

Dépannage des proxies HTTP pour le client d'itinérance Umbrella sous Windows

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Aperçu](#)

[Symptômes](#)

[Identifier s'il existe un proxy](#)

[Scénario 1](#)

[Scénarios 2 et 3](#)

[Scénario 4](#)

[Ajouter ou supprimer des paramètres de proxy](#)

[PsExec et Internet Explorer \(IE 10 ou version ultérieure\)](#)

[Autre \(Registre\)](#)

[PsExec et MMC \(IE9 ou antérieure\)](#)

[Modifier le registre](#)

Introduction

Ce document décrit comment dépanner les proxys HTTP pour le client d'itinérance Umbrella sous Windows.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Umbrella Roaming Client sous Windows.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Aperçu

Sur certains ou tous les ordinateurs de votre déploiement Umbrella, le client d'itinérance Umbrella ne s'enregistre pas correctement. Vous remarquerez ceci parce que l'icône de la barre d'état du client d'itinérance Umbrella est rouge sur une machine, ou parce que le client d'itinérance Umbrella n'apparaît pas dans le tableau de bord comme prévu. En outre, vous utilisez actuellement, ou avez déjà utilisé, un proxy HTTP sur votre réseau. Si un client est en itinérance, il s'est connecté derrière un proxy HTTP.

Vous exécutez actuellement un proxy HTTP : Le client d'itinérance Umbrella utilise l'utilisateur « SYSTEM », car il s'exécute en tant que service système, et vous avez transmis les paramètres de configuration via l'objet de stratégie de groupe (GPO) ou un autre outil de surveillance et de gestion à distance (RMM), qui a fourni des paramètres de proxy HTTP spécifiques à l'utilisateur aux utilisateurs de votre organisation. En outre, vous avez des règles de refus par défaut dans votre pare-feu de passerelle qui n'autorisent pas le trafic HTTP/HTTPS à moins qu'il ne passe par le proxy.

Vous avez exécuté un proxy HTTP dans le passé : L'utilisateur « SYSTEM » avait précédemment défini des paramètres de proxy HTTP à un moment donné dans le passé, et maintenant ce proxy n'existe plus. Comme le proxy n'existe plus, l'utilisateur SYSTEM reçoit un délai d'attente lorsqu'il tente d'accéder aux ressources via HTTP/HTTPS.

Il s'agit d'un outil utile pour vérifier les autorisations utilisateur SYSTEM. Complétez ces étapes avec l'utilitaire :

1. Utilisez l'utilitaire pour lancer « C:\Program Files\Internet Explorer\iexplore.exe ».
2. Accédez à <https://api.opendns.com/v2/OnPrem.Asset>.
3. Recherchez « 1005 Missing API Key » sans aucune invite de sécurité. Si des invites s'affichent, assurez-vous que UDP/TCP 443 est ouvert sur « api.opendns.com », « crl4.digicert.com », « ocsf.digicert.com » et que l'autorité de certification racine DigiCert est présente sur le système.

Si votre pare-feu empêche les comptes non authentifiés (comme le compte SYSTEM) d'accéder aux sites nécessaires, les domaines d'enregistrement Umbrella doivent être exemptés. Puisque le client d'itinérance appelle l'enregistrement à partir du compte utilisateur SYSTEM, celui-ci doit être ouvert pour les conditions préalables d'Umbrella à un accès non authentifié.

Symptômes

Le symptôme le plus courant est l'échec de l'enregistrement sur le tableau de bord ou de la synchronisation avec l'API Umbrella. Cela peut empêcher le client de s'enregistrer (et donc de passer en mode protégé) ou de mettre à jour le tableau de bord.

Si ces symptômes apparaissent, redémarrez le service client d'itinérance, puis envoyez un journal de rapport de diagnostic à l'assistance immédiatement après le redémarrage. Le client inclut une vérification de proxy qui ne s'exécute qu'au démarrage.

Identifier s'il existe un proxy

Vérifiez d'abord les journaux.

