

# ةق داصم مادخت ساب SAML SSO دادع| نيوكت Kerberos

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [التكوين](#)
- [تهيئة AD FS](#)
- [تكوين المستعرض](#)
- [برنامج Microsoft Internet Explorer](#)
- [Mozilla Firefox](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)

## المقدمة

يوضح هذا المستند كيفية تكوين الإصدار 2.0 من خدمة اتحاد خدمة (AD FS) Active Directory و (Active Directory) Directory لتمكينها من استخدام مصادقة Kerberos بواسطة عملاء Jabber (في Microsoft Windows فقط)، والتي تتيح للمستخدمين تسجيل الدخول باستخدام تسجيل الدخول إلى Microsoft Windows وعدم مطالبهم ببيانات الاعتماد.

تحذير: يستند هذا المستند إلى بيئة معملية ويفترض أنك على دراية بتأثير التغييرات التي تقوم بها. ارجع إلى وثائق المنتج ذات الصلة لفهم تأثير التغييرات التي تقوم بها.

## المتطلبات الأساسية

### المتطلبات

توصي Cisco بأن يكون لديك:

- AD FS الإصدار 2.0 المثبت والمهيئة باستخدام منتجات التعاون من Cisco كثقة جهة معتمدة
- منتجات التعاون مثل المراسلة الفورية IM and Cisco Unified Communications Manager (CUCM) (Presence، Cisco Unity Connection (UCXN)، و CUCM الممكنة من أجل استخدام لغة تمييز تأكيد الأمان (SAML) تسجيل الدخول الأحادي (SSO)

### المكونات المستخدمة

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

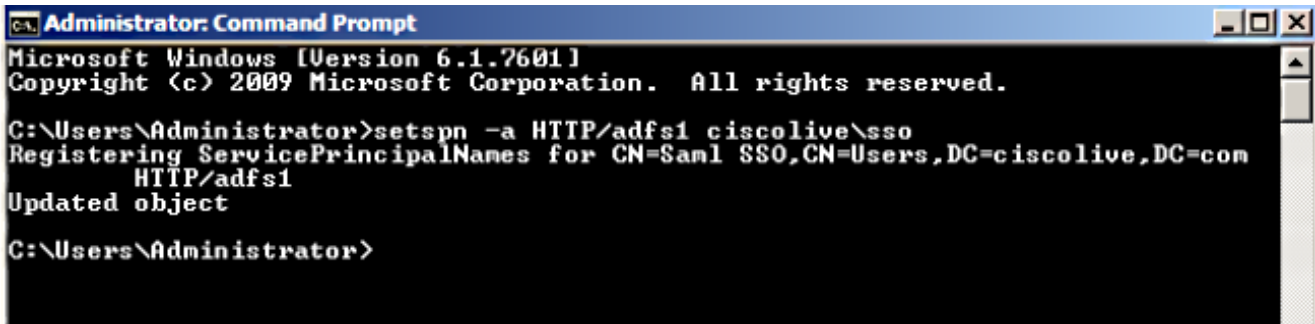
- Active Directory 2008 (اسم المضيف: ADFS1.ciscolive.com)
- AD FS الإصدار 2.0 (اسم المضيف: ADFS1.ciscolive.com)
- CUCM (اسم المضيف: CUCM1.ciscolive.com)
- Microsoft Internet Explorer، الإصدار 10
- موزيلا فايرفوكس الإصدار 34
- تيلريك فيدler الإصدار 4

