

Configuration de SAML SSO avec authentification Kerberos

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Configurer AD FS](#)

[Configurer le navigateur](#)

[Microsoft Internet Explorer](#)

[Mozilla FireFox](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer Active Directory et Active Directory Federation Service (AD FS) Version 2.0 afin de lui permettre d'utiliser l'authentification Kerberos par des clients Jabber (Microsoft Windows uniquement), qui permet aux utilisateurs de se connecter avec leur connexion Microsoft Windows et de ne pas être invités à entrer des informations d'identification.

Attention : Ce document est basé sur un environnement de travaux pratiques et suppose que vous connaissez l'impact des modifications que vous apportez. Reportez-vous à la documentation produit pertinente afin de comprendre l'impact des modifications que vous apportez.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez :

- AD FS version 2.0 installé et configuré avec les produits de collaboration Cisco en tant que confiance de la partie de confiance
- Produits de collaboration tels que la messagerie instantanée et la présence de Cisco Unified Communications Manager (CUCM), Cisco Unity Connection (UCXN) et CUCM activés afin

d'utiliser le langage de balisage de sécurité (SAML) SSO (Single Sign-on)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

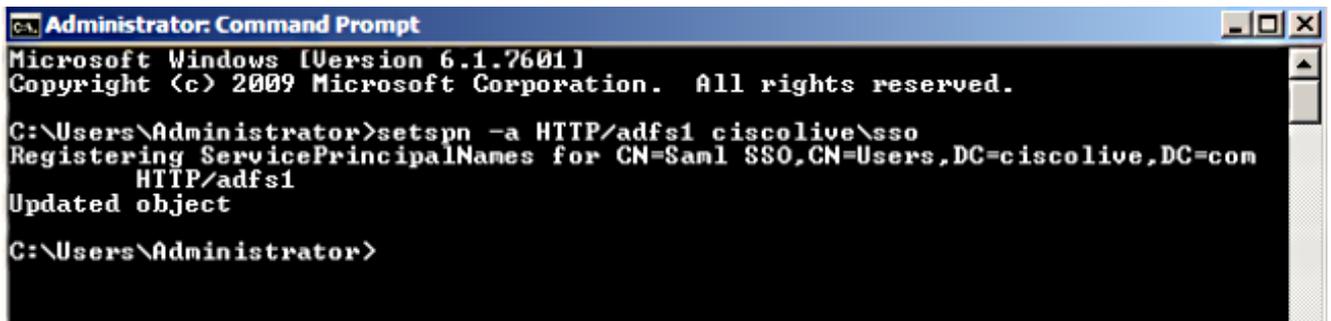
- Active Directory 2008 (Nom d'hôte : ADFS1.ciscolive.com)
- AD FS version 2.0 (nom d'hôte : ADFS1.ciscolive.com)
- CUCM (nom d'hôte : CUCM1.ciscolive.com)
- Microsoft Internet Explorer version 10
- Mozilla Firefox version 34
- Telerik Fiddler Version 4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

