Java 7 Issues with AnyConnect, CSD/Hostscan, and WebVPN - Troubleshooting Guide

Contents

Introduction

General Troubleshooting

- Windows
- Mac

Specific Troubleshooting

- AnyConnect
  - Windows
  - Mac
  - Miscellaneous
- CSD/Hostscan
  - Windows
  - Mac
- WebVPN
  - Security Features in Java 7 U51 and How That Affects WebVPN Users
  - Windows

Introduction

This document describes how to troubleshoot issues with Java 7 on Cisco AnyConnect Secure Mobility Client, Cisco Secure Desktop (CSD)/Cisco Hostscan, and clientless SSL VPN (WebVPN).

Note: Cisco bug IDs marked as investigative are not restricted to the symptoms described. If you face issues with Java 7, ensure that you upgrade the AnyConnect client version to the latest client version or to at least the 3.1 maintenance release 3 version available on Cisco Connection Online (CCO).

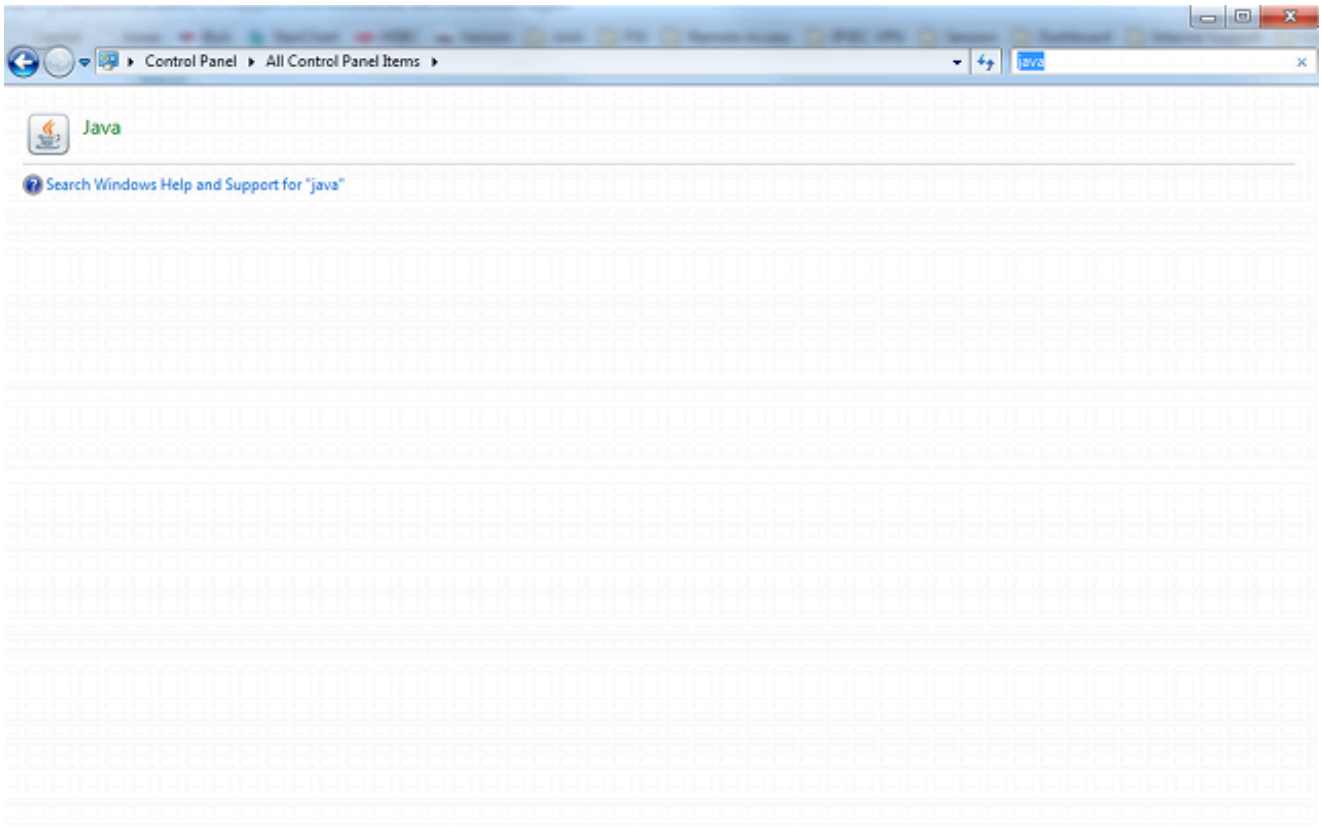
General Troubleshooting

Run the Java Verifier in order to check if Java is supported on the browsers in use. If Java is enabled properly, review the Java console logs in order to analyze the problem.

Windows

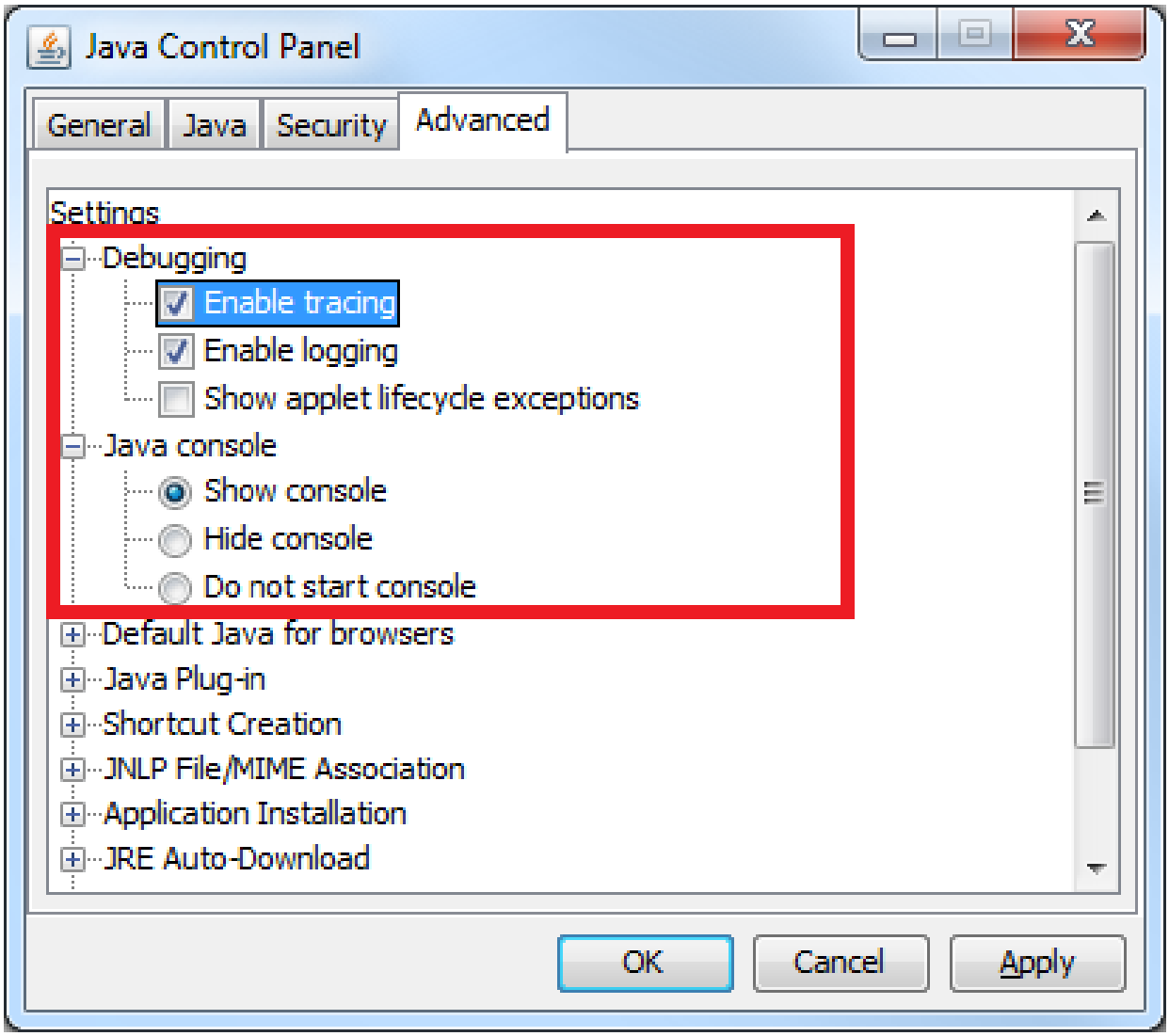
This procedure describes how to enable the console logs in Windows:

1. Open the Windows Control Panel, and search for Java.



2. Double-click **Java** (the coffee cup icon). The Java Control Panel appears.
3. Click the **Advanced** tab.

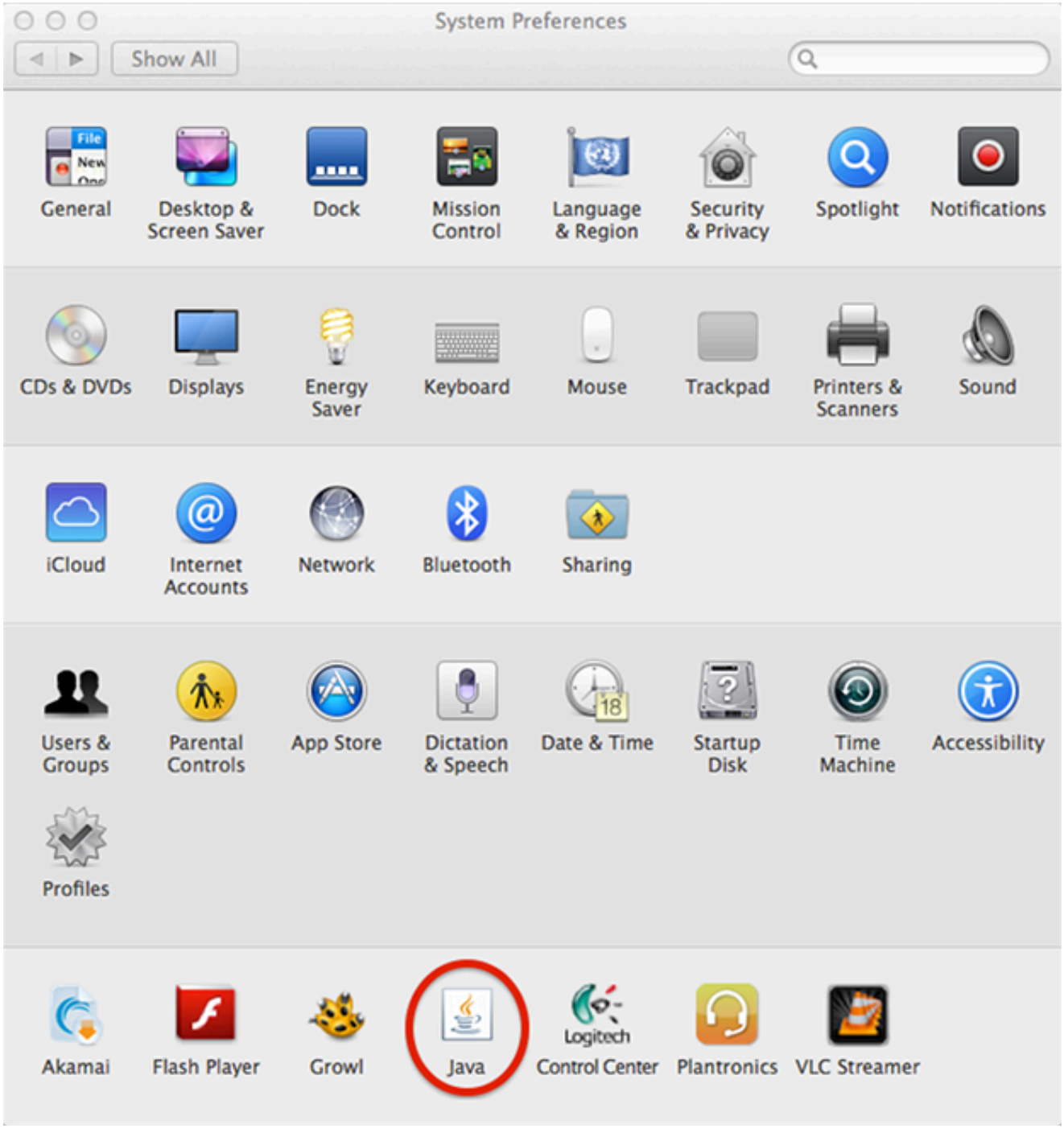
    a. Expand **Debugging**, and select **Enable tracing** and **Enable logging**.
    b. Expand **Java console**, and click **Show console**.



