# Contents

Getting Started .......................................................................................................................... 2  
   Overview of Browser Application .......................................................................................... 2  
   Respondus Monitor ............................................................................................................... 3  
   Minimum System Requirements for LockDown Browser Client Installation ....................... 3  
Administrator Functions ........................................................................................................ 3  
   Login to Administrator Area ............................................................................................... 3  
   Institution ID ...................................................................................................................... 3  
   Control Panel ...................................................................................................................... 4  
   Server Profiles .................................................................................................................... 4  
   Displaying Hidden Profiles ................................................................................................. 6  
Respondus LockDown Browser External Learning Tool .......................................................... 6  
   Configuring the LockDown Browser Dashboard (External Learning Tool) ......................... 6  
   Configuring the Brightspace Server for LockDown Browser ............................................. 10  
   Final Configuration and Integration Test ........................................................................... 14  
Distribution and Installation of Respondus LockDown Browser .......................................... 16  
   Student and Lab Editions .................................................................................................... 16  
   Managed Installations and Updates .................................................................................... 17  
   Distribution of the Setup Program ...................................................................................... 18  
   Installation of LockDown Browser ...................................................................................... 18  
   LockDown Browser for Windows ....................................................................................... 18  
   LockDown Browser for Mac ............................................................................................... 19  
   Updating LockDown Browser ............................................................................................. 19  
   Issues with Firewalls, Content Filters and Proxy Servers ................................................... 19  
Additional Information for Instructors .................................................................................. 21  
   Background information ..................................................................................................... 21  
   Determining if the LockDown Browser Settings Are Set Correctly .................................... 21  
   Additional Tips and Suggestions ......................................................................................... 21  
Instructor Advanced Settings ................................................................................................. 22  
   Lock Students into Browser ............................................................................................... 22  
   iPad Edition of LockDown Browser ................................................................................... 22  
   Calculator, Printing and Spreadsheet support ..................................................................... 23
GETTING STARTED

Introduction
Respondus LockDown Browser® is a custom browser that locks down the quizzing environment within D2L Brightspace. 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 D2L Brightspace. The integration requires the installation of a External Learning Tool on the D2L Brightspace server. The External Learning Tool will allow instructors to go to the Course Tools in D2L Brightspace itself to set up a quiz for use with LockDown Browser.

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

LockDown Browser creates a “locked” quizzing environment for D2L Brightspace assessments and includes the following features:

1. Assessments are displayed full-screen and cannot be minimized
2. Assessments cannot be exited until submitted by users for grading
3. Task switching or access to other applications is prevented
4. Printing functions are disabled
5. Print Screen and capturing functions are disabled
6. Copying and pasting anything to and from an assessment is prohibited
7. Right-click menu options are disabled (Windows); key + click options are disabled (Mac)
8. Browser menu and toolbar options are disabled except Back, Forward, Refresh and Stop
9. Function keys (F1-F12) are disabled
10. Source code for the HTML page cannot be viewed
11. URLs cannot be typed by the user
12. Hundreds of screen capture, messaging, screen-sharing and network monitoring applications are blocked from running
13. The browser automatically starts at the institution’s login page for D2L Brightspace
14. Links in questions that point to other servers don’t compromise the “locked” quizzing environment
15. Pages from the assessment aren’t cached or stored in the browser’s history listing
16. And many other features...

LockDown Browser is not intended to replace the browser used by faculty or students within D2L Brightspace. 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 D2L Brightspace.
**Respondus Monitor**

Respondus Monitor™ © is a companion product for LockDown Browser for higher education institutions 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*
1. Windows 10, Windows 8, Windows 7
2. 75 MB of permanent space on the hard drive

Mac*
1. MacOS 10.12 to 10.15
2. 120 MB of permanent space on the hard drive

The most up-to-date system requirements will be listed in "LockDown Browser System Requirements" at [https://www.respondus.com/products/lockdown-browser/requirements.shtml](https://www.respondus.com/products/lockdown-browser/requirements.shtml)

*As supported and configured to the requirements for the D2L Brightspace platform. The client browser may continue to run in older operating systems that have reached “end-of-life” but students may encounter unexpected results.

---

**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/](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 External Learning Tool, 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 an 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 profiles in 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 license administrator 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 D2L Brightspace 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. A separate profile is required for each system including production systems and test/development systems.

