LockDown Browser Administrator Guide

Revised September 2015

Blackboard Learn 9.x Edition

CONTENTS

Getting Started 2
- Introduction
- Overview of Browser Application
- Respondus Monitor
- System Requirements

Administrator Functions 3
- Login to Administrator Area
- Institution ID
- Control Panel
- Server Profiles

Respondus LockDown Browser Building Block 7
- Downloading the Respondus LockDown Browser Building Block
- Installing the LockDown Browser Building Block

Distribution and Installation of Respondus LockDown Browser 8
- Student and Lab Editions
- Managed Installations and Updates
- Distribution of the Setup Program
- Installation of Browser
- Updating LockDown Browser
- Issues with Firewalls, Content Filters and Proxy Servers

Additional Information for Instructors 13
- Quick Start Guides
- Background Information
- Determining if the LockDown Browser Settings are Set Correctly
- Additional Tips and Suggestions
- Advanced Features

Instructor Advanced Settings 14
- Lock Students into Browser
- iPad Edition
- Accessibility Mode
- Calculator, Printing and Spreadsheet support

GETTING STARTED

Introduction

Respondus LockDown Browser® is a custom browser that locks down the testing environment within Blackboard Learn. When students use LockDown Browser to access an assessment, they are unable to print, copy, go to another URL, or access other applications. Students are locked into an assessment until it is submitted for grading.

LockDown Browser works with Blackboard Learn 9.x. The integration requires the installation of a Building Block on the Blackboard Learn server. The "Respondus LockDown Browser Building Block" can be downloaded from the Administrator Area of the Respondus web site. The Building Block will allow instructors to go to the Course Tools in Blackboard itself to set up a test for use with LockDown Browser.

Overview of Browser Application

Respondus LockDown Browser is a client application that is installed to a local computer. The Windows edition of the browser is based on Google's open source framework Chromium. Students do NOT need Google's Chrome browser installed; nor will this version affect a Chrome browser that's already installed.

The Mac edition of LockDown Browser is based on the same system components and settings that make up Safari, which is already installed on the computer. It does not modify an existing copy of Safari, but rather, installs a separate program that will display the custom browser when it is started. The Mac LockDown Browser uses the same security features and service packs that are currently installed for Safari. Installing LockDown Browser won't modify the current version of Safari in any way.

LockDown Browser creates a "locked" testing environment for Blackboard assessments and includes the following features:

- Assessments are displayed full-screen and cannot be minimized
- Assessments cannot be exited until submitted by users for grading
- Task switching or access to other applications is prevented
- Printing functions are disabled
- Print Screen and capturing functions are disabled
- Copying and pasting anything to and from an assessment is prohibited
- Right-click menu options are disabled (Windows); key + click options are disabled (Mac)
- Browser menu and toolbar options are disabled except Back, Forward, Refresh and Stop
- Function keys (F1-F12) are disabled
- Source code for the HTML page cannot be viewed
- URLs cannot be typed by the user
- Hundreds of screen capture, messaging, screen-sharing and network monitoring applications are blocked from running
- The browser automatically starts at the institution's login page for Blackboard

- Links in questions that point to other servers don't compromise the "locked" testing environment
- Pages from the assessment aren't cached or stored in the browser's history listing
- And many other features...

LockDown Browser is not intended to replace the browser used by faculty or students within Blackboard. LockDown Browser is only intended for use by students while taking assessments that have been prepared for use with LockDown Browser. This browser has not been tested for use in other areas of Blackboard Learn.

Respondus Monitor

Respondus Monitor™ is a companion product for LockDown Browser that enables institutions to protect the integrity of non-proctored, online exams. Students use their own computer and a webcam to record assessment sessions, all without leaving the institution's learning management system. Full details of the administrator functions for Respondus Monitor can be found in the Respondus Monitor administrator guide located in the Administrator Area of the Respondus web site.

