Kerberos with ADFS 2.0 for End User SAML SSO for Jabber配置示例

目錄

簡介

本文說明如何使用Active Directory聯合身份驗證服務(ADFS)2.0配置Kerberos。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

終端使用者安全斷言標籤語言(SAML)單一登入(SSO)配置要求配置Kerberos，以允許用於Jabber的終端使用者SAML SSO使用域身份驗證。當使用Kerberos實現SAML SSO時，輕量目錄訪問協定(LDAP)處理所有授權和使用者同步，而Kerberos管理身份驗證。Kerberos是一種身份驗證協定，旨在與啟用LDAP的例項結合使用。

在加入Active Directory域的Microsoft Windows和Macintosh電腦上，使用者無需輸入使用者名稱或密碼即可無縫登入到Cisco Jabber，甚至看不到登入螢幕。未登入其電腦上的域的使用者仍會看到標準登入表單。

由於身份驗證使用從作業系統傳遞的單個令牌，因此不需要重定向。權杖會根據已設定的金鑰網域控制器(KDC)進行驗證，如果權杖有效，使用者就會登入。

組態

以下是使用ADFS 2.0設定Kerberos的程式。

1. 在電腦上安裝Microsoft Windows Server 2008 R2。

2. 在同一台電腦上安裝Active Directory域服務(ADDS)和ADFS。

3. 在安裝了Microsoft Windows Server 2008 R2的電腦上安裝Internet Information Services(IIS)。

4. 為IIS建立自簽名證書。

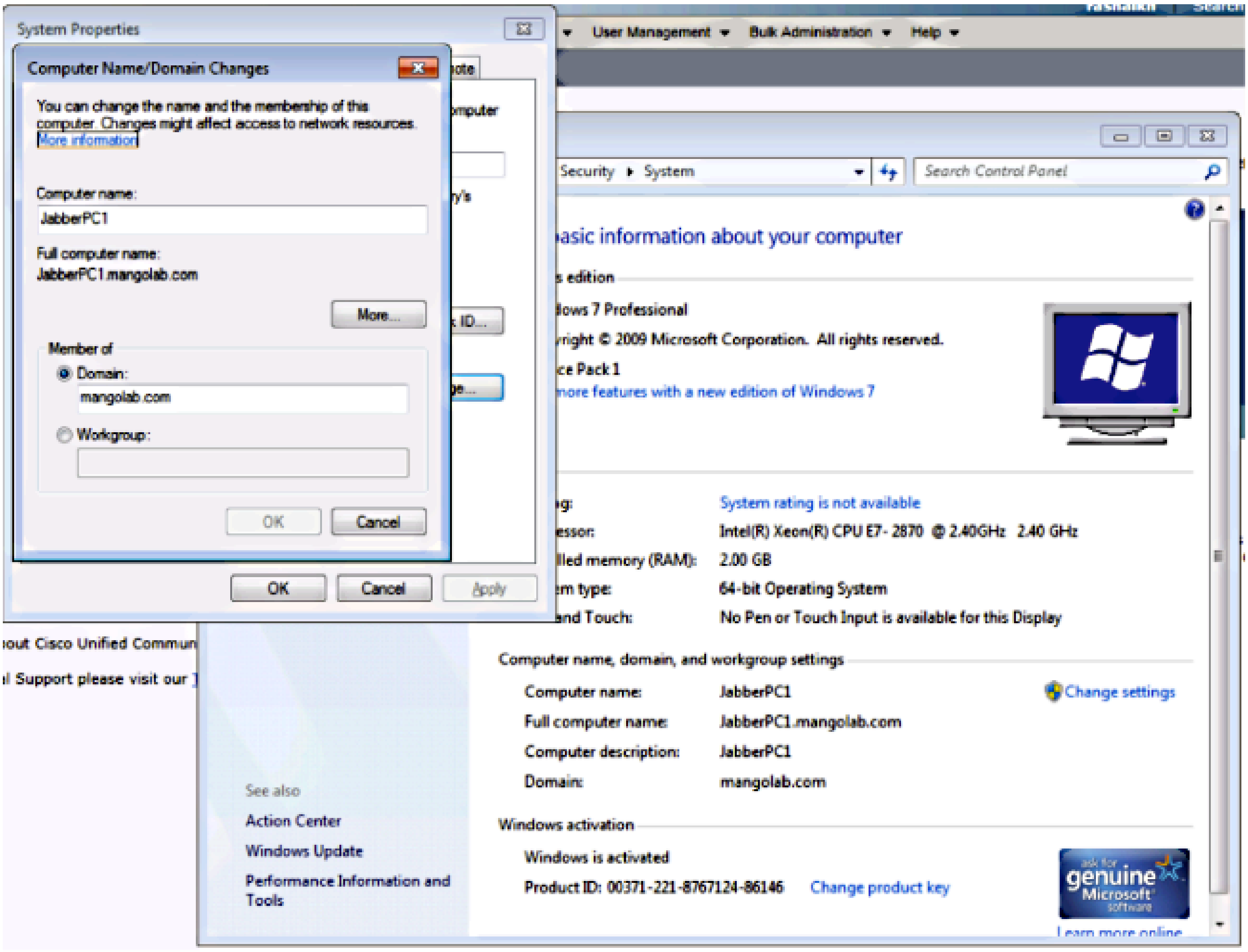
5. 將自簽名證書匯入IIS並將其用作HTTPS伺服器證書。

6. 在其他電腦上安裝Microsoft Windows7，並將其用作客戶端。

   將域名伺服器(DNS)更改為安裝了ADDS的電腦。

   將此電腦新增到在安裝ADDS時建立的域。

   轉至**開始**。按一下右鍵**Computer**。按一下「**Properties**」。按一下視窗右側的**Change Settings**。按一下**Computer Name**頁籤。按一下「**Change**」。新增您建立的域。



