LOCKDOWN BROWSER GUIDE FOR SCHOOL-MANAGED DEVICE

Please share this guide with your System Administrator or IT staff before the exam date

EXAM URL FOR LOCKDOWN BROWSER PRACTICE EXAM AND EXAM

https://asoexams.edu.au

EXAM SUPPORT

asi@asi.edu.au
026125 6228
7 AM - 6 PM AEST
Monday to Friday

JUNIOR SCIENCE OLYMPIAD EXAM DATES

Years 9 & 10: Wednesday 11 June 2025
Years 7 & 8: Friday 13 June 2025

AUSTRALIAN SCIENCE OLYMPIAD EXAM DATES

PHYSICS (pen and paper): Monday 4 August 2025
BIOLOGY: Tuesday 5 August 2025
EES: Wednesday 6 August 2025
CHEMISTRY: Thursday7 August 2025

Contents

LOCKDOWN BROWSER 2

Introduction 2

Overview of Browser Application 2

How does LockDown Browser work? 2

MINIMUM SYSTEM REQUIREMENTS FOR LOCKDOWN BROWSER INSTALLATION 3

ADDITIONAL MEASURES ON TOP OF LOCKDOWN BROWSER 4

DISTRIBUTION AND INSTALLATION OF LOCKDOWN BROWSER – for Windows Devices 6

LockDown Browser for Managed Computers (Windows) pre-installation requirements 6

Installer for LockDown Browser for Managed Computers (Windows) 6

More Information Concerning the MSI Install Process 7

MSI instructions for institutions using Microsoft Intune 8

Known Bug When Launching LockDown Browser in Google Chrome in Windows 9

DISTRIBUTION AND INSTALLATION OF LOCKDOWN BROWSER – for Mac Devices 11

DISTRIBUTION AND INSTALLATION OF LOCKDOWN BROWSER – for Chromebook Devices ... 12

Manual Installation 12

Automatically Installed 13

Domain and URL Pattern Filtering 14

Removal of the older Chromebook App 14

DETERMINING IF THE LOCKDOWN BROWSER SETTINGS ARE SET CORRECTLY (For All System Operations) 15

UPDATING LOCKDOWN BROWSER 16

ISSUES WITH FIREWALLS, CONTENT FILTERS AND PROXY SERVERS 17

LOCKDOWN BROWSER

Introduction

Respondus LockDown Browser® is a custom browser that locks down the quizzing environment within Moodle, where all Science Olympiad exams (Junior Science Olympiad exam and discipline specific exams) are hosted. 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.

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 opensource Chromium framework. Students do **NOT** need Google's Chrome browser installed; nor will this version affect a Chrome browser that's already installed.

How does LockDown Browser work?

LockDown Browser creates a "locked" quizzing environment for Moodle assessments and includes the following features:

1. Assessments are displayed full-screen and cannot be minimised.
2. Assessments cannot be exited until submitted by users for grading.
3. Task switching or access to other applications is prevented.
4. Printing and screen capture functions are disabled.
5. Copying and pasting anything to and from an assessment is prohibited.
6. Right-click menu options, function keys, keyboard shortcuts and task switching are disabled.
7. Browser menu and toolbar options are disabled except Back, Forward, Refresh and Stop.
8. Prevents access to other applications including messaging, screen-sharing, virtual machines and remote desktops.
9. URLs cannot be typed by the user.
10. An assessment cannot be exited until the student submits it for grading.
11. Assessments that are set up for use with LockDown Browser cannot be accessed with other browsers.
12. Pages from the assessment aren't cached or stored in the browser's history listing.

