

# 使用Kerberos身份驗證配置SAML SSO設定

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[配置AD FS](#)

[配置瀏覽器](#)

[Microsoft Internet Explorer](#)

[Mozilla Firefox](#)

[驗證](#)

[疑難排解](#)

## 簡介

本文檔介紹如何配置Active Directory和Active Directory聯合身份驗證服務(AD FS)版本2.0，以使其能夠通過Jabber客戶端（僅限Microsoft Windows）使用Kerberos身份驗證，從而允許使用者使用其Microsoft Windows Logon登入，而不提示輸入憑據。

**注意：**本文基於實驗室環境，並假設您已瞭解所做更改的影響。請參閱相關產品文檔以瞭解變更的影響。

## 必要條件

### 需求

思科建議您：

- 安裝AD FS 2.0版，並將思科合作產品配置為信賴方信任
- 合作產品(例如Cisco Unified Communications Manager(CUCM)IM and Presence、Cisco Unity Connection(UCXN)和CUCM)，支援使用安全斷言標籤語言(SAML)單一登入(SSO)

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Active Directory 2008(主機名：ADFS1.ciscolive.com)

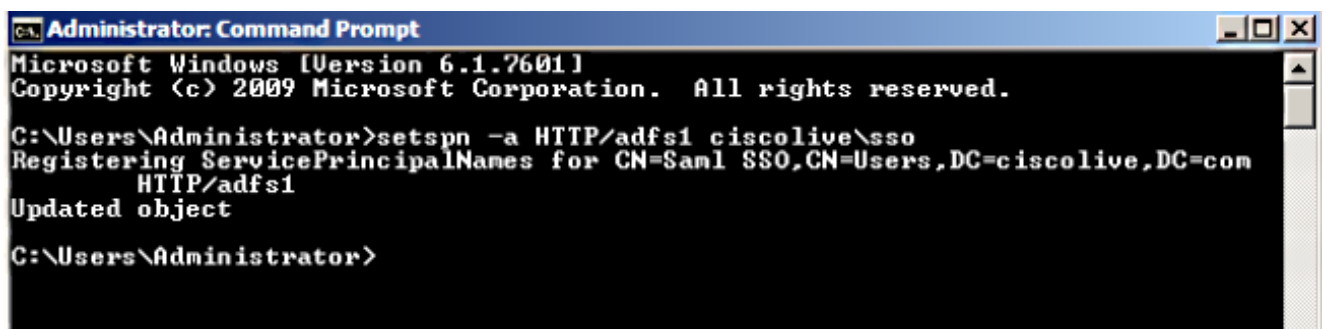
- AD FS 2.0版(主機名：ADFS1.ciscolive.com)
- CUCM(主機名：CUCM1.ciscolive.com)
- Microsoft Internet Explorer版本10
- Mozilla Firefox版本34
- Telerik Fiddler版本4

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 設定

### 配置AD FS

1. 使用服務主體名稱(SPN)配置AD FS版本2.0，以使安裝Jabber的客戶端電腦能夠請求票證，從而使得客戶端電腦能夠與AD FS服務通訊。



```

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=Sam1 SSO,CN=Users,DC=ciscolive,DC=com
HTTP/adfs1
Updated object

C:\Users\Administrator>

