# ASA Clientless SSL VPN (WebVPN) Problemen oplossen Technische opmerking

## Inhoud


Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Conventies
Probleemoplossing
ASA versie 7.1/7.2 Clientloos
ASA versie 8.0 Clientloos
Procedures
ASA als betrouwbare website toevoegen
Cookies inschakelen
De browser wissen
Java-cache wissen
Debugopties voor Java-applicatie inschakelen
HTML-opnametools inschakelen
Gerelateerde informatie


## Inleiding

Dit document maakt een lijst van de Clientless SSL VPN (WebVPN) hoe de problemen worden opgelost die voor ASA versies 7.1, 7.2 en 8.0 zijn goedgekeurd. Er zijn belangrijke vooruitgang tussen deze releases die verschillende technieken voor het oplossen van problemen vereisen om te worden goedgekeurd.

## Voorwaarden

### Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

### Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco 5500 Series ASA die softwareversie 7.1 of hoger uitvoeren.

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

### Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

## Probleemoplossing

De voorwaarde voor het oplossen van clientloze SSL VPN-verbindingen (WebVPN) op de ASA is om zichtbaarheid in zowel de clientervaring te verkrijgen via screenshots als de HTML-opnamemiddelen en dan deze te vergelijken met dezelfde informatie wanneer direct verbonden met de URL/Application die benaderd wordt.

### ASA versie 7.1/7.2 Clientloos

In dit gedeelte worden de technieken voor het opsporen en verhelpen van problemen beschreven voor ASA versies 7.1/7.2 en alle toepassingen tot en met, maar niet met, de 8.0-release.

In deze release als de complexe Java/Javascript-functies problemen hebben, kunnen andere opties (zoals het verzenden van de applicatie-toegangspoort of het gebruik van proxy-bypass) overwogen worden. Raadpleeg Toepassingstoegang configureren en Proxy-bypass gebruiken voor meer informatie over deze alternatieven.

In de meeste scenario's, als de URL die door Clientless SSL VPN wordt benaderd voor Internet Explorer faalt, zal deze ook voor een andere browser falen.

Om ervoor te zorgen dat dit niet afhankelijk is van de PC of het besturingssysteem van de cliënt, gebruikt u een andere client vanaf een andere locatie. Het gebruik van een IPsec of SSL VPN-client kan ook worden getest.

Zorg ervoor dat de ASA in de browser Trusted Zone is opgenomen zoals beschreven in Cookies op Browsers voor WebVPN en dat de koekjes zijn ingeschakeld zoals beschreven in Enable Cookies.

Als het proces nog steeds mislukt, voert u deze stappen uit om de benodigde informatie te verzamelen en vervolgens een TAC-case te openen.

1. Schakel de browser cache uit zoals beschreven in de browser Cache.
2. Schakel de Java-cache uit zoals in het Java-caches is beschreven.
3. Schakel het WebVPN cache op de ASA uit zoals beschreven in Caching configureren.
4. Als er een Java-applet aanwezig is, kunt u niveau 5 debug in het applet-venster gebruiken zoals wordt beschreven in Afbeeldingsopties voor Java inschakelen.
5. Log in op de ASA via Clientless SSL VPN.
6. Bij de URL net vóór de problematische URL, schakelt u een HTML-opnamegereedschap in de browser in zoals beschreven in de HTML Capture Gereedschappen inschakelen.
7. Leg de opeenvolging van dit punt aan de problematische URL vast.
8. Druk op **Ctrl+**Scherm op het toetsenbord om een screenshot vast te leggen.

9. Stop het HTML-opnamegereedschap.
10. Voer dezelfde stappen 1 tot en met 9 uit wanneer u rechtstreeks via een IPsec- of SSL VPN-sessie verbinding maakt met de URL via de ASA of rechtstreeks verbinding maakt met hetzelfde LAN-segment (indien mogelijk) en de gegevens naar TAC stuurt voor analyse.

## ASA versie 8.0 Clientloos

In dit gedeelte worden de technieken voor het oplossen van problemen beschreven die voor ASA versies 8.0 en alle doelstellingen worden gebruikt.

In deze release als complexe URL's of toepassingen moeite hebben met clientloze SSL VPN zijn andere opties (zoals het gebruik van slimme tunnels) een krachtig alternatief. Zie Smart Tunnel access configureren voor meer informatie over slimme tunnels.

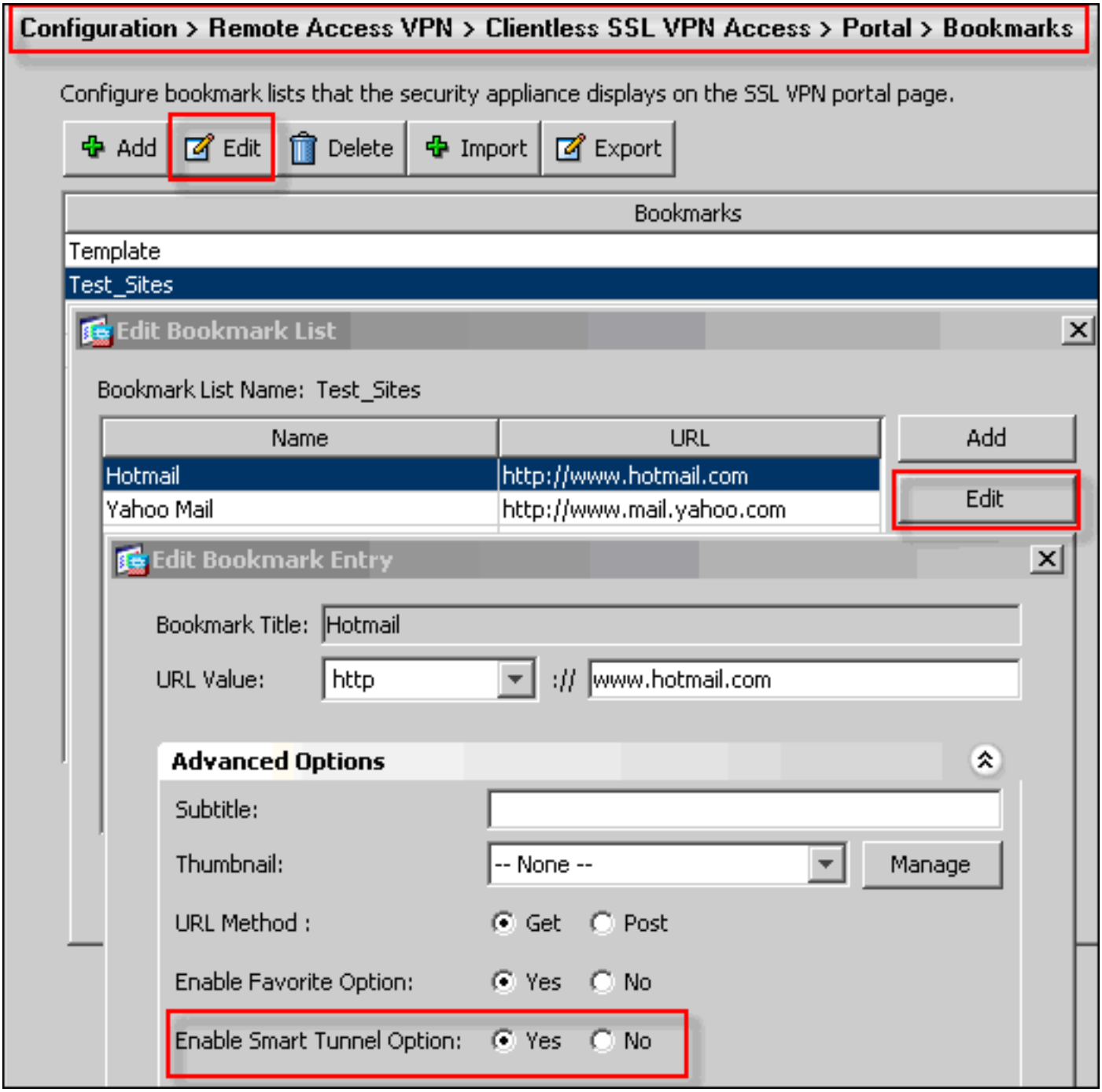
U kunt ook overwegen om poort te gebruiken voor toegang tot de toepassing of proxy-bypass te gebruiken. Raadpleeg Toepassingstoegang configureren en Proxy-bypass gebruiken voor meer informatie over deze alternatieven.

