

# ASA 无客户端 SSL VPN (WebVPN) 故障排除技术说明

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[排除故障](#)

[ASA 版本 7.1/7.2 无客户端](#)

[ASA 版本 8.0 无客户端](#)

[步骤](#)

[将 ASA 添加为可信站点](#)

[启用 Cookie](#)

[清除浏览器缓存](#)

[清除 Java 缓存](#)

[启用 Java 小程序调试选项](#)

[启用 HTML 捕获工具](#)

[相关信息](#)

## [简介](#)

本文档列出了适用于 ASA 版本 7.1、7.2 和 8.0 的无客户端 SSL VPN (Webvpn) 故障排除技术。这些版本之间存在巨大的改进，需要采用不同的故障排除技术。

## [先决条件](#)

### [要求](#)

本文档没有任何特定的要求。

### [使用的组件](#)

本文档中的信息基于运行软件版本 7.1 或更高版本的 Cisco 5500 系列 ASA。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

### [规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## 排除故障

在 ASA 上排除无客户端 SSL VPN 连接 (Webvpn) 故障的目的，是为了通过屏幕截图和 HTML 捕获工具以了解客户端体验，然后将此体验与直接连接要访问的 URL/应用程序时的相同信息进行比较。

### [ASA 版本 7.1/7.2 无客户端](#)

本部分介绍了适用于 ASA 版本 7.1/7.2 和所有过渡版本的故障排除技术，但不包括 8.0 版本。

在此版本中，如果无法使用复杂的 Java 或 Javascript 功能，可以考虑使用其他选项（例如应用程序访问端口转发或使用代理旁路）。有关这些替代方案的详细信息，请参阅[配置应用程序访问](#)和[使用代理旁路](#)。

在多数情况下，如果 Internet Explorer 无法访问可以通过无客户端 SSL VPN 访问的 URL，则使用其他浏览器也将无法访问。

为确保此行为与客户端 PC 或操作系统无关，请从其他位置使用另一个客户端进行访问。您还可以测试 Ipsec 或 SSL VPN 客户端的使用。

请确保按照“在浏览器中启用 WebVPN 的 Cookie”的说明将 ASA 包含到[浏览器可信区域](#)中，并按照[启用 Cookie](#)的说明启用 Cookie。

如果此过程仍失败，请执行以下步骤以采集必要信息，然后打开 TAC 案例。

1. 按照[清除浏览器缓存](#)的说明清除浏览器缓存。
2. 按照[清除 Java 缓存](#)的说明清除 Java 缓存。
3. 按照[配置缓存](#)的说明在 ASA 上禁用 Webvpn 缓存。
4. 如果存在 Java 小程序，请按照[启用 Java 小程序调试选项](#)的说明在小程序窗口中使用调试级别 5。
5. 通过无客户端 SSL VPN 登录 ASA。
6. 在问题 URL 之前的 URL 上，按照[启用 HTML 捕获工具](#)的说明在浏览器中启用 HTML 捕获工具。
7. 捕获从此点发往问题 URL 的序列。
8. 按键盘上的 **Ctrl+Print Screen** 以捕获屏幕截图。
9. 停止 HTML 捕获工具。
10. 当您使用 Ipsec 或 SSL VPN 会话通过 ASA 直接连接到 URL 时，请执行相同的第 1 步至第 9 步；或是直接连接相同 LAN 网段（如果可能），然后将数据发送到 TAC 以供分析。

### [ASA 版本 8.0 无客户端](#)

本部分介绍用于 ASA 版本 8.0 和所有过渡版本的故障排除技术。

在此版本中，如果无法通过无客户端 SSL VPN 使用复杂的 URL 或应用程序，则可以考虑使用其他选项（例如使用智能隧道）。有关智能隧道的详细信息，请参阅[配置智能隧道访问](#)。

您也可以考虑使用应用程序访问端口转发或使用代理旁路。有关这些替代方案的详细信息，请参阅[配置应用程序访问](#)和[使用代理旁路](#)。

在多数情况下，如果 Internet Explorer 无法访问可以通过无客户端 SSL VPN 访问的 URL，则使用其他浏览器也将无法访问。

为确保此行为与客户端 PC 或操作系统无关，请从其他位置使用另一个客户端进行访问。您还可以测试 Ipsec 或 SSL VPN 客户端的使用。

请确保按照“在浏览器中启用 WebVPN 的 Cookie”的说明将 ASA 包含到[浏览器可信区域](#)中，并按照[启用 Cookie](#)的说明启用 Cookie。

如果应用程序遇到无客户端内容转换引擎 (CTE/rewriter) 的问题，您可以修改此应用程序的书签以启用“智能隧道”选项，如下图所示：

**Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks**

Configure bookmark lists that the security appliance displays on the SSL VPN portal page.

+ Add **Edit** Delete + Import Export

Bookmarks

Template  
Test\_Sites

Edit Bookmark List

Bookmark List Name: Test\_Sites

Name	URL	Add
Hotmail	http://www.hotmail.com	<b>Edit</b>
Yahoo Mail	http://www.mail.yahoo.com	

Edit Bookmark Entry

Bookmark Title: Hotmail

URL Value: http :// www.hotmail.com

**Advanced Options**

Subtitle:

Thumbnail: -- None --

URL Method :  Get  Post

Enable Favorite Option:  Yes  No

**Enable Smart Tunnel Option:  Yes  No**

为书签启用此选项不需要其他额外的配置。与端口转发类似，您可以通过单击书签打开一个新窗口，以使用智能隧道传递应用程序流量并避免重写问题，这也是一种简单的办法。

当您为 TCP Winsock 32 应用程序（例如 RDP）使用此功能时，则要求管理员识别要通过智能隧道

使用的进程。例如，RDP 使用 mstsc.exe 进程；您可以为此进程创建一个简单的智能隧道条目。

更复杂的应用程序可能产生多个进程。从 Webvpn 门户页中，选择 **Application Access** 面板。当它装载时，*allowed applications* 列表将连接到网络的专用部分。