```

請參閱[AD FS 2.0:如何為服務帳戶配置SPN\(servicePrincipalName\)以瞭解詳細資訊](#)。

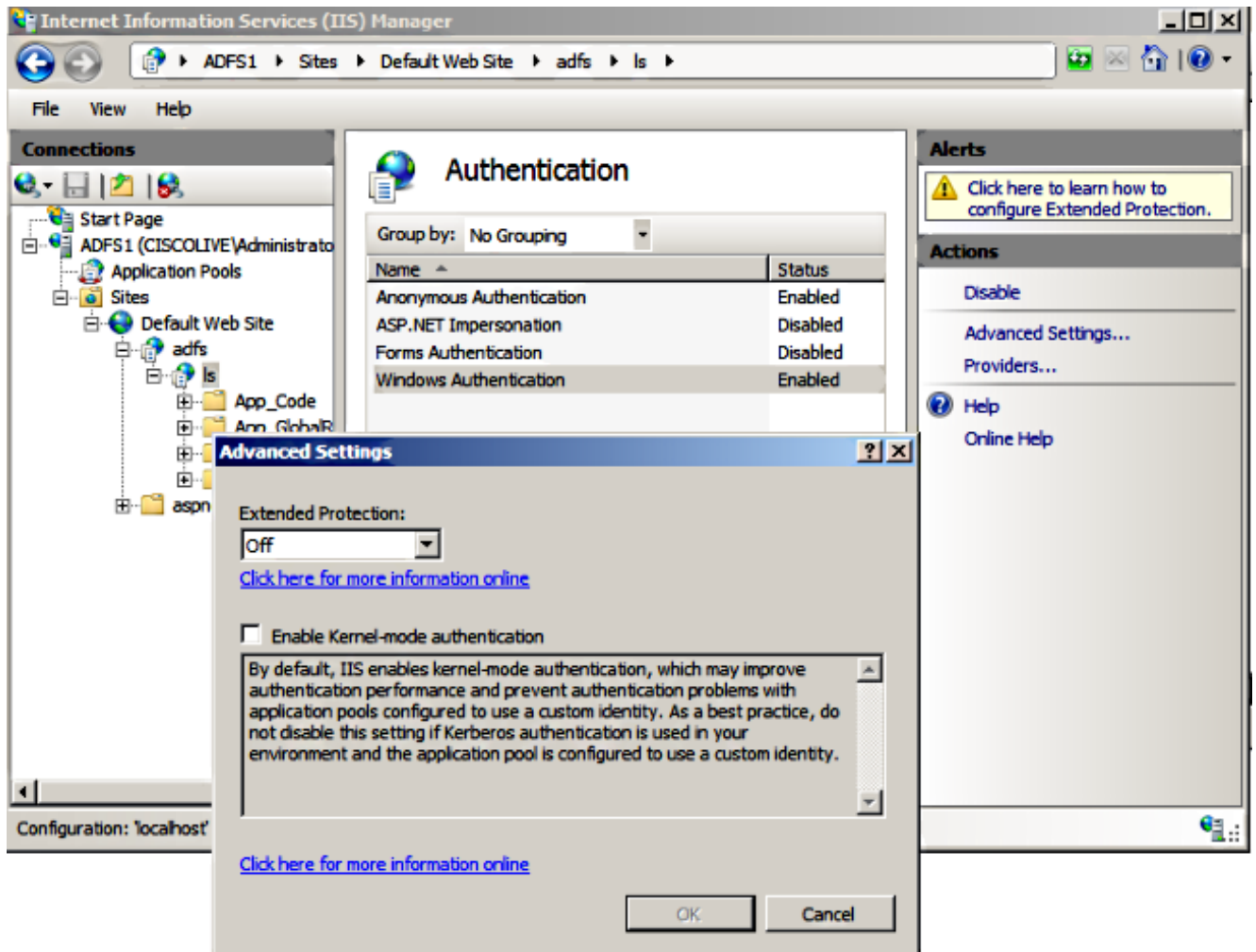
2. 確保AD FS服務的預設身份驗證配置(在C:\inetpub\adfs\ls\web.config中)為整合Windows身份驗證。確保它未更改為基於表格的身份驗證。

```

<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 sam1="true" wsFederation="true" />
  <homeRealmDiscovery page="HomeRealmDiscovery.aspx" />
  <persistIdentityProviderInformation enabled="true" lifetimeInDays="30" />
  <singleSignOn enabled="true" />
</microsoft.identityserver.web>

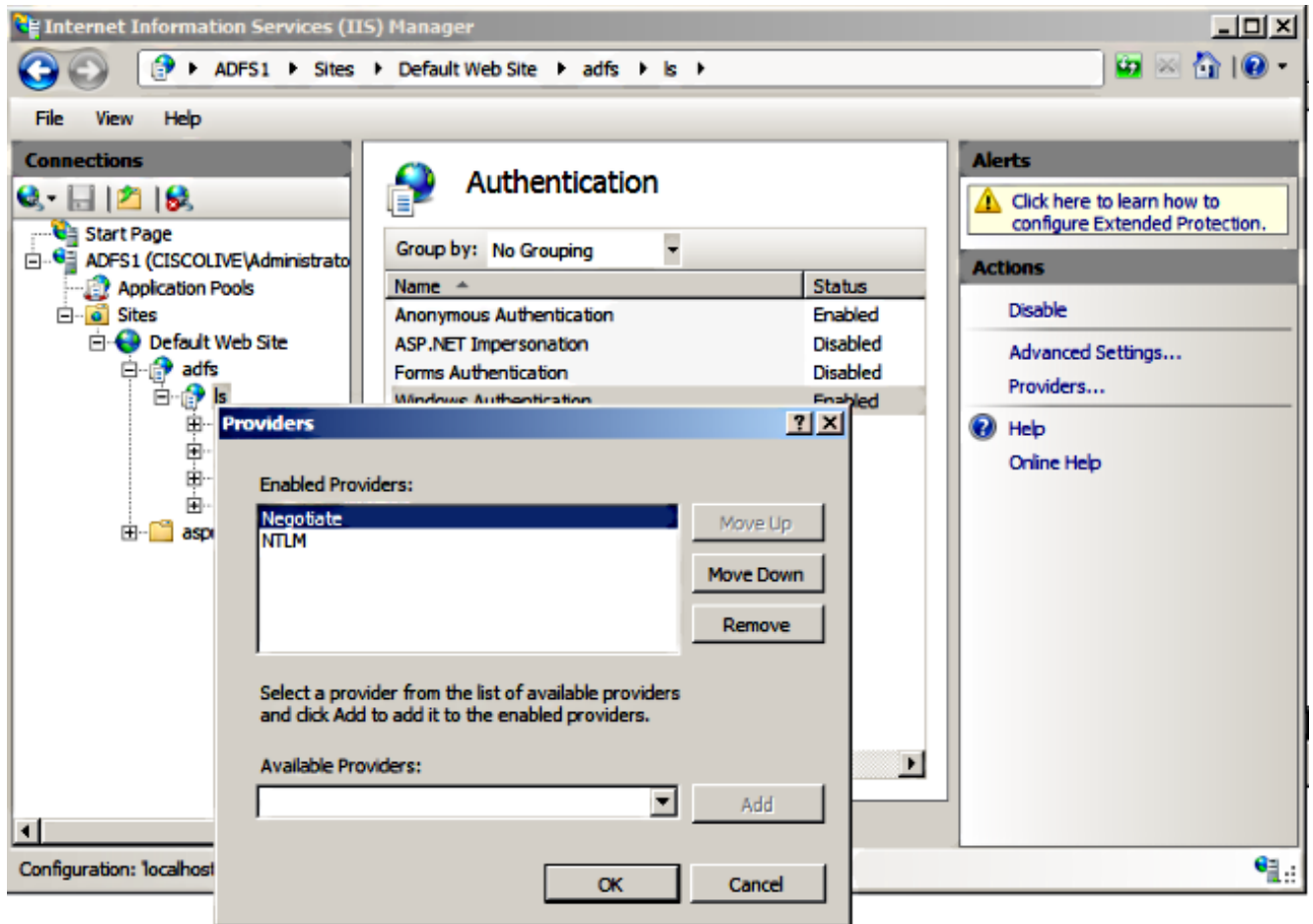
```

