Exemple de configuration de Kerberos avec ADFS 2.0 pour l'utilisateur final SAML SSO pour Jabber

Contenu

Introduction

Ce document décrit comment configurer Kerberos avec Active Directory Federation Services (ADFS) 2.0.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

Informations générales

La configuration SSO (Single Sign On) SAML (End User Security Assertion Markup Language)

nécessite la configuration de Kerberos afin de permettre à l'utilisateur final SAML SSO pour Jabber de fonctionner avec l'authentification de domaine. Lorsque SAML SSO est implémenté avec Kerberos, le protocole LDAP (Lightweight Directory Access Protocol) gère toutes les autorisations et la synchronisation utilisateur, tandis que Kerberos gère l'authentification. Kerberos est un protocole d'authentification qui est destiné à être utilisé conjointement avec une instance compatible LDAP.

Sur les machines Microsoft Windows et Macintosh qui sont jointes à un domaine Active Directory, les utilisateurs peuvent se connecter de manière transparente à Cisco Jabber sans avoir à entrer un nom d'utilisateur ou un mot de passe et ils ne voient même pas d'écran de connexion. Les utilisateurs qui ne sont pas connectés au domaine sur leurs ordinateurs voient toujours un formulaire de connexion standard.

Étant donné que l'authentification utilise un jeton unique transmis par les systèmes d'exploitation, aucune redirection n'est requise. Le jeton est vérifié par rapport au contrôleur de domaine de clé (KDC) configuré et, s'il est valide, l'utilisateur est connecté.

Configuration

Voici la procédure à suivre pour configurer Kerberos avec ADFS 2.0.

1. Installez Microsoft Windows Server 2008 R2 sur une machine.

2. Installez les services de domaine Active Directory (ADDS) et ADFS sur le même ordinateur.

3. Installez Internet Information Services (IIS) sur l'ordinateur Microsoft Windows Server 2008 R2 installé.

4. Créez un certificat auto-signé pour IIS.

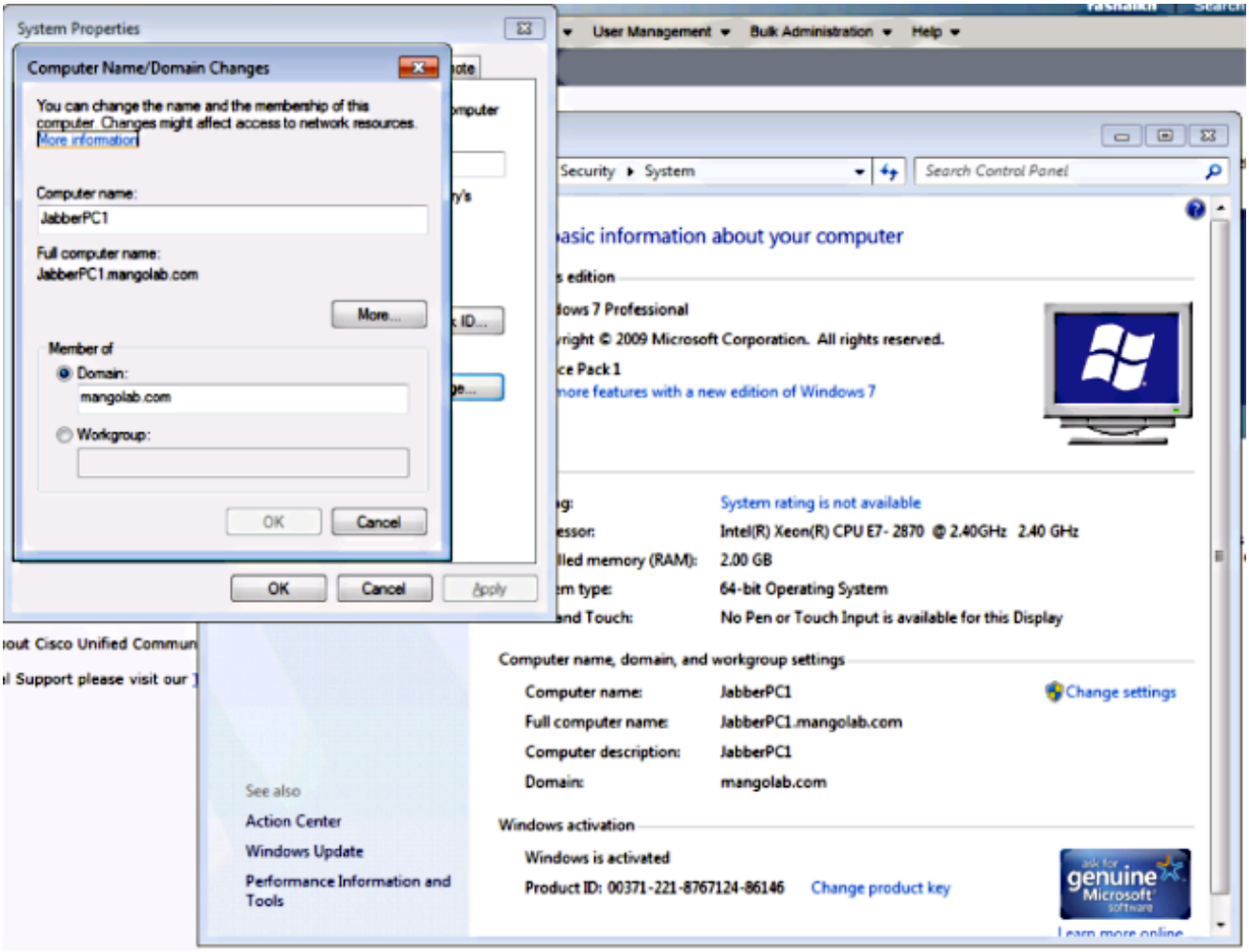
5. Importez le certificat auto-signé dans IIS et utilisez-le comme certificat de serveur HTTPS.

