Note technique concernant le dépannage VPN SSL (WebVPN) sans client ASA

Contenu

Introduction

Ce document répertorie les techniques de dépannage VPN SSL sans client (WebVPN) adoptées pour les versions 7.1, 7.2 et 8.0 d'ASA. Il existe des avancées significatives entre ces versions qui nécessitent l'adoption de différentes techniques de dépannage.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur l'ASA de la gamme Cisco 5500 qui exécute la version 7.1 ou ultérieure du logiciel.

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Dépannage

La condition préalable au dépannage des connexions VPN SSL sans client (WebVPN) sur l'ASA est d'obtenir une visibilité à la fois sur l'expérience du client via des captures d'écran et des outils de capture HTML, puis de comparer ces informations aux mêmes informations lorsqu'elles sont connectées directement à l'URL/l'application à laquelle on accède.

ASA version 7.1/7.2 sans client

Cette section décrit les techniques de dépannage pour les versions 7.1/7.2 d'ASA et tous les intervalles jusqu'à la version 8.0, mais sans inclure cette version.

Dans cette version, si des fonctions Java/Javascript complexes ont des difficultés, d'autres options (telles que le transfert de port d'accès aux applications ou l'utilisation de contournement de proxy) peuvent être prises en compte. Référez-vous à Configuration de l'accès aux applications et Utilisation du contournement du proxy pour plus d'informations sur ces alternatives.

Dans la plupart des scénarios, si l'URL accessible via le VPN SSL sans client échoue pour Internet Explorer, elle échouera également pour un autre navigateur.

Afin de s'assurer que cela ne dépend pas du PC ou du système d'exploitation client, utilisez un autre client à partir d'un autre emplacement. L'utilisation d'un client VPN IPsec ou SSL peut également être testée.

Assurez-vous que l'ASA est inclus dans la zone de confiance du navigateur comme décrit dans Activation des cookies sur les navigateurs pour WebVPN et que les cookies sont activés comme décrit dans Activer les cookies.

Si le processus échoue toujours, complétez ces étapes afin de recueillir les informations nécessaires, puis ouvrez un dossier TAC.

1. Effacez le cache du navigateur comme décrit dans Effacer le cache du navigateur.
2. Effacez le cache Java comme décrit dans Effacer le cache Java.
3. Désactivez le cache WebVPN sur l'ASA comme décrit dans Configuration de la mise en cache.
4. Si une applet Java est présente, utilisez le niveau de débogage 5 dans la fenêtre de l'applet comme décrit dans Activer les options de débogage de l'applet Java.
5. Connectez-vous à l'ASA via un VPN SSL sans client.
6. ÀlURL juste avant l'URL problématique, activez un outil de capture HTML dans le navigateur comme décrit dans Activer les outils de capture HTML.
7. Capturez la séquence de ce point vers l'URL problématique.
8. Appuyez sur **Ctrl+Impr écran** sur votre clavier afin de capturer une capture d'écran.
9. Arrêtez l'outil de capture HTML.

10. Effectuez les mêmes étapes 1 à 9 lorsque vous vous connectez directement à l'URL via une session VPN IPsec ou SSL via l'ASA ou que vous vous connectez directement sur le même segment LAN (si possible) et envoyez les données au TAC pour analyse.

ASA version 8.0 sans client

Cette section décrit les techniques de dépannage utilisées pour ASA Versions 8.0 et tous les intervalles.

Dans cette version, si des URL ou des applications complexes ont des difficultés via un VPN SSL sans client, d'autres options (telles que l'utilisation de tunnels intelligents) sont une alternative puissante. Référez-vous à Configuration de Smart Tunnel Access pour plus d'informations sur les Smart Tunnel.

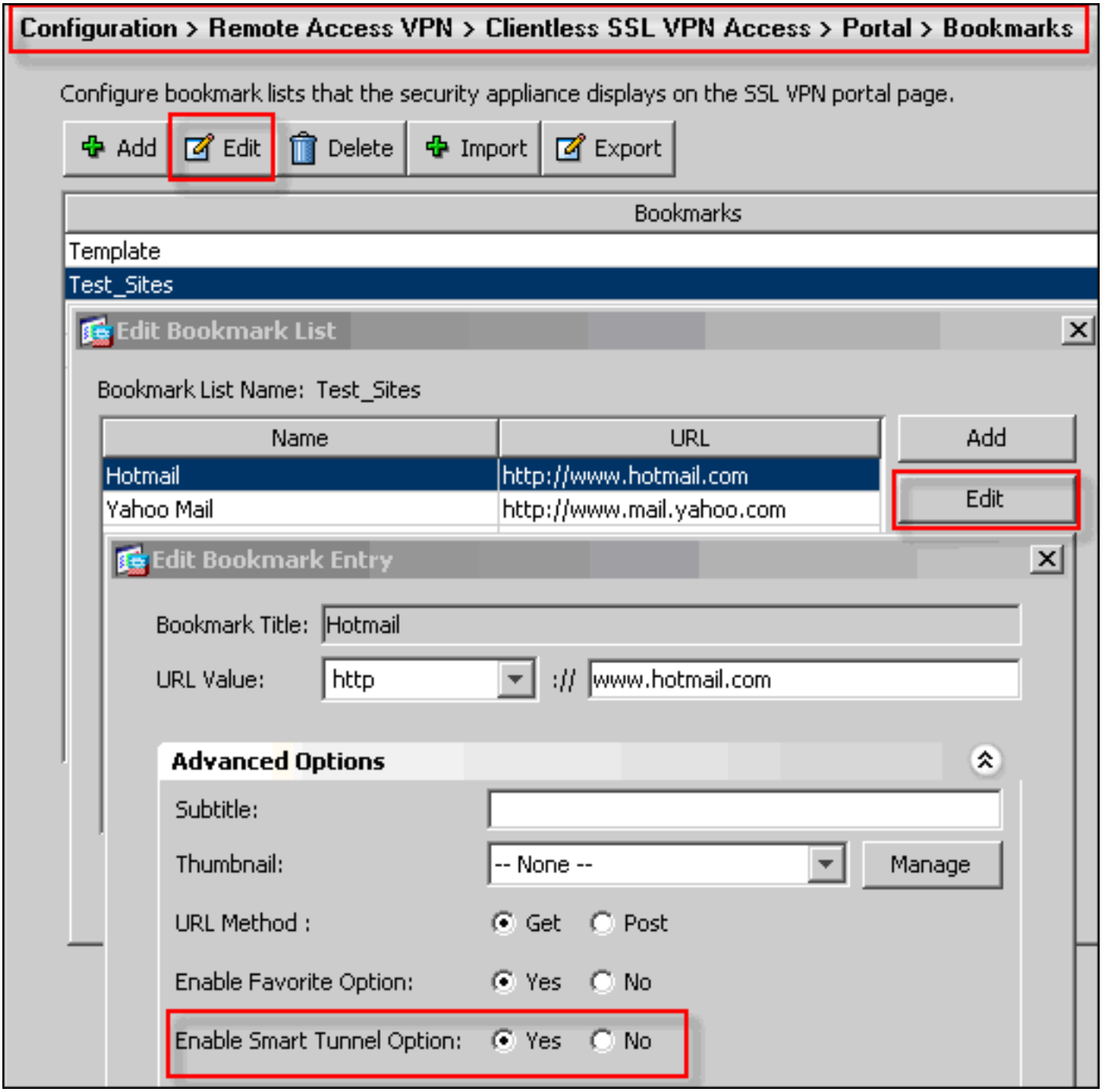
Vous pouvez également envisager le transfert de port d'accès aux applications ou l'utilisation du contournement de proxy. Référez-vous à Configuration de l'accès aux applications et Utilisation du contournement du proxy pour plus d'informations sur ces alternatives.