3. 選擇Windows Authentication，然後按一下右窗格下的Advanced Settings。在「Advanced Settings」中，取消選中Enable Kernel-mode authentication，確保Extended Protection為Off，然後按一下OK。



4. 確保AD FS版本2.0同時支援Kerberos協定和NT LAN Manager(NTLM)協定，因為所有非Windows客戶端都不能使用Kerberos並依賴NTLM。

在右窗格中，選擇**Providers**，並確保**Negotiate**和**NTLM**位於Enabled Providers:



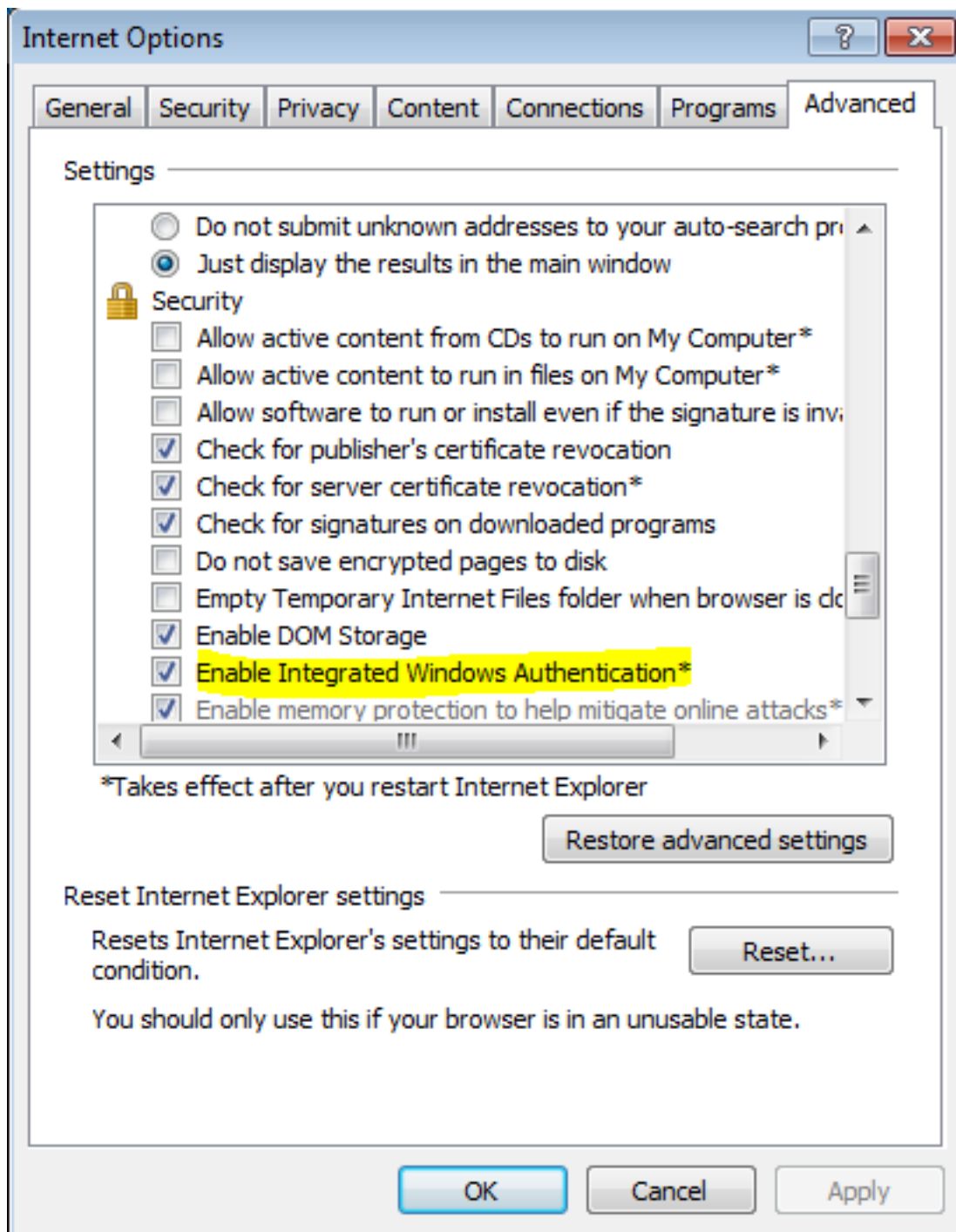
**附註：** 使用整合Windows身份驗證對客戶端請求進行身份驗證時，AD FS會傳遞Negotiate安全標頭。協商安全標頭允許客戶端在Kerberos身份驗證和NTLM身份驗證之間進行選擇。除非以下條件之一為真，否則協商過程將選擇Kerberos身份驗證：

- 身份驗證中涉及的某個系統不能使用Kerberos身份驗證。
- 呼叫應用程式沒有提供足夠的資訊來使用Kerberos身份驗證。
- 為了啟用協商過程以選擇用於網路身份驗證的Kerberos協定，客戶端應用程式必須提供SPN、使用者主體名稱(UPN)或網路基本輸入/輸出系統(NetBIOS)帳戶名稱作為目標名稱。否則，協商過程始終會選擇NTLM協定作為首選身份驗證方法。

