Esempio di configurazione di Kerberos con ADFS 2.0 per l'utente finale SAML SSO per Jabber

Sommario

Introduzione

In questo documento viene descritto come configurare Kerberos con Active Directory Federation Services (ADFS) 2.0.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La configurazione di Single Sign-On (SSO) SAML (End User Security Assertion Markup Language) richiede la configurazione di Kerberos per consentire a Jabber di utilizzare l'SSO SAML utente finale per l'autenticazione del dominio. Quando SAML SSO viene implementato con Kerberos, il protocollo LDAP (Lightweight Directory Access Protocol) gestisce tutte le autorizzazioni e la sincronizzazione degli utenti, mentre Kerberos gestisce l'autenticazione. Kerberos è un protocollo di autenticazione da utilizzare in combinazione con un'istanza abilitata per LDAP.

Sui computer Microsoft Windows e Macintosh che fanno parte di un dominio di Active Directory, gli utenti possono accedere senza problemi a Cisco Jabber senza dover immettere un nome utente o una password e non visualizzano neanche una schermata di accesso. Gli utenti che non hanno effettuato l'accesso al dominio sui propri computer continuano a visualizzare un modulo di accesso standard.

Poiché l'autenticazione utilizza un singolo token passato dai sistemi operativi, non è necessario alcun reindirizzamento. Il token viene verificato rispetto al controller di dominio chiave (KDC) configurato e, se è valido, l'utente ha eseguito l'accesso.

Configurazione

Di seguito viene riportata la procedura per configurare Kerberos con ADFS 2.0.

1. Installare Microsoft Windows Server 2008 R2 in un computer.

2. Installare Servizi di dominio Active Directory (ADDS) e ADFS nello stesso computer.

3. Installare Internet Information Services (IIS) nel computer in cui è installato Microsoft Windows Server 2008 R2.

4. Creare un certificato autofirmato per IIS.

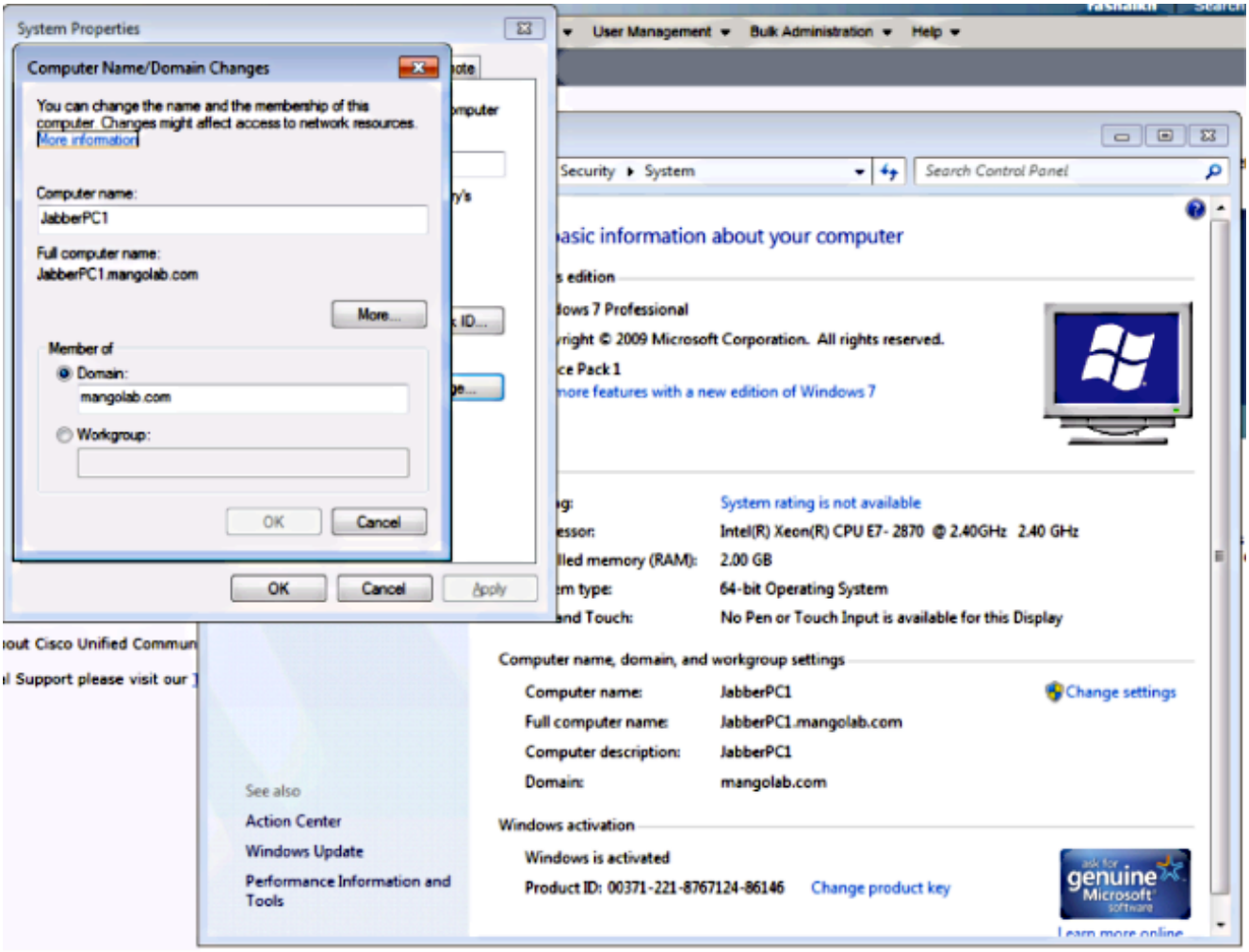
5. Importare il certificato autofirmato in IIS e utilizzarlo come certificato del server HTTPS.