Configurer AD FS

1. Configurez AD FS version 2.0 avec le nom principal de service (SPN) afin d'activer l'ordinateur client sur lequel Jabber est installé pour demander des tickets, ce qui permet à son tour à l'ordinateur client de communiquer avec un service 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>
```

Reportez-vous à [AD FS 2.0 : Comment configurer le SPN \(servicePrincipalName\) pour le compte de service](#) pour plus d'informations.

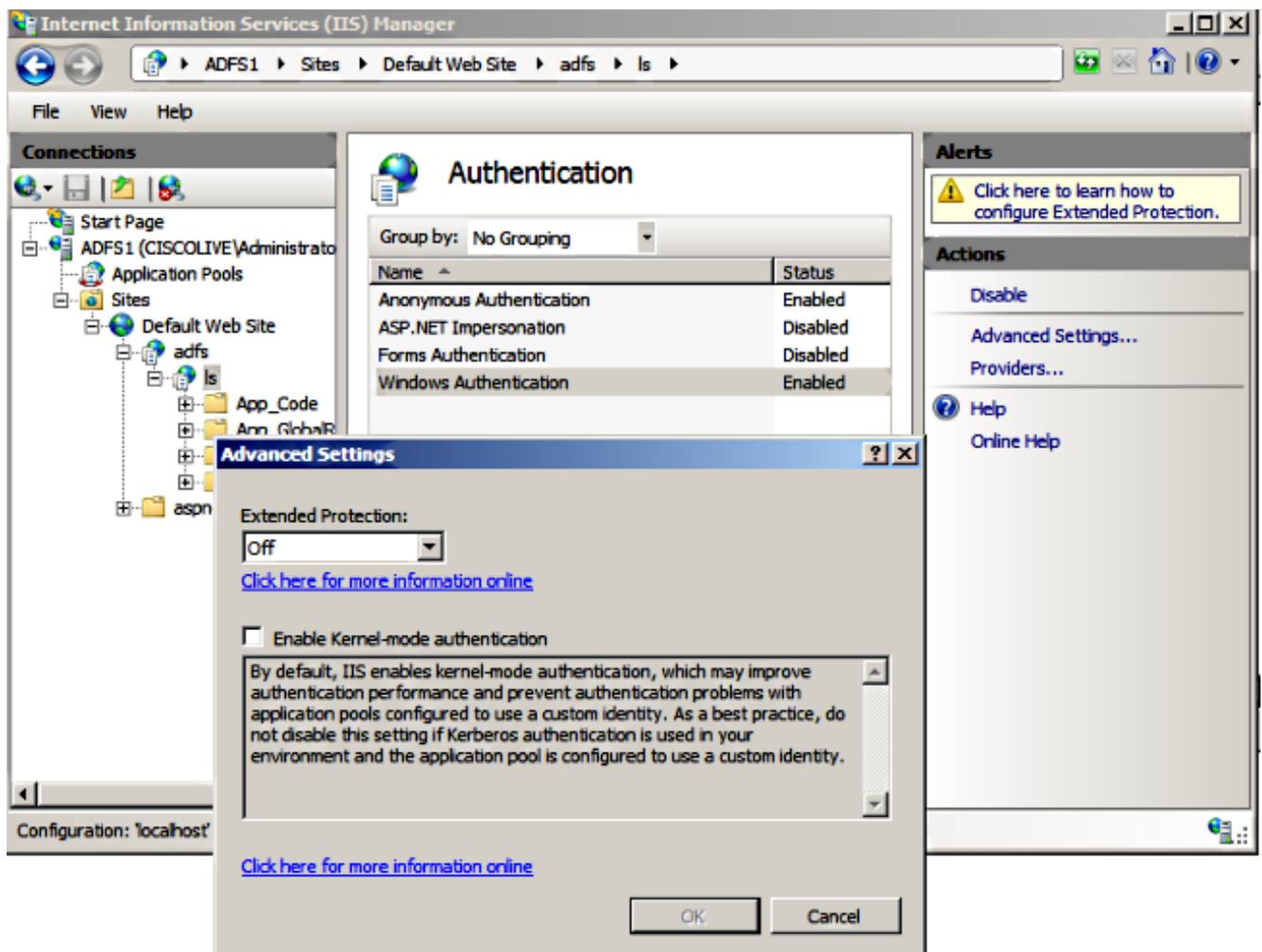
2. Assurez-vous que la configuration d'authentification par défaut pour le service AD FS (dans `C:\inetpub\adfs\ls\web.config`) est **Authentification Windows intégrée**. Assurez-vous qu'il n'a pas été modifié en **Authentification basée sur les formulaires**.