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.
- **Server Profile Name** - Enter a name that succinctly describes the learning management system server (e.g. “D2L Brightspace 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 is sorted alphabetically where test/development servers should be named to sort lower in the list than production servers. (Also, see the sections “Hide this server from LDB (student and lab editions):” and “Displaying Hidden Profiles”.)
- **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: D2L Brightspace, Moodle, Canvas, Blackboard, etc.
- **Login Page for LMS as accessed by students** - Enter the URL for the start page or login page of your institution’s D2L Brightspace 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 D2L Brightspace system, as used by External Learning Tool (Include HTTPS, e.g. https://lms.D2L.Brightspace.com/)** – Enter the URL for the actual D2L Brightspace server including the HTTPS:// 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 D2L Brightspace server** – This setting, which is used for Respondus Monitor reports and Early Exit Review reports, allows timestamps 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 during 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 Exit, and then entering the password. **Note:** The LockDown Browser External Learning Tool 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 Blocklist** - Hundreds of 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 blocklist, 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 Blocklist** - Hundreds of applications are blocked 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 blocked program to run in the background when LockDown Browser is started. This option, essentially, removes an application from the blocklist. *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 Blocklist (Lab Edition only)** – If you wish to remove applications from the blocklist for ONLY the "Lab Edition" of LockDown Browser, enter those below. Use the same guidelines as described above.

- **Hide this server from LDB (student and lab editions)** - When there are 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. Note: Do not apply this setting when there is only one profile.

**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\Respondus2\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 EXTERNAL LEARNING TOOL**

The Respondus LockDown Browser integration requires the administrator to perform the following steps:

- Configuring the LockDown Browser Dashboard External Learning Tool
- Configuring the Brightspace server
- Setting the Instructor Roles and Permissions
- Performing an Integration Test

Each of these steps are outlined below.

**Configuring the LockDown Browser Dashboard (External Learning Tool)**

LockDown Browser uses the “External Learning Tools” functionality in Brightspace for integration purposes. Follow these steps:

1. Login to the Administrator Area of Respondus.com, select the “Respondus LockDown Browser” product, and go to the Control Panel.
2. Locate the Server Profile that matches your Brightspace server. Then select “Download settings for D2L External Tool”. Download and save the text document for the following steps.

3. Login as an administrator to the Brightspace server, locate the Admin Tools menu, and select “External Learning Tools”.

4. Create a “New Link” with the title “LockDown Browser Dashboard” and enter the URL value from the settings file obtained in step 2 above.

5. Select the “Link key/secret” option. Use the information contained in the settings file to enter the Key and Secret. Click Save.
6. Go to the Custom Parameters section and click “Add custom parameters.” Enter “profile_name” for the Name. For the Value, enter the exact value text contained in the settings file.

7. In the Security Settings section, select “Use link security settings”. Then select all checkboxes except for “Send user email to the tool provider” as this value is not required.

8. Select the “Add Org Units” button and make it available in “Every Course Offering under the Organization”. This is achieved by selecting the desired Organization, then selecting “All Descendants of Type”, followed by “Course Offering” in the drop down menu. Next, click “Insert” to save your added org units.

10. Lastly, determine the “linkId” for the External Learning Tool that was just created. This is accomplished by hovering the mouse over the “LockDown Browser Dashboard” link in the list of External Learning Tools (see screenshot below) ...

... and then viewing the “linkId” value that appears within the URL that is displayed at the bottom of the browser window (see screenshot below):
An alternative method to obtaining the “linkId” value is to select the LockDown Browser Dashboard tool and view the URL from the browser:

![LinkId Value Example](image)

The “linkId” value will be used in a Config Variable Browser setting in the next section.

**Configuring the Brightspace Server for LockDown Browser**

The Respondus LockDown Browser integration requires a few Config Variable Browser settings to be enabled.

1. Login to Brightspace as the System Administrator
2. Access the Admin Tools and navigate to Config Variable Browser → All Variables → 3rdParty → Respondus
3. Click on the variable “HasLockDownBrowser”. Select “Add Value”, enter the Org Unit, and save it.
4. Select the “LockDownBrowserDownloadURL” variable. Click “Add Value”, select the Org Unit and enter the URL as explained below. Save this new value.

