

Windows에서 Umbrella Roaming Client에 대한 HTTP 프록시 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[개요](#)

[증상](#)

[프록시가 있는지 확인](#)

[시나리오 1](#)

[시나리오 2 및 3](#)

[시나리오 4](#)

[프록시 설정 추가 또는 제거](#)

[PsExec 및 Internet Explorer\(IE 10 이상\)](#)

[Alternative\(레지스트리\)](#)

[PsExec 및 MMC\(IE9 이전\)](#)

[레지스트리 편집](#)

소개

이 문서에서는 Windows의 Umbrella Roaming Client에 대한 HTTP 프록시 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Windows의 Umbrella Roaming Client를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

Umbrella 배포의 일부 또는 모든 컴퓨터에서 Umbrella 로밍 클라이언트가 올바르게 등록되지 않습

니다. Umbrella Roaming Client 트레이 아이콘이 시스템의 빨간색 상태이거나 Umbrella Roaming Client가 예상대로 대시보드에 표시되지 않기 때문에 이 메시지가 표시됩니다. 또한 현재 또는 한 시점에 네트워크에서 HTTP 프록시를 사용하고 있습니다. 클라이언트가 로밍하는 경우 HTTP 프록시 뒤에서 온라인 상태가 됩니다.

현재 HTTP 프록시를 실행하고 있습니다. Umbrella Roaming Client는 시스템 서비스로 실행되므로 "SYSTEM" 사용자를 사용하며, 사용자가 GPO(Group Policy Object) 또는 다른 RMM(Remote Monitoring and Management) 도구를 통해 컨피그레이션 설정을 푸시하여 조직 내 사용자에게 사용자 특정 HTTP 프록시 설정을 제공했습니다. 또한 게이트웨이 방화벽에는 프록시를 거치지 않는 한 HTTP/HTTPS 트래픽을 허용하지 않는 기본 거부 규칙이 있습니다.

과거에 HTTP 프록시를 실행했습니다. "SYSTEM" 사용자는 이전에 어떤 시점에 HTTP 프록시 설정이 설정되어 있었으나 이제 프록시가 더 이상 존재하지 않습니다. 프록시가 더 이상 존재하지 않으므로 SYSTEM 사용자는 HTTP/HTTPS를 통해 리소스에 액세스하려고 할 때 시간 제한을 받습니다.

시스템 사용자 권한을 확인하는 데 유용한 도구입니다. 유틸리티를 사용하여 다음 단계를 완료합니다.

1. 이 유틸리티를 사용하여 "C:\Program Files\Internet Explorer\iexplore.exe"를 실행합니다.
2. <https://api.opendns.com/v2/OnPrem.Asset>으로 [이동합니다](#).
3. 보안 프롬프트 없이 "1005 Missing API Key"를 찾습니다. 프롬프트가 있는 경우 UDP/TCP 443이 "api.opendns.com", "crl4.digicert.com", "ocsp.digicert.com"에 열려 있고 DigiCert Root CA가 시스템에 있는지 확인합니다.

방화벽에서 인증되지 않은 계정(예: SYSTEM 계정)의 필수 사이트 액세스를 제한하는 경우 Umbrella 등록 도메인은 제외되어야 합니다. 로밍 클라이언트가 SYSTEM 사용자 계정에서 등록을 호출하므로 인증되지 않은 액세스를 위해서는 Umbrella의 사전 요구 사항에 대해 이 설정을 열어야 합니다.

증상

가장 일반적인 증상은 대시보드에 등록하지 못하거나 Umbrella API와 동기화하지 못하는 것입니다. 이로 인해 클라이언트가 등록하지 않거나(따라서 보호 모드로 들어가지 않음) 대시보드 업데이트를 중단할 수 있습니다.

이러한 증상이 나타나면 로밍 클라이언트 서비스를 다시 시작한 다음 진단 보고서 로그를 전송하여 다시 시작한 직후에 지원을 요청하십시오. 클라이언트는 시작할 때만 실행되는 프록시 검사를 포함합니다.

프록시가 있는지 확인

먼저 로그를 확인하십시오.