Minimum System Requirements for LockDown Browser Client Installation

Windows*

- Windows 10, Windows 8, Windows 7, Vista
- 75 MB of permanent space on the hard drive

Mac*

- OS X 10.7 or higher
- Safari browser
- 3 MB of permanent space on the hard drive

*As supported and configured to the requirements for the Blackboard Learn platform.

ADMINISTRATOR FUNCTIONS

Login to Administrator Area

The login page for the Administrator Area of the Respondus web site is located at the Customer Login (https://www.respondus.com/campus-portal/). The User ID and Password for accessing this area is contained in the welcome email that was sent to the administrator of the license.

Once logged in, select the product link "LockDown Browser & Respondus Monitor." This page will display account information, a link for the LockDown Browser Control Panel, server profiles including download links for the Building Block, a download area for the LockDown Browser software, user guides, and other information.

Institution ID

Each institution is provided with a unique "Institution ID" which is displayed throughout the Administrator Area for Respondus LockDown Browser. The Institution ID is used to link a client installation of LockDown Browser to a particular institution.

In situations where the administrator or user is asked to enter the Institution ID, only enter the numeric portion of the Institution ID (not the name of the institution itself).

Control Panel

The Control Panel allows the administrator to create, modify or delete a "server profile" for an institution.

> **Warning: Changes to the Control Panel are institution-wide and will appear immediately to faculty and students. Use extra caution within the Control Panel area.**

Server Profiles

The server profile(s) created by the administrator of the license determines the functions and appearance of Respondus LockDown Browser. For example, one setting in the server profile specifies the login page for the institution's Blackboard server, which is then used by the browser when it is first started.

A server profile is created for each distinct learning management system that's in use at an institution. Most institutions will have only one server profile. If more than one server profile is created, such as two different learning management systems at the institution or separate production and tests systems, students must select from a list of servers each time LockDown Browser is started.

The server profile data for an institution is stored at the Respondus web site. When LockDown Browser is started, it will automatically go to the Respondus web site to obtain this information.

Server profiles are created, modified, and deleted from the Control Panel area. A server profile requires the following information:

- **Institution** - The name and ID number assigned to the institution are displayed here. Consortium licenses may have multiple institution names and IDs listed. Make sure the correct institution is selected before making changes to a server profile.
- **Server Profile Name** - Enter a name that succinctly describes the learning management system server (e.g. "Blackboard at ABC College"). *If two or more server profiles are created for an institution, students will be presented with a list of the server profile names when Respondus LockDown Browser is started. They will need to choose a server before continuing.* **Note**: The list of server profile names are sorted alphabetically where test/development servers should be named to sort lower in the list than production servers.
- **Enable Respondus Monitor for this server** – Upon acceptance of the Terms of Use, the administrator settings for Respondus Monitor become available from the main administrator page. (Note, this setting will NOT make Respondus Monitor available to

instructors and students; a different setting makes that possible. See the *Respondus Monitor Administrator Guide* for more details.)

- **Learning Management System** - Select the learning management system being used at the institution: Blackboard, Moodle, Canvas, etc.
- **Login Page for LMS as accessed by students** - Enter the URL for the login page of your institution's Blackboard server. If the login page is only available via a portal page, enter that URL instead. (The URL that is entered will be the start page for Respondus LockDown Browser.)
- **URL for actual Blackboard system, as used by Building Blocks (Include HTTP/S and port if not 80 or 443, e.g. https://lms.blackboard.com/)** – Enter the URL for the actual Blackboard server including the HTTP:// or HTTPS:// along with any non-standard port numbers and a trailing slash ("/"). *Do not include any path or parameters after the initial trailing slash.*

The following settings are optional for a server profile:

- **Time zone for Blackboard server, used for Respondus Monitor reports** – This setting, which is used for Respondus Monitor reports, allows times to appear in the correct time zone.
- **Exit Password (to allow a proctor to close the browser during quiz)** - If a password is entered here, it will allow a proctor to assist a student in closing LockDown Browser <u>during</u> an assessment. This function is generally not needed because a key goal of LockDown Browser is to force students to complete the assessment before closing the browser. Administrators should be careful about distributing this system-wide exit password to proctors because if it falls into the hands of students, it will allow them to exit the browser at will during an assessment. During an assessment, the proctor can use this feature by clicking the **(i)** button on the toolbar, selecting Proctor Options, and then entering the password. **Note:** The LockDown Browser Building Block allows instructors to specify a unique exit password for each assessment. If the instructor enters an exit password, the system-wide exit password won't work for that assessment.
- **Add to Blacklist** - Hundreds of "blacklist" applications are prevented from running concurrently with LockDown Browser, including screen-capture, internet messaging, screen-sharing, virtual desktop, remote desktop, VNC, network monitoring and other communication applications. To append to the built-in blacklist, enter the executable file name. If the application uses a different "image name" in the Windows Task Manager, enter that name instead. For Mac applications, enter the application name without the ".app" extension (e.g. MacMonitor). A comma should separate applications added to this list (e.g. ScreenWatcher.exe, VideoGrabber.exe, MacMonitor). LockDown Browser will block these applications at startup and offer to close the applications for the user.
- **Remove from Blacklist** - Hundreds applications are blocked (i.e. blacklisted) by LockDown Browser, including screen-capture, internet messaging, screen-sharing, virtual desktop, remote desktop, VNC, network monitoring and other communication applications. However, it is possible for an administrator to allow a blacklisted program to run in the background when Respondus LockDown Browser is started. This option, essentially, removes an application from the blacklist. *It's important to note that students will be unable to "switch" to such an application once the browser has started.*

It simply allows the other application to continue running. Thus, this feature is only useful for certain applications, such as screen monitoring software or video capture software, where it runs in the background. To allow a Windows application to run in the background, enter the executable file name (e.g. XYZ-Monitor.exe). If the Windows application uses a different “image name” in the Windows Task Manager, enter that name instead. For Mac applications, enter the application name without the ".app" extension (e.g. MacMonitor). A comma should separate applications added to this list (e.g. XYZ-Monitor.exe, ABC-Chat.exe, MacMonitor).

- **Remove from Blacklist (Lab Edition only) –** If you wish to remove applications from the blacklist for ONLY the "Lab Edition" of LockDown Browser, enter those below. Use the same guidelines as described above. Requires LDB version 2.0.0.00+ (Windows) or 1.0.7.10+ (OS X).
- **Hide this server from student copies of LDB** - When there multiple server profiles, students must select from a pull down list of servers each time LockDown Browser is started. This pull down list includes any profiles for test and development systems. By selecting "Yes" for this setting, the profile will not be included in the pull down list of servers displayed to the students.

Displaying Hidden Profiles

To display hidden profiles in the Respondus Administrator Area, an additional flag or setting needs to be added to the LockDown Browser installation on the client system.

For Windows computers, create a new Windows Registry key string entry, HKEY_CLASSES_ROOT\Respondus\ldbhp with "on" as the string entry.

For Mac computers, control-click or right-click on the application to bring up the context menu and select "Show Package Contents." Create a new file named **hp.txt** (plain text UTF-8 format) that contains a single word “on” and place the file in the package contents folder.

RESPONDUS LOCKDOWN BROWSER BUILDING BLOCK

The Respondus LockDown Browser Building Block can be used with Blackboard Learn release 9.x and higher.

The LockDown Browser Building Block can *only* be downloaded from the Administrator Area of the Respondus web site. Each Building Block is customized during the download process from the Administrator Area, thus it cannot be obtained from any other location. Note: The same Respondus LockDown Browser Building Block Building Block cannot be used across different Blackboard systems such as production and test/development.

Downloading the Respondus LockDown Browser Building Block

Log into the Respondus Administrator Area and then go to the LockDown Browser Control Panel.

1. Create a server profile for the Blackboard server that will use the Respondus LockDown Browser Building Block.

2. Click “Save Changes”.
3. Once the server profile is created, select the link “Download Building Block for Blackboard Learn”
4. Verify the settings that will be included in the Building Block.
5. Download the “Building Block 3.x” and save as **Respondus_LDB_BuildingBlock_x.y.z,war**, where “x.y.z” is the version of the Building Block.