In de meeste scenario's, als de URL die door Clientless SSL VPN wordt benaderd voor Internet Explorer faalt, zal deze ook voor een andere browser falen.

Om ervoor te zorgen dat dit niet afhankelijk is van de PC of het besturingssysteem van de cliënt, gebruikt u een andere client vanaf een andere locatie. Het gebruik van een IPsec of SSL VPN-client kan ook worden getest.

Zorg ervoor dat de ASA in de browser Trusted Zone is opgenomen zoals beschreven in Cookies op Browsers voor WebVPN en dat de koekjes zijn ingeschakeld zoals beschreven in Enable Cookies.

Als een toepassing een probleem ervaart met de clientloze motor van de contenttransformatie (CTE/rewriter), kunt u de favoriet voor die toepassing wijzigen om de Smart Tunnel optie in te schakelen zoals in deze afbeelding wordt getoond:




Het inschakelen van deze optie voor een favoriet vereist geen extra configuratie. Vergelijkbaar met havenverzending is dit een andere handige optie om op een favoriet te klikken om een nieuw venster te openen dat de slimme tunnel gebruikt om toepassingsverkeer door te geven en om herschrijfkwesties te vermijden.

Wanneer u deze functie gebruikt voor TCP Winsock 32-toepassingen (zoals RDP), moet de beheerder de proces(s) identificeren die gebruikt moeten worden door slimme tunnels. RDP gebruikt bijvoorbeeld het proces mstsc.exe; voor dit proces kan een eenvoudige slimme tunnelingang worden gecreëerd .

ingewikkelder toepassingen kunnen meerdere processen veroorzaken. Kies in het WebVPN Portal Page het paneel **Toepassingstoegang**. Zodra het geladen is, kan de lijst met *toegestane toepassingen* verbinding maken met de privékant van het netwerk.

Als het proces nog steeds mislukt, voert u deze stappen uit om de benodigde informatie te verzamelen en vervolgens een TAC-case te openen.

1. Schakel de browser cache uit zoals beschreven in de browser Cache.
2. Schakel de Java-cache uit zoals in het Java-caches is beschreven.
3. Schakel het WebVPN cache op de ASA uit zoals beschreven in Caching configureren.
4. Als er een Java-applet aanwezig is, kunt u niveau 5 debug in het applet-venster gebruiken zoals wordt beschreven in Afbeeldingsopties voor Java inschakelen.
5. Log in op de ASA via Clientless SSL VPN.
6. Bij de URL net vóór de problematische URL, schakelt u een HTML-opnamegereedschap in de browser in zoals beschreven in de HTML Capture Gereedschappen inschakelen.
7. Leg de opeenvolging van dit punt aan de problematische URL vast.
8. Druk op **Ctrl+**Scherm op het toetsenbord om een screenshot vast te leggen.
9. Stop het HTML-opnamegereedschap.
10. Voer de stappen 1 tot en met 9 uit wanneer u rechtstreeks verbinding maakt met de URL via een IPsec of een Any Connect SSL-sessie via de ASA of sluit rechtstreeks aan op hetzelfde LAN-segment (indien mogelijk), voltooi deze stappen en verstuur de gegevens naar TAC voor analyse

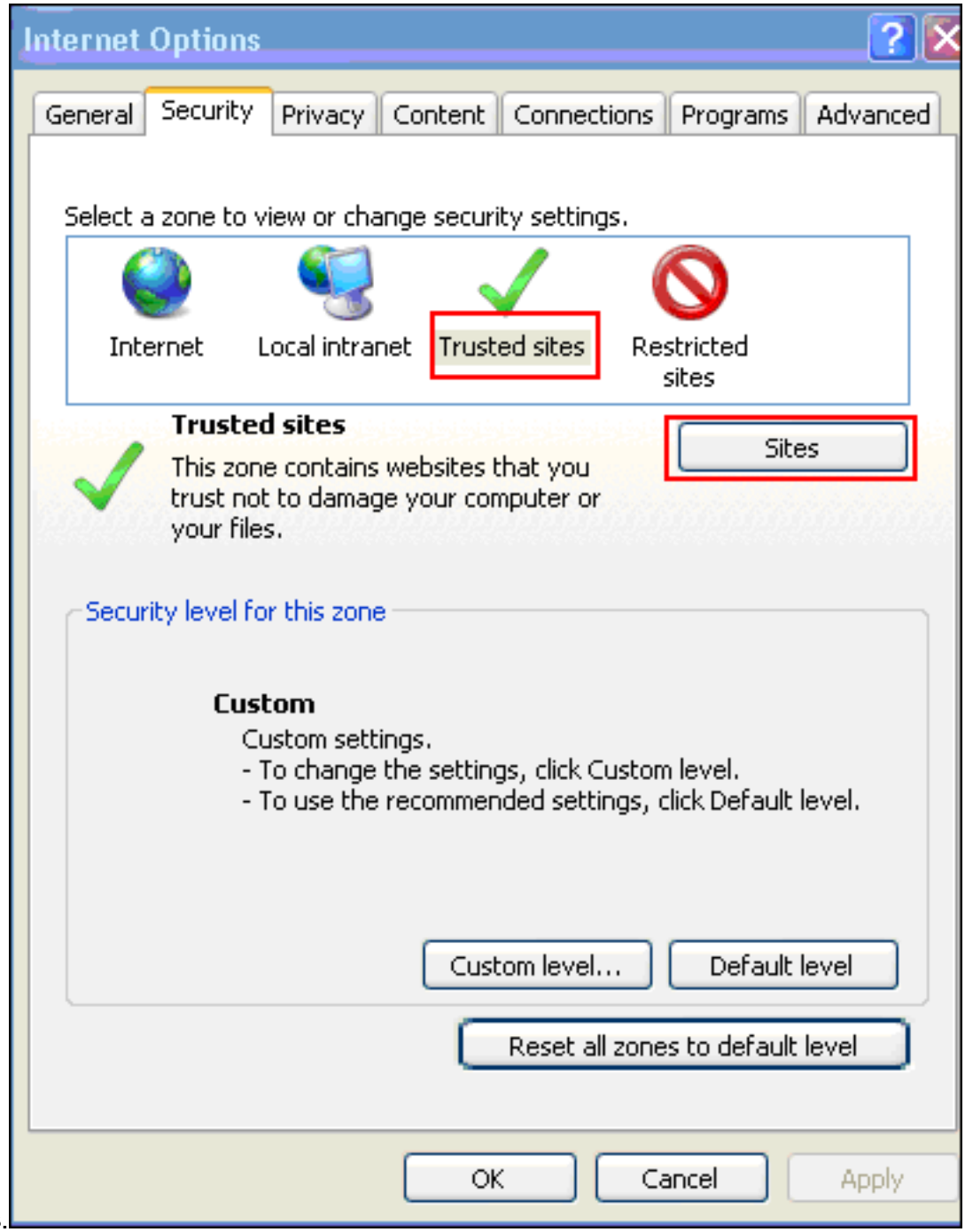
# Procedures

## ASA als betrouwbare website toevoegen

Wanneer u in Internet Explorer toegang hebt tot de ASA, ontvangt u een certificaatfout als de site niet als een vertrouwde site is opgenomen.