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

## التكوين

### تهيئة AD FS

قم بتكوين AD FS الإصدار 2.0 باستخدام اسم الخدمة الأساسي (SPN) لتمكين كمبيوتر العميل المثبت عليه 1. Jabber لطلب التذاكر، مما يمكن كمبيوتر العميل بدوره من الاتصال بخدمة AD FS.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>setspn -a HTTP/adfs1 ciscolive\sso
Registering ServicePrincipalNames for CN=Saml SSO,CN=Users,DC=ciscolive,DC=com
HTTP/adfs1
Updated object
C:\Users\Administrator>
```

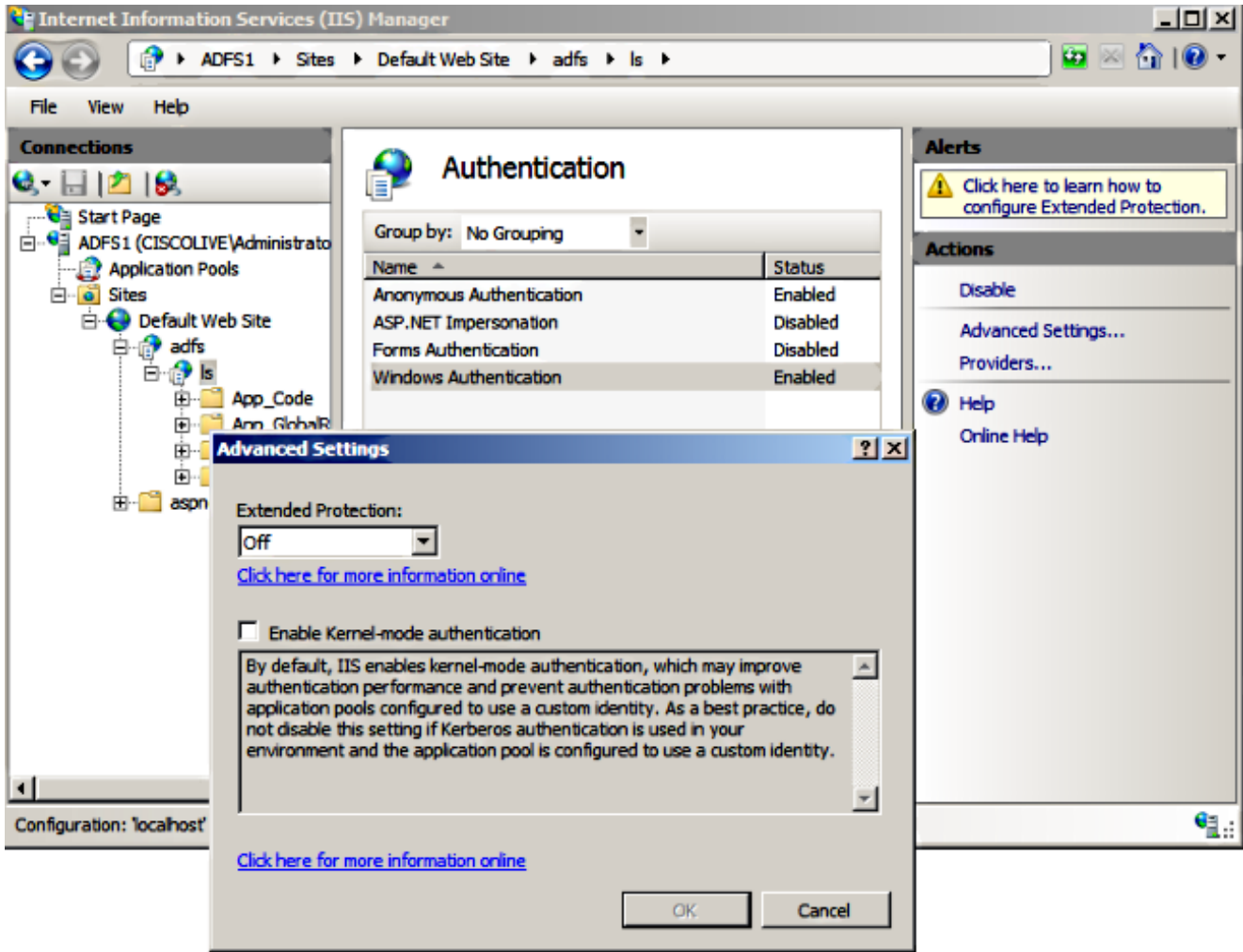
راجع [AD FS 2.0: كيفية تكوين \(servicePrincipalName\) \(SPN\) لحساب الخدمة](#) للحصول على مزيد من المعلومات.

تأكد من أن تكوين المصادقة الافتراضي لخدمة AD FS (في C:\inetpub\adfs\ls\web.config) هو مصادقة Windows المدمجة. تأكد من أنه لم يتم تغييره إلى مصادقة مستندة إلى نموذج.

