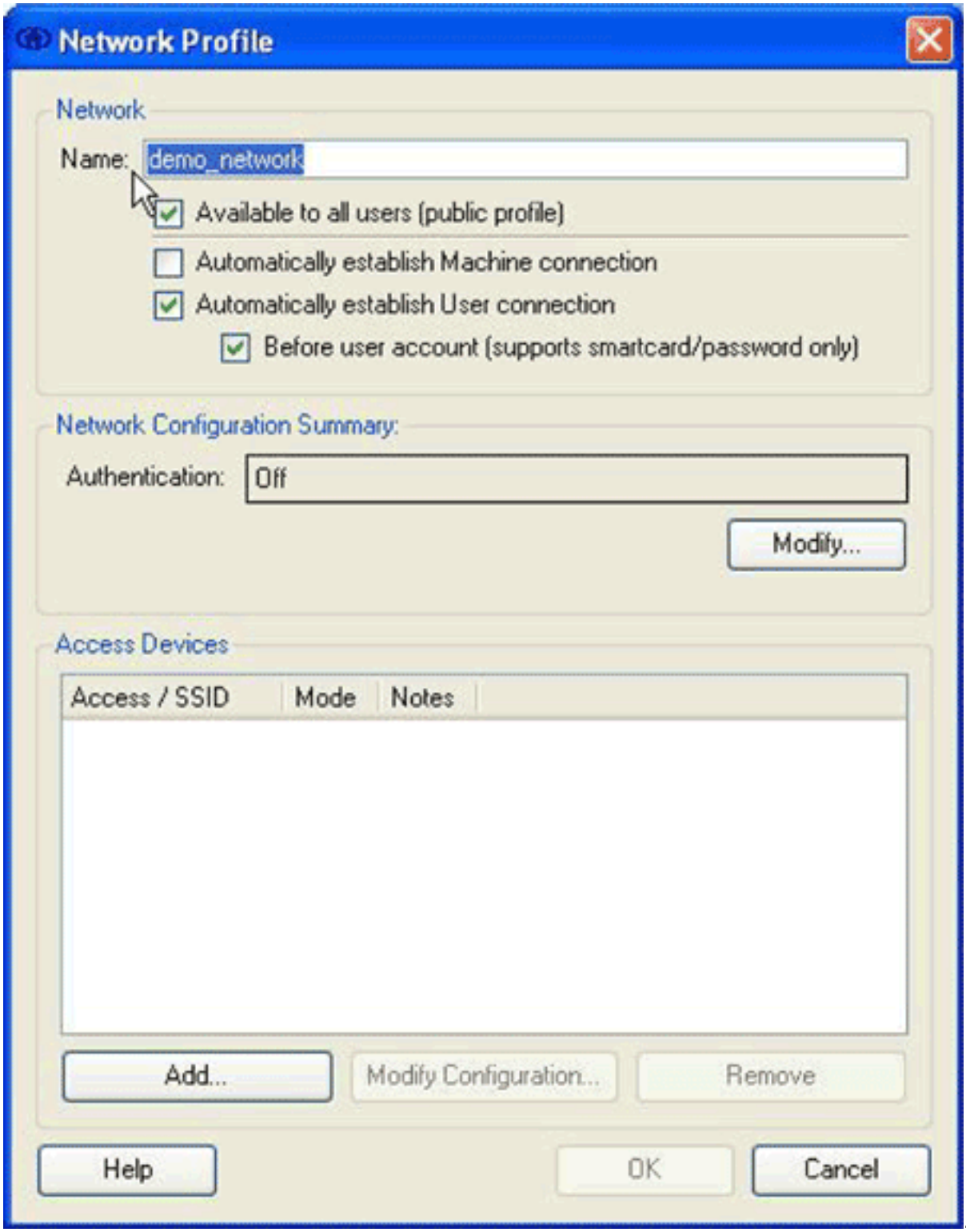
لتكوين Cisco Secure Services Client باستخدام PEAP/GTC WPA، أكمل الخطوات التالية:

1. انقر بزر الماوس الأيمن فوق رمز درج نظام Cisco Secure Services Client، واختر **فتح**.**ملاحظة:** إذا لم تكن متصلا بشبكة، فإن أيقونة درج النظام تكون خافتة.تظهر شاشة توصيل



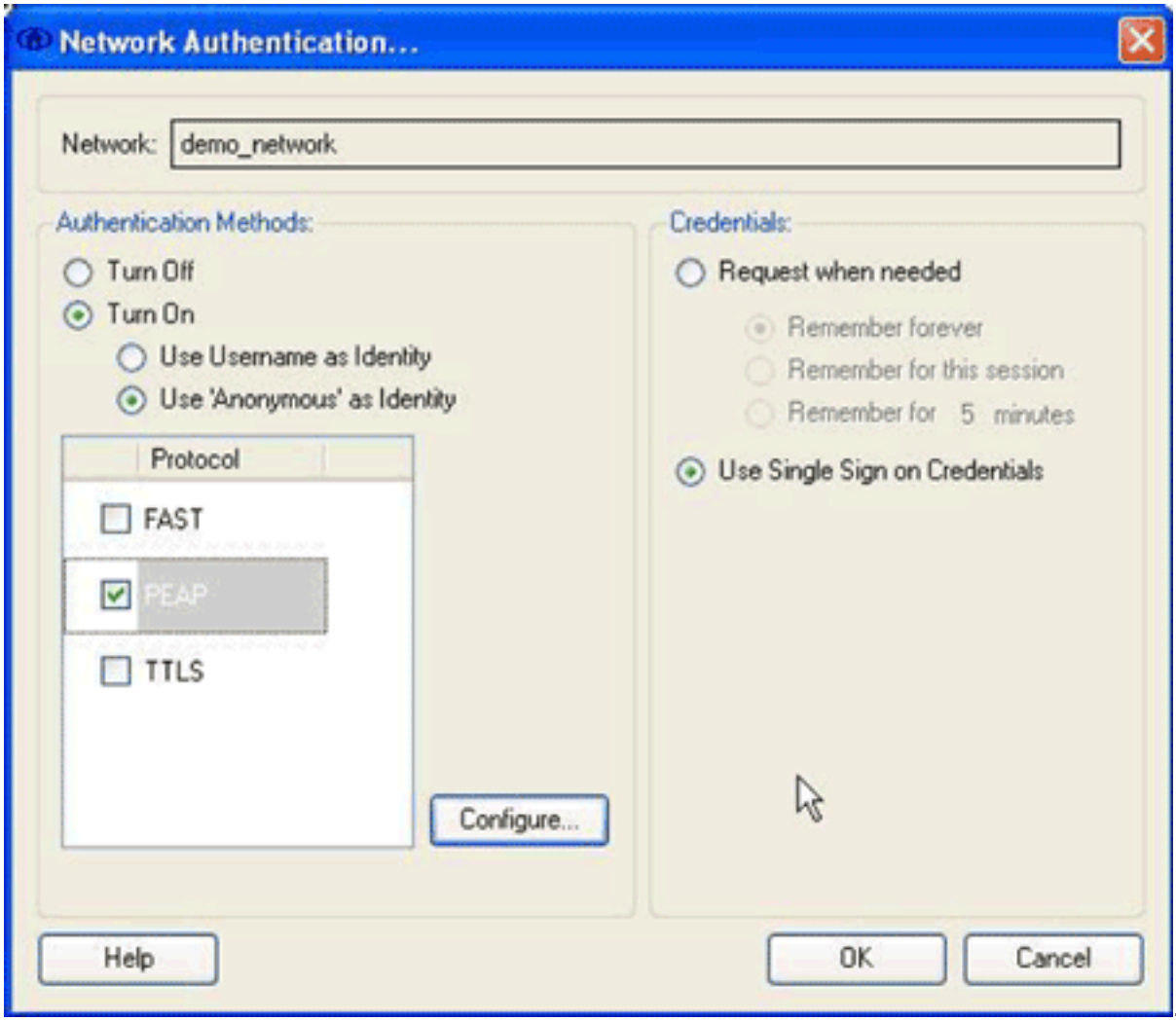
مؤسسة.

