Kerberos مع ADFS 2.0 للمستخدم النهائي SAML SSO لمثال تكوين Jabber

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين Kerberos باستخدام خدمات إتحاد Active Directory (ADFS) 2.0.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يتطلب تكوين تسجيل الدخول الأحادي (SSO) الخاص ب تأكيد أمان المستخدم النهائي تكوين Kerberos للسماح للمستخدم النهائي SAML SSO ل Jabber بالعمل مع مصادقة المجال. عند تنفيذ SAML SSO باستخدام Kerberos، يقوم البروتوكول الخفيف للوصول إلى الدليل (LDAP) بمعالجة كل التخويل ومزامنة المستخدم، بينما يقوم Kerberos بإدارة المصادقة. Kerberos هو بروتوكول مصادقة تم إستخدامه بالاقتران مع المثيل الذي تم تمكين

LDAP به.

على أجهزة Microsoft Windows و Macintosh المرتبطة بمجال Active Directory، يمكن للمستخدمين تسجيل الدخول إلى Cisco Jabber بسلاسة دون الحاجة إلى إدخال اسم مستخدم أو كلمة مرور ولا يشاهدون حتى شاشة تسجيل دخول. لا يزال المستخدمون الذين لم يتم تسجيل دخولهم إلى المجال على أجهزة الكمبيوتر لديهم يرون نموذج تسجيل دخول قياسي.

نظرا لأن المصادقة تستخدم رمزا مميزا فرديا تم تمريره من أنظمة التشغيل، فلا حاجة لإعادة التوجيه. يتم التحقق من الرمز المميز مقابل وحدة التحكم بالمجال الأساسية (KDC) التي تم تكوينها، وإذا كان صحيحا، فيتم تسجيل دخول المستخدم.

التكوين

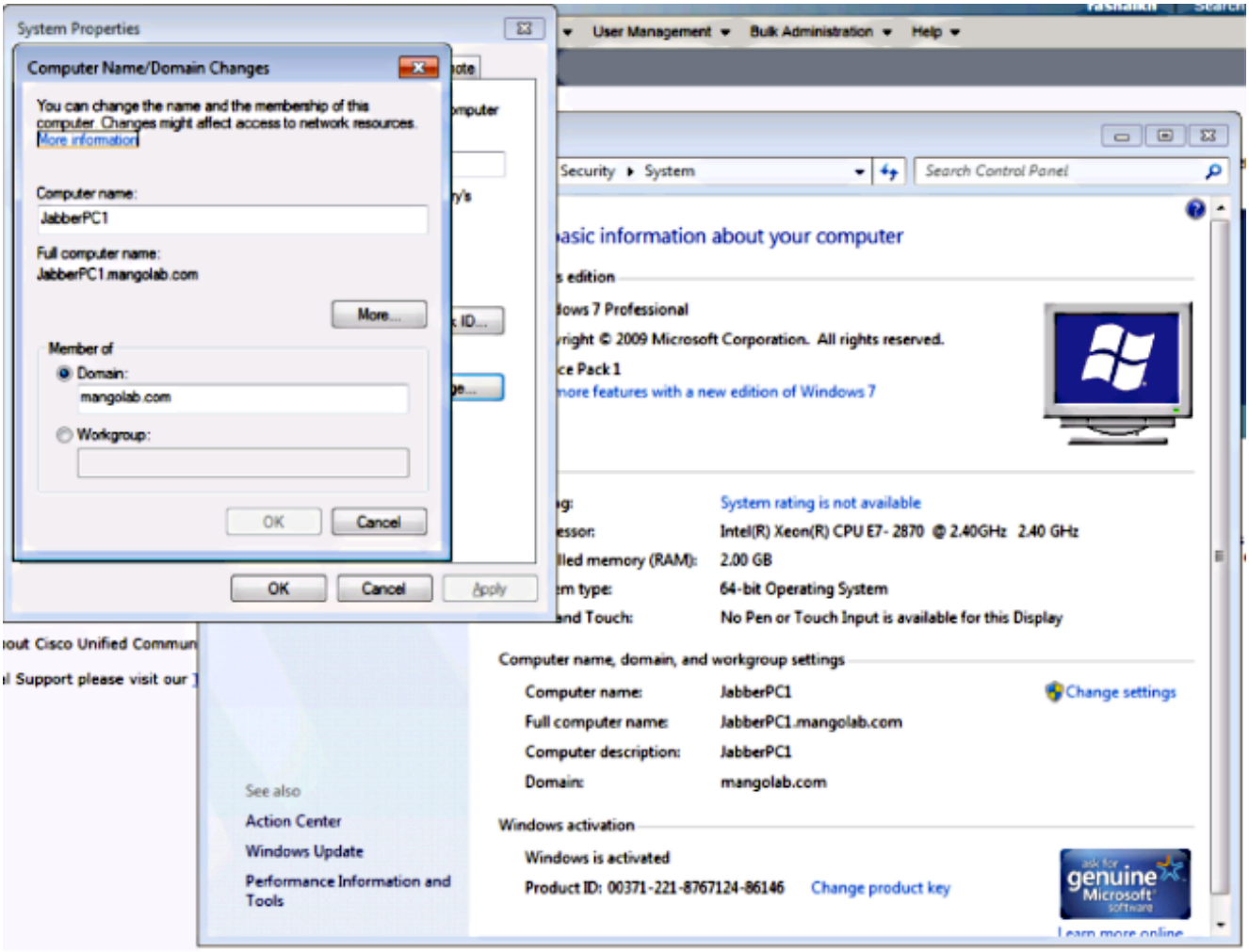
فيما يلي الإجراء لتكوين Kerberos باستخدام ADFS 2.0.