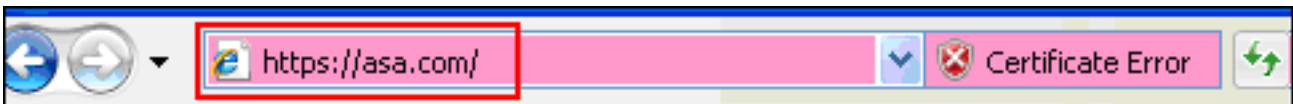
如果此过程仍失败，请执行以下步骤以采集必要信息，然后打开 TAC 案例。

1. 按照[清除浏览器缓存](#)的说明清除浏览器缓存。
2. 按照[清除 Java 缓存](#)的说明清除 Java 缓存。
3. 按照[配置缓存](#)的说明在 ASA 上禁用 Webvpn 缓存。
4. 如果存在 Java 小程序，请按照[启用 Java 小程序调试选项](#)的说明在小程序窗口中使用调试级别 5。
5. 通过无客户端 SSL VPN 登录 ASA。
6. 在问题 URL 之前的 URL 上，按照[启用 HTML 捕获工具](#)的说明在浏览器中启用 HTML 捕获工具。
7. 捕获从此点发往问题 URL 的序列。
8. 按键盘上的 **Ctrl+Print Screen** 以捕获屏幕截图。
9. 停止 HTML 捕获工具。
10. 当您使用 Ipsec 或 Any Connect SSL 会话通过 ASA 直接连接到 URL 时，请执行相同的第 1 步至第 9 步；或是直接连接相同 LAN 网段（如果可能），执行以下步骤，然后将数据发送到 TAC 以供分析。

## 步骤

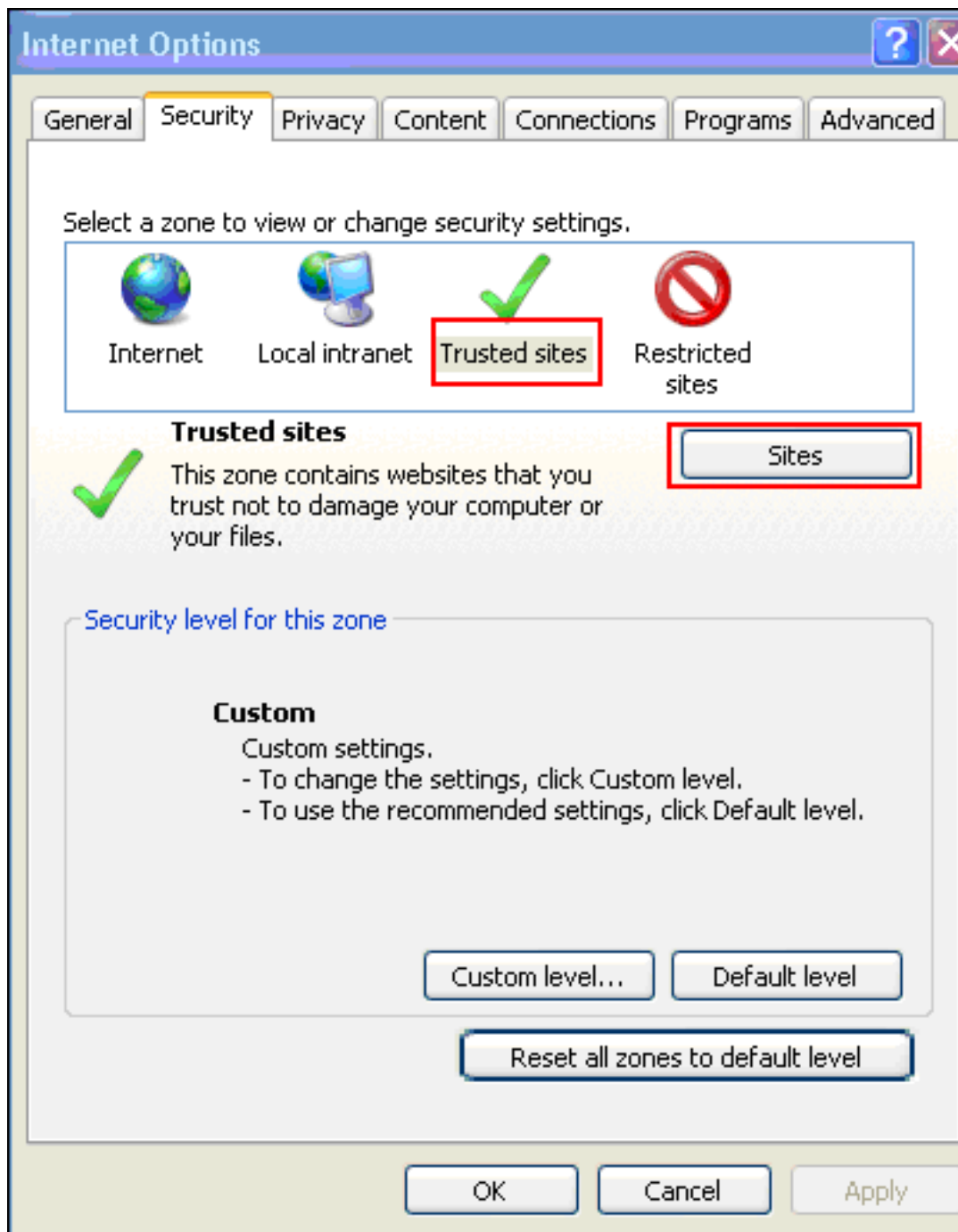
### [将 ASA 添加为可信站点](#)

当您在 Internet Explorer 中访问 ASA 时，如果此站点未包含在可信站点列表中，您将收到一条验证错误。



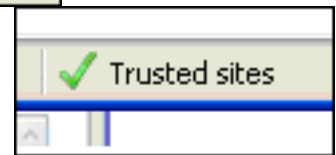
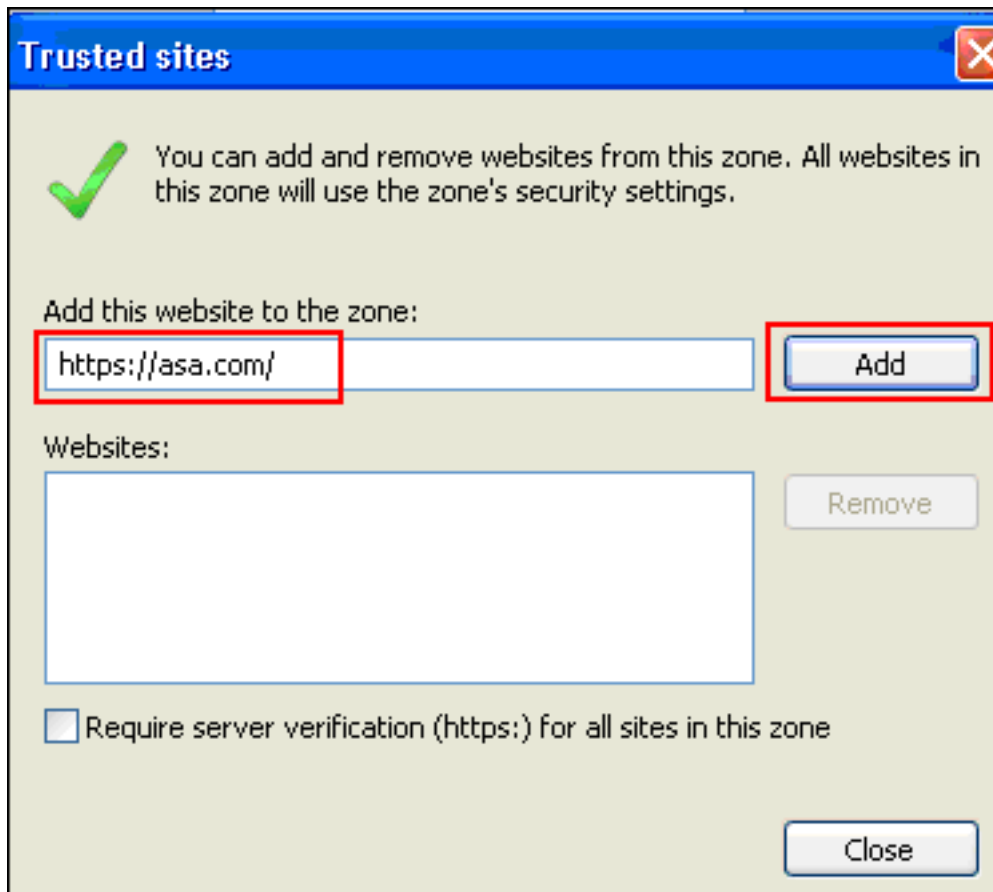
执行以下步骤以将 ASA 添加为可信站点：

