Java 7 Problemen met AnyConnect, CSD/Hostscan en WebVPN - Handleiding voor probleemoplossing

Inhoud

Inleiding

Dit document beschrijft hoe u problemen met uw probleemoplossing kunt oplossen met Java 7 op Cisco AnyConnect Secure Mobility Client, Cisco Secure Desktop (CSD)/Cisco Hostscan en clientloze SSL VPN (WebeVPN).

> Opmerking: Cisco bug-ID's die als onderzoek zijn gemarkeerd, zijn niet beperkt tot de beschreven symptomen. Als u problemen met Java 7 hebt, zorg er dan voor dat u de AnyConnect-clientversie naar de nieuwste clientversie of ten minste de 3.1 versie met onderhoudsrelease 3 die beschikbaar is op Cisco Connection Online (CCO) upgrades uitvoert.

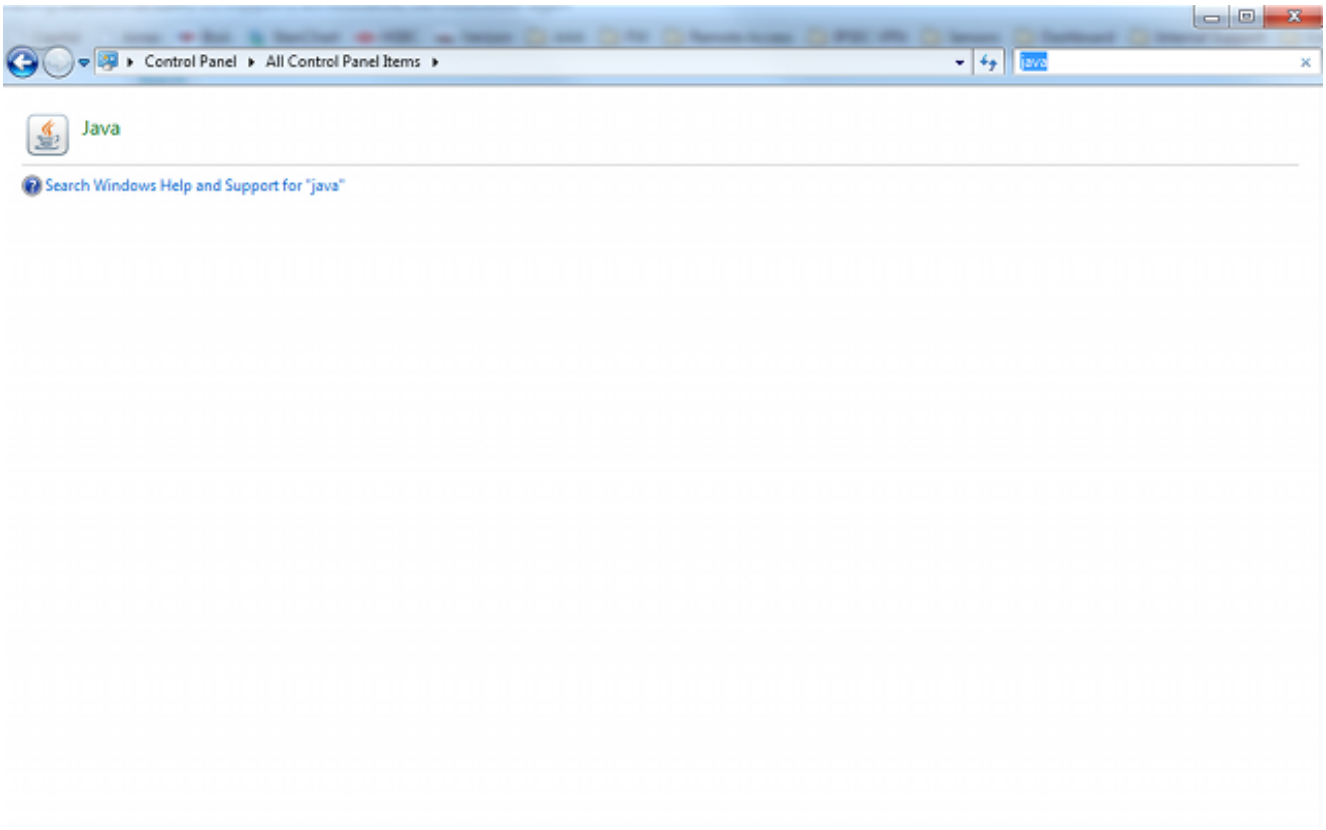
Algemene probleemoplossing

Start de Java-verificateur om te controleren of Java wordt ondersteund op de browsers in gebruik. Als Java goed is ingeschakeld, controleert u de logbestanden van de Java-console om het probleem te analyseren.

Windows

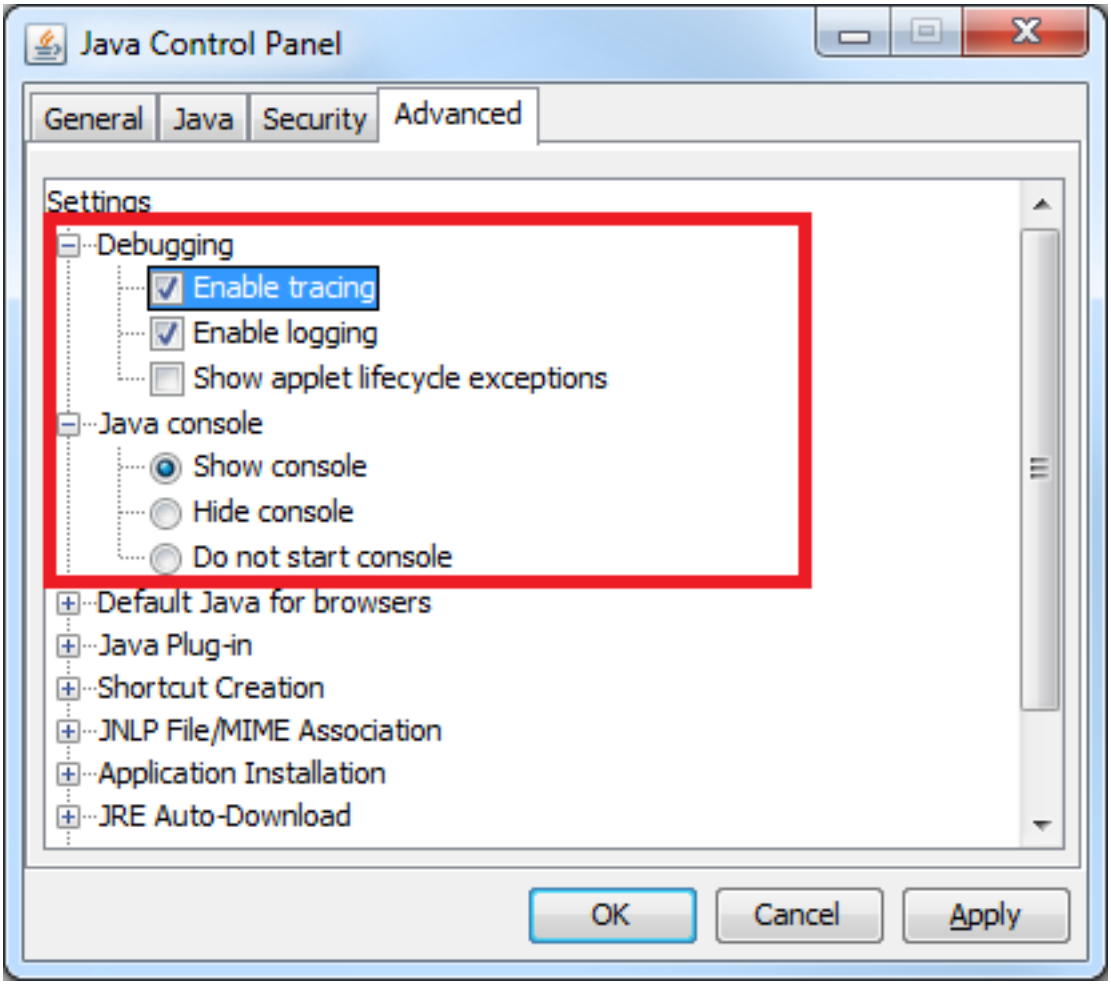
In deze procedure wordt beschreven hoe u de logbestanden van de console in Windows kunt inschakelen:

1. Open het Configuratiescherm van Windows en zoek naar Java.



2. Dubbelklik op **Java** (het pictogram kop koffie). Het Java Control Panel wordt weergegeven.
3. Klik op het tabblad **Geavanceerd**.

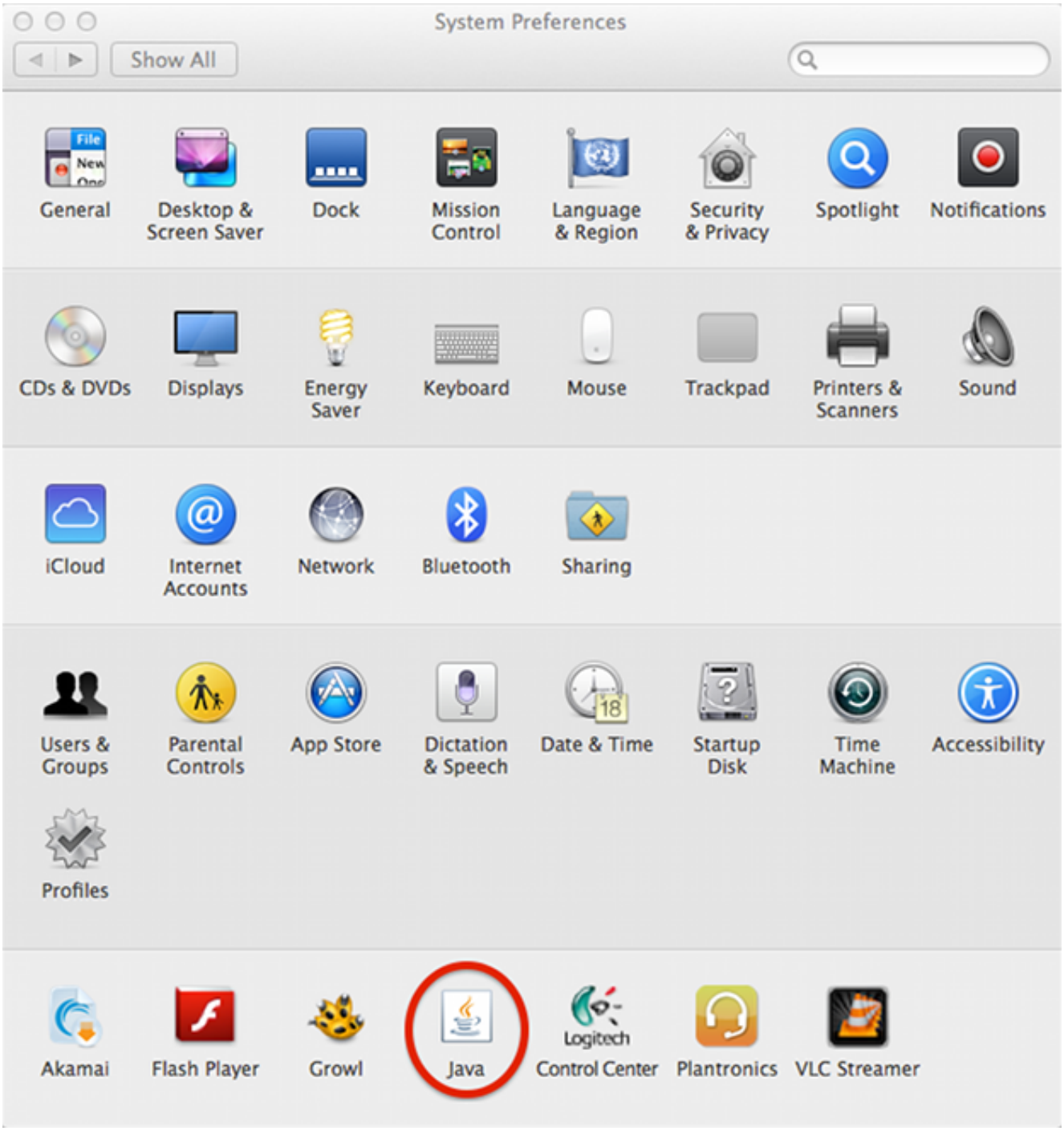
   Uitvouwen **het fouilleren** en selecteren **Overtrekken inschakelen** en **loggen inschakelen**.Vul de **Java-console uit** en klik op **console tonen**.



