تكوين تسجيل الدخول الأحادي باستخدام AD FS 2.0 و CUCM

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين تسجيل الدخول الأحادي (SSO) على Cisco Unified Communications Manager وخدمة إتحاد Active Directory.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- برنامج Cisco Unified Communications Manager (CUCM)
- معرفة أساسية بخدمة إتحاد Active Directory (AD FS)

لتمكين SSO في بيئة المختبر، يلزمك هذا التكوين:

- Windows Server مع AD FS المثبت.
- CUCM مع تكوين مزامنة LDAP.
- مستخدم نهائي مع تحديد دور CCM Super Users القياسي.

المكونات المستخدمة

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

- Windows Server مع AD FS 2.0
- CUCM 10.5.2

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يتم توفير الإجراء الخاص ب AD FS 2.0 مع Windows Server 2008 R2. تعمل هذه الخطوات أيضا مع AD FS 3.0 على Windows Server 2016.

تنزيل AD FS 2.0 وتثبيته على خادم Windows

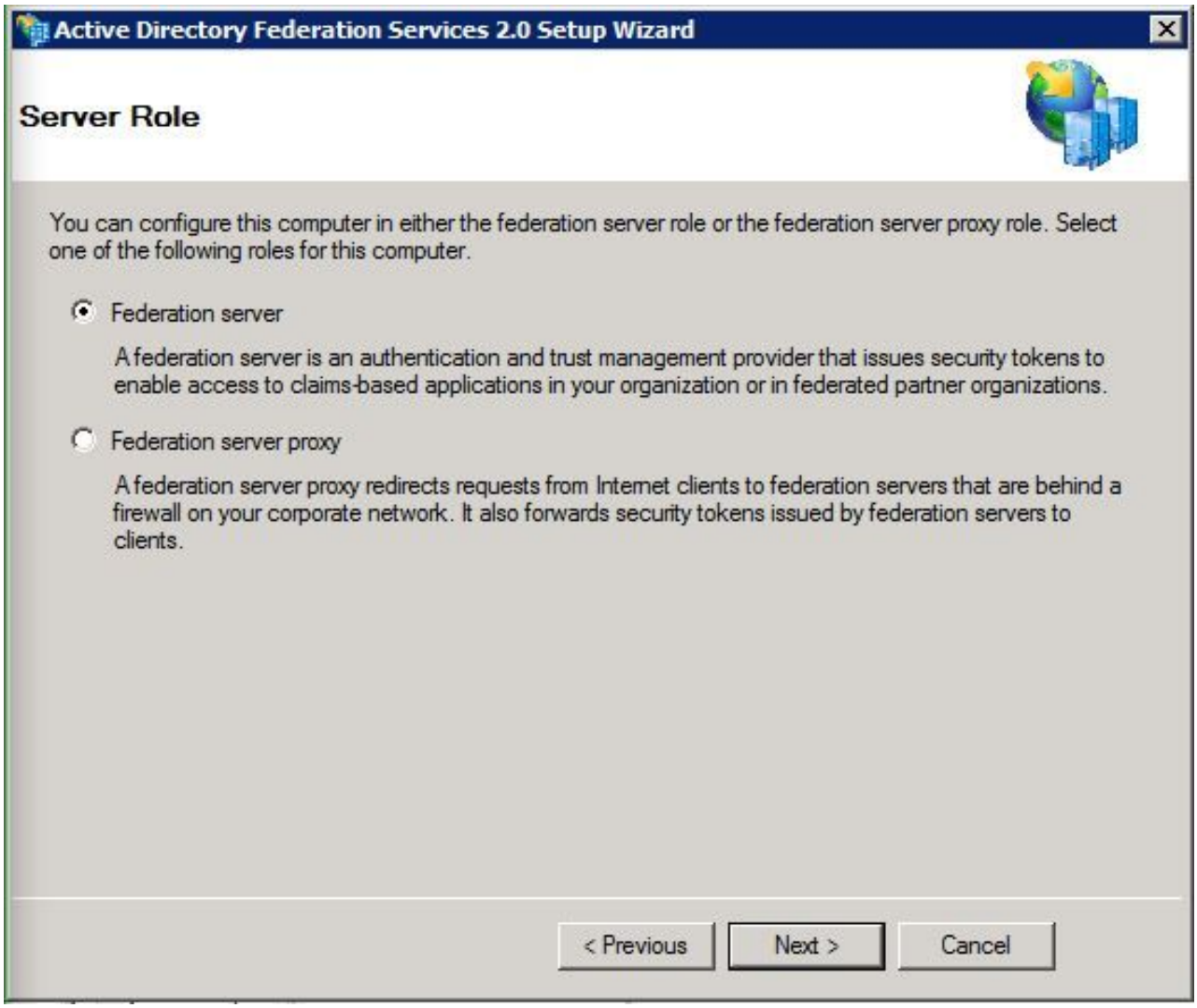
الخطوة 1. انتقل إلى تنزيل AD FS 2.0.

الخطوة 2. تأكد من تحديد التنزيل المناسب استنادا إلى خادم Windows.

الخطوة 3. انقل الملف الذي تم تنزيله إلى خادم Windows.

الخطوة 4. متابعة التثبيت:

الخطوة 5. عند المطالبة، أختر Federation Server:



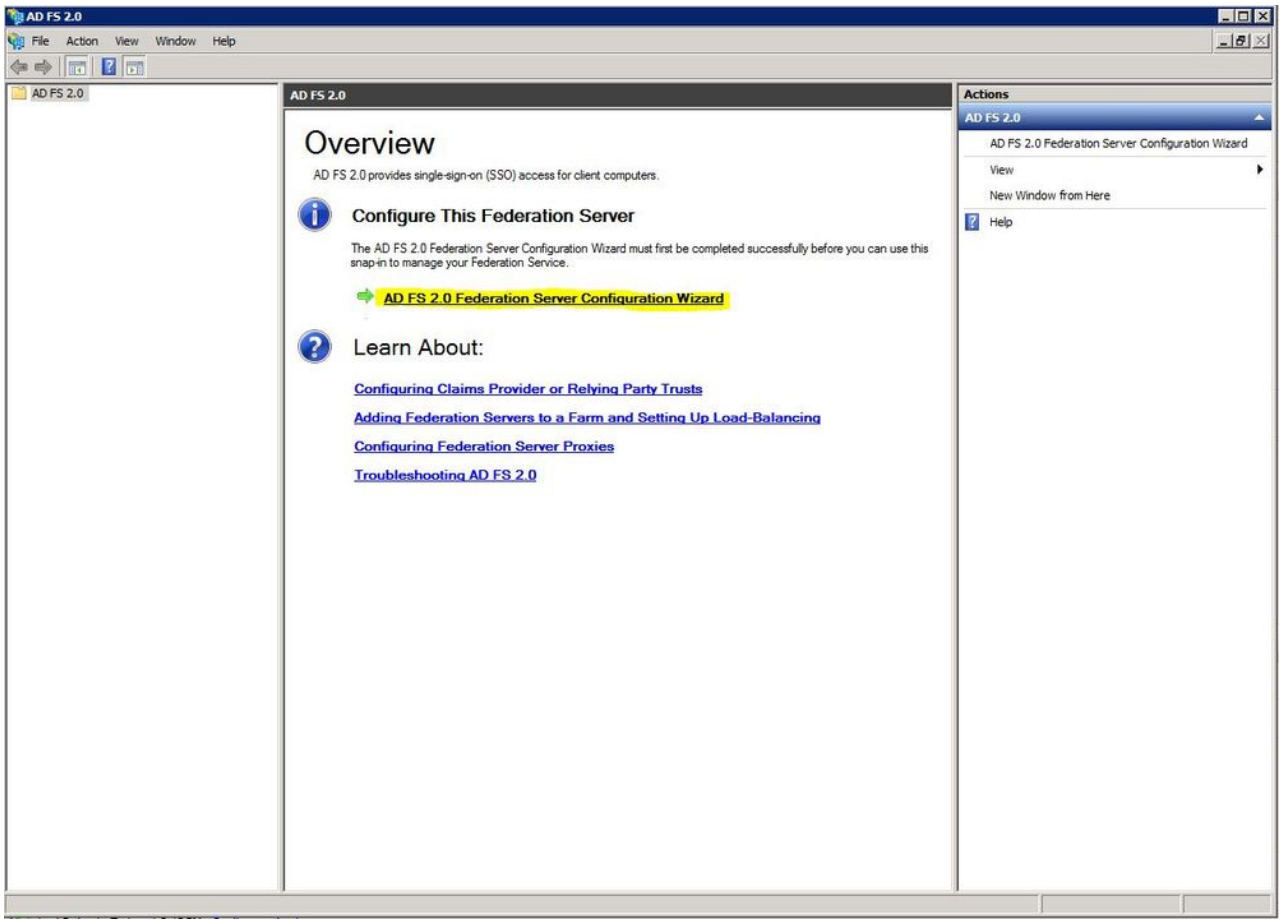
الخطوة 6. يتم تثبيت بعض التبعيات تلقائيا - بمجرد أن يتم ذلك، انقر فوق إنهاء.