로그에 다음과 유사한 로그 항목이 표시되는 경우

<#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/roaming
2014-03-14 09:39:43 [2252] [ERROR]
Error creating DeviceID
: The remote name could not be resolved: '
api.opendns.com'
```

다음 항목을 참조하십시오.

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

또는

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

프록시 설정이 이와 관련이 있을 수 있습니다.

시나리오 1

로그에 "api.opendns.com"을 확인할 수 없다는 메시지가 표시됩니다.

```
<#root>
```

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

다음과 같은 몇 가지 문제로 인해 발생할 수 있습니다.

- 네트워크 연결에서 DNS 확인이 실패했습니다. 타사 DNS 서버를 차단할 경우 Umbrella의 DNS 서버가 방화벽에서 허용되는지 확인하십시오.
- 연결을 허용하지 않는 프록시 서버가 있습니다. 프록시 서버가 있는 경우 "*.opendns.com" 목록을 허용하는 것이 가장 좋습니다. 그러면 등록이나 API 동기화에 방해가 되지 않습니다.
- 포트 443/TCP가 특정 IP 범위로 제한되어 있습니다. 매우 엄격한 방화벽 규칙을 사용하는 경우 모든 아웃바운드 연결에 대해 일시적으로 443/TCP를 열어야 합니다. Umbrella Roaming Client는 GeoTrust IP/도메인 공간에서 SSL 인증서를 가져와야 합니다.

HTTP 프록시를 호출하는 Umbrella의 로밍 클라이언트 사전 요구 사항 문서에서 Umbrella의 특정 방화벽 요구 사항에 대해 읽을 수 있습니다.

시나리오 2 및 3

로그에 "proxyserver.exampdomain.com"을 확인할 수 없다는 메시지가 표시됩니다.

```
<#root>
```

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

```
Error creating DeviceID
```

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

