ASA Clientless SSL VPN(WebVPN) 문제 해결 기술 노트

목차

소개

이 문서에는 ASA 버전 7.1, 7.2 및 8.0에 대해 채택된 클라이언트리스 SSL VPN(WebVPN) 문제 해결 기술이 나열되어 있습니다. 이러한 릴리스 간에는 다양한 문제 해결 기술을 사용해야 하는 상당한 발전이 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 소프트웨어 버전 7.1 이상을 실행하는 Cisco 5500 Series ASA를 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

명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

문제 해결

ASA에서 클라이언트리스 SSL VPN 연결(WebVPN)을 트러블슈팅하기 위한 전제 조건은 스크린샷 및 HTML 캡처 툴을 통해 클라이언트 환경에 대한 가시성을 확보한 다음 액세스 중인 URL/애플리케이션에 직접 연결할 때 동일한 정보와 비교해야 합니다.

ASA 버전 7.1/7.2 클라이언트리스

이 섹션에서는 ASA 버전 7.1/7.2 및 8.0 릴리스까지는 포함하되 포함하지 않는 모든 인터페이스의 트러블슈팅 기술에 대해 설명합니다.

이 릴리스에서는 복잡한 Java/Javascript 기능에 문제가 있는 경우 애플리케이션 액세스 포트 포워딩 또는 프록시 우회 사용과 같은 다른 옵션이 고려될 수 있습니다. 이러한 대체 방법에 대한 자세한 내용은 애플리케이션 액세스 구성 및 프록시 우회 사용을 참조하십시오.

대부분의 경우 클라이언트리스 SSL VPN을 통해 액세스하는 URL이 Internet Explorer에 대해 실패하면 다른 브라우저에서도 실패합니다.

클라이언트 PC 또는 운영 체제에 종속되지 않도록 하려면 다른 위치에서 다른 클라이언트를 사용합니다. IPsec 또는 SSL VPN 클라이언트의 사용도 테스트할 수 있습니다.

WebVPN용 브라우저에서 쿠키 활성화에 설명된 대로 브라우저의 신뢰할 수 있는 영역에 ASA가 포함되어 있고 쿠키가 Enable Cookies(쿠키 활성화)에 설명된 대로 활성화되어 있는지 확인합니다.

프로세스가 계속 실패하면 필요한 정보를 수집하기 위해 다음 단계를 완료한 다음 TAC 케이스를 엽니다.

1. 브라우저 캐시 지우기에 설명된 대로 브라우저 캐시를 지웁니다.
2. Java 캐시 지우기에 설명된 대로 Java 캐시를 지웁니다.
3. 캐싱 구성에 설명된 대로 ASA에서 WebVPN 캐시를 비활성화합니다.
4. Java 애플릿이 있는 경우 Enable Java Applet Debugging Options(Java 애플릿 디버깅 옵션 활성화)에 설명된 대로 애플릿 창에서 디버그 레벨 5를 사용합니다.
5. 클라이언트리스 SSL VPN을 통해 ASA에 로그인합니다.
6. 문제가 되는 URL 바로 앞의 URL에서 HTML 캡처 도구 사용에 설명된 대로 브라우저에서 HTML 캡처 도구를 활성화합니다.
7. 이 지점에서 문제가 있는 URL로 시퀀스를 캡처합니다.
8. 스크린샷**을 캡처하려면** 키보드에서 Ctrl+Print Screen을 누릅니다.
9. HTML 캡처 도구를 중지합니다.
10. ASA를 통해 IPsec 또는 SSL VPN 세션을 통해 URL에 직접 연결하거나 동일한 LAN 세그먼트에 직접 연결하고(가능한 경우) 분석을 위해 데이터를 TAC에 보낼 때 동일한 단계 1~9를 수행합니다.

ASA 버전 8.0 클라이언트리스

이 섹션에서는 ASA 버전 8.0 및 모든 인터페이스에 사용되는 트러블슈팅 기술에 대해 설명합니다.

이 릴리스에서는 클라이언트리스 SSL VPN을 통해 복잡한 URL 또는 애플리케이션에 문제가 발생하는 경우 스마트 터널 사용과 같은 다른 옵션이 강력한 대안입니다. 스마트 터널에 대한 자세한 내용은 스마트 터널 액세스 구성을 참조하십시오.

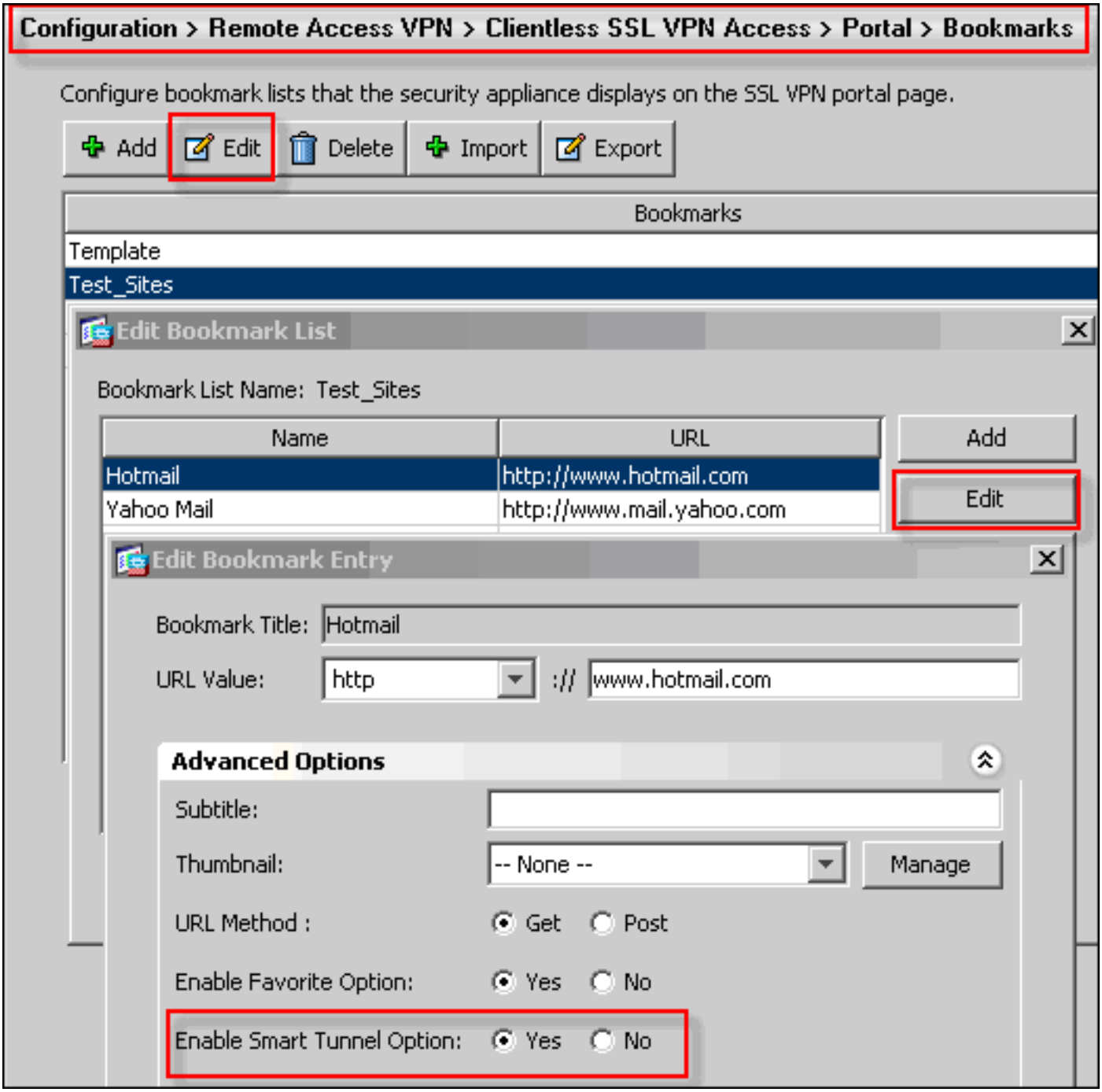
애플리케이션 액세스 포트 전달 또는 프록시 우회 사용을 고려할 수도 있습니다. 이러한 대체 방법에 대한 자세한 내용은 애플리케이션 액세스 구성 및 프록시 우회 사용을 참조하십시오.

