

Kerberos与ADFS 2.0的最终用户SAML SSO的Jabber配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[验证](#)

[故障排除](#)

简介

本文档介绍如何使用Active Directory联合身份验证服务(ADFS)2.0配置Kerberos。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

背景信息

最终用户安全断言标记语言(SAML)单点登录(SSO)配置要求配置Kerberos,以便允许最终用户SAML SSO用于Jabber使用域身份验证。使用Kerberos实施SAML SSO时,轻量目录访问协议(LDAP)处理所有授权和用户同步,而Kerberos管理身份验证。Kerberos是一种身份验证协议,旨在与启用LDAP的实例结合使用。

在加入Active Directory域的Microsoft Windows和Macintosh计算机上，用户可以无缝登录Cisco Jabber，而无需输入用户名或密码，甚至看不到登录屏幕。未登录其计算机上的域的用户仍会看到标准登录表单。

由于身份验证使用从操作系统传递的单个令牌，因此无需重定向。令牌根据已配置的密钥域控制器(KDC)进行验证，如果该令牌有效，则用户登录。

配置

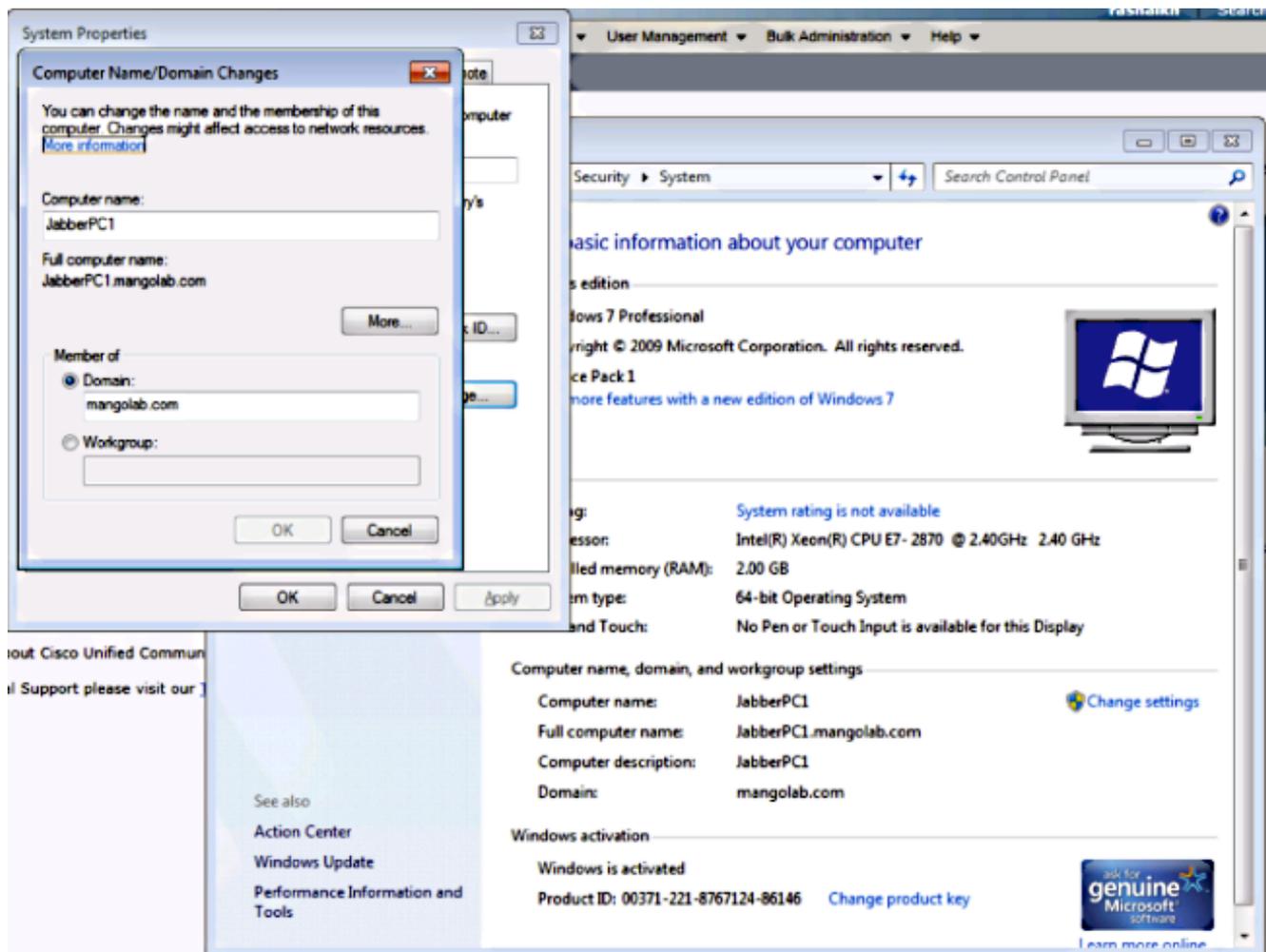
以下是使用ADFS 2.0配置Kerberos的步骤。

1. 在计算机上安装Microsoft Windows Server 2008 R2。
2. 在同一台计算机上安装Active Directory服务(ADDS)和ADFS。
3. 在安装了Microsoft Windows Server 2008 R2的计算机上安装Internet信息服务(IIS)。
4. 为IIS创建自签名证书。
5. 将自签名证书导入IIS，并将其用作HTTPS服务器证书。
6. 在另一台计算机上安装Microsoft Windows7并将其用作客户端。

将域名服务器(DNS)更改为安装ADDS的计算机。

将此计算机添加到您在安装ADDS时创建的域。

转到“开始”。右键单击**Computer**。单击 **Properties**。单击窗口右侧的**更改设置**。单击 **Computer Name** 选项卡。单击 **Change**。添加您创建的域。



7. 检查Kerberos服务是否在两台计算机上生成。

以管理员身份登录到服务器计算机并打开命令提示符。然后执行以下命令：

```
cd \windows\System32Klist票
```

```
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
Kerberos Ticket Encryption Type: AES-256-CIS-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-CIS-HMAC-SHA1-96
```

