

# Configurazione dell'installazione di SAML SSO con autenticazione Kerberos

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Configurare ADFS](#)

[Configura browser](#)

[Microsoft Internet Explorer](#)

[Mozilla Firefox](#)

[Verifica](#)

[Risoluzione dei problemi](#)

## Introduzione

In questo documento viene descritto come configurare Active Directory e Active Directory Federation Service (ADFS) versione 2.0 in modo da consentire l'utilizzo dell'autenticazione Kerberos da parte dei client Jabber (solo Microsoft Windows), che consente agli utenti di eseguire l'accesso con l'accesso a Microsoft Windows senza che vengano richieste le credenziali.

**Attenzione:** Questo documento si basa su un ambiente lab e presuppone che l'utente sia a conoscenza dell'impatto delle modifiche apportate. Per comprendere l'impatto delle modifiche apportate, consultare la documentazione del prodotto in uso.

## Prerequisiti

### Requisiti

Cisco raccomanda:

- AD FS versione 2.0 installato e configurato con i prodotti Cisco Collaboration come attendibilità componente
- Prodotti per la collaborazione come Cisco Unified Communications Manager (CUCM), IM e Presenza, Cisco Unity Connection (UCXN) e CUCM abilitati per l'utilizzo di SAML (Security Assertion Markup Language) Single Sign-On (SSO)

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

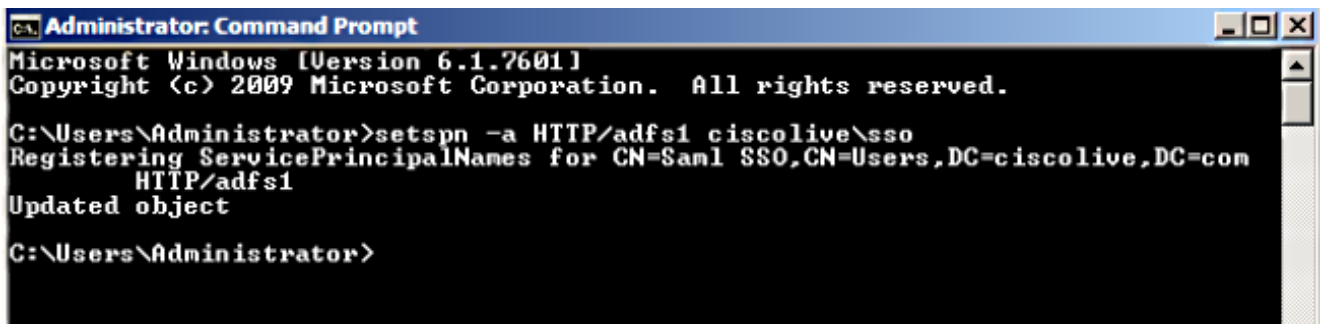
- Active Directory 2008 (nome host: ADFS1.ciscolive.com)
- AD FS versione 2.0 (nome host: ADFS1.ciscolive.com)
- CUCM (nome host: CUCM1.ciscolive.com)
- Microsoft Internet Explorer versione 10
- Mozilla Firefox versione 34
- Telerik Fiddler versione 4

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Configurazione

### Configurare ADFS

1. Configurare AD FS versione 2.0 con il nome dell'entità servizio (SPN) per consentire al computer client in cui è installato Jabber di richiedere i ticket, che a sua volta consente al computer client di comunicare con un servizio AD FS.



```
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>
```

Per ulteriori informazioni, fare riferimento al documento [ADFS 2.0: Come configurare l'SPN \(servicePrincipalName\) per l'account del servizio](#) per ulteriori informazioni.

