Saras local network and device configuration guidance

1. Scope

This guidance applied to in-centre assessments only delivered via the Saras platforming using the Respondus Locked Down Browser.

This document does not apply to remote invigilation assessments.

2. Overview

To ensure successful delivery assessment, centres must configure their local networks, devices and security settings appropriately. Failure to do so may result in:

- Inability to launch assessments
- Disrupted assessment sessions
- Loss of learner responses

3. Mandatory Network requirements

Whitelisting for proxy servers, firewalls, and anti-virus

The following URLs must be whitelisted on:

- Firewalls
- Proxy servers
- Antivirus and endpoint protection software

URLs:

- https://assessments-admin.vtctskills.org.uk/TNA/eassessment/#/
- https://assessments.vtctskills.org.uk/TNA/testplayer
- www.googletagmanager.com
- www.google-analytics.com

These URLs must also be added to any ‘safe list’ or ‘allow list’.

IP addresses must not be used as these may change without notice.

SSL inspection/decryption

If SSL inspection/decryption is in place, these URLs must be excluded from SSL inspection to prevent interference with assessment delivery.

Proxy servers and web filtering

If proxy servers or web filtering are used:

- The URLs listed must be configured as exceptions

- These URLs must not be sandboxed or blocked
- Proxy setting must allow standard web traffic required for assessment delivery

Firewall configuration

Firewalls must allow outbound HTTPS (TCP port 443) access to all Saras platform URLs listed above. Where required, centres should contact their IT team or managed service provider to implement this.

4. Device configuration requirements

Respondus Locked Down Browser

All assessments must be delivered using the Respondus Locked Down Browser

- This must be installed on all assessment machines
- No other browser should be used during assessments

Time zone settings

Each assessment device must be set to the correct local time zone. Incorrect time settings may prevent access to assessments or cause submission issues.

System Updates

All Windows / MacOS updates must be completed outside of assessment hours. Devices must be fully updated and restarted prior to assessments. Devices must not begin updates during an assessment session.

Virtual memory and performance

Devices should be restarted regularly and free from excessive background usage. This ensures sufficient memory and stable performance during assessments.

5. File retention requirements

In the event of a technical issue or failed submission, learner responses may need to be recovered and uploaded. Therefore, files generated within the Respondus Locked Down Browser must be retained for a minimum of 14 days after the assessment.

6. Applications and background processes

Before each assessment session:

- All non-essential applications must be closed
- All background processes must be stopped

This includes:

- Software updates
- Scheduled scans
- Antivirus real time scans

The Respondus Locked Down Browser must be the only active application during the assessment.

Processes can be checked via:

- Task Manager (Windows)
- Activity Monitor (Mac)

7. Pre-assessment checks (Mandatory)

Centre must complete the following checks before an assessment session:

- Saras test player URL is accessible
- Respondus Locked Down Browser is installed and launches correctly
- All required URLs are accessible without restriction
- Devices meet the minimum hardware and software requirements
- Devices are fully updated and restarted
- No background applications are running