以域用户身份登录到客户端并执行相同的命令。

```

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
Kerberos Ticket 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
Kerberos Ticket 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
Kerberos Ticket 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
Kerberos Ticket 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
Kerberos Ticket 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. 在安装ADDS的计算机上创建ADFS Kerberos标识。

Microsoft Windows管理员以<domainname>\administrator的身份登录到Microsoft Windows域（例如在Microsoft Windows域控制器上），创建ADFS Kerberos标识。ADFS HTTP服务必须具有名为服务主体名称(SPN)的Kerberos身份，格式如下：
 : HTTP/DNS_name_of_ADFS_server。

此名称必须映射到代表ADFS HTTP服务器实例的Active Directory用户。使用Microsoft Windows **setspn**实用程序，该实用程序在Microsoft Windows 2008 Server上应默认可用。

步骤 注册ADFS服务器的SPN。在Active Directory域控制器上，运行setspn命令。

例如，当ADFS主机为adfs01.us.renovations.com，而Active Directory域为US.RENOVES.COM时，命令为：

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

SPN的HTTP/部分适用，即使ADFS服务器通常由安全套接字层(SSL) (即HTTPS) 访问。

使用setspn命令检查是否已正确创建ADFS服务器的SPN并查看输出。

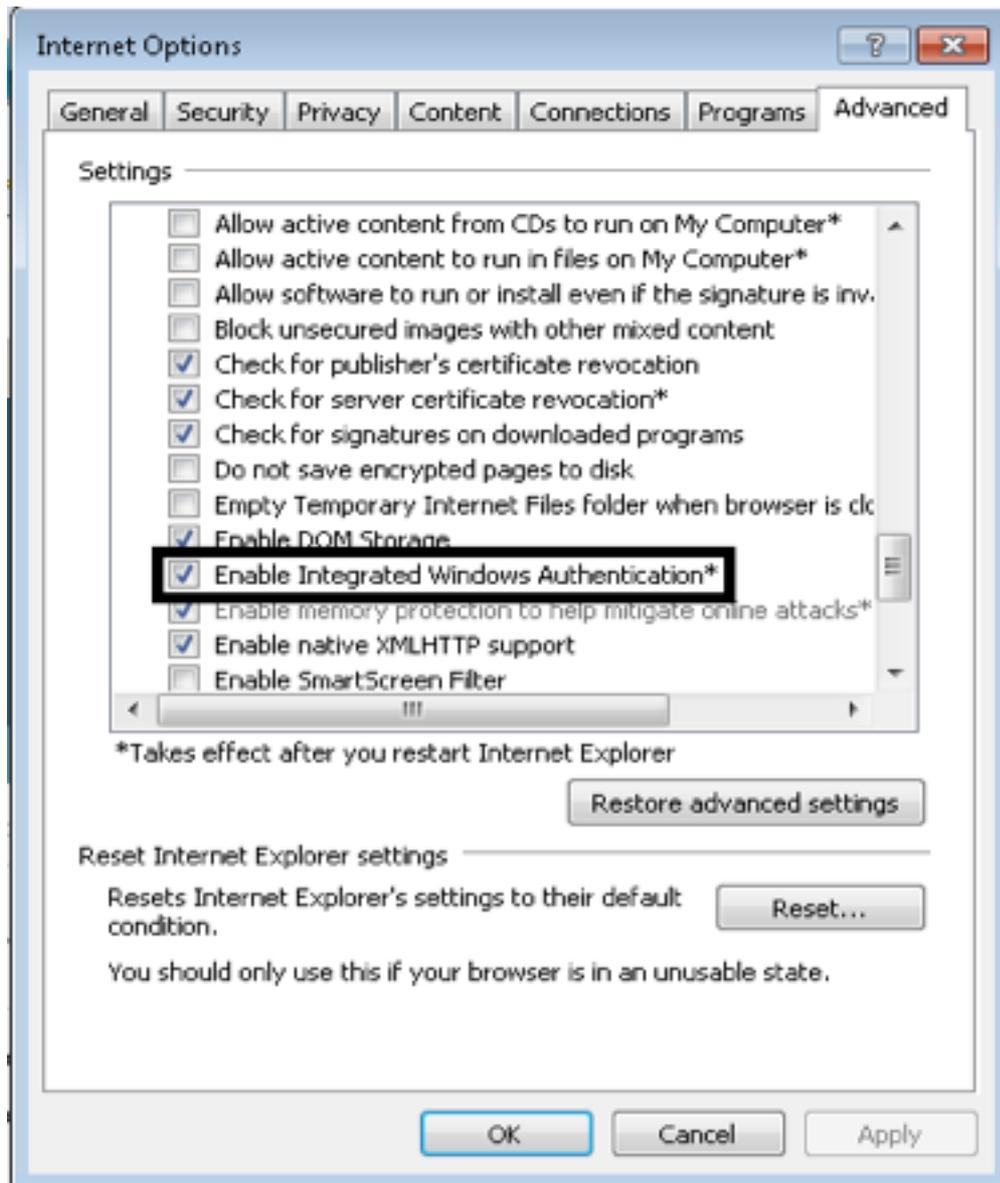
```
setspn -L
```