```

<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>

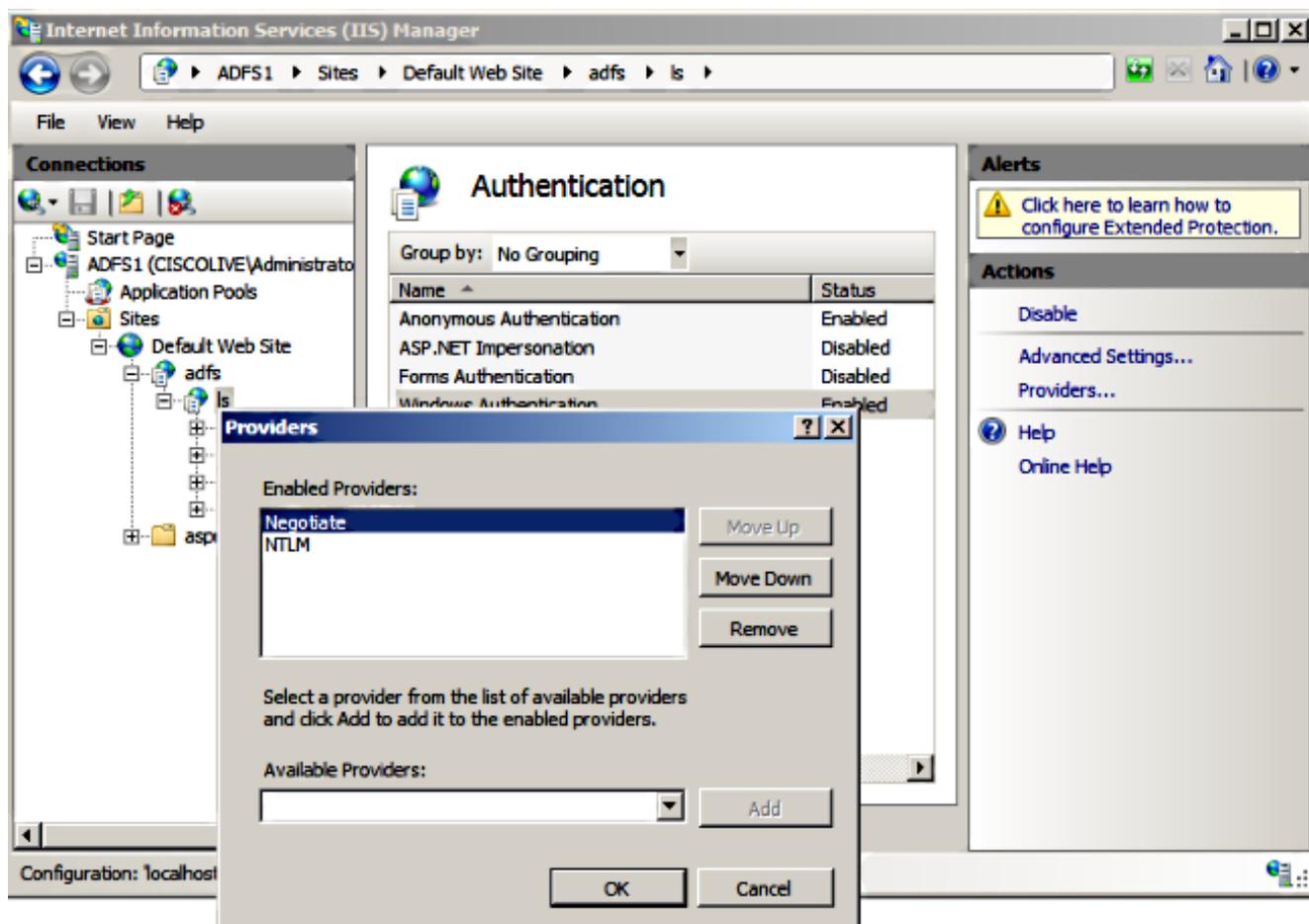
```

3. Sélectionnez **Authentification Windows** et cliquez sur **Paramètres avancés** dans le volet de droite. Dans Paramètres avancés, décochez **Activer l'authentification en mode noyau**, assurez-vous que la protection étendue est **désactivée**, puis cliquez sur **OK**.



4. Assurez-vous qu'AD FS version 2.0 prend en charge le protocole Kerberos et le protocole NTLM (NT LAN Manager), car tous les clients non Windows ne peuvent pas utiliser Kerberos et utiliser NTLM.

