Kerberos mit ADFS 2.0 für Endbenutzer SAML SSO für Jabber - Konfigurationsbeispiel

Inhalt

Einführung

Dieses Dokument beschreibt, wie Kerberos mit Active Directory Federation Services (ADFS) 2.0 konfiguriert wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Für die SSO-Konfiguration (Single Sign On) der Endbenutzer Security Assertion Markup Language (SAML) muss Kerberos konfiguriert werden, damit die Endbenutzer-SAML SSO für

Jabber mit der Domänenauthentifizierung arbeiten kann. Wenn SAML SSO mit Kerberos implementiert wird, übernimmt das Lightweight Directory Access Protocol (LDAP) die gesamte Autorisierung und Benutzersynchronisierung, während Kerberos die Authentifizierung übernimmt. Kerberos ist ein Authentifizierungsprotokoll, das in Verbindung mit einer LDAP-fähigen Instanz verwendet werden soll.

Bei Microsoft Windows- und Macintosh-Computern, die einer Active Directory-Domäne angehören, können sich Benutzer problemlos bei Cisco Jabber anmelden, ohne einen Benutzernamen oder ein Kennwort eingeben zu müssen. Es wird nicht einmal ein Anmeldebildschirm angezeigt. Benutzer, die nicht bei der Domäne auf ihrem Computer angemeldet sind, sehen immer noch ein Standard-Anmeldeformular.

Da bei der Authentifizierung ein einzelnes Token verwendet wird, das von den Betriebssystemen übergeben wird, ist keine Umleitung erforderlich. Das Token wird anhand des konfigurierten Key Domain Controller (KDC) überprüft. Wenn es gültig ist, ist der Benutzer angemeldet.

Konfiguration

Hier ist die Prozedur zur Konfiguration von Kerberos mit ADFS 2.0.

1. Installieren Sie Microsoft Windows Server 2008 R2 auf einem Computer.

2. Installieren Sie Active Directory Domain Services (ADDS) und ADFS auf demselben Computer.

3. Installieren Sie Internetinformationsdienste (IIS) auf dem Computer, auf dem Microsoft Windows Server 2008 R2 installiert ist.

4. Erstellen Sie ein selbstsigniertes Zertifikat für IIS.

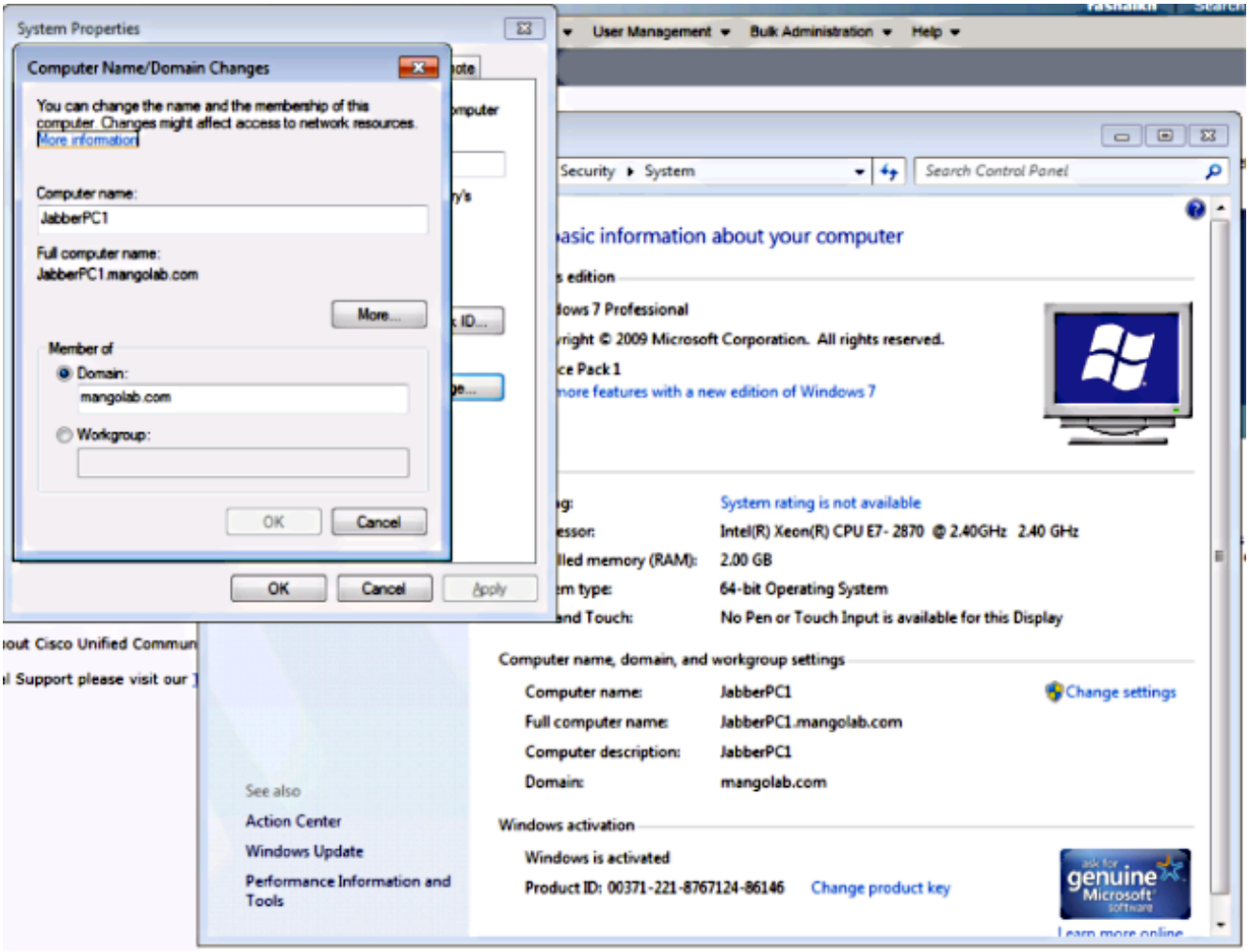
5. Importieren Sie das selbstsignierte Zertifikat in IIS, und verwenden Sie es als HTTPS-Serverzertifikat.

