

[Java Update 1.6.0.19 & .20](#)

Java versions 1.6.0_19 & _20 were recently released. Oracle/Sun has introduced a new practice with these releases where users will be presented with a warning dialog when a program they are using contains both signed and unsigned components.

Details are available here: http://java.sun.com/javase/6/docs/technotes/guides/jweb/mixed_code.html

The warning states "Java has discovered application components that could indicate a security concern". Users are asked if they wish to block potentially unsafe components from being run. If they click Yes (which is recommended on the warning and is the default selection), the Java components will not work.

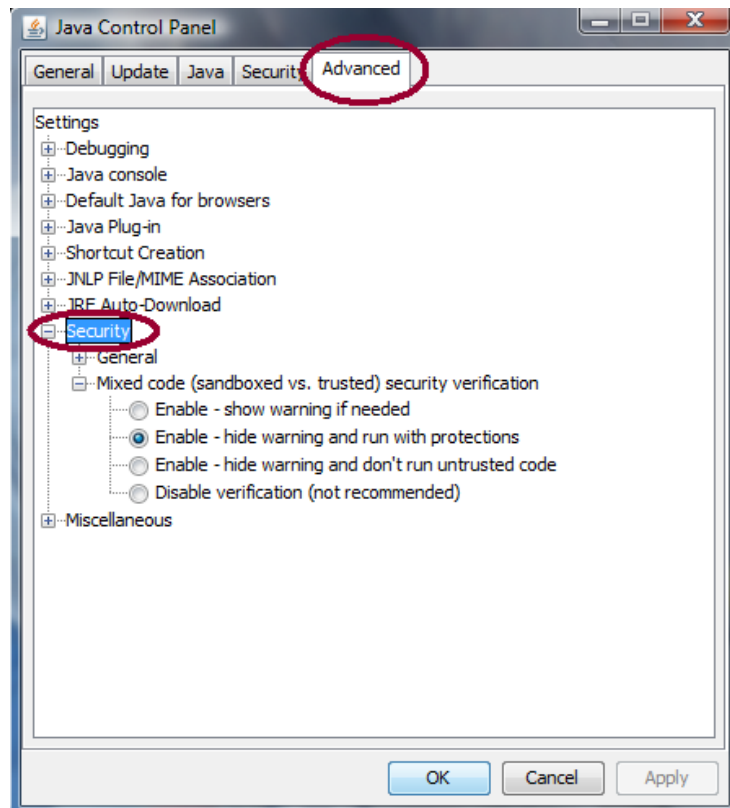
Blackboard Vista 8 users who have upgraded to Java 1.6.0_19 or _20 are presented with this warning when they login to Blackboard Vista 8 (for Who's Online), when they enable the HTML Creator, when they use the Chat tool, or when they access the My Computer applet. If they click Yes, the tool will not run. They must click No to use that Java tool in Blackboard Vista 8.

This only affects Microsoft Windows users.

Mixed Code Protection Options for Users:

User can manage how mixed code programs are handled via the Java Control Panel. The following screen shot shows the four levels of control available. See the Mixed code heading towards the bottom of the Java Control Panel.

Note: To access the Java Control Panel goto, Start menu > Control Panel > Java Control Panel. Choose the Advanced tab, expand security and Mixed Code. Select the second option, "Enable – hide warning and run with protections."



Below are the details of the available options.

1. Enable – show warning if needed.

This is the default setting. When a potential security risk is encountered, a warning dialog is raised. Clicking **Yes** blocks potentially unsafe components from running and may terminate the program. When the user clicks **No**, the application or applet continues execution with protections (packages or resources that are later encountered with the same names but have different trust levels, i.e., signed vs unsigned, will not be loaded).

2. Enable – hide warning and run with protections.

This option suppresses the warning dialog. The code executes as if the user had clicked **No** from the warning dialog.

3. Enable – hide warning and don't run untrusted code.

This option suppresses the warning dialog and behaves as if the user had clicked **Yes** from the warning dialog.

4. Disable verification.

This option is not recommended. This option completely disables the software from checking for mixing trusted and untrusted code, leaving the user to run potentially unsafe code without protections.

A full description of this is available at http://www.java.com/en/download/help/error_mixedcode.xml