Ejemplo de Configuración de Kerberos con ADFS 2.0 para el Usuario Final SAML SSO para Jabber

Contenido

Introducción

Este documento describe cómo configurar Kerberos con los Servicios de federación de Active Directory (ADFS) 2.0.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

Antecedentes

La configuración de Lenguaje de marcado de aserción de usuario final (SAML) de inicio de sesión único (SSO) requiere la configuración de Kerberos para permitir que el SSO de usuario final SAML para Jabber funcione con la autenticación de dominio. Cuando se implementa SAML SSO con Kerberos, el protocolo ligero de acceso a directorios (LDAP) controla toda la autorización y la sincronización de usuarios, mientras que Kerberos administra la autenticación. Kerberos es un protocolo de autenticación que se pretende utilizar junto con una instancia habilitada para LDAP.

En los equipos Microsoft Windows y Macintosh que se unen a un dominio de Active Directory, los usuarios pueden iniciar sesión de forma fluida en Cisco Jabber sin necesidad de introducir un nombre de usuario o una contraseña y ni siquiera ven una pantalla de inicio de sesión. Los usuarios que no han iniciado sesión en el dominio de sus equipos siguen viendo un formulario de inicio de sesión estándar.

Debido a que la autenticación utiliza un único token pasado desde los sistemas operativos, no se requiere redirección. El token se verifica con el controlador de dominio de clave (KDC) configurado y, si es válido, el usuario inicia sesión.

Configuración

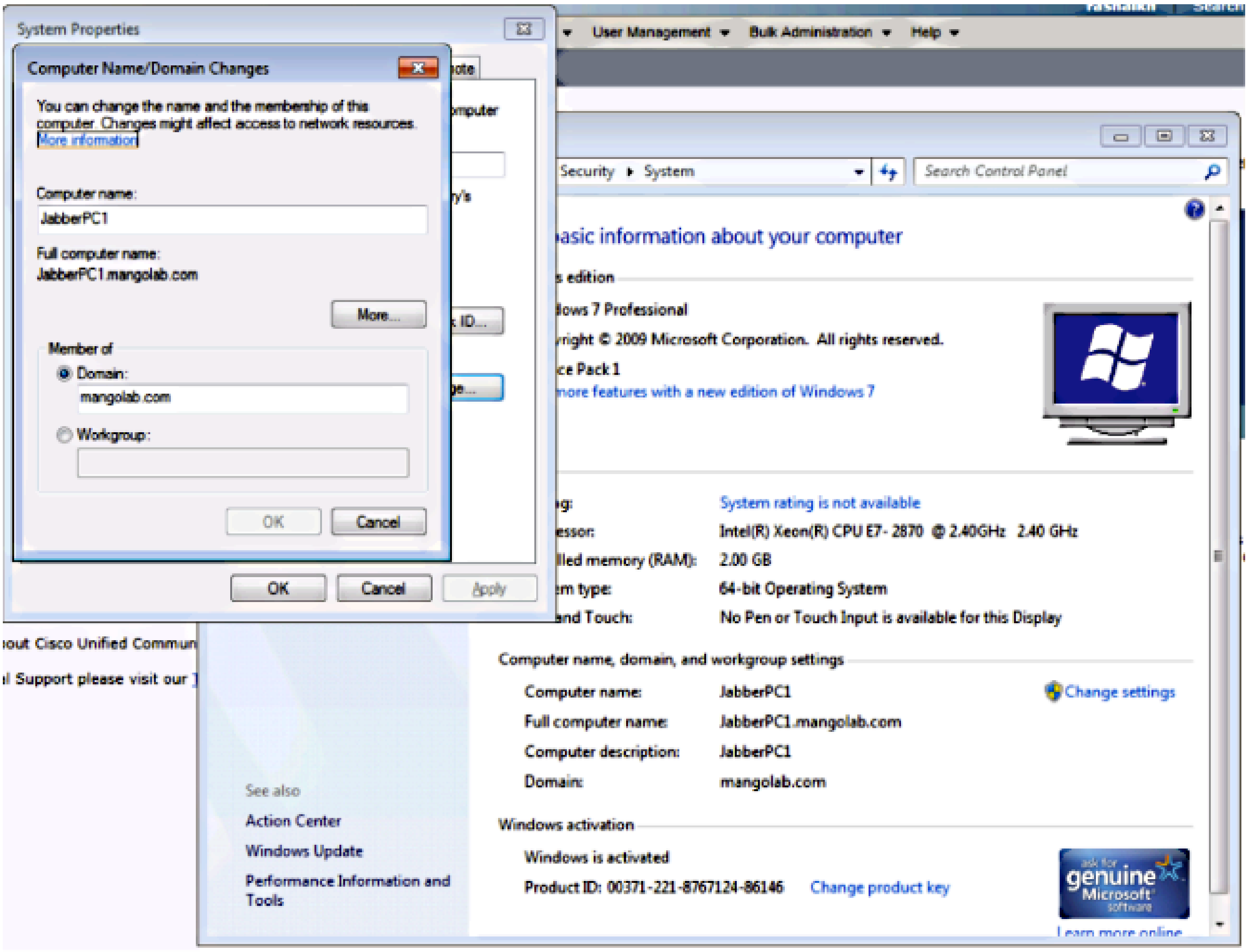
Este es el procedimiento para configurar Kerberos con ADFS 2.0.

