

# Configurar SAML SSO com autenticação Kerberos

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configurar o AD FS](#)

[Configurar navegador](#)

[Microsoft Internet Explorer](#)

[Mozilla FireFox](#)

[Verificar](#)

[Troubleshoot](#)

## Introduction

Este documento descreve como configurar o Ative Directory e o Ative Directory Federation Service (AD FS) Versão 2.0 para permitir que ele use a autenticação Kerberos por clientes Jabber (Microsoft Windows apenas), que permite que os usuários façam login com seu login do Microsoft Windows e não sejam solicitados a fornecer credenciais.

**Caution:** Este documento é baseado em um ambiente de laboratório e pressupõe que você está ciente do impacto das alterações feitas. Consulte a documentação relevante do produto para entender o impacto das alterações feitas.

## Prerequisites

## Requirements

A Cisco recomenda que você:

- O AD FS Versão 2.0 foi instalado e configurado com os produtos Cisco Collaboration como Confiança de terceira parte confiável
- Produtos de colaboração como Cisco Unified Communications Manager (CUCM) IM and Presence, Cisco Unity Connection (UCXN) e CUCM habilitados para usar o Security Assertion Markup Language (SAML) Single Sign-on (SSO)

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

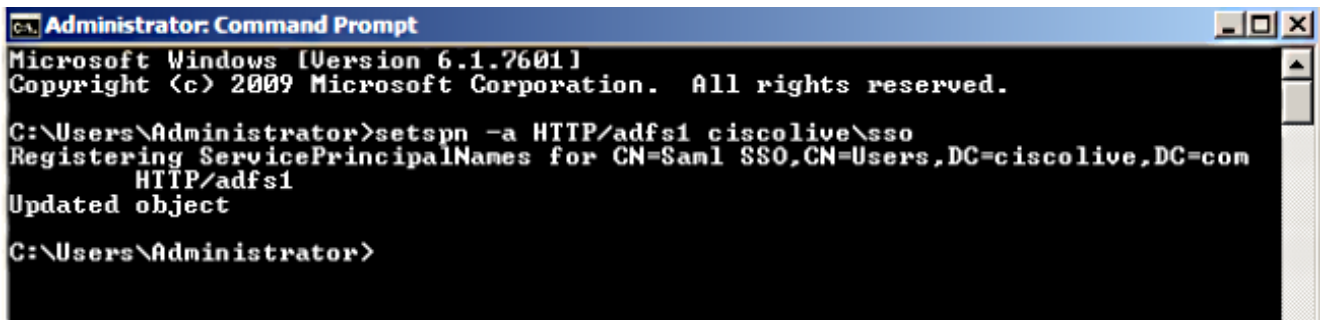
- Ative Directory 2008 (nome de host: ADFS1.ciscolive.com)
- AD FS Versão 2.0 (Nome do host: ADFS1.ciscolive.com)
- CUCM (nome de host: CUCM1.ciscolive.com)
- Microsoft Internet Explorer versão 10
- Mozilla Firefox versão 34
- Telerik Fiddler versão 4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Configurar

### Configurar o AD FS

1. Configure o AD FS Versão 2.0 com Service Principal Name (SPN) para habilitar o computador cliente no qual o Jabber está instalado para solicitar tíquetes, o que, por sua vez, permite que o computador cliente se comunique com um serviço do 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=Sam1 SSO,CN=Users,DC=ciscolive,DC=com
HTTP/adfs1
Updated object

