SDM을 사용하여 Cisco IOS에서 CSD 구성

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[네트워크 다이어그램](#)
[관련 제품](#)
[표기 규칙](#)
[구성](#)
[1단계:SDM을 사용하여 CSD 컨피그레이션을 위한 라우터를 준비합니다.](#)
[1단계:1단계:WebVPN 게이트웨이, WebVPN 컨텍스트 및 그룹 정책을 구성합니다.](#)
[1단계:2단계:WebVPN 컨텍스트에서 CSD를 활성화합니다.](#)
[2단계:웹 브라우저를 사용하여 CSD를 구성합니다.](#)
[2단계:1단계:Windows 위치를 정의합니다.](#)
[2단계:2단계:위치 기준 식별](#)
[2단계:3단계:Windows 위치 모듈 및 기능을 구성합니다.](#)
[2단계:4단계:Windows CE, Macintosh 및 Linux 기능을 구성합니다.](#)
[다음을 확인합니다.](#)
[CSD 작업 테스트](#)
[명령](#)
[문제 해결](#)
[명령](#)
[관련 정보](#)

소개

SSL(Secure Sockets Layer) VPN(Cisco WebVPN) 세션은 안전하지만 세션이 완료된 후에도 클라이언트는 쿠키, 브라우저 파일 및 이메일 첨부 파일을 계속 보유할 수 있습니다.Cisco CSD(Secure Desktop)는 세션 데이터를 암호화된 형식으로 기록하여 클라이언트 디스크의 특수 *볼팅* 영역에 SSL VPN 세션의 고유한 보안을 확장합니다.또한 이 데이터는 SSL VPN 세션이 끝날 때 디스크에서 제거됩니다.이 문서에서는 Cisco IOS® 라우터의 CSD에 대한 샘플 컨피그레이션을 제공합니다.

CSD는 다음 Cisco 디바이스 플랫폼에서 지원됩니다.

- Cisco IOS Router 버전 12.4(6)T 이상
- Cisco 870,1811,1841, 2801, 2811, 2821, 2851, 3725, 3745, 3825, 3845, 7200 및 7301 라우터
- Cisco VPN 3000 Series Concentrator 버전 4.7 이상
- Cisco ASA 5500 Series Security Appliances 버전 7.1 이상
- Cisco Catalyst 및 Cisco 7600 Series 버전 1.2 이상용 Cisco WebVPN Services Module

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

Cisco IOS 라우터의 요구 사항

- Advanced Image 12.4(6T) 이상이 포함된 Cisco IOS 라우터
- Cisco SDM(Router Secure Device Manager) 2.3 이상
- 관리 스테이션의 IOS용 CSD 패키지 사본
- CA(Certificate Authority)를 사용하는 라우터 자체 서명 디지털 인증서 또는 인증**참고:** 디지털 인증서를 사용할 때마다 라우터의 호스트 이름, 도메인 이름 및 날짜/시간/시간대를 올바르게 설정해야 합니다.
- 라우터에서 비밀번호 활성화
- 라우터에서 DNS가 활성화되었습니다.여러 WebVPN 서비스가 제대로 작동하려면 DNS가 필요합니다.

클라이언트 컴퓨터의 요구 사항

- 원격 클라이언트에는 로컬 관리 권한이 있어야 합니다.필수 사항은 아니지만, 매우 권장됩니다.
- 원격 클라이언트에는 JRE(Java Runtime Environment) 버전 1.4 이상이 있어야 합니다.
- 원격 클라이언트 브라우저:Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2 또는 Firefox 1.0
- 원격 클라이언트에서 쿠키 사용 및 팝업 허용

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

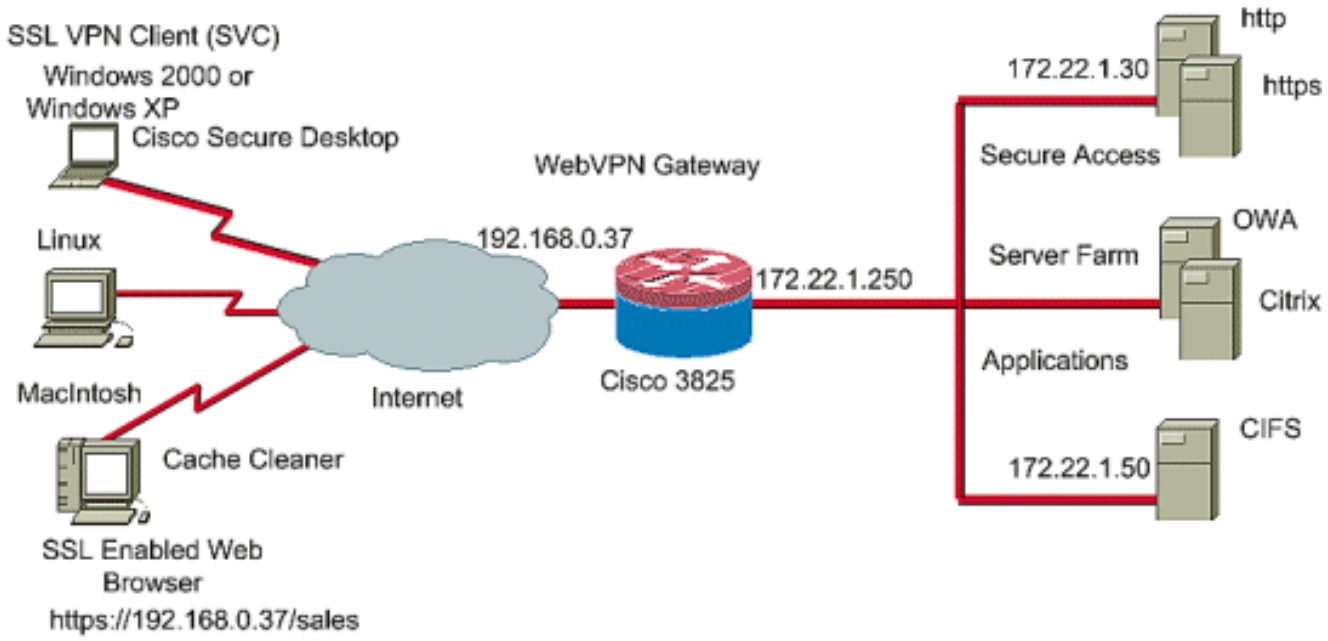
- 버전 12.9(T)가 포함된 Cisco IOS 라우터 3825
- SDM 버전 2.3.1

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

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.

이 예에서는 Cisco 3825 Series 라우터를 사용하여 회사의 인트라넷에 안전하게 액세스할 수 있도록 합니다.Cisco 3825 Series 라우터는 구성 가능한 CSD 기능 및 특성으로 SSL VPN 연결의 보안을 강화합니다.클라이언트는 다음 3가지 SSL VPN 방법 중 하나를 통해 CSD 지원 라우터에 연결할 수 있습니다.클라이언트리스 SSL VPN(WebVPN), 씬 클라이언트 SSL VPN(포트 전달) 또는 SSL VPN 클라이언트(전체 터널링 SVC).



관련 제품

이 컨피그레이션은 다음 하드웨어 및 소프트웨어 버전과 함께 사용할 수도 있습니다.

- Cisco 라우터 플랫폼 870,1811,1841,2801,2811,2821 2851,3725,3745.3825,3845, 7200 및 7301
- Cisco IOS Advanced Security Image 버전 12.4(6)T 이상

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

구성

WebVPN 게이트웨이를 사용하면 사용자가 SSL VPN 기술 중 하나를 통해 라우터에 연결할 수 있습니다.둘 이상의 WebVPN 컨텍스트를 WebVPN 게이트웨이에 연결할 수 있지만 IP 주소당 하나의 WebVPN 게이트웨이만 디바이스에서 허용됩니다.각 컨텍스트는 고유한 이름으로 식별됩니다.그룹 정책은 특정 WebVPN 컨텍스트에서 사용 가능한 구성된 리소스를 식별합니다.

IOS 라우터에서 CSD 컨피그레이션은 두 단계로 이루어집니다.

1단계:SDM을 사용하여 CSD 컨피그레이션을 위한 라우터 준비

1. WebVPN 게이트웨이, WebVPN 컨텍스트 및 그룹 정책을 구성합니다.**참고:** 이 단계는 선택 사항이며 이 문서에서 자세히 다루지 않습니다.SSL VPN 기술 중 하나에 대해 라우터를 이미 구성한 경우 이 단계를 생략합니다.
2. WebVPN 컨텍스트에서 CSD를 활성화합니다.

2단계:웹 브라우저를 사용하여 CSD를 구성합니다.

1. *Windows 위치를* 정의합니다.
2. 위치 기준을 식별합니다.
3. Windows 위치 모듈 및 기능을 구성합니다.

4. Windows CE, Macintosh 및 Linux 기능을 구성합니다.

1단계:SDM을 사용하여 CSD 컨피그레이션을 위한 라우터를 준비합니다.

CSD는 SDM 또는 CLI(Command Line Interface)에서 구성할 수 있습니다. 이 구성에서는 SDM 및 웹 브라우저를 사용합니다.

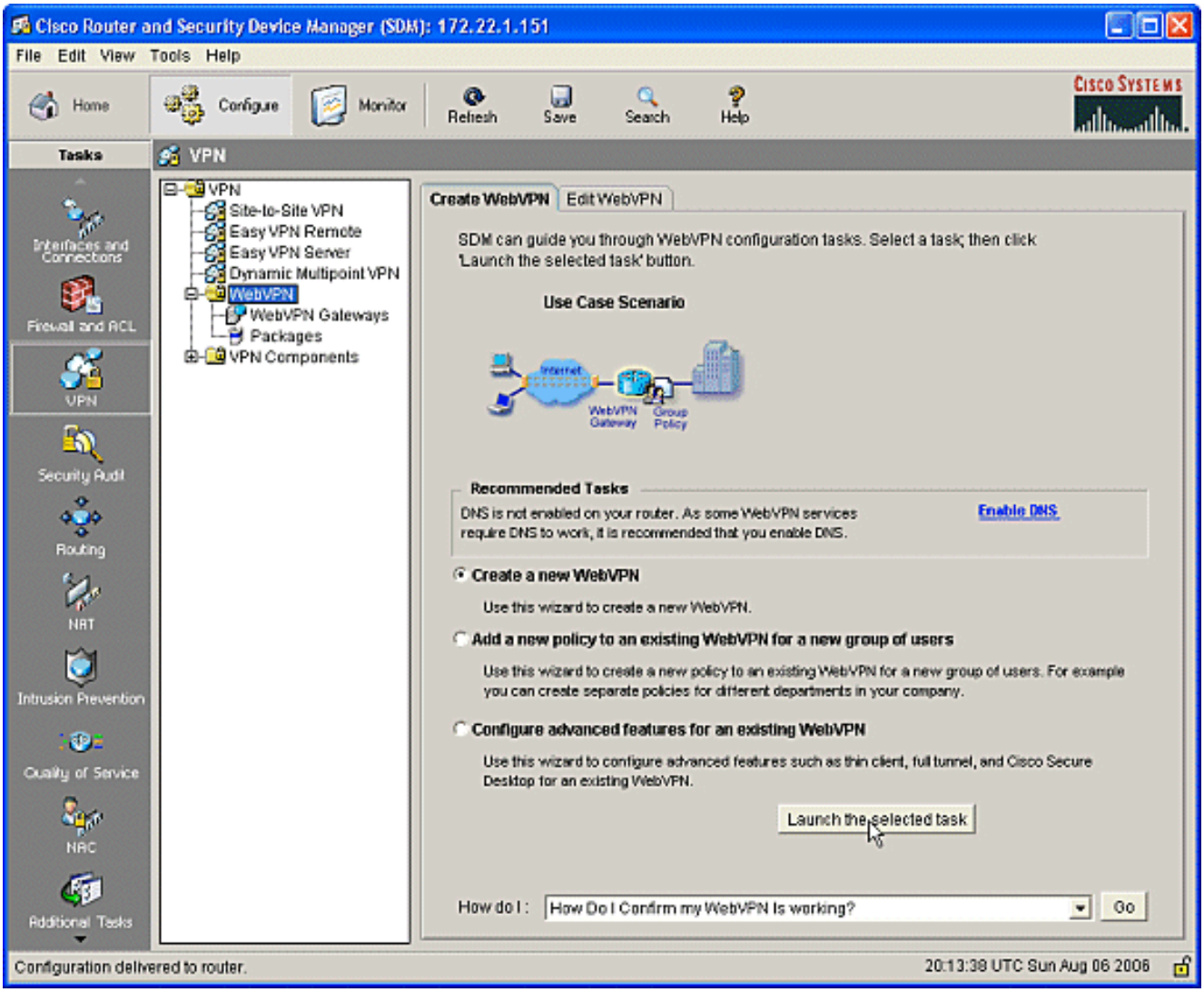
이 단계는 IOS 라우터에서 CSD 컨피그레이션을 완료하는 데 사용됩니다.

1단계:1단계:WebVPN 게이트웨이, WebVPN 컨텍스트 및 그룹 정책을 구성합니다.

WebVPN 마법사를 사용하여 이 작업을 수행할 수 있습니다.

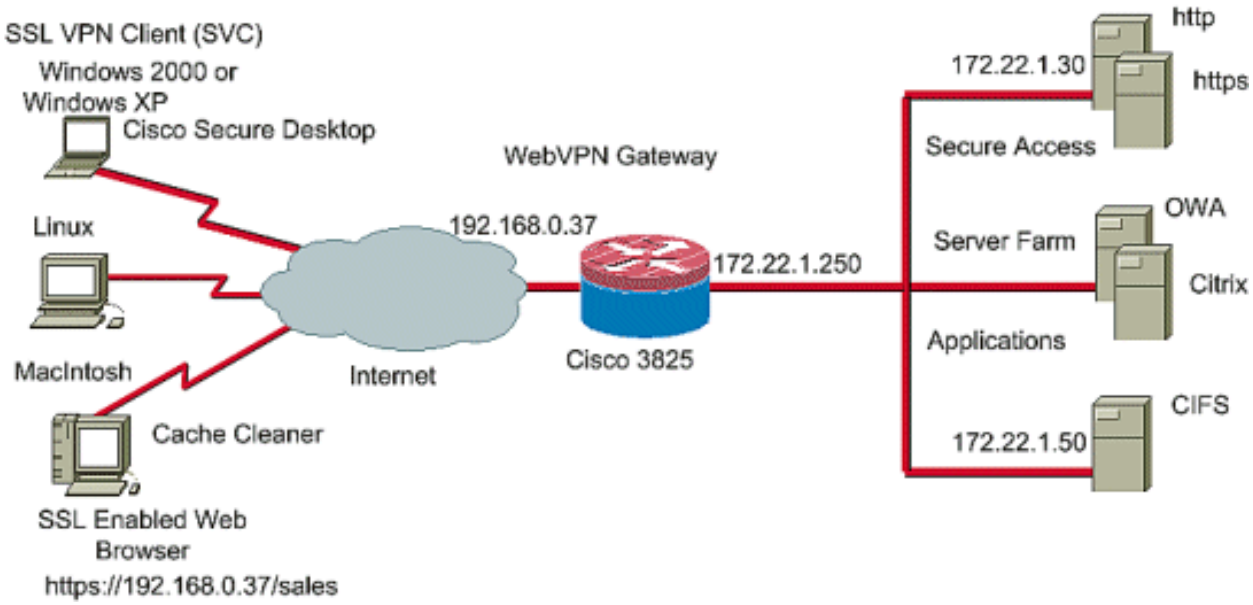
1. SDM을 열고 Configure(구성) **> VPN > WebVPN으로 이동합니다**.Create **WebVPN(WebVPN 생성)** 탭을 클릭하고 **Create a new WebVPN(새 WebVPN 생성)** 라디오 버튼을 선택합니다.**선택한 작업 시작을** 클릭합니다

.



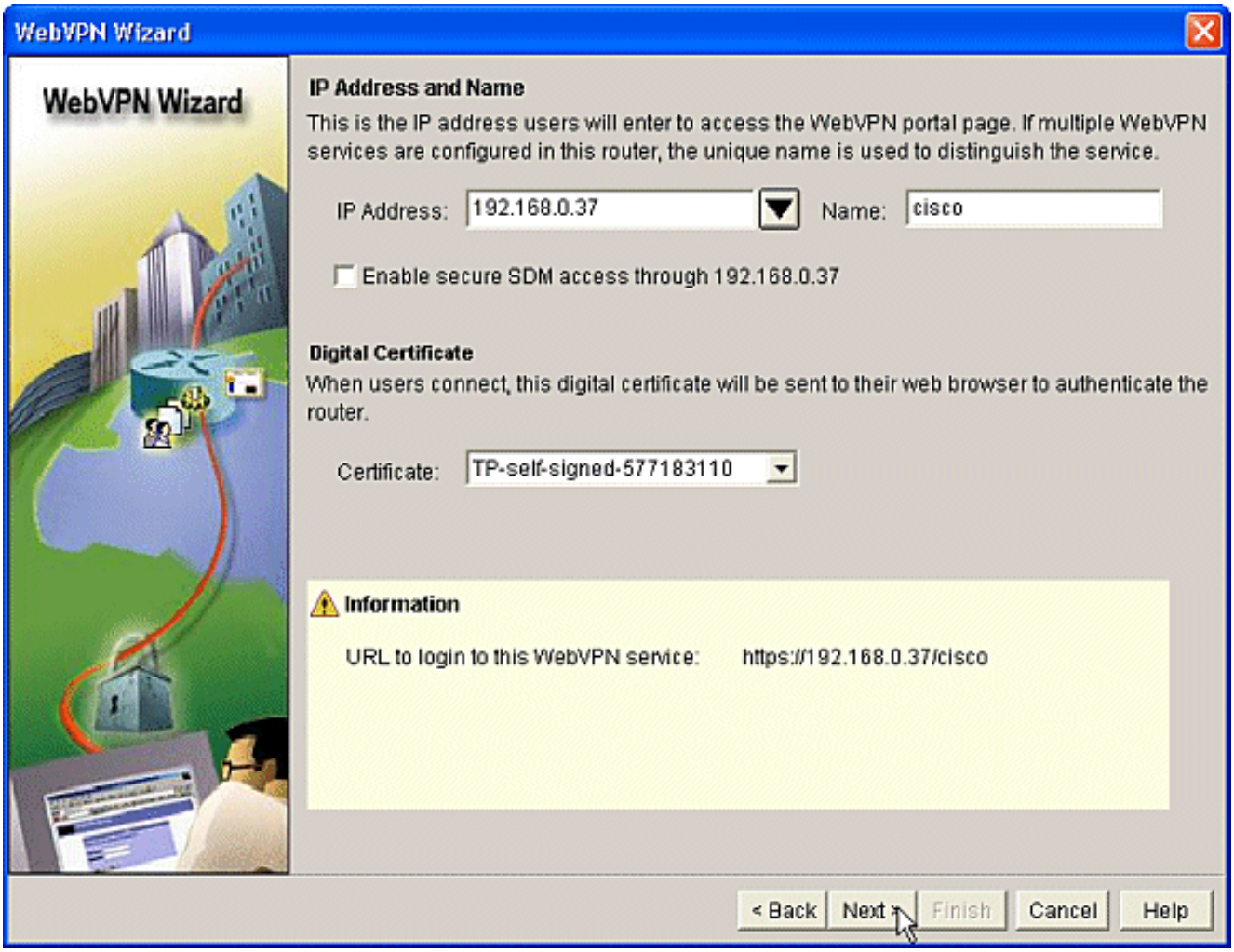
2. WebVPN Wizard(WebVPN 마법사) 화면에는 구성할 수 있는 매개변수가 나열됩니다.Next(**다음)를 클릭합니다**

.



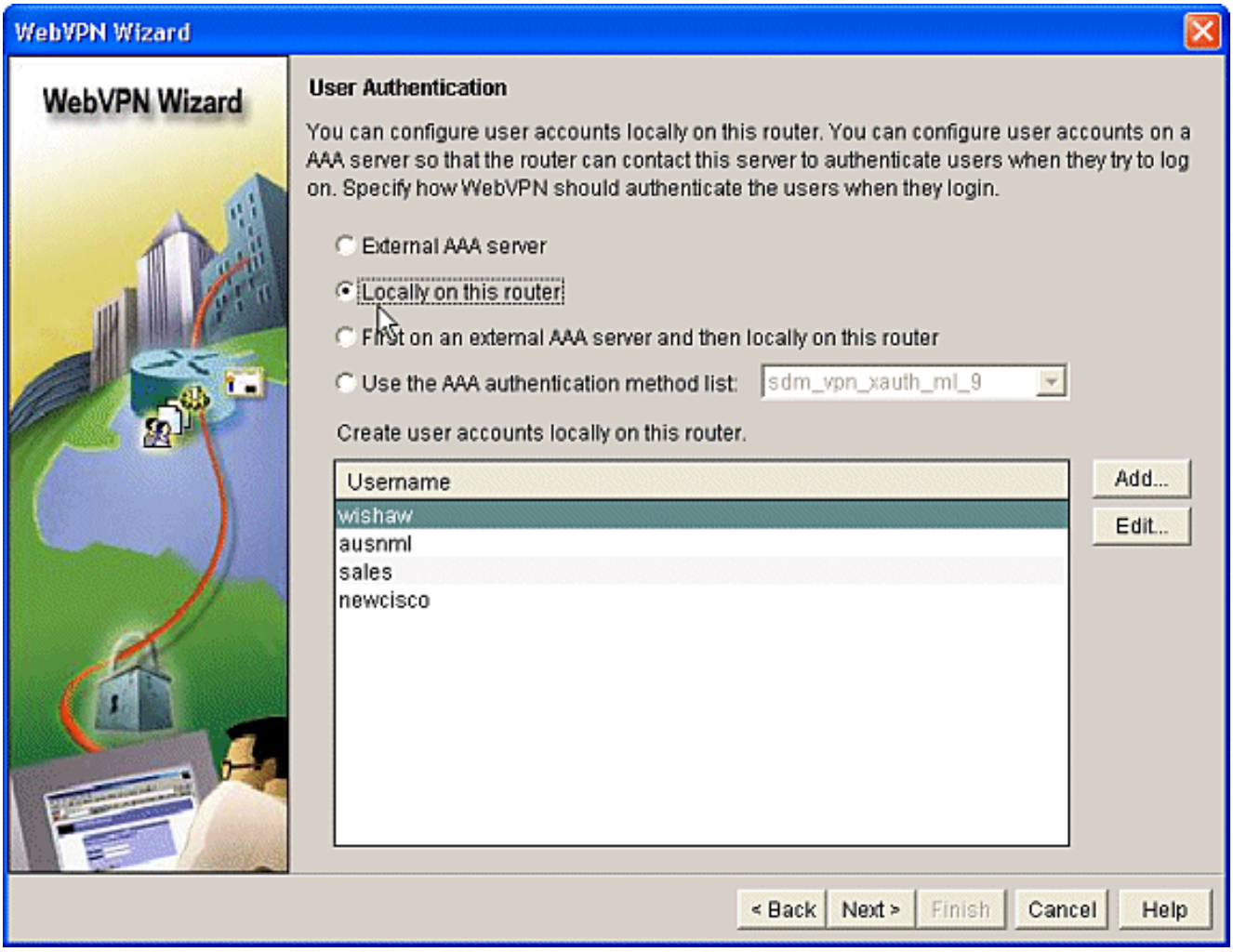
3. WebVPN 게이트웨이의 IP 주소, 서비스의 고유한 이름 및 디지털 인증서 정보를 입력합니다 .Next(**다음)를 클릭합니다**

.