1. Instale Microsoft Windows Server 2008 R2 en un equipo.
2. Instale Active Directory Domain Services (ADDS) y ADFS en el mismo equipo.
3. Instale Internet Information Services (IIS) en el equipo instalado en Microsoft Windows Server 2008 R2.
4. Cree un certificado autofirmado para IIS.
5. Importe el certificado autofirmado en IIS y utilícelo como certificado de servidor HTTPS.
6. Instale Microsoft Windows7 en otro equipo y utilícelo como cliente.

   Cambie el servidor de nombres de dominio (DNS) a la máquina en la que instaló ADDS.

   Agregue esta máquina al dominio que creó en la instalación de ADDS.

   Vaya a **Inicio**.Haga clic con el botón derecho del ratón en **Equipo**.Haga clic en Properties (Propiedades).Haga clic en **Cambiar configuración** en el lado derecho de la ventana.Haga clic en la **ficha Nombre del equipo**.Haga clic en **Cambiar**.Agregue el dominio que creó.



7. Compruebe si el servicio Kerberos se genera en ambos equipos.

   Inicie sesión como administrador en el equipo servidor y abra el símbolo del sistema. A continuación, ejecute estos comandos:

   cd \windows\System32Entradas de Klist

```
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
        KerbTicket Encryption Type: AES-256-CTS-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-CTS-HMAC-SHA1-96
```

