Jabber 컨피그레이션을 위한 최종 사용자 SAML SSO용 ADFS 2.0이 포함된 Kerberos 예

목차

소개

이 문서에서는 ADFS(Active Directory Federation Services) 2.0을 사용하여 Kerberos를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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.

배경 정보

SAML(End User Security Assertion Markup Language) SSO(Single Sign On) 구성을 사용하려면 Jabber용 최종 사용자 SAML SSO가 도메인 인증과 작동하도록 Kerberos를 구성해야 합니다 .SAML SSO가 Kerberos와 함께 구현되면 LDAP(Lightweight Directory Access Protocol)는 모든 권

한 부여 및 사용자 동기화를 처리하며 Kerberos는 인증을 관리합니다.Kerberos는 LDAP 지원 인스턴스와 함께 사용할 인증 프로토콜입니다.

Active Directory 도메인에 가입된 Microsoft Windows 및 Macintosh 시스템에서 사용자는 사용자 이름 또는 비밀번호를 입력하지 않고도 Cisco Jabber에 원활하게 로그인할 수 있으며 로그인 화면도 볼 수 없습니다.컴퓨터의 도메인에 로그인하지 않은 사용자도 표준 로그인 양식을 볼 수 있습니다.

인증은 운영 체제에서 전달된 단일 토큰을 사용하므로 리디렉션이 필요하지 않습니다.구성된 KDC(Key Domain Controller)에 대해 토큰이 확인되며, 유효한 경우 사용자가 로그인됩니다.

구성

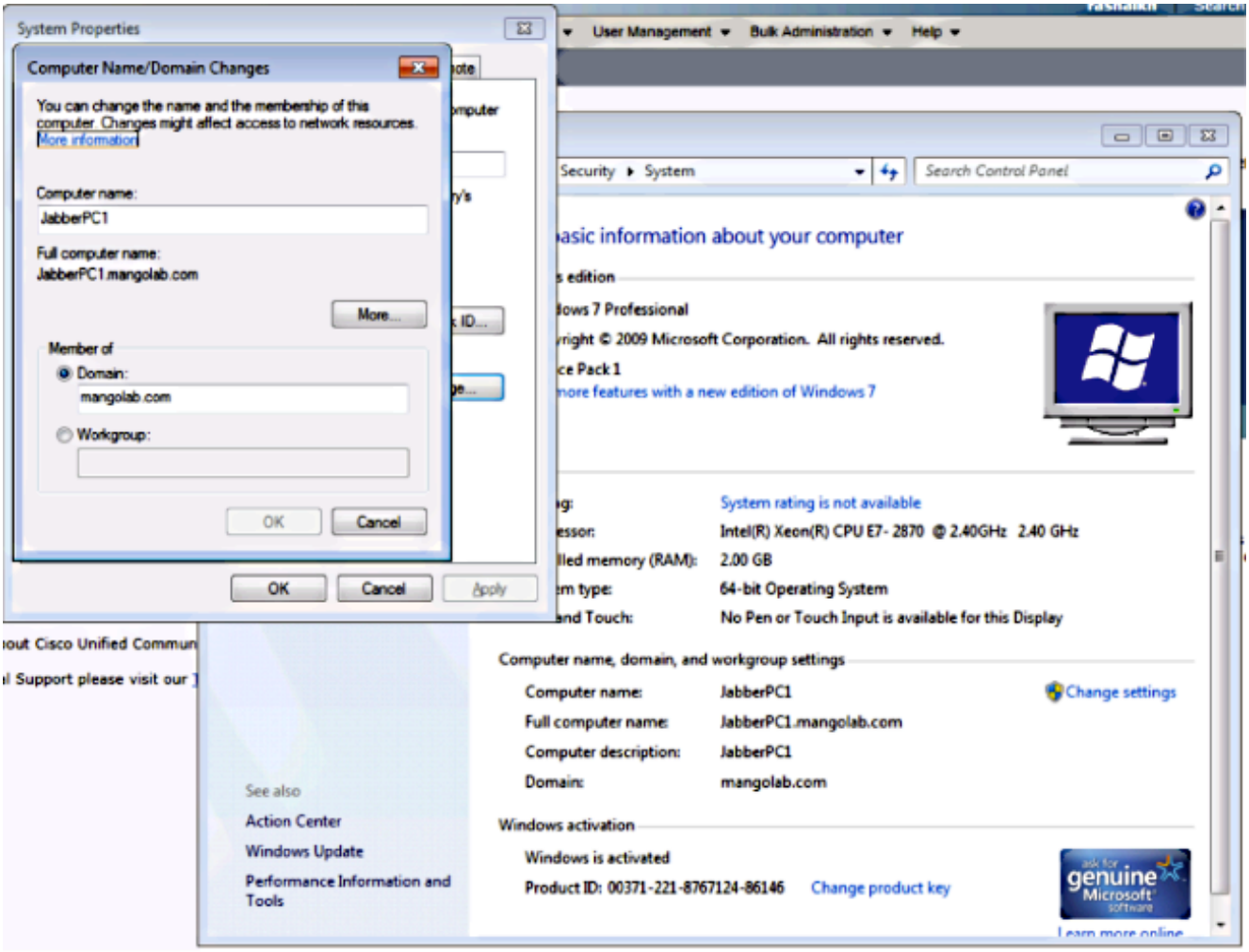
다음은 ADFS 2.0으로 Kerberos를 구성하는 절차입니다.

1. 컴퓨터에 Microsoft Windows Server 2008 R2를 설치합니다.
2. ADDS(Active Directory Domain Services) 및 ADFS를 동일한 컴퓨터에 설치합니다.
3. Microsoft Windows Server 2008 R2 설치 컴퓨터에 IIS(인터넷 정보 서비스)를 설치합니다.
4. IIS용 자체 서명 인증서를 만듭니다.
5. 자체 서명 인증서를 IIS로 가져와 HTTPS 서버 인증서로 사용합니다.
6. 다른 컴퓨터에 Microsoft Windows7을 설치하고 클라이언트로 사용합니다.

   DNS(Domain Name Server)를 ADDS를 설치한 시스템으로 변경합니다.

   ADDS 설치에서 만든 도메인에 이 컴퓨터를 추가합니다.

   시작으로 **이동합니다**.**컴퓨터**를 마우스 오른쪽 단추로 클릭합니다.속성**을 클릭합니다**.창 오른쪽에서 Change Settings를 클릭합니다.**컴퓨터 이름 탭**을 클릭합니다.**변경**을 **클릭합니다**.생성한 도메인을 추가합니다.



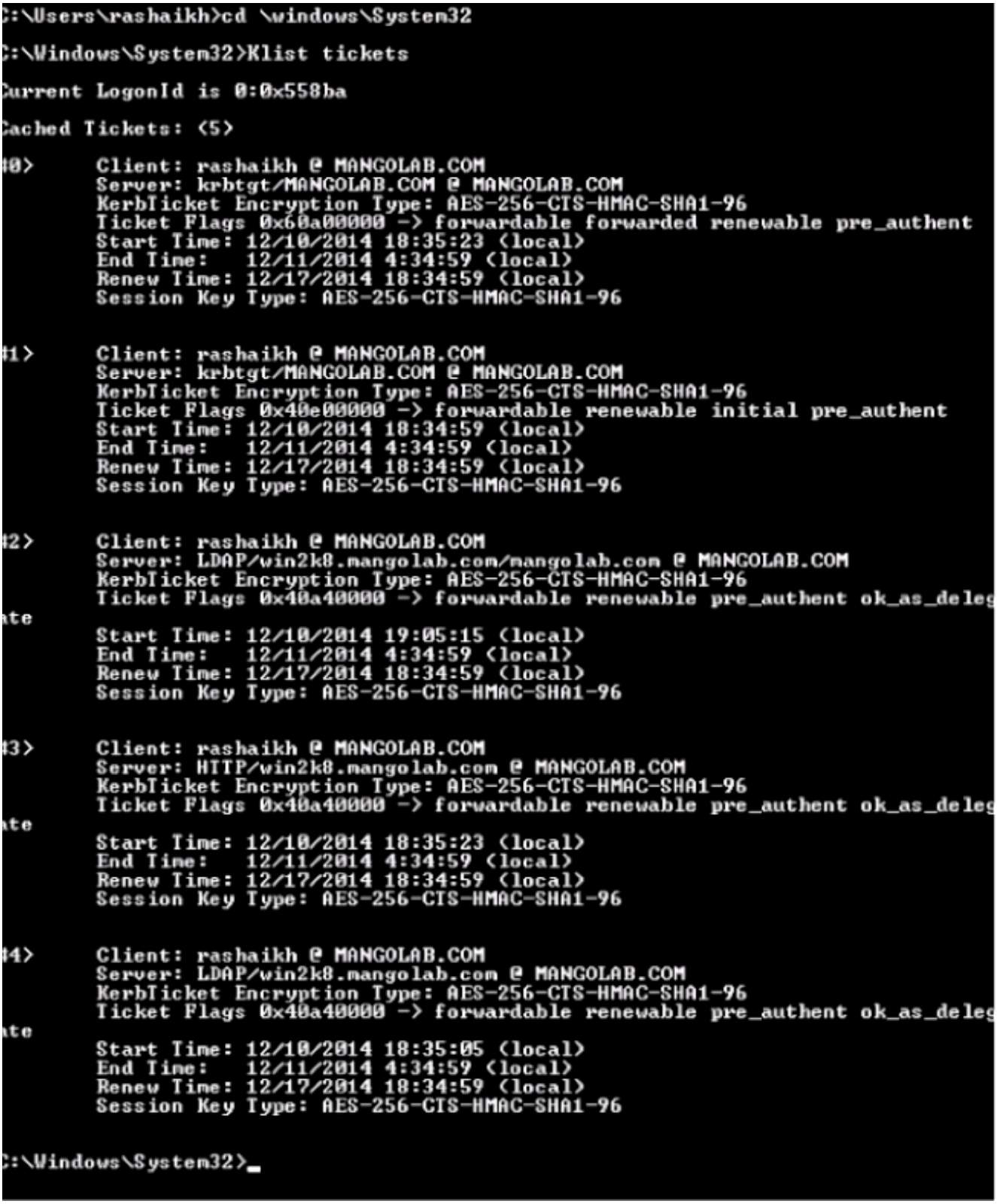
7. Kerberos 서비스가 두 컴퓨터에서 생성되는지 확인합니다.

   서버 시스템에서 관리자로 로그인하고 명령 프롬프트를 엽니다.그런 다음 다음 다음 명령을 실행합니다.

   cd \windows\System32Klist 티켓

```
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
```

   클라이언트 시스템에서 도메인 사용자로 로그인하고 동일한 명령을 실행합니다.



8. ADDS를 설치한 컴퓨터에 ADFS Kerberos ID를 만듭니다.

   Microsoft Windows 도메인(예: Microsoft Windows 도메인 컨트롤러)에 로그인한 Microsoft Windows 관리자는 ADFS Kerberos ID를 생성합니다.ADFS HTTP 서비스에는 다음 형식의 SPN(서비스 사용자 이름)이라는 Kerberos ID가 있어야 합니다 .**HTTP/DNS_name_of_ADFS_server**.

   이 이름은 ADFS HTTP 서버 인스턴스를 나타내는 Active Directory 사용자에게 매핑되어야 합니다.Microsoft Windows 2008 Server에서 기본적으로 사용할 수 있는 Microsoft Windows

setspn 유틸리티를 사용합니다.

절차 ADFS 서버의 SPN을 등록합니다.Active Directory 도메인 컨트롤러에서 setspn 명령을 실행합니다.

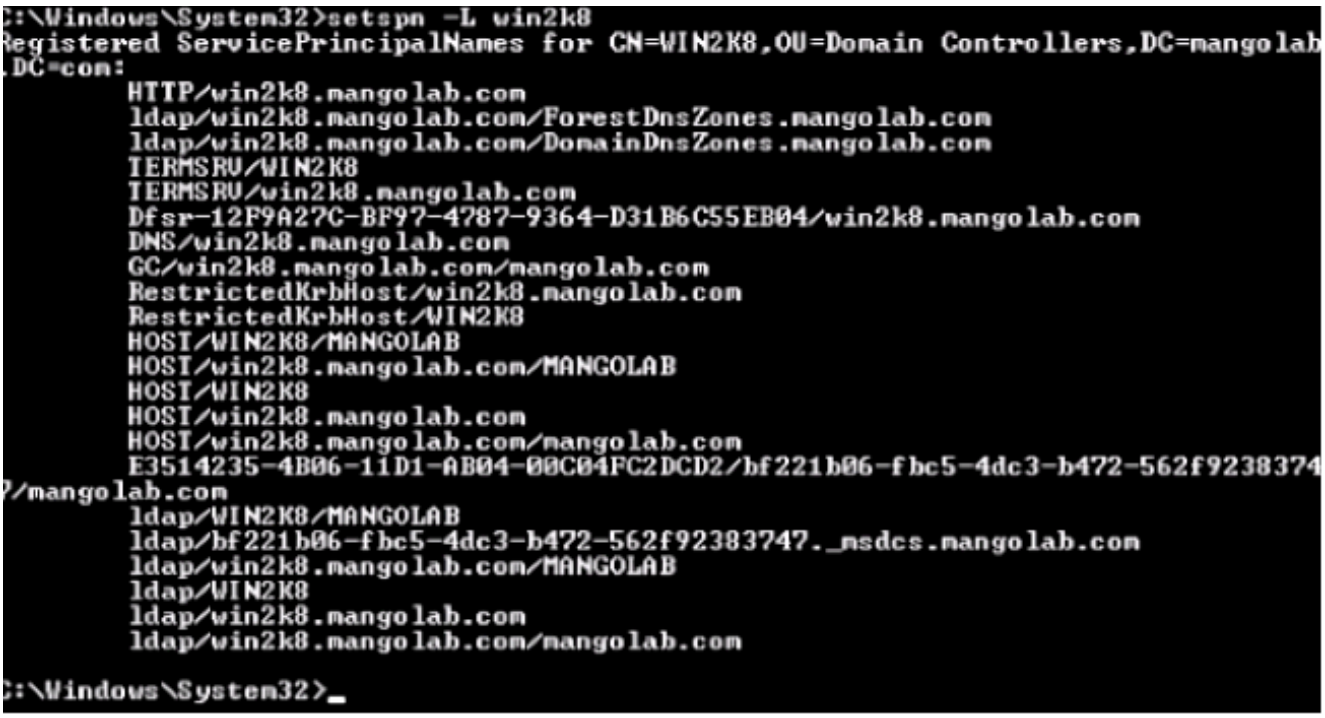
예를 들어 ADFS 호스트가 adfs01.us.renoverations.com이고 Active Directory 도메인이 US.REFRESH.COM인 경우 명령은 다음과 같습니다.

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

SPN의 HTTP/부분은 HTTPS인 SSL(Secure Sockets Layer)에서 일반적으로 ADFS 서버에 액세스하지만 적용됩니다.

setspn 명령을 사용하여 ADFS 서버의 SPN이 제대로 만들어졌는지 확인하고 출력을 봅니다.

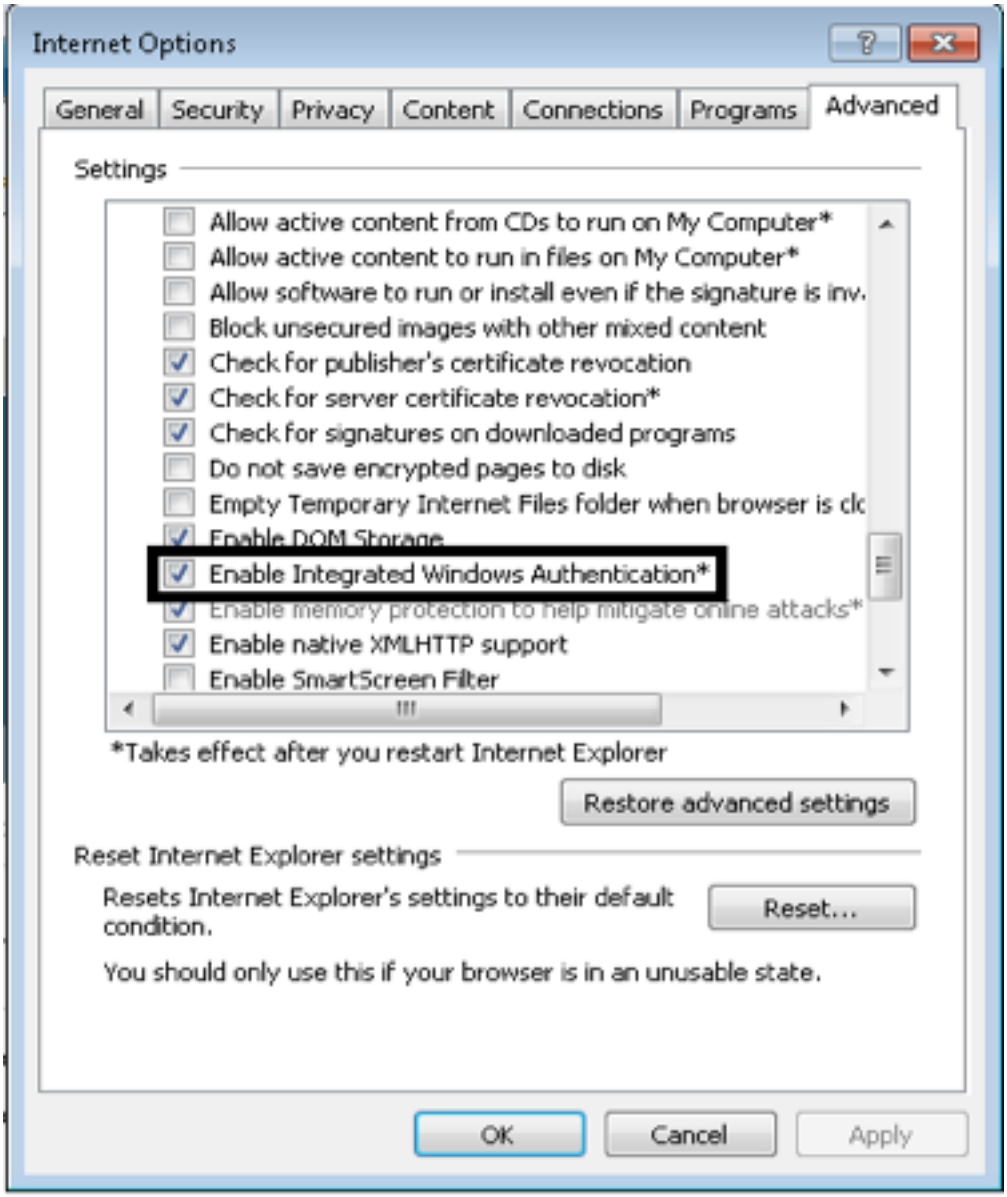
```
setspn -L
```



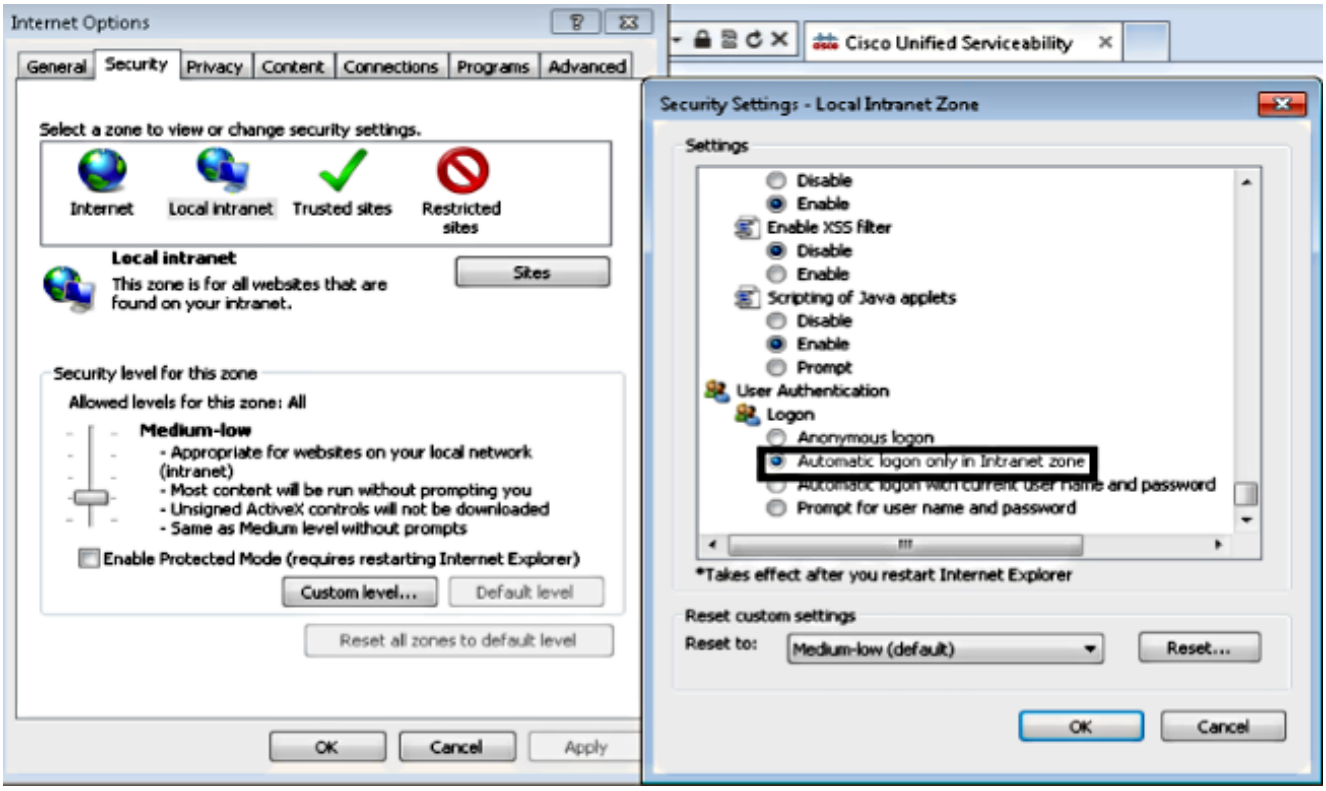
9. Microsoft Windows 클라이언트의 브라우저 설정을 구성합니다.

통합 Windows 인증을 **활성화하려면 Tools > InternetOptions > Advanced**로 이동합니다.

Enable Integrated **Windows Authentication 확인란을 선택합니다**.

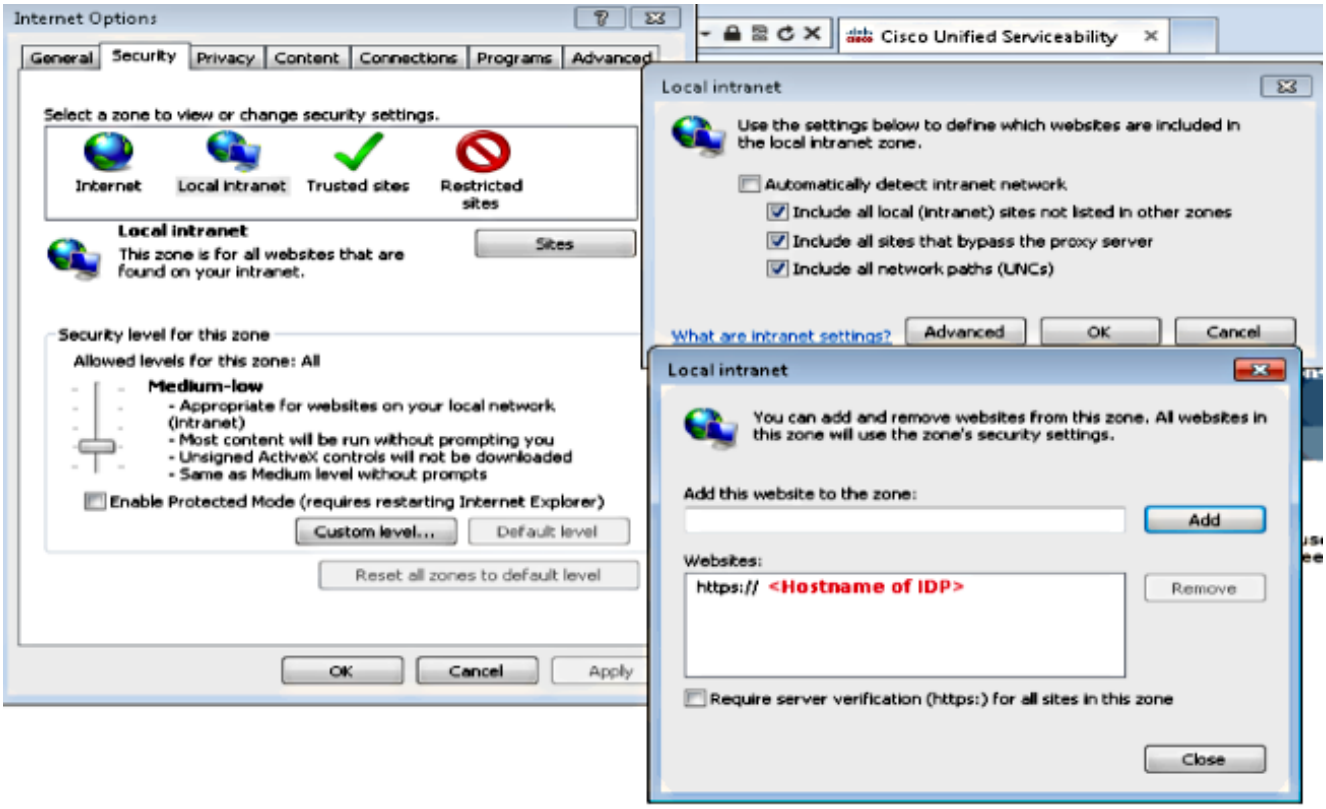


인트라넷 영역에서 자동 로그온만**을** 선택하려면 **도구 > 인터넷 옵션 > 보안 > 로컬 인트라넷 > 사용자 지정 수준**으로 **이동합니다**.

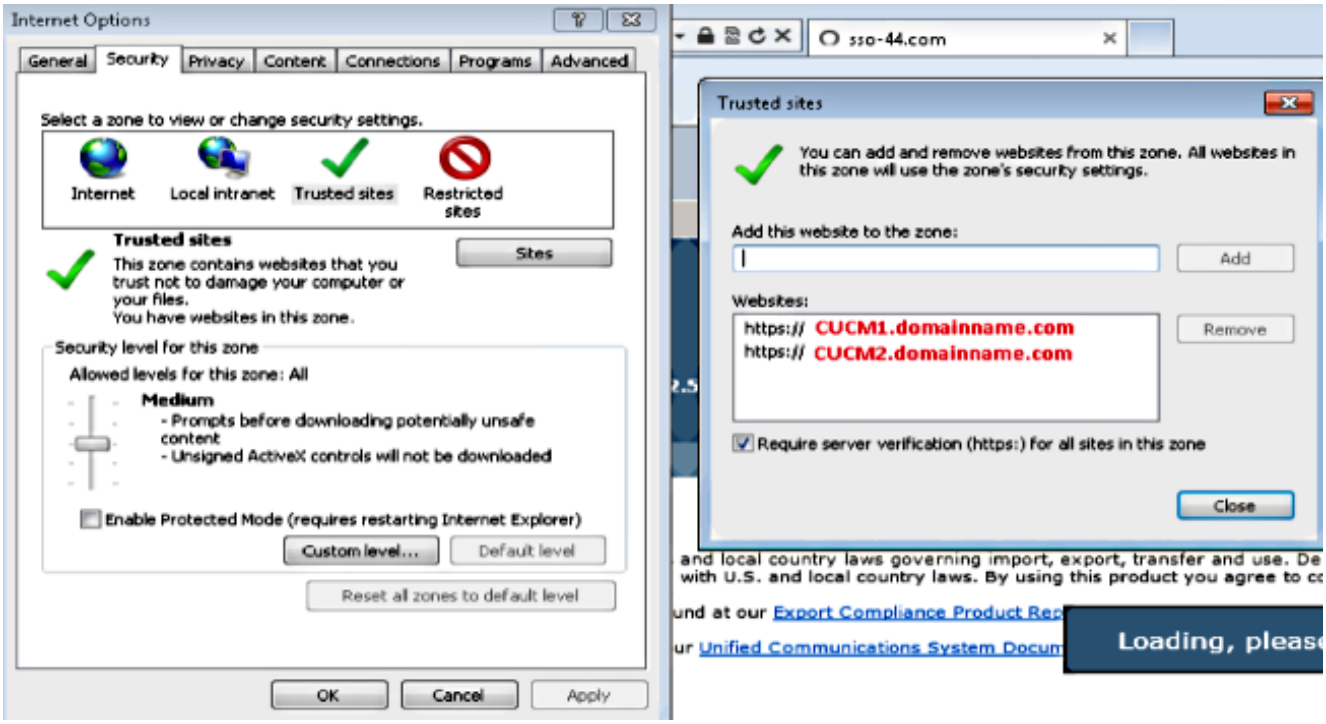


Tools(**툴**) > **Internet Options(인터넷 옵션) > Security(보안) > Local intranet(로컬 인트라넷) > Sites(사이트) > Advanced(고급)로 이동하여** IDP(Intrusion Detection & Prevention) URL을 로컬 인트라넷 사이트에 추가합니다.

참고:로컬 인트라넷 대화 상자에서 모든 확인란을 선택하고 **고급 탭**을 클릭합니다.



CUCM 호스트 이름**을 신뢰할 수 있는 사이트에** 추가하려면 Tools(툴) > Security(보안) > Trusted sites(신뢰할 수 있는 사이트) > Sites(사이트)로 이동합니다.



다음을 확인합니다.

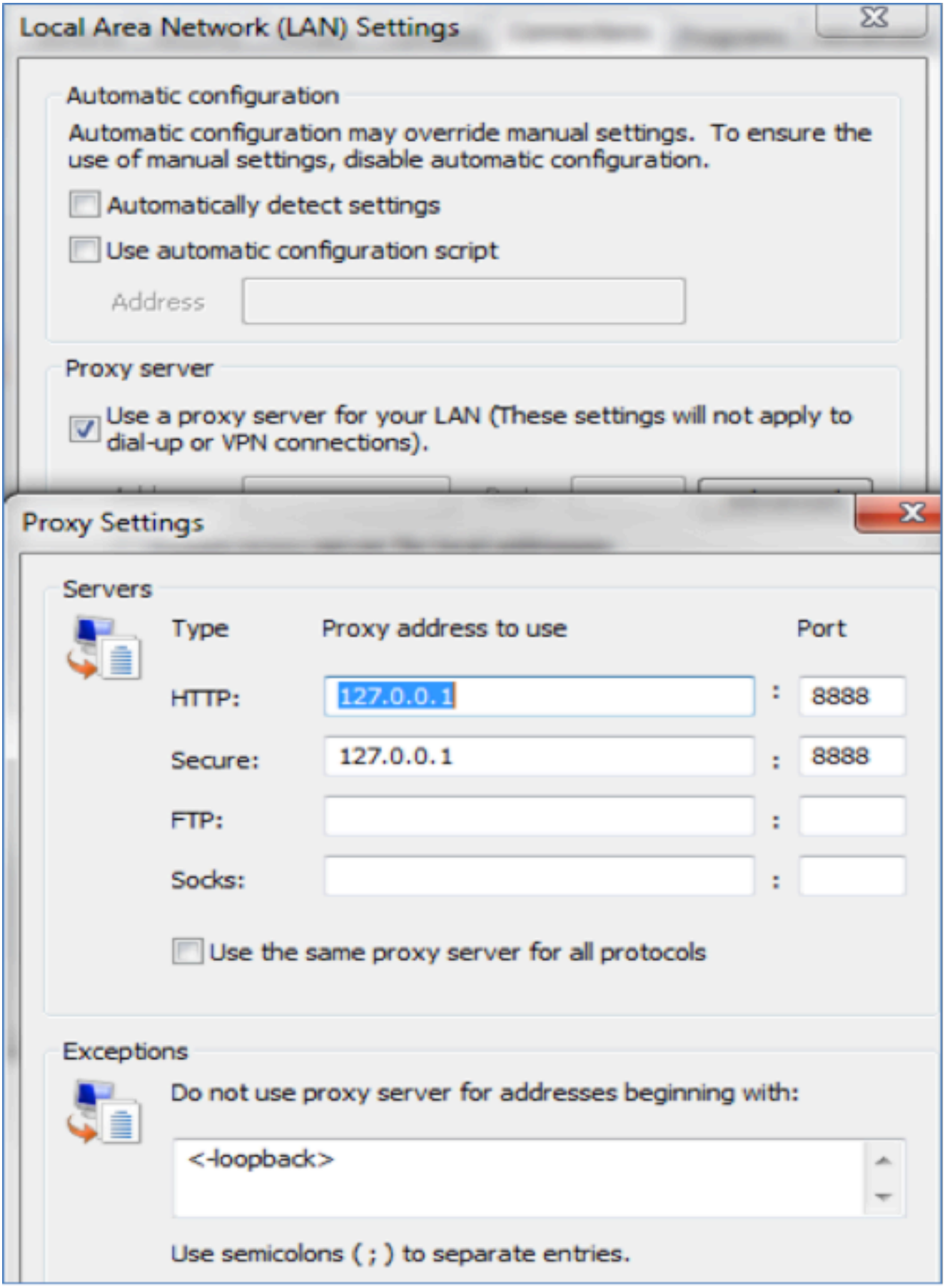
이 섹션에서는 어떤 인증(Kerberos 또는 NTLM(NT LAN Manager) 인증을 사용하는지 확인하는 방법에 대해 설명합니다.

1. 클라이언트 컴퓨터에 Windows Media Player 도구를 다운로드하여 설치합니다.

2. 모든 Internet Explorer 창을 닫습니다.

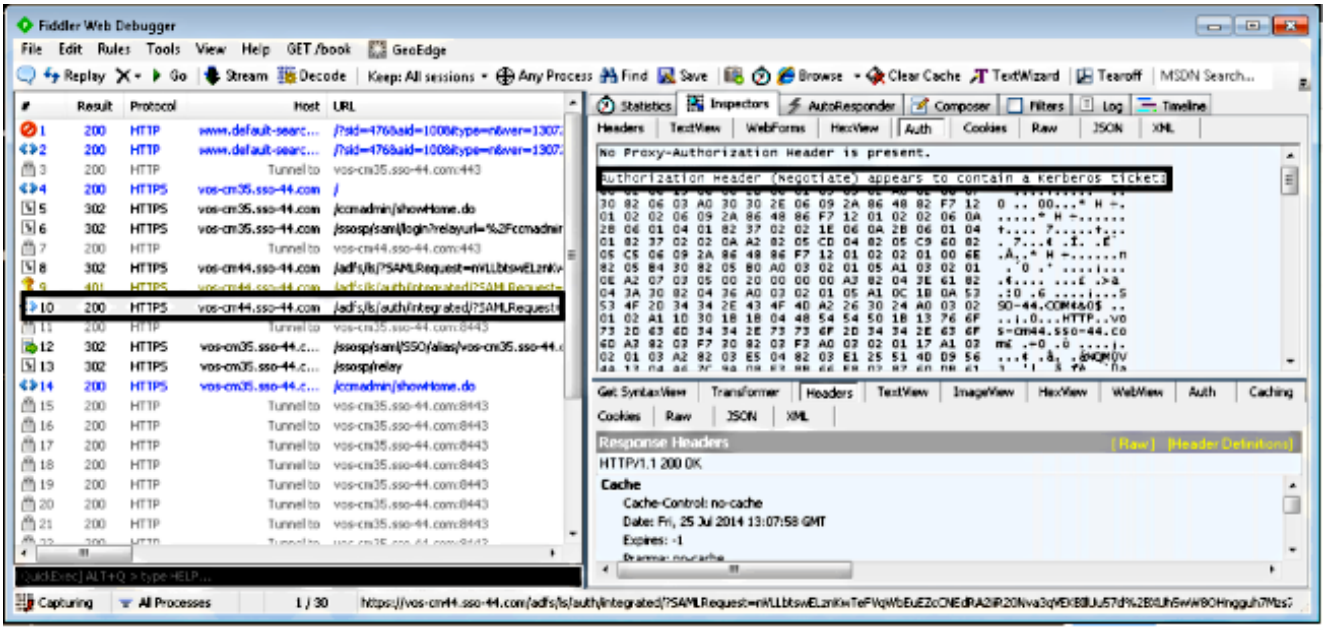
3. File Tool을 실행하고 File 메뉴에서 **Capture Traffic** 옵션이 활성화되었는지 확인합니다.

   Fiddler는 클라이언트 시스템과 서버 간의 통과 프록시 역할을 하며 모든 트래픽을 수신하며, 이 경우 Internet Explorer 설정을 다음과 같이 일시적으로 설정합니다.

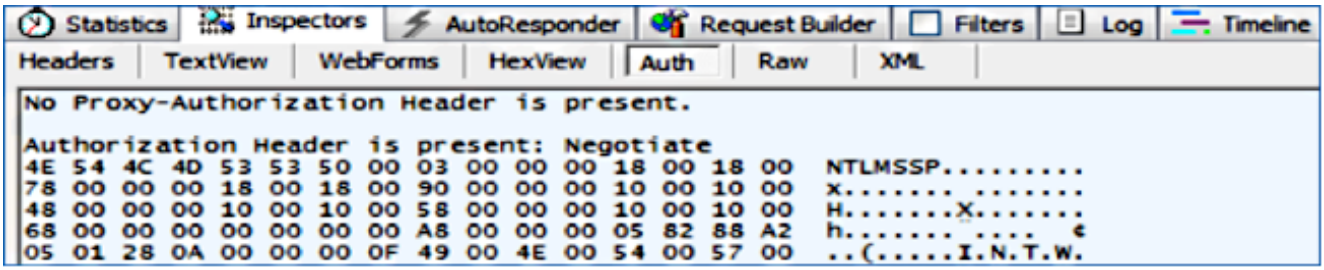


4. Internet Explorer를 열고 CRM(Customer Relationship Management) 서버 URL을 찾은 다음 링크를 클릭하여 트래픽을 생성합니다.

5. Windows Media Player 기본 창을 다시 참조하고 Frames(프레임) 중 하나를 선택합니다(성공).



인증 유형이 NTLM인 경우 프레임 시작**에 협상 - NTLMSSP**가 표시됩니다(아래 참조).



문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.