System Properties

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
right © 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

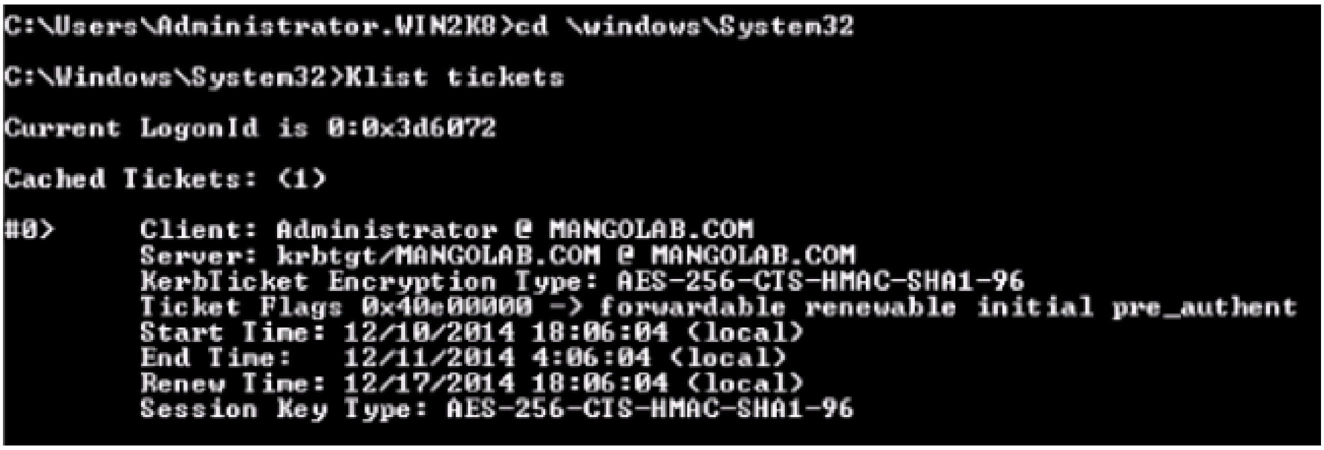
Computer name, domain, and workgroup settings
Computer name: JabberPC1
Full computer name: JabberPC1.mangolab.com
Computer description: JabberPC1
Domain: mangolab.com

