

Respondus LockDown Browser™

Troubleshooting checklist:

1. **Internet Explorer**

Check that Internet Explorer (specifically, not just other browsers) can connect to the course server and pass its browser check. This may include having Java installed, JavaScript enabled, and any pop-up blocking disabled.

2. **Java (1.6)**

Currently, Java 1.6 does not always pass browser checks. To fix this,

- a. Go to **Start, Settings, Control Panel, Add/Remove Programs**. Scroll down to **Java™ SE Runtime Environment 6** and remove it.
- b. Go to the site below and download **Java Runtime Environment (JRE) 5.0 Update 12**:
http://java.sun.com/javase/downloads/index_jdk5.jsp
- c. Install the update, then select **Start, Settings, Control Panel**, and open the **Java** icon. Click the **Update** tab, uncheck **Check for Updates Automatically**, and click **OK**.

3. **Run LockDown Browser twice if it freezes**

A freeze may be caused by some information popup appearing "underneath" the browser where a student is unable to click [ok]. LockDown Browser will attempt to move up known messages like Java applet warnings so they become visible but this might not always succeed. Some messages only appear once so running again could get the browser past the freezing point. LockDown Browser shares its applets, viewers, and security certificates with Internet Explorer, so some freezes can be resolved by making sure you select "Yes" to trust a certificate.

4. **Select "Yes" to Diagnostics if it freezes again**

Select "Yes" to running Diagnostics. Run the **Network Connection Test**, use the **Copy to Clipboard** button, then paste the results into an email or text file. This will also tell you the version of LockDown Browser that is installed to make sure it is up-to-date. If you don't see anything suspicious in the results, Respondus support might be able to discover something from the included process list.

Possible Program Conflicts:

1. Firewalls, Internet Security, Privacy applications

For all such applications the first thing to try is to look in their "programs" or "applications" list for **LockDown.exe** or "**LockDown MFC Application**" and change the access rights to "trusted" or "allow all" or similar.

2. Viruses, Spyware, Trojans

Many of these applications can hijack the network connection and interfere with its normal operation, and a virus can infect and damage LockDown Browser. Make sure your PC is running up-to-date antivirus software.

2. P2P / File Sharing programs

File-sharing, bitorrent, and concealment software like Peer Guardian can all interfere with the network connection.

3. Other applications

Students can have any of tens of thousands of different applications installed. LockDown Browser is updated as we discover new conflicts, but students will continue to find and install new conflicting programs. Reviewing your network-using programs or checking Add/Remove Programs for what is installed might turn up something new to disable or temporarily uninstall.

If you find a new application that conflicts with LockDown Browser, please let us know so we can report them to Respondus so that they may attempt to add automatic detection of the conflict to a future update to the browser. All application conflicts should be forwarded to the LockDown System Administrator at lockdown@athens.edu.