Nota técnica de resolución de problemas de ASA Clientless SSL VPN (WebVPN)

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Convenciones
Resolución de problemas
ASA versión 7.1/7.2 sin cliente
ASA versión 8.0 sin cliente
Procedimientos
Agregar ASA como sitio de confianza
Habilitar cookies
Borrar la caché del explorador
Borrar la memoria caché de Java
Habilitar opciones de depuración de subprogramas Java
Habilitar las herramientas de captura HTML
Información Relacionada

Introducción

Este documento enumera las técnicas de solución de problemas de Clientless SSL VPN (WebVPN) adoptadas para las versiones 7.1, 7.2 y 8.0 de ASA. Hay avances significativos entre estas versiones que requieren la adopción de diversas técnicas de resolución de problemas.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en el Cisco 5500 Series ASA que ejecuta la versión de software 7.1 o superior.

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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Resolución de problemas

El requisito previo para la resolución de problemas de las conexiones VPN SSL (WebVPN) sin cliente en ASA es obtener visibilidad de la experiencia del cliente a través de capturas de pantalla y herramientas de captura HTML y, a continuación, compararla con la misma información cuando se conecta directamente a la URL/aplicación a la que se está accediendo.

ASA versión 7.1/7.2 sin cliente

Esta sección describe las técnicas de solución de problemas para las versiones 7.1/7.2 de ASA y todos los intervalos hasta la versión 8.0, pero sin incluirla.

En esta versión, si las funciones complejas de Java/Javascript tienen dificultades, se podrían considerar otras opciones (como el reenvío de puertos de acceso a aplicaciones o el uso de proxy-bypass). Refiérase a Configuración del Acceso a la Aplicación y Uso de Omisión de Proxy para obtener más información sobre estas alternativas.

En la mayoría de los escenarios, si la URL a la que se accede a través de Clientless SSL VPN falla para Internet Explorer, también fallará para otro navegador.

Para asegurarse de que esto no depende del equipo cliente o del sistema operativo, utilice otro cliente desde una ubicación diferente. También se puede probar el uso de un cliente VPN IPsec o SSL.

Asegúrese de que el ASA esté incluido en la zona de confianza del navegador como se describe en Habilitación de cookies en exploradores para WebVPN y que las cookies estén habilitadas como se describe en Habilitar cookies.

Si el proceso aún falla, complete estos pasos para reunir la información necesaria y luego abra un caso TAC.

1. Borre la memoria caché del navegador como se describe en Borrar la Memoria Caché del Navegador.
2. Borre la memoria caché de Java como se describe en Clear the Java Cache.
3. Inhabilite la memoria caché WebVPN en el ASA como se describe en Configuración del Almacenamiento en Caché.
4. Si hay un applet Java, utilice debug level 5 en la ventana del applet como se describe en Habilitar las Opciones de Debugging de Applet Java.
5. Inicie sesión en ASA a través de Clientless SSL VPN.
6. En la URL justo antes de la URL problemática, habilite una herramienta de captura HTML en el navegador como se describe en Habilitar las Herramientas de Captura HTML.
7. Capture la secuencia desde este punto hasta la URL problemática.
8. Presione **Ctrl+Imprimir pantalla** en el teclado para capturar una captura de pantalla.

9. Detenga la herramienta de captura HTML.
10. Realice los mismos pasos del 1 al 9 cuando se conecte directamente a la URL a través de una sesión IPsec o SSL VPN a través del ASA o se conecte directamente en el mismo segmento LAN (si es posible) y envíe los datos al TAC para su análisis.

ASA versión 8.0 sin cliente

En esta sección se describen las técnicas de solución de problemas utilizadas para ASA versión 8.0 y todos los intervalos.

En esta versión, si las URL o aplicaciones complejas tienen dificultades a través de SSL VPN sin cliente, otras opciones (como el uso de túneles inteligentes) son una potente alternativa. Refiérase a Configuración de Smart Tunnel Access para obtener más información sobre los túneles inteligentes.

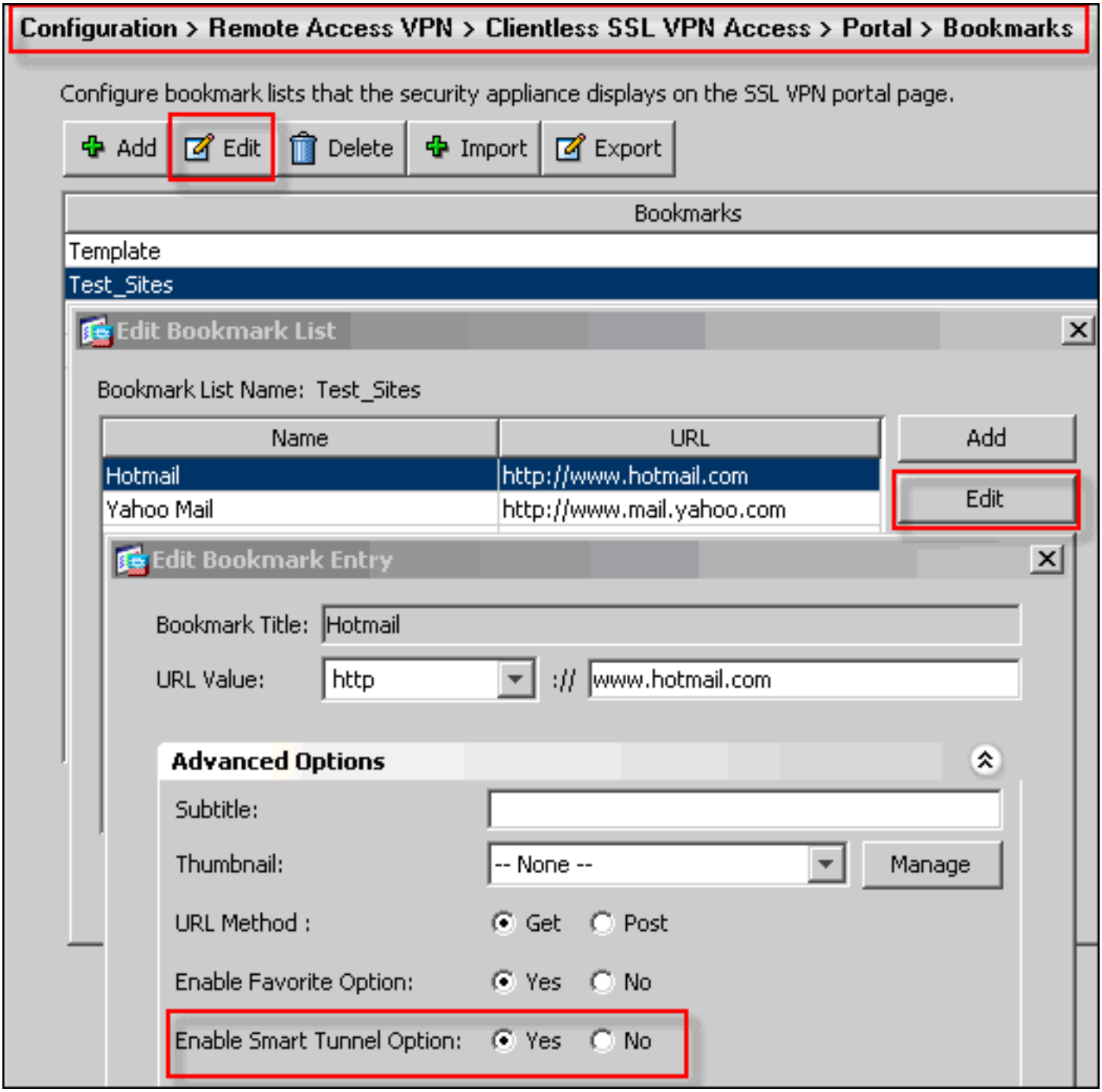
También puede considerar el reenvío de puertos de acceso a la aplicación o el uso de la omisión de proxy. Refiérase a Configuración del Acceso a la Aplicación y Uso de Omisión de Proxy para obtener más información sobre estas alternativas.

