Java 7-Probleme mit AnyConnect, CSD/Hostscan und WebVPN - Leitfaden zur Fehlerbehebung

Inhalt

[Einführung](#)
[Allgemeine Fehlerbehebung](#)
[Windows](#)
[Mac](#)
[Spezifische Fehlerbehebung](#)
[AnyConnect](#)
[Windows](#)
[Mac](#)
[Verschiedenes](#)
[CSD/Hostscan](#)
[Windows](#)
[Mac](#)
[WebVPN](#)
[Sicherheitsfunktionen in Java 7 U51 und Auswirkungen auf WebVPN-Benutzer](#)
[Windows](#)

Einführung

Dieses Dokument beschreibt, wie Sie Probleme mit Java 7 auf dem Cisco AnyConnect Secure Mobility Client, dem Cisco Secure Desktop (CSD)/Cisco Hostscan und dem clientlosen SSL VPN (WebVPN) beheben können.

> **Hinweis**: Cisco Bug-IDs, die als untersuchend gekennzeichnet sind, sind nicht auf die beschriebenen Symptome beschränkt. Wenn bei Java 7 Probleme auftreten, stellen Sie sicher, dass Sie die AnyConnect Client-Version auf die neueste Client-Version oder auf die 3.1-Wartungsversion 3 aktualisieren, die auf Cisco Connection Online (CCO) verfügbar ist.

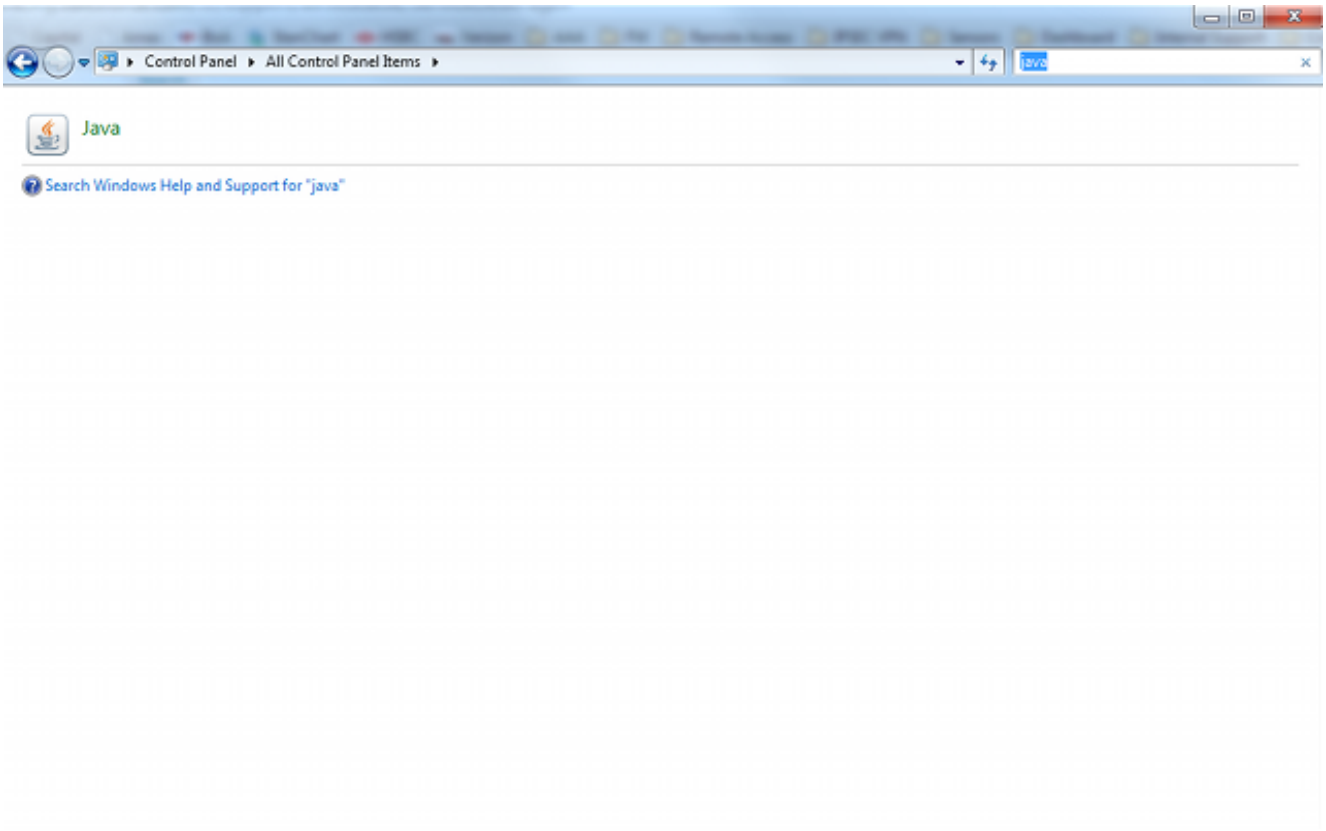
Allgemeine Fehlerbehebung

Führen Sie den Java Verifier aus, um zu überprüfen, ob Java in den verwendeten Browsern unterstützt wird. Wenn Java ordnungsgemäß aktiviert ist, überprüfen Sie die Java-Konsolenprotokolle, um das Problem zu analysieren.

