

HESI[®]

iNet – Windows Workstation Requirements

SYSTEM REQUIREMENTS

Operating System	Windows 8.1 and up	Note: Windows 10 Pro N is not supported because it does not include the media pack and therefore will not support audiovisual exam items
Processor	32/64 bit	See requirements for OS
Memory	See requirements for OS	
Network Connection	<u>Download Speed:</u> <ul style="list-style-type: none"> • Minimum: 25 Mbps • Recommended: 100 Mbps + <u>Upload Speed:</u> <ul style="list-style-type: none"> • Minimum: 3 Mbps 	Broadband or fiber connection recommended
Video	1280 x 800 or better	
Port	80,443	For outgoing traffic
Browser	Edge Google Chrome Internet Explorer (IE) Mozilla Firefox	Latest version
Software Apps	Windows	For test taking security-Microsoft Outlook must be closed when running secure browser Adobe Acrobat Reader 11.0.17 or above

Devices Not Supported
Chromebook
Computers using Windows XP or previous versions
iPad Air
iPad 4 th generation and older

BROWSER SETTINGS

Your organization may have one or more security controls in place that may interfere with testing. Below are some common security settings changes you may be able to make yourself. Note you must have computer workstation IP addresses when setting up your exams. Please contact your IT staff for more assistance in these areas.

CHROME


1. In the Chrome browser to access the tools bar, click on the three dots on the right-hand side.
2. From there select Settings.

Another way to access this page is by typing `chrome://settings` in your address bar.

Please note that each header will also have a hyper link that will direct you to the place in your Chrome browser.

TRUSTED SITES

1. Click the 3 horizontal lines icon on the far right of the Address bar.
2. Click on Settings, then under Privacy and Security click Site Settings.
3. Scroll down to Additional Content Settings and look for Insecure Content and click that option.
4. From there you will see at the bottom of the page you can see the section that says:
5. Allowed to show insecure content
6. From there click the button on the right that says Add.
7. From here you will be able to add the following URLs and click the Add button
 - `https://hesi.elsevier.com`
 - `https://eolsapi.elsevier.com`
 - `https://eolscontent.elsevier.com`
 - `https://hesifacultyaccess.elsevier.com`
 - `https://service.elsevier.com`
 - `https://www.hesiinet.com`
 - `https://hesiinet.elsevier.com`
 - `https://hesimmx.elsevier.com`
 - `https://hesisecurebrowser.elsevier.com`
 - `https://hesiinetvalidation.elsevier.com`



The list will populate under the Allowed to show insecure content header.

POP-UP BLOCKER

1. From Settings, click Privacy and security.
2. Then select Site Settings.
3. Scroll down till you see Pop-ups and redirects. Click on that link.
4. Under Allowed to send pop-ups and use redirects we can add the following URL's
 - <https://hesi.elsevier.com>
 - <https://eolsapi.elsevier.com>
 - <https://eolscontent.elsevier.com>
 - <https://hesifacultyaccess.elsevier.com>
 - <https://service.elsevier.com>
 - <https://www.hesiinet.com>
 - <https://hesiinet.elsevier.com>
 - <https://hesimmx.elsevier.com>
 - <https://hesisecurebrowser.elsevier.com>
 - <https://hesiinetvalidation.elsevier.com>
5. Once done, feel free to close the settings tab.

FIREFOX

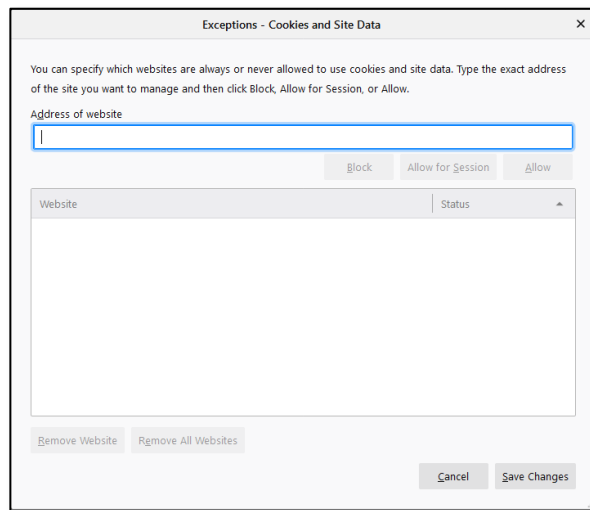
1. Open Mozilla Firefox.
2. Click the 3 dashes on the right-hand side of the window and choose Options.
3. Then choose Privacy & Security on the left-hand side of the screen.

