SAML SSO Setup with Kerberos Authentication Configuration Example

Document ID: 118773

Contributed by A.M.Mahesh Babu, Cisco TAC Engineer.
Jan 21, 2015

Contents

Introduction
Prerequisites
Requirements
Components Used
Configure
Configure AD FS
Configure Browser
Microsoft Internet Explorer
Mozilla FireFox
Verify
Troubleshoot

Introduction

This document describes how to configure Active Directory and Active Directory Federation Service (AD FS) Version 2.0 in order to enable it to use Kerberos Authentication by Jabber Clients (Microsoft Windows only), which allows users to log in with their Microsoft Windows Logon and not be prompted for credentials.

Caution: This document is based on a lab environment and assumes that you are aware of the impact of changes that you make. Refer to the relevant product documentation in order to understand the impact of changes you make.

Prerequisites

Requirements

Cisco recommends that you have:

- AD FS Version 2.0 installed and configured with Cisco Collaboration products as Relying Party Trust
- Collaboration products such as Cisco Unified Communications Manager (CUCM) IM and Presence, Cisco Unity Connection (UCXN), and CUCM enabled in order to use Security Assertion Markup Language (SAML) Single Sign−on (SSO)

Components Used

The information in this document is based on these software and hardware versions:

- Active Directory 2008 (Hostname: ADFS1.ciscolive.com)
- AD FS Version 2.0 (Hostname: ADFS1.ciscolive.com)

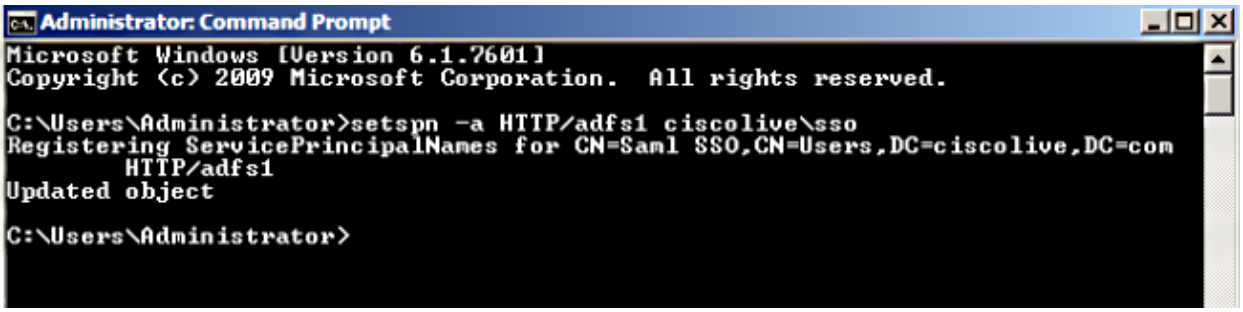
- CUCM (Hostname: CUCM1.ciscolive.com)
- Microsoft Internet Explorer Version 10
- Mozilla Firefox Version 34
- Telerik Fiddler Version 4

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.

Configure

Configure AD FS

1. Configure AD FS Version 2.0 with Service Principal Name (SPN) in order to enable the client computer on which Jabber is installed to request tickets, which in turn enables the client computer to communicate with an AD FS service.