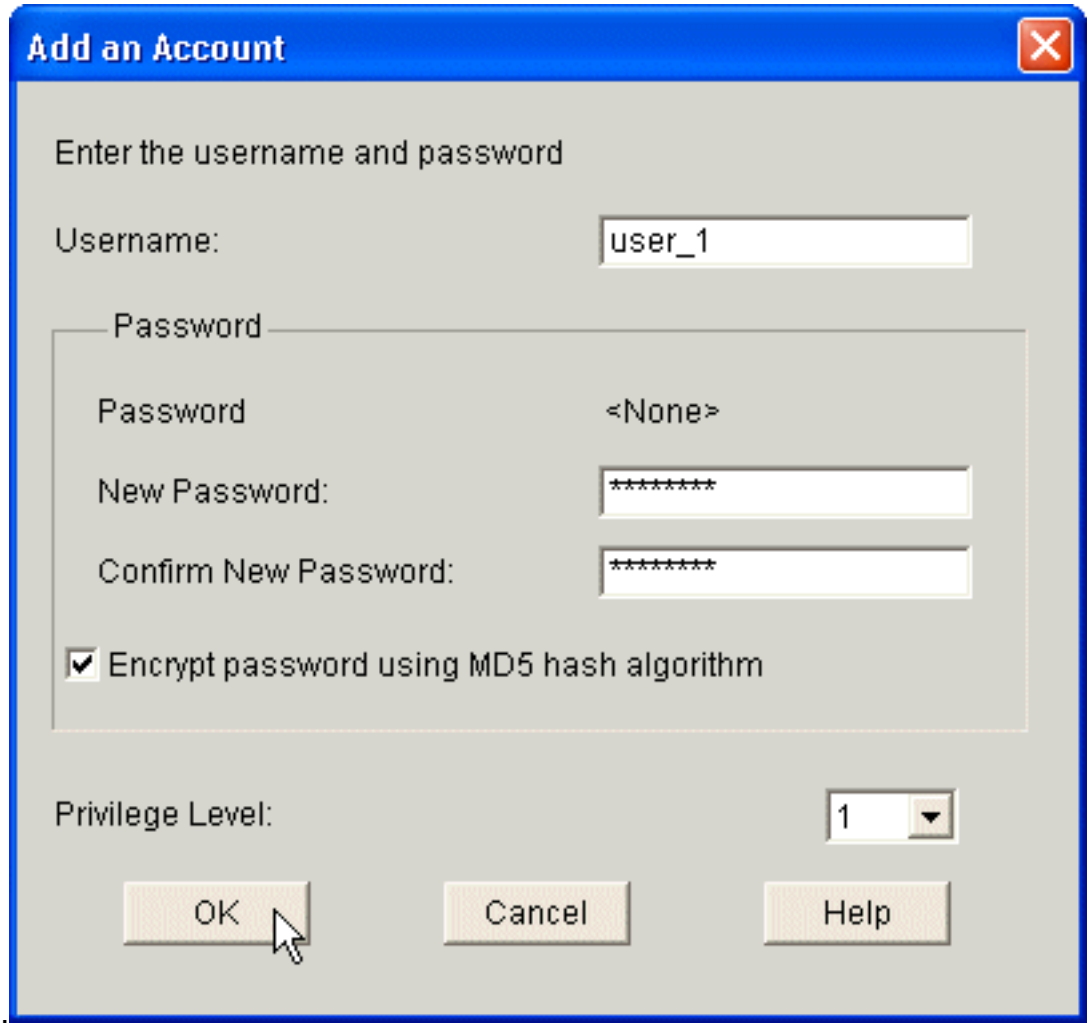


4. 이 WebVPN 게이트웨이에 대한 인증을 위해 사용자 계정을 만들 수 있습니다.로컬 계정 또는 외부 AAA(Authentication, Authorization, and Accounting) 서버에서 생성된 계정을 사용할 수 있습니다.이 예에서는 라우터의 로컬 계정을 사용합니다.**이 라우터**에서 **로컬로** 라디오 버튼**을 선택하고 Add(추가)**를 **클릭합니다**

.

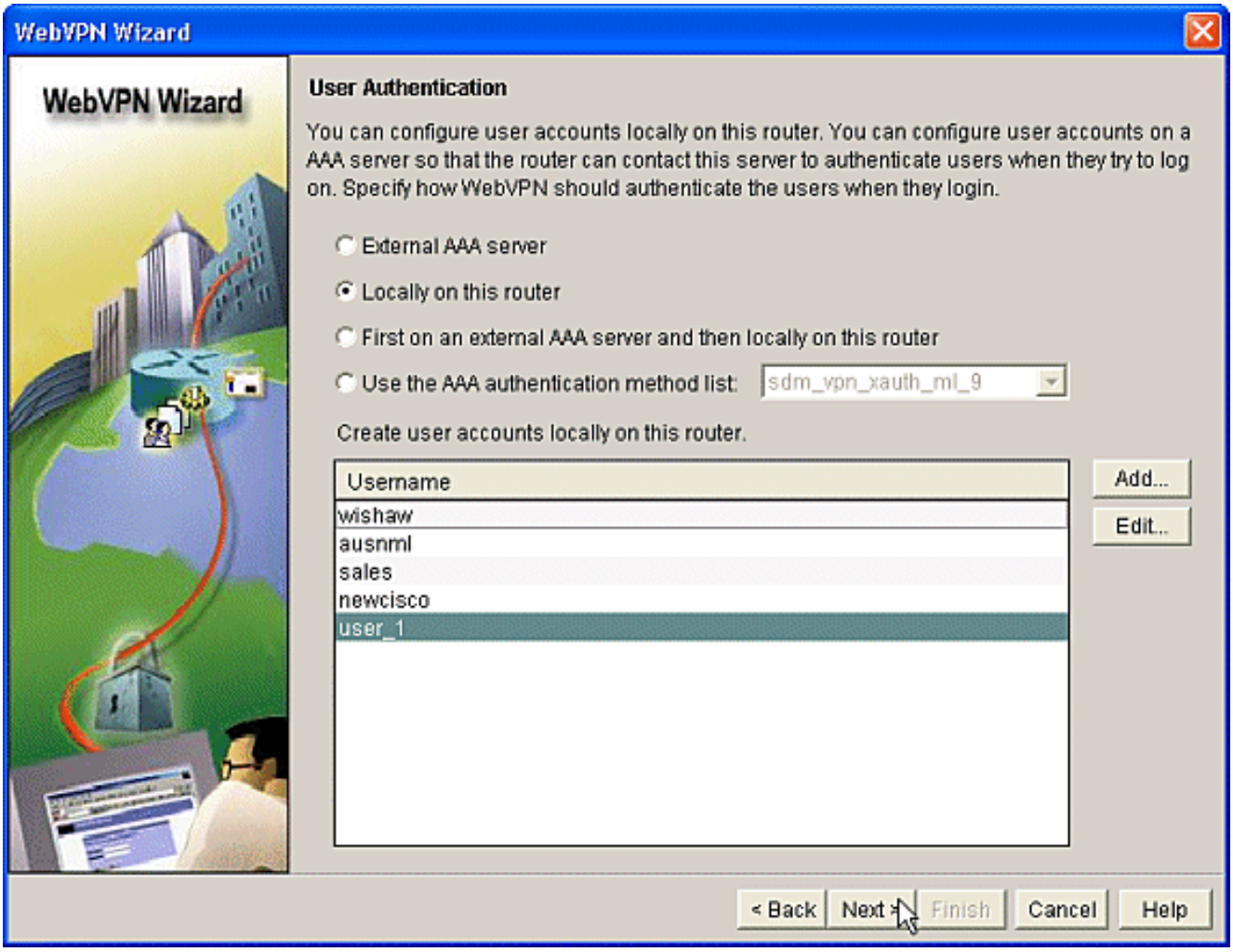


5. Add an Account(계정 추가) 화면에서 새 사용자에 대한 계정 정보를 입력하고 **OK**(확인)를 클



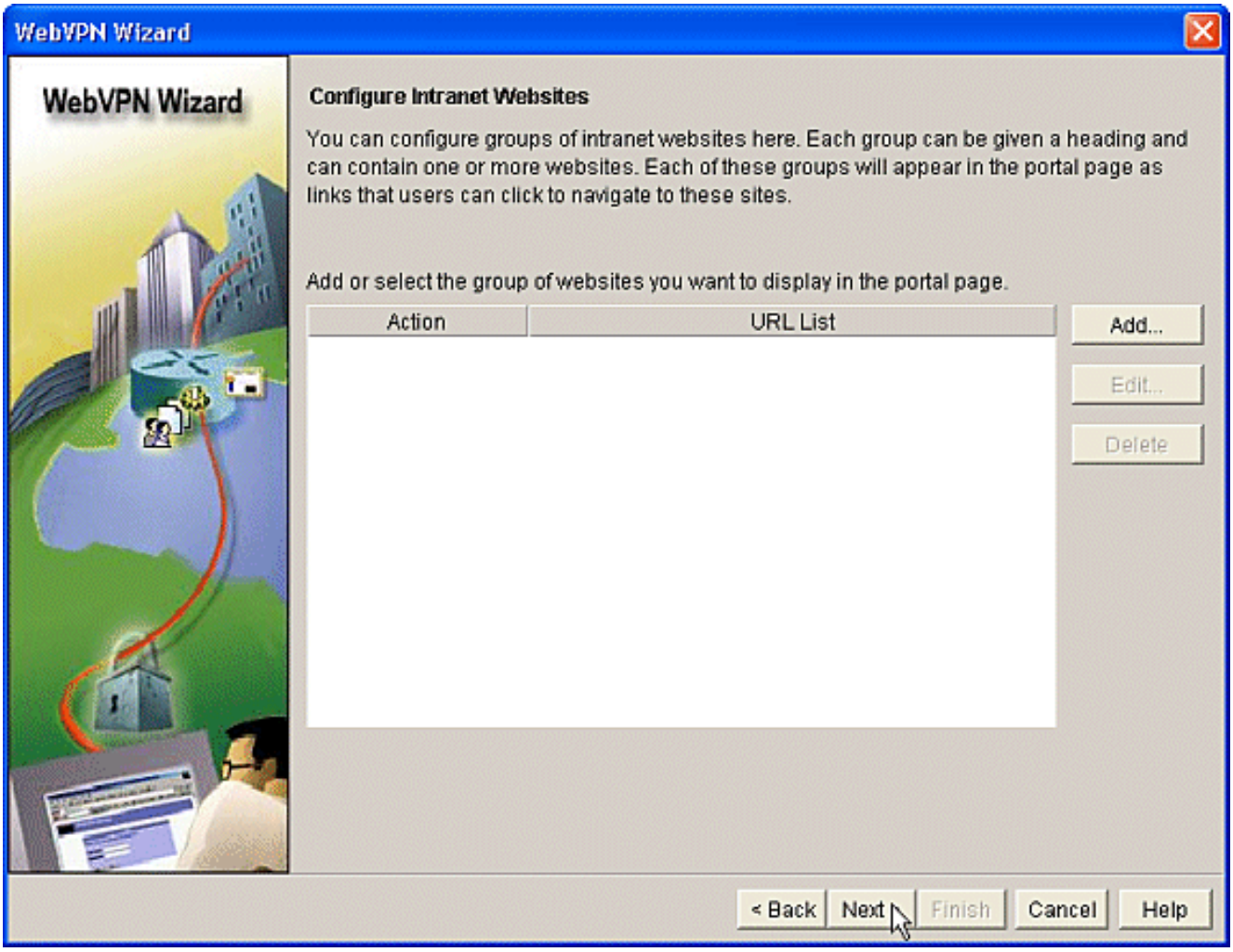
릭합니다.

6. 사용자를 생성한 후 User Authentication(사용자 인증) 페이지에서 Next(다음)를 클릭합니다
.



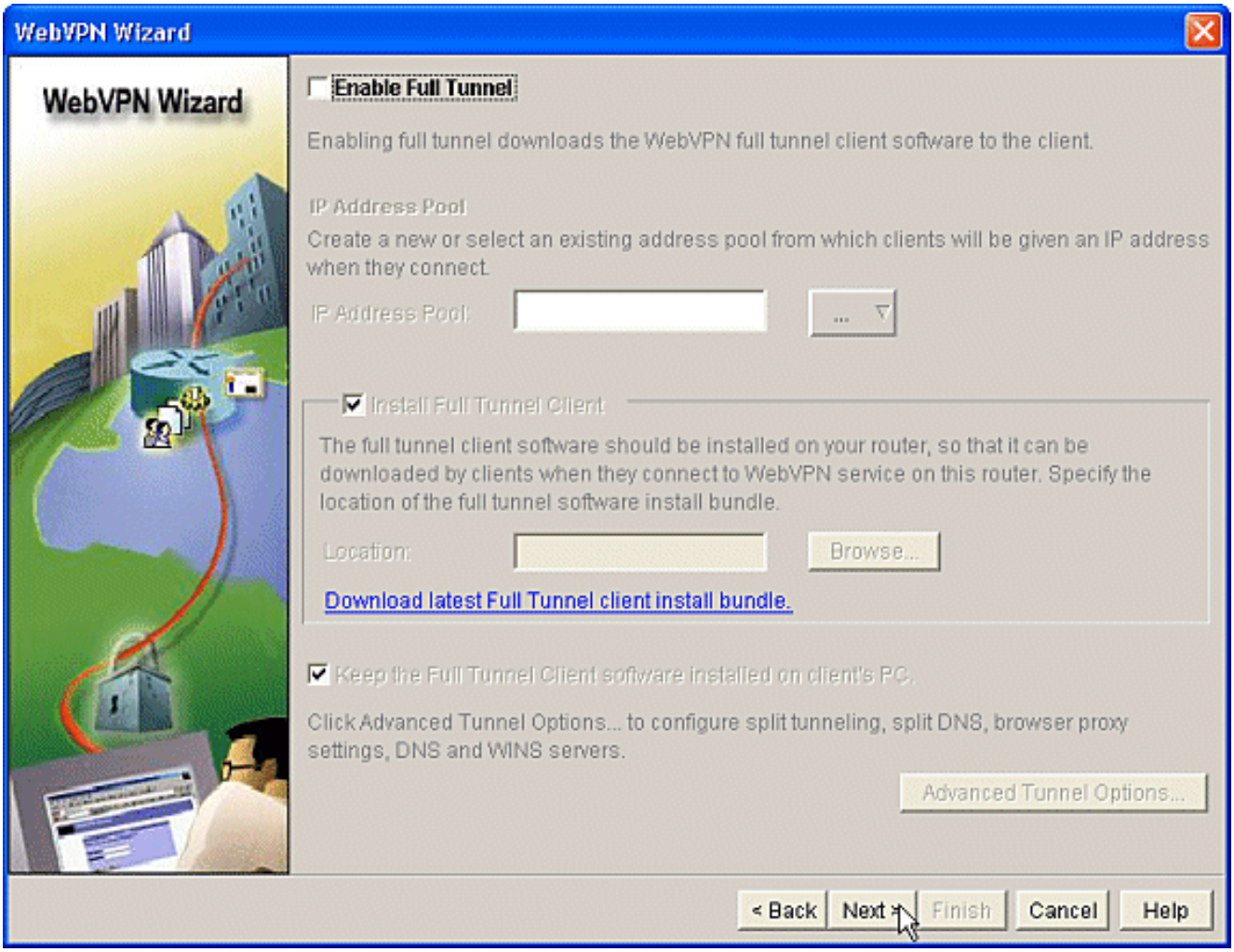
7. Configure Intranet Websites(인트라넷 웹 사이트 구성) 화면에서는 WebVPN 게이트웨이 사용자가 사용할 수 있는 웹 사이트를 구성할 수 있습니다.이 문서는 CSD의 컨피그레이션에 중점을 두고 있으므로 이 페이지를 무시하십시오.Next(**다음)를 클릭합니다**

.



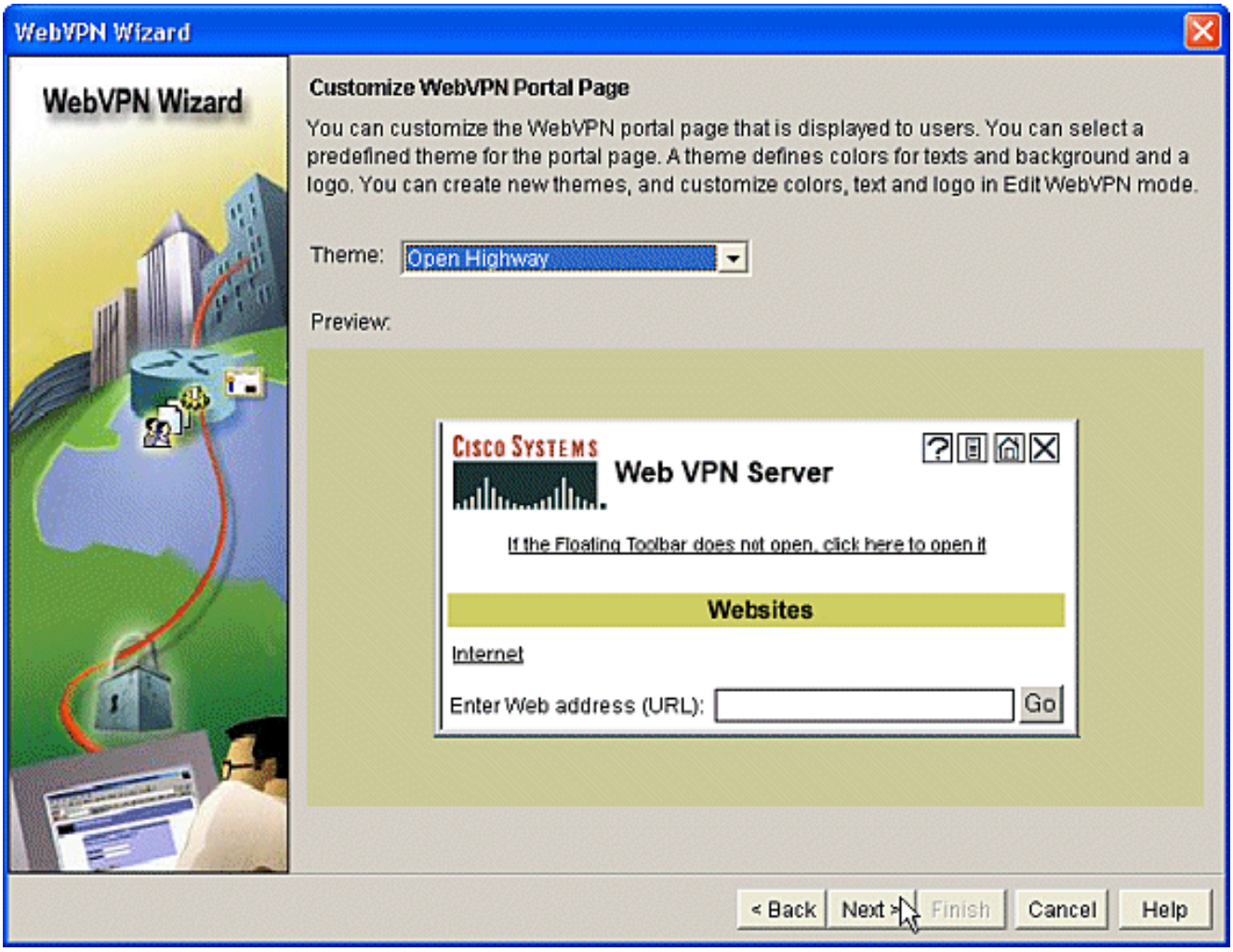
8. 다음 WebVPN Wizard(웹 VPN 마법사) 화면에서 전체 터널 SSL VPN 클라이언트를 사용하도록 선택할 수 있지만, 이 문서의 핵심은 CSD를 활성화하는 방법입니다.Enable **Full Tunnel(전체 터널 활성화)**을 선택 취소하고 **Next(다음)**를 클릭합니다

.