6. Installieren Sie Microsoft Windows7 auf einem anderen Computer, und verwenden Sie es als Client.

   Ändern Sie den Domain Name Server (DNS) auf den Computer, auf dem ADDS installiert ist.

   Fügen Sie diesen Computer der Domäne hinzu, die Sie bei der Installation von ADDS erstellt haben.

   Klicken Sie auf **Start**.Klicken Sie mit der rechten Maustaste auf **Computer**.Klicken Sie auf **Eigenschaften**.Klicken Sie rechts im Fenster auf **Einstellungen ändern**.Klicken Sie auf die **Registerkarte Computername**.Klicken Sie auf **Ändern**.Fügen Sie die von Ihnen erstellte Domäne hinzu.



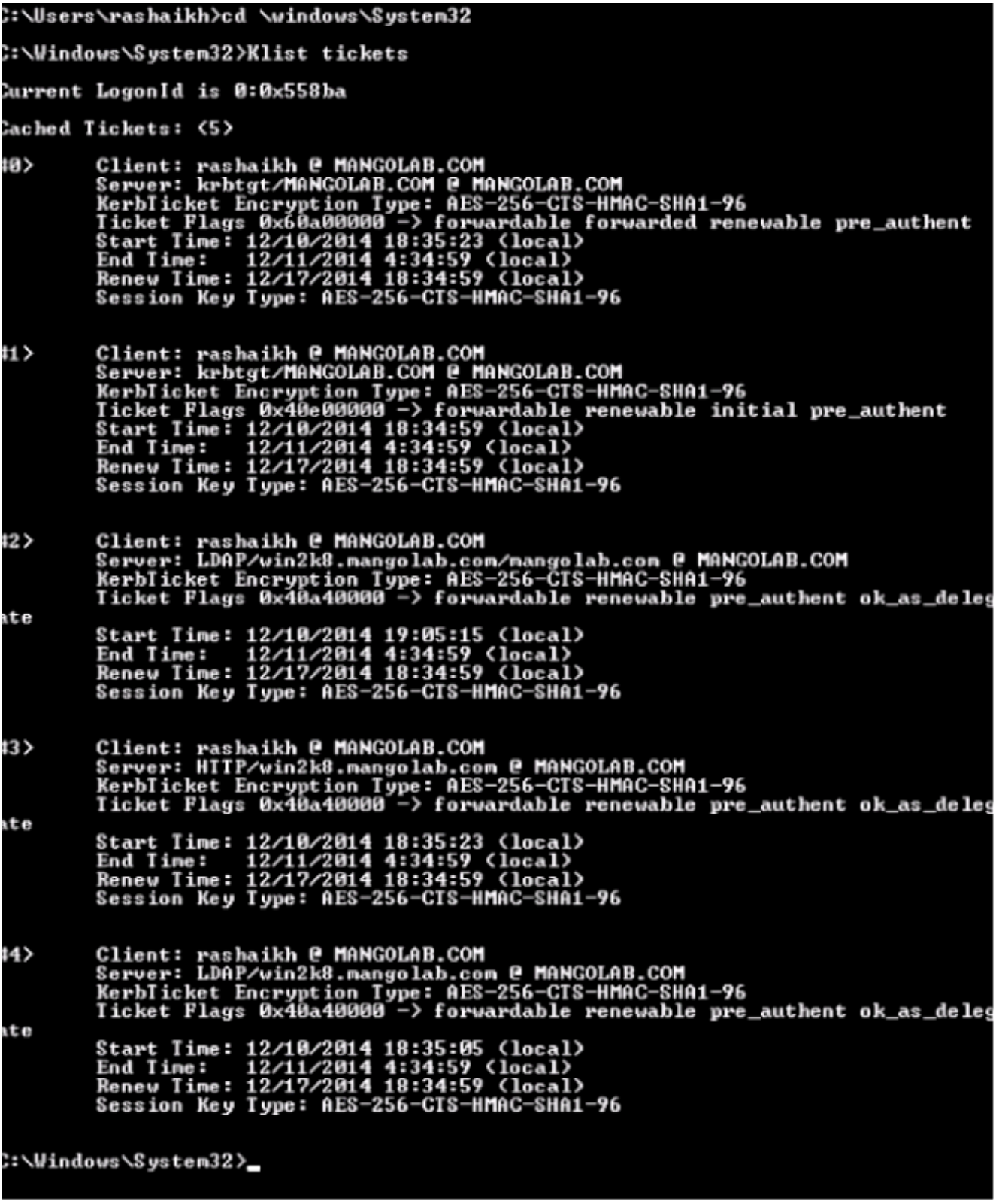
7. Überprüfen Sie, ob der Kerberos-Dienst auf beiden Computern generiert wird.

