Jabber のエンドユーザ SAML SSO 向け ADFS 2.0 での Kerberos 設定例

内容

概要

このドキュメントでは、Active Directory フェデレーション サービス（ADFS）2.0 で Kerberos を設定する方法を説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

End User Security Assertion Markup Language（SAML）シングル サインオン（SSO）を設定す

るには、Jabber がドメイン認証と連動できるよう End User SAML SSO を有効にするために、Kerberos を設定する必要があります。Kerberos を使用して SAML SSO を実装すると、すべてのアクセス許可とユーザ同期が Lightweight Directory Access Protocol（LDAP）で処理される一方、認証は Kerberos で管理されるようになります。Kerberos は、LDAP 対応インスタンスと併せて使用するよう意図された認証プロトコルです。

Active Directory ドメインに参加する Microsoft Windows および Macintosh マシン上では、ユーザはユーザ名やパスワードを入力することなくシームレスに Cisco Jabber にログインすることができ、ユーザにログイン画面が表示されることさえありません。コンピュータ上で Active Directory ドメインにログインしないユーザには、引き続き標準のログイン フォームが表示されます。

認証ではオペレーティング システムから渡される単一のトークンが使用されるため、リダイレクトの必要はありません。トークンは設定済みのキー ドメイン コントローラに照らし合わせて確認され、トークンが有効であればユーザがログインされます。

コンフィギュレーション

ADFS 2.0 で Kerberos を設定する手順は以下のとおりです。

1. マシンに Microsoft Windows Server 2008 R2 をインストールします。

2. Active Directory ドメイン サービス（ADDS）と ADFS を同じマシンにインストールします。

3. Microsoft Windows Server 2008 R2 がインストールされたマシンに、インターネット インフォメーション サービス（IIS）をインストールします。

4. IIS 用の自己署名証明書を作成します。

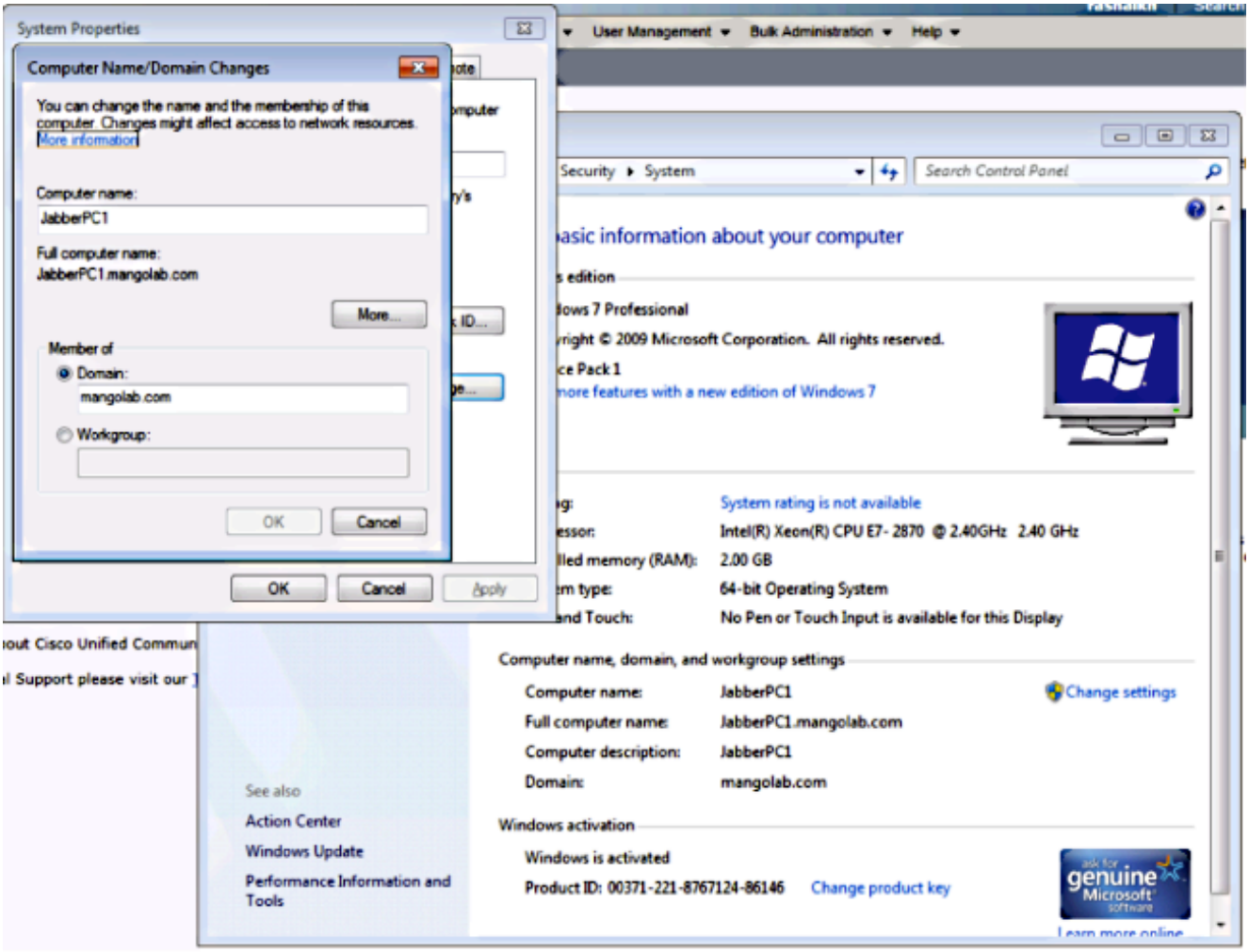
5. 自己署名証明書を IIS にインポートし、その自己署名証明書を HTTPS サーバ証明書として使用します。