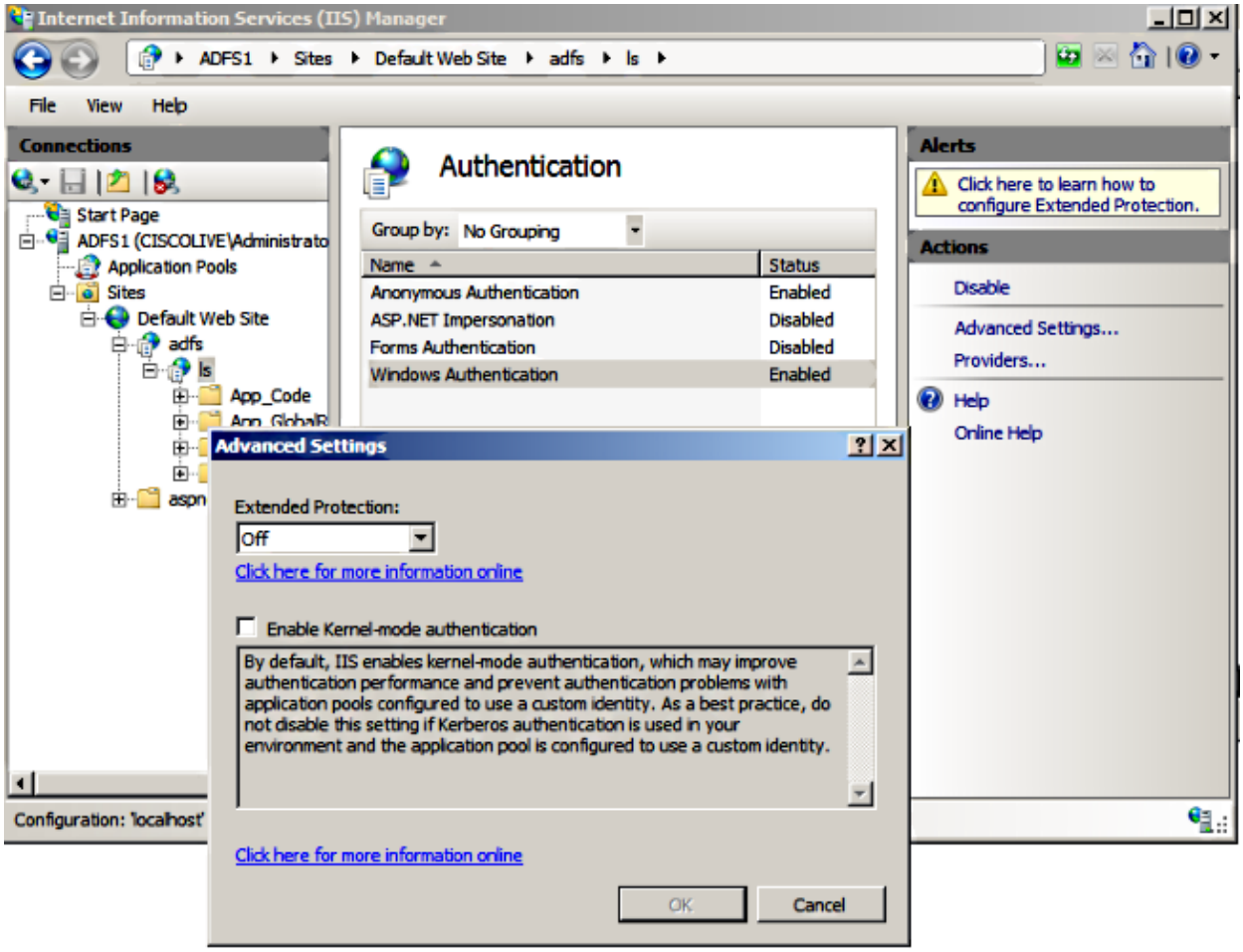
Refer to AD FS 2.0: How to Configure the SPN (servicePrincipalName) for the Service Account for more information.

2. Ensure that the default authentication configuration for the AD FS service (in ***C:\inetpub\adfs\ls\web.config***) is ***Integrated Windows Authentication***. Ensure that it has not been changed to ***Form−based Authentication***.

```
<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>
  <commonDomainCookie writer="" 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>
```

