

Configuración de SAML SSO con autenticación Kerberos

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configurar AD FS](#)

[Configurar explorador](#)

[Microsoft Internet Explorer](#)

[Mozilla FireFox](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar Active Directory y Active Directory Federation Service (AD FS) versión 2.0 para permitirle utilizar la autenticación Kerberos por parte de los clientes Jabber (sólo Microsoft Windows), que permite a los usuarios iniciar sesión con su inicio de sesión de Microsoft Windows y no se les solicita las credenciales.

Precaución: Este documento se basa en un entorno de laboratorio y asume que es consciente del impacto de los cambios que realiza. Consulte la documentación del producto correspondiente para comprender el impacto de los cambios que realice.

Prerequisites

Requirements

Cisco recomienda que tenga:

- AD FS versión 2.0 instalada y configurada con productos de Cisco Collaboration como confianza de terceros
- Productos de colaboración como Cisco Unified Communications Manager (CUCM) IM and Presence, Cisco Unity Connection (UCXN) y CUCM habilitados para utilizar el lenguaje de marcado de aserción de seguridad (SAML) Single Sign-on (SSO)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

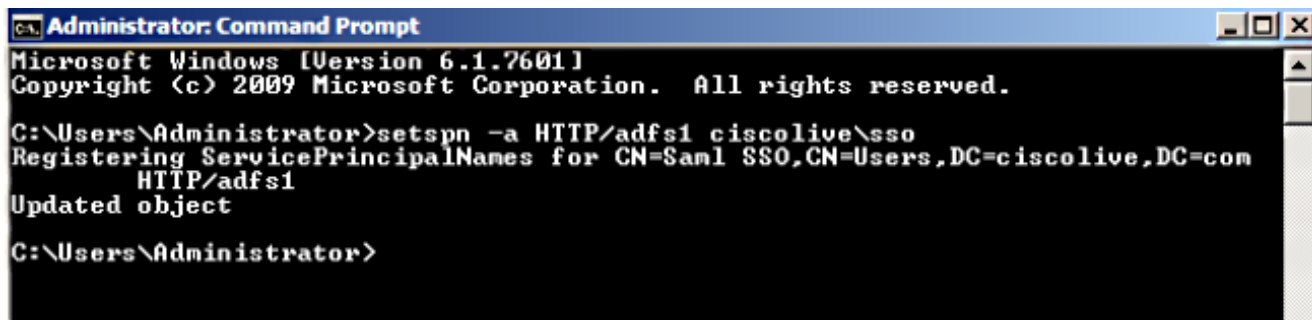
- Active Directory 2008 (Nombre de host: ADFS1.ciscolive.com)
- AD FS versión 2.0 (nombre de host: ADFS1.ciscolive.com)
- CUCM (Nombre de host: CUCM1.ciscolive.com)
- Microsoft Internet Explorer versión 10
- Mozilla Firefox versión 34
- Telerik Fiddler Versión 4

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 AD FS

1. Configure AD FS versión 2.0 con Service Principal Name (SPN) para habilitar el equipo cliente en el que Jabber está instalado para solicitar entradas, lo que a su vez permite que el equipo cliente se comuniquen con un servicio 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 [AD FS 2.0: Cómo Configurar el SPN \(servicePrincipalName\) para la Cuenta de Servicio](#) para obtener más información.

