Exemplo de Kerberos com ADFS 2.0 para SAML SSO de usuário final para configuração Jabber

Contents

Introduction

Este documento descreve como configurar o Kerberos com o Ative Diretory Federation Services (ADFS) 2.0.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Informações de Apoio

A configuração do SSO (Single Sign On, login único) SAML (End User Security Assertion Markup Language) exige que o Kerberos seja configurado para permitir que o SSO SAML do usuário final para o Jabber trabalhe com autenticação de domínio. Quando SAML SSO é implementado com

Kerberos, o Lightweight Diretory Access Protocol (LDAP) manipula toda a autorização e a sincronização do usuário, enquanto Kerberos gerencia a autenticação. Kerberos é um protocolo de autenticação que deve ser usado em conjunto com uma instância habilitada para LDAP.

Em máquinas Microsoft Windows e Macintosh que estão associadas a um domínio do Ative Diretory, os usuários podem fazer login no Cisco Jabber sem precisar inserir um nome de usuário ou senha e nem mesmo ver uma tela de login. Os usuários que não estão conectados ao domínio em seus computadores ainda veem um formulário de login padrão.

Como a autenticação usa um único token passado dos sistemas operacionais, não é necessário redirecionamento. O token é verificado em relação ao KDC (Key Domain Controller) configurado e, se for válido, o usuário está conectado.

Configuração

Este é o procedimento para configurar Kerberos com ADFS 2.0.

1. Instale o Microsoft Windows Server 2008 R2 em uma máquina.

2. Instale os Serviços de Domínio do Ative Diretory (ADDS) e o ADFS na mesma máquina.

3. Instale o Internet Information Services (IIS) na máquina instalada do Microsoft Windows Server 2008 R2.

4. Crie um certificado autoassinado para o IIS.

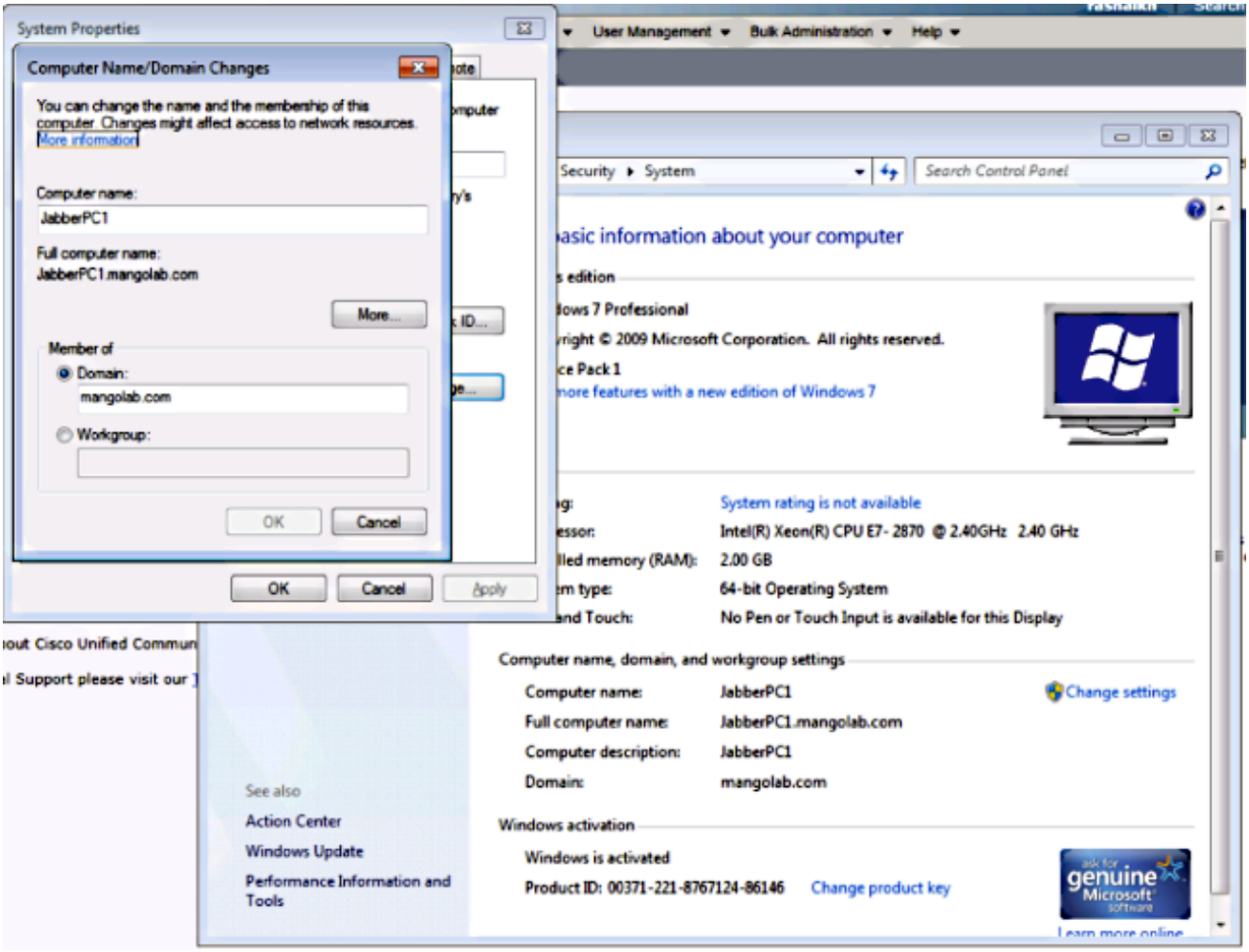
5. Importar o certificado autoassinado para o IIS e usá-lo como certificado do servidor HTTPS.