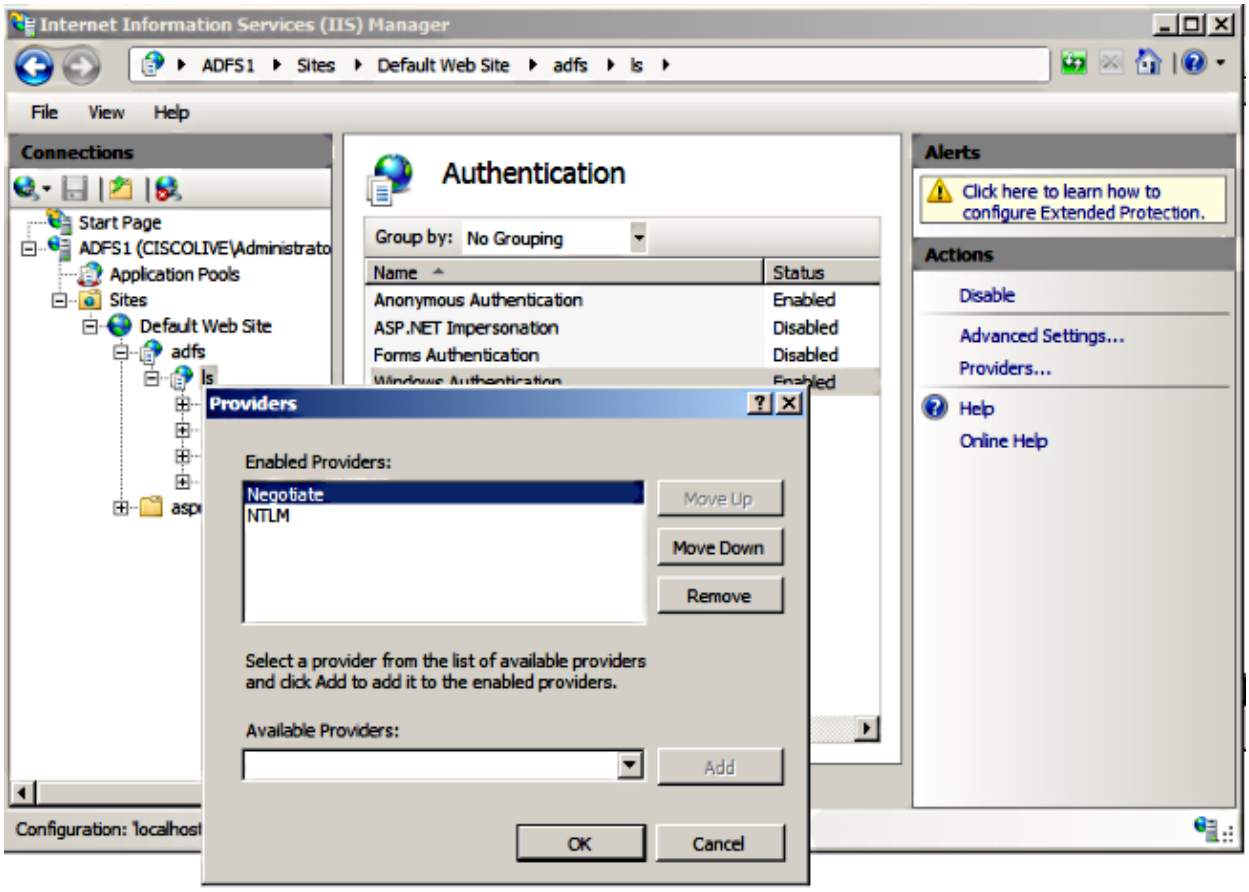
3. Select ***Windows Authentication*** and click ***Advanced Settings*** under the right−pane. In Advanced

Settings, uncheck ***Enable Kernel−mode authentication***, make sure Extended Protection is ***Off***, and click ***OK***.



4. Ensure that AD FS Version 2.0 supports both the Kerberos protocol and the NT LAN Manager (NTLM) protocol because all Non−Windows clients cannot use Kerberos and rely on NTLM.

   In the right−pane, select ***Providers*** and make sure ***Negotiate*** and ***NTLM*** are present under Enabled Providers:



Note: AD FS passes the Negotiate security header when Integrated Windows authentication is used in order to authenticate client requests. The Negotiate security header lets clients select between Kerberos authentication and NTLM authentication. The Negotiate process selects Kerberos authentication unless one of these conditions is true:

− One of the systems that is involved in the authentication cannot use Kerberos authentication.