Installing the Respondus LockDown Browser Building Block

As the Blackboard Administrator, log in with an account that can see the System Admin tab, and specifically, the Building Blocks section.

1. From the System Admin tab, click the **Building Blocks** link and then select **Installed Tools**.
2. Click the **Upload Building Blocks** tab and the **Install Building Block** page will open.
3. From here, click **Browse** and locate the Building Block file called **Respondus_LDB_BuildingBlock_x.y.z.war**. The path to the Building Block should appear in the field.
4. Click **Submit** to upload the .war file to Blackboard Learn.
5. From the **Installed Tools** page, find the **Respondus LockDown Browser** Building Block within the list of installed Building Blocks.
6. To enable the Respondus LockDown Browser Building Block, select **Available** from the drop-down list. When the Building Block is first made available the list of permissions required by the Building Block is displayed. This is a security feature to protect Blackboard Learn from dangerous content.
7. To make the Building Block available for all courses on the server select **Set Available** from the context menu next to the Respondus LockDown Browser name. (varies with Service Packs.)
8. Click **OK** to make the Building Block available [to courses] and allow the listed permissions. The system will display a confirmation message that the Building Block is enabled.
9. Click **OK** to return to the Installed Building Blocks page. The Building Block should now have a status of Available.

Note: If installing this Building Block on the October 2014 release of Bb Learn 9.1 (or later), a server restart is required.

Reinstalling the LockDown Browser Building Block

The installation instructions (above) can be followed to re-install the LockDown Browser Building Block. There is no need to remove the Building Block first, but it is important to follow the post installation steps described below.

Post Installation of the Respondus LockDown Browser Building Block

Important: After installing the Building Block, return to the Respondus Administrator area, go to the LockDown Browser Control Panel and select the link "After installing the Building Block - Click here to test the integration" to verify that the Building Block was installed and configured properly.

DISTRIBUTION AND INSTALLATION OF RESPONDUS LOCKDOWN BROWSER

The extent to which the Respondus LockDown Browser software is distributed and installed is largely up to the institution itself (assuming it has a campus-wide license for the software). Some institutions may limit the installation to computer labs where proctored assessments are delivered. Other institutions may distribute the software widely, making it available to all faculty and students.

Student and Lab Editions

There are two types of installers available from the Administrator Area of Respondus LockDown Browser. In Windows the "Student Edition" requires the user to have administrator rights to install, update and run the browser. This version of LockDown Browser is what's distributed to students for installation to their own computers.

The installer for the "Lab Edition" of LockDown Browser, which is for Windows-based computer labs, doesn't require users to have administrator rights in Windows to launch LockDown Browser. If installing the Lab Edition of LockDown Browser, a separate Windows account should be used on the lab computers where the Task Manager and Fast User Switching are disabled. The Task Manager and Fast User Switching can be disabled with the Windows Group Policy Editor, as detailed here:
http://windows.microsoft.com/en-US/windows7/Group-Policy-management-for-IT-pros.

Important: The "Lab Edition" of LockDown Browser should never be given to students since it would allow them to access the Task Manager and Fast User Switching during an exam. Another difference with the Lab Edition of LockDown Browser is that automatic managed updates are not enforced. This keeps the client application updated on students' computers, while allowing managers of computer labs to update the browser on their own schedule.

The Mac browser doesn't have the same "administrator" restriction that occurs with the Windows browser, but a Lab Edition of the Mac browser is still available that allows managers of computer labs to update the browser on their own schedule. See the section "LockDown Browser Lab Edition for Mac" for further details.

Finally, if you want to run the Lab Edition of Respondus LockDown Browser (Windows only) on a virtual machine, please contact Respondus Support at support.respondus.com for guidance on how to accomplish this.

Managed Installations and Updates

The LockDown Browser Lab Edition files can be installed to a shared network folder, or installed on each machine to reduce traffic.

