使用Kerberos身份验证配置SAML SSO设置

目录

简介
先决条件
要求
使用的组件
配置
配置AD FS
配置浏览器
Microsoft Internet Explorer
Mozilla Firefox
验证
故障排除

简介

本文档介绍如何配置Active Directory和Active Directory联合身份验证服务(AD FS)版本2.0，以使其能够使用Jabber客户端（仅限Microsoft Windows）的Kerberos身份验证，这允许用户使用其Microsoft Windows登录登录登录，并且不会提示用户输入凭据。

> **警告**：本文档基于实验环境，并假设您了解所做更改的影响。请参阅相关产品文档，了解所做更改的影响。

先决条件

要求

Cisco 建议您：

- AD FS 2.0版安装并配置了思科协作产品作为信赖方信任
- 协作产品(如思科统一通信管理器(CUCM)IM and Presence、Cisco Unity Connection(UCXN)和CUCM)已启用，以便使用安全断言标记语言(SAML)单点登录(SSO)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Active Directory 2008(主机名：ADFS1.ciscolive.com）

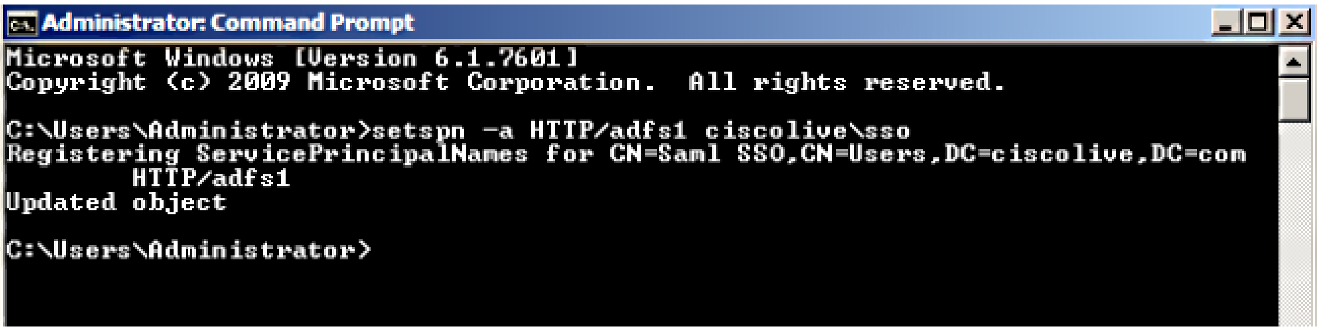
- AD FS版本2.0(主机名：ADFS1.ciscolive.com）
- CUCM(主机名：CUCM1.ciscolive.com）
- Microsoft Internet Explorer版本10
- Mozilla Firefox版本34
- 特莱里克·菲德勒第4版

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。

配置

配置AD FS

1. 使用服务主体名称(SPN)配置AD FS版本2.0，以使安装Jabber的客户端计算机能够请求票证，从而使客户端计算机能够与AD FS服务通信。



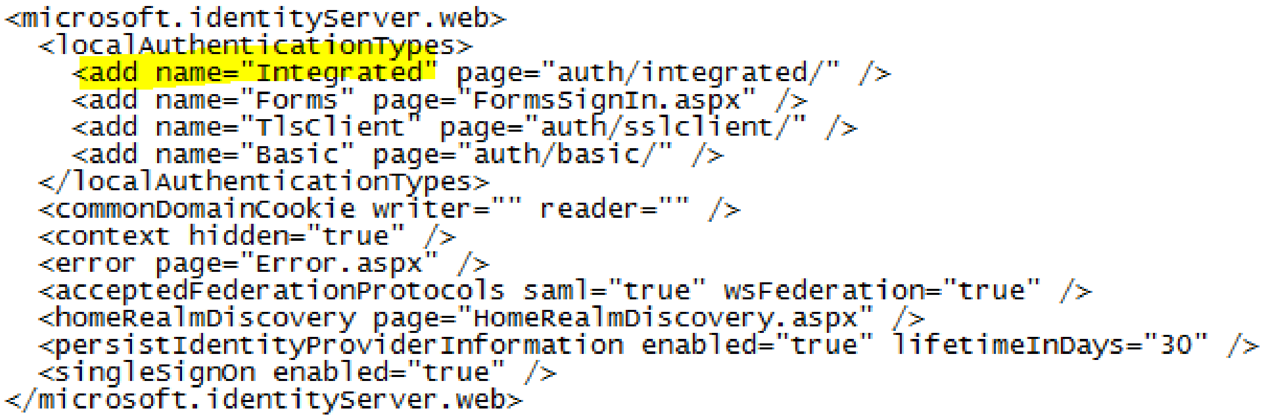
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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>
```

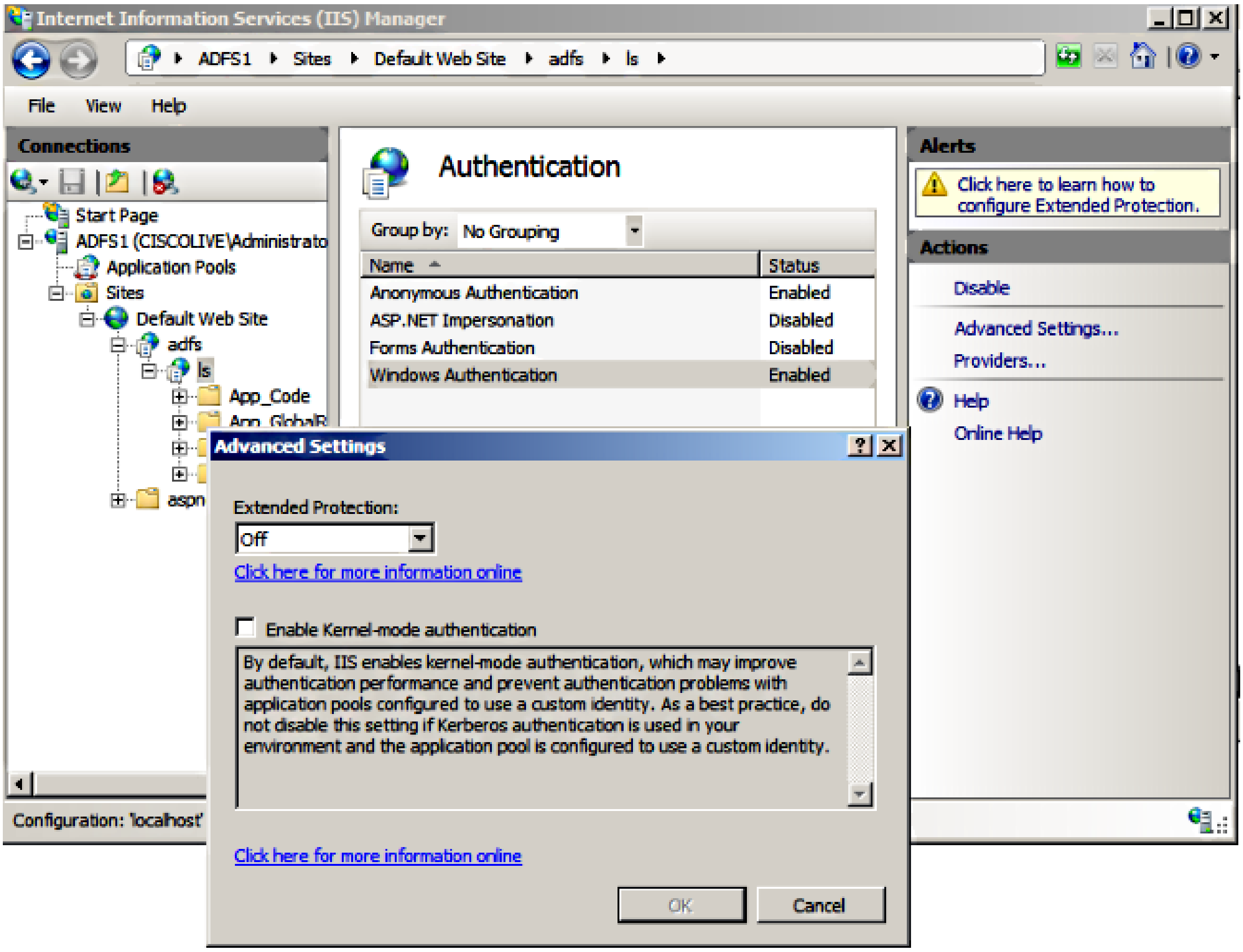
   请参阅[AD FS 2.0:如何为服务帐户配置SPN(servicePrincipalName)以了解](#)详细信息。

2. 确保AD FS服务(在C:\inetpub\adfs\ls\web.config中)的默认身份验证配置**为集**成Windows**身份验证**。确保它未更改为基于表**单的身份验证**。