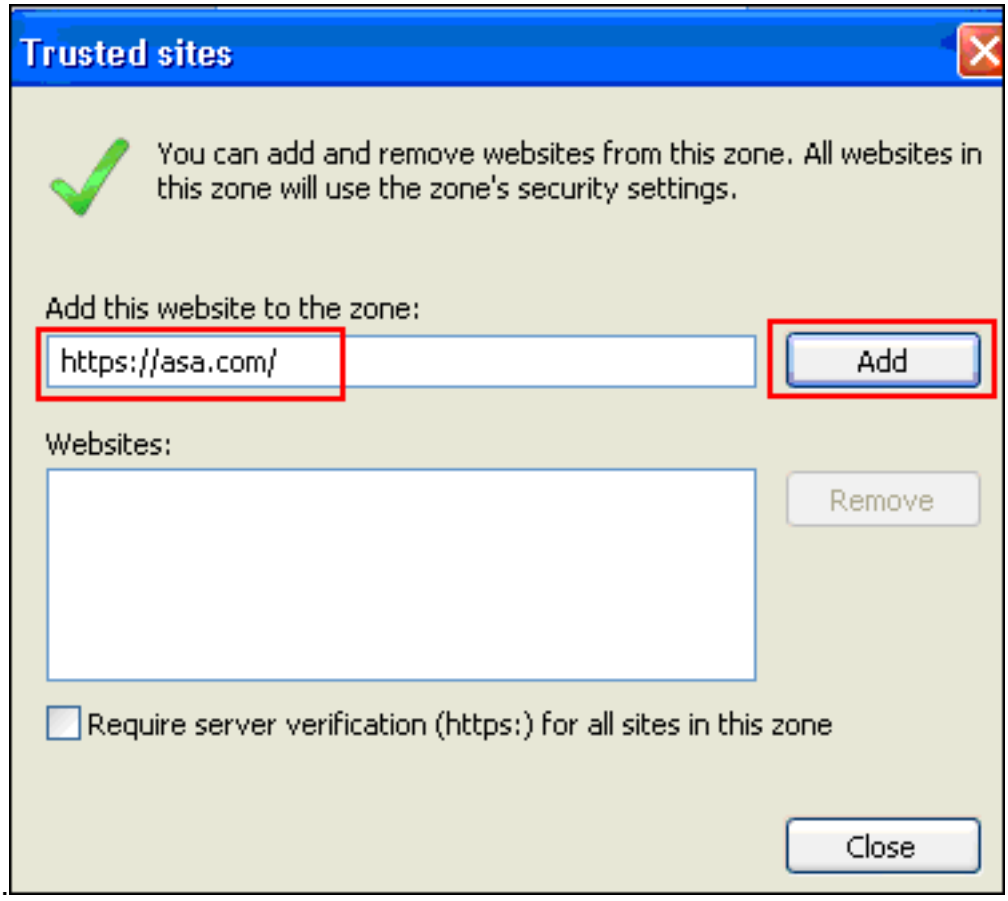

Voltooi deze stappen om de ASA als een vertrouwde site toe te voegen:

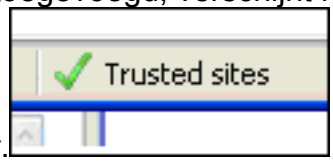
1. Kies in Internet Explorer **Gereedschappen > Internet-opties**.
2. Klik op het tabblad **Beveiliging** en kies **Vertaalde**




**sites**.

3. Klik op **Plaatsen**.
4. Voeg het https:// adres van de ASA toe, en klik

Add. 

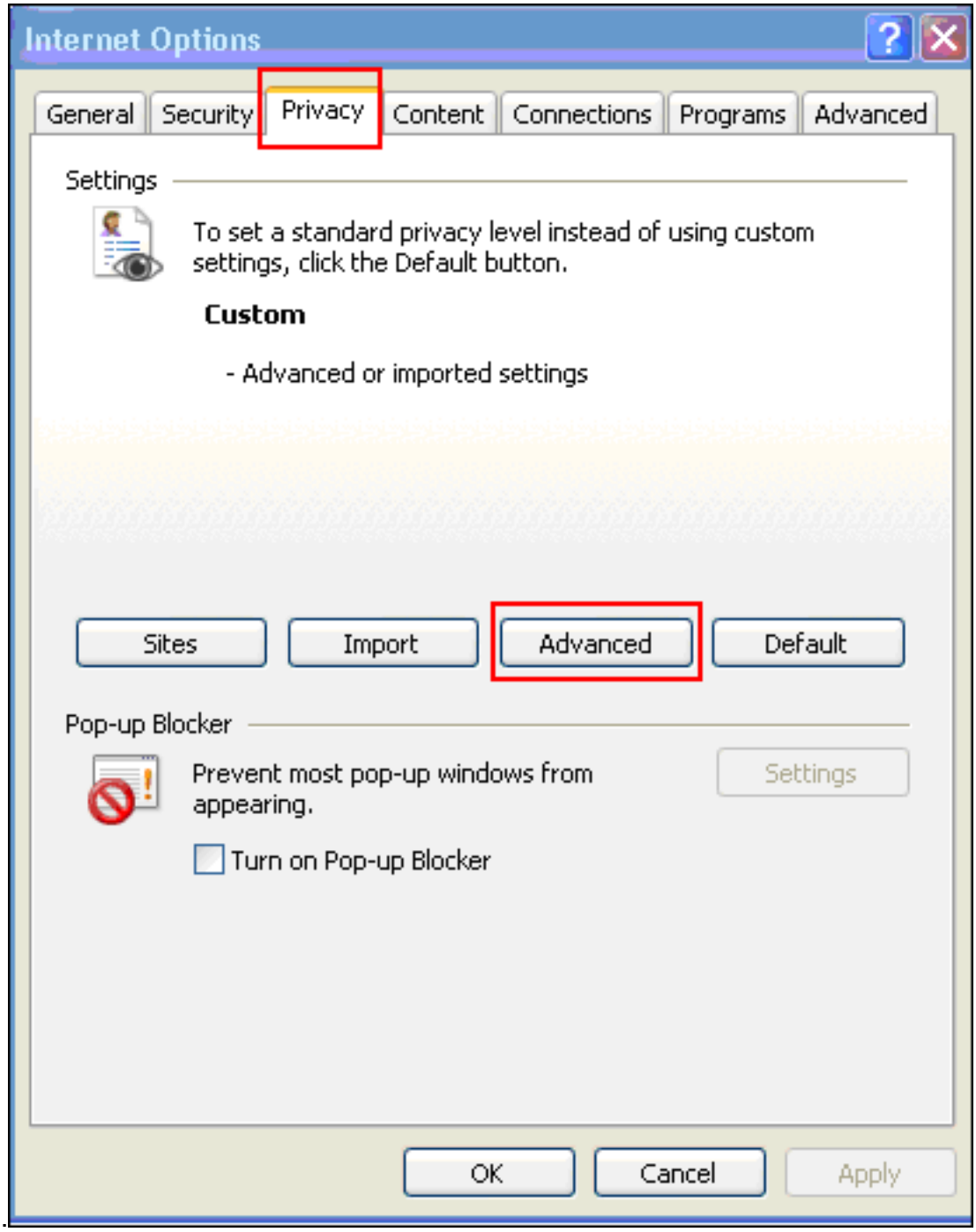

5. Zodra de site is toegevoegd, verschijnt het pictogram Betrouwbare sites in de statusbalk van Internet Explorer. 


**Opmerking:** Raadpleeg Werken met Internet Explorer 6 Beveiligingsinstellingen voor meer informatie over deze procedure.