```
<microsoft.identityServer.web>
  <localAuthenticationTypes>
    <add name="Integrated" page="auth/integrated/" />
    <add name="Forms" page="Formssignin.aspx" />
    <add name="TlsClient" page="auth/sslclient/" />
    <add name="Basic" page="auth/basic/" />
  </localAuthenticationTypes>
  <commonDomainCookie writer="" reader="" />
  <context hidden="true" />
  <error page="Error.aspx" />
  <acceptedFederationProtocols saml="true" wsFederation="true" />
  <homeRealmDiscovery page="HomeRealmDiscovery.aspx" />
  <persistIdentityProviderInformation enabled="true" lifetimeInDays="30" />
  <singleSignon enabled="true" />
</microsoft.identityServer.web>
```

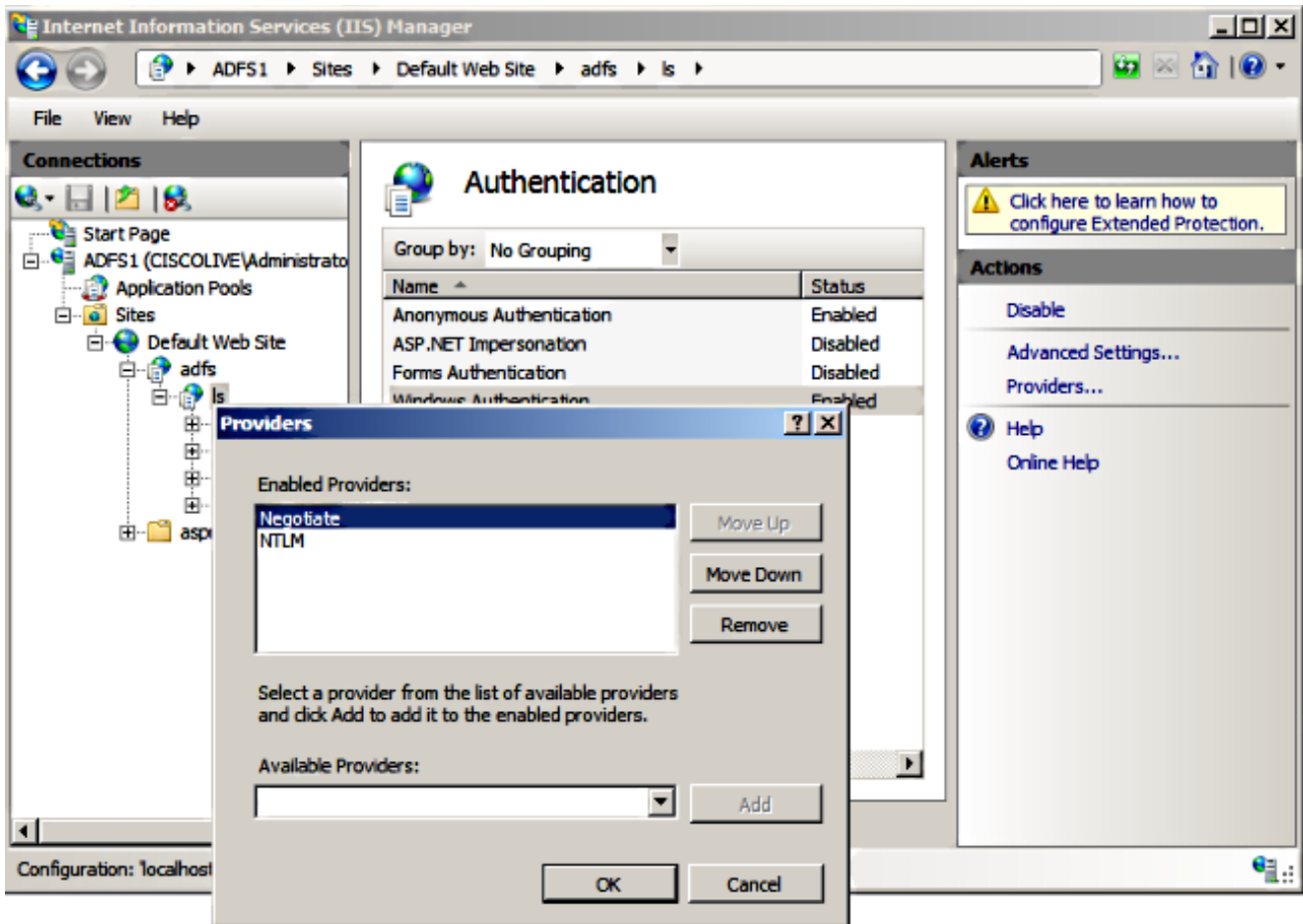
3. حدد مصادقة Windows وانقر فوق إعدادات متقدمة أسفل الجزء الأيمن. في الإعدادات المتقدمة، قم بإلغاء

تحديد تمكين مصادقة وضع kernel، وتأكد من إيقاف تشغيل الحماية الموسعة، ثم انقر على موافق.



