Java 7 - Guida alla risoluzione dei problemi di AnyConnect, CSD/Hostscan e WebVPN

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi con Java 7 su Cisco AnyConnect Secure Mobility Client, Cisco Secure Desktop (CSD)/Cisco Hostscan e SSL VPN (WebVPN) senza client.

> **Nota:** Gli ID dei bug Cisco contrassegnati come investigativi non sono limitati ai sintomi descritti. In caso di problemi con Java 7, verificare di aggiornare il client AnyConnect alla versione più recente o almeno alla versione 3.1 della release 3 di manutenzione disponibile su Cisco Connection Online (CCO).

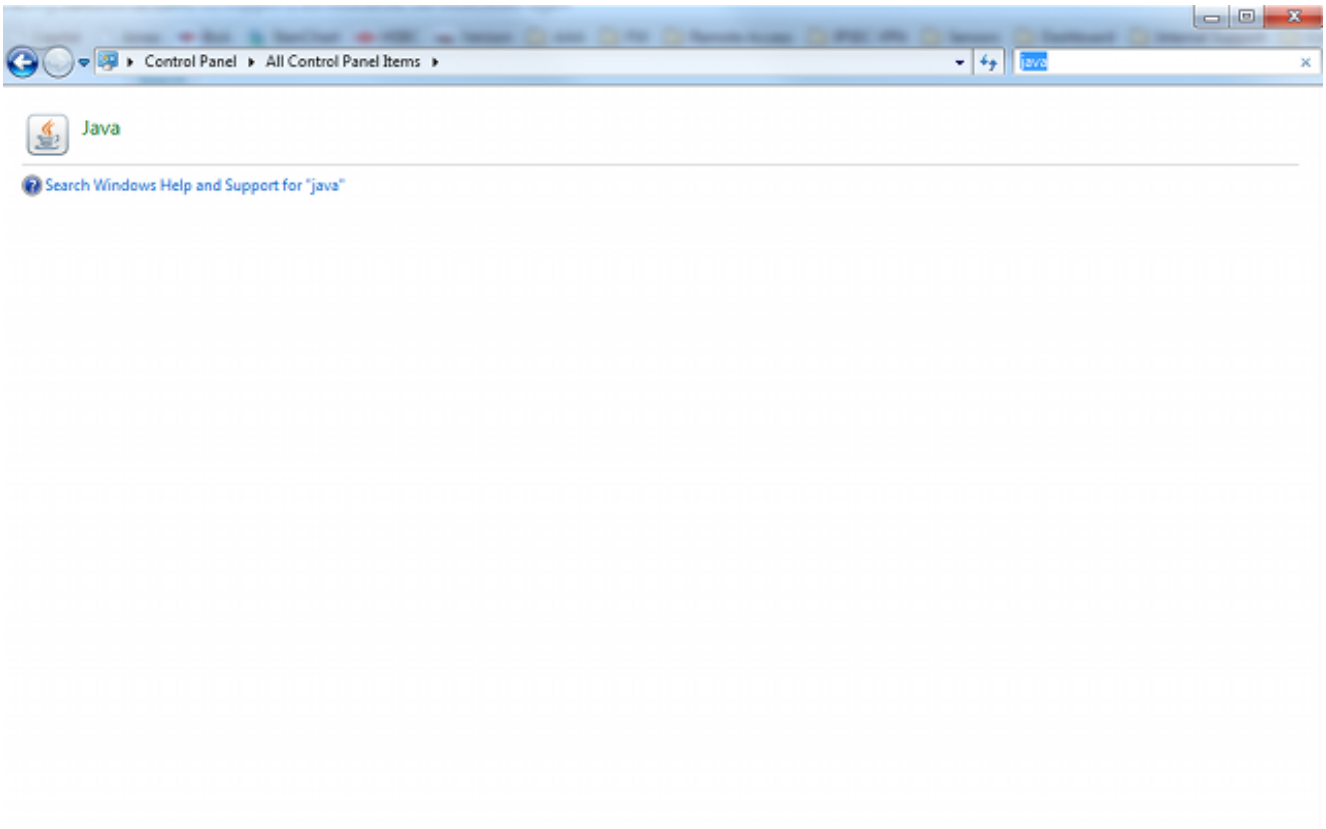
Risoluzione dei problemi generali

Eseguire Java Verifier per verificare se Java è supportato sui browser in uso. Se Java è abilitato correttamente, esaminare i log della console Java per analizzare il problema.

Windows

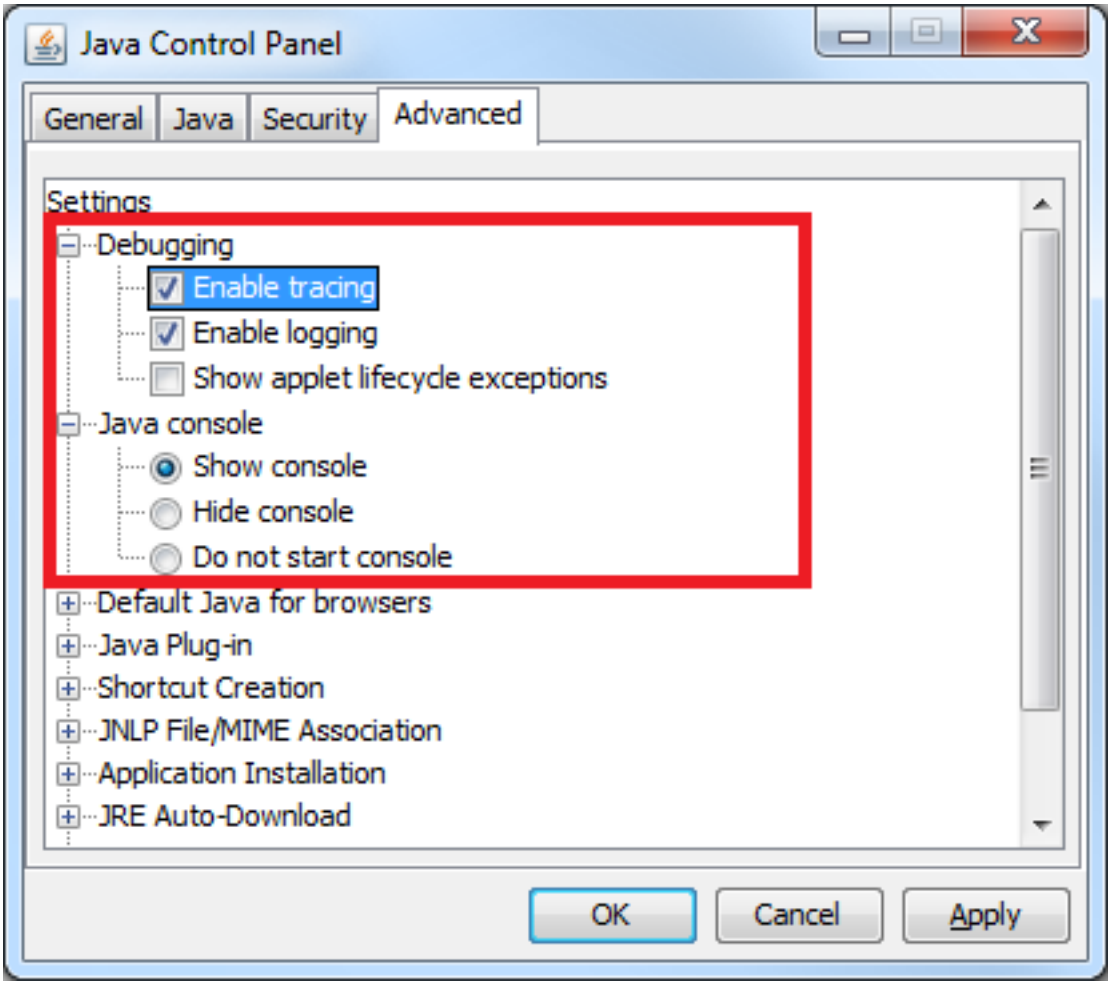
In questa procedura viene descritto come abilitare i log della console in Windows:

1. Aprire il Pannello di controllo di Windows e cercare Java.



2. Fare doppio clic su **Java** (icona della tazza di caffè). Viene visualizzato il Pannello di controllo Java.
3. Fare clic sulla scheda **Avanzate**.

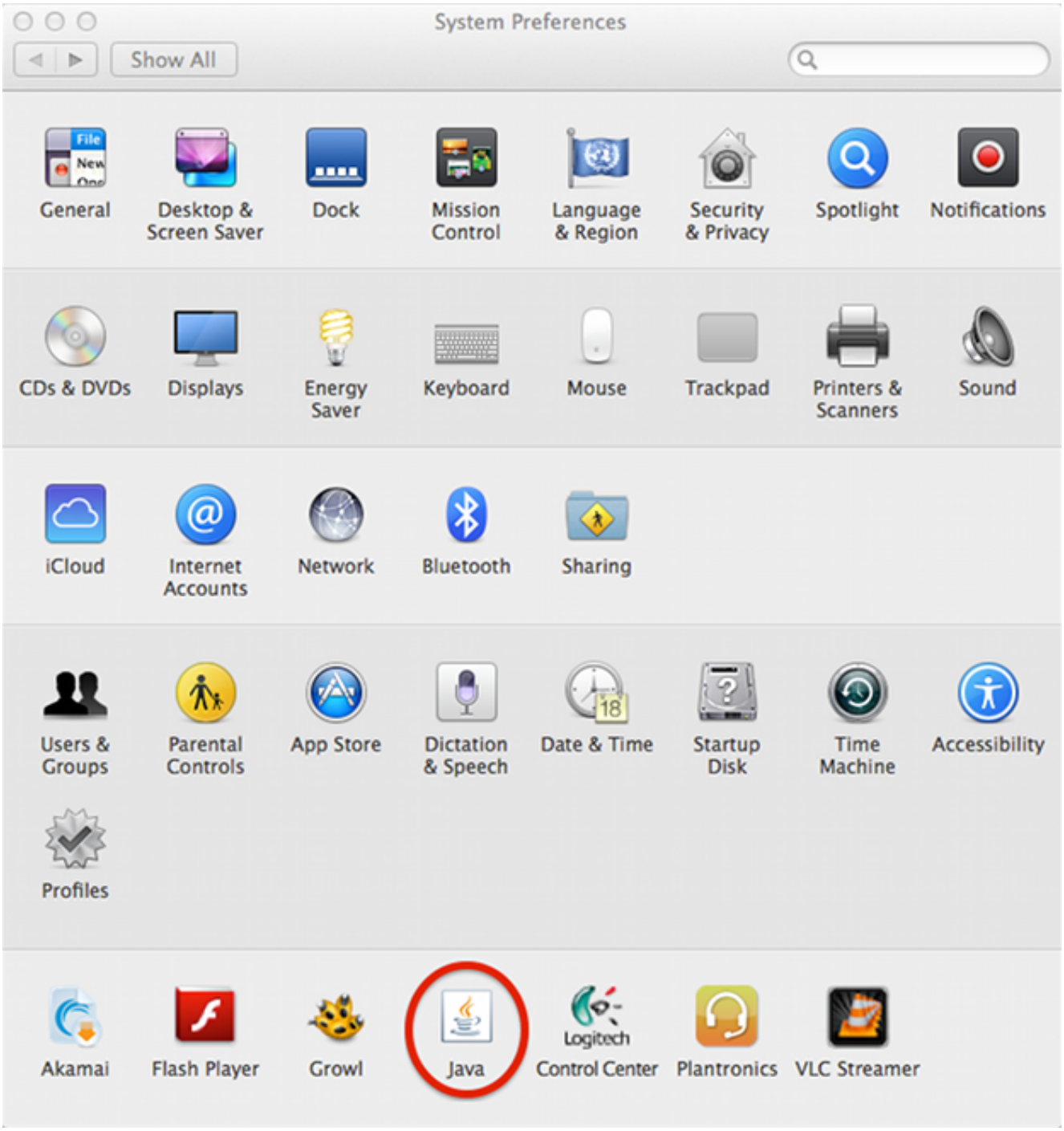
   Espandere **Debug** e selezionare **Abilita traccia** e **Abilita registrazione**.Espandere **Console Java** e fare clic su **Mostra console**.



