

Firewall Configuration Guidelines

These are common configuration steps for granting firewall permission to CASAS eTests. These steps are necessary for the CASAS eTests secure browser to communicate freely between your agency and the CASAS eTests server when your students are testing. Many agencies will not need these instructions; however, we are providing them for your Information Technology Department. Corrections facilities may have specifications that exceed these guidelines; therefore, they should contact CASAS Tech Support for assistance.

For questions and assistance, please contact CASAS Tech Support.

- Email: techsupport@casas.org
- Phone: 1-858-292-2900 or 1-800-255-1036, option 2
- Available: 6 a.m. to 5 p.m. (Pacific), M – F

1. The following outbound ports are fully open and can freely communicate:

Http (80)

Https (443)

2. The following IP address is set as approved / unblocked / or given the highest priority:

64.106.220.0/24

Note: This is an IP range. If your system does not accept 0/24, try using just 0 at the end.

3. If your agency or district firewall or access control devices are configured to allow only a certain set of IP addresses to be accessed from your network, you will need to include the following IP addresses:

192.16.58.8

117.18.237.29

93.184.220.29

72.21.91.29

66.225.197.197

4. The following domains have been approved and given unrestricted access:

http://*.programworkshop.com

https://*.programworkshop.com

<https://ecasas.org/>

<https://etestsonline.org/>

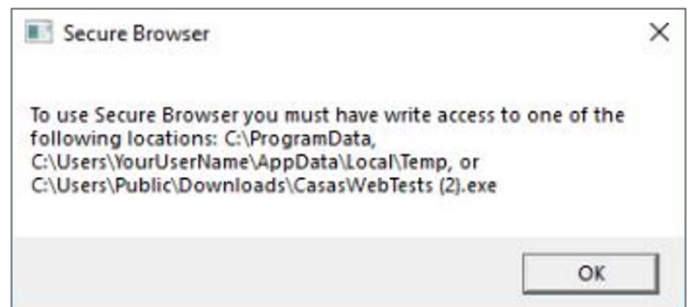
5. The secure browser requires write and execute privileges to run. On **Launch**, the secure browser will attempt to create a folder within the %ProgramData% folder, extract its security library, and launch. If it does not have rights to that directory, it will try the temporary folder in %LocalAppData%. If it does not have the needed access there, it will try the running location.

6. You need the most recent version of Microsoft® Edge installed for Windows 10 and 11 devices. The secure browser requires either Edge Chromium v91 or newer, or the Microsoft WebView2 runtime.

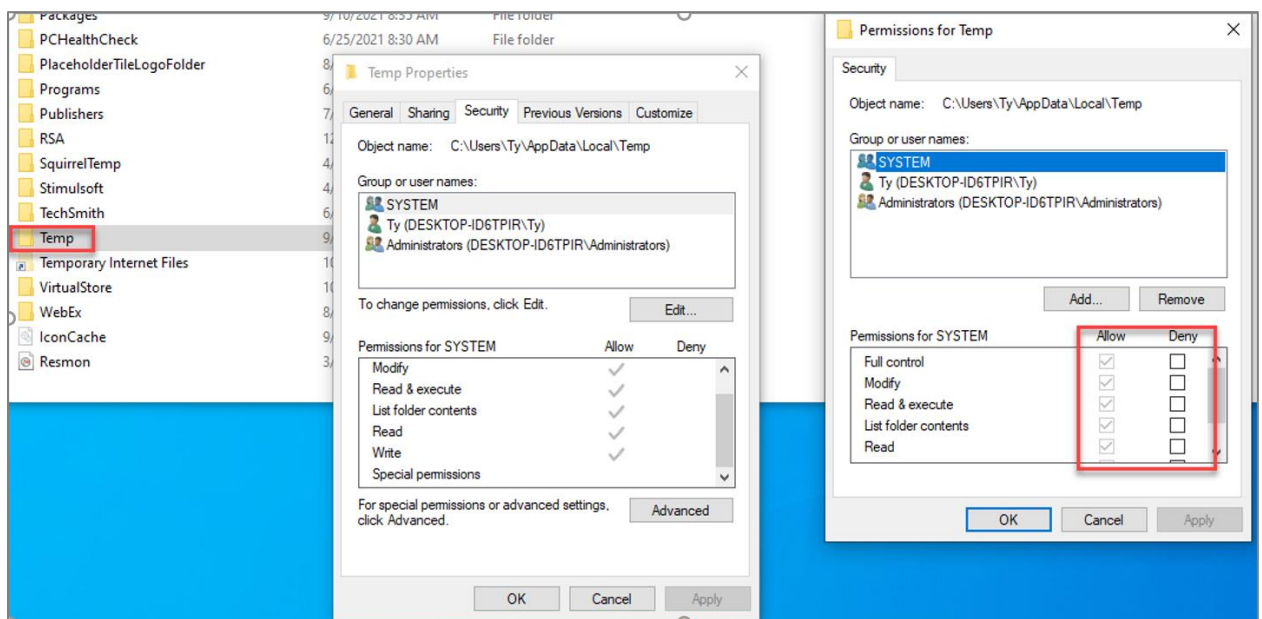


If you do not want to allow Edge Chromium, you can install the runtime. The runtime requires administrator privileges to install and can be downloaded from <https://go.microsoft.com/fwlink/p/?LinkId=2124703>. Note: The runtime cannot be used as a regular web browser.

7. Permission issues can arise with new installations, such as this error:



This screenshot shows how to troubleshoot this.



8. If all else fails, consider configuring your third-party security program to exclude SSL traffic from decryption with [\[https://*.programworkshop.com\]](https://*.programworkshop.com) [ecasas.org](https://*.ecasas.org), and [etestsonline.org](https://*.etestsonline.org).