1. تثبيت Microsoft Windows Server 2008 R2 على جهاز.
2. تثبيت خدمات مجال خدمة Active Directory (ADDS) و ADFS على نفس الجهاز.
3. تثبيت "خدمات معلومات الإنترنت" (IIS) على الجهاز المثبت على Microsoft Windows Server 2008 R2.
4. إنشاء شهادة موقعة ذاتيا ل IIS.
5. قم باستيراد الشهادة الموقعة ذاتيا إلى IIS واستخدمها كشهادة خادم HTTPS.
6. قم بتثبيت Microsoft Windows7 على جهاز آخر واستخدمه كعميل.

قم بتغيير خادم اسم المجال (DNS) إلى الجهاز الذي قمت بتثبيت "إضافة" فيه.

أضف هذا الجهاز إلى المجال الذي أنشأته في تثبيت ADDS.

انتقل إلى **البدء**.انقر بزر الماوس الأيمن على **الكمبيوتر**.انقر فوق **خصائص**.انقر على **تغيير الإعدادات** في الجانب الأيمن من النافذة.انقر على **علامة التبويب اسم الكمبيوتر**.طقطقة **تغير**.إضافة المجال الذي قمت بإنشائه.



7. تحقق ما إذا كانت خدمة Kerberos تقوم بتوليد على كلا الجهازين.

قم بتسجيل الدخول كمسؤول على جهاز الخادم وافتح موجه الأوامر. بعد ذلك قم بتنفيذ هذه الأوامر:

القرص المضغوط \Windows\System32تذاكر قائمة

```
C:\Users\Administrator.WIN2K8>cd \windows\System32

C:\Windows\System32>Klist tickets

Current LogonId is 0:0x3d6072

Cached Tickets: (1)

#0>     Client: Administrator @ MANGOLAB.COM
        Server: krbtgt/MANGOLAB.COM @ MANGOLAB.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
        Start Time: 12/10/2014 18:06:04 (local)
        End Time:   12/11/2014 4:06:04 (local)
        Renew Time: 12/17/2014 18:06:04 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
```

قم بتسجيل الدخول كمستخدم مجال على جهاز العميل وقم بتنفيذ الأوامر نفسها.

```
C:\Users\rashaikh>cd \windows\System32

C:\Windows\System32>Klist tickets

Current LogonId is 0:0x558ba

Cached Tickets: (5)

#0>     Client: rashaikh @ MANGOLAB.COM
        Server: krbtgt/MANGOLAB.COM @ MANGOLAB.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x60a00000 -> forwardable forwarded renewable pre_authent
        Start Time: 12/10/2014 18:35:23 (local)
        End Time:   12/11/2014 4:34:59 (local)
        Renew Time: 12/17/2014 18:34:59 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96

#1>     Client: rashaikh @ MANGOLAB.COM
        Server: krbtgt/MANGOLAB.COM @ MANGOLAB.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
        Start Time: 12/10/2014 18:34:59 (local)
        End Time:   12/11/2014 4:34:59 (local)
        Renew Time: 12/17/2014 18:34:59 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96

#2>     Client: rashaikh @ MANGOLAB.COM
        Server: LDAP/win2k8.mangolab.com/mangolab.com @ MANGOLAB.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_deleg
ate
        Start Time: 12/10/2014 19:05:15 (local)
        End Time:   12/11/2014 4:34:59 (local)
        Renew Time: 12/17/2014 18:34:59 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96

#3>     Client: rashaikh @ MANGOLAB.COM
        Server: HTTP/win2k8.mangolab.com @ MANGOLAB.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_deleg
ate
        Start Time: 12/10/2014 18:35:23 (local)
        End Time:   12/11/2014 4:34:59 (local)
        Renew Time: 12/17/2014 18:34:59 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96

#4>     Client: rashaikh @ MANGOLAB.COM
        Server: LDAP/win2k8.mangolab.com @ MANGOLAB.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_deleg
ate
        Start Time: 12/10/2014 18:35:05 (local)
        End Time:   12/11/2014 4:34:59 (local)
        Renew Time: 12/17/2014 18:34:59 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96

C:\Windows\System32>_
```

8. قم بإنشاء هوية ADFS Kerberos على الجهاز حيث قمت بتثبيت ADDS.

