Nota tecnica sulla risoluzione dei problemi relativi alla VPN SSL senza client ASA (WebVPN)

Sommario

Introduzione

In questo documento vengono elencate le tecniche di risoluzione dei problemi di SSL VPN (WebVPN) senza client adottate per le versioni ASA 7.1, 7.2 e 8.0. Tra queste versioni sono stati compiuti progressi significativi che richiedono l'uso di diverse tecniche di risoluzione dei problemi.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la stesura del documento, è stata usata un'appliance ASA Cisco serie 5500 con software versione 7.1 o successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Risoluzione dei problemi

Il prerequisito per la risoluzione dei problemi delle connessioni VPN SSL senza client (WebVPN) sull'appliance ASA è ottenere visibilità sia sull'esperienza del client tramite screenshot e strumenti di acquisizione HTML, quindi confrontare le informazioni raccolte con quelle visualizzate quando si è connessi direttamente all'URL/applicazione a cui si sta accedendo.

ASA versione 7.1/7.2 senza client

In questa sezione vengono descritte le tecniche di risoluzione dei problemi per ASA versioni 7.1/7.2 e per tutti gli intervalli fino alla release 8.0 esclusa.

In questa release, se le funzioni Java/Javascript complesse hanno difficoltà, è possibile prendere in considerazione altre opzioni (come l'inoltro delle porte di accesso alle applicazioni o l'uso di proxy-bypass). Per ulteriori informazioni su queste alternative, fare riferimento a Configurazione dell'accesso all'applicazione e Uso del bypass proxy.

Nella maggior parte degli scenari, se l'URL a cui si accede tramite VPN SSL senza client ha esito negativo per Internet Explorer, avrà esito negativo anche per un altro browser.

Per garantire che ciò non dipenda dal PC client o dal sistema operativo, utilizzare un altro client da una posizione diversa. È inoltre possibile verificare l'utilizzo di un client VPN IPsec o SSL.

Verificare che l'ASA sia inclusa nell'area attendibile del browser come descritto in Abilitazione dei cookie sui browser per WebVPN e che i cookie siano abilitati come descritto in Abilitazione dei cookie.

Se il processo non riesce, completare la procedura descritta di seguito per raccogliere le informazioni necessarie e quindi aprire una richiesta TAC.

1. Cancellare la cache del browser come descritto in Cancellare la cache del browser.
2. Cancellare la cache Java come descritto in Cancellare la cache Java.
3. Disabilitare la cache della WebVPN sull'appliance ASA come descritto in Configurazione della memorizzazione nella cache.
4. Se è presente un'applet Java, utilizzare il livello di debug 5 nella finestra dell'applet come descritto in Abilitazione delle opzioni di debug dell'applet Java.
5. Accedere all'ASA tramite la VPN SSL senza client.
6. Nell'URL immediatamente precedente all'URL con problemi, attivare uno strumento di acquisizione HTML nel browser come descritto in Attivazione degli strumenti di acquisizione HTML.

7. Acquisire la sequenza da questo punto all'URL con problemi.
8. Premere **Ctrl+Stamp** sulla tastiera per acquisire uno screenshot.
9. Arrestare lo strumento di acquisizione HTML.
10. Eseguire gli stessi passaggi da 1 a 9 quando ci si connette direttamente all'URL tramite una sessione VPN IPsec o SSL tramite l'ASA o direttamente sullo stesso segmento LAN (se possibile) e si inviano i dati a TAC per l'analisi.

ASA versione 8.0 senza client

In questa sezione vengono descritte le tecniche di risoluzione dei problemi utilizzate per ASA versione 8.0 e per tutti gli intervalli.

In questa release, se si verificano problemi con URL o applicazioni complesse tramite VPN SSL senza client, altre opzioni (ad esempio l'utilizzo di tunnel intelligenti) rappresentano una valida alternativa. Per ulteriori informazioni sui tunnel intelligenti, fare riferimento a Configurazione dell'accesso ai tunnel intelligenti.

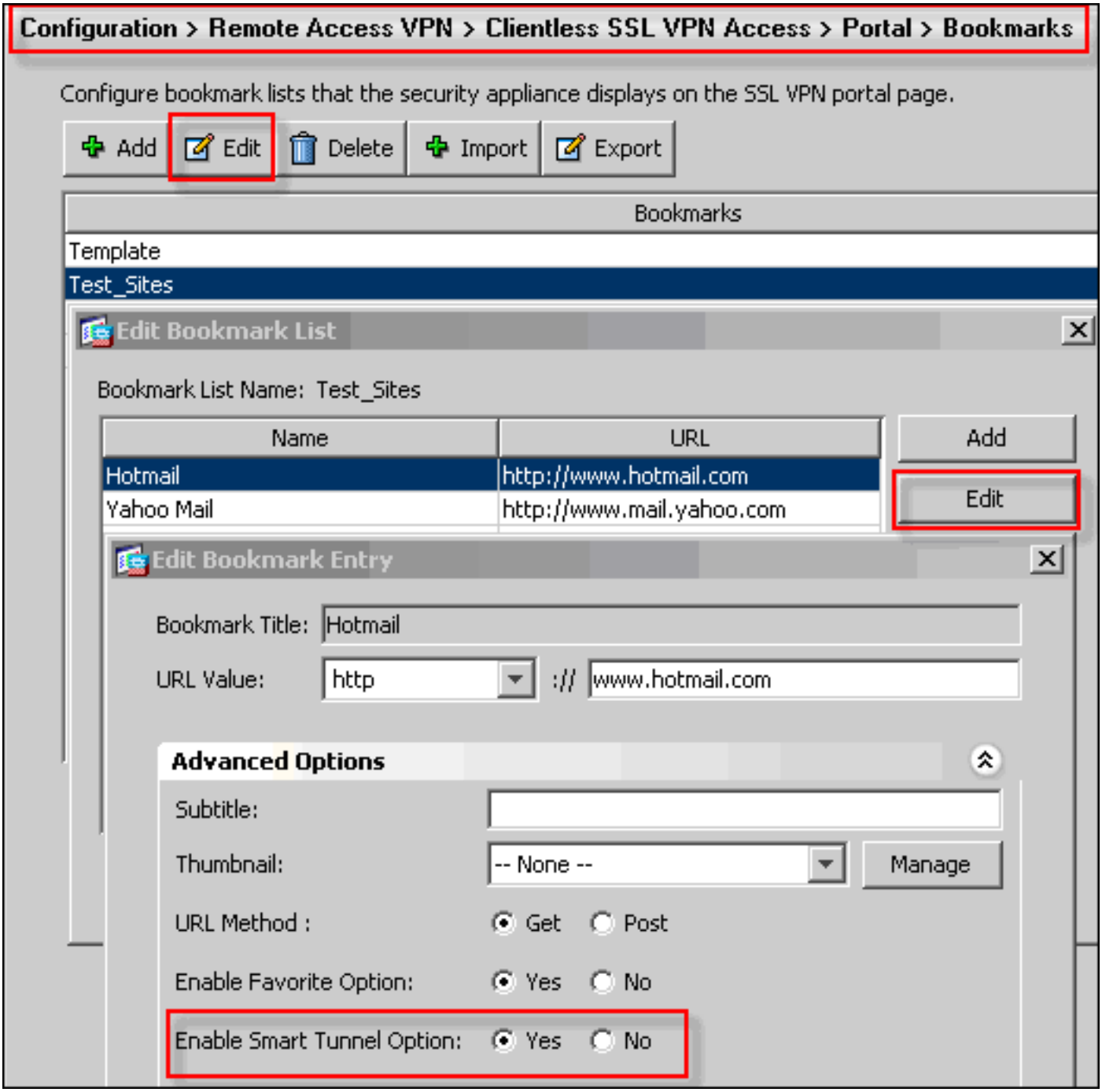
Si potrebbe anche prendere in considerazione l'inoltro delle porte di accesso alle applicazioni o l'uso di proxy-bypass. Per ulteriori informazioni su queste alternative, fare riferimento a Configurazione dell'accesso all'applicazione e Uso del bypass proxy.