```
proxy1.exampdomain.com'
```

로그는 Umbrella API("api.opendns.com")로 정보를 보내려고 시도하지만, 그 결과 발생한 오류로 인해 "proxy1.exampdomain.com"에 연결하려고 시도했음을 나타냅니다.

이 문제가 발생하는 이유는 Umbrella Roaming Client가 WebRequest.DefaultWebProxy의 .NET Framework 호출을 사용하여 컴퓨터의 "SYSTEM" 사용자 프록시 설정을 사용하기 때문입니다. 이 문제는 일반적으로 GPO(그룹 정책 개체)를 통해 설정되며, 이 키를 특별히 삭제하지 않는 한 레지스트리에 오래 머물 수 있습니다. 이 프록시 서버가 더 이상 존재하지 않거나 다른 호스트로 업데이트해야 하는 경우 아래 방법을 통해 설정을 수정할 수 있습니다.

시나리오 4

로그에는 다음 메시지가 표시됩니다.

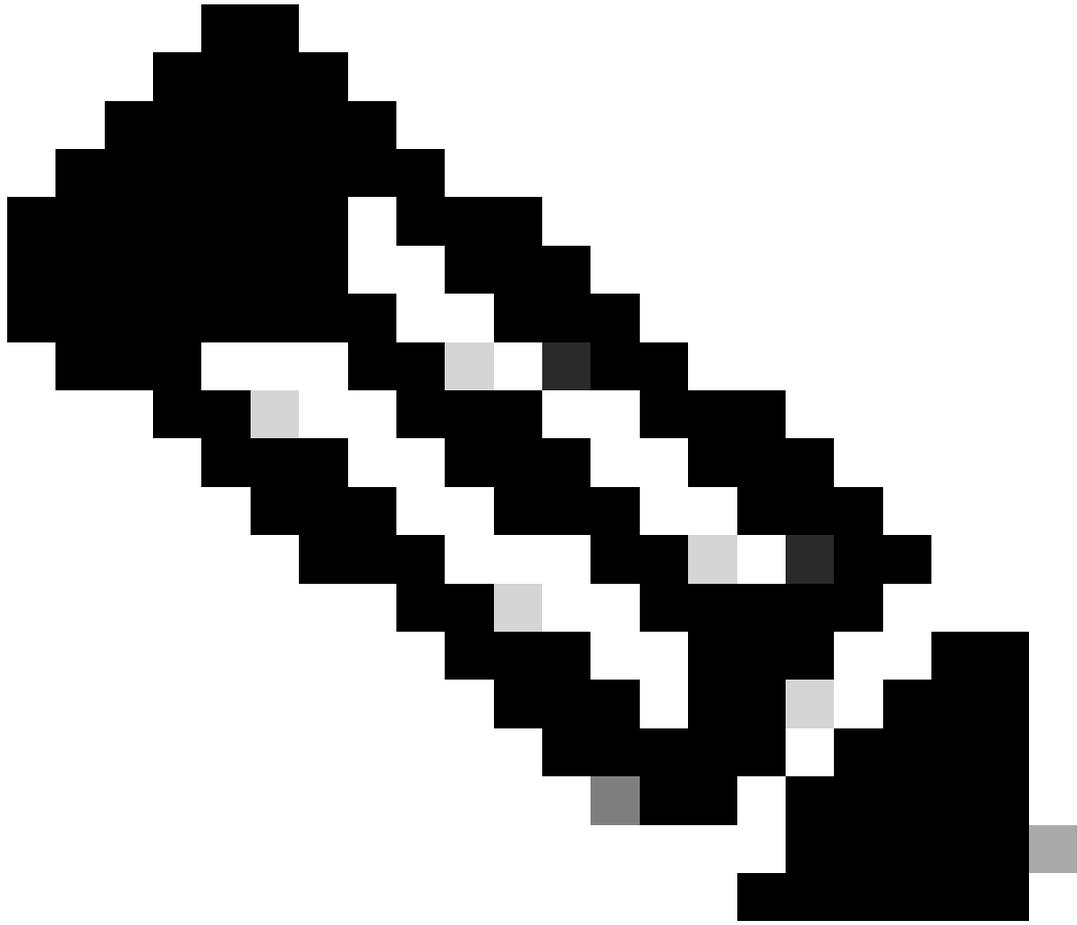
```
Error creating DeviceID: The underlying connection was closed: Could not establish trust relationship f
```

그러나 UDP/TCP crl4.digicert.com 또는 ocsp.digicert.com에는 방화벽 블록이 없습니다. 컴퓨터를 다른 네트워크(예: 모바일 핫스팟)로 가져가면 문제가 계속 발생합니다.

이 명령을 실행하여 여기에 설정된 프록시가 있는지 확인합니다.