6. Installare Microsoft Windows7 in un altro computer e utilizzarlo come client.

   Modificare il DNS (Domain Name Server) nel computer in cui è stato installato ADDS.

   Aggiungere il computer al dominio creato durante l'installazione di ADDS.

   Vai a **Start**.Fare clic con il pulsante destro del mouse su **Computer**.Fare clic su **Proprietà**.Fare clic su **Cambia impostazioni** sul lato destro della finestra.Fare clic sulla **scheda Nome computer**.Fare clic su **Cambia**.Aggiungere il dominio creato.



7. Verificare se il servizio Kerberos viene generato in entrambi i computer.

   Accedere come amministratore sul computer server e aprire il prompt dei comandi. Eseguire quindi i seguenti comandi:

   cd \windows\System32Biglietti 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
```

   Accedere come utente di dominio sul computer client ed eseguire gli stessi comandi.

```
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. Creare l'identità Kerberos ADFS nel computer in cui è installato ADDS.

   L'amministratore di Microsoft Windows ha eseguito l'accesso al dominio di Microsoft Windows (come <nomedominio>\amministratore), ad esempio nel controller di dominio di Microsoft Windows, e crea l'identità Kerberos ADFS. Il servizio HTTP ADFS deve disporre di un'identità Kerberos denominata nome dell'entità servizio (SPN) nel formato seguente: **HTTP/nome_DNS_del_server_ADFS**.

   Questo nome deve essere mappato all'utente di Active Directory che rappresenta l'istanza

del server HTTP ADFS. Utilizzare l'utilità **setspn di** Microsoft Windows, che dovrebbe essere disponibile per impostazione predefinita in un server Microsoft Windows 2008.

Procedura Registrare gli SPN per il server ADFS. Eseguire il comando **setspn** nel controller di dominio Active Directory.

Ad esempio, quando l'host ADFS è **adfs01.us.renovations.com** e il dominio di Active Directory è **US.RENOVATIONS.COM**, il comando è:

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

Viene applicata la parte **HTTP/**SPN, anche se al server ADFS si accede in genere tramite SSL (Secure Sockets Layer), ovvero HTTPS.