En la mayoría de los escenarios, si la URL a la que se accede a través de Clientless SSL VPN falla para Internet Explorer, también fallará para otro navegador.

Para asegurarse de que esto no depende del equipo cliente o del sistema operativo, utilice otro cliente desde una ubicación diferente. También se puede probar el uso de un cliente VPN IPsec o SSL.

Asegúrese de que el ASA esté incluido en la zona de confianza del navegador como se describe en Habilitación de cookies en exploradores para WebVPN y que las cookies estén habilitadas como se describe en Habilitar cookies.

Si una aplicación experimenta un problema con el motor de transformación de contenido sin cliente (CTE/rewriter), puede modificar el marcador de esa aplicación para habilitar la opción Túnel inteligente como se muestra en esta imagen:



Para habilitar esta opción para un marcador no se requiere configuración adicional. Similar al reenvío de puertos, esta es otra opción conveniente para hacer clic en un marcador para abrir una nueva ventana que utilice el túnel inteligente para pasar el tráfico de la aplicación y evitar problemas de reescritura.

Cuando utiliza esta función para aplicaciones TCP Winsock 32 (como RDP), el administrador debe identificar los procesos que se utilizarán a través de túneles inteligentes. Por ejemplo, RDP utiliza el proceso mstsc.exe; se puede crear una entrada de túnel inteligente simple para este proceso.

Las aplicaciones más complicadas pueden generar varios procesos. Desde la página del portal WebVPN, elija el panel **Acceso a la aplicación**. Tan pronto como se carga, la lista de *aplicaciones permitidas* pueden conectarse al lado privado de la red.

Si el proceso aún falla, complete estos pasos para reunir la información necesaria y luego abra un caso TAC.

1. Borre la memoria caché del navegador como se describe en Borrar la Memoria Caché del Navegador.
2. Borre la memoria caché de Java como se describe en Clear the Java Cache.
3. Inhabilite la memoria caché WebVPN en el ASA como se describe en Configuración del Almacenamiento en Caché.
4. Si hay un applet Java, utilice debug level 5 en la ventana del applet como se describe en Habilitar las Opciones de Debugging de Applet Java.
5. Inicie sesión en ASA a través de Clientless SSL VPN.
6. En la URL justo antes de la URL problemática, habilite una herramienta de captura HTML en el navegador como se describe en Habilitar las Herramientas de Captura HTML.
7. Capture la secuencia desde este punto hasta la URL problemática.
8. Presione **Ctrl+Imprimir pantalla** en el teclado para capturar una captura de pantalla.
9. Detenga la herramienta de captura HTML.
10. Realice los pasos del 1 al 9 cuando se conecte directamente a la URL a través de una sesión IPsec o Any Connect SSL a través del ASA o se conecte directamente al mismo segmento LAN (si es posible), complete estos pasos y envíe los datos al TAC para su análisis

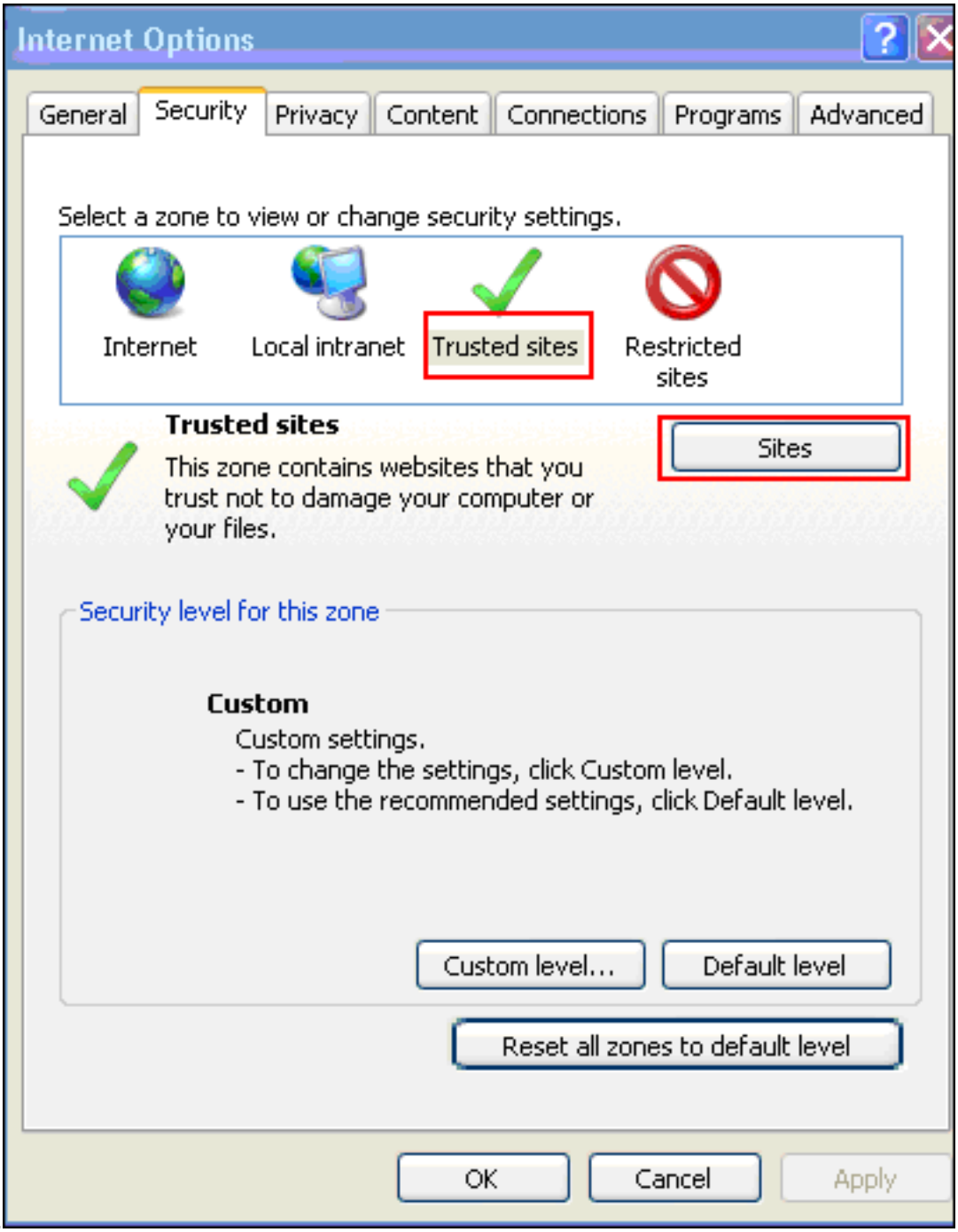
Procedimientos

Agregar ASA como sitio de confianza

Cuando acceda al ASA en Internet Explorer, recibirá un error de certificado si el sitio no se incluye como sitio de confianza.