TRUSTED SITES

Javascript is enabled by default in most Firefox browsers

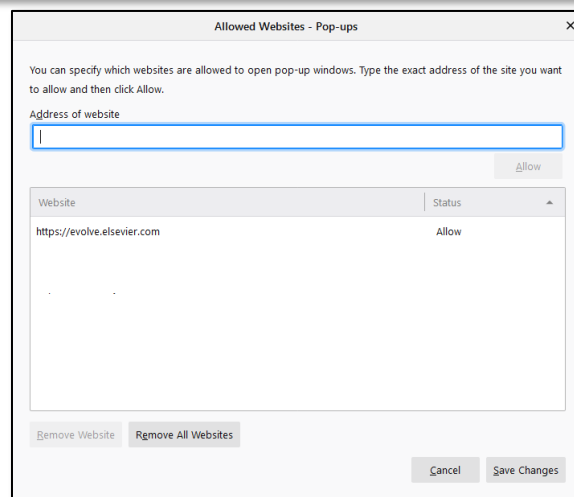
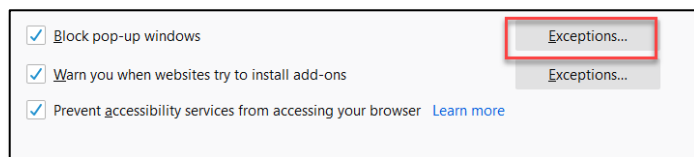
PRIVACY TAB SETTINGS

1. Click on the Privacy & Security option on the left-hand side of the window.
2. Scroll till you see Cookies and Site Data. Then click the Manage Permissions button.
3. An Exceptions box will pop up.
4. Enter each URL below and click the button Allow. When done click Save Changes and the box will close.
 - <https://hesi.elsevier.com>
 - <https://eolsapi.elsevier.com>
 - <https://eolscontent.elsevier.com>
 - <https://hesifacultyaccess.elsevier.com>
 - <https://service.elsevier.com>
 - <https://www.hesiinet.com>
 - <https://hesiinet.elsevier.com>
 - <https://hesimx.elsevier.com>
 - <https://hesisecurebrowser.elsevier.com>
 - <https://hesiinetvalidation.elsevier.com>



POP-UP BLOCKER

1. Scroll down further on the page till you see Block pop-up windows. There should be a box that says Exceptions.
2. When you click on the Exceptions tab, you will see the following box.
3. Enter the following websites one by one and click allow.
 - <https://hesi.elsevier.com>
 - <https://eolsapi.elsevier.com>
 - <https://eolscontent.elsevier.com>
 - <https://hesifacultyaccess.elsevier.com>
 - <https://service.elsevier.co>
 - <https://www.hesiinet.com>
 - <https://hesiinet.elsevier.com>
 - <https://hesimx.elsevier.com>
 - <https://hesisecurebrowser.elsevier.com>
 - <https://hesiinetvalidation.elsevier.com>
4. When done click save changes and the box will close. Then close that tab.



Note: If you are using other pop-up blockers, contact your IT team for assistance.

INTERNET EXPLORER

Open Microsoft Internet Explorer. Click the “Tools” menu and click the “Internet Options” option.