```
netsh winhttp show proxy
```

이 프록시 설정 위치는 Microsoft Cryptography API v2에서 .NET Framework 인증서 유효성 검사的一部分로 사용됩니다. 이 프록시가 있으면 이 검증이 실패할 수 있습니다. 자세한 내용은 Microsoft 지원 문서 "CRL 배포 지점에서 CRL(Certificate Revocation List)을 다운로드할 때 암호화 API 프록시 탐지 메커니즘에 대한 설명"을 참조하십시오.



참고: 또한 TLS 1.0이 비활성화된 경우 PCI 규정준수 설정 및 .NET으로 인해 시나리오 4가 발생할 수 있습니다. 자세한 내용은 이 Umbrella 기술 문서를 참조하십시오.

프록시 설정 추가 또는 제거



경고: 이 설정은 일반적으로 GPO 또는 일종의 스크립트를 사용하여 설정됩니다. 개별 컴퓨터에서 설정되는 것은 일반적이지 않습니다. Umbrella에서는 개별 컴퓨터에서 테스트하려는 경우 또는 이 설정이 이 컴퓨터에서만 고유하다고 생각하는 경우에만 이 방법을 사용할 것을 권장합니다. 전체 그룹에 대한 GPO 사용에 대한 자세한 내용은 다음 방법을 건너뛰니다.

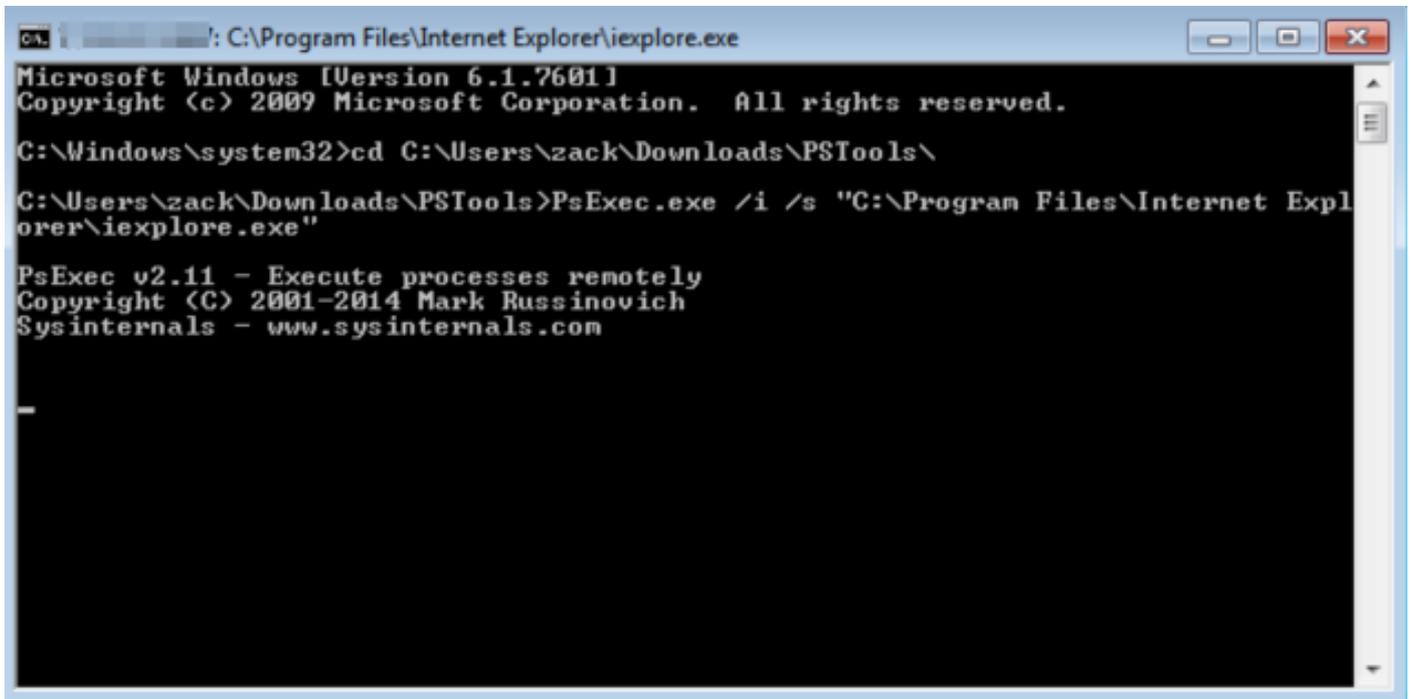
PsExec 및 Internet Explorer(IE 10 이상)

1. PsExec을 다운로드하고 압축을 풉니다.
2. 관리 명령 프롬프트를 로드합니다(마우스 오른쪽 버튼 > 관리자로 실행).
3. "cd"를 사용하여 추출된 PSTools 디렉토리로 변경합니다.

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

4. 다음 명령을 실행하여 Internet Explorer를 "SYSTEM" 사용자로 엽니다.

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



```
ca. [redacted]; 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"