   Melden Sie sich als Administrator auf dem Servercomputer an, und öffnen Sie die Eingabeaufforderung. Führen Sie dann die folgenden Befehle aus:

   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
```

   Melden Sie sich als Domänenbenutzer auf dem Client-Computer an, und führen Sie die gleichen Befehle aus.



8. Erstellen Sie die ADFS Kerberos-Identität auf dem Computer, auf dem Sie ADDS installiert haben.

   Der Microsoft Windows-Administrator, der sich bei der Microsoft Windows-Domäne angemeldet hat (z. B. als <Domänenname>\administrator), erstellt die ADFS Kerberos-Identität. Der ADFS-HTTP-Service muss eine Kerberos-Identität aufweisen, die als Service Principal Name (SPN) bezeichnet wird. Dieses Format hat folgende Eigenschaften: HTTP/DNS_Name_of_ADFS_Server.

Dieser Name muss dem Active Directory-Benutzer zugeordnet werden, der die ADFS-HTTP-Serverinstanz darstellt. Verwenden Sie das Microsoft Windows **setspn**-Dienstprogramm, das standardmäßig auf einem Microsoft Windows 2008-Server verfügbar sein sollte.

Vorgehensweise Registrieren Sie die SPNs für den ADFS-Server. Führen Sie auf dem Active Directory-Domänencontroller den Befehl **setspn aus**.

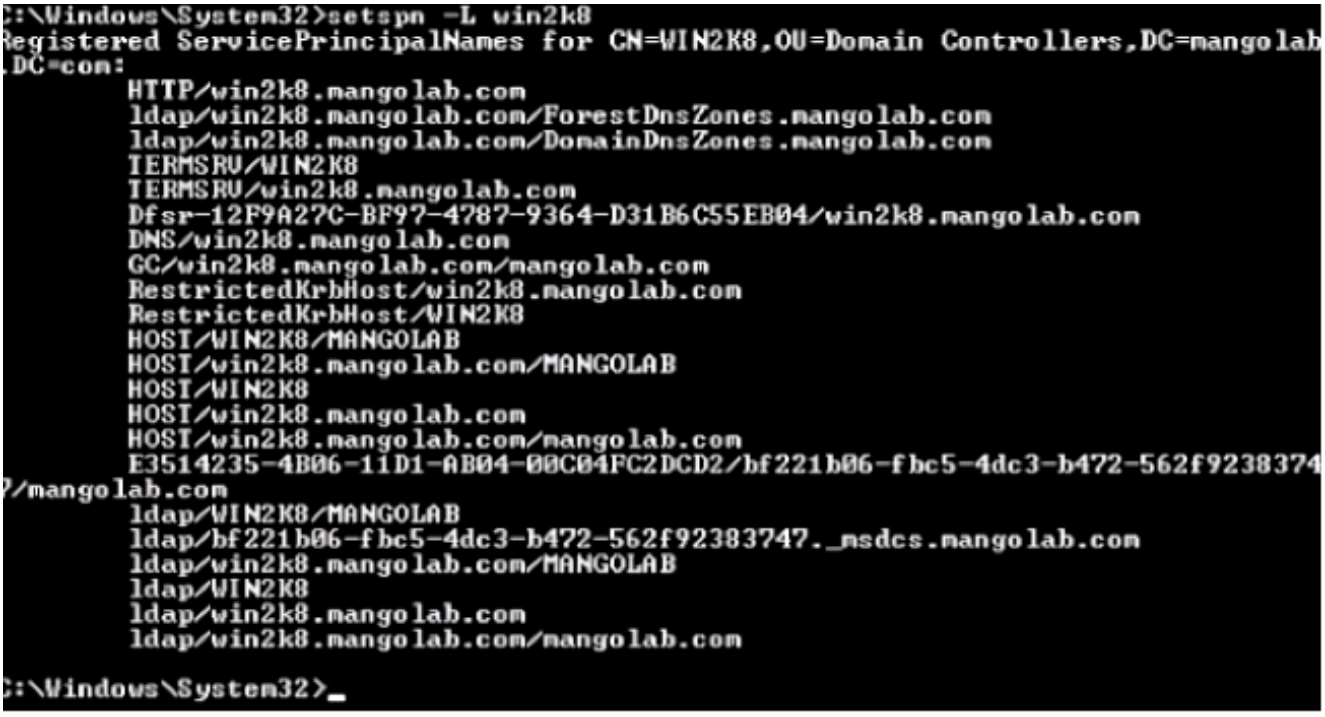
Wenn beispielsweise der ADFS-Host **adfs01.us.renovations.com** ist und die Active Directory-Domäne **US.RENOVATIONS.COM** ist, lautet der Befehl:

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

Der **HTTP/**Teil des SPN gilt, obwohl der Zugriff auf den ADFS-Server in der Regel über Secure Sockets Layer (SSL) erfolgt, d. h. HTTPS.

Überprüfen Sie, ob die SPNs für den ADFS-Server mit dem Befehl **setspn** korrekt erstellt wurden und zeigen Sie die Ausgabe an.

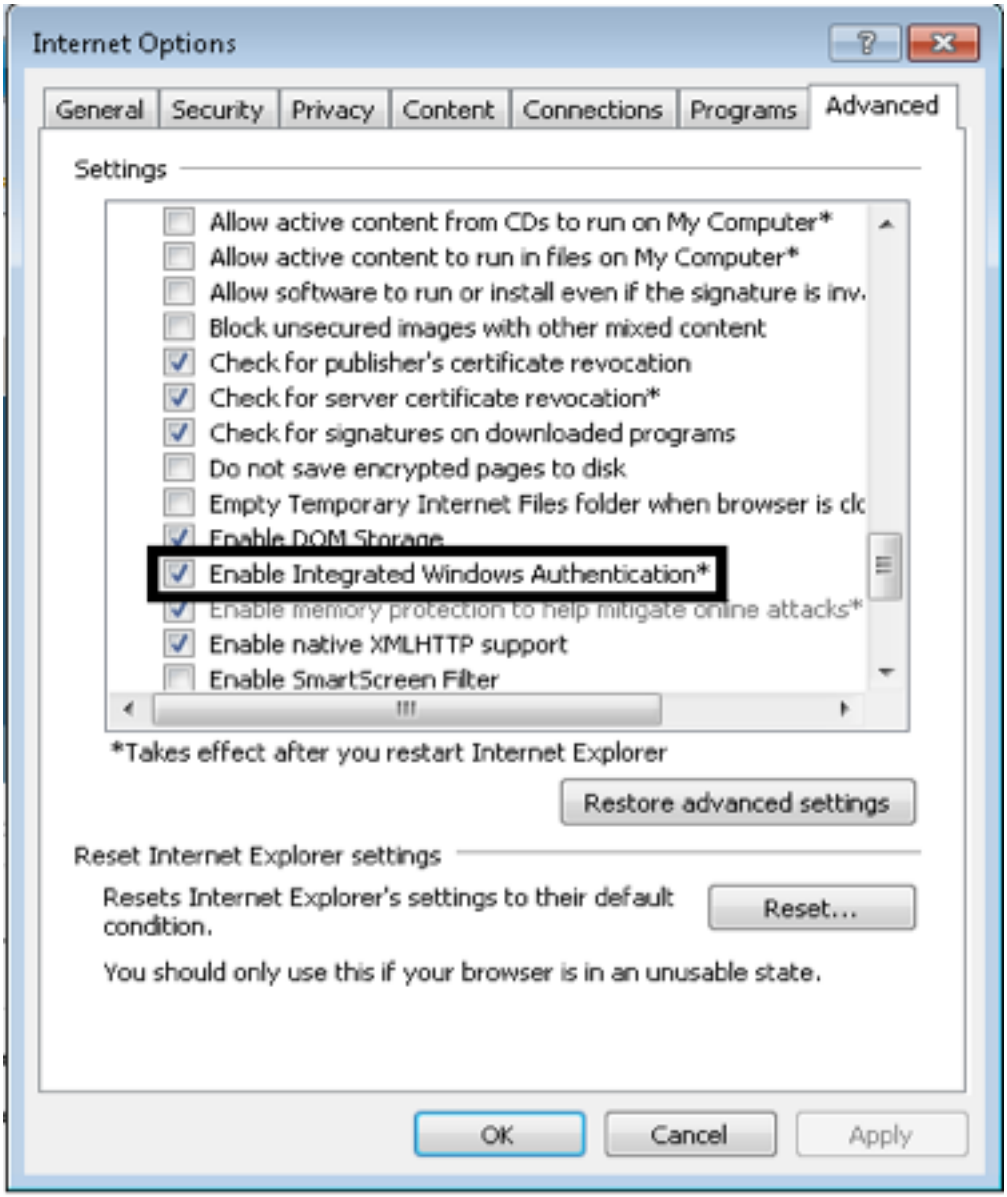
```
setspn -L
```



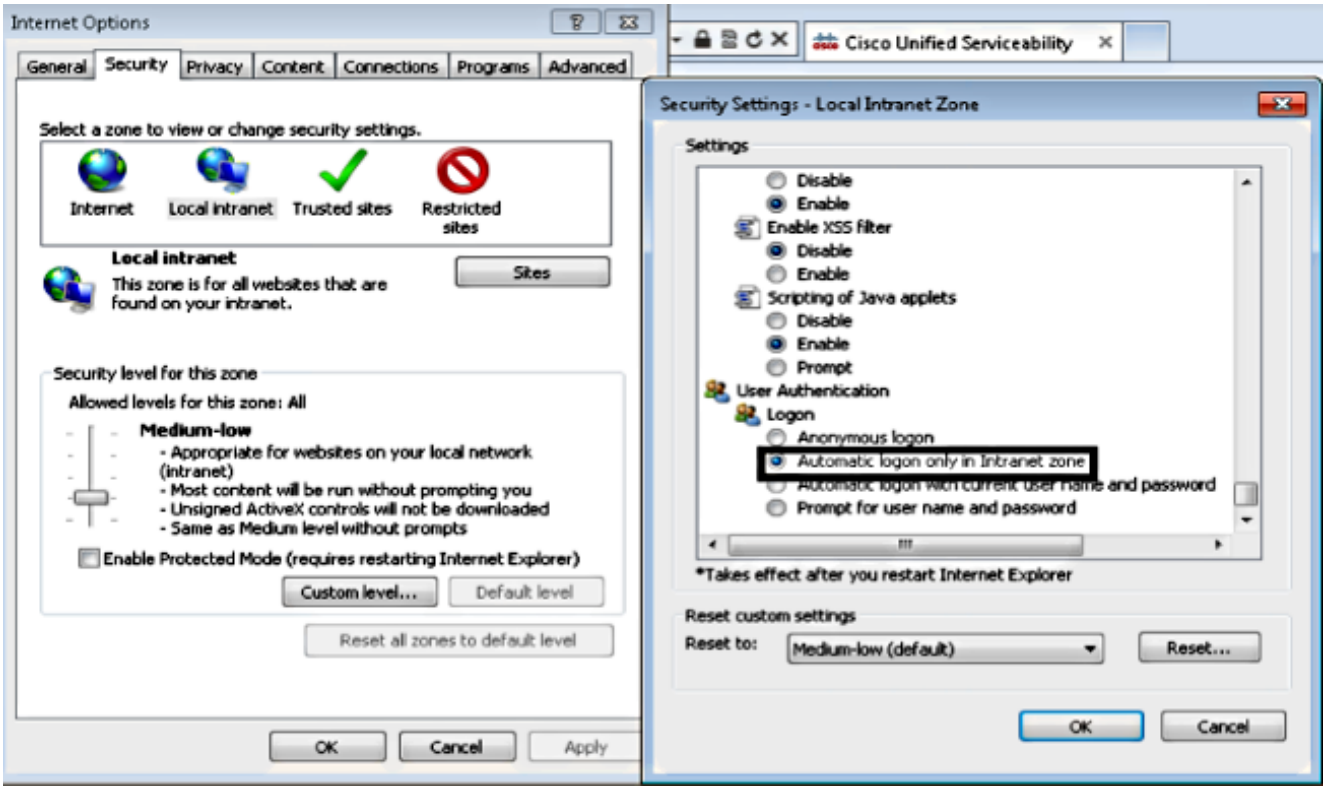
9. Konfigurieren Sie die Browsereinstellungen des Microsoft Windows-Clients.

   Navigieren Sie zu **Extras > Internetoptionen > Erweitert**, um die integrierte Windows-Authentifizierung zu aktivieren.