2. انقر فوق علامة التبويب **إنشاء شبكات**.تعرض منطقة إنشاء الشبكات الشبكات التي تبث معرف مجموعة الخدمة (SSID) الخاص بها.
3. انقر على الزر **إنشاء شبكة**.يظهر مربع الحوار ملف تعريف



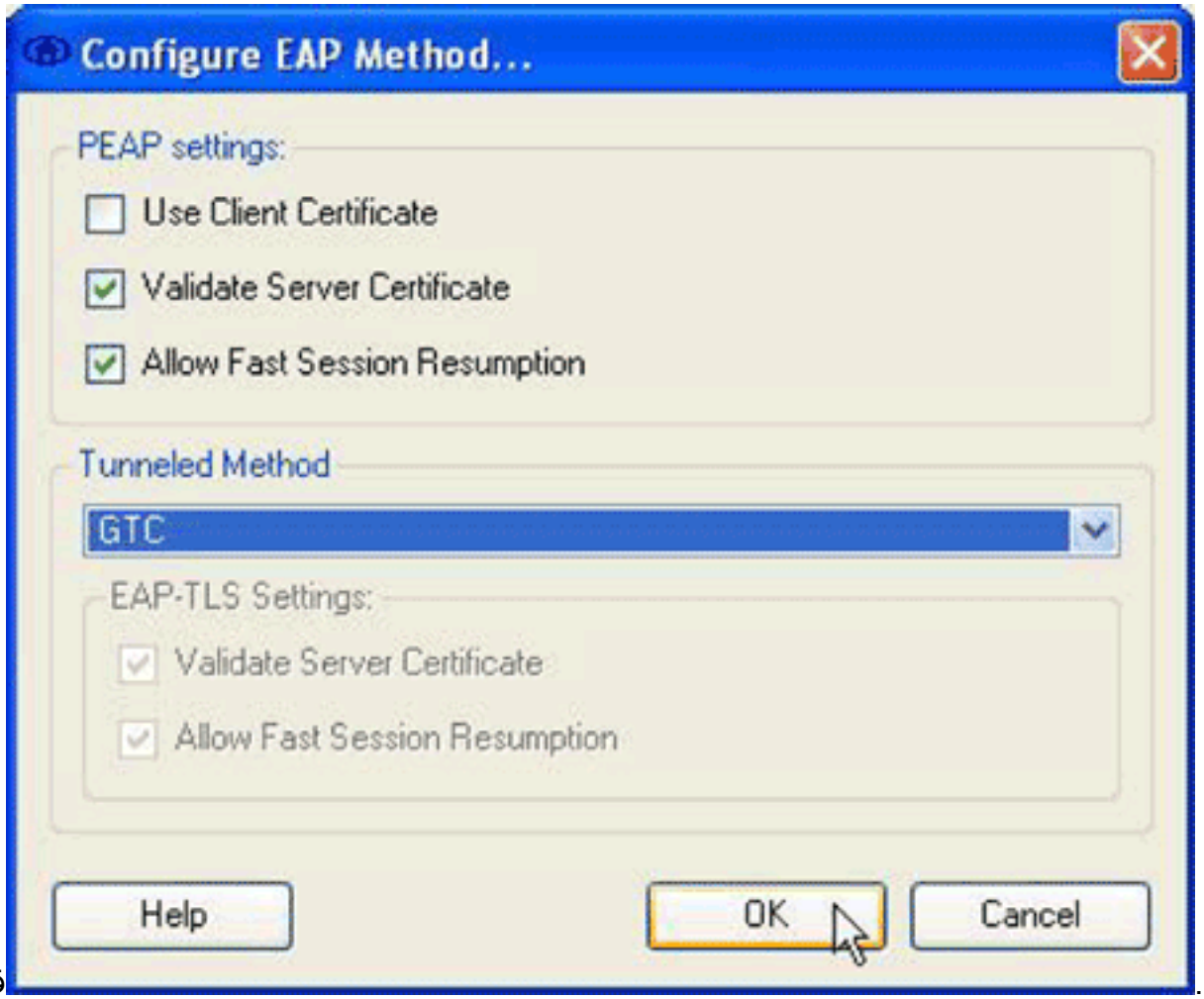
الشبكة.