MINIMUM SYSTEM REQUIREMENTS FOR LOCKDOWN BROWSER INSTALLATION

Operating System	Windows: 11 and 10*	* Includes x86 32 and 64 bit processors, ARM 64 bit processors using x86 emulation including CoPilot+PC devices. * Windows 10/11 "S mode" is not a compatible operating system, nor can LockDown Browser be obtained via the Windows App Store. At present, support for Windows 10/11 "S Mode" isn't on the roadmap for LockDown Browser. * Windows 10/11 "SE" is currently not a compatible operating system for LockDown Browser.
	Mac	MacOS 11 to 15.0+
	Chromebook	LockDown Browser for Chromebook minimally requires the version of ChromeOS that Google makes available via their Long Term Support (LTS) channel. Respondus recommends keeping your Chromebook updated to the most recent version that is available via Google's ChromeOS "Stable" channel.
Memory	Windows	75 MB permanent space on the hard drive
	Mac	120 MB permanent space on the hard drive

ADDITIONAL MEASURES ON TOP OF LOCKDOWN BROWSER

HELP US TO MAINTAIN OUR EXAM INTEGRITY
With AI websites easily accessible these days, **we are looking for ways to minimise any collusion/cheating during exams.** Please block these websites so they are not accessible during the exam period: 1. ChatGPT 4.0 https://chatgpt.com/ 2. Copilot https://copilot.microsoft.com/ 3. Gemini https://gemini.google.com/ 4. AnonChatGPT https://anonchatgpt.com/ 5. Chatsonic https://writesonic.com/chat 6. Ask AI https://iask.ai/ We understand that not all schools have adequate IT support to complete these tasks. If you cannot block these sites your students will still be able to access the exam.

TECHNOLOGY PROFILE	
Exam URL	https://asoexams.edu.au Please ensure **the exam URL and noreply@asolearn.net.au** are not blocked by your school's firewall. ***Account confirmation email will be sent to students through this email address.***
Hardware	Laptop, Desktop PC, Chromebook
Operating system	Mac OS X MS Windows XP, Vista, 7, 8 and 10 Chrome OS 38+

Web browsers	In order of preference: 1. Google Chrome 28+ (XP, Vista, Windows 7, 8 and 10, OSX, Chrome OS) 2. Firefox 20+ (XP, Vista, Windows 7, 8 and 10, OSX) 3. Internet Explorer 10+ (Windows 7, 8 and 10) 4. Internet Explorer 9 (Vista, Windows 7) 5. Safari 6+ (OSX) **Please note:** Internet Explorer 8 is not supported.
Bandwidth	512 KB bandwidth for up to 20 users 2 MB bandwidth for up 100 users 5 MB bandwidth for more than 100 users
Settings	A minimum screen resolution of 1024 x 768. During online exams, other traffic should be kept to a minimum at the school. Pre-cache digital content ability is supported and preferred.

DISTRIBUTION AND INSTALLATION OF LOCKDOWN BROWSER – for Windows Devices

LockDown Browser for Managed Computers enables LockDown Browser to be run on computers without administrator rights. It also bypasses the auto-update feature, allowing managers of computer labs to update the browser on their own schedule.

LockDown Browser for Managed Computers (Windows) pre-installation requirements

1. LockDown Browser for Managed Computers (Windows) requires an account with administrator access to install and update the browser. However, it does not require such access to run.
2. 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 for Managed Computers.

Please note that all installations of LockDown Browser for Managed Computers 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.

Important: LockDown Browser for Managed Computers **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.

Installer for LockDown Browser for Managed Computers (Windows)

IMPORTANT: If the students have administrator access to the devices, please use the students- managed device' installer instead, not the MSI installer mentioned in this section. Please follow the students-managed device guide.

For Windows, computer desktop management systems (Microsoft SCCM, Altiris, Dell KACE, etc.) can use the MSI installer to install LockDown Browser on all managed lab computers.