Dans la plupart des scénarios, si l'URL accessible via le VPN SSL sans client échoue pour Internet Explorer, elle échouera également pour un autre navigateur.

Afin de s'assurer que cela ne dépend pas du PC ou du système d'exploitation client, utilisez un autre client à partir d'un autre emplacement. L'utilisation d'un client VPN IPsec ou SSL peut également être testée.

Assurez-vous que l'ASA est inclus dans la zone de confiance du navigateur comme décrit dans Activation des cookies sur les navigateurs pour WebVPN et que les cookies sont activés comme décrit dans Activer les cookies.

Si une application rencontre un problème avec le moteur de transformation de contenu sans client (CTE/rewriter), vous pouvez modifier le signet de cette application afin d'activer l'option Smart Tunnel comme illustré dans cette image :



L'activation de cette option pour un signet ne nécessite aucune configuration supplémentaire. Comme pour le transfert de port, il s'agit d'une autre option pratique pour cliquer sur un signet afin d'ouvrir une nouvelle fenêtre qui utilise le tunnel intelligent pour transmettre le trafic d'application et éviter les problèmes de réécriture.

Lorsque vous utilisez cette fonctionnalité pour les applications TCP Winsock 32 (telles que RDP), l'administrateur doit identifier le ou les processus à utiliser via des tunnels intelligents. Par exemple, RDP utilise le processus mstsc.exe ; une entrée de tunnel intelligent simple peut être créée pour ce processus.

Des applications plus complexes peuvent générer plusieurs processus. Dans la page WebVPN Portal, sélectionnez le panneau **Accès aux applications**. Dès qu'elle se charge, la liste des *applications autorisées* peut se connecter au côté privé du réseau.

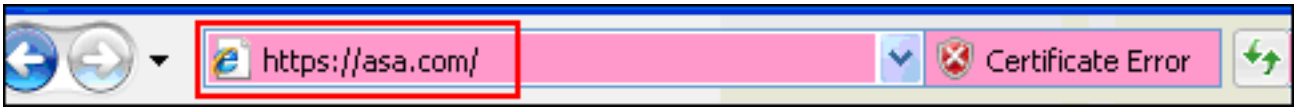
Si le processus échoue toujours, complétez ces étapes afin de recueillir les informations nécessaires, puis ouvrez un dossier TAC.

1. Effacez le cache du navigateur comme décrit dans Effacer le cache du navigateur.
2. Effacez le cache Java comme décrit dans Effacer le cache Java.
3. Désactivez le cache WebVPN sur l'ASA comme décrit dans Configuration de la mise en cache.
4. Si une applet Java est présente, utilisez le niveau de débogage 5 dans la fenêtre de l'applet comme décrit dans Activer les options de débogage de l'applet Java.
5. Connectez-vous à l'ASA via un VPN SSL sans client.
6. ÀlURL juste avant l'URL problématique, activez un outil de capture HTML dans le navigateur comme décrit dans Activer les outils de capture HTML.
7. Capturez la séquence de ce point vers l'URL problématique.
8. Appuyez sur **Ctrl+Impr écran** sur votre clavier afin de capturer une capture d'écran.
9. Arrêtez l'outil de capture HTML.
10. Exécutez les étapes 1 à 9 lorsque vous vous connectez directement à l'URL via une session IPsec ou Any Connect SSL via l'ASA ou que vous vous connectez directement sur le même segment LAN (si possible), complétez ces étapes et envoyez les données au TAC pour analyse

Procédures

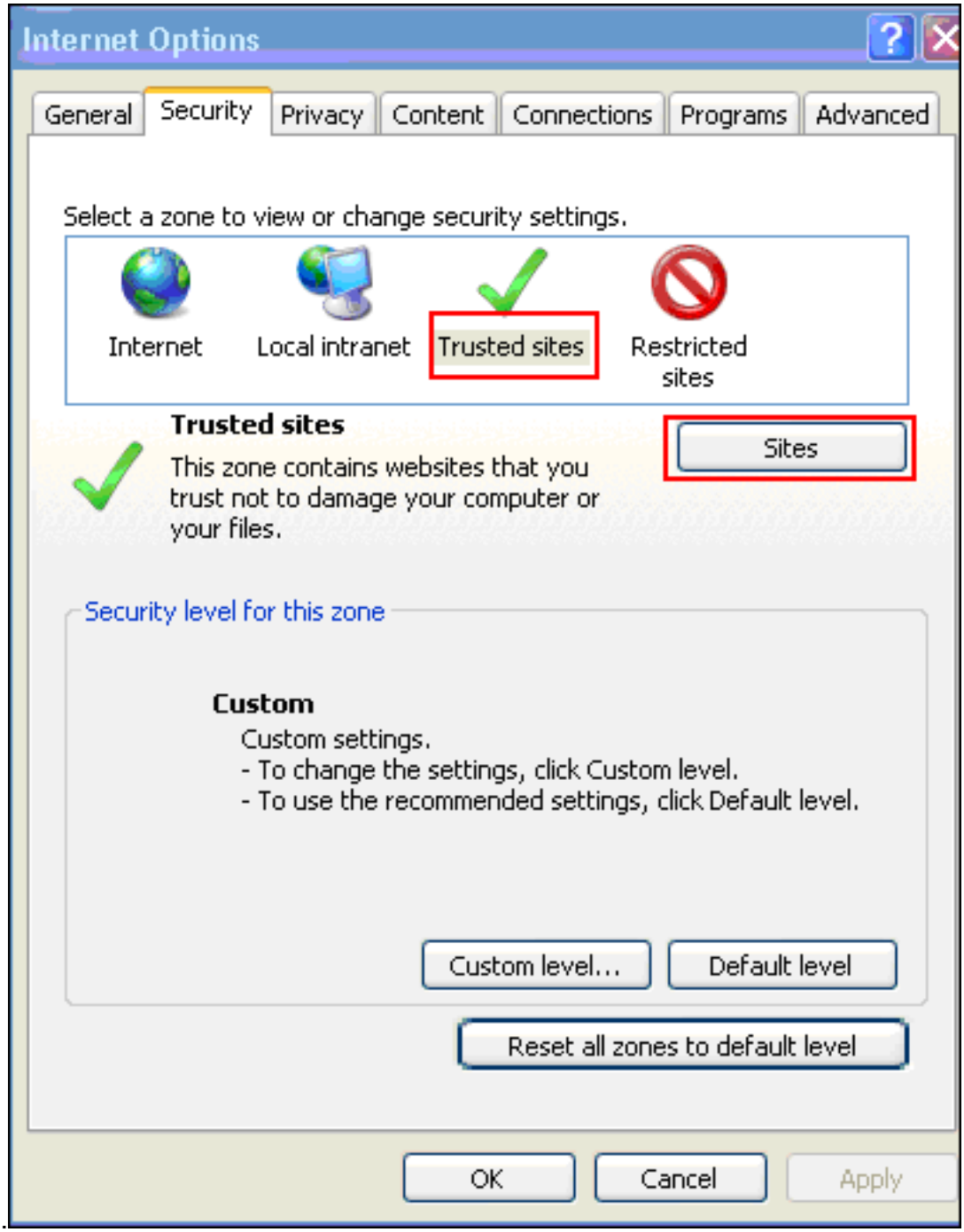
Ajouter l'ASA en tant que site de confiance

Lorsque vous accédez à l'ASA dans Internet Explorer, vous recevez une erreur de certificat si le site n'est pas inclus en tant que site approuvé.



