Kerberos met ADFS 2.0 voor SAML van eindgebruiker voor Jabber Configuration Voorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u Kerberos kunt configureren met ADFS (Active Directory Federation Services) 2.0.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Voor de configuratie van één enkel teken (End User Security Assessment Markup Language, SAML) moeten Kerberos (SSO) en de configuratie worden geconfigureerd zodat de end User SAML SIP voor Jabber kan werken met domeinverificatie. Wanneer SAML SSO met Kerberos wordt geïmplementeerd, verwerkt Lichtgewicht Directory Access Protocol (LDAP) alle autorisatie- en gebruikerssynchronisatie, terwijl Kerberos de authenticatie beheert. Kerberos is een verificatieprotocol dat bedoeld is om te worden gebruikt in combinatie met een instantie die met de LDAP is ingeschakeld.

Op Microsoft Windows- en Macintosh-machines die worden aangesloten op een Active Directory-domein, kunnen gebruikers moeiteloos inloggen in Cisco Jabber zonder dat ze een gebruikersnaam of wachtwoord moeten invoeren en worden ze niet eens een inlogscherm weergegeven. Gebruikers die niet op hun computers zijn aangemeld, zien nog steeds een standaard inlogformulier.

Omdat de authenticatie één enkel token gebruikt dat van de besturingssystemen wordt doorgegeven, is geen omleiding vereist. De token is geverifieerd tegen de geconfigureerde Key Domain Controller (KDC) en als deze geldig is, is de gebruiker aangemeld.

Configuratie

Hier is de procedure om Kerberos met ADFS 2.0 te configureren.

1. Installeer Microsoft Windows Server 2008 R2 op een machine.

2. Installeer Active Directory Domain Services (ADDS) en ADFS op dezelfde machine.

3. Installeer Internet Information Services (IS) op de Microsoft Windows Server 2008 R2-geïnstalleerde machine.

4. Maak een zelf-ondertekend certificaat voor ISIS.

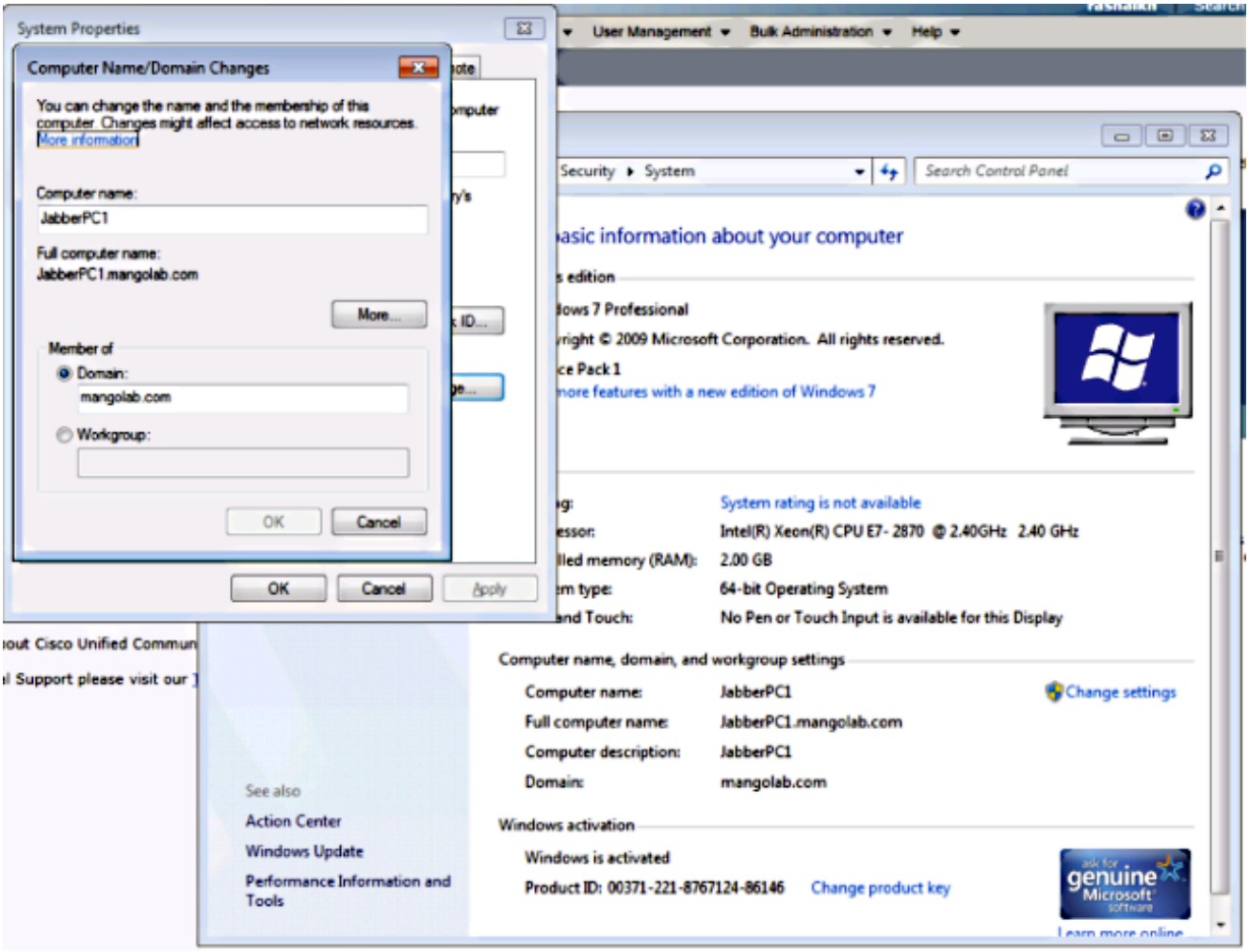
5. Importeer het zelf-ondertekende certificaat in IS en gebruik het als HTTPS servercertificaat.

