

# SAML SFS-instellingen configureren met Kerberos-verificatie

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[AD FS configureren](#)

[browser configureren](#)

[Microsoft Internet Explorer](#)

[Mozilla FireFox](#)

[Verifiëren](#)

[Problemen oplossen](#)

## Inleiding

In dit document wordt beschreven hoe u Active Directory en Active Directory Federation Service (AD FS) versie 2.0 kunt configureren om Kerberos-verificatie door Jabber Clients (alleen Microsoft Windows) te kunnen gebruiken, waardoor gebruikers inloggen met hun Microsoft Windows-inlognaam en niet worden gevraagd naar aanmeldingsgegevens.

**Voorzichtig:** Dit document is gebaseerd op een labomgeving en gaat ervan uit dat u zich bewust bent van de impact van veranderingen die u maakt. Raadpleeg de relevante productdocumentatie om het effect van veranderingen te begrijpen.

## Voorwaarden

### Vereisten

Cisco raadt u aan:

- AD FS versie 2.0 geïnstalleerd en geconfigureerd met Cisco Collaboration-producten als Relay Party Trust
- Collaboration-producten zoals Cisco Unified Communications Manager (CUCM) IM and Presence, Cisco Unity Connection (UCXN) en CUCM-enabled voor het gebruik van Security Association Markup Language (SAML) met één aanmelding (SSO)

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

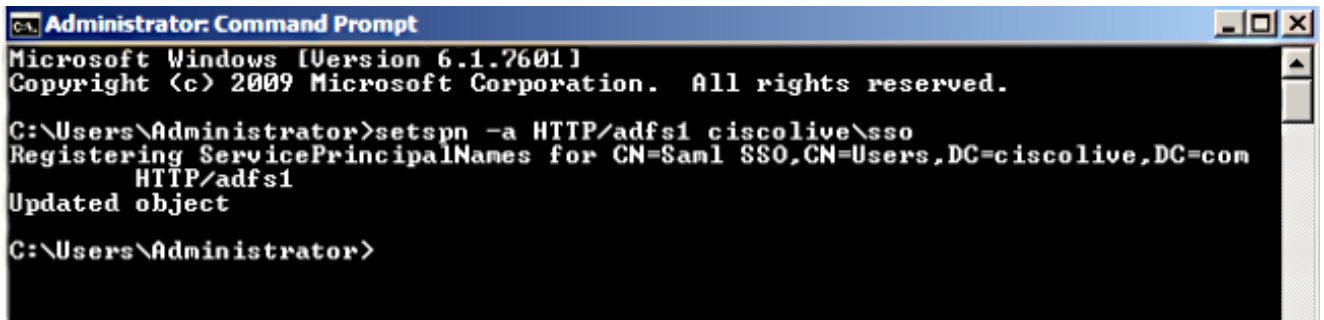
- Active Directory 2008 (Hostname: ADFS1.ciscolive.com)
- AD FS versie 2.0 (Hostname: ADFS1.ciscolive.com)
- CUCM (Hostname: CUCM1.ciscolive.com)
- Microsoft Internet Explorer versie 1.0
- Mozilla Firefox versie 3.4
- Telerik Fidler versie 4

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Configureren

### AD FS configureren

1. Configureer AD FS versie 2.0 met Service Principal Name (SPN) om de clientcomputer waarop Jabber is geïnstalleerd in staat te stellen om tickets te vragen, zodat de clientcomputer op zijn beurt kan communiceren met een AD FS-dienst.



```
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>
```

Raadpleeg [AD FS 2.0: Het configureren van de SPN \(servicePrincipalName\) voor de servicekaccount](#) voor meer informatie.