   Inicie sesión como usuario de dominio en el equipo cliente y ejecute los mismos comandos.

```
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
        KerbTicket 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
        KerbTicket 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
        KerbTicket 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
        KerbTicket 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
        KerbTicket 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. Cree la identidad ADFS Kerberos en el equipo donde instaló ADDS.

   El administrador de Microsoft Windows inició sesión en el dominio de Microsoft Windows (como <domainname>\administrator), por ejemplo en el controlador de dominio de Microsoft Windows, crea la identidad ADFS Kerberos. El servicio ADFS HTTP debe tener una identidad Kerberos denominada nombre principal de servicio (SPN) con este formato: **HTTP/DNS_name_of_ADFS_server**.

   Este nombre debe asignarse al usuario de Active Directory que representa la instancia del servidor HTTP de ADFS. Utilice la utilidad **setspan** de Microsoft Windows, que debe estar disponible de forma predeterminada en un servidor de Microsoft Windows 2008.

Procedimiento Registre los SPN para el servidor ADFS. En el controlador de dominio de Active Directory, ejecute el comando **setspan**.

Por ejemplo, cuando el host ADFS es **adfs01.us.renovations.com** y el dominio de Active Directory es **US.RENOVATIONS.COM**, el comando es:

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

Se aplica la parte **HTTP/** del SPN, aunque el servidor ADFS suele tener acceso a través de Secure Sockets Layer (SSL), que es HTTPS.

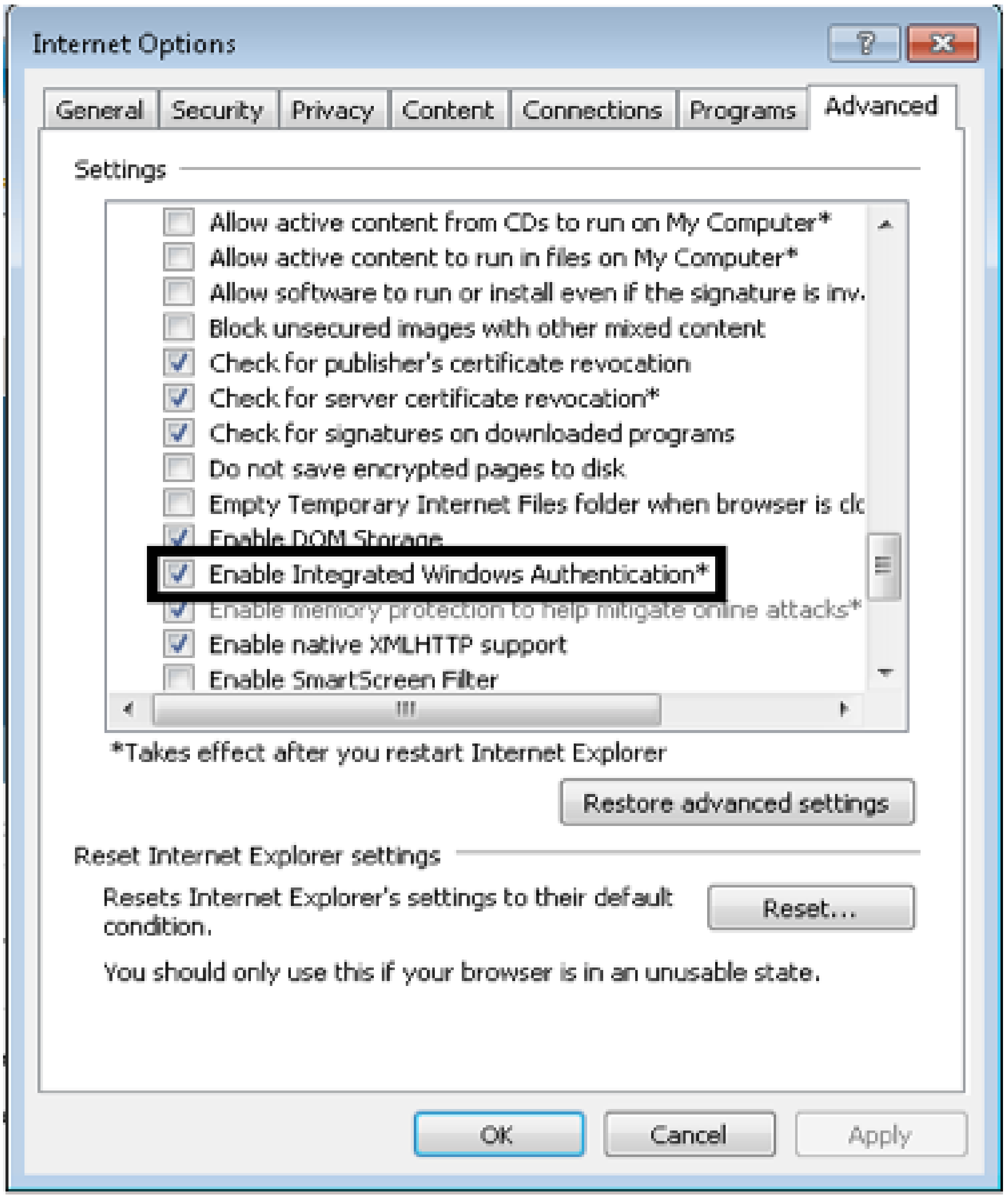
Verifique que los SPNs para el servidor ADFS se crean correctamente con el comando **setspan** y vea el resultado.