6. Instale o Microsoft Windows7 em outra máquina e use-o como um cliente.

   Altere o Domain Name Server (DNS) para a máquina onde você instalou o ADDS.

   Adicione esta máquina ao domínio criado na instalação do ADDS.

   Vá para **Start (Iniciar)**.Clique com o botão direito do mouse em **Computador**.Clique em Propriedades.Clique em **Alterar configurações** no lado direito da janela.Clique na **guia Nome do computador**.Clique em **Alterar**.Adicione o domínio criado.



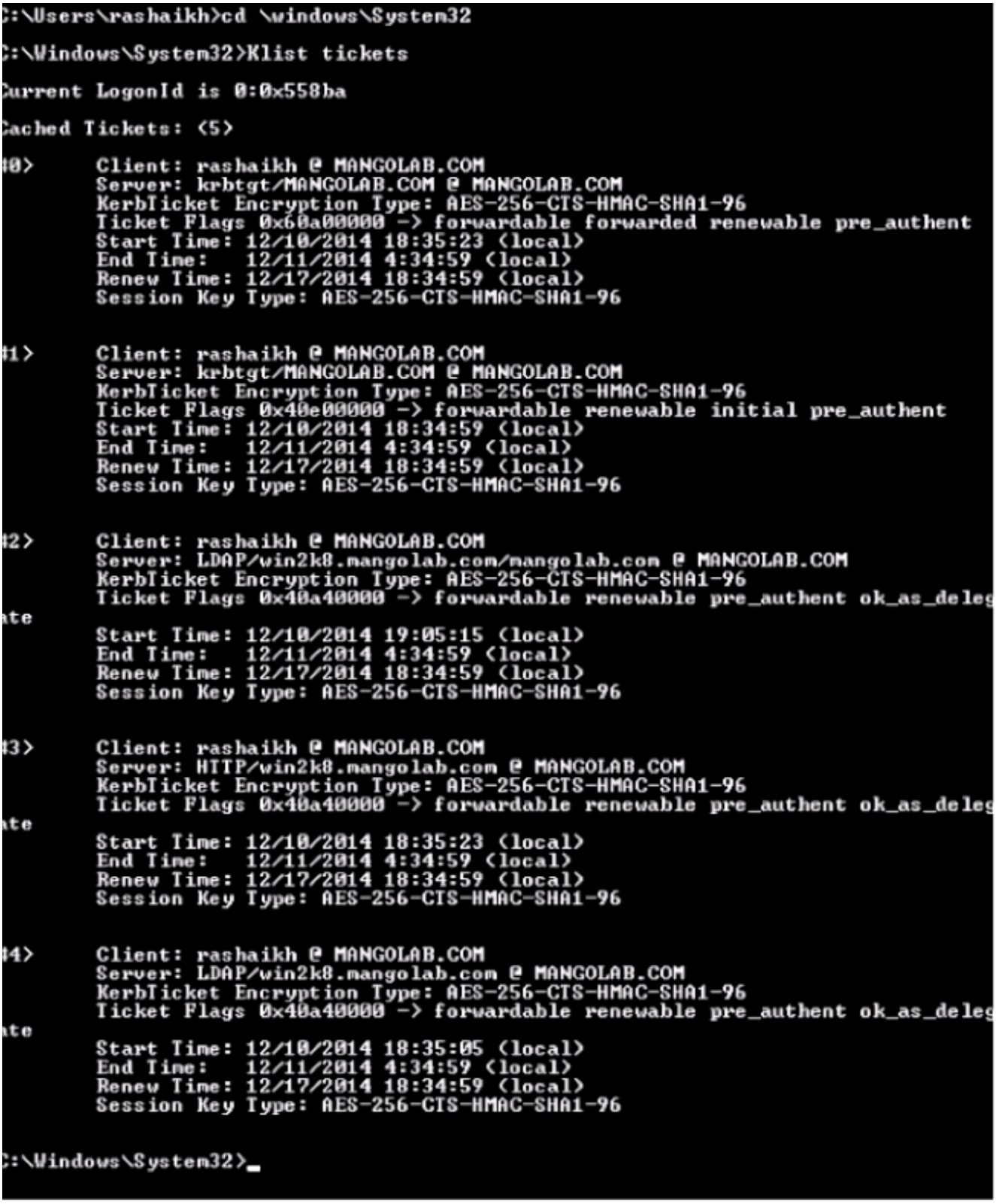
7. Verifique se o serviço Kerberos é gerado em ambas as máquinas.