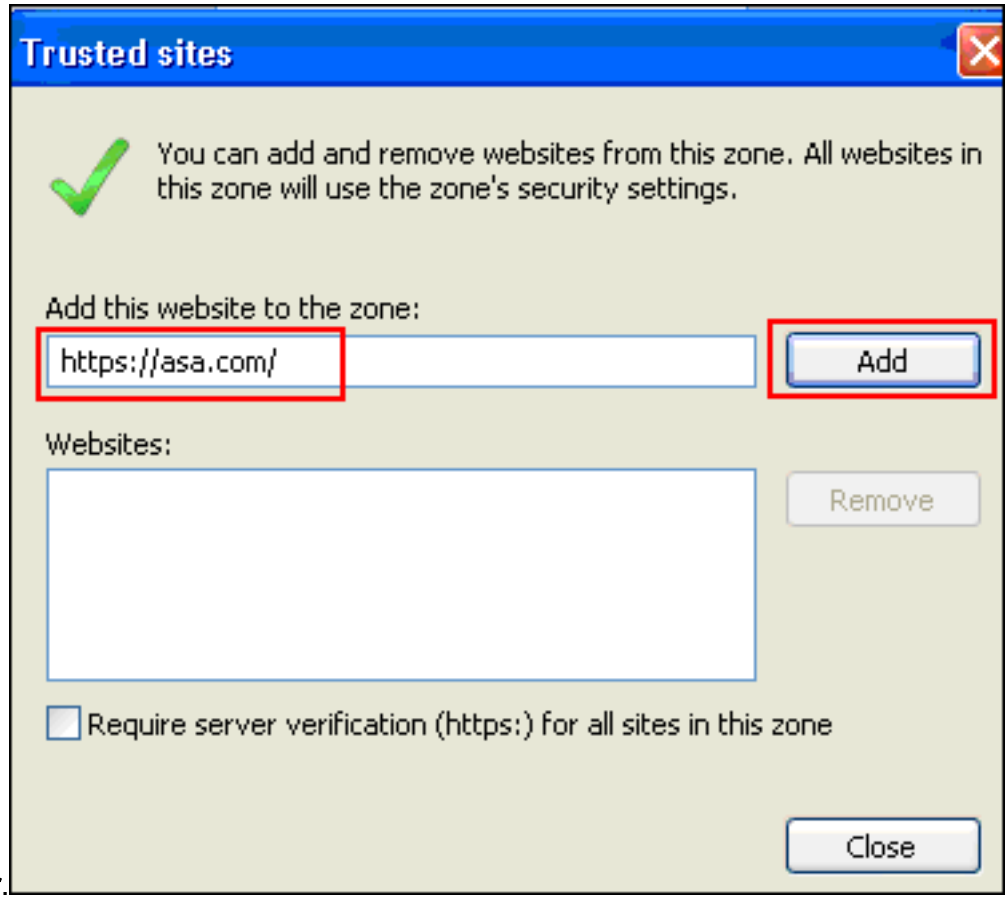
Complétez ces étapes afin d'ajouter l'ASA en tant que site approuvé :

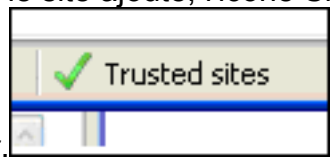
1. Dans Internet Explorer, sélectionnez **Outils > Options Internet**.
2. Cliquez sur l'onglet **Sécurité**, puis sélectionnez **Sites de**



confiance.

3. Cliquez sur **Sites**.
4. Ajoutez l'adresse https:// de l'ASA, puis cliquez sur

Ajouter. 

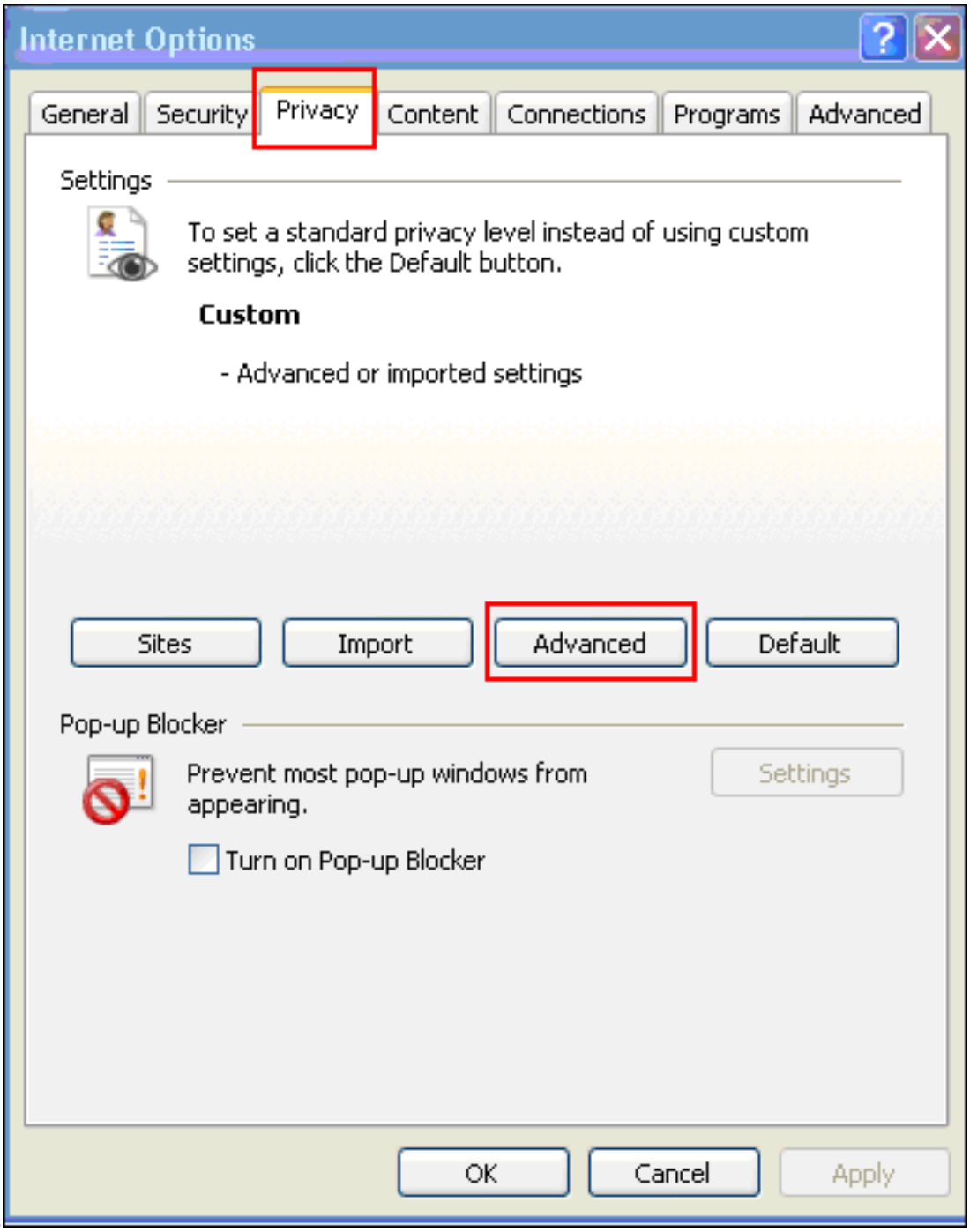
5. Une fois le site ajouté, l'icône Sites de confiance apparaît dans la barre d'état d'Internet Explorer. 