6. Installez Microsoft Windows7 sur un autre ordinateur et utilisez-le comme client.

   Remplacez le serveur de noms de domaine (DNS) par l'ordinateur sur lequel vous avez installé ADDS.

   Ajoutez cet ordinateur au domaine que vous avez créé lors de l'installation d'ADDS.

   Allez à **Démarrer**.Cliquez avec le bouton droit sur **Ordinateur**.Cliquez sur **Properties**.Cliquez sur **Modifier les paramètres** à droite de la fenêtre.Cliquez sur l'onglet **Computer Name.**Cliquez sur **Change**.Ajoutez le domaine que vous avez créé.



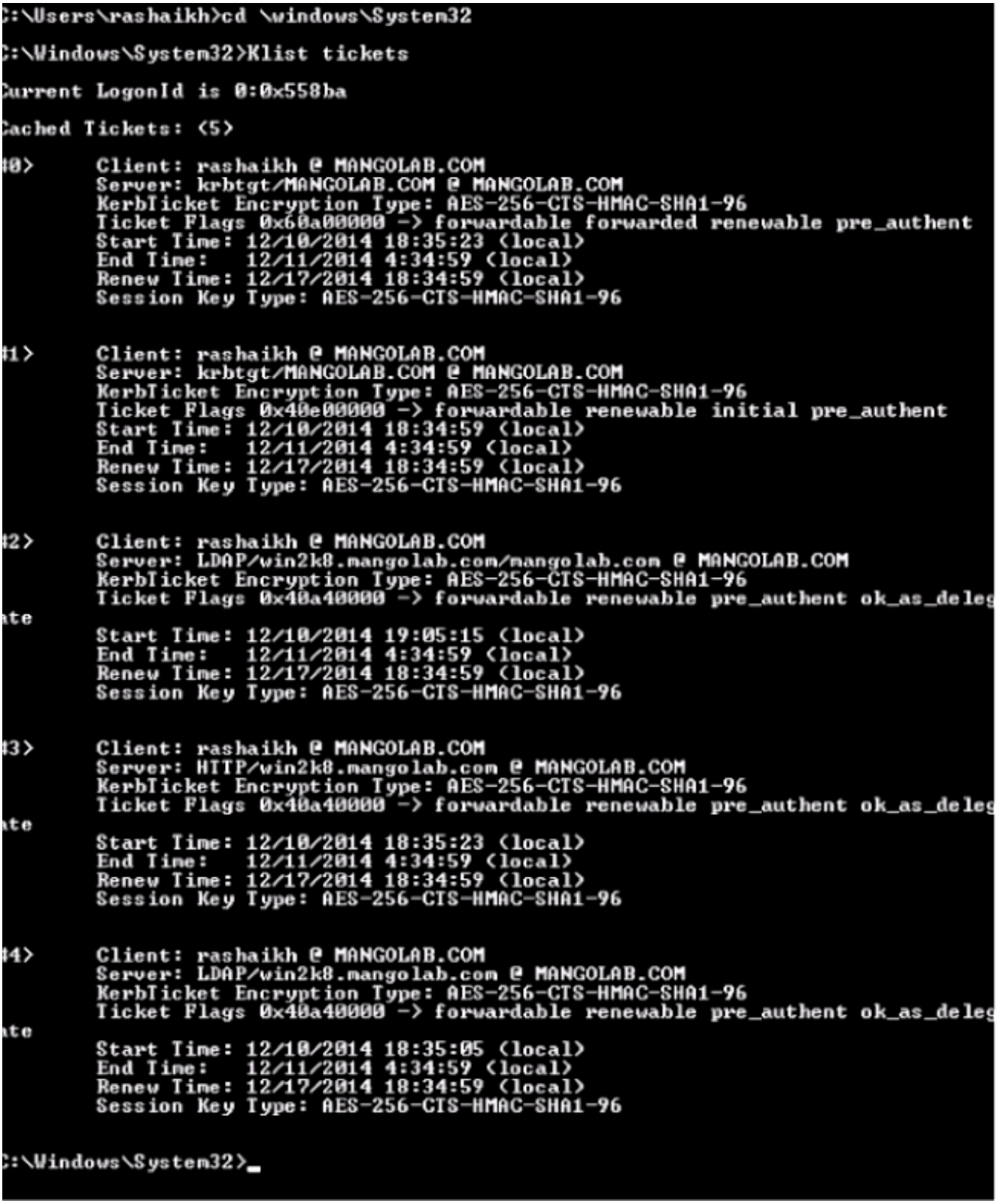
7. Vérifiez si le service Kerberos génère sur les deux machines.