Nella maggior parte degli scenari, se l'URL a cui si accede tramite VPN SSL senza client ha esito negativo per Internet Explorer, avrà esito negativo anche per un altro browser.

Per garantire che ciò non dipenda dal PC client o dal sistema operativo, utilizzare un altro client da una posizione diversa. È inoltre possibile verificare l'utilizzo di un client VPN IPsec o SSL.

Verificare che l'ASA sia inclusa nell'area attendibile del browser come descritto in Abilitazione dei cookie sui browser per WebVPN e che i cookie siano abilitati come descritto in Abilitazione dei cookie.

Se un'applicazione presenta un problema con il motore di trasformazione del contenuto senza client (CTE/rewriter), è possibile modificare il segnalibro per tale applicazione per abilitare l'opzione Smart Tunnel, come mostrato nell'immagine:



L'attivazione di questa opzione per un segnalibro non richiede una configurazione aggiuntiva. Analogamente all'inoltro delle porte, questa è un'altra opzione utile per fare clic su un segnalibro e aprire una nuova finestra che utilizza lo smart tunnel per trasmettere il traffico delle applicazioni ed evitare problemi di riscrittura.

Quando si utilizza questa funzione per le applicazioni TCP Winsock 32 (ad esempio RDP), l'amministratore deve identificare i processi da utilizzare tramite i tunnel intelligenti. Ad esempio, RDP utilizza il processo mstsc.exe; è possibile creare una voce smart tunnel semplice per questo processo.

Applicazioni più complesse possono generare più processi. Dalla pagina WebVPN Portal, scegliere il pannello **Accesso applicazione**. Non appena viene caricato, l'elenco delle *applicazioni consentite* è in grado di connettersi al lato privato della rete.

Se il processo non riesce, completare la procedura descritta di seguito per raccogliere le informazioni necessarie e quindi aprire una richiesta TAC.

1. Cancellare la cache del browser come descritto in Cancellare la cache del browser.
2. Cancellare la cache Java come descritto in Cancellare la cache Java.
3. Disabilitare la cache della WebVPN sull'appliance ASA come descritto in Configurazione della memorizzazione nella cache.
4. Se è presente un'applet Java, utilizzare il livello di debug 5 nella finestra dell'applet come descritto in Abilitazione delle opzioni di debug dell'applet Java.
5. Accedere all'ASA tramite la VPN SSL senza client.
6. Nell'URL immediatamente precedente all'URL con problemi, attivare uno strumento di acquisizione HTML nel browser come descritto in Attivazione degli strumenti di acquisizione HTML.
7. Acquisire la sequenza da questo punto all'URL con problemi.
8. Premere **Ctrl+Stamp** sulla tastiera per acquisire uno screenshot.
9. Arrestare lo strumento di acquisizione HTML.
10. Eseguire i passaggi da 1 a 9 quando ci si connette direttamente all'URL tramite una sessione IPsec o Any Connect SSL tramite l'ASA o si connette direttamente allo stesso segmento LAN (se possibile), completare la procedura descritta e inviare i dati a TAC per l'analisi