تأكد من أن AD FS الإصدار 2.0 يدعم كلا من بروتوكول Kerberos وبروتوكول مدير شبكة NTLM (NTLMA) لأن جميع العملاء بخلاف Windows لا يمكنهم استخدام Kerberos والاعتماد على NTLM.

في الجزء الأيمن، حدد الموفرين وتأكد من وجود التفاوض وNTLM ضمن الموفرين الذين تم تمكينهم:



ملاحظة: يمرر AD FS رأس أمان التفاوض عند استخدام مصادقة Windows المتكاملة لمصادقة طلبات العميل. يتيح رأس أمان التفاوض للعملاء إمكانية التحديد بين مصادقة Kerberos ومصادقة NTLM. تحدد عملية التفاوض مصادقة Kerberos ما لم يكن أحد هذه الشروط صحيحاً:

- يتعذر على أحد الأنظمة المشاركة في المصادقة استخدام مصادقة Kerberos.

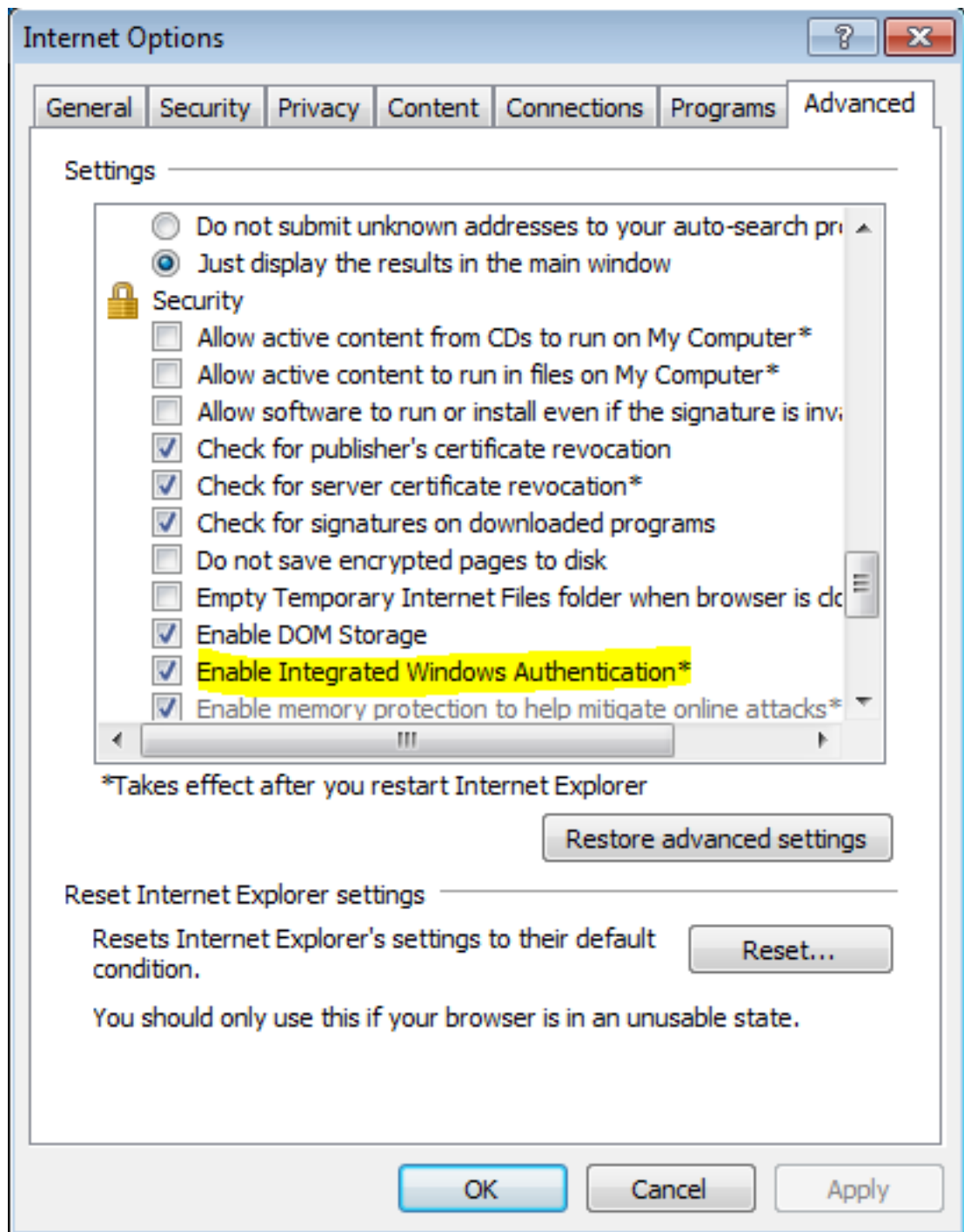
- لا يوفر تطبيق الاتصال معلومات كافية لاستخدام مصادقة Kerberos.

- لتمكين عملية التفاوض لتحديد بروتوكول Kerberos لمصادقة الشبكة، يجب أن يوفر تطبيق العميل اسم SPN أو اسم مستخدم أساسي (UPN) أو اسم حساب نظام الإدخال/الإخراج الأساسي للشبكة (NetBIOS) كاسم هدف. وإلا، فتقوم عملية التفاوض دائماً بتحديد بروتوكول NTLM كطريقة المصادقة المفضلة.