```
C:\Windows\System32>setspn -L win2k8
Registered ServicePrincipalNames for CN=WIN2K8,OU=Domain Controllers,DC=mangolab
,DC=con:
HTTP/win2k8.mangolab.com
ldap/win2k8.mangolab.com/ForestDnsZones.mangolab.com
ldap/win2k8.mangolab.com/DomainDnsZones.mangolab.com
IERSRU/WIN2K8
IERSRU/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
/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>_
```

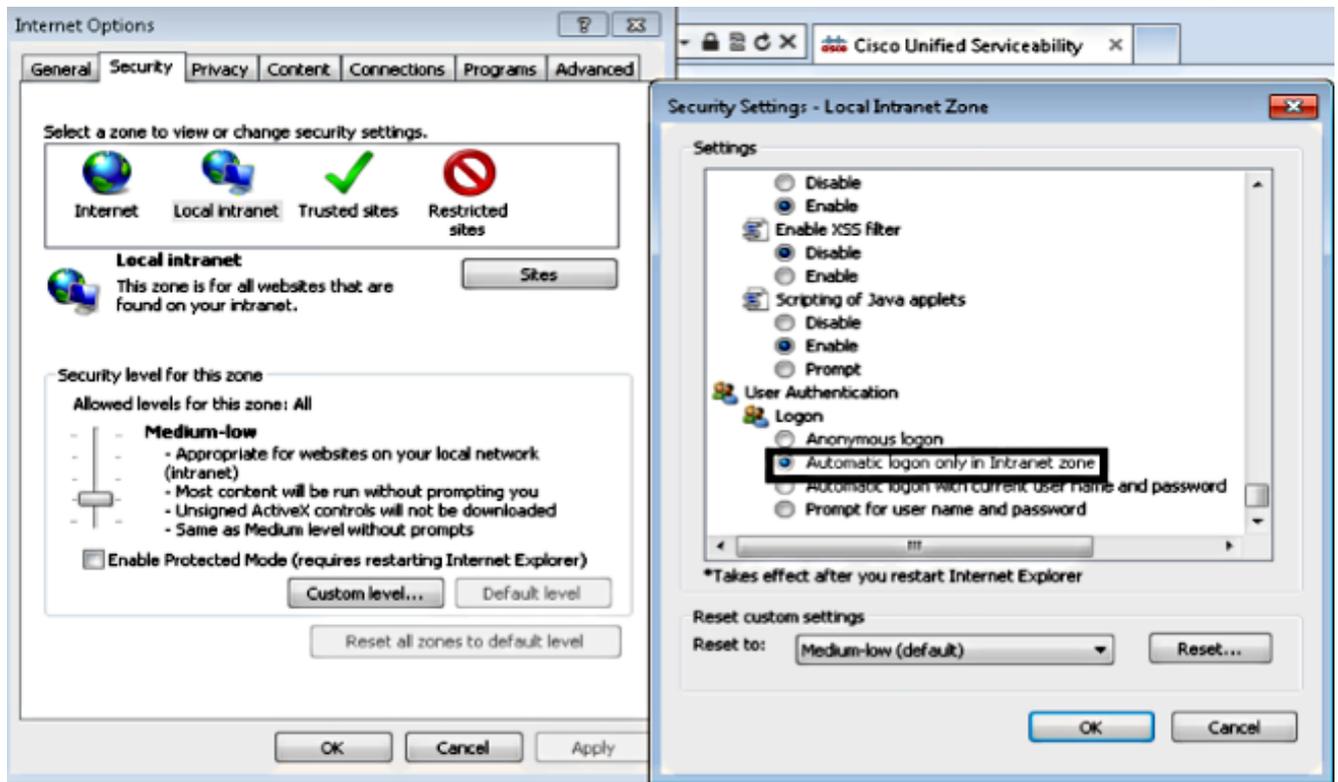
9. 配置Microsoft Windows客户端的浏览器设置。

导航至“工具”>“Internet选项”>“高级”以启用集成Windows身份验证。

选中启用集成Windows身份验证复选框:

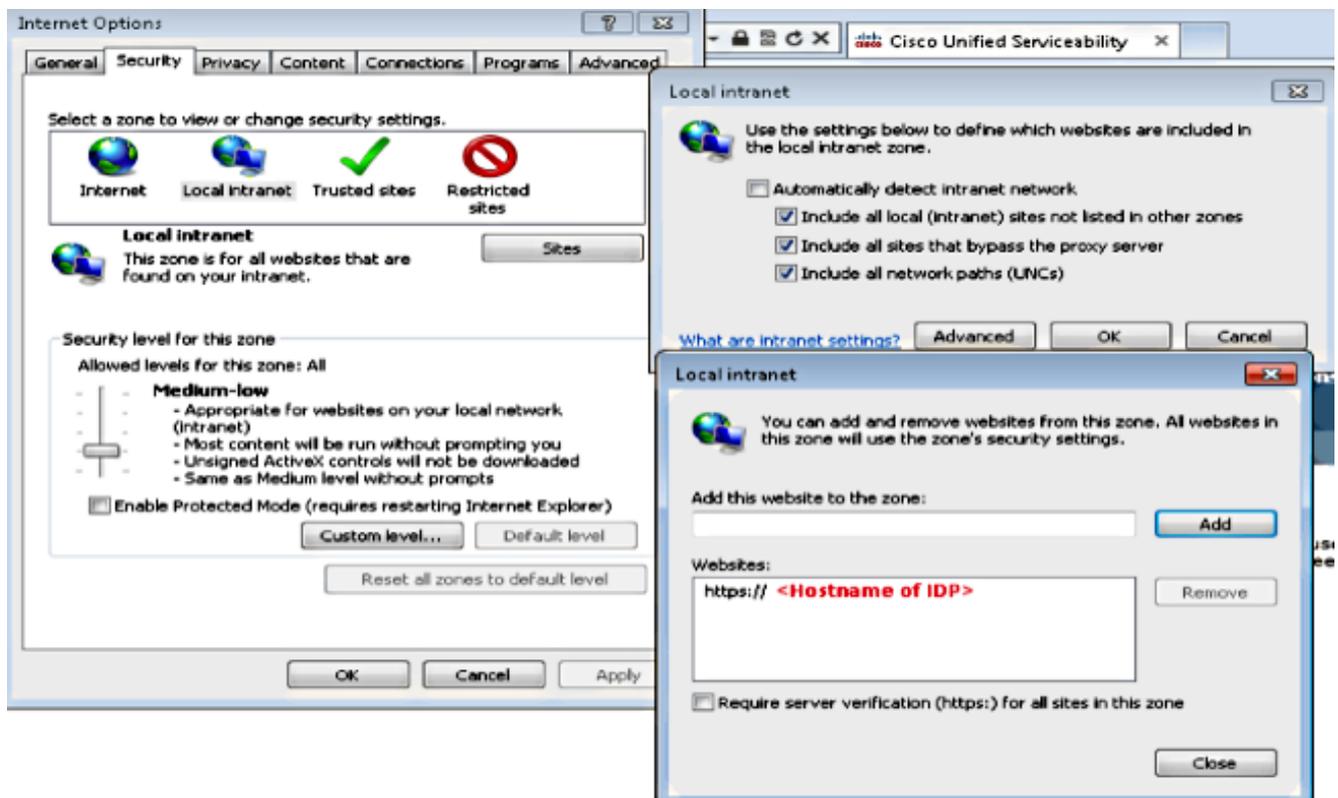


导航至工具> Internet选项>安全>本地Intranet >自定义级别.....以便选择仅在Intranet区域中自动登录。

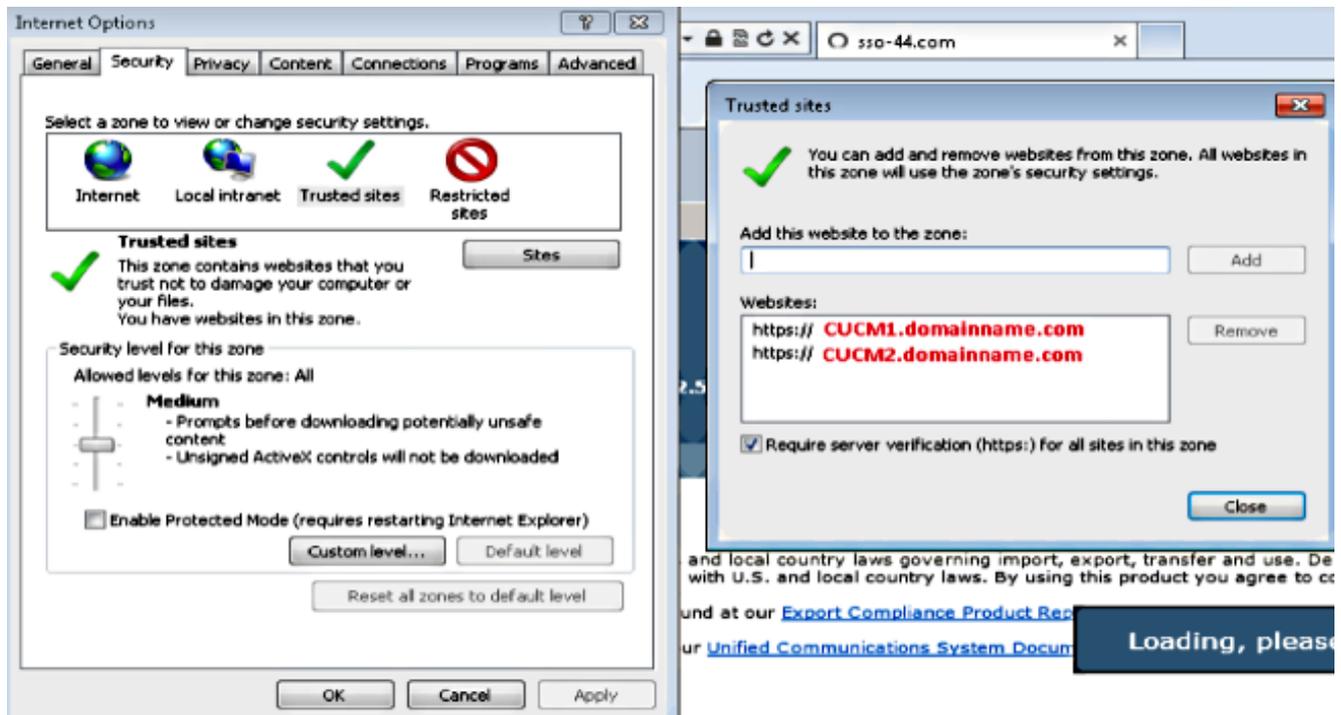


导航至工具> Internet选项>安全>本地Intranet >站点>高级，以便将入侵检测和防御 (IDP)URL添加到本地Intranet站点。

注意：选中Local intranet对话框中的所有复选框，然后单击Advanced选项卡。