الآن بعد أن أصبح لديك AD FS 2.0 مثبتا على الخادم الخاص بك، تحتاج إلى إضافة بعض التهيئة.

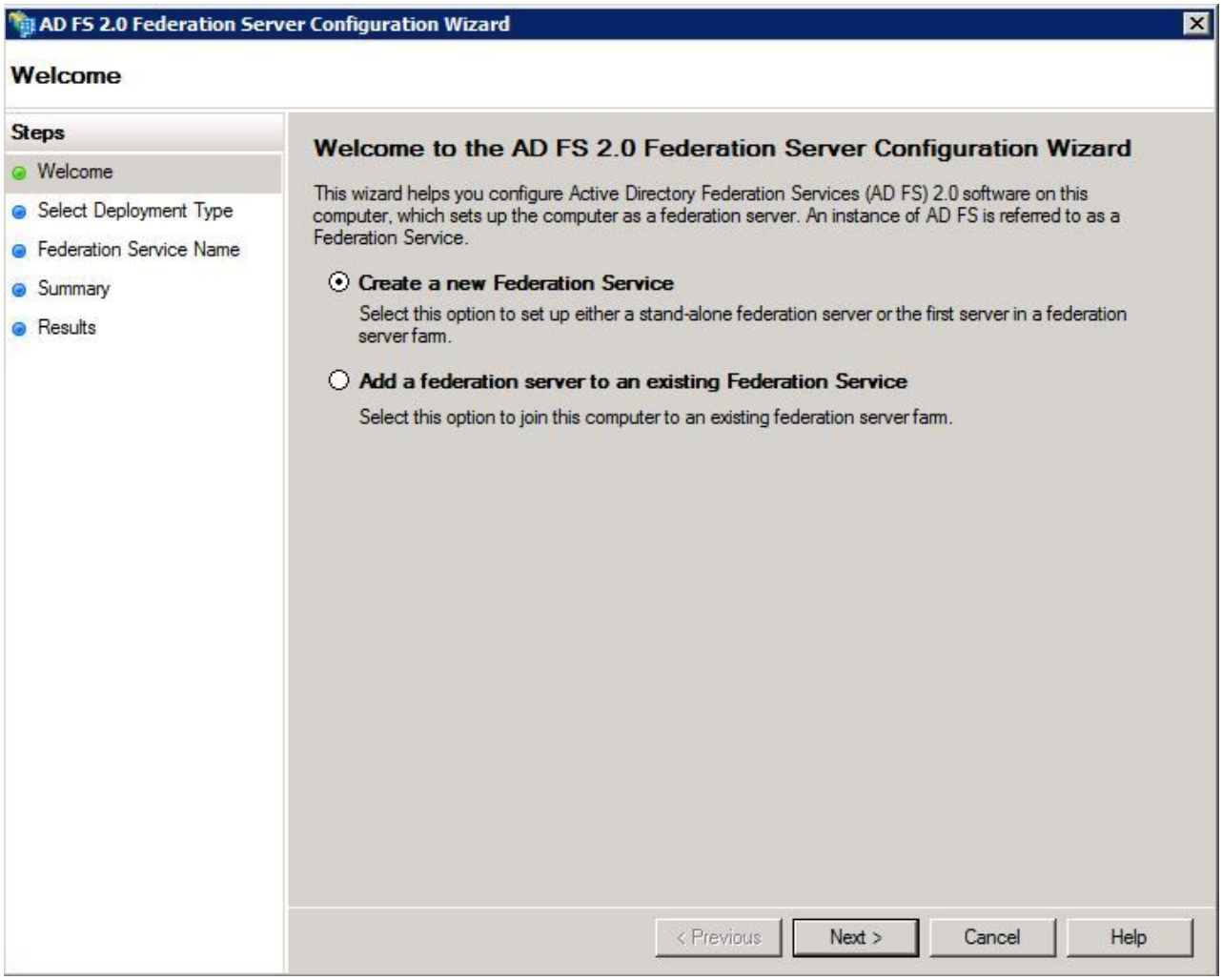
تكوين AD FS 2.0 على خادم Windows

الخطوة 1. إذا لم تفتح نافذة AD FS 2.0 تلقائيا بعد التثبيت، يمكنك النقر فوق بدء والبحث عن إدارة AD FS 2.0 لفتحها يدويا.

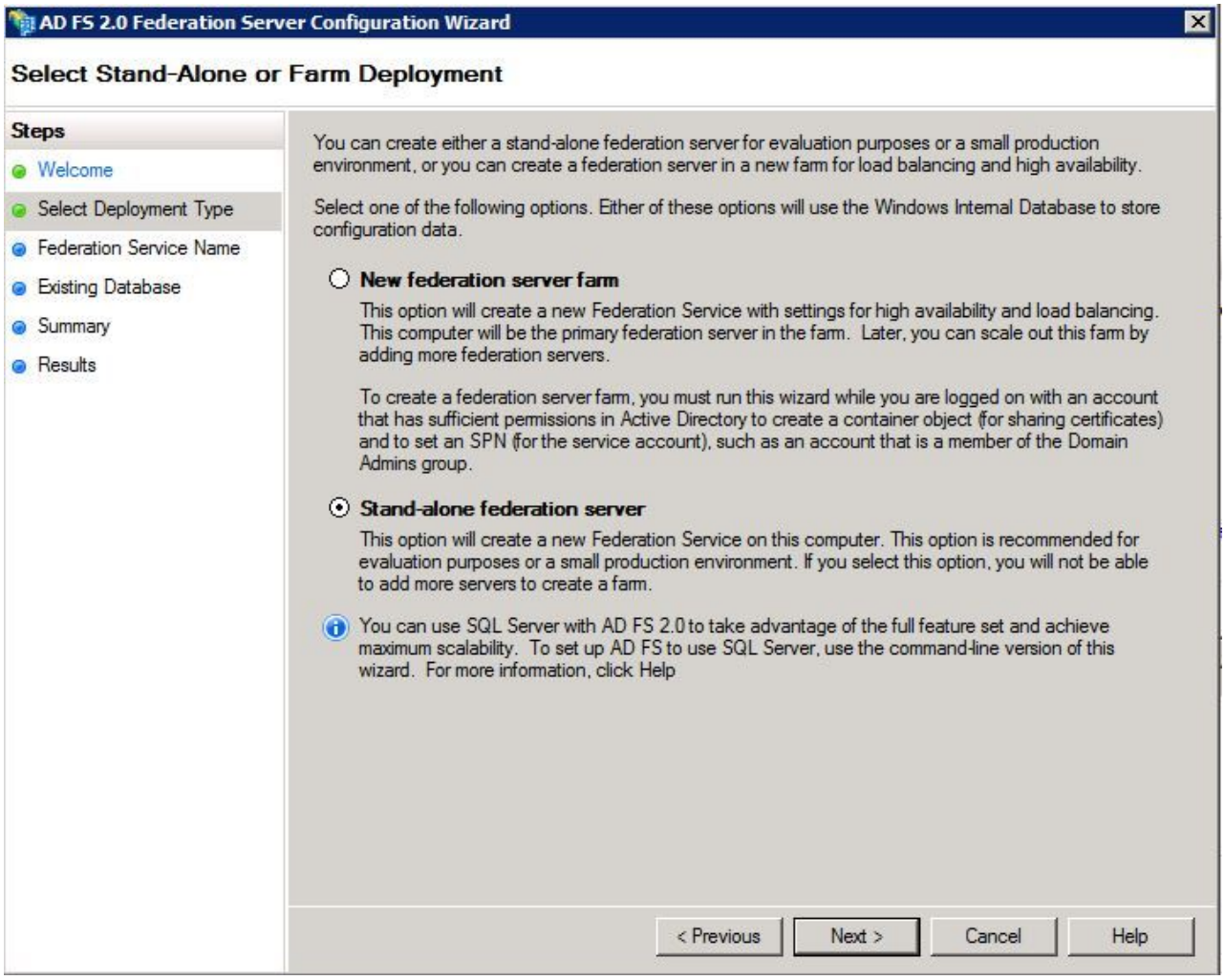
الخطوة 2. أختر معالج تكوين خادم الاتحاد AD FS 2.0.



