Kerberos with ADFS 2.0 for End User SAML SSO for Jabber Configuration Example

Contents

Introduction

This document describes how to configure Kerberos with Active Directory Federation Services (ADFS) 2.0.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

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.

Background Information

End User Security Assertion Markup Language (SAML) Single Sign On (SSO) configuration requires Kerberos to be configured in order to allow End User SAML SSO for Jabber to work with domain authentication. When SAML SSO is implemented with Kerberos, Lightweight Directory

Access Protocol (LDAP) handles all the authorization and user synchronization, while Kerberos manages authentication. Kerberos is an authentication protocol that is meant to be used in conjunction with an LDAP-enabled instance.

On Microsoft Windows and Macintosh machines that are joined to an Active Directory domain, users can seamlessly log into Cisco Jabber without the requirement to enter a username or password and they do not even see a login screen. Users who are not logged into the domain on their computers still see a standard login form.

Because authentication uses a single token passed from the operating systems, no redirect is required. The token is verified against the configured Key Domain Controller (KDC), and if it is valid, the user is logged in.

Configuration

Here is the procedure to configure Kerberos with ADFS 2.0.

1. Install Microsoft Windows Server 2008 R2 on a machine.

2. Install Active Directory Domain Services (ADDS) and ADFS on the same machine.

3. Install Internet Information Services (IIS) on the Microsoft Windows Server 2008 R2-installed machine.

4. Create a self-signed certificate for IIS.

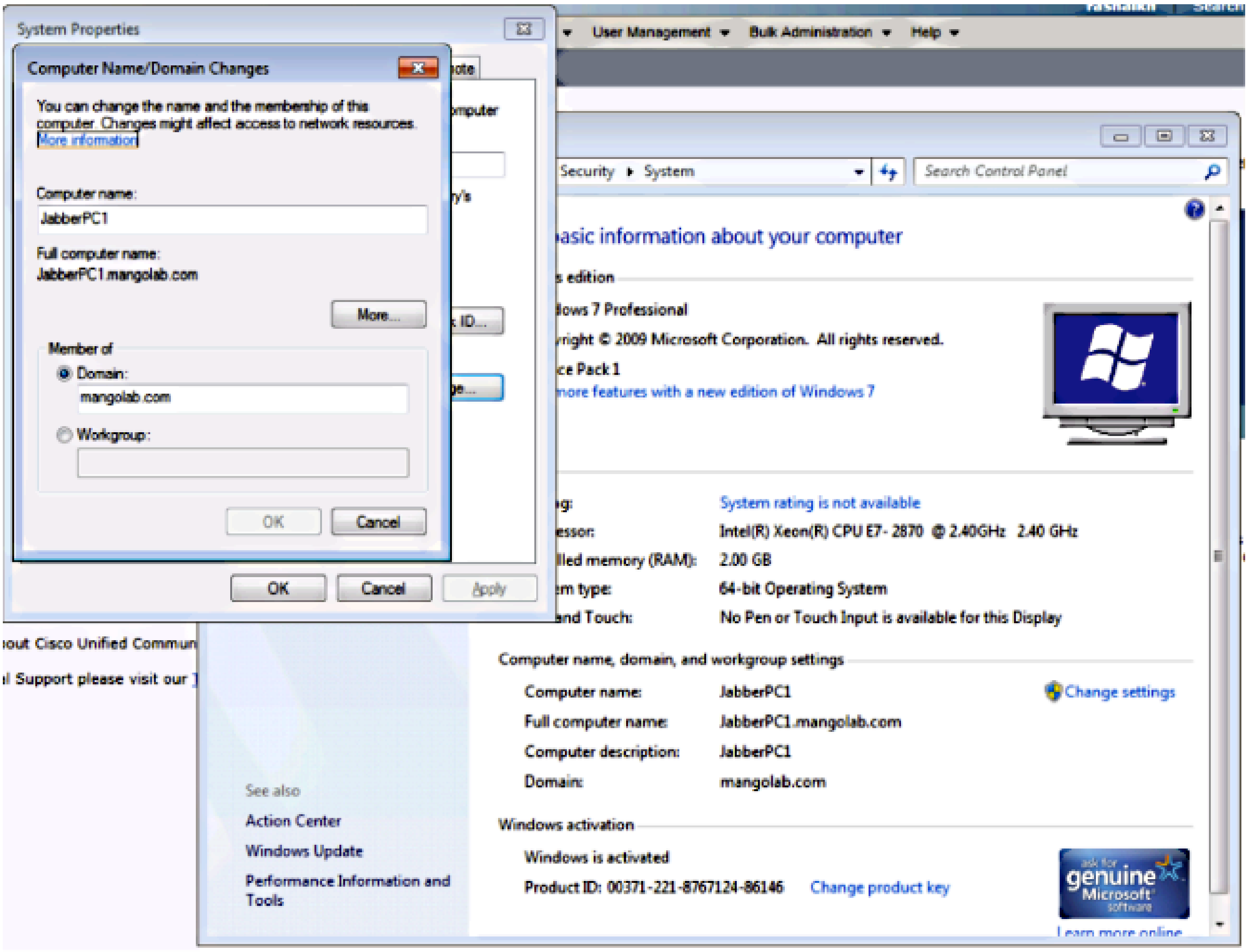
5. Import the self-signed certificate into IIS and use it as the HTTPS server certificate.

6. Install Microsoft Windows7 on another machine and use it as a client.

   Change the Domain Name Server (DNS) to the machine where you installed ADDS.

   Add this machine to the domain you created in the installation of ADDS.

   Go to **Start**.Right-click **Computer**.Click **Properties**.Click **Change Settings** on the right-hand side of window.Click the **Computer Name tab**.Click **Change**.Add the domain you created.