LockDown Browser Lab Edition for Windows

For Windows, computer desktop management software (Altiris, Microsoft SMS, etc.) can be used to "push" the initial install as long as it supports creating folders, copying files, creating

desktop/start menu shortcuts, and setting registry keys. Here are the details for new installations:

First, do a manual install of LockDown Browser Lab Edition to one PC to obtain the files and registry keys that are required.

1. Push all files from Program Files (x86) > Respondus > LockDown Browser Lab, including the "locales" sub-folder.
2. A registry key string must be set with the 9-digit "Institution ID" provided to the administrator: HKEY_CLASSES_ROOT\Respondus\ldbsk
3. A registry key string must be set with the "institution specific string" that can be found by looking at the key after manually installing: HKEY_CLASSES_ROOT\LRRKFLD\startup
4. Desktop and/or Start menu shortcuts to the LockDownBrowserLab.exe file.

A silent install using InstallShield's response recording is detailed in a Respondus Support knowledge base article:

Does the LockDown Browser Lab Edition support silent or unattended installs under Windows?
http://support.respondus.com/support/index.php?/Knowledgebase/Article/View/136/

Is there a ".msi" version of the LockDown Browser Lab Edition installer?
http://support.respondus.com/support/index.php?/default_import/Knowledgebase/Article/View/158/0/

LockDown Browser Lab Edition for Mac

For Mac computers, the installer ("Install Respondus LockDown Browser xxxxxxxxx0.pkg" - where "xxxxxxxxx" is the institution ID) downloaded from the Respondus web site, can be pushed to other Mac computers for installation purposes.

LockDown Browser-Mac includes an additional option to provide some of the same functions as LockDown Browser Lab Edition for Windows. When the option is enabled, automatic managed updates are not enforced so lab managers can update Lockdown Browser-Mac in managed Mac computer labs on their schedule.

To enable the Lab Edition of LockDown Browser-Mac:

1. Log into the Respondus Campus-portal and go to "LockDown Browser installer (Lab edition)"

2. Right click on the "LockDown Browser: Lab Edition (Windows)" link and select "Copy Link" from the context menu.

3. Open a text editor and paste in the copied link.

4. Delete the beginning of the text up to and including “kc=“, leaving only the ending 32-character “institution specific string” on the first line.

5. Save the text file as “lab.txt”.

6. In LockDown Browser-Mac installed on a managed Mac computer, right click on the "LockDown Browser" icon and select "Show Package Contents".

7. Copy the "lab.txt" file into the package in the same location as the "id.txt" file.

8. Close the package

9. Start LockDown Browser-Mac and go to the "About" button in the LockDown Browser toolbar.

10. Verify the word "(lab)" appears in the version information to indicate the setting is active.

Distribution of the Setup Program

The setup program or installer for Respondus LockDown Browser must be downloaded from a unique URL for your institution. The URL that contains the setup application for your institution is available from the Administrator Area of Respondus.com. The URL is the same as the one shown below; however, the "123456789" at the end of the URL is replaced by the 9-digit Institution ID for your own institution.

http://www.respondus.com/lockdown/download.php?id=123456789

Again, the complete URL, including the Institution ID for your institution, can be found in the Administrator Area for Respondus LockDown Browser.

For Windows users, the LockDown Browser installer will be downloaded as a file named “LockDownBrowser-xxx-yyy.exe” (where "xxx-yy" is the version number). For Mac users, the LockDown Browser installer will be downloaded as a file named “Install Respondus LockDown Browser xxxxxxxxx0.pkg” where “xxxxxxxxx” is the institution ID.

For the Mac version of LockDown Browser, the installer (Install Respondus LockDown Browser xxxxxxxxx0pkg) downloaded from the Respondus web site, can be distributed as needed to Mac users.

Installation of Browser (Windows)

Follow these steps to install Respondus LockDown Browser (Windows):

1. Download and install the LockDown Browser software using a method described in the previous section “Distribution of the Setup Program.”