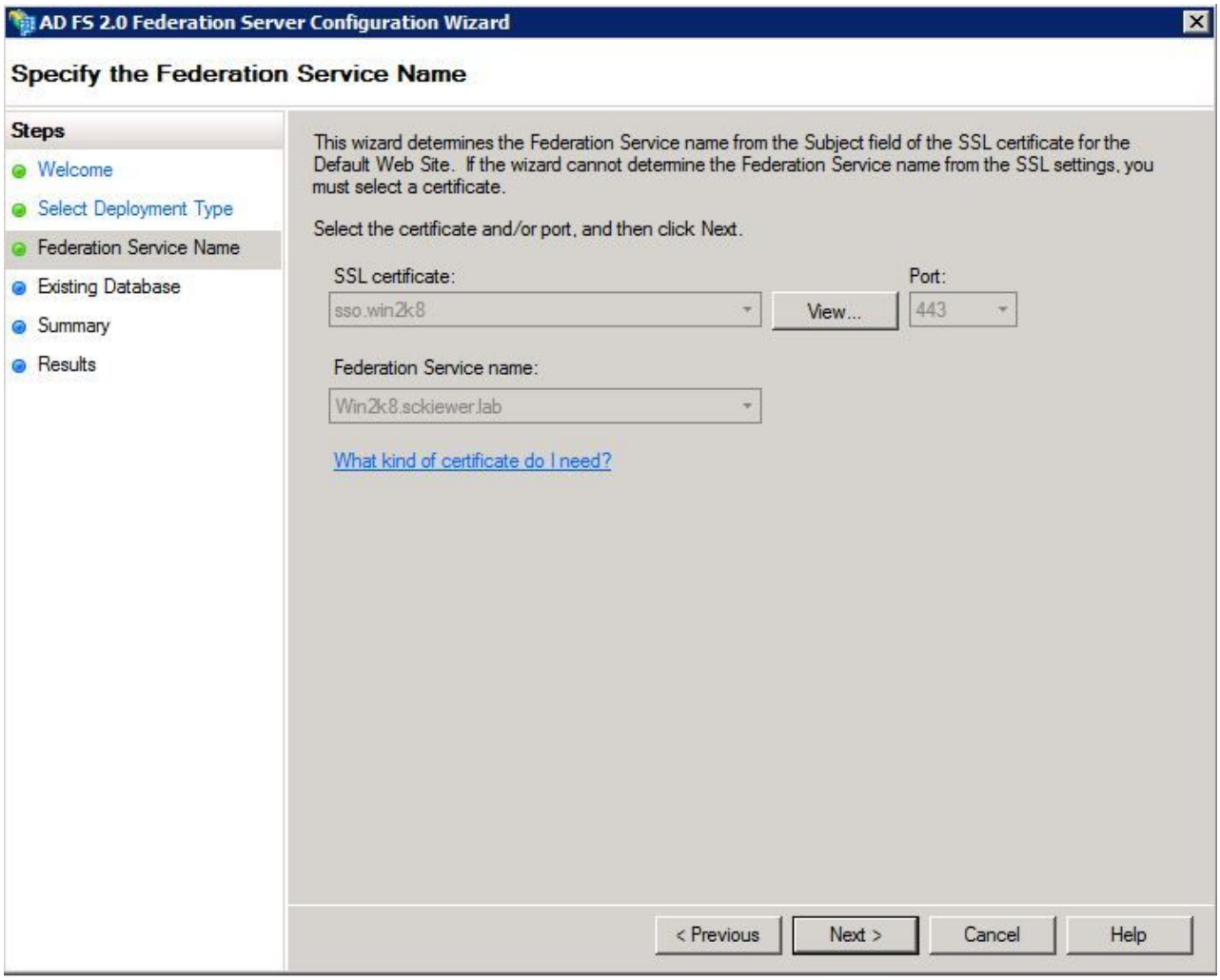
الخطوة 3. بعد ذلك، انقر فوق إنشاء خدمة إتحاد جديدة.



الخطوة 4. في معظم البيئات، يكون خادم الاتحاد المستقل كافيا.



الخطوة 5. بعد ذلك، يطلب منك إختيار شهادة. يتم تلقائيا ملء هذا الحقل طالما كان لدى الخادم شهادة.



الخطوة 6. إذا كان لديك بالفعل قاعدة بيانات AD FS على الخادم، فأنت بحاجة إلى إزالتها للمتابعة.

الخطوة 7. أخيرا، أنت على شاشة ملخص حيث يمكنك النقر فوق التالي.

إستيراد بيانات تعريف المشردين إلى CUCM / تنزيل بيانات تعريف CUCM

الخطوة 1. قم بتحديث عنوان URL باسم المضيف/FQDN الخاص بخادم Windows وتنزيل بيانات التعريف من خادم AD FS الخاص بك - https://hostname/federationmetadata/2007-06/federationmetadata.xml

الخطوة 2. انتقل إلى إدارة Cisco Unified CM > النظام > تسجيل دخول أحادي SAML.

الخطوة 3. طقطقة يمكن SAML sso.

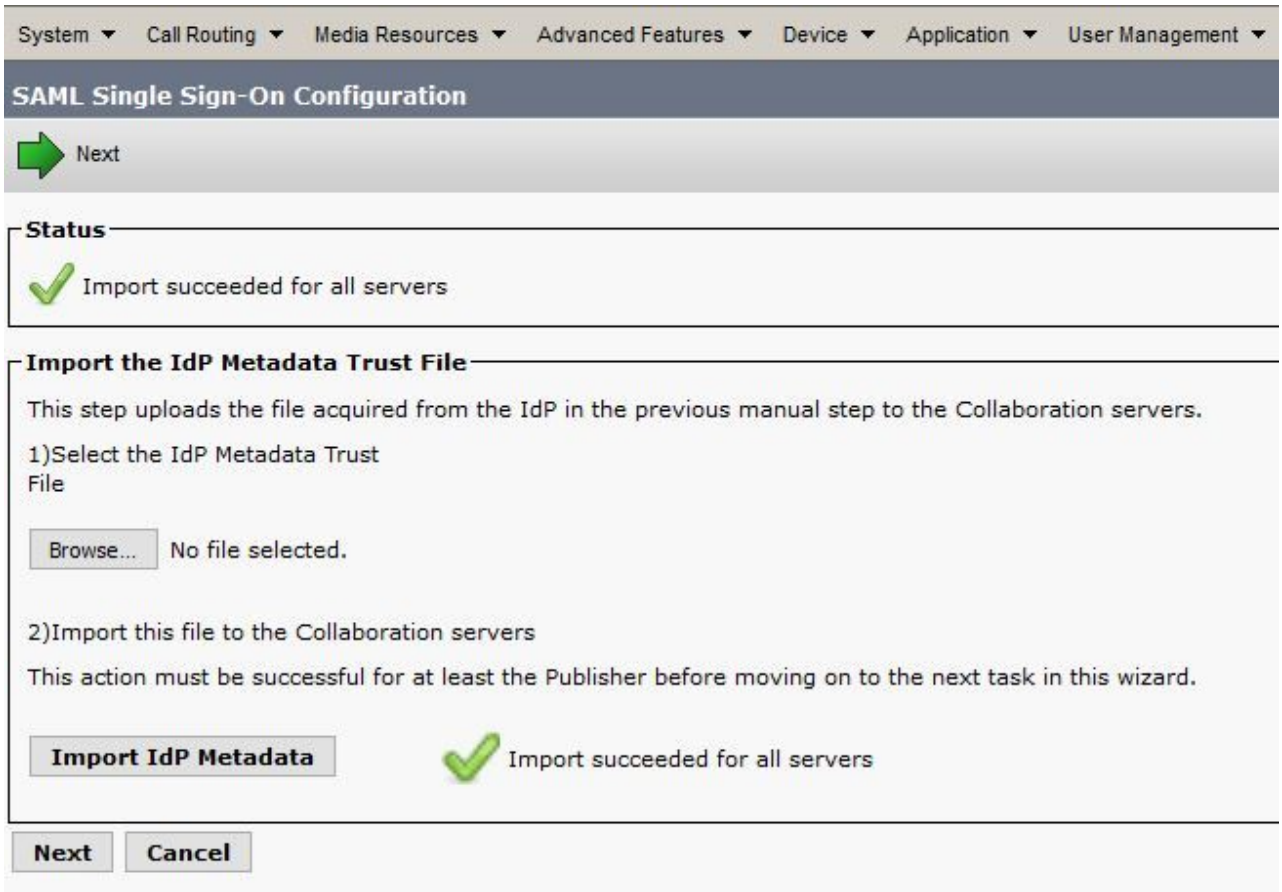
الخطوة 4. إذا تلقيت تنبيها حول إتصالات خادم الويب، انقر فوق متابعة.