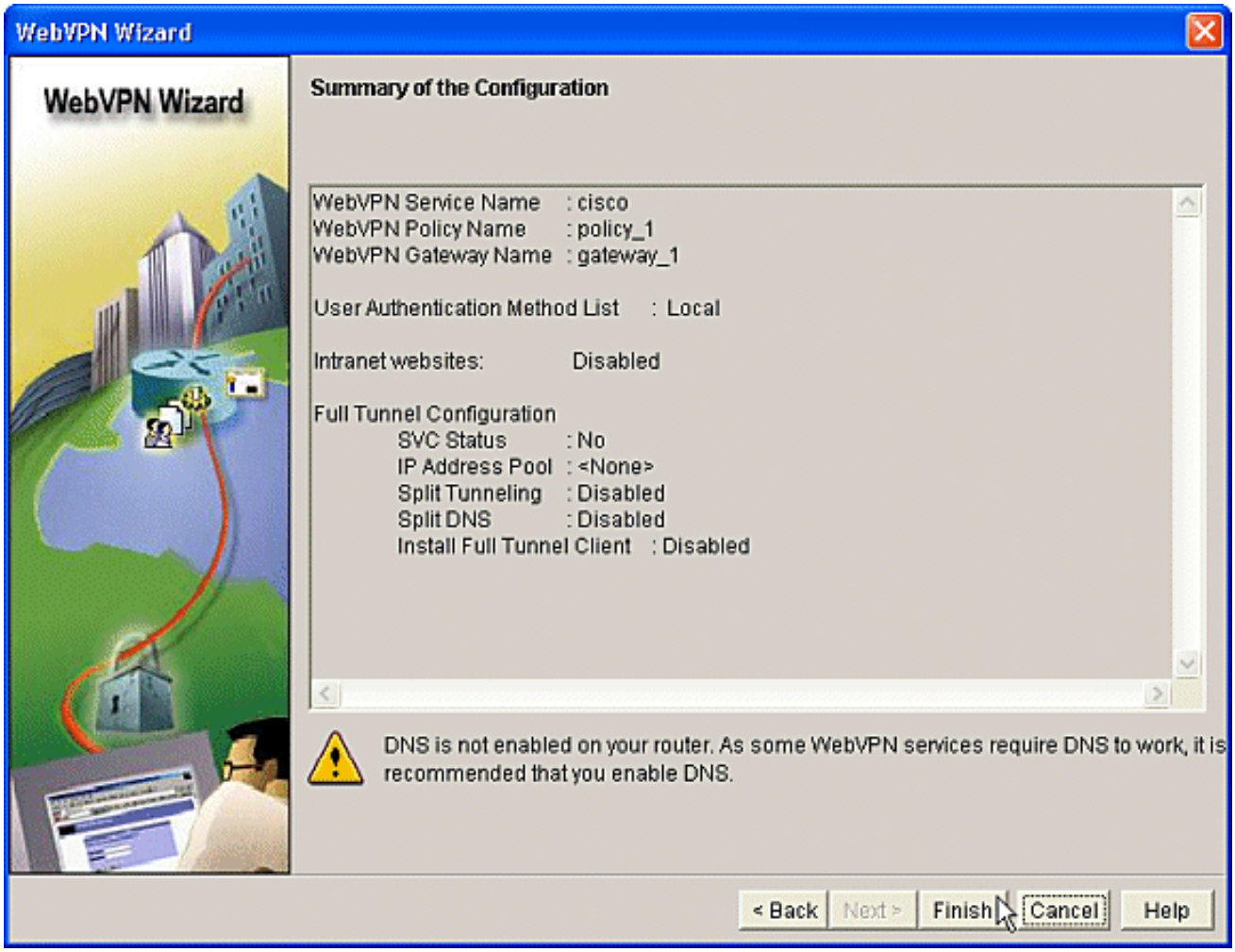


9. 사용자에게 WebVPN 포털 페이지의 모양을 사용자 지정할 수 있습니다.이 경우 기본 모양새가 허용됩니다.Next(**다음)를 클릭합니다**

.



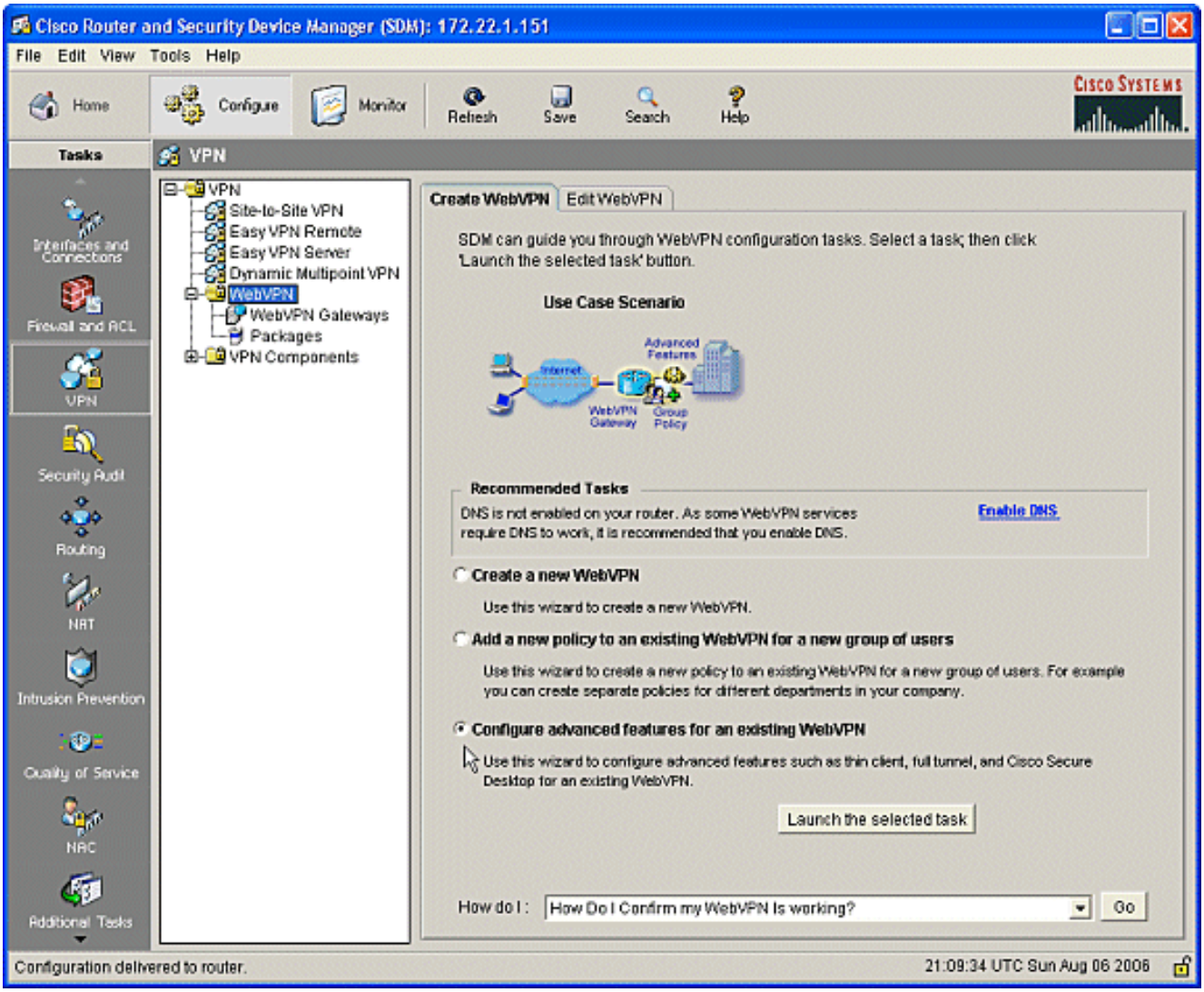
10. 이 시리즈의 마지막 화면이 표시됩니다.WebVPN 게이트웨이에 대한 컨피그레이션 요약을 표시합니다.Finish(**마침**)를 클릭하고 프롬프트가 표시되면 **OK**(확인)를 클릭합니다
.



1단계:2단계:WebVPN 컨텍스트에서 CSD를 활성화합니다.

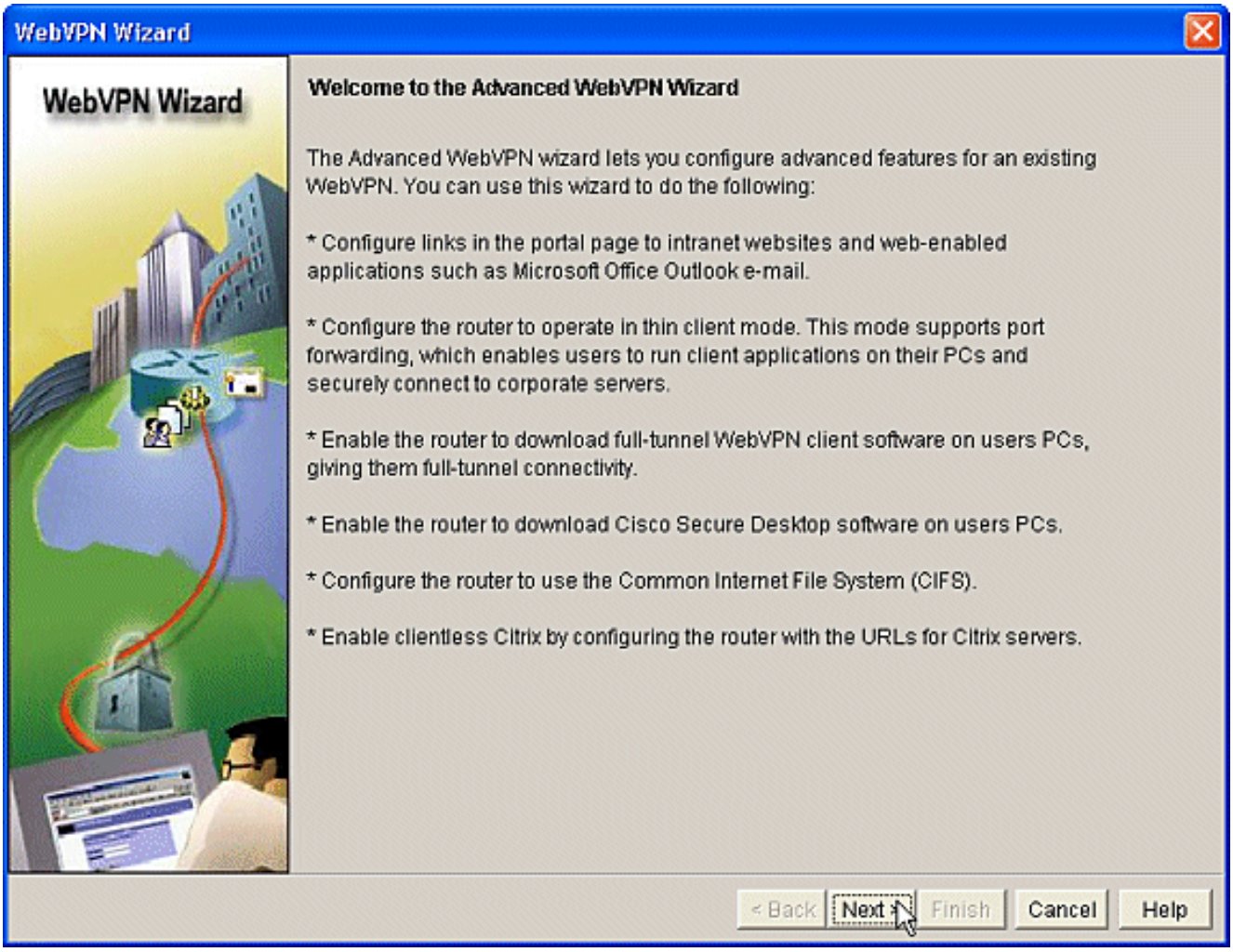
WebVPN Wizard를 사용하여 WebVPN 컨텍스트에서 CSD를 활성화합니다.

1. WebVPN 마법사의 고급 기능을 사용하여 새로 생성된 컨텍스트에 대해 CSD를 활성화합니다.CSD 패키지가 아직 설치되지 않은 경우 이 마법사를 통해 CSD 패키지를 설치할 수 있습니다.SDM에서 구성 탭을 클릭합니다.탐색 창에서 **VPN > WebVPN**을 클릭합니다.Create **WebVPN(WebVPN 생성)** 탭을 클릭합니다.**기존 WebVPN** 라디오 버튼**에 대한 고급 기능 구성**을 선택합니다.**선택한 작업 시작** 버튼**을** 클릭합니다
.



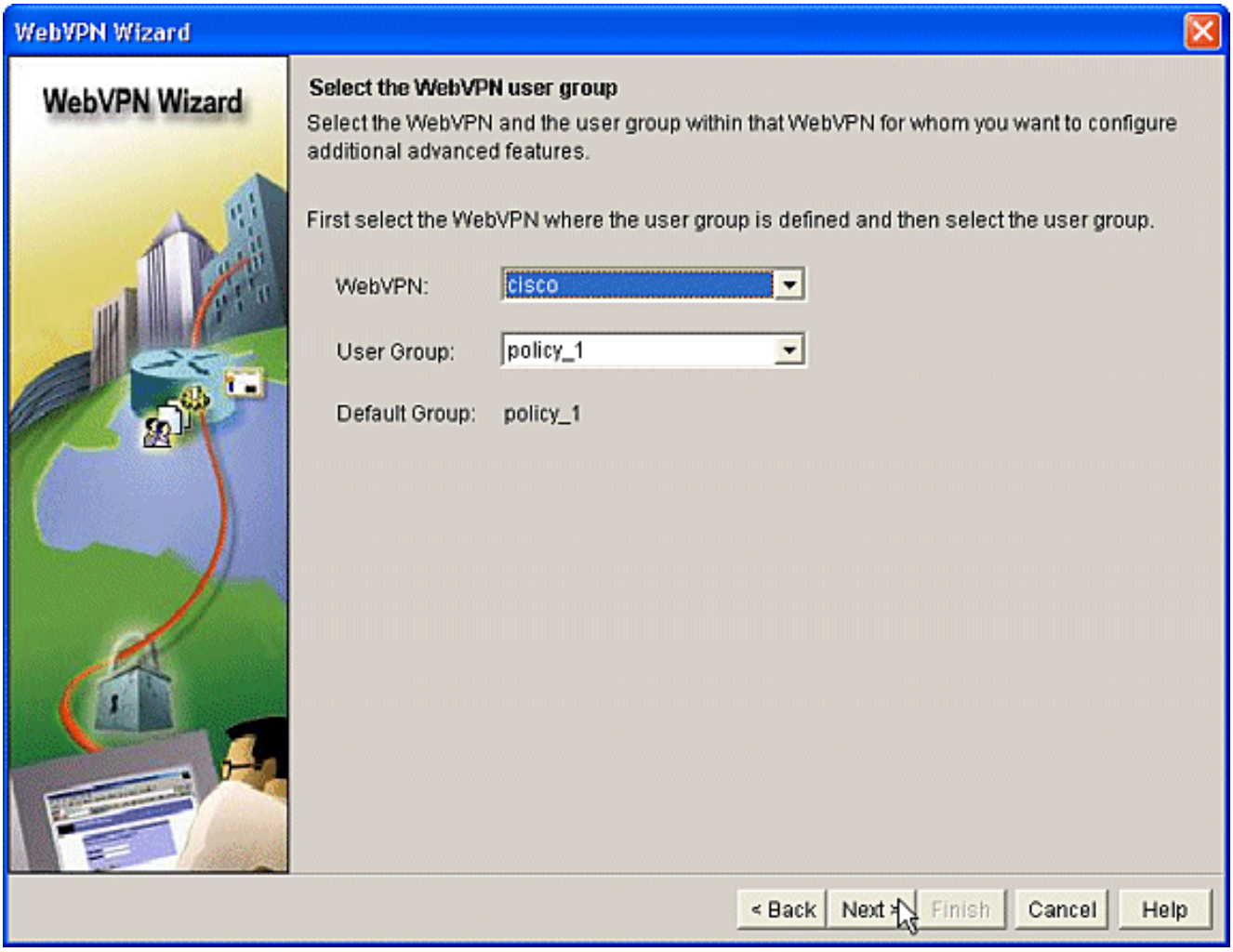
2. 고급 WebVPN 마법사의 시작 페이지가 표시됩니다.Next(**다음)를 클릭합니다**

.



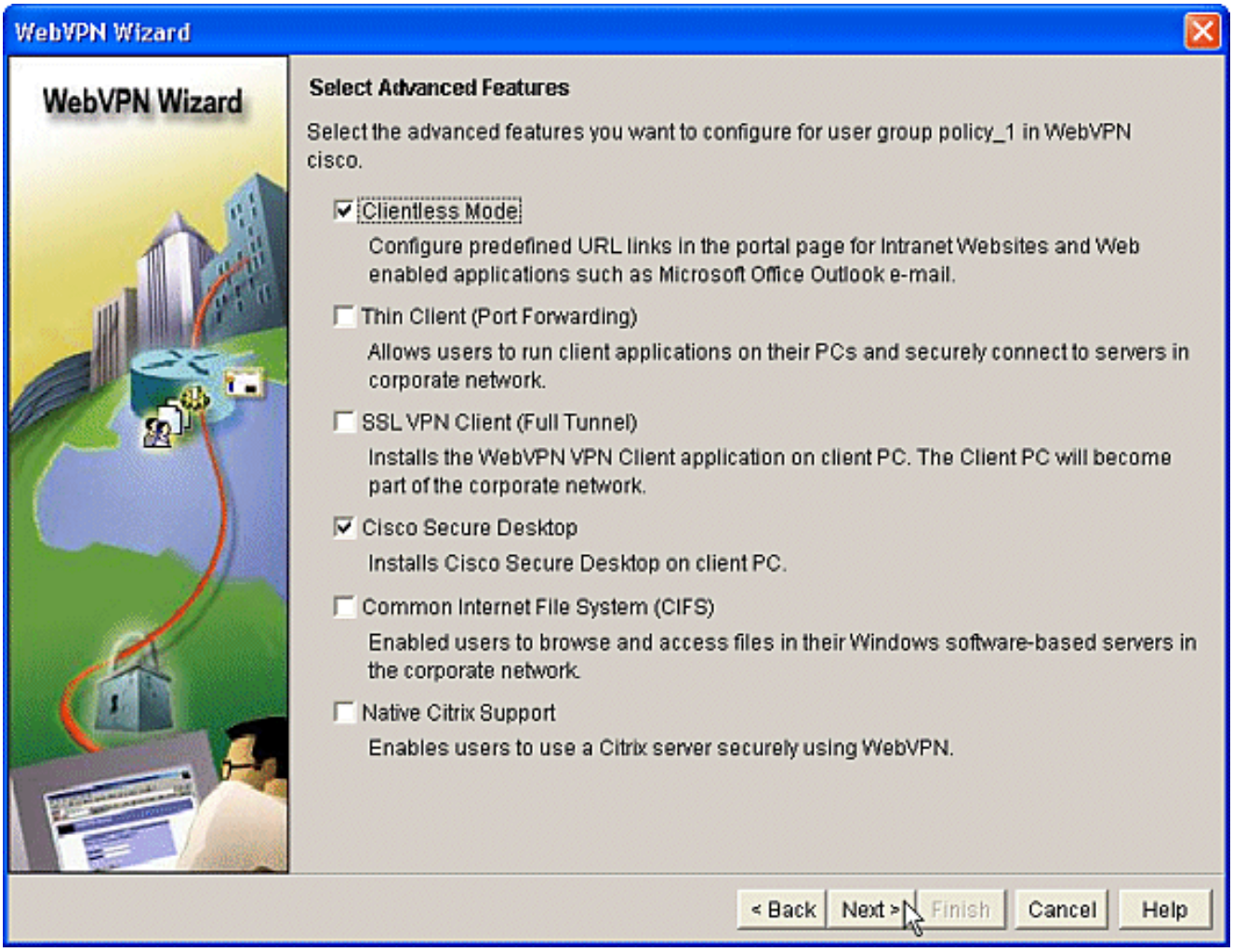
3. 필드의 드롭다운 상자에서 WebVPN 및 사용자 그룹을 선택합니다.선택 항목에 고급 WebVPN 마법사 기능이 적용됩니다.Next(**다음)를 클릭합니다**

.

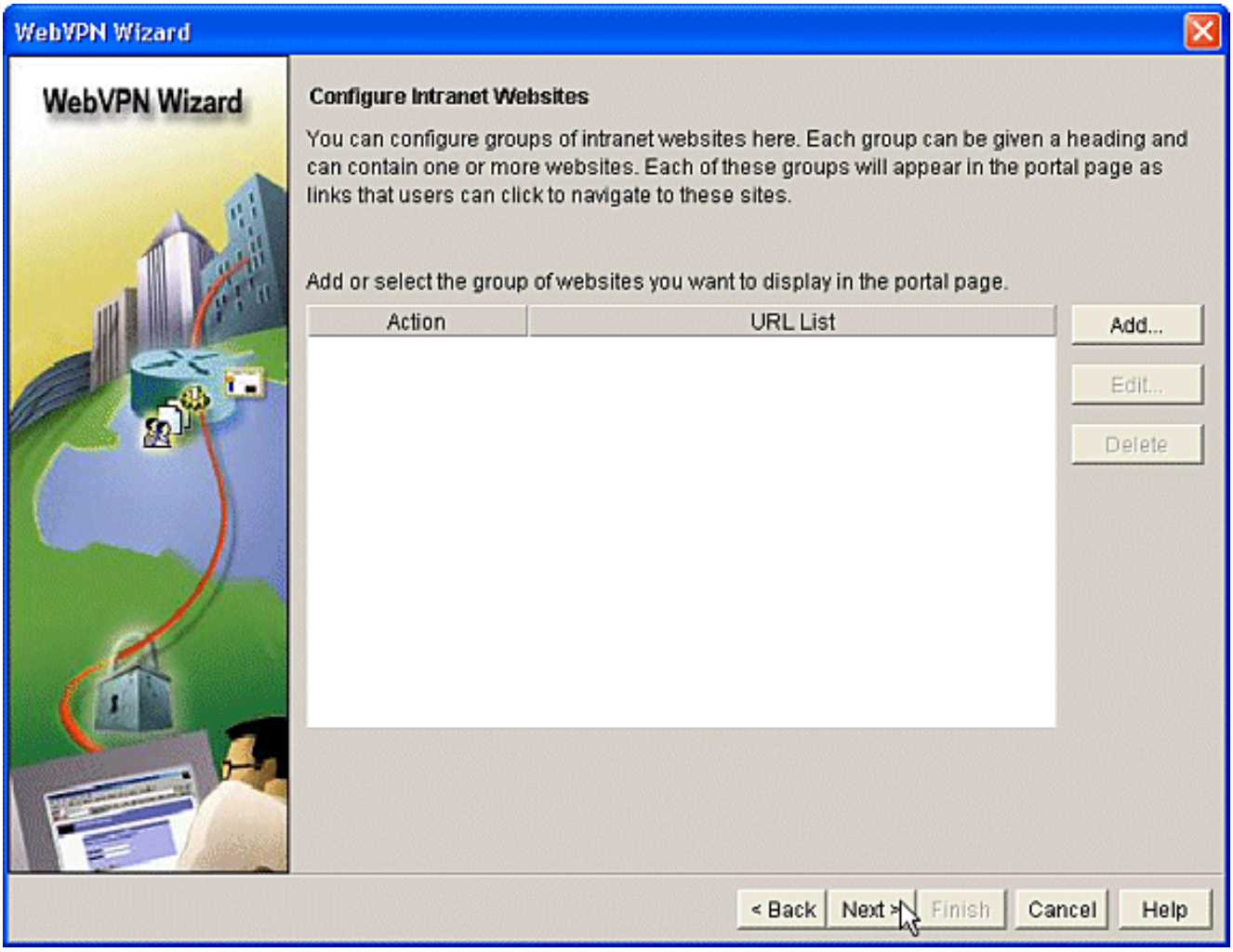


4. 고급 기능 선택 화면에서는 나열된 기술 중에서 선택할 수 있습니다.**Cisco Secure Desktop을 확인합니다**.이 예에서는 클라이언트리스 **모드**를 선택합니다.나열된 다른 기술을 선택하면 관련 정보를 입력할 수 있는 추가 창이 열립니다.**다음** 버튼을 클릭합니다

.