Dans le volet de droite, sélectionnez **Fournisseurs** et assurez-vous que **Négociateur** et **NTLM** sont présents sous Fournisseurs activés :



Note: AD FS transmet l'en-tête de sécurité Negotiate lorsque l'authentification Windows intégrée est utilisée afin d'authentifier les requêtes client. L'en-tête de sécurité Negotiate permet aux clients de sélectionner entre l'authentification Kerberos et l'authentification NTLM. Le processus de négociation sélectionne l'authentification Kerberos, sauf si l'une de ces conditions est vraie :

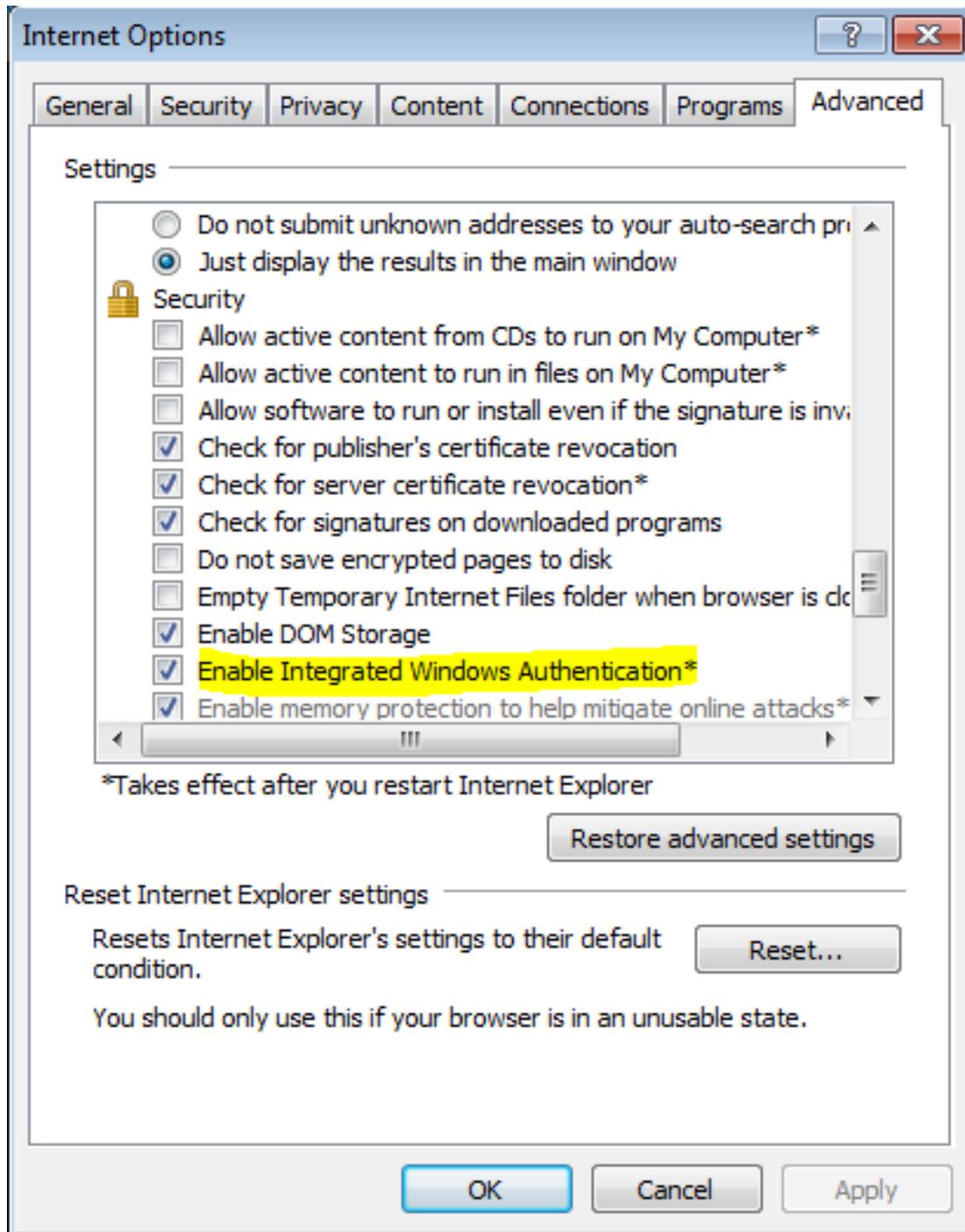
- Un des systèmes impliqués dans l'authentification ne peut pas utiliser l'authentification Kerberos.