Mac

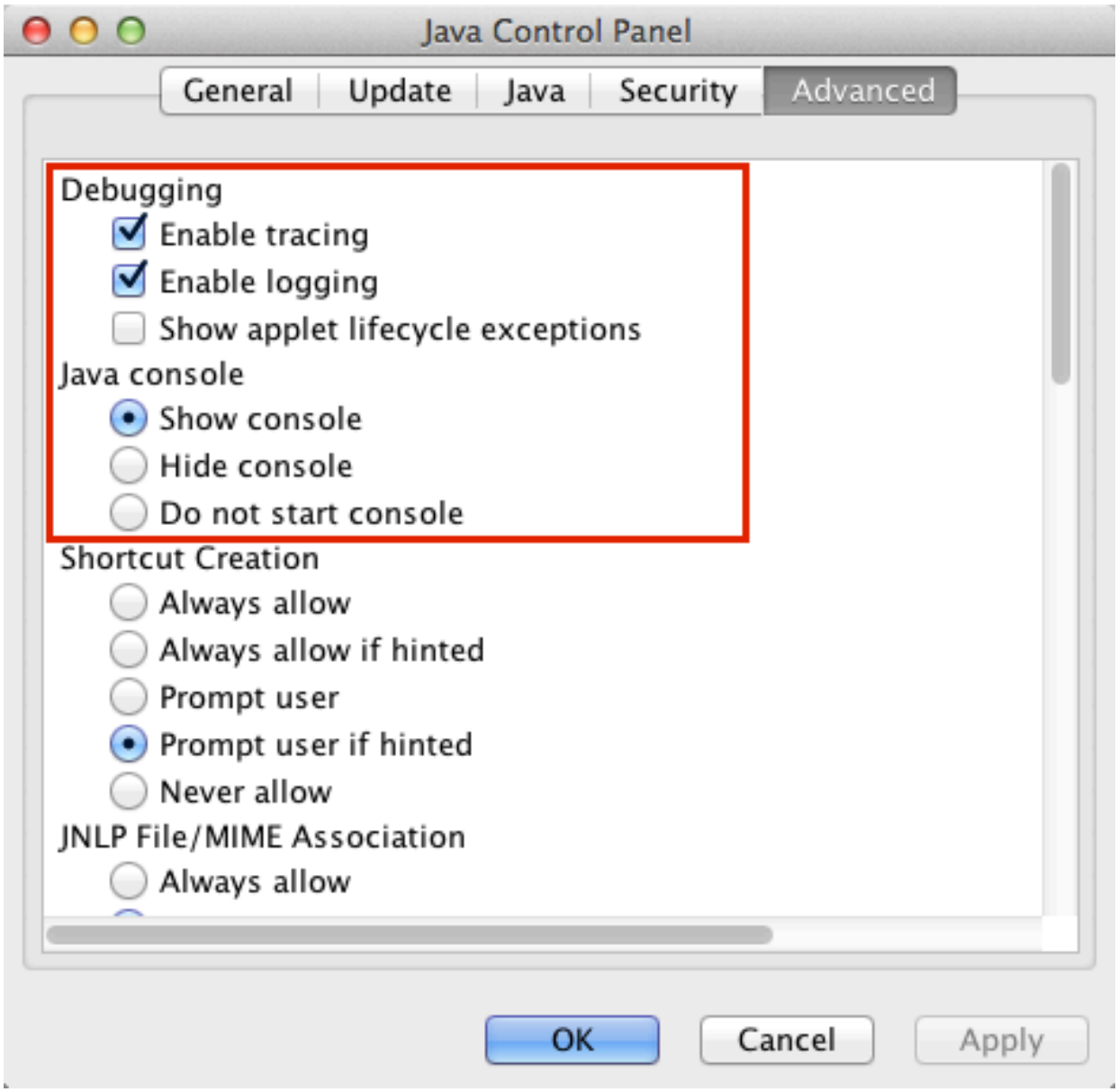
This procedure describes how to enable the console logs on a Mac:

1. Open System Preferences, and double-click the Java icon (coffee cup). The Java Control Panel appears.



2. Click the **Advanced** tab.

    a. Under Java console, click **Show console**.
    b. Under Debugging, click **Enable tracing** and **Enable logging**.



Specific Troubleshooting

AnyConnect

For AnyConnect-related issues, collect the Diagnostic AnyConnect Reporting (DART) logs as well as the Java console logs.

Windows

Cisco bug ID CSCuc55720, "IE crashes with Java 7 when 3.1.1 package is enabled on the ASA," was a known issue, where Internet Explorer crashed when a WebLaunch was performed and AnyConnect 3.1 was enabled on the headend. This bug has been fixed.

You might encounter issues when you use some versions of AnyConnect and Java 7 with Java apps. For further information, see Cisco bug ID CSCue48916, "Java App(s) Break when using AnyConnect 3.1.00495 or 3.1.02026 & Java v7."

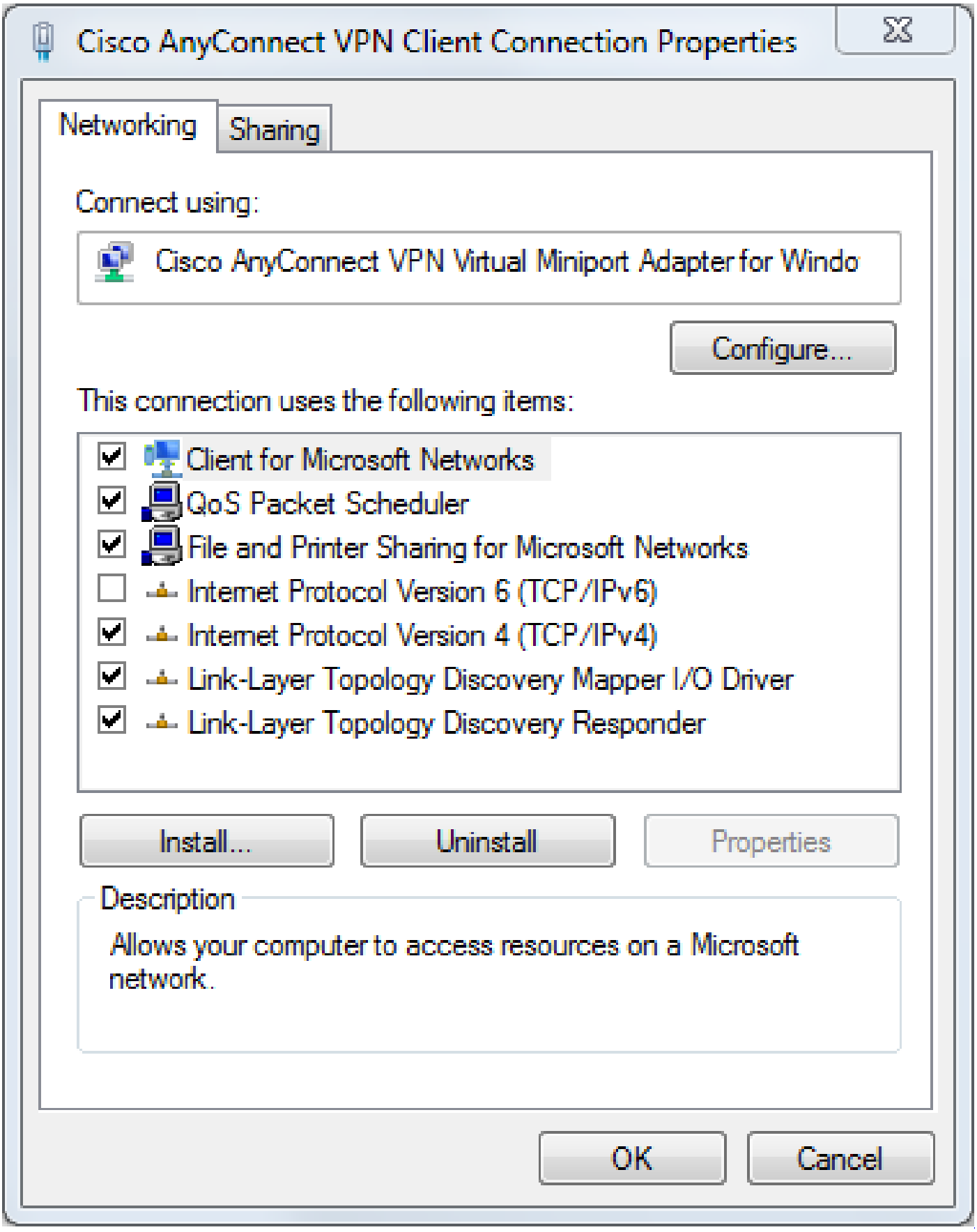
Issues with Java 7 and IPv6 Socket Calls