   Connectez-vous en tant qu'administrateur sur l'ordinateur serveur et ouvrez l'invite de commandes. Exécutez ensuite ces commandes :

   cd \windows\System32Billets Klist

```
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
```

   Connectez-vous en tant qu'utilisateur de domaine sur l'ordinateur client et exécutez les mêmes commandes.



8. Créez l'identité Kerberos ADFS sur l'ordinateur sur lequel vous avez installé ADDS.

   L'administrateur Microsoft Windows connecté au domaine Microsoft Windows (en tant que <nom du domaine>\administrateur), par exemple sur le contrôleur de domaine Microsoft Windows, crée l'identité Kerberos ADFS. Le service HTTP ADFS doit avoir une identité Kerberos appelée SPN (Service Principal Name) au format suivant : **HTTP/DNS_name_of_ADFS_server**.

   Ce nom doit être mappé à l'utilisateur Active Directory qui représente l'instance du serveur

HTTP ADFS. Utilisez l'utilitaire **setspn** Microsoft Windows, qui doit être disponible par défaut sur un serveur Microsoft Windows 2008.

Procédure Enregistrez les SPN pour le serveur ADFS. Sur le contrôleur de domaine Active Directory, exécutez la commande **setspn**.

Par exemple, lorsque l'hôte ADFS est **adfs01.us.renovations.com** et que le domaine Active Directory est **US.RENOVATIONS.COM**, la commande est :

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

La partie **HTTP/**du SPN s'applique, même si le serveur ADFS est généralement accessible par SSL (Secure Sockets Layer), qui est HTTPS.

