



FOCUS LOCK

Device Configuration Guide for School and District IT Administrators

Document	Focus Lock Device Configuration Guide
Audience	School and district IT administrators, network administrators, and test coordinators
Applies to	Managed and unmanaged Chromebook, iPad, macOS, and Windows devices used for E-SESS assessments
Companion document	Focus Lock Feature Guide (E-SESS)
Purpose	Prepare testing devices so Focus Lock operates as designed and unintended activations are minimized

CONTENTS

1. Purpose and Scope.....	2
2. What Focus Lock Requires From a Device.....	2
3. Configuration Summary by Platform.....	3
4. Chromebook.....	4
5. iPad.....	6
6. macOS.....	7
7. Windows 10 and Windows 11.....	8
8. Confirming Full Screen Mode Is Allowed.....	9
9. Network and Content Filtering.....	10
10. Pre-Window Verification.....	10
11. Test Day Quick Reference.....	11
12. Support and Escalation.....	11

1. Purpose and Scope

Focus Lock is the browser detection feature built into the E-SESS assessment engine. When a participant clicks Begin, Focus Lock expands the assessment to full screen and monitors whether that window retains focus for the duration of the test. If the participant navigates away, Focus Lock issues a structured sequence of three warnings. If the final warning is not acknowledged within its response window, the assessment is submitted as is.

The feature works as designed. The issues districts report are almost never caused by participant behavior. They are caused by device configuration: a notification banner appearing over the assessment, a background application taking focus without warning, an operating system update starting mid-test, or a browser that has not been permitted to enter full screen. Every one of those conditions is within the control of the IT team, and every one of them can be resolved before a testing window opens.

This guide provides the specific settings required on Chromebook, iPad, macOS, and Windows devices, along with the browser and network checks that confirm full screen mode will be allowed. It is written for the person who administers the devices, not for the person proctoring the room.

1.1 How to Use This Guide

- Start with Section 3 to identify which controls apply to the platforms in your environment.
- Work through the platform section that matches each device image you support.
- Complete Section 8 for every browser participants will use, on every platform.
- Run the verification procedure in Section 10 before the testing window opens, not on test day.
- Keep Section 11 available to proctors and support staff during the window.

Before you begin

Management console menu paths change as vendors update their platforms. Treat the paths in this guide as a reliable starting point and confirm them against current vendor documentation for the version you are running.

Apply and test these settings on one representative device per image, in the same organizational unit or device group participants will test from, before deploying broadly.

2. What Focus Lock Requires From a Device

Three conditions must be true on every testing device. Every recommendation in this guide exists to satisfy one of them.

Requirement	Why It Matters	Consequence If Not Met
Full screen mode is permitted	Focus Lock expands the assessment to full screen automatically when the participant clicks Begin.	The assessment does not launch and the test cannot proceed.

Requirement	Why It Matters	Consequence If Not Met
Notifications are suppressed	An on-screen notification or a pop-up that takes focus is interpreted as navigating away from the test.	A warning is issued, and the assessment may auto-submit if the warning is not acknowledged in time.
Background applications stay quiet	Updaters, mail clients, chat tools, streaming applications, and antivirus scans can all take focus without the participant touching the device.	A warning is issued mid-test with no visible cause, which is difficult for a proctor to explain or resolve in the moment.

Full screen mode is worth particular attention. In addition to being a launch requirement, it materially reduces exposure to the other two conditions by covering notification areas and preventing incidental clicks outside the assessment window.

3. Configuration Summary by Platform

The table below is the working checklist. Detailed procedures for each platform follow in Sections 4 through 7.

Platform	Primary Control	Supporting Controls
Chromebook (managed)	Kiosk mode or managed guest session, configured in the Google Admin Console	Block site notifications, restrict device auto-updates, confirm full screen policy is not blocked, restrict navigation by URL
iPad (supervised)	Single App Mode deployed by MDM, or Guided Access enabled on the device	Enable Do Not Disturb, silence messaging and mail notifications, disable automatic system and app updates
macOS	Do Not Disturb focus, scheduled to cover the testing window	Deploy a notifications configuration profile by MDM, pause software updates, quit background applications, extend display sleep
Windows 10 and 11	Do not disturb (Windows 11) or Focus assist (Windows 10)	Assigned Access kiosk or browser kiosk shortcut, pause Windows Update, disable toast notifications by policy, adjust power plan

4. Chromebook

Managed Chromebooks offer the most complete control of any platform covered in this guide. All settings below are configured in the Google Admin Console and should be applied to the organizational unit that contains your testing devices.