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources. More information

Computer name:
JabberPC1

Full computer name:
JabberPC1.mangolab.com

Member of
● Domain:
mangolab.com
○ Workgroup:

asic information about your computer

s edition
lows 7 Professional
yright © 2009 Microsoft Corporation. All rights reserved.
ce Pack 1
nore features with a new edition of Windows 7

g: System rating is not available
essor: Intel(R) Xeon(R) CPU E7- 2870 @ 2.40GHz 2.40 GHz
lled memory (RAM): 2.00 GB
m type: 64-bit Operating System
nd Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings
Computer name: JabberPC1
Full computer name: JabberPC1.mangolab.com
Computer description: JabberPC1
Domain: mangolab.com

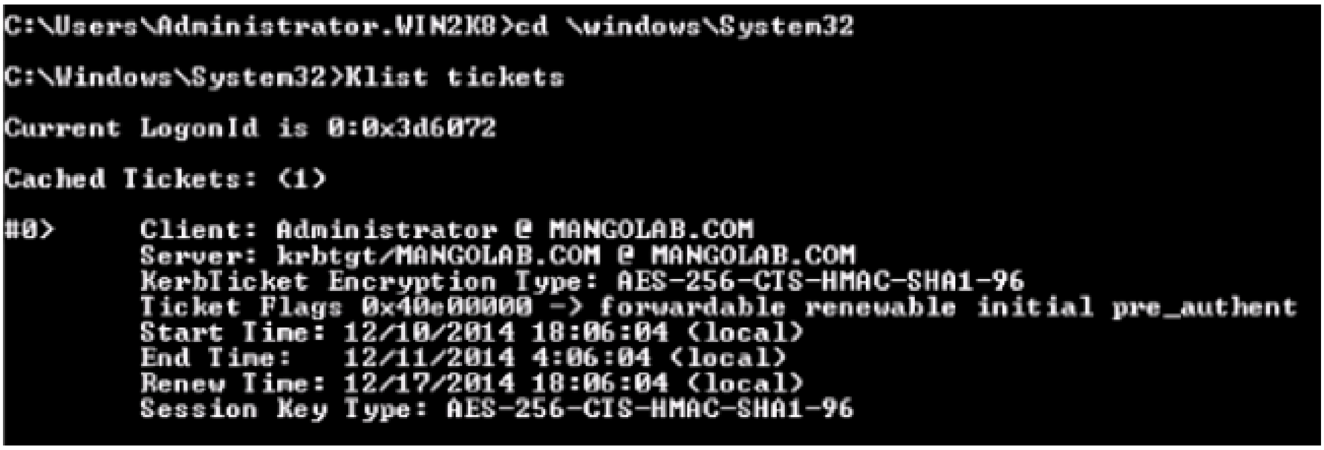
Windows activation
Windows is activated
Product ID: 00371-221-8767124-86146

out Cisco Unified Commun
l Support please visit our

7. Check whether the Kerberos service generates on both machines.

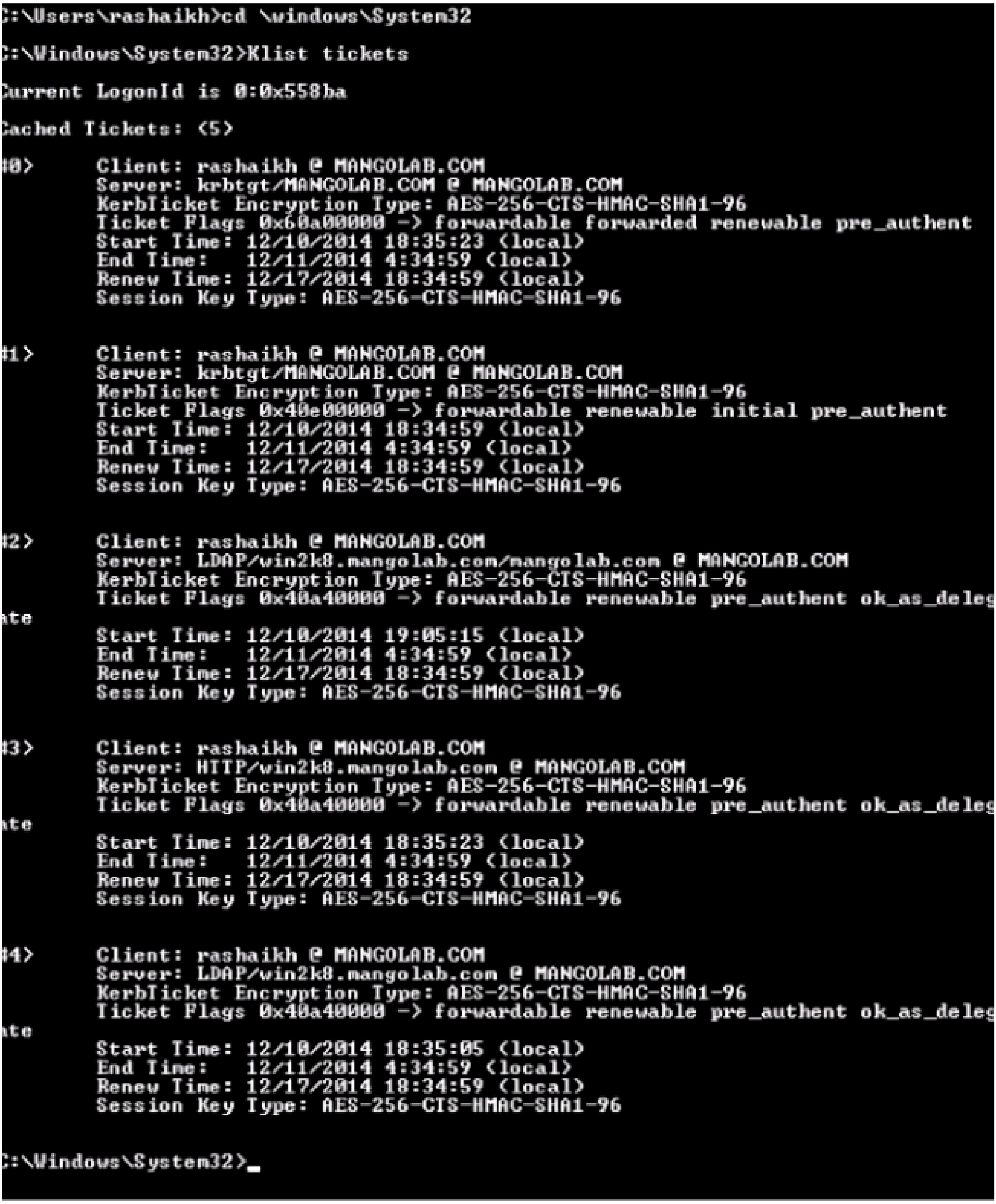
   Log in as administrator on the server machine and open the command prompt. Then execute these commands:

   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 as domain user on the client machine and execute the same commands.



```
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. Create the ADFS Kerberos identity on the machine where you installed ADDS.

   The Microsoft Windows administrator logged into the Microsoft Windows domain (as <domainname>\administrator), for example on the Microsoft Windows domain controller, creates the ADFS Kerberos identity. The ADFS HTTP service must have a Kerberos identity called a Service Principal Name (SPN) in this format: **HTTP/DNS_name_of_ADFS_server**.

   This name must be mapped to the Active Directory user that represents the ADFS HTTP server instance. Use the Microsoft Windows **setspn** utility, which should be available by default on a Microsoft Windows 2008 Server.

Procedure Register the SPNs for the ADFS server. On the Active Directory domain controller, run the **setspn** command.

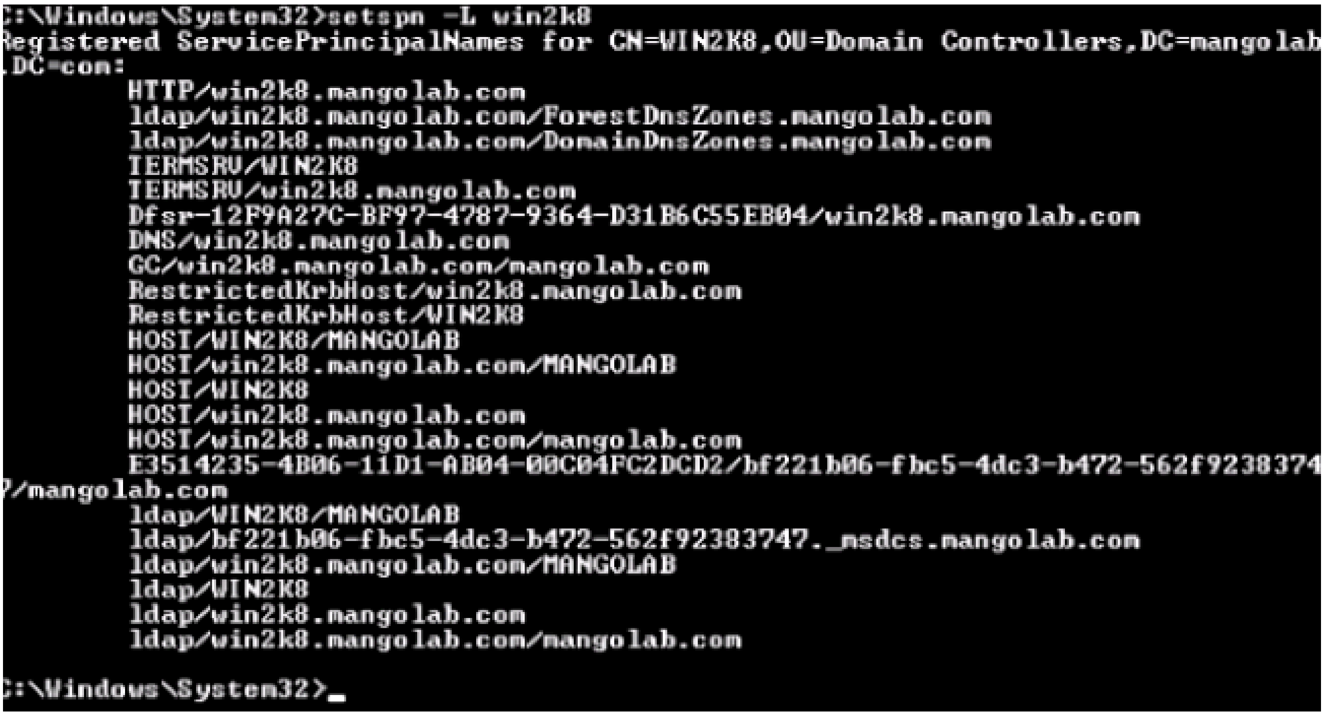
For example, when the ADFS host is **adfs01.us.renovations.com**, and the Active Directory domain is **US.RENOVATIONS.COM**, the command is:

```
 setspn -a HTTP/adfs01.us.renovations.com <ActiveDirectory user>
setspn -a HTTP/adfs01 <ActiveDirectory user>
```

The **HTTP/** portion of the SPN applies, even though the ADFS server is typically accessed by Secure Sockets Layer (SSL), which is HTTPS.

Check that the SPNs for the ADFS server are properly created with the **setspn** command and view the output.