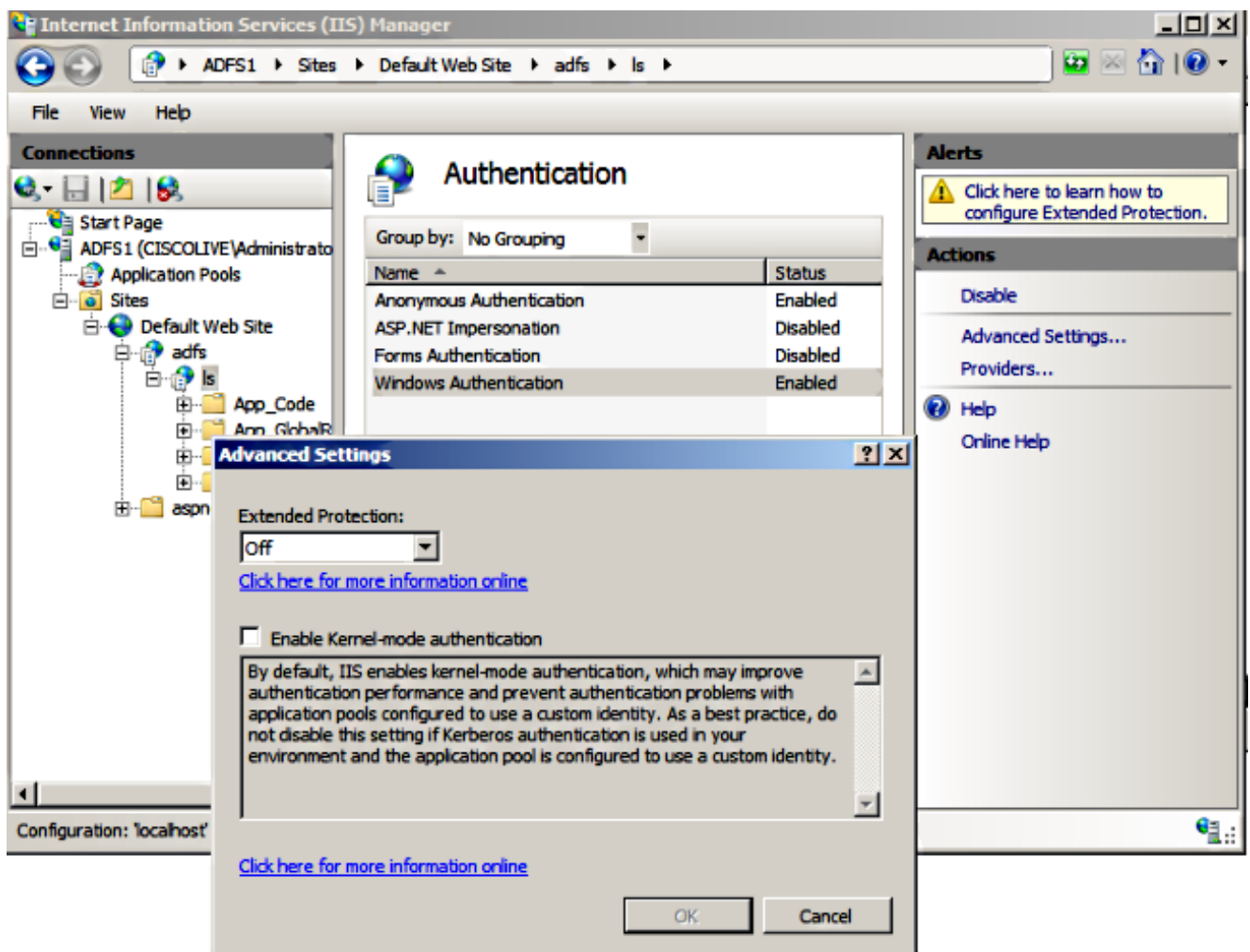
2. Zorg ervoor dat de standaardverificatieconformatie voor de AD FS-service (C:\inetpub\adfs\ls\web.config) **Geïntegreerde Windows-verificatie** is. Zorg