ERROR MESSAGE:

'The application was unable to route the session back to the login page.'

This Application Message often occurs due to a browser requirement to accept third party cookies. **Third-Party Cookies** are nothing but cookies from another website requested via an embedded code. These have no real benefit to the user as they are only used for data gathering purposes.

UCIBuy (powered by Jaggaer / aka SciQuest) relies on Third-Party Cookies being enabled in the browser setting.

RESOLUTION:

Use the steps detailed below by browser type to **Enable Third Party Cookies in the browser of choice.**

⊗ The application was unable to route the session back to the login page.

The application was unable to determine your session and your login page. A possible cause could be using a bookmark to access the application. In order to start a new session, return to your organization's main login page.

Mozilla Firefox is the recommended browser for UCIBuy. Remember to close all open browser tabs after changing settings before reopening and logging back into UCIBuy.

Note: Internet Explorer is no longer a supported browser for UCIBuy.

Scroll down to view Browser Specific, Step-by-Step Instructions for enabling third party cookies for following:
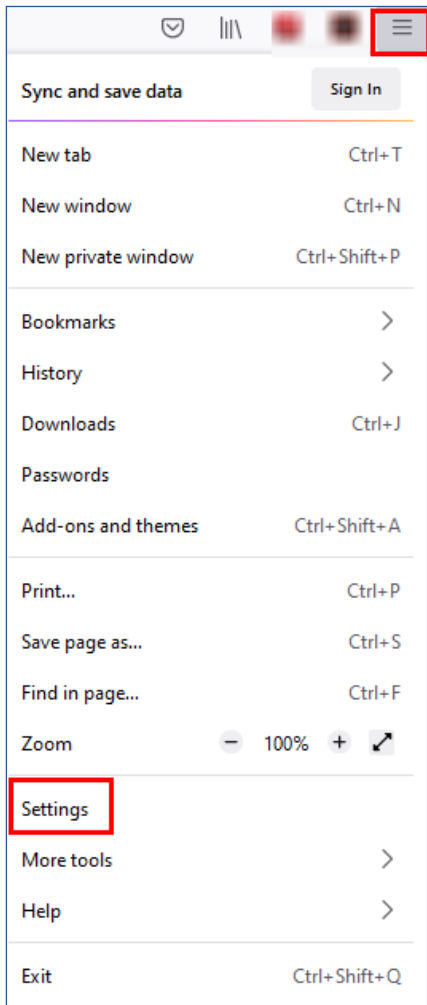
Mozilla Firefox (preferred)