```
setspn -L <ActiveDirectory user>
```

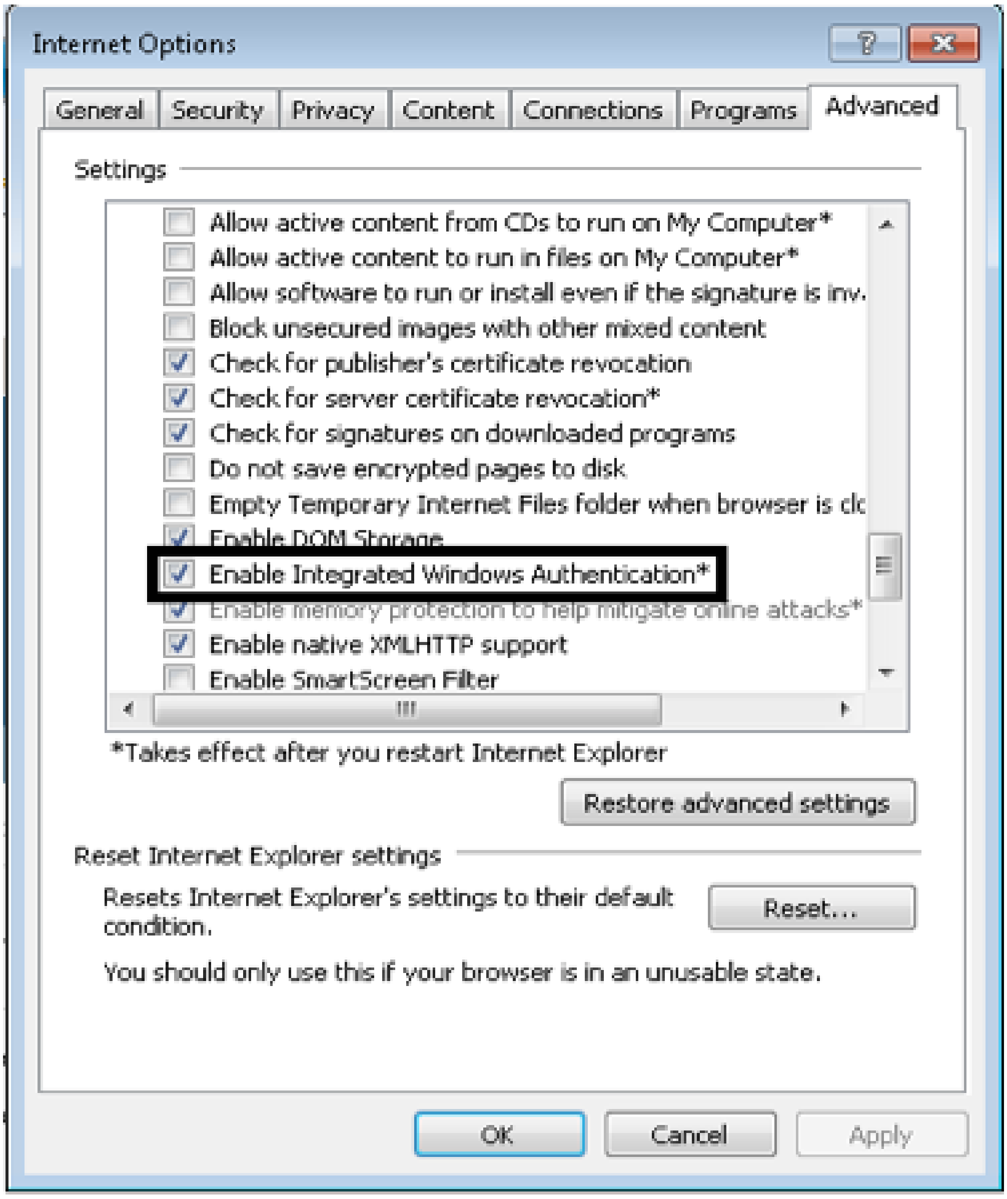


```
:\Windows\System32>setspn -L win2k8
egistered ServicePrincipalNames for CN=WIN2K8,OU=Domain Controllers,DC=mangolab
.DC=com:
        HTTP/win2k8.mangolab.com
        ldap/win2k8.mangolab.com/ForestDnsZones.mangolab.com
        ldap/win2k8.mangolab.com/DomainDnsZones.mangolab.com
        TERMSRV/WIN2K8
        TERMSRV/win2k8.mangolab.com
        Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/win2k8.mangolab.com
        DNS/win2k8.mangolab.com
        GC/win2k8.mangolab.com/mangolab.com
        RestrictedKrbHost/win2k8.mangolab.com
        RestrictedKrbHost/WIN2K8
        HOST/WIN2K8/MANGOLAB
        HOST/win2k8.mangolab.com/MANGOLAB
        HOST/WIN2K8
        HOST/win2k8.mangolab.com
        HOST/win2k8.mangolab.com/mangolab.com
        E3514235-4B06-11D1-AB04-00C04FC2DCD2/bf221b06-fbc5-4dc3-b472-562f9238374
7/mangolab.com
        ldap/WIN2K8/MANGOLAB
        ldap/bf221b06-fbc5-4dc3-b472-562f92383747._msdcs.mangolab.com
        ldap/win2k8.mangolab.com/MANGOLAB
        ldap/WIN2K8
        ldap/win2k8.mangolab.com
        ldap/win2k8.mangolab.com/mangolab.com