1. 在 Internet Explorer 中，选择 **工具 > Internet 选项**。
2. 单击 **安全选项卡**，然后选择“可信站点”。



3. 单击**站点**。

4. 添加 ASA 的 https:// 地址，然后单击**添加**。



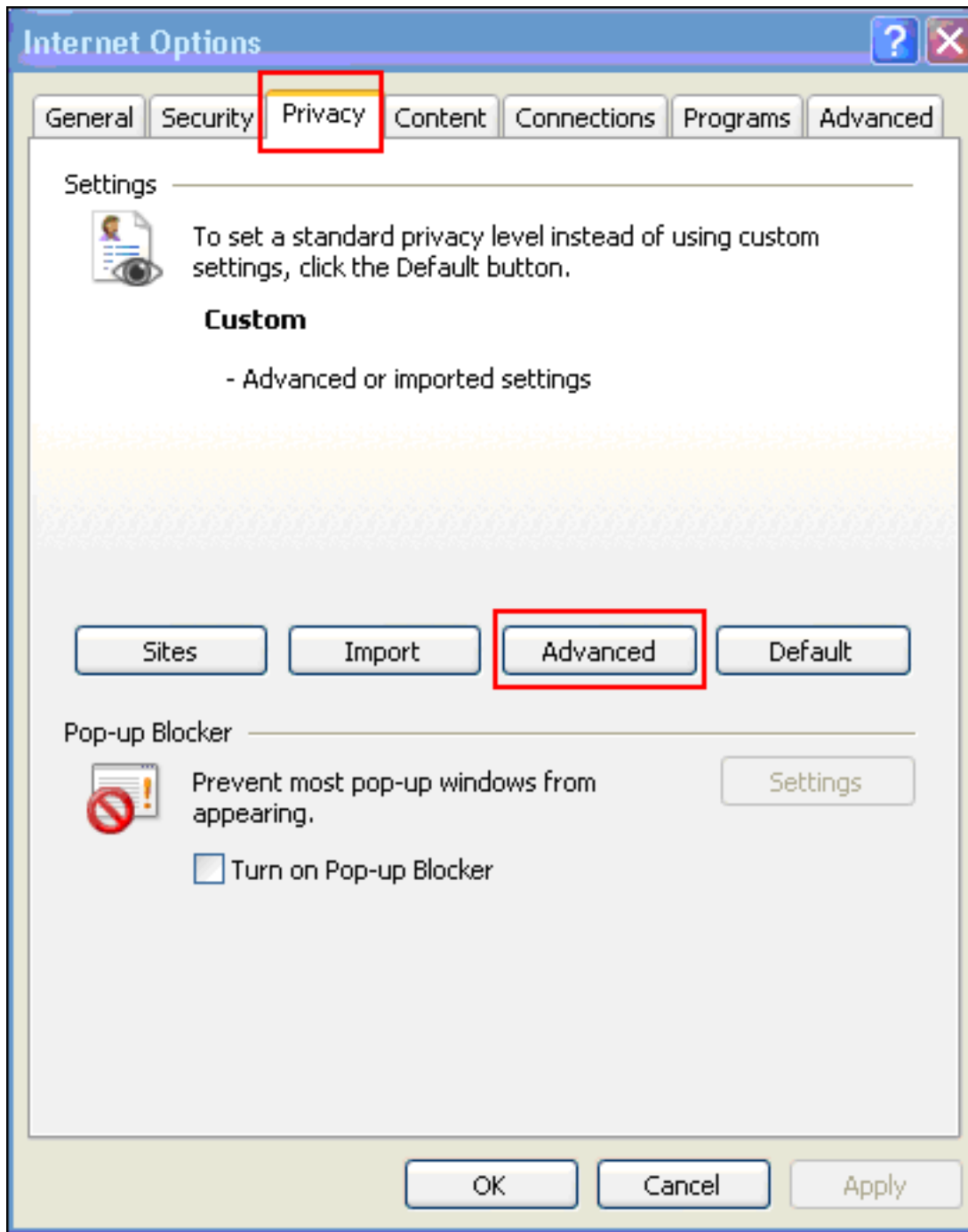
5. 添加站点后，“可信站点”图标将显示在 Internet Explorer 状态栏中。