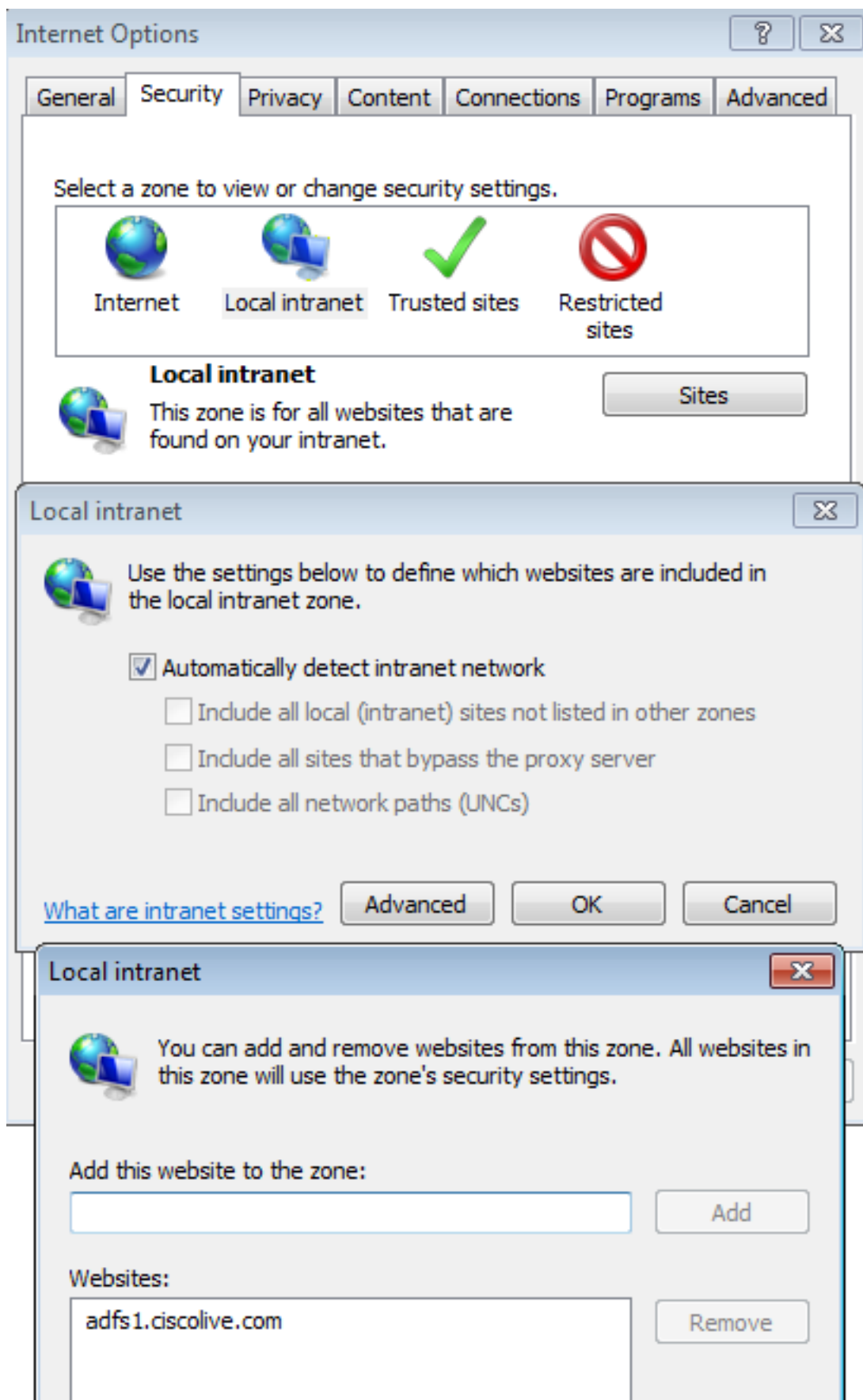
## 配置瀏覽器

### Microsoft Internet Explorer

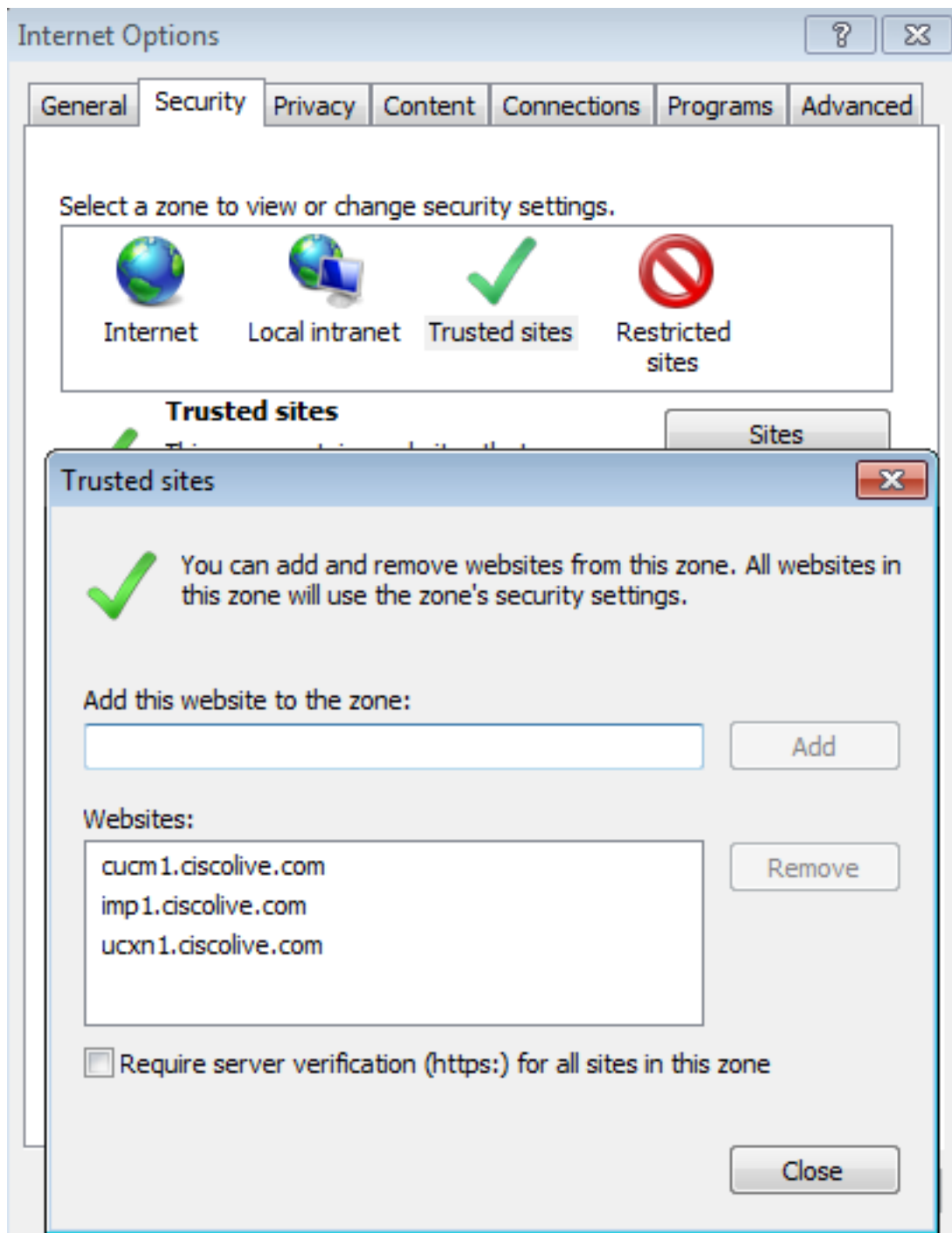
1. 確保選中Internet Explorer > Advanced > Enable Integrated Windows Authentication。