대부분의 경우 클라이언트리스 SSL VPN을 통해 액세스하는 URL이 Internet Explorer에 대해 실패하면 다른 브라우저에서도 실패합니다.

클라이언트 PC 또는 운영 체제에 종속되지 않도록 하려면 다른 위치에서 다른 클라이언트를 사용합니다. IPsec 또는 SSL VPN 클라이언트의 사용도 테스트할 수 있습니다.

WebVPN용 브라우저에서 쿠키 활성화에 설명된 대로 브라우저의 신뢰할 수 있는 영역에 ASA가 포함되어 있고 쿠키가 Enable Cookies(쿠키 활성화)에 설명된 대로 활성화되어 있는지 확인합니다.

애플리케이션에서 클라이언트리스 콘텐츠 변환 엔진(CTE/rewriter)에 문제가 발생하는 경우 이 이미지에 표시된 대로 스마트 터널 옵션을 활성화하기 위해 해당 애플리케이션에 대한 책갈피를 수정할 수 있습니다.



북마크에 대해 이 옵션을 활성화할 경우 추가 컨피그레이션이 필요하지 않습니다. 포트 전달과 마찬가지로, 스마트 터널을 사용하여 애플리케이션 트래픽을 전달하고 재작성 문제를 방지하는 새 창을 열기 위해 책갈피를 클릭하는 또 다른 편리한 옵션입니다.

TCP Winsock 32 애플리케이션(예: RDP)에 이 기능을 사용할 경우 관리자가 스마트 터널을 통해 사용할 프로세스를 식별해야 합니다. 예를 들어 RDP는 mstsc.exe 프로세스를 사용합니다. 이 프로세스에 대해 간단한 스마트 터널 항목을 생성할 수 있습니다.

더 복잡한 애플리케이션은 여러 프로세스를 생성할 수 있습니다. WebVPN Portal Page(WebVPN 포털 페이지)에서 Application **Access(애플리케이션 액세스)** 패널을 선택합니다. 로드되는 즉시 *허용된 애플리케이션* 목록이 네트워크의 프라이빗 측면에 연결할 수 있습니다.

프로세스가 계속 실패하면 필요한 정보를 수집하기 위해 다음 단계를 완료한 다음 TAC 케이스를 엽니다.

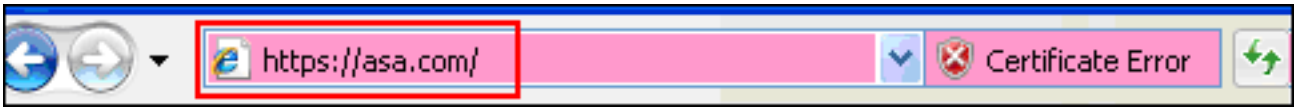
1. 브라우저 캐시 지우기에 설명된 대로 브라우저 캐시를 지웁니다.

2. Java 캐시 지우기에 설명된 대로 Java 캐시를 지웁니다.
3. 캐싱 구성에 설명된 대로 ASA에서 WebVPN 캐시를 비활성화합니다.
4. Java 애플릿이 있는 경우 Enable Java Applet Debugging Options(Java 애플릿 디버깅 옵션 활성화)에 설명된 대로 애플릿 창에서 디버그 레벨 5를 사용합니다.
5. 클라이언트리스 SSL VPN을 통해 ASA에 로그인합니다.
6. 문제가 되는 URL 바로 앞의 URL에서 HTML 캡처 도구 사용에 설명된 대로 브라우저에서 HTML 캡처 도구를 활성화합니다.
7. 이 지점에서 문제가 있는 URL로 시퀀스를 캡처합니다.
8. 스크린샷**을 캡처하려면** 키보드에서 Ctrl+Print Screen을 누릅니다.
9. HTML 캡처 도구를 중지합니다.
10. ASA를 통해 IPsec 또는 Any Connect SSL 세션을 통해 URL에 직접 연결하거나 동일한 LAN 세그먼트에 직접 연결할 경우(가능한 경우), 이 단계를 완료하고 분석을 위해 데이터를 TAC에 보낼 때 1~9단계를 수행합니다.

절차

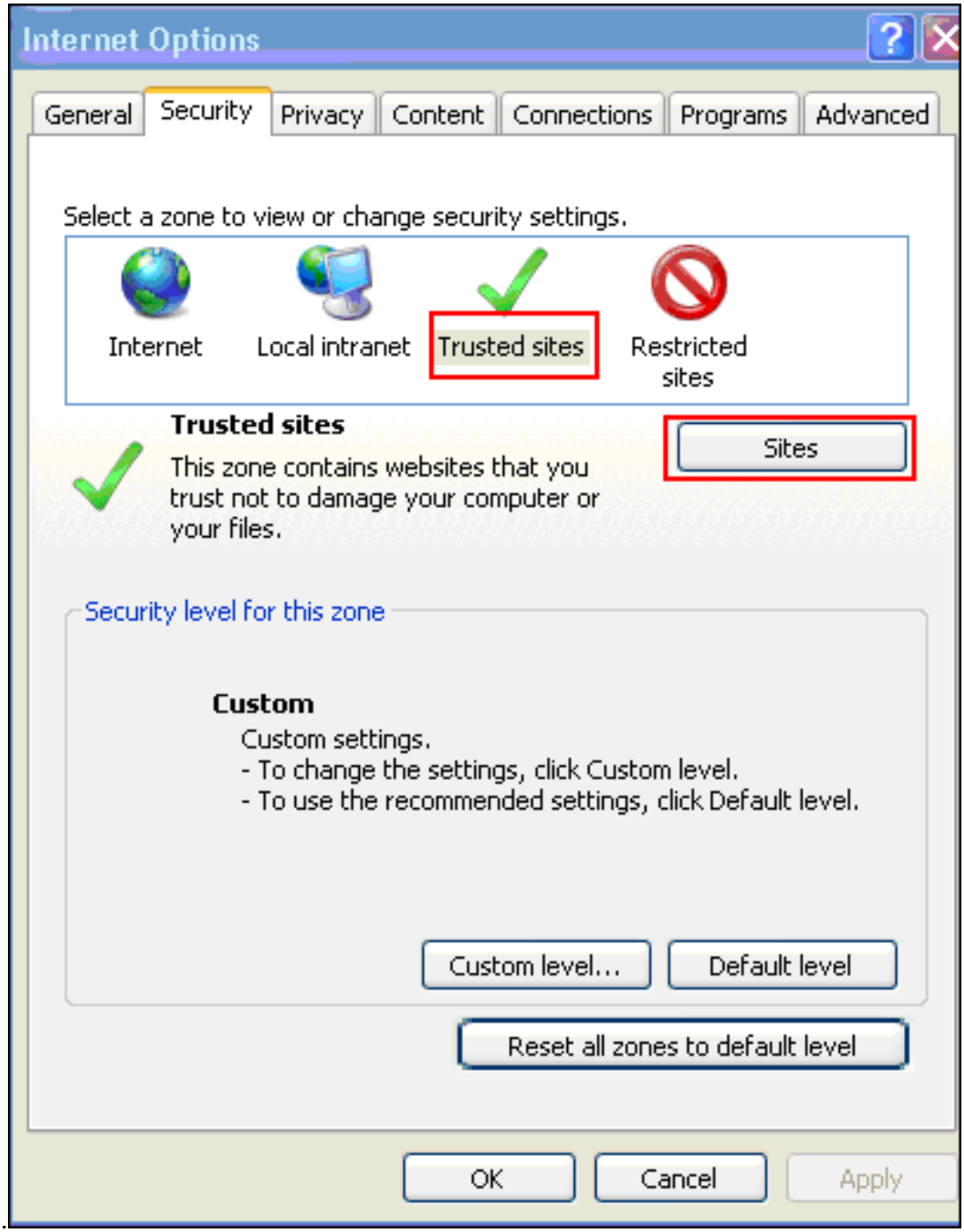
ASA를 신뢰할 수 있는 사이트로 추가

Internet Explorer에서 ASA에 액세스할 때 사이트가 신뢰할 수 있는 사이트로 포함되지 않은 경우 인증서 오류가 발생합니다.