قام مسؤول Microsoft Windows بتسجيل الدخول إلى مجال Microsoft Windows (باسم <domainName>\administrator)، على سبيل المثال على وحدة التحكم بالمجال ل Microsoft Windows، بإنشاء هوية ADFS Kerberos. يجب أن تحتوي خدمة ADFS HTTP على هوية Kerberos تسمى اسم الخدمة الأساسي (SPN) بهذا التنسيق: **HTTP/DNS_name_of_ADFS_server**.

يجب تعيين هذا الاسم لمستخدم Active Directory الذي يمثل مثيل خادم ADFS HTTP. أستخدم الأداة المساعدة ل **SetSPN** Microsoft Windows، والتي يجب أن تكون متوفرة بشكل افتراضي على خادم

.Microsoft Windows 2008

الإجراء قم بتسجيل SPNs لخادم ADFS. على وحدة التحكم بمجال Active Directory، قم بتشغيل الأمر **setSPN**.

على سبيل المثال، عندما يكون مضيف ADFS هو **adfs01.us.renovations.com**، ويكون مجال Active Directory هو **US.RENOVATIONS.COM**، فإن الأمر هو:

```
setspn -a HTTP/adfs01.us.renovations.com
```

يتم تطبيق جزء **HTTP/** من SPN، حتى وإن كان خادم ADFS يتم الوصول إليه عادة من خلال طبقة مآخذ التوصيل الآمنة (SSL)، والتي هي HTTPS.

تحقق من أن SPNs لخادم ADFS تم إنشائها بشكل صحيح باستخدام أمر **setSPN** وعرض المخرجات.

```
setspn -L
```

