Network Requirements and Guidelines

For details on support changes, see the **Recently Updated** page.

Firewall/Proxy Servers/Content Filtering Requirements

Open the following URLs and ports in any firewalls, proxy servers, or software used for Internet content filtering. In addition to the firewall itself, Pearson recommends checking content filtering and advanced malware configurations for additional places to add whitelist entries.

See the table and tabbed instructions below it to fulfill requirements.

TestNav Test Delivery URLs URL:Port[2]
Your test delivery URL, for example: *.testnav.com:80 *.testnav.com:443
*.pearsontestcontent.com:80 *.pearsontestcontent.com:443
Certificate Authority URLs
*.thawte.com
*.usertrust.com
*.comodoca.com
google-analytics.com (optional)

[2] TestNav content is dynamically hosted in the cloud. No static IP addresses or ranges can be provided.

> For help configuring your specific security products, contact their product support teams. You can also contact Pearson support in the event of technical difficulties during testing.

Expand each service below for general guidelines.

Proxy servers...

Exempt **127.0.0.1** from all proxy services.

Proxy servers can cause delays in TestNav traffic that can sometimes cause communication timeouts. Some web-based content filters can act as a proxy. As a result, Pearson support recommends that you add TestNav URLs to proxy bypass lists, when possible.

Firewalls...

Exempt TestNav URLs from firewall inspection, when possible.

Gateway antivirus inspection, deep packet inspection, reverse DNS checks, gateway SSL decryption/inspection are some firewall services that can interrupt TestNav traffic.

Content Filtering...

Whitelist TestNav URLs within any applicable services.

Security/content filter services can interrupt TestNav traffic. Services such as reverse-DNS checks, SSL decryption/inspection, deep packet inspection, HTTP inspection, blocking audio/multimedia files, and blocking archival files have all been known to cause TestNav interruptions.

Anti-virus...

Exempt TestNav URLs and file directories from antivirus scanning or inspecting.

Install paths vary by platform and installation method. Windows and Mac devices have an additional path where they store minor updates:

- Windows: {user_home}\AppData\Local\Pearson
- Mac: {user_home}/Library/Application Support/Pearson

Some antivirus software uses real-time protection to scan network traffic and file downloads, which may cause issues in test data transfers during secure online testing.

Wireless Network Best Practices

The increase in devices accessing school networks increases the need for stable WiFi networks, daily monitoring, and maintenance. To help network admins stabilize WiFi for online testing and classroom activities, Pearson field engineers collaborated with IT departments to present these requirements, recommendations, and troubleshooting tips.

Minimizing Impact

You can take steps to minimize the network impact.

Before testing:

- Disable low end wireless protocols that are not being used.
- Turn off students' mobile devices to avoid potential interference during testing.

Before the Sign in and preparation phase:

- Ask classrooms to stagger logins to minimize initial loading time.
  For example, in a class of 30 students, the proctor can have 10 students log in each minute, decreasing the strain on the network.

Evaluating Site Readiness

The following information will help you to evaluate and improve your testing readiness.

Conduct a site survey

Evaluate the district's infrastructure, network design, and WiFi needs to determine how many wireless access points (APs) each school will need.

A site survey should include:

- Evaluating the existing infrastructure.
- Counting the number of user devices.
- Examining the type of user traffic and interference.

Design for density

1. **Install APs more densely to decrease potential for overload with too many student devices.**
2. **Reduce WiFi interference from construction materials.**
   Construction materials in schools can impact WiFi coverage and speed. The following solid materials can slow WiFi speed or completely block wireless signals:
   - Brick, concrete, and metal
   - Filing bookshelves
   - Cabinets
3. **If your WiFi access points have adjustable antennas, point the antenna to aim the signal at the student devices to improve the throughput.**
   If possible, move the student devices directly under the AP. Even just couple of feet can make a big difference in throughput and signal strength.
4. **Reduce interference from other WiFi networks.**
   When WiFi networks are set to use the same channel, they compete for limited bandwidth. Check for other WiFi names by opening the wireless options on your device for a list of WiFi networks. If you see many networks to choose from, you may encounter interference from these other networks.
5. **Check your AP user guide to find out whether your APs can detect the least congested WiFi channel.**
6. **Reduce interference from other devices.**
   Electronic devices that are not connected to the school's WiFi network, can still use the same 2.4GHz or 5GHz frequencies to connect. These can include:
   - Cordless phones
   - Bluetooth-enabled devices
   - Student mobile devices
7. **Temporarily turn off or unplug electronics to reduce wireless interference during testing.**
   Personal devices communicate on the network, even while inside backpacks or bags. Email and social media notifications require the devices to send requests to maintain connectivity with the AP.

If you previously had channel auto-switching allowed, but notice slow speeds or poor connections, manually configure the channel and perform speed tests to find the fastest channel.