# HESI®

# MAC Workstation Requirements

## SYSTEM REQUIREMENTS

| Workstation | PC | |
|---|---|---|
| Operating System | MAC 10.14+<br>iOS 15+ | |
| Processor | 32/64 bit | See requirements for OS |
| Memory | See requirements for OS | |
| Network Connection | Download Speed:<br>• Minimum: 25 Mbps<br>• Recommended: 100 Mbps +<br>Upload Speed:<br>Minimum: 3 Mbps | Broadband or fiber connection recommended<br>Mac Network Settings<br>iOS Network Settings |
| Video | 1200 x 800 or better | |
| Browser | Google Chrome<br>Mozilla Firefox<br>Safari | Latest version |
| Software Apps | MAC | Adobe Acrobat Reader 11.0.17 or above (if printing/viewing reports) |

| Devices Not Supported |
|---|
| iPad Air 1st generation |
| iPad 4th generation and older |
| Computers using Windows XP or older |

*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.*

## SAFARI

Open Safari. Click "Safari" menu and click the "Preferences" option.

### Privacy Tab Settings

1. Click the **Privacy** tab.
2. Check "*Never*" under Block Cookies.

### Privacy Tab Settings

1. Click the **Security** tab.
2. Check "*Enable Javascript"*

### Websites

3. Click "*Pop-up windows"* at the bottom of the page.
    a. Under "*When visiting other websites*:" choose Allow.

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

## 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.

### Trusted Sites

Click the 3 horizontal lines icon on the far right of the Address bar.

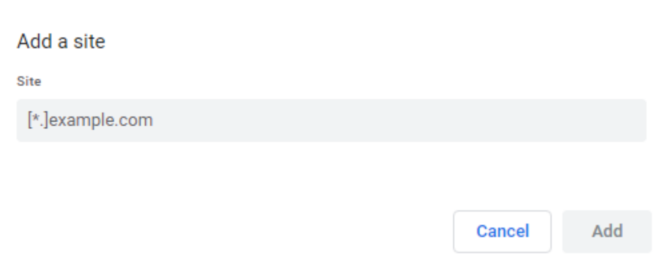
Click on Settings, then under Privacy and Security click Site Settings.

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

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.

## 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

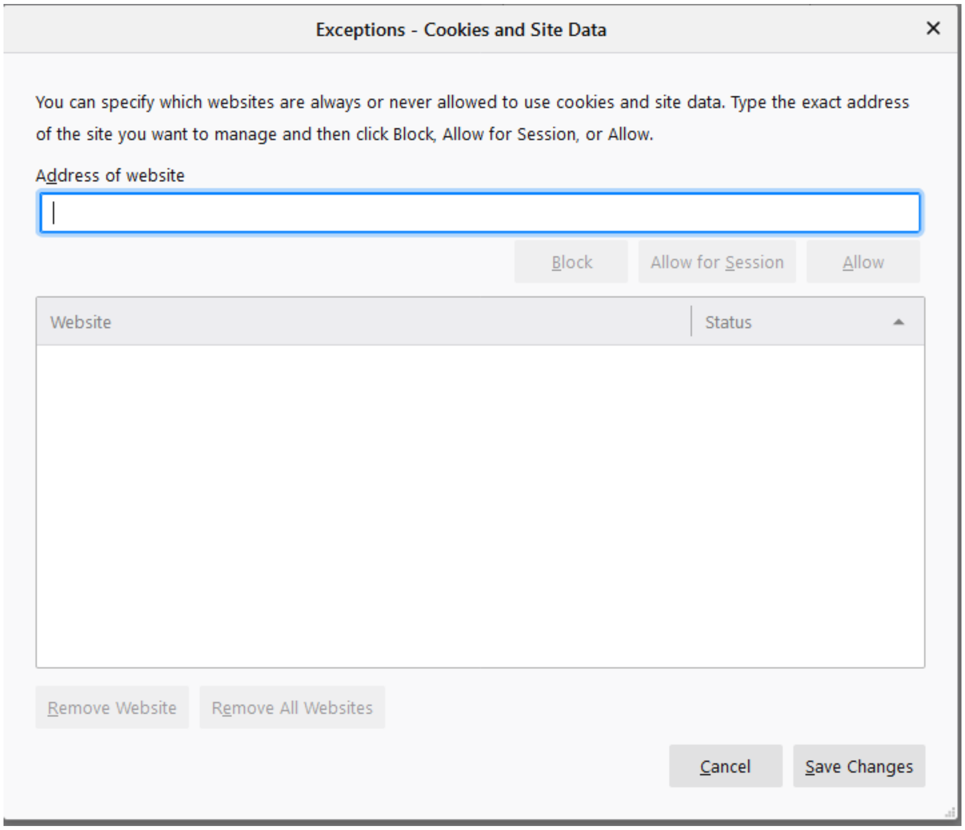
Javascript is enabled by default in most Firefox browsers.