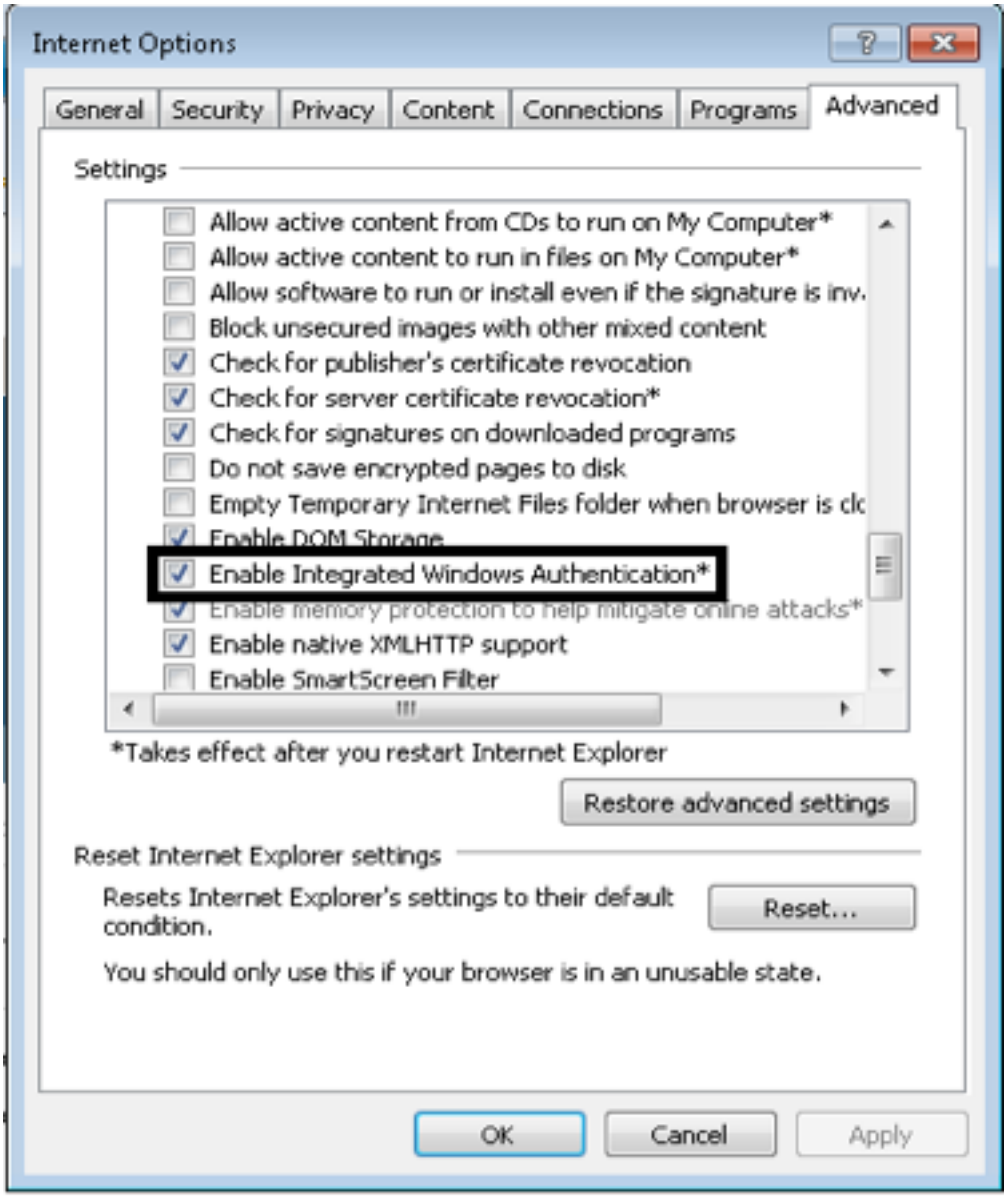
```
C:\Windows\System32>setspn -L win2k8
Registered ServicePrincipalNames for CN=WIN2K8,OU=Domain Controllers,DC=mangolab
,DC=com:
        HTTP/win2k8.mangolab.com
        ldap/win2k8.mangolab.com/ForestDnsZones.mangolab.com
        ldap/win2k8.mangolab.com/DomainDnsZones.mangolab.com
        TERMSRV/WIN2K8
        TERMSRV/win2k8.mangolab.com
        Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/win2k8.mangolab.com
        DNS/win2k8.mangolab.com
        GC/win2k8.mangolab.com/mangolab.com
        RestrictedKrbHost/win2k8.mangolab.com
        RestrictedKrbHost/WIN2K8
        HOST/WIN2K8/MANGOLAB
        HOST/win2k8.mangolab.com/MANGOLAB
        HOST/WIN2K8
        HOST/win2k8.mangolab.com
        HOST/win2k8.mangolab.com/mangolab.com
        E3514235-4B06-11D1-AB04-00C04FC2DCD2/bf221b06-fbc5-4dc3-b472-562f9238374
7/mangolab.com
        ldap/WIN2K8/MANGOLAB
        ldap/bf221b06-fbc5-4dc3-b472-562f92383747._msdcs.mangolab.com
        ldap/win2k8.mangolab.com/MANGOLAB
        ldap/WIN2K8
        ldap/win2k8.mangolab.com
        ldap/win2k8.mangolab.com/mangolab.com

C:\Windows\System32>_
```