**注意：**有关此过程的详细信息，请参阅[使用 Internet Explorer 6 安全设置](#)。

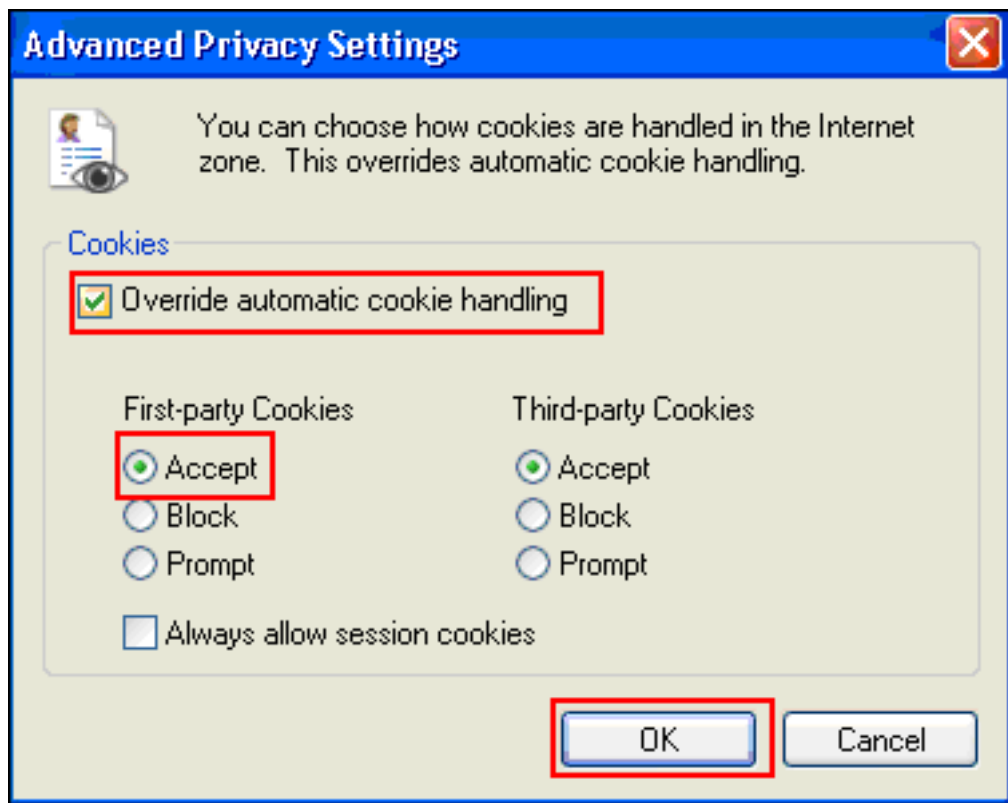
## 启用 Cookie

执行以下步骤以启用 Cookie：

1. 在 Internet Explorer 中，选择**工具 > Internet 选项**。
2. 单击**隐私**选项卡，然后单击“高级”。



3. 在“高级隐私设置”对话框中，选中替代自动 cookie 处理复选框，单击“接受”单选按钮，然后单



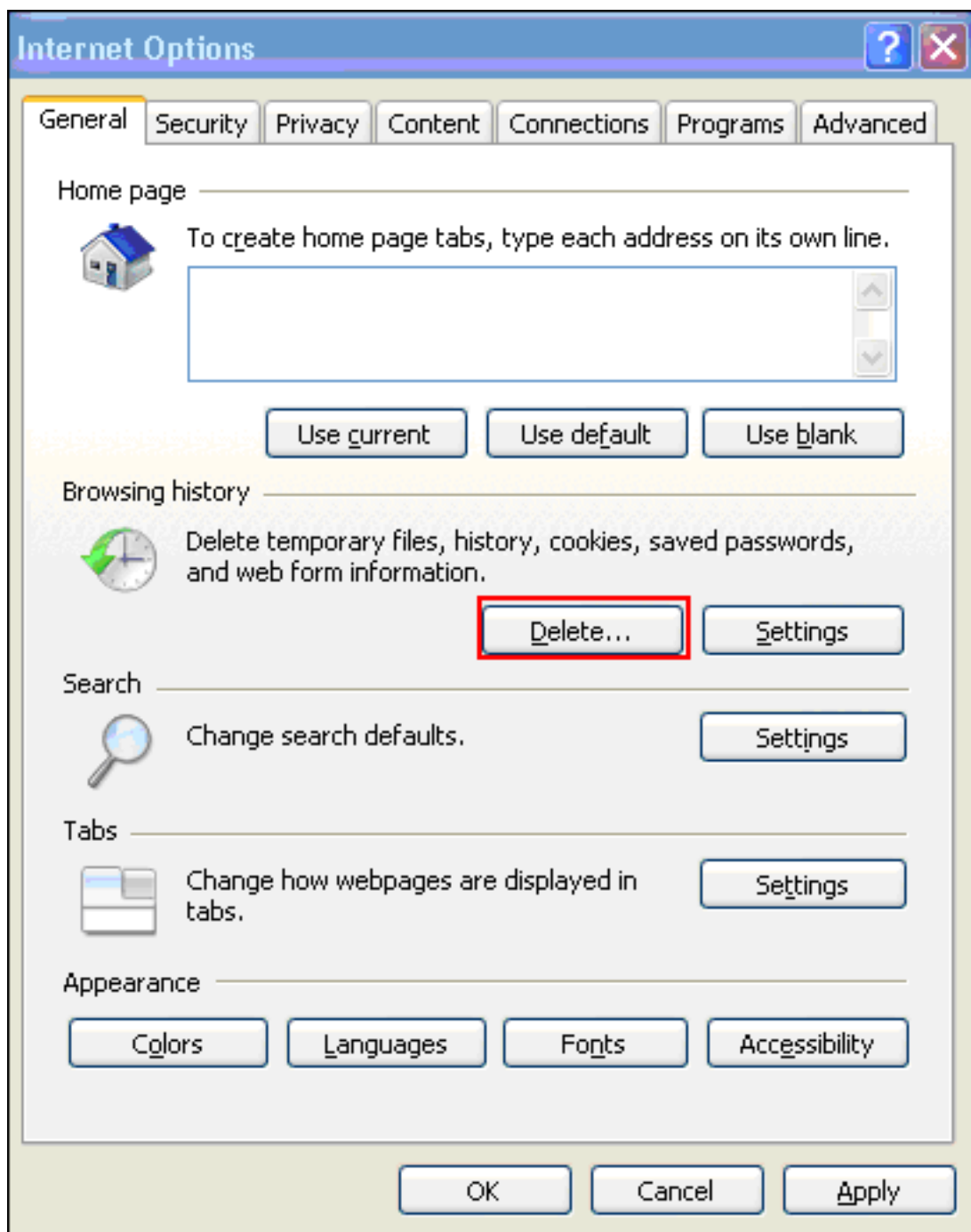
击“确定”。