## تكوين المستعرض

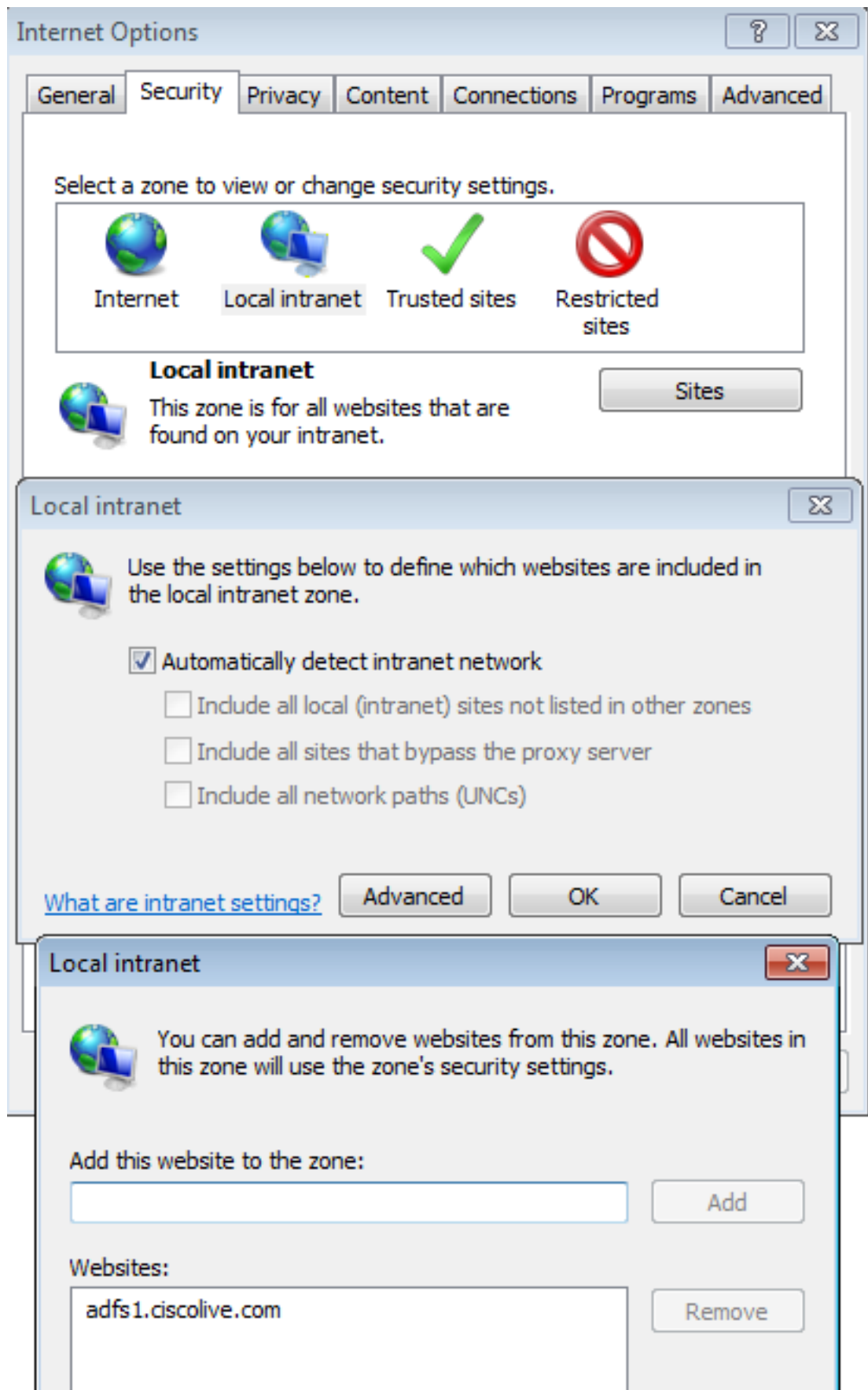
برنامج Microsoft Internet Explorer

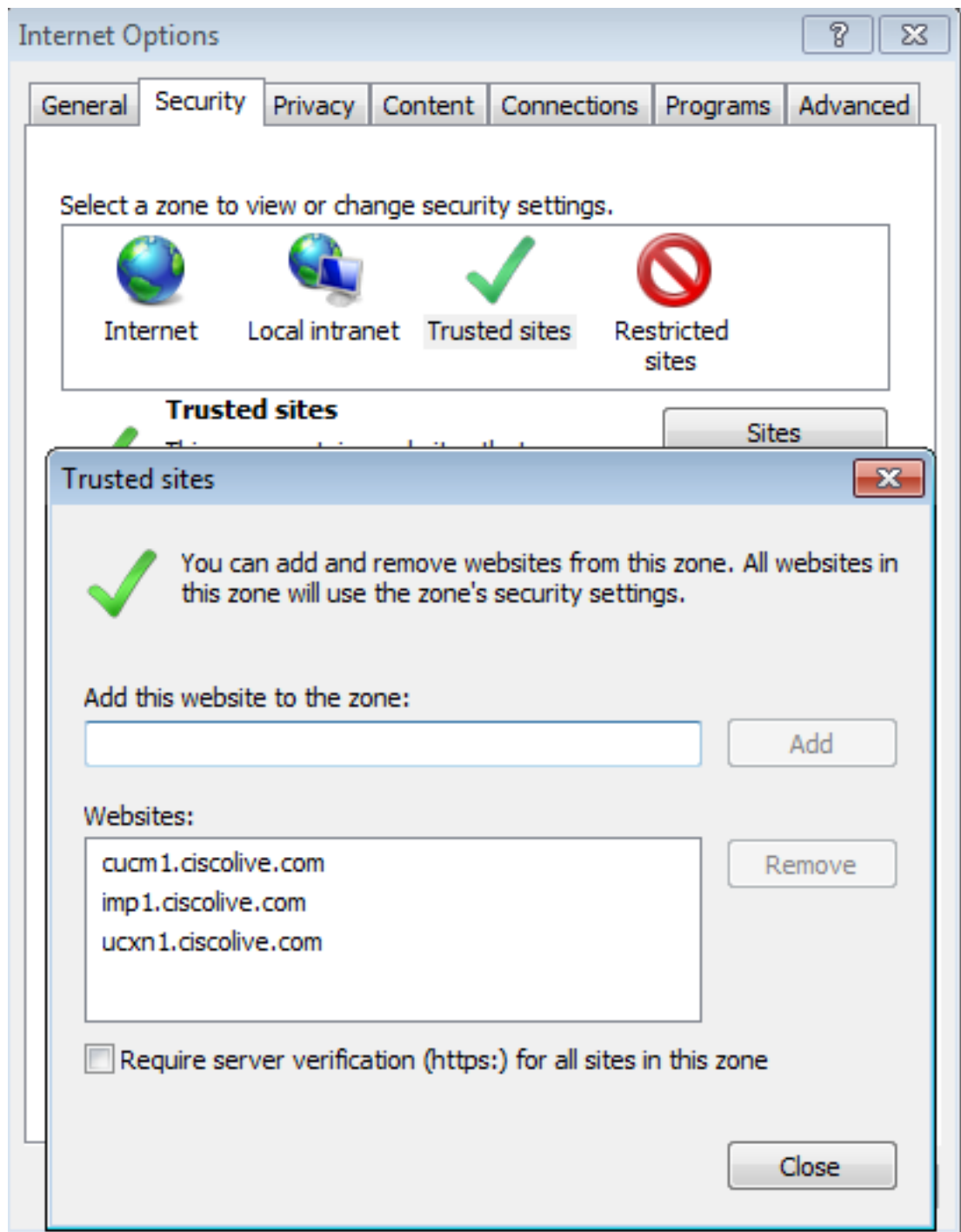
1. تأكد من أن Internet Explorer < متقدم > تمكين المصادقة المتكاملة ل Windows تم التحقق.



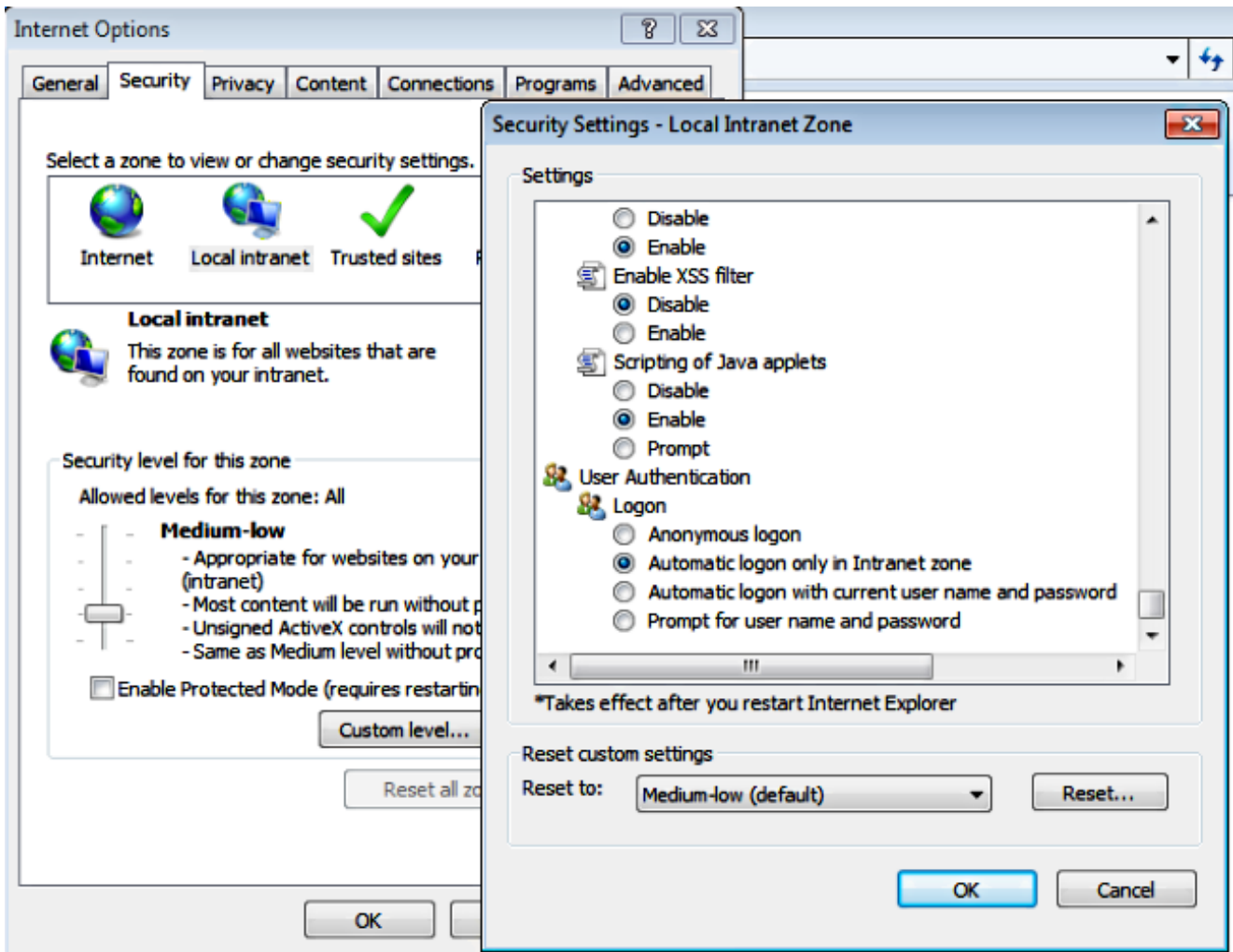
.2

إضافة عنوان URL ل AD FS تحت الأمان <مناطق إترانت > المواقع.



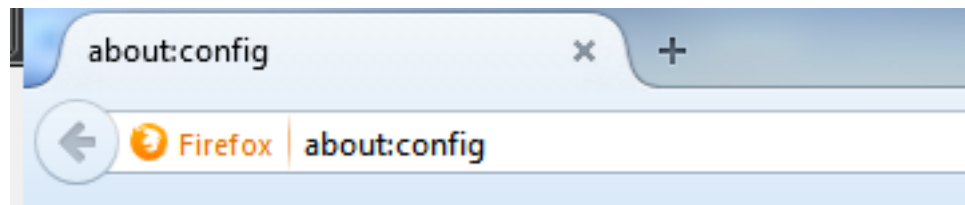


تأكد من أن Internet Explorer < أمان > إترانت المحلية < إعدادات الأمان > مصادقة المستخدم - تم تكوين 4. تسجيل الدخول لاستخدام بيانات الاعتماد التي تم تسجيل الدخول لمواقع إترانت.



## Mozilla Firefox

1. افتح Firefox وأدخل حول:config في شريط العناوين.



2. انقر سأكون حذرا، أعدك!





3. انقر نقرًا مزدوجًا على اسم التفضيل `network.negotiate-auth.allow non-fqdn` إلى `true` و `network.negotiate-auth.trusted-uris` إلى `ciscolive.com.adfs1.ciscolive.com` من أجل التعديل.

Preference Name	Status	Type	Value
<code>network.negotiate-auth.allow-insecure-ntlm-v1</code>	default	boolean	false
<code>network.negotiate-auth.allow-insecure-ntlm-v1-https</code>	default	boolean	true
<b><code>network.negotiate-auth.allow-non-fqdn</code></b>	<b>user set</b>	<b>boolean</b>	<b>true</b>
<code>network.negotiate-auth.allow-proxies</code>	default	boolean	true
<code>network.negotiate-auth.delegation-uris</code>	default	string	
<code>network.negotiate-auth.gsslib</code>	default	string	
<b><code>network.negotiate-auth.trusted-uris</code></b>	<b>user set</b>	<b>string</b>	<b>adfs1.adfs1.ciscolive.com,ciscolive.com</b>
<code>network.negotiate-auth.using-native-gsslib</code>	default	boolean	true
<code>network.ntlm.send-lm-response</code>	default	boolean	false

4. إغلاق Firefox وإعادة فتحه.

## التحقق من الصحة

للتحقق من إنشاء SPNs لخادم AD FS بشكل صحيح، أدخل أمر `setSPN` وعرض المخرجات.