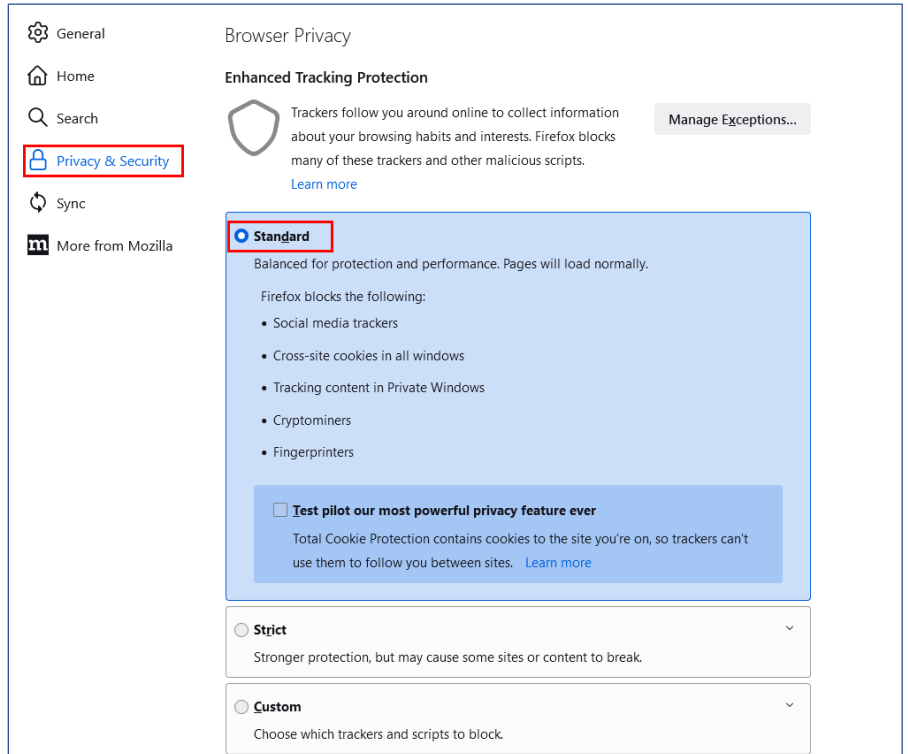**Google Chrome**

Safari (Apple)
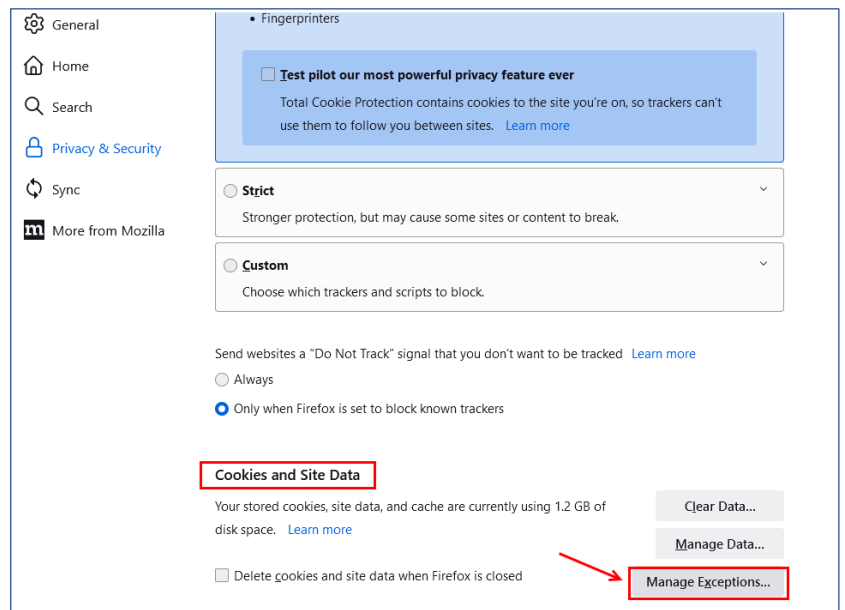
Microsoft Edge

Mozilla Firefox:

1. Open application menu (three horizontal lines) appearing at the top right of the browser > **Settings**

2. Settings > Privacy & Security > select **Standard** button

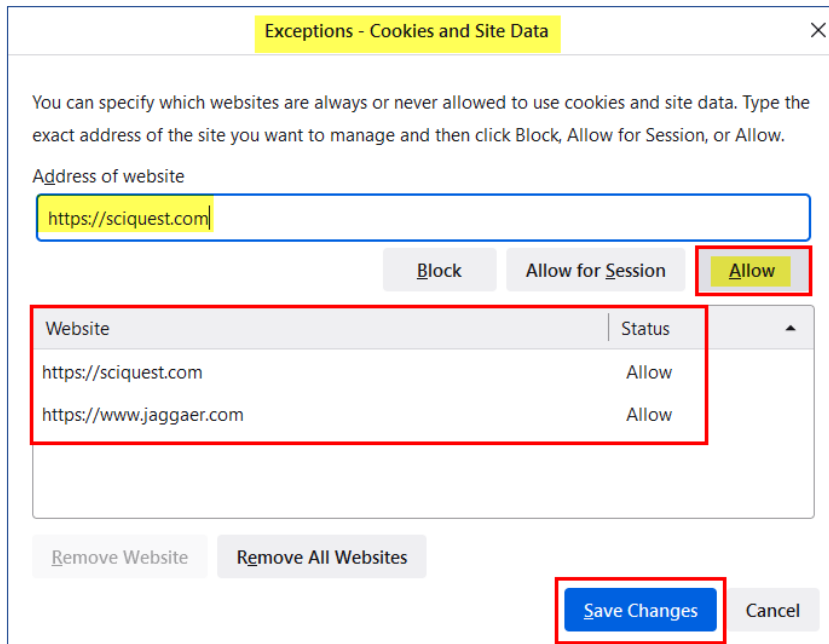3. Settings > Privacy & Security > **Cookies and Site Data > Manage Exceptions**