Si, dans les journaux, vous voyez une entrée de journal semblable à celle-ci :

```
<#root>
```

```
2014-03-14 09:39:43 [2252] [INFO ] Trying to get Device ID from API...
2014-03-14 09:39:43 [2252] [DEBUG] Sending GET to https://api.opendns.com/v3/organizations/XXXXX/roamin
2014-03-14 09:39:43 [2252] [ERROR]

Error creating DeviceID

: The remote name could not be resolved: '
api.opendns.com'
```

Ceci :

```
2014-12-08 09:25:27 [5700] [ERROR] POST failed: The operation has timed out
```

Ou ceci :

```
2015-03-05 12:41:11 [4084] [ERROR] Error creating DeviceID: Unable to connect to the remote server
```

Il est probable que les paramètres du proxy y sont pour quelque chose.

Scénario 1

Le journal indique qu'il ne peut pas résoudre « api.opendns.com ».

```
<#root>
```

```
The remote name could not be resolved: '
api.opendns.com'
```

Cela peut être dû à plusieurs problèmes :

- Échec de la résolution DNS sur votre connexion réseau : assurez-vous que les serveurs DNS d'Umbrella sont autorisés dans votre pare-feu si vous bloquez les serveurs DNS tiers.

- Vous avez un serveur proxy qui n'autorise pas la connexion : Si vous avez un serveur proxy, il est probablement préférable d'autoriser la liste "*.opendns.com" afin qu'elle n'interfère pas avec l'enregistrement ou la synchronisation de l'API.
- Le port 443/TCP est limité à des étendues IP spécifiques : Si vous utilisez des règles de pare-feu très strictes, vous devez ouvrir temporairement 443/TCP à toutes les connexions sortantes. Le client d'itinérance Umbrella doit récupérer le certificat SSL à partir de l'espace de domaine/IP GeoTrust.

Vous pouvez en savoir plus sur les besoins spécifiques d'Umbrella en matière de pare-feu dans l'article Prérequis pour le client d'itinérance d'Umbrella, qui fait appel à des proxies HTTP.

Scénarios 2 et 3

Le journal indique qu'il ne peut pas résoudre « proxyserver.exampldomain.com ».

```
<#root>
```

```
2014-03-14 09:39:43 [2252] [ERROR]
```

```
Error creating DeviceID
```

```
: The remote name could not be resolved: '
```

```
proxy1.exampldomain.com'
```

Le journal indique qu'il tente d'envoyer des informations à l'API Umbrella ("api.opendns.com"), mais l'erreur qui en résulte indique qu'il a tenté de se connecter à "proxy1.exampldomain.com"

La raison en est que le client d'itinérance Umbrella utilise les paramètres proxy de l'utilisateur « SYSTEM » de l'ordinateur à l'aide de l'appel .NET Framework de WebRequest.DefaultWebProxy. Ce paramètre est généralement défini via l'objet de stratégie de groupe (GPO) et, à moins que cette clé ne soit spécifiquement supprimée, peut rester dans le Registre à long terme. Si ce serveur proxy n'existe plus ou doit être mis à jour vers un autre hôte, vous pouvez modifier les paramètres via les méthodes ci-dessous.

Scénario 4

Le journal affiche ce message :