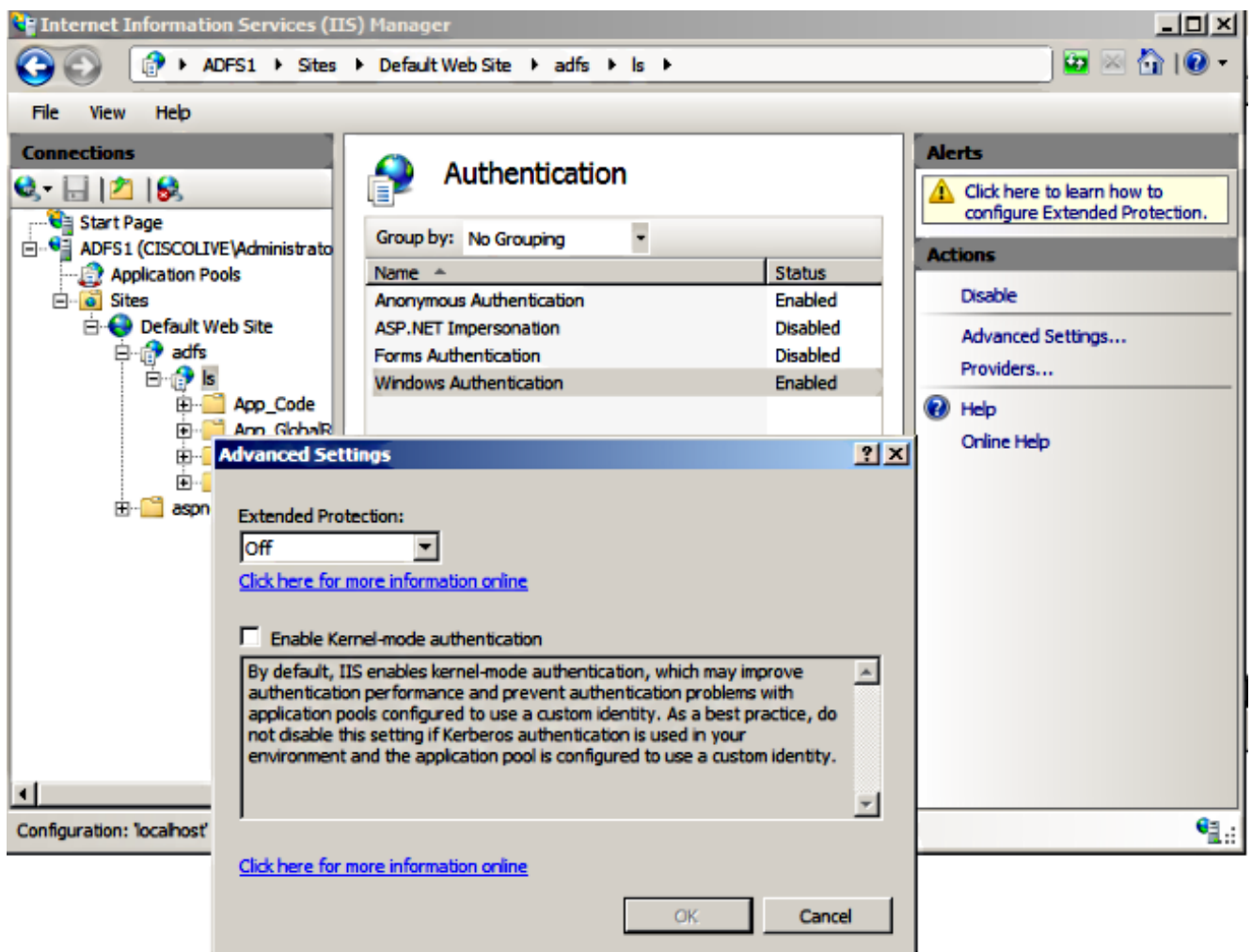
2. Asegúrese de que la configuración de autenticación predeterminada para el servicio AD FS (en C:\inetpub\adfs\ls\web.config) sea **Autenticación integrada de