## 清除浏览器缓存

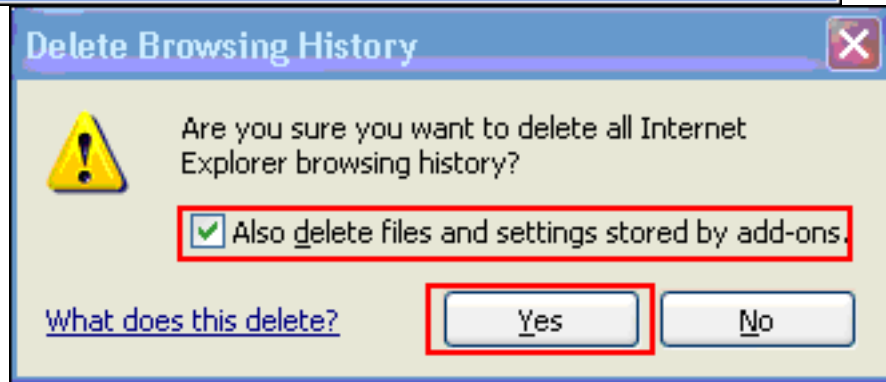
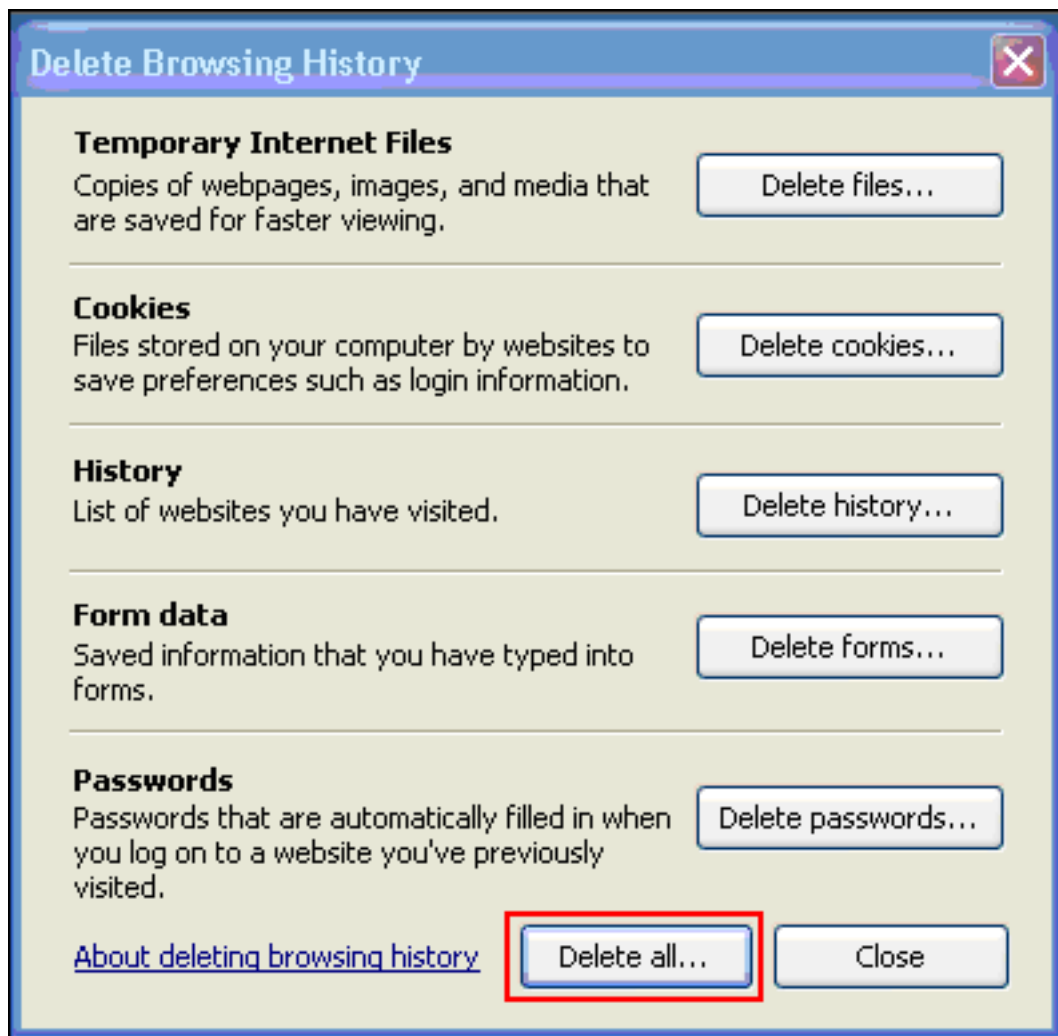
执行以下步骤以清除 Internet Explorer 的缓存：

1. 在 Internet Explorer 中，选择工具 > Internet 选项。





2. 在“常规”选项卡中，单击“浏览历史记录”部分中的删除。



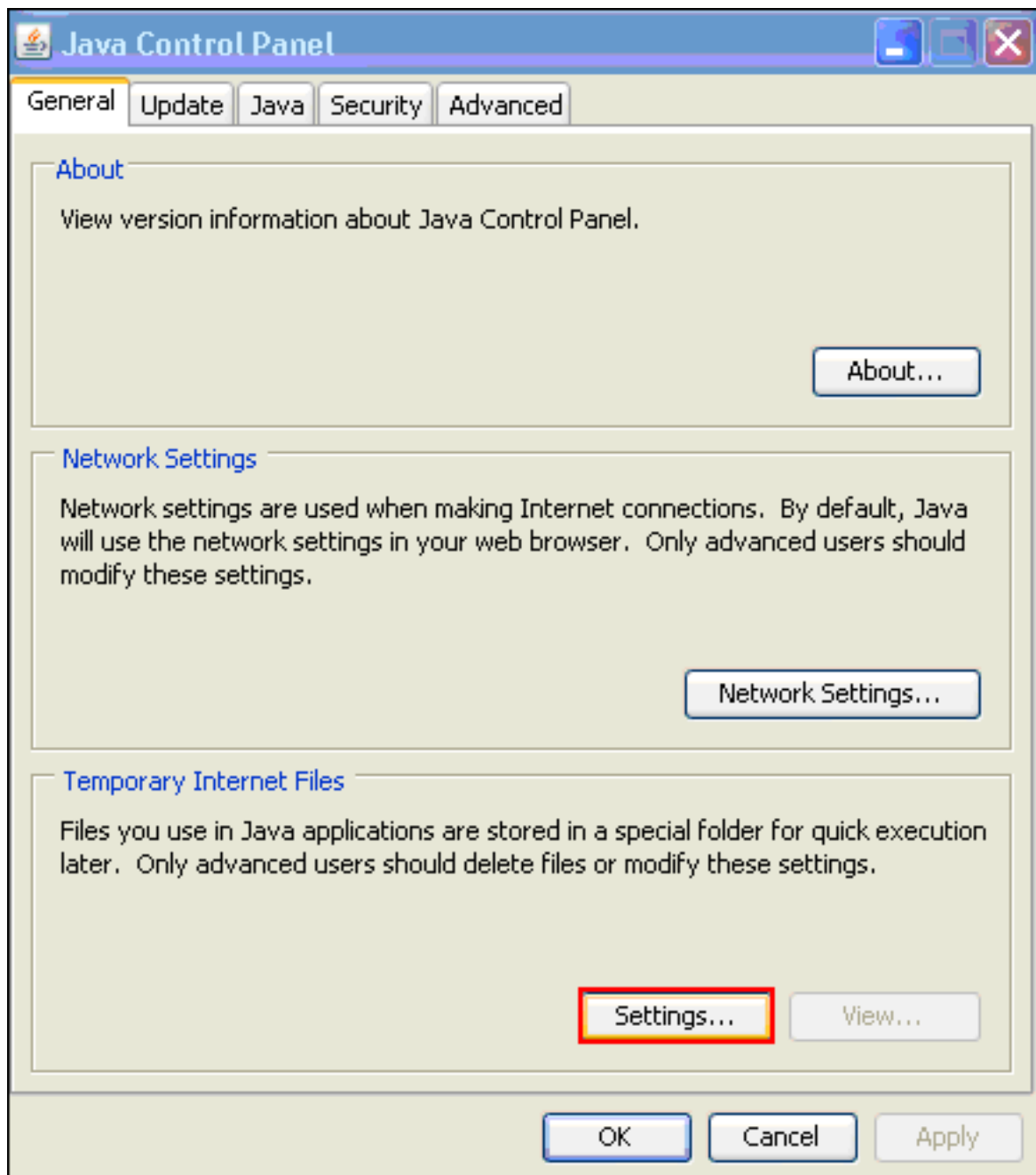
3. 单击**全部删除**。
4. 选中同时删除加载项存储的文件和设置复选框，然后单击“是”。
5. 清除缓存后，关闭所有浏览器实例，然后重新启动浏览器。