## Cookies inschakelen

Voltooi deze stappen om koekjes in staat te stellen:

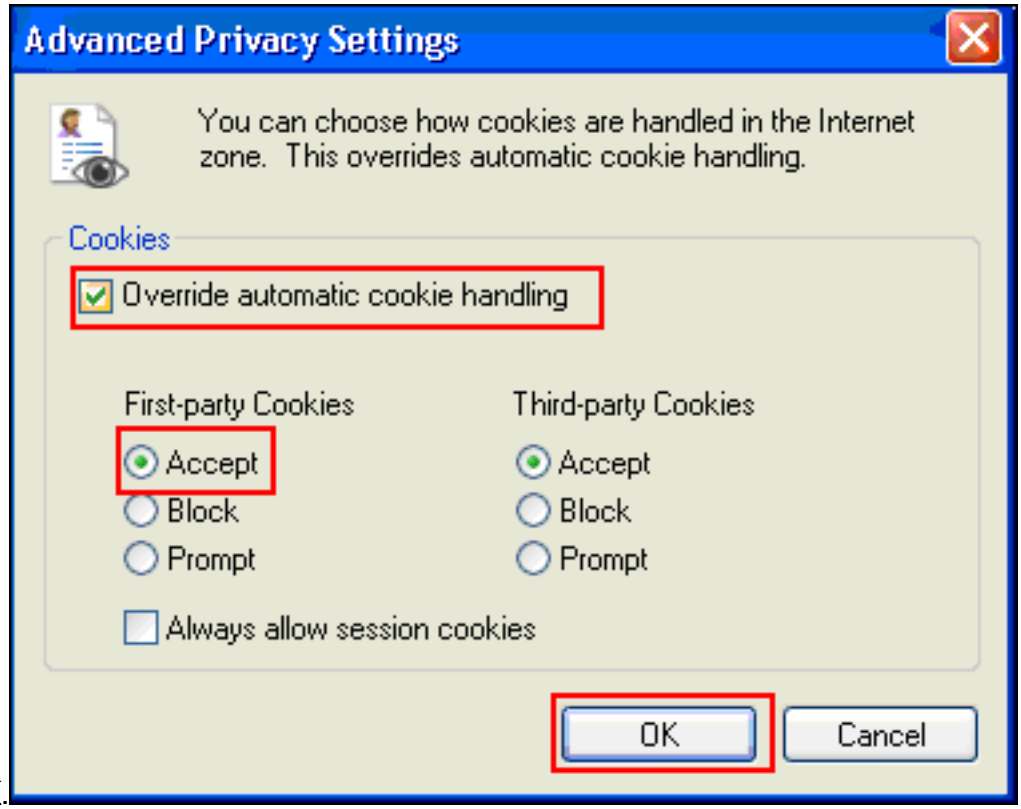
1. Kies in Internet Explorer **Gereedschappen > Internet-opties**.
2. Klik op het tabblad **Privacy** en klik vervolgens op




**Advanced**.

3. Selecteer in het dialoogvenster Geavanceerde Privacyinstellingen het dialoogvenster **Automatische** verwerking van **koekjes negeren**, klik op de radioknop **Accept** en klik op

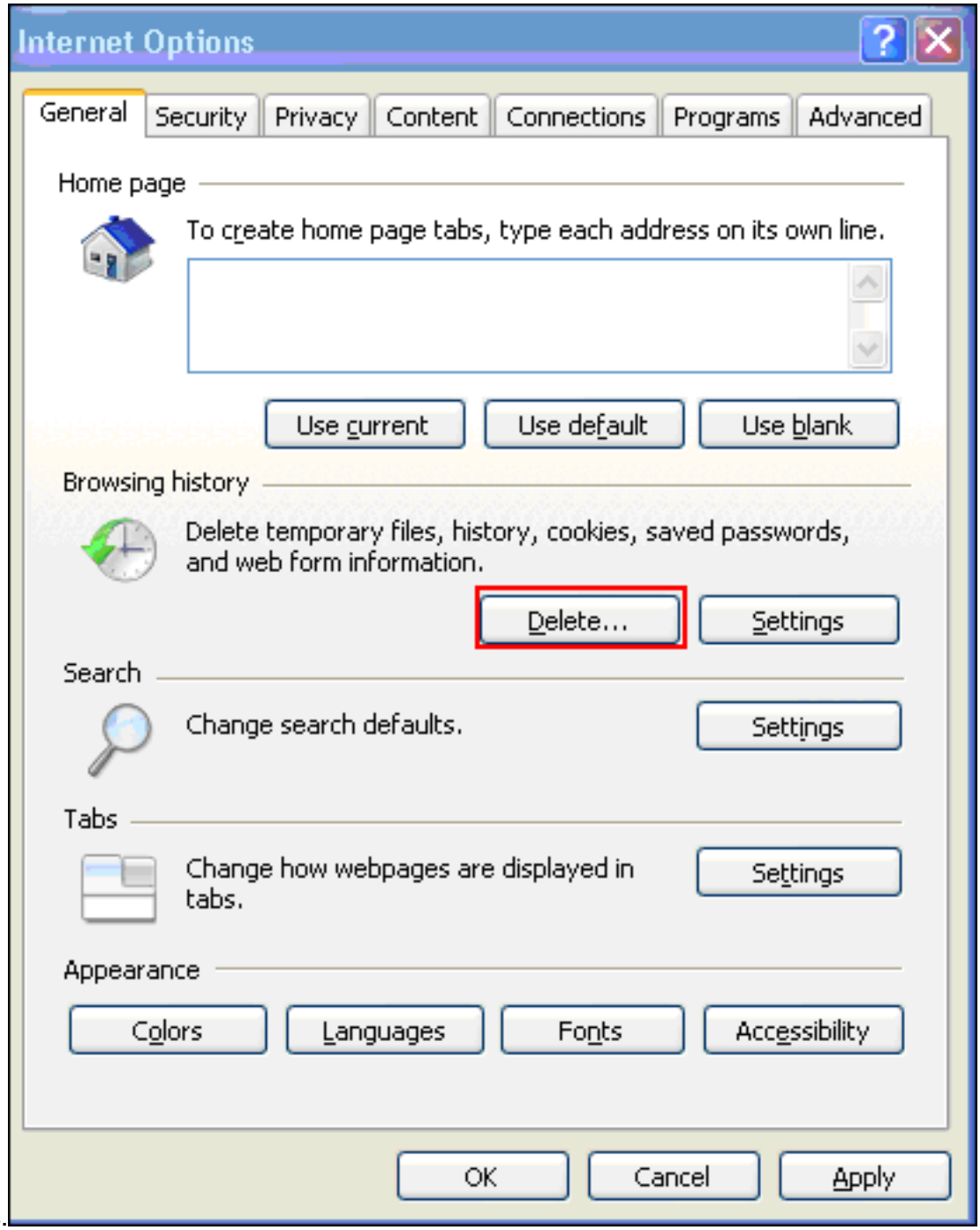
OK.