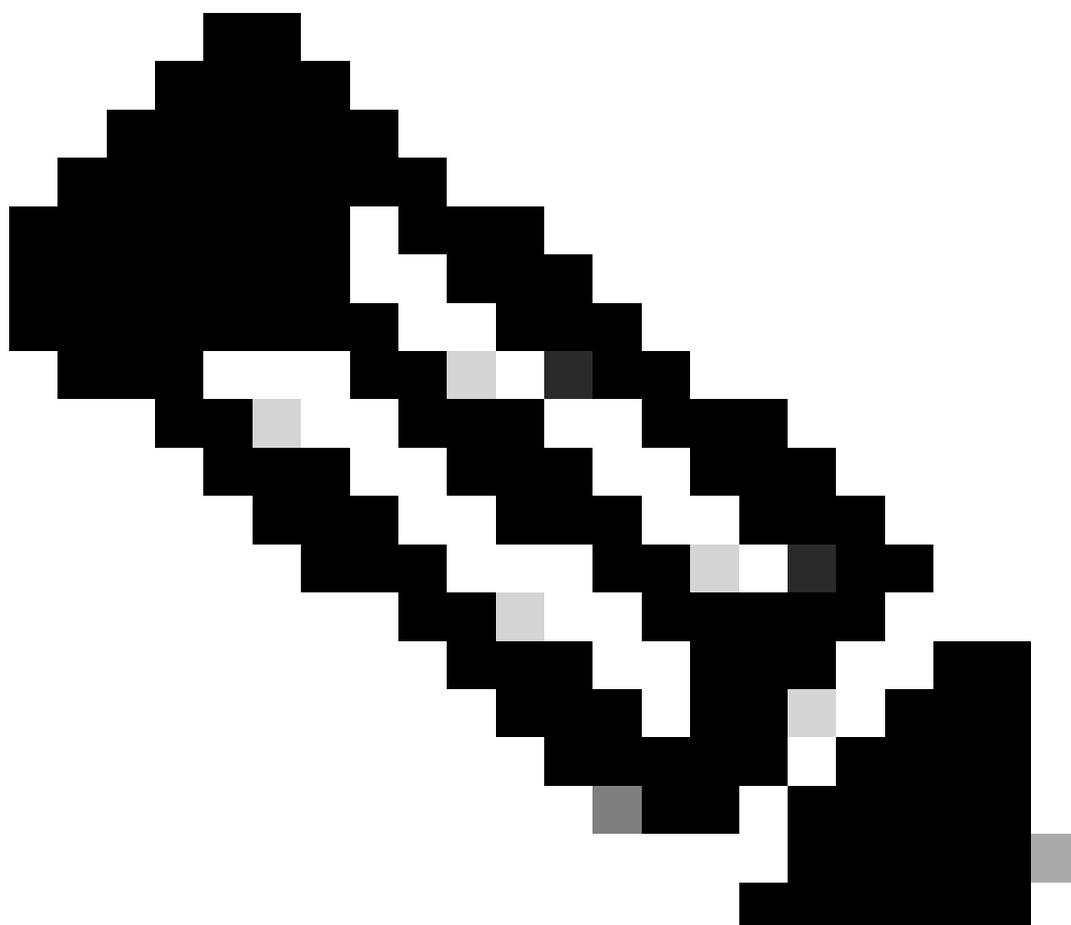
```
Error creating DeviceID: The underlying connection was closed: Could not establish trust relationship f
```

Cependant, aucun pare-feu n'est en place pour UDP/TCP cri4.digicert.com ou ocsip.digicert.com. Si l'ordinateur est relié à un autre réseau (par exemple, un point d'accès mobile), le problème persiste.

Exécutez cette commande pour déterminer si un proxy est encore défini ici :

```
netsh winhttp show proxy
```

Cet emplacement des paramètres proxy est utilisé par l'API de chiffrement Microsoft v2 dans le cadre de la validation du certificat .NET Framework. Si ce proxy est en place, il peut entraîner l'échec de cette validation. Pour plus d'informations, référez-vous à l'article de support Microsoft « Description du mécanisme de détection proxy de l'API de cryptographie lors du téléchargement d'une liste de révocation de certificats (CRL) à partir d'un point de distribution CRL ».



Remarque : Le scénario 4 peut également être provoqué par les paramètres de conformité PCI et .NET si TLS 1.0 est désactivé. Pour plus d'informations, consultez cet article de la base de connaissances Umbrella.