```
<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. 选择**Windows Authentication**，然**后单击右窗格下的Advanced Settings**。在高级设置中，取消选中**启用内核模式身份验证**，确保扩展保护处于**关闭**状态，然后单击**确定**。



Group by: No Grouping

Name	Status
Anonymous Authentication	Enabled
ASP.NET Impersonation	Disabled
Forms Authentication	Disabled
Windows Authentication	Enabled

Click here to learn how to configure Extended Protection.

Extended Protection: Off

Click here for more information online

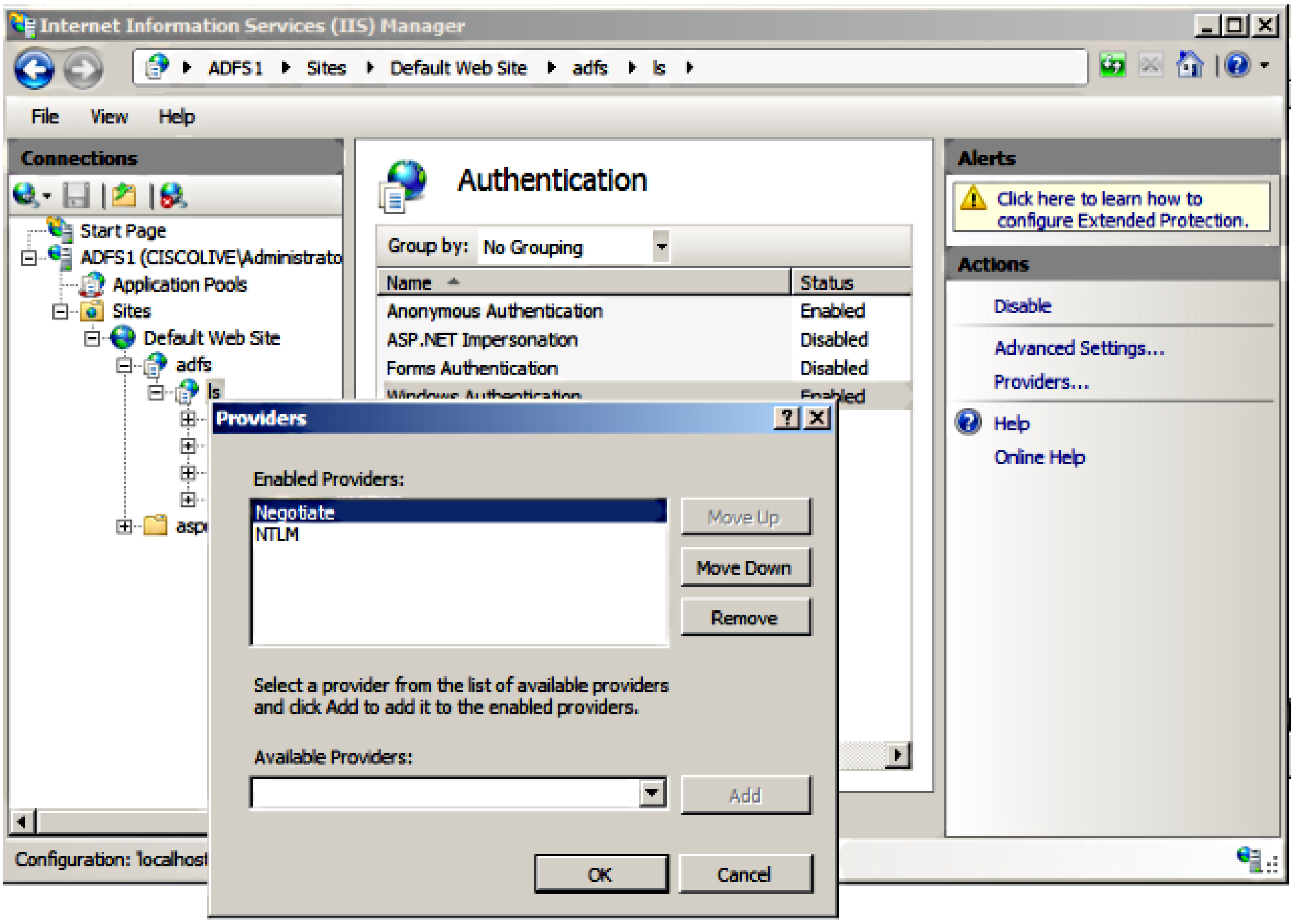
□ Enable Kernel-mode authentication

By default, IIS enables kernel-mode authentication, which may improve authentication performance and prevent authentication problems with application pools configured to use a custom identity. As a best practice, do not disable this setting if Kerberos authentication is used in your environment and the application pool is configured to use a custom identity.

Click here for more information online

4. 确保AD FS版本2.0同时支持Kerberos协议和NT LAN Manager(NTLM)协议，因为所有非Windows客户端都无法使用Kerberos并依赖NTLM。

   在右窗格中，选择“提供程序”，**并**确保“已启用的提供程序”下**存在“协商”和NTLM**:



Group by: No Grouping

Name	Status
Anonymous Authentication	Enabled
ASP.NET Impersonation	Disabled
Forms Authentication	Disabled
Windows Authentication	Enabled

Enabled Providers:

Negotiate
NTLM

Select a provider from the list of available providers and click Add to add it to the enabled providers.