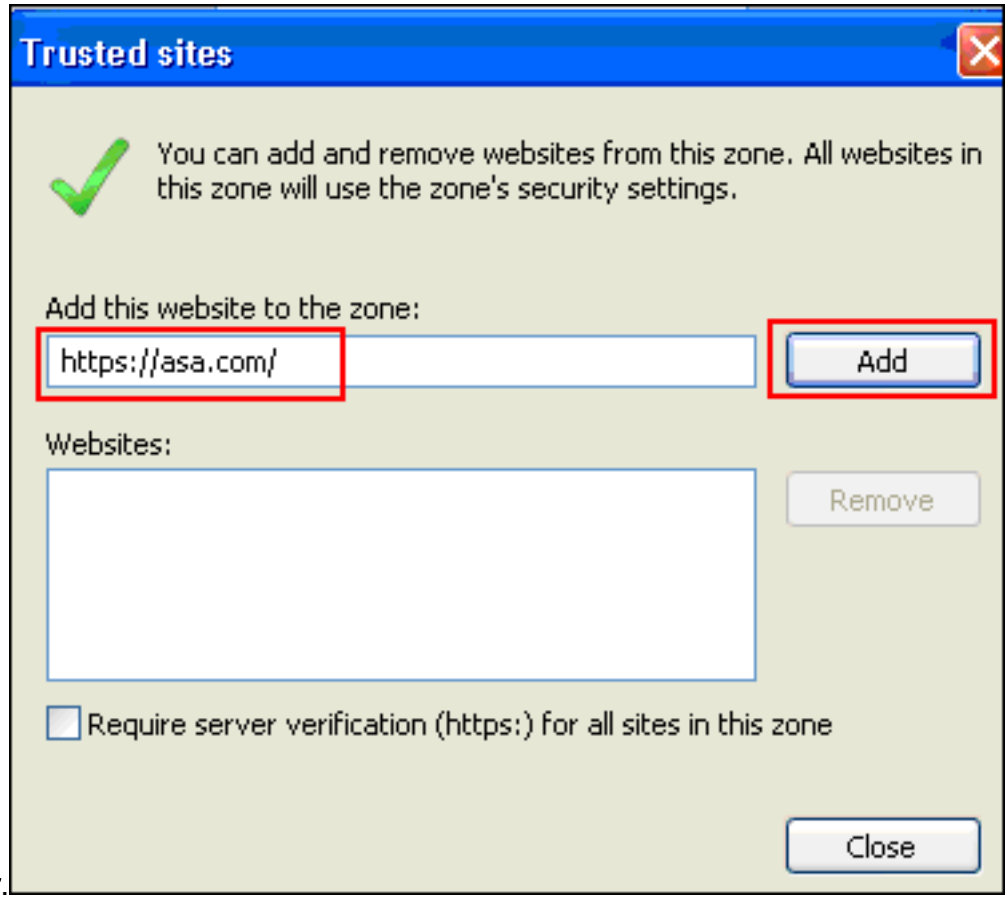
Complete estos pasos para agregar el ASA como un sitio de confianza:

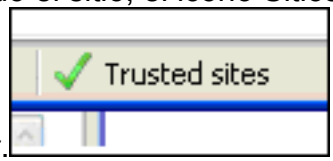
1. En Internet Explorer, elija **Herramientas > Opciones de Internet**.
2. Haga clic en la ficha **Seguridad** y elija **Sitios en los que se haya realizado la**



prueba.

3. Haga clic en **Sitios**.
4. Agregue la dirección https:// del ASA y haga clic en

Agregar. 

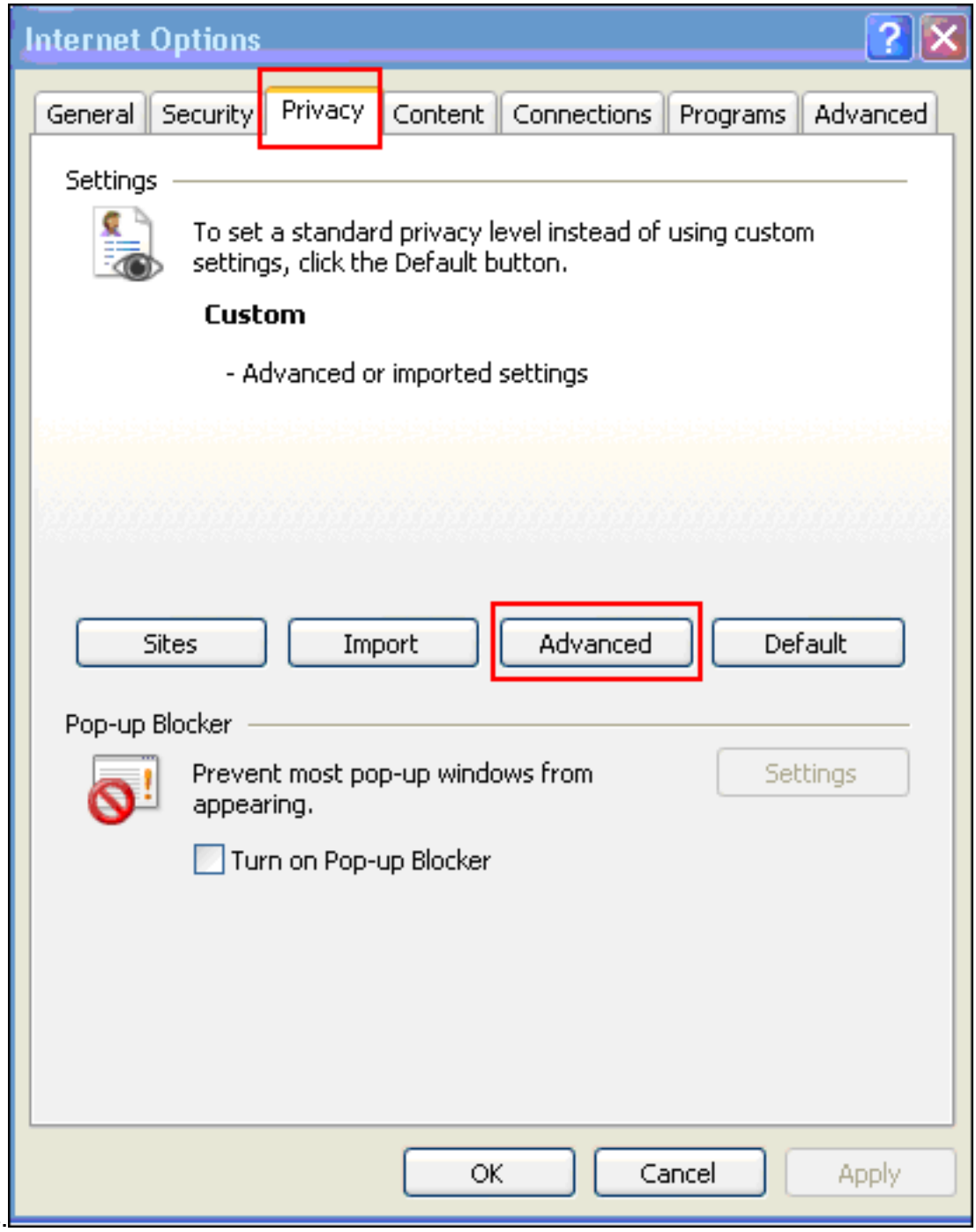
5. Una vez agregado el sitio, el icono Sitios de confianza aparece en la barra de estado de Internet Explorer. 