- L'application appelante ne fournit pas suffisamment d'informations pour utiliser l'authentification Kerberos.
- Pour permettre au processus de négociation de sélectionner le protocole Kerberos pour l'authentification réseau, l'application cliente doit fournir un nom de compte SPN, un nom d'utilisateur principal (UPN) ou un nom de compte NetBIOS (Network Basic Input/Output System) comme nom cible. Sinon, le processus de négociation sélectionne toujours le protocole NTLM comme méthode d'authentification préférée.

Configurer le navigateur

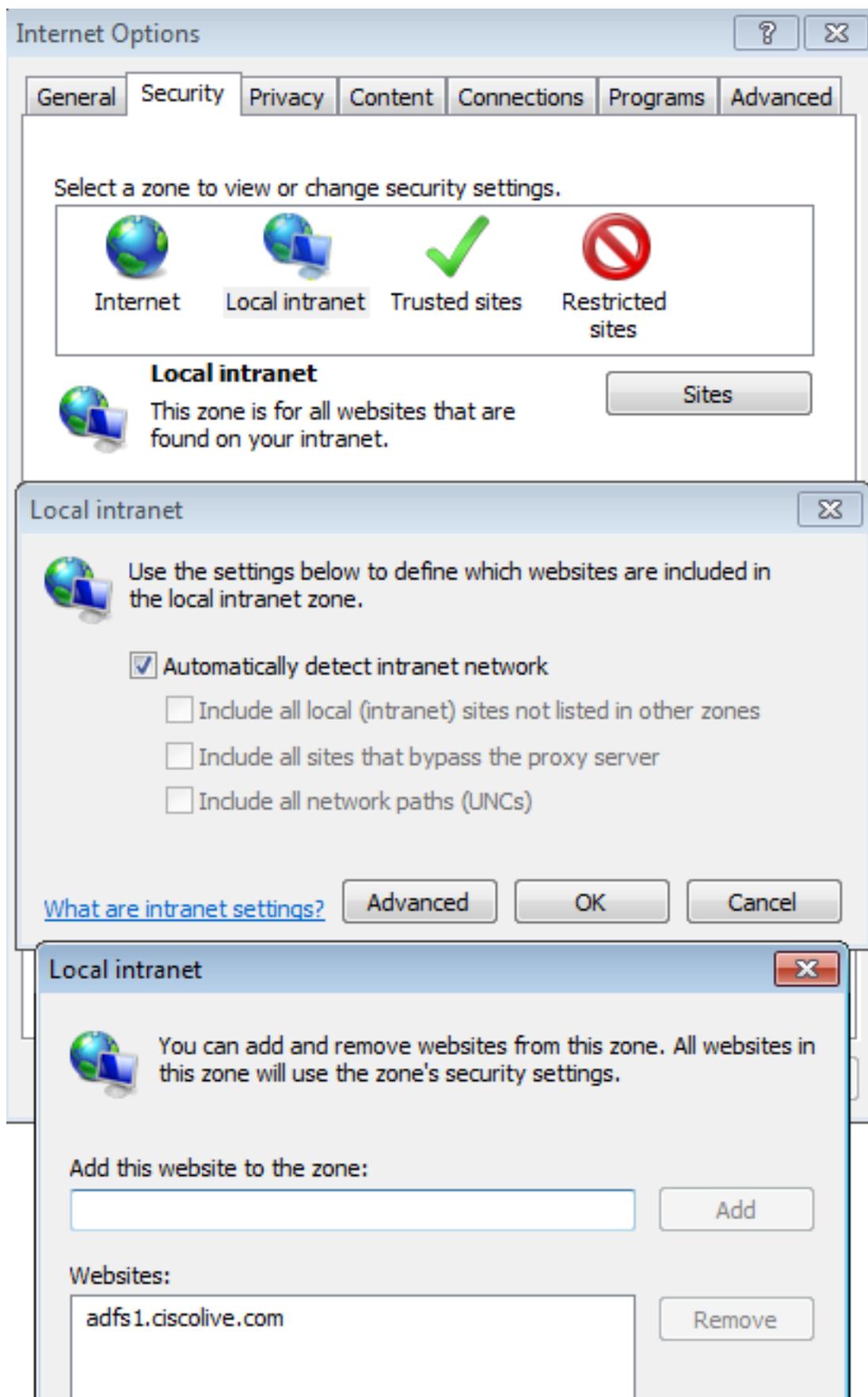