Windows**. Asegúrese de que no se haya cambiado a **Autenticación basada en formulario**.

```

<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>

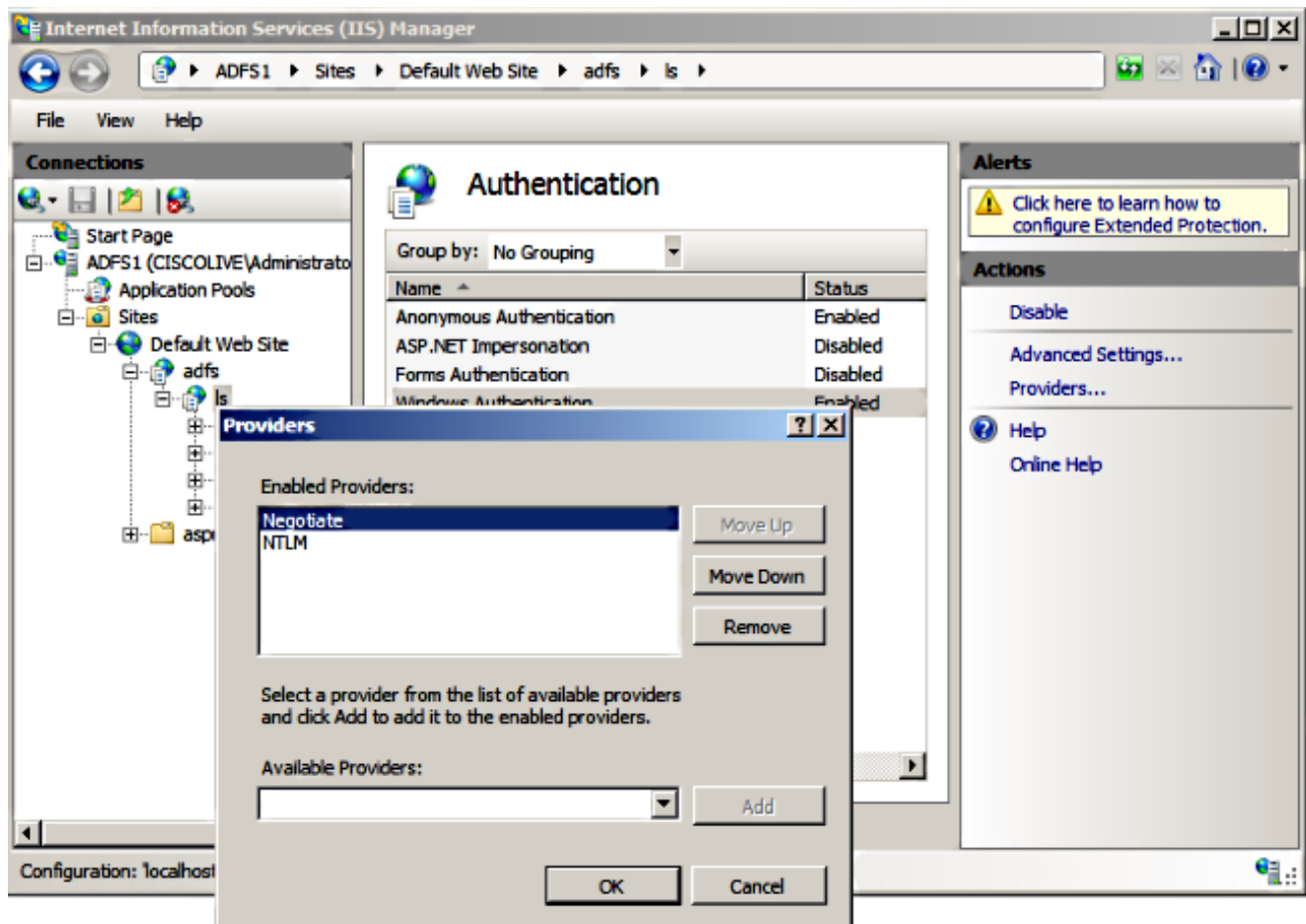
```