The URL entered for "LockDownBrowserDownloadURL" should match the page where instructors and students can download the setup program for the Respondus LockDown Browser client software. (The URL for your institution is provided in the Administrator Area of the Respondus web site.) If a student attempts to use a regular browser to access an assessment that requires Respondus LockDown Browser, a warning message will be displayed along with the link for downloading the LockDown Browser software.

An entry is required for this URL field, so if students aren't permitted to install the LockDown Browser themselves (i.e. it is only used on machines set up by IT staff), then this URL should be set to an internal page that describes the computer lab locations where Respondus LockDown Browser is available (or offer some other explanation).
The download URL will look similar to what appears below, but **BE SURE** to replace the 9-digit ID at the end of the URL with the “Institution ID” that has been provided for your institution:

https://download.respondus.com/lockdown/download.php?ID=123456789

Again, be sure to replace the 9-digit ID with the “Institution ID” provided for your institution.

5. Select the “DashboardLTIlinkId” variable. Click “Add Value” and enter the Org Unit with the “linkId” value for the newly created External Learning Tool noted in the previous section. (In the example above, the linkId value is 2.)

This will place the LockDown Browser Dashboard in the Brightspace Quizzing Tool.

6. **Brightspace 10.5.1 and higher only** supports “auto-launch” for LockDown Browser. This means a student must login to Brightspace using a standard browser (Firefox, Chrome, Internet Explorer, Safari) and have LockDown Browser automatically launched when the exam requires it. “Auto-launch” must be enabled by selecting the “SecretKeyIndex” variable and entering the value of “bm”.

When a quiz requires LockDown Browser, a student will be presented with the following:

The first link will enable a student to install LockDown Browser to the computer. If the computer already has LockDown Browser installed, the user simply clicks “Launch LockDown Browser”.
Instructor Roles and Permissions for IMS Configuration

Instructors using the LockDown Browser Dashboard require additional permissions in the IMS Configuration setting. Follow these steps to ensure all instructor roles have the associated IMS roles:

1. Login as an administrator to the Brightspace server, locate the Admin Tools menu, and select “IMS Configuration”.

2. The default Instructor role requires only the instructor permission checked.

3. If a custom instructor role is defined on your server, ensure that this role has the same permissions checked.

The instructor roles including custom instructor roles also require Organization and Course Offering permissions. Follow these steps to ensure the permissions are set correctly:

1. Login as an administrator to the Brightspace server, locate the Admin Tools menu, and select “Roles and Permissions”. Select the “Instructor” role, then select “Users” from the “Filter by Tool” pull-down menu, and click **Apply Filter**.

2. Check the “Organization” and “Course Offering” checkboxes for “View User Enrollments”.

3. Check the “Organization” and “Course Offering” checkboxes for “Search for ‘Student’”. Click **Save**.

4. Next select the “Instructor” role and select filter by “External Learning Tools”. Ensure that the instructor role has permission to “Launch External Learning Tool Links” in the course.
5. Next select the “Instructor” role and select filter by “User Information Privacy”. Ensure that the instructor role has permission to see First Names, Last Names and Usernames in the course.

6. Next select the “Instructor” role and select filter by “Course Management Console”. Ensure that the instructor role has permission to “See Course Info” at the Course Offering level.

7. Next select the “Instructor” role and select filter by “Quizzes”. Ensure that the instructor role has permission to add/remove questions from quizzes, create quizzes, delete quizzes, edit quiz properties, and preview quizzes.
8. Next select the “Instructor” role and select filter by “Survey”. Ensure that the instructor role has permission to add/remove questions from surveys, create surveys, delete surveys, Edit survey properties, and preview surveys.

9. Next select the “Instructor” role and filter by “Self Assessments”. Ensure that the instructor role has permission to add/remove questions from self-assessments, create self-assessments, delete self-assessments, Edit self-assessment properties, and preview self-assessments.

10. The following Config Variable needs to be enabled by the D2L Administrator:

   **d2l.Tools.ClassList.DisplayUsername**

   1. Login to Brightspace as the System Administrator
   2. Access the Admin Tools and navigate to Config Variable Browser → All Variables → Tools → Classlist
   3. Click on the variable “DisplayUsername”. Click “Add Value”, enter the Org Unit, select “on” and save it.

   **Note:** the username does not need to be displayed to students -- that is controlled by a separate permission in Roles and Permissions.