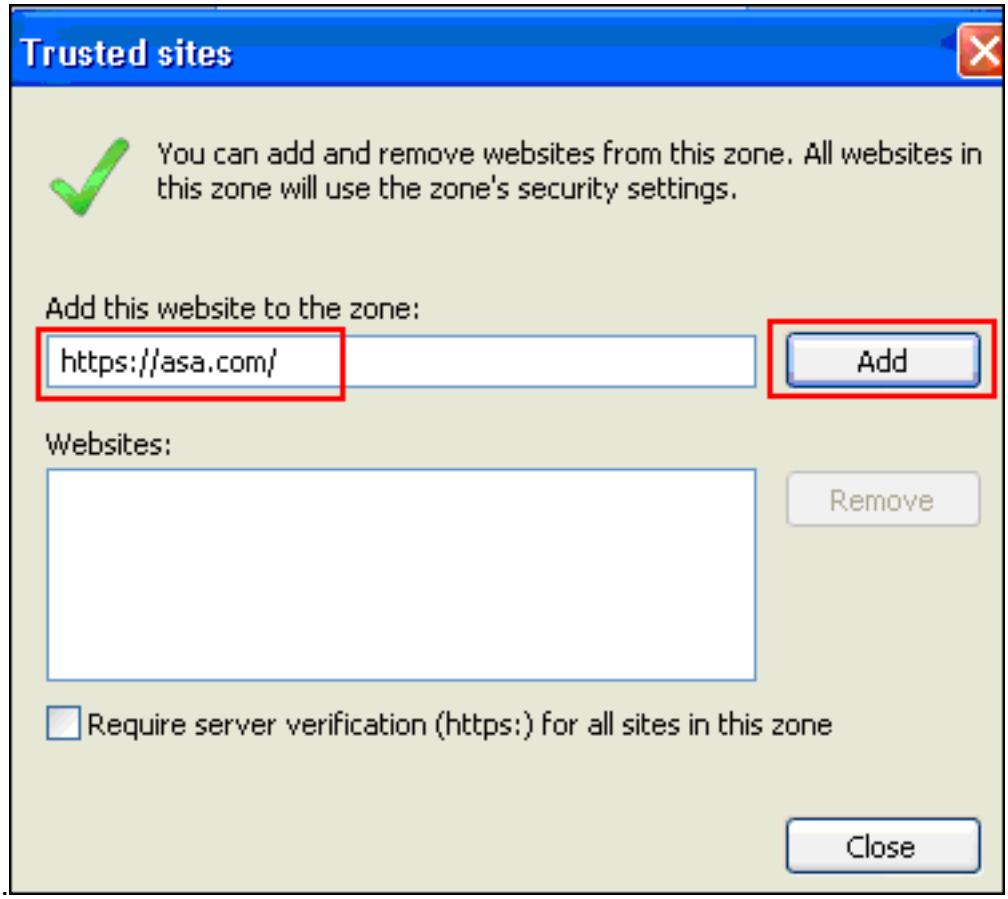


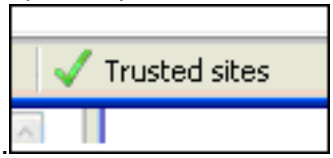
ASA를 신뢰할 수 있는 사이트로 추가하려면 다음 단계를 완료하십시오.

1. Internet Explorer에서 **도구 > 인터넷 옵션을** 선택합니다.
2. **보안** 탭을 클릭하고 신뢰할 수 있는 **사이트를 선택합니다**



3. Sites(**사이트)를 클릭합니다**.
4. ASA의 https:// 주소를 추가하고 Add를 **클릭합니다**



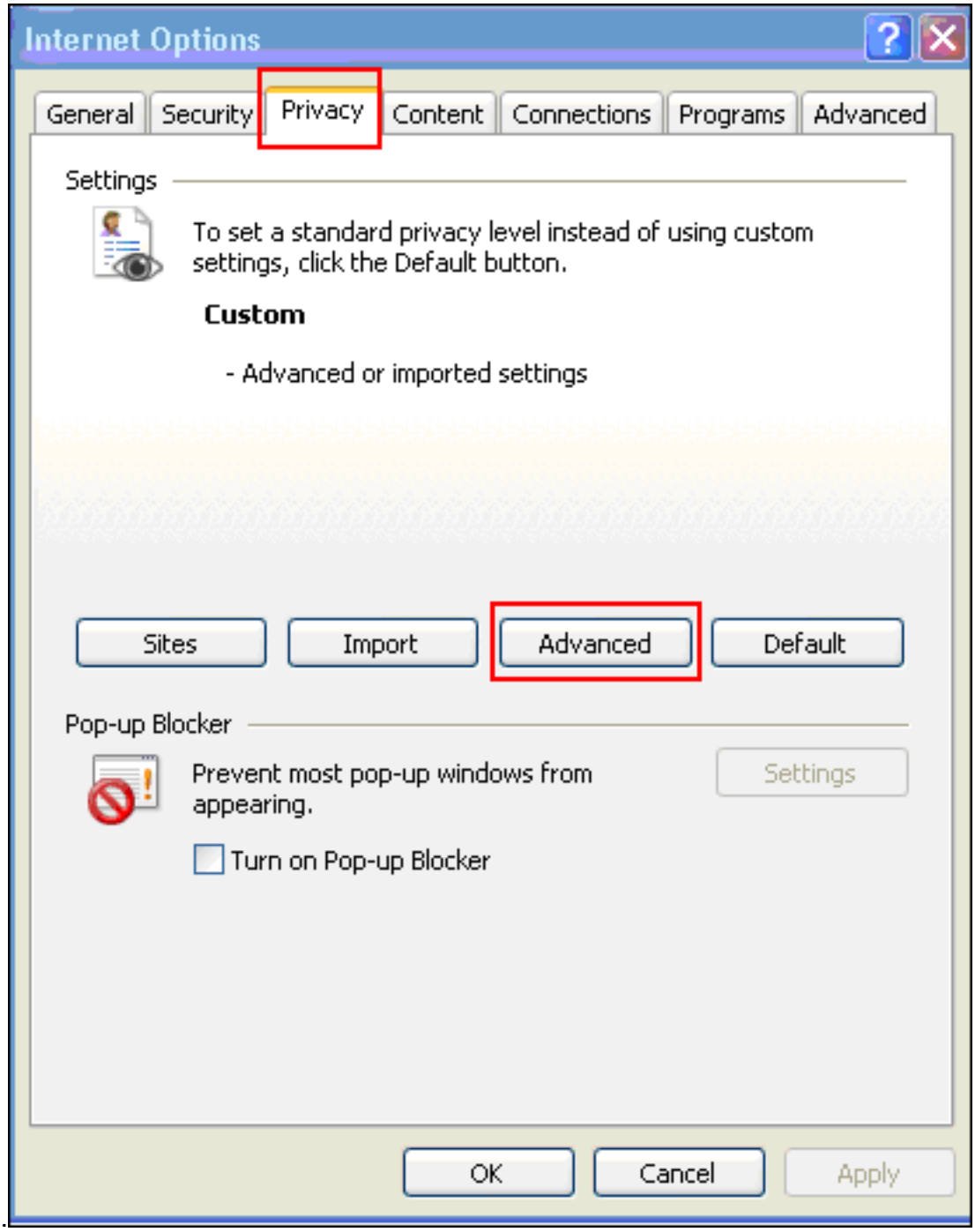
5. 사이트가 추가되면 Internet Explorer 상태 표시줄에 신뢰할 수 있는 사이트 아이콘이 나타납니다. 