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

7. 檢查Kerberos服務是否在這兩個電腦上生成。

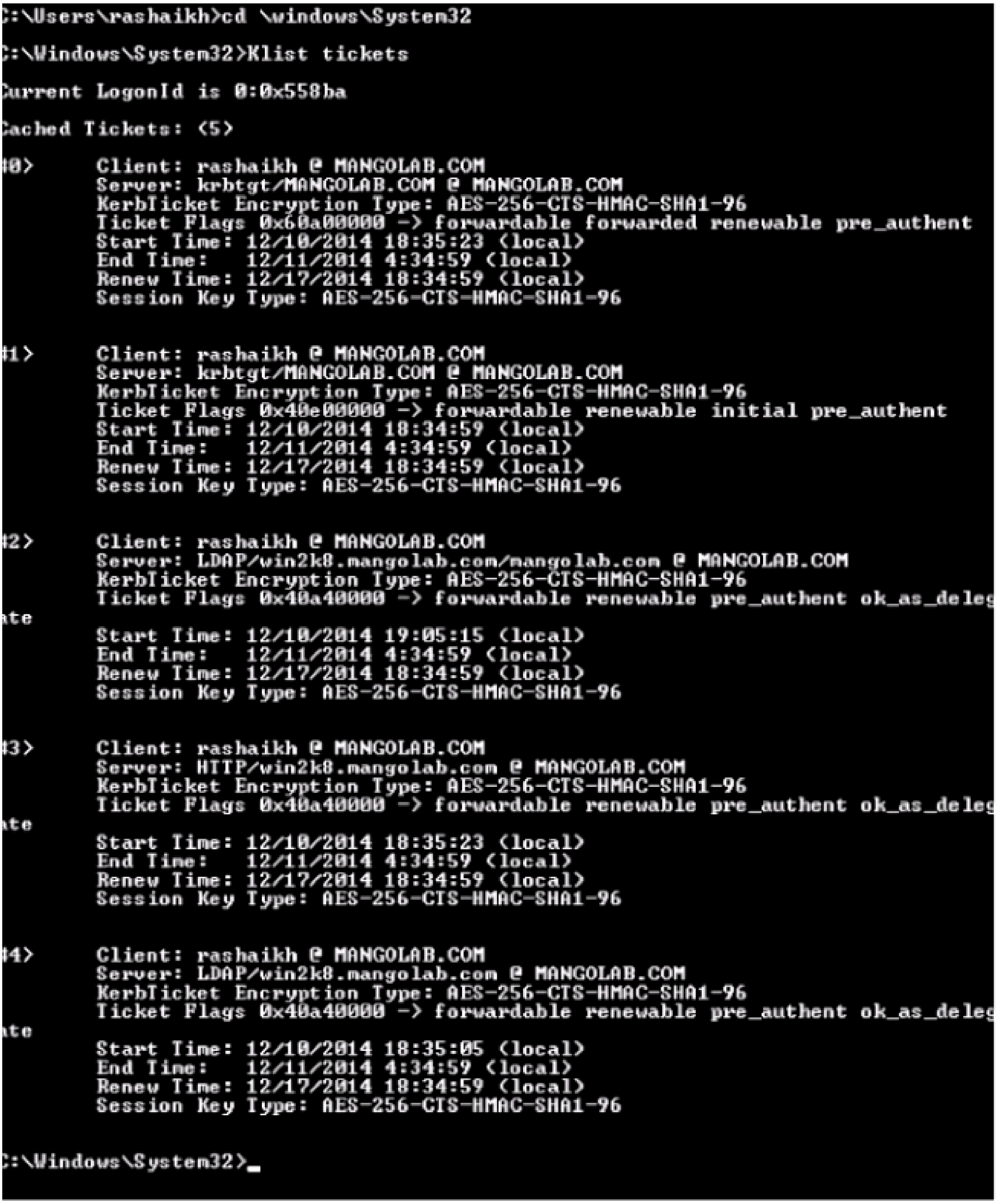
以管理員身份登入到伺服器電腦並開啟命令提示符。然後執行以下命令：

cd \windows\System32Klist票證



```
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
```

以域使用者身份登入到客戶端電腦並執行相同的命令。



```
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. 在安裝ADDS的電腦上建立ADFS Kerberos標識。

   Microsoft Windows管理員登入到Microsoft Windows域（例如，以<domainname>\administrator身份）在Microsoft Windows域控制器上建立ADFS Kerberos標識。ADFS HTTP服務必須具有稱為服務主體名稱(SPN)的Kerberos標識，格式如下：**HTTP/DNS_name_of_ADFS_server**。

   此名稱必須對映到表示ADFS HTTP伺服器例項的Active Directory使用者。使用Microsoft Windows **setspn**實用程式，該實用程式預設情況下應在Microsoft Windows 2008 Server上可

用。

程式 註冊ADFS伺服器的SPN。在Active Directory域控制器上，運行**setspn**命令。

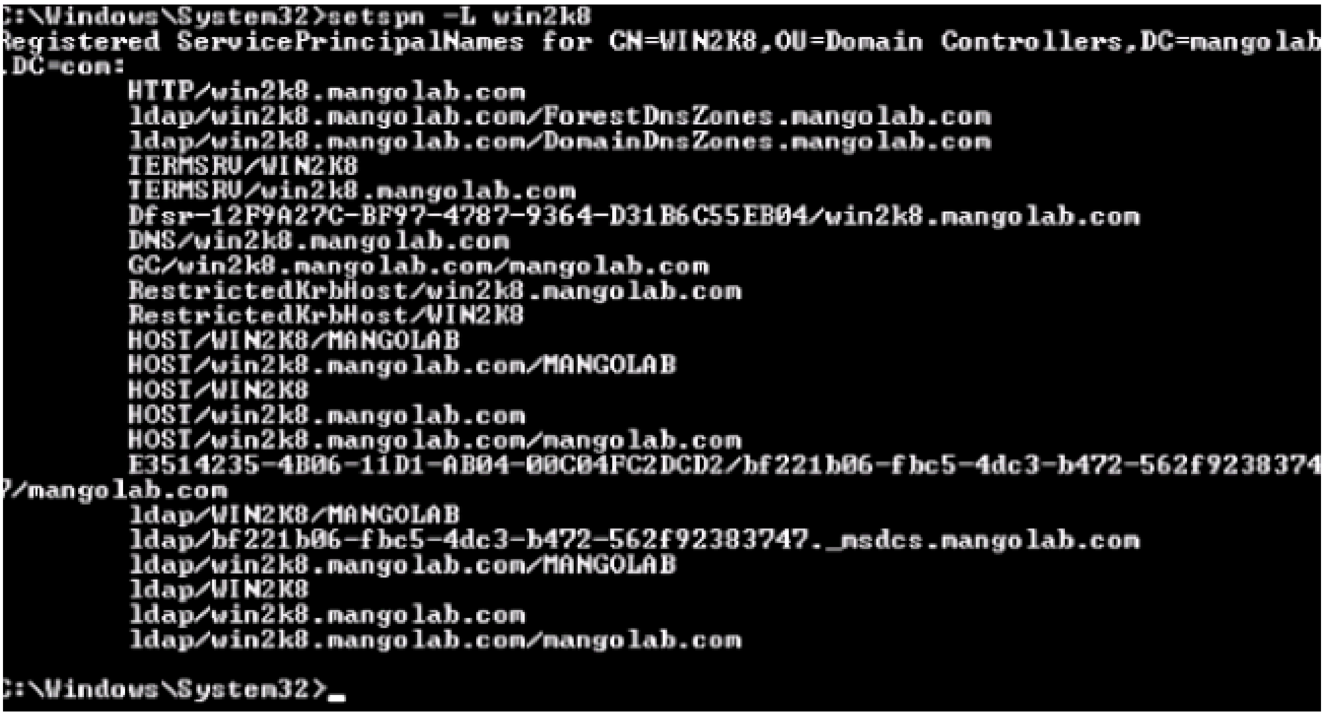
例如，當ADFS主機為**adfs01.us.renovations.com**，而Active Directory域為**US.RENOVATIONS.COM**時，命令為：

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

SPN的**HTTP/**部分適用，即使ADFS伺服器通常由安全套接字層(SSL)（即HTTPS）訪問。

使用**setspn**命令檢查ADFS伺服器的SPN是否正確建立，並檢視輸出。