Remarque : Reportez-vous à Utilisation des paramètres de sécurité d'Internet Explorer 6 pour obtenir des informations détaillées sur cette procédure.

Activer les cookies

Complétez ces étapes afin d'activer les cookies :

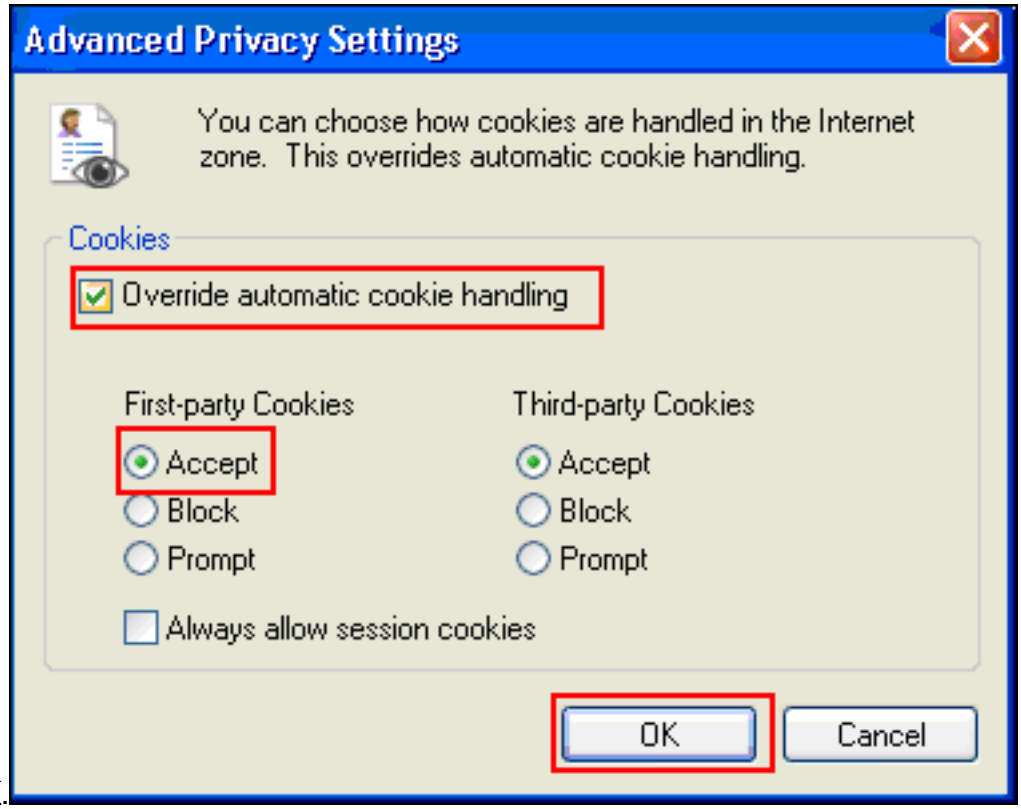
1. Dans Internet Explorer, sélectionnez **Outils > Options Internet**.
2. Cliquez sur l'onglet **Confidentialité**, puis sur



Avancé.

3. Dans la boîte de dialogue Paramètres de confidentialité avancés, cochez la case **Remplacer la gestion automatique des cookies**, cliquez sur la case d'option **Accepter**, puis cliquez sur

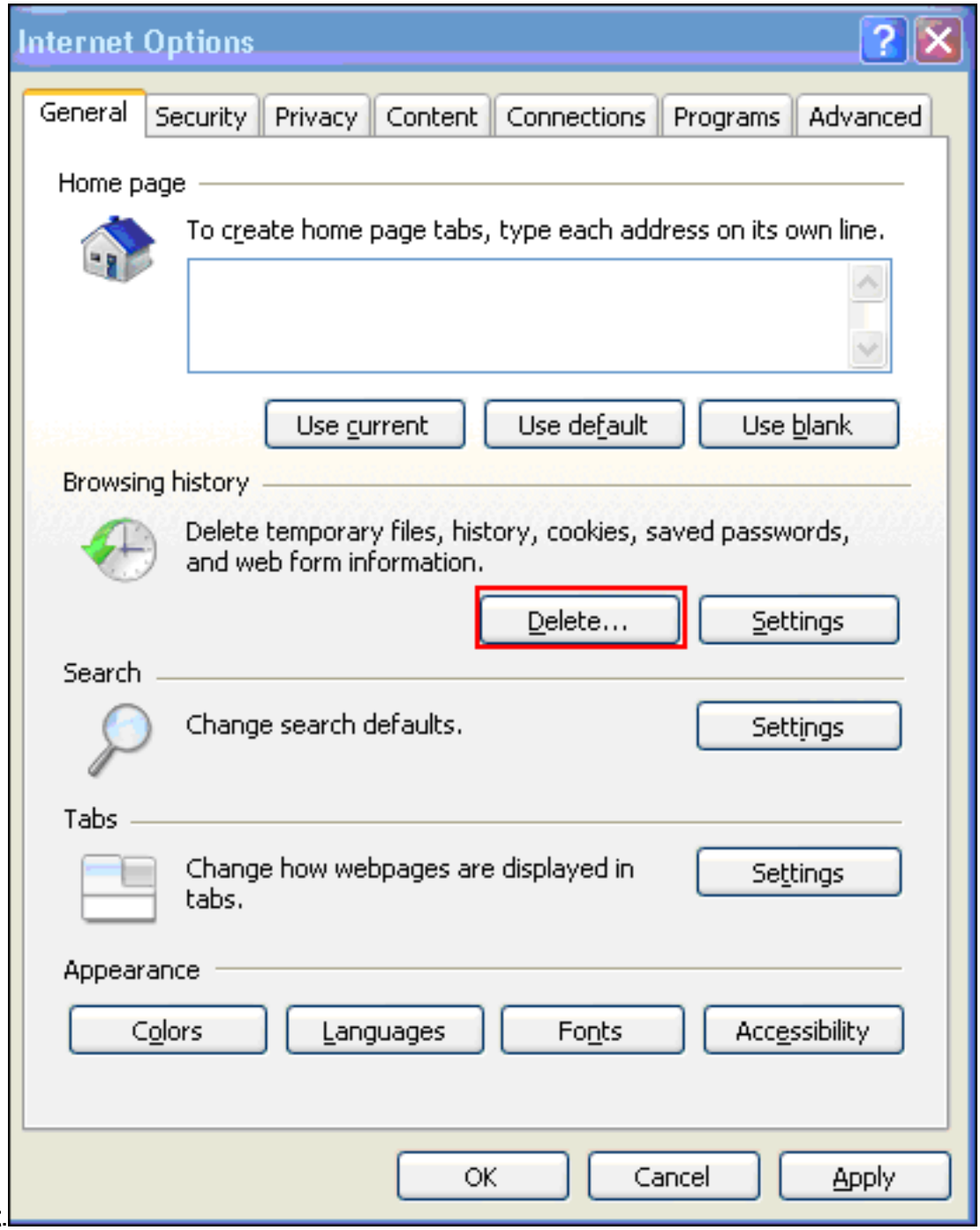
OK.