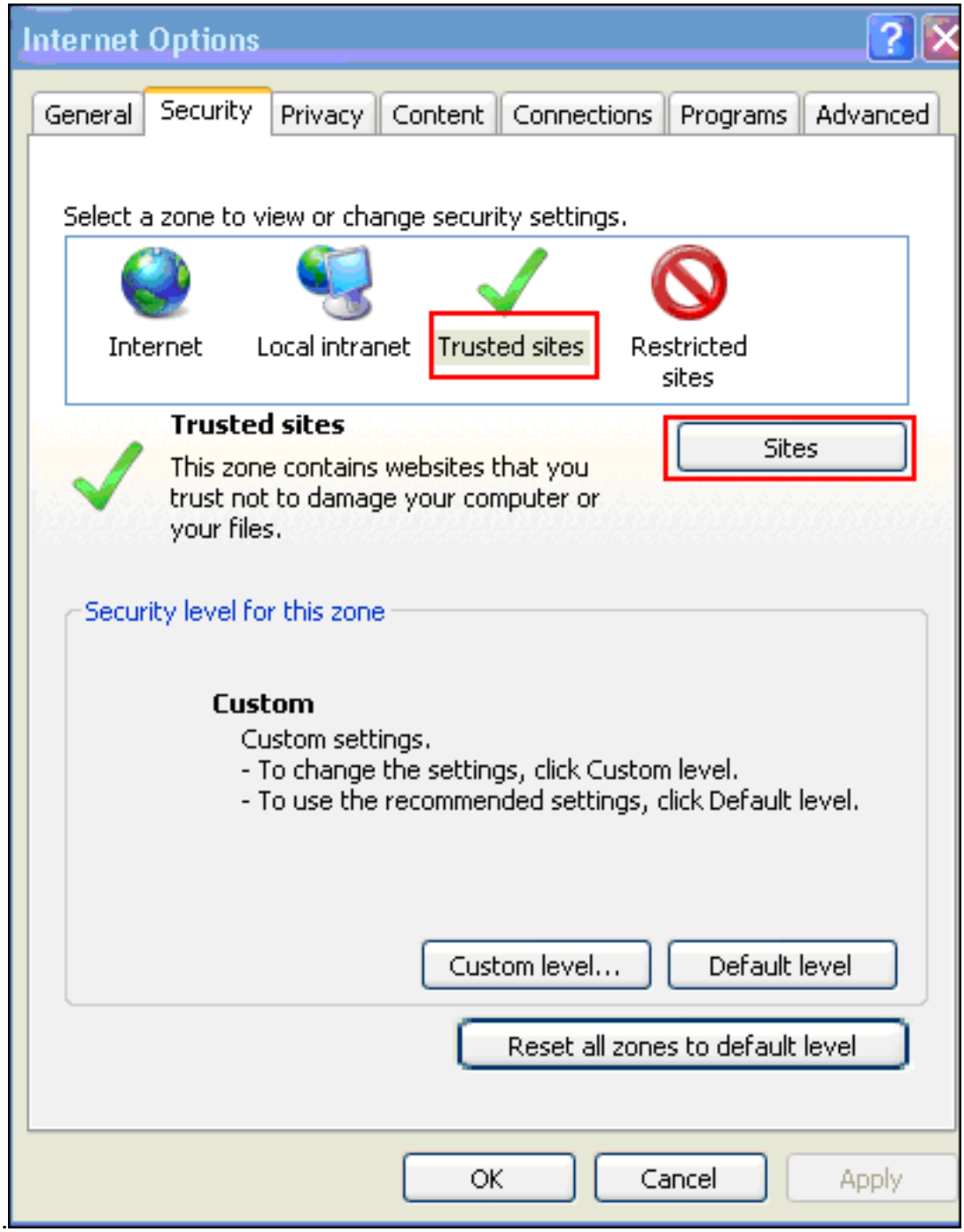
Procedure

Aggiunta dell'appliance ASA come sito attendibile

Quando si accede all'appliance ASA in Internet Explorer, si riceverà un errore di certificato se il sito non è incluso come sito attendibile.

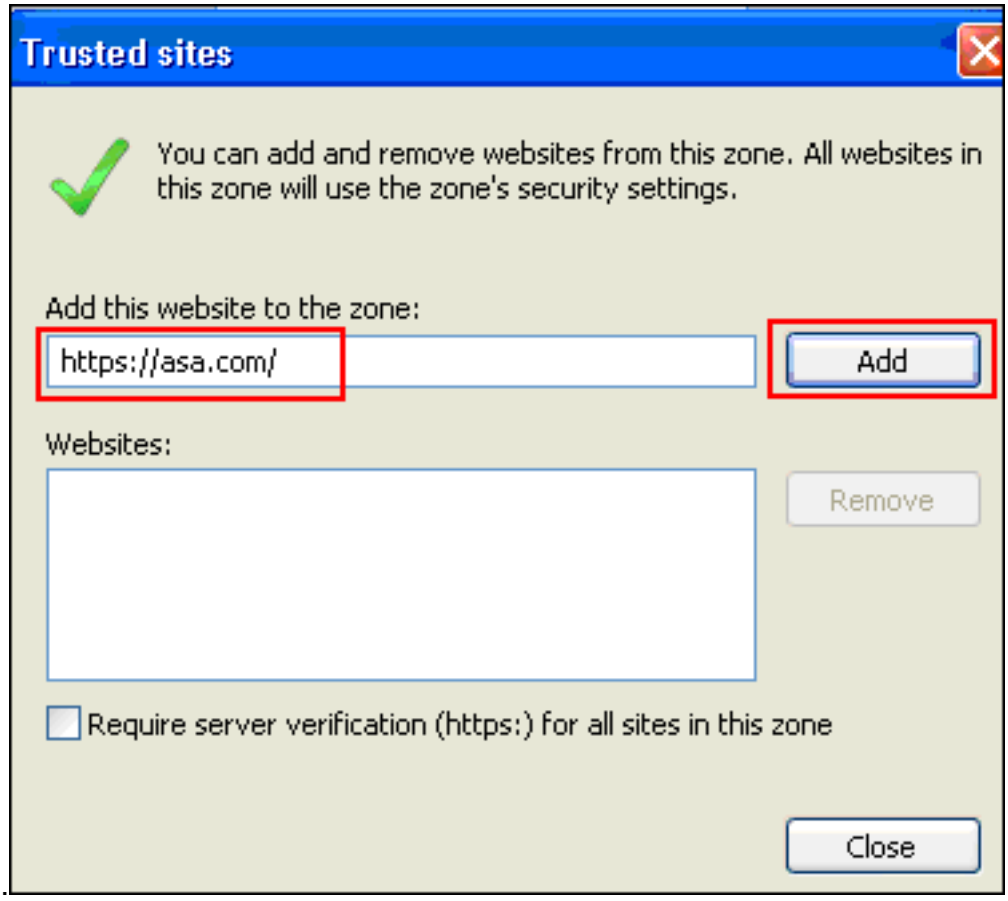
Per aggiungere l'appliance ASA come sito attendibile, completare la procedura seguente:

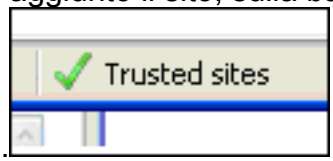
1. In Internet Explorer, scegliere **Strumenti > Opzioni Internet**.
2. Fare clic sulla scheda **Protezione** e scegliere **Siti**



attendibili.

3. Fare clic su **Siti**.
4. Aggiungere l'indirizzo https:// dell'appliance ASA e fare clic su

Add. 

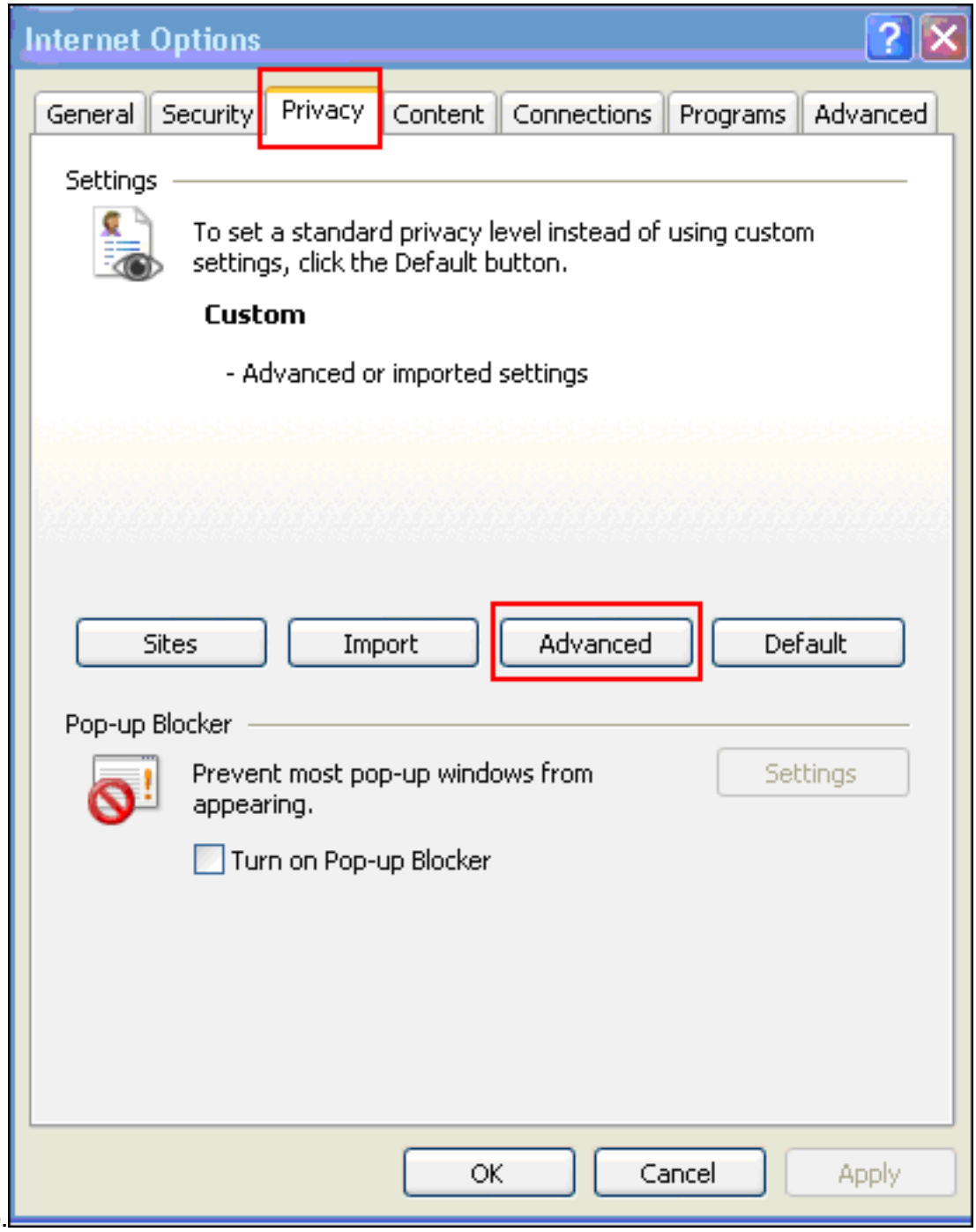
5. Una volta aggiunto il sito, sulla barra di stato di Internet Explorer viene visualizzata l'icona Siti attendibili. 