3. Seleccione **Autenticación de Windows** y haga clic en **Configuración avanzada** en el panel derecho. En Advanced Settings, desmarque **Enable Kernel-mode authentication**, asegúrese de que Extended Protection esté **Off** y haga clic en **OK**.



4. Asegúrese de que AD FS versión 2.0 admita tanto el protocolo Kerberos como el protocolo NT LAN Manager (NTLM) porque todos los clientes que no son de Windows no pueden utilizar Kerberos y confían en NTLM.

En el panel derecho, seleccione **Proveedores** y asegúrese de que **Negociar** y **NTLM** estén presentes en Proveedores habilitados:



Nota: AD FS pasa el encabezado Negotiate security cuando se utiliza la autenticación integrada de Windows para autenticar las solicitudes del cliente. El encabezado de seguridad Negotiate permite a los clientes seleccionar entre la autenticación Kerberos y la autenticación NTLM. El proceso Negotiate selecciona la autenticación Kerberos a menos que una de estas condiciones sea verdadera:

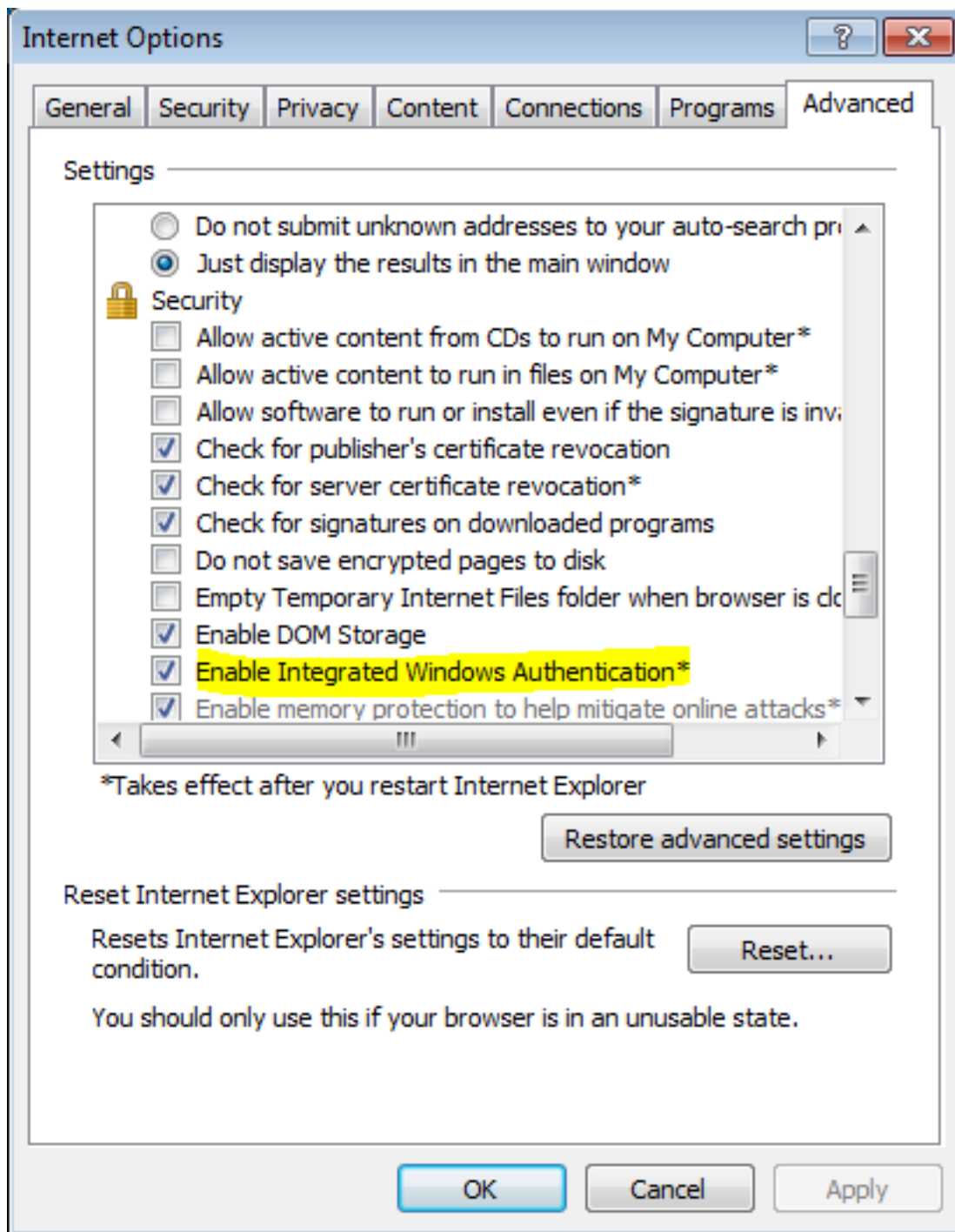
- Uno de los sistemas involucrados en la autenticación no puede utilizar la autenticación Kerberos.
- La aplicación que llama no proporciona información suficiente para utilizar la autenticación Kerberos.
- Para habilitar el proceso Negotiate para seleccionar el protocolo Kerberos para la autenticación de red, la aplicación cliente debe proporcionar un SPN, un nombre de usuario principal (UPN) o un nombre de cuenta de Network Basic Input/Output System (NetBIOS) como nombre de destino. De lo contrario, el proceso Negotiate siempre selecciona el protocolo NTLM como el método de autenticación preferido.