## De browser wissen

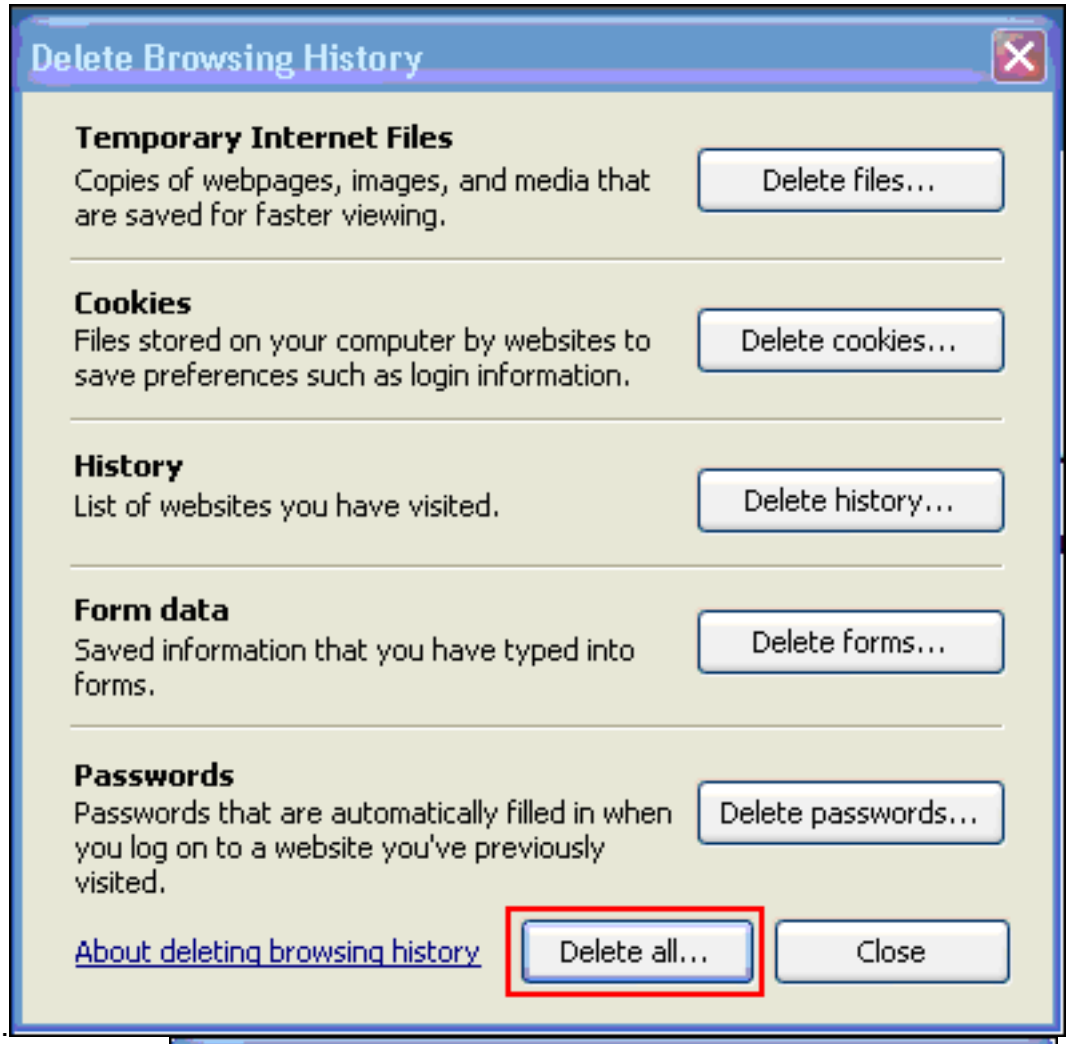
Voltooi deze stappen om de cache voor Internet Explorer te verwijderen:

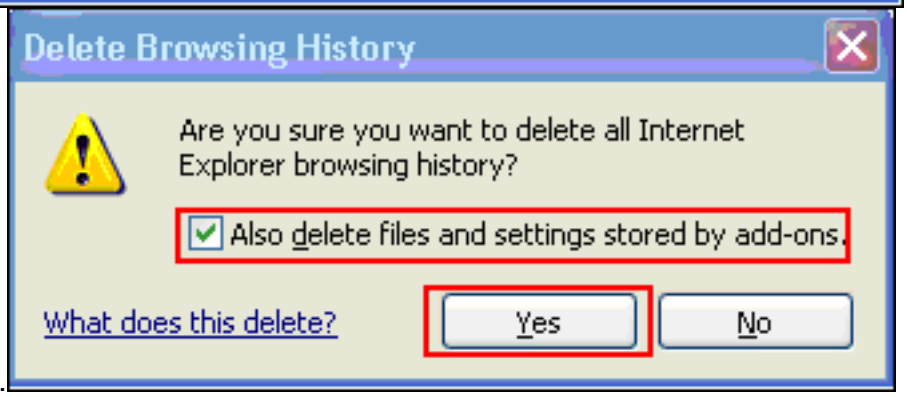
1. Kies in Internet Explorer **Gereedschappen > Internet-**




**opties**.

2. Op het tabblad Algemeen klikt u op **Verwijderen** in het gedeelte Bladeren

geschiedenis. 