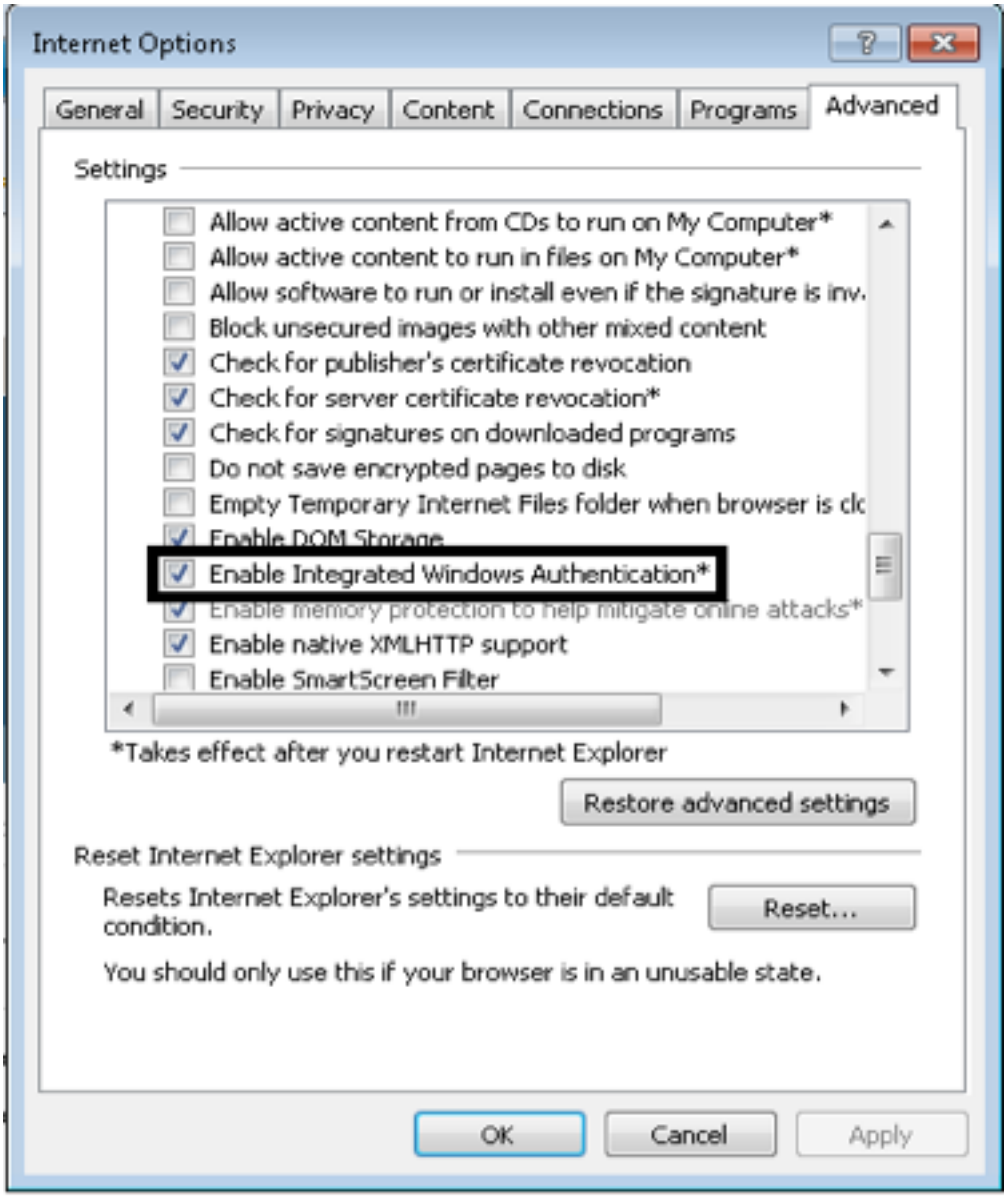
Vérifiez que les SPN du serveur ADFS sont correctement créés à l'aide de la commande **setspn** et affichez le résultat.