C:\Users\Administrator>
```

Consulte o [AD FS 2.0: Como configurar o SPN \(servicePrincipalName\) para a conta de serviço](#) para obter mais informações.

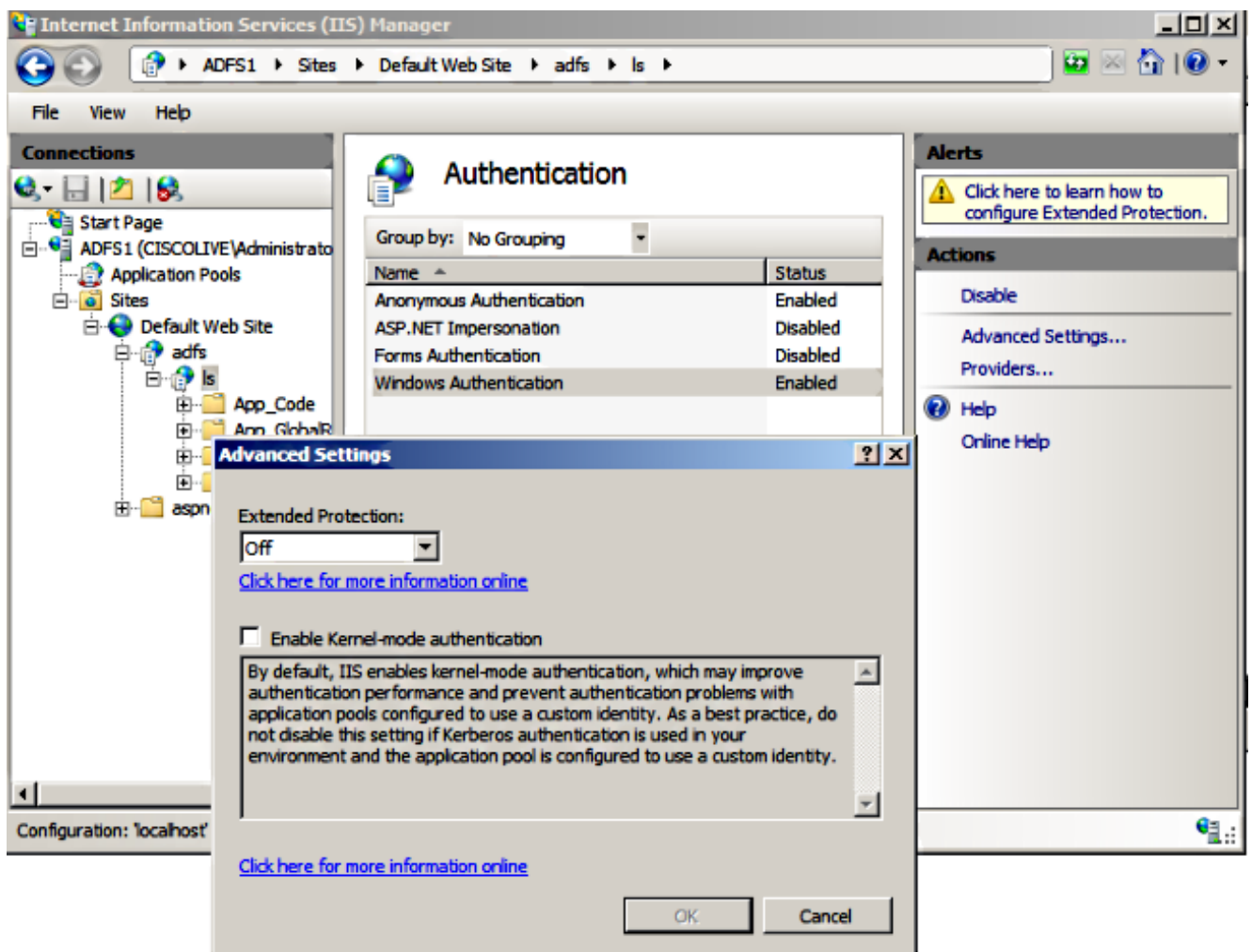
2. Certifique-se de que a configuração de autenticação predefinida para o serviço AD FS (em `C:\inetpub\adfs\ls\web.config`) é **Autenticação Integrada do Windows**. Verifique se ele não foi alterado para **Autenticação baseada em formulário**.

```

<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>
  <commonDomainCookieWriter="" 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>

