

Kerberos認証を使用したSAML SSOセットアップの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[AD FS の設定](#)

[ブラウザの設定](#)

[Microsoft Internet Explorer](#)

[Mozilla Firefox](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Jabber クライアントによる Kerberos 認証 (Microsoft Windows のみ) を使用するために Active Directory および Active Directory Federation Service (AD FS) バージョン 2.0 を有効にする方法を説明します。これにより、ユーザは Microsoft Windows ログオンでログインし、クレデンシャルの入力を求められません。

注意：このドキュメントは、ラボ環境に基づいており、前提として、変更を実行したことによる影響を認識しておいてください。実行した変更の影響を理解するために、関連する製品ドキュメントを参照してください。

前提条件

要件

Cisco では次の前提を満たす推奨しています。

- AD FS バージョン 2.0 がインストールされ、シスコ コラボレーション製品を使用して信頼できるパーティとして設定している
- Security Assertion Markup Language (SAML) シングル サインオン (SSO) を使用するために、Cisco Unified Communications Manager (CUCM) IM および Presence、Cisco Unity Connection (UCXN)、CUCM が有効化されている

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

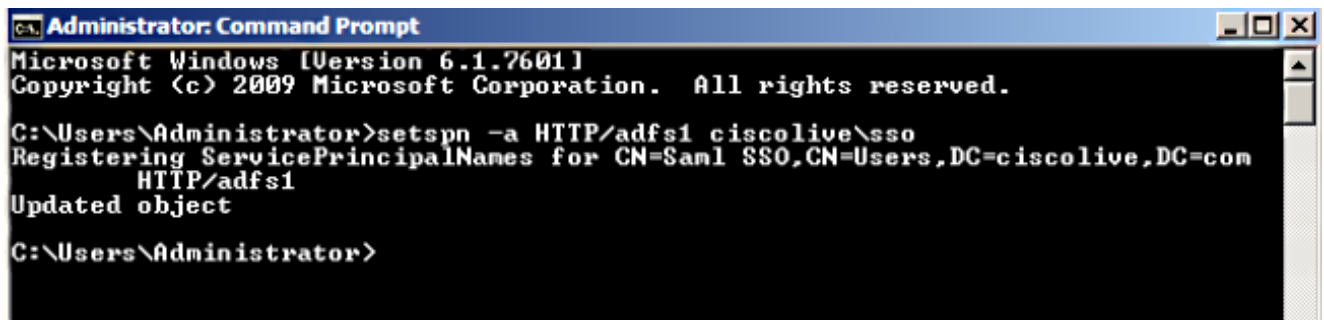
- Active Directory 2008 (ホスト名 : ADFS1.ciscolive.com)
- AD FS バージョン 2.0 (ホスト名 : ADFS1.ciscolive.com)
- CUCM (ホスト名 : CUCM1.ciscolive.com)
- Microsoft Internet Explorer バージョン 10
- Mozilla Firefox バージョン 34
- Telerik Fiddler バージョン 4

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。

設定

AD FS の設定

1. Jabber がインストールされているクライアントコンピュータを有効化してチケットをリクエストし、AD FS サービスと通信するためのクライアント コンピュータを有効化するために、Service Principal Name (SPN) を使用して AD FS バージョン 2.0 を設定します。



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>setspn -a HTTP/adfs1 ciscolive\sso
Registering ServicePrincipalNames for CN=Sam1 SSO,CN=Users,DC=ciscolive,DC=com
HTTP/adfs1
Updated object

C:\Users\Administrator>
```

詳細については、「[AD FS 2.0 : サービスアカウント用に SPN \(servicePrincipalName \) を設定する方法](#)」を参照してください。

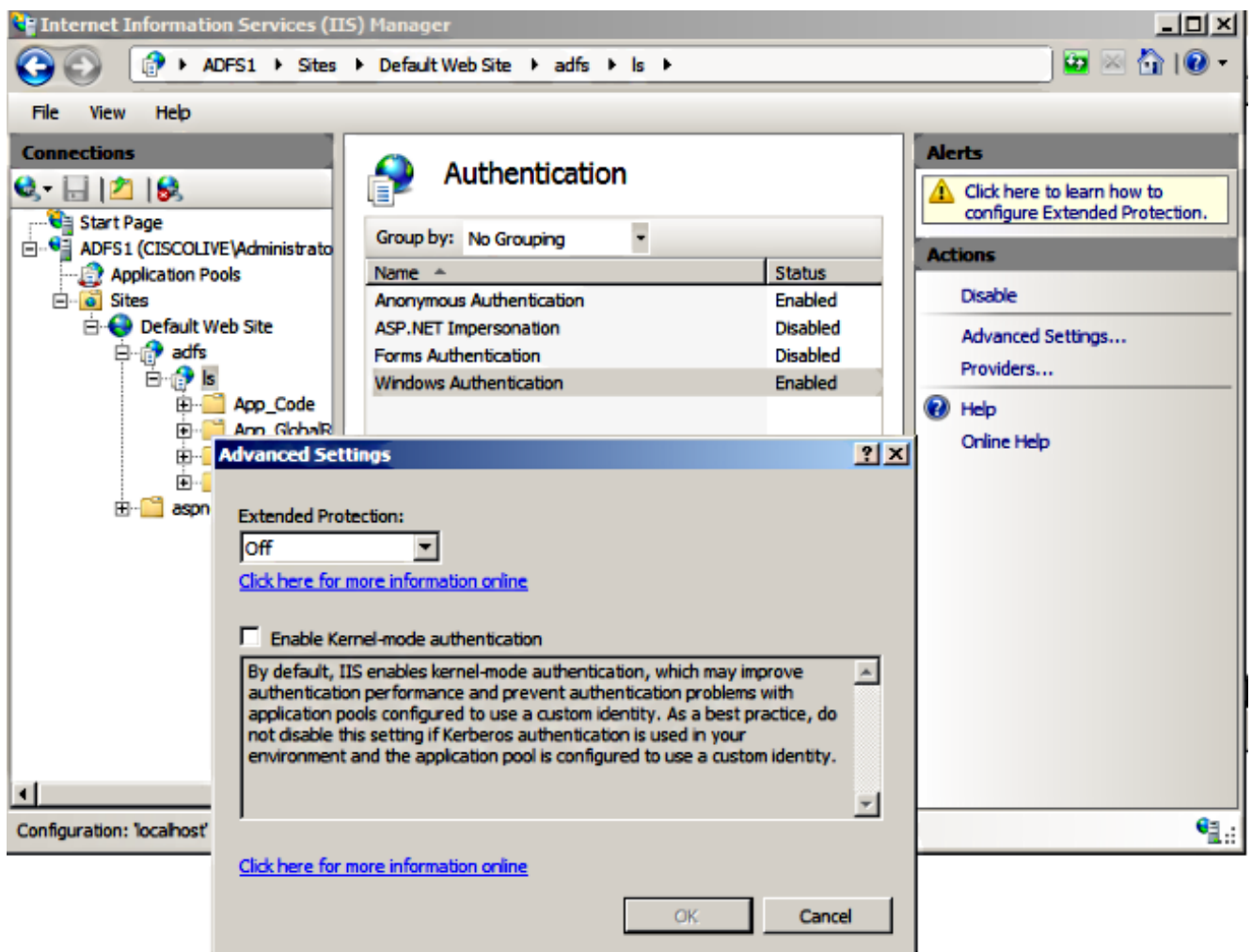
2. AD FS サービス用のデフォルトの認証設定 (C:\inetpub\adfs\ls\web.config に含まれる) が統合 Windows 認証であることを確認します。それがフォームベース認証に変更されていないことを確認します。

```

<microsoft.identityserver.web>
  <localAuthenticationTypes>
    <add name="Integrated" page="auth/integrated/" />
    <add name="Forms" page="FormsSignIn.aspx" />
    <add name="TlsClient" page="auth/sslclient/" />
    <add name="Basic" page="auth/basic/" />
  </localAuthenticationTypes>
  <commonDomainCookieWriter="" reader="" />
  <context hidden="true" />
  <error page="Error.aspx" />
  <acceptedFederationProtocols saml="true" wsFederation="true" />
  <homeRealmDiscovery page="HomeRealmDiscovery.aspx" />
  <persistIdentityProviderInformation enabled="true" lifetimeInDays="30" />
  <singleSignon enabled="true" />
</microsoft.identityserver.web>

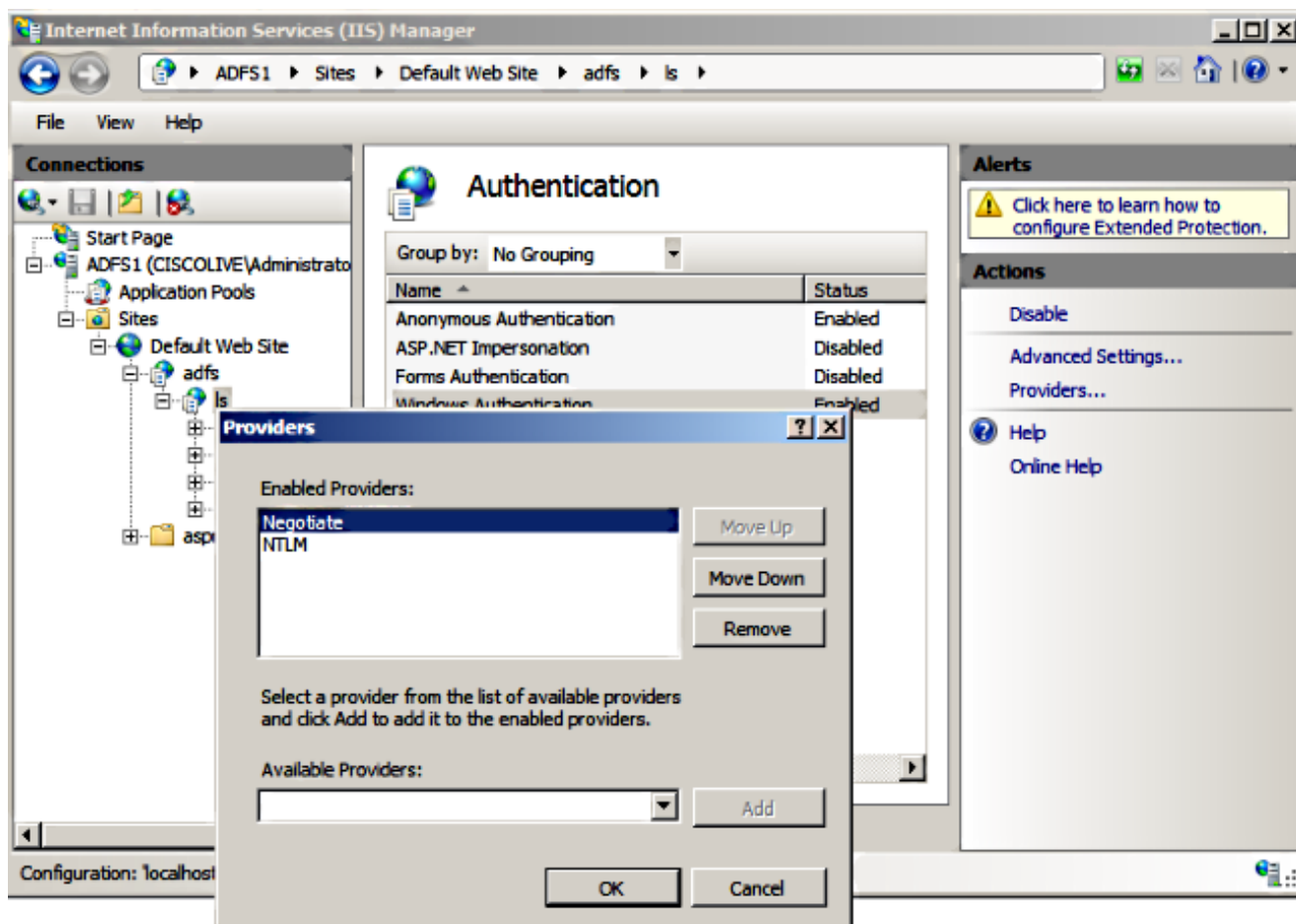
```

3. [Windows Authentication] を選択し、右ペインにある [Advanced Settings] をクリックします。
 。 [Advanced Settings] で、[Enable Kernel-mode authentication] をオフにし、[Extended Protection] が [Off] であることを確認し、[OK] をクリックします。



4. Windows 以外のすべてのクライアントは、Kerberos を使用できず、NTLM に依存するため、AD FS バージョン 2.0 が Kerberos プロトコルと NT LAN Manager (NTLM) プロトコルの両方をサポートすることを確認します。

右ペインで [Providers] を選択し、[Enabled Providers] の下に [Negotiate] と [NTLM] が存在することを確認します。



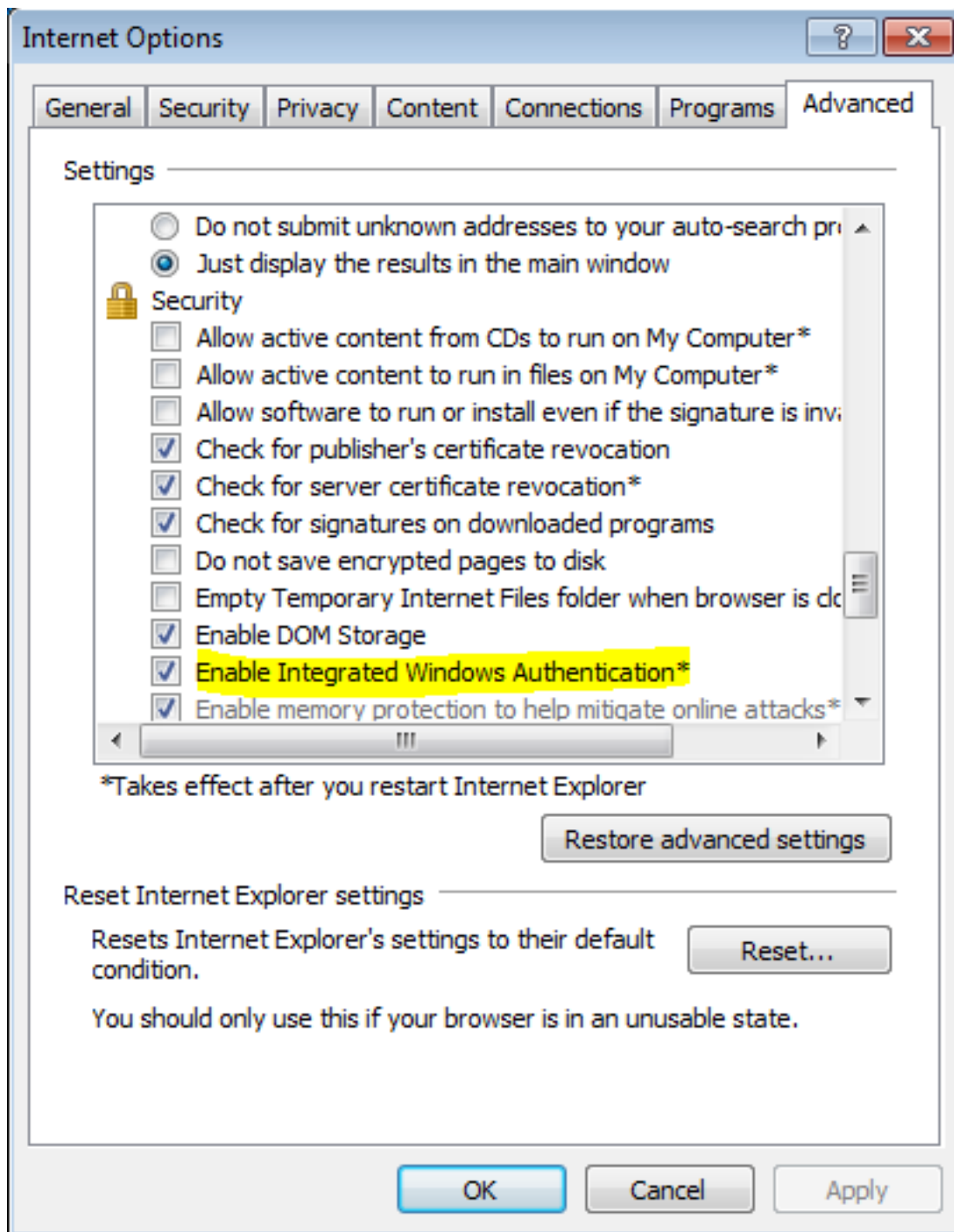
注：統合 Windows 認証を使用すると、AD FS は、クライアントの要求を認証するためにネゴシエート セキュリティ ヘッダーを渡します。ネゴシエート セキュリティ ヘッダーは、クライアントが Kerberos 認証と NTLM 認証のいずれかを選択できるようにします。次のいずれかの条件に該当する場合を除き、ネゴシエート プロセスは Kerberos 認証を選択します。

- 認証に関与するシステムのいずれかが Kerberos 認証を使用できない。
- 発信側のアプリケーションが、Kerberos 認証を使用するための十分な情報を提供しない。
- ネットワーク認証に Kerberos プロトコルを選択するように、ネゴシエート プロセスを有効化する目的で、クライアント アプリケーションが SPN、ユーザ プリンシパル名 (UPN)、または Network Basic Input/Output System (NetBIOS) アカウント名をターゲット名として提供する必要がある。そうしないと、ネゴシエート プロセスは、優先認証方法として NTLM プロトコルを常に選択します。

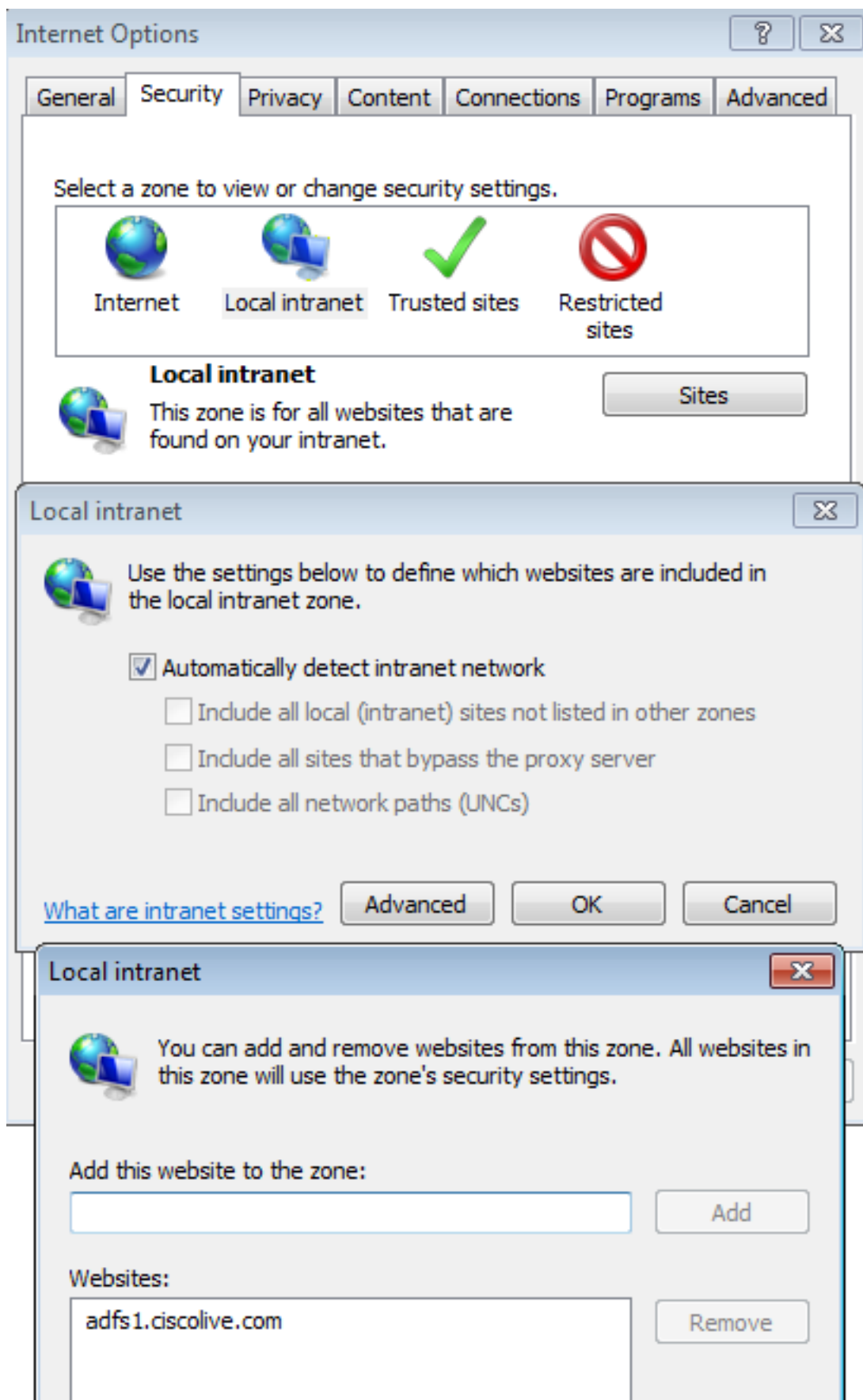
ブラウザの設定

Microsoft Internet Explorer

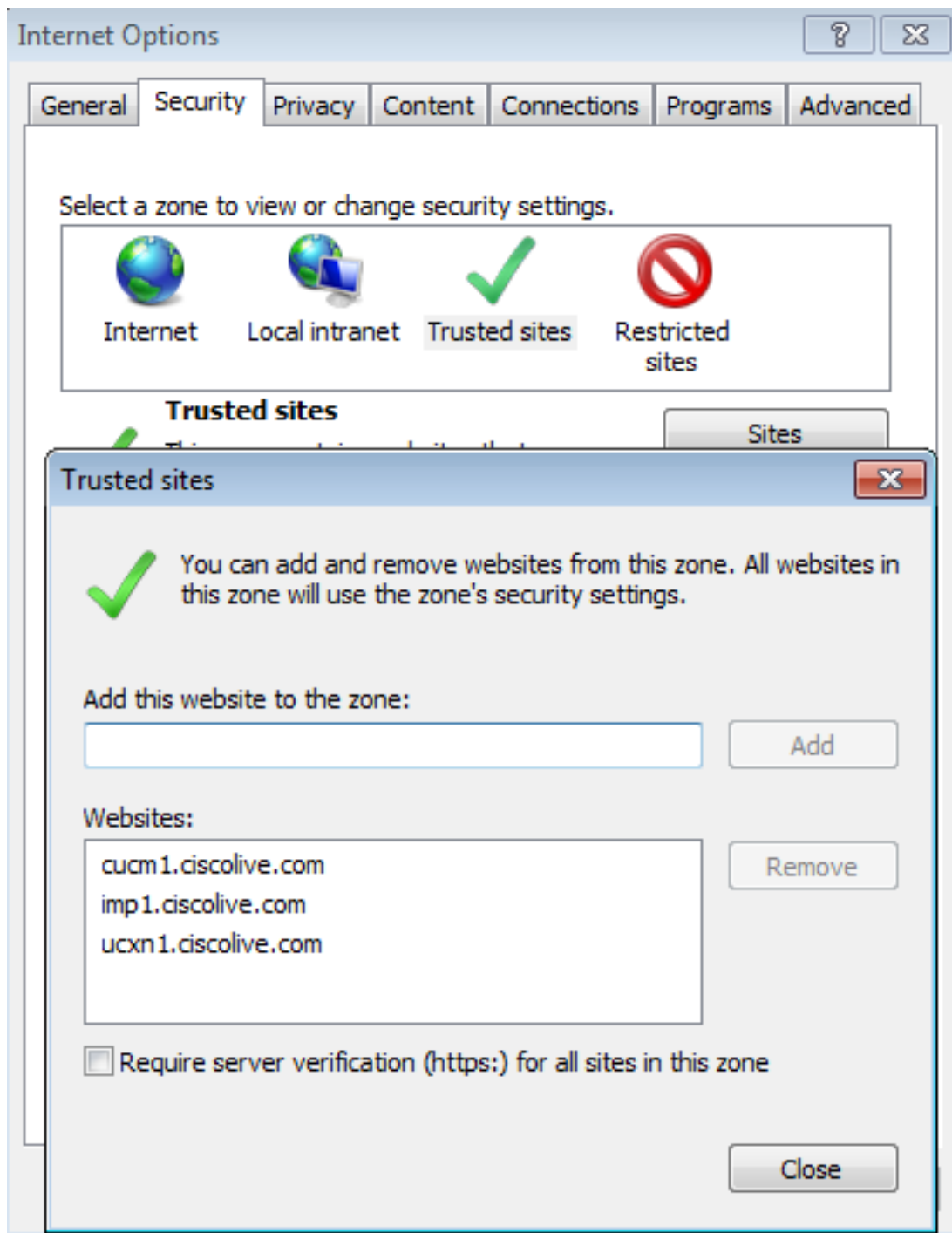
1. [Internet Explorer] > [Advanced] > [Enable Integrated Windows Authentication] がオンになっていることを確認します。



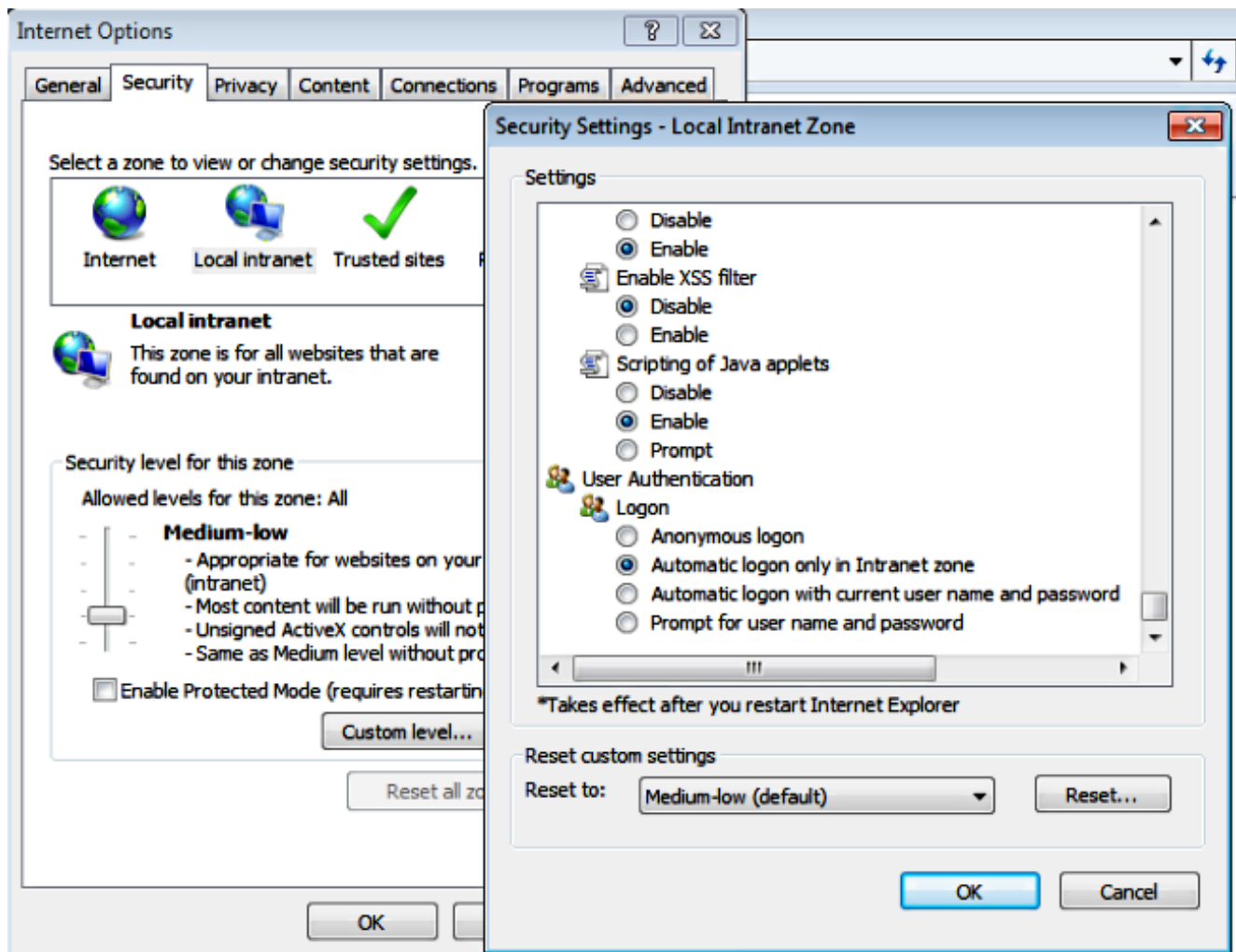
2. [Security] > [Intranet zones] > [sites] に AD FS の URL を追加します。



3. CUCM、IMP、および Unity のホスト名を [Security] > [Trusted sites] に追加します。

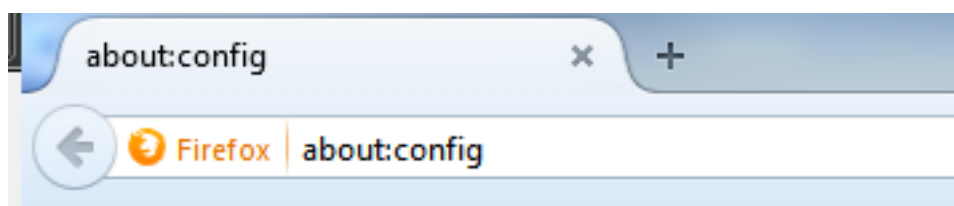


4. イン트라ネット サイト用にログイン クレデンシャルを使用するために、[Internet Explorer] > [security] > [Local Intranet] > [Security Settings] > [User Authentication - Logon] が設定されていることを確認します。



Mozilla Firefox

1. Firefoxを開き、アドレスバーにabout:configと入力します。



2. [I'll be careful, I promise!] をクリックします。



- 変更するには、プリファレンス名 `network.negotiate-auth.allow-non-fqdn` を `true` に、`network.negotiate-auth.trusted-uris` を `ciscolive.com,adfs1.ciscolive.com` にダブルクリックします。

Preference Name	Status	Type	Value
<code>network.negotiate-auth.allow-insecure-ntlm-v1</code>	default	boolean	false
<code>network.negotiate-auth.allow-insecure-ntlm-v1-https</code>	default	boolean	true
<code>network.negotiate-auth.allow-non-fqdn</code>	user set	boolean	true
<code>network.negotiate-auth.allow-proxies</code>	default	boolean	true
<code>network.negotiate-auth.delegation-uris</code>	default	string	
<code>network.negotiate-auth.gsslib</code>	default	string	
<code>network.negotiate-auth.trusted-uris</code>	user set	string	<code>adfs1,adfs1.ciscolive.com,ciscolive.com</code>
<code>network.negotiate-auth.using-native-gsslib</code>	default	boolean	true
<code>network.ntlm.send-lm-response</code>	default	boolean	false

- Firefox を閉じ、再度開きます。

確認

AD FS 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。

```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>setspn -L sso
Registered ServicePrincipalNames for CN=Sam1 SSO,CN=Users,DC=ciscolive,DC=com:
HTTP/adfs1

C:\Users\Administrator>_
```

クライアント マシンが Kerberos チケットを持っているかどうか確認します。

```
C:\Windows\system32\cmd.exe
C:\Users\user1.CISCOLIVE>klist tickets

Current LogonId is 0:0xabc6d

Cached Tickets: (2)

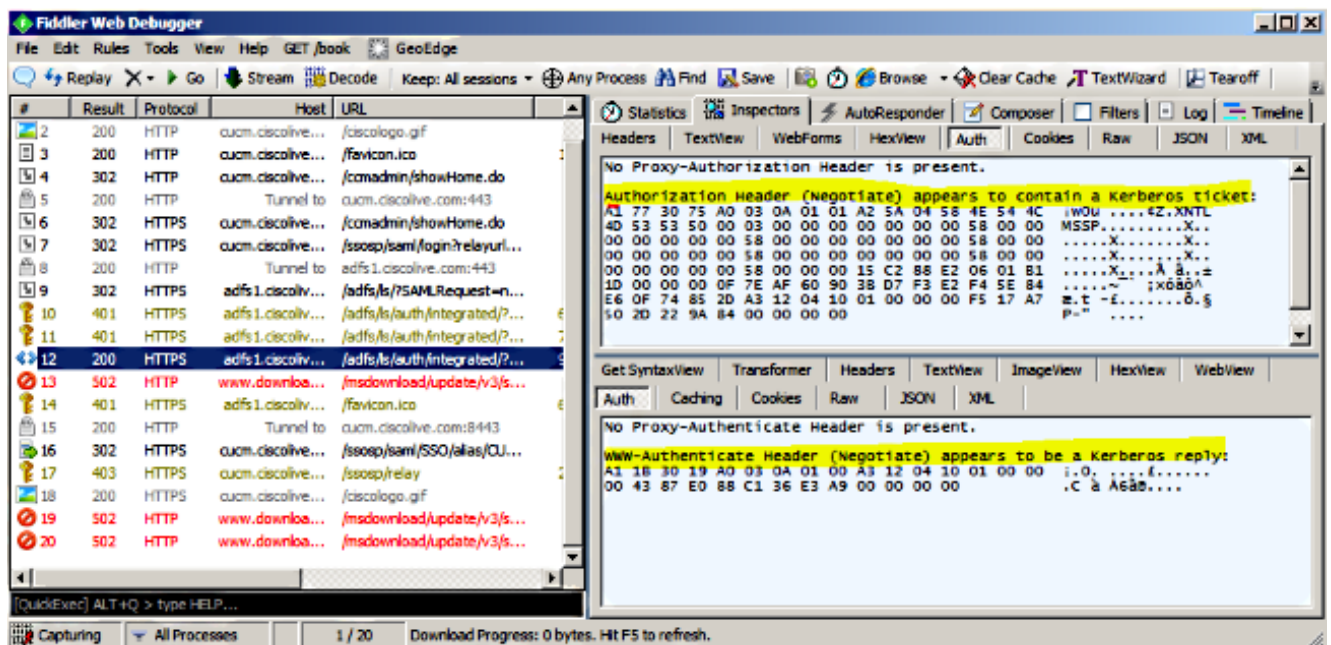
#0> Client: user1 @ CISCOLIVE.COM
Server: krbtgt/CISCOLIVE.COM @ CISCOLIVE.COM
Kerberos Ticket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
Start Time: 1/17/2015 20:52:47 (local)
End Time: 1/18/2015 6:52:47 (local)
Renew Time: 1/24/2015 20:52:47 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96

#1> Client: user1 @ CISCOLIVE.COM
Server: host/pc1.ciscolive.com @ CISCOLIVE.COM
Kerberos Ticket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
Start Time: 1/17/2015 20:52:47 (local)
End Time: 1/18/2015 6:52:47 (local)
Renew Time: 1/24/2015 20:52:47 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96

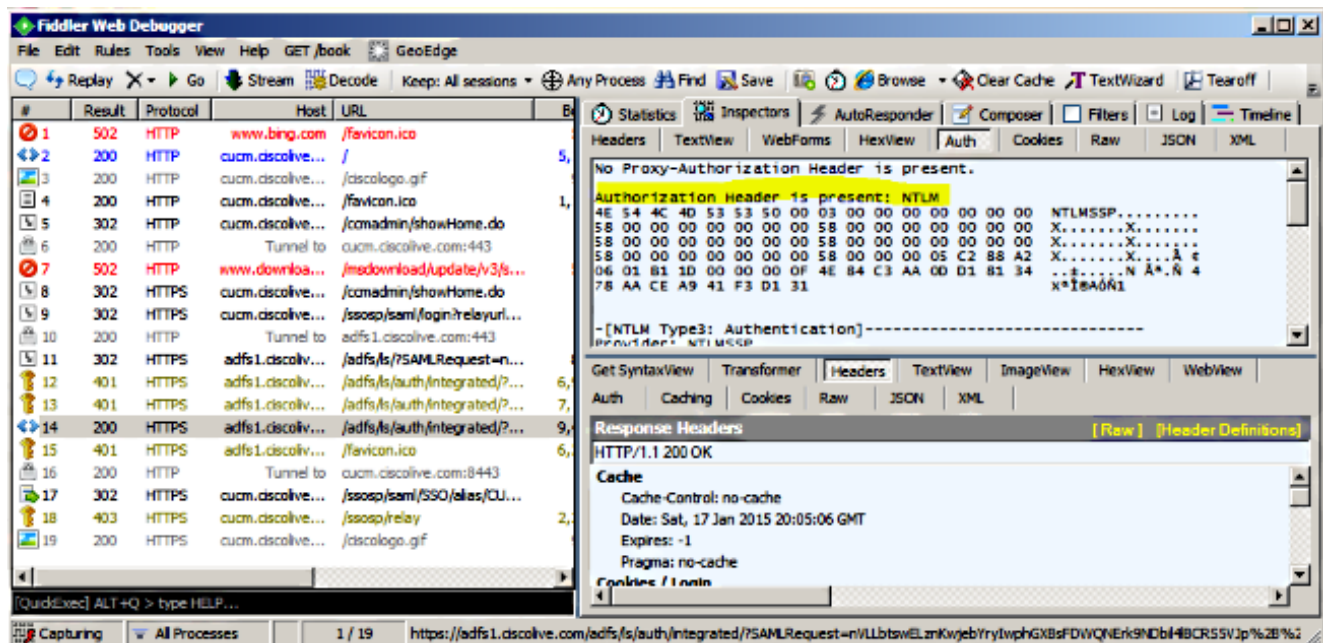
C:\Users\user1.CISCOLIVE>_
```

これらの手順を完了し、どの認証 (Kerberos または NTLM 認証) が使用されているか検証します。

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 Microsoft 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 マシンとサーバ間でパススループロキシとして動作し、すべてのトラフィックをリッスンします。
4. Microsoft Internet Explorer を開いてから CUCM を参照し、リンクをいくつか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) であるいずれかのフレームを選択すると、Kerberos が認証メカニズムであることがわかります。



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



トラブルシューティング

このドキュメントの記載に従って、すべての設定手順および検証手順を完了してもまだログインの問題が発生する場合は、Microsoft Windows の Active Directory / AD FS 管理者に相談する必要があります。