Mozilla Firefox:

4. Manage Exceptions:

UCIBuy is powered by Jaggaer (previously known as SciQuest). Enter both web addresses shown below (individually) in the Address of website field, select Allow and Save Changes. This will enable Third Party Cookies from the website addresses that are indicated as Allow.
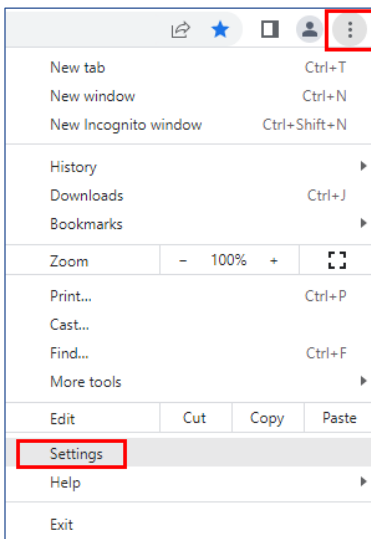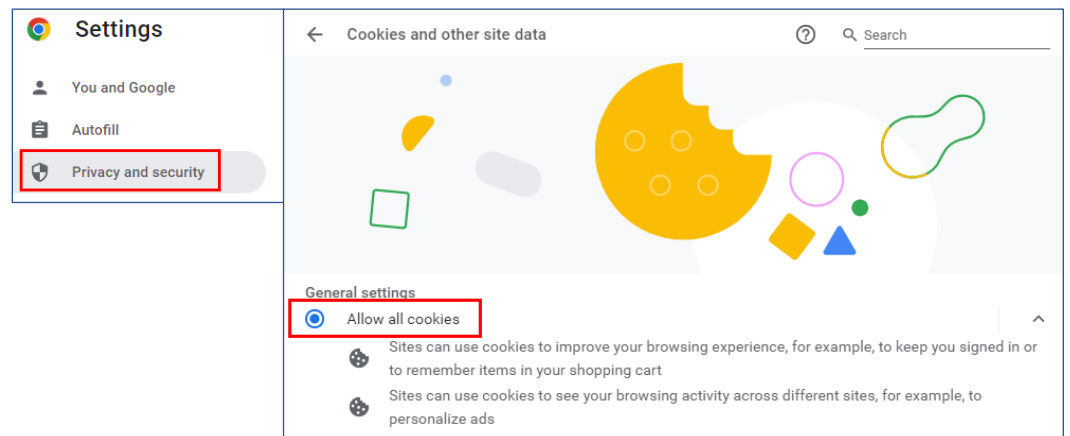
https://sciquest.com

https://jaggaer.com

5. Close all open browser tabs and open a new browser tab to access UCIBuy
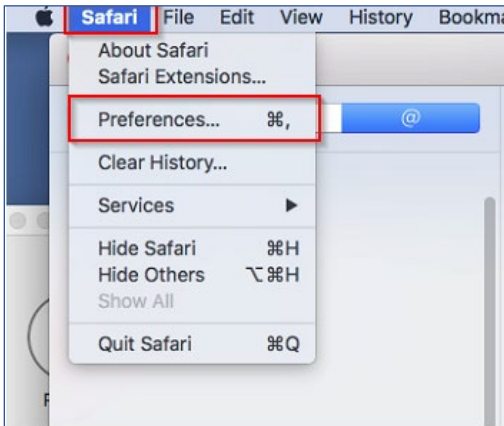
Google Chrome:

1. Chrome application menu > **Settings**
2. Settings > **Privacy and Security**
3. Privacy and Security > **Cookies and other site data**
4. Cookies and other site data > **Allow all cookies**

SAFARI:

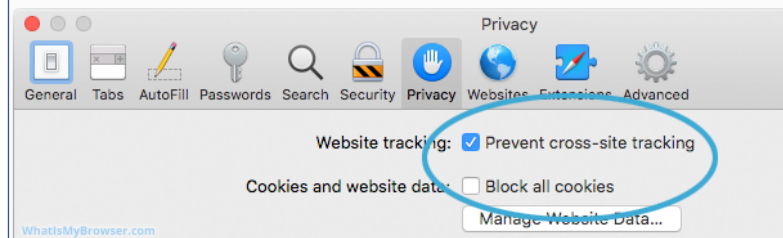**NOTE:** As of Safari 13.1 and later, third party cookies are blocked by default

1. Open Safari and go to the left-hand corner
2. Expand Safari menu > **Preferences**

3. Navigate to **Privacy** tab
4. Website tracking > **Enable** 'Prevent cross-site tracking'
5. **Cookies and website data: Disable** 'Block all Cookies'
6. Close the Preferences window and continue using Safari.

Choose your preferred Cookies and tracking settings

On the Privacy Preferences tab, you will see the "**Website tracking:**" and "**Cookies and website data:**" checkboxes.

Enabling **Prevent cross-site tracking** blocks third-party cookies from being set as well as third-party websites from storing data on your computer. Enabling this option is a good step in helping prevent companies from tracking your activity online.
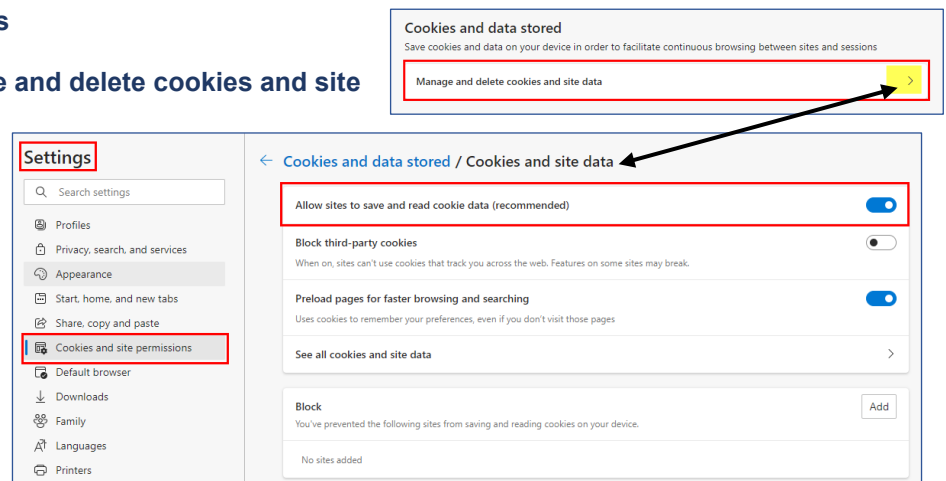
Enabling **Block all cookies** will prevent block First-Party cookies, as well as Third-Party cookies. Enabling this may cause websites to not work properly, and Safari will warn you about this if you choose this option.

A good balance of settings is to enable **Prevent cross-site tracking** and disable **Block all cookies.**

If you click the **Manage Website Data** button you'll see a list of website domains which have stored data on your computer. You can remove some or all of them.

Microsoft Edge

1. Settings > **Cookies and site permissions**

2. Cookies and data stored > Select **Manage and delete cookies and site data** fly out menu

3. **Cookies and site data > Enable:** Allow sites to save and read cookie data

4. Close and reopen browser