   Faça login como administrador na máquina do servidor e abra o prompt de comando. Em seguida, execute estes comandos:

   cd \windows\System32Bilhetes 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
```

   Faça login como usuário de domínio na máquina cliente e execute os mesmos comandos.



8. Crie a identidade do Kerberos do ADFS na máquina onde você instalou o ADDS.

   O administrador do Microsoft Windows fez login no domínio do Microsoft Windows (como <nome do domínio>\administrador), por exemplo no controlador de domínio do Microsoft Windows, cria a identidade do Kerberos do ADFS. O serviço HTTP do ADFS deve ter uma identidade Kerberos chamada Nome do Principal do Serviço (SPN - Service Principal Name) neste formato: **HTTP/DNS_name_of_ADFS_server**.

   Esse nome deve ser mapeado para o usuário do Ative Diretory que representa a instância

do servidor HTTP do ADFS. Use o utilitário **setspn** do Microsoft Windows, que deve estar disponível por padrão em um Microsoft Windows 2008 Server.

Procedimento Registre os SPNs para o servidor ADFS. No controlador de domínio do Ative Diretory, execute o comando **setspn**.

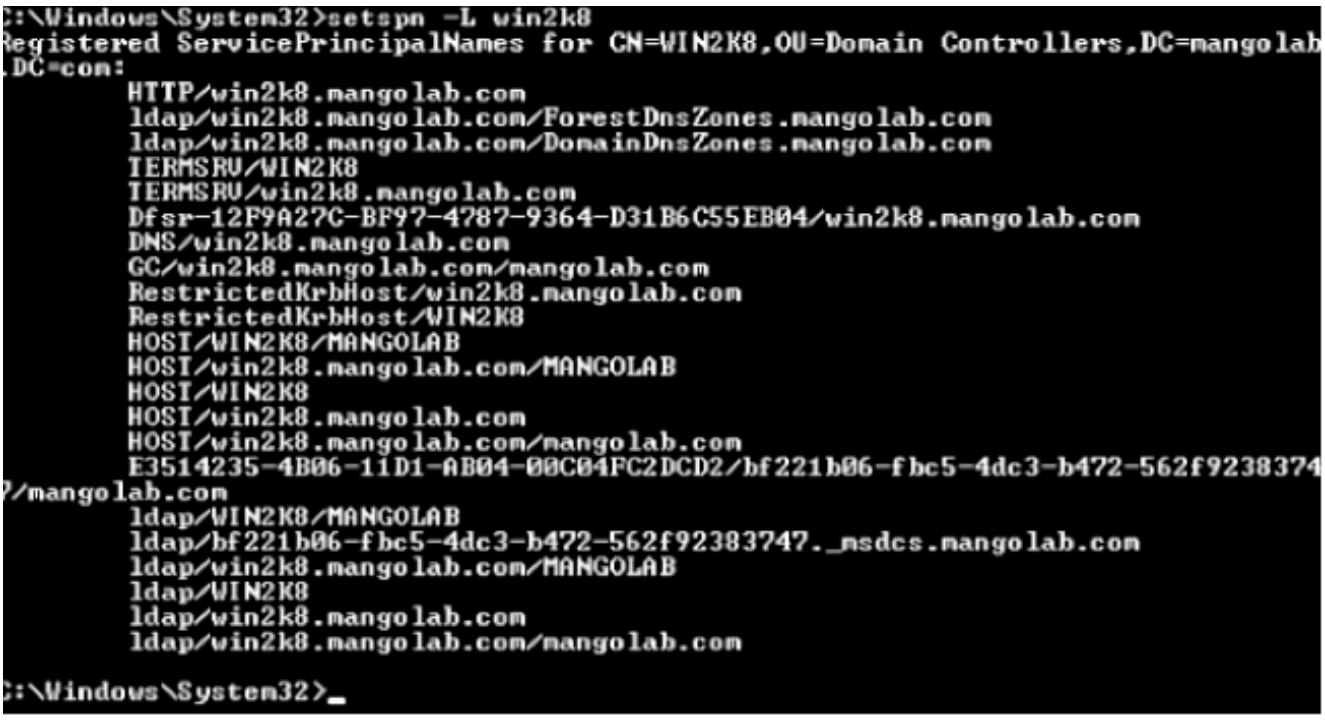
Por exemplo, quando o host ADFS é **adfs01.us.renovations.com**, e o domínio do Ative Diretory é **US.RENOVATIONS.COM**, o comando é:

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

A parte **HTTP/**SPN se aplica, mesmo que o servidor ADFS seja normalmente acessado pela SSL (Secure Sockets Layer), que é HTTPS.

Verifique se os SPNs do servidor ADFS foram criados corretamente com o comando **setspn** e veja a saída.

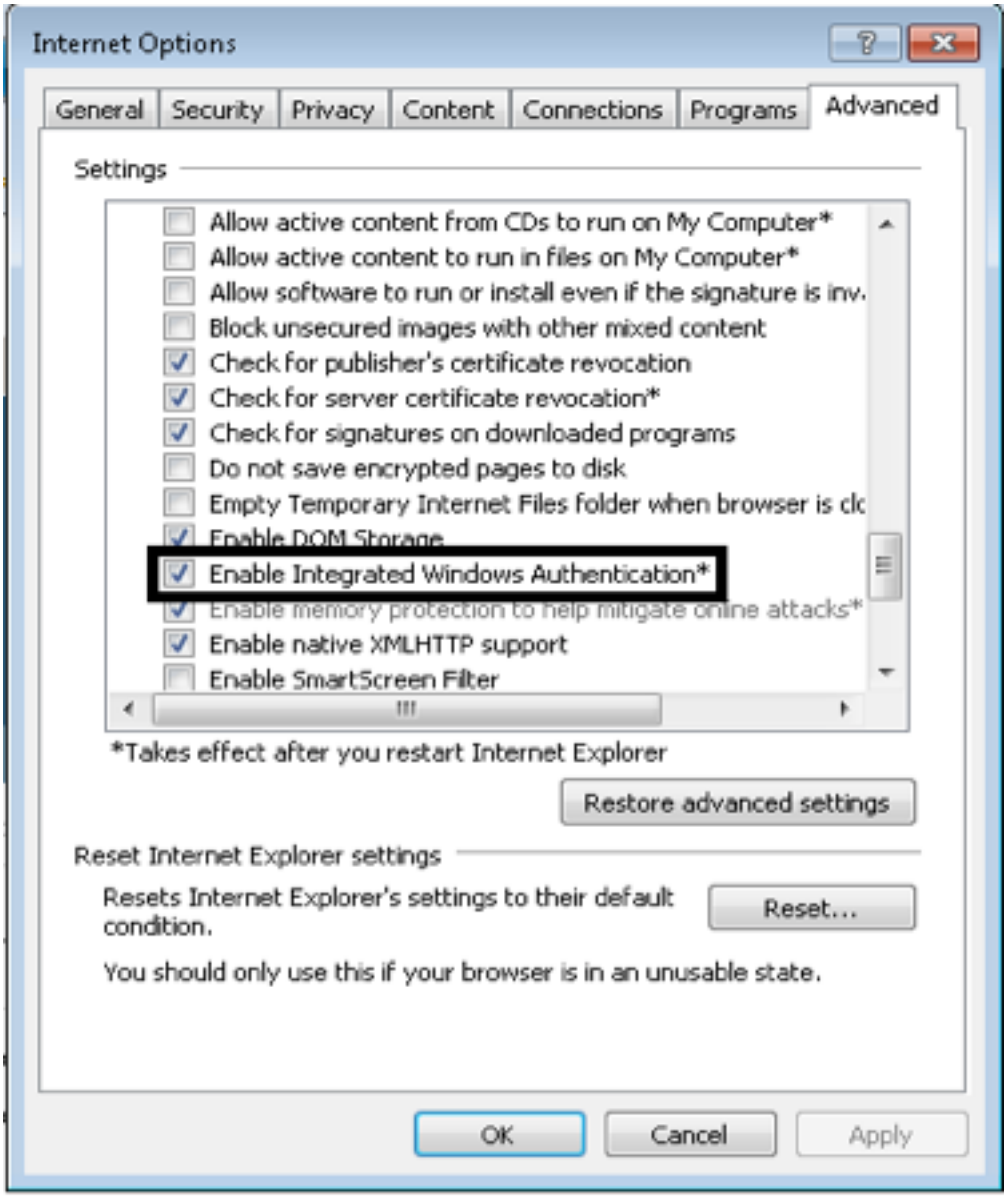
```
setspn -L
```



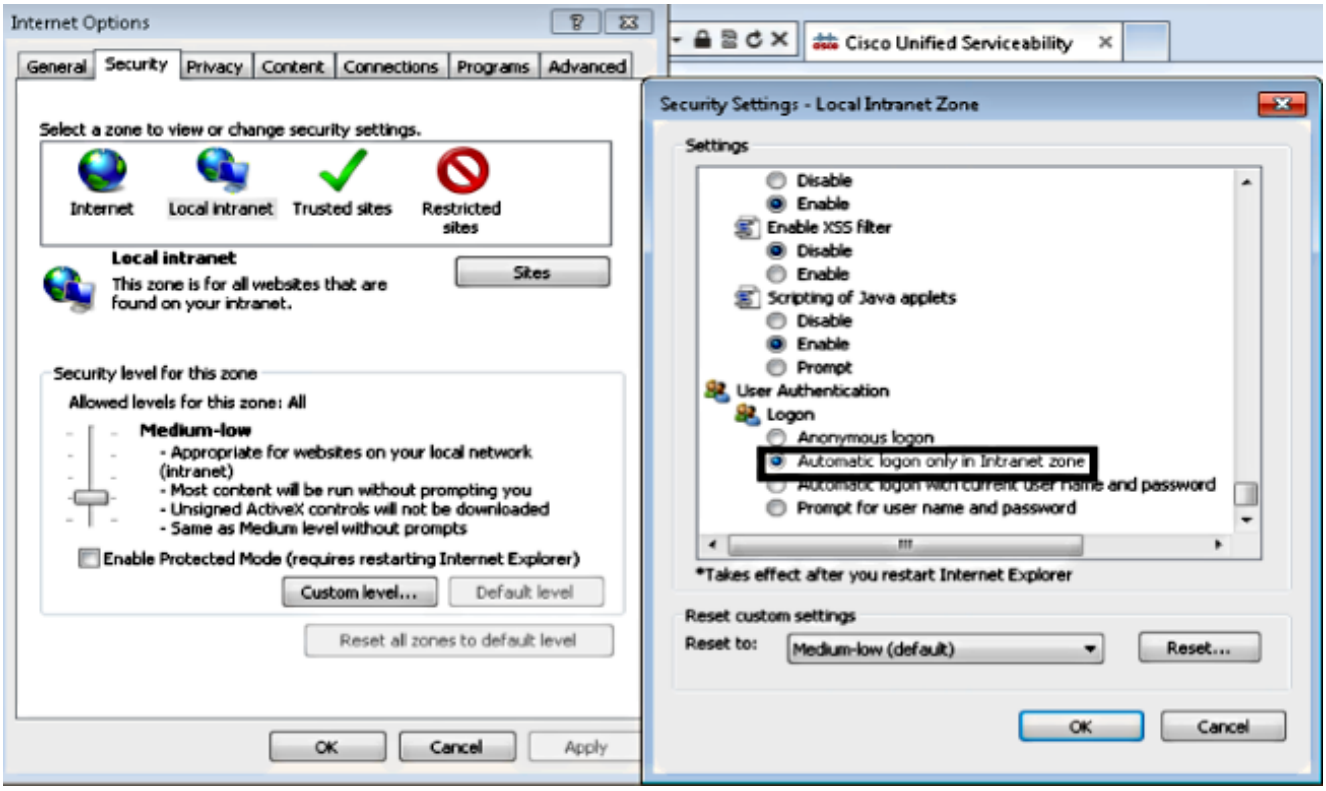
9. Defina as configurações do navegador do Microsoft Windows Client.

   Navegue até **Ferramentas > Opções da Internet > Avançado** para habilitar a Autenticação Integrada do Windows.