:\Windows\System32>_
```

9. Configure the browser settings of the Microsoft Windows Client.

   Navigate to **Tools > InternetOptions > Advanced** in order to enable Integrated Windows Authentication.

   Check the **Enable Integrated Windows Authentication check box**:



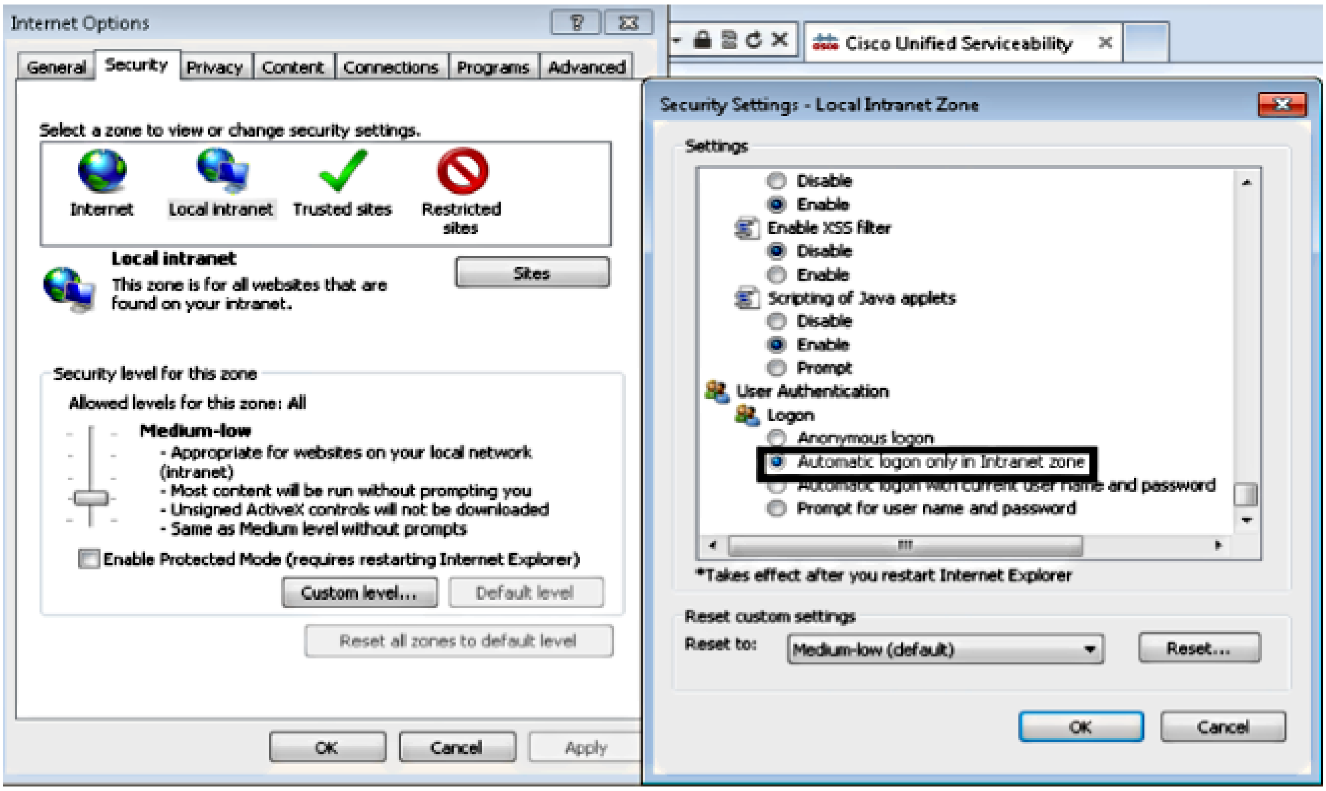
- □ Allow active content from CDs to run on My Computer*
- □ Allow active content to run in files on My Computer*
- □ Allow software to run or install even if the signature is inv.
- □ Block unsecured images with other mixed content
- ☑ Check for publisher's certificate revocation
- ☑ Check for server certificate revocation*
- ☑ Check for signatures on downloaded programs
- □ Do not save encrypted pages to disk
- □ Empty Temporary Internet Files folder when browser is clc
- ☑ Enable DOM Storage
- ☑ Enable Integrated Windows Authentication*
- ☑ Enable memory protection to help mitigate online attacks*
- ☑ Enable native XMLHTTP support
- □ Enable SmartScreen Filter

*Takes effect after you restart Internet Explorer

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

Navigate to **Tools > Internet Options > Security > Local intranet > Custom level...** in order to select **Automatic logon only in Intranet zone**.



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Restricted sites

Local intranet
This zone is for all websites that are found on your intranet.

Sites

Security level for this zone
Allowed levels for this zone: All

Medium-low
- Appropriate for websites on your local network (intranet)
- Most content will be run without prompting you
- Unsigned ActiveX controls will not be downloaded
- Same as Medium level without prompts

□ Enable Protected Mode (requires restarting Internet Explorer)

Custom level... | Default level

Reset all zones to default level

OK | Cancel | Apply

Cisco Unified Serviceability

Security Settings - Local Intranet Zone

Settings
- ○ Disable
- ● Enable
- Enable XSS filter
  - ● Disable
  - ○ Enable
- Scripting of Java applets
  - ○ Disable
  - ● Enable
  - ○ Prompt
- User Authentication
  - Logon
    - ○ Anonymous logon
    - ● Automatic logon only in Intranet zone
    - ○ Automatic logon with current user name and password
    - ○ Prompt for user name and password

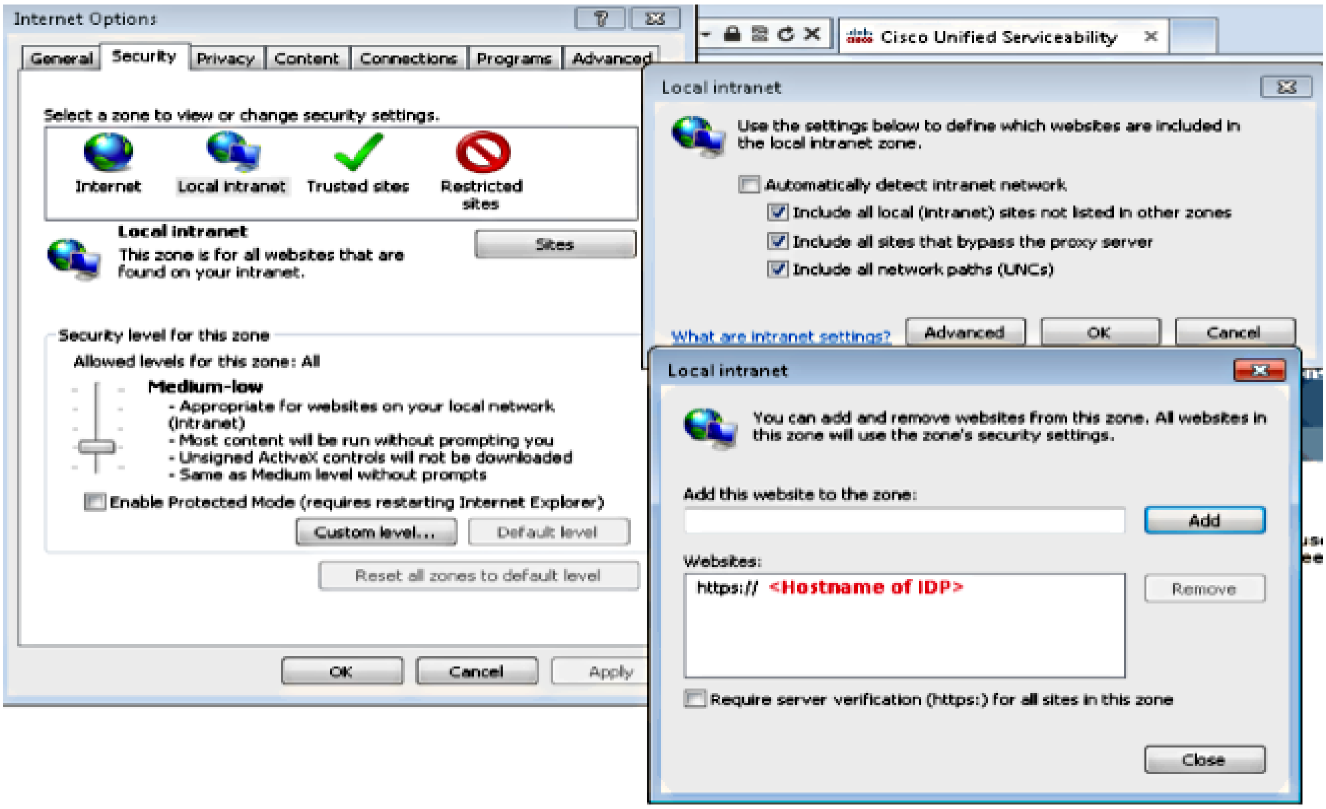
*Takes effect after you restart Internet Explorer

Reset custom settings
Reset to: Medium-low (default) | Reset...

OK | Cancel

Navigate to **Tools > Internet Options > Security > Local intranet > Sites > Advanced** in order to add the Intrusion Detection & Prevention (IDP) URL to Local intranet sites.