Mac

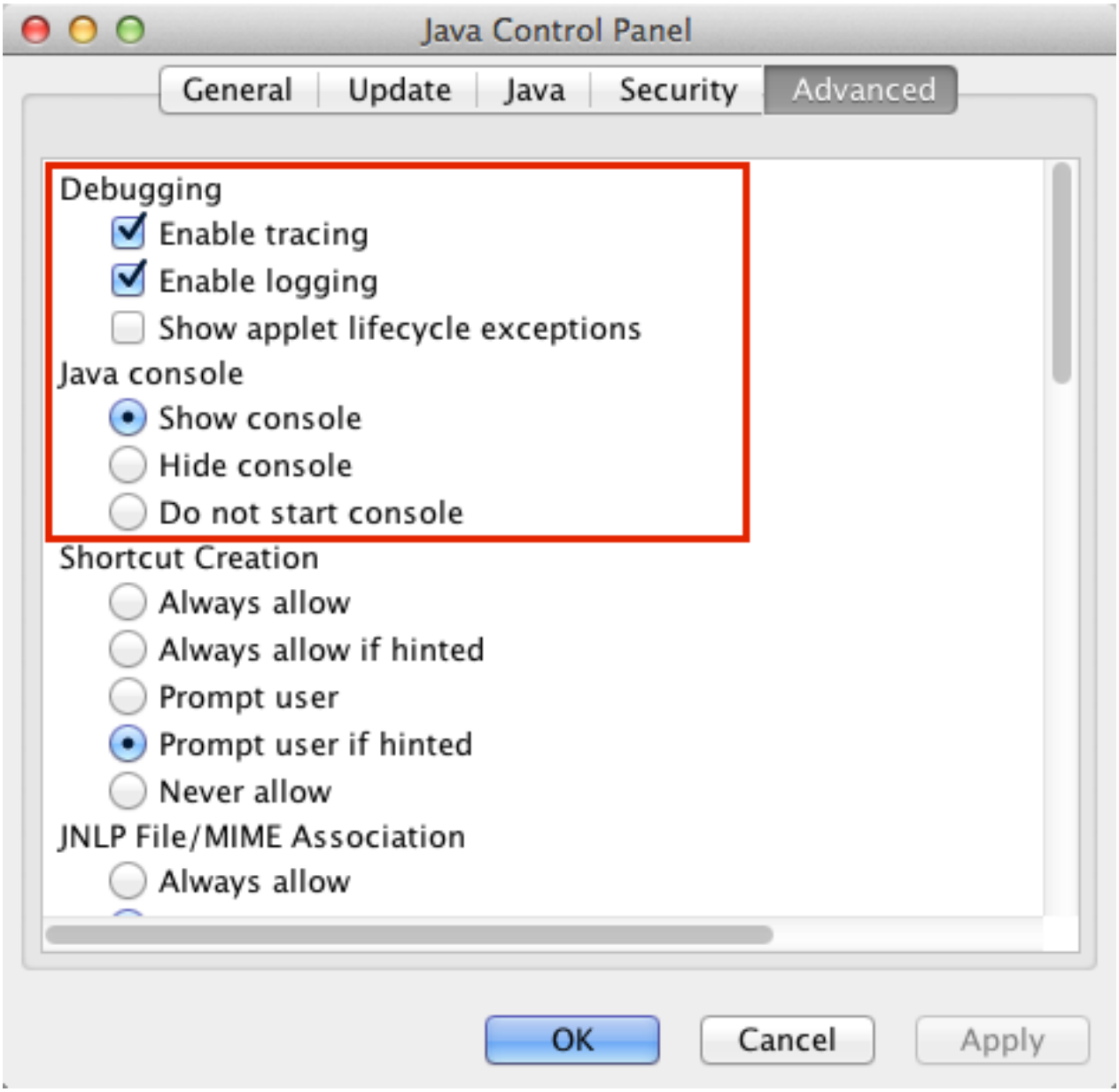
In deze procedure wordt beschreven hoe u de console kunt inschakelen voor een Mac:

1. Open systeemvoorkeuren en dubbelklik op het pictogram Java (koffiekopje). Het Java Control Panel wordt weergegeven.



2. Klik op het tabblad **Geavanceerd**.

   Klik onder Java-console op **console tonen**.Klik onder Debugging, op **Overtrekken inschakelen** en **registreren inschakelen**.



Specifieke probleemoplossing

AnyConnect

Verzamel voor AnyConnect-gerelateerde problemen de DART-logbestanden (Diagnostic AnyConnect Reporting) en de Java-console.

Windows

Cisco bug-ID CSCuc55720, "IE crashes met Java 7 wanneer 3.1.1-pakket in de ASA is ingeschakeld" was een bekend probleem, toen Internet Explorer crashte toen er een Webex-lancering werd uitgevoerd en AnyConnect 3.1 op het head-end werd geactiveerd. Dit insect is gerepareerd.

U kunt problemen krijgen wanneer u bepaalde versies van AnyConnect en Java 7 met Java gebruikt. Voor meer informatie, zie Cisco bug-ID CSCue48916, "Java-app(s) Break bij gebruik van AnyConnect 3.1.00495 of 3.1.2026 en Java v7."

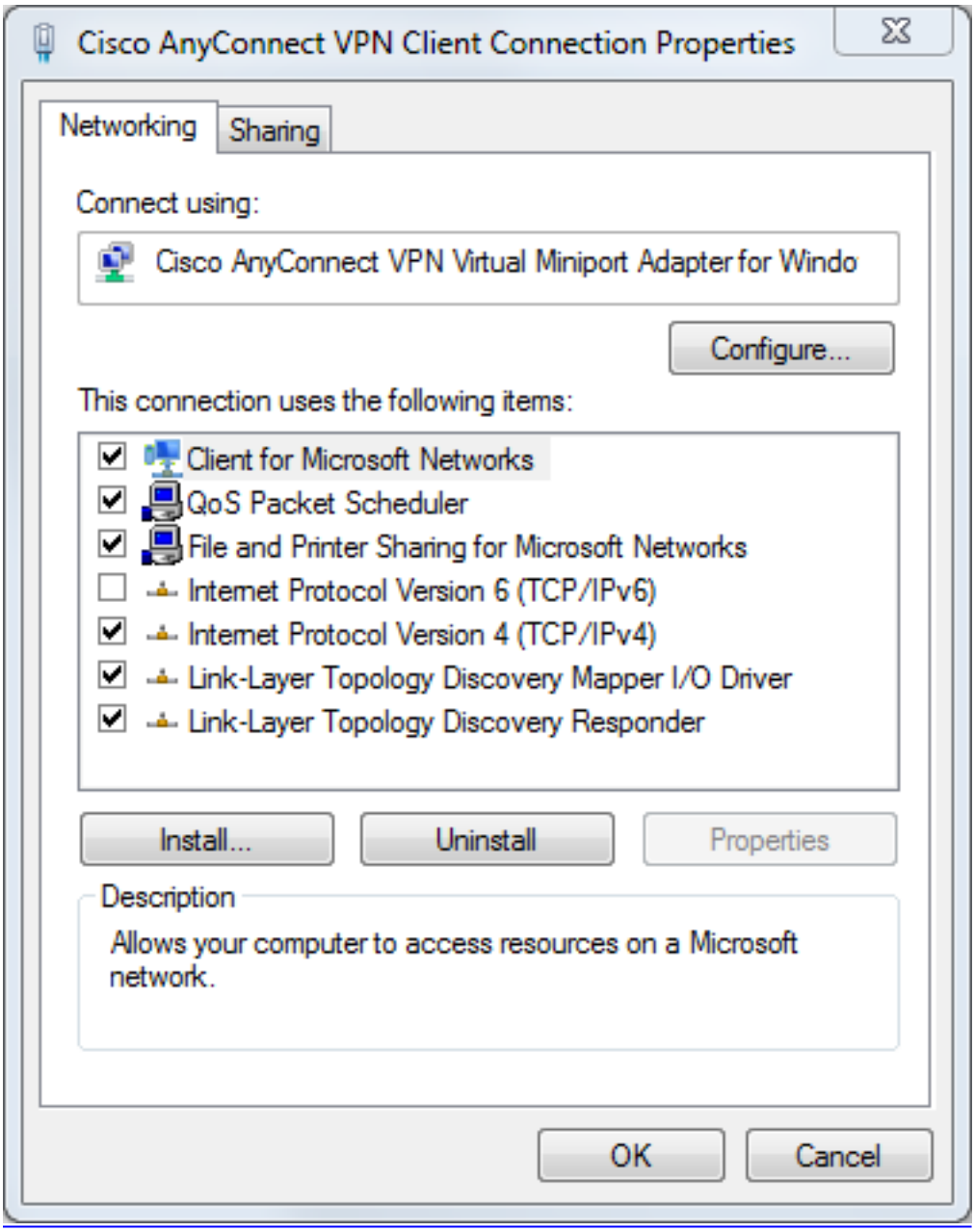
Problemen met Java 7 en IPv6 Socket-oproepen