ervoor dat deze niet is gewijzigd in **Formulier-gebaseerde verificatie**.

```

<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>

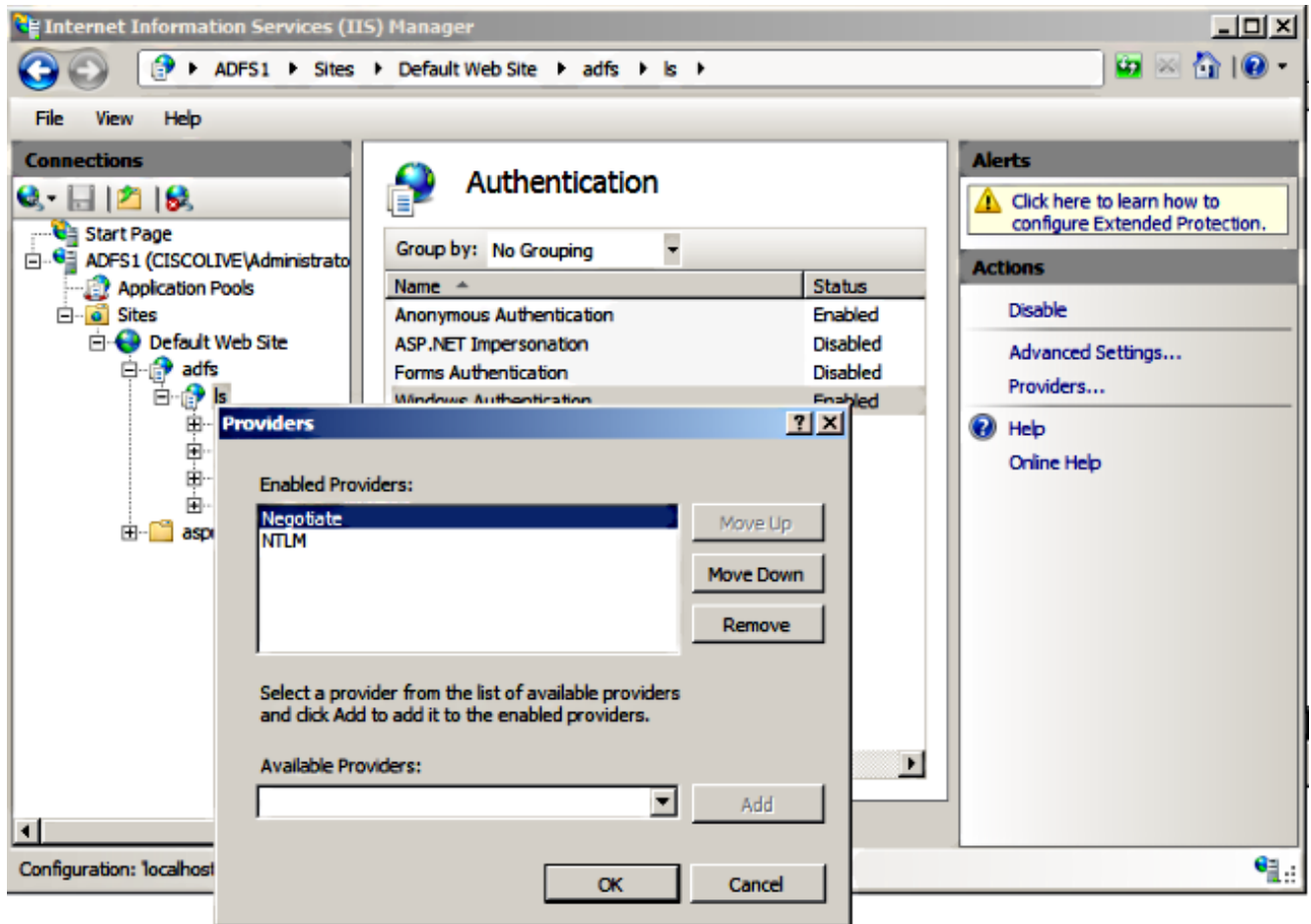
```