Microsoft Internet Explorer

1. Assurez-vous que Internet Explorer > Advanced > Enable Integrated Windows Authentication

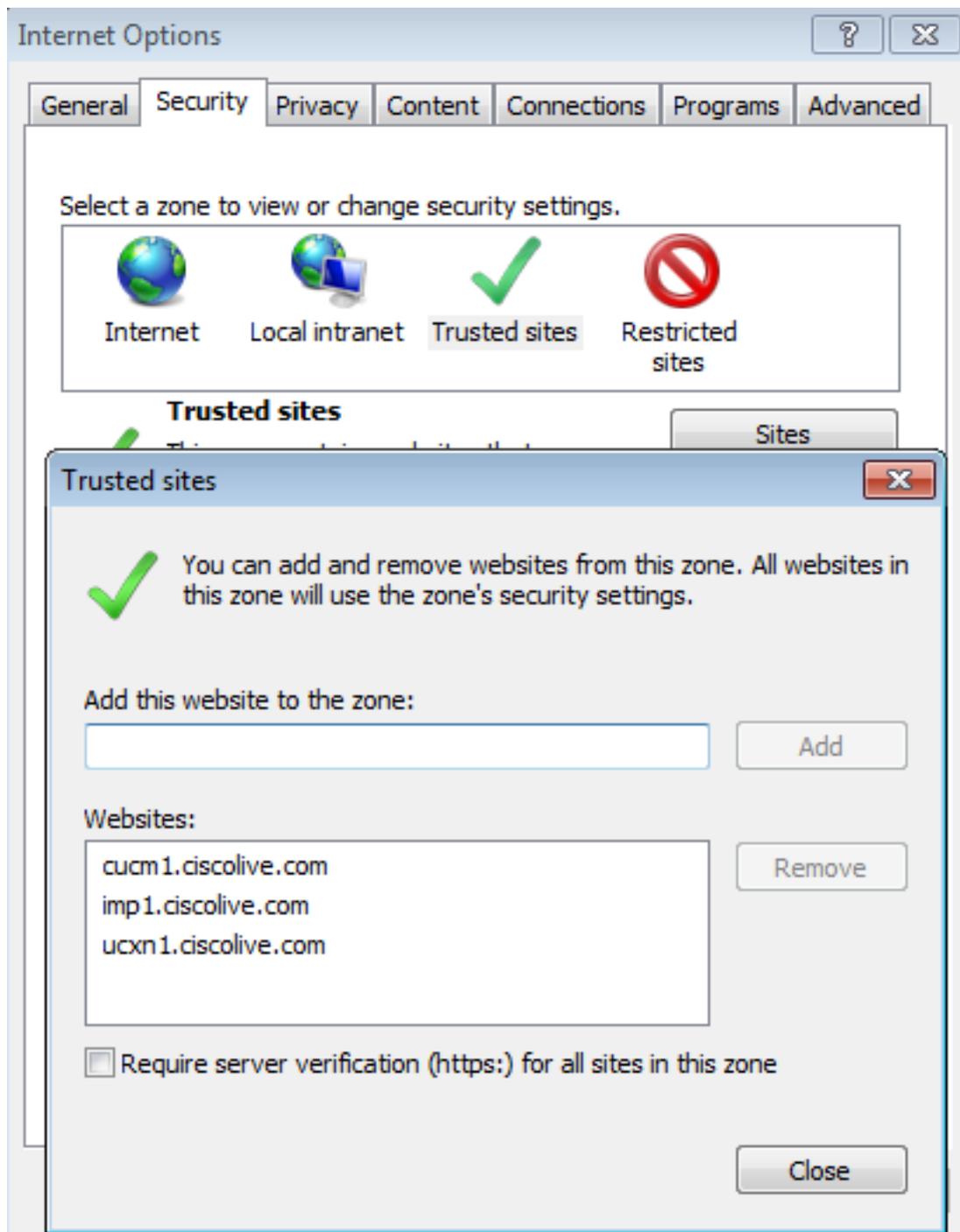
est coché.



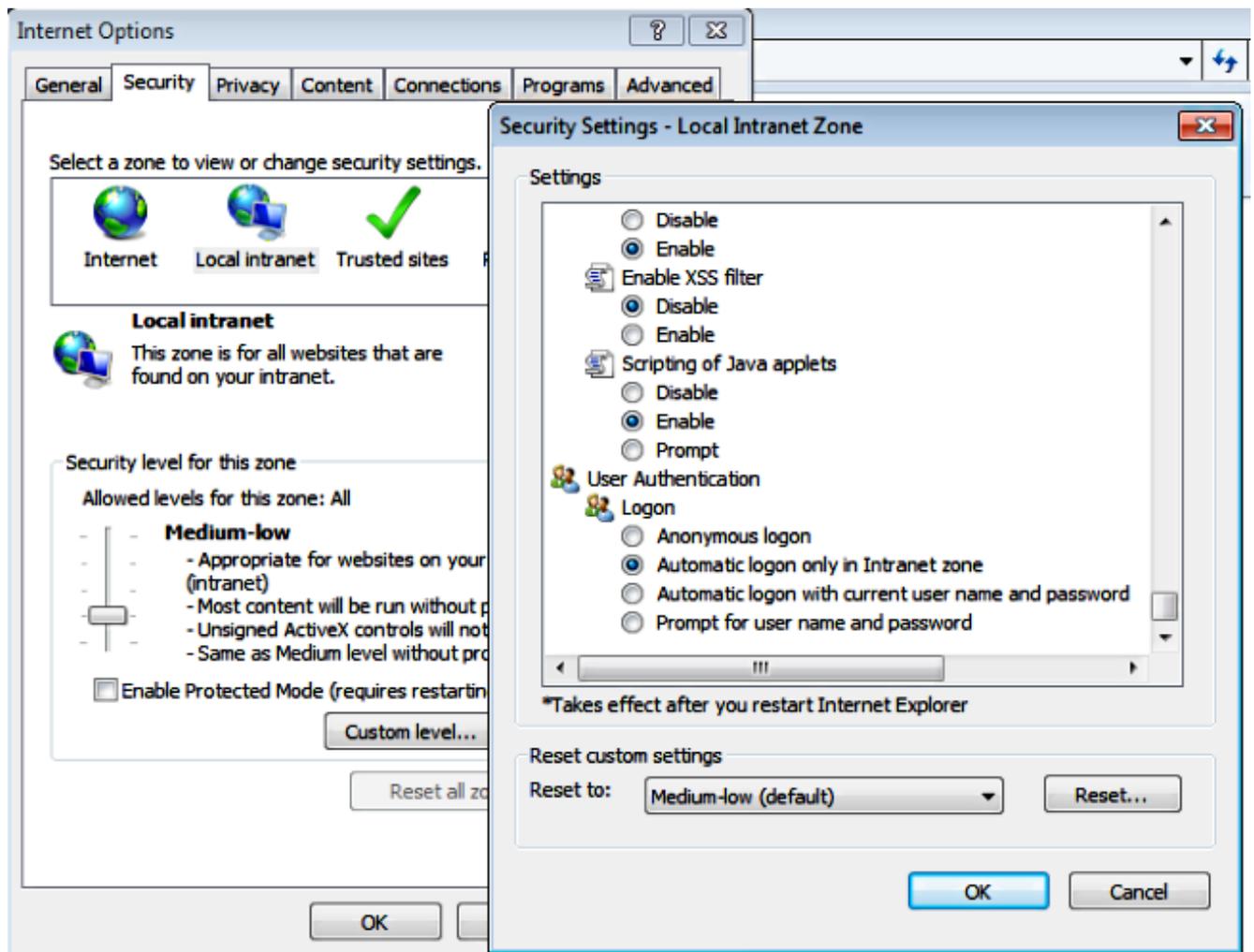
2. Ajoutez l'URL AD FS sous **Sécurité >Zones Intranet > Sites**.



3. Ajoutez les noms d'hôte CUCM, IMP et Unity à **Security >Trusted Sites**.

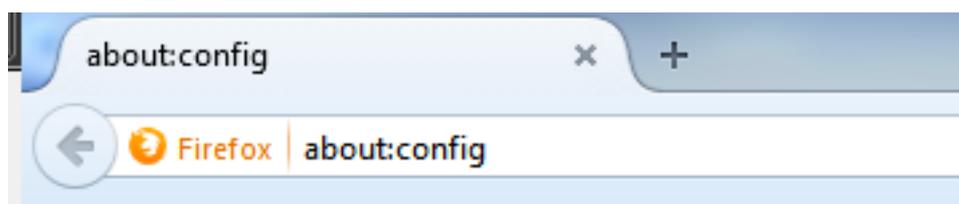


4. Assurez-vous que Internet Explorer > **security** > **Local Intranet** > **Security Settings** > **User Authentication - Logon** est configuré afin d'utiliser les informations d'identification de connexion pour les sites intranet.



Mozilla FireFox

1. Ouvrez Firefox et entrez **about:config** dans la barre d'adresse.



2. Cliquez sur **Je serai prudent, je vous le promets !**



3. Double-cliquez sur le nom de préférence `network.negotiation-auth.allow-non-fqdn` pour `true` et `network.negotiation-auth.trusted-uris` pour `ciscolive.com,adfs1.ciscolive.com` afin de modifier.

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. Fermez Firefox et rouvrez-vous.

Vérification

Afin de vérifier que les SPN du serveur AD FS sont correctement créés, entrez la commande `setspn` et affichez le résultat.