6. Installeer Microsoft Windows7 op een andere machine en gebruik dit als een client.

   Wijzig de Domain Name Server (DNS) in de machine waar u ADDS hebt geïnstalleerd.

   Voeg deze machine toe aan het domein dat u met de installatie van ADDS hebt gemaakt.

   Ga naar **Start**.Klik met de rechtermuisknop op **Computer**.Klik op **Eigenschappen**.Klik aan de rechterkant van het venster op **Instellingen wijzigen**.Klik op het **tabblad Computer Name**.Klik op **Wijzigen**.Voeg het domein toe dat u hebt gemaakt.



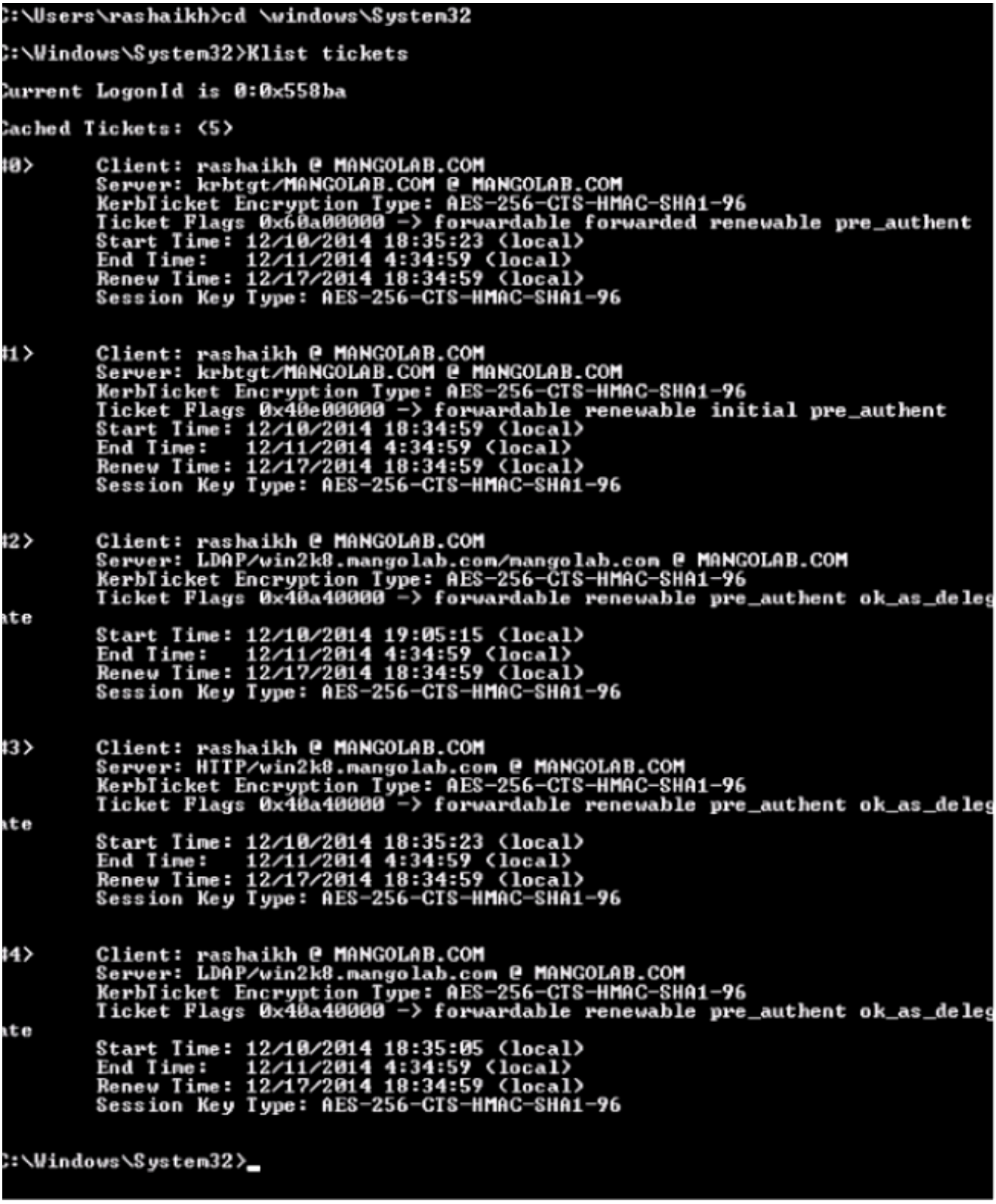
7. Controleer of de Kerberos-service op beide machines genereert.