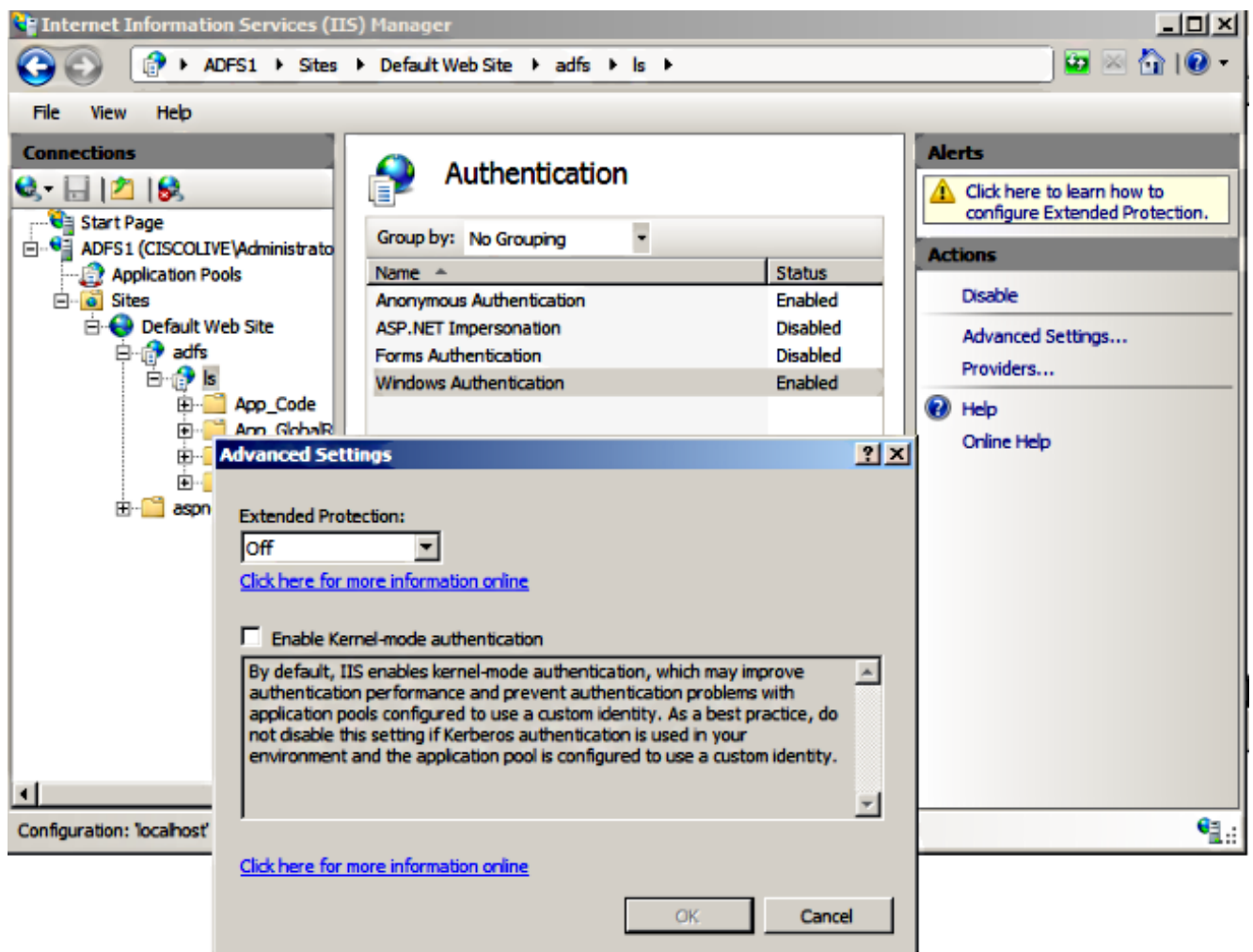
2. Verificare che la configurazione di autenticazione predefinita per il servizio AD FS (in `C:\inetpub\adfs\ls\web.config`) sia **Autenticazione integrata di Windows**. Verificare che non sia stata