الخطوة 5. بعد ذلك، يرشدك CUCM لتنزيل ملف بيانات التعريف من المعرف الخاص بك. في هذا السيناريو، يكون خادم AD FS الخاص بك هو المعرف (IDp)، وقد قمت بتنزيل

بيانات التعريف في الخطوة 1، لذلك انقر فوق التالي.

الخطوة 6. انقر فوق إستعراض > تحديد .xml من الخطوة 1 > انقر فوق إستيراد بيانات تعريف IdP.

الخطوة 7. تشير رسالة إلى أن عملية الاستيراد كانت ناجحة:



الخطوة 8. انقر فوق Next (التالي).

الخطوة 9. الآن بعد أن حصلت على بيانات تعريف IDp المستوردة إلى CUCM، تحتاج إلى إستيراد بيانات تعريف CUCM إلى المعرف الخاص بك.

الخطوة 10. انقر فوق تنزيل ملف بيانات تعريف الثقة.

الخطوة 11. انقر فوق Next (التالي).

الخطوة 12. انقل ملف .zip إلى خادم Windows واستخرج المحتويات إلى مجلد.

إستيراد بيانات تعريف CUCM إلى خادم AD FS 2.0 وإنشاء قواعد المطالبات

الخطوة 1. انقر على بدء والبحث عن إدارة AD FS 2.0.

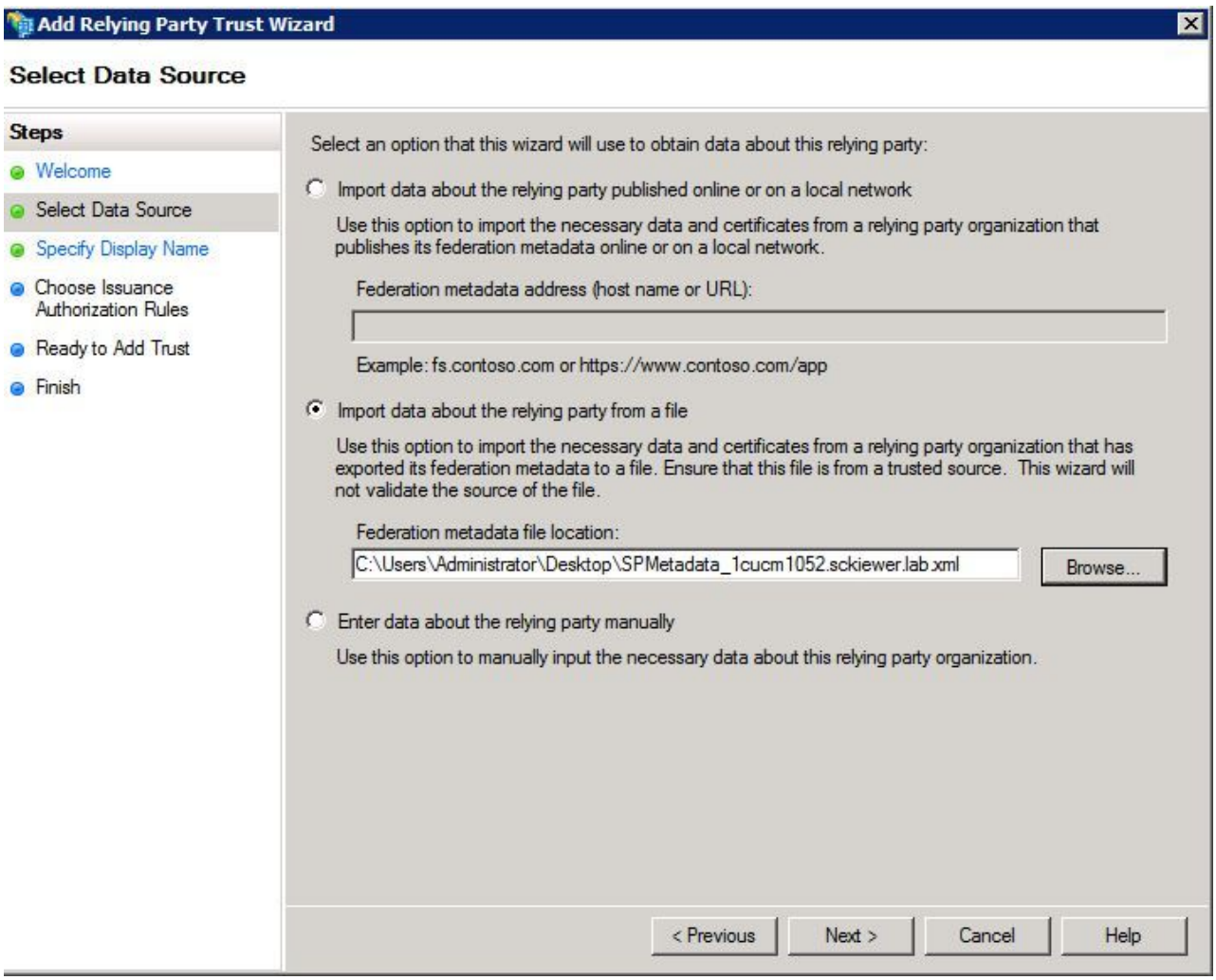
الخطوة 2. انقر فوق مطلوب: إضافة جهة اعتماد موثوق بها.

ملاحظة: إذا لم ترى هذا الخيار، تحتاج إلى إغلاق النافذة وفتحها مرة أخرى.

الخطوة 3. بمجرد أن يتم فتح معالج إضافة ثقة جهة الاعتماد، انقر فوق بدء.

الخطوة 4. هنا، تحتاج إلى إستيراد ملفات XML التي قمت باستخراجها في الخطوة 12. حدد إستيراد بيانات حول الطرف المعول من ملف واستعرض إلى ملفات المجلد واختر XML لنا شرك.

ملاحظة: أستخدم الخطوات السابقة لأي خادم تعاون موحد تريد إستخدام SSO عليه.



الخطوة 5. انقر فوق Next (التالي).

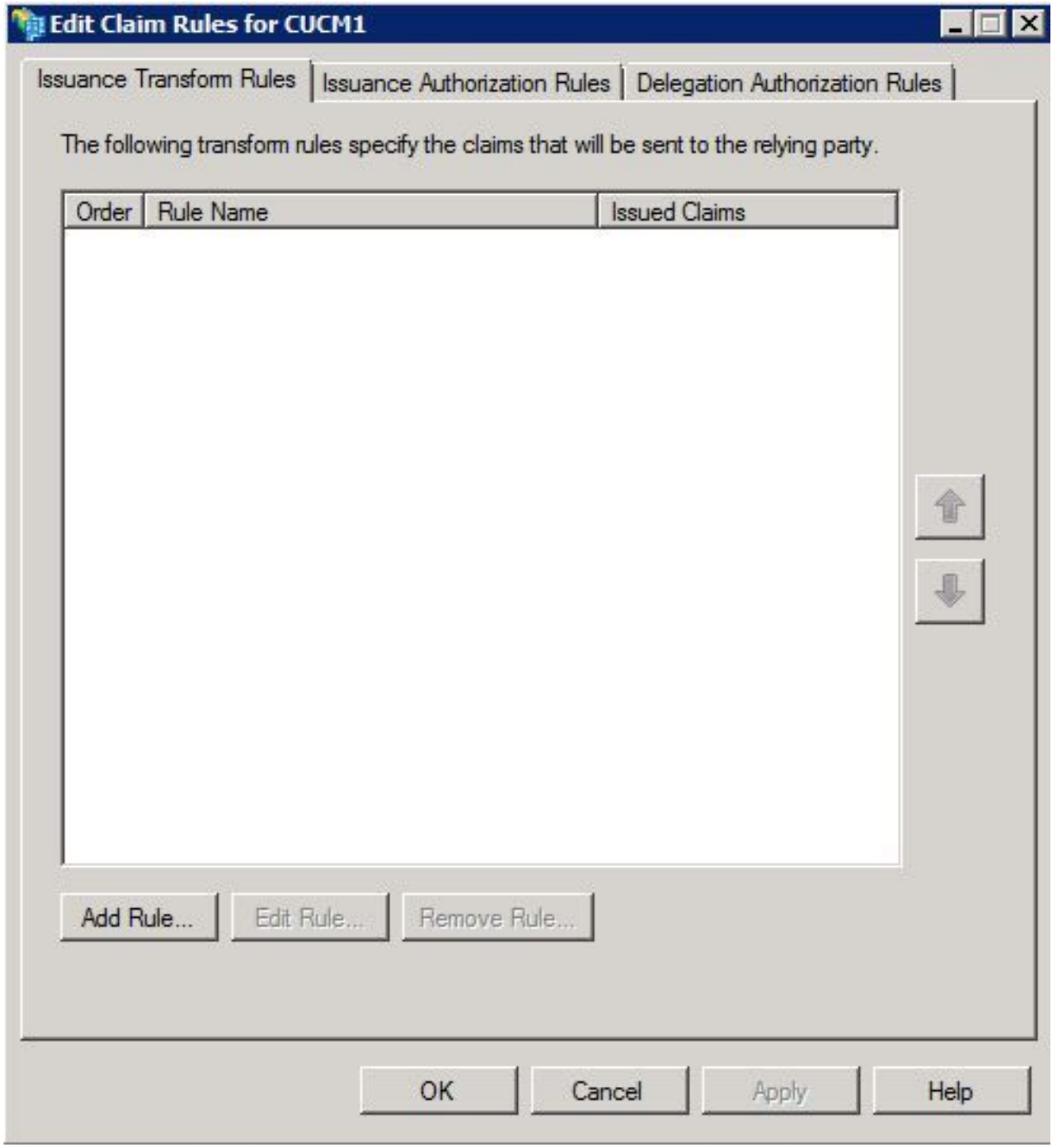
الخطوة 6. حرر اسم العرض وانقر بعد ذلك.