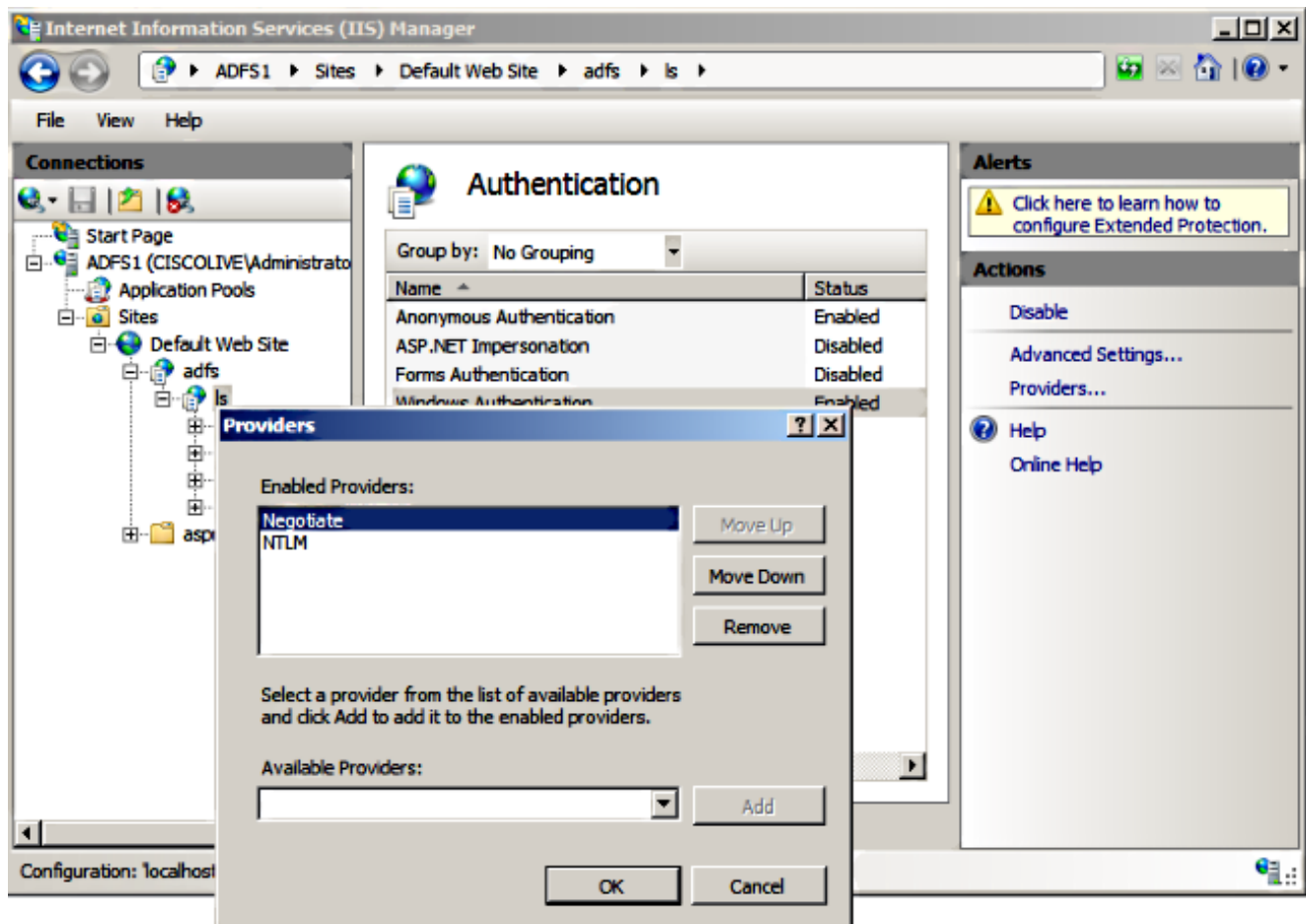
```

3. Selecione **Autenticação do Windows** e clique em **Configurações avançadas** no painel direito. Em Advanced Settings (Configurações avançadas), desmarque **Enable Kernel-mode authentication**, verifique se Extended Protection está **desativado** e clique em **OK**.



4. Certifique-se de que o AD FS Versão 2.0 suporta o protocolo Kerberos e o protocolo NT LAN Manager (NTLM) porque todos os clientes não Windows não podem usar Kerberos e dependem do NTLM.

No painel direito, selecione **Provedores** e verifique se **Negociar** e **NTLM** estão presentes em Provedores Habilitados:



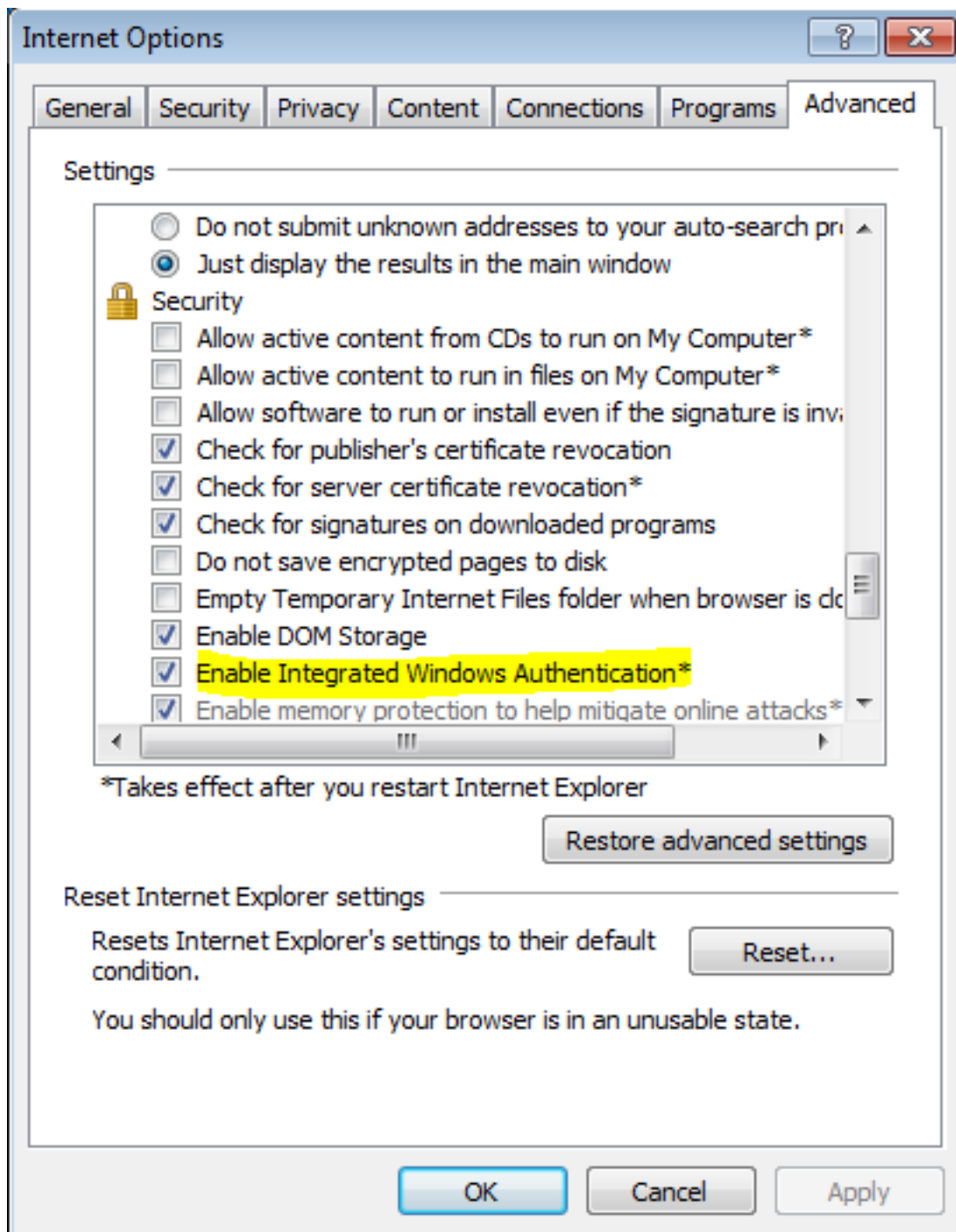