Als AnyConnect geen verbinding maakt, zelfs nadat u de Java Runtime Environment (JRE) hebt geüpload naar Java 7, of als een Java-toepassing niet via de VPN-tunnel kan verbinden, kunt u de Java-console opnieuw bekijken en deze berichten bekijken:

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

Deze logitems geven aan dat de client/toepassing IPv6-oproepen doet.

Eén oplossing voor dit probleem is IPv6 uit te schakelen (als dit niet in gebruik is) op de Ethernet-adapter en de AnyConnect Virtual Adapter (VA):



Een tweede oplossing is om Java te configureren dat IPv4 liever IPv4 dan IPv6 geeft. Stel de systeemeigenschap 'java.net.preferIPv4Stack' in op 'waar' zoals in deze voorbeelden wordt getoond:

- Voeg code voor het systeembezit aan de code van Java toe (voor Java toepassingen die door de klant worden geschreven):

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

- Voeg code voor de systeemeigenschap van de opdrachtregel toe:

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

- Stel de omgevingsvariabelen _JPI_VM_OPTIONS en_JAVA_OPTIONS in om de systeemeigenschap op te nemen:

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

Zie voor meer informatie:

- Hoe stelt u java.net.preferIPv4Stack=waar in de javcode in?
- Hoe wordt java gedwongen om ipv4 te gebruiken in plaats daarvan ipv6?

Een derde oplossing is IPv6 volledig uit te schakelen op Windows-machines; de registratie bewerken:

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

Zie Hoe u IP, versie 6 of de specifieke onderdelen ervan in Windows kunt uitschakelen voor meer informatie.

Problemen met AnyConnect Webech na upgrade met Java 7

Cisco JavaScript-code heeft Sun eerder als waarde voor de Java-verkoper gezocht. Oracle veranderde echter die waarde zoals beschreven in JDK7: Java verandert de eigenschap. Dit probleem is opgelost door Cisco bug-ID CSCub46241: "AnyConnect-weblancering mislukt vanuit Internet Explorer met Java 7."

Mac

Er zijn geen problemen gemeld. De testen met AnyConnect 3.1 (met de configuratie van Webex / Safari/Mac 10.7.4 / Java 7.10) laten geen fouten zien.

Diversen

Problemen met Java 7 Apps op Cisco AnyConnect

Cisco bug-ID CSCue48916, "Java-app(s) voor Breking bij gebruik van AnyConnect 3.1.00495 of 3.1.2026 en Java v7" is geactiveerd. Aanvankelijk onderzoek wijst uit dat de problemen geen bug aan de kant van de klant zijn, maar in plaats daarvan verband kunnen houden met de configuratie van de virtuele machine (VM) van Java.

Eerder, om Java 7-apps te kunnen gebruiken op de AnyConnect 3.1(2026) client, heeft u de instellingen van de IPv6 virtuele adapter niet ingeschakeld. Het is nu echter noodzakelijk alle stappen in deze procedure te voltooien:

1. Installeer AnyConnect versie 3.1(2026).
2. Installeer Java 7.
3. Herstart.
4. Installeer Java SE 6, update 38, beschikbaar op de Oracle-website.
5. Navigeer naar de instellingen van het bedieningspaneel van Java 6 en klik vervolgens op het tabblad **Update** om de nieuwste versie van Java 7 te verbeteren.
6. Open een opdrachtmelding en voer in:

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

7. Log in met AnyConnect en Java moet werken.

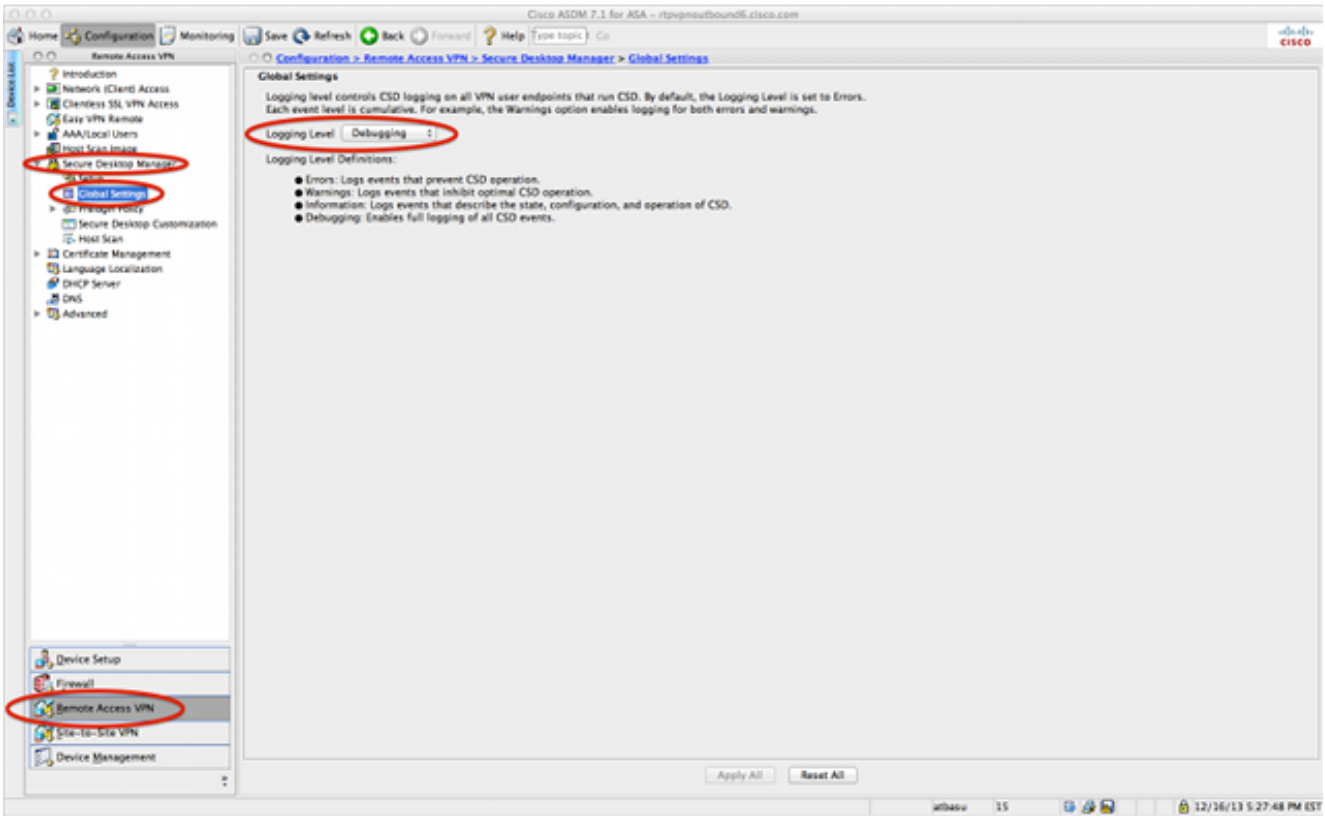
Opmerking: Deze procedure is getest met Java 7 updates 9, 10 en 11.

CSD/Hostscan

Voor CSD/Hostscan-gerelateerde problemen verzamelt u de DART-logbestanden evenals de Java-console-logbestanden.

Om de DART-documenten te verkrijgen, moet het CSD-logingniveau worden gericht op het fouilleren van de ASA:

1. Navigeer naar **ASDM > Configuration > Remote Access VPN > Secure Desktop Manager > Global Settings.**
2. Zet CSD-loggen op om te fouilleren op de Cisco Adaptieve Security Devices Manager (ASDM).
3. Gebruik DART om de CSD/Hostscan-logbestanden te verzamelen.



Windows

Een Hostscan is vergelijkbaar met de crashes die eerder voor AnyConnect in Windows zijn beschreven (Cisco bug-ID CSCuc5720). Het hostscanprobleem is opgelost door Cisco bug-ID CSCuc48299, "IE met Java 7 crashes op HostScan Weblunch".

Mac

Emissies met CSD versies 3.5.x en Java 7

In CSD 3.5.x gaan alle WebeVPN-verbindingen niet door; Dit omvat AnyConnect-weblanceringen. De logbestanden van Java onthullen geen problemen:

```
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>
----------------------------------------------------
```

Als u teruggraaft naar JRE 6 of CSD-upgrade naar 3.6.6020 of hoger, dan worden de problemen met de Java-console duidelijk:

```
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.
```

De oplossing is om Java te moderniseren of af te bouwen. Omdat Cisco u aanraadt de nieuwste versie van CSD te starten, moet u een upgrade van CSD uitvoeren in plaats van een lagere kwaliteit van Java, vooral omdat een Java-disfunctie moeilijk op een Mac kan zijn.

Problemen met Chrome en Safari met Webex in Mac 10.8

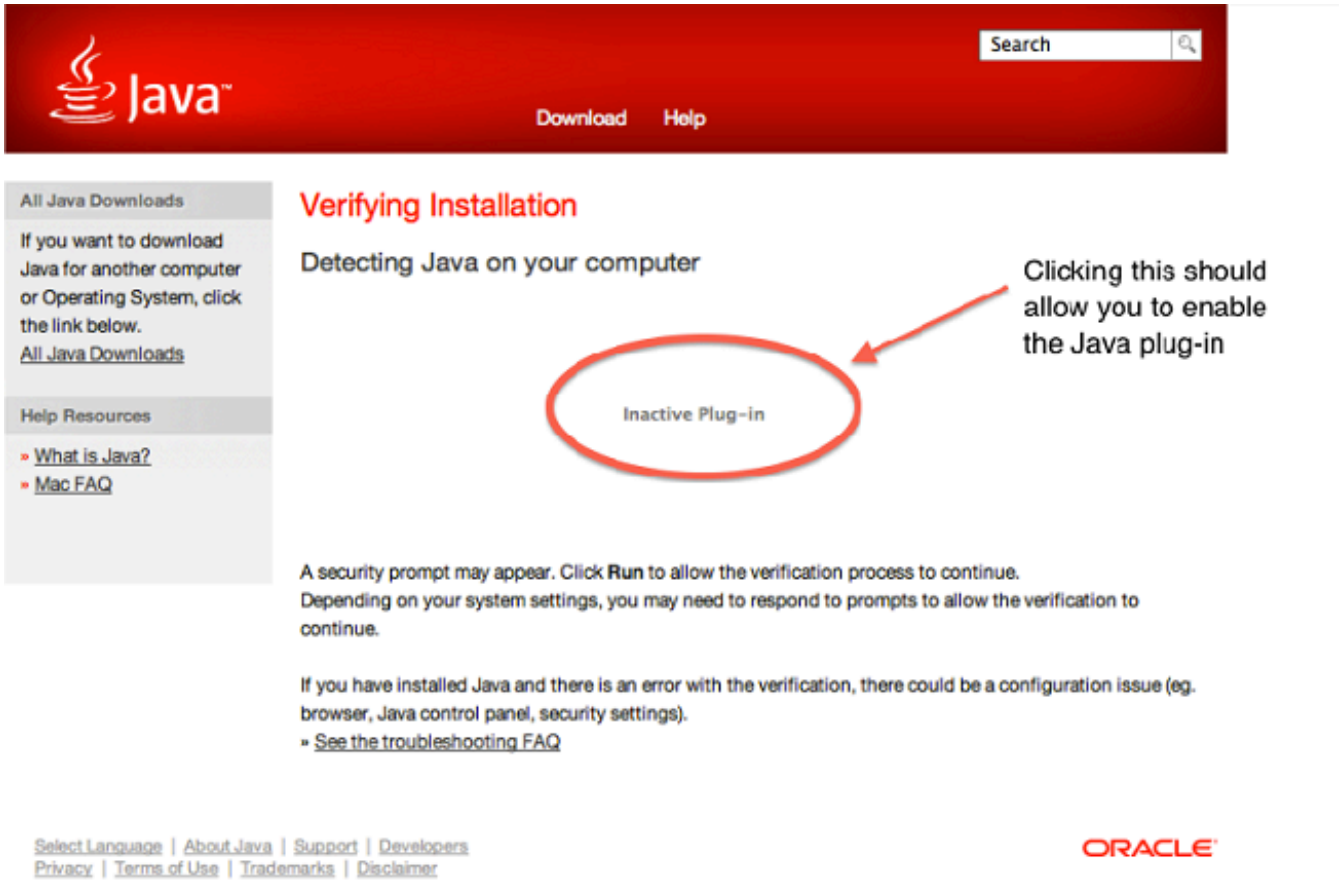
Verschillen met Chrome en Safari worden verwacht:

- Chrome is een browser met 32 bits en ondersteunt Java 7 niet.
- Chrome is nooit een officieel ondersteunde browser voor Webex.
- Mac 10.8 uitgeschakeld het gebruik van Java 7 op Safari, en oudere versies van Java worden standaard niet ingeschakeld.

Als u Java 7 al hebt geïnstalleerd, worden de resoluties:

- Gebruik Firefox.
- Java 7 inschakelen voor Safari:

  Controleer dat Java 7 op de Mac is geïnstalleerd en dat de Mac opnieuw is gestart. Open Firefox en ga naar de Java Verifier.Open Safari en ga opnieuw naar Java Verkenner. U dient dit scherm nu te bekijken:



- Schakel Java 7 uit en schakelt Java 6 in dat door Apple wordt geleverd.

  Tip: Als Java niet is geïnstalleerd of als u een oudere versie van Java hebt, ziet u waarschijnlijk de foutmelding 'Java geblokkeerd voor deze website' op java.com. Zie Java-updates beschikbaar voor OS X op 28 augustus 2013 op het Apple-ondersteuningsforum voor informatie over de installatie van Java-updates.

Problemen met Safari met Webex op Mac 10.9

Als u op Mac 10.9 bent en u al de Java plug-in hebt ingeschakeld (zoals wordt beschreven in de sectie Problemen met Chrome en Safari met Webex 10.8), zal Webex mogelijk falen. Alle Java-applets worden gestart, maar de browser blijft gewoon draaien. Als Java-logbestanden zijn ingeschakeld zoals in het gedeelte Algemene probleemoplossing wordt beschreven, worden de logbestanden snel ingevuld zoals hier wordt weergegeven:

```
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
```