الخطوة 7. أختر السماح لجميع المستخدمين بالوصول إلى جهة الاعتماد هذه وانقر فوق التالي.

الخطوة 8. طقطقت بعد ذلك ثانية.

الخطوة 9. على هذه الشاشة، تأكد من أنك قمت بفتح مربع الحوار "تحرير قواعد المطالبة" لثقة الطرف المعول هذه عند إغلاق المعالج للتدقيق، ثم انقر فوق إغلاق.

الخطوة 10. يتم فتح الإطار تحرير قواعد المطالبات:



الخطوة 11. في هذا الإطار، انقر فوق إضافة قاعدة.

الخطوة 12. ل قالب قاعدة المطالبة، أختر إرسال سمات LDAP كمطالبات وانقر فوق التالي.

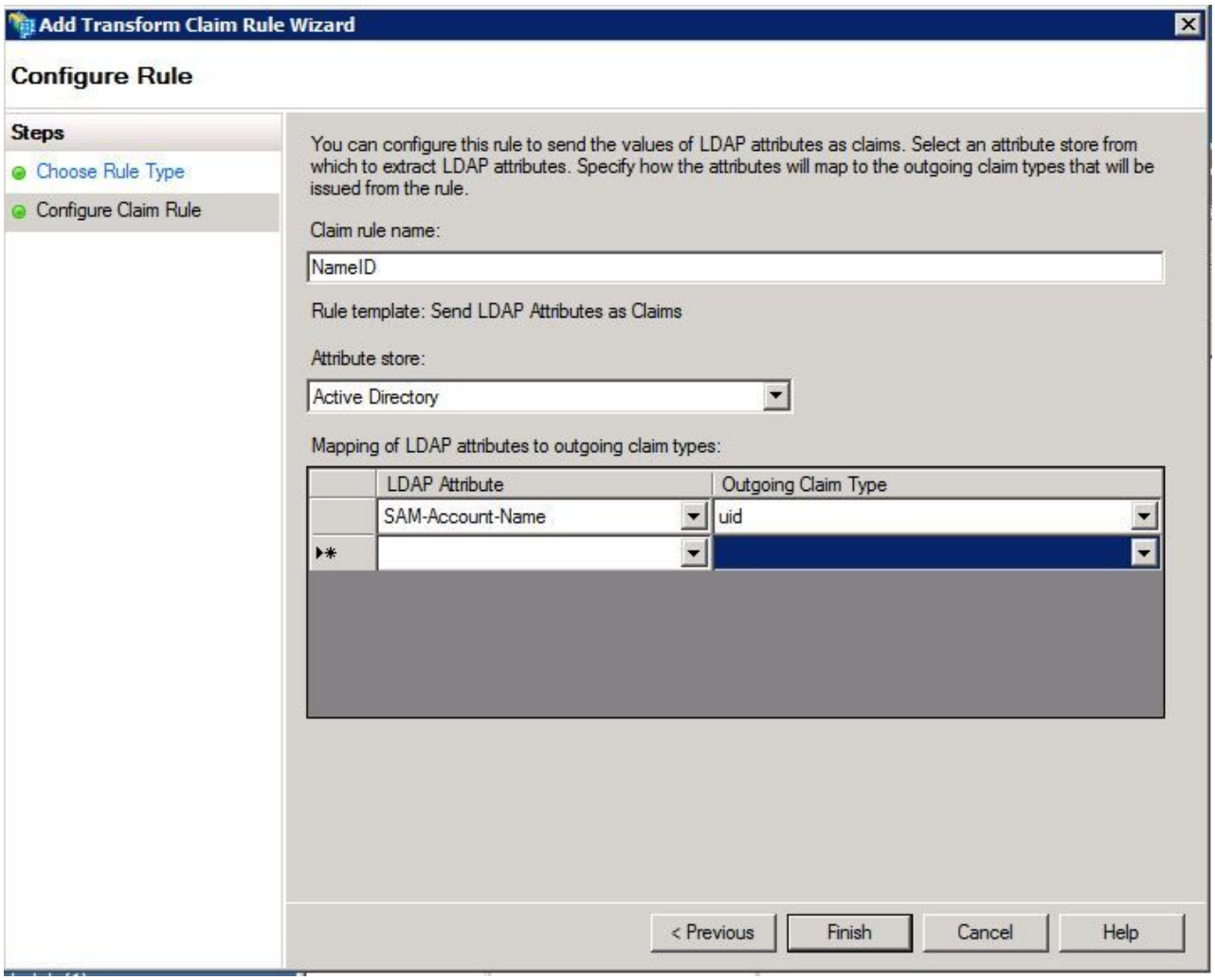
الخطوة 13. في الصفحة التالية، أدخل NameID لاسم قاعدة المطالبة.

الخطوة 14. أختر Active Directory لمخزن السمات.

الخطوة 15. أخترت SAM-account-name ل ال LDAP سمة.

الخطوة 16. أدخل id ل نوع المطالبة الصادرة.

ملاحظة: المعرف الفريد ليس خيارا في القائمة المنسدلة - يجب إدخاله يدويا.



الخطوة 17. انقر فوق إنهاء.

الخطوة 18. انتهت القاعدة الأولى الآن. انقر فوق إضافة قاعدة مرة أخرى.

الخطوة 19. أختر إرسال المطالبات باستخدام قاعدة مخصصة.

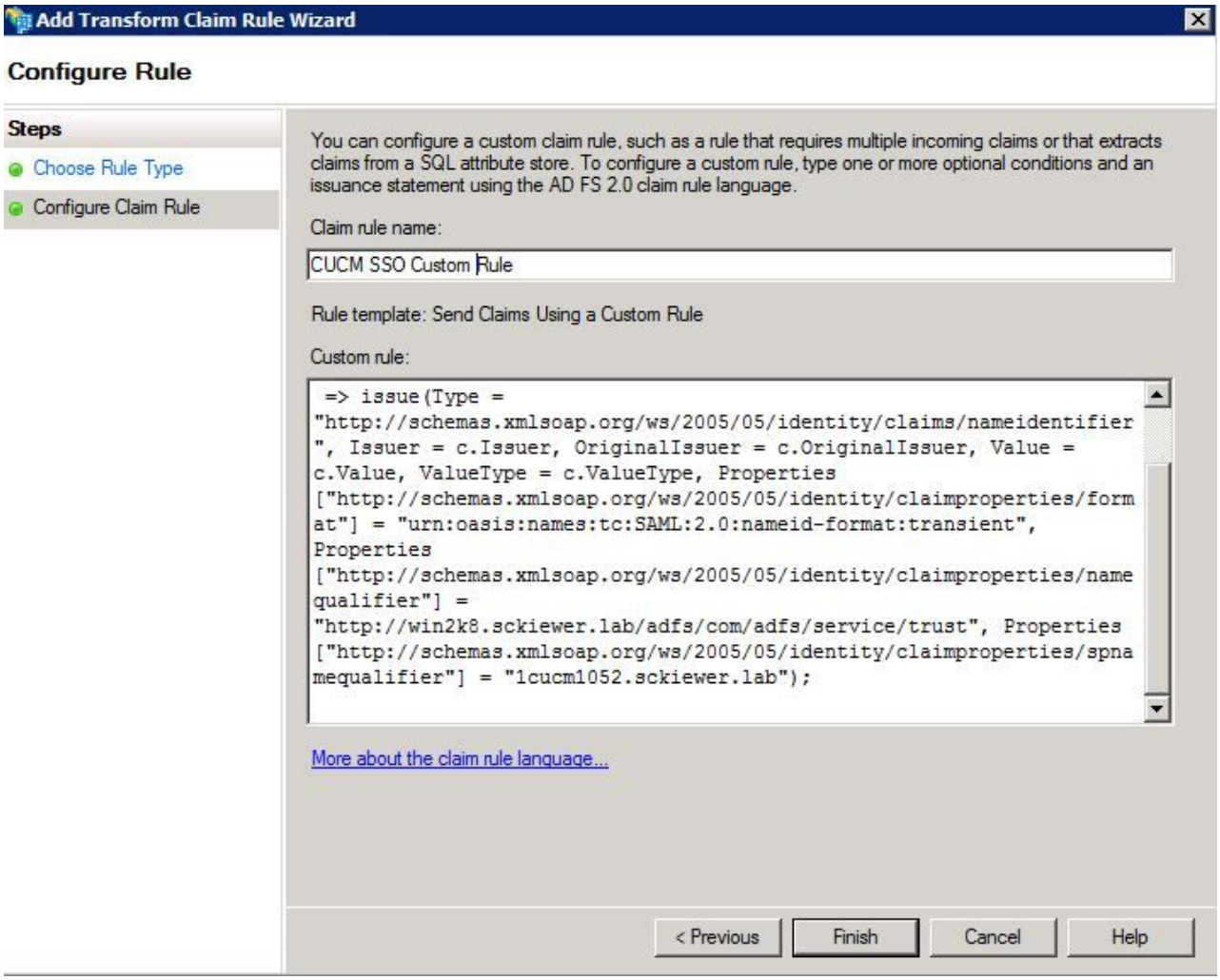
الخطوة 20. أدخل اسم قاعدة مطالبة.