참고: 이 절차에 대한 자세한 내용은 Internet Explorer 6 보안 설정 작업을 참조하십시오.

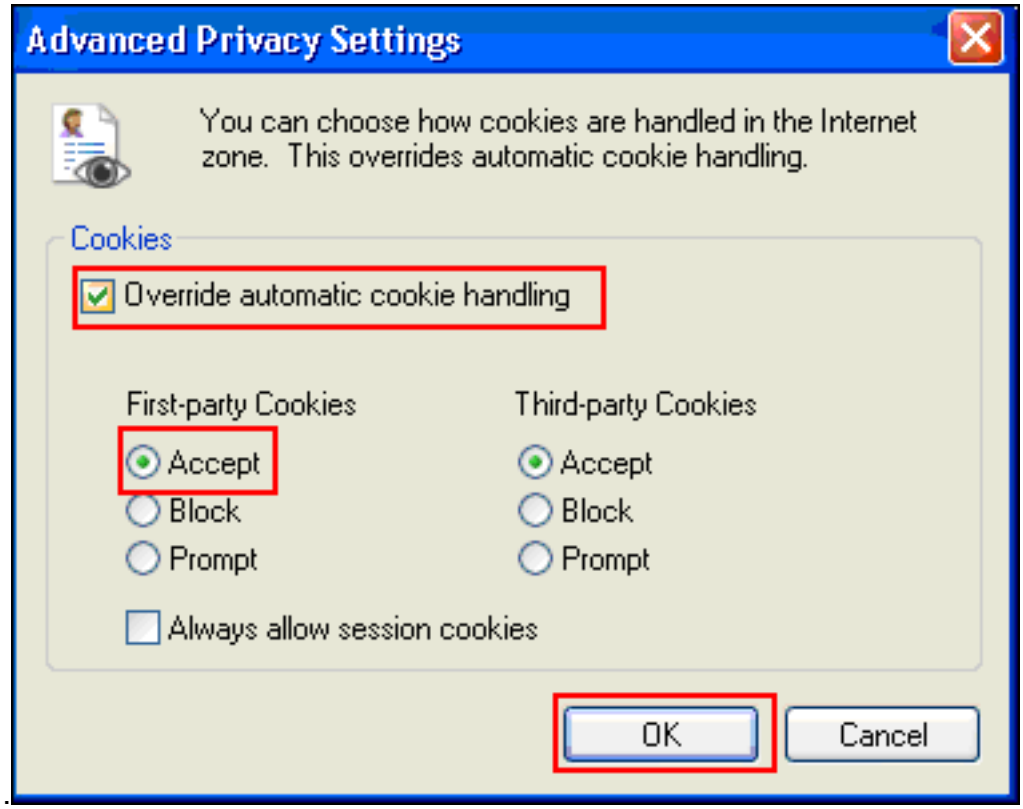
쿠키 사용

쿠키를 활성화하려면 다음 단계를 완료하십시오.

1. Internet Explorer에서 **도구 > 인터넷 옵션을** 선택합니다.
2. 개인 정보 탭을 클릭한 다음 **고급**을 클릭합니다



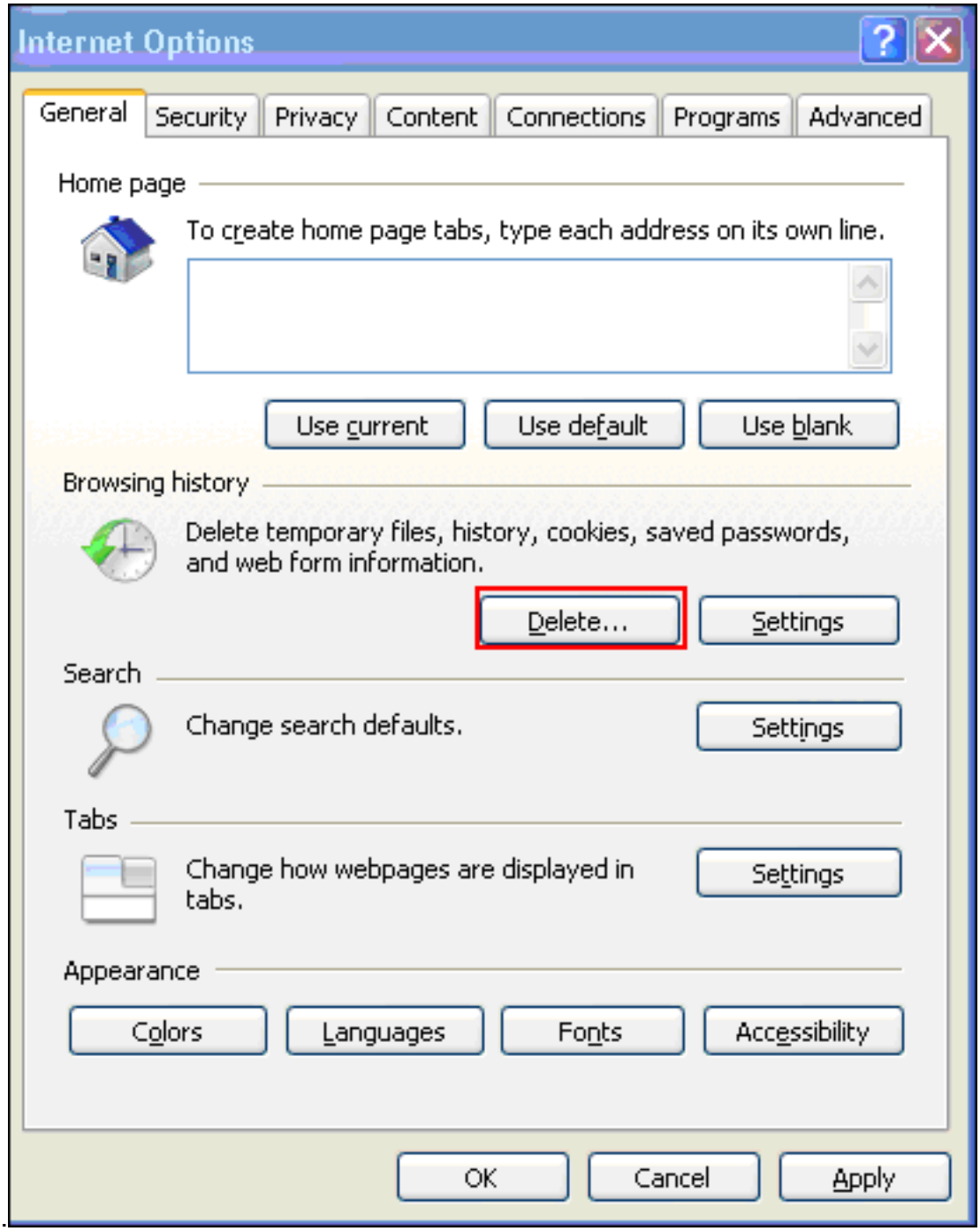
3. Advanced Privacy Settings(고급 개인 정보 설정) 대화 상자에서 Override **automatic cookie handling(자동 쿠키 처리 재정의)** 확인란을 선택하고 **Accept(수락)** 라디오 버튼을 클릭한 다음 **OK(확인)를 클릭합니다**