modificata in **Autenticazione basata su form**.

```

<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>
  <commonDomainCookieWriter="" 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>

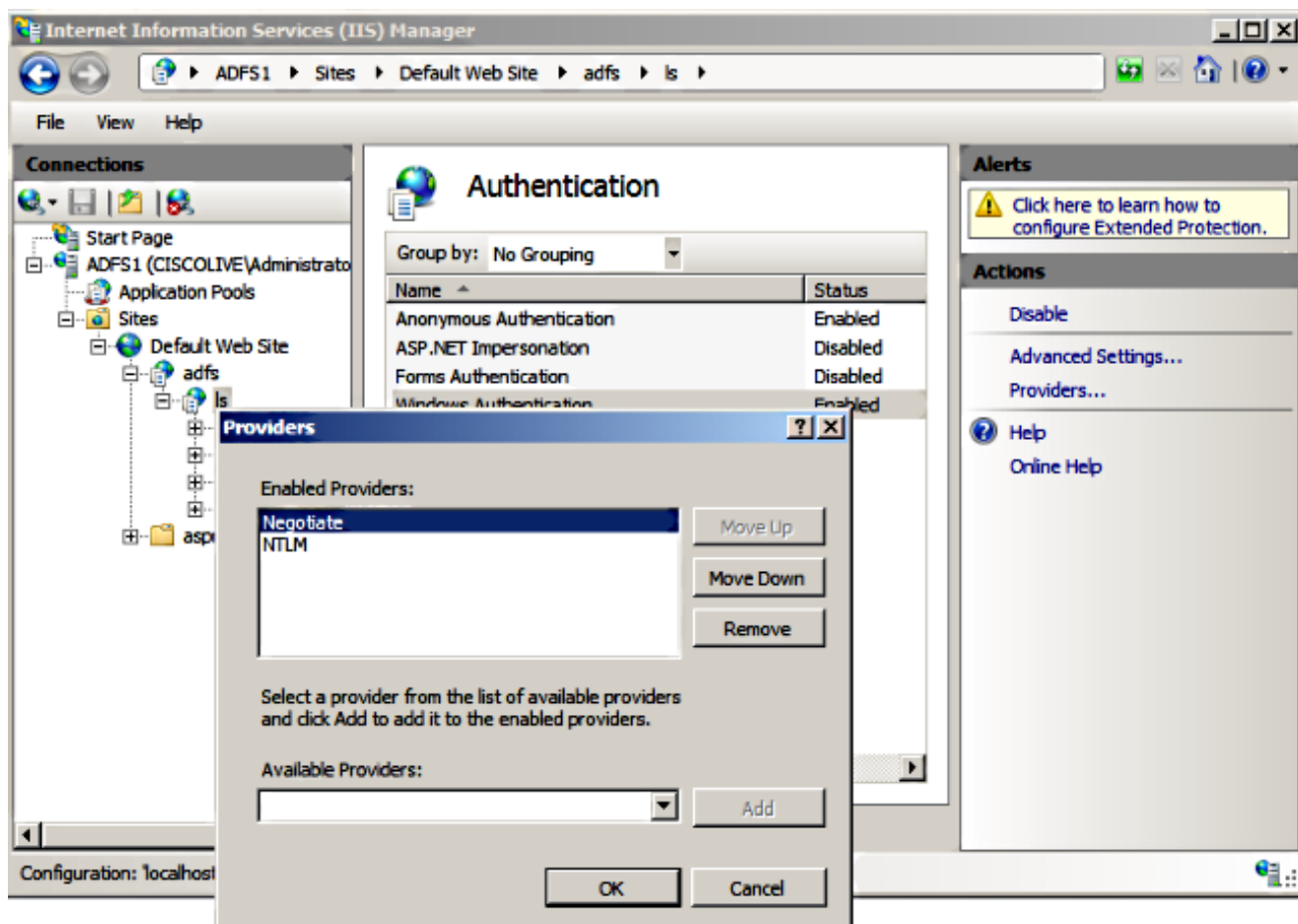
```