2. 在Security > Intranet zones > sites下新增AD FS URL。

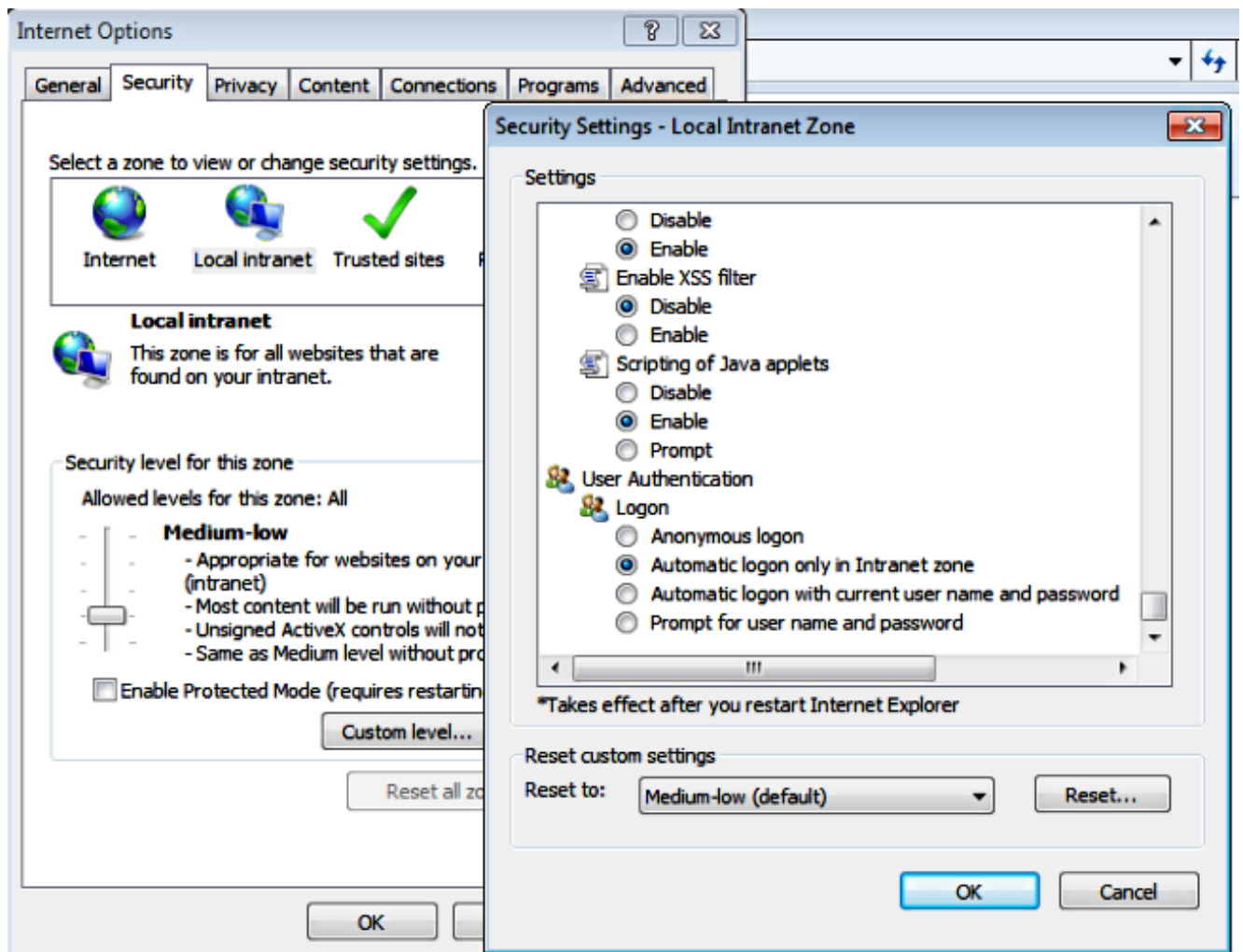


3. 將CUCM、IMP和Unity主機名新增到Security >Trusted sites。



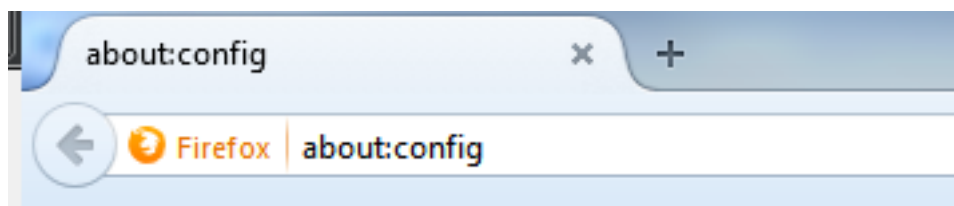
4. 確保已配置Internet Explorer > **security** > **Local Intranet** > **Security Settings** > **User Authentication - Logon** , 以便使用Intranet站點的登入憑據。





## Mozilla Firefox

1. 開啟Firefox，在位址列中輸入about:config。

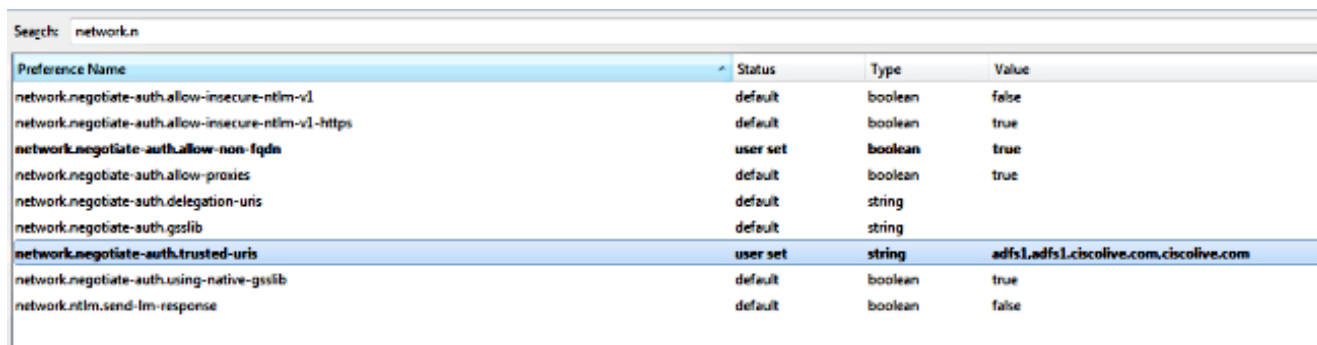


2. 單擊「我會小心的，我保證！」