## PRIVACY TAB SETTINGS

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.



You can specify which websites are always or never allowed to use cookies and site data. Type the exact address of the site you want to manage and then click Block, Allow for Session, or Allow.

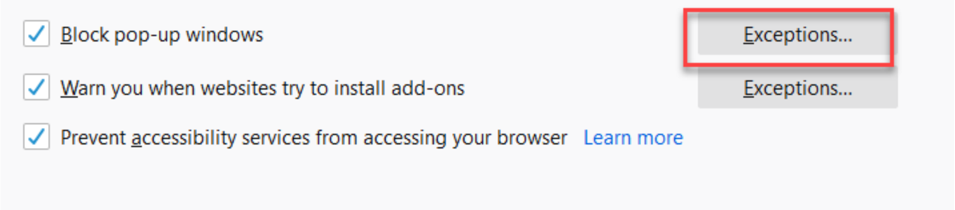
Enter each URL below and click the button Allow. When done click Save Changes and the box will close.

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.

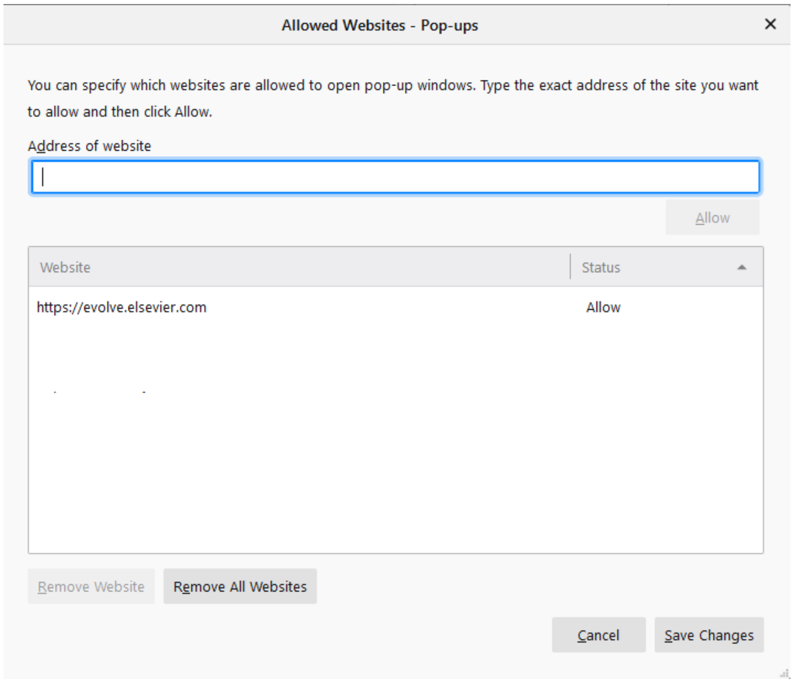


☑ Block pop-up windows

☑ Warn you when websites try to install add-ons

☑ Prevent accessibility services from accessing your browser

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



Allowed Websites - Pop-ups

You can specify which websites are allowed to open pop-up windows. Type the exact address of the site you want to allow and then click Allow.

Address of website

| Website | Status |
|---|---|
| https://evolve.elsevier.com | Allow |

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.

## 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 |
| | *.starttestrp.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 |

***Note****: Security software such as virus protection packages and security appliances (ie, Barracuda) may need to be set to allow the Reach browser. Application to load at run time. These software packages and appliances may need to be setup to allow two-way communications over the Internet. Please reference the above table for the domain names and public IP addresses needed to establish this connection. If you need any assistance, please contact Technical Support at 1-800-950-2728, option 1.*

## ADDITIONAL SETTINGS

- Verify your DHCP Lease Time is set to at least one day. If it is set to renew its lease sooner, it can add unnecessary network traffic.
- Ensure that any anti-virus, security programs, or other scans are not set to scan daily during testing times.
- As needed, apply these settings to any anti-virus program on the local computers.