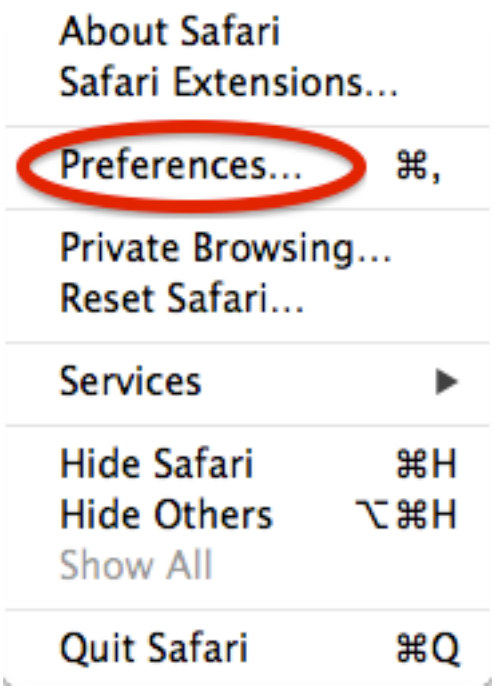
```
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45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

Bekijk dit type vermelding eerder in het logbestand:

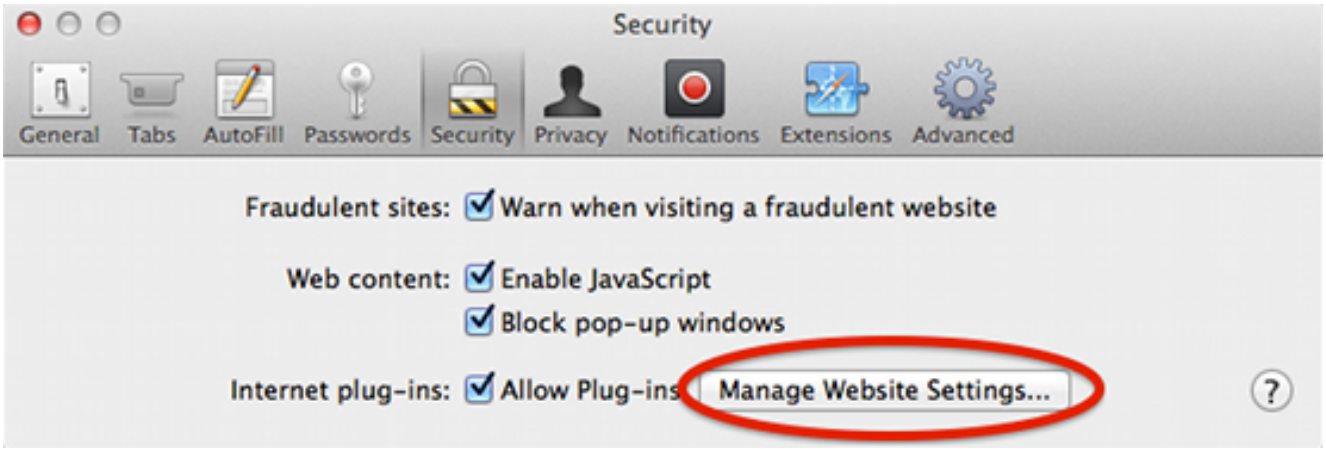
```
Mon Dec 16 16:00:17 EST 2013 Downloaded https://rave.na.sage.com/CACHE/
sdesktop/hostscan/darwin_i386/manifest java.io.FileNotFoundException:
/Users/user1/.cisco/hostscan/bin/cstub (Operation not permitted) at
java.io.FileInputStream.open(Native Method)
```

Dit geeft aan dat u bij Cisco bug-ID CSCuj02425 tegenkomt, dat "Webex10.9 niet werkt als de onveilige modus van java is uitgeschakeld." Wijzig de instellingen van Java om dit probleem aan te pakken zodat Java in een onveilige modus voor Safari kan lopen:

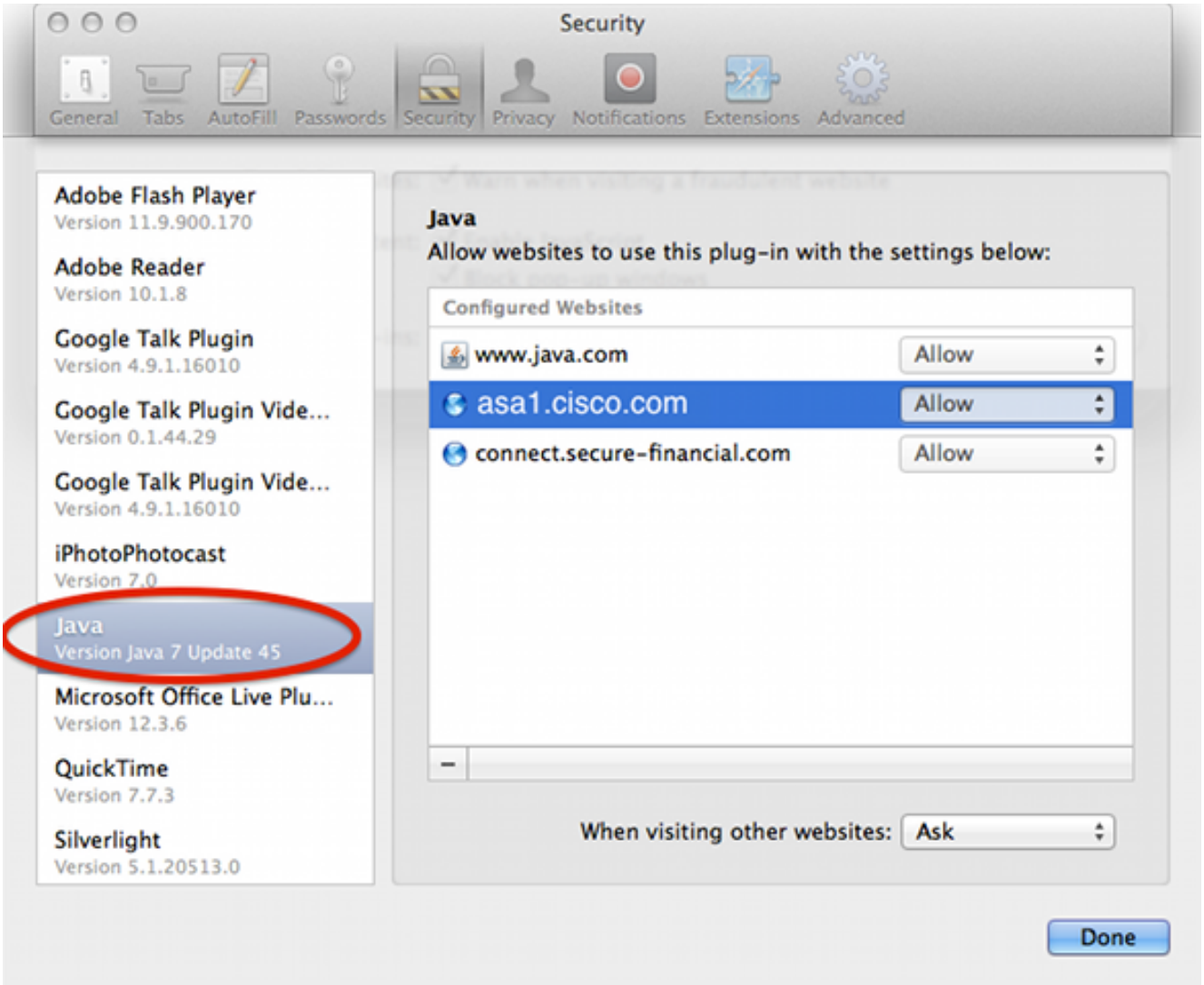
1. Klik op **Voorkeuren**.



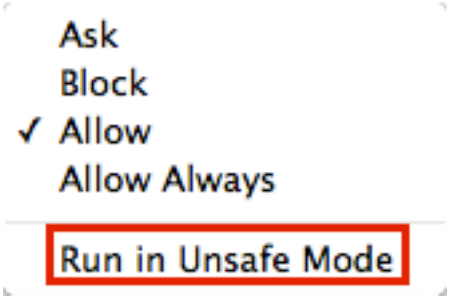
2. Klik op **Website beheren**.



3. Selecteer in het tabblad **Beveiliging Java** en let er op dat **Sta** standaard **toe**.



4. Verander **toestaan** om **in onveilige modus** te **lopen**.



WebVPN

Voor WebVPN-problemen met betrekking tot Java verzamelt u deze gegevens voor probleemoplossing:

- Uitvoer van de **show tech-support** opdracht.
- Java-console logt met en zonder adaptieve security applicatie (ASA) zoals uitgelegd in het gedeelte Algemene probleemoplossing.
- WebVPN opneemt.
- HTTP watch neemt lokale machines op met en zonder de ASA.
- Standaardpakketjes nemen op de ASA en de lokale machine op. Op de lokale machine kunnen deze beelden worden gemaakt met Wireshark.Zie Packet Captures configureren voor informatie over het opnemen van verkeer op de ASA.
- Alle bestanden van de pot zijn gedownload naar de Java cache wanneer ze door de ASA gaan. Dit is een voorbeeld uit de Java-console:

```
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 dit voorbeeld is 6a0665e9-1f510559.idx de gecached versie van mffta.jar 7. Als je geen toegang hebt tot deze bestanden, kan je ze van de Java cache verzamelen wanneer je directe verbinding gebruikt.

Een testinstelling kan de resolutie bespoedigen.