```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>setspn -L sso
Registered ServicePrincipalNames for CN=Sam1 SSO,CN=Users,DC=ciscolive,DC=com:
HTTP/adfs1

C:\Users\Administrator>_
```

تحقق مما إذا كانت أجهزة العميل تحتوي على تذاكر Kerberos:

```
C:\Windows\system32\cmd.exe
C:\Users\user1.CISCOLIVE>klist tickets

Current LogonId is 0:0xabc6d

Cached Tickets: (2)

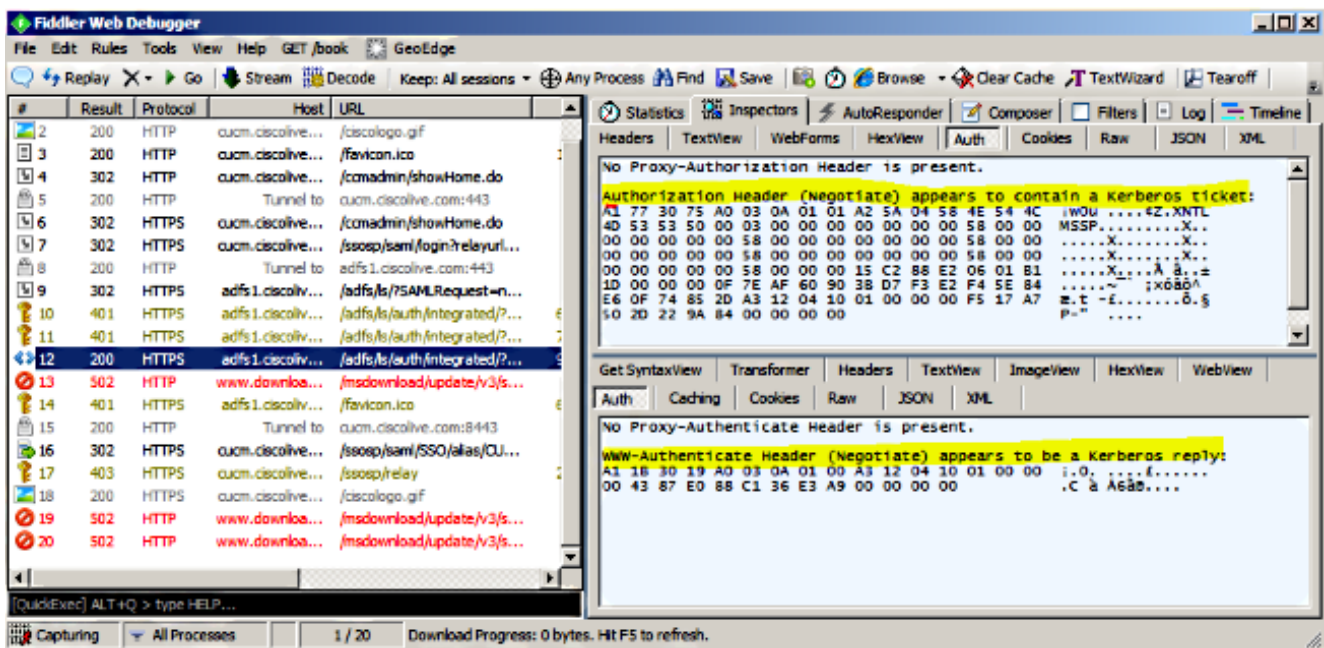
#0> Client: user1 @ CISCOLIVE.COM
Server: krbtgt/CISCOLIVE.COM @ CISCOLIVE.COM
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
Start Time: 1/17/2015 20:52:47 (local)
End Time: 1/18/2015 6:52:47 (local)
Renew Time: 1/24/2015 20:52:47 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96