3. Selezionare **Autenticazione di Windows** e fare clic su **Impostazioni avanzate** nel riquadro di destra. In Impostazioni avanzate, deselezionare **Abilita autenticazione in modalità kernel**, accertarsi che la protezione estesa sia **disattivata** e fare clic su **OK**.



4. Verificare che AD FS versione 2.0 supporti sia il protocollo Kerberos che il protocollo NTLM (NT LAN Manager), poiché tutti i client non Windows non possono utilizzare Kerberos e si basano su NTLM.

Nel riquadro di destra, selezionare **Provider** e assicurarsi che **Negotiate** e **NTLM** siano presenti in Provider abilitati:



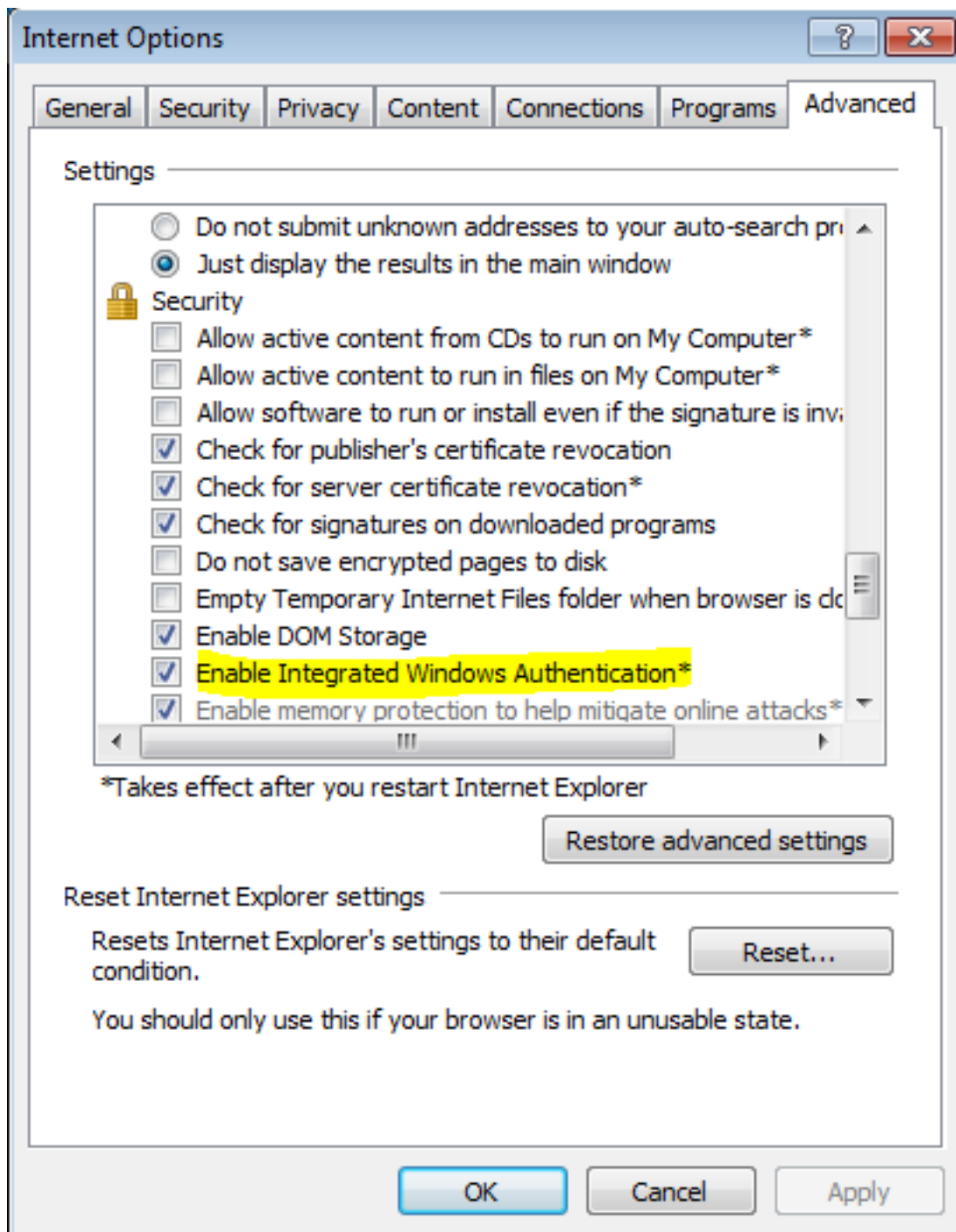
**Nota:** ADFS passa l'intestazione di sicurezza Negotiate quando viene utilizzata l'autenticazione integrata di Windows per autenticare le richieste client. L'intestazione Negotiate consente ai client di scegliere tra l'autenticazione Kerberos e l'autenticazione NTLM. Il processo Negotiate seleziona l'autenticazione Kerberos a meno che non si verifichi una delle seguenti condizioni:

- Uno dei sistemi coinvolti nell'autenticazione non può utilizzare l'autenticazione Kerberos.
- L'applicazione chiamante non fornisce informazioni sufficienti per utilizzare l'autenticazione Kerberos.
- Per consentire al processo Negotiate di selezionare il protocollo Kerberos per l'autenticazione di rete, l'applicazione client deve fornire un nome SPN, un nome dell'entità utente (UPN) o un nome account NetBIOS (Network Basic Input/Output System) come nome della destinazione. In caso contrario, il processo Negotiate seleziona sempre il protocollo NTLM come metodo di autenticazione preferito.