Ajouter ou supprimer des paramètres de proxy



Avertissement : Ce paramètre est normalement défini à l'aide d'un objet de stratégie de groupe ou d'un script. Il n'est pas courant que cette option soit définie sur un ordinateur individuel. Umbrella recommande d'utiliser cette méthode uniquement si vous souhaitez effectuer un test sur un ordinateur individuel ou si vous pensez que ce paramètre est unique pour cet ordinateur. Passez à la méthode suivante pour obtenir des informations sur l'utilisation de l'objet de stratégie de groupe pour un groupe entier.

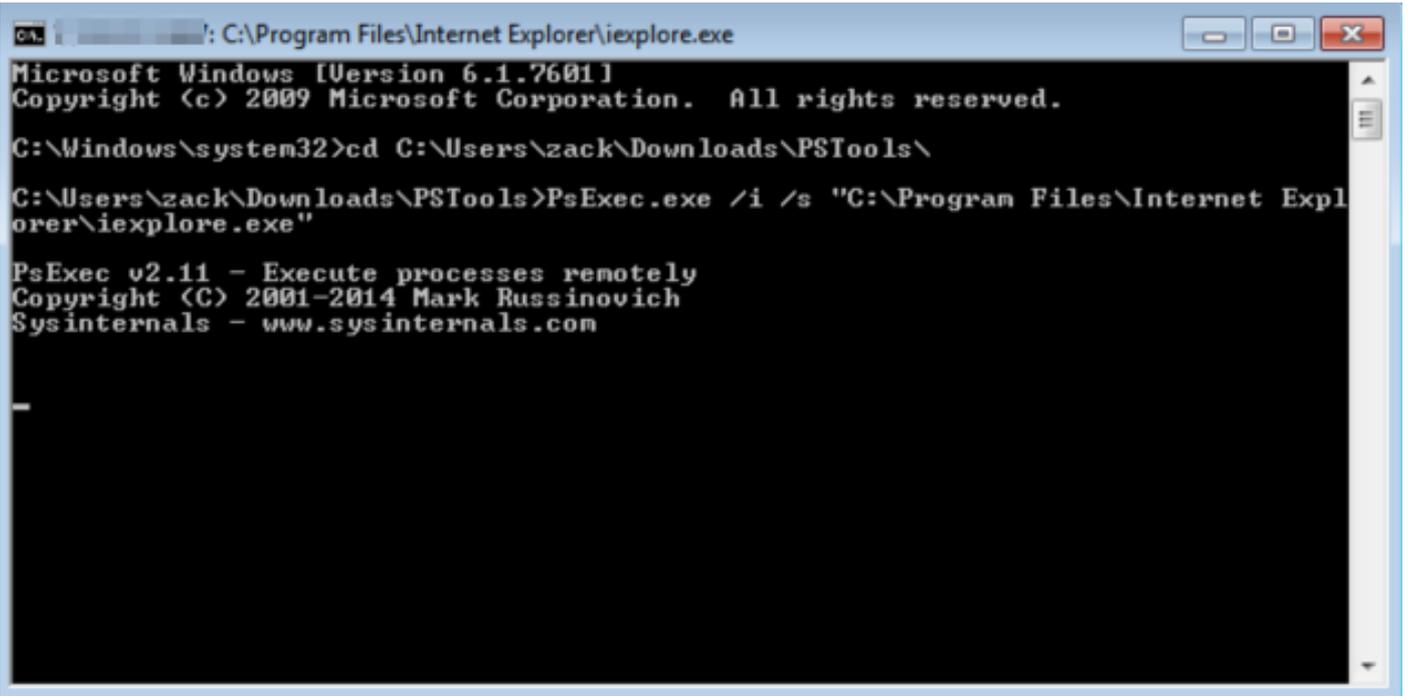
PsExec et Internet Explorer (IE 10 ou version ultérieure)

1. Téléchargez et décompressez PsExec.
2. Chargez une invite de commandes d'administration (clic droit > Exécuter en tant qu'administrateur).
3. Utilisez "cd" pour passer au répertoire PSTools extrait.

```
cd C:\Path\To\PSTools\
```