Configurar explorador

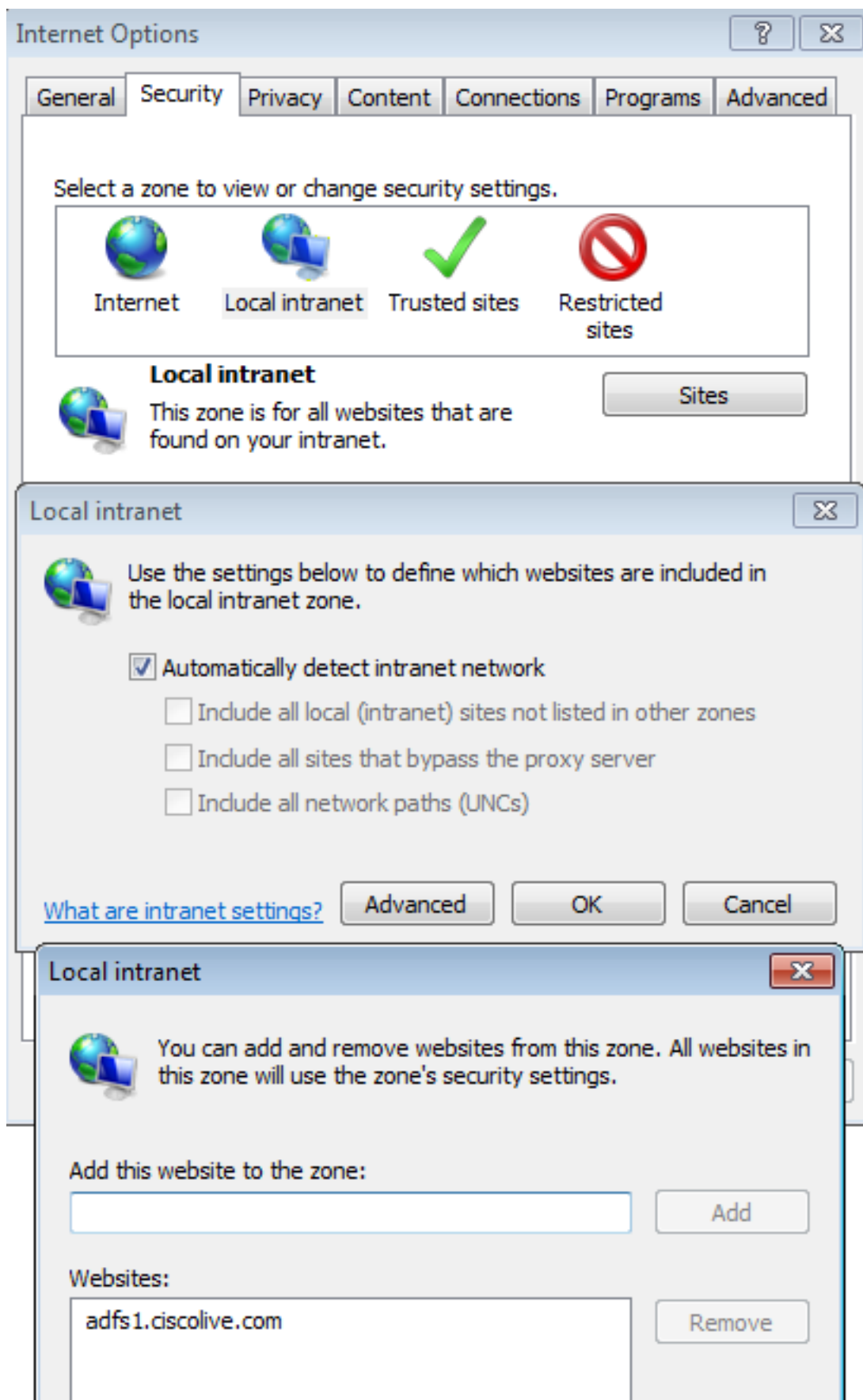
Microsoft Internet Explorer

1. Asegúrese de que **Internet Explorer > Advanced > Enable Integrated Windows**

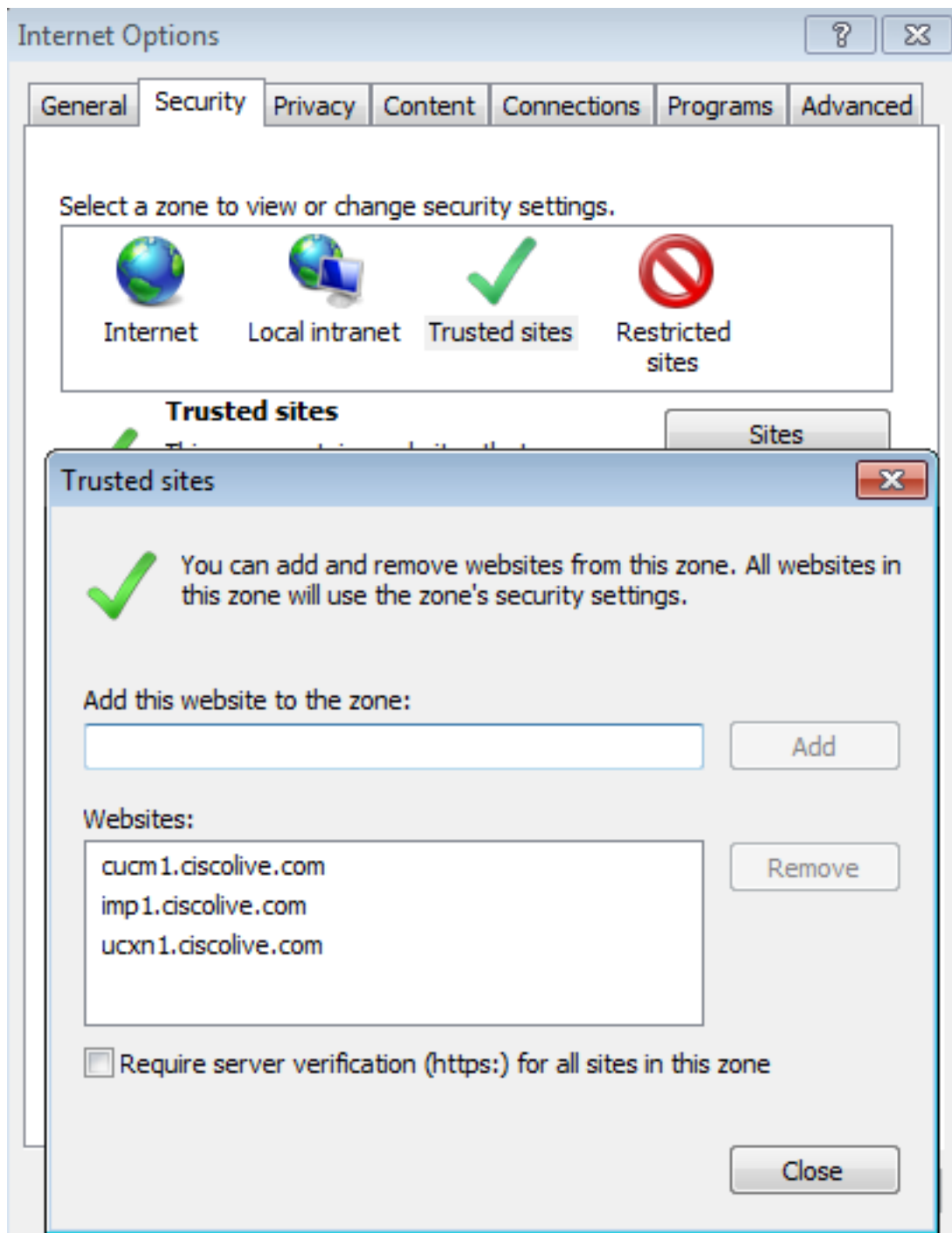
Authentication está marcado.