导航至工具>安全>受信任站点>站点，以便将CUCM主机名添加到受信任站点：

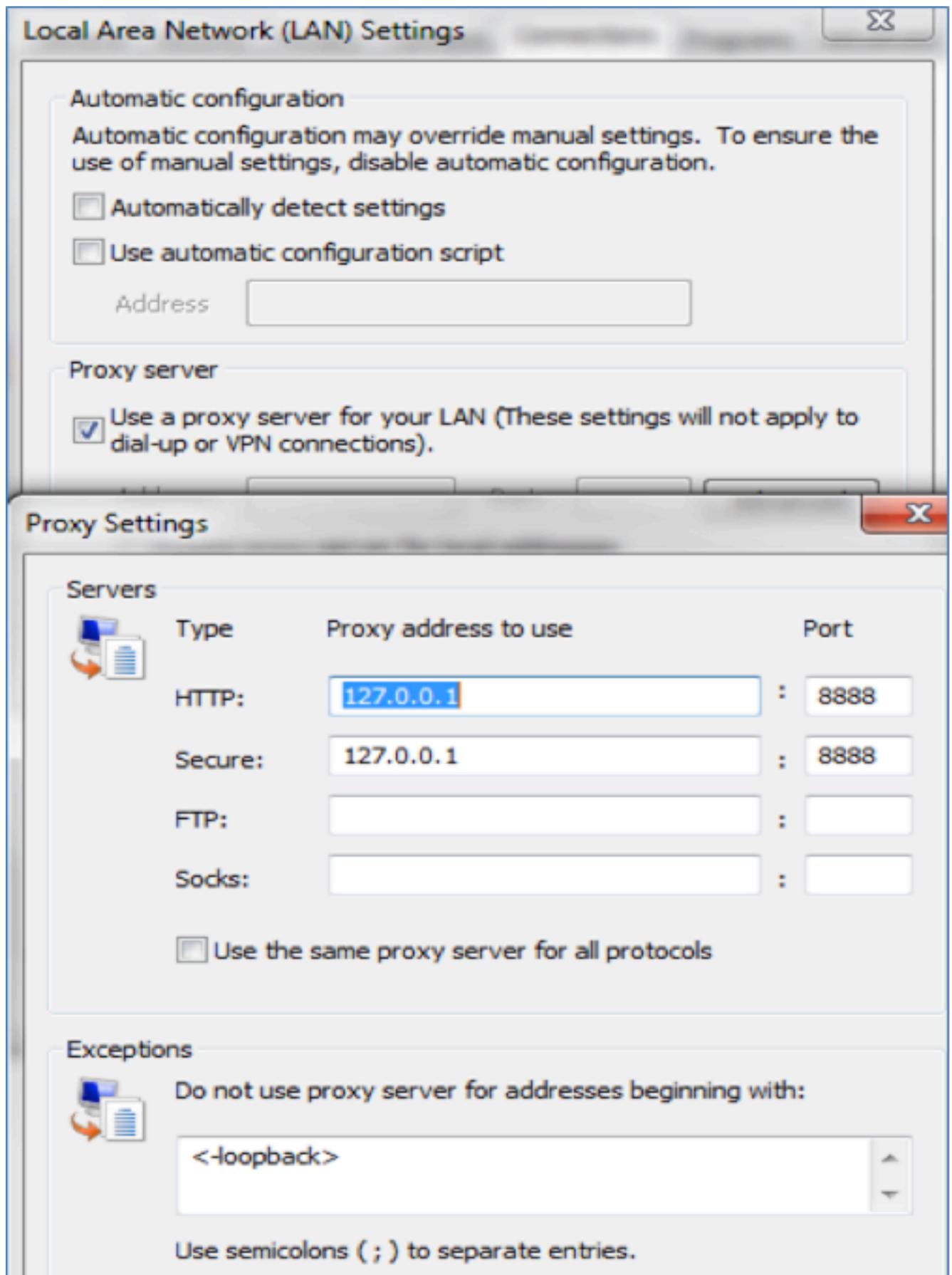


验证

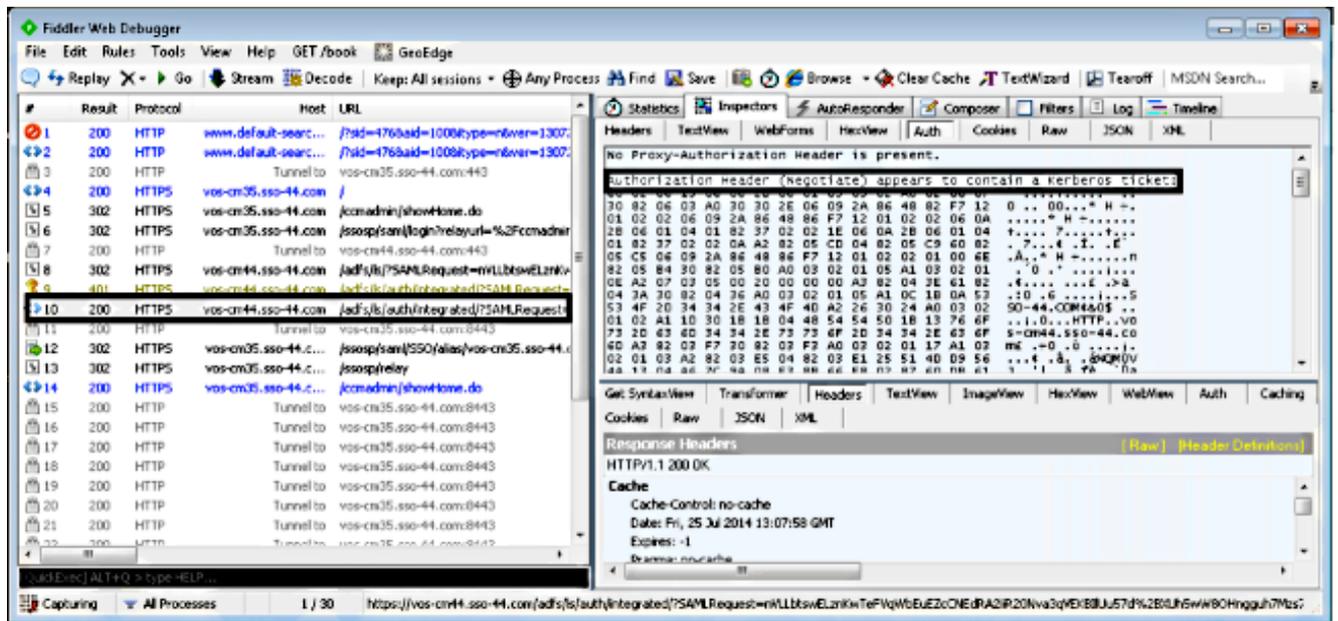
本节介绍如何验证使用的身份验证(Kerberos或NT LAN Manager(NTLM)身份验证)。

1. 将Fiddler工 [具下载](#) 到您的客户机并安装它。
2. 关闭所有 Internet Explorer 窗口。
3. 运行Fiddler工具，并检查File菜单下是否启用了Capture Traffic选项。