4. في منطقة الشبكة، قم بتكوين الخيارات التالية:في حقل "الاسم"، أدخل اسما لشبكتك.يظهر هذا الاسم ك SSID لهذه الشبكة. لهذا المثال، الاسم هو *demo_network*.حدد خانة الاختيار **متاح لجميع المستخدمين (ملف التعريف العام)**.حدد خانة الاختيار **إنشاء اتصال المستخدم تلقائيا**، وتحقق من عدم تحديد خانة الاختيار إنشاء اتصال الجهاز تلقائيا.حدد خانة الاختيار **قبل حساب المستخدم (يدعم البطاقة الذكية/كلمة المرور فقط)**.**ملاحظة:** عند تحديد خانة الاختيار **قبل حساب المستخدم (يدعم البطاقة الذكية/كلمة المرور فقط)**، تنطلق المصادقة مباشرة بعد إدخال بيانات الاعتماد، ولكن قبل حدوث تسجيل الدخول إلى المجال. إذا كنت تستخدم شهادات المستخدم، فلا تقم بالتحقق من خانة الاختيار **قبل حساب المستخدم (يدعم البطاقة الذكية/كلمة المرور فقط)**. نظرا لأنها غير متوفرة قبل تسجيل دخول Windows، لا يمكنك إستخدام شهادات المستخدم التي تحتوي على تسجيلات المجال.
5. في منطقة ملخص تكوين الشبكة، انقر على زر **تعديل**.يظهر مربع الحوار مصادقة



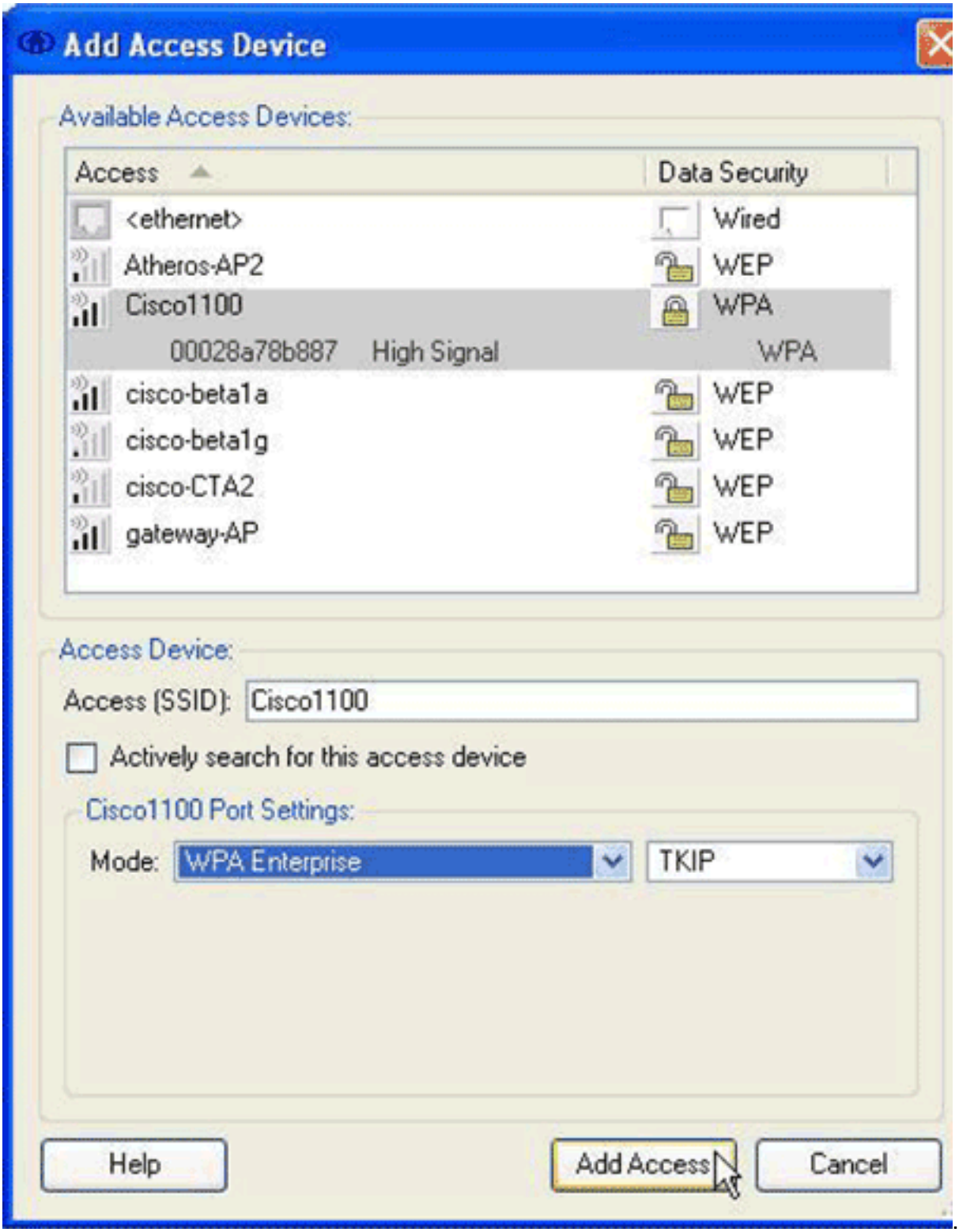
الشبكة.