   Marque a **caixa de seleção Ativar autenticação integrada do Windows**:

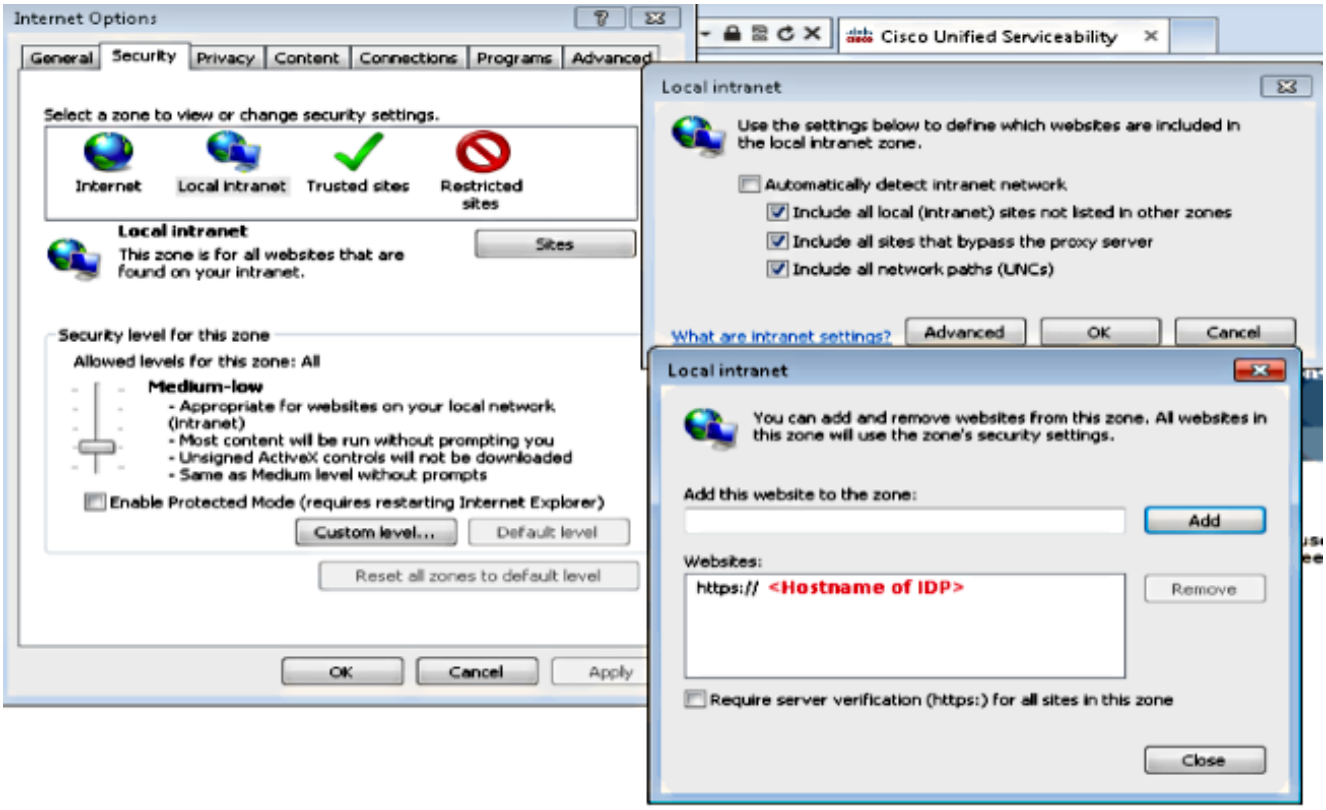


   Navegue até **Ferramentas > Opções da Internet > Segurança > Intranet local > Nível personalizado...** para selecionar **Logon automático somente na zona Intranet**.



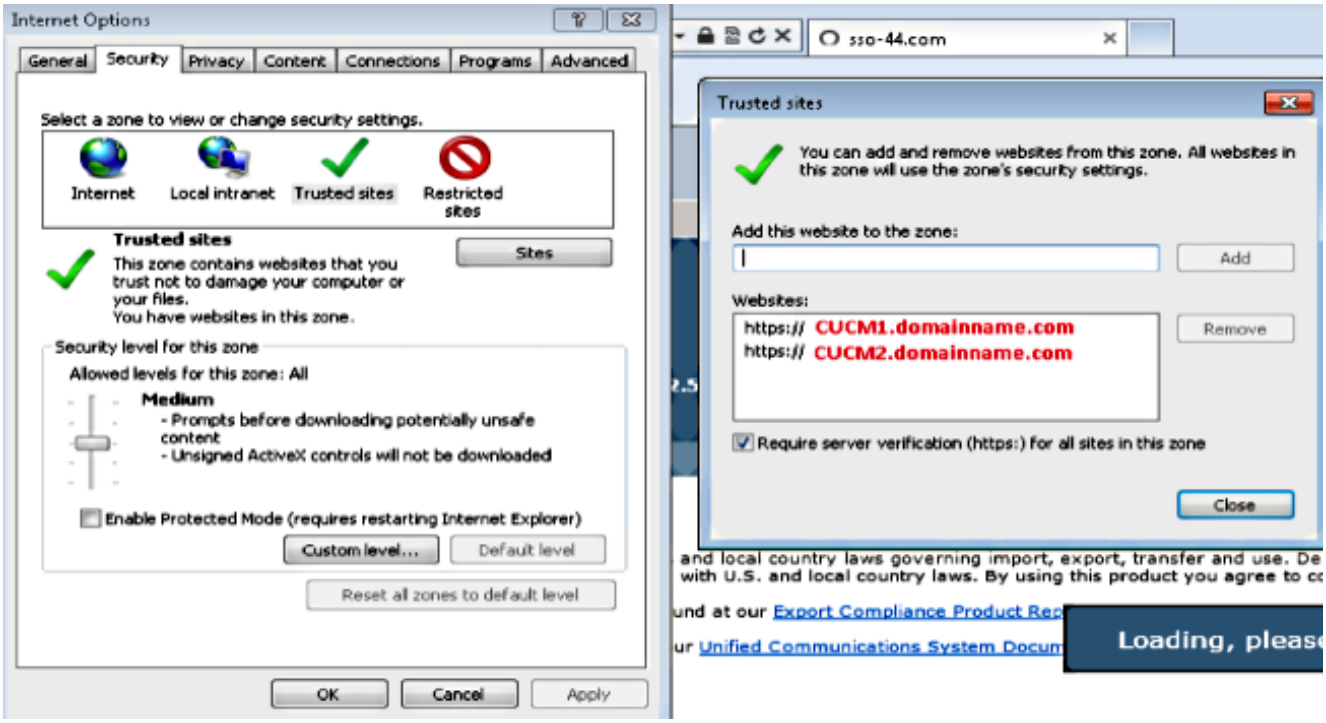
Navegue até **Ferramentas > Opções da Internet > Segurança > Intranet Local > Sites > Avançado** para adicionar o URL da IDP (Intrusion Detection & Prevention, Detecção e Prevenção de Intrusão) a sites de intranet locais.