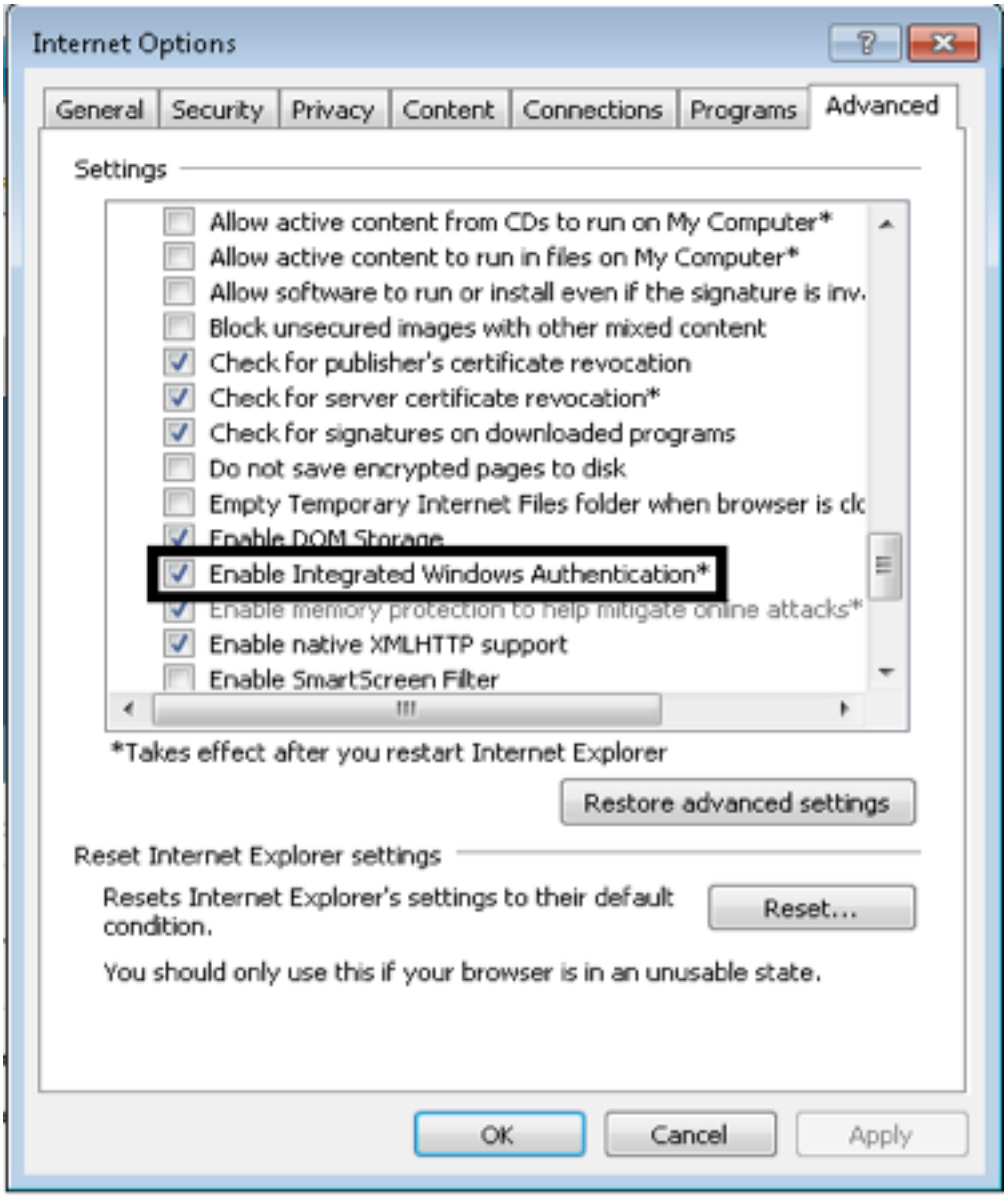
Verificare che gli SPN per il server ADFS siano stati creati correttamente con il comando **setspn** e visualizzare l'output.

```
setspn -L
```