4. Exécutez cette commande pour ouvrir Internet Explorer en tant qu'utilisateur « SYSTEM » :

```
PsExec.exe /i /s "C:\Program Files\Internet Explorer\iexplore.exe"
```



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

C:\Windows\system32>cd C:\Users\zack\Downloads\PSTools\

C:\Users\zack\Downloads\PSTools>PsExec.exe /i /s "C:\Program Files\Internet Explorer\iexplore.exe"

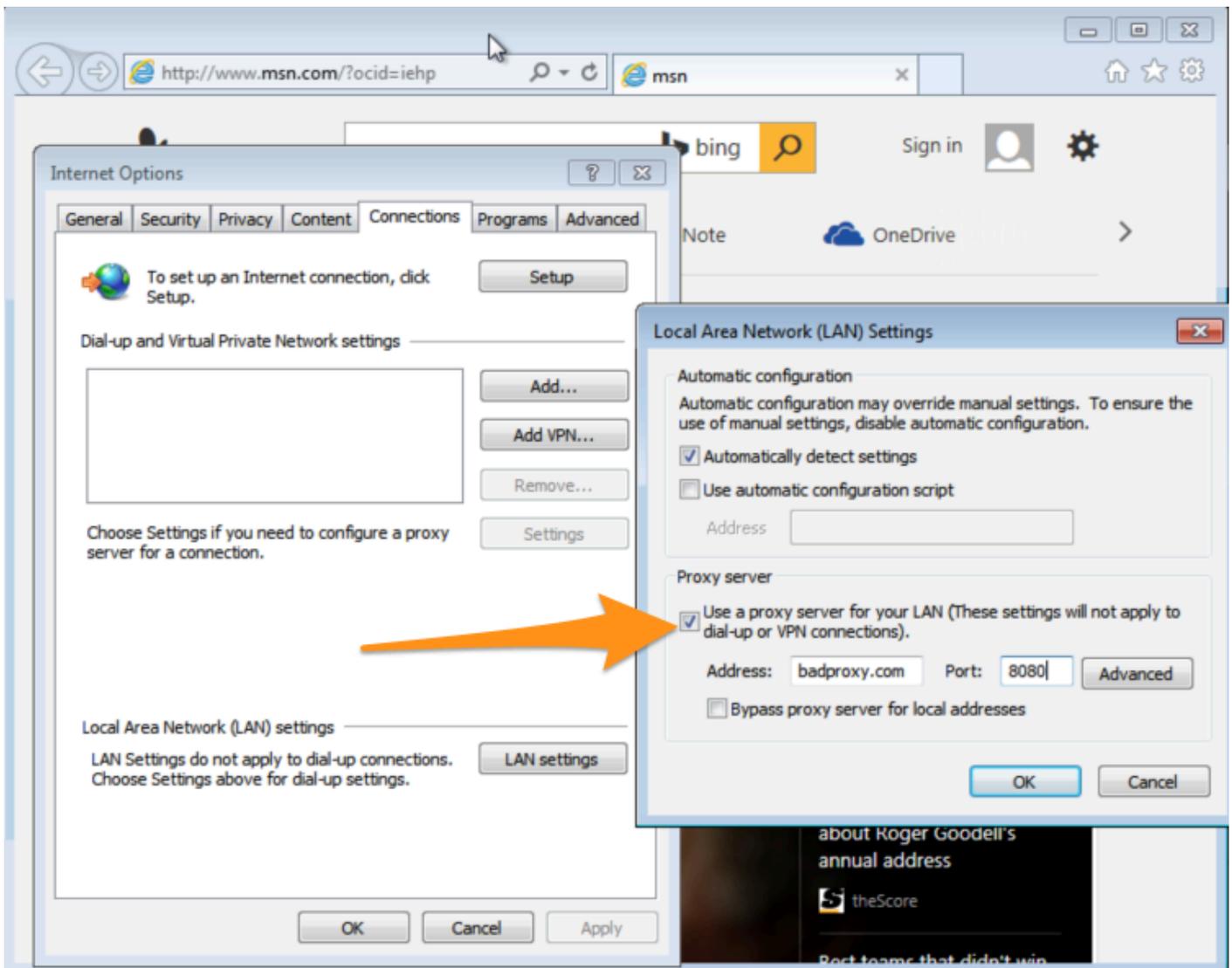
PsExec v2.11 - Execute processes remotely
Copyright (C) 2001-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

-
```

Exécutez PsExec.exe en tant qu'utilisateur SYSTEM

5. Ouvrez Options Internet à partir du menu Paramètres (cog) dans Internet Explorer.

6. Dans l'onglet Connexions, sélectionnez Paramètres du réseau local (LAN) et modifiez ou supprimez les paramètres du proxy selon les besoins.



Modifier ou supprimer les paramètres de proxy dans les paramètres LAN

7. Sélectionnez OK, puis Apply et fermez Internet Explorer.

Le client Umbrella Roaming s'enregistre en trois minutes environ.