**注意：**要清除其他浏览器的缓存，请参阅[如何清除浏览器缓存（以提高其性能）？](#)

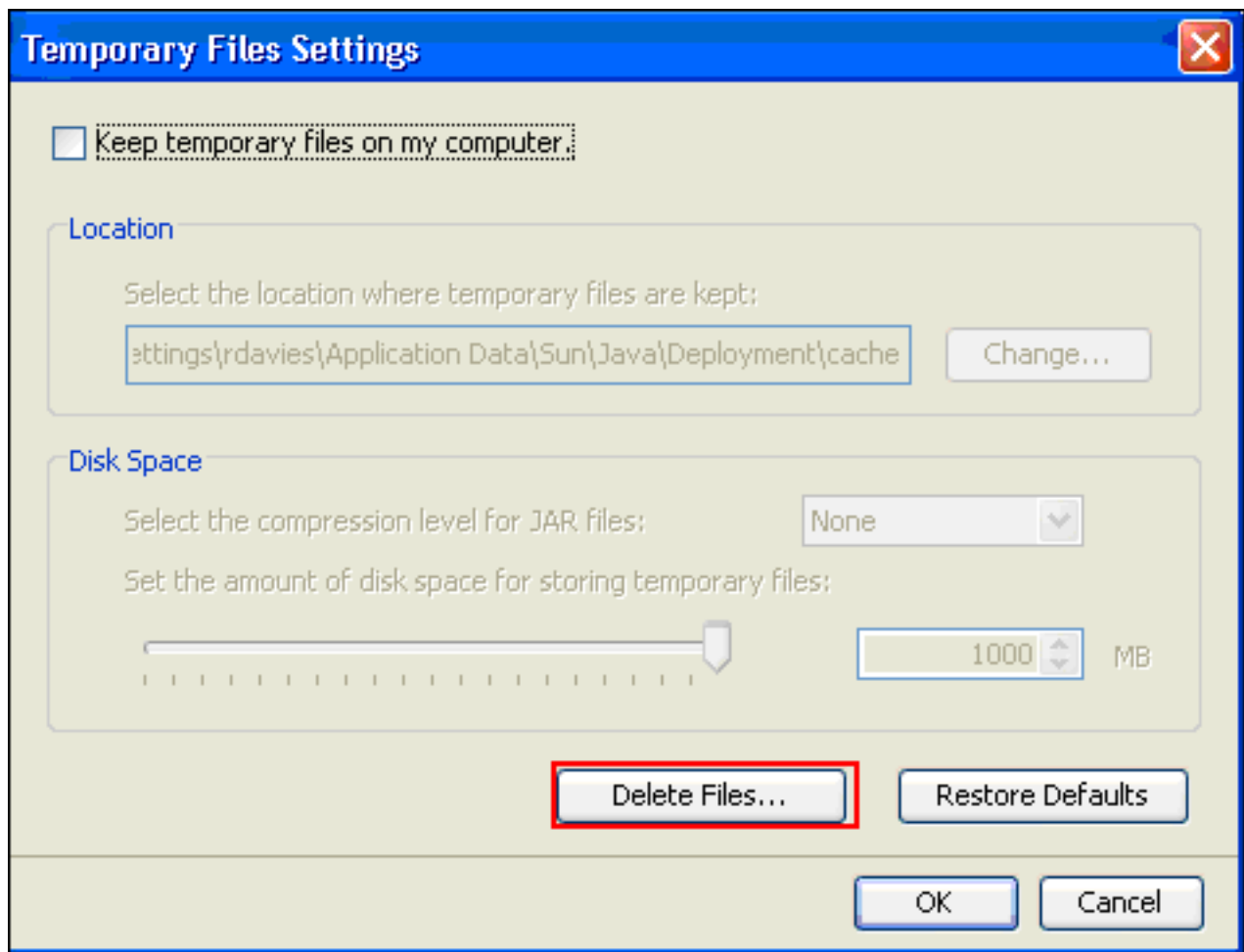
## 清除 Java 缓存

执行以下步骤以清除 Java 缓存：

1. 从 Windows“开始”菜单中选择**控制面板**。