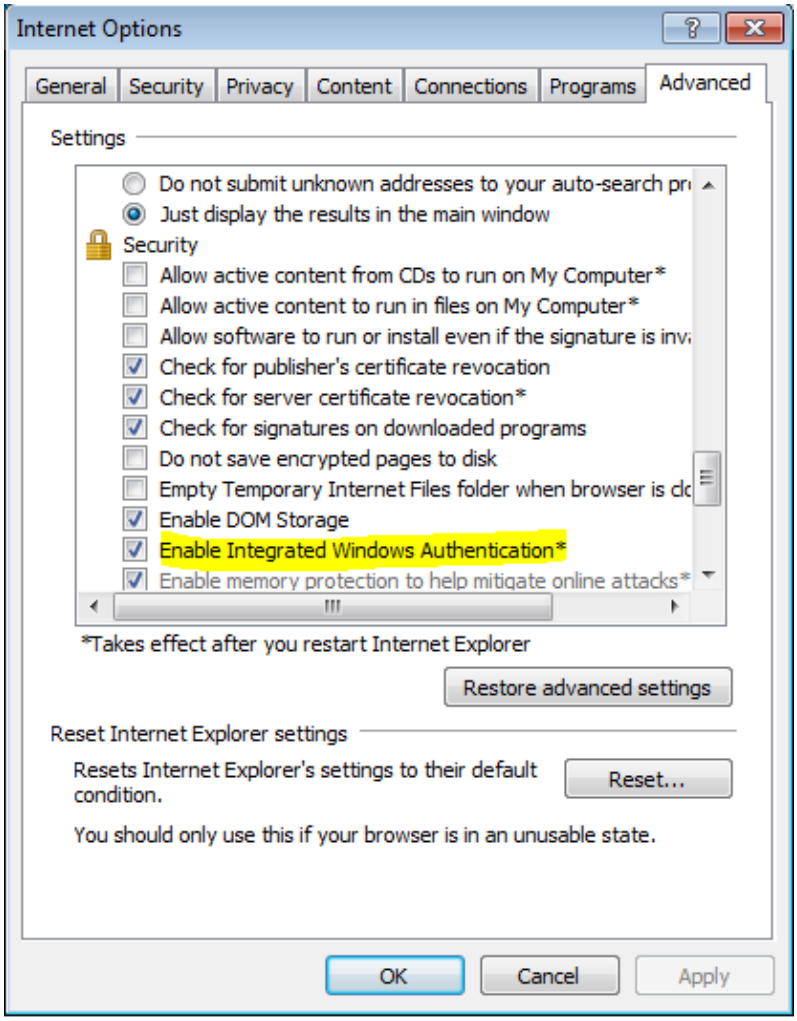
− The calling application does not provide sufficient information to use Kerberos authentication.

− In order to enable the Negotiate process to select the Kerberos protocol for network authentication, the client application must provide an SPN, a User Principal Name (UPN), or a Network Basic Input/Output System (NetBIOS) account name as the target name. Otherwise, the Negotiate process always selects the NTLM protocol as the preferred authentication method.