Autre (Registre)

1. Vérifiez les paramètres du proxy à l'adresse HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet

Settings\Connections\DefaultConnectionSettings. Si un proxy est présent, il s'affichera plus tôt sous les paramètres de connexion de l'IE de l'utilisateur système.

2. Pour supprimer dans le Registre, procédez comme suit pour copier les paramètres sans proxy de l'utilisateur actuel :

1. Ouvrez la clé à l'adresse HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings et copiez la valeur.

2. Copiez-le dans la même clé sous HKEY_USERS\S-1-5-18 (l'utilisateur SYSTEM).

3. Redémarrez le client d'itinérance pour vérifier si l'inscription a réussi.

PsExec et MMC (IE9 ou antérieure)

1. Téléchargez et décompressez PsExec.

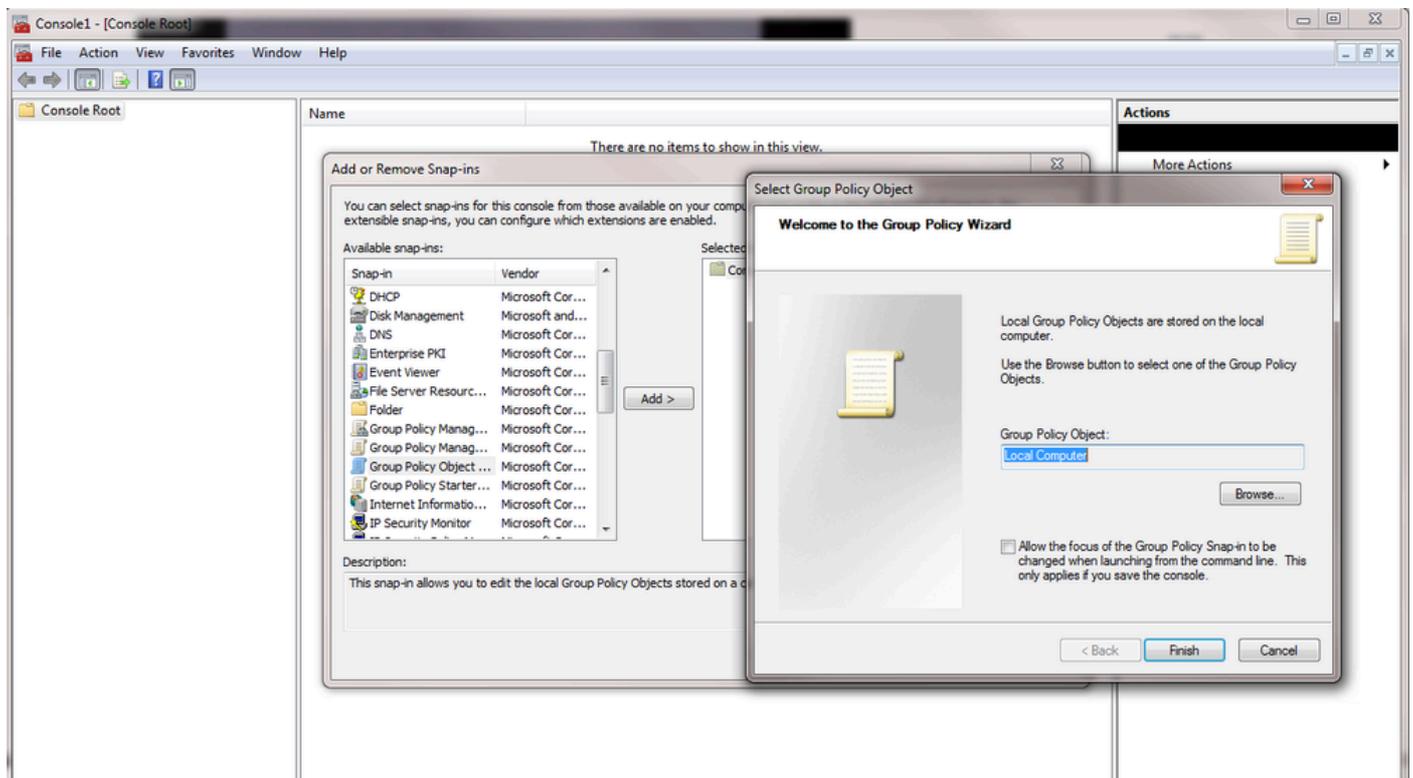
2. Chargez une invite de commandes d'administration (clic droit > Exécuter en tant qu'administrateur).

3. Utilisez "cd" pour passer au répertoire PSTools extrait.

4. Exécutez cette commande :