5. 인트라넷 웹 사이트 구성 화면에서는 사용자가 사용할 웹 사이트 리소스를 구성할 수 있습니다.OWA(Outlook Web Access)와 같은 회사의 내부 웹 사이트를 추가할 수 있습니다
.

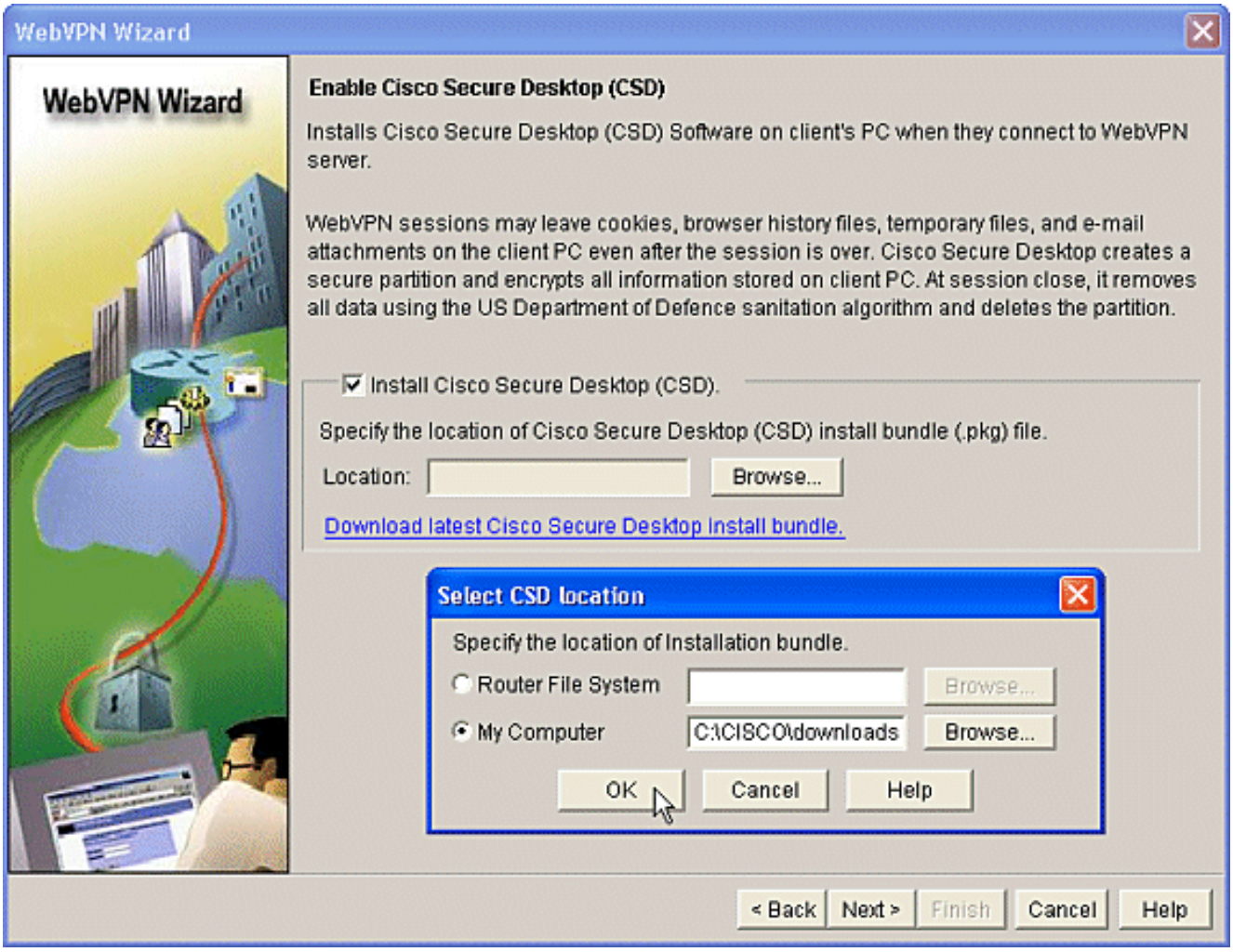


6. Enable Cisco Secure Desktop (CSD)(Cisco Secure Desktop(CSD) 활성화) 화면에서 이 컨텍스트에 대해 CSD를 활성화할 수 있습니다.Install **Cisco Secure Desktop (CSD)(Cisco Secure Desktop 설치)(CSD(Cisco Secure Desktop) 설치)** 옆의 상자를 선택하고 Browse(찾아보기)를 **클릭합니다**

.

7. Select CSD Location(CSD 위치 선택) 영역에서 **My Computer(내 컴퓨터)를** 선택합니다 .Browse(찾아보기) 버튼**을** 클릭합니다.관리 워크스테이션에서 CSD IOS 패키지 파일을 선택합니다.**확인** 버튼을 클릭합니다.**다음** 버튼을 클릭합니다

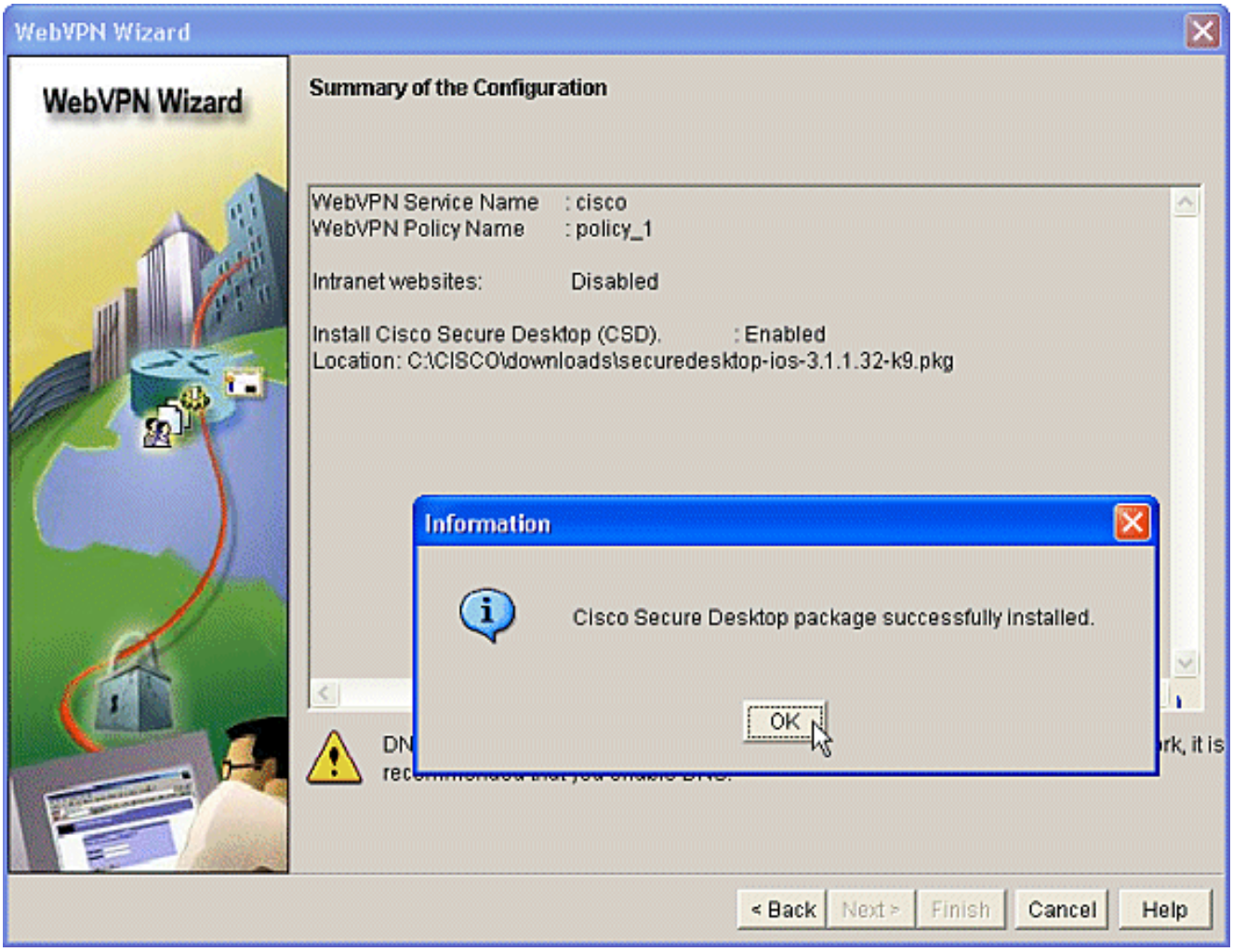
.



8. '구성' 화면의 요약이 표시됩니다.**Finish** 버튼을 클릭합니다

.

9. CSD 패키지 파일이 성공적으로 설치되었다는 메시지가 표시되면 OK를 클릭합니다
.



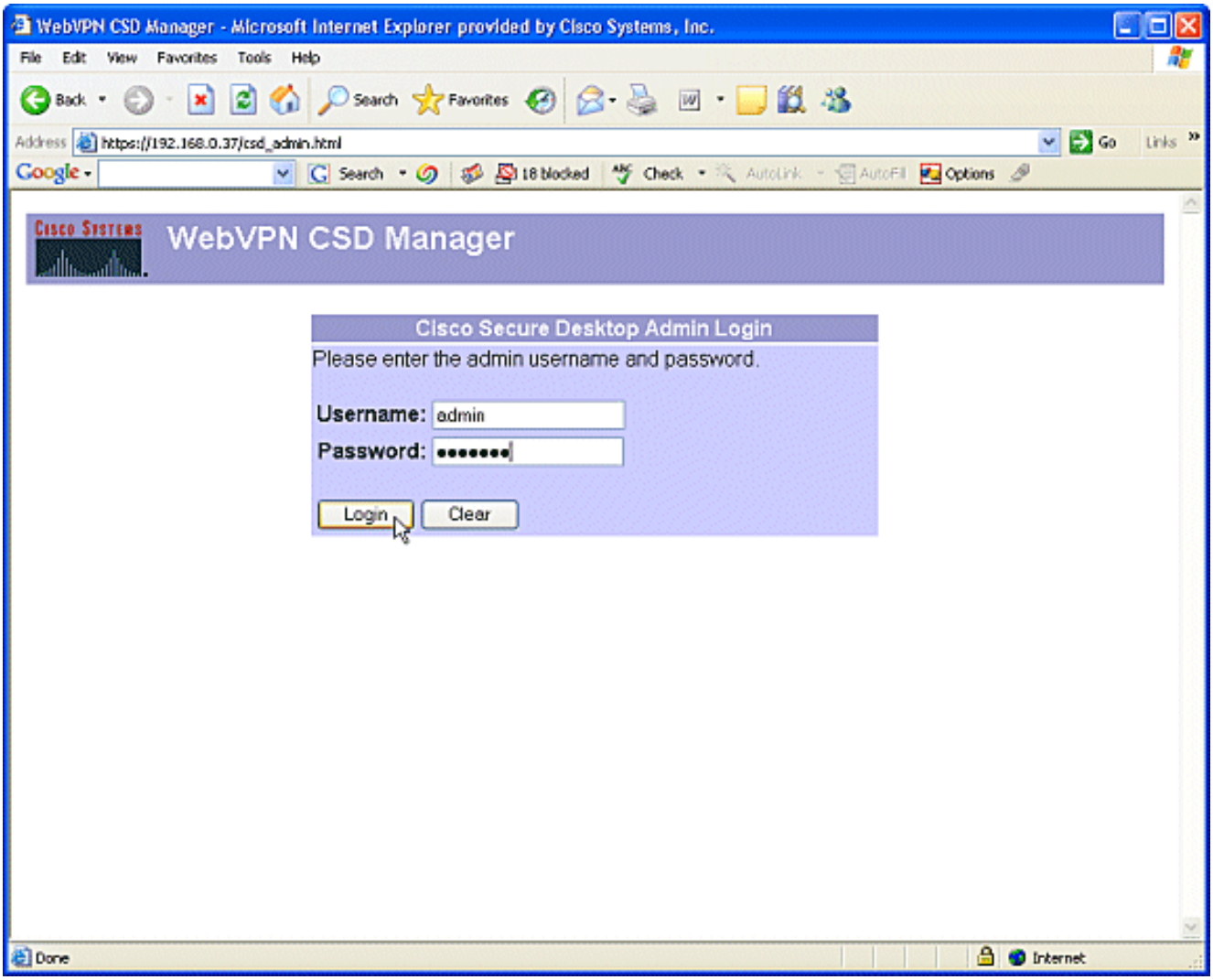
2단계:웹 브라우저를 사용하여 CSD를 구성합니다.

이 단계는 웹 브라우저에서 CSD 컨피그레이션을 완료하는 데 사용됩니다.

2단계:1단계:Windows 위치를 정의합니다.

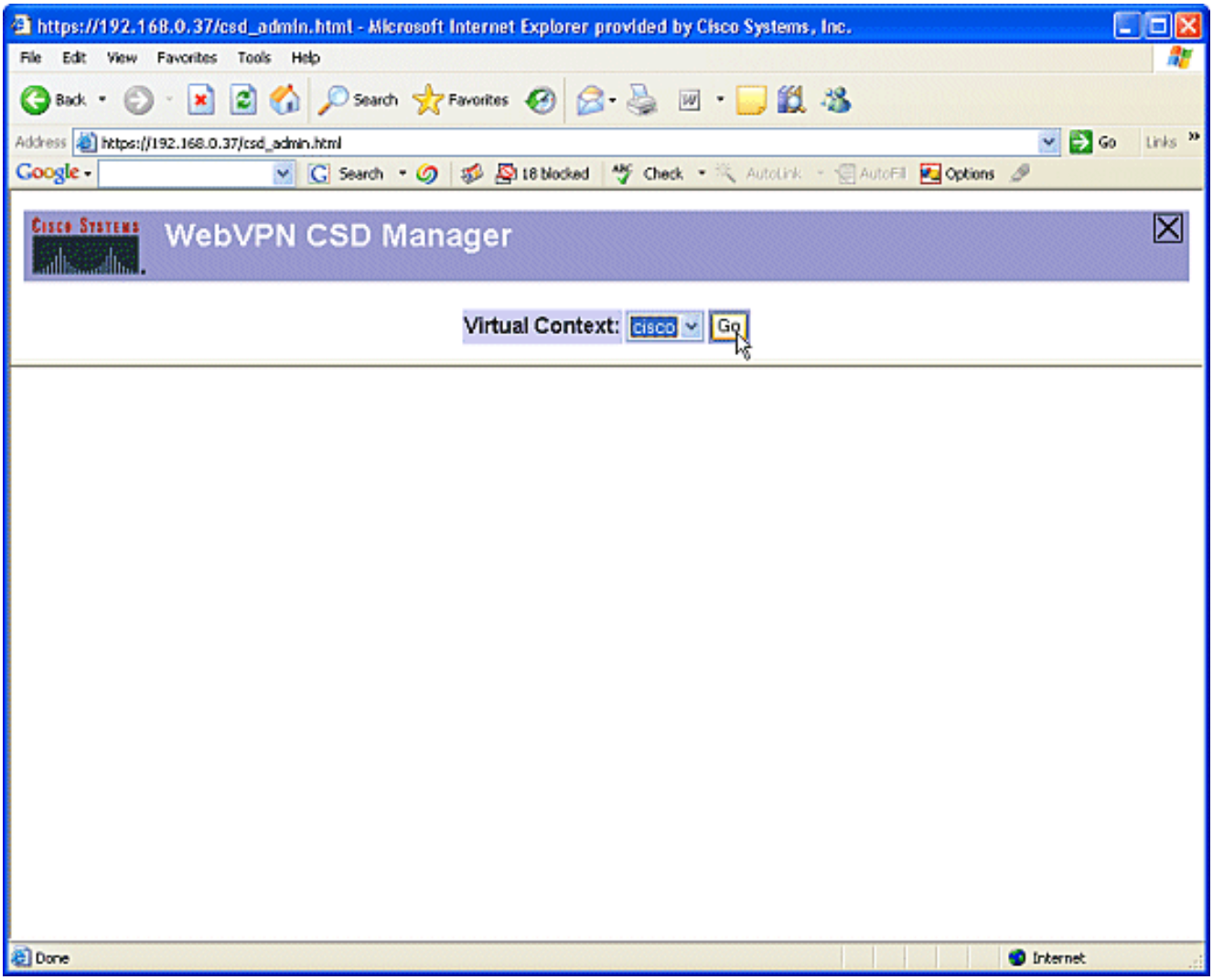
Windows 위치를 정의합니다.

1. 웹 브라우저(예: **https://WebVPNgateway_IP Address/csd_admin.html**)를 **엽니다**.
2. 사용자 이름 admin을 **입력합니다**.라우터의 enable secret인 비밀번호를 입력합니다.Login(**로그인)을 클릭합니다**
.



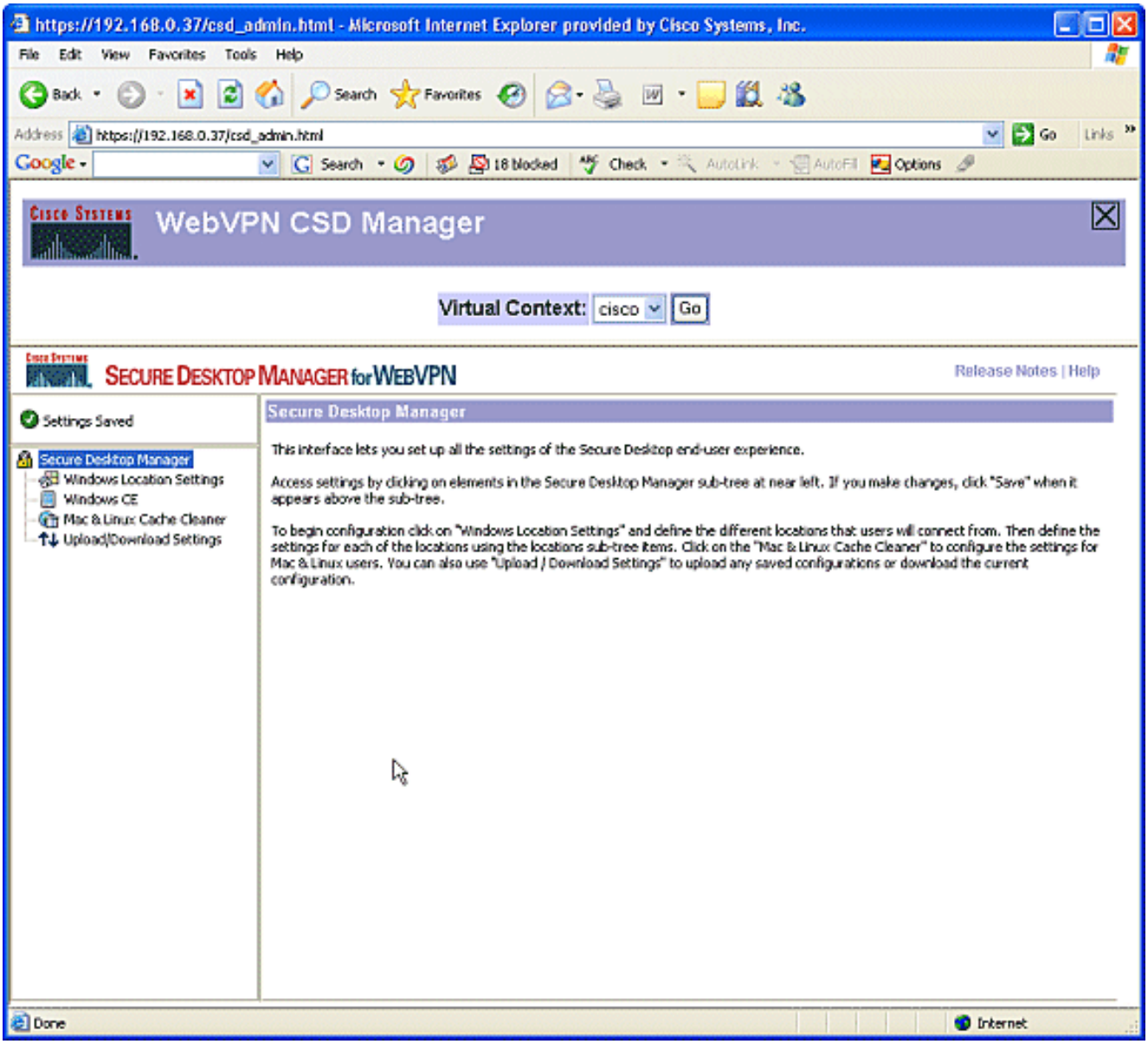
3. 라우터에서 제공하는 인증서를 수락하고 드롭다운 상자에서 컨텍스트를 선택하고 **Go**를 클릭합니다

.