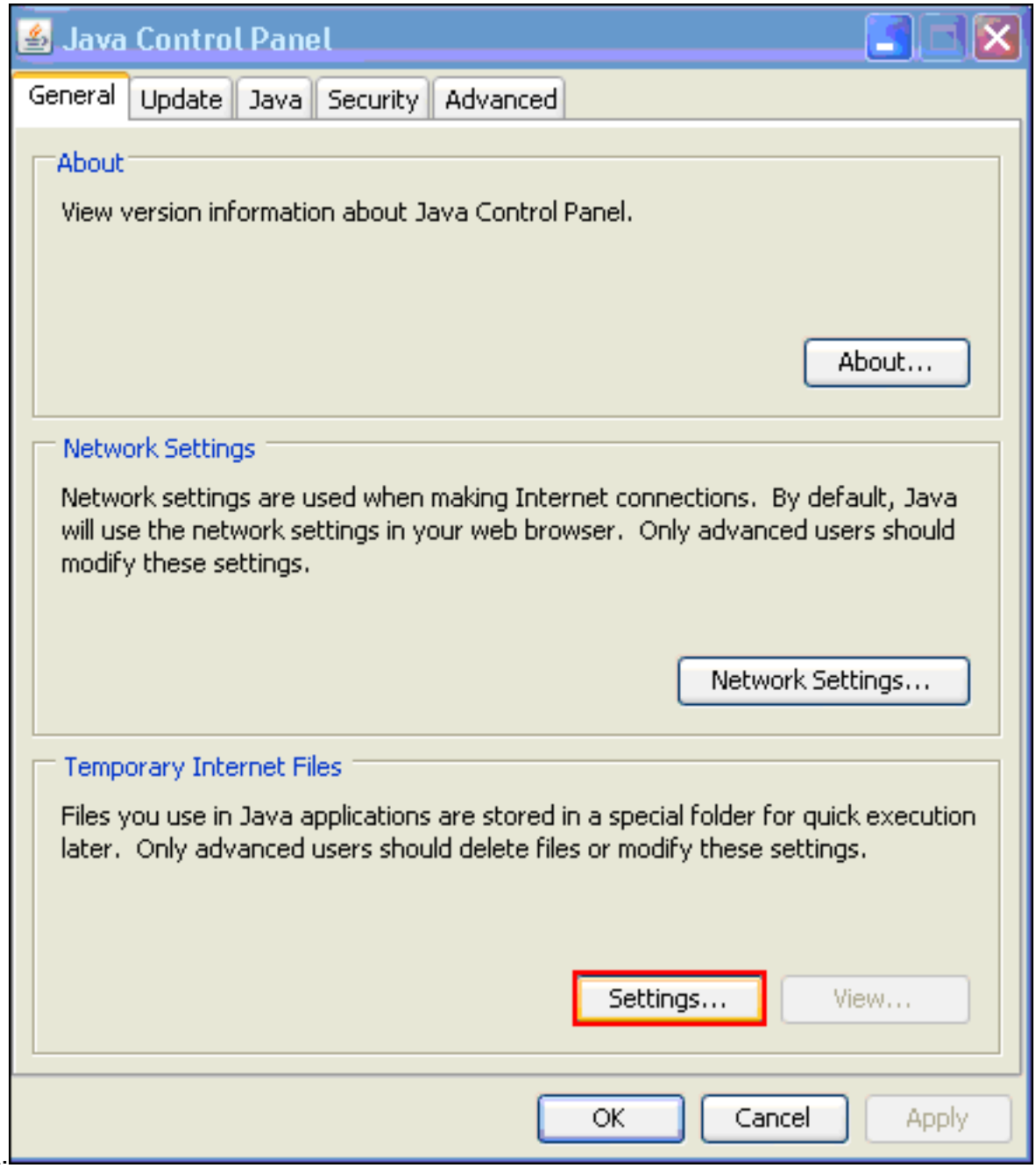

3. Klik op **Alles verwijderen**.
4. Controleer **ook de bestanden en instellingen die zijn opgeslagen door** het aanvinkvakje **toe te voegen**, en klik op **Ja**.
5. Zodra de cache is gewist, sluit u alle exemplaren van de browser af en start u de browser opnieuw.

**Opmerking:** Om de cache voor andere browsers te wissen, raadpleeg Hoe kan ik de cache van mijn browser schoonmaken (om de prestaties te verbeteren)?

## Java-cache wissen

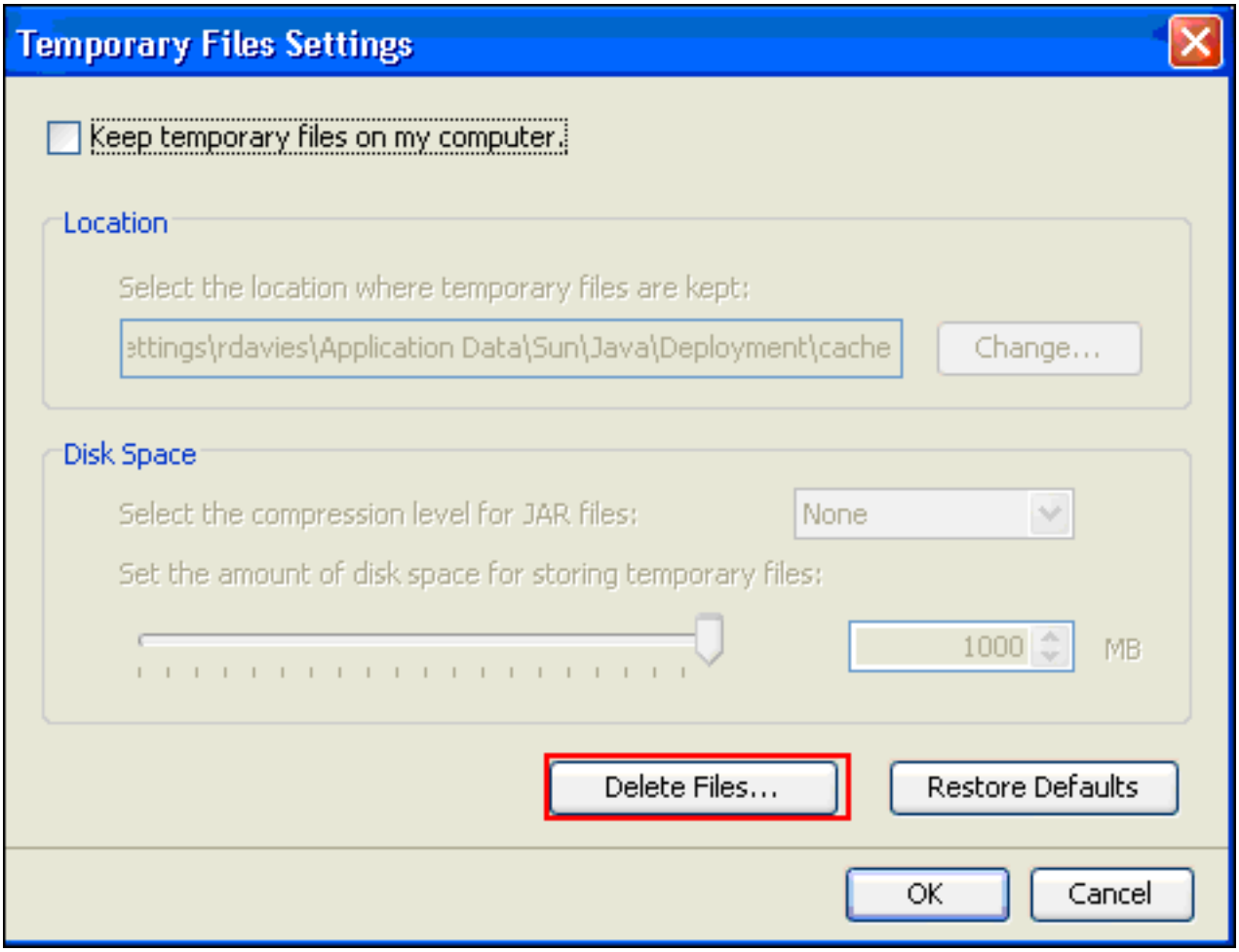
Voltooi deze stappen om het Java-cache te verwijderen:

1. Kies **Configuratiescherm** in het menu Windows Start.
2. Dubbelklik op




**Java**.

3. Klik op **Instellingen**.
4. Klik op **Bestanden verwijderen**.

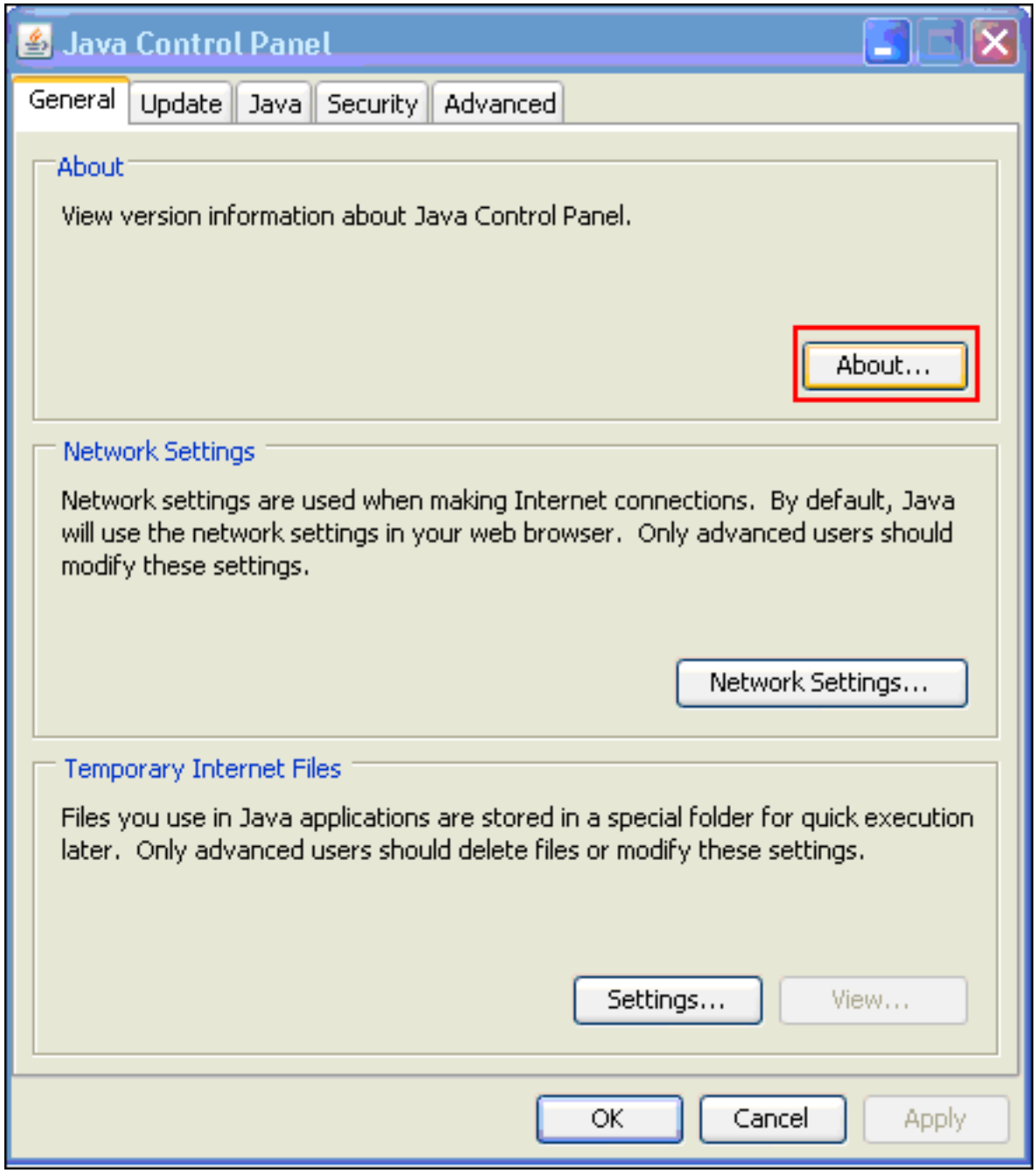


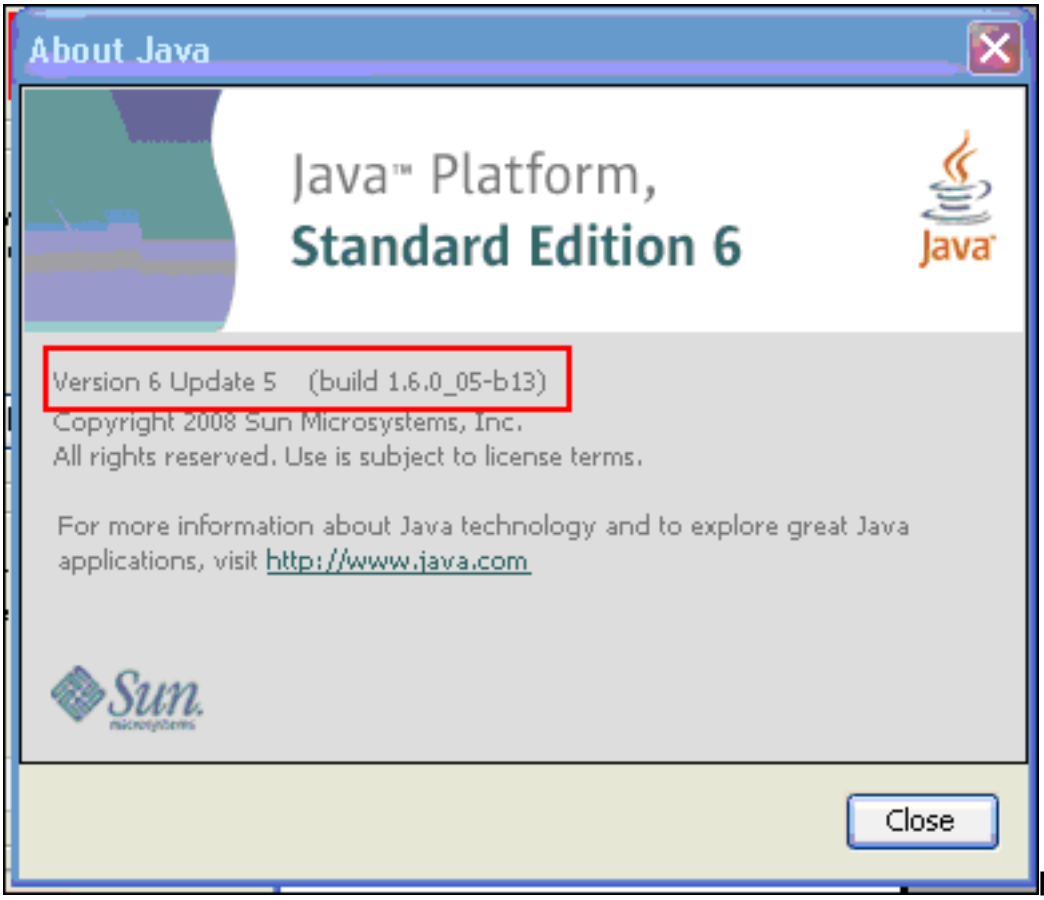

**Opmerking:** Hoe kan ik mijn Java cache wissen? voor meer informatie over deze procedure .

## Debugopties voor Java-applicatie inschakelen

Voltooi deze stappen om de optie van het debuggen van Java toe te staan:

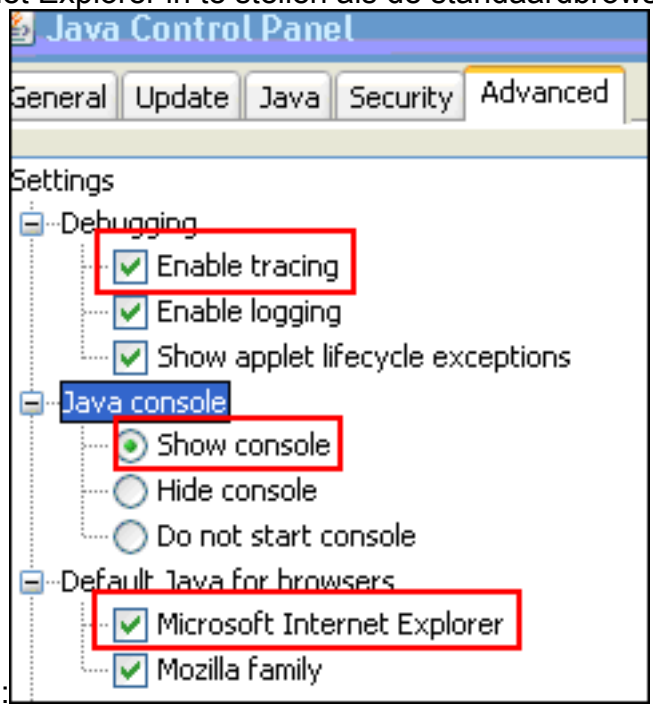
1. Zorg ervoor dat Java 1.4 of hoger is ingeschakeld:Kies **Configuratiescherm** in het menu Windows Start.Dubbelklik op **Java**.Klik op **About** en controleer het versienummer.