الخطوة 21. في حقل القاعدة المخصصة، الصق هذا النص:

ج:[النوع == http://schemas.microsoft.com/ws/2008/06/identity/المطالبات/windowsAccountName] => إصدار(النوع = http://schemas.xmlsoap.org/ws/2005/05/identity/cltarget/nameIdentifier"، المصدر = c.Issuer، OriginalIssuer = c.OriginalIssuer، القيمة = c.Value، ValueType = c.ValueType، Properties["http://schemas.xmlsoap.org/ws/2005/05/الهوية/الكليات/التنسيق"] = "urn:oasis:names:tc:saml:2.0:nameid-format:transient،خصائص["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier" = http://ADFS_FEDERATION_SERVICE_NAME/com/adfs/service/trust"، Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] = "CUCM_ENTITY_ID")؛

الخطوة 22. تأكد من تغيير AD_FS_SERVICE_NAME و CUCM_ENTITY_ID إلى القيم المناسبة.

ملاحظة: إذا لم تكن متأكدا من اسم خدمة AD FS، يمكنك اتباع الخطوات للعثور عليه. يمكن سحب معرف كيان CUCM من السطر الأول في ملف بيانات تعريف CUCM. يوجد معرف كيان على السطر الأول من الملف وبدو كهذا، entityID=1cucm1052.sciewer.lab،. يجب إدخال القيمة المسطرة في القسم المناسب من قاعدة المطالبة.



الخطوة 23. انقر فوق إنهاء.

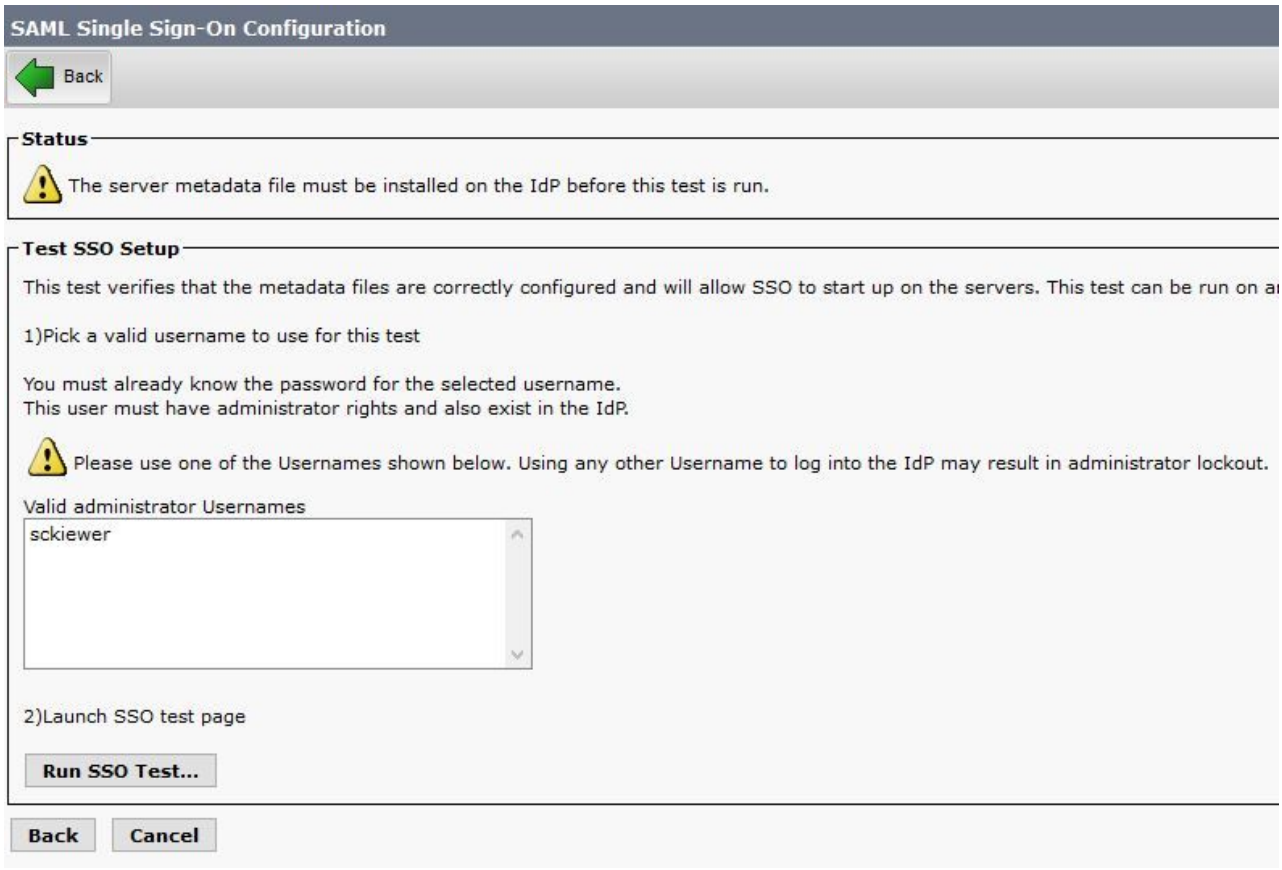
الخطوة 24. وانقر فوق OK.

ملاحظة: يلزم توفر قواعد المطالبات لأي خادم تعاون موحد تنوي إستخدام SSO عليه.

إنهاء تمكين SSO على CUCM وتشغيل إختبار SSO

الخطوة 1. الآن بعد تهيئة خادم AD FS بشكل كامل، يمكنك الرجوع إلى CUCM.

الخطوة 2. لقد توقفت في صفحة التكوين النهائي:



الخطوة 3. حدد المستخدم النهائي الذي تم تحديد دور CCM Super Users القياسي وانقر فوق تشغيل إختبار SSO...

الخطوة 4. تأكد من أن المستعرض الخاص بك يسمح بالإطارات المنبثقة، وأدخل بيانات الاعتماد الخاصة بك في موجه الأمر.

الخطوة 5. انقر إغلاق على النافذة المنبثقة، ثم إنهاء.

الخطوة 6. بعد إعادة تشغيل قصيرة لتطبيقات الويب، يتم تمكين SSO.

استكشاف الأخطاء وإصلاحها

تعيين سجلات SSO إلى تصحيح الأخطاء

لتعيين سجلات SSO إلى تصحيح الأخطاء، يجب عليك تشغيل هذا الأمر في CLI الخاص ب CUCM: set samltrace level debug

يمكن تنزيل سجلات SSO من RTMT. اسم مجموعة السجلات هو Cisco SSO.

البحث عن اسم خدمة الاتحاد

للعثور على اسم خدمة الاتحاد، انقر فوق بدء وابحث عن إدارة AD FS 2.0.