Nota: per informazioni dettagliate su questa procedura, fare riferimento a Utilizzo delle impostazioni di protezione di Internet Explorer 6.

Abilita cookie

Completare questi passaggi per abilitare i cookie:

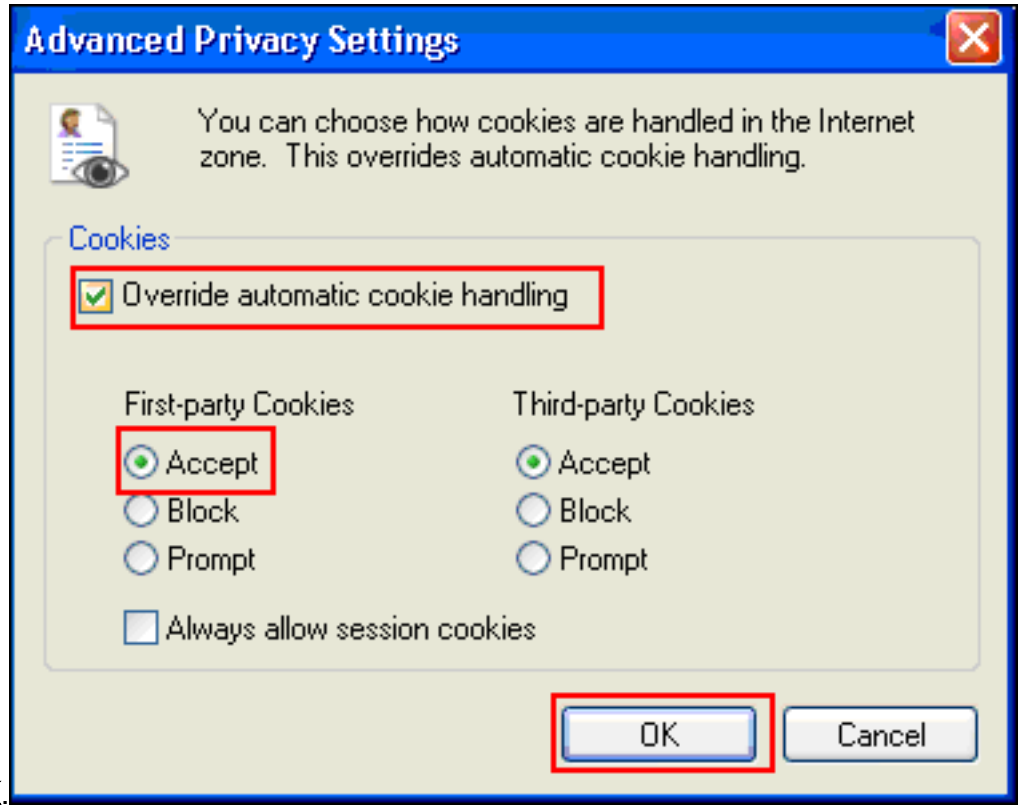
1. In Internet Explorer, scegliere **Strumenti > Opzioni Internet**.
2. Fare clic sulla scheda **Privacy** e quindi su



Avanzate.

3. Nella finestra di dialogo Impostazioni avanzate privacy selezionare la casella di controllo **Ignora gestione automatica cookie**, fare clic sul pulsante di opzione **Accetta** e quindi su

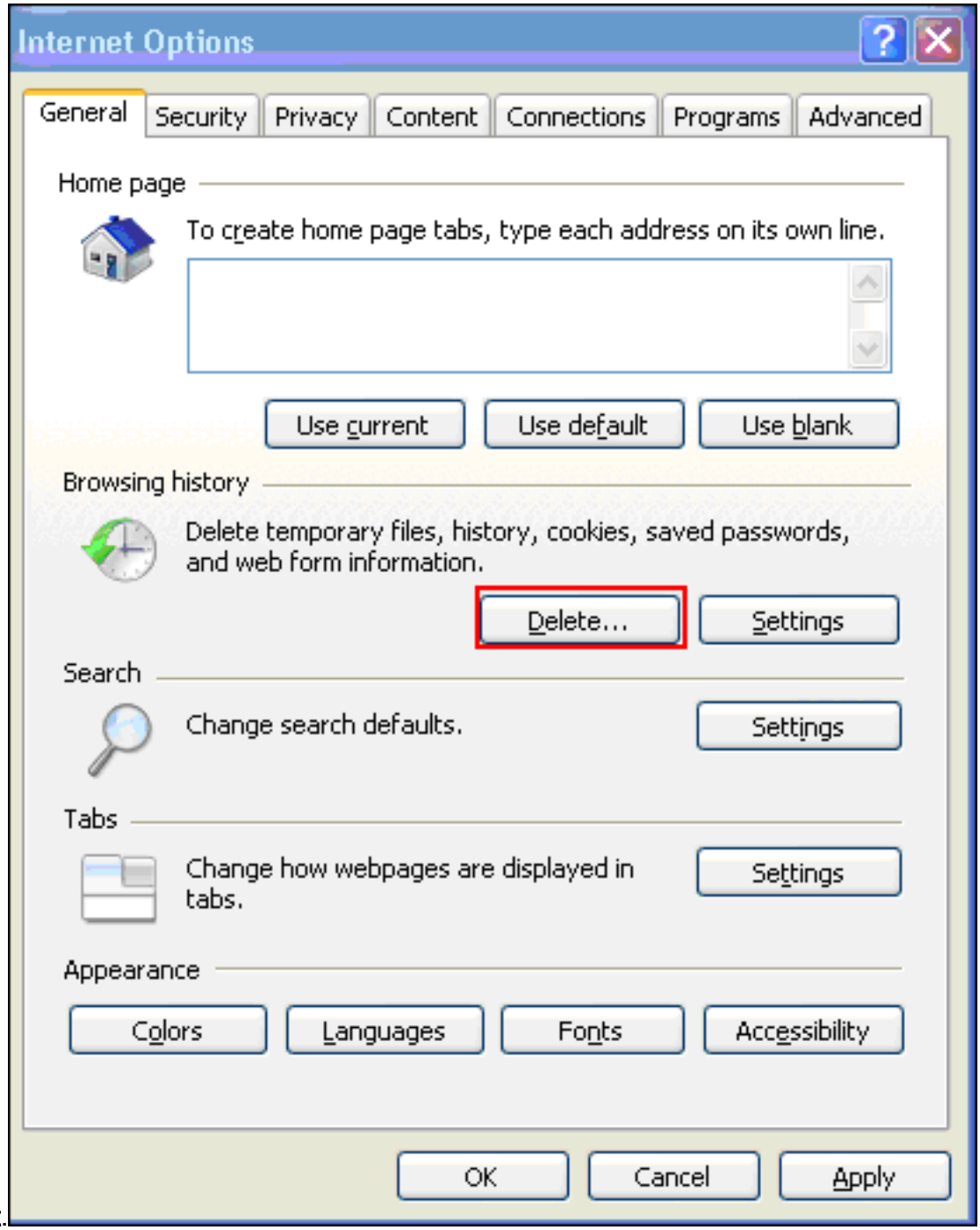
OK.