If AnyConnect does not connect even after you upgrade the Java Runtime Environment (JRE) to Java 7, or if a Java application is unable to connect over the VPN tunnel, review the Java console logs and look for these messages:

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

These log entries indicate that the client/application makes IPv6 calls.

One solution for this issue is to disable IPv6 (if it is not in use) on the Ethernet adapter and the AnyConnect Virtual Adapter (VA):



A second solution is to configure Java to prefer IPv4 over IPv6. Set the system property 'java.net.preferIPv4Stack' to 'true' as shown in these examples:

- Add code for the system property to the Java code (for Java applications written by the customer):

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

- Add code for the system property from the command line:

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

- Set the environment variables _JPI_VM_OPTIONS and _JAVA_OPTIONS in order to include the system property:

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

For additional information, refer to:

- How to set java.net.preferIPv4Stack=true in the java code?
- How to force java to use ipv4 instead ipv6?

A third solution is to disable IPv6 completely on Windows machines; edit this registry entry:

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

For additional information, see How to disable IP version 6 or its specific components in Windows.

Issues with AnyConnect WebLaunch After Java 7 Upgrade

Cisco JavaScript code previously looked for Sun as the value for the Java vendor. However, Oracle changed that value as described in JDK7: Java vendor property changes. This issue was fixed by Cisco bug ID CSCub46241, "AnyConnect weblaunch fails from Internet Explorer with Java 7."

Mac

No issues have been reported. Tests with AnyConnect 3.1 (with the WebLaunch / Safari / Mac 10.7.4 / Java 7.10 configuration) show no errors.

Miscellaneous

Issues with Java 7 Apps on Cisco AnyConnect

Cisco bug ID CSCue48916, "Java App(s) Break when using AnyConnect 3.1.00495 or 3.1.02026 & Java v7," has been filed. Initial investigation indicates that the issues are not a bug on the client side, but might be related to the Java virtual machine (VM) configuration instead.

Previously, in order to use Java 7 apps on the AnyConnect 3.1(2026) client, you unchecked the IPv6 virtual adapter settings. However, it is now necessary to complete all of the steps in this procedure:

1. Install AnyConnect Version 3.1(2026).
2. Uninstall Java 7.
3. Reboot.
4. Install Java SE 6, update 38, available on the Oracle web site.
5. Navigate to the Java 6 control panel settings, then click the **Update** tab to upgrade to the latest version of Java 7.
6. Open a command prompt and enter:

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

7. Log in with AnyConnect, and the Java apps should work.

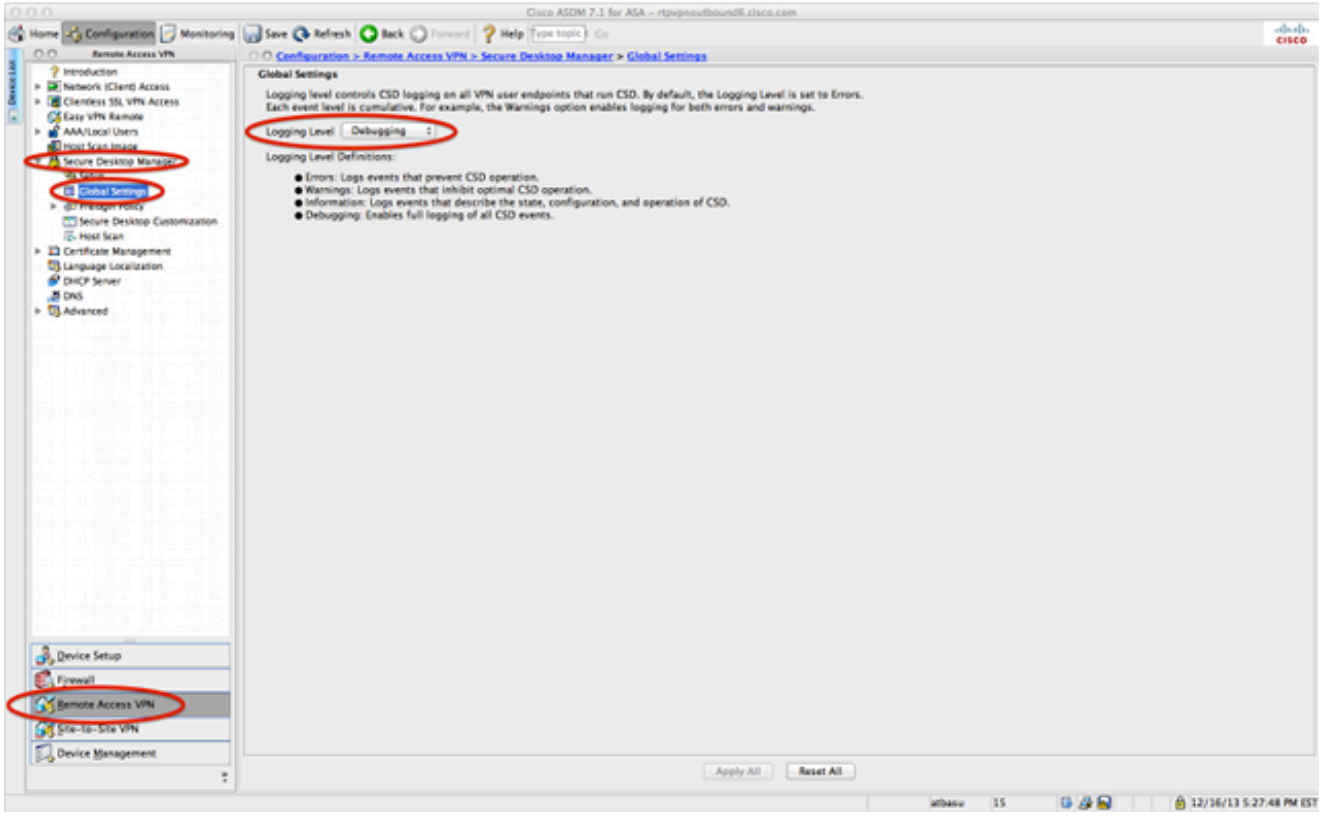
Note: This procedure has been tested with Java 7 updates 9, 10, and 11.