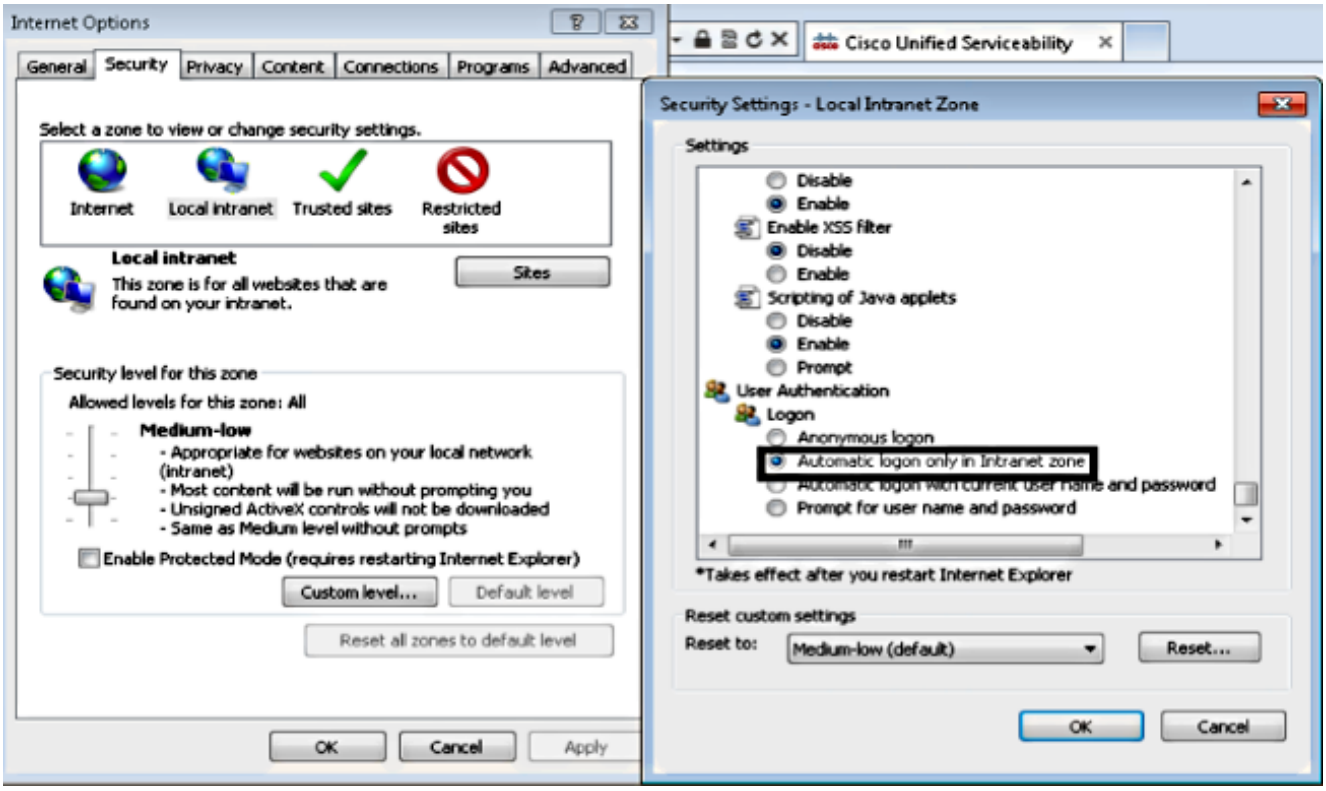
9. Configurare le impostazioni del browser del client di Microsoft Windows.

   Per abilitare l'autenticazione integrata di Windows, selezionare **Strumenti > Opzioni Internet > Avanzate**.