   Aktivieren Sie das **Kontrollkästchen Integrierte Windows-Authentifizierung aktivieren**:

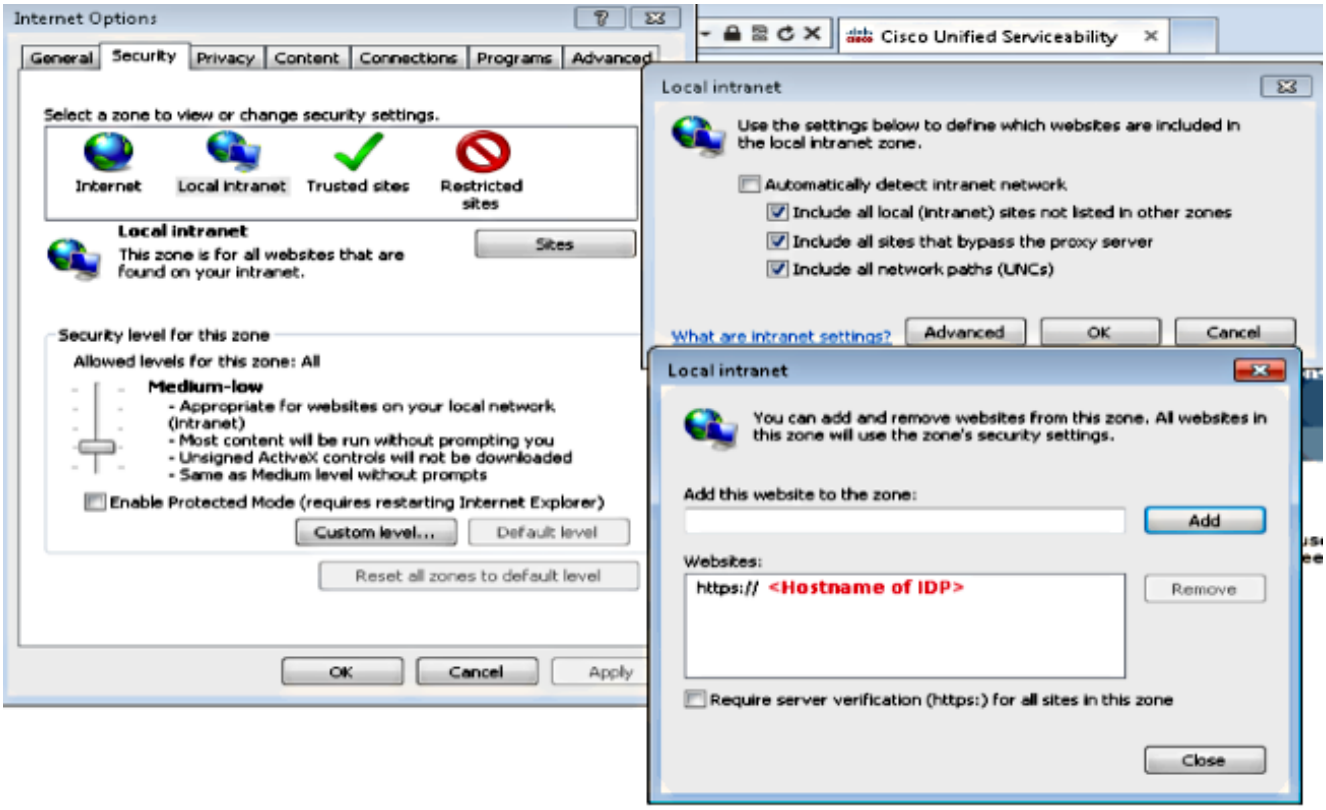


Navigieren Sie zu **Extras > Internetoptionen > Sicherheit > Lokales Intranet > Benutzerdefiniert..** um die Option **Automatische Anmeldung nur in der Intranetzone** auszuwählen.



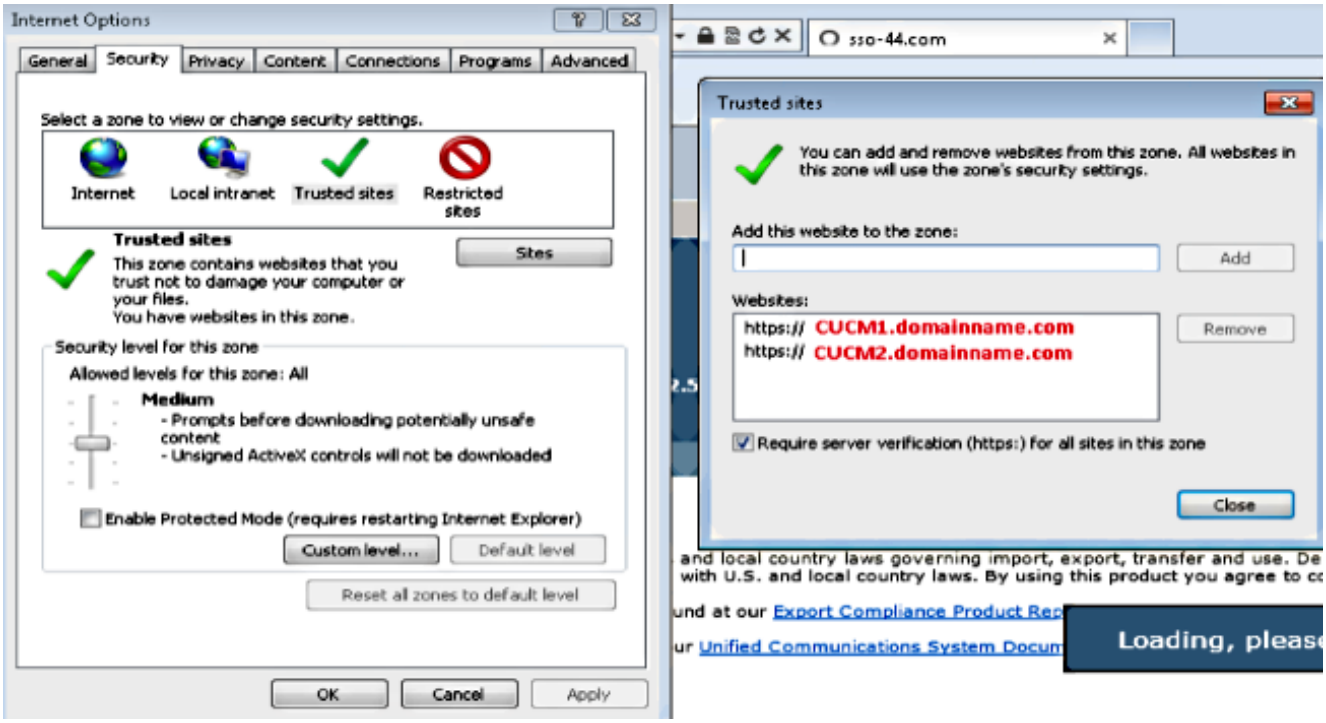
Navigieren Sie zu **Extras > Internetoptionen > Sicherheit > Lokales Intranet > Sites > Erweitert**, um die IDP-URL (Intrusion Detection & Prevention) zu lokalen Intranet-Sites hinzuzufügen.

Hinweis: Aktivieren Sie alle Kontrollkästchen im Dialogfeld Lokales Intranet, und klicken Sie auf die **Registerkarte Erweitert**.