Nota: Refiérase a Trabajar con la Configuración de Seguridad de Internet Explorer 6 para obtener información detallada sobre este procedimiento.

Habilitar cookies

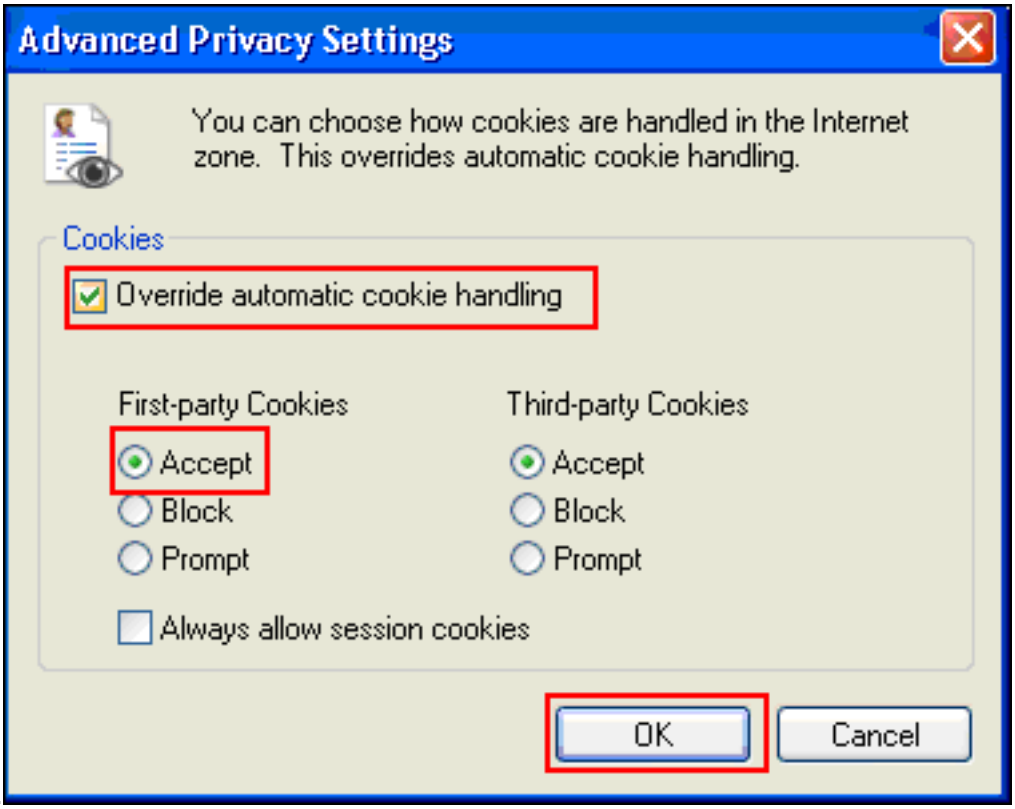
Complete estos pasos para habilitar las cookies:

1. En Internet Explorer, elija **Herramientas > Opciones de Internet**.
2. Haga clic en la ficha **Privacidad** y, a continuación, haga clic en



Avanzadas.

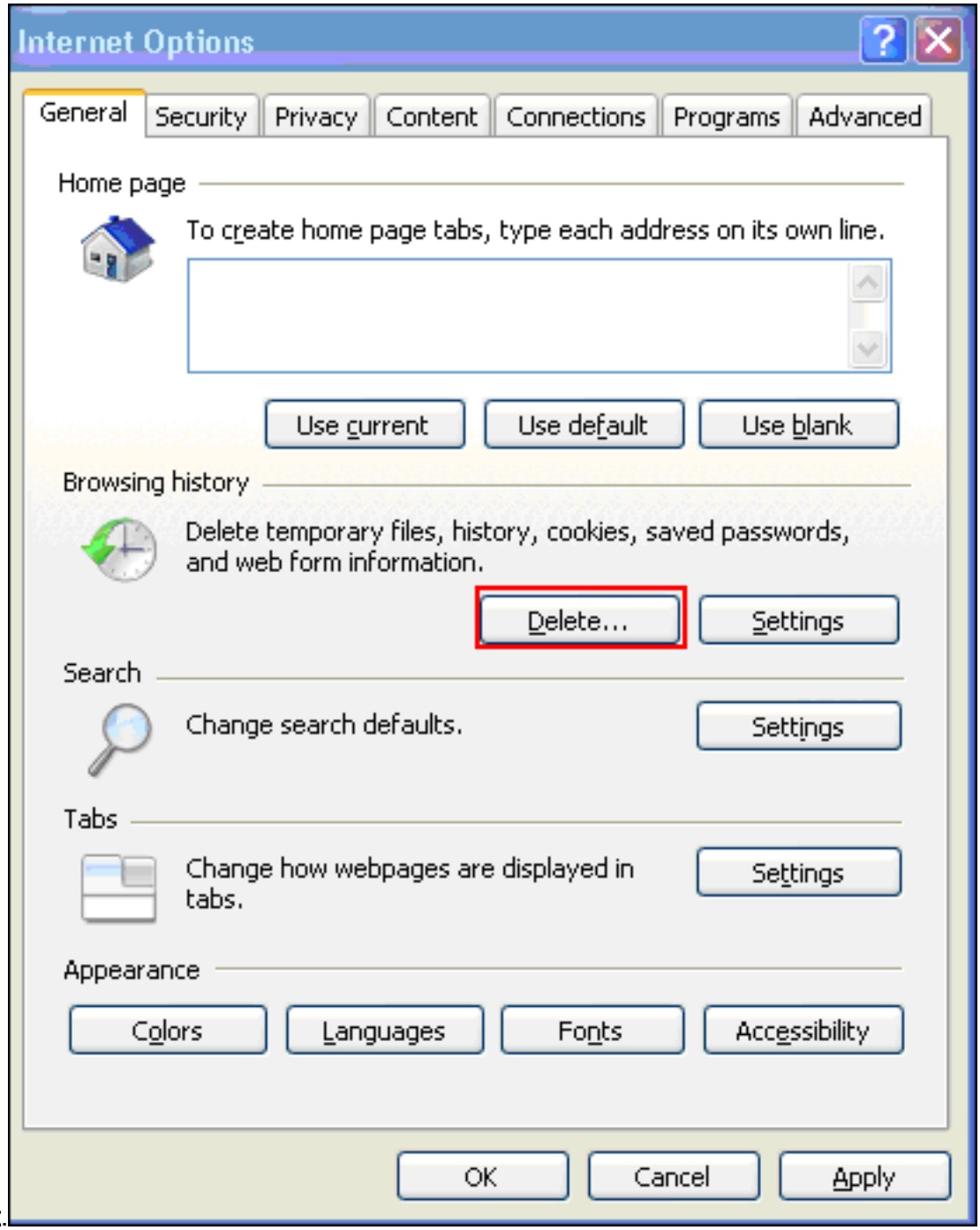
3. En el cuadro de diálogo Advanced Privacy Settings, marque la casilla de verificación **Override automatically cookie management**, haga clic en el botón de opción **Accept** y haga

clic en **OK**. 

