

Kerberos 인증으로 SAML SSO 설정 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[AD FS 구성](#)

[브라우저 구성](#)

[Microsoft Internet Explorer](#)

[모질라 파이어폭스](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 Jabber 클라이언트에서 Kerberos 인증(Microsoft Windows만 해당)을 사용하도록 Active Directory 및 AD FS(Active Directory Federation Service) 버전 2.0을 구성하는 방법에 대해 설명합니다. 이 방법을 사용하면 사용자가 Microsoft Windows 로그온을 사용하여 로그인할 수 있으며 자격 증명을 묻는 메시지가 표시되지 않습니다.

주의: 이 문서는 랩 환경을 기반으로 하며 변경 사항이 미치는 영향을 알고 있다고 가정합니다. 변경 사항의 영향을 알아보려면 관련 제품 설명서를 참조하십시오.

사전 요구 사항

요구 사항

Cisco는 다음과 같은 기능을 권장합니다.

- AD FS 버전 2.0이 Cisco Collaboration 제품을 Relying Party Trust로 설치 및 구성
- SAML(Security Assertion Markup Language) SSO(Single Sign-On)를 사용하기 위해 Cisco CUCM(Unified Communications Manager) IM and Presence, Cisco UCXN(Unity Connection) 및 CUCM과 같은 협업 제품

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

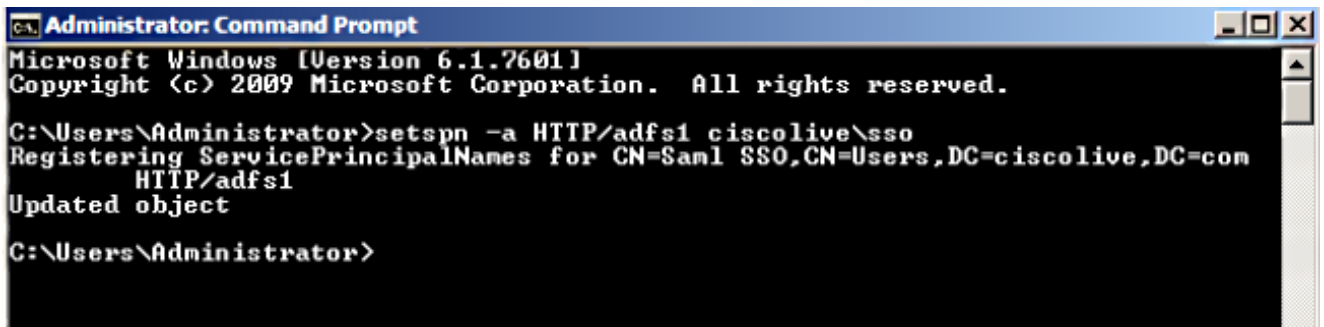
- Active Directory 2008(호스트 이름: ADFS1.ciscolive.com)
- AD FS 버전 2.0(호스트 이름: ADFS1.ciscolive.com)
- CUCM(호스트 이름: CUCM1.ciscolive.com)
- Microsoft Internet Explorer 버전 10
- Mozilla Firefox 버전 34
- Telerik Fiddler 버전 4

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

AD FS 구성

1. Jabber가 설치된 클라이언트 컴퓨터가 티켓을 요청하도록 AD FS 버전 2.0을 SPN(서비스 사용자 이름)으로 구성하여 클라이언트 컴퓨터가 AD FS 서비스와 통신할 수 있게 합니다.



```

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>
  
```

[AD FS 2.0](#)을 참조하십시오. [자세한 내용을 보려면 서비스 계정에 대한 SPN\(servicePrincipalName\)을 구성하는 방법](#)

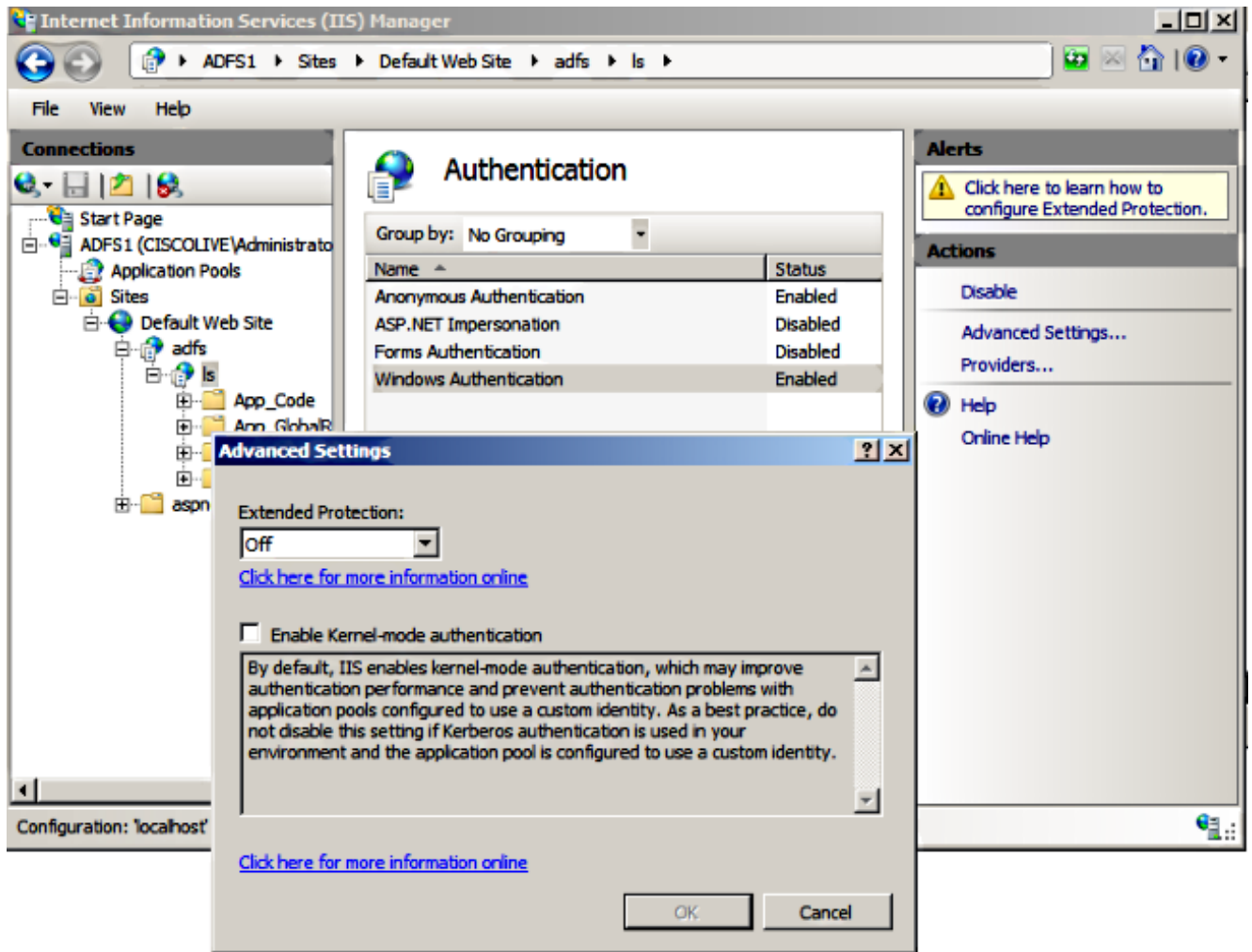
2. AD FS 서비스에 대한 기본 인증 컨피그레이션(C:\inetpub\adfs\ls\web.config에서)이 통합 Windows 인증인지 확인합니다. 양식 기반 인증으로 변경되지 않았는지 확인합니다.

```

<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 sam1="true" wsFederation="true" />
  <homeRealmDiscovery page="HomeRealmDiscovery.aspx" />
  <persistIdentityProviderInformation enabled="true" lifetimeInDays="30" />
  <singleSignOn enabled="true" />
</microsoft.identityserver.web>
  
```

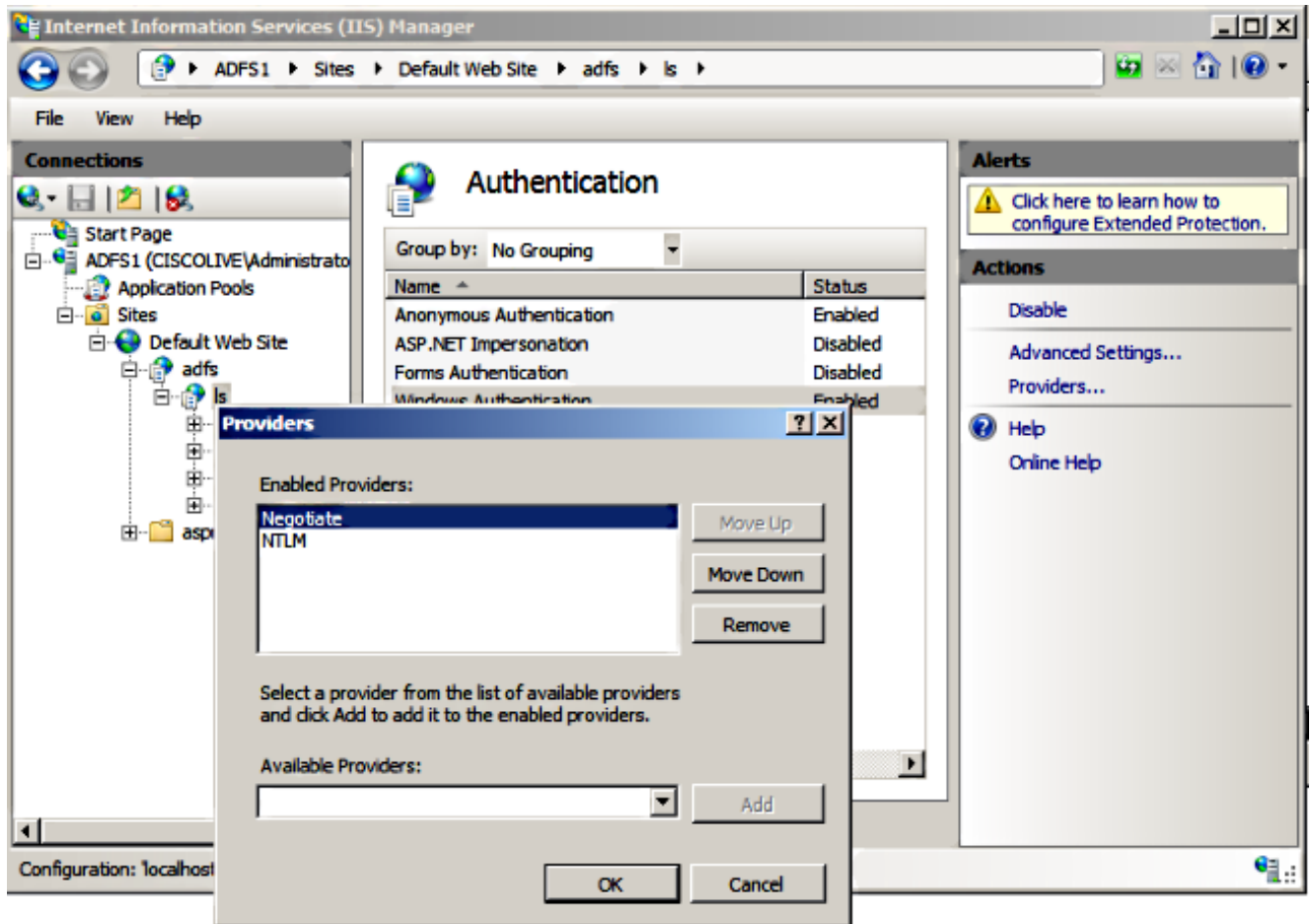
3. Windows 인증을 선택하고 오른쪽 창 아래에서 Advanced Settings를 클릭합니다. Advanced Settings(고급 설정)에서 Enable Kernel-mode authentication(커널 모드 인증 활성화)의 선택을

취소하고 Extended Protection(확장 보호)이 Off(꺼짐)인지 확인하고 OK(확인)를 클릭합니다.



4. 모든 비 Windows 클라이언트는 Kerberos를 사용할 수 없고 NTLM을 사용할 수 없으므로 AD FS 버전 2.0이 Kerberos 프로토콜과 NTLM(NT LAN Manager) 프로토콜을 모두 지원하는지 확인하십시오.

오른쪽 창에서 Providers(공급자)를 선택하고 Enabled Providers(활성화된 공급자) 아래에 Negotiate(협상) 및 NTLM이 있는지 확인합니다.



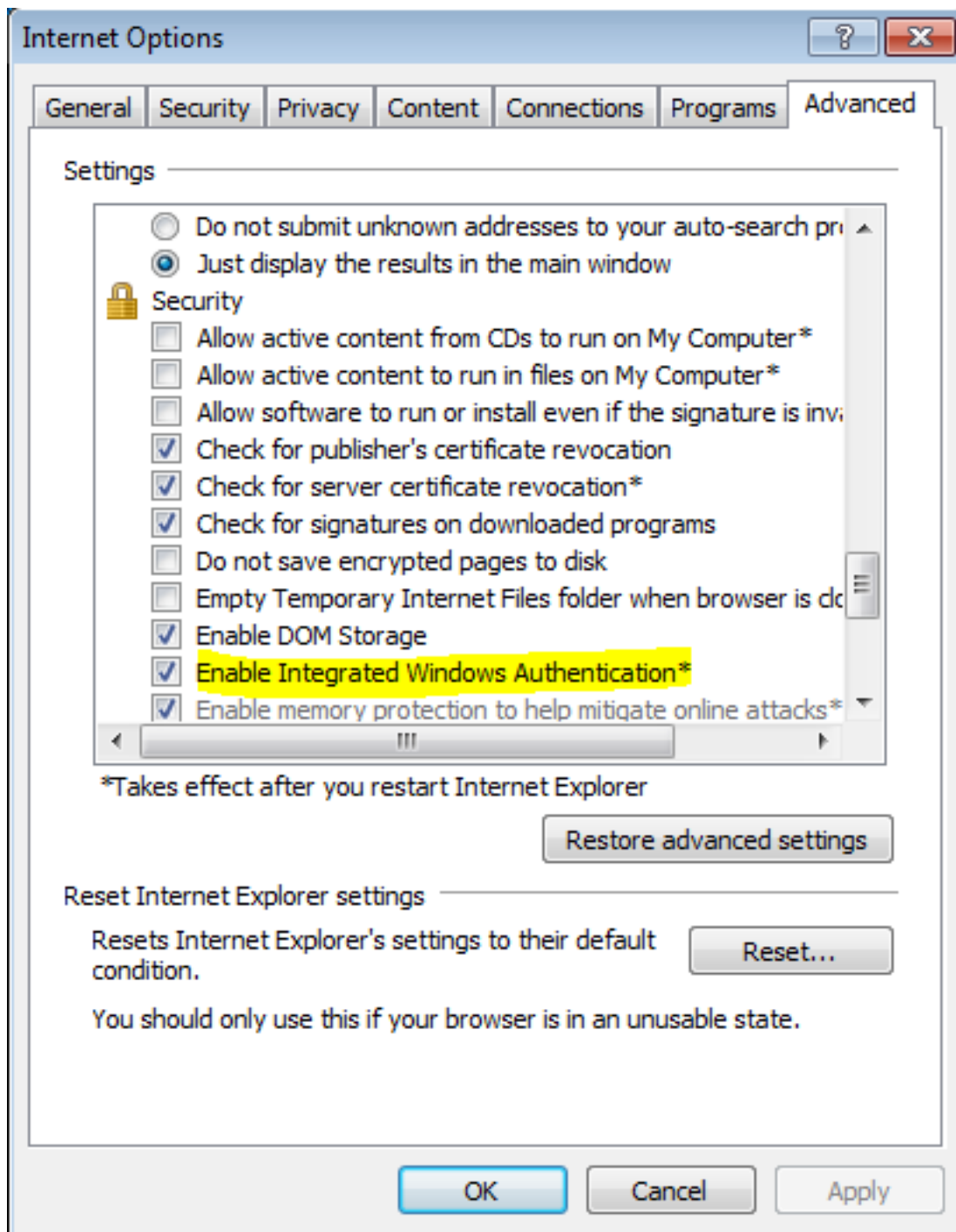
참고: AD FS는 클라이언트 요청을 인증하기 위해 통합 Windows 인증을 사용할 때 협상 보안 헤더를 전달합니다. Negotiate 보안 헤더를 사용하면 클라이언트가 Kerberos 인증과 NTLM 인증 사이에서 선택할 수 있습니다. 협상 프로세스는 다음 조건 중 하나가 참인 경우를 제외하고 Kerberos 인증을 선택합니다.

- 인증과 관련된 시스템 중 하나가 Kerberos 인증을 사용할 수 없습니다.
- 발신 응용 프로그램이 Kerberos 인증을 사용할 수 있는 충분한 정보를 제공하지 않습니다.
- 협상 프로세스에서 네트워크 인증을 위해 Kerberos 프로토콜을 선택할 수 있도록 하려면 클라이언트 응용 프로그램이 대상 이름으로 SPN, UPN(사용자 계정 이름) 또는 NetBIOS(Network Basic Input/Output System) 계정 이름을 제공해야 합니다. 그렇지 않으면 협상 프로세스는 항상 기본 인증 방법으로 NTLM 프로토콜을 선택합니다.

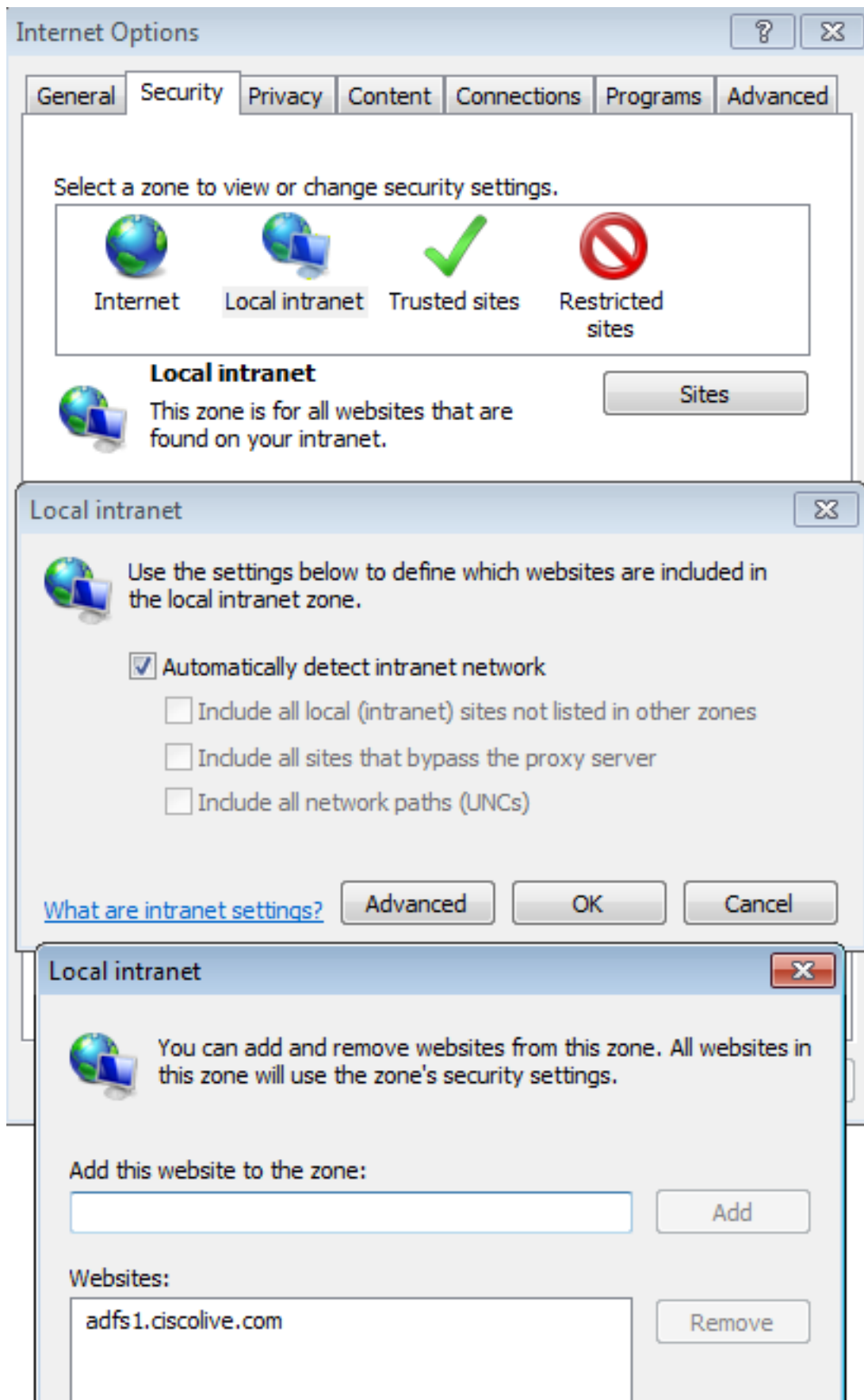
브라우저 구성

Microsoft Internet Explorer

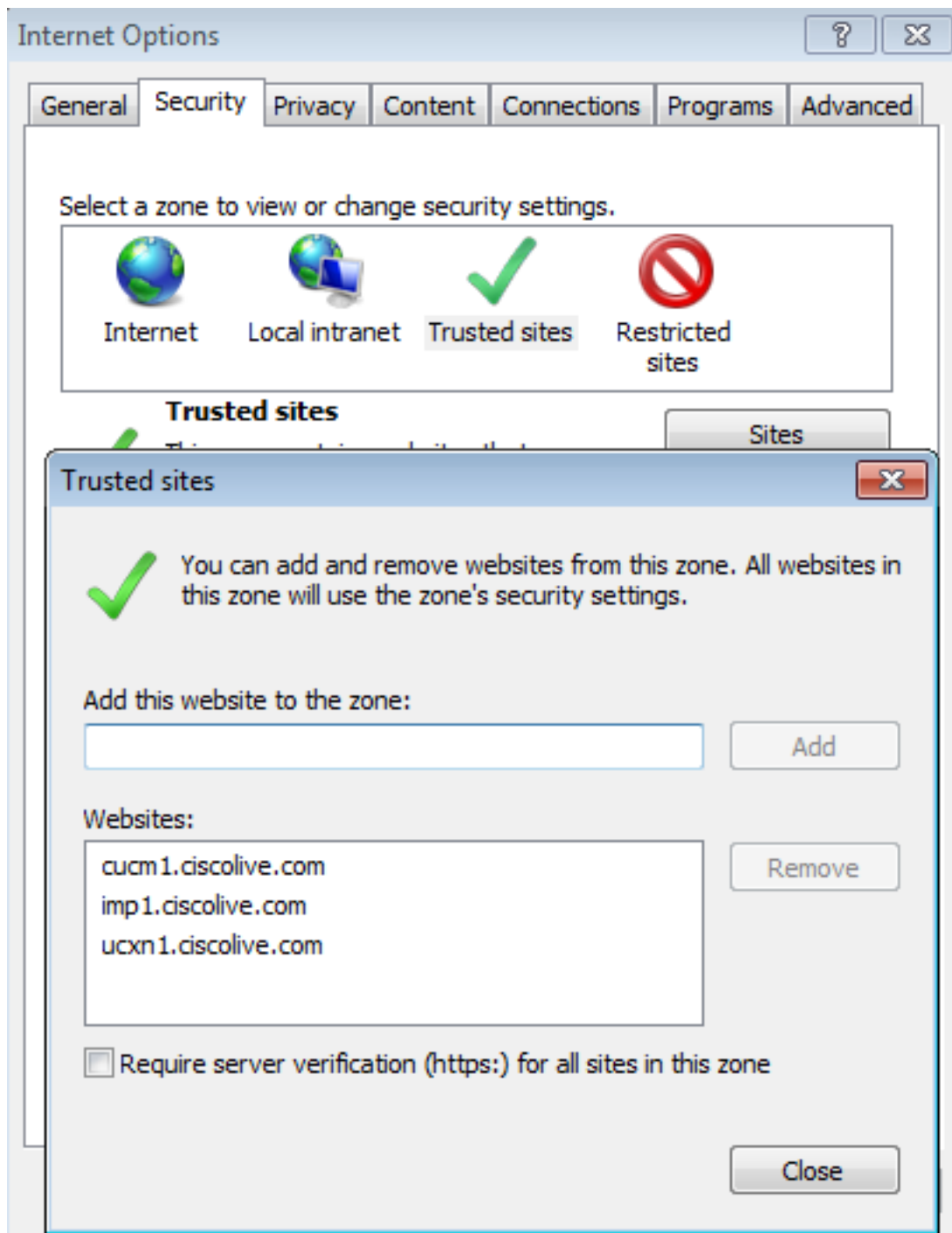
1. Internet Explorer > Advanced > Enable Integrated Windows Authentication(통합 Windows 인증 사용)이 선택되어 있는지 확인합니다.



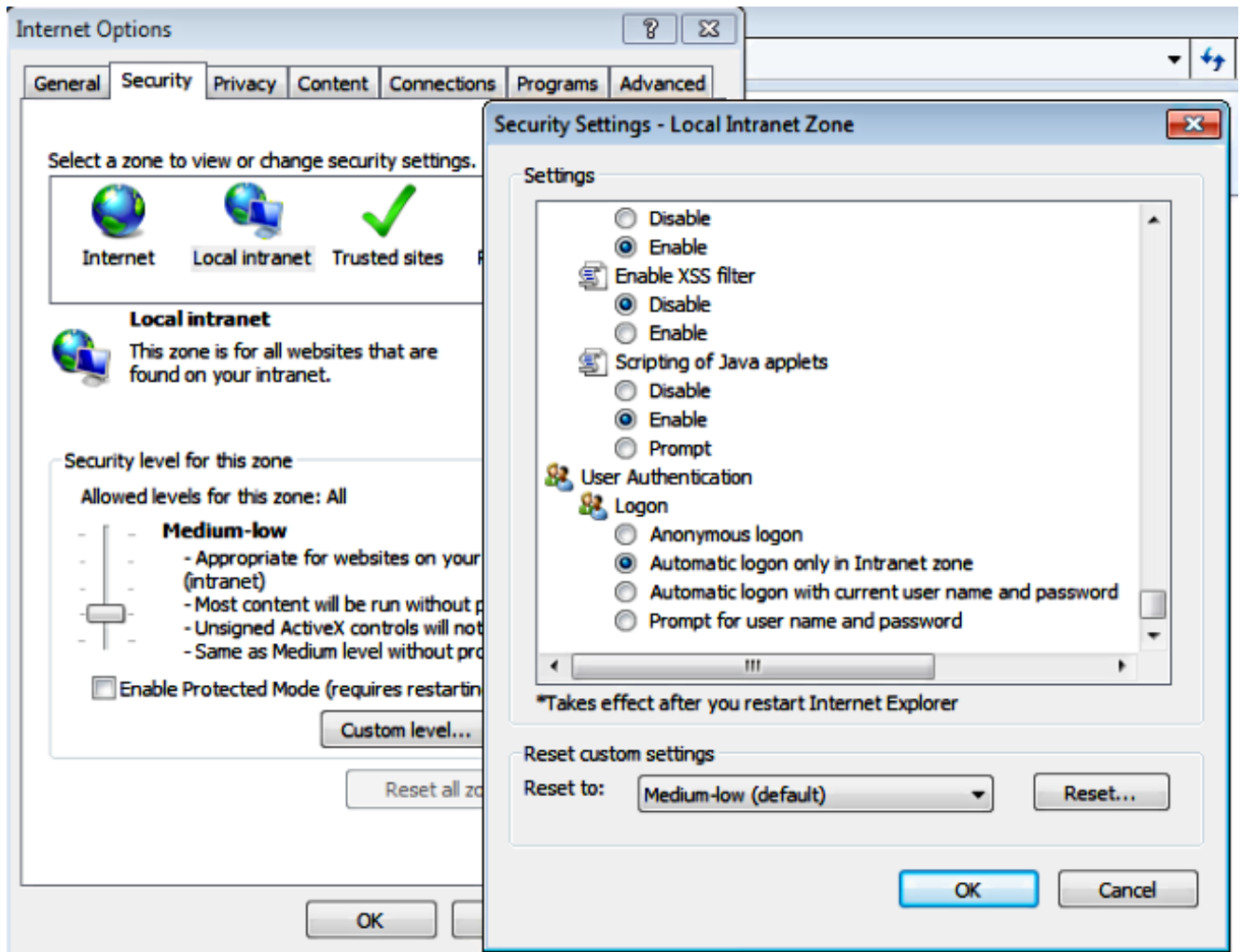
2. Security(보안) > Intranet zones(인트라넷 영역) > sites(사이트)에서 AD FS URL을 추가합니다.



3. CUCM, IMP 및 Unity 호스트 이름을 Security(보안) >Trusted sites(신뢰할 수 있는 사이트)에 추가합니다.

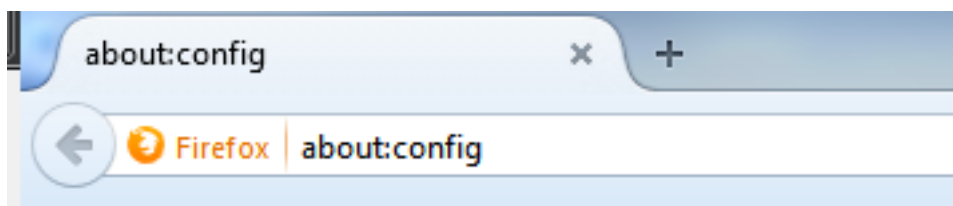


4. Internet Explorer > **security** > **Local Intranet** > **Security Settings** > **User Authentication - Logon**이 인트라넷 사이트에 로그인된 자격 증명을 사용하도록 구성되어 있는지 확인합니다.



모질라 파이어폭스

1. Firefox를 열고 주소 표시줄에 **about:config**를 입력합니다.



2. I'll be 주의, I promise!(주의하겠습니다, 약속합니다!)를 클릭합니다.



- 기본 설정 이름 `network.negotiate-auth.allow-non-fqdn`을 `true`로 두 번 클릭하고 `ciscolive.com`, `adfs1.ciscolive.com`에 대한 `network.negotiate-auth.trusted-uris`를 클릭하여 수정합니다.

| 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 |

- Firefox를 닫고 다시 엽니다.

다음을 확인합니다.

AD FS 서버의 SPN이 제대로 만들어졌는지 확인하려면 `setspn` 명령을 입력하고 출력을 봅니다.

```
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>_
```

클라이언트 컴퓨터에 Kerberos 티켓이 있는지 확인합니다.

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

Current LogonId is 0:0xabc6d
Cached Tickets: (2)

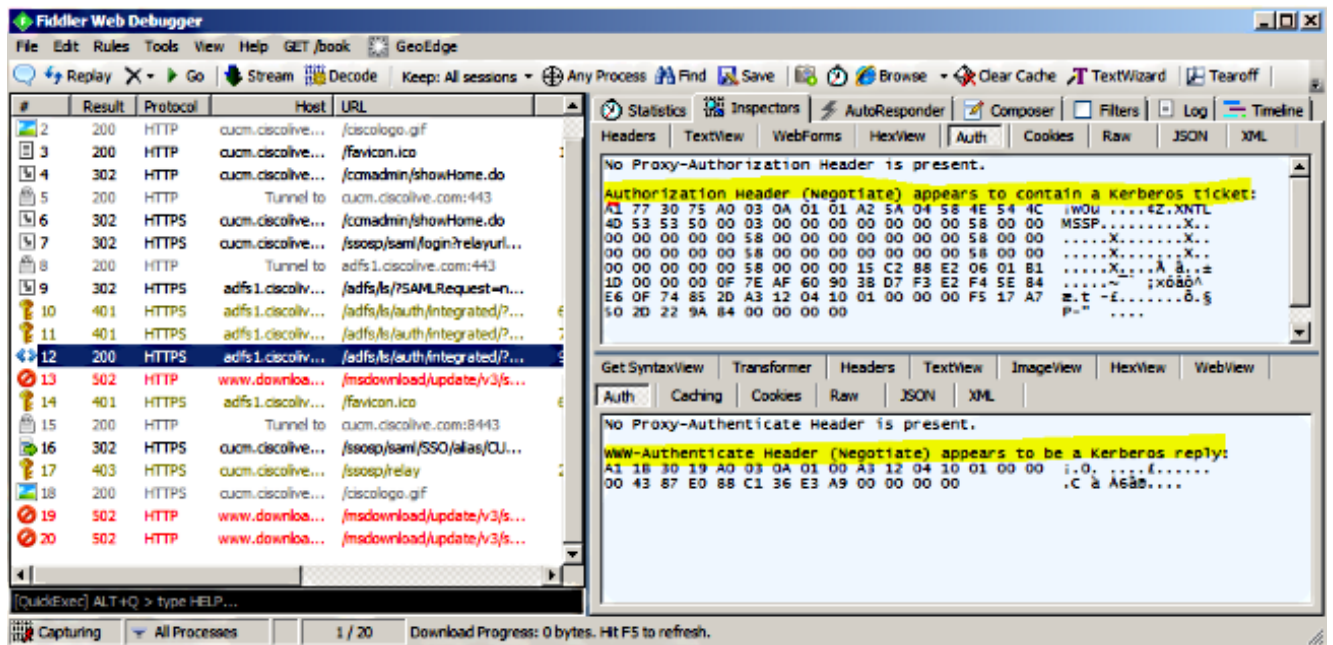
#0> Client: user1 @ CISCOLIVE.COM
Server: krbtgt/CISCOLIVE.COM @ CISCOLIVE.COM
KerberosTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
Start Time: 1/17/2015 20:52:47 (local)
End Time: 1/18/2015 6:52:47 (local)
Renew Time: 1/24/2015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

#1> Client: user1 @ CISCOLIVE.COM
Server: host/pci.ciscolive.com @ CISCOLIVE.COM
KerberosTicket 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

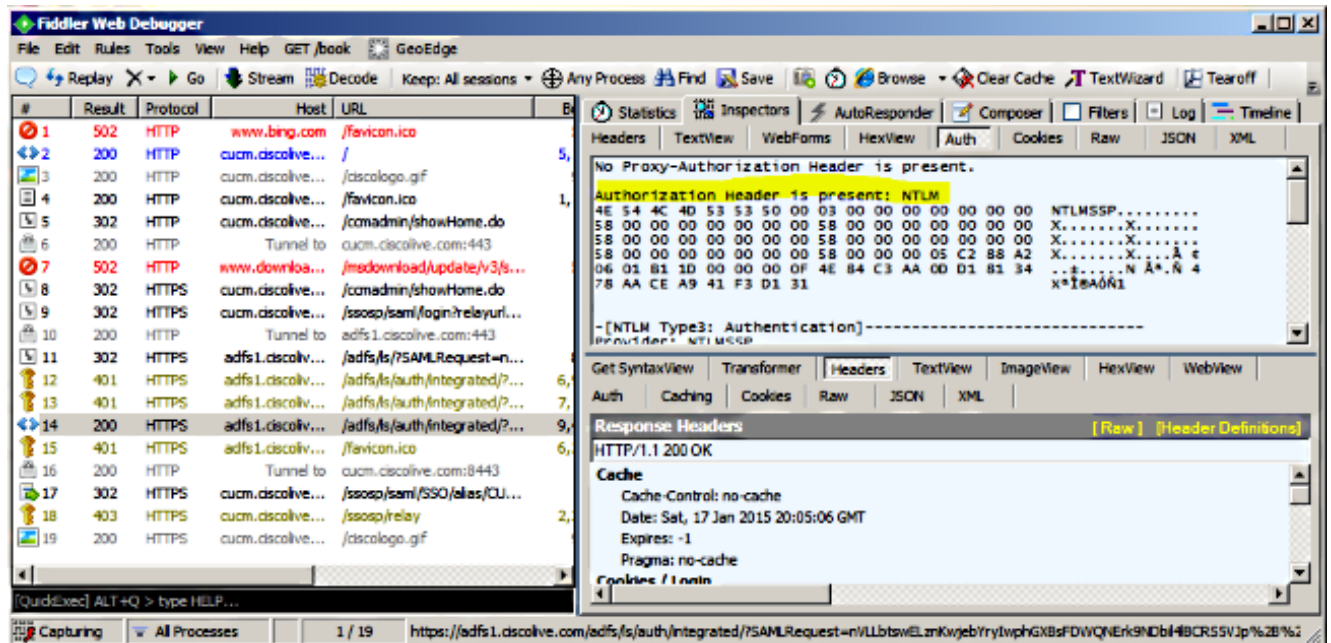
C:\Users\user1.CISCOLIVE>_
```

사용 중인 인증(Kerberos 또는 NTLM 인증)을 확인하려면 다음 단계를 완료하십시오.

1. 클라이언트 컴퓨터에 Windows Installer 도구를 다운로드하여 설치합니다.
2. 모든 Microsoft Internet Explorer 창을 닫습니다.
3. File Tool을 실행하고 File 메뉴에서 **Capture Traffic** 옵션이 활성화되었는지 확인합니다.
Fiddler는 클라이언트 시스템과 서버 간에 통과 프록시 역할을 하며 모든 트래픽을 수신합니다.
4. Microsoft Internet Explorer를 열고 CUCM을 찾은 다음 일부 링크를 클릭하여 트래픽을 생성합니다.
5. Windows 주 창을 다시 참조하여 Frames(결과200(성공) 중 하나를 선택하고 Kerberos를 인증 메커니즘으로 볼 수 있습니다.



6. 인증 유형이 NTLM이면 프레임 시작에 **협상 - NTLMSSP**가 표시됩니다(아래 참조).



문제 해결

이 문서에 설명된 대로 모든 컨피그레이션 및 확인 단계가 완료되었지만 로그인 문제가 있는 경우 Microsoft Windows Active Directory/AD FS 관리자에게 문의해야 합니다.