```
setspn -L
```

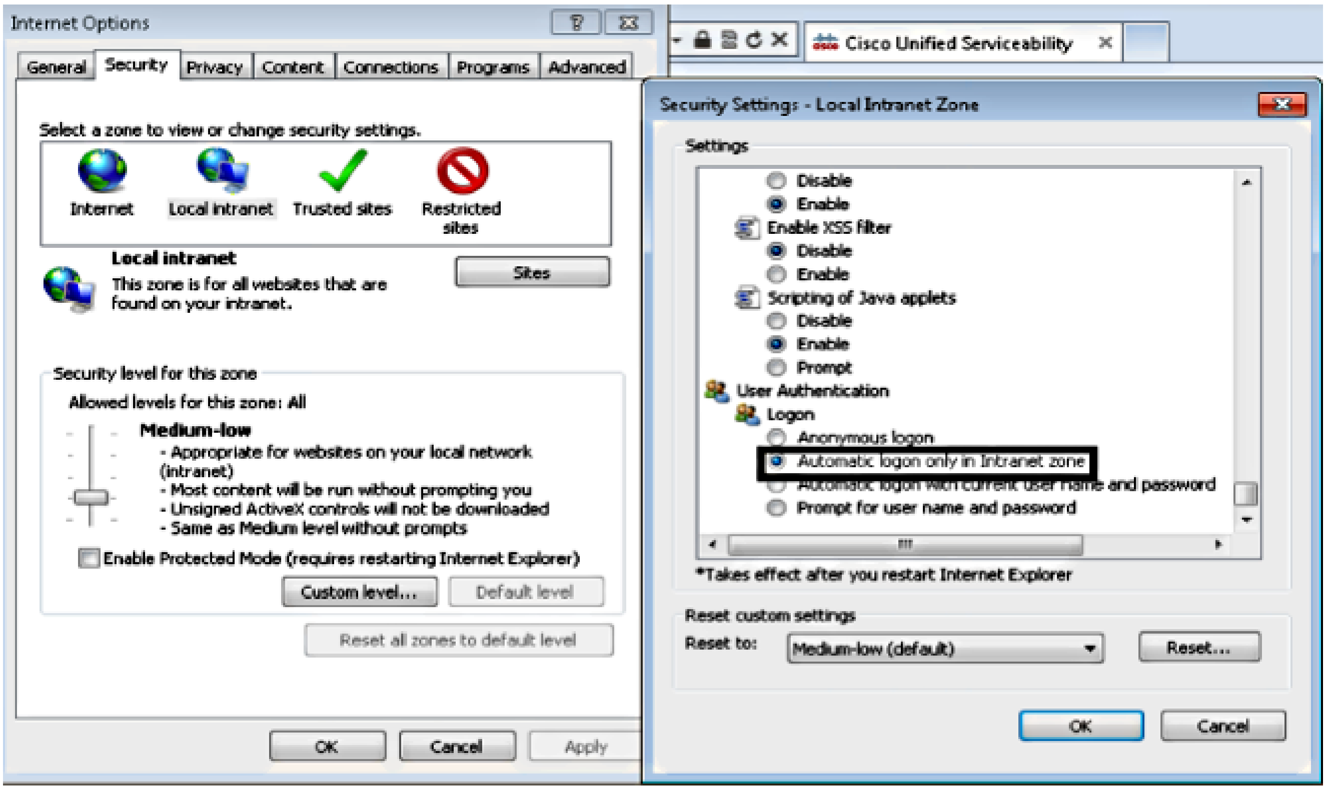
9. Configure los parámetros del explorador del cliente de Microsoft Windows.

   Navegue hasta **Herramientas > Opciones de Internet > Avanzadas** para habilitar la autenticación integrada de Windows.

   Marque la **casilla de verificación Habilitar autenticación integrada de Windows**:

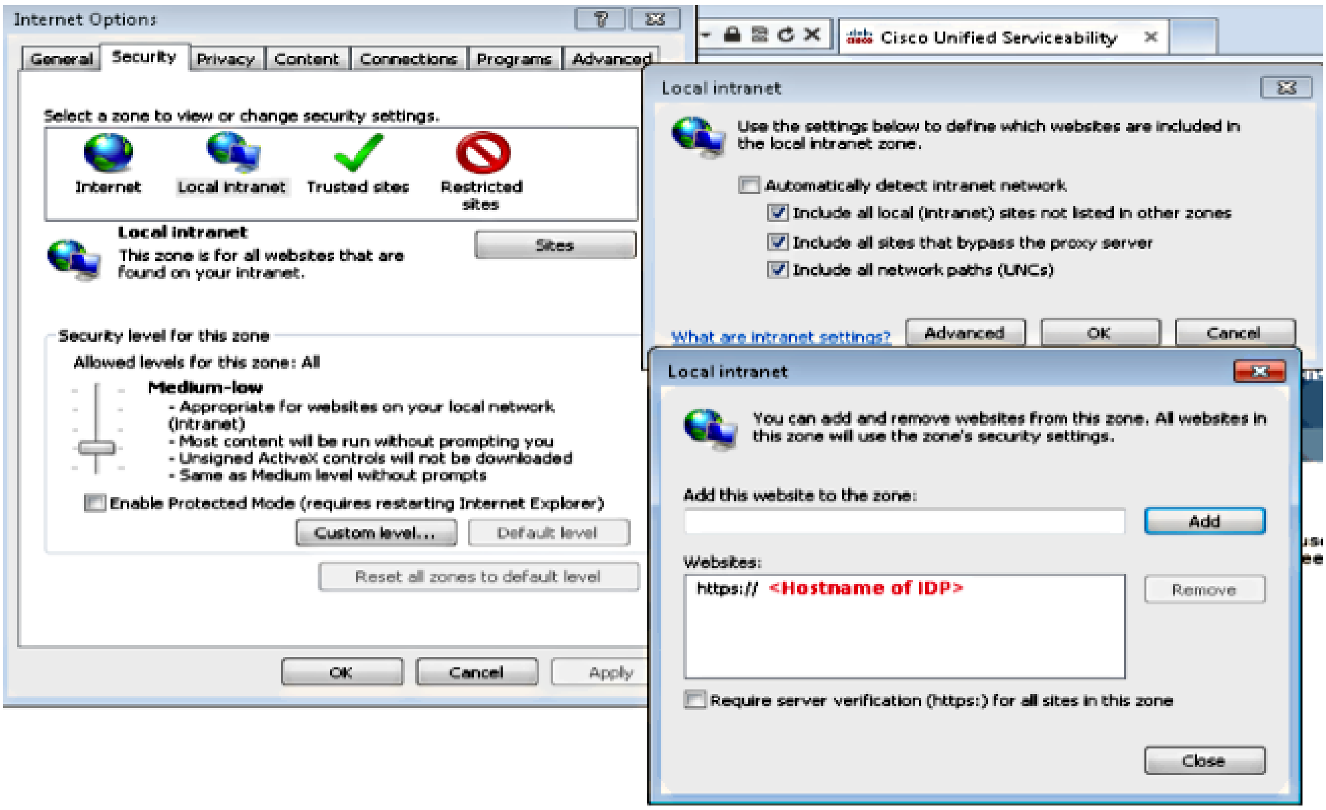