- 按兩下偏好設定network.negotiate-auth.allow-non-fqdn至true，按兩下偏好設定network.negotiate-auth.trusted-uris至ciscolive.com,adfs1.ciscolive.com以進行修改。

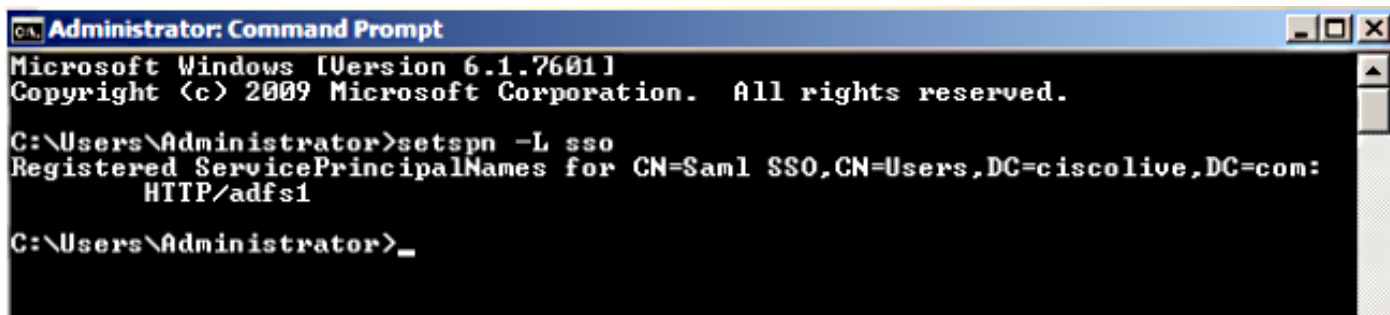


Preference Name	Status	Type	Value
network.negotiate-auth.allow-insecure-ntlm-v1	default	boolean	false
network.negotiate-auth.allow-insecure-ntlm-v1-https	default	boolean	true
network.negotiate-auth.allow-non-fqdn	user set	boolean	true
network.negotiate-auth.allow-proxies	default	boolean	true
network.negotiate-auth.delegation-uris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