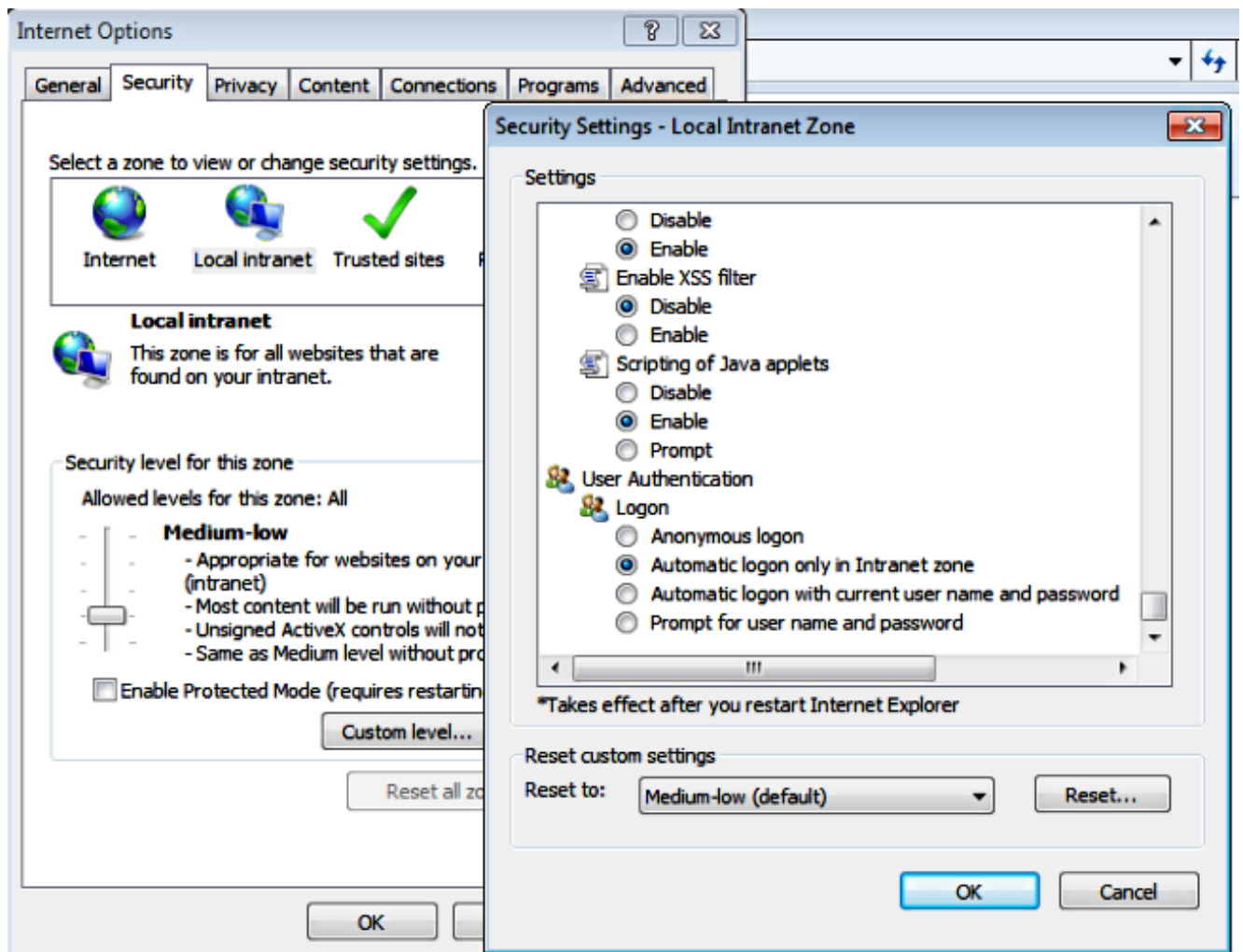
2. Agregue AD FS URL bajo **Security >Intranet zones > sites**.



3. Agregue los nombres de host CUCM, IMP y Unity a **Security >Trusted sites**.

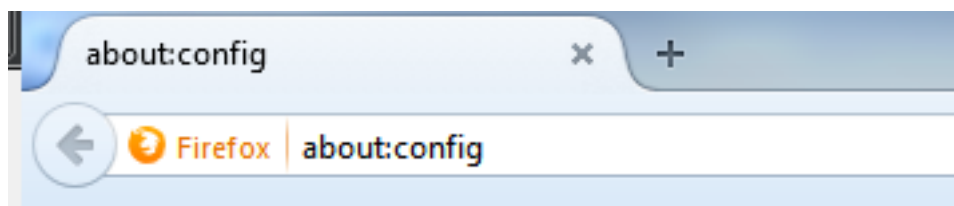


4. Asegúrese de que Internet Explorer > **security** > **Local Intranet** > **Security Settings** > **User Authentication - Logon** esté configurado para utilizar las credenciales de inicio de sesión para los sitios de intranet.



Mozilla FireFox

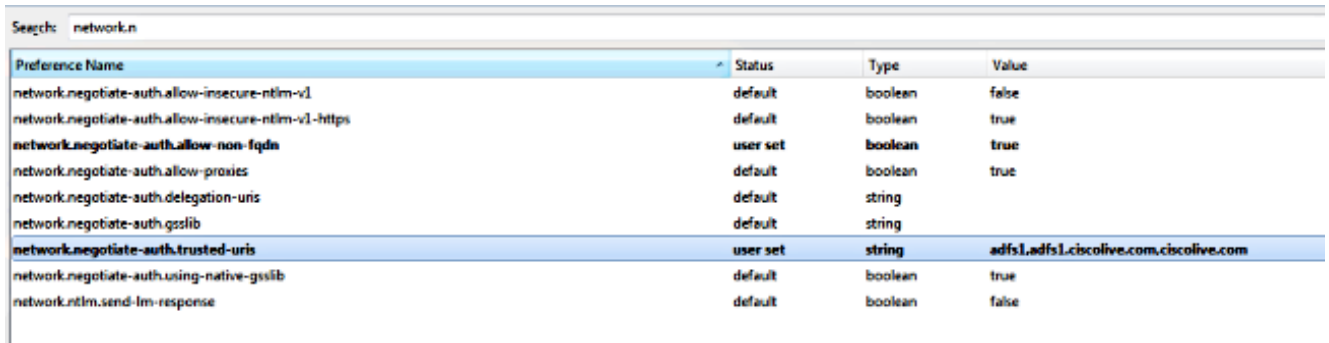
1. Abra Firefox e introduzca **about:config** en la barra de direcciones.