   Selezionare la **casella di controllo Abilita autenticazione integrata di Windows**:

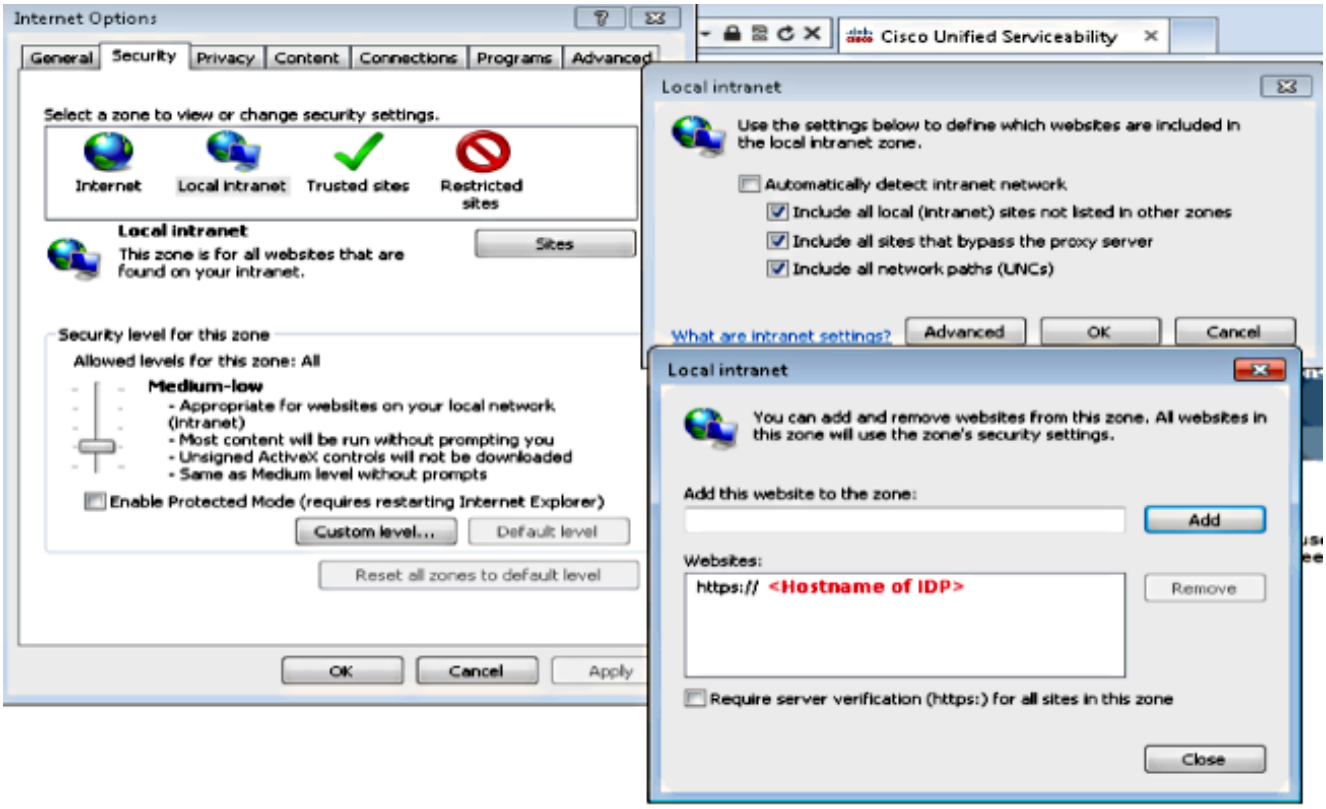


   Selezionare **Strumenti > Opzioni Internet > Protezione > Intranet locale > Livello personalizzato** per selezionare **Accesso automatico solo nell'area Intranet**.