   Vaya a **Herramientas > Opciones de Internet > Seguridad > Intranet local > Nivel personalizado...** para seleccionar **Inicio de sesión automático solamente en la zona Intranet.**

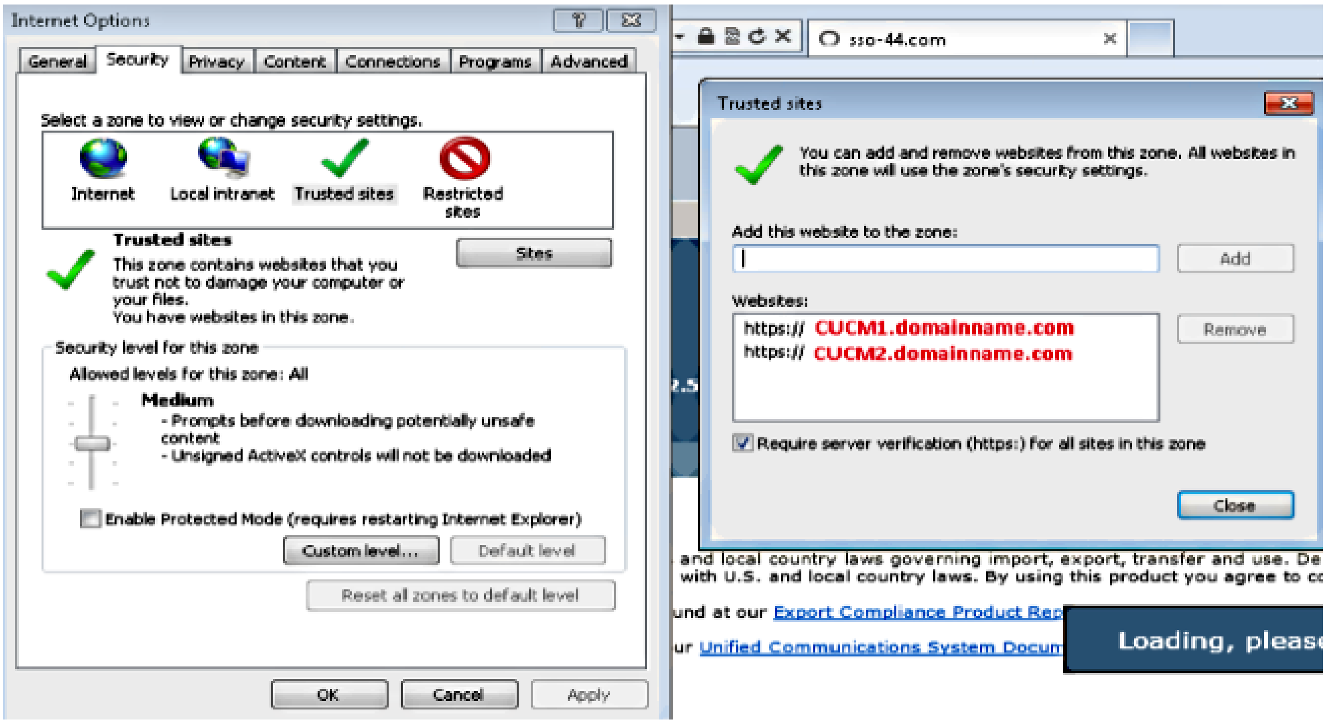


Navegue hasta **Herramientas > Opciones de Internet > Seguridad > Intranet local > Sitios > Avanzado** para agregar la URL de Detección y Prevención de Intrusiones (IDP) a sitios de Intranet local.