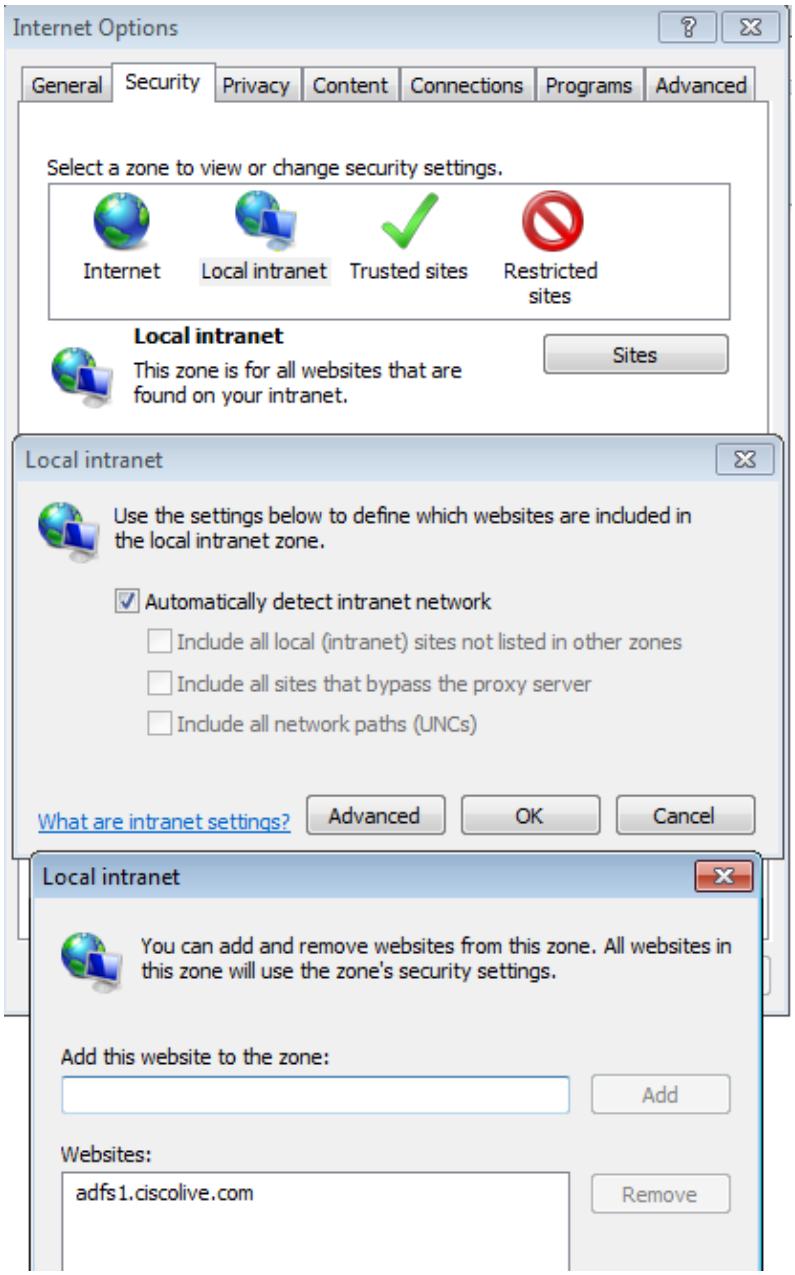
Configure Browser

Microsoft Internet Explorer

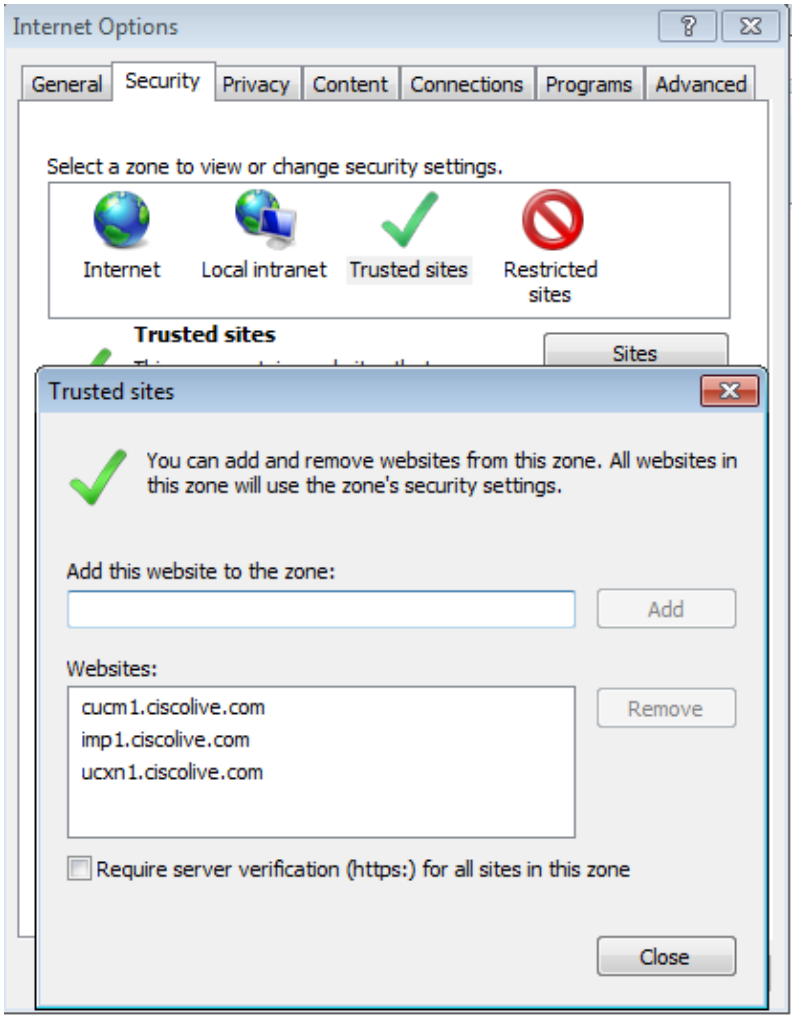
1. Ensure that ***Internet Explorer*** > ***Advanced*** > ***Enable Integrated Windows Authentication*** is checked.