4.1 Kiosk Mode (Recommended)

Kiosk mode launches the assessment as the only application running on the device. There is no shelf, no additional tabs, and no other application available to take focus. This is the single most effective mitigation available on a Chromebook and is strongly recommended for any high-stakes testing window.

Access kiosk settings

1. Sign in to the Google Admin Console using an administrator account.
2. Navigate to Devices, then Chrome, then Apps and extensions, then Kiosks.
3. Select the organizational unit that contains the testing devices.

Add and configure the application

1. Click the add icon and select the option to add by web URL.
2. Enter the E-SESS assessment URL used by your participants.
3. Select the application from the Auto-Launch Kiosk App menu so it starts automatically when the device boots.
4. Save the configuration, then power cycle a test device to confirm the kiosk launches as expected.

Validate the kiosk session before deployment

A web kiosk runs the site in a full screen window with no browser chrome. On a test device, confirm that participants can sign in successfully inside the kiosk session and can still reach any tool they are permitted to use during the assessment.

4.2 Managed Guest Session (Alternative)

If kiosk mode is too restrictive for your workflow, a managed guest session provides a clean, policy-controlled session that discards its state at sign-out. Configure this under Devices, then Chrome, then Settings, then Managed guest session settings. A managed guest session should always be paired with the notification and navigation controls described below, since it does not restrict the device to a single application on its own.

4.3 Supporting Chromebook Settings

Block site notifications

Navigate to Devices, then Chrome, then Settings, then Users and browsers. Locate the notifications content setting and set it to do not allow sites to show desktop notifications. This prevents a notification permission granted previously on an unrelated site from interrupting an assessment.

Confirm full screen is not blocked

Chrome permits full screen by default. If your environment has ever applied the FullscreenAllowed policy, confirm it is set to allow or left unconfigured for the testing organizational unit. Policy inherited from a parent

organizational unit is a common and easily overlooked cause. If your Chrome version exposes the automatic full screen content setting, add the E-SESS domain to the allowed list.

Restrict device auto-updates

Navigate to Devices, then Chrome, then Settings, then Device, and review the device update settings. Use the scatter factor and update restriction options so that ChromeOS updates neither download nor prompt during your testing window.

Restrict navigation

If you are not deploying kiosk mode, consider applying a URL blocklist with an allowlist entry for the E-SESS domain for the duration of the testing window. This is configured under Users and browsers settings and should be removed once testing concludes.

5. iPad

Confirm platform support before committing to iPads

Full screen behavior on iPadOS differs from desktop browsers. Before scheduling a testing window on iPads, run a practice assessment on a representative device and confirm with Pitsco or CTECS that your specific device and browser combination is supported.

5.1 Single App Mode by MDM (Recommended for District-Owned iPads)

Single App Mode locks a supervised iPad to one application. The participant cannot switch applications, and notifications from other applications are suppressed. The device must be supervised through Apple School Manager or Apple Business Manager and enrolled in your mobile device management platform.

1. In your MDM platform, create a configuration profile scoped to the testing device group.
2. Add the Single App Mode or App Lock payload and select the browser or E-SESS application participants will use.
3. Schedule the profile so it applies for the duration of the testing window.
4. Remove or unscope the profile once testing is complete so devices return to normal use.

5.2 Guided Access (On-Device Alternative)

Guided Access is the manual equivalent and can be started by a proctor on any iPad without MDM involvement. It locks the device to the current application until a passcode is entered, which makes it a practical option for schools with unmanaged or mixed device fleets.

1. Open Settings, then Accessibility, then Guided Access, and turn it on.
2. Set a Guided Access passcode that participants do not have access to.
3. Open the assessment, then triple-click the top or home button and tap Start.
4. To end the session, triple-click again and enter the passcode.

5.3 Supporting iPad Settings

Enable Do Not Disturb

Open Settings, then Focus, then Do Not Disturb, and turn it on. For district-managed fleets, push a Focus configuration or use MDM notification settings to silence messaging and mail applications for the testing window rather than relying on participants to set this themselves.

Disable automatic updates

Open Settings, then General, then Software Update, then Automatic Updates, and turn off both automatic downloads and automatic installs. In Settings, then App Store, turn off automatic app updates. Under MDM, apply software update deferral through your update policy.