Navigieren Sie zu **Extras > Sicherheit > Vertrauenswürdige Sites > Sites**, um die CUCM-

Hostnamen vertrauenswürdigen Sites hinzuzufügen:



Überprüfen

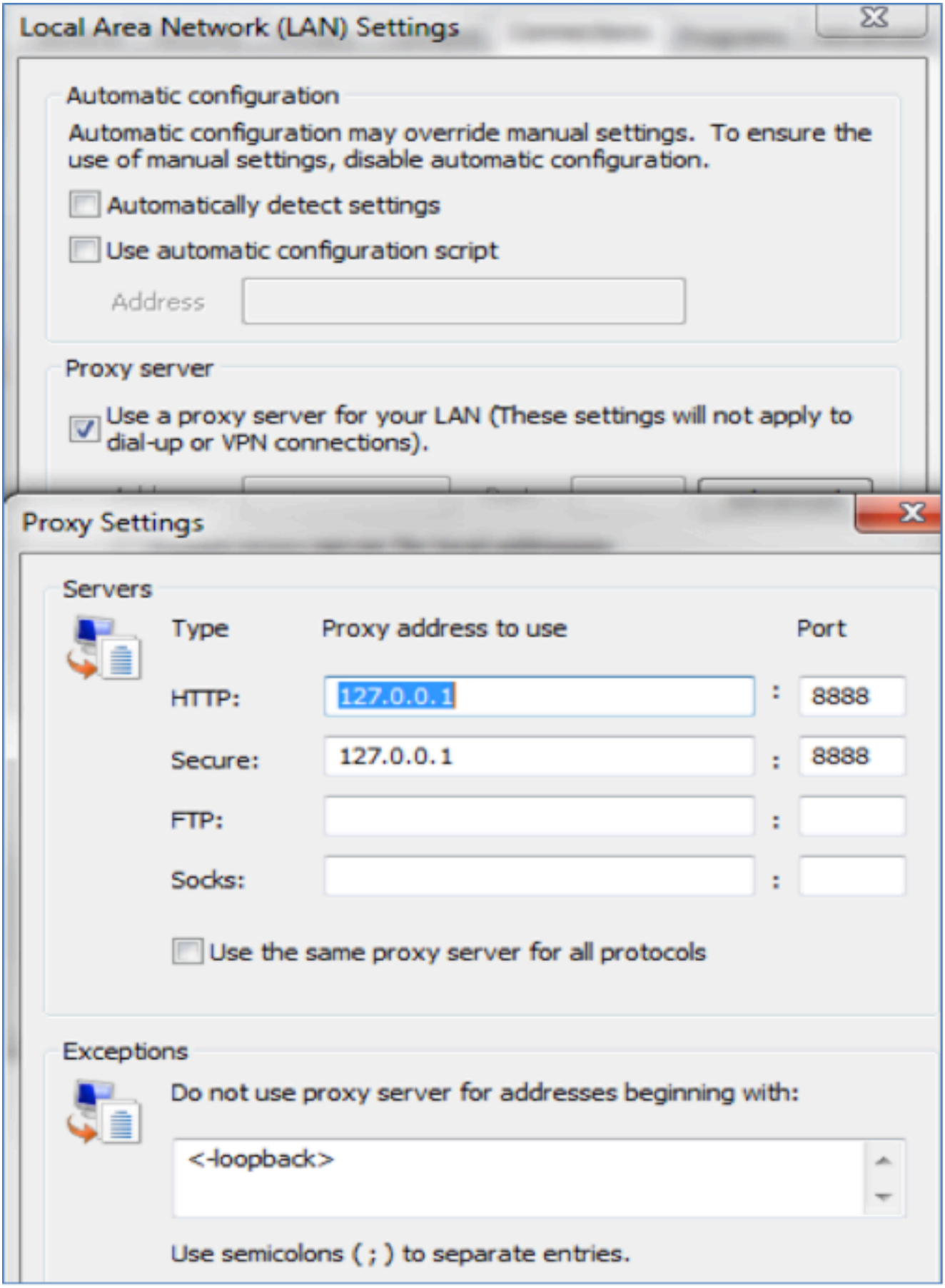
In diesem Abschnitt wird erläutert, wie Sie überprüfen, welche Authentifizierung (Kerberos- oder NT LAN Manager-(NTLM-)Authentifizierung) verwendet wird.

1. Laden Sie das Tool "Ordner" auf Ihren Client-Computer herunter und installieren Sie es.

2. Schließen Sie alle Internet Explorer-Fenster.

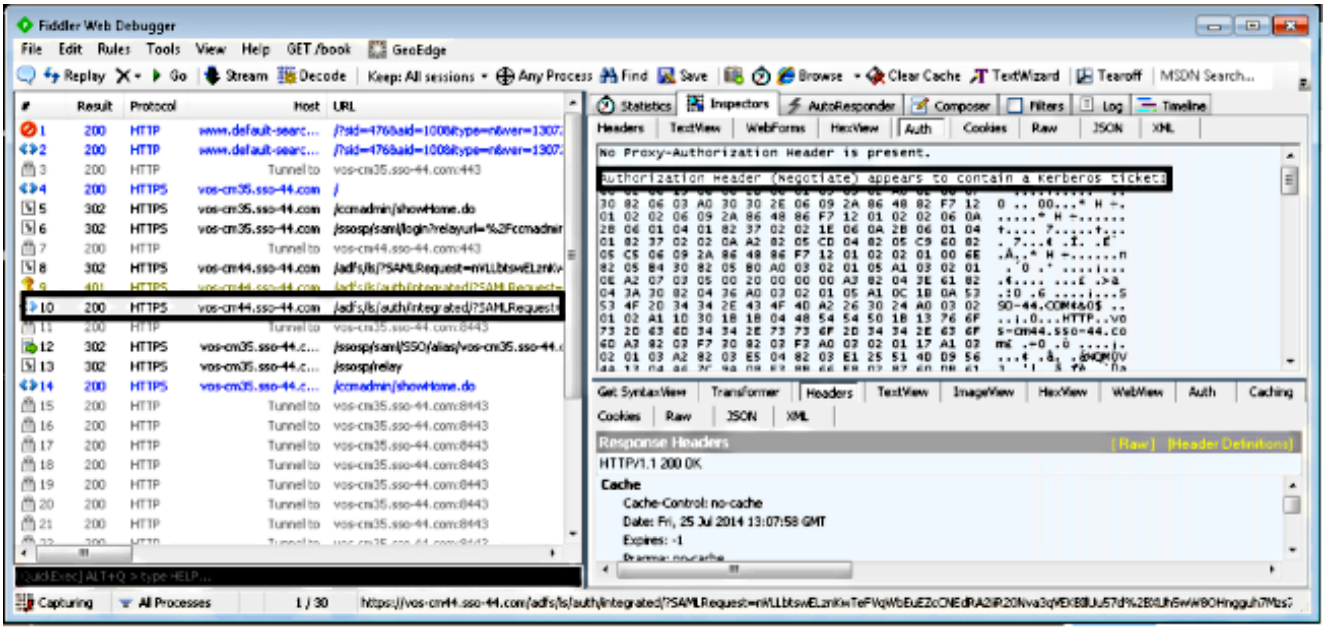
3. Führen Sie das Tool Ordner aus, und überprüfen Sie, ob die Option **Datenverkehr erfassen** im Menü Datei aktiviert ist.