6. 別のマシンに Microsoft Windows 7 をインストールして、そのマシンをクライアントとして使用します。

   ドメイン ネーム サーバ（DNS）を変更し、ADDS がインストールされているマシンを DNS とします。

   このマシンを、ADDS のインストール時に作成したドメインに追加します。

   [Start]に移動します。[Computer]を右クリックします。[Properties] をクリックします。ウィンドウの右側にある [Change Settings]をクリックします。[Computer Name]タブをクリックします。[Change] をクリックします。作成したドメインを追加します。



7. Kerberos サービスが両方のマシンで生成されるかどうかを確認します。

   管理者としてサーバ マシンにログインし、コマンド プロンプトを開きます。以下のコマンドを実行します。

   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
```

   ドメイン ユーザとしてクライアント マシンにログインし、同じコマンドを実行します。

```
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. ADDS がインストールされているマシンで、ADFS Kerberos ID を作成します。

   Microsoft Windows ドメインにログインしている Microsoft Windows 管理者（たとえば、Microsoft Windows ドメイン コントローラに <domainname>\administrator としてログインしているユーザ）が ADFS Kerberos ID を作成します。ADFS HTTP サービスには、サービス プリンシパル名（SPN）と呼ばれる Kerberos ID が**HTTP/DNS_name_of_ADFS_server** 形式で設定されてるはずです。

   この名前を、ADFS HTTP サーバ インスタンスを表す Active Directory ユーザにマッピング

する必要があります。それには、Microsoft Windows の **setspn ユーティリティを使用します。このユーティリティはデフォルトで Microsoft Windows 2008 Server で使用可能になっているはずです。**