3. Selecteer **Windows-verificatie** en klik op **Geavanceerde instellingen** onder het rechter deelvenster. Schakel in het geval van geavanceerde instellingen de optie **Kernel-mode-verificatie uit**, zorg ervoor dat de uitgebreide bescherming **uit** is en klik op OK.



4. Zorg ervoor dat AD FS versie 2.0 zowel het Kerberos-protocol als het NTLM-protocol (NT LAN Manager) ondersteunt omdat alle niet-Windows-clients Kerberos niet kunnen gebruiken en niet op NTLM kunnen vertrouwen.

Selecteer in het rechter deelvenster de optie **Leveranciers** en zorg ervoor dat **onderhandeling** en **NTLM** aanwezig zijn onder Ingeschakelde providers:



**Opmerking:** AD FS geeft de onderhandelingstafel over wanneer de Geïntegreerde Windows-authenticatie wordt gebruikt om clientverzoeken te authenticeren. De onderhandelingshoofdlijst laat klanten tussen Kerberos authenticatie en NTLM authenticatie selecteren. In het onderhandelingsproces wordt Kerberos-verificatie geselecteerd, tenzij een van deze voorwaarden waar is:

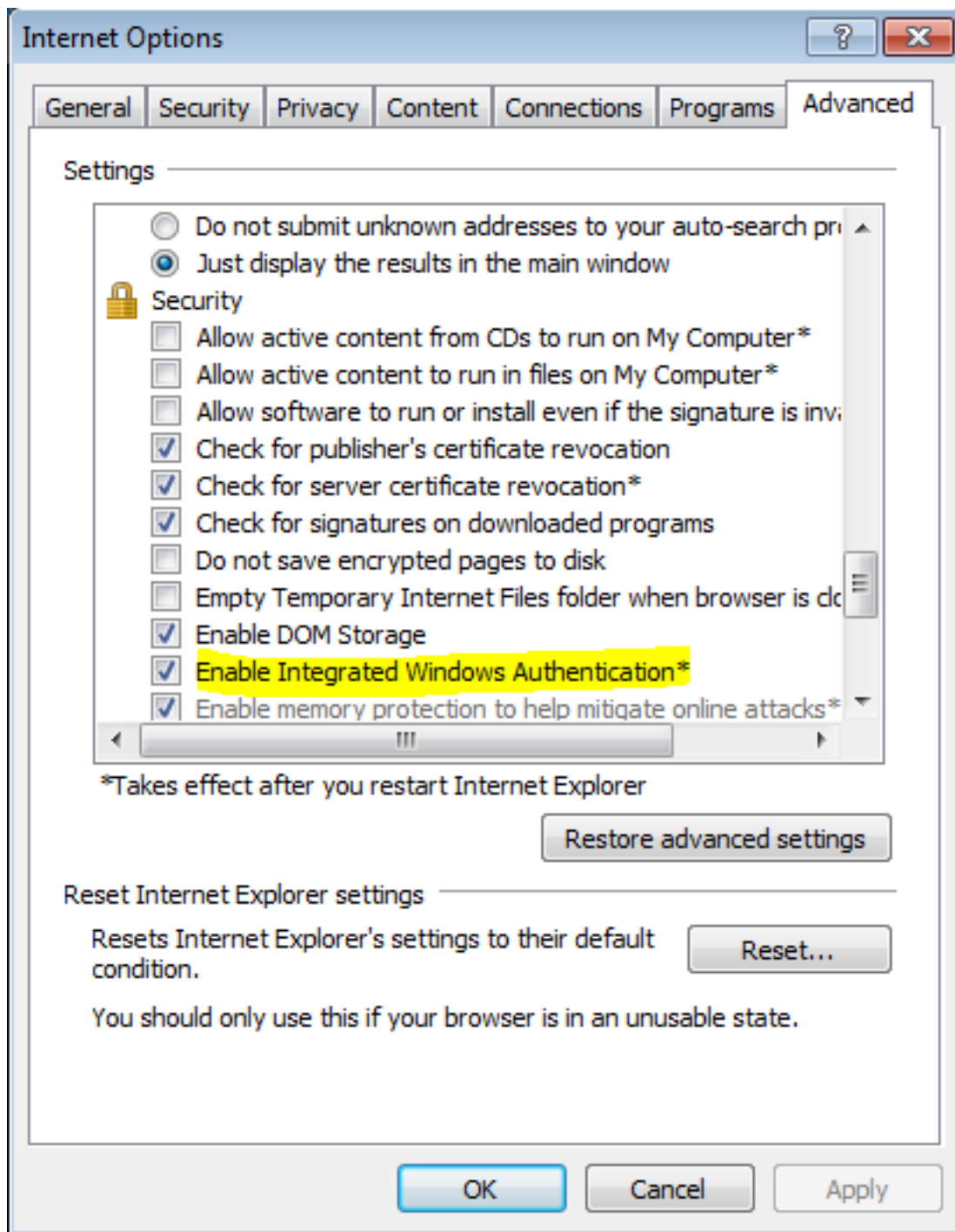
- Een van de systemen die bij de authenticatie betrokken is, kan geen Kerberos-authenticatie gebruiken.
- De oproepende toepassing verschaft niet voldoende informatie om Kerberos-authenticatie te gebruiken.
- Om het onderhandelingsproces in staat te stellen het Kerberos-protocol voor netwerkverificatie te selecteren, moet de clienttoepassing een SPN-, een User Principal Name (UPN) of een Network Basic I/O System (Netopgemerkt)-naam als doelnaam bieden. Anders selecteert het onderhandelingsproces altijd het NTLM-protocol als de meest geprefereerde authenticatiemethode.