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

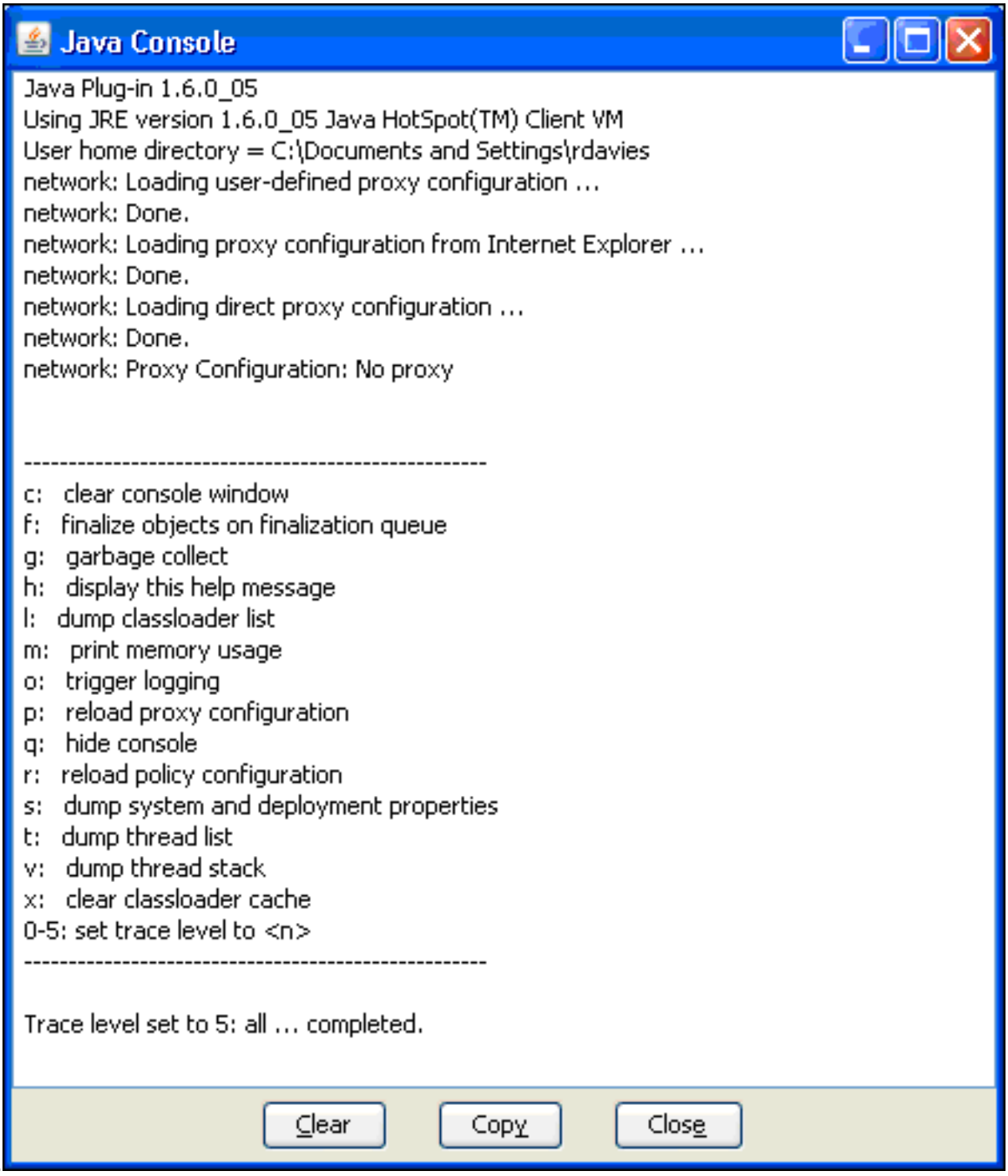



**N.B.:** U kunt Java-updates downloaden op http://java.com/en/ .

2. Zorg ervoor dat Java is ingesteld om overtrekken mogelijk te maken, de console weer te geven en Microsoft Internet Explorer in te stellen als de standaardbrowser zoals in deze afbeelding wordt getoond:




3. Zorg ervoor dat het Java cache wordt gewist zoals beschreven in Schakel het Java-cache uit.
4. Kies in Internet Explorer **Gereedschappen > Java-console** om het Java-bug-venster te

openen. 


5. Wanneer het venster Java Console debug is geopend, drukt u op **5** om het overtrek-niveau in te stellenWanneer een URL wordt benaderd die een Java-applicatie bevat, wordt de activiteit in dit venster opgenomen.
6. Klik op **Kopiëren** om de informatie te kopiëren.

## HTML-opnametools inschakelen

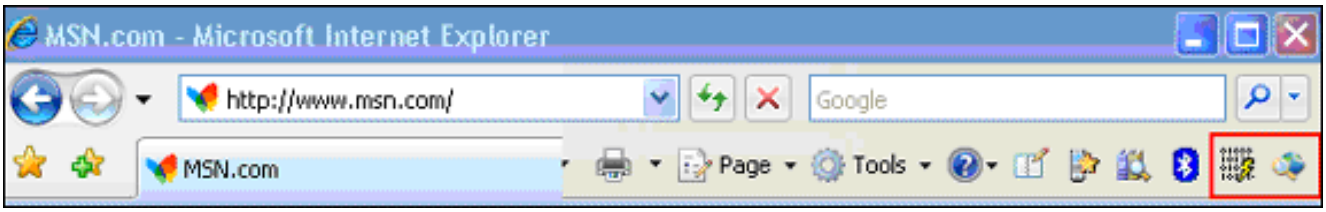
Er is een aantal verschillende HTML Capture tools beschikbaar om gegevens te verzamelen, waarvan een aantal hier zijn opgesomd. Installeer een van deze HTML Capture tools op de client-PC die wordt gebruikt voor de gegevensverzamelingsoefening:

- HTTPWatch
- IE-inspecteur
- Debug Proxy

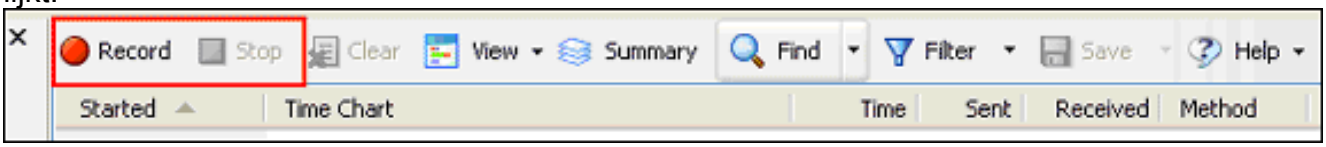
**Opmerking:** Deze procedure gebruikt de HTTPWatch-toepassing.

Voltooi de volgende stappen zodra de applicatie is geïnstalleerd:

1. Druk op Shift+P+F+2 of op het pictogram in het browser om deze functie in te schakelen.




2. Zodra de toepassing is ingeschakeld, verschijnt er een venster dat is ingesloten in het browser venster dat op deze afbeelding lijkt:




3. Klik op **Record** om gegevens op te nemen; Klik op **Stop** om de opname te stoppen.

**Opmerking:** Aanbevolen wordt om HttpWatch 7.x te gebruiken om de gegevens op te nemen.

## Gerelateerde informatie

- Clientloze SSL VPN (WebVPN) op ASA Configuration Voorbeeld
- Adaptieve security applicaties van Cisco ASA 5500 Series
- Technische ondersteuning en documentatie – Cisco Systems