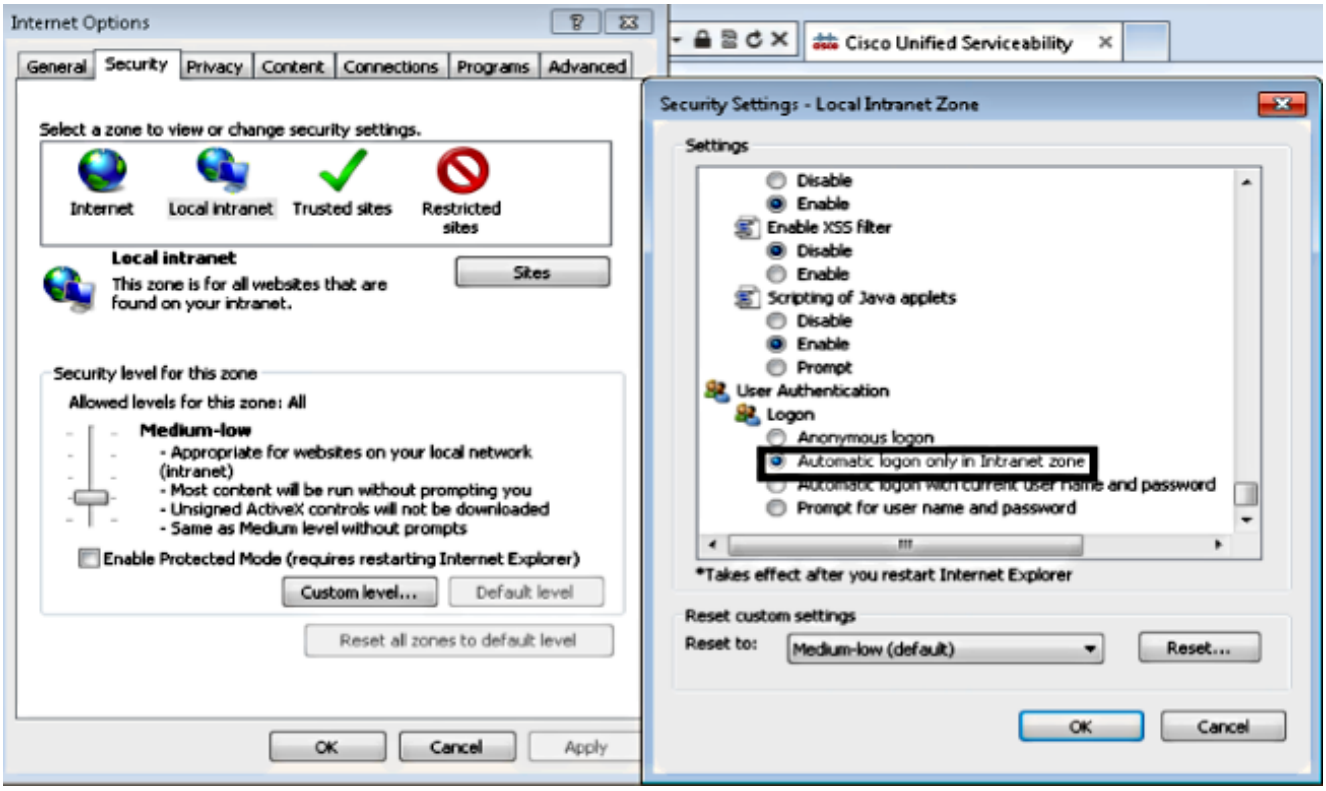
9. قم بتكوين إعدادات المستعرض لعميل Microsoft Windows.

انتقل إلى **أدوات > InternetOptions > متقدمة** لتمكين المصادقة المتكاملة ل Windows.

حدد خانة الاختيار **تمكين مصادقة Windows المتكاملة**:

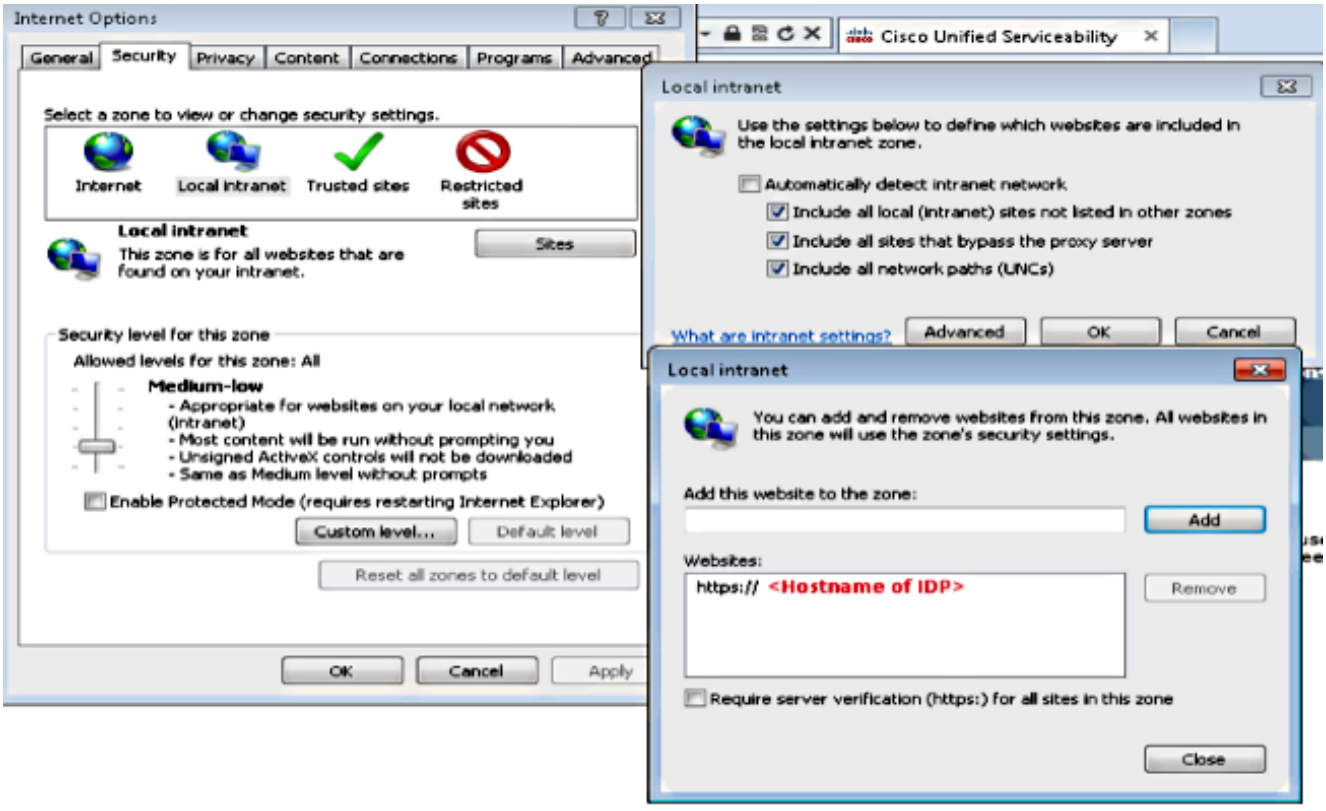


انتقل إلى **أدوات > خيارات الإنترنت > الأمان > إنترانت المحلية > مستوى مخصص..** لتحديد **تسجيل الدخول التلقائي فقط في منطقة إنترانت**.

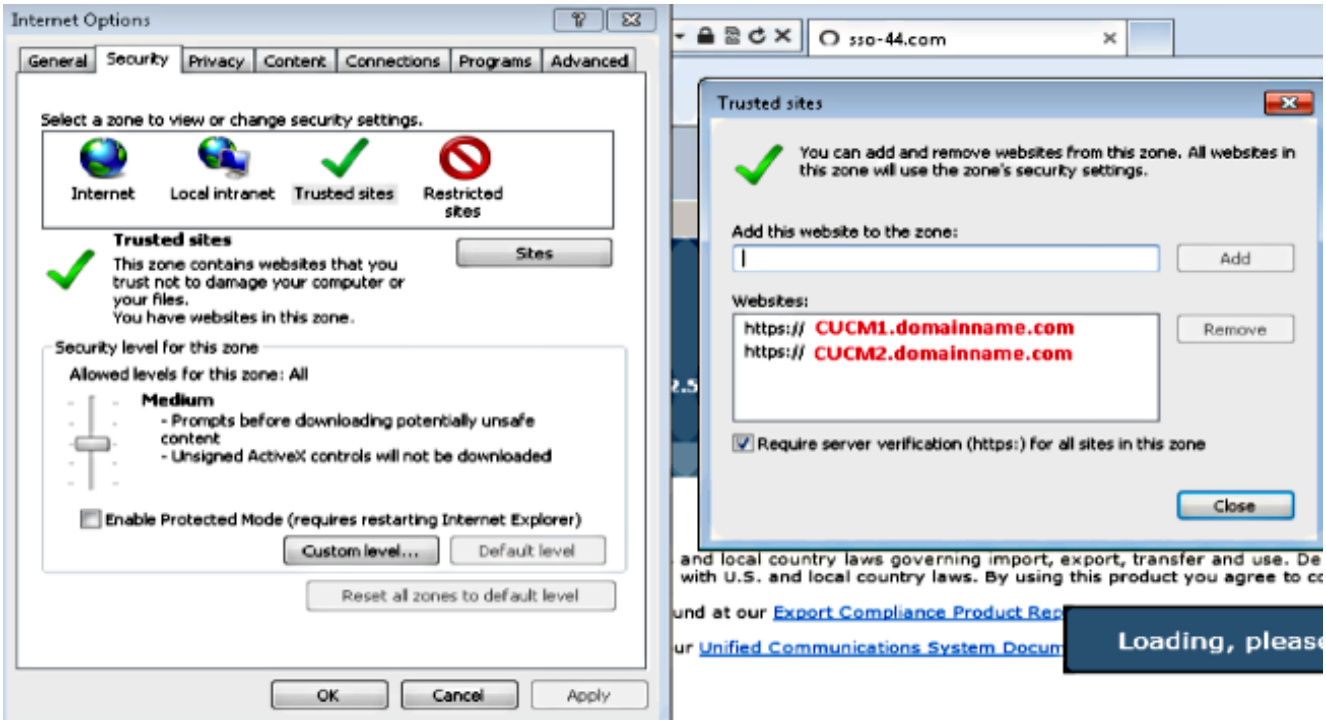


انتقل إلى **أدوات > خيارات الإنترنت > الأمان > إنترانت المحلية > المواقع > خيارات متقدمة** لإضافة عنوان URL لاكتشاف التسلل ومنعه (IDP) إلى مواقع إنترانت المحلية.

ملاحظة: تحقق من كافة خانات الاختيار الموجودة في شاشة إنترانت المحلية وانقر فوق **علامة التبويب خيارات متقدمة**.