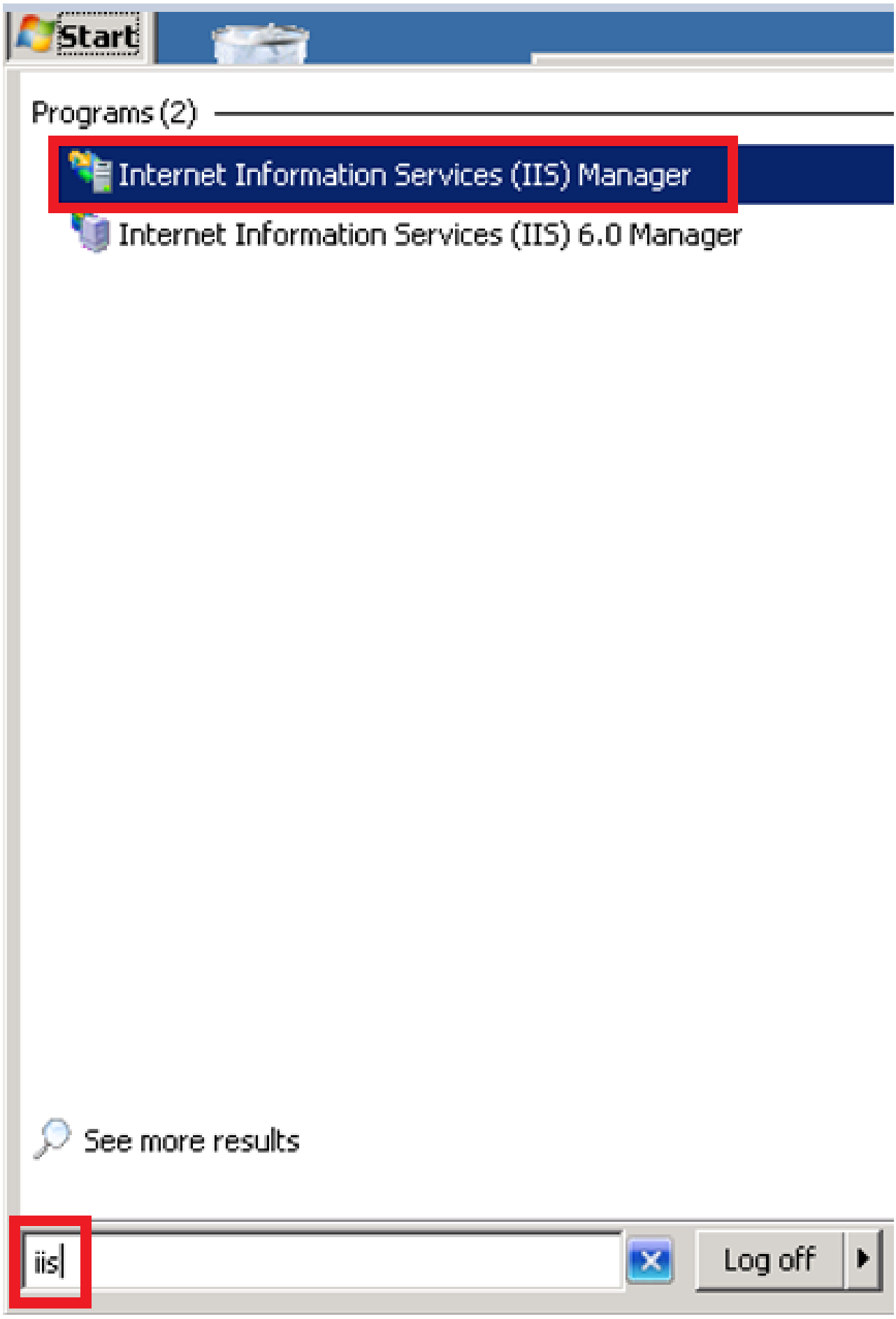
· انقر فوق تحرير خصائص خدمة الاتحاد...
· أثناء وجودك في علامة التبويب "عام"، ابحث عن اسم خدمة Federation

اسم خدمة Federation وDoWithout Certificate

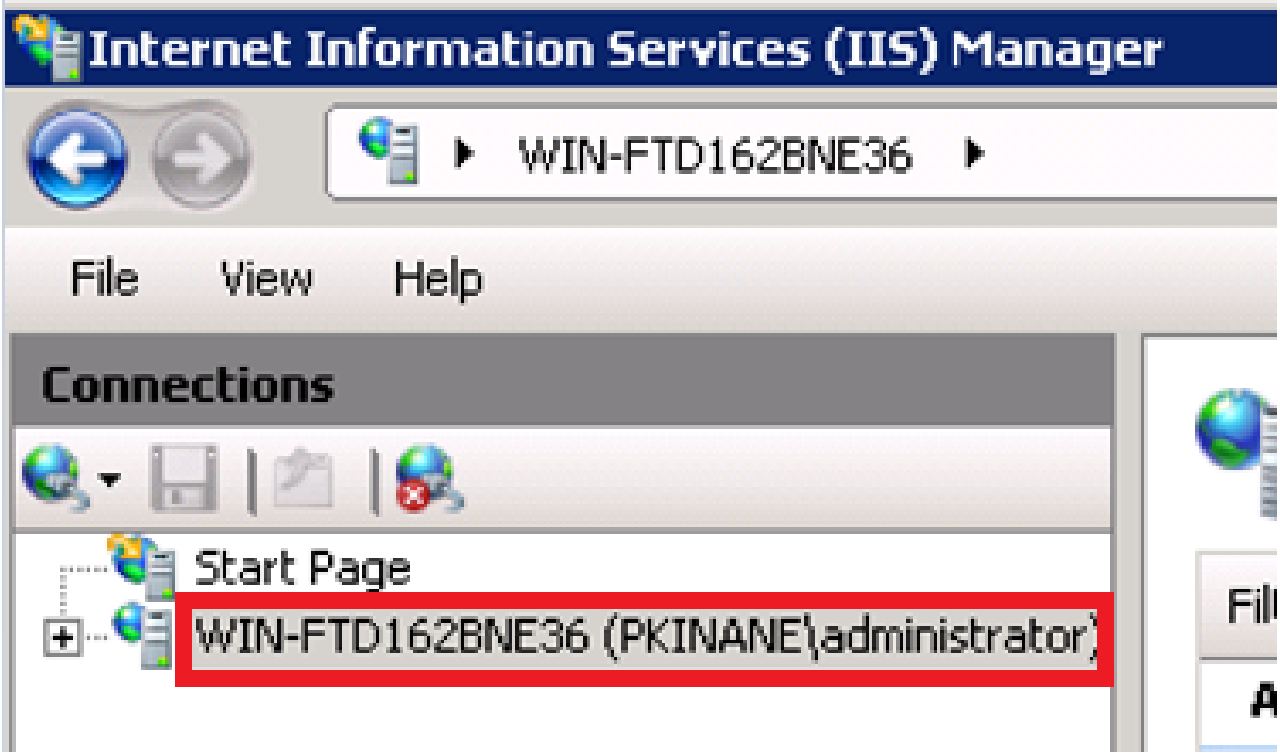
إذا إستلمت رسالة الخطأ هذه في معالج تكوين AD FS، فإنك تحتاج إلى إنشاء شهادة جديدة.

يتعذر إستخدام الشهادة المحددة لتحديد اسم خدمة الاتحاد لأن الشهادة المحددة لها اسم موضوع بال علامة (قصير الاسم). حدد شهادة أخرى بدون اسم موضوع بال علامة (مسمى قصير)، ثم حاول مرة أخرى.

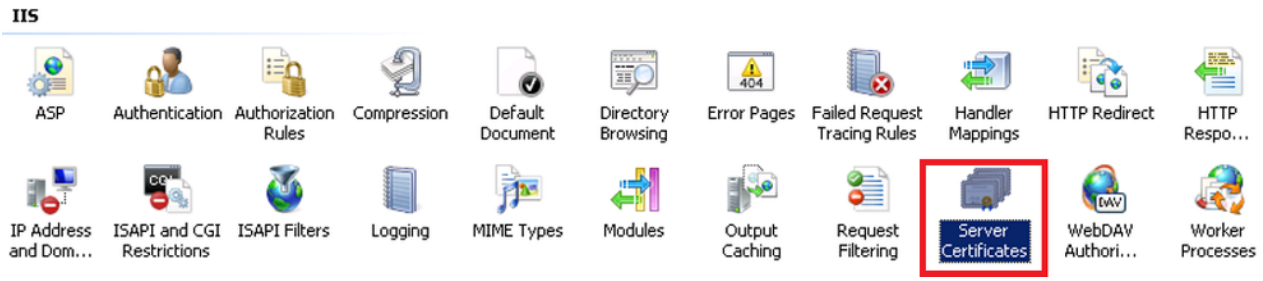
الخطوة 1. انقر فوق "أبدأ" وابحث عن IIS، ثم افتح "إدارة خدمات معلومات الإنترنت" (IIS)