```
setspn -L
```

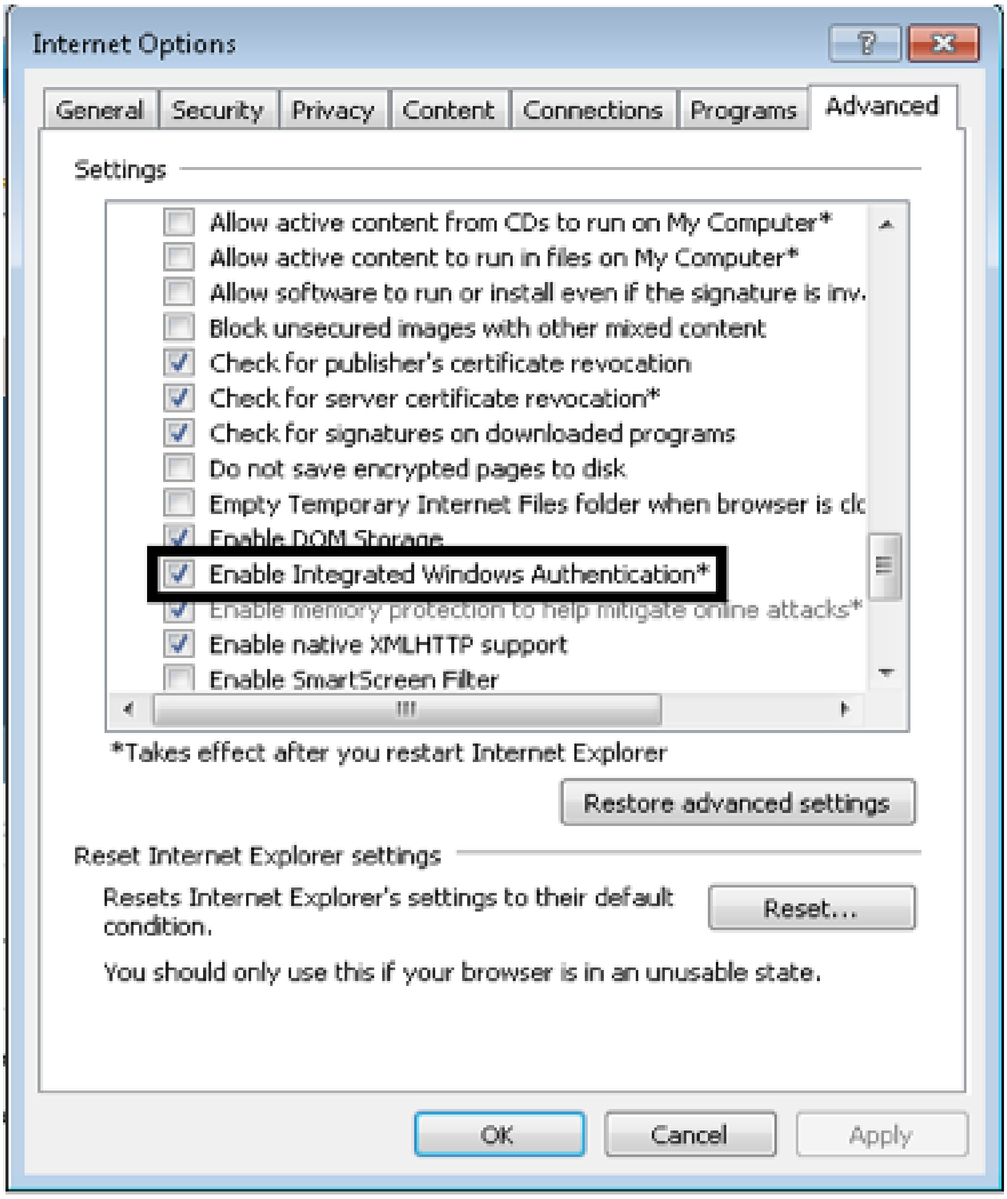


```
C:\Windows\System32>setspn -L win2k8
Registered ServicePrincipalNames for CN=WIN2K8,OU=Domain Controllers,DC=mangolab
.DC=com:
        HTTP/win2k8.mangolab.com
        ldap/win2k8.mangolab.com/ForestDnsZones.mangolab.com
        ldap/win2k8.mangolab.com/DomainDnsZones.mangolab.com
        TERMSRV/WIN2K8
        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