2. Start LockDown Browser using either the shortcut that appears on the Windows desktop or by going to Start > All Programs > Respondus > LockDown Browser 2.

Installation of Browser (Mac)

Follow these steps to install the Mac version of Respondus LockDown Browser:

1. Confirm that a supported version of Safari is installed to your computer. This is accomplished by doing the following:

   - Start Safari. (if you are unsure how to do this, click the “Finder”, select the “Applications” folder, select “Safari”)

   - Select “Safari” from the menu bar in Safari and then select “About Safari” to make sure the version meets the required version of Safari supported by Blackboard Learn.

2. Download and install the LockDown Browser software using a method described in the previous section “Distribution of the Setup Program.”

3. Start LockDown Browser by going to Finder > Applications > LockDown Browser.

Updating LockDown Browser

The Student Editions of LockDown Brower (Windows and Mac) will be automatically updated as needed during the initial startup of the browser.

To manually update to the latest version of the Respondus LockDown Browser, start the browser, click the “Information” (**i**) button (LockDown Browser – Windows) or the “About” button (LockDown Browser – Mac) on the toolbar, then the "Check for Newer Version" button. If an update is available, information about the update and a "Get Update" button will be displayed (unless administrator access isn't available on a computer). Click the button, wait for the download to complete, and then exit the browser to complete the update.

Administrator note: If access to Respondus servers (respondus.com and respondus2.com) is blocked by a firewall, the “Check for Newer Version” feature will display an error message.

Issues with Firewalls, Content Filters and Proxy Servers

Firewalls, content filters, proxy servers and security software with similar functions can interfere with the installations, updates or operation of Respondus LockDown Browser. Problems can be related to other applications that are running on the client computer or on the institution gateway servers, or both.

If the client computer allows full Internet access to the "LockDown Browser" application, and if the gateway servers allow port 80 HTTP and port 443 HTTPS access to www.respondus.com and www.respondus2.com, then most problems can be avoided.

<u>”Installation” Issues</u>

The standard setup program or installer for LockDown Browser is delivered from "www.respondus7.com" and "www.respondus.com", so HTTP access to these sites is required unless the installer is hosted on an institution's local server.

”Updating” Issues

To use the "Check for Newer Version" feature in LockDown Browser (available from the “i” button or “About” button on the toolbar), the computer must be able to connect to all domains on *.respondus.com on standard ports.

”Running” Issues

The Respondus LockDown Browser application ("LockDownBrowser.exe" for Windows, "LockDown Browser" for Mac) must be granted network access for any firewall, proxy or filtering applications running on the client computer. LockDown Browser blocks application switching, so changes must be applied to the computer before the browser is started. In fact, any "allow access?" popups that appear while LockDown Browser is running will be hidden underneath the browser so there is no way to answer yes or OK.

The browser must make a connection on standard ports to either "www.respondus.com" or "www.respondus2.com" to obtain the server settings for the institution.

LockDown Browser required domains

1. Retrieval of the LockDown Browser server profiles on the Respondus Administrator Area:

respondus2.com
respondus.com

2. Download of the LockDown Browser Student Edition full installer:

respondus7.com
respondus.com

3. Check for updates and apply any updates for LockDown Browser Student Edition:

respondus.com

As the Respondus servers are "in the cloud", the IP addresses are dynamically assigned and subject to change without notice. It is highly recommend using URLs or domains resolved through DNS whenever possible in any firewall, router or similar security software settings.

ADDITIONAL INFORMATION FOR INSTRUCTORS

Instructor and student quick start guides for Respondus LockDown Browser and Respondus Monitor are available from http://www.respondus.com/products/lockdown-browser/guides.shtml. These guides are the easiest way to get instructors ready to use LockDown Browser. You may also want to distribute the supplemental information below, depending on the needs of instructors and how LockDown Browser is being used at your institution.