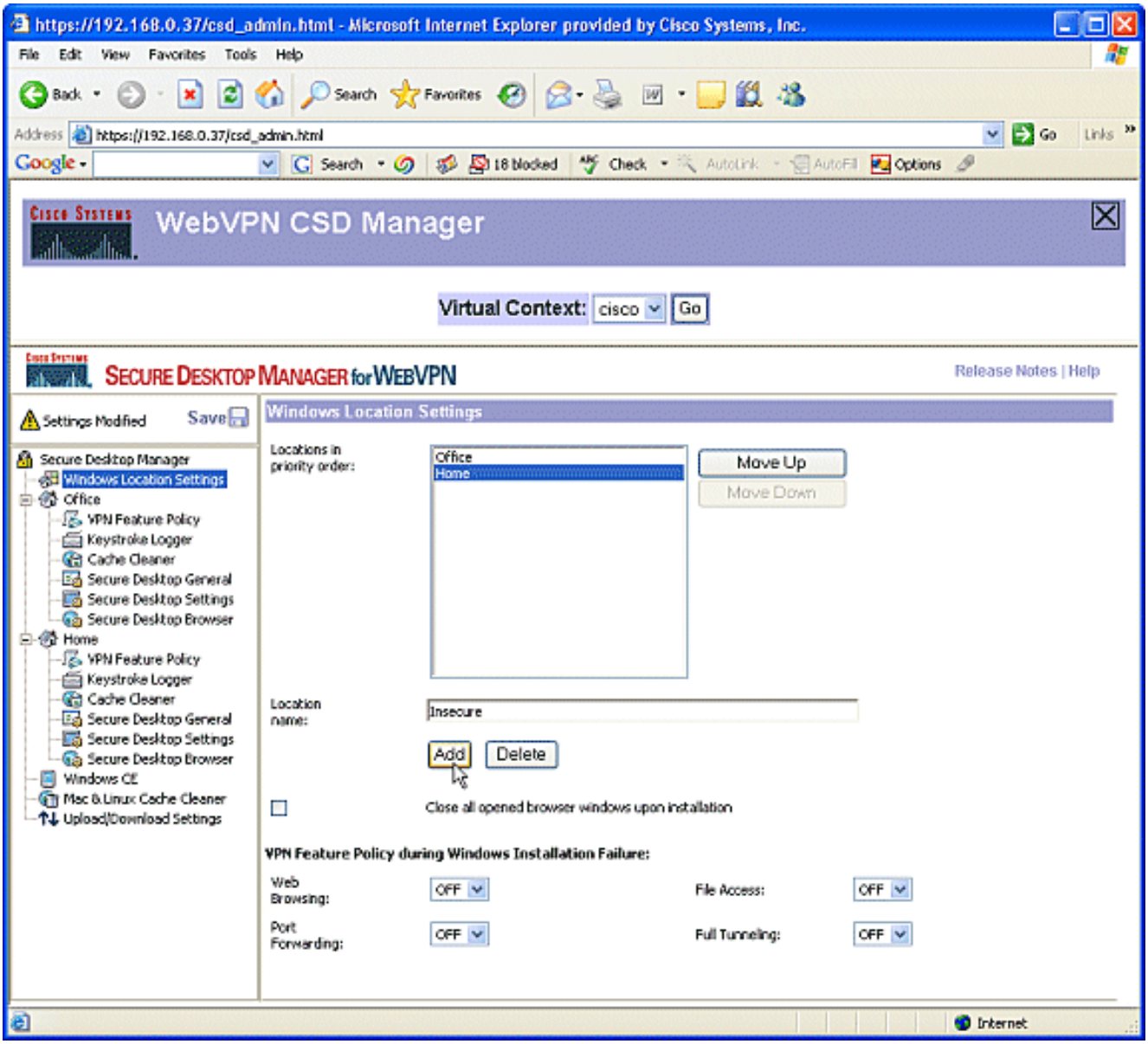
4. Secure Desktop Manager for WebVPN이 열립니다

.



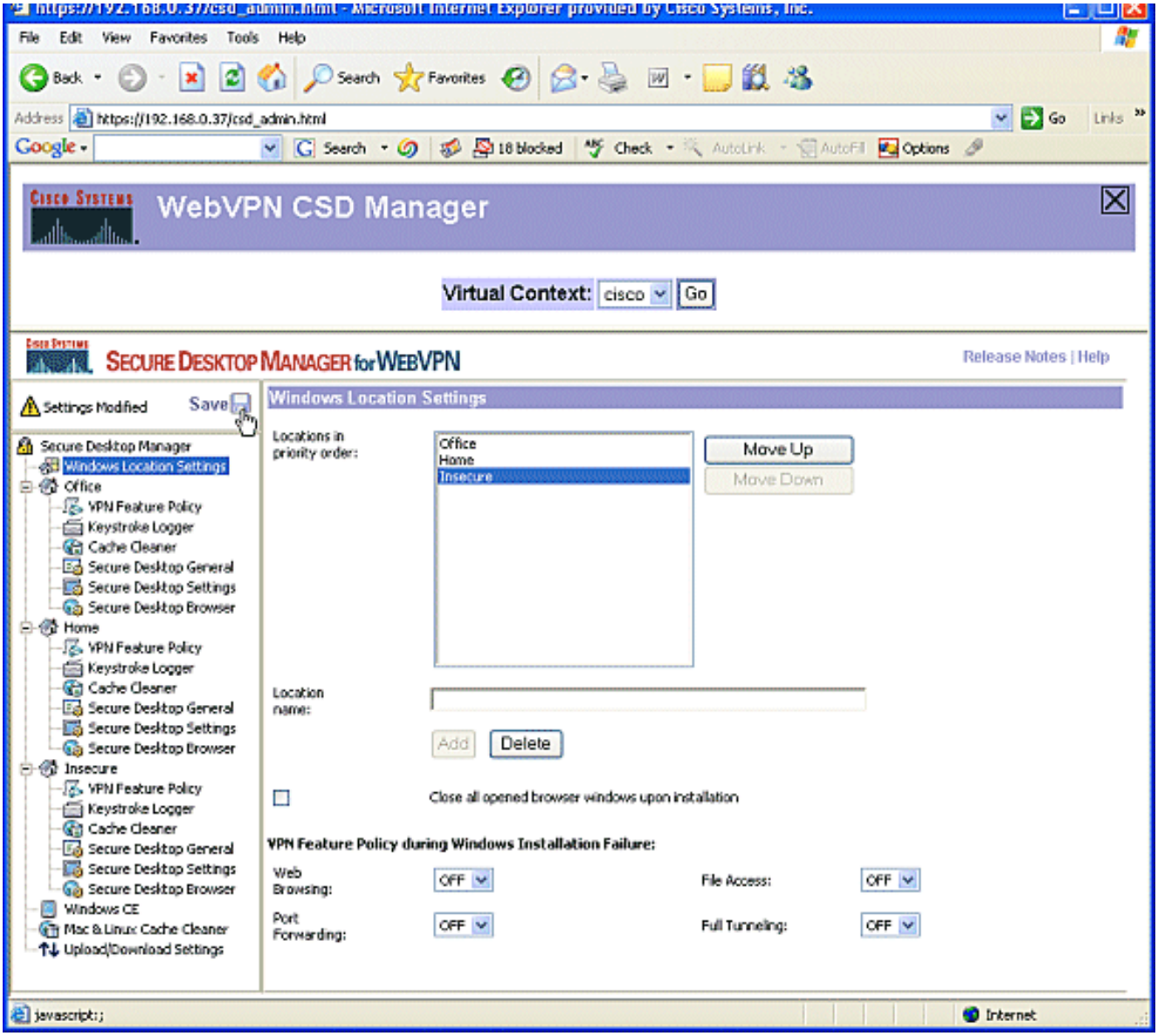
5. 왼쪽 창에서 **Windows 위치 설정**을 선택합니다.위치 이름 옆에 있는 상자에 커서를 놓고 위치 이름을 입력합니다.Add(**추가)를 클릭합니다**.이 예에서는 세 개의 위치 이름이 표시됩니다.사무실, 집 및 안전하지 않습니다.새 위치가 추가될 때마다 왼쪽 창이 확장되어 해당 위치에 대한 구성 가능한 매개변수가 표시됩니다

.



6. Windows 위치를 만든 후 왼쪽 창 상단에서 저장을 클릭합니다.**참고:** 웹 브라우저에서 연결이 끊어지면 설정이 손실되므로 구성을 자주 저장합니다

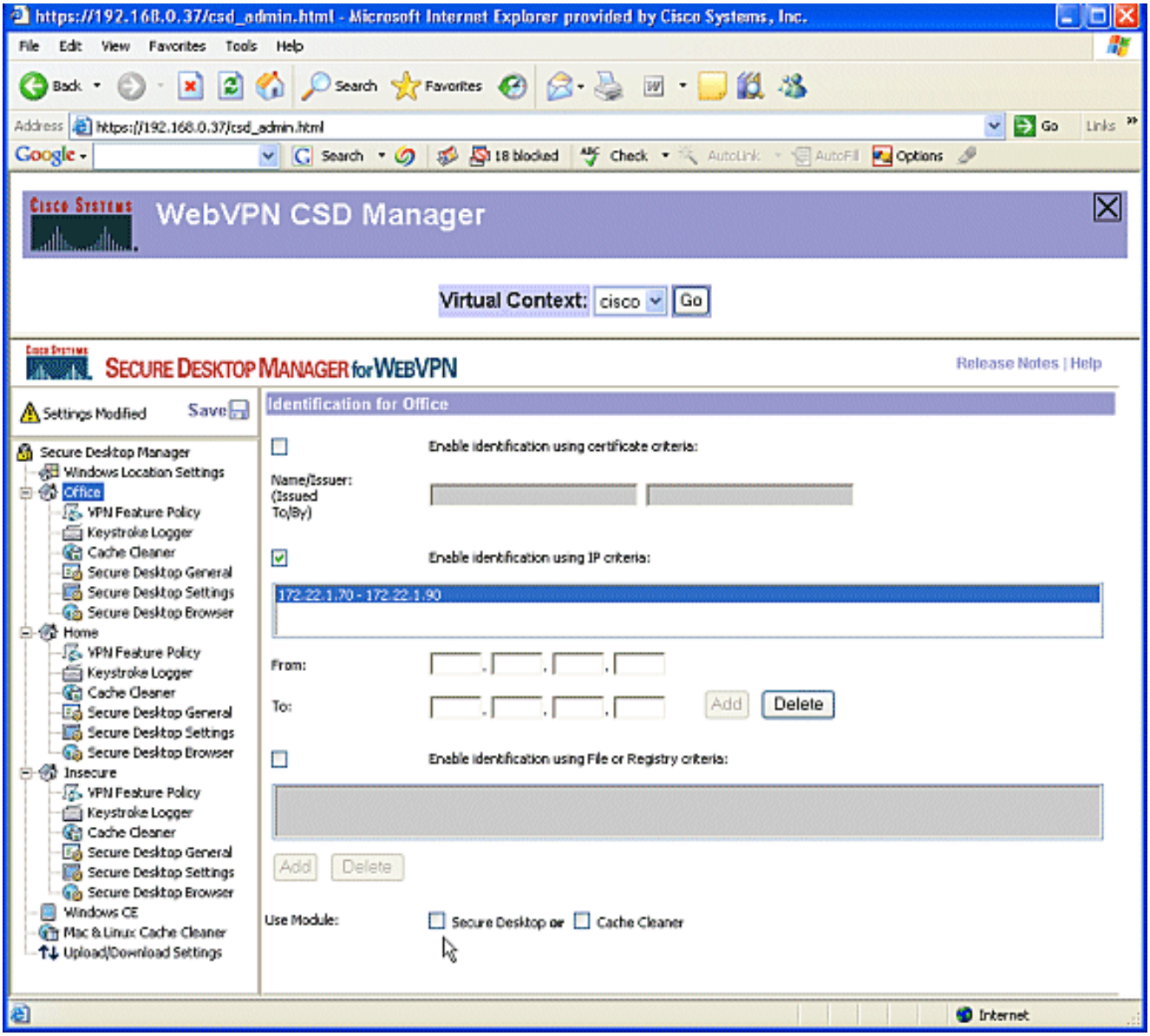
.



2단계:2단계:위치 기준 식별

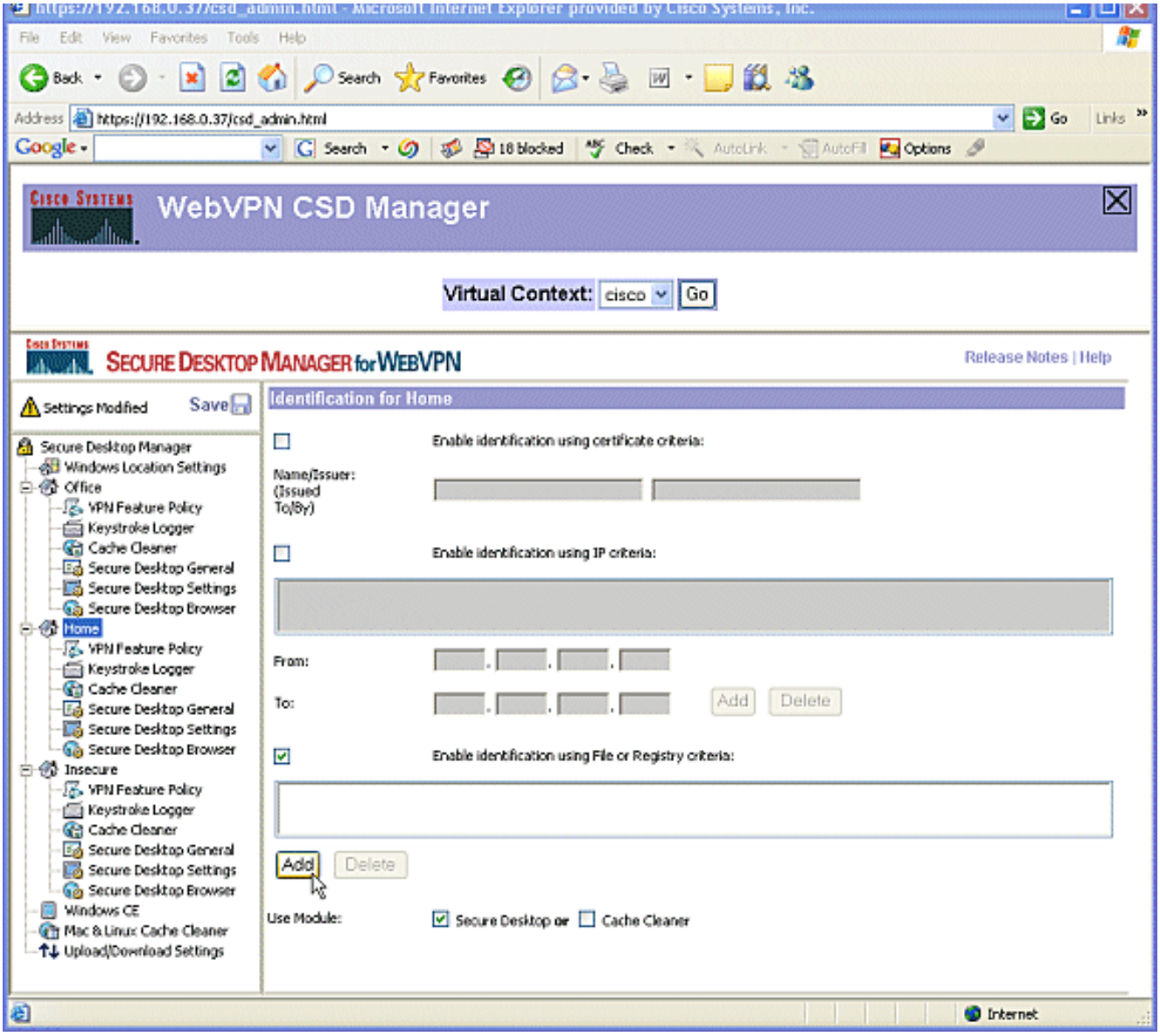
Windows 위치를 서로 구분하려면 각 위치에 특정 기준을 할당합니다.이를 통해 CSD는 특정 Windows 위치에 적용할 기능을 결정할 수 있습니다.

1. 왼쪽 창에서 **Office**를 클릭합니다.인증서 기준, IP 기준, 파일 또는 레지스트리 기준으로 Windows 위치를 식별할 수 있습니다.이러한 클라이언트에 대해 보안 데스크톱 또는 캐시 클리너를 선택할 수도 있습니다.이러한 사용자는 내부 사무실 직원이므로 IP 기준으로 식별합니다.From(시작) 및 **To(끝)** 상자에 IP 주소 범위**를** 입력합니다.Add(**추가)를 클릭합니다**.Use **Module(모듈 사용)의 선택을 취소합니다.보안 데스크톱**.메시지가 나타나면 **Save**(저장)를 클릭하고 **OK(확인)**를 클릭합니다
.



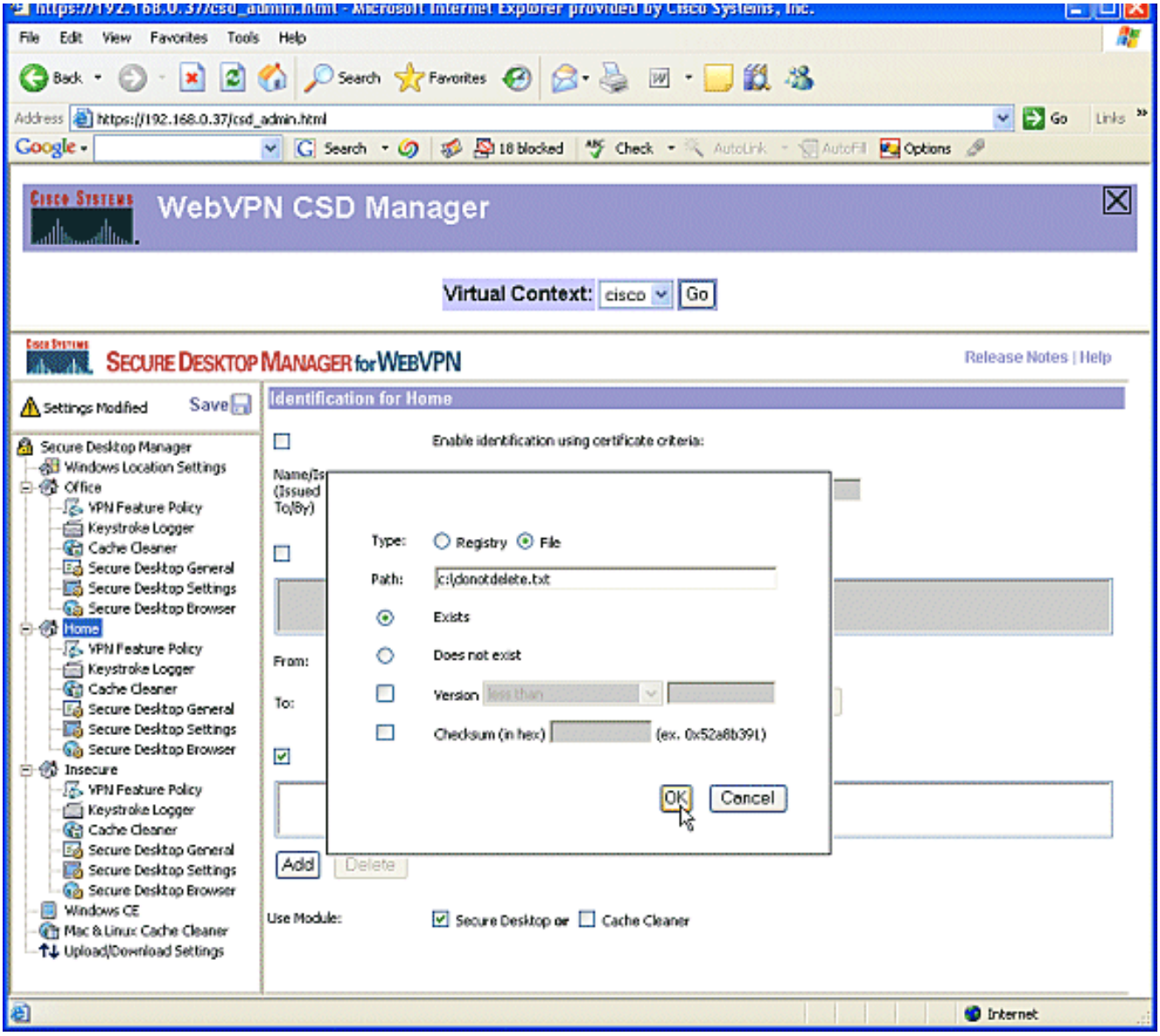
2. 왼쪽 창에서 두 번째 Windows 위치 설정 **홈**을 클릭합니다.**모듈 사용** 확인**Secure Desktop**이 선택되어 있습니다.이러한 클라이언트를 식별하는 파일이 배포됩니다.이러한 사용자에 대한 인증서 및/또는 레지스트리 기준을 배포하도록 선택할 수 있습니다.Enable identification using **File or Registry criteria를 선택합니다**.Add(**추가)를 클릭합니다**

.



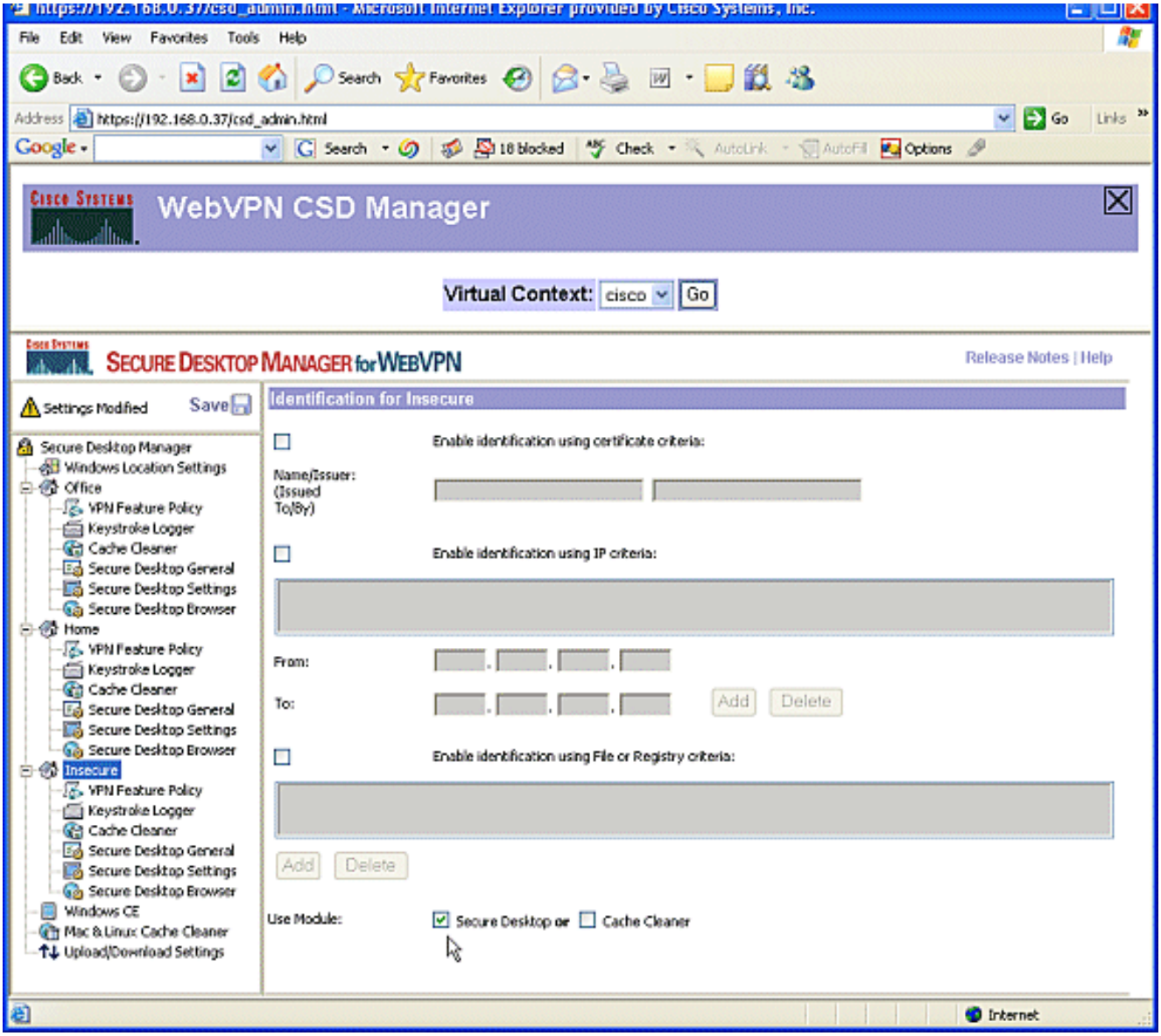
3. 대화 상자에서 **파일**을 선택하고 파일의 경로를 입력합니다.이 파일은 모든 홈 클라이언트에 배포되어야 합니다.라디오 버튼 Exists(있음)를 **확인합니다**.메시지가 표시되면 **확인**을 클릭하고 **저장**을 클릭합니다

.