Windows

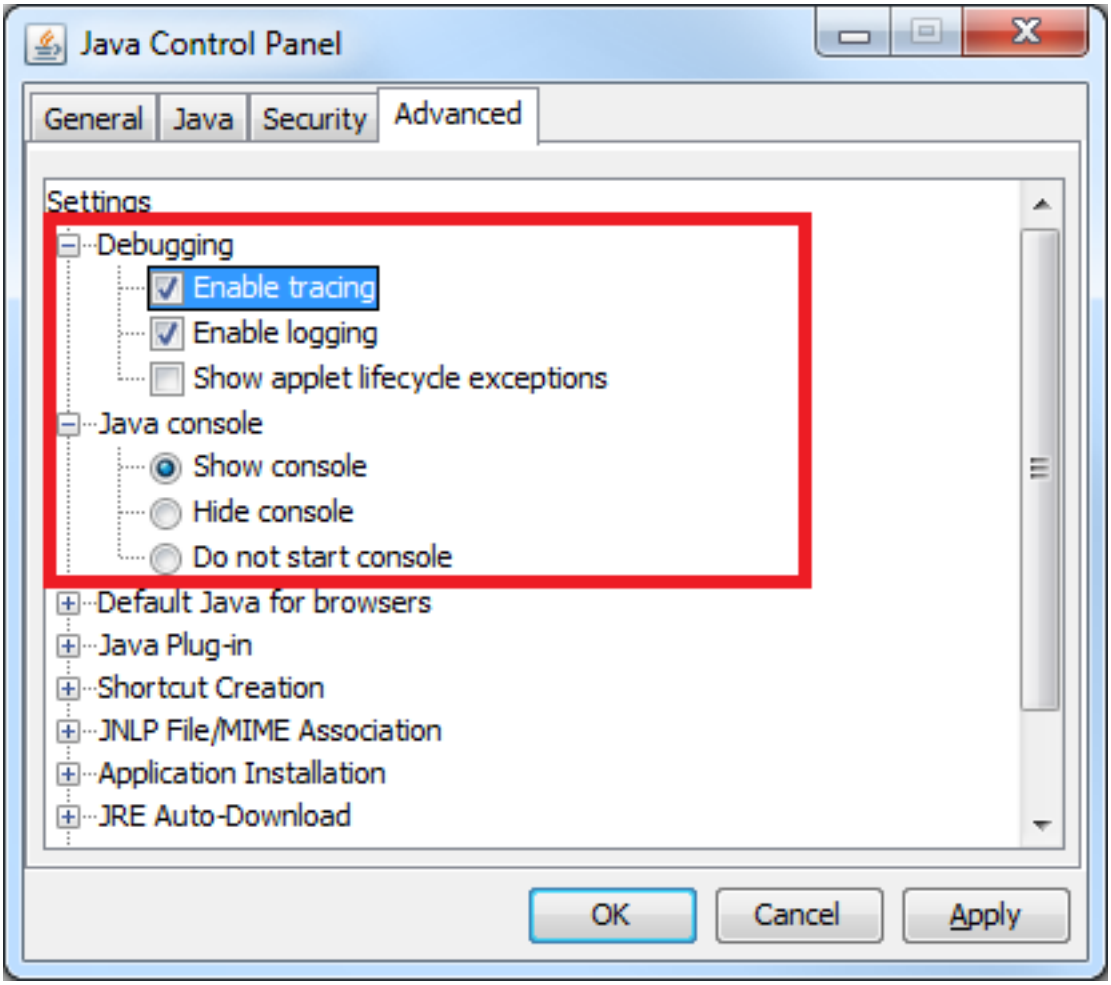
In diesem Verfahren wird beschrieben, wie die Konsolenprotokolle in Windows aktiviert werden:

1. Öffnen Sie die Windows-Systemsteuerung, und suchen Sie nach Java.



2. Doppelklicken Sie auf **Java** (das Kaffeetasse-Symbol). Das Java-Bedienungsfeld wird angezeigt.
3. Klicken Sie auf die Registerkarte **Erweitert**.

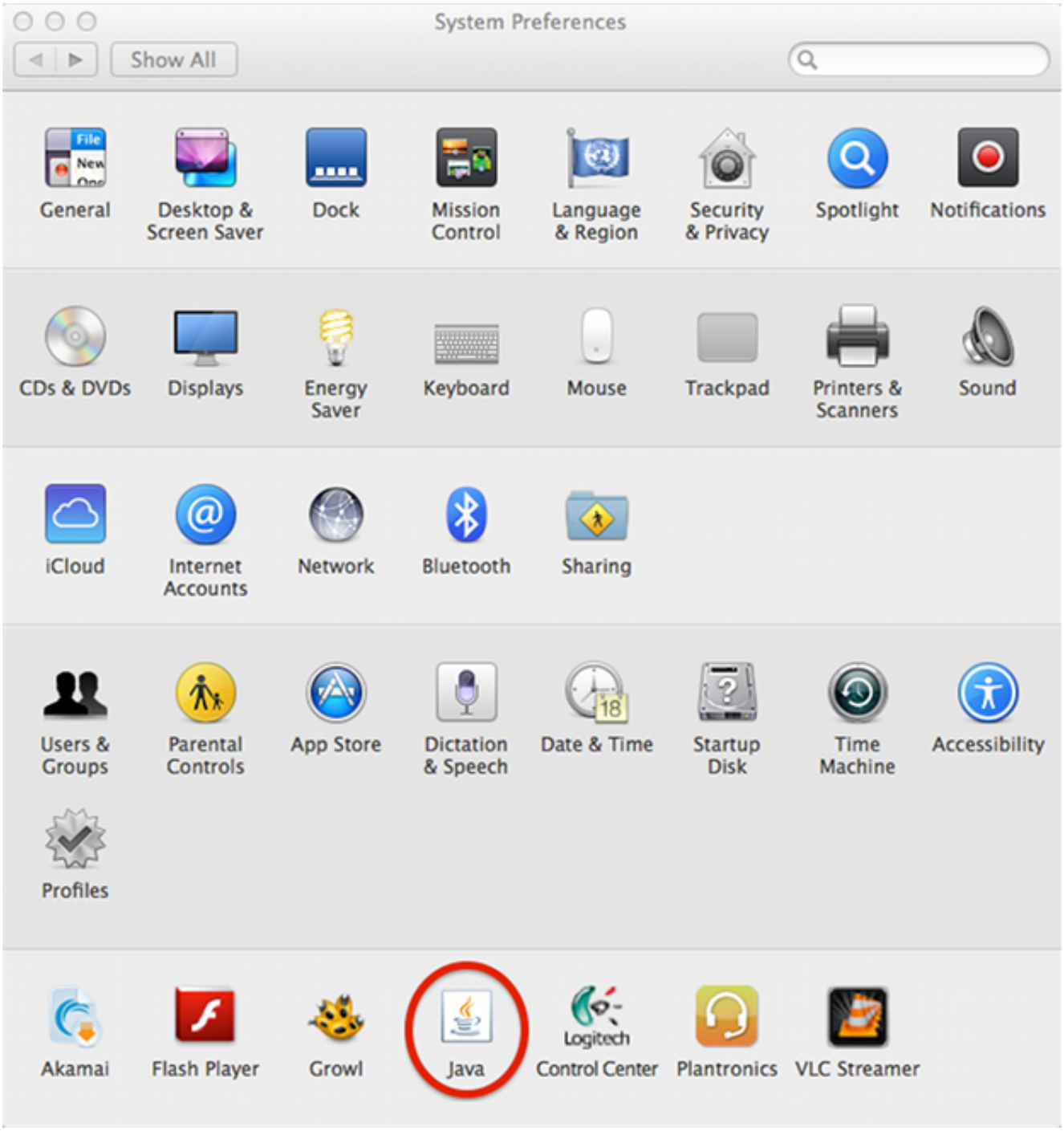
   Erweitern Sie **Debuggen**, und wählen Sie **Ablaufverfolgung aktivieren** und **Protokollierung aktivieren aus**.Erweitern Sie die **Java-Konsole**, und klicken Sie auf **Konsole anzeigen**.