6. في شاشة مصادقة الشبكة، قم بتكوين الخيارات التالية:في منطقة بيانات الاعتماد، انقر على زر **إستخدام** إرسال **بيانات اعتماد الدخول الموحد**.في منطقة طرق المصادقة، انقر على زر **تشغيل** الراديو ، ثم انقر على **إستخدام 'مجهول' كهوية**.يقوم زر تشغيل الراديو بتعميم قائمة البروتوكولات المعروضة في منطقة طرق المصادقة. يحدد زر إستخدام 'مجهول' كمرجع هوية القائمة ببروتوكولات المصادقة النفقي فقط.حدد خانة الاختيار **PEAP**، ثم انقر **تكوين**.سوف يظهر مربع الحوار تكوين أسلوب



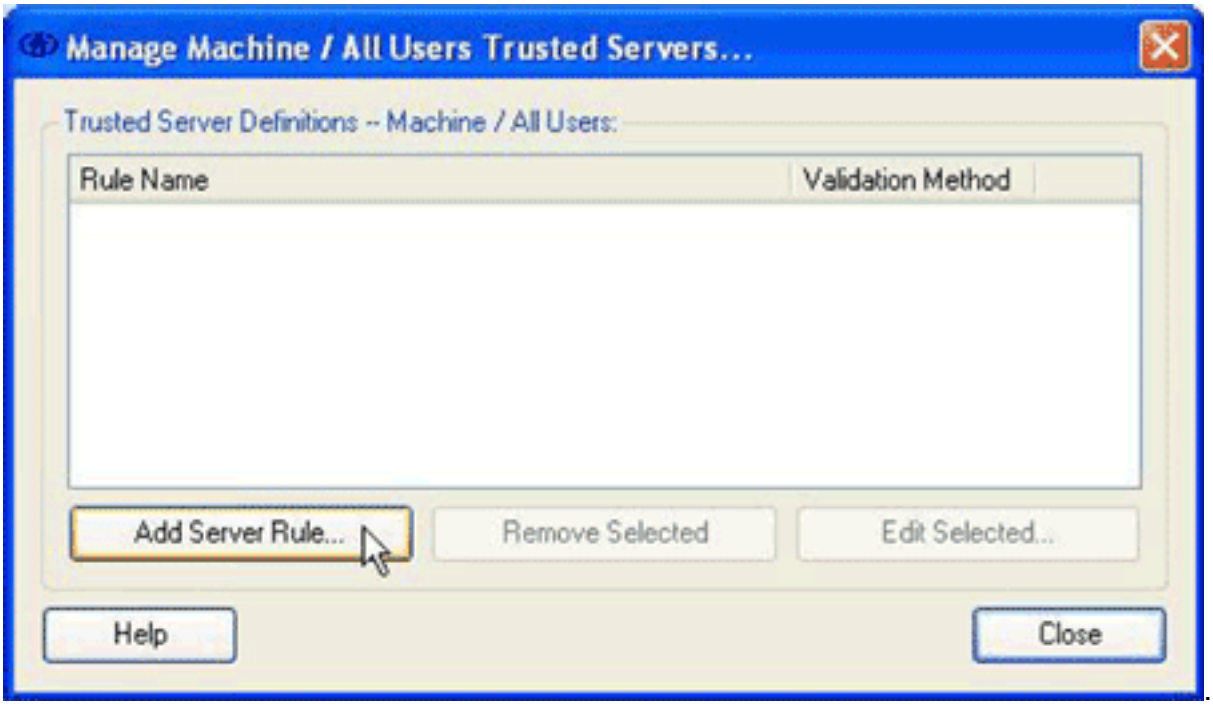
قم بإلغاء تحديد خانة الاختيار **إستخدام شهادة العميل**.حدد **التحقق من شهادة الخادم** و**السماح باستئناف الجلسة السريعة** خانات الاختيار.من القائمة المنسدلة أسلوب النفق، أختر **GTC**.انقر على **موافق** للعودة إلى شاشة مصادقة الشبكة، ثم انقر على **موافق** للعودة إلى شاشة ملف تعريف الشبكة.

7. في منطقة أجهزة الوصول من شاشة ملف تعريف الشبكة، انقر على **إضافة**.سوف يظهر مربع الحوار إضافة جهاز



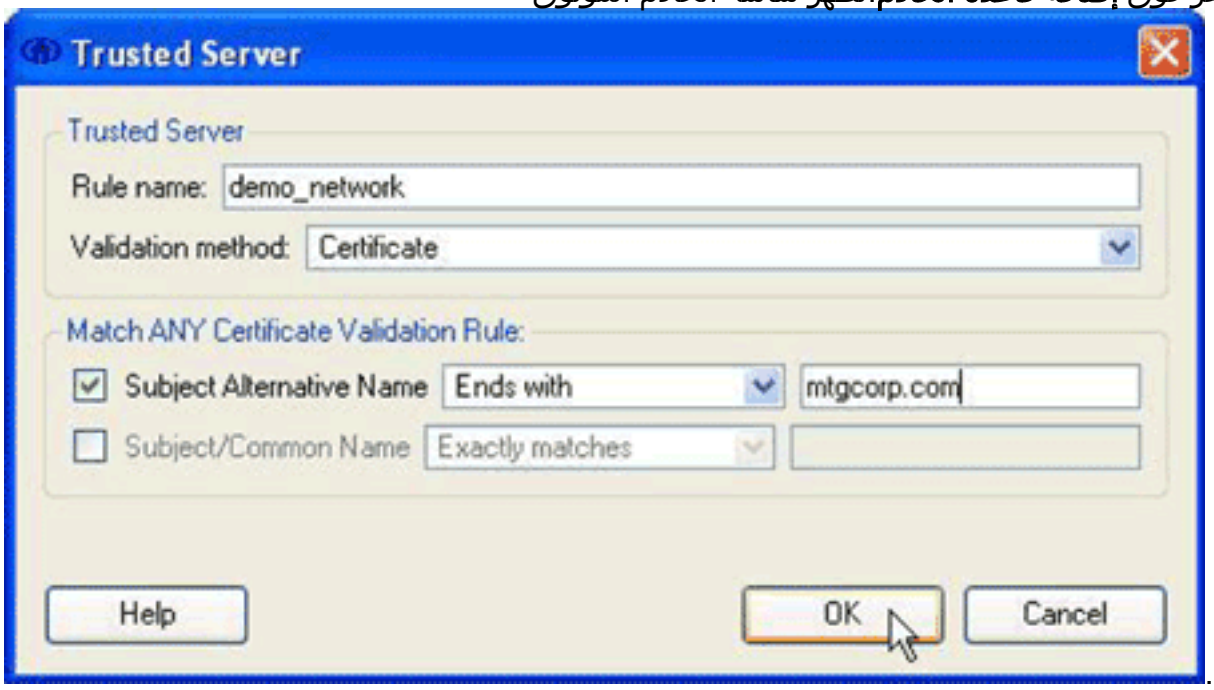
الوصول.