Mac

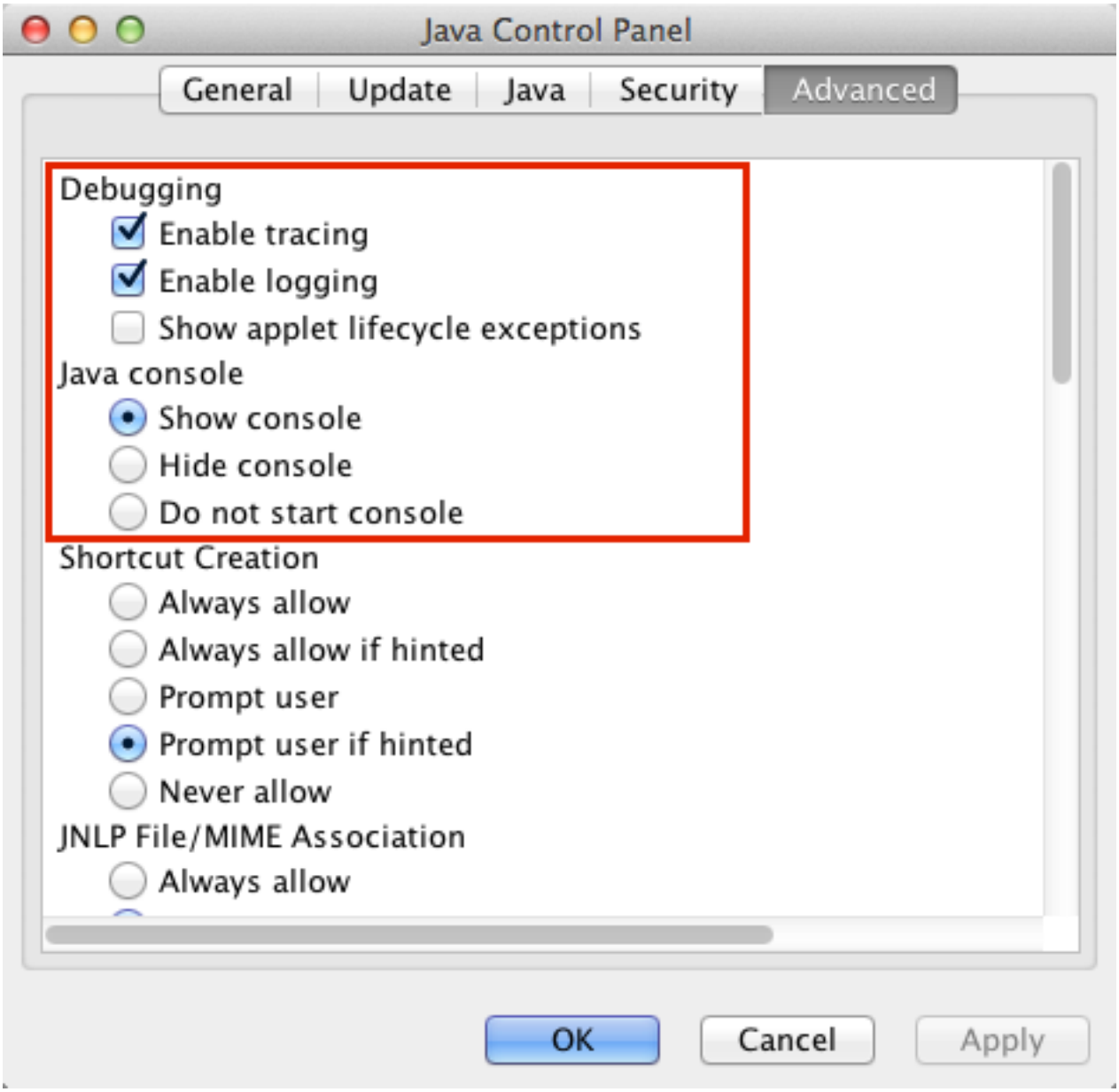
In questa procedura viene descritto come abilitare i log della console su un Mac:

1. Aprire Preferenze di sistema e fare doppio clic sull'icona Java (tazza da caffè). Viene visualizzato il Pannello di controllo Java.



2. Fare clic sulla scheda **Avanzate**.

   In Console Java fare clic su **Mostra console**.In Debug fare clic su **Attiva traccia** e **Attiva registrazione**.



Risoluzione dei problemi specifici

AnyConnect

Per i problemi relativi a AnyConnect, raccogliere i log di Diagnostic AnyConnect Reporting (DART) e i log della console Java.

Windows

L'ID bug Cisco CSCuc55720, "IE si blocca con Java 7 quando il pacchetto 3.1.1 è abilitato sull'appliance ASA", è un problema noto, quando Internet Explorer si blocca durante l'esecuzione di un WebLaunch e AnyConnect 3.1 viene abilitato sull'headend. Questo bug è stato risolto.

Potresti riscontrare dei problemi quando usi alcune versioni di AnyConnect e Java 7 con le app Java. Per ulteriori informazioni, vedere l'ID bug Cisco CSCue48916, "Java App(s) Break when using AnyConnect 3.1.00495 or 3.1.02026 & Java v7".

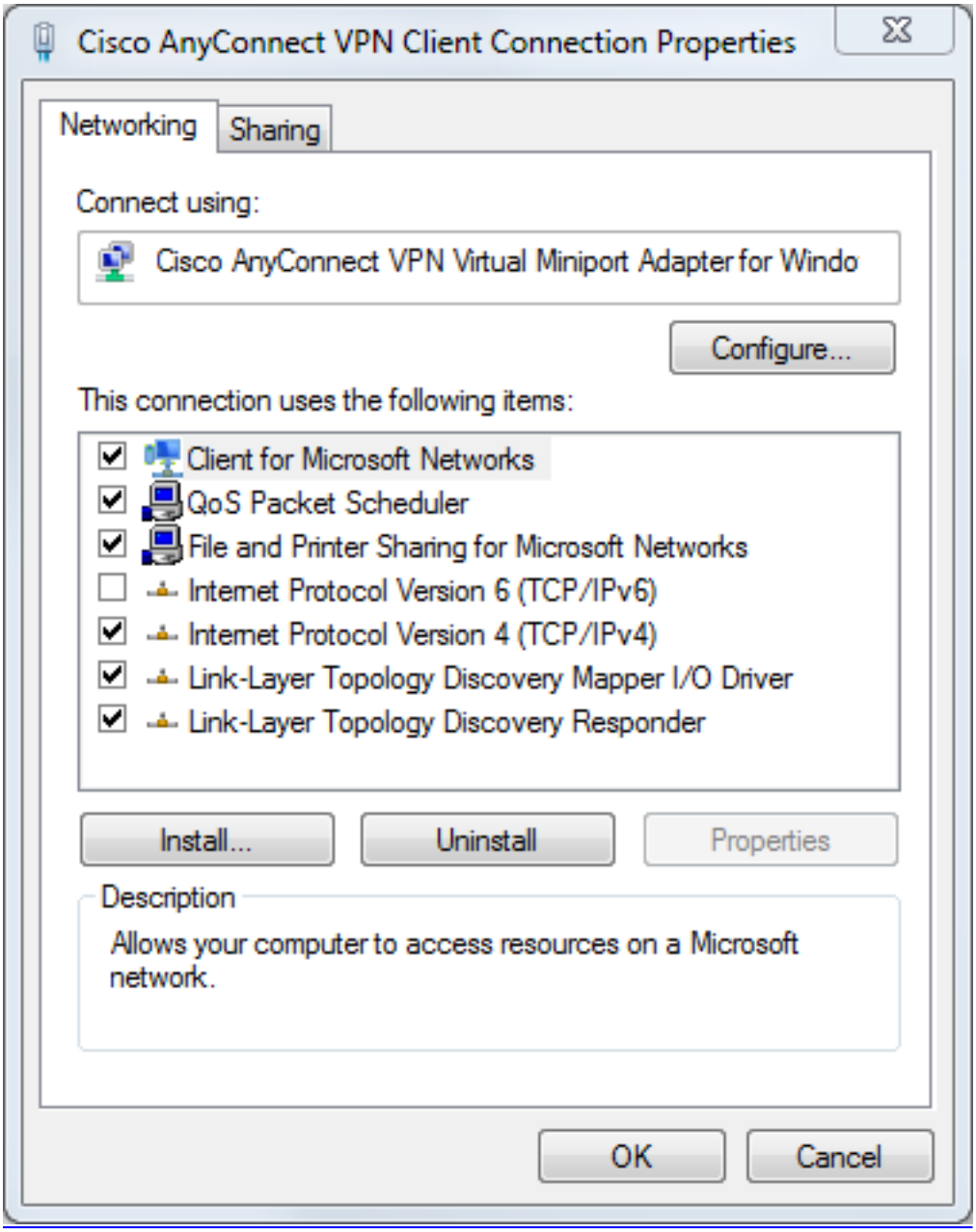
Problemi con le chiamate di socket Java 7 e IPv6