4. 비보안 위치의 ID를 구성하려면 식별 기준을 적용하지 마십시오.왼쪽 창에서 Unsecure를 클릭합니다.모든 기준을 선택하지 않은 상태로 둡니다.**모듈 사용 확인:보안 데스크톱**.메시지가 나타나면 **Save**(저장)를 클릭하고 **OK(확인)**를 클릭합니다

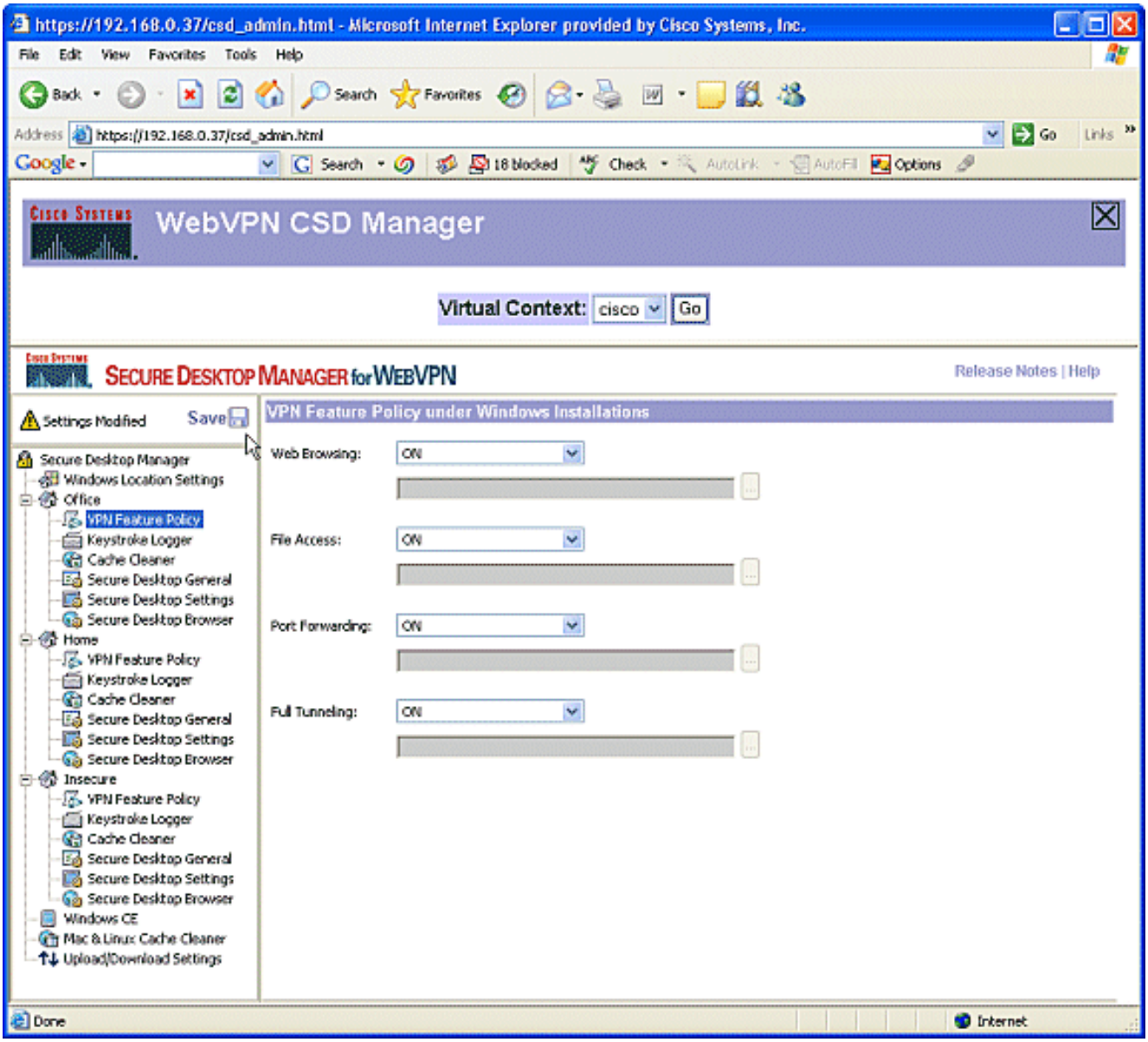
.



2단계:3단계:Windows 위치 모듈 및 기능을 구성합니다.

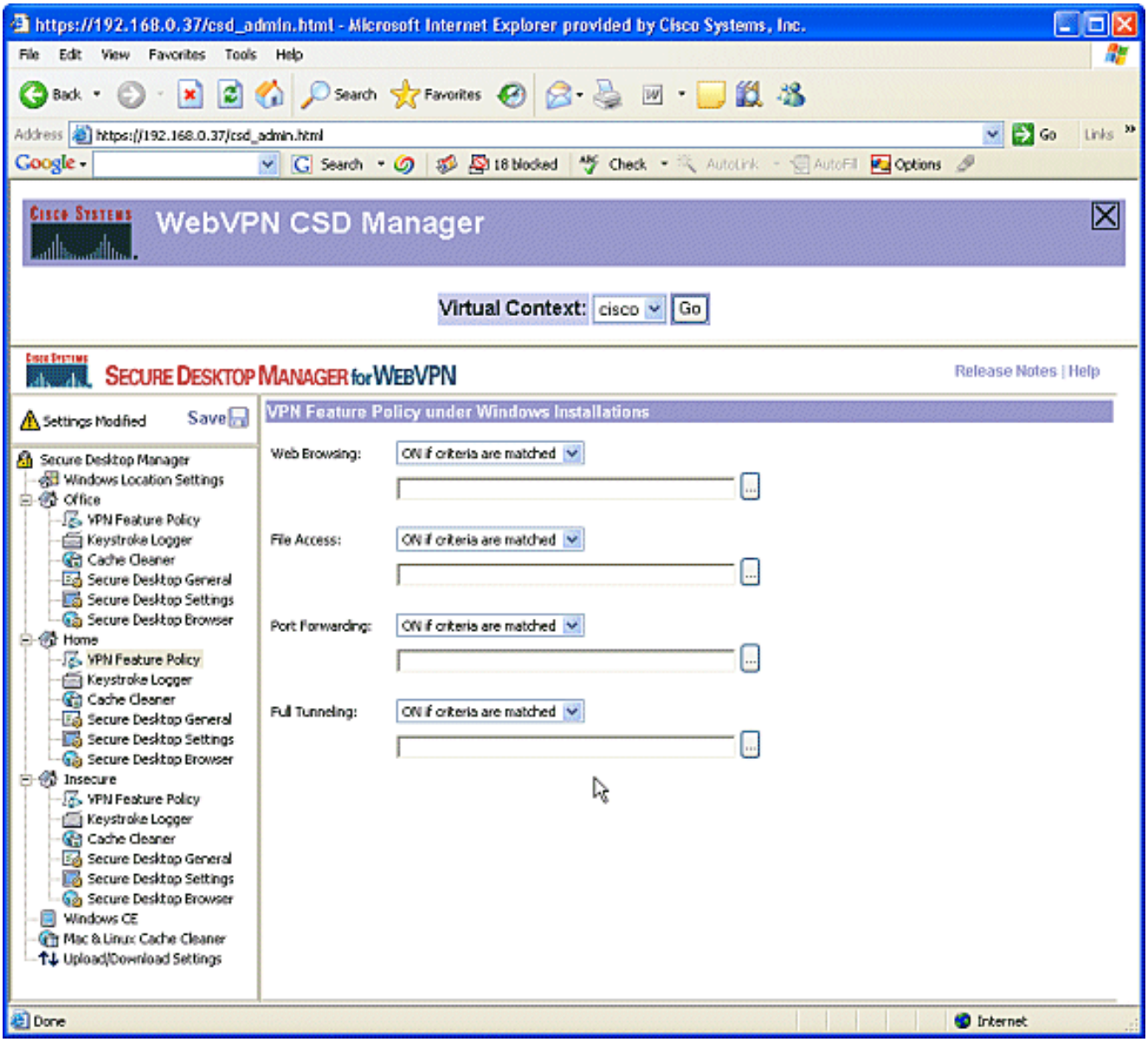
각 Windows 위치에 대해 CSD 기능을 구성합니다.

1. **Office**에서 **VPN Feature Policy(VPN 기능 정책)를 클릭합니다**.이러한 클라이언트는 신뢰할 수 있는 내부 클라이언트이므로 CSD 및 캐시 클리너가 활성화되지 않았습니다.다른 매개 변수는 사용할 수 없습니다
.



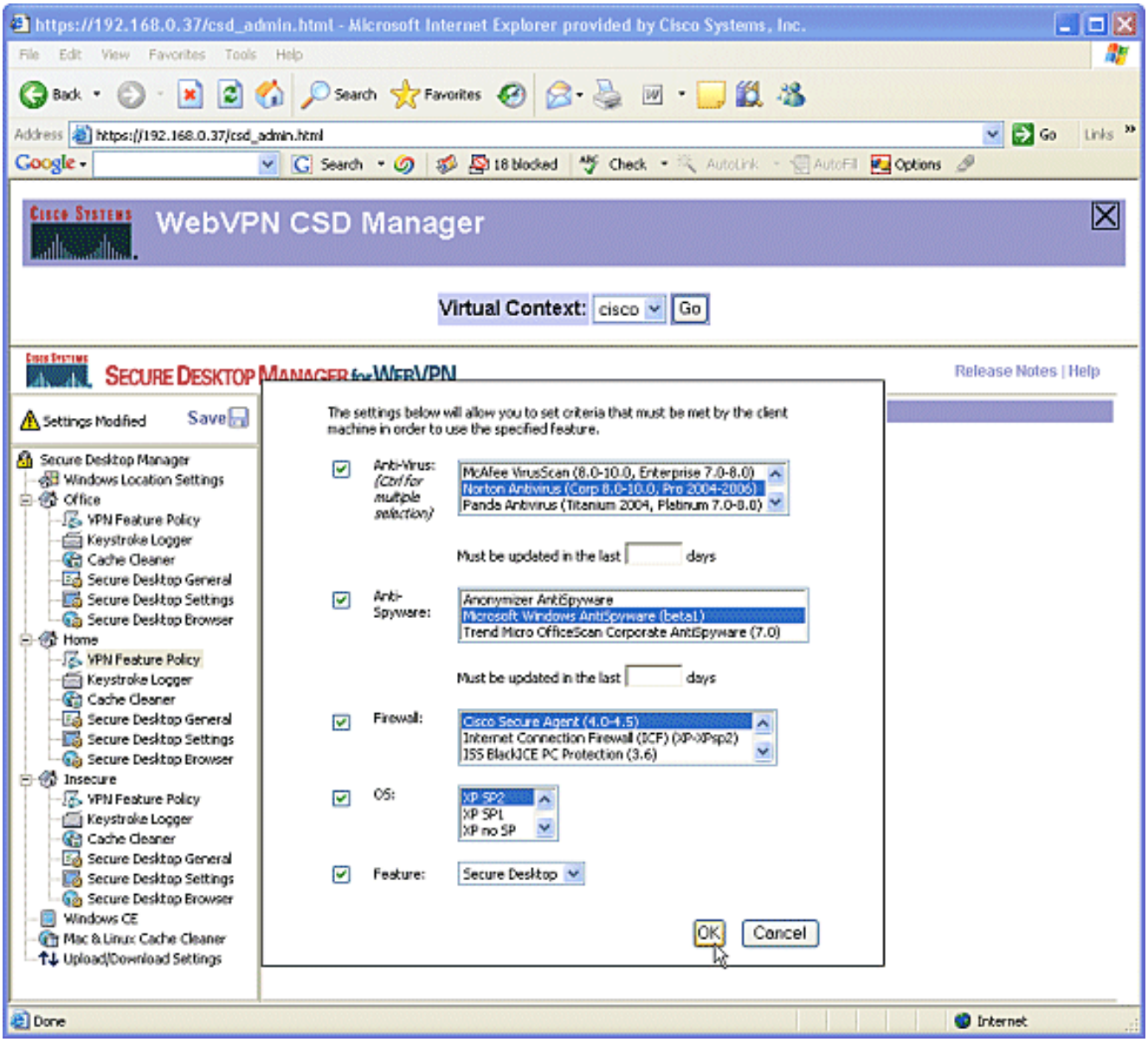
2. 표시된 대로 기능을 설정합니다.왼쪽 창의 **Home** 아래에서 **VPN Feature Policy**를 선택합니다.클라이언트가 특정 기준을 충족하면 가정 사용자가 기업 LAN에 액세스할 수 있습니다.각 액세스 방법 아래에서 **기준이 일치하면 ON을** 선택합니다

.



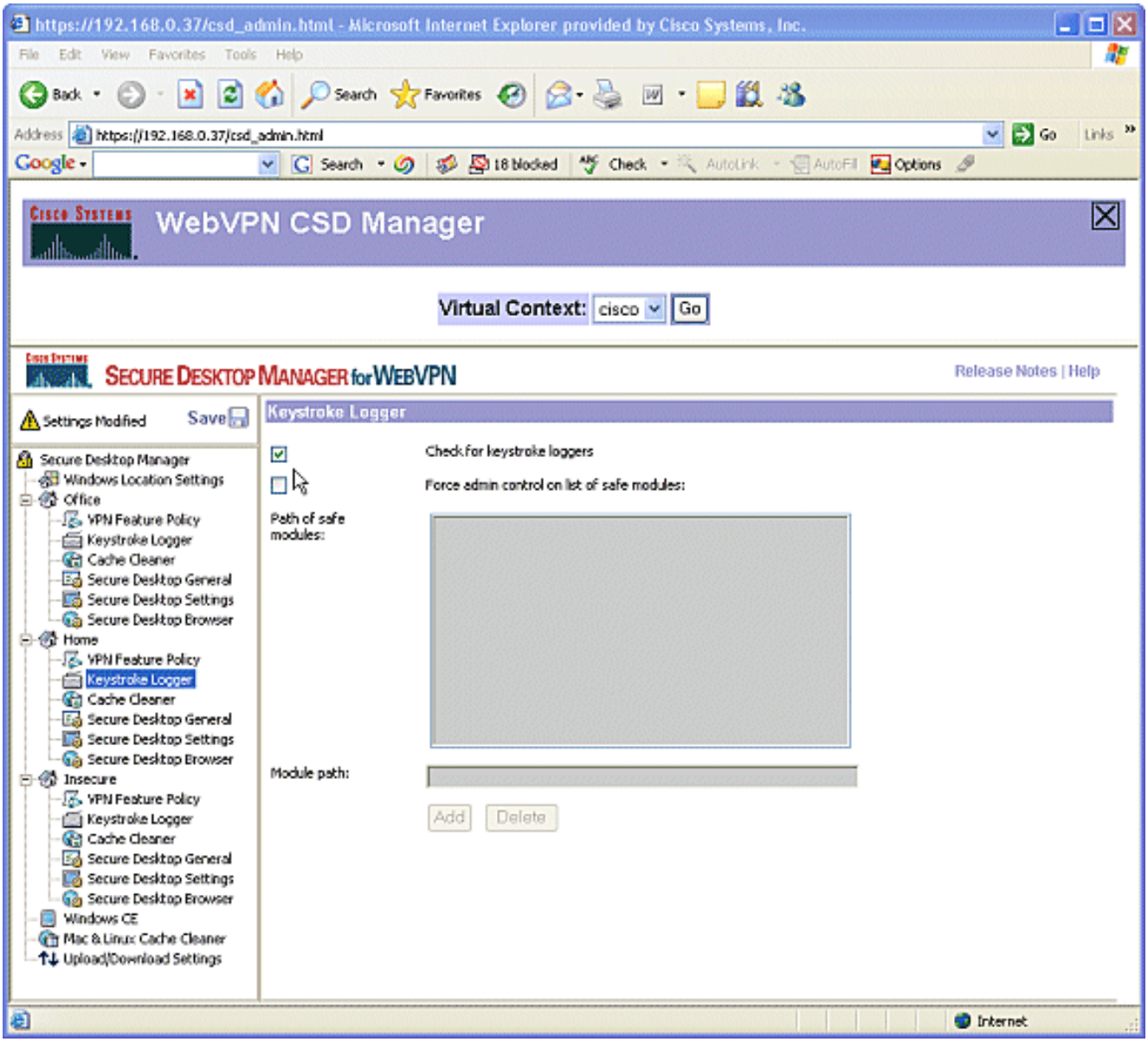
3. 웹 브라우징의 경우 줄임표 단추를 클릭하고 일치해야 하는 기준을 선택합니다.대화 상자에서 OK를 클릭합니다

.

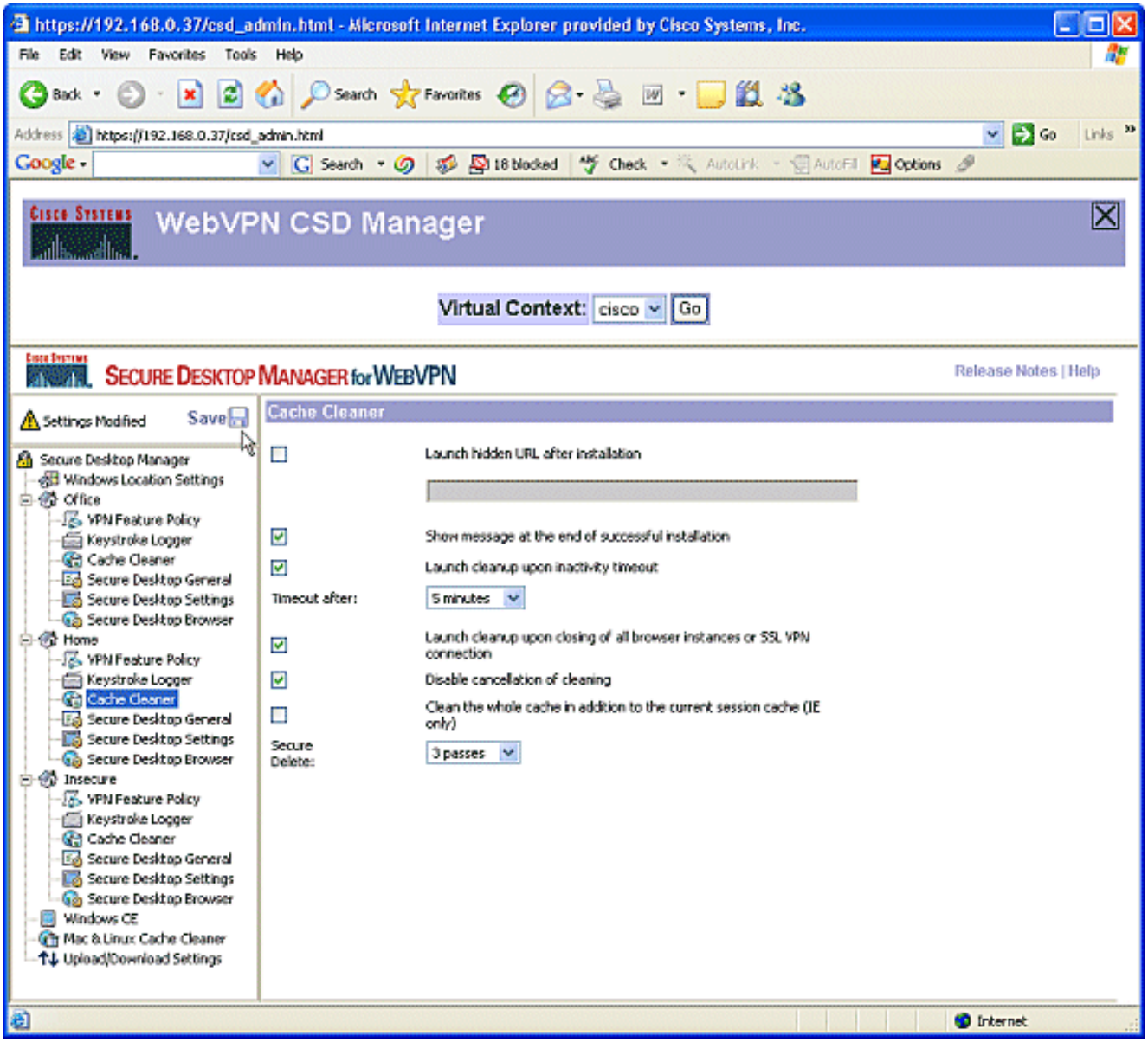


4. 유사한 방식으로 다른 액세스 방법을 구성할 수 있습니다.**홈에서** 키 입력 **로거를 선택합니다** .Check for keystroke loggers(키스트로크 로거 **확인)** 옆에 체크 **표시를 합니다**.메시지가 나타나면 **Save**(저장)를 클릭하고 **OK(확인)**를 클릭합니다

.