```
PsExec.exe /i /s mmc
```

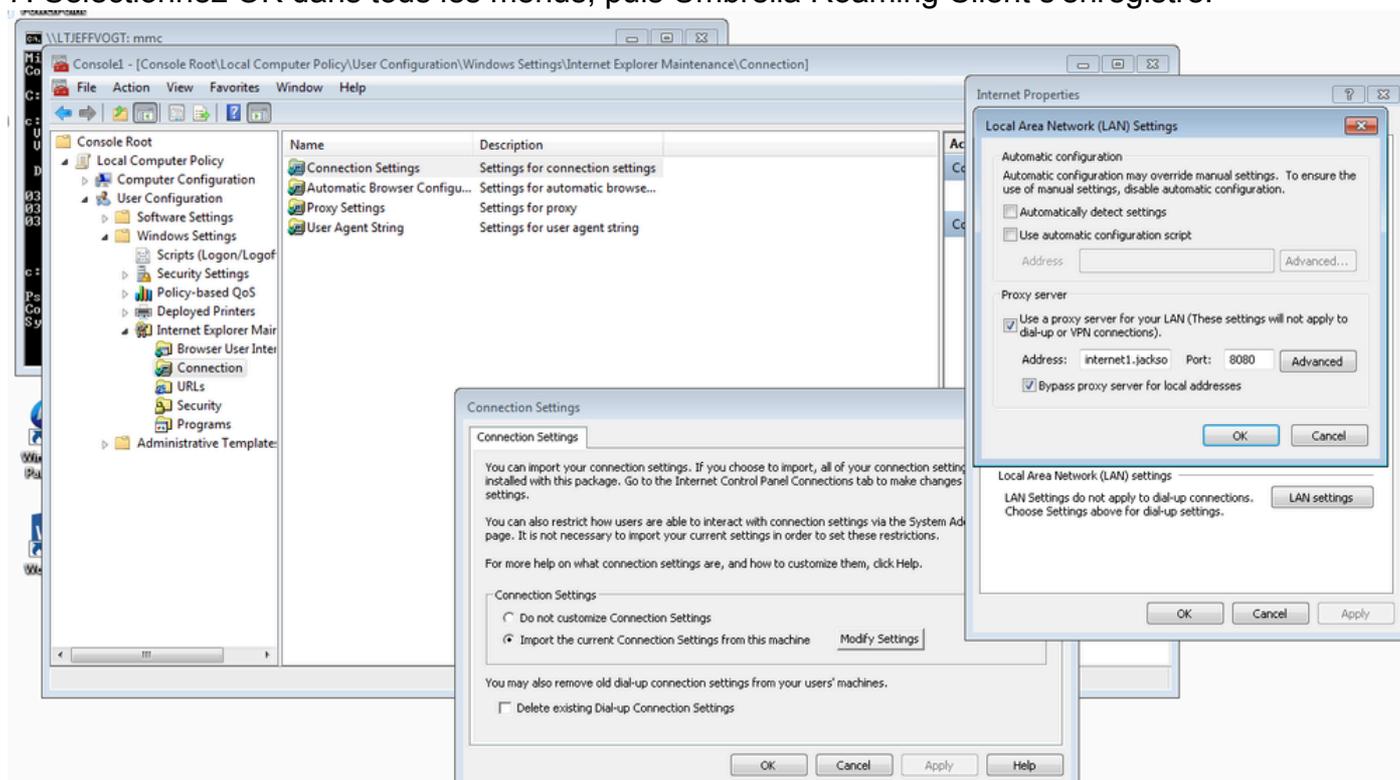
5. Une fois la console MMC chargée, chargez le composant logiciel enfichable Objet de stratégie de groupe.



Composant logiciel enfichable GPO

6. Accédez aux Paramètres de connexion locaux et modifiez ou supprimez les informations du serveur proxy si nécessaire.

7. Sélectionnez OK dans tous les menus, puis Umbrella Roaming Client s'enregistre.



Paramètres de connexion locale

Modifier le registre

En fonction de votre version de Windows Server, l'utilisation des étapes mentionnées ci-dessus à l'aide de la console MMC et la sélection du groupe approprié fonctionnent.

Si votre version de Windows Server ne dispose pas de ces paramètres, vous pouvez modifier ou supprimer ce paramètre via le Registre afin de purger ce paramètre au niveau global (plusieurs ordinateurs).

UTILISATEURS_CLÉS

.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet
Paramètres\Connexions\ParamètresConnexionParDéfaut

| | |
|--------------------------------------|--|
| ProxyEnable (Order: 1) | show |
| ProxyEnable (Order: 2) | show |
| ProxyEnable (Order: 3) | show |
| DefaultConnectionSettings (Order: 4) | hide |
| General | hide |
| Action | Delete |
| Properties | |