11. Double-check that the Respondus tool is currently enabled in Admin Tools->Managed Extensibility. There should be a "green check" next to the "Respondus" tool.

![](image)

12. Lastly navigate to admin tools > organizational tools and ensure that both the Self-Assessments and Survey tools are activated.

<table>
<thead>
<tr>
<th>Self Assessments</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>![Checkmark]</td>
</tr>
</tbody>
</table>

| Survey          | ![Checkmark] |

**Final Configuration and Integration Test**
The final step of the configuration process is to activate and test the External Learning Tool configuration. Follow these steps:

1. Login to the Administrator Area of Respondus.com, select the “LockDown Browser & Respondus Monitor” product, and go to the Control Panel.
2. Locate the Server Profile for your Brightspace server. Then select “Click here to activate and test the integration”.

3. You will be presented with the Brightspace server login page where you must authenticate with your D2L admin account.

This will activate your Respondus Monitor integration and display the status of the integration test.

Note: Until the final configuration step is completed, instructors will receive an error if they try to access the “Video Review” area of the LockDown Browser Dashboard.
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. 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 for students to use on personal computer systems.

Student and Lab Editions
There are two types of installers available from the Administrator Area of Respondus LockDown Browser. For Windows, the “Student Edition” requires the user to have local administrator rights to install, update and run the browser. With Mac, the user needs to have local administrator rights to install and update the browser but can run the browser under a non-administrator account. These are the editions of LockDown Browser distributed to students for installation to their own computers.

For Windows, the “Lab Edition” does not require students to have local administrator rights to run the browser, the same as Macs.

An additional feature of the Lab Edition (Windows and Macs) 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.

Please note that all Lab Edition installations have a one-year expiration from the release date of the version. After 365 days from the release date, students will see a warning even though they will still be able to use the browser. The only option to remove the warning is to update to the latest release.

LockDown Browser 2.0 Lab Edition for Windows pre-installation requirements

The LockDown Browser Lab Edition for Windows requires an account with administrator access to install and update the browser. However, it does not require such access to run. Access to the Task Manager and Fast User Switching must be disabled for the Browser so that it is operating in a locked down manner. This can be disabled using Windows Group Policy Manager, Windows Registry, or Windows Group Policy Objects (GPO). Although these are acceptable options, it is easier to manage via GPO as it controls the account at the user level.

A separate Windows user account should be used on lab computers where the Task Manager and User Switching are disabled. This will allow students to continue to use a regular Windows user account on the managed computers when not using LockDown Browser Lab Edition.

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, potentially compromising the academic integrity of exams.

Finally, if you want to run the Lab Edition of Respondus LockDown Browser (Windows only) on a virtual machine, please have the institution’s designated Respondus License Administrator or
Local Support Contacts, contact Respondus Support at support.respondus.com for guidance on how to accomplish this.

**LockDown Browser 2.0 Lab Edition for Mac pre-installation requirements**

For Macs, there are no additional user account requirements to run the browser.

**Managed Installations and Updates**

**LockDown Browser Lab Edition for Windows**

For Windows, computer desktop management systems (Microsoft SCCM, Altiris, Dell KACE, etc.) can run silent installs across all managed lab computers.

For assistance with silent installation options, please [open a ticket](https://support.respondus.com) with Respondus Technical Support.

As an alternative, desktop management systems can be used to "push out" an existing installation if it supports creating folders, copying files, creating desktop/start menu shortcuts, and setting registry keys. For new installations:

1. Download the LockDown Browser 2.0 Lab Edition (Windows) installer from the Respondus Administrator Area.
2. Do a manual install of LockDown Browser Lab Edition to one PC to obtain the files and registry keys that are required.
3. Start LockDown Browser Lab Edition 2.0 at least one time to verify the installation.
4. Push all files from Program Files (x86) > Respondus > LockDown Browser Lab, including the "locales" sub-folder.
5. A registry key string must be set with the 9-digit “Institution ID” provided to the administrator: HKEY_CLASSES_ROOT\Respondus2\ldbsk
6. 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
7. Registry keys can optionally be set with the version information by looking at the keys after manually installing: HKEY_CLASSES_ROOT\Respondus2\ldbver and HKEY_CLASSES_ROOT\Respondus2\dbvernum
8. Desktop and/or Start menu shortcuts to the LockDownBrowserLab.exe file.