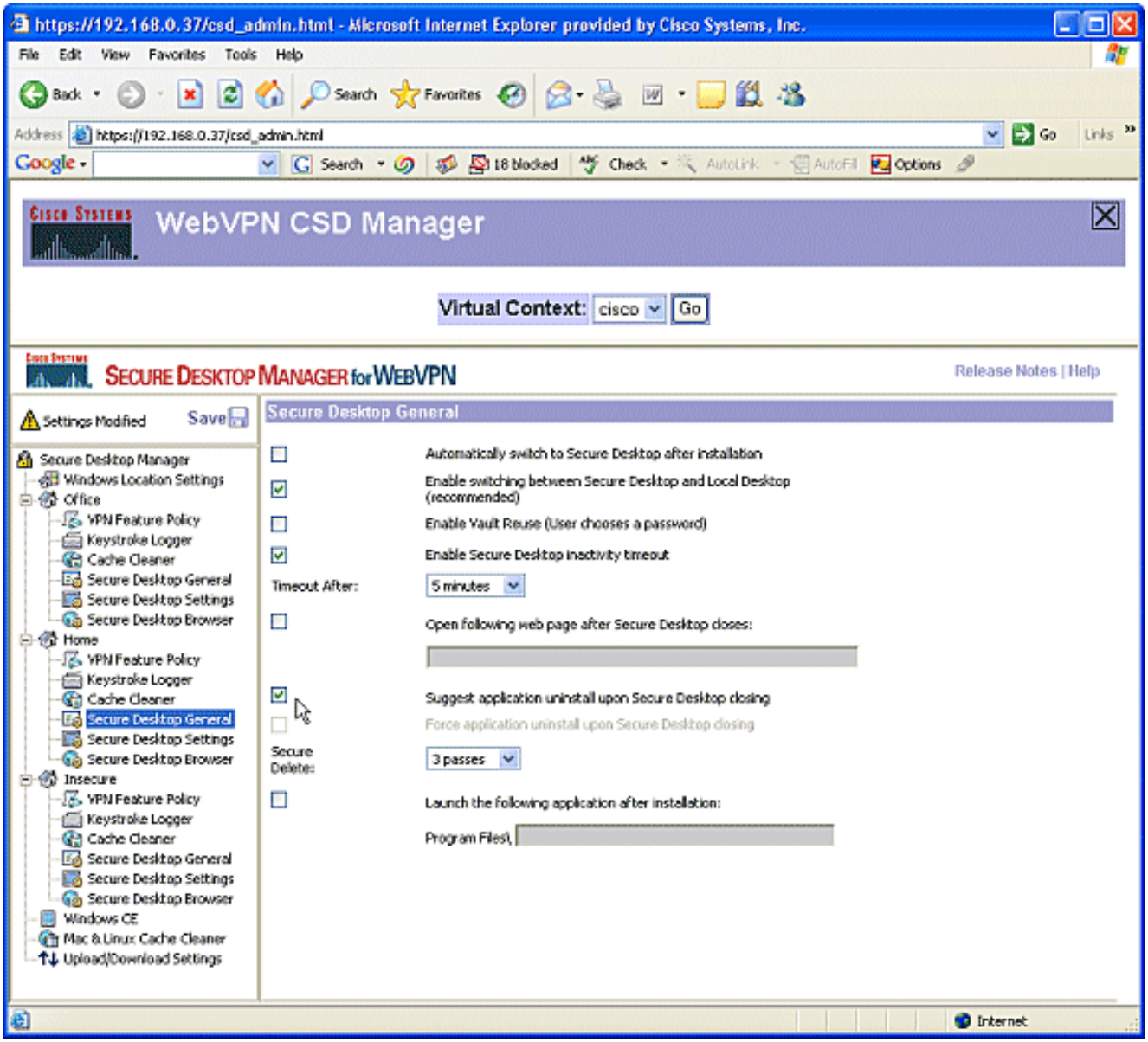


5. 홈 창 위치 아래에서 **캐시 클리너**를 선택합니다.스크린 샷과 같이 기본 설정을 유지합니다
.



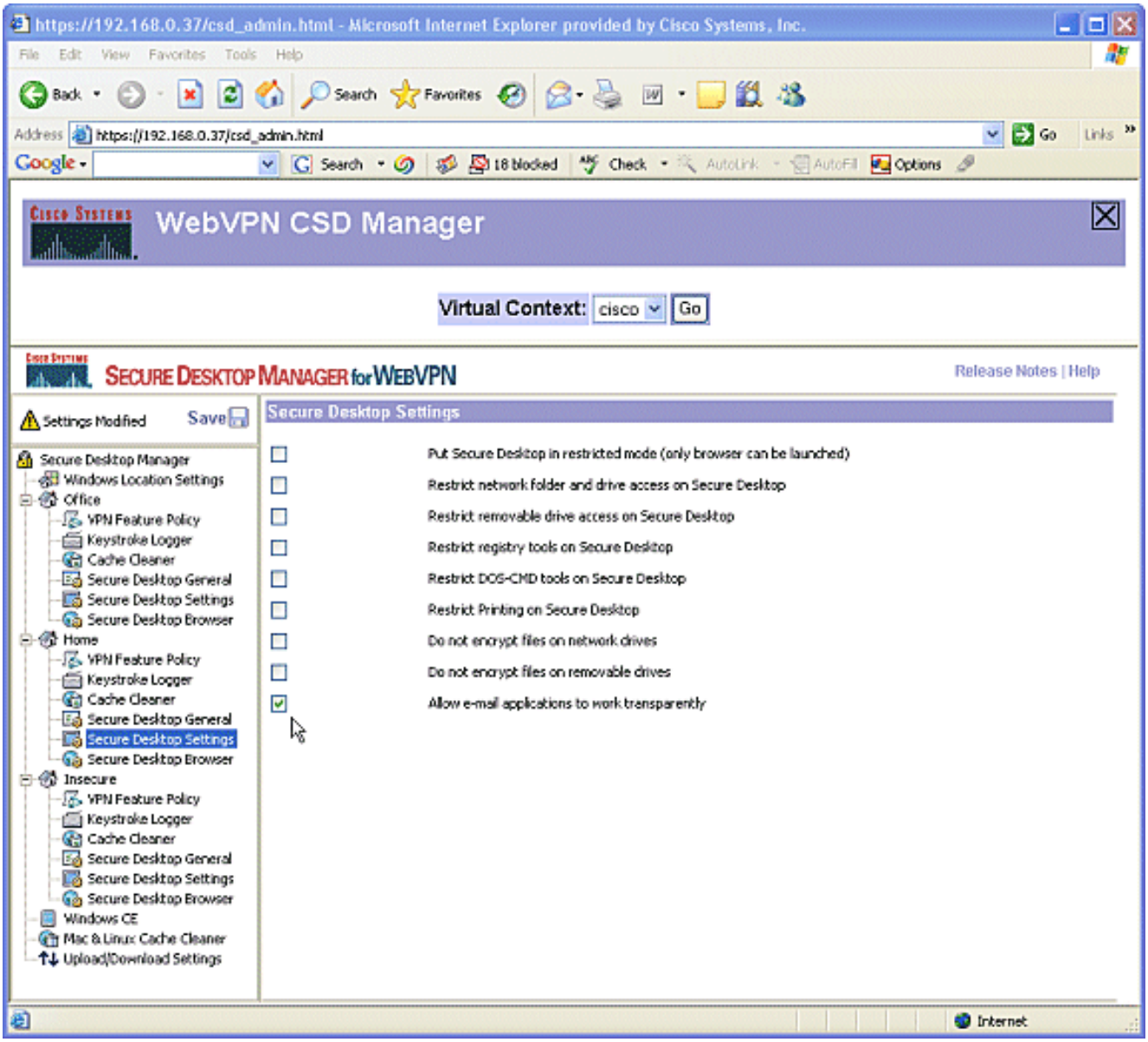
6. 홈에서 Secure **Desktop General을** 선택합니다.Secure **Desktop을 닫을 때 응용 프로그램 제거 제안 을 선택합니다**.다른 모든 매개 변수는 스크린 샷과 같이 기본 설정으로 둡니다

.



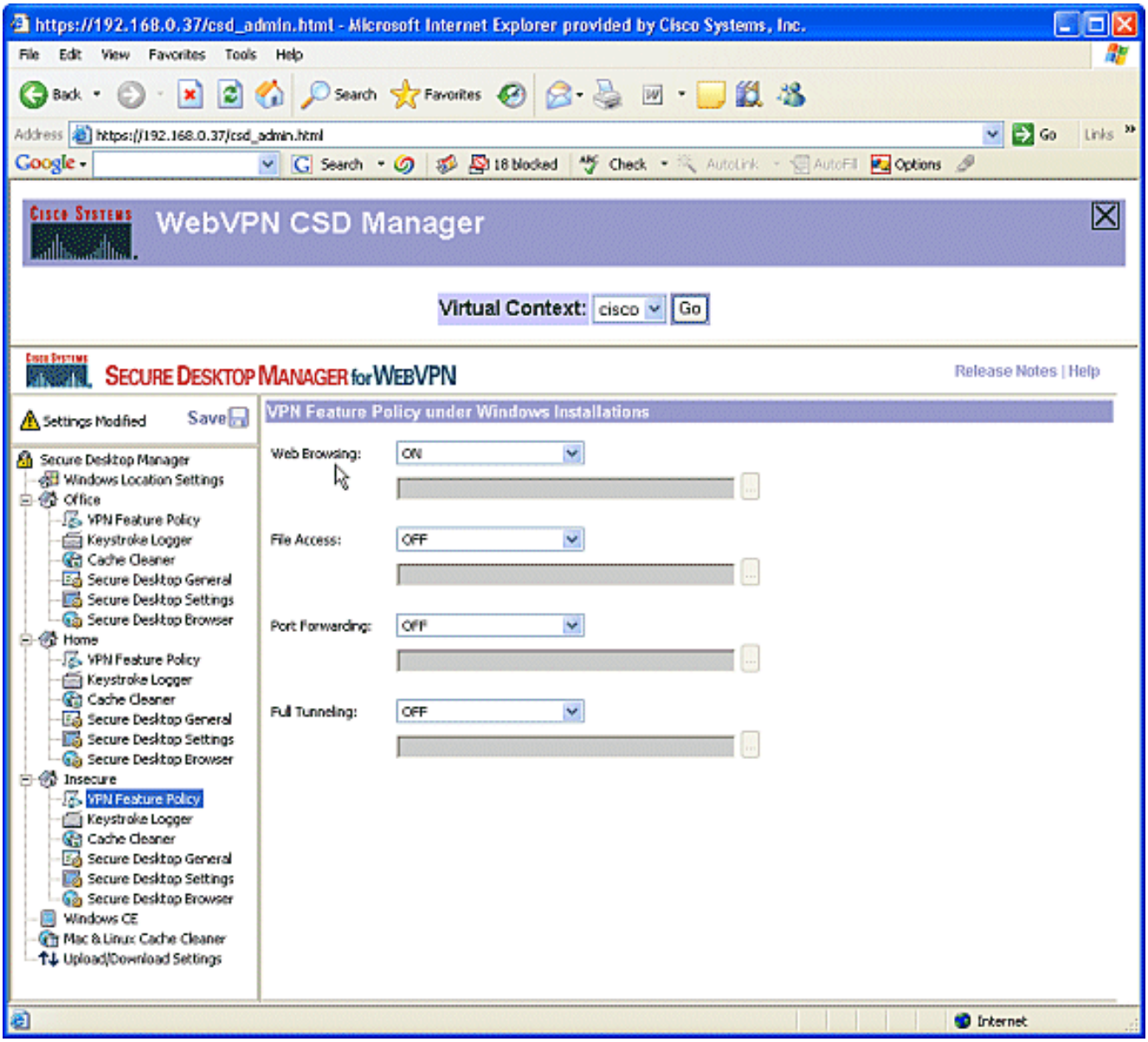
7. 홈 아래의 Secure Desktop Settings(보안 데스크톱 설정)에서 **Allow e-mail applications to work transparently(이메일 응용 프로그램이 투명하게 작동하도록 허용)**를 선택합니다.메시지가 나타나면 **Save**(저장)를 클릭하고 **OK(확인)**를 클릭합니다

.

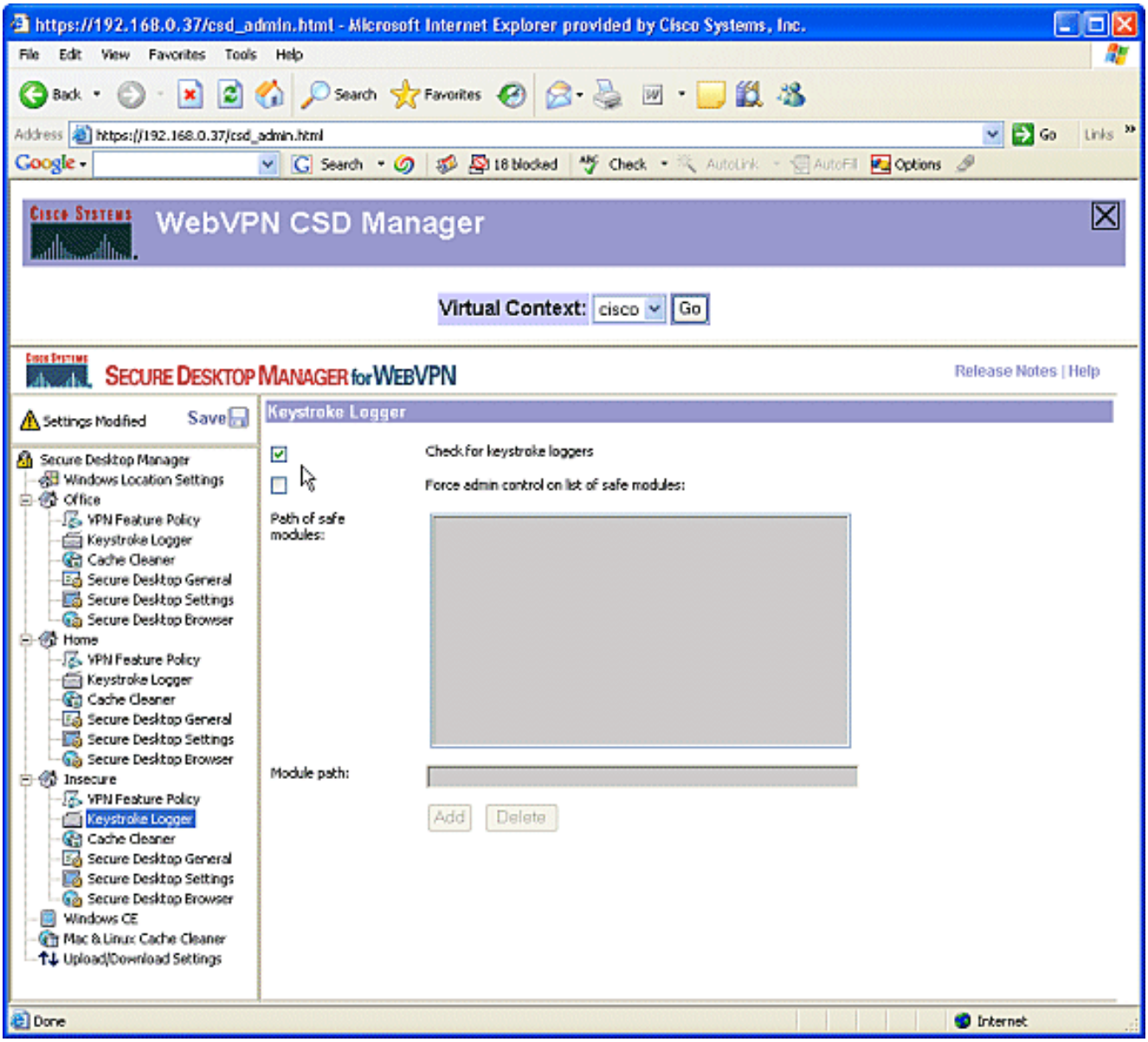


8. **Secure Desktop Browser**의 컨피그레이션은 이러한 사용자가 사전 구성된 즐겨찾기로 회사 웹 사이트에 액세스하도록 할지 여부에 따라 달라집니다.Insecure(비보안)에서 **VPN Feature Policy(VPN 기능 정책)를** 선택합니다.신뢰할 수 있는 사용자가 아니므로 웹 검색만 허용합니다.**웹 브라우징**을 위해 드롭다운 메뉴에서 ON을 선택합니다.다른 모든 액세스는 OFF로 **설정됩니다**

.

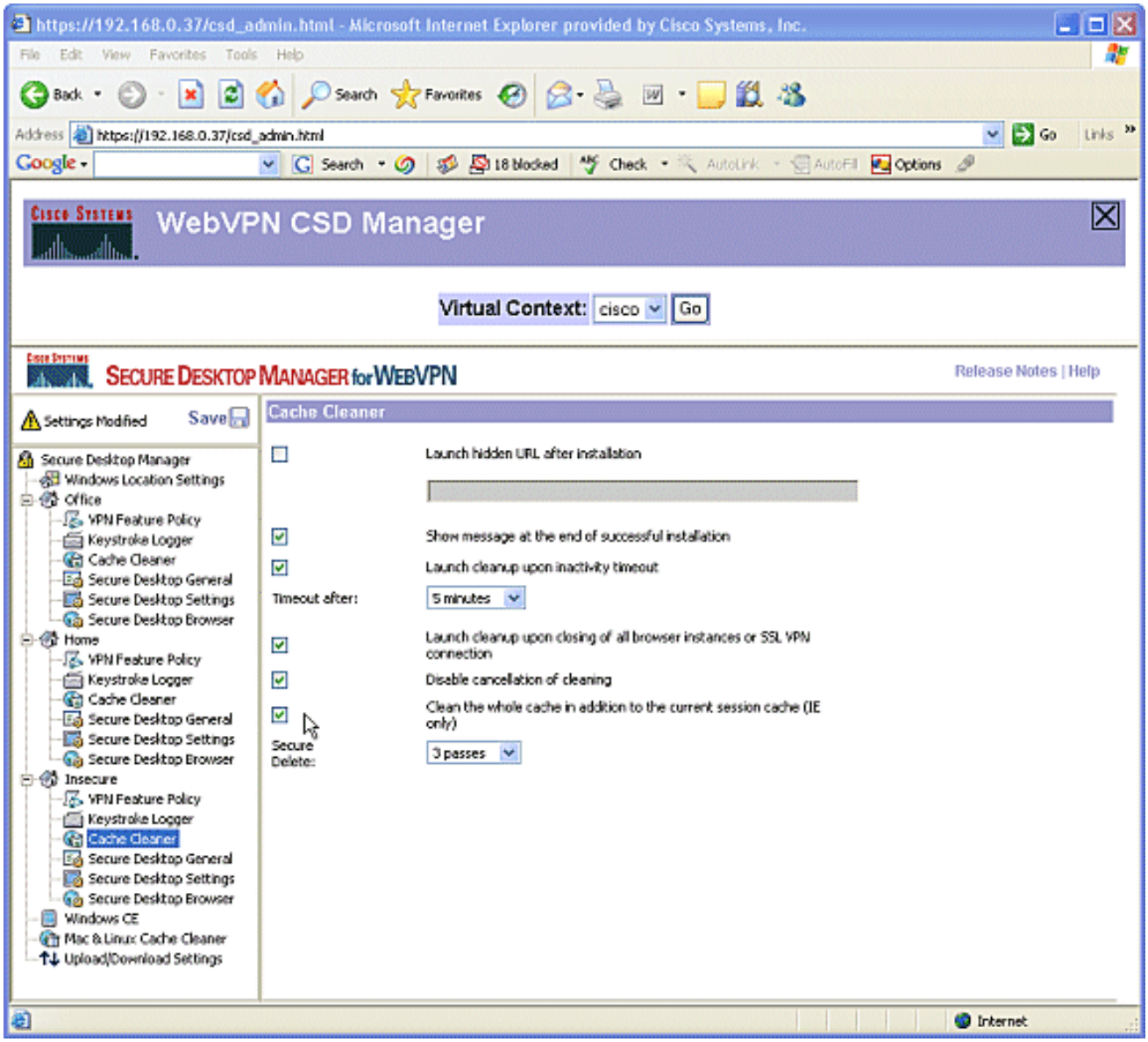


9. Check for keystroke loggers(**키스트로크 로거 확인**) 확인란을 선택합니다
.



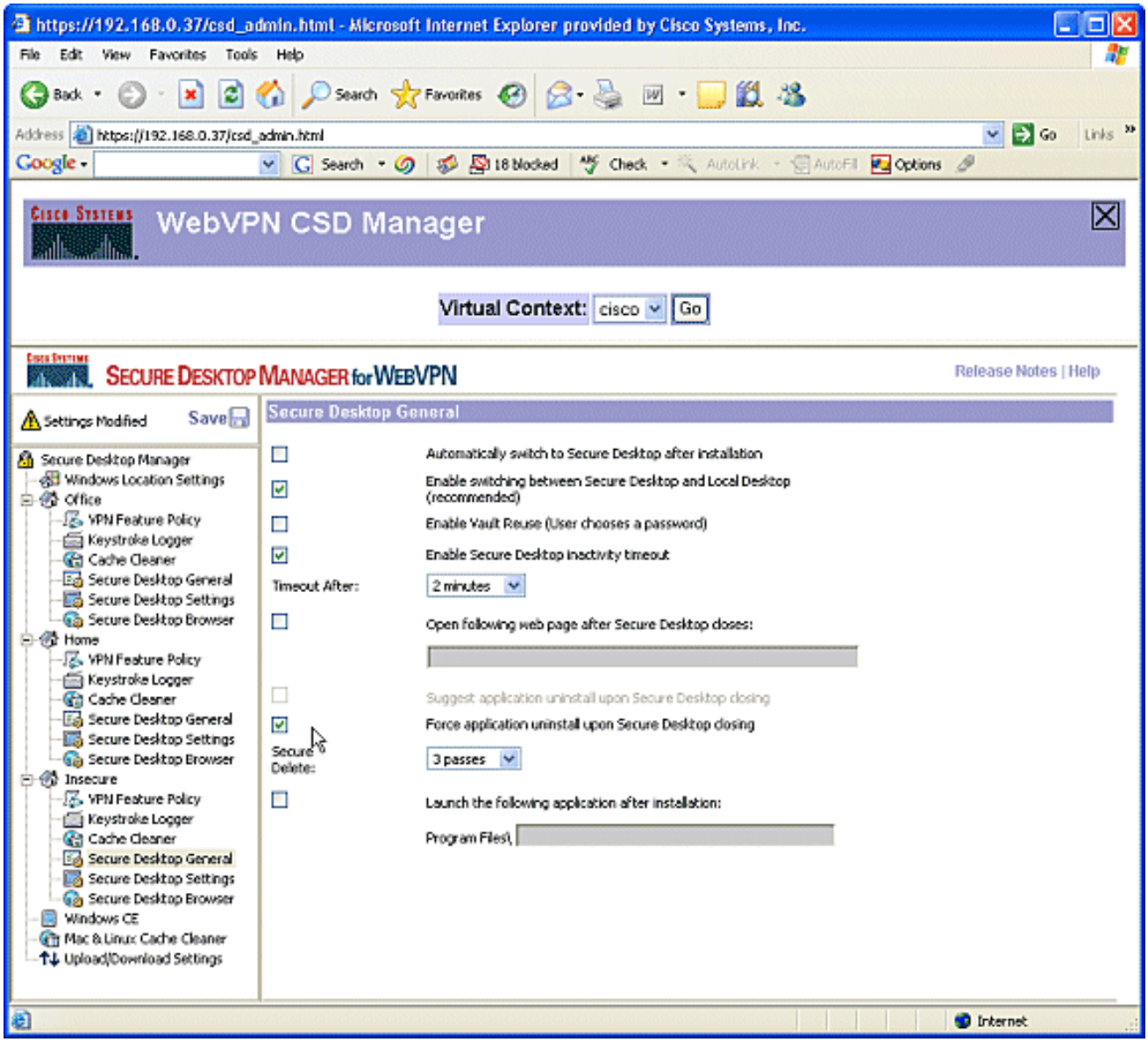
10. 안전하지 않은 캐시 클리너를 구성합니다.**현재 세션 캐시(IE만 해당) 외에 전체 캐시 지우기** 확인란을 선택합니다.다른 설정은 기본값으로 둡니다

.