8. في شاشة إضافة أجهزة وصول، أختر الجهاز الذي تريد تكوينه، ثم انقر **إضافة وصول**.**ملاحظة:** إذا كان الجهاز الذي تريد تكوينه يقع ضمن النطاق، فيجب أن يظهر اسم SSID الخاص بهذا الجهاز في قائمة أجهزة الوصول المتاحة. إذا لم يظهر الجهاز، فأدخل SSID للجهاز في حقل الوصول (SSID)، وأدخل إعدادات المنفذ في منطقة إعدادات المنفذ Cisco 1100، ثم انقر على **إضافة وصول**.
9. في شاشة ملف تعريف الشبكة، انقر على **موافق** للعودة إلى شاشة توصيل مؤسسة.
10. في شاشة توصيل مؤسسة، أختر **خوادم موثوق بها > إدارة الجهاز / كافة المستخدمين خوادم موثوق بها** من قائمة العميل.سوف يظهر مربع الحوار إدارة الجهاز / كافة المستخدمين للخوادم الموثوق



بها.

11. انقر فوق **إضافة قاعدة الخادم**.تظهر شاشة الخادم الموثوق



به.

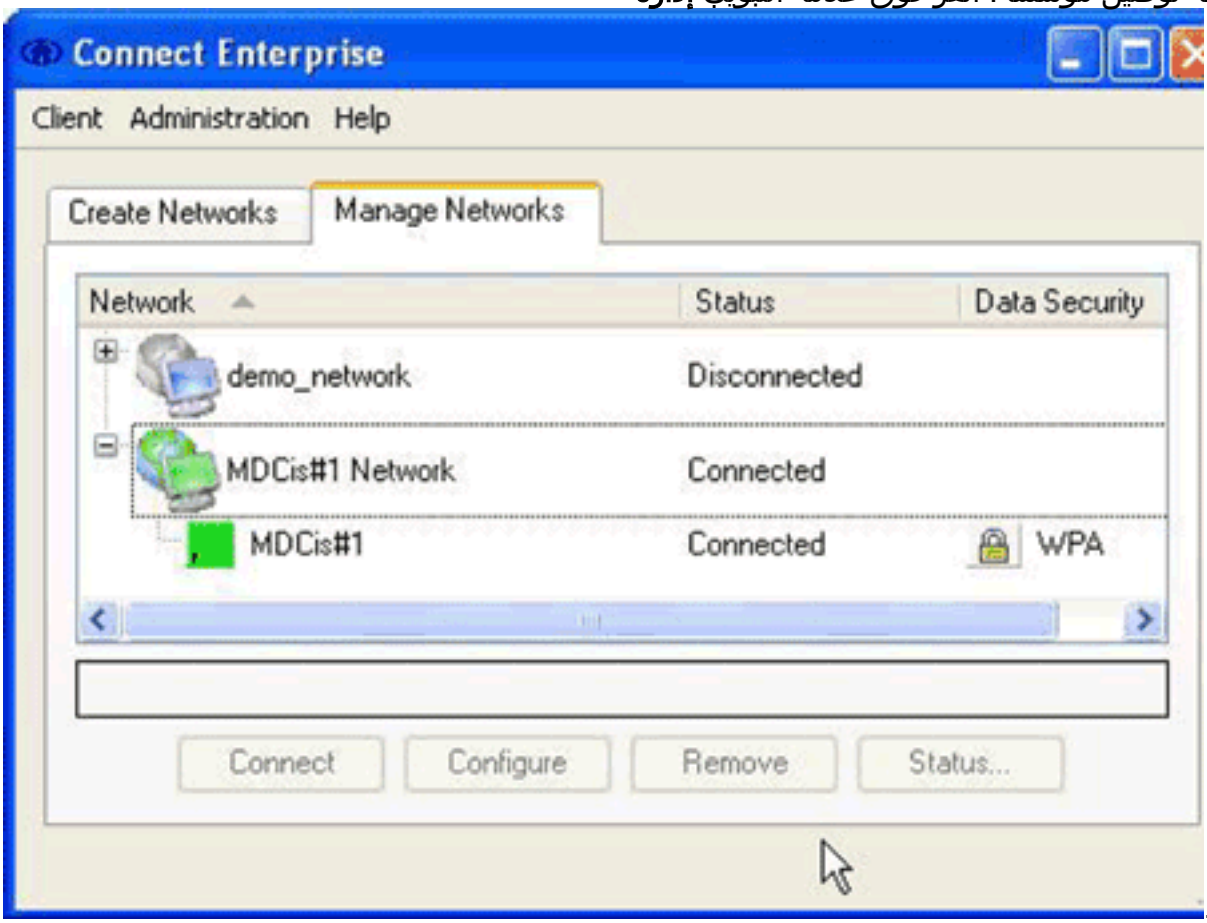
12. في شاشة الخادم الموثوق به، قم بتكوين الخيارات التالية:في حقل اسم القاعدة، أدخل اسما للقاعدة.من القائمة المنسدلة أسلوب التحقق، أختر **شهادة**.في المطابقة أي منطقة في قاعدة التحقق من صحة الشهادة، قم بتكوين خيارات للقاعدة.لإنشاء قاعدة، يجب أن تعرف محتوى شهادة الخادم وتدخل تلك القيم في مطابقة أي منطقة من قواعد التحقق من صحة الشهادة. على سبيل المثال، إذا كان اسم الموضوع البديل يحتوي على اسم مجال للخادم، *mtgcorpserver.mtgcorp.com*، أختر **End with** من القائمة المنسدلة اسم الموضوع البديل، ثم أدخل **mtgcorp.com** في حقل النص.