手順 ADFS サーバの SPN を登録します。Active Directory ドメイン コントローラで、**setspn コマンドを実行します。**

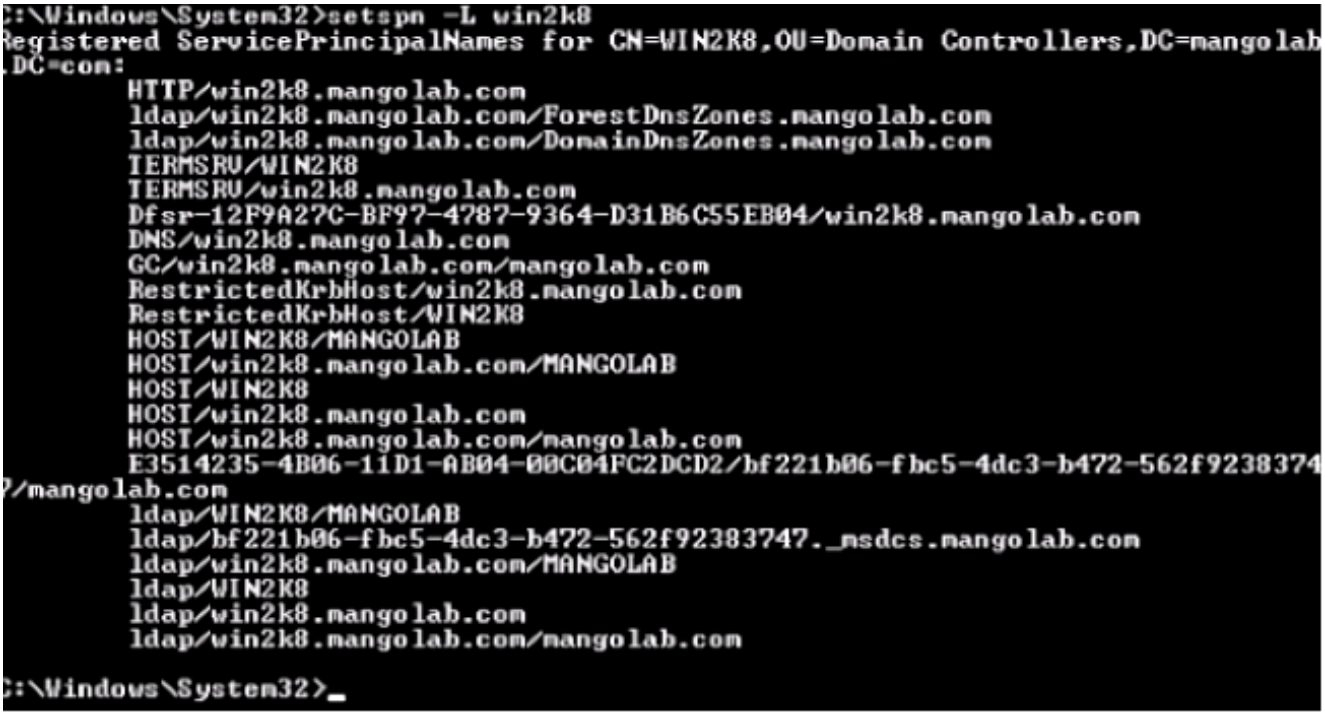
たとえば、ADFS ホストが **adfs01.us.renovations.com** で、Active Directory ドメインが **US.RENOVATIONS.COM の場合、以下のコマンドを実行します。**