## browser configureren

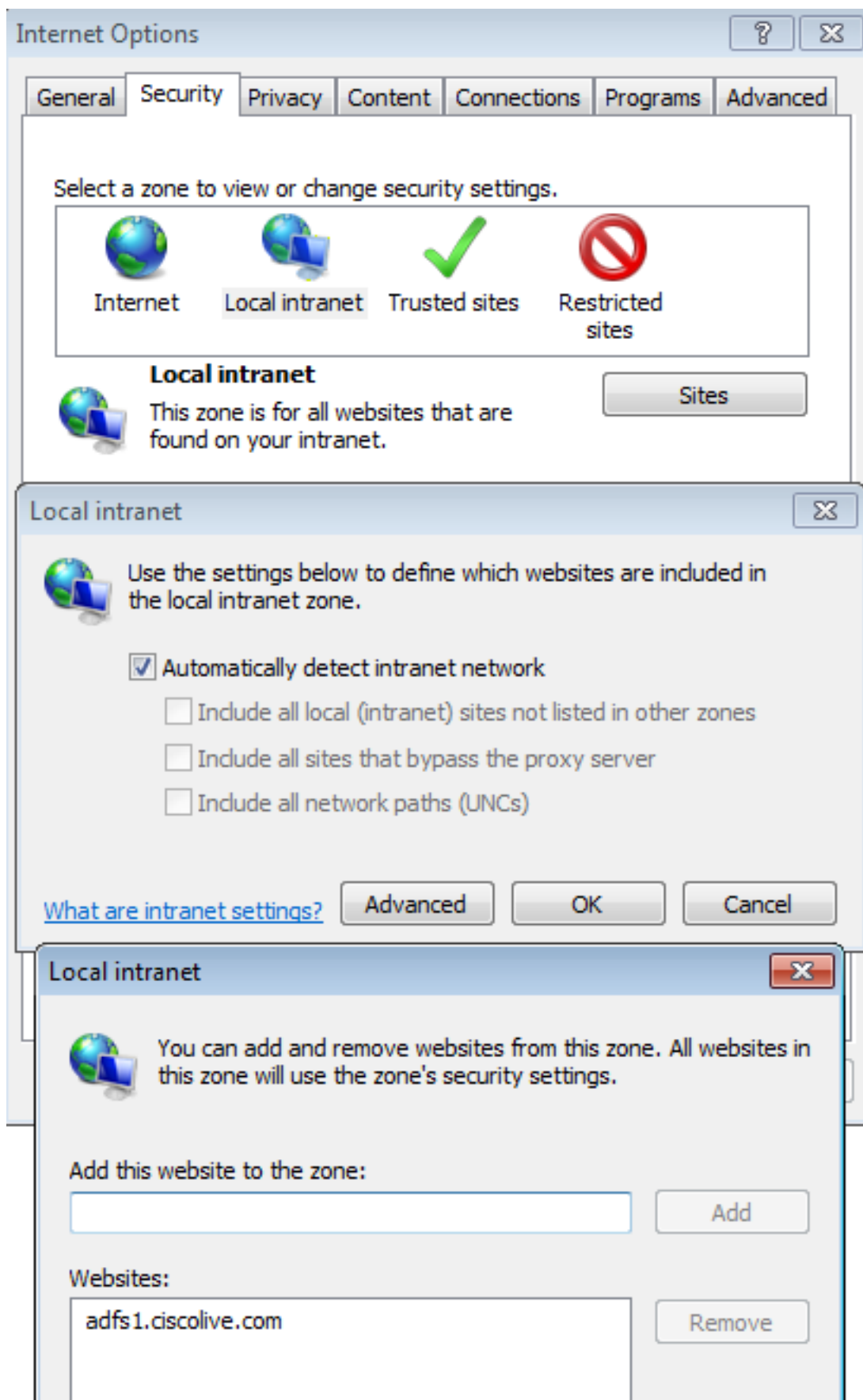
### Microsoft Internet Explorer

1. Zorg ervoor dat **Internet