Note: Check all of the check boxes in the Local intranet dialog box and click the **Advanced tab**.



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Restricted sites

Local intranet
This zone is for all websites that are found on your intranet.

Sites

Security level for this zone
Allowed levels for this zone: All

Medium-low
- Appropriate for websites on your local network (intranet)
- Most content will be run without prompting you
- Unsigned ActiveX controls will not be downloaded
- Same as Medium level without prompts

□ Enable Protected Mode (requires restarting Internet Explorer)

Custom level... | Default level

Reset all zones to default level

OK | Cancel | Apply

Cisco Unified Serviceability

Local intranet

Use the settings below to define which websites are included in the local intranet zone.

□ Automatically detect intranet network
- ☑ Include all local (intranet) sites not listed in other zones
- ☑ Include all sites that bypass the proxy server
- ☑ Include all network paths (UNCs)

What are intranet settings? | Advanced | OK | Cancel

Local intranet

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

Add

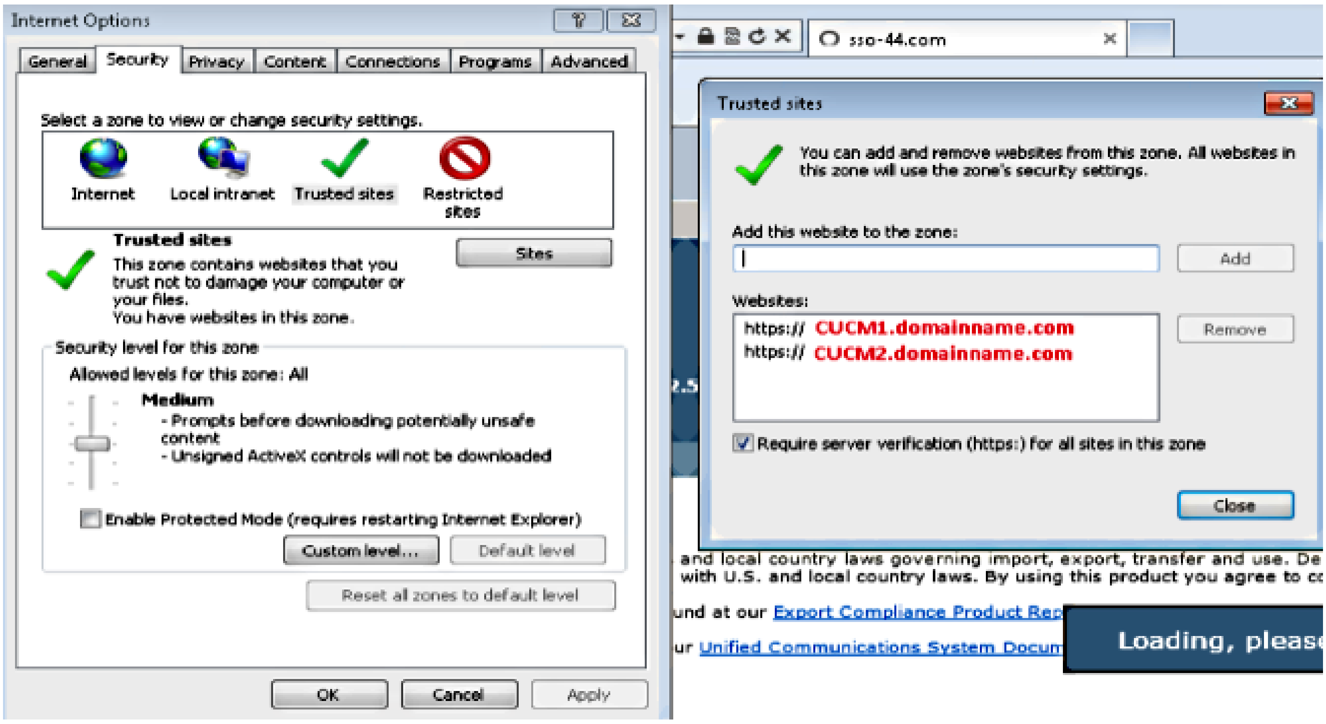
Websites:
https:// <Hostname of IDP>

Remove

□ Require server verification (https:) for all sites in this zone

Close

Navigate to **Tools > Security > Trusted sites > Sites** in order to add the CUCM hostnames to Trusted sites:



Select a zone to view or change security settings.

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.

You have websites in this zone.

Security level for this zone

Allowed levels for this zone: All

Medium

- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

□ Enable Protected Mode (requires restarting Internet Explorer)

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

Websites:

https:// CUCM1.domainname.com

https:// CUCM2.domainname.com

☑ Require server verification (https:) for all sites in this zone

and local country laws governing import, export, transfer and use. De with U.S. and local country laws. By using this product you agree to cc

und at our Export Compliance Product Rep

ur Unified Communications System Docum

Verify

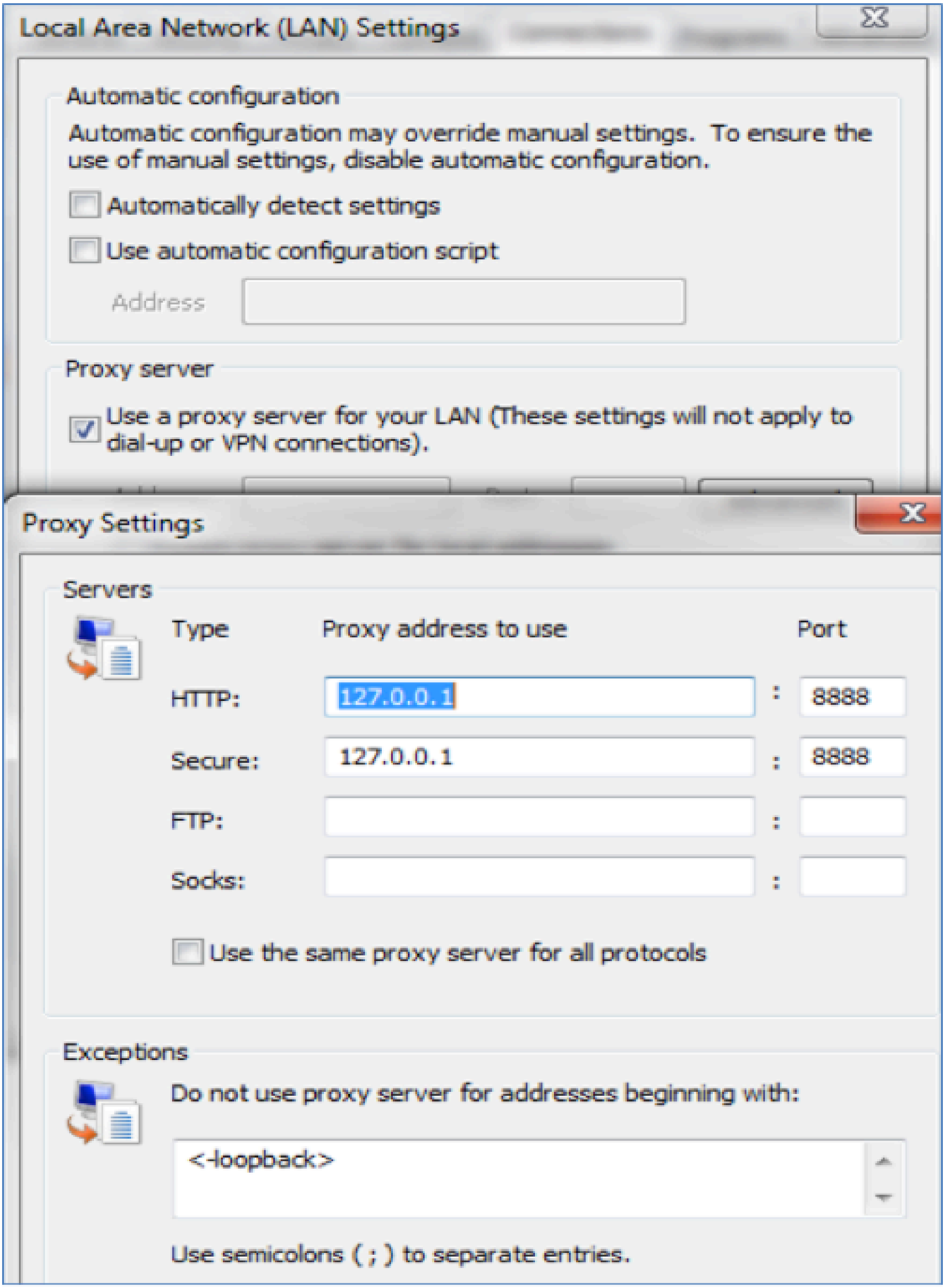
This section explains how to verify which authentication (Kerberos or NT LAN Manager (NTLM) authentication) is used.

1. Download the Fiddler Tool to your client machine and install it.

2. Close all Internet Explorer windows.

3. Run the Fiddler Tool and check that the **Capture Traffic** option is enabled under the File menu.