- 關閉Firefox並重新開啟。

## 驗證

若要檢查AD FS伺服器的SPN是否正確建立，請輸入setspn命令並檢視輸出。

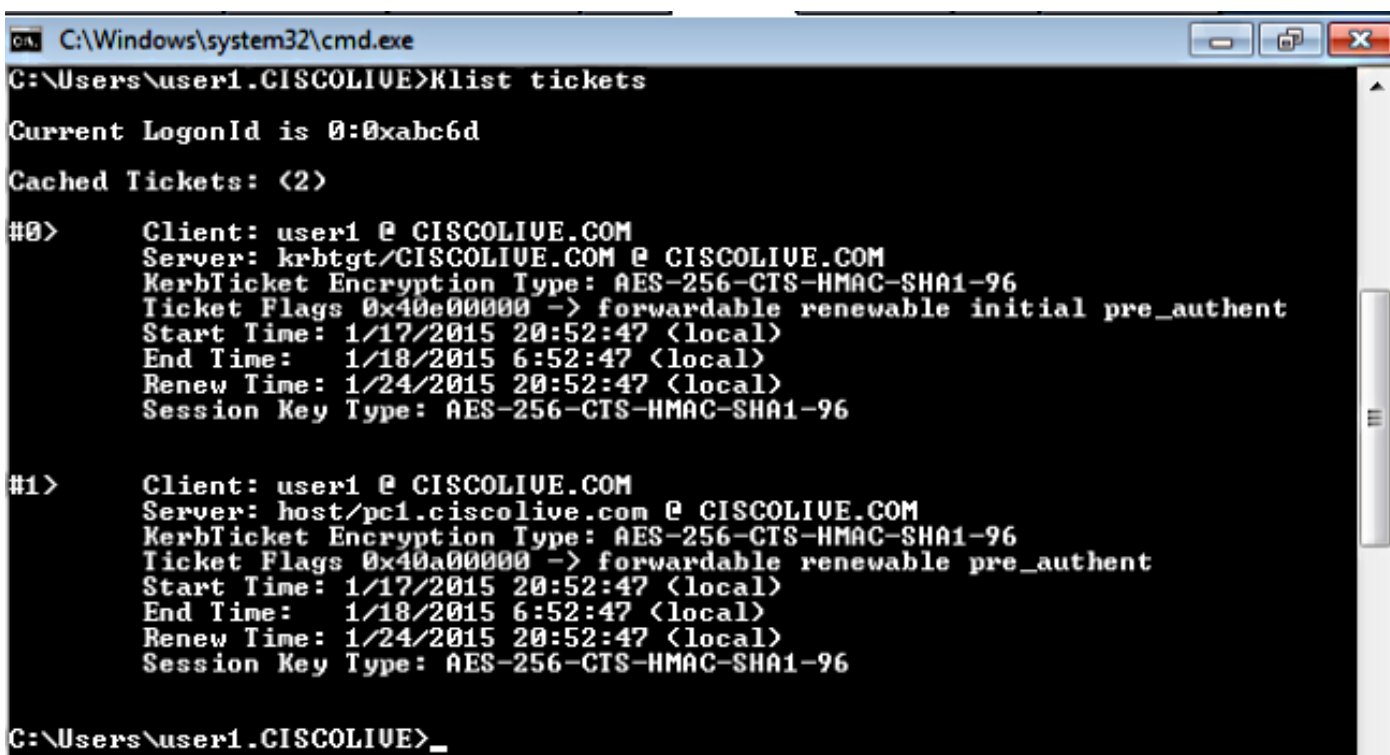


```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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

C:\Users\Administrator>_
```

檢查客戶端電腦是否具有Kerberos票證：



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

Current LogonId is 0:0xabc6d

Cached Tickets: (2)

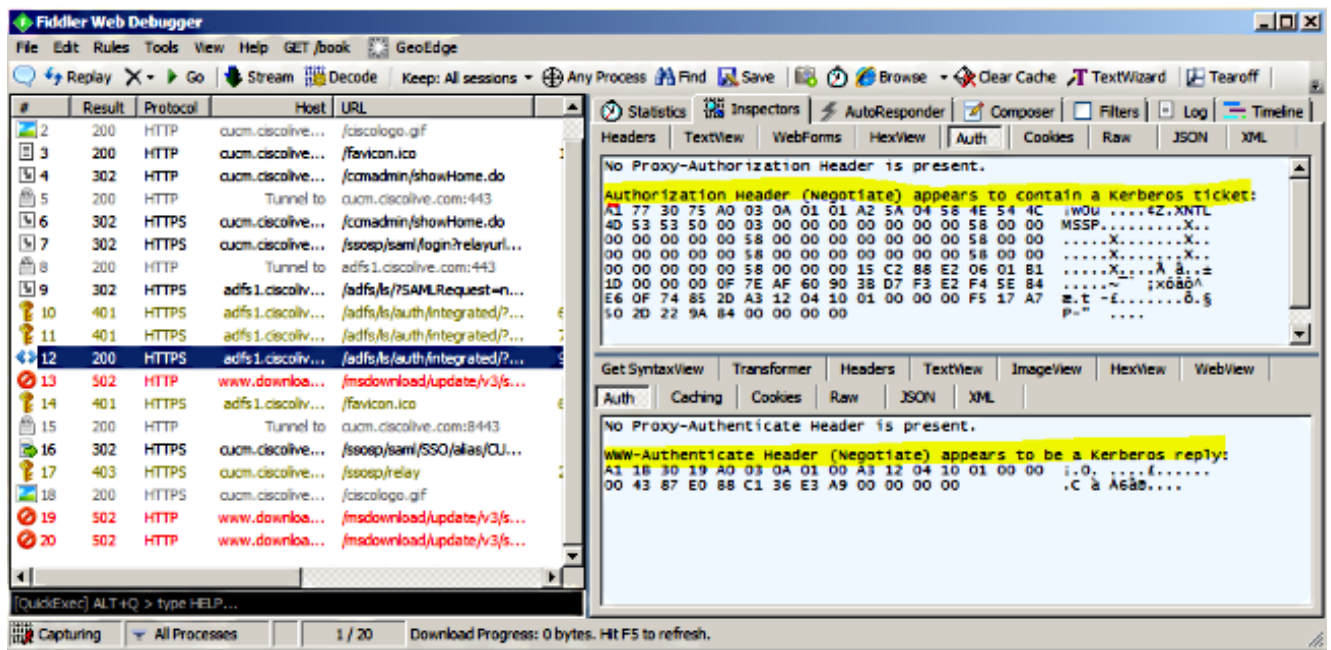
#0> Client: user1 @ CISCOLIVE.COM
Server: krbtgt/CISCOLIVE.COM @ CISCOLIVE.COM
KerberosTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
Start Time: 1/17/2015 20:52:47 (local)
End Time: 1/18/2015 6:52:47 (local)
Renew Time: 1/24/2015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