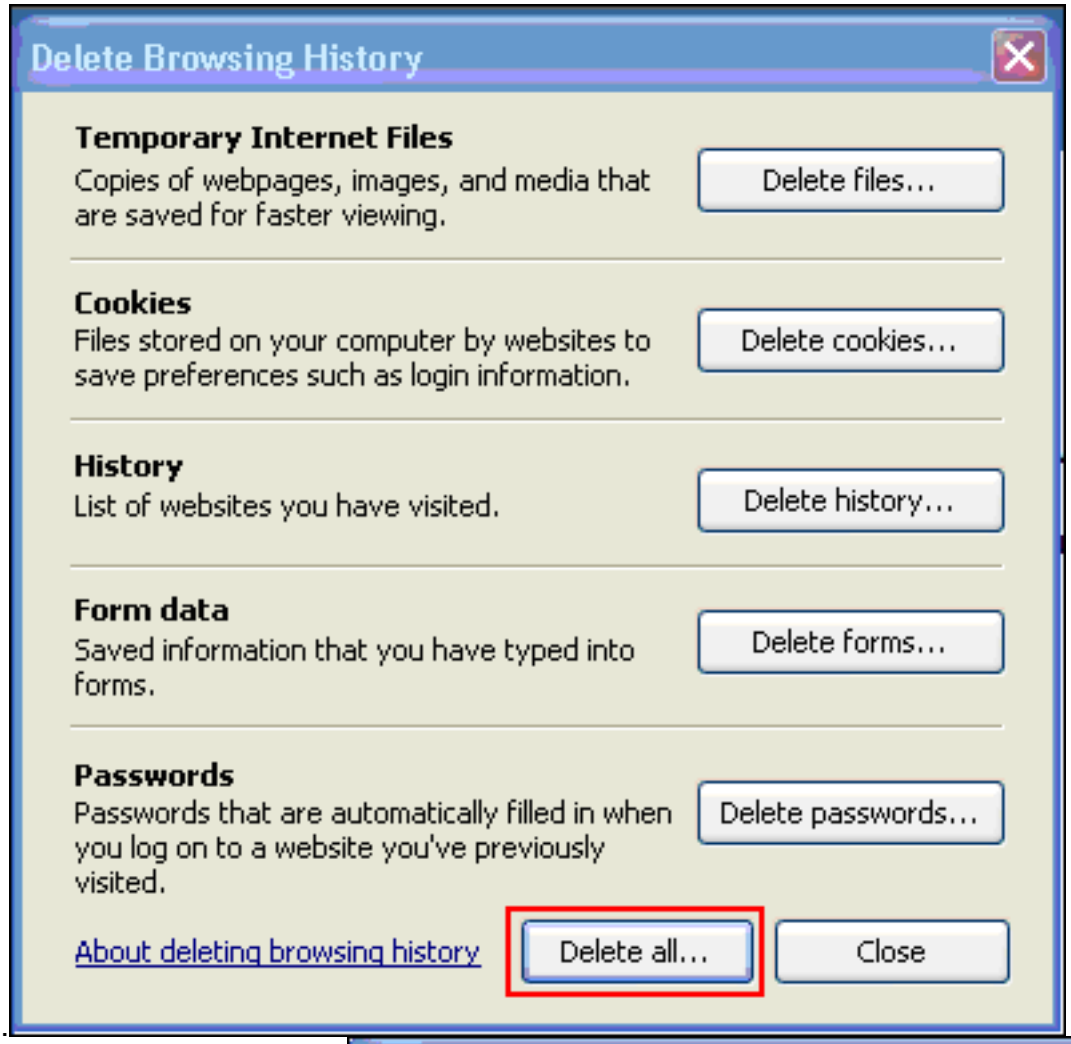
브라우저 캐시 지우기

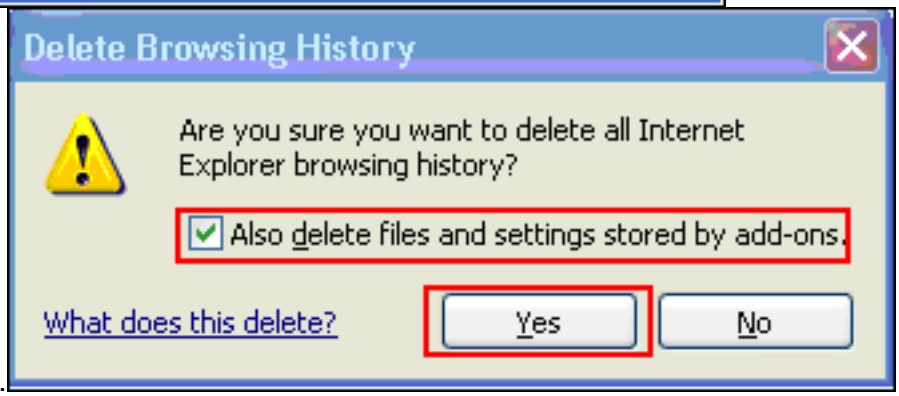
Internet Explorer의 캐시를 지우려면 다음 단계를 완료합니다.

1. Internet Explorer에서 **도구 > 인터넷 옵션을** 선택합니다



2. General(일반) 탭의 Browsing History(찾아보기 기록) 섹션 내에서 **Delete(삭제)**를 클릭합니다





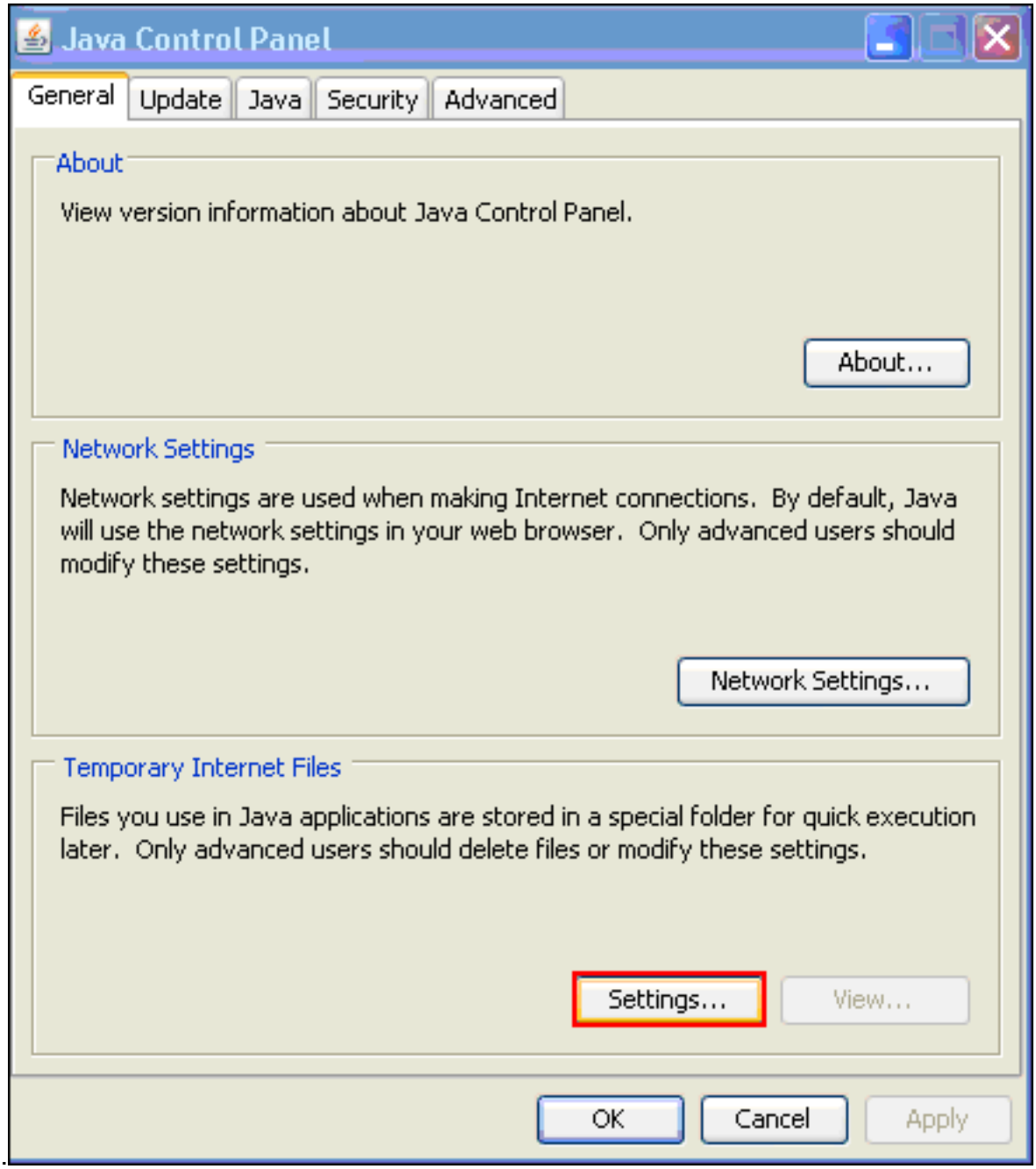
3. Delete **All을 클릭합니다**.
4. 추가 **기능으로 저장된 파일 및 설정도 삭제** 확인란을 선택하고 **예**를 클릭합니다.
5. 캐시가 지워지면 브라우저의 모든 인스턴스를 종료하고 브라우저를 다시 시작합니다.