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

ADFS サーバに通常はセキュア ソケット レイヤ（SSL）（つまり、HTTPS）でアクセスするとしても、SPN の **HTTP/の部分は適用されます。**

ADFS サーバの SPN が正しく作成されたことを確認するために、**setspn コマンドを入力し、出力を表示します。**

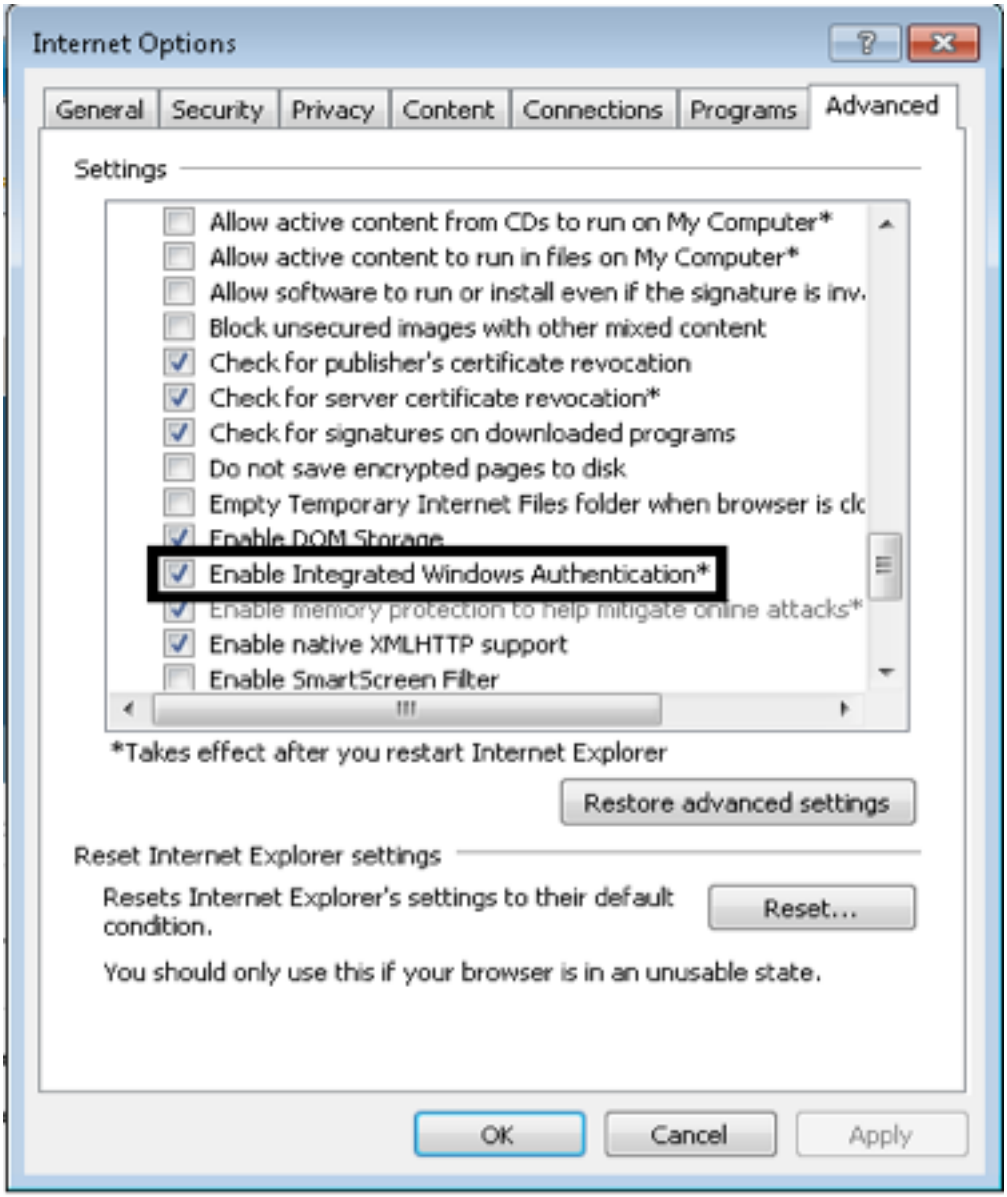
```
setspn -L
```



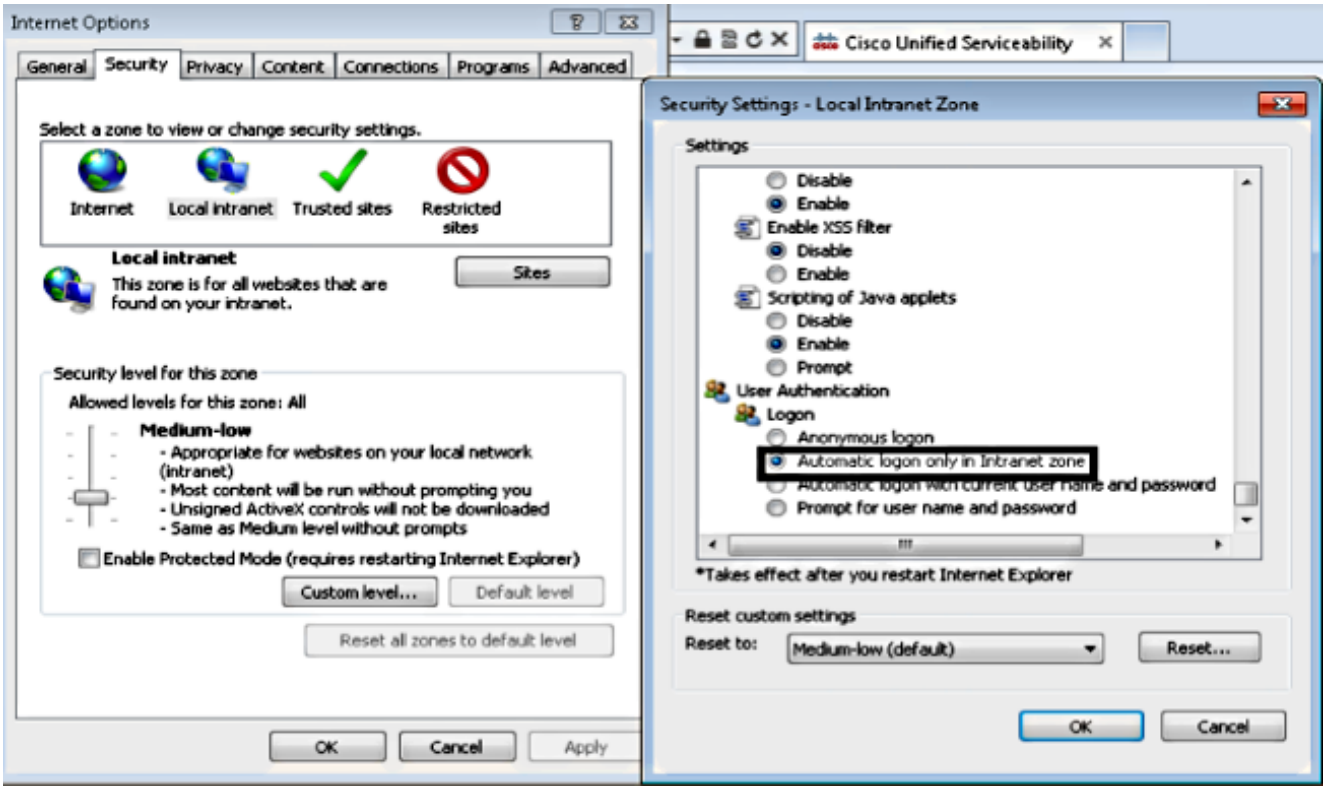
9. Microsoft Windows クライアントのブラウザ設定を構成します。

