HESI®

Windows Workstation Requirements

SYSTEM REQUIREMENTS

Workstation	PC	Notes
Operating System	Windows 10 and up	Minimum of Windows 10 April 2018 Update (version 1803, build 10.0.17134)
Processor	32/64 bit x86	ARM processors (e.g. SQ1, Snapdragon) are not supported
Memory	See requirements for OS	
Network Connection	<u>Download Speed:</u> • Minimum: 25 Mbps • Recommended: 100 Mbps + <u>Upload Speed:</u> • Minimum: 3 Mbps	Broadband of fiber connection recommended Wireless not recommended
Video	1280 x 800 or better	
Port	80, 443	For outgoing traffic
Browser	Google Chrome Mozilla Firefox Edge	Latest Version
Software Apps	Windows	The Secure Browser requires either Microsoft Edge Chromium or the WebView2 runtime to be installed on the device.
		JAWS: current version or one version prior
		Adobe Acrobat Reader 11.0.17 or above
		.NET Framework 4.8 required

Windows

		Use of virtual machines requires advance notification, as client systems must be configured with a specialized setup to ensure compatibility. Clinical Practice Readiness (CPRA) exams are not compatible with virtual machines.

Devices Not Supported
Computers using Windows XP or older
Computers with ARM processors, including but not limited to: – Microsoft Surface Pro X – Microsoft Surface Pro 9 (5G variant only) – Samsung Galaxy Book Go – Lenovo ThinkPad X13s
iPad Air 1st generation
iPad 4th generation and older

Note: iPads, Chromebooks, and virtual machines are not supported for CPRA exams.

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.

JUMP TO A SECTION:

CHROME

In the Chrome browser to access the tools bar, click on the three dots on the right-hand side.

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.

Windows

TRUSTED SITES (LINK)

- Click the 3 horizontal lines icon on the far right of the Address bar.
- Click on Settings, then under Privacy and Security click Site Settings.
- Scroll down to Additional Content Settings and look for Insecure Content and click that option.
- From there you will see at the bottom of the page you can see the section that says:
    - Allowed to show insecure content
- From there click the button on the right that says Add.

- 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 (LINK)

- From Settings, click Privacy and security.
- Then select Site Settings.
- Scroll down till you see Pop-ups and redirects. Click on that link.
- 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

- Once done, feel free to close the settings tab.

Windows

FIREFOX

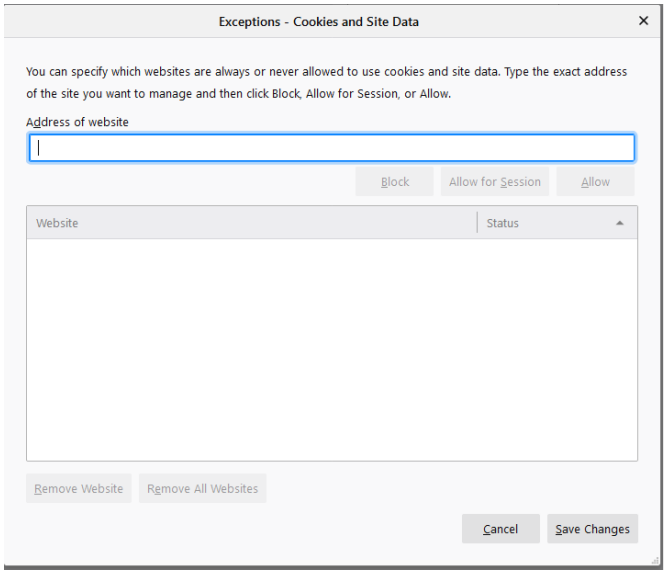
- Open Mozilla Firefox.
- Click the 3 dashes on the right-hand side of the window and choose Options.
- Then choose Privacy & Security on the left-hand side of the screen.

TRUSTED SITES

Javascript is enabled by default in most Firefox browsers.

PRIVACY TAB SETTINGS (LINK)

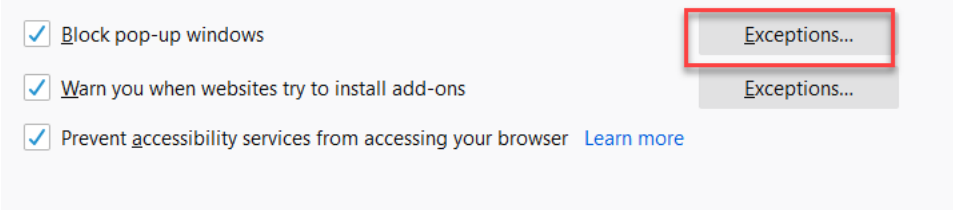
- Click on the Privacy & Security option on the left-hand side of the window.
- Scroll till you see Cookies and Site Data. Then click the Manage Permissions button.
- An Exceptions box will pop up.