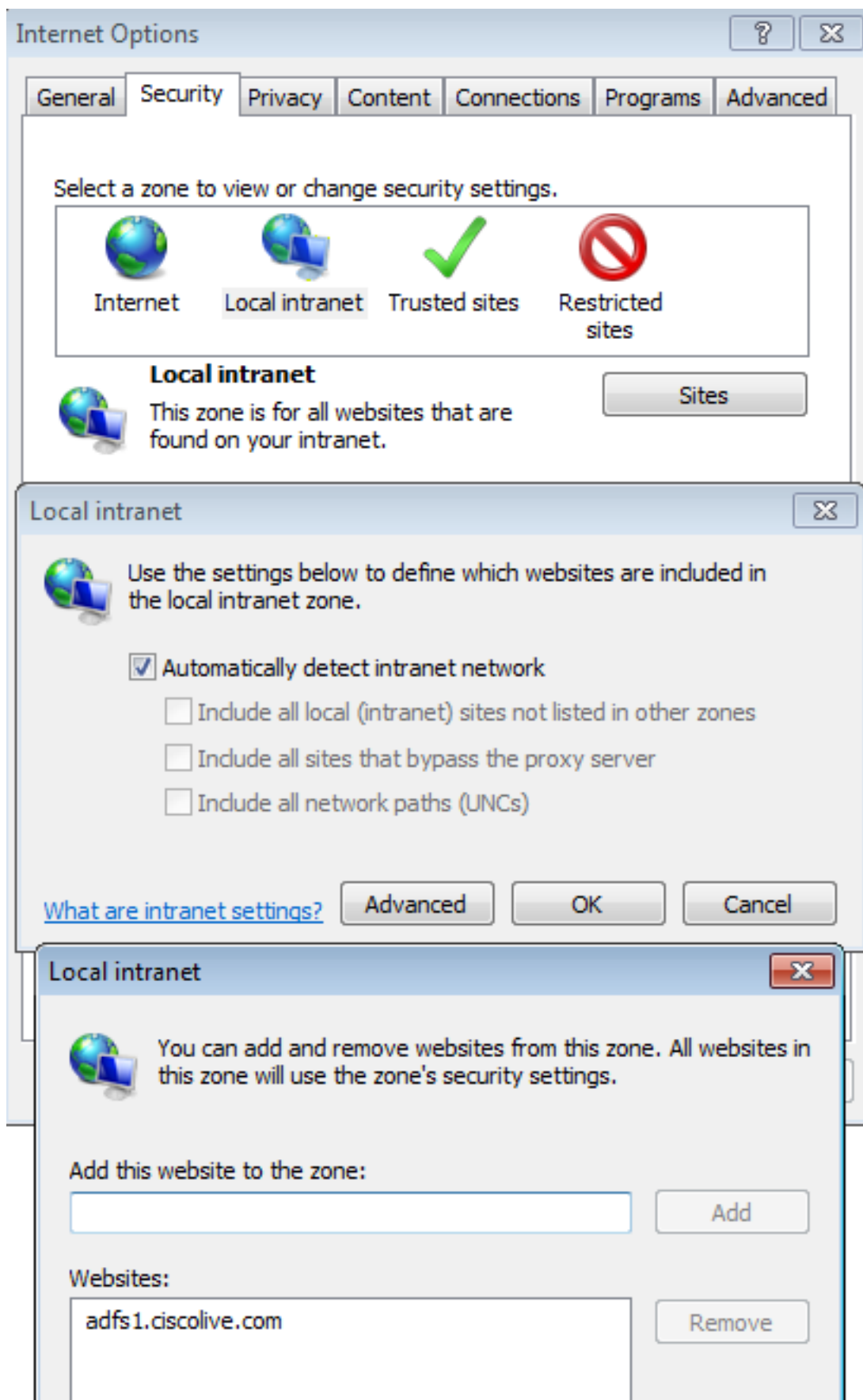
## Configura browser

### Microsoft Internet Explorer

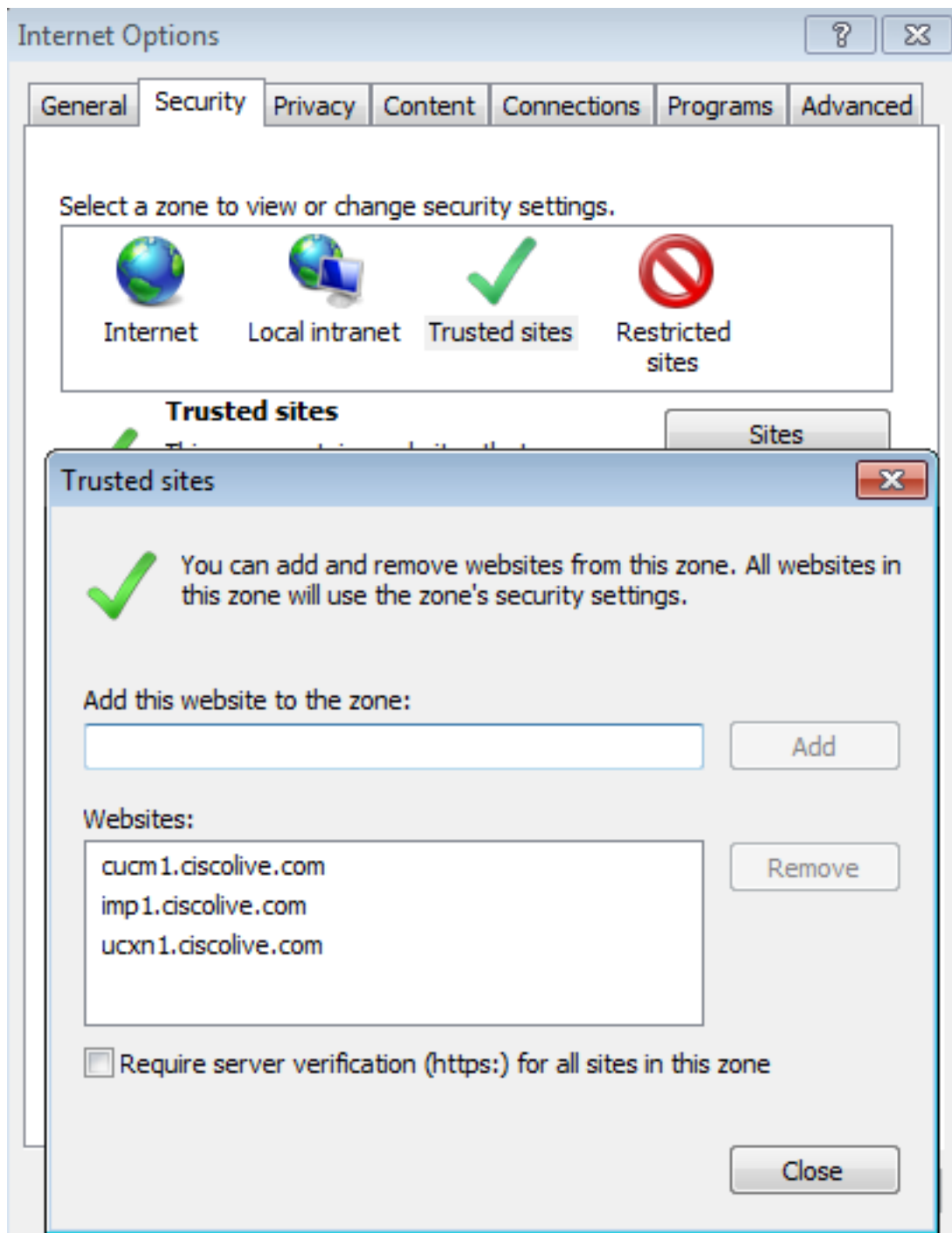
1. Verificare che Internet Explorer > Avanzate > Abilita autenticazione integrata di Windows sia selezionato.