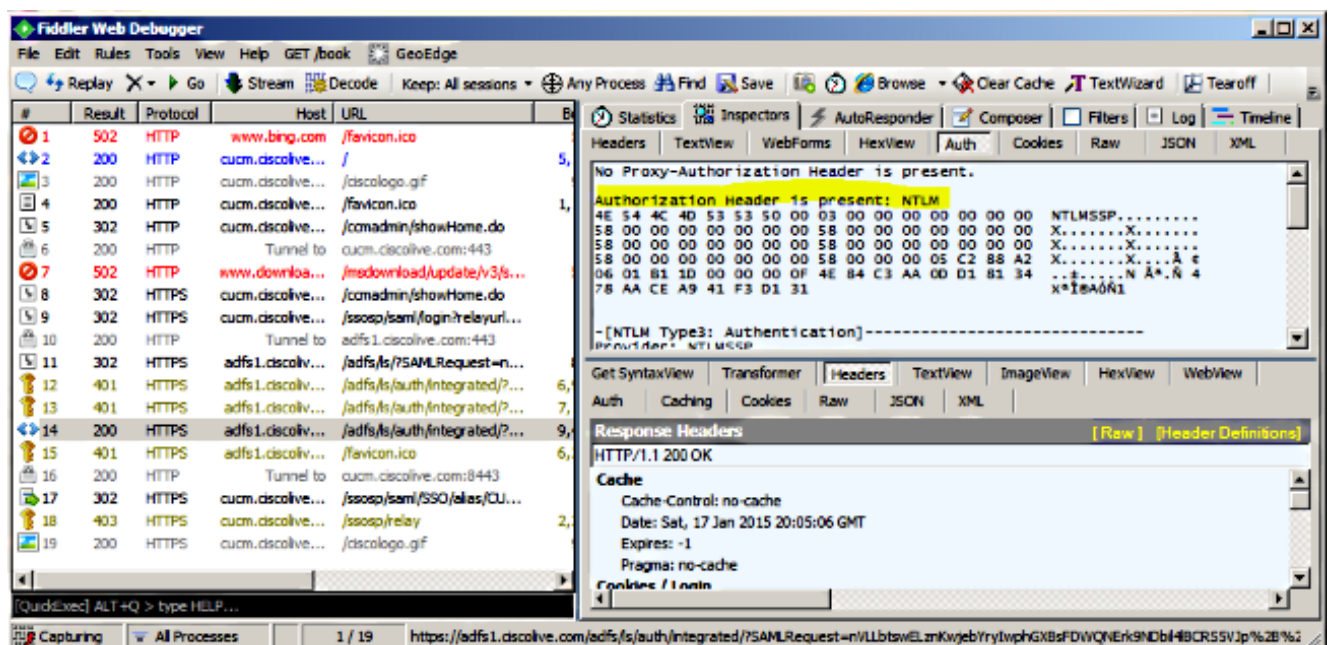
C:\Users\user1.CISCOLIVE>_
```

完成以下步驟以驗證正在使用哪些身份驗證（Kerberos或NTLM身份驗證）。

1. 將Fiddler工具下載到您的客戶端電腦並進行安裝。
2. 關閉所有Microsoft Internet Explorer視窗。
3. 運行Fiddler Tool並檢查File選單下的**Capture Traffic**選項是否已啟用。Fiddler充當客戶端電腦和伺服器之間的傳遞代理，並偵聽所有流量。
4. 開啟Microsoft Internet Explorer，瀏覽到您的CUCM，然後按一下某些連結以生成流量。
5. 返回到Fiddler主視窗，並選擇結果為200（成功）的其中一個幀，您可以看到Kerberos作為身份驗證機制



6. 如果身份驗證型別為NTLM，則會在幀的開頭看到協商 — NTLMSSP，如下所示。



如果所有配置和驗證步驟均按本文檔所述完成，並且您仍存在登入問題，則必須諮詢Microsoft Windows Active Directory/AD FS管理員。