   Fiddler agiert als Pass-Through-Proxy zwischen dem Client-Computer und dem Server und überwacht den gesamten Datenverkehr, der Ihre Internet Explorer-Einstellungen vorübergehend wie folgt festlegt:

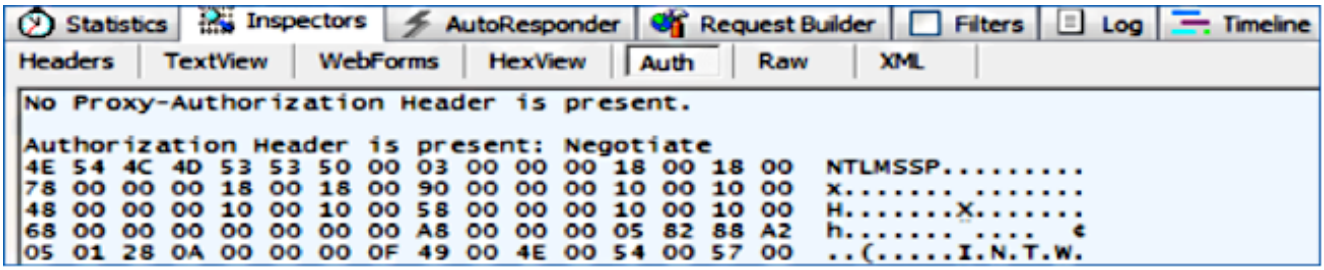


4. Öffnen Sie Internet Explorer, rufen Sie die URL des CRM-Servers (Customer Relationship Management) auf, und klicken Sie auf einige Links, um Datenverkehr zu generieren.

5. Rufen Sie das Hauptfenster der Ordner auf, und wählen Sie eines der Frames aus, in dem das Ergebnis 200 (Erfolg) lautet:



Wenn der Authentifizierungstyp NTLM ist, sehen Sie am Anfang des Frames **Negotiate - NTLMSSP**, wie hier gezeigt:



Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.