Recommendations to prepare for testing on an iPad

You will need to apply these settings to any proxy, firewall, content filter, or other security device that is setup on your local machines or local network.

If your institution is part of a larger network such as a district, county, or any sort of parent institution, then please share this info with the appropriate parties at that location as well (such as a Network Administrator):

1. Please ensure that HTTPS Inspection is turned OFF. This can be very resource intensive, as it decrypts and encrypts every packet. This setting is usually turned on by default with most firewalls, so it is important to check before testing.
2. Please check to see if there are any cap limitations on your HTTP and HTTPS communications. If either or both of those are capped at a certain limit of MBs, then that limitation could affect testing.
3. The following Ports are fully opened and can freely communicate:

Http (80)

Https (443)

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

64.106.220.0/24

This is an IP Range, but if your system does not accept '0/24', then please try using just '0' at the end.

5. If your corporate firewall and/or access control devices are configured to allow only a certain set of IP addresses to be accessed from your network, you'll 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

Last Revised:
8/8/2022

6. The following Domains have been approved and given unrestricted access:

http://*.starttest.com

https://*.starttest.com

http://*.starttest2.com

https://*.starttest2.com

http://*.startpractice.com

https://*.startpractice.com

http://*.programworkshop.com

https://*.programworkshop.com

NOTE – Sometimes it works better on certain systems if you add them in one of these fashions: (1) http://starttest.com (2) http://starttest2.com (3) ***.starttest.com*** (4) ***.starttest2.com***(5) ***.programworkshop.com***

7. Please also make sure that "Do not save encrypted pages to disk" is not selected under the Advance tab within Internet Options for Internet Explorer.
8. Please ensure your DHCP Lease Time is set to at least 1 day. If it is set to renew its lease sooner, it can add unnecessary network traffic. Please note, we typically recommend setting it to 1 day, as opposed to the 24 hour option.
9. Please ensure that any anti-virus, security programs or other scans are not set to scan daily during testing times. You do not have to totally disable auto-scan, but it would be beneficial to set it so it doesn't scan during testing.
10. If the options above do not resolve the issue, then you may also want to apply these settings to the Windows Firewall or any anti-virus program on the local computers. Try it on just one machine first. You can do this in the Windows Firewall by:
    a) Open Internet Explorer
    b) B) Go to the Tools menu and select Internet Options
    c) C) Click on the Privacy tab and then select the Sites button
    d) D) Please add the Domains above [and/or IP Addresses] as sites in that list and select Allow
    e) E) Click OK and then OK again to exit that window
    f) F) Close down Internet Explorer and see if that resolves the issue. Please apply these various settings and let us know if you need further assistance.

NOTE – The anti-virus or security programs would be things such as Norton, MacAfee, AVG, F-Secure, etc. Adjusting the settings for each will vary, but in general you will want to add the Domains or IP Addresses above to that program's list of safe sites or safe zone.