Explorer > Geavanceerd > Geïntegreerde Windows-verificatie**

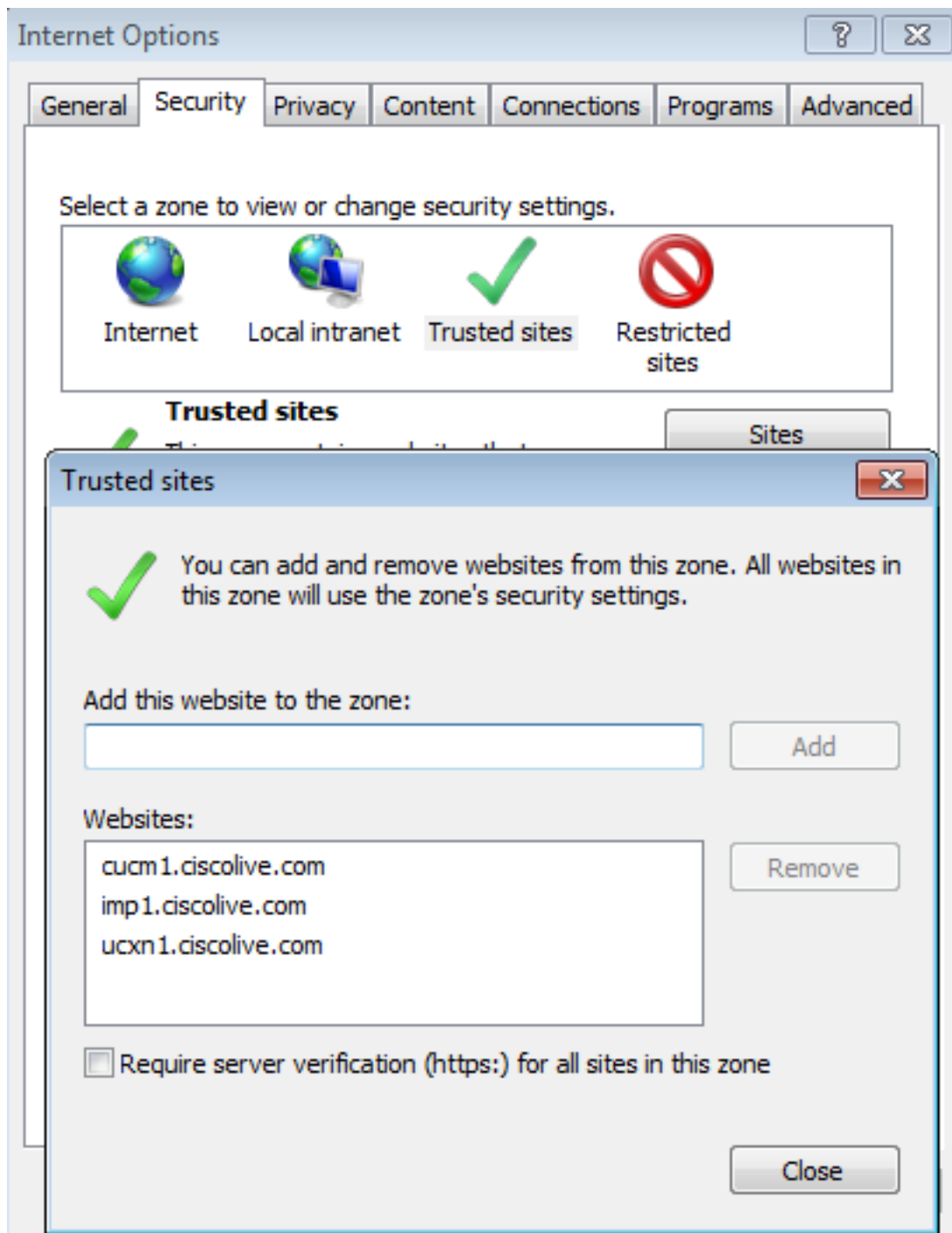
inschakelen is ingeschakeld.