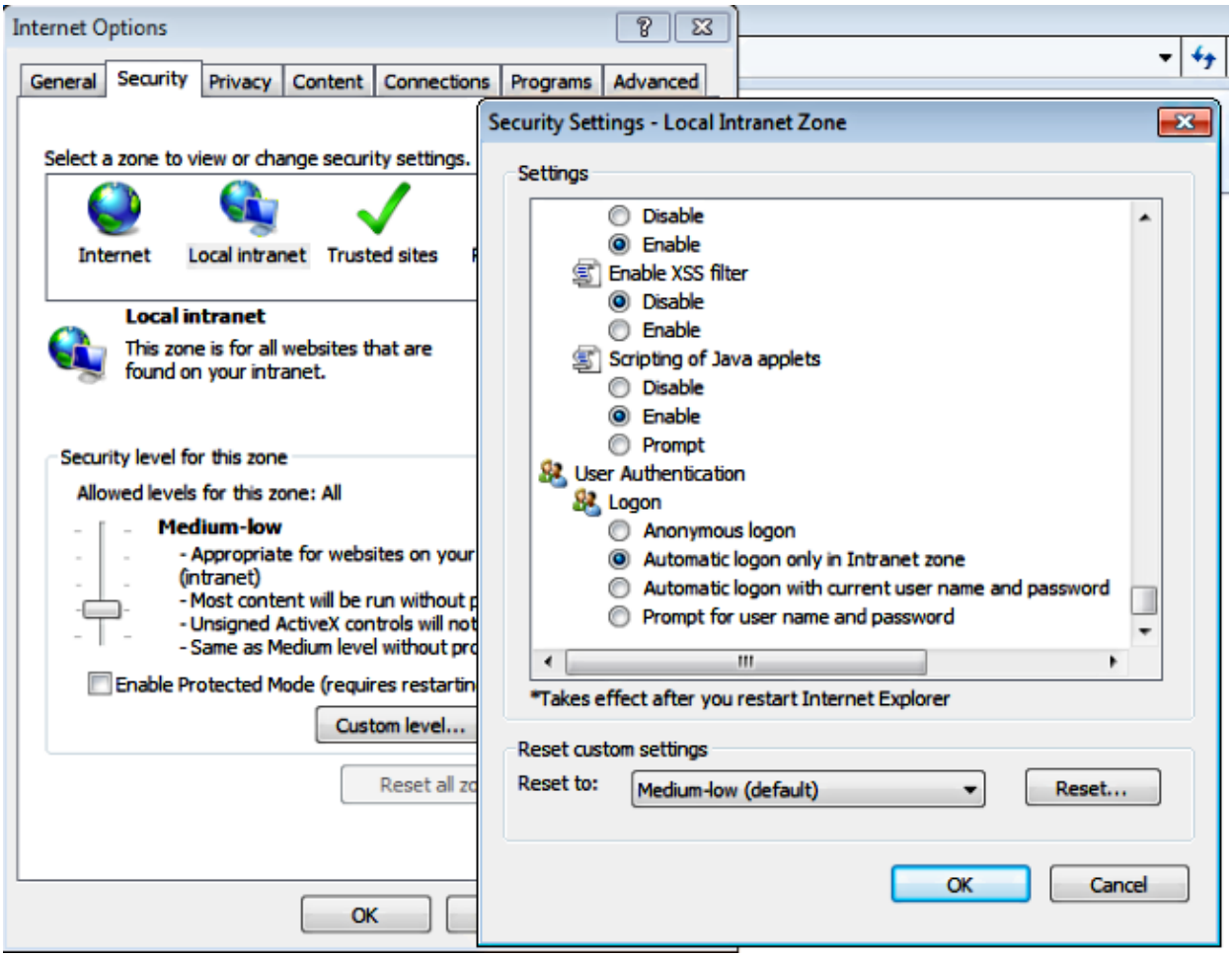
2. Add AD FS URL under ***Security >Intranet zones*** > ***sites***.



3. Add the CUCM, IMP, and Unity hostnames to ***Security >Trusted sites***.

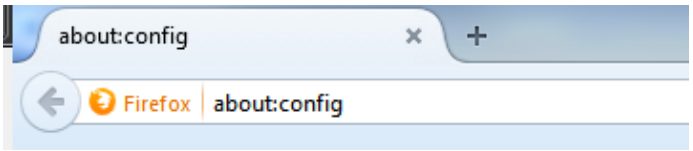


4. Ensure that ***Internet Exporer*** > ***security*** > ***Local Intranet*** > ***Security Settings*** > U***ser Authentication − Logon*** is configured in order to use the logged−in credentials for intranet sites.