Review classroom management tools

Confirm that mail, messaging, and classroom management applications are not configured to push banners during the testing window. Classroom management tools that take control of the screen or push an attention command are a frequent cause of unintended activations and are easily overlooked, because the interruption originates from the school rather than from the participant.

6. macOS

macOS provides reliable notification suppression, but the setting is user-controlled by default. On managed fleets, deploying the configuration by MDM is more dependable than instructing participants to enable it.

6.1 Enable Do Not Disturb

1. Open System Settings, then Focus.
2. Select Do Not Disturb and turn it on.
3. Add a schedule that covers the full testing window so the setting does not depend on the participant remembering to enable it.
4. Turn off Share Across Devices so that a phone or tablet cannot toggle the focus off mid-test.

On earlier macOS versions, enable Do Not Disturb through Notification Center preferences. On all versions, review the option that permits notifications while the display is mirrored or shared, and turn it off.

6.2 Deploy Notification Settings by MDM

For managed Macs, a Notifications configuration profile is the preferred approach. Build a profile that disables Notification Center alerts for mail, messaging, collaboration, and update applications, then scope it to the testing device group. This removes the setting from the participant's control entirely and eliminates the most common point of failure.

6.3 Pause Software Updates

Open System Settings, then General, then Software Update, and open the automatic updates detail. Turn off automatic download and install for the duration of the testing window. Under MDM, apply software update deferral so that macOS and application updates cannot install during testing.

6.4 Quit Background Applications

Before the assessment begins, participants should quit mail clients, collaboration and chat tools, streaming and music applications, cloud sync clients, and any calendar or reminder utility. On macOS, closing a window does not quit the application, so confirm applications are fully closed rather than minimized to the dock.

6.5 Additional macOS Considerations

- Set display sleep and screen saver timeouts longer than the maximum test duration.
- Turn off AirDrop and Handoff prompts on shared devices.
- Schedule antivirus and endpoint protection scans outside the testing window.
- On multi-display configurations, confirm the assessment enters full screen on the display the participant is actually using.

7. Windows 10 and Windows 11

Windows presents the widest range of potential interruptions, primarily from Windows Update and from third-party applications that launch at sign-in. Address both centrally where possible.

7.1 Enable Do Not Disturb or Focus Assist

Windows 11

1. Open Settings, then System, then Notifications.
2. Turn on Do not disturb.
3. Expand the automatic rules and set a schedule covering the testing window.

Windows 10

1. Open Settings, then System, then Focus assist.
2. Select Alarms only, which suppresses all other notifications.
3. Under automatic rules, add a time window covering the assessment period.

7.2 Suppress Notifications by Policy

For managed fleets, apply this centrally rather than device by device. In Group Policy, under User Configuration, Administrative Templates, Start Menu and Taskbar, enable the policy that turns off toast notifications. Intune administrators can achieve the same outcome through a settings catalog policy scoped to the testing device group.

7.3 Control Windows Update

Windows Update restarts and update notifications are among the most common causes of an unexplained Focus Lock warning, and they typically affect an entire lab at once.

- Set active hours to cover the school day so restarts cannot occur during testing.
- Pause updates for the testing window under Settings, then Windows Update, then Advanced options.
- For managed devices, configure update rings with deadlines and deferral periods that fall outside your testing calendar.

7.4 Kiosk Options

Assigned Access

Assigned Access configures a Windows device to run a single application in a locked-down account. Open Settings, then Accounts, then Other users, and set up a kiosk. Select Microsoft Edge and configure it to launch the E-SESS assessment URL. This configuration can also be deployed at scale through Intune or a provisioning package.

Browser kiosk shortcut

A lighter alternative that requires no account changes is launching the browser directly into kiosk mode from a shortcut. Create a desktop shortcut that calls the browser executable with the kiosk switch followed by the assessment URL. The browser opens full screen with no address bar and no tabs. Confirm the shortcut behaves correctly on your standard image before distributing it.

7.5 Additional Windows Considerations

- Close Outlook, Teams, and any other collaboration client before the assessment begins.
- Set the power plan so the display and system do not sleep within the maximum test duration.
- Schedule antivirus scans and third-party updaters, including Java, Adobe, and printer utilities, outside the testing window.
- Disable auto-launch of vendor support and driver update tools on managed images.