Cancella la cache del browser

Completare questa procedura per cancellare la cache per Internet Explorer:

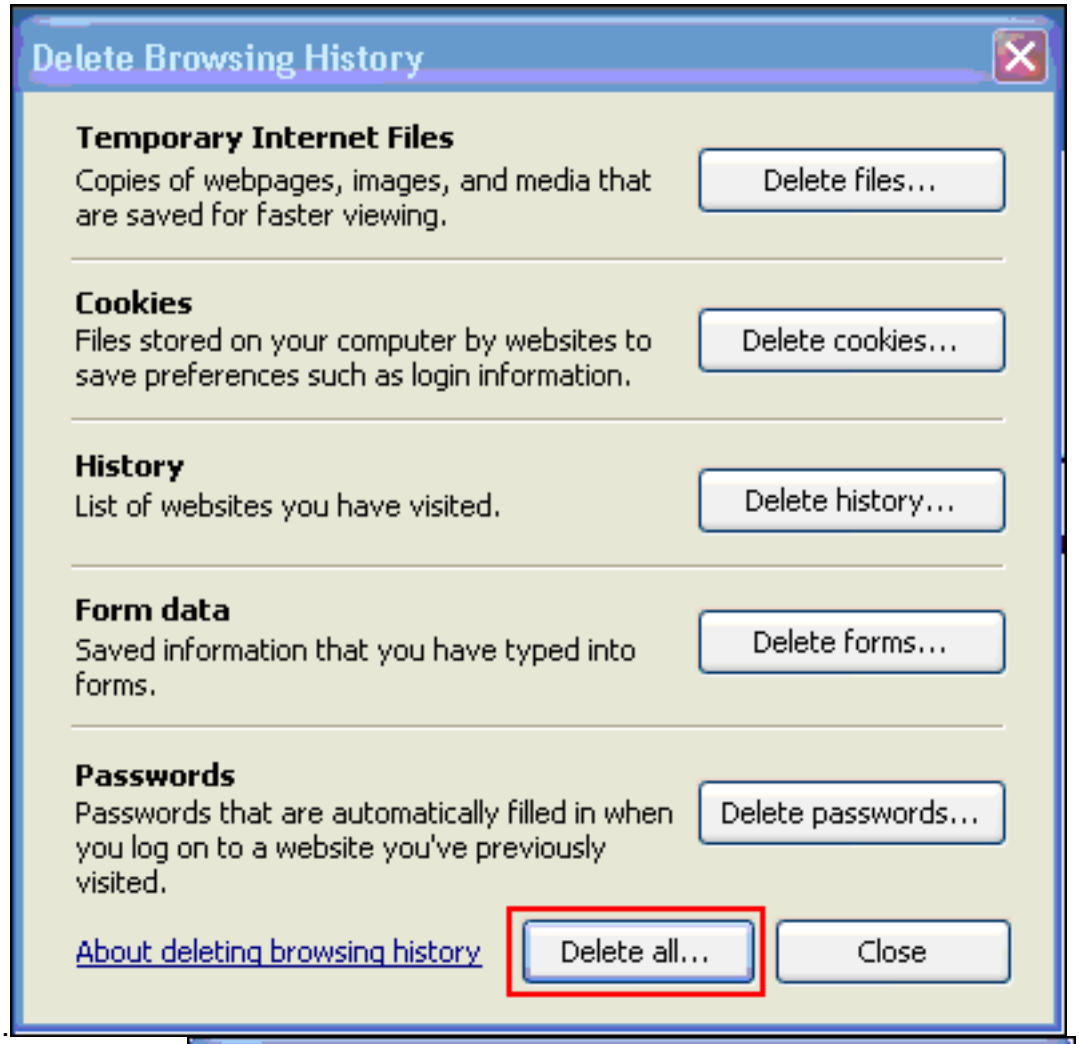
1. In Internet Explorer, scegliere **Strumenti > Opzioni**

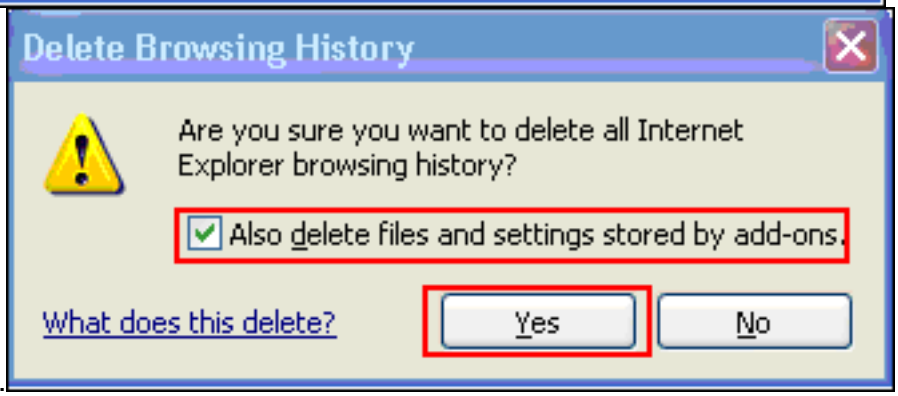


Internet.

2. Nella scheda Generale fare clic su **Elimina** nella sezione Cronologia

esplorazioni.