Available Providers:

注意：当使用集成Windows身份验证对客户端请求进行身份验证时，AD FS会传递Negotiate安全报头。Negotiate安全报头允许客户端在Kerberos身份验证和NTLM身份验证之间进行选择。协商过程选择Kerberos身份验证，除非以下条件之一为真：

— 身份验证中涉及的其中一个系统无法使用Kerberos身份验证。

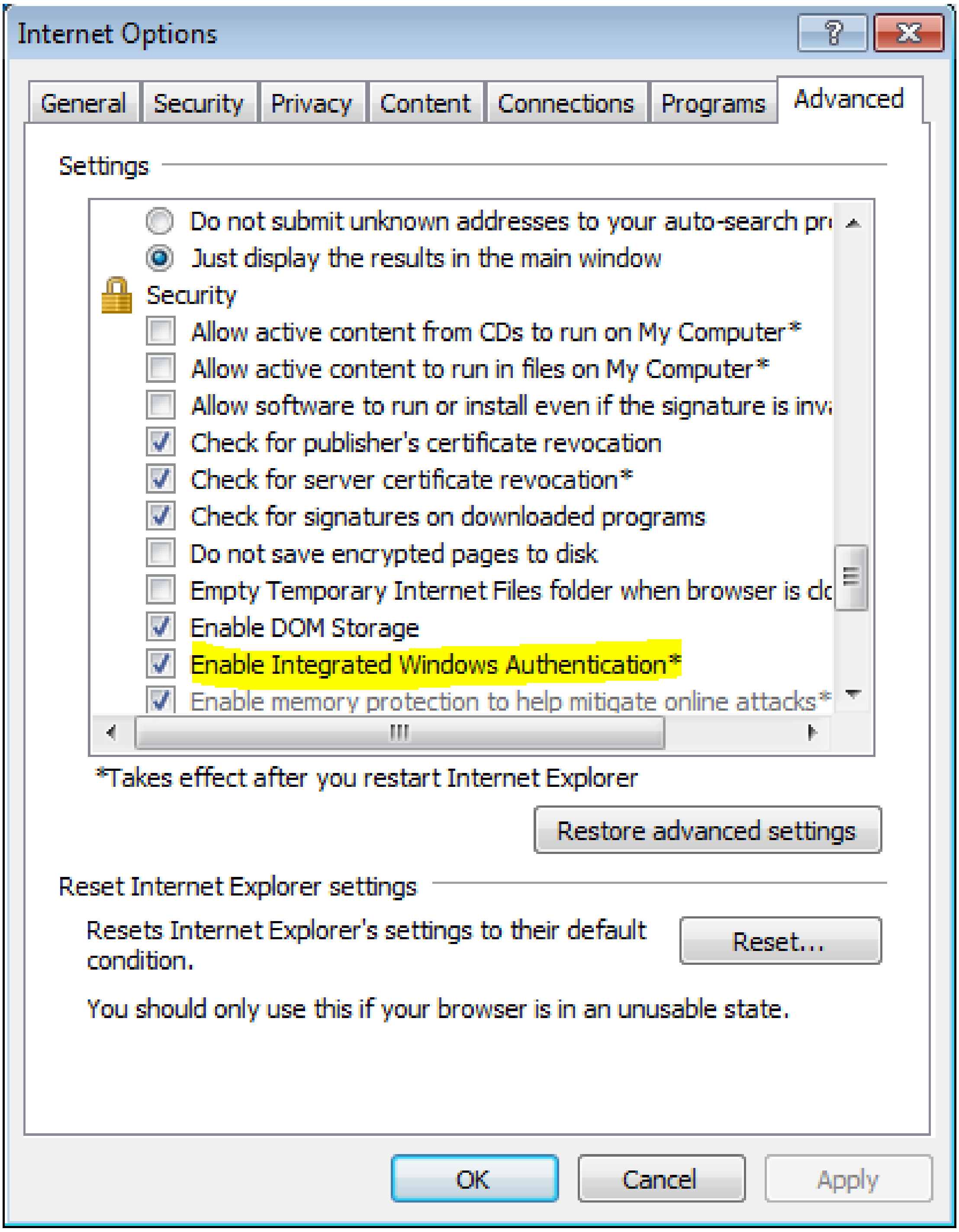
— 调用应用程序不提供足够的信息来使用Kerberos身份验证。

— 要启用协商进程以选择用于网络身份验证的Kerberos协议，客户端应用程序必须提供SPN、用户主体名称(UPN)或网络基本输入/输出系统(NetBIOS)帐户名作为目标名称。否则，协商进程始终选择NTLM协议作为首选身份验证方法。

配置浏览器

Microsoft Internet Explorer

1. 确保选**中Internet Explorer** > **Advanced** > **Enable Integrated Windows Authentication**。