**Note:** O AD FS passa o cabeçalho de segurança Negociar quando a autenticação integrada do Windows é usada para autenticar solicitações de clientes. O cabeçalho de segurança Negociar permite que os clientes selecionem entre a autenticação Kerberos e a autenticação NTLM. O processo Negociar seleciona a autenticação Kerberos, a menos que uma destas condições seja verdadeira:

- Um dos sistemas envolvidos na autenticação não pode usar a autenticação Kerberos.
- O aplicativo de chamada não fornece informações suficientes para usar a autenticação Kerberos.
- Para permitir que o processo de negociação selecione o protocolo Kerberos para autenticação de rede, o aplicativo cliente deve fornecer um SPN, um UPN (User Principal Name, nome principal do usuário) ou um NetBIOS (Network Basic Input/Output System, sistema básico de entradas e saídas) como o nome de destino. Caso contrário, o processo Negociar sempre seleciona o protocolo NTLM como o método de autenticação preferencial.

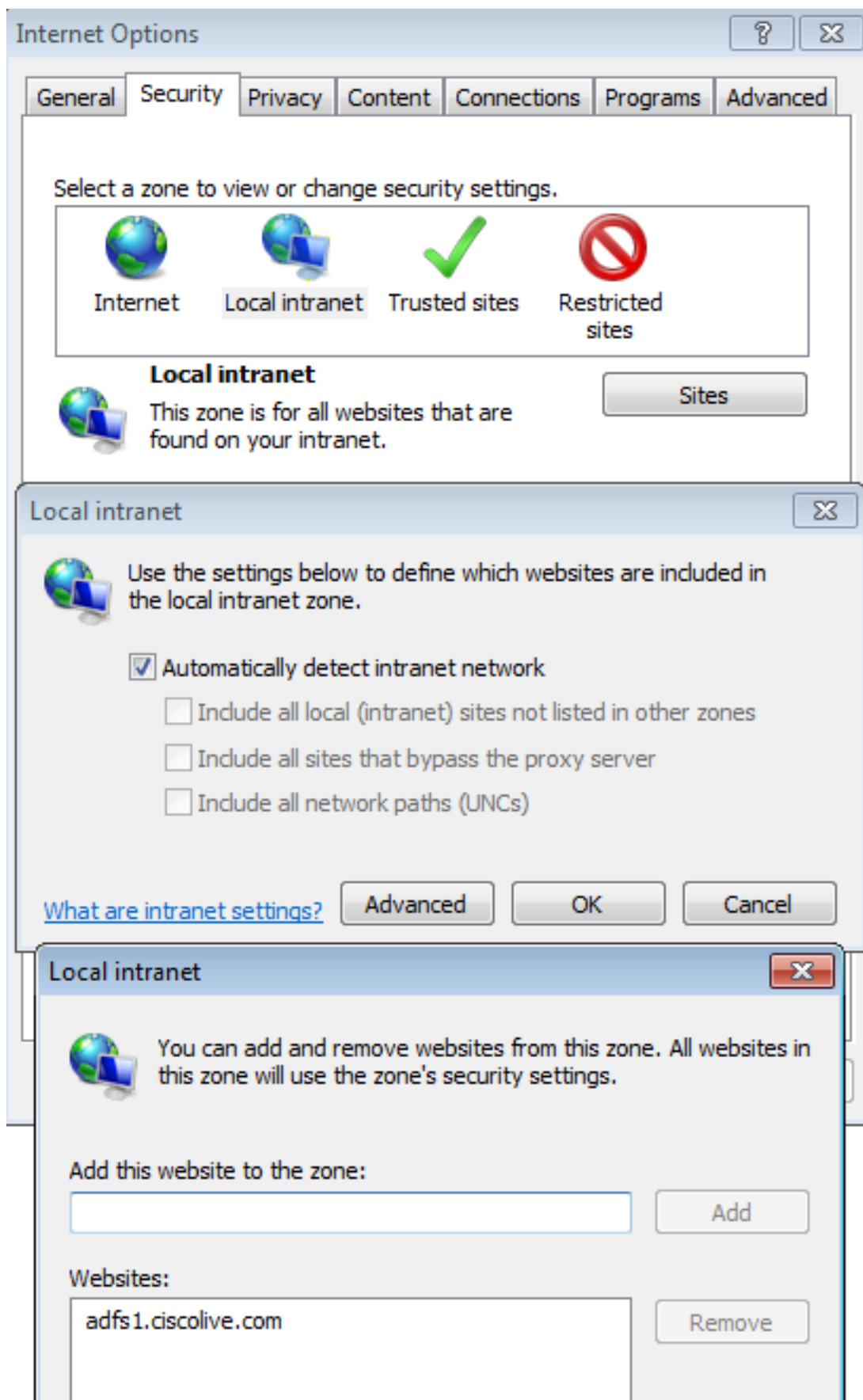
## Configurar navegador

### Microsoft Internet Explorer

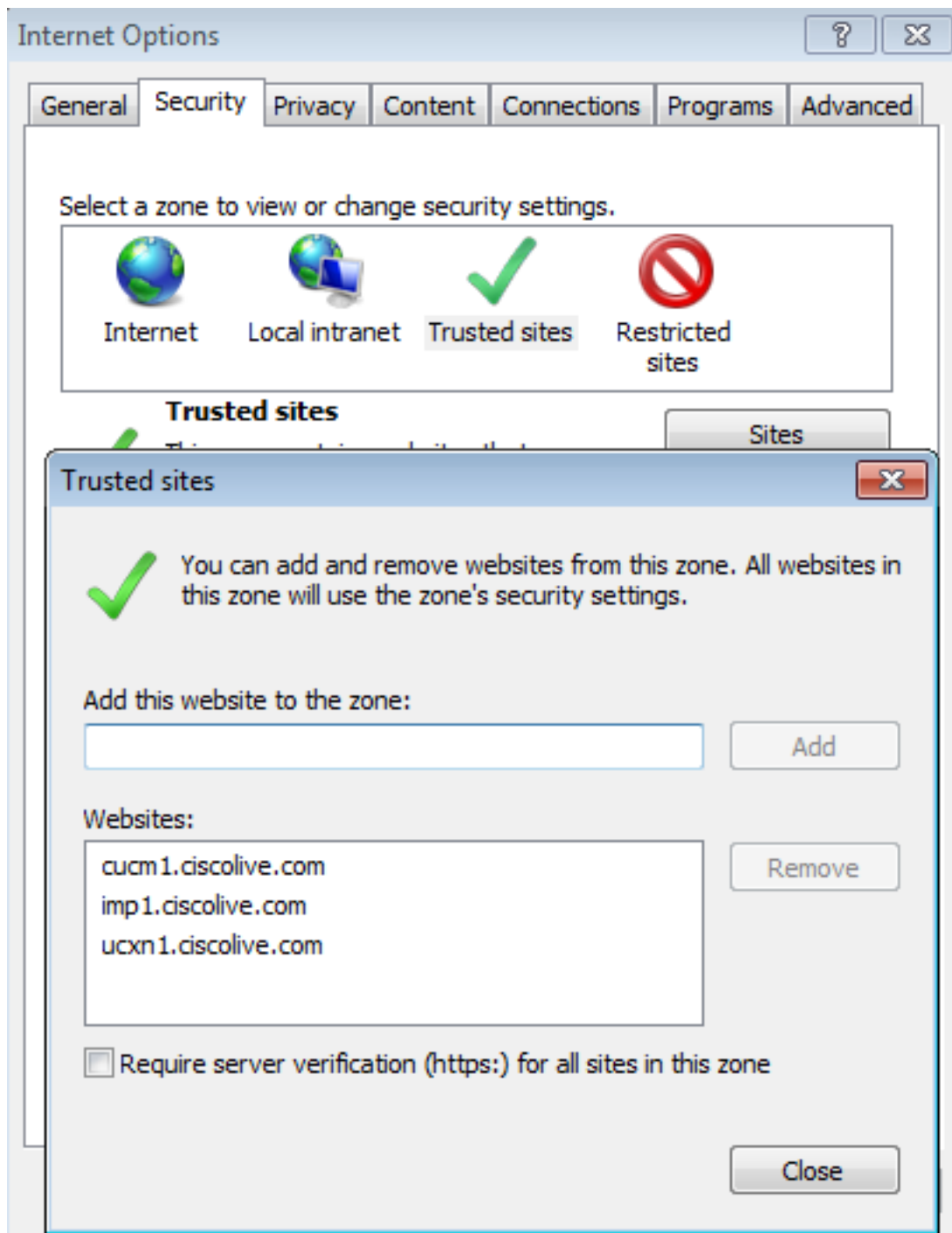
1. Verifique se Internet Explorer > Advanced > Enable Integrated Windows Authentication está marcado.



2. Adicione a URL do AD FS em **Segurança > Zonas de intranet > sites**.