انقر فوق **موافق** للعودة إلى مربع الحوار إدارة الجهاز / كافة المستخدمين الخوادم الموثوق بها.
13. في شاشة إدارة الجهاز / كافة المستخدمين للخوادم الموثوق بها، انقر فوق **إغلاق**" للعودة إلى مربع الحوار "توصيل مؤسسة".

اكتمل التكوين، ويمكنك الاتصال بالشبكة.

الاتصال بالشبكة

للاتصال بشبكتك الجديدة، أكمل الخطوات التالية:

1. في شاشة توصيل مؤسسة، انقر فوق علامة التبويب **إدارة الشبكات**.



2. انفصل عن أي شبكة موصلة بالمحول المستخدم من قبل شبكتك الجديدة.
3. من لائحة الشبكات حدد التوصيف الجديد ثم انقر على **توصيل**.

عند نجاح التكوين والاتصال، يعرض رمز درج نظام Cisco Secure Services Client اللون الأخضر.

ملاحظة: إذا تم تثبيت برنامج الحماية من الفيروسات على الكمبيوتر الخاص بك وتم تكوينه لتحليل دليل سجل عميل "الخدمات الآمنة من Cisco"، فقد تواجه دورات عالية لوحدة المعالجة المركزية باستخدام مصادقة عميل "الخدمات الآمنة من Cisco". لتحسين الأداء، قم بتكوين برنامج الحماية من الفيروسات لاستبعاد دليل سجل عميل الخدمات الآمنة من Cisco.

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).