Note: Marque todas as caixas de seleção na caixa de diálogo Intranet local e clique na **guia Avançado**.



Navegue até **Ferramentas > Segurança > Sites confiáveis > Sites** para adicionar os nomes

de host do CUCM a sites confiáveis:



Verificar

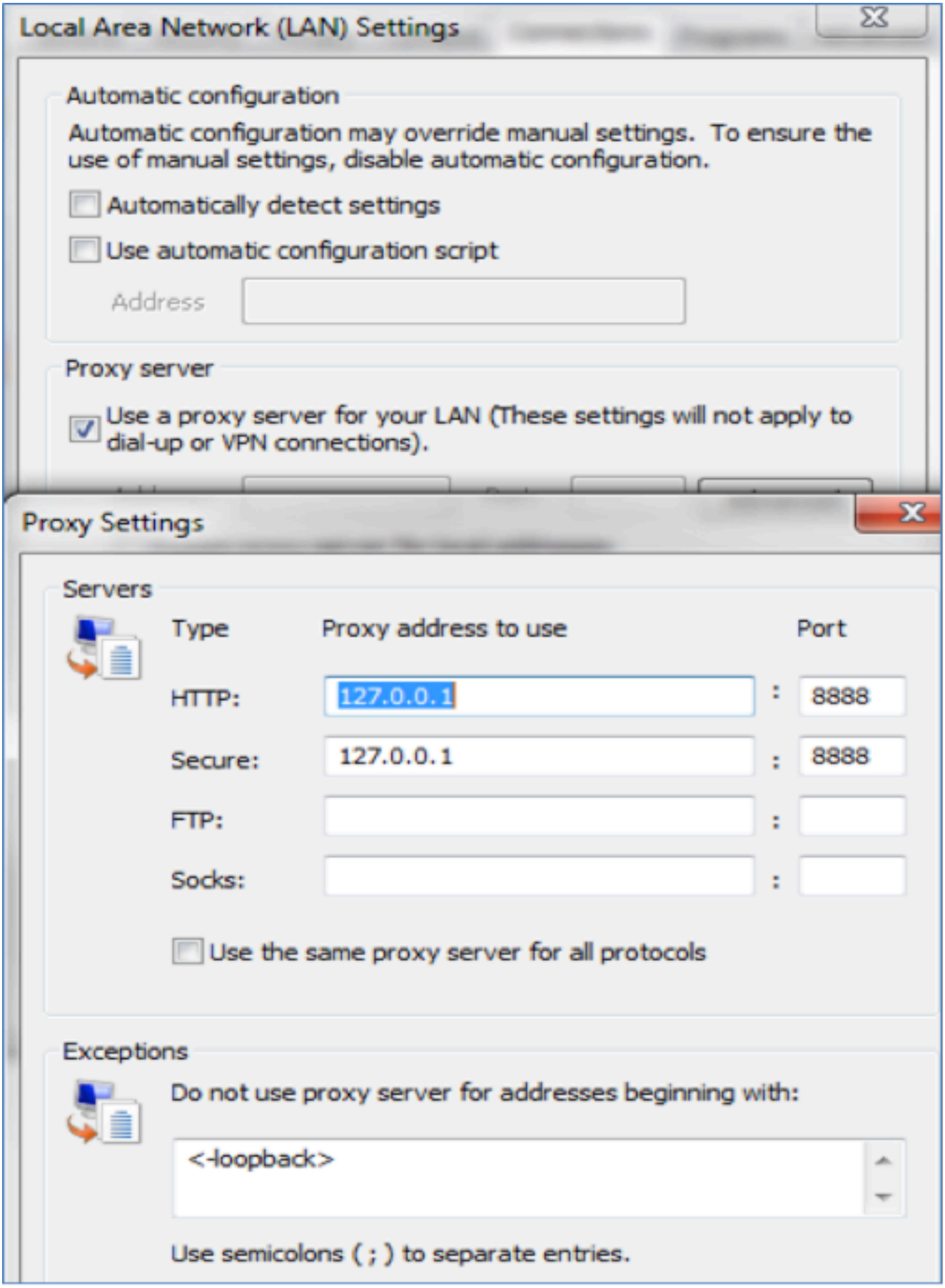
Esta seção explica como verificar qual autenticação (autenticação Kerberos ou NT LAN Manager (NTLM) é usada).

1. Baixe a Fiddler Tool em sua máquina cliente e instale-a.

2. Feche todas as janelas do Internet Explorer.

3. Execute a ferramenta Fiddler e verifique se a opção **Capture Traffic** está ativada no menu File (Arquivo).

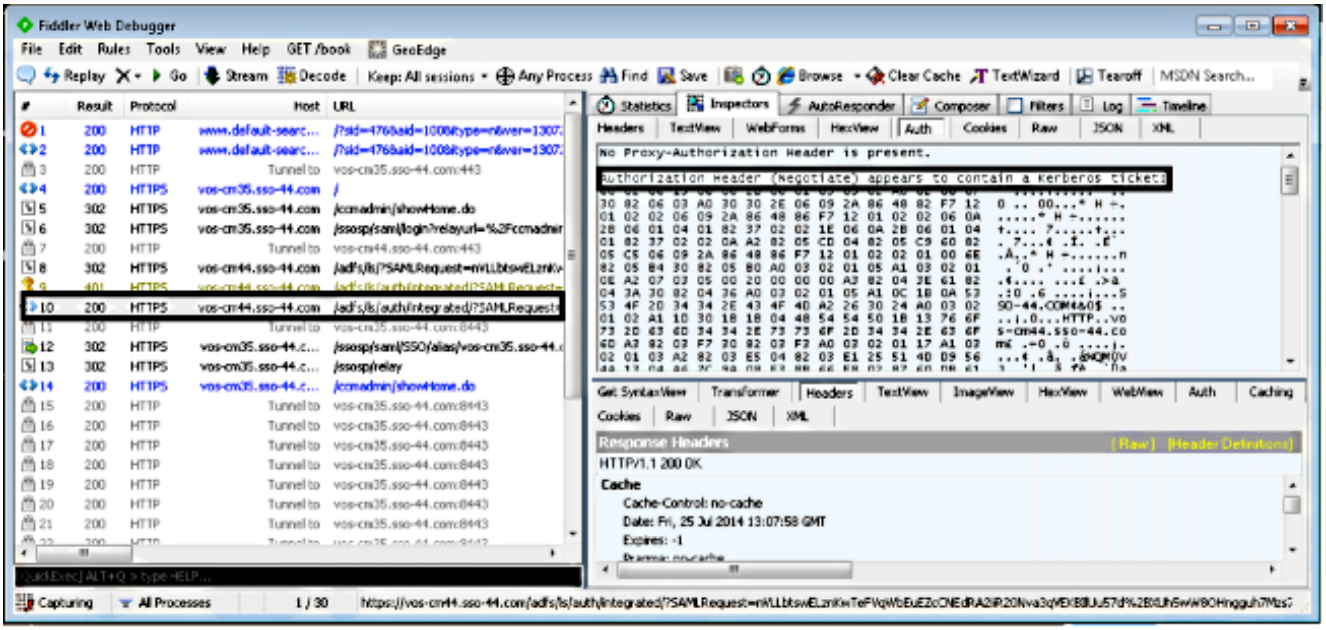