Borrar la caché del explorador

Complete estos pasos para borrar la memoria caché para Internet Explorer:

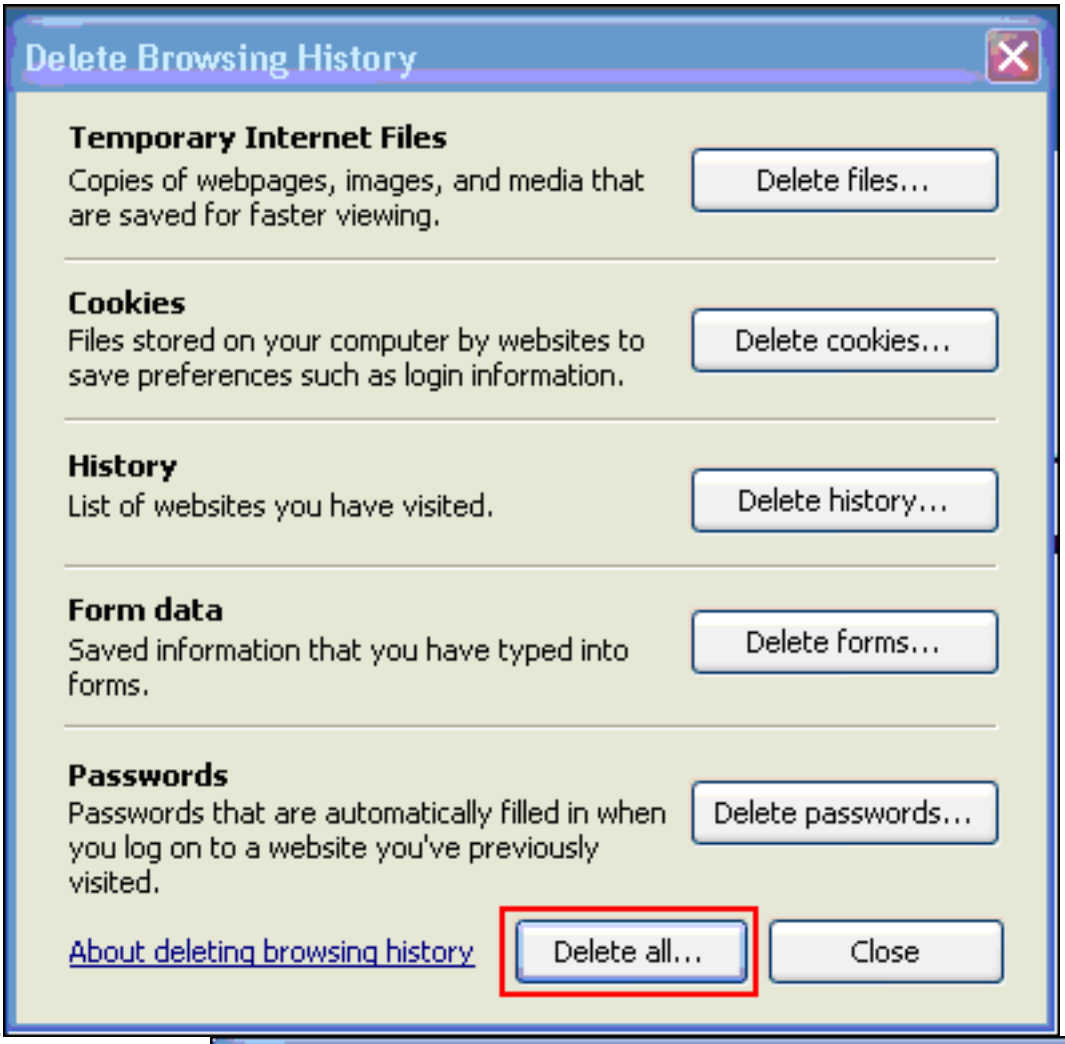
1. En Internet Explorer, elija **Herramientas > Opciones de**

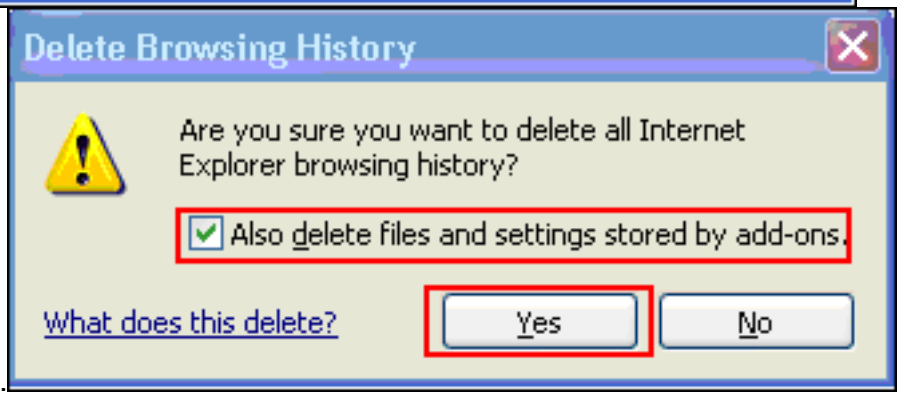


Internet.

2. En la ficha General, haga clic en **Eliminar** en la sección Historial de

exploración.





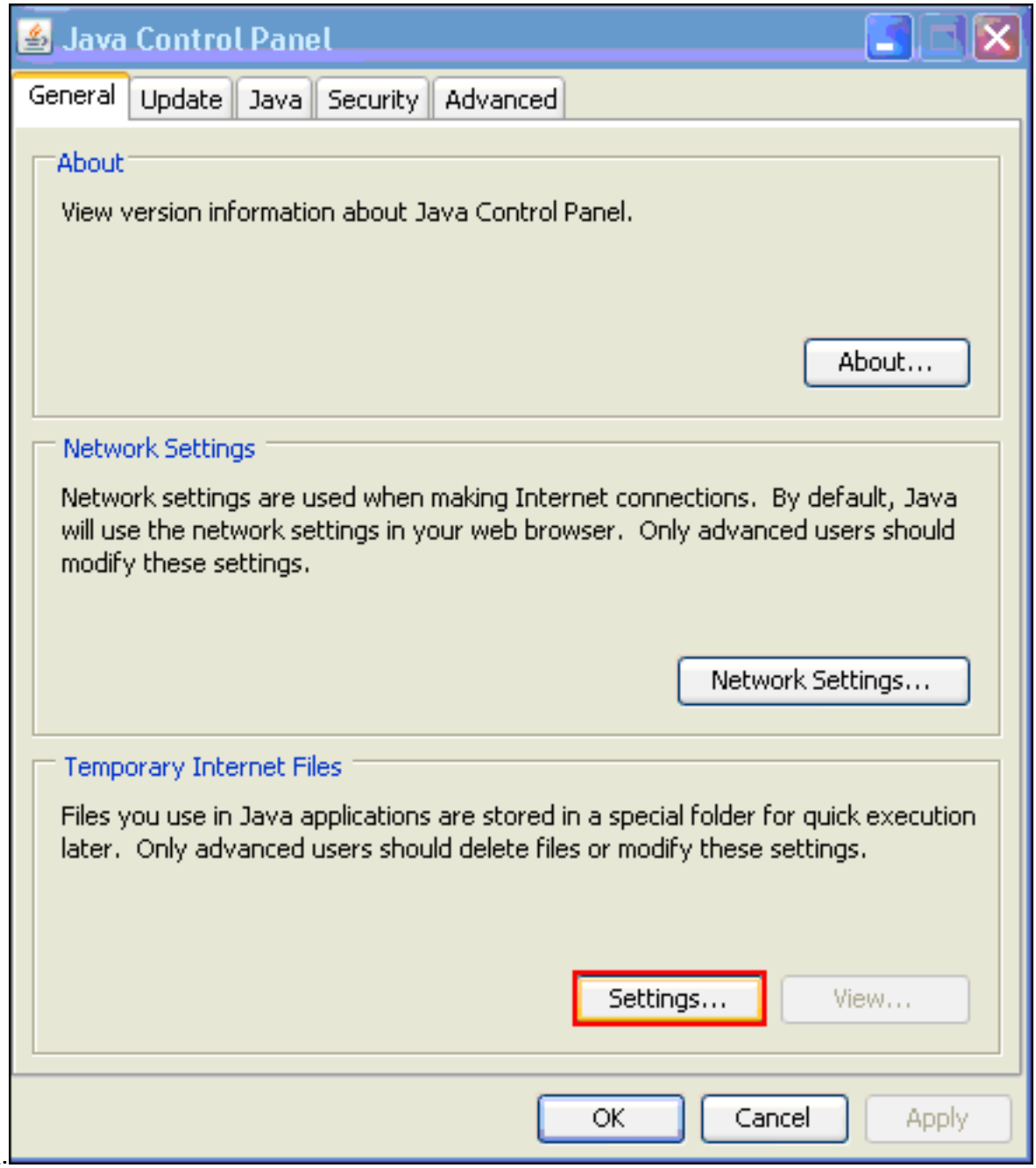
3. Haga clic en **Eliminar todo**.
4. Marque la casilla de verificación **Eliminar también archivos y configuraciones almacenados por complementos** y haga clic en **Sí**.
5. Una vez borrada la memoria caché, apague todas las instancias del explorador y reinicie el explorador.