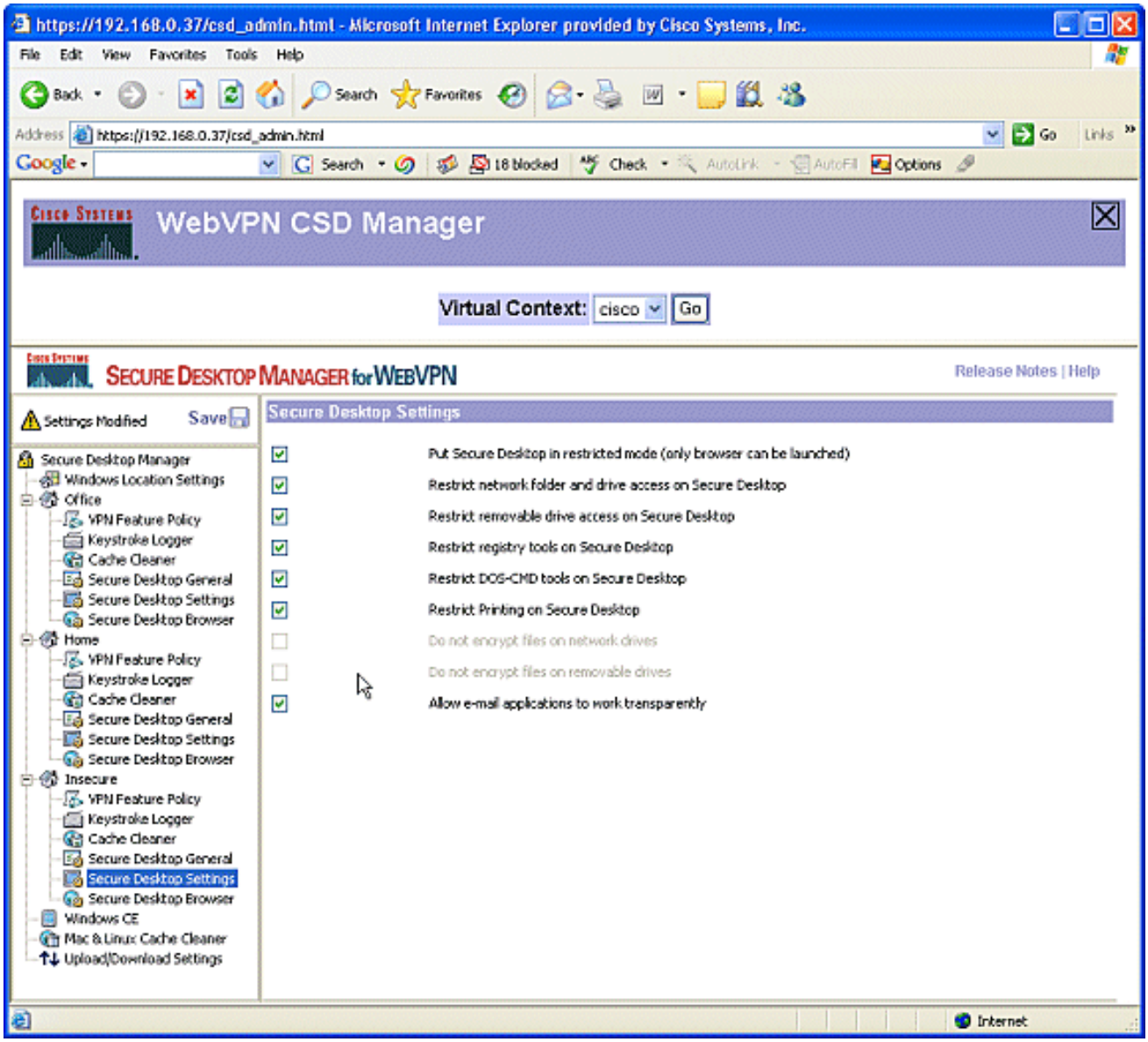
11. Unsecure Desktop(비보안)에서 Secure **Desktop General(보안 데스크톱 일반)을 선택합니다**.시간 제한 비활성화 시간을 2분으로 줄입니다.Secure **Desktop 닫기 시 응용 프로그램 제거 강제** 확인란을 선택합니다

.



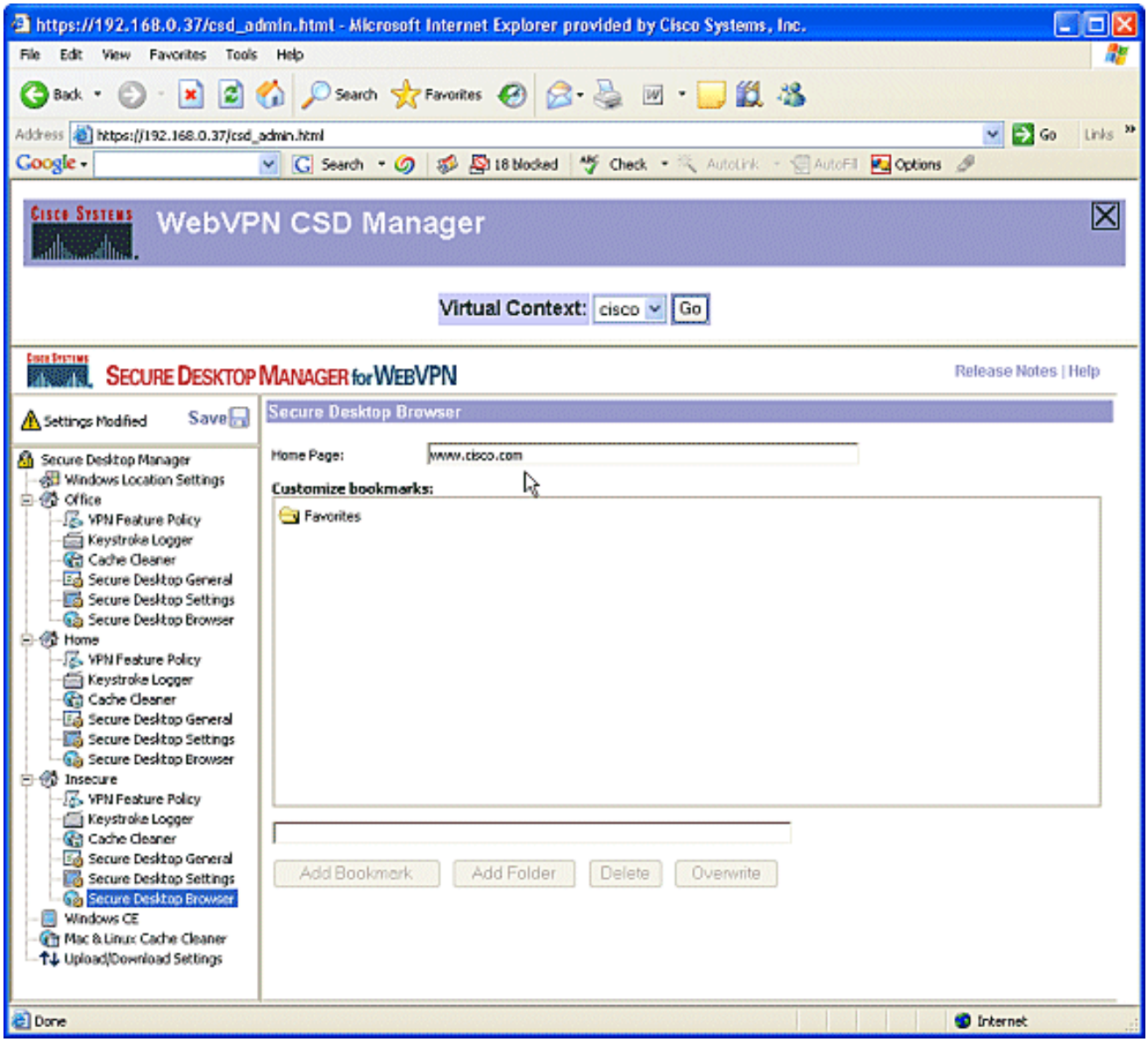
12. Secure **Desktop Settings(보안 데스크톱 설정)**를 Unsecure Secure Desktop Settings(비보안 설정)에서 선택하고 표시된 대로 매우 제한적인 설정을 구성합니다

.



13. Secure **Desktop Browser를 선택합니다**.Home Page(홈 페이지) 필드에 이러한 클라이언트가 홈 페이지에 대해 안내될 웹 사이트를 입력합니다

.



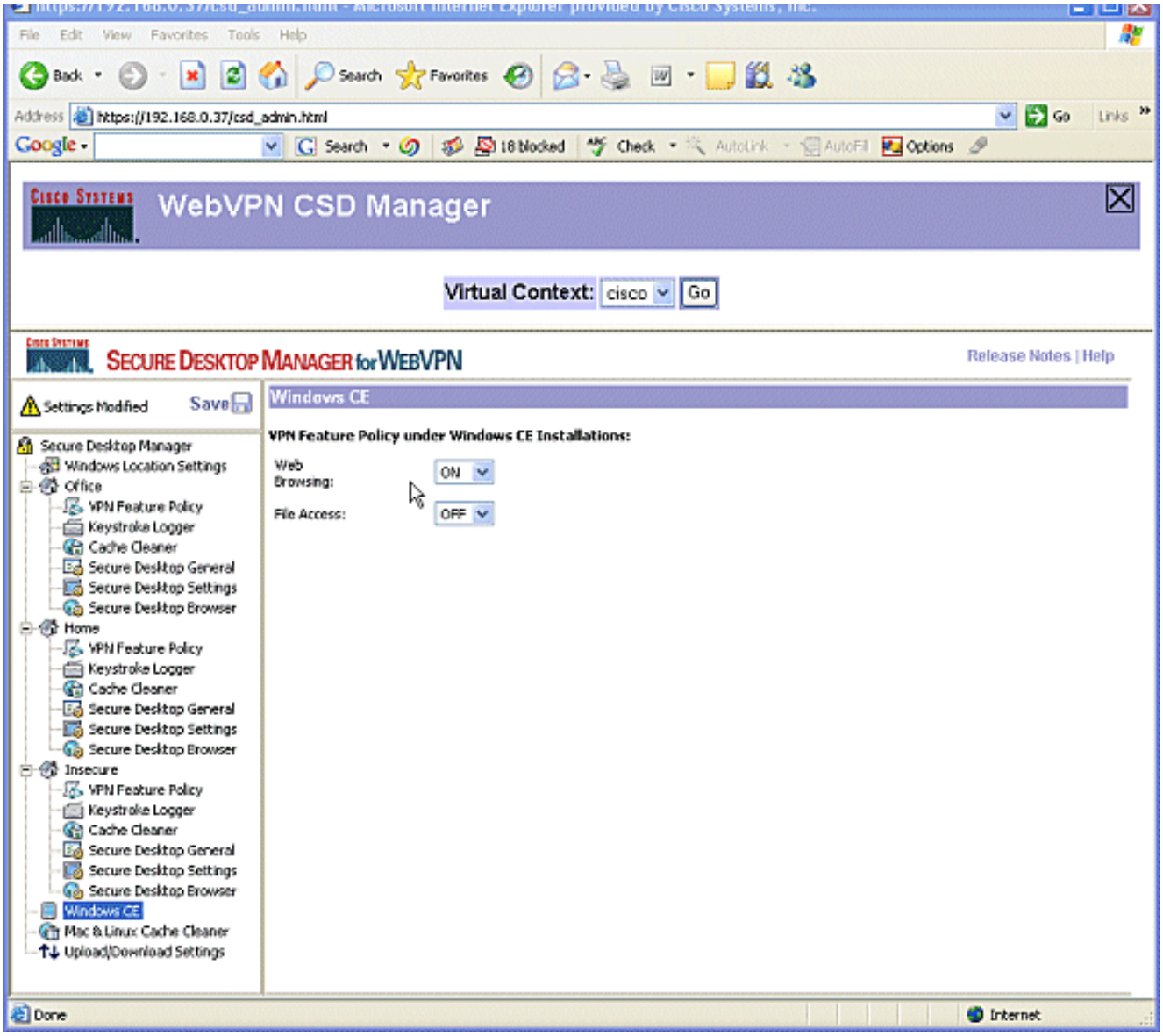
2단계:4단계:Windows CE, Macintosh 및 Linux 기능을 구성합니다

.

Windows CE, Macintosh 및 Linux용 CSD 기능을 구성합니다.

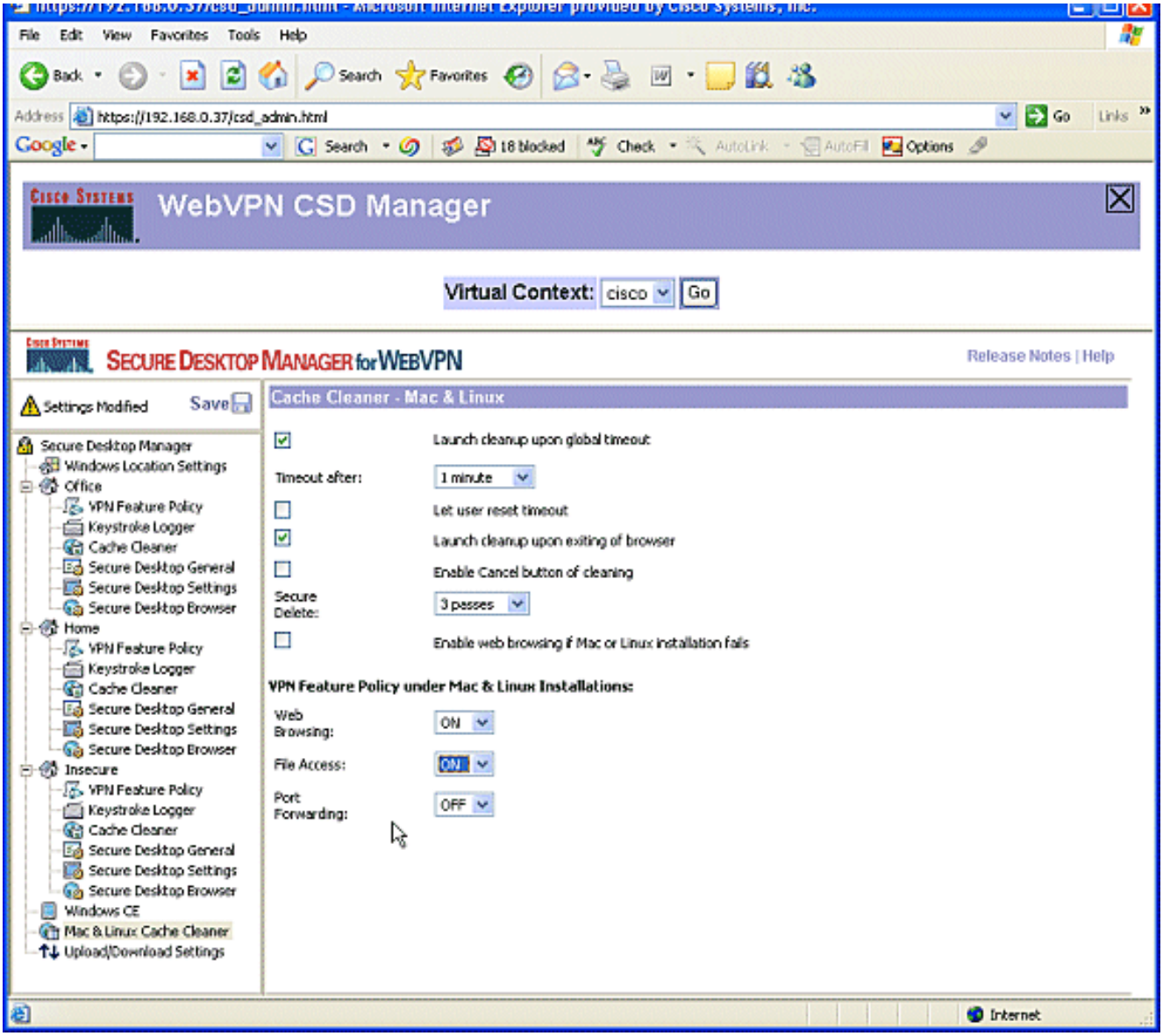
1. Secure Desktop Manager 아래에서 Windows CE를 선택합니다.Windows CE에는 제한된 VPN 기능이 있습니다.**웹 브라우징을 켜십시오**

   .



2. **Mac 및 Linux Cache Cleaner를 선택합니다**.Macintosh 및 Linux 운영 체제는 CSD의 캐시 클리너 측면에만 액세스할 수 있습니다.그림과 같이 구성합니다.메시지가 나타나면 **Save**(저장)를 클릭하고 **OK(확인)**를 클릭합니다

.

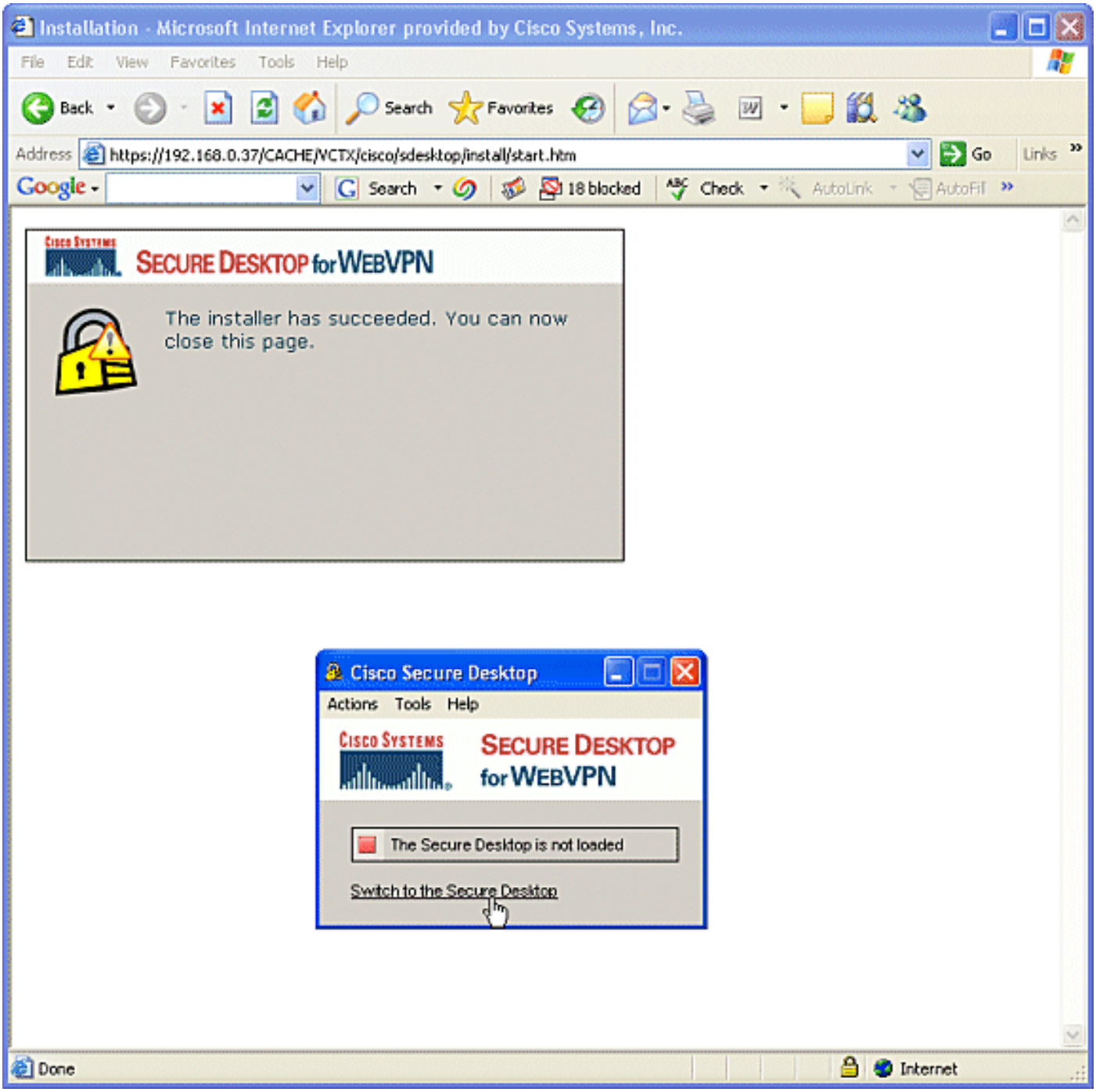


다음을 확인합니다.

CSD 작업 테스트

SSL이 활성화된 브라우저(https://WebVPN_Gateway_IP **주소**)를 사용하여 WebVPN 게이트웨이에 연결하여 CSD의 작동을 **테스트합니다**.

참고: 다른 WebVPN 컨텍스트를 생성한 경우(예: https://192.168.0.37/cisco)의 고유한 컨텍스트 이름을 사용해야 **합니다**.



명령

여러 **show** 명령이 WebVPN과 연결되어 있습니다.CLI(Command Line Interface)에서 이러한 명령을 실행하여 통계 및 기타 정보를 표시할 수 있습니다.**show 명령**에 대한 자세한 내용은 WebVPN 컨피그레이션 확인을 참조하십시오.

참고: CLI Analyzer(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.CLI Analyzer를 사용하여 **show** 명령 출력의 분석을 봅니다.

문제 해결

명령

여러 **디버그** 명령이 WebVPN과 연결됩니다.이러한 명령에 대한 자세한 내용은 WebVPN 디버그 명

령 사용을 참조하십시오.

참고: debug 명령을 사용하면 Cisco 디바이스에 부정적인 영향을 미칠 수 있습니다.debug 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

clear 명령에 대한 자세한 내용은 WebVPN Clear 명령 사용을 참조하십시오.

관련 정보

- WebVPN 및 DMVPN 통합 구축 설명서
- SSL VPN - WebVPN
- Cisco IOS SSLVPN
- 기술 지원 및 문서 – Cisco Systems