**LockDown Browser Lab Edition for Mac**

For Macs, computer desktop management software (Apple Remote Desktop, JAMF, Cisco Meraki, Filewave, LanDesk, etc.) can be used to "push" an existing installation to other Macs:

1. Download the LockDown Browser 2.0 Lab Edition (Mac) installer from the Respondus Administrator Area.
2. Install LockDown Browser 2.0 Lab Edition (Mac) on at least one Mac.
3. Start LockDown Browser 2.0 Lab Edition (Mac) and then close the browser, to verify the installation.
4. Copy the LockDown Browser app in Finder->Applications to other Macs in the same Finder->Applications folder.

Note: Do not use desktop management systems to run the LockDown Browser 2.0 Lab Edition (Mac) installer. Instead, install LockDown Browser-Mac at least one time then copy/push/deploy the installed LockDown Browser app to other Macs.

A silent install for LockDown Browser 2.0 Student Edition (Mac only) is detailed in a Respondus Support Knowledge Base article:

**Does the LockDown Browser-Mac support silent or unattended installs on Macs?**

**Distribution of the Setup Program**
The 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 at [https://www.respondus.com/campus-portal](https://www.respondus.com/campus-portal)

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.

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

For Windows users, the LockDown Browser installer will download as a file named “LockDownBrowser-2-0-x-yy.exe” (where "2-0-x-yy" is the version number).

For the Mac version of LockDown Browser, the installer downloads as zip file named "InstallLD Package64c-2-0-x-yy.zip" (where "2-0-x-yy" is the version number) and will expand to "Install Respondus LockDown Browser (x64c) xxxxxxxxx0.pkg" where "xxxxxxxxx" is the institution ID.

Both installers can be distributed to students through other means such as network folders or USB flash drives. However, it is highly recommended students always download the installer from the institution's unique web address URL on the Respondus site.

**Installation of LockDown Browser**

*LockDown Browser for Windows*

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

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

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

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

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

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

For students, there is a helpful article including video tutorials:

**How do I install 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 (Windows) or "Check for Update" (Mac) 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.

Note: If access to Respondus servers (respondus.com, respondus2.com, amazonaws.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](http://www.respondus.com), [www.respondus2.com](http://www.respondus2.com) and amazonaws.com, then most problems can be avoided.

“Installation” Issues

The standard setup program or installer for LockDown Browser is delivered by a page from [www.respondus.com](http://www.respondus.com), so HTTP access to these sites is required unless the installer is hosted on an institution's local server.

Note: The administrator must not provide students with any secondary links from the primary LockDown Browser download site at “https://download.respondus.com/lockdown/download.php?id=xxxxxxxxxx”
“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 and *.respondus2.com and *.amazonaws.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 "*.respondus.com", "*.respondus2.com" or "*.amazonaws.com" to obtain the server settings for the institution.

---

**LockDown Browser required domains**

Along with the D2L Brightspace server domain, LockDown Browser need access to the following domains:

**Primary Domains:**
- amazonaws.com
- respondus.com
- respondus2.com

**Mirror Domains:**
- respondus7.com
- respondus4.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 [https://www.respondus.com/products/lockdown-browser(guides.shtml](https://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 and Mac 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.

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 D2L Brightspace. 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 D2L Brightspace using a valid student account enrolled in the course, and attempt to start the assessment. If everything is set correctly, you should be able to start the assessment with LockDown Browser.

*Note:* If you log into D2L Brightspace 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 a direct log in with a valid student account in the course since instructor logins have different access rights. Previewing a quiz with a valid student account is an especially good idea if a quiz password is being used.

Once a D2L Brightspace 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” quizzing 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 D2L Brightspace. The LockDown Browser Dashboard has several advanced settings for the instructor.

![Advanced Settings](image)

**Lock Students into Browser**

The first option can be selected to prevent students from exiting LockDown Browser before a quiz is submitted for grading. If this setting is NOT selected, students can exit the browser during a quiz, 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 a quiz.

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 Knowledge Base article.

Can an iPad be used with LockDown Browser?  
[https://support.respondus.com/support/index.php?/Knowledgebase/Article/View/186/0/](https://support.respondus.com/support/index.php?/Knowledgebase/Article/View/186/0/)
Calculator, Printing and Spreadsheet support

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 Knowledge Base article explains how spreadsheets can be used in LockDown Browser.

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