```
setspn -L
```

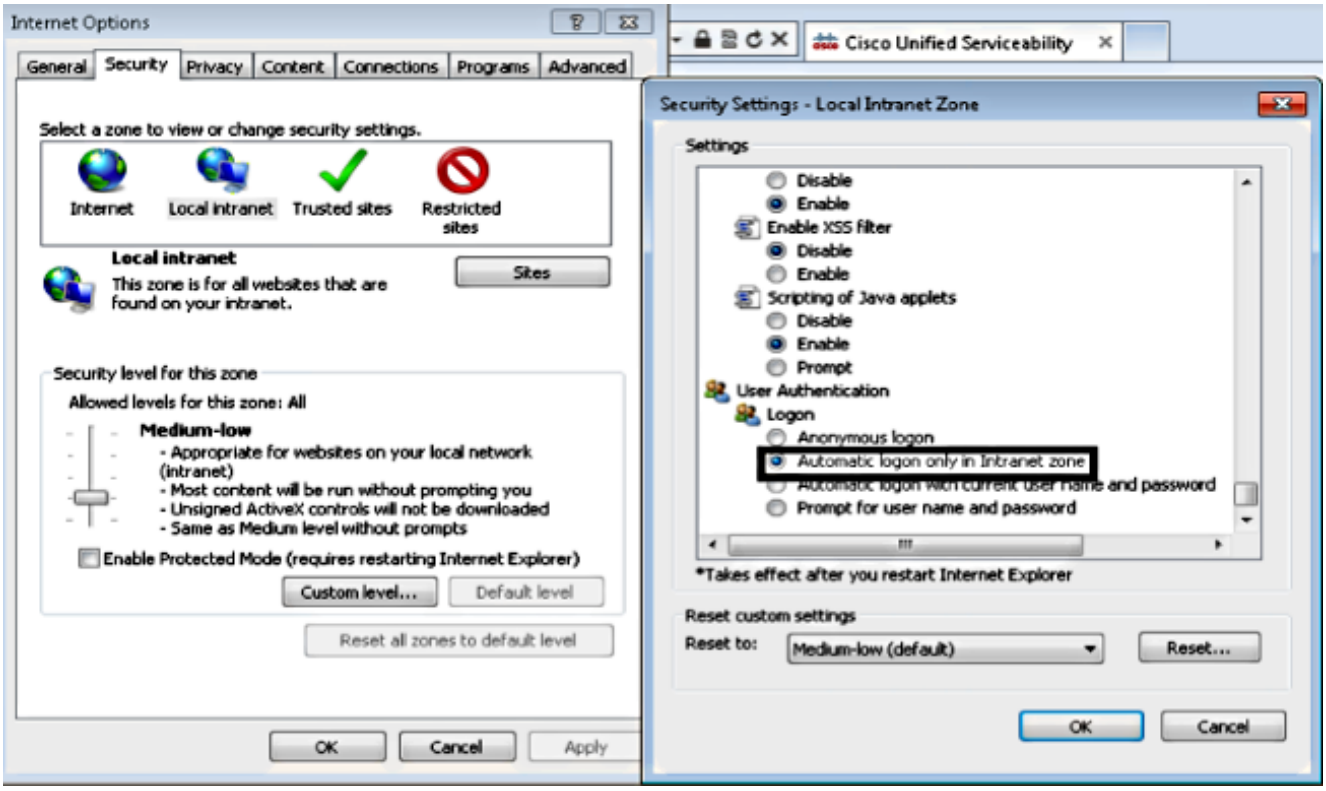
9. Configurez les paramètres du navigateur du client Microsoft Windows.