Nota: Para borrar la memoria caché de otros exploradores, consulte ¿Cómo borro la memoria caché de mi navegador (para mejorar su rendimiento)?

Borrar la memoria caché de Java

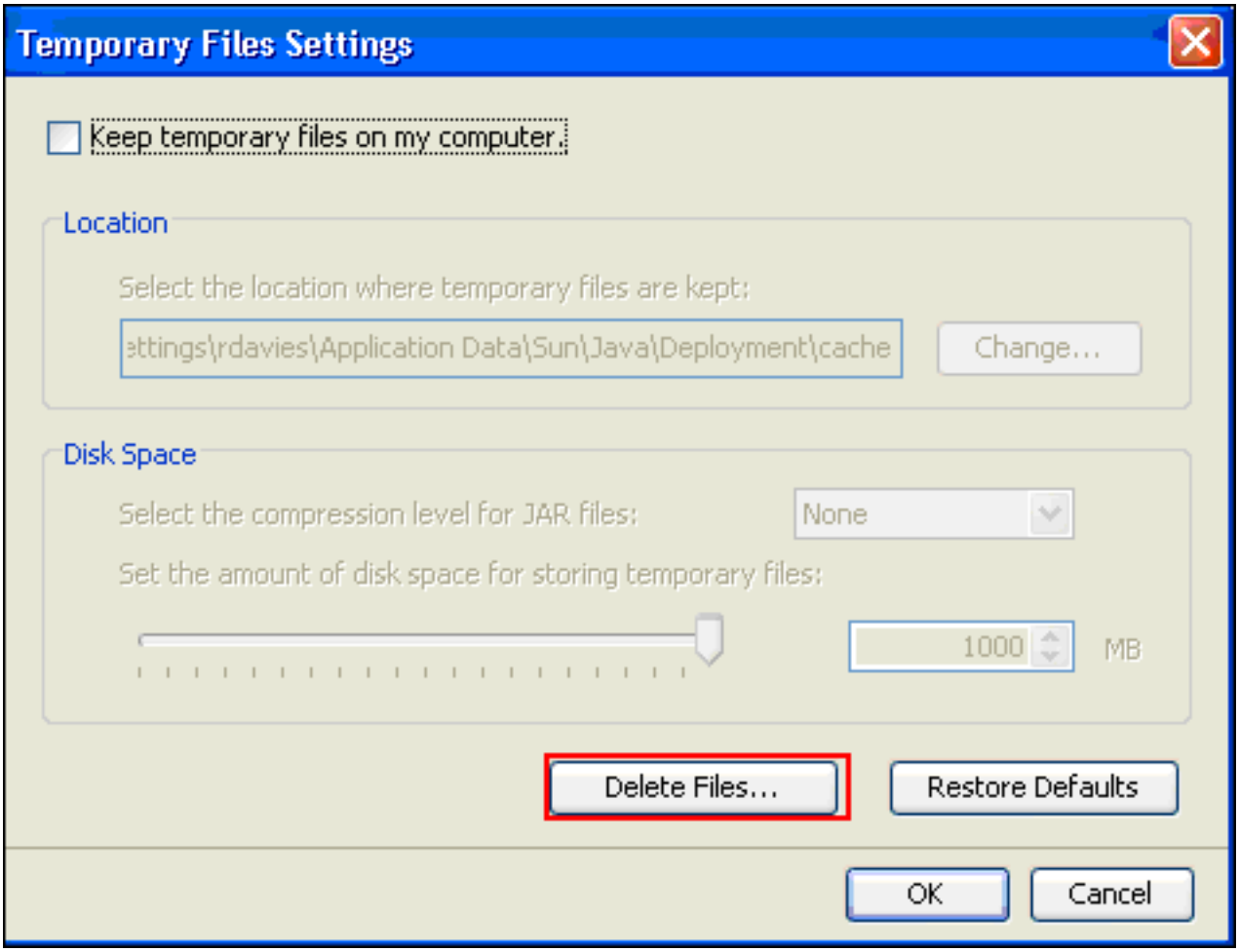
Complete estos pasos para borrar la memoria caché de Java:

1. Elija **Panel de control** en el menú Inicio de Windows.
2. Haga doble clic en



Java.