Mac

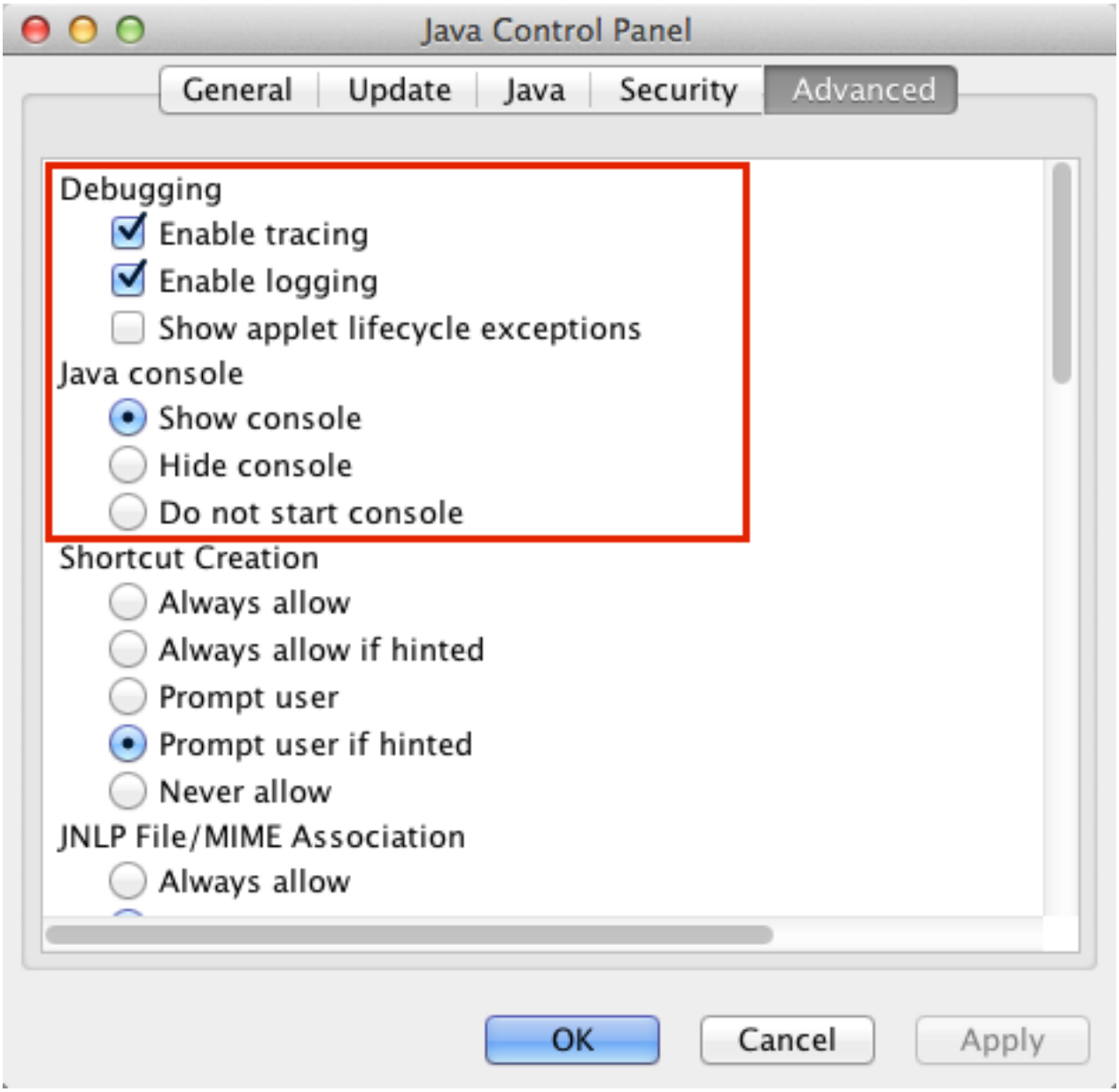
Dieses Verfahren beschreibt, wie die Konsolenprotokolle auf einem Mac aktiviert werden:

1. Öffnen Sie die Systemeinstellungen, und doppelklicken Sie auf das Java-Symbol (Kaffeetasse). Das Java-Bedienungsfeld wird angezeigt.



2. Klicken Sie auf die Registerkarte **Erweitert**.

   Klicken Sie unter "Java-Konsole" auf **Konsole anzeigen**.Klicken Sie unter Debuggen auf **Ablaufverfolgung aktivieren** und **Protokollierung aktivieren**.



Spezifische Fehlerbehebung

AnyConnect

Bei Problemen im Zusammenhang mit AnyConnect sollten Sie die Diagnostic AnyConnect Reporting (DART)-Protokolle sowie die Java-Konsolenprotokolle sammeln.

Windows

Die Cisco Bug-ID CSCuc55720, "IE stürzt mit Java 7 ab, wenn 3.1.1-Paket auf der ASA aktiviert ist", war ein bekanntes Problem, bei dem Internet Explorer abstürzte, als ein WebLaunch durchgeführt wurde und AnyConnect 3.1 am Headend aktiviert wurde. Dieser Fehler wurde behoben.

Wenn Sie einige Versionen von AnyConnect und Java 7 mit Java-Anwendungen verwenden, können Probleme auftreten. Weitere Informationen finden Sie unter Cisco Bug ID CSCue48916, "Java App Break when using AnyConnect 3.1.00495 or 3.1.02026 & Java v7".

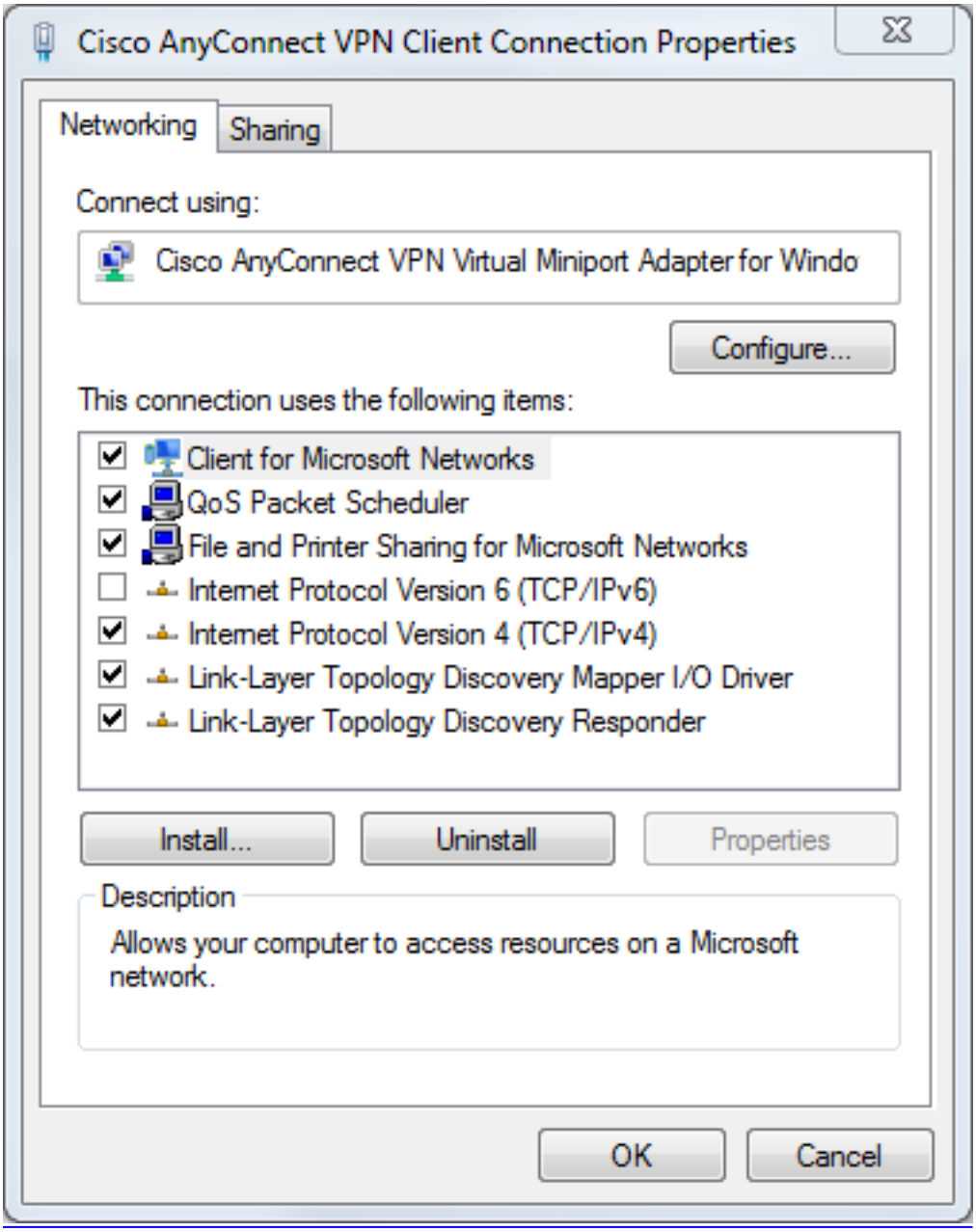
Probleme mit Java 7- und IPv6-Socket-Anrufen