   Meld u aan als beheerder in de servermachine en open de opdrachtmelding. Voert vervolgens deze opdrachten uit:

   cd \windows\System32Klist tickets

```
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
```

   Log in als domeingebruiker op de client en voer dezelfde opdrachten uit.



8. Maak de ADFS Kerberos-identiteit op de machine waar u ADDS installeerde.

   De Microsoft Windows-beheerder inlogt in het Microsoft Windows-domein (als <naam>\beheerder), bijvoorbeeld in de Microsoft Windows-domeincontroller, maakt de ADFS Kerberos-identiteit aan. De ADFS HTTP-service moet een Kerberos-identiteit hebben, die een Service Principal Name (SPN) wordt genoemd in deze indeling: HTTP/DNS_name_of_ADFS_server.

   Deze naam moet in kaart worden gebracht aan de Active Directory-gebruiker die de ADFS

HTTP-serverinstantie vertegenwoordigt. Gebruik het Microsoft Windows **software**-hulpprogramma dat standaard beschikbaar zou moeten zijn op een Microsoft Windows 2008-server.

Procedure Registreer de SPN's voor de ADFS-server. Draai de **ingestelde** opdracht op de Active Directory-controller.

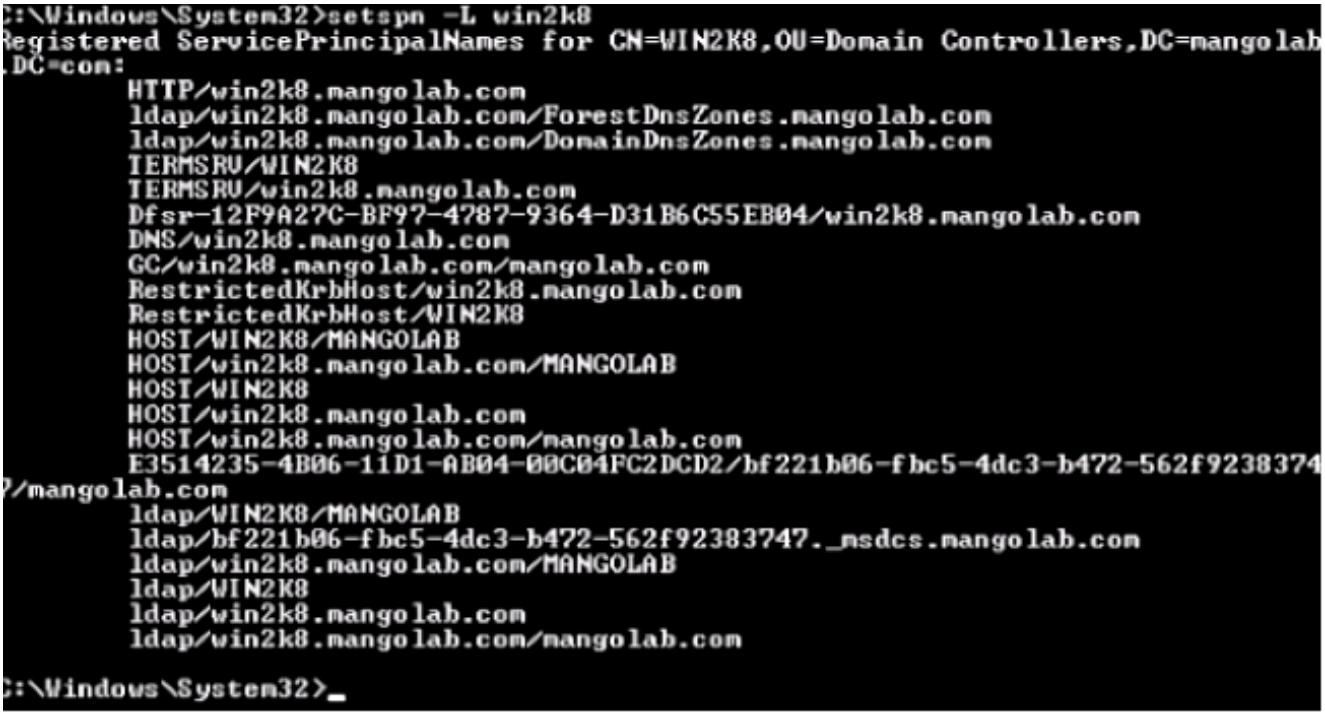
Bijvoorbeeld, wanneer de ADFS-host **adfs01.us.renovations.com** is en het Active Directory-domein **US.RENOVATIONS.COM** is, is de opdracht:

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

Het **HTTP/**gedeelte van de SPN is van toepassing, ook al heeft de ADFS-server doorgaans toegang tot Secure Socket Layer (SSL), wat HTTPS is.