3. Haga clic en **Settings**.
4. Haga clic en **Eliminar archivos**.

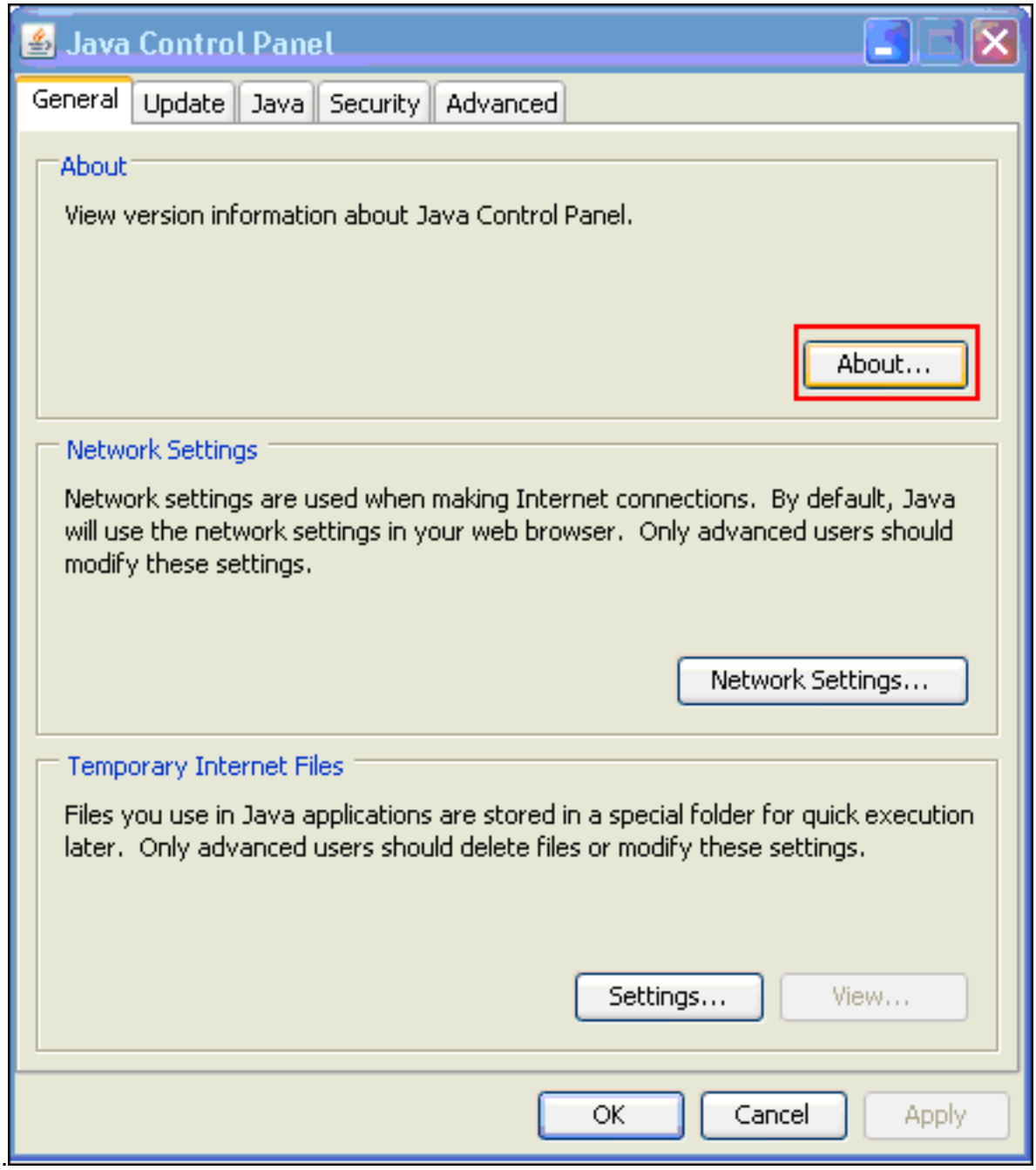


Nota: Consulte Cómo borro mi caché de Java? para obtener más información sobre este procedimiento.

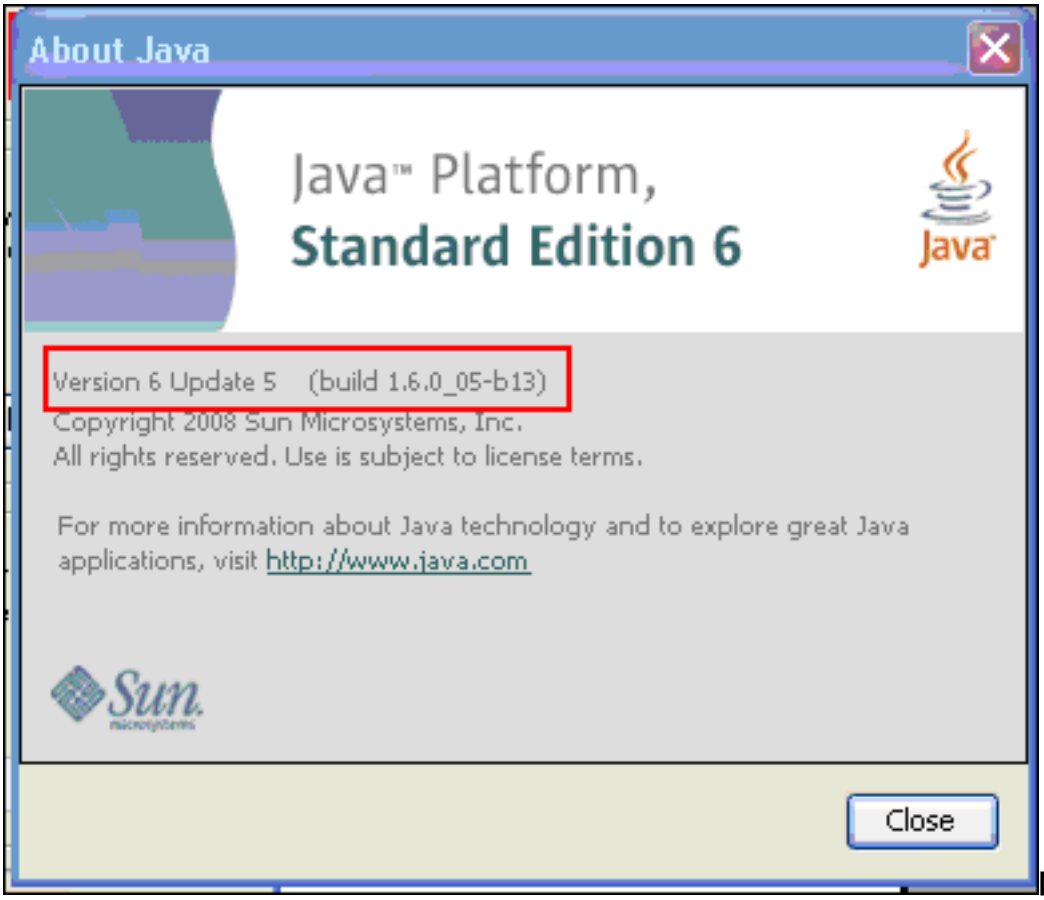
Habilitar opciones de depuración de subprogramas Java

Complete estos pasos para habilitar la opción de depuración del applet Java:

1. Asegúrese de que Java 1.4 o superior esté habilitado:Elija **Panel de control** en el menú Inicio de Windows.Haga doble clic en **Java**.Haga clic en **About** y verifique el número de

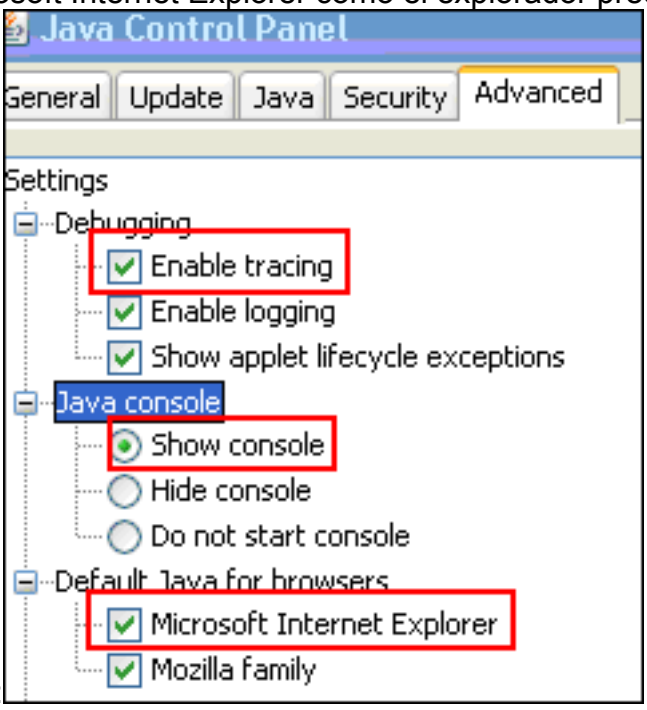

Java Control Panel
General
Update
Java
Security
Advanced
About
View version information about Java Control Panel.
About...
Network Settings
Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify 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

versión.