2. Aggiungere l'URL ADFS in **Protezione >Aree Intranet > Siti**.

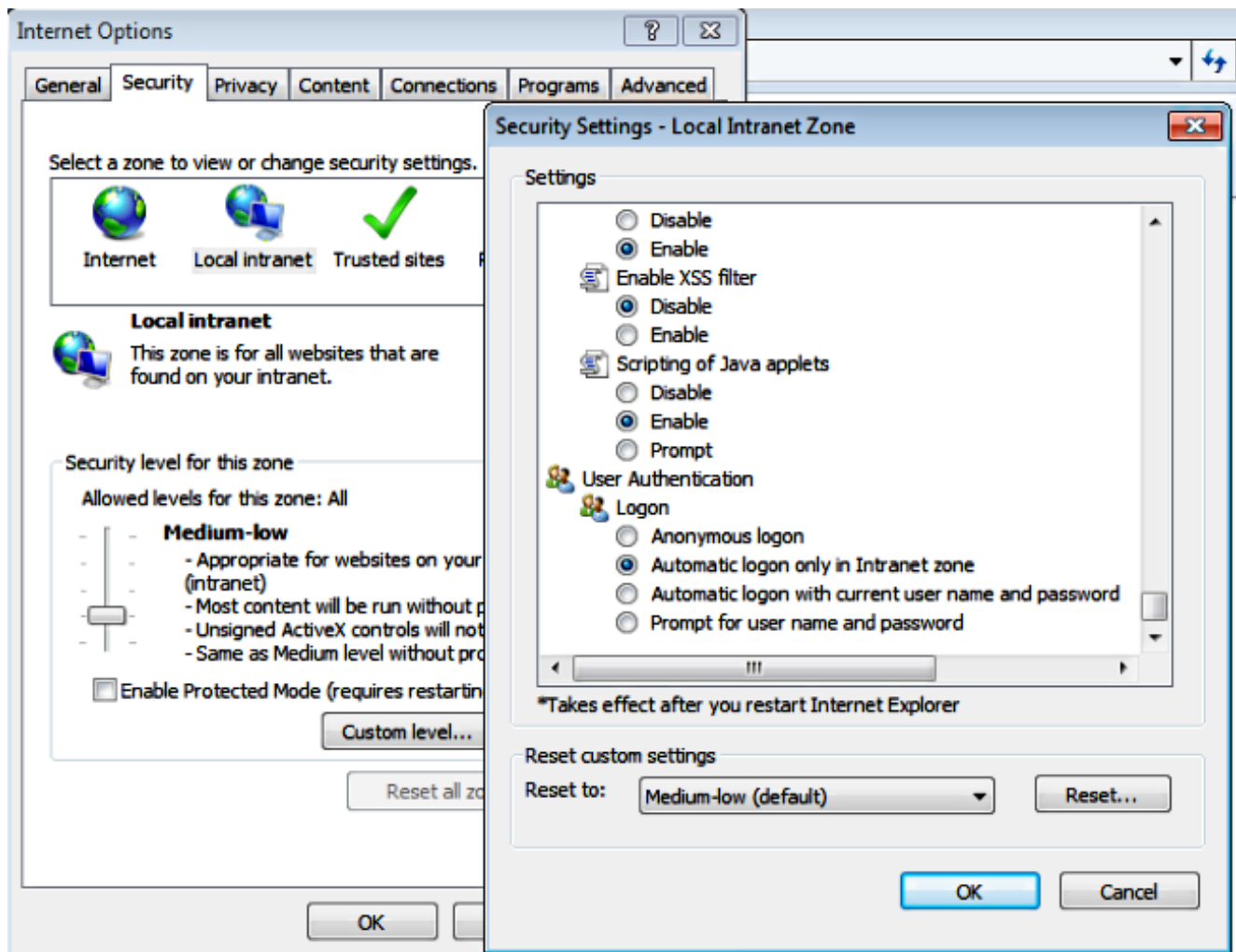


3. Aggiungere i nomi host CUCM, IMP e Unity a **Sicurezza > Siti attendibili**.



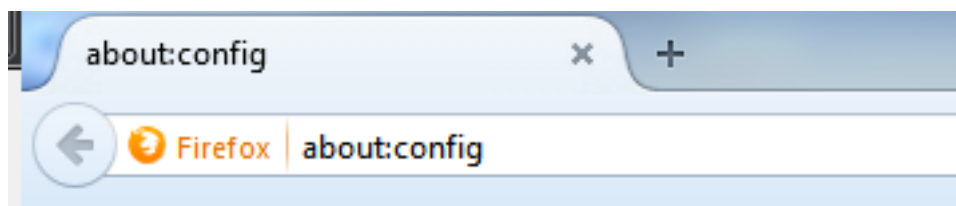
4. Verificare che Internet Explorer > **protezione** > **Intranet locale** > **Impostazioni protezione** > **Autenticazione utente - Accesso** sia configurato per utilizzare le credenziali di accesso per i siti Intranet.





## Mozilla Firefox

1. Aprire Firefox e immettere **about:config** nella barra degli indirizzi.

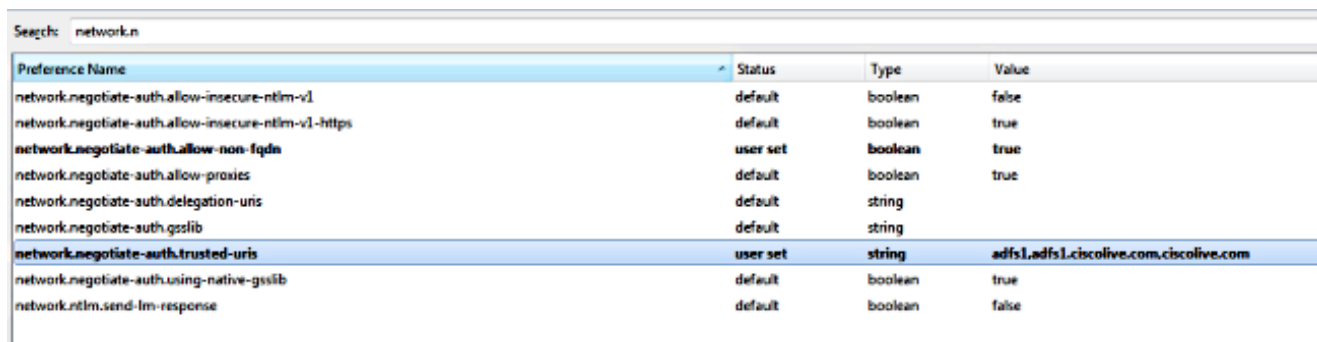


2. Clicca su **Attenzione, te lo prometto!**





3. Fare doppio clic sul nome della preferenza `network.negotiation-auth.allow-non-fqdn` su `true` e `network.negotiation-auth.trusted-uris` su `ciscolive.com,adfs1.ciscolive.com` per apportare modifiche.