انتقل إلى **أدوات > التأمين > المواقع الموثوق بها > المواقع** لإضافة أسماء مضيف CUCM إلى المواقع الموثوق بها:

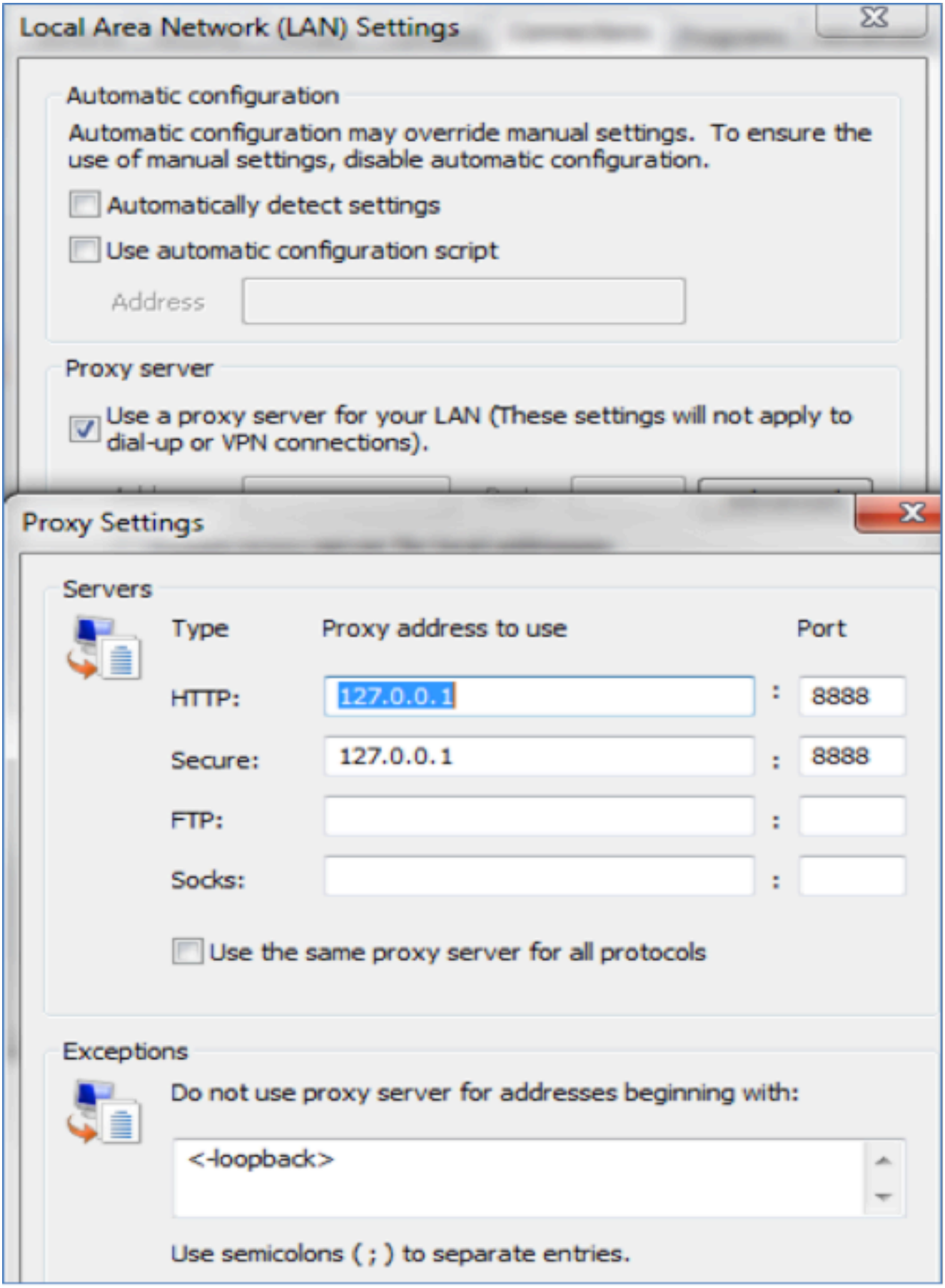


التحقق من الصحة

يشرح هذا القسم كيفية التحقق من المصادقة (مصادقة Kerberos أو مصادقة مدير شبكة LAN (NTLM المستخدمة.