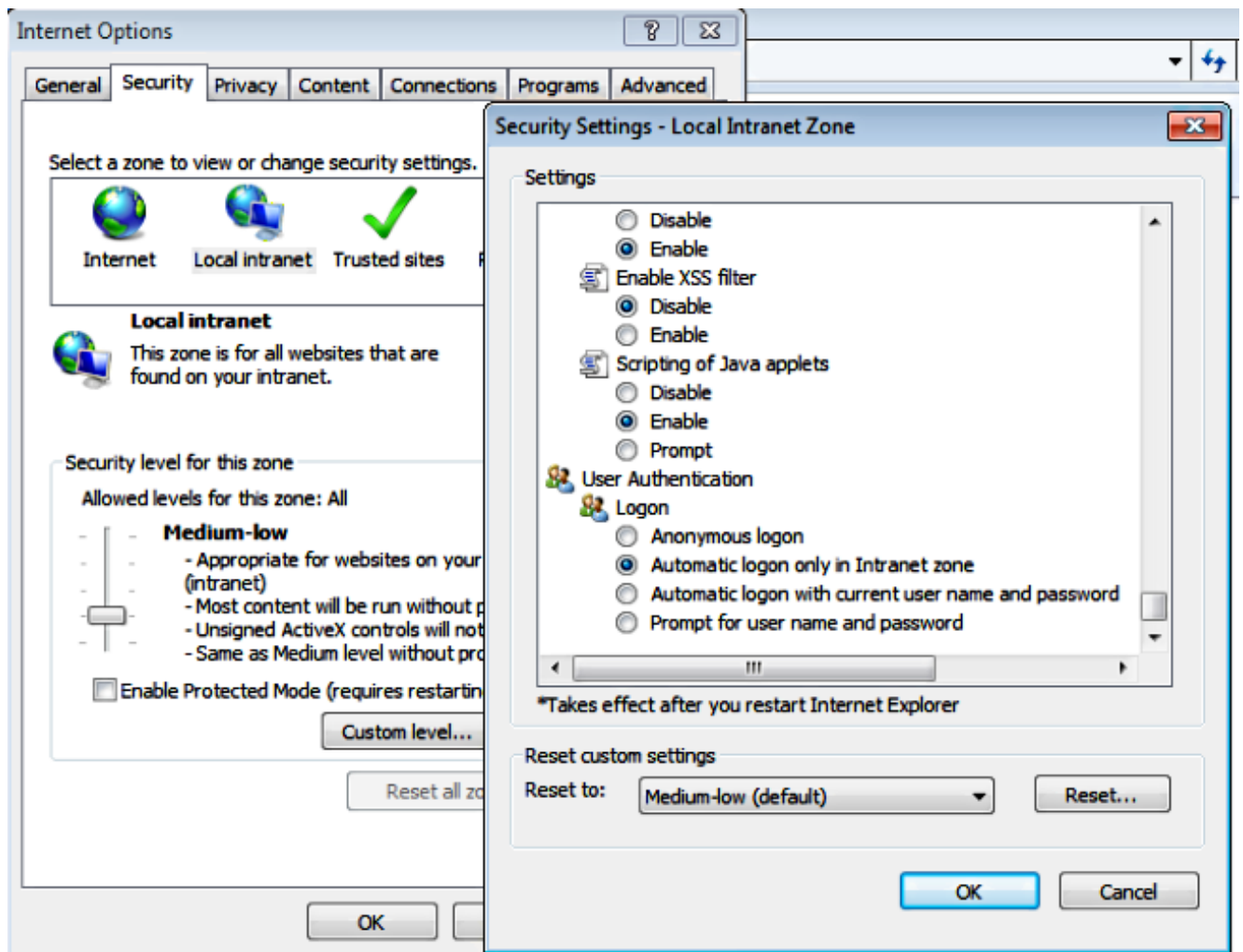
2. Voeg AD FS URL toe onder **Security > Intranet zones > sites**.



3. Voeg de CUCM, IMP, en Unity hostname toe aan **Security >Trusted sites**.

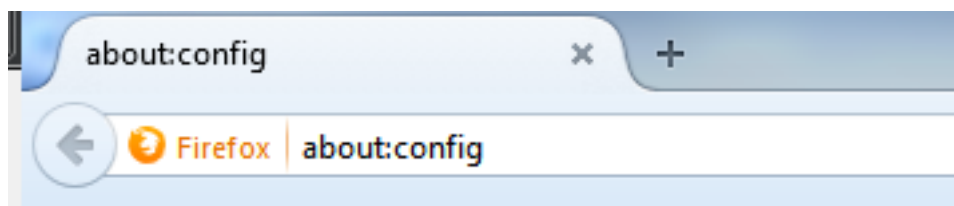


4. Zorg ervoor dat Internet-exporteur > beveiliging > Lokaal intranet > Beveiligingsinstellingen > Gebruikersverificatie - Aanmelden is ingesteld om intranetsites te kunnen gebruiken.



## Mozilla FireFox

1. Open Firefox en voer **over:fig** in de adresbalk in.



2. Klik ik zal voorzichtig zijn.





- Dubbelklik op de naam Preferentie `network.onderhandelingen-auth.allow-non-fqdn` om waar te zijn en `network.onderhandelingen-auth.vertrouwde-uris` naar `ciscolive.com`, `adfs1.ciscolive.com` om te wijzigen.

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

- Sluit Firefox en open deze opnieuw.