2. 双击 **Java**。



3. 单击设置。
4. 单击删除文件。

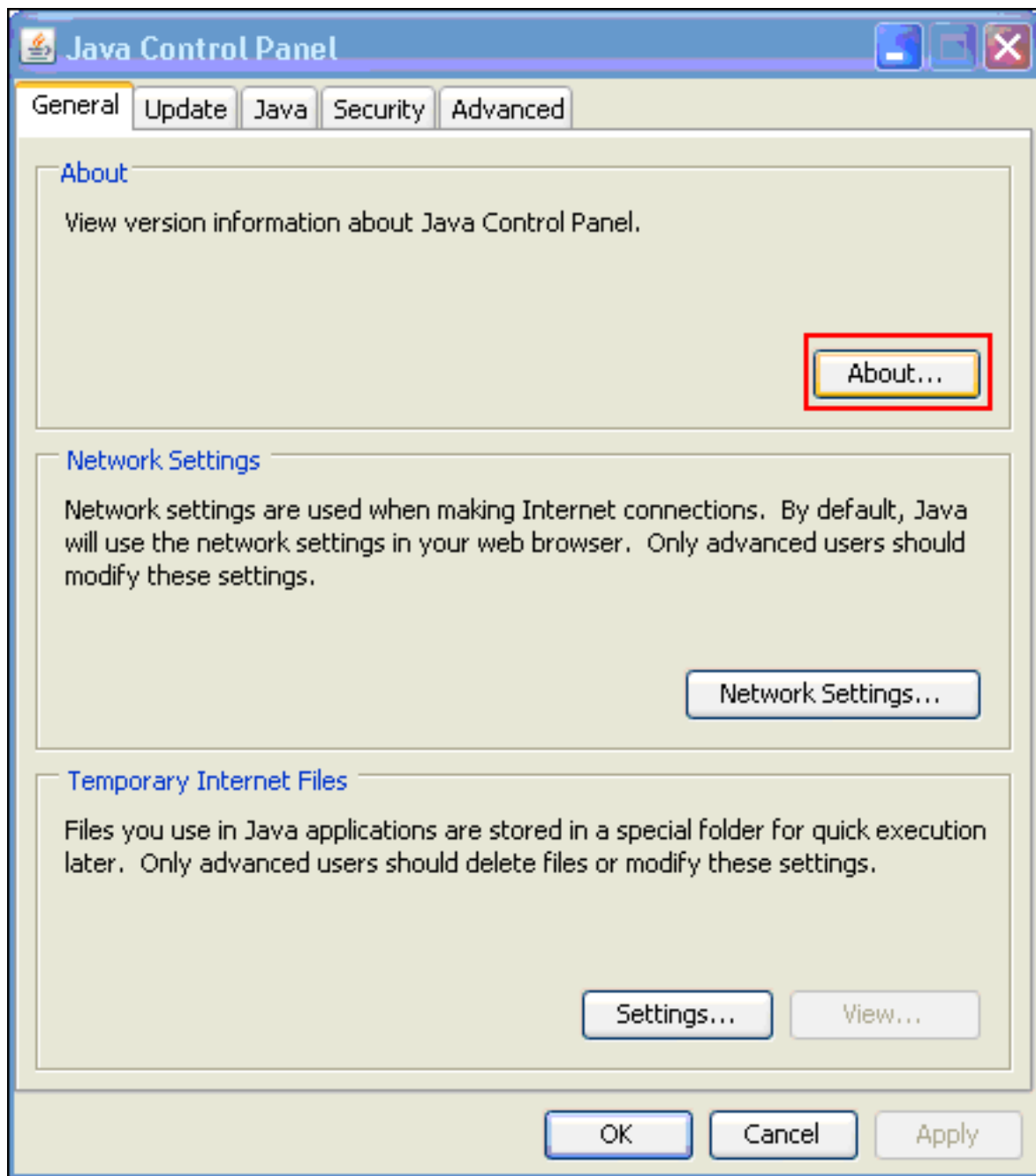


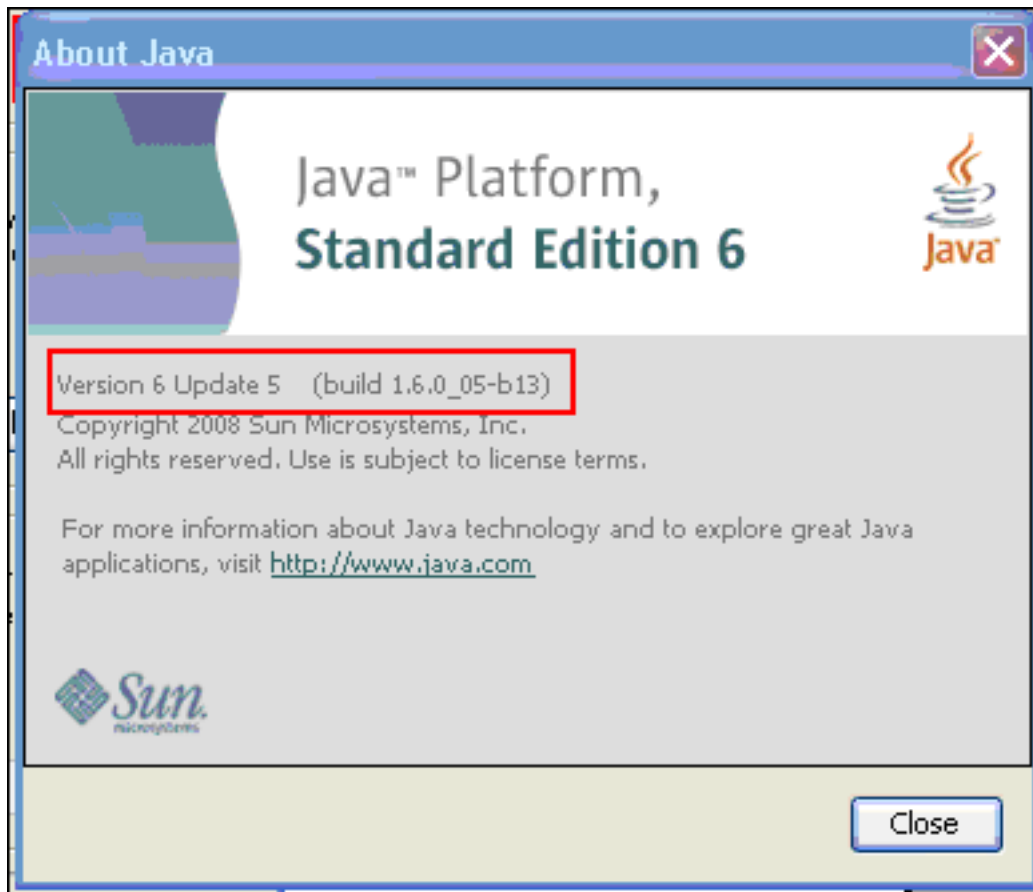
**注意：** 有关此过程的详细信息，请参阅[如何清除 Java 缓存？](#)。