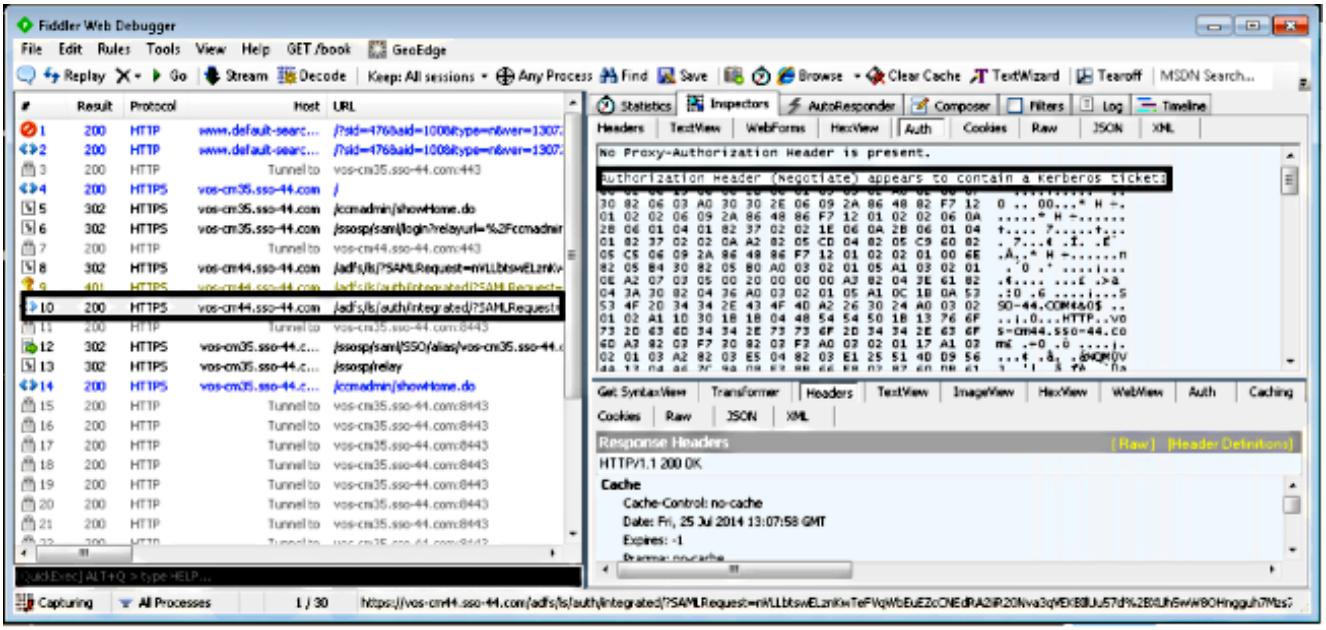
1. قم بتنزيل أداة Fiddler إلى جهاز العميل وقم بتثبيتها.
2. إغلاق كافة نوافذ Internet Explorer.
3. قم بتشغيل أداة الفواصل وتحقق من أن خيار **التقاط حركة مرور** متاح تحت قائمة الملف.

يعمل Fiddler كوكيل مرور بين جهاز العميل والخادم ويستمع إلى كل حركة مرور، والتي تقوم مؤقتا بتعيين إعدادات Internet Explorer مثل:

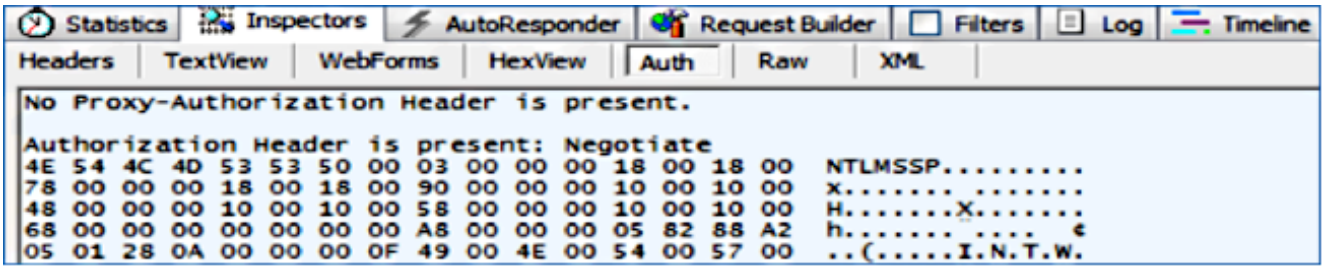


4. افتح Internet Explorer، واستعرض عنوان URL لخادم إدارة علاقات العملاء (CRM)، وانقر فوق بعض الارتباطات لإنشاء حركة مرور البيانات.

5. ارجع إلى نافذة Fiddler الرئيسية واختر أحد الإطارات حيث تكون النتيجة 200 (نجاح):



إذا كان نوع المصادقة NTLM، فأنت ترى **التفاوض - NTLMSSP** في بداية الإطار، كما هو موضح هنا:



استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

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).