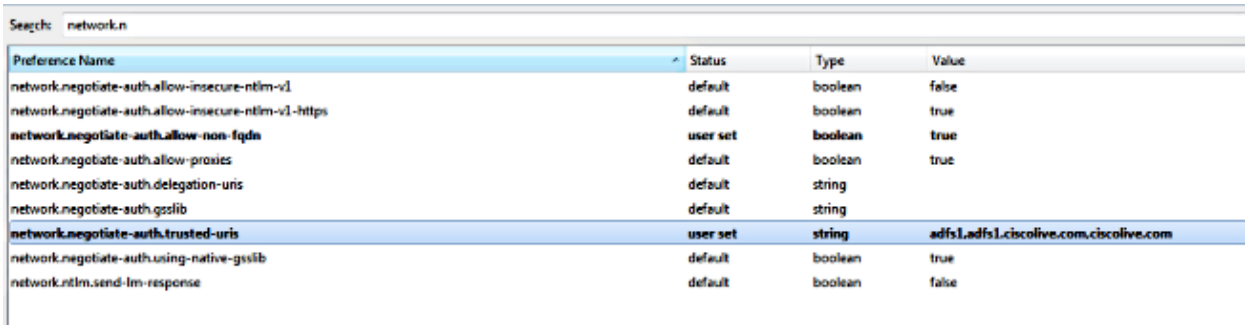
Mozilla FireFox

1. Open Firefox and enter ***about:config*** in the address bar.



2. Click ***I'll be careful, I promise!***

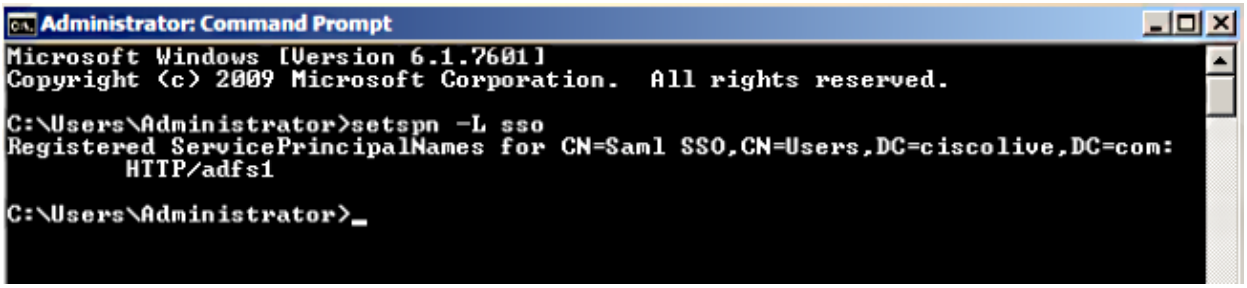
3. Double−click the Preference name ***network.negotiate−auth.allow−non−fqdn*** to ***true*** and ***network.negotiate−auth.trusted−uris*** to ***ciscolive.com,adfs1.ciscolive.com*** in order to modify.



4. Close Firefox and re−open.

Verify

In order to check that the SPNs for the AD FS server are properly created, enter the ***setspn*** command and view the output.



Check if the client machines have Kerberos tickets:

```
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
        KerbTicket 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
        KerbTicket 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>_
```

Complete these steps in order to verify which authentication (Kerberos or NTLM authentication) is in use.

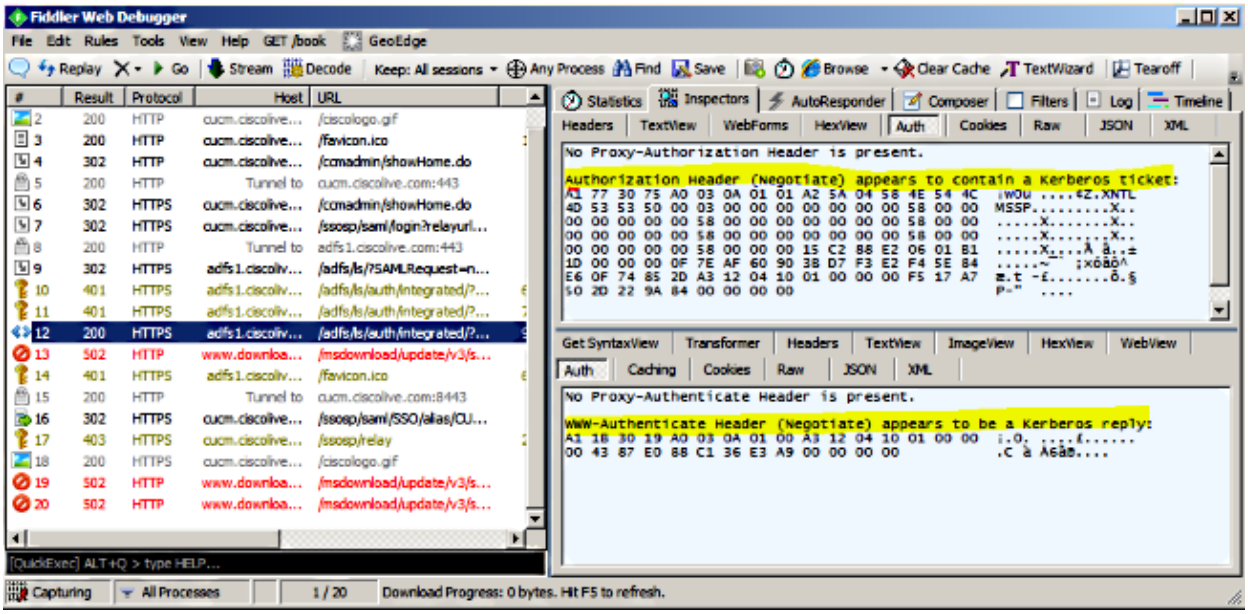
1. Download the Fiddler tool to your client machine and install it.

2. Close all Microsoft Internet Explorer windows.

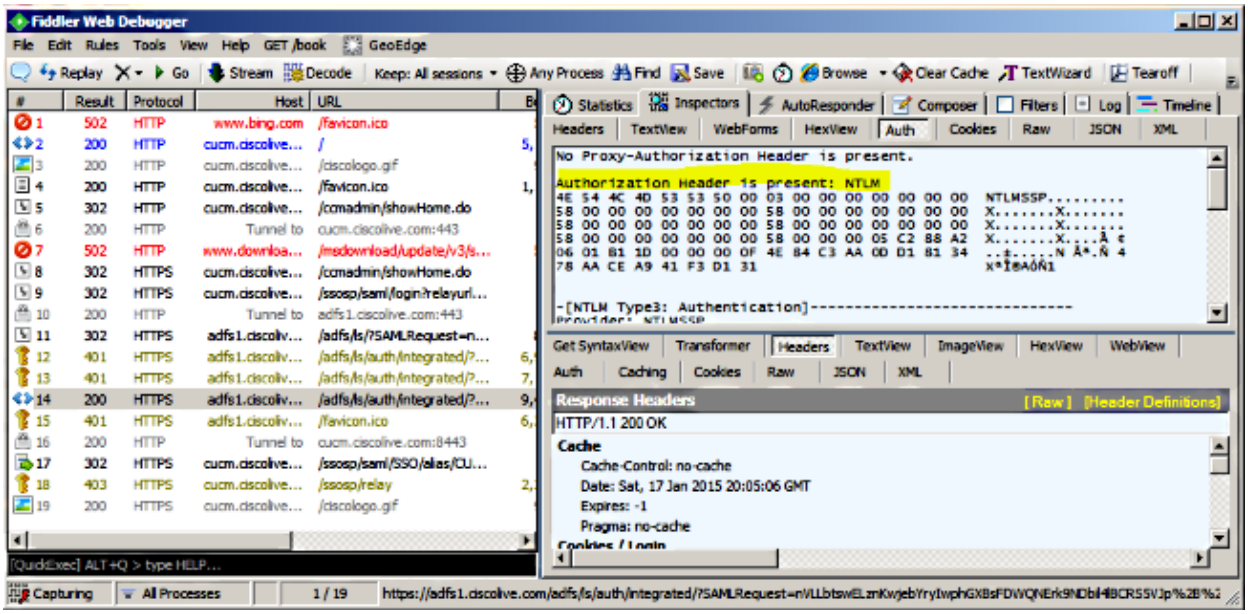
3. Run the Fiddler Tool and check that the ***Capture Traffic*** option is enabled under the File menu. Fiddler works as a pass−through proxy between the client machine and the server and listens to all traffic.

4. Open Microsoft Internet Explorer, browse into your CUCM, and click some 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) and you can see Kerberos as Authentication Mechanism



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



Troubleshoot

If all of the configuration and verification steps are completed as described in this document and you still have login issues, then you must consult a Microsoft Windows Active Directory / AD FS Administrator.

Updated: Jan 21, 2015 Document ID: 118773