CSD/Hostscan

For CSD/Hostscan-related issues, collect the DART logs as well as the Java console logs.

In order to obtain the DART logs, the CSD logging level must be turned to debugging on the ASA:

1. Navigate to **ASDM** > **Configuration** > **Remote Access VPN** > **Secure Desktop Manager** > **Global Settings**.
2. Turn up CSD logging to debugging on the Cisco Adaptive Security Device Manager (ASDM).
3. Use DART in order to collect the CSD/Hostscan logs.



Windows

Hostscan is susceptible to crashes similar to those described previously for AnyConnect in Windows (Cisco bug ID CSCuc55720). The hostscan issue has been resolved by Cisco bug ID CSCuc48299, "IE with Java 7 crashes on HostScan Weblaunch."

Mac

Issues with CSD Versions 3.5.x and Java 7

In CSD 3.5.x, all WebVPN connections fail; this includes AnyConnect web launches. The Java console logs do not reveal any problems:

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

If you downgrade to JRE 6 or upgrade CSD to 3.6.6020 or later, the Java console logs do reveal the problems:

<#root>

```
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.

The resolution is to upgrade CSD or downgrade Java. Because Cisco recommends that you run the latest version of CSD, you should upgrade CSD, rather than downgrade Java, especially since a Java downgrade can be difficult on a Mac.

Issues with Chrome and Safari with WebLaunch on Mac 10.8

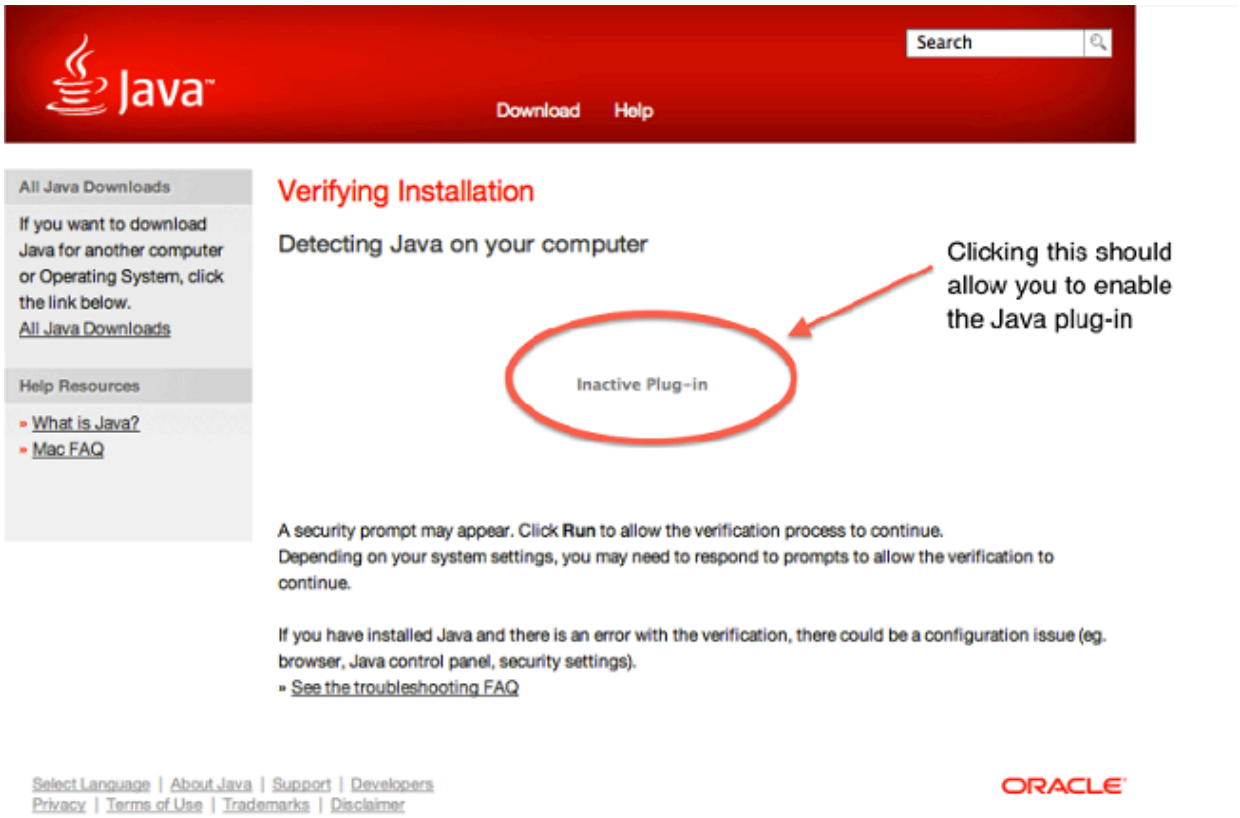
Issues with Chrome and Safari are expected behavior:

- Chrome is a 32-bit browser and does not support Java 7.
- Chrome has never been an officially supported browser for WebLaunch.
- Mac 10.8 disabled the use of Java 7 on Safari, and older versions of Java are not enabled by default.

If you already have Java 7 installed, the resolutions are:

- Use Firefox.
- Enable Java 7 on Safari:

    1. Verify that Java 7 is installed on the Mac and that the Mac has been restarted. Open Firefox, and go to the Java Verifier.
    2. Open Safari, and go the Java Verifier again. You should now see this screen:



- Disable Java 7, and enable Java SE 6 provided by Apple.

Tip: If you do not have Java installed or you have an older version of Java, you are likely to see the error message 'Java blocked for this web site' on java.com . See Java updates available for OS X on August 28, 2013 on the Apple support forum for information on installation of Java updates.

Issues with Safari with WebLaunch on Mac 10.9

If you you are on Mac 10.9 and already have the Java plugin enabled (as described in the Issues with Chrome and Safari with WebLaunch on Mac 10.8 section), the WebLaunch might continue to fail. All Java applets are initiated, but the browser simply continues to spin. If Java logs are enabled as described in the General Troubleshooting section, the logs quickly fill up as shown here:

```
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
```

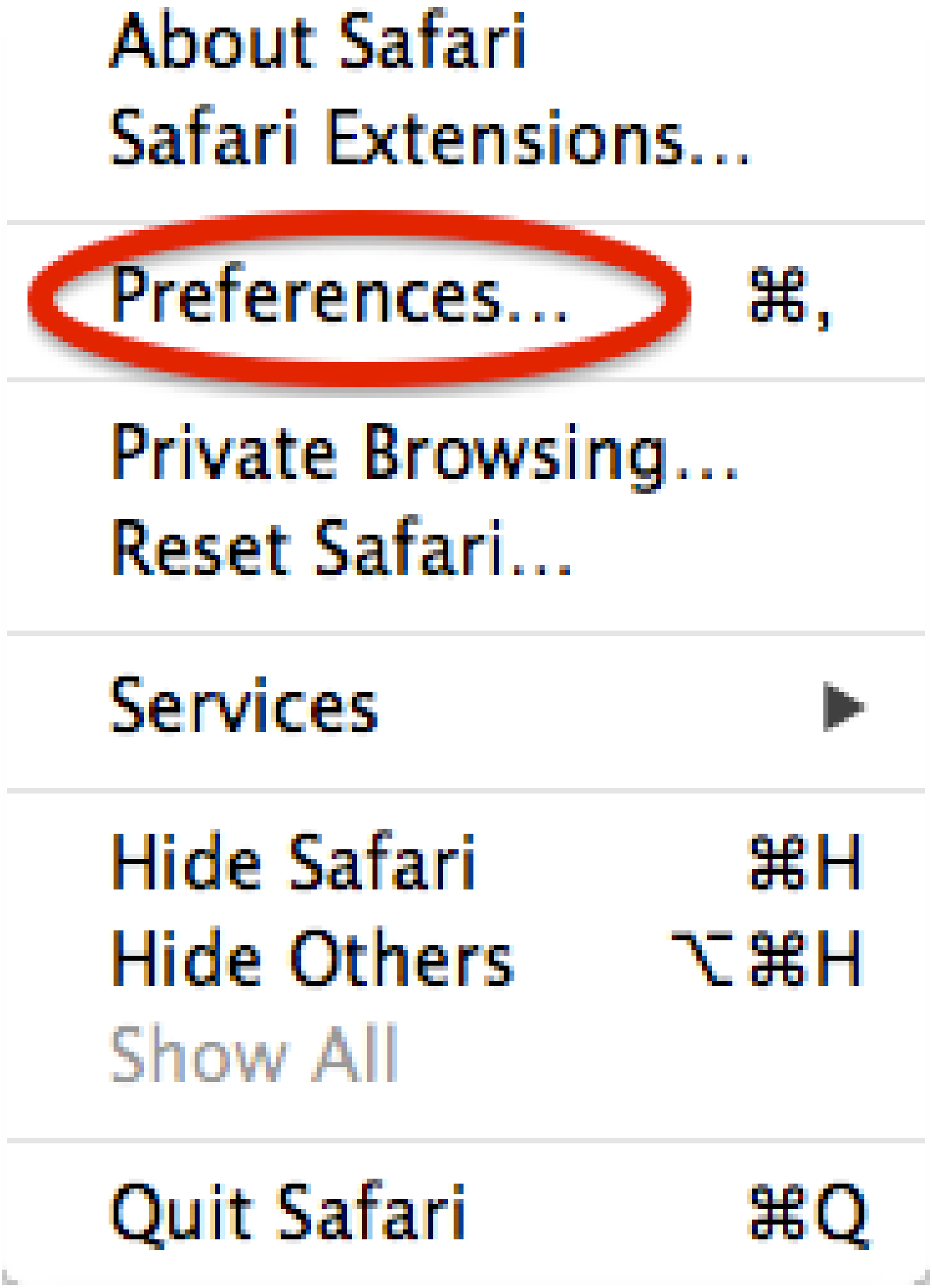
```
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45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

Look for this type of entry earlier in the log:

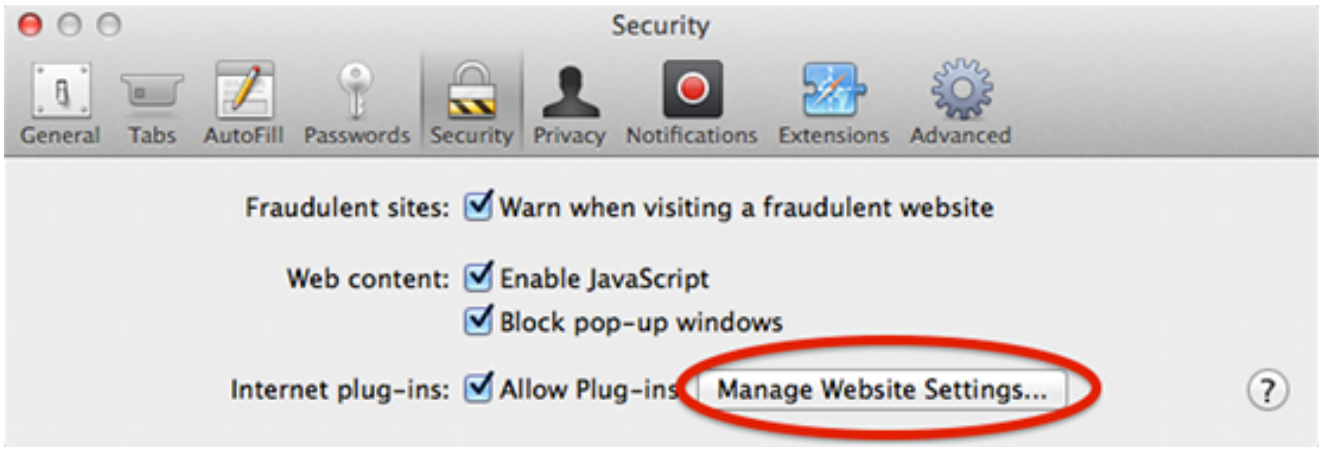
```
Mon Dec 16 16:00:17 EST 2013 Downloaded https://rave.na.sage.com/CACHE/
   sdesktop/hostscan/darwin_i386/manifest java.io.FileNotFoundException:
   /Users/user1/.cisco/hostscan/bin/cstub (Operation not permitted) at
   java.io.FileInputStream.open(Native Method)
```

This indicates that you are encountering Cisco bug ID CSCuj02425, "WebLaunch on OSX 10.9 fails if java unsafe mode is disabled." In order to workaround this issue, modify the Java preferences so Java can run in unsafe mode for Safari:

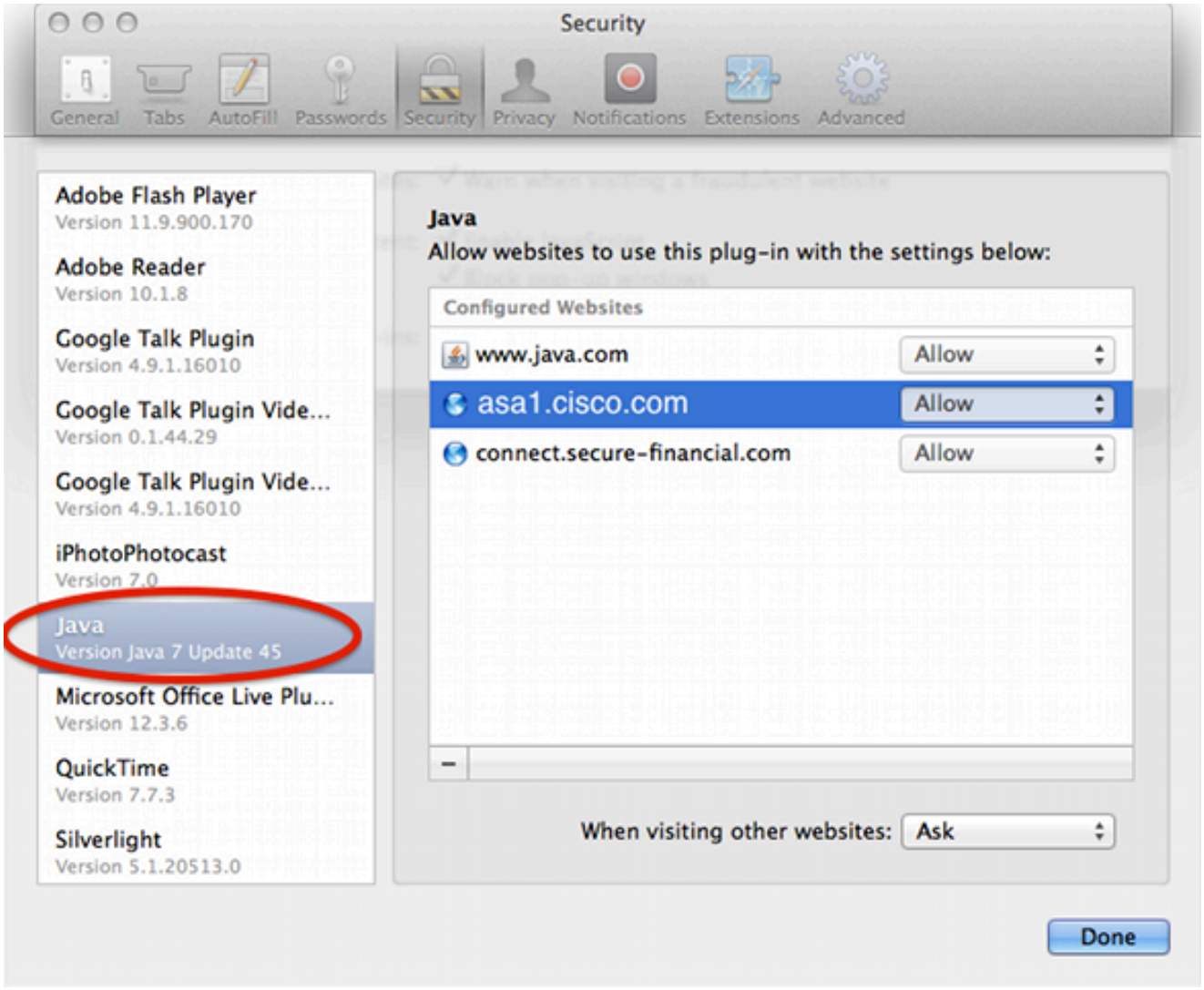
1. Click **Preferences**.



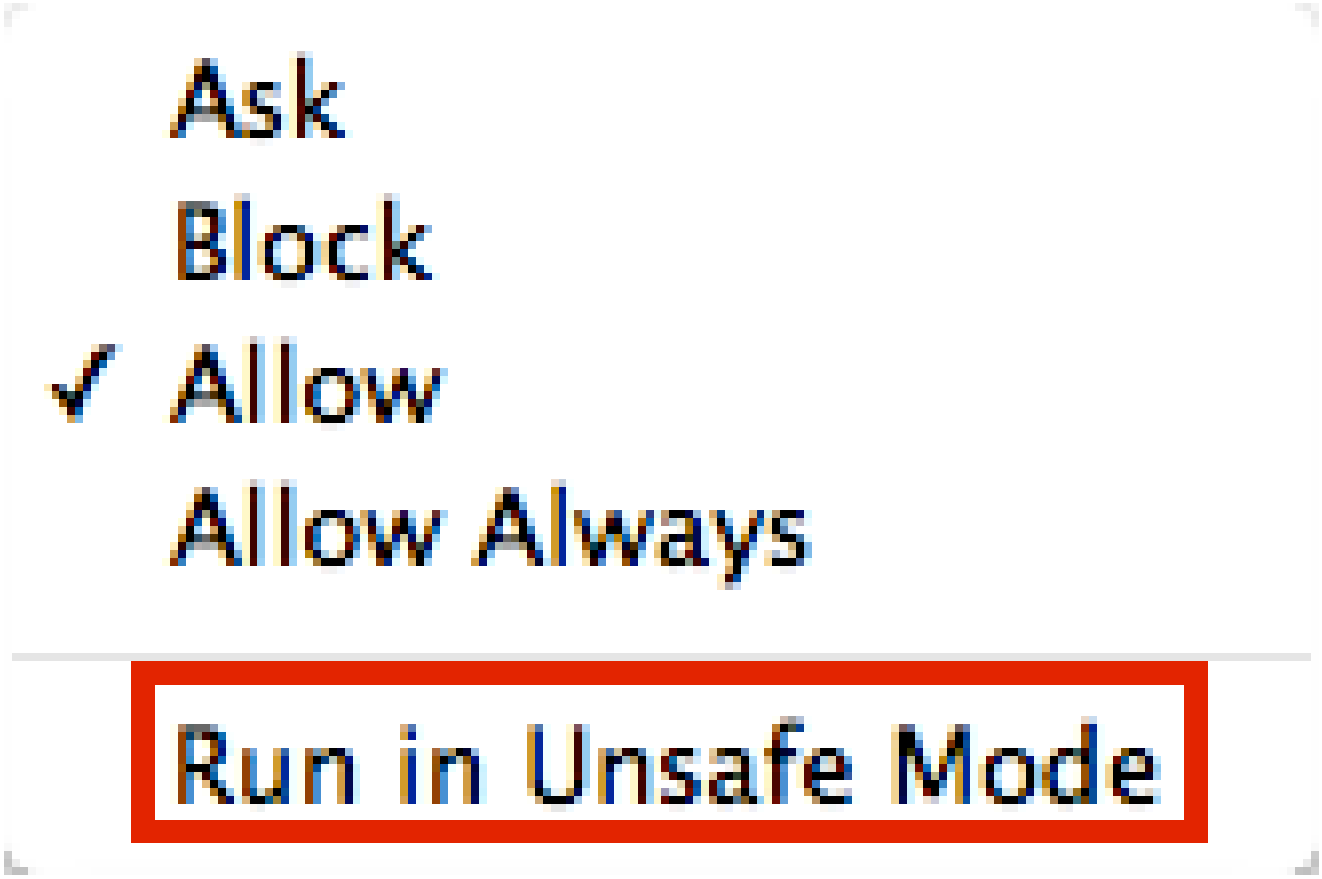
2. Click **Manage Website Settings**.