   Accédez à **Outils > Options Internet > Avancé** afin d'activer l'authentification Windows intégrée.

   Cochez la **case Activer l'authentification Windows intégrée** :

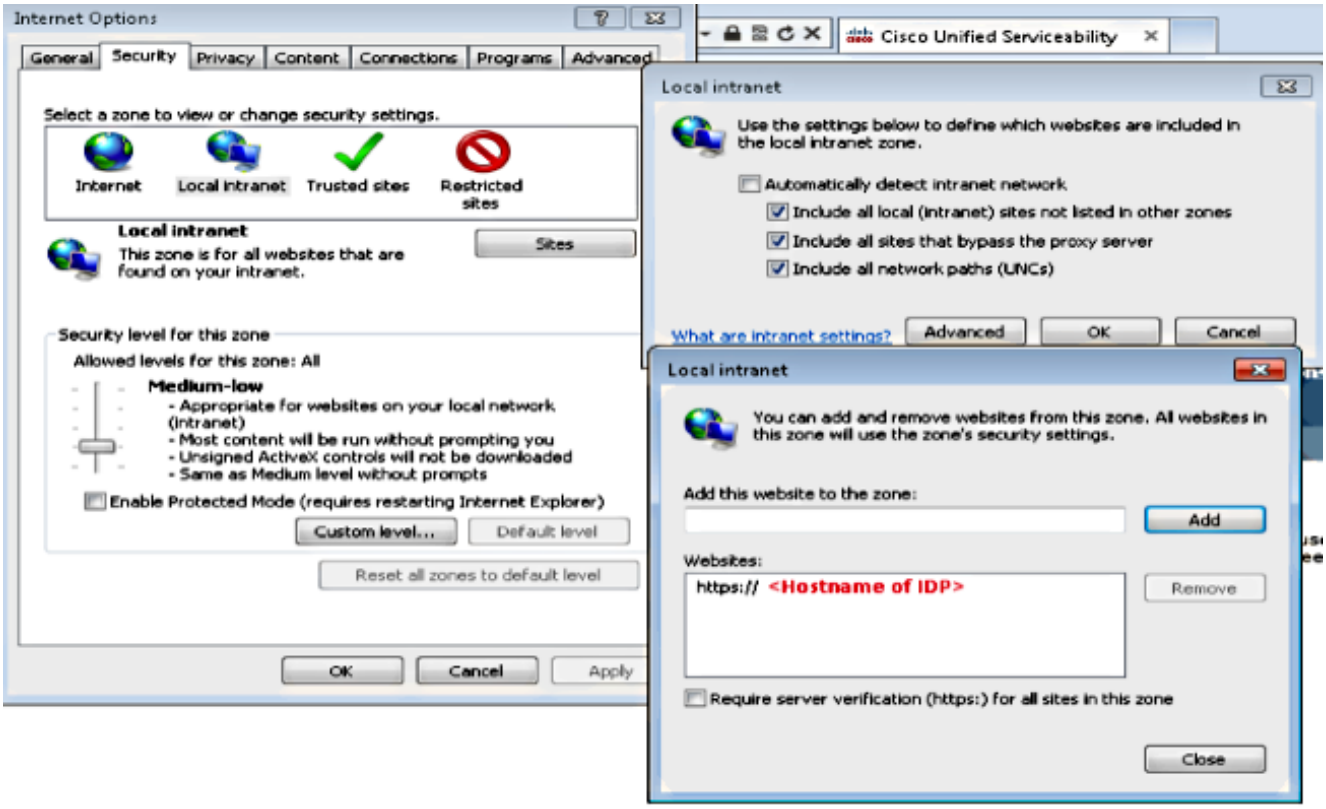


   Accédez à **Outils > Options Internet > Sécurité > Intranet local > Niveau personnalisé...** afin de sélectionner **Connexion automatique uniquement dans la zone Intranet**.

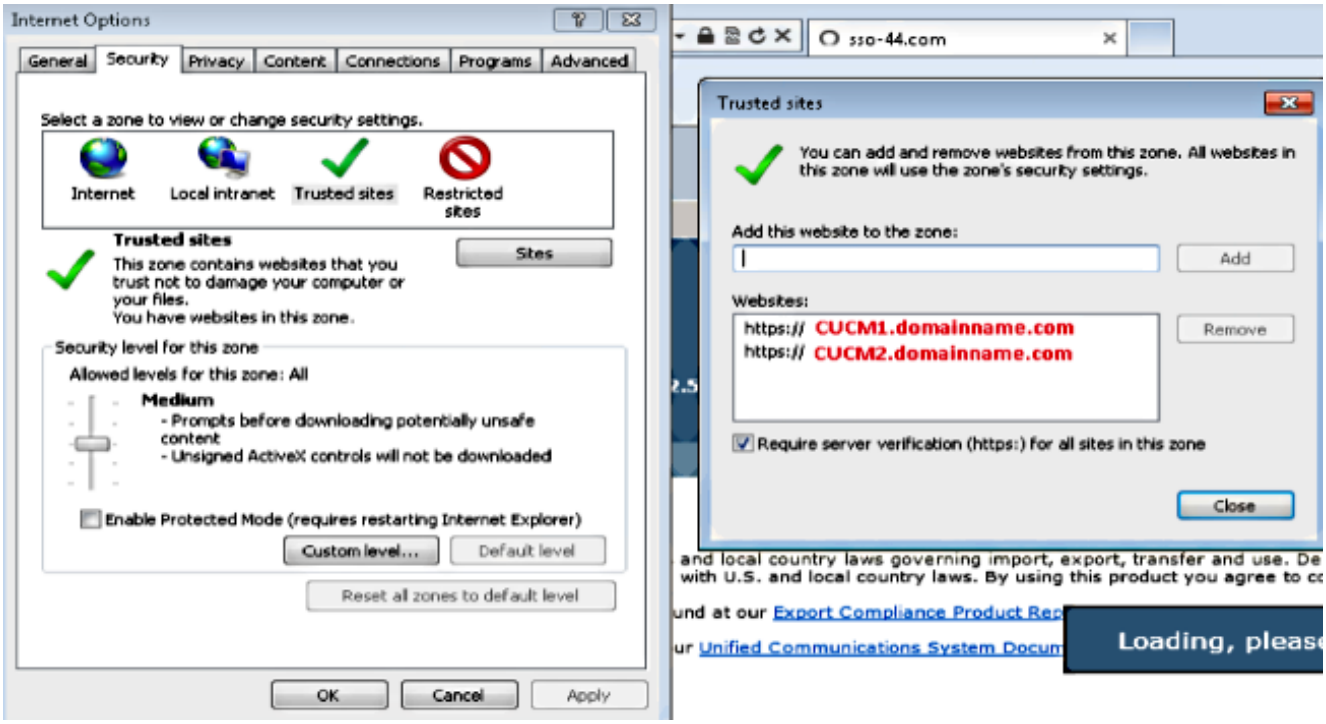


Accédez à **Outils > Options Internet > Sécurité > Intranet local > Sites > Avancé** afin d'ajouter l'URL de détection et de prévention des intrusions (IDP) aux sites Intranet local.

Note: Cochez toutes les cases de la boîte de dialogue Intranet local et cliquez sur l'**onglet Avancé**.