Nota: Marque todas las casillas de verificación del cuadro de diálogo Intranet local y haga clic en la **ficha Avanzadas**.



Navegue hasta **Herramientas > Seguridad > Sitios de confianza > Sitios** para agregar los nombres de host de CUCM a sitios de confianza:



Verificación

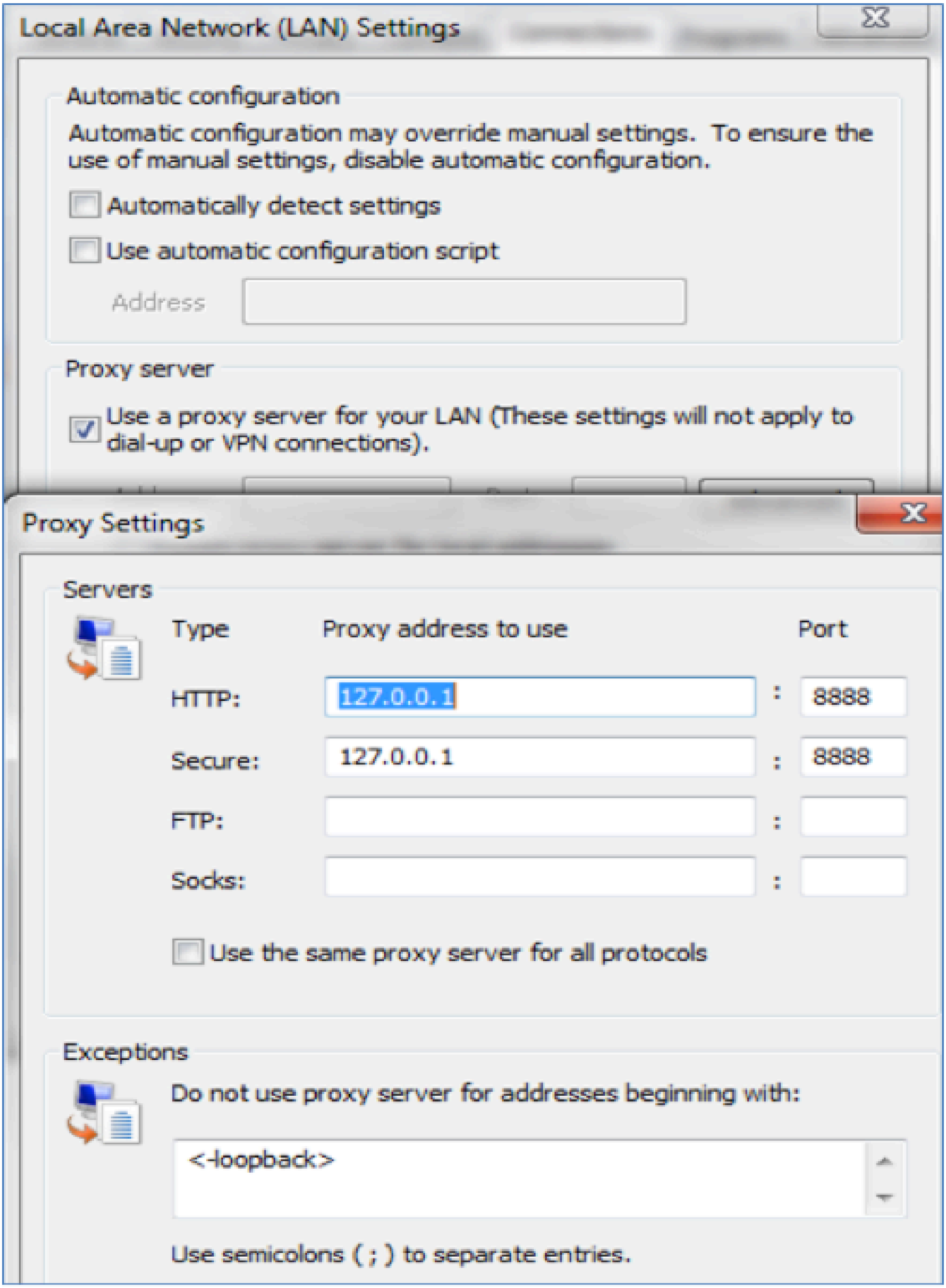
Esta sección explica cómo verificar qué autenticación (Kerberos o NT LAN Manager (NTLM)) se utiliza.

1. Descargue la [herramienta Fiddler] en su equipo cliente e instálela.