C:\Windows\System32>_
```

9. 配置Microsoft Windows客戶端的瀏覽器設定。

導航到**工具> Internet選項>高級**以啟用整合的Windows身份驗證。

選中Enable Integrated Windows Authentication覈取方塊:



Internet Options

Settings

- ☐ 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

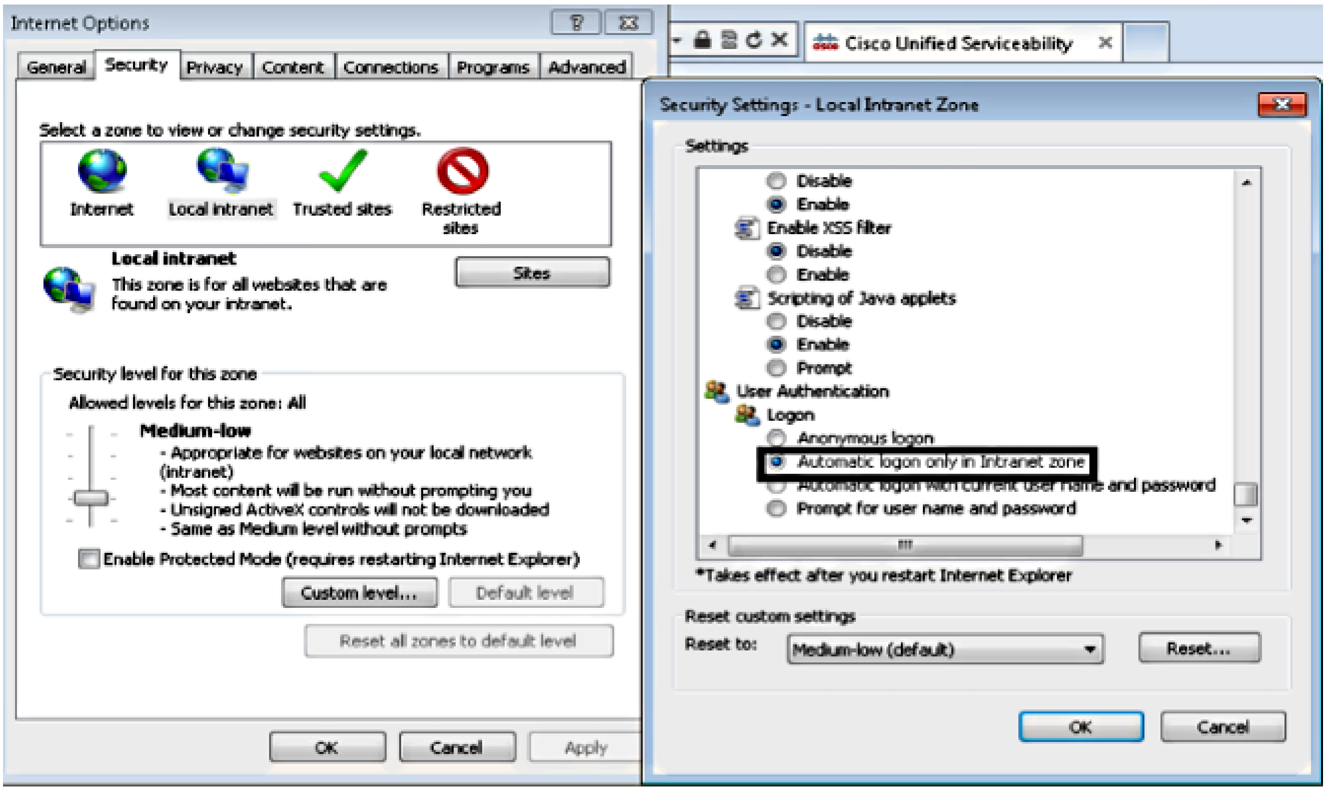
*Takes effect after you restart Internet Explorer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

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

導航到工具> Internet選項>安全>本地Intranet >自定義級別……以選擇僅在Intranet區域中自動登入。



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

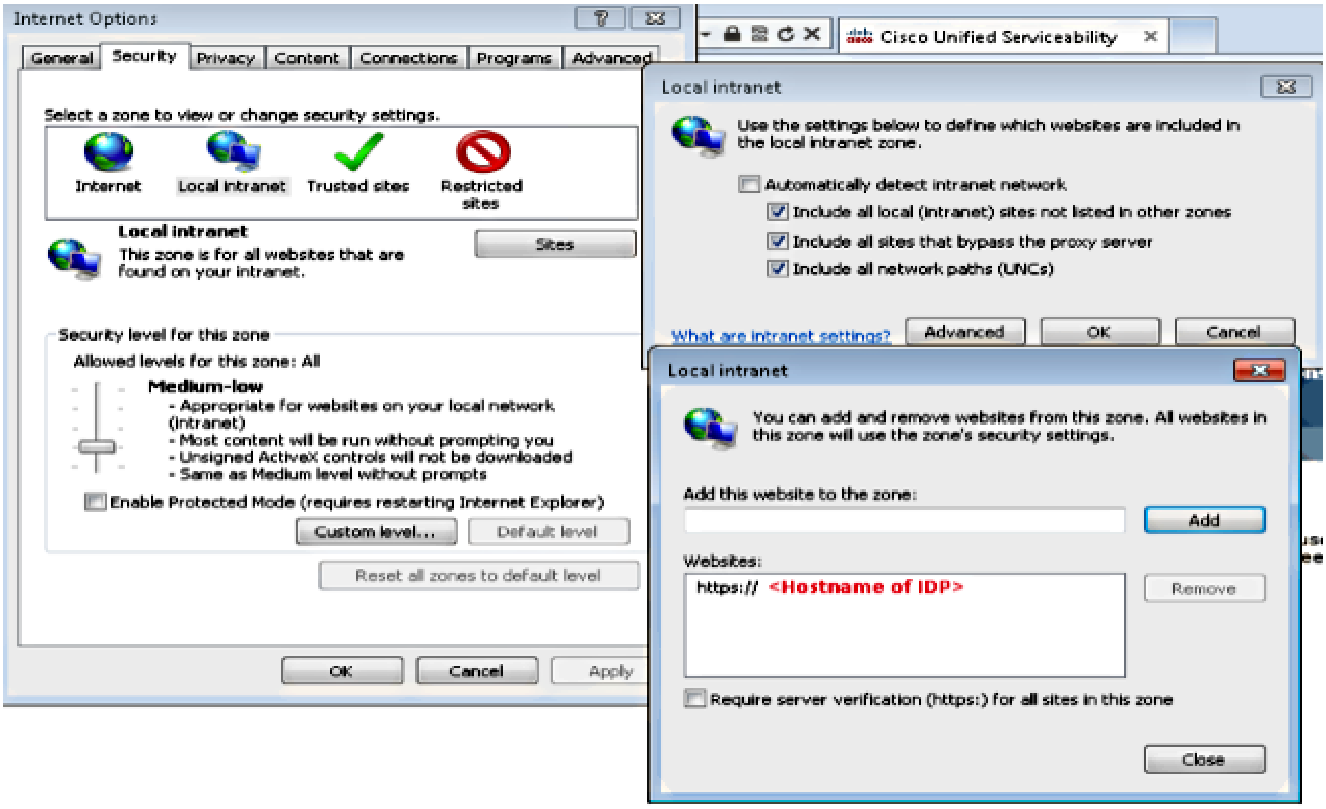
*Takes effect after you restart Internet Explorer