Controleer of de SPN's voor de ADFS-server goed met de **ingestelde** spn-opdracht zijn gemaakt en bekijk de uitvoer.

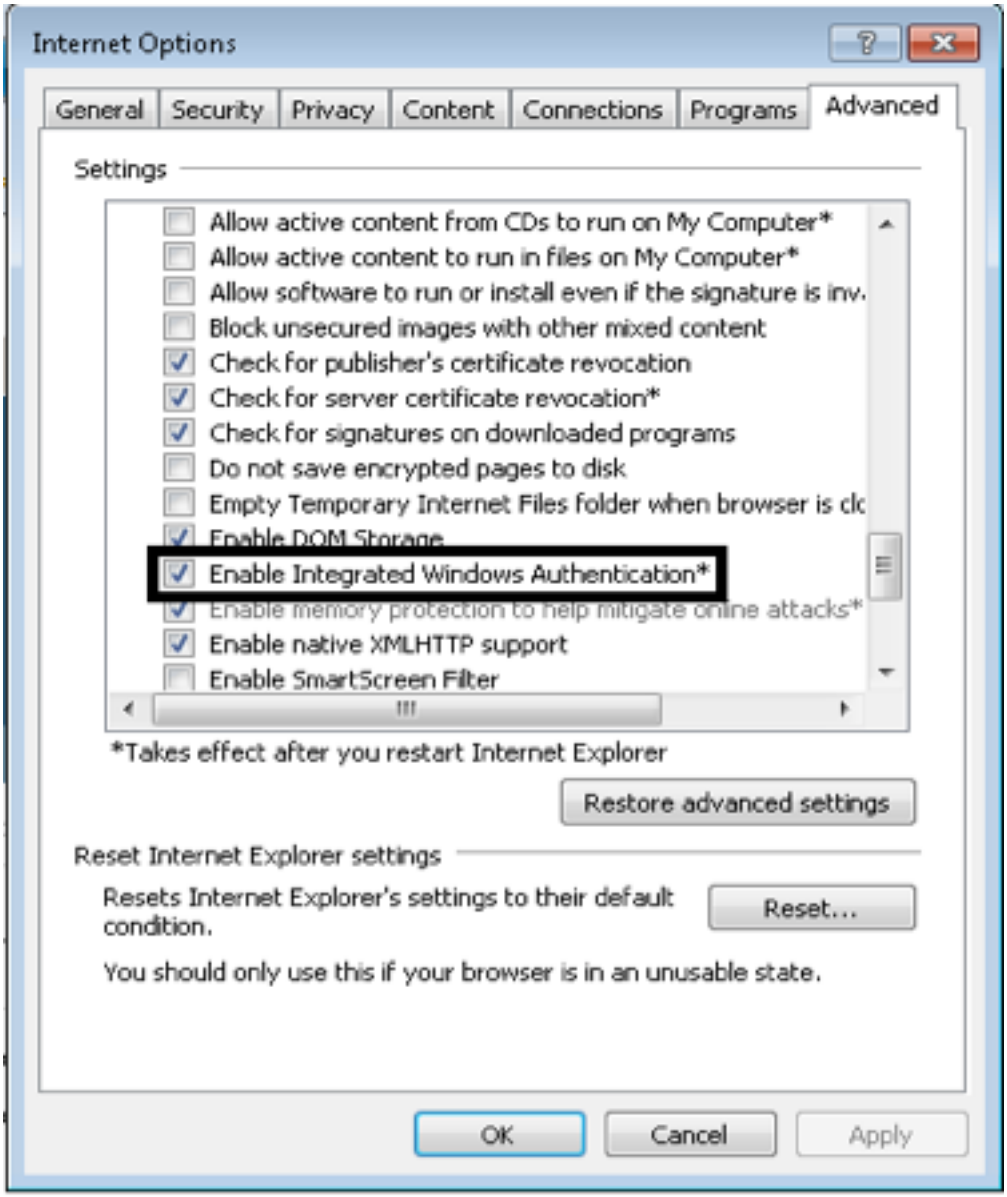
```
setspn -L
```



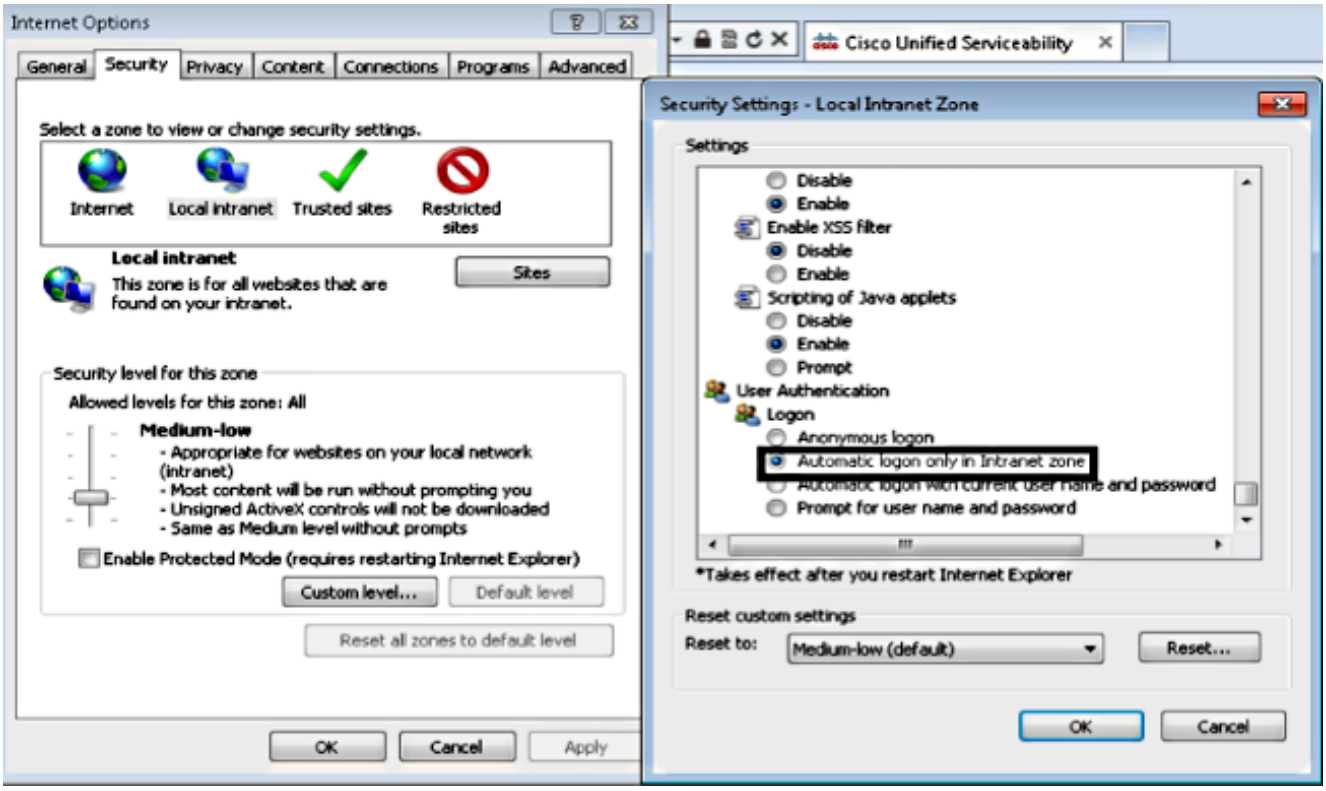
9. Configureer de instellingen van de Microsoft Windows-client.

   Navigeer naar **Gereedschappen > Internet-opties > Geavanceerd** om geïntegreerde Windows-verificatie in te schakelen.

   Controleer het **vakje Geïntegreerde Windows-verificatie inschakelen**:

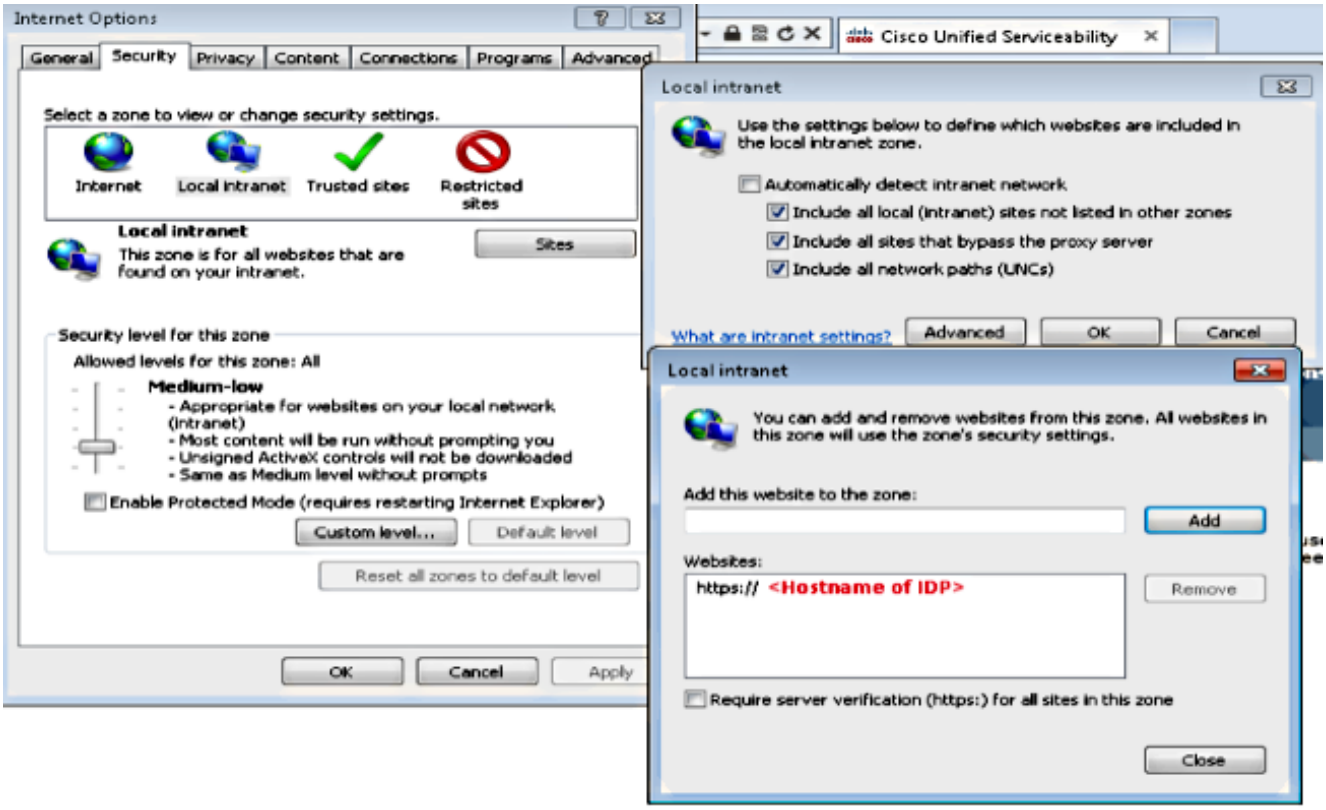


Navigeer naar **Gereedschappen > Internet-opties > Beveiliging > Lokaal intranet > Aangepast niveau...** om **alleen** de optie **Automatisch aanmelden in Intranet zone** te selecteren.



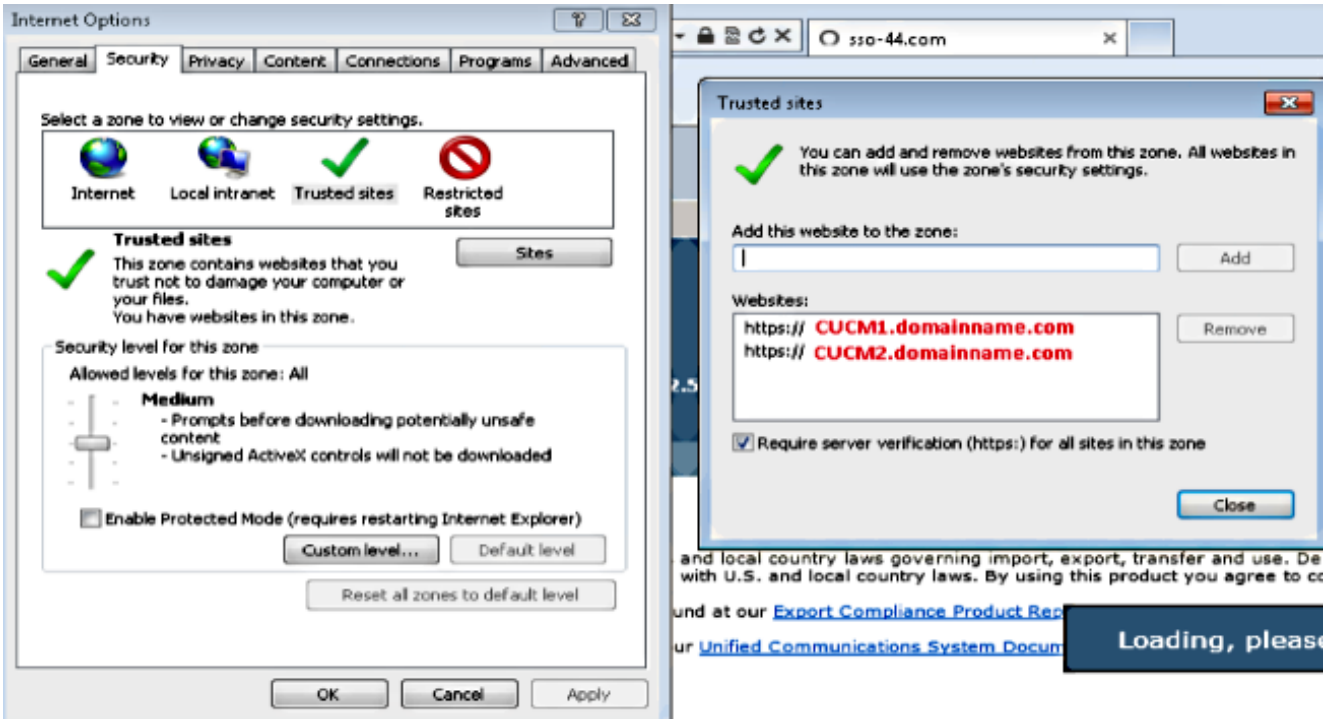
Navigeer naar **Gereedschappen > Internet-opties > Beveiliging > Lokaal intranet > Sites > Geavanceerd** om de URL van inbraakdetectie en -preventie (IDP) aan lokale intranet toe te voegen.