2. Cierre todas las ventanas de Internet Explorer.

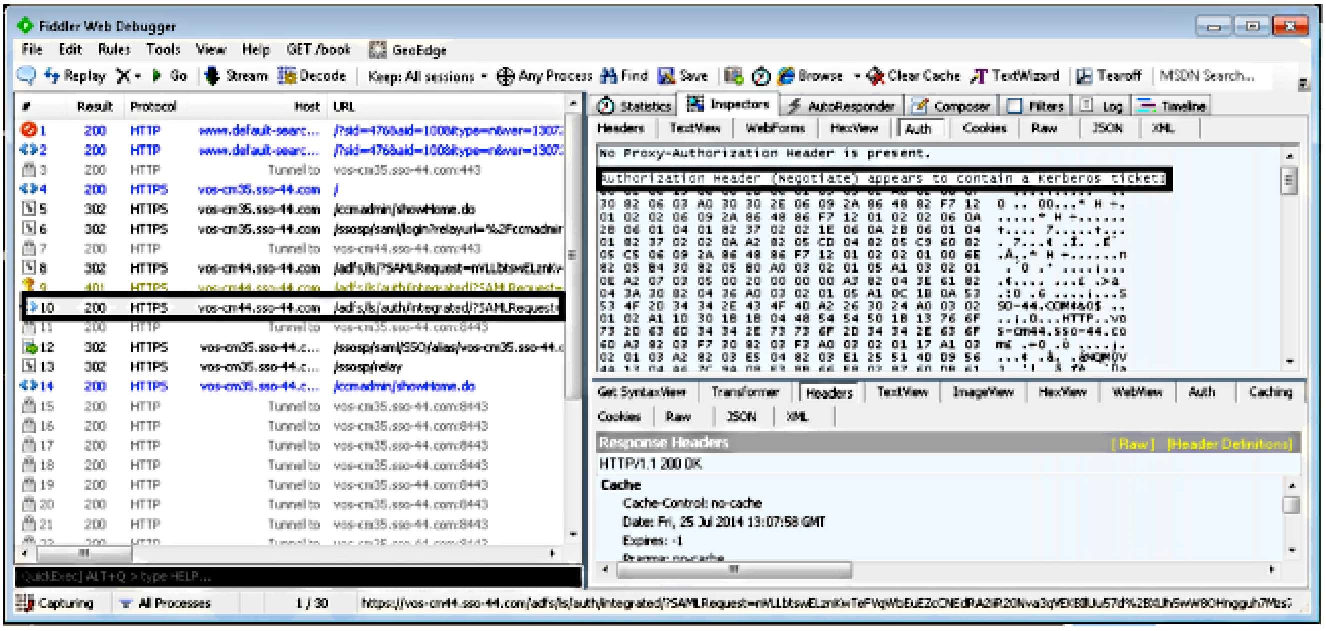
3. Ejecute la herramienta Fiddler y verifique que la opción **Capturar tráfico** esté habilitada en el menú Archivo.

   Fiddler funciona como proxy de paso entre el equipo cliente y el servidor y escucha todo el tráfico, lo que establece temporalmente los parámetros de Internet Explorer de la siguiente manera:

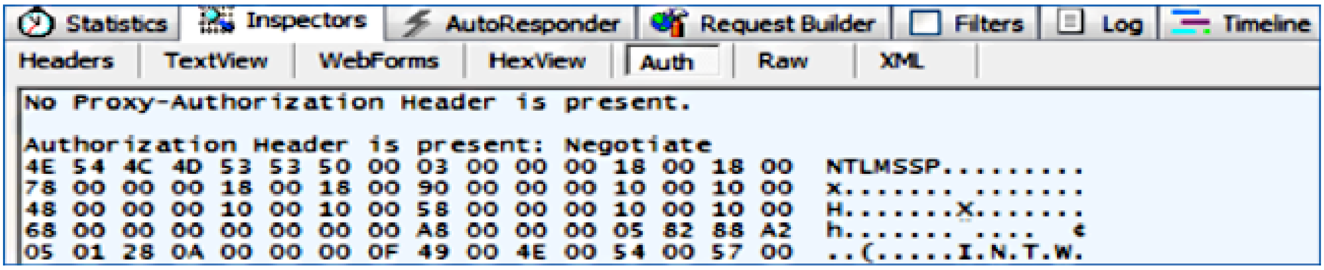


4. Abra Internet Explorer, busque la URL del servidor de gestión de relaciones con el cliente (CRM) y haga clic en algunos enlaces para generar tráfico.

5. Vuelva a la ventana principal de Fiddler y elija una de las tramas donde el resultado es 200 (correcto):



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



Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.