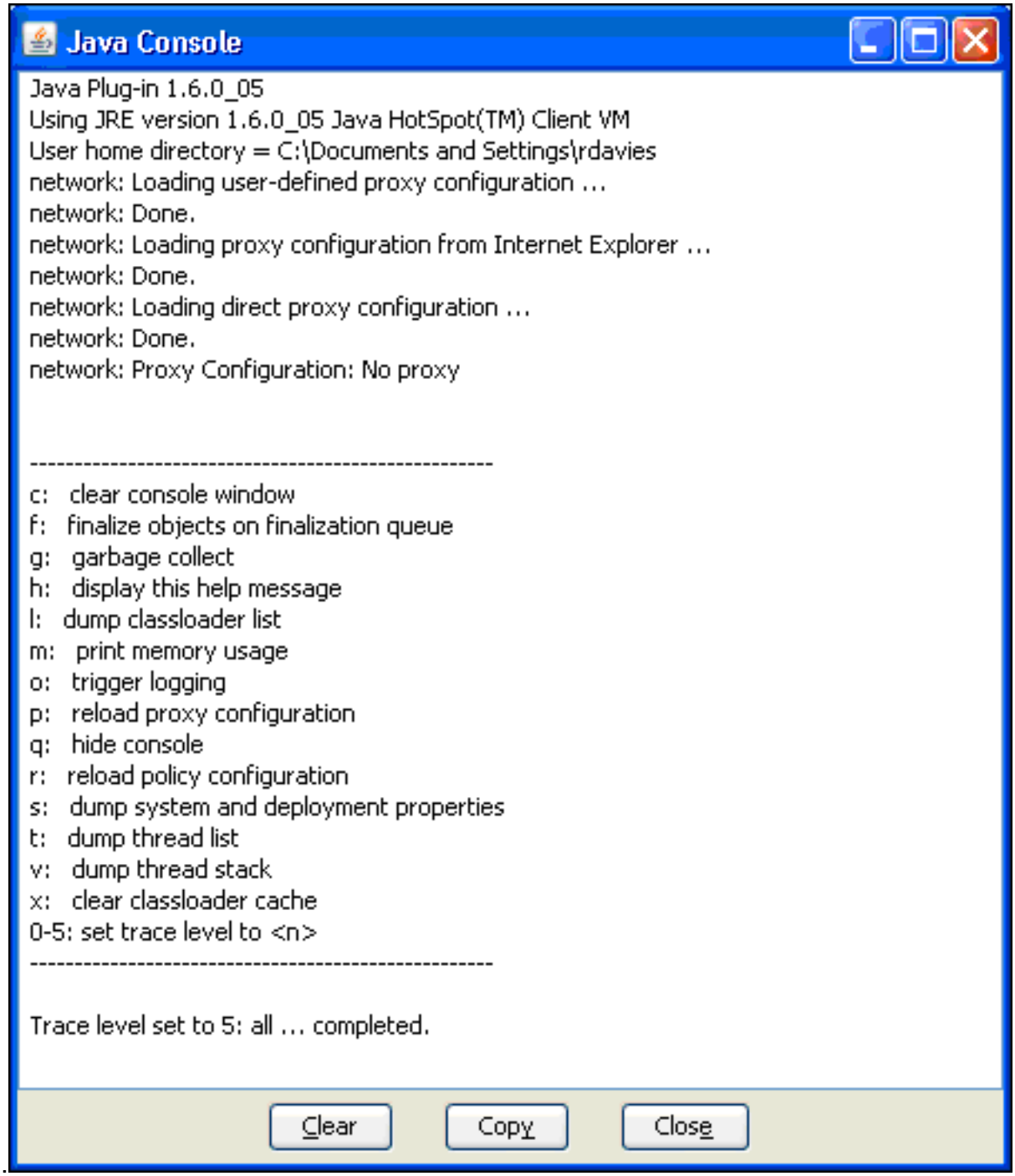


Nota: Puede descargar actualizaciones de Java desde http://java.com/en/ .

2. Asegúrese de que Java esté configurado para activar el seguimiento, mostrar la consola y establecer Microsoft Internet Explorer como el explorador predeterminado, como se muestra en esta imagen:



3. Asegúrese de borrar la memoria caché de Java como se describe en Borrar la Memoria Caché de Java.
4. En Internet Explorer, elija **Tools > Java Console** para abrir la ventana de depuración de

Java. 

5. Una vez abierta la ventana de depuración de la consola Java, presione **5** para establecer el nivel de seguimientoCuando se accede a una URL que contiene un subprograma Java, la actividad se captura en esta ventana.
6. Haga clic en **Copiar** para copiar la información.

Habilitar las herramientas de captura HTML

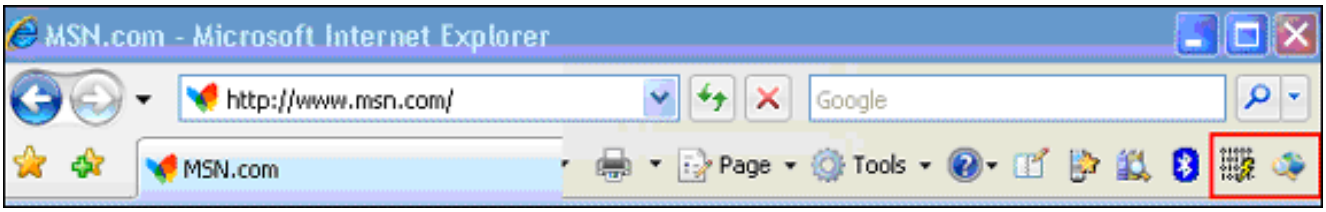
Hay varias herramientas de captura HTML disponibles para recopilar datos, algunas de las cuales se han enumerado aquí. Instale una de estas herramientas de captura HTML en el equipo cliente para el que se utiliza su ejercicio de recopilación de datos:

- HttpWatch
- Inspector de IE
- Proxy de depuración

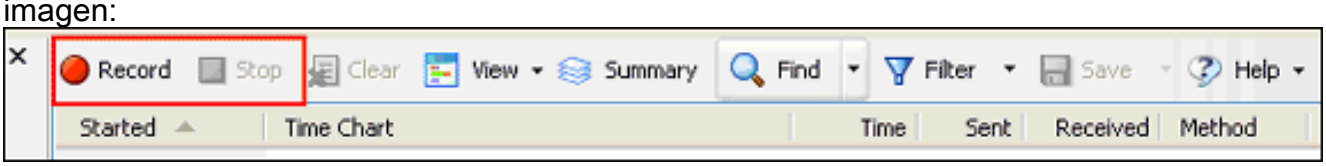
Nota: Este procedimiento utiliza la aplicación HTTPWatch.

Una vez instalada la aplicación, complete estos pasos:

1. Presione Mayús+P+F+2 o haga clic en el icono en la ventana del navegador para habilitar HTTPWatch.



2. Una vez habilitada la aplicación, aparece una ventana incrustada en la parte inferior de la ventana del navegador similar a esta imagen:



3. Haga clic en **Grabar** para grabar datos; haga clic en **Detener** para detener la grabación.

Nota: Se recomienda utilizar HttpWatch 7.x para registrar los datos.

Información Relacionada

- Ejemplo de Configuración de Clientless SSL VPN (WebVPN) en ASA
- Cisco ASA 5500 Series Adaptive Security Appliances
- Soporte Técnico y Documentación - Cisco Systems