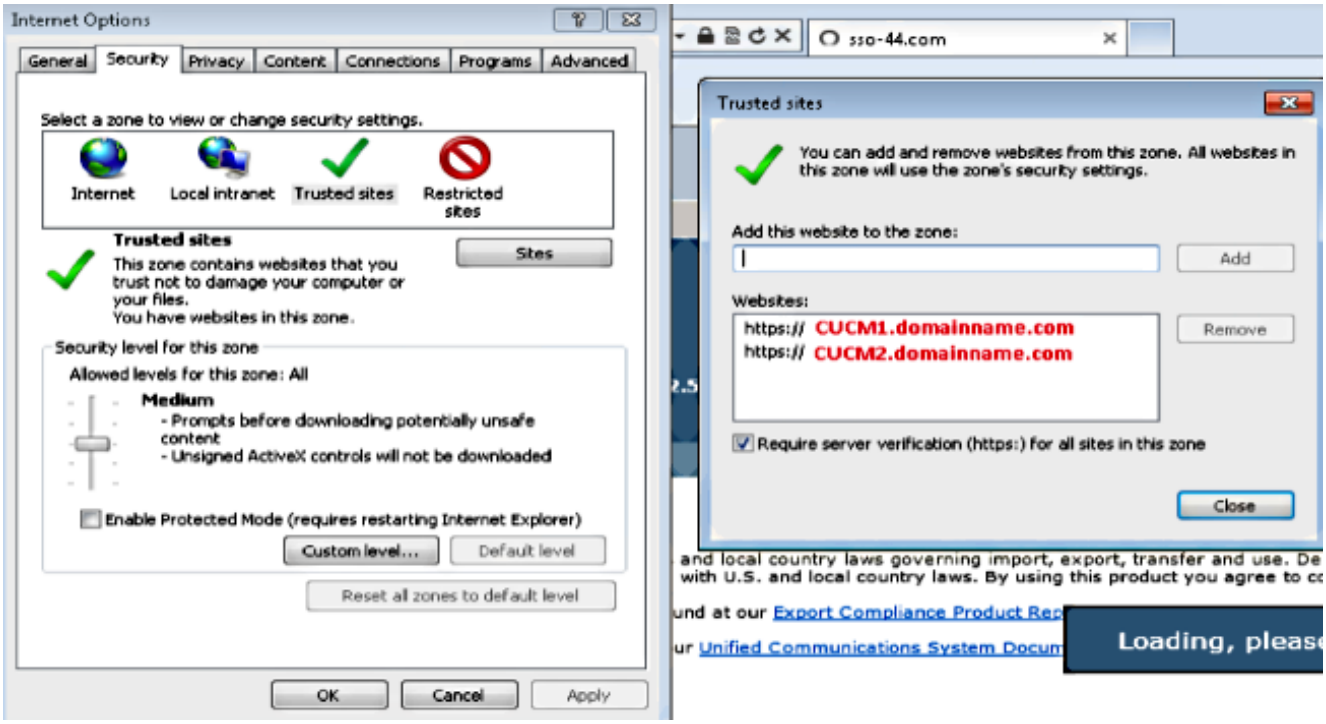


Selezionare **Strumenti > Opzioni Internet > Sicurezza > Intranet locale > Siti > Avanzate** per aggiungere l'URL di Rilevamento e prevenzione intrusioni (IDP) ai siti Intranet locali.

Nota: Selezionare tutte le caselle di controllo nella finestra di dialogo Intranet locale e fare clic sulla **scheda Avanzate**.



Per aggiungere i nomi host CUCM ai siti attendibili, selezionare **Strumenti > Protezione > Siti attendibili > Siti**:



Verifica

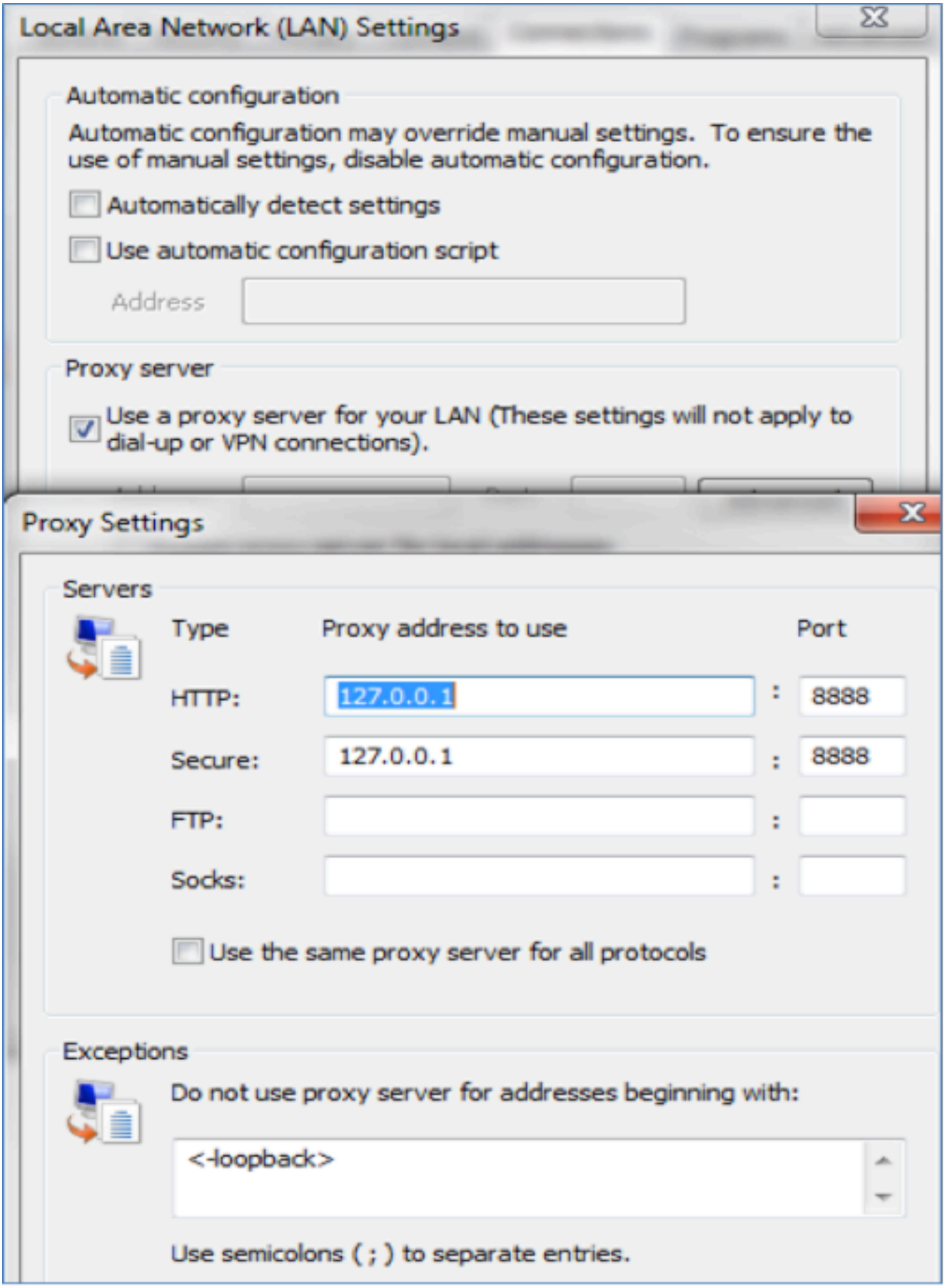
Questa sezione spiega come verificare quale autenticazione (Kerberos o NTLM) viene utilizzata.