참고: 다른 브라우저의 캐시를 지우려면 브라우저 캐시를 지우려면 어떻게 해야 합니까?를 참조하십시오.

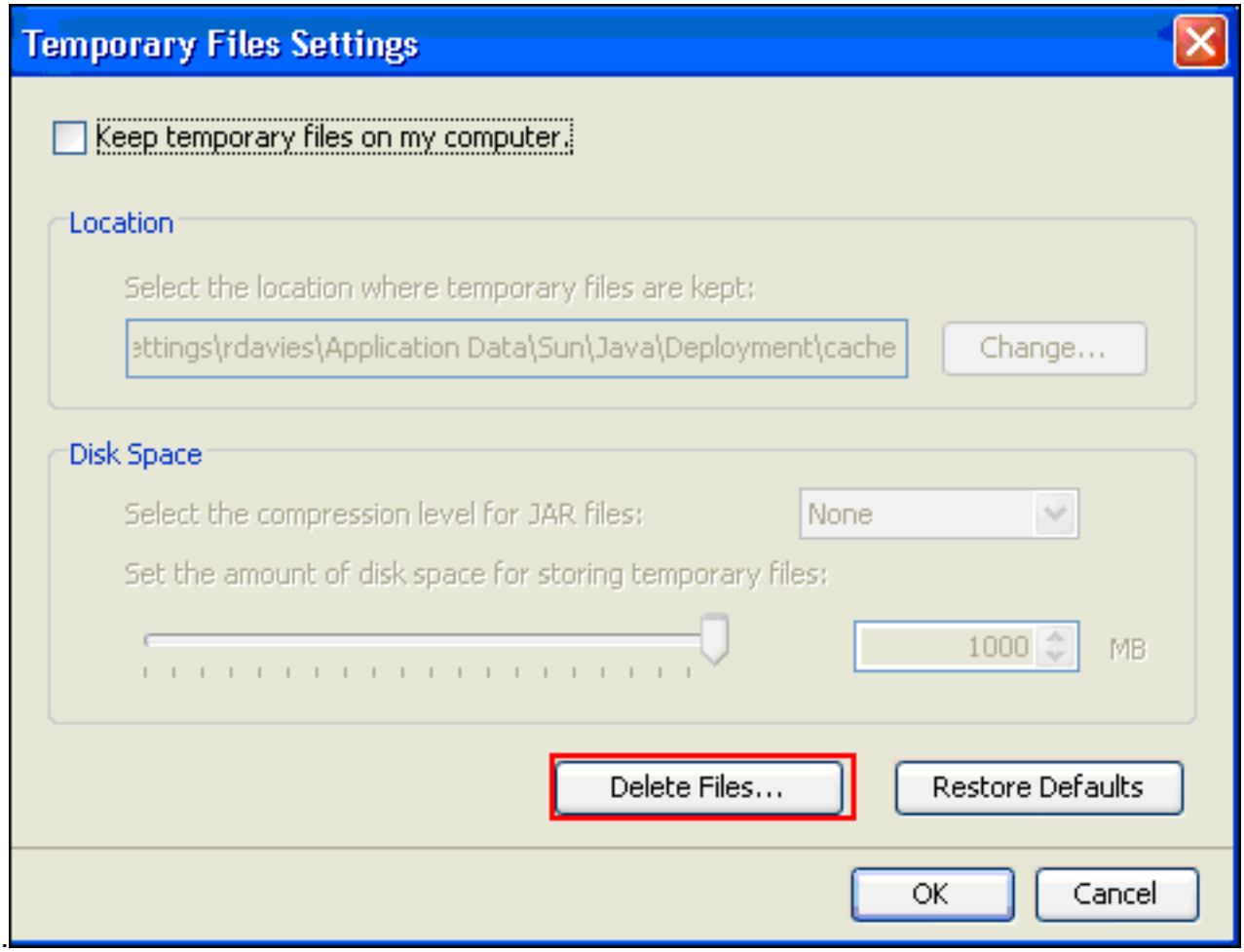
Java 캐시 지우기

Java 캐시를 지우려면 다음 단계를 완료합니다.

