

# 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 allowlist entries.

See current requirements below:

TestNav Test Delivery URLs:Port
<p><i>TestNav content is dynamically hosted in the cloud. No static IP addresses or ranges can be provided.</i></p> <p>Your test delivery URL, for example:</p> <ul style="list-style-type: none"><li>▪ *.testnav.com:80</li><li>▪ *.testnav.com:443</li><li>▪ *.pearsonusercontent.com:80</li><li>▪ *.pearsonusercontent.com:443</li><li>▪ *.chime.aws<ul style="list-style-type: none"><li>▪ TCP:443</li><li>▪ UDP:3478</li></ul></li><li>▪ *.adamexam.com</li></ul>
ACT Test Delivery URLs:Port
<ul style="list-style-type: none"><li>• *.act.org:80</li><li>• *.act.org:443</li></ul>
Certificate Authority URLs
<ul style="list-style-type: none"><li>▪ *.thawte.com</li><li>▪ *.usertrust.com</li><li>▪ *.comodoca.com</li><li>▪ google-analytics.com (optional)</li></ul>
Tool/Assistive Technology URLs
<p>Co:Writer</p> <ul style="list-style-type: none"><li>▪ *.cowriter.dev</li><li>▪ *.donjohnston.net</li><li>▪ cw-ws.qadji.com</li></ul> <p>Speechstream</p> <ul style="list-style-type: none"><li>▪ *.speechstream.net<ul style="list-style-type: none"><li>◦ toolbar.speechstream.net</li><li>◦ cache.speechstream.net</li><li>◦ speech.speechstream.net</li></ul></li></ul> <p>Prediction</p> <ul style="list-style-type: none"><li>▪ rwgoogle-webservices-7.texthelp.com</li></ul> <p>Microsoft Speech-to-Text</p> <ul style="list-style-type: none"><li>▪ testnav-cognitive-auth.dev.texthelp.com</li></ul> <p>Web Socket</p> <ul style="list-style-type: none"><li>▪ wss://eastus.stt.speech.microsoft.com/</li></ul>
Remote Test Proctoring as a Service (RTPaaS)

- ably.com
- \* rest.ably.io
- \* realtime.ably.io
- \* a.ably-realtime.com, b.ably-realtime.com, c.ably-realtime.com, d.ably-realtime.com, e.ably-realtime.com
- avs.rtpaas.pearson.com
- \* .sd-rtn.com
- \* .edge.sd-rtn.com
- upload.rtpaas.pearson.com
- rtpaas.pearson.com

**Exempt all TCP and UDP ports for the above URLs.**

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
+	Firewalls
+	Content Filtering
+	Anti-Virus

## 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.*

---

Tiny link: <https://support.assessment.pearson.com/x/AxZgAQ>