Se AnyConnect non si connette anche dopo aver aggiornato Java Runtime Environment (JRE) a Java 7 o se un'applicazione Java non è in grado di connettersi sul tunnel VPN, esaminare i log della console Java e cercare questi messaggi:

```
java.net.SocketException: Permission denied: connect
at java.net.DualStackPlainSocketImpl.waitForConnect(Native Method)
at java.net.DualStackPlainSocketImpl.socketConnect(Unknown Source)
```

Queste voci di registro indicano che il client/applicazione effettua chiamate IPv6.

Per risolvere questo problema, disabilitare il protocollo IPv6 (se non è in uso) sulla scheda Ethernet e sulla scheda virtuale AnyConnect (VA):



La seconda soluzione consiste nel configurare Java in modo che preferisca IPv4 a IPv6. Impostare la proprietà di sistema 'java.net.preferIPv4Stack' su 'true', come mostrato negli esempi seguenti:

- Aggiungere il codice per la proprietà di sistema al codice Java (per le applicazioni Java scritte dal cliente):

```
System.setProperty("java.net.preferIPv4Stack" , "true");
```

- Aggiungere il codice per la proprietà system dalla riga di comando:

```
-Djava.net.preferIPv4Stack=true
```

- Impostare le variabili di ambiente _JPI_VM_OPTIONS e _JAVA_OPTIONS in modo da includere la proprietà di sistema:

```
-Djava.net.preferIPv4Stack=true
```

Per ulteriori informazioni, fare riferimento a:

- Come impostare java.net.preferIPv4Stack=true nel codice Java?
- Come forzare Java a utilizzare ipv4 anziché ipv6?

Una terza soluzione consiste nel disabilitare completamente IPv6 sui computer Windows; modificare questa voce del registro di sistema:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TCPIP6\Parameters
```

Per ulteriori informazioni, vedere Come disabilitare IP versione 6 o i relativi componenti specifici in Windows.

Problemi di AnyConnect WebLaunch dopo l'aggiornamento a Java 7

Il codice JavaScript Cisco cercava Sun come valore per il fornitore Java. Tuttavia, Oracle ha modificato tale valore come descritto in JDK7: Modifiche alle proprietà del fornitore Java. Il problema è stato risolto con l'ID bug Cisco CSCub46241, "AnyConnect weblaunch fail from Internet Explorer with Java 7".

Mac

Non sono stati segnalati problemi. I test con AnyConnect 3.1 (con la configurazione WebLaunch / Safari / Mac 10.7.4 / Java 7.10) non mostrano errori.

Varie

Problemi con le applicazioni Java 7 su Cisco AnyConnect

Èstato archiviato l'ID bug Cisco CSCue48916, "Java App(s) Break when using AnyConnect 3.1.00495 or 3.1.02026 & Java v7". L'indagine iniziale indica che i problemi non sono un bug sul lato client, ma potrebbero essere correlati alla configurazione della Java Virtual Machine (VM).

In precedenza, per usare le app Java 7 sul client AnyConnect 3.1(2026), sono state deselezionate le impostazioni della scheda virtuale IPv6. Tuttavia, è ora necessario completare tutte le fasi di questa procedura:

1. Installare AnyConnect versione 3.1(2026).
2. Disinstallare Java 7.
3. Riavviare.
4. Installare Java SE 6, update 38, disponibile sul sito Web Oracle.
5. Passare alle impostazioni del Pannello di controllo di Java 6, quindi fare clic sulla scheda **Aggiorna** per eseguire l'aggiornamento alla versione più recente di Java 7.
6. Aprire un prompt dei comandi e immettere:

```
setx _JAVA_OPTIONS -Djava.net.preferIPv4Stack=true
```

7. Accedere con AnyConnect e le app Java dovrebbero funzionare.

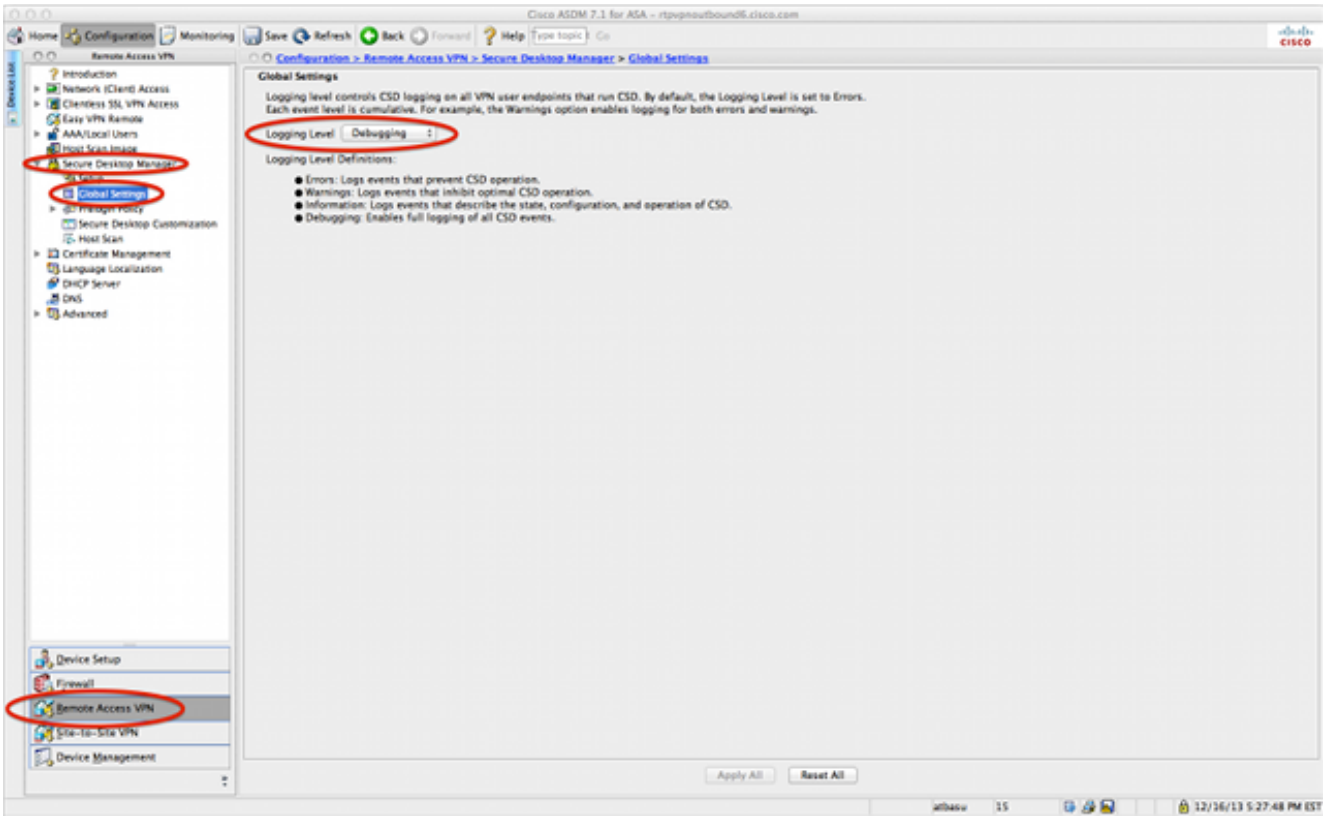
Nota: Questa procedura è stata testata con Java 7 aggiornamenti 9, 10 e 11.

CSD/Hostscan

Per i problemi relativi a CSD/Hostscan, raccogliere i log DART e i log della console Java.

Per ottenere i log DART, il livello di log CSD deve essere impostato su debug sull'appliance ASA:

1. Selezionare ASDM > **Configurazione > VPN ad accesso remoto > Secure Desktop Manager > Impostazioni globali**.
2. Attivare la registrazione CSD per il debug in Cisco Adaptive Security Device Manager (ASDM).
3. Utilizzare DART per raccogliere i registri CSD/Hostscan.



Windows

Hostscan è suscettibile di arresti anomali simili a quelli descritti precedentemente per AnyConnect in Windows (ID bug Cisco CSCuc5720). Il problema relativo all'hostscan è stato risolto dall'ID bug Cisco CSCuc48299, "IE with Java 7 crashed on HostScan Weblaunch".

Mac

Problemi con CSD versioni 3.5.x e Java 7

In CSD 3.5.x, tutte le connessioni WebVPN hanno esito negativo; tra cui l'avvio del sito Web AnyConnect. I log della console Java non rivelano alcun problema:

```
Java Plug-in 10.10.2.12
Using JRE version 1.7.0_10-ea-b12 Java HotSpot(TM) 64-Bit Server VM
User home directory = /Users/rtpvpn
----------------------------------------------------
c: clear console window
f: finalize objects on finalization queue
g: garbage collect
h: display this help message
l: dump classloader list
m: print memory usage
o: trigger logging
q: hide console
r: reload policy configuration
s: dump system and deployment properties
t: dump thread list
v: dump thread stack
x: clear classloader cache
```

```
0-5: set trace level to <n>
----------------------------------------------------
```

Se si esegue il downgrade a JRE 6 o si aggiorna CSD alla versione 3.6.6020 o successive, i log della console Java rivelano i problemi:

```
Java Plug-in 10.10.2.12
Using JRE version 1.7.0_10-ea-b12 Java HotSpot(TM) 64-Bit Server VM
User home directory = /Users/rtpvpn
----------------------------------------------------
c: clear console window
f: finalize objects on finalization queue
g: garbage collect
h: display this help message
l: dump classloader list
m: print memory usage
o: trigger logging
q: hide console
r: reload policy configuration
s: dump system and deployment properties
t: dump thread list
v: dump thread stack
x: clear classloader cache
0-5: set trace level to <n>
----------------------------------------------------
CacheEntry[ https://rtpvpnoutbound6.cisco.com/CACHE/sdesktop/install/binaries/
instjava.jar ]: updateAvailable=false,lastModified=Wed Dec 31 19:00:00 EST
1969,length=105313
Fri Oct 19 18:12:20 EDT 2012 Downloaded
https://rtpvpnoutbound6.cisco.com/CACHE/sdesktop/hostscan/darwin_i386/cstub
to /var/folders/zq/w7l9gxks7512fsl4vk07v9nc0000gn/T/848638312.tmp/cstub
Fri Oct 19 18:12:20 EDT 2012 file signature verification
PASS: /var/folders/zq/w7l9gxks7512fsl4vk07v9nc0000gn/T/848638312.tmp/cstub
Fri Oct 19 18:12:20 EDT 2012 Spawned CSD stub.
```

La soluzione è aggiornare CSD o declassare Java. Poiché Cisco consiglia di eseguire l'ultima versione di CSD, è consigliabile aggiornare CSD, anziché eseguire il downgrade di Java, soprattutto perché un downgrade di Java può essere difficile su un Mac.

Problemi con Chrome e Safari con WebLaunch su Mac 10.8

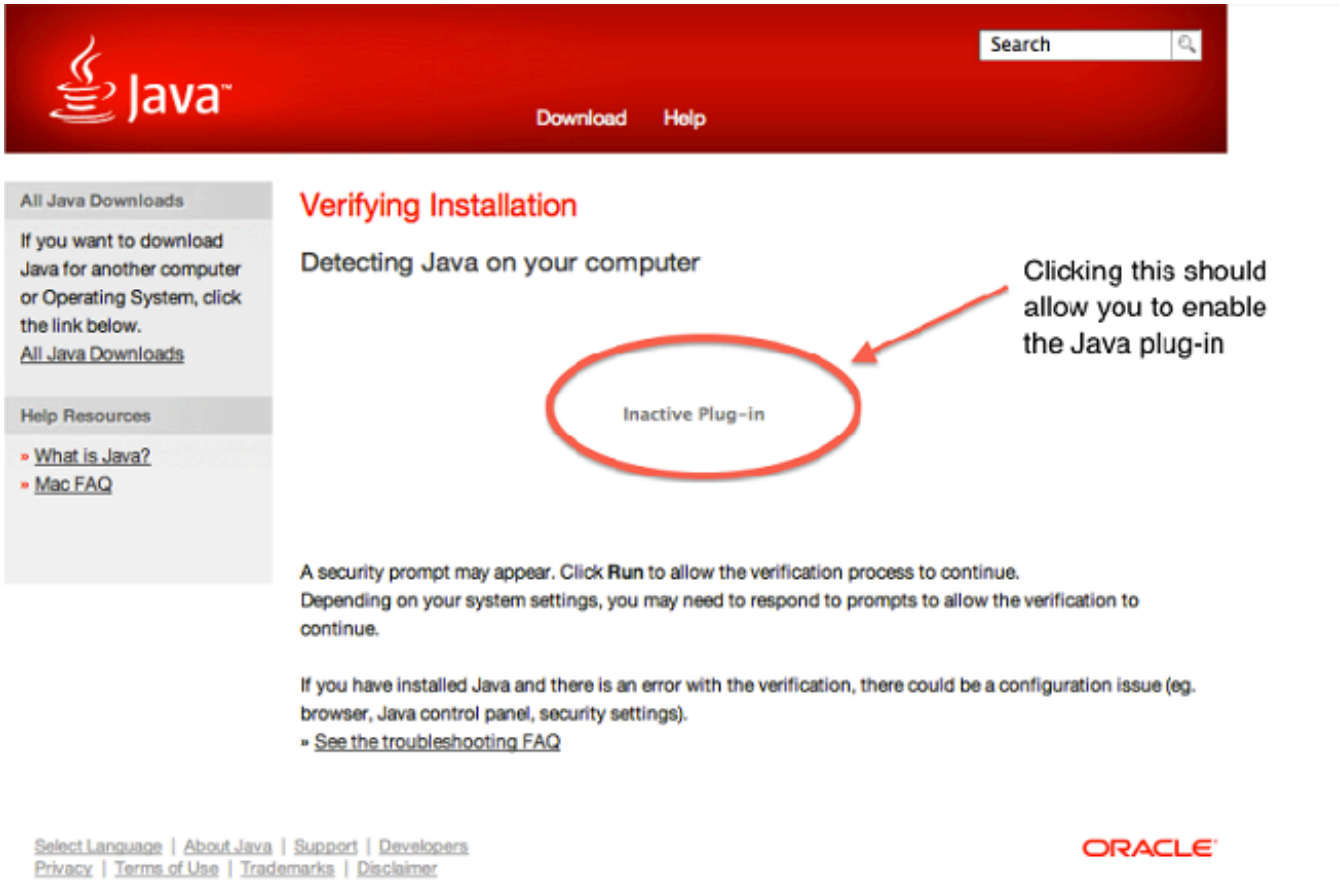
Problemi con Chrome e Safari sono attesi comportamento:

- Chrome è un browser a 32 bit e non supporta Java 7.
- Chrome non è mai stato un browser ufficialmente supportato per WebLaunch.
- Mac 10.8 disabilitò l'uso di Java 7 su Safari, e le versioni precedenti di Java non sono abilitate per impostazione predefinita.

Se Java 7 è già installato, le risoluzioni sono:

- Usa Firefox.
- Abilita Java 7 su Safari:

  Verificare che Java 7 sia installato sul Mac e che il Mac sia stato riavviato. Aprire Firefox e passare a Java Verifier.Aprire Safari e andare nuovamente a Java Verifier. A questo punto dovrebbe essere visualizzata questa schermata:



- Disabilitare Java 7 e abilitare Java SE 6 fornito da Apple.

  Suggerimento: Se non si dispone di Java o se si dispone di una versione precedente di Java, è probabile che venga visualizzato il messaggio di errore 'Java bloccato per questo sito Web' su java.com . Per informazioni sull'installazione degli aggiornamenti Java, vedere gli aggiornamenti Java disponibili per OS X il 28 agosto 2013 sul forum di supporto Apple.

Problemi con Safari con WebLaunch su Mac 10.9

Se siete su Mac 10.9 e avete già abilitato il plugin Java (come descritto nella sezione Problemi con Chrome e Safari con WebLaunch su Mac 10.8), WebLaunch potrebbe continuare a fallire. Tutte le applet Java vengono avviate, ma il browser continua semplicemente a girare. Se i log Java sono abilitati come descritto nella sezione Risoluzione dei problemi generali, i log vengono compilati rapidamente come mostrato di seguito:

```
at java.lang.Thread.run(Thread.java:744)
Mon Dec 16 16:00:17 EST 2013 Failed to download cstub
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
```

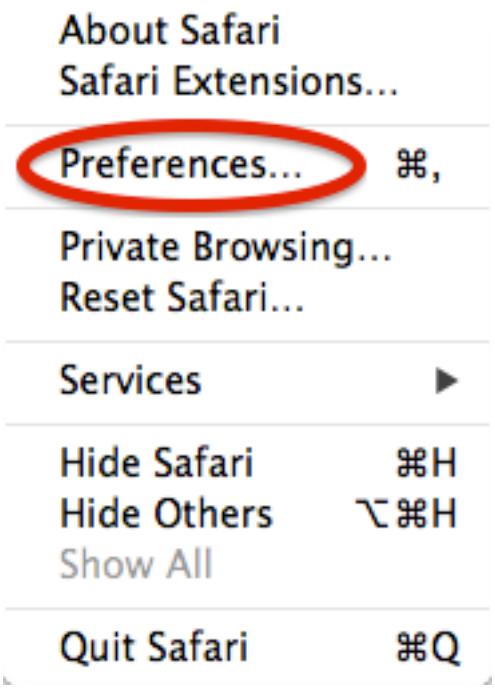
```
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
```

Cercare questo tipo di voce nel registro:

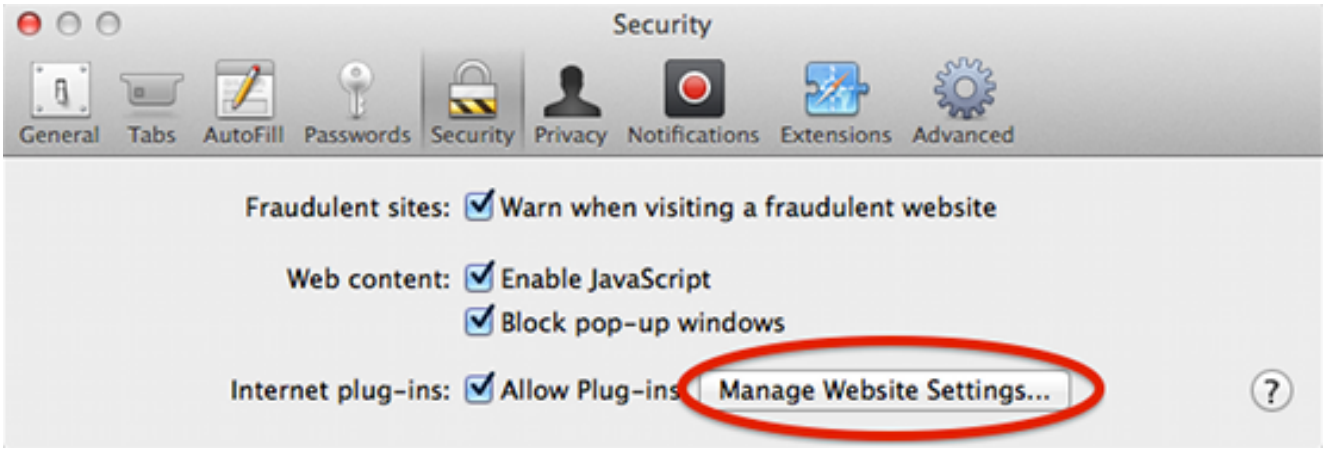
```
Mon Dec 16 16:00:17 EST 2013 Downloaded https://rave.na.sage.com/CACHE/
sdesktop/hostscan/darwin_i386/manifest java.io.FileNotFoundException:
/Users/user1/.cisco/hostscan/bin/cstub (Operation not permitted) at
java.io.FileInputStream.open(Native Method)
```

Ciò significa che si sta riscontrando l'ID bug Cisco CSCuj02425, "WebLaunch on OSX 10.9 fail if java unsafe mode is disabled" (Avvio Web su OSX 10.9 non riuscito se la modalità java unsafe è disabilitata). Per risolvere questo problema, modificare le preferenze Java in modo che Java possa essere eseguito in modalità non sicura per Safari:

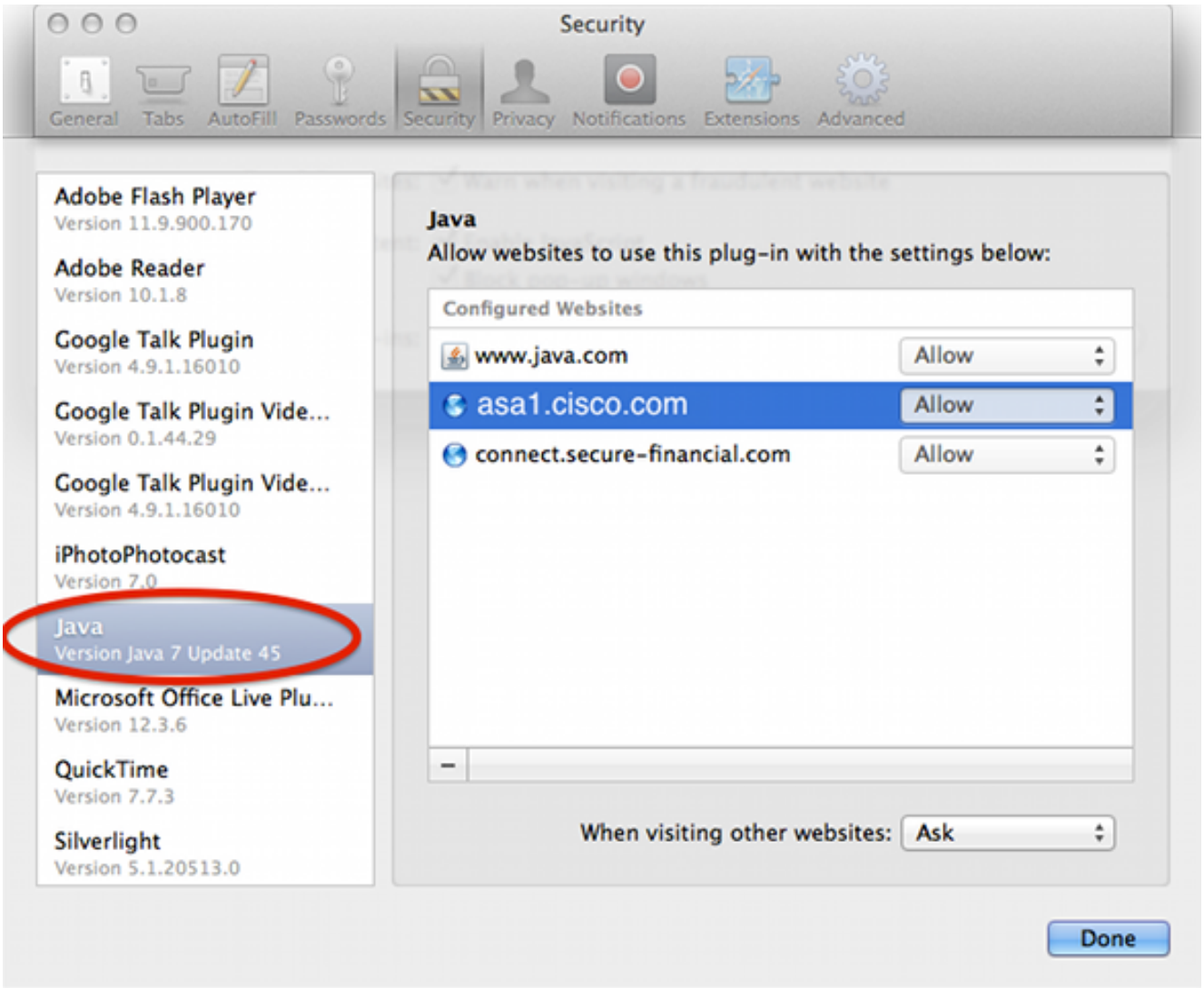
1. Fare clic su **Preferenze**.



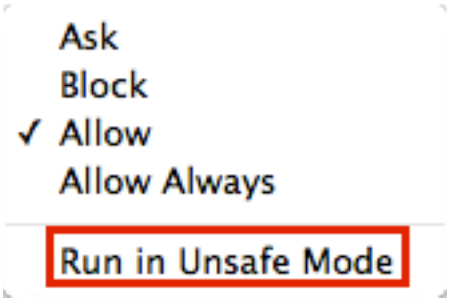
2. Fare clic su **Gestisci impostazioni sito Web**.



3. Nella scheda **Protezione**, selezionare **Java**, e notare che **Consenti** è selezionato per impostazione predefinita.



4. Modifica **Consenti l'esecuzione in modalità non sicura**.



WebVPN

Per i problemi di WebVPN relativi a Java, raccogliere questi dati per la risoluzione dei problemi:

- Output del comando **show tech-support**.
- I log della console Java vengono eseguiti con e senza Adaptive Security Appliance (ASA), come spiegato nella sezione Risoluzione dei problemi generali.
- Clip WebVPN.
- Il controllo HTTP viene acquisito sul computer locale con e senza ASA.
- I pacchetti standard vengono acquisiti sull'appliance ASA e sul computer locale. Sul computer locale, queste riprese possono essere effettuate con Wireshark.Per informazioni su come acquisire il traffico sull'appliance ASA, vedere Configurazione delle acquisizioni di pacchetti.
- Tutti i file jar scaricati nella cache Java durante l'esecuzione dell'appliance ASA. Questo è un esempio tratto dalla console Java:

```
Reading Signers from 8412
https://rtpvpnoutbound6.cisco.com/+CSCO+00756767633A2F2F7A2D73767972662E6
E7067727A76687A2E6179++/mffta.jar
C:\Users\wvoosteren\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\41\
6a0665e9-1f510559.idx
```

  In questo esempio, 6a0665e9-1f510559.idx è la versione memorizzata nella cache di mffta.jar 7. Se non si dispone dell'accesso a questi file, è possibile raccoglierli dalla cache Java quando si utilizza la connessione diretta.

Una configurazione di test può accelerare la risoluzione.

Funzioni di sicurezza in Java 7 U51 e impatto sugli utenti WebVPN

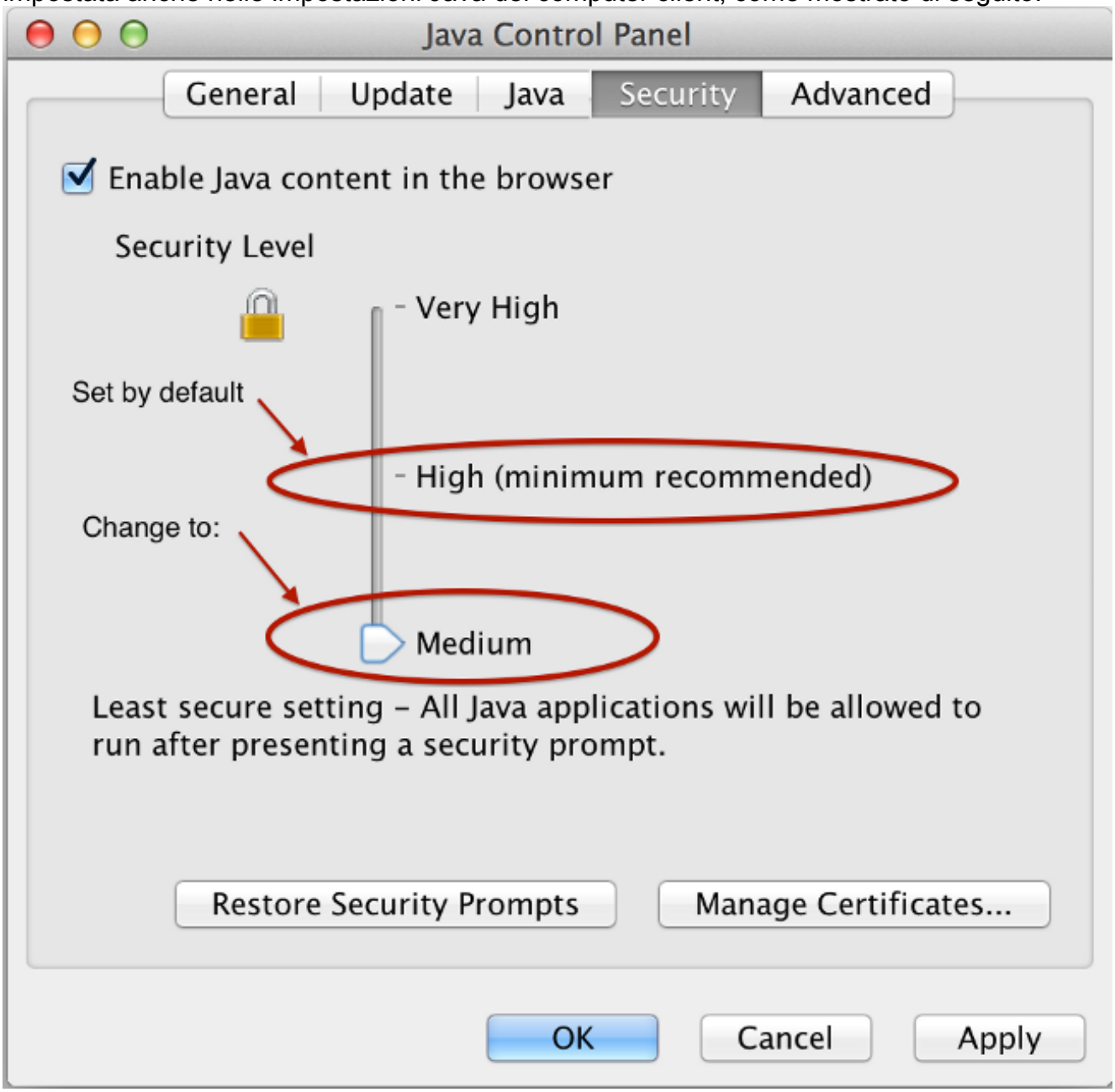
Le modifiche annunciate di recente e pianificate per l'aggiornamento di Java 7 51 (gennaio 2014) hanno stabilito che il dispositivo di scorrimento di sicurezza predefinito richiede firme di codice e l'attributo Manifesto autorizzazioni. In sintesi, tutte le applet Java richiedono:

- da firmare (applet e applicazioni Web Start).
- per impostare l'attributo "Permissions" all'interno del manifesto.

Le applicazioni sono interessate se utilizza Java avviato tramite un browser Web. Le applicazioni vengono eseguite da qualsiasi punto esterno a un browser Web. Ciò significa che per WevVPN potrebbero essere interessati tutti i plug-in client distribuiti da Cisco. Poiché questi plug-in non sono gestiti o supportati da Cisco, Cisco non può apportare modifiche al certificato di firma del codice o all'applet per garantirne la conformità a queste restrizioni. La soluzione adatta a questo problema è l'uso del certificato di firma del codice temporaneo sull'appliance ASA. Le appliance ASA forniscono un certificato di firma del codice temporaneo per firmare le applet Java (per il

rewriter Java e i plug-in). Il certificato temporaneo consente alle applet Java di eseguire le funzioni previste senza visualizzare alcun messaggio di avviso. Prima della scadenza, gli amministratori ASA devono sostituire il certificato temporaneo con il proprio certificato di firma del codice rilasciato da un'autorità di certificazione (CA) attendibile. Se non è possibile utilizzare questa opzione, per risolvere il problema, procedere come segue:

1. Èpossibile utilizzare la funzionalità Elenco siti eccezioni nelle impostazioni Java del computer client finale per eseguire le applicazioni bloccate dalle impostazioni di protezione. I passaggi per farlo sono descritti in Problemi con Safari con WebLaunch su Mac 10.9.
2. Èinoltre possibile ridurre le impostazioni di protezione Java. Questa impostazione viene impostata anche nelle impostazioni Java del computer client, come mostrato di seguito:



Avviso: L'utilizzo di queste soluzioni offre ancora alcuni errori, ma Java non blocca l'applicazione come avrebbe fatto senza le soluzioni implementate.

Windows

Le applicazioni che avviano le applet Java sono state segnalate per il failover su WebVPN dopo un aggiornamento a Java 7. Questo problema è causato dalla mancanza di supporto SHA-256 per il riscrittura Java. per questo problema è stato archiviato l'ID bug Cisco CSCud54080, "SHA-256 support for webvpn Java rewriter".

Le applicazioni che avviano le applet Java tramite il portale con Smart Tunnel potrebbero avere esito negativo quando si utilizza JRE7. questo è il più comune nei sistemi a 64 bit. Nelle clip, la Java VM invia i pacchetti in testo non crittografato, non tramite la connessione Smart Tunnel all'ASA. La questione è stata affrontata con l'ID bug Cisco CSCue17876, "Some java applets will not connect via smart tunnel on windows with jre1.7" (Alcune applet Java non si connetteranno tramite smart tunnel su Windows con jre1.7).