Settings

○ Do not submit unknown addresses to your auto-search pr

● Just display the results in the main window

Security

□ Allow active content from CDs to run on My Computer*

□ Allow active content to run in files on My Computer*

□ Allow software to run or install even if the signature is inv

☑ Check for publisher's certificate revocation

☑ Check for server certificate revocation*

☑ Check for signatures on downloaded programs

□ Do not save encrypted pages to disk

□ Empty Temporary Internet Files folder when browser is clo

☑ Enable DOM Storage

☑ Enable Integrated Windows Authentication*

☑ Enable memory protection to help mitigate online attacks*

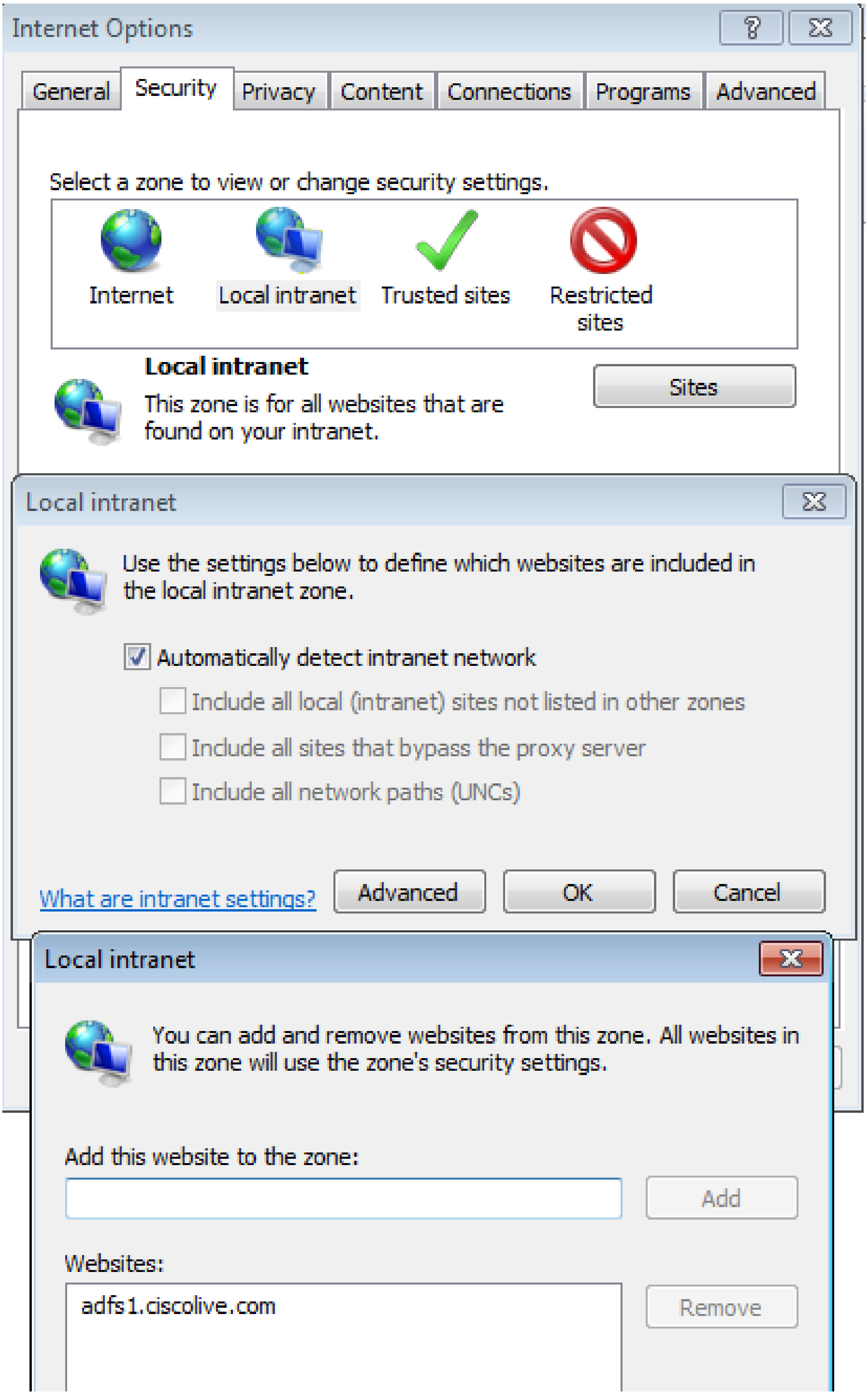
*Takes effect after you restart Internet Explorer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

2. 在“安全”>“内部网区**”>“站点”**下添加**AD FS URL**。



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet　Local intranet　Trusted sites　Restricted sites

Local intranet

This zone is for all websites that are found on your intranet.

Sites

Local intranet

Use the settings below to define which websites are included in the local intranet zone.

☑ Automatically detect intranet network

□ Include all local (intranet) sites not listed in other zones

□ Include all sites that bypass the proxy server

□ Include all network paths (UNCs)

What are intranet settings?　Advanced　OK　Cancel

Local intranet

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

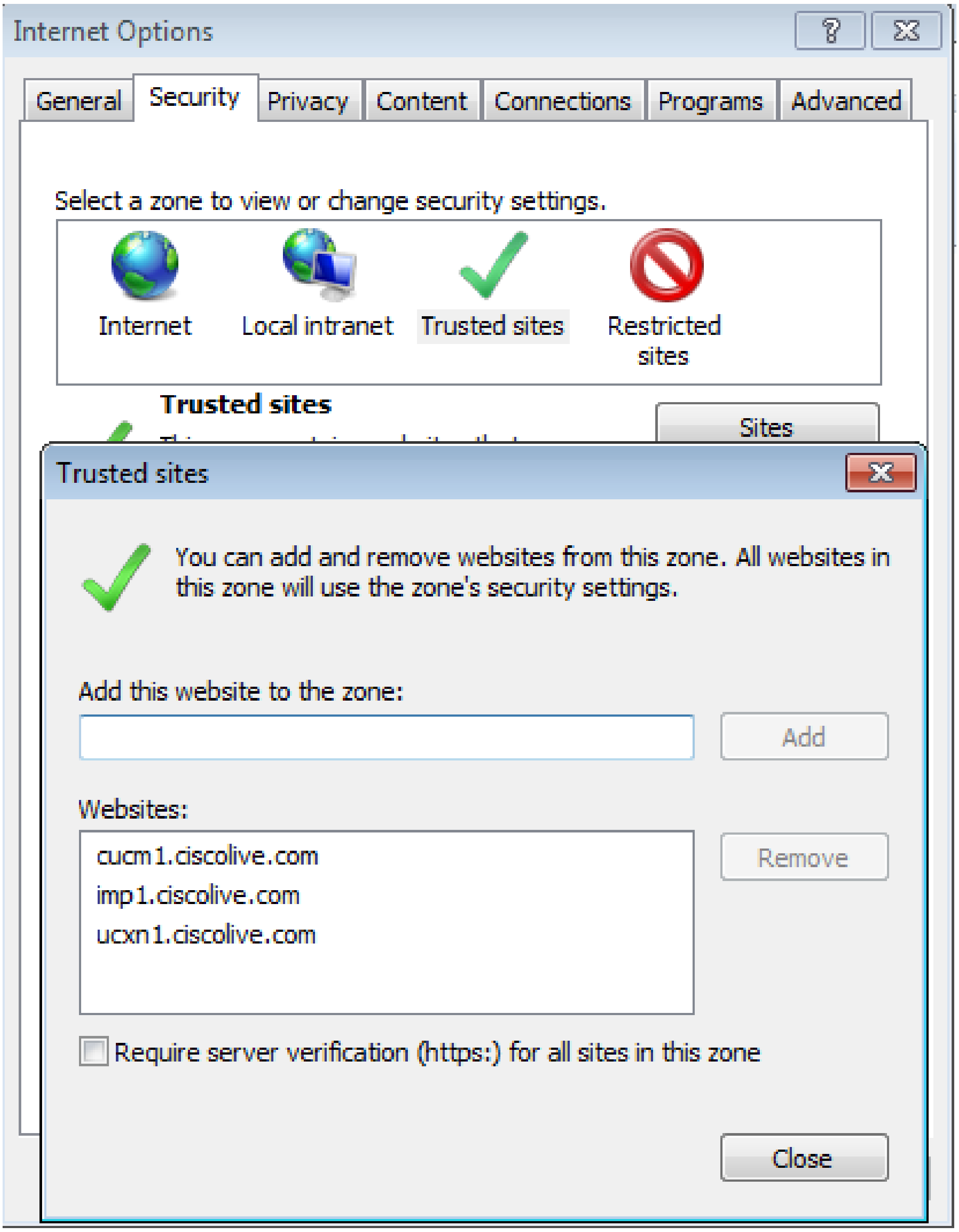
Add

Websites:

adfs1.ciscolive.com

Remove

3. 将CUCM、IMP和Unity主机名添加到“安全”(Security)>“受**信任的站点”(Trusted sites)**。



You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

Add

Websites:

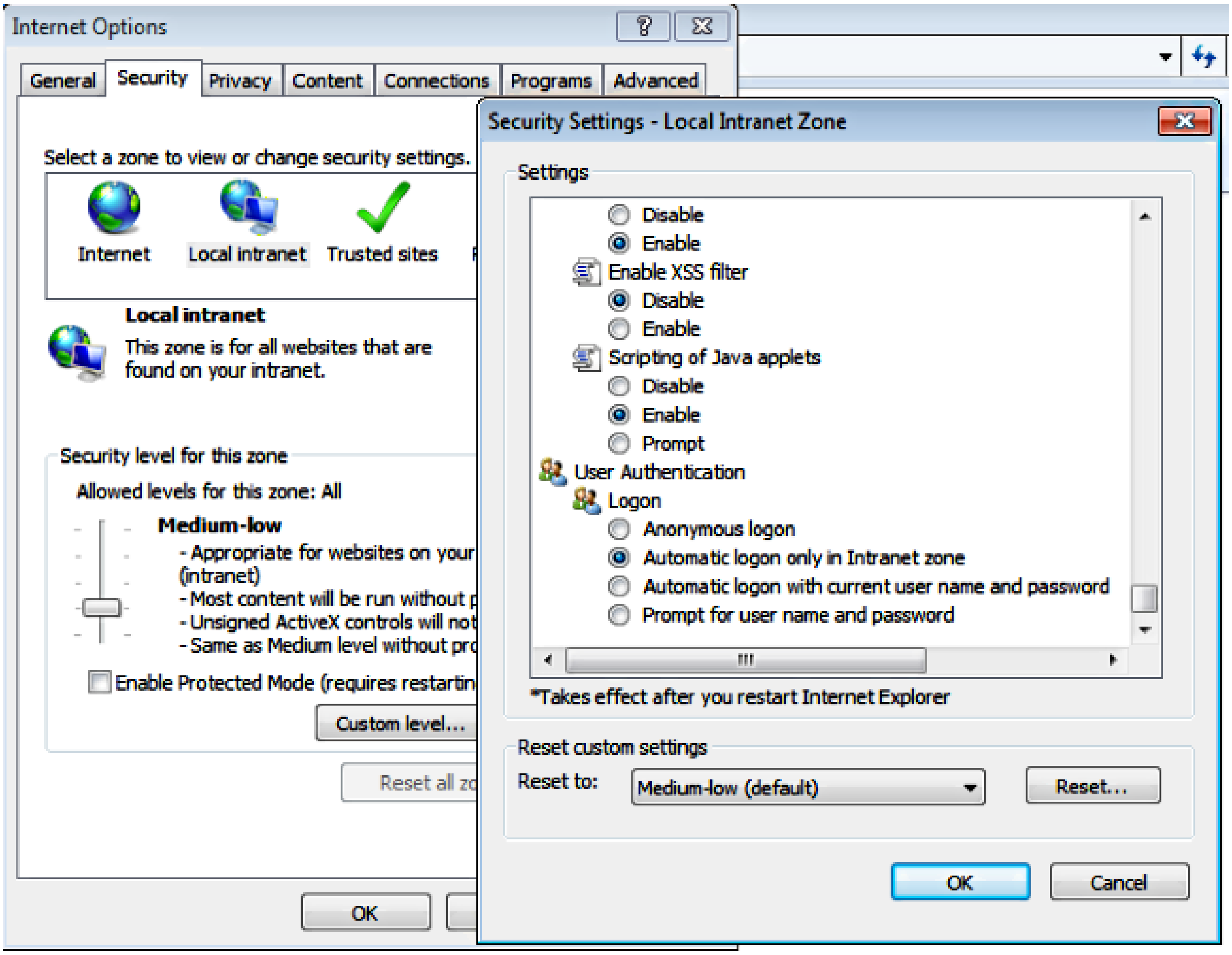
cucm1.ciscolive.com
imp1.ciscolive.com
ucxn1.ciscolive.com

Remove

□ Require server verification (https:) for all sites in this zone

Close

4. 确保配置了Internet Exporer > **security** > Local Intranet > Security Settings > User Authentication - Logon ，以便为Intranet站点使用登录凭据。



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites

Local intranet

This zone is for all websites that are found on your intranet.

Security level for this zone

Allowed levels for this zone: All

Medium-low

- Appropriate for websites on your (intranet)
- Most content will be run without p
- Unsigned ActiveX controls will not
- Same as Medium level without pro

□ Enable Protected Mode (requires restartin

Custom level...

Reset all zo

OK

Security Settings - Local Intranet Zone

Settings

○ Disable
● Enable
Enable XSS filter
● Disable
○ Enable
Scripting of Java applets
○ Disable
● Enable
○ Prompt
User Authentication
Logon
○ Anonymous logon
● Automatic logon only in Intranet zone
○ Automatic logon with current user name and password
○ Prompt for user name and password

*Takes effect after you restart Internet Explorer

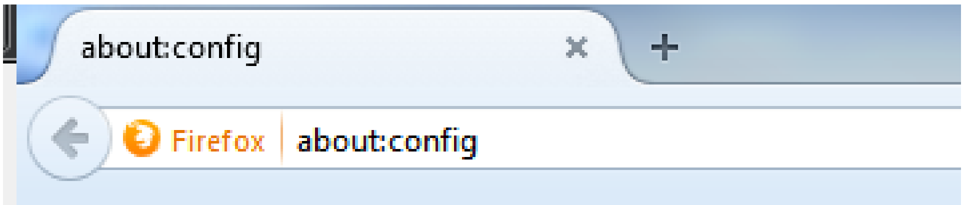
Reset custom settings

Reset to: Medium-low (default) | Reset...