```
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>_
```

Vérifiez si les ordinateurs clients ont des tickets Kerberos :

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

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

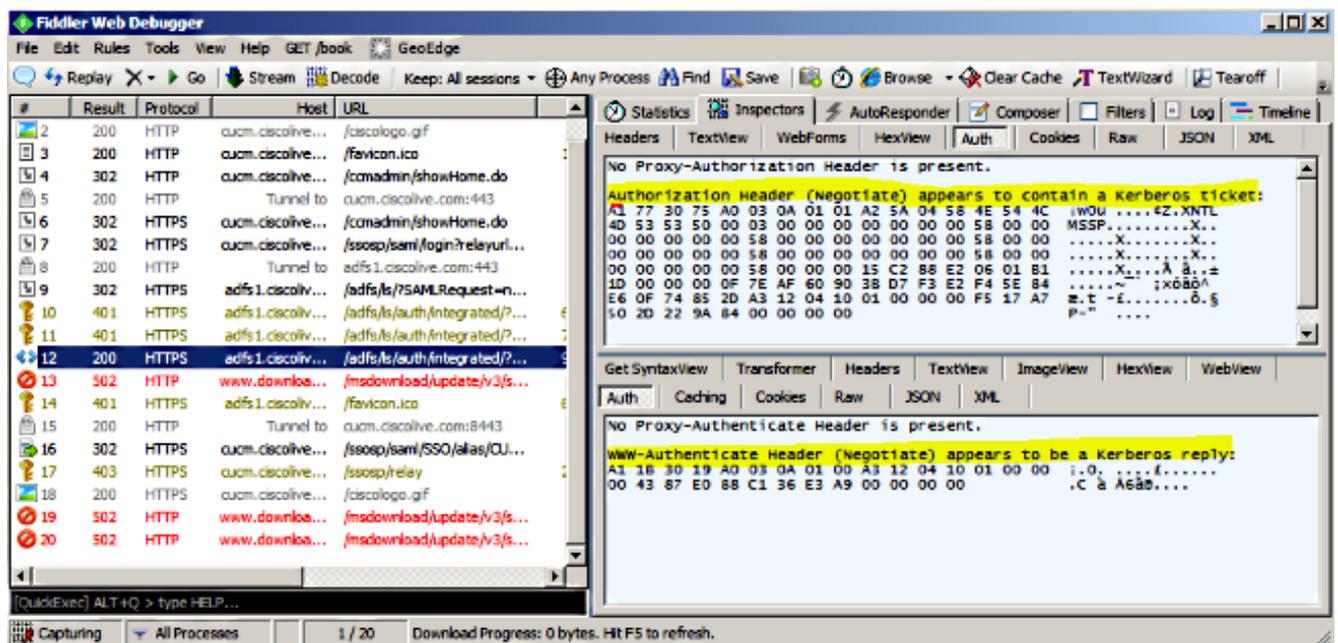
#0> Client: user1 @ CISCOLIVE.COM
Server: krbtgt/CISCOLIVE.COM @ CISCOLIVE.COM
KerberosTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
Start Time: 1/17/2015 20:52:47 (local)
End Time: 1/18/2015 6:52:47 (local)
Renew Time: 1/24/2015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

Complétez ces étapes afin de vérifier quelle authentification (authentification Kerberos ou NTLM) est utilisée.

1. Téléchargez l'outil Fiddler sur votre ordinateur client et installez-le.
2. Fermez toutes les fenêtres de Microsoft Internet Explorer.
3. Exécutez l'outil Fiddler et vérifiez que l'option **Capture Traffic** est activée dans le menu Fichier. Fiddler fonctionne comme un proxy de transfert entre la machine cliente et le serveur et écoute tout le trafic.
4. Ouvrez Microsoft Internet Explorer, accédez à CUCM et cliquez sur quelques liens pour générer du trafic.
5. Reportez-vous à la fenêtre principale de Fiddler et choisissez l'une des trames où le résultat est **200** (réussite) et vous pouvez voir Kerberos comme mécanisme d'authentification



6. Si le type d'authentification est NTLM, vous voyez **Negotiate - NTLMSSP** au début de la trame, comme indiqué ici.