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

OK | Cancel

導覽至**Tools > Internet Options > Security > Local intranet > Sites > Advanced**，以便將Intrusion Detection & Prevention(IDP)URL新增到Local intranet站點。

附註：選中Local intranet對話方塊中的所有覈取方塊，然後按一下**Advanced**頁籤。



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

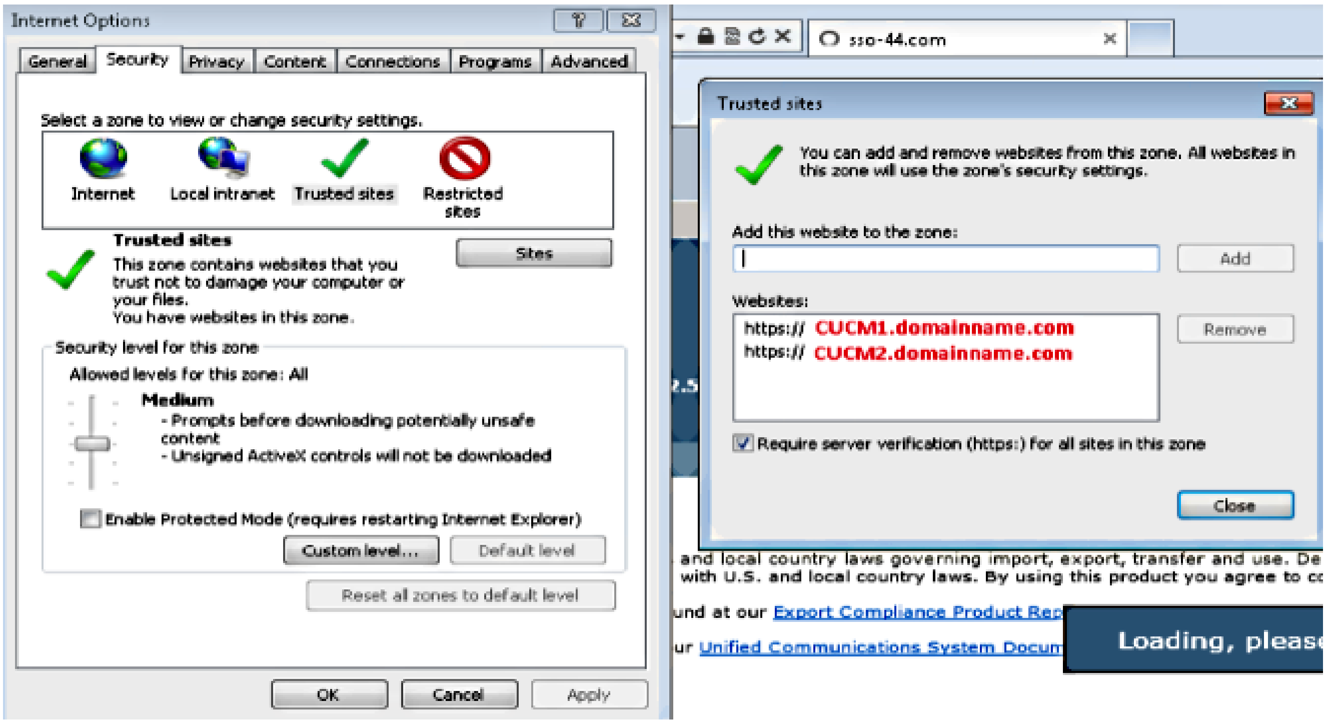
Websites:
https:// <Hostname of IDP>

Remove

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

Close

導航到**Tools > Security > Trusted sites > Sites**，將CUCM主機名新增到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 co

und at our Export Compliance Product Rep

ur Unified Communications System Docum

驗證

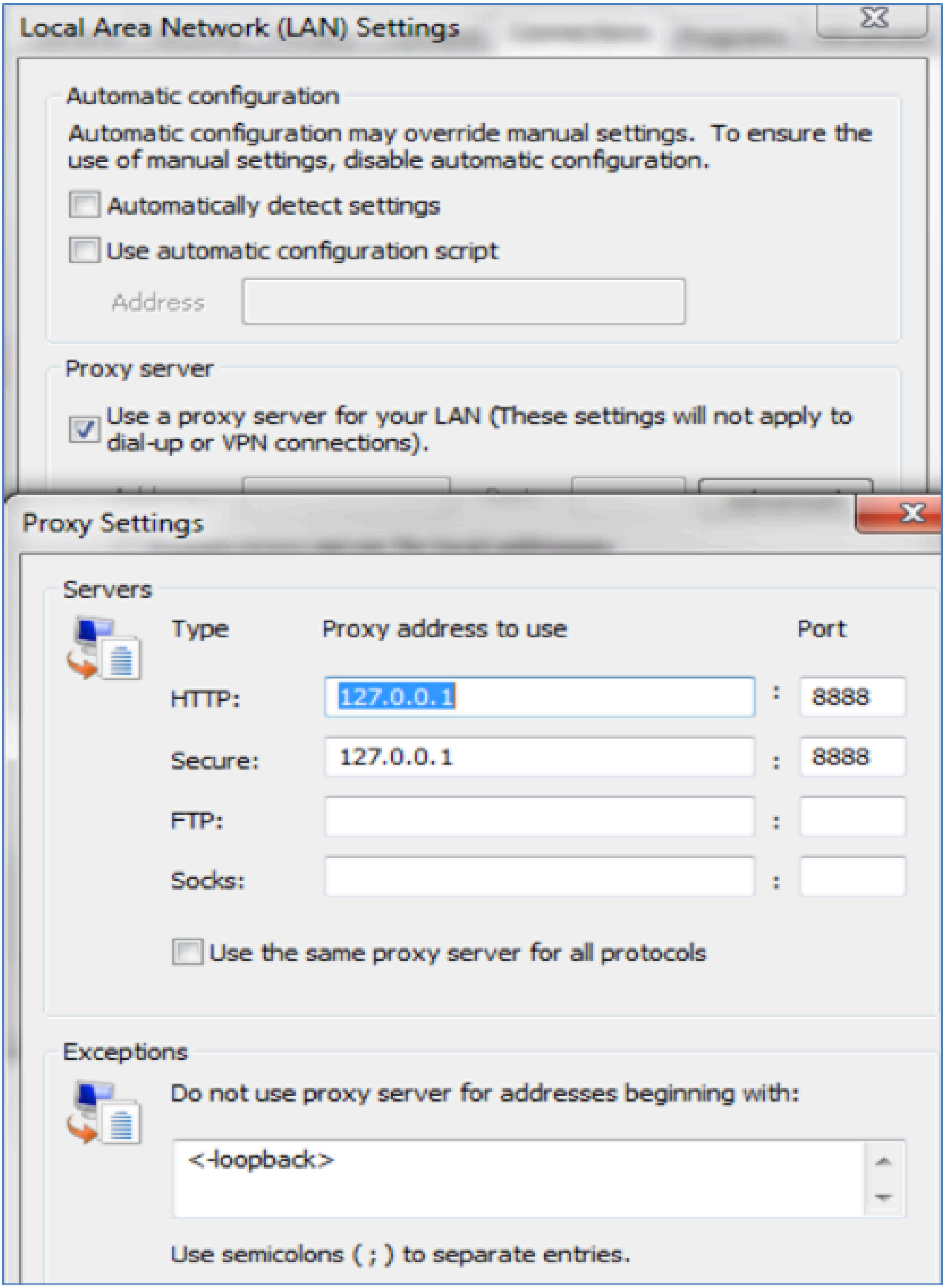