Accédez à **Outils > Sécurité > Sites de confiance > Sites** afin d'ajouter les noms d'hôte CUCM aux sites de confiance :



Vérification

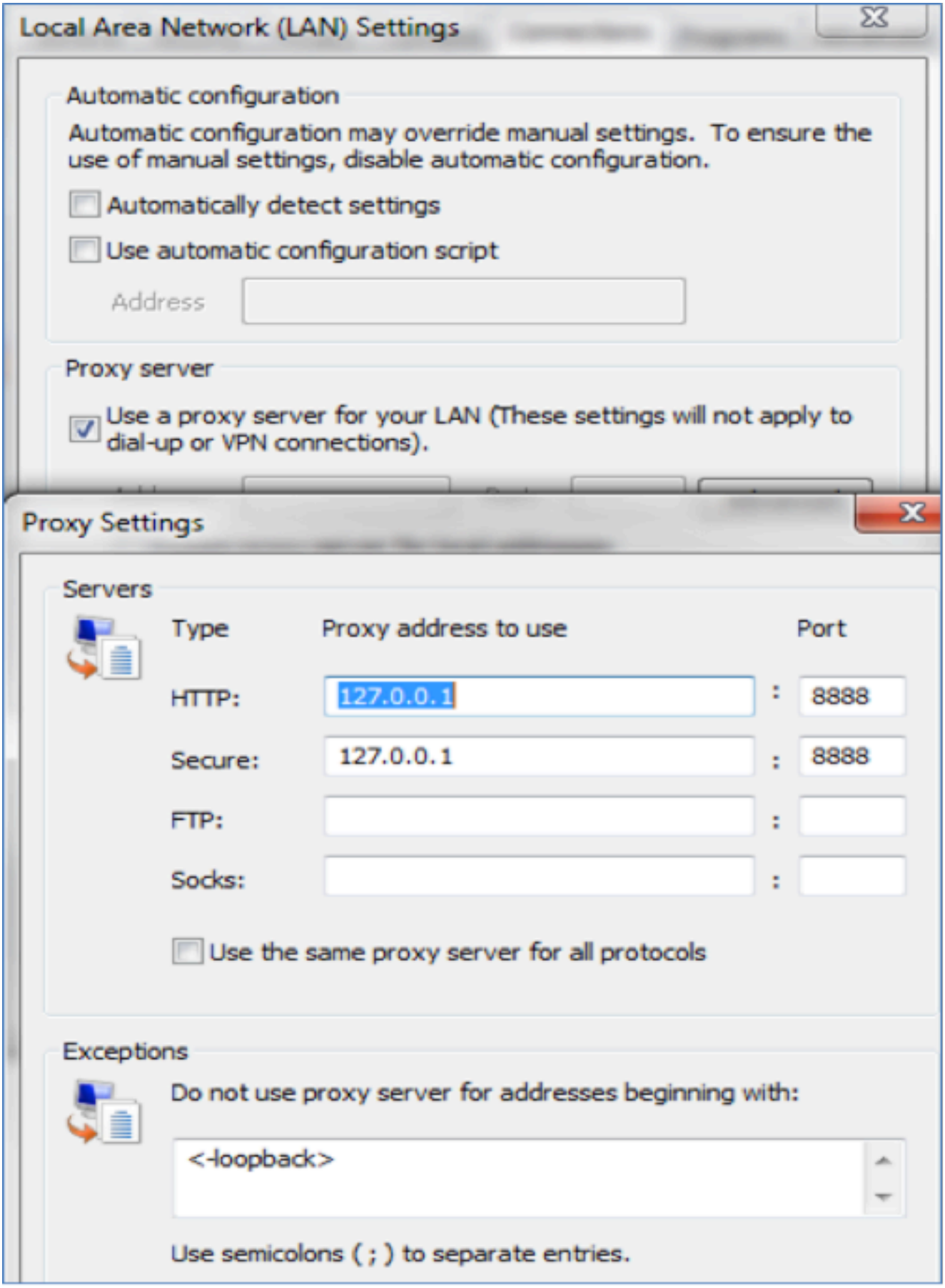
Cette section explique comment vérifier quelle authentification (authentification Kerberos ou NT LAN Manager (NTLM)) est utilisée.