2. Haga clic y **tendré cuidado, ¡lo prometo!**



- Haga doble clic en el nombre de preferencia `network.negotiation-auth.allow-non-fqdn` para `true` y `network.negotiation-auth.trusted-uris` para `ciscolive.com,adfs1.ciscolive.com` para modificarlo.

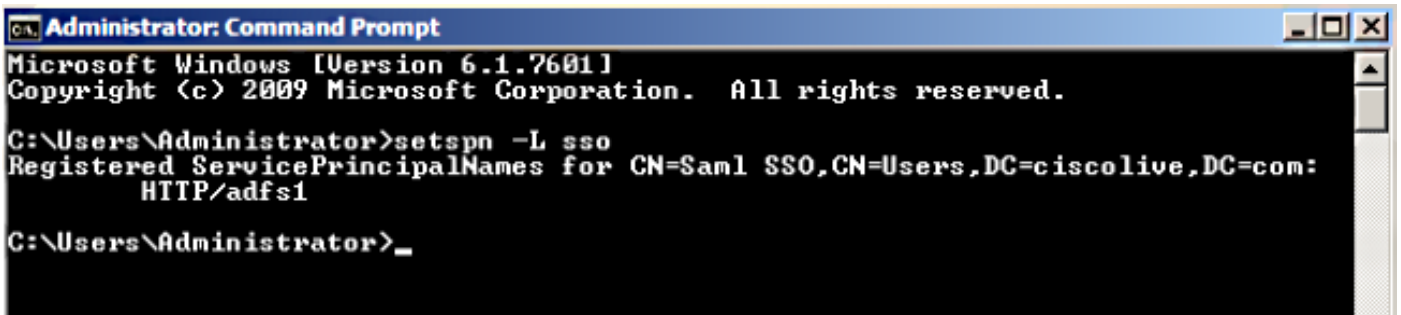


Preference Name	Status	Type	Value
network.negotiate-auth.allow-insecure-ntlm-v1	default	boolean	false
network.negotiate-auth.allow-insecure-ntlm-v1-https	default	boolean	true
network.negotiate-auth.allow-non-fqdn	user set	boolean	true
network.negotiate-auth.allow-proxies	default	boolean	true
network.negotiate-auth.delegation-uris	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

- Cierre Firefox y vuelva a abrirlo.

Verificación

Para verificar que los SPN para el servidor AD FS se han creado correctamente, ingrese el comando `setspn` y vea el resultado.

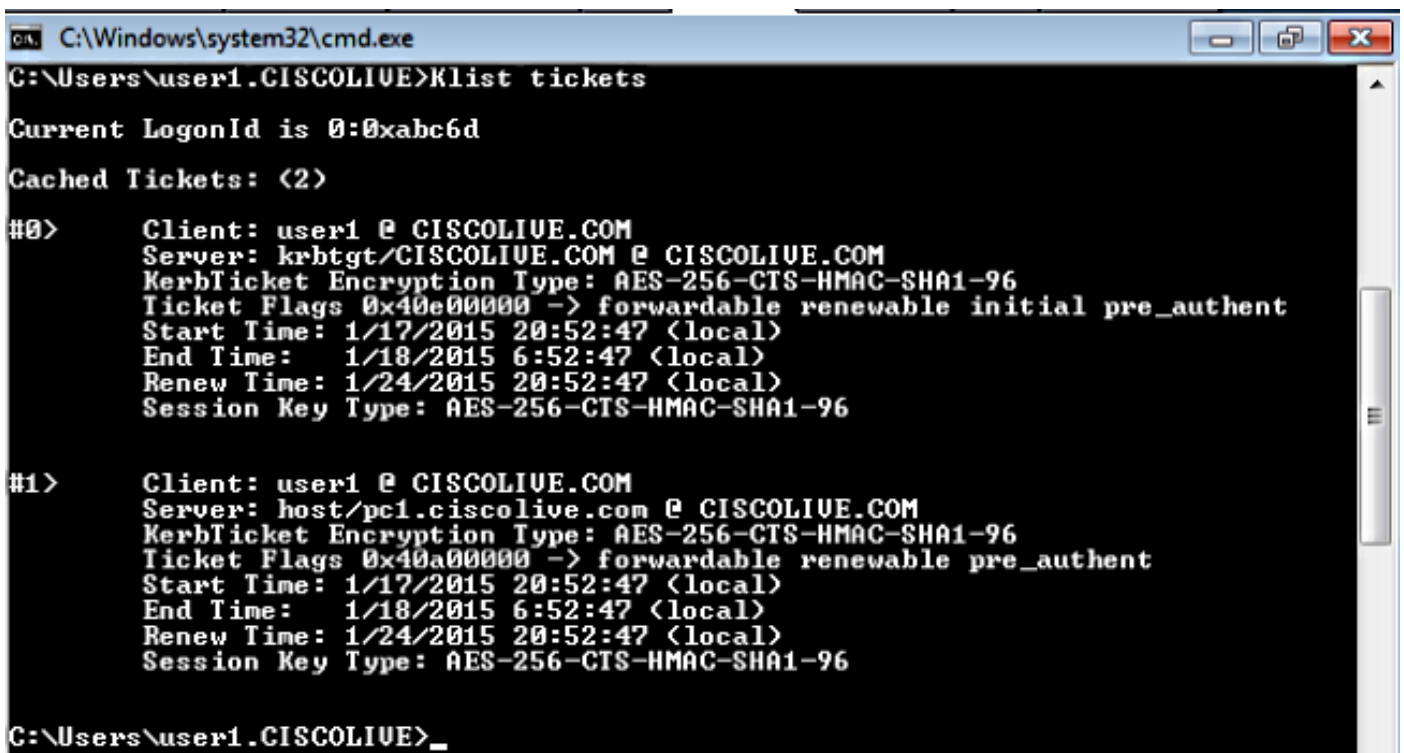


```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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

C:\Users\Administrator>_
```