Effacer le cache du navigateur

Complétez ces étapes afin de vider le cache d'Internet Explorer :

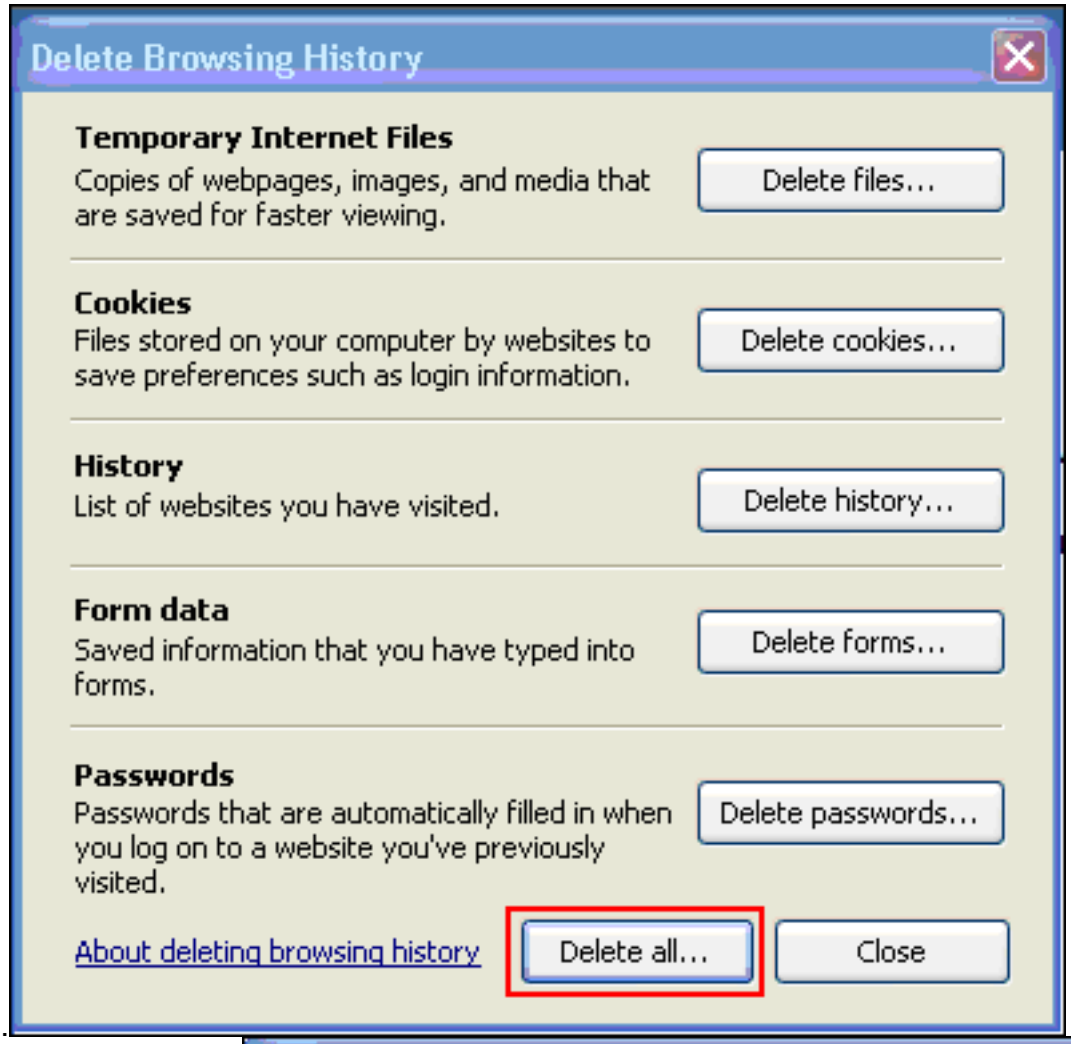
1. Dans Internet Explorer, sélectionnez **Outils > Options**

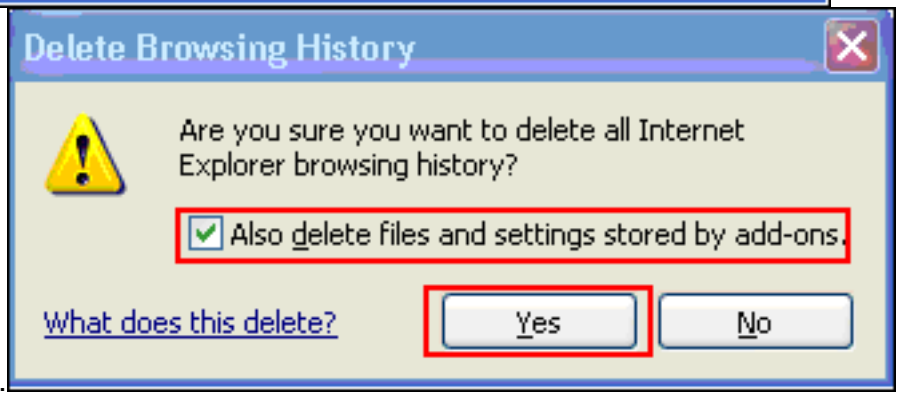


Internet.

2. Dans l'onglet Général, cliquez sur **Supprimer** dans la section Historique de

navigation.





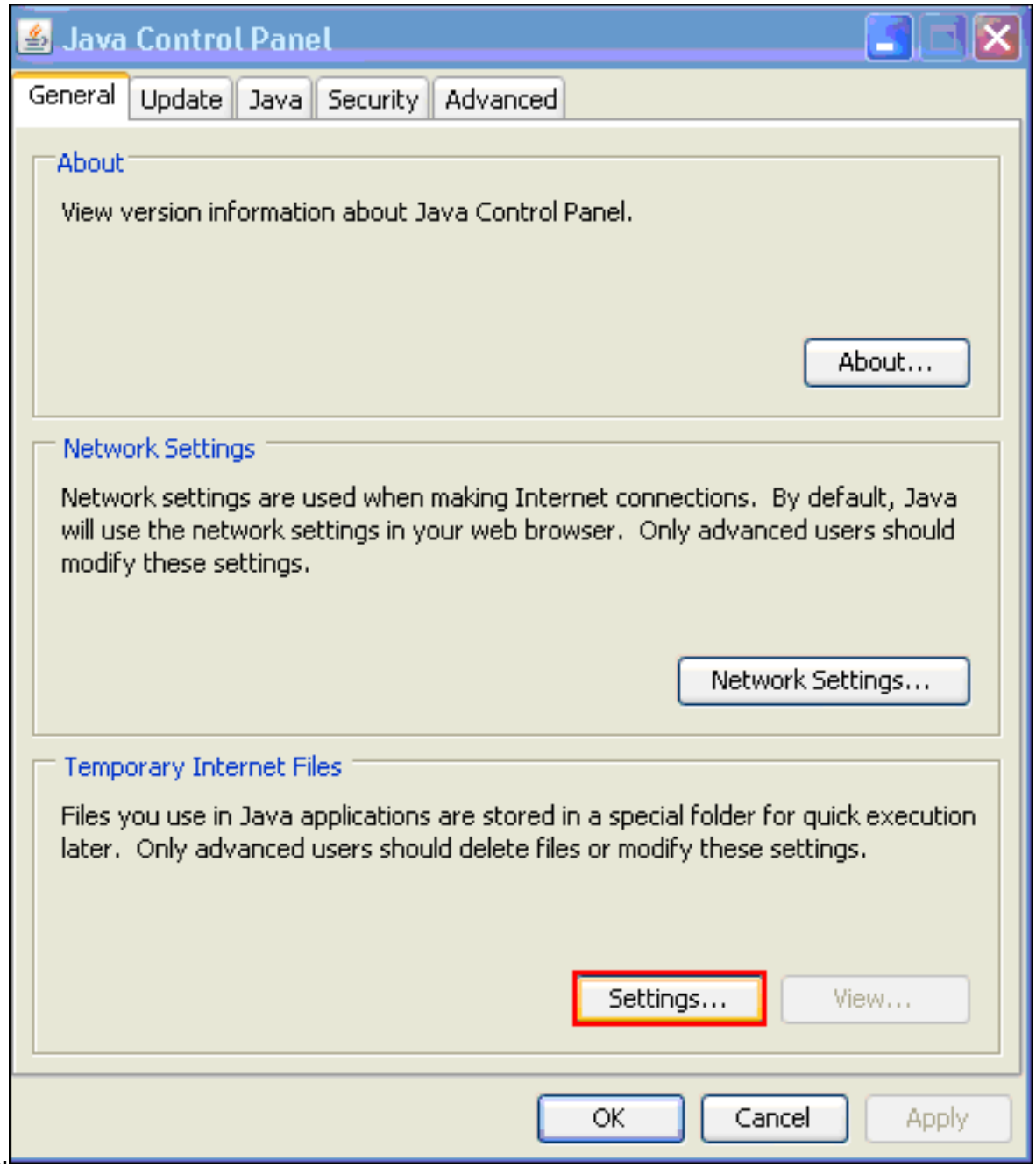
3. Cliquez sur **Supprimer tout**.
4. Cochez la case **Supprimer également les fichiers et les paramètres stockés par les modules complémentaires**, puis cliquez sur **Oui**.
5. Une fois le cache effacé, arrêtez toutes les instances du navigateur et redémarrez le navigateur.