Beveiligingsfuncties in Java 751 en hoe dit gebruikers van WebVPN beïnvloedt

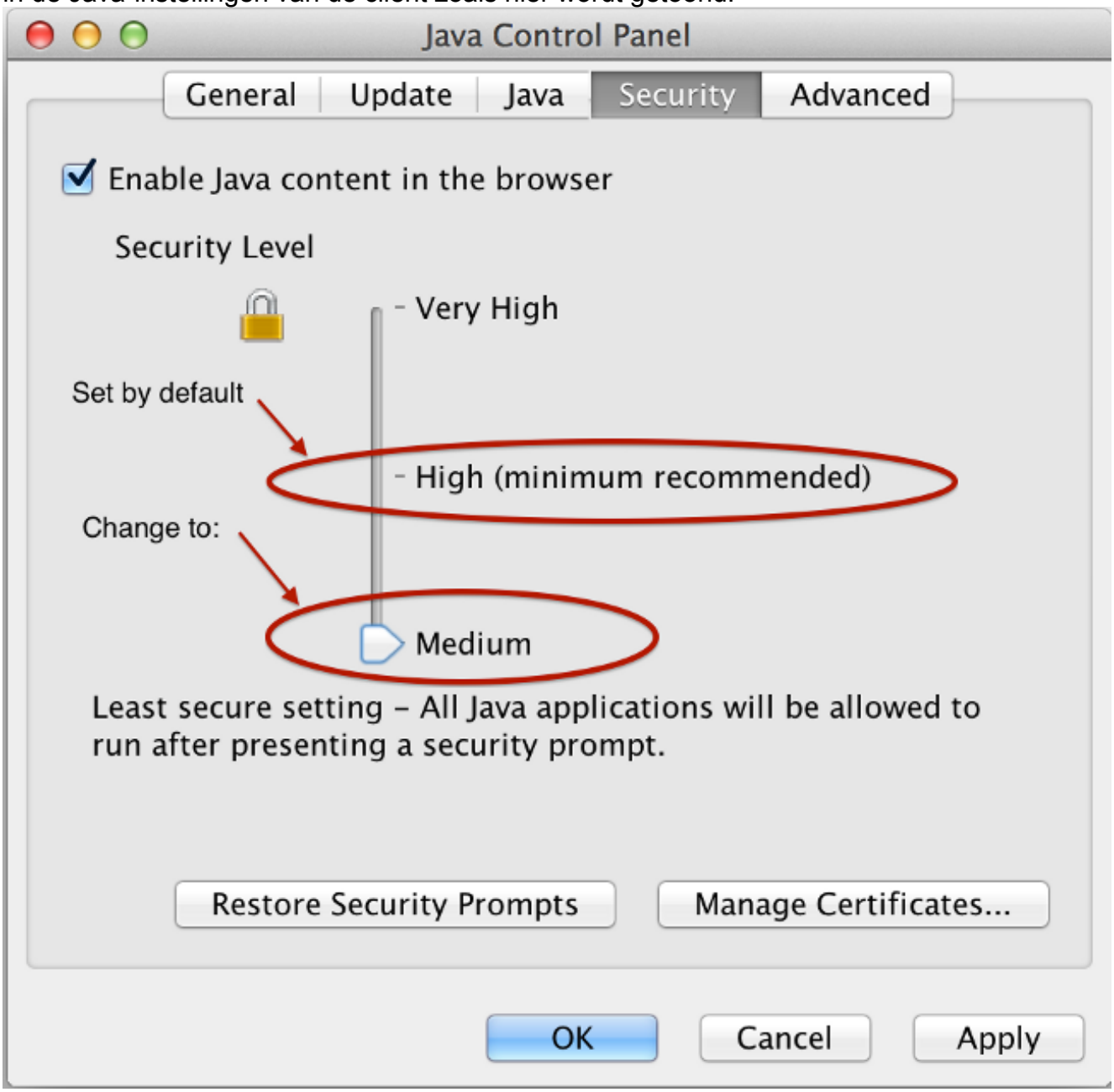
Onlangs aangekondigde veranderingen die voor Java 7 update 51 (januari 2014) zijn gepland, hebben aangetoond dat de standaard beveiligingsschuifschakelaar codehandtekeningen en de eigenschap Permissions Manifest vereist. Samengevat, alle Java-applets vereisen:

- te ondertekenen (applicaties en toepassingen voor het starten van het web).
- om de eigenschap "toegangsrechten" in het manifest in te stellen.

De toepassingen worden beïnvloed als Java wordt gebruikt dat via een webbrowser is gestart. Toepassingen kunnen worden uitgevoerd vanuit alle gebieden waar een webbrowser niet geschikt is. Wat dit voor WevVPN betekent, zijn alle client plug-ins die door Cisco zijn gedistribueerd. Aangezien deze stekkers niet worden onderhouden of ondersteund door Cisco, kan Cisco geen wijzigingen aanbrengen in het codeponeringscertificaat of in de applicatie om er zeker van te zijn dat deze aan deze beperkingen voldoet. De juiste oplossing voor dit is het gebruik van het tijdelijk

code gebarende certificaat op de ASA. ASA's voorzien in een tijdelijk code gebarend certificaat om Java applets te ondertekenen (voor Java rewriter en plug-ins). Met het tijdelijke certificaat kan Java-applicaties hun functies zonder waarschuwingsbericht uitvoeren. ASA-beheerders dienen het tijdelijke certificaat te vervangen voordat het verstrijkt door hun eigen code-gebarentekencertificaat, afgegeven door een vertrouwde certificeringsinstantie (CA). Als dit geen haalbare optie is, moet het werkterrein zijn om deze stappen te voltooien:

1. U kunt de optie Exception Site list gebruiken in de Java-instellingen van de eindclient om de toepassingen te kunnen uitvoeren die geblokkeerd worden door beveiligingsinstellingen. De stappen hiervoor worden beschreven in Issues with Safari met Webex op Mac 10.9.
2. U kunt ook de instellingen voor Java-beveiliging verlagen. Deze instelling wordt ook ingesteld in de Java-instellingen van de client zoals hier wordt getoond:



Waarschuwing: Het gebruik van deze tijdelijke vaste verbindingen geeft u nog steeds een aantal fouten, maar Java blokkeert de toepassing niet omdat deze niet met de beschikbare werkronden kan worden afgesloten.

Windows

Toepassingen die Java starten, zijn gemeld dat ze via WebVPN mislukt na een upgrade naar Java 7. Dit probleem wordt veroorzaakt door het gebrek aan SHA (Secure Hash Algorithm)-256-ondersteuning voor Java-herschrijver. Cisco bug-ID CSCud54080, "SHA-256 ondersteuning voor webVPN-Java-rewriter", is voor dit probleem gedeponeerd.

Toepassingen die Java-applets starten door het portaal met Smart Tunnel kunnen mislukken wanneer JRE7 wordt gebruikt; dit komt het meest voor bij 64-bits systemen. Houd er rekening mee dat Java VM de pakketten in duidelijke tekst verstuurt en niet via de Smart Tunnel-verbinding naar de ASA. Dit is aangepakt door Cisco bug ID CSCue17876, "Sommige javetjes zullen niet via een slimme tunnel op vensters met jre1.7 verbonden zijn."