3. In the **Security** tab, select **Java**, and note that **Allow** is selected by default.



4. Change **Allow** to **Run in Unsafe Mode**.



WebVPN

For WebVPN issues related to Java, collect this data for troubleshooting purposes:

- Output from the **show tech-support** command.
- Java console logs with and without Adaptive Security Appliance (ASA) as explained in the General Troubleshooting section.
- WebVPN captures.
- HTTP watch captures on local machine with and without the ASA.
- Standard packets captures on the ASA and on the local machine.
  - On the local machine, these captures can be done with Wireshark.
  - For information on how to capture traffic on the ASA, see Configuring Packet Captures.
- All jar files downloaded to the Java cache when going through the ASA. This is an example from the 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 this example, 6a0665e9-1f510559.idx is the cached version of mffta.jar 7. If you do not have access to these files, you can collect them from the Java cache when using direct connection.

A test setup can expedite the resolution.

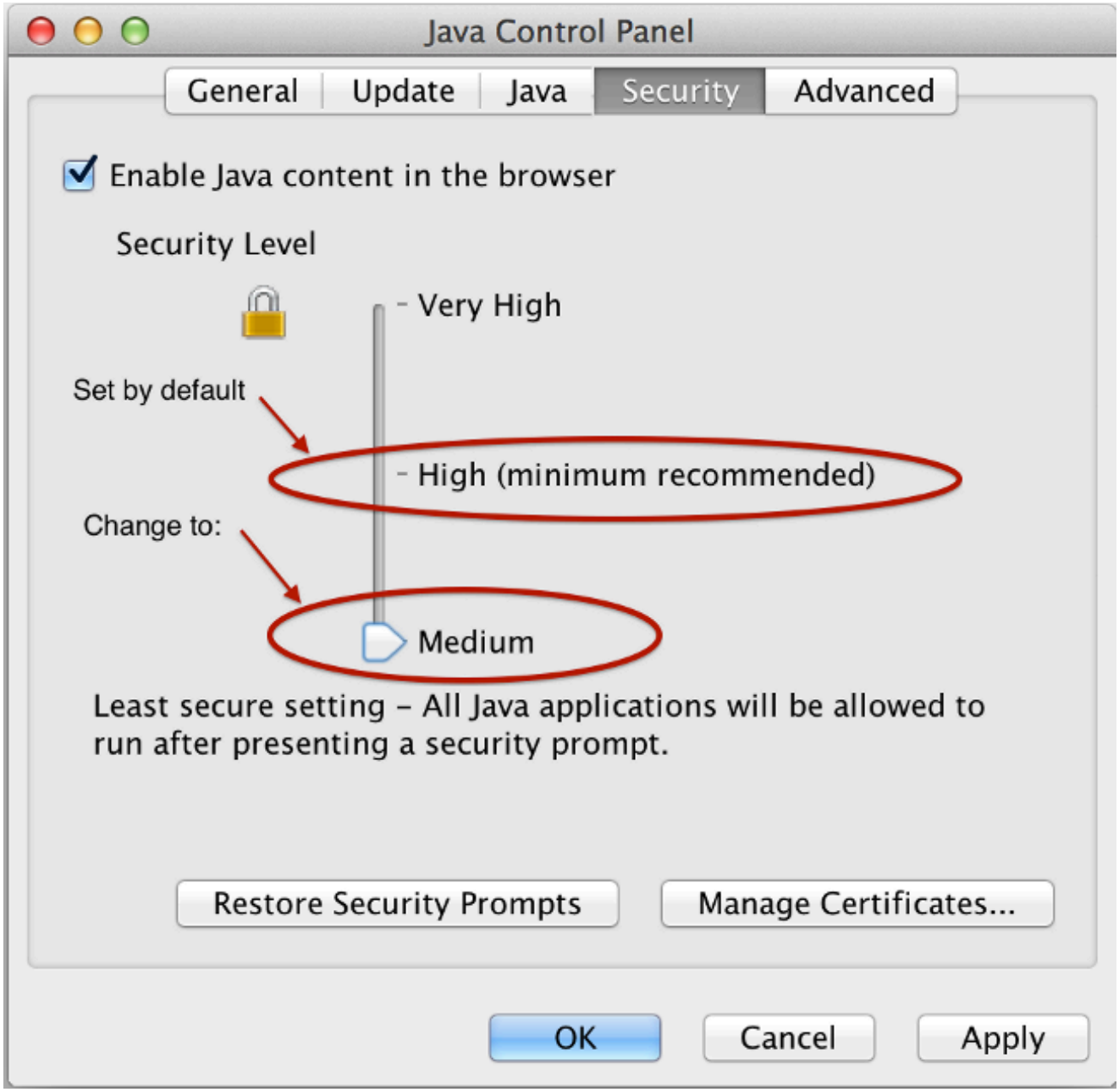
Security Features in Java 7 U51 and How That Affects WebVPN Users

Recently announced changes scheduled for Java 7 update 51 (January 2014) have established that the default security slider requires code signatures and the Permissions Manifest attribute. In summary, all Java applets require:

- to be signed (Applets and Web Start applications).
- to set the "Permissions" attribute within the Manifest.

The applications are affected if it uses Java started through a web browser. Applications run from any where outside a web browser are fine. What this means for WevVPN is all the client plugins that are distributed by Cisco could be impacted. Since these plugins are not maintained or supported by Cisco, Cisco cannot make changes to the code signing certificate or to the applet in order to ensure it complies with these restrictions. The proper solution for this is to use the temporary code signing certificate on the ASA. ASAs provide a temporary code signing certificate to sign Java applets (for Java rewriter and plugins). The temporary certificate lets Java applets perform their intended functions without a warning message. ASA administrators should replace the temporary certificate before it expires with their own code signing certificate issued by a trusted certificate authority (CA). If this is not a viable option, the workaround is to complete these steps:

1. You can use the Exception Site list feature on the end client machine's Java settings in order to run the applications blocked by security settings. The steps to do this are described in .
2. You can also lower the Java Security settings. This setting is also set in the client machine's Java settings as shown here:



Warning: The use of the these workarounds still gives you some errors, but Java does not block the application as it would have done without the workarounds in place

Windows

Applications that launch Java applets have been reported to fail over WebVPN after an upgrade to Java 7. This problem is caused by the lack of Secure Hash Algorithm (SHA)-256 support for the Java rewriter. Cisco bug ID CSCud54080, "SHA-256 support for webvpn Java rewriter," has been filed for this issue.

Applications that start Java applets through the portal with Smart Tunnel might fail when JRE7 is used; this is most common with 64-bit systems. In the captures, note that the Java VM sends the packets in clear text, not through the Smart Tunnel connection to the ASA . This has been addressed by Cisco bug ID CSCue17876, "Some java applets won't connect via smart tunnel on windows with jre1.7."