1. Windows 시작 메뉴에서 제어판을 선택합니다.
2. **Java**를 두 번 클릭합니다



3. **설정**을 **클릭합니다**.
4. Delete **Files**를 **클릭합니다**

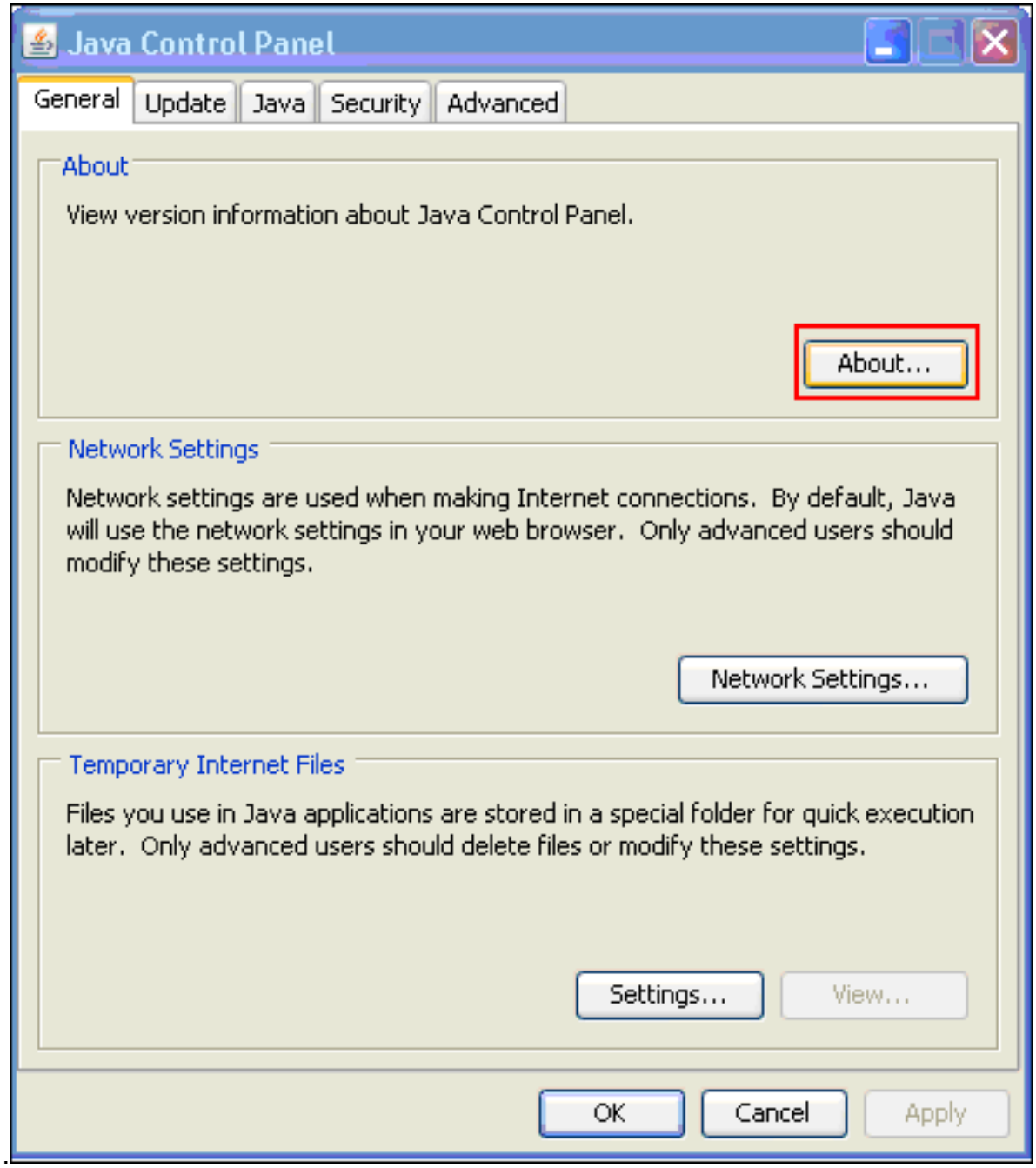


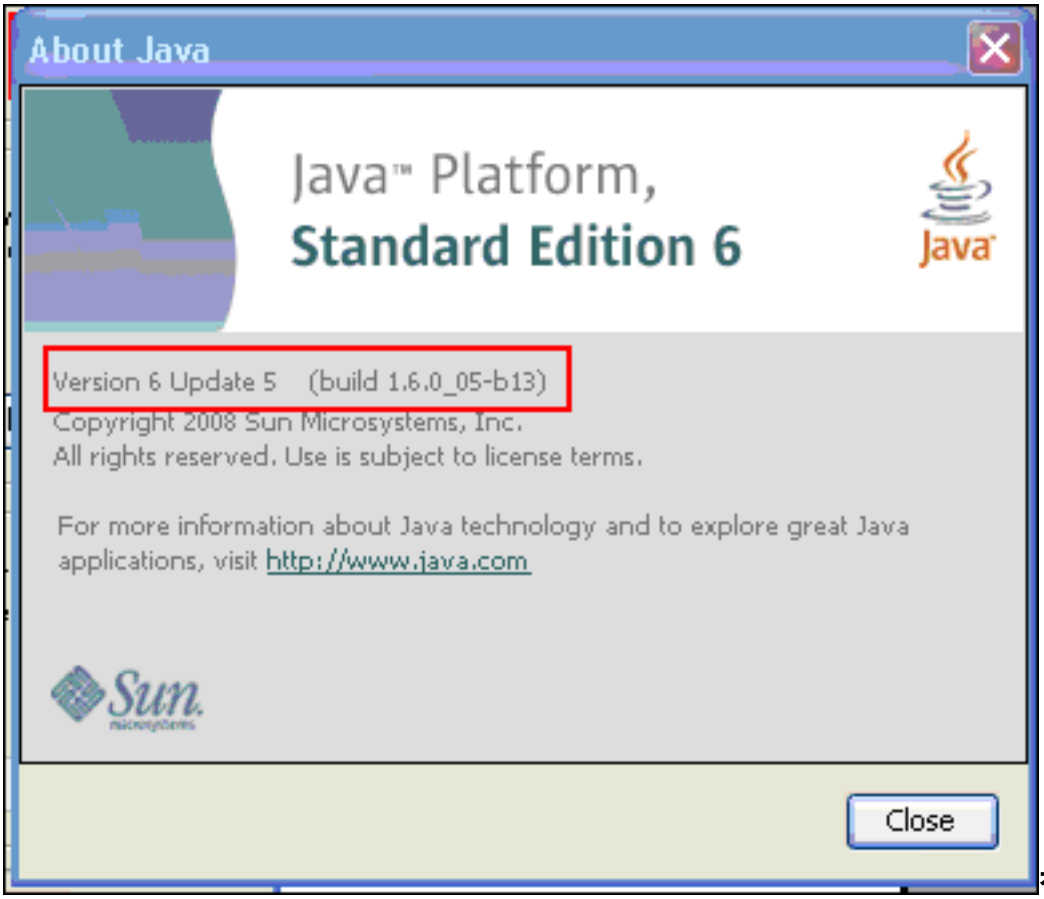
참고: Java 캐시를 지우려면 어떻게 합니까? 를 참조하십시오. 을 참조하십시오.

Java 애플릿 디버깅 옵션 활성화

Java 애플릿 디버깅 옵션을 활성화하려면 다음 단계를 완료합니다.

1. Java 1.4 이상이 활성화되었는지 확인합니다.Windows 시작 메뉴에서 제어판을 선택합니다 .**Java**를 두 번 클릭합니다.**정보**를 클릭하고 버전 번호를 확인합니다

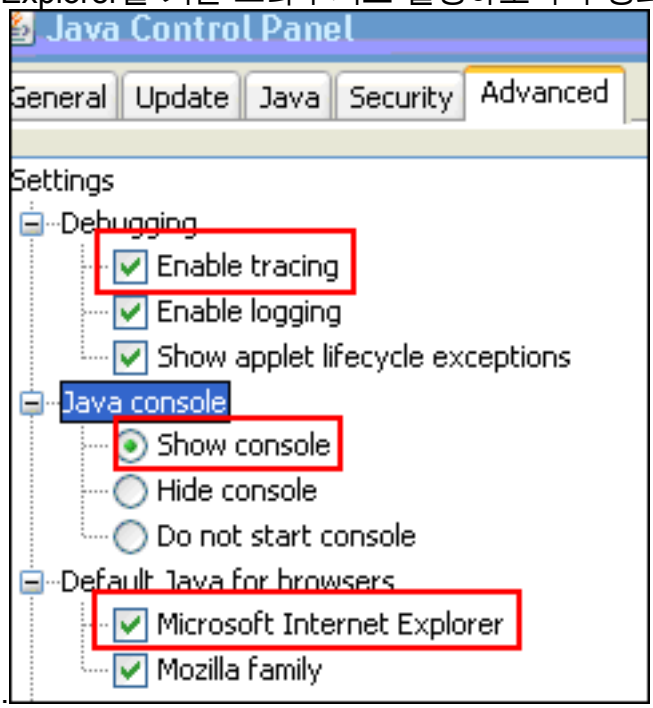

Java Control Panel
General
Update
Java
Security
Advanced
About
View version information about Java Control Panel.
About...
Network Settings
Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings.
Network Settings...
Temporary Internet Files
Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.
Settings...
View...
OK
Cancel
Apply