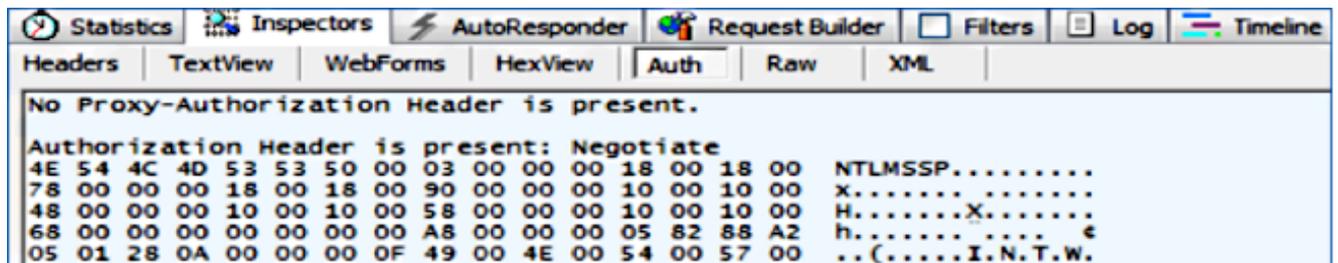
Fiddler充当客户端计算机和服务器的传递代理并侦听所有流量，这会临时设置Internet Explorer设置，如下所示：



4. 打开Internet Explorer，浏览到您的客户关系管理(CRM)服务器URL，然后单击几个链接以生成流量。
5. 返回Fiddler主窗口，选择结果为200（成功）的帧之一：



如果身份验证类型为NTLM，则在帧的开头看到协商 — NTLMSSP，如下所示：



故障排除

目前没有针对此配置的故障排除信息。