| Hive | HKEY_USERS |
| Key path | .DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections |
| Value name | DefaultConnectionSettings |
| Common | show |
| ProxyServer (Order: 5) | hide |
| General | show |

Supprimer les paramètres de connexion dans l'objet GPO

Cette capture d'écran est un exemple d'ancienne version d'IE pour les applications héritées. La suppression des valeurs de proxy de l'objet de stratégie de groupe ou des paramètres locaux permettrait au client d'itinérance Umbrella de se connecter et de s'enregistrer en tant qu'utilisateur système (sous réserve de ces paramètres de proxy IE).

| Name | Type | Data |
|-------------------|------------|--|
| (Default) | REG_SZ | (value not set) |
| EnableNegotiate | REG_DWORD | 0x00000001 (1) |
| IE5_UA_Backup_... | REG_SZ | 5.0 |
| ProxyEnable | REG_DWORD | 0x00000001 (1)  |
| ProxyServer | REG_SZ | pmfsrvisa:8080  |
| User Agent | REG_SZ | Mozilla/4.0 (compatible; MSIE 8.0; Win32) |
| ZonesSecurityU... | REG_BINARY | d2 80 a9 04 3f 04 ca 01 |

Supprimer les valeurs de proxy

Si l'une de ces méthodologies ne fonctionne pas, ouvrez un ticket d'assistance Umbrella via le tableau de bord et reportez-vous à cet article.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.