8. Confirming Full Screen Mode Is Allowed

Focus Lock cannot launch an assessment if the browser will not enter full screen. When full screen is blocked, the participant clicks Begin and the assessment simply does not proceed, which is difficult to diagnose in the moment. Verify the following for every browser participants will use, on every platform.

Browser	What to Verify	Notes
Chrome and Edge	Full screen is permitted by default. Confirm no enterprise policy blocks it, and that the E-SESS domain is allowed under the automatic full screen content setting if your version exposes it.	Verify at the policy level rather than only on the device. The browser policy page on a test device will show what is actually applied.
Safari (macOS)	Confirm no extension or accessibility utility is intercepting full screen, and that the assessment window is not in a Space or Stage Manager configuration that prevents it.	Test on a device carrying your standard extension set, not a clean profile.
Firefox	Full screen is enabled by default. Confirm the full screen API has not been disabled in a hardened configuration file or enterprise policy.	Review any customized policy file deployed to your standard image.
Safari (iPadOS)	Full screen behavior differs from desktop browsers. Validate with a practice assessment before the live window.	Guided Access or Single App Mode serves as the functional equivalent of a full screen lock on iPadOS.

8.1 Common Causes of Full Screen Failure

- Browser extensions that overlay content, including grammar checkers, ad blockers, screen readers, and screenshot utilities.
- Pop-up blockers configured more aggressively than the browser default.
- Content filters or proxy tools that inject a frame or banner into the page.
- Kiosk or classroom management software that reserves part of the screen for a persistent toolbar.
- Enterprise policy applied at a parent organizational unit and inherited by the testing unit without review.

Quick verification

On a representative device, open the assessment platform and confirm the browser enters full screen when prompted. If the window expands and hides the address bar and tabs, full screen is permitted. If nothing happens, resolve the cause before test day rather than during it.

9. Network and Content Filtering

The Processing screen in E-SESS indicates the device has lost its internet connection. Intermittent connectivity produces the same symptom, which means filtering behavior and wireless stability matter as much as available bandwidth.

- Allow the E-SESS assessment domains through your content filter, firewall, and any SSL inspection appliance. Confirm the current domain list with Pitsco or CTECS before the testing window opens.
- Exclude assessment traffic from SSL inspection if inspection is contributing to session interruptions.
- Confirm wireless coverage and access point capacity in the rooms being used, at the device density you will actually be testing at.
- Avoid scheduling large image deployments, backups, or software distribution during testing windows.

If a Processing screen appears, the assessment remains unlocked. The participant should reconnect to the network, refresh the browser, and continue from where they left off. Pitsco, CTECS, or a CTECS-approved administrator can adjust the test duration if time was lost.

10. Pre-Window Verification

Configuration that has not been tested on the actual device image is an assumption rather than a control. Complete this procedure once per device type before the testing window opens.

Step	What to Confirm
1. Launch a practice assessment	The assessment expands to full screen automatically when Begin is clicked.
2. Sit idle for several minutes	No notification, banner, or update prompt appears on screen.
3. Deliberately navigate away	The Focus Lock warning appears as expected, confirming the feature is active.
4. Return and acknowledge	The warning clears and the assessment resumes normally.
5. Hold for the full duration	The display does not sleep and the screen saver does not engage within the maximum test length.
6. Repeat for each image	Every distinct device model, operating system version, and organizational unit is validated separately.

11. Test Day Quick Reference

Provide this table to proctors and building-level support staff. Most issues resolve locally without escalation.

Symptom	Likely Cause	First Action
Assessment does not start after clicking Begin	Full screen is blocked by policy, an extension, or a browser setting	Check applied browser policy and disable extensions on the affected device
Warning appears with no participant action	A background application or notification took focus	Identify and quit the application, then confirm do not disturb is active
Warnings across an entire lab at once	A scheduled update, scan, or management push fired	Check update and deployment schedules, then pause the task in progress
Processing screen	The device lost its internet connection	Reconnect to the network, refresh the browser, and continue the test
Assessment submitted automatically	The third warning expired without acknowledgement	Escalate to Pitsco, CTECS, or a CTECS-approved administrator

12. Support and Escalation

Technical support is available during assessments to assist with unintended Focus Lock activations. Route device and network issues through your local IT team first, since the majority of causes are configuration issues that can be resolved on site. Escalate to Pitsco or CTECS for test reopening, duration adjustments, and platform questions.

Local reference

District IT contact: _____

Test coordinator: _____

E-SESS assessment URL: _____

Testing window dates: _____