## Verifiëren

Om te controleren of de SPN's voor de AD FS-server goed zijn gemaakt, voert u de ingestelde spn-opdracht in en geeft u de uitvoer weer.

```
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>_
```

Controleer of de clientmachines Kerberos-tickets hebben:

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

Current LogonId is 0:0xabc6d

Cached Tickets: (2)

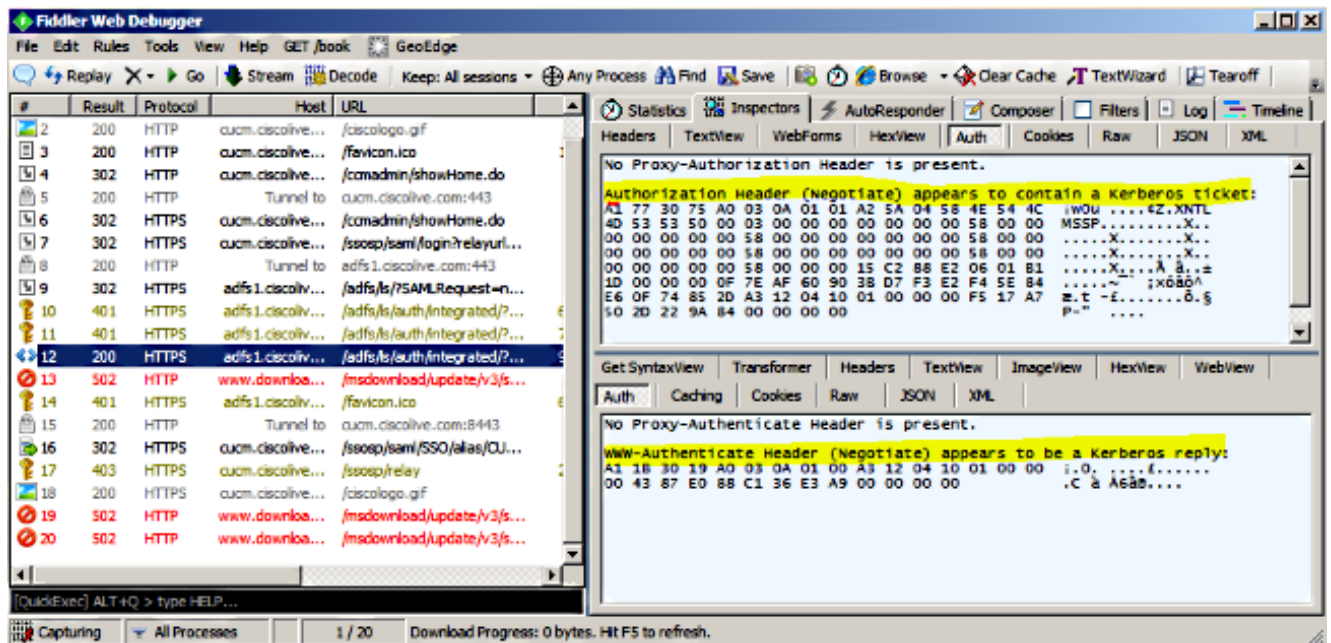
#0> Client: user1 @ CISCOLIVE.COM
Server: krbtgt/CISCOLIVE.COM @ CISCOLIVE.COM
Kerberos Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
Start Time: 1/17/2015 20:52:47 (local)
End Time: 1/18/2015 6:52:47 (local)
Renew Time: 1/24/2015 20:52:47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

#1> Client: user1 @ CISCOLIVE.COM
Server: host/pc1.ciscolive.com @ CISCOLIVE.COM
Kerberos 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>_
```

Voltooi deze stappen om te verifiëren welke verificatie (Kerberos of NTLM-verificatie) in gebruik is.

1. Download het gereedschap van de Fiddler aan uw clientmachine en installeer het.
2. Sluit alle Microsoft Internet Explorer-vensters.
3. Start het bestandsindeling en controleer of de optie **Opname verkeer** is ingeschakeld in het menu Bestand. Fiddler werkt als een passthrough-proxy tussen de client en de server en luistert naar al het verkeer.
4. Open Microsoft Internet Explorer, blader in de CUCM en klik op bepaalde koppelingen om verkeer te genereren.
5. Raadpleeg het hoofdvenster van FormFiller en kies een van de frames waarin het resultaat **200** is (succes) en u kunt Kerberos als verificatiemechanisme zien



6. Als het verificatietype NTLM is, dan ziet u **Negotiate - NTLMSSP** in het begin van het frame zoals hier wordt getoond.