   O Fiddler funciona como um proxy de passagem entre a máquina cliente e o servidor e ouve todo o tráfego, o que temporariamente define suas Configurações do Internet Explorer como esta:



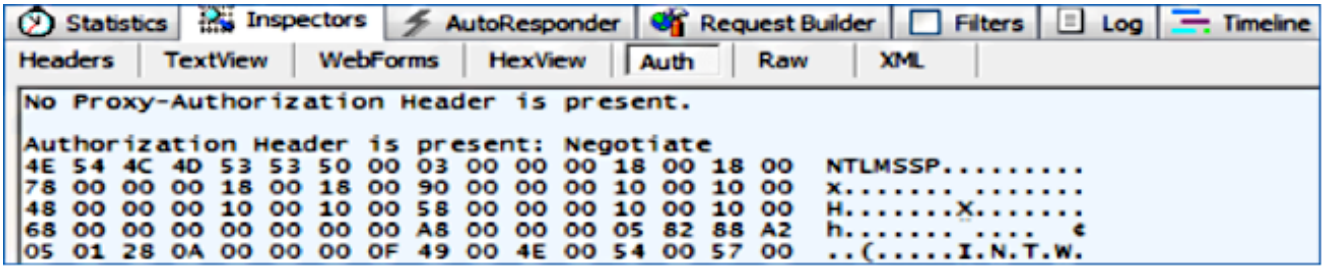
4. Abra o Internet Explorer, navegue até a URL do servidor do CRM (Customer Relationship Management, gerenciamento de relacionamento com o cliente) e clique em alguns links para gerar tráfego.

5. Consulte a janela principal do Fiddler e escolha um dos Quadros em que o Resultado é 200

(sucesso):



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



Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.