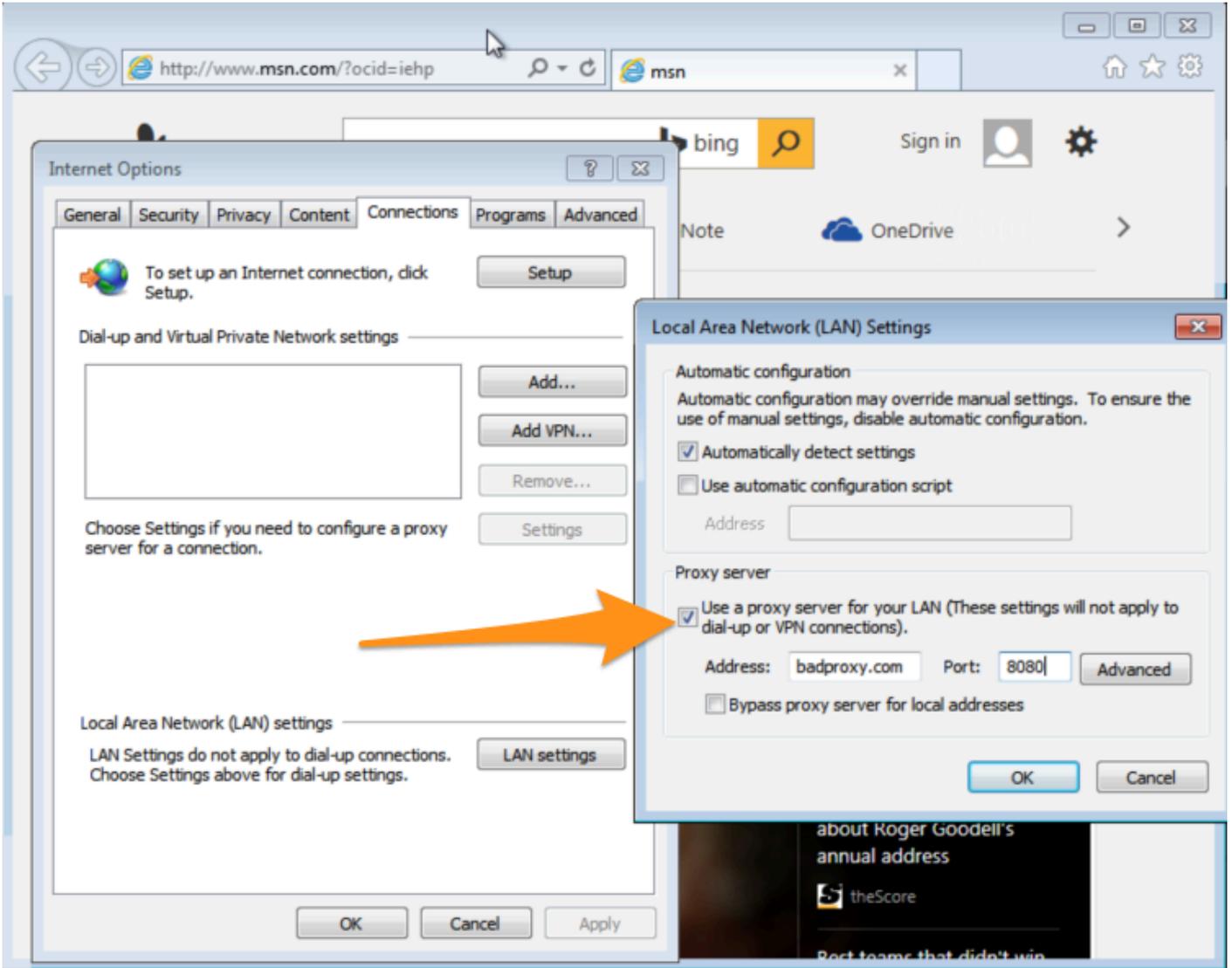
PsExec v2.11 - Execute processes remotely
Copyright (C) 2001-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

-
```

SYSTEM 사용자로 PsExe.exe 실행

5. Internet Explorer의 cog(설정 메뉴)에서 인터넷 옵션을 엽니다.

6. 연결 탭에서 LAN(Local Area Network) 설정을 선택하고 필요에 따라 프록시 설정을 변경하거나 삭제합니다.



LAN 설정에서 프록시 설정 변경 또는 삭제

7. 확인, 적용을 차례로 선택하고 Internet Explorer를 닫습니다.

Umbrella Roaming Client는 약 3분 내에 등록됩니다.

Alternative(레지스트리)

1. HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings에서 프록시 설정에 대한 키를 확인합니다. 프록시 설정이 있는 경우 시스템 사용자 IE 연결 설정 아래에 프록시가 먼저 표시됩니다.

2. 레지스트리에서 제거하려면 다음 단계를 완료하여 현재 사용자로부터 프록시 없는 설정을 복사합니다.

1. HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings에서 키를 열고 값을 복사합니다.

2. HKEY_USERS\S-1-5-18(시스템 사용자)의 동일한 키에 복사합니다.

3. 로밍 클라이언트를 다시 시작하여 등록이 성공했는지 확인합니다.

PsExec 및 MMC(IE9 이전)

1. PsExec을 다운로드하고 압축을 풉니다.

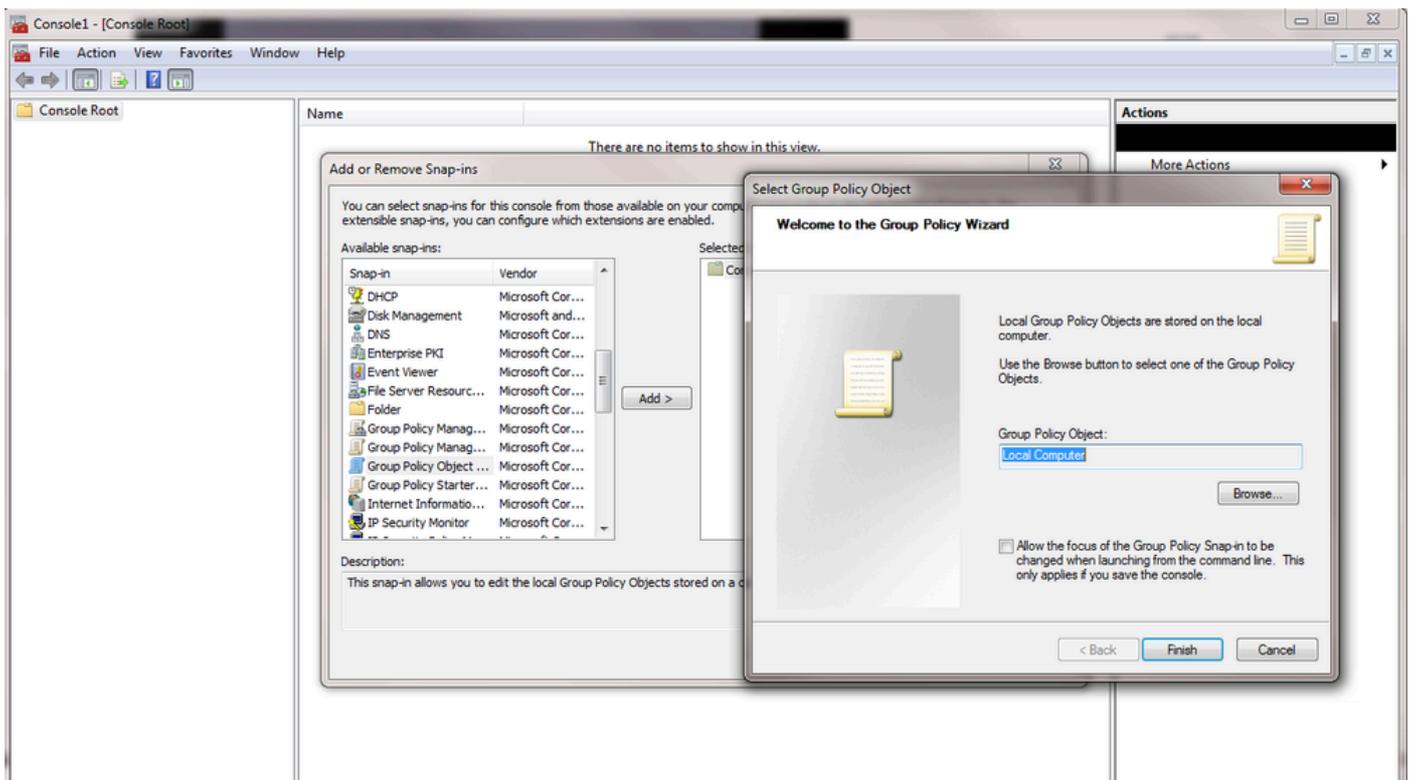
2. 관리 명령 프롬프트를 로드합니다(마우스 오른쪽 버튼 > 관리자로 실행).

3. "cd"를 사용하여 추출된 PSTools 디렉토리로 변경합니다.