Wenn AnyConnect auch nach dem Upgrade der Java Runtime Environment (JRE) auf Java 7 keine Verbindung herstellt oder eine Java-Anwendung keine Verbindung über den VPN-Tunnel herstellen kann, überprüfen Sie die Java-Konsolenprotokolle, und suchen Sie nach folgenden Meldungen:

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

Diese Protokolleinträge weisen darauf hin, dass der Client/die Anwendung IPv6-Anrufe durchführt.

Eine Lösung für dieses Problem ist die Deaktivierung von IPv6 (wenn IPv6 nicht verwendet wird) auf dem Ethernet-Adapter und dem AnyConnect Virtual Adapter (VA):



Eine zweite Lösung besteht darin, Java so zu konfigurieren, dass IPv4 gegenüber IPv6 bevorzugt wird. Legen Sie die Systemeigenschaft "java.net.preferIPv4Stack" auf "true" fest, wie in den

folgenden Beispielen gezeigt:

- Fügen Sie dem Java-Code Code für die Systemeigenschaft hinzu (für vom Kunden geschriebene Java-Anwendungen):

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

- Fügen Sie in der Befehlszeile Code für die Systemeigenschaft hinzu:

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

- Legen Sie die Umgebungsvariablen _JPI_VM_OPTIONS und _JAVA_OPTIONS fest, um die Systemeigenschaft einzuschließen:

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

Weitere Informationen finden Sie unter:

- Wie wird java.net.preferIPv4Stack=true im Java-Code festgelegt?
- Wie zwingt Java, ipv4 anstelle von ipv6 zu verwenden?

Eine dritte Lösung ist die vollständige Deaktivierung von IPv6 auf Windows-Computern. Diesen Registrierungseintrag bearbeiten:

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

Weitere Informationen finden Sie unter Deaktivieren von IP-Version 6 oder bestimmten Komponenten in Windows.

Probleme mit dem AnyConnect WebLaunch nach dem Java 7-Upgrade

Cisco JavaScript-Code hatte zuvor Sun als Wert für den Java-Anbieter gesucht. Oracle hat diesen Wert jedoch wie in JDK7 beschrieben geändert: Änderungen am Eigentum von Java-Anbietern. Dieses Problem wurde durch die Cisco Bug-ID CSCub46241 "AnyConnect Weblaunch schlägt mit Java 7 im Internet Explorer fehl" behoben.

Mac

Es wurden keine Probleme gemeldet. Tests mit AnyConnect 3.1 (mit der Konfiguration WebLaunch / Safari / Mac 10.7.4 / Java 7.10) zeigen keine Fehler.

Verschiedenes

Probleme mit Java 7-Apps auf Cisco AnyConnect

Die Cisco Bug-ID CSCue48916, "Java App(s) Break when using AnyConnect 3.1.00495 or 3.1.02026 & Java v7" wurde abgelegt. Die erste Untersuchung weist darauf hin, dass es sich bei

den Problemen nicht um einen Fehler auf Client-Seite handelt, sondern vielmehr um die Konfiguration der virtuellen Java-Maschine (VM).

Bisher haben Sie für die Verwendung von Java 7-Anwendungen auf dem AnyConnect 3.1(2026)-Client die Einstellungen für den virtuellen IPv6-Adapter deaktiviert. Nun müssen jedoch alle Schritte in diesem Verfahren abgeschlossen werden:

1. Installieren Sie AnyConnect Version 3.1(2026).
2. Deinstallieren Sie Java 7.
3. Neustart.
4. Installieren Sie Java SE 6, Update 38, verfügbar auf der Oracle-Website.
5. Navigieren Sie zu den Einstellungen des Java 6-Bedienfelds, und klicken Sie dann auf die Registerkarte **Update**, um ein Upgrade auf die neueste Version von Java 7 durchzuführen.
6. Öffnen Sie eine Eingabeaufforderung, und geben Sie Folgendes ein:

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

7. Melden Sie sich bei AnyConnect an, und die Java-Anwendungen sollten funktionieren.

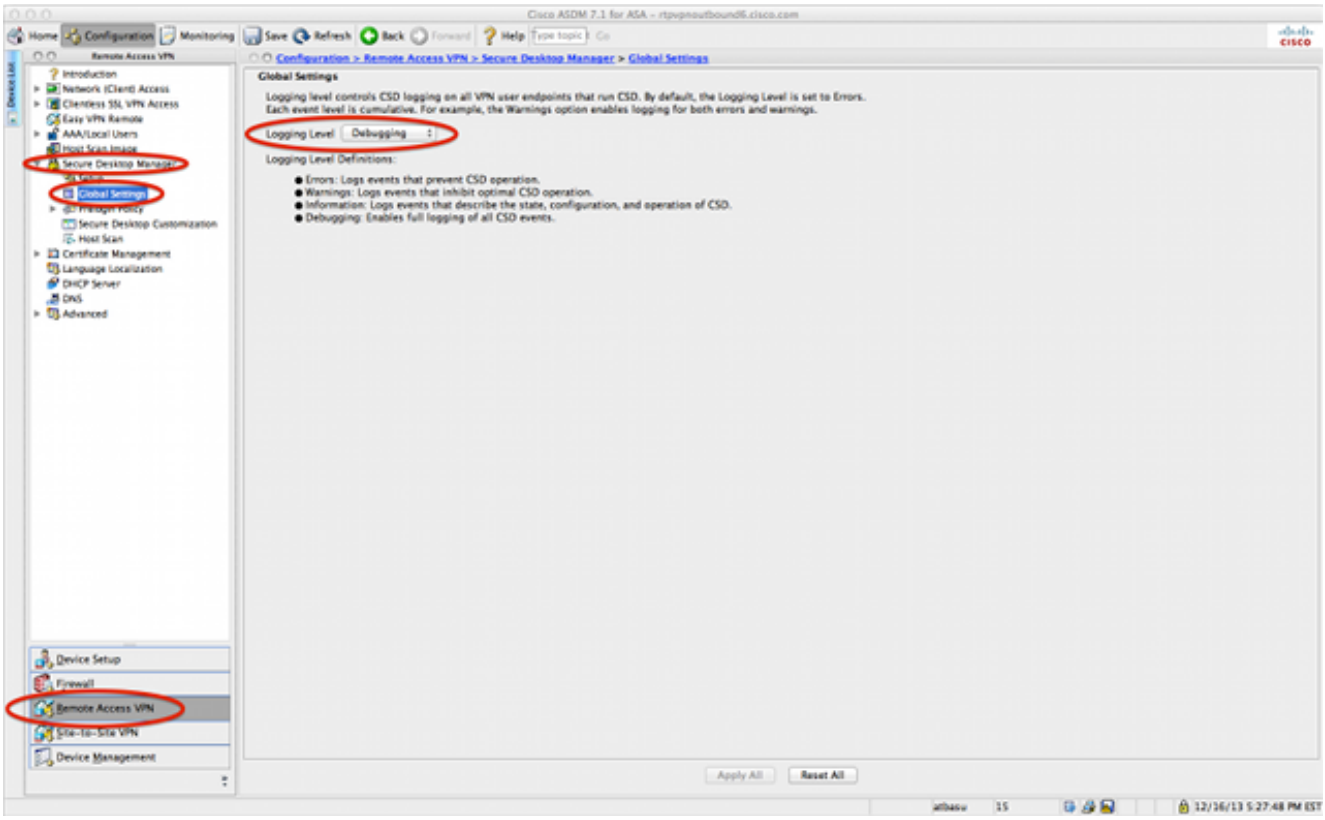
Hinweis: Dieses Verfahren wurde mit Java 7-Updates 9, 10 und 11 getestet.

CSD/Hostscan

Bei CSD/Hostscan-bezogenen Problemen erfassen Sie die DART-Protokolle sowie die Java-Konsolenprotokolle.

Um die DART-Protokolle abzurufen, muss die CSD-Protokollierungsebene auf das Debugging auf der ASA-Plattform gestellt werden:

1. Navigieren Sie zu **ASDM > Configuration > Remote Access VPN > Secure Desktop Manager > Global Settings.**
2. Aktivieren Sie die CSD-Protokollierung für das Debugging im Cisco Adaptive Security Device Manager (ASDM).
3. Verwenden Sie DART, um die CSD/Hostscan-Protokolle zu erfassen.



Windows

Hostscan ist anfällig für Abstürze, die den zuvor für AnyConnect in Windows beschriebenen ähnlich sind (Cisco Bug ID CSCuc55720). Das Problem mit dem Hostscan wurde durch die Cisco Bug-ID CSCuc48299, "IE mit Java 7-Abstürzen beim HostScan-Weblaunch", gelöst.

Mac

Probleme mit CSD 3.5.x und Java 7

In CSD 3.5.x schlagen alle WebVPN-Verbindungen fehl. dies umfasst AnyConnect-Webeinführungen. Die Java-Konsolenprotokolle zeigen keine Probleme an:

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

Wenn Sie ein Downgrade auf JRE 6 durchführen oder CSD auf 3.6.6020 oder höher aktualisieren, werden in den Java-Konsolenprotokollen die folgenden Probleme angezeigt:

```
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.
```

Die Lösung ist ein Upgrade von CSD oder ein Downgrade von Java. Da Cisco empfiehlt, die neueste CSD-Version auszuführen, sollten Sie statt Java-Downgrades ein CSD-Upgrade durchführen, insbesondere da ein Java-Downgrade auf einem Mac schwierig sein kann.

Probleme mit Chrome und Safari mit WebLaunch auf Mac 10.8

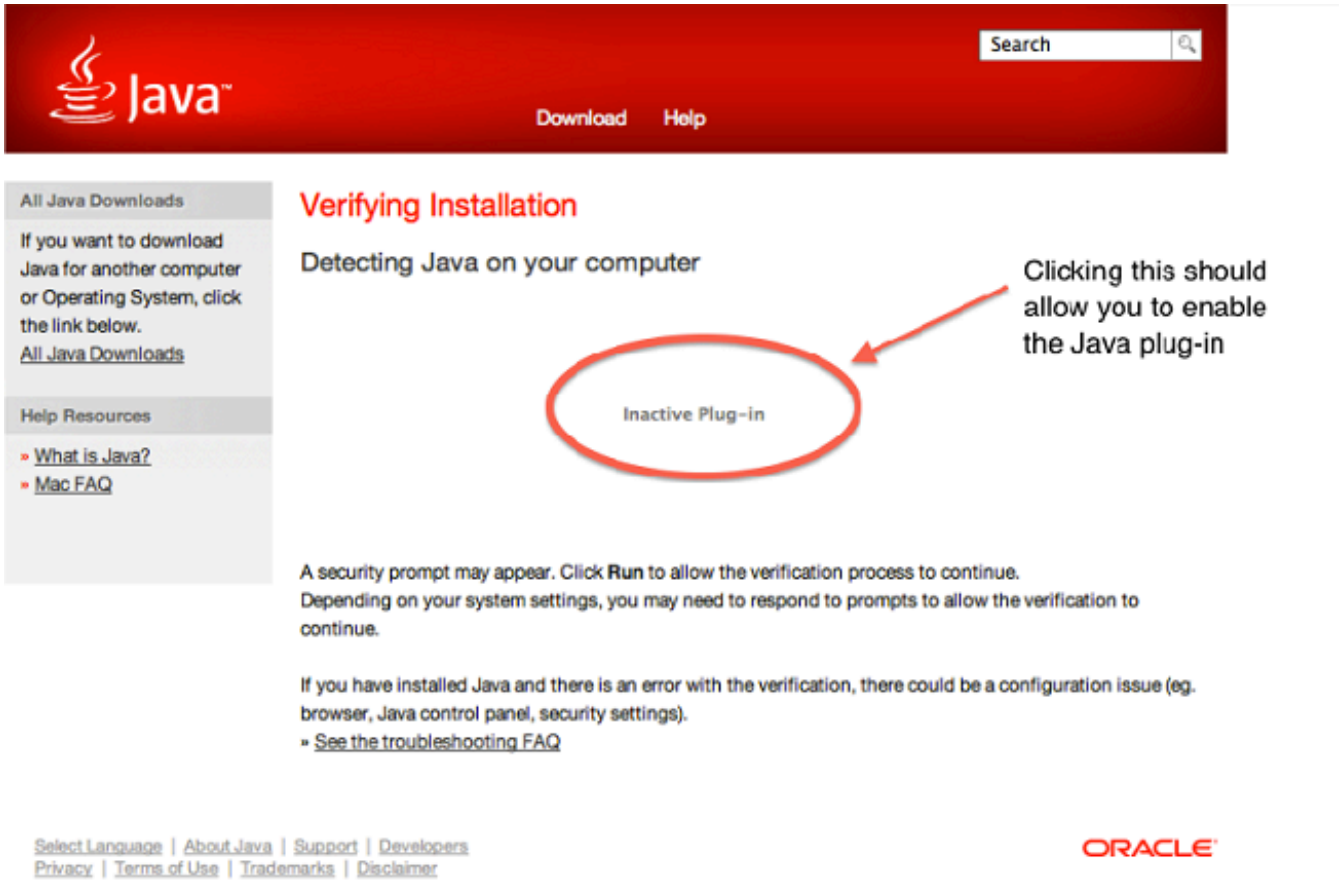
Probleme mit Chrome und Safari werden erwartet:

- Chrome ist ein 32-Bit-Browser und unterstützt Java 7 nicht.
- Chrome war noch nie ein offiziell unterstützter Browser für WebLaunch.
- Mac 10.8 deaktiviert die Verwendung von Java 7 auf Safari, und ältere Versionen von Java sind nicht standardmäßig aktiviert.

Wenn Sie bereits Java 7 installiert haben, sind folgende Auflösungen verfügbar:

- Verwenden Sie Firefox.
- Java 7 auf Safari aktivieren:

  Überprüfen Sie, ob Java 7 auf dem Mac installiert ist und der Mac neu gestartet wurde. Öffnen Sie Firefox, und wechseln Sie zum Java Verifier.Öffnen Sie Safari, und gehen Sie zum Java Verifier erneut. Dieser Bildschirm wird angezeigt:



- Java 7 deaktivieren und Java SE 6 von Apple aktivieren.

  Tipp: Wenn Sie Java nicht installiert haben oder eine ältere Version von Java haben, sehen Sie wahrscheinlich die Fehlermeldung "Java für diese Website blockiert" auf java.com . Informationen zur Installation von Java-Updates finden Sie im Apple Support-Forum am 28. August 2013 unter Java-Updates für OS X.

Probleme mit Safari mit WebLaunch auf Mac 10.9

Wenn Sie auf Mac 10.9 sind und das Java-Plugin bereits aktiviert ist (wie im Abschnitt Probleme mit Chrome und Safari mit WebLaunch auf Mac 10.8 beschrieben), kann der WebLaunch weiterhin fehlschlagen. Alle Java-Applets werden initiiert, aber der Browser dreht sich einfach weiter. Wenn Java-Protokolle wie im Abschnitt Allgemeine Fehlerbehebung beschrieben aktiviert sind, füllen die Protokolle schnell aus, wie hier gezeigt:

```
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
```