OK | Cancel

Mozilla Firefox

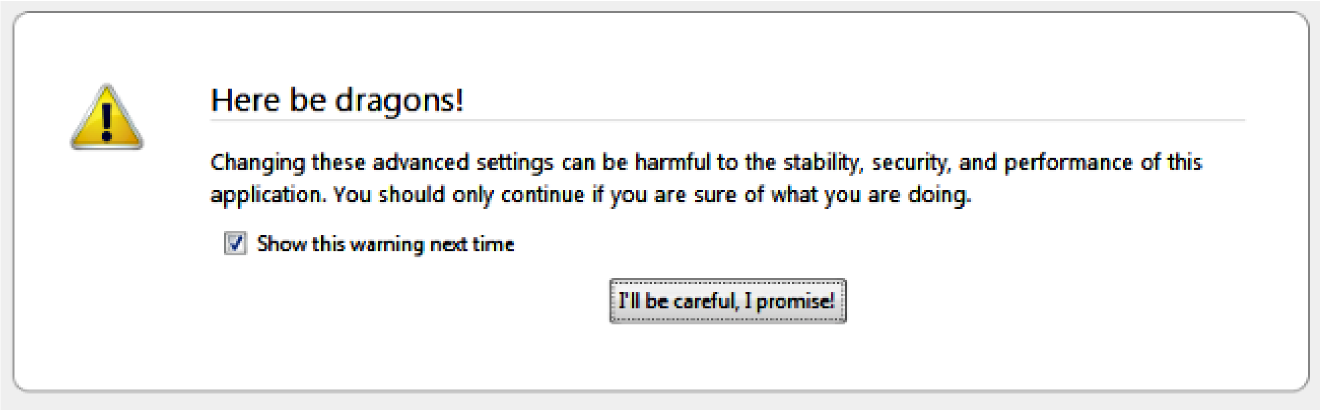
1. 打开Firefox，在**地址栏**中输入about:config。



about:config

Firefox | about:config

2. 单击**我会小心的，我保证！**



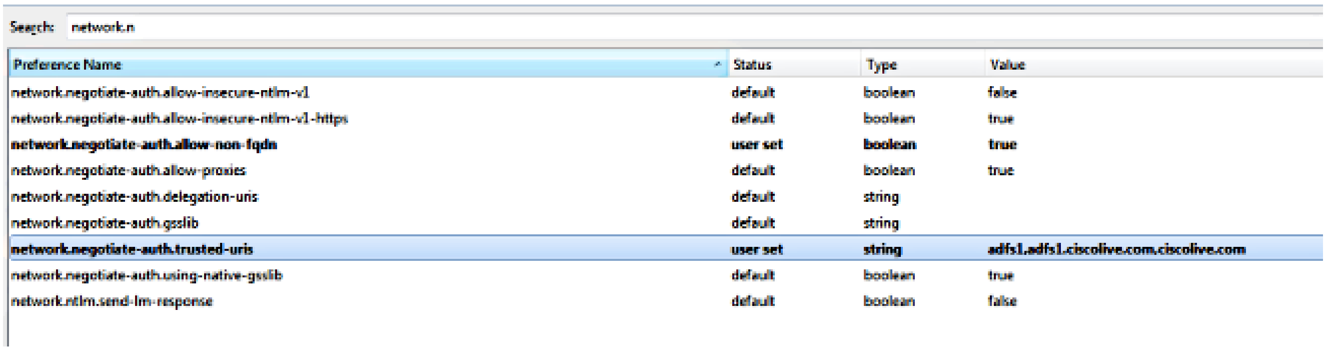
Here be dragons!

Changing these advanced settings can be harmful to the stability, security, and performance of this application. You should only continue if you are sure of what you are doing.

☑ Show this warning next time

I'll be careful, I promise!

3. 双击首选项名称**network.negotiate-auth.allow-non-fqdn**为**true**,**network.negotiate-auth.trusted-uris** 为**ciscolive.com**，**adfs1.ciscolive.com**以进行修改。



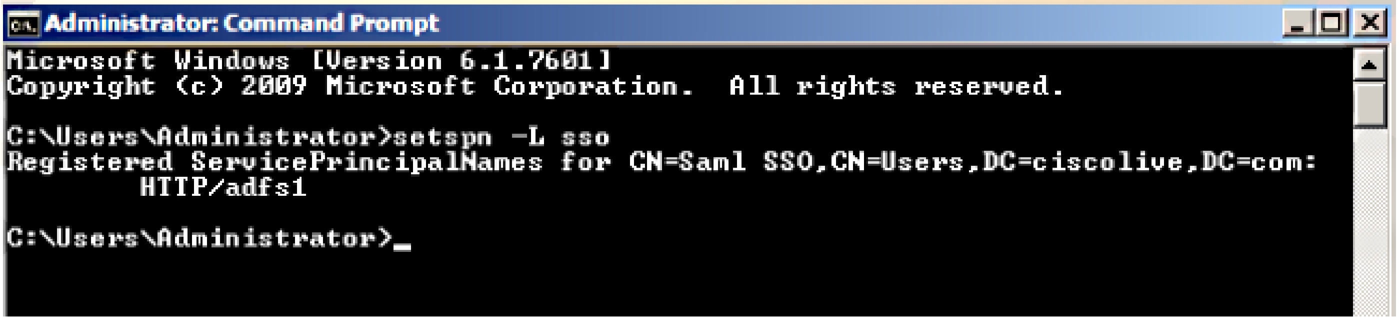
Search: network.n

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

4. 关闭Firefox并重新打开。

验证

要检查AD FS服务器的SPN是否已正确创建，请输入**setspn**命令并查看输出。

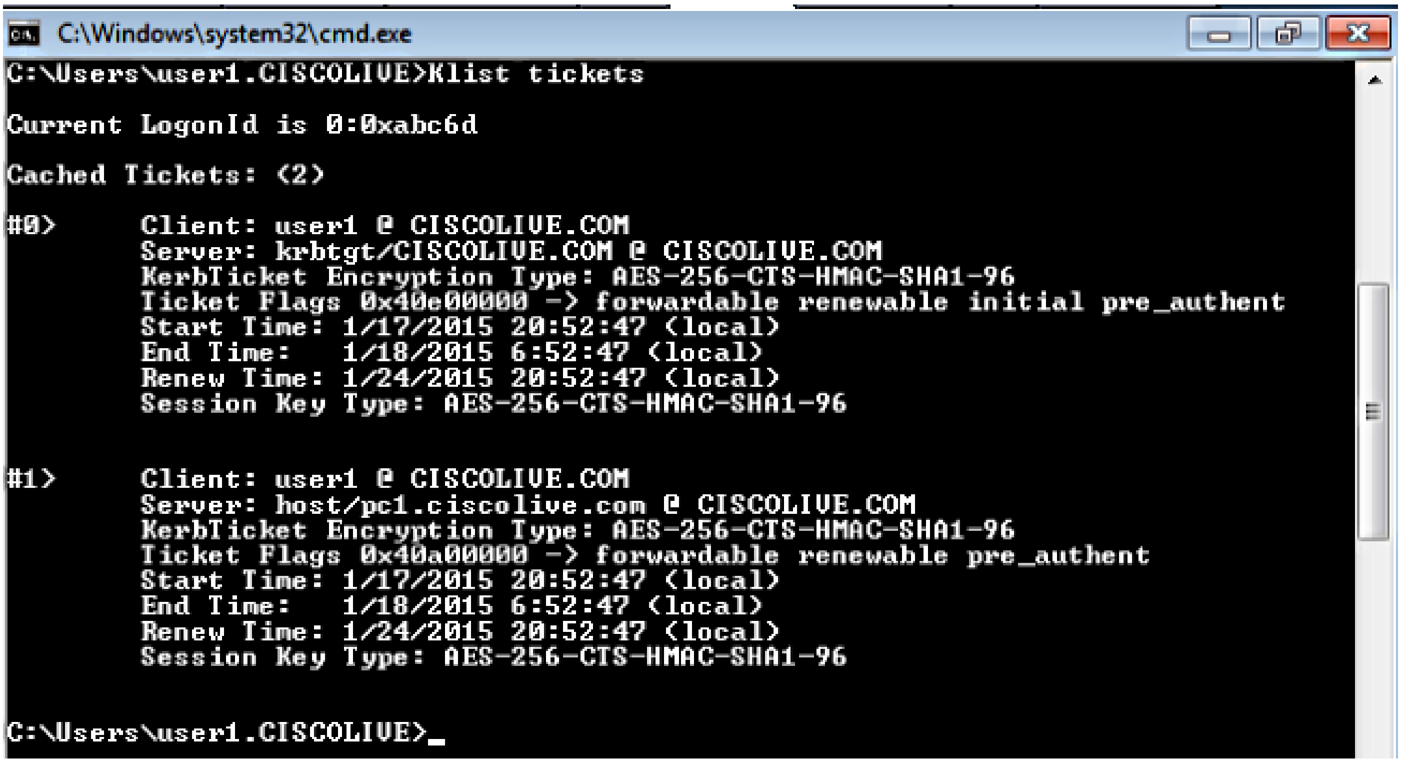


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\Users\Administrator>_
```

检查客户端计算机是否具有Kerberos票证：