Opmerking: Controleer alle vinkjes in het dialoogvenster Local Intranet en klik op het **tabblad Advanced**.



Navigeer naar **Gereedschappen > Beveiliging > Vertrouwde sites > Plaatsen** om de CUCM-

hostnamen aan Trusted-sites toe te voegen:



Verifiëren

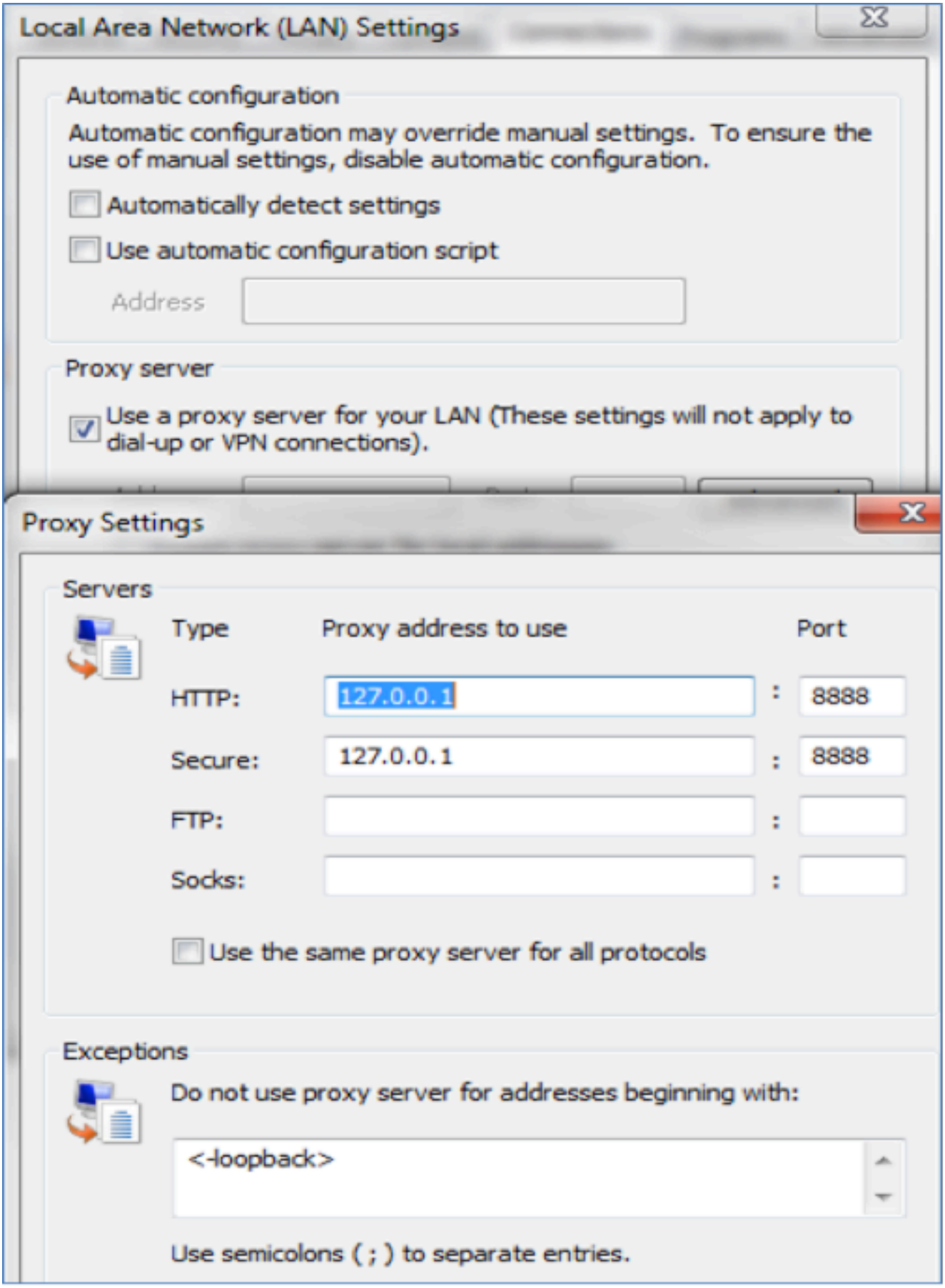
In deze sectie wordt uitgelegd hoe u controleert welke verificatie (Kerberos of NT LAN Manager (NTLM) wordt gebruikt.