LockDown Browser Windows URL: https://asi.sharefile.com/d-se40a410bd31044c9982cc986da955f2d

More Information Concerning the MSI Install Process

- **The MSI installer can't be run from within the zip file by clicking on it and viewing the contents.** All files must be extracted to a folder first. If you try to run the MSI from within the zip file, you will likely see this error occur:

- For the LockDown Browser for Managed Computers MSI installer, the zip file contains the MSI file, id.txt, and other files. This is needed because of the "custom action" that reads id.txt to set the institution ID and license key. Unzip the file and then right click the MSI to install. The MSI installer uses the custom action (VBScript) to set the values RSP_ID and RSP_KEY for the registry keys HKCR
  > Respondus2 > ldbsk and HKCR > LRRKFLD2. If this custom action is disabled by antivirus software, you must set these values to match the contents of id.txt lines 1 and 2.

- The MSI installer does not support installing the exact same version twice. Windows will display an error that it is already installed. If you need to repair/replace a version with itself, then uninstall and reinstall.

- When pushing out the MSI package to multiple lab computers, **you should first perform an uninstall of any existing version of LockDown Browser for Managed Computers**. Once the uninstall of the old version is performed, you can then do a silent install of the MSI package. If you do not perform this uninstall first, the "Add/Remove Programs" display in Windows will show two installs of LockDown Browser.

MSI instructions for institutions using Microsoft Intune

Note: we provide the below instructions as a courtesy to our customers, but **we cannot provide support for MS Intune beyond what is specified below**. If problems persist, please contact Microsoft for assistance.

The existing LockDown Browser MSI installers are fully compatible with Intune for normal Windows versions. They just need to be placed into Intunewin packages using Microsoft's content prep tool and then deployed as a Win32 application.

Microsoft's content prep tool is available here: https://github.com/microsoft/Microsoft-Win32-Content- Prep-Tool

Installation Steps:

1. Download the MSI install
2. Unzip into a folder like c: > intune > 20903 (for LockDown Browser version 2.0.9.03)
3. Run the content prep tool
4. Add the new or updated app into intune as a win32 app, using (or updating) the MSI detection rule

Content prep tool answers example:

c:\intune\IntuneWinAppUtil.exe

c:\intune\20903

Respondus LockDown Browser - Lab

Edition.msi c:\intune

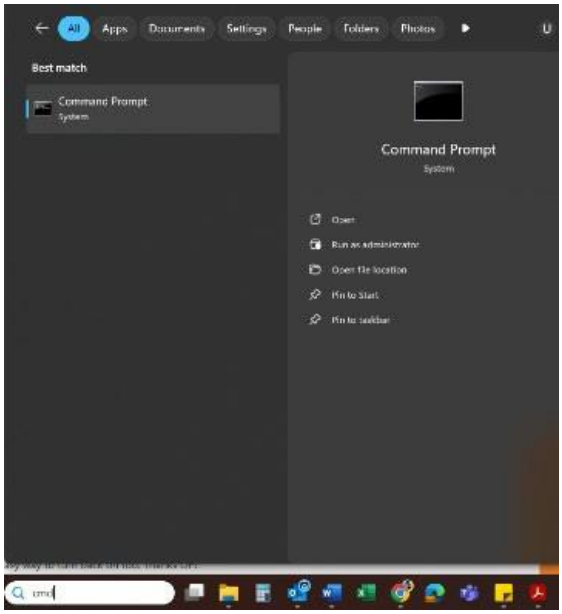
N (catalog folder)

Known Bug When Launching LockDown Browser in Google Chrome in Windows

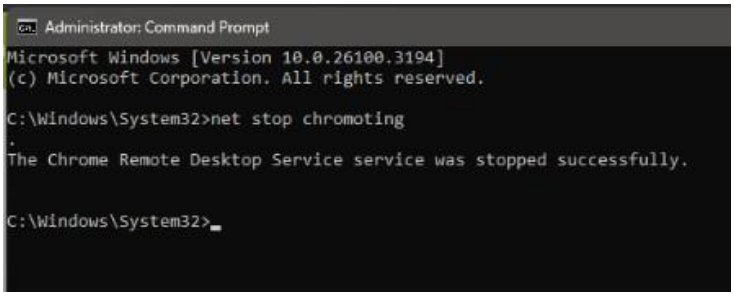
LockDown Browser is unable to launch due to Chrome Remote Desktop running on the background. Chrome Remote Desktop is one of many applications on the blocklisted application list. This does not happen to all Windows laptop.