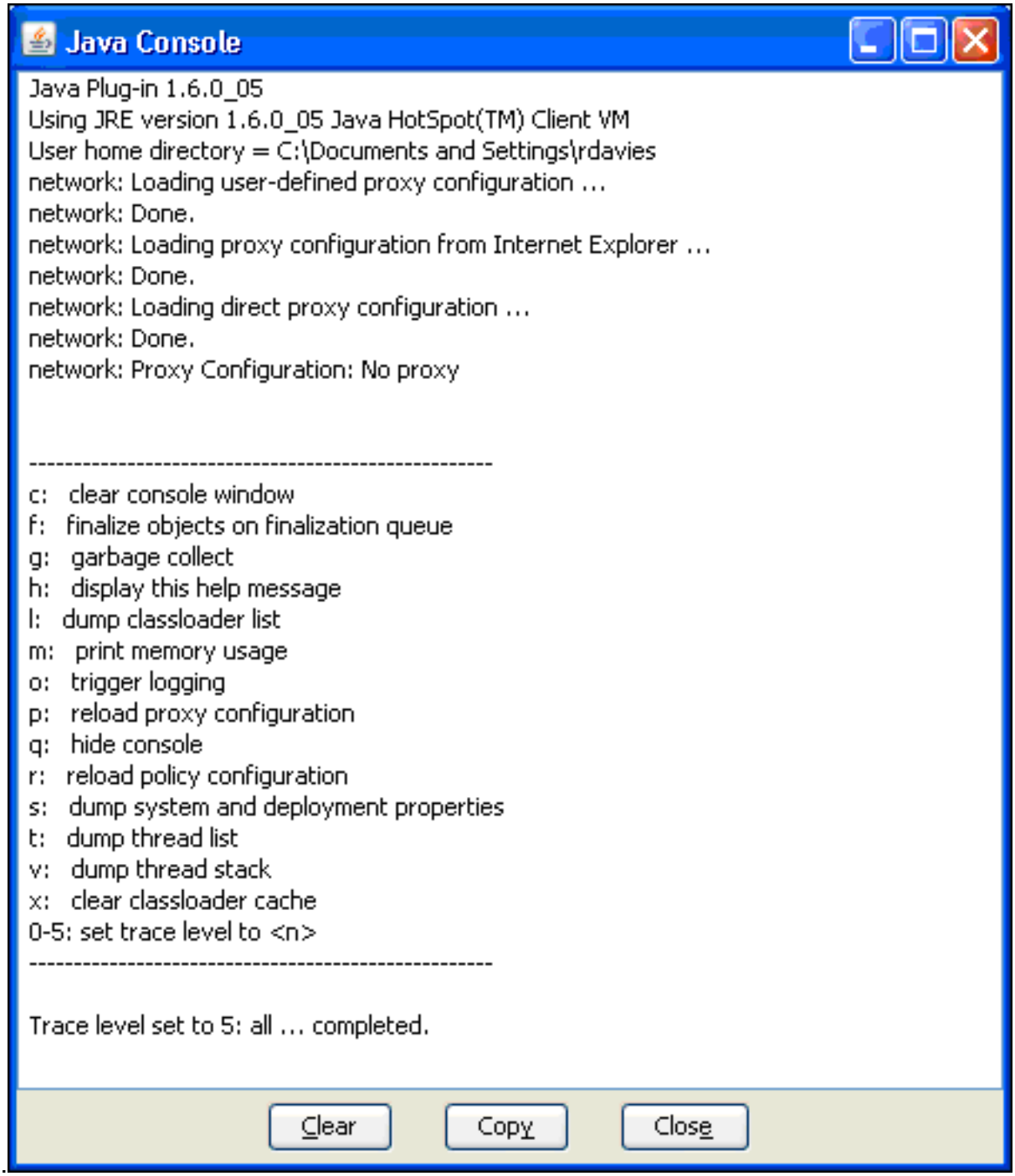
참고:

http://java.com/en/에서 Java 업데이트를 다운로드할 수 [있습니다](#) .

2. Java가 추적을 활성화하고, 콘솔을 표시하고, 다음 이미지에 표시된 대로 Microsoft Internet Explorer를 기본 브라우저로 설정하도록 구성되어 있는지 확인합니다



3. Java 캐시 지우기에 설명된 대로 Java 캐시[가 지워졌는지 확인합니다](#).
4. Internet Explorer에서 **Java 디버그** 창을 열려면 Tools > Java Console을 선택합니다



5. Java 콘솔 디버그 창이 열리면 **5**를 눌러 추적 레벨을 설정합니다.Java 애플릿을 포함하는 URL에 액세스하면 이 창에서 활동이 캡처됩니다.
6. 정보를 복사하려면 **복사**를 클릭합니다.

HTML 캡처 도구 사용

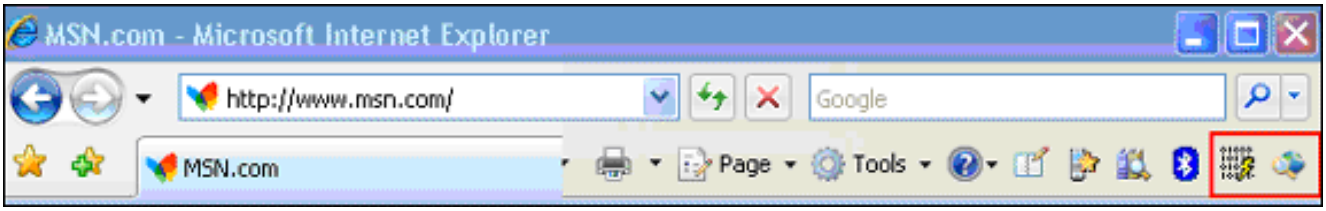
다양한 HTML 캡처 툴을 사용하여 데이터를 수집할 수 있으며, 그 중 일부는 여기에 나열되어 있습니다. 데이터 수집 연습에 사용되는 클라이언트 PC에 다음 HTML 캡처 도구 중 하나를 설치합니다.

- HttpWatch
- IE 인스펙터
- 디버그 프록시

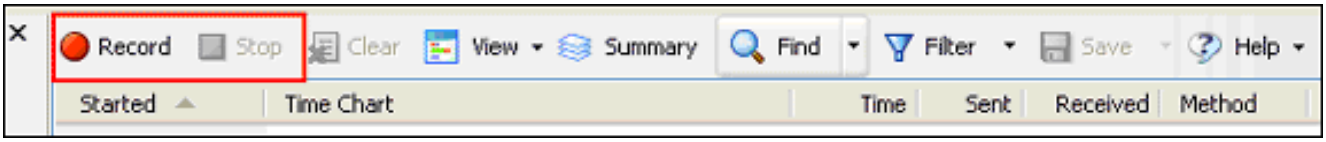
참고: 이 절차에서는 HTTPWatch 응용 프로그램을 사용합니다.

응용 프로그램이 설치되면 다음 단계를 완료합니다.

1. Shift+P+F+2를 누르거나 브라우저 창에서 아이콘을 클릭하여 HTTPWatch를 활성화합니다
.



2. 응용 프로그램이 활성화되면 브라우저 창의 아래쪽에 이 이미지와 유사한 창이 나타납니다
.



3. 데이터를 기록하려면 **레코드**를 클릭합니다. 녹음**을** 중지하려면 중지를 클릭합니다.

참고: 데이터를 기록하려면 HttpWatch 7.x를 사용하는 것이 좋습니다.

관련 정보

- ASA 컨피그레이션의 클라이언트리스 SSL VPN(WebVPN) 예
- Cisco ASA 5500 Series Adaptive Security Appliance
- 기술 지원 및 문서 – Cisco Systems