1. Scaricare lo strumento Finder sul computer client e installarlo.

2. Chiudere tutte le finestre di Internet Explorer.

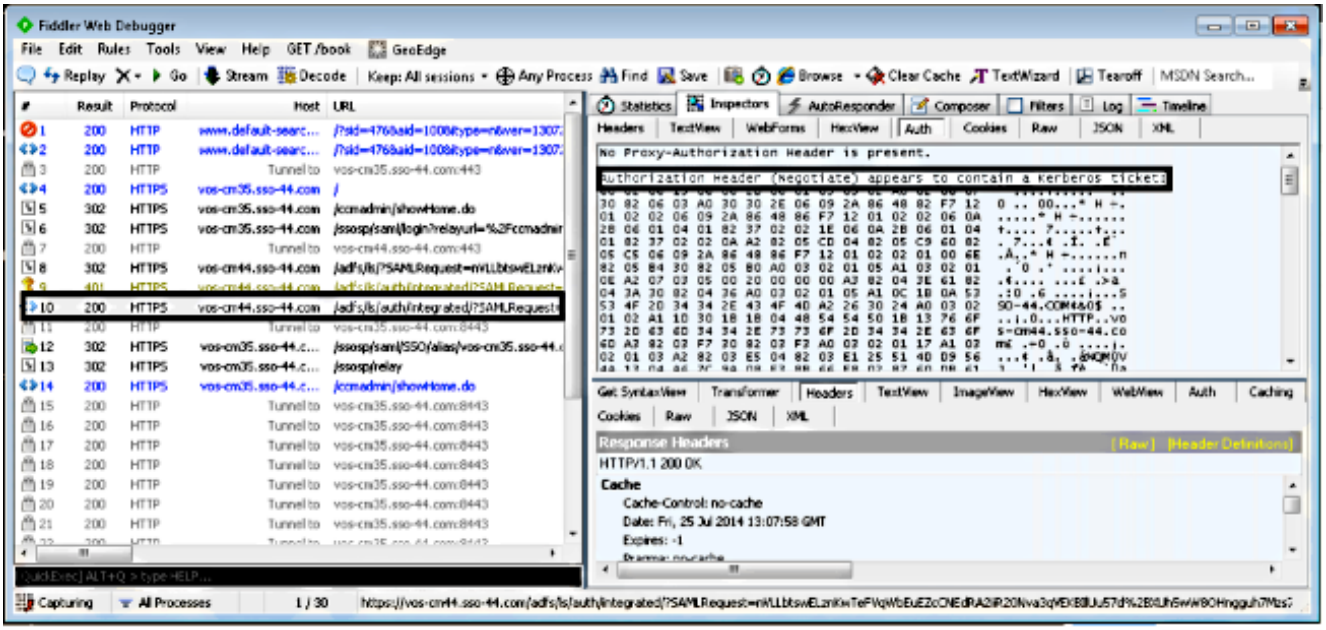
3. Eseguire lo strumento Trova e verificare che l'opzione **Cattura traffico** sia attivata nel menu File.

   Fiddler funge da proxy pass-through tra il computer client e il server ed è in ascolto di tutto il traffico, che imposta temporaneamente le impostazioni di Internet Explorer nel modo seguente:

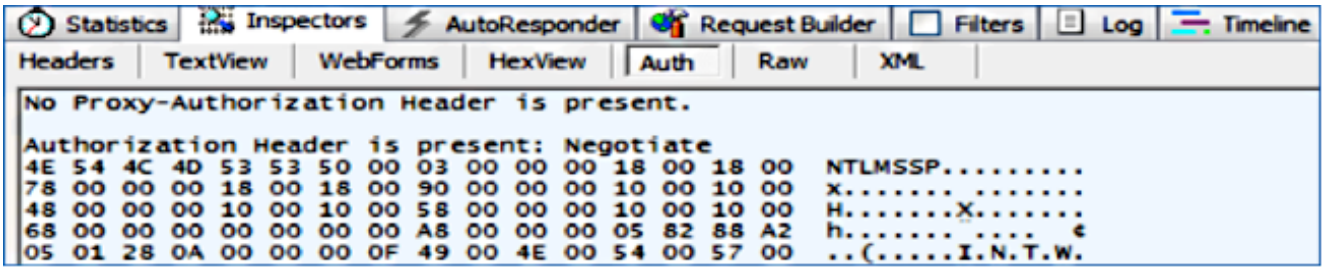


4. Aprire Internet Explorer, individuare l'URL del server CRM e fare clic su alcuni collegamenti per generare traffico.

5. Fate riferimento alla finestra principale del Finder e scegliete uno dei fotogrammi in cui il risultato è 200 (esito positivo):



Se il tipo di autenticazione è NTLM, all'inizio del frame viene visualizzato **Negotiate - NTLMSSP**, come mostrato di seguito:



Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.