本節介紹如何驗證使用了哪些身份驗證(Kerberos或NT LAN Manager(NTLM)身份驗證)。

1. 將Fiddler Tool下載到客戶端電腦並進行安裝。

2. 關閉所有Internet Explorer視窗。

3. 運行Fiddler工具，並檢查「檔案」選單下是否啟用了**Capture Traffic**選項。

   Fiddler充當客戶端電腦和伺服器之間的傳遞代理，並偵聽所有流量，這將臨時設定您的Internet Explorer設定，如下所示：



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

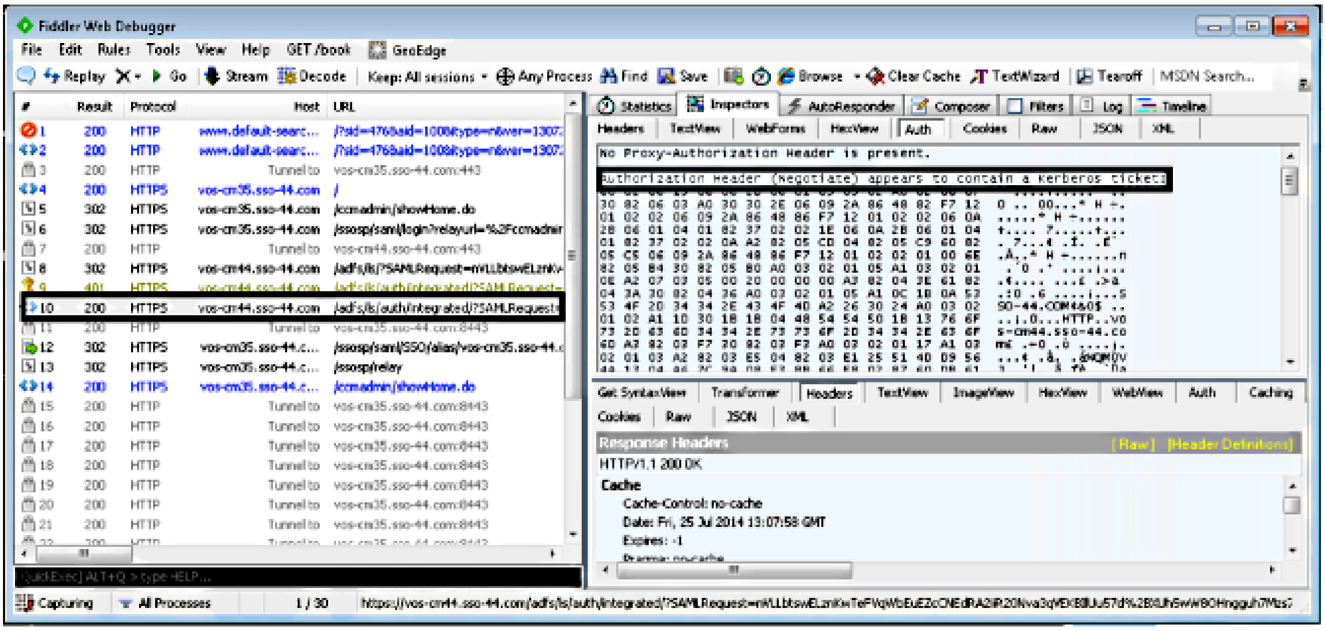
Do not use proxy server for addresses beginning with:

<-loopback>

Use semicolons (;) to separate entries.

4. 開啟Internet Explorer，瀏覽到Customer Relationship Management(CRM)伺服器URL，然後按一下幾個連結以生成流量。

5. 返回Fiddler主視窗，選擇結果為200（成功）的幀之一：



#	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 40 09 56  ...¢ .å. .á%Q@.V
```