4. 다음 명령을 실행합니다.

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

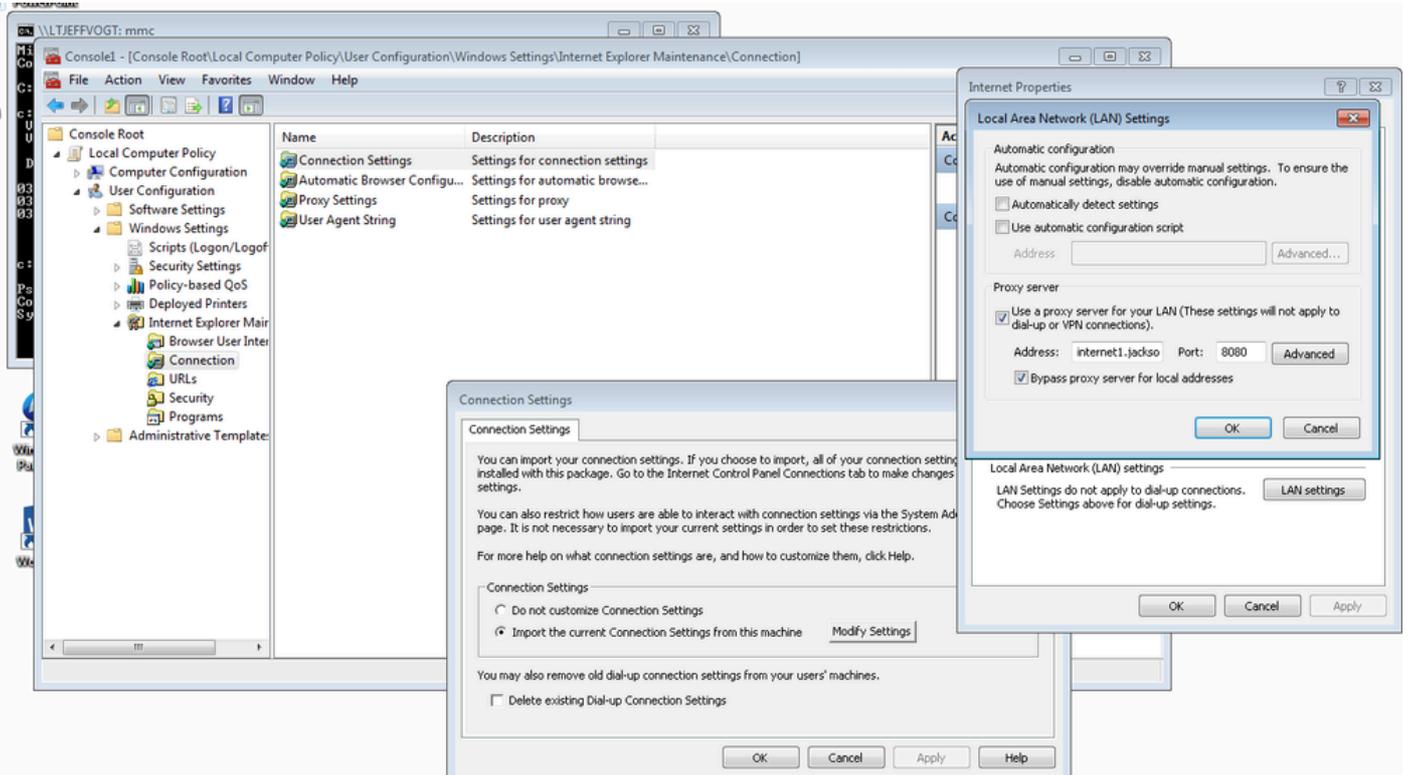
5. MMC가 로드되면 그룹 정책 개체 스냅인을 로드합니다.



GPO 스냅인

6. 로컬 연결 설정으로 이동하여 필요에 따라 프록시 서버 정보를 변경하거나 삭제합니다.

7. 모든 메뉴에서 확인을 선택하면 Umbrella Roaming Client가 등록됩니다.



로컬 연결 설정

레지스트리 편집

사용 중인 Windows Server의 버전에 따라 MMC 콘솔을 사용하고 올바른 그룹을 선택하는 앞에서 설명한 단계를 사용할 수 있습니다.

Windows Server 버전에 이러한 설정이 없는 경우 레지스트리를 통해 이 설정을 수정하거나 삭제하여 전역 수준(여러 컴퓨터)에서 이 설정을 제거할 수 있습니다.

HKEY_사용자