Remarque : Pour effacer le cache des autres navigateurs, référez-vous à Comment effacer le cache de mon navigateur (pour améliorer ses performances) ?

Effacer le cache Java

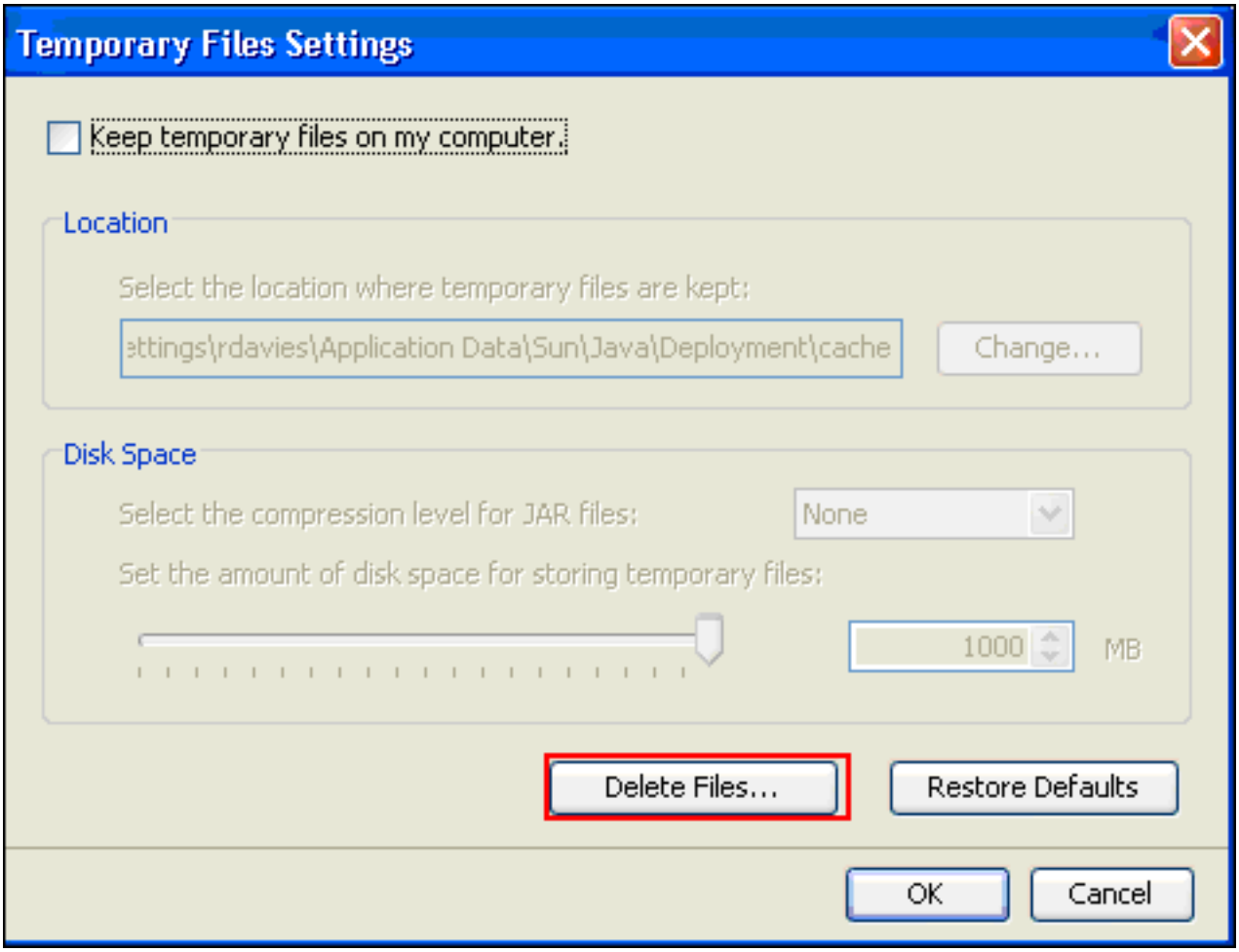
Complétez ces étapes afin d'effacer le cache Java :

1. Choisissez **Panneau de configuration** dans le menu Démarrer de Windows.
2. Double-cliquez sur



Java.