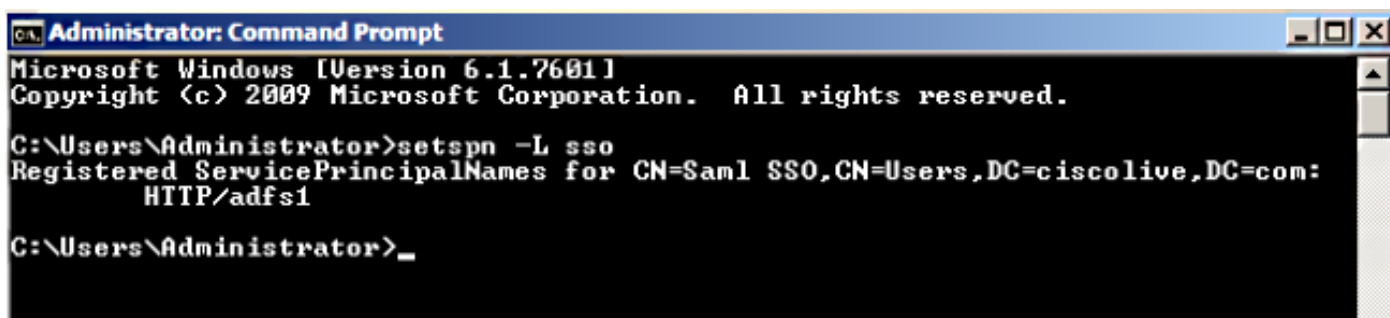


Preference Name	Status	Type	Value
network.negotiate-auth.allow-insecure-ntlm-v1	default	boolean	false
network.negotiate-auth.allow-insecure-ntlm-v1-https	default	boolean	true
network.negotiate-auth.allow-non-fqdn	user set	boolean	true
network.negotiate-auth.allow-proxies	default	boolean	true
network.negotiate-auth.delegation-uris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

4. Chiudere Firefox e riaprire.

## Verifica

Per verificare che gli SPN per il server AD FS siano stati creati correttamente, immettere il comando `setspn` e visualizzare l'output.

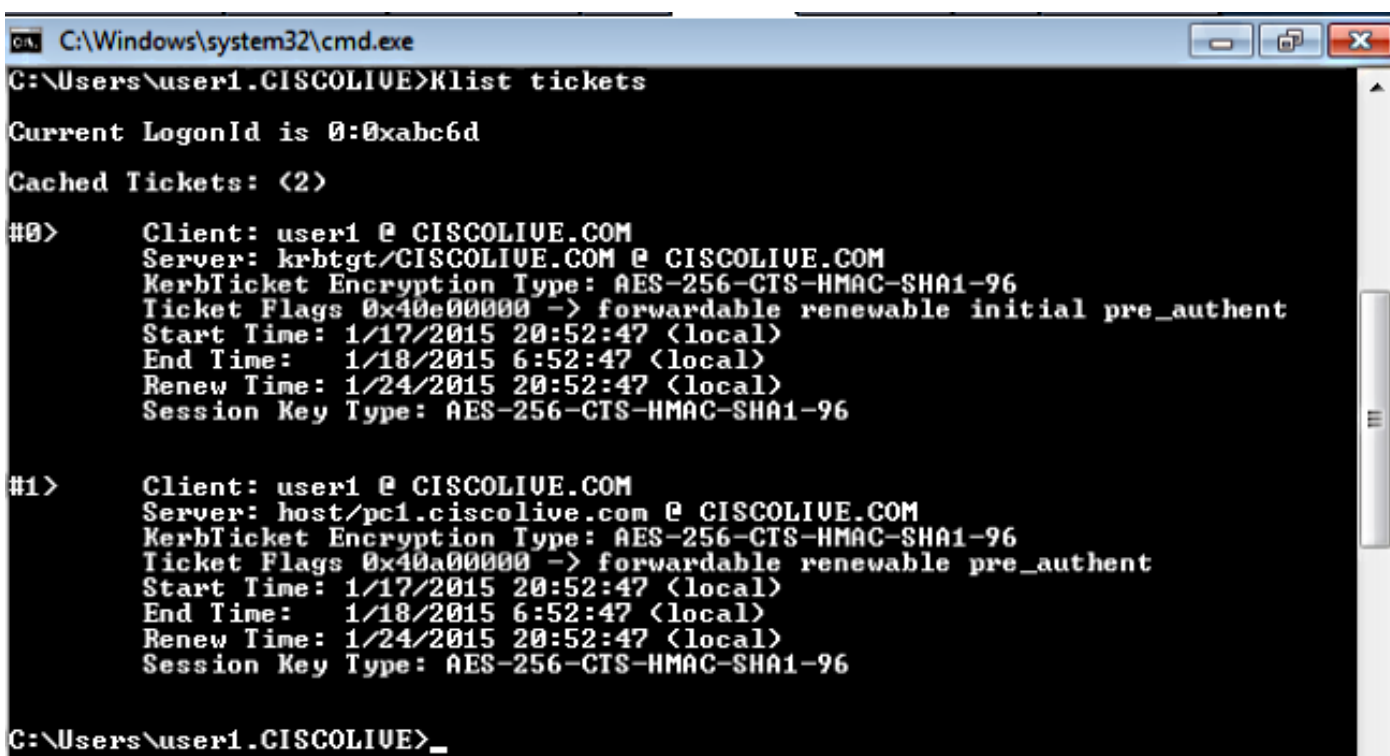


```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>setspn -L sso
Registered ServicePrincipalNames for CN=Sam1 SSO,CN=Users,DC=ciscolive,DC=com:
    HTTP/adfs1

C:\Users\Administrator>_
```

Verificare se i computer client dispongono di ticket Kerberos:



```
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/pci.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>_
```



