Online Testing Network & Security Readiness Guide

This guide outlines the network, wireless, and device configurations required for reliable online test delivery. It follows the flow of network traffic—from the external internet connection down to each device—and includes a consolidated testing-day checklist. It is strongly recommended that locations ensure appropriate technical staff are available on test days, including individuals with access and authority to make required changes or assist with troubleshooting.

1. Internet Connection & External Uplink

A stable, high-capacity internet connection prevents loading delays when many candidates begin testing simultaneously.

Required

- Minimum 300 Mbps down and 300 Mbps up available
- Gigabit symmetrical recommended for events with 100+ candidates

Recommended (Optional)

- Backup internet (dual ISP or LTE/5G) recommended
- Ensure uplinks between switches and APs are not undersized (prevents internal bottlenecks)

2. Firewall, Network Filtering & Inspection Controls

Firewall inspection and filtering features can add latency or block secure content. The goal is to reduce load on inspection engines, not bypass security.

Required Ports

- http (80)
- https (443)

Required Domains

- *.starttest.com
- *.starttest2.com
- *.programworkshop.com
- *.programworkshop2.com
- *.gettesting.com
- *.startpractice.com
- *.verifyreadiness.com
- *.webspellchecker.net
- *.starttestrp.com (optional, for remote proctoring)

Filtering and Inspection Adjustments

- Disable HTTPS inspection (decrypts and re-encrypts packets; resource-intensive under load)
- Disable deep packet inspection (reduces latency with encrypted content)

- Disable application-layer filtering (prevents evaluation delays on secure traffic)
- Remove or increase HTTP/HTTPS bandwidth caps (caps slow initial loading for large groups)
- Adjust QoS policies that throttle guest or shared-use networks
- Pause or adjust per-device bandwidth limiting
- Block non-critical traffic such as streaming or gaming

3. DHCP, DNS & Authentication Systems

Stable addressing and predictable device identity prevent repeated login prompts and connection churn.

- DHCP scope supports all devices expected on test day
- DHCP lease duration ≥ 1 day; 48 hours recommended (reduces renewal congestion)
- DNS filters do not block required domains
- Captive portals disabled or streamlined (reduces onboarding delays)

Note: Devices using randomized MAC addresses may trigger additional DHCP requests or repeated authentication prompts. See Section 7 for device-level guidance.

4. Switching, Backhaul & Wired Infrastructure

Internal network performance depends on efficient switching and sufficient uplink capacity.

- Minimize network hops between router and access points
- Ensure backhaul/uplink capacity supports peak test traffic
- Use PoE+ or PoE++ switches for high-performance APs
- Maintain redundant switches in critical areas

5. Network Access Control (NAC) & Local Enforcement Policies

NAC policies may introduce delays or misidentify devices during testing.

- Review NAC posture checks that could slow or block devices
- Pause or adjust per-device rate limits
- Evaluate DNS filtering or enforcement rules affecting BYOD devices
- For institution-owned devices with GPO restrictions, verify that download controls do not block the Secure Browser and that the Secure Browser launches successfully prior to testing.

Note: Randomized MAC addresses can cause NAC systems to misidentify devices. See Section 7 for device-level instructions.

6. Wi-Fi Infrastructure & Configuration

Wi-Fi stability is critical during simultaneous test starts. Proper design reduces interference and supports consistent performance.

SSID Configuration

- Use a dedicated SSID for testing
- Temporary event SSID reduces conflicts with existing policies

Guest Network Practices

- Prioritize test traffic on guest Wi-Fi if used
- Avoid mixing general guest traffic with testing traffic

Filtering at the Wi-Fi Layer

- Disable content filtering on the testing SSID (reduces compounded latency)
- Disable DPI and application-layer controls
- Ensure required ports and domains are unrestricted

Channel and Frequency Management

- Avoid co-channel and adjacent-channel interference
- Use band steering to move capable devices to 5 GHz or 6 GHz
- Use Wi-Fi 6 or Wi-Fi 6E access points where possible
- Enable OFDMA and MU-MIMO

Access Point Density & Performance

- Plan for no more than ~25 active users per AP (reduces airtime contention)
- Use high-density APs with directional antennas where needed
- Enable load balancing and adaptive transmit power
- Discourage personal hotspots to reduce interference

7. End-User Devices & Local Machine Settings

Device configuration affects how content loads and how consistently a device maintains its connection.

Device Requirements

- 1024×768 or higher resolution recommended
- 16-bit color depth or greater recommended
- 802.11n or newer wireless; 802.11ac/ax preferred

Security Software and Background Tasks

- Disable antivirus scans during testing (scans may interrupt loading)
- Disable OS updates and scheduled background tasks
- Confirm that 'Do not save encrypted pages to disk' is not enabled

Private Wi-Fi Address (Apple Devices)

macOS and iPadOS can use randomized MAC addresses for each Wi-Fi network. This may cause repeated authentication, inconsistent NAC enforcement, or DHCP churn. Disable 'Private Wi-Fi Address' on Apple devices during testing to maintain stable identity.

8. Testing Day Checklist

Use this checklist to verify readiness before testing begins. Critical requirements are bolded.

Internet Connection

☐ **Minimum 300 Mbps down/up available**
☐ **Gigabit connection for 100+ candidates**
☐ Backup internet connection ready

Firewall & Traffic Controls

☐ **Ports 80 and 443 open**
☐ **Required domains allowed**
☐ **HTTPS inspection disabled**
☐ **DPI disabled**
☐ **No HTTP/HTTPS bandwidth caps**
☐ **QoS adjusted for testing**
☐ **Non-critical traffic blocked**

DHCP, DNS & Authentication

☐ **DHCP scope supports all devices**
☐ **Lease duration ≥ 1 day (48 hours preferred)**
☐ **DNS filters do not block testing domains**
☐ **Access portals disabled or streamlined**
☐ **Private Wi-Fi Address disabled on Apple devices**

Switching & Backhaul

☐ **Minimal hops between router and APs**
☐ **Backhaul/uplink capacity confirmed**
☐ PoE+ or PoE++ available
☐ Redundant switches ready

NAC & BYOD

☐ **Per-device rate limiting paused**
☐ **DNS filtering relaxed for BYOD if needed**
☐ NAC policies reviewed

Wi-Fi

☐ **Guest Wi-Fi prioritizes testing traffic**
☐ **Band steering enabled**
☐ **≤ 25 users per AP**
☐ Channel plan optimized
☐ Dedicated or event SSID active
☐ Wi-Fi 6/6E available where possible
☐ OFDMA/MU-MIMO enabled
☐ Load balancing active
☐ Hotspots discouraged

Device Readiness

☐ **Resolution ≥ 1024×768**
☐ **16-bit color depth confirmed**
☐ **Background scans/updates disabled**
☐ **Private Wi-Fi Address disabled (Apple devices)**