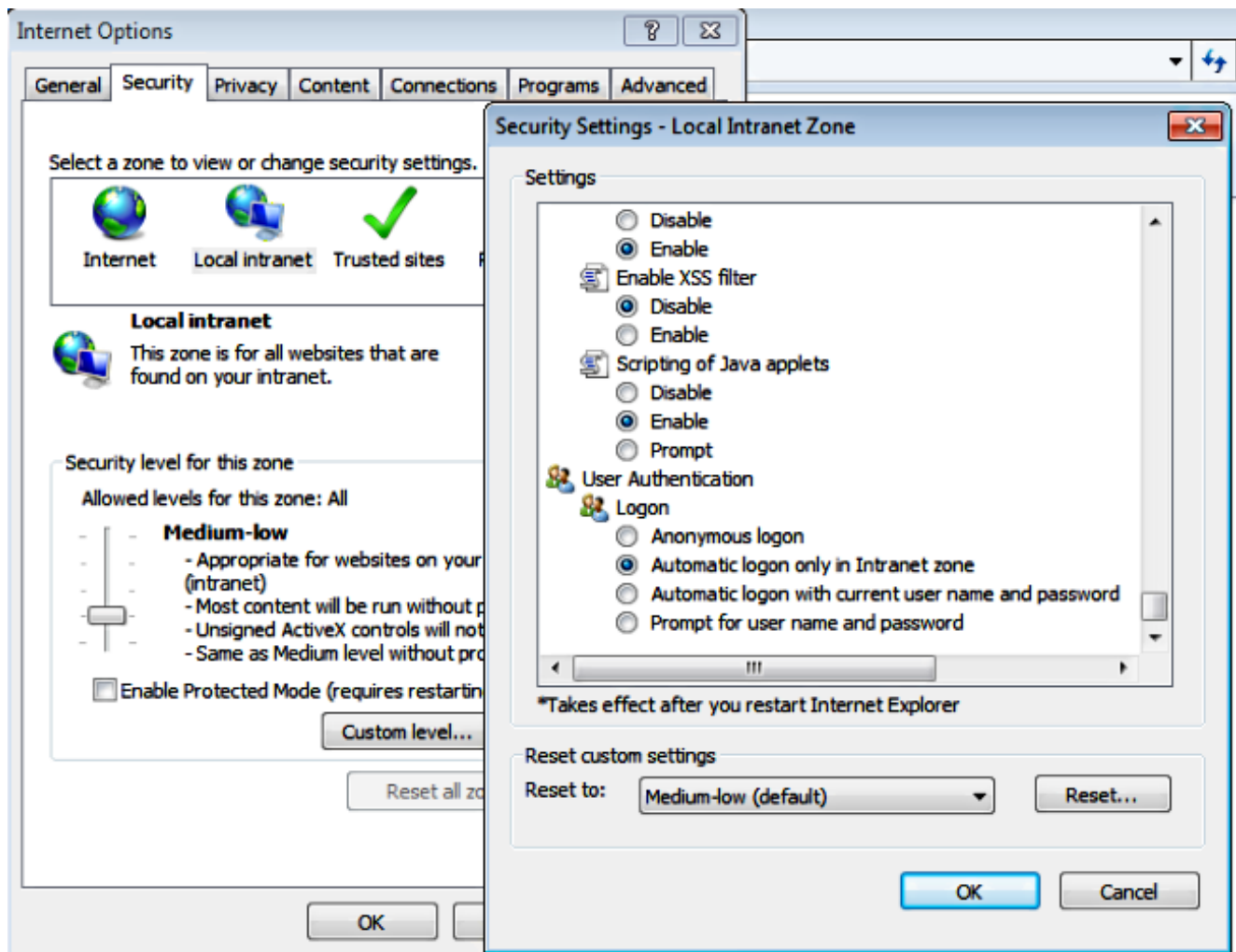


3. Adicione os nomes de host CUCM, IMP e Unity a **Segurança > Sites confiáveis**.



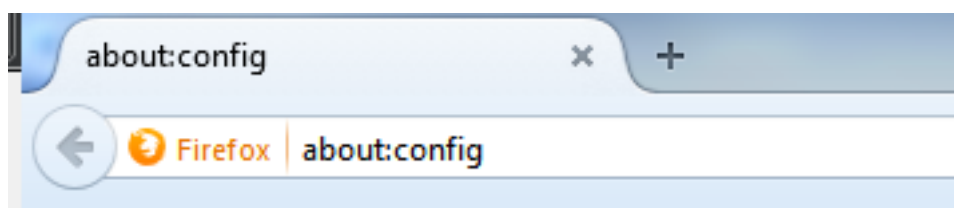
4. Certifique-se de que o Internet Explorer > **segurança** > **Intranet local** > **Configurações de segurança** > **Autenticação do usuário - Logon** esteja configurado para usar as credenciais de login para sites de intranet.





## Mozilla FireFox

1. Abra o Firefox e digite **about:config** na barra de endereços.



2. Clique em **Eu serei cuidadoso, prometo!**





3. Clique duas vezes no nome de preferência `network.negotiation-auth.allow-non-fqdn` para `true` e `network.negotiation-auth.trusted-uris` para `ciscolive.com,adfs1.ciscolive.com` para modificar.

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
<code>network.negotiate-auth.allow-non-fqdn</code>	user set	boolean	true
<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	
<code>network.negotiate-auth.trusted-uris</code>	user set	string	<code>adfs1,adfs1.ciscolive.com,ciscolive.com</code>
<code>network.negotiate-auth.using-native-gsslib</code>	default	boolean	true
<code>network.ntlm.send-lm-response</code>	default	boolean	false

4. Feche o Firefox e reabra.

## Verificar

Para verificar se os SPNs do servidor AD FS foram criados corretamente, insira o comando `setspn` e exiba a saída.