   統合 Windows 認証を有効にするために、[Tools] > [Internet Options] > [Advanced]に移動します。

   [Enable Integrated Windows Authentication]チェックボックスをオンにします。

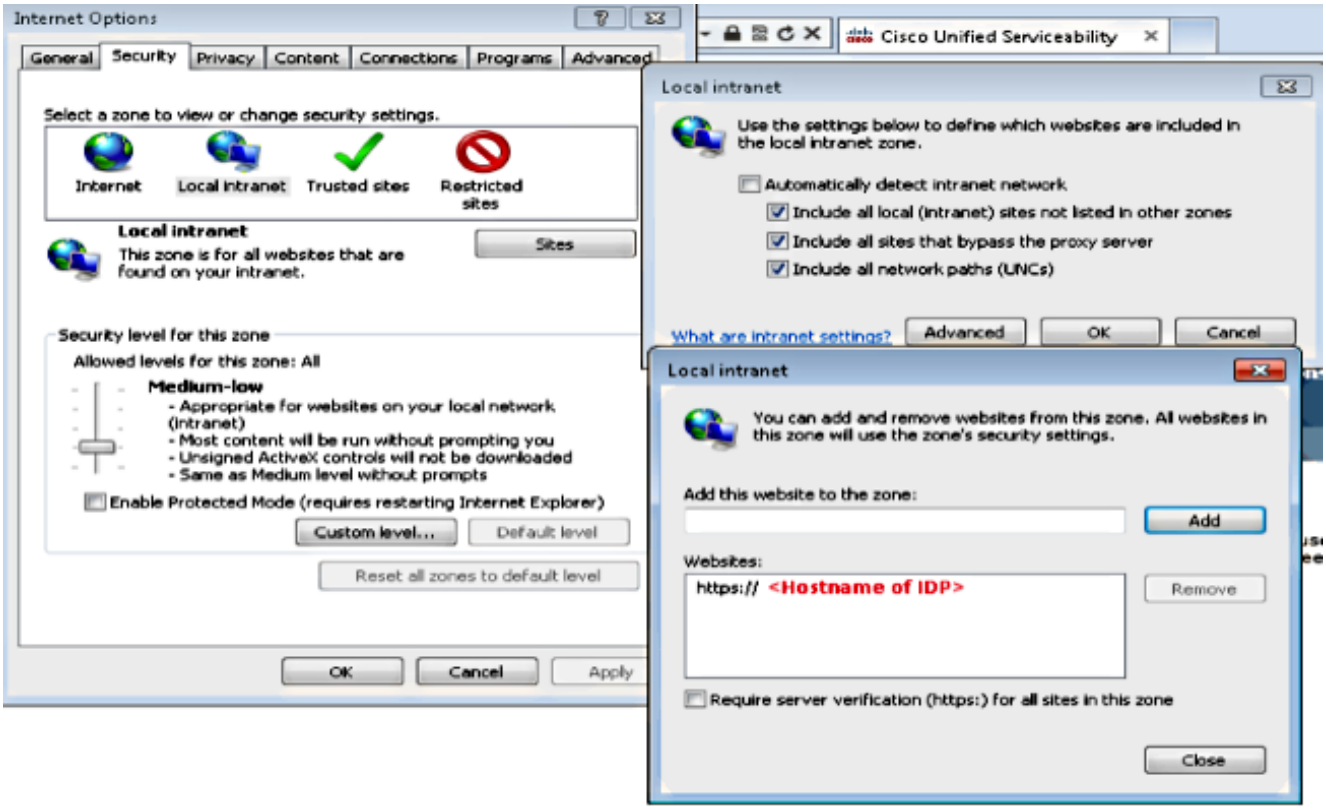


[Tools] > [Internet Options] > [Security] > [Local intranet] > [Custom level...] に移動して、[Automatic logon only in Intranet zone] をオンにします。