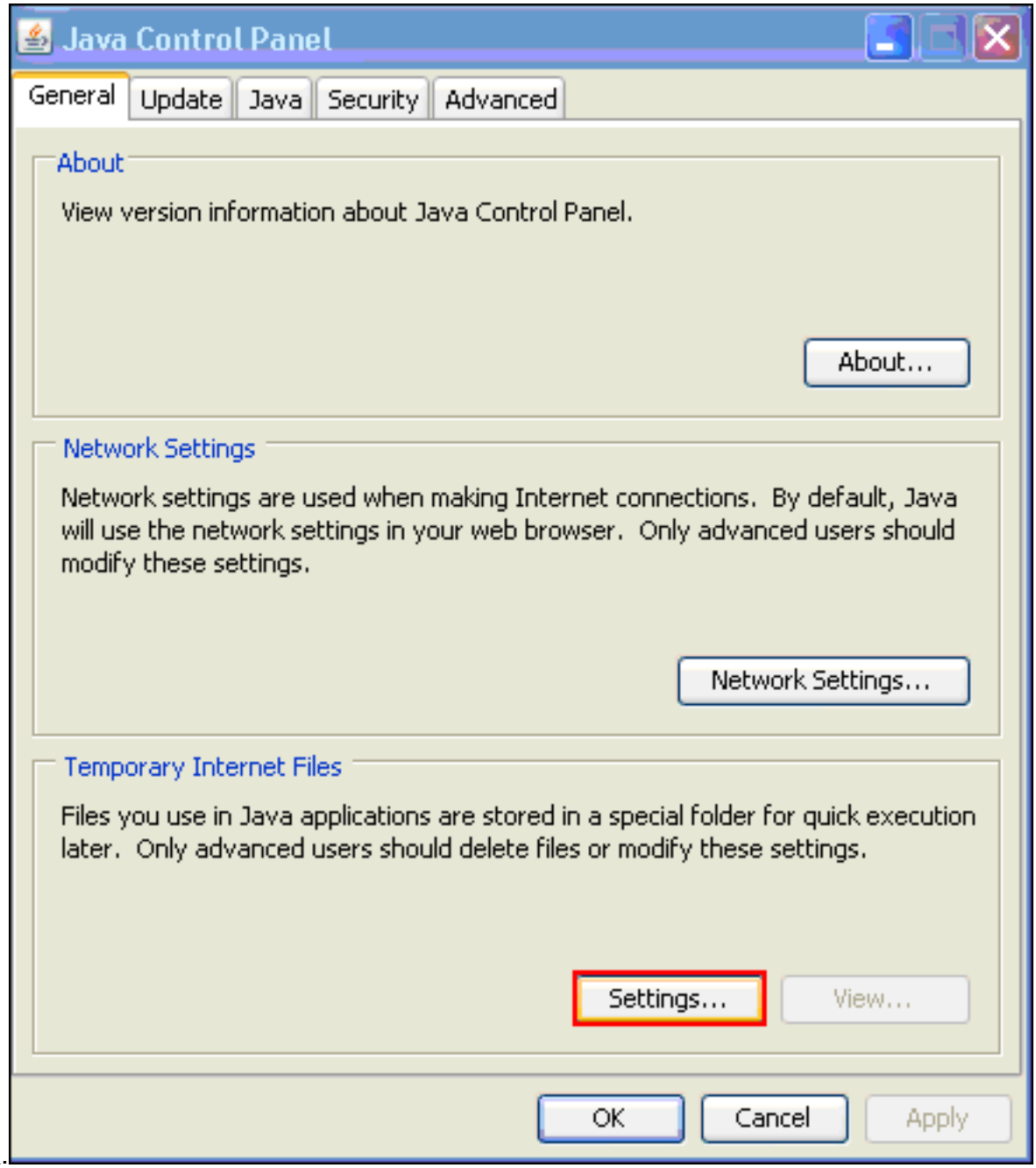
3. Fare clic su **Elimina tutto**.
4. Selezionare la casella di controllo **Elimina anche i file e le impostazioni memorizzati dai componenti aggiuntivi** e fare clic su **Sì**.
5. Una volta cancellata la cache, chiudere tutte le istanze del browser e riavviare il browser.

Nota: per cancellare la cache per altri browser, fare riferimento a Come cancellare la cache del browser (per migliorarne le prestazioni)?

Cancella la cache Java

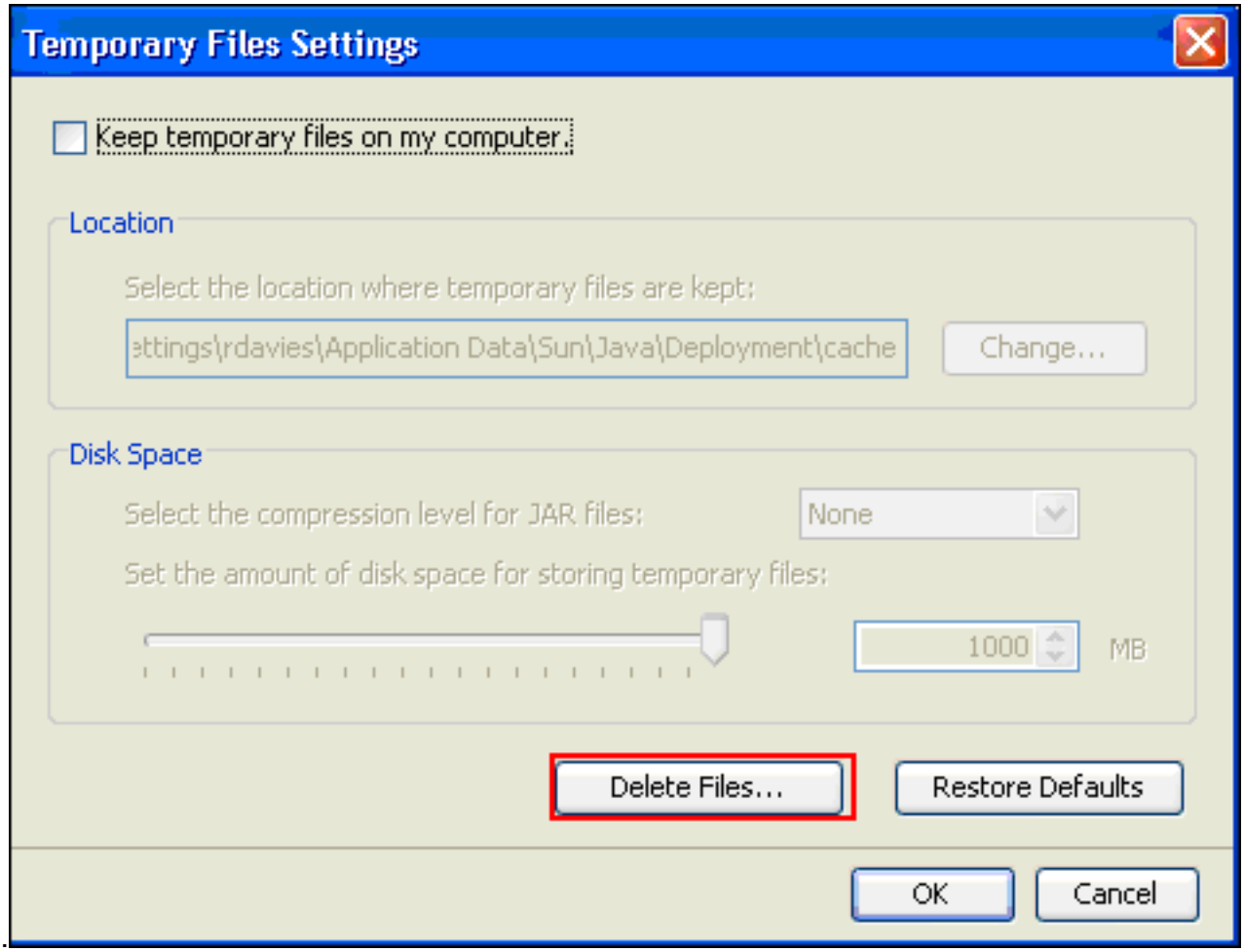
Completare questi passaggi per cancellare la cache Java:

1. Scegliere **Pannello di controllo** dal menu Start di Windows.
2. Fare doppio clic su



Java.

3. Fare clic su **Impostazioni**.
4. Fare clic su **Elimina**



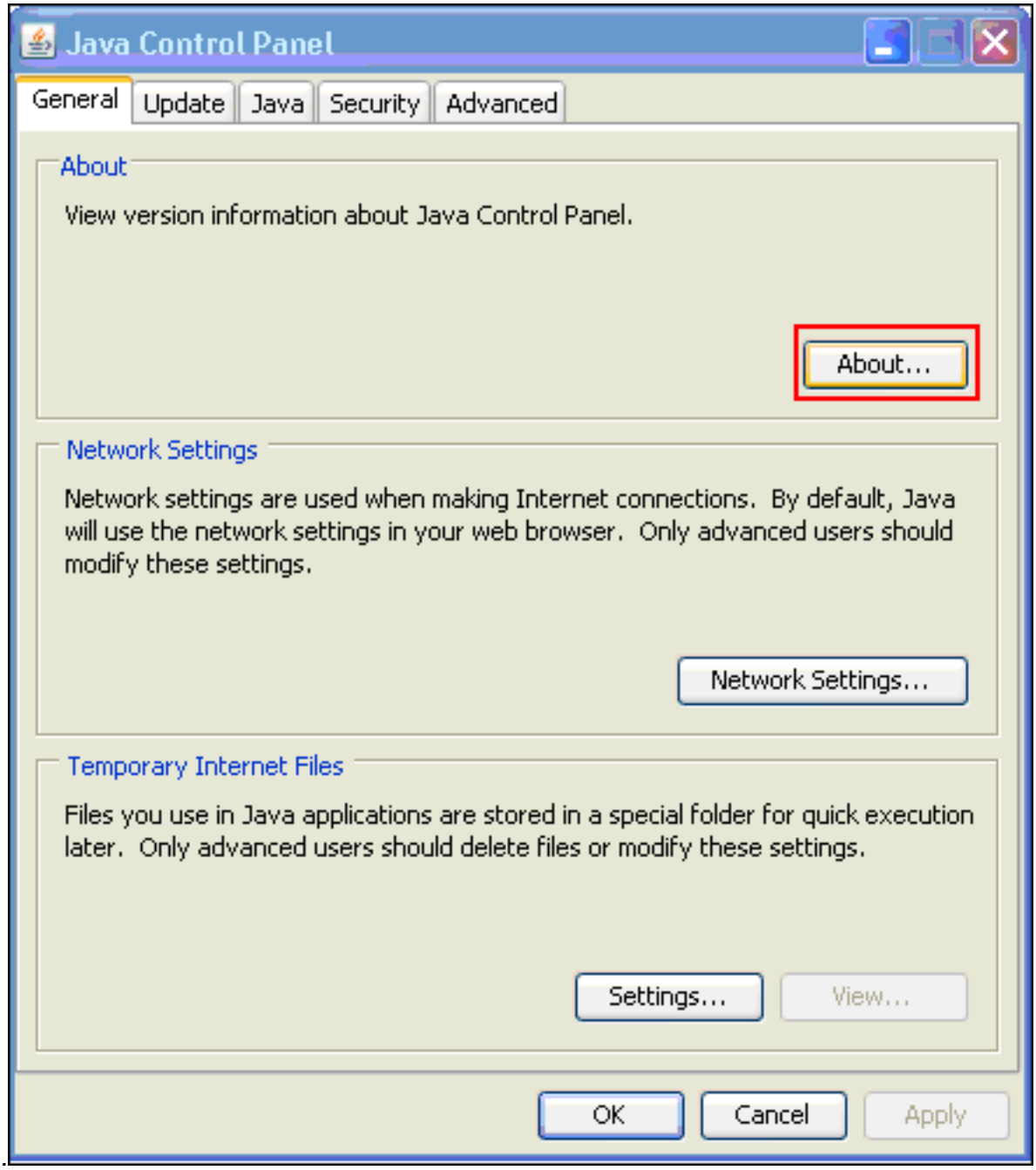
file.

Nota: fare riferimento alla sezione Come cancellare la cache Java? per ulteriori informazioni su questa procedura.