3. Cliquez sur **Paramètres**.
4. Cliquez sur **Supprimer les fichiers**.

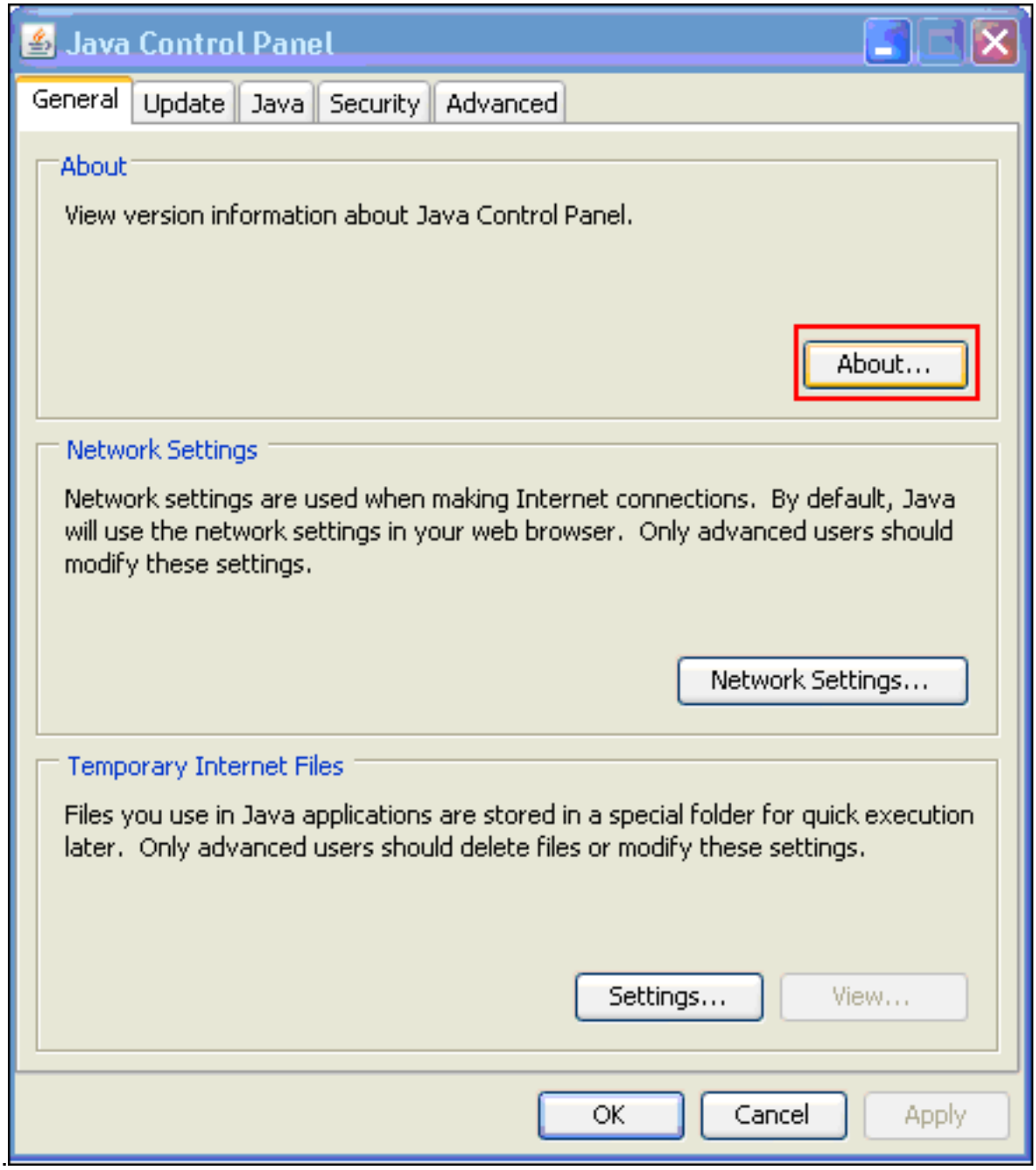


Note : Reportez-vous à Comment effacer mon cache Java ? pour plus d'informations sur cette procédure.

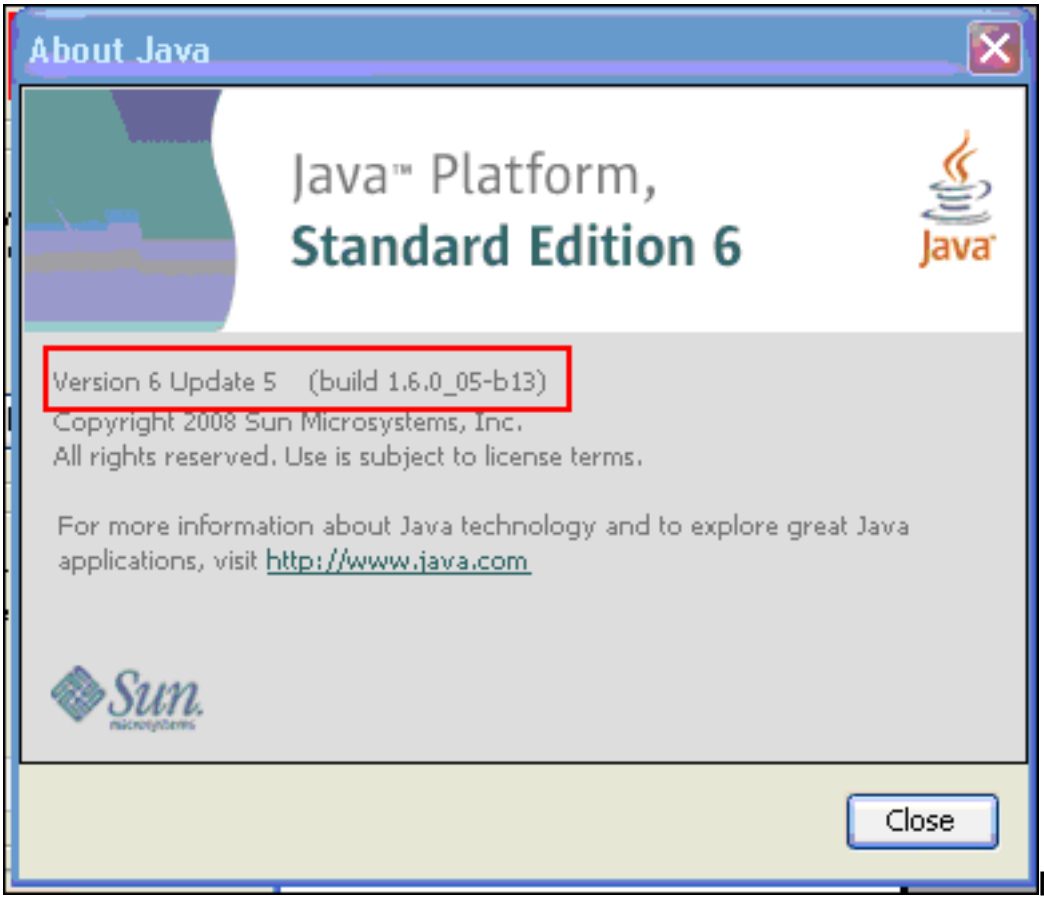
Activer les options de débogage d'applet Java

Complétez ces étapes afin d'activer l'option de débogage de l'applet Java :

1. Vérifiez que Java 1.4 ou version ultérieure est activé :Choisissez **Panneau de configuration** dans le menu Démarrer de Windows.Double-cliquez sur **Java**.Cliquez sur **À propos**, puis vérifiez le numéro de

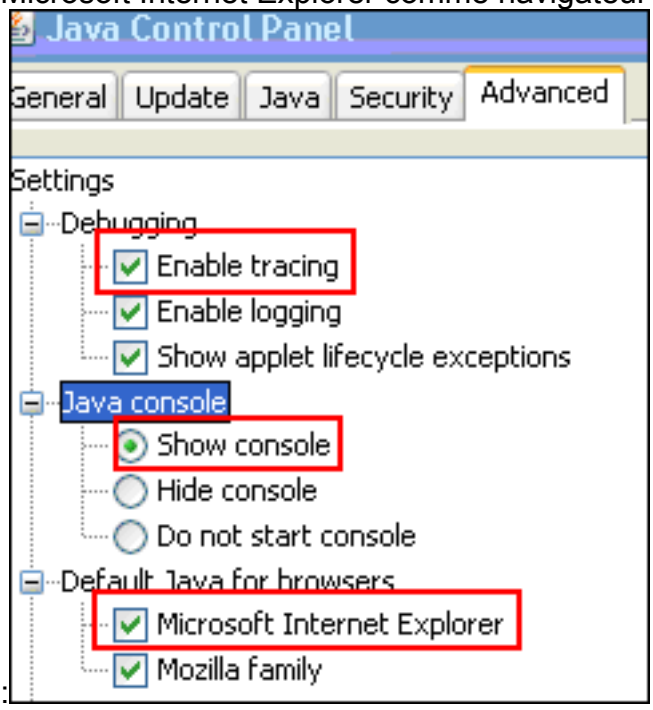

Java Control Panel
General
Update
Java
Security
Advanced
About
View version information about Java Control Panel.
About...
Network Settings
Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify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

version.