```
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>_
```

Verifique se as máquinas clientes têm tíquetes Kerberos:

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

Current LogonId is 0:0xabc6d

Cached Tickets: (2)

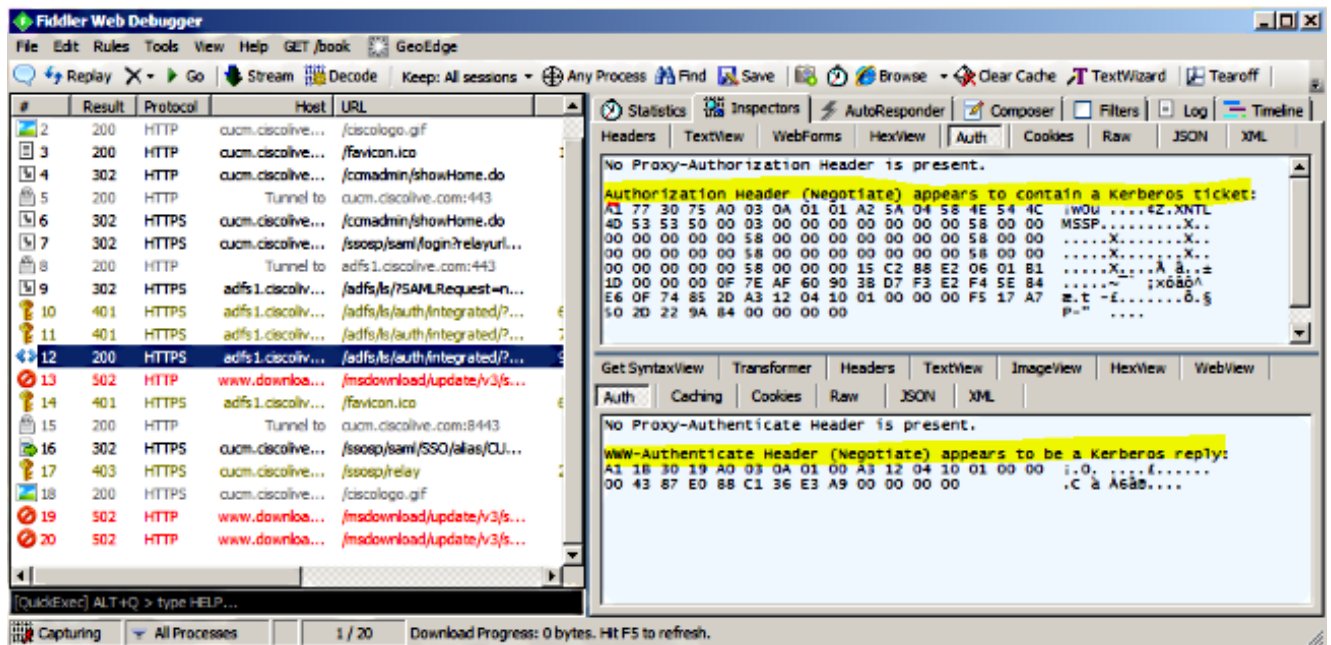
#0> Client: user1 @ CISCOLIVE.COM
Server: krbtgt/CISCOLIVE.COM @ CISCOLIVE.COM
Kerberos Ticket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
Start Time: 1/17/2015 20:52:47 (local)
End Time: 1/18/2015 6:52:47 (local)
Renew Time: 1/24/2015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

#1> Client: user1 @ CISCOLIVE.COM
Server: host/pci.ciscolive.com @ CISCOLIVE.COM
Kerberos Ticket 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

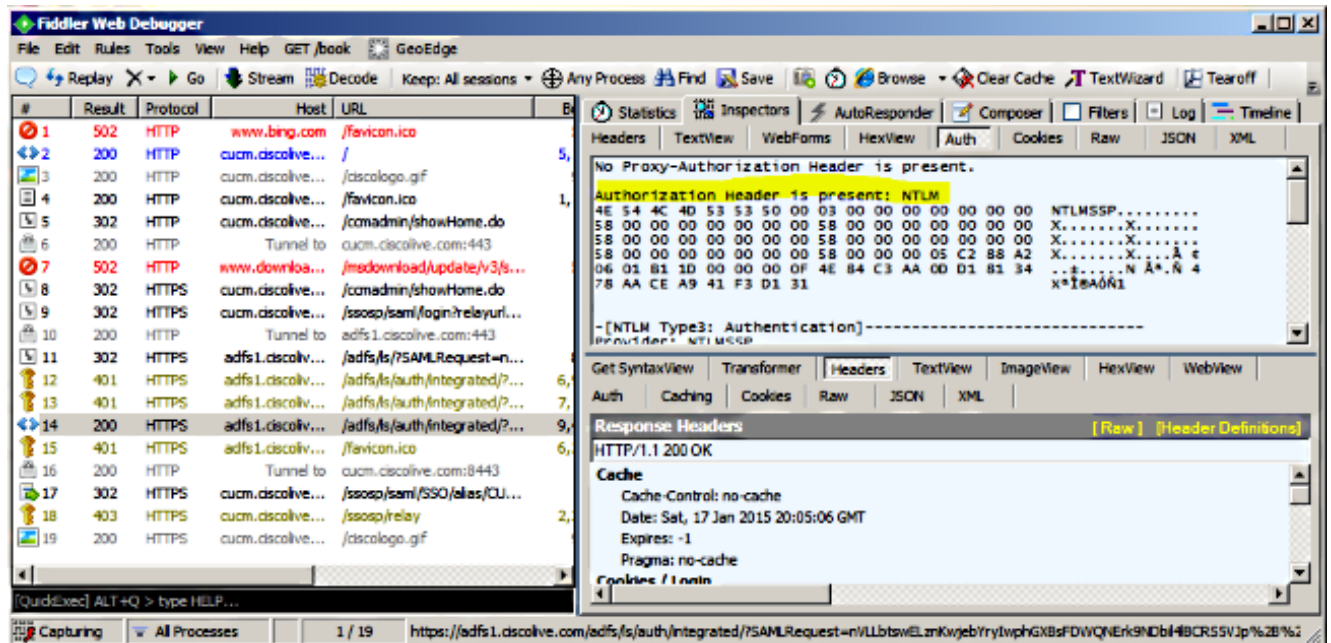
C:\Users\user1.CISCOLIVE>_
```

Conclua estes passos para verificar qual autenticação (autenticação Kerberos ou NTLM) está sendo usada.

1. Baixe a ferramenta Fiddler na sua máquina cliente e instale-a.
2. Feche todas as janelas do Microsoft Internet Explorer.
3. Execute a ferramenta Fiddler e verifique se a opção **Capture Traffic** está ativada no menu File (Arquivo). O Fiddler funciona como um proxy de passagem entre a máquina cliente e o servidor e escuta todo o tráfego.
4. Abra o Microsoft Internet Explorer, navegue até o CUCM e clique em alguns links para gerar tráfego.
5. Consulte a janela principal do Fiddler e escolha um dos Quadros em que o Resultado é 200 (sucesso) e você pode ver Kerberos como Mecanismo de Autenticação



6. Se o tipo de autenticação for NTLM, você verá **Negotiate - NTLMSSP** no início do quadro, como mostrado aqui.



## Troubleshoot

Se todas as etapas de configuração e verificação forem concluídas conforme descrito neste documento e você ainda tiver problemas de login, consulte um Administrador do Microsoft Windows Active Directory / AD FS.