1. Download het Verkenner gereedschap naar uw clientmachine en installeer het.

2. Sluit alle Internet Explorer-vensters.

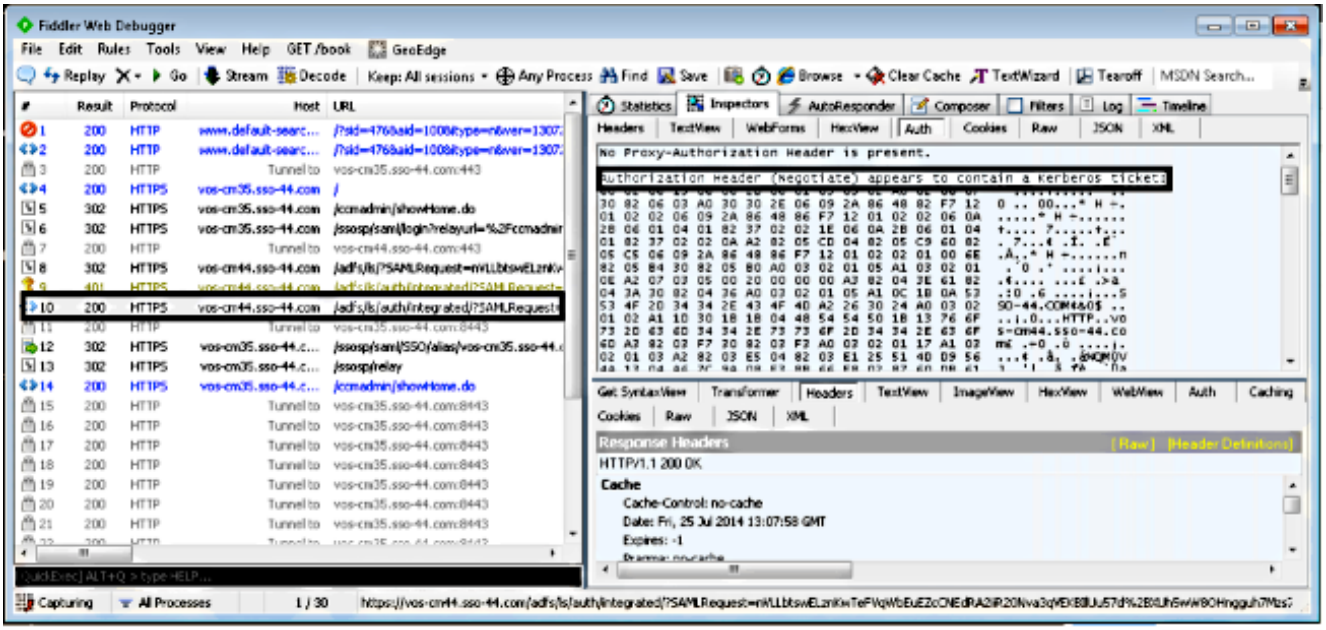
3. Draai het gereedschap Fuzler en controleer of de optie **Opname verkeer** is ingeschakeld onder het menu Bestand.

   Fiddler werkt als een passthrough-proxy tussen de client en de server en luistert naar al het verkeer, waarbij tijdelijk de instellingen van Internet Explorer op deze manier worden ingesteld:

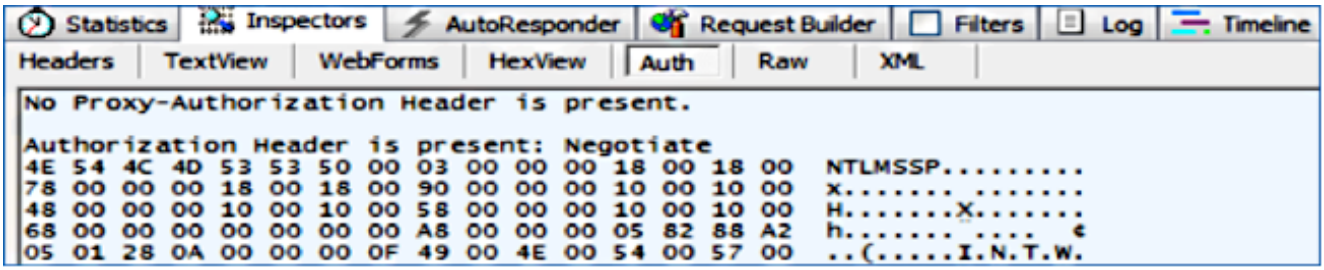


4. Open Internet Explorer, blader in de URL van de CRM-server (Customer Relation Management) en klik op een paar koppelingen om verkeer te genereren.

5. Raadpleeg het hoofdvenster van Fidler en kies een van de frames waarin het resultaat 200 is (succes):



Als het verificatietype NTLM is, dan ziet u **Negotiate - NTLMSSP** in het begin van het frame zoals hier wordt getoond:



Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.