```
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>_
```

完成以下步骤，以验证正在使用哪种身份验证（Kerberos或NTLM身份验证）。

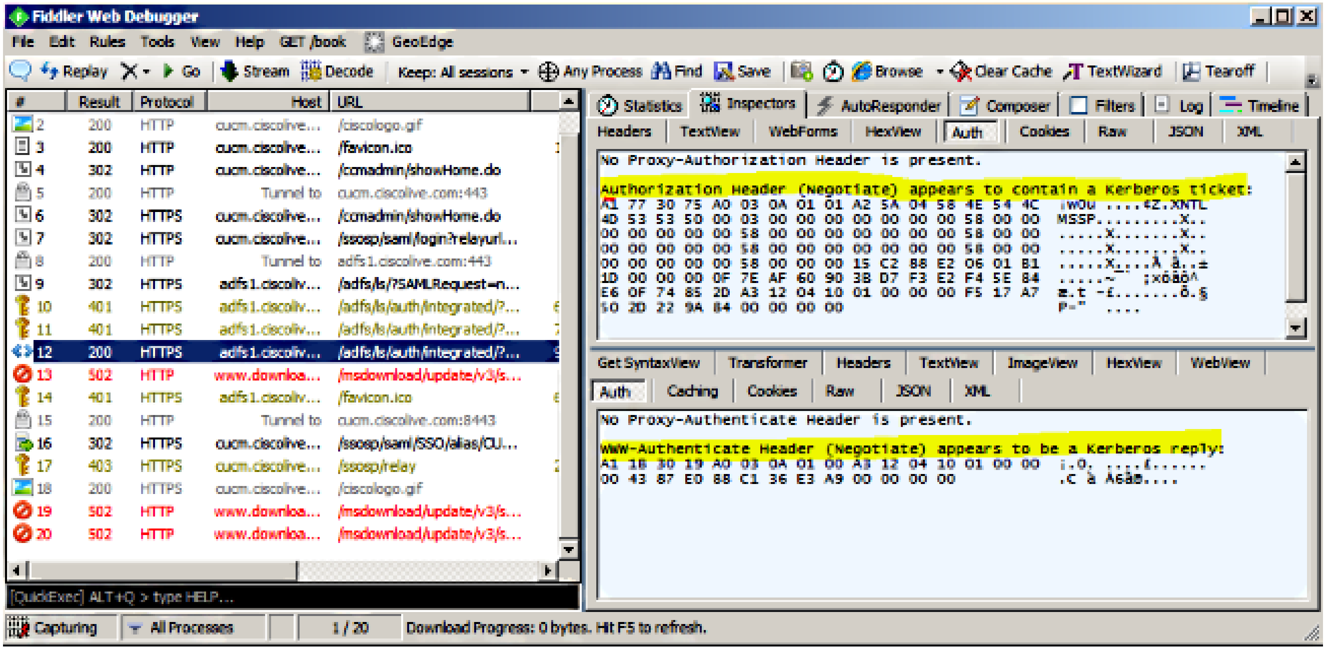
1. 将Fiddler工具下载到您的客户端并安装。

2. 关闭所有Microsoft 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之间的传递代理并侦听所有流量。

4. 打开Microsoft Internet Explorer，浏览到CUCM，然后点击一些链接以生成流量。

5. 返回到Fiddler主窗口，选择其结果为200（成功）的帧之一，您可以将Kerberos视为**身份验证**机制


Fiddler Web Debugger
File Edit Rules Tools View Help GET /book GeoEdge
Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff
Statistics Inspectors AutoResponder Composer Filters Log Timeline
Headers TextView WebForms HexView Auth Cookies Raw JSON XML
Get SyntaxView Transformer Headers TextView ImageView HexView WebView
Auth Caching Cookies Raw JSON XML
[QuickExec] ALT+Q > type HELP...
Capturing All Processes 1 / 20
Download Progress: 0 bytes. Hit F5 to refresh.

#	Result	Protocol	Host	URL
2	200	HTTP	cucm.ciscolive...	/ciscologo.gif
3	200	HTTP	cucm.ciscolive...	/favicon.ico
4	302	HTTP	cucm.ciscolive...	/ccmadmin/showHome.do
5	200	HTTP	Tunnel to	cucm.ciscolive.com:443
6	302	HTTPS	cucm.ciscolive...	/ccmadmin/showHome.do
7	302	HTTPS	cucm.ciscolive...	/ssosp/saml/login?relayurl...
8	200	HTTP	Tunnel to	adfs1.ciscolive.com:443
9	302	HTTPS	adfs1.ciscoliv...	/adfs/ls/?SAMLRequest=n...
10	401	HTTPS	adfs1.ciscoliv...	/adfs/ls/auth/integrated/?...
11	401	HTTPS	adfs1.ciscoliv...	/adfs/ls/auth/integrated/?...
12	200	HTTPS	adfs1.ciscoliv...	/adfs/ls/auth/integrated/?...
13	502	HTTP	www.downloa...	/msdownload/update/v3/s...
14	401	HTTPS	adfs1.ciscoliv...	/favicon.ico
15	200	HTTP	Tunnel to	cucm.ciscolive.com:8443
16	302	HTTPS	cucm.ciscolive...	/ssosp/saml/SSO/alias/CU...
17	403	HTTPS	cucm.ciscolive...	/ssosp/relay
18	200	HTTPS	cucm.ciscolive...	/ciscologo.gif
19	502	HTTP	www.downloa...	/msdownload/update/v3/s...
20	502	HTTP	www.downloa...	/msdownload/update/v3/s...

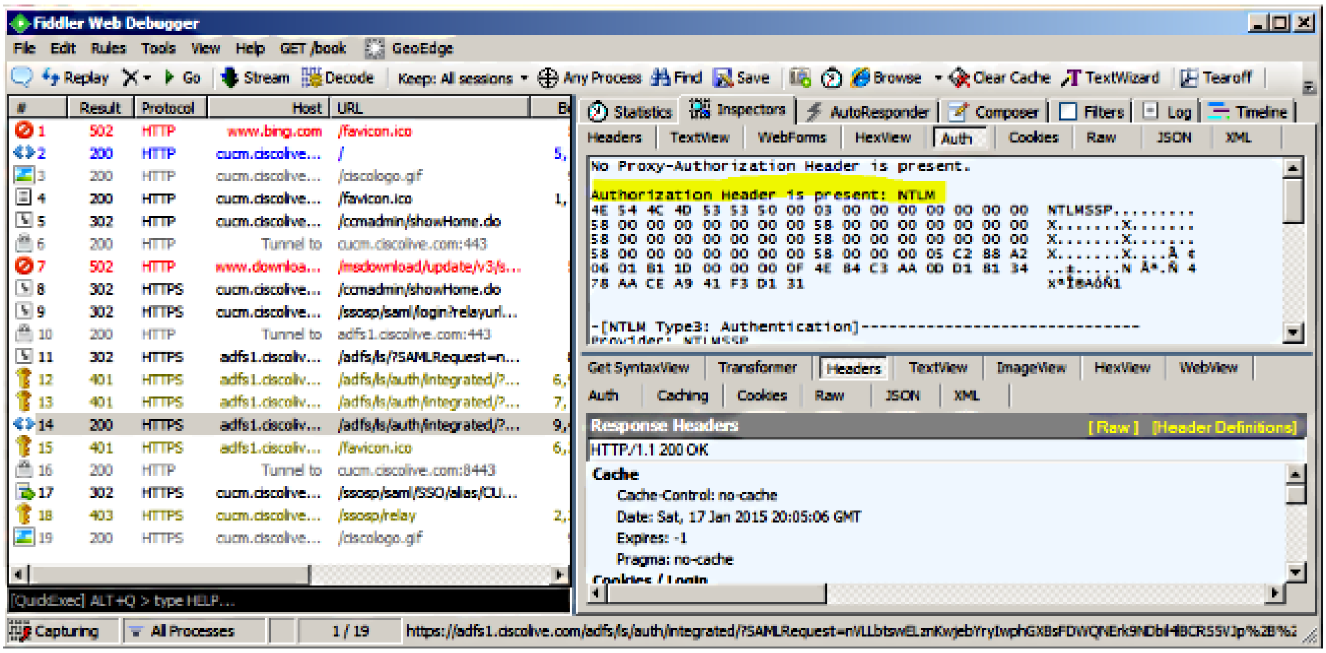
```
No Proxy-Authorization Header is present.