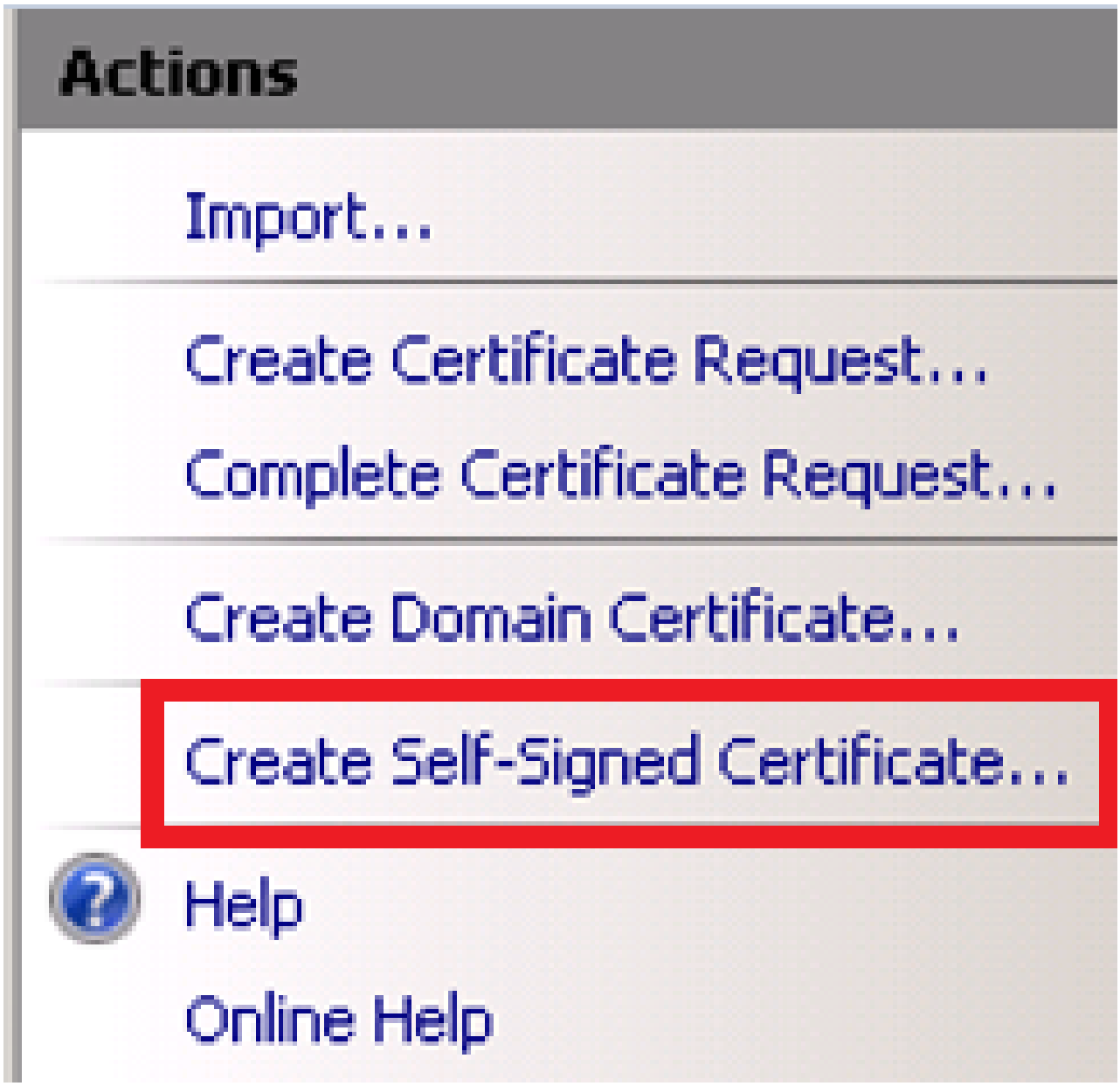
الخطوة 2. انقر فوق اسم الخادم.



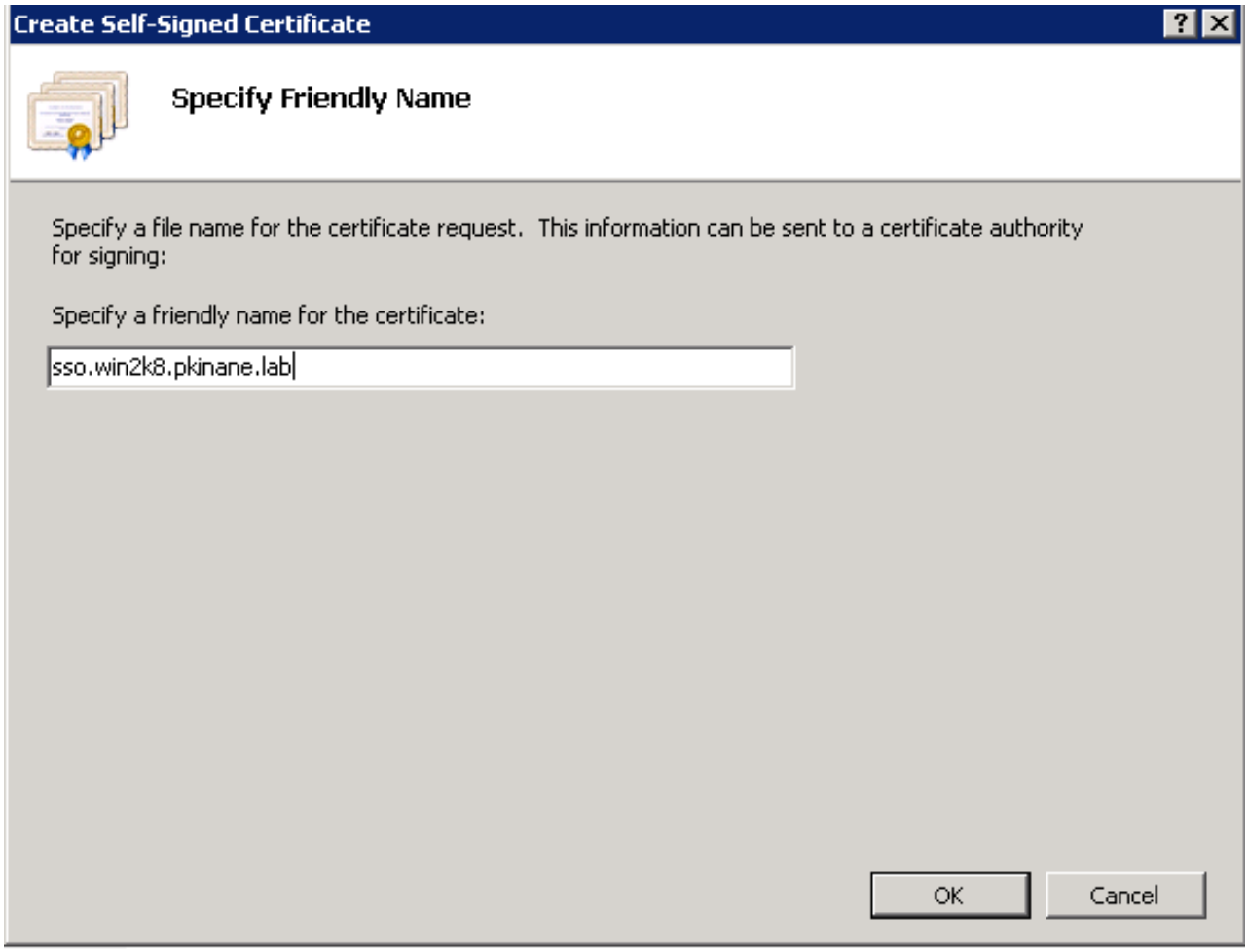
الخطوة 3. انقر على شهادات الخادم.



الخطوة 4. انقر إنشاء شهادة موقعة ذاتيا.



الخطوة 5. أدخل الاسم المستعار للشهادة.



الوقت غير متزامن بين خوادم CUCM و IDP

إذا إستلمت هذا خطأ عند تشغيل إختبار SSO من CUCM، تحتاج إلى تكوين Windows Server لاستخدام نفس خادم (خوادم) NTP مثل CUCM.

إستجابة SAML غير صالحة. وقد يحدث هذا عندما يكون الوقت غير متزامن بين مدير الاتصالات الموحدة من Cisco وخوادم IDP. الرجاء التحقق من تكوين NTP على كل الخادمين. قم بتشغيل "حالة بروتوكول وقت الشبكة (NTP)" من واجهة سطر الأوامر (CLI) للتحقق من هذه الحالة على Cisco Unified Communications Manager.

بمجرد أن يحتوي Windows Server على خوادم NTP الصحيحة المحددة، تحتاج إلى إجراء إختبار SSO آخر ومعرفة ما إذا كانت المشكلة مستمرة. وفي بعض الحالات، من الضروري تشويه فترة صحة التأكيد. المزيد من التفاصيل حول تلك العملية هنا.

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).