## [启用 Java 小程序调试选项](#)

执行以下步骤以启用 Java 小程序调试选项：

1. 确保启用 Java 1.4 或更高版本：从 Windows“开始”菜单中选择**控制面板**。双击 **Java**。单击**关于**，然后检查版本号。

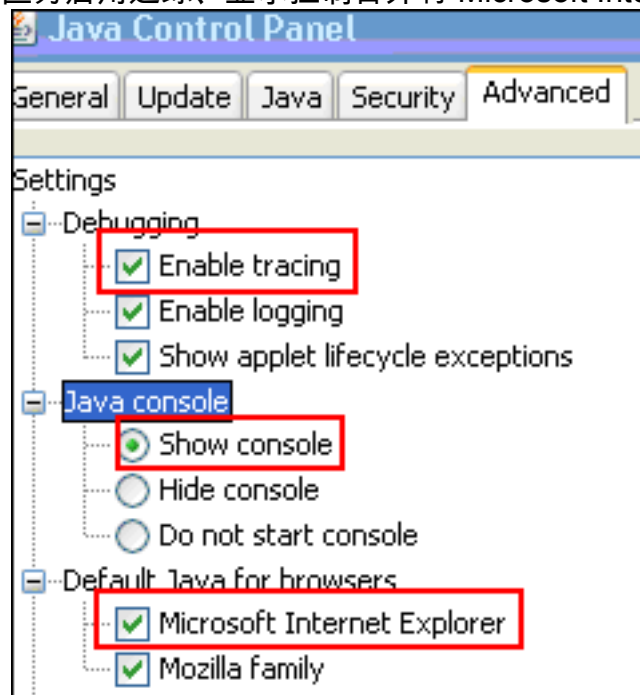




注意：您可以从

<http://java.com/en/> 下载 Java 更新。

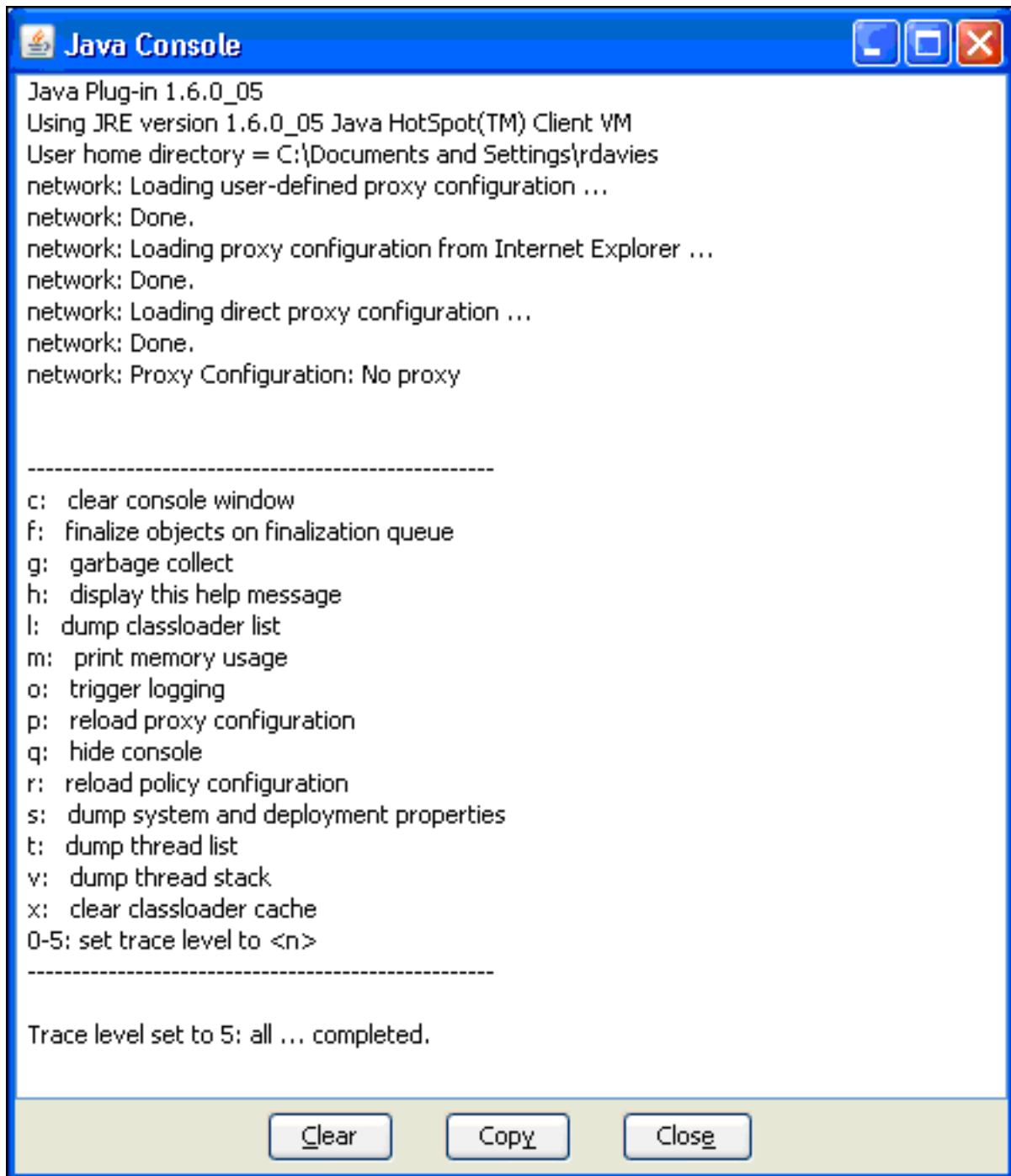
2. 确保将 Java 配置为启用追踪、显示控制台并将 Microsoft Internet Explorer 设置为默认浏览器



，如下图所示：

3. 确保按照[清除 Java 缓存](#)的说明清除 Java 缓存。

4. 在 Internet Explorer 中，选择工具 > JAVA 控制台以打开 Java 调试窗口。



5. 打开 JAVA 控制台调试窗口后，按 **5** 以设置跟踪级别当访问包含 Java 小程序的 URL 时，在此窗口中将会捕获此活动。
6. 单击**复制**以复制信息。

## 启用 HTML 捕获工具

有多种 HTML 捕获工具可用于收集数据，其中一些工具已在此处列出。在客户端 PC 上安装以下一种 HTML 捕获工具以用于练习收集数据：

- [HttpWatch](#)
- [IE Inspector](#)
- [Debug Proxy](#)

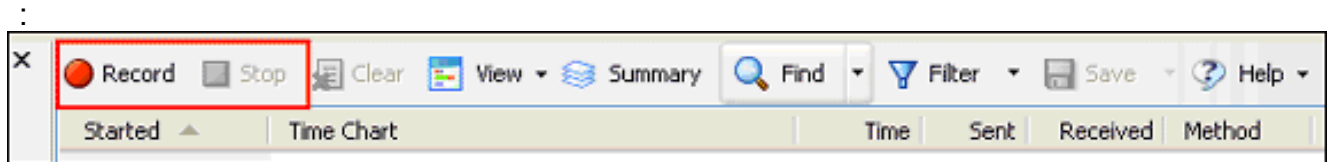
**注意：**本过程使用 HTTPWatch 应用程序。

安装此应用程序后，请执行以下步骤：

1. 按 Shift+P+F+2 或单击浏览器窗口中的图标以启用 HTTPWatch。



2. 启用此应用程序后，浏览器窗口底部将会出现一个嵌入式窗口，如下图所示



3. 单击**记录**以记录数据；单击**停止**以停止记录。

**注意：** 推荐使用HttpWatch 7.x为了记录数据。

## 相关信息

- [ASA 上的无客户端 SSL VPN \(WebVPN\) 配置示例](#)
- [Cisco ASA 5500 系列自适应安全设备](#)
- [技术支持和文档 - Cisco Systems](#)