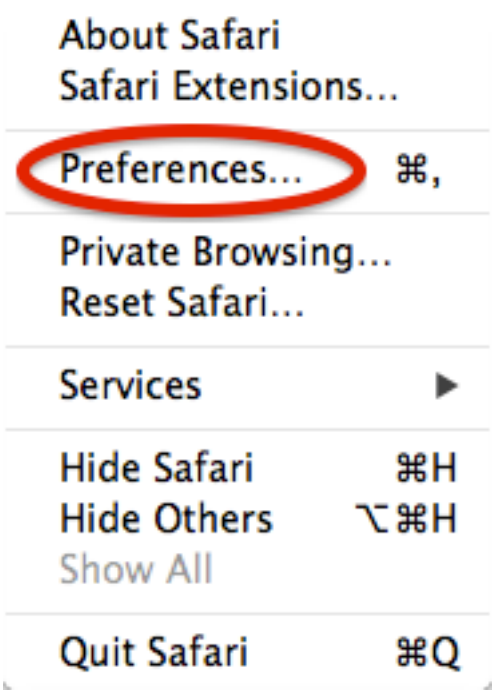
```
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45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

Suchen Sie diesen Eintrag im Protokoll weiter oben:

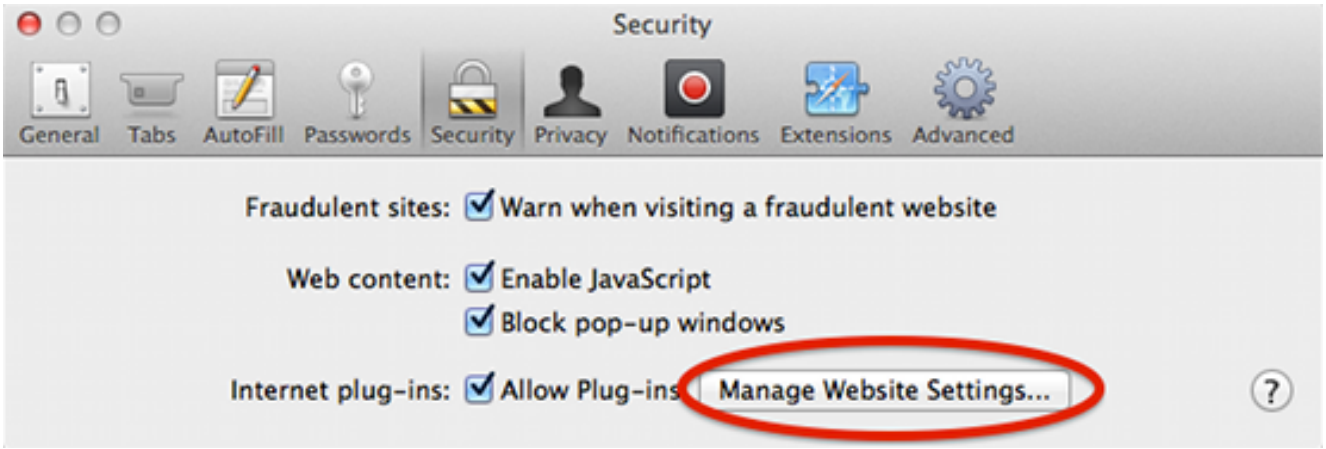
```
Mon Dec 16 16:00:17 EST 2013 Downloaded https://rave.na.sage.com/CACHE/
sdesktop/hostscan/darwin_i386/manifest java.io.FileNotFoundException:
/Users/user1/.cisco/hostscan/bin/cstub (Operation not permitted) at
java.io.FileInputStream.open(Native Method)
```

Dies weist darauf hin, dass Sie die Cisco Bug-ID CSCuj02425 "WebLaunch on OSX 10.9 failed if java unsafe mode is disabled" (Web-Launch auf OSX 10.9 fehlgeschlagen) erhalten. Um dieses Problem zu umgehen, ändern Sie die Java-Einstellungen so, dass Java im unsicheren Modus für Safari ausgeführt werden kann:

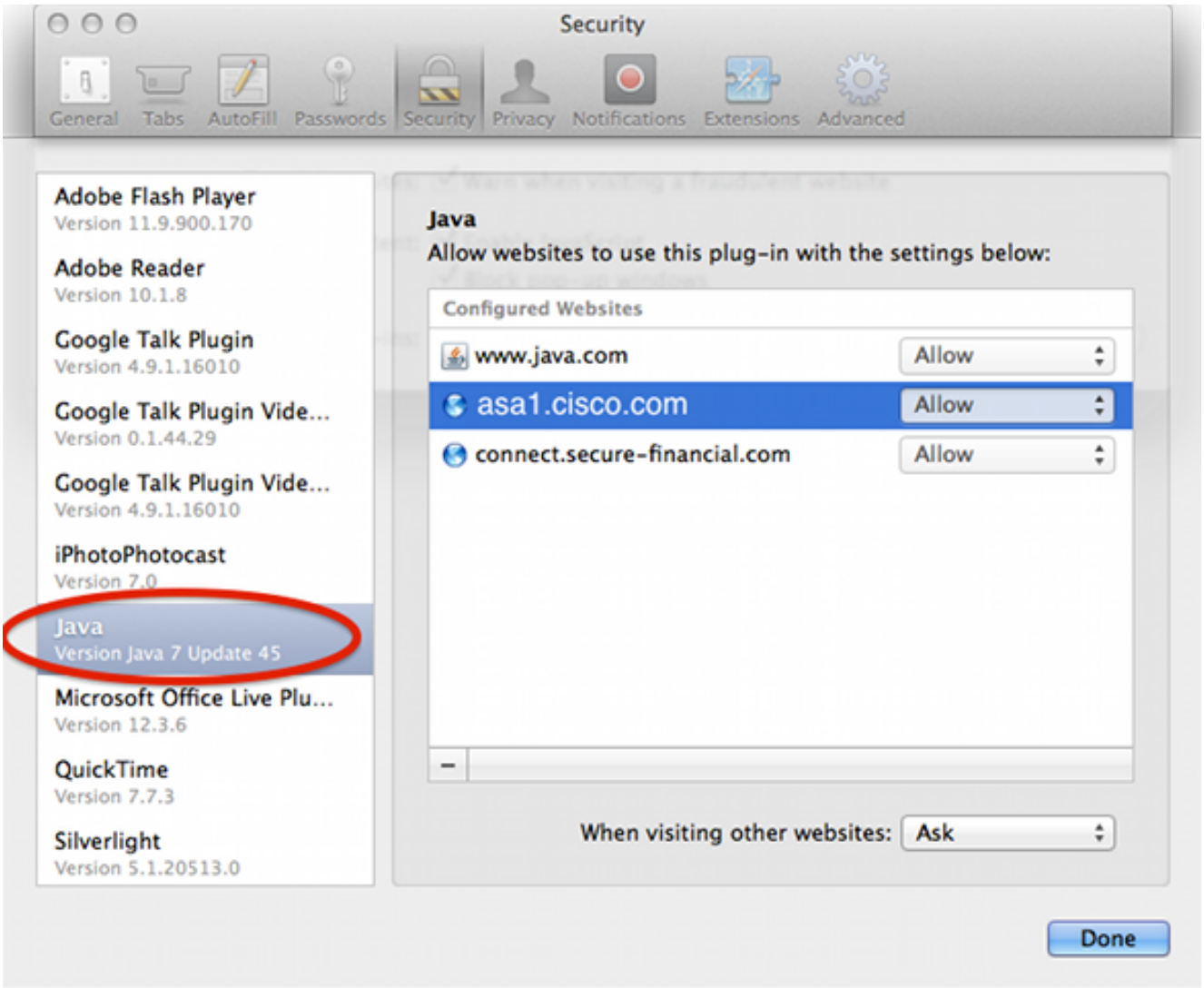
1. Klicken Sie auf **Voreinstellungen**.



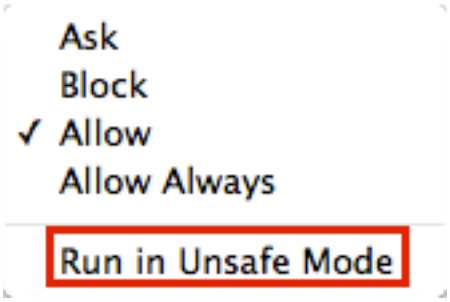
2. Klicken Sie auf **Websiteeinstellungen verwalten**.



3. Wählen Sie auf der Registerkarte **Sicherheit Java aus**, und beachten Sie, dass **Allow** standardmäßig ausgewählt ist.



4. Ändern **Zulassen** für **die Ausführung im ungesicherten Modus**.



WebVPN

Für WebVPN-Probleme im Zusammenhang mit Java sollten Sie diese Daten zu Fehlerbehebungszwecken erfassen:

- Ausgabe über den Befehl **show tech-support**.
- Java-Konsole protokolliert mit und ohne Adaptive Security Appliance (ASA), wie im Abschnitt Allgemeine Fehlerbehebung beschrieben.
- WebVPN-Erfassung.
- HTTP-Überwachungsaufzeichnungen auf lokalen Computern mit und ohne ASA.
- Standardpakete werden auf der ASA und auf dem lokalen Computer erfasst. Auf dem lokalen Computer können diese Aufnahmen mit Wireshark durchgeführt werden.Informationen zur Erfassung von Datenverkehr auf der ASA finden Sie unter Konfigurieren der Paketerfassung.
- Alle Jar-Dateien, die beim Durchlaufen der ASA in den Java-Cache heruntergeladen wurden. Dies ist ein Beispiel von der Java-Konsole:

```
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 diesem Beispiel ist 6a0665e9-1f510559.idx die zwischengespeicherte Version von mffta.jar 7. Wenn Sie keinen Zugriff auf diese Dateien haben, können Sie diese im Java-Cache sammeln, wenn Sie eine direkte Verbindung verwenden.

Eine Testeinrichtung kann die Auflösung beschleunigen.