#1> Client: user1 @ CISCOLIVE.COM
Server: host/pc1.ciscolive.com @ CISCOLIVE.COM
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
Start Time: 1/17/2015 20:52:47 (local)
End Time: 1/18/2015 6:52:47 (local)
Renew Time: 1/24/2015 20:52:47 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96

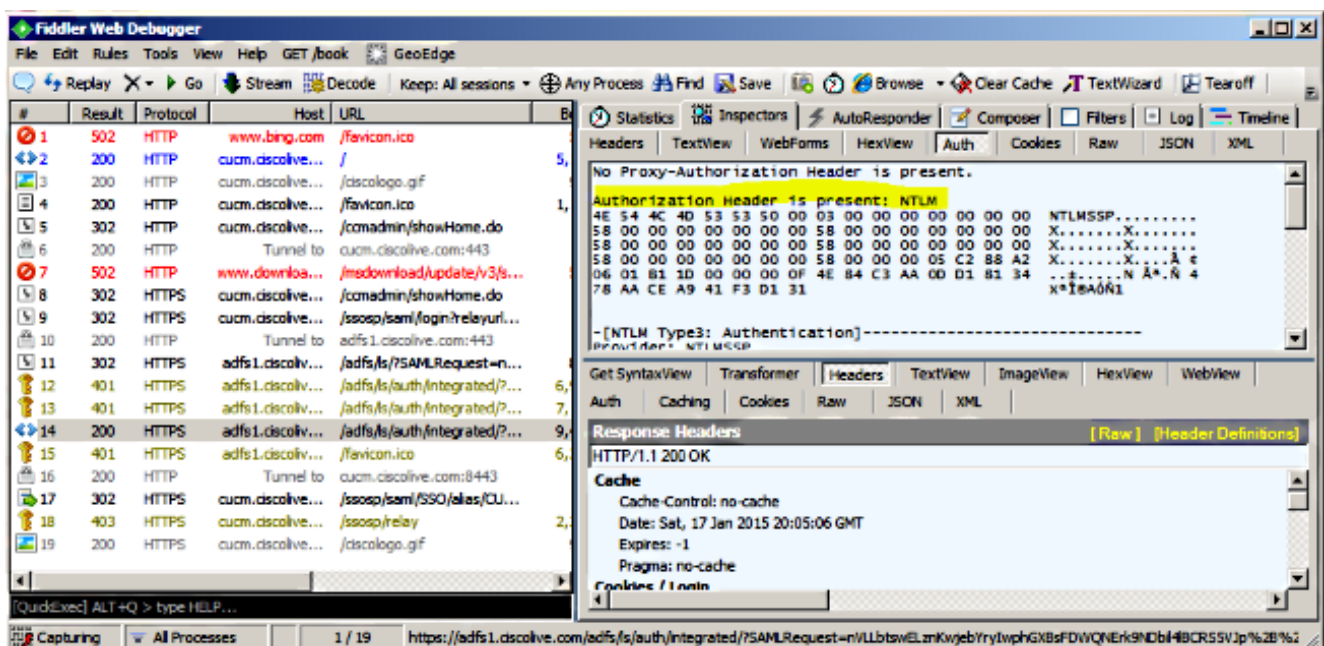
C:\Users\user1.CISCOLIVE>_
```

أكمل هذه الخطوات للتحقق من المصادقة (مصادقة Kerberos أو NTLM) قيد الاستخدام.

1. قم بتنزيل أداة Fiddler إلى جهاز العميل وقم بتشغيلها.
2. إغلاق كافة نوافذ Microsoft Internet Explorer.
3. قم بتشغيل أداة fiddler وتحقق من أن خيار التقاط حركة مرور يكون مكنة تحت القائمة ملف. يعمل Fiddler. كوكيل مرور بين جهاز العميل والخادم ويستمتع إلى كل حركة مرور.
4. افتح Microsoft Internet Explorer، واستعرض إلى CUCM، وانقر فوق بعض الارتباطات لإنشاء حركة مرور البيانات.
5. ارجع إلى الإطار الرئيسي ل Fiddler واختر أحد الإطارات حيث تكون النتيجة 200 (نجاح) ويمكنك أن ترى Kerberos كآلية مصادقة



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



## استكشاف الأخطاء وإصلاحها

إذا تم إكمال جميع خطوات التكوين والتحقق كما هو موضح في هذا المستند وكانت لا تزال لديك مشاكل في تسجيل الدخول، فيجب عليك مراجعة مسؤول Microsoft Windows Active Directory / AD FS.

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن ت س م ل ا اذ ه Cisco ت مچرت  
م ل ا ل ا اء ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و  
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems ( ر ف و ت م ط ب ا ر ل ا ) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا