

# Konfigurieren des SAML SSO-Setups mit Kerberos-Authentifizierung

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Konfigurieren von AD FS](#)

[Browser konfigurieren](#)

[Microsoft Internet Explorer](#)

[Mozilla Firefox](#)

[Überprüfung](#)

[Fehlerbehebung](#)

## Einleitung

In diesem Dokument wird beschrieben, wie Active Directory und Active Directory Federation Service (AD FS) Version 2.0 konfiguriert werden, um die Verwendung der Kerberos-Authentifizierung durch Jabber-Clients (nur Microsoft Windows) zu ermöglichen. Dadurch können sich Benutzer bei ihrer Microsoft Windows-Anmeldung anmelden und nicht zur Eingabe von Anmeldeinformationen aufgefordert werden.

**Vorsicht:** Dieses Dokument basiert auf einer Laborumgebung und geht davon aus, dass Sie sich der Auswirkungen der vorgenommenen Änderungen bewusst sind. Lesen Sie die entsprechende Produktdokumentation, um die Auswirkungen der vorgenommenen Änderungen zu verstehen.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt Folgendes:

- Installation und Konfiguration von AD FS Version 2.0 mit Cisco Collaboration-Produkten als Relying Party Trust
- Collaboration-Produkte wie Cisco Unified Communications Manager (CUCM) IM und Presence, Cisco Unity Connection (UCXN) und CUCM-fähig zur Verwendung von Single

## Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

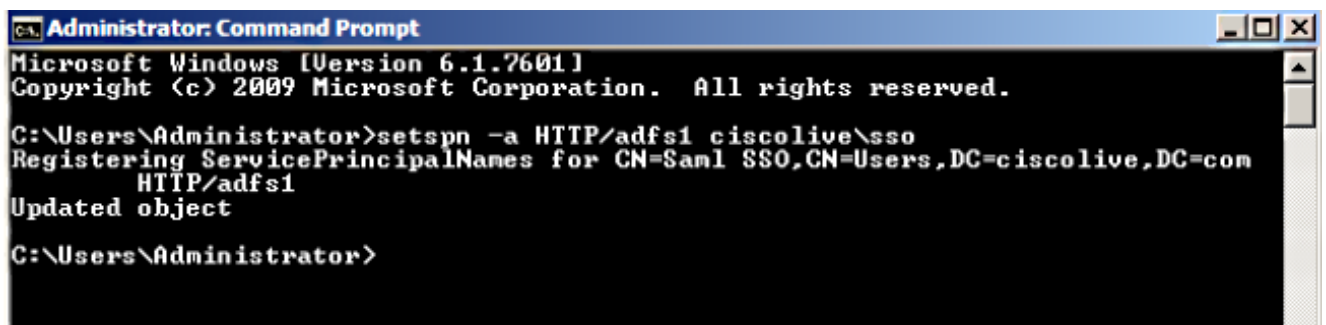
- Active Directory 2008 (Hostname: ADFS1.ciscolive.com)
- AD FS Version 2.0 (Hostname: ADFS1.ciscolive.com)
- CUCM (Hostname: CUCM1.ciscolive.com)
- Microsoft Internet Explorer Version 10
- Mozilla Firefox Version 34
- Telerik Fiddler Version 4

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

## Konfigurieren

### Konfigurieren von AD FS

1. Konfigurieren Sie AD FS Version 2.0 mit Service Principal Name (SPN), um den Client-Computer, auf dem Jabber installiert ist, für die Anforderung von Tickets zu aktivieren. Dadurch kann der Client-Computer wiederum mit einem AD FS-Dienst kommunizieren.



```
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>
```

Siehe [AD FS 2.0: Konfigurieren des SPN \(servicePrincipalName\) für das Dienstkonto](#) für weitere Informationen

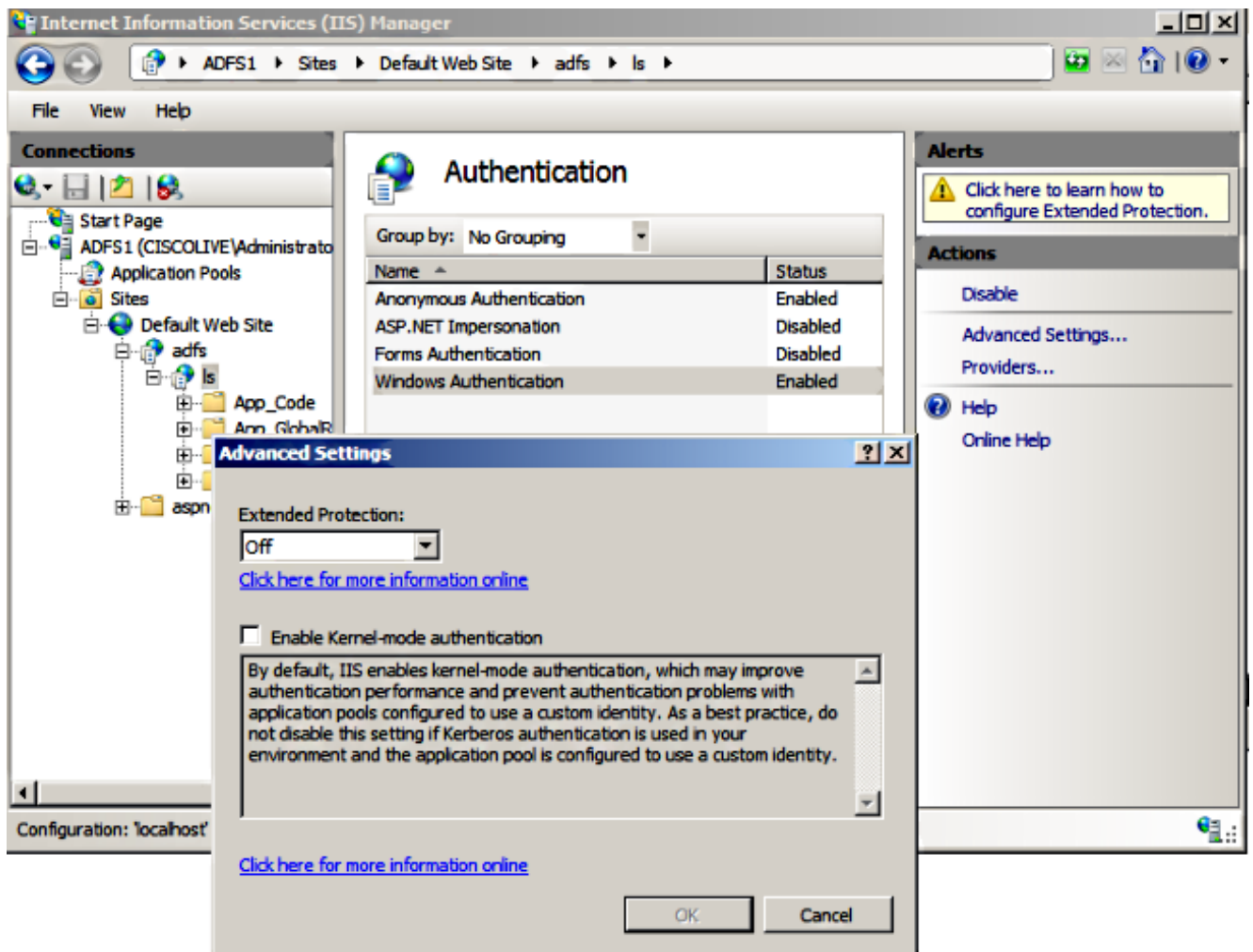
2. Stellen Sie sicher, dass die Standardauthentifizierungskonfiguration für den AD FS-Dienst (in `C:\inetpub\adfs\ls\web.config`) **Integrierte Windows-Authentifizierung** ist. Vergewissern Sie sich, dass die Option nicht in **Form-basierte Authentifizierung** geändert wurde.

```

<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>

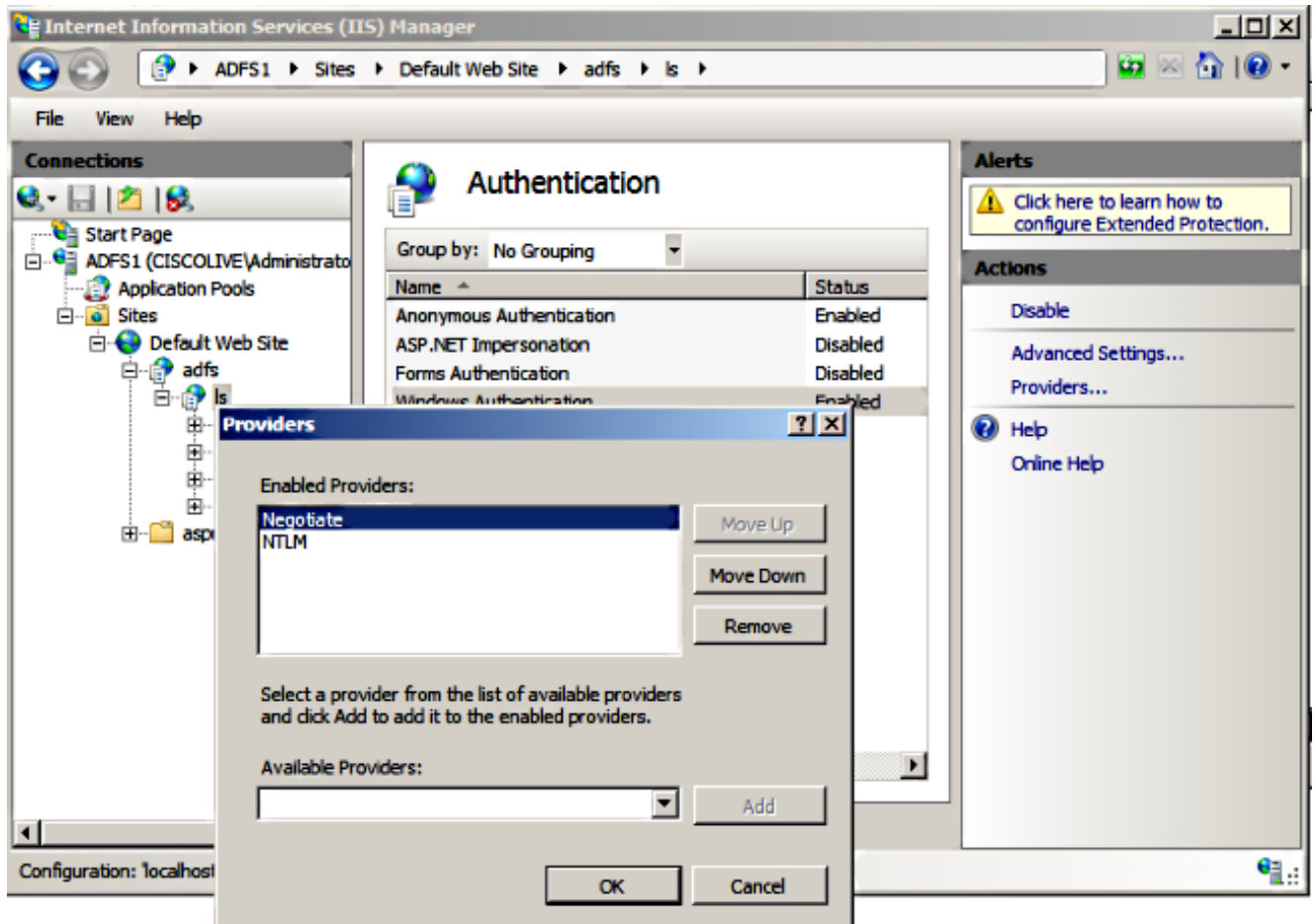
```

3. Wählen Sie **Windows-Authentifizierung** aus, und klicken Sie im rechten Bereich auf **Erweiterte Einstellungen**. Deaktivieren Sie unter Erweiterte Einstellungen die Option **Kernel-Modus-Authentifizierung aktivieren**, stellen Sie sicher, dass der erweiterte Schutz **deaktiviert** ist, und klicken Sie auf **OK**.



4. Stellen Sie sicher, dass AD FS Version 2.0 sowohl das Kerberos-Protokoll als auch das NT LAN Manager-Protokoll (NTLM) unterstützt, da alle Nicht-Windows-Clients Kerberos nicht verwenden können und sich auf NTLM verlassen.

Wählen Sie im rechten Teilfenster **Provider** aus, und stellen Sie sicher, dass **Negotiate** und **NTLM** unter Enabled Providers (Aktivierte Anbieter) vorhanden sind:



**Anmerkung:** AD FS übergibt den Negotiate Security-Header, wenn zur Authentifizierung von Client-Anforderungen eine integrierte Windows-Authentifizierung verwendet wird. Mit dem Sicherheitsheader "Negotiate" können Clients zwischen der Kerberos-Authentifizierung und der NTLM-Authentifizierung wählen. Beim Verhandlungsprozess wird die Kerberos-Authentifizierung ausgewählt, es sei denn, eine der folgenden Bedingungen ist zutreffend:

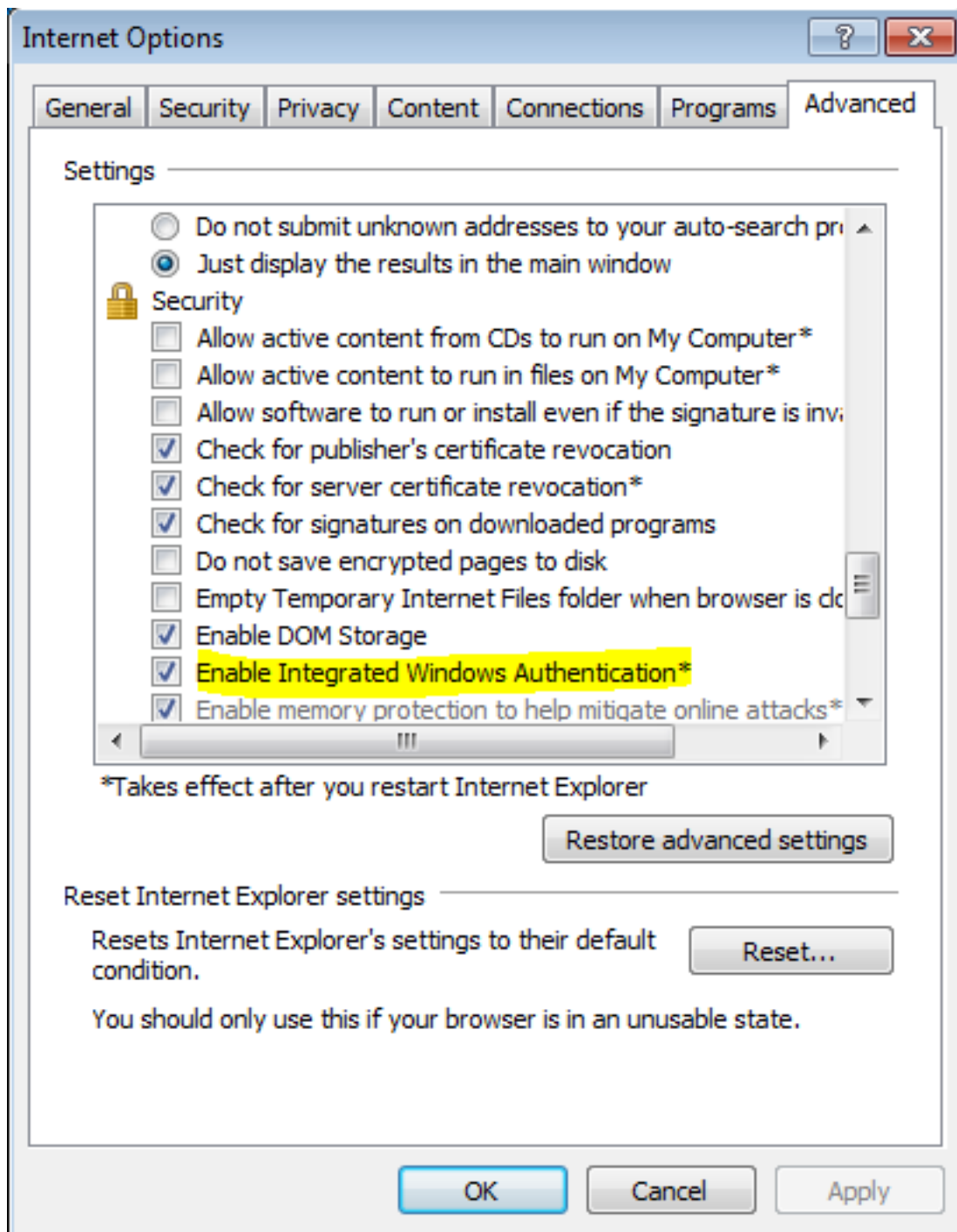
- Eines der Systeme, das an der Authentifizierung beteiligt ist, kann die Kerberos-Authentifizierung nicht verwenden.
- Die aufrufende Anwendung stellt keine ausreichenden Informationen bereit, um die Kerberos-Authentifizierung zu verwenden.
- Damit der Verhandlungsprozess das Kerberos-Protokoll für die Netzwerkauthentifizierung auswählen kann, muss die Client-Anwendung als Zielname ein SPN, einen User Principal Name (UPN) oder einen Network Basic Input/Output System (NetBIOS)-Kontonamen angeben. Andernfalls wählt der Verhandlungsprozess immer das NTLM-Protokoll als bevorzugte Authentifizierungsmethode aus.

## Browser konfigurieren

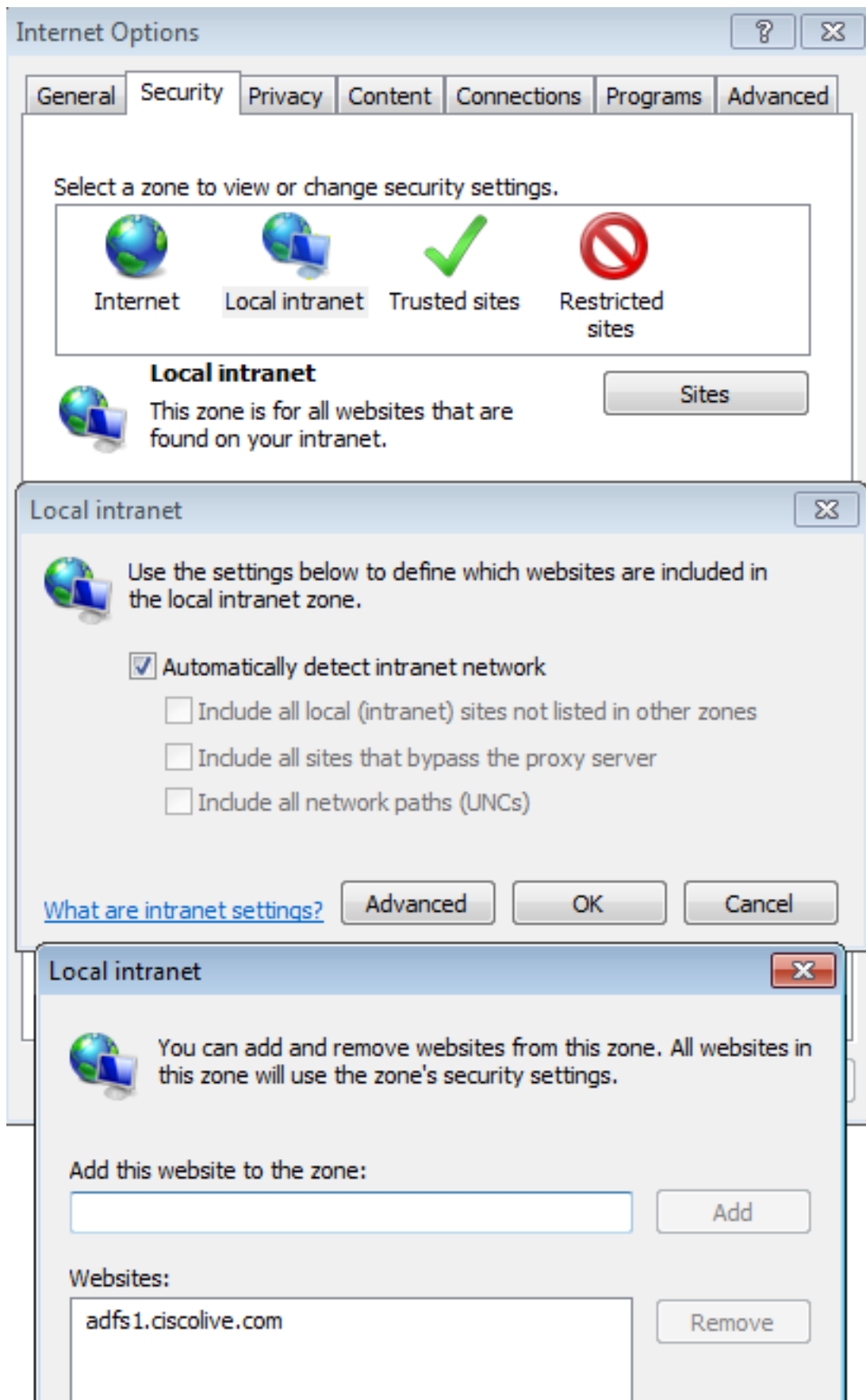
### Microsoft Internet Explorer

1. Stellen Sie sicher, dass **Internet Explorer > Erweitert > Integrierte Windows-Authentifizierung**

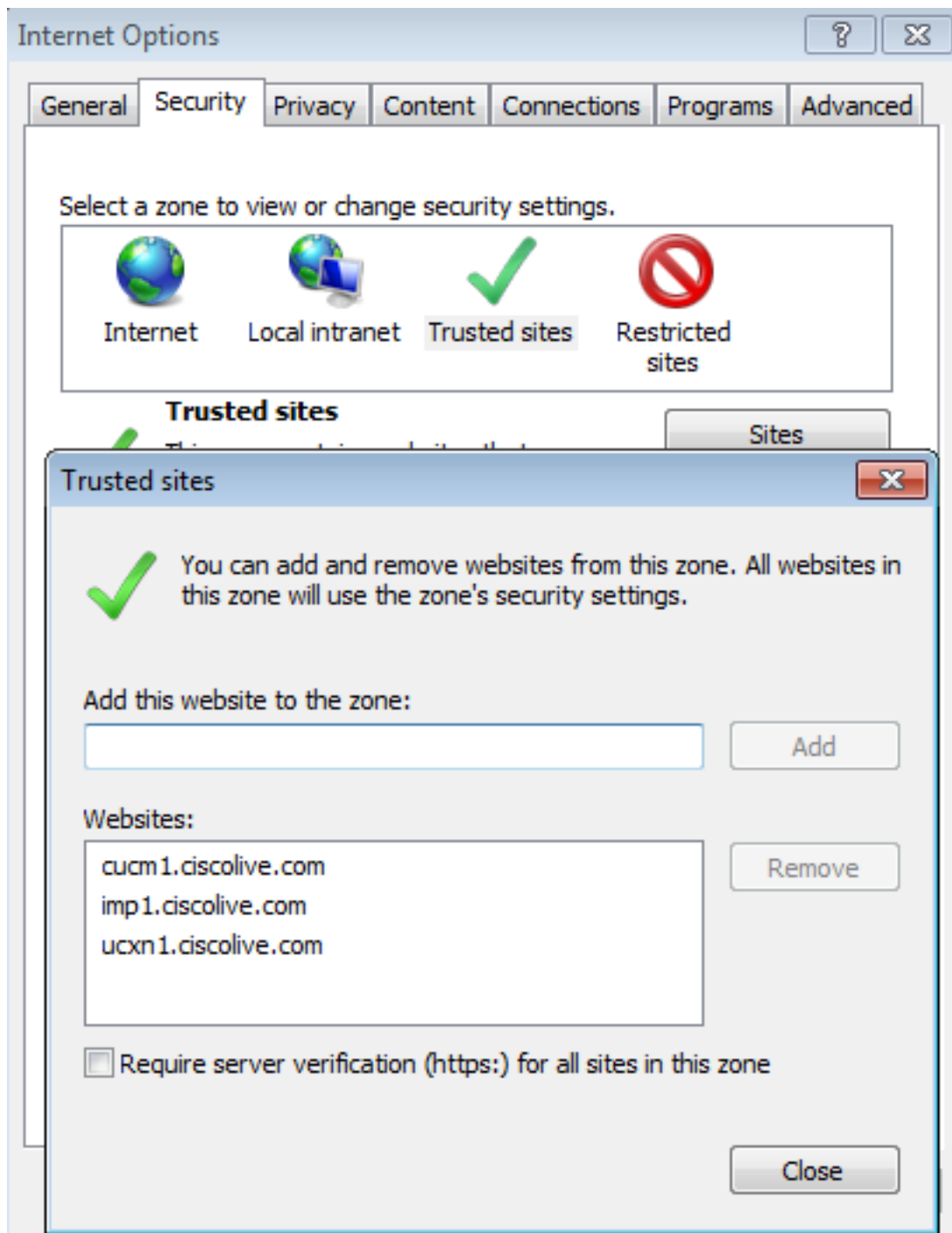
aktivieren aktiviert ist.



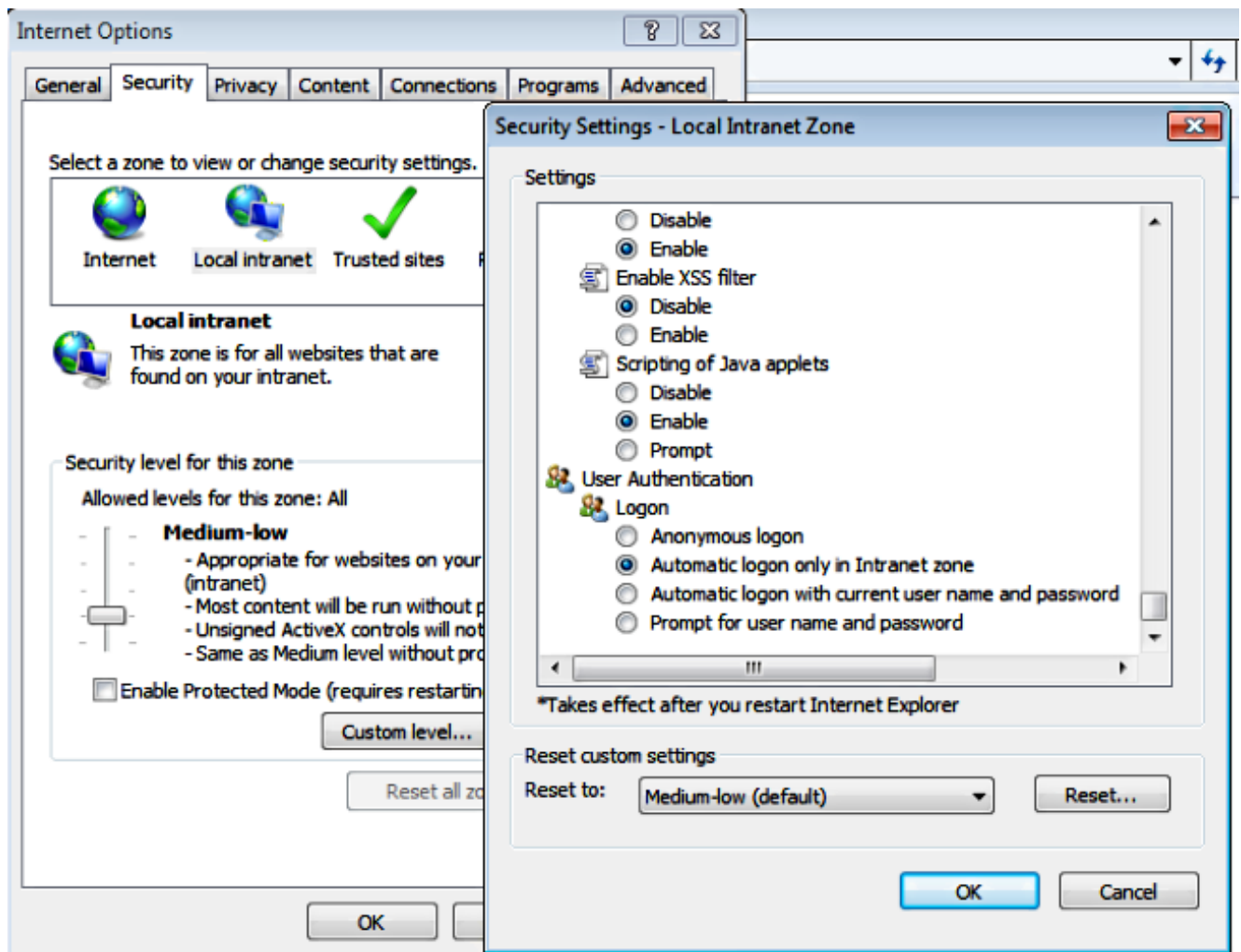
2. AD FS-URL unter **Sicherheit > Intranetzonen > Sites** hinzufügen.



3. Fügen Sie die CUCM-, IMP- und Unity-Hostnamen zu **Sicherheit > Vertrauenswürdige Sites** hinzu.

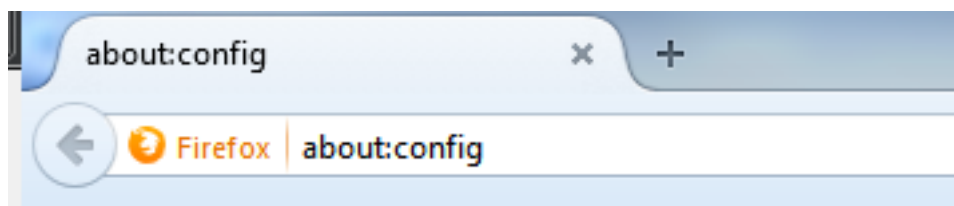


4. Stellen Sie sicher, dass Internet Explorer > **Security** > **Local Intranet** > **Security Settings** > **User Authentication - Logon** konfiguriert ist, um die Anmeldeinformationen für Intranet-Sites zu verwenden.



## Mozilla Firefox

1. Öffnen Sie Firefox, und geben Sie **about:config** in die Adressleiste ein.



2. Klicken Sie auf **Ich werde vorsichtig sein, verspreche ich!**





- Doppelklicken Sie auf den Präferenznamen **network.negotiate-auth.allow-non-fqdn** auf **true** und **network.negotiate-auth.trusted-uris** auf **ciscolive.com,adfs1.ciscolive.com**, um Änderungen vorzunehmen.

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

- Schließen Sie Firefox, und öffnen Sie es erneut.

## Überprüfung

Um zu überprüfen, ob die SPNs für den AD FS-Server korrekt erstellt wurden, geben Sie den **setspn**-Befehl ein und zeigen die Ausgabe an.

```
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>_
```

Überprüfen Sie, ob die Client-Computer Kerberos-Tickets besitzen:

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

Current LogonId is 0:0xabc6d

Cached Tickets: (2)

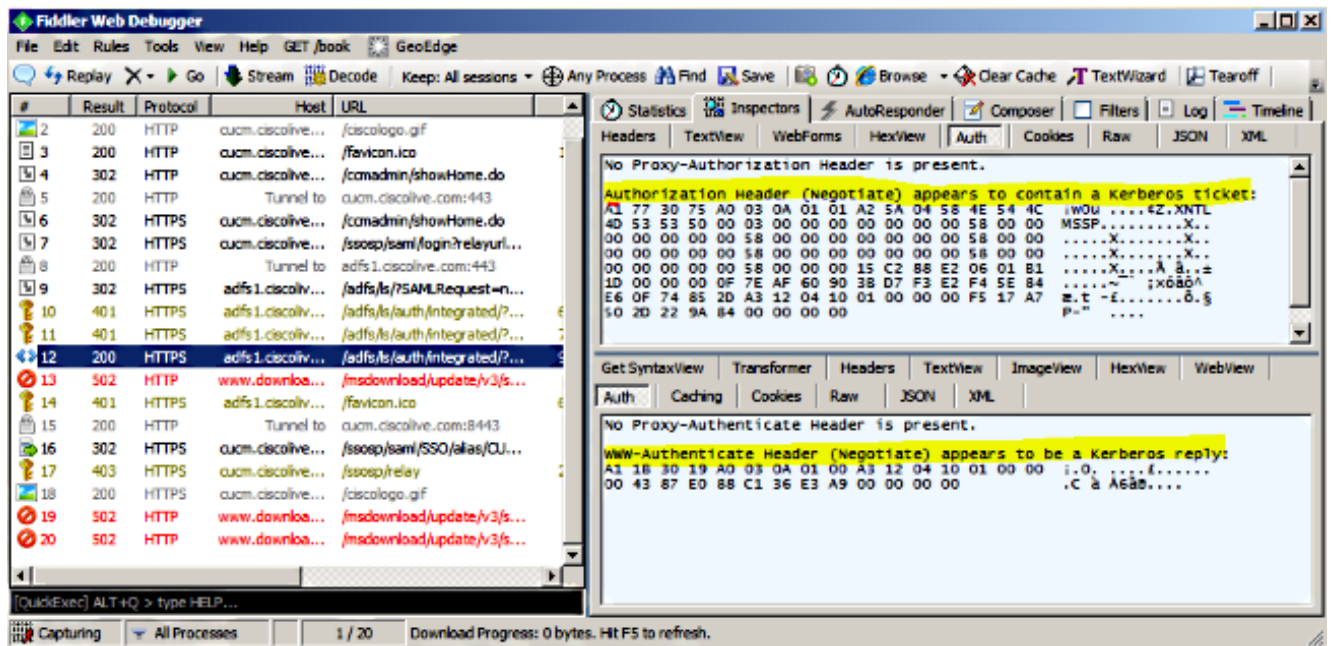
#0> Client: user1 @ CISCOLIVE.COM
Server: krbtgt/CISCOLIVE.COM @ CISCOLIVE.COM
Kerberos Ticket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
Start Time: 1/17/2015 20:52:47 (local)
End Time: 1/18/2015 6:52:47 (local)
Renew Time: 1/24/2015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

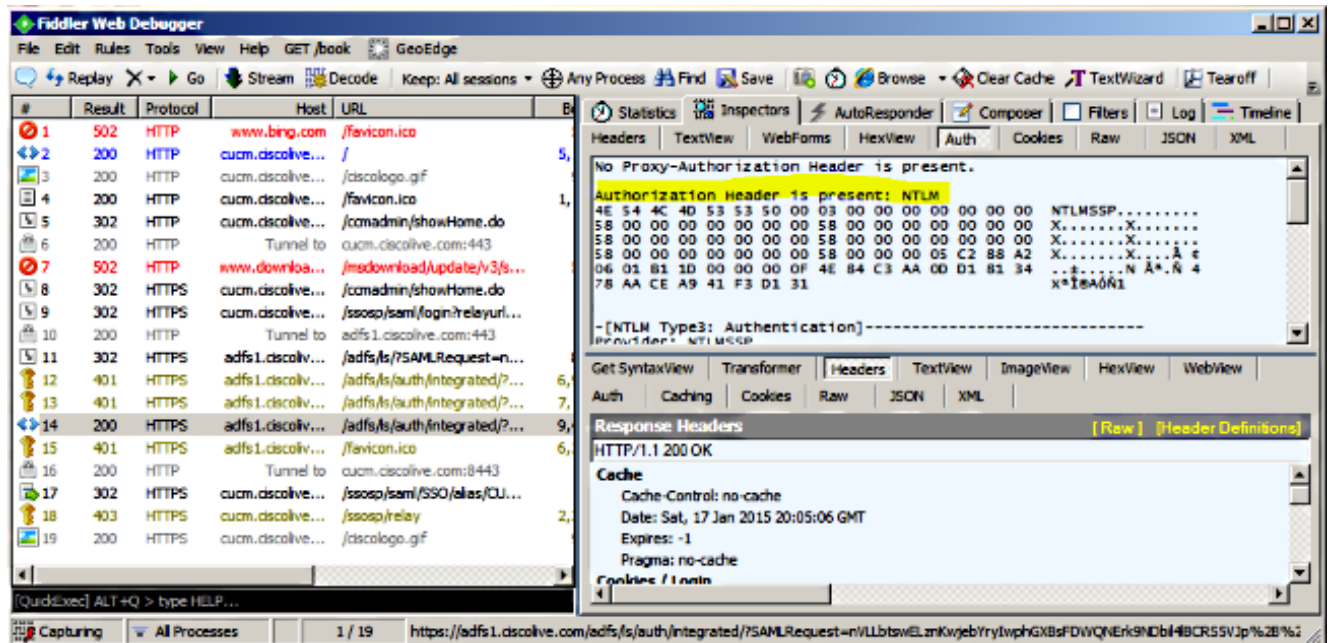
C:\Users\user1.CISCOLIVE>_
```

Führen Sie diese Schritte aus, um zu überprüfen, welche Authentifizierung (Kerberos- oder NTLM-Authentifizierung) verwendet wird.

1. Laden Sie das Programm Fiddler auf Ihren Client-Computer herunter und installieren Sie es.
2. Schließen Sie alle Fenster von Microsoft Internet Explorer.
3. Führen Sie das Tool Ordner aus, und überprüfen Sie, ob die Option **Datenverkehr erfassen** im Menü Datei aktiviert ist. Fiddler fungiert als Pass-Through-Proxy zwischen dem Client-Computer und dem Server und überwacht den gesamten Datenverkehr.
4. Öffnen Sie Microsoft Internet Explorer, rufen Sie den CUCM auf, und klicken Sie auf einige Links, um Datenverkehr zu generieren.
5. Rufen Sie das Hauptfenster von Ordner auf, und wählen Sie eines der Frames aus, in dem das Ergebnis **200** ist (Erfolg), und Kerberos wird als Authentifizierungsmechanismus angezeigt.



6. Wenn der Authentifizierungstyp NTLM ist, sehen Sie **Negotiate - NTLMSSP** am Anfang des Frames, wie hier gezeigt.



## Fehlerbehebung

Wenn alle Konfigurations- und Überprüfungsschritte wie in diesem Dokument beschrieben abgeschlossen wurden und Sie weiterhin Anmeldeprobleme haben, müssen Sie sich an einen Microsoft Windows Active Directory/AD FS-Administrator wenden.