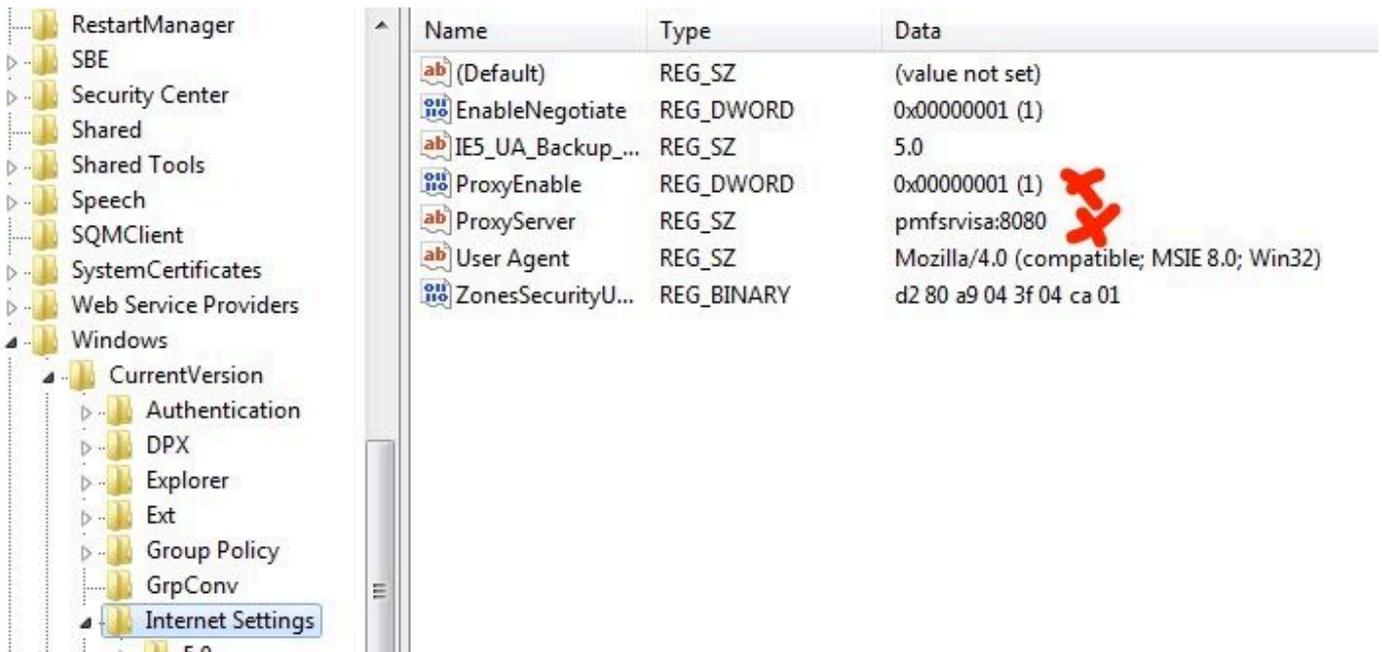
.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings

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

GPO에서 연결 설정 삭제

이 스크린샷은 레거시 애플리케이션용 IE의 이전 버전에 대한 예입니다. GPO 또는 로컬 설정에서 프록시 값을 제거하면 Umbrella 로밍 클라이언트가 연결하여 시스템 사용자로 등록할 수 있습니다

(이러한 IE 프록시 설정에 따라 다름).



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

프록시 값 제거

이러한 방법론 중 하나가 작동하지 않을 경우 대시보드를 통해 Umbrella 지원 티켓을 열고 이 문서를 참조하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.