Sicherheitsfunktionen in Java 7 U51 und Auswirkungen auf WebVPN-Benutzer

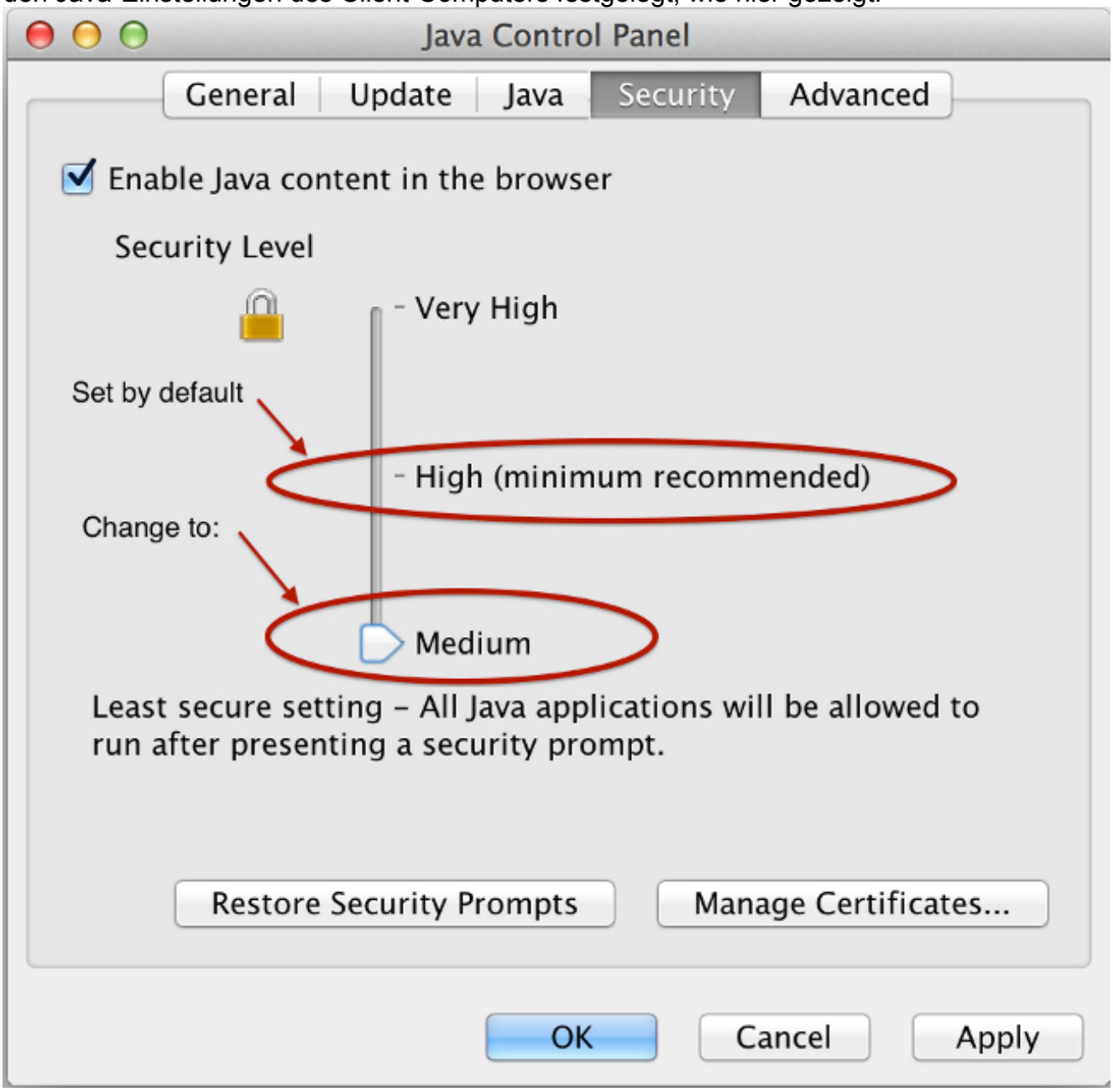
Kürzlich angekündigte Änderungen für Java 7 Update 51 (Januar 2014) haben festgestellt, dass der Standard-Sicherheitsregler Codesignaturen und das Permissions Manifest-Attribut erfordert. Zusammenfassend lässt sich sagen, dass alle Java-Applets Folgendes erfordern:

- zu signieren (Applets und Web Start-Anwendungen).
- um das Attribut "Berechtigungen" im Manifest festzulegen.

Die Anwendungen sind betroffen, wenn Java über einen Webbrowser gestartet wird. Anwendungen werden von einem beliebigen Ort aus ausgeführt, in dem ein Webbrowser nicht funktioniert. Dies bedeutet für WevVPN, dass alle von Cisco verteilten Client-Plugins betroffen sein können. Da diese Plug-Ins nicht von Cisco verwaltet oder unterstützt werden, kann Cisco keine Änderungen am Code-Signaturzertifikat oder am Applet vornehmen, um sicherzustellen, dass diese Einschränkungen eingehalten werden. Die richtige Lösung dafür ist die Verwendung

des temporären Code-Signaturzertifikats auf der ASA. ASAs stellen ein temporäres Code Signing-Zertifikat bereit, um Java-Applets zu signieren (für Java Rewriter und Plugins). Mit dem temporären Zertifikat können Java-Applets ihre vorgesehenen Funktionen ohne Warnmeldung ausführen. ASA-Administratoren sollten das temporäre Zertifikat ersetzen, bevor es abläuft, mit einem eigenen Code Signing Certificate, das von einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) ausgestellt wird. Wenn dies keine praktikable Option ist, besteht die Problemumgehung darin, die folgenden Schritte auszuführen:

1. Sie können die Funktion der Ausnahmeliste in den Java-Einstellungen des Endclientcomputers verwenden, um die von Sicherheitseinstellungen blockierten Anwendungen auszuführen. Die Schritte hierzu werden in Issues with Safari with WebLaunch unter Mac 10.9 beschrieben.
2. Sie können auch die Java-Sicherheitseinstellungen senken. Diese Einstellung wird auch in den Java-Einstellungen des Client-Computers festgelegt, wie hier gezeigt:



Warnung: Die Verwendung dieser Workarounds gibt Ihnen noch einige Fehler, aber Java blockiert die Anwendung nicht, wie es ohne die vorhandenen Workarounds getan hätte.

Windows

Anwendungen, die Java-Applets starten, sind nach einem Upgrade auf Java 7 über WebVPN fehlerhaft. Dieses Problem wird durch die fehlende Unterstützung von Secure Hash Algorithm (SHA)-256 für den Java Rewriter verursacht. Die Cisco Bug-ID CSCud54080, "SHA-256 support for webvpn Java rewriter", wurde für dieses Problem abgelegt.

Anwendungen, die Java-Applets über das Portal mit Smart Tunnel starten, können fehlschlagen, wenn JRE7 verwendet wird. Dies ist bei 64-Bit-Systemen am häufigsten der Fall. Beachten Sie in den Aufnahmen, dass die Java VM die Pakete in Klartext sendet, nicht über die Smart Tunnel-Verbindung an die ASA. Dies wurde mit der Cisco Bug-ID CSCue17876 "Einige Java-Applets werden nicht über Smart Tunnel auf Fenstern mit jre1.7 verbunden."