   Fiddler works as a pass-through proxy between the client machine and the server and listens to all traffic, which temporarily sets your Internet Explorer Settings like this:



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Proxy Settings

Servers

Type	Proxy address to use	Port
HTTP:	127.0.0.1	8888
Secure:	127.0.0.1	8888
FTP:		
Socks:		

□ Use the same proxy server for all protocols

Exceptions

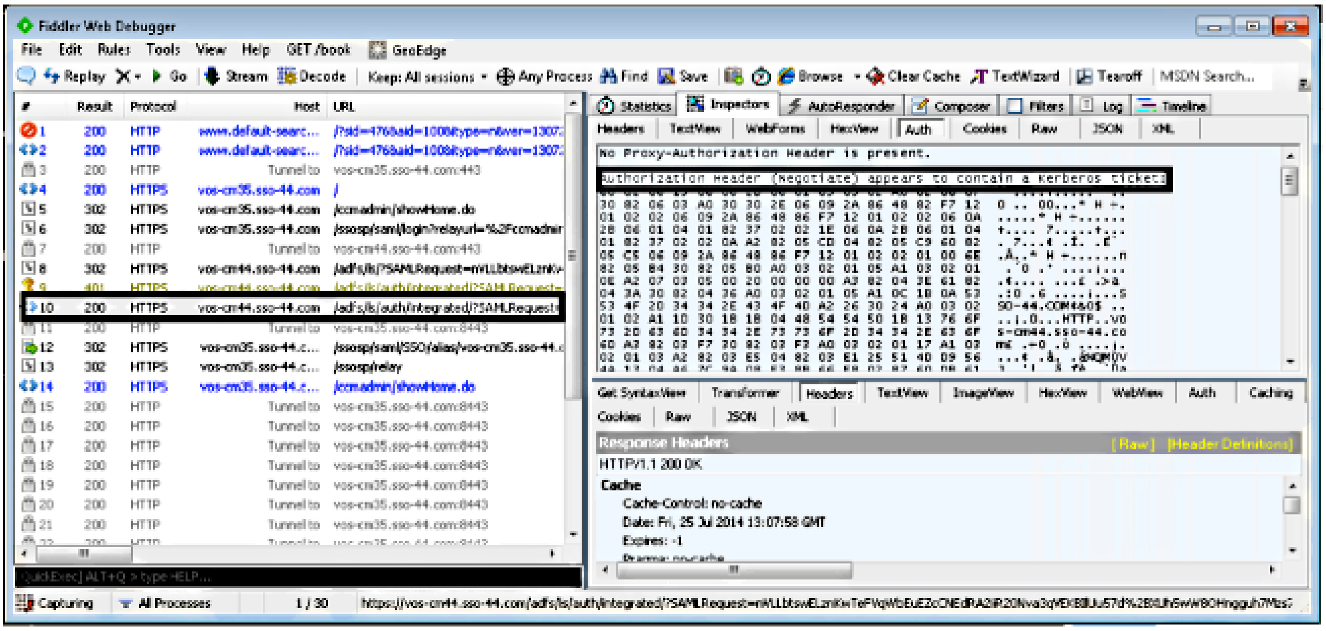
Do not use proxy server for addresses beginning with:

<-loopback>

Use semicolons (;) to separate entries.

4. Open Internet Explorer, browse into your Customer Relationship Management (CRM) Server URL, and click a few links in order to generate traffic.

5. Refer back to the Fiddler main window and choose one of the Frames where the Result is 200 (success):



Fiddler Web Debugger
File Edit Rules Tools View Help GET /book GeoEdge
Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN Search...
Statistics Inspectors AutoResponder Composer Filters Log Timeline
Headers TextView WebForms HexView Auth Cookies Raw JSON XML
Get SyntaxView Transformer Headers TextView ImageView HexView WebView Auth Caching
Cookies Raw JSON XML
[QuickExec] ALT+Q > type HELP...
Capturing All Processes 1 / 30

#	Result	Protocol	Host	URL
1	200	HTTP	www.default-searc...	/?sid=476&aid=100&itype=n&ver=1307
2	200	HTTP	www.default-searc...	/?sid=476&aid=100&itype=n&ver=1307
3	200	HTTP	Tunnel to	vos-cm35.sso-44.com:443
4	200	HTTPS	vos-cm35.sso-44.com	/
5	302	HTTPS	vos-cm35.sso-44.com	/ccmadmin/showHome.do
6	302	HTTPS	vos-cm35.sso-44.com	/ssosp/saml/login?relayurl=%2Fccmadmin
7	200	HTTP	Tunnel to	vos-cm44.sso-44.com:443
8	302	HTTPS	vos-cm44.sso-44.com	/adfs/ls/?SAMLRequest=nVLLbtswELznKv
9	401	HTTPS	vos-cm44.sso-44.com	/adfs/ls/auth/integrated/?SAMLRequest=
10	200	HTTPS	vos-cm44.sso-44.com	/adfs/ls/auth/integrated/?SAMLRequest=
11	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443
12	302	HTTPS	vos-cm35.sso-44.c...	/ssosp/saml/SSO/alias/vos-cm35.sso-44.c
13	302	HTTPS	vos-cm35.sso-44.c...	/ssosp/relay
14	200	HTTPS	vos-cm35.sso-44.c...	/ccmadmin/showHome.do
15	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443
16	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443
17	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443
18	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443
19	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443
20	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443
21	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443