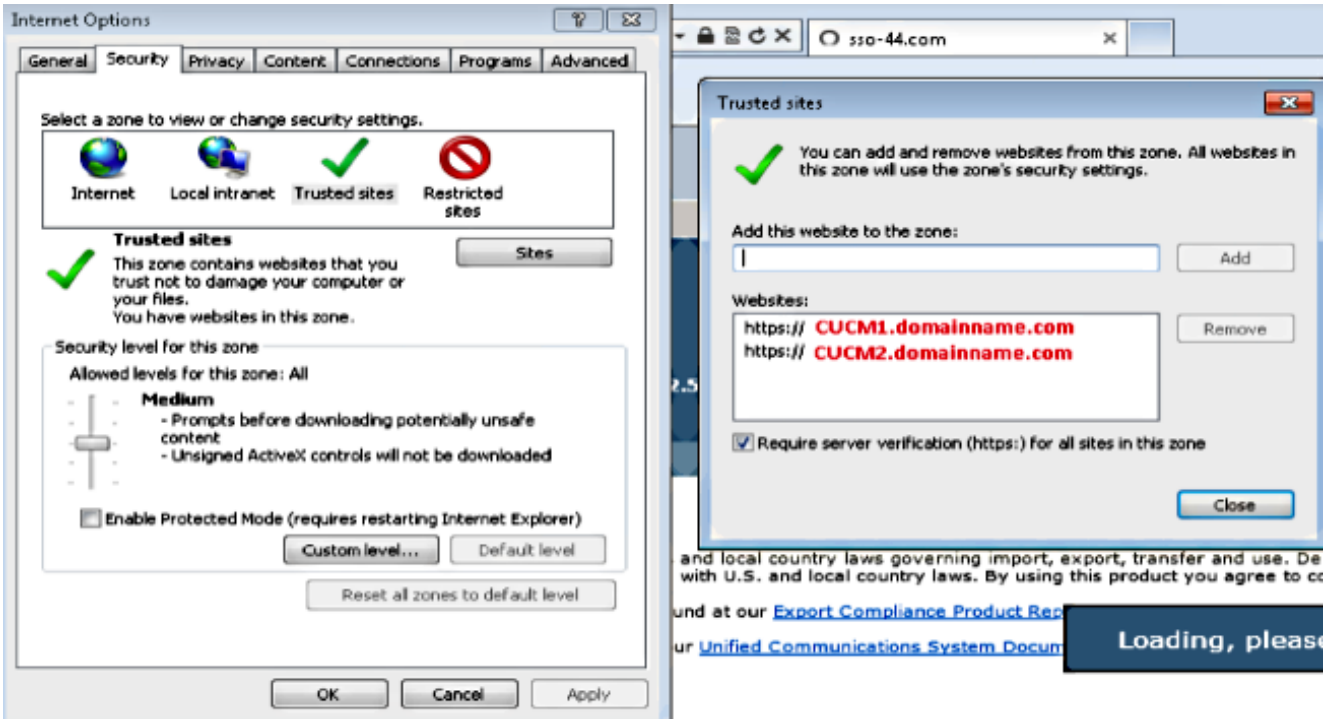
[Tools] > [Internet Options] > [Security] > [Local intranet] > [Sites] > [Advanced]に移動して、Intrusion Detection & Prevention（IDP）URL をローカル イントラネット サイトに追加します。

注：[Local intranet] ダイアログボックスのすべてのチェックボックスをオンにして、[Advanced]タブをクリックします。



[Tools] > [Security] > [Trusted sites] > [Sites]に移動して、CUCM ホスト名を [Trusted sites]

に追加します。



確認

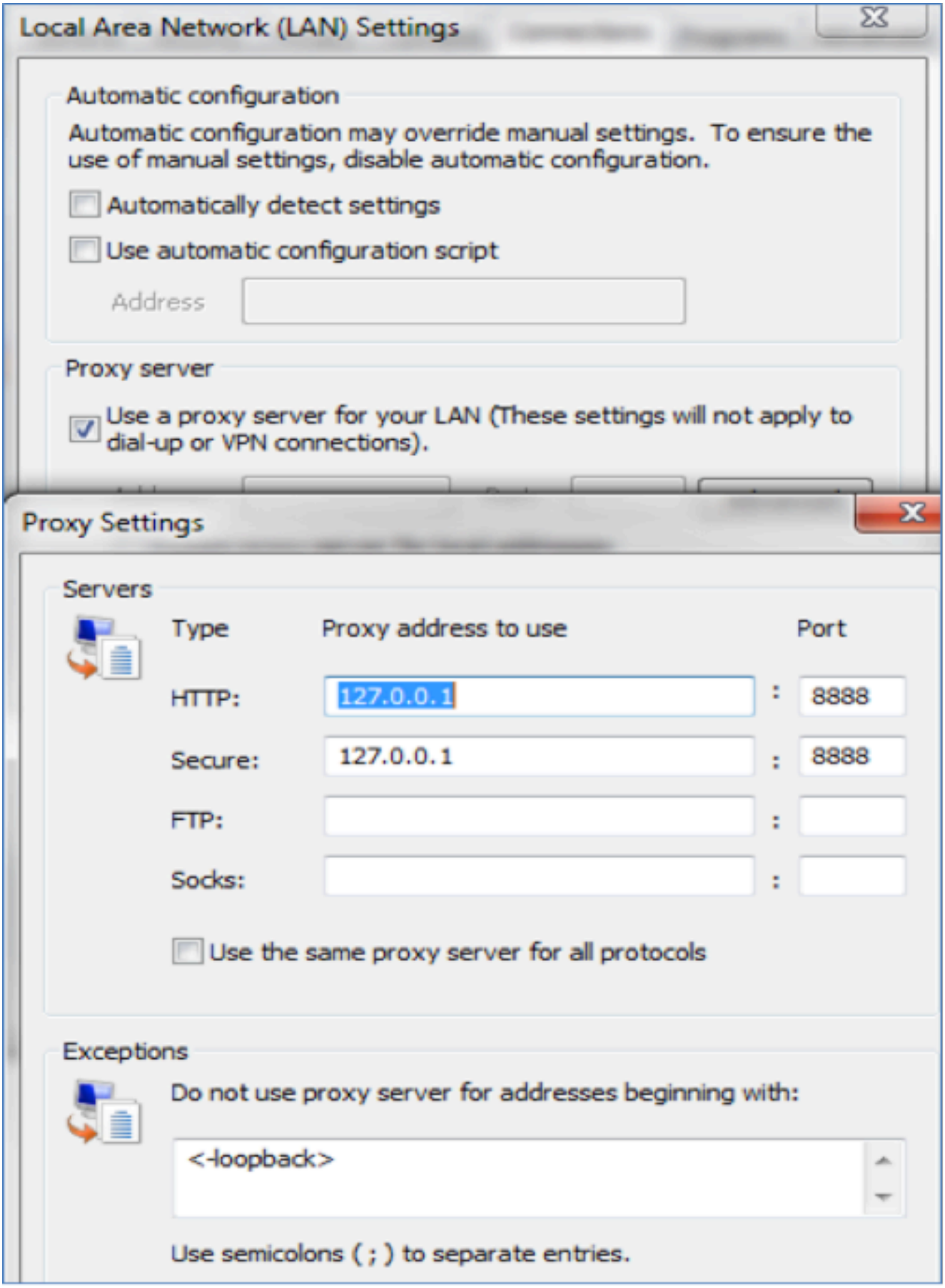
このセクションでは、使用されている認証（Kerberos 認証または NT LAN Manager（NTLM）認証）を確認する方法を説明します。

1. クライアント マシンに Fiddler ツールをダウンロードしてインストールします。

2. すべての Internet Explorer ウィンドウを閉じます。

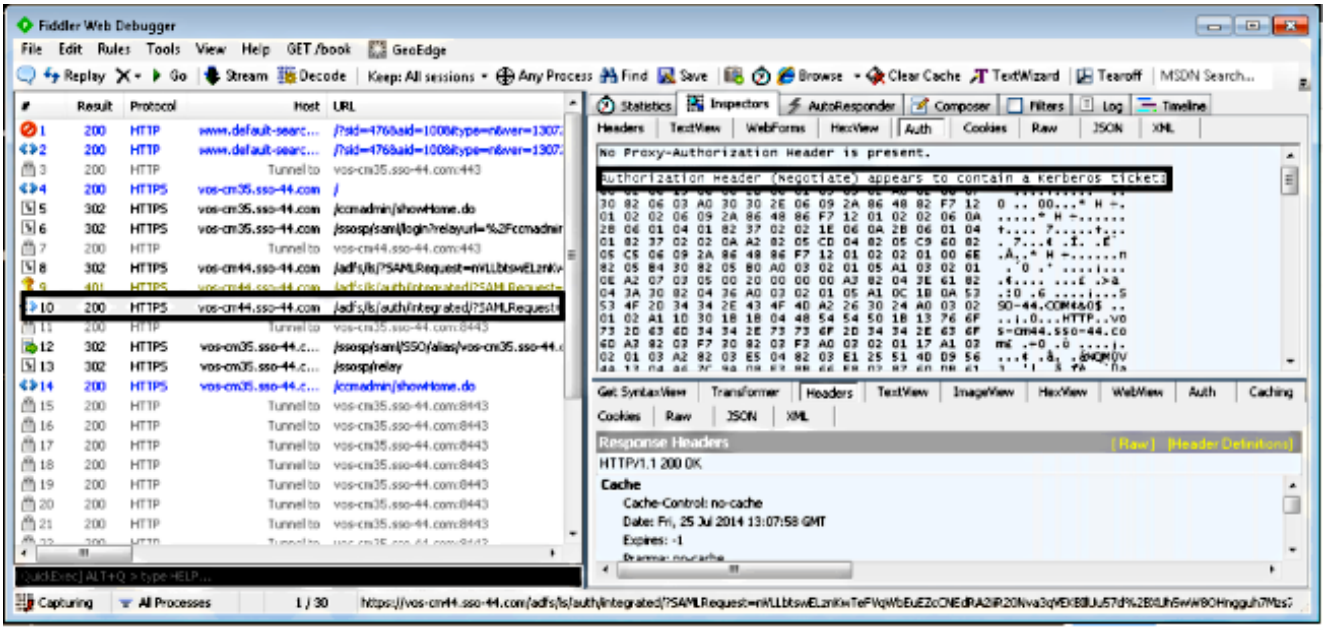
3. Fiddler ツールを実行し、[File] メニューの [Capture Traffic] オプションが有効であることを確認します。

   Fiddler は、クライアント マシンとサーバ間のパススルー プロキシとして機能し、すべてのトラフィックをリッスンします。Fiddler により、Internet Explorer 設定は一時的に以下のように変更されます。

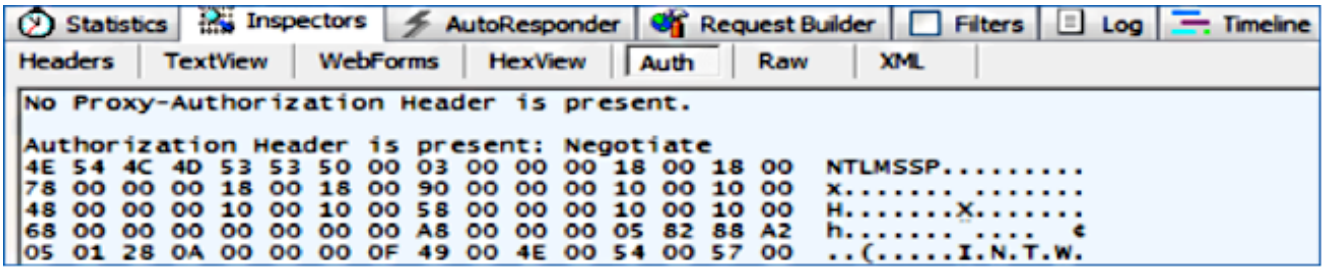


4. Internet Explorer を開いて顧客関係管理（CRM）サーバの URL を参照し、いくつかのリンクをクリックしてトラフィックを生成します。

5. Fiddler のメイン ウィンドウに戻り、結果が 200（成功）となっているフレームのいずれかを選択します。



認証タイプが NTLM の場合、以下のようにフレームの先頭に [Negotiate - NTLMSSP] と表示されます。



トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。