Solution:

1. Run Command Prompt as Administrator:
   - Click on the Windows logo icon
   - Type in Cmd
   - Right Click on Command Prompt > Run as Administrator



2. On Command Prompt, type in this command: net stop chromoting. Press Enter.



AUSTRALIAN SCIENCE INNOVATIONS

3. You will be able to launch the LockDown Browser from the exam page.

4. To enable the Chrome Remote Desktop back on, follow the above steps to access Command Prompt and type in net start chromoting. Press Enter. Chrome Remote Desktop will run again in the background.

DISTRIBUTION AND INSTALLATION OF LOCKDOWN BROWSER – for Mac Devices

IMPORTANT: If the students have administrator access to the their devices, please use the students-managed device' installer instead, not the installer mentioned in this section. Please follow the students-managed device guide.

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 LockDown Browser for Managed Computers (Mac) installer: https://asi.sharefile.com/d- sf8ac2d7186d34a8abedd93280a0ec961
2. Install LockDown Browser for Managed Computers (Mac) on at least one Mac.
3. Start LockDown Browser for Managed Computers (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 for Managed Computers installer. Instead, install LockDown Browser-Mac at least one time then copy/push/deploy the installed LockDown Browser app to other Macs.

Unattended Installs on Managed Macs

LockDown Brower for Managed Computers 2.1 for Mac can be installed without prompts through the Terminal or deployed with desktop management systems that support commands through the Terminal.

The recommended steps for installing on a managed Mac are:

1. Download the LockDown Browser for Managed Computers (Mac), "InstallLDBLabPackage64c-2-1- 0-xx.zip"
2. Unzip the file
3. Open the Terminal
4. Run the command: echo password | sudo -S installer -pkg "/full/path/to/install/file/Install Respondus LockDown Browser (x64c) xxxxxxxxx{yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy}.pkg" -target /Applications -verboseR > /full/path/to/log/file/ldb-install-silent.log" where password is the root or administrator password.

Example:

echo Mister-Mxyzptlk | sudo -S installer -pkg "/Users/student1/Downloads/Install Respondus LockDown Browser (x64c) 999999999{eb4b6c70eda22d6c34a7858e9bb216b0}.pkg" -target /Applications - verboseR > "/Users/student1/Library/Logs/ldb-install-silent.log

DISTRIBUTION AND INSTALLATION OF LOCKDOWN BROWSER – for Chromebook Devices

IMPORTANT: If the students have administrator access to the devices, please use the students- managed device' installer instead, not the installer mentioned in this section. Please follow the students-managed device guide.

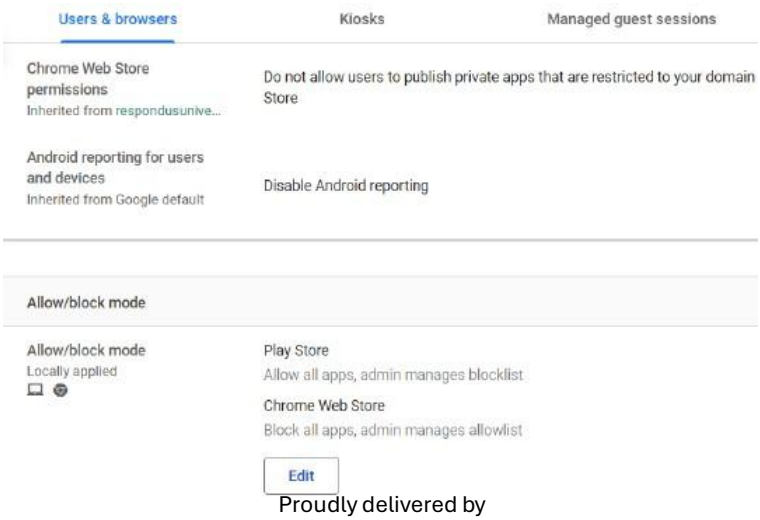
There are two basic options for Google administrators to make the LockDown Browser Chrome Extension available on managed Chromebook devices. The Chromebook Extension can be made available for manual installation by the student, or it can be automatically installed on each of the managed devices.