Authorization Header (Negotiate) appears to contain a Kerberos ticket:
A1 77 30 75 A0 03 0A 01 01 A2 5A 04 58 4E 54 4C   ¡w0u .....¢Z.XNTL
4D 53 53 50 00 03 00 00 00 00 00 00 00 58 00 00   MSSP.........X..
00 00 00 00 00 58 00 00 00 00 00 00 00 58 00 00   .....X.......X..
00 00 00 00 00 58 00 00 00 00 00 00 00 58 00 00   .....X.......X..
00 00 00 00 00 58 00 00 00 15 C2 88 E2 06 01 B1   .....X....Â â..±
1D 00 00 00 0F 7E AF 60 90 3B D7 F3 E2 F4 5E 84   .....~¯`  ;×óâô^
E6 0F 74 85 2D A3 12 04 10 01 00 00 00 F5 17 A7   æ.t -£.......õ.§
50 2D 22 9A 84 00 00 00 00                        P-"  ....
```

```
No Proxy-Authenticate Header is present.

WWW-Authenticate Header (Negotiate) appears to be a Kerberos reply:
A1 18 30 19 A0 03 0A 01 00 A3 12 04 10 01 00 00   ¡.0. ....£......
00 43 87 E0 88 C1 36 E3 A9 00 00 00 00            .C à Á6ã©....
```

6. 如果身份验证类型为NTLM，则在帧的开头看到**Negotiate - NTLMSSP**，如下所示。


Fiddler Web Debugger
File Edit Rules Tools View Help GET /book GeoEdge
Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff
Statistics Inspectors AutoResponder Composer Filters Log Timeline
Headers TextView WebForms HexView Auth Cookies Raw JSON XML
Get SyntaxView Transformer Headers TextView ImageView HexView WebView
Auth Caching Cookies Raw JSON XML
[QuickExec] ALT+Q > type HELP...
Capturing All Processes 1 / 19
https://adfs1.ciscolive.com/adfs/ls/auth/integrated/?SAMLRequest=nVLLbtswELznKwjebYry1wphGXBsFDWQNErk9NDbl4BCRS5VJp%2B%2

#	Result	Protocol	Host	URL	B
1	502	HTTP	www.bing.com	/favicon.ico	
2	200	HTTP	cucm.ciscolive...	/	5,
3	200	HTTP	cucm.ciscolive...	/ciscologo.gif	
4	200	HTTP	cucm.ciscolive...	/favicon.ico	1,
5	302	HTTP	cucm.ciscolive...	/ccmadmin/showHome.do	
6	200	HTTP	Tunnel to	cucm.ciscolive.com:443	
7	502	HTTP	www.downloa...	/msdownload/update/v3/s...	
8	302	HTTPS	cucm.ciscolive...	/ccmadmin/showHome.do	
9	302	HTTPS	cucm.ciscolive...	/ssosp/saml/login?relayurl...	
10	200	HTTP	Tunnel to	adfs1.ciscolive.com:443	
11	302	HTTPS	adfs1.ciscoliv...	/adfs/ls/?SAMLRequest=n...	
12	401	HTTPS	adfs1.ciscoliv...	/adfs/ls/auth/integrated/?...	6,
13	401	HTTPS	adfs1.ciscoliv...	/adfs/ls/auth/integrated/?...	7,
14	200	HTTPS	adfs1.ciscoliv...	/adfs/ls/auth/integrated/?...	9,
15	401	HTTPS	adfs1.ciscoliv...	/favicon.ico	6,
16	200	HTTP	Tunnel to	cucm.ciscolive.com:8443	
17	302	HTTPS	cucm.ciscolive...	/ssosp/saml/SSO/alias/CU...	
18	403	HTTPS	cucm.ciscolive...	/ssosp/relay	2,
19	200	HTTPS	cucm.ciscolive...	/ciscologo.gif	

```
No Proxy-Authorization Header is present.

Authorization Header is present: NTLM
4E 54 4C 4D 53 53 50 00 03 00 00 00 00 00 00 00   NTLMSSP.........
58 00 00 00 00 00 00 00 58 00 00 00 00 00 00 00   X.......X.......
58 00 00 00 00 00 00 00 58 00 00 00 00 00 00 00   X.......X.......
58 00 00 00 00 00 00 00 58 00 00 00 05 C2 88 A2   X.......X....Â ¢
06 01 B1 1D 00 00 00 0F 4E 84 C3 AA 0D D1 81 34   ..±.....N Ãª.Ñ 4
78 AA CE A9 41 F3 D1 31                           xªÎ©AóÑ1


-[NTLM Type3: Authentication]------------------------------
Provider: NTLMSSP
```

Response Headers [Raw] [Header Definitions]

HTTP/1.1 200 OK

Cache

Cache-Control: no-cache
Date: Sat, 17 Jan 2015 20:05:06 GMT
Expires: -1
Pragma: no-cache

Cookies / Login

故障排除

如果所有配置和验证步骤都按照本文档所述完成，并且您仍有登录问题，则必须咨询Microsoft Windows Active Directory / AD FS管理员。