Background Information

Respondus LockDown Browser is a client application available for Windows, Mac or iPads. The Windows edition of the browser is based on Google's "Chromium" engine. Students do NOT need Google's Chrome browser installed; nor will this version affect a Chrome browser that's already installed.

The Mac edition of LockDown Browser is based on the same system components and settings that make up Safari, which is already installed on the computer. It does not modify an existing copy of Safari, but rather, installs a separate program that will display the custom browser when it is started. The Mac LockDown Browser uses the same security features and service packs that are currently installed for Safari. Installing LockDown Browser won't modify the current version of or Safari in any way.

LockDown Browser is also available for the iPad. See the section below "iPad Edition of LockDown Browser" for further details.

LockDown Browser is not intended to replace the browser used by faculty or students within Blackboard. LockDown Browser is only intended for use by students taking assessments that have been set up to use LockDown Browser.

Determining if the LockDown Browser Settings are Set Correctly

To confirm that an assessment is properly set to require students to use LockDown Browser, open a standard web browser, log into Blackboard using a student account, and attempt to start the assessment. You should be unable to start the assessment if everything is set correctly.

Next, start LockDown Browser, log into Blackboard using a student account, and then start the assessment that requires LockDown Browser. If everything is set correctly, you should be able to start the assessment with LockDown Browser.

Note: If you log into Blackboard as a student and access an assessment with LockDown Browser, you must "Finish" the assessment before the browser will let you exit.

Additional Tips and Suggestions

Make sure students know, well in advance, that they must use Respondus LockDown Browser to take an online exam. This is particularly important if students are required to install LockDown Browser to their own computer. It's recommended that you create a "practice exam" that requires the use of LockDown Browser.

It's a good practice for instructors to preview the exam using LockDown Browser. The best approach is to log in as a student since instructor logins have different access rights. Previewing an exam is an especially good idea if a test password is being used.

Once a Blackboard assessment is started with LockDown Browser, the exam will appear in a full-screen window and all other applications and links are locked down.

LockDown Browser will maintain the "locked" testing environment even if a question contains a link to another web page (which opens another, locked browser window). However, all links that may appear on the new web page will be blocked, so be sure the content that students must see is available from the initial, linked page.

INSTRUCTOR ADVANCED SETTINGS

Instructors manage the settings for LockDown Browser from the "LockDown Browser Dashboard" located within the Tools area of Blackboard Learn. The LockDown Browser Dashboard has several advanced settings for the instructor.

Lock Students into Browser

The first option can be selected to prevent students from exiting LockDown Browser before an exam is submitted for grading. If this setting is NOT selected, students can exit the browser during an exam, but will be prompted to enter a reason for exiting the exam early. The student's response is available to the instructor from the LockDown Browser Dashboard.

If the setting "Lock students into the browser..." is selected, an optional password can be entered to enable a proctor to close the browser during an exam.

We don't recommend selecting this setting outside of a proctored environment. If selected, a student will be unable to exit the browser if their Internet connection fails or there is an emergency.

iPad Edition of LockDown Browser

The setting to allow students to use the iPad Edition of LockDown Browser is explained in this Knowledgebase article.

Can an iPad be used with LockDown Browser?
http://support.respondus.com/support/index.php?/Knowledgebase/Article/View/186/0/

Accessibility Mode for LockDown Browser

The accessibility mode is intended for students with disabilities. The use of this setting is explained in the following Knowledgebase article.

Is LockDown Browser accessible to those with disabilities?
http://support.respondus.com/support/index.php?/Knowledgebase/Article/View/187/0/

Enable Calculator on the toolbar

Select the "Enable Calculator..." setting to make a standard or scientific calculator available to students from the toolbar in LockDown Browser.

Enable Printing on the toolbar

Select the "Enable Printing..." setting to make a print button available to students from the toolbar in LockDown Browser.

Spreadsheet support in LockDown Browser

This Knowledgebase article explains how spreadsheets can be used in LockDown Browser.

Can spreadsheets be used with LockDown Browser?
http://support.respondus.com/support/index.php?/Knowledgebase/Article/View/233/19/