NOTE: *The Chromebook management settings change frequently, so the instructions that follow may not exactly match. If your institution manages Chromebooks, simply follow the same process you would for installing any extension.*

Manual Installation

Follow these instructions to make available the LockDown Browser Chrome Extension for students to manually install on their managed Chromebook devices.

1. Log into the Google management interface with your admin account.
2. Access Devices > Chrome > Apps & extensions > Users & browsers

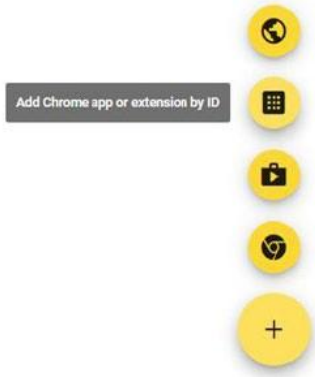


3. Select “ADDITIONAL SETTINGS” and edit the “Allow/block mode” settings for the Chrome Web Store to be: “Block all apps, admin managed allowlist”

4. Access Devices > Chrome > Apps & extensions > Users & browsers

5. Select the organization unit where you wish to install the Chrome extension.

6. Press the yellow plus button and select “Add Chrome app or extension by ID”



7. Enter this value: fogjeanjfbiombghnmkmmophfeccjdki and press Save.

8. Select “Allow Install” to add the LockDown Browser to the allowlist.

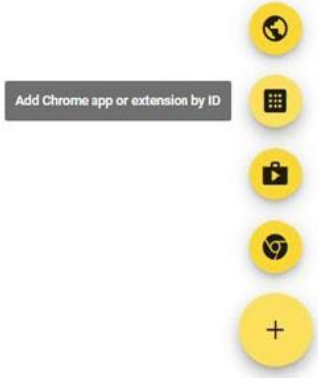
Automatically Installed

1. Log into the Google management interface with your admin account.

2. Access Devices > Chrome > Apps & extensions

3. Select the organization unit where you wish to install the Chrome extension

4. Press the yellow plus button and select “Add Chrome app or extension by ID”



5. Enter this value: fogjeanjfbiombghnmkmmophfeccjdki and press Save.
6. Lastly change the Installation Type from “Allow Install” to “Force Install” and press Save.
7. The LockDown Browser Chromebook extension will now be pushed out to all the managed Chromebook devices.

Domain and URL Pattern Filtering

The respondus2.com domain will need to be allowlisted if you have a content filter applied to the managed Chromebook devices.

The following two URL patterns should also be allowed in the Chrome browser:

rldb:

data://text/plain:

Removal of the older Chromebook App

To remove the older Chromebook App from managed devices:

i. Log into the Google management interface with your admin account.

ii. Access Devices > Chrome > Apps & extensions

iii. Select the Kiosk App “LockDown Browser” and then Delete.

DETERMINING IF THE LOCKDOWN BROWSER SETTINGS ARE SET CORRECTLY
(For All System Operations)

To confirm that the LockDown Browser is installed properly, follow these steps:

1. Access the exam URL: https://**asoexams.edu.au**

2. Create an account to access the LockDown Browser Practice Exam. In school code field, type in '00000'.

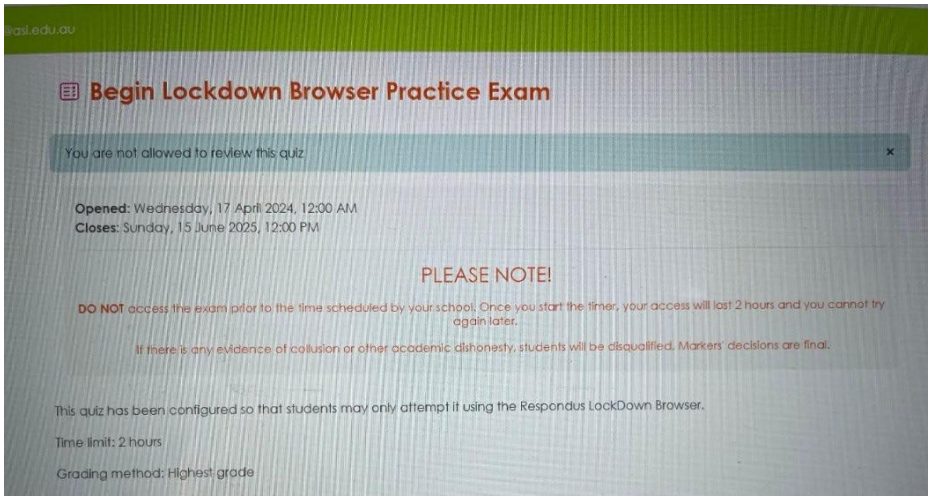
3. Once you have created your account and logged in, click on the "LockDown Browser Practice Exam" course.

4. Type in the Self-Enrolment Key: **PracExam25**

5. You will be asked to launch LockDown Browser to be able to start your attempt in the Practice Exam. If the installation is successful, the LockDown Browser will launch.

IMPORTANT: Please submit all answers to exit the LockDown Browser properly. Logging out of the exam website IS NOT the correct way as you still will be stuck in the LockDown Browser mode and will not be able to use their devices properly. If this happens, contact asi@asi.edu.au or call 02 6125 6228 for assistance.

1. Once you have submitted all their answers, you will be redirected back to the practice exam page:



AUSTRALIAN SCIENCE INNOVATIONS

2. Scrolling down to the bottom page, you will see this:

3. Click on “Exit Browser” button. LockDown Browser will automatically close and back to normal browser.

UPDATING LOCKDOWN BROWSER

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:

1. Start the browser
2. 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 (Windows) or "Check for Update" (Mac).
3. 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.

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.

LockDown Browser and Respondus Monitor needs to connect to the Respondus servers.

For the various LockDown Browser LMS server integrations (blocks, modules, LTI tools) the Respondus servers need access to the integration or module on the LMS server and the integration on the LMS needs to access the Respondus servers at: https://smc-service-cloud.respondus2.com

The LockDown Browser client web browser and Respondus Monitor "webcam" option use the following domains when accessing the Respondus servers:

- *.amazonaws.com
- *.respondus.com
- *.respondus2.com
- *.respondus7.com

We recommend including the "*.amazonaws.com" primary domain as some of the Respondus domains actually redirect to secure servers hosted on AWS. Also several of the LMSs, such as Instructure Canvas and D2L Brightspace use AWS and it's related Amazon Cloudfront.

For the client web browser used by students, the more specific domains

are: Server profiles: server-profiles-respondus-com.s3-external-

1.amazonaws.com Update server: static-public-downloads-

cloud.respondus.com Installs/Downloads: download.respondus.com

Monitor server: smc-service-

cloud.respondus2.com For all domains, the

protocols and ports are:

All connections, for all domains, are on port 443 only and require TLS 1.2+.

Outgoing access must be allowed to:

- *.amazonaws.com port 443 (HTTPS)
- *.respondus.com port 443 (HTTPS)

- *.respondus2.com port 443 (HTTPS)
- *.respondus7.com port 443 (HTTPS)

The LMS must allow incoming access from: 34.199.184.160 (VPC NAT)

As the Respondus servers are "in the cloud", unless specified, 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.

The latest IP address ranges for Amazon Web Services US East (Northern Virginia) can be found at: http://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html