SECURITY TAB SETTINGS

1. Click the Security tab.
2. Highlight the “Trusted Sites” option.
3. Click the Sites button.
4. Add “https://hesi.elsevier.com”
5. Add “https://eolsapi.elsevier.com”
6. Add “https://eolscontent.elsevier.com”
7. Add “https://hesifacultyaccess.elsevier.com”
8. Add “https://service.elsevier.com”
9. Add “https://www.hesiinet.com”
10. Add “https://hesiinet.elsevier.com”
11. Add “https://hesimmx.elsevier.com”
12. Add “https://hesisecurebrowser.elsevier.com”
13. Add “https://hesiinetvalidation.elsevier.com”
14. Then click the Custom level... button.

Then on the Security Settings – Trusted Sites Zone pop up do the following:

- a) The following must be enabled:
 - a. In the ActiveX controls and plug-ins section:
 - i. Run ActiveX controls and plug-ins
 - ii. Script ActiveX controls marked safe for scripting*
 - iii. Allow Programmatic clipboard access
 - b. In the Scripting section:
 - i. Scripting of Java Applet
- b) The following must be enabled
 - a. In the Scripting section:
 - i. Active Scripting

Privacy Tab Settings

1. Click the Privacy tab.
2. Set at medium-high or lower.
3. Click on the **Advanced** button.
4. Then on the Advanced Privacy Settings pop up do the following:
 - a) Click the *Override automatic cookie handling* check box.
 - b) Verify the “Accept” option is selected in the *First-party Cookies* section.
 - c) Check the *Always allow session cookies* check box.

Pop-Up Blocker

In the Pop-up Blocker section, if the *Turn on Pop-up Blocker* check box is checked, do the following:

1. Click the Settings button.
2. Click in the *Address of website to allow field*.
3. Enter “*.hesiinet.com”
4. Click the **Add** button.
5. Enter “hesiinet.elsevier.com”
6. Click the **Add** button.
7. Enter “eolscontent.elsevier.com”
8. Click the **Add** button.
9. Enter “hesifacultyaccess.elsevier.com”
10. Click the **Add** button.
11. Enter “service.elsevier.com”
12. Click the **Add** button.
13. Enter “hesisecurebrowser.elsevier.com”
14. Click the **Add** button.
15. Enter “hesimmx.elsevier.com”
16. Click the **Add** button.
17. Enter “hesiinetvalidation.elsevier.com”
18. Click the **Add** button.
19. Click the **Close** button.

Note: *If you are using other pop-up blockers, contact your IT team for assistance.*

DOMAIN, FIREWALL & IPs

Domain/Firewalls	Domain Name	Port
<i>Please include the following domains as trusted sites</i>	https://hesi.elsevier.com	80,443
	https://eolsapi.elsevier.com	80,443
	https://eolscontent.elsevier.com	80,443
	https://hesifacultyaccess.elsevier.com	80,443
	https://service.elsevier.com	80,443
	https://www.hesiinet.com	80,443
	https://hesiinet.elsevier.com	80,443
	https://hesimmx.elsevier.com	80,443
	https://hesisecurebrowser.elsevier.com	80,443
	https://hesiinetvalidation.elsevier.com	80,443

IP Information	IPv4	Port	
<p><i>We recommend you to configure your environment to use the domain names. The IP addresses are subject to change due to infrastructure updates.</i></p>	103.21.244.0/22	80,443	
	103.22.200.0/22	80,443	
	103.31.4.0/22	80,443	
	104.16.0.0/12	80,443	
	108.162.192.0/18	80,443	
	131.0.72.0/22	80,443	
	141.101.64.0/18	80,443	
	162.158.0.0/15	80,443	
	172.64.0.0/13	80,443	
	173.245.48.0/20	80,443	
	188.114.96.0/20	80,443	
	190.93.240.0/20	80,443	
	197.234.240.0/22	80,443	
	198.41.128.0/17	80,443	
	199.27.128.0/21	80,443	
		IPv6	Port
		2400:cb00::/32	80,443
		2405:8100::/32	80,443
	2405:b500::/32	80,443	
	2606:4700::/32	80,443	
	2803:f800::/32	80,443	
	2c0f:f248::/32	80,443	
	2a06:98c0::/29	80,443	