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

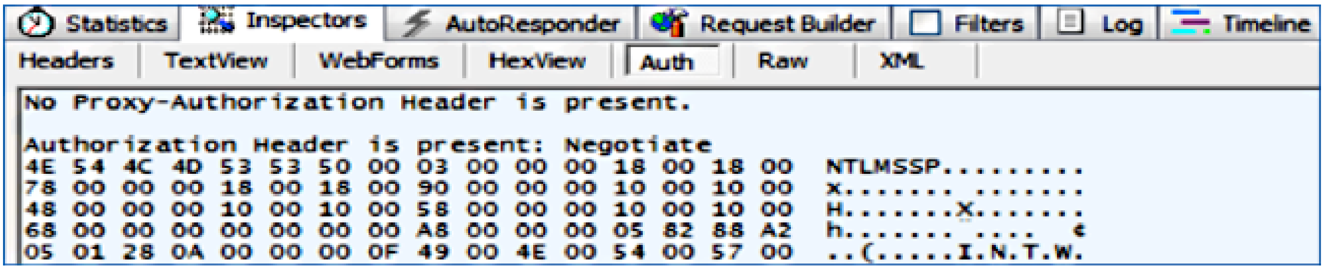
Pragma: no-cache

QuickExec] ALT+Q > type HELP...

Capturing | All Processes | 1 / 30 | https://vos-cm44.sso-44.com/adfs/ls/auth/integrated/?SAMLRequest=nVLLbtswELznKwTeFVqWbEuEZcCNEdRA2iR20Nva3qVEKB0Uu57d%2BXUh5wW8OHngguh7Mzs7

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

如果身份驗證型別為NTLM，則會在幀的開頭看到**協商 — NTLMSSP**，如下所示：



```
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.
```

Statistics Inspectors AutoResponder Request Builder Filters Log Timeline
Headers TextView WebForms HexView Auth Raw XML

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。