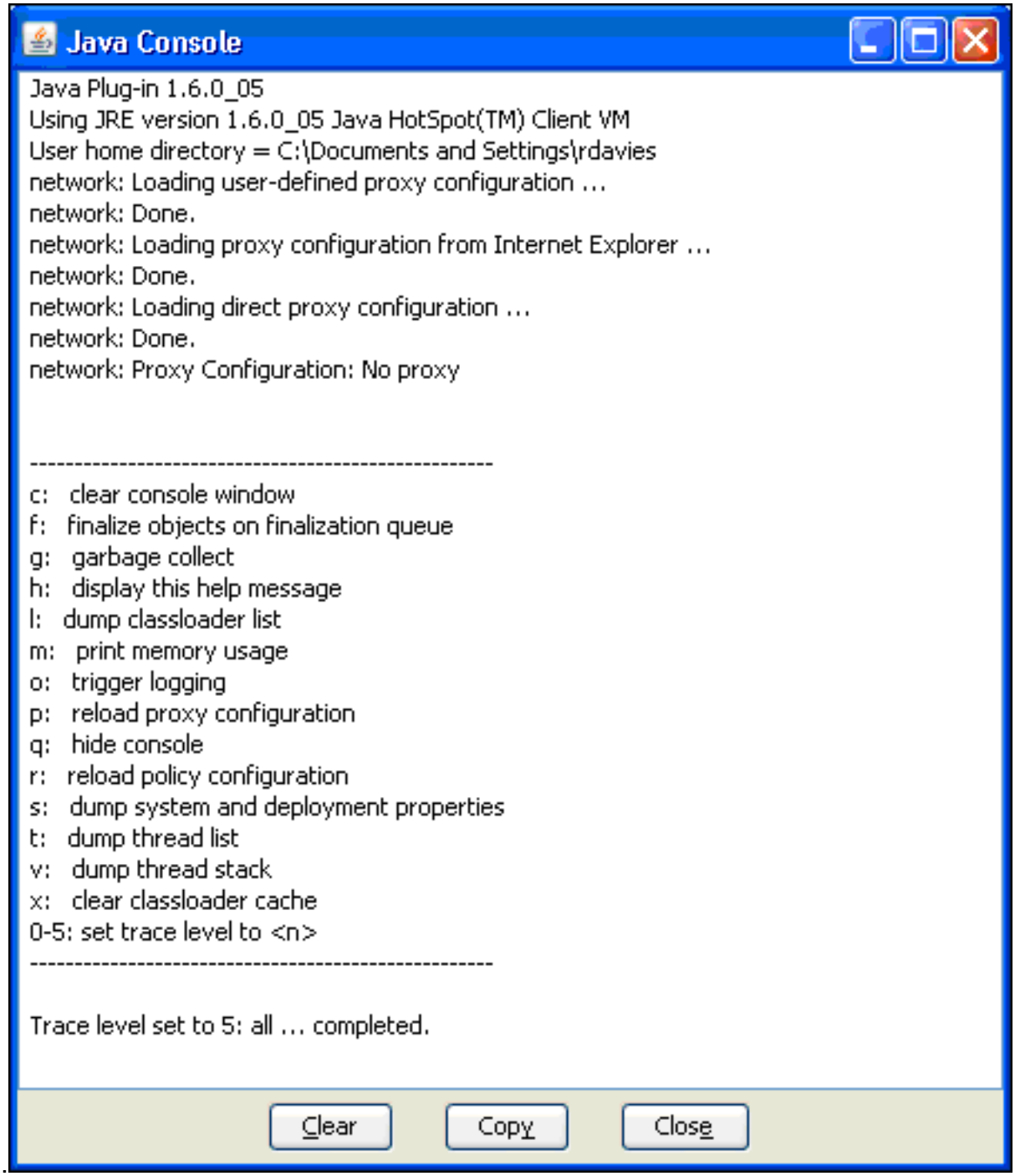


Note : Vous pouvez télécharger les mises à jour Java à partir de http://java.com/en/ .

2. Assurez-vous que Java est configuré pour activer le suivi, afficher la console et définir Microsoft Internet Explorer comme navigateur par défaut, comme illustré dans cette image :



3. Assurez-vous que le cache Java est effacé comme décrit dans Effacer le cache Java.
4. Dans Internet Explorer, sélectionnez **Outils > Console Java** afin d'ouvrir la fenêtre de débogage



Java.

5. Une fois la fenêtre de débogage de la console Java ouverte, appuyez sur **5** afin de définir le niveau de traceLorsqu'une URL contient une applet Java, l'activité est capturée dans cette fenêtre.
6. Cliquez sur **Copier** afin de copier les informations.

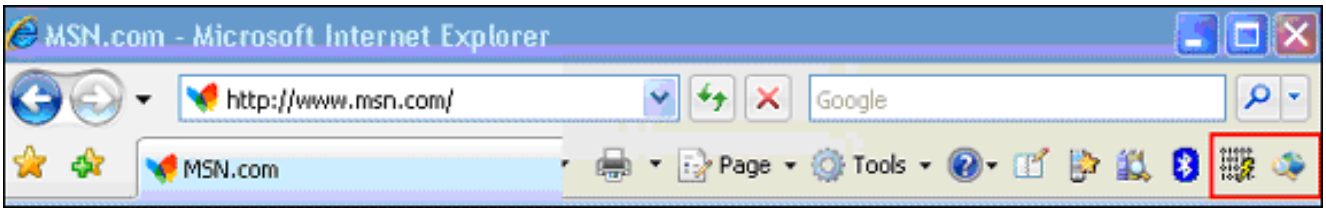
Activer les outils de capture HTML

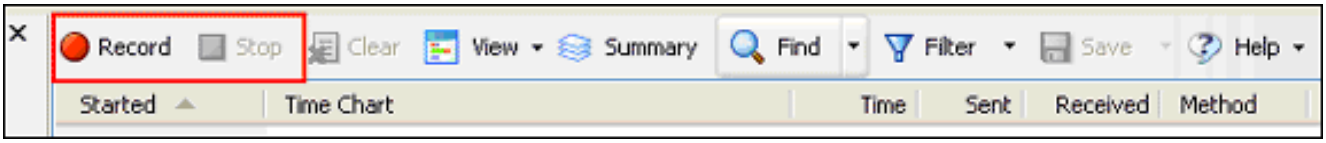
Différents outils de capture HTML sont disponibles pour recueillir des données, dont certaines sont répertoriées ici. Installez l'un de ces outils de capture HTML sur le PC client utilisé pour son exercice de collecte de données :

- HttpWatch
- Inspecteur IE
- Proxy de débogage

Remarque : cette procédure utilise l'application HTTPWatch.

Une fois l'application installée, procédez comme suit :

1. Appuyez sur Maj+P+F+2 ou cliquez sur l'icône dans la fenêtre du navigateur afin d'activer HTTPWatch.


2. Une fois l'application activée, une fenêtre s'affiche en bas de la fenêtre du navigateur, similaire à cette image
:


3. Cliquez sur **Enregistrer** afin d'enregistrer les données ; cliquez sur **Arrêter** afin d'arrêter l'enregistrement.

Note : Il est recommandé d'utiliser HttpWatch 7.x pour enregistrer les données.

Informations connexes

- Exemple de configuration d'un VPN SSL sans client (WebVPN) sur ASA
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Support et documentation techniques - Cisco Systems