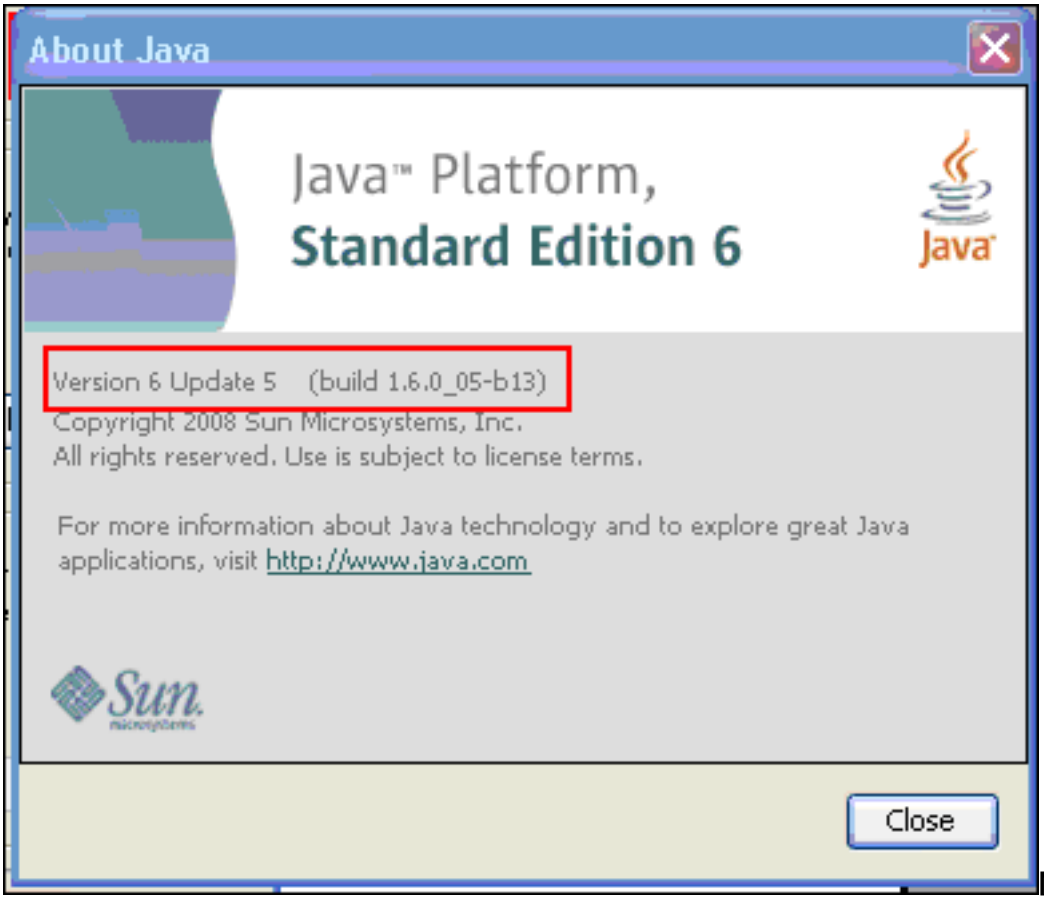
Abilita opzioni di debug applet Java

Completare questi passaggi per abilitare l'opzione di debug dell'applet Java:

1. Assicurarsi che Java 1.4 o versione successiva sia abilitato:Scegliere **Pannello di controllo** dal menu Start di Windows.Fare doppio clic su **Java**.Fare clic su **Informazioni su** e verificare il numero di

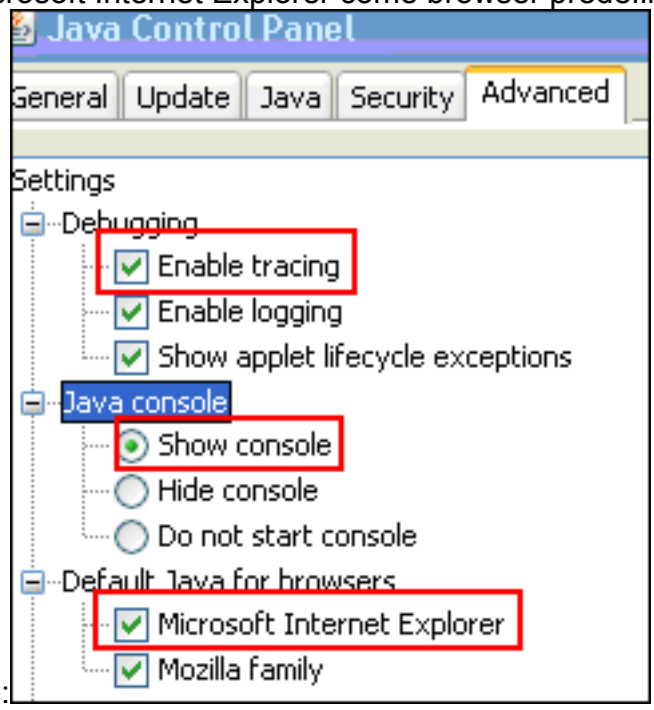

Java Control Panel
General
Update
Java
Security
Advanced
About
View version information about Java Control Panel.
About...
Network Settings
Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify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

versione.



Nota: è possibile scaricare gli aggiornamenti Java da http://java.com/en/ .

2. Verificare che Java sia configurato per abilitare il trace, per visualizzare la console e per impostare Microsoft Internet Explorer come browser predefinito, come mostrato nell'immagine:



3. Verificare che la cache Java sia stata cancellata come descritto in Cancellazione della cache Java.
4. In Internet Explorer, scegliere **Strumenti > Console Java** per aprire la finestra di debug di

Java.

5. Una volta aperta la finestra di debug di Java Console, premere **5** per impostare il livello di tracciaQuando si accede a un URL che contiene un'applet Java, l'attività viene acquisita in questa finestra.
6. Per copiare le informazioni, fare clic su **Copia**.

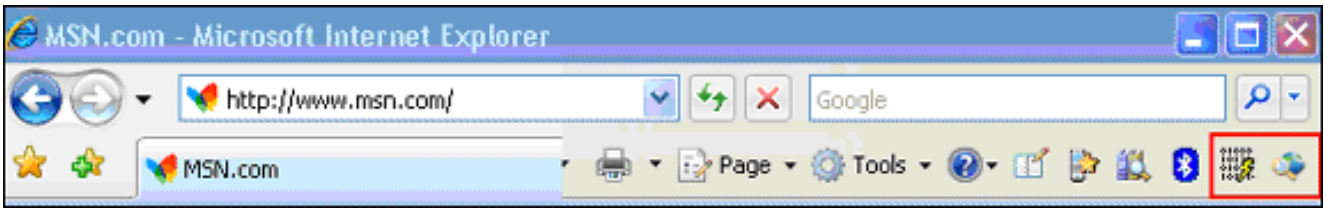
Attivazione degli strumenti di acquisizione HTML

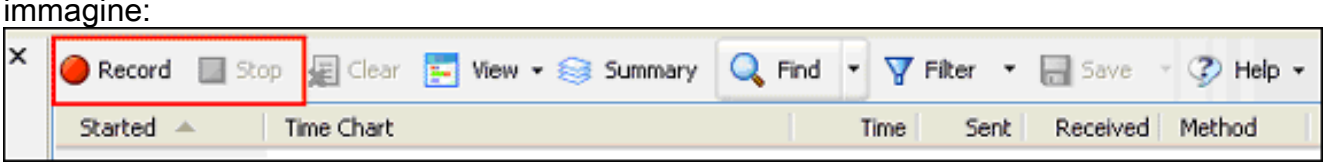
Per la raccolta dei dati sono disponibili diversi strumenti di acquisizione HTML, alcuni dei quali sono elencati di seguito. Installare uno di questi strumenti di acquisizione HTML nel PC client utilizzato per l'esercizio di raccolta dei dati:

- ControlloHTTP
- IE Inspector
- Debug proxy

Nota: in questa procedura viene utilizzata l'applicazione HTTPWatch.

Una volta installata l'applicazione, procedere come segue:

1. Premere Maiusc+P+F+2 o fare clic sull'icona nella finestra del browser per abilitare HTTPWatch.


2. Una volta attivata l'applicazione, nella parte inferiore della finestra del browser appare una finestra simile a questa immagine:


3. Fare clic su **Record** per registrare i dati; per interrompere la registrazione, fare clic su **Stop**.

Nota: si consiglia di utilizzare HttpWatch 7.x per registrare i dati.

Informazioni correlate

- Esempio di configurazione di una VPN SSL senza client (WebVPN) su ASA
- Cisco ASA serie 5500 Adaptive Security Appliance
- Documentazione e supporto tecnico – Cisco Systems