1. Téléchargez l'outil Fiddler sur votre machine cliente et installez-le.

2. Fermez toutes les fenêtres Internet Explorer.

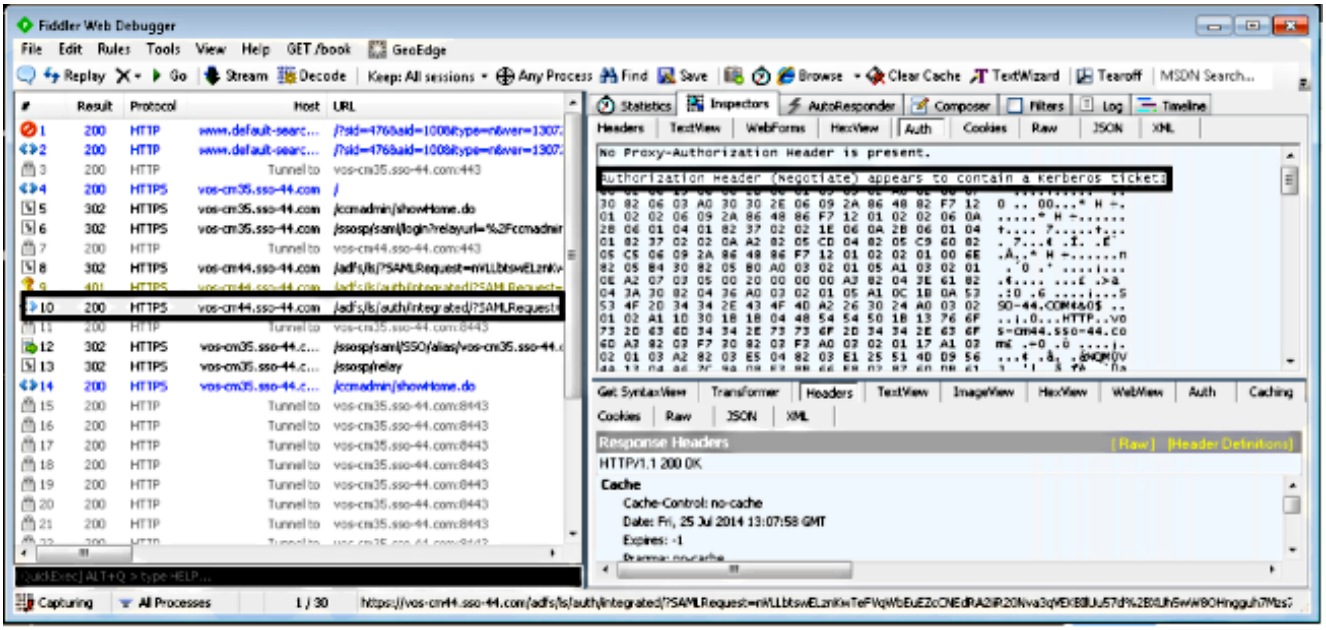
3. Exécutez l'outil Fiddler et vérifiez que l'option **Capture Traffic** est activée dans le menu Fichier.

   Fiddler fonctionne comme un proxy de transfert entre l'ordinateur client et le serveur et écoute tout le trafic, qui définit temporairement vos paramètres Internet Explorer comme suit :

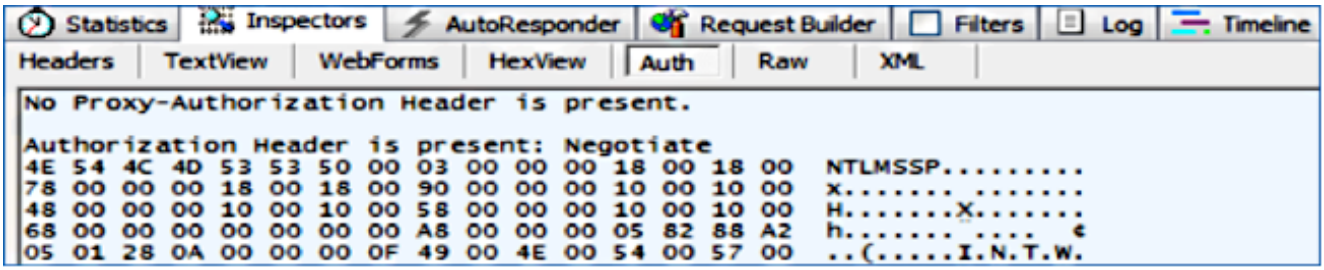


4. Ouvrez Internet Explorer, accédez à l'URL de votre serveur de gestion de la relation client (CRM) et cliquez sur quelques liens pour générer du trafic.

5. Reportez-vous à la fenêtre principale de Fiddler et choisissez l'une des trames dont le résultat est 200 (réussite) :



Si le type d'authentification est NTLM, **Negotiate - NTLMSSP** apparaît au début de la trame, comme indiqué ici :



Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.