```
No Proxy-Authorization Header is present.

Authorization Header (Negotiate) appears to contain a Kerberos ticket:
30 82 06 03 A0 30 30 2E 06 09 2A 86 48 82 F7 12   0 .. 00...* H ÷.
01 02 02 06 09 2A 86 48 86 F7 12 01 02 02 06 0A   .....* H ÷......
2B 06 01 04 01 82 37 02 02 1E 06 0A 2B 06 01 04   +.... 7.....+...
01 82 37 02 02 0A A2 82 05 CD 04 82 05 C9 60 82   . 7...¢ .Í. .É`
05 C5 06 09 2A 86 48 86 F7 12 01 02 02 01 00 6E   .Å..* H ÷......n
82 05 B4 30 82 05 B0 A0 03 02 01 05 A1 03 02 01    . ´0 .° .....¡...
0E A2 07 03 05 00 20 00 00 00 A3 82 04 3E 61 82   .¢.... ...£ .>a
04 3A 30 82 04 36 A0 03 02 01 05 A1 0C 1B 0A 53   .:0 .6 .....¡...S
53 4F 2D 34 34 2E 43 4F 4D A2 26 30 24 A0 03 02   SO-44.COM¢&0$ ..
01 02 A1 1D 30 1B 1B 04 48 54 54 50 1B 13 76 6F   ..¡.0...HTTP..vo
73 2D 63 6D 34 34 2E 73 73 6F 2D 34 34 2E 63 6F   s-cm44.sso-44.co
6D A3 82 03 F7 30 82 03 F3 A0 03 02 01 17 A1 03   m£ .÷0 .ó .....¡.
02 01 03 A2 82 03 E5 04 82 03 E1 25 51 4D D9 56   ...¢ .å. .á%QMÙV
```

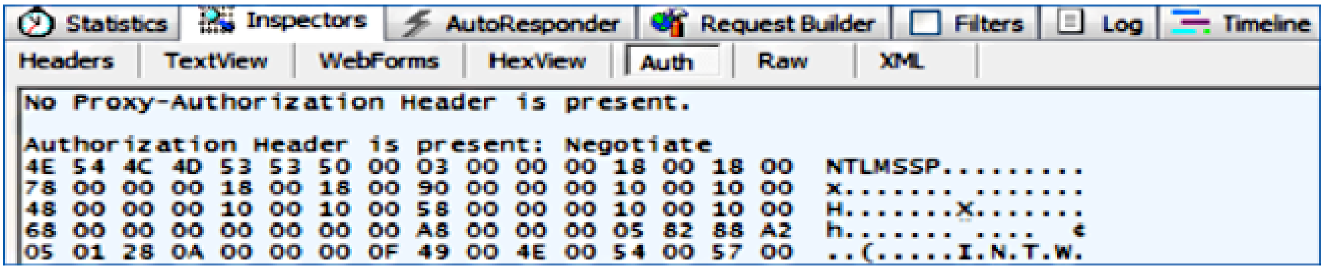
Response Headers [Raw] [Header Definitions]

HTTP/1.1 200 OK

Cache
Cache-Control: no-cache
Date: Fri, 25 Jul 2014 13:07:58 GMT
Expires: -1
Pragma: no-cache

https://vos-cm44.sso-44.com/adfs/ls/auth/integrated/?SAMLRequest=nVLLbtswELznKwTeFVqWbEuEZoCNEdRA2iR20Nva3qVEKBIUu57d%2BXUhSwWBOHngguh7Mzs?

If the Authentication type is NTLM, then you see **Negotiate - NTLMSSP** in the beginning of the frame, as shown here:



```
No Proxy-Authorization Header is present.

Authorization Header is present: Negotiate
4E 54 4C 4D 53 53 50 00 03 00 00 00 18 00 18 00   NTLMSSP.........
78 00 00 00 18 00 18 00 90 00 00 00 10 00 10 00   x....... .......
48 00 00 00 10 00 10 00 58 00 00 00 10 00 10 00   H.......X.......
68 00 00 00 00 00 00 00 A8 00 00 00 05 82 88 A2   h.......  ....  ¢
05 01 28 0A 00 00 00 0F 49 00 4E 00 54 00 57 00   ..(.....I.N.T.W.
```

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.