Verifique si los equipos cliente tienen entradas Kerberos:



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

Current LogonId is 0:0xabc6d

Cached Tickets: (2)

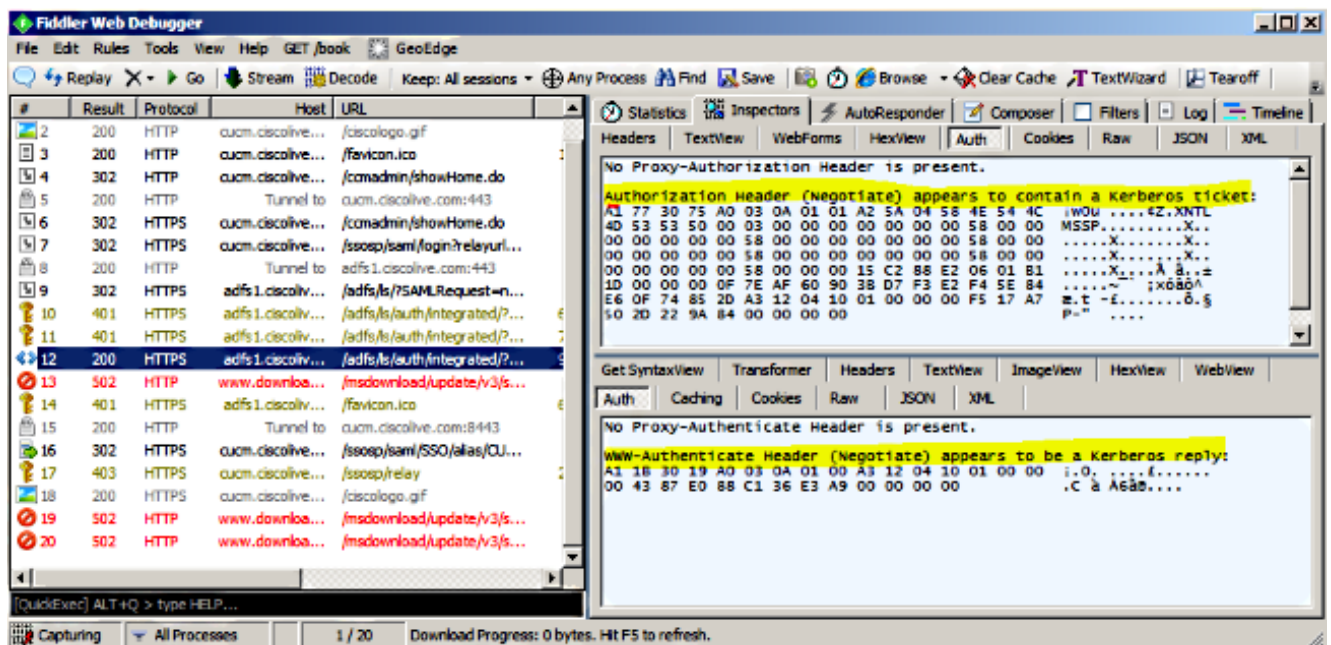
#0> Client: user1 @ CISCOLIVE.COM
Server: krbtgt/CISCOLIVE.COM @ CISCOLIVE.COM
Kerberos Ticket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
Start Time: 1/17/2015 20:52:47 (local)
End Time: 1/18/2015 6:52:47 (local)
Renew Time: 1/24/2015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

#1> Client: user1 @ CISCOLIVE.COM
Server: host/pc1.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>_
```

Complete estos pasos para verificar que autenticación (autenticación Kerberos o NTLM) está en uso.

1. Descargue la herramienta Fiddler en su equipo cliente e instálela.
2. Cierre todas las ventanas de Microsoft Internet Explorer.
3. Ejecute la herramienta Fiddler y verifique que la opción **Capturar tráfico** esté habilitada en el menú Archivo. Fiddler funciona como proxy de paso entre la máquina cliente y el servidor y escucha todo el tráfico.
4. Abra Microsoft Internet Explorer, busque su CUCM y haga clic en algunos enlaces para generar tráfico.
5. Vuelva a la ventana principal de Fiddler y elija una de las tramas donde el resultado es 200 (correcto) y puede ver Kerberos como mecanismo de autenticación



6. Si el tipo de autenticación es NTLM, verá **Negotiate - NTLMSSP** al principio de la trama, como se muestra aquí.