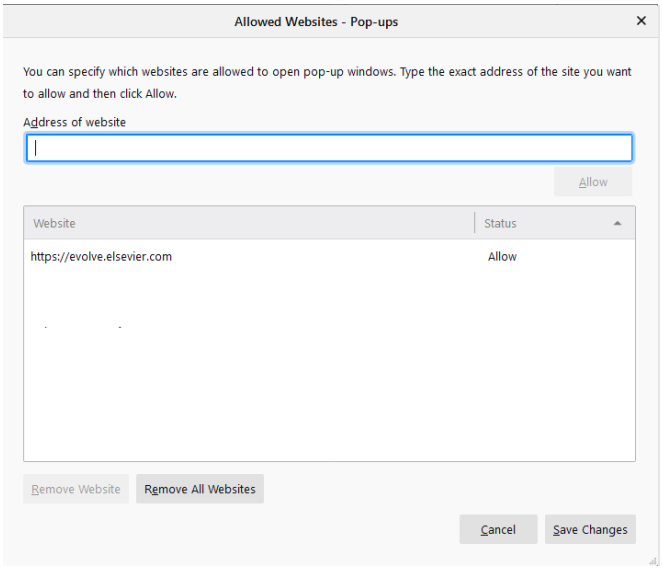
- Enter each URL below and click the button Allow. When done click Save Changes and the box will close.
- https://hesi.elsevier.com
  - https://eolsapi.elsevier.com
  - https://eolscontent.elsevier.com
  - https://hesifacultyaccess.elsevier.com
  - https://service.elsevier.com
  - https://www.hesiinet.com
  - https://hesiinet.elsevier.com
  - https://hesimmx.elsevier.com
  - https://hesisecurebrowser.elsevier.com
  - https://hesiinetvalidation.elsevier.com

POP-UP BLOCKER

- Scroll down further on the page till you see Block pop-up windows. There should be a box that says Exceptions.



- When you click on the Exceptions tab, you will see the following box.



- 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://hesimmx.elsevier.com
  - https://hesisecurebrowser.elsevier.com
  - https://hesiinetvalidation.elsevier.com
- 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.*

EDGE

Open Edge. Click the three dots in the upper right menu and select “More Tools” and then 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://www.hesiinet.com”
5. Add “https://hesiinet.elsevier.com”
6. Add “https://hesimmx.elsevier.com”
7. Add “https://hesisecurebrowser.elsevier.com”
8. Add “https://hesiinetvalidation.elsevier.com”
9. 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

Please also make sure that "Do not save encrypted pages to disk" is not selected under the Advance tab within Internet Options for Edge.

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

a) Click the Settings button.
b) Click in the *Address of website to allow field*.
c) Enter "*.hesiinet.com"
d) Click the ***Add*** button.
e) Enter "hesiinet.elsevier.com"
f) Click the ***Add*** button.
g) Enter "hesisecurebrowser.elsevier.com
h) Click the ***Add*** button.
i) Enter hesimmx.elsevier.com
j) Click the ***Add*** button.
k) Enter hesiinetvalidation.elsevier.com
l) Click the ***Add*** button.
m) Click the ***Close*** button.

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

Advanced Tab Settings

1. Ensure "Do not save encrypted pages to disk" is not selected under the Advance tab within Internet Options for Edge.

DOMAINS & FIREWALLS

Domain/Firewalls	Domain Name	Port
	hesiinetadmin.elsevier.com	80,443
	hesiinetmon-ws.elsevier.com	80,443
	hesiinet.elsevier.com	80,443
	hesisecurebrowser.elsevier.com	80,443
	hesiinetvalidation.elsevier.com	80,443
	hesicdn-private.hesiinet.com	80,443
	hesicdn-public.hesiinet.com	80,443
	*.starttest.com	80,443
	*.starttest2.com	80,443
	*.gettesting.com	80,443
	*.programworkshop.com	80,443
	*.programworkshop2.com	80,443

***Note:** depending on your networking solution, you may need to add these domains in a different format. If the above does not work, please try adding them without asterisks (for example: http://starttest.com), without the http/https prefix (for example: *.starttest.com), or with asterisks on either side of the domain (for example: *.programworkshop.com*).*

IP Information	IPv4	Port
We recommend you to configure your environment to use the domain names. The IP addresses are subject to change due to infrastructure updates.	66.225.197.197	80,443
	72.21.91.29	80,443
	93.184.220.29	80,443
	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
	117.18.237.29	80,443
	131.0.72.0/22	80,443
	141.101.64.0/18	80,443
	151.139.128.14	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

ADDITIONAL SETTINGS

- Verify that your DHCP lease time is set to at least one day. If the lease is renewed more frequently, it can create unnecessary network traffic.
- Ensure that HTTPS Inspection is turned off. This feature decrypts and re-encrypts every packet, which can be very resource-intensive. Because it is usually enabled by default on many firewalls, it is important to check this setting before testing.
- Check for any cap limitations on HTTP and HTTPS communications. If either protocol is capped at a specific MB limit, that restriction may affect testing.
- Confirm that anti-virus, security programs, or other scans are not scheduled to run during testing times. You do not need to disable auto-scans completely, but it is recommended to adjust the schedule so they do not run during testing.

- If the options above do not resolve the issue, apply the same